Administration Guide

FortiEDR 7.2.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

FORTINET®

February 25, 2026
FortiEDR 7.2.0 Administration Guide
63-720-1167914-20260225

TABLE OF CONTENTS

Change log

Date	Change Description
2025-09-29	Initial release.
2025-10-10	Updated the following: • FortiAnalyzer or FortiAnalyzer Cloud on page 358 • Introducing the Incidents view on page 85 • Audit Trail on page 314
2025-10-24	• Added Generating reports on page 83. • Updated Installing a FortiEDR Collector on Linux on page 53 and Introducing the Incidents view on page 85.
2025-11-17	Updated Setting up a VM to be the FortiEDR Aggregator on page 481 and Setting up a VM to be the FortiEDR Central Manager on page 465.
2025-11-24	Updated Requesting and obtaining a mobile installer on page 412 and Appendix C – ON PREMISE DEPLOYMENTS on page 459.
2025-11-25	Updated Host Firewall Collector 6.1 or later on page 194 and Appendix C – ON PREMISE DEPLOYMENTS on page 459.
2025-12-09	Updated Setting up the FortiEDR reputation server on page 508 and Appendix C – ON PREMISE DEPLOYMENTS on page 459
2026-01-07	Updated Appendix C – ON PREMISE DEPLOYMENTS on page 459 and Disk Encryption Collector 6.1 or later on page 253.
2026-01-09	Added Deployment URL on page 316.
2026-01-12	Updated Disk Encryption Collector 6.1 or later on page 253.
2026-02-06	Updated Sandbox integration on page 356 and Using FortiEDR - workflow on page 17.
2026-02-02	Updated Inventory on page 256.
2026-02-06	Updated Setting up the FortiEDR Core on page 511.
2026-02-20	Updated Host Firewall Collector 6.1 or later on page 194.

Introducing FortiEDR

This chapter describes the FortiEDR system components, FortiEDR technology and the workflow for protecting your organization using FortiEDR.

Introduction

FortiEDR provides multi-layered, post- and pre-infection protection that stops advanced malware in real time. FortiEDR recognizes that external threat actors cannot be prevented from infiltrating networks, and instead focuses on preventing the exfiltration and ransoming of critical data in the event of a cyber-attack. FortiEDR's unique virtual patching technique, which only blocks malicious outbound communications, enables employees to continue working as usual even when their devices are infected.

Execution prevention

FortiEDR stops both known and unknown malware types using machine-learning-based Next-Generation Anti-Virus (NGAV), a signature-less approach that detects and mitigates zero-day attacks by filtering out known malware variations. This blocks the execution of files that are identified as malicious or suspected to be malicious. For this policy, each file is analyzed to find evidence for malicious activity.

In addition to machine-learning-based NGAV protection, Execution Prevention policy is augmented by other techniques such as signature-based detection, sandboxing, and more.

Data exfiltration

Data exfiltration is the unauthorized transfer of sensitive information from a target’s network to a location that a threat actor controls.

FortiEDR is a realtime targeted-attack exfiltration prevention platform.

Threat actors only benefit when they actually succeed in stealing your data.

FortiEDR ensures that your data is not exfiltrated by threat actors, regardless of the methods that they use.

FortiEDR can prevent malicious exfiltration attempts of any kind of data, from any application, from any process, using any protocol or port.

FortiEDR becomes your last line of defense in case of a data exfiltration attempt. All malicious connections are blocked and precise details of the infected devices and their associated components are available for your review.

FortiEDR is a software-only solution that can be installed with your current standard equipment.

FortiEDR protects your data from exfiltration both On-Premises and Off-Premises.

Ransomware

Ransomware is malware used by attackers to infect a device, hijack files on that device and then lock them, via encryption, so that they cannot be accessed until the attacker decrypts and releases them. A successful ransomware attack represents the exploit of a greater security vulnerability in your environment. Paying the attacker is only a short-term solution that does not address the root of the problem, as it may likely lead to another attack that is even more malicious and more expensive than the previous one.

FortiEDR prevents, in real time, an attacker’s attempt to encrypt or modify data. FortiEDR then generates an alert that contains the information needed to initiate an investigation, so the root breach can be uncovered and fully remediated. Moreover, the end user can continue to work as usual even on an infected device.

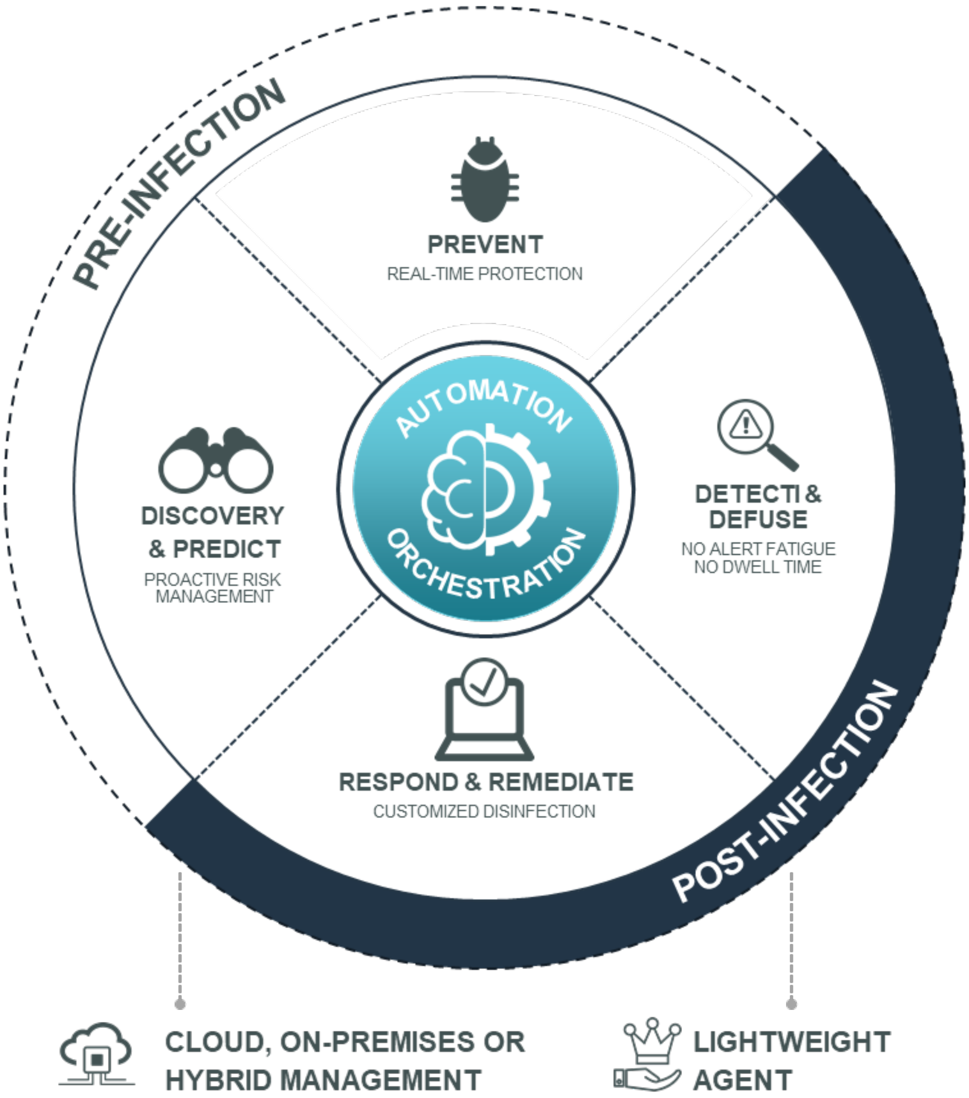
Threat hunting

FortiEDR’s threat-hunting capabilities features a set of software tools and information sources focused on detecting, investigating, containing and mitigating suspicious activities on end-user devices.

FortiEDR provides post- and pre-infection endpoint protection management, while delivering high detection rates with realtime blocking and response capabilities when compared to traditional Endpoint Detection and Response (EDR) tools.

FortiEDR provides malware classification, displays Indicators of Compromise (IOCs) and delivers full attack-chain views – all while simultaneously enabling users to conduct further threat hunting, if and when needed.

FortiEDR technology



When looking at how external threat actors operate, we recognize two important aspects. The first is that the threat actors use the network in order to exfiltrate data from an organization. Second, they try to remain as stealthy as possible in order to avoid existing security measures. This means that threat actors must establish outbound communications in a non-standard manner.

FortiEDR's technology prevents data exfiltration by identifying, in real time, malicious outgoing communications that were generated by external threat actors. Identification of malicious outgoing communications is the result of our research conducted on both operating system internals and malware operation methods.

Our research revealed that all legitimate outgoing communications must pass through the operating system. Thus, by monitoring the operating system internals it is possible to verify that a connection was established in a valid manner. FortiEDR gathers OS stack data, thread and process related data and conducts executable file analysis to determine the nature of the connection. Additionally, any type of threat attempting to bypass the FortiEDR driver is detected as the connection will not have the corresponding data from FortiEDR.

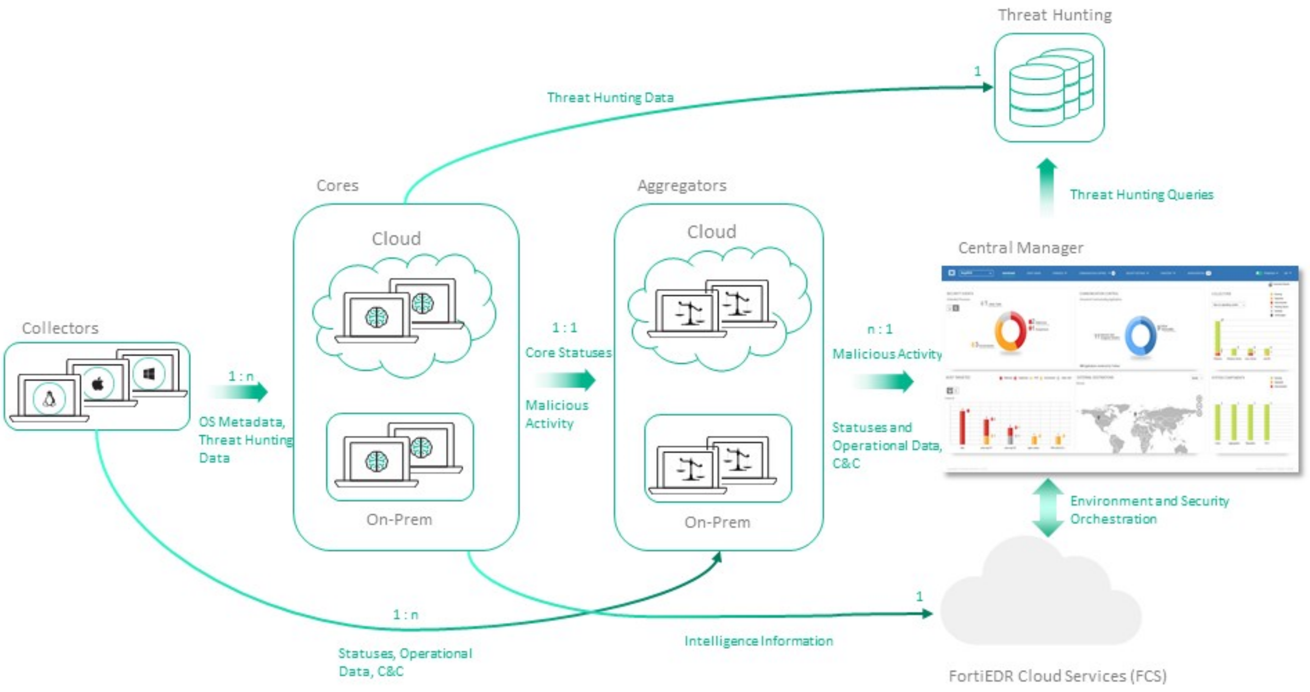
FortiEDR's technology prevents data exfiltration by identifying, in real time, malicious outgoing communications that were generated by external threat actors. Identification of malicious outgoing communications is the result of our research conducted on both operating system internals and malware operation methods.

FortiEDR components

Overview

The FortiEDR platform is a distributed architecture that collects the connection establishment flow of your organization's communicating devices directly from each device's operating system internals. FortiEDR analyzes the flow of events that preceded the connection establishment and determines whether the connection establishment request was malicious. The system can enforce your organization's policy by blocking the connection establishment request in order to prevent exfiltration.

The FortiEDR platform is comprised of the following components:



FortiEDR Collector

The FortiEDR Collector is an agent that resides on every communicating device in your enterprise, including desktops, laptops and servers.

By default, the Collector runs in autonomous mode. Upon every attempt made by the communicating device to establish a network connection or change a file, the Collector collects all required metadata and analyzes it to determine whether the process performing the action is legitimate. You can configure the Collector to use a Core for the metadata analysis, in which case the Collector holds the establishment of the connection until authorization is received from the Core.

- **Pass**: Legitimate requests are allowed with extremely negligible latency.
- **Block**: Malicious exfiltration and file changing attempts are blocked.

If third-party software attempts to stop the FortiEDR Collector service, the system prompts for the registration password. This is the same password used when installing the Collector. If an incorrect password is supplied at the prompt, the message Access Denied displays on the Collector device. In this case, the FortiEDR Collector service is not stopped. For more details about the required password to supply in this situation, you may refer to Component Authentication on page 316.

A FortiEDR Collector should be installed on each communicating device in your organization. The same FortiEDR Collector can be installed on all Windows, macOS, and Linux systems. The following are the connections established between the FortiEDR Collector and other FortiEDR components:

- **To the FortiEDR Aggregator**: The FortiEDR Collector initially sends registration information to the FortiEDR Aggregator via SSL and then it sends ongoing health, status information, and security events.
- **From the FortiEDR Aggregator**: The FortiEDR Collector receives its configuration from the FortiEDR Aggregator.
- **To the FortiEDR Core**: The FortiEDR Collector sends the following information:
  - Compressed activity events that are later used for Threat Hunting
  - Communication-related data to be used for the Communication Control
  - **(Non-autonomous mode only)** Metadata for determining whether a specific action should be blocked or passed

  When a Core is used for the metadata analysis, which means the Collector is not running in autonomous mode, if all Cores are unreachable due to connection issues or errors, the Collector switches to autonomous mode automatically after one minute where it continues to run and protect the device by analyzing the metadata locally. The Collector then keeps trying to establish a connection with the Core every few seconds to few minutes, depending on the number of errors in previous attempts.

- **From the FortiEDR Core**: The FortiEDR Collector receives connection establishment authorization or denial (blocking) from the FortiEDR Core.

Negligible footprint

The FortiEDR Collector retains only a limited amount of metadata on the device in order to keep CPU usage to virtually zero and the storage requirements to a minimum. FortiEDR's traffic consumption requirements are low because the FortiEDR Collector sends to the Core its activity events, the size of which depends on the amount of activity, and sends to the Aggregator security events which are small in size. Additionally, FortiEDR uses message compression in order to further reduce the traffic sent to the network. You may refer to Collector System Requirements for the exact specifications of the system requirements.

Quick and easy installation

The FortiEDR Collector comes as a standard installer package that is easily installed via standard remote unattended deployment tools, such as Microsoft SCCM. No local configuration or reboot is required; however, a reboot of the system ensures that any malicious connections that were previously established before the installation are thwarted and tracked via FortiEDR after the reboot is complete. Upgrades can be performed remotely and are rarely needed, because all the brains of the FortiEDR system are in the FortiEDR Core.

Incidents view

The Windows *Incidents* view records whenever a FortiEDR Collector blocks communication from a device, as described in Incidents on page 85.

FortiEDR Core

The FortiEDR Core is the security policy enforcer and decision-maker. It determines whether a connection establishment request is legitimate or represents a malicious exfiltration attempt that must therefore be blocked.

FortiEDR collects OS stack data, thread and process-related data and conducts executable file analysis to determine the nature of every connection request, as follows.

- When working in prevention mode, all the connection establishment requests in your organization must be authorized by a FortiEDR Core, thus enabling it to block each outgoing connection establishment request that is malicious.
- When the FortiEDR Core receives a connection establishment request, it comes enriched with metadata collected by the FortiEDR Collector that describes the operating system activities that preceded it.
- The FortiEDR Core analyzes the flow of events that preceded the connection request and determines whether the connection request was malicious. The system then enforces your organization's policy by blocking (or only logging) the connection request in order to prevent/log exfiltration.
- The collection of the flow of events that preceded the connection request enables FortiEDR to determine where the foul occurred.

One or more FortiEDR Cores are required, according to the size of your network based on deployment size (up to 50 FortiEDR Cores). Refer to Appendix C – ON PREMISE DEPLOYMENTS on page 459 for the exact specifications of the system requirements.) The following are the connections established between the FortiEDR Core and other FortiEDR components:

- **To the FortiEDR Aggregator**: The FortiEDR Core sends registration information the first time it connects to the FortiEDR Aggregator and then sends events and ongoing health and status information.
- **From the FortiEDR Aggregator**: The FortiEDR Core receives its configuration from the FortiEDR Aggregator.

The FortiEDR Core is located on exit points from your organization. It only reviews FortiEDR Collector metadata; it does not see the outgoing traffic. It is a central Linux-based software-only entity that can run on any workstation or VM that is assigned with a static IP address.

FortiEDR Aggregator

The FortiEDR Aggregator is a software-only entity that acts as a proxy for the FortiEDR Central Manager and provides processing load handling services. All FortiEDR Collectors and FortiEDR Cores interact with the Aggregator for registration, configuration and monitoring purposes. The FortiEDR Aggregator aggregates this information for the FortiEDR Central Manager and distributes the configurations defined in the FortiEDR Central Manager (such as exceptions, policies, and rules) to the FortiEDR Collectors and FortiEDR Cores. The configuration update latency is usually around 60-120 seconds but can take up to 20 minutes in edge cases.

Most deployments only require a single FortiEDR Aggregator. Additional FortiEDR Aggregators may be required for larger deployments of over 10,000 FortiEDR Collectors.

FortiEDR Central Manager

The FortiEDR Central Manager is a software-only central web user interface and backend server for viewing and analyzing events and configuring the system. Chapters from Security Settings on page 196 to Threat Hunting on page 125 describe the user interface of the FortiEDR Central Manager. The FortiEDR Central Manager is the only component that has a user interface. It enables you to:

- Control and configure FortiEDR system behavior
- Monitor and handle FortiEDR events
- Perform deep forensic analysis of security issues
- Monitor system status and health

FortiEDR Cloud Service

The FortiEDR Cloud Service (FCS) enriches and enhances system security by performing deep, thorough analysis and investigation about the classification of a security event. The FCS is a cloud-based, GDPR-compliant, software-only service that determines the exact classification of security events and acts accordingly based on that classification – all with a high degree of accuracy.

The FCS security event classification process is done via data enrichment and enhanced deep, thorough analysis and investigation, enabled by automated and manual processes. The enhanced processes may include (partial list) intelligence services, file analysis (static and dynamic), sandboxing, flow analysis via machine learning, commonalities analysis, crowdsourced data deduction and more.

Along with potential classification reassurance or reclassification, once connected, FCS can also enable several followed actions, which can be divided into two main activities:

- Tuning: Automated security event exception (allowlisting). After a triggered security event is reclassified as Safe, an automated cross-environment exception can be pushed downstream and expire the event, preventing it from triggering again. For more details, see Exception Manager on page 207
- Playbook Actions: All Playbook policy remediation actions are based on the final determination of the FCS. For more details see Remediation on page 251.

How does FortiEDR work?

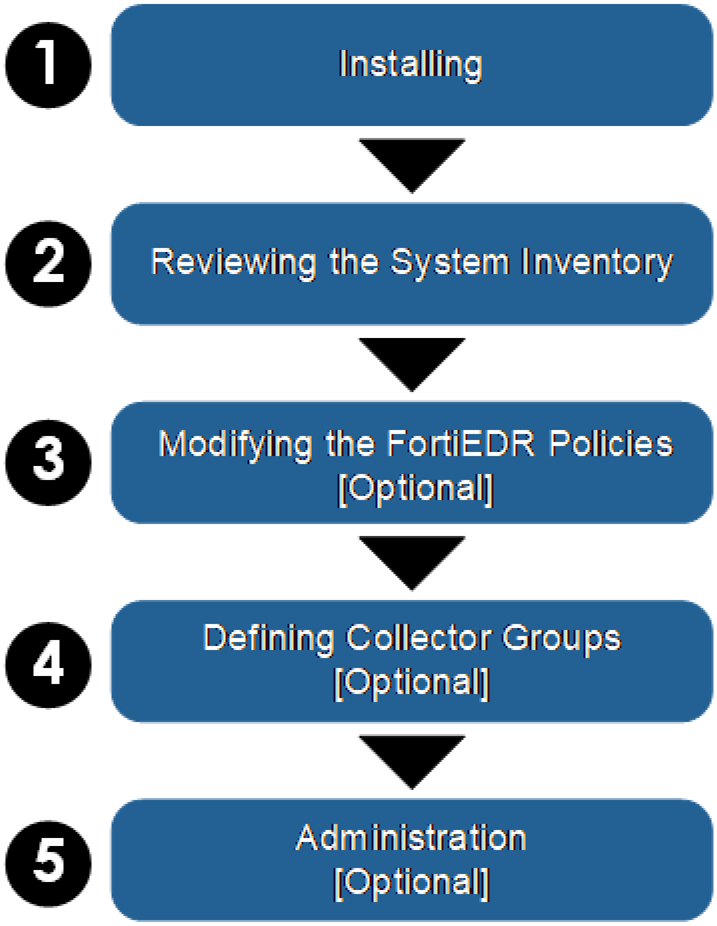
1. **The FortiEDR Collector collects OS metadata**: A FortiEDR Collector runs on each communicating device in the organization and transparently collects OS metadata on the computing device.
2. **Communicating device makes a connection establishment request**: When any connection establishment request is made on a device, the FortiEDR Collector sends a snapshot of the OS connection establishment to the FortiEDR Core, enriched with the collected OS metadata. Meanwhile, FortiEDR does not allow the connection request to be established.
3. **The FortiEDR Core identifies malicious requests**: Using FortiEDR’s patented technology, the FortiEDR Core analyzes the collected OS metadata and enforces the policies.
4. **Pass or block**: Only legitimate connections are allowed outbound communication. Malicious outbound connection attempts are blocked.
5. **Event Generation**: Each FortiEDR policy violation generates a realtime security event (alert) that is packaged with an abundance of device metadata describing the internals of the operating system leading up to the malicious connection establishment request. This security event is triggered by the FortiEDR Core and is viewable in the FortiEDR Central Manager console. FortiEDR can also send email alerts and/or be integrated with any standard Security Information and Event Management (SIEM) solution via Syslog.
6. **Forensic analysis**: The Forensic Analysis add-on enables the security team to use the various options provided by the FortiEDR Central Manager console to delve deeply into the actual security event and the internal stack data that led up to it.

Using FortiEDR - workflow

The following is a general guideline for the general workflow of using FortiEDR and specifies which steps are optional.

Setup workflow overview

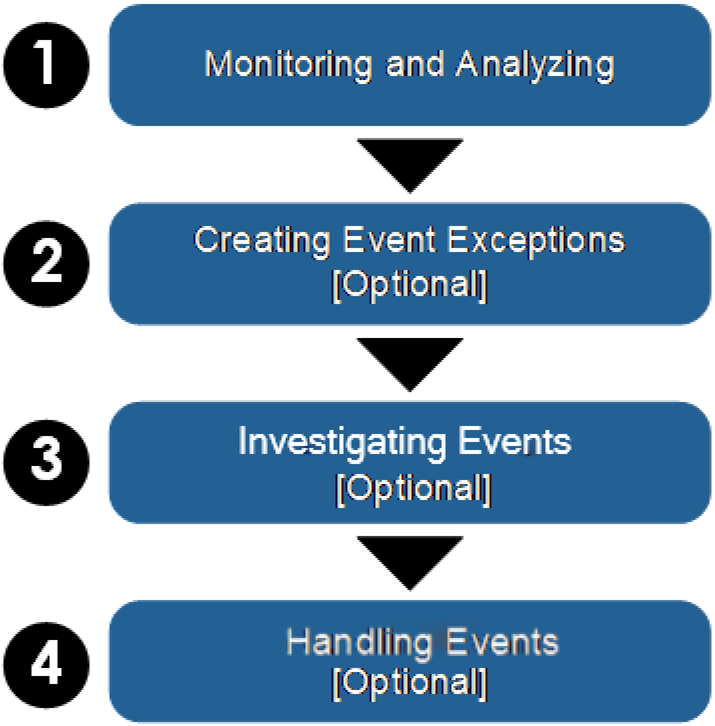
The following describes the workflow for getting FortiEDR up and running in your organization:


1
Installing
2
Reviewing the System Inventory
3
Modifying the FortiEDR Policies [Optional]
4
Defining Collector Groups [Optional]
5
Administration [Optional]

1. **Installing**: Install all FortiEDR components, as described in Installing FortiEDR Collectors on page 23 and Appendix C – ON PREMISE DEPLOYMENTS on page 459.
2. **Reviewing the Inventory**: Review the health status and details of all the FortiEDR components in the Dashboard on page 75 and Assets on page 256. FortiEDR Collectors are automatically assigned FortiEDR's default policies.
3. **[Optional] Modifying the FortiEDR Policies**: By default, the FortiEDR policies are ready to log out-of-the-box. If needed, use the Security Settings on page 196 to modify the default policies for blocking and/or to create additional policies.
4. **[Optional] Defining Collector Groups**: By default, the FortiEDR default policies are assigned to a default Collector Group that contains all FortiEDR Collectors. Policies in FortiEDR are assigned per Collector Group. You can define additional Collector Groups in . You can then assign the required policy to each Collector Group (see Assigning a security policy to a Collector Group on page 205)
5. **[Optional] Administration**: The FortiEDR system installs with a single administrator user. This user can:
   - Create additional users of the FortiEDR Central Manager.
   - Define the recipients to receive email notifications of FortiEDR events.
   - Configure a SIEM to receive notifications of FortiEDR events via Syslog.

Ongoing workflow overview

The following is the workflow for monitoring and handling FortiEDR security events on an ongoing basis:



- **Monitoring**: Monitor and analyze the events triggered by FortiEDR in the following locations:
  - Dashboard on page 75
  - Incidents on page 85
  - Syslog on page 310
- **[Optional] Creating Event Exceptions**: FortiEDR precisely pinpoints interesting system events. However, if needed, you can create exceptions in order to stop certain events from being triggered for certain IP addresses, applications, protocols and so on. See Playbook policies on page 244.
- **[Optional] Investigating Events**: Deep investigation into a security event, including meta data. With a Threat Hunting on page 125 license add-on, you can also audit all operating system activities.
- **[Optional] Handling Events**: Mark security events that you have handled and optionally describe how they were handled. See Marking a security event as handled/unhandled on page 115.

Deploying FortiEDR Cloud

This topic explains how to deploy FortiEDR Cloud. This topic assumes that you already purchased the desired subscription licenses for your deployment from a Fortinet partner or reseller and received your license activation codes.

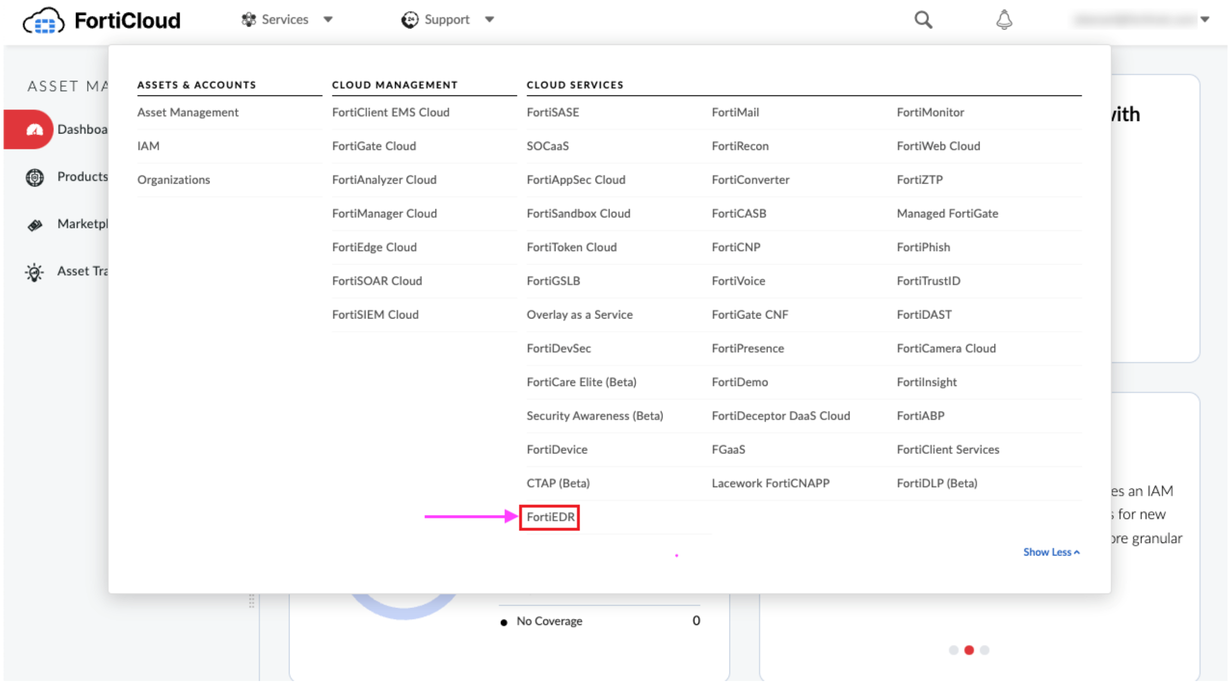
You can create only one FortiEDR Cloud instance per FortiCloud account.

To deploy FortiEDR Cloud:

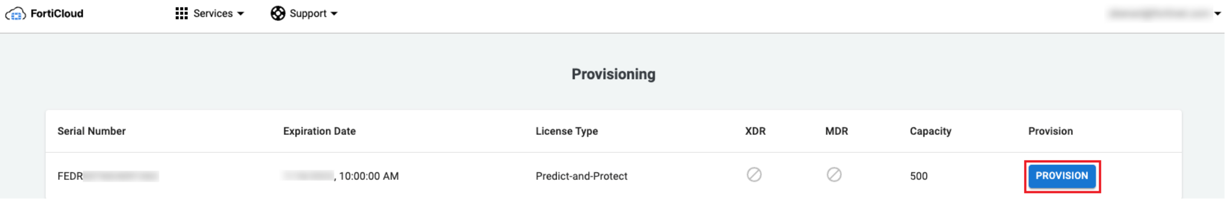
1. Register the FortiEDR Cloud subscription contract to your FortiCloud account:
   a. On the Customer Service & Support site, go to *Asset Management > Register Now*.
   b. In the *Registration Code* field, enter your license activation code and select *Next* to continue registering the product.
   c. Enter your details in the other fields and complete the registration.

   You may need to wait a few minutes for the cloud instance to initialize before you can proceed.

2. Provision your FortiEDR Cloud environment:
   a. In FortiCloud, go to *Services > Cloud Services* and click *FortiEDR*.



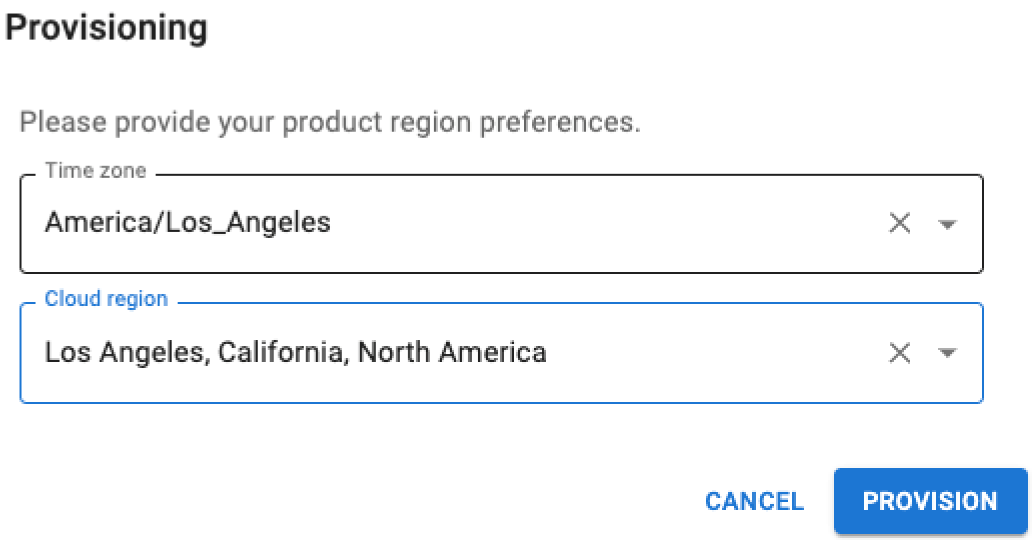
b. Click *PROVISION*.



Provisioning

Serial Number	Expiration Date	License Type	XDR	MDR	Capacity	Provision
FEDR[redacted]	[redacted], 10:00:00 AM	Predict-and-Protect	⊘	⊘	500	PROVISION

c. Select the time zone and cloud region to provision your FortiEDR Cloud instance.



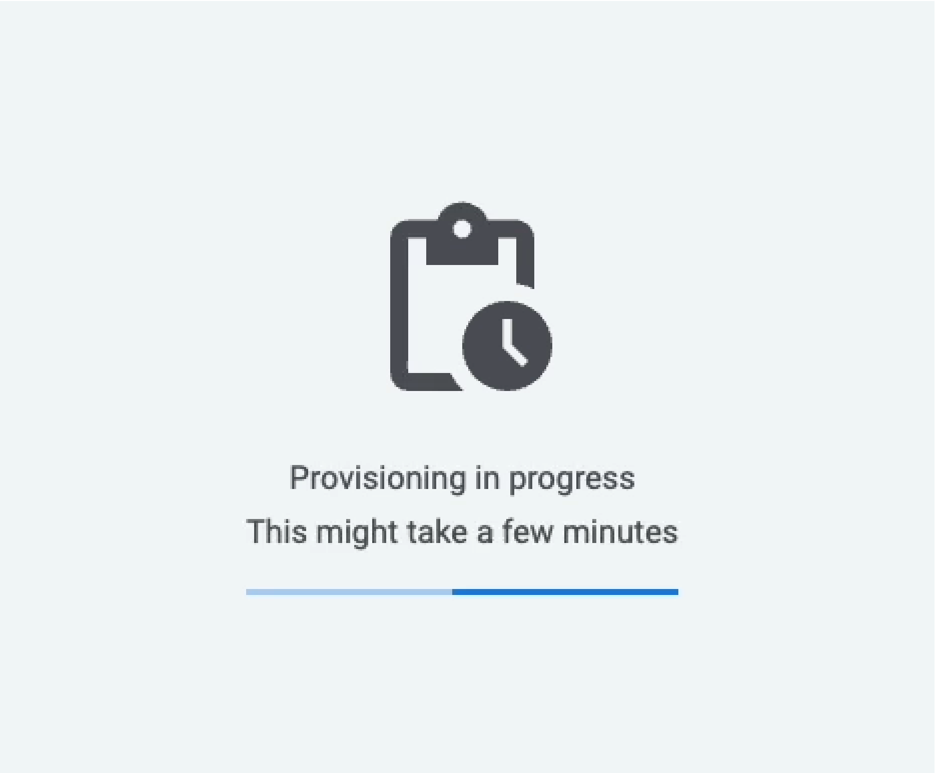
Provisioning

Please provide your product region preferences.

Time zone: America/Los_Angeles

Cloud region: Los Angeles, California, North America

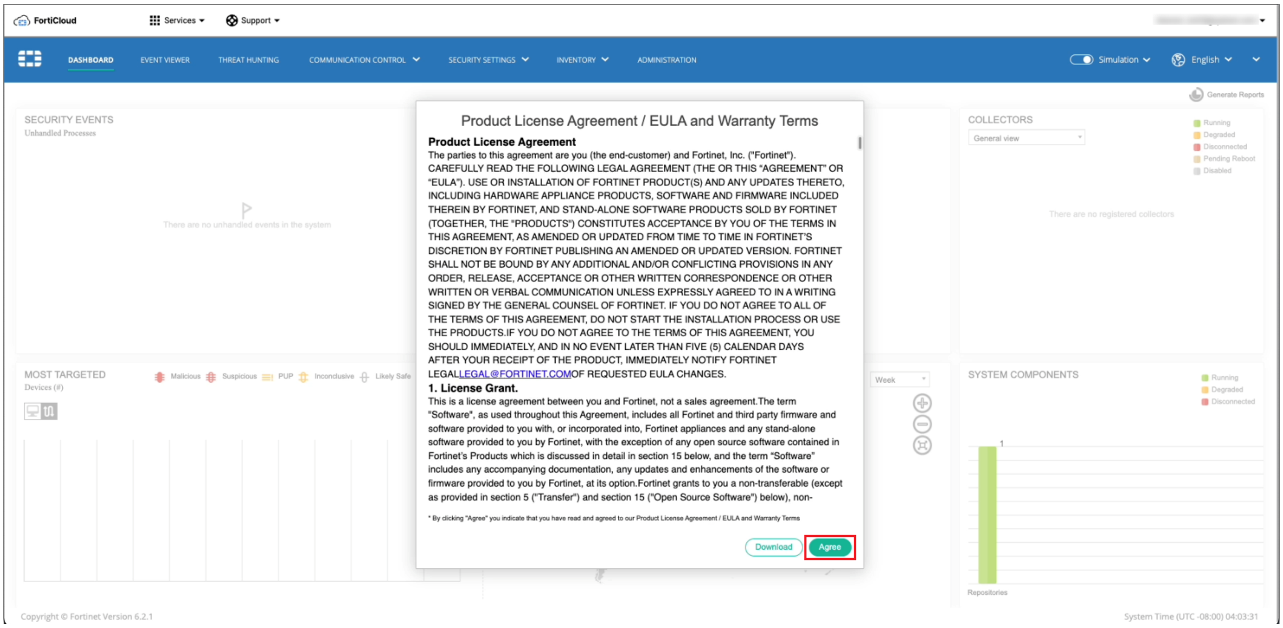
d. Click *PROVISION* to start the provisioning process, which takes about 5 minutes for a new organization in a shared environment and 40 minutes for a dedicated environment.



Provisioning in progress

This might take a few minutes

3. After the provisioning process is complete and the environment is ready, click *Agree* to access the FortiEDR Central Manager console.



Product License Agreement / EULA and Warranty Terms

Product License Agreement

The parties to this agreement are you (the end-customer) and Fortinet, Inc. ("Fortinet"). CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT (THE OR THIS “AGREEMENT” OR “EULA”). USE OR INSTALLATION OF FORTINET PRODUCT(S) AND ANY UPDATES THERETO, INCLUDING HARDWARE APPLIANCE PRODUCTS, SOFTWARE AND FIRMWARE INCLUDED THEREIN BY FORTINET, AND STAND-ALONE SOFTWARE PRODUCTS SOLD BY FORTINET (TOGETHER, THE "PRODUCTS") CONSTITUTES ACCEPTANCE BY YOU OF THE TERMS IN THIS AGREEMENT, AS AMENDED OR UPDATED FROM TIME TO TIME IN FORTINET’S DISCRETION BY FORTINET PUBLISHING AN AMENDED OR UPDATED VERSION. FORTINET SHALL NOT BE BOUND BY ANY ADDITIONAL AND/OR CONFLICTING PROVISIONS IN ANY ORDER, RELEASE, ACCEPTANCE OR OTHER WRITTEN CORRESPONDENCE OR OTHER WRITTEN OR VERBAL COMMUNICATION UNLESS EXPRESSLY AGREED TO IN A WRITING SIGNED BY THE GENERAL COUNSEL OF FORTINET. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, DO NOT START THE INSTALLATION PROCESS OR USE THE PRODUCTS.IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, YOU SHOULD IMMEDIATELY, AND IN NO EVENT LATER THAN FIVE (5) CALENDAR DAYS AFTER YOUR RECEIPT OF THE PRODUCT, IMMEDIATELY NOTIFY FORTINET LEGALLEGAL@FORTINET.COMOF REQUESTED EULA CHANGES.

1. License Grant.

This is a license agreement between you and Fortinet, not a sales agreement.The term "Software", as used throughout this Agreement, includes all Fortinet and third party firmware and software provided to you with, or incorporated into, Fortinet appliances and any stand-alone software provided to you by Fortinet, with the exception of any open source software contained in Fortinet’s Products which is discussed in detail in section 15 below, and the term “Software” includes any accompanying documentation, any updates and enhancements of the software or firmware provided to you by Fortinet, at its option.Fortinet grants to you a non-transferable (except as provided in section 5 ("Transfer") and section 15 ("Open Source Software") below), non-

* By clicking "Agree" you indicate that you have read and agreed to our Product License Agreement / EULA and Warranty Terms

Download Agree

Deploying FortiEDR Collectors

This chapter describes how to deploy FortiEDR Collectors, which is the only component you need to install for FortiEDR cloud deployment. All backend components, including FortiEDR Central Manager, Aggregator, Threat Hunting Repository, and Core, are installed and managed in the cloud by Fortinet.

- Installing FortiEDR Collectors on page 23
- Uninstalling FortiEDR Collectors on page 70
- Upgrading the Collector on page 73

If you want to deploy any of the backend components on your organization's premises (on-premises), see Appendix C – ON PREMISE DEPLOYMENTS on page 459.

Installing FortiEDR Collectors

You can install the FortiEDR Collector on any communicating device that meets the requirements in Collector System Requirements. Your license determines the number of FortiEDR Collectors allowed to register with the FortiEDR Central Manager. When you reach the maximum number of Collectors, you must uninstall a FortiEDR Collector from a device and delete it from the FortiEDR INVENTORY before you can add another FortiEDR Collector.

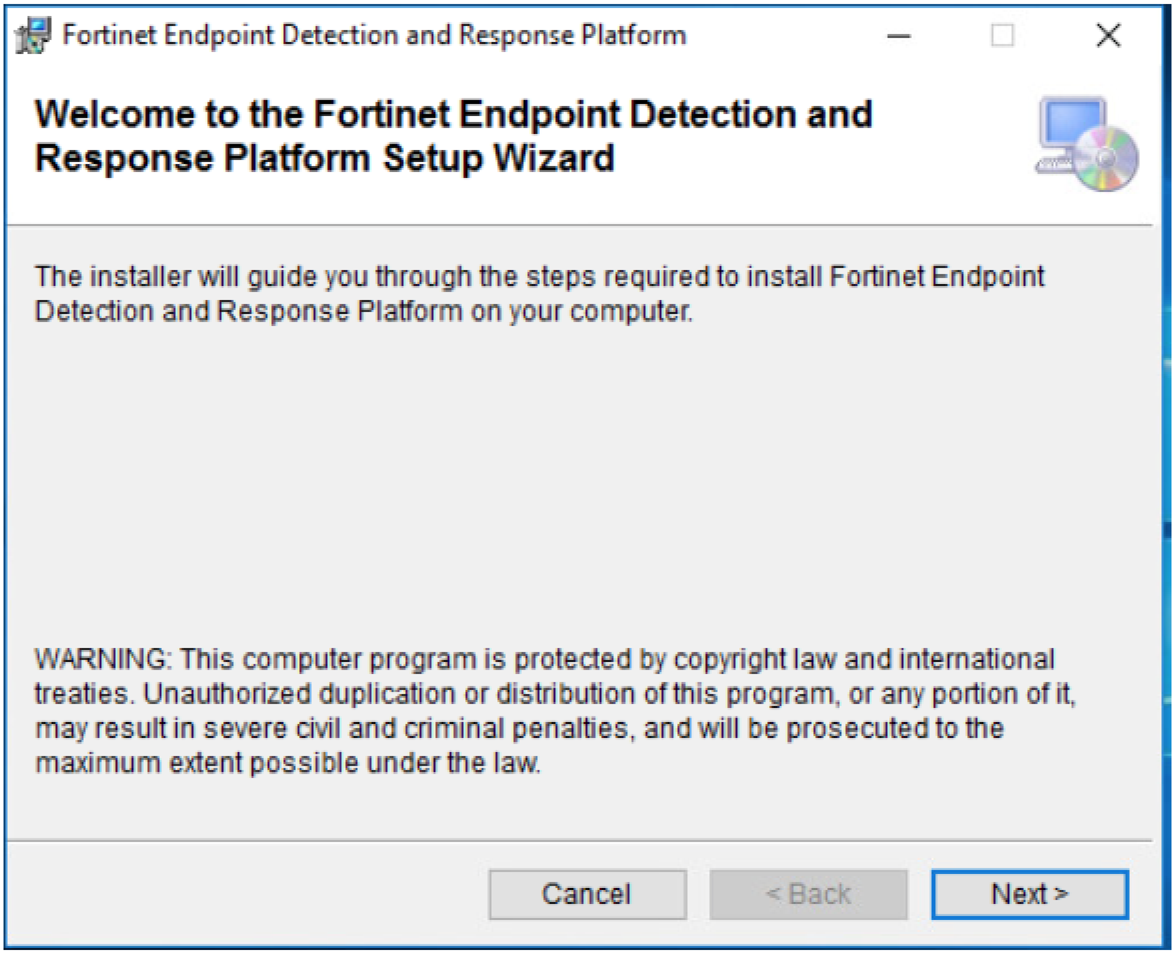
You can get a Collector that is customized to your environment's settings, as described in Requesting and obtaining a Collector installer on page 409. If a custom Collector is used during the installation, all input fields such as Aggregator address and registration password are auto-filled.

- Installing a FortiEDR Collector on Windows on page 23
- Installing a FortiEDR Collector on macOS on page 28
- Installing a FortiEDR Collector on Linux on page 53
- Automated FortiEDR Collector deployment on page 55
- Installing FortiEDR on MacOS devices using Jamf PRO on page 58
- Working with FortiEDR on VDI environments on page 69

For more details about installing a Collector in a multi-organization environment, see Collector registration on page 416.

Installing a FortiEDR Collector on Windows

1. It is recommended to get a pre-populated customized Collector installer for Windows, as described in Requesting and obtaining a Collector installer on page 409.

2. Run the FortiEDR Collector installation file. Use the `FortiEDRCollectorInstaller32.msi` file if you are using a 32-bit operating system; or use the `FortiEDRCollectorInstaller64.msi` file if you are using a 64-bit operating system.
3. 

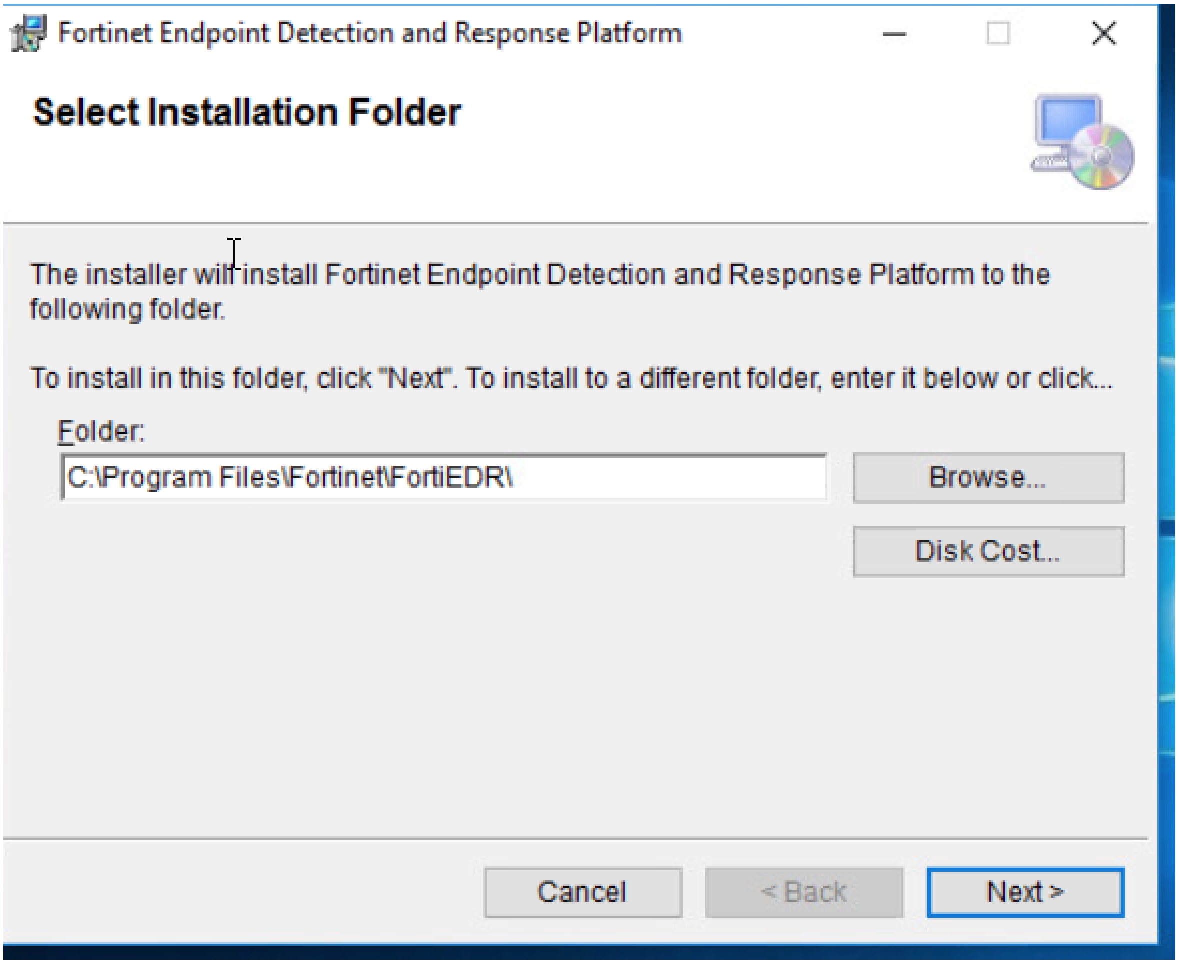
   Fortinet Endpoint Detection and Response Platform

   Welcome to the Fortinet Endpoint Detection and Response Platform Setup Wizard

   The installer will guide you through the steps required to install Fortinet Endpoint Detection and Response Platform on your computer.

   WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

   Click *Next*.

4. 

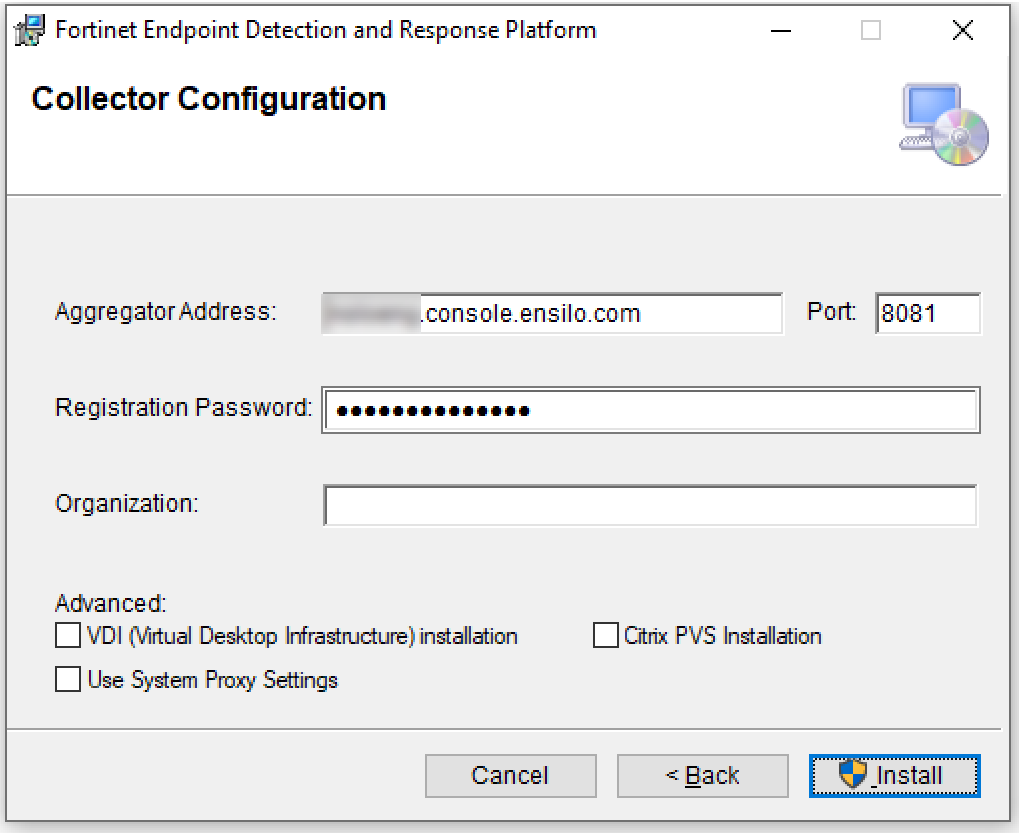
Select Installation Folder

The installer will install Fortinet Endpoint Detection and Response Platform to the following folder.

To install in this folder, click "Next". To install to a different folder, enter it below or click...

Folder: C:\Program Files\Fortinet\FortiEDR\

Leave the default FortiEDR Collector installation folder or change it as necessary. Click *Next*.

5. 

Collector Configuration

Aggregator Address: [redacted].console.ensilo.com Port: 8081

Registration Password: ●●●●●●●●●●●●●●

Organization:

Advanced:

□ VDI (Virtual Desktop Infrastructure) installation □ Citrix PVS Installation

□ Use System Proxy Settings

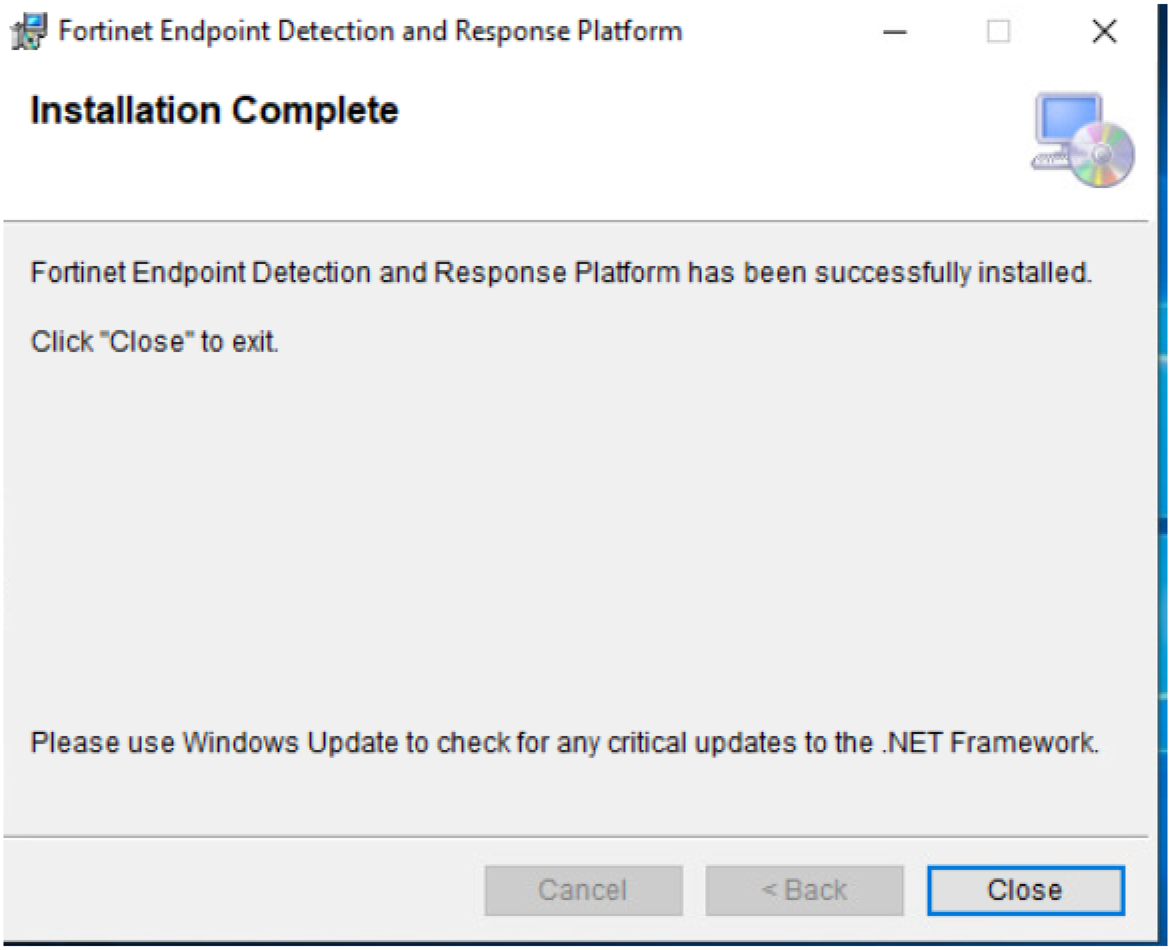
If a non-customized installer is used, in the *Aggregator Address* field, specify the FortiEDR Aggregator domain name or IP address.

6. If a non-customized installer is used, in the *Port* field, specify the FortiEDR Aggregator port (8081).

When upgrading a FortiEDR Collector, the Aggregator address field can be left empty – in order to retain the previously defined Aggregator address.

7. If a non-customized installer is used, in the *Registration Password* field, enter the device registration password that you defined, as described in Configuring the FortiEDR Central Manager server and console on page 474.
8. For a multi-organization FortiEDR system, enter the name of the organization in the *Organization* field. For more details, see the Collector registration on page 416.
9. If you are installing the Collector on a VDI environment, check the *VDI* checkbox. For more details, see Working with FortiEDR on VDI environments on page 69.
10. If you use a web proxy to filter requests in this device's network, then check the *Use System Proxy Settings* checkbox. Note that Windows must be configured to use a proxy and tunneling must be allowed from the Collector to the Aggregator on port 8081 and from the Collector to the Core on port 555. (Run as Administrator: **netsh winhttp set proxy <proxy IP >**).
11. If you are installing the Collector on a Citrix PVS golden image, check the *Citrix PVS installation* checkbox.
12. Click *Next* twice to start the installation. Windows may possibly display a message requesting that you confirm the installation. Please do so.

13. After the installation of the FortiEDR Collector has been successfully completed, the following window displays:



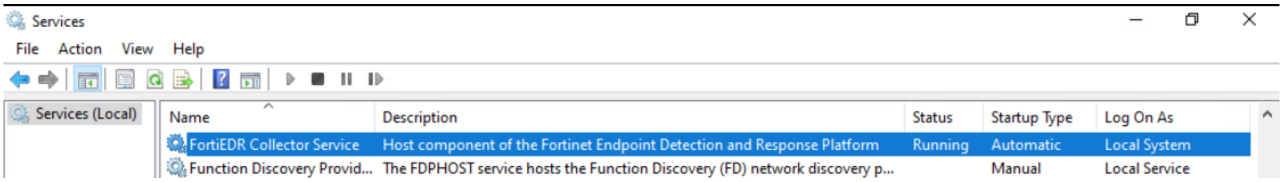
Installation Complete

Fortinet Endpoint Detection and Response Platform has been successfully installed.

Click "Close" to exit.

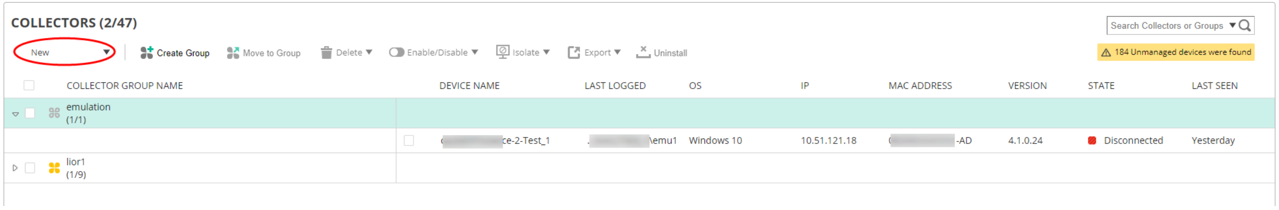
Please use Windows Update to check for any critical updates to the .NET Framework.

Check Windows Services to verify that the FortiEDR Collector Service is running, as shown below:



Name	Description	Status	Startup Type	Log On As
FortiEDR Collector Service	Host component of the Fortinet Endpoint Detection and Response Platform	Running	Automatic	Local System
Function Discovery Provid...	The FDPHOST service hosts the Function Discovery (FD) network discovery p...		Manual	Local Service

14. Verify that the FortiEDR Collector details are listed in the INVENTORY tab of the FortiEDR Central Manager console (see Assets on page 256. Select the New filter to display a list of newly registered FortiEDR Collectors, as shown below:



COLLECTOR GROUP NAME	DEVICE NAME	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	STATE	LAST SEEN
emulation (1/1)								
	[redacted]ce-2-Test_1	[redacted]\emu1	Windows 10	10.51.121.18	[redacted]-AD	4.1.0.24	🟥 Disconnected	Yesterday
lior1 (1/9)								

15. If another AV product is also installed on the machine, exclude AV exceptions by following the instructions in Exclusion paths.

Installing a FortiEDR Collector on macOS

The process described below includes a description of how to allow the following upon first FortiEDR Collector installation:

- System Extensions
- Network Extensions
- Full Disk Access

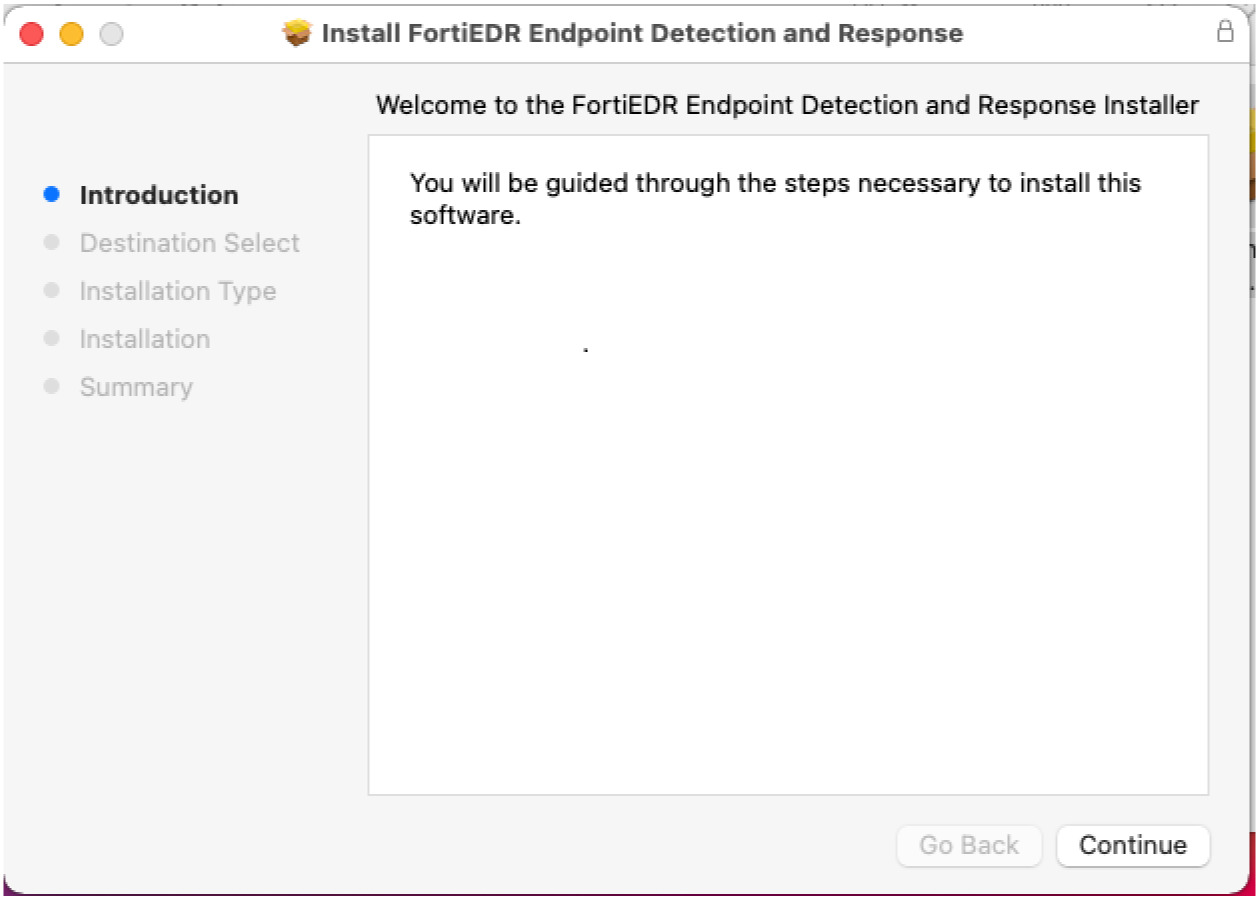
IMPORTANT: Failure to add these permissions will result in incomplete protection.

Deployment can also be managed using an MDM, such as Jamf.

To install a FortiEDR Collector on macOS that is running with Big Sur (version 11) or later:

To start the installation:

1. It is recommended to get a pre-populated customized Collector installer for macOS, as described in Requesting and obtaining a Collector installer on page 409.
2. Double-click the `*.dmg` file named `FortiEDRCollectorInstallerOSX_<version>.dmg`.
3. Click *Continue*.

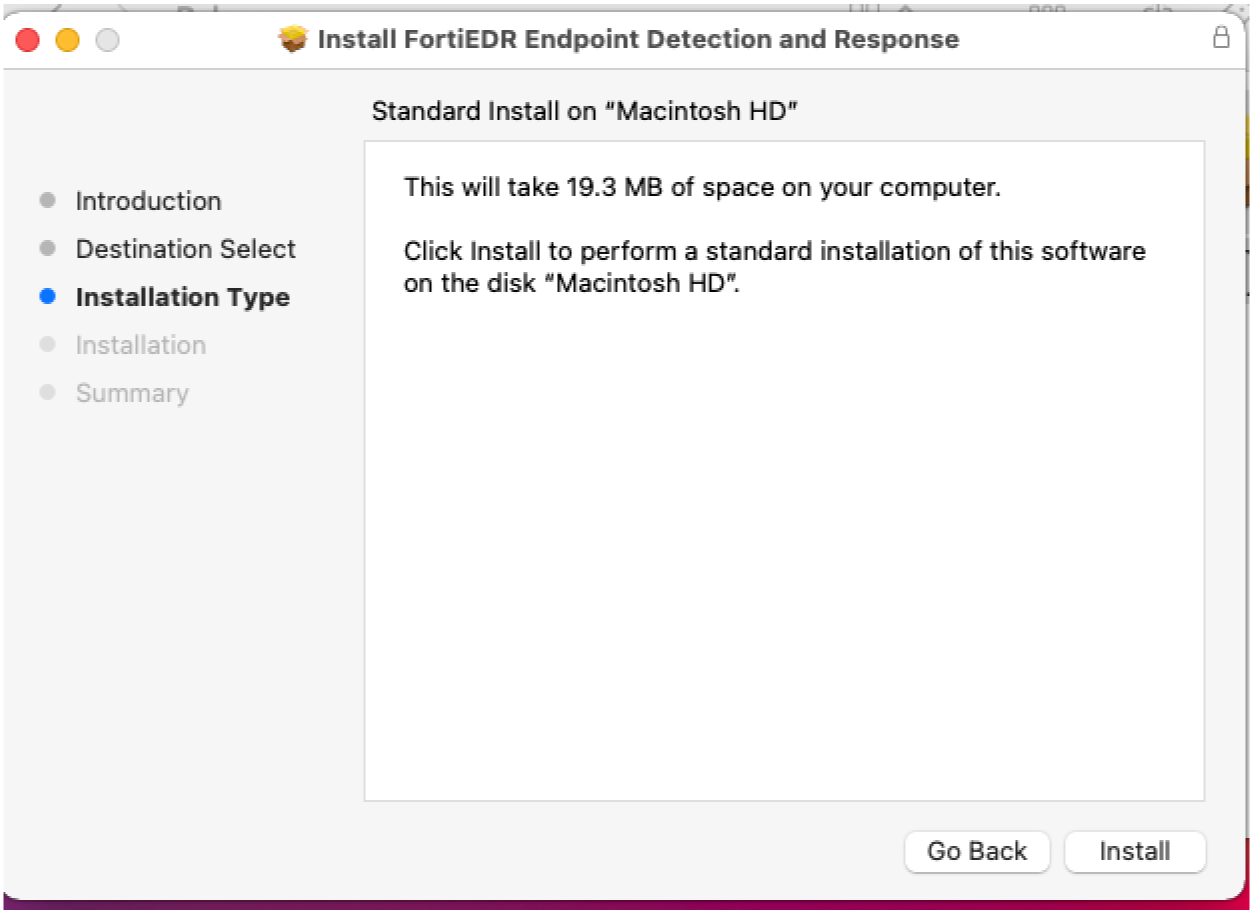


Install FortiEDR Endpoint Detection and Response

Welcome to the FortiEDR Endpoint Detection and Response Installer

You will be guided through the steps necessary to install this software.

4. Click *Install*.



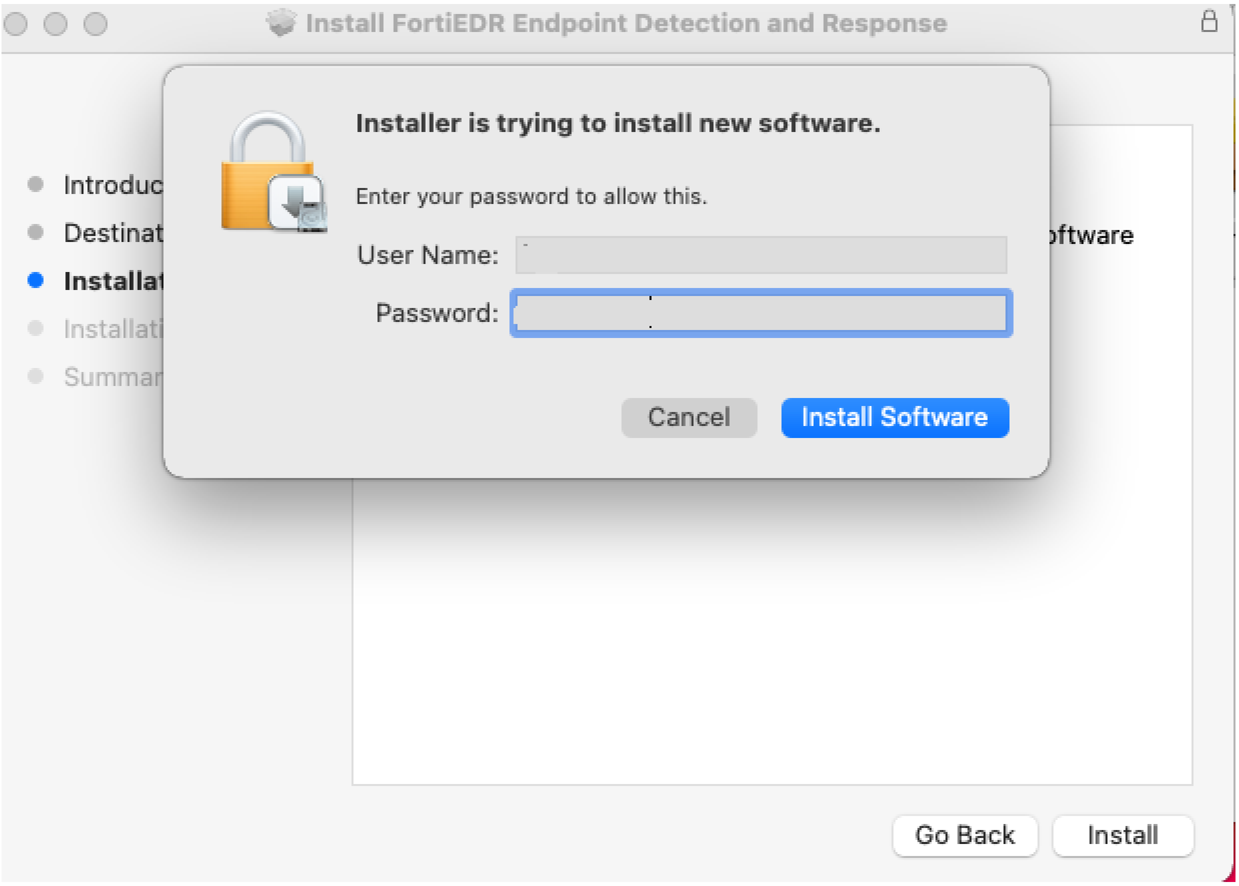
Install FortiEDR Endpoint Detection and Response

Standard Install on "Macintosh HD"

This will take 19.3 MB of space on your computer.

Click Install to perform a standard installation of this software on the disk "Macintosh HD".

5. Enter the Mac password at the prompt and click *Install Software*.



Install FortiEDR Endpoint Detection and Response

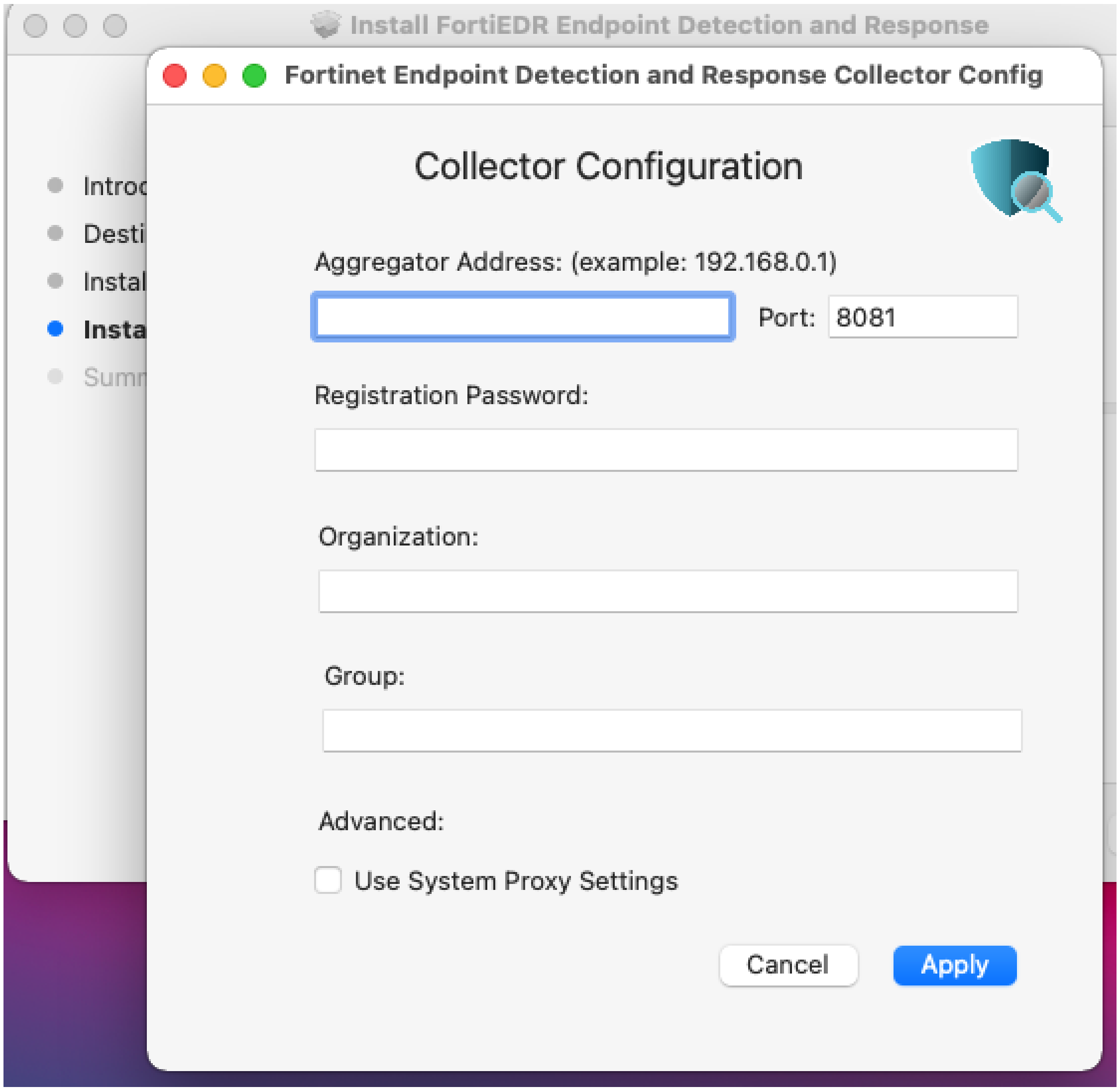
Installer is trying to install new software.

Enter your password to allow this.

User Name:

Password:

6. If a non-customized installer is used, in the *Collector Conifguration* page, specify the Aggregator's address and FortiEDR registration password. Optionally, you can select a destination Organization and Collector Group and/or installation using a system proxy.


Install FortiEDR Endpoint Detection and Response
Introd
Desti
Instal
Insta
Sumr
Fortinet Endpoint Detection and Response Collector Config

Collector Configuration

Aggregator Address: (example: 192.168.0.1)

Port: 8081

Registration Password:

Organization:

Group:

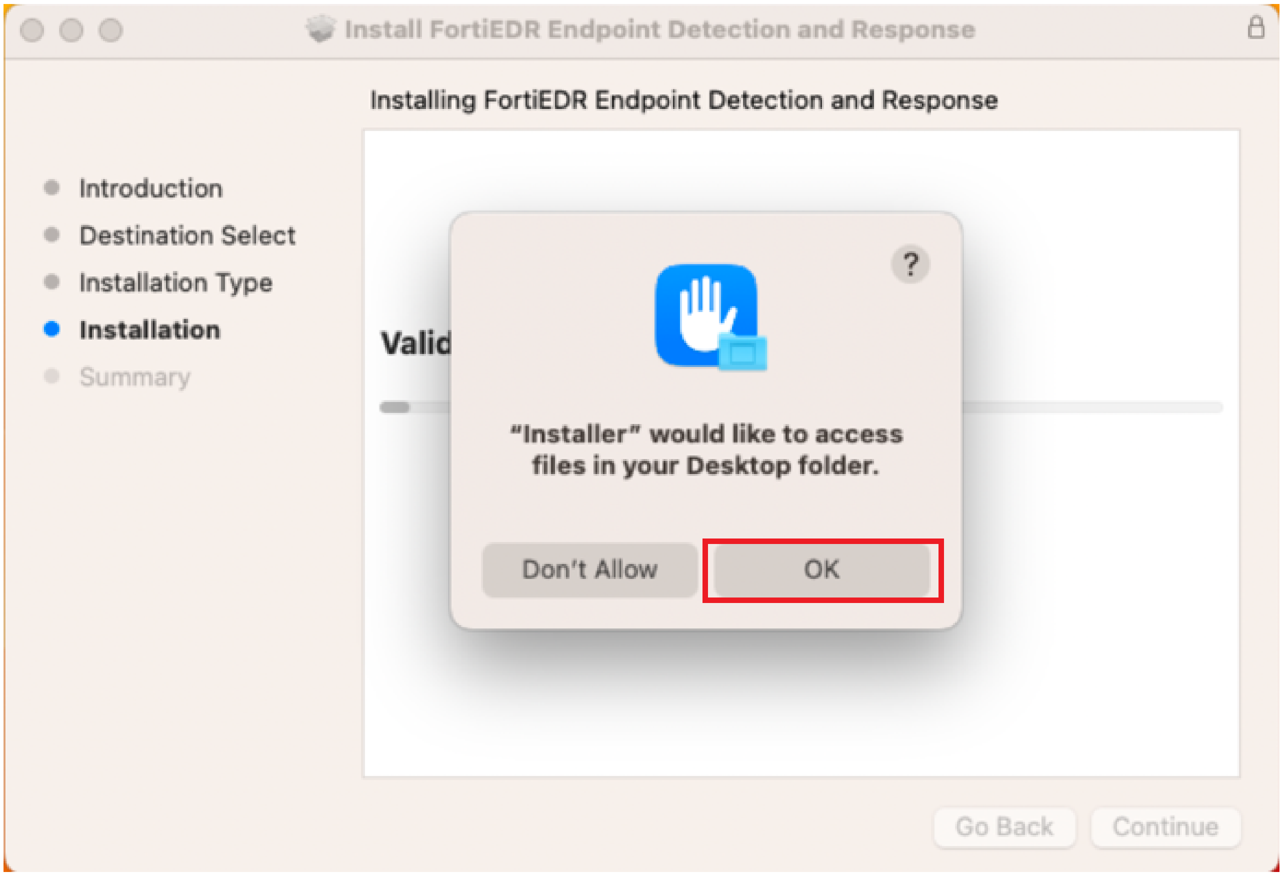
Advanced:

☐ Use System Proxy Settings

7. Click *Apply* to start the installation process.
8. Continue the installation:
   - macOS 15 or later
   - macOS 13 or 14
   - macOS 11 or 12

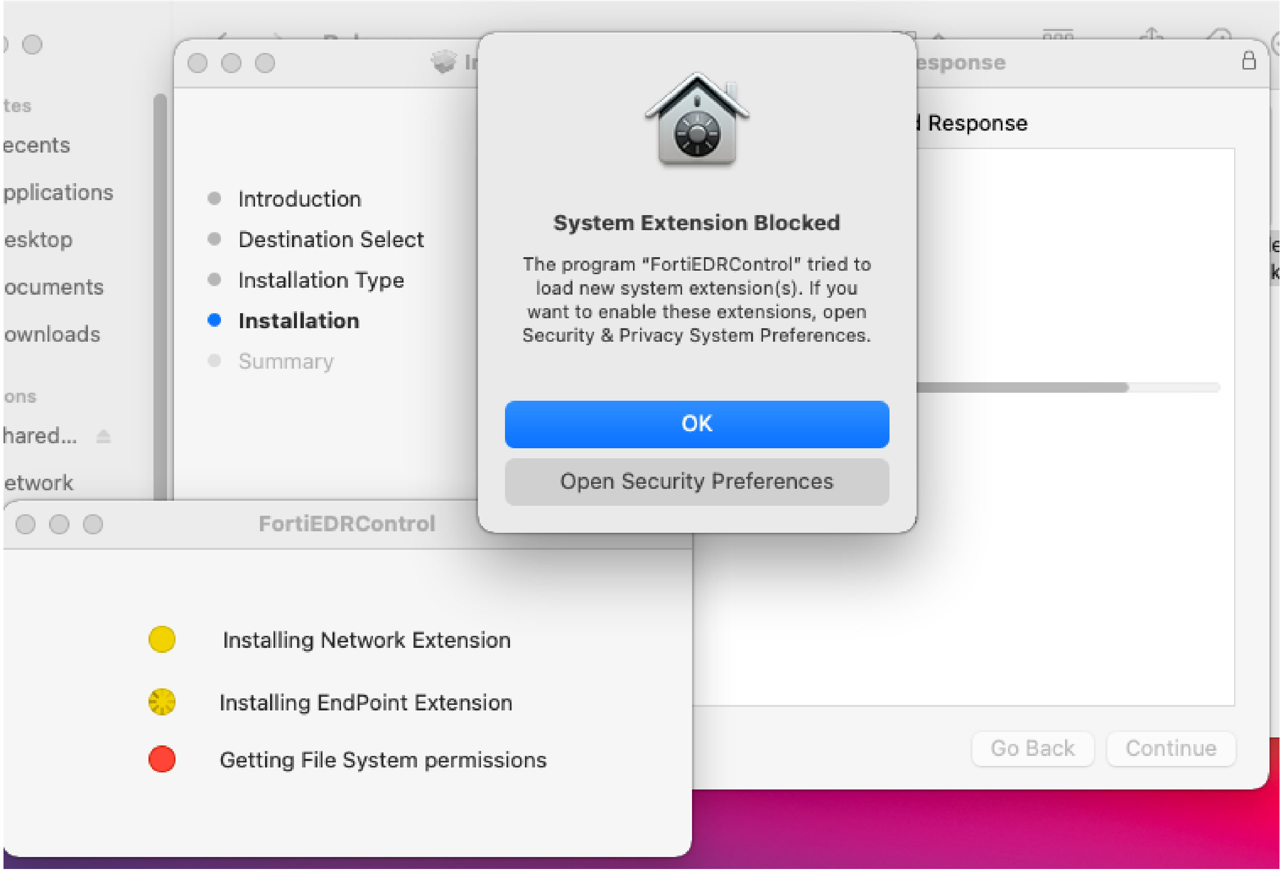
To continue the installation on macOS 15 or later:

1. In the popup window, click *OK* to allow the installer to access files:



Install FortiEDR Endpoint Detection and Response
Installing FortiEDR Endpoint Detection and Response
Introduction
Destination Select
Installation Type
Installation
Summary
Valid
"Installer" would like to access files in your Desktop folder.
Don't Allow
OK
Go Back
Continue

2. Enable Network and System Extensions:



System Extension Blocked

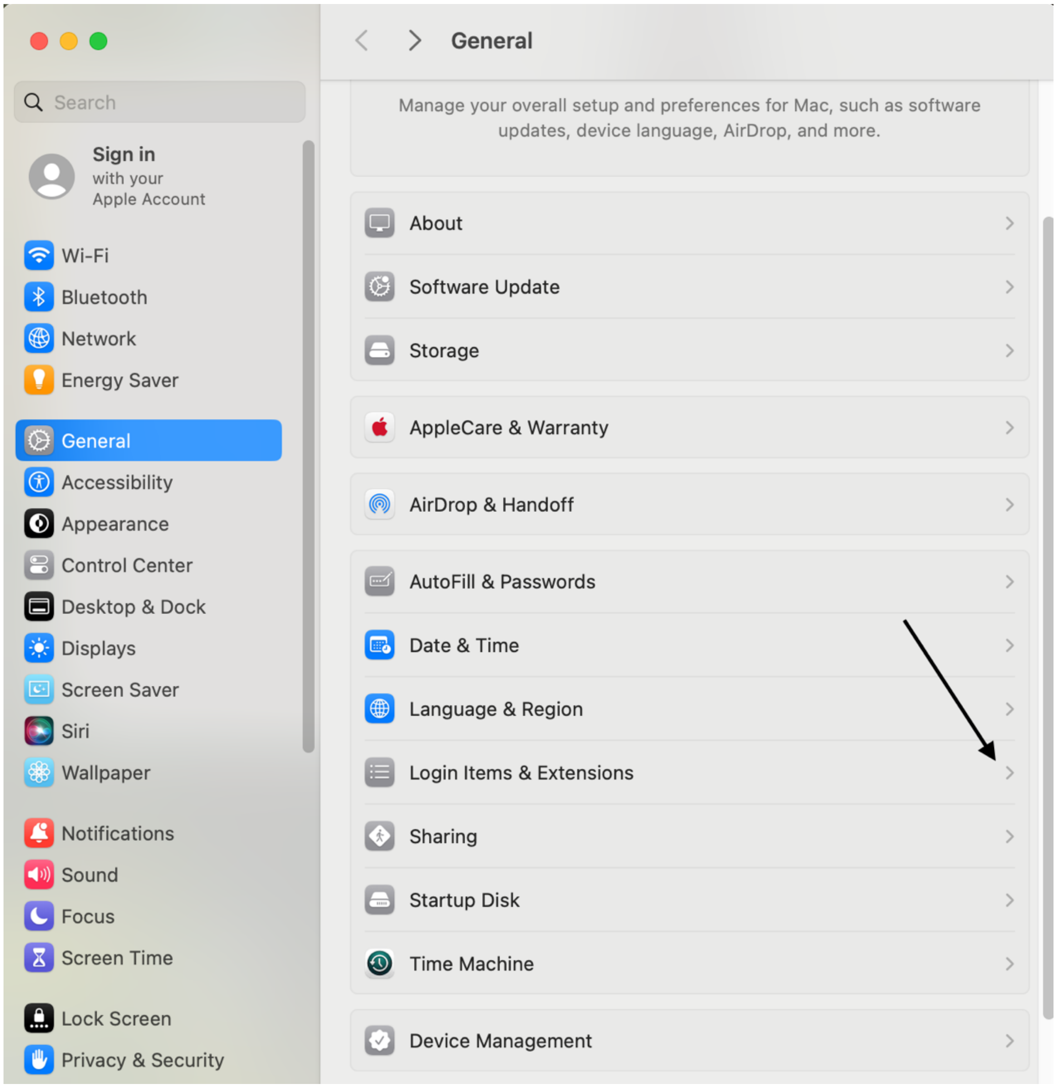
The program "FortiEDRControl" tried to load new system extension(s). If you want to enable these extensions, open Security & Privacy System Preferences.

Installing Network Extension

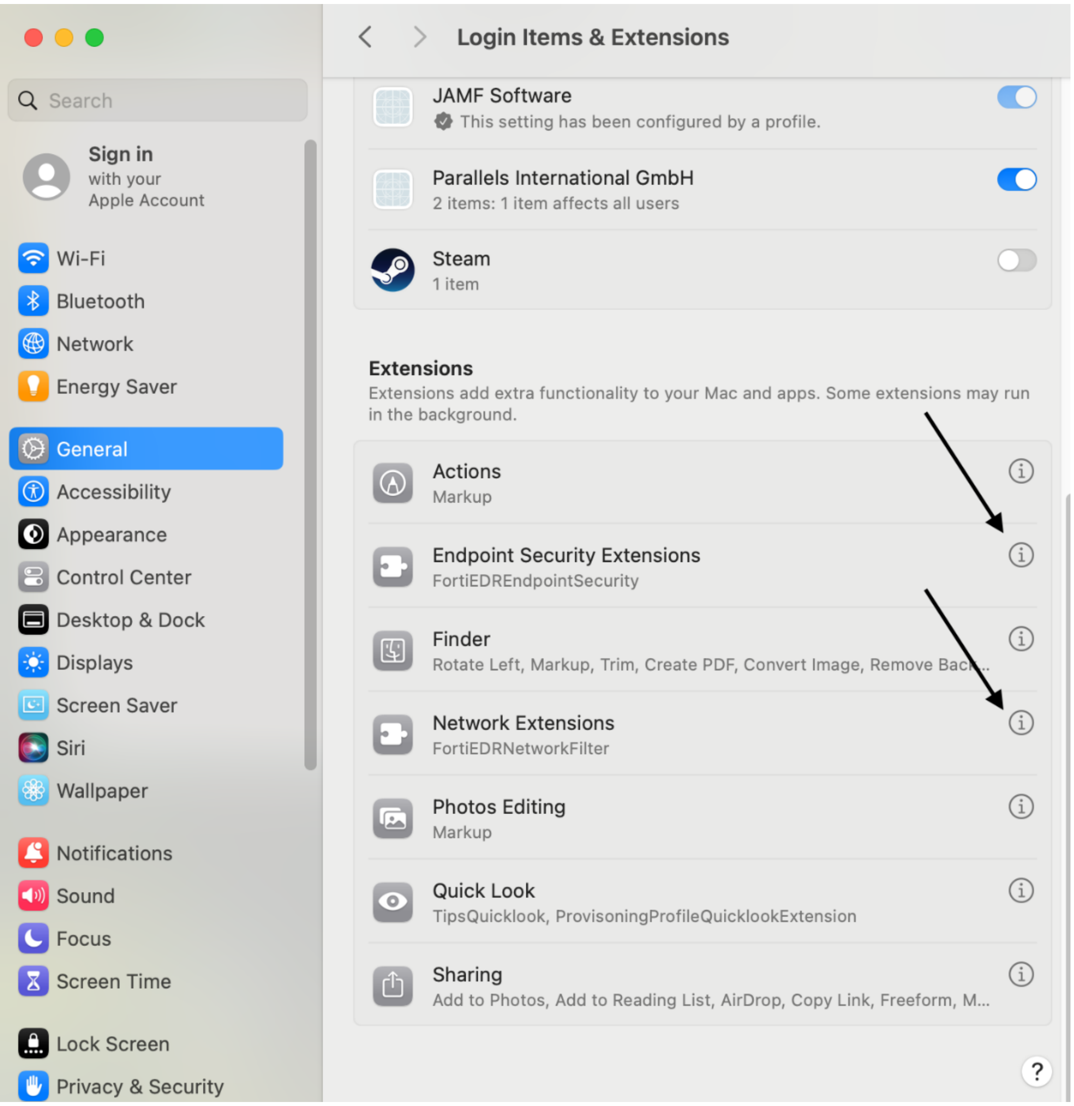
Installing EndPoint Extension

Getting File System permissions

a. Open *General > Login Items & Extensions* and scroll down to *Extensions*.



Manage your overall setup and preferences for Mac, such as software updates, device language, AirDrop, and more.



Login Items & Extensions

JAMF Software
This setting has been configured by a profile.

Parallels International GmbH
2 items: 1 item affects all users

Steam
1 item

Extensions
Extensions add extra functionality to your Mac and apps. Some extensions may run in the background.

Actions
Markup

Endpoint Security Extensions
FortiEDREndpointSecurity

Finder
Rotate Left, Markup, Trim, Create PDF, Convert Image, Remove Back...

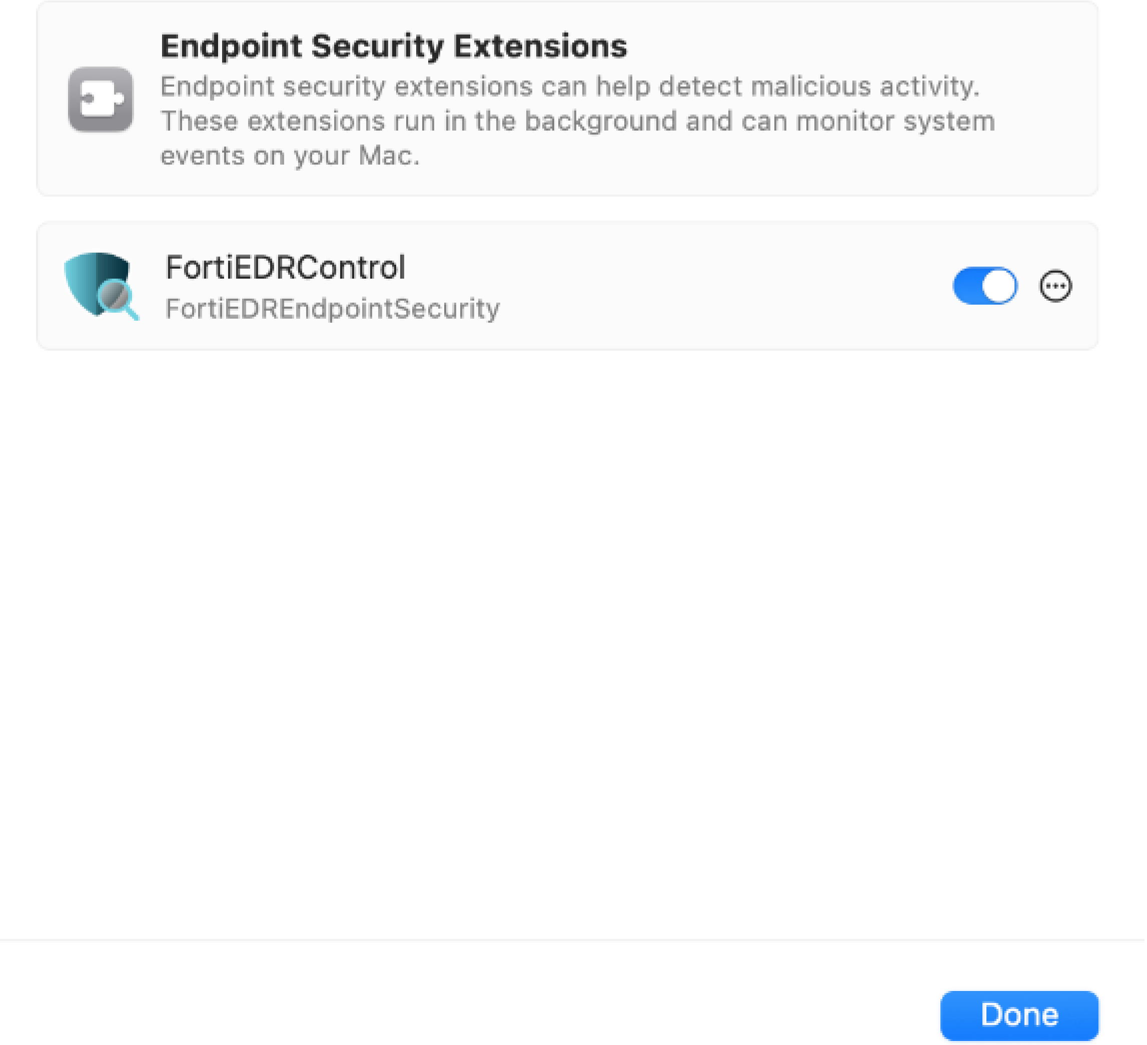
Network Extensions
FortiEDRNetworkFilter

Photos Editing
Markup

Quick Look
TipsQuicklook, ProvisoningProfileQuicklookExtension

Sharing
Add to Photos, Add to Reading List, AirDrop, Copy Link, Freeform, M...

b. Click *Endpoint Security Extension* and toggle on *FortiEDRControl*.
The Mac password is required for this change.



Endpoint Security Extensions

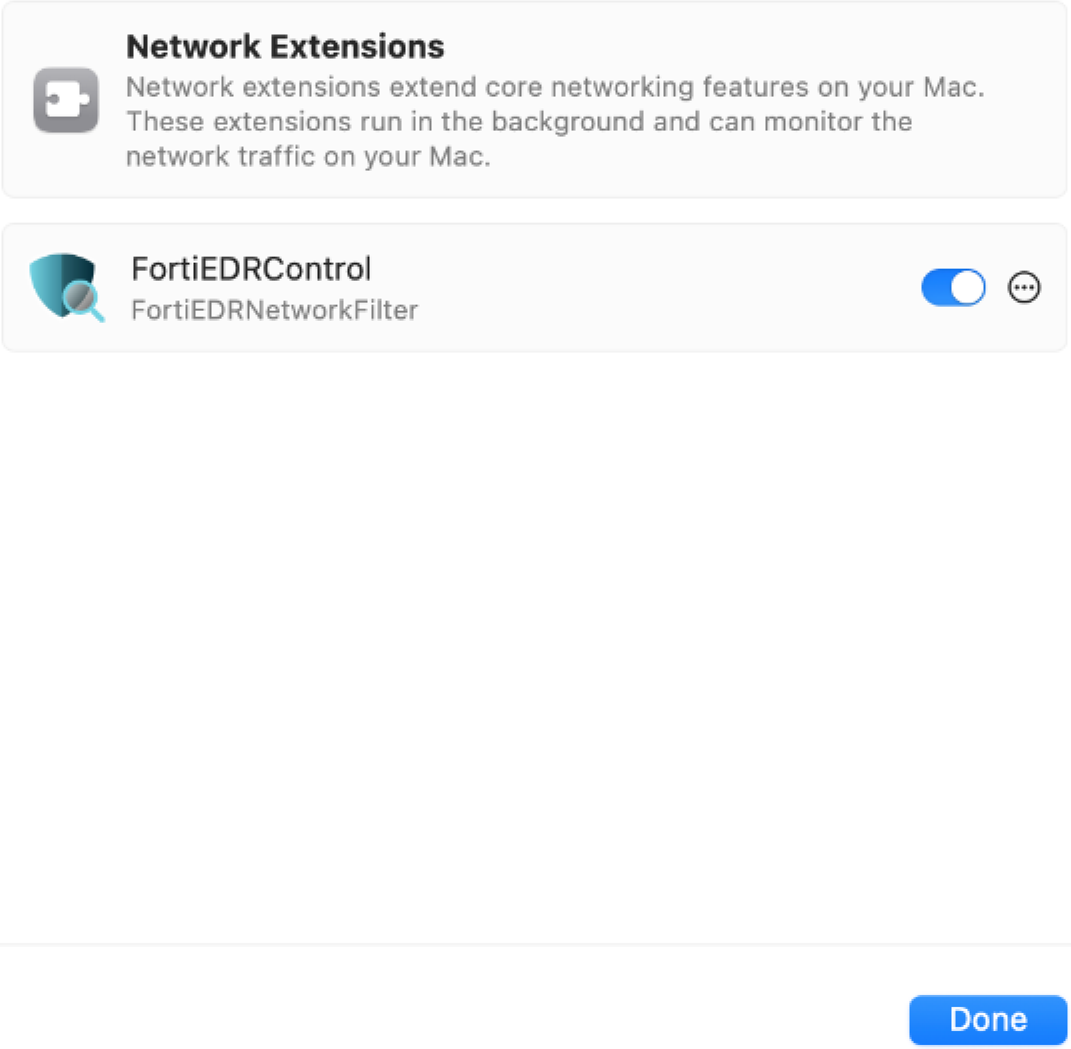
Endpoint security extensions can help detect malicious activity. These extensions run in the background and can monitor system events on your Mac.

FortiEDRControl
FortiEDREndpointSecurity

c. Click *Done*.

d. Click *Network Extension* and toggle on *FortiEDRControl*.

The Mac password is required for this change.

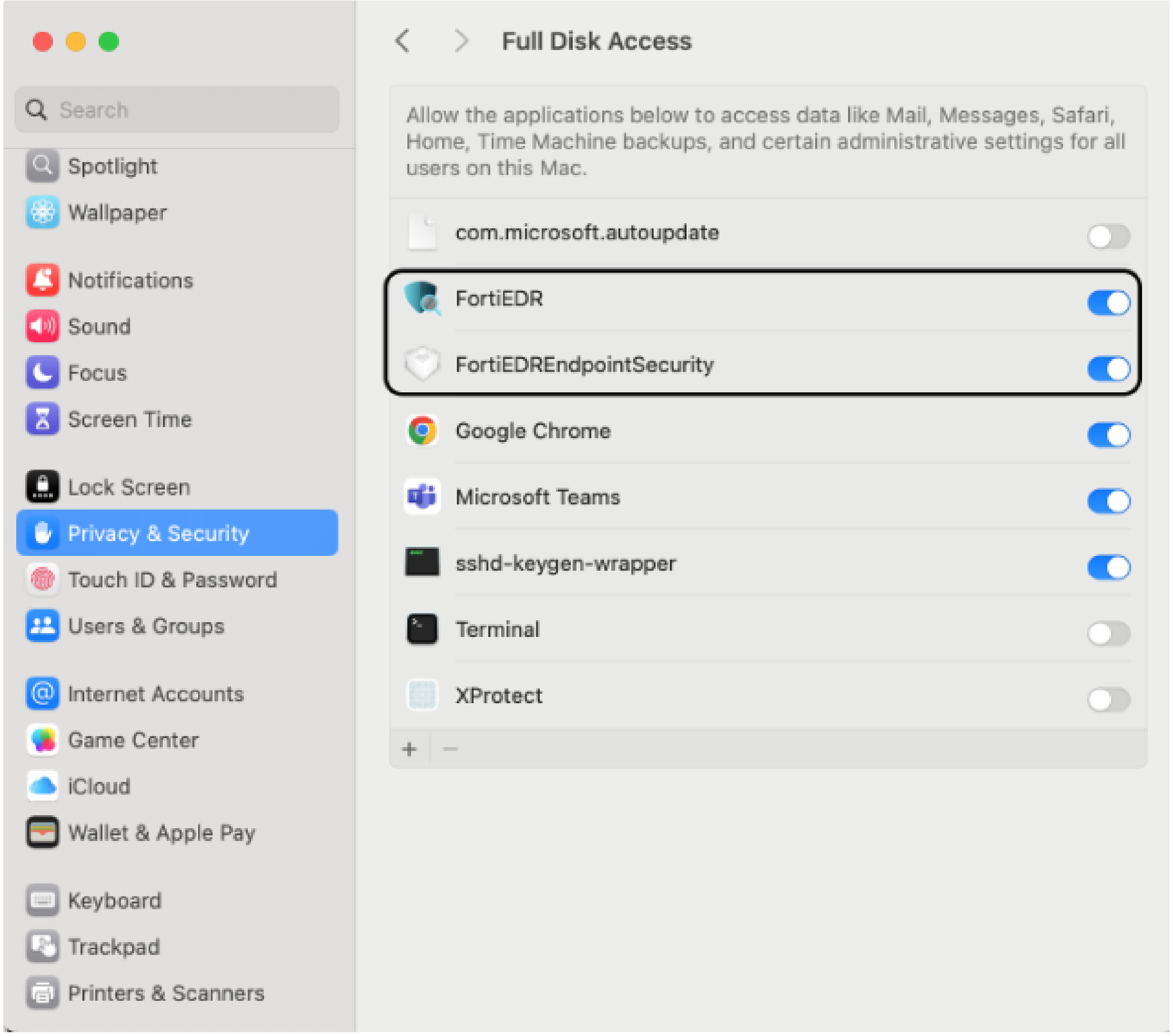


Network Extensions

Network extensions extend core networking features on your Mac. These extensions run in the background and can monitor the network traffic on your Mac.

FortiEDRControl
FortiEDRNetworkFilter

  e. Click *Done*.
3. Enable Full Disk Access:
  a. Open Full Disk Access on *Privacy & Security*.
  b. Toggle on the two FortiEDR-related options to authorize full disk access for FortiEDR, as shown below:



Full Disk Access

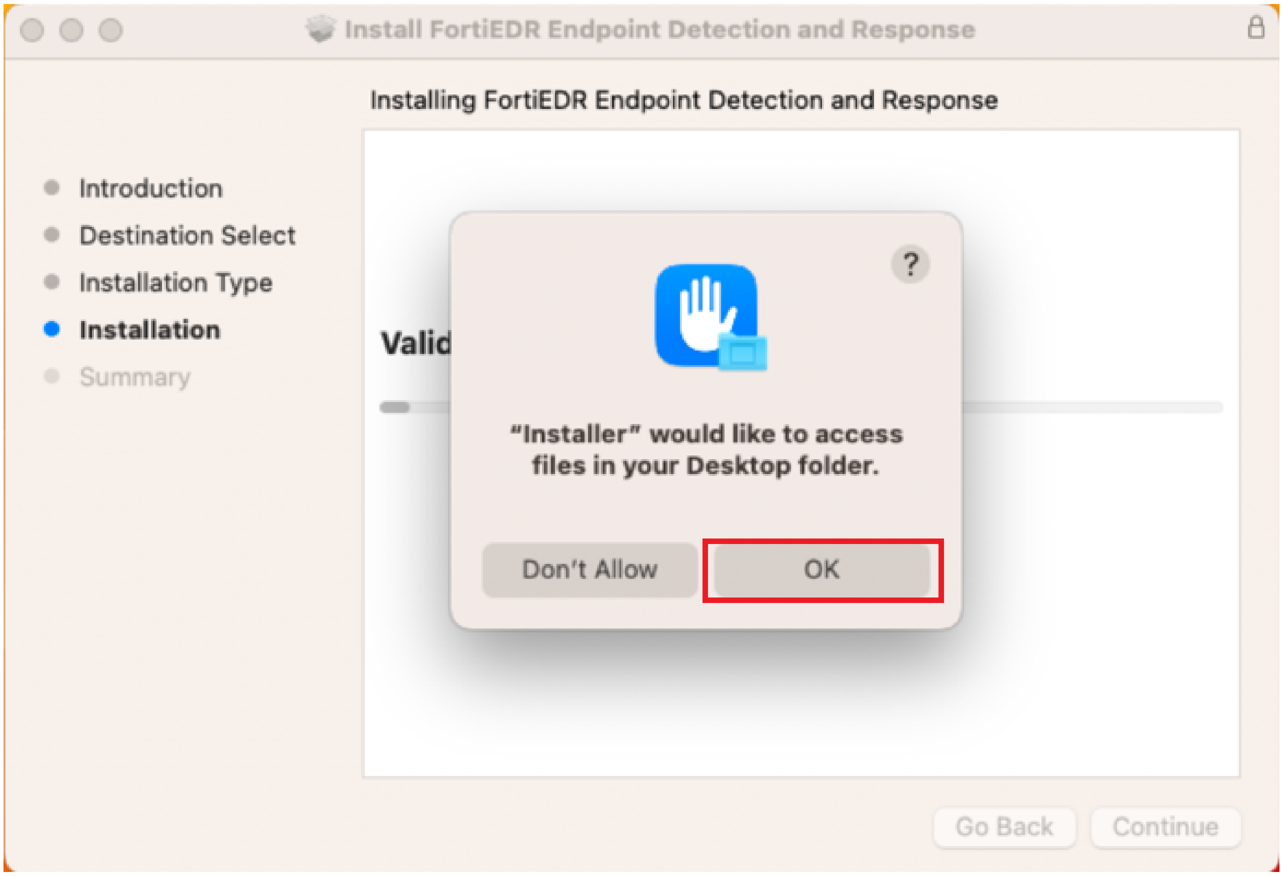
Allow the applications below to access data like Mail, Messages, Safari, Home, Time Machine backups, and certain administrative settings for all users on this Mac.

com.microsoft.autoupdate	○
FortiEDR	●
FortiEDREndpointSecurity	●
Google Chrome	●
Microsoft Teams	●
sshd-keygen-wrapper	●
Terminal	○
XProtect	○

4. See To finish the installation.

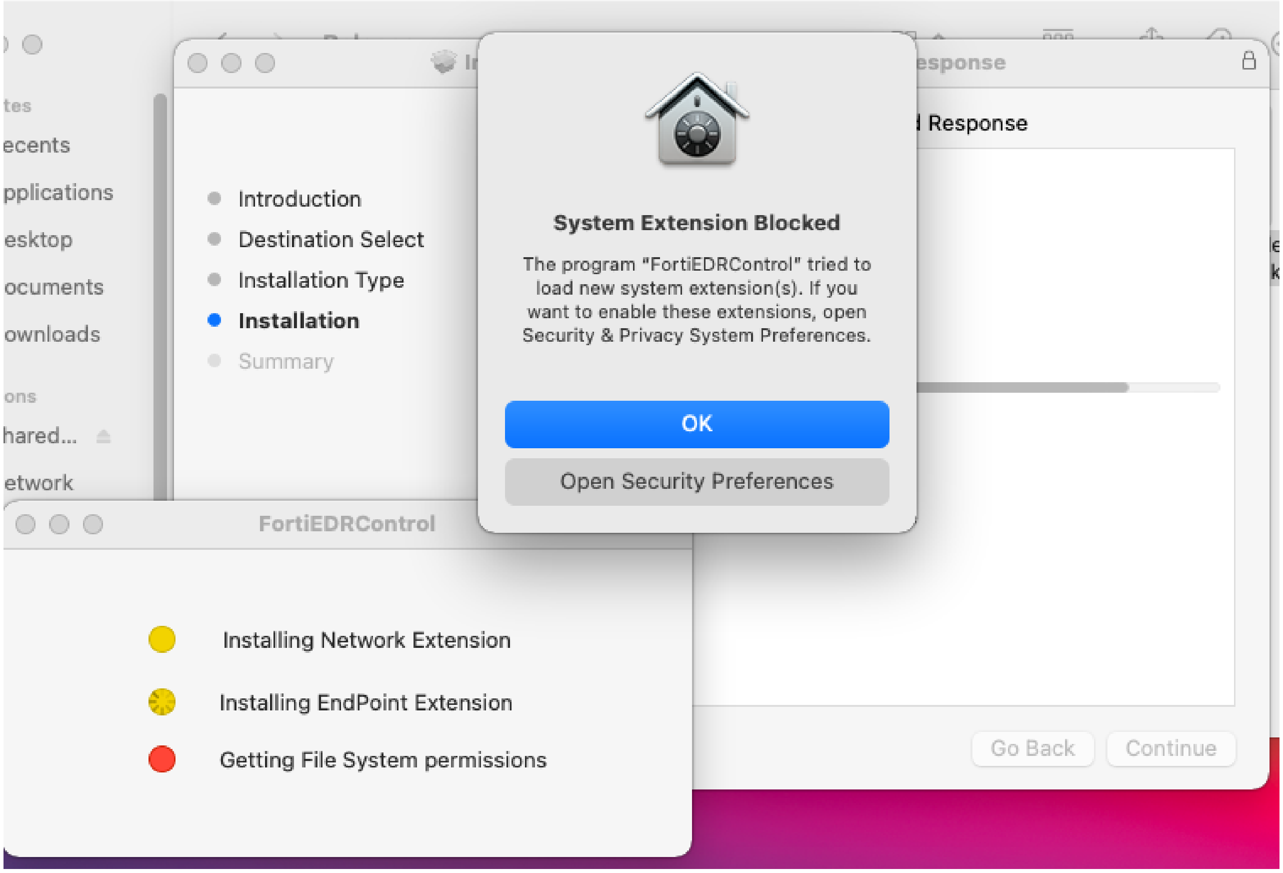
To continue the installation on macOS 13 or 14:

1. In the popup window, click *OK* to allow the installer to access files:



Install FortiEDR Endpoint Detection and Response
Installing FortiEDR Endpoint Detection and Response
Introduction
Destination Select
Installation Type
Installation
Summary
Valid
?
"Installer" would like to access files in your Desktop folder.
Don't Allow
OK
Go Back
Continue

2. Enable Network and System Extensions:



System Extension Blocked

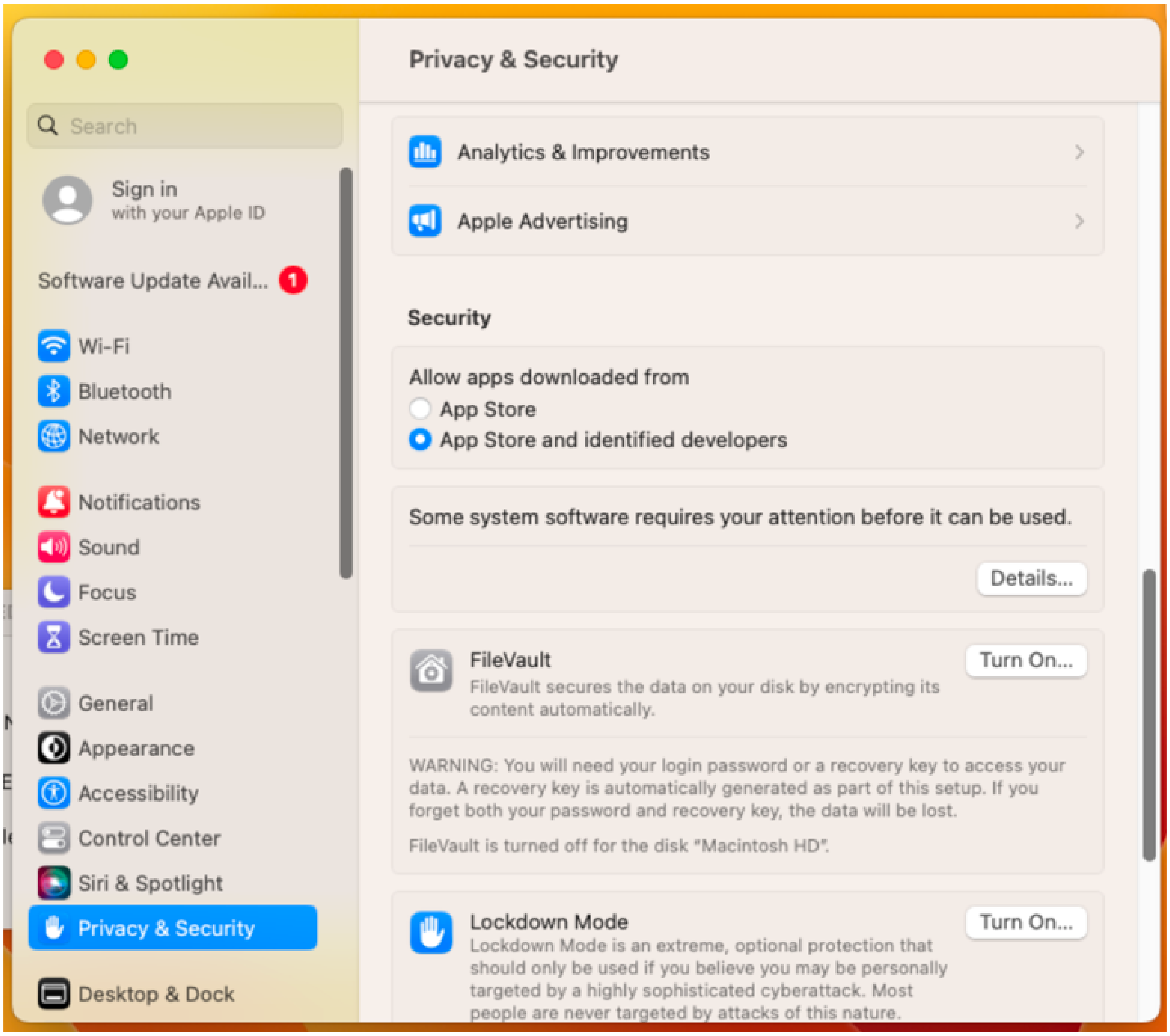
The program "FortiEDRControl" tried to load new system extension(s). If you want to enable these extensions, open Security & Privacy System Preferences.

● Installing Network Extension

● Installing EndPoint Extension

● Getting File System permissions

a. Open *Privacy & Security* and scroll down to the *Security* section:



Privacy & Security

Security

Allow apps downloaded from

○ App Store

● App Store and identified developers

Some system software requires your attention before it can be used.

FileVault

FileVault secures the data on your disk by encrypting its content automatically.

WARNING: You will need your login password or a recovery key to access your data. A recovery key is automatically generated as part of this setup. If you forget both your password and recovery key, the data will be lost.

FileVault is turned off for the disk "Macintosh HD".

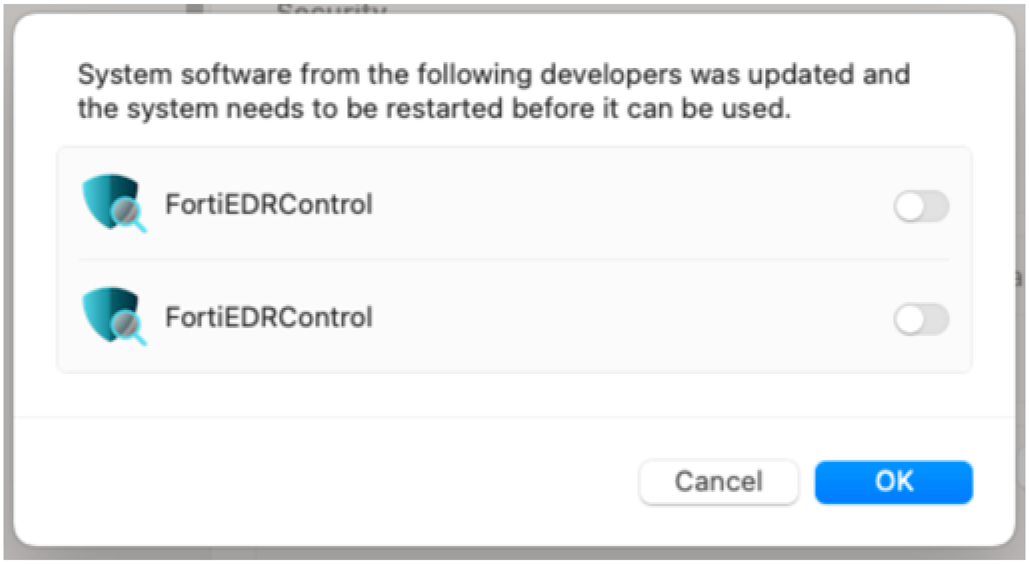
Lockdown Mode

Lockdown Mode is an extreme, optional protection that should only be used if you believe you may be personally targeted by a highly sophisticated cyberattack. Most people are never targeted by attacks of this nature.

b. Under *Some system software requires your attention before it can be used*, Click *Details*.

c. Enter the Mac password at the prompt.

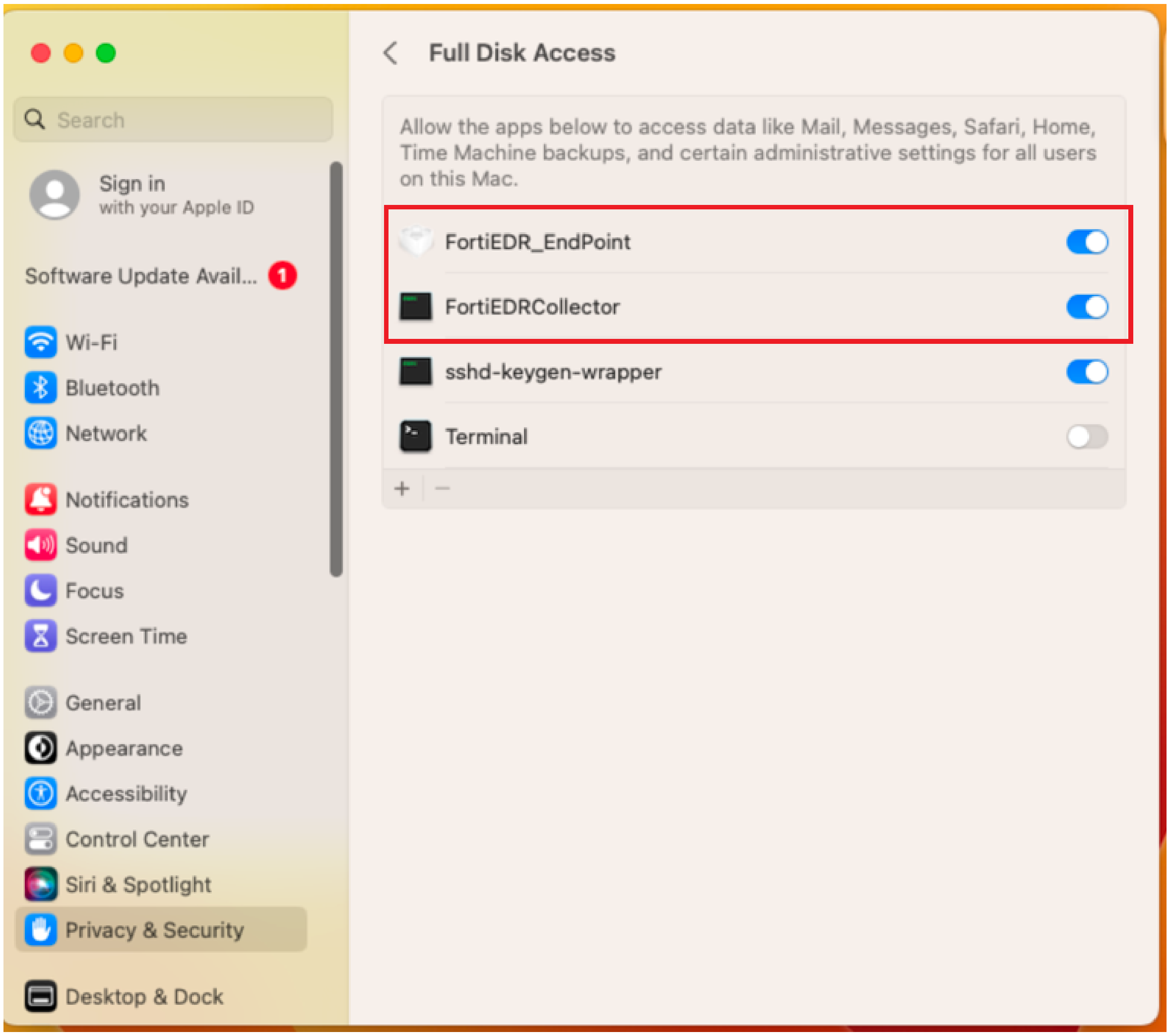
d. Toggle on both toggles in order to allow FortiEDR to use Network and System Extensions and click *OK*.



System software from the following developers was updated and the system needs to be restarted before it can be used.

3. Enable Full Disk Access:
   a. Open Full Disk Access on *Security Preferences*.
   b. Toggle on the two FortiEDR-related options to authorize full disk access for FortiEDR, as shown below:

- **Collector earlier than 6.0:**



Full Disk Access

Allow the apps below to access data like Mail, Messages, Safari, Home, Time Machine backups, and certain administrative settings for all users on this Mac.

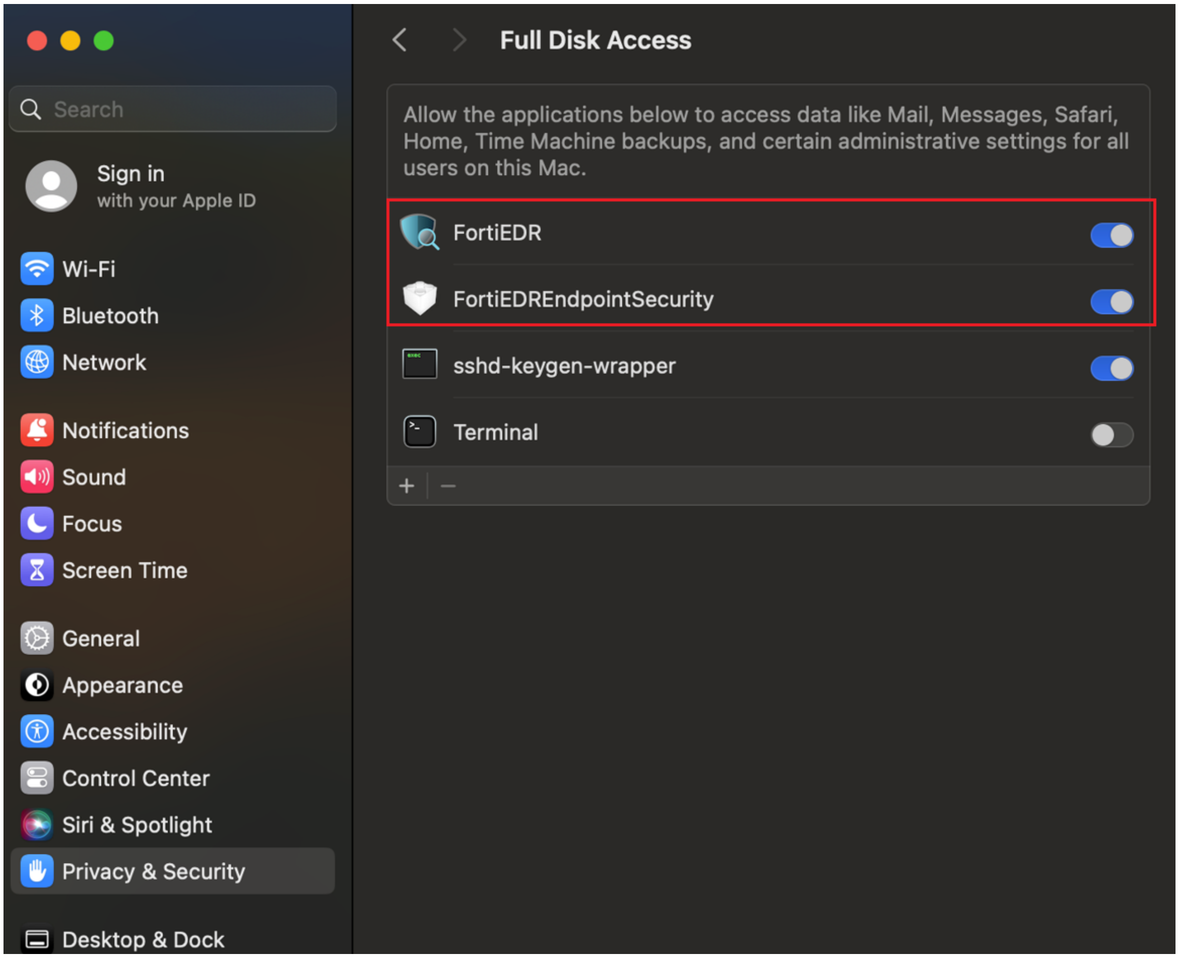
FortiEDR_EndPoint ●

FortiEDRCollector ●

sshd-keygen-wrapper ●

Terminal ○

- **Collector 6.0 or later:**



Full Disk Access

Allow the applications below to access data like Mail, Messages, Safari, Home, Time Machine backups, and certain administrative settings for all users on this Mac.

FortiEDR

FortiEDREndpointSecurity

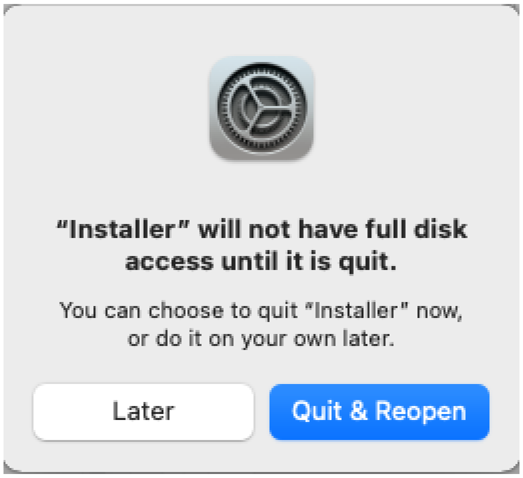
sshd-keygen-wrapper

Terminal

4. See To finish the installation.

To continue the installation on macOS 11 or 12:

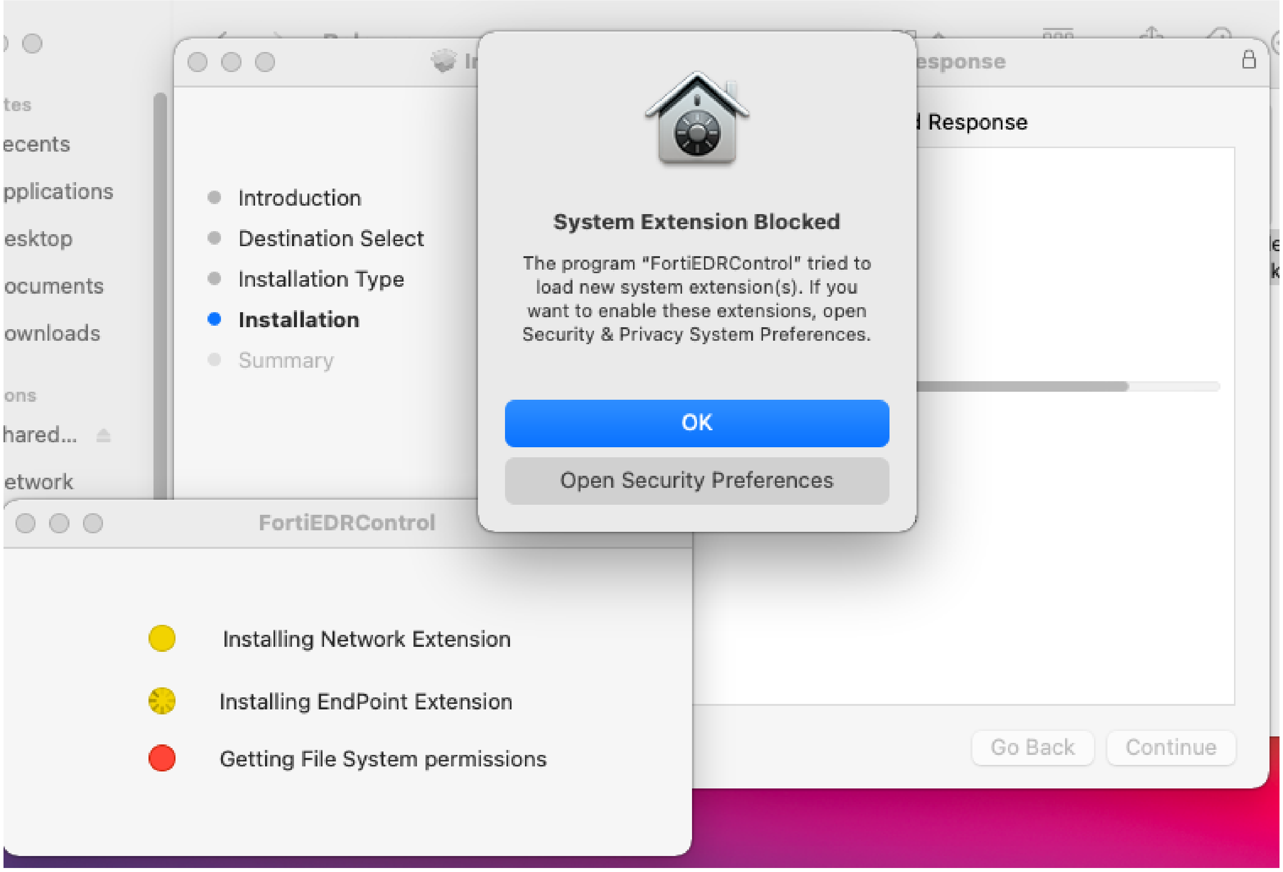
1. In the popup window, click *Later*:



“Installer” will not have full disk access until it is quit.

You can choose to quit “Installer” now, or do it on your own later.

2. Enable Network and System Extensions:



System Extension Blocked

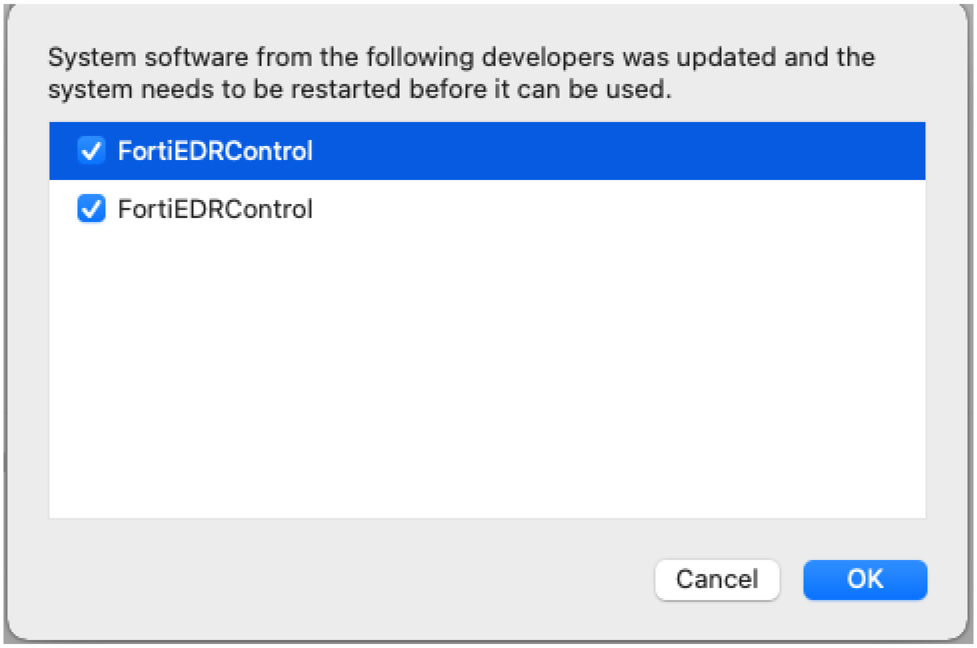
The program "FortiEDRControl" tried to load new system extension(s). If you want to enable these extensions, open Security & Privacy System Preferences.

Installing Network Extension

Installing EndPoint Extension

Getting File System permissions

   a. Open *Security Preferences*.
   b. Click the lock at the bottom of the window in order to make changes.
   c. In the *General* tab, click *Details*.
   d. Mark both checkboxes to allow FortiEDR to use Network and System Extensions. Click *OK*.

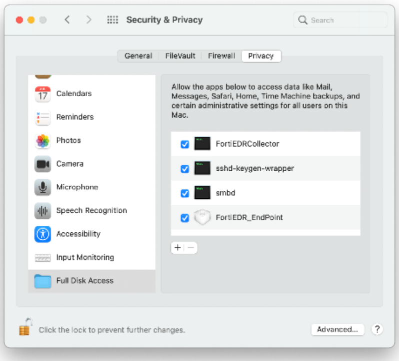


System software from the following developers was updated and the system needs to be restarted before it can be used.

☑ FortiEDRControl

☑ FortiEDRControl

3. Enable Full Disk Access:
   a. Open *Security Preferences*.
   b. Click the lock at the bottom of the window in order to make changes.
   c. In the *Privacy* tab, select *Full Disk Access* from the left pane.
   d. Select the checkboxes of both the *FortiEDRCollector* and the *FortiEDR_EndPoint* applications:



Allow the apps below to access data like Mail, Messages, Safari, Home, Time Machine backups, and certain administrative settings for all users on this Mac.

☑ FortiEDRCollector

☑ sshd-keygen-wrapper

☑ smbd

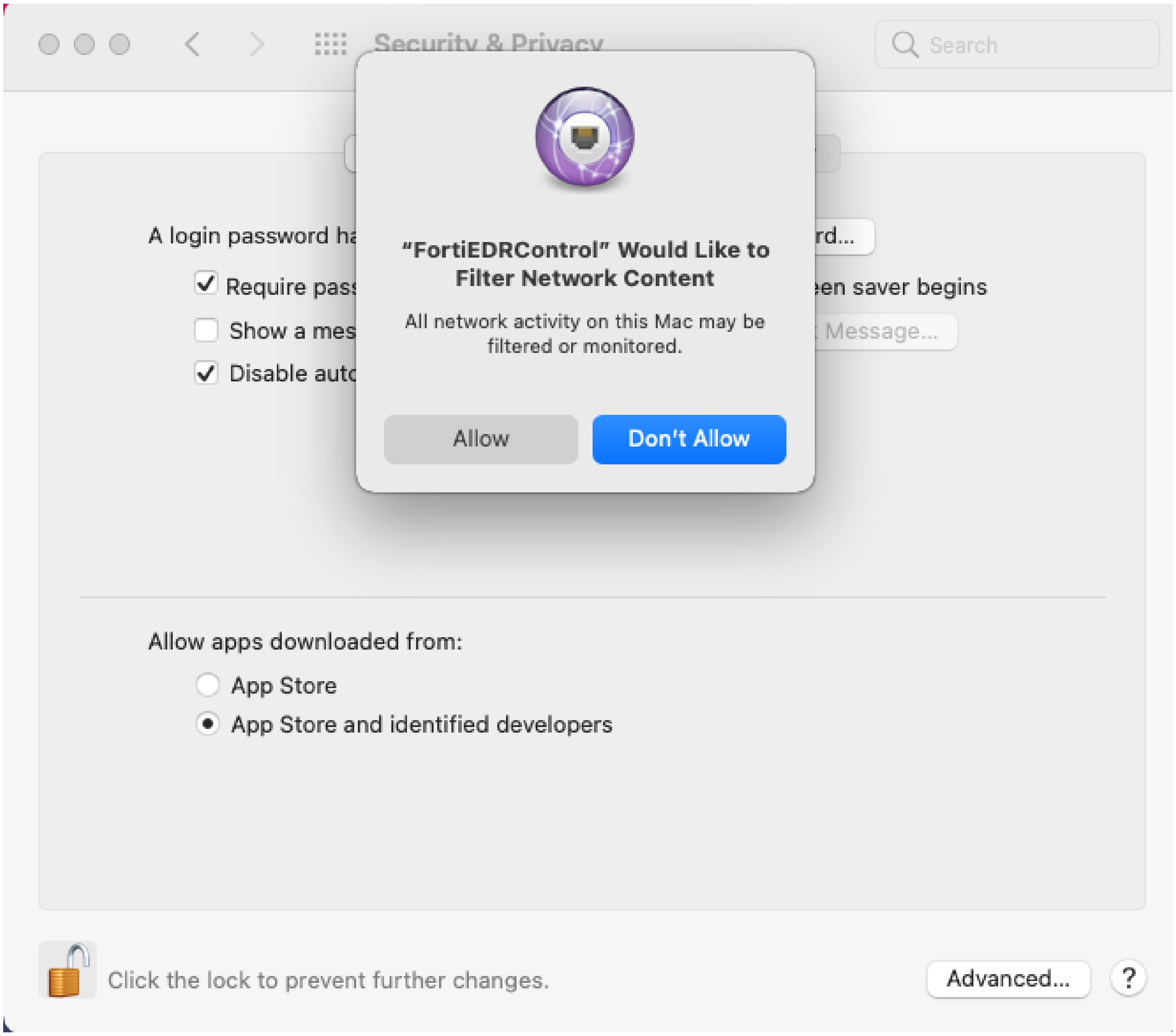
☑ FortiEDR_EndPoint

Click the lock to prevent further changes.

4. See To finish the installation.

To finish the installation:

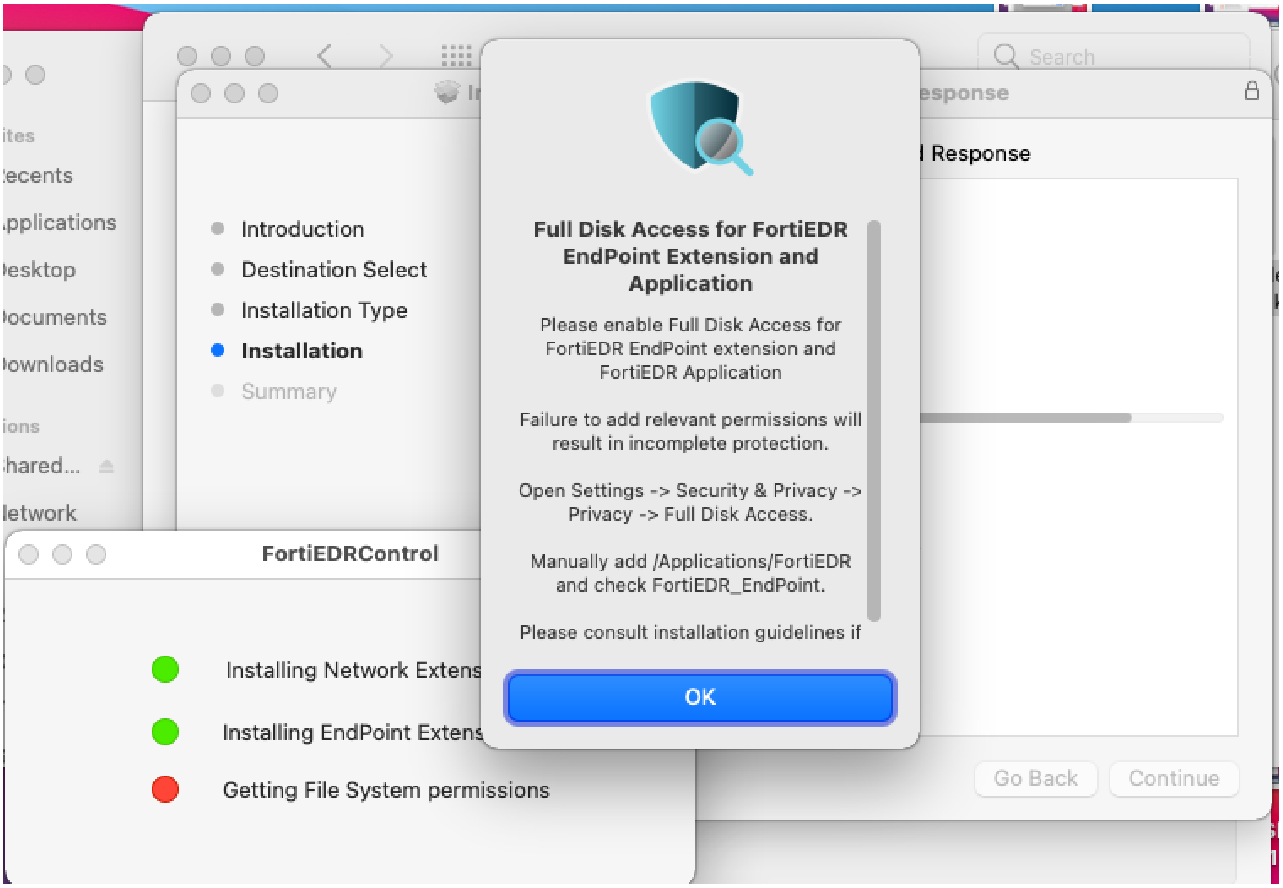
1. Click *Allow*.



"FortiEDRControl" Would Like to Filter Network Content

All network activity on this Mac may be filtered or monitored.

2. Click *OK*.



Full Disk Access for FortiEDR EndPoint Extension and Application

Please enable Full Disk Access for FortiEDR EndPoint extension and FortiEDR Application

Failure to add relevant permissions will result in incomplete protection.

Open Settings -> Security & Privacy -> Privacy -> Full Disk Access.

Manually add /Applications/FortiEDR and check FortiEDR_EndPoint.

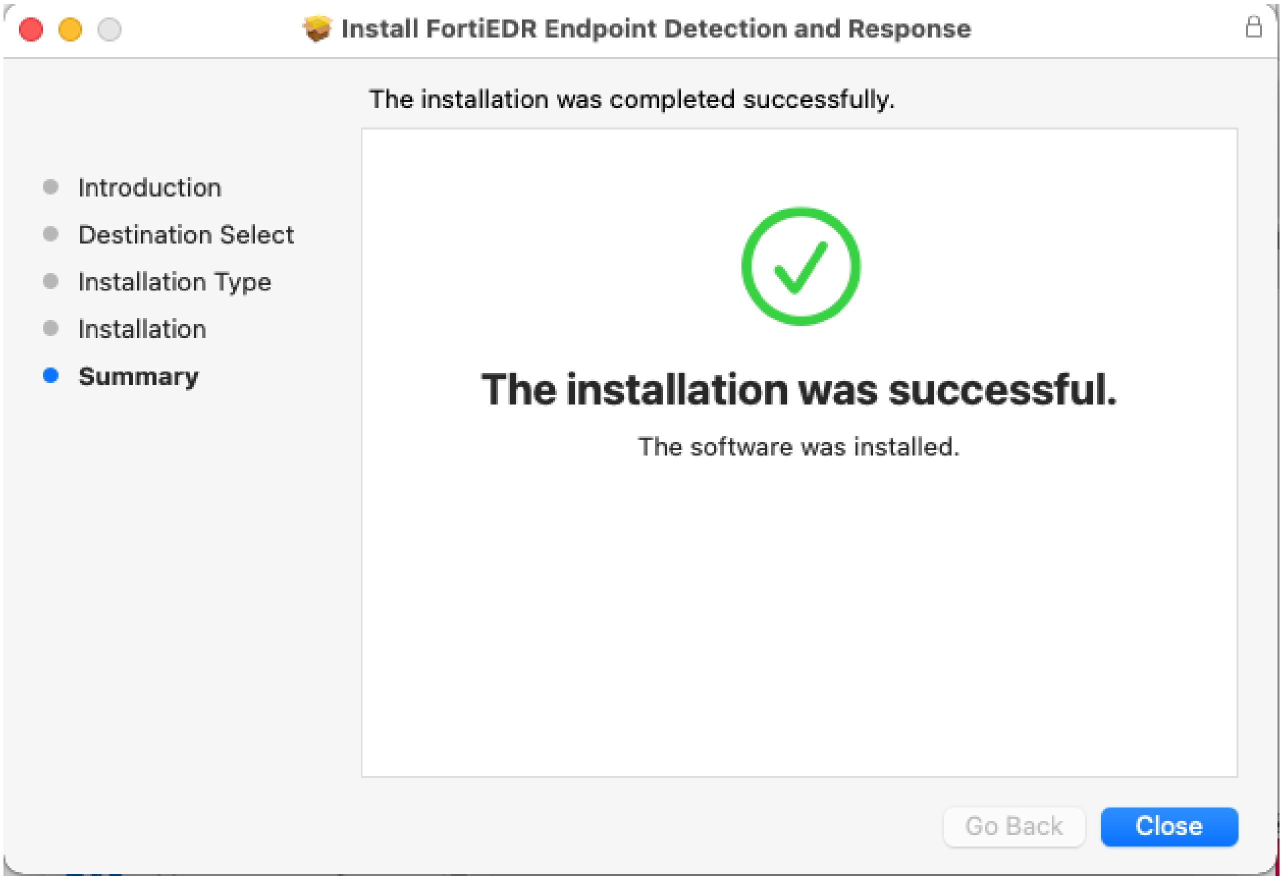
Please consult installation guidelines if

🟢 Installing Network Extens

🟢 Installing EndPoint Extens

🔴 Getting File System permissions

3. Click *Close* to complete the process.

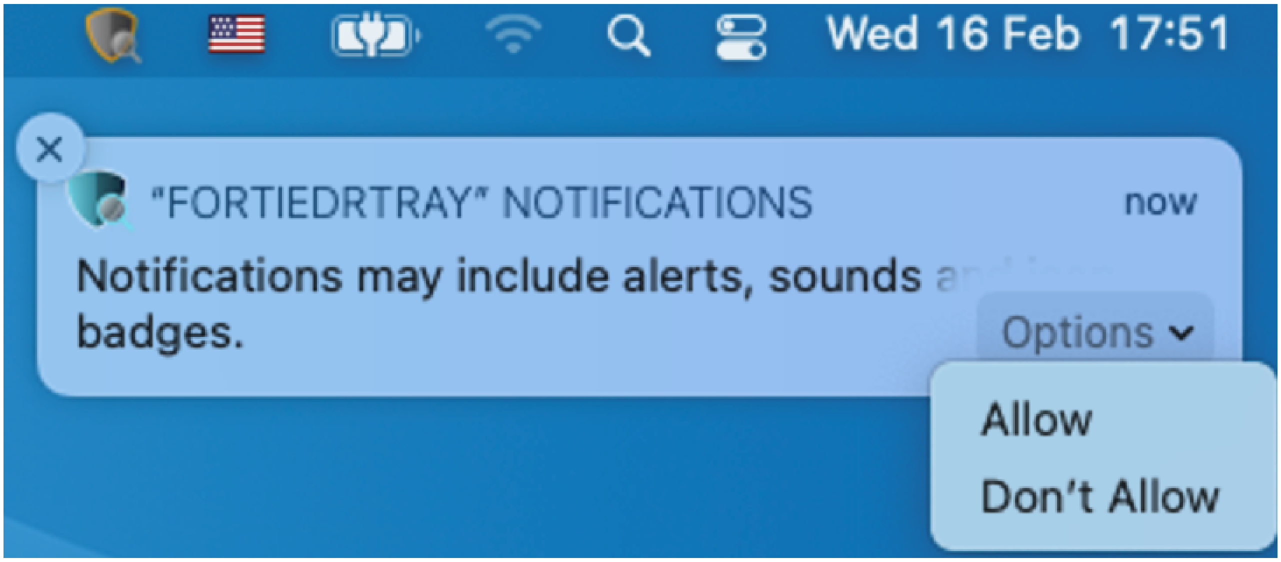


The installation was completed successfully.

The installation was successful.

The software was installed.

4. When prompted to allow FORTIEDRTRAY notifications, click *Allow*.



Notifications may include alerts, sounds a
badges.

5. Reboot the device.
6. Run the following command to check the status of the Collector:

- **Collector 6.0 or later**:

  ```
  /Applications/FortiEDR.app/Contents/Library/LaunchServices/fortiedr_collector.sh status
  ```

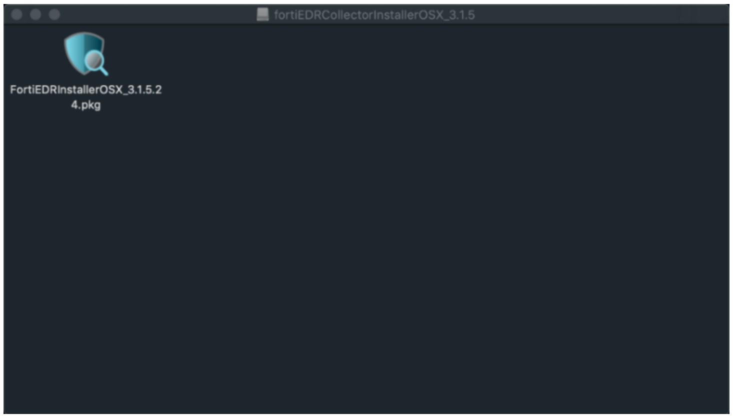
- **Collector earlier than 6.0**:

  ```
  /Applications/FortiEDR.app/fortiedr_collector.sh status
  ```

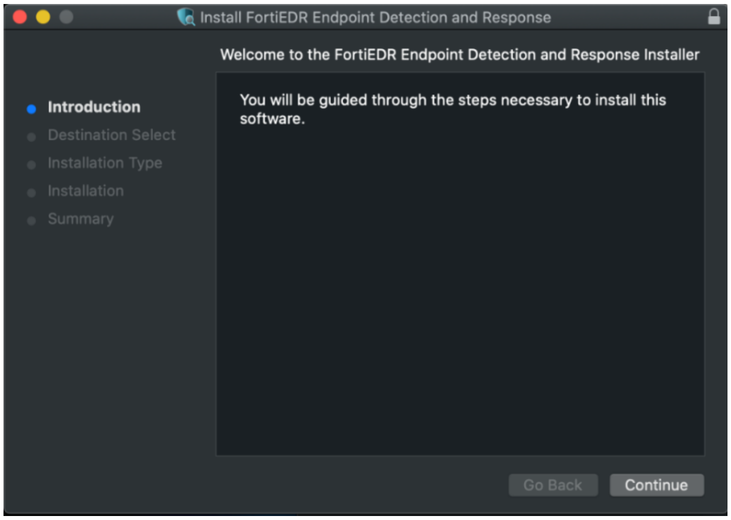
7. If another AV product is also installed on the machine, exclude AV exceptions by following the instructions in Setting up exclusions with other AV products on page 69.

To install a FortiEDR Collector on macOS with versions prior to Big Sur (11), such as Catalina or Mojave:

1. It is recommended to get a pre-populated customized Collector installer for macOS, as described in Requesting and obtaining a Collector installer on page 409.
2. Double-click the `*.dmg` file named `FortiEDRCollectorInstallerOSX_1.3.0.xxx.dmg`.
3. Double-click the `*.pkg` file named `FortiEDRCollectorInstallerOSX_1.3.0.xxx.pkg`.


fortiEDRCollectorInstallerOSX_3.1.5
FortiEDRInstallerOSX_3.1.5.24.pkg

4. Click *Continue*.

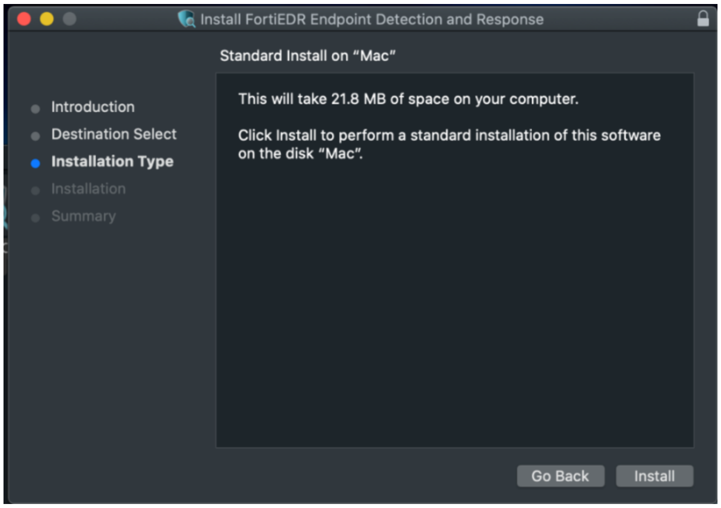


Install FortiEDR Endpoint Detection and Response

Welcome to the FortiEDR Endpoint Detection and Response Installer

You will be guided through the steps necessary to install this software.

5. Select the destination disk and click *Continue*.
6. Specify the installation location and click *Install*.



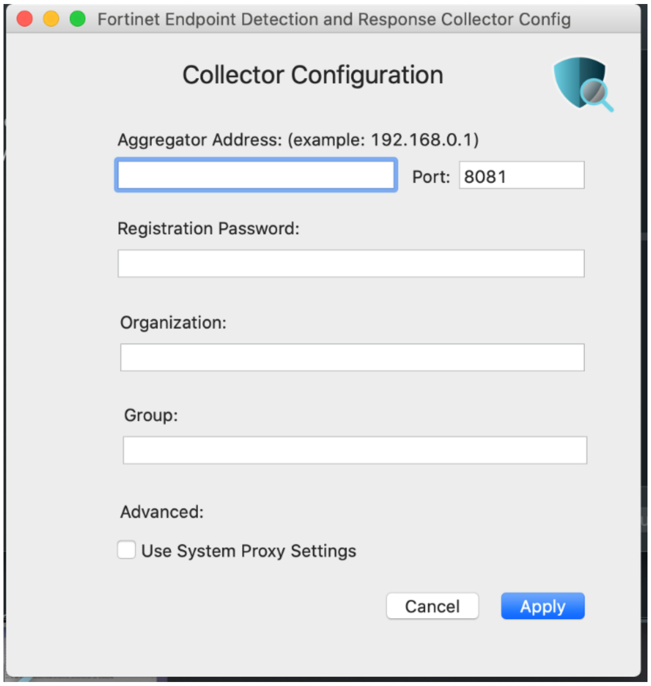
Install FortiEDR Endpoint Detection and Response

Standard Install on “Mac”

This will take 21.8 MB of space on your computer.

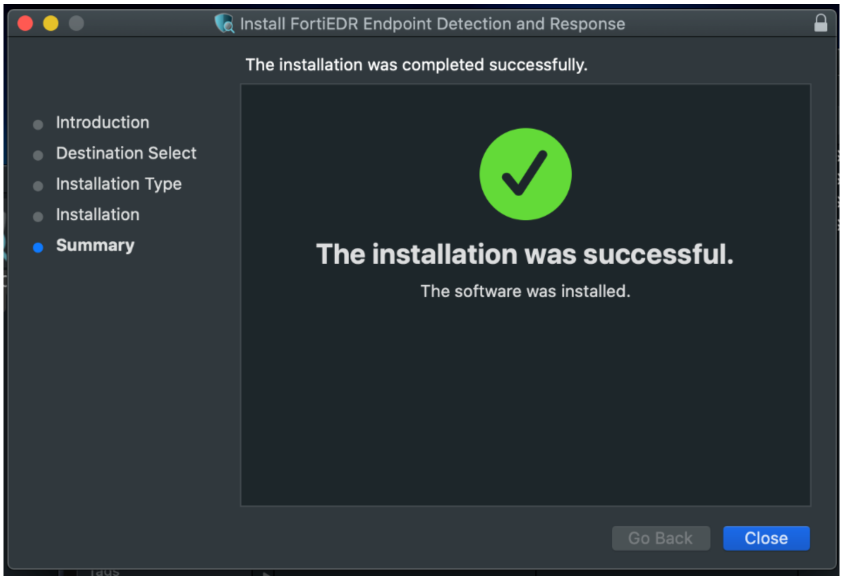
Click Install to perform a standard installation of this software on the disk “Mac”.

7. If a non-customized installer is used, in the *Aggregator Address* field, enter the IP address of the Aggregator in the first box and the port of the Aggregator in the adjacent (*Port*) box.


Fortinet Endpoint Detection and Response Collector Config
Collector Configuration
Aggregator Address: (example: 192.168.0.1)
Registration Password:
Organization:
Group:
Advanced:
□ Use System Proxy Settings
Cancel
Apply

Port: 8081

8. If a non-customized installer is used, in the *Registration Password* field, enter the registration password as described in Configuring the FortiEDR Central Manager server and console on page 474.
9. Leave the *Organization* field empty or for a multi-tenant setup, insert the organization to which this Collector belongs (as it appears under the *ADMINISTRATION > ORGANIZATIONS* tab of the FortiEDR Central Manager).
10. If you use a web proxy to filter requests in this device's network, then check the *Use System Proxy Settings* checkbox. Note that the MacOS must be configured to use a proxy and that the proxy must support HTTPS before installing the Collector (*System Preferences > Network > Advanced > Proxies*).
11. Click *Apply*.
12. Click *Close*.



The installation was completed successfully.

The installation was successful.

The software was installed.

13. If another AV product is also installed on the machine, exclude AV exceptions by following the instructions in Setting up exclusions with other AV products on page 69.

Installing a FortiEDR Collector on Linux

The FortiEDR Collector installation requires some dependencies. Ensure the Linux endpoint has network connection to the respective upstream package managers.

To install a customized FortiEDR Collector on Linux:

1. It is recommended to get a pre-populated customized Collector installer for Linux, as described in Requesting and obtaining a Collector installer on page 409.
2. Copy the custom Linux Collector installer zip file, `FortiEDRSilentInstall_5.1.0.195_envname_Tenant.zip` to the device. This file was downloaded from the provided link as described in Requesting and obtaining a Collector installer on page 409.
3. Unzip using the following command:

   ```
   sudo unzip ./FortiEDRSilentInstall_5.1.0.195_envname_Tenant.zip
   ```

   If you don’t have zip software on the device, install it using:

   ```
   yum install zip
   ```

4. Extract the installer using the following command:

   ```
   sudo gunzip ./FortiEDRSilentInstall_5.1.0.195_envname_Tenant.sh.gz
   ```

5. Change the installation script permission with the following command:

   ```
   chmod 755 FortiEDRSilentInstall_5.1.0.195_envname_Tenant.sh
   ```

6. Run the following to execute the installation script:

   ```
   sudo ./FortiEDRSilentInstall_5.1.0.195_envname_Tenant.sh
   ```

7. If another AV product is also installed on the machine, exclude AV exceptions by following the instructions in Exclusion paths.

To install a non-customized FortiEDR Collector on Linux:

1. Run the FortiEDR Collector installation file for 64-bit servers using the following command:
   - CentOS/RHEL/Oracle/AMI:

     `sudo yum install ./FortiEDRCollectorInstaller_%Linux_distribution%-%version_number%.x86_64.rpm`

     For example, `sudo yum install ./FortiEDRCollectorInstaller_CentOS6-3.1.0-74.x86_64.rpm`.
   - Ubuntu:

     `sudo apt-get install ./FortiEDRCollectorInstaller_Ubuntu-%version_number%.deb`

     For example, `sudo apt-get install ./FortiEDRCollectorInstaller_Ubuntu-3.1.0-74.deb`.
   - SUSE Linux:

     `rpm --import RPM-GPG-KEY.key`

     The FortiEDR PGP key is included in the download link of the pre-populated installer, see the Requesting and obtaining a Collector installer on page 409.

     `zypper install FortiEDRCollectorInstaller_%distribution% -%version_number%.rpm`

     For example: `zypper install FortiEDRCollectorInstaller_openSUSE15-4.5.0-88.x86_64.rpm`
2. After the installation is completed, run the following:

   ```
   sudo /opt/FortiEDRCollector/scripts/fortiedrconfig.sh
   ```
3. Specify the domain name/IP address and port (8081) of the Aggregator that the Collector registers with.

   > If you are installing the Linux Collector on an Aggregator, you cannot register the Collector with the same Aggregator that the Collector runs on. Register the Collector with another Aggregator instead.
4. For a multi-tenant setup, enter the organization. Otherwise, leave the organization empty.
5. Enter Collector Group information or leave empty to be registered to the default Collector Group.
6. Enter the device registration password, described in Configuring the FortiEDR Central Manager server and console on page 474.
7. At the *Do you want to connect via proxy (Y/N)?* prompt, type `Y` if your setup includes a web proxy.
8. If you are installing the Linux Collector build 5.1.5.1062 or later on a machine with secure boot enabled, at the *One or more modules are not signed. Would you like to sign them now?* prompt, type *Y* to sign the unsigned kernel modules or *N* to leave them unsigned.
9. If your software distribution system does not allow the addition of specific parameters to the command, you can use the custom FortiEDR Collector installer, which can be accessed via the Central Manager Console using the required DNS or IP address and password that is already embedded inside. For more details, see Requesting and obtaining a Collector installer on page 409.
10. If another AV product is also installed on the machine, exclude AV exceptions by following the instructions in Exclusion paths.

Automated FortiEDR Collector deployment

Automated FortiEDR Collector deployment on Windows

FortiEDR can be installed automatically via any software installation and distribution system.

To deploy a custom FortiEDR Windows Collector via a command line:

1. Get a pre-populated customized Collector installer for Windows, as described in Requesting and obtaining a Collector installer on page 409.
2. Use the following command syntax:

```
msiexec /i FortiEDRCollectorInstaller64.msi
```

3. If another AV product is also installed on the machine, exclude AV exceptions by following the instructions in Setting up exclusions with other AV products on page 69.

To deploy a non-customized FortiEDR Windows Collector via a command line:

1. Use the following command syntax:

```
msiexec /i FortiEDRCollectorInstaller64.msi /qn AGG=10.0.0.1:8081 PWD=1234
```

For example, to install a FortiEDR Collector on a 64-bit machine, connect it to a FortiEDR Aggregator on IP address 10.0.0.1 and use the device registration password 1234, enter the following command:

```
msiexec /i FortiEDRCollectorInstaller64.msi /qn AGG=10.0.0.1:8081 PWD=1234
```

You can specify which organization or Collector group to assign this Collector to by adding the ORG or DEFGROUP parameter. These parameters are optional. Values with spaces must be wrapped in double quotation marks.

For example, to install a FortiEDR Collector with the same configurations as above and assign it to the default organization and default Collector group, enter the following command:

```
msiexec /i FortiEDRCollectorInstaller64.msi /qn ORG="Default Organization" AGG=10.0.0.1:8081
PWD=1234 DEFGROUP="Default Collector Group"
```

The name of the Collector MSI file may be different.

For Collectors version 3.0.0 and above, you can set a designated group and/or organization. To do so, enter the following command:

```
./CustomerBootstrapGenerator --aggregator [IP] --password '[PASSWORD]' --organization '
[ORGANIZATION]' --group '[GROUP]' > CustomerBootstrap.js
```

2. Using web proxy can be configured for Collectors version 3.0.0 and above. To do so, append the parameter PROXY=1 to the command syntax shown above.
3. In general, a FortiEDR Collector does not require the device on which it is installed to reboot after its installation. However, in some cases, you may want to couple the installation of the FortiEDR Collector with a reboot of the device. To do so, append the parameter NEEDREBOOT=1 to the command syntax shown above.
   Collectors that are installed with this flag appear in the FortiEDR Central Manager as Pending Reboot (page 87) and will not start operating until the after the device is rebooted.

   In general, rebooting the device after installing a FortiEDR Collector is good practice, but is not mandatory. Rebooting may prevent a threat actor from attempting to exfiltrate data on a previously existing connection that was established before installation of the FortiEDR Collector.

4. When installing on a Citrix PVS golden image, append the parameter **CITRIXPVS=1** to the command syntax shown above.
5. If your software distribution system does not allow the addition of specific parameters to the command, you can use the custom FortiEDR Collector installer, which can be accessed via the Central Manager Console using the required DNS or IP address and password that is already embedded inside. For more details see Requesting and obtaining a Collector installer on page 409.
6. If another AV product is also installed on the machine, exclude AV exceptions by following the instructions in Setting up exclusions with other AV products on page 69.

Automated FortiEDR Collector deployment on Mac

To deploy a custom FortiEDR macOS Collector via a command line:

1. Get a pre-populated customized Collector installer for macOS as described in Requesting and obtaining a Collector installer on page 409.
2. Run the following command in order to install using the specified settings:

   ```
   sudo installer -pkg <package path> -target /
   ```

   For example, if the package file is FortiEDRInstallerOSX_2.5.2.38.pkg, use the following command:

   ```
   sudo installer -pkg ./FortiEDRInstallerOSX_2.5.2.38.pkg -target /
   ```

To deploy a non-customized FortiEDR macOS Collector via a command line:

Run the following command line to generate the settings file:

```
./CustomBootstrapGenerator --aggregator [IP] --password [PASSWORD] > CustomerBootstrap.jsn
```

If the Aggregator port is different than 8081 (which is set by default), you can add the following:

```
./CustomBootstrapGenerator --aggregator [IP] --password [PASSWORD] --port 8083 >
CustomerBootstrap.jsn
```

The following are optional parameters that can be used with the custom installer generator:

- If the Collector should be part of a designated Collector Group, use --group ‘[GROUP]’.
- For a multi-tenant setup, the organization to which this device belongs to can be added using

  ```
  --organization ‘[ORGANIZATION]’
  ```

- If a web proxy is being used to filter requests in this device’s network, use

  ```
   --useProxy '1'
  ```

The following is an example that includes all optional parameters:

```
./CustomBootstrapGenerator --aggregator [IP] --password [PASSWORD] --useProxy '1' --organization
‘[ORGANIZATION]’ --group ‘[GROUP]’ > CustomerBootstrap.jsn
```

If another AV product is also installed on the machine, exclude AV exceptions by following the instructions in Setting up exclusions with other AV products on page 69.

Automated FortiEDR macOS Collector deployment on Big Sur operating system devices with MDM

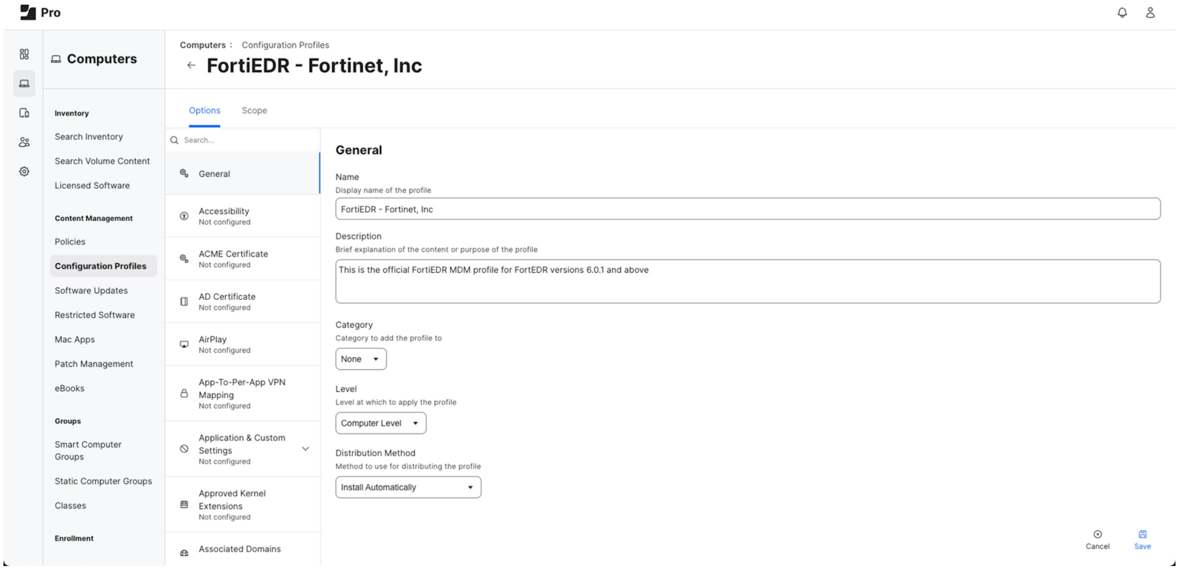
When distributed with MDM solutions such as Jamf, FortiEDR can be allowlisted with the following Team ID and Bundle ID identifiers:

- A97R6J3L29 com.ensilo.ftnt
- A97R6J3L29 com.ensilo.ftnt.sysext

Installing FortiEDR on MacOS devices using Jamf PRO

To install FortiEDR using Jamf PRO:

1. In Jamf PRO, navigate to *Computers* > *Configuration Profiles* > *New*.
2. Create a configuration profile as shown in the following screenshots:
   - **Collector version 6.0 and later:**
     i. Go to *Computer* > *Configuration Profiles*.
     ii. In the *General* tab, click *Edit*.



FortiEDR - Fortinet, Inc

General

Name
Display name of the profile
FortiEDR - Fortinet, Inc

Description
Brief explanation of the content or purpose of the profile
This is the official FortiEDR MDM profile for FortEDR versions 6.0.1 and above

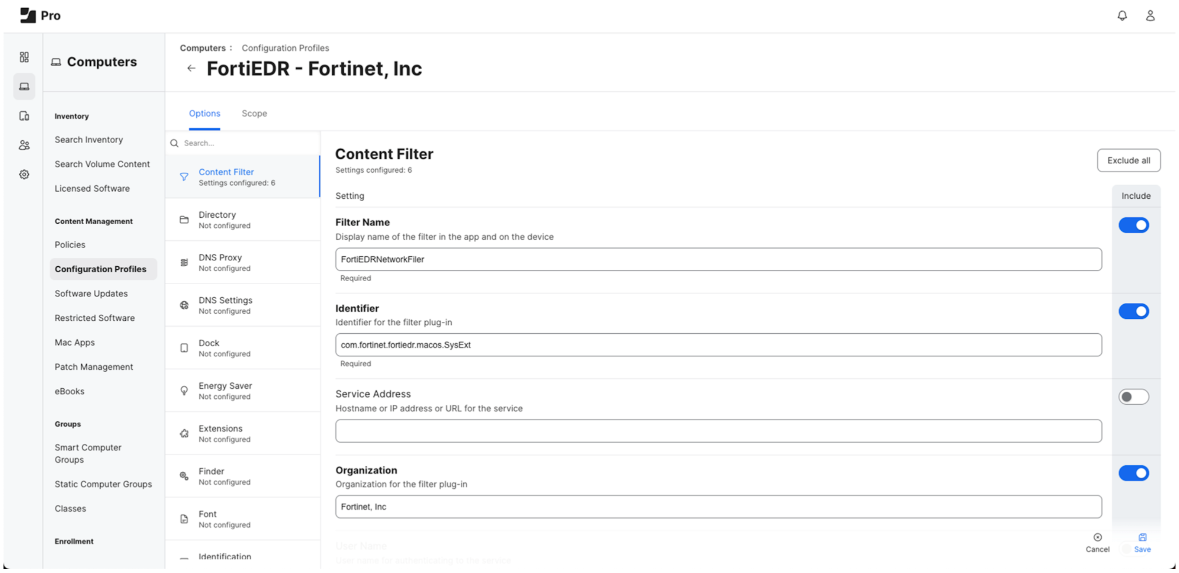
Category
Category to add the profile to
None

Level
Level at which to apply the profile
Computer Level

Distribution Method
Method to use for distributing the profile
Install Automatically

     iii. Configure the relevant settings, then click *Save*.
     iv. In the *Content Filter* tab, click *Edit*, and configure the relevant settings.
     Specify the values for the following fields:

Filter Name	FortiEDRNetworkFilter
Identifier	com.fortinet.fortiedr.macos.SysExt
Organization	Fortinet Inc.



Computers : Configuration Profiles

FortiEDR - Fortinet, Inc

Content Filter
Settings configured: 6

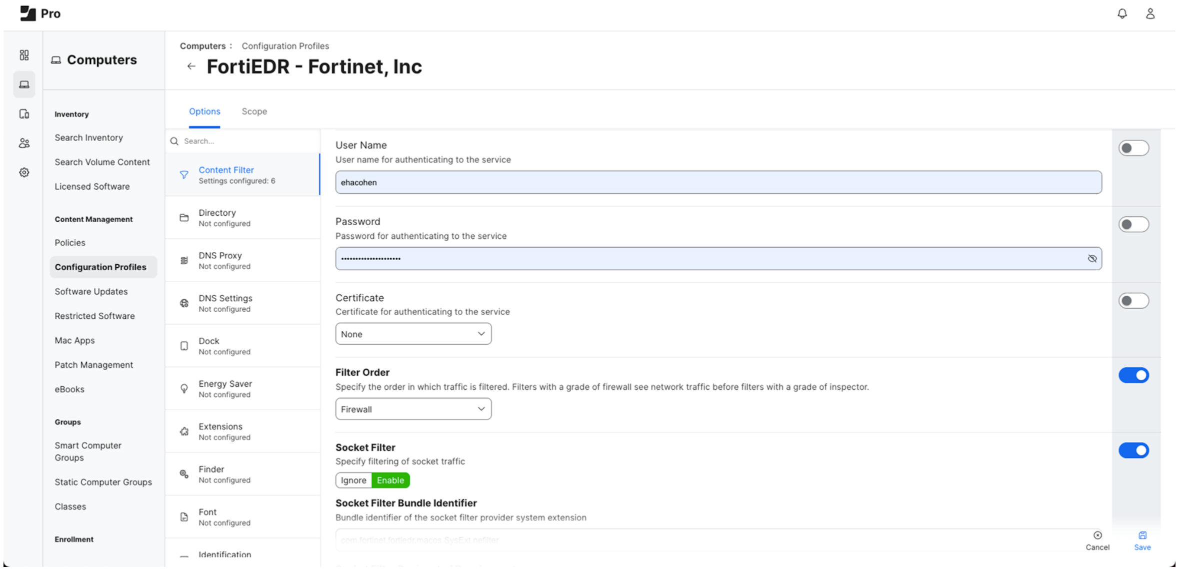
Setting

Filter Name
Display name of the filter in the app and on the device
FortiEDRNetworkFiler
Required

Identifier
Identifier for the filter plug-in
com.fortinet.fortiedr.macos.SysExt
Required

Service Address
Hostname or IP address or URL for the service

Organization
Organization for the filter plug-in
Fortinet, Inc



Computers : Configuration Profiles

FortiEDR - Fortinet, Inc

User Name
User name for authenticating to the service
ehacohen

Password
Password for authenticating to the service
••••••••••••••••••••

Certificate
Certificate for authenticating to the service
None

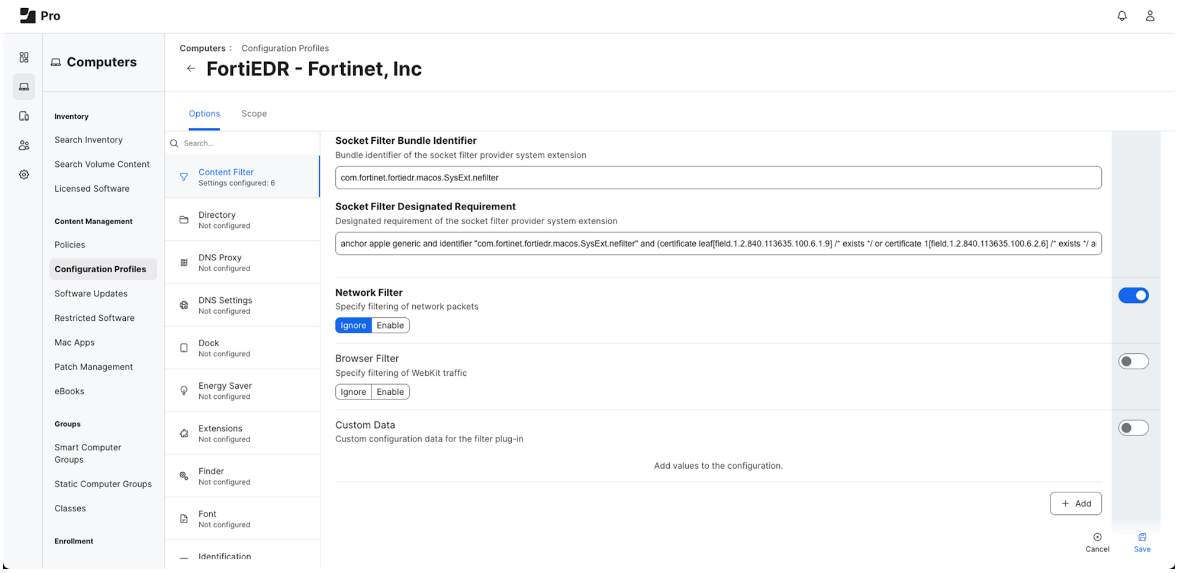
Filter Order
Specify the order in which traffic is filtered. Filters with a grade of firewall see network traffic before filters with a grade of inspector.
Firewall

Socket Filter
Specify filtering of socket traffic
Ignore [✓ Enable]

Socket Filter Bundle Identifier
Bundle identifier of the socket filter provider system extension

Specify the values for the following fields:

Socket Filter Bundle Identifier	com.fortinet.fortiedr.macos.SysExt.nefilter
Socket Filter Designated Requirement	anchor apple generic and identifier "com.fortinet.fortiedr.macos.SysExt.nefilter" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf [field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf [subject.OU] = AH4XFXJ7DK)



FortiEDR - Fortinet, Inc

Socket Filter Bundle Identifier
Bundle identifier of the socket filter provider system extension
com.fortinet.fortiedr.macos.SysExt.nefilter

Socket Filter Designated Requirement
Designated requirement of the socket filter provider system extension
anchor apple generic and identifier "com.fortinet.fortiedr.macos.SysExt.nefilter" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ a

Network Filter
Specify filtering of network packets
Ignore | Enable

Browser Filter
Specify filtering of WebKit traffic
Ignore | Enable

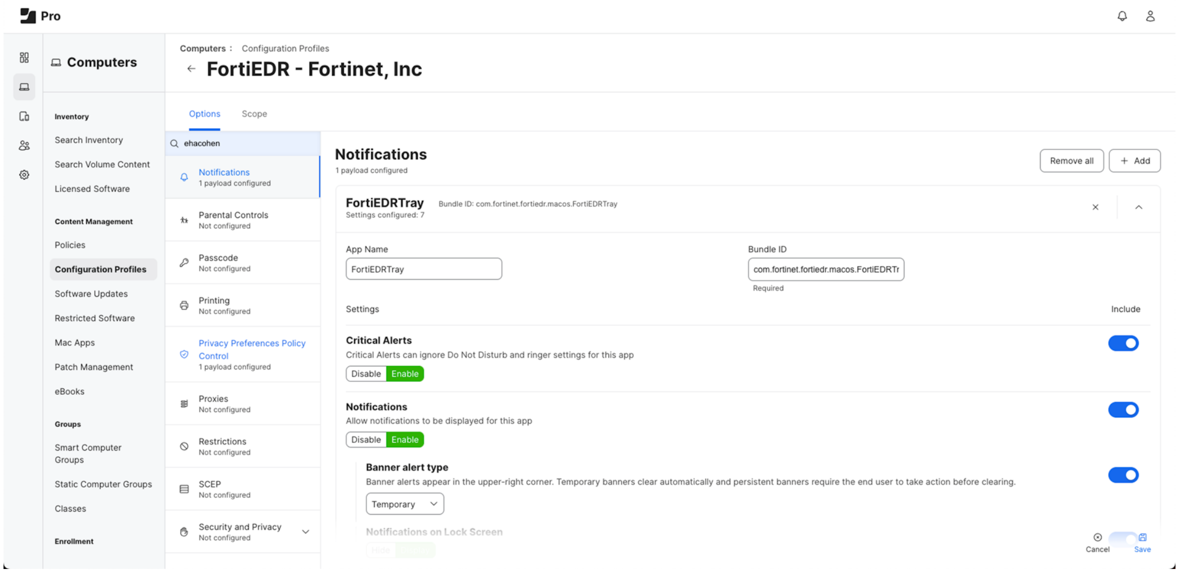
Custom Data
Custom configuration data for the filter plug-in

Add values to the configuration.

v. Click *Save*.

vi. In the *Notifications* tab, click *Edit*, and configure the relevant settings.

App Name	FortiEDRTray
Bundle ID	com.fortinet.fortiedr.macos.FortiEDRTray



FortiEDR - Fortinet, Inc

Notifications
1 payload configured

FortiEDRTray Bundle ID: com.fortinet.fortiedr.macos.FortiEDRTray
Settings configured: 7

App Name: FortiEDRTray

Bundle ID: com.fortinet.fortiedr.macos.FortiEDRTr
Required

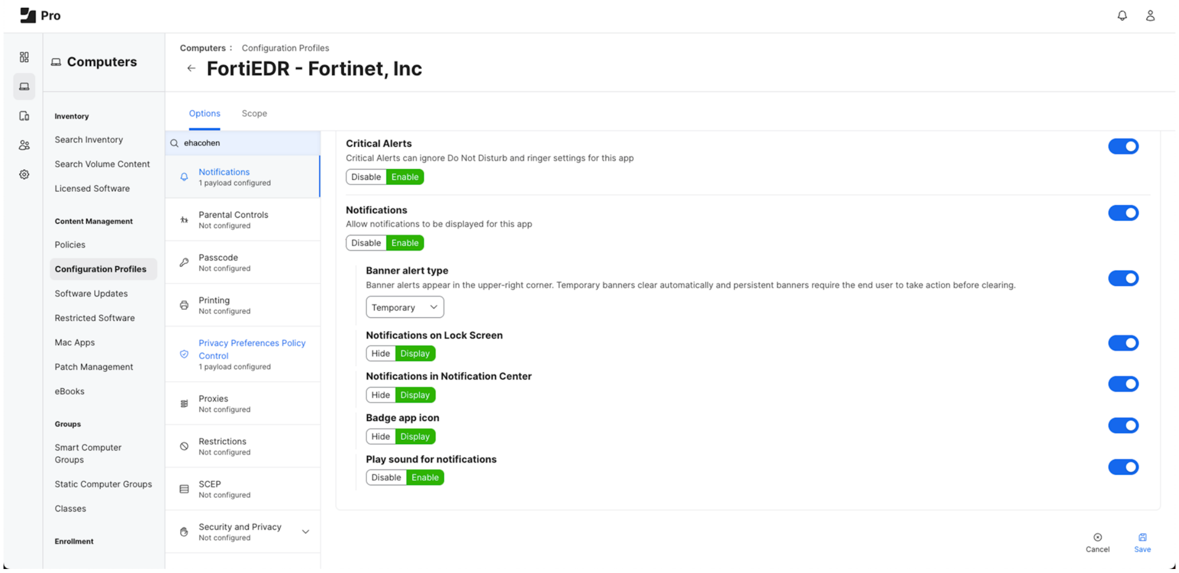
Settings | Include

Critical Alerts
Critical Alerts can ignore Do Not Disturb and ringer settings for this app
Disable | Enable

Notifications
Allow notifications to be displayed for this app
Disable | Enable

Banner alert type
Banner alerts appear in the upper-right corner. Temporary banners clear automatically and persistent banners require the end user to take action before clearing.
Temporary

Notifications on Lock Screen



FortiEDR - Fortinet, Inc

Critical Alerts
Critical Alerts can ignore Do Not Disturb and ringer settings for this app
Disable [✓ Enable]

Notifications
Allow notifications to be displayed for this app
Disable [✓ Enable]

Banner alert type
Banner alerts appear in the upper-right corner. Temporary banners clear automatically and persistent banners require the end user to take action before clearing.
Temporary

Notifications on Lock Screen
Hide [✓ Display]

Notifications in Notification Center
Hide [✓ Display]

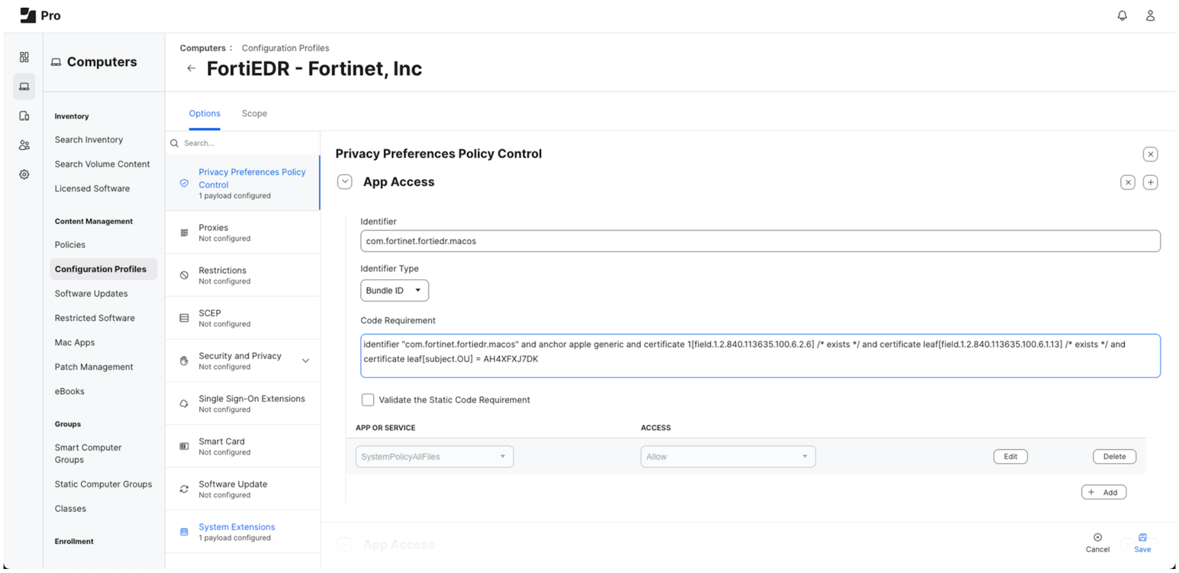
Badge app icon
Hide [✓ Display]

Play sound for notifications
Disable [✓ Enable]

vii. Click *Save*.

viii. In the *Privacy Preferences Policy Control* tab, click *Edit*, and configure three apps using the following values.

	App 1	App 2	App 3
Identifier	com.fortinet.fortiedr.macos	com.fortinet.fortiedr.macos.SysExt.esclient	com.fortinet.fortiedr.macos.FortiEDRCollector
Identifier Type	Bundle ID		
Code Requirement	identifier "com.fortinet.fortiedr.macos" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf [field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf [subject.OU] = AH4XFXJ7DK	anchor apple generic and identifier "com.fortinet.fortiedr.macos.SysExt.esclient" and (certificate leaf [field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf [field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = AH4XFXJ7DK)	identifier "com.fortinet.fortiedr.macos.FortiEDRCollector" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf [field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = AH4XFXJ7DK
Access	Allow		



Privacy Preferences Policy Control

App Access

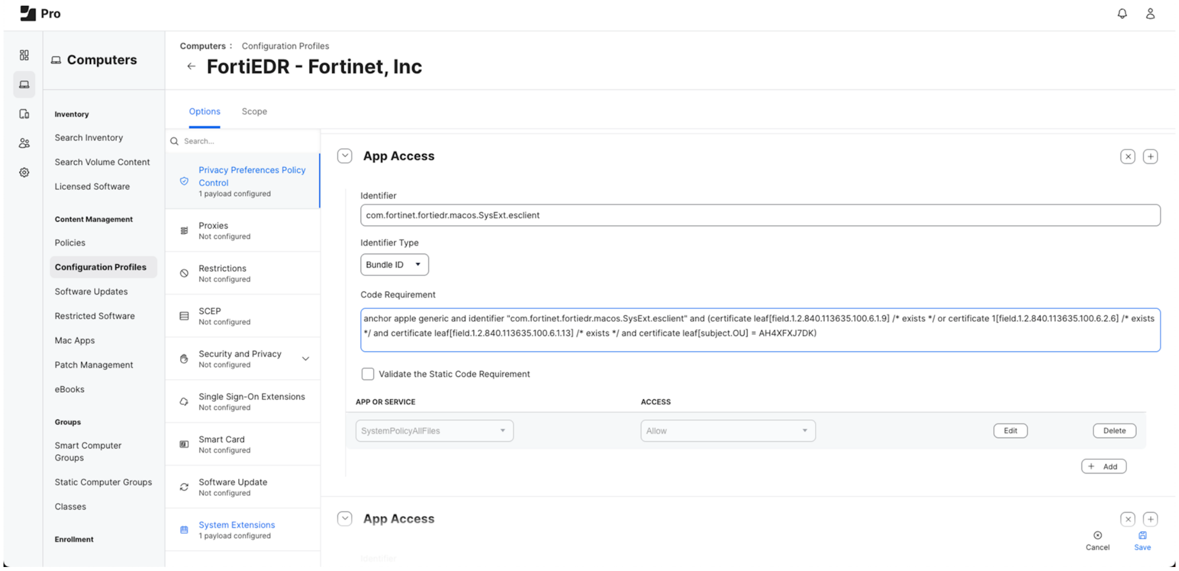
Identifier: com.fortinet.fortiedr.macos

Identifier Type: Bundle ID

Code Requirement: identifier "com.fortinet.fortiedr.macos" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = AH4XFXJ7DK

□ Validate the Static Code Requirement

APP OR SERVICE	ACCESS
SystemPolicyAllFiles	Allow



App Access

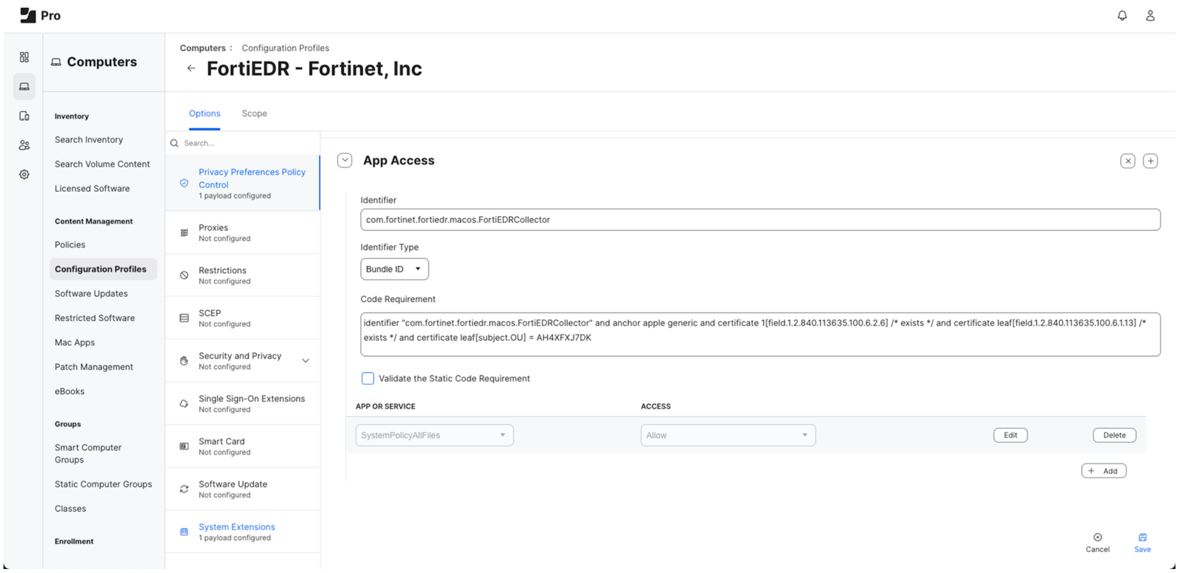
Identifier: com.fortinet.fortiedr.macos.SysExt.esclient

Identifier Type: Bundle ID

Code Requirement: anchor apple generic and identifier "com.fortinet.fortiedr.macos.SysExt.esclient" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = AH4XFXJ7DK)

□ Validate the Static Code Requirement

APP OR SERVICE	ACCESS
SystemPolicyAllFiles	Allow



App Access

Identifier: com.fortinet.fortiedr.macos.FortiEDRCollector

Identifier Type: Bundle ID

Code Requirement: identifier "com.fortinet.fortiedr.macos.FortiEDRCollector" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = AH4XFXJ7DK

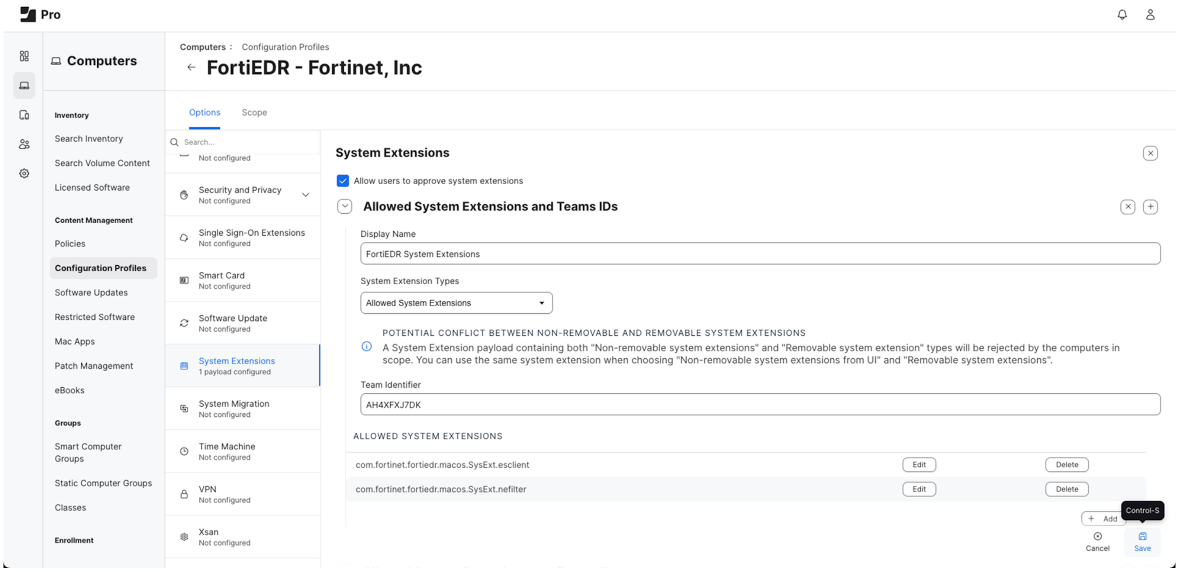
☐ Validate the Static Code Requirement

APP OR SERVICE	ACCESS
SystemPolicyAllFiles	Allow

ix. Click *Save*.

x. In the *System Extensions* tab, click *Edit*, and configure the relevant settings.

Display Name	FortiEDR System Extensions
System Extensions Types	Allowed System Extensions
Team Identifier	AH4XFXJ7DK
Allowed System Extensions	• com.fortinet.fortiedr.macos.SysExt.esclient • com.fortinet.fortiedr.macos.SysExt.nefilter



System Extensions

☑ Allow users to approve system extensions

Allowed System Extensions and Teams IDs

Display Name: FortiEDR System Extensions

System Extension Types: Allowed System Extensions

POTENTIAL CONFLICT BETWEEN NON-REMOVABLE AND REMOVABLE SYSTEM EXTENSIONS

A System Extension payload containing both "Non-removable system extensions" and "Removable system extension" types will be rejected by the computers in scope. You can use the same system extension when choosing "Non-removable system extensions from UI" and "Removable system extensions".

Team Identifier: AH4XFXJ7DK

ALLOWED SYSTEM EXTENSIONS

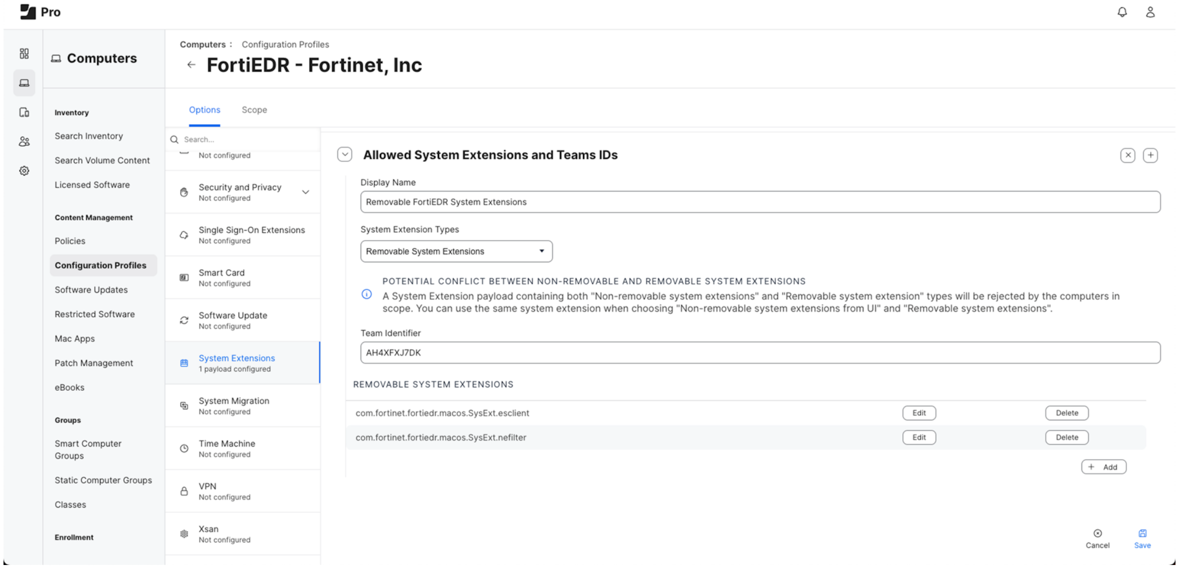
com.fortinet.fortiedr.macos.SysExt.esclient

com.fortinet.fortiedr.macos.SysExt.nefilter

Click *Add* and configure another system extension with the following values:

Display Name	Removeable FortiEDR System Extensions

System Extensions Types	Removeable System Extensions
Team Identifier	AH4XFXJ7DK
Allowed System Extensions	• com.fortinet.fortiedr.macos.SysExt.esclient • com.fortinet.fortiedr.macos.SysExt.nefilter



Computers : Configuration Profiles

FortiEDR - Fortinet, Inc

Allowed System Extensions and Teams IDs

Display Name: Removable FortiEDR System Extensions

System Extension Types: Removable System Extensions

POTENTIAL CONFLICT BETWEEN NON-REMOVABLE AND REMOVABLE SYSTEM EXTENSIONS
A System Extension payload containing both "Non-removable system extensions" and "Removable system extension" types will be rejected by the computers in scope. You can use the same system extension when choosing "Non-removable system extensions from UI" and "Removable system extensions".

Team Identifier: AH4XFXJ7DK

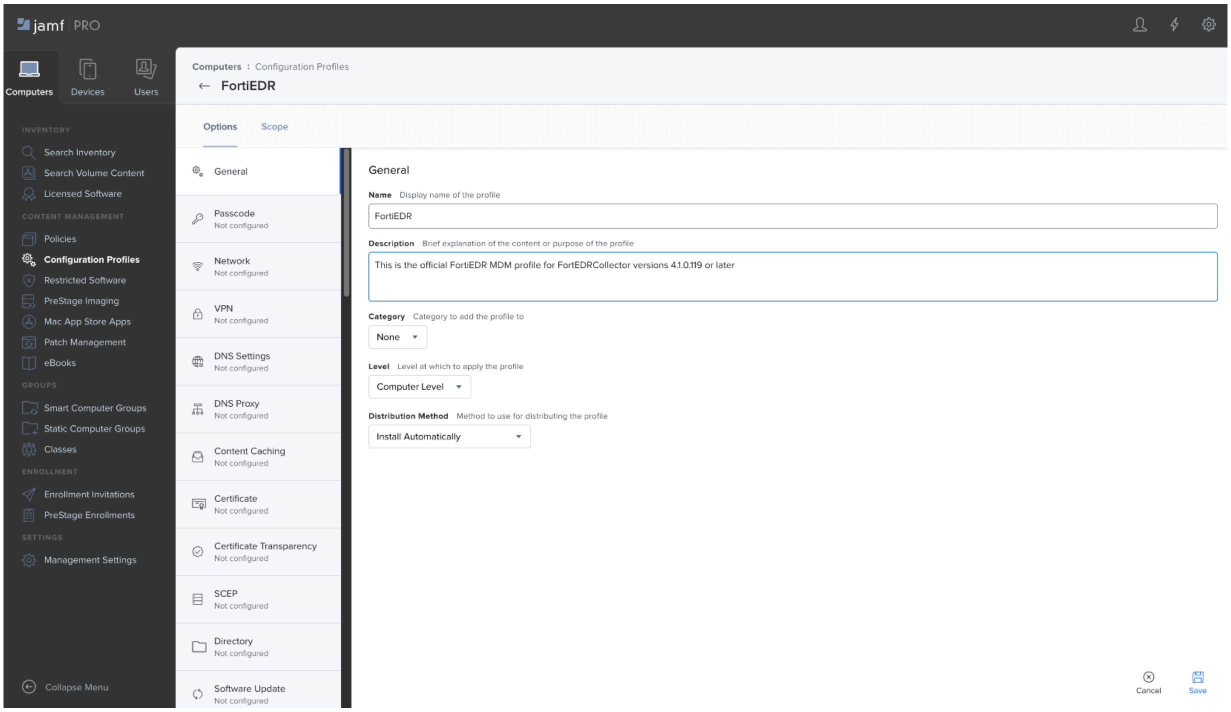
REMOVABLE SYSTEM EXTENSIONS

com.fortinet.fortiedr.macos.SysExt.esclient

com.fortinet.fortiedr.macos.SysExt.nefilter

xi. Click *Save*.

- **Collector versions earlier than 6.0:**



Computers : Configuration Profiles

FortiEDR

General

Name Display name of the profile: FortiEDR

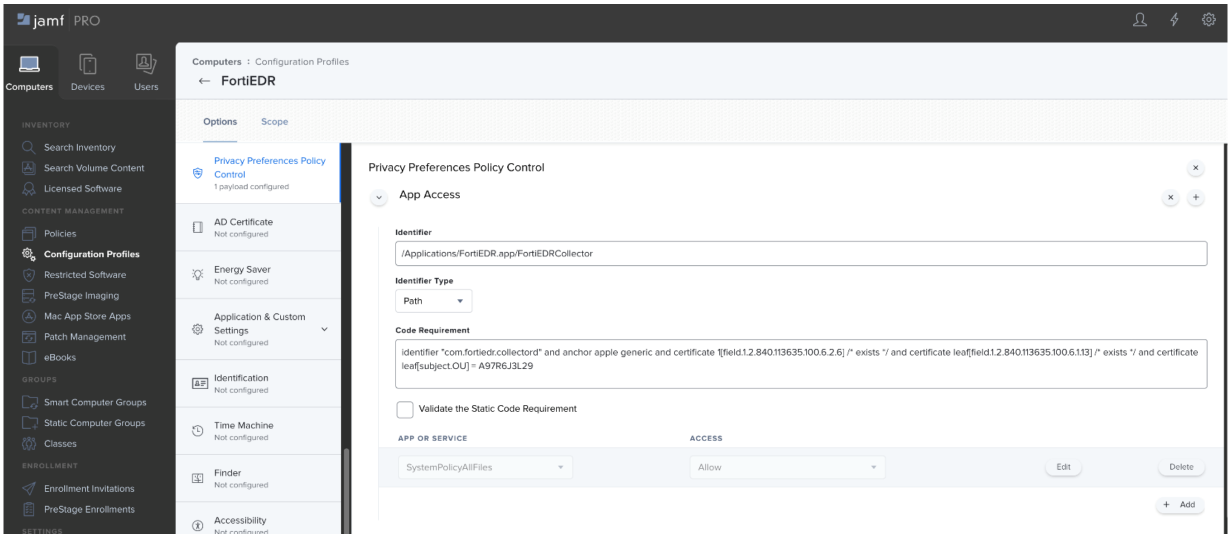
Description Brief explanation of the content or purpose of the profile: This is the official FortiEDR MDM profile for FortEDRCollector versions 4.1.0.119 or later

Category Category to add the profile to: None

Level Level at which to apply the profile: Computer Level

Distribution Method Method to use for distributing the profile: Install Automatically

	App 1	App 2
Identifier	/Applications/FortiEDR.app/FortiEDRCollector	com.ensilo.ftnt.sysext
Identifier Type	Path	Bundle ID
Code Requirement	identifier "com.fortiedr.collectord" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf [field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = A97R6J3L29	anchor apple generic and identifier "com.ensilo.ftnt.sysext" and (certificate leaf [field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf [field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf [subject.OU] = A97R6J3L29)
Access	Allow	



Privacy Preferences Policy Control

App Access

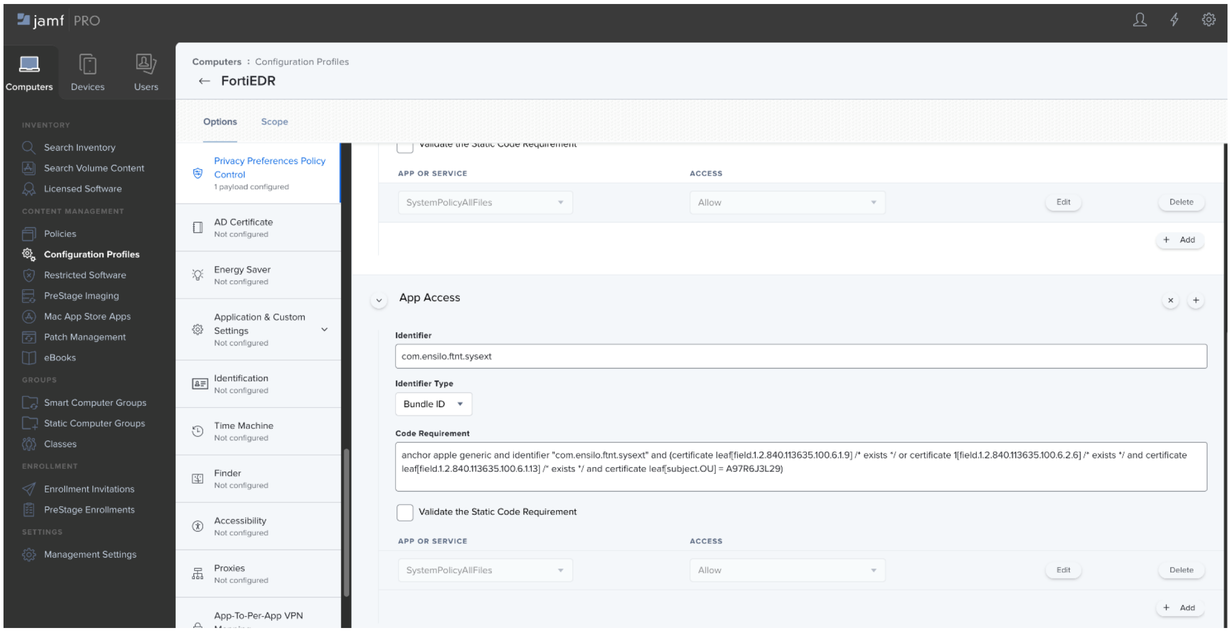
Identifier: /Applications/FortiEDR.app/FortiEDRCollector

Identifier Type: Path

Code Requirement: identifier "com.fortiedr.collectord" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = A97R6J3L29

□ Validate the Static Code Requirement

APP OR SERVICE	ACCESS
SystemPolicyAllFiles	Allow



App Access

Identifier: com.ensilo.ftnt.sysext

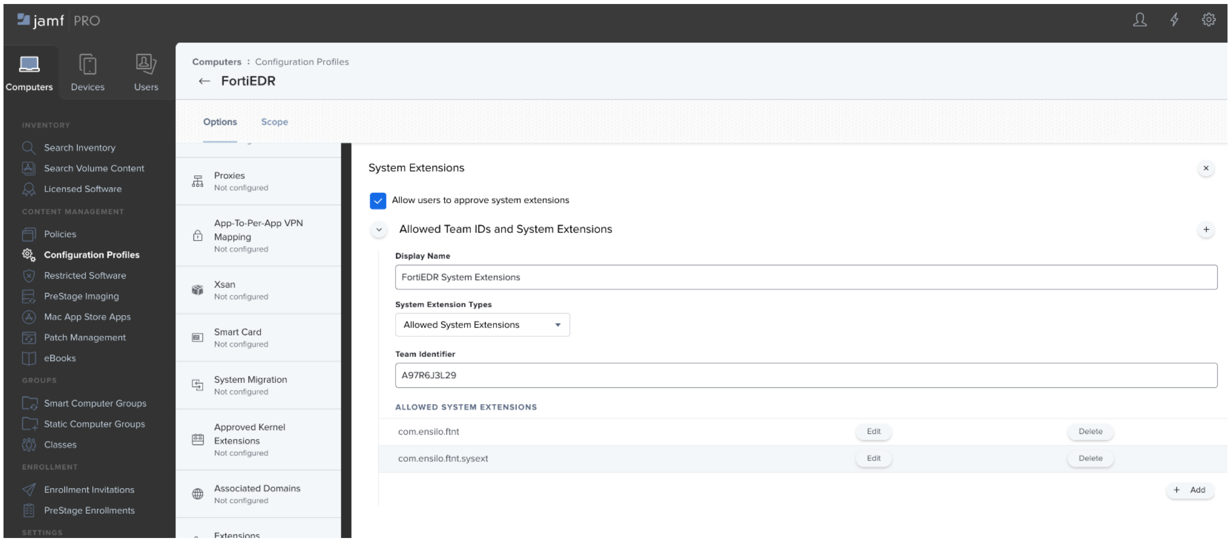
Identifier Type: Bundle ID

Code Requirement: anchor apple generic and identifier "com.ensilo.ftnt.sysext" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = A97R6J3L29)

☐ Validate the Static Code Requirement

APP OR SERVICE	ACCESS
SystemPolicyAllFiles	Allow

Display Name	FortiEDR System Extensions
System Extensions Types	Allowed System Extensions
Team Identifier	A97R6J3L29
Allowed System Extensions	• com.ensilo.ftnt • com.ensilo.ftnt.sysext



System Extensions

☑ Allow users to approve system extensions

Allowed Team IDs and System Extensions

Display Name: FortiEDR System Extensions

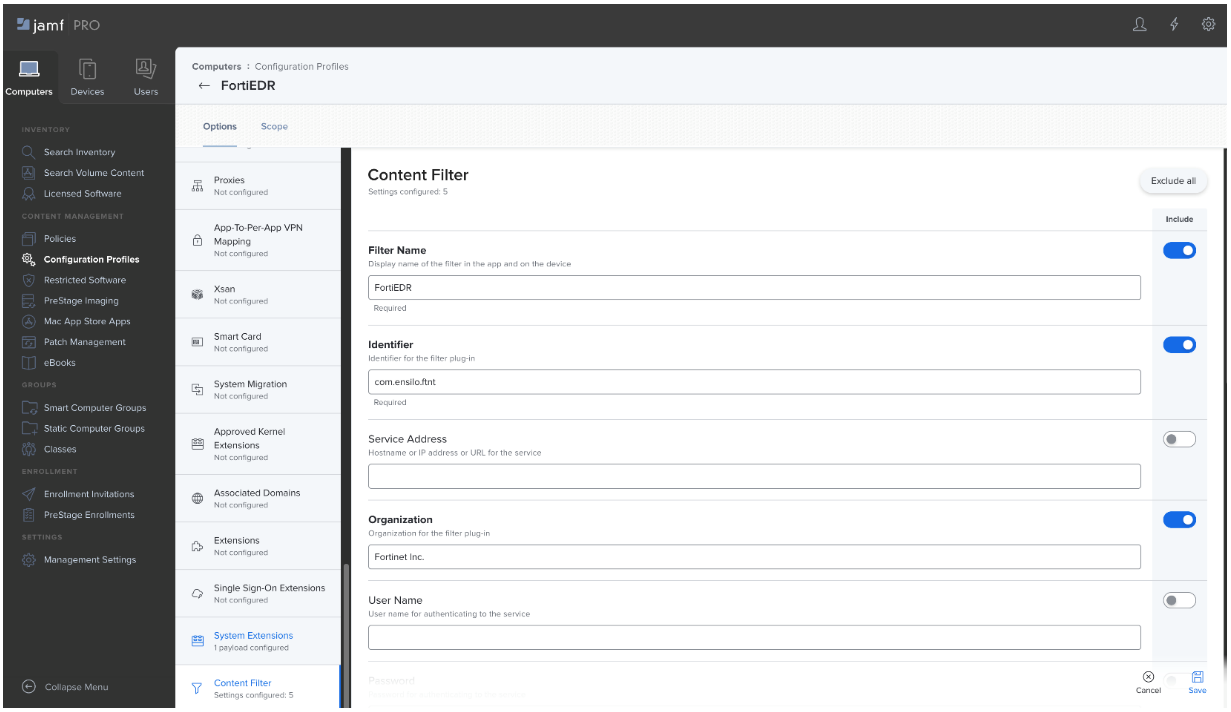
System Extension Types: Allowed System Extensions

Team Identifier: A97R6J3L29

ALLOWED SYSTEM EXTENSIONS

- com.ensilo.ftnt
- com.ensilo.ftnt.sysext

Filter Name	FortiEDR
Identifier	com.ensilo.ftnt
Organization	Fortinet Inc.



Content Filter
Settings configured: 5

Filter Name
Display name of the filter in the app and on the device
FortiEDR
Required

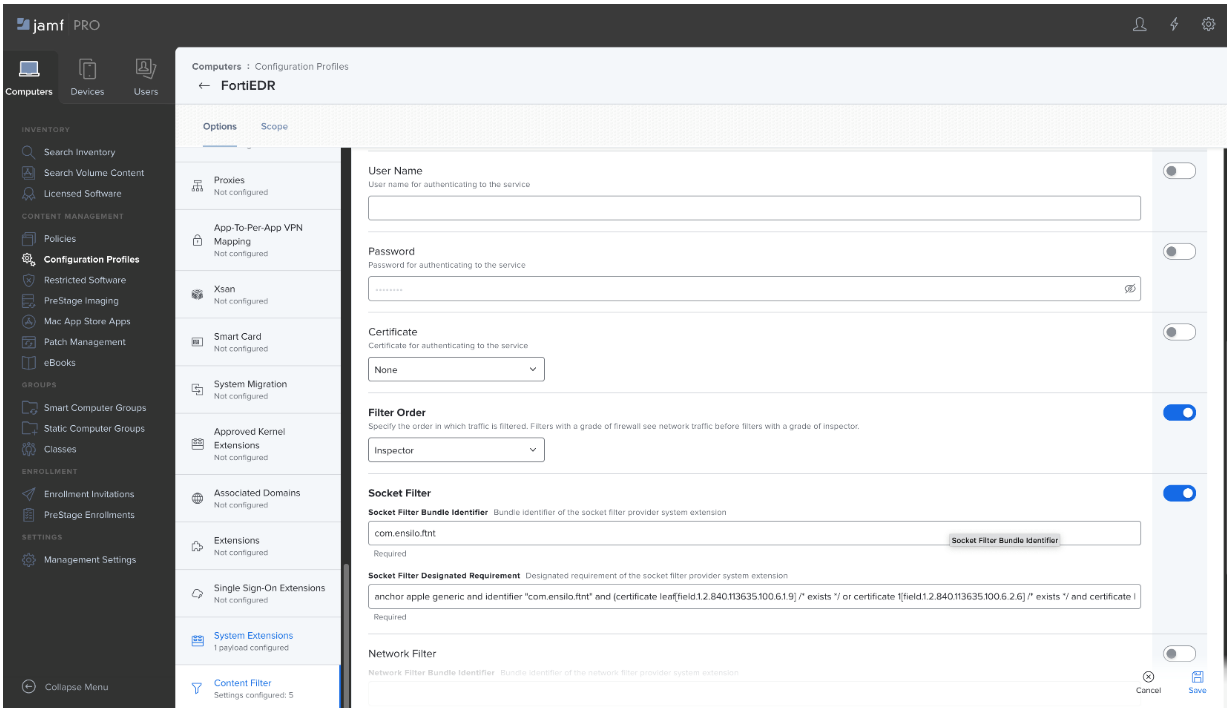
Identifier
Identifier for the filter plug-in
com.ensilo.ftnt
Required

Service Address
Hostname or IP address or URL for the service

Organization
Organization for the filter plug-in
Fortinet Inc.

User Name
User name for authenticating to the service

Password
Password for authenticating to the service



User Name
User name for authenticating to the service

Password
Password for authenticating to the service
....

Certificate
Certificate for authenticating to the service
None

Filter Order
Specify the order in which traffic is filtered. Filters with a grade of firewall see network traffic before filters with a grade of inspector.
Inspector

Socket Filter

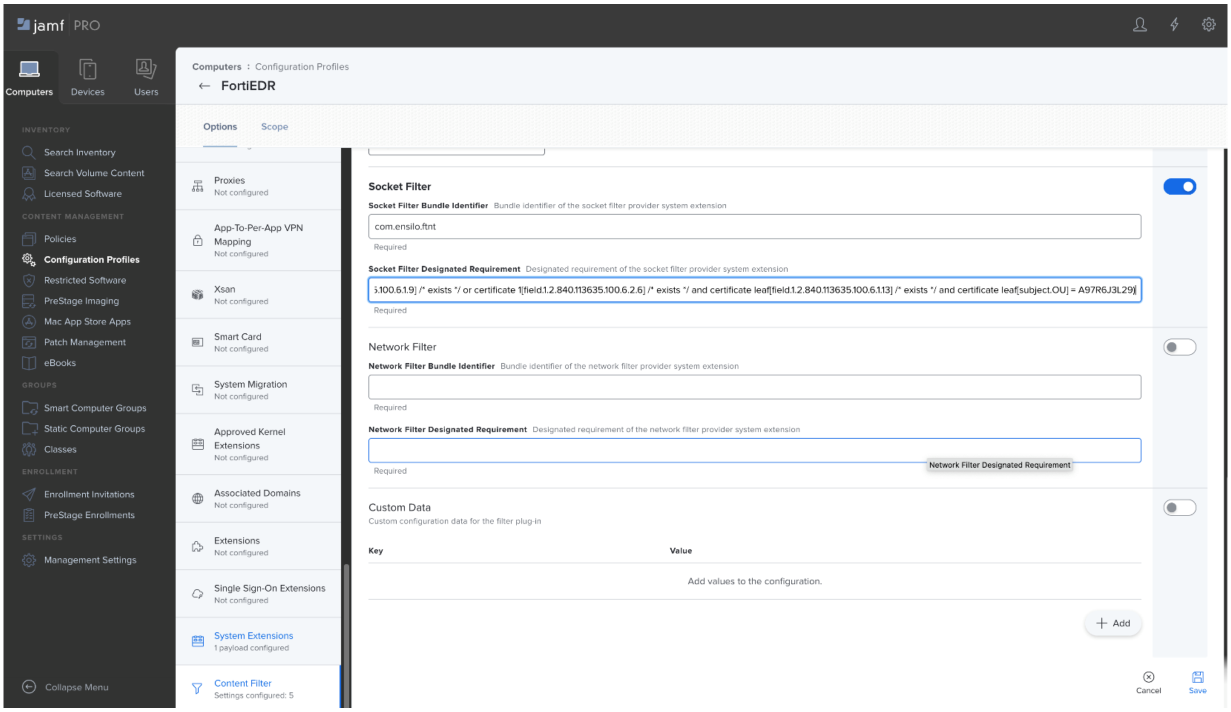
Socket Filter Bundle Identifier Bundle identifier of the socket filter provider system extension
com.ensilo.ftnt
Required

Socket Filter Designated Requirement Designated requirement of the socket filter provider system extension
anchor apple generic and identifier "com.ensilo.ftnt" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate l
Required

Network Filter
Network Filter Bundle Identifier Bundle identifier of the network filter provider system extension

Socket Filter	com.ensilo,ftnt
Socket Filter Designated Requirement	anchor apple generic and identifier "com.fortinet.fortiedr.macos.SysExt.nefilter" and (certificate leaf [field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf

	[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf [subject.OU] = A97R6J3L29)



Socket Filter

Socket Filter Bundle Identifier Bundle identifier of the socket filter provider system extension

com.ensilo.ftnt

Required

Socket Filter Designated Requirement Designated requirement of the socket filter provider system extension

5.100.6.1.9] /* exists */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = A97R6J3L29)

Required

Network Filter

Network Filter Bundle Identifier Bundle identifier of the network filter provider system extension

Required

Network Filter Designated Requirement Designated requirement of the network filter provider system extension

Network Filter Designated Requirement

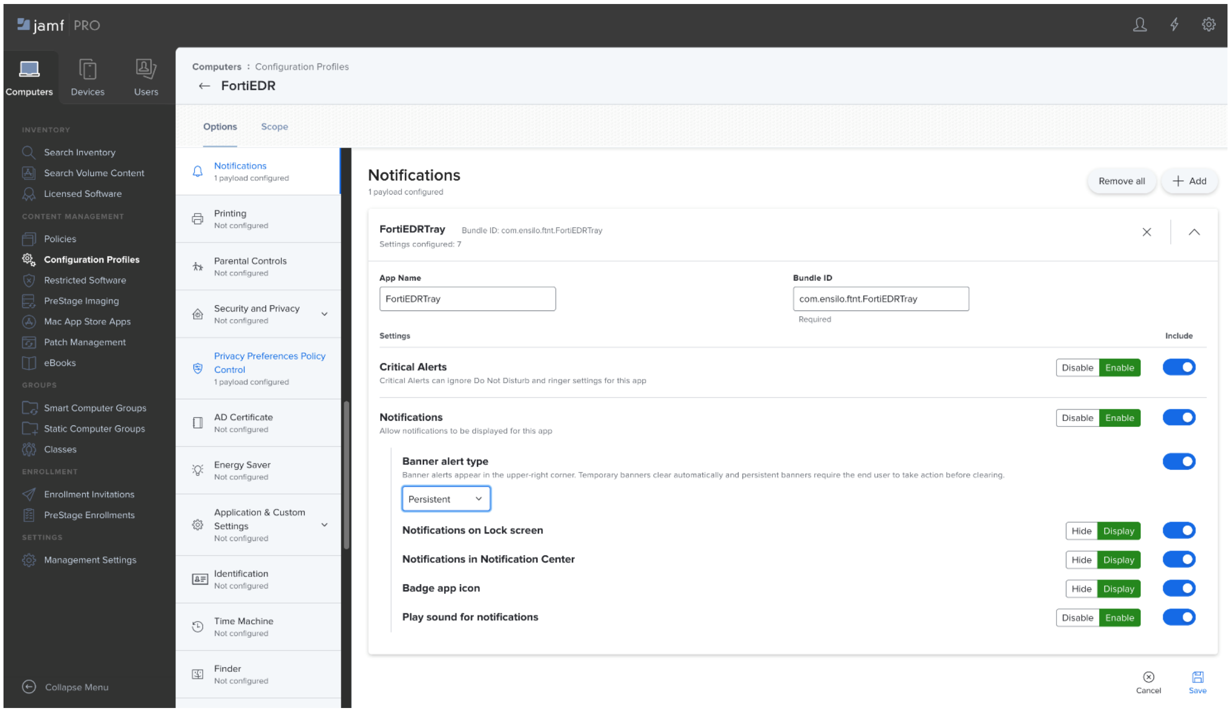
Required

Custom Data

Custom configuration data for the filter plug-in

Key	Value
Add values to the configuration.	

App Name	FortiEDRTray
Bundle ID	com.ensilo.ftnt.FortiEDRTray



Notifications

1 payload configured

FortiEDRTray Bundle ID: com.ensilo.ftnt.FortiEDRTray

Settings configured: 7

App Name: FortiEDRTray

Bundle ID: com.ensilo.ftnt.FortiEDRTray

Required

Settings		Include
Critical Alerts Critical Alerts can ignore Do Not Disturb and ringer settings for this app	Disable [✓ Enable]	●
Notifications Allow notifications to be displayed for this app	Disable [✓ Enable]	●
Banner alert type Banner alerts appear in the upper-right corner. Temporary banners clear automatically and persistent banners require the end user to take action before clearing. Persistent		●
Notifications on Lock screen	Hide [✓ Display]	●
Notifications in Notification Center	Hide [✓ Display]	●
Badge app icon	Hide [✓ Display]	●
Play sound for notifications	Disable [✓ Enable]	●

A sample Jamf profile for upload can be provided upon request.

3. If another AV product is also installed on the machine, exclude AV exceptions by following the instructions in Exclusion paths.

Setting up exclusions with other AV products

If another AV product (such as FortiClient) is also installed on the machine, you must exclude AV exceptions in both FortiEDR and the other AV product to avoid collision which might cause the endpoint to run slowly or hang:

1. In FortiEDR, add exclusion paths for the other AV product according to the directions in the other AV product. Note that FortiEDR supports exclusions on Windows only.
2. In the other AV product, add the following exclusion paths for FortiEDR:

Windows	macOS	Linux
• `%ProgramData%\FortiEDR\` • `%ProgramFiles%\Fortinet\FortiEDR` • `%ProgramFiles%\Fortinet\FortiEDR\FortiEDRCollector.exe` • `%ProgramFiles%\Fortinet\FortiEDR\FortiEDRCollectorService.exe` • `%ProgramFiles%\Fortinet\FortiEDR\FortiEDRAvScanner.exe` • `%ProgramFiles%\Fortinet\FortiEDR\FortiEDRInventoryScanner.exe` • `%ProgramFiles%\Fortinet\FortiEDR\FortiEDRIotDiscovery.exe` • `%windir%\System32\drivers\FortiEDRAvDriver_*.sys` • `%windir%\System32\drivers\FortiEDRBaseDriver_*.sys` • `%windir%\System32\drivers\FortiEDRElamDriver_*.sys` • `%windir%\System32\drivers\FortiEDRIotDriver_*.sys` • `%windir%\System32\drivers\FortiEDRWinDriver_*.sys`	• `/Library/FortiEDR` • `/Applications/FortiEDR.app` • `/Library/FortiEDR/FortiEDRCollector` • `/Library/FortiEDR/FortiEDRCollectorTray` • `/Library/FortiEDR/FortiEDRConfig` • `/Library/FortiEDR/FortiEDRDrive` • `/Library/Extensions/FortiEDRDriver.kext`	• `/opt/FortiEDRCollector`

Working with FortiEDR on VDI environments

The FortiEDR Collector must only be installed on the master image (not on a clone) of the VMware Horizon or Citrix XenDesktop in order to ensure that the virtual environment is protected. On Citrix, it is also recommended to install the Collector on the Windows servers that run the entire Citrix platform.

When installing the Collector, set the VDI-designated installation flag. To do so, append the parameter **VDI=1** to the command syntax shown above or check the *VDI* checkbox in the installation wizard, as shown in Installing FortiEDR Collectors on page 23.

When installing on a Citrix PVS golden image, append an additional parameter **CITRIXPVS=1** to the command syntax shown above.

After the Collector is successfully installed and running on the golden image and before the image is being cloned, the FortiEDR Collector configuration must be erased such so that cloned images will not show up as the same Collector on the Central Manager console. To do that so, run the following command as an administrator:

```
FortiEDRCollectorService.exe --stop --clean
```

In VDI installations where VDI pools are used, there is no need to generate Collector groups in the user interface. Any newly generated virtual desktop is automatically assigned to the default VDI Collectors group. Upon first user login to the virtual desktop, FortiEDR automatically generates a Collector group that corresponds with the respective pool name, as specified in VMware Horizon. Any Collector that is installed on a virtual desktop that is part of this pool is automatically assigned from the default VDI Collectors group to the corresponding Collector group, regardless of whether the pool definition in VMware is *dedicated* or *floating*. In effect, Collector groups in the FortiEDR user interface are a copy of the virtual machines' pool on VMware Horizon or Citrix.

Any newly created Collector group is automatically assigned to an out-of-the-box predefined policy. This mechanism ensures that any newly created virtual machine is automatically and immediately protected by a unique instance of the FortiEDR Collector.

When using FortiEDR automatic updates to Collectors via the Central Manager, make sure to update the master image too. Otherwise, every time that a new environment is created from the master image, an automatic update is performed, which can overload network traffic.

Uninstalling FortiEDR Collectors

You can uninstall a FortiEDR Collector using the following methods:

- From the Central Manager *INVENTORY > Collectors* page

  This method is recommended for Windows, Linux, and macOS 10.11 to 10.15.

  For macOS 11 or later, due to a macOS design limitation, this method does not remove the FortiEDR Collector system extension, which can only be uninstalled using an MDM solution.

- Through the operating system's application management (for example, Add or Remove Programs on Windows)
- Using dedicated FortiEDR scripts

The following section describes how to uninstall a FortiEDR Collector with Fortinet scripts.

Windows

Uninstall the Collector by running either of the following commands as administrator. Replace ***REGPWD*** with the registration password used for the installation, which is available in Component Authentication on page 316.

- `msiexec.exe /x GUID /qn UPWD=REGPWD RMCONFIG=1 /l*vx log.txt`

  Replace ***GUID*** with the FortiEDR uninstallation product key, which can be found by following the steps below:

  a. Select *Start >> Run*.

  b. Type `regedit` to open the *Registry Editor* window.

  c. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\`.

  d. Expand the *Uninstall* subkeys in the left-hand pane and search for "FortiEDR" to locate the subkey for FortiEDR.

  e. Open the FortiEDR subkey and copy the *UninstallString* value in the right pane, for example, *{01C88AE6-6782-4798-81C6-954E0D14FCF5}*.

  f. Close the *Registry Editor* window.
- `msiexec /x FortiEDRCollectorInstaller_X.msi /qn UPWD=REGPWD RMCONFIG=1`

  You must run this command from same directory as the msi installer. Or you can replace the msi filename with the full path to the msi file, such as `C:\Users\Allen\Desktop\FortiEDRCollectorInstaller64_4.1.0.491.msi`, which allows you to run the command anywhere.

macOS

To uninstall the Collector on macOS with versions prior to Big Sur (11), such as Catalina or Mojave:

```
sudo /Library/FortiEDR/fortiedr_uninstaller.sh 'REGISTRATION PASSWORD'
```

It is good practice to use REGISTRATION PASSWORD wrapped with single quotes so that it is interpreted correctly by the shell. For example,

```
sudo /Library/FortiEDR/fortiedr_uninstaller.sh '!EPdzv30break'
```

To uninstall the Collector on macOS with Big Sur (version 11) or above:

- **Collector versions earlier than 6.0:**

  ```
  /Applications/FortiEDR.app/fortiedr_uninstaller.sh 'REGISTRATION PASSWORD'
  ```
- **Collector version 6.0:**

```
/Applications/FortiEDR.app/Contents/Library/LaunchServices/fortiedr_uninstaller.sh
'REGISTRATION_PASSWORD'
```

Linux

Uninstalling a Linux Collector removes all configuration files. You must reconfigure all settings after installing a new Linux Collector.

If you are uninstalling a non-customized Linux Collector installer and would like to retain the configuration for later use, Fortinet recommends that you upgrade the Linux Collector instead of uninstalling the current Collector and re-installing a new one. However, you cannot perform an upgrade on a custom Linux Collector.

To uninstall a Collector on Linux:

1. Check the status of the Collector using the following command:

   ```
   /opt/FortiEDRCollector/control.sh --status
   ```

   The Collector should be stopped before running the uninstall command.
2. If the status is not stopped, stop the Collector using the following command:

   ```
    /opt/FortiEDRCollector/control.sh --stop <registration password>
   ```

   For example:

   ```
   / opt/FortiEDRCollector/control.sh --stop 12345678
   ```
3. Uninstall the Collector using the following command:
   - CentOS, RHEL, Oracle, AMI, SLES:

     -
       ```
       yum remove <package name>
       ```

       OR

     -
       ```
       rpm -qa | grep -i fortiedr | xargs rpm –e
       ```

- Ubuntu:

```
sudo dpkg --purge fortiedrcollectorinstaller
```

Upgrading the Collector

After a Collector has been installed in the system, you can upgrade it using one of the following methods:

- Updating the Collector version on page 405
- As described in the procedure below.

To upgrade the Collector manually (not via the user interface):

Windows

1. Copy the `FortiEDRCollectorInstallaler32_x.x.x.xxx.msi` or `FortiEDRCollectorInstallaler64_x.x.x.xxx.msi` file (as appropriate) to the Collector machine. For example, `FortiEDRCollectorInstallaler32_2.0.0.330.msi` or `FortiEDRCollectorInstallaler64_2.0.0.330.msi`.
2. Double-click the `FortiEDRCollectorInstallaler32_x.x.x.xxx.msi` or `FortiEDRCollectorInstallaler64_x.x.x.xxx.msi` file and follow the displayed instructions.

Linux

You can only manually upgrade non-customized Linux Collectors. For custom Linux Collectors, you must first uninstall the current Collector and then install a new one, which requires reconfiguration.

To upgrade a non-customized Collector on Linux:

1. Check the status of the Collector using the following command:

```
/opt/FortiEDRCollector/control.sh --status
```

   The Collector should be stopped before running the upgrade command.

2. If the status is not stopped, stop the Collector using the following command:

```
 /opt/FortiEDRCollector/control.sh --stop <registration password>
```

   For example:

```
/ opt/FortiEDRCollector/control.sh --stop 12345678
```

3. Copy the installer file to the Collector machine (either `FortiEDRCollectorInstaller_Linux_distribution-version_number.x86_64.rpm` or `FortiEDRCollectorInstaller_Ubuntuversion_number.deb`).
4. Upgrade the Collector using the following command:
   - CentOS/RHEL/Oracle/AMI:

     ```
     sudo yum install FortiEDRCollectorInstaller_Linux_distribution-version_number.x86_64.rpm
     ```

   - Ubuntu:

     ```
     Ubuntu: Run sudo apt install FortiEDRCollectorInstaller_Ubuntu-version_number.deb
     ```

   - SLES:

     ```
     zypper install FortiEDRCollectorInstaller_distribution-version_number.rpm
     ```

5. Enter y when asked if you want to upgrade.
6. After the upgrade is complete, start the Collector using the following command:

   ```
   /opt/FortiEDRCollector/control.sh --start
   ```

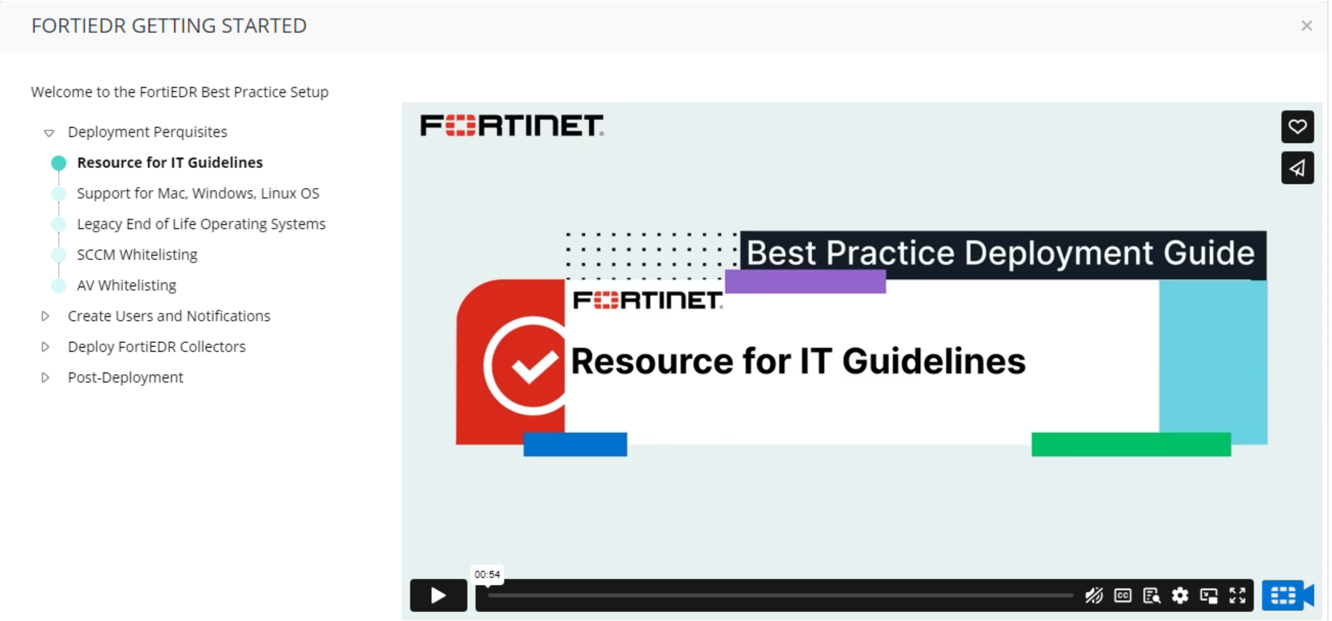
If your FortiEDR Threat Hunting Repository, Central Manager, Aggregator or Core are deployed on your organization’s premises (on-premises), see Upgrading FortiEDR components on page 524 for instructions of upgrading these components.

Dashboard

This chapter describes the FortiEDR DASHBOARD for monitoring security events.

Introduction

The FortiEDR Dashboard provides a visual overview of the FortiEDR protection of your organization. It provides an at-a-glance view of the current security events and system health. The first time you log in, the *FortiEDR Getting Started*window launches where you can watch a series of getting started videos for orientation within the FortiEDR environment. Use the videos to learn more about how to deploy and use FortiEDR.



FORTIEDR GETTING STARTED

Welcome to the FortiEDR Best Practice Setup

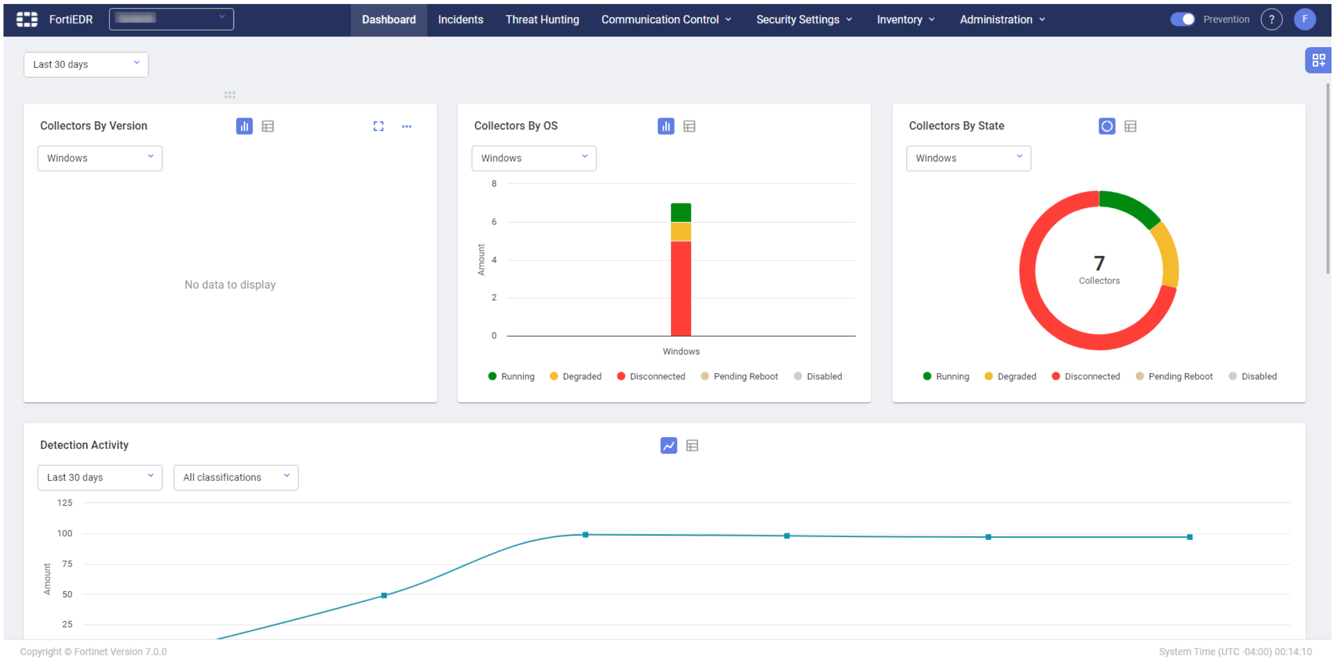
- Deployment Perquisites
  - **Resource for IT Guidelines**
  - Support for Mac, Windows, Linux OS
  - Legacy End of Life Operating Systems
  - SCCM Whitelisting
  - AV Whitelisting
- Create Users and Notifications
- Deploy FortiEDR Collectors
- Post-Deployment

You can change the window location over the screen, resize or minimize the window using the provided buttons at the bottom right. Progress of the current video is not kept after you switch to another one. You have to start over with the current video after switching back.

The following videos are currently available but the list is subject to change without notice:

Section	Videos
Deployment Perquisites	Resource for IT Guidelines
	Support for Mac, Windows, Linux OS
	Legacy End of Life Operating Systems
	SCCM Whitelisting
	AV Whitelisting
Create Users and Notifications	Central Manager: Create Secondary Admin
	Enable 2FA
	Create Email Distribution List
Deploy FortiEDR Collectors	Request FortiEDR Collector
	Create Server Collector Group
	Install Collector Win64
	Win Collector Command Line Install
	Linux Collector Command Line Install
	Win Collector Troubleshooting
Post-Deployment	BPS Lite Checklist
	Collector Troubleshooting

The Dashboard is automatically displayed after you exit the getting started window or when you click the *DASHBOARD* tab.



The system time is displayed in all pages at the bottom right of the status bar. It represents the local FortiEDR server time. For example, if the FortiEDR server is located in London, and you log in from Los Angeles, USA, then the time shown is the current time in London, and not the current time in Los Angeles.

System Time (UTC +03:00) 10:17:49

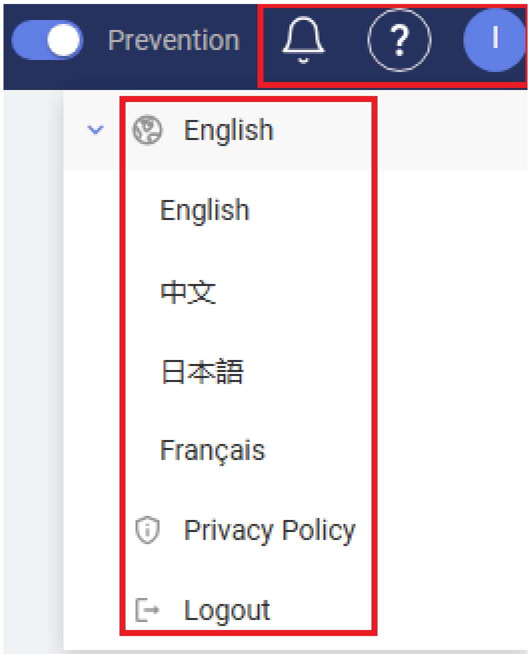
The Dashboard enables you to display two different slices or views of the data collected by FortiEDR in each widget. Click the applicable view button at the top left of the window to display that view in the *DASHBOARD* tab:

- *Graph View* (): This view presents information in a graph or pie chart.
- *Table View* (): This view presents information in a table.

The information presented in the Dashboard represents an aggregation of events. For more details, you may refer to the Event Aggregation on page 85. FortiEDR aggregates security events in both the Device view and the Process view in the Dashboard.

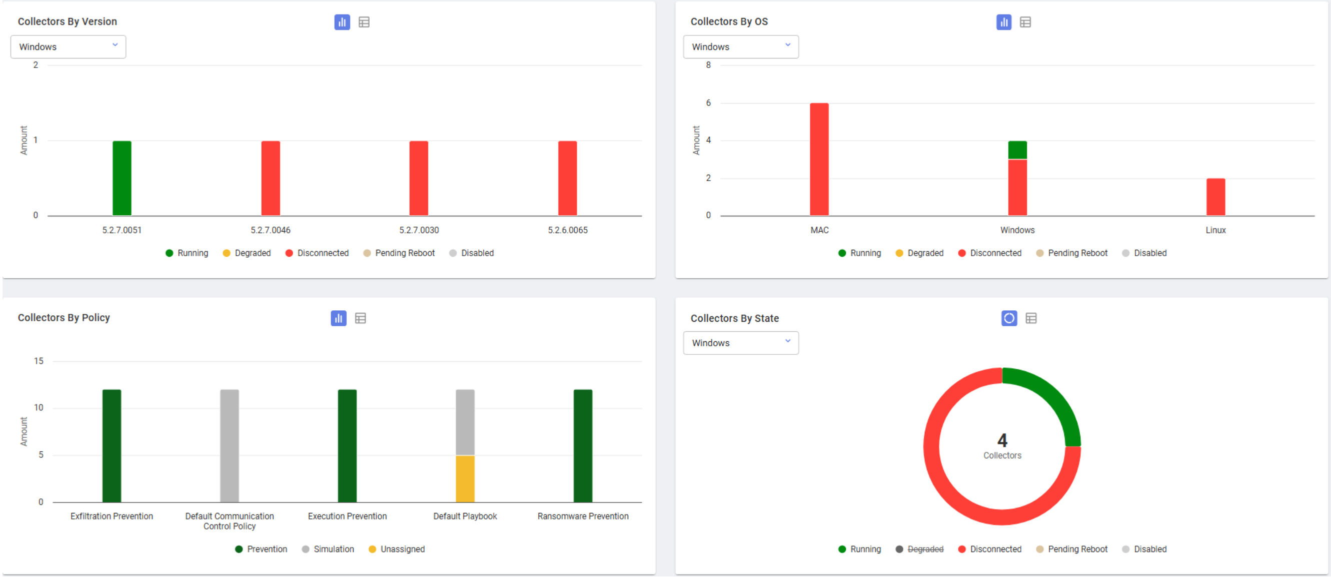
The top right corner includes the notification center where you can access notifications, the *Help* button to access the FortiEDR documentation portal where you can access all FortiEDR documents, such as the FortiEDR Administration Guide and Release Notes, and the *Logged-in User* dropdown list with the following options:

- *English*: Expand to switch the UI language from English to a supported language, such as Japanese. The default is English.
- *Privacy Policy*: Downloads the FortiEDR privacy policy.
- *Logout*: Exits the FortiEDR application.



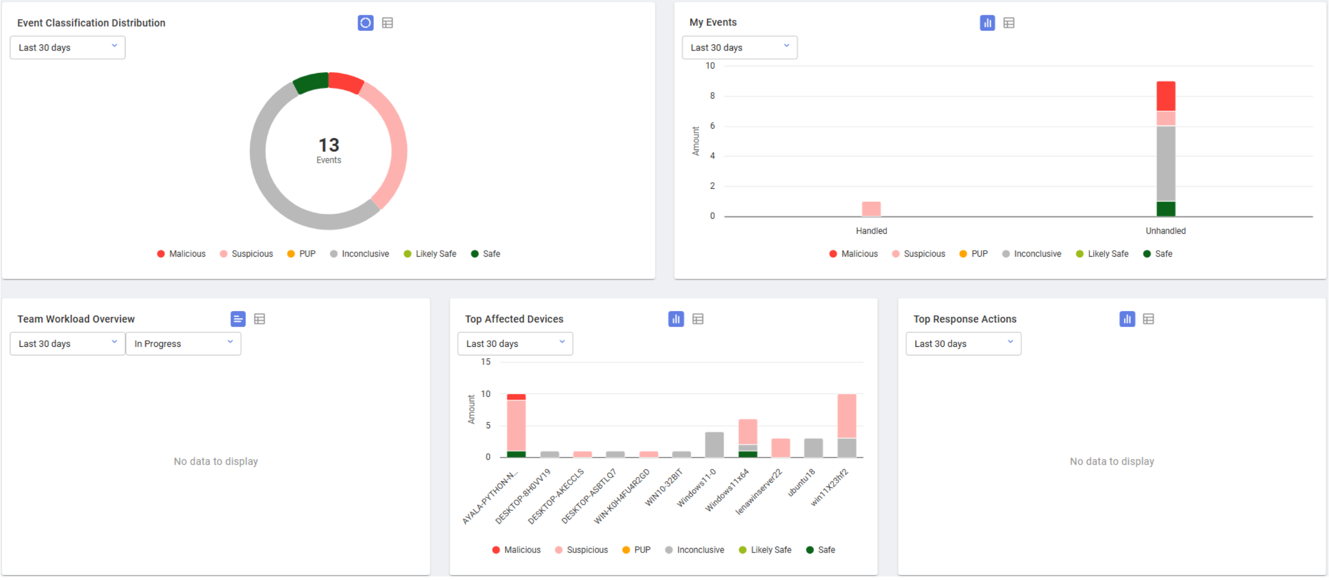
Collectors chart

The *COLLECTORS* chart provides an overview of FortiEDR Collectors. You can view Collectors by OS, policy, state, or version.



Disconnected status may indicate that the device on which the FortiEDR Collector is installed is simply powered down or disconnected from the network. It does not necessarily mean that there is a problem with that FortiEDR Collector or that device.

Event Handling widgets

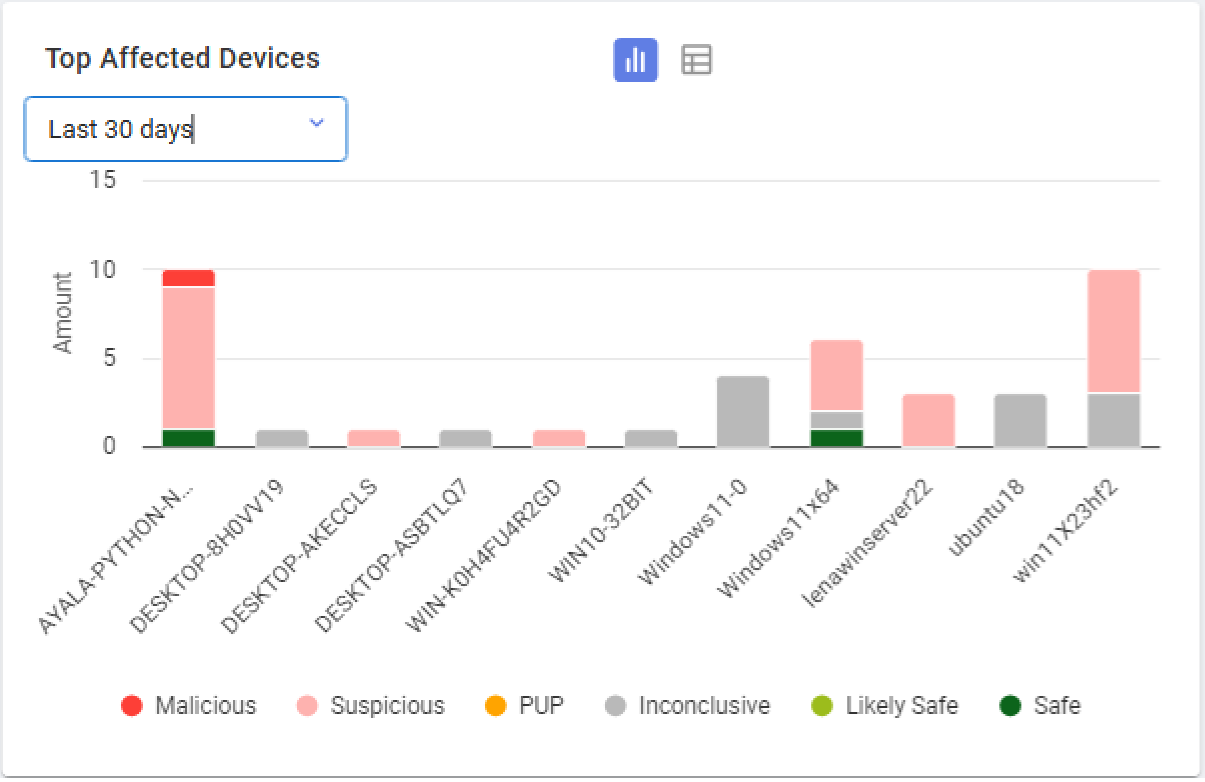


The *Event Handling* widgets show the number and classification of the FortiEDR security events. The charts and graphs are color-coded according to security event classification:

- **Red**: Critical
- **Yellow**: High
- **Grey**: Medium
- **Green**: Safe

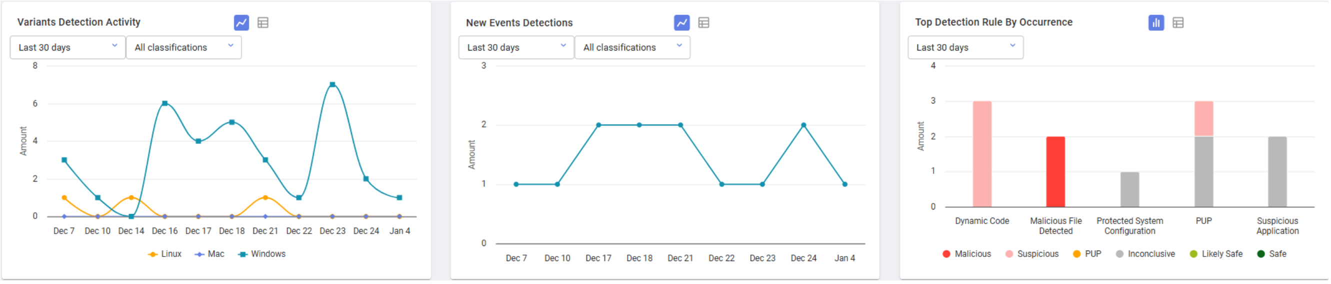
Each security event that is detected by the FortiEDR system is initially marked as unread and unhandled. Multiple users may be using the FortiEDR Central Manager in parallel. The *Unread* and *Unhandled* statuses enable users to keep track of whether anyone has read and handled the message.

Top Affected Devices chart



The *Top Affected Devices* chart displays the history of the most-infected and targeted processes, applications and devices. This chart is color-coded according to the classification of the attacks. The information is displayed per last day, last week or last month, according to your selection.

Detection trends and analysis widgets



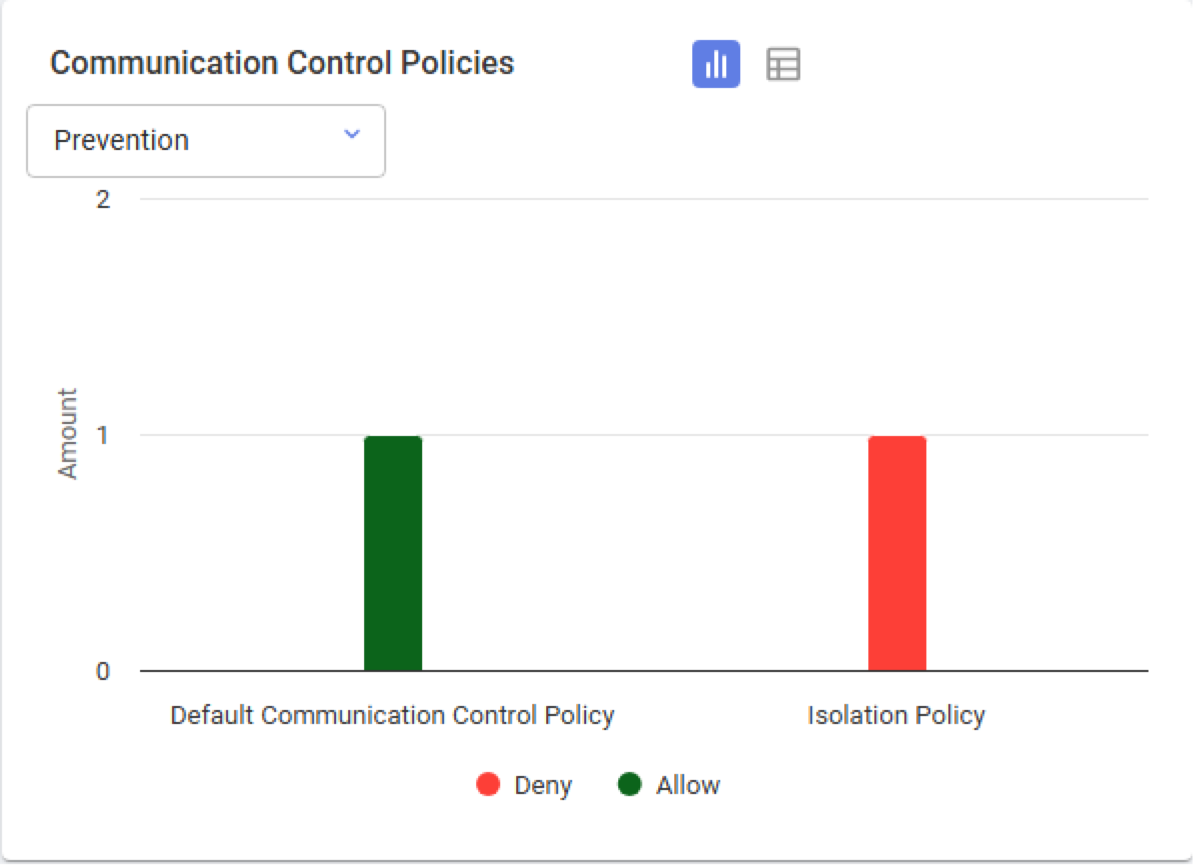
The *Detection trends and analysis* widgets show the trends and analysis of the FortiEDR security events.

The graphs in the *Top Detection Rule By Occurrence* widget are color-coded according to security event classification:

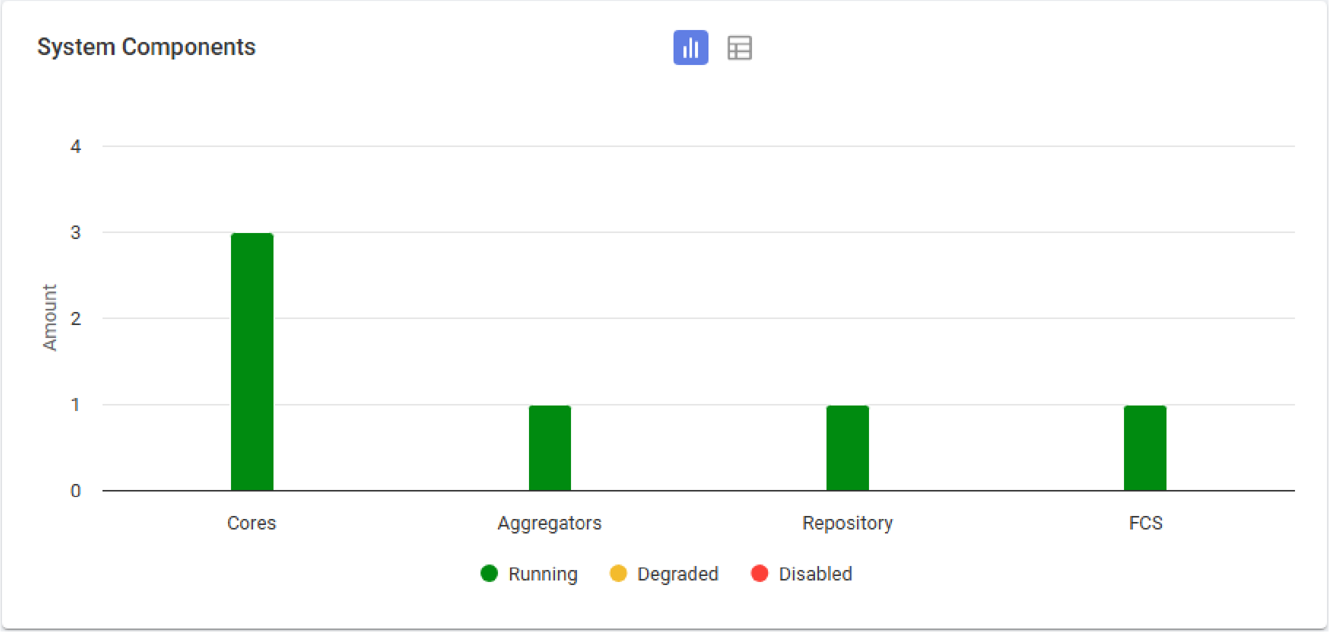
- **Red**: Critical
- **Yellow**: High
- **Grey**: Medium
- **Green**: Safe

Communication Control Policies graph

The *Communication Control Policies* graph displays a breakdown of the applications that are allowed or denied in your organization.

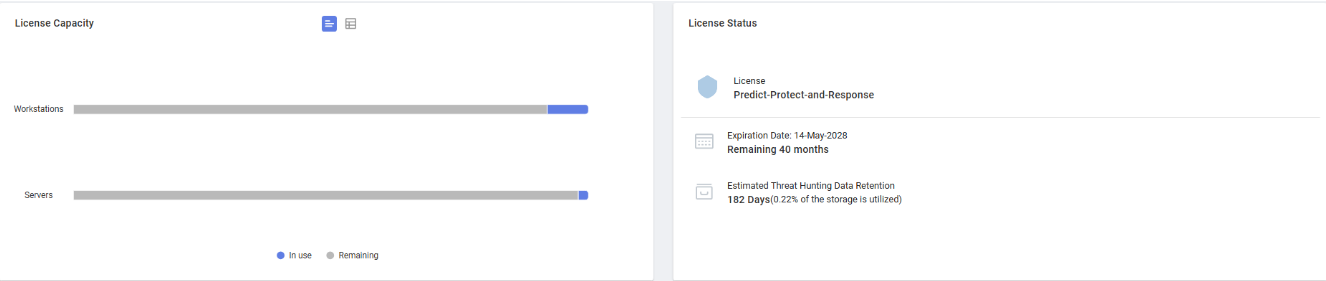

Communication Control Policies
Prevention
Amount
2
1
0
Default Communication Control Policy
Isolation Policy
● Deny
● Allow

System Components



The *System Components* graph shows the status of the Cores, Aggregators, Threat Hunting Repository, and FCS.

Licensing widgets



License Status

License
Predict-Protect-and-Response

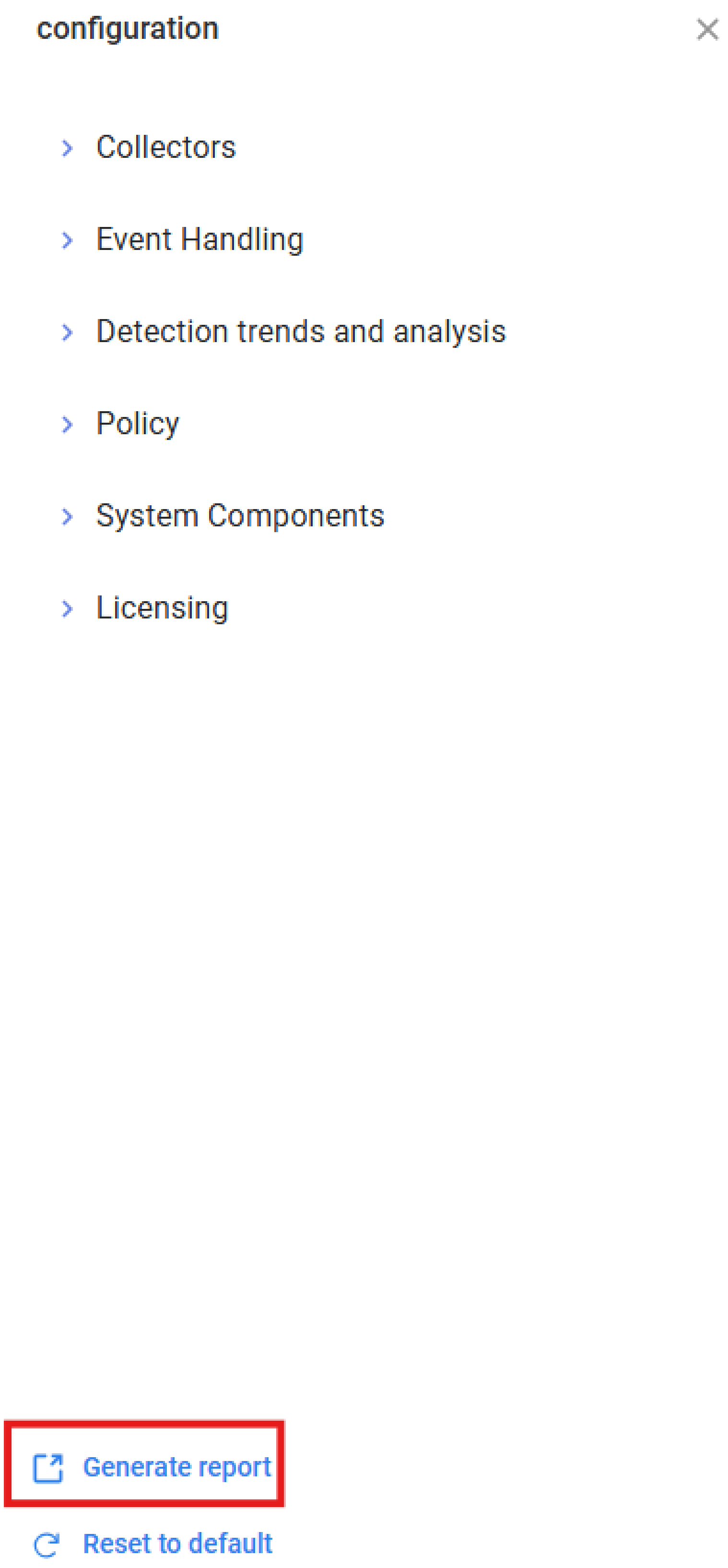
Expiration Date: 14-May-2028
Remaining 40 months

Estimated Threat Hunting Data Retention
182 Days(0.22% of the storage is utilized)

The *Licensing* widgets provide an overview of the FortiEDR license status, including licensing type and status, capacity and usage information, and threat hunting data retention usage.

Generating reports

On the dashboard, click the *Configuration* icon (⊞) on the top-right of the dashboard and click *Generate report* to download a PDF report with a summary of the security events and system health within the specified time range.


configuration
×
› Collectors
› Event Handling
› Detection trends and analysis
› Policy
› System Components
› Licensing
Generate report
Reset to default

Incidents

This chapter describes the FortiEDR Incidents view for monitoring and handling security events.

Introducing the Incidents view

Upon connection establishment attempt, each FortiEDR Collector sends relevant metadata to the FortiEDR Core, which sends it on to the FortiEDR Aggregator so that it can be displayed in the FortiEDR Central Manager Incidents view. The *Incidents* tab enables you to view, investigate, and acknowledge handling of each such security event. A row is displayed for each event.

The *Incidents* tab enables you to display two different views of the event data collected by FortiEDR:

- *All Incidents* (): This view shows all the security events detected on all devices within the specified time range (up to 30 days).
- *Mobile Incidents* (): This view shows security events detected on mobile devices within the specified time range (up to 30 days).

Security events that were triggered by Saved Queries appear slightly different in the *Incidents* tab.

Event Aggregation

For convenience and easier navigation, FortiEDR aggregates security events in the *Incidents* tab.

- Each primary-level row represents an incident entity with its own state independent from the associated child events.

  You can filter incidents with a time rang of up to 30 days. Filters are applied to both the top-level incidents and their child events. An incident may appear on its own if it matches the filter criteria even if none of its child events do.

- You can drill down on a device/process to display the security events for that device/process. Each security event row is marked with a flag ⚑ indicator.

  In the Process view, the Destinations column indicates the number of destinations to which the process attempted to connect. If only one destination was accessed, its IP address is shown. If more than one destination was accessed, the number of destination IPs is shown in the Destinations column.

  In the Process view, the Device column indicates the number of devices the malware attempted to attack. If only one device was attacked, its device name is shown. If more than one device was

attacked, the number of devices is shown in the Device column.
- You can drill down further in a security event row to view the raw data items for that event by clicking on the ▷ icon. Raw data items display the relevant information collected by FortiEDR from the device. For example, if a specific process was connecting to 500 destinations, then 500 raw data item rows display for that security event. For example, in the figure below, the security event comprises 2 raw data items, coming from different devices and going to different destinations. You can click the < Back icon to return to the aggregated security event view.

The following actions can be performed in the Incidents view:

- Marking a security event as handled/unhandled on page 115
- Manually changing the classification of a security event on page 116
- Viewing Application Control security events on page 123
- Viewing Device Control security events on page 123
- Other options in the Incidents viewer on page 124

When a new security event is generated by FortiEDR, an indicator number displays or is incremented.

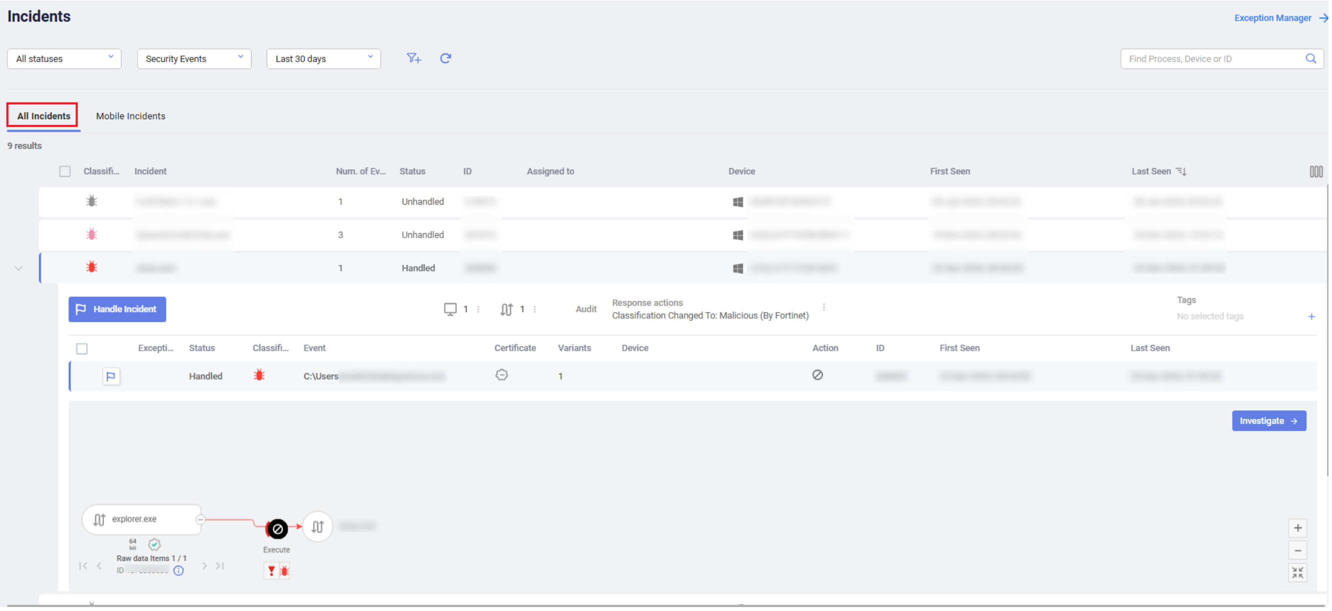
Hovering over this number indicates the number of new unread security events.

In some cases, *Updated* displays next to the number of new unread security events indicator. Updated means that FortiEDR originally classified one of the unread events, but that classification was later changed by the user. After more data for this security event was received, FortiEDR overrode the manual classification of the event by the user and changed the classification for the event again, based on the newly received data.

Incidents pane

Clicking a security event expands it to show more details and enables the buttons at the top of the window. The following information is provided for each security event:

Desktop incidents:



9 results

Classifi...	Incident	Num. of Ev...	Status	ID	Assigned to	Device	First Seen	Last Seen
	[illegible]	1	Unhandled	[illegible]		[illegible]	[illegible]	[illegible]
	[illegible]	3	Unhandled	[illegible]		[illegible]	[illegible]	[illegible]
	[illegible]	1	Handled	[illegible]		[illegible]	[illegible]	[illegible]

1 | 1 | Audit | Response actions
Classification Changed To: Malicious (By Fortinet)

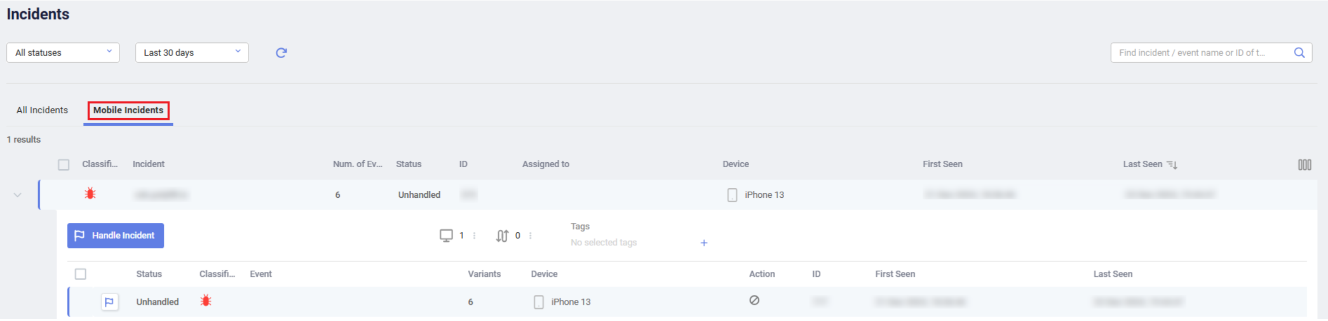
Tags
No selected tags

Excepti...	Status	Classifi...	Event	Certificate	Variants	Device	Action	ID	First Seen	Last Seen
	Handled		C:\Users[illegible]		1		⊘	[illegible]	[illegible]	[illegible]

The Extended Detection policy provides detection features (meaning that events are logged and displayed in the *Incidents* tab). No protection (blocking) features are provided. The exceptions options are not available in the *Incidents* tab for security events triggered by the Extended Detection policy, because these events were not collected by a FortiEDR Collector.

Mobile incidents:

The *Mobile incidents* tab is available only if mobile is enabled in the organization setting. See Step 2 – Defining or importing an organization on page 419.



1 results

Classifi...	Incident	Num. of Ev...	Status	ID	Assigned to	Device	First Seen	Last Seen
	[illegible]	6	Unhandled	[illegible]		iPhone 13	[illegible]	[illegible]

1 | 0 | Tags
No selected tags

Status	Classifi...	Event	Variants	Device	Action	ID	First Seen	Last Seen
Unhandled			6	iPhone 13	⊘	[illegible]	[illegible]	[illegible]

The mobile incidents view displays incidents specific to mobile devices. The details for each mobile incident are similar to those in the desktop incidents view except that the *Investigate* button is unavailable for mobile incidents.

Information Field	Description
View Indicator	Indicates the view context for the security event aggregation. 🖵 displays for a device and ⇅ displays for a process.

<table>
<tr><th>Information Field</th><th>Description</th></tr>
<tr><td>Handled/Not Handled ⚑</td><td>Specifies whether any FortiEDR Central Manager user handled this security event, as described on Marking a security event as handled/unhandled on page 115</td></tr>
<tr><td>ID</td><td>Specifies an automatically assigned unique identifier for each security event generated by FortiEDR. This identifier is particularly useful for security event tracking purposes when monitoring security events using an external system, such as a SIEM.</td></tr>
<tr><td>Device</td><td>Specifies the device name on which the security event has occurred.</td></tr>
<tr><td>Process</td><td>Specifies the process that is infected. This is not necessarily the process that made the connection establishment request (such as Firefox, which might be being controlled by the infected application). If the security event was triggered by a script, then the script name is specified.</td></tr>
<tr><td>Classification</td><td>Specifies how malicious the security event is, if at all. Classifications are initially determined by the Core but can be changed either automatically as the result of additional post-processing, deep, thorough analysis and investigation by the FortiEDR Cloud Service (FCS) or manually. See Overview on page 90 for more detailed information about the classification of the event, such as the classification history. Classifications are as follows:
<table>
<tr><th>Icon</th><th>Classification</th><th>Definition</th><th>Recommended Action</th></tr>
<tr><td>🐞</td><td>Malicious</td><td>Events with the following characteristics:
• Verified to have malicious capability
• Intended to harm the infected device
• Have no commercially viable use</td><td>Remediate</td></tr>
<tr><td>🐞</td><td>Suspicious</td><td>Events that behave in ways that strongly indicate malware, but are not verified malware.</td><td>Review and remediate</td></tr>
<tr><td>🐞</td><td>Inconclusive</td><td>Further investigation needed to determine</td><td>Administrator review</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Information Field</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Icon</th><th>Classification</th><th>Definition</th><th>Recommended Action</th></tr>
<tr><td></td><td></td><td>if the event is malicious.</td><td></td></tr>
<tr><td>🐞</td><td>PUP (Potentially Unwanted Program)</td><td>Events triggered by programs that are bundled with legitimate software or commercial software that may be used for malicious purposes, for example, torrents.</td><td>Administrator to review whether the program should be removed (recommended) or allowed</td></tr>
<tr><td>✅</td><td>Likely Safe</td><td>Events that probably carry no risk, and are most likely legitimate.</td><td>Administrator review</td></tr>
<tr><td>≡✓</td><td>Safe (Confirmed Safe Software)</td><td>Events triggered by legitimate software that was intended for use by the customer, for example, security software.</td><td>No action necessary</td></tr>
</table>
</td></tr>
<tr><td>Received</td><td>Specifies the first time that this security event was triggered. For aggregations, the earliest received time is displayed.</td></tr>
<tr><td>Last Updated</td><td>Specifies the last time that the security event was triggered. For aggregations, the most-recent time is displayed.</td></tr>
<tr><td>Action</td><td>Specifies the action that was enforced:
• <b>Block</b> ⊘: The exfiltration attempt was blocked and this blocking event was generated.
• <b>Simulated Block</b> ⊘: The policy that protected this device was set to <i>Simulation</i> mode. Therefore, the exfiltration attempt was <b>NOT</b> blocked and this blocking event was generated. FortiEDR would have blocked this exfiltration security event if the policy had been set to <i>Prevention</i> mode.
• <b>Log</b> 🗋: The security event was only logged and was not blocked.</td></tr>
</table>

For raw data items, the following information is available:

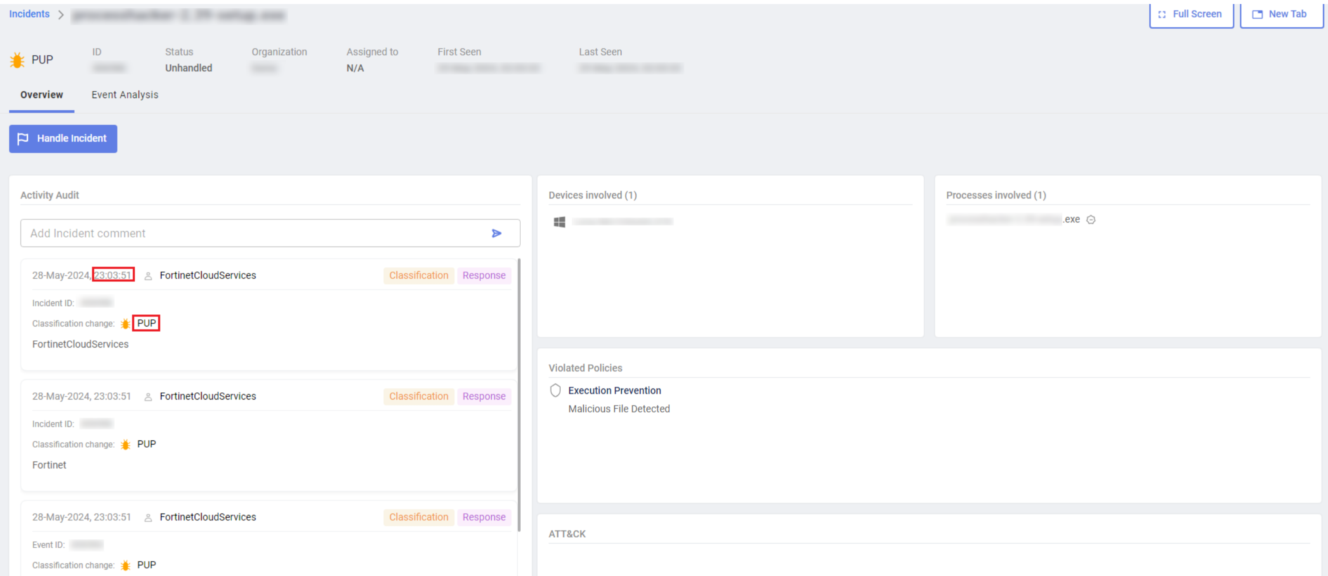
Information	Description
Device	Specifies the device name on which the security event has occurred.

Information	Description
First Seen	The *Incidents* tab aggregates the occurrences of the same security events into a single row when it represents the same attack on the same device. This timestamp specifies the first time this security event occurred. The row of this security event pops to the top of the list in the *Incidents* tab each time it occurs again. If a change is made to the FortiEDR policy used by a specific FortiEDR Collector, then the security events before and after that change are not aggregated together.
Last Seen	Specifies the most recent time this same security event occurred. See FIRST SEEN described above.
Process Owner	Specifies the user who ran the process that triggered the security event.
Process Type	Specifies whether the infected process is 32-bit or 64-bit.
Use	Specifies the domain of the computer/user of the device.
Process Path	Specifies the path of the infected process.
Count	Specifies the number of occurrences of the same raw event on the same device.

Overview

After you select an incident in the Incidents pane on page 86 and click *Investigate*, the *Overview* pane displays detailed information about the audit history, violated policies, and rules assigned to the FortiEDR Collector that triggered this security event.

The audit history shows the chronology for classifying the security event, and the actions performed by FortiEDR for that event. This area also displays relevant details when the FortiEDR Cloud Service (FCS) reclassifies a security event after its initial classification by the Core. For example, the following example shows that the security event was reclassified by the FCS and given a notification status of *PUP* at 23:03:51.



PUP

ID: [redacted]

Status: Unhandled

Organization: [redacted]

Assigned to: N/A

First Seen: [redacted]

Last Seen: [redacted]

Activity Audit

28-May-2024, 23:03:51 FortinetCloudServices

Incident ID: [redacted]

Classification change: PUP

FortinetCloudServices

28-May-2024, 23:03:51 FortinetCloudServices

Incident ID: [redacted]

Classification change: PUP

Fortinet

28-May-2024, 23:03:51 FortinetCloudServices

Event ID: [redacted]

Classification change: PUP

Devices involved (1)

[redacted]

Processes involved (1)

[redacted].exe

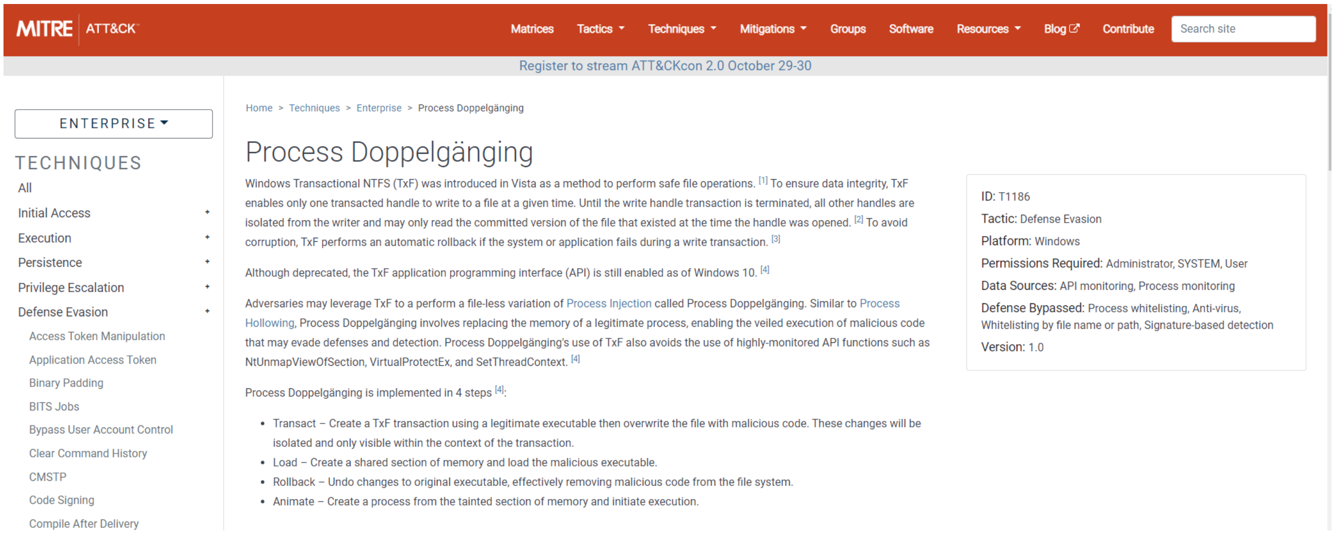
Violated Policies

Execution Prevention

Malicious File Detected

ATT&CK

The ATT&CK section lists techniques that were used in this incident based on the MITRE ATT&CK common techniques scheme. Clicking the technique opens the MITRE web page, providing additional details, as shown below.



Process Doppelgänging

Windows Transactional NTFS (TxF) was introduced in Vista as a method to perform safe file operations. [1] To ensure data integrity, TxF enables only one transacted handle to write to a file at a given time. Until the write handle transaction is terminated, all other handles are isolated from the writer and may only read the committed version of the file that existed at the time the handle was opened. [2] To avoid corruption, TxF performs an automatic rollback if the system or application fails during a write transaction. [3]

Although deprecated, the TxF application programming interface (API) is still enabled as of Windows 10. [4]

Adversaries may leverage TxF to a perform a file-less variation of Process Injection called Process Doppelgänging. Similar to Process Hollowing, Process Doppelgänging involves replacing the memory of a legitimate process, enabling the veiled execution of malicious code that may evade defenses and detection. Process Doppelgänging's use of TxF also avoids the use of highly-monitored API functions such as NtUnmapViewOfSection, VirtualProtectEx, and SetThreadContext. [4]

Process Doppelgänging is implemented in 4 steps [4]:

- Transact – Create a TxF transaction using a legitimate executable then overwrite the file with malicious code. These changes will be isolated and only visible within the context of the transaction.
- Load – Create a shared section of memory and load the malicious executable.
- Rollback – Undo changes to original executable, effectively removing malicious code from the file system.
- Animate – Create a process from the tainted section of memory and initiate execution.

ID: T1186

Tactic: Defense Evasion

Platform: Windows

Permissions Required: Administrator, SYSTEM, User

Data Sources: API monitoring, Process monitoring

Defense Bypassed: Process whitelisting, Anti-virus, Whitelisting by file name or path, Signature-based detection

Version: 1.0

In the *Violated Policies* pane, only policies that were violated are displayed. The rule's configured action is displayed for each rule, as defined in *POLICIES*. The Action that was actually executed is displayed in the action column of the *Incidents* pane of this window. The action taken is determined by the rule with the highest priority.

Investigation View

The *Investigation View* is accessible in the Event Analysis tab using the *Investigation* button (

) when you select an incident in the *Incidents* tab. It helps understand the flow of activity events during Threat Hunting with a dynamic and interactive graphical view of the activity events details: source, action and target.

The graphical view provides the ability to add more activity events to the graph and show the relationship and timeline of the occurrence of those activities, such as the following:

- All actions performed by a given process
- All files the process has created or updated
- All IPs the process has initiated communication with

It also allows you to interactively view a chain of activity events in the following ways:

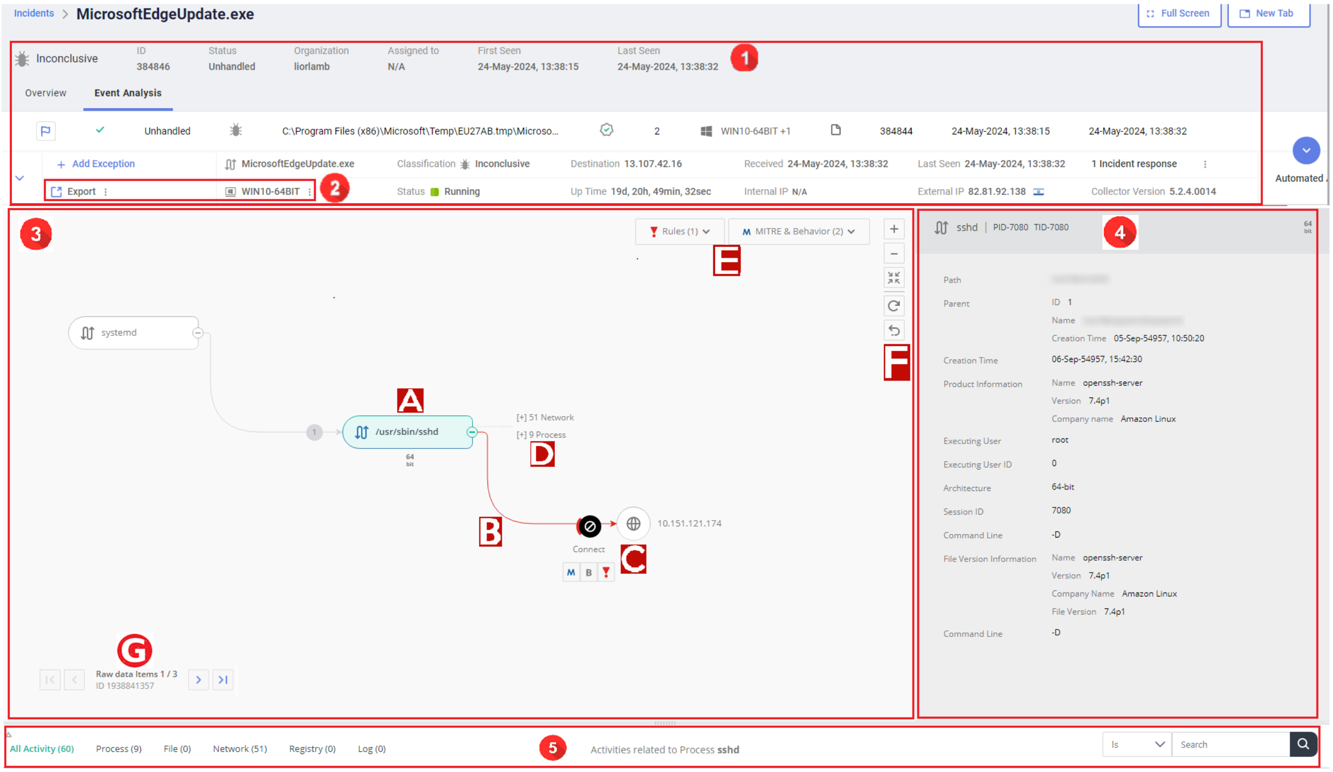
- Browse between the various processes involved in the chain
- See all activity events related to one node in the Security Event graph
- Filter activity events table to include or exclude a specific value
- Switch and see the graph chain on the other involved endpoints while analyzing security event on one device

You can also perform certain actions, such as:

- Retrieve or remediate files
- Connect to a device or isolate a device
- Move a device to high security group
- See the graph chain on the other involved endpoints while analyzing security event on one device

- The *Investigation View* is not available to IT users (see Users on page 277). *Read-Only* user can only view and manipulate graphs but cannot remediate or perform other actions.
- The view adds visualization and interaction of existing data that is already available in other non-graphical and non-interactive forms without creating or generating any additional data.

The following figure illustrates the various components of an *Investigation View* window launched from the *Incidents* view.



Incidents > MicrosoftEdgeUpdate.exe

Inconclusive | ID 384846 | Status Unhandled | Organization liorlamb | Assigned to N/A | First Seen 24-May-2024, 13:38:15 | Last Seen 24-May-2024, 13:38:32

Unhandled | C:\Program Files (x86)\Microsoft\Temp\EU27AB.tmp\Microso... | 2 | WIN10-64BIT +1 | 384844 | 24-May-2024, 13:38:15 | 24-May-2024, 13:38:32

MicrosoftEdgeUpdate.exe | Classification Inconclusive | Destination 13.107.42.16 | Received 24-May-2024, 13:38:32 | Last Seen 24-May-2024, 13:38:32 | 1 Incident response

WIN10-64BIT | Status Running | Up Time 19d, 20h, 49min, 32sec | Internal IP N/A | External IP 82.81.92.138 | Collector Version 5.2.4.0014

sshd | PID-7080 TID-7080

Path
Parent: ID 1; Name; Creation Time 05-Sep-54957, 10:50:20
Creation Time: 06-Sep-54957, 15:42:30
Product Information: Name openssh-server; Version 7.4p1; Company name Amazon Linux
Executing User: root
Executing User ID: 0
Architecture: 64-bit
Session ID: 7080
Command Line: -D
File Version Information: Name openssh-server; Version 7.4p1; Company Name Amazon Linux; File Version 7.4p1
Command Line: -D

Raw data Items 1 / 3
ID 1938841357

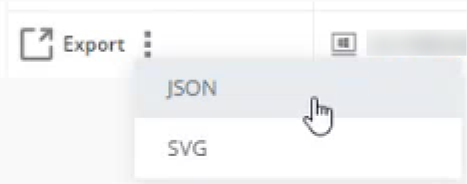
All Activity (60) | Process (9) | File (0) | Network (51) | Registry (0) | Log (0)

Activities related to Process **sshd**

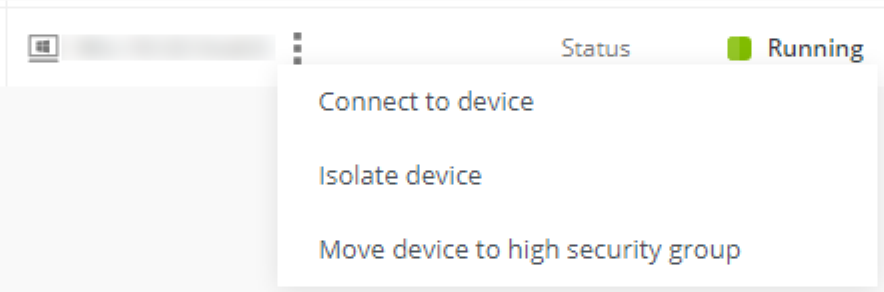
Is | Search

Compared with the investigation view window launched from the *Details Pane* under *Threat Hunting*, this view includes the following additional functionality:

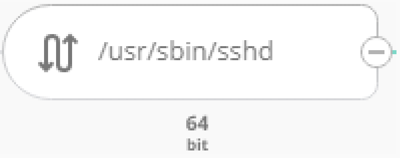
- Advanced threat hunting and investigation capabilities, such as exporting the graph as JSON, raw data items navigation graph, and Stacks view on page 99.
- General event details in the first row, such as classification and incident response.

Component	Description
1	General details about the event, such as event ID, process name, classification, IP address, and incident responses.
2	• Use the *Export* button (Export) to save files for sharing or record reasons: • *JSON*—Export the event data as a JSON file. • *SVG*—Export the investigation view graph as an SVG file. This is the only option to save a graph that includes dynamic changes based on the default graph view, such as adding processes.  • Use the following buttons, accessible by clicking the eclipses on the right of the

<table>
<tr><th>Component</th><th colspan="2">Description</th></tr>
<tr><td></td><td colspan="2">device name, to connect to a device, isolate a device, or move the device to high security group.

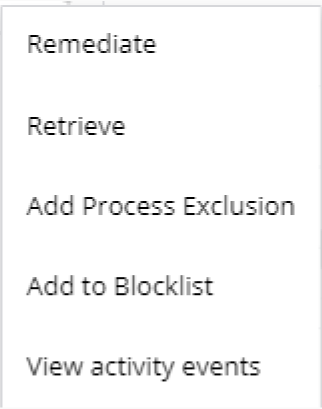
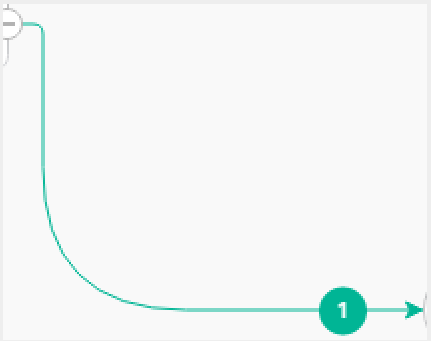
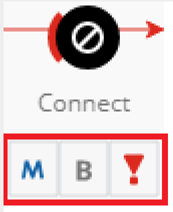


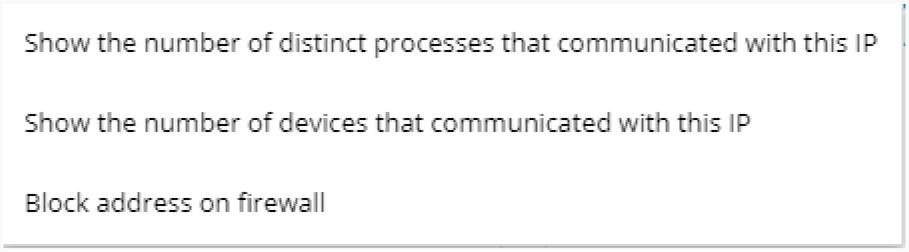
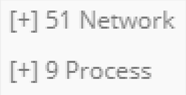
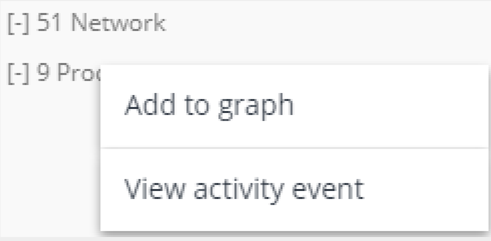
</td></tr>
<tr><td>3</td><td colspan="2">Graphical flow diagram with a process tree that you can build according to your investigation needs, from left to right and top to bottom. The tree is also interactive, which means you can click on a specific component to drill down for more details or contextual actions.</td></tr>
<tr><td></td><td>A</td><td><b>Node</b>—Source of an activity or event, which can be a process, an endpoint, a thread or service, or another security product. Nodes are represented by boxes with icons for the activity type, some with descriptions under the boxes.

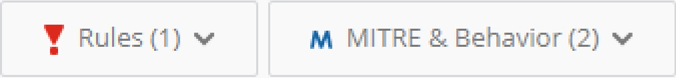
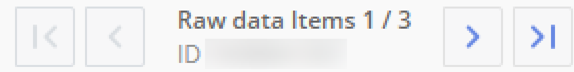


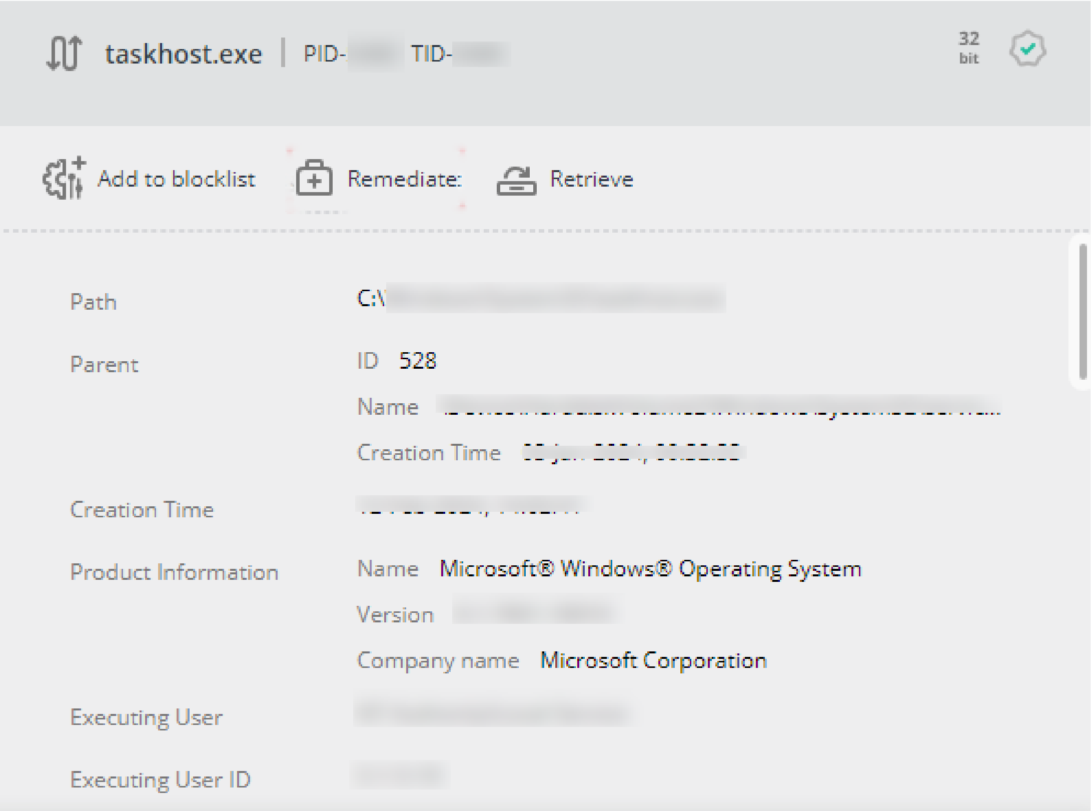
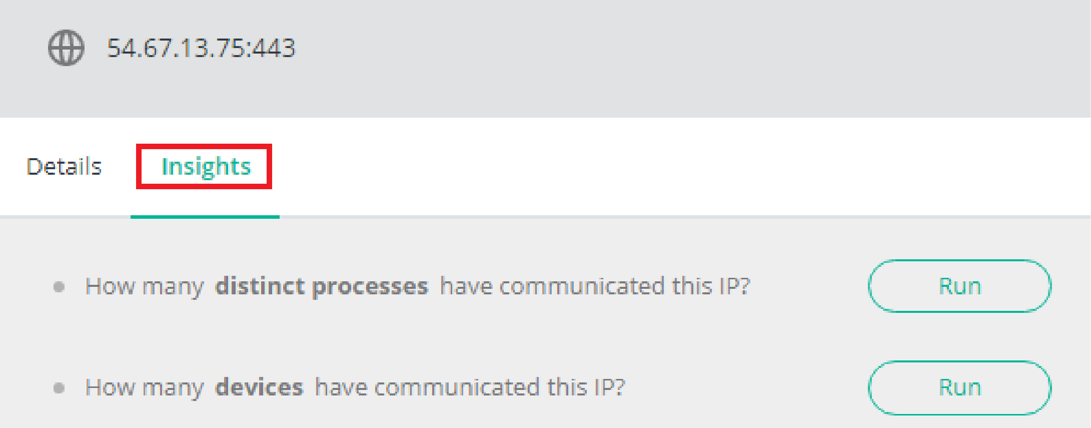
- Click on a node to display the Details pane on page 145 on the right and the Activity events tables on page 141 on the bottom with contextual information about that specific node.
- Click the *Collapse* (⊖) or *Expand* (⊕) icon in the right of a node icon to show or hide all the downstream nodes, edges, and leaves.
- Right-click a node to perform actions allowed on the node, including any custom actions you defined. These action buttons also appear in the *Details Pane*, which is available on the right after you click the node.

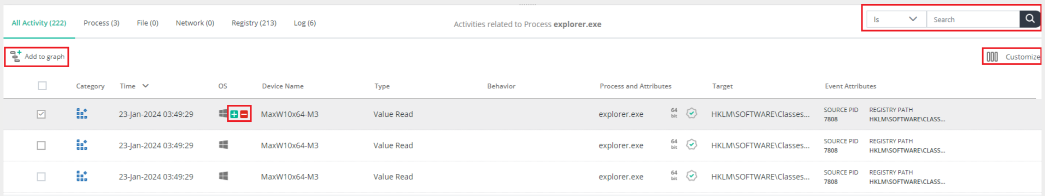
  The list of available options varies by node type. The following is an example list of actions for a process node.</td></tr>
</table>

Component	Description	
	 Remediate Retrieve Add Process Exclusion Add to Blocklist View activity events	
	B	**Edge**—Activity event type or action represented by a curved line with an arrow. An edge can be one activity event/action or an aggregation of several. The numbered arrows indicate the sequence of actions and specify the action that was performed, such as *Process Creation*, *Socket Close*, *Block* and so on. Multiple operations performed between two processes are represented by multiple arrows between them. Edges that triggered the event are indicated in red.  Click on an edge to display the Details pane on page 145 on the right and the Stacks view on page 99 on the bottom with contextual information about that specific edge. Edges may also have icons below them indicating classification or violation of certain rules and MITRE & Behavior models. Click on an icon for more detailed information. 

Component	Description	
	C	**Leaf**—Target of activity event of type File, Registry Key, Registry Value, Network components (IP/DNS/URL). A leaf can also be a group of artifacts. For example, all the files created or modified by a process. Leaves have a round shape (🌐). • Click on a leaf to display the Details pane on page 145 on the right and the Activity events tables on page 141 on the bottom with contextual information about that specific leaf. • Right-click a leaf to perform actions allowed on the leaf, including any custom actions you defined. These action buttons are also available in the *Details Pane*, which appear on the right after you click the leaf. The list of available options varies by leaf type. The following is an example list of actions for a network leaf:  Show the number of distinct processes that communicated with this IP Show the number of devices that communicated with this IP Block address on firewall
	D	**Hint**—Categorized groups of activities related to a node that are not part of the main chain of activity events and thus not represented in the graphical diagram. Click a node to show the number of relevant activities. The hints no longer display after you move the selection to another node or edge.  [+] 51 Network [+] 9 Process • Click the *Expand* ([+]) or *Collapse* ([-]) icon near a leaf hint to show or hide the node or leaf list of that type. • Right-click the type name of a hint and select *Add to graph* to add the relevant leaves to the graph or select *View activity event* to pull out the Activity events tables on page 141 for this specific file type. The *Add to graph* option is unavailable when the number of hints exceeds 500, in which case you can only choose to view the activity event.  [-] 51 Network [-] 9 Proc Add to graph View activity event

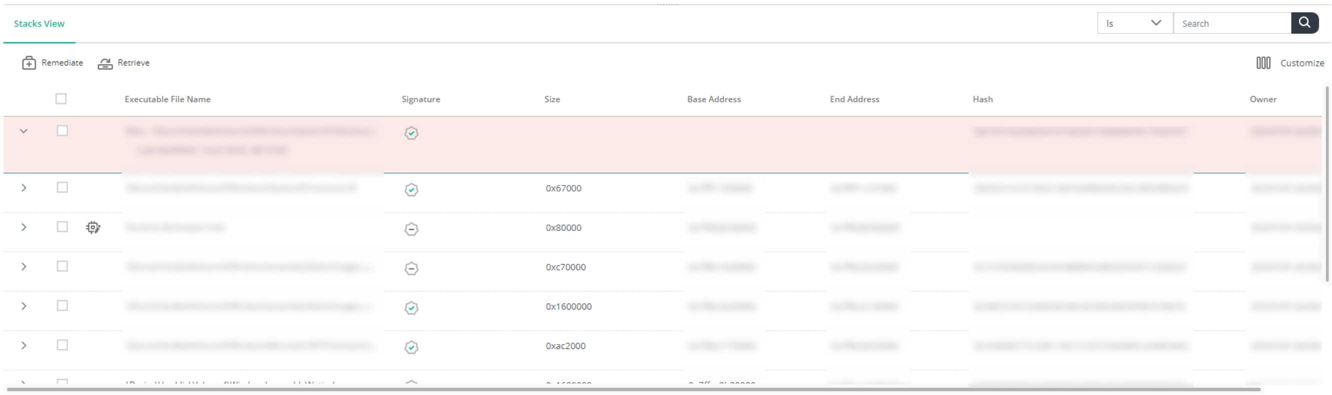
Component	Description	
	E	Use the *Rules* or *MITRE & Behavior* legends to highlight the corresponding icons below relevant edges in the diagram. 
	F	- Use the *Zoom In* (+), *Zoom Out* (−), and *Zoom To Fit* (⤡) buttons to adjust the graph window size. - Use the *Reset* (↻) button to restore the graph to the default view. - Use the *Undo* (↶) button to cancel an operation.
	G	Navigate between the graphs of the various raw data items for a security event using the right and left arrows. 
4	Details pane on page 145 for the selected node, edge, or leaf where you can view details of the activity, action, or target, and perform common actions on a node or leaf, such as retrieving a file, remediating devices upon malware detection, or adding an application to the Application Control policy blocklist. The actions can also be performed by right-clicking a node or leaf and selecting the option from the menu.	

Component	Description
	 taskhost.exe | PID-[redacted] TID-[redacted] 32 bit Add to blocklist Remediate Retrieve Path C:\[redacted] Parent ID 528 Name [redacted] Creation Time [redacted] Creation Time [redacted] Product Information Name Microsoft® Windows® Operating System Version [redacted] Company name Microsoft Corporation Executing User [redacted] Executing User ID [redacted] For specific leaf types, this pane also includes an *Insights* tab which allows you to run queries to retrieve analytics data, such as the number of communicating processes or devices of a certain IP. The *Insights* options are also available from the right-click menu of those leaf types.  54.67.13.75:443 Details Insights How many **distinct processes** have communicated this IP? Run How many **devices** have communicated this IP? Run
5	• When a node or leaf is selected, the contextual Activity events tables on page 141 appears at the bottom, which is organized by tabs of activity types. Drag the top edge of the table up for a fuller view of the table. Activities with a number at the front of the row are already in the graph and the number matches the one in the graph.

Component	Description
	 All Activity (222) · Process (3) · File (0) · Network (0) · Registry (213) · Log (6) · Activities related to Process **explorer.exe** · Is · Search Add to graph · Customize ☐ · Category · Time · OS · Device Name · Type · Behavior · Process and Attributes · Target · Event Attributes ☑ · 23-Jan-2024 03:49:29 · MaxW10x64-M3 · Value Read · explorer.exe 64 bit · HKLM\SOFTWARE\Classes... · SOURCE PID 7808 · REGISTRY PATH HKLM\SOFTWARE\CLASS... ☐ · 23-Jan-2024 03:49:29 · MaxW10x64-M3 · Value Read · explorer.exe 64 bit · HKLM\SOFTWARE\Classes... · SOURCE PID 7808 · REGISTRY PATH HKLM\SOFTWARE\CLASS... ☐ · 23-Jan-2024 03:49:29 · MaxW10x64-M3 · Value Read · explorer.exe 64 bit · HKLM\SOFTWARE\Classes... · SOURCE PID 7808 · REGISTRY PATH HKLM\SOFTWARE\CLASS... - To add activities to the graph, select the corresponding rows and click *Add to graph* (Add to graph). - To customize the columns to display in the table, click *Customize* (Customize). - To search for a specific activity or event, enter keywords in the search bar on the top right corner (Is Search). - To filter the results in the Activity Events table to include or exclude a specific value, use the green plus (+) and red minus (−) icons that appear when you hover over the value. Multiple filters are supported. To delete a filter, click the cancel icon that appear when you hover over the filter on the top-left of the table. - When an edge is selected, the Stacks view on page 99 appears at the bottom instead.

Stacks view

The stacks view displays the stacks that were collected during the action performed between two process nodes in the Investigation View on page 92 when an edge is selected. The stack entries include the executables and DLLs involved in the process stack. The stack entries due to which the event was triggered are highlighted with a red background. The main stack entry, which means the first one, is marked with a separator.



Stacks View · Is · Search

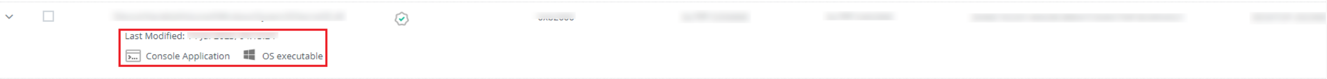
Remediate · Retrieve · Customize

☐	Executable File Name	Signature	Size	Base Address	End Address	Hash	Owner
☐	[redacted]	✓				[redacted]	[redacted]
☐	[redacted]	✓	0x67000	[redacted]	[redacted]	[redacted]	[redacted]
☐	[redacted]	⊖	0x80000	[redacted]	[redacted]		[redacted]
☐	[redacted]	⊖	0xc70000	[redacted]	[redacted]	[redacted]	[redacted]
☐	[redacted]	✓	0x1600000	[redacted]	[redacted]	[redacted]	[redacted]
☐	[redacted]	✓	0xac2000	[redacted]	[redacted]	[redacted]	[redacted]

For each executable, you can see the following information:

- Executable File Name: Specifies the filename of the executable.
- Signature: Specifies whether or not the file was signed. Possible values: Signed, Unsigned, Self-signed, Invalid timestamp, Signed (no timestamp).
- Size: Specifies the size of the file.
- Base Address of this entry in memory.
- End Address of this entry in memory.
- Hash: Specifies the file hash. No hash is available for memory items.
- Owner: Specifies the owner of the file.
- Writable memory is indicated by the icon at the front of the stack.

You can also expand a stack to view more details, such as the last modified time (not available for writable memory entries), whether or not the stack entry is of OS executable or console application for executables and DLLs.



You can perform the following actions in the stacks view table:

- Remediate a file or retrieve memory using the *Remediate* or *Retrieve* buttons (Remediate Retrieve) at the top-left of the table.
- Customize the columns to display in the table using the *Customize* button (Customize).
- Search for a specific stack entry using the search bar on the top right corner (Is ⌄ Search 🔍).

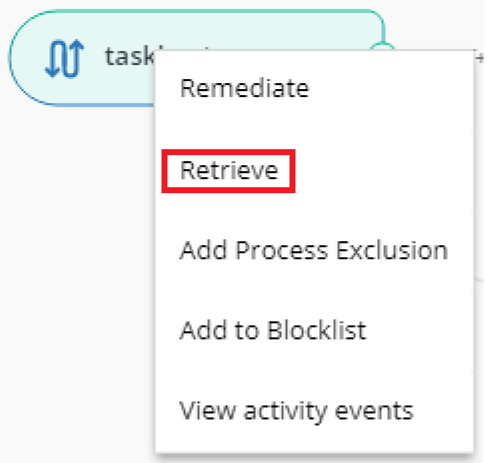
Retrieving memory

The Retrieve Memory function enables you to retrieve the stack-memory of a specific Collector to perform deeper analysis by analyzing the actual memory from the device. Memory is fetched by the Collector in binary (`*.bin`) format, compressed, encrypted and then sent to the user's local machine. The returned file is password-protected with the password `enCrypted`. If the file cannot be sent, it is saved locally on the host by the Collector.

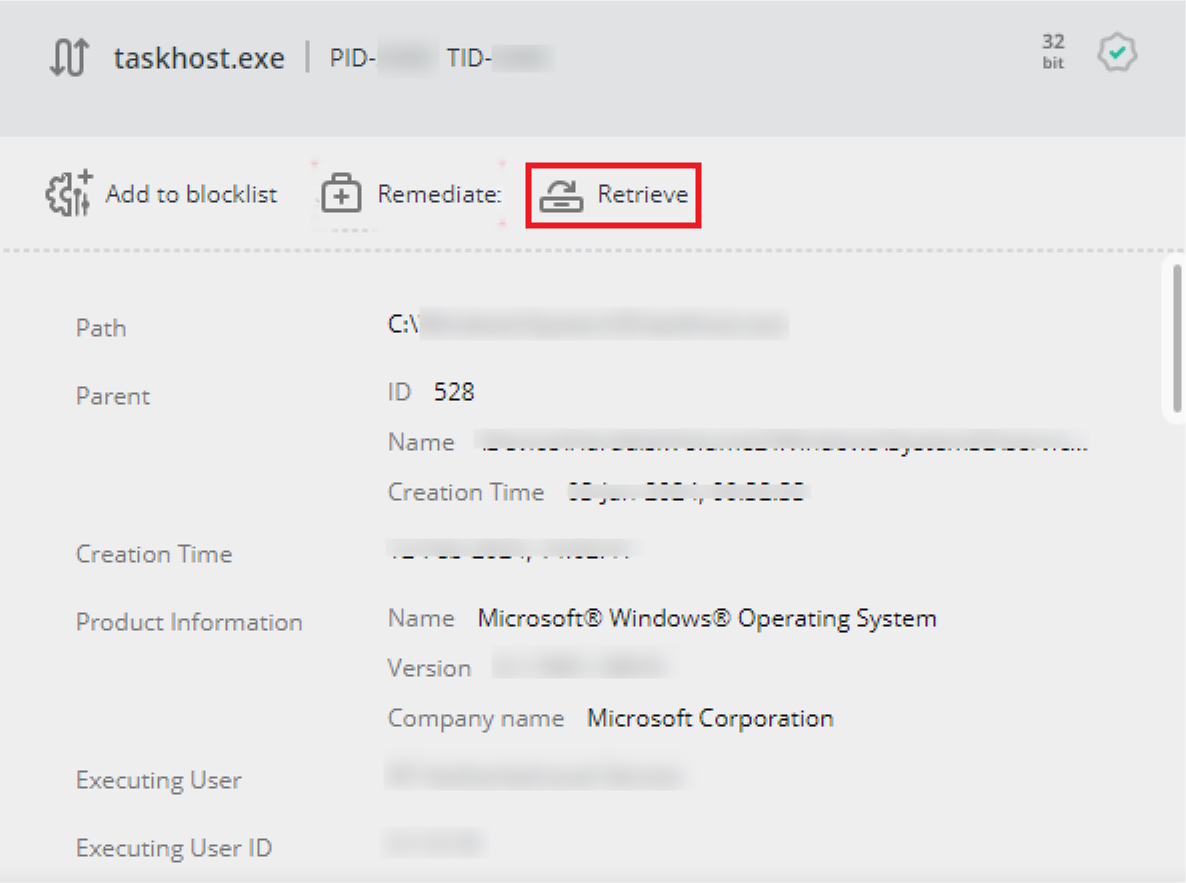
This function is accessible from the Investigation View on page 92 (detailed in the procedure below) or by connecting to the device directly using the FortiEDR Connect on page 109 functionality.

To retrieve memory for a Collector from the investigation view:

1. Right-click the node of the relevant activity event and select *Retrieve*.



Alternatively, select the node of the relevant activity event and click the *Retrieve* button in the *Details Pane* that appears on the right.



taskhost.exe | PID-[redacted] TID-[redacted] 32 bit

Path C:\[redacted]

Parent ID 528
Name [redacted]
Creation Time [redacted]

Creation Time [redacted]

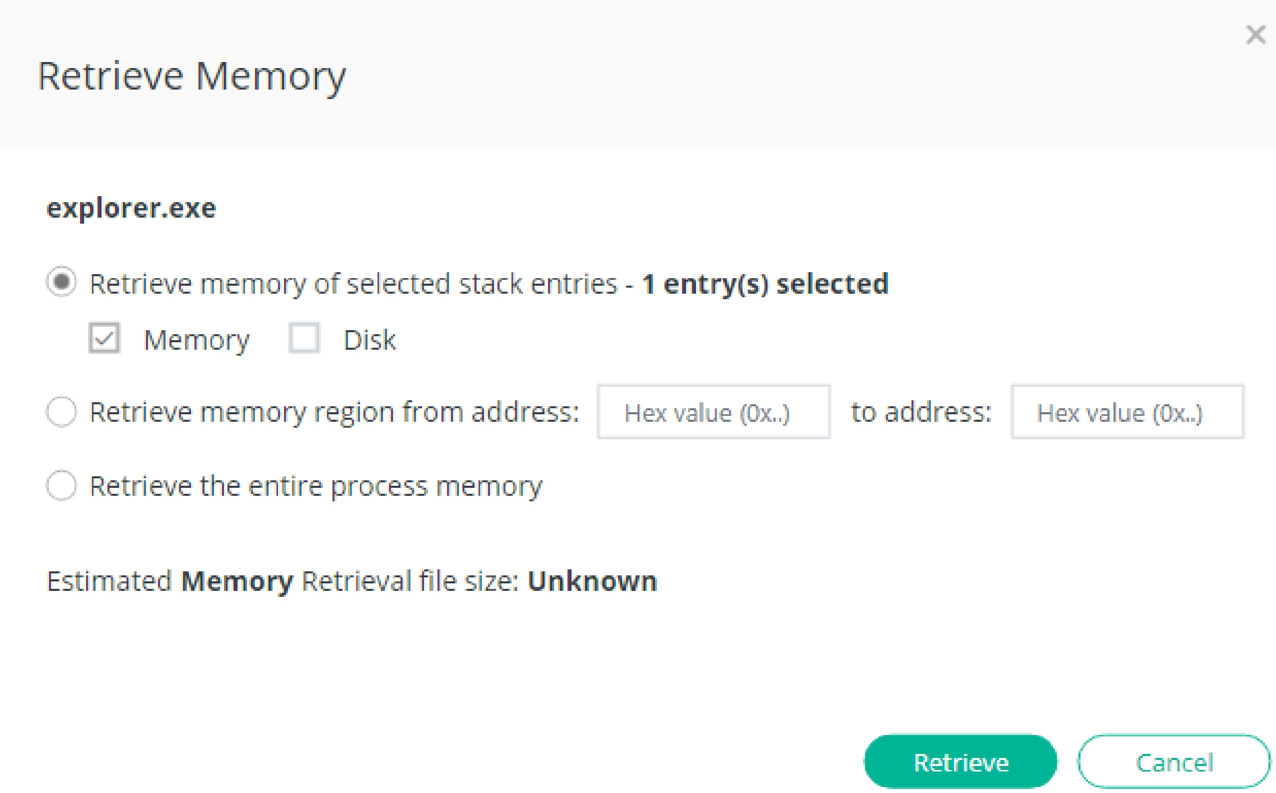
Product Information Name Microsoft® Windows® Operating System
Version [redacted]
Company name Microsoft Corporation

Executing User [redacted]

Executing User ID [redacted]

The *Retrieve* button is also available from the Stacks view on page 99, which is available when an edge is selected.

2. The following window displays:



Retrieve Memory

explorer.exe

● Retrieve memory of selected stack entries - **1 entry(s) selected**

☑ Memory ☐ Disk

○ Retrieve memory region from address: Hex value (0x..) to address: Hex value (0x..)

○ Retrieve the entire process memory

Estimated **Memory** Retrieval file size: **Unknown**

3. Select one of the following options:
   1. *Retrieve memory of selected stack entries*: Select this radio button to retrieve memory for one or more specific stack entries. Then, select the stack entries you want to analyze by checking their checkboxes.
      You must also specify whether to retrieve the memory from memory, disk, or both by selecting the respective checkbox. The *Memory* option is the default. You can select either option or both options. It is important to remember that the retrievable data may be different in the memory and on disk. In addition, the stack entry may no longer reside in memory, for example, if the system was rebooted. After you make your selection, the window indicates how many stack entries were selected.
   2. *Retrieve memory region from address*: Select this option to retrieve memory from a specific memory region. Specify the *To* and *From* addresses for the region in the adjacent fields.
   3. *Retrieve the entire process memory*: Select this option to retrieve memory for an entire process. This option retrieves all the stack entries comprising the process.
4. Click *Retrieve*.

Isolating a device

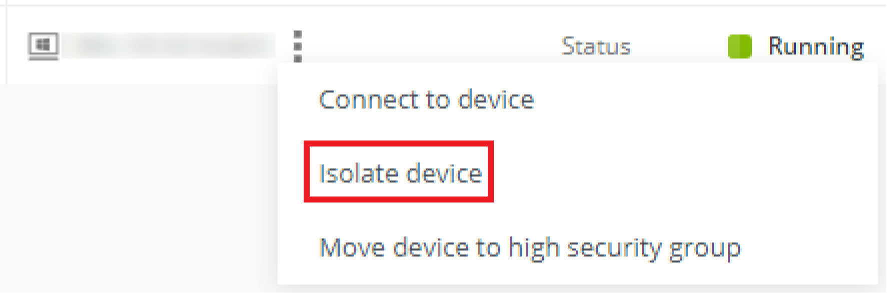
An isolated device is one that is blocked from communicating with the outside world (for both sending and receiving). A device can be isolated manually from the *Inventory > Collectors* page or the Investigation View on page 92 (detailed below).

Isolation mode takes effect upon any attempt to establish a network session after isolation mode has been initiated. Connections that were established before device isolation was initiated remain intact. The same applies for Communication Control denial configuration changes. Note that both Isolation mode and Communication Control denial do not apply on incoming RDP connections and ICMP connections.

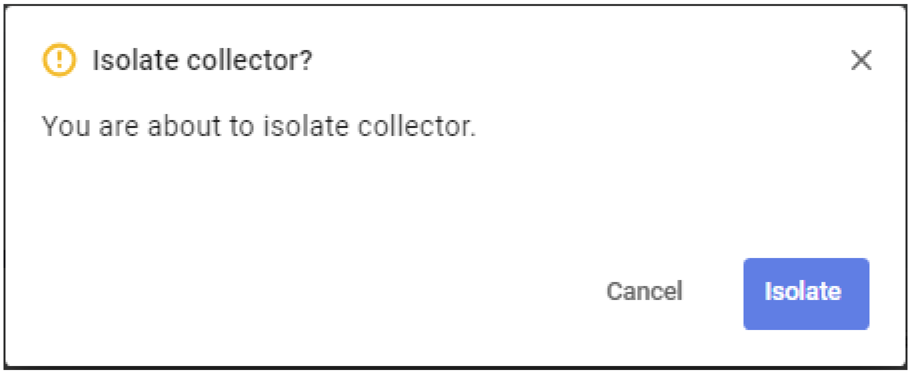
For more details about device isolation, see Investigation on page 249.

To isolate a device from the investigation view:

1. In the Investigation View on page 92 of an event with an associated device that you want to isolate, click the eclipses on the right of the device name and select *Isolate device*, as shown below:



2. In the window that appears, click *Isolate*.

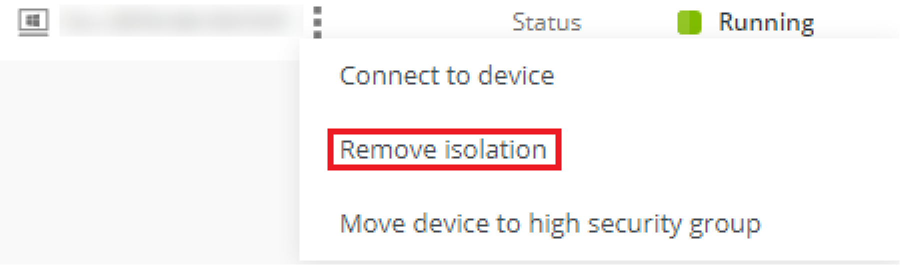


Isolate collector?

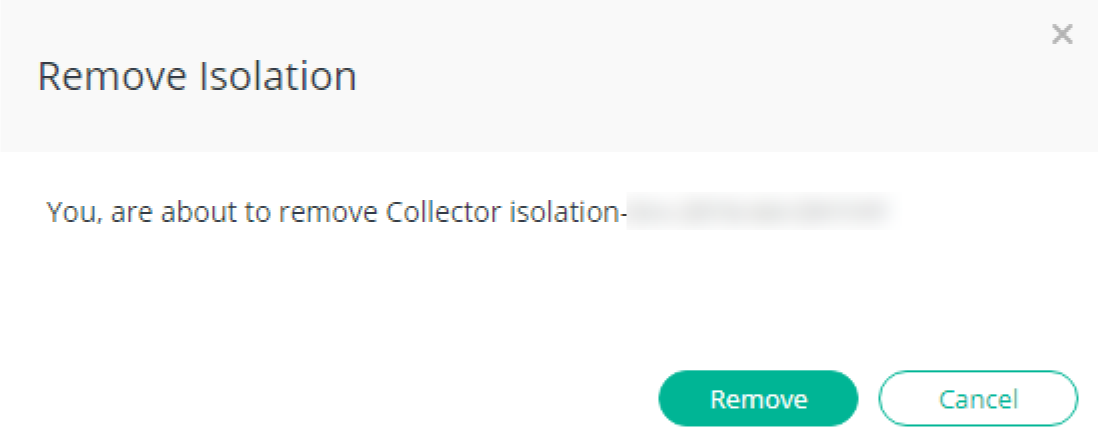
You are about to isolate collector.

To remove isolation from a device in the investigation view:

1. In the Investigation View on page 92 of the same event, click the eclipses on the right of the device name and select *Remove isolation*, as shown below:



2. In the window that appears, click *Remove*.



Remove Isolation

You, are about to remove Collector isolation-[redacted]

Remediating a device upon malware detection

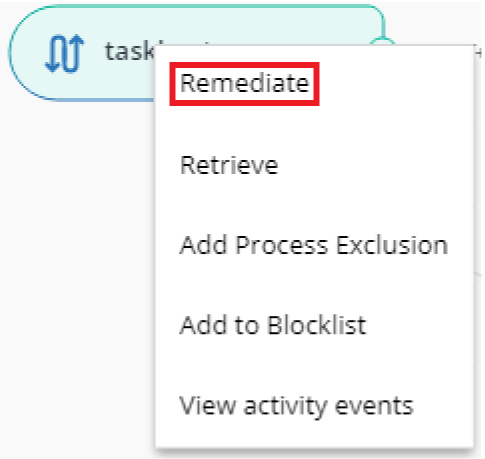
After malware is detected on a device, you can remediate the device from the Investigation View on page 92 (detailed in the procedure below) or by connecting to the device directly using the FortiEDR Connect on page 109 functionality.

The following options are available when you remediate the situation in the FortiEDR system:

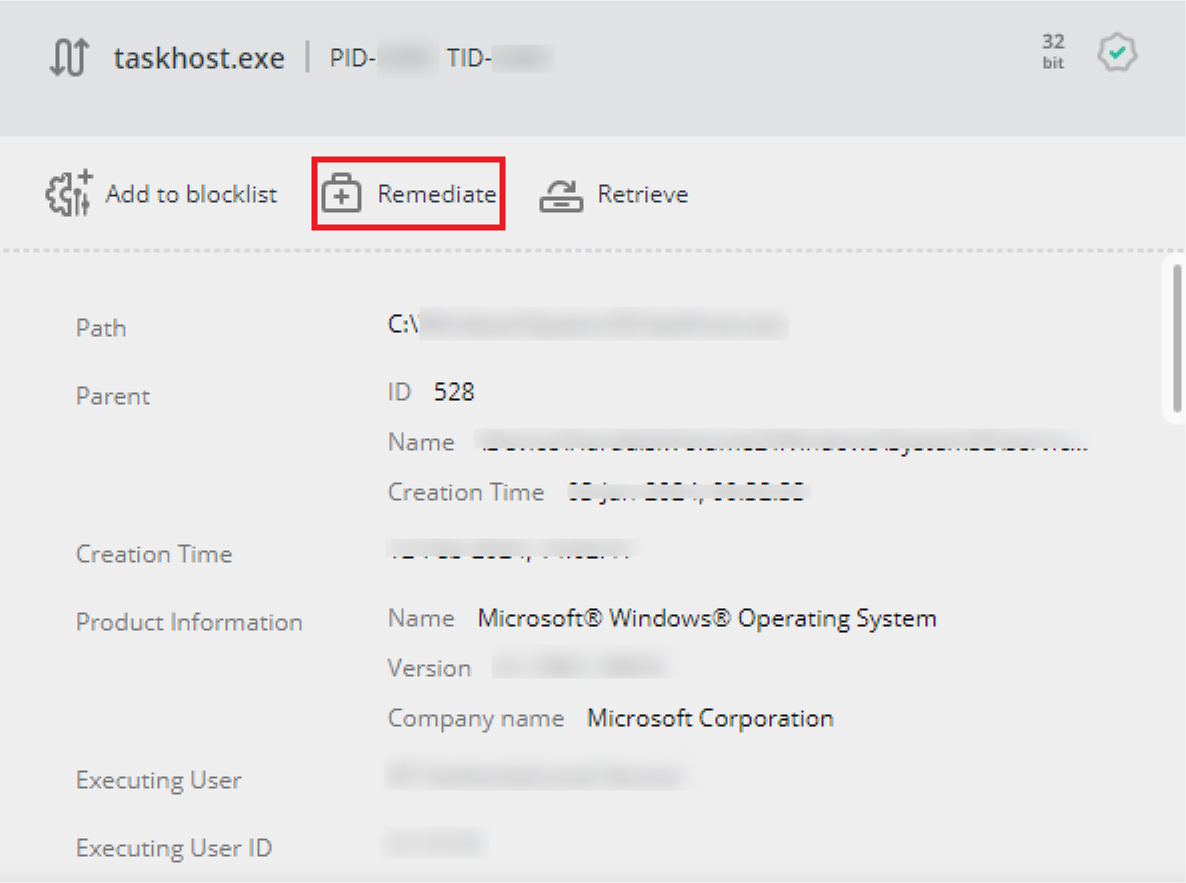
Method	Description
Terminate the Process	This method does not guarantee that the affected process will not attempt to execute again.
Delete the Affected File from the Computer	This method ensures that the file does not attempt to exfiltrate data again, as the file is permanently removed from the device. When using this method, be careful not to delete files that are important to the system, in order to protect system stability.
Remove or Modify the Registry Key	This method removes a registry key or updates a registry key's value. This method changes malicious registry key modifications by removing newly created keys or returning key values to their original form. Some malware have persistency capabilities, which makes the infection appear again. In addition, in some rare cases, malware can cause the system to crash if you try to remove them. Both of these methods can be performed using the Forensics add-on.

To remediate a device from the Investigation View on page 92:

1. Right-click the node of the relevant activity event and select *Remediate*.



Alternatively, select the node of the relevant activity event and click the *Remediate* button in the *Details Pane* that appears on the right.

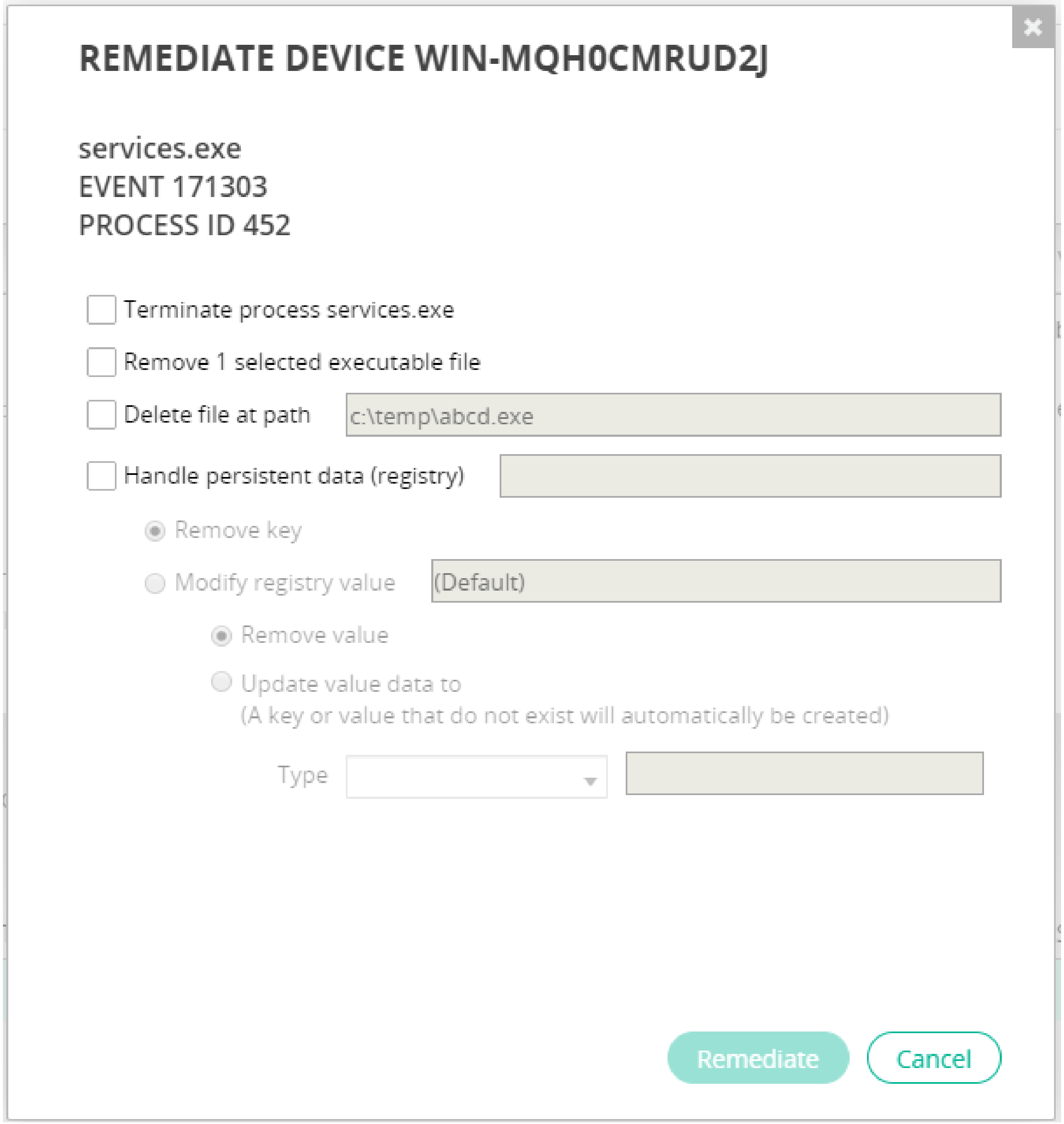


taskhost.exe | PID-[redacted] TID-[redacted]

Path	C:\[redacted]
Parent	ID 528 Name [redacted] Creation Time [redacted]
Creation Time	[redacted]
Product Information	Name Microsoft® Windows® Operating System Version [redacted] Company name Microsoft Corporation
Executing User	[redacted]
Executing User ID	[redacted]

The *Remediate* button is also available from the Stacks view on page 99, which is available when an edge is selected.

2. The following window displays:



REMEDIATE DEVICE WIN-MQH0CMRUD2J

services.exe
EVENT 171303
PROCESS ID 452

□ Terminate process services.exe

□ Remove 1 selected executable file

□ Delete file at path c:\temp\abcd.exe

□ Handle persistent data (registry)

● Remove key

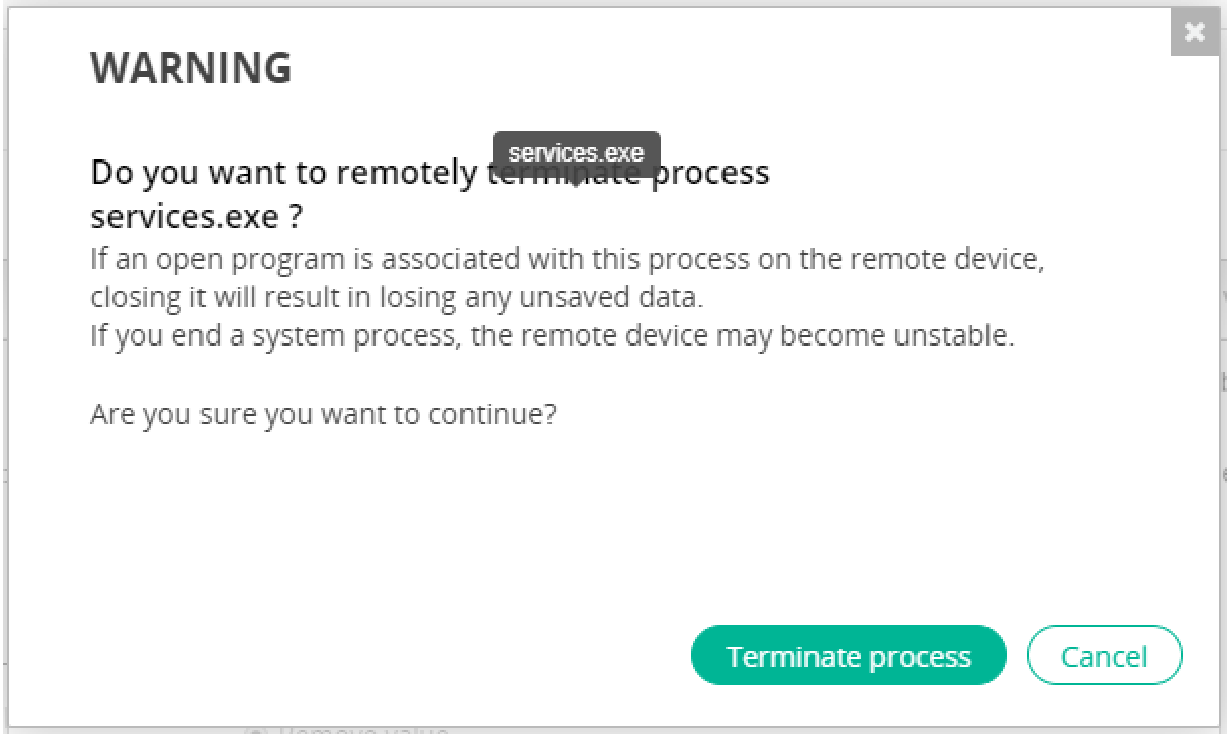
○ Modify registry value (Default)

● Remove value

○ Update value data to
(A key or value that do not exist will automatically be created)

Type

3. Do one of the following:
   a. Check the *Terminate process* checkbox to terminate the selected process. A warning message displays.



WARNING

Do you want to remotely terminate process services.exe ?

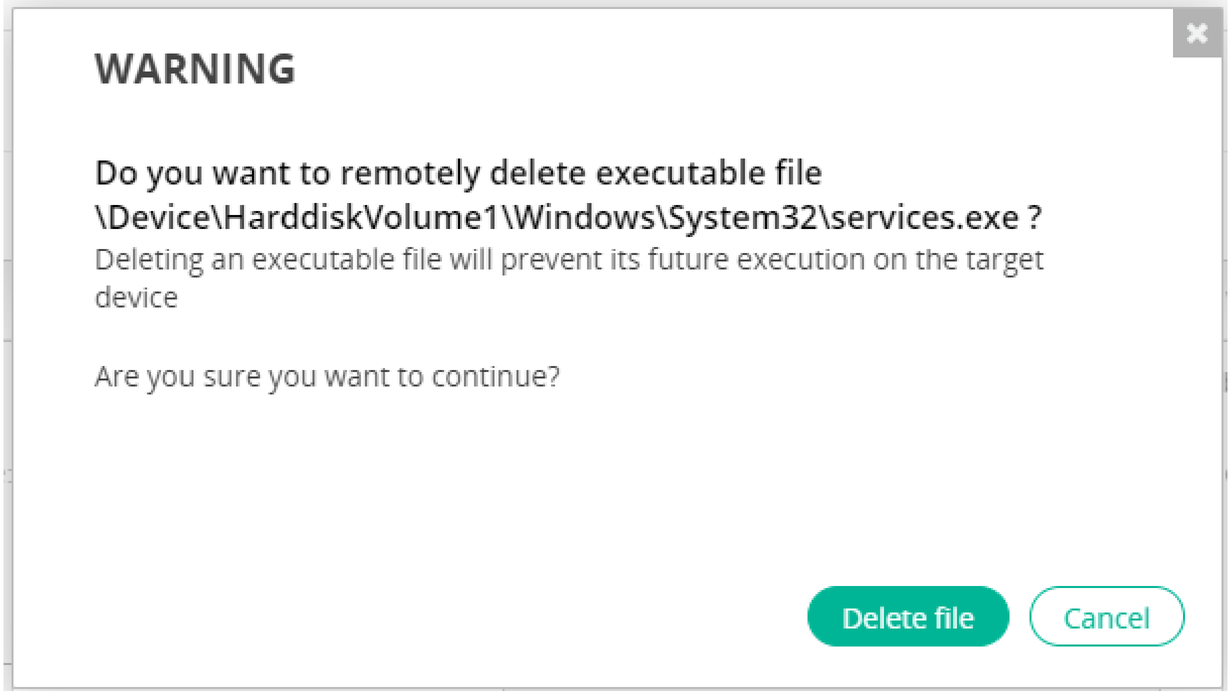
If an open program is associated with this process on the remote device, closing it will result in losing any unsaved data.

If you end a system process, the remote device may become unstable.

Are you sure you want to continue?

Click *Terminate process* to terminate the selected process.

b. Check the *Remove selected executable file* checkbox to delete the specified file from the device. A warning message displays.



WARNING

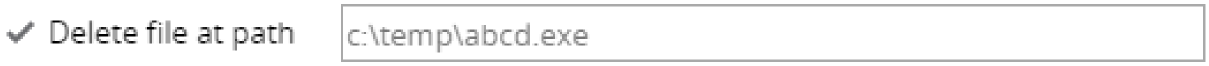
Do you want to remotely delete executable file \Device\HarddiskVolume1\Windows\System32\services.exe ?

Deleting an executable file will prevent its future execution on the target device

Are you sure you want to continue?

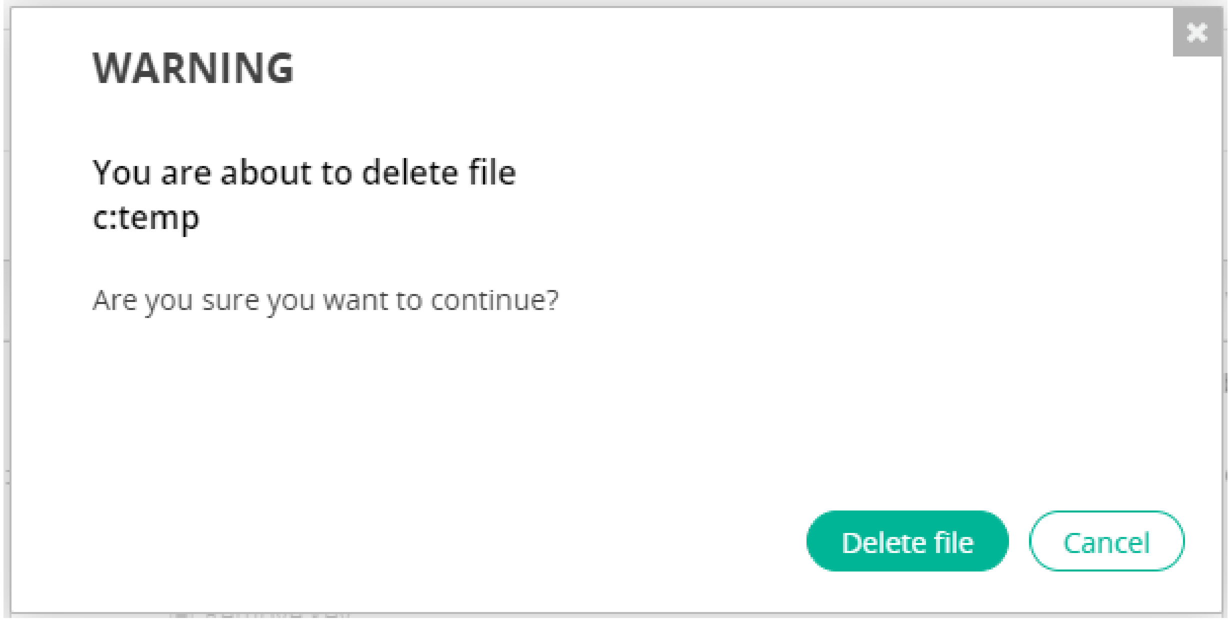
Click *Delete file* to remove the selected file.

c. Check the *Delete file at path* checkbox. In the adjacent field, enter the file path on the device that contains the file to be removed.



✓ Delete file at path c:\temp\abcd.exe

A warning message displays.



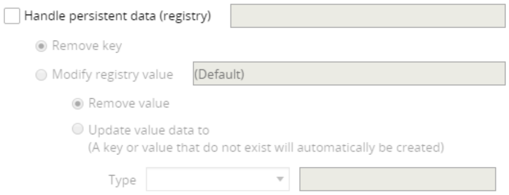
WARNING

You are about to delete file c:temp

Are you sure you want to continue?

Click *Delete file* to remove the file from the specified path.

d. Check the *Handle persistent data (registry)* checkbox to clean the registry keys in Windows. In the adjacent field, enter the value of the registry key to be removed or modified.



☐ Handle persistent data (registry)

● Remove key

○ Modify registry value (Default)

● Remove value

○ Update value data to
(A key or value that do not exist will automatically be created)

Type

Value data should be provided in the required format, based on the value type selected in the dropdown list, as follows:

- *String* for types REG_SZ(1), REG_EXPAND_SZ(2), REG_DWORD(4) and REG_QWORD(11).
- *Base64* for types REG_BINARY(3), REG_DWORD_BIG_ENDIAN(5), REG_LINK(6), REG_MULTI_SZ (7), REG_RESOURCE_LIST(8), REG_FULL_RESOURCE_DESCRIPTOR(9) and REG_RESOURCE_REQUIREMENTS_LIST(10).

Select the *Remove key* radio button to remove the registry key value.

Select the *Modify registry value* radio button to change the current registry key value. When selecting this option, you must also specify the new value for the registry key in the gray box and the key's value type in the adjacent dropdown menu (for example, string, binary and so on).

4. Click *Remediate*.

FortiEDR Connect

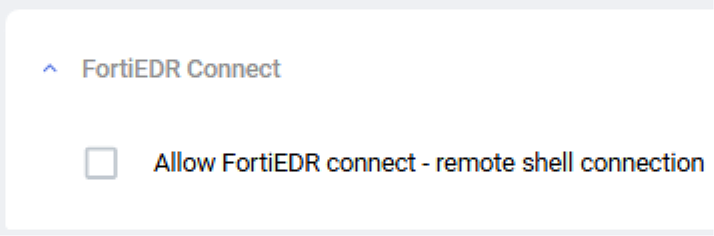
The FortiEDR Connect feature opens a console that provides direct access to a FortiEDR-protected device running a v5.2 Windows Collector through a remote Shell connection. This enables you to respond to incidents immediately and to perform in-depth investigation by running commands and scripts on the device, collecting and downloading forensic data from the device, remediating threats, and so on.

A FortiEDR Connect console can be accessed from various FortiEDR pages that list devices, such as such as the *Inventory* tab, the *Threat Hunting on page 125* tab, and the Investigation View on page 92.

- A *Connect to Device* button appears at the top of these pages, which enables you to connect to the device that is selected in the list.
- You can only connect to a single device in each FortiEDR Connect session. See Connecting to a FortiEDR-protected device on page 109.
- A device can only be connected to a single session at a time.
- Each FortiEDR user can have up to ten FortiEDR Connect sessions open and connected at the same time – each to a different device.
- Multiple users in your organization can open up FortiEDR Connect sessions (on the FortiEDR Manager), but no more than 30 sessions can be opened at the same time.

To allow a user access to the FortiEDR Connect functionality, configure the following options. Otherwise, the *Connect to Device* button is deactivated for the user.

- In *Administration > Settings*, ensure that the *Allow FortiEDR Connect – remote shell connection* checkbox is selected, which enables the FortiEDR Connect functionality for the organization. See FortiEDR Connect on page 334.



FortiEDR Connect

□ Allow FortiEDR connect - remote shell connection

- Select the *FortiEDR Connect* option in the user role capability to grant the user access to the FortiEDR Connect functionality. See Users on page 277.

This checkbox is available for Admin, Analyst, and Senior Analyst users only.

Connecting to a FortiEDR-protected device

The following describes how to open a FortiEDR Connect console session that connects you directly to a FortiEDR-protected device.

To directly access a FortiEDR-protected device:

1. A FortiEDR Connect console can be accessed from various FortiEDR pages that list devices, such as the *Assets on page 256* tab, the *Threat Hunting on page 125* tab, and the Investigation View on page 92. The operation of the FortiEDR Connect console is the same regardless of where it was accessed from.
2. Select the relevant device from the list.
   You can only connect to a single device at a time, and therefore, if you select more than one device, the *Connect to Device* button is deactivated.

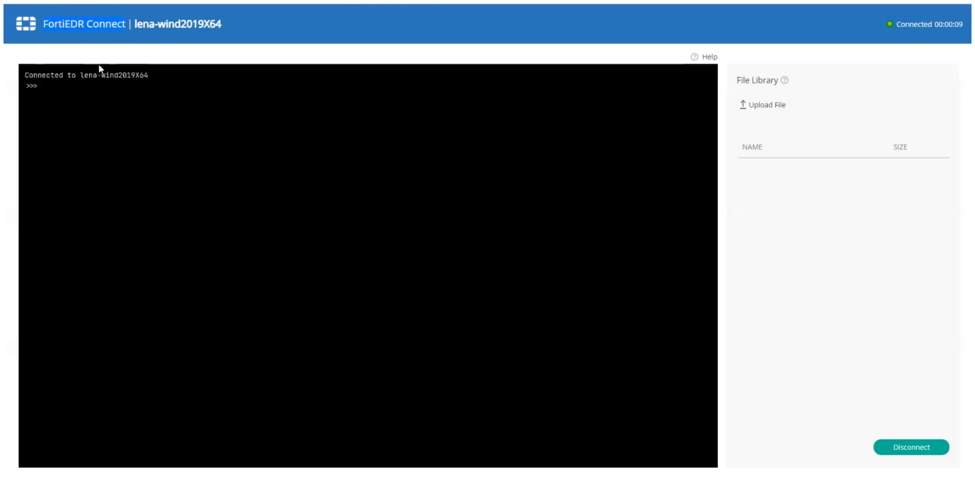
   You can only connect to accessible devices. For example, the *Connect to Device* button is deactivated, when you select a disconnected device.

   If the list only displays a single device, then the *Connect to Device* button automatically applies to that device without you needing to select it.

3. Click the *Connect to Device* button at the top of the list. For example, as shown below –

   Connect to Device

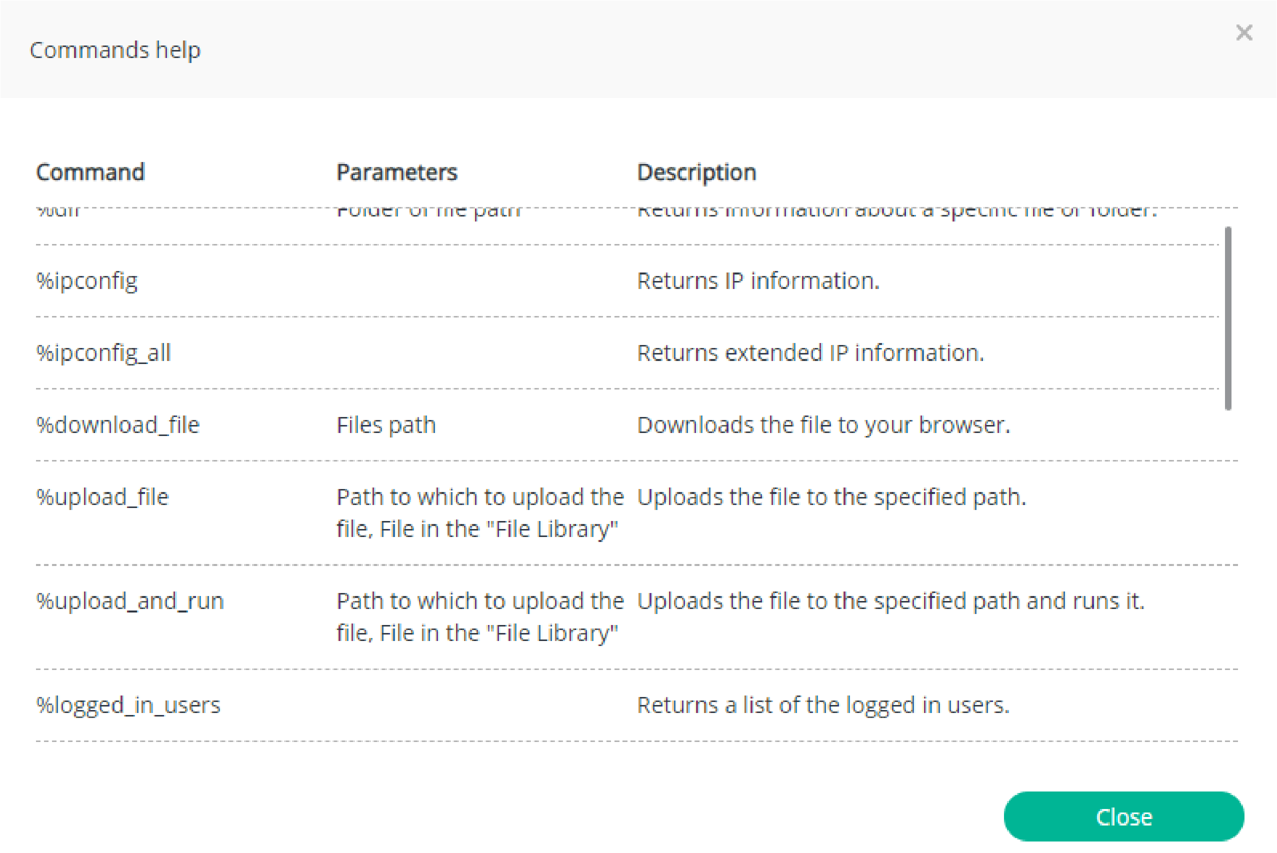
   A Shell window opens in a new browser tab. You may be requested to wait while the connection is established.
   The following displays after the connection has been established:



```
Connected to lena-wind2019X64
>>>
```

   The name of the device is displayed in the top left corner of the page.

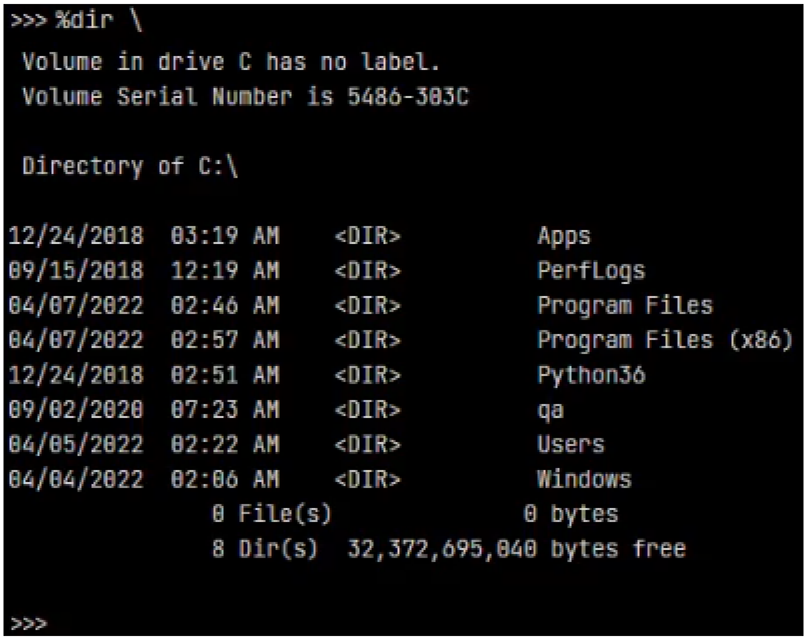
   The connection status and a timer is displayed in the top right corner of the page.
4. The main part of this page shows a terminal screen (black) with a prompt (>>>) at the top left where you can type commands.
   Clicking the *Help* button at the top right of the terminal screen displays a list of the commands (and their parameters) that you can run. To run a command, simply type it (for example, %dir) with its parameters and press `Enter`. Note that when the parameter should be Path, full path should be provided. For example: `c:\MyDirectory or c:\MyDirectory\MyPath.`



Commands help

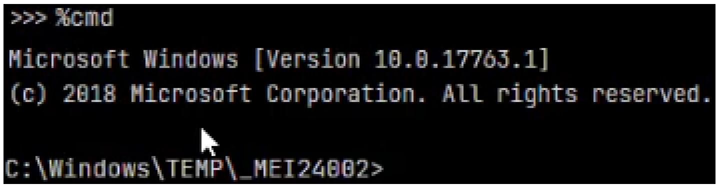
Command	Parameters	Description
%dir	Folder or file path	Returns information about a specific file or folder.
%ipconfig		Returns IP information.
%ipconfig_all		Returns extended IP information.
%download_file	Files path	Downloads the file to your browser.
%upload_file	Path to which to upload the file, File in the "File Library"	Uploads the file to the specified path.
%upload_and_run	Path to which to upload the file, File in the "File Library"	Uploads the file to the specified path and runs it.
%logged_in_users		Returns a list of the logged in users.

Most of these are FortiEDR-specific commands. For example, typing `%dir \` displays the following:



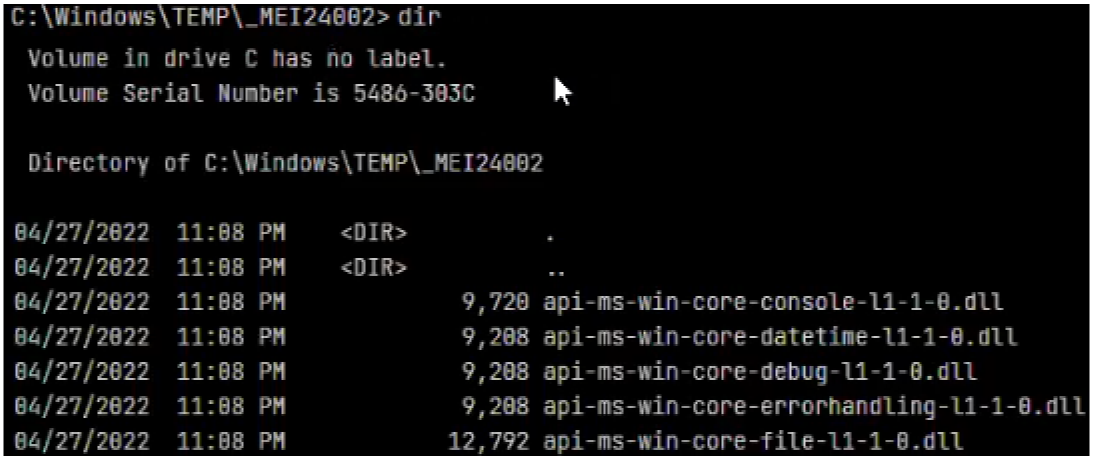
```
>>> %dir \
 Volume in drive C has no label.
 Volume Serial Number is 5486-303C

 Directory of C:\

12/24/2018  03:19 AM    <DIR>          Apps
09/15/2018  12:19 AM    <DIR>          PerfLogs
04/07/2022  02:46 AM    <DIR>          Program Files
04/07/2022  02:57 AM    <DIR>          Program Files (x86)
12/24/2018  02:51 AM    <DIR>          Python36
09/02/2020  07:23 AM    <DIR>          qa
04/05/2022  02:22 AM    <DIR>          Users
04/04/2022  02:06 AM    <DIR>          Windows
               0 File(s)              0 bytes
               8 Dir(s)  32,372,695,040 bytes free

>>>
```

In addition, you can use the `%cmd` command to open a command prompt view, as shown below.



```
>>> %cmd
Microsoft Windows [Version 10.0.17763.1]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\TEMP\_MEI24002>
```

This view enables you to enter standard Microsoft terminal (cmd) commands, such as `dir`. For example, the following displays:



```
C:\Windows\TEMP\_MEI24002> dir
 Volume in drive C has no label.
 Volume Serial Number is 5486-303C

 Directory of C:\Windows\TEMP\_MEI24002

04/27/2022  11:08 PM    <DIR>          .
04/27/2022  11:08 PM    <DIR>          ..
04/27/2022  11:08 PM             9,720 api-ms-win-core-console-l1-1-0.dll
04/27/2022  11:08 PM             9,208 api-ms-win-core-datetime-l1-1-0.dll
04/27/2022  11:08 PM             9,208 api-ms-win-core-debug-l1-1-0.dll
04/27/2022  11:08 PM             9,208 api-ms-win-core-errorhandling-l1-1-0.dll
04/27/2022  11:08 PM            12,792 api-ms-win-core-file-l1-1-0.dll
```

In addition, you can run Python command at the prompt. The supported Python version is 3.*x*.

The FortiEDR Audit Trail on page 314 feature records the connection of a FortiEDR Connect session and every action that was performed in the session.

File Library pane

The File Library pane on the right enables you to upload, download and reuse files during FortiEDR Connect sessions from/to FortiEDR-protected device. No other users can see these files or upload/download from/to your FortiEDR Connect session. These files are deleted everywhere when you close the FortiEDR Connect Console, as described in Disconnecting FortiEDR Connect session on page 114. A FortiEDR Connect session enables you to:

- Upload a file to the FortiEDR File Library on the FortiEDR Manager.
- Upload a file from the FortiEDR File Library to a FortiEDR-protected device by running the `%upload_file` or `%upload_and_run` command. For example, to upload a forensics script to the device.
- Download a file from the FortiEDR-protected device. For example, to download an executable from the device for further inspection in a sandbox.

Uploading a file to the FortiEDR file library

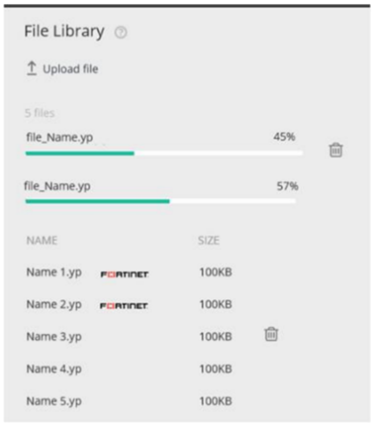
The *File Library* page lists the files that you have uploaded to the FortiEDR file library on the FortiEDR Manager during the current FortiEDR Connect sessions, and that are available to be uploaded on the devices.

To upload a file to the FortiEDR file library:

1. Open a FortiEDR Connect session with a FortiEDR-protected device, as described on Updating the Collector version on page 405.
2. Click the *Upload File* button in the *File Library* pane. A standard file selection window is displayed.
3. Select a file and click the *Open* button.

   You can hover over the question mark icon (?) at the top right of the *File Library* pane to display a tooltip showing the file size limitation.

   A progress bar is displayed while the file is uploading, as shown below. After the file has been uploaded (100%), it appears in the list at the bottom of the pane.



File Library ?

5 files

file_Name.yp 45%

file_Name.yp 57%

NAME	SIZE
Name 1.yp	100KB
Name 2.yp	100KB
Name 3.yp	100KB
Name 4.yp	100KB
Name 5.yp	100KB

- To stop an upload that is in progress, click the *Delete* button (🗑) next to its progress bar.
- To delete a file that has already been uploaded into the file library, click the *Delete* button (🗑) next to its name.

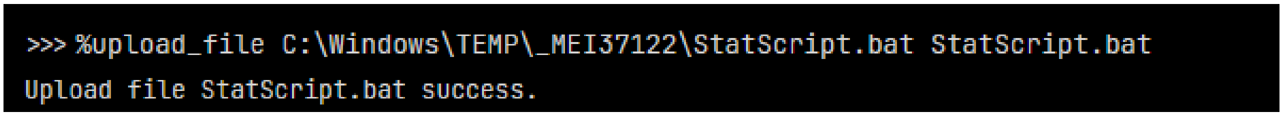
Uploading a file from the FortiEDR file library to a FortiEDR-protected device

The following describes how to upload a file from the FortiEDR file library to a FortiEDR-protected device.

To upload a file to a FortiEDR-protected device:

1. Open a FortiEDR Connect session with a FortiEDR-protected device, as Connecting to a FortiEDR-protected device on page 109.

2. In case the file doesn't appear at the file library, upload a file to the FortiEDR file library on the FortiEDR Manager, as described on File Library pane on page 112. The File Library page lists the files that you have uploaded to the FortiEDR file library.
3. At the prompt in the FortiEDR console, enter the `%upload_file` or `%upload_and_run` command and specify the path to which it should be uploaded, including the name it should have at the uploaded location, and file name to be uploaded. For example:



```
>>> %upload_file C:\Windows\TEMP\_MEI37122\StatScript.bat StatScript.bat
Upload file StatScript.bat success.
```

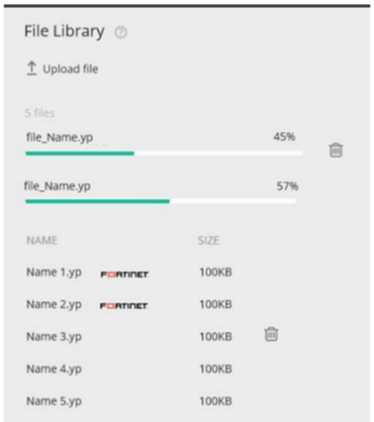
Download a file from a FortiEDR-protected device

The following describes how to download a file from a FortiEDR-protected device.

To download a file from a FortiEDR-protected device:

Open a FortiEDR Connect session with a FortiEDR-protected device, as described on Connecting to a FortiEDR-protected device on page 109. At the prompt in the FortiEDR console, enter the `%download_file` command and specify the full path and file name to be downloaded. For example, `%download_file c:\SuspiciousDir\abcfilename`

Files are downloaded directly to the `Downloads` folder on the device in which the FortiEDR Connect session is running in a browser.



File Library

Upload file

5 files

file_Name.yp 45%

file_Name.yp 57%

NAME	SIZE
Name 1.yp	100KB
Name 2.yp	100KB
Name 3.yp	100KB
Name 4.yp	100KB
Name 5.yp	100KB

Disconnecting FortiEDR Connect session

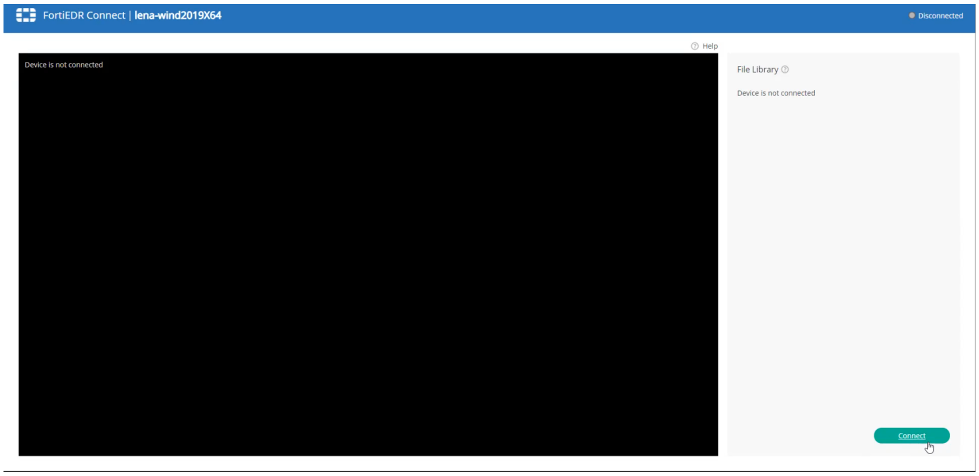
Disconnect a FortiEDR Connect session in one of the following ways:

- Clicking the *Disconnect* button at the bottom right of the *File Library* pane.
- Closing the browser tab by clicking the *Close* button.
- Logging out of the FortiEDR Console.
- Rebooting/shutting down the FortiEDR-protected device. For example, using `reboot/sh`.

- Timing out. If you are not working with the FortiEDR console session, then at some point the session will timeout and disconnect it.

After you disconnect, the message `Device is not connected` is displayed in the FortiEDR console session.

A connected button is then displayed which you can click to reconnect to the same session, as shown below:



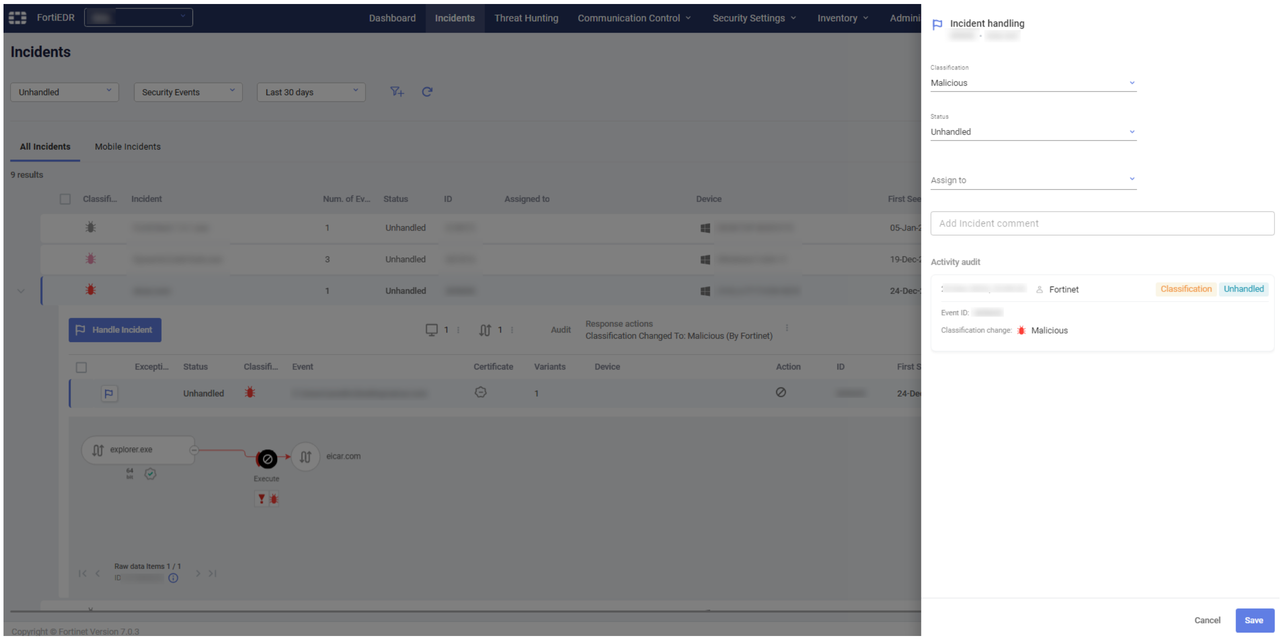
Device is not connected

Device is not connected

Marking a security event as handled/unhandled

The following describes how to specify that you have handled a security event. When any FortiEDR Central Manager user marks a security event as *Handled*, all users see it as having been handled.

1. Select the rule's checkbox and then click the *Handle Incident* button or just click the flag icon of the security event row. The *Incident handling* window displays.



Incident handling

[redacted]

Classification
Malicious

Status
Unhandled

Assign to

Add Incident comment

Activity audit

[redacted] Fortinet Classification Unhandled

Event ID: [redacted]

Classification change: Malicious

Cancel Save

If an exception was already defined for this security event, then the words event includes exceptions are displayed at the top of the *Incident handling* window.

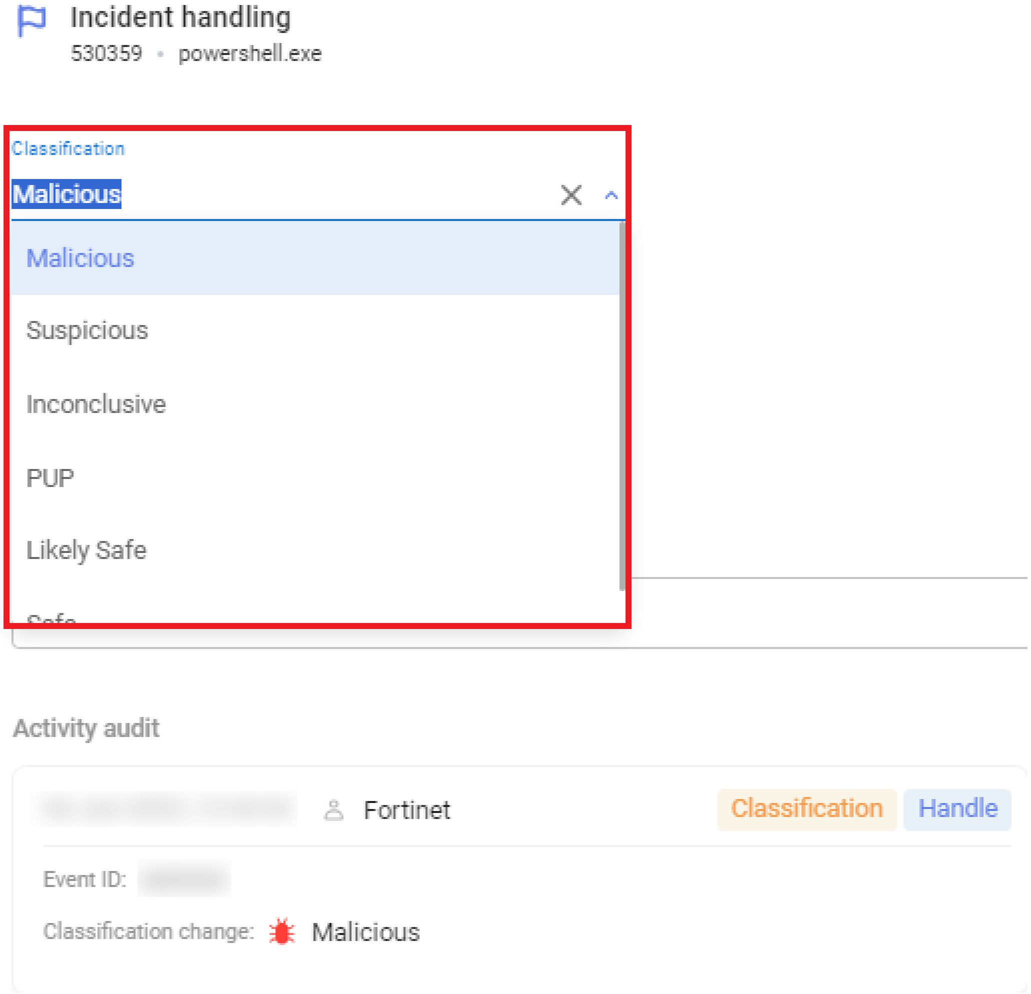
2. In the *Classification* dropdown list, change the classification for the security event, if needed. For more details, see Manually changing the classification of a security event on page 116.
3. In the comments box, use free text to describe how you handled the security event.
4. Click the *Save* button.

Manually changing the classification of a security event

You can manually change the classification of a security event, if needed.

1. Select the rule’s checkbox and then click the *Handle Incident* button or just click the flag icon of the security event row. The *Incident handling* window displays.

2. In the *Classification* dropdown list, change the classification for the security event, as needed.



Incident handling

530359 • powershell.exe

Classification

Malicious

Activity audit

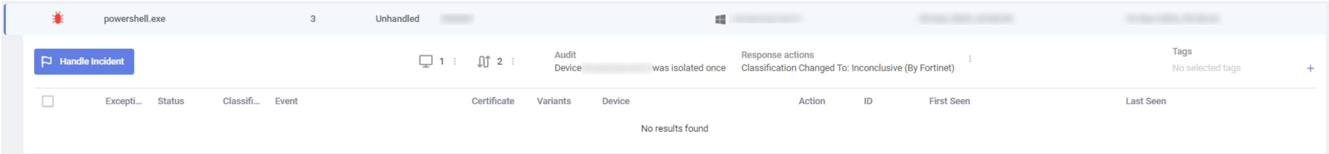
[redacted] Fortinet Classification Handle

Event ID: [redacted]

Classification change: Malicious

3. Click *Save*.

After changing the classification of a security event, the Overview on page 90 pane displays the history of any actions (Playbook policy-related actions and others) that were made automatically by FortiEDR. For Playbook policy actions, the timestamp shows when the action was performed, as defined in the Playbook policy. For more details about Playbook policy actions, see Playbook policies on page 244.



powershell.exe 3 Unhandled [redacted] [redacted] [redacted] [redacted]

Audit
Device [redacted] was isolated once

Response actions
Classification Changed To: Inconclusive (By Fortinet)

Tags
No selected tags

□	Excepti...	Status	Classifi...	Event	Certificate	Variants	Device	Action	ID	First Seen	Last Seen

No results found

When the Fortinet logo appears next to an entry in the Overview on page 90 pane, it indicates that the security event was automatically classified by FortiEDR. Security events that are manually classified do not display the Fortinet logo.

Notifications for security events are not shown in the *Overview* pane.

Defining security event exceptions

The following describes how to create a new exception and how to edit an existing one.

Exceptions enable you to limit the enforcement of a rule, meaning to create a white list for a specific flow of security events that was used to establish a connection request or perform a specific operation.

FortiEDR exception management is highly flexible and provides various options that enable you to define pinpointed, granular exceptions.

Details describing how to edit an existing exception are described in Editing security event exceptions on page 121. You can access the Exception Manager by clicking the *Exception Manager* button at the top of the *Incidents* pane or by selecting *SECURITY SETTINGS > Exception Manager*. Additional options for managing exceptions are provided in the *SECURITY SETTINGS* tab, as described in Exception Manager on page 207.

An exception that applies to a security event can result in the creation of several exception pairs.

An exception pair specifies the rule that was violated and the *process* on which the violation occurred, including or excluding its entire location path. For more details, see Playbook policies on page 244

After an exception is defined for a security event, new identical events are not triggered.

Security events that occurred in the past appear with an icon to indicate that an exception has been defined for them, even though at the time they were triggered, the exception did not exist. This icon on past security events serves as an indication to you that there is no need to create an exception for it, since one was already created (but after the event occurred).

In cases where an exception was defined for the security event but it does not fully cover all the existing occurrences or raw data items of this event, a slightly different icon is displayed, as described and shown below.

When defining an exception for Listen on Port Attempt events, listening on 0.0.0.0 means listening on all interfaces. In such cases, you should use All Destinations.

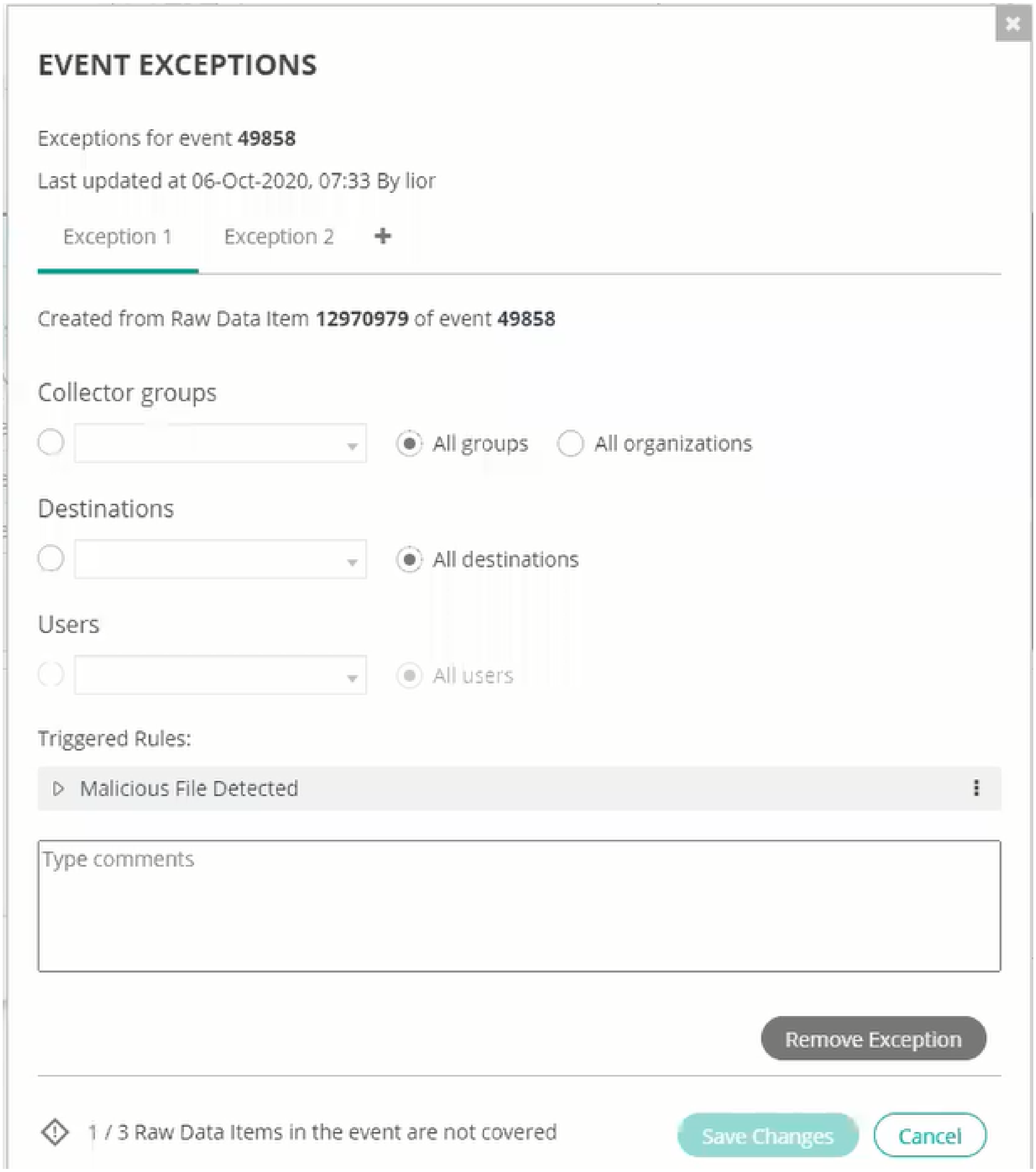
Defining the scope of an exception

When defining an exception, it is important not to make it too broad or too narrow in scope, so that it properly identifies and *catches* the data items that you want.

If an exception does not cover all the raw data items for a security event, the icon displays for that exception. This can happen, for example if the exception was defined only on part of the collector groups and the security event occurred on devices that are not part of the collector groups on which the exception was set.

In addition, the raw data items comprising a security event distinguish between data items that are covered (◈) and not covered (!) by the exception, based on the exception’s current definition.

For example, if you see that the current exception is too narrow and excludes a raw data item that you want to include in the exception, you can click the ! icon and then modify and broaden the exception sufficiently so that it will also include that raw data item. When you click the ! icon, the *Event Exceptions* window automatically opens and displays the existing exception which can be broadened. Alternatively, you can click the **+** icon to create another exception that will include the non-covered raw data item. Clicking the **+** icon after the exception is opened using the covered icon next to the raw data item opens a new exception from the perspective of that raw data item, meaning that it includes all the data that is relevant for that raw data item, as shown below:



EVENT EXCEPTIONS

Exceptions for event **49858**

Last updated at 06-Oct-2020, 07:33 By lior

Created from Raw Data Item **12970979** of event **49858**

Collector groups

○ ● All groups ○ All organizations

Destinations

○ ● All destinations

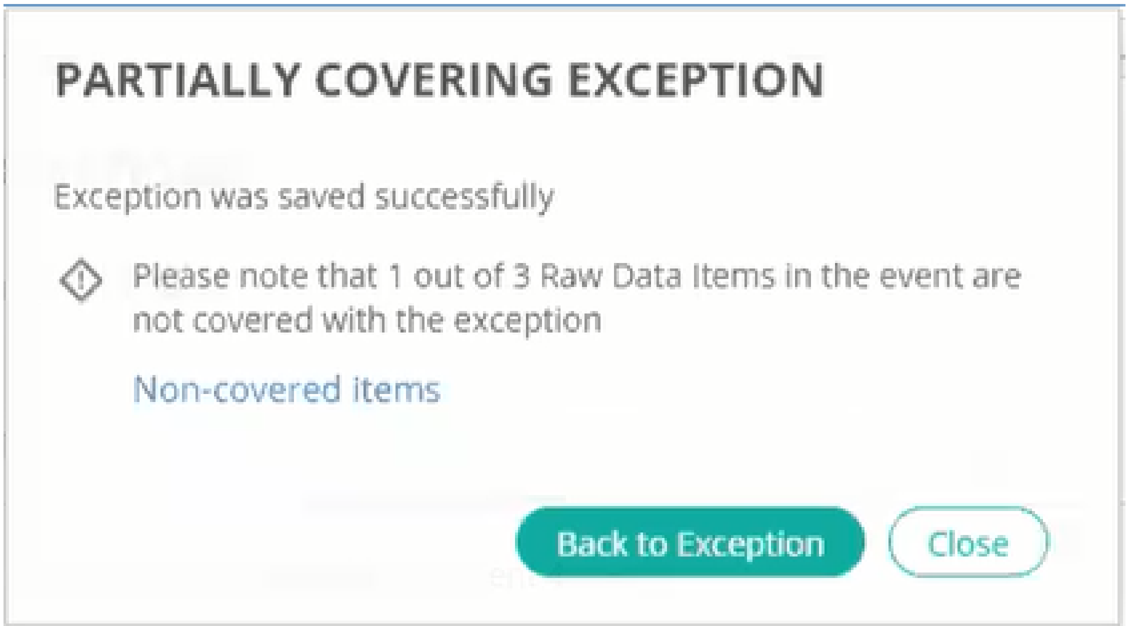
Users

○ ● All users

Triggered Rules:

1 / 3 Raw Data Items in the event are not covered

In addition, when saving an exception, if the exception does not cover all raw data items for a security event, a message such as the following displays.



PARTIALLY COVERING EXCEPTION

Exception was saved successfully

Please note that 1 out of 3 Raw Data Items in the event are not covered with the exception

Non-covered items

You can click the *Non-covered items* link in this message to open the *Incidents* tab in a new window, and display only not-covered raw data items.

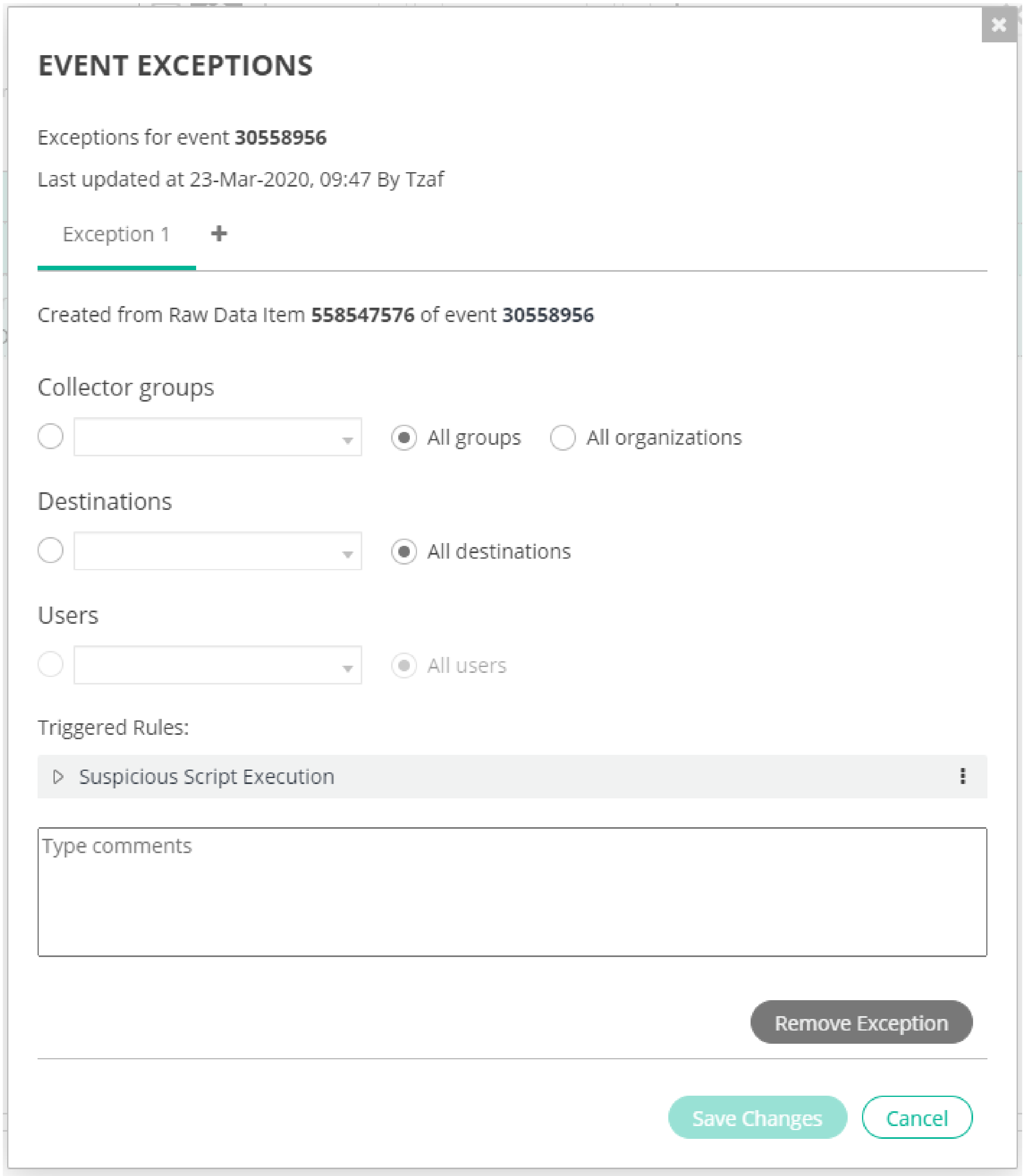
Device Control exceptions

Exceptions on device control security events are similar to other exceptions, with several additional capabilities that enable you to set the exception on a device name, description, serial number or a combination, as follows:

- The USB device's description is specified under the *Process Name* field.
- The device's serial number is listed in order to exclude a specific USB device with the designated serial number.
- The device's name is specified under the second *Process name*.

Editing security event exceptions

1. Click the *Edit Exception* button in the security event row for the exception you want to modify. The following window displays:



EVENT EXCEPTIONS

Exceptions for event **30558956**

Last updated at 23-Mar-2020, 09:47 By Tzaf

Created from Raw Data Item **558547576** of event **30558956**

Collector groups

○ ● All groups ○ All organizations

Destinations

○ ● All destinations

Users

○ ● All users

Triggered Rules:

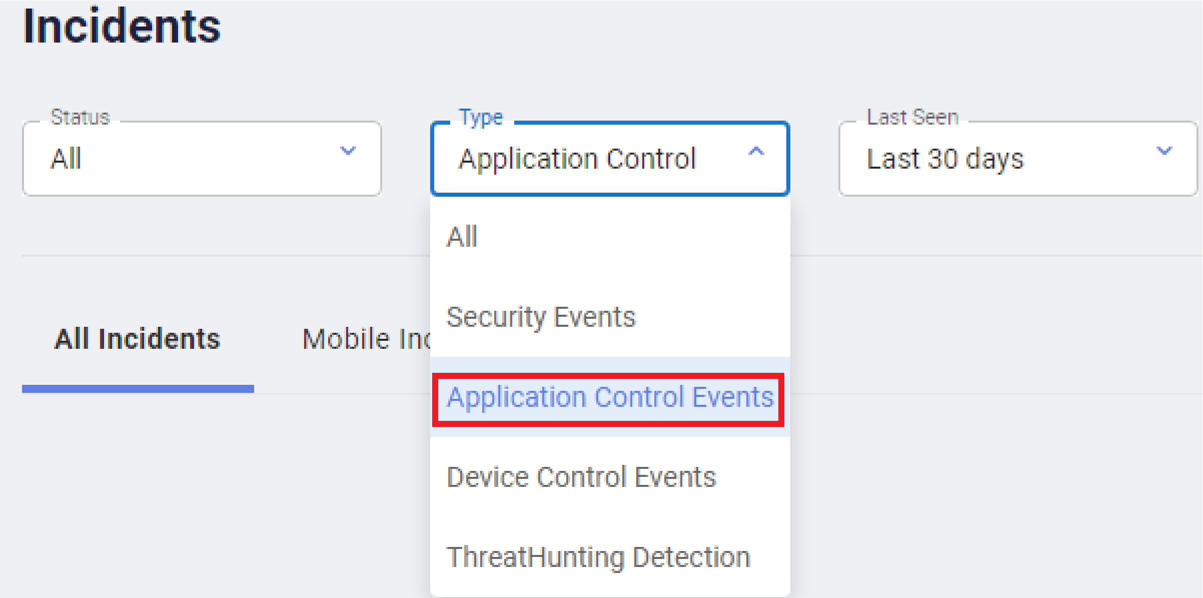
▷ Suspicious Script Execution

2. Modify the Collector Groups, Destinations and Users to which the exception applies and the pairs of rules and processes that operate together to define an exception in the *Triggered Rules* area, as needed.
   For a multi-organization FortiEDR system, an Administrator can also specify whether the exception applies to all organizations. The *All organizations* option applies the exception to all organizations, regardless of whether or not the security event already occurred.

3. Click *Save Changes*.

Viewing Application Control security events

Security events in the *Incidents* tab can be filtered to show only Application Control security events. Application control security events are events that were triggered on rules that are part of the Application Control policy. Such events do not necessarily mean that there was malicious activity but indicate an attempt to execute an application that is listed in the user-defined blocklist. These security events are displayed separately from other security events. Defining an exception for them can be done in a similar manner as for other security events. The exception specifies which applications are blocked by its hash.



Incidents

Status: All

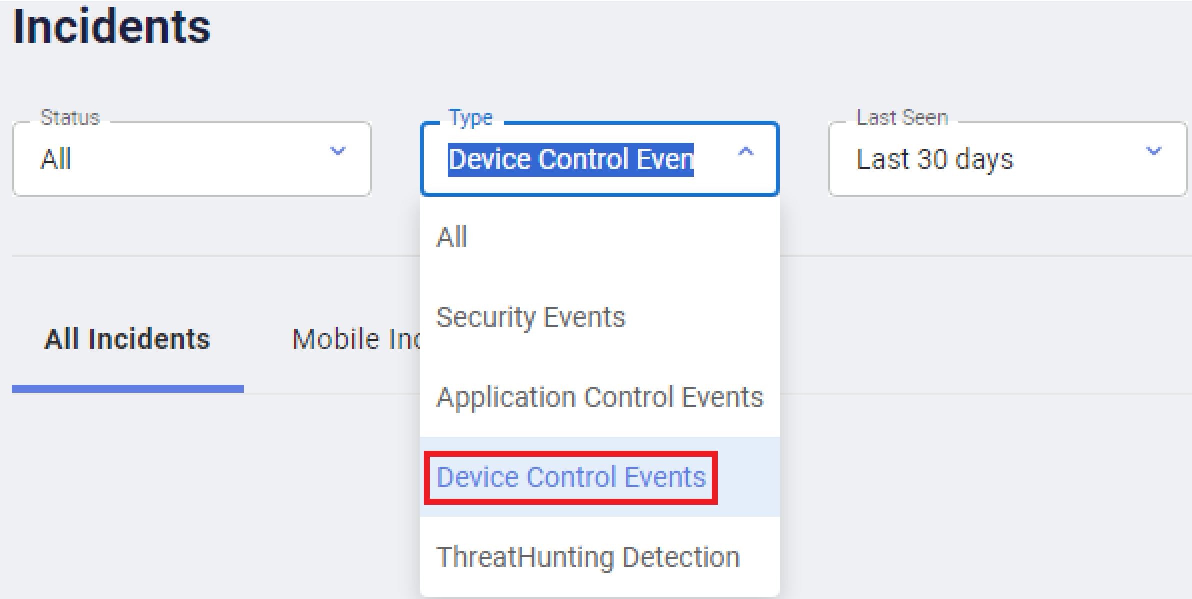
Type: Application Control

Last Seen: Last 30 days

Viewing Device Control security events

Device Control capabilities are license-dependent. You may contact Fortinet Support for more information.

Security events in the *Incidents* view can be filtered to show device control security events. Device control security events are events that were triggered on rules that are part of the Device Control policy. Such events do not necessarily mean that there was malicious activity but indicate USB peripheral access. These security events are displayed separately from other security events. Defining an exception for them can be done in a similar manner as for other security events. The exception can be set on the device name, vendor, serial number or a combination.



Incidents

Status: All

Type: Device Control Even

Last Seen: Last 30 days

Other options in the Incidents viewer

Option	Description
Sorting incidentss	Click any column name to sort security events. For example, you may want to sort by process and collector in order to see the history of everything that happened to that process on that device.
Free text search	Enter text in the search field to search by process, device, or ID.
Time Filter	Click the down arrow in the Time Filter to display a list of time period options. The default is *Last 30 days*.
Deleting incidents	Select an event and click the *Delete* button (🗑) to completely delete a security event from the FortiEDR system. A deleted incident cannot be restored or retrieved. Unless you are having storage capacity issues, we highly recommend just hiding incidents and not deleting them.
Exception Manager	Click the *Exception Manager* button (Exception Manager →) at the top right corner to access the Exception Manager on page 207.
Investigating incidents	Click the *Investigate* (Investigate →) button for a graphical and interactive view to further drill down the chain of activities involved in the event. See Investigation View on page 92.

Threat Hunting

FortiEDR's Threat Hunting functionality enables you to search for many types of Indicators of Compromise (IOCs) and malware across your entire environment in order to enable enhanced detection. Searching can be based on various attributes of files, registry keys and values, network, processes, event log and activity event types. Search operations apply to both Windows and Linux operating system activity.

Threat Hunting is ideal in situations where you have identified malware on one endpoint and want to search throughout your organization to determine whether this same malware exists on another endpoint, even though it may not be currently running (stealth mode) or in situations where you would like to hunt for the existence of a specific IoC within your organization.

Threat Hunting is a license-dependent add-on and supports only Collectors that run FortiEDR 5.0 or later. You may contact Fortinet Support for more information.

Threat Hunting utilizes *activity events*, which specify an action taken by an entity. Each type of entity may be involved in a variety of types of actions. An activity event consists of a *source* (usually a process), an *action* (the activity event type) and a *target* (Process, file, Registry key/value, network item(, where the source performs the designated action on the target.

For example, when a process runs, it can perform various actions on files, such as File Open, File Read, File Delete and so on. In this case, the process is the source, and it performs an action such as File Open on a target File.

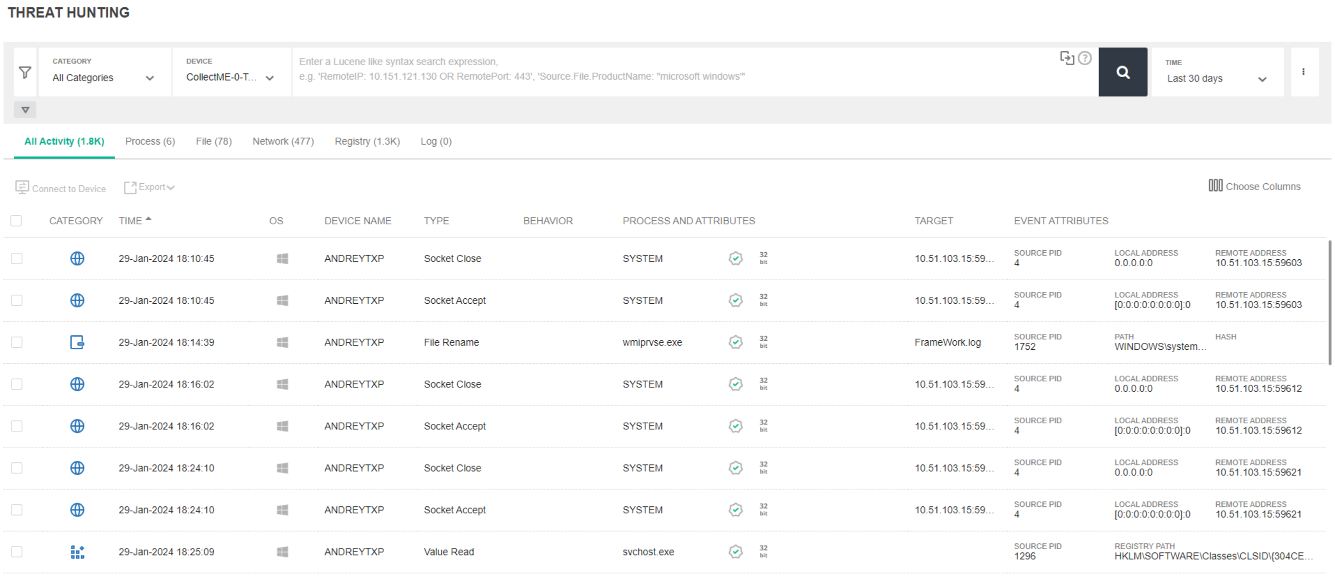
Activity events are not the same as the security events identified in the *Incidents* tab. Unlike *Incidents* tab security events, which are only reported in the *Incidents* tab as they occur and are detected, activity events are continuously collected based on a wealth of data, activity and actions occurring in your system and the chosen Threat Hunting Profile. You may refer to Threat Hunting on page 233 for more information.

FortiEDR categorizes the various actions that can be performed into the following categories:

Action	Description
Registry Key Actions	All targets are either registry keys or registry values and all actions are registry-related, such as Key Created, Key Deleted, Value Set and so on.
File Actions	All targets identify the target file on which the action was performed and all actions are file-related, such as File Create, File Delete, File Rename and so on.
Process Actions	The target is another process and all actions are process related, such as Process Termination, Process Creation, Executable Loaded and so on.
Network Actions	The target is a network item (such as connection or URL) and all actions are Network related, such as Socket Connect, Socket Close and Socket

Action	Description
	Bind.
Event Log Actions	The only action is Log Entry Created and relates to the logs of the operating system - Windows and Linux.

The *Threat Hunting* page contains the following areas:



THREAT HUNTING

CATEGORY: All Categories
DEVICE: CollectME-0-T...
Enter a Lucene like syntax search expression,
e.g. 'RemoteIP: 10.151.121.130 OR RemotePort: 443', 'Source.File.ProductName: "microsoft windows"'
TIME: Last 30 days

All Activity (1.8K) | Process (6) | File (78) | Network (477) | Registry (1.3K) | Log (0)

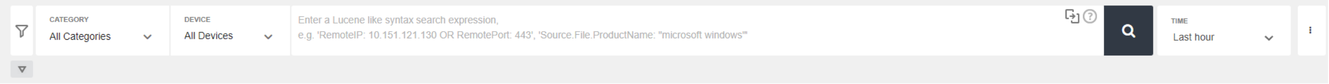
Connect to Device | Export | Choose Columns

CATEGORY	TIME	OS	DEVICE NAME	TYPE	BEHAVIOR	PROCESS AND ATTRIBUTES	TARGET	EVENT ATTRIBUTES
🌐	29-Jan-2024 18:10:45		ANDREYTXP	Socket Close		SYSTEM ✓ 32 bit	10.51.103.15:59...	SOURCE PID 4 LOCAL ADDRESS 0.0.0.0:0 REMOTE ADDRESS 10.51.103.15:59603
🌐	29-Jan-2024 18:10:45		ANDREYTXP	Socket Accept		SYSTEM ✓ 32 bit	10.51.103.15:59...	SOURCE PID 4 LOCAL ADDRESS [0:0:0:0:0:0:0:0]:0 REMOTE ADDRESS 10.51.103.15:59603
	29-Jan-2024 18:14:39		ANDREYTXP	File Rename		wmiprvse.exe ✓ 32 bit	FrameWork.log	SOURCE PID 1752 PATH WINDOWS\system... HASH
🌐	29-Jan-2024 18:16:02		ANDREYTXP	Socket Close		SYSTEM ✓ 32 bit	10.51.103.15:59...	SOURCE PID 4 LOCAL ADDRESS 0.0.0.0:0 REMOTE ADDRESS 10.51.103.15:59612
🌐	29-Jan-2024 18:16:02		ANDREYTXP	Socket Accept		SYSTEM ✓ 32 bit	10.51.103.15:59...	SOURCE PID 4 LOCAL ADDRESS [0:0:0:0:0:0:0:0]:0 REMOTE ADDRESS 10.51.103.15:59612
🌐	29-Jan-2024 18:24:10		ANDREYTXP	Socket Close		SYSTEM ✓ 32 bit	10.51.103.15:59...	SOURCE PID 4 LOCAL ADDRESS 0.0.0.0:0 REMOTE ADDRESS 10.51.103.15:59621
🌐	29-Jan-2024 18:24:10		ANDREYTXP	Socket Accept		SYSTEM ✓ 32 bit	10.51.103.15:59...	SOURCE PID 4 LOCAL ADDRESS [0:0:0:0:0:0:0:0]:0 REMOTE ADDRESS 10.51.103.15:59621
	29-Jan-2024 18:25:09		ANDREYTXP	Value Read		svchost.exe ✓ 32 bit		SOURCE PID 1296 REGISTRY PATH HKLM\SOFTWARE\Classes\CLSID\{304CE...

- Filters on page 126
- Facets on page 138
- Activity events tables on page 141
- Details pane on page 145
- Investigation View on page 155
- Exporting threat hunting logs on page 166

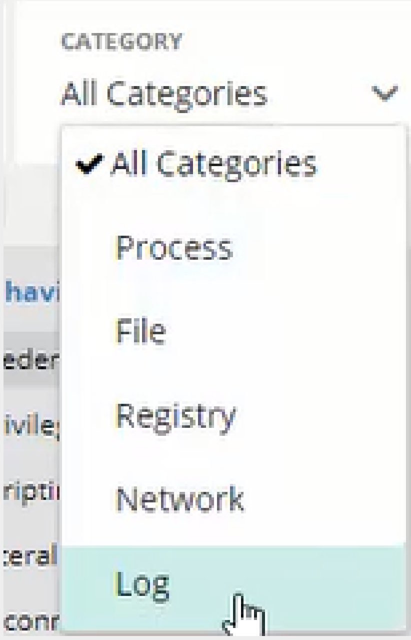
Filters

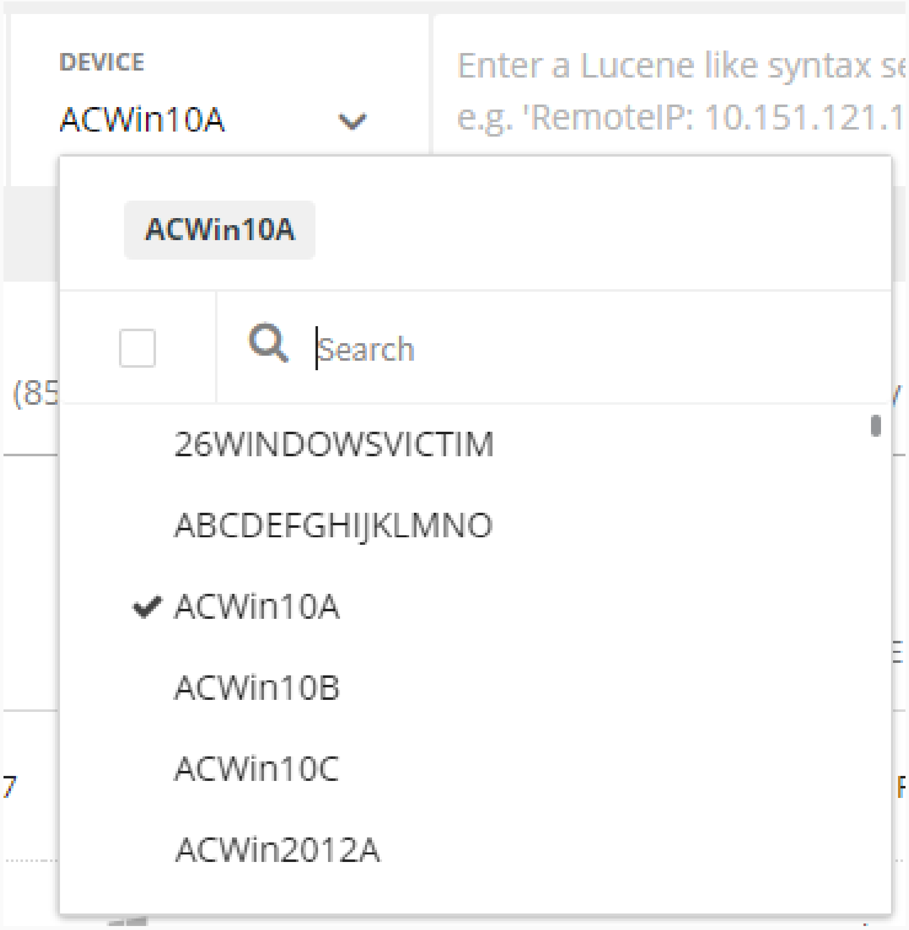
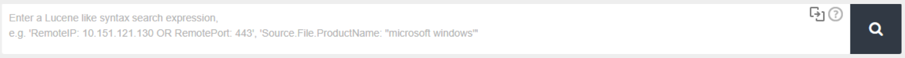
The Filters area enables you to define a query that filters the activity events to display in the result tables. It comprises the following filters:

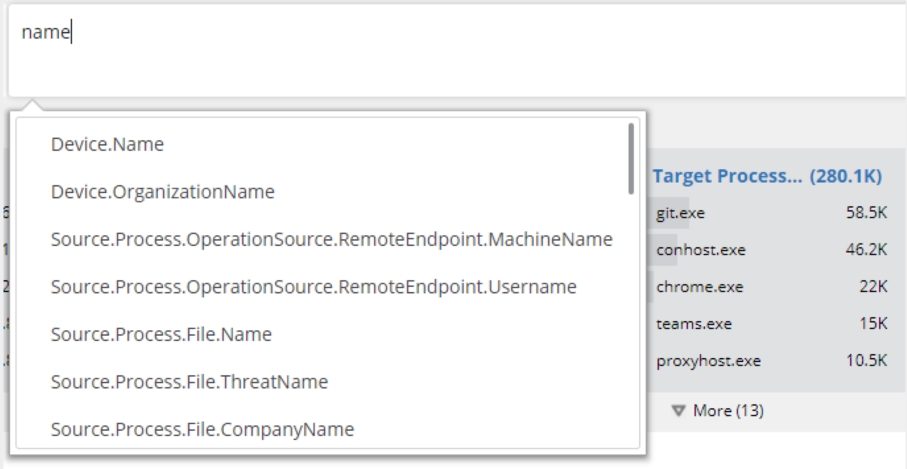


CATEGORY: All Categories
DEVICE: All Devices
Enter a Lucene like syntax search expression,
e.g. 'RemoteIP: 10.151.121.130 OR RemotePort: 443', 'Source.File.ProductName: "microsoft windows"'
TIME: Last hour

This area also enables you to save queries and to redisplay saved queries, as described in Saving queries and saved queries on page 131.

Filter	Description
Category	The *Category* filter enables you to filter the activity events by their category.  CATEGORY All Categories ✓ All Categories Process File Registry Network Log
Device	The *Device* filter enables you to filter by a specific device[s].

Filter	Description
	 DEVICE ACWin10A Enter a Lucene like syntax se e.g. 'RemoteIP: 10.151.121.1 ACWin10A Search 26WINDOWSVICTIM ABCDEFGHIJKLMNO ✓ ACWin10A ACWin10B ACWin10C ACWin2012A
Free-text Query	This filter enables you to specify a free-text Lucene-syntax query to filter the results. You can also convert STIX JSON and STIX XML syntax queries into Lucene syntax using the *Convert Query* button.  Enter a Lucene like syntax search expression, e.g. 'RemoteIP: 10.151.121.130 OR RemotePort: 443', 'Source.File.ProductName: "microsoft windows"' For Lucene-syntax queries, to simplify definition, the free-text query filter has an auto-complete helper dropdown list that contains all the available activity event fields, as well as available syntax operators. Simply start typing to see a dropdown menu of options. The automatic-complete helper guides you through the process of creating a query by displaying appropriate options in the dropdown menus, such as fields and operators when appropriate.

<table>
<tr><th>Filter</th><th>Description</th></tr>
<tr><td></td><td>


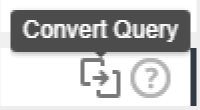
name

Device.Name
Device.OrganizationName
Source.Process.OperationSource.RemoteEndpoint.MachineName
Source.Process.OperationSource.RemoteEndpoint.Username
Source.Process.File.Name
Source.Process.File.ThreatName
Source.Process.File.CompanyName
More (13)

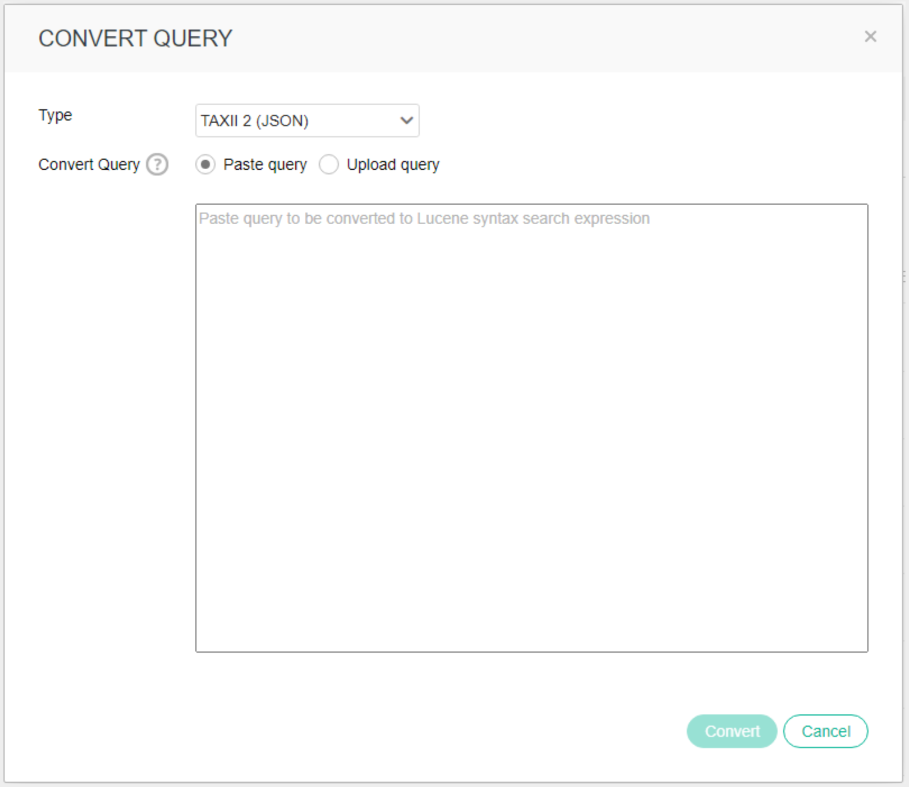
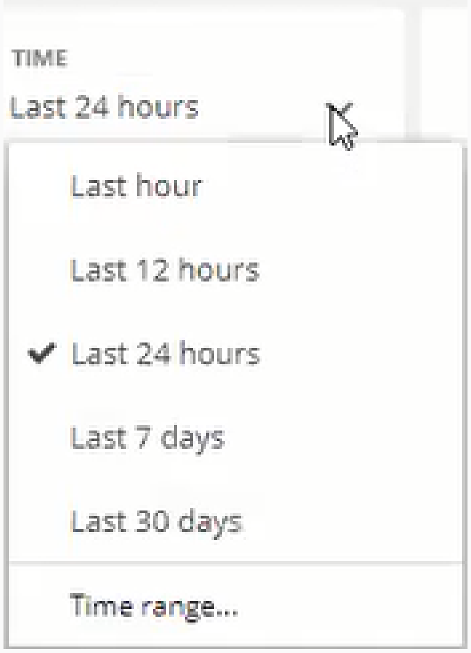
Target Process... (280.1K)

git.exe 58.5K
conhost.exe 46.2K
chrome.exe 22K
teams.exe 15K
proxyhost.exe 10.5K

For JSON and XML syntax queries, use the <i>Convert Query</i> button to convert the query into Lucene syntax.



You can then select the file type and paste the query or upload a JSON or XML file in the <i>CONVERT QUERY</i> window. The following indicators are supported and will be translated into Lucene syntax: hashes, file names, files size, paths, IPs, usernames, registry keys, URLs and domain names.
</td></tr>
</table>

Filter	Description
	 CONVERT QUERY Type: TAXII 2 (JSON) Convert Query: ● Paste query ○ Upload query Paste query to be converted to Lucene syntax search expression
Time	The *Time* filter enables you to filter for a specific time period. The default is the last hour.  TIME: Last 24 hours Last hour Last 12 hours ✓ Last 24 hours Last 7 days Last 30 days Time range...

Filter	Description
	When you run a Threat Hunting query with a *Time* filter, the response time can vary depending on the period and the amount of collected data. When the time is set to *Last 30 days*, the query can run for a few minutes.

To clear the contents of all the filters in the *Filters* area, at the far right of the page, click the eclipsis icon (⋮) and select *Clear all*.

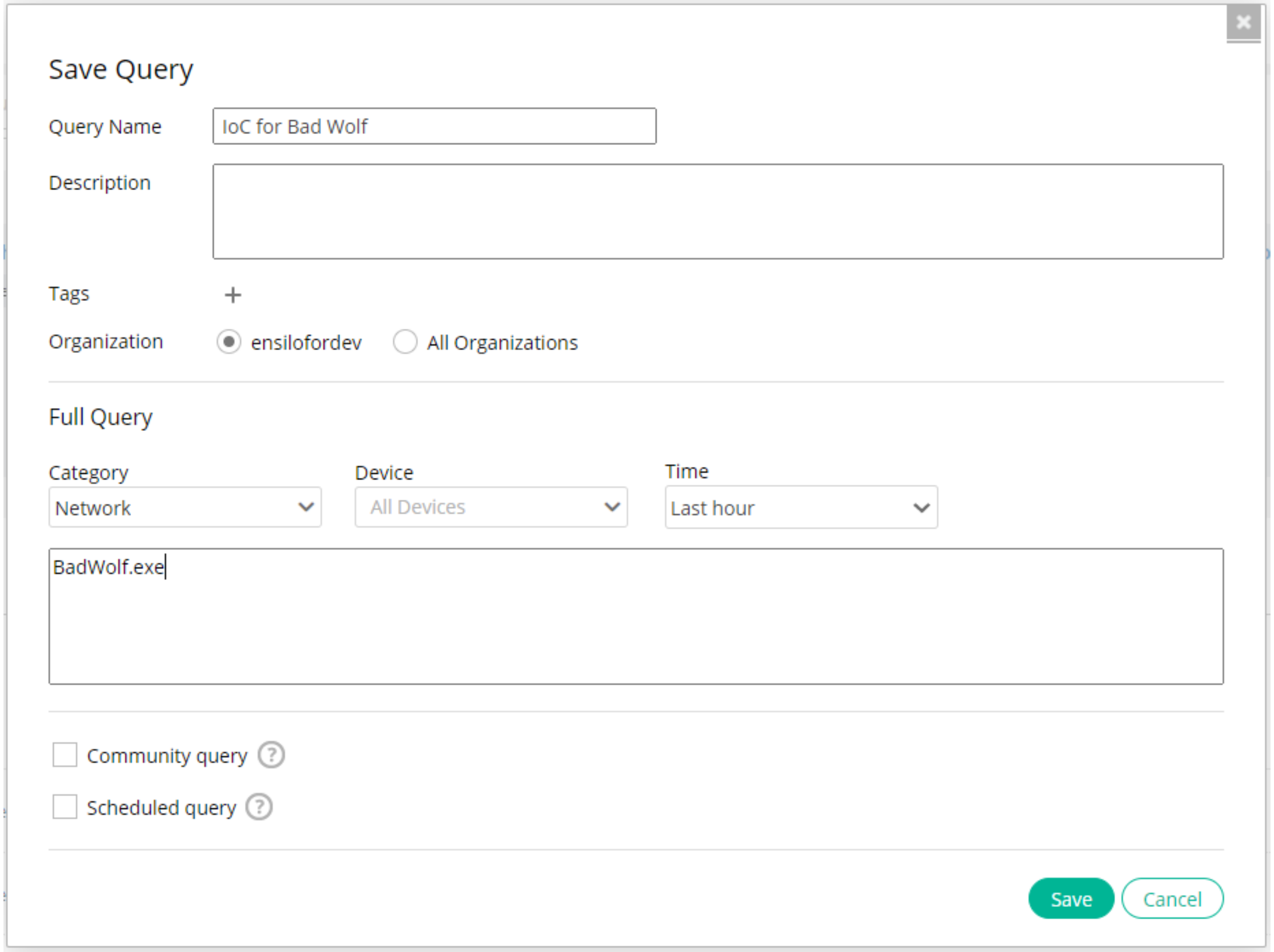
Saving queries and saved queries

After filtering the activity events displayed in the result tables, you can save the query to be redisplayed when needed. Saving a query in this manner also enables you to define it as a scheduled query in order to automate the process of threat detection.

Out-of-the-box queries, provided by Fortinet, are marked with the logo FORTINET. You can change the scheduling of a query defined by Fortinet and/or disable the execution of a query. However, the query itself and its name cannot be edited. If you need to edit one of the Fortinet-defined queries, copy the query itself and paste it in a newly created query. In this case, it is recommended to disable the original Fortinet-defined query.

To save a query:

1. Use the filters to display the desired filtered events in the result tables.
2. In the Filters area, at the far right of the page, click the ⋮ button and select *Save Query*. The following displays populated with the current filter definitions. The *Category*, *Device*, and *Time* dropdown menus show the filter selections and the box underneath it shows the actual query string. For example, as shown below:



Save Query

Query Name: IoC for Bad Wolf

Description:

Tags +

Organization ● ensilofordev ○ All Organizations

Full Query

Category: Network

Device: All Devices

Time: Last hour

BadWolf.exe

□ Community query ?

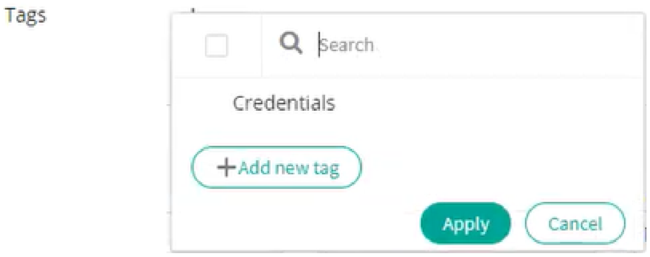
□ Scheduled query ?

3. Fill in or modify the definitions of this saved query, as follows:
   - *Query Name*: Enter any free text name describing this query.
   - *Description*: Enter any free text description of this query.
   - *Tags*: Enables you to assign one or more metadata tags to this query. You can assign a previously defined tag to this query or define a new tag. These tags can then be used for general information purposes and for searching through queries in the *Incidents* tab.

     These tags only relate to saved queries.

     Tags +

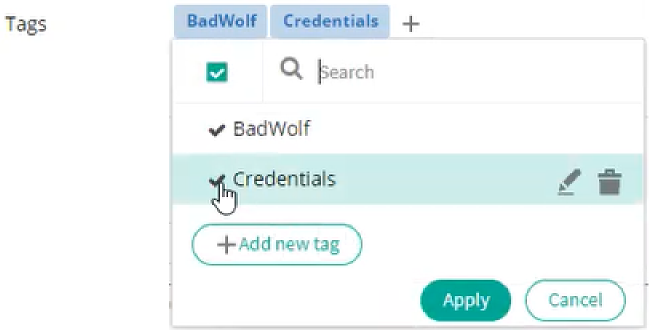
     Click the *Add* button to assign tag(s) to this query. The following displays:



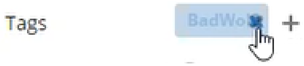
All previously defined tags (for any query in your organization) are listed for your selection.

If this tag is assigned to this query, a checkmark appears on its left: ✓ Credentials .

To assign a tag to this query, simply click on it. It will then show the checkmark to its left. Each tag that you assign appears as an icon, as follows:



To unassigned a tag from a query, click on it in the list so that its checkmark is removed or hover over it to display a *Cancel* button (X) and then click the *Cancel* button (X) to delete it, as shown below:



To create a new tag, click the *+ Add new tag* button.

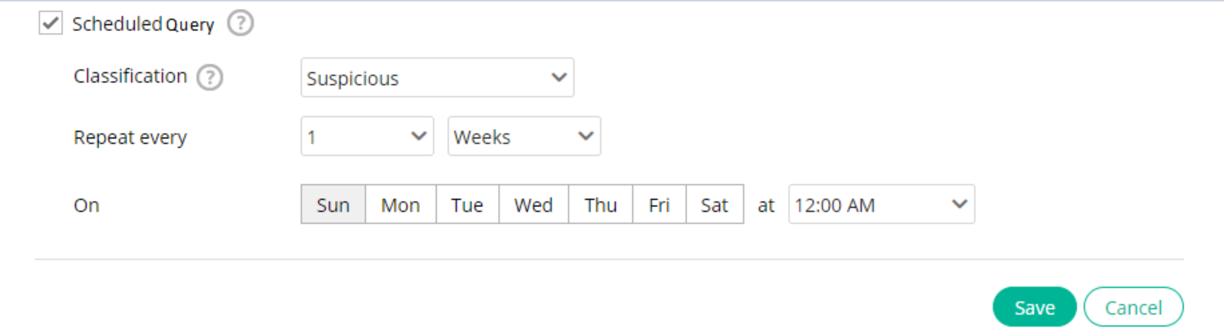
To modify the name of the tag or to delete it from the list (and from all queries to which it was assigned previously in the organization(s) of the logged in user), hover over it and click the *Edit* or *Delete* icon, as needed.

Click the *Apply* button to assign all the selected tags (with checkmarks) to this query.

- *Organization*: Specifies the name of the organization in a multi-organization FortiEDR environment when the logged in user has a Hoster role. In a single-organization FortiEDR system, this field does not appear.
- The *Category, Device and Time* dropdown menus show the filter selections and enable you to modify the selection.
- *Query String Box*: Displays the actual query string according to the selections made above and enables you to modify it.
- *Community Query*: Select this option to specify that it is shared with the entire FortiEDR community including other organizations.

After you have defined a Community Query and saved it, you can edit it. Unchecking the Community Query option means that this query is no longer available to the FortiEDR community. If however, a community member already copied this query, they will still have it, even after you unshare it here.

- *Scheduled Query*: Mark this option to automate the process of detecting threats so that this query is run automatically according to the schedule that you define. A security event is automatically created in the *Incidents* tab upon detecting threats (query matches). Notifications are sent according to the security event's definition, such as via email, Syslog and so on. You can also configure playbook actions for the triggered security events from the scheduled query.
  Enabling this checkbox shows the following options:



☑ Scheduled Query

Classification: Suspicious

Repeat every: 1 Weeks

On: Sun Mon Tue Wed Thu Fri Sat at 12:00 AM

The time range of the activity events that this query matches is determined by the frequency of the schedule. For example, if you define that the query automatically runs once a week, then each time it runs, it will match and create a security event for all the activity events in the most recent week; the same goes for it being scheduled once a month – in this case, the query will match all the activity events in the most recent month.

Define the scheduled query, as follows:

Field	Definition
Classification	Select the classification of the Security Event to be issued when the scheduled query has run and found matches. The Classification specifies how malicious the security event is, if at all. Classifications are initially determined by FortiEDR automatically or manually and are shown in the *Incidents* tab, as described in Overview on page 90. They can be: • Malicious • Suspicious • Inconclusive • Likely Safe • PUP (Potentially Unwanted Program) • Safe
Repeat Every/On	These options enable you to define the frequency and schedule when this query will be run. For example, to repeat the query every week on Sunday, make the selections shown in the screen above.
Trigger Playbook Actions	Specifies whether to allow FortiEDR to trigger the corresponding Playbook action of the triggered security event from the scheduled query. Enabling this checkbox allows FortiEDR to automatically apply the action of the Playbook that is assigned to the Collector Group the triggering device belongs to. Configure the following options:

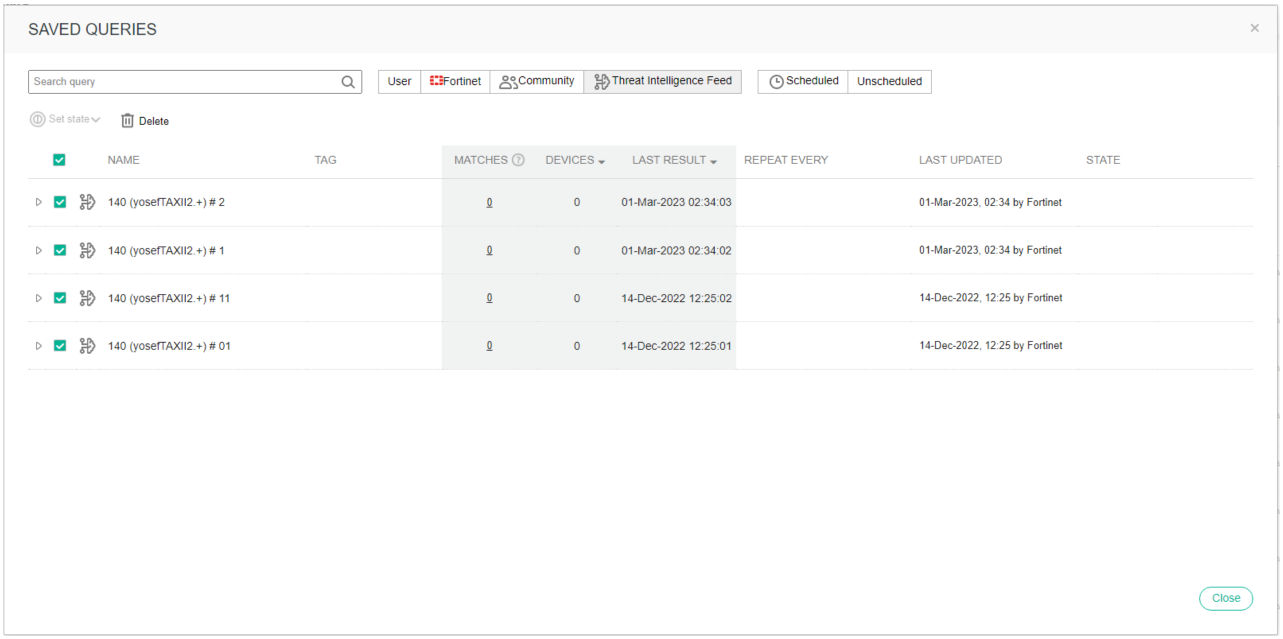
Field	Definition
	• *Terminate Process*—Specifies which process in the Activity Event, which resulted from the execution of the saved query, should be terminated: • *Source Process* • *Source Process Parent* • *Target Process* • *Delete File*—Specifies which file in the Activity Event, which resulted from the execution of the saved query, should be deleted: • *Source Process File* • *Target File* • *Target Process File* • *Target Executable Image File*

4. Click *Save* to save this query so that it is available to be redisplayed, as described below. The system runs the query immediately in order to verify that it is functional.

> If the system detects a large quantity of events about which to send notifications, then a warning message is displayed suggesting that you refine the query so that there are fewer matches. The reason being that extremely large quantities of notifications may be more of a hindrance than a help.

To display a saved query:

1. In the *Filters* area, at the far right of the page, click the eclipsis icon (⋮) and select *Saved Queries*. The following displays listing all the queries that were saved using the *Save Query* option.



SAVED QUERIES

Search query

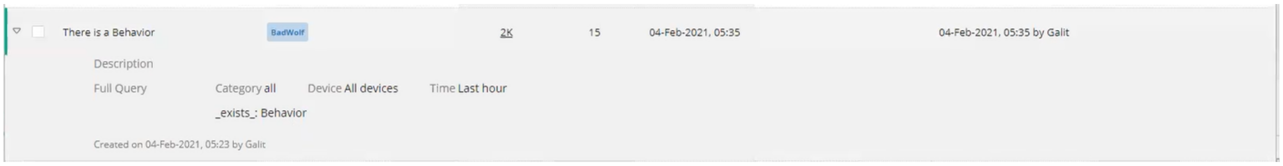
User | Fortinet | Community | Threat Intelligence Feed | Scheduled | Unscheduled

Set state | Delete

☑	NAME	TAG	MATCHES	DEVICES	LAST RESULT	REPEAT EVERY	LAST UPDATED	STATE
☑	140 (yosefTAXII2.+) # 2		0	0	01-Mar-2023 02:34:03		01-Mar-2023, 02:34 by Fortinet	
☑	140 (yosefTAXII2.+) # 1		0	0	01-Mar-2023 02:34:02		01-Mar-2023, 02:34 by Fortinet	
☑	140 (yosefTAXII2.+) # 11		0	0	14-Dec-2022 12:25:02		14-Dec-2022, 12:25 by Fortinet	
☑	140 (yosefTAXII2.+) # 01		0	0	14-Dec-2022 12:25:01		14-Dec-2022, 12:25 by Fortinet	

For each saved query, this list shows the quantity of matches detected (*MATCHES*), the quantity of devices on which these matches were detected and the last time the query was run (*LAST RESULT*). These three columns are highlighted in gray, as shown above. Additional details about the queries definition are also displayed in each row. Out-of-the-box queries, provided by Fortinet, are marked with the Fortinet logo FORTINET .

2. Click on the row of a saved query to display additional details about that query's most recent run. For example, as shown below:



▽ □ There is a Behavior BadWolf 2K 15 04-Feb-2021, 05:35 04-Feb-2021, 05:35 by Galit

Description

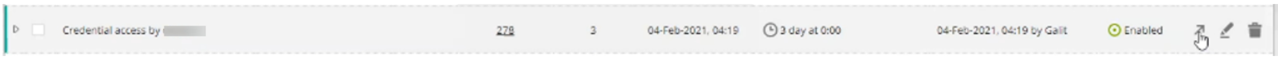
Full Query Category all Device All devices Time Last hour

exists: Behavior

Created on 04-Feb-2021, 05:23 by Galit

3. You can filter this list of saved queries by typing into the *Search* field and/or selecting one of the following options:
   a. FORTINET /*User*: To select FORTINET defined queries. Selecting *User* filters by saved queries that were created by a user.
   b. *Community/User*: To specify that Community Queries are listed in this window, click the *Community* option. A Community Query is one whose Community Query field was marked when it was created/modified. 👥 appears in the list next to *Community Queries*. *User* refers to queries that are not Community Queries, meaning that each one is only available to the Organization for which it was created.
   c. *Threat Intelligence Feed*: To specify that Threat Intelligence queries are listed in this window, click the *Threat Intelligence Feed* option. Upon each retrieval of Threat Intelligence Collection data, one or multiple queries with the name *Collection ID/Name (Connector Name) #x* are created by the Threat Intelligence Feed connector that you configure under *Administration -> Connectors*. As one Threat Hunting query can include only 150 to 1000 conditions, depending on the indicator type, FortiEDR may create multiple Threat Intelligence query entries for the same Collection.
   d. *Scheduled/Unscheduled*: To specify that Scheduled Queries are listed in this window, click the *Scheduled* option. A Scheduled Query is one with the *Scheduled Query* field marked when it was created/modified.

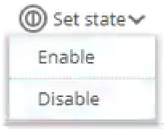
4. You can modify a saved query by hovering over it. The following tools are displayed on the right of the row:



▷ □ Credential access by [redacted] 278 3 04-Feb-2021, 04:19 3 day at 0:00 04-Feb-2021, 04:19 by Galit Enabled

Tool	Definition
Run Now ↗	To run and detect activity events now according to this saved query.
Edit ✎	To edit the *Saved Query* definition.
Delete 🗑	To delete the saved query. Multiple queries can be deleted at once by marking the checkboxes on the left side of each row and then clicking the *Delete* 🗑 icon at the top of the window.

5. To enable/disable a saved query, mark the checkboxes on the left side of the relevant rows and select the *Enable/Disable* option in the *Set State* dropdown menu.

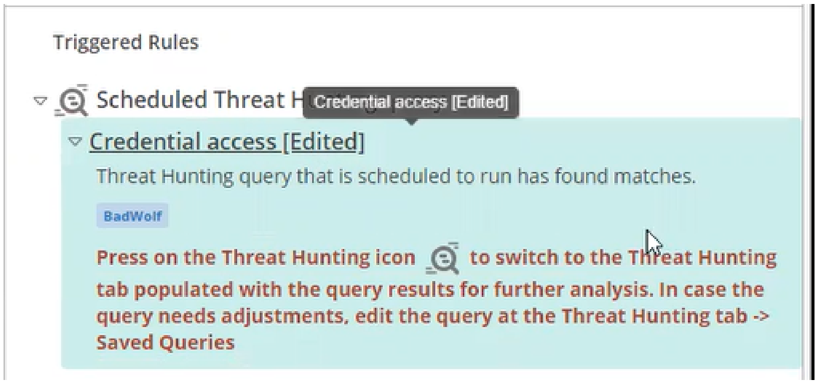


Scheduled queries

Scheduled queries enable you to automate the process of detecting threats so that it is activated automatically according to the schedule that you define. This will enable timely and continuous detection and notification of threats. A scheduled query runs automatically when you define a query as a scheduled query, as described below. Each time it runs and detects a match, it generates a security event in the *Incidents* tab, and sends a notification (via email, Syslog and so on) according to the security event's definition.

The security event that is generated by a scheduled query in the *Incidents* tab is similar to a standard security event, except for the following:

- The *Create Exception* () button is not available as you cannot define an exception for saved query security events.
- In the Process View of the *Incidents* tab, a saved query security event shows the name of the saved query instead of the process name.
  The classification (in the *CLASSIFICATION* column) is determined by the definition of the saved query.
  In the same manner as other security events it indicates the quantity of devices (in the *DEVICE* column) on which this type of activity events were found. All other aspects of a saved query security event are the same as other security events.
- Clicking the *Threat Hunting* option on the right side of the saved query security event in the *Incidents* tab displays the *Threat Hunting* tab and the saved query that was run, because that is what triggered the security event.
- The *Incidents* tab does not show any advanced data for a saved query security event.
- *Triggered Rules*: When a saved query security event is selected in the *Incidents* tab, the *Triggered Rules* pane on the bottom right of the page indicates that this security event was triggered by a *Scheduled Threat Hunting Query*, as shown below:
  The name of the saved query is listed below it. Click that saved query's name (for example, *Credential Access (Edited)*) to display additional details about this saved query, such as its description and the tags that were defined when it was created/modified, as shown below:



Credential access [Edited]

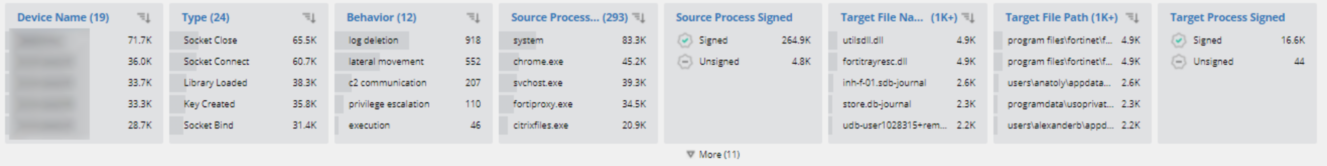
Threat Hunting query that is scheduled to run has found matches.

Press on the Threat Hunting icon to switch to the Threat Hunting tab populated with the query results for further analysis. In case the query needs adjustments, edit the query at the Threat Hunting tab -> Saved Queries

- In the *Device View* of the *Incidents* tab, a saved query security event appears under the devices that were affected. It also shows the name of the saved query instead of the process name.
  If this security event was triggered for more than 100 devices, then this row shows a notification indicating that they are not all listed here and that you can use the *Threat Hunting* option on the right of this event's row to investigate further.

Facets

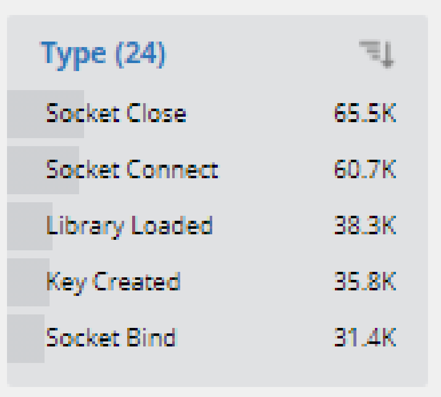
As expected, the continuous, realtime collection of Threat Hunting data produces numerous activity events. The sheer volume of activity data makes working directly with these activity events almost unmanageable. Therefore, FortiEDR uses facets to summarize the data displayed in the results tables. Facets are predefined in FortiEDR and represent the same data that is displayed in the results tables, but in an aggregated form. As such, facets represent the aggregation of the values in the results tables.



Device Name (19)		Type (24)		Behavior (12)		Source Process... (293)		Source Process Signed		Target File Na... (1K+)		Target File Path (1K+)		Target Process Signed	
[redacted]	71.7K	Socket Close	65.5K	log deletion	918	system	83.3K	Signed	264.9K	utilsdll.dll	4.9K	program files\fortinet\f...	4.9K	Signed	16.6K
[redacted]	36.0K	Socket Connect	60.7K	lateral movement	552	chrome.exe	45.2K	Unsigned	4.8K	fortitrayresc.dll	4.9K	program files\fortinet\f...	4.9K	Unsigned	44
[redacted]	33.7K	Library Loaded	38.3K	c2 communication	207	svchost.exe	39.3K			inh-f-01.sdb-journal	2.6K	users\anatoly\appdata...	2.6K		
[redacted]	33.3K	Key Created	35.8K	privilege escalation	110	fortiproxy.exe	34.5K			store.db-journal	2.3K	programdata\usoprivat...	2.3K		
[redacted]	28.7K	Socket Bind	31.4K	execution	46	citrixfiles.exe	20.9K			udb-user1028315+rem...	2.2K	users\alexanderb\appd...	2.2K		

Each individual facet pane summarizes the top five items for that facet. For example, in the *Type* (action) facet below, the facet lists the top five actions, based on the filters applied in the query. The number at the top in parentheses () indicates the total number of different values for this facet in the results table, in this case 24. In this case, the top five actions are *Socket Close*, *Socket Connect*, *Library Loaded*, *Key created*, and *Socket ind*.

Facet can show the bottom five instead of the top five. In order to switch from the top five to the bottom five for this specific facet, click on the arrow on the right side of the number ⇊.

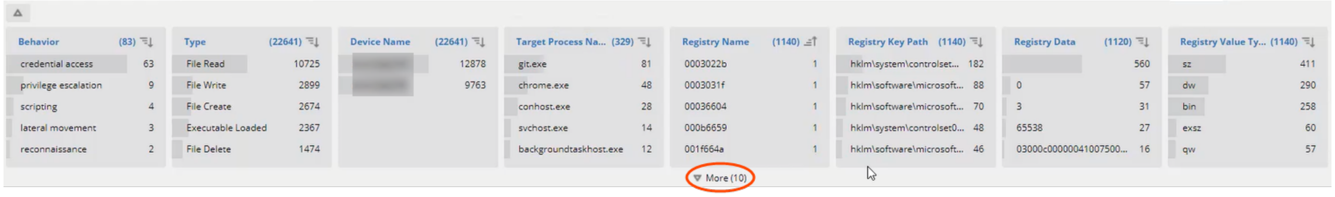


Type (24)	
Socket Close	65.5K
Socket Connect	60.7K
Library Loaded	38.3K
Key Created	35.8K
Socket Bind	31.4K

The filters applied in the *Filters* area affect the results displayed in the *Facets* and *Results Tables* areas.

The displayed facets vary according to the filters used in the *Filters* area.

You can click the *More* link to display additional facets.



△

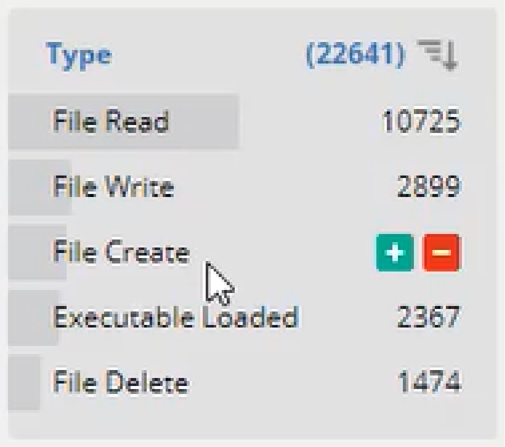
Behavior	(83)	Type	(22641)	Device Name	(22641)	Target Process Na...	(329)	Registry Name	(1140)	Registry Key Path	(1140)	Registry Data	(1120)	Registry Value Ty...	(1140)
credential access	63	File Read	10725	[redacted]	12878	git.exe	81	0003022b	1	hklm\system\controlset...	182		560	sz	411
privilege escalation	9	File Write	2899	[redacted]	9763	chrome.exe	48	0003031f	1	hklm\software\microsoft...	88	0	57	dw	290
scripting	4	File Create	2674			conhost.exe	28	00036604	1	hklm\software\microsoft...	70	3	31	bin	258
lateral movement	3	Executable Loaded	2367			svchost.exe	14	000b6659	1	hklm\system\controlset0...	48	65538	27	exsz	60
reconnaissance	2	File Delete	1474			backgroundtaskhost.exe	12	001f664a	1	hklm\software\microsoft...	46	03000c00000041007500...	16	qw	57

▽ More (10)

You can click the ▲ button to minimize the *Facets* area.

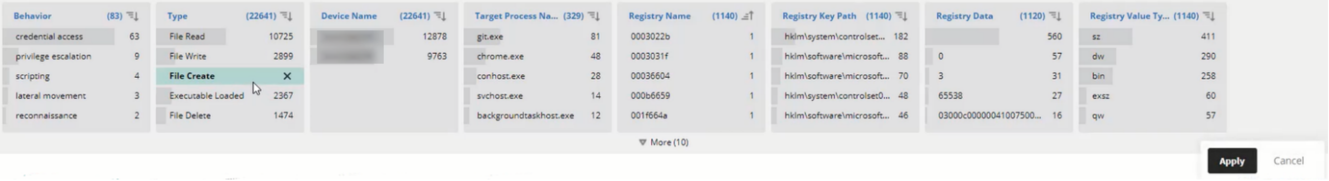
Filtering using facets

Facets provide an easy-to-use mechanism to aggregate the results in the *Activity Events* tables. In addition, you can also further narrow the results in the *Activity Events* table directly from the facets by including or excluding specific values. For example, when you hover over an item in a facet pane, a green and red button appear in its row. Click the green plus + button to include that item as a filter or click the red minus − button to exclude that item as a filter.



Type	(22641)
File Read	10725
File Write	2899
File Create	+ −
Executable Loaded	2367
File Delete	1474

Then, click the *Apply* button.



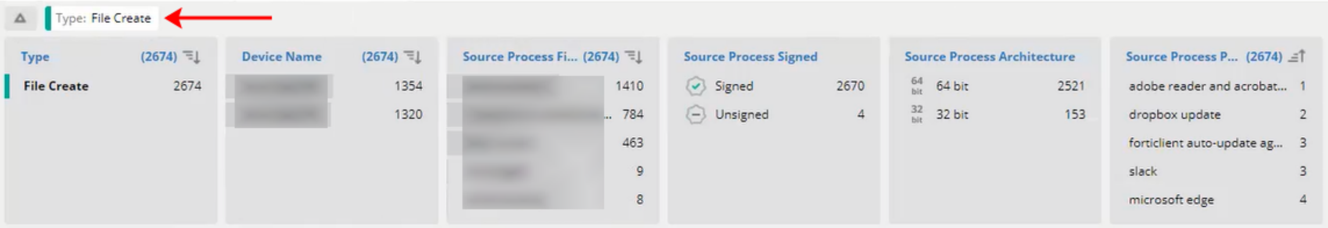
Behavior	(83)	Type	(22641)	Device Name	(22641)	Target Process Na...	(329)	Registry Name	(1140)	Registry Key Path	(1140)	Registry Data	(1120)	Registry Value Ty...	(1140)
credential access	63	File Read	10725	[redacted]	12878	git.exe	81	0003022b	1	hklm\system\controlset...	182		560	sz	411
privilege escalation	9	File Write	2899	[redacted]	9763	chrome.exe	48	0003031f	1	hklm\software\microsoft...	88	0	57	dw	290
scripting	4	File Create	×			conhost.exe	28	00036604	1	hklm\software\microsoft...	70	3	31	bin	258
lateral movement	3	Executable Loaded	2367			svchost.exe	14	000b6659	1	hklm\system\controlset0...	48	65538	27	exsz	60
reconnaissance	2	File Delete	1474			backgroundtaskhost.exe	12	001f664a	1	hklm\software\microsoft...	46	03000c00000041007500...	16	qw	57

▽ More (10)

Apply Cancel

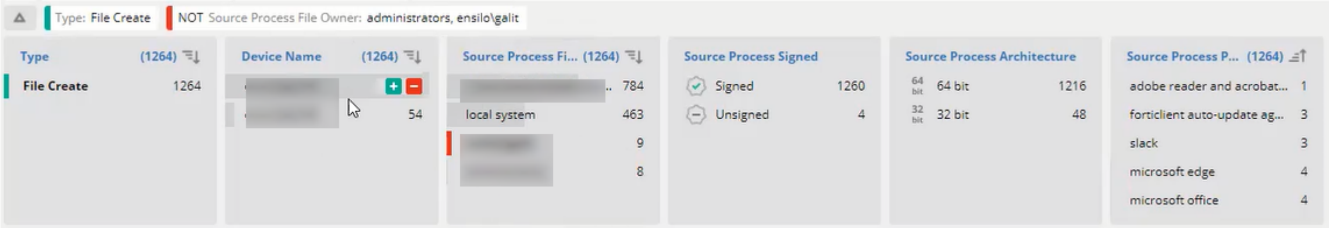
An item highlighted in green File Create ✕ indicates that it has been marked as an inclusion filter, but has not yet been applied by clicking the *Apply* button. An item highlighted in red ✓ Signed 2670 indicates that it has been marked as an exclusion filter, but has not yet been applied by clicking *Apply*.

Clicking the *Apply* button applies the additional filtering criteria to the threat hunting query. In addition, it creates a *chip* (indicated by the arrow in the following picture), which represents that additional filter and displays it at the top of the Facets area. In the example below, the query has been further filtered to only show the *File Create* type of action. Each chip is also part of the threat hunting query.



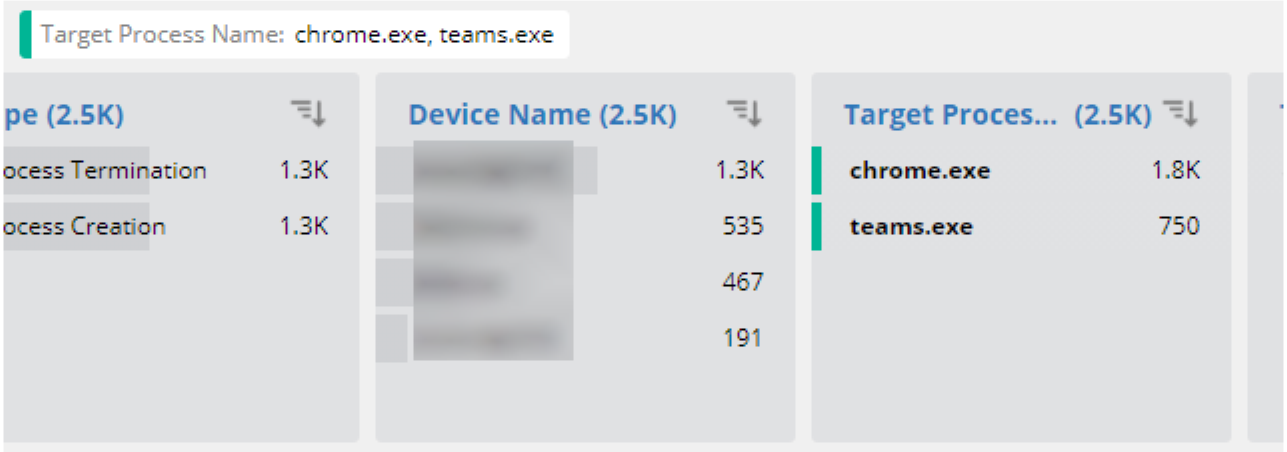
Each chip has either a green or red border on its left side to indicate whether it was defined to include (green) or exclude (red) that item in the filter.

Each Facet pane may have a green or red left border to indicate whether it has been applied in the query, meaning that the displayed results are filtered by it.

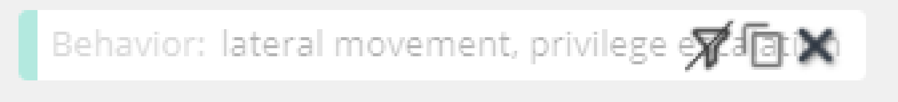

Type: File Create
NOT Source Process File Owner: administrators, ensilo\galit
Type (1264)
File Create 1264
Device Name (1264)
54
Source Process Fi... (1264)
784
local system 463
9
8
Source Process Signed
Signed 1260
Unsigned 4
Source Process Architecture
64 bit 1216
32 bit 48
Source Process P... (1264)
adobe reader and acrobat... 1
forticlient auto-update ag... 3
slack 3
microsoft edge 4
microsoft office 4

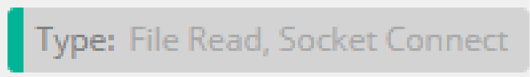
You can define an unlimited number of chip filters, with an AND relationship between multiple filters. Each facet can create up to two chips, one for the inclusion of values and one for the exclusion of values.

If two values have been added to the query from the same *Facet* pane, the relationship between the values in the chip is OR. The following example shows that the query includes activity events in which their *Target Process Name* is either `chrome.exe` or `teams.exe`, which is shown below in both the chip and in the facet.



Hovering over a chip enables you to remove, disable or copy it, as follows:

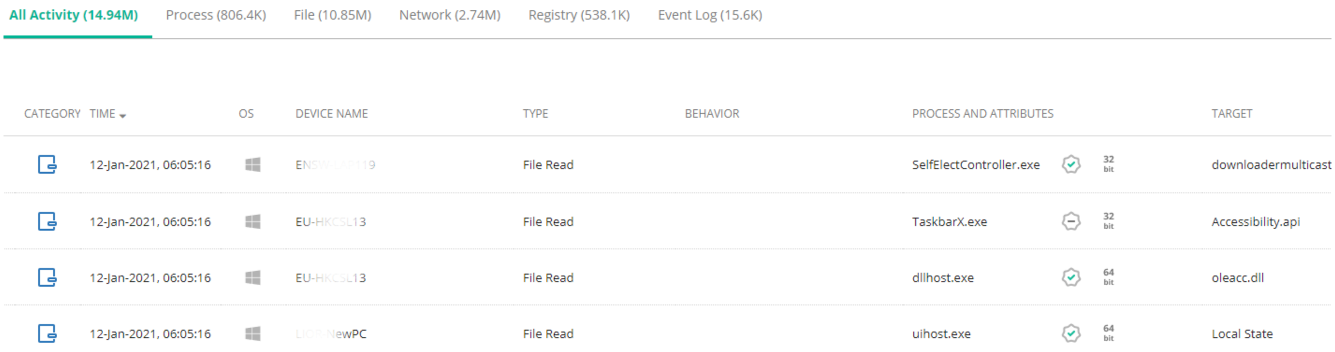


Tool	Definition
Remove	The chip is removed and the Facets and Result tables are updated accordingly.
Disable	A disabled chip no longer affects the results. The Facets and the Results tabs are updated as if the chip was removed and the chip appears as follows:  Type: File Read, Socket Connect
Copy	The chip content is copied to memory and can be pasted into the query for further editing.

In order to enable a disabled chip and update the results according to its criteria, click the *Enable* icon.

Activity events tables

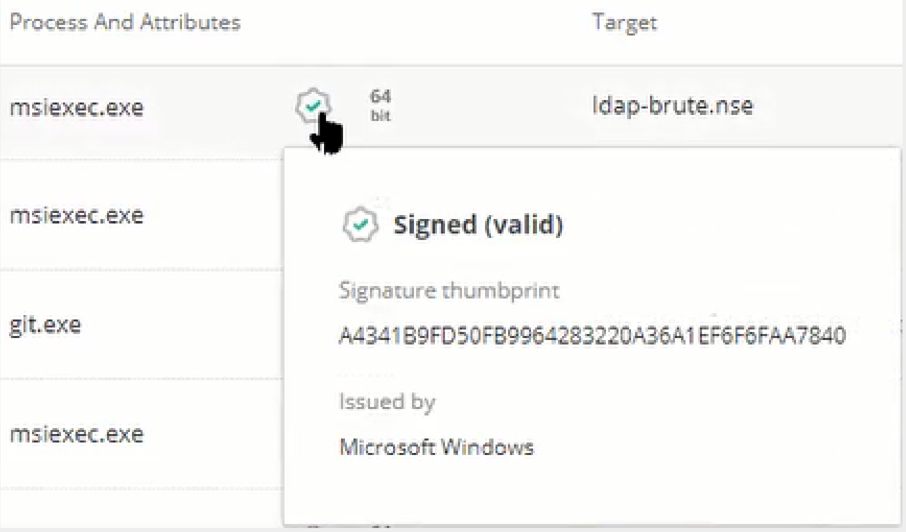
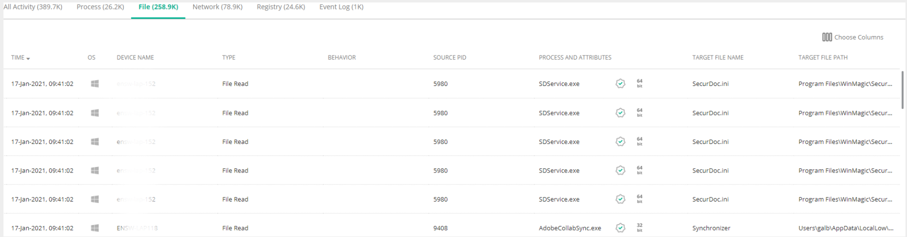
The results presented in the tables in this area are activity events. The activity events table area contains six tabs, each representing one category of activity events, as follows:



All Activity (14.94M) Process (806.4K) File (10.85M) Network (2.74M) Registry (538.1K) Event Log (15.6K)

CATEGORY	TIME	OS	DEVICE NAME	TYPE	BEHAVIOR	PROCESS AND ATTRIBUTES	TARGET
	12-Jan-2021, 06:05:16		EN[redacted]19	File Read		SelfElectController.exe 32 bit	downloadermulticast
	12-Jan-2021, 06:05:16		EU-H[redacted]13	File Read		TaskbarX.exe 32 bit	Accessibility.api
	12-Jan-2021, 06:05:16		EU-H[redacted]13	File Read		dllhost.exe 64 bit	oleacc.dll
	12-Jan-2021, 06:05:16		[redacted]NewPC	File Read		uihost.exe 64 bit	Local State

Category	Definition
All Activity	This tab lists all activity events, based on the filters defined for the Threat Hunting query. The number in parentheses () specifies the total number of activity events, based on your query criteria. This total equals the sum of the activity events in the other five tabs. Each Category of activity events is represented by a different icon, as follows: • Process • File • Registry • Network

Category	Definition
	• 🗋 Log You can hover over the icon in the *Process and Attributes* column to temporarily display additional details about the source process, including whether it is signed, its signature, issuer and so on.  Process And Attributes Target msiexec.exe 64 bit ldap-brute.nse msiexec.exe git.exe msiexec.exe Signed (valid) Signature thumbprint A4341B9FD50FB9964283220A36A1EF6F6FAA7840 Issued by Microsoft Windows There are several types of attribute icons, such as Signed/Unsigned.
Process	This tab shows all matching activity events of category Process.
File	This tab shows all matching activity events of category File. 

All Activity (389.7K) Process (26.2K) **File (258.9K)** Network (78.9K) Registry (24.6K) Event Log (1K)

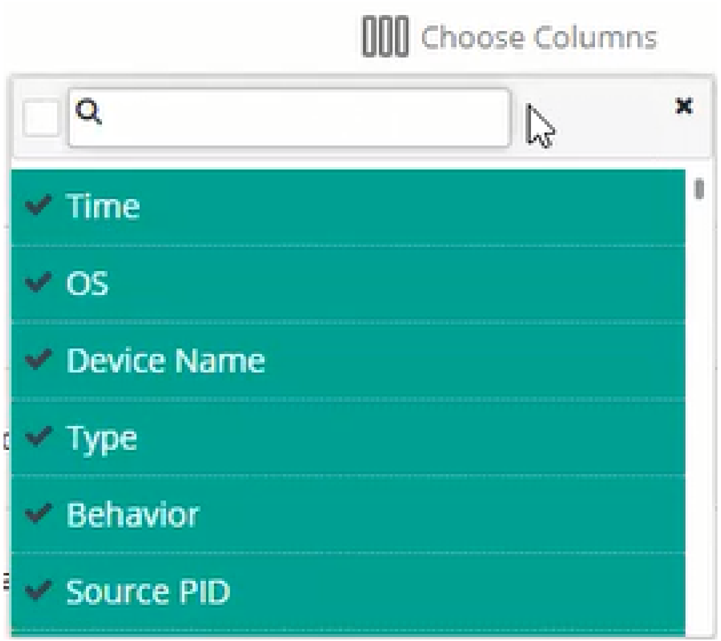
Choose Columns

TIME	OS	DEVICE NAME	TYPE	BEHAVIOR	SOURCE PID	PROCESS AND ATTRIBUTES	TARGET FILE NAME	TARGET FILE PATH
17-Jan-2021, 09:41:02	⊞	ensw-lap-152	File Read		5980	SDService.exe ✓ 64 bit	SecurDoc.ini	Program Files\WinMagic\Secur...
17-Jan-2021, 09:41:02	⊞	ensw-lap-152	File Read		5980	SDService.exe ✓ 64 bit	SecurDoc.ini	Program Files\WinMagic\Secur...
17-Jan-2021, 09:41:02	⊞	ensw-lap-152	File Read		5980	SDService.exe ✓ 64 bit	SecurDoc.ini	Program Files\WinMagic\Secur...
17-Jan-2021, 09:41:02	⊞	ensw-lap-152	File Read		5980	SDService.exe ✓ 64 bit	SecurDoc.ini	Program Files\WinMagic\Secur...
17-Jan-2021, 09:41:02	⊞	ensw-lap-152	File Read		5980	SDService.exe ✓ 64 bit	SecurDoc.ini	Program Files\WinMagic\Secur...
17-Jan-2021, 09:41:02	⊞	ENSW-LAP118	File Read		9408	AdobeCollabSync.exe ✓ 32 bit	Synchronizer	Users\galb\AppData\LocalLow\...

Category	Definition
Network	This tab shows all matching activity events of type Network.
Registry	This tab shows all matching activity events of type Registry.
Event Log	This tab shows all matching activity events of type Event Log.

Each table contains a row for each matching activity event and each table includes different columns according to the category.

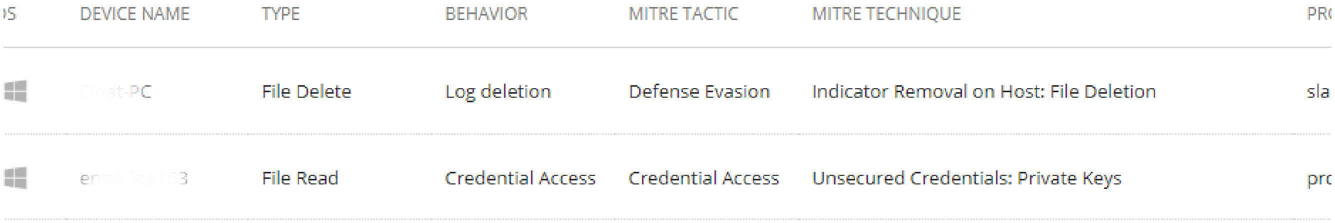
You can select which columns should appear in any of the tables using the *Choose Columns* option at the far right of the page. You can type in the *Search* box to help narrow the list of columns that display.



- ✓ Time
- ✓ OS
- ✓ Device Name
- ✓ Type
- ✓ Behavior
- ✓ Source PID

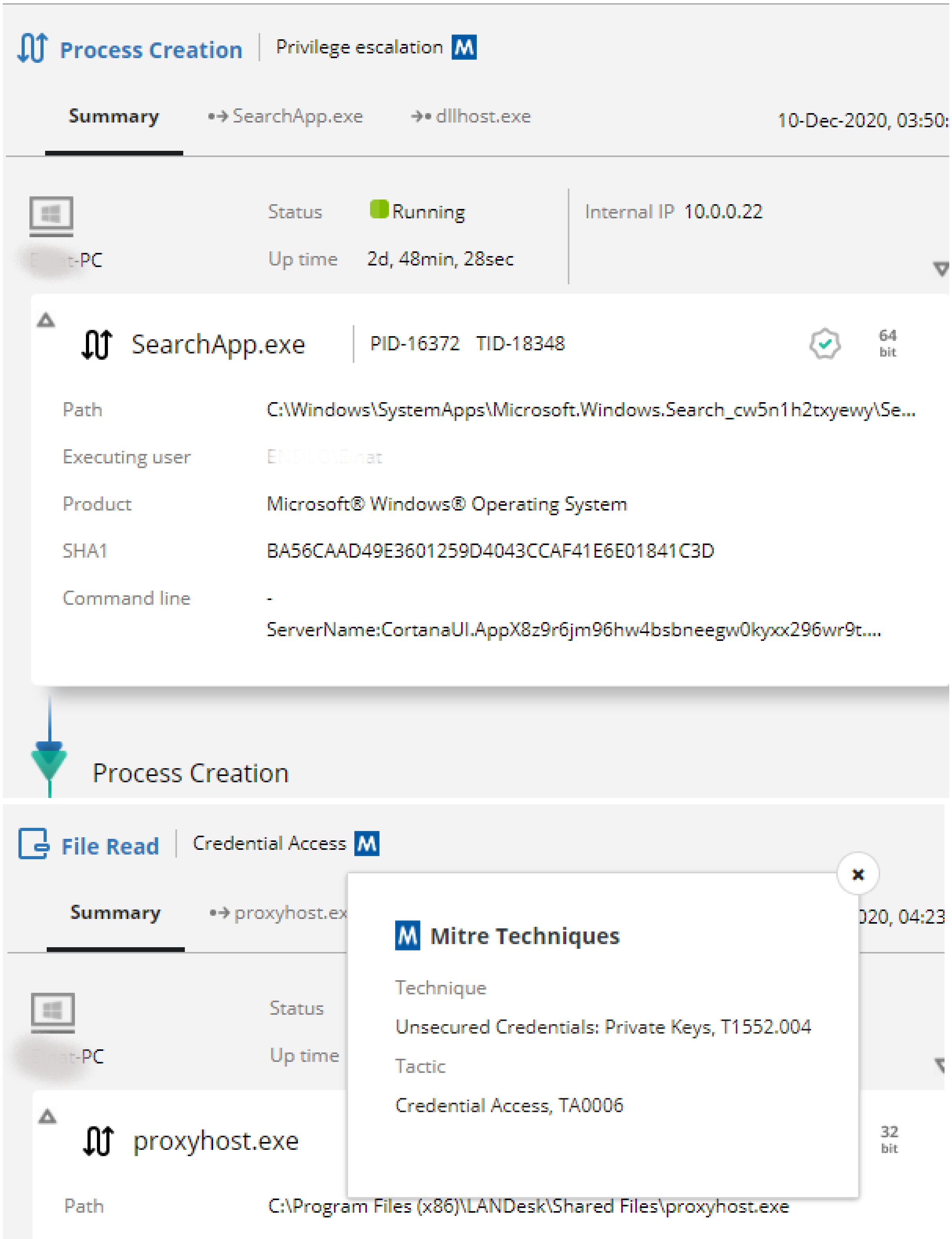
Each activity event may also be a part of a *behavior* and/or a MITRE Technique. A behavior indicates that this activity event is part of a specific behavior as determined by FortiEDR. A MITRE type (Technique or Tactic) indicates that the activity event is part of specification of a technique and tactic as classified by MITRE.

The activity events that have such behaviors and/or MITRE indications have values in the related columns in the activity events tables, as shown below:



S	DEVICE NAME	TYPE	BEHAVIOR	MITRE TACTIC	MITRE TECHNIQUE	PR
⊞	[redacted]	File Delete	Log deletion	Defense Evasion	Indicator Removal on Host: File Deletion	sla
⊞	[redacted]	File Read	Credential Access	Credential Access	Unsecured Credentials: Private Keys	prc

When an activity event has a related MITRE indication, it is indicated in the Details pane on page 145 (see below). You can hover over the associated icon to display more details.



Process Creation | Privilege escalation

Summary | SearchApp.exe | dllhost.exe | 10-Dec-2020, 03:50:

[redacted]-PC

Status: 🟩 Running

Up time: 2d, 48min, 28sec

Internal IP: 10.0.0.22

SearchApp.exe | PID-16372 TID-18348 | 64 bit

Path	C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\Se...
Executing user	[redacted]
Product	Microsoft® Windows® Operating System
SHA1	BA56CAAD49E3601259D4043CCAF41E6E01841C3D
Command line	- ServerName:CortanaUI.AppX8z9r6jm96hw4bsbneegw0kyxx296wr9t....

Process Creation

File Read | Credential Access

Summary | proxyhost.ex | 020, 04:23

[redacted]-PC

Status

Up time

proxyhost.exe | 32 bit

Path: C:\Program Files (x86)\LANDesk\Shared Files\proxyhost.exe

Mitre Techniques

Technique

Unsecured Credentials: Private Keys, T1552.004

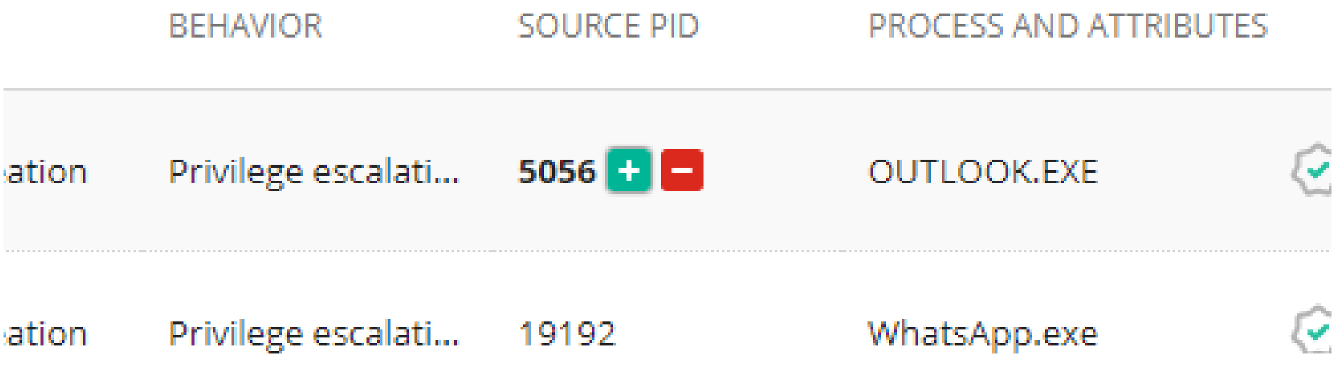
Tactic

Credential Access, TA0006

Filtering using activity events tables

The activity events tables area can be used to add filters to the query in a similar manner as facets.

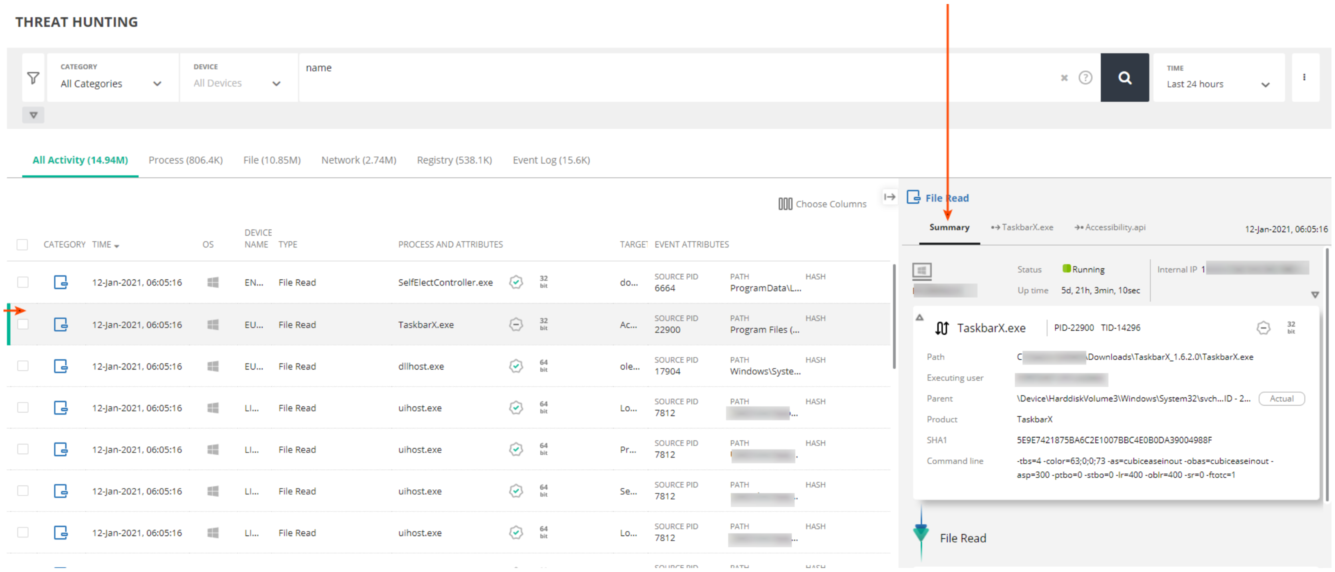
When you hover over an item in the table, a green and red button appear to its right. Click the green plus button (＋)to include that item as a filter or click the red minus button (−) to exclude that item as a filter. For more details, see Filtering using facets on page 139.



	BEHAVIOR	SOURCE PID	PROCESS AND ATTRIBUTES	
ation	Privilege escalati...	5056 ＋ −	OUTLOOK.EXE	✓
ation	Privilege escalati...	19192	WhatsApp.exe	✓

Details pane

You can click anywhere in a row in any of the Activity Events tables to display more details about the specific activity event in a Details pane on the right. The selected row is marked by a green border on its left.



THREAT HUNTING

CATEGORY: All Categories | DEVICE: All Devices | name | TIME: Last 24 hours

All Activity (14.94M) | Process (806.4K) | File (10.85M) | Network (2.74M) | Registry (538.1K) | Event Log (15.6K)

CATEGORY	TIME	OS	DEVICE NAME	TYPE	PROCESS AND ATTRIBUTES		TARGET	EVENT ATTRIBUTES		
	12-Jan-2021, 06:05:16		EN...	File Read	SelfElectController.exe	32 bit	do...	SOURCE PID 6664	PATH ProgramData\L...	HASH
	12-Jan-2021, 06:05:16		EU...	File Read	TaskbarX.exe	32 bit	Ac...	SOURCE PID 22900	PATH Program Files (...	HASH
	12-Jan-2021, 06:05:16		EU...	File Read	dllhost.exe	64 bit	ole...	SOURCE PID 17904	PATH Windows\Syste...	HASH
	12-Jan-2021, 06:05:16		LI...	File Read	uihost.exe	64 bit	Lo...	SOURCE PID 7812	PATH [redacted]...	HASH
	12-Jan-2021, 06:05:16		LI...	File Read	uihost.exe	64 bit	Pr...	SOURCE PID 7812	PATH [redacted].	HASH
	12-Jan-2021, 06:05:16		LI...	File Read	uihost.exe	64 bit	Se...	SOURCE PID 7812	PATH [redacted].	HASH
	12-Jan-2021, 06:05:16		LI...	File Read	uihost.exe	64 bit	Lo...	SOURCE PID 7812	PATH [redacted]...	HASH

File Read

Summary | TaskbarX.exe | Accessibility.api | 12-Jan-2021, 06:05:16

[redacted]

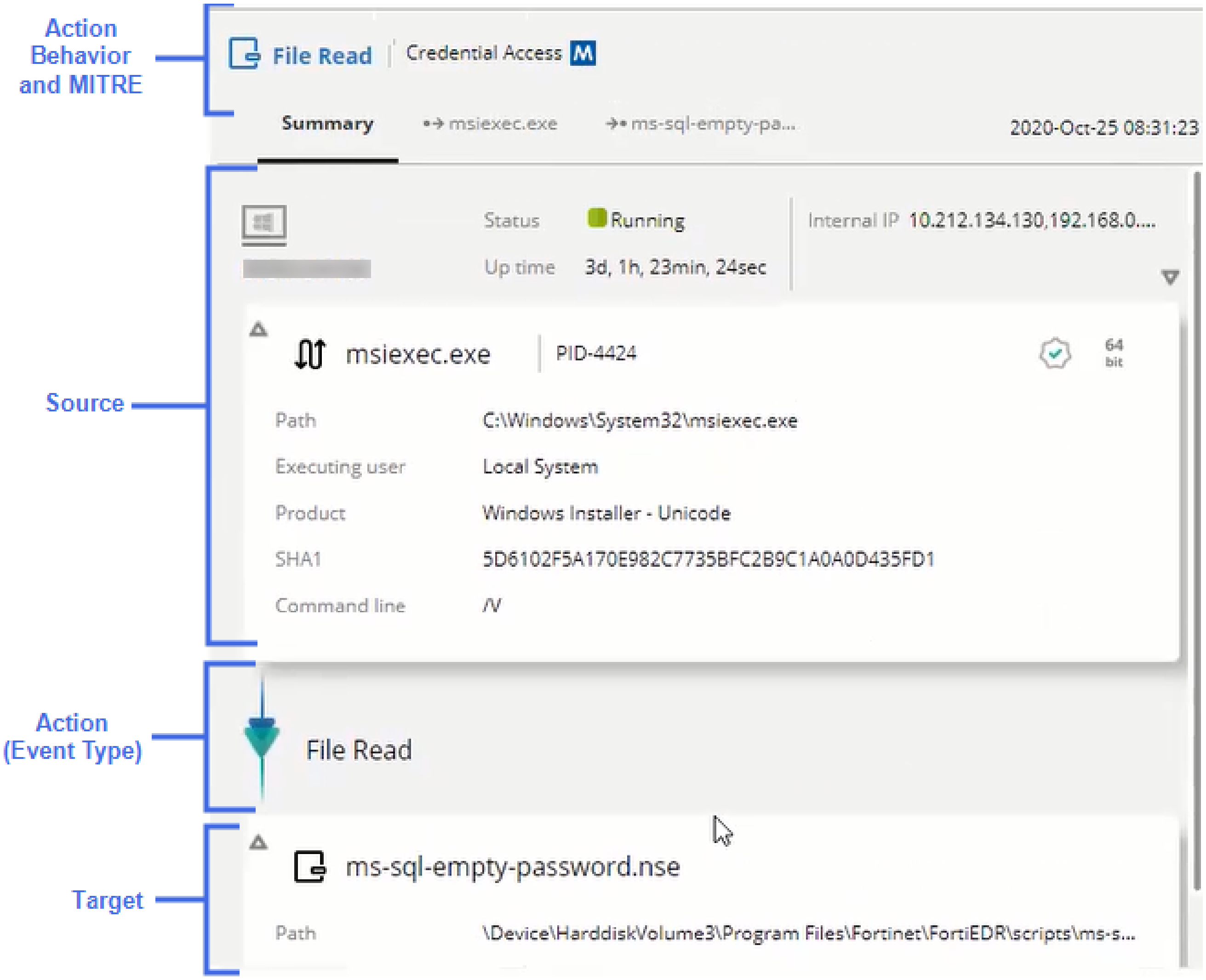
Status: Running
Up time: 5d, 21h, 3min, 10sec
Internal IP: 1[redacted]

TaskbarX.exe | PID-22900 TID-14296 | 32 bit

Path	C[redacted]\Downloads\TaskbarX_1.6.2.0\TaskbarX.exe
Executing user	[redacted]
Parent	\Device\HarddiskVolume3\Windows\System32\svch...ID - 2... Actual
Product	TaskbarX
SHA1	5E9E7421875BA6C2E1007BBC4E0B0DA39004988F
Command line	-tbs=4 -color=63;0;0;73 -as=cubiceaseinout -obas=cubiceaseinout -asp=300 -ptbo=0 -stbo=0 -lr=400 -oblr=400 -sr=0 -ftotc=1

File Read

The Details pane for an activity event contains a *Summary* tab, one or two other tabs, and the *Investigation View* (Investigate →) button, as follows:



File Read | Credential Access M

Summary | msiexec.exe | ms-sql-empty-pa... | 2020-Oct-25 08:31:23

[redacted]

Status: Running
Up time: 3d, 1h, 23min, 24sec
Internal IP: 10.212.134.130,192.168.0....

msiexec.exe | PID-4424 | 64 bit

Path: C:\Windows\System32\msiexec.exe
Executing user: Local System
Product: Windows Installer - Unicode
SHA1: 5D6102F5A170E982C7735BFC2B9C1A0A0D435FD1
Command line: /V

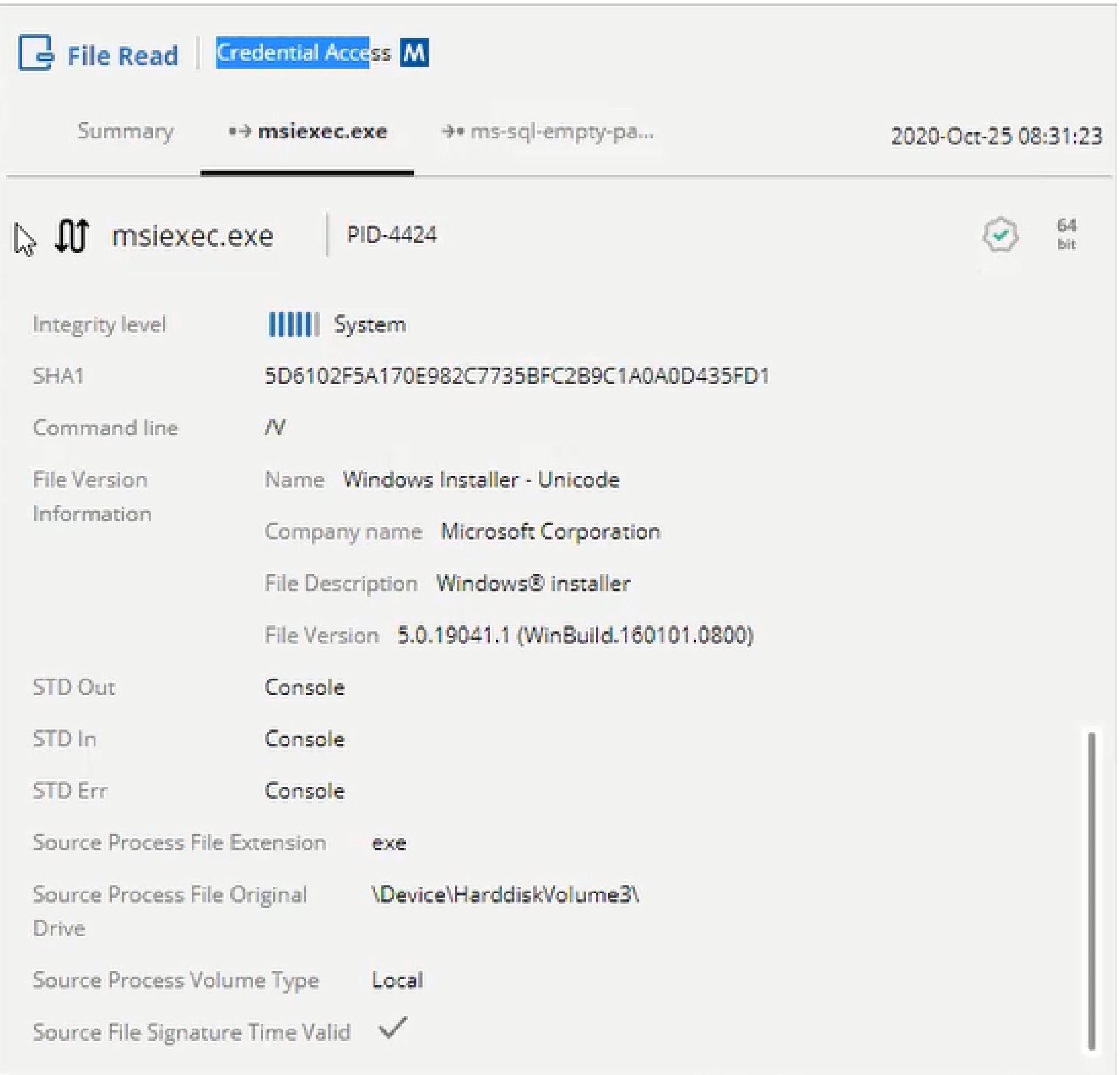
File Read

ms-sql-empty-password.nse

Path: \Device\HarddiskVolume3\Program Files\Fortinet\FortiEDR\scripts\ms-s...

- *Summary* tab: This tab specifies a summary of the activity event. At the top of the tab, it shows details about the endpoint, including the endpoint and its IP, path, operating system, and so on. The area below the endpoint section shows the source process and its detail. The area below the source graphically shows the action again, which is the activity event type, as well as some additional data regarding the action, if any. The area at the bottom of the pane shows the target and its details. You can click the *Expand* (▼) or *Collapse* (▲) arrows in an area of this pane to show or hide additional relevant details, respectively.

- *Process* tab: This tab shows additional details about the source process.

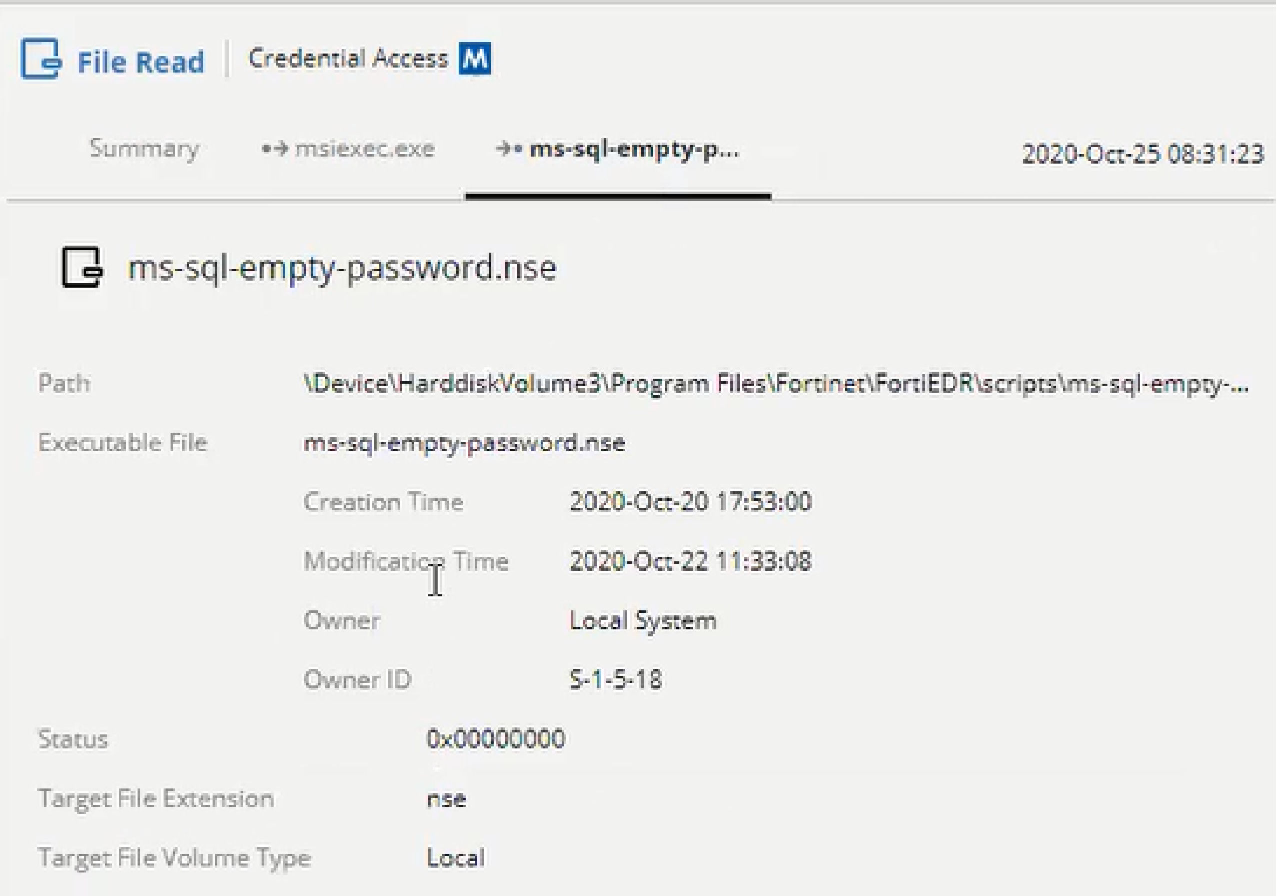


2020-Oct-25 08:31:23

msiexec.exe | PID-4424

Integrity level	System
SHA1	5D6102F5A170E982C7735BFC2B9C1A0A0D435FD1
Command line	/V
File Version Information	Name Windows Installer - Unicode Company name Microsoft Corporation File Description Windows® installer File Version 5.0.19041.1 (WinBuild.160101.0800)
STD Out	Console
STD In	Console
STD Err	Console
Source Process File Extension	exe
Source Process File Original Drive	\Device\HarddiskVolume3\
Source Process Volume Type	Local
Source File Signature Time Valid	✓

- *Target* tab: This tab only displays if the target is of type *Process* or *File*, and details additional data regarding such.



2020-Oct-25 08:31:23

ms-sql-empty-password.nse

Path \Device\HarddiskVolume3\Program Files\Fortinet\FortiEDR\scripts\ms-sql-empty-...

Executable File ms-sql-empty-password.nse

Creation Time 2020-Oct-20 17:53:00

Modification Time 2020-Oct-22 11:33:08

Owner Local System

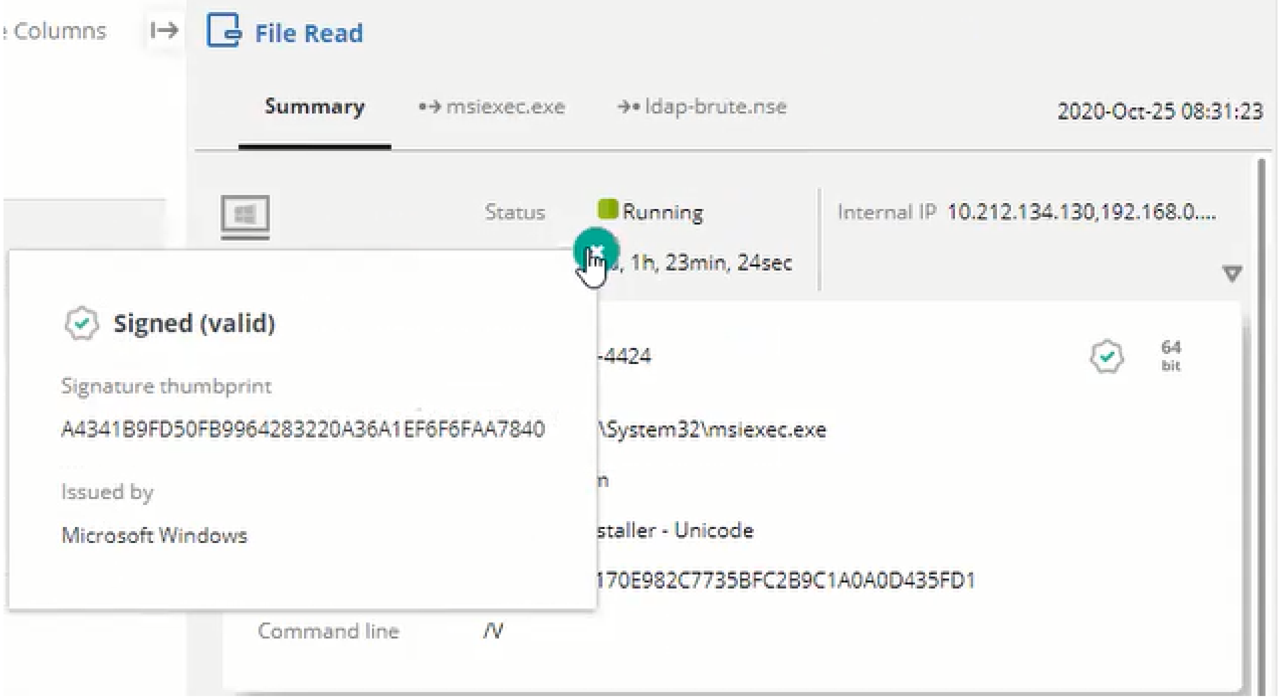
Owner ID S-1-5-18

Status 0x00000000

Target File Extension nse

Target File Volume Type Local

You can click an icon in the Details pane to display additional details, as shown below:



2020-Oct-25 08:31:23

Status Running

, 1h, 23min, 24sec

Internal IP 10.212.134.130,192.168.0....

Signed (valid)

Signature thumbprint

A4341B9FD50FB9964283220A36A1EF6F6FAA7840

Issued by

Microsoft Windows

-4424

64 bit

\System32\msiexec.exe

n

staller - Unicode

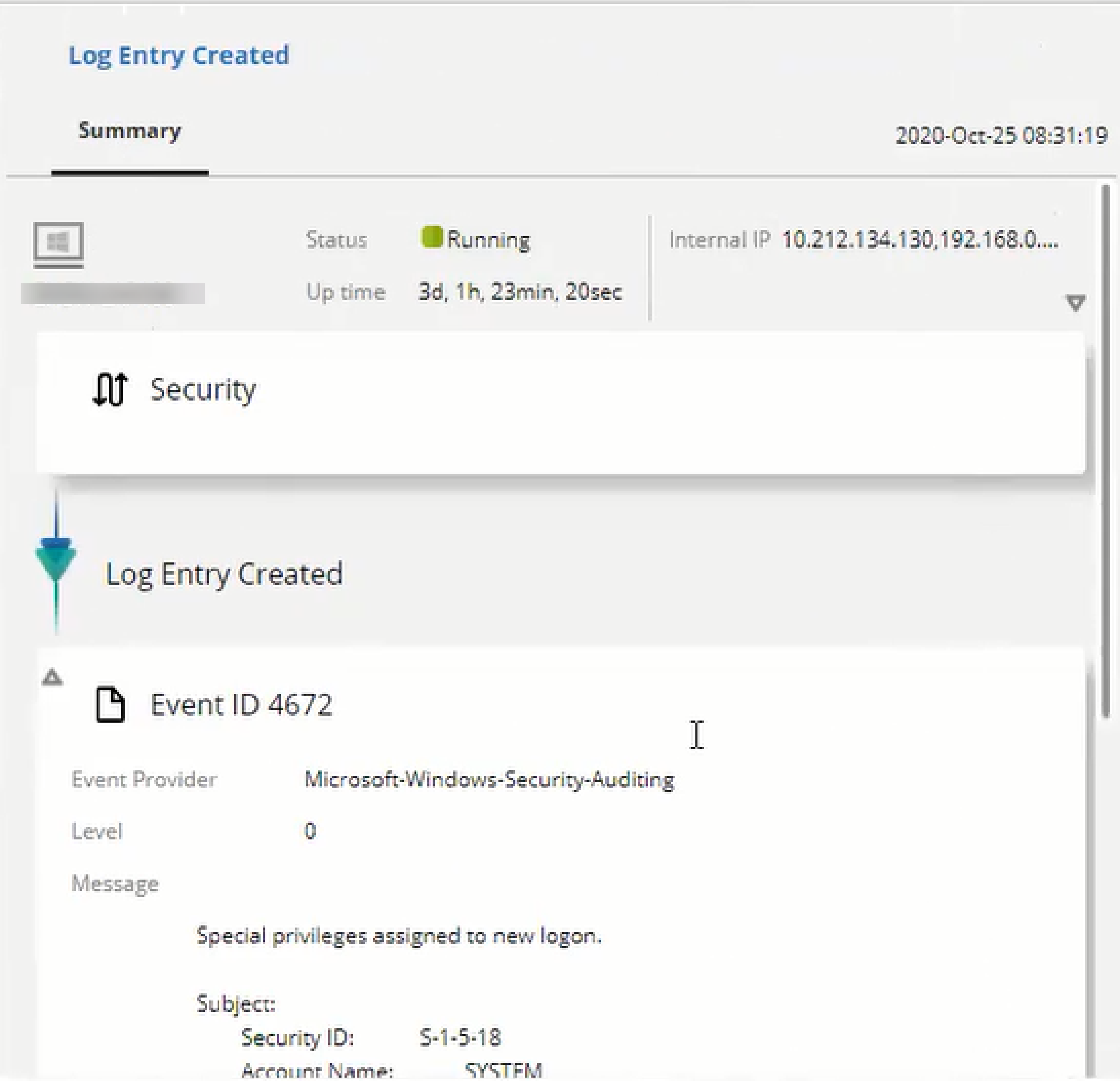
170E982C7735BFC2B9C1A0A0D435FD1

Command line /V

- *Investigation View* (Investigate →) button: This button opens a graphical Investigation View on page 155 of the activity events details: source, action and target. The graphical view provides the ability to add more activity events to the graph and show the relationship and timeline of the occurrence of those activities for better understanding of the flow of activity events.

Event Log Details pane

The Details pane for an activity event of type Event Log Created appears somewhat differently, as shown below. In this case, the action is always *Log Entry Created* and the target is always the event ID.



Log Entry Created

Summary

2020-Oct-25 08:31:19

[redacted]

Status 🟩 Running

Up time 3d, 1h, 23min, 20sec

Internal IP 10.212.134.130,192.168.0....

Security

Log Entry Created

Event ID 4672

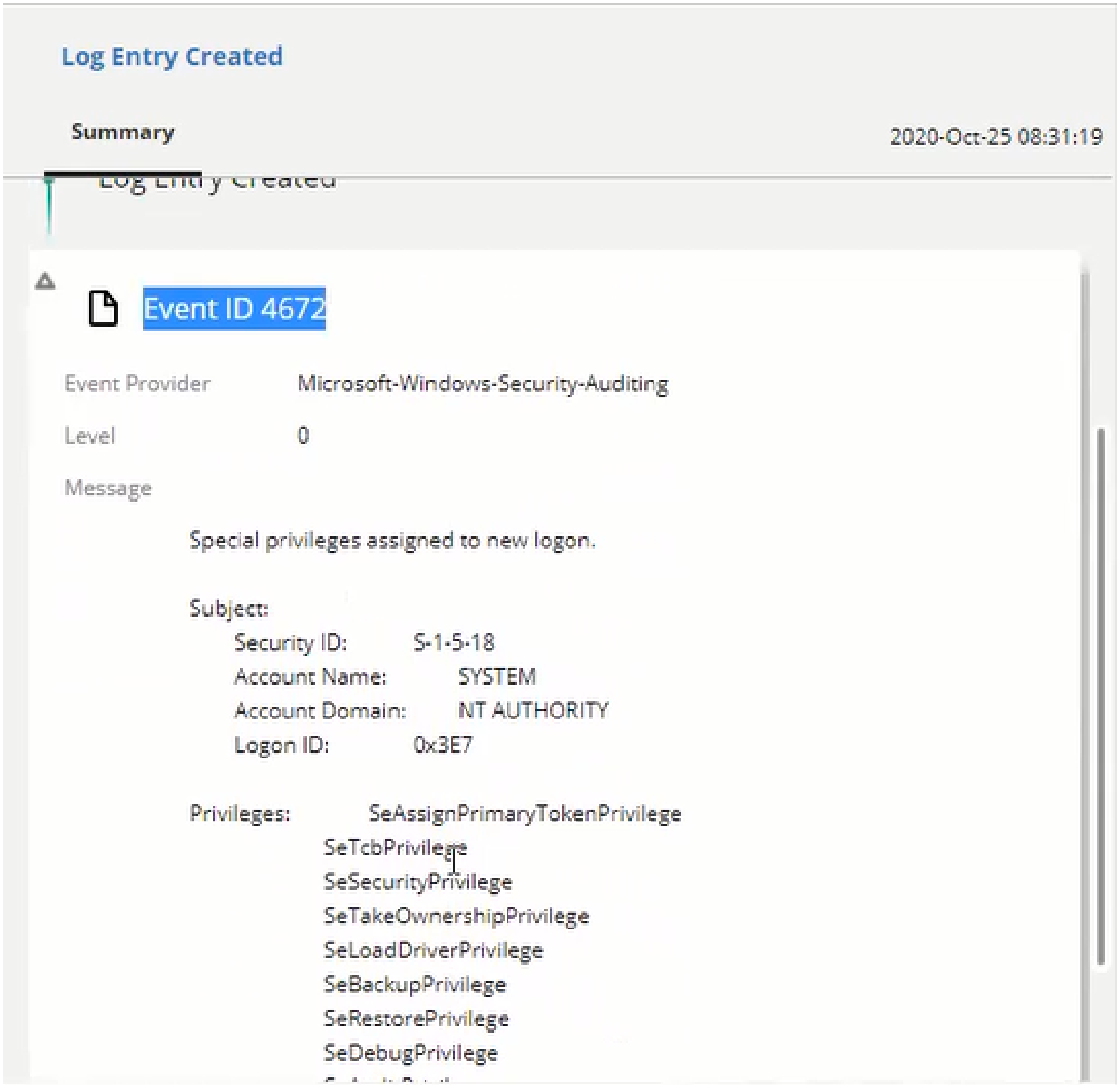
Event Provider Microsoft-Windows-Security-Auditing

Level 0

Message

```
Special privileges assigned to new logon.

Subject:
    Security ID:        S-1-5-18
    Account Name:          SYSTEM
```

You can scroll down in the Target area to view the actual log entry.



Event ID 4672

Event Provider Microsoft-Windows-Security-Auditing

Level 0

Message

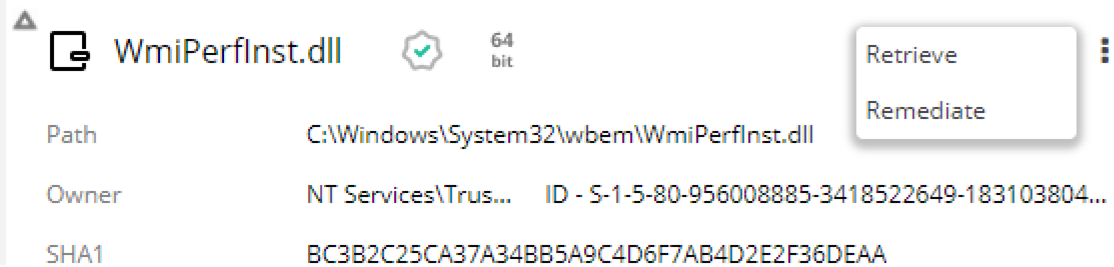
```
Special privileges assigned to new logon.

Subject:
        Security ID:        S-1-5-18
        Account Name:           SYSTEM
        Account Domain:         NT AUTHORITY
        Logon ID:           0x3E7

Privileges:         SeAssignPrimaryTokenPrivilege
            SeTcbPrivilege
            SeSecurityPrivilege
            SeTakeOwnershipPrivilege
            SeLoadDriverPrivilege
            SeBackupPrivilege
            SeRestorePrivilege
            SeDebugPrivilege
```

Retrieving a file / Remediating devices upon malware detection

You can remediate any file that is a target of an activity event. You can also download a copy of any file (Retrieve action) that is a target of an activity event.

To retrieve a file or remediate the process:

1. Select the relevant activity event and open its Details Pane.
2. When hovering over the filename, you can select either of the following options:
   - In the *Summary* pane, select the three dot dropdown menu and then select *Retrieve* of *Remediate* the file, as shown below:



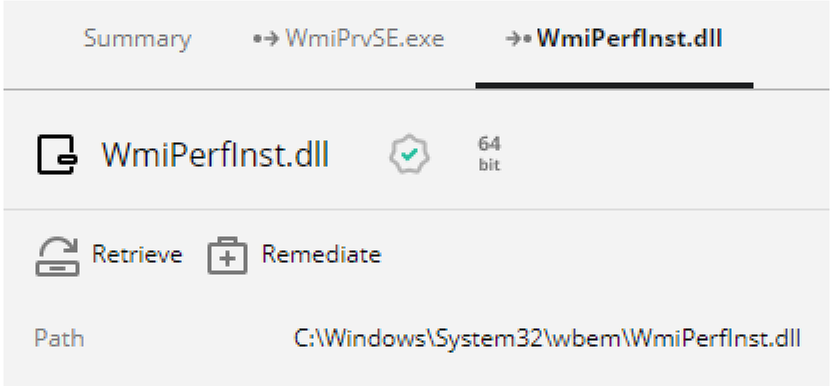
Path C:\Windows\System32\wbem\WmiPerfInst.dll

Owner NT Services\Trus... ID - S-1-5-80-956008885-3418522649-183103804...

SHA1 BC3B2C25CA37A34BB5A9C4D6F7AB4D2E2F36DEAA

– OR –

   - In the Details pane, click the *Retrieve* or *Remediate* button, as shown below:



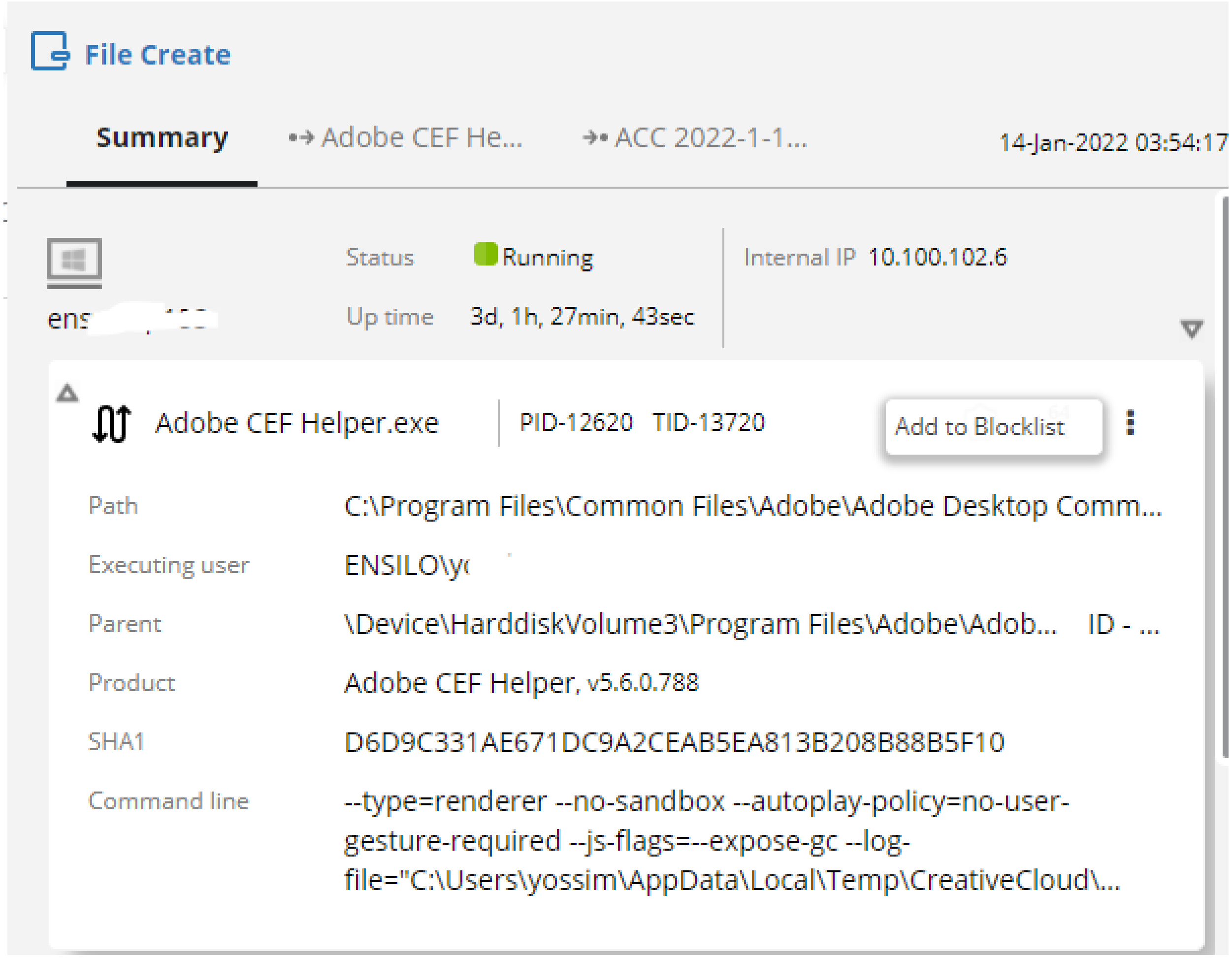
Path C:\Windows\System32\wbem\WmiPerfInst.dll

Adding an application to the Application Control policy blocklist

You can add any process that is either the source or the target of an activity event to the Application Control Policy blocklist such that this process won't launch on the devices that are assigned to that Application Control policy.

To add a process to an Application Control policy:

1. Select the relevant activity event and open its Details Pane.
2. In the *Summary* page, click the *More* (⋮) option next to the process name and select *Add to Blocklist*, as shown below:



File Create

Summary | •→ Adobe CEF He... | →• ACC 2022-1-1... | 14-Jan-2022 03:54:17

ens[redacted]

Status 🟩 Running

Up time 3d, 1h, 27min, 43sec

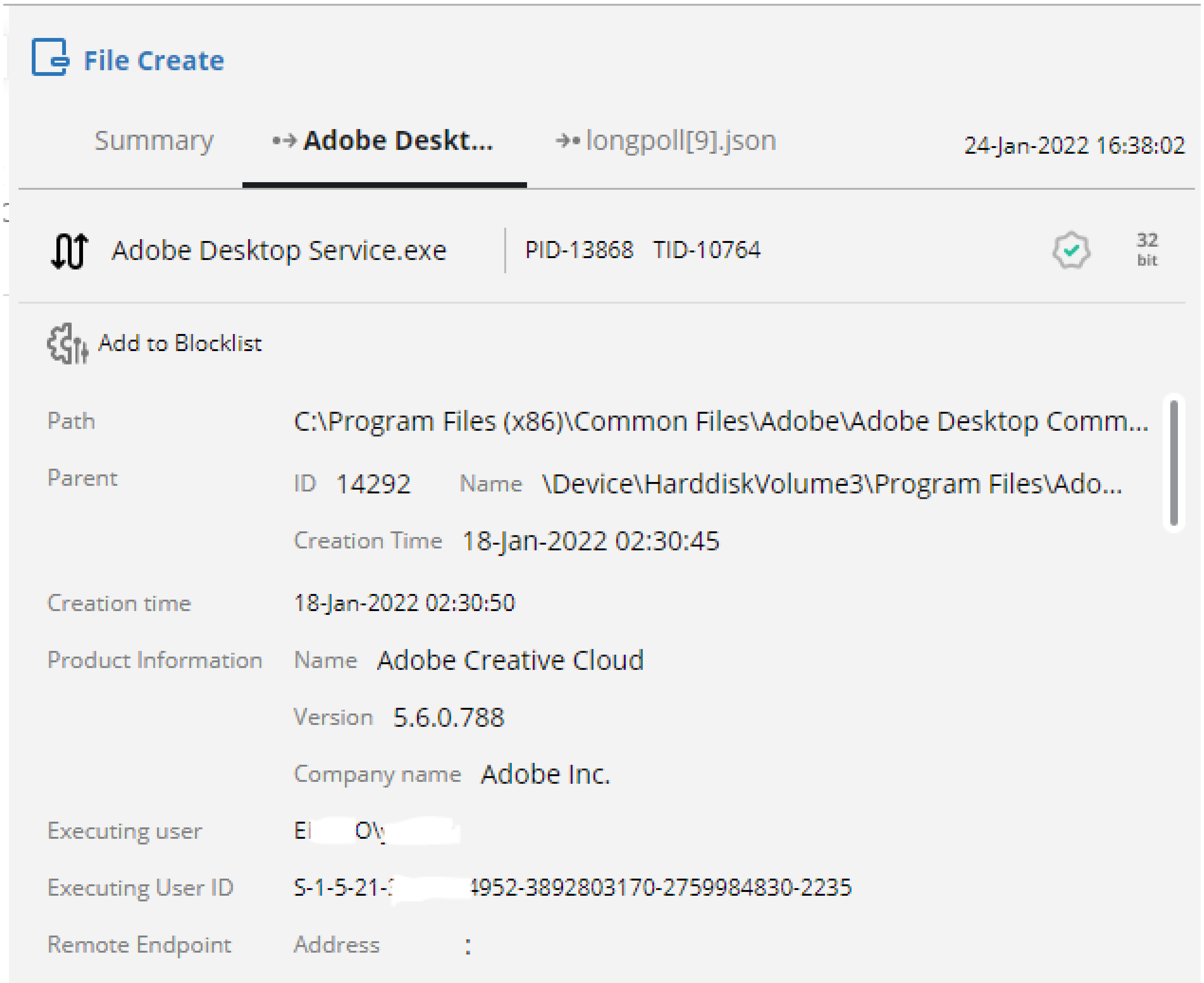
Internal IP 10.100.102.6

Adobe CEF Helper.exe | PID-12620 TID-13720 | Add to Blocklist

Path	C:\Program Files\Common Files\Adobe\Adobe Desktop Comm...
Executing user	ENSILO\y[redacted]
Parent	\Device\HarddiskVolume3\Program Files\Adobe\Adob... ID - ...
Product	Adobe CEF Helper, v5.6.0.788
SHA1	D6D9C331AE671DC9A2CEAB5EA813B208B88B5F10
Command line	--type=renderer --no-sandbox --autoplay-policy=no-user-gesture-required --js-flags=--expose-gc --log-file="C:\Users\yossim\AppData\Local\Temp\CreativeCloud\...

OR

Go to either the *Source* or the *Target* tab of type process and click the *Add to Blocklist* button, as shown below:

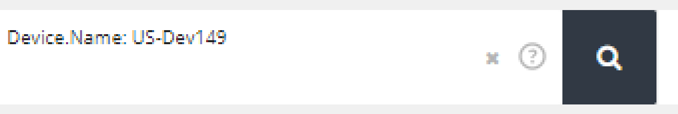


Adobe Desktop Service.exe | PID-13868 TID-10764

Path	C:\Program Files (x86)\Common Files\Adobe\Adobe Desktop Comm...
Parent	ID 14292 Name \Device\HarddiskVolume3\Program Files\Ado... Creation Time 18-Jan-2022 02:30:45
Creation time	18-Jan-2022 02:30:50
Product Information	Name Adobe Creative Cloud Version 5.6.0.788 Company name Adobe Inc.
Executing user	E[redacted]
Executing User ID	S-1-5-21-[redacted]4952-3892803170-2759984830-2235
Remote Endpoint	Address :

GDPR and activity event data

The FortiEDR system fully complies with the General Data Protection Regulation (GDPR) standard, as described in Personal Data Handling on page 325. When you use the Personal Data Handling feature to delete data, it also deletes activity event data. However, the *Personal Data Handling Search* option does not search for and display the activity data that it will delete. Just for your own knowledge, in order to see a list of the activity data that will be deleted you can view it here before you delete it. To do so, simply enter a query here that includes the chosen record from the Activity Report (that can be accessed by selecting *Administration* > *Settings* > *Personal Data Handling*) in order to find the data to be removed. For example, if you have provided the string `149` in *Personal Data Handling* for Search by *Device name*, then in the displayed Activity Report, select the record containing the device name to be deleted. In this example, it is *US-Dev149*. Then, in order to display all the activity events that are related to this device, enter the query `Device.Name: US-Dev149`, as shown below in order to display the relevant records.



Device.Name: US-Dev149

To find all activity related to a user chosen from a Personal Data Handling Activity Report, enter the following query, and select the required time range:

"Source.File.Owner:<*username*> OR Source.User:<*username*> OR Process.File.Owner:<*username*> OR Process.User:<*username*> OR Target.File.Owner:<*username*>"

Similarly, to find all activity related to an IP chosen from a Personal Data Handling Activity Report, enter the following query:

"Device.IPInternal:<*IP*> OR LocalIP:< *IP* > OR RemoteIP:< *IP* > OR Target.Network.AdditionalData.RemoteIp:<*IP*>"

Investigation View

The *Investigation View* window is accessible from the Details Pane using the *Investigation View* button ( ) of an event under *Threat Hunting*. It helps understand the flow of activity events during Threat Hunting with a dynamic and interactive graphical view of the activity events details: source, action and target.

The graphical view provides the ability to add more activity events to the graph and show the relationship and timeline of the occurrence of those activities, such as the following:

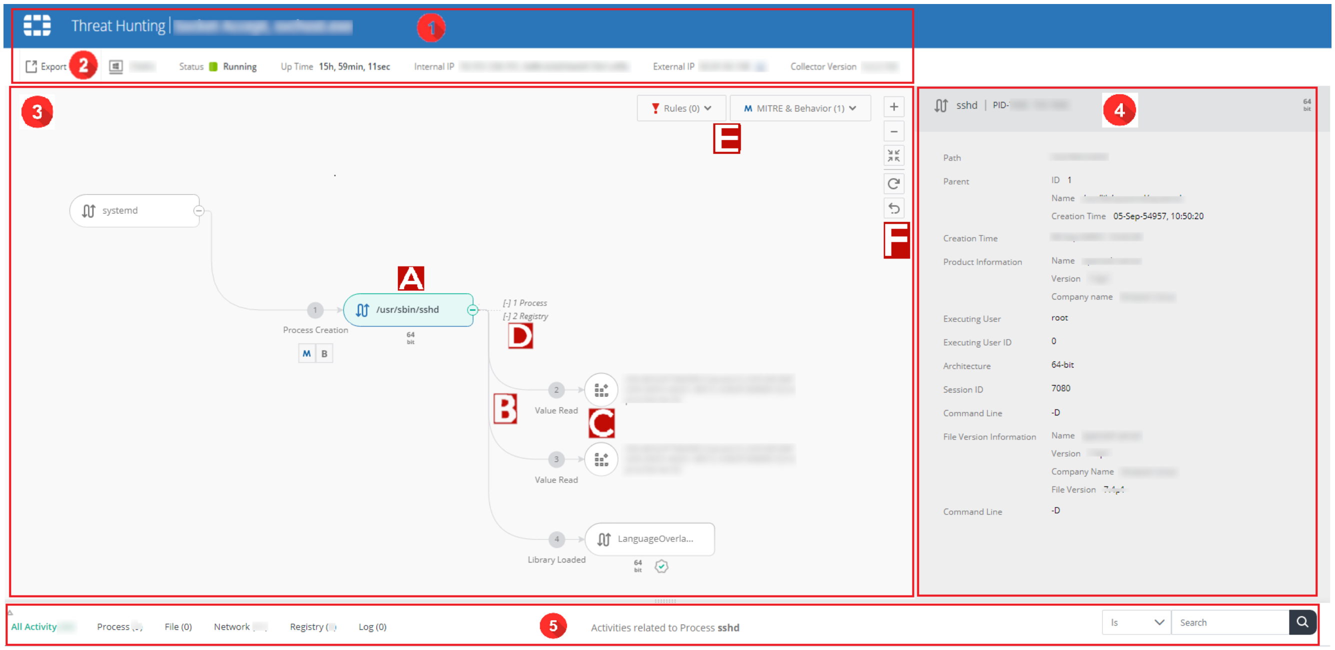
- All actions performed by a given process
- All files the process has created or updated
- All IPs the process has initiated communication with

It also allows you to interactively view a chain of activity events in the following ways:

- Browse between the various processes involved in the chain
- See all activity events related to one node and decide which nodes to add to the graph

- The *Investigation View* is not available to IT users (see Users on page 277). *Read-Only* user can only view and manipulate graphs but cannot remediate or perform other actions.
- The view adds visualization and interaction of existing data that is already available in other non-graphical and non-interactive forms without creating or generating any additional data.

The following figure illustrates the various components of an *Investigation View* window launched from the *Details Pane* under *Threat Hunting*, which has the window title "*Threat Hunting* + `activity name`.

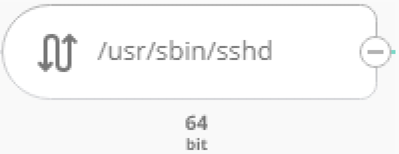
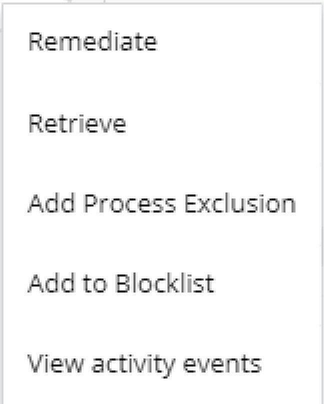
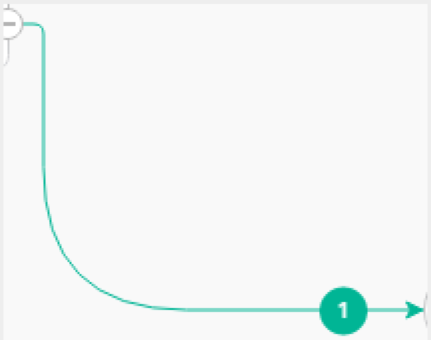


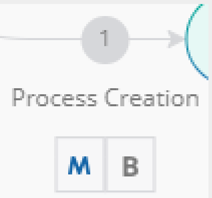
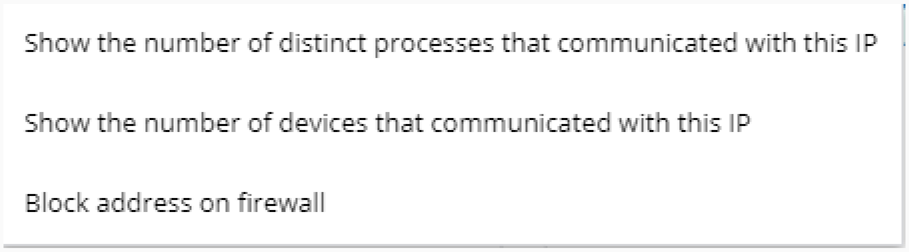
Path	[redacted]
Parent	ID 1 Name [redacted] Creation Time 05-Sep-54957, 10:50:20
Creation Time	[redacted]
Product Information	Name [redacted] Version [redacted] Company name [redacted]
Executing User	root
Executing User ID	0
Architecture	64-bit
Session ID	7080
Command Line	-D
File Version Information	Name [redacted] Version [redacted] Company Name [redacted] File Version [redacted]
Command Line	-D

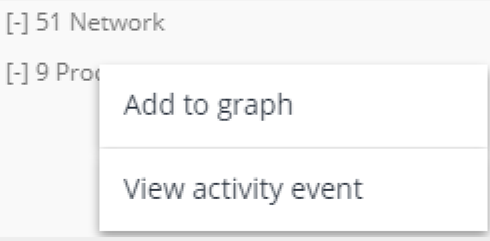
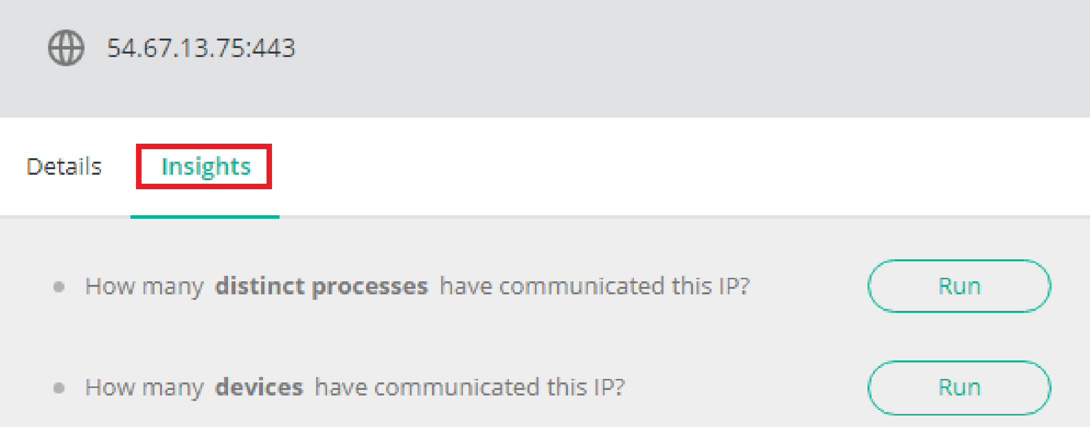
Compared with the Investigation View on page 92 window launched from the *Incidents* view, this view has the following limitations:

- Some threat hunting and investigation capabilities are unavailable, such as exporting the graph as JSON, raw data items navigation graph, and Stacks view on page 99.
- Some general event details are missing in the first row, such as classification and incident response.

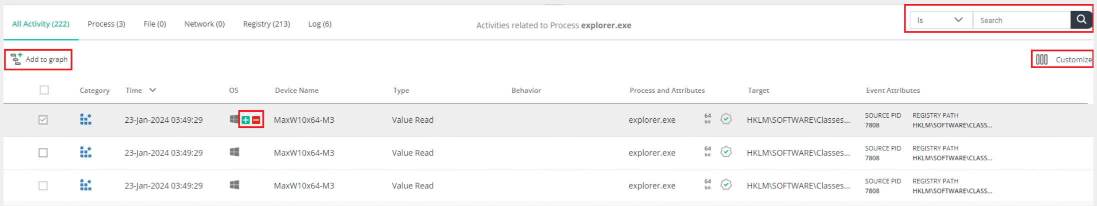
Component	Description
1	General details about the device that generated the event, such as Collector status, process name, and IP address.
2	Use the *Export* button (Export) to export the *Investigation View* window as an SVG file to share with others or for record reasons. This is the only option to save a graph that includes dynamic changes based on the default graph view, such as adding processes.
3	Graphical flow diagram with a process tree that you can build according to your investigation needs, from left to right and top to bottom. The tree is also interactive, which means you can click on a specific component to drill down for more details or contextual actions. A **Node**—Source of an activity or event, which can be a process, an endpoint, a thread or service, or another security product. Nodes are represented by boxes with icons for the activity type, some with descriptions under the boxes.

Component	Description
	 - Click on a node to display the Details pane on page 145 on the right and the Activity events tables on page 141 on the bottom with contextual information about that specific node. - Click the *Collapse* (⊖) or *Expand* (⊕) icon in the right of a node icon to show or hide all the downstream nodes, edges, and leaves. - Right-click a node to perform actions allowed on the node, including any custom actions you defined. These action buttons also appear in the *Details Pane*, which is available on the right after you click the node. The list of available options varies by node type. The following is an example list of actions for a process node.  Remediate Retrieve Add Process Exclusion Add to Blocklist View activity events
B	**Edge**—Activity event type or action represented by a curved line with an arrow. An edge can be one activity event/action or an aggregation of several. The numbered arrows indicate the sequence of actions and specify the action that was performed, such as *Process Creation*, *Socket Close*, *Block* and so on. Multiple operations performed between two processes are represented by multiple arrows between them. Edges that triggered the event are indicated in red. 

Component	Description	
		Click on an edge to display the Details pane on page 145 on the right with contextual information about that specific edge. Edges may also have icons below them indicating classification or MITRE & Behavior models. Click on an icon for more detailed information. 
	C	**Leaf**—Target of activity event of type File, Registry Key, Registry Value, Network components (IP/DNS/URL). A leaf can also be a group of artifacts. For example, all the files created or modified by a process. Leaves have a round shape (🌐). • Click on a leaf to display the Details pane on page 145 on the right and the Activity events tables on page 141 on the bottom with contextual information about that specific leaf. • Right-click a leaf to perform actions allowed on the leaf, including any custom actions you defined. These action buttons are also available in the *Details Pane*, which appear on the right after you click the leaf. The list of available options varies by leaf type. The following is an example list of actions for a network leaf:  Show the number of distinct processes that communicated with this IP Show the number of devices that communicated with this IP Block address on firewall
	D	**Hint**—Categorized groups of activities related to a node that are not part of the main chain of activity events and thus not represented in the graphical diagram. Click a node to show the number of relevant activities. The hints no longer display after you move the selection to another node or edge. [+] 51 Network [+] 9 Process • Click the *Expand* ([+]) or *Collapse* ([-]) icon near a leaf hint to show or hide the node or leaf list of that type. • Right-click the type name of a hint and select *Add to graph* to add the relevant leaves to the graph or select *View activity event* to pull out the

Component	Description	
		Activity events tables on page 141 for this specific file type. The *Add to graph* option is unavailable when the number of hints exceeds 500, in which case you can only choose to view the activity event.  [-] 51 Network [-] 9 Proc Add to graph View activity event
	E	Use the *MITRE & Behavior* legend to highlight the corresponding icons below relevant edges in the diagram.
	F	- Use the *Zoom In* (+), *Zoom Out* (−), and *Zoom To Fit* (⤡) buttons to adjust the graph window size. - Use the *Reset* (↻) button to restore the graph to the default view. - Use the *Undo* (↶) button to cancel an operation.
4	Details pane on page 145 for the selected node, edge, or leaf where you can view details of the activity, action, or target, and perform common actions on a node or leaf, such as retrieving a file, remediating devices upon malware detection, or adding an application to the Application Control policy blocklist. The actions can also be performed by right-clicking a node or leaf and selecting the option from the menu. For specific leaf types, this pane also includes an *Insights* tab which allows you to run queries to retrieve analytics data, such as the number of communicating processes or devices of a certain IP. The *Insights* options are also available from the right-click menu of those leaf types.  54.67.13.75:443 • How many **distinct processes** have communicated this IP? • How many **devices** have communicated this IP?	

<table>
<tr><th>Component</th><th>Description</th></tr>
<tr><td>5</td><td>
Contextual Activity events tables on page 141 for the selected node or leaf organized by tabs of activity types. Drag the top edge of the table up for a fuller view of the table. Activities with a number at the front of the row are already in the graph and the number matches the one in the graph.



All Activity (222) Process (3) File (0) Network (0) Registry (213) Log (6)

Activities related to Process **explorer.exe**

<table>
<tr><th>☐</th><th>Category</th><th>Time</th><th>OS</th><th>Device Name</th><th>Type</th><th>Behavior</th><th>Process and Attributes</th><th>Target</th><th>Event Attributes</th></tr>
<tr><td>☑</td><td></td><td>23-Jan-2024 03:49:29</td><td>+ −</td><td>MaxW10x64-M3</td><td>Value Read</td><td></td><td>explorer.exe 64 bit</td><td>HKLM\SOFTWARE\Classes...</td><td>SOURCE PID 7808 REGISTRY PATH HKLM\SOFTWARE\CLASS...</td></tr>
<tr><td>☐</td><td></td><td>23-Jan-2024 03:49:29</td><td></td><td>MaxW10x64-M3</td><td>Value Read</td><td></td><td>explorer.exe 64 bit</td><td>HKLM\SOFTWARE\Classes...</td><td>SOURCE PID 7808 REGISTRY PATH HKLM\SOFTWARE\CLASS...</td></tr>
<tr><td>☐</td><td></td><td>23-Jan-2024 03:49:29</td><td></td><td>MaxW10x64-M3</td><td>Value Read</td><td></td><td>explorer.exe 64 bit</td><td>HKLM\SOFTWARE\Classes...</td><td>SOURCE PID 7808 REGISTRY PATH HKLM\SOFTWARE\CLASS...</td></tr>
</table>

- To add activities to the graph, select the corresponding rows and click *Add to graph* (Add to graph).
- To customize the columns to display in the table, click *Customize* (Customize).
- To search for a specific activity or event, enter keywords in the search bar on the top right corner (Is Search).
- To filter the results in the Activity Events table to include or exclude a specific value, use the green plus (+) and red minus (−) icons that appear when you hover over the value. Multiple filters are supported. To delete a filter, click the cancel icon that appear when you hover over the filter on the top-left of the table.
</td></tr>
</table>

Remediating a device upon malware detection

After malware is detected on a device, you can remediate the device from the Investigation View on page 92 (detailed in the procedure below) or by connecting to the device directly using the FortiEDR Connect on page 109 functionality.

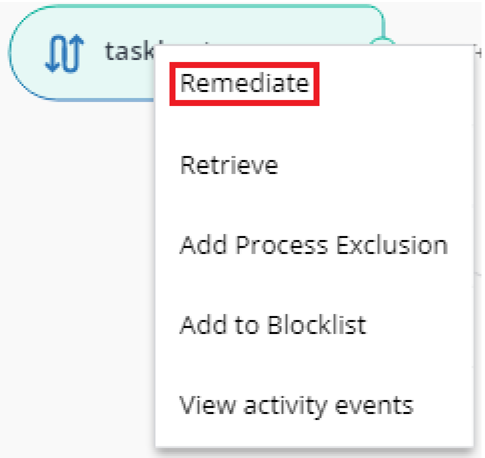
The following options are available when you remediate the situation in the FortiEDR system:

Method	Description
Terminate the Process	This method does not guarantee that the affected process will not attempt to execute again.
Delete the Affected File from the Computer	This method ensures that the file does not attempt to exfiltrate data again, as the file is permanently removed from the device. When using this method, be careful not to delete files that are important to the system, in order to protect system stability.
Remove or Modify the Registry Key	This method removes a registry key or updates a registry key's value. This method changes malicious registry key modifications by removing newly created keys or returning key values to their original form.

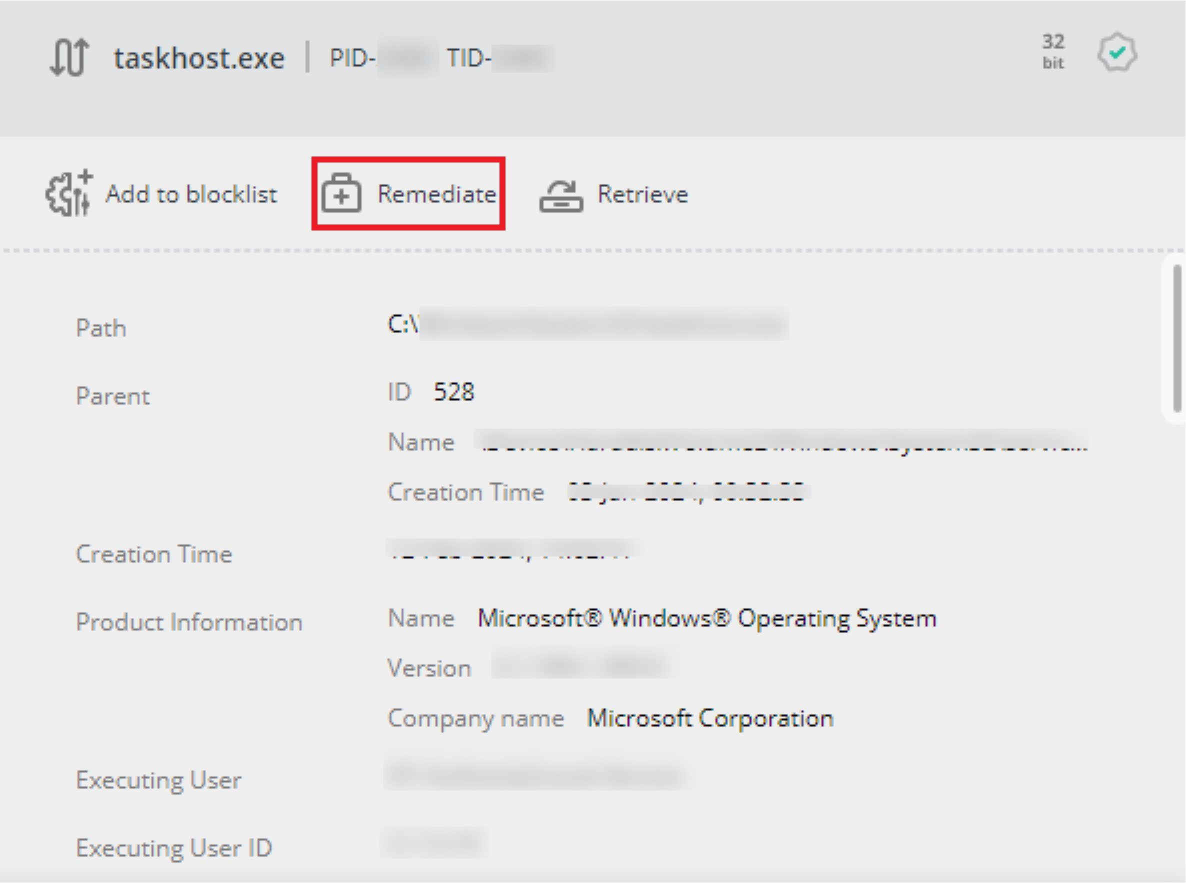
Method	Description
	Some malware have persistency capabilities, which makes the infection appear again. In addition, in some rare cases, malware can cause the system to crash if you try to remove them. Both of these methods can be performed using the Forensics add-on.

To remediate a device from the Investigation View on page 92:

1. Right-click the node of the relevant activity event and select *Remediate*.



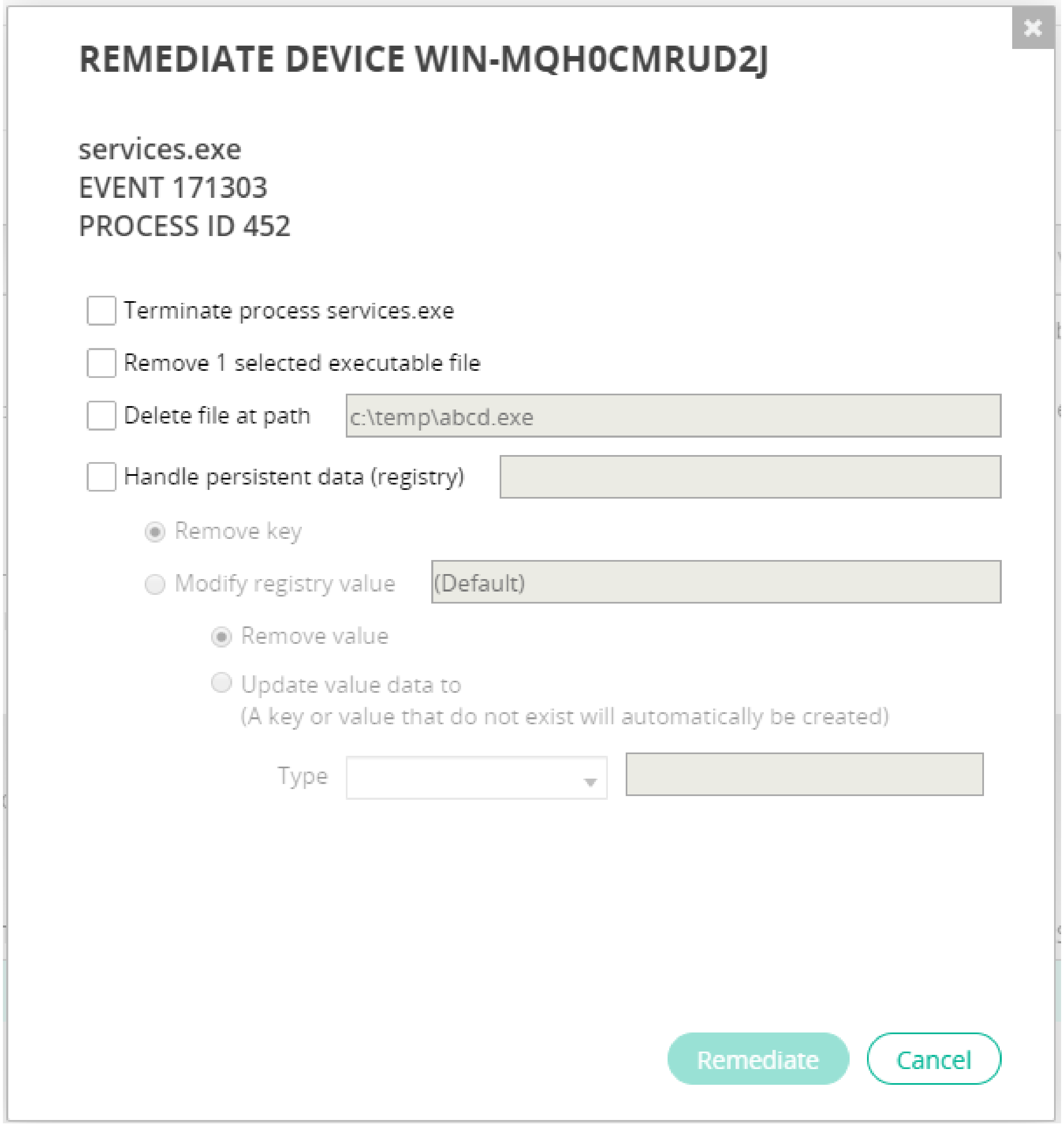
Alternatively, select the node of the relevant activity event and click the *Remediate* button in the *Details Pane* that appears on the right.



Path	C:\[redacted]
Parent	ID 528 Name [redacted] Creation Time [redacted]
Creation Time	[redacted]
Product Information	Name Microsoft® Windows® Operating System Version [redacted] Company name Microsoft Corporation
Executing User	[redacted]
Executing User ID	[redacted]

The *Remediate* button is also available from the Stacks view on page 99, which is available when an edge is selected.

2. The following window displays:



REMEDIATE DEVICE WIN-MQH0CMRUD2J

services.exe
EVENT 171303
PROCESS ID 452

□ Terminate process services.exe

□ Remove 1 selected executable file

□ Delete file at path c:\temp\abcd.exe

□ Handle persistent data (registry)

● Remove key

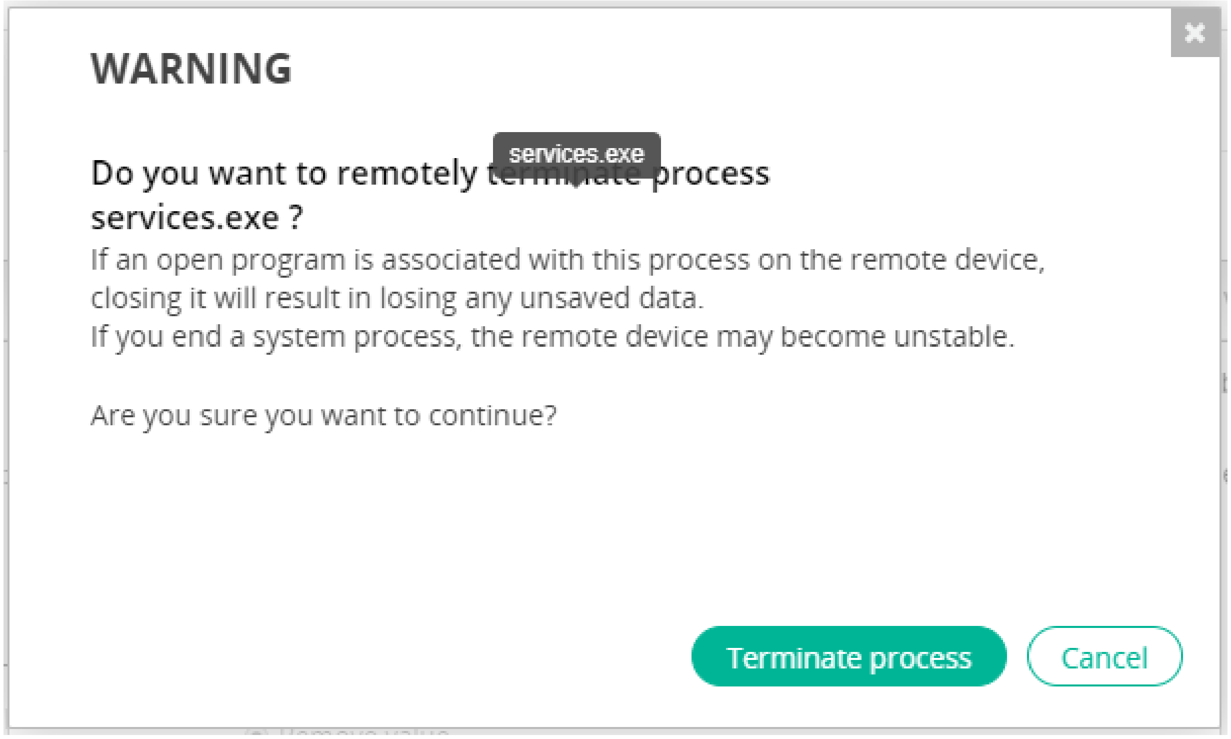
○ Modify registry value (Default)

● Remove value

○ Update value data to
(A key or value that do not exist will automatically be created)

Type

3. Do one of the following:
   a. Check the *Terminate process* checkbox to terminate the selected process. A warning message displays.



WARNING

Do you want to remotely terminate process services.exe ?

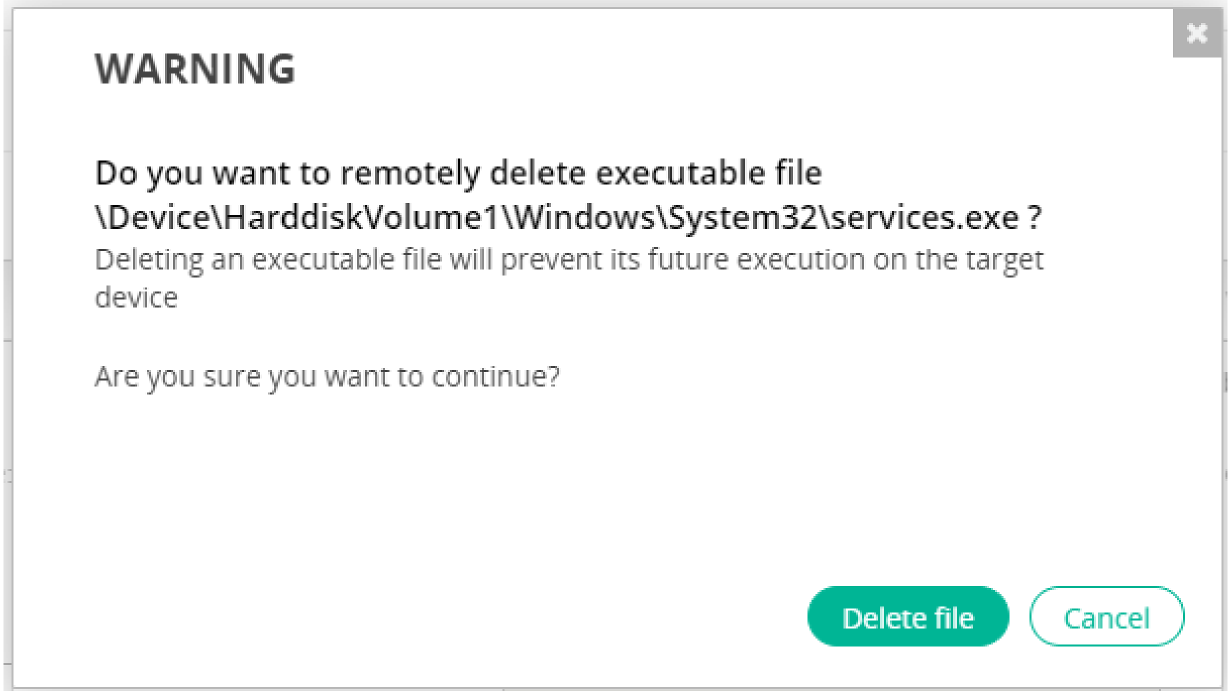
If an open program is associated with this process on the remote device, closing it will result in losing any unsaved data.

If you end a system process, the remote device may become unstable.

Are you sure you want to continue?

Click *Terminate process* to terminate the selected process.

b. Check the *Remove selected executable file* checkbox to delete the specified file from the device. A warning message displays.



WARNING

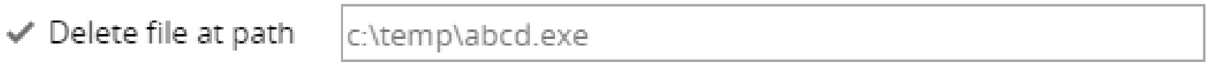
Do you want to remotely delete executable file \Device\HarddiskVolume1\Windows\System32\services.exe ?

Deleting an executable file will prevent its future execution on the target device

Are you sure you want to continue?

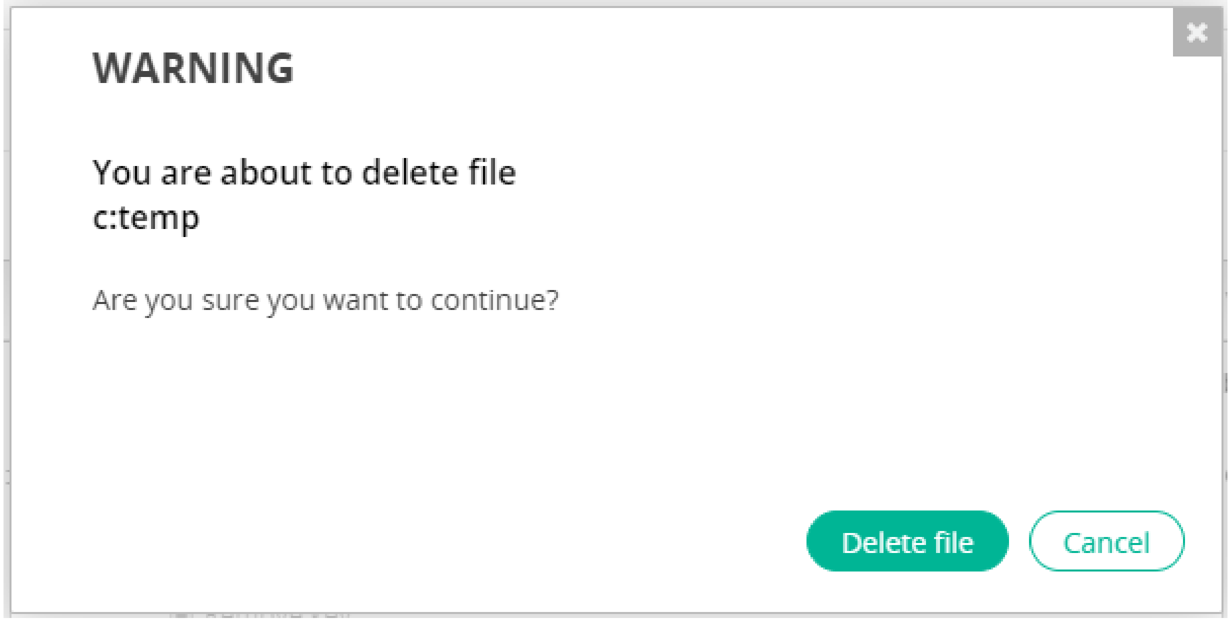
Click *Delete file* to remove the selected file.

c. Check the *Delete file at path* checkbox. In the adjacent field, enter the file path on the device that contains the file to be removed.



✓ Delete file at path c:\temp\abcd.exe

A warning message displays.



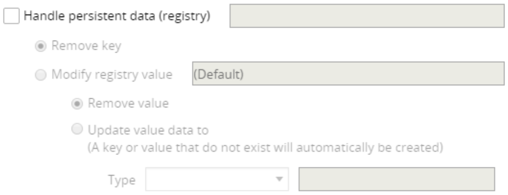
WARNING

You are about to delete file
c:temp

Are you sure you want to continue?

Click *Delete file* to remove the file from the specified path.

d. Check the *Handle persistent data (registry)* checkbox to clean the registry keys in Windows. In the adjacent field, enter the value of the registry key to be removed or modified.



□ Handle persistent data (registry)

● Remove key

○ Modify registry value (Default)

● Remove value

○ Update value data to
(A key or value that do not exist will automatically be created)

Type

Value data should be provided in the required format, based on the value type selected in the dropdown list, as follows:

- *String* for types REG_SZ(1), REG_EXPAND_SZ(2), REG_DWORD(4) and REG_QWORD(11).
- *Base64* for types REG_BINARY(3), REG_DWORD_BIG_ENDIAN(5), REG_LINK(6), REG_MULTI_SZ (7), REG_RESOURCE_LIST(8), REG_FULL_RESOURCE_DESCRIPTOR(9) and REG_RESOURCE_ REQUIREMENTS_LIST(10).

Select the *Remove key* radio button to remove the registry key value.

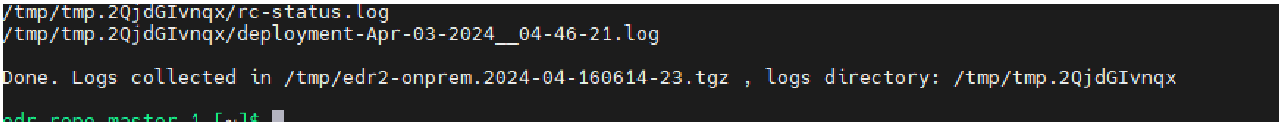
Select the *Modify registry value* radio button to change the current registry key value. When selecting this option, you must also specify the new value for the registry key in the gray box and the key's value type in the adjacent dropdown menu (for example, string, binary and so on).

4. Click *Remediate*.

Exporting threat hunting logs

For on-premise deployments, when you submit a support ticket about issues with Threat Hunting Repository installation, upgrade, or general functioning, you must include the threat hunting logs.

To collect threat hunting logs:

1. Run the following command:
   `sudo bash /opt/FortiEDR/deployments/latest/deployment/ci-tools/get_logs.sh`
   The script will create logs archive in the `/tmp/` directory.
   
   ```
   /tmp/tmp.2QjdGIvnqx/rc-status.log
   /tmp/tmp.2QjdGIvnqx/deployment-Apr-03-2024__04-46-21.log

   Done. Logs collected in /tmp/edr2-onprem.2024-04-160614-23.tgz , logs directory: /tmp/tmp.2QjdGIvnqx

   edr_repo_master_1 [~]$
   ```
2. Use the SCP client to download the `.tgz` file.
   You can then attach the file to the support ticket.

To retrieve Collector, Core, and Aggegator logs, see the following:

- Exporting logs for Collectors on page 273
- Exporting logs for Cores on page 274
- Exporting logs for Aggregators on page 275

Communication control

This chapter describes the FortiEDR communication control mechanism for monitoring and handling non-disguised security events.

Application communication control - how does it work?

FortiEDR provides visibility into any communicating application in your organization, enabling you to control which applications can communicate.

After FortiEDR installation, the system automatically maps all applications in your network that communicate externally. After that, you then decide which of these applications to allow to communicate externally when used by a legitimate user in your organization (allowlist). After the allowlist of communicating applications is defined, only applications in the allowlist can communicate externally. If an attacker abuses an application in the allowlist, FortiEDR's patented technology (Exfiltration and Ransomware prevention policies) blocks the communication and displays a security event in the *Incidents* tab.

FortiEDR Communication Control uses a set of policies that contain recommendations about whether an application should be approved or denied of communication. These policies can be configured as a next-generation firewall in order to automatically block communications of potentially unwanted applications. For example, applications with a known bad reputation or that are distributed by questionable vendors.

Moreover, FortiEDR Communication Control provides data and tools for efficient vulnerability assessment and control. Virtual patching is made possible with Communication Control policies that can be configured to automatically block connections from vulnerable applications.

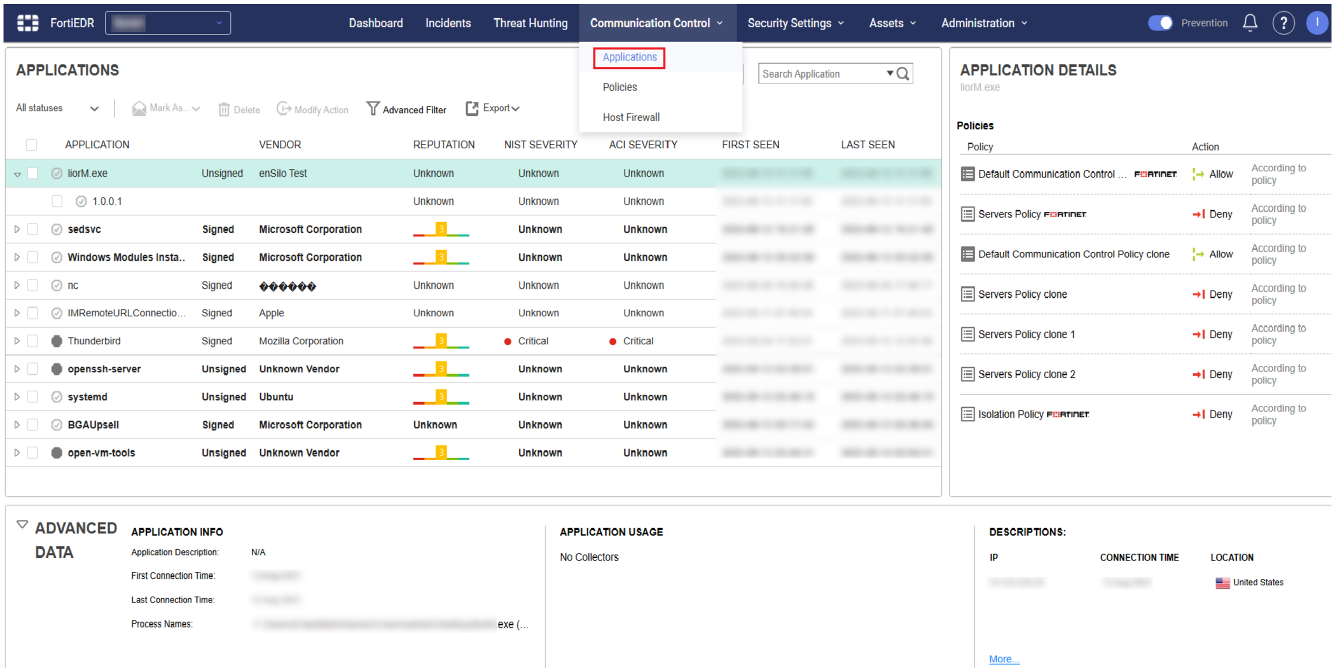
You can also configure host firewall policies to control incoming and outgoing in network traffic to protect endpoints against unwanted connections based on remote addresses, protocols, or applications in use to reflect the organization's network policies.

FortiEDR's Communication Control mechanism provides the following key advantages:

Mechanism	Description
Realtime Proactive Risk Mitigation	Attack surface reduction using risk-based proactive policies that are based on application CVE and rating data.
Avoids Productivity Inhibitors	Non-authorized applications can still execute. Only their outgoing communication is prevented.
Manageability	Reduces the scope of the problem, which means that Security/IT needs to handle only applications that communicate externally.
Frictionless Application Control	Reduces users' requests from Security/IT to approve applications.

Introducing communication control

The *COMMUNICATION CONTROL* tab identifies all the communicating applications detected in your organization. To access this page, click the down arrow next to *COMMUNICATION CONTROL* and then select *Applications*.



APPLICATIONS

APPLICATION		VENDOR	REPUTATION	NIST SEVERITY	ACI SEVERITY	FIRST SEEN	LAST SEEN
liorM.exe	Unsigned	enSilo Test	Unknown	Unknown	Unknown	[redacted]	[redacted]
1.0.0.1			Unknown	Unknown	Unknown	[redacted]	[redacted]
sedsvc	**Signed**	**Microsoft Corporation**	3	**Unknown**	**Unknown**	[redacted]	[redacted]
Windows Modules Insta..	**Signed**	**Microsoft Corporation**	3	**Unknown**	**Unknown**	[redacted]	[redacted]
nc	Signed	������	Unknown	Unknown	Unknown	[redacted]	[redacted]
IMRemoteURLConnectio...	Signed	Apple	Unknown	Unknown	Unknown	[redacted]	[redacted]
Thunderbird	Signed	Mozilla Corporation	3	● Critical	● Critical	[redacted]	[redacted]
openssh-server	**Unsigned**	**Unknown Vendor**	3	**Unknown**	**Unknown**	[redacted]	[redacted]
systemd	**Unsigned**	**Ubuntu**	3	**Unknown**	**Unknown**	[redacted]	[redacted]
BGAUpsell	**Signed**	**Microsoft Corporation**	**Unknown**	**Unknown**	**Unknown**	[redacted]	[redacted]
open-vm-tools	**Unsigned**	**Unknown Vendor**	3	**Unknown**	**Unknown**	[redacted]	[redacted]

APPLICATION DETAILS

liorM.exe

Policies

Policy	Action	
Default Communication Control ... FORTINET	Allow	According to policy
Servers Policy FORTINET	Deny	According to policy
Default Communication Control Policy clone	Allow	According to policy
Servers Policy clone	Deny	According to policy
Servers Policy clone 1	Deny	According to policy
Servers Policy clone 2	Deny	According to policy
Isolation Policy FORTINET	Deny	According to policy

ADVANCED DATA

APPLICATION INFO

Application Description:	N/A
First Connection Time:	[redacted]
Last Connection Time:	[redacted]
Process Names:	[redacted] exe (...

APPLICATION USAGE

No Collectors

DESCRIPTIONS:

IP	CONNECTION TIME	LOCATION
[redacted]	[redacted]	United States

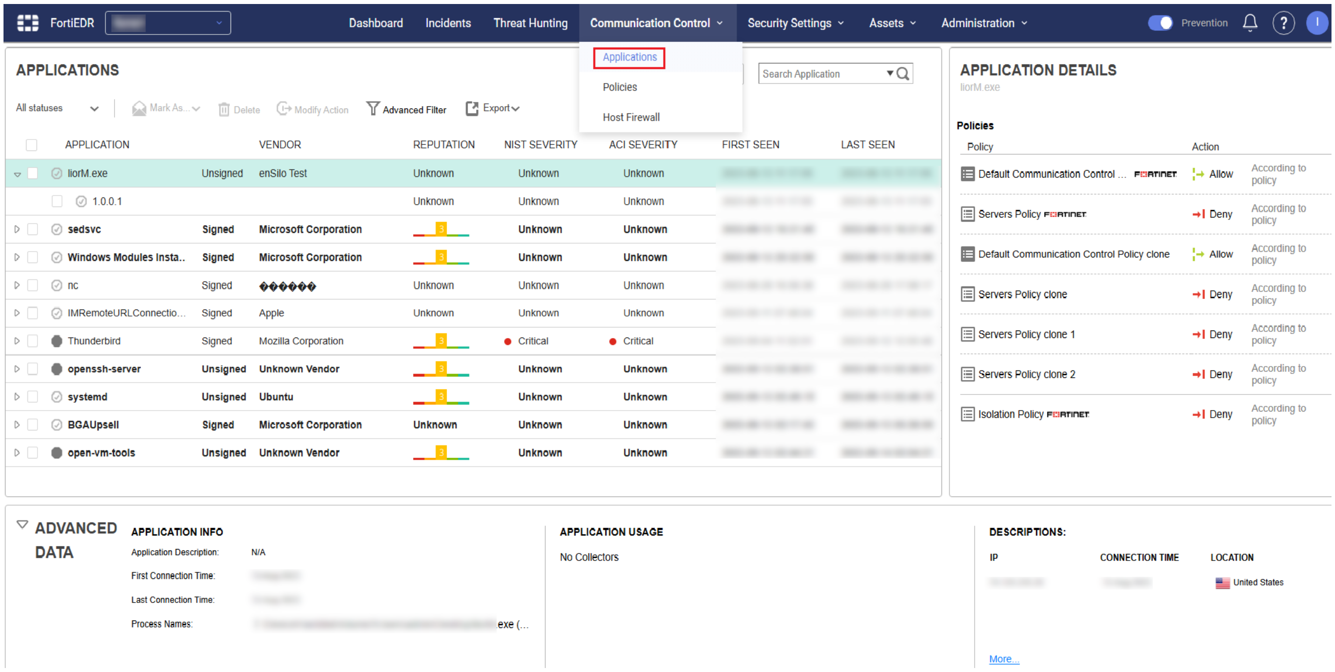
More...

The *COMMUNICATION CONTROL* tab contains the following pages:

- Applications on page 168
- Policies on page 184
- Host Firewall Collector 6.1 or later on page 194

Applications

The *APPLICATIONS* page lists all communicating applications detected in your organization that have ever attempted to communicate. By default, applications are sorted according to their first-seen indicator, placing new applications at the top. To access this page, click the down arrow next to *COMMUNICATION CONTROL* and then select *Applications*.



APPLICATIONS

APPLICATION		VENDOR	REPUTATION	NIST SEVERITY	ACI SEVERITY	FIRST SEEN	LAST SEEN
liorM.exe	Unsigned	enSilo Test	Unknown	Unknown	Unknown	[redacted]	[redacted]
1.0.0.1			Unknown	Unknown	Unknown	[redacted]	[redacted]
sedsvc	Signed	Microsoft Corporation	3	Unknown	Unknown	[redacted]	[redacted]
Windows Modules Insta..	Signed	Microsoft Corporation	3	Unknown	Unknown	[redacted]	[redacted]
nc	Signed	������	Unknown	Unknown	Unknown	[redacted]	[redacted]
IMRemoteURLConnectio...	Signed	Apple	Unknown	Unknown	Unknown	[redacted]	[redacted]
Thunderbird	Signed	Mozilla Corporation	3	● Critical	● Critical	[redacted]	[redacted]
openssh-server	Unsigned	Unknown Vendor	3	Unknown	Unknown	[redacted]	[redacted]
systemd	Unsigned	Ubuntu	3	Unknown	Unknown	[redacted]	[redacted]
BGAUpsell	Signed	Microsoft Corporation	Unknown	Unknown	Unknown	[redacted]	[redacted]
open-vm-tools	Unsigned	Unknown Vendor	3	Unknown	Unknown	[redacted]	[redacted]

APPLICATION DETAILS

liorM.exe

Policies

Policy	Action	
Default Communication Control ... FORTINET	Allow	According to policy
Servers Policy FORTINET	Deny	According to policy
Default Communication Control Policy clone	Allow	According to policy
Servers Policy clone	Deny	According to policy
Servers Policy clone 1	Deny	According to policy
Servers Policy clone 2	Deny	According to policy
Isolation Policy FORTINET	Deny	According to policy

ADVANCED DATA

APPLICATION INFO

Application Description: N/A

First Connection Time: [redacted]

Last Connection Time: [redacted]

Process Names: [redacted]exe (...

APPLICATION USAGE

No Collectors

DESCRIPTIONS:

IP	CONNECTION TIME	LOCATION
[redacted]	[redacted]	United States

More...

Information is organized hierarchically in a two-level tree. The first (top) level specifies the name of the application. The second level specifies the application version.

The following information displays for each application in the application list:

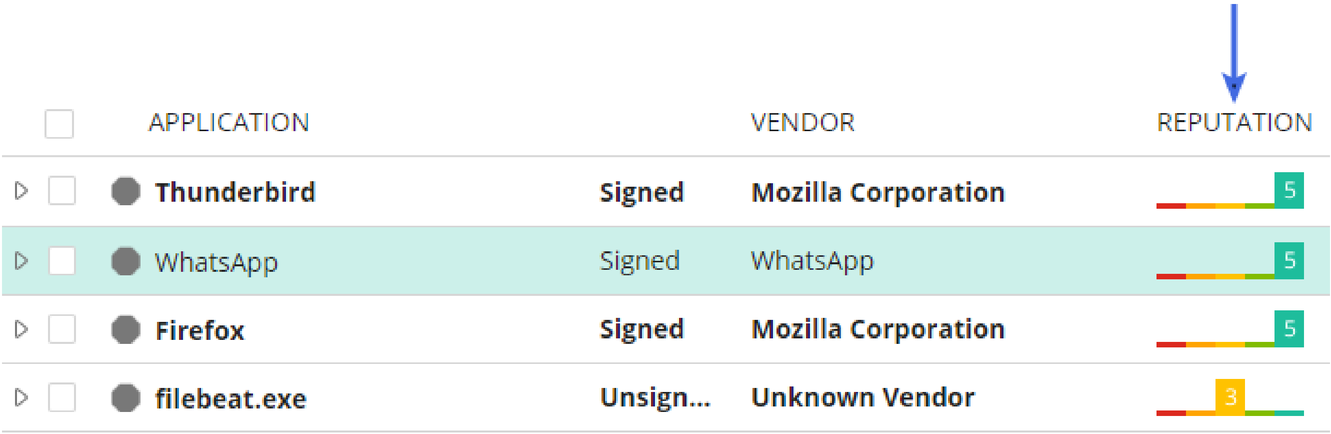
- Selection checkbox
- Resolving status icon
- Signed/Unsigned indication
- *APPLICATION/VERSION*: The name of the application/version.
- *VENDOR*: The application's vendor and certificate details.
- *REPUTATION*: The reputation score of the application. For more details, Reputation score on page 169
- *VULNERABILITY*: The highest CVE vulnerability score for the application. For more details, see Severity on page 170
- *FIRST SEEN*: The date and time when the application was first seen in the organization.
- *LAST SEEN*: The date and time of the last connection of this application.

The *APPLICATION DETAILS* area of the window on the right displays policy-related details for the entity (application or version) selected in the application list. This area displays the policy action (Allow or Deny) for each communication control policy.

The *Advanced Data* area at the bottom of the window presents statistics about the selected application/version in the application list. For more details, see Advanced Data on page 178.

Reputation score

Each application in the *APPLICATIONS* page shows a *REPUTATION* indicator. Reputation scores are determined by a third-party service, and are based on the hash (signature) of the file.



	APPLICATION		VENDOR	REPUTATION
▷ □ ●	Thunderbird	Signed	Mozilla Corporation	5
▷ □ ●	WhatsApp	Signed	WhatsApp	5
▷ □ ●	Firefox	Signed	Mozilla Corporation	5
▷ □ ●	filebeat.exe	Unsign...	Unknown Vendor	3

Reputation scores use the following range to indicate the reputation for an application:

Reputation Score	Reputation Description
1	Known as bad
2	Assumed as bad
3	Unclear, indication a contradiction or inability to determine the reputation
4	Assumed as good
5	Known as good

The *REPUTATION* indicator displays *Unknown* if the reputation score is unknown.

Severity

FortiEDR's severity scoring system provides a useful tool for vulnerability assessment and enables you to review the weaknesses detected in your environment that could be exploited by attackers before they actually occur. You can then use virtual patching to block applications with known critical vulnerabilities so that they cannot connect until the system is patched for the CVEs listed.

It also provides comprehensive visibility into the organization's external attack surface so that analysts can prioritize security alerts and incidents based on risk factors such as severity of vulnerabilities, relevance of threat intelligence feeds, and severity of affected endpoints, ensuring that efforts are focused on addressing the most significant risks to the organization.

Each application and version in the application list shows two severity ratings:

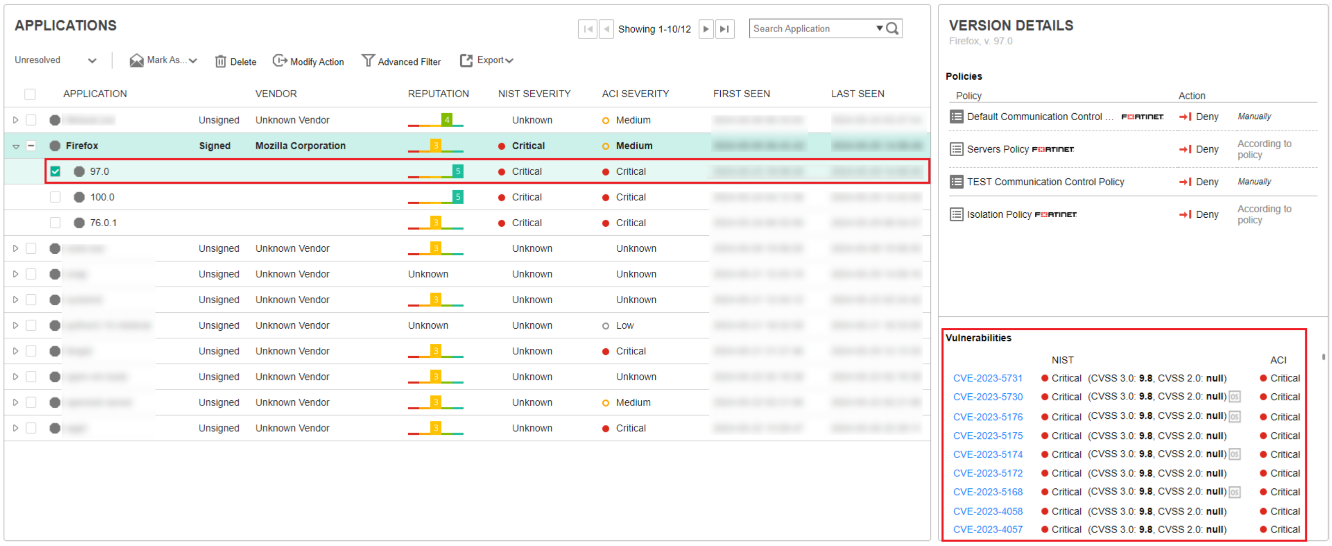
The ratings are only available to users who have purchased the *Discover and Protect* license or the *Discover, Protect and Response* license.

- NIST Severity—Rating provided by FortiEDR's vulnerability scoring system leveraging the NIST Cybersecurity Framework.

- ACI Severity—Adversary Centric Intelligence (ACI) rating provided by FortiRecon leveraging FortiGuard Threat Analysts to provide comprehensive coverage of dark web, open source, and technical threat intelligence, including threat actor insights. This information enables administrators to proactively assess risks, respond faster to incidents, better understand their attackers, and protect assets.

FortiEDR categories vulnerabilities into the following categories based on National Vulnerability Database (NVD) severity ratings:

- Unknown
- Low
- Medium
- High
- Critical



APPLICATION		VENDOR	REPUTATION	NIST SEVERITY	ACI SEVERITY	FIRST SEEN	LAST SEEN
□ [redacted]	Unsigned	Unknown Vendor	4	Unknown	○ Medium	[redacted]	[redacted]
Firefox	**Signed**	**Mozilla Corporation**	3	● **Critical**	○ **Medium**	[redacted]	[redacted]
☑ 97.0			5	● Critical	● Critical	[redacted]	[redacted]
□ 100.0			5	● Critical	● Critical	[redacted]	[redacted]
□ 76.0.1			3	● Critical	● Critical	[redacted]	[redacted]
□ [redacted]	Unsigned	Unknown Vendor	3	Unknown	Unknown	[redacted]	[redacted]
□ [redacted]	Unsigned	Unknown Vendor	Unknown	Unknown	Unknown	[redacted]	[redacted]
□ [redacted]	Unsigned	Unknown Vendor	3	Unknown	Unknown	[redacted]	[redacted]
□ [redacted]	Unsigned	Unknown Vendor	Unknown	Unknown	○ Low	[redacted]	[redacted]
□ [redacted]	Unsigned	Unknown Vendor	3	Unknown	● Critical	[redacted]	[redacted]
□ [redacted]	Unsigned	Unknown Vendor	3	Unknown	Unknown	[redacted]	[redacted]
□ [redacted]	Unsigned	Unknown Vendor	3	Unknown	○ Medium	[redacted]	[redacted]
□ [redacted]	Unsigned	Unknown Vendor	3	Unknown	● Critical	[redacted]	[redacted]

VERSION DETAILS

Firefox, v. 97.0

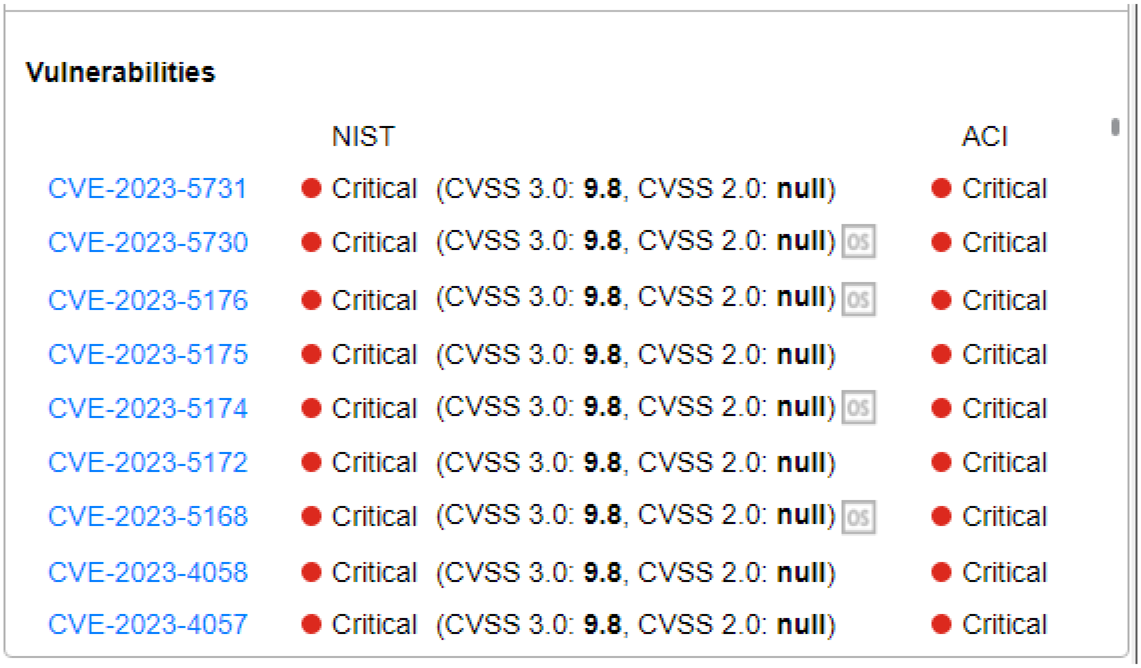
Policies

Policy	Action	
Default Communication Control ... FORTINET	Deny	*Manually*
Servers Policy FORTINET	Deny	According to policy
TEST Communication Control Policy	Deny	*Manually*
Isolation Policy FORTINET	Deny	According to policy

Vulnerabilities

	NIST	ACI
CVE-2023-5731	● Critical (CVSS 3.0: **9.8**, CVSS 2.0: **null**)	● Critical
CVE-2023-5730	● Critical (CVSS 3.0: **9.8**, CVSS 2.0: **null**) OS	● Critical
CVE-2023-5176	● Critical (CVSS 3.0: **9.8**, CVSS 2.0: **null**) OS	● Critical
CVE-2023-5175	● Critical (CVSS 3.0: **9.8**, CVSS 2.0: **null**)	● Critical
CVE-2023-5174	● Critical (CVSS 3.0: **9.8**, CVSS 2.0: **null**) OS	● Critical
CVE-2023-5172	● Critical (CVSS 3.0: **9.8**, CVSS 2.0: **null**)	● Critical
CVE-2023-5168	● Critical (CVSS 3.0: **9.8**, CVSS 2.0: **null**) OS	● Critical
CVE-2023-4058	● Critical (CVSS 3.0: **9.8**, CVSS 2.0: **null**)	● Critical
CVE-2023-4057	● Critical (CVSS 3.0: **9.8**, CVSS 2.0: **null**)	● Critical

The Vulnerabilities area at the bottom right of the window lists the CVE-identified vulnerabilities for the selected application and version. Each CVE row includes the CVE identifier, the NIST and ACI severity category and the Common Vulnerability Scoring System (CVSS) vulnerability score .

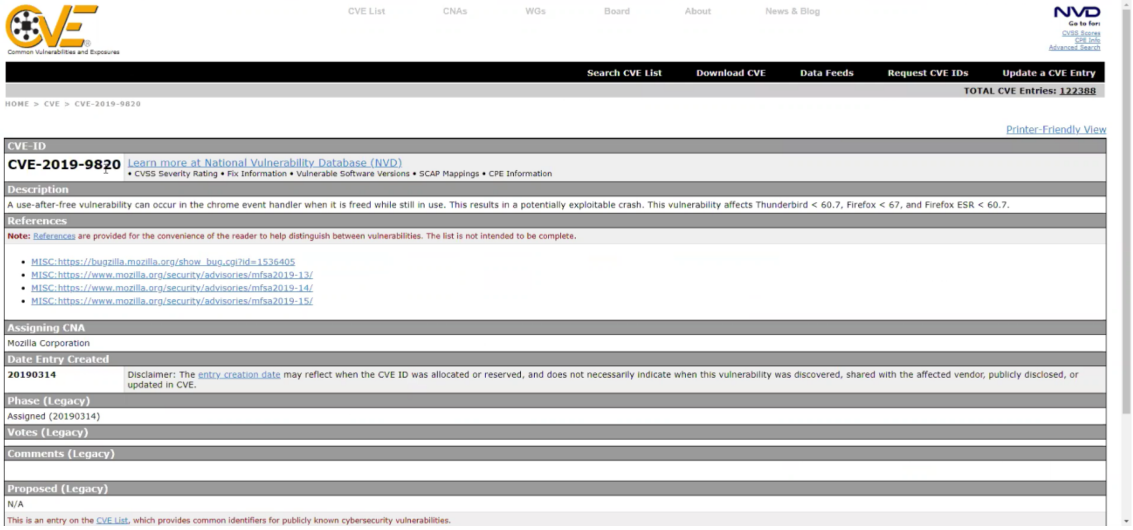


Vulnerabilities

	NIST			ACI
CVE-2023-5731	● Critical	(CVSS 3.0: **9.8**, CVSS 2.0: **null**)		● Critical
CVE-2023-5730	● Critical	(CVSS 3.0: **9.8**, CVSS 2.0: **null**)	OS	● Critical
CVE-2023-5176	● Critical	(CVSS 3.0: **9.8**, CVSS 2.0: **null**)	OS	● Critical
CVE-2023-5175	● Critical	(CVSS 3.0: **9.8**, CVSS 2.0: **null**)		● Critical
CVE-2023-5174	● Critical	(CVSS 3.0: **9.8**, CVSS 2.0: **null**)	OS	● Critical
CVE-2023-5172	● Critical	(CVSS 3.0: **9.8**, CVSS 2.0: **null**)		● Critical
CVE-2023-5168	● Critical	(CVSS 3.0: **9.8**, CVSS 2.0: **null**)	OS	● Critical
CVE-2023-4058	● Critical	(CVSS 3.0: **9.8**, CVSS 2.0: **null**)		● Critical
CVE-2023-4057	● Critical	(CVSS 3.0: **9.8**, CVSS 2.0: **null**)		● Critical

CVSS scoring utilizes two systems: CVSS 3.0, the most recent, and CVSS 2.0, its predecessor. FortiEDR vulnerability information presents both CVSS 3.0 and CVSS 2.0 scores.s

You can click a CVE identifier link to view more details about that vulnerability in your browser, including the type of vulnerability, the application(s) it affects, the version(s) it affects and so on.



TOTAL CVE Entries: 122388

HOME > CVE > CVE-2019-9820

CVE-ID

CVE-2019-9820 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

A use-after-free vulnerability can occur in the chrome event handler when it is freed while still in use. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:https://bugzilla.mozilla.org/show_bug.cgi?id=1536405
- MISC:https://www.mozilla.org/security/advisories/mfsa2019-13/
- MISC:https://www.mozilla.org/security/advisories/mfsa2019-14/
- MISC:https://www.mozilla.org/security/advisories/mfsa2019-15/

Assigning CNA

Mozilla Corporation

Date Entry Created

20190314 Disclaimer: The entry creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20190314)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

N/A

This is an entry on the CVE List, which provides common identifiers for publicly known cybersecurity vulnerabilities.

After a vulnerability is detected in your system, you can decide the type of the action needed to address it. Typically, it is recommended to upgrade to a newer version of the application, meaning one that does not have the identified vulnerability. Alternatively, virtual patching can be applied with vulnerability-based policy that is configured to block communication of any application with known critical vulnerability. For more details, see Policies on page 184. The information presented in the *Advanced Data* area of the window also provides useful information to help protect against vulnerabilities. For more details, see Advanced Data on page 178.

Resolved vs. unresolved applications

By default, all new applications have an Unresolved status. Unresolved means that either FortiEDR or the user have not examined the application to ensure that it is safe. Applications with the Unresolved status are indicated by the ● icon in the application list.

FortiEDR automatically resolves an application as safe by checking the application's characteristics. For example, checking the application's reputation and vulnerabilities to ensure that it does not have a bad reputation or critical vulnerabilities. Applications that meet these criteria are automatically changed to the Resolved status by FortiEDR. Applications with the Resolved status are indicated by the ✓ icon in the application list. You can also change applications to the Resolved status manually.

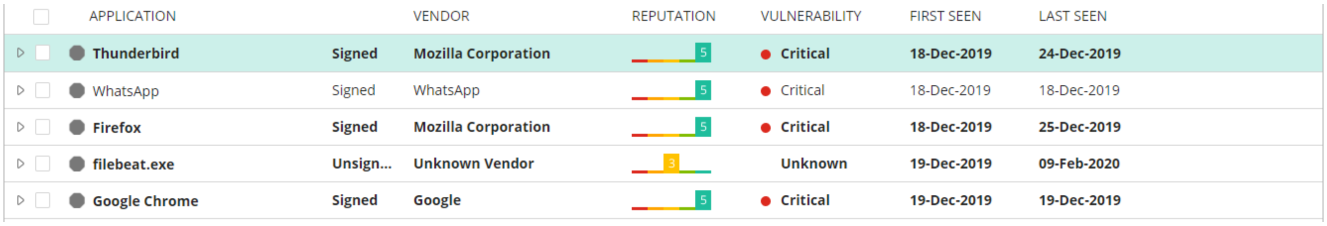
Sorting the Application List

The application list can be sorted alphabetically by product, vendor, reputation score, vulnerability or arrival time (first seen or last seen). By default, the list is sorted by arrival time, with the most recent communication at the top.

Marking an Entry as Read/Unread

The following describes how to specify that you have viewed an entity in the application list. You can mark applications or versions as read/unread.

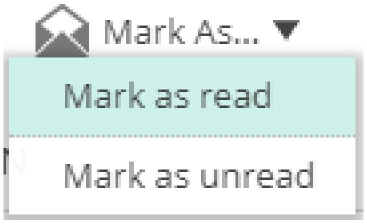
The first time that an application/version is detected in the application list, it is shown in **bold**. **Bold** indicates that the item is unread (see below).



□	APPLICATION		VENDOR	REPUTATION	VULNERABILITY	FIRST SEEN	LAST SEEN
▷ □	● **Thunderbird**	**Signed**	**Mozilla Corporation**	5	● **Critical**	**18-Dec-2019**	**24-Dec-2019**
▷ □	● WhatsApp	Signed	WhatsApp	5	● Critical	18-Dec-2019	18-Dec-2019
▷ □	● **Firefox**	**Signed**	**Mozilla Corporation**	5	● **Critical**	**18-Dec-2019**	**25-Dec-2019**
▷ □	● **filebeat.exe**	**Unsign...**	**Unknown Vendor**	3	**Unknown**	**19-Dec-2019**	**09-Feb-2020**
▷ □	● **Google Chrome**	**Signed**	**Google**	5	● **Critical**	**19-Dec-2019**	**19-Dec-2019**

To mark an entity as read:

Select the entity's (application or version) checkbox and then click the down arrow on the Mark As... ▼ button and select **Mark as read**. The text no longer displays in bold.

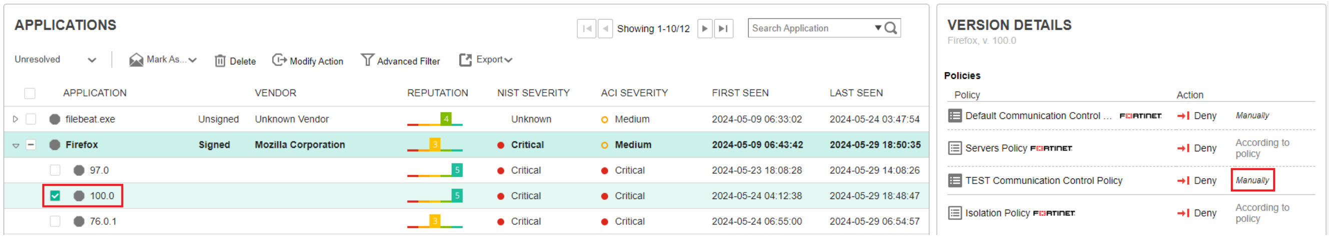


Note – If you mark an application version as read, all lower levels in the version hierarchy for that application are also marked as read.

Modifying a Policy Action

The following describes how to apply a different action to an application/version other than that specified in the current policy for that application/version. In this case, the application/version is excluded from the current action defined in the policy (Allow or Deny).

When modifying a policy action in this manner, the Application/Version Details area displays **Manually** to indicate that the action was modified manually, and is excluded from the action defined in the policy.



APPLICATION		VENDOR	REPUTATION	NIST SEVERITY	ACI SEVERITY	FIRST SEEN	LAST SEEN
▷ □ ● filebeat.exe	Unsigned	Unknown Vendor	4	Unknown	○ Medium	2024-05-09 06:33:02	2024-05-24 03:47:54
▽ ⊟ ● **Firefox**	**Signed**	**Mozilla Corporation**	3	● **Critical**	○ **Medium**	**2024-05-09 06:43:42**	**2024-05-29 18:50:35**
□ ● 97.0			5	● Critical	● Critical	2024-05-23 18:08:28	2024-05-29 14:08:26
☑ ● 100.0			5	● Critical	● Critical	2024-05-24 04:12:38	2024-05-29 18:48:47
□ ● 76.0.1			3	● Critical	● Critical	2024-05-24 06:55:00	2024-05-29 06:54:57

VERSION DETAILS

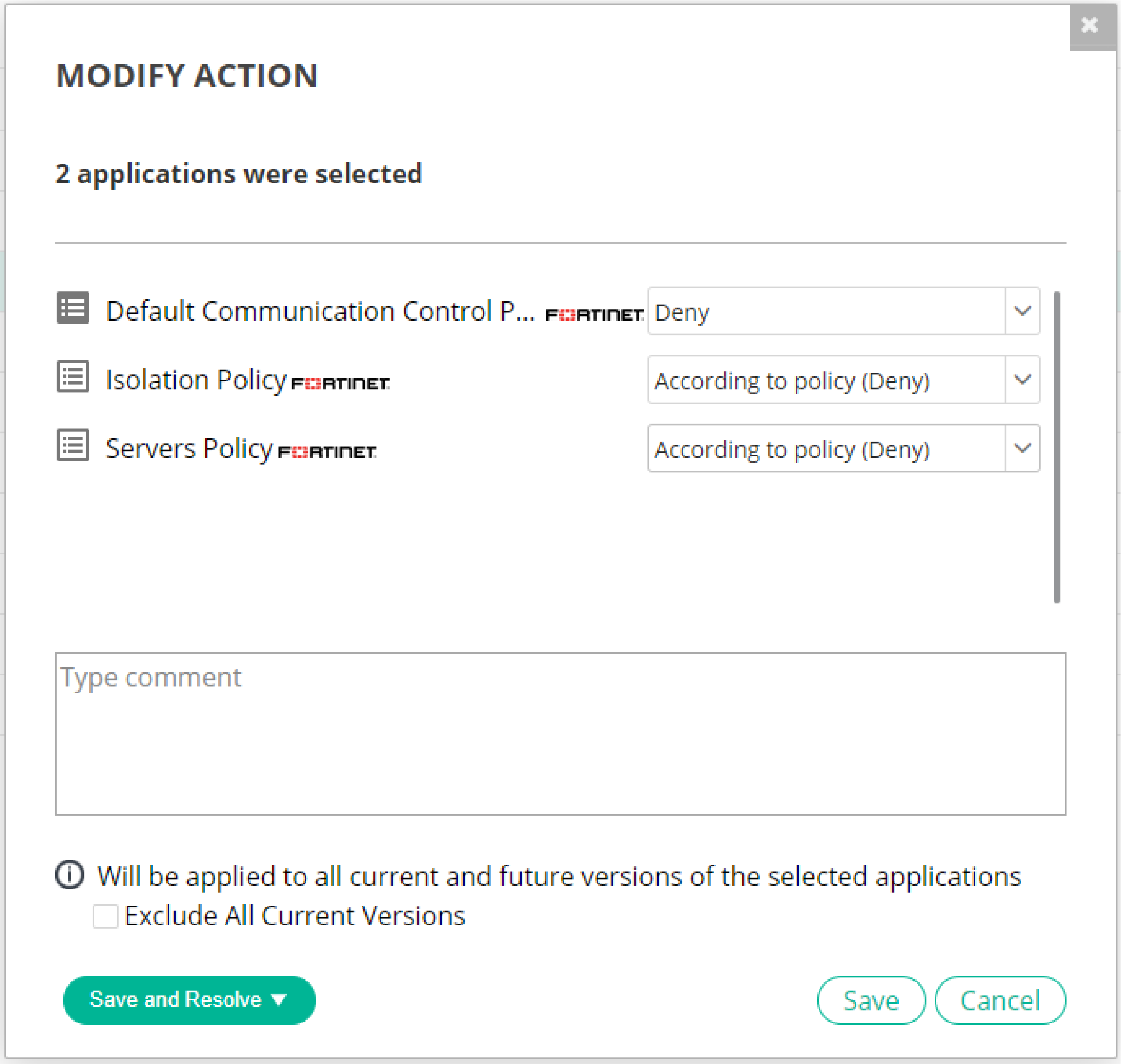
Firefox, v. 100.0

Policies

Policy	Action	
Default Communication Control ...	Deny	*Manually*
Servers Policy	Deny	According to policy
TEST Communication Control Policy	Deny	*Manually*
Isolation Policy	Deny	According to policy

To modify a policy action:

1. Select the application/version checkbox and then click the Modify action button. The Modify Action window displays.



MODIFY ACTION

2 applications were selected

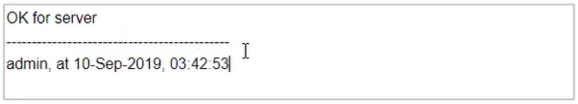
Default Communication Control P... FORTINET	Deny
Isolation Policy FORTINET	According to policy (Deny)
Servers Policy FORTINET	According to policy (Deny)

Type comment

Will be applied to all current and future versions of the selected applications

□ Exclude All Current Versions

2. In the dropdown list on the right of the policy row whose action you want to change, click the down arrow and then select the action to apply to the selected entity. You can change the action for one or more policies.
3. [Optional] In the Comment field, enter a free-text comment describing the action change. By default, the date and time when the policy action was changed automatically displays.



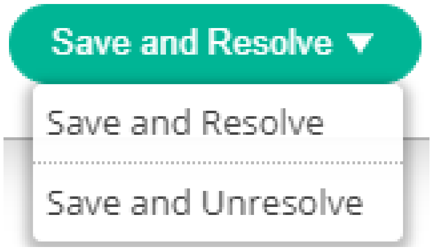
OK for server

----

admin, at 10-Sep-2019, 03:42:53

4. [Optional] Check the Exclude All Current Versions checkbox if you want to exclude existing application versions from the decision. In this case, the new communication control decision only applies to a future version of the product. The application of the policy action change applies for current versions of the application. When this checkbox is not selected, the change is applied to all versions of the application.

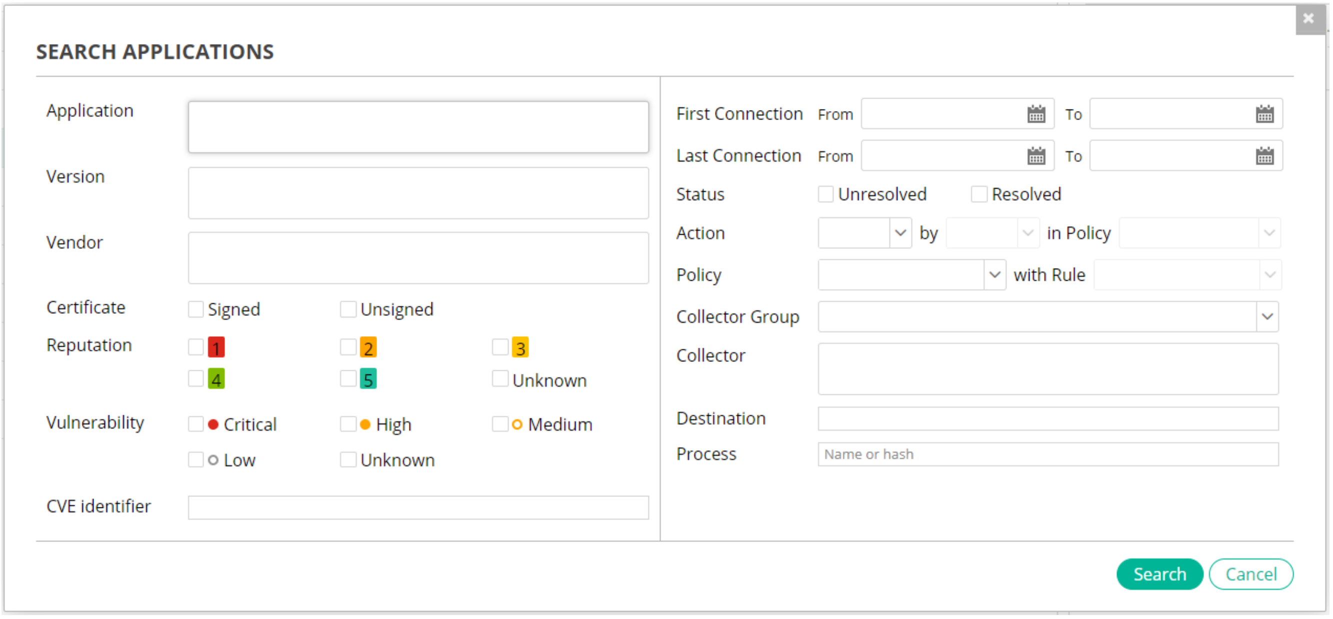
5. Click the arrow next to the button to save the new communication control decision for the selected application(s).



When any FortiEDR Central Manager user marks an application/version as **Resolved**, all users see it as having been resolved. You can also mark an application/version as resolved using the ✓ icon in its row in the application list.

Searching the Application List

You can use the field to perform an advanced search. Click the down arrow to open the Search Applications window, in which you specify your search criteria.



SEARCH APPLICATIONS

Application

Version

Vendor

Certificate □ Signed □ Unsigned

Reputation □ 1 □ 2 □ 3 □ 4 □ 5 □ Unknown

Vulnerability □ ● Critical □ ● High □ ○ Medium □ ○ Low □ Unknown

CVE identifier

First Connection From To

Last Connection From To

Status □ Unresolved □ Resolved

Action by in Policy

Policy with Rule

Collector Group

Collector

Destination

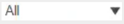
Process Name or hash

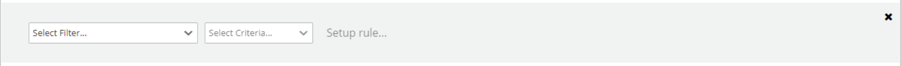
You can filter the application list by the following criteria:

Filter	Criteria
Application	Filters by application name
Version	Filters by version. This is a free-text field.
Vendor	Filters by vendor name.
Certificate	Filters by signed or unsigned certificate.
Reputation	Filters by reputation score. Check the checkbox(es) for the reputation

Filter	Criteria
	score(s) of interest.
Vulnerability	Filters by vulnerability score.
CVE Identifier	Filters by exact match of the vulnerability identifier, using the following format – CVE-YYYY-nnnn.
First Connection / Last Connection	Filters by the specified date range when the first/last connection of the application was detected in the system.
Status	Filters by status (Resolved, Unresolved,).
Action	Filters by action.
In Policy	Filters by policy. If you specify a specific action in the Action field, then you can only select from policies with that specific action.
Policy	Filters by a specific policy.
With Rule	Filters by a specific policy predefined rule.
Collector Group	Filters by the Collector Group used to communicate. This means that a device(s) in the specified Collector Group was used to communicate.
Collector	Filters by the Collector (device) used to communicate.
Destination	Filters by the Collector destination (IP address).
Process (Name/Hash)	Filters by the process name or hash value.

Other options in the Application pane

Option	Function
 All ▾	Click the down arrow in the All ▾ button and then select an option in the dropdown list to filter the application list accordingly. You can filter the list by:
All	Lists all applications for the organization.
Unresolved	Lists applications that have not been resolved by either the user or FortiEDR. Applications with this status are indicated by the ● icon in the application list. This is the default filter.
Resolved	Lists applications that have been resolved by either the user or FortiEDR. Applications with this status are indicated by the ✓ icon in the application list.
Unknown Vendors	Lists applications whose for which the vendor is not known in the system.
Low Reputation	Lists applications with a low reputation score.

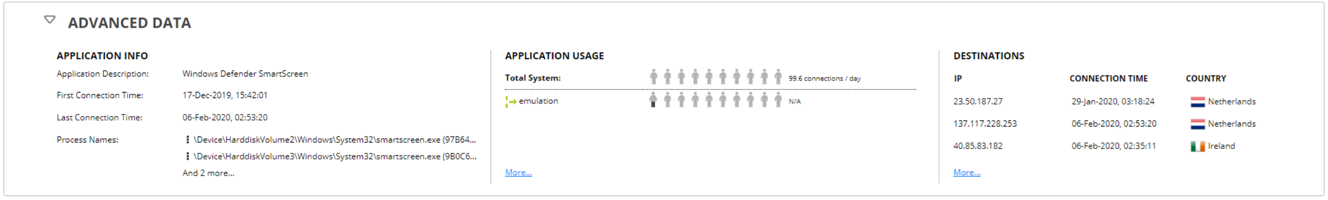
Option	Function
Critical CVE	Lists applications with a Critical CVE score.
Unread	Lists applications that have not yet been viewed in the application list.
Mark As... ▼	Click the down arrow on the Mark As... ▼ button and then select *Mark as read* or *Mark as unread*. For more details, you may refer to the Marking an Entry as Read/Unread on page 173.
Delete	Click to delete the entity selected in the application list. Note that if the deleted entity attempts external communication again, it will be added back to the application list. In this case, any action defined in the policy for this entity must be redefined.
Modify action	Click the button to change the current policy action to be applied for the selected entity, as described in Modifying a Policy Action on page 174
Advanced filter	Click the advanced filter to review applications by suspicious characteristics, such as existing vulnerabilities or reputation score. This filter can be used to set up policy rules. See Policy rules on page 188.  Select Filter... ▾ Select Criteria... ▾ Setup rule... ×
Export ▾	Click the down arrow in the *Export* button (Export ▾ and select the format for exporting data. You can select *Excel* or *JSON*.
Search Application	Use the *Search Application* field to perform an advanced search, as described in Searching the Application List on page 176.

Advanced Data

The Advanced Data area presents statistics about the selected entity in the application list. The information that displays varies, depending on the entity selected (application or version).

Application Advanced Data

When an application is selected in the application list, the *ADVANCED DATA* area displays the following information for it:



ADVANCED DATA

APPLICATION INFO

Application Description: Windows Defender SmartScreen
First Connection Time: 17-Dec-2019, 15:42:01
Last Connection Time: 06-Feb-2020, 02:53:20
Process Names: \Device\HarddiskVolume2\Windows\System32\smartscreen.exe (97B64...
\Device\HarddiskVolume3\Windows\System32\smartscreen.exe (9B0C6...
And 2 more...

APPLICATION USAGE

Total System: 99.6 connections / day
emulation N/A

More...

DESTINATIONS

IP	CONNECTION TIME	COUNTRY
23.50.187.27	29-Jan-2020, 03:18:24	Netherlands
137.117.228.253	06-Feb-2020, 02:53:20	Netherlands
40.85.83.182	06-Feb-2020, 02:35:11	Ireland

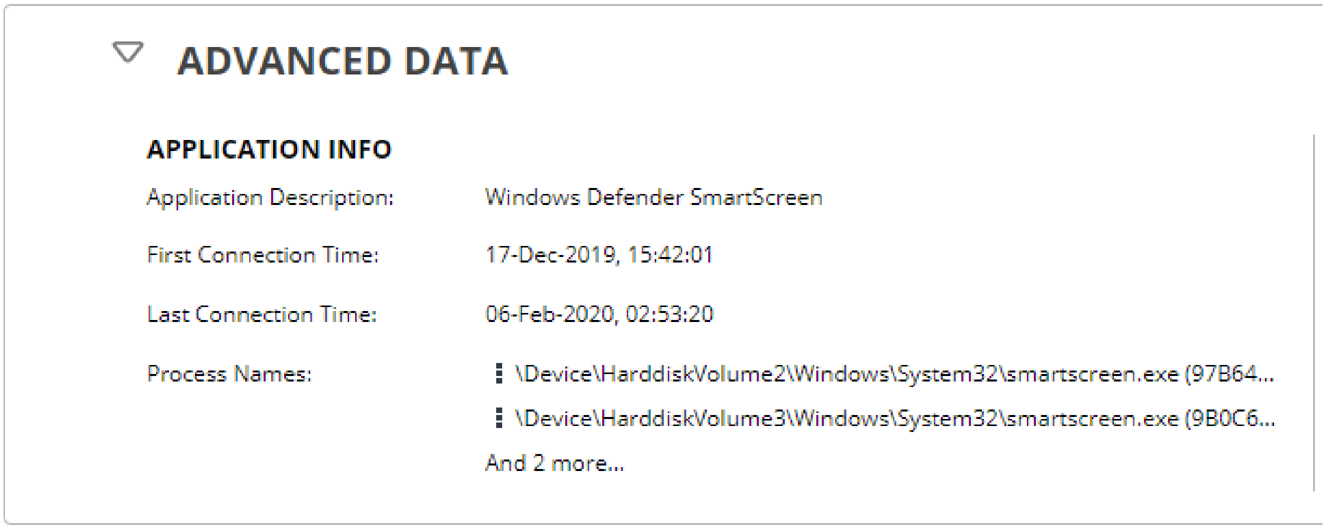
More...

- Application information on page 179
- Application Usage on page 180

- Destinations on page 181

Application information

The *APPLICATION INFO* area displays summary information about the selected application.



APPLICATION INFO

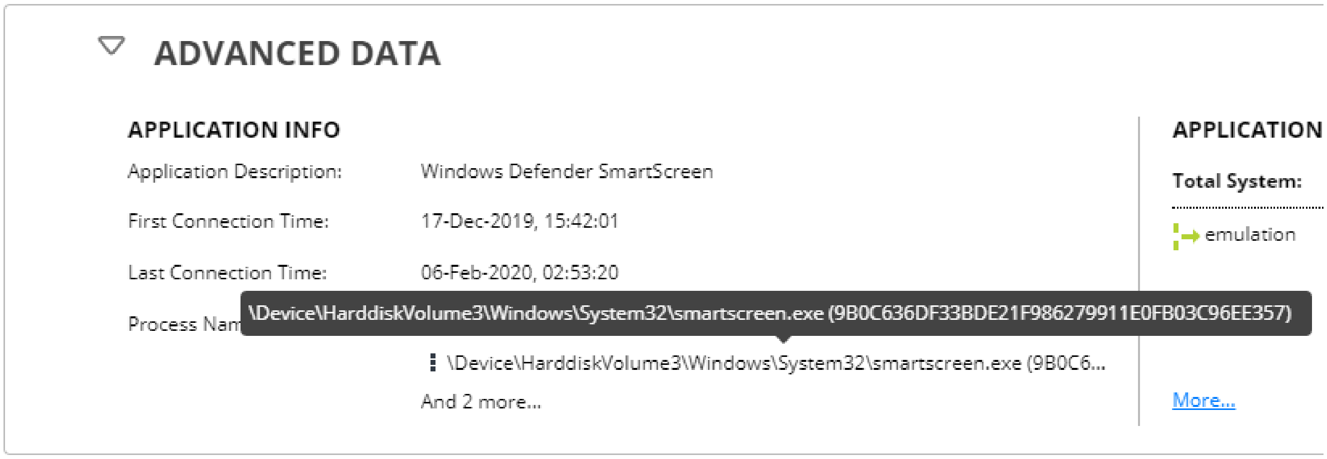
Application Description: Windows Defender SmartScreen

First Connection Time: 17-Dec-2019, 15:42:01

Last Connection Time: 06-Feb-2020, 02:53:20

Process Names: \Device\HarddiskVolume2\Windows\System32\smartscreen.exe (97B64...
\Device\HarddiskVolume3\Windows\System32\smartscreen.exe (9B0C6...
And 2 more...

In the *Process Names* field, a separate row appears for each application that shares the same vendor, product and version properties. The *Process Names* field displays the full file path for each such application.



APPLICATION INFO

Application Description: Windows Defender SmartScreen

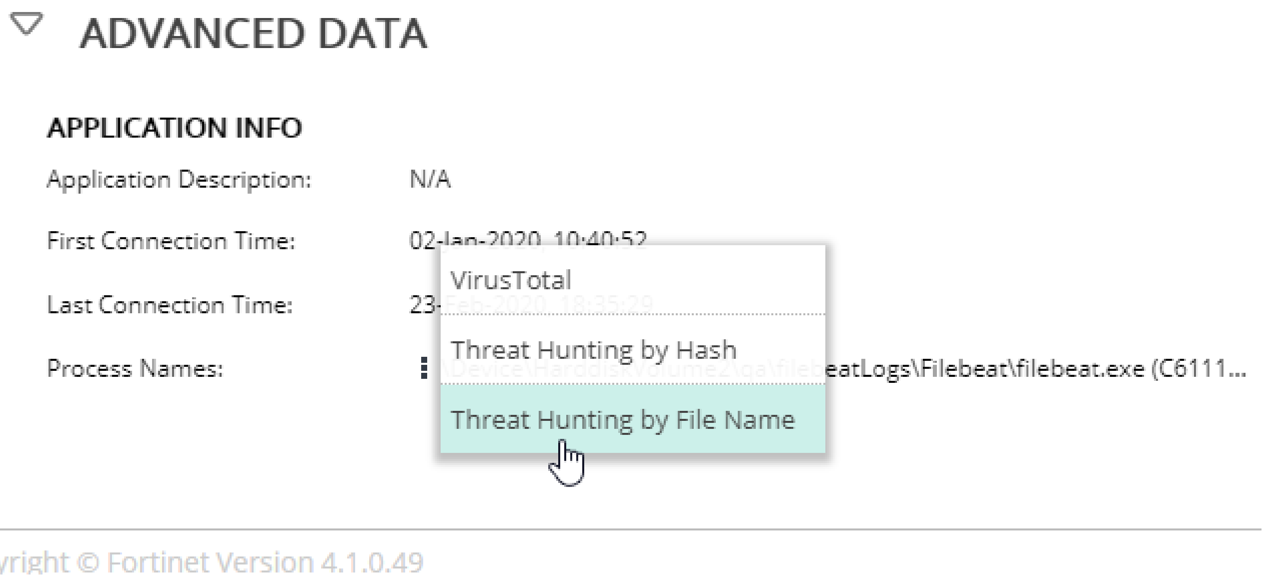
First Connection Time: 17-Dec-2019, 15:42:01

Last Connection Time: 06-Feb-2020, 02:53:20

Process Nam \Device\HarddiskVolume3\Windows\System32\smartscreen.exe (9B0C636DF33BDE21F986279911E0FB03C96EE357)
\Device\HarddiskVolume3\Windows\System32\smartscreen.exe (9B0C6...
And 2 more...

Total System:
emulation

You can click the three dots next to the *Process names* field to navigate to the Threat Hunting window for that process name or hash, or to explore the hash in VirusTotal, as shown below:



ADVANCED DATA

APPLICATION INFO

Application Description: N/A

First Connection Time: 02-Jan-2020, 10:40:52

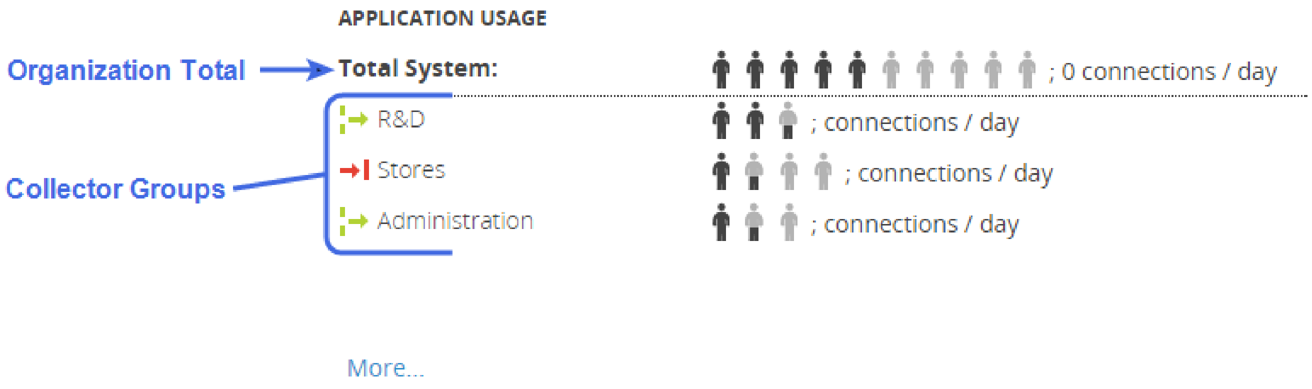
Last Connection Time: 23-Feb-2020, 18:35:29

Process Names: \Device\Harddisk\Volume2\ga\filebeatLogs\Filebeat\filebeat.exe (C6111...

VirusTotal
Threat Hunting by Hash
Threat Hunting by File Name
Copyright © Fortinet Version 4.1.0.49

Application Usage

The *APPLICATION USAGE* area displays details about usage of the selected application.



APPLICATION USAGE

Total System: ; 0 connections / day

R&D ; connections / day

Stores ; connections / day

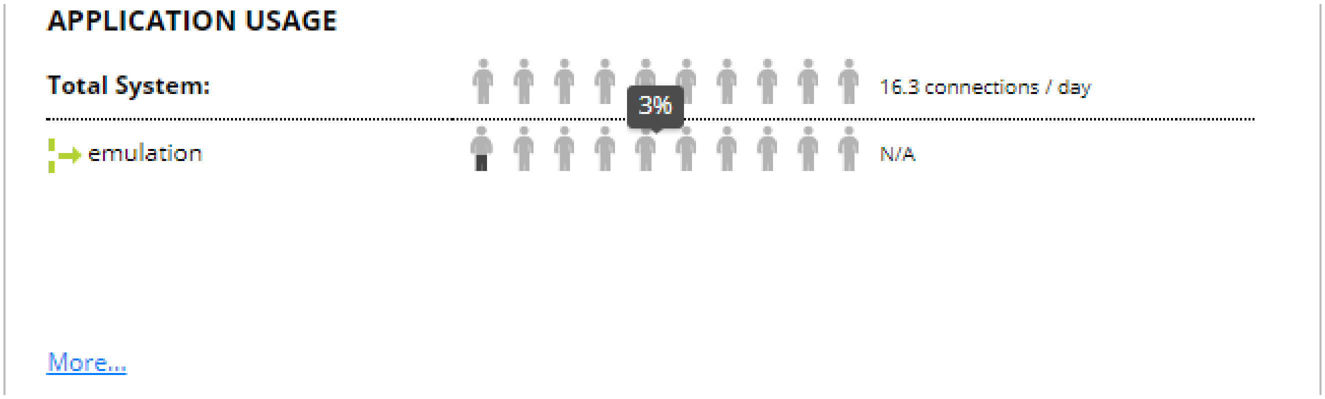
Administration ; connections / day

This area shows the number of connections (communication sessions) per day. The top line shows the total number of devices within the organization on which the selected application is installed.

Each row below the underline represents a different Collector Group, and shows the number of devices in the organization in that Collector Group.

Each person 👤 icon represents 10% of the total devices in the organization/Collector Group. Black 👤 icons represent devices that communicate externally using the selected application, and gray 👤 icons represent devices that did not communicate externally using the application.

You can hover over the people icons to see the percentage of devices that communicate externally per day using the selected application. For example, the figure below shows that only 3% of the devices in the organization have the selected application installed.

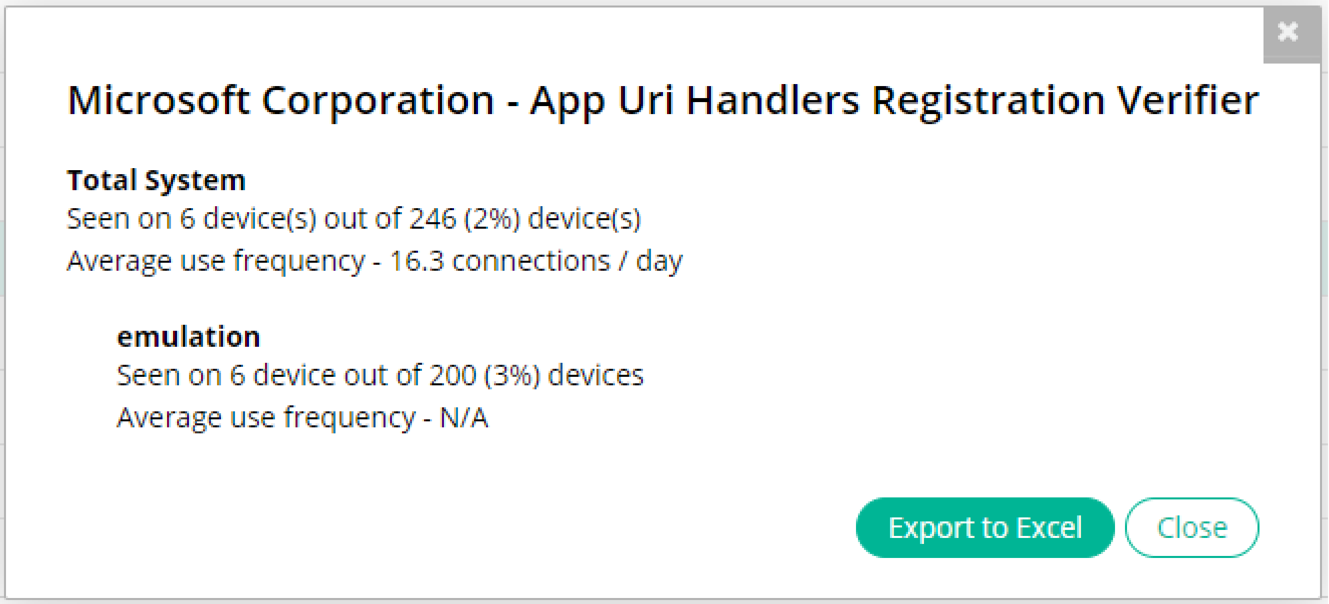


APPLICATION USAGE

Total System: 16.3 connections / day

emulation N/A

Click the *More* link to open the following window, in which you can view additional details about the selected application.



Microsoft Corporation - App Uri Handlers Registration Verifier

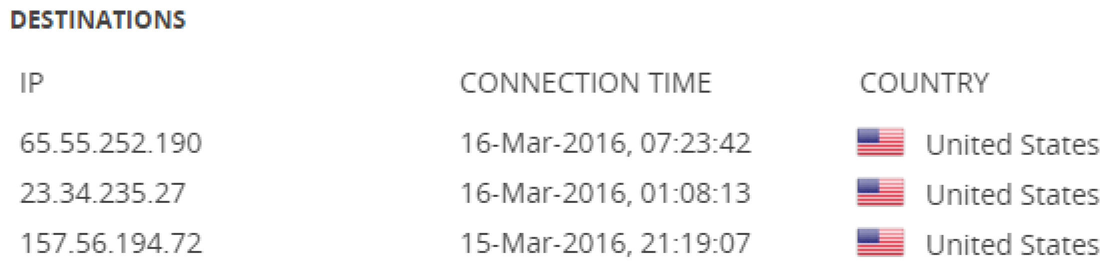
Total System
Seen on 6 device(s) out of 246 (2%) device(s)
Average use frequency - 16.3 connections / day

emulation
Seen on 6 device out of 200 (3%) devices
Average use frequency - N/A

Click the *Export to Excel* button in this window to export application usage information to Excel.

Destinations

The *Destinations* area shows the destinations to which the selected application communicated (Allowed) or attempted to communicate (Denied).

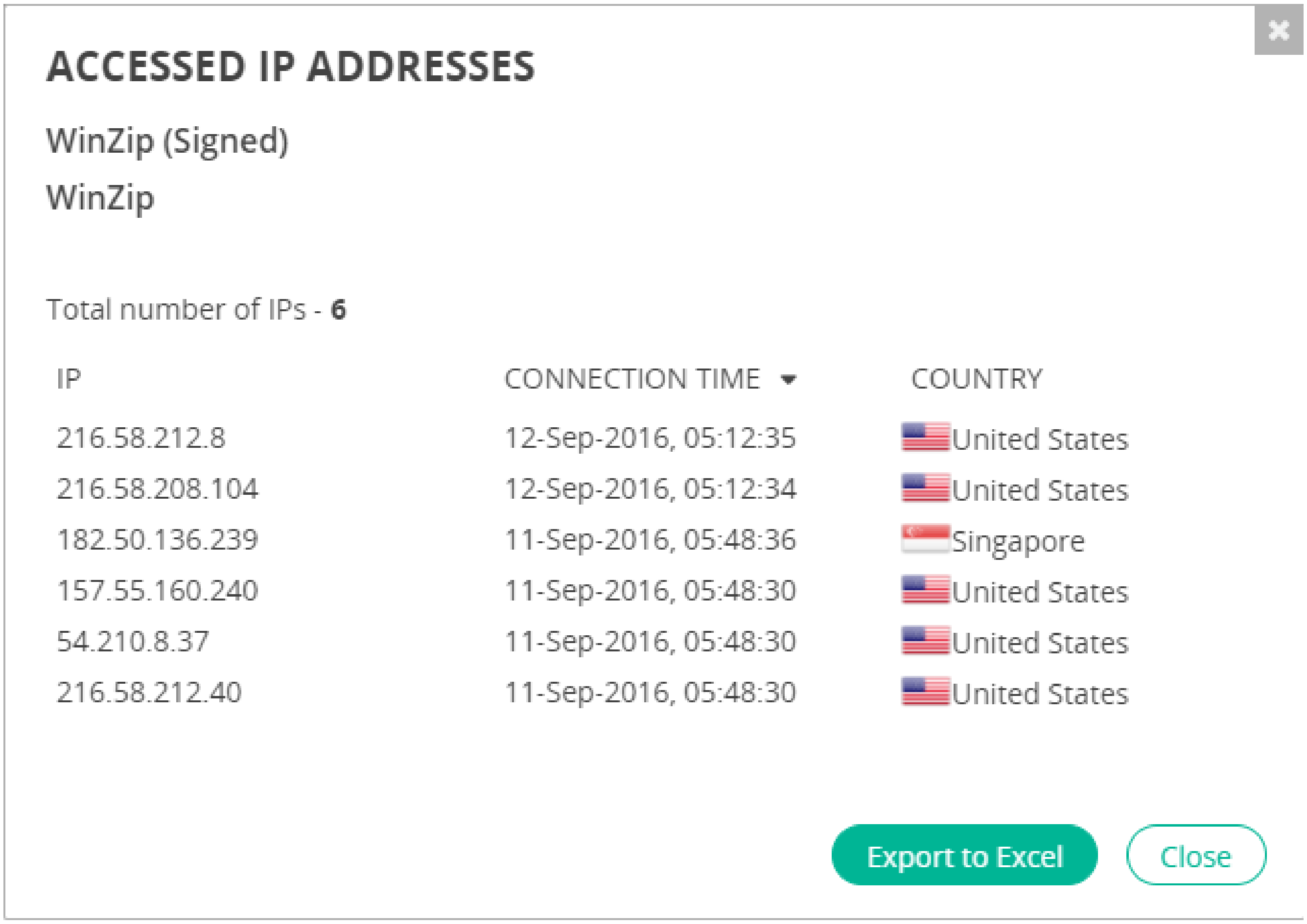


DESTINATIONS

IP	CONNECTION TIME	COUNTRY
65.55.252.190	16-Mar-2016, 07:23:42	United States
23.34.235.27	16-Mar-2016, 01:08:13	United States
157.56.194.72	15-Mar-2016, 21:19:07	United States

Each row shows the IP address, connection time and country of the destination.

By default, this area displays the five most-recent destinations. Click the *More* link to open the following window, which displays the last 50 destinations.



ACCESSED IP ADDRESSES

WinZip (Signed)

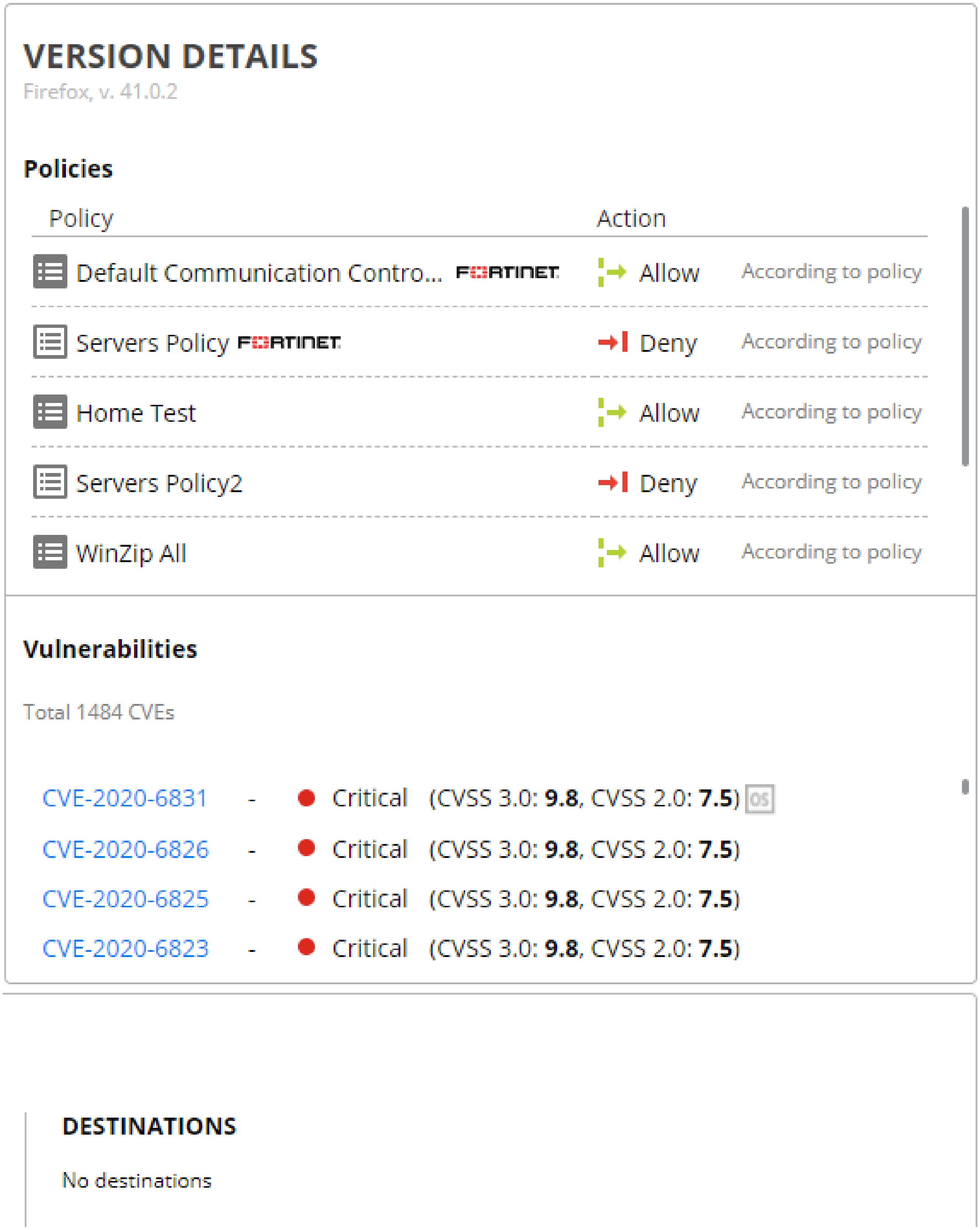
WinZip

Total number of IPs - **6**

IP	CONNECTION TIME ▾	COUNTRY
216.58.212.8	12-Sep-2016, 05:12:35	United States
216.58.208.104	12-Sep-2016, 05:12:34	United States
182.50.136.239	11-Sep-2016, 05:48:36	Singapore
157.55.160.240	11-Sep-2016, 05:48:30	United States
54.210.8.37	11-Sep-2016, 05:48:30	United States
216.58.212.40	11-Sep-2016, 05:48:30	United States

Version Details

The *Version Details* area displays the action defined for the application in each policy, plus its vulnerability details and affected destinations.



VERSION DETAILS

Firefox, v. 41.0.2

Policies

Policy	Action	
Default Communication Contro... FORTINET	Allow	According to policy
Servers Policy FORTINET	Deny	According to policy
Home Test	Allow	According to policy
Servers Policy2	Deny	According to policy
WinZip All	Allow	According to policy

Vulnerabilities

Total 1484 CVEs

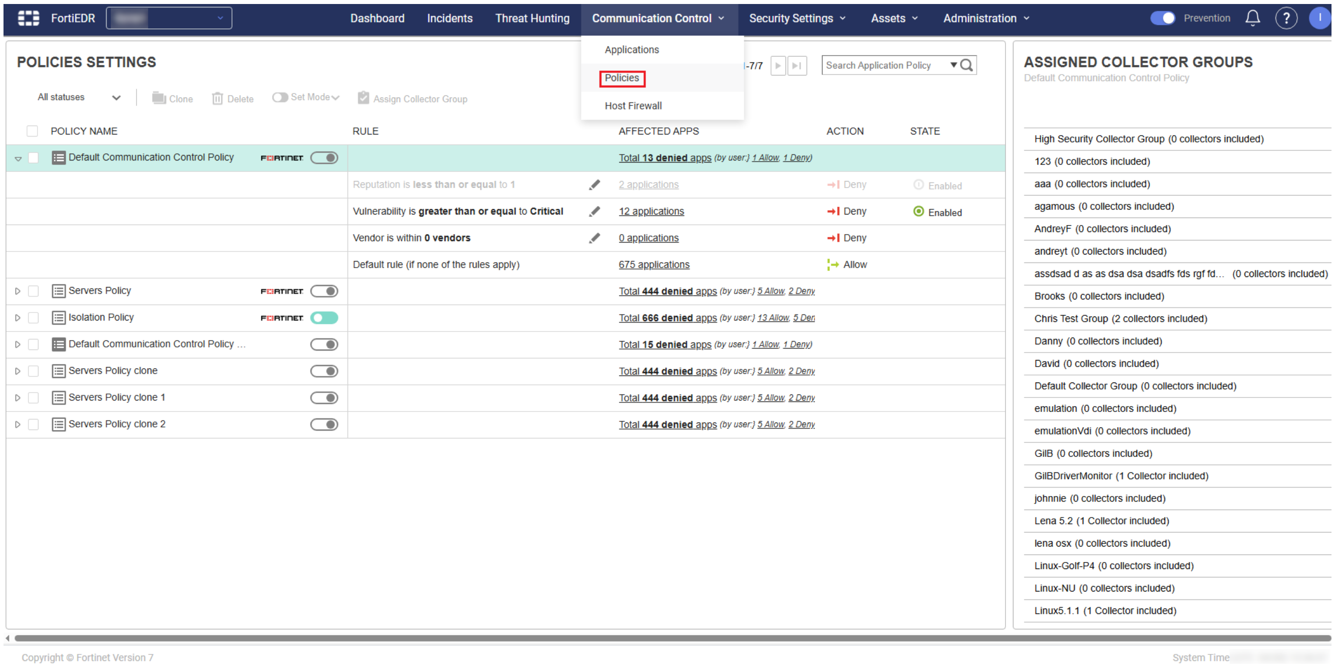
CVE-2020-6831	-	●	Critical	(CVSS 3.0: **9.8**, CVSS 2.0: **7.5**) OS
CVE-2020-6826	-	●	Critical	(CVSS 3.0: **9.8**, CVSS 2.0: **7.5**)
CVE-2020-6825	-	●	Critical	(CVSS 3.0: **9.8**, CVSS 2.0: **7.5**)
CVE-2020-6823	-	●	Critical	(CVSS 3.0: **9.8**, CVSS 2.0: **7.5**)

DESTINATIONS

No destinations

Policies

The *POLICY SETTINGS* page displays the Communication Control policies that can be applied to an application or version in the application list. Communication Control has its own policies. Each policy row can be expanded to show the rules for that policy. To access this page, click the down arrow next to *COMMUNICATION CONTROL* and then select the Policies.



POLICIES SETTINGS

POLICY NAME	RULE	AFFECTED APPS	ACTION	STATE
Default Communication Control Policy FORTINET		Total **13 denied** apps *(by user:} 1 Allow, 1 Deny)*		
	Reputation is **less than or equal** to **1**	2 applications	Deny	Enabled
	Vulnerability is **greater than or equal** to **Critical**	12 applications	Deny	Enabled
	Vendor is within **0 vendors**	0 applications	Deny	
	Default rule (if none of the rules apply)	675 applications	Allow	
Servers Policy FORTINET		Total **444 denied** apps *(by user:} 5 Allow, 2 Deny*		
Isolation Policy FORTINET		Total **666 denied** apps *(by user:} 13 Allow, 5 Den*		
Default Communication Control Policy ...		Total **15 denied** apps *(by user:} 1 Allow, 1 Deny)*		
Servers Policy clone		Total **444 denied** apps *(by user:} 5 Allow, 2 Deny*		
Servers Policy clone 1		Total **444 denied** apps *(by user:} 5 Allow, 2 Deny*		
Servers Policy clone 2		Total **444 denied** apps *(by user:} 5 Allow, 2 Deny*		

ASSIGNED COLLECTOR GROUPS

Default Communication Control Policy

- High Security Collector Group (0 collectors included)
- 123 (0 collectors included)
- aaa (0 collectors included)
- agamous (0 collectors included)
- AndreyF (0 collectors included)
- andreyt (0 collectors included)
- assdsad d as as dsa dsa dsadfs fds rgf fd... (0 collectors included)
- Brooks (0 collectors included)
- Chris Test Group (2 collectors included)
- Danny (0 collectors included)
- David (0 collectors included)
- Default Collector Group (0 collectors included)
- emulation (0 collectors included)
- emulationVdi (0 collectors included)
- GilB (0 collectors included)
- GilBDriverMonitor (1 Collector included)
- johnnie (0 collectors included)
- Lena 5.2 (1 Collector included)
- lena osx (0 collectors included)
- Linux-Golf-P4 (0 collectors included)
- Linux-NU (0 collectors included)
- Linux5.1.1 (1 Collector included)

Copyright © Fortinet Version 7

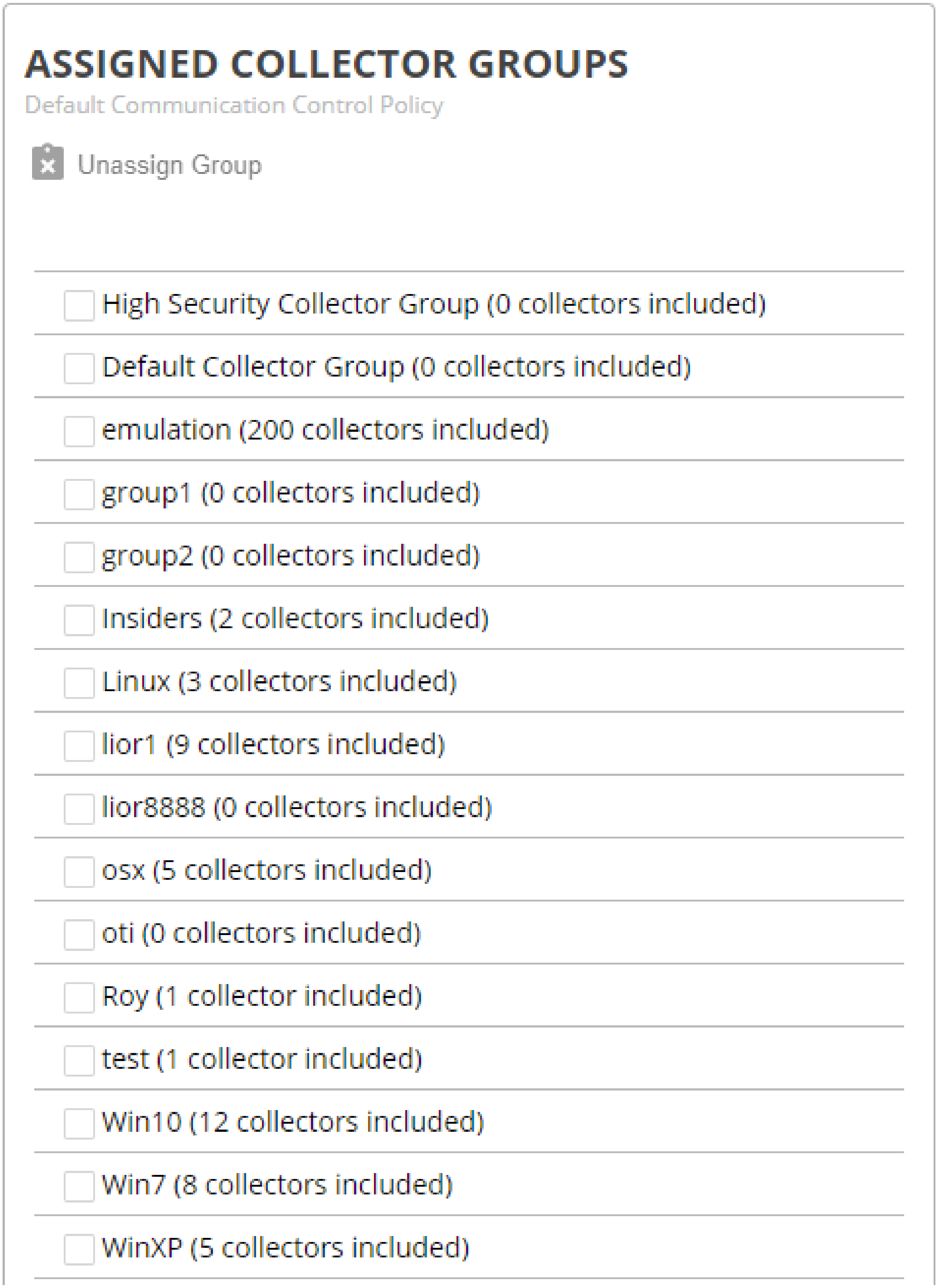
System Time [redacted]

Communication Control policies define the actions to be taken for a given application or application version. Each policy applies to a different Collector Group(s), and all the devices that belong to that Collector Group (s). A Collector Group can only be assigned to one policy.

The following information is defined for each communication policy:

Information Field	Description
Policy Name	The policy name appears in the leftmost column. The policy name is defined when the policy is created.
Rule	The rule as it applies to the policy. The default action for the policy is displayed under the default rule of the policy. For more details, see the Policy rules on page 188.
Affected Apps	The number of applications affected by the policy.
Action	Specifies the action that is enforced when this rule is violated (Allow or Deny).
State (Enabled/Disabled)	This option enables you to disable/enable this rule.

The Assigned Collector Groups area on the right lists the Collector Group(s) assigned to the policy.



ASSIGNED COLLECTOR GROUPS

Default Communication Control Policy

Unassign Group

- □ High Security Collector Group (0 collectors included)
- □ Default Collector Group (0 collectors included)
- □ emulation (200 collectors included)
- □ group1 (0 collectors included)
- □ group2 (0 collectors included)
- □ Insiders (2 collectors included)
- □ Linux (3 collectors included)
- □ lior1 (9 collectors included)
- □ lior8888 (0 collectors included)
- □ osx (5 collectors included)
- □ oti (0 collectors included)
- □ Roy (1 collector included)
- □ test (1 collector included)
- □ Win10 (12 collectors included)
- □ Win7 (8 collectors included)
- □ WinXP (5 collectors included)

Predefined policies

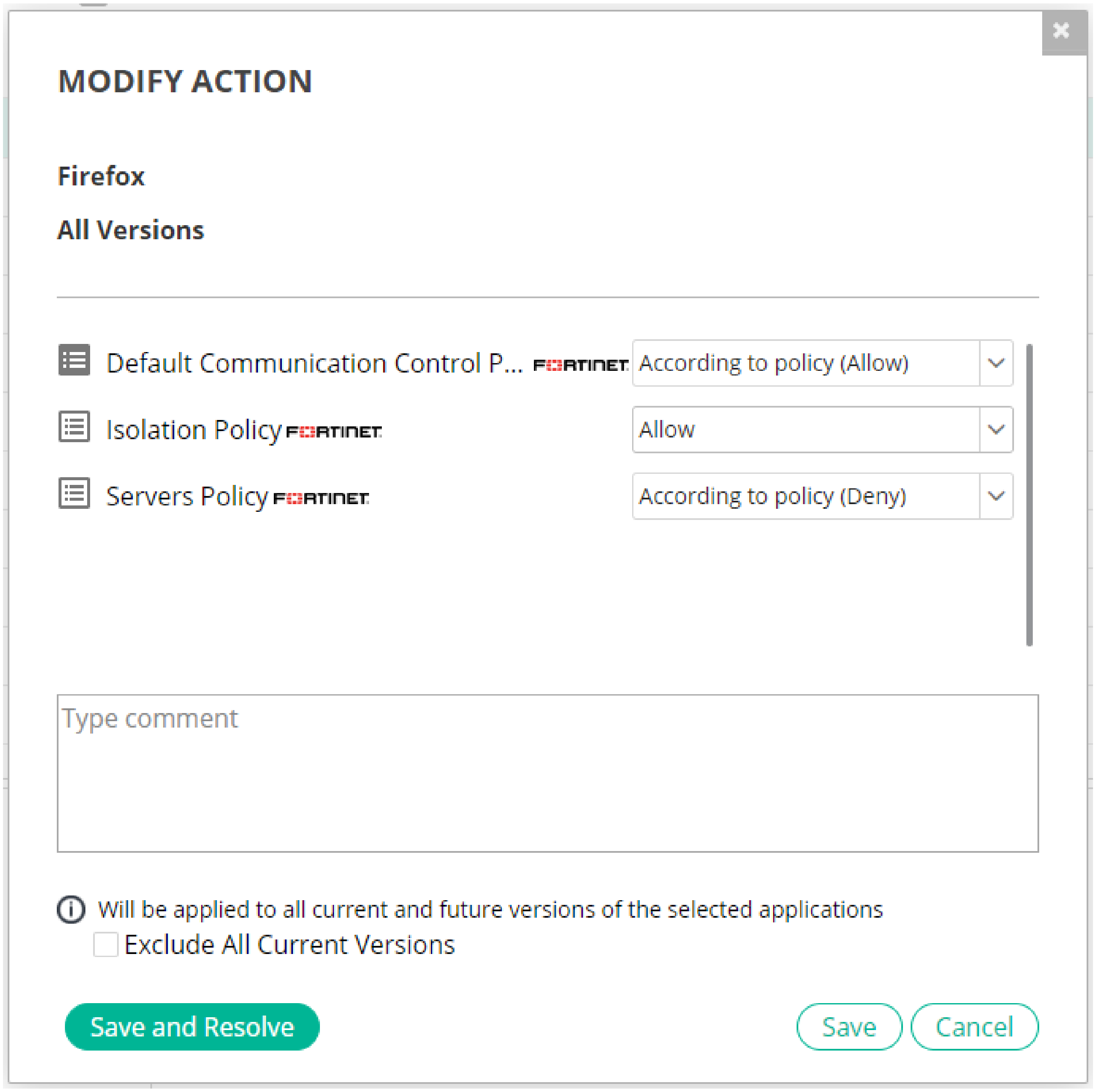
FortiEDR is provided out-of-the-box with several predefined policies, ready for you to get started. These policies are marked with the FORTINET logo.

- The Default Communication Control policy is one such policy, and is always listed first in the list of policies. The Default Communication Control policy is a blocklisting policy that is automatically applied to any Collector Group that is not assigned to any of the other Communication Control policies.
- The *Servers* predefined policy is an allowlist policy that assigns a Deny action to all applications by default, except for a list of known, recognized and legitimate applications, which are allowed. This policy gives your organization a jump-start, as some of the leg work to identify legitimate applications in your organization has already been done for you.
- The Isolation predefined policy isolates (blocks) communication to/from a device. This policy cannot be deleted and only applies in Prevention mode. When this policy is in force and communication for a given device has been blocked, you can manually permit communication to/from the device for a specific application using the procedure below.

To permit communication to/from the device for a specific application:

1. Select the *APPLICATIONS* page.
2. Select the application/version to which you want to permit communication.

3. Click the *Modify Action* button. The following displays:



MODIFY ACTION

Firefox

All Versions

Default Communication Control P... FORTINET	According to policy (Allow)
Isolation Policy FORTINET	Allow
Servers Policy FORTINET	According to policy (Deny)

Type comment

Will be applied to all current and future versions of the selected applications

□ Exclude All Current Versions

4. In the *Isolation Policy* row, select *Allow* in the dropdown menu.

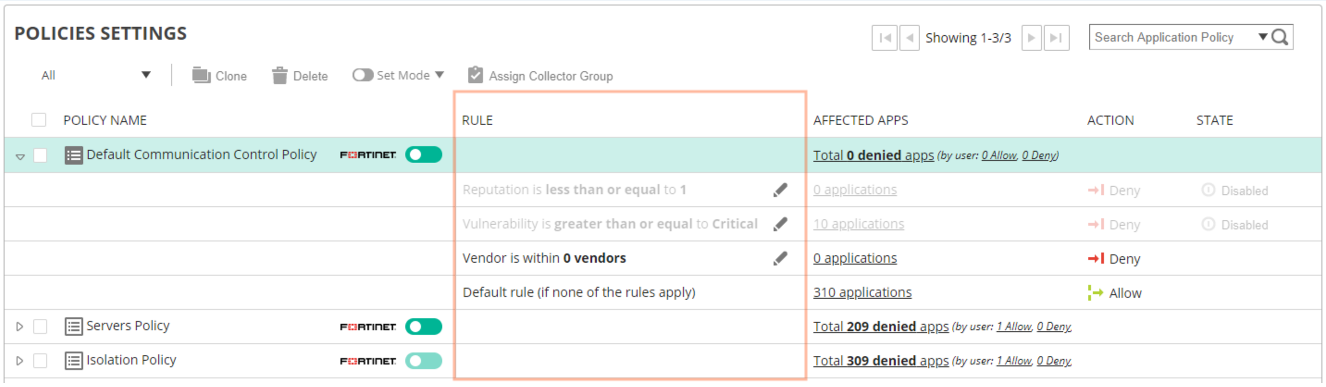
Policy mode

The slider for a policy indicates the current mode for the policy. A green slider indicates Prevention mode and a gray slider indicates Simulation mode. You can change the mode using the *Set mode* (

Set mode ▾) button at the top of the *Policies* pane. For more details about these modes, you may refer to Protection or Simulation mode on page 198.

Policy rules

For each communication policy, FortiEDR provides four rules out of the box. These rules can be modified to specify the connections to be blocked/unblocked according to several parameters. FortiEDR provides the following communication policy rules:



POLICIES SETTINGS

Showing 1-3/3 | Search Application Policy

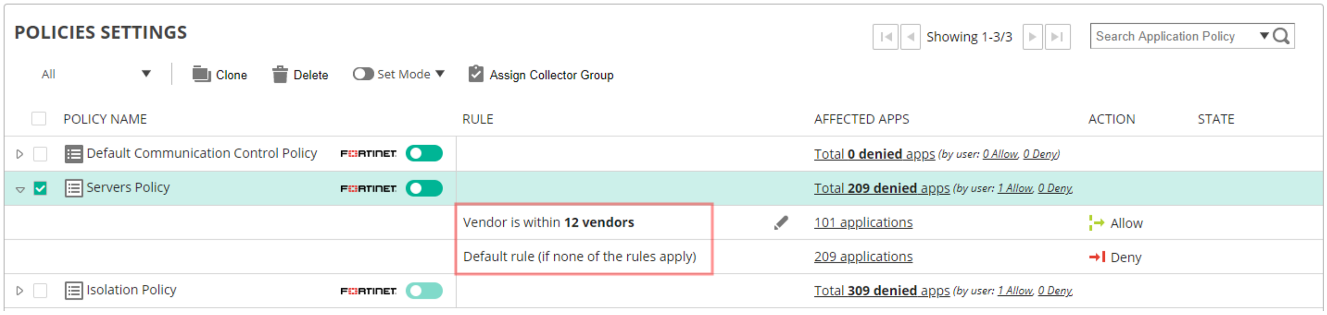
All ▾ | Clone | Delete | Set Mode ▾ | Assign Collector Group

POLICY NAME		RULE	AFFECTED APPS	ACTION	STATE
Default Communication Control Policy	FORTINET		Total 0 denied apps (by user: 0 Allow, 0 Deny)		
		Reputation is less than or equal to 1	0 applications	Deny	Disabled
		Vulnerability is greater than or equal to Critical	10 applications	Deny	Disabled
		Vendor is within 0 vendors	0 applications	Deny	
		Default rule (if none of the rules apply)	310 applications	Allow	
Servers Policy	FORTINET		Total 209 denied apps (by user: 1 Allow, 0 Deny		
Isolation Policy	FORTINET		Total 309 denied apps (by user: 1 Allow, 0 Deny		

Policy Rule	Description
Default rule	This rule applies when none of the other three rules apply.
Reputation is less than or equal to X	This rule enables FortiEDR to block/unblock by reputation score.
Vendor is within X vendors	This rule enables FortiEDR to block/unblock by vendor. For this rule, you specify the vendor(s) to include and to exclude.
Vulnerability is greater than or equal to X	This rule enables FortiEDR to block/unblock by vulnerability. In the rules, X represents a user-defined value.

In the rules, **X** represents a user-defined value.

For example, the figure below shows that the Servers Policy has the following rules defined for it:



POLICIES SETTINGS

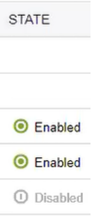
Showing 1-3/3 | Search Application Policy

All ▾ | Clone | Delete | Set Mode ▾ | Assign Collector Group

POLICY NAME		RULE	AFFECTED APPS	ACTION	STATE
Default Communication Control Policy	FORTINET		Total 0 denied apps (by user: 0 Allow, 0 Deny)		
☑ Servers Policy	FORTINET		Total 209 denied apps (by user: 1 Allow, 0 Deny		
		Vendor is within 12 vendors	101 applications	Allow	
		Default rule (if none of the rules apply)	209 applications	Deny	
Isolation Policy	FORTINET		Total 309 denied apps (by user: 1 Allow, 0 Deny		

- Vendor is within 12 vendors. This rule is enabled for the policy. The action for this rule is Allow.
- Default rule (if none of the rules apply). This rule is always enabled.

You can enable or disable a rule for a policy by clicking the Enabled/Disabled button in the State column of the applicable rule. This button toggles between **Enabled/Disabled**.



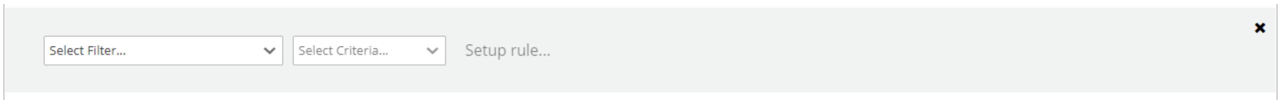
STATE
● Enabled
● Enabled
○ Disabled

Editing a policy rule

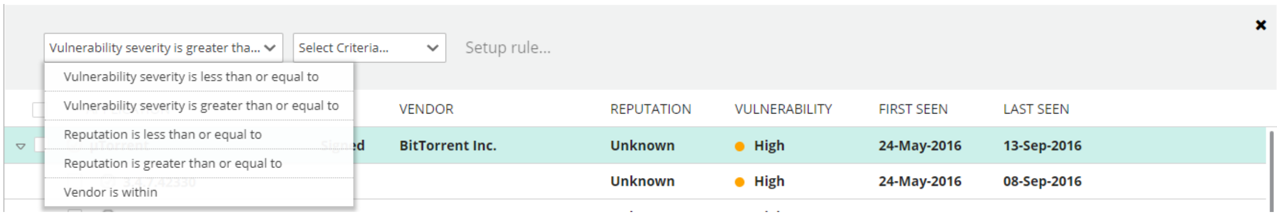
The four rules for a policy can be modified, as needed.

To edit a rule:

1. Click the *Edit* (✎) button for the rule of the policy that you want to modify. This switches the view to the *APPLICATIONS* page, enabling you to review the applications affected by this rule before saving it. The following displays:

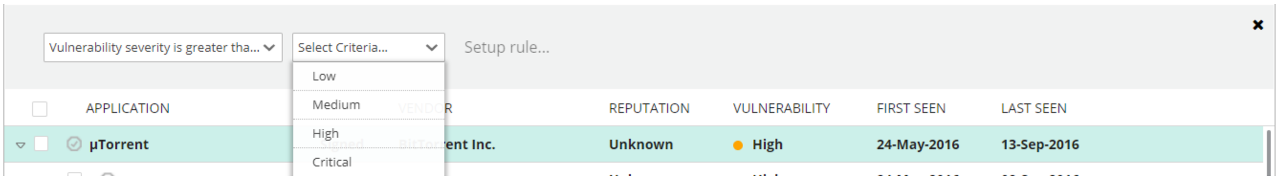


2. In the *Select Filter* dropdown list, select the parameter whose value you want to set in the rule. This dropdown list lists the parameters available to configure for the rule.


Vulnerability severity is greater tha...
Select Criteria...
Setup rule...
×
Vulnerability severity is less than or equal to
Vulnerability severity is greater than or equal to
Reputation is less than or equal to
Reputation is greater than or equal to
Vendor is within

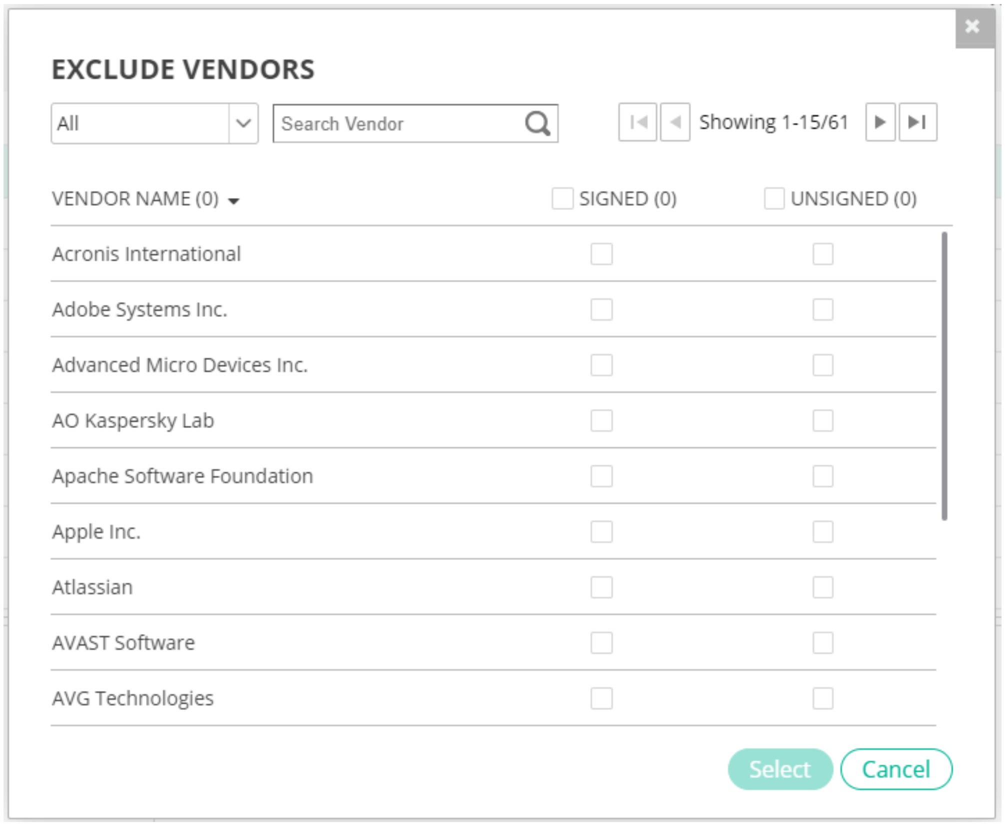
VENDOR	REPUTATION	VULNERABILITY	FIRST SEEN	LAST SEEN
BitTorrent Inc.	Unknown	● High	24-May-2016	13-Sep-2016
	Unknown	● High	24-May-2016	08-Sep-2016

3. In the rightmost *Select Criteria* dropdown list, select the value for the parameter. This dropdown list lists the values available to configure for the parameter specified in step 2.



APPLICATION	VENDOR	REPUTATION	VULNERABILITY	FIRST SEEN	LAST SEEN
µTorrent	...ent Inc.	Unknown	● High	24-May-2016	13-Sep-2016

When modifying the Vendor is within X vendors rule, you specify the vendor(s) to include and those to exclude for the rule.

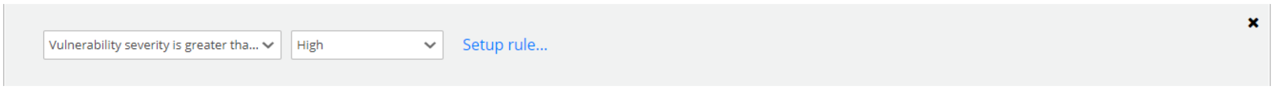


EXCLUDE VENDORS

All | Search Vendor | Showing 1-15/61

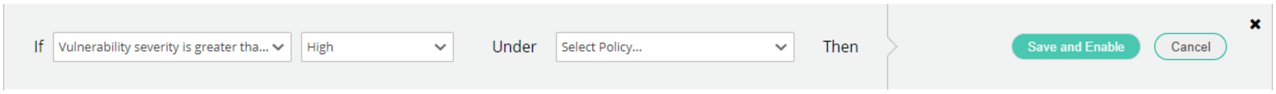
VENDOR NAME (0)	□ SIGNED (0)	□ UNSIGNED (0)
Acronis International	□	□
Adobe Systems Inc.	□	□
Advanced Micro Devices Inc.	□	□
AO Kaspersky Lab	□	□
Apache Software Foundation	□	□
Apple Inc.	□	□
Atlassian	□	□
AVAST Software	□	□
AVG Technologies	□	□

4. Click the *Setup rule* link.



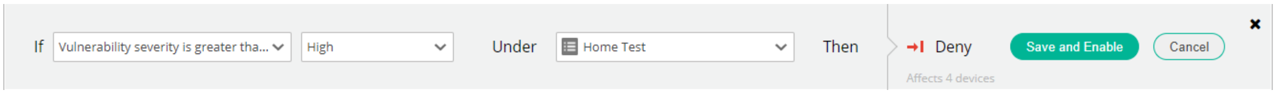
Vulnerability severity is greater tha... | High | Setup rule...

5. In the *Under* dropdown list, select the policy to which this rule applies.



If Vulnerability severity is greater tha... | High | Under Select Policy... | Then

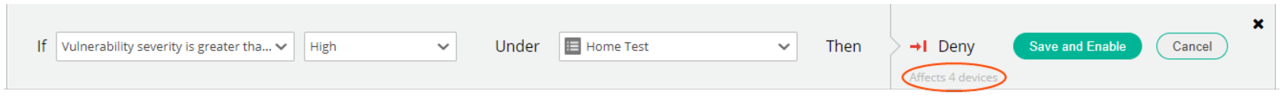
6. In the *Then* field, specify whether to Allow or Deny the application based on this rule.



If Vulnerability severity is greater tha... | High | Under Home Test | Then Deny

Affects 4 devices

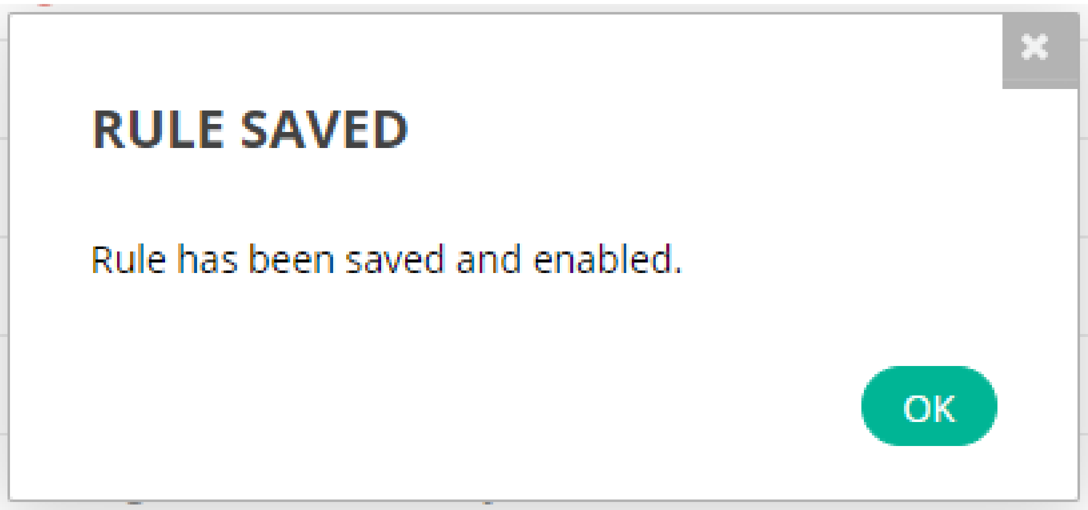
The application list now shows the number of application(s) affected by the rule change.



If Vulnerability severity is greater tha... | High | Under Home Test | Then Deny

Affects 4 devices

7. Click the *Save and Enable* button to save and enable the changes to the rule. A confirmation window displays, confirming the rule change.



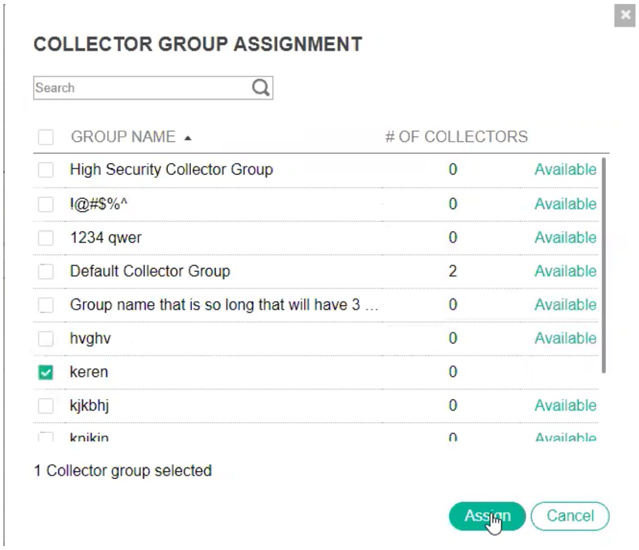
RULE SAVED

Rule has been saved and enabled.

8. Click *OK*.

Assigning a policy to a Collector Group

1. Check the policy that you want to change in the policy list and then click the*Assign Collector Group* button. The following displays:



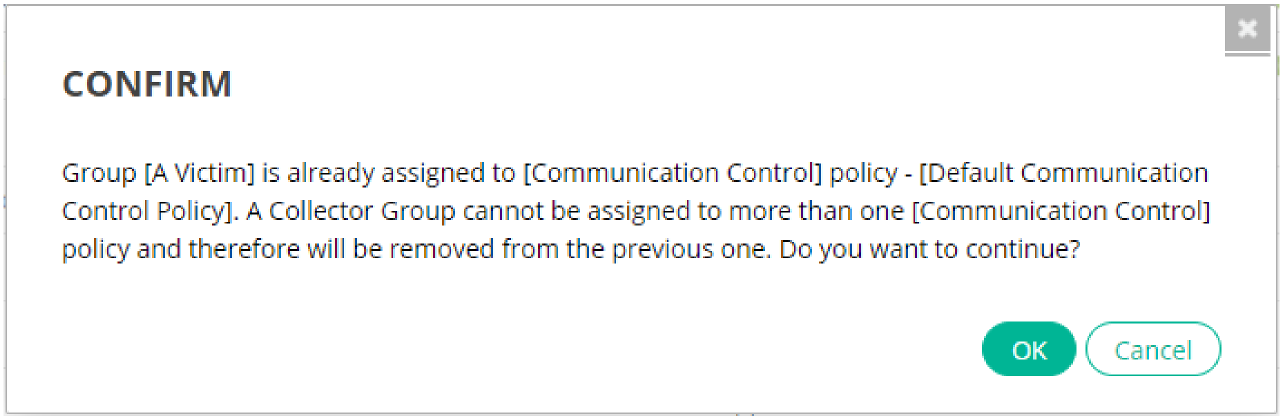
COLLECTOR GROUP ASSIGNMENT

	GROUP NAME ▲	# OF COLLECTORS	
□	High Security Collector Group	0	Available
□	!@#$%^	0	Available
□	1234 qwer	0	Available
□	Default Collector Group	2	Available
□	Group name that is so long that will have 3 ...	0	Available
□	hvghv	0	Available
☑	keren	0	
□	kjkbhj	0	Available
□	knikin	0	Available

1 Collector group selected

2. Check the checkbox of the Collector Group you want to assign to the policy.

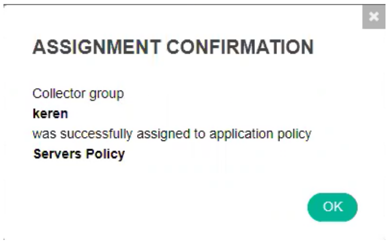
3. Click *Assign*. A window displays, prompting you to confirm the reassignment.



CONFIRM

Group [A Victim] is already assigned to [Communication Control] policy - [Default Communication Control Policy]. A Collector Group cannot be assigned to more than one [Communication Control] policy and therefore will be removed from the previous one. Do you want to continue?

4. Click *OK*. The following displays:



ASSIGNMENT CONFIRMATION

Collector group
keren
was successfully assigned to application policy
Servers Policy

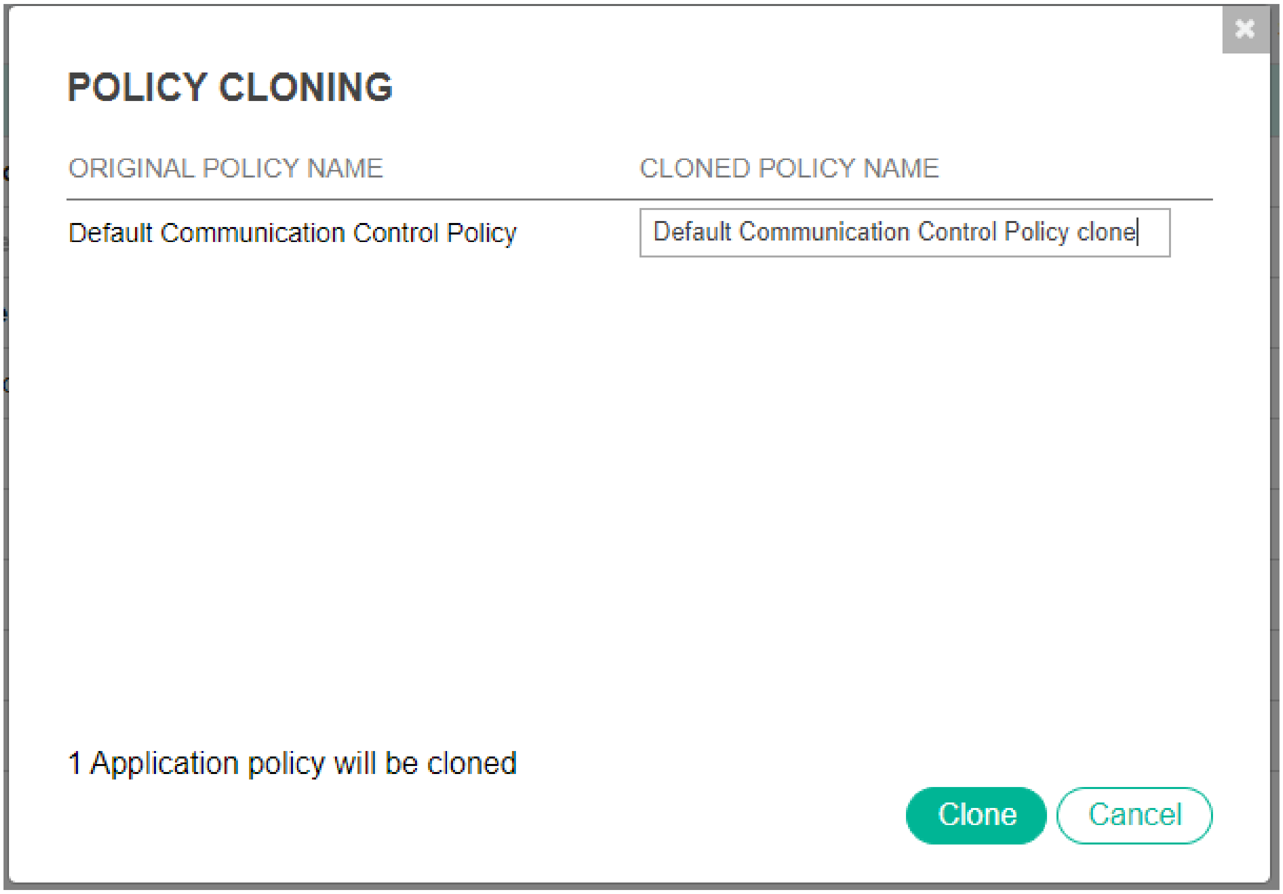
5. Click *OK*.

Creating a new Communication Control policy

A new Communication Control policy can be created by cloning an existing policy, as described below. New policies are only needed if you are going to assign different policies to different Collector Groups. Otherwise, you can simply modify one of the default policies that come out-of-the-box and apply it to all FortiEDR Collector Groups by default. Modifications made on one policy do not affect any other policies.

1. In the policy list, check the policy that you want to clone. There are two types of Communication Control policies: blocklisting policies (☰), such as the Default communication control policy, which allows any connection by default, and allowlisting policies (☰), such as the Servers policy, which denies any connection by default.

2. Click the *Clone* button. The following window displays:



POLICY CLONING

ORIGINAL POLICY NAME	CLONED POLICY NAME
Default Communication Control Policy	Default Communication Control Policy clone

1 Application policy will be cloned

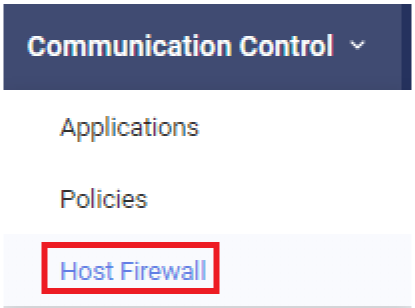
3. In the *Cloned Policy Name* field, specify a name for the cloned policy.
4. Click *Clone*.

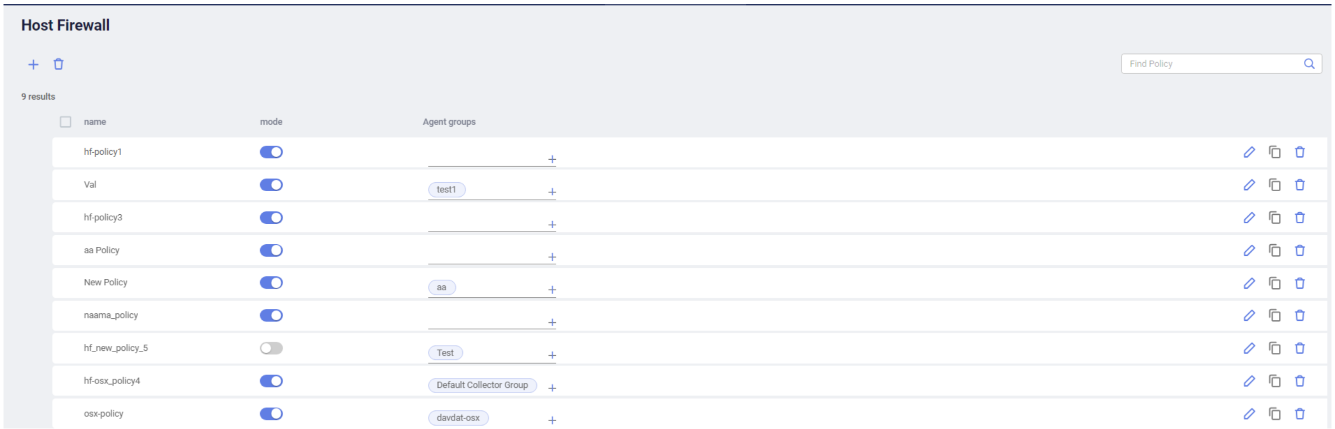
Other options in the Policies pane

Option	Description
All ▾	Click the down arrow in the All ▾ button and then select an option in the dropdown list to filter the policy list accordingly.
Clone	Click this button to clone a policy.
Delete	Click this button to delete a policy. Before deletion, a confirmation message displays, prompting you to confirm the deletion of the policy.
Set mode ▾	Click the down arrow in the Set mode ▾ button and then select the mode for the policy, as described in Policy mode on page 187

Host Firewall COLLECTOR 6.1 OR LATER

Use the *Communications Control > Host Firewall* page to configure host firewall policies to control incoming and outgoing network traffic to protect endpoints against unwanted connections based on remote addresses, protocols, or applications in use to reflect the organization’s network policies. Host firewall policies reduce the attack surface by protecting the host while working outside the enterprise network (public Internet, home, or other networks).





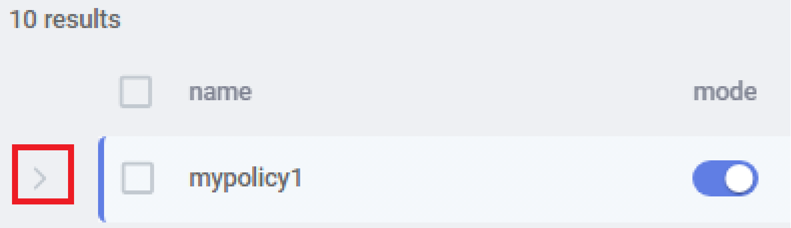
9 results

□	name	mode	Agent groups
	hf-policy1	●	+
	Val	●	test1 +
	hf-policy3	●	+
	aa Policy	●	+
	New Policy	●	aa +
	naama_policy	●	+
	hf_new_policy_5	○	Test +
	hf-osx_policy4	●	Default Collector Group +
	osx-policy	●	davdat-osx +

To configure a host firewall policy:

1. In the *Communications Control > Host Firewall* page, click the *Add* button at the top left corner.
2. Specify a name for the host firewall policy.
3. Select the Collector groups that the host firewall policy applies to.
4. Click *Save* to save the host firewall policy.
   The host firewall policy appears in the list.
5. **(Optional)** Add or remove Collector groups for the host firewall policy in the *Agent groups* column.
6. Define rules to associate with the host firewall policy:

a. Expand the row of the host firewall policy in the table.



10 results

	□	name	mode
>	□	mypolicy1	●

b. Click the *Add* button under the host firewall policy.

c. Enable the rule if you want to enforce the rule immediately after creation. You can also choose to enable it later.

d. Specify a name for the rule.

e. Specify the application name or IP address and port combination that the rule applies to.

   The IP address and port can be single or a range, including wildcard. For example, 192.168.0.1 or 192.168.0.1-192.168.0.100.

f. Select the protocol, which can be TCP, UDP, or any.

g. In the *Process* field, specify an application name to apply the rule to one specific application or use the default *Any*, which means the rule applies to all applications.

h. In the *Action* dropdown, select whether to allow or deny matching connections.

   The action applies to both incoming and outgoing traffic.

i. **(Optional)** Add a description for the rule.

j. Click *Save* to save the rule.

   The rule appears under the host firewall policy in the table.

k. Add more rules by repeating the steps above as needed.

l. When more than one rule exists, drag and drop the rules in the order of priority. When the criteria of multiple groups are met, the first matching rule will be used.

7. Enable or disable the host firewall policy or a specific rule using the mode button.
8. To log connections blocked by a Collector, check the *Firewall Block* action in the Collector's assigned Threat Hunting Collection profiles on page 233.

Host firewall policies work side by side with existing Communication Control policies. In case of contradictions, FortiEDR applies the more restrictive out of the two. For example, if a group is assigned to a host firewall policy that allows any connection to a specific remote address but the Communication Control policy assigned to the group restricts connections to low reputation applications, connections to the remote address will be blocked if the connection goes to low reputation applications.

Security Settings

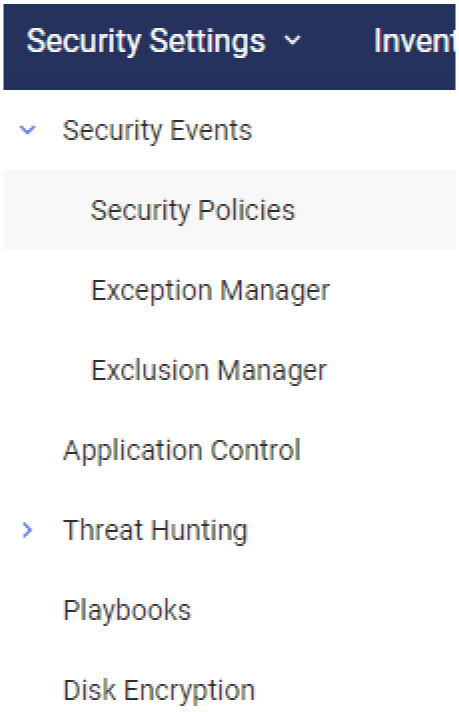
This chapter describes FortiEDR security policies and Playbook policies for defining, monitoring and handling FortiEDR security.

Security events

FortiEDR security policies

The most powerful proprietary feature of the FortiEDR platform is its predefined and configurable security policies.

To access the FortiEDR *Security Policies* page, click the down arrow next to *SECURITY SETTINGS > Security Events > Security Policies*.



Out-of-the-box policies

FortiEDR provides the following out-of-the-box policies. Each policy comes with multiple highly intelligent rules that enforce it.

You will receive one or all policies, depending on your FortiEDR license.

- *Application Control*: This policy enables FortiEDR to block user-defined applications from running, so that they do not launch. Blocklist management is done on the Application Control on page 223 page.

  Application Control security events are displayed under dedicated *Application Control* filter in the *Incidents* page and are not listed as part of the *All* filter.

- *Device Control*: This policy enables FortiEDR to detect and block the usage of USB devices, such as USB mass storage devices. In this policy, detection is based on the device type.

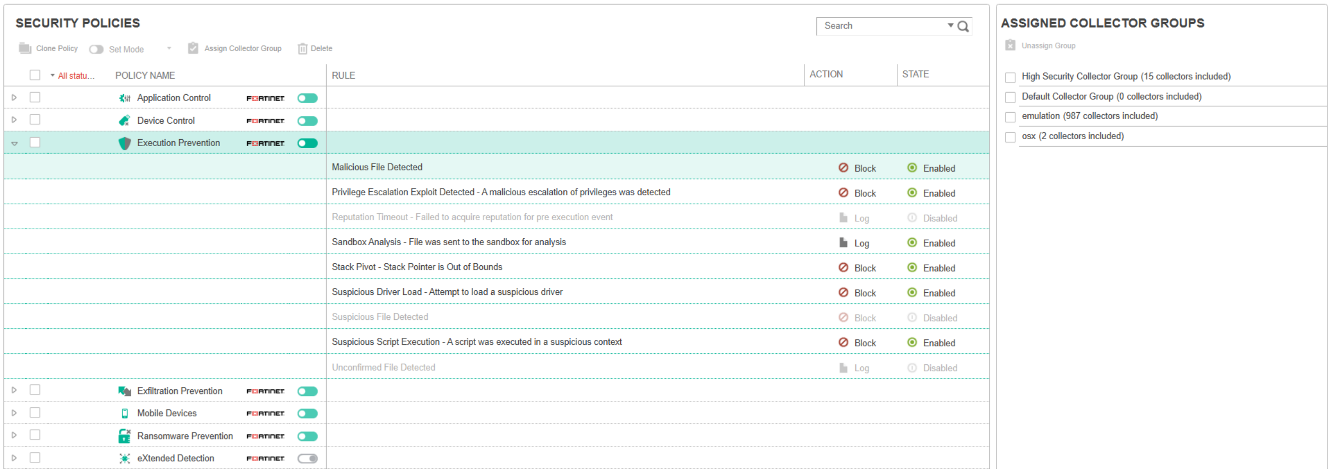
  This feature is a license-dependent and requires the Vulnerability Management add-on (meaning License Type that is either Discover and Protect or Discover, Protect and Response). Device Control security events are displayed under dedicated *Device Control* filter in the *Incidents* page and are not listed as part of the *All* filter.

- *Execution Prevention*: This policy blocks the execution of files that are identified as malicious or suspected to be malicious. For this policy, each file is analyzed to find evidence for malicious activity. One of the following rules is triggered, based on the analysis result:
  - *Most Likely a Malicious File*: A Malicious File Execution rule is triggered with a critical severity. By default, the file is blocked.
  - *Probably a Malicious File*: A Suspicious File Execution rule is triggered with a high severity. By default, the file is blocked.
  - *Show Evidence of Malicious File*: An Unresolved file rule is triggered with a medium severity. By default, the file is logged, but is not blocked.
- *Exfiltration Prevention*: This policy enables FortiEDR to distinguish which connection establishment requests are malicious ones.
- *Mobile Devices*: This policy enables FortiEDR to detect and prevent access to malicious URL and IP addresses from the mobile devices.

  The *Mobile Devices* policies are available only if mobile is enabled in the organization setting. See Step 2 – Defining or importing an organization on page 419.

- *Ransomware Prevention*: This policy enables FortiEDR to detect and block malware that prevents or limits users from accessing their own system.
- *eXtended Detection Policy*: This policy provides visibility into data across multiple security systems and identifies abnormal or malicious activity by applying analytics and correlating data from various systems. Events are logged and displayed in the *Incidents* tab. No blocking options are provided. The exceptions options are not available in the *Incidents* tab for security events triggered by this policy.

This policy requires that you configure an XDR source connector in the *Administration > Connectors* section. This feature is a license-dependent add-on. You may contact Fortinet Support for more information.



SECURITY POLICIES

☐ All statu...	POLICY NAME	RULE	ACTION	STATE
▷ ☐	Application Control FORTINET			
▷ ☐	Device Control FORTINET			
▽ ☐	Execution Prevention FORTINET			
		Malicious File Detected	Block	Enabled
		Privilege Escalation Exploit Detected - A malicious escalation of privileges was detected	Block	Enabled
		Reputation Timeout - Failed to acquire reputation for pre execution event	Log	Disabled
		Sandbox Analysis - File was sent to the sandbox for analysis	Log	Enabled
		Stack Pivot - Stack Pointer is Out of Bounds	Block	Enabled
		Suspicious Driver Load - Attempt to load a suspicious driver	Block	Enabled
		Suspicious File Detected	Block	Disabled
		Suspicious Script Execution - A script was executed in a suspicious context	Block	Enabled
		Unconfirmed File Detected	Log	Disabled
▷ ☐	Exfiltration Prevention FORTINET			
▷ ☐	Mobile Devices FORTINET			
▷ ☐	Ransomware Prevention FORTINET			
▷ ☐	eXtended Detection FORTINET			

ASSIGNED COLLECTOR GROUPS

- ☐ High Security Collector Group (15 collectors included)
- ☐ Default Collector Group (0 collectors included)
- ☐ emulation (987 collectors included)
- ☐ osx (2 collectors included)

All security policies can run simultaneously. However, these security policies detect rule violations at different places and points in time in the operating system. When multiple security policies are triggered, FortiEDR uses the following guidelines to avoid generating duplicate security events:

- For connection establishment attempts, the Exfiltration Prevention rule violation is detected.
- For attempts to lock files or access their data (for example, by encrypting the data), the Ransomware rule violation is detected.
- When a malicious file is being executed by the user or by the operation system, the Execution Prevention rule violation is detected.
- For attempts to use a USB device, such as a mass storage device, the Device Control rule violation is detected. It is supported on Windows devices only.
- For execution attempts of an application that is included in the blocklist, the Application Control rule violation is detected.
- When malicious activity is identified across network, endpoints, and cloud, an Extended Detection rule violation is detected.

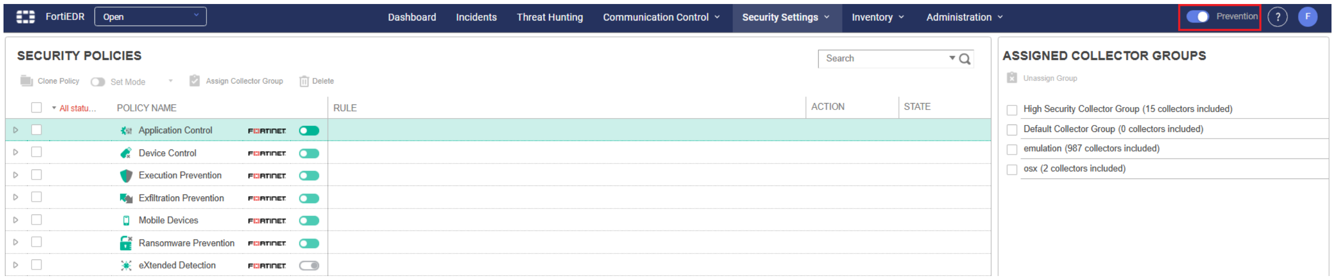
Protection or Simulation mode

During an initial acquaintance period or at any time, you can decide that FortiEDR acts as either of the following:

- *Protection:* FortiEDR enforces its active exfiltration prevention policy that blocks all connections that violate the relevant FortiEDR security policy rules.
- *Simulation (Notification Only):* FortiEDR *only* issues an alert (described below) for all connections that violate any rule in the FortiEDR security policy. In this mode, FortiEDR does not block exfiltration. FortiEDR comes out-of-the-box set to this mode.

If you have purchased a Content add-on license, policy rules and built-in exceptions are periodically automatically added or updated by Fortinet. When a new security policy is added, an indicator number displays on the *SECURITY SETTINGS* tab.

Use the *Protection/Simulation* slider at the far right of the window to enable the applicable mode, as shown below:



SECURITY POLICIES

Search

Clone Policy · Set Mode · Assign Collector Group · Delete

All statu...	POLICY NAME		RULE	ACTION	STATE
▷ □	Application Control	FORTINET			
▷ □	Device Control	FORTINET			
▷ □	Execution Prevention	FORTINET			
▷ □	Exfiltration Prevention	FORTINET			
▷ □	Mobile Devices	FORTINET			
▷ □	Ransomware Prevention	FORTINET			
▷ □	eXtended Detection	FORTINET			

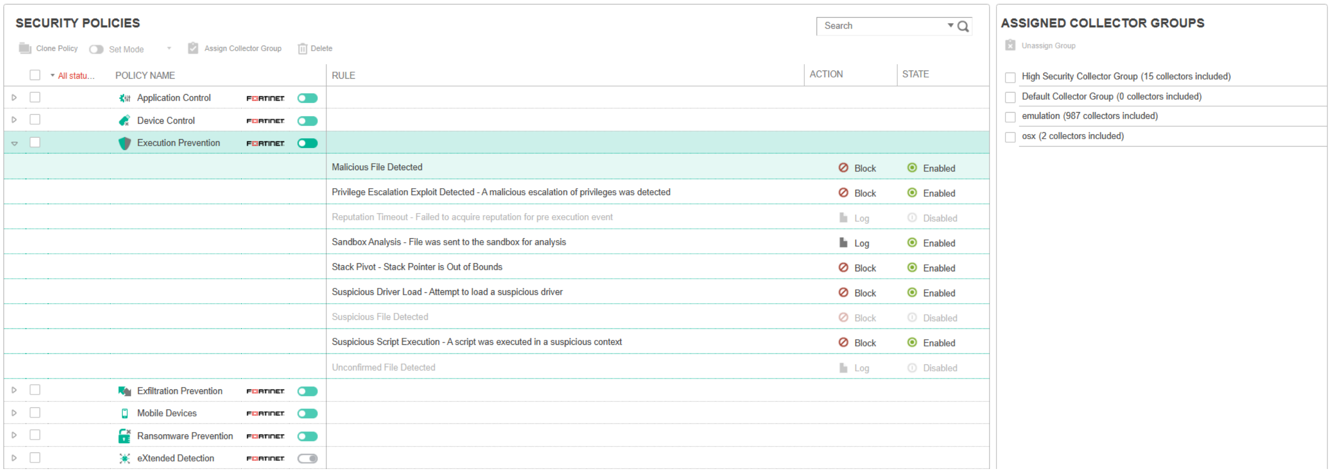
ASSIGNED COLLECTOR GROUPS

Unassign Group

□ High Security Collector Group (15 collectors included)
□ Default Collector Group (0 collectors included)
□ emulation (987 collectors included)
□ osx (2 collectors included)

Security Policies page

The *SECURITY POLICIES* page displays a row for each security policy. Each policy row can be expanded to show the rules that it contains, as shown below. To access this page, click the down arrow next to *SECURITY SETTINGS* and then select *Security Policies*.



SECURITY POLICIES

Search

Clone Policy · Set Mode · Assign Collector Group · Delete

All statu...	POLICY NAME		RULE	ACTION	STATE
▷ □	Application Control	FORTINET			
▷ □	Device Control	FORTINET			
▽ □	Execution Prevention	FORTINET			
			Malicious File Detected	Block	Enabled
			Privilege Escalation Exploit Detected - A malicious escalation of privileges was detected	Block	Enabled
			Reputation Timeout - Failed to acquire reputation for pre execution event	Log	Disabled
			Sandbox Analysis - File was sent to the sandbox for analysis	Log	Enabled
			Stack Pivot - Stack Pointer is Out of Bounds	Block	Enabled
			Suspicious Driver Load - Attempt to load a suspicious driver	Block	Enabled
			Suspicious File Detected	Block	Disabled
			Suspicious Script Execution - A script was executed in a suspicious context	Block	Enabled
			Unconfirmed File Detected	Log	Disabled
▷ □	Exfiltration Prevention	FORTINET			
▷ □	Mobile Devices	FORTINET			
▷ □	Ransomware Prevention	FORTINET			
▷ □	eXtended Detection	FORTINET			

ASSIGNED COLLECTOR GROUPS

Unassign Group

□ High Security Collector Group (15 collectors included)
□ Default Collector Group (0 collectors included)
□ emulation (987 collectors included)
□ osx (2 collectors included)

FortiEDR is provided out-of-the-box with several predefined security policies (depending on your license), ready for you to get started. By default, all policies are set to Simulation mode (meaning that they only log and do not block) and show the FORTINET logo. This page also enables you to define additional policies. See Out-of-the-box policies on page 196 for more details.

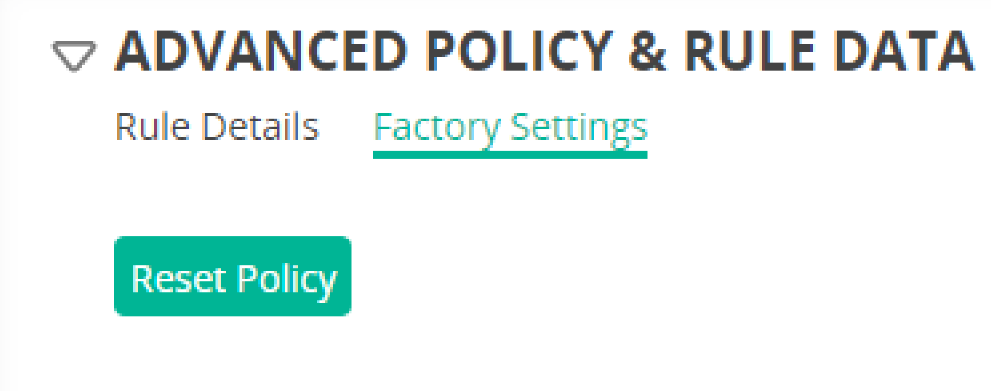
Security Policy	Icon
Application Control Policies	

Security Policy	Icon
Device Control Policies	🔌
Execution Prevention	🛡
Exfiltration Prevention	⇄
Mobile Devices This section is available only if mobile is enabled in the organization setting. See Step 2 – Defining or importing an organization on page 419.	📱
Ransomware Prevention	🔓
Extended Detection	✷

The following information is defined per security policy:

Information Field	Description
Policy Name	The policy name appears in the left most column. The policy name is defined when the policy is created. The name of the *Default Policy* cannot be changed.
Rule Name	FortiEDR's proprietary rules come predefined and are the primary component of FortiEDR's proprietary security solution. This column displays a short description for the purpose of this rule. You can expand the *ADVANCED POLICY & RULES DATA* area at the bottom left of the window to display a more detailed description of what the rule does and how it works.
Action	Specifies the action that is enforced when this rule is violated. You can change this field, as follows: • *Block* ⊘ Block: When this policy is set to *Prevention* mode (Setting a security policy's Prevention or Simulation mode on page 201), the exfiltration attempt is blocked and a blocking event is generated. When this policy is set to *Simulation* mode, the outgoing connection attempt is NOT blocked and a simulated-blocking event is generated (this indicates that FortiEDR ***would have*** blocked the exfiltration if the policy had been set to Prevention mode). • *Log* Log : The event is only logged regardless of whether the policy is set to Prevention or Simulation mode. The outgoing connection attempt is not blocked.
State	(Enabled/Disabled) This option enables you to disable/enable this rule. FortiEDR's rules have been created as a result of extensive expertise and experience. Therefore, we do not recommend disabling any of them.

To reset a FortiEDR security policy to its out-of-the-box settings, click the *Reset Policy* button in the *ADVANCED POLICY & RULE DATA* section, as shown below:



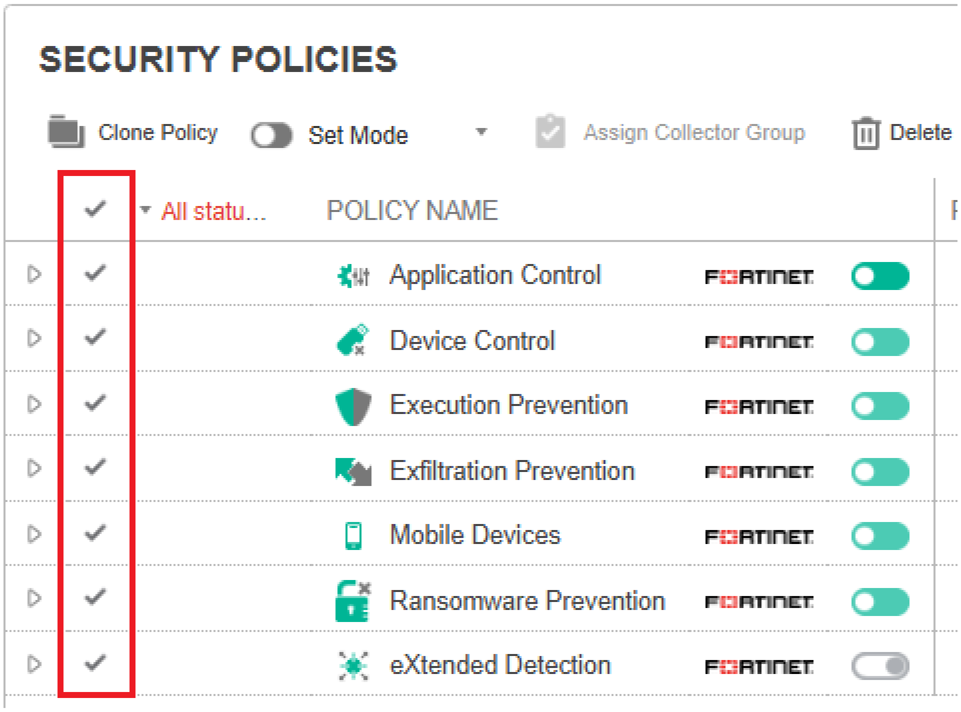
Setting a security policy’s Prevention or Simulation mode

Each FortiEDR security policy can be set to operate in one of the following modes:

- *Prevention*: FortiEDR enforces its active prevention policy that blocks all activity that violates relevant rules in the FortiEDR security policy.
- *Simulation/Notification Only*: FortiEDR logs and alerts only violations of FortiEDR security policy. The events are shown in the FortiEDR Central Manager. In this mode, FortiEDR does not block malicious activity. This is the default mode of all FortiEDR security policies out of the box. You can decide to use this mode during an initial acquaintance period or at any time.

To set a security policy to Prevention or Simulation mode:

1. Select the checkbox of the security policy to be configured. Alternatively, you can select the top-left checkbox to configure all security policies at once.

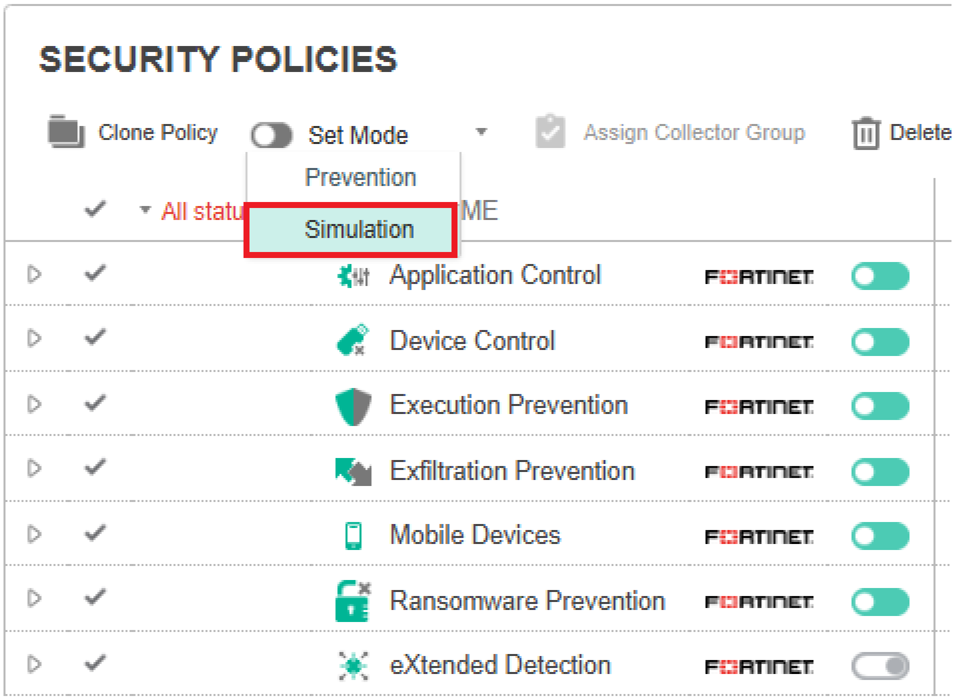


2. You can now either:

   a. ○ Set mode : Click *Set Mode* and select either *Prevention* or *Simulation*, as shown above.

   b. ●: Move the slider to the left for Prevention or to the right for Simulation.

You can also set all FortiEDR policies to Simulation mode at once by moving the slider at the top-left corner to Simulation, as shown below:

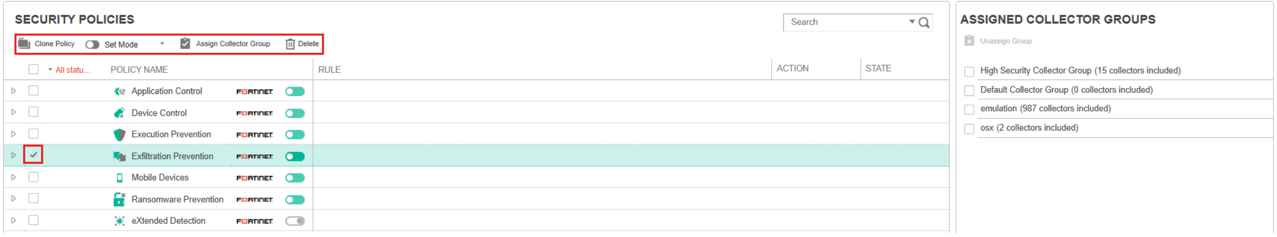


Creating a new security policy

A new security policy can be created by cloning an existing policy, as described below. New security policies are only needed if you are going to assign different policies to different Collector Groups. Otherwise, you can simply modify one of the default policies that are provided out-of-the-box and apply it to all FortiEDR Collectors by default. Modifications made on one security policy do not affect any other policies.

To create a new security policy:

1. In the *SECURITY POLICIES* page, check the checkbox of the security policy to be cloned. The buttons at the top of the window then become active.



SECURITY POLICIES

Clone Policy | Set Mode | Assign Collector Group | Delete

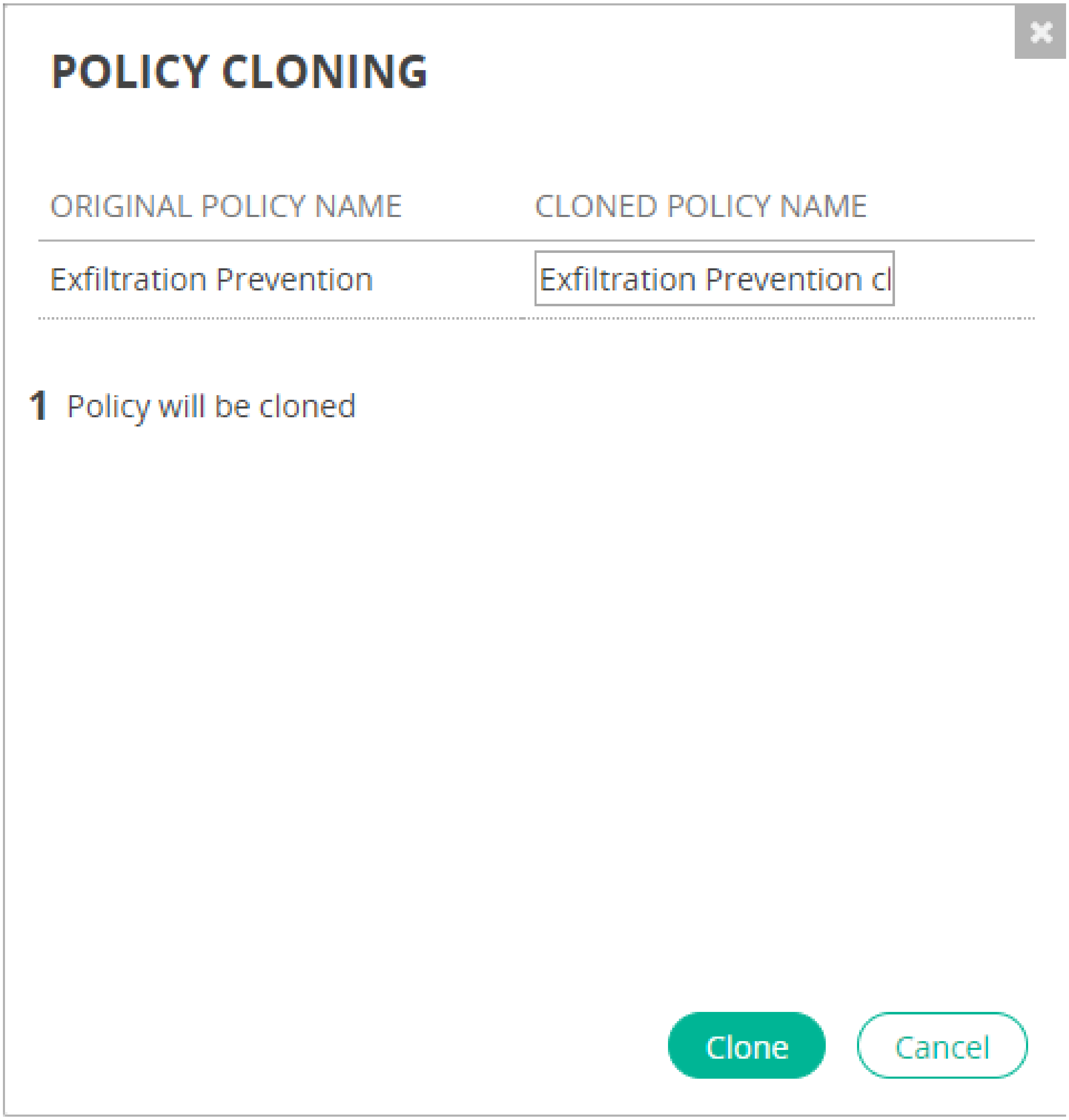
		All statu...	POLICY NAME			RULE	ACTION	STATE
▷	□		Application Control	FORTINET	●			
▷	□		Device Control	FORTINET	●			
▷	□		Execution Prevention	FORTINET	●			
▷	☑		Exfiltration Prevention	FORTINET	●			
▷	□		Mobile Devices	FORTINET	●			
▷	□		Ransomware Prevention	FORTINET	●			
▷	□		eXtended Detection	FORTINET	○			

ASSIGNED COLLECTOR GROUPS

Unassign Group

□ High Security Collector Group (15 collectors included)
□ Default Collector Group (0 collectors included)
□ emulation (987 collectors included)
□ osx (2 collectors included)

2. Select the *Clone Policy* button. The following window displays:



POLICY CLONING

ORIGINAL POLICY NAME	CLONED POLICY NAME
Exfiltration Prevention	Exfiltration Prevention cl

1 Policy will be cloned

3. Specify the name of the new security policy and click the *Clone* button.
4. If needed, assign the security policy to the required Collector Group so that it protects all the FortiEDR Collectors in that group, as described in Assigning a security policy to a Collector Group on page 205.

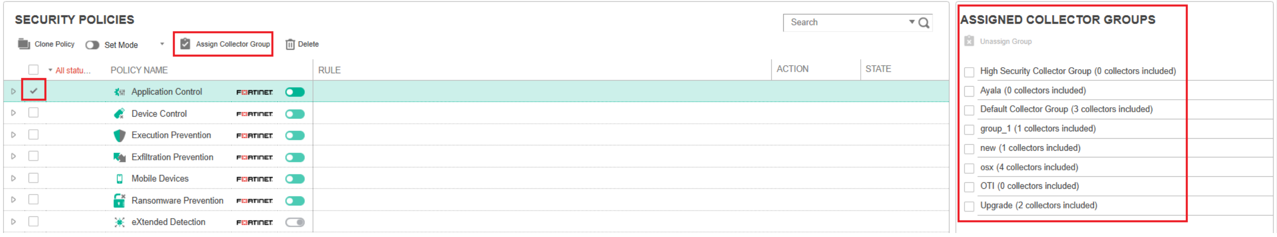
Assigning a security policy to a Collector Group

By default, a security policy protects the FortiEDR Collectors that belong to that Collector Group. A security policy can be assigned to more than one Collector Group. Multiple security policies can be assigned to each Collector Group.

It is not recommended to assign multiple security policies that have the same or overlapping rules to a Collector Group, as this means that the same security events will be triggered in response to both policies, producing duplicated events.

Refer to Defining a new Collector Group on page 262 for a description of how to define a new Collector Group in the *INVENTORY* tab.

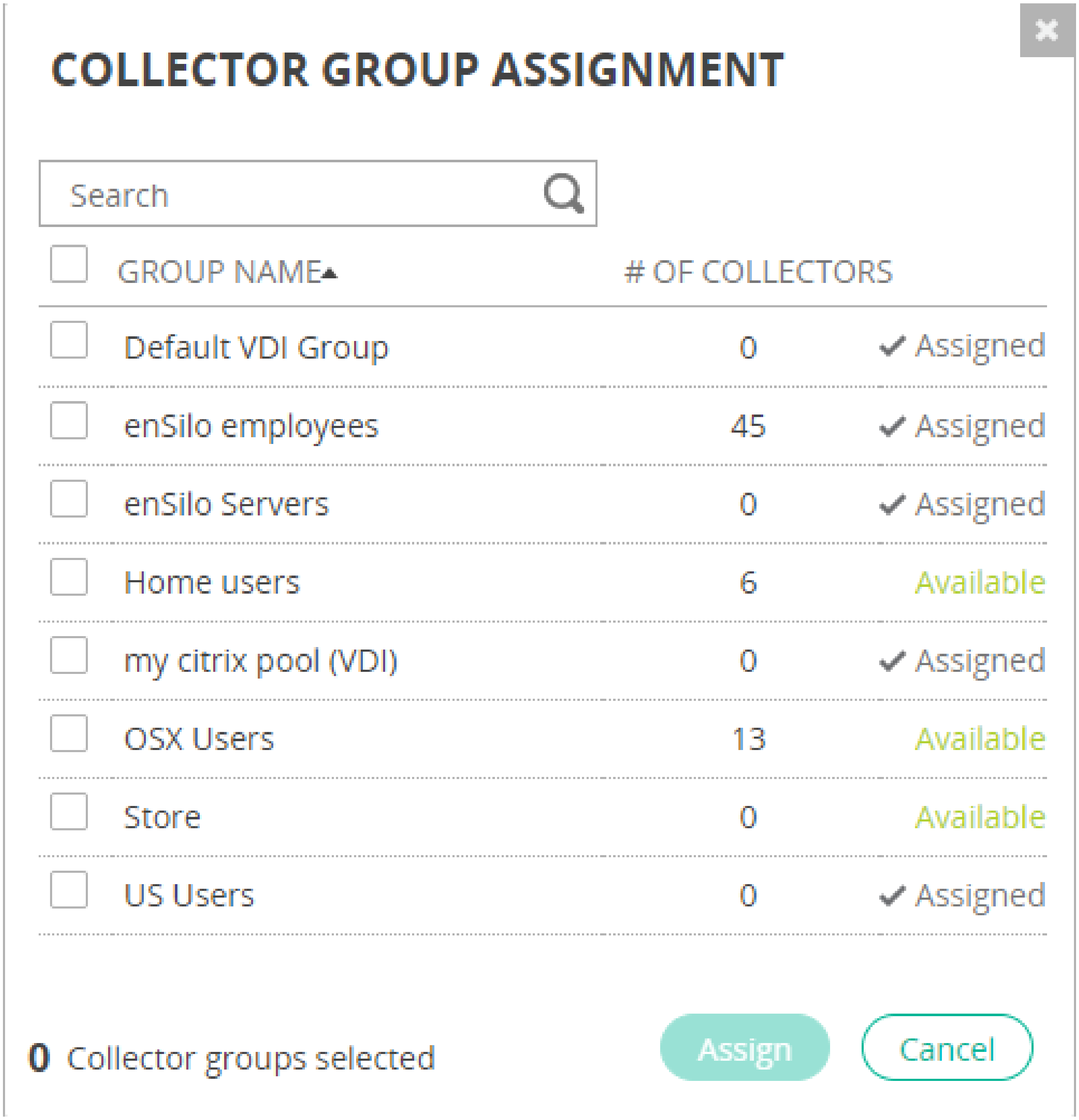
1. In the *SECURITY POLICIES* page, select the name of the security policy to be assigned by clicking its checkbox. The right side of the window displays the Collector Groups to which this policy is assigned.



	All statu...	POLICY NAME			RULE	ACTION	STATE
▷	☑	Application Control	FORTINET	●			
▷	□	Device Control	FORTINET	●			
▷	□	Execution Prevention	FORTINET	●			
▷	□	Exfiltration Prevention	FORTINET	●			
▷	□	Mobile Devices	FORTINET	●			
▷	□	Ransomware Prevention	FORTINET	●			
▷	□	eXtended Detection	FORTINET	○			

- □ High Security Collector Group (0 collectors included)
- □ Ayala (0 collectors included)
- □ Default Collector Group (3 collectors included)
- □ group_1 (1 collectors included)
- □ new (1 collectors included)
- □ osx (4 collectors included)
- □ OTI (0 collectors included)
- □ Upgrade (2 collectors included)

2. Click the *Assign Collector Group* toolbar button, which displays the following window in which you can select the Collector Groups to which to assign this policy.



COLLECTOR GROUP ASSIGNMENT

□	GROUP NAME▲	# OF COLLECTORS	
□	Default VDI Group	0	✓ Assigned
□	enSilo employees	45	✓ Assigned
□	enSilo Servers	0	✓ Assigned
□	Home users	6	Available
□	my citrix pool (VDI)	0	✓ Assigned
□	OSX Users	13	Available
□	Store	0	Available
□	US Users	0	✓ Assigned

0 Collector groups selected

The *ASSIGNED COLLECTORS GROUPS* area lists all the Collector Groups that have been assigned a security policy to protect them. You can also simply drag-and-drop a Collector Group from this list onto a policy in the left pane of this window to assign the Collector Group to be protected by that policy.

Deleting a security policy

Select the policy's checkbox and then click the *Delete* button.

The Exfiltration Prevention, Ransomware Prevention, Device Control, Application Control, eXtended Detection, and Execution Prevention FortiEDR security policies provided out-of-the-box (FORTINET) cannot be deleted.

Exception Manager

Exceptions enable you to limit the enforcement of a rule, meaning to create a white list for a specific flow of events that was used to establish a connection request or perform a specific operation.

An exception can be made for a Collector Group (several specific ones or for all) and a destination IP (a specific one, IP-set or all). The event is then no longer triggered for that specific Collector Group or destination IP. This exception can be added on part or the entire set of rules and the process that triggered this event.

When an exception is defined, it results in one or more exception pairs. An exception pair specifies the rule that was violated, and the process on which the violation occurred, including its entire location path. For example, the following shows several examples of exception pairs:

- Rule – File encryptor with Process – `c:\users\root\Desktop\ransom\RnsmTOX.exe`
- Rule – Process hollowing with Process – `c:\users\root\AppData\Local\hipmiav.exe`

An exception that applies to a security event can result in the creation of several exception pairs. Each exception is associated with a specific process path. You determine whether the exception pair can run from the event-specific path or whether to apply the exception for this process so that it can run from any path.

If the exception pair includes more than one process, you can include the other processes too, as well as determine whether they can run from the event-specific path or from any path.

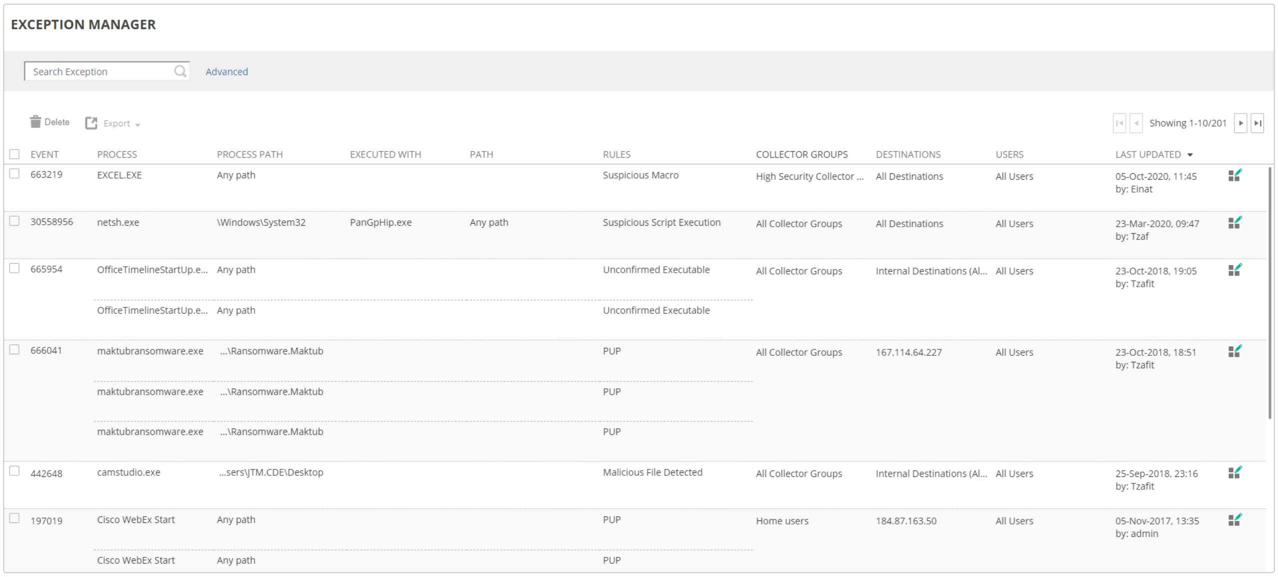
Any exception that you define applies to all policies.

Exceptions are created in the *Incidents* tab, as described onDefining security event exceptions on page 118

Fortinet Cloud Services (FCS) may push an automated exception in cases where extended analysis and investigation of a security event leads to its reclassification as Safe. This prevents the security event from triggering again. In such cases, the security event is moved under handled events and the exception that was set is added in the Exception Manager with FortiEDRCloudServices as the handling user.

To manage exceptions:

1. Select *SECURITY SETTINGS > Security Events > Exception Manager*. Alternatively, in the *Incidents* tab, click the *Exception Manager* button. The following window displays, showing the list of previously created exceptions:



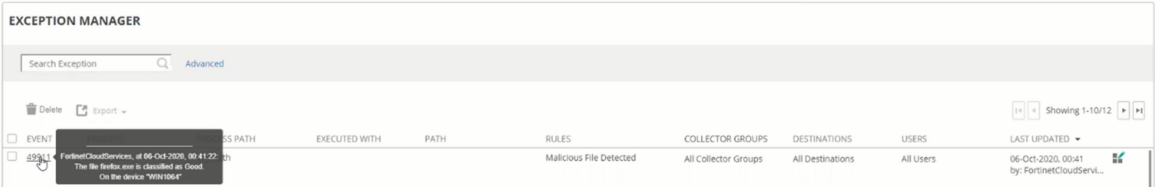
EXCEPTION MANAGER

Search Exception | Advanced

Delete | Export ▾ | Showing 1-10/201

□	EVENT	PROCESS	PROCESS PATH	EXECUTED WITH	PATH	RULES	COLLECTOR GROUPS	DESTINATIONS	USERS	LAST UPDATED ▾
□	663219	EXCEL.EXE	Any path			Suspicious Macro	High Security Collector ...	All Destinations	All Users	05-Oct-2020, 11:45 by: Einat
□	30558956	netsh.exe	\Windows\System32	PanGpHip.exe	Any path	Suspicious Script Execution	All Collector Groups	All Destinations	All Users	23-Mar-2020, 09:47 by: Tzaf
□	665954	OfficeTimelineStartUp.e... OfficeTimelineStartUp.e...	Any path Any path			Unconfirmed Executable Unconfirmed Executable	All Collector Groups	Internal Destinations (Al...	All Users	23-Oct-2018, 19:05 by: Tzafit
□	666041	maktubransomware.exe maktubransomware.exe maktubransomware.exe	...\Ransomware.Maktub ...\Ransomware.Maktub ...\Ransomware.Maktub			PUP PUP PUP	All Collector Groups	167.114.64.227	All Users	23-Oct-2018, 18:51 by: Tzafit
□	442648	camstudio.exe	...sers\JTM.CDE\Desktop			Malicious File Detected	All Collector Groups	Internal Destinations (Al...	All Users	25-Sep-2018, 23:16 by: Tzafit
□	197019	Cisco WebEx Start Cisco WebEx Start	Any path Any path			PUP PUP	Home users	184.87.163.50	All Users	05-Nov-2017, 13:35 by: admin

If the exception includes a free-text comment, you can hover over the Event ID in the Exception Manager to display it.



EXCEPTION MANAGER

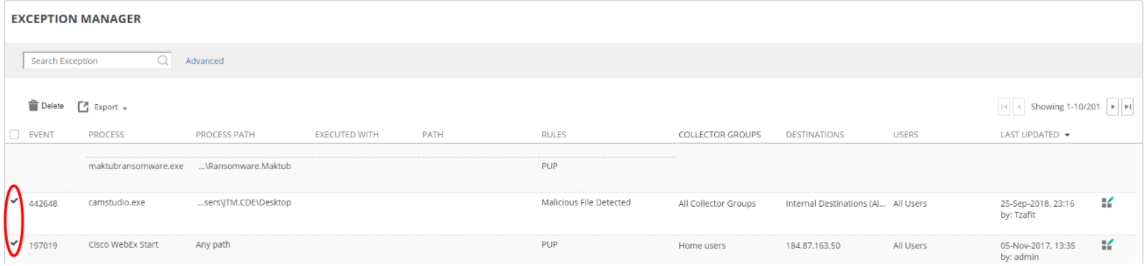
Search Exception | Advanced

Delete | Export ▾ | Showing 1-10/12

□	EVENT	PROCESS	PROCESS PATH	EXECUTED WITH	PATH	RULES	COLLECTOR GROUPS	DESTINATIONS	USERS	LAST UPDATED ▾
□	49911		th			Malicious File Detected	All Collector Groups	All Destinations	All Users	06-Oct-2020, 00:41 by: FortinetCloudServi...

FortinetCloudServices, at 06-Oct-2020, 00:41:22:
The file firefox.exe is classified as Good.
On the device "WIN1064"

You can delete one or more exceptions simultaneously by selecting the checkbox at the beginning of its row and then clicking the *Delete* button.



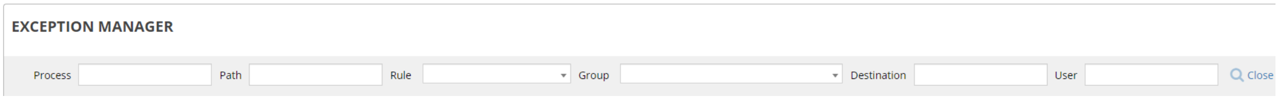
EXCEPTION MANAGER

Search Exception | Advanced

Delete | Export ▾ | Showing 1-10/201

□	EVENT	PROCESS	PROCESS PATH	EXECUTED WITH	PATH	RULES	COLLECTOR GROUPS	DESTINATIONS	USERS	LAST UPDATED ▾
		maktubransomware.exe	...\Ransomware.Maktub			PUP				
✓	442648	camstudio.exe	...sers\JTM.CDE\Desktop			Malicious File Detected	All Collector Groups	Internal Destinations (Al...	All Users	25-Sep-2018, 23:16 by: Tzafit
✓	197019	Cisco WebEx Start	Any path			PUP	Home users	184.87.163.50	All Users	05-Nov-2017, 13:35 by: admin

2. To filter the exception list, click the *Advanced* button. The window displays various filter boxes at the top of the window, which you can use to filter the list by specific criteria.



EXCEPTION MANAGER

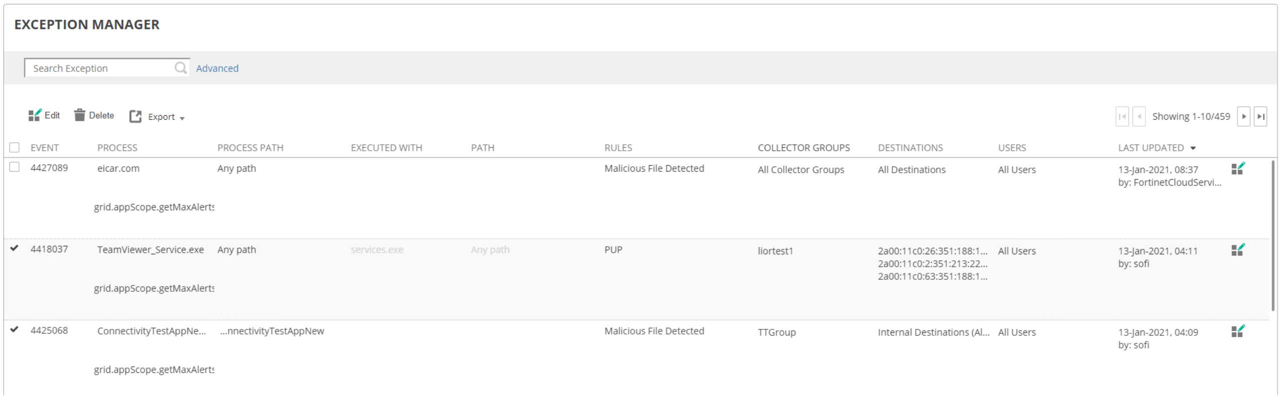
Process | Path | Rule ▾ | Group ▾ | Destination | User | Close

Click the *Basic search* button to access the standard search options.

Click the *Edit Exception* button in an exception row to edit that exception. For more details, see Editing Security Event Exceptions on Editing security event exceptions on page 121.

Click the *Delete* 🗑 button in an exception row to delete that exception.

Changes can be made on multiple exceptions at the same time by checking the Exceptions that you would like to edit and then clicking on the Edit tool, as shown below:



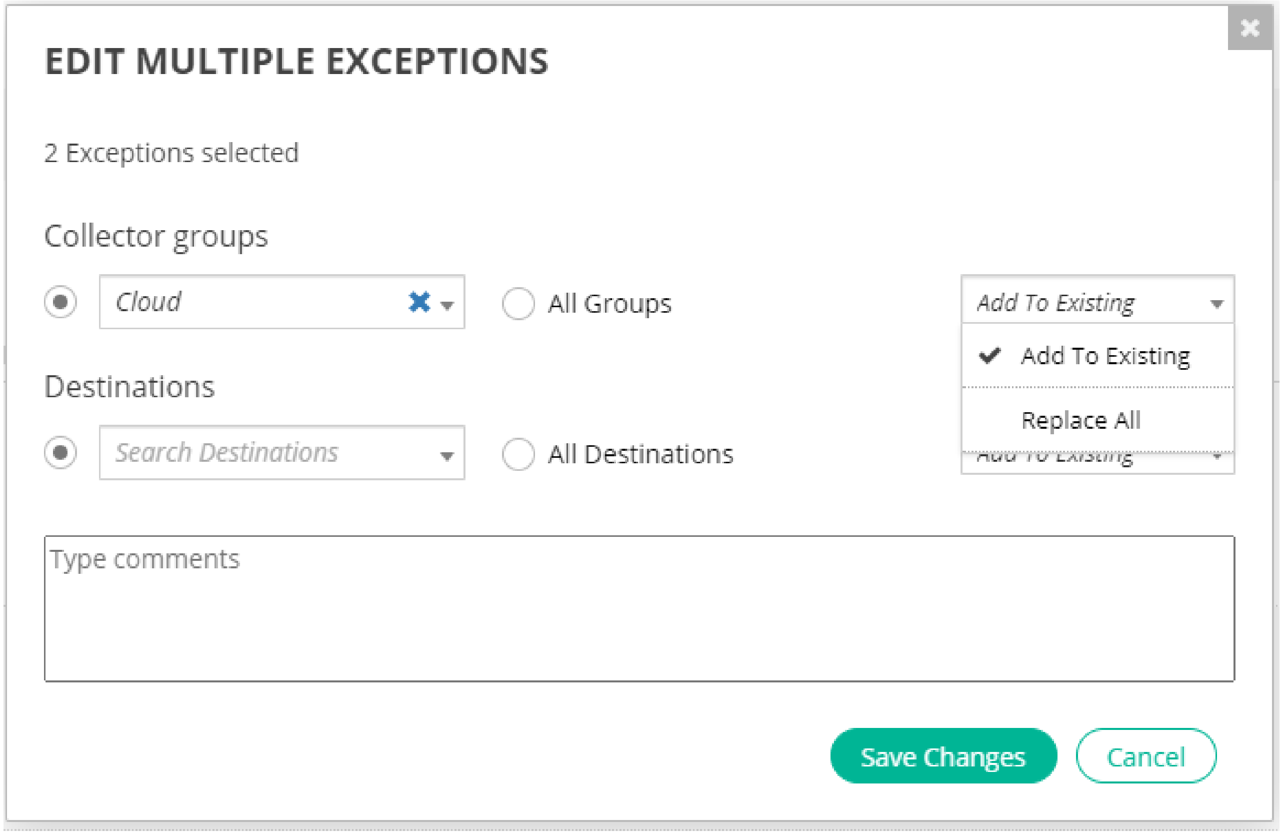
EXCEPTION MANAGER

Search Exception | Advanced

Edit | Delete | Export ▾ | Showing 1-10/459

□	EVENT	PROCESS	PROCESS PATH	EXECUTED WITH	PATH	RULES	COLLECTOR GROUPS	DESTINATIONS	USERS	LAST UPDATED ▾
□	4427089	eicar.com grid.appScope.getMaxAlerts	Any path			Malicious File Detected	All Collector Groups	All Destinations	All Users	13-Jan-2021, 08:37 by: FortinetCloudServi...
✓	4418037	TeamViewer_Service.exe grid.appScope.getMaxAlerts	Any path	services.exe	Any path	PUP	liortest1	2a00:11c0:26:351:188:1... 2a00:11c0:2:351:213:22... 2a00:11c0:63:351:188:1...	All Users	13-Jan-2021, 04:11 by: sofi
✓	4425068	ConnectivityTestAppNe... grid.appScope.getMaxAlerts	...nnectivityTestAppNew			Malicious File Detected	TTGroup	Internal Destinations (Al...	All Users	13-Jan-2021, 04:09 by: sofi

The following window displays in the which you can choose to add new Collector Groups in addition to existing ones or to replace all Collector Groups with the new Collector Group values that you select:



EDIT MULTIPLE EXCEPTIONS

2 Exceptions selected

Collector groups

● Cloud ○ All Groups | Add To Existing ▾

✓ Add To Existing

Replace All

Destinations

● Search Destinations ○ All Destinations

Type comments

This same procedure can be used to edit the IP sets of the destination addresses of the selected exceptions.

Exclusion Manager

The Exclusion Manager enables you to define which processes, files, or domains are excluded from Security Policies monitoring. Three types of exclusions can be defined in the Exclusion Manager:

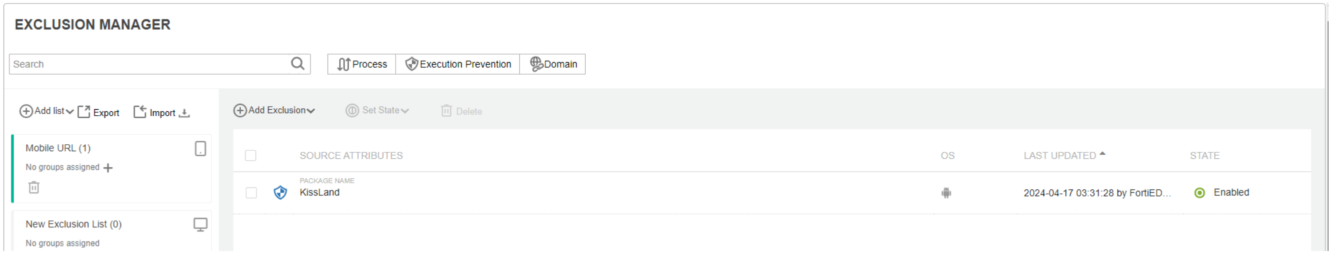
- **(PC only) Process Exclusions**: This type of exclusion specifies that FortiEDR does not inspect the actions that are performed by specific processes, so that these processes do not trigger security events. The processes that are excluded are identified by the attributes of the processes, according to your definitions.

  There may be various reasons for excluding a process in this manner. For example, when a process's performance/functionality is affected by FortiEDR's inspection, but the customer knows that this process is good/safe (this example is relevant, even when the process does not trigger security events). Therefore, in this case, the exclusion will specify that FortiEDR no longer inspects the specified processes.

  Please note that adding this type of exclusion excludes this process from being monitored by all FortiEDR features and all activities of this process are ignored.
- **Execution Prevention Exclusions**: The Execution Prevention policy inspects/scans files and then blocks their execution if they are identified as malicious or suspected to be malicious. Execution Prevention Exclusions specify that FortiEDR does not apply the Execution Prevention policy inspection, which analyzes files in order to find evidence of malicious activity, as described in Security Settings on page 196. The files that are excluded are identified by the attributes of the files that are the target of the Execution Prevention actions, according to your definitions.
- **(Mobile only) Domain Exclusions**: The Malicious URL/IP Detected policy inspects/scans URLs/domains and blocks connections to them if they are identified as malicious or suspected to be malicious. Domain Exclusions specify that FortiEDR does not apply the Malicious URL/IP Detected policy inspection. The domains that are excluded are identified according to your definitions.

To manage exclusions:

Select *SECURITY SETTINGS* > *Security Events* > *Exclusion Manager*. The following window displays, showing the list of previously created exclusions:



Mobile URL (1)
No groups assigned

New Exclusion List (0)
No groups assigned

	SOURCE ATTRIBUTES	OS	LAST UPDATED	STATE
□	PACKAGE NAME KissLand		2024-04-17 03:31:28 by FortiED...	● Enabled

The list of exclusions in the *Exclusion Manager* page contains the following columns:

Column	Description
Checkbox	Enables you to select multiple rows.
Icon	Represents the type of exclusion • - Process

Column	Description
	• 🛡 - Execution Prevention • 🌐 - Domain
SOURCE ATTRIBUTES	Specifies the attributes that were defined in order to identify the Process/File/Domain, as described in Defining exclusions on page 213
OS	Specifies the operating system to which the exclusion applies.
LAST UPDATED	Specifies when this exclusion was last updated and by whom.
STATE	Specifies whether this exclusion is enabled or disabled.
✎ 🗑	Edit and delete excursion tools.

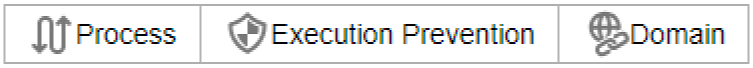
The following actions can be performed in the *Exclusion Manager* page:

- Filtering on page 211
- Defining Exclusion Lists on page 211
- Defining exclusions on page 213
- Exporting and importing exclusion lists on page 222

Filtering

To filter the Exclusion List names and their content, simply enter text in the *Search* field. Afterwards, only the Exclusion Lists that match the provided text are displayed showing only the relevant exclusions.

To filter the list of exclusions by type, click one of the following options:



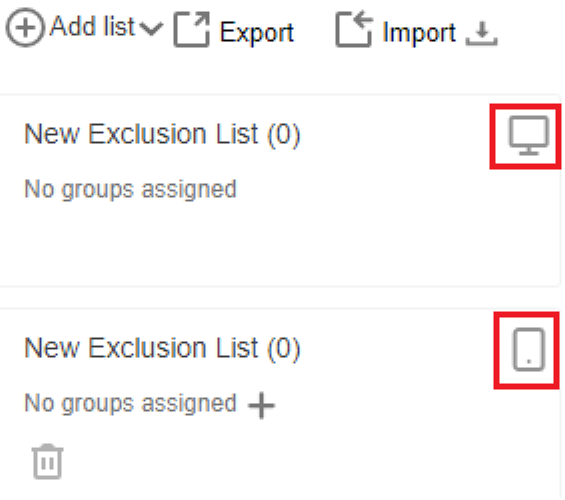
Defining Exclusion Lists

An Exclusion List contains a list of exclusions. You can assign Collector Groups to an Exclusion List in order to specify that the exclusions in the Exclusion List apply to the Collectors in the Collector Groups assigned to it. Exclusion Lists enable you to logically organize, categorize and group exclusions based on the type of activity data they are to exclude.

For example, let’s say that you want to collect network activity data for your system, but a specific application generates quite a bit of uninteresting logistical network activity that you do not want to collect. In this case, you can define an Exclusion List named after that application that contains one or more exclusions that relate specifically to the network activity generated by that application. Exclusion Lists can be organized anyway you see fit. For example, you can create an Exclusion List for security products, a different one for PDF documents, a different one for HR-related software and so on.

FortiEDR provides two types of exclusion lists: PC and mobile, which can be applied to PC Collector groups and mobile Collector groups, respectively. The type is indicated by the PC or mobile icon at the top right corner of the exclusion list card.

The *Mobile* option is available only if mobile is enabled in the organization setting. See Step 2 – Defining or importing an organization on page 419.



Adding an Exclusion List

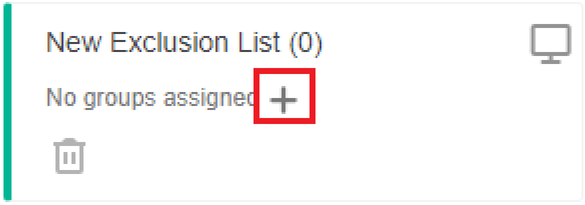
To define an Exclusion List:

1. Click the *+ Add List* option, select the type (*PC* or *Mobile*), and provide a name to create a new Exclusion List.

   The *Mobile* option is available only if mobile is enabled in the organization setting. See Step 2 – Defining or importing an organization on page 419.

2. Add (define) the exclusions of this Exclusion List (as described on the following page). Each exclusion that you add belongs to a specific Exclusion List.
3. Assign Collector Groups to this Exclusion List (as described below) in order to determine to which Collector Groups these exclusions apply. A Collector Group can be assigned to multiple Exclusion Lists.

Assigning a Collector Group to an Exclusion List



You can perform the following operations on an Exclusion List:

Operation	Description
Assign a Collector Group	Click the + button in the Exclusion List to which to assign a Collector Group. Then, select the Collectors groups to which to assign this list and approve it. Note that a Collector Group can be assigned to multiple Exclusion Lists.
Unassign a Collector Group	Click the + button and uncheck the Collector Group to be removed from an Exclusion List.
Delete Exclusions List	Click the *Delete* 🗑 button. Note that all Exclusions in this list will be removed and will no longer be applied to the assigned Collector groups.

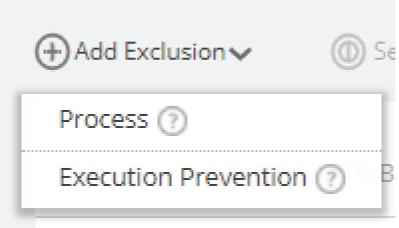
Defining exclusions

All exclusions must belong to an exclusion list. Select an exclusion list on the left to display the exclusions that are defined in it.

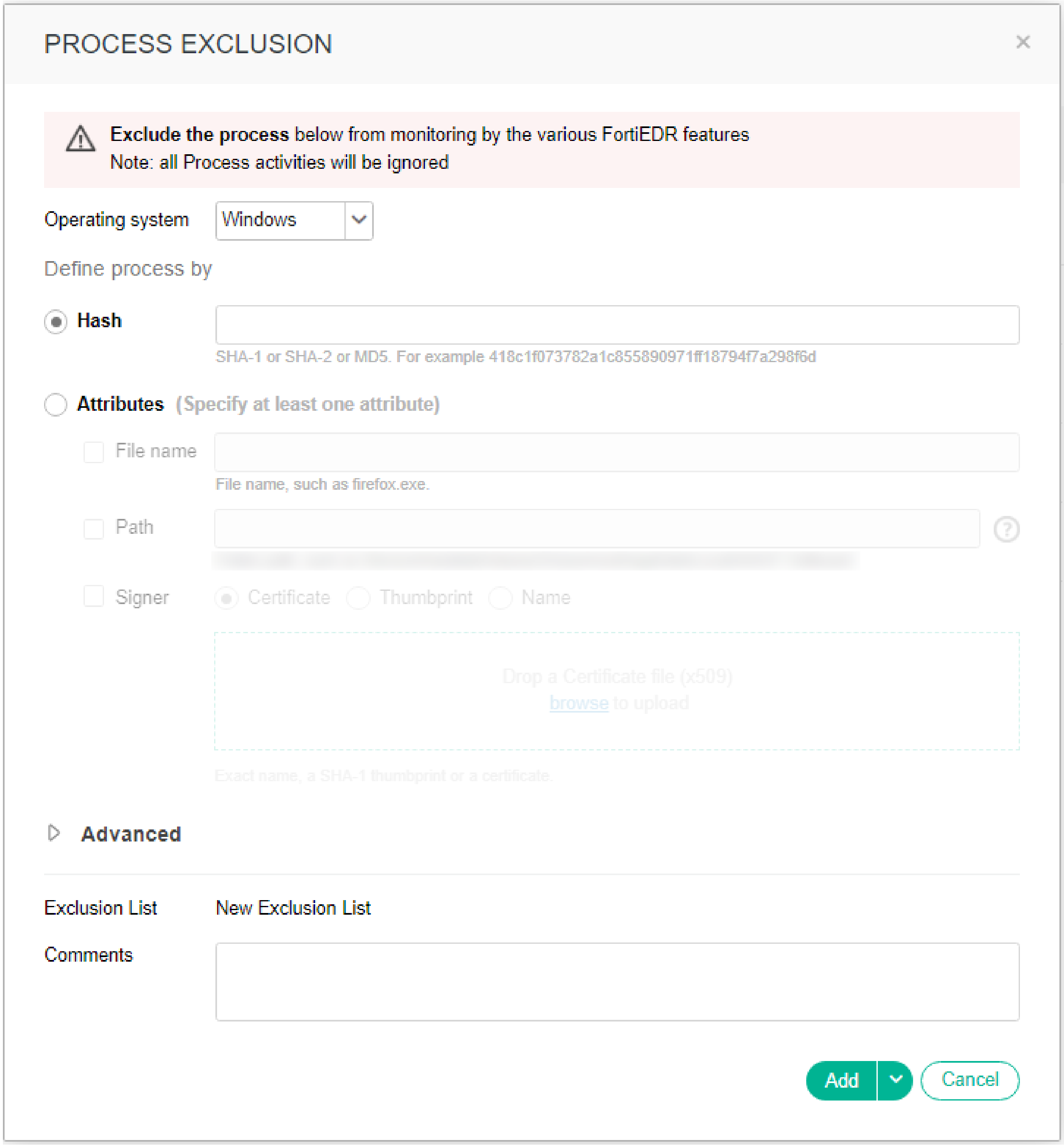
The following describes how to define a Process Exclusion (PC only), Execution Prevention Exclusion, and Domain Exclusion (mobile only).

Adding a Process Exclusion

1. In the left pane, click the PC Exclusion List to which to add the process exclusion.
2. In the right pane, click the *+ Add Exclusion* button. The following displays providing a choice of the two types of exclusions that you can define.



3. Select *Process*. The following displays:



PROCESS EXCLUSION ×

⚠ **Exclude the process** below from monitoring by the various FortiEDR features
Note: all Process activities will be ignored

Operating system: Windows

Define process by

● **Hash**
SHA-1 or SHA-2 or MD5. For example 418c1f073782a1c855890971ff18794f7a298f6d

○ **Attributes** (Specify at least one attribute)

□ File name
File name, such as firefox.exe.

□ Path ?

□ Signer ● Certificate ○ Thumbprint ○ Name

Drop a Certificate file (x509)
browse to upload

Exact name, a SHA-1 thumbprint or a certificate.

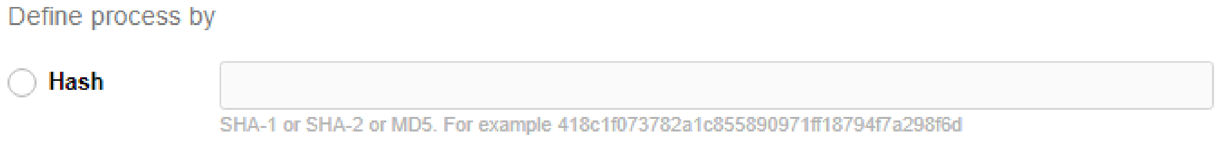
▷ **Advanced**

Exclusion List: New Exclusion List

Comments

4. The *Operating system* dropdown menu specifies *Windows*, which is currently the only operating system supported for exclusions.
5. Define the processes to be excluded using one of the following options: **Hash** or any combination of **File Name / Path / Signer**, as follows:

- **Hash**: Mark the Hash radio button and specify the Hash that uniquely identifies this process.

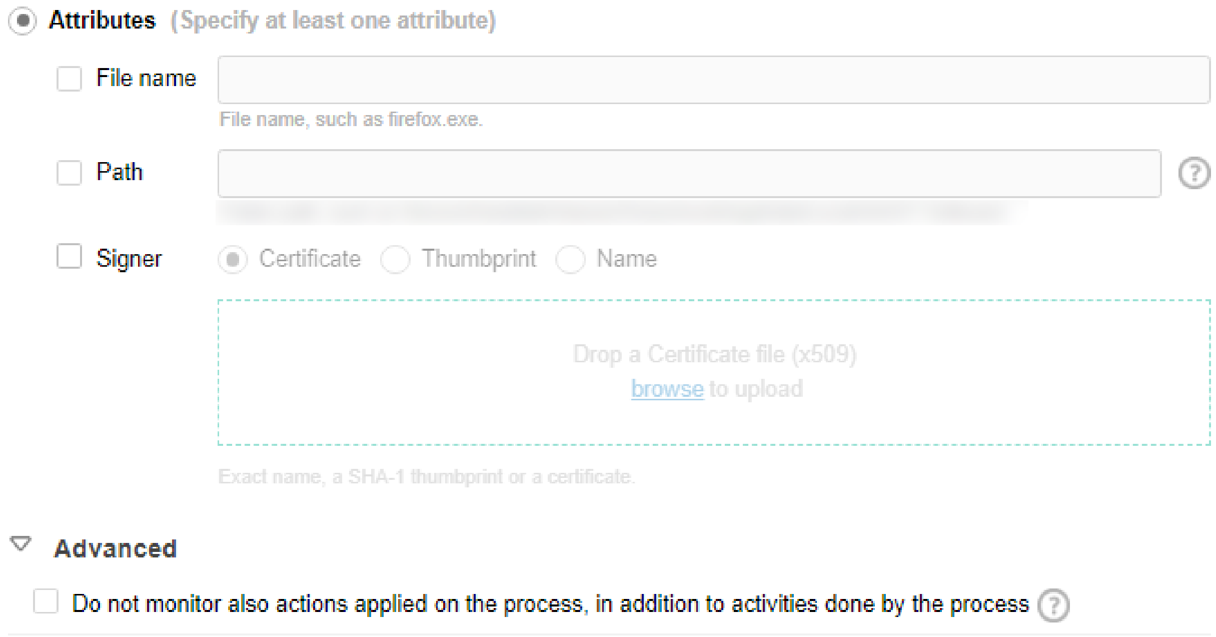


Define process by

○ Hash

SHA-1 or SHA-2 or MD5. For example 418c1f073782a1c855890971ff18794f7a298f6d

- **File Name / Path / Signer**: Mark the *Attributes* radio button and check at least one of the *File Name / Path / Signer* fields checkboxes and fill the relevant values, as follows:



● Attributes (Specify at least one attribute)

□ File name

File name, such as firefox.exe.

□ Path

□ Signer ● Certificate ○ Thumbprint ○ Name

Drop a Certificate file (x509)
browse to upload

Exact name, a SHA-1 thumbprint or a certificate.

▽ Advanced

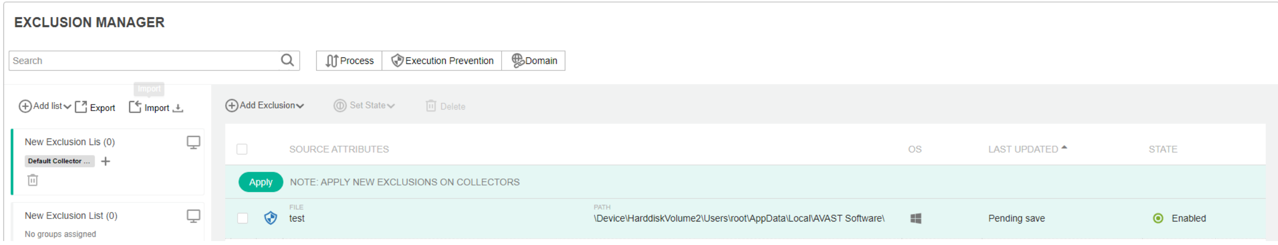
□ Do not monitor also actions applied on the process, in addition to activities done by the process

  - Specify the file and/or directory to be excluded by filling in the *File name* field, the *Path* field or both. If you fill in both fields, then that file is only excluded in that path. If you only fill in the *File name* field, then that file is excluded wherever it appears. Refer to the Defining an exclusion path on page 220 section for more details about defining an exclusion path.
  - If you want to specify a signer, select *Signer*, then either upload the Signer's Certificate, provide its thumbprint or provide the Signer's name.
  - When a process is identified by file name and/or path only (which means *Signer* is not selected), you can disable monitoring of the process completely, including actions applied on the process, by selecting *Do not monitor also actions applied on the process, in addition to activities done by the process* under *Advanced*.

This option significantly reduces FortiEDR protection on the process and lowers the security level of the process. Use this option only for issues that regular exclusions cannot solve, such as VDI freezes or other application malfunctions due to basic monitoring of the process by the FortiEDR Collector.

6. The *Exclusion List* field specifies the Exclusion List that was selected, when the *Add Exclusion* option was selected. This field is not editable.

7. Click the *Add* button. This new exclusion is then listed in the *Exclusion Manager* page, as shown below:



NOTE: APPLY NEW EXCLUSIONS ON COLLECTORS

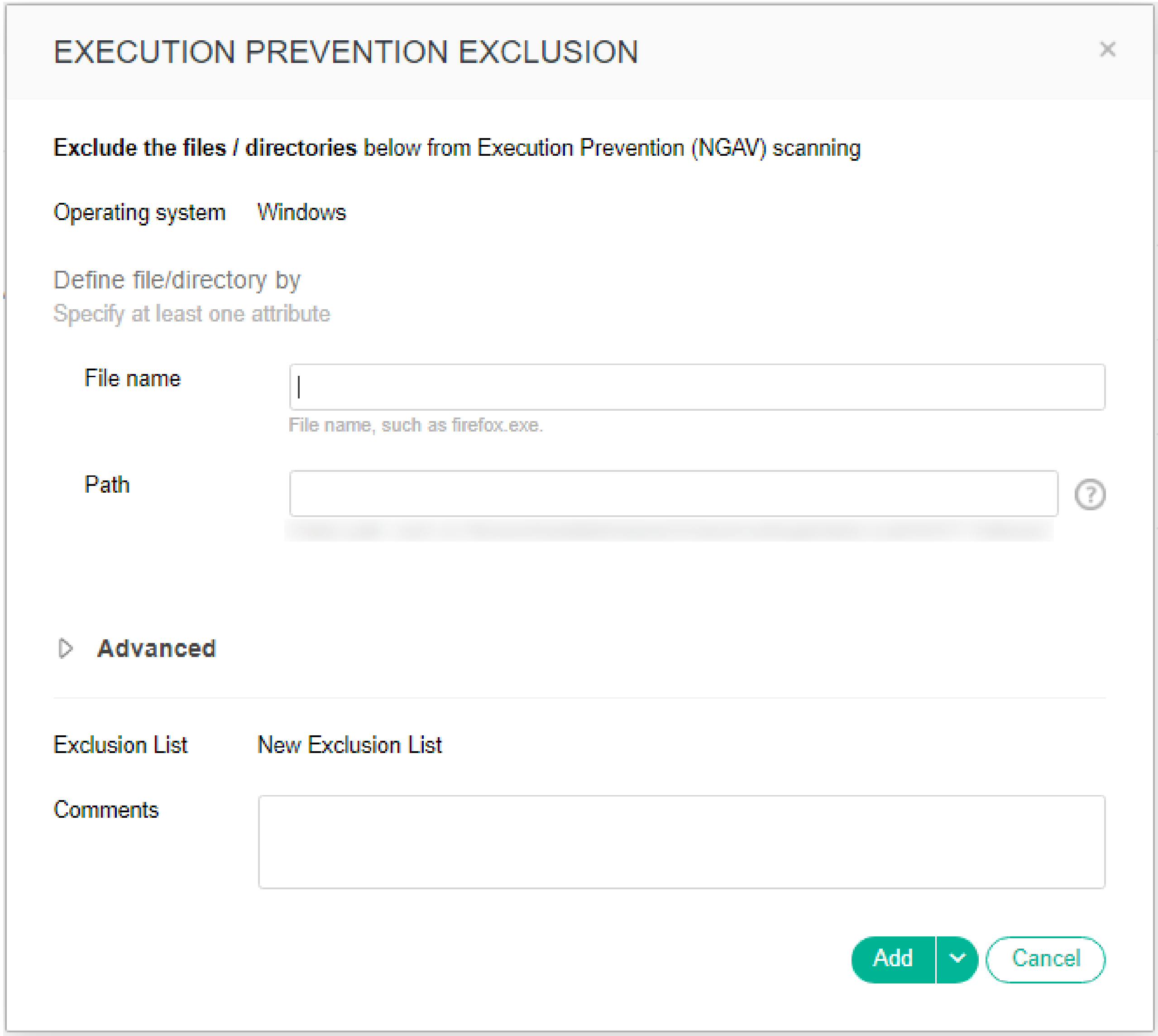
SOURCE ATTRIBUTES		OS	LAST UPDATED	STATE
FILE test	PATH \Device\HarddiskVolume2\Users\root\AppData\Local\AVAST Software\		Pending save	Enabled

8. The newly defined exclusions appear with a green background and the words *Pending save* appear in their *LAST UPDATED* column. To define that these exclusions take effect, you must click the *Apply* button and then click the *Save* button in the window that pops up. Their *LAST UPDATED* column then shows the timestamp when they were saved.

Adding an Execution Prevention Exclusion

1. In the left pane, click the Exclusion List to which to add the exclusion.
2. In the right pane, click the *+ Add Exclusion* button and select *Execution Prevention*. Depending on the exclusion list type (PC or mobile), one of the following windows displays:

3.



EXECUTION PREVENTION EXCLUSION

Exclude the files / directories below from Execution Prevention (NGAV) scanning

Operating system: Windows

Define file/directory by

Specify at least one attribute

File name: |

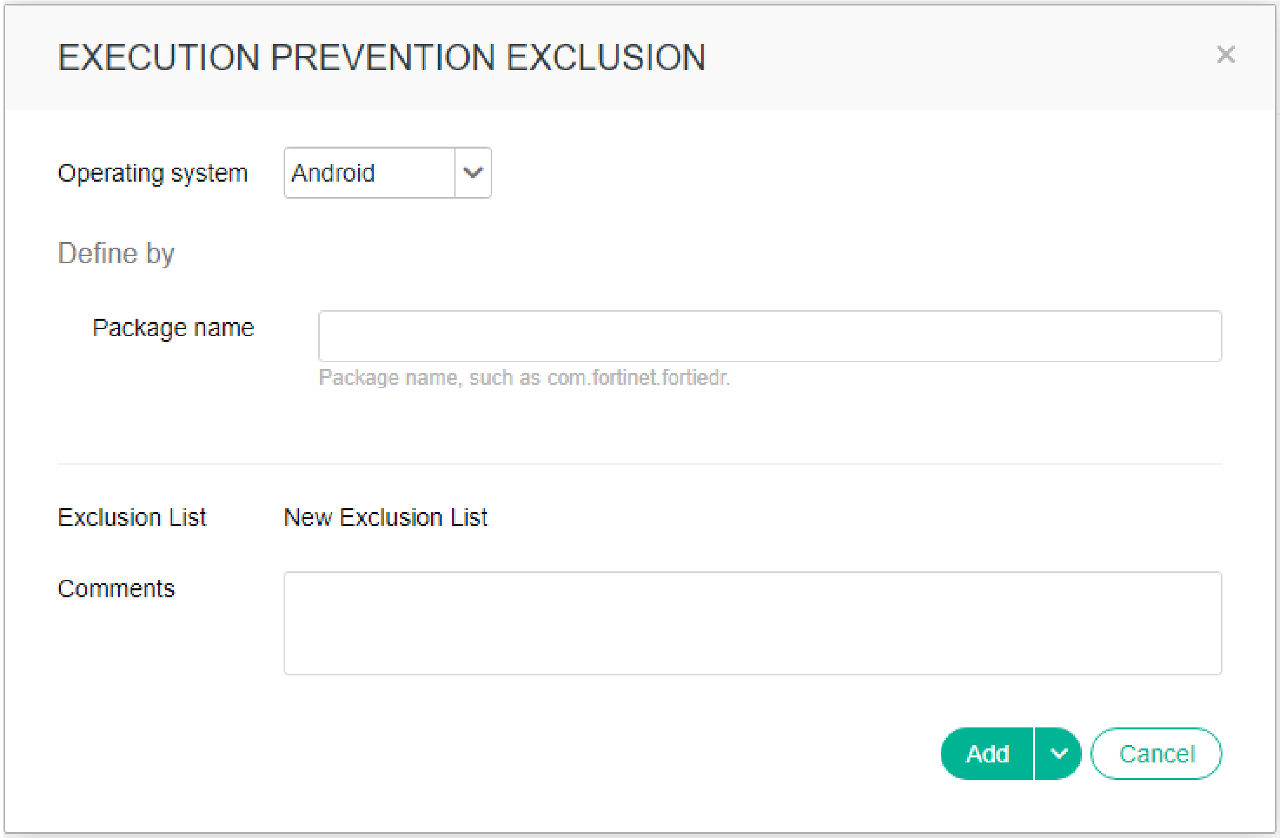
File name, such as firefox.exe.

Path:

[illegible]

Exclusion List: New Exclusion List

Comments:



EXECUTION PREVENTION EXCLUSION

Operating system: Android

Define by

Package name

Package name, such as com.fortinet.fortiedr.

Exclusion List: New Exclusion List

Comments

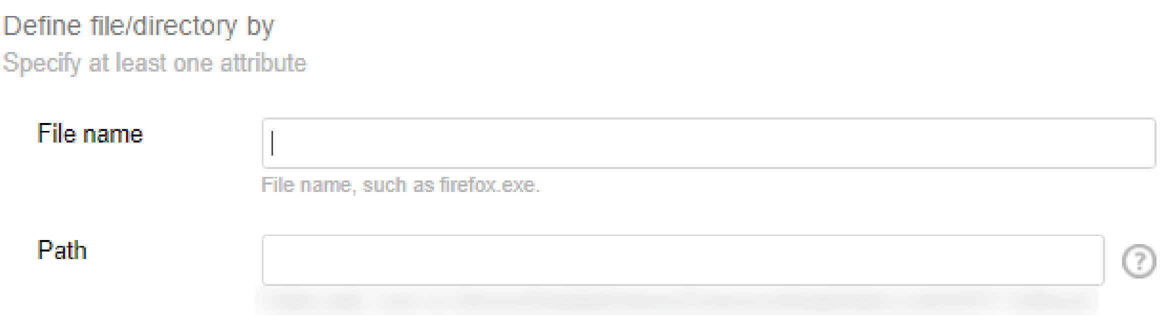
The *Android* option is available only if mobile is enabled in the organization setting. See Step 2 – Defining or importing an organization on page 419.

4. Specify the values to define the exclusion:

- For PC, follow the steps below:

  The *Operating system* dropdown menu specifies *Windows*, which is currently the only operating system supported for exclusions.

  i. Specify the file and/or directory to be excluded by filling in the *File name* field, the *Path* field or both. If you fill in both fields, then that file is only excluded in that path. If you only fill in the *File name* field, then that file is excluded wherever it appears. Refer to the Defining an exclusion path on page 220 section for more details about defining an exclusion path.



Define file/directory by

Specify at least one attribute

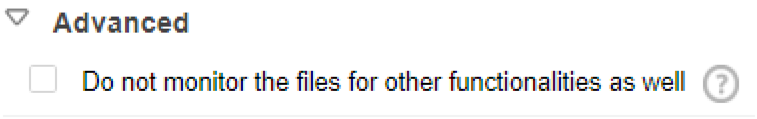
File name

File name, such as firefox.exe.

Path

ii. Under *Advanced*, you can select *Do not monitor the files for other functionalities as well* to disable monitoring of the file/directory completely, including backup of the files for Ransomware protection.

> This option significantly reduces FortiEDR protection on the files and lowers the security level of the files. Use this option only for issues that regular exclusions cannot solve, such as VDI freezes or other application malfunctions due to basic monitoring of the files by the FortiEDR Collector.



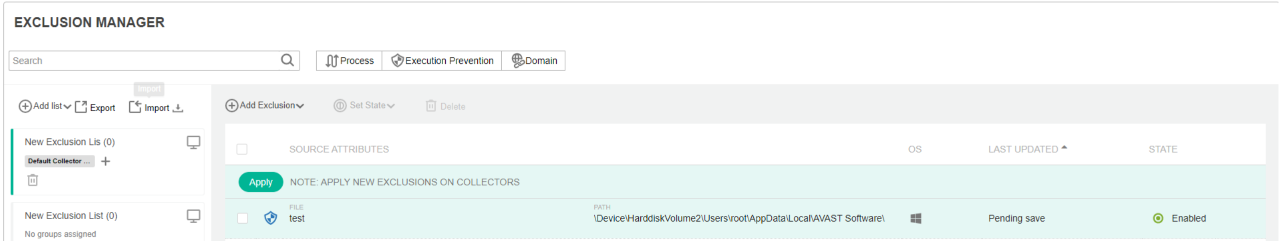
Advanced

□ Do not monitor the files for other functionalities as well

iii. The *Exclusion List* field specifies the Exclusion List that was selected, when the *Add Exclusion* option was selected. This field is not editable.

- For mobile, select *Android* for *Operating system* and specify the package name. Note that FortiEDR does not support execution prevention on iOS.

5. Click the *Add* button. This new exclusion is then listed in the *Exclusion Manager* page, as shown below:



EXCLUSION MANAGER

New Exclusion Lis (0)

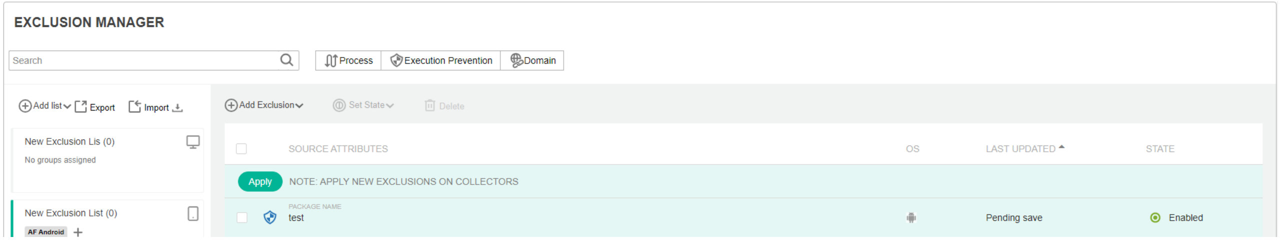
Default Collector ...

New Exclusion List (0)

No groups assigned

	SOURCE ATTRIBUTES		OS	LAST UPDATED	STATE
Apply	NOTE: APPLY NEW EXCLUSIONS ON COLLECTORS				
□	FILE test	PATH \Device\HarddiskVolume2\Users\root\AppData\Local\AVAST Software\		Pending save	Enabled

6.



EXCLUSION MANAGER

New Exclusion Lis (0)

No groups assigned

New Exclusion List (0)

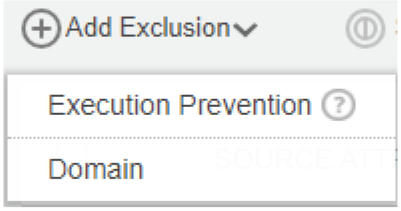
AF Android

	SOURCE ATTRIBUTES	OS	LAST UPDATED	STATE
Apply	NOTE: APPLY NEW EXCLUSIONS ON COLLECTORS			
□	PACKAGE NAME test		Pending save	Enabled

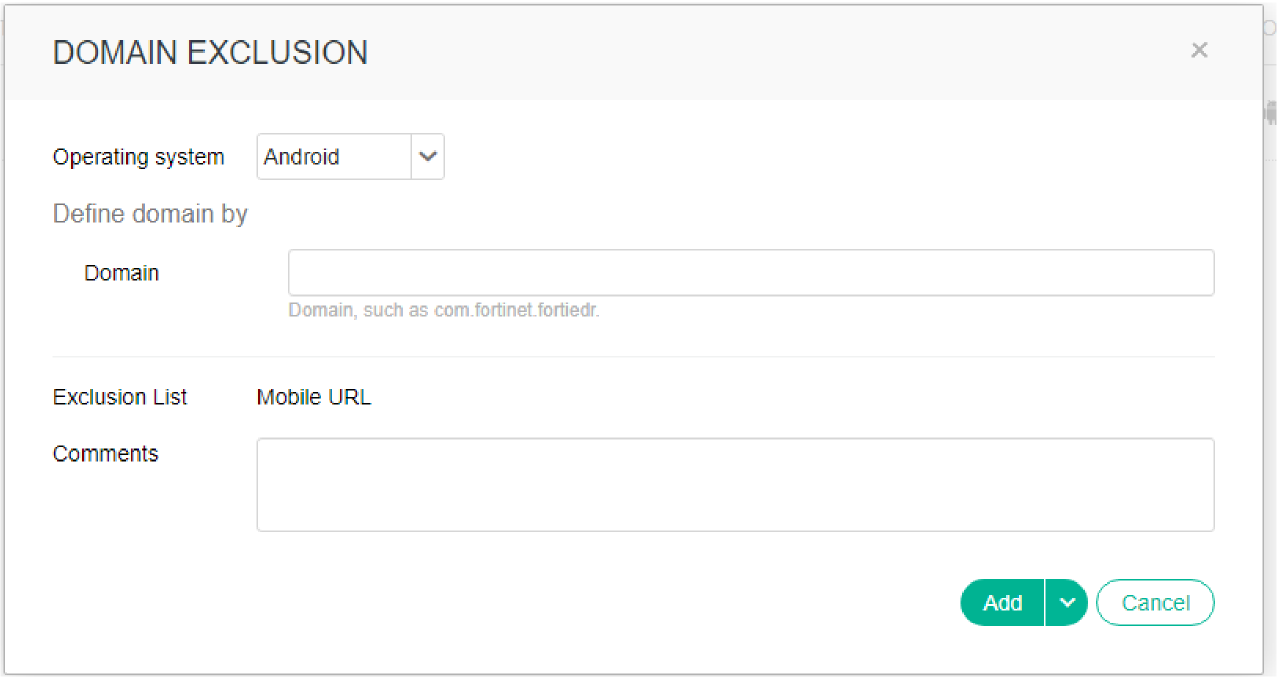
7. The newly defined exclusion appears with a green background and the words *Pending save* appear in its *LAST UPDATED* column. To define that these exclusions take effect, you must click the *Apply* button and then click the *Save* button in the window that pops up. Their *LAST UPDATED* column then shows the timestamp when they were saved.

(Mobile only) Adding a Domain Exclusion

1. In the left pane, click the mobile Exclusion List to which to add the domain exclusion.
2. In the right pane, click the *+ Add Exclusion* button. The following displays providing a choice of the two types of exclusions that you can define.



3. Select *Domain*. The following displays:



Operating system: Android

Exclusion List: Mobile URL

4. In the *Operating system* dropdown menu, select *Android* or *iOS*.
5. Specify the domain to exclude.
6. Click the *Add* button. This new exclusion is then listed in the *Exclusion Manager* page., as shown below:
7. The newly defined exclusions appear with a green background and the words *Pending save* appear in their *LAST UPDATED* column. To define that these exclusions take effect, you must click the *Apply* button and then click the *Save* button in the window that pops up. Their *LAST UPDATED* column then shows the timestamp when they were saved.

Defining an exclusion path

The table below provides examples of exclusion paths with explanations of which folders apply or do not apply:

Exclusion path	Folders that apply	Folders that do not apply
\Documents\Personal\	\Documents\Personal	• \Documents • \Documents\Personal\temp
\Documents\Personal\*	• \Documents\Personal\subfolder\ • \Documents\Personal\subfolder\subfolder\etc\	• \Documents • \Documents\Personal
\Documents\Personal*\	• \Documents\Personal • \Documents\Personal2 • \Documents\Personal\subfolder\	\Documents
*\Documents\Personal\	• \Documents\Personal • \Windows\Documents\Personal	• \Documents • \Documents\Personal\temp
*\Documents\Personal\*	• \Documents\Personal\subfolder\ • \Parent\Documents\Personal\subfolder	• \Documents • \Documents\Personal

- Including a wildcard in a path excludes only the parent folders and/or sub-folders and files within those parent and/or sub-folders but not the folder itself. To exclude a directory and also the parent or sub-directories, you must define an exclusion path for each case. For example, to exclude `\Documents\Personal` and all the sub-folders, define the following exclusion paths:
  - `\Documents\Personal`
  - `\Documents\Personal\*`
- Physical prefix (e.g. `\Device`) and logical prefix or drive (e.g., `C:\`) are not required in the exclusion path.

Setting the state of an exclusion

The *Set State* button enables you to enable or disable the selected exclusion(s). By default, an exclusion is enabled.

For changing the state of multiple Exclusions, check the checkboxes of all relevant exclusions and then select the state from the *Set State* dropdown under the toolbar.

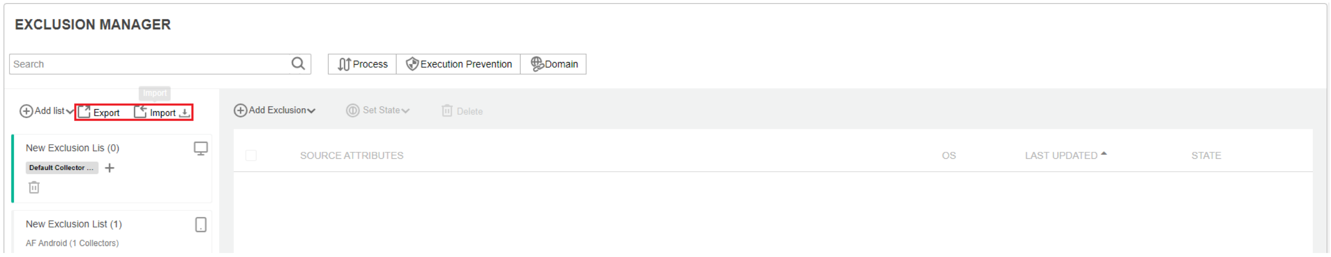
Deleting an exclusion

The *Delete* Exclusion button enables you to delete the selected exclusion(s).

To delete multiple Exclusions, check the checkboxes of all relevant exclusions and then select the *Delete* option in the toolbar.

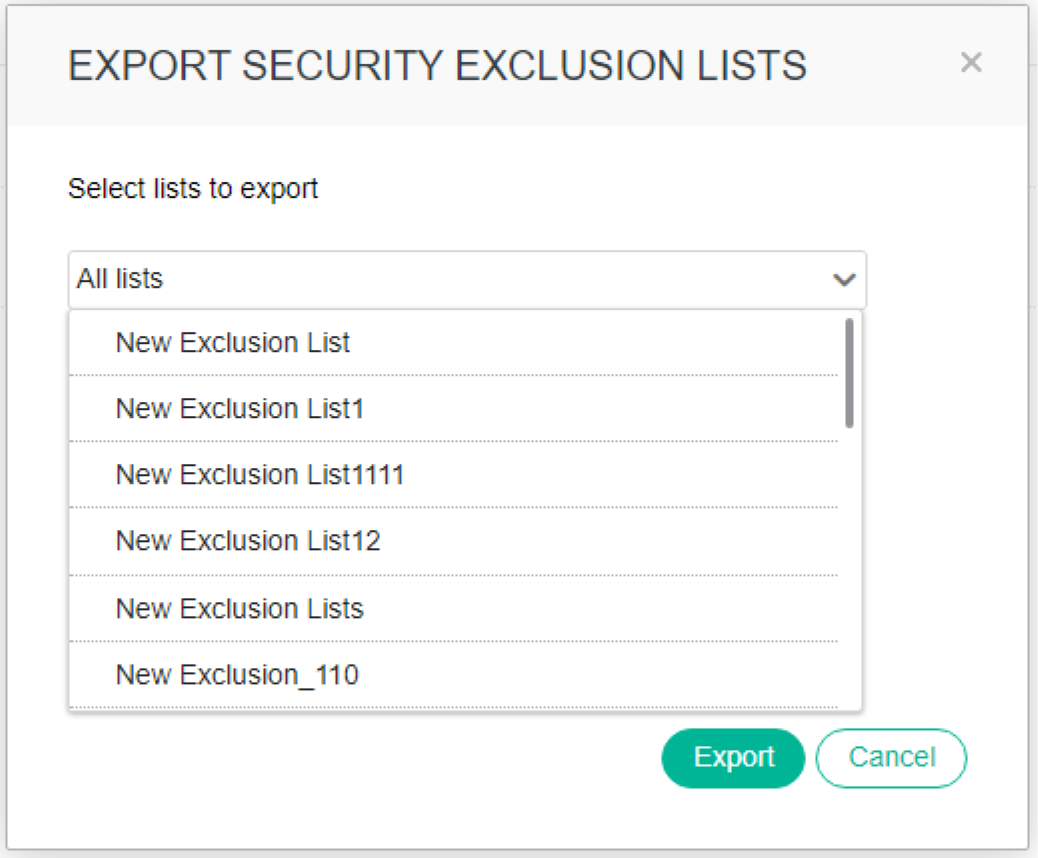
Exporting and importing exclusion lists

You can export or import exclusion lists for Process Exclusions and Execution Prevention Exclusions using the *Export* and *Import* buttons at the top-left of the Exclusion Manager page. This function is handy in a muiti-tenant environment where you can easily duplicate the exclusion lists for some or all organizations without the need to re-define exclusions for each organization separately.



To export one or multiple exclusion lists:

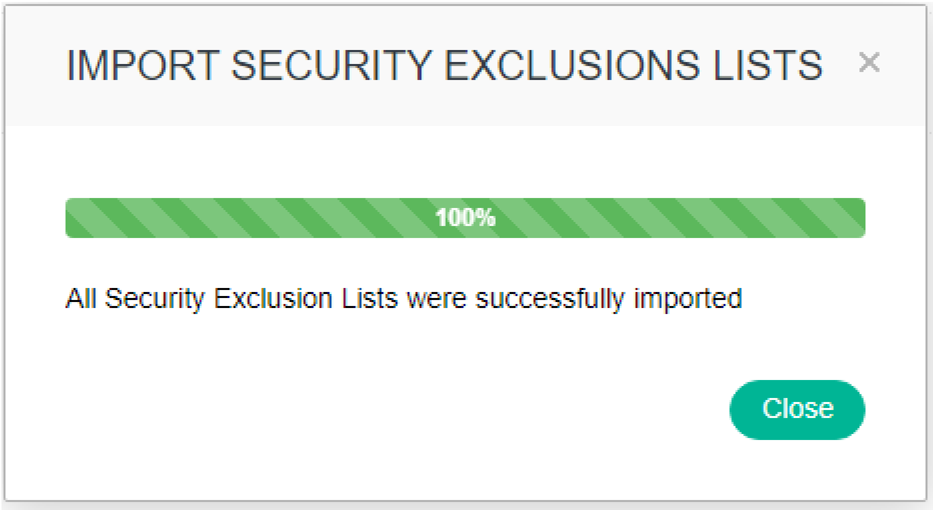
1. In the Exclusion Manager page, click *Export* at the top-left corner.
2. In the window that appears, select the list(s) to export. To export all lists, select *All lists*.



3. Click *Export*.
4. After the export is complete, click *Download* to save the file and then click *Close*.
   The file includes all exported exclusions and the exclusion lists that each exclusion belongs to.

To import one or multiple exclusion lists:

1. In the Exclusion Manager page, click *Import* at the top-left corner.
2. Select the list(s) to import (that you have saved or exported) and click *Open*.
3. Wait for the import to complete and click *Close*.



IMPORT SECURITY EXCLUSIONS LISTS

All Security Exclusion Lists were successfully imported

If a list name in the imported list already exists in the system, FortiEDR adds a suffix to the name of the newly imported list without touching the existing list.

For example, if the list name "AV" already exists, FortiEDR renames the imported list as "AV_1" that will appear in addition to the existing "AV" list. If such a list name ("AV") gets imported again, FortiEDR increments the number in the suffix of the list name for each subsequent import, which would be "AV_2", "AV_3", etc.

Application Control

The Application Control policy enables FortiEDR to block pre-defined applications from running, so that it does not launch. It enables limiting the usage of non-desired applications on specific collector groups.

This differs from Applications on page 168 under *Communication Control*, which enables you to control which applications can communicate outside of the organization, but does not stop them from launching.

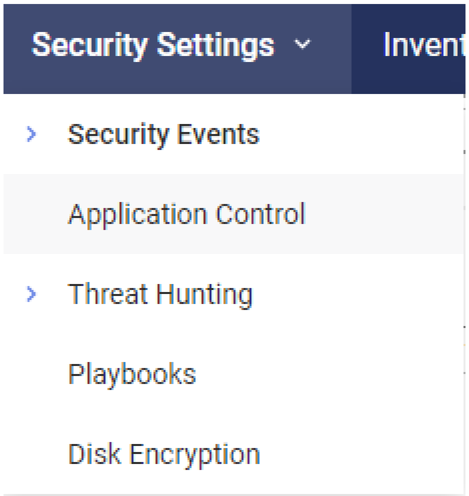
This section describes how to define the applications to be blocked by adding them in the Application Control. In addition, applications can be added to the list of applications to be blocked by adding them from the Investigation View on page 92. These applications are then listed in the Application Control Manager.

In general, in order to block applications so that they are not launched

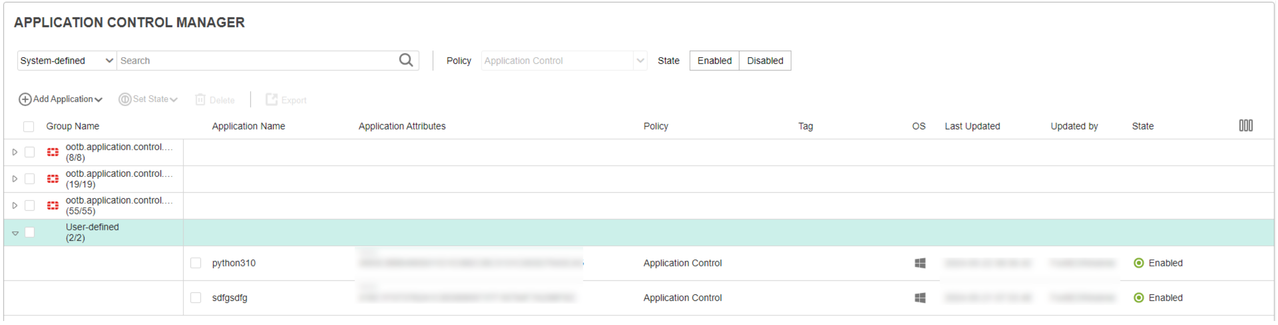
- The applications must be added to the Application Control Manager under the user-defined group
- Collector groups must be assigned to this policy
- The blocklist rule must be enabled on the Application Control Policy.

To add applications to the blocklist:

1. Select *SECURITY SETTINGS > Application Control* .



The following window displays, showing a list of different groups of applications that have been defined to be blocked by the Application Control policies.



Group Name	Application Name	Application Attributes	Policy	Tag	OS	Last Updated	Updated by	State
ootb.application.control.... (8/8)								
ootb.application.control.... (19/19)								
ootb.application.control.... (55/55)								
User-defined (2/2)								
	python310	[redacted]	Application Control		⊞	[redacted]	[redacted]	● Enabled
	sdfgsdfg	[redacted]	Application Control		⊞	[redacted]	[redacted]	● Enabled

Predefined application groups (indicated by the Fortinet logo by the group name) are always at the top of the application list and are assigned to the *Application Control* policy by default. You cannot add or delete applications from predefined application groups but you can disable specific applications or change the policy settings.

Applications added by the user are automatically categorized under the *User-defined* group with a default state of disabled, which means they are not blocked by default.

> To change the default state of new applications to enabled so that they are blocked by default, enable the *Enable Default application state* option in the *Application Control Manager on page 334* section under *Administration > Tools*.

2. You can then perform any of the following actions:
   - Adding application(s) to be blocked on page 225
   - Exporting the list of applications to be blocked on page 230
   - Enabling/disabling application blocking on page 231
   - Changing the policy under which the application is blocked on page 231
   - Searching and filtering applications on page 232
   - Editing an Application by selecting the *Edit* ✎ button on the right side of that Application’s row.

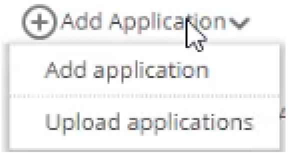
- Deleting an Application by selecting the *Delete Application* option at the top of the window or selecting the *Delete* 🗑 button on the right side of that Application's row.

You cannot delete a group, change or search any group names.

Adding application(s) to be blocked

To add an application(s) to be blocked:

1. Click the + *Add Application* option. The following displays:



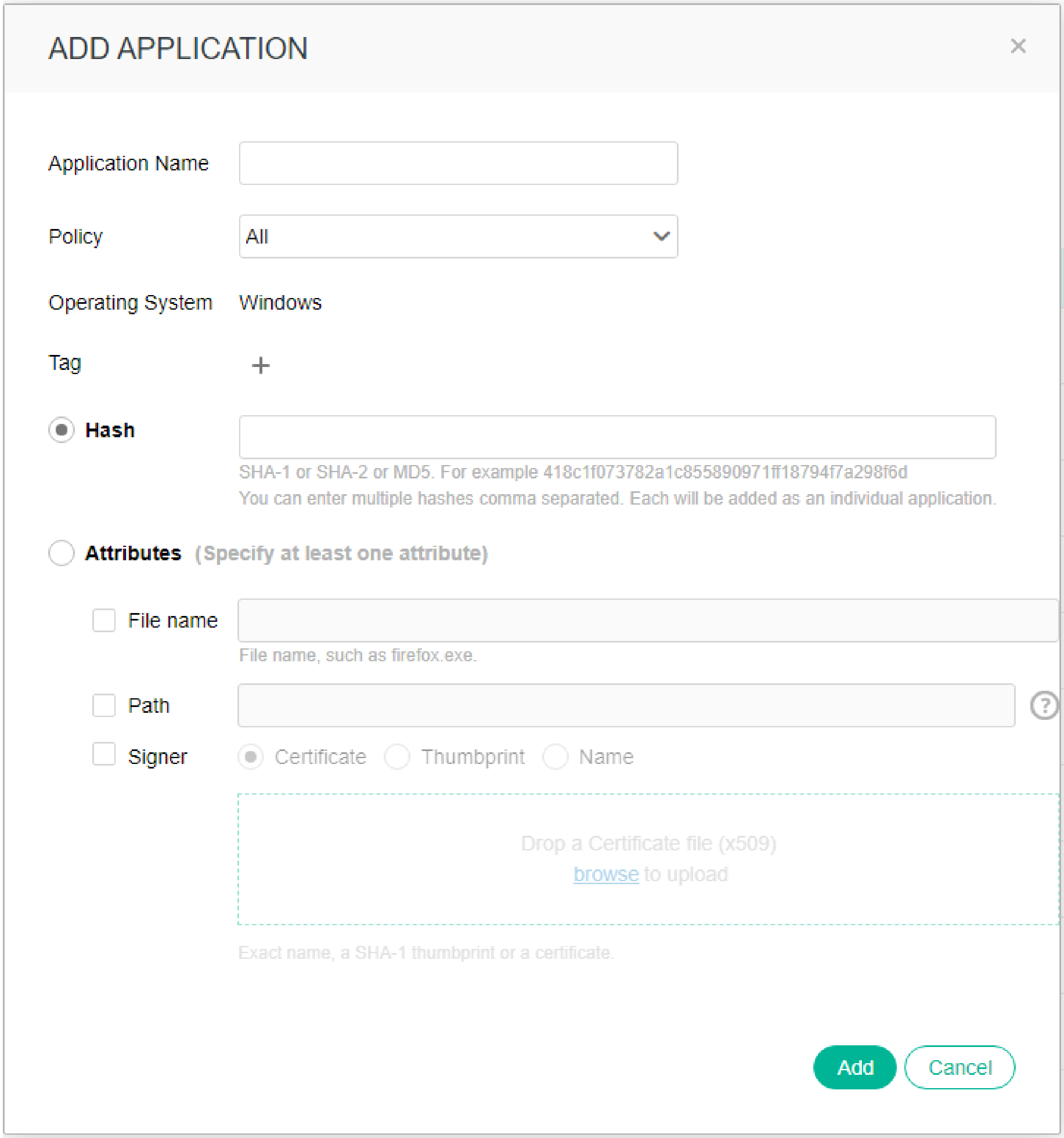
This dropdown menu provides two options for adding applications to be blocked:

- Manually adding an application to be blocked on page 226
- Uploading application(s) to be blocked on page 229

Manually adding an application to be blocked

To manually add an application to be blocked:

1. Select *Add application*. The following displays:



ADD APPLICATION

Application Name

Policy: All

Operating System: Windows

Tag +

● **Hash**

SHA-1 or SHA-2 or MD5. For example 418c1f073782a1c855890971ff18794f7a298f6d
You can enter multiple hashes comma separated. Each will be added as an individual application.

○ **Attributes** (Specify at least one attribute)

□ File name

File name, such as firefox.exe.

□ Path

□ Signer ● Certificate ○ Thumbprint ○ Name

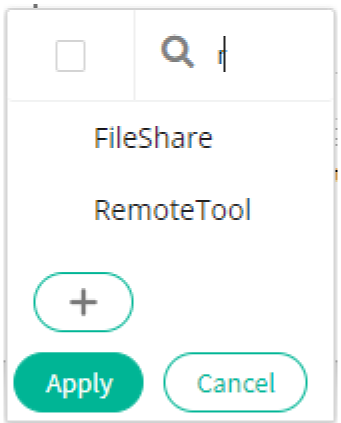
Drop a Certificate file (x509)
browse to upload

Exact name, a SHA-1 thumbprint or a certificate.

Add Cancel

2. In the *Application Name* field, specify a name to identify the application. The application name must be unique within the *User-defined* group.

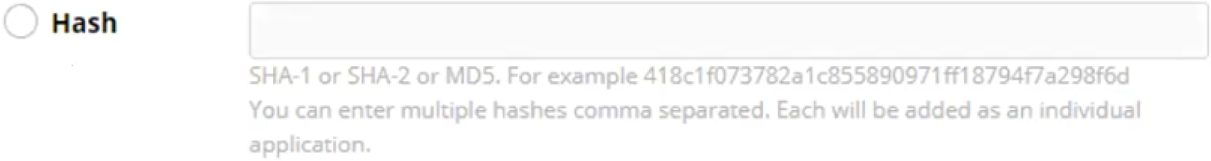
3. From the *Policy* dropdown menu, select one or more of the *Application Control* policies in which to block this application or select the *All* option to specify that this application is to be blocked by all Application Control type policies. FortiEDR is provided out-of-the-box with a single Application Control type policy and you can clone it in order to create additional Application Control type policies as needed.
4. You can optionally use the *Tag* field in order to classify this application. Tags can be helpful for classifying and filtering long lists of applications. In the *Tag* field, click the *Add* button + to specify the tag to be added to the application. You can assign a previously defined tag or define a new tag.



5. Define the application(s) to be blocked (so that they are not executed) using one of the following options: **Hash** or any combination of **File Name / Path / Signer**, as follows:

> FortiEDR blocks only executables and DLLs that meet the defined criteria. When determining whether a file is an executable, DLL, or another type, FortiEDR adheres to the file nature rather than the file name (such as the `.exe` extension).

- Hash: Mark the Hash radio button and specify one or more Hashes. Each hash is the unique identifier of an individual application. If you enter multiple hashes, then they must be comma separated. Supported hash formats are specified under the field.



SHA-1 or SHA-2 or MD5. For example 418c1f073782a1c855890971ff18794f7a298f6d
You can enter multiple hashes comma separated. Each will be added as an individual application.

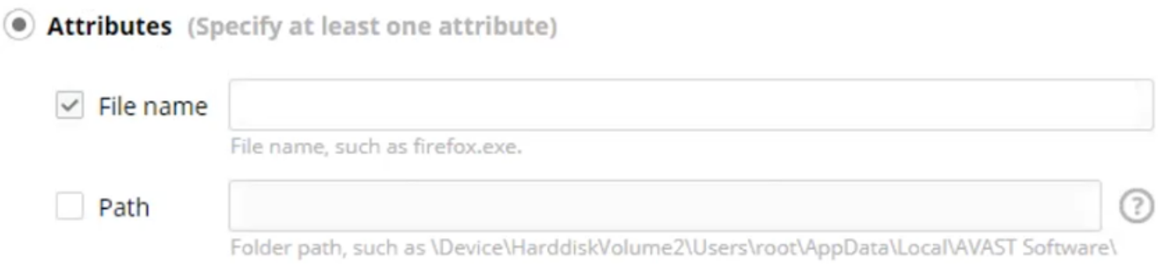
OR

- **File Name / Path / Signer**: Mark the *Attributes* radio button, check at least one of the *File Name / Path / Signer* fields checkboxes and fill the relevant values, as follows:
  - Specify the executable file of the application to be blocked by filling in the *File name* field.
  - Specify the path to the executable file of the application to be blocked by filling in the Path field.

    If you fill in both the *File name* field (described above) and the *Path* field, then that application is only blocked if its executable is in that path. If you only fill in the *File name* field, then that application is blocked no matter where its executable file appears.

    Wildcards can be used in a folder name by placing a single wildcard (*) at the beginning, end and middle of the path.

    For example: `*\folder0\folder1*\folder2*`



● **Attributes** (Specify at least one attribute)

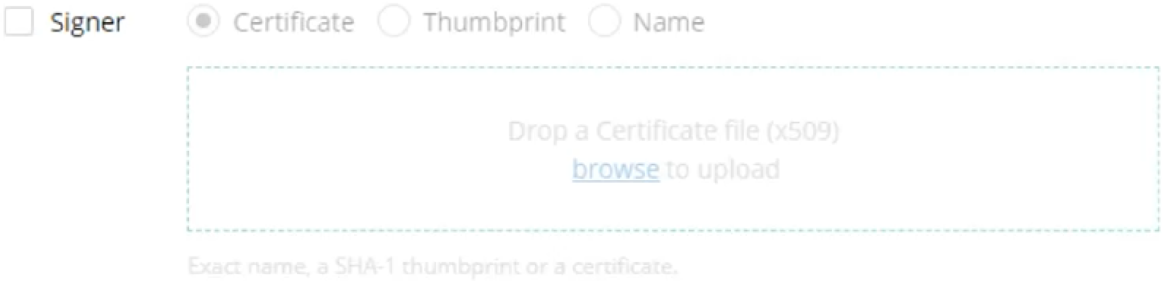
☑ File name

File name, such as firefox.exe.

□ Path

Folder path, such as \Device\HarddiskVolume2\Users\root\AppData\Local\AVAST Software\

- If you select *Signer*, then either upload the Signer's Certificate (as shown below), provide its thumbprint or type in the Signer's name. Uploading a certificate or specifying thumbprint is more secured that specifying signer name and hence recommended.

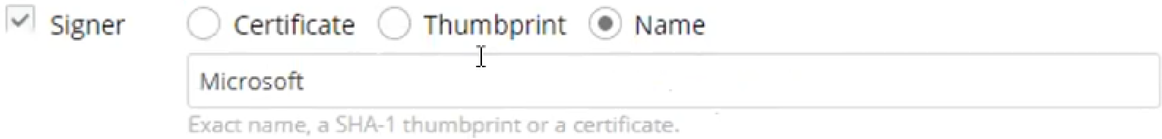


□ Signer ● Certificate ○ Thumbprint ○ Name

Drop a Certificate file (x509)
browse to upload

Exact name, a SHA-1 thumbprint or a certificate.

For example, selecting the *Name* radio button, then entering the word `Microsoft`, blocks the execution of any application that was signed by Microsoft. You must enter the exact name of the Signer.



☑ Signer ○ Certificate ○ Thumbprint ● Name

Microsoft

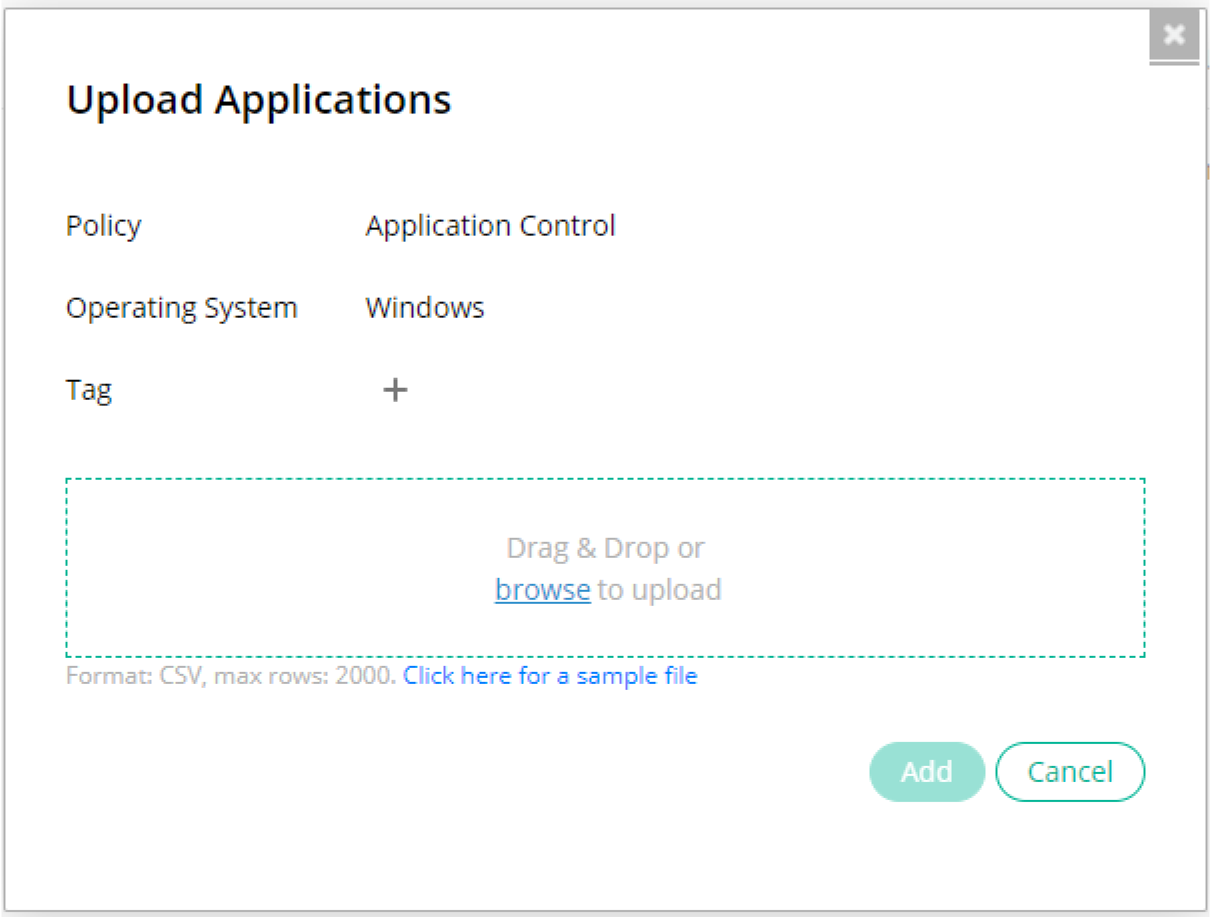
Exact name, a SHA-1 thumbprint or a certificate.

6. Click the *Add* button. The application is then listed under the *User-defined* group.
   When a Collector Group is assigned to the application control policy (specify above), then all these applications are blocked and cannot be launched.

Uploading application(s) to be blocked

To upload a list of applications to be blocked from a file:

1. Select *Add Application* > *Upload Applications*. The following displays:



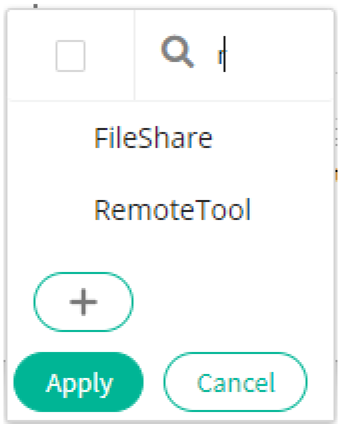
Upload Applications

Policy Application Control

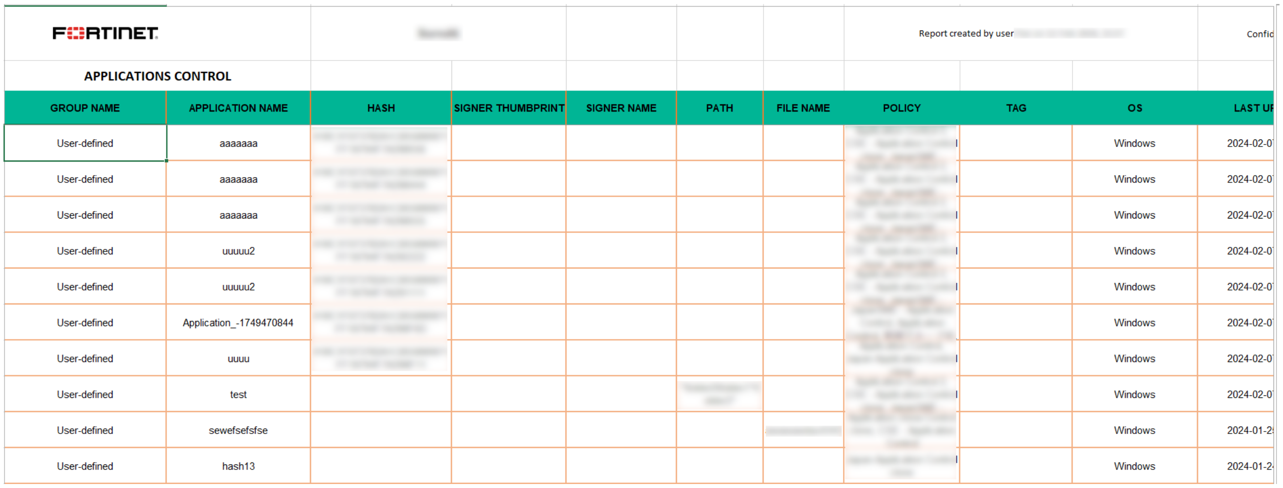
Operating System Windows

Tag +

2. From the *Policy* dropdown menu, select one or more of the *Application Control* policies in which to block the applications specified in the file to be uploaded.
3. You can optionally use the *Tag* field in order to classify this application. Tags can be helpful for classifying and filtering long lists of applications. In the *Tag* field, click to specify the tag to be added to the application. You can assign a previously defined tag or define a new tag.



4. In the bottommost field of this window, select the CSV file that contains the list of applications to be blocked. This file should be a CSV file in which the five leftmost columns (shown below) identify the application to be blocked. A sample file can be downloaded from this window. Alternatively, you can use the same file as can be exported, as described in Exporting the list of applications to be blocked on page 230.



FORTINET	[redacted]					Report created by user [redacted]			Confid
APPLICATIONS CONTROL									
GROUP NAME	APPLICATION NAME	HASH	SIGNER THUMBPRINT	SIGNER NAME	PATH	FILE NAME	POLICY	TAG	OS	LAST UP
User-defined	aaaaaaa	[redacted]					[redacted]		Windows	2024-02-0
User-defined	aaaaaaa	[redacted]					[redacted]		Windows	2024-02-0
User-defined	aaaaaaa	[redacted]					[redacted]		Windows	2024-02-0
User-defined	uuuuu2	[redacted]					[redacted]		Windows	2024-02-0
User-defined	uuuuu2	[redacted]					[redacted]		Windows	2024-02-0
User-defined	Application_-1749470844	[redacted]					[redacted]		Windows	2024-02-0
User-defined	uuuu	[redacted]					[redacted]		Windows	2024-02-0
User-defined	test				[redacted]		[redacted]		Windows	2024-02-0
User-defined	sewefsefsfse					[redacted]	[redacted]		Windows	2024-01-2
User-defined	hash13						[redacted]		Windows	2024-01-2

5. Click the *Add* button. The Application Control Manager then lists a row for each application in the uploaded file under the *User-defined* group.
When a Collector Group is assigned to the Application Control policy (specify above), then all the applications that are added will be blocked and will not be launched.

Exporting the list of applications to be blocked

To export the list of FortiEDR applications to be blocked:

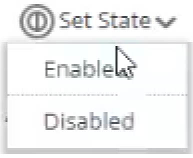
1. Select the group(s) that you want to export.
2. Click *Export* to export the applications list as an Excel file.

Enabling/disabling application blocking

If you wish to disable the blocking of all the applications that are under a specific policy, we recommend simply disabling the blocklist rule of that policy. Alternatively, in order to temporarily block only specific applications, then we recommend enabling/disabling each application separately. If an application no longer needs to be on the blocklist, then we recommend deleting it using the *Delete* button in the right-most column or in the toolbar.

To enable/disable the blocking of specific applications:

1. Select *SECURITY SETTINGS > Application Control* to display the Application Control Manager. Each row represents an application to be blocked.
2. Select the application(s) to block. To block all applications in a specific group, select the group instead.
3. In the *STATUS* column on the right, toggle the value between *Enabled* and *Disabled*. Alternatively, you can check the checkboxes of the desired application rows, and then select the *Enabled* or the *Disabled* option from the *Set State* dropdown.



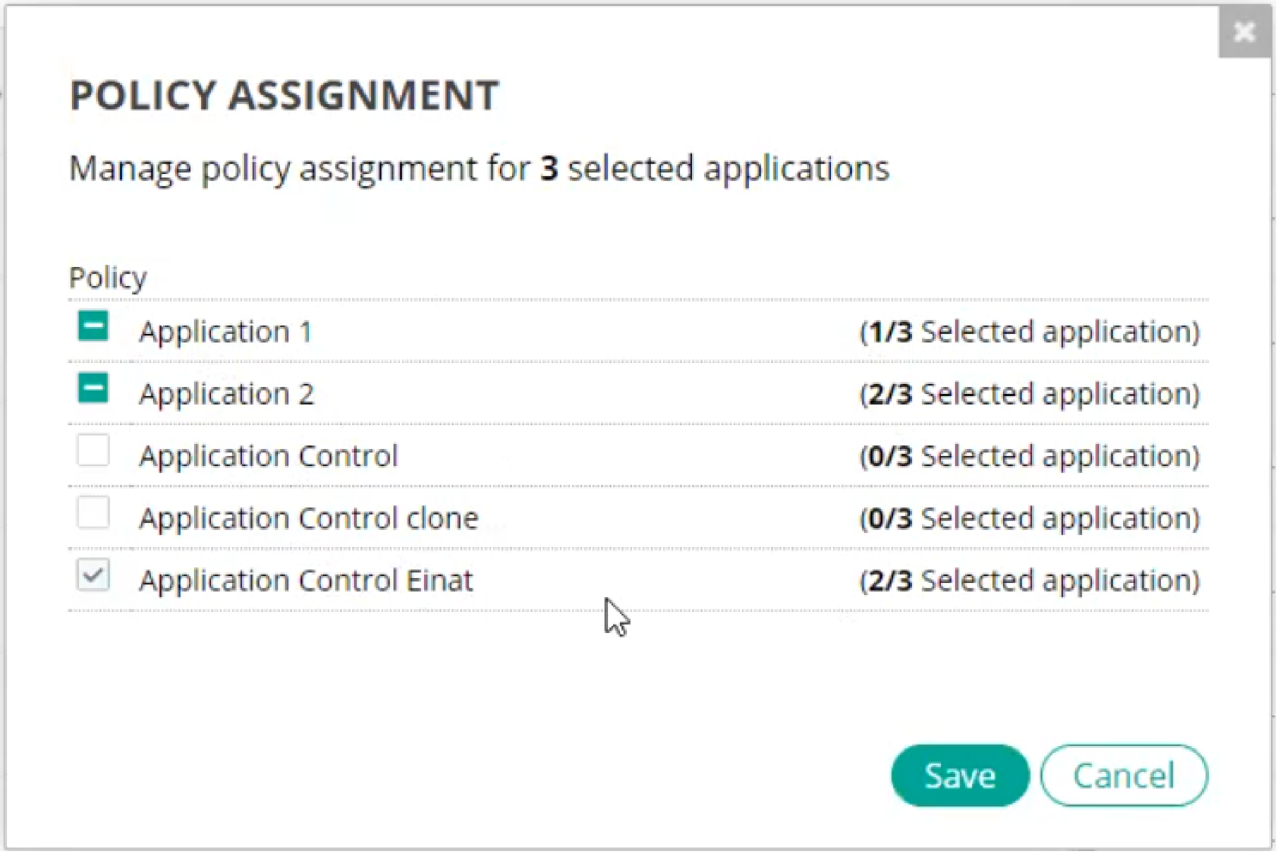
Newly added applications are set to be disabled by default, which means they are not blocked. To change the default state of new applications to enabled (so that they are blocked by default), enable the *Enable Default application state* option in the *Application Control Manager on page 334* section under *Administration > Settings*.

Changing the policy under which the application is blocked

To change the policy that blocks an application:

1. Select *SECURITY SETTINGS > Application Control* to display the Application Control Manager. Each row represents an application to be blocked.
2. In the Application Control Manager window, select the application(s) to change policy. To change policy of all applications in a specific group, select the group instead.

3. Click the *Policy Assignment* option. The following displays.



POLICY ASSIGNMENT

Manage policy assignment for **3** selected applications

Policy	
⊟ Application 1	(**1/3** Selected application)
⊟ Application 2	(**2/3** Selected application)
□ Application Control	(**0/3** Selected application)
□ Application Control clone	(**0/3** Selected application)
☑ Application Control Einat	(**2/3** Selected application)

The policies that have a checkbox ☑ to their left have already been assigned all the selected applications. The policies that have a green minus sign ⊟ to their left have already been assigned some of the applications. The right side of the window indicates how many of the applications that you selected in the Application Control Manager window have been assigned to that policy. The policies that have an empty box to their left were not assigned any of the selected applications.

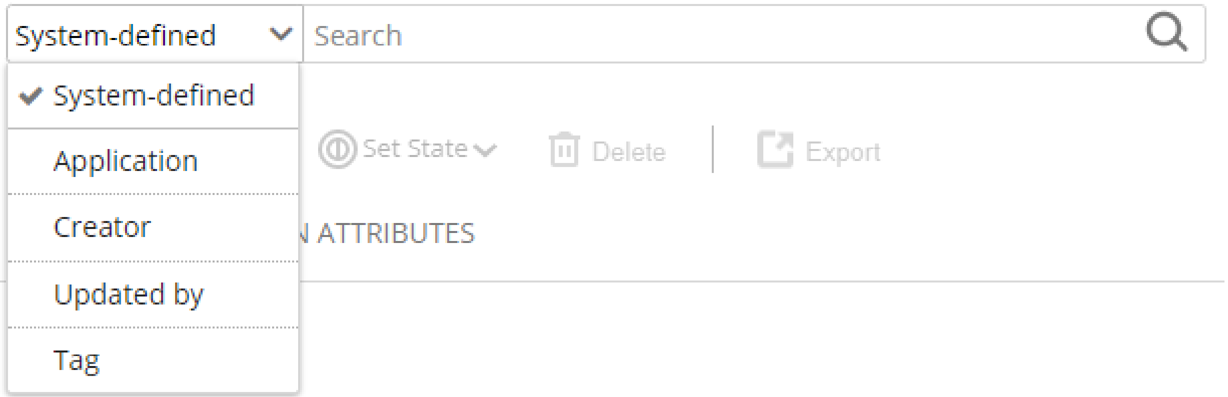
4. In the *Policy Assignment* window, check (or uncheck) the checkboxes of the policies that should block the currently selected applications.
5. Click the *Save* button.

Alternatively, in order to modify the policy to which a specific application is assigned, select the *Edit* ✎ button in the Application Control Manager window in the right side of that application's row.

Searching and filtering applications

To filter the list of applications defined in the Application Control Manager, use the fields at the top of the window, as follows:

1. Enter text in the *Search* field. This search field uses exact word matching.
   - By default, the *System-defined* option is selected, which specifies that the search is performed on the most relevant fields and then the list is filtered accordingly. Alternatively, from this dropdown menu, you can select the column that is searched, as follows:



2. Select the relevant policy from the *Policy* field.
3. In the *State* field, select *Enabled* or *Disabled*.

Threat Hunting

FortiEDR's threat-hunting capabilities feature a set of software tools and information sources focused on detecting, investigating, containing, and mitigating suspicious activities on end-user devices.

Threat Hunting Settings is a license-dependent add-on. You may contact Fortinet Support for more information.

To set up Threat Hunting in FortiEDR, configure the following:

- Collection profiles on page 233
- Collection Exclusions on page 236
- Threat Hunting data retention on page 243

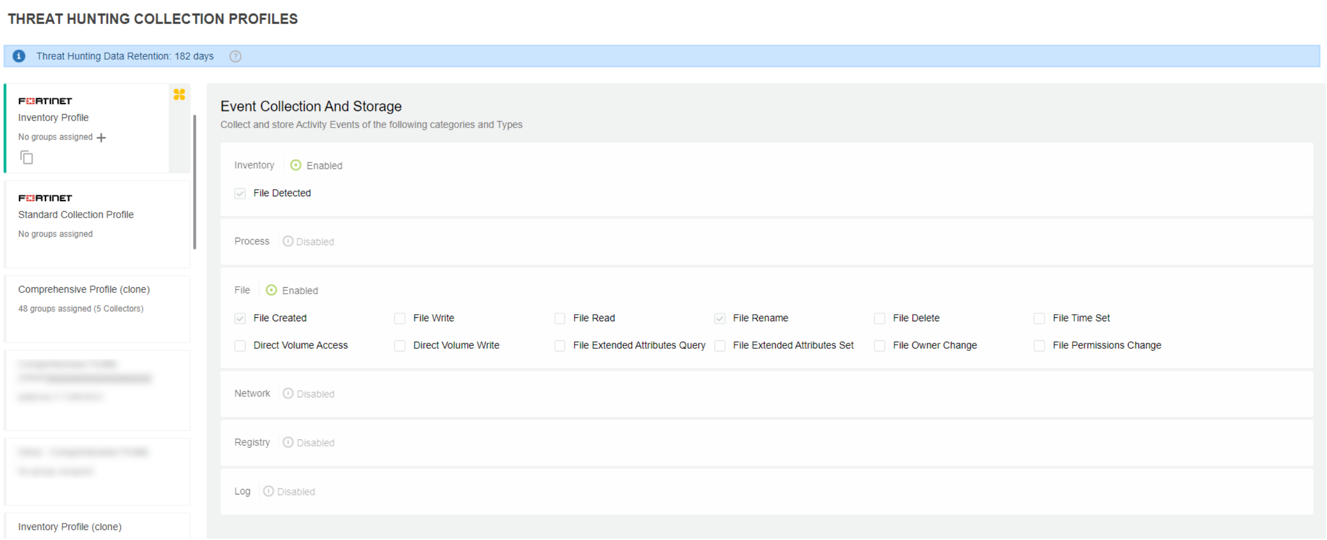
Collection profiles

Threat Hunting Settings is a license-dependent add-on. You may contact Fortinet Support for more information.

Threat Hunting Collection Profiles control the type of activity data that is collected for the Threat Hunting feature (which is described in Threat Hunting on page 125). Activity data that is collected is stored on the Repository server.

To access Threat Hunting settings, select *SECURITY SETTINGS* > *Threat Hunting Setting* > *Collection Profiles*.

The following page displays:



THREAT HUNTING COLLECTION PROFILES

Threat Hunting Data Retention: 182 days

FORTINET
Inventory Profile
No groups assigned +

FORTINET
Standard Collection Profile
No groups assigned

Comprehensive Profile (clone)
48 groups assigned (5 Collectors)

[redacted]

[redacted]

Inventory Profile (clone)

Event Collection And Storage
Collect and store Activity Events of the following categories and Types

Inventory ⊙ Enabled
☑ File Detected

Process ⓘ Disabled

File ⊙ Enabled
☑ File Created □ File Write □ File Read ☑ File Rename □ File Delete □ File Time Set
□ Direct Volume Access □ Direct Volume Write □ File Extended Attributes Query □ File Extended Attributes Set □ File Owner Change □ File Permissions Change

Network ⓘ Disabled

Registry ⓘ Disabled

Log ⓘ Disabled

The left side of the *Threat Hunting Settings* page shows a list of profiles. A profile defines the activity event categories and actions to be collected. FortiEDR comes with several predefined profiles, which cannot be modified. In addition to the pre-defined profiles, you can define your own custom profiles by cloning an existing profile.

The default collection profile for Collector groups is *Inventory Profile*, which is indicated by the *Default Collection Profile* (⌘) icon). To change the default profile, hover over to the top-right corner of the target profile card and click the *Set profile as the default profile* (⌘) icon.

You can also assign a collection profile to one or more Collector groups. See Assigning a Collector group to a profile on page 234.

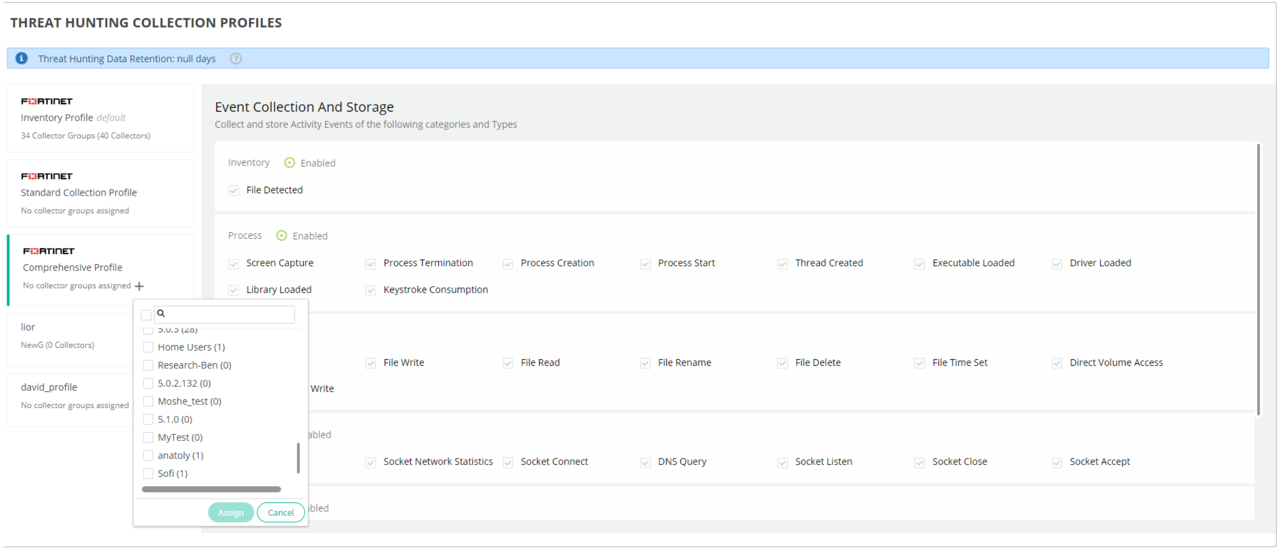
The pane on the right side of the page lists all activity event categories and their associated actions. These categories are the same as those described on Threat Hunting on page 125. Selecting a profile on the left displays the categories and actions defined for that profile in the right pane. Check the checkboxes of the actions for which FortiEDR will collect activity data.

Assigning a Collector group to a profile

Profiles are assigned to Collector groups. Only a single profile can be assigned to each Collector group.

To assign a Collector group to a profile:

1. In the *Profiles* pane, click the + button of the profile to which to assign a Collector group. The following displays showing the list of all Collector groups:

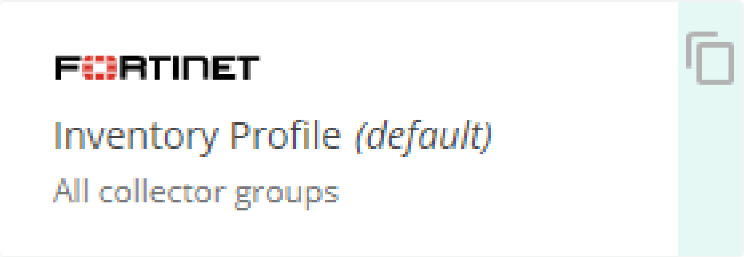


2. Select the checkbox(s) of the Collector group(s) to assign to the profile.
3. Click *Assign*.
4. When prompted with a message that the selected groups are currently assigned to another profile and will be reassigned, click *Assign* to confirm.

Creating/cloning a profile

In order to create a new Profile, you must first clone an existing Profile and then customize the clone.

1. Click the *Clone* icon that appears on the right of the profile to be cloned.



2. Enter the name of the new profile.
3. On the right side, enable the activity events to be collected and disable the activity events that should not be collected.
4. Click *Save*.
5. Assign the Collector group(s) on which to apply the newly created profile. See Assigning Collectors to a Collector Group on page 263.

Collection Exclusions

Exclusions are needed for reducing the amount of Threat Hunting data that is collected and by doing so prolonging the data retention. The less data that is collected, the longer it will be stored in the databases.

Exclusions enable you to define certain types of activity events to be excluded from being collected by Threat Hunting data (even though should be collected according to the Threat Hunting Collection Profile assigned to a Collector group, which was described in Collection profiles on page 233). For example, if you know that a certain process is legitimate, but it creates many activity events that are not relevant to your Threat Hunting investigation, you can use the Collection Exclusions to define that these activities are not collected.

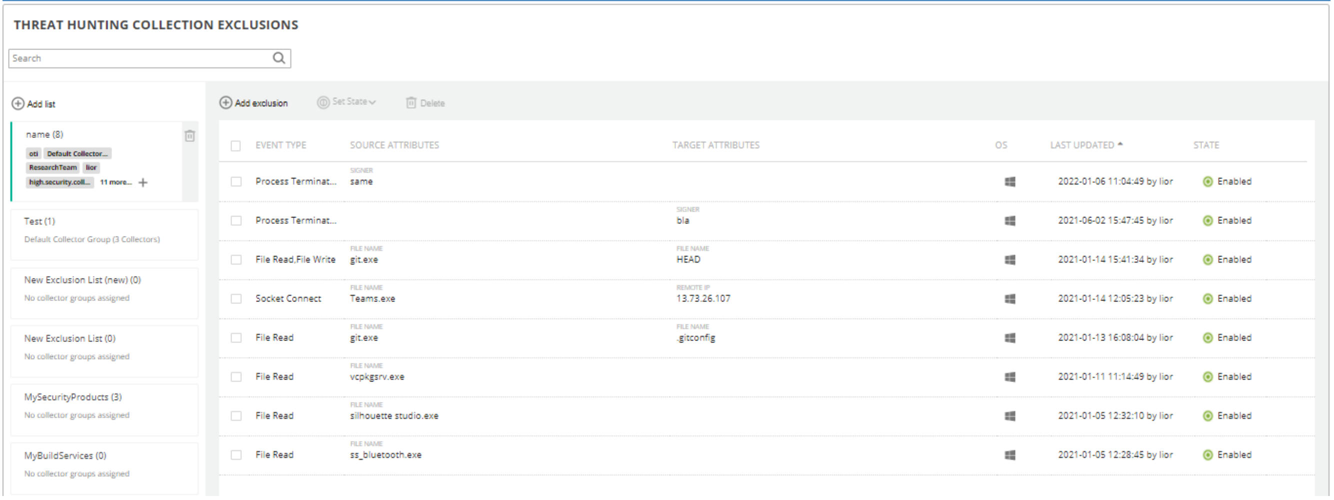
The Collection Exclusions enables you to define and manage exclusion lists and the exclusions that they contain.

Exclusions are different than security event exceptions, as follows:

- Exclusions define which activity events should be collected. They are exclusions to the Threat Hunting Profile.
- Security event exceptions are defined after a particular security event has occurred. They are an exception to the assigned Security Policy.

To access the Collection Exclusions, select *SECURITY SETTINGS* > *Threat Hunting* > *Collection Exclusions*.

The Collection Exclusions page contains the following areas:



name (8)
oti | Default Collector... | ResearchTeam | lior | high.security.coll... | 11 more...

Test (1)
Default Collector Group (3 Collectors)

New Exclusion List (new) (0)
No collector groups assigned

New Exclusion List (0)
No collector groups assigned

MySecurityProducts (3)
No collector groups assigned

MyBuildServices (0)
No collector groups assigned

□	EVENT TYPE	SOURCE ATTRIBUTES	TARGET ATTRIBUTES	OS	LAST UPDATED	STATE
□	Process Terminat...	SIGNER same		⊞	2022-01-06 11:04:49 by lior	Enabled
□	Process Terminat...		SIGNER bla	⊞	2021-06-02 15:47:45 by lior	Enabled
□	File Read,File Write	FILE NAME git.exe	FILE NAME HEAD	⊞	2021-01-14 15:41:34 by lior	Enabled
□	Socket Connect	FILE NAME Teams.exe	REMOTE IP 13.73.26.107	⊞	2021-01-14 12:05:23 by lior	Enabled
□	File Read	FILE NAME git.exe	FILE NAME .gitconfig	⊞	2021-01-13 16:08:04 by lior	Enabled
□	File Read	FILE NAME vcpkgsrv.exe		⊞	2021-01-11 11:14:49 by lior	Enabled
□	File Read	FILE NAME silhouette studio.exe		⊞	2021-01-05 12:32:10 by lior	Enabled
□	File Read	FILE NAME ss_bluetooth.exe		⊞	2021-01-05 12:28:45 by lior	Enabled

Filters

To filter the Collection Exclusion list names and its content, simply enter text in the *Search* field. Afterwards, only the Exclusion lists that match the provided text are displayed showing only the relevant exclusions.

Defining Collection Exclusion Lists

A Collection Exclusion List contains a list of exclusions. You can assign Collector Groups to an Exclusion List in order to specify that the exclusions in the Exclusion List apply to the Collectors in the Collector Groups assigned to it. Exclusion Lists enable you to logically organize, categorize and group exclusions based on the type of activity data they are to exclude.

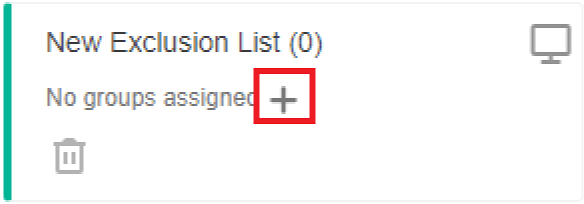
For example, let's say that you want to collect network activity data for your system, but a specific application generates quite a bit of uninteresting logistical network activity that you do not want to collect. In this case, you can define an Exclusion List named after that application that contains one or more exclusions that relate specifically to the network activity generated by that application. Exclusion Lists can be organized anyway you see fit. For example, you can create an Exclusion List for security products, a different one for PDF documents, a different one for HR-related software and so on.

Adding an Exclusion List

To define an Exclusion List:

1. Click the *+ Add List* option and provide a name to create a new Exclusion List.
2. Add (define) the exclusions of this Exclusion List (as described on the following page). Each exclusion that you add belongs to a specific Exclusion List.
3. Assign Collector Groups to this Exclusion List (as described below) in order to determine to which Collector Groups these exclusions apply. A Collector Group can be assigned to multiple Exclusion Lists.

Assigning a Collector Group to an Exclusion List



You can perform the following operations on an Exclusion List:

Operation	Description
Assign a Collector Group:	Click the + button in the Exclusion List to which to assign a Collector Group. Then, select the Collectors groups to which to assign this list and approve it. Note that a Collector Group can be assigned to multiple Exclusion Lists.
Unassign a Collector Group	Click the + button and uncheck the Collector Group to be removed from an Exclusion List.
Delete Exclusions List	Click on the *Delete* 🗑 button. Note that all Exclusions in this list will be removed and will no longer be applied to the assigned Collector groups.

Defining Collection Exclusions

All exclusions must belong to an Exclusion List. Select an Exclusion List on the left to display the exclusions that are defined in it.

Exclusions can be defined for a

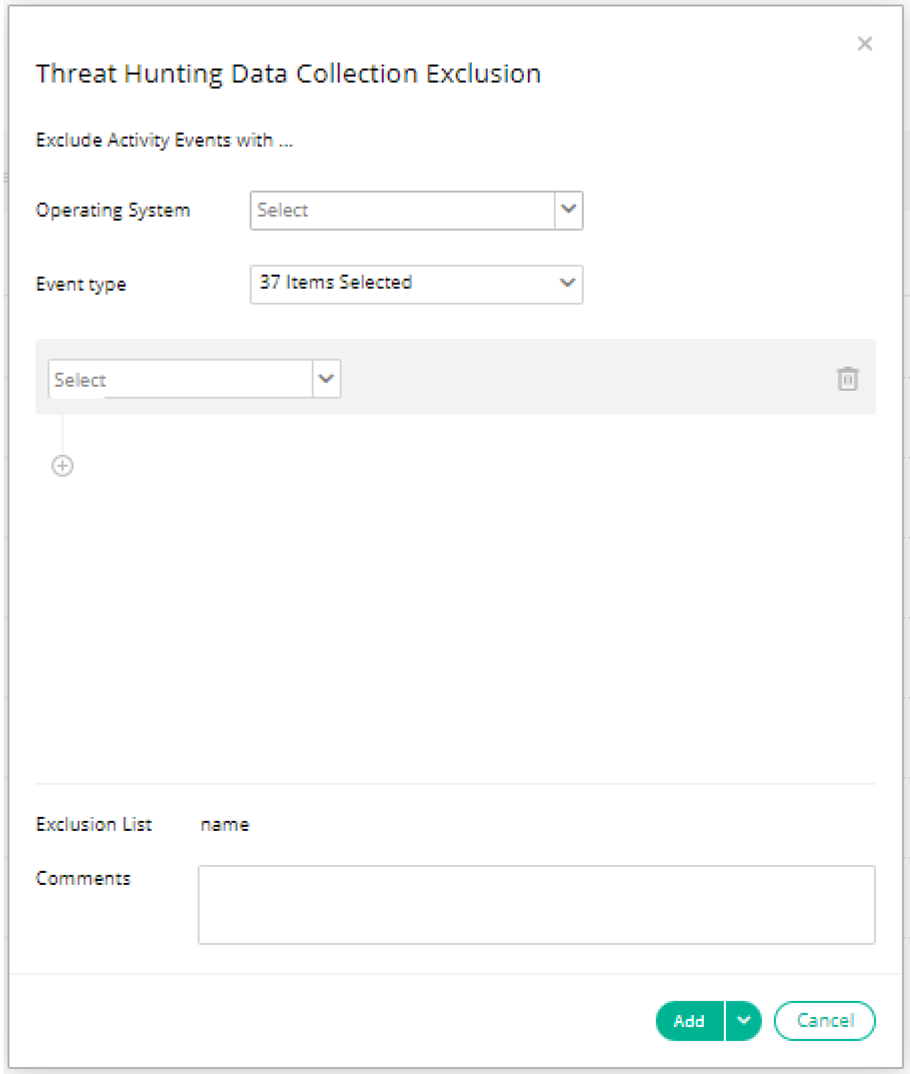
- **Source (process)** – Which is identified by a source attribute, such as a Signer.
- **Type/Action** – Activity event types, as described in Threat Hunting on page 125.
- **Target** – Which is identified by a target attribute, such as IP & Port.

Exclusion can include all of these three or any combination. However, defining an exclusion that only contains a Type is not valid, because this kind of exclusion should be defined in a Threat Hunting Profile.

For example, you can define to exclude activity events of a specific Type that have a specific source and a specific target or to exclude (for example) activity events that have a specific source and any activity or target.

Adding an Exclusion

1. In the left pane, click the Exclusion List to which to add the exclusion.
2. In the right pane, click the *+ Add Exclusion* button. The following displays:



Threat Hunting Data Collection Exclusion

Exclude Activity Events with ...

Operating System: Select

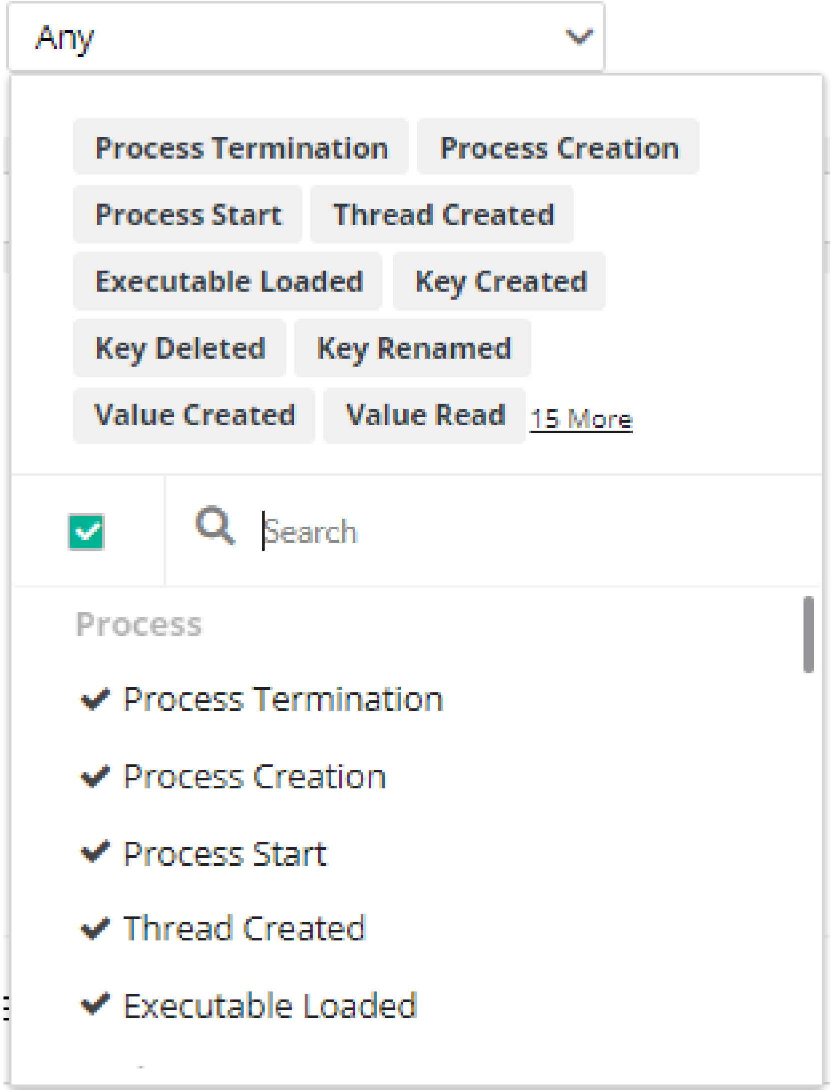
Event type: 37 Items Selected

Select

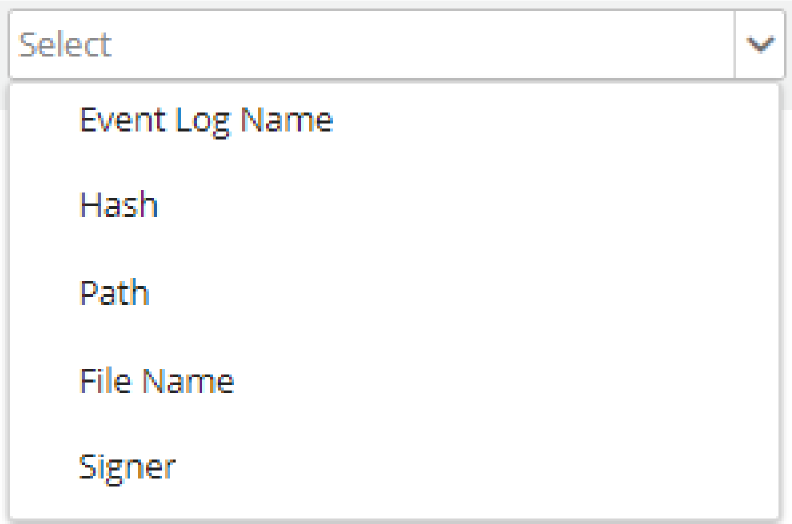
Exclusion List: name

Comments

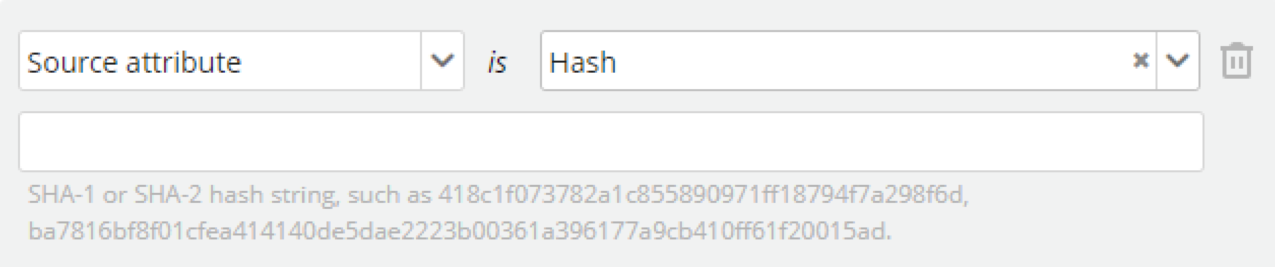
3. From the *Operating system* dropdown menu, select the OS, such as *Windows*.
4. To define that an exclusion includes a specific Activity Event Type, select the type of action(s) to exclude from the displayed dropdown list. Alternatively, select the Any option (the default option), which means that you are not specifying a specific action type.
   All action types to be collected are listed according to Category. You can select one or more actions from a single Category. Actions cannot be selected from different categories. For example, you can select the *Process Termination* and the *Process Start* options from the Process Category in the same exclusion. However, you cannot select the *Key Created* option together and the *Thread Created* options in the same exclusion – to do this you must create two different exclusions.



5. To define that an exclusion includes a *Source* attribute condition, from the *Select* box, select *Source attribute*, which can be identified by file name, path, hash and signer for Source Process or Event Log Name for event log related activity events, as shown below:



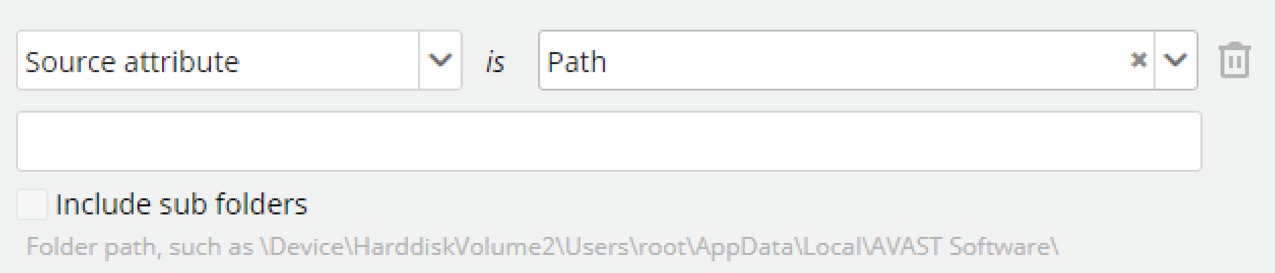
If you select *Hash*, then specify the hash, as shown below:



Source attribute *is* Hash

SHA-1 or SHA-2 hash string, such as 418c1f073782a1c855890971ff18794f7a298f6d, ba7816bf8f01cfea414140de5dae2223b00361a396177a9cb410ff61f20015ad.

If you select *Path*, then specify the *Path*, as shown below. A path can include wild cards. If you wish to include sub-folders as well, check the *Select sub folders* checkbox.



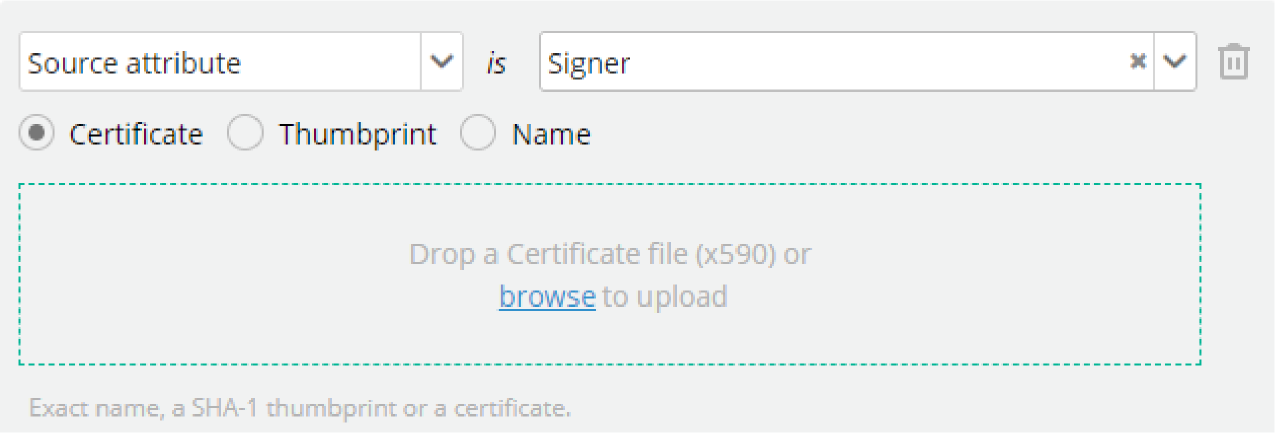
Source attribute *is* Path

□ Include sub folders

Folder path, such as \Device\HarddiskVolume2\Users\root\AppData\Local\AVAST Software\

If you select File Name, then enter the file name.

If you select Signer, then either upload the Signer’s Certificate, provide its thumbprint or provide the Signer’s name.



Source attribute *is* Signer

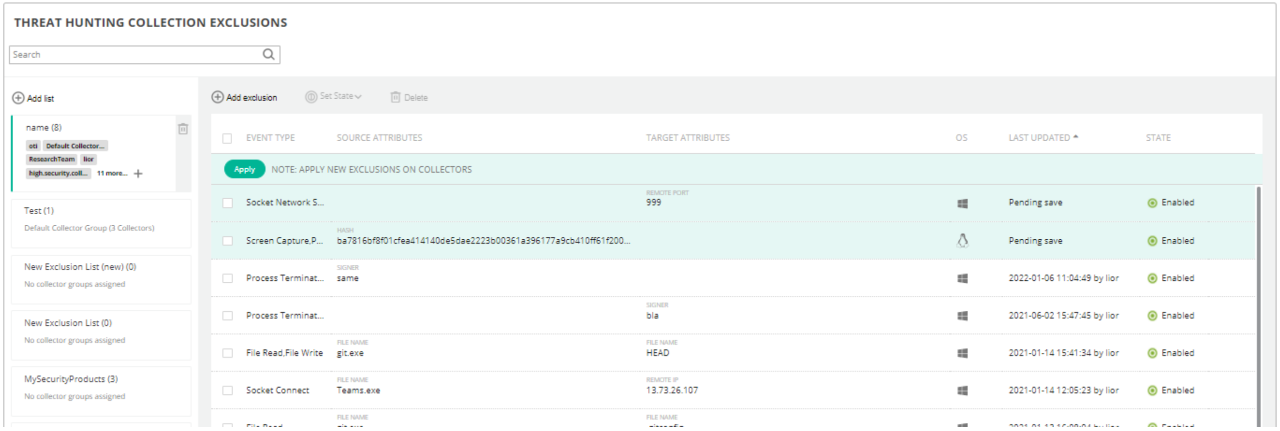
● Certificate ○ Thumbprint ○ Name

Drop a Certificate file (x590) or browse to upload

Exact name, a SHA-1 thumbprint or a certificate.

6. To define that an exclusion includes a *Target* attribute condition, click the + button. From the *Select* box, select the *Target Attribute* and then define the target criteria, as described below:
   Targets can be identified by various criteria, depending on the selected Activity Event Category.
   - A process Category event is identified by hash, path, file name or Signer.
   - A network Category event is identified by network-related properties, such as a remote IP and port.
   - A registry Category event is identified by a registry key path, value name, value type or value size.
   - An Event log Category event is identified by the Event Log ID.
     When defining an exclusion that contains multiple conditions, an AND relationship exists between the conditions.

     Note: If an OR relationship is needed between the conditions that you define, simply create another exclusion.
7. Click the *Add* button. This new exclusion is then listed in the Collection Exclusions page, as shown below:



THREAT HUNTING COLLECTION EXCLUSIONS

Search

Add list

name (8)
oti | Default Collector... | ResearchTeam | lior | high.security.coll... | 11 more...

Test (1)
Default Collector Group (3 Collectors)

New Exclusion List (new) (0)
No collector groups assigned

New Exclusion List (0)
No collector groups assigned

MySecurityProducts (3)
No collector groups assigned

Add exclusion | Set State | Delete

Apply NOTE: APPLY NEW EXCLUSIONS ON COLLECTORS

EVENT TYPE	SOURCE ATTRIBUTES	TARGET ATTRIBUTES	OS	LAST UPDATED	STATE
Socket Network S...		REMOTE PORT 999		Pending save	Enabled
Screen Capture,P...	HASH ba7816bf8f01cfea414140de5dae2223b00361a396177a9cb410ff61f200...			Pending save	Enabled
Process Terminat...	SIGNER same			2022-01-06 11:04:49 by lior	Enabled
Process Terminat...		SIGNER bla		2021-06-02 15:47:45 by lior	Enabled
File Read,File Write	FILE NAME git.exe	FILE NAME HEAD		2021-01-14 15:41:34 by lior	Enabled
Socket Connect	FILE NAME Teams.exe	REMOTE IP 13.73.26.107		2021-01-14 12:05:23 by lior	Enabled

8. The newly defined exclusions appear with a green background and the words **Pending save** appear in their **LAST UPDATED** column. To define that these exclusions take effect, you must click the Apply button and then click the Save button in the window that pops up. Their *LAST UPDATED* column then shows the timestamp when they were saved.

Setting the state of an Exclusion

The *Set State* button enables you to enable or disable the selected exclusion(s). By default, an exclusion is enabled.

Deleting an Exclusion

The *Delete* button enables you to delete the selected exclusion(s).

To delete multiple exclusions, check the requested exclusions checkboxes and click *Delete* in the toolbar.

Threat Hunting data retention

Because the size of the Threat Hunting Repository database is limited, the data that is written to it is overwritten in a cyclical manner when it gets full.

Therefore, the amount of time that the data is retained is dependent upon –

- The size of the repository database.
  – AND –
- The amount of data that is collected.

The amount of data that is collected is dependent upon –

- The Threat Hunting Data Collection Profiles, which is defined in *SECURITY SETTINGS > Threat Hunting > Collection Profiles*
  – AND –
- The Threat Hunting Data Collection Exclusions, which is defined in *SECURITY SETTINGS > Threat Hunting > Collection Exclusions*

In order to extend the data retention period, you can –

- Increase the size of the repository database by purchasing additional Threat Hunting Repository add-ons.
  – AND/OR –
- Reduce the amount of data that is collected, by either defining the Collection Profiles (so that they collect less data) or defining more Collection Exclusions (so that they exclude more data), as described above.

Regarding Threat Hunting Collection Profiles, switching from the Inventory Scan Profile typically reduces data retention by at least 50% and switching to the Comprehensive Profile typically reduces data retention by an additional 50%.

To see an estimate of the Threat Hunting data retention:

- Select *ADMINISTRATION > LICENSING* and look next to the *Threat Hunting* row.
  – OR –
- Select *SECURITY SETTINGS > Collection Profiles*. The data retention period is displayed in the top left corner.

Playbook policies

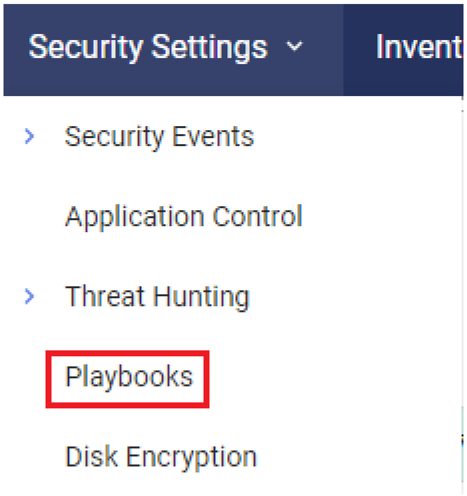
The FortiEDR Playbooks feature determines which automatic actions are triggered, based on the classification of a security event. Playbook policies enable administrators to preconfigure the action(s) to be automatically executed according to a security event's classification. Typically, Playbook policies only need be configured once, and can be modified thereafter, if needed. FortiEDR classifies each security event into one of five categories.

FortiEDR provides the following Playbook policy out of the box:

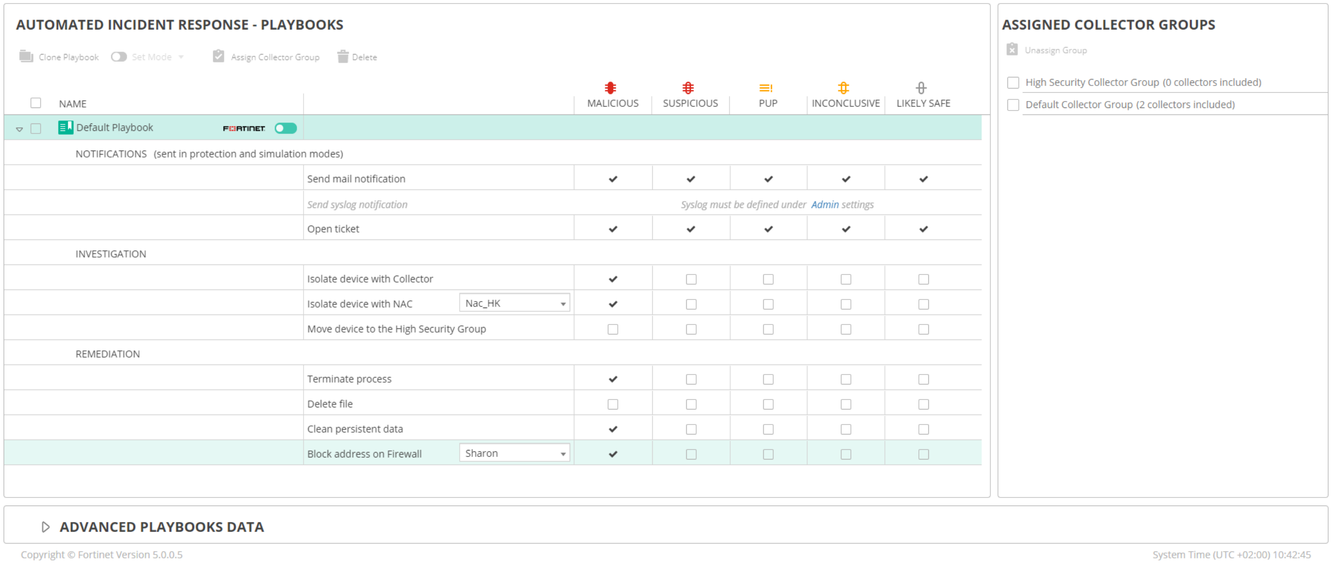
- **Default Playbook**: This Playbook policy specifies the default actions for the Collector Groups assigned to the policy. By default, all Collector Groups are assigned to this policy.

Automated Incident Response - Playbooks Page

The *AUTOMATED INCIDENT RESPONSE – PLAYBOOKS* page displays a row for each Playbook policy. To access this page,select *SECURITY SETTINGS > Playbooks*.



Each Playbook policy row can be expanded to show the actions that it contains, as shown below:



AUTOMATED INCIDENT RESPONSE - PLAYBOOKS

□ NAME		MALICIOUS	SUSPICIOUS	PUP	INCONCLUSIVE	LIKELY SAFE
□ Default Playbook FORTINET						
NOTIFICATIONS (sent in protection and simulation modes)						
	Send mail notification	✓	✓	✓	✓	✓
	Send syslog notification	*Syslog must be defined under Admin settings*				
	Open ticket	✓	✓	✓	✓	✓
INVESTIGATION						
	Isolate device with Collector	✓	□	□	□	□
	Isolate device with NAC Nac_HK	✓	□	□	□	□
	Move device to the High Security Group	□	□	□	□	□
REMEDIATION						
	Terminate process	✓	□	□	□	□
	Delete file	□	□	□	□	□
	Clean persistent data	✓	□	□	□	□
	Block address on Firewall Sharon	✓	□	□	□	□

ASSIGNED COLLECTOR GROUPS

□ High Security Collector Group (0 collectors included)

□ Default Collector Group (2 collectors included)

ADVANCED PLAYBOOKS DATA

Copyright © Fortinet Version 5.0.0.5

System Time (UTC +02:00) 10:42:45

You can drill down in a Playbook policy row to view the actions for that policy by clicking the icon.

- There are more options and actions than those shown above that can be added to a Playbook policy, such as the blocking of a malicious IP address. You may consult Fortinet Support about how to add them.
- Automatic Incident Response Playbook features can also be triggered by extended detection events when follow-up actions are configured for the Collector Group of a device on which the event triggered. This enables the system to follow up upon the detection of such an event and execute a sequence of actions, such as to block an address on a firewall or to isolate the device in which part of the event occurred.

Assigned Collector Groups

The Assigned Collector Groups pane on the right lists the various Collector Groups in the system. By default, all Collector Groups are assigned to the Default Playbook policy. You can reassign one or more Collector Groups to different Playbook policies, if preferred.

Note: When upgrading your FortiEDR system, all existing Collector Groups are automatically assigned to the Default Playbook policy.

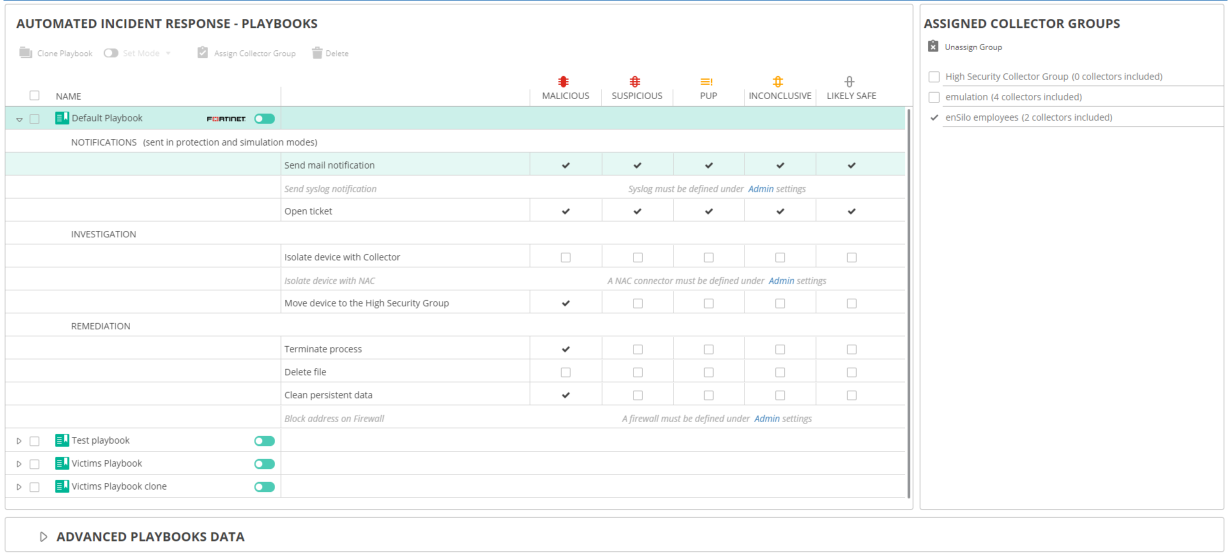
Cloning a Playbook Policy

Cloning a Playbook policy unassigns the policy from one Collector Group and then reassigns it to a different Collector Group. A Collector Group can only be assigned to one Playbook policy.

1. In the *AUTOMATED INCIDENT RESPONSE - PLAYBOOKS* page, select the Playbook policy row that you want to clone in the *Playbook Policies* list.

2. Do one of the following:

   a. Select the checkbox(es) of the Collector Group(s) in the *Assigned Collector Groups* pane that you want to assign to the cloned Playbook policy. Then, click the *Unassign Group* button in the *Assigned Collector Groups* pane.



AUTOMATED INCIDENT RESPONSE - PLAYBOOKS

NAME		MALICIOUS	SUSPICIOUS	PUP	INCONCLUSIVE	LIKELY SAFE
▽ □ Default Playbook FORTINET						
NOTIFICATIONS (sent in protection and simulation modes)						
	Send mail notification	✓	✓	✓	✓	✓
	Send syslog notification	*Syslog must be defined under Admin settings*				
	Open ticket	✓	✓	✓	✓	✓
INVESTIGATION						
	Isolate device with Collector	□	□	□	□	□
	Isolate device with NAC	*A NAC connector must be defined under Admin settings*				
	Move device to the High Security Group	✓	□	□	□	□
REMEDIATION						
	Terminate process	✓	□	□	□	□
	Delete file	□	□	□	□	□
	Clean persistent data	✓	□	□	□	□
	Block address on Firewall	*A firewall must be defined under Admin settings*				
▷ □ Test playbook						
▷ □ Victims Playbook						
▷ □ Victims Playbook clone						

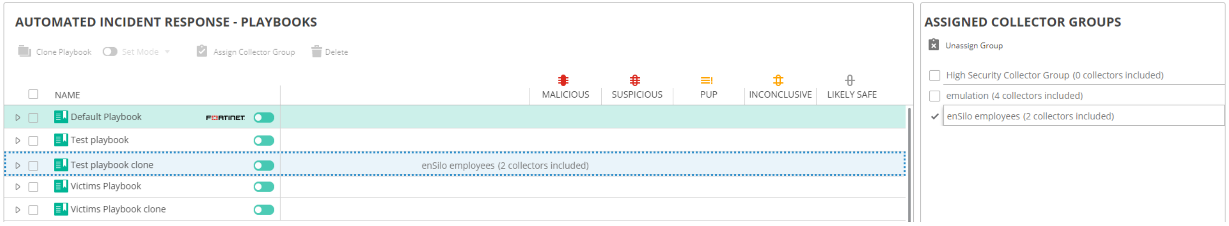
ASSIGNED COLLECTOR GROUPS

Unassign Group

□ High Security Collector Group (0 collectors included)
□ emulation (4 collectors included)
✓ enSilo employees (2 collectors included)

▷ ADVANCED PLAYBOOKS DATA

   b. Click *Collector Group* in the *Assigned Collector Groups* pane that you want to assign to the cloned Playbook policy. Then, drag the Collector Group onto the cloned Playbook policy in the *Playbook Policies* list, as shown below:



AUTOMATED INCIDENT RESPONSE - PLAYBOOKS

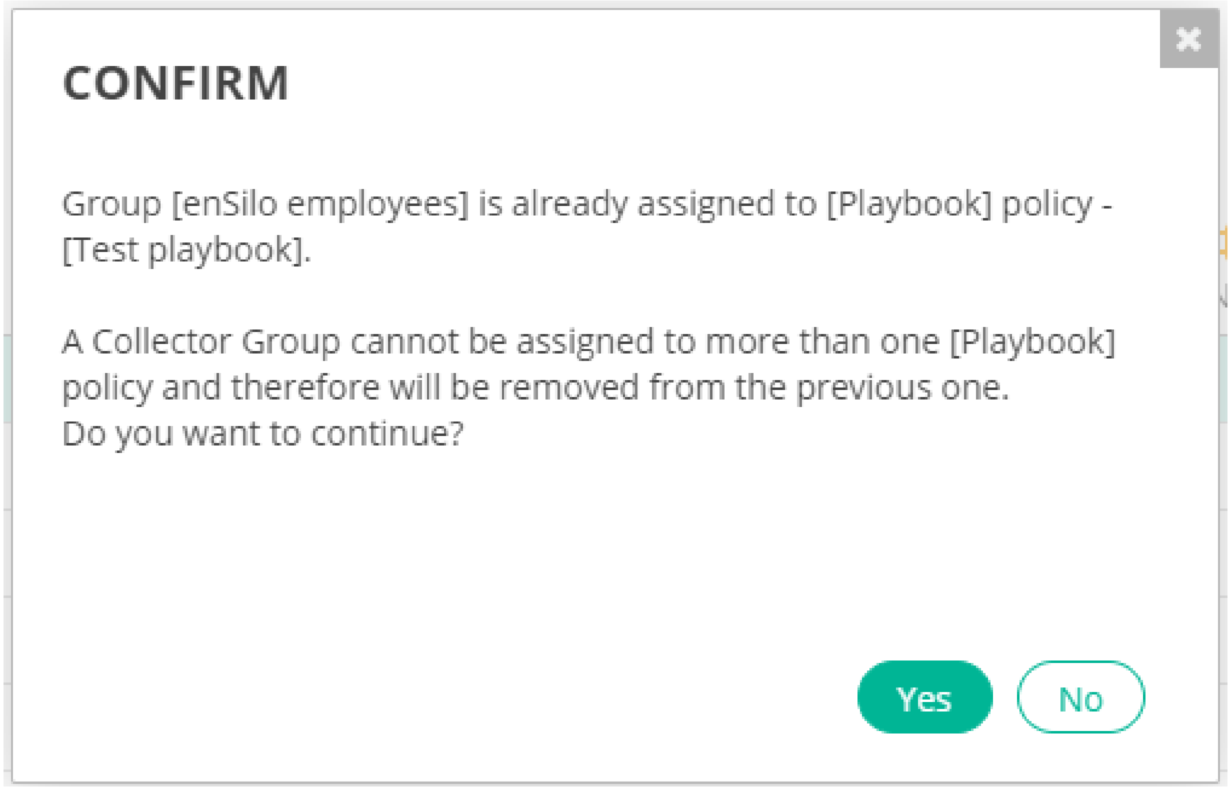
NAME		MALICIOUS	SUSPICIOUS	PUP	INCONCLUSIVE	LIKELY SAFE
▷ □ Default Playbook FORTINET						
▷ □ Test playbook						
▷ □ Test playbook clone	enSilo employees (2 collectors included)					
▷ □ Victims Playbook						
▷ □ Victims Playbook clone						

ASSIGNED COLLECTOR GROUPS

Unassign Group

□ High Security Collector Group (0 collectors included)
□ emulation (4 collectors included)
✓ enSilo employees (2 collectors included)

   The following message displays.



CONFIRM

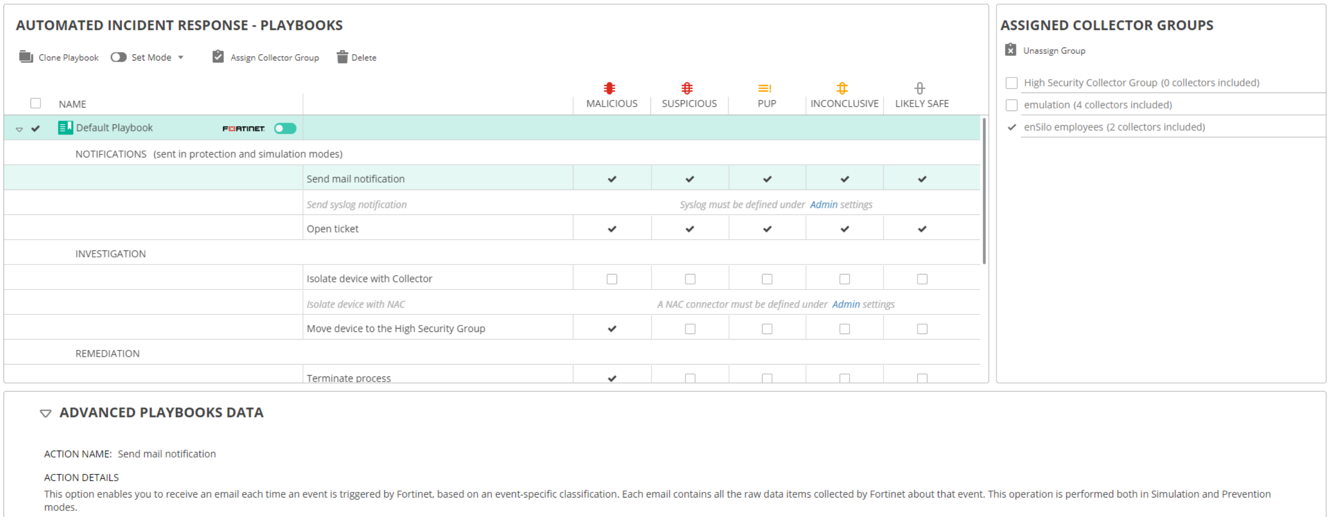
Group [enSilo employees] is already assigned to [Playbook] policy - [Test playbook].

A Collector Group cannot be assigned to more than one [Playbook] policy and therefore will be removed from the previous one.
Do you want to continue?

Click *Yes*.

Advanced Playbooks Data

The *ADVANCED PLAYBOOKS DATA* area at the bottom of the *AUTOMATED INCIDENT RESPONSE – PLAYBOOKS* page displays more details about the action selected in the *Playbook Policy* list.



AUTOMATED INCIDENT RESPONSE - PLAYBOOKS

□ NAME		MALICIOUS	SUSPICIOUS	PUP	INCONCLUSIVE	LIKELY SAFE
✓ Default Playbook FORTINET						
NOTIFICATIONS (sent in protection and simulation modes)						
	Send mail notification	✓	✓	✓	✓	✓
	Send syslog notification	*Syslog must be defined under Admin settings*				
	Open ticket	✓	✓	✓	✓	✓
INVESTIGATION						
	Isolate device with Collector	□	□	□	□	□
	Isolate device with NAC	*A NAC connector must be defined under Admin settings*				
	Move device to the High Security Group	✓	□	□	□	□
REMEDIATION						
	Terminate process	✓	□	□	□	□

ASSIGNED COLLECTOR GROUPS

- □ High Security Collector Group (0 collectors included)
- □ emulation (4 collectors included)
- ✓ enSilo employees (2 collectors included)

ADVANCED PLAYBOOKS DATA

ACTION NAME: Send mail notification

ACTION DETAILS

This option enables you to receive an email each time an event is triggered by Fortinet, based on an event-specific classification. Each email contains all the raw data items collected by Fortinet about that event. This operation is performed both in Simulation and Prevention modes.

Playbook policy actions

Playbook policy actions are divided into the following types:

- Notifications on page 248
- Investigation on page 249
- Remediation on page 251
- Custom on page 252

Each of these categories contains different types of actions that can be performed when a security event is triggered.

Notifications

Notification actions send a notification when a relevant security event is triggered. These actions are implemented in both FortiEDR modes (Simulation and Prevention).

Notifications can be one of the following types:

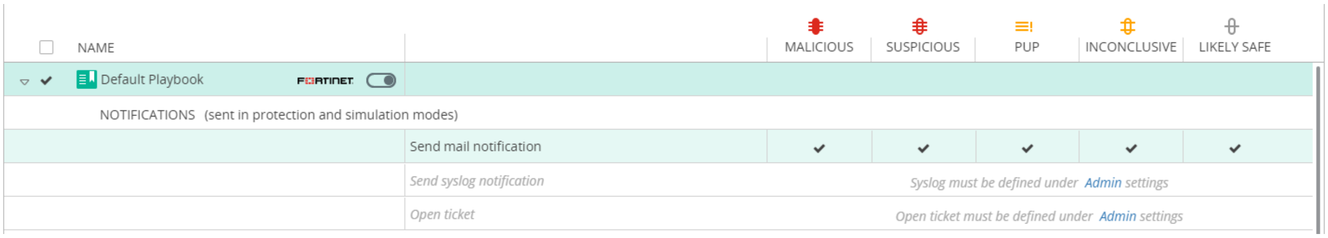
- Emails
- Syslog
- Open Ticket

Notification actions must be enabled in order to be implemented by a Playbook policy. If notifications are disabled, they are not implemented by the Playbook policy, even if that policy is configured to send notifications. For more details see SMTP on page 308.

Each row under *Notifications* corresponds to a single type of notification (mail [email] notification, Syslog notification or Open Ticket notification). In the *Notifications* area, you configure each notification type to indicate whether or not it is to automatically send the relevant notification, once triggered by a security event.

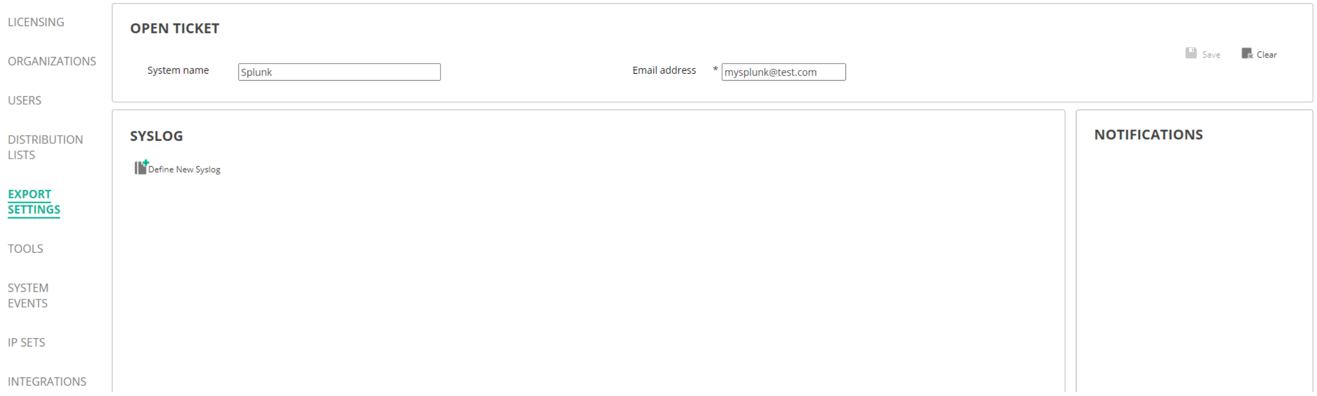
The *Malicious*, *Suspicious*, *PUP*, *Inconclusive*, and *Likely Safe* columns correspond to the possible classifications (see Overview on page 90 and Incidents pane on page 86) for a security event. When a checkmark ✓ appears in one of these columns, it means that a notification of the specified type is sent when an event is triggered with that classification.

By default, the *Default Playbook* policy is set to Simulation mode, and only email notifications are automatically enabled, as shown below:



□ NAME		MALICIOUS	SUSPICIOUS	PUP	INCONCLUSIVE	LIKELY SAFE
✓ Default Playbook FORTINET						
NOTIFICATIONS (sent in protection and simulation modes)						
	Send mail notification	✓	✓	✓	✓	✓
	Send syslog notification	*Syslog must be defined under Admin settings*				
	Open ticket	*Open ticket must be defined under Admin settings*				

SMTP, Syslog and Open Ticket must already be configured in order to send their respective notifications. If their settings are not already configured, the relevant row in the Notifications list displays a message indicating that you must first configure it, The word *Admin* in each of these messages points to the following configuration page when clicked:



OPEN TICKET

System name: Splunk

Email address *: mysplunk@test.com

SYSLOG

NOTIFICATIONS

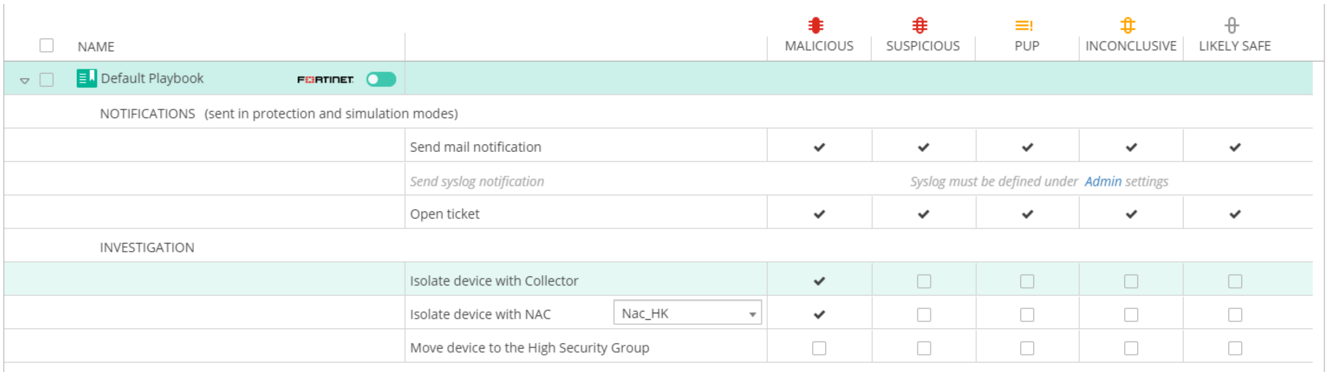
Notifications are sent based on the Core or FortiEDR Cloud Service (FCS) classification of the event, depending on whether the FCS classification happens within the timeout period and whether the FCS classification result differs from the one from the Core:

The default timeout period for FCS classification is 3 minutes. To change the default FCS timeout value for your dedicated environment, contact Fortinet Support.

- If the FCS classification is received within the timeout period, the notification is sent based on the FCS classification.
- If the FCS classification result is not received within the timeout period, a notification is sent by the end of the timeout based on the initial Core classification.
- If the FCS classification comes in after the timeout with a different result from the Core classification, an updated notification is sent based on the final classification by the FCS.

Investigation

Investigation actions enable you to isolate a device or assign it to a high-security Collector Group, in order to further investigate the relevant device's activity.



□ NAME		MALICIOUS	SUSPICIOUS	PUP	INCONCLUSIVE	LIKELY SAFE
□ Default Playbook FORTINET						
NOTIFICATIONS (sent in protection and simulation modes)						
	Send mail notification	✓	✓	✓	✓	✓
	Send syslog notification		*Syslog must be defined under Admin settings*			
	Open ticket	✓	✓	✓	✓	✓
INVESTIGATION						
	Isolate device with Collector	✓	□	□	□	□
	Isolate device with NAC Nac_HK	✓	□	□	□	□
	Move device to the High Security Group	□	□	□	□	□

Investigation actions can be one of the following types:

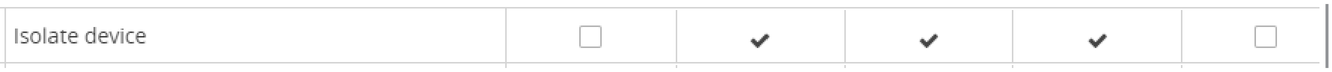
- Isolate device with Collector on page 250
- Isolate device with NAC on page 250
- Move device to High Security Group on page 250

All investigation actions are performed based on FortiEDR Cloud Service (FCS) classification. If FCS is not running, FortiEDR performs investigation actions based on Core classification instead.

Isolate device with Collector

This action blocks the communication to/from the affected Collector. This action only applies for endpoint Collectors. For example, if the Playbook policy is configured to isolate the device for a malicious event, then whenever a maliciously classified security event is triggered from a device, then that device is isolated (blocked) from communicating with the outside world (for both sending and receiving). This means, for example, that applications that communicate with the outside world, such as Google Chrome, Firefox and so on, will be blocked for outgoing communications.

A checkmark ✓ in a classification column here means that the device is automatically isolated when a security event is triggered with that classification.



Isolate device	□	✓	✓	✓	□

Isolate device with NAC

This action blocks the communication to/from the affected device by disabling this host on an external Network Access Control system. A NAC connector must already be configured in order to perform this action. For details about how to configure NAC connectors, see Network Access Control (NAC) integration on page 350.

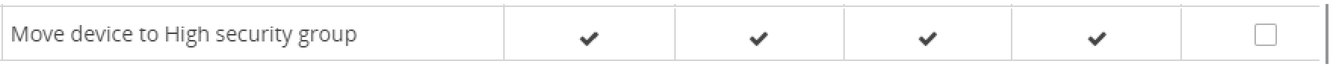
In the dropdown menu next to the action, you can specify which NAC to use for disabling the host or select all of them.

Unlike devices that are isolated using the FortiEDR Collector for which there is an isolation indication on *Inventory* tab and un-isolation is available, devices that were isolated using an external system such as a NAC are not indicated as such on the FortiEDR Console and un-isolation is only possible on the external NAC system.

Move device to High Security Group

FortiEDR provides two default Collector Groups: the Default Collector Group and the High Security Collector Group. Both of these default Collector Groups are initially assigned to the Default Playbook policy, and cannot be deleted.

A checkmark ✓ in a classification column here means that the device is automatically moved (assigned) to the High Security Collector Group when a security event is triggered that has that classification. This feature is useful when you want to mark Collectors that triggered malicious events.

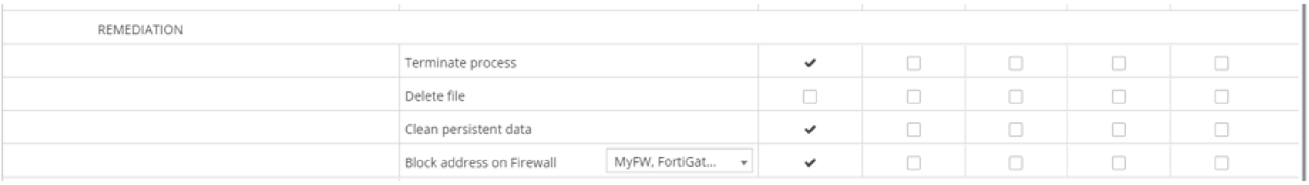


Move device to High security group	✓	✓	✓	✓	□

Remediation

Remediation actions enable you to remediate a situation in the FortiEDR system, should malware be detected on a device.

All FortiEDR remediation actions are based on the final classification of a security event by the FortiEDR Cloud Service (FCS), which is a cloud-based, software only service that determines the exact classification of security events with a high degree of accuracy.



REMEDIATION						
	Terminate process	✓	□	□	□	□
	Delete file	□	□	□	□	□
	Clean persistent data	✓	□	□	□	□
	Block address on Firewall MyFW, FortiGat... ▾	✓	□	□	□	□

Remediation actions can be one of the following types:

- Terminate process on page 251
- Delete file on page 251
- Clean persistent data on page 251
- Block address on Firewall on page 252

Terminate process

This action terminates the affected process. It does not guarantee that the affected process will not attempt to execute again. This action can also be performed manually using the Forensics add-on, as described on Remediating a device upon malware detection on page 160

A checkmark ✓ in a classification column here means that the affected process is automatically terminated on the device when a security event is triggered that has that classification.

Delete file

This action ensures that the file does not attempt to exfiltrate data again, as the file is permanently removed from the device. This action can also be performed manually using the Forensics add-on, as described on Remediating a device upon malware detection on page 160

A checkmark ✓ in a classification column here means that the affected file is automatically removed on the device when a security event is triggered that has that classification.

Clean persistent data

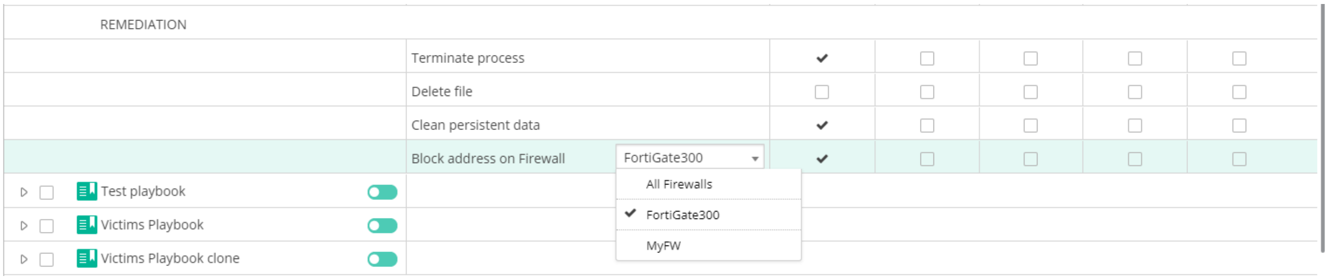
This action cleans the registry keys in Windows. This action can also be performed manually using the Forensics add-on, as described on Remediating a device upon malware detection on page 160.

A checkmark ✓ in a classification column here means that the affected registry key is automatically cleaned on the device when a security event is triggered that has that classification.

Block address on Firewall

This action ensures that connections to remote malicious addresses that are associated with the security event are blocked. A Firewall Connector must already be configured in order to perform this action. For details about how to configure firewall connectors, see Firewall Integration on Firewall integration on page 341.

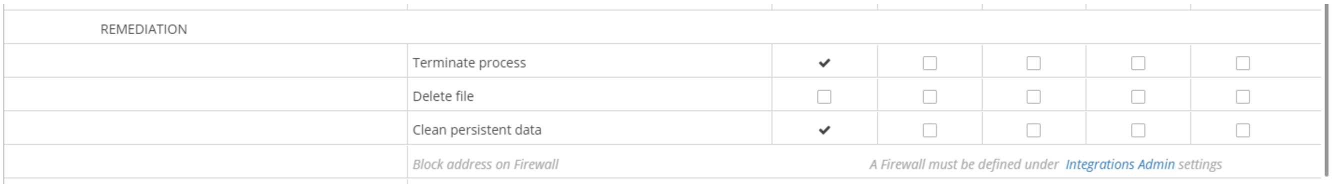
In the dropdown menu next to the action, you can specify which firewalls are used to perform the blocking or select all of them, as shown below:



REMEDIATION							
	Terminate process		✓	□	□	□	□
	Delete file		□	□	□	□	□
	Clean persistent data		✓	□	□	□	□
	Block address on Firewall	FortiGate300 ▾	✓	□	□	□	□
▷ □ Test playbook							
▷ □ Victims Playbook							
▷ □ Victims Playbook clone							

A checkmark ✓ in a Classification column means that communication with the affected destination is automatically blocked when a security event is triggered that has that classification.

The firewall must already be configured in order to add malicious destinations to blocked addresses. If its settings are not already configured, the relevant row in the Remediation list displays a message indicating that you must first configure it, as shown below:

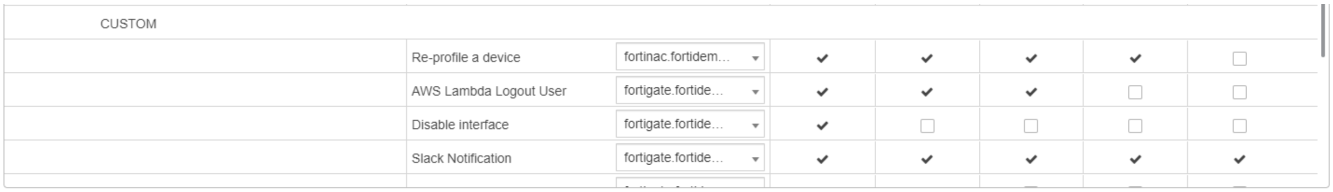


REMEDIATION						
	Terminate process	✓	□	□	□	□
	Delete file	□	□	□	□	□
	Clean persistent data	✓	□	□	□	□
	Block address on Firewall	*A Firewall must be defined under Integrations Admin settings*				

Clicking the Integration Admin link in this message jumps to the relevant place in the user interface to configure it (in the *Integration* page under the *Administration* tab).

Custom

Custom actions enable you to automatically trigger an incident response in a third-party system as the result of a security event detected by FortiEDR, according to the Custom Integration connector (and its actions) that you define.



CUSTOM							
	Re-profile a device	fortinac.fortidem... ▾	✓	✓	✓	✓	□
	AWS Lambda Logout User	fortigate.fortide... ▾	✓	✓	✓	□	□
	Disable interface	fortigate.fortide... ▾	✓	□	□	□	□
	Slack Notification	fortigate.fortide... ▾	✓	✓	✓	✓	✓

The *CUSTOM* section of the *Playbook* page lists the actions that have been defined for Custom Integration Connectors, as described on Custom integration on page 370.

This list appears empty if no custom integration connector has been defined.

A checkmark ✓ in a classification column here means that the defined action is triggered in the third-party system when a security event is triggered that has that classification.

Other options in the Playbooks tab

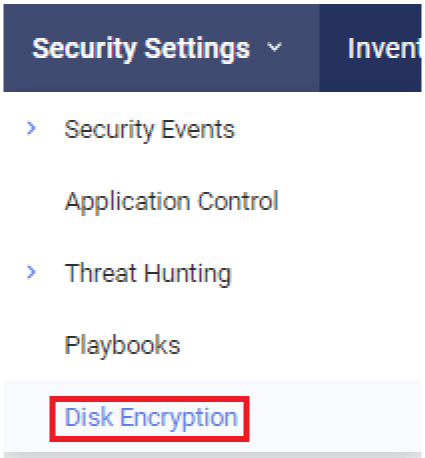
You can perform the following operations using the toolbar at the top of the tab:

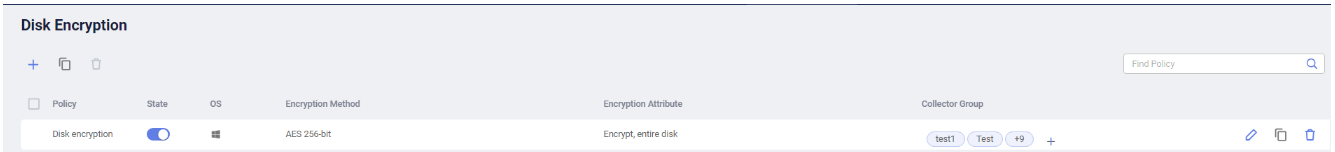
- *Clone Playbook*: Clones a Playbook policy, as described on Playbook policies on page 244.
- *Set Mode*: Changes the mode of the Playbook policy. This process is similar to that for setting the mode for a standard security policy, which is described on Setting a security policy's Prevention or Simulation mode on page 201
- *Assign Collector Group*: Assigns a Playbook policy to a Collector Group. This process is similar to that for assigning a standard security policy to a Collector Group, which is described on Assigning a security policy to a Collector Group on page 205.
- *Delete*: Deletes a cloned Playbook policy. Default Playbook policies cannot be deleted.

The default Playbook policy (named Default Playbook) is mandatory and cannot be deleted.

Disk Encryption COLLECTOR 6.1 OR LATER

Use the *Security Settings > Disk Encryption* page to configure disk encryption policies to enforce disk encryption on Windows 7 or later (using BitLocker, TPM required) and macOS (using FileVault) endpoints to ensure consistent security configurations and compliance with regulatory requirements. You can also configure disk decryption policies to allow users to decrypt an encrypted disk.





Disk Encryption

Find Policy

Policy	State	OS	Encryption Method	Encryption Attribute	Collector Group
Disk encryption	●	⊞	AES 256-bit	Encrypt, entire disk	test1 Test +9 +

To configure a disk encryption policy to enforce disk encryption on specific Collector groups:

1. In the *Security Settings > Disk Encryption* page, click the *Add* button at the top left corner.
2. Specify a name for the policy.
3. Enable the policy if you want to enforce the policy immediately after creation. You can also choose to enable it later.
4. Select the OS and configure the relevant options:

Windows	macOS
1. Under *Action*, select *Encrypt all disks* or *Encrypt only used disk*. 2. Under *Method*, select an encryption method for Windows 10 or later.	1. Under *Action*, select *Encrypt*. 2. Under *Method*, select the number of allowed user logins with an unencrypted disk. For example, if *3* is selected, the user will not be able to log in on the third attempt without confirming the disk encryption. 3. Upload the FileVaultMaster certificate.

5. Click *Save*.

   The policy appears in the disk encryption policies table.
6. Enable or disable the policy by toggling the button in the *State* column.
7. Add or remove Collector groups for the policy in the *Collector Group* column.
8. **(macOS)** To verify the disk encryption status, run `sudo fdesetup status` on the endpoint. You can run the command multiple times to see the progress. When the encryption is complete, the status will show that FileVault is on. Encryption speed depends on HD size and Mac model.

To configure a disk decryption policy to allow users of specific Collector groups to decrypt an encrypted disk:

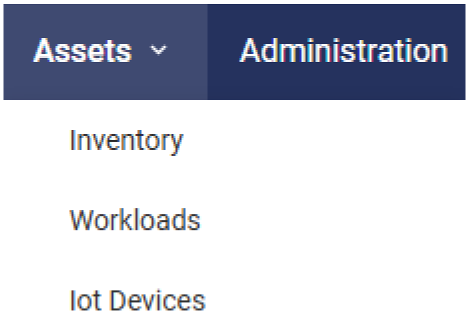
1. In the *Security Settings > Disk Encryption* page, click the *Add* button at the top left corner.
2. Specify a name for the policy.
3. Enable the policy if you want to enforce the policy immediately after creation. You can also choose to enable it later.
4. Select the OS and select *Decrypt* under *Action*.
5. Click *Save*.

   The policy appears in the disk encryption policies table.
6. Enable or disable the policy by toggling the button in the *State* column.
7. Add or remove Collector groups for the policy in the *Collector Group* column.

   (macOS) Users from those Collector groups can then manually disable FileVault (user credentials required) from *Setting > FileVault > Disable FileVault*. If the Collector is not assigned to the decrypt policy, the disk will be automatically encrypted again even after the user manually disables FileVault.
8. **(macOS)** To verify the disk decryption status, run `sudo fdesetup status` on the endpoint. You can run the command multiple times to see the progress. When the decryption is complete, the status will show that FileVault is off. Decryption speed depends on HD size and Mac model.

Assets

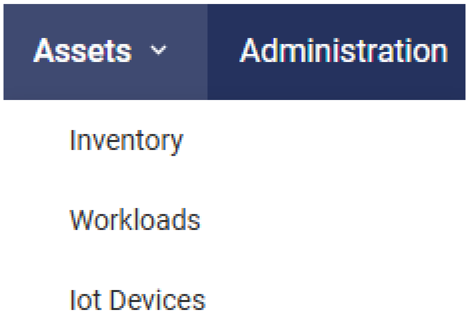
The *Assets* tab displays separate pages for *Inventory on page 256* and *IoT devices on page 269*.

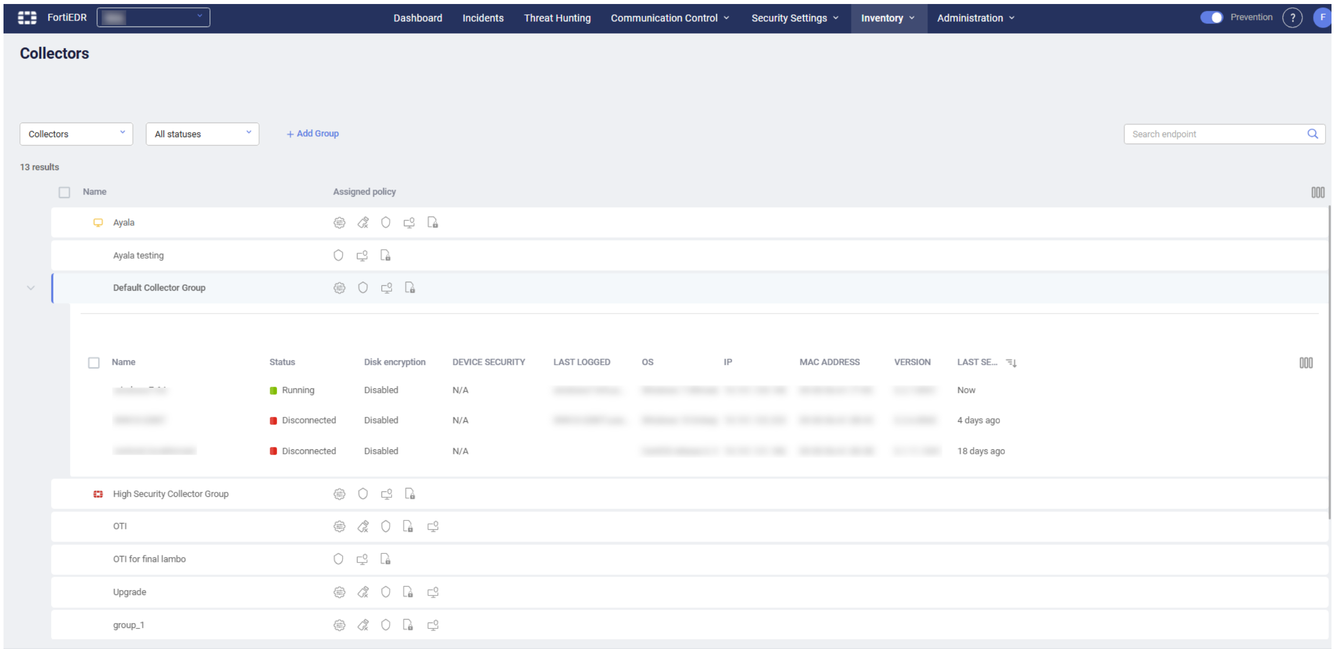


Inventory

The *Inventory* page displays a list of the previously defined Collector Groups, which can be expanded to show the FortiEDR Collectors that each contains. Additional Collector Groups can be defined by you, as described on Defining a new Collector Group on page 262. FortiEDR Collectors automatically register with the system after installation. By default, each FortiEDR Collector is added to the Collector Group called *All*. You can move any Collector to another Collector Group, as described on Assigning Collectors to a Collector Group on page 263.

To access this page, click the down arrow next to *Assets* and then select *Inventory*, as shown below.





Collectors

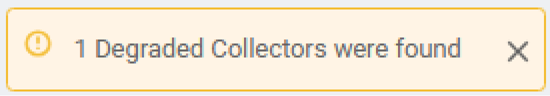
Collectors | All statuses

13 results

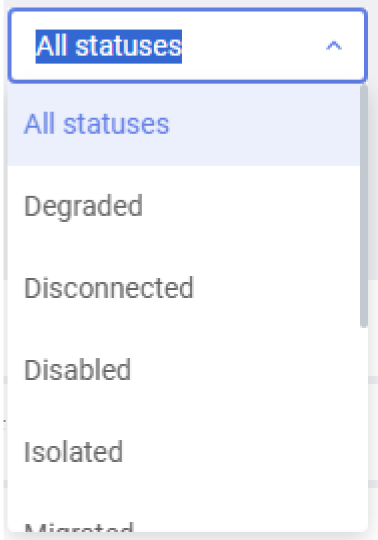
Name	Assigned policy
Ayala	
Ayala testing	
Default Collector Group	
High Security Collector Group	
OTI	
OTI for final lambo	
Upgrade	
group_1	

Name	Status	Disk encryption	DEVICE SECURITY	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	LAST SE...
[redacted]	🟩 Running	Disabled	N/A	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Now
[redacted]	🟥 Disconnected	Disabled	N/A	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	4 days ago
[redacted]	🟥 Disconnected	Disabled	N/A		[redacted]	[redacted]	[redacted]	[redacted]	18 days ago

If there are Collectors in the Degraded state, the following indication appears at the right top corner, which you can click to filter the view to only show the Collectors in the Degraded state.

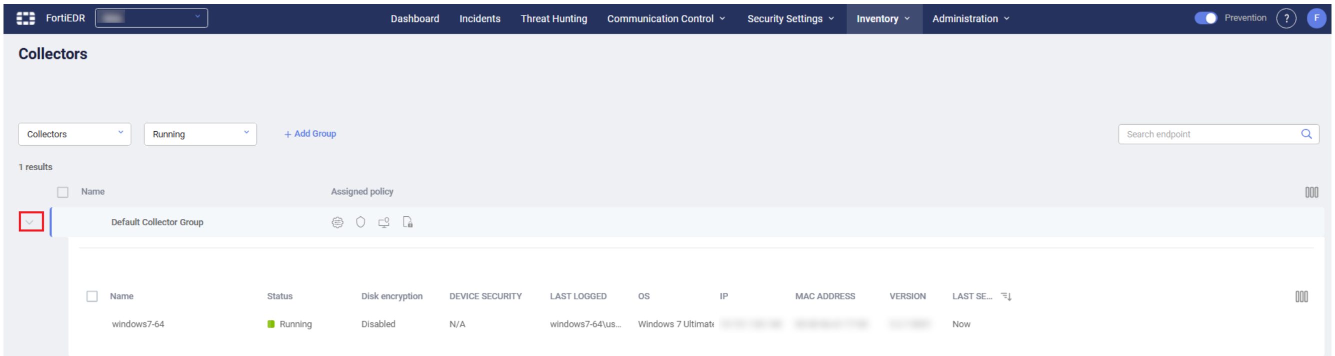

1 Degraded Collectors were found

You can select to display all Collectors that are in one of the specific states (*New*, *Running*, *Disabled*, *Degraded*, *Disconnected*, *Isolated*, *Selected*, *Pending Reboot*, *Migrated*, *Pending Migration*, or *Unmanaged*) using the dropdown menu at the top left of the window, as shown below:



The default Collector Group is a group to which new Collectors are automatically added.

Click the *Expand* icon to expand the list and display the FortiEDR Collectors that the Collector Group contains.



Name	Status	Disk encryption	DEVICE SECURITY	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	LAST SE...
windows7-64	🟩 Running	Disabled	N/A	windows7-64\us...	Windows 7 Ultimate	[redacted]	[redacted]	[redacted]	Now

The following information is provided for each Collector. Some columns are hidden by default. You can toggle them on using the *Choose Columns* button (▯▯▯ Choose Columns) at the top right corner of the page.

Information Field	Description
Checkbox	Check this checkbox to select the Collector. You can then use one of the buttons at the top left of the window, such as the *Delete* button.
Collector Group Name	Name of the Collector Group to which the Collector is assigned.
Device Name	Device name taken from the communicating device on which a FortiEDR Collector is installed.
OS	Operating system of the communicating device on which the FortiEDR Collector is installed.
IP	IP address of the communicating device on which the FortiEDR Collector is installed.
Version	Version of the FortiEDR Collectors installed on the communicating device.
State	Current state of the FortiEDR Collector. Hovering over the STATE value pops up the last time the STATE was changed. Possible value for STATE are as follows:

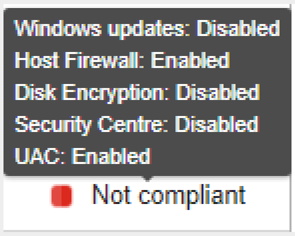
State	Description
Running	The FortiEDR Collector is up and all is well.
Disconnected	The device is offline, powered down or is not connected to the FortiEDR Aggregator.

<table>
<tr><th>Information Field</th><th>Description</th></tr>
<tr><td></td><td><table>
<tr><th>State</th><th>Description</th></tr>
<tr><td>Pending Reboot</td><td>After the FortiEDR Collector is installed, you may want some devices to be rebooted before the FortiEDR Collector can start running. This status means that the FortiEDR Collector is ready to run after this device is rebooted. The reboot is performed in the usual manner on the device itself.</td></tr>
<tr><td>Disabled</td><td>The FortiEDR Collector was disabled in the FortiEDR Central Manager. This feature is not yet available in version 1.2.</td></tr>
<tr><td>Degraded</td><td>The FortiEDR Collector is prevented from performing to its full capacity (for example, due to lack of resources on the device on which it is installed or compatibility issues).</td></tr>
</table></td></tr>
<tr><td>Last Seen</td><td>Counts the number of days passed from the last time this Collector communicated with the Core.</td></tr>
<tr><td>Last Logged</td><td>Specifies the last user that logged into the device on which the Collector is installed. It shows the domain of the computer/username. If this device has not been logged into, then this column is blank. In addition, if the Collector is not V3.0.0.0 or above, then this column is empty and the events from this Collector will not contain the user from which the security event was triggered.</td></tr>
<tr><td>MAC Address</td><td>Physical address of the device. If a device has multiple MAC addresses, three dots (...) display. You can hover over the MAC Address to display the value (or values, in case of multiple MAC addresses) in a tooltip.</td></tr>
<tr><td>Device Security</td><td>Security posture indicator of Windows and macOS endpoints based on OS-level configurations. The device is marked as compliant if two or more of the following criteria are met.
The device security compliance status is informational and has no impact on FortiEDR protection effectiveness. Endpoints are always protected by FortiEDR, regardless of the compliance status.<table>
<tr><th>Windows</th><th>macOS</th></tr>
<tr><td>• <b>Host Firewall</b>—Host firewall is enabled to control incoming and outgoing network traffic to protect the endpoint against</td><td>• <b>Host Firewall</b>—Host firewall is enabled to control incoming and outgoing network traffic</td></tr>
</table></td></tr>
</table>

Information Field	Description

Windows	macOS
unwanted connections. - **Security Centre**—FortiEDR is registered as anti-virus and threat protection agents in *Administration > Settings > Windows Security Center on page 333*. - **Disk Encryption**—Disk encryption is enforced on the endpoint using BitLocker (TPM required). - **User Account Control (UAC)**—Windows User Account Control is enabled to protect the operating system from unauthorized changes. - **Windows updates**—The latest Windows update has been installed.	to protect the endpoint against unwanted connections. - **Disk Encryption**—Disk encryption is enforced on the Mac using FileVault. - **Gatekeeper Status**—Gatekeeper is enabled to ensure that only trusted software runs on the Mac. - **System Integrity Protection (SIP) Status**—System Integrity Protection is enabled to help protect the Mac from malicious software.

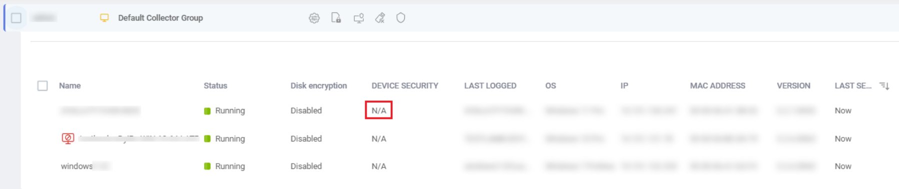
To view compliance details of each criteria, hover over the status text.



Windows updates: Disabled
Host Firewall: Enabled
Disk Encryption: Disabled
Security Centre: Disabled
UAC: Enabled

🟥 Not compliant

Endpoints that are not in connected state show *N/A*.



□ [redacted] Default Collector Group

□	Name	Status	Disk encryption	DEVICE SECURITY	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	LAST SE...
	[redacted]	🟩 Running	Disabled	N/A	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Now
	[redacted]	🟩 Running	Disabled	N/A	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Now
	windows[redacted]	🟩 Running	Disabled	N/A	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Now

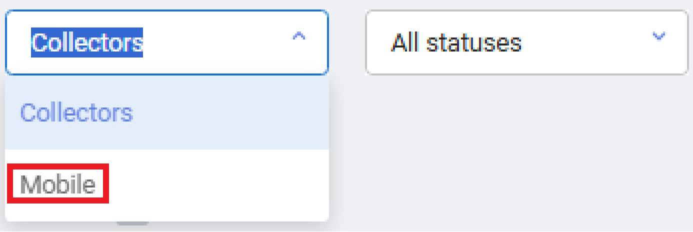
Uninstalling a Collector

Use the *Uninstall* button to uninstall a Collector from a device. Use caution when using this option, as a Collector cannot be reinstalled after removal using the FortiEDR user interface. Therefore, it is recommended to disable a Collector using the *Enable/Disable* option rather than uninstalling it.

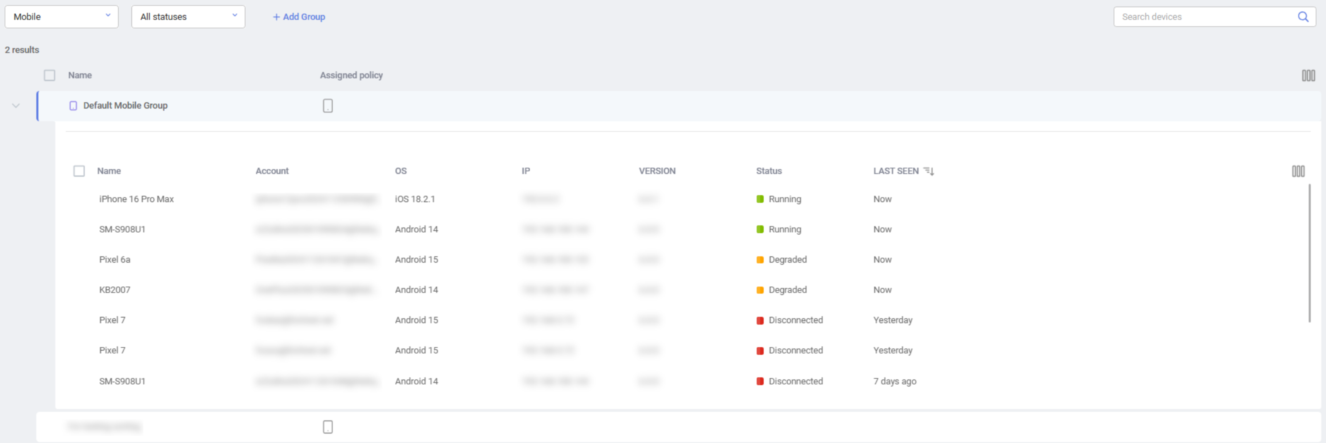
Mobile

To access the mobile Collectors page, use the following filter at the top left of the *Assets* > *Inventory* page.

The *Mobile* option is available only if mobile is enabled in the organization setting. See Step 2 – Defining or importing an organization on page 419.



The *Mobile* page displays a list of the previously defined mobile Collector Groups, which can be expanded to show the FortiEDR mobile Collectors that each contains.



2 results

Name	Assigned policy
Default Mobile Group	
[redacted]	

Name	Account	OS	IP	VERSION	Status	LAST SEEN
iPhone 16 Pro Max	[redacted]	iOS 18.2.1	[redacted]	[redacted]	🟩 Running	Now
SM-S908U1	[redacted]	Android 14	[redacted]	[redacted]	🟩 Running	Now
Pixel 6a	[redacted]	Android 15	[redacted]	[redacted]	🟧 Degraded	Now
KB2007	[redacted]	Android 14	[redacted]	[redacted]	🟧 Degraded	Now
Pixel 7	[redacted]	Android 15	[redacted]	[redacted]	🟥 Disconnected	Yesterday
Pixel 7	[redacted]	Android 15	[redacted]	[redacted]	🟥 Disconnected	Yesterday
SM-S908U1	[redacted]	Android 14	[redacted]	[redacted]	🟥 Disconnected	7 days ago

Additional mobile Collector Groups can be defined by you, as described in Defining a new Collector Group on page 262. FortiEDR mobile Collectors automatically register with the system after installation. By default, each FortiEDR mobile Collector is added to the *Default Mobile Group*. You can move any mobile Collector to another Collector Group, as described in Assigning Collectors to a Collector Group on page 263.

The following information is provided for each Collector:

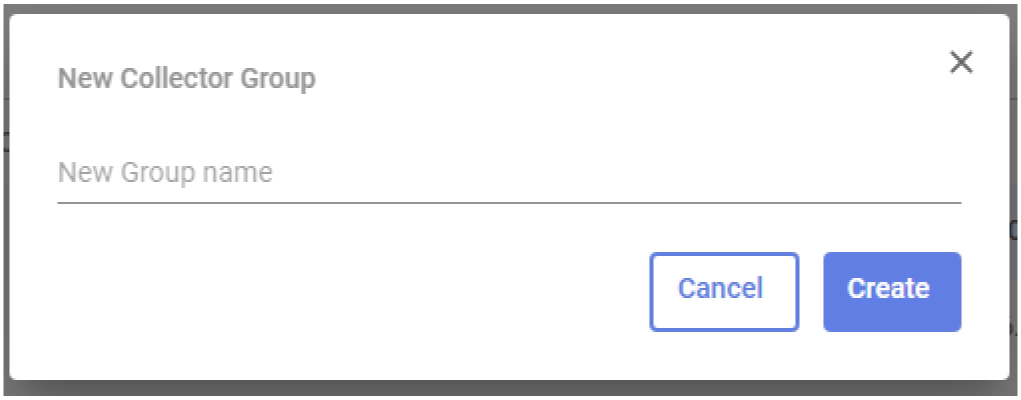
Information Field	Description
Checkbox	Check this checkbox to select the mobile Collector. You can then use one of the buttons at the top left of the window, such as the *Delete* button.
Collector Group Name	Name of the mobile Collector Group to which the mobile Collector is assigned.
Device Name	Device name taken from the communicating device on which a FortiEDR mobile Collector is installed.

<table>
<tr><th>Information Field</th><th>Description</th></tr>
<tr><td>OS</td><td>Operating system of the communicating device on which the FortiEDR mobile Collector is installed.</td></tr>
<tr><td>IP</td><td>IP address of the communicating device on which the FortiEDR mobile Collector is installed.</td></tr>
<tr><td>Version</td><td>Version of the FortiEDR mobile Collector installed on the communicating device.</td></tr>
<tr><td>State</td><td>Current state of the FortiEDR mobile Collector. Hovering over the STATE value pops up the last time the STATE was changed. Possible value for STATE are as follows:
<table>
<tr><th>State</th><th>Description</th></tr>
<tr><td>Running</td><td>The FortiEDR mobile Collector is up and all is well.</td></tr>
<tr><td>Disconnected</td><td>The device is offline, powered down or is not connected to the FortiEDR Aggregator.</td></tr>
<tr><td>Disconnected (Expired)</td><td></td></tr>
<tr><td>Pending Reboot</td><td>After the FortiEDR mobile Collector is installed, you may want some devices to be rebooted before the FortiEDR mobile Collector can start running. This status means that the FortiEDR Collector is ready to run after this device is rebooted. The reboot is performed in the usual manner on the device itself.</td></tr>
<tr><td>Disabled</td><td>The FortiEDR mobile Collector was disabled in the FortiEDR Central Manager.</td></tr>
<tr><td>Degraded</td><td>The FortiEDR mobile Collector is prevented from performing to its full capacity (for example, due to lack of resources on the device on which it is installed or compatibility issues).</td></tr>
</table>
</td></tr>
<tr><td>Last Seen</td><td>Counts the number of days passed from the last time this mobile Collector communicated with the Core.</td></tr>
</table>

Defining a new Collector Group

Creating multiple Collector Groups enables you to assign different FortiEDR policies to different FortiEDR Collectors, which means to different end user groups. In addition, it enables data segmentation in FortiEDR and reports according to user groups. For example, you may want to assign a more permissive policy to the CEO of your organization.

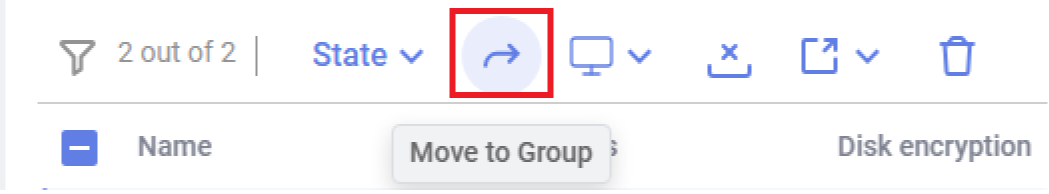
1. Click the *Add Group* button. The following window displays:



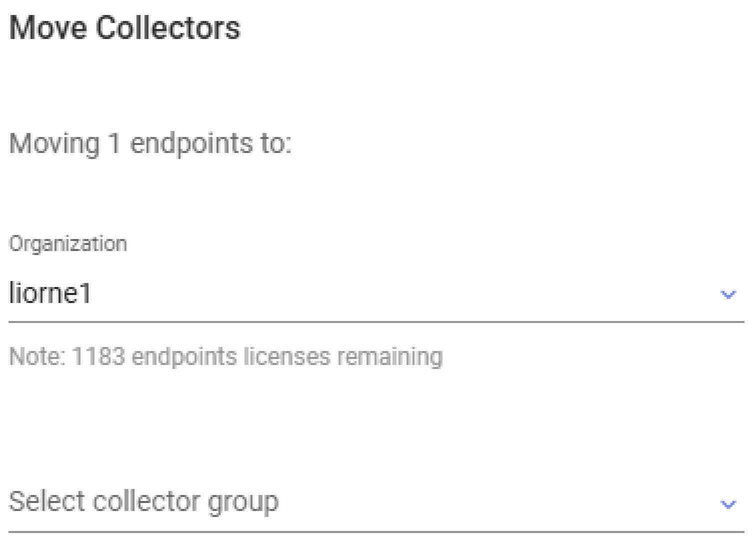
2. Enter any name for this group and click *Create*.

Assigning Collectors to a Collector Group

1. In the *Inventory* page, select the checkboxes of the FortiEDR Collectors to be moved to a different group.
2. Select the *Move to Group* button.



The following window displays with the name of the current Collector Group selected:



Move Collectors

Moving 1 endpoints to:

Organization: liorne1

Note: 1183 endpoints licenses remaining

3. Select the Collector Group to which to move the selected Collectors. FortiEDR shows how many Collectors each group contains.
4. Click the *Move* button.

Deleting a Collector Group/Collector

Deleting a Collector Group simply means that you are deleting a logical grouping of Collectors. These Collectors then become available to be selected in the default Collector Group. The Collector Group assigned as the default Collector Group cannot be deleted.

Deleting a Collector only deletes it from the FortiEDR Central Manager's console. If the FortiEDR Collector is not uninstalled on the device, it will automatically reappear in the FortiEDR Central Manager's COLLECTOR list.

To delete a Collector Group/Collector:

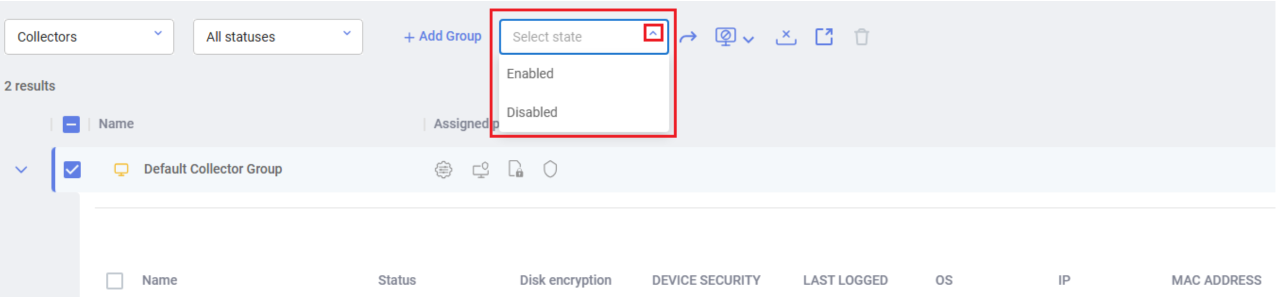
1. Select the Collector Group's/Collector's checkbox.
2. Click the *Delete* button.

Enabling/disabling a Collector

You can enable or disable one or more Collectors simultaneously.

To enable one or more Collectors simultaneously:

1. In the *Inventory* page, select the checkboxes of the FortiEDR Collectors to be enabled. All selected Collectors must be in a Disabled (▨) state.
2. Click the down arrow in the *Select state* dropdown and select *Enabled*.

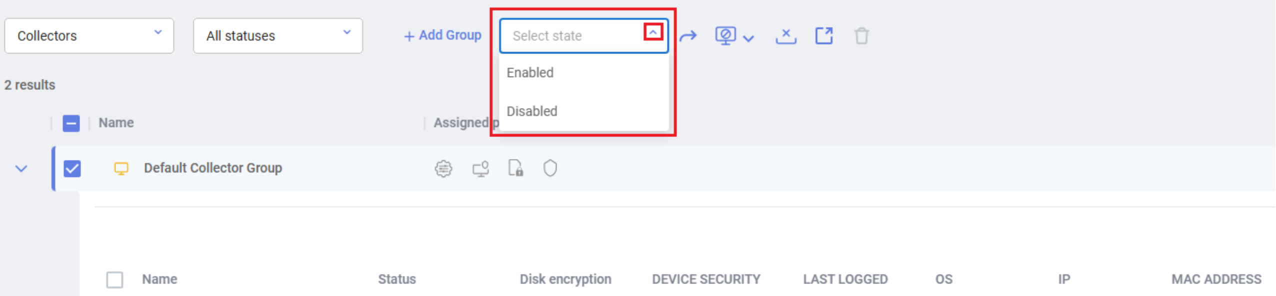


The *Select state* dropdown is available only if one or more Collectors are selected.
3. Click *Enable*.

To disable one or more Collectors simultaneously:

1. In the *COLLECTORS* page, select the checkboxes of the FortiEDR Collectors to be disabled. All selected Collectors must be in a *Running* (🟩) state.

2. Click the down arrow in the *Select state* dropdown and select *Disabled*.



The *Select state* dropdown is available only if one or more Collectors are selected.

3. Click *Disable*.

Device isolation

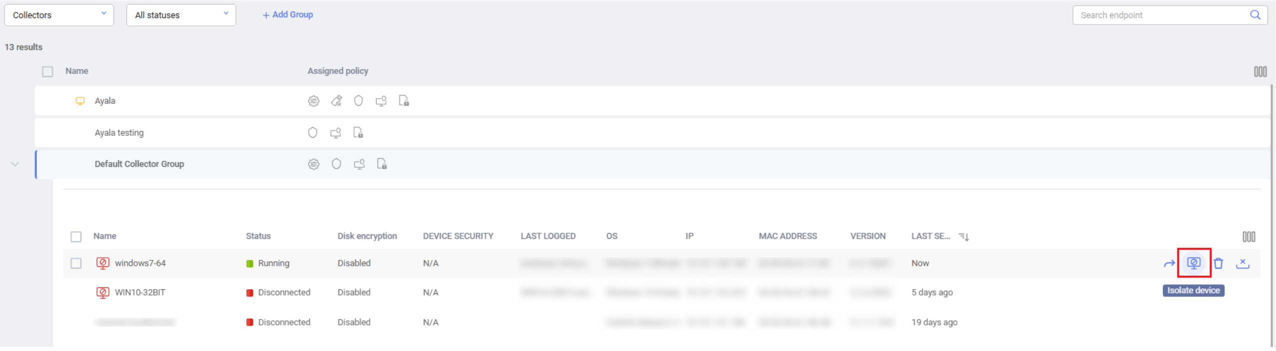
An isolated device is one that is blocked from communicating with the outside world (for both sending and receiving). A device can be isolated manually from the *Assets > Inventory* page or the Investigation View on page 92.

Isolation mode takes effect upon any attempt to establish a network session after isolation mode has been initiated. Connections that were established before device isolation was initiated remain intact. The same applies for Communication Control denial configuration changes. Note that both Isolation mode and Communication Control denial do not apply on incoming RDP connections and ICMP connections.

For more details about device isolation, see Investigation on page 249.

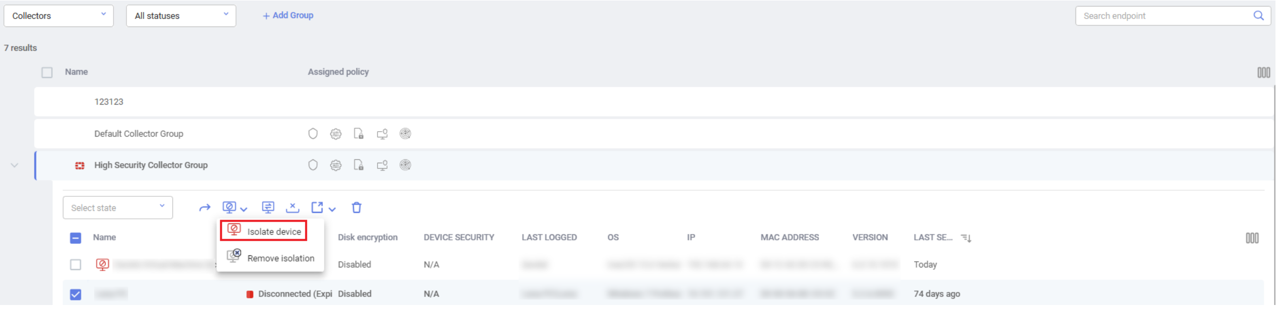
To isolate a device from the *Assets > Inventory* page:

1. In the *Inventory* page, hover your mouse to the right of the row of the FortiEDR Collector that you want to isolate and click the *Isolate device* button.



Name	Status	Disk encryption	DEVICE SECURITY	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	LAST SE...
windows7-64	🟩 Running	Disabled	N/A	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Now
WIN10-32BIT	🟥 Disconnected	Disabled	N/A	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	5 days ago
[redacted]	🟥 Disconnected	Disabled	N/A		[redacted]	[redacted]	[redacted]	[redacted]	19 days ago

Alternatively, select the Collector and click *Isolate* device button.



Collectors ˅ | All statuses ˅ | + Add Group | Search endpoint

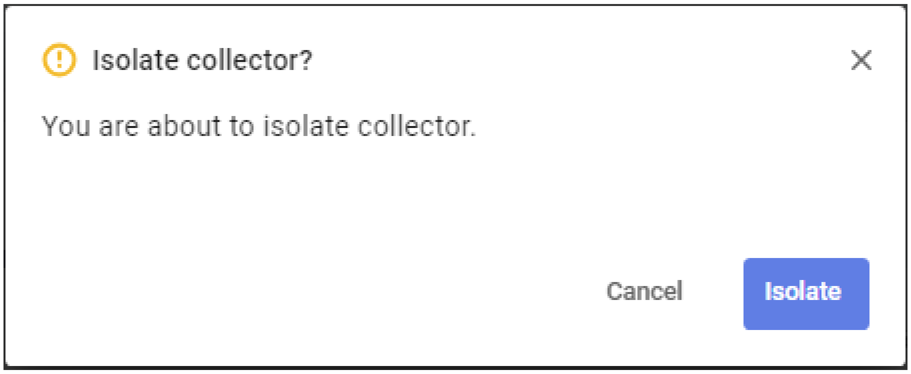
7 results

Name	Assigned policy
123123	
Default Collector Group	
High Security Collector Group	

Select state ˅

	Name	Status	Disk encryption	DEVICE SECURITY	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	LAST SE...
□	[redacted]		Disabled	N/A	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Today
☑	[redacted]	Disconnected (Expi	Disabled	N/A	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	74 days ago

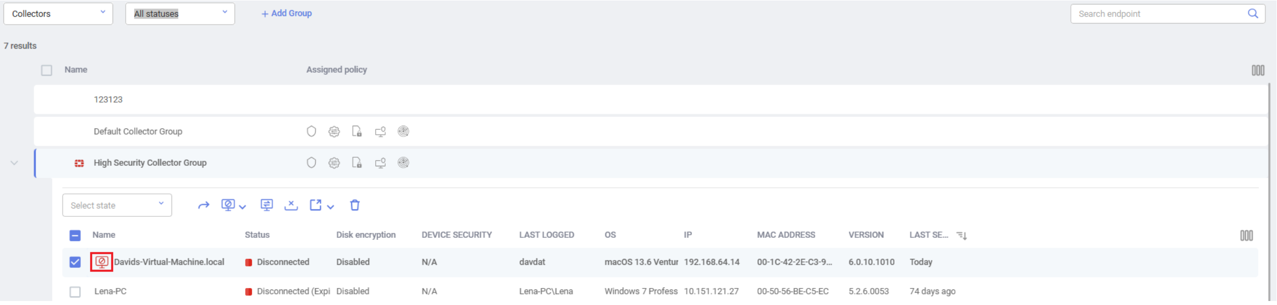
2. Click *Isolate*.



Isolate collector?

You are about to isolate collector.

The *Isolate* icon appears next to the relevant Collector to indicate that the Collector has been isolated, as shown below:



Collectors ˅ | All statuses ˅ | + Add Group | Search endpoint

7 results

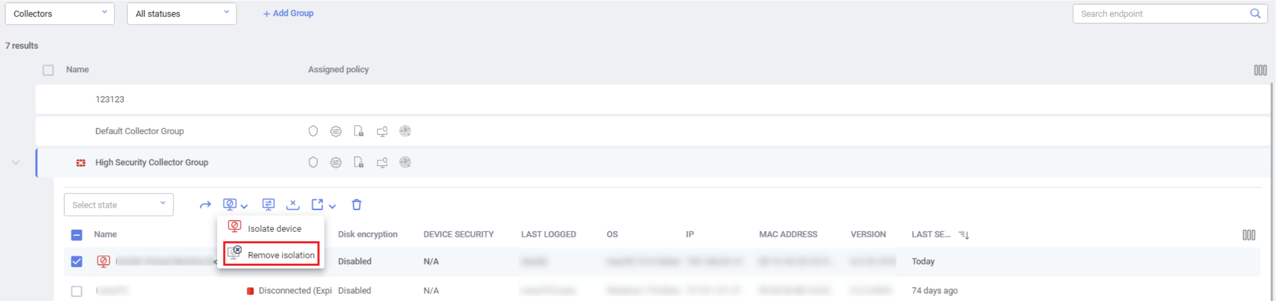
Name	Assigned policy
123123	
Default Collector Group	
High Security Collector Group	

Select state ˅

	Name	Status	Disk encryption	DEVICE SECURITY	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	LAST SE...
☑	Davids-Virtual-Machine.local	Disconnected	Disabled	N/A	davdat	macOS 13.6 Ventur	192.168.64.14	00-1C-42-2E-C3-9...	6.0.10.1010	Today
□	Lena-PC	Disconnected (Expi	Disabled	N/A	Lena-PC\Lena	Windows 7 Profess	10.151.121.27	00-50-56-BE-C5-EC	5.2.6.0053	74 days ago

To remove isolation from a device from the *Inventory > Collectors* page:

1. In the *COLLECTORS* page, select the checkbox(es) of the FortiEDR Collector(s) whose isolation you want to remove.
2. Click the down arrow on the *Isolate* button and select *Remove isolation*, as shown below.



Collectors ˅ | All statuses ˅ | + Add Group | Search endpoint

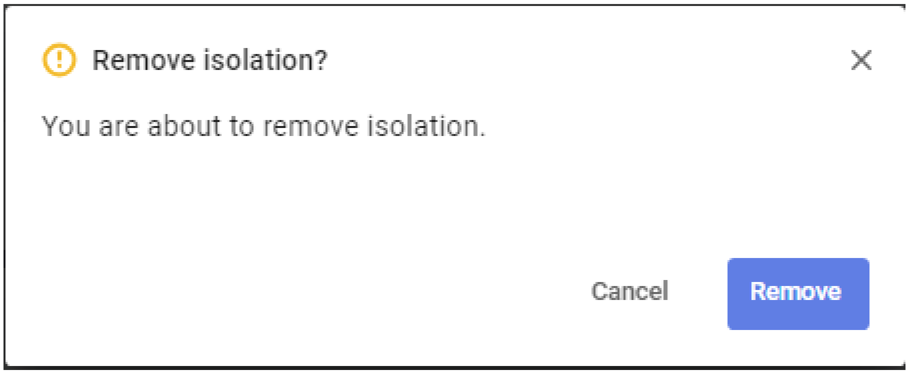
7 results

Name	Assigned policy
123123	
Default Collector Group	
High Security Collector Group	

Select state ˅

	Name	Status	Disk encryption	DEVICE SECURITY	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	LAST SE...
☑	[redacted]		Disabled	N/A	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Today
□	[redacted]	Disconnected (Expi	Disabled	N/A	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	74 days ago

3. Click *Remove*.

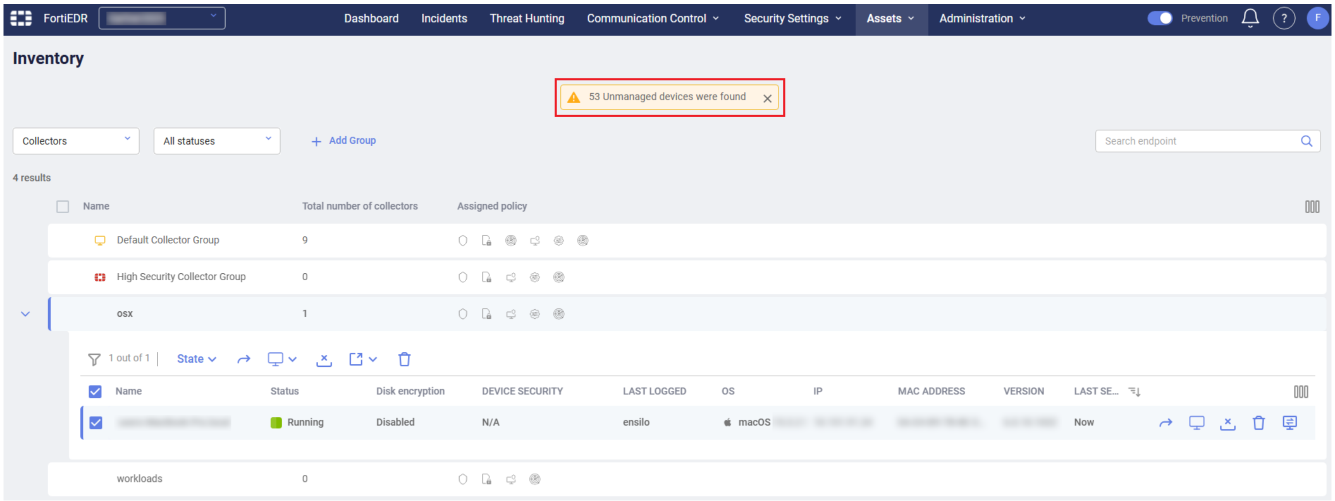


Remove isolation?

You are about to remove isolation.

Unmanaged devices

The *Inventory* page also indicates the number of unmanaged devices found in the system at the top of the page, meaning those non-IoT devices on which no Collector is installed.



Inventory

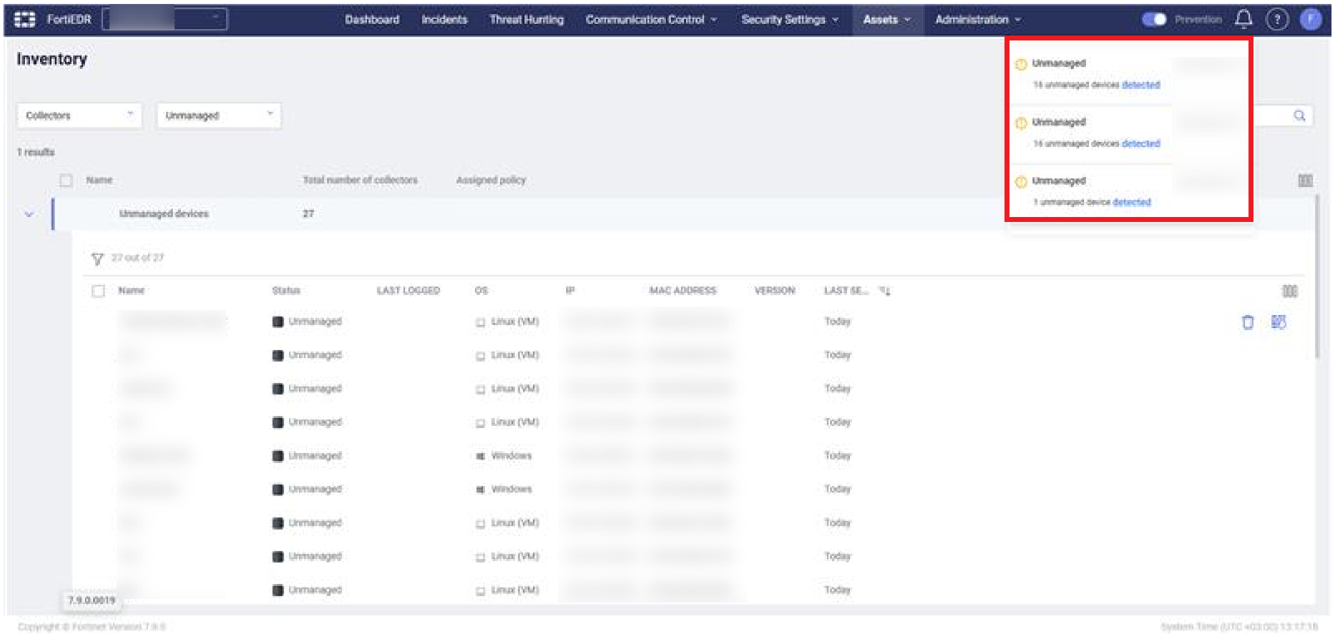
53 Unmanaged devices were found

4 results

Name	Total number of collectors	Assigned policy
Default Collector Group	9	
High Security Collector Group	0	
osx	1	
workloads	0	

☑	Name	Status	Disk encryption	DEVICE SECURITY	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	LAST SE...
☑	[redacted]	🟩 Running	Disabled	N/A	ensilo	macOS [redacted]	[redacted]	[redacted]	[redacted]	Now

When new unmanaged devices are detected, FortiEDR sends real-time notifications with a link that redirects to the unmanaged devices view.



Inventory

Collectors | Unmanaged

Unmanaged
16 unmanaged devices detected

Unmanaged
16 unmanaged devices detected

Unmanaged
1 unmanaged device detected

1 results

Name	Total number of collectors	Assigned policy
Unmanaged devices	27	

27 out of 27

Name	Status	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	LAST SE...
[redacted]	Unmanaged		Linux (VM)	[redacted]	[redacted]		Today
[redacted]	Unmanaged		Linux (VM)	[redacted]	[redacted]		Today
[redacted]	Unmanaged		Linux (VM)	[redacted]	[redacted]		Today
[redacted]	Unmanaged		Linux (VM)	[redacted]	[redacted]		Today
[redacted]	Unmanaged		Windows	[redacted]	[redacted]		Today
[redacted]	Unmanaged		Windows	[redacted]	[redacted]		Today
[redacted]	Unmanaged		Linux (VM)	[redacted]	[redacted]		Today
[redacted]	Unmanaged		Linux (VM)	[redacted]	[redacted]		Today
[redacted]	Unmanaged		Linux (VM)	[redacted]	[redacted]		Today

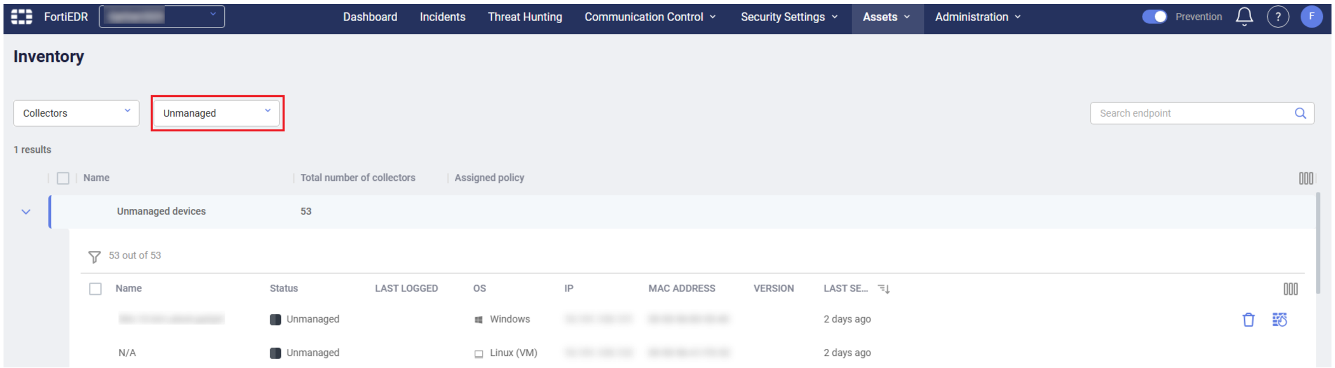
7.9.0.0019

Copyright © Fortinet Version 7.9.0

System Time (UTC +03:00) 13:17:18

Unmanaged devices are not protected in the system. Therefore, it is recommended that you either install a Collector on each such device or remove it from your network.

To view the list of unmanaged devices, ensure you have enabled IoT Device Discovery on page 331 at least once after deploying Collectors and then select *Unmanaged* in the filter at the top left of the page.



Inventory

Collectors | Unmanaged

Search endpoint

1 results

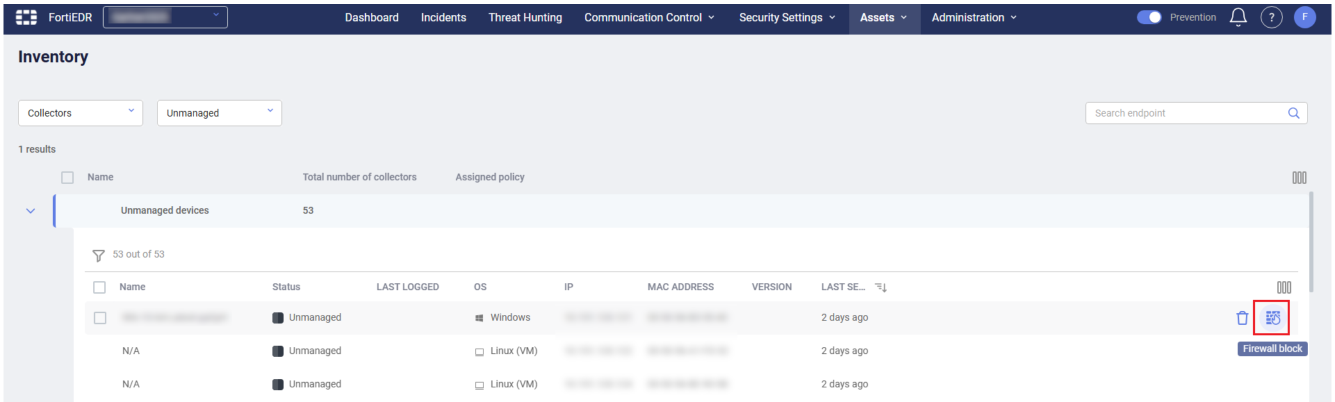
Name	Total number of collectors	Assigned policy
Unmanaged devices	53	

53 out of 53

Name	Status	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	LAST SE...
[redacted]	Unmanaged		Windows	[redacted]	[redacted]		2 days ago
N/A	Unmanaged		Linux (VM)	[redacted]	[redacted]		2 days ago

None of the action buttons for managed Collectors are available for unmanaged devices, as there is no Collector installed on these devices.

You can activate the firewall playbook to block address on firewall for unmanaged devices. The block action triggers an integration using the firewall connector to block the device.



Inventory

1 results

Name	Total number of collectors	Assigned policy
Unmanaged devices	53	

53 out of 53

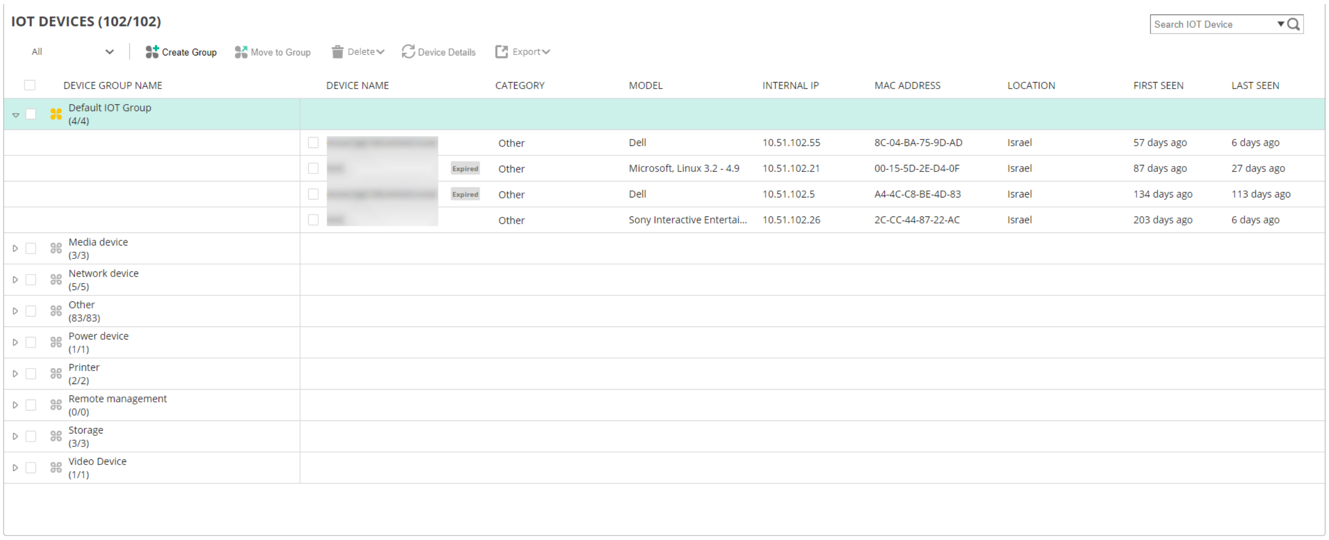
Name	Status	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	LAST SE...
[redacted]	Unmanaged		Windows	[redacted]	[redacted]		2 days ago
N/A	Unmanaged		Linux (VM)	[redacted]	[redacted]		2 days ago
N/A	Unmanaged		Linux (VM)	[redacted]	[redacted]		2 days ago

IoT devices

The *IOT DEVICES* page lists the non-workstation devices, such as printers, cameras and so on, that are part of your network. To access this page, click the down arrow next to *INVENTORY* and then select *IoT*.

This option is only available to users who have purchased the *Discover and Protect* or the *Discover, Protect and Response* license.

FortiEDR provides you with visibility to any device in your network, including those on which FortiEDR components are not installed. IoTs are proactively discovered from existing FortiEDR Collectors. For more details, see IoT Device Discovery on page 331.



IOT DEVICES (102/102)

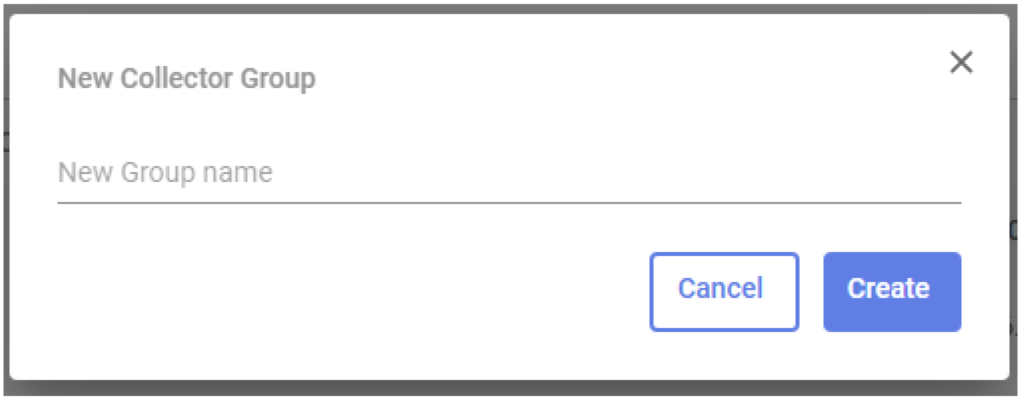
DEVICE GROUP NAME	DEVICE NAME	CATEGORY	MODEL	INTERNAL IP	MAC ADDRESS	LOCATION	FIRST SEEN	LAST SEEN
Default IOT Group (4/4)								
	[redacted]	Other	Dell	10.51.102.55	8C-04-BA-75-9D-AD	Israel	57 days ago	6 days ago
	[redacted] Expired	Other	Microsoft, Linux 3.2 - 4.9	10.51.102.21	00-15-5D-2E-D4-0F	Israel	87 days ago	27 days ago
	[redacted] Expired	Other	Dell	10.51.102.5	A4-4C-C8-BE-4D-83	Israel	134 days ago	113 days ago
	[redacted]	Other	Sony Interactive Entertai...	10.51.102.26	2C-CC-44-87-22-AC	Israel	203 days ago	6 days ago
Media device (3/3)								
Network device (5/5)								
Other (83/83)								
Power device (1/1)								
Printer (2/2)								
Remote management (0/0)								
Storage (3/3)								
Video Device (1/1)								

This page provides all the collected information about each discovered device, including its name, Category (device type), model number, internal IP address, MAC address, the physical location where the device was detected (based on its external IP address) and when it was first and last seen. FortiEDR presents all the information it collected for each device. Information that was not available for a device is marked as N/A in that device's row in the table. The *New* indication indicates that the device was discovered within the last three days. The *Expired* indication indicates that the device has not been seen for more than one week.

The default IoT Group to which new IoT devices are automatically added is marked with a yellow group icon. You can change to a different default IoT Group by clicking the group icon of another IoT Group. Alternatively, you can use Category-based grouping, where each new IoT device is automatically added to the group that represents its Category (for example, network devices, cameras, printers and so on).

Defining a new IoT group

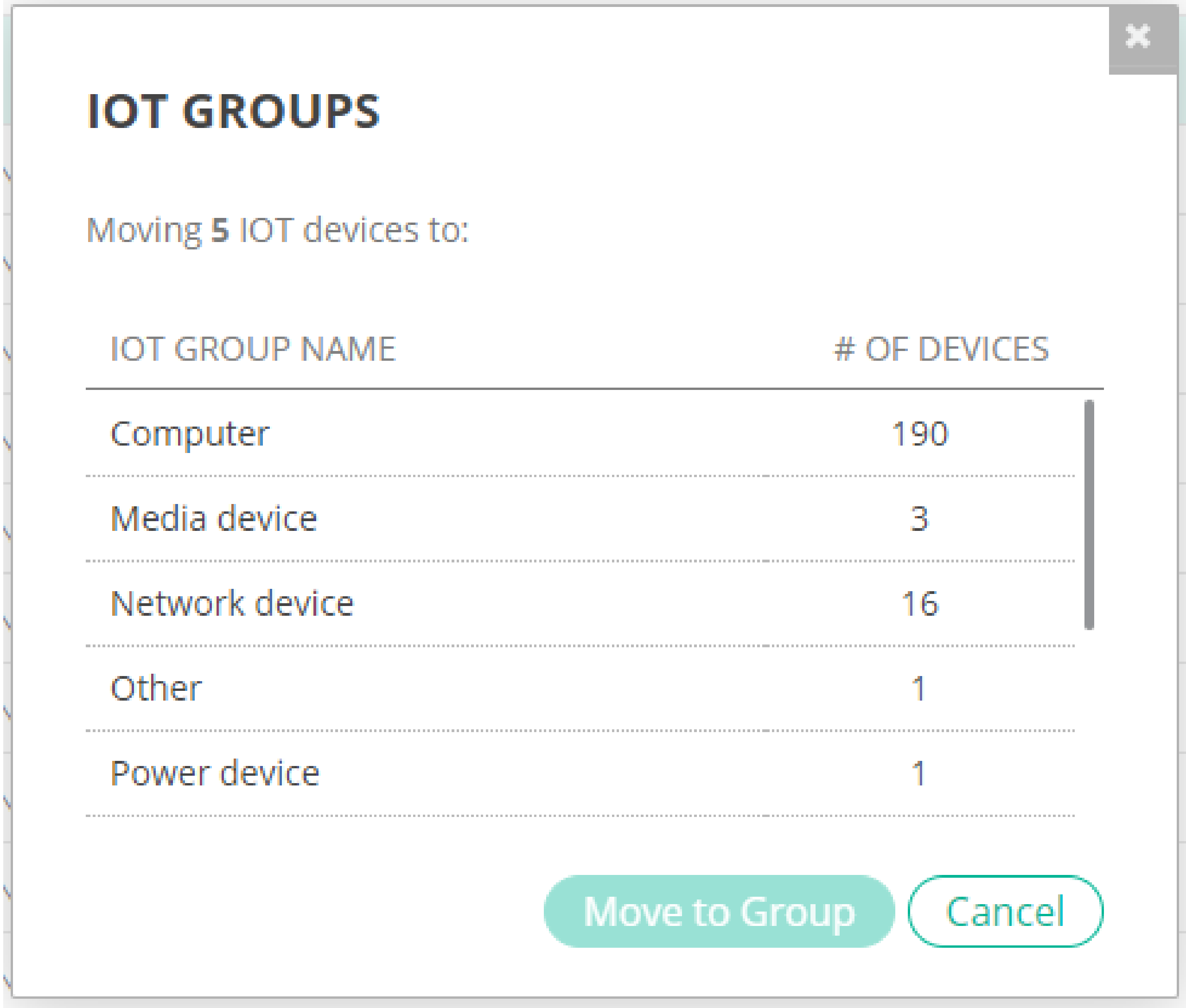
1. Click the *Create group* button. The following window displays:



2. Enter any name for this group.
3. Click *Create new group*.

Assigning devices to an IoT group

1. In the *IOT DEVICES* page, select the checkboxes of the IoT devices to be moved to a different group.
2. Select the *Move to group* button. The following window displays showing the names of the current IoT Groups and how many devices each contains:



IOT GROUPS

Moving **5** IOT devices to:

IOT GROUP NAME	# OF DEVICES
Computer	190
Media device	3
Network device	16
Other	1
Power device	1

3. Select the IoT Group to which to move the selected devices.
4. Click *Move to Group*.

Deleting an IoT device/IoT group

Deleting an IoT Group simply means that you are deleting a logical grouping of IoT devices. These devices then become available to be selected in the default IoT Group. The IoT Group assigned as the default IoT Group cannot be deleted.

Deleting an IoT device deletes it from the FortiEDR Central Manager's console. However, if the device is still connected to your network, it will re-appear following the next network scan.

To delete an IoT device/IoT group:

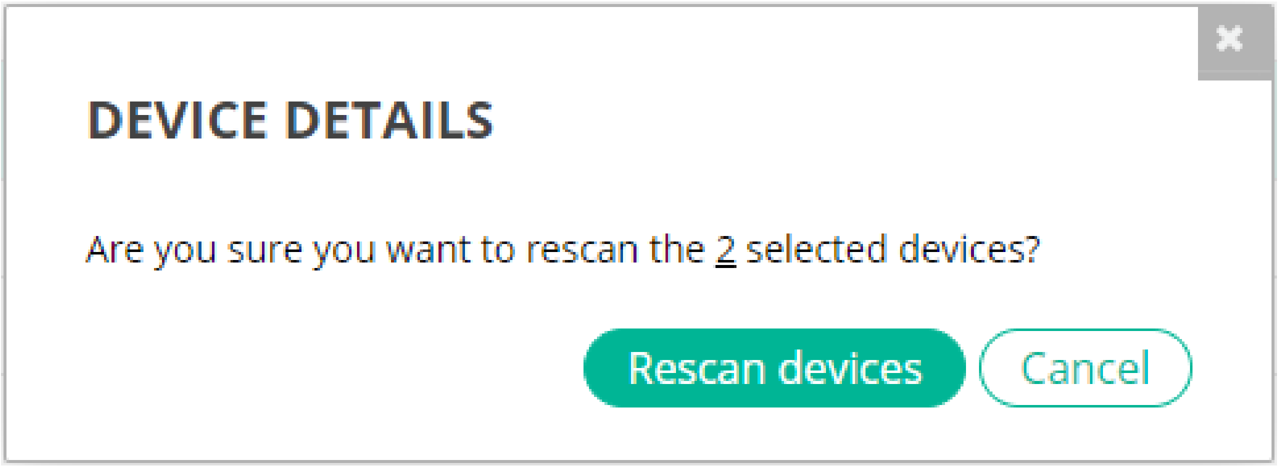
1. Select the IoT group's/IoT device's checkbox.
2. Click *Delete*.

Refreshing IoT device data

You can run a scan for a specific IoT device to recollect data for that device.

To rescan an IoT device(s):

1. Select the IoT device's checkbox for the device(s) that you want to scan and then click the *Device Details* button. A confirmation window displays.



DEVICE DETAILS

Are you sure you want to rescan the 2 selected devices?

2. Click *Rescan devices*.

Exporting IoT information

To export the list of IoT devices:

1. Click the *Export* button.
2. Select *Excel*.

To export details for an IoT device:

1. Check the checkbox of the device of interest.
2. Select *Device Info* under the *Export* button.

You can only export details for one device at a time. This report exports all collected data for the IoT device of interest, including additional data beyond what is presented in the user interface.

Exporting logs

The Export Logs feature enables you to retrieve technical information from the FortiEDR devices deployed in the organization, such as from Collectors, Cores, Aggregators and the Management server. The retrievable technical content describes the activities of each FortiEDR device. Typically, the technical content contains logs and statistical information. The retrieved technical content is password-protected. The password is `enCrypted`.

Logs only need to be retrieved when Fortinet technical support requests that you provide them. There is no need for you to analyze the data contained in the FortiEDR logs. You can retrieve logs for the following:

- Exporting logs for Collectors on page 273
- Exporting logs for Cores on page 274
- Exporting logs for Aggregators on page 275

To retrieve threat hunting logs, see Exporting threat hunting logs on page 166.

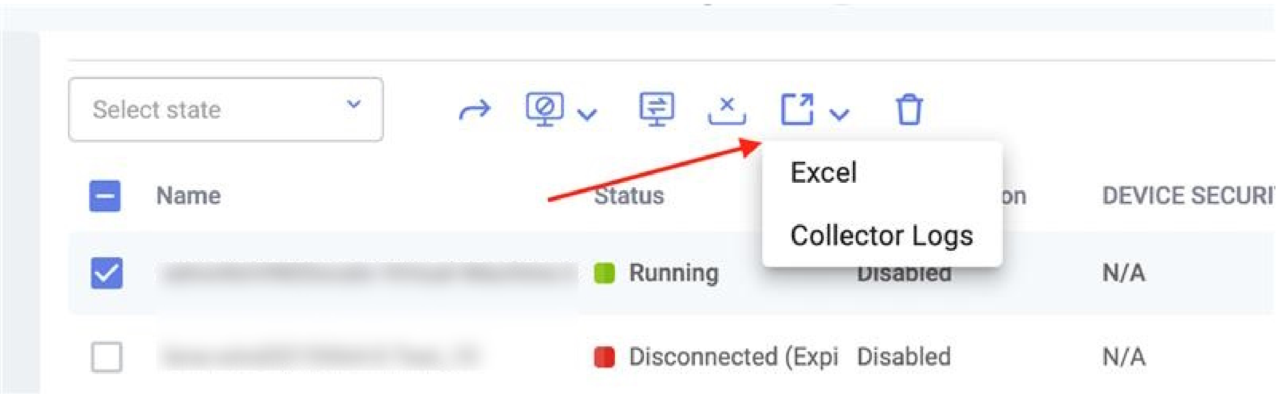
Exporting logs for Collectors

You can export logs for Collectors that are in *Running* status.

To export Collector logs:

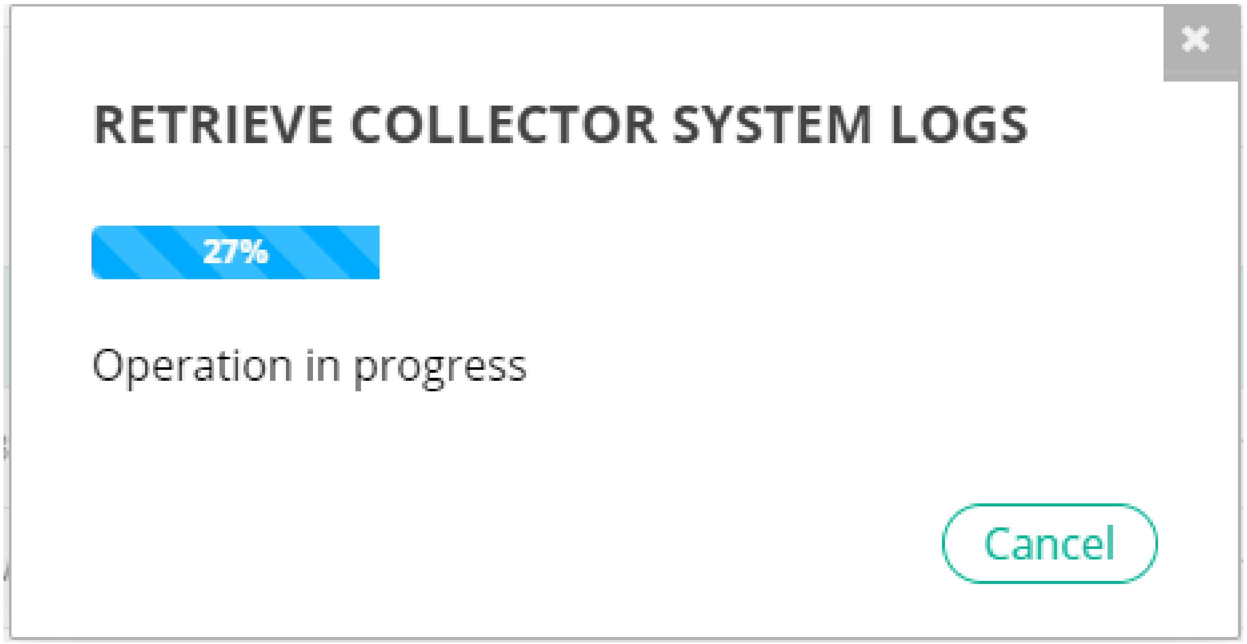
1. In the *Collectors* page, select the checkbox of the FortiEDR Collector for which you want to export logs and click the down arrow on the *Export* dropdown menu and select *Collector Logs*.
   Note you can only export the logs for one Collector at a time and the Collector has to be in *Running* status.

2.



☐	Name	Status	on	DEVICE SECURI
☑	[redacted]	🟩 Running	Disabled	N/A
☐	[redacted]	🟥 Disconnected (Expi	Disabled	N/A

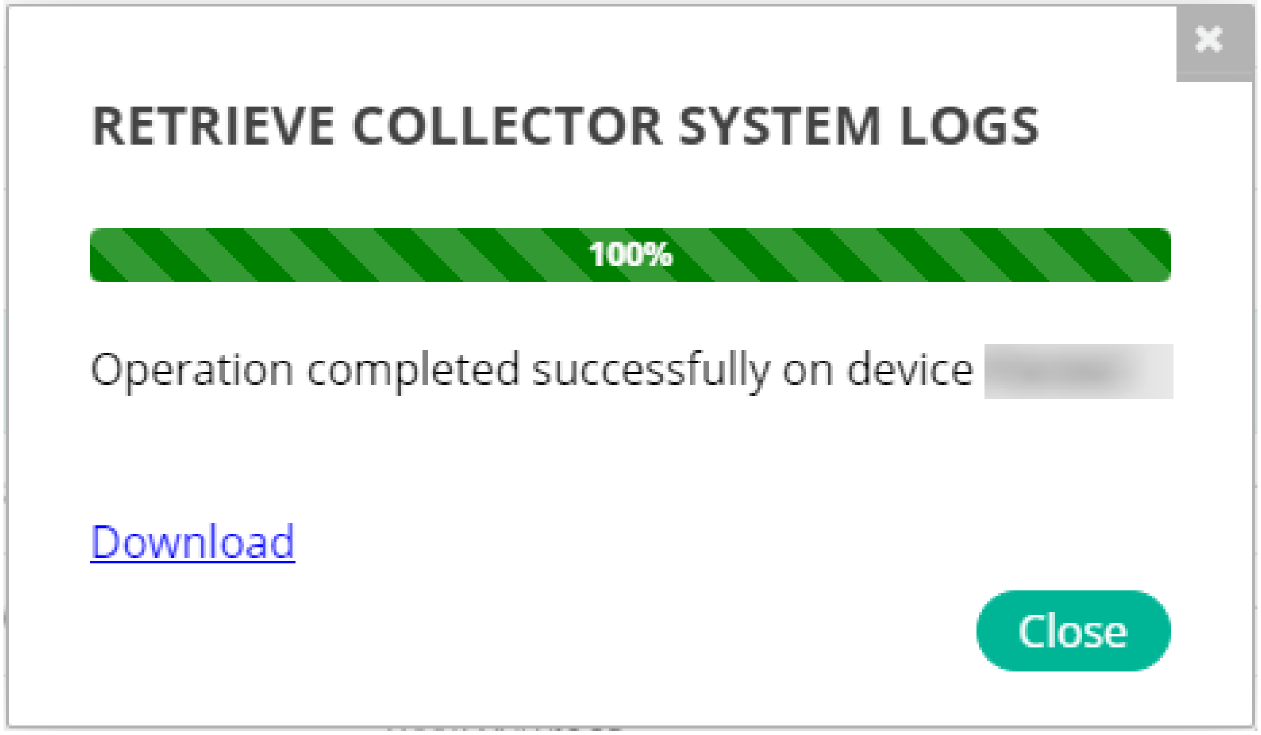
3. A progress window displays, showing the status of the Collector log retrieval process:



RETRIEVE COLLECTOR SYSTEM LOGS

Operation in progress

After the retrieval process completes, the following window displays:



RETRIEVE COLLECTOR SYSTEM LOGS

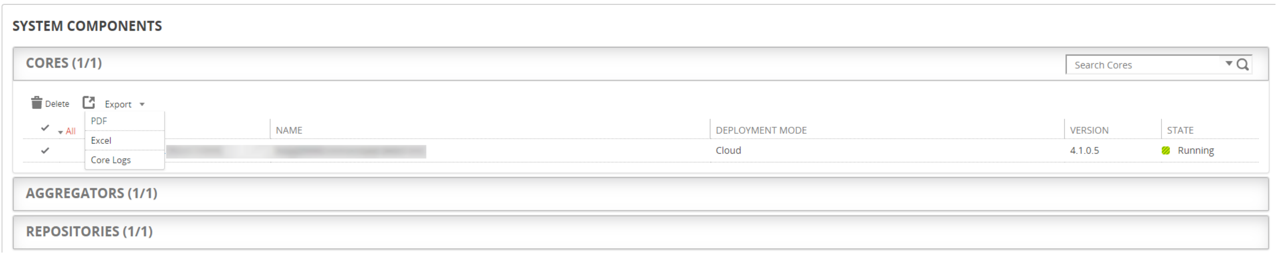
Operation completed successfully on device [redacted]

4. Click *Download* to automatically send the retrieved logs to Fortinet technical support.

Exporting logs for Cores

1. In the *SYSTEM COMPONENTS* page, select the checkboxes of the FortiEDR Cores for which you want to export logs.

2. Click the down arrow on the *Export* dropdown menu and select *Core Logs*.



SYSTEM COMPONENTS

CORES (1/1)

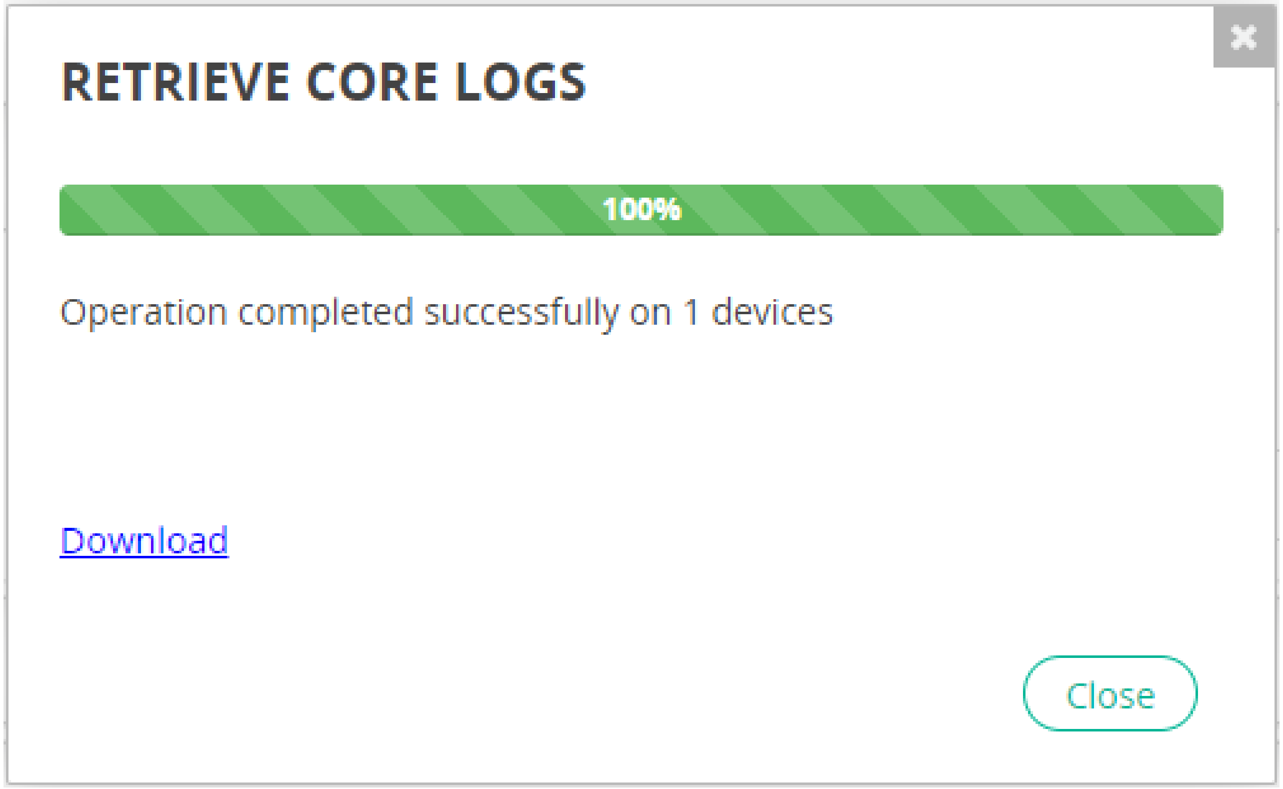
✓ All	NAME	DEPLOYMENT MODE	VERSION	STATE
✓	[redacted]	Cloud	4.1.0.5	🟩 Running

AGGREGATORS (1/1)

REPOSITORIES (1/1)

A progress window displays, showing the status of the log retrieval process:

After the retrieval process completes, the following window displays:



RETRIEVE CORE LOGS

100%

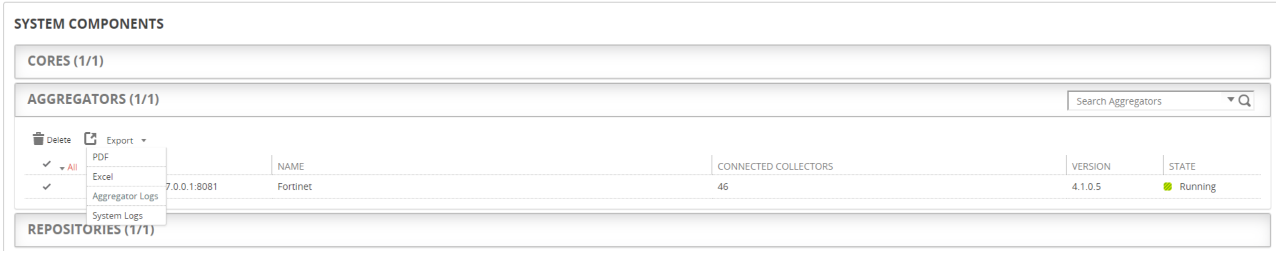
Operation completed successfully on 1 devices

3. Click *Download* to automatically send the retrieved logs to Fortinet technical support.

Exporting logs for Aggregators

1. In the *SYSTEM COMPONENTS* page, select the checkboxes of the FortiEDR Aggregator for which you want to export logs.

2. Click the down arrow on the *Export* dropdown menu and select one of the following options:



SYSTEM COMPONENTS

CORES (1/1)

AGGREGATORS (1/1)

✓ All		NAME	CONNECTED COLLECTORS	VERSION	STATE
✓	7.0.0.1:8081	Fortinet	46	4.1.0.5	🟩 Running

REPOSITORIES (1/1)

   a. *Aggregator Logs*: Exports the log for the selected Aggregator(s).
   b. *System Logs*: Exports the logs of the central Manager.
      A progress window displays.
      After the retrieval process completes, a window displays.
      Click *Download* to automatically send the retrieved logs to Fortinet technical support.

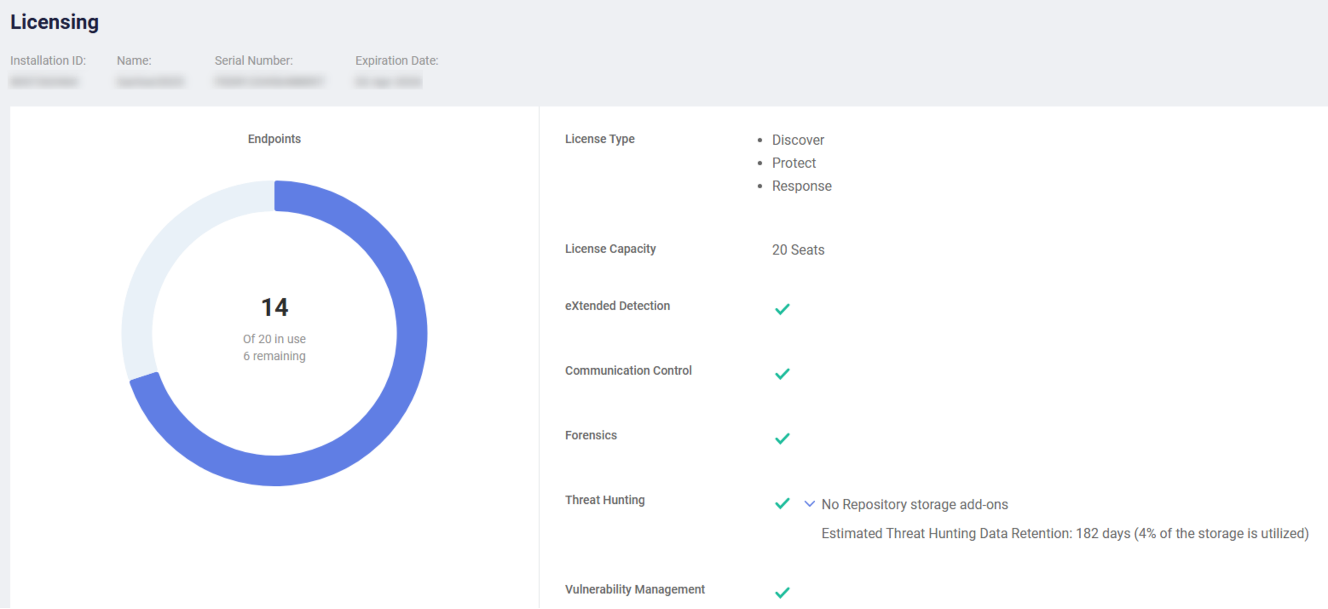
Administration

This chapter describes the FortiEDR Administration options, which are fully available to users with Admin permissions, partially available to users with IT or Senior Analyst permissions, and read-only for users with read-only permissions.

Licensing

Selecting *LICENSING* in the *ADMINISTRATION* tab displays all the entitlements provided by your license.

This window also shows your Serial Number, which is your FortiEDR unique identifier with Fortinet.



Licensing

Installation ID:	Name:	Serial Number:	Expiration Date:
[redacted]	[redacted]	[redacted]	[redacted]

License Type	- Discover - Protect - Response
License Capacity	20 Seats
eXtended Detection	✓
Communication Control	✓
Forensics	✓
Threat Hunting	✓ No Repository storage add-ons Estimated Threat Hunting Data Retention: 182 days (4% of the storage is utilized)
Vulnerability Management	✓

The tab bar at the top of the window may display a white circle(s) with a number inside the circle to indicate that new security events have not been read by the user. For Administration, the number represents the number of unread system events.

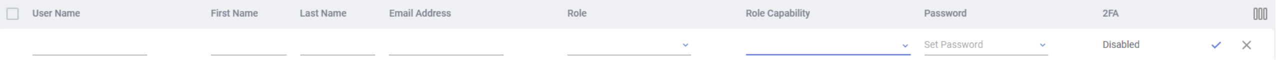
Users

The USERS option specifies who is allowed to use the FortiEDR Central Manager console. During installation of the FortiEDR Central Manager, you must specify the user name and password of the first FortiEDR Central

Manager console user. This is the only user who can log in to the FortiEDR Central Manager console for the first time.

To add a user:

1. Click the *Add User* button (+ Add User).
2. Fill in the displayed window.



□ User Name	First Name	Last Name	Email Address	Role	Role Capability	Password	2FA	
						Set Password	Disabled	✓ ✕

3. Define this user's password. Make sure to remember it and notify the user about this password.
4. Select the user's role. The system comes with the following predefined user roles:

Role	Description
Admin	Highest-level super user that can perform all operations in the FortiEDR Central Manager console for the organization.
Senior Analyst	Analysts supervisor who can define security policies in addition to all the actions that can be performed by an Analyst. Similar to admin users but without system configuration privileges under the *ADMINISTRATION* tab. A senior analyst can view information and perform actions, such as marking security events as handled, changing policies and defining exceptions, but cannot access the system configuration options under the *ADMINISTRATION* tab.
Analyst	SOC/MDR service analyst who can perform actions as required in the day-to-day activities of handling events. Similar to senior analyst users but without access to security configuration. An analyst can view information and perform actions, such as marking security events as handled, but cannot access the *ADMINISTRATION* tab or define/change policies.
IT	IT staff who can define settings related to the FortiEDR integration with the customer ecosystem. This role has system configuration access only. They can deploy and upgrade system components and perform system integration with external systems using the *ADMINISTRATION* tab but do not have access to other areas, such as security configuration, alert monitoring, or Forensics options.
Read-Only	Basic role with read-only access to all functions except system configuration.

For Multi-tenancy (organizations) on page 415 systems, you can also configure the user with role-specific access to all organizations.

5. Select any advanced options as needed. Some options are available to users with specific permissions only.

Option	Description
Rest API	Specifies whether to allow the user to access the FortiEDR Central Manager through API calls. For more information about APIs, see the FortiEDR RESTful API Guide. You must log in to the Fortinet Developer Network to access the guide.
Custom script	Specifies whether to allow the user to upload and manage (add, modify and delete) Python scripts that call third-party system APIs (see Connectors on page 339). Those scripts will then be automatically triggered by FortiEDR as incident responses. This option is only available to users with Admin and IT permissions.
FortiEDR Connect	Specifies whether to allow the user to use FortiEDR Connect capabilities which provide direct access to FortiEDR-protected devices running on Windows through a remote Shell connection, as described in FortiEDR Connect on page 109. This option is only available to users with Admin, Analyst, and Senior Analyst permissions. This option takes effect only when the *Allow FortiEDR Connect - remote shell connection* checkbox is selected under *Administration > Settings*, which means the FortiEDR Connect functionality is enabled at the organization level.

6. If the *Require 2FA* option is disabled in *Password Policy*, you can enable 2FA for this particular user by configuring the 2FA prompt frequency to be *Always*, *Daily*, or *Weekly*. See Two-factor authentication on page 279 for more information.

   This option is available only if *Require 2FA* is disabled in *Password Policy*.

7. Click *Apply* (the checkmark) to save the user.

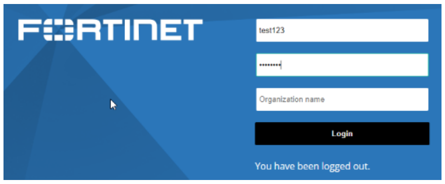
Two-factor authentication

You can require two-factor authentication for all FortiEDR users or specific users, which means those users must provide additional proof in addition to his or her user name and password when logging in to FortiEDR. To verify the user’s identity, FortiEDR supports two-factor authentication using FortiToken or any third-party authentication application, such as Google Authenticator, Microsoft Authenticator, Okta, or Duo.

- To enforce two-factor authentication on all users, check the *Require 2FA* checkbox when setting up the password policy.
- To require two-factor authentication on specific users, disable the *Require 2FA* checkbox in *Password Policy* and check the enable the *2FA* option for that user, as described in Users on page 277.

The following is an example of how a user logs in using two-factor authentication with Google Authenticator:

1. When prompted with the following window during your first login, enter the user name and password and click *LOGIN*.



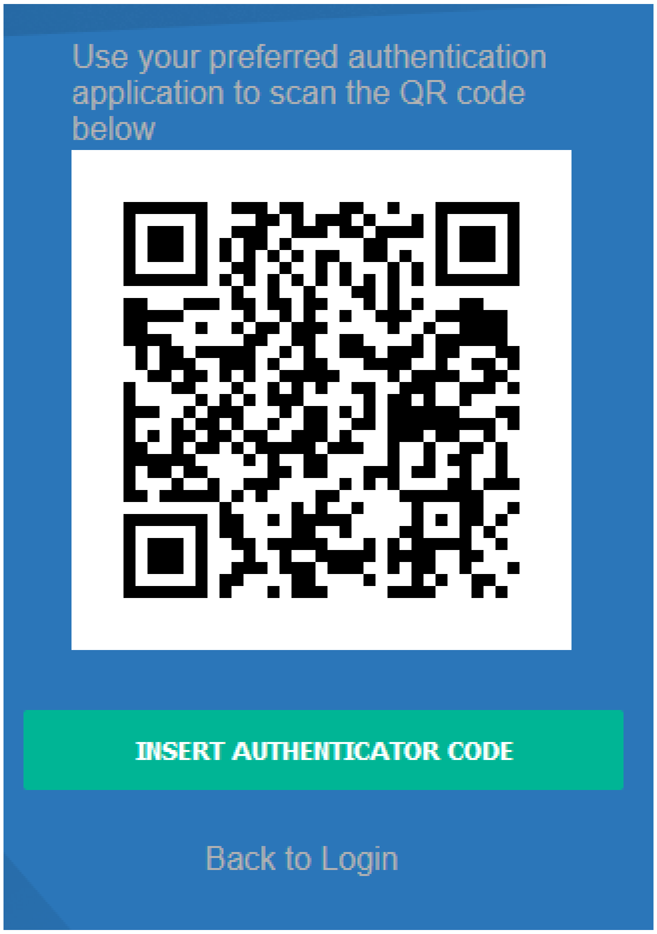
test123

••••••••

Organization name

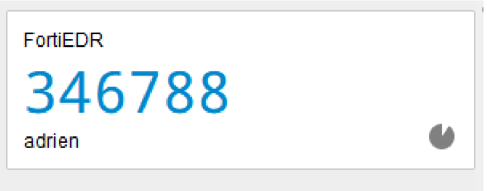
You have been logged out.

2. On your mobile device, click the *Google Authenticator* icon to launch Google Authenticator. A QR code displays in the FortiEDR window, as shown below:

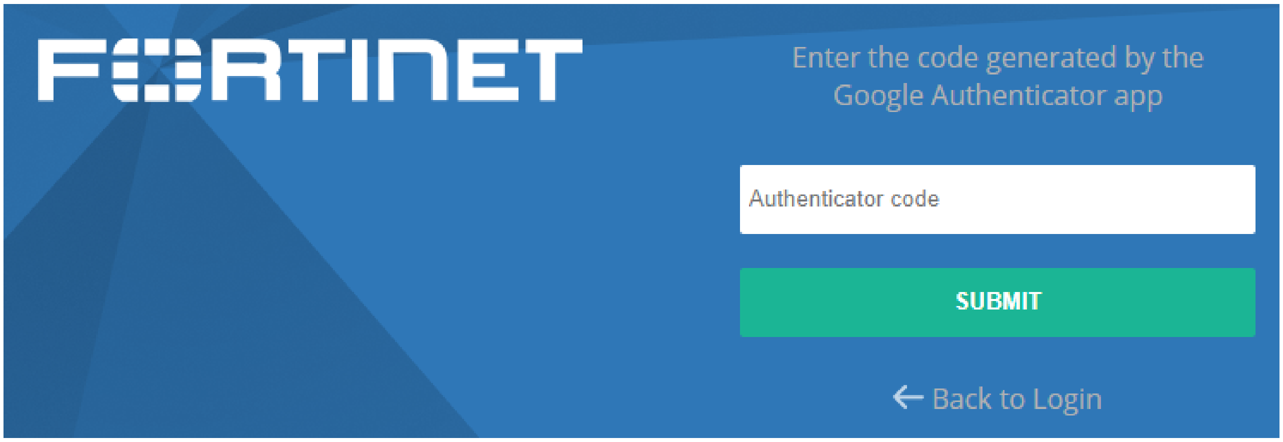


Use your preferred authentication application to scan the QR code below

3. Scan the QR code using your mobile device. A FortiEDR token appears on the mobile device, as shown below. Note that this token (code) changes every 30 seconds.



4. In the FortiEDR login window, click the *INSERT AUTHENTICATOR CODE* button. The following window displays:



5. Enter the authentication token (code) you received in step 3, and then click *SUBMIT*. Be sure to enter the latest code, as the code changes every 30 seconds.
   Depending on the 2FA prompt frequency you set up for the user(s), FortiEDR verifies the user's identity for each login or on a daily or weekly basis by asking for a new token, when the user has to repeat steps 1 through 5 to re-authenticate. To set a different cycle on a standalone environment, please contact Fortinet Support.

Resetting a user password

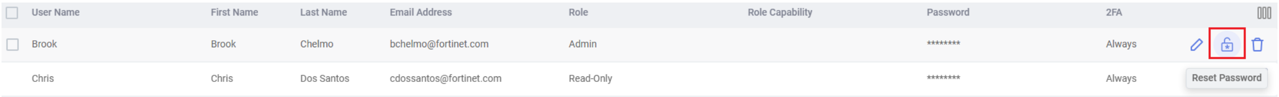
You can set a new password for a user in the following cases:

- A user forgets his or her password and cannot log in.
- A user password is compromised and poses a security risk.
- A user account gets locked after five or more consecutive failed login attempts due to an incorrect password.

If a user who must use two-factor authentication cannot access the FortiEDR application because of a lost or replaced mobile device, that user must repeat the procedure in Two-factor authentication on page 279 in order to log in. Before performing this procedure, you must first reset that user’s password to accept a new two-factor authentication token.

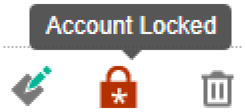
To reset a user password:

1. In the *ADMINISTRATION* tab, click the *USERS* link. The user list displays.
2. Place your cursor on the row of the user whose password you want to reset and click the *Reset Password* button.

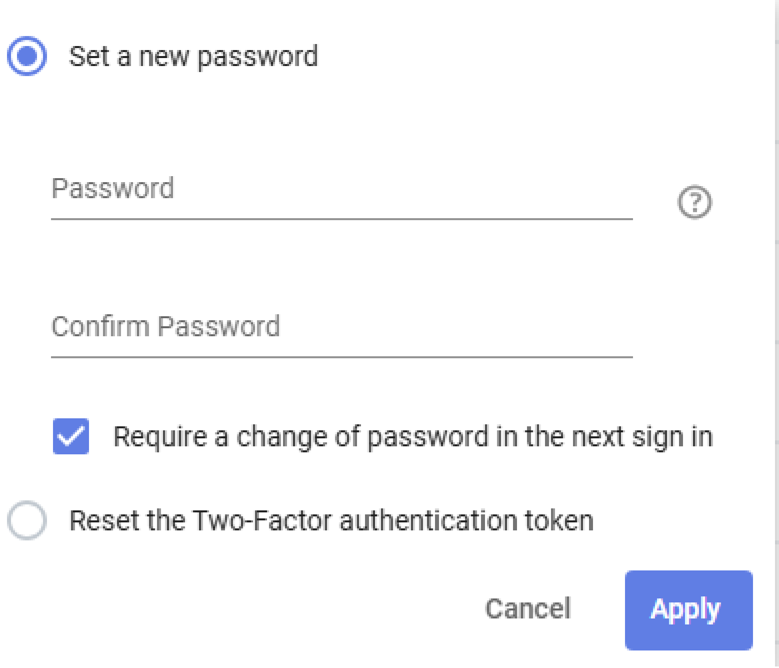


☐ User Name	First Name	Last Name	Email Address	Role	Role Capability	Password	2FA	
☐ Brook	Brook	Chelmo	bchelmo@fortinet.com	Admin		********	Always	
Chris	Chris	Dos Santos	cdossantos@fortinet.com	Read-Only		********	Always	Reset Password

If the user account is locked, the button is in red.



3. In the *Reset Password* window that appears:



● Set a new password

Password

Confirm Password

☑ Require a change of password in the next sign in

○ Reset the Two-Factor authentication token

Cancel Apply

Do one of the following:

- Click the *Set a new password* radio button and define a new password for the user. Make sure the password follows the password policy. You can also require the user to change the password during the next login.
- For a user that must use two-factor authentication, click the *Reset the Two-Factor authentication token* radio button to force user identity verification using two-factor authentication during that user's next login. This means that the user must complete the procedure in Two-factor authentication on page 279 in order to log in.

4. Click *Apply*.

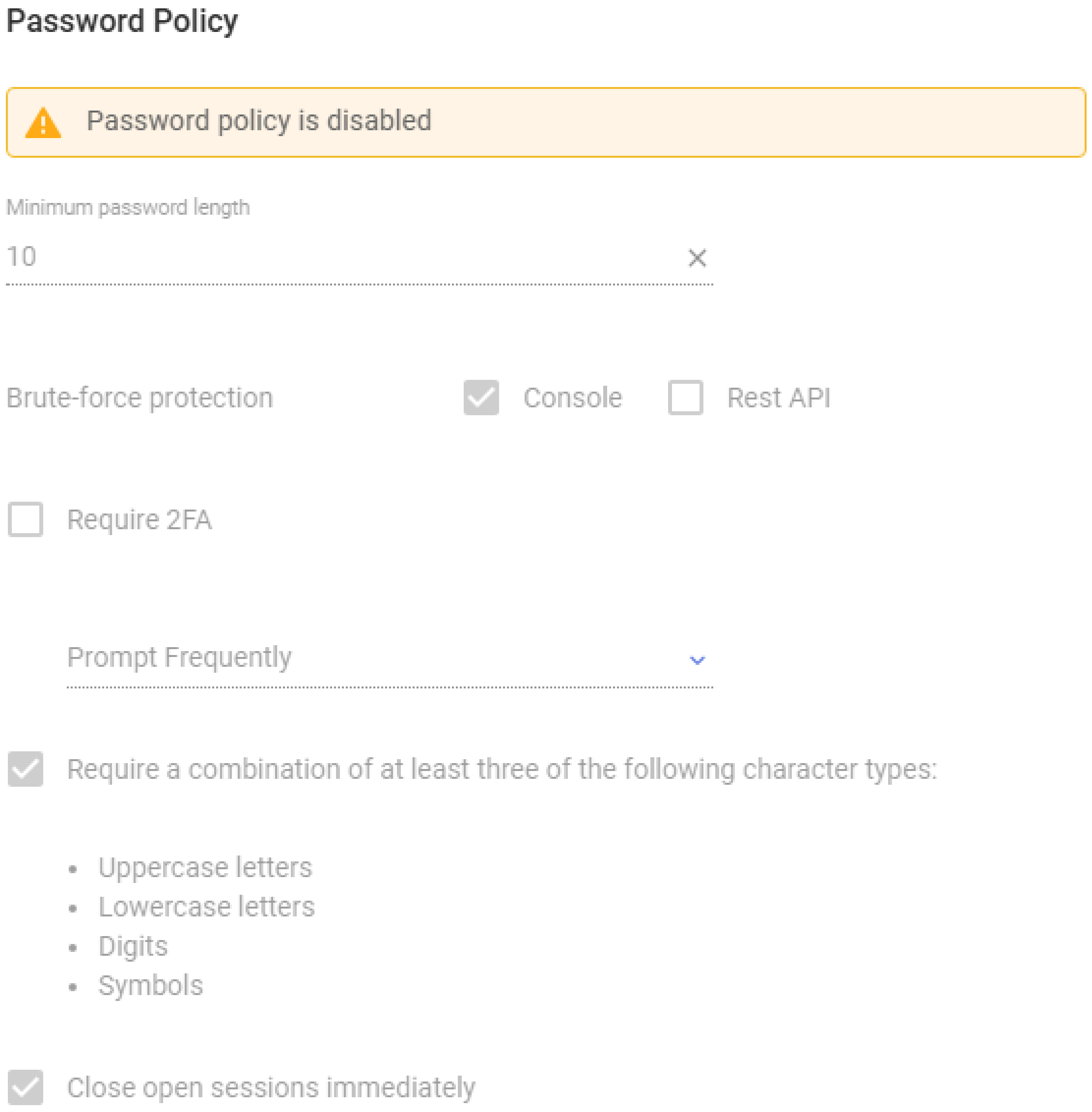
Now you can ask the user to log in using the new password.

Defining a password policy

To enhance security and better secure the access to the FortiEDR system, you can define a password policy to enforce some basic rules that apply to all user passwords, including the default password you create for each user and existing users that are created before the password policy is defined. All existing users with a password that does not comply with the new password policy will be prompted to change the password at their next login.

To define a password policy:

1. Click the *Password Policy* button (Password Policy).
2. Fill in the displayed window. The requirements you define will be applied to all new and existing users.



Password Policy

⚠ Password policy is disabled

Minimum password length

10 ✕

Brute-force protection ☑ Console □ Rest API

□ Require 2FA

Prompt Frequently

☑ Require a combination of at least three of the following character types:

- Uppercase letters
- Lowercase letters
- Digits
- Symbols

☑ Close open sessions immediately

Option	Description
Minimum password length	Specify the minimum number of characters the password must include.

Option	Description
Brute-force protection	Specify whether to block user login after five failed login attempts in the Manager console or Rest API. Blocked users will not be able to log in before an administrator resets the password in the *Administration > Users* tab.
Require 2FA	Require all users to use Two-factor authentication on page 279. You can further configure the 2FA prompt frequency to be one of the following: • *Always*—The user has to re-authenticate for each login. • *Daily*—The user has to re-authenticate every 24 hours. • *Weekly*—The user has to re-authenticate every 7 days. This option enforces 2FA on all users. To require only specific users to use 2FA, leave this option empty and enable the 2FA option for specific users, as described in Users on page 277.
Require a combination of at least three of the following character types	Require all passwords to include at least three of the following character types: • Uppercase letters • Lowercase letters • Digits • Symbols
Close open sessions immediately	Force close any open sessions from users that do not comply with the password policy.

3. Click *Save*.

After you save the password policy, all new users must follow the password policy. Existing users with a password that does not comply with the new password policy will be prompted to change the password at their next login.

LDAP authentication

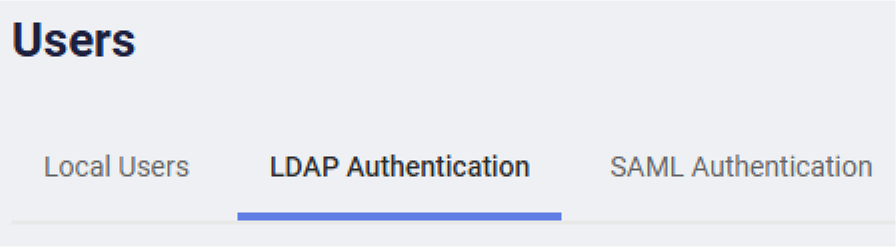
Lightweight Directory Access Protocol (LDAP) authentication is an open, industry-standard application protocol for accessing and maintaining distributed directory information services over an IP network. LDAP provides a central place to store usernames and passwords. This enables many different applications and services to connect to an LDAP server to validate users. This has a major benefit that allows a central place to update and change user passwords.

When LDAP authentication is enabled in FortiEDR, whenever a user attempts to log in to FortiEDR, the system looks for that user name and password in the central directory, instead of within the FortiEDR directory. If the user is not found on the LDAP server, the system checks whether the user is defined locally (under *Administration > Users > Local Users*).

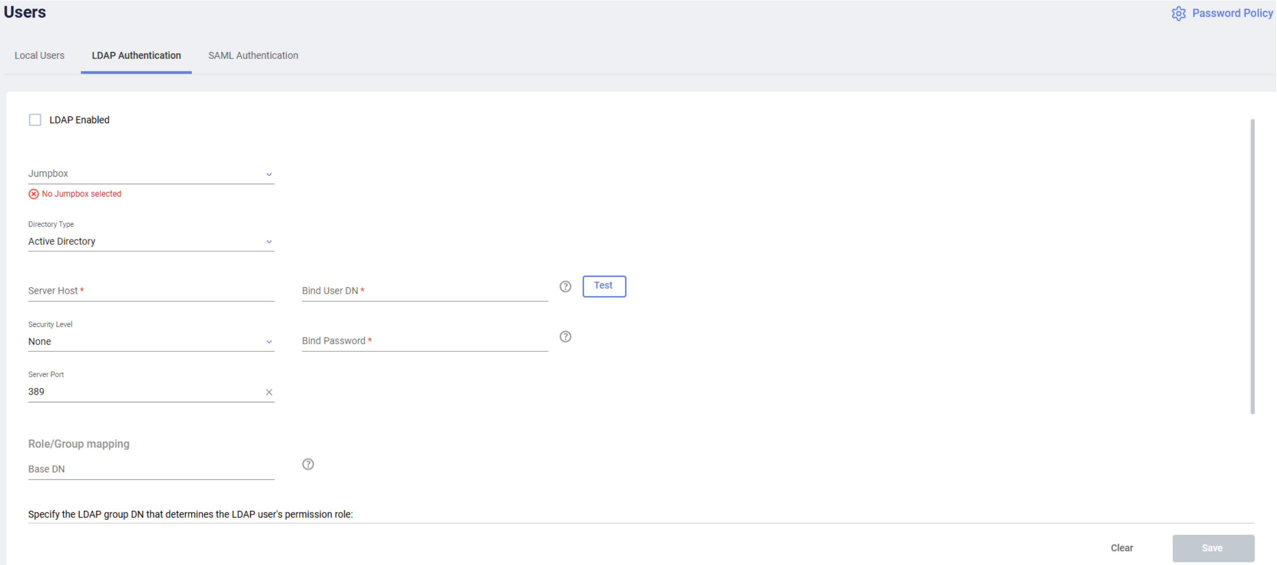
Before you start firewall configuration, make sure that your FortiEDR deployment includes an on-premise Core that has connectivity to the LDAP server. Details about how to install a FortiEDR on-premise Core can be found in Setting up the FortiEDR Core on page 511.

To set up LDAP authentication in FortiEDR:

1. For multi-tenancy environments, in the *Organization* dropdown list at the top left, verify the selected organization is the one that you want to grant the LDAP users access to. To grant the LDAP users access to all organizations, select *Hoster View*.
2. In the Organization dropdown list at the top left, select the organization that you want to grant the user access or select Hoster View if you want to grant the user access to all organizations.
3. Select Admin in the Role list for the group when you configure LDAP or SAML users.
4. Click the *LDAP AUTHENTICATION* tab.



The following page displays:



□ LDAP Enabled

Jumpbox

No Jumpbox selected

Directory Type: Active Directory

Server Host *

Bind User DN *

Security Level: None

Bind Password *

Server Port: 389

Role/Group mapping

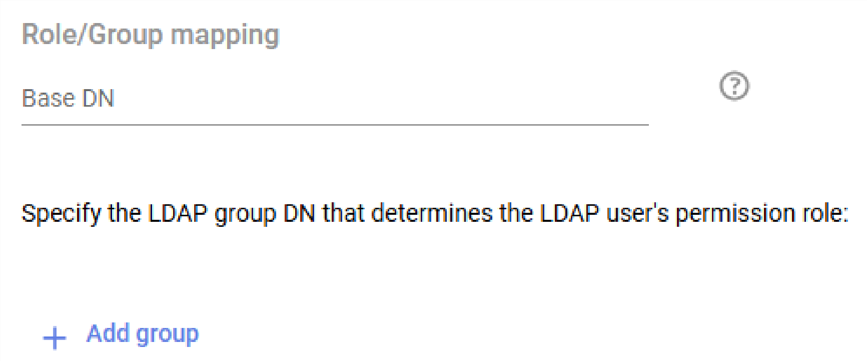
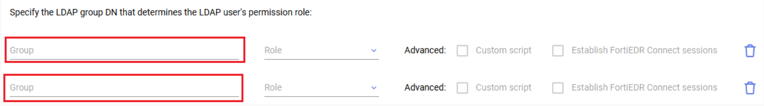
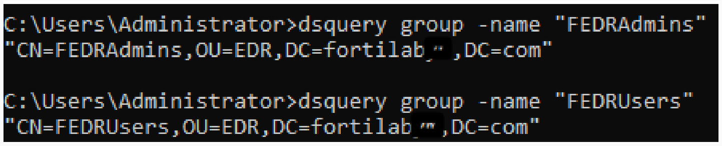
Base DN

Specify the LDAP group DN that determines the LDAP user's permission role:

5. Fill in the following fields:

Field	Definition
LDAP Enabled	Check this checkbox to enable LDAP authentication in FortiEDR.
Jumpbox	Select the FortiEDR Core to communicate with the LDAP server. Only FortiEDR Cores on page 403 configured with Jumpbox functionality appear in the list. If no such core exists in the system, the list is empty and FortiEDR displays a warning message.

Field	Definition
Directory Type	Specify the type of central directory in use. FortiEDR supports Active Directory and OpenLDAP. The default is *Active Directory*.
Server Host	Specify the IP address of your LDAP server.
Security Level	Specify the protocol to be used for the secured connection: *TLS*, *SSL*, or *None*.
Server Port	This value is dependent on the security protocol that was selected.
Bind User DN/Bind Password	Specify the user and password for the authentication of FortiEDR in the Central Directory.

Role/Group mapping	Specify the base DN and define group/role mapping and permissions of the group:
	
	Role/Group mapping
	Base DN
	Specify the LDAP group DN that determines the LDAP user's permission role:
	
	1. In *Base DN*, specify the location in the Central Directory hierarchy where the Groups that are used for permission mapping can be found. For example, the DN for the root of the domain should always work, but results in low performance.
	2. Click *Add group*.
	3. Define group/role mapping and permissions of the group:
	a. In the *Group* field, specify the LDAP group DN as defined in your central directory (Active Directory or OpenLDAP).
	
	Specify the LDAP group DN that determines the LDAP user's permission role:
	Group — Role — Advanced: □ Custom script □ Establish FortiEDR Connect sessions
	Group — Role — Advanced: □ Custom script □ Establish FortiEDR Connect sessions
	To check the LDAP group DN, run `dsquery group -name "`*`Group_Name`*`"` on the Active Directory server.
	
	`C:\Users\Administrator>dsquery group -name "FEDRAdmins"`
	`"CN=FEDRAdmins,OU=EDR,DC=fortilab`[redacted]`,DC=com"`
	
	`C:\Users\Administrator>dsquery group -name "FEDRUsers"`
	`"CN=FEDRUsers,OU=EDR,DC=fortilab`[redacted]`,DC=com"`
	b. Under *Role*, select a role from the list. See Users on page 277 for more information about the roles.
	c. Under *Advanced*, enable any additional privileges for the group. Some options are role-dependent.

Field	Definition
	4. Click *Add group* and repeat step 2 for each role you want to map to a group or multiple groups. **For example**: To give the user John Admin permissions in FortiEDR (for both the FortiEDR application and the custom script), assign John to a FortiEDRUsers group that is defined in your Central Directory: **1.** Under *Group*, specify the LDAP group DN of the FortiEDRUsers group. **2.** Select *Admin* under *Role*. **3.** Check the *Custom script* checkbox under *Advanced*. During authentication, FortiEDR determines the relevant role for the user John by checking that the Central Directory exists and that the password used in the FortiEDR login page matches the password in the Central Directory. If both exist and are correct, FortiEDR then checks the FortiEDRUsers group to which John is assigned and matches the user role permissions.

6. If users must use two-factor authentication to log in, check the *Require two-factor authentication for LDAP logins* checkbox. For more details about two-factor login, see the Two-factor Authentication section in Two-factor authentication on page 279.

Click the *Reset 2FA Token* button to reset the two-factor authentication token for a specific user. This process works in the same way as described in Resetting a user password on page 281.

7. Click *Save*.

Users in Active Directory must not have a backslash (\) in the user name, in order for the name be supported by the FortiEDR Console. In some cases in Active Directory, a backslash is added when there is a space between a user's first and last names. For example, `CN=Yell\,`.

SAML authentication

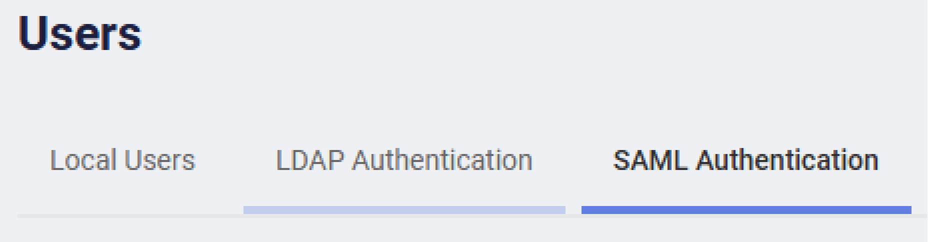
Security Assertion Markup Language (SAML) is an XML-based open standard for exchanging authentication and authorization data between parties, particularly between an identity provider (IdP) and a service provider (SP).

FortiEDR can act as an SP to authenticate users with a third-party IdP, enabling transparent user sign-in to the FortiEDR Central Manager Console.

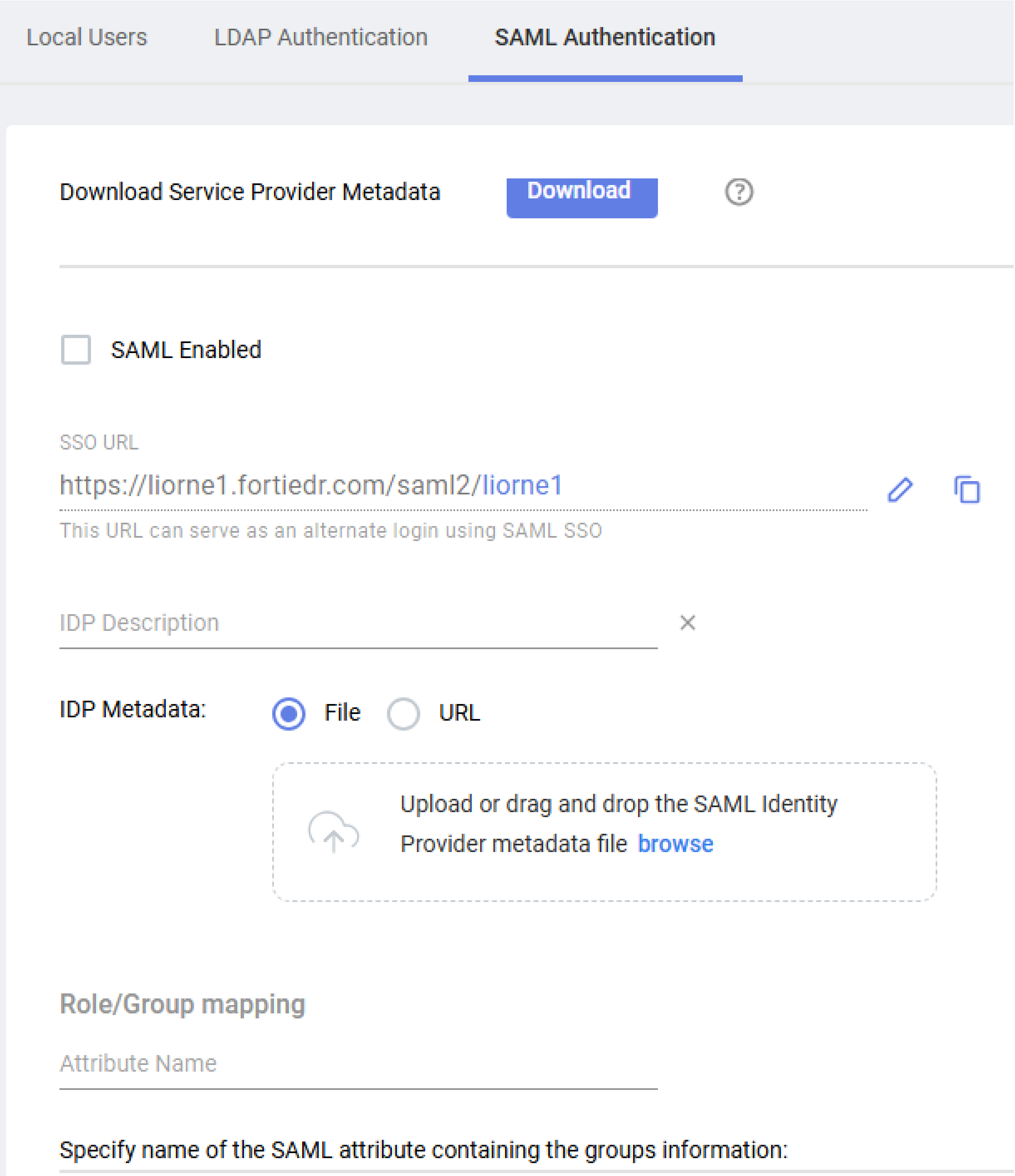
To set up SAML authentication in FortiEDR:

1. For multi-tenancy environments, in the *Organization* dropdown list at the top left, verify the selected organization is the one that you want to grant the SAML users access to. To grant the SAML users access to all organizations, select *Hoster View*.

2. In the *Administration > Users* page, go to the *SAML Authentication* tab.



The following window displays:



Local Users
LDAP Authentication
SAML Authentication
Download Service Provider Metadata
Download
?

□ SAML Enabled

SSO URL
https://liorne1.fortiedr.com/saml2/liorne1
This URL can serve as an alternate login using SAML SSO

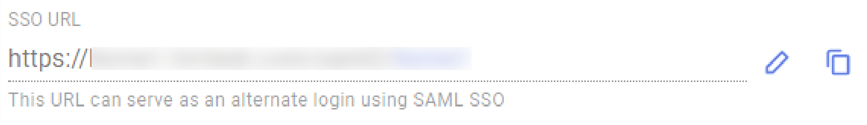
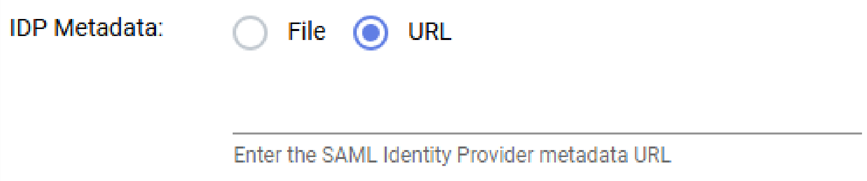
IDP Metadata: ● File ○ URL

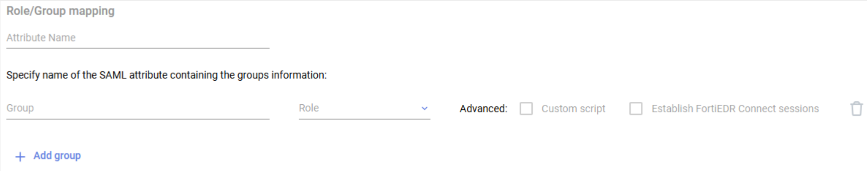
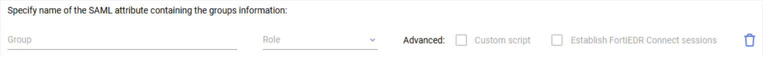
Upload or drag and drop the SAML Identity Provider metadata file browse
Role/Group mapping
Attribute Name
Specify name of the SAML attribute containing the groups information:

3. Click the *Download* button to download and save SP data from FortiEDR, which is used by your IdP server during SAML authentication. Then, upload this FortiEDR data as is to your IdP server using a standard method.
   If your IdP requires manual configuration, you can extract the following fields from the XML file that you downloaded and use them for manual configuration:

Field	Description
Entity ID	Located under the `md:EntityDescriptor` tag, in the `entityID` attribute.
Logout Address Value	Located under the `md:SingleLogoutService` tag, in the `Location` attribute.
Login Address Value	Located under the `md:AssertionConsumerService` tag, in the `Location` attribute.
Certificate Value (Public)	Located under the `ds:X509Certificate` tag.

4. Fill in the following fields:

Field	Definition
SAML Enabled	Check this checkbox to enable SAML authentication in FortiEDR.
SSO URL	Specify the URL to be used by users to log in to FortiEDR. If necessary, you can edit the suffix of this URL (shown in green) by clicking the *Edit* button ✎ and then modifying it as needed. You can also copy the URL to the clipboard using the *Copy* button ⧉ (for example, in order to email the FortiEDR SAML login page to your users).  SSO URL https://l[redacted] This URL can serve as an alternate login using SAML SSO Make sure that the suffix does not include any spaces and is comprised of only letters, numbers and underscores.
IDP Description	Specify a free-text description. For example, you may want to specify the IdP server that you are using here.
IDP Metadata	Upload the IdP metadata to FortiEDR. You can either upload an XML file or a URL. To upload a file, click the *File* radio button and then click the *Select File* button to navigate to and select the applicable *.XML file. To upload a URL, click the *URL* radio button and then specify the requisite URL.  IDP Metadata: ○ File ● URL Enter the SAML Identity Provider metadata URL
Role/Group mapping	Specify the attribute name and define group/role mapping and permissions of the group:

Field	Definition
	 Role/Group mapping Attribute Name Specify name of the SAML attribute containing the groups information: Group Role Advanced: □ Custom script □ Establish FortiEDR Connect sessions + Add group 1. In *Attribute Name*, specify the name of the attribute to be read by FortiEDR, in order to determine the permissions and role to be assigned to that user in FortiEDR. This attribute must be included as part of the response from the identify provider server to FortiEDR when a user attempts to log in to FortiEDR. 2. Click *Add group*. 3. Define group/role mapping and permissions of the group:  Specify name of the SAML attribute containing the groups information: Group Role Advanced: □ Custom script □ Establish FortiEDR Connect sessions a. In the *Group* field, specify an attribute value to be granted FortiEDR permissions. b. Under *Role*, select a role from the list. See Users on page 277 for more information about the roles. c. Under *Advanced*, enable any additional privileges for the group. Some options are role-dependent. 4. Click *Add group* and repeat step 2 for each role you want to map to an attribute value. If more than a single role is mapped to the user, FortiEDR expects to get multiple roles as a list of values and not in bulk in the SAML assertion that is sent by IdP.

5. Click *Save*.

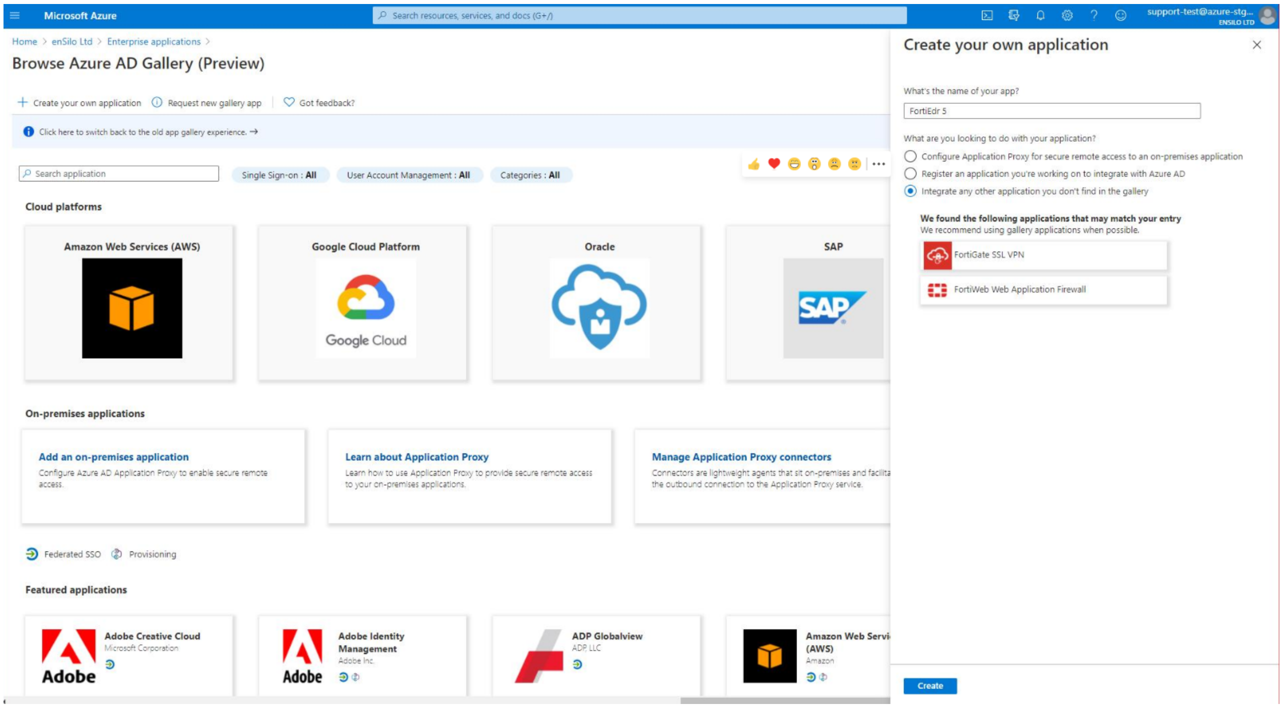
The examples below describe how the Azure, Okta or FortiAuthenticator SSO services can be used as an IdP that provides authorization and authentication for users attempting to access the FortiEDR Central Manager console. It demonstrates how to exchange metadata between the two entities, how to define group attributes and how to associate them with SAML users so that user permissions are dictated by the Group/Roles mapping in FortiEDR SAML configuration.

SAML IdP configuration with Azure

Azure may require a license to support SAML integration with their Enterprise Application. Contact Microsoft's support for further information.

To configure general SAML IdP portal settings:

1. Before you start configuring SAML on Azure, download and save SP data from the FortiEDR SAML configuration page (`fortiEDR.sp.metedata.id.1.xml`), as described in SAML authentication on page 287.
2. Sign in to the Azure Dashboard.
3. In the Azure services, select and navigate to the Azure Active Directory.
4. From the left menu, select *Enterprise applications*.
5. Click *New Application* and then *Create your own application*.
6. In the window that appears, leave the default and click *Create*.


Microsoft Azure
Search resources, services, and docs (G+/)
support-test@azure-stg...
ENSILO LTD
Home > enSilo Ltd > Enterprise applications >
Browse Azure AD Gallery (Preview)
+ Create your own application
Request new gallery app
Got feedback?
Click here to switch back to the old app gallery experience. →
Search application
Single Sign-on : All
User Account Management : All
Categories : All
Cloud platforms
Amazon Web Services (AWS)
Google Cloud Platform
Google Cloud
Oracle
SAP
On-premises applications
Add an on-premises application
Configure Azure AD Application Proxy to enable secure remote access.
Learn about Application Proxy
Learn how to use Application Proxy to provide secure remote access to your on-premises applications.
Manage Application Proxy connectors
Connectors are lightweight agents that sit on-premises and facilita the outbound connection to the Application Proxy service.
Federated SSO
Provisioning
Featured applications
Adobe Creative Cloud
Microsoft Corporation
Adobe
Adobe Identity Management
Adobe Inc.
Adobe
ADP Globalview
ADP, LLC
Amazon Web Servi (AWS)
Amazon

Create your own application

What's the name of your app?

FortiEdr 5

What are you looking to do with your application?

○ Configure Application Proxy for secure remote access to an on-premises application

○ Register an application you're working on to integrate with Azure AD

● Integrate any other application you don't find in the gallery

We found the following applications that may match your entry
We recommend using gallery applications when possible.

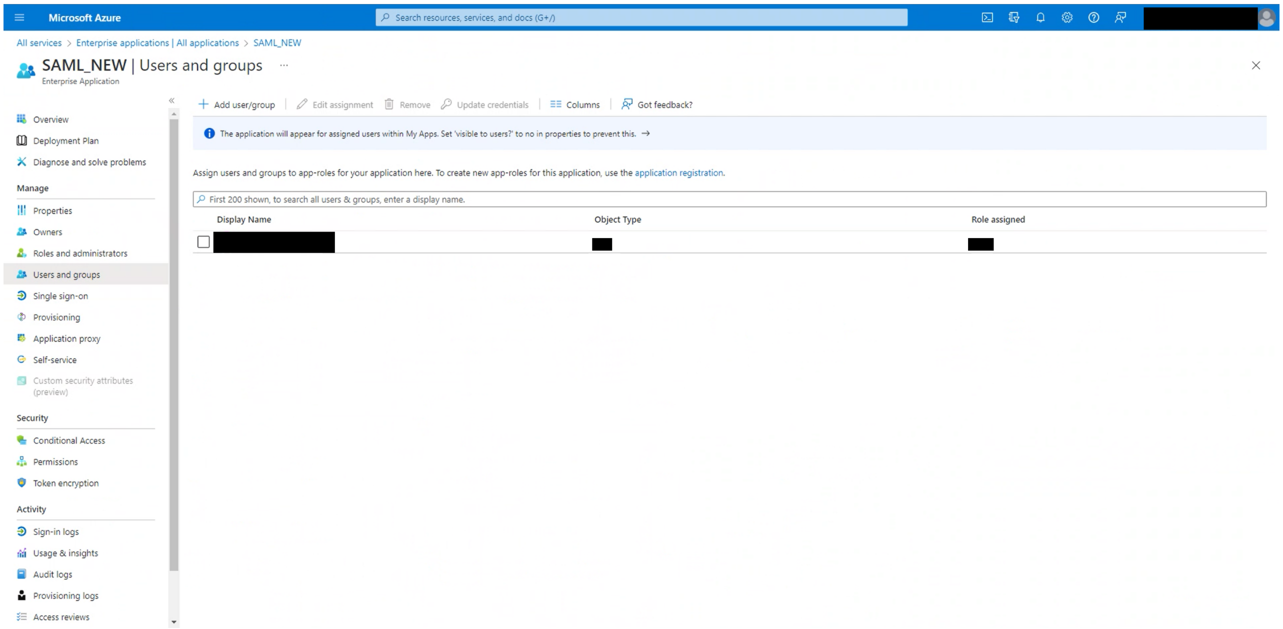
FortiGate SSL VPN

FortiWeb Web Application Firewall

Create

7. Click *Assign users and groups* to configure the users and groups to grant access to the FortiEDR application.
8. Select *Users and groups* and then *+ Add user/group* to create a new user group.

9. Add users to the group so that they will be eligible to authenticate with FortiEDR Manager.



The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. →

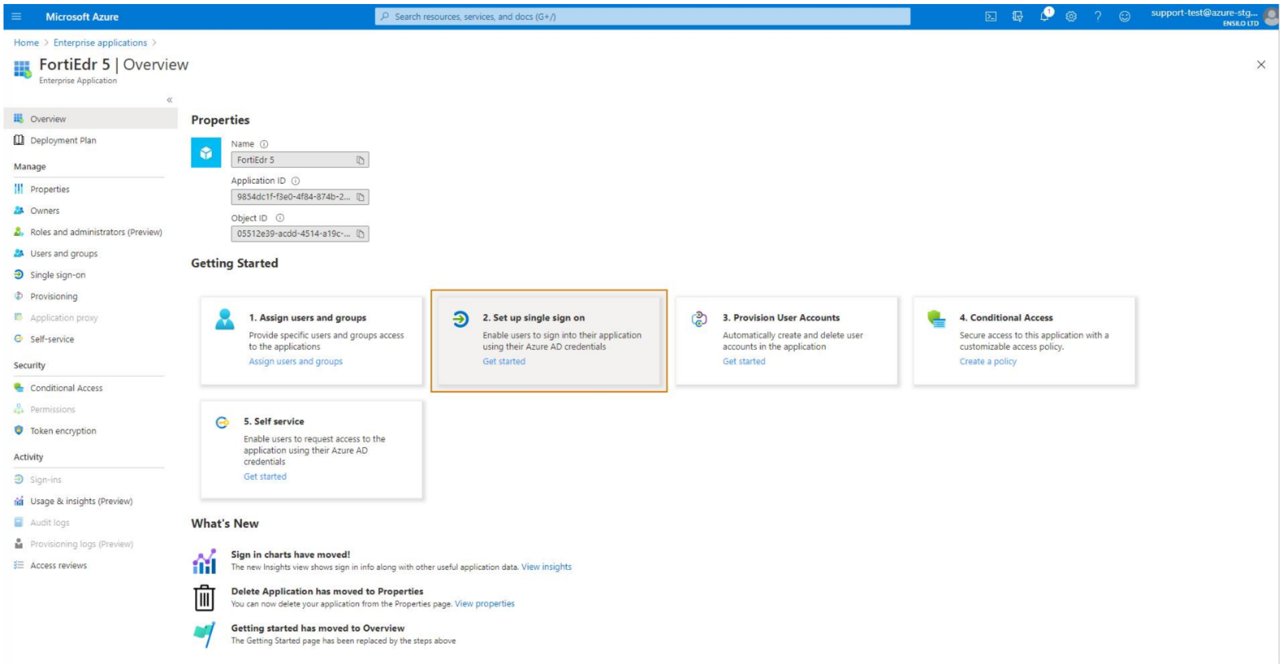
Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the application registration.

First 200 shown, to search all users & groups, enter a display name.

Display Name	Object Type	Role assigned
□ [redacted]	[redacted]	[redacted]

10. Go to the groups properties and note down the object Id which will be used in later steps.

11. Click *Set up single sign on*.



Properties

Name: FortiEdr 5

Application ID: 9854dc1f-f3e0-4f84-874b-2...

Object ID: 05512e39-acdd-4514-a19c-...

Getting Started

1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

2. Set up single sign on
Enable users to sign into their application using their Azure AD credentials
Get started

3. Provision User Accounts
Automatically create and delete user accounts in the application
Get started

4. Conditional Access
Secure access to this application with a customizable access policy.
Create a policy

5. Self service
Enable users to request access to the application using their Azure AD credentials
Get started

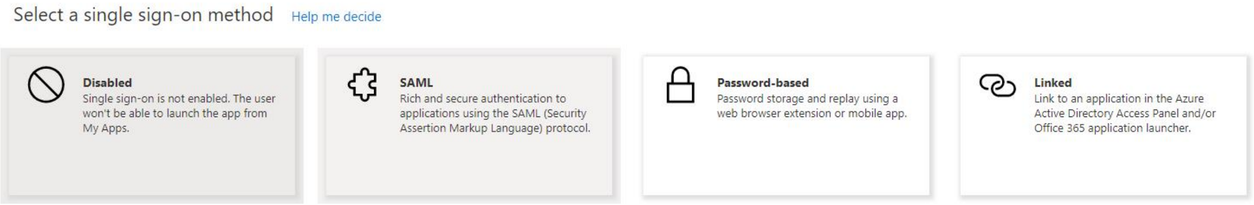
What's New

Sign in charts have moved!
The new Insights view shows sign in info along with other useful application data. View insights

Delete Application has moved to Properties
You can now delete your application from the Properties page. View properties

Getting started has moved to Overview
The Getting Started page has been replaced by the steps above

12. When prompted to select a single sign-on method, select *SAML*.


Select a single sign-on method Help me decide

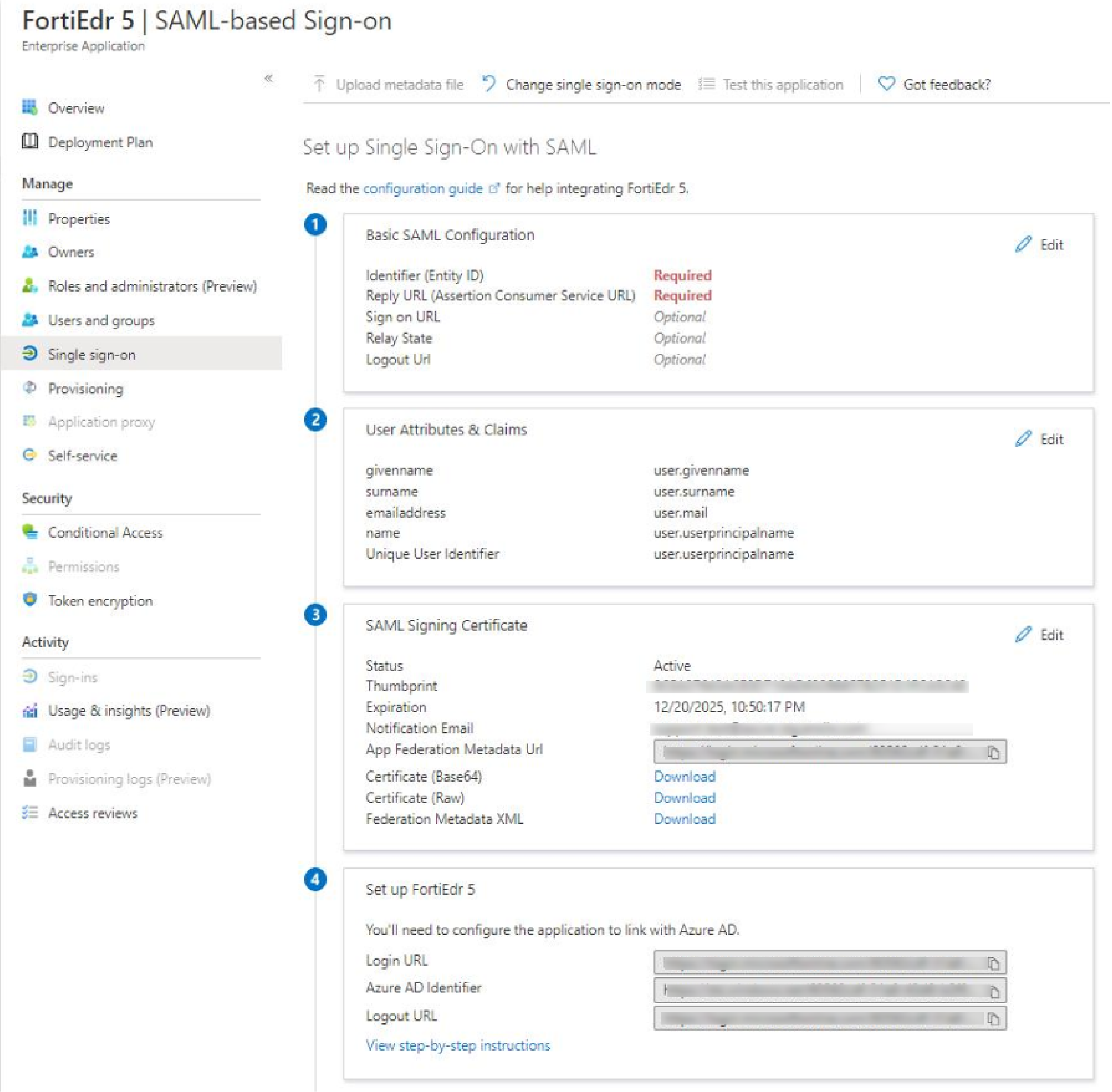
Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Password-based
Password storage and replay using a web browser extension or mobile app.

Linked
Link to an application in the Azure Active Directory Access Panel and/or Office 365 application launcher.

13. Click *Edit* in the *Basic SAML Configuration* box.



FortiEdr 5 | SAML-based Sign-on
Enterprise Application

Set up Single Sign-On with SAML

Read the configuration guide for help integrating FortiEdr 5.

1 Basic SAML Configuration — Edit

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Optional
Relay State	Optional
Logout Url	Optional

2 User Attributes & Claims — Edit

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

3 SAML Signing Certificate — Edit

Status	Active
Thumbprint	[redacted]
Expiration	12/20/2025, 10:50:17 PM
Notification Email	[redacted]
App Federation Metadata Url	[redacted]
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

4 Set up FortiEdr 5

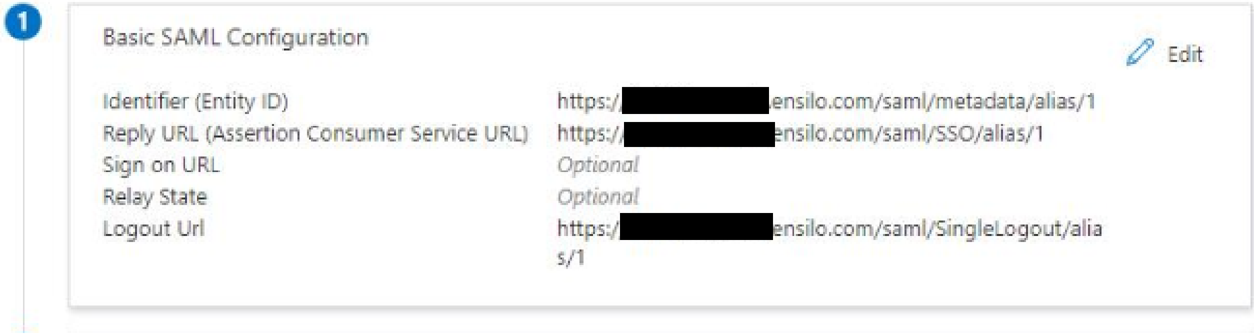
You'll need to configure the application to link with Azure AD.

Login URL	[redacted]
Azure AD Identifier	[redacted]
Logout URL	[redacted]

View step-by-step instructions

14. Click *Upload metadata file* and browse to select the FortiEDR SP metadata file (`fortiEDR.sp.metedata.id.1.xml`) that was downloaded from FortiEDR SAML configuration page during SAML authentication on page 287. Alternatively, you can manually copy the entityID and the Reply URL values from FortiEDR metadata file and paste them to the relevant input text boxes.

15. Click *Save*. The required SAML configuration fields displays populated with details, as shown below:

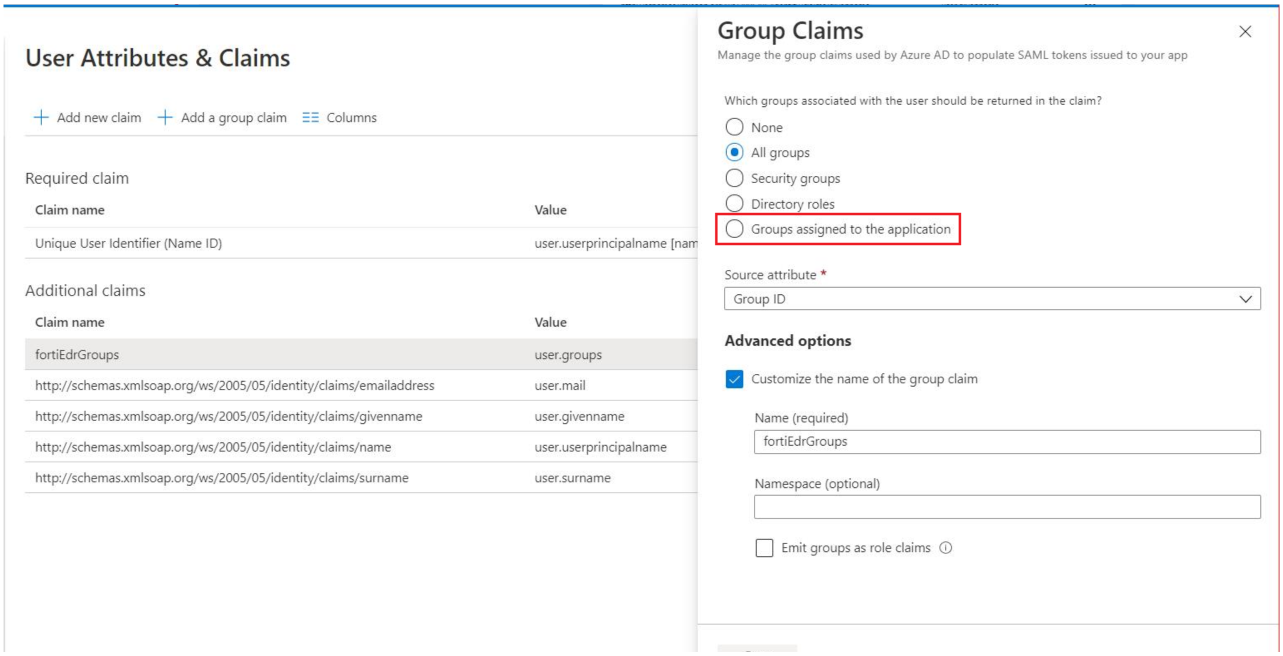


Basic SAML Configuration

Identifier (Entity ID)	https:/[redacted]ensilo.com/saml/metadata/alias/1
Reply URL (Assertion Consumer Service URL)	https:/[redacted]ensilo.com/saml/SSO/alias/1
Sign on URL	*Optional*
Relay State	*Optional*
Logout Url	https:/[redacted]ensilo.com/saml/SingleLogout/alias/1

16. Click *Edit* in the *Attributes & Claims* box.
17. In the *Attributes & Claims* window, click *Add a group claim*.
18. In the *Group Claims* window, select *Groups assigned to the application* to include groups assigned to the FortiEDR application in the token.

These specific groups should be specified in the Role/Group mapping on the SAML configuration page of the FortiEDR console in order to determine the permissions of the signed in user.



User Attributes & Claims

Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nam

Additional claims

Claim name	Value
fortiEdrGroups	user.groups
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname

Group Claims

Manage the group claims used by Azure AD to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

○ None
● All groups
○ Security groups
○ Directory roles
○ Groups assigned to the application

Source attribute *: Group ID

Advanced options

☑ Customize the name of the group claim

Name (required): fortiEdrGroups

Namespace (optional):

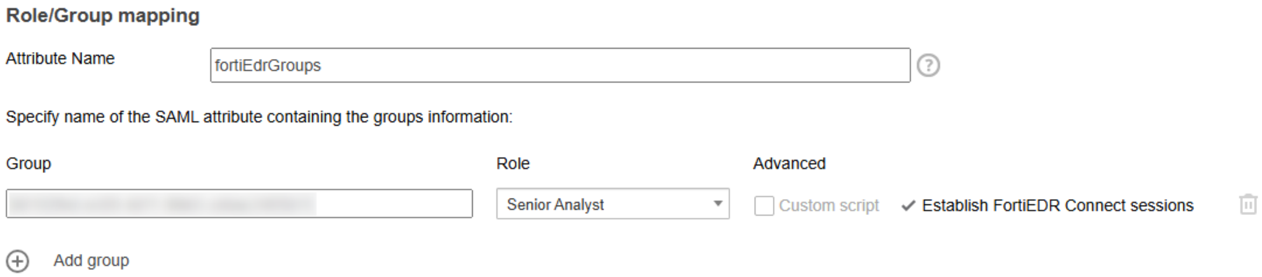
□ Emit groups as role claims

FortiEDR does not currently support consuming group overage (group.links) claim resolution or nested group resolution.

19. Select the *Customize the name of the group claim* checkbox.

Note down the Azure "name of the group claim", which you will need to specify as *Attribute Name* when configuring SAML in FortiEDR later.

20. In the FortiEDR Central Manager console, in the *Attribute Name* field, enter the attribute name that was specified on the SAML configuration page of the FortiEDR console during SAML authentication on page 287. In our example, it is *fortiEdrGroups*, as shown below. The *Group* should be the *Azure Group object Id* noted earlier in step 10.



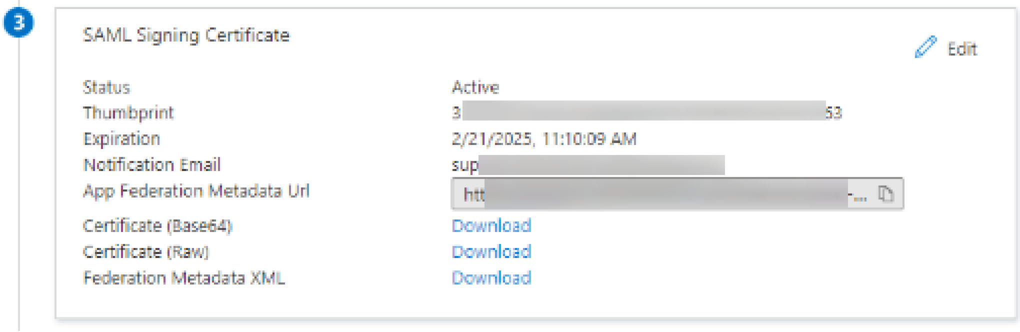
Role/Group mapping

Attribute Name: fortiEdrGroups

Specify name of the SAML attribute containing the groups information:

Group	Role	Advanced
[redacted]	Senior Analyst	□ Custom script ✓ Establish FortiEDR Connect sessions

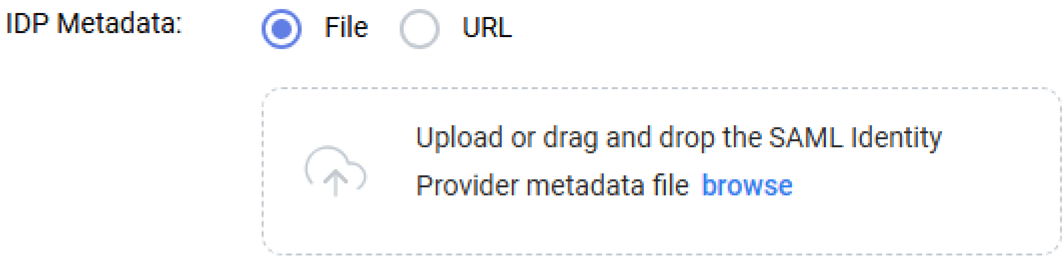
21. Click *Save*.
22. Download the Federation Metadata XML file from the *SAML Signing Certificate* section on Azure, as shown below:



SAML Signing Certificate

Status	Active
Thumbprint	3[redacted]53
Expiration	2/21/2025, 11:10:09 AM
Notification Email	sup[redacted]
App Federation Metadata Url	htt[redacted]
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

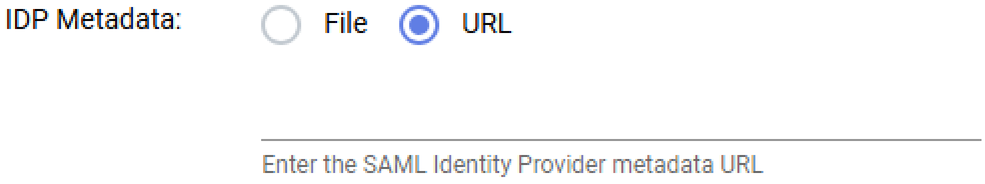
23. Inspect the SAML assertion using SAML Tracer or Azure Token View to verify claim emission.
24. Select and upload the XML file into the FortiEDR Central Manager, as follows:



IDP Metadata: ● File ○ URL

Upload or drag and drop the SAML Identity Provider metadata file browse

Alternatively, you can use the App Federation Metadata URL from Azure, select the *URL* radio button in the IDP Metadata configuration on the FortiEDR console and paste it to the same location:



IDP Metadata: ○ File ● URL

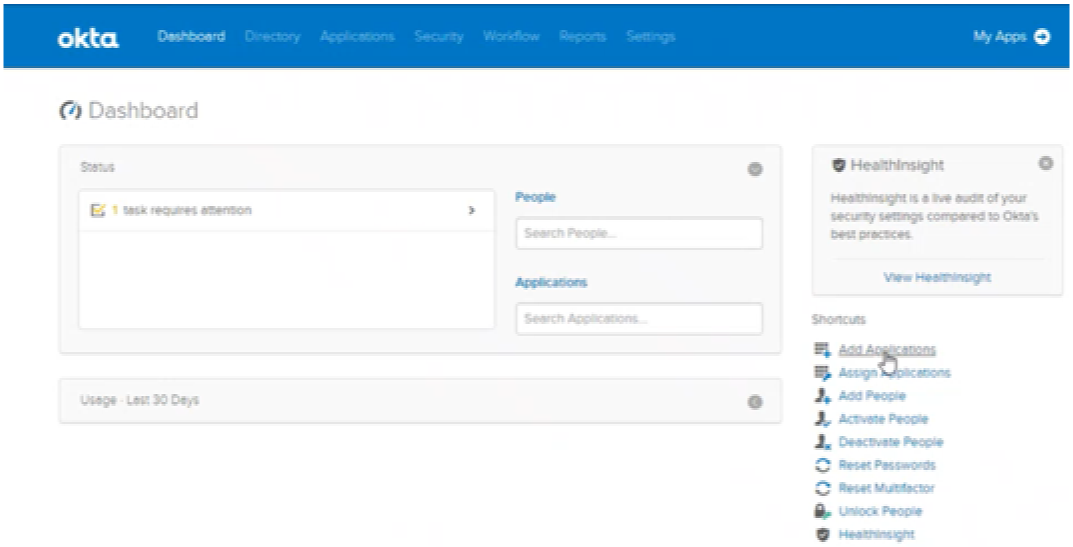
Enter the SAML Identity Provider metadata URL

Azure can now be used as an IdP that awards authorization and authentication to users trying to access the FortiEDR Central Manager console. When logging into the FortiEDR console via an SSO URL that is specified under the SAML settings page, an Azure user is awarded access rights to the FortiEDR Central Manager according to the User Groups to which that user was added in Azure.

SAML IdP configuration with Okta

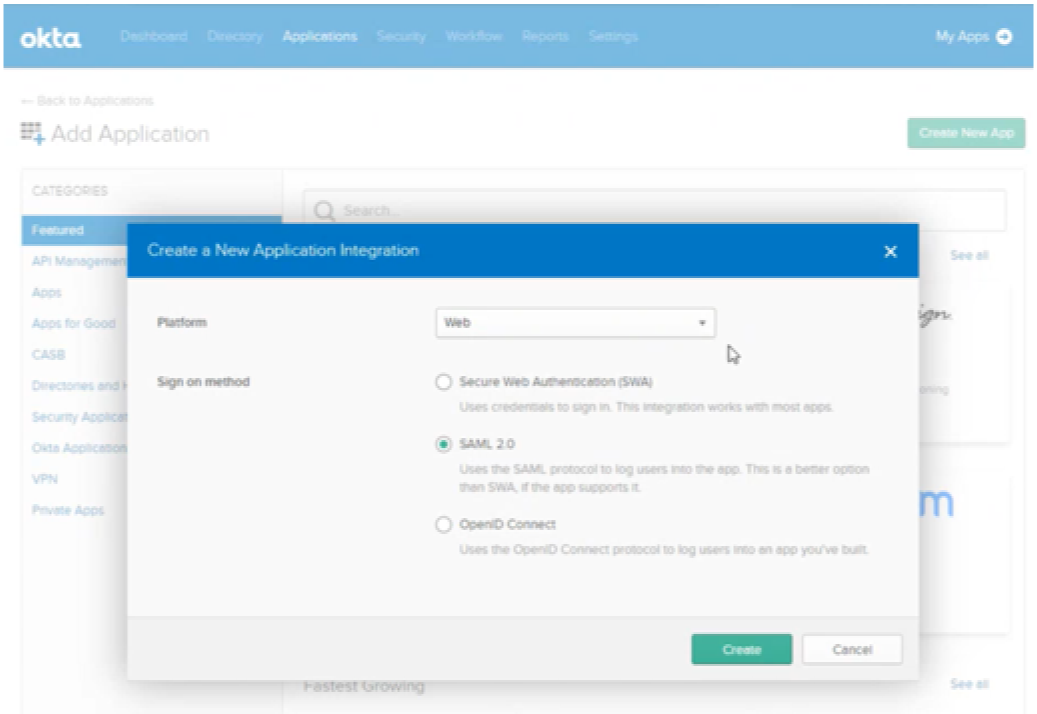
To configure general SAML IdP portal settings:

1. Before starting to configure SAML on Okta, you must download and save SP data from the FortiEDR SAML configuration page (`fortiEDR.sp.metedata.id.1.xml`), as described in SAML authentication on page 287
2. Sign in to the Okta Admin dashboard. The following displays:



HealthInsight is a live audit of your security settings compared to Okta's best practices.

3. In your Okta org, click *Applications* and then *Add Applications*.
4. Click *Create New App* . The following displays:



Platform: Web

Sign on method:

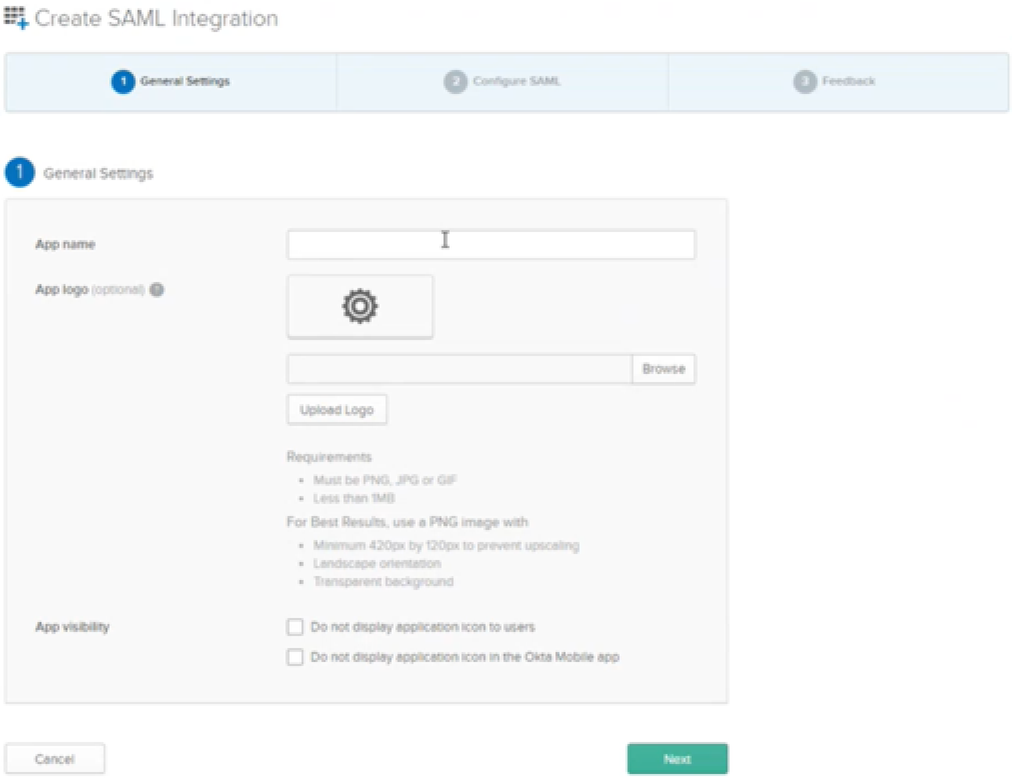
○ Secure Web Authentication (SWA)
Uses credentials to sign in. This integration works with most apps.

● SAML 2.0
Uses the SAML protocol to log users into the app. This is a better option than SWA, if the app supports it.

○ OpenID Connect
Uses the OpenID Connect protocol to log users into an app you've built.

5. In the *Platform* field, select *Web*.

6. In the *Sign on method* field, select *SAML 2.0*.
7. Click *Create*.
8. In the *General Settings* page, select a name for the application. For example, FortiEDRConsole. Optionally, you can also add the FortiEDR logo here.



App name

App logo (optional)

Requirements

- Must be PNG, JPG or GIF
- Less than 1MB

For Best Results, use a PNG image with

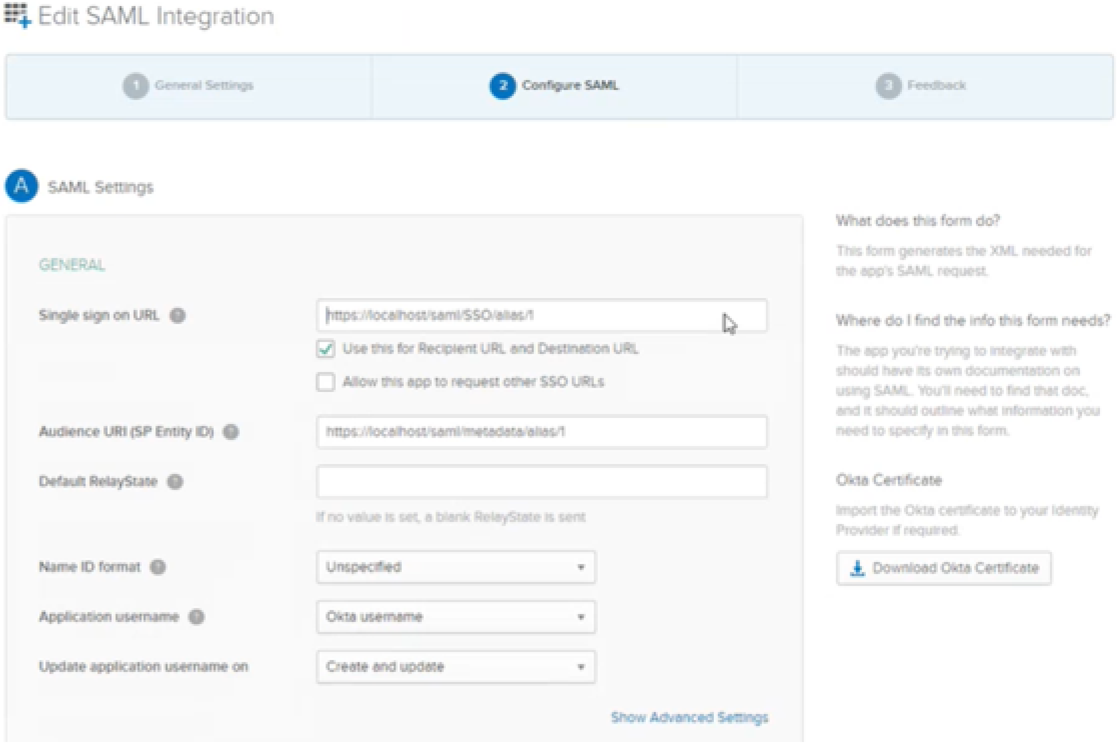
- Minimum 420px by 120px to prevent upscaling
- Landscape orientation
- Transparent background

App visibility

□ Do not display application icon to users

□ Do not display application icon in the Okta Mobile app

9. Click *Next*. The Configure SAML page displays:



Edit SAML Integration

A SAML Settings

GENERAL

Single sign on URL: https://localhost/saml/SSO/alias/1

☑ Use this for Recipient URL and Destination URL

☐ Allow this app to request other SSO URLs

Audience URI (SP Entity ID): https://localhost/saml/metadata/alias/1

Default RelayState:

If no value is set, a blank RelayState is sent

Name ID format: Unspecified

Application username: Okta username

Update application username on: Create and update

What does this form do?

This form generates the XML needed for the app's SAML request.

Where do I find the info this form needs?

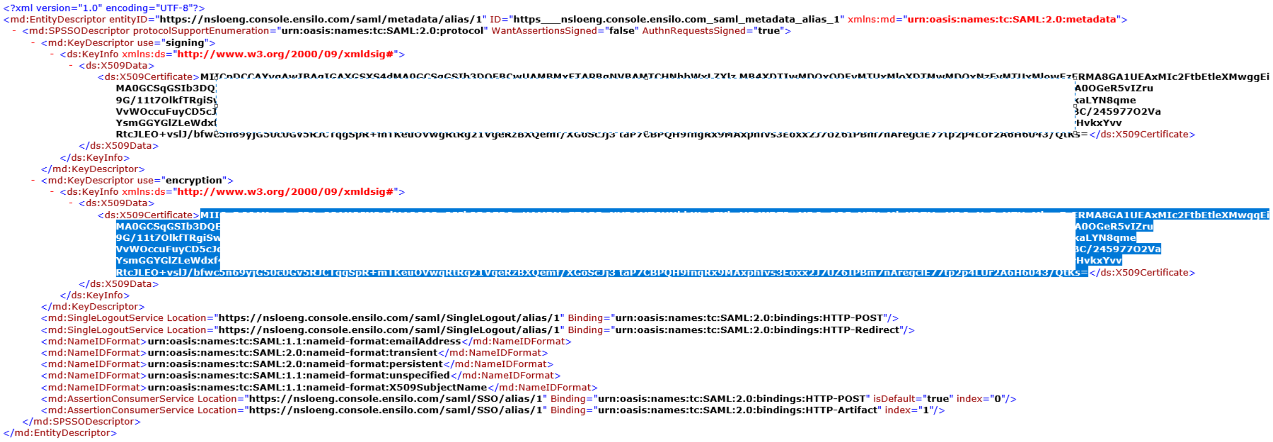
The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

Okta Certificate

Import the Okta certificate to your Identity Provider if required.

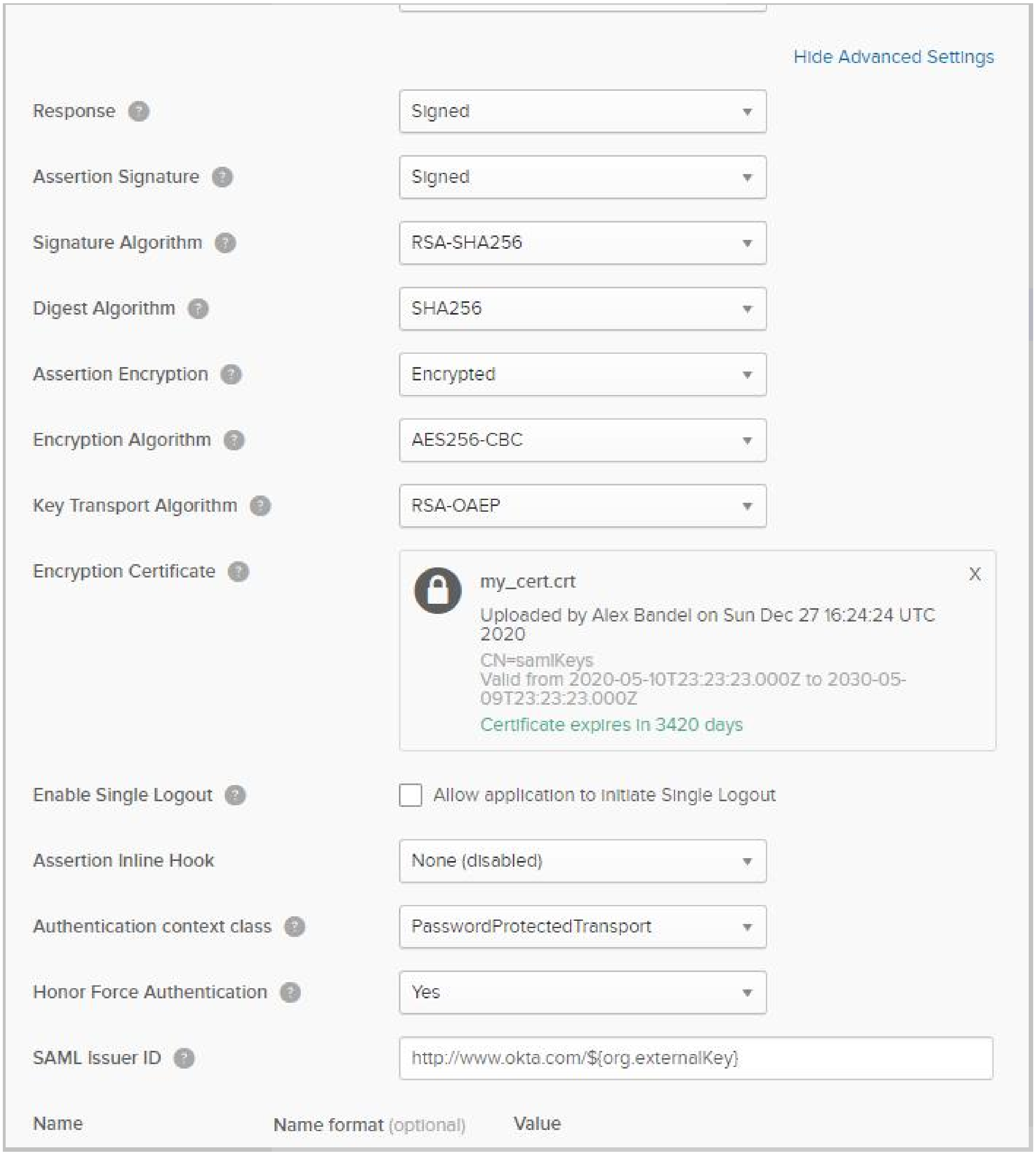
10. Copy the following values that are taken from the FortiEDR SP metadata file (`fortiEDR.sp.metedata.id.1.xml`) that was downloaded from FortiEDR SAML configuration page, as described in SAML authentication on page 287.
    - *Single sign on URL*: Under the `md:AssertionConsumerService` tag, in the *Location* attribute (For example, `https://myexample.fortiedr.com/saml/SSO/alias/1`).
    - *Audience URI (SP entity ID)*: Under the `md:EntityDescriptor` tag, in the `entityID` attribute (For example, `https://myexample.fortiedr.com/saml/metadata/alias/1`).
11. In *Advanced Settings*, in the *Assertion Encryption* field, select *Encrypted*.
12. Use Notepad or another text editor to copy the entire attribute `<ds:X509Certificate>XXX </ds:X509Certificate>` from the FortiEDR SP metadata file (`fortiEDR.sp.metedata.id.1.xml`) that was downloaded from FortiEDR SAML configuration page. Then, save this attribute as a `.crt` file to be used as a certificate.

13. Upload this `.crt` file to the Encryption Certificate box on Okta, as shown below:



```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor entityID="https://nsloeng.console.ensilo.com/saml/metadata/alias/1" ID="https___nsloeng.console.ensilo.com_saml_metadata_alias_1" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
 - <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="false" AuthnRequestsSigned="true">
   - <md:KeyDescriptor use="signing">
     - <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
       - <ds:X509Data>
           <ds:X509Certificate>MI[redacted]ERMA8GA1UEAxMIc2FtbEtleXMwggEi
             MA0GCSqGSIb3DQ                                         A0OGeR5vIZru
             9G/11t7OlkfTRgiS                                       xaLYN8qme
             VvWOccuFuyCD5cJ                                        3C/24597702Va
             YsmGGYGlZLeWdx                                         HvkxYvv
             RtcJLEO+vslJ/bfw                                       s=</ds:X509Certificate>
         </ds:X509Data>
       </ds:KeyInfo>
     </md:KeyDescriptor>
   - <md:KeyDescriptor use="encryption">
     - <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
       - <ds:X509Data>
           <ds:X509Certificate>MII[redacted]ERMA8GA1UEAxMIc2FtbEtleXMwggEi
             MA0GCSqGSIb3DQE                                        A0OGeR5vIZru
             9G/11t7OlkfTRgiSw                                      xaLYN8qme
             VvWOccuFuyCD5cJc                                       3C/24597702Va
             YsmGGYGlZLeWdxf                                        HvkxYvv
             RtcJLEO+vslJ/bfw                                       s=</ds:X509Certificate>
         </ds:X509Data>
       </ds:KeyInfo>
     </md:KeyDescriptor>
     <md:SingleLogoutService Location="https://nsloeng.console.ensilo.com/saml/SingleLogout/alias/1" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
     <md:SingleLogoutService Location="https://nsloeng.console.ensilo.com/saml/SingleLogout/alias/1" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"/>
     <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
     <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
     <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat>
     <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>
     <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName</md:NameIDFormat>
     <md:AssertionConsumerService Location="https://nsloeng.console.ensilo.com/saml/SSO/alias/1" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" isDefault="true" index="0"/>
     <md:AssertionConsumerService Location="https://nsloeng.console.ensilo.com/saml/SSO/alias/1" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" index="1"/>
   </md:SPSSODescriptor>
</md:EntityDescriptor>
```

14. Leave the default values in the rest of the settings. For example, as shown below:

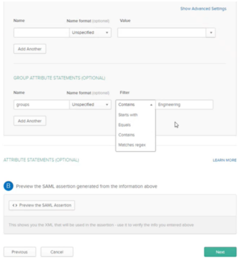


Hide Advanced Settings

Response	Signed
Assertion Signature	Signed
Signature Algorithm	RSA-SHA256
Digest Algorithm	SHA256
Assertion Encryption	Encrypted
Encryption Algorithm	AES256-CBC
Key Transport Algorithm	RSA-OAEP
Encryption Certificate	my_cert.crt Uploaded by Alex Bandel on Sun Dec 27 16:24:24 UTC 2020 CN=samlKeys Valid from 2020-05-10T23:23:23.000Z to 2030-05-09T23:23:23.000Z Certificate expires in 3420 days
Enable Single Logout	□ Allow application to initiate Single Logout
Assertion Inline Hook	None (disabled)
Authentication context class	PasswordProtectedTransport
Honor Force Authentication	Yes
SAML Issuer ID	http://www.okta.com/${org.externalKey}

Name | Name format (optional) | Value

15. Groups will be used in the assertion so that FortiEDR roles will be assigned according to the current groups in the Okta directory. For example, to assign the *Okta Engineering* group to have Admin roles on FortiEDR, add it to Okta as follows:



Name	Name format (optional)	Value
	Unspecified	

GROUP ATTRIBUTE STATEMENTS (OPTIONAL)

Name	Name format (optional)	Filter	
groups	Unspecified	Contains	Engineering

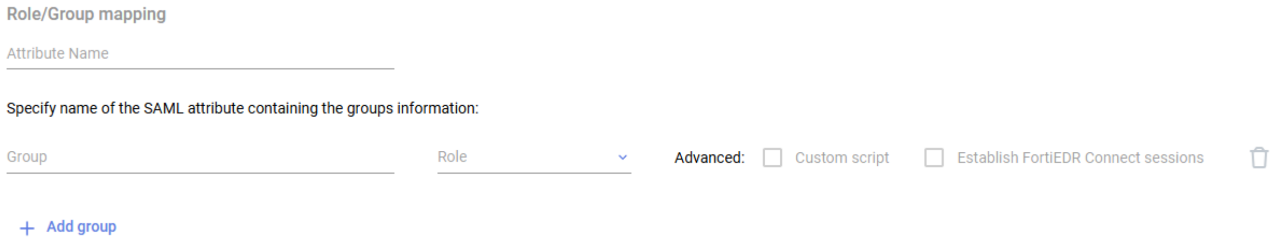
Starts with
Equals
Contains
Matches regex

ATTRIBUTE STATEMENTS (OPTIONAL)

B Preview the SAML assertion generated from the information above

This shows you the XML that will be used in the assertion - use it to verify the info you entered above

The mapping of this group to the FortiEDR Admin role is then performed in the SAML settings page of the FortiEDR Central Manager console as follows:


Role/Group mapping

Attribute Name

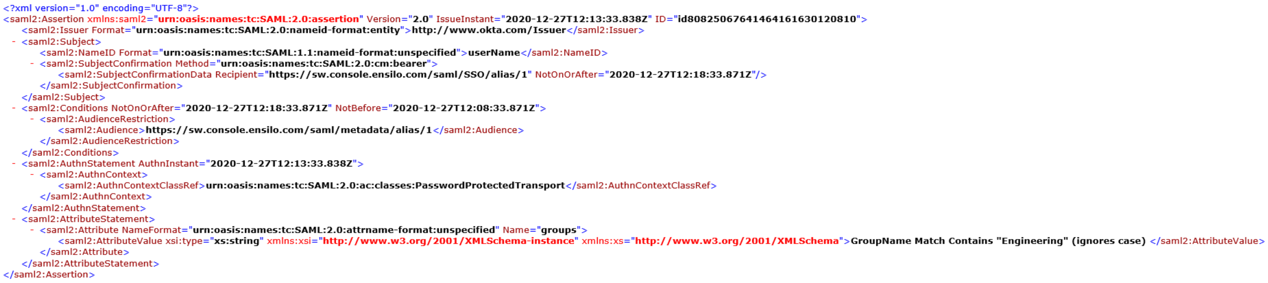
Specify name of the SAML attribute containing the groups information:

Group

Role

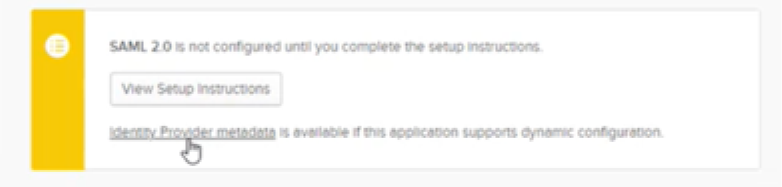
Advanced: □ Custom script □ Establish FortiEDR Connect sessions

16. Previewing the assertion should appear similar to the following example:



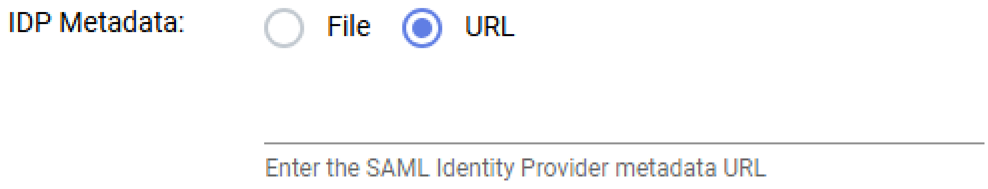
```
<?xml version="1.0" encoding="UTF-8"?>
<saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" Version="2.0" IssueInstant="2020-12-27T12:13:33.838Z" ID="id808250676414641616301208 10">
   <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">http://www.okta.com/Issuer</saml2:Issuer>
 - <saml2:Subject>
      <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">userName</saml2:NameID>
    - <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
         <saml2:SubjectConfirmationData Recipient="https://sw.console.ensilo.com/saml/SSO/alias/1" NotOnOrAfter="2020-12-27T12:18:33.871Z"/>
      </saml2:SubjectConfirmation>
   </saml2:Subject>
 - <saml2:Conditions NotOnOrAfter="2020-12-27T12:18:33.871Z" NotBefore="2020-12-27T12:08:33.871Z">
    - <saml2:AudienceRestriction>
         <saml2:Audience>https://sw.console.ensilo.com/saml/metadata/alias/1</saml2:Audience>
      </saml2:AudienceRestriction>
   </saml2:Conditions>
 - <saml2:AuthnStatement AuthnInstant="2020-12-27T12:13:33.838Z">
    - <saml2:AuthnContext>
         <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml2:AuthnContextClassRef>
      </saml2:AuthnContext>
   </saml2:AuthnStatement>
 - <saml2:AttributeStatement>
    - <saml2:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified" Name="groups">
         <saml2:AttributeValue xsi:type="xs:string" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xs="http://www.w3.org/2001/XMLSchema">GroupName Match Contains "Engineering" (ignores case) </saml2:AttributeValue>
      </saml2:Attribute>
   </saml2:AttributeStatement>
</saml2:Assertion>
```

17. Click *Next* and then click *Finish*.
18. When you configure SAML SSO on the FortiEDR console, use the URL for *Identity Provide Metadata* from the application Sign On settings in Okta, as shown below:


SAML 2.0 is not configured until you complete the setup instructions.

Identity Provider metadata is available if this application supports dynamic configuration.

19. Paste it into the FortiEDR Central Manager as follows:


IDP Metadata: ○ File ● URL

Enter the SAML Identity Provider metadata URL

Okta can now be used as an IdP that awards authorization and authentication to users trying to access the FortiEDR Central Manager console. When logging into FortiEDR console via the SSO URL that is specified under the SAML settings page, an Okta user is awarded access rights to the FortiEDR Central Manager according to the User Groups to which that user was added in Okta.

SAML IdP Configuration with FortiAuthenticator

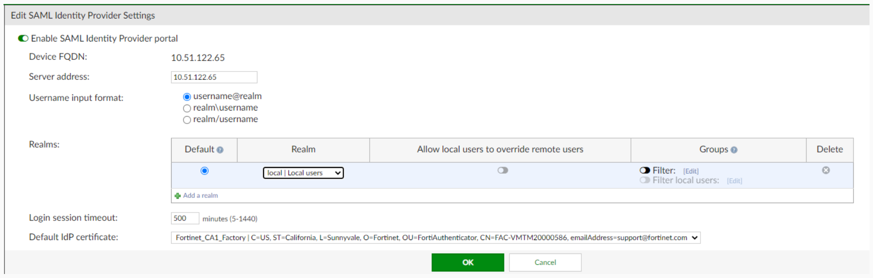
FortiAuthenticator configuration is comprised of the following steps:

1. Setting up FortiAuthenticator as an IdP on page 303
2. Setting up user group management on page 303 (if not configured already)
3. Setting up service provider for FortiEDR on page 305

Setting up FortiAuthenticator as an IdP

To configure general SAML IdP portal settings:

1. Go to *Authentication > SAML IdP > General* and select *Enable SAML Identity Provider portal*.
2. Configure the following settings:

Setting	Definition
Device FQDN	To configure this setting, you must enter a Device FQDN in the System Information widget in the Dashboard.
Server address	Enter the IP address or FQDN of the FortiAuthenticator device.
Username input format	Select one of the provided options. In our example, we used *username@realm*.
Realms	Select *Add a realm* to add the default local realm to which the users will be associated.
Login session timeout	Set the user's login session timeout limit to between 5 – 1440 minutes (one day). In our example, we used `500 minutes`.
Default IdP certificate	Select a default certificate the IdP uses to sign SAML assertions from the dropdown menu.  Edit SAML Identity Provider Settings Enable SAML Identity Provider portal Device FQDN: 10.51.122.65 Server address: 10.51.122.65 Username input format: ● username@realm ○ realm\username ○ realm/username Realms: Default: ● / Realm: local | Local users / Allow local users to override remote users: off / Groups: Filter: [Edit] Filter local users: [Edit] / Delete Add a realm Login session timeout: 500 minutes (5-1440) Default IdP certificate: Fortinet_CA1_Factory | C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=FortiAuthenticator, CN=FAC-VMTM20000586, emailAddress=support@fortinet.com

3. Click *OK* to apply these changes.

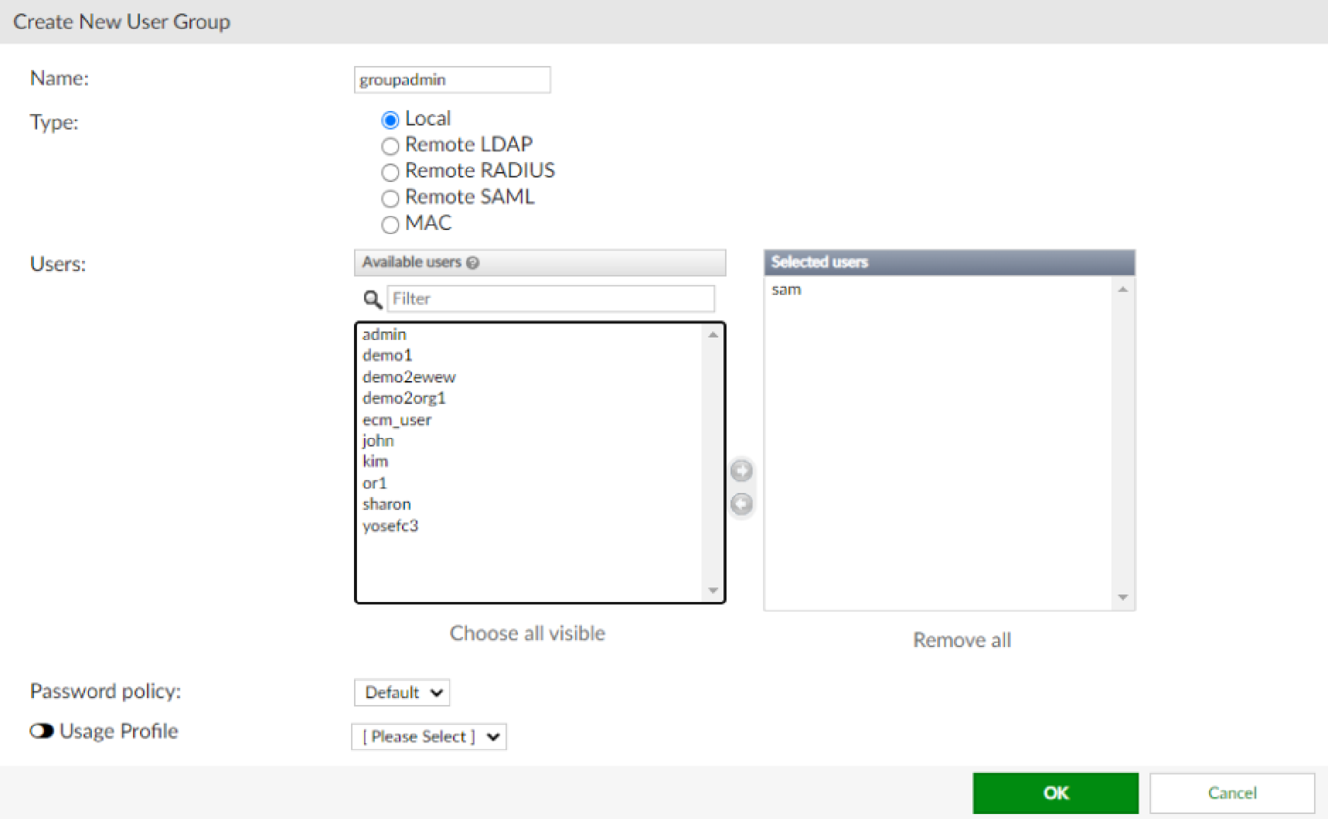
Setting up user group management

To configure on FortiAuthenticator the assertion attribute that will be used to map users' permissions to access FortiEDR:

1. Go to *Authentication > User Management > User Groups*.
2. Select *Create New*.

3. Specify a name for the group to be used for setting User access permissions for FortiEDR. In our example, we used `groupuser`.
4. In the *Users* section, select all the FortiAuthenticator users to be assigned with User permission to the FortiEDR Central Manager Console in order to add them to this User Group.
5. Click *OK* to save the configuration.
6. Repeat steps 1 – 5 above to create a group for each role and select the users to be assigned to that group with the corresponding permissions to the FortiEDR Central Manager Console.

In our example, we created a group named *groupadmin* and assigned this user the same Admin permissions to the FortiEDR Central Manager Console, as shown below:



Create New User Group

Name: groupadmin

Type:
● Local
○ Remote LDAP
○ Remote RADIUS
○ Remote SAML
○ MAC

Users:

Available users
Filter
admin
demo1
demo2ewew
demo2org1
ecm_user
john
kim
or1
sharon
yosefc3

Selected users
sam

Choose all visible

Remove all

Password policy: Default

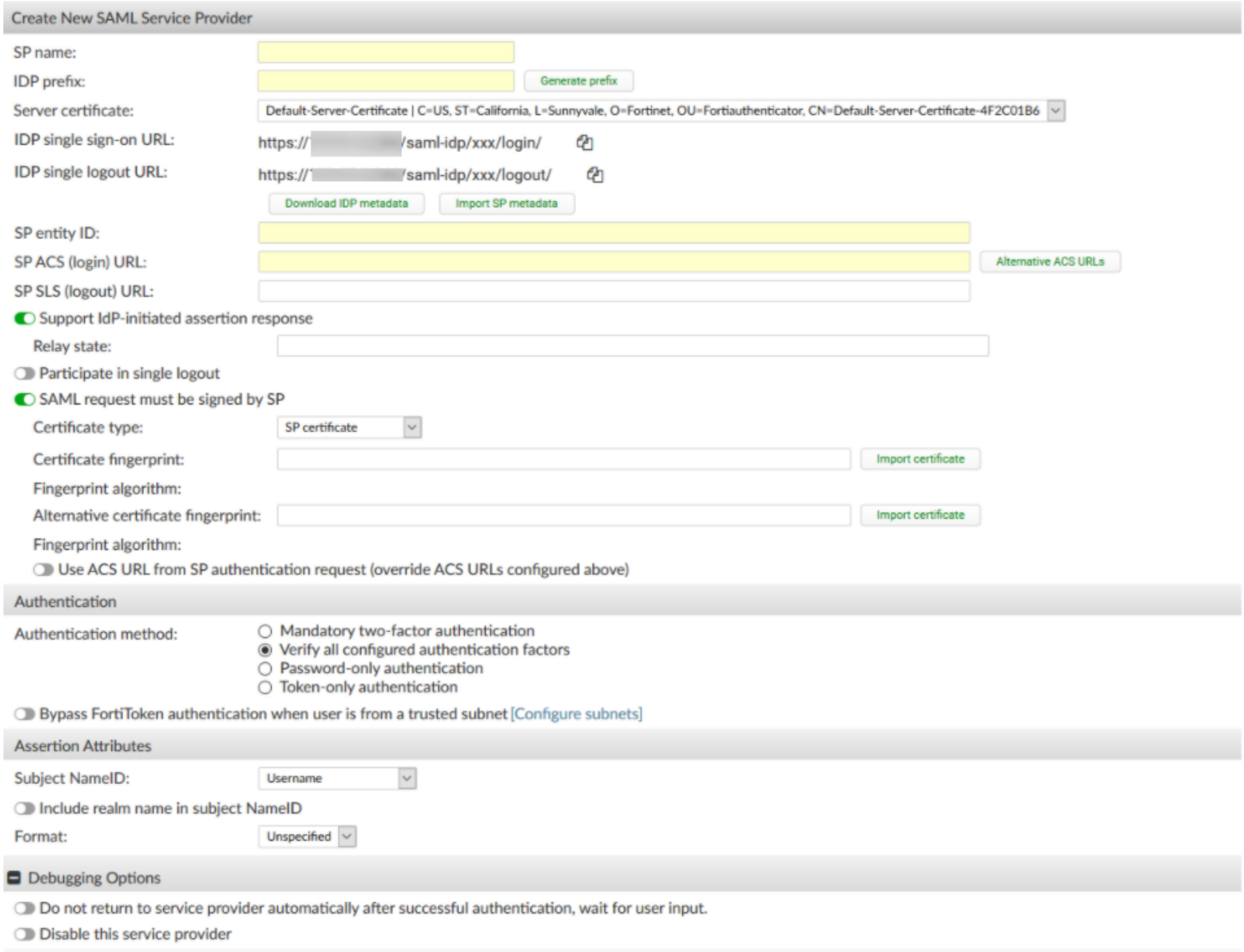
Usage Profile: [Please Select]

New or existing FortiAuthenticator users can also be configured into groups on the Local Users create and edit page.

Setting up service provider for FortiEDR

To configure FortiEDR as a SAML service provider on FortiAuthenticator:

1. Go to *Authentication > SAML IdP > Service Providers*.
2. Select *Create New*.



Create New SAML Service Provider

SP name:

IDP prefix:

Server certificate: Default-Server-Certificate | C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=Fortiauthenticator, CN=Default-Server-Certificate-4F2C01B6

IDP single sign-on URL: https://[redacted]/saml-idp/xxx/login/

IDP single logout URL: https://[redacted]/saml-idp/xxx/logout/

SP entity ID:

SP ACS (login) URL:

SP SLS (logout) URL:

Support IdP-initiated assertion response

Relay state:

Participate in single logout

SAML request must be signed by SP

Certificate type: SP certificate

Certificate fingerprint:

Fingerprint algorithm:

Alternative certificate fingerprint:

Fingerprint algorithm:

Use ACS URL from SP authentication request (override ACS URLs configured above)

Authentication

Authentication method:
○ Mandatory two-factor authentication
● Verify all configured authentication factors
○ Password-only authentication
○ Token-only authentication

Bypass FortiToken authentication when user is from a trusted subnet [Configure subnets]

Assertion Attributes

Subject NameID: Username

Include realm name in subject NameID

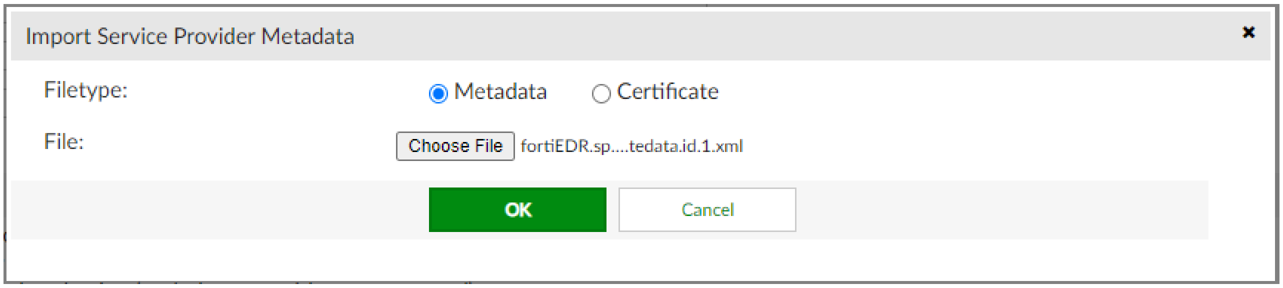
Format: Unspecified

Debugging Options

Do not return to service provider automatically after successful authentication, wait for user input.

Disable this service provider

3. Fill in the following fields:
   - *SP name*: Enter a name for the FortiEDR SP.
   - *IDP prefix*: Select *Generate prefix* in order to generate a random 16-digit alphanumeric string or alternatively enter a prefix for the IDP that is appended to the end of the IDP URLs.
4. Click *Download IDP metadata* to save the FortiAuthenticator IDP data file to be used for uploading into FortiEDR. Refer to step 3 in SAML authentication on page 287 for more information.
5. Click *Import SP metadata* and select the SP data file that was downloaded from FortiEDR. Refer to step 2 in SAML authentication on page 287 for more information.

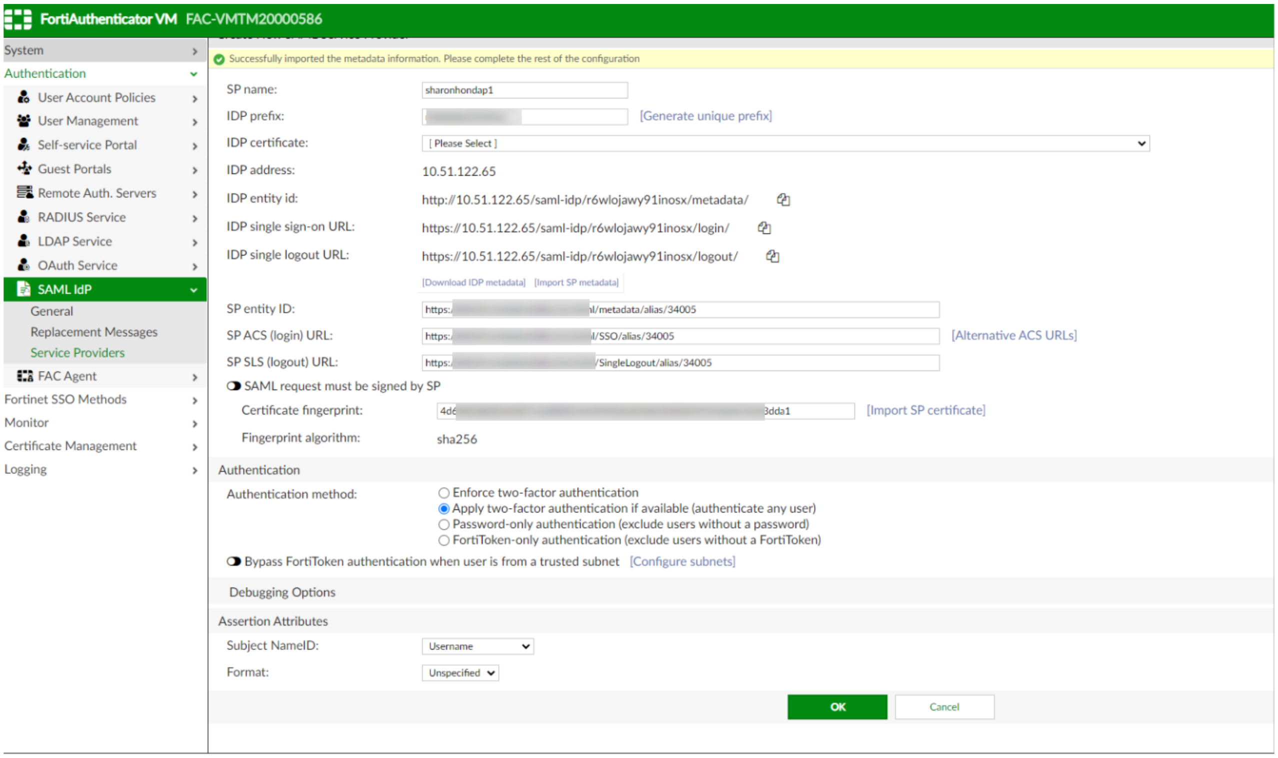


Import Service Provider Metadata

Filetype: ● Metadata ○ Certificate

File: Choose File fortiEDR.sp....tedata.id.1.xml

6. All other service provider configuration fields are auto-filled after the SP data file import:



Successfully imported the metadata information. Please complete the rest of the configuration

SP name: sharonhondap1

IDP prefix: [redacted] [Generate unique prefix]

IDP certificate: [Please Select]

IDP address: 10.51.122.65

IDP entity id: http://10.51.122.65/saml-idp/r6wlojawy91inosx/metadata/

IDP single sign-on URL: https://10.51.122.65/saml-idp/r6wlojawy91inosx/login/

IDP single logout URL: https://10.51.122.65/saml-idp/r6wlojawy91inosx/logout/

[Download IDP metadata] [Import SP metadata]

SP entity ID: https:[redacted]l/metadata/alias/34005

SP ACS (login) URL: https:[redacted]l/SSO/alias/34005 [Alternative ACS URLs]

SP SLS (logout) URL: https:[redacted]/SingleLogout/alias/34005

SAML request must be signed by SP

Certificate fingerprint: 4d[redacted]3dda1 [Import SP certificate]

Fingerprint algorithm: sha256

Authentication

Authentication method:
○ Enforce two-factor authentication
● Apply two-factor authentication if available (authenticate any user)
○ Password-only authentication (exclude users without a password)
○ FortiToken-only authentication (exclude users without a FortiToken)

Bypass FortiToken authentication when user is from a trusted subnet [Configure subnets]

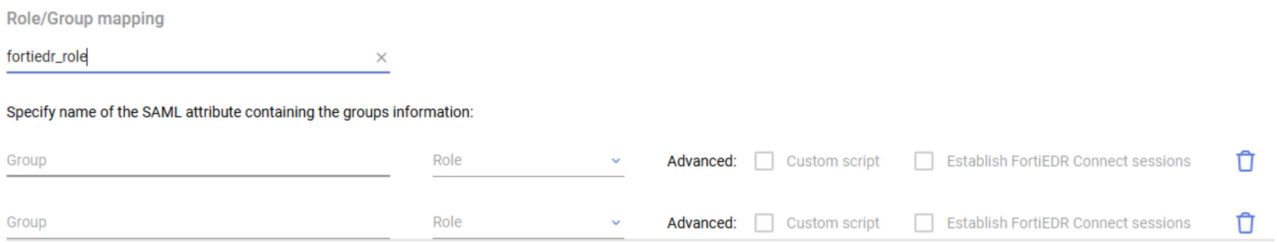
Debugging Options

Assertion Attributes

Subject NameID: Username

Format: Unspecified

7. Click *OK* to apply the changes.
8. Go to *Authentication* > *SAML IdP* > *Service Providers* and double-click to open the Service Provider that you created in the previous step.
9. In the *SAML Attribute* section, click *Create New*.
10. In the popup window, enter the attribute name that was configured in the FortiEDR SAML Authentication settings and select *FortiAuthenticator Group* as the User Attribute.
    In our example, we use `fortiedr_role` as an attribute name, as shown below:



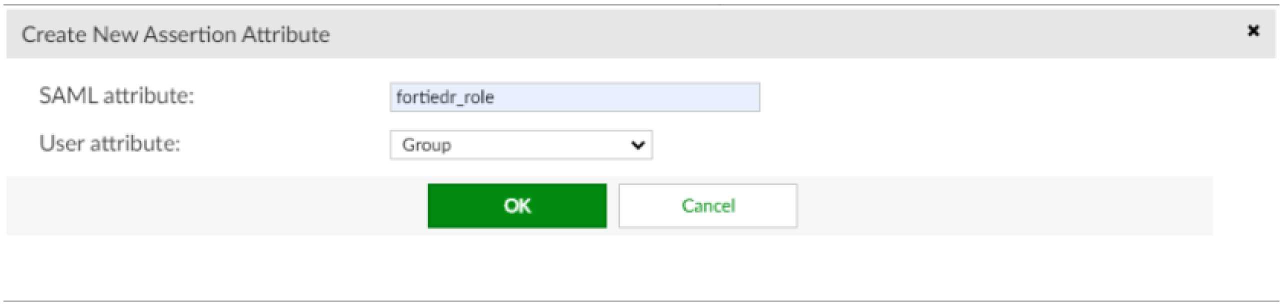
Role/Group mapping

fortiedr_role

Specify name of the SAML attribute containing the groups information:

Group
Role
Advanced: □ Custom script □ Establish FortiEDR Connect sessions
Group
Role
Advanced: □ Custom script □ Establish FortiEDR Connect sessions

And therefore the configuration on FortiAuthenticator appears as follows:



Create New Assertion Attribute

SAML attribute: fortiedr_role

User attribute: Group

11. Click *OK* to save the changes.

FortiAuthenticator can now be used as the IdP, which provides authorization and authentication for users trying to access the FortiEDR Central Manager Console. When logging into the FortiEDR Console via the SSO url that is specified in the SAML settings page, a FortiAuthenticator user is awarded access permissions to the FortiEDR Central Manager according to the User Groups into which he/she was added.

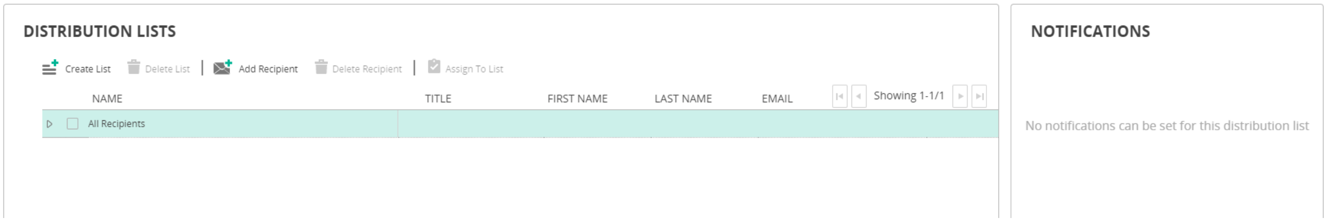
Distribution lists

The *DISTRIBUTION LISTS* option enables you to specify recipients who will receive an email each time a security event is triggered by FortiEDR.

You must configure SMTP before using the *Distribution List* option. For more details, see SMTP on page 308.

Emails are only sent for security events that occur on devices that are part of Collector Groups that are assigned to a Playbook policy in which the *Send Email Notification* option is checked.

Each email contains all the raw data items collected by FortiEDR about that security event. The system is provided with a Distribution List called All Recipients that contains all FortiEDR Central Manager users. All other recipients that are added to the system are also automatically added to the *All Recipients* list.



DISTRIBUTION LISTS

	NAME	TITLE	FIRST NAME	LAST NAME	EMAIL
▷ □	All Recipients				

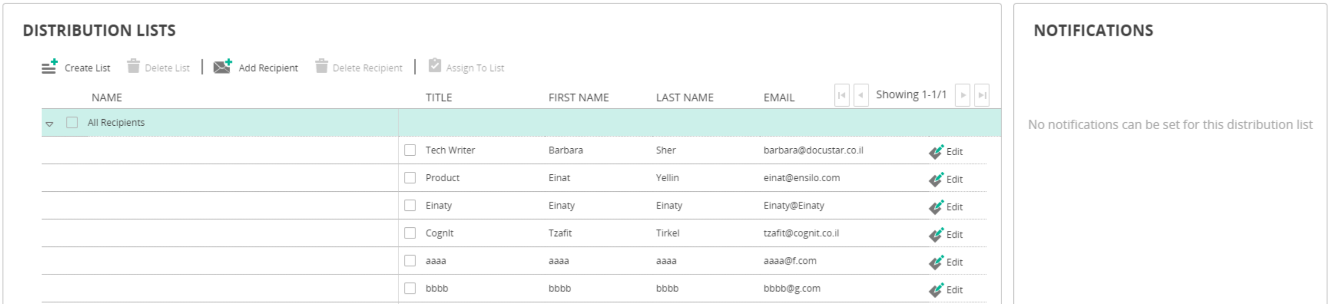
NOTIFICATIONS

No notifications can be set for this distribution list

This window displays a row for each Distribution List. Click the *Expand* button (▽) in a row to view the recipients assigned to that list.

Use the *Create List* button (Create List) to create a new distribution list.

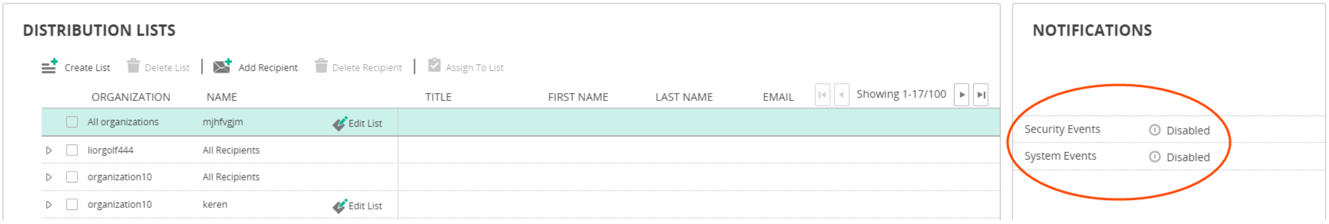
Use the *Add Recipient* button (Add Recipient) to add a recipient or user to a distribution list.



NAME	TITLE	FIRST NAME	LAST NAME	EMAIL	
▽ □ All Recipients					
	□ Tech Writer	Barbara	Sher	barbara@docustar.co.il	Edit
	□ Product	Einat	Yellin	einat@ensilo.com	Edit
	□ Einaty	Einaty	Einaty	Einaty@Einaty	Edit
	□ CognIt	Tzafit	Tirkel	tzafit@cognit.co.il	Edit
	□ aaaa	aaaa	aaaa	aaaa@f.com	Edit
	□ bbbb	bbbb	bbbb	bbbb@g.com	Edit

No notifications can be set for this distribution list

Select a distribution list row and then use the *Enabled/Disabled* option in the *NOTIFICATIONS* pane on the right to enable or disable the list per event type (system events or security events).



ORGANIZATION	NAME		TITLE	FIRST NAME	LAST NAME	EMAIL
□ All organizations	mjhfvgjm	Edit List				
▷ □ liorgolf444	All Recipients					
▷ □ organization10	All Recipients					
▷ □ organization10	keren	Edit List				

Security Events	ⓘ Disabled
System Events	ⓘ Disabled

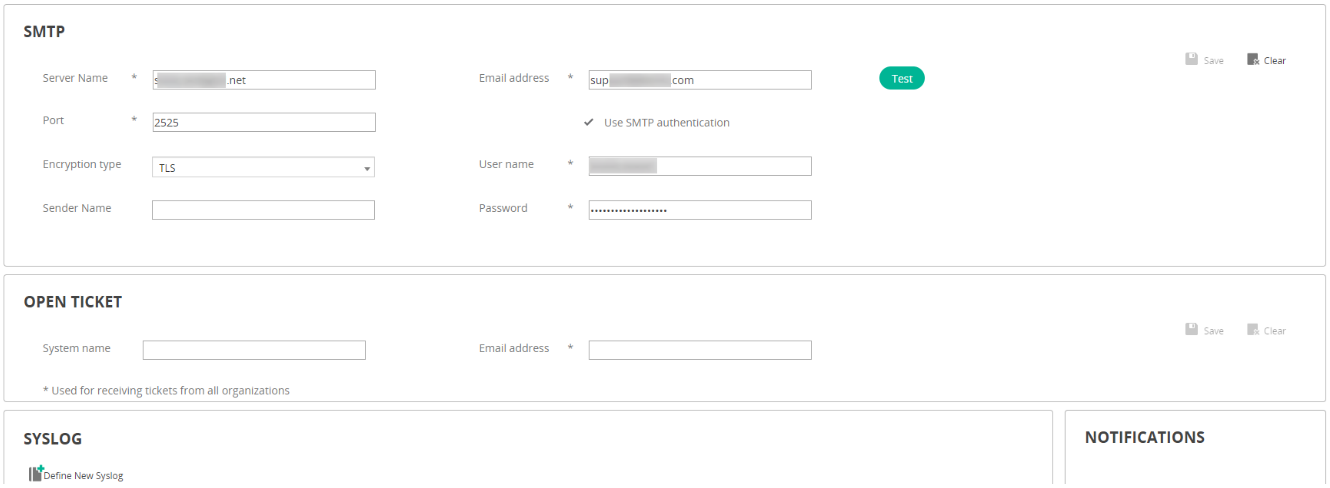
Export settings

The *EXPORT SETTINGS* option provides access to the following options:

- SMTP on page 308
- Open Ticket on page 309
- Syslog on page 310

SMTP

The SMTP option enables you to configure the SMTP server to be used for sending emails. You can also check the connectivity to the SMTP server.



SMTP

Server Name * s[redacted].net

Port * 2525

Encryption type TLS

Sender Name

Email address * sup[redacted]com

✓ Use SMTP authentication

User name * [redacted]

Password * ••••••••••••••••••••

OPEN TICKET

System name

Email address *

* Used for receiving tickets from all organizations

SYSLOG

NOTIFICATIONS

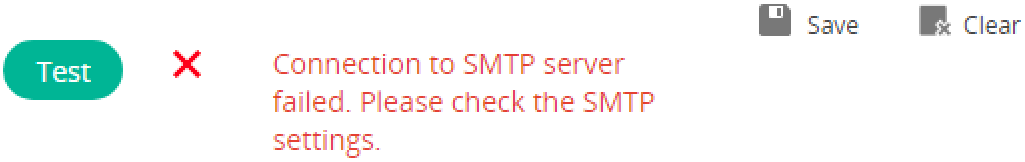
In a single-organization system, SMTP settings are only accessible in Hoster view (for administrators of all organization), or to the administrator of that organization.

To configure SMTP server settings:

1. In the SMTP area, enter standard SMTP settings and then click *Save*.

To test SMTP server connectivity:

1. In the SMTP area, click *Test*. An error message displays if there is no connectivity to the server.



Connection to SMTP server failed. Please check the SMTP settings.

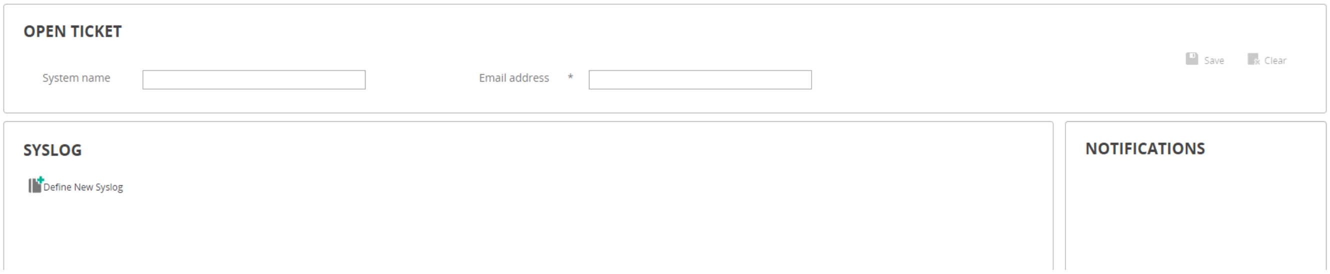
Open Ticket

The *Open Ticket* option enables you to send events to an event-management tool such as Jira or ServiceNow. Open Ticket automatically opens a ticket and attaches the relevant event to a ticket.

In order for the Open Ticket feature to work properly, you must set up an email feed in the event-management tool to be used.

Most event-management tools are supported. FortiEDR has tested and verified that Open Ticket works with the ServiceNow and Jira systems. For more details about setting up the email feed required for this feature, see Appendix A – Setting up an email feed for open ticket on page 448.

Security events are only sent to a ticketing system when they occur on devices that are part of Collector Groups that are assigned to a Playbook policy in which the *Open Ticket* option is checked.

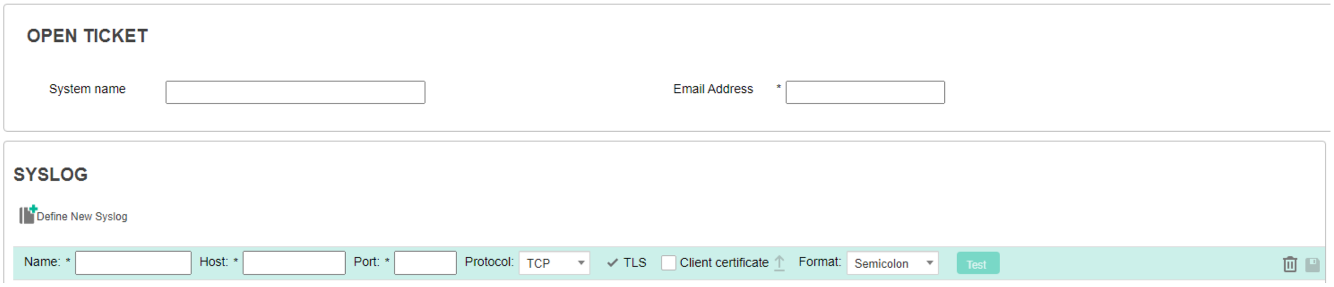


To configure Open Ticket settings:

1. In the *Open Ticket* area, in the *System name* field, enter the system name for the tool to be used for event management. This is a free-text field.
2. In the *Email address* field, enter the email address that is the destination to which all tickets are to be sent from FortiEDR. All tickets from all organizations are sent to this email.
3. Click *Save*.

Syslog

The *SYSLOG* option enables you to configure FortiEDR to automatically send FortiEDR events to one or more standard Security Information and Event Management (SIEM) solutions (such as FortiAnalyzer) via Syslog.



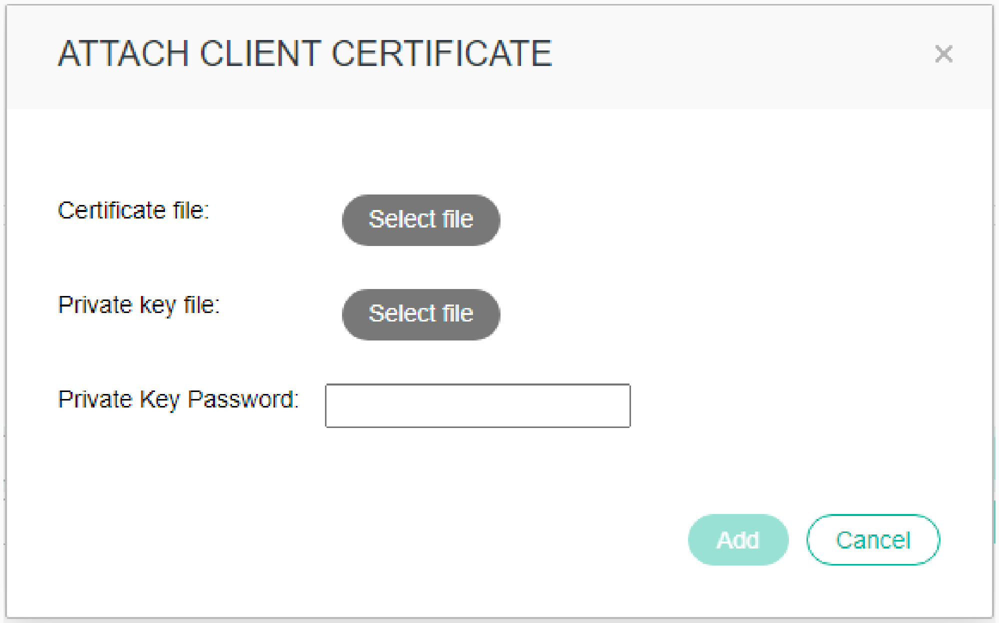
Protocol: TCP ✓ TLS □ Client certificate Format: Semicolon

All Syslog messages in FortiEDR originate from the Central Manager. The source IP address for syslog messages is the IP of the Central Manager. The FortiEDR Central Manager server sends the raw data for security event aggregations. Each entry contains a raw data ID and an event ID. Raw data items belonging to the same security event aggregation share the same event ID, which enables the SIEM to combine them into one security event on the SIEM side, in order to remain aligned with the FortiEDR system.

Syslog messages are only sent for security events that occur on devices that are part of Collector Groups that are assigned to a Playbook policy in which the *Send Syslog Notification* option is checked.

To define a new Syslog destination:

1. Click the Define New Syslog button.
2. Specify the following attributes:

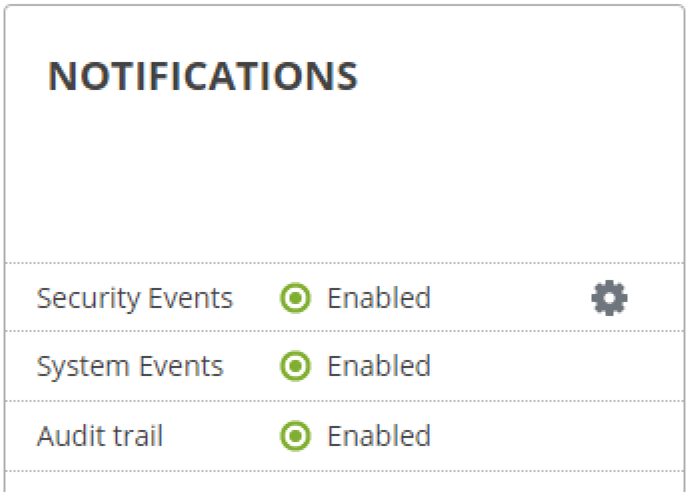
Attribute	Description
Syslog Name	Free-text field that identifies this destination in the FortiEDR.
Host	Host name of the Syslog server.
Port	Port of the Syslog server.
Protocol	Protocol of the Syslog server. You can select *TCP* or *UDP*.
TLS	When *TCP* is selected in *Protocol*, use this option to specify whether to enable TLS. If the Syslog server requires a client-side certificate, you must enable *TLS* before you can upload the certificate.
Client Certificate	If the Syslog server requires a client-side certificate, enable *TLS* and use this option to upload a certificate. For example, if your FortiAnalyzer server requires a client-side certificate, contact Fortinet Support to obtain appropriate client certificate files and upload them here.  ATTACH CLIENT CERTIFICATE × Certificate file: Select file Private key file: Select file Private Key Password: Add Cancel
Format	Select the type of the syslog server: • *Semicolon*—Select this option if the syslog server is not one the following three. FortiEDR then uses the default CSV syslog format.

Attribute	Description
	• *FAZ*—The syslog server is FortiAnalyzer. FortiAnalyzer Cloud is not supported. • *CEF*—The syslog server uses the CEF syslog format. • *LEEF*—The syslog server uses the LEEF syslog format. Refer to FortiEDR Syslog Message Reference for more details about syslog message fields for different formats.

3. Click the *Test* button to test the connection to the Syslog destination server.
4. Click the 💾 button to save the Syslog destination.

To select which syslog messages to send:

1. Select a syslog destination row.
2. Use the sliders in the *NOTIFICATIONS* pane on the right to enable or disable the destination per event type (system events, security events or audit trail) as shown below:

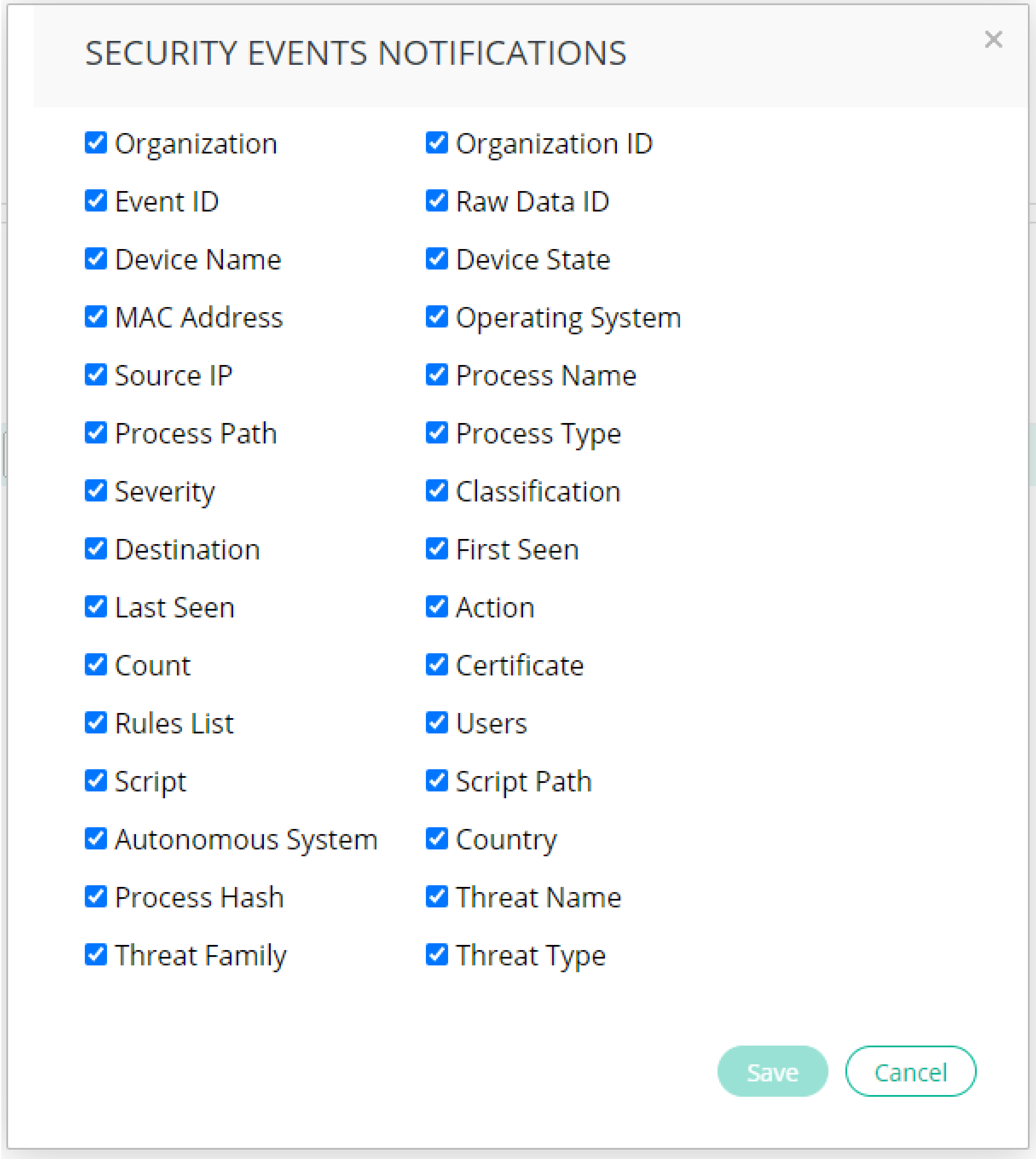


NOTIFICATIONS

Security Events	● Enabled	⚙
System Events	● Enabled	
Audit trail	● Enabled	

To select which fields will be included in the syslog messages:

Click the ⚙ button on the right of the event type and check the checkbox of the fields that you want to be sent to your Syslog.



SECURITY EVENTS NOTIFICATIONS

☑ Organization
☑ Event ID
☑ Device Name
☑ MAC Address
☑ Source IP
☑ Process Path
☑ Severity
☑ Destination
☑ Last Seen
☑ Count
☑ Rules List
☑ Script
☑ Autonomous System
☑ Process Hash
☑ Threat Family

☑ Organization ID
☑ Raw Data ID
☑ Device State
☑ Operating System
☑ Process Name
☑ Process Type
☑ Classification
☑ First Seen
☑ Action
☑ Certificate
☑ Users
☑ Script Path
☑ Country
☑ Threat Name
☑ Threat Type

You can also define a Syslog destination via REST API, including the upload of a certificate using Rest API during the process. By default, all available syslog fields and all notifications options, including security, system, and audit events, are enabled. For more details, refer to the FortiEDR RESTful API Guide. You must log in to the Fortinet Developer Network to access the guide.

Warning: If syslog is configured for both Hoster view and an organization, two syslog events will be sent.

For more information on syslog messages, such as message types and fields, see FortiEDR Syslog Message Reference.

Settings

The *Administration* > *Settings* page provides access to the following configuration options:

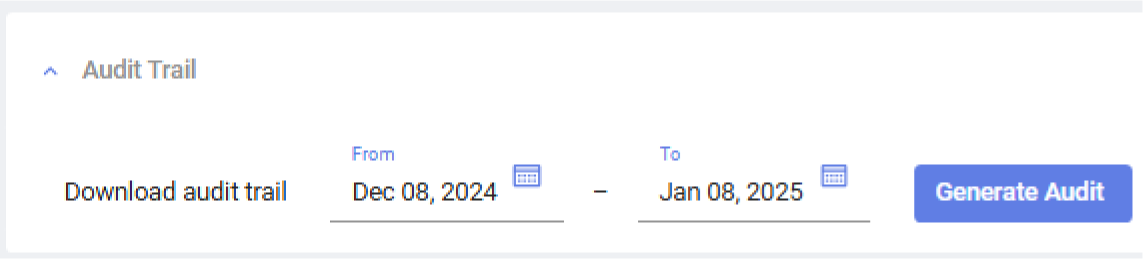
Some options are only available to specific roles. For more information about user roles and permissions, see Users on page 277.

- Audit Trail on page 314
- Deployment URL on page 316
- Component Authentication on page 316
- File Scan on page 319
- End Users Notifications on page 320
- Personal Data Handling on page 325
- IoT Device Discovery on page 331
- Windows Security Center on page 333
- Application Control Manager on page 334
- FortiEDR Connect on page 334
- Reputation Service on page 335

Audit Trail

FortiEDR's audit mechanism records every user action in the FortiEDR system. System actions are not recorded. You can download the audit trail (up to 30 days) to a CSV file for further analysis.

Each time a new audit trail is created, it can be sent through the Syslog.



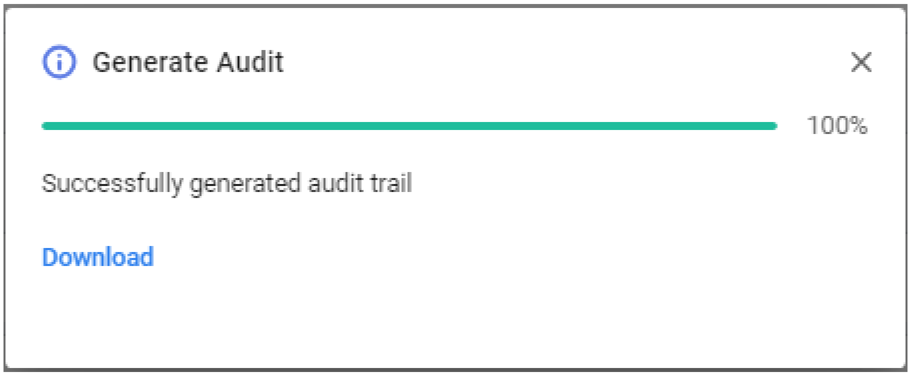
Download audit trail

From: Dec 08, 2024 – To: Jan 08, 2025

To generate the audit trail:

1. Navigate to the *Administration* > *Settings* page.
2. Expand the *Audit Trail* section and specify the *From* and *To* dates in the respective fields.

3. Click the *Generate Audit* button. A progress window displays:



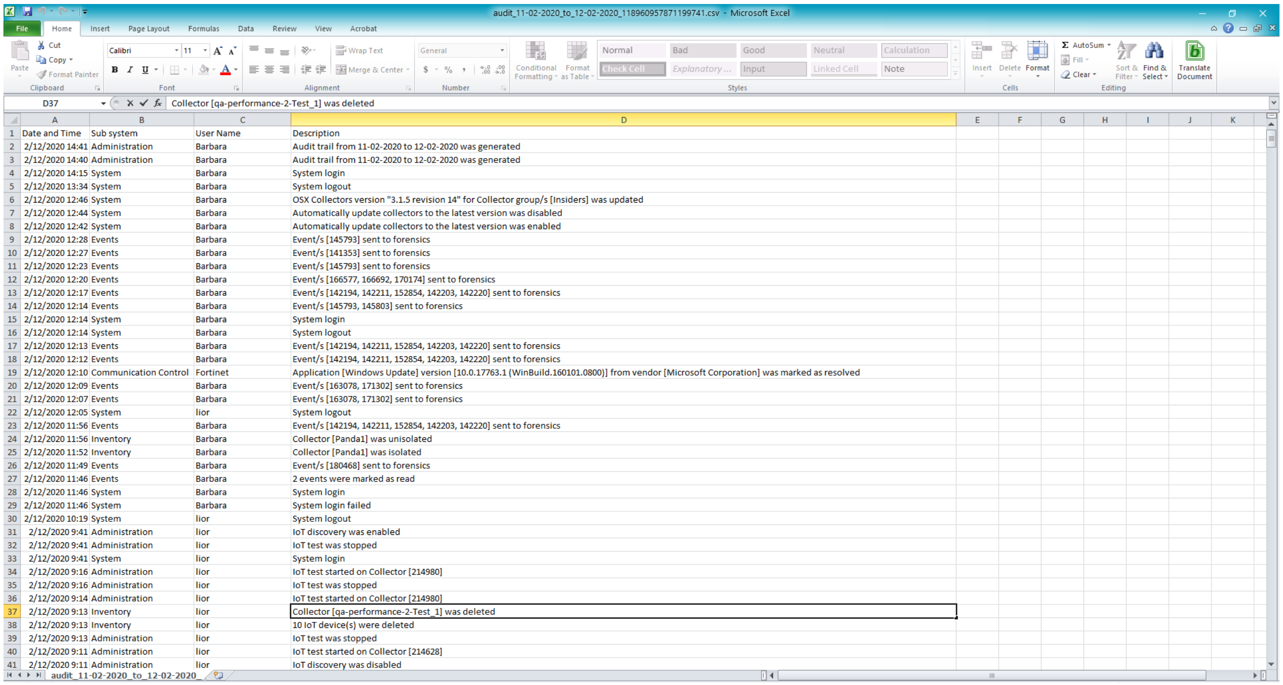
Generate Audit

100%

Successfully generated audit trail

Download

4. Click the *Download* link to download the audit trail to a CSV file or spreadsheet, such as the example shown below, displays:



audit_11-02-2020_to_12-02-2020_118960957871199741.csv - Microsoft Excel

D37 Collector [qa-performance-2-Test_1] was deleted

Date and Time	Sub system	User Name	Description
2/12/2020 14:41	Administration	Barbara	Audit trail from 11-02-2020 to 12-02-2020 was generated
2/12/2020 14:40	Administration	Barbara	Audit trail from 11-02-2020 to 12-02-2020 was generated
2/12/2020 14:15	System	Barbara	System login
2/12/2020 13:34	System	Barbara	System logout
2/12/2020 12:46	System	Barbara	OSX Collectors version "3.1.5 revision 14" for Collector group/s [Insiders] was updated
2/12/2020 12:44	System	Barbara	Automatically update collectors to the latest version was disabled
2/12/2020 12:42	System	Barbara	Automatically update collectors to the latest version was enabled
2/12/2020 12:28	Events	Barbara	Event/s [145793] sent to forensics
2/12/2020 12:27	Events	Barbara	Event/s [141353] sent to forensics
2/12/2020 12:23	Events	Barbara	Event/s [145793] sent to forensics
2/12/2020 12:20	Events	Barbara	Event/s [166577, 166692, 170174] sent to forensics
2/12/2020 12:17	Events	Barbara	Event/s [142194, 142211, 152854, 142203, 142220] sent to forensics
2/12/2020 12:14	Events	Barbara	Event/s [145793, 145803] sent to forensics
2/12/2020 12:14	System	Barbara	System login
2/12/2020 12:14	System	Barbara	System logout
2/12/2020 12:13	Events	Barbara	Event/s [142194, 142211, 152854, 142203, 142220] sent to forensics
2/12/2020 12:12	Events	Barbara	Event/s [142194, 142211, 152854, 142203, 142220] sent to forensics
2/12/2020 12:10	Communication Control	Fortinet	Application [Windows Update] version [10.0.17763.1 (WinBuild.160101.0800)] from vendor [Microsoft Corporation] was marked as resolved
2/12/2020 12:09	Events	Barbara	Event/s [163078, 171302] sent to forensics
2/12/2020 12:07	Events	Barbara	Event/s [163078, 171302] sent to forensics
2/12/2020 12:05	System	lior	System logout
2/12/2020 11:56	Events	Barbara	Event/s [142194, 142211, 152854, 142203, 142220] sent to forensics
2/12/2020 11:56	Inventory	Barbara	Collector [Panda1] was unisolated
2/12/2020 11:52	Inventory	Barbara	Collector [Panda1] was isolated
2/12/2020 11:49	Events	Barbara	Event/s [180468] sent to forensics
2/12/2020 11:46	Events	Barbara	2 events were marked as read
2/12/2020 11:46	System	Barbara	System login
2/12/2020 11:46	System	Barbara	System login failed
2/12/2020 10:19	System	lior	System logout
2/12/2020 9:41	Administration	lior	IoT discovery was enabled
2/12/2020 9:41	Administration	lior	IoT test was stopped
2/12/2020 9:41	System	lior	System login
2/12/2020 9:16	Administration	lior	IoT test started on Collector [214980]
2/12/2020 9:16	Administration	lior	IoT test was stopped
2/12/2020 9:14	Administration	lior	IoT test started on Collector [214980]
2/12/2020 9:13	Inventory	lior	Collector [qa-performance-2-Test_1] was deleted
2/12/2020 9:13	Inventory	lior	10 IoT device(s) were deleted
2/12/2020 9:13	Administration	lior	IoT test was stopped
2/12/2020 9:11	Administration	lior	IoT test started on Collector [214628]
2/12/2020 9:11	Administration	lior	IoT discovery was disabled

audit_11-02-2020_to_12-02-2020_

Each row in the audit trail file contains the following columns of information:

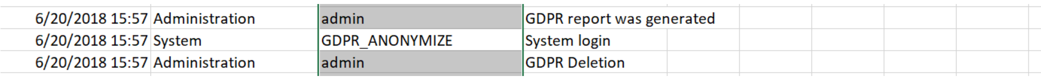
Field	Definition
Date and Time	Displays the date and time in the format *yyyy-mm-dd hh:mm:ss*.
Sub system	Displays the change type, such as System, Configuration, Administration, Forensics, Events, Inventory, Communication Control or Health.
User Name	Displays the name of the user.
Description	Displays the action and/or a description.

The following actions can be audited:

- Policy actions
- Forensic actions

- Administrative actions
- Events
- Inventory actions
- System health changes

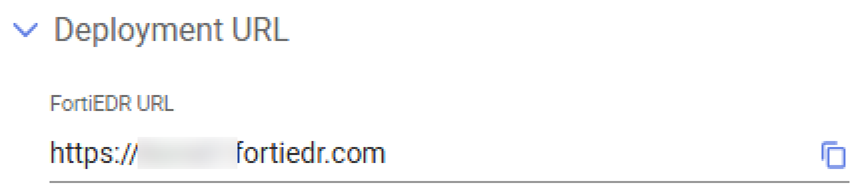
If an employee's/user's data was removed from FortiEDR for GDPR compliance, then the affected record for that person still displays in the audit trail but shows *GDPR_ ANONYMIZE* instead of actual user data. For example, as shown below:



6/20/2018 15:57	Administration	admin	GDPR report was generated
6/20/2018 15:57	System	GDPR_ANONYMIZE	System login
6/20/2018 15:57	Administration	admin	GDPR Deletion

Deployment URL

This section displays the URL of the environment that you can copy. The URL is read-only and includes the domain information that you will need in order to use FortiEDR APIs.



Deployment URL

FortiEDR URL

https://[redacted]fortiedr.com

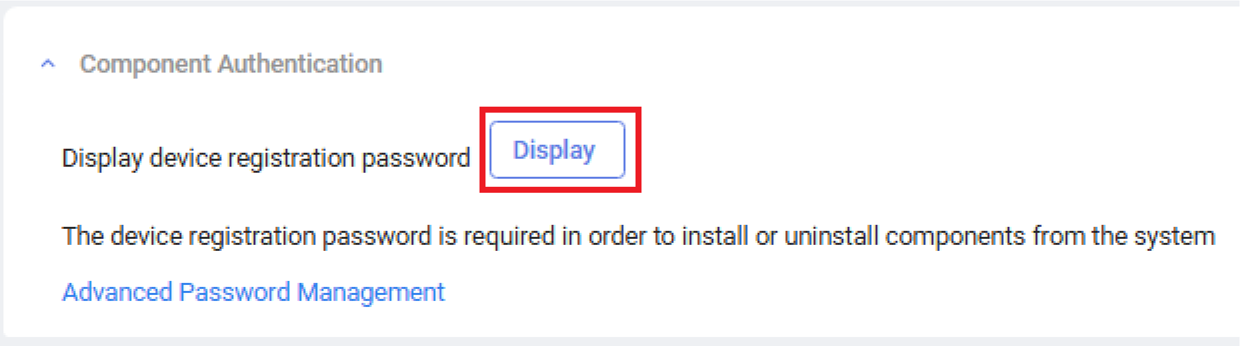
Component Authentication

In order to install, upgrade or uninstall a Collector, you must supply the registration password. The registration password is the same for all Collectors in the FortiEDR system. This password is defined when you configure the FortiEDR Central Manager Server and console.

The *Component Authentication* section provides options to retrieve a lost registration password or revoke a compromised registration password.

If you forget the registration password, retrieve it by following the steps below:

1. Navigate to the *Administration* > *Settings* page.
2. Expand the *Component Authentication* section and click the *Display* button.



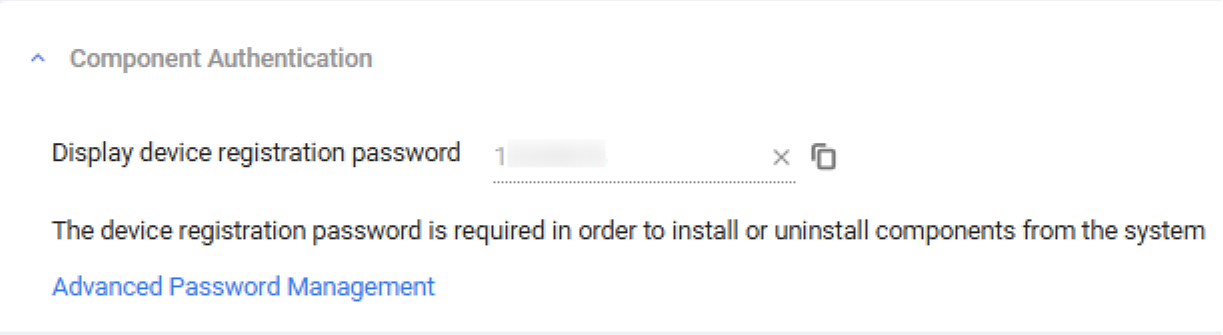
Component Authentication

Display device registration password Display

The device registration password is required in order to install or uninstall components from the system

Advanced Password Management

The password is shown temporarily for you to view to copy.



Component Authentication

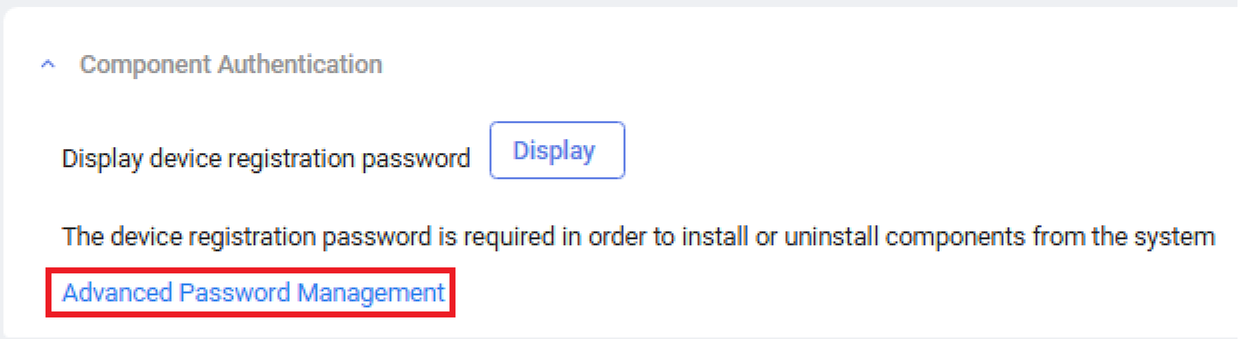
Display device registration password 1[redacted]

The device registration password is required in order to install or uninstall components from the system

Advanced Password Management

To revoke a compromised registration password:

1. Navigate to the *Administration* > *Settings* page.
2. Expand the *Component Authentication* section and click *Advanced Password Management*.



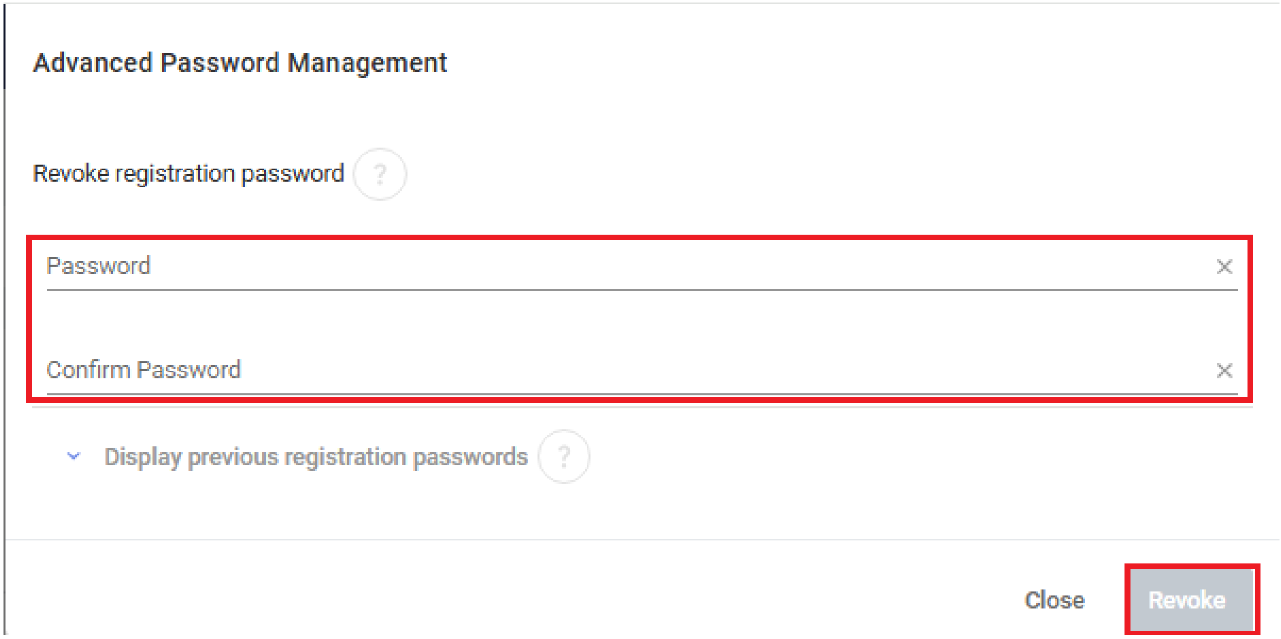
Component Authentication

Display device registration password Display

The device registration password is required in order to install or uninstall components from the system

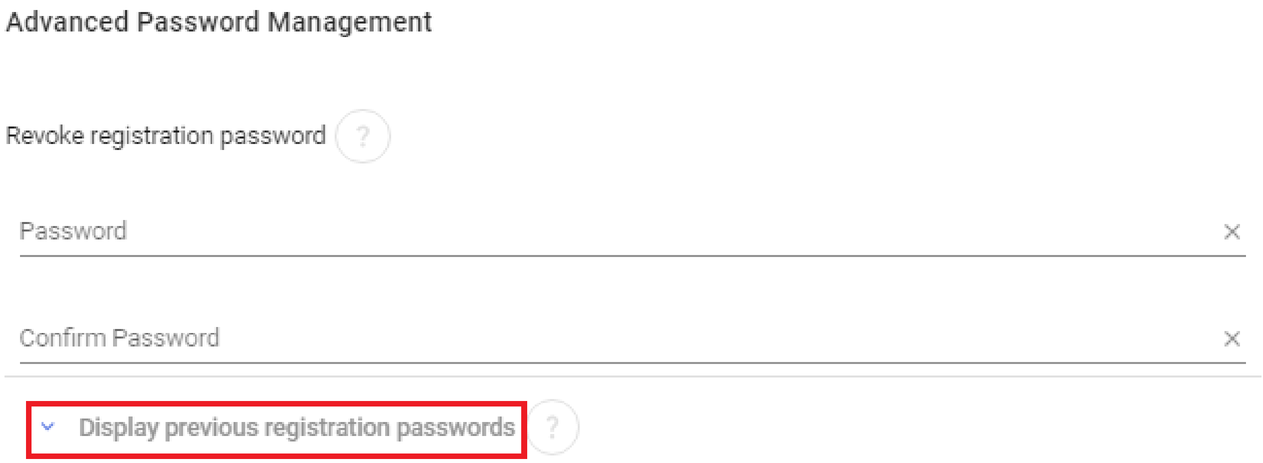
Advanced Password Management

3. Enter the new password, confirm it, and click *Revoke*.



Advanced Password Management
Revoke registration password
Password
Confirm Password
Display previous registration passwords
Close
Revoke

After you revoke an existing registration password with a new one, the new password is required for subsequent connections with connected or new Collectors. However, you still need the revoked password for reconnection or uninstallation of disconnected Collectors. You can see a list of revoked passwords under *Display Previous Registration Passwords* with information of revoked time and number of Collectors still using that password.



Advanced Password Management
Revoke registration password
Password
Confirm Password
Display previous registration passwords

You can revoke the registration password four times maximum, after which the *Revoke* button is disabled and you must delete an old password in order to create a new one.

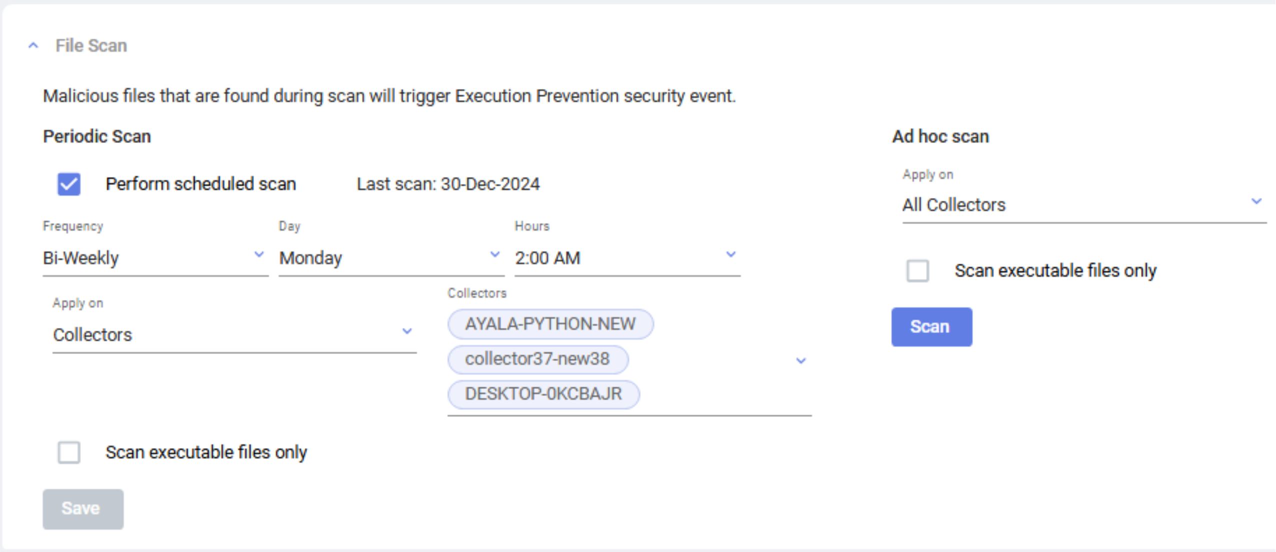
Fortinet recommends that you generate a new custom Collector after revoking a compromised registration password.

File Scan

FortiEDR can perform periodic scans of the files in the system on a scheduled or on-demand basis, based on its execution prevention policy. During a periodic scan, only the files on the hard drive are scanned and no memory scan is performed. For a periodic scan, each file on the hard drive is scanned. If a malicious file is identified during a scan, a security event is triggered.

To schedule a periodic scan:

1. Navigate to the *Administration* > *Settings* page.
2. In the *File Scan* area, check the *Perform scheduled scan* checkbox. This checkbox must be checked to perform the scan according to the designated schedule.



File Scan

Malicious files that are found during scan will trigger Execution Prevention security event.

Periodic Scan

☑ Perform scheduled scan   Last scan: 30-Dec-2024

Frequency: Bi-Weekly

Day: Monday

Hours: 2:00 AM

Apply on: Collectors

Collectors: AYALA-PYTHON-NEW, collector37-new38, DESKTOP-0KCBAJR

□ Scan executable files only

Save

Ad hoc scan

Apply on: All Collectors

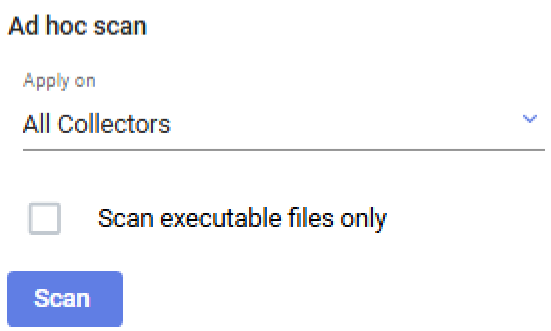
□ Scan executable files only

Scan

3. In the *Frequency* dropdown list, select how frequently to execute the scan. Options are *Weekly*, *Bi-Weekly* (every two weeks), or *Monthly*.
4. In the *Day* dropdown list, select the day of the week to execute the scan.
5. In the *Hours* dropdown list, select the hour of the day to execute the scan.
6. Use the radio button to select on which devices the scheduled scan should be performed. When selecting Collector Groups or Collectors, you should specify which Groups or Collectors should be included in the scan. Devices that are not listed here are not scanned.
7. Click the *Save* button. The scan is performed as scheduled.

To perform an on-demand file scan:

1. Navigate to the *Administration* > *Settings* page.
2. In the *Ad hoc scan* area, select which devices to scan by specifying one or more Collectors or Collector Groups, or selecting the *All Collectors* option to scan all devices with installed Collectors.



Ad hoc scan

Apply on

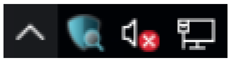
All Collectors

□ Scan executable files only

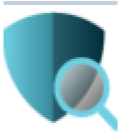
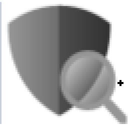
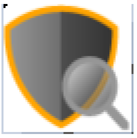
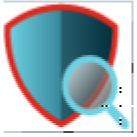
3. Check the *Scan executable files only* checkbox to only scan executable files. This option enables a quicker scan, but neglects documents, scripts and other potentially malicious files.
4. Click *Scan*. The scan is performed immediately.

End Users Notifications

Each device protected by FortiEDR can display an icon in the system tray to indicate its state.

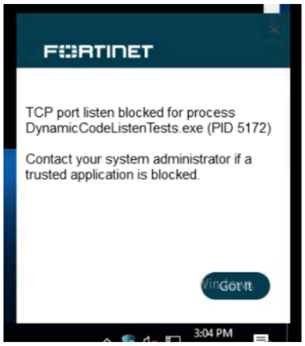


The FortiEDR icon indicates the current state of the device, as follows:

-  Protection On
-  Protection Off/Disabled
-  Degraded
-  Isolated

Terminating a FortiEDR process ends this process and stops the display of the FortiEDR icon in the system tray, but does not stop FortiEDR protection.

When the FortiEDR icon is configured to display on FortiEDR-protected devices, a popup message displays whenever something is blocked on a protected device (based on the blocking policy set for that device). File modifications (due to suspected ransomware), the exfiltration of external connections and execution prevention actions can be blocked. For example, the following shows that a TCP port listening action was blocked for the `DynamicCodeListenTests.exe` process.

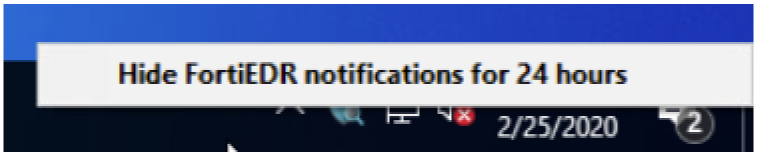


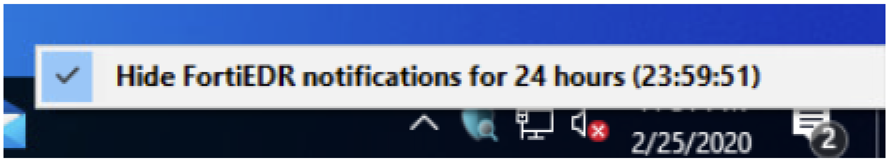
TCP port listen blocked for process DynamicCodeListenTests.exe (PID 5172)

Contact your system administrator if a trusted application is blocked.

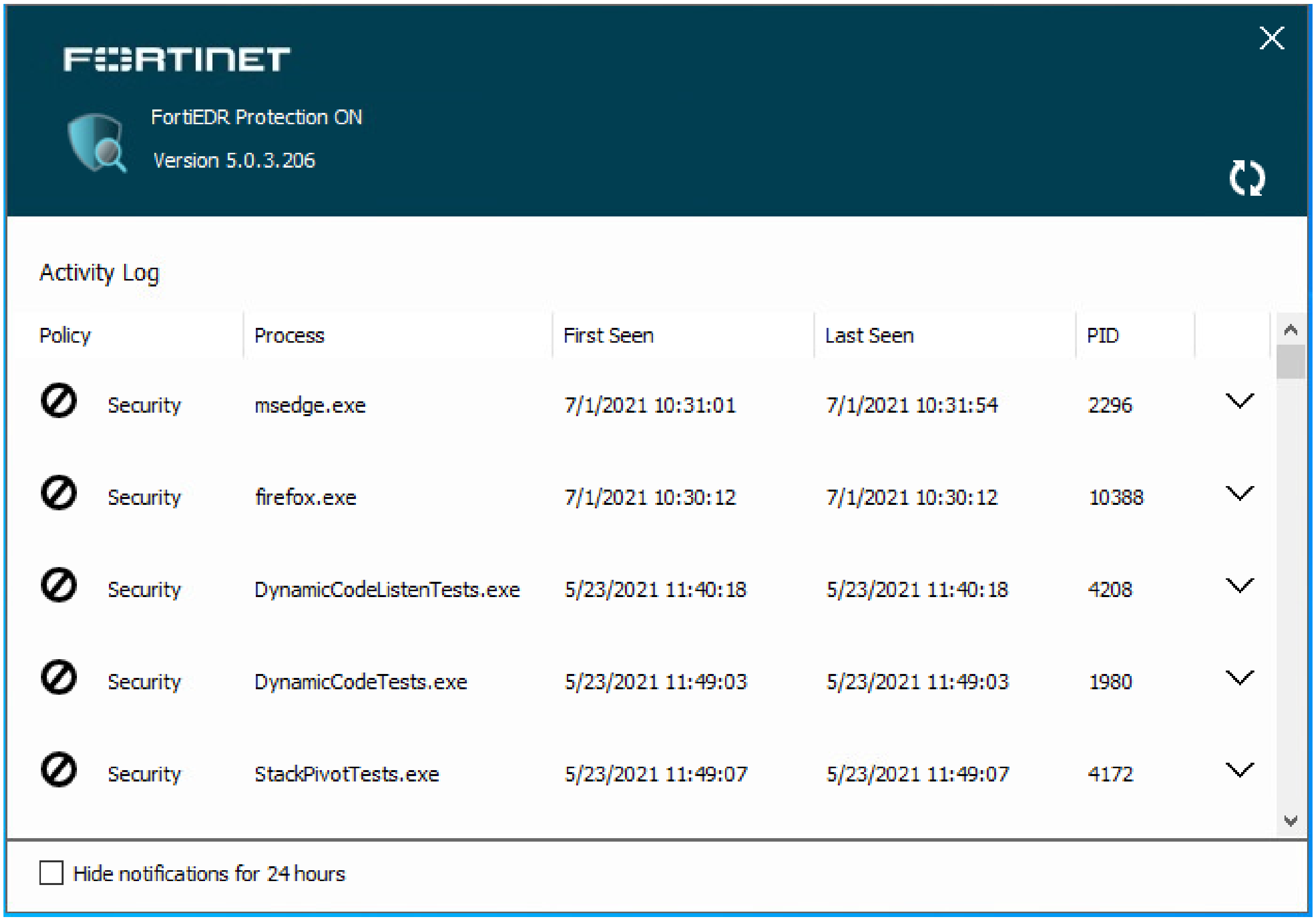
This notification is displayed only once for the same process. If the same process is blocked multiple times, only a single FortiEDR pop up is displayed.

You can choose to show or hide end-user notifications (pop-ups) for the next 24 hours. To do so, right-click the FortiEDR icon in the system tray and then check the checkbox to hide notifications or leave the checkbox unchecked to display notifications.





You can double-click the FortiEDR icon in the system tray to review recent blocking activity on the device as shown below. Each row includes a single event (that can be composed of multiple occurrences) and displays the process name, the first and last occurrences times, the process ID, and the type of blocking: either security or communication control.



FortiEDR Protection ON

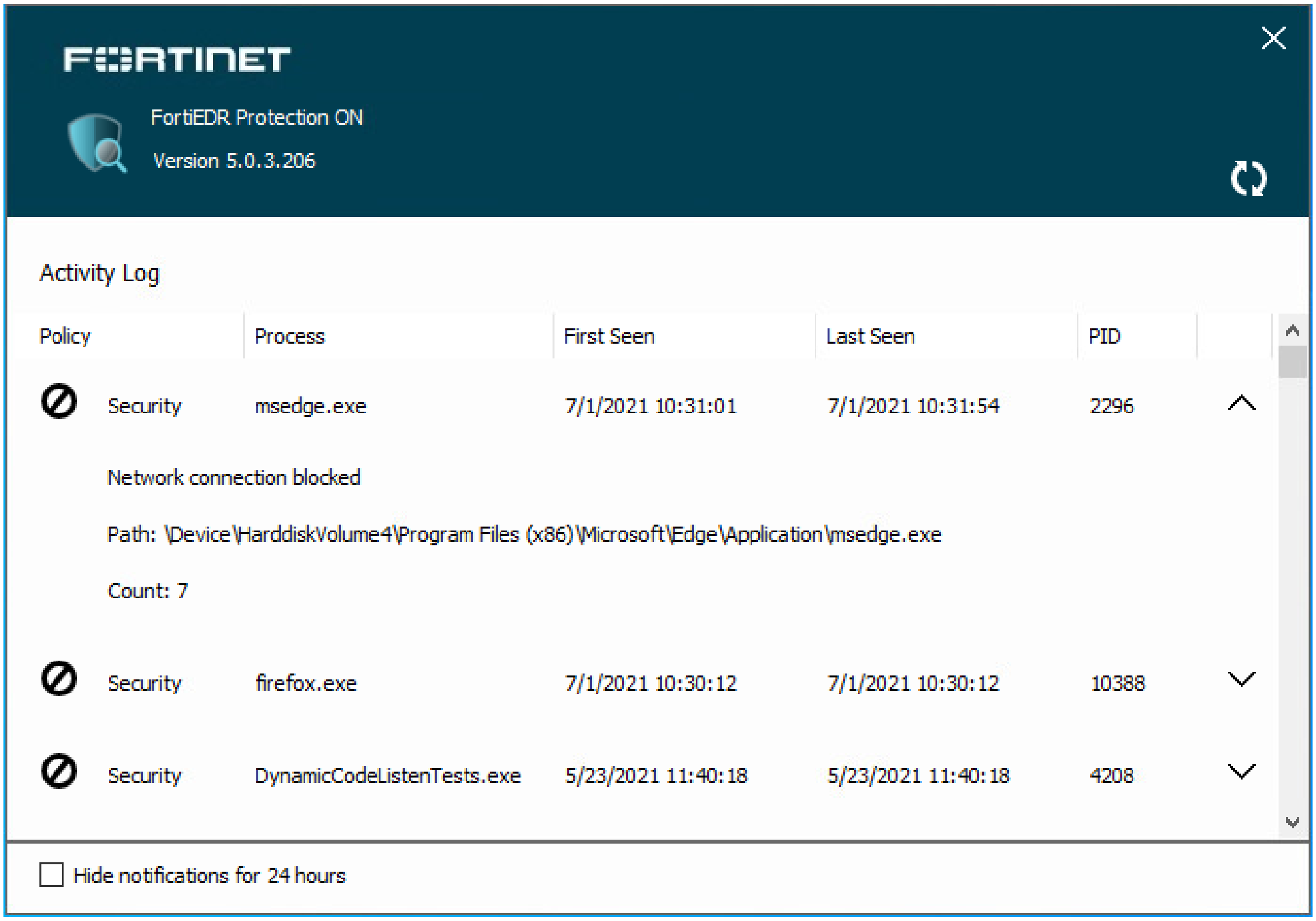
Version 5.0.3.206

Activity Log

Policy	Process	First Seen	Last Seen	PID
⊘ Security	msedge.exe	7/1/2021 10:31:01	7/1/2021 10:31:54	2296
⊘ Security	firefox.exe	7/1/2021 10:30:12	7/1/2021 10:30:12	10388
⊘ Security	DynamicCodeListenTests.exe	5/23/2021 11:40:18	5/23/2021 11:40:18	4208
⊘ Security	DynamicCodeTests.exe	5/23/2021 11:49:03	5/23/2021 11:49:03	1980
⊘ Security	StackPivotTests.exe	5/23/2021 11:49:07	5/23/2021 11:49:07	4172

☐ Hide notifications for 24 hours

Expanding the arrow on the right of each event reveals more details per event including the process path and the number of occurrences of the same blocking event:



Policy		Process	First Seen	Last Seen	PID
⊘	Security	msedge.exe	7/1/2021 10:31:01	7/1/2021 10:31:54	2296
⊘	Security	firefox.exe	7/1/2021 10:30:12	7/1/2021 10:30:12	10388
⊘	Security	DynamicCodeListenTests.exe	5/23/2021 11:40:18	5/23/2021 11:40:18	4208

Network connection blocked

Path: \Device\HarddiskVolume4\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

Count: 7

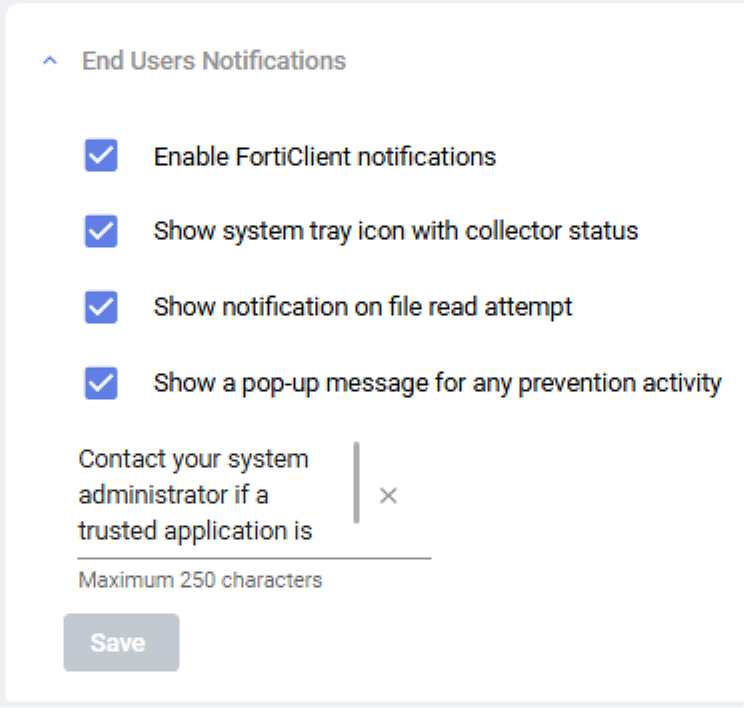
☐ Hide notifications for 24 hours

FortiEDR icon configuration

The behavior of the FortiEDR icon in the system tray must be configured in the *Administration > Settings* page.

To configure FortiEDR icon behavior:

1. Navigate to the *Administration* > *Settings* page.
2. In the *End Users Notifications* area, configure the following settings:



End Users Notifications

☑ Enable FortiClient notifications

☑ Show system tray icon with collector status

☑ Show notification on file read attempt

☑ Show a pop-up message for any prevention activity

Contact your system administrator if a trusted application is

Maximum 250 characters

Setting	Definition
Enable FortiClient notifications	Check this checkbox to display notifications sourced from FortiClient. This option is specific to FortiEndpoint deployments. See the FortiEndpoint Administration Guide for more details.
Show system tray icon with collector status	Check this checkbox to display the FortiEDR icon on each FortiEDR-protected device or leave the checkbox unchecked to hide the icon on each protected device. Your selection here is applied on all protected devices. The default is checked.
Show notification on file read attempt	Check this checkbox to enable notifications for file read attempts.
Show a pop-up message for any prevention activity	Check this checkbox to enable the display of pop-up messages (end-user notifications) on FortiEDR-protected devices. Pop-up messages display whenever a process was prevented. By default, the name of the activity of the blocked process is displayed in the pop-up message. The default is checked.

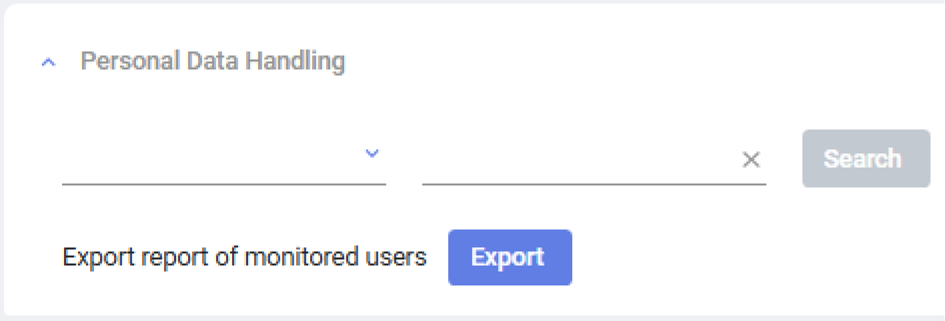
In the text box below the checkboxes, you can customize the text that is displayed in the pop-up message. Enter the text you want to display in the text box.

3. Click the *Save* button.

Personal Data Handling

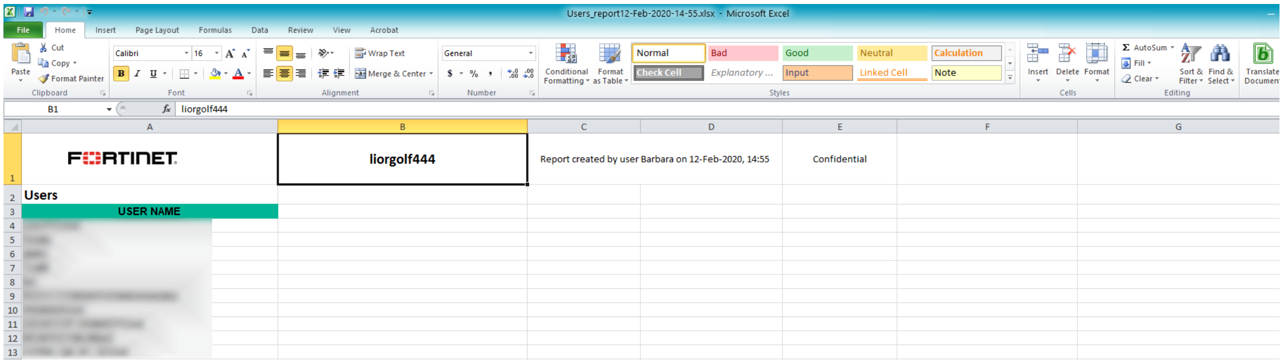
The FortiEDR system fully complies with the General Data Protection Regulation (GDPR) standard. The GDPR is a regulation in European Union (EU) law regarding data protection and privacy for all individuals within the EU and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA areas. The goal of the GDPR is primarily to give control to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

In FortiEDR, the GDPR feature is implemented in the *Personal Data Handling* section of the *Administration > Settings* page.



Use this section for the following GDPR compliance purposes:

- Remove all relevant data for an employee of a company that is using the FortiEDR system or a FortiEDR user from the FortiEDR system, once he/she no longer has access to or uses the FortiEDR system. The data includes the employee's/user's device name, IP address, MAC address, and user name.
- Notify your users, should the FortiEDR system be hacked. To export the list of monitored users in the FortiEDR system, use the *Export report of monitored users* button. See example report below:



liorgolf444

Report created by user Barbara on 12-Feb-2020, 14:55

Confidential

Users

USER NAME

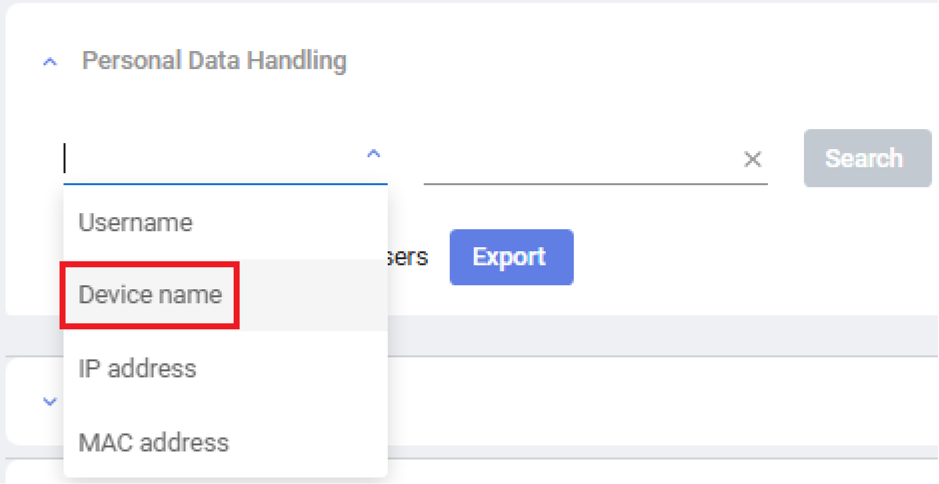
[redacted]

To remove employee/user data from the FortiEDR system for GDPR compliance:

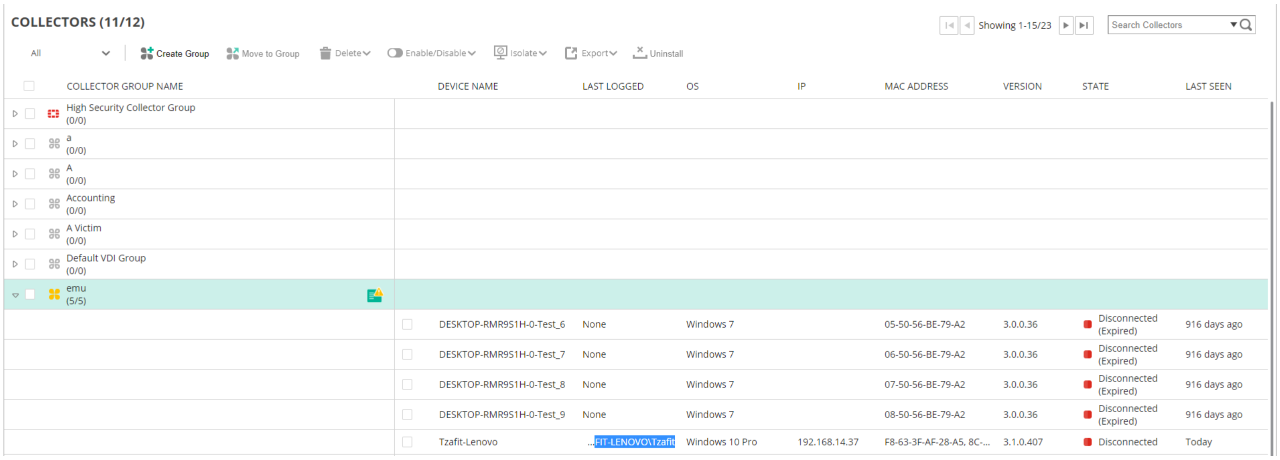
1. Uninstall the Collector from the employee's/user's computer. This step is important, so that no further data is collected from that Collector. For more details about uninstalling, see Uninstalling FortiEDR Collectors on page 70.
2. Navigate to the *Administration > Settings* page.
3. Expand the *Personal Data Handling* section, specify the device name, IP address, MAC address, or user name of the employee/user to be removed from FortiEDR.

You must remove all device name, IP address, MAC address, and user name data from FortiEDR in order to fully comply with the GDPR standard. This is an iterative process that must be performed four times in order to remove the device name, IP address, MAC address, and user name of the employee/user successively, one after another. You can remove this data in any order that you prefer. This example starts by removing all Device name data for the employee/user.

4. In the *Search by* dropdown list, select *Device name*. This field determines which criterion to search for in the FortiEDR system (device name, IP address, MAC address or user name).
5. In the adjacent field, enter the device name for the employee/user whose data you want to remove.



You can copy/paste this information into the adjacent field after locating it elsewhere in the FortiEDR user interface. For example, you can locate the relevant device name in the Last Logged column in the Collectors list in the Inventory window, such as shown below, and then copy that value into the relevant field in the *Personal Data Handling* area. Similarly, you can also readily locate the MAC address and IP address using the Collectors list in the *Inventory* window.

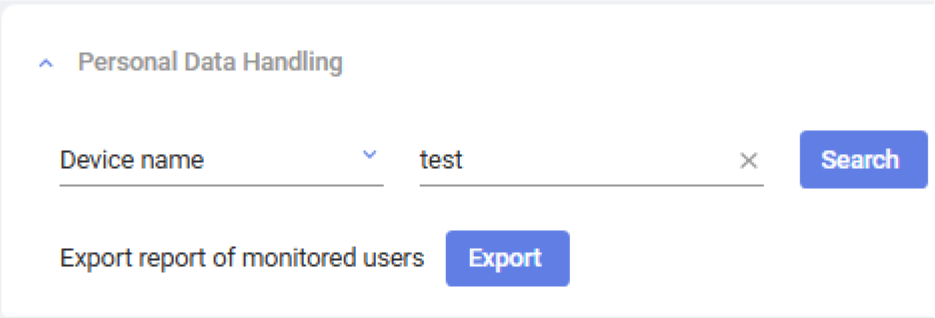


COLLECTORS (11/12)

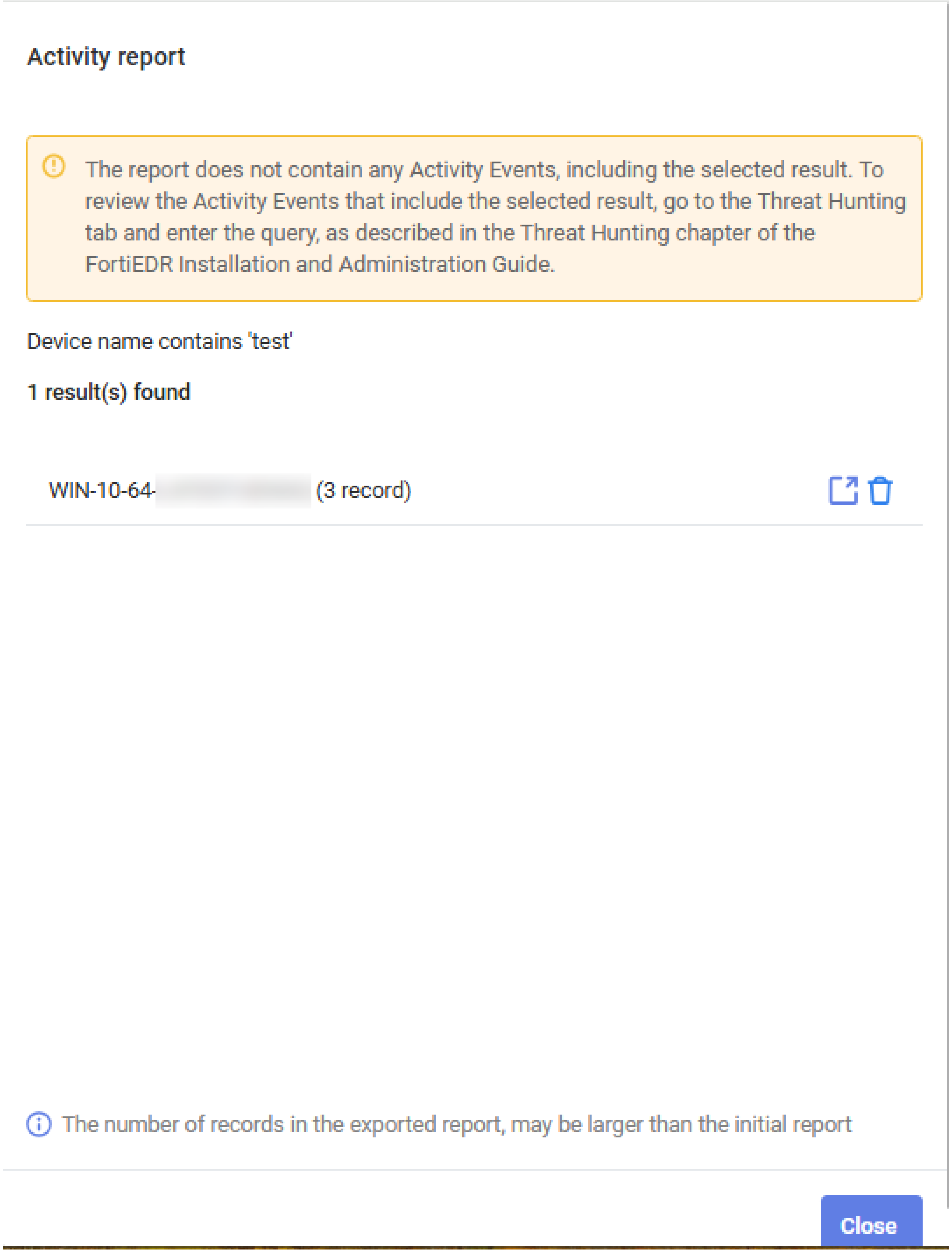
COLLECTOR GROUP NAME	DEVICE NAME	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	STATE	LAST SEEN
High Security Collector Group (0/0)								
a (0/0)								
A (0/0)								
Accounting (0/0)								
A Victim (0/0)								
Default VDI Group (0/0)								
emu (5/5)								
	DESKTOP-RMR9S1H-0-Test_6	None	Windows 7		05-50-56-BE-79-A2	3.0.0.36	Disconnected (Expired)	916 days ago
	DESKTOP-RMR9S1H-0-Test_7	None	Windows 7		06-50-56-BE-79-A2	3.0.0.36	Disconnected (Expired)	916 days ago
	DESKTOP-RMR9S1H-0-Test_8	None	Windows 7		07-50-56-BE-79-A2	3.0.0.36	Disconnected (Expired)	916 days ago
	DESKTOP-RMR9S1H-0-Test_9	None	Windows 7		08-50-56-BE-79-A2	3.0.0.36	Disconnected (Expired)	916 days ago
	Tzafit-Lenovo	...FIT-LENOVO\Tzafit	Windows 10 Pro	192.168.14.37	F8-63-3F-AF-28-A5, 8C-...	3.1.0.407	Disconnected	Today

If you prefer, you can use another method of your choice to identify the device name.

6. After entering the details for the device name, click *Search* to search for all occurrences of the device name in the FortiEDR system.



The following displays, listing all matching results.



Activity report

The report does not contain any Activity Events, including the selected result. To review the Activity Events that include the selected result, go to the Threat Hunting tab and enter the query, as described in the Threat Hunting chapter of the FortiEDR Installation and Administration Guide.

Device name contains 'test'

1 result(s) found

WIN-10-64-[redacted] (3 record)

The number of records in the exported report, may be larger than the initial report

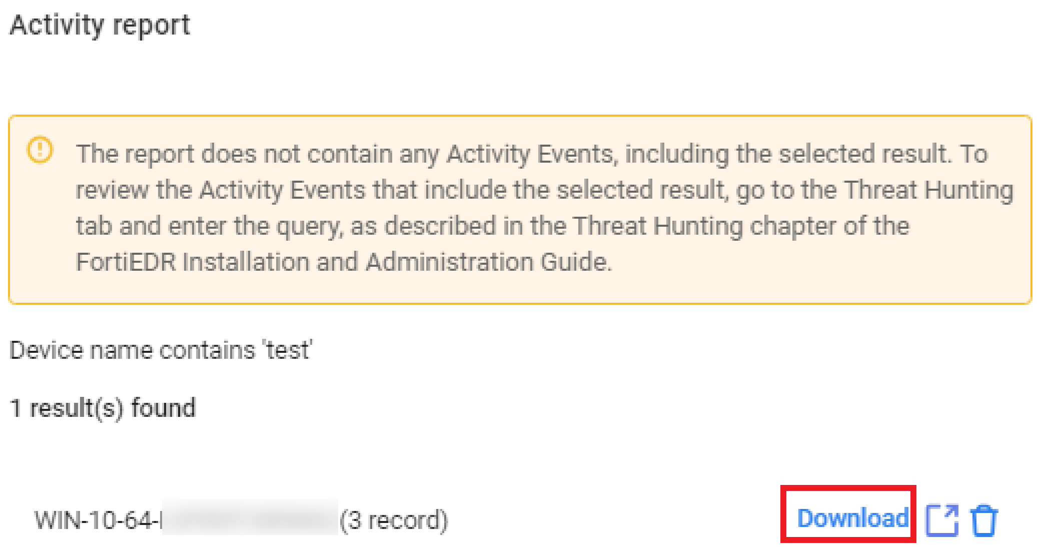
Threat hunting activity event data is not included in the search result but will be deleted. To see the activity data that will be deleted, use the Search option of the Threat Hunting feature, as described in Threat Hunting on page 125.

7. Select an entry in the search result list and do one of the following:

- To verify the data or to keep a record of the data:

  i. Click the *Export* (↗) icon to export the data to a report.

  ii. When the report is ready, click the *Download* link to download the Excel report.



Activity report

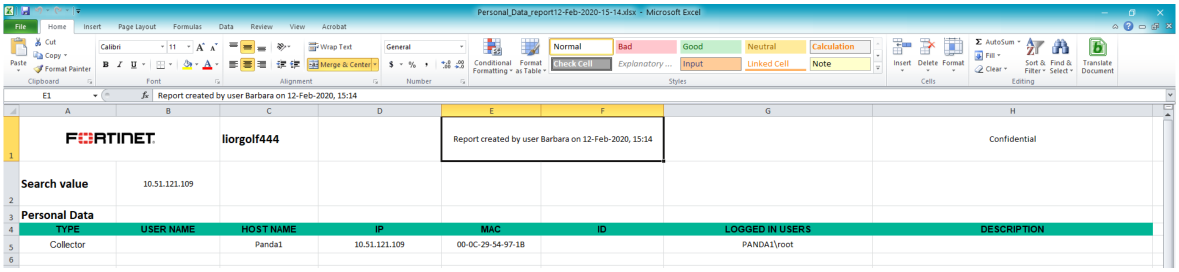
The report does not contain any Activity Events, including the selected result. To review the Activity Events that include the selected result, go to the Threat Hunting tab and enter the query, as described in the Threat Hunting chapter of the FortiEDR Installation and Administration Guide.

Device name contains 'test'

1 result(s) found

WIN-10-64-[redacted] (3 record)

See example report below:



Personal_Data_report12-Feb-2020-15-14.xlsx - Microsoft Excel

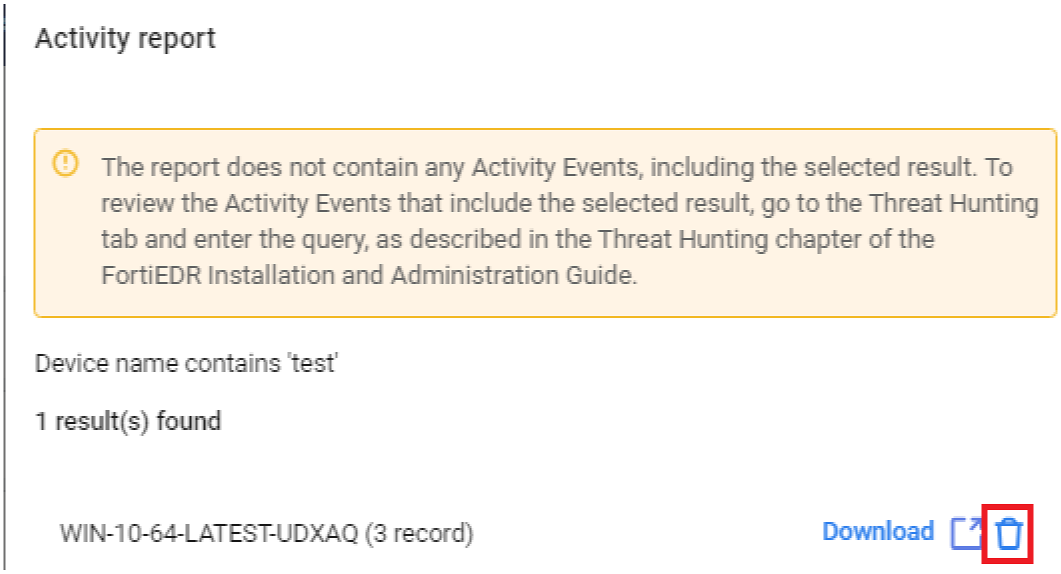
E1 — Report created by user Barbara on 12-Feb-2020, 15:14

FORTINET	liorgolf444		Report created by user Barbara on 12-Feb-2020, 15:14			Confidential
Search value	10.51.121.109					
Personal Data						

TYPE	USER NAME	HOST NAME	IP	MAC	ID	LOGGED IN USERS	DESCRIPTION
Collector		Panda1	10.51.121.109	00-0C-29-54-97-1B		PANDA1\root	

GDPR compliance requires that all traces of the employee's/user's data be permanently removed, including this report.

- To remove all the data for the employee/user, click the *Delete* () icon.



Activity report

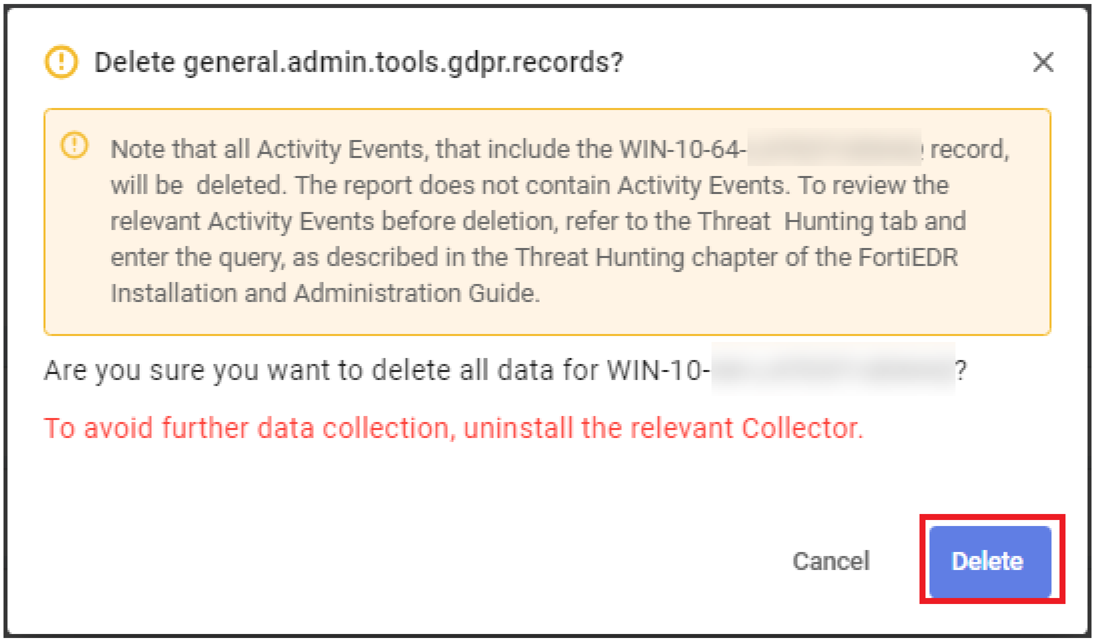
The report does not contain any Activity Events, including the selected result. To review the Activity Events that include the selected result, go to the Threat Hunting tab and enter the query, as described in the Threat Hunting chapter of the FortiEDR Installation and Administration Guide.

Device name contains 'test'

1 result(s) found

WIN-10-64-LATEST-UDXAQ (3 record)

i. Click *Delete* to remove all device name data for the employee/user from FortiEDR.



Delete general.admin.tools.gdpr.records?

Note that all Activity Events, that include the WIN-10-64-[redacted] record, will be deleted. The report does not contain Activity Events. To review the relevant Activity Events before deletion, refer to the Threat Hunting tab and enter the query, as described in the Threat Hunting chapter of the FortiEDR Installation and Administration Guide.

Are you sure you want to delete all data for WIN-10-[redacted]?

To avoid further data collection, uninstall the relevant Collector.

The data is deleted from FortiEDR in real time, from everywhere that it appears in the FortiEDR system (for example, from the *Inventory*, *Incidents* tab, Audit Trail and so on).

8. Click *Continue* to proceed with removing the other required data for the employee/user (IP address, MAC address and user name).
9. Repeat steps 4–8 to remove the relevant IP address from FortiEDR. Be sure to select *IP Address* in step 4.
10. Repeat steps 4–8 to remove the relevant MAC address from FortiEDR. Be sure to select *MAC Address* in step 4.
11. Repeat steps 4–8 to remove the relevant user name data from FortiEDR. Be sure to select *User Name* in step 4.
12. Delete any reports that might include data about this user as required by GDPR.

13. If the employee/user has multiple computers on which Collectors are installed, repeat the steps above for each of his/her computers.

IoT Device Discovery

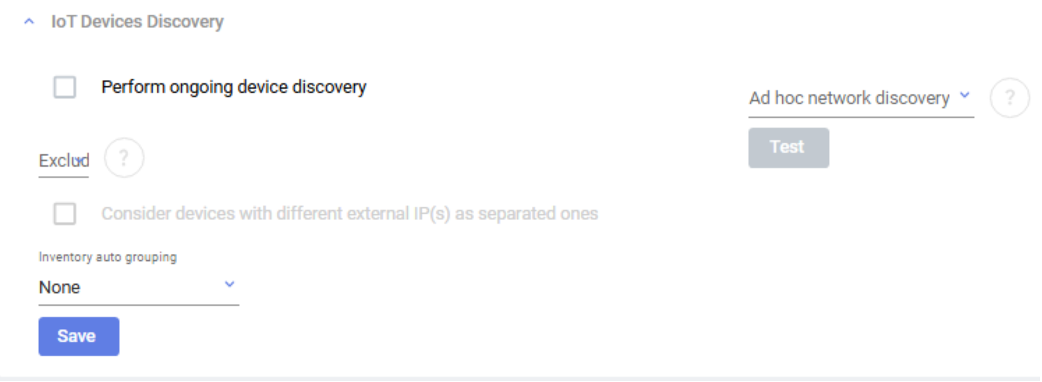
IoT device discovery enables you to continuously perform discovery to identify newly connected non-workstation devices in the system, such as printers, cameras, media devices and so on. During the discovery process, each relevant Collector in the system periodically probes all its nearby neighboring devices. Most nearby devices will respond to these requests by pinging the originating Collector device and providing information about itself, such as its device/host name (for example, ABC PC, Camera123), IP address and so on.

Such discovered devices can be seen in the *IOT DEVICES* page, as described in IoT devices on page 269.

The following default configuration applies to IoT scans by the FortiEDR Collectors:

- For operational reasons, Collectors that are running on servers or Collectors that are reported to be in one of the following states: degraded, disabled or isolated. Collectors do not take part in the IoT probing process.
- In order to refrain from scans on home or other non-enterprise networks, only subnets in which there is a minimal number of Windows Collectors are scanned in order to find Connected IoT devices.
- Extremely large subnets are excluded from scans.

If needed, in order to tune the scans to be more comprehensive and more granular, contact Fortinet Support who will change the default configuration.



IoT Devices Discovery

□ Perform ongoing device discovery

Ad hoc network discovery

Exclud

□ Consider devices with different external IP(s) as separated ones

Inventory auto grouping: None

To enable IoT device discovery, check the *Perform ongoing device discovery* checkbox. Note that when doing so, all relevant Collectors in the system perform sniffing in order to identify new connected devices in the system. When performing this discovery process, FortiEDR uses only the most powerful Collectors in each sub-network to perform sniffing, and excludes weaker Collectors for this process (disabled and degraded Collectors). This means that FortiEDR collects all the required information in the most efficient manner possible.

You can exclude specific Collector Groups from this discovery process. To do so, select the relevant Collector Group(s) in the *Exclude Collector Groups* dropdown list.

By default and when your organization has more than a single external IP address, FortiEDR ignores the external IP address of the IoT device while identifying and matching them. You can choose to list devices that use different external IP addresses separately by unchecking the checkbox next to the *Consider devices with different external IP(s) as separated ones* option. However, in this case the same device might be listed more than once in the *IoT inventory* page.

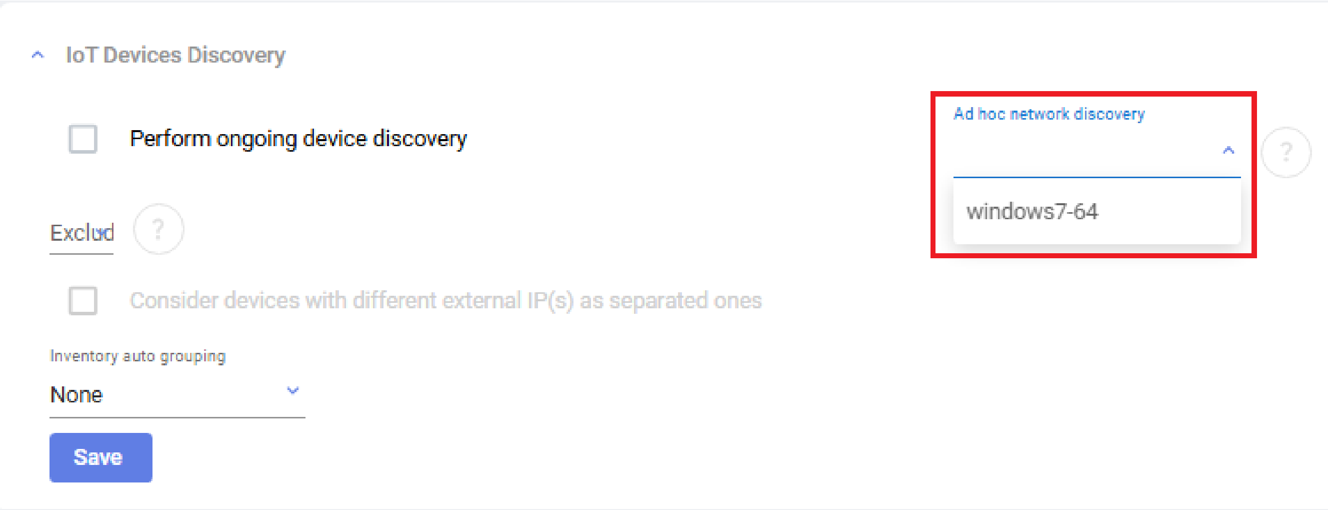
The Inventory *Auto Grouping* option enables you to group discovered devices by device type. For example, cameras, network devices, media devices, printers and so on. Select the *Category* option in the dropdown list to group discovered devices by device type or *None*. When you select *Category*, devices are auto-grouped in the *IOT DEVICES* page, as shown on IoT devices on page 269.

Click *Save* to save the configuration.

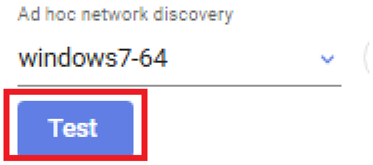
We recommend testing IoT the device discovery process to ensure that it works as expected across all your organizations before enabling the on-going periodic network scan. Testing can only be performed when IoT device discovery is not enabled, meaning the *Perform ongoing device discovery* checkbox is not checked. Select the Collector to use to test the IoT device discovery process in the *Ad Hoc Network Discovery* dropdown list and then click the *Test* button, as shown below.

You can search in the *Ad Hoc Network Discovery* dropdown list. For example, searching for "a" results in all collectors with letter "a" in their name being displayed in the list. An exception is when the search results list includes more than 100 entries, only exact matches will be displayed. If no exact match is found, the list will be empty.

If searching for a single letter or a broad term does not return the expected results, we recommend entering at least three or more specific characters in the search box to narrow down the list and ensure the correct collectors are displayed.

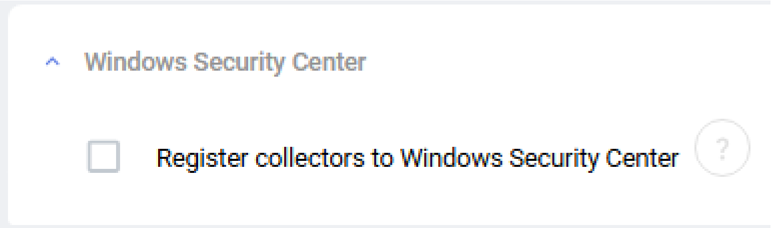

IoT Devices Discovery
Perform ongoing device discovery
Exclud
?
Consider devices with different external IP(s) as separated ones
Inventory auto grouping
None
Save
Ad hoc network discovery
windows7-64
?

The selected Collector sniffs the network once to identify new connected devices. After the test discovery process begins, you can stop it at any time by clicking the *Stop* button. In all cases, the scan will be stopped within a predefined time period (usually 30 minutes).



Windows Security Center

FortiEDR is fully integrated with Windows Security Center and has been certified by Microsoft as an anti-virus and threat protection application. You can choose whether to register FortiEDR Collectors as anti-virus and threat protection agents in Windows Security Center. The default is no registration. The registration status has no impact on FortiEDR protection.



Windows Security Center

□ Register collectors to Windows Security Center

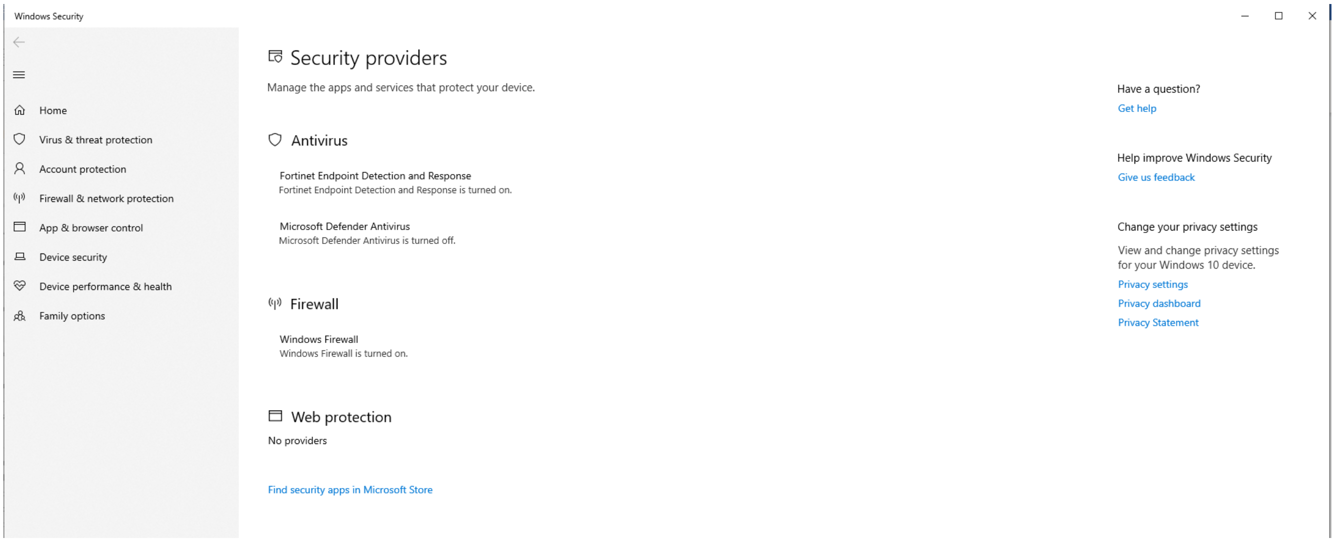
When multiple AV products are installed, refer to the following guidelines for configuring this option:

- To consolidate all SOC activities to FortiEDR, you must register FortiEDR Collectors with Windows Security Center.
- To maximize protection from multiple AV products without the need of SOC activity consolidation in FortiEDR, do not register FortiEDR Collectors with Windows Security Center as the registration may prevent other AV products from installing or functioning properly.

To register FortiEDR Collectors with Windows Security Center:

In the *Administration > Settings* page, expand the *Windows Security Center* section and check the *Register collectors to Windows Security Center* checkbox.

When registered, FortiEDR will be listed under *Windows Security* (as shown below) and all SOC activities will be consolidated to FortiEDR if multiple AV products are installed.



Security providers

Manage the apps and services that protect your device.

Antivirus

Fortinet Endpoint Detection and Response
Fortinet Endpoint Detection and Response is turned on.

Microsoft Defender Antivirus
Microsoft Defender Antivirus is turned off.

Firewall

Windows Firewall
Windows Firewall is turned on.

Web protection

No providers

Find security apps in Microsoft Store

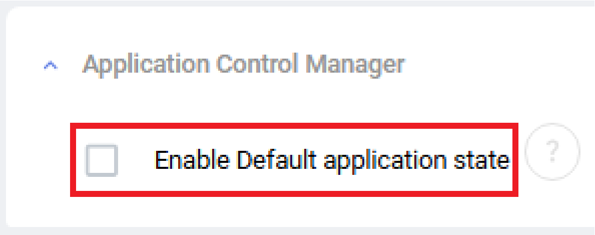
Have a question?
Get help

Help improve Windows Security
Give us feedback

Change your privacy settings
View and change privacy settings for your Windows 10 device.
Privacy settings
Privacy dashboard
Privacy Statement

Application Control Manager

Under *Security Settings* > *Application Control on page 223*, the default block state of new applications is disabled, which means new applications are not blocked by default. To change the default block state of new applications so that they are blocked by default, check the *Enable Default application state* option under *Administration* > *Settings* > *Application Control Manager*.



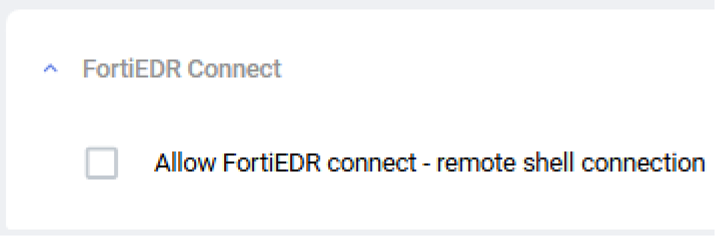
Application Control Manager

□ Enable Default application state

FortiEDR Connect

The FortiEDR Connect feature opens a console that provides direct access to FortiEDR-protected devices (endpoints) that are running a Windows operating system through a remote Shell connection, as described in FortiEDR Connect on page 109. This enables you to respond to incidents immediately and to perform in-depth investigation by running commands on the device, running scripts on the device, collecting and downloading forensic data from the device, remediating threats and so on.

Select the *Allow FortiEDR connect - remote shell connection* checkbox to enable the FortiEDR Connect functionality for the organization. Otherwise, the *Connect to Device* button is deactivated for all users of the organization.



FortiEDR Connect

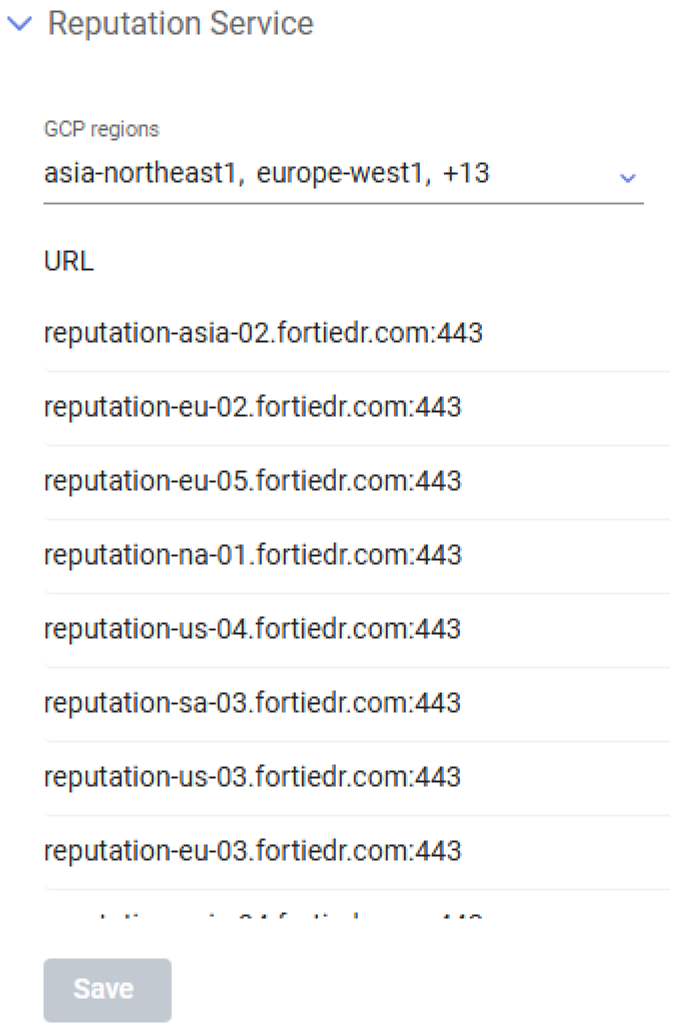
□ Allow FortiEDR connect - remote shell connection

To further allow a user access to the FortiEDR Connect functionality, select the *Establish FortiEDR Connect sessions* checkbox in the user profile. Otherwise, the *Connect to Device* button is deactivated for the user. For more information about user roles and permissions, see Users on page 277.

The *Establish FortiEDR Connect sessions* checkbox is available for Admin, Analyst, and Senior Analyst users only.

Reputation Service

This section displays a list of GCP regions where a reputation service instance is installed on and the relevant URLs of all selected regions. You can select any region you want to connect to. By default, all regions are selected. When a region is selected, the relevant reputation service URLs are displayed so that you can open them in your firewall.



GCP regions: asia-northeast1, europe-west1, +13

URL

reputation-asia-02.fortiedr.com:443

reputation-eu-02.fortiedr.com:443

reputation-eu-05.fortiedr.com:443

reputation-na-01.fortiedr.com:443

reputation-us-04.fortiedr.com:443

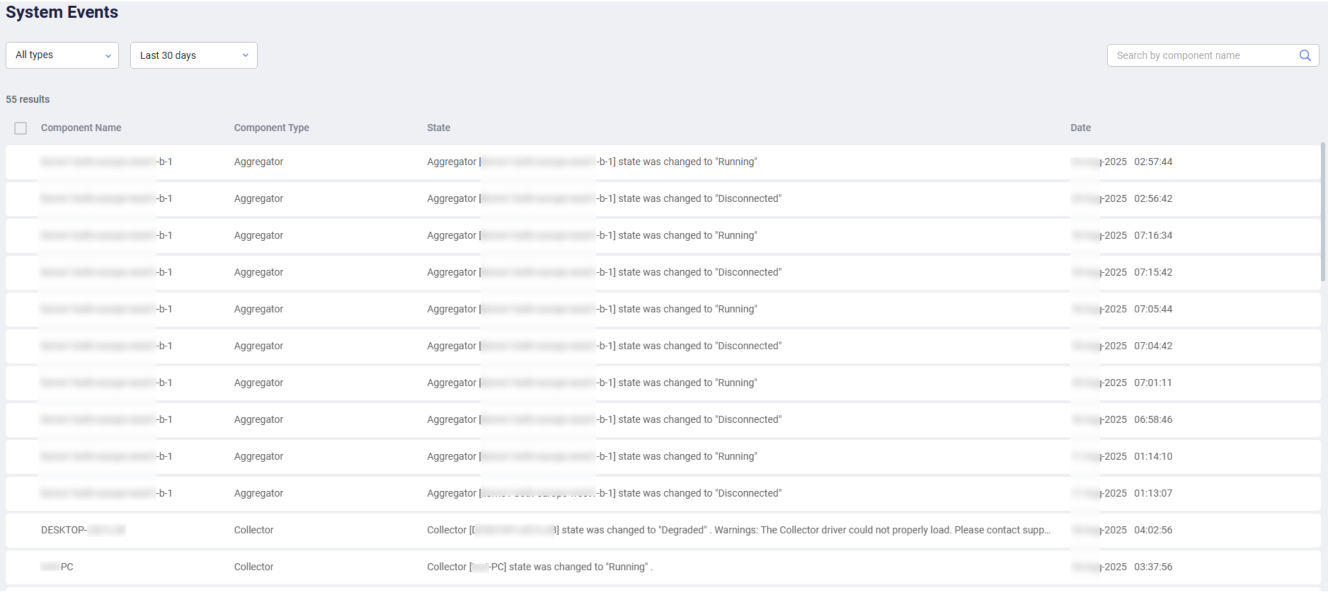
reputation-sa-03.fortiedr.com:443

reputation-us-03.fortiedr.com:443

reputation-eu-03.fortiedr.com:443

System events

Selecting *SYSTEM EVENTS* in the *ADMINISTRATION* tab displays all the system events relevant to the FortiEDR system.



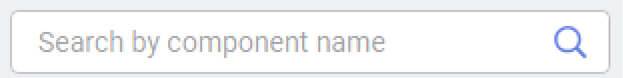
System Events

All types | Last 30 days | Search by component name

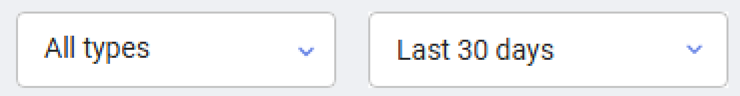
55 results

☐ Component Name	Component Type	State	Date
[redacted]-b-1	Aggregator	Aggregator [[redacted]-b-1] state was changed to "Running"	[redacted]-2025 02:57:44
[redacted]-b-1	Aggregator	Aggregator [[redacted]-b-1] state was changed to "Disconnected"	[redacted]-2025 02:56:42
[redacted]-b-1	Aggregator	Aggregator [[redacted]-b-1] state was changed to "Running"	[redacted]-2025 07:16:34
[redacted]-b-1	Aggregator	Aggregator [[redacted]-b-1] state was changed to "Disconnected"	[redacted]-2025 07:15:42
[redacted]-b-1	Aggregator	Aggregator [[redacted]-b-1] state was changed to "Running"	[redacted]-2025 07:05:44
[redacted]-b-1	Aggregator	Aggregator [[redacted]-b-1] state was changed to "Disconnected"	[redacted]-2025 07:04:42
[redacted]-b-1	Aggregator	Aggregator [[redacted]-b-1] state was changed to "Running"	[redacted]-2025 07:01:11
[redacted]-b-1	Aggregator	Aggregator [[redacted]-b-1] state was changed to "Disconnected"	[redacted]-2025 06:58:46
[redacted]-b-1	Aggregator	Aggregator [[redacted]-b-1] state was changed to "Running"	[redacted]-2025 01:14:10
[redacted]-b-1	Aggregator	Aggregator [[redacted]-b-1] state was changed to "Disconnected"	[redacted]-2025 01:13:07
DESKTOP-[redacted]	Collector	Collector [D[redacted]] state was changed to "Degraded" . Warnings: The Collector driver could not properly load. Please contact supp...	[redacted]-2025 04:02:56
[redacted]PC	Collector	Collector [[redacted]-PC] state was changed to "Running" .	[redacted]-2025 03:37:56

Use the search bar on the top right corner to filter system events by keywords.



Use the following filters to filter system events by component with a date range.



System events can also be retrieved using an API command. For more details, refer to the FortiEDR RESTful API Guide. You must log in to the Fortinet Developer Network to access the guide.

Each time a system event is triggered and created, the user receives an email notification for each of them if that system event is enabled for the user's Distribution lists on page 307. You can also configure Syslog on page 310 to send system events messages.

The following events are defined as system events in the system:

- Core state was changed to Disconnected (and another event when the Core state was returned to the Connected state immediately afterward)
- Core state was changed to Degraded (and another event when the Core state was returned to THE Connected state immediately afterward)
- Aggregator state was changed to Disconnected (and another event when the Aggregator state was returned to the Connected state immediately afterward)
- Aggregator state was changed to Degraded (and another event when the Aggregator state was returned to the Connected state immediately afterward)
- Threat Hunting Repository state was changed to Disconnected (and another event when the Repository state was returned to the Connected state immediately afterward).

- Threat Hunting Repository state was changed to Degraded (and another event when the Repository state was returned to the Connected state immediately afterward).
- Collector registered for the first time (only UI/API; is not sent by email/Syslog)
- Collector was uninstalled via the Central Manager console
- Collector state was changed to Disconnected Expired
- Collector state was changed to Degraded

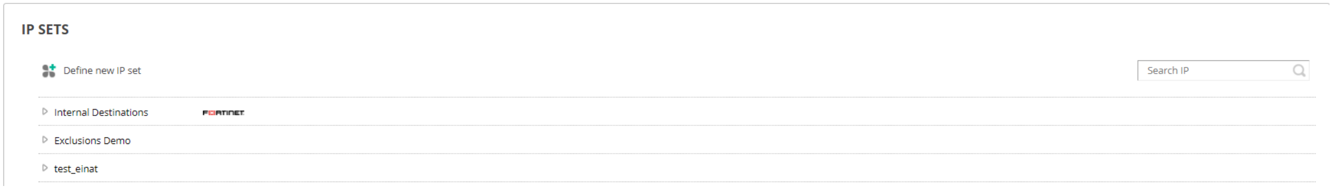
This event is disabled by default. To enable it, please contact Fortinet support to apply a configuration change on the backend.

- License will expire in 21/7 days/1 day
- License expired
- License capacity of workstations has reached 90/95/100%
- License capacity of servers has reached 90/95/100%
- System mode was changed from Prevention to Simulation or vice versa
- FortiEDR Cloud Service (FCS) connectivity is down

IP sets

IP Sets enable you to define a set(s) of IPs to include or exclude for some security events. This feature is used when defining exceptions.

This page is only available to users with Admin, IT, or Senior Analyst permissions.

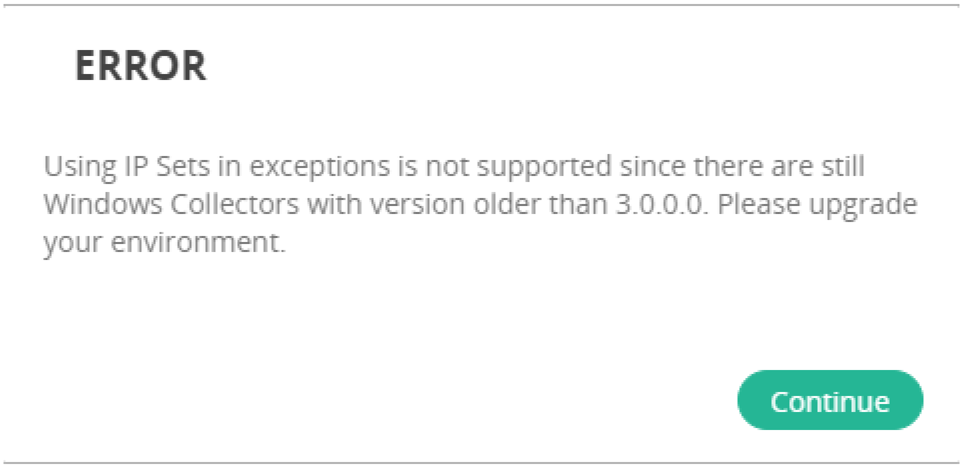

IP SETS

Define new IP set

Search IP

- Internal Destinations FORTINET
- Exclusions Demo
- test_einat

IP Sets can only be defined if all Collectors are V3.0.0.0 and up. If you attempt to define an exception and all Collectors are not V3.0.0.0 or above, the following error message displays:



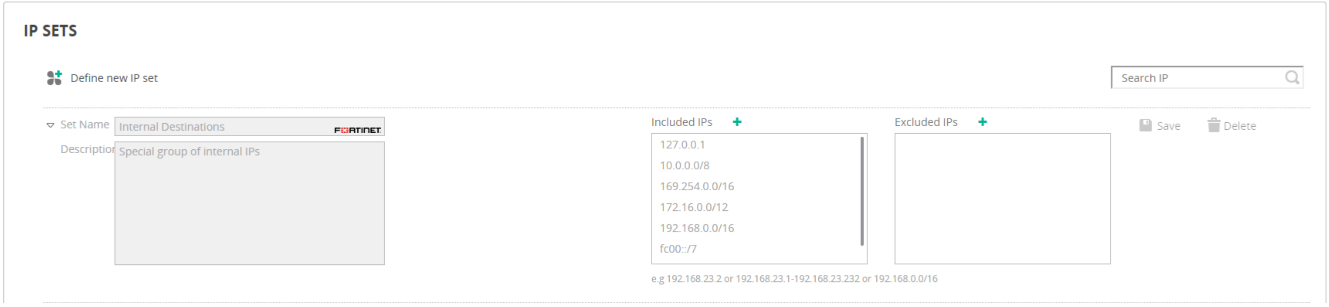
ERROR

Using IP Sets in exceptions is not supported since there are still Windows Collectors with version older than 3.0.0.0. Please upgrade your environment.

Each row in the IP Sets window represents an IP inclusion/exclusion definition. The *Internal Destinations* row is provided by default (as indicated by the adjacent FortiEDR logo), which defines the default IPs that are included in and excluded from the FortiEDR system. All organizations in a multi-organization system are provided with this default IP set. In a single-organization system, the main organization is provided with it. The Internal Destinations IP set cannot be deleted. However, an Administrator can add Included IPs or Excluded IPs to it.

The *IP Sets* page lists all the IP sets. Users can only edit an IP set that was specifically created for his/her organization. For example, if the administrator is assigned to only organization A, he/she can edit an IP set create for organization A but not an IP set that applies to all organizations.

Click the FORTINET logo in the Internal Destinations row to view its definition, as shown below:



IP SETS

Set Name: Internal Destinations

Description: Special group of internal IPs

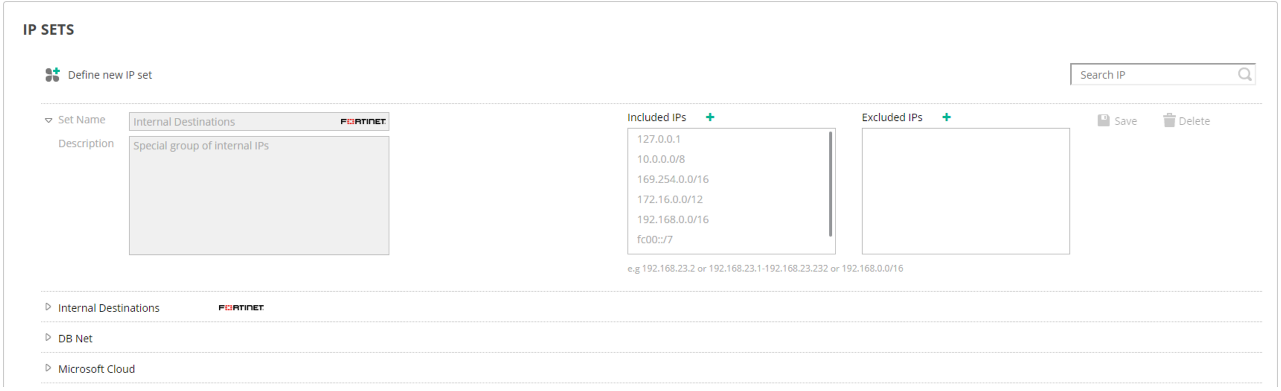
Included IPs:
127.0.0.1
10.0.0.0/8
169.254.0.0/16
172.16.0.0/12
192.168.0.0/16
fc00::/7

Excluded IPs:

e.g 192.168.23.2 or 192.168.23.1-192.168.23.232 or 192.168.0.0/16

To define an IP set:

1. Click the *Define new IP set* button (Define new IP set) button. The following window displays:



Set Name: Internal Destinations

Description: Special group of internal IPs

Included IPs:

```
127.0.0.1
10.0.0.0/8
169.254.0.0/16
172.16.0.0/12
192.168.0.0/16
fc00::/7
```

e.g 192.168.23.2 or 192.168.23.1-192.168.23.232 or 192.168.0.0/16

2. In the *Set Name* field, enter a name for the IP set.
3. In the *Organization* dropdown list, select the organization to which the IP set applies or select All organizations for the IP set to apply to all organizations in the FortiEDR system.
4. In the *Description* field, enter a description for the IP set.
5. In the *Included IPs* area, click the *Add* button (+) to add an IP, IP range, or IP mask to be included in the IP set's definition. Each click of the *Add* button (+) adds a new line to the list. Each entry appears in its own line. For example, you could add 192.168.23.2, 192.168.23.1-192.168.232 or 192.168.0.0/16. Similarly, in the *Excluded IPs* area, click the *Add* button (+) to add an IP, IP range, or IP mask that is to be excluded.
6. Click the *Save* button.

The *Search IP* field at the top-right of the page enables you to search for a specific IP in all of the IP sets defined. The search option identifies matching IPs, even if they are part of a range in an IP set's definition.

To use an IP set:

Select an IP set in the *Destinations* area when defining an exception.

Connectors

Connectors enable you to configure connectors to external systems, which enables you to trigger predefined types of actions. FortiEDR provides various connectors out-of-the-box, such as Firewalls and NAC systems. The out-of-the-box FortiEDR connectors utilize Fortinet products' APIs to automatically perform the required actions in order to extend its automatic Playbook actions.

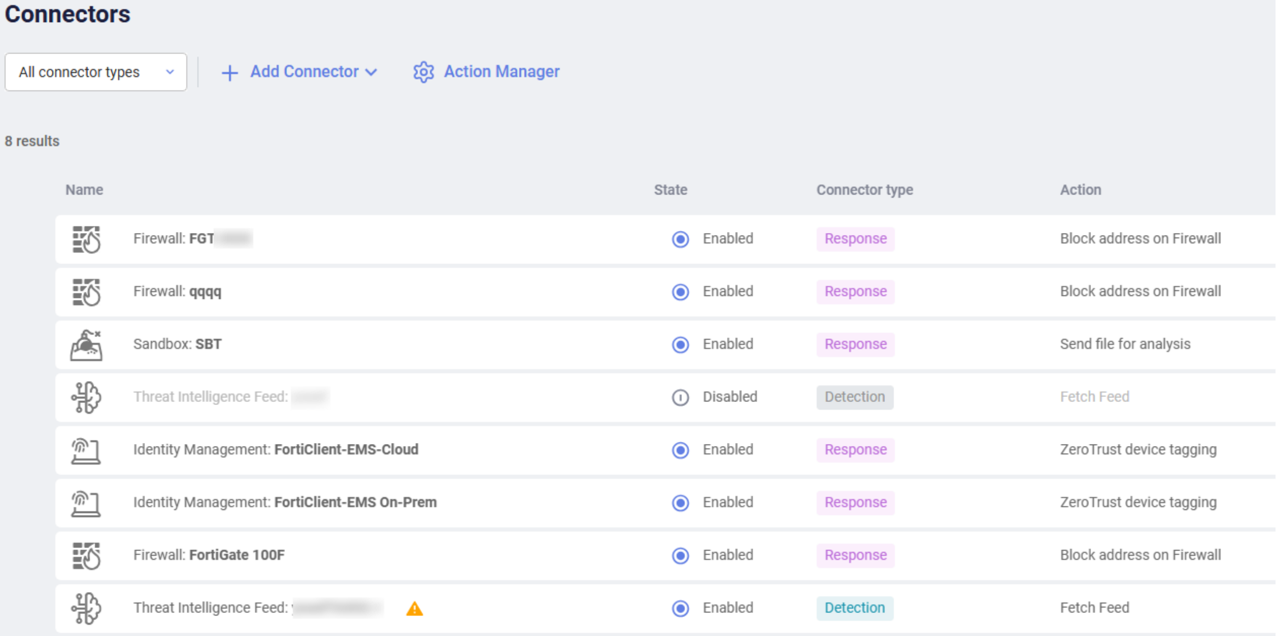
Admin and IT users with custom script permission can also define customized connectors to any third-party system in order to trigger any action on that system using an API. For more information about user roles and permissions, see Users on page 277.

You can set up an unlimited number of connectors for each type and use them by associating Playbook policies or Security policies to the actions defined for these integration connectors, as described below.

The *Connectors* menu is only available when the environment is connected to Fortinet Cloud Services (FCS).

To display the *Connectors* page:

1. Select *Administration* > *Connectors*.



Connectors

8 results

Name	State	Connector type	Action
Firewall: FGT[redacted]	Enabled	Response	Block address on Firewall
Firewall: qqqq	Enabled	Response	Block address on Firewall
Sandbox: SBT	Enabled	Response	Send file for analysis
Threat Intelligence Feed: [redacted]	Disabled	Detection	Fetch Feed
Identity Management: FortiClient-EMS-Cloud	Enabled	Response	ZeroTrust device tagging
Identity Management: FortiClient-EMS On-Prem	Enabled	Response	ZeroTrust device tagging
Firewall: FortiGate 100F	Enabled	Response	Block address on Firewall
Threat Intelligence Feed: [redacted] ⚠	Enabled	Detection	Fetch Feed

The top left of this page provides two buttons, as shown below:

- Adding connectors on page 340 enables you to add and configure connectors for integration with FortiEDR.
- Action Manager on page 393 enables you to upload and manage (add, modify and delete) actions (Python scripts that call third-party system APIs) to be automatically triggered by FortiEDR as incident responses. Python 2.7 or later is supported.

The *Action Manager* button is only available to users with Admin or IT permissions and have the *Custom script* option enabled. For more information about user roles and permissions, see Users on page 277.

Adding connectors

The following types of integration connectors are provided to be configured:

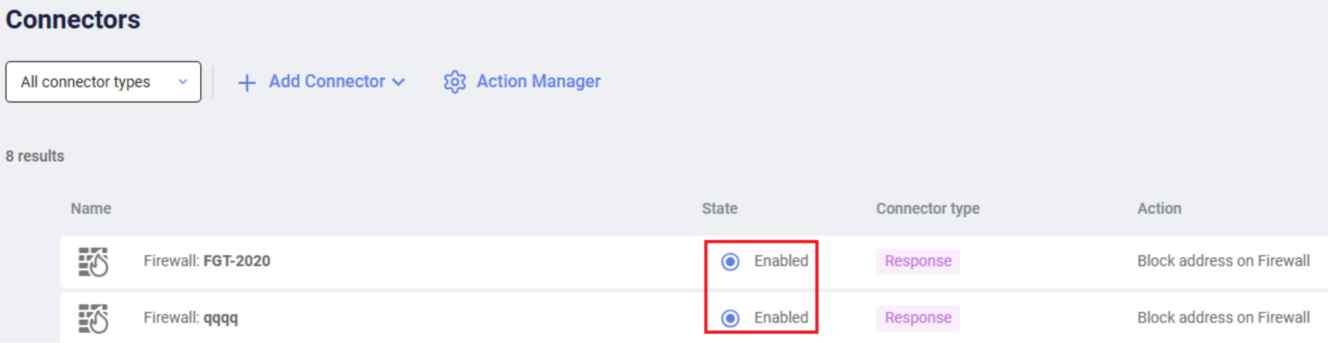
- Firewall integration on page 341
- Network Access Control (NAC) integration on page 350

- Sandbox integration on page 356
- eXtended detection source integration on page 358
- Custom integration on page 370

> Custom integration is only available to users with Admin or IT permissions and have the *Custom script* option enabled. For more information about user roles and permissions, see Users on page 277.

- Identity Management integration on page 376
- User Access integration on page 384
- Threat Intelligence Feed integration on page 391

You can enable or disable a connector by clicking the *Enabled/Disabled* button next to the connector name. This button toggles between *Enabled/Disabled*.



8 results

Name	State	Connector type	Action
Firewall: **FGT-2020**	● Enabled	Response	Block address on Firewall
Firewall: **qqqq**	● Enabled	Response	Block address on Firewall

Firewall integration

When a firewall connector is set and Playbook policies are configured, automatic incident response actions can include blocking of malicious IP addresses by a firewall upon security event triggering.

For more details about integrating FortiEDR with FortiGate or FortiManager, refer to the FortiGate Integration Guide or FortiManager Integration Guide.

Before you start firewall configuration, make sure that:

- Your FortiEDR deployment includes a Jumpbox that has connectivity to the firewall. Details about how to install a FortiEDR Core and configure it as a Jumpbox are described in Setting up the FortiEDR Core on page 511. You may refer to Cores on page 403 for more information about configuring a Jumpbox.
- The FortiEDR Central Manager has connectivity to the Fortinet Cloud Services (FCS).
- You have a valid API user with access to the external firewall. See the FortiGate Integration Guide or FortiManager Integration Guide for detailed instructions.

Follow the steps below to automatically deny access on the firewall to malicious destination addresses detected by FortiEDR.

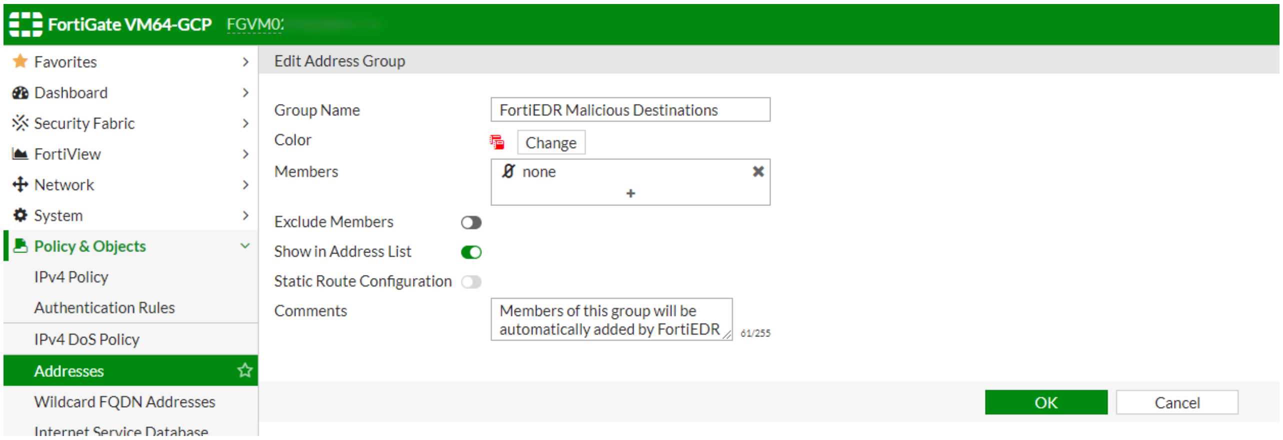
The example below describes how to define an address group on FortiGate and associate it with a FortiGate policy rule, such that it blocks connections to the addresses in the group. The address group is then used when configuring the FortiEDR connector so that it is automatically populated with malicious destinations upon detection by FortiEDR.

The same address group can obviously be used for multiple firewall policies in order to cover any VLAN-to-WAN interface in the network.

FortiGate configuration

To set up an address group and policy on FortiGate:

1. Go to *Policy & Objects* > *Addresses*.
2. Create a new address group to be populated by FortiEDR. The new address group now appears in the FortiGate Addresses table.



Edit Address Group

Group Name: FortiEDR Malicious Destinations

Color: Change

Members: none

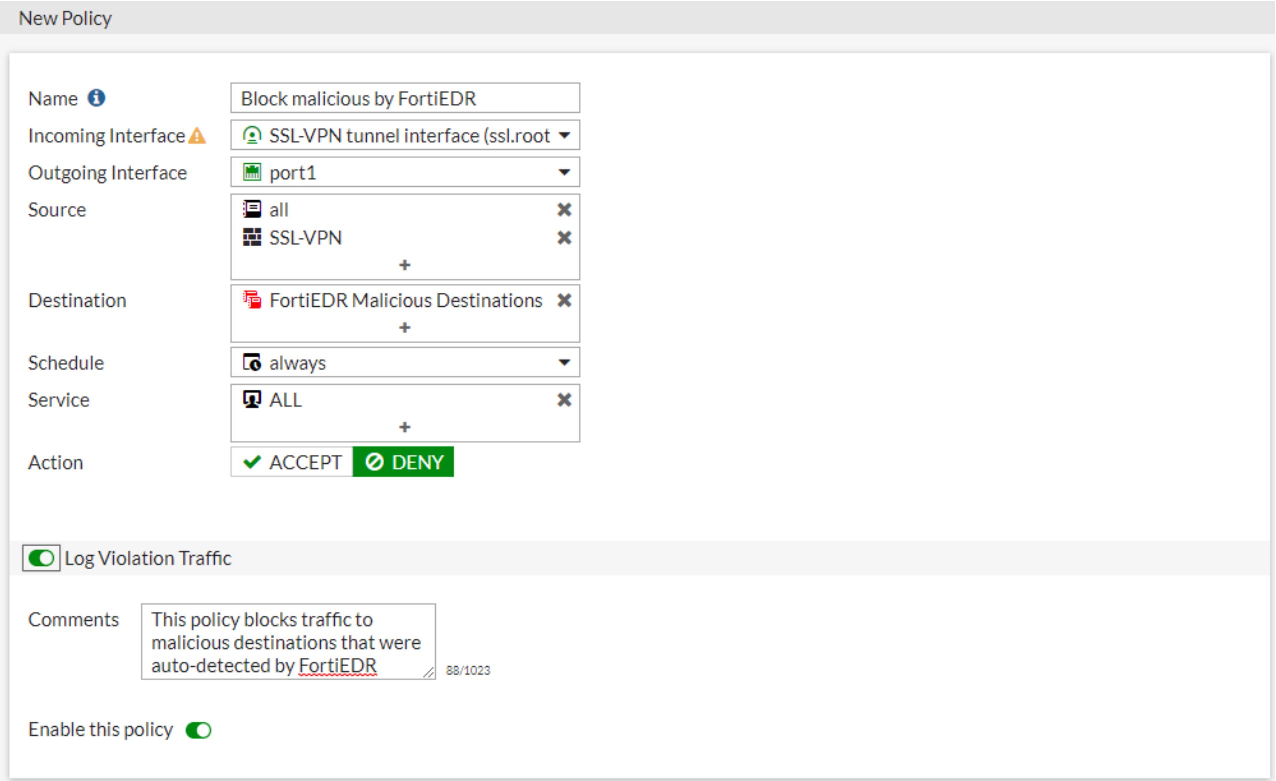
Exclude Members: ○

Show in Address List: ●

Static Route Configuration: ○

Comments: Members of this group will be automatically added by FortiEDR 61/255

3. Go to *Policy & Objects* > *IPv4 Policy*.
4. Create a new policy to deny traffic to any address in the address group that was created as part of step 2. The new policy now appears in the FortiGate Policies table.



New Policy

Name: Block malicious by FortiEDR

Incoming Interface: SSL-VPN tunnel interface (ssl.root

Outgoing Interface: port1

Source: all
SSL-VPN

Destination: FortiEDR Malicious Destinations

Schedule: always

Service: ALL

Action: ✓ ACCEPT | ⊘ DENY

Log Violation Traffic

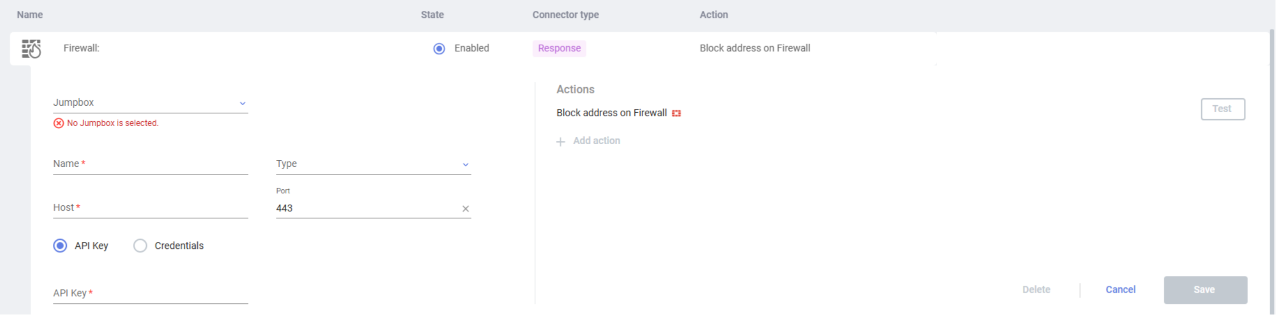
Comments: This policy blocks traffic to malicious destinations that were auto-detected by FortiEDR 88/1023

Enable this policy

FortiEDR firewall connector configuration

To set up a Firewall connector with FortiEDR:

1. Click the *Add Connector* button and select *Firewall* in the *Connectors* dropdown list. The following displays:



Name	State	Connector type	Action
Firewall:	● Enabled	Response	Block address on Firewall

Jumpbox

No Jumpbox is selected.

Name *

Type

Host *

Port: 443

● API Key ○ Credentials

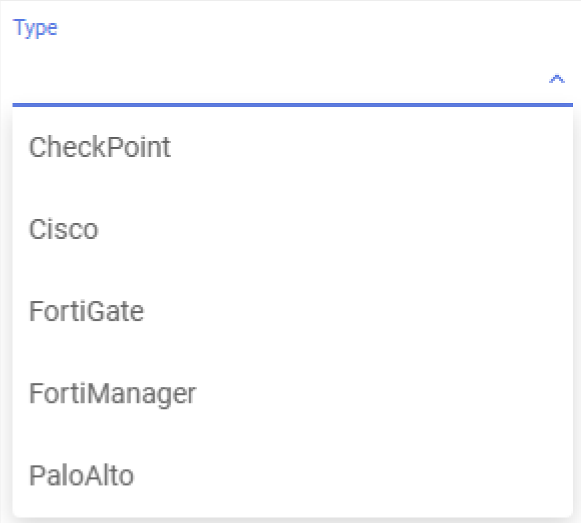
API Key *

Actions

Block address on Firewall

2. Fill in the following fields:

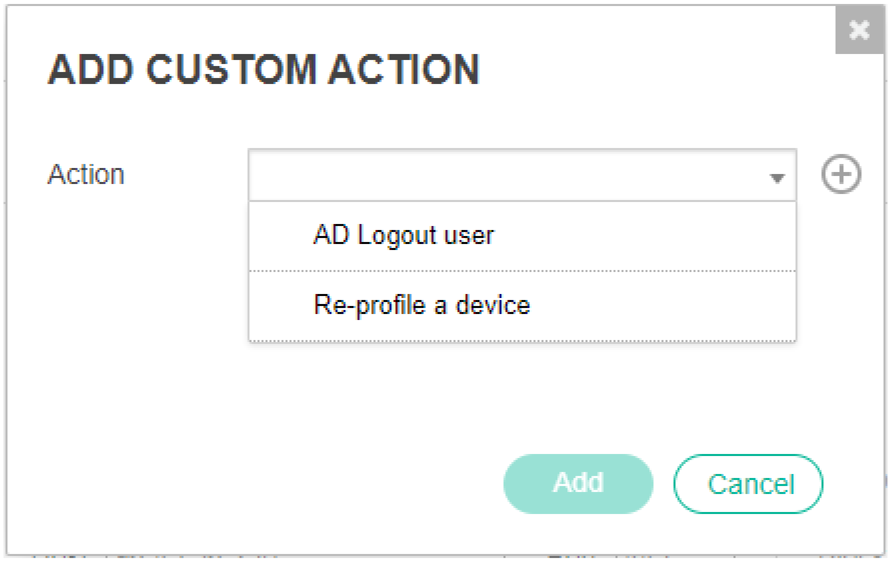
Field	Definition
Jumpbox	Select the FortiEDR Jumpbox to communicate with the firewall.
Name	Specify a name of your choice to be used to identify this firewall.
Type	Select the type of firewall to be used in the dropdown list.

Field	Definition
	 Type CheckPoint Cisco FortiGate FortiManager PaloAlto
Host	Specify the IP or DNS address of your firewall.
Port	Specify the port that is used for API communication with your firewall.
API Key / Credentials	Specify authentication details of your firewall. To use an API token, click the *API Key* radio button and copy the token value into the text box. To use API credentials, click the *Credentials* radio button and enter the Firewall API username and password.

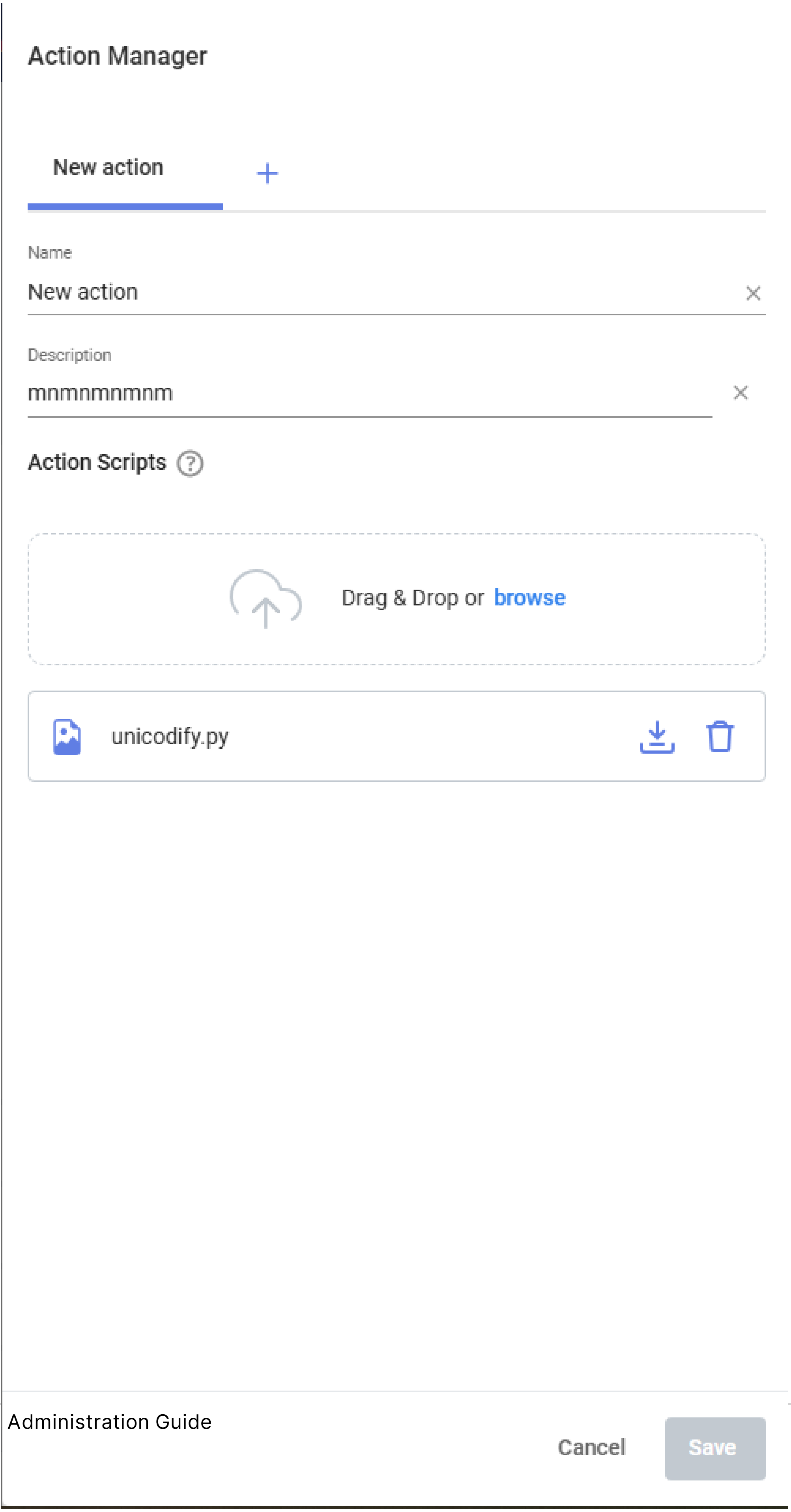
3. In the *Actions* area on the right, define an action to be taken by this connector.
You have the option to either use an action provided out-of-the-box with FortiEDR (for example, *Block address on Firewall*) or to create and use your own custom actions.

a. To block an address on the Firewall, in the *Address Group* field, specify the name of a previously defined address group on the firewall. For FortiManager and FortiGate integrations, you can optionally specify the name of the VDOM domain in the *VDOM* field. FortiEDR uses the default root VDOM if the *VDOM* field is empty.
- OR -

b. To trigger a custom action on the Firewall, click the *Add Action* button to display the following popup window:



- In the *Action* dropdown menu, select one of the previously defined custom integration actions (which were defined in FortiEDR as described in Custom integration on page 370).
  – OR –
- Click the *Create New Action* ⊕ button in this popup window to define a new action on the Firewall to be triggered according to the definitions in the Playbook, as described below. The following displays:



Action Manager

New action

Name: New action

Description: mnmnmnmnm

Action Scripts

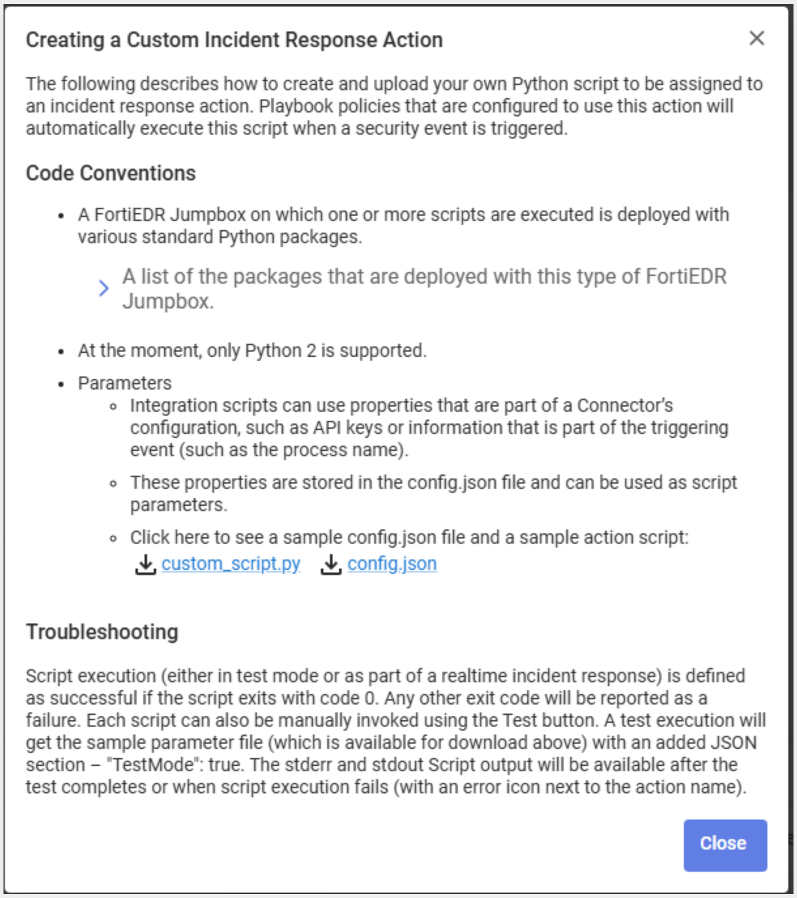
Drag & Drop or browse

unicodify.py

Fill out the fields of this window as follows in order to define a new action to be triggered in response to an incident.

In order to trigger this action, a Playbook policy must be defined that triggers this action to execute the script when a security event is triggered. The definition of this new action here automatically adds this action as an option in a Playbook policy. This action however, is not selected by default in the Playbook policy. Therefore, you must go to the Playbook policy and select it in order for it to be triggered when a security event is triggered.

Field	Definition
Name	Enter any name for this action.
Description	Enter a description of this action.
Upload	Upload a Python script that calls an API in the third-party system in order to perform the relevant action. Python 2.7 or later is supported. This Python script must be created according to the coding conventions that can be displayed by clicking the icon ⓘ next to the *Action Scripts* field. The following displays providing an explanation of these coding conventions and provides various links that you can click to see more detail and or/to download sample files.

Field	Definition
	 **Creating a Custom Incident Response Action** ✕ The following describes how to create and upload your own Python script to be assigned to an incident response action. Playbook policies that are configured to use this action will automatically execute this script when a security event is triggered. **Code Conventions** - A FortiEDR Jumpbox on which one or more scripts are executed is deployed with various standard Python packages. › A list of the packages that are deployed with this type of FortiEDR Jumpbox. - At the moment, only Python 2 is supported. - Parameters ◦ Integration scripts can use properties that are part of a Connector's configuration, such as API keys or information that is part of the triggering event (such as the process name). ◦ These properties are stored in the config.json file and can be used as script parameters. ◦ Click here to see a sample config.json file and a sample action script: custom_script.py config.json **Troubleshooting** Script execution (either in test mode or as part of a realtime incident response) is defined as successful if the script exits with code 0. Any other exit code will be reported as a failure. Each script can also be manually invoked using the Test button. A test execution will get the sample parameter file (which is available for download above) with an added JSON section – "TestMode": true. The stderr and stdout Script output will be available after the test completes or when script execution fails (with an error icon next to the action name). Close

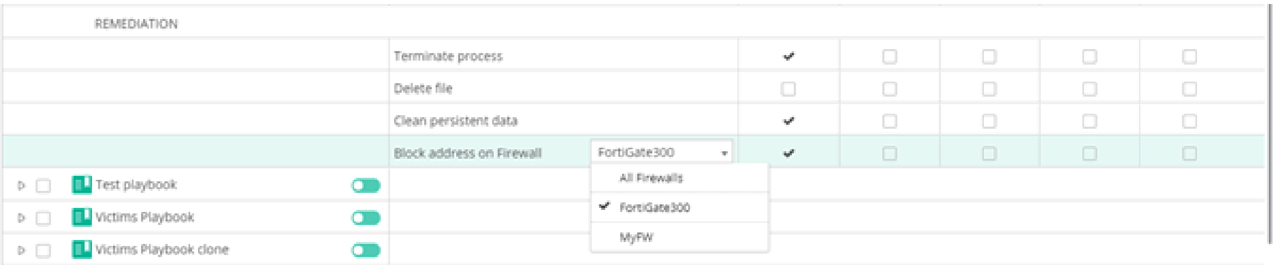
4. Click *Save*. The new action is then listed in the *Actions* area.
5. You can click the *Test* button next to an action to execute that action.

If you are working with a FortiManager in order to manage firewalls, use the same instructions to integrate with the firewall, but select *FortiManager* as the integrated device Type when configuring the FortiEDR Connector in the *Administration > Integration* page.

Playbooks configuration

To configure an automated incident response that uses a firewall connector to block malicious destinations upon security event triggering:

1. Navigate to the *SECURITY SETTINGS > Playbooks* page.
2. Open the Playbook policy that is applied on devices for which you want the block IP incident response to apply and place a checkmark in the relevant *Classification* column next to the *Block address on Firewall* row that is under the *REMEDIATION* section. In the dropdown menu next to the action, you can specify which firewalls to use to perform the block or select all of them, as shown below:



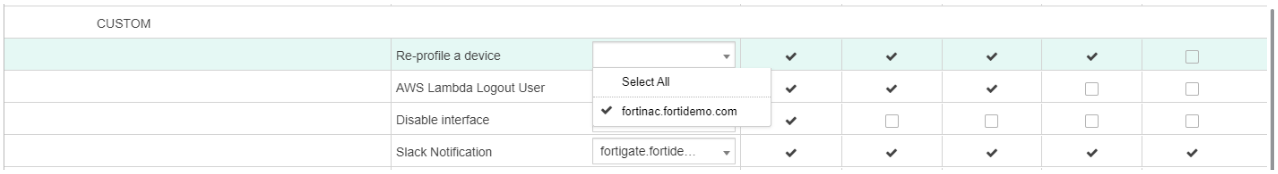
REMEDIATION

Terminate process		✓	□	□	□	□
Delete file		□	□	□	□	□
Clean persistent data		✓	□	□	□	□
Block address on Firewall	FortiGate300 ▾	✓	□	□	□	□

FortiEDR is now configured to add malicious IP addresses to the blocking policy on the firewall upon triggering of a security event. You can check that malicious IP addresses are added to the address group that was configured on the firewall following FortiEDR security events.

To configure an automated incident response that uses a firewall connector to perform a custom action upon the triggering of a security event:

1. Navigate to the *SECURITY SETTINGS* > *Playbooks* page.
2. Open the Playbook policy that is applied on devices for which you want the custom action (defined above) to apply.
3. In the *CUSTOM* section, place a checkmark in the relevant *Classification* columns next to the row of the relevant custom action.
4. In the dropdown menu next to the relevant custom action, select the relevant firewall connector with which to perform the action, as shown below:

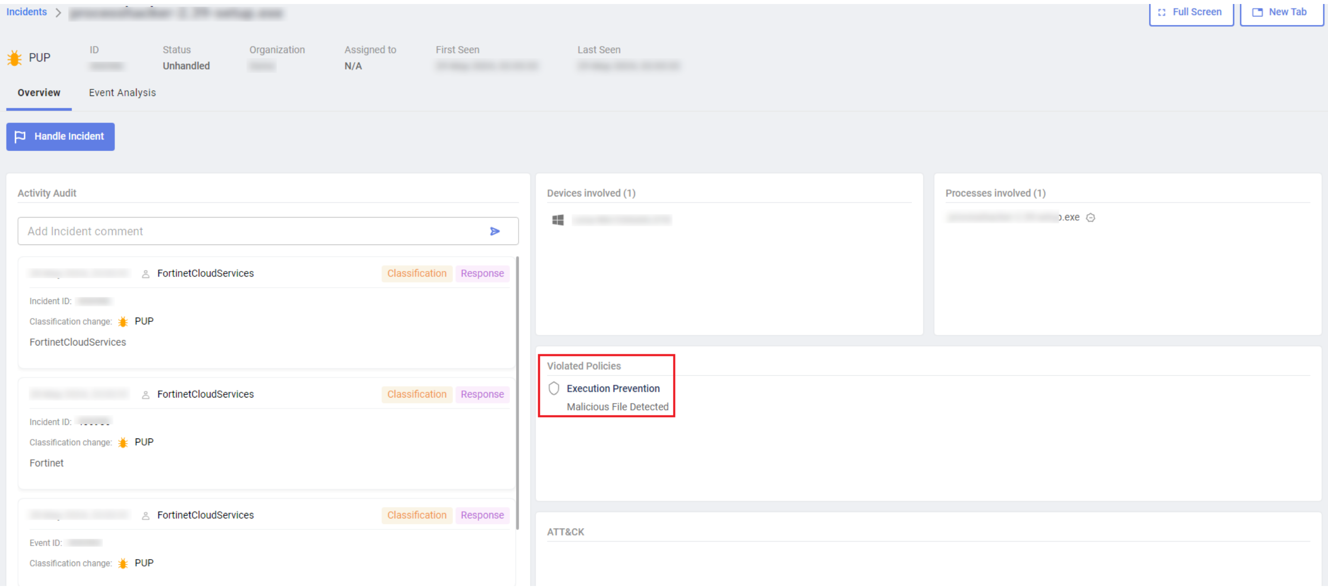


CUSTOM

Re-profile a device	▾	✓	✓	✓	✓	□
AWS Lambda Logout User		✓	✓	✓	□	□
Disable interface		✓	□	□	□	□
Slack Notification	fortigate.fortide... ▾	✓	✓	✓	✓	✓

FortiEDR is now configured to trigger this action in the third-party system upon the triggering of a security event.

Automatic incident response actions are listed in the *Overview* tab when you select the incident and click *Investigate* in the *Incidents* pane, as shown below:



Incidents > [redacted]

PUP

ID [redacted]

Status Unhandled

Organization [redacted]

Assigned to N/A

First Seen [redacted]

Last Seen [redacted]

Activity Audit

Add Incident comment

[redacted] FortinetCloudServices Classification Response
Incident ID: [redacted]
Classification change: PUP
FortinetCloudServices

[redacted] FortinetCloudServices Classification Response
Incident ID: [redacted]
Classification change: PUP
Fortinet

[redacted] FortinetCloudServices Classification Response
Event ID: [redacted]
Classification change: PUP

Devices involved (1)
[redacted]

Processes involved (1)
[redacted].exe

Violated Policies
Execution Prevention
Malicious File Detected

ATT&CK

Network Access Control (NAC) integration

When a Network Access Control connector such as FortiNAC is set and Playbook policies are configured, automatic incident response actions can include isolating a device by a NAC system upon security event triggering.

Before you start NAC configuration, make sure that:

- Your FortiEDR deployment includes a Jumpbox that has connectivity to the NAC server.
  Details about how to install a FortiEDR Core and configure it as a Jumpbox are described in Setting up the FortiEDR Core on page 511. You may refer to Cores on page 403 for more information about configuring a Jumpbox.
- The FortiEDR Central Manager has connectivity to the Fortinet Cloud Services (FCS).
- You have a valid API user with access to FortiNAC or equivalent network access control system.

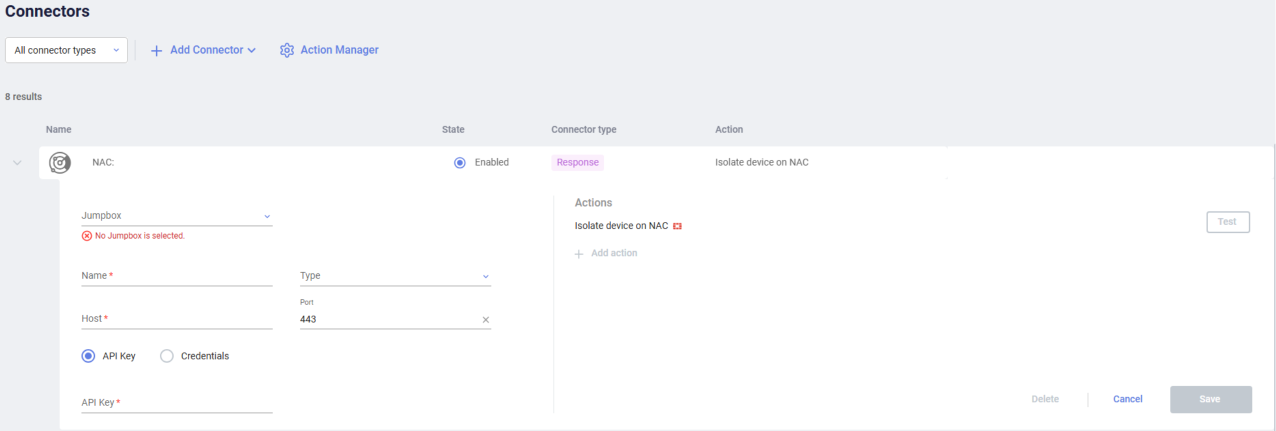
Follow the steps below in order to automatically isolate a device by NAC upon the detection of a FortiEDR security event. The example below describes how to define an API user on FortiNAC in order to enable FortiEDR to perform automatic device isolation after a FortiEDR security event.

Make sure to add FortiEDR domains and/or IP addresses to the exclusion list on the VLAN that is being used for isolation on the FortiNAC system such that the FortiEDR Collector would still be able to communicate with its servers when the device is being isolated.

FortiEDR Connector configuration

To configure NAC integration:

1. Click the *Add Connector* button and select *NAC* in the *Connectors* dropdown list. The following displays:



8 results

Name	State	Connector type	Action
NAC:	● Enabled	Response	Isolate device on NAC

Jumpbox
No Jumpbox is selected.

Name *
Type
Host *
Port 443
● API Key ○ Credentials
API Key *

Actions
Isolate device on NAC

2. Fill in the following fields:

Field	Definition
Jumpbox	Select the FortiEDR Jumpbox that will communicate with this NAC system.

Field	Definition
Name	Specify a name of your choice which will be used to identify this NAC system.
Type	Select the type of NAC to be used in the dropdown list, for example: FortiNAC.
Host	Specify the IP or DNS address of the external NAC system.
Port	Specify the port that is used for communication with the external NAC system.
API Key	Specify authentication details of the external NAC system. To use an API token, click the API Key radio button and copy the token value into the text box. To use API credentials, click the *Credentials* radio button and fill in the external NAC system API username and password.

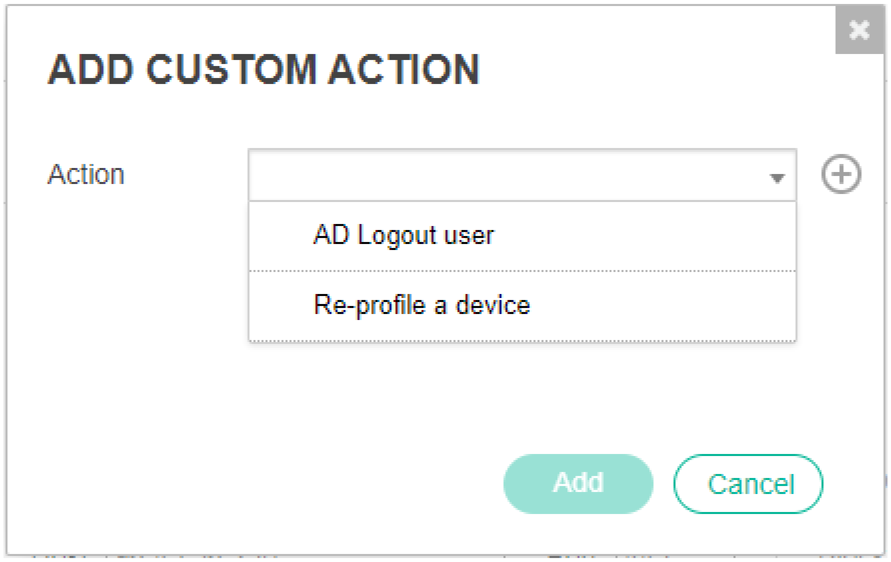
3. 3 In the *Actions* area on the right, define the action to be taken by this connector.

You have the option to either use an action provided out-of-the-box with FortiEDR (for example, *Isolate Device on NAC*)

– OR –

To create or select one of the Custom Integration actions (if one or more have already been defined in FortiEDR, as described in Custom integration on page 370.

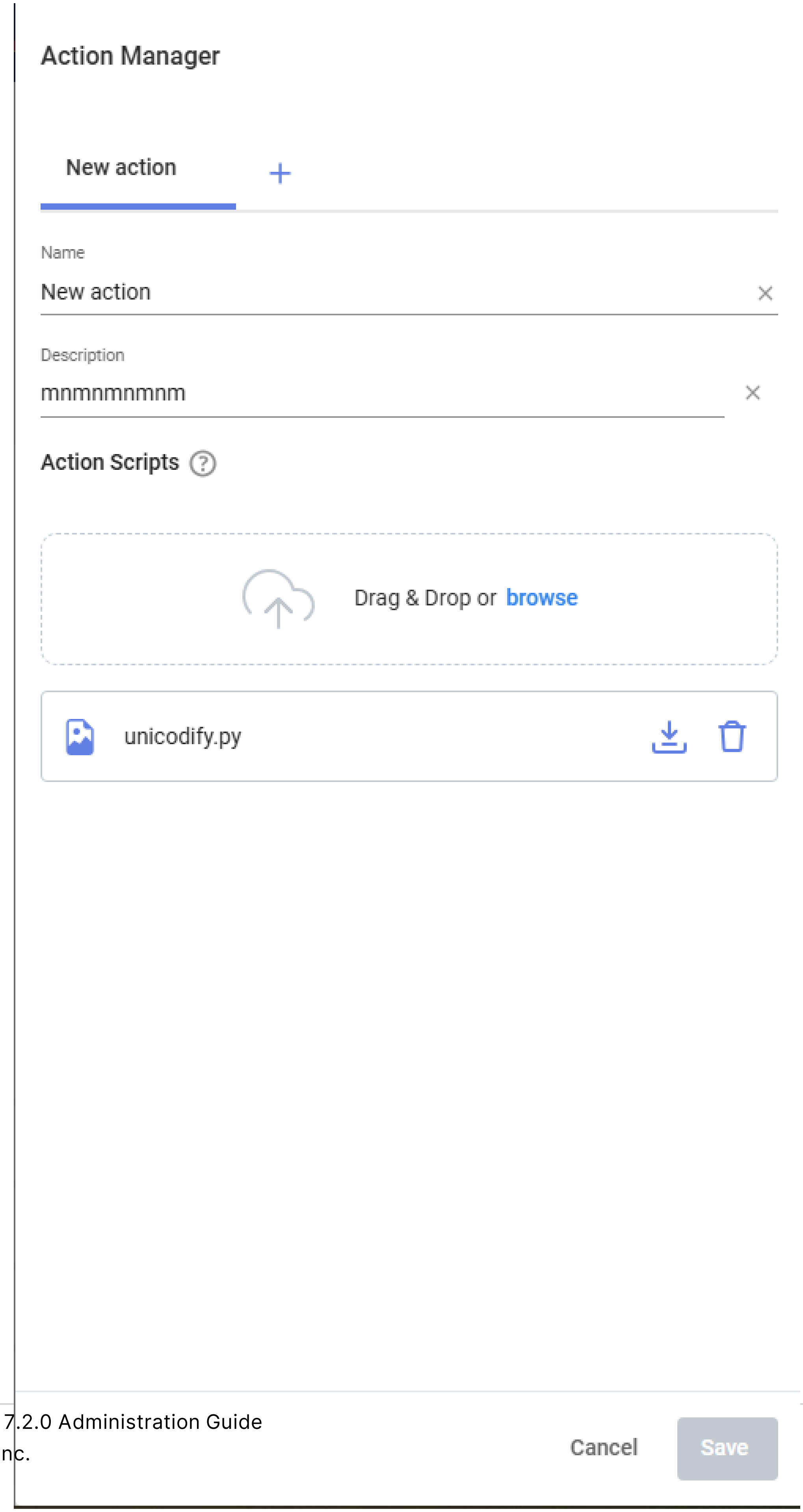
- To trigger an action on a custom connected third-party system, click the + *Add Action* button to display the following popup window:



a. In the *Action* dropdown menu, select one of the previously defined actions (which were defined in FortiEDR as described in Custom integration on page 370).

- OR -

b. Click the *Create New Action* ⊕ button in this popup window to define a new action that can be triggered according to the definitions in the Playbook, as described below. The following displays:



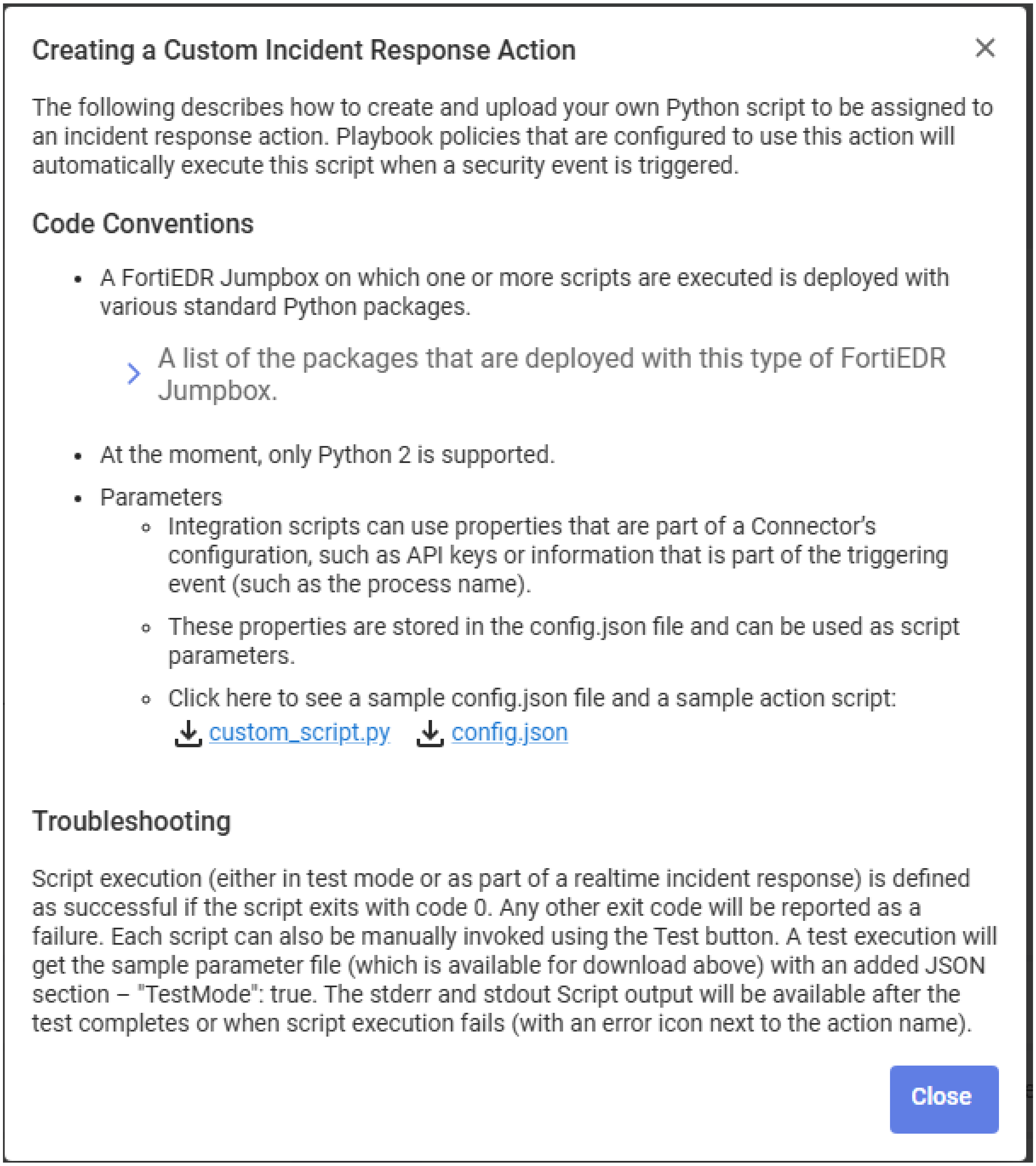
Name
New action

Description
mnmnmnmnm

Fill out the fields of this window as follows in order to define a new action to be triggered in response to an incident.

In order to trigger this action, a Playbook policy must be defined that triggers this action to execute the script when a security event is triggered. The definition of this new action here automatically adds this action as an option in a Playbook policy. This action however, is not selected by default in the Playbook policy. Therefore, you must go to the Playbook policy and select it in order for it to be triggered when a security event is triggered.

Field	Definition
Name	Enter any name for this action
Description	Enter a description of this action
Upload	Upload a Python script that calls an API from the third-party system in order to perform the relevant action. Python 2.7 or later is supported. This Python script must be created according to the coding conventions that can be displayed by clicking the icon ? next to the *Action Scripts* field. The following displays providing an explanation of these coding conventions and provides various links that you can click to see more detail and/or to download sample files.



Creating a Custom Incident Response Action

The following describes how to create and upload your own Python script to be assigned to an incident response action. Playbook policies that are configured to use this action will automatically execute this script when a security event is triggered.

Code Conventions

- A FortiEDR Jumpbox on which one or more scripts are executed is deployed with various standard Python packages.

  > A list of the packages that are deployed with this type of FortiEDR Jumpbox.

- At the moment, only Python 2 is supported.
- Parameters
  - Integration scripts can use properties that are part of a Connector's configuration, such as API keys or information that is part of the triggering event (such as the process name).
  - These properties are stored in the config.json file and can be used as script parameters.
  - Click here to see a sample config.json file and a sample action script:
    custom_script.py config.json

Troubleshooting

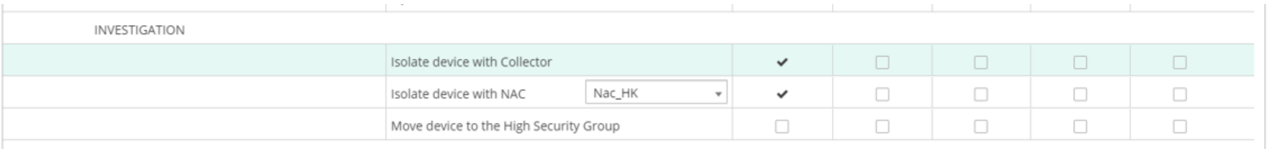
Script execution (either in test mode or as part of a realtime incident response) is defined as successful if the script exits with code 0. Any other exit code will be reported as a failure. Each script can also be manually invoked using the Test button. A test execution will get the sample parameter file (which is available for download above) with an added JSON section – "TestMode": true. The stderr and stdout Script output will be available after the test completes or when script execution fails (with an error icon next to the action name).

4. Click *Save*. The new action is then listed in the Actions area.
5. You can click the *Test* button next to an action to execute that action.

Playbooks configuration

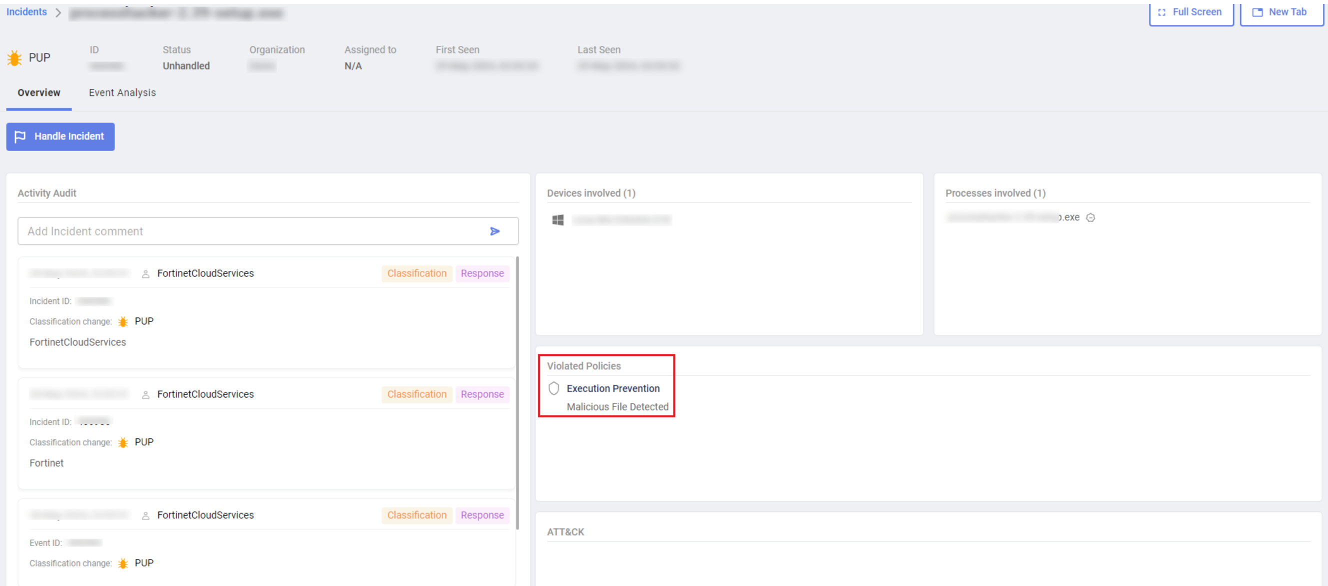
To configure an automated incident response that uses a NAC connector to isolate a device upon security event triggering:

1. Navigate to the *SECURITY SETTINGS* > *Playbooks* page.
2. Open the Playbook policy that is applied on devices for which you want the isolation response to apply and place a checkmark in the relevant Classification column next to the Isolate device with NAC row that is under the *INVESTIGATION* section.



INVESTIGATION						
	Isolate device with Collector	✓	□	□	□	□
	Isolate device with NAC Nac_HK ▾	✓	□	□	□	□
	Move device to the High Security Group	□	□	□	□	□

FortiEDR is now configured to automatically isolate the device upon triggering of a security event. Automatic incident response actions are listed in the *Overview* tab when you select the incident and click *Investigate* in the *Incidents* pane, as shown below:



PUP

ID [redacted]

Status Unhandled

Organization [redacted]

Assigned to N/A

First Seen [redacted]

Last Seen [redacted]

Activity Audit

[redacted] FortinetCloudServices Classification Response
Incident ID: [redacted]
Classification change: PUP
FortinetCloudServices

[redacted] FortinetCloudServices Classification Response
Incident ID: [redacted]
Classification change: PUP
Fortinet

[redacted] FortinetCloudServices Classification Response
Event ID: [redacted]
Classification change: PUP

Devices involved (1)
[redacted]

Processes involved (1)
[redacted].exe

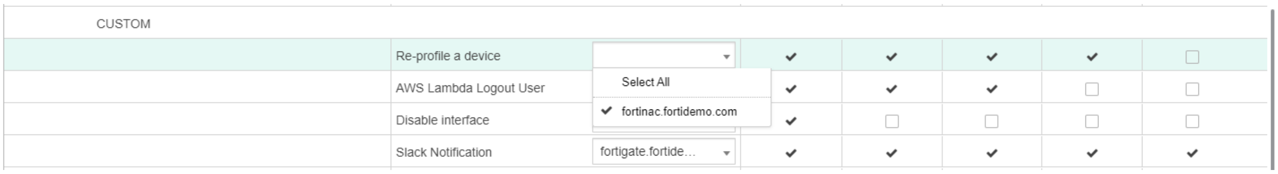
Violated Policies
Execution Prevention
Malicious File Detected

ATT&CK

Note that isolation by NAC will only be done for devices that are managed on the specified NAC.

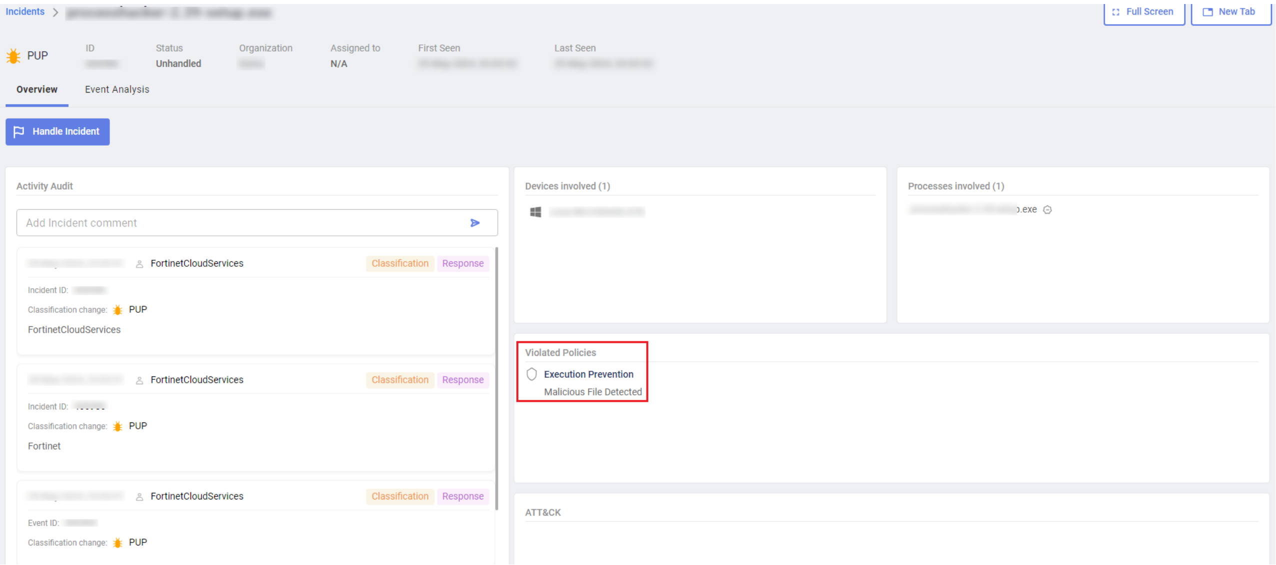
To configure an automated incident response that uses a NAC connector to perform a custom action upon the triggering of a security event:

1. Navigate to the *SECURITY SETTINGS* > *Playbooks* page.
2. Open the Playbook policy that is applied on devices for which you want the custom action (defined above) to apply.
3. In the *CUSTOM* section, place a checkmark in the relevant *Classification* columns next to the row of the relevant custom action.
4. In the dropdown menu next to the relevant custom action, select the relevant NAC connector with which to perform the action, as shown below:



CUSTOM						
Re-profile a device		✓	✓	✓	✓	☐
AWS Lambda Logout User	Select All	✓	✓	✓	☐	☐
Disable interface	✓ fortinac.fortidemo.com	✓	☐	☐	☐	☐
Slack Notification	fortigate.fortide...	✓	✓	✓	✓	✓

FortiEDR is now configured to trigger this action in the third-party system upon the triggering of a security event. This automatic incident response action appears in the*Overview* tab when you select the incident and click *Investigate*.



Incidents > [redacted]

Full Screen | New Tab

PUP | ID: [redacted] | Status: Unhandled | Organization: [redacted] | Assigned to: N/A | First Seen: [redacted] | Last Seen: [redacted]

Overview | Event Analysis

Handle Incident

Activity Audit

Add Incident comment

[redacted] FortinetCloudServices — Classification, Response
Incident ID: [redacted]
Classification change: PUP
FortinetCloudServices

[redacted] FortinetCloudServices — Classification, Response
Incident ID: [redacted]
Classification change: PUP
Fortinet

[redacted] FortinetCloudServices — Classification, Response
Event ID: [redacted]
Classification change: PUP

Devices involved (1)
[redacted]

Processes involved (1)
[redacted].exe

Violated Policies
Execution Prevention
Malicious File Detected

ATT&CK

Sandbox integration

When a sandbox such as FortiSandbox is configured and the Sandbox Analysis Policy rule is enabled, files that meet several conditions and that have not been previously analyzed trigger a sandbox analysis event on FortiEDR and are sent to the sandbox. The conditions are a combination of several items, such as the file was downloaded from the Internet and was not signed by a known vendor. If the file is found to be clean, the event is automatically classified as safe and marked as handled. If the file is determined by the sandbox to be suspicious or malicious, then the event is classified as non-safe and any future execution attempt of the file in the environment is blocked by one of the Pre-execution (NGAV) Policy rules. Note that in all cases the first file execution is not delayed or blocked.

For more details about integrating FortiEDR with FortiSandbox, refer to the FortiSandbox Integration Guide.

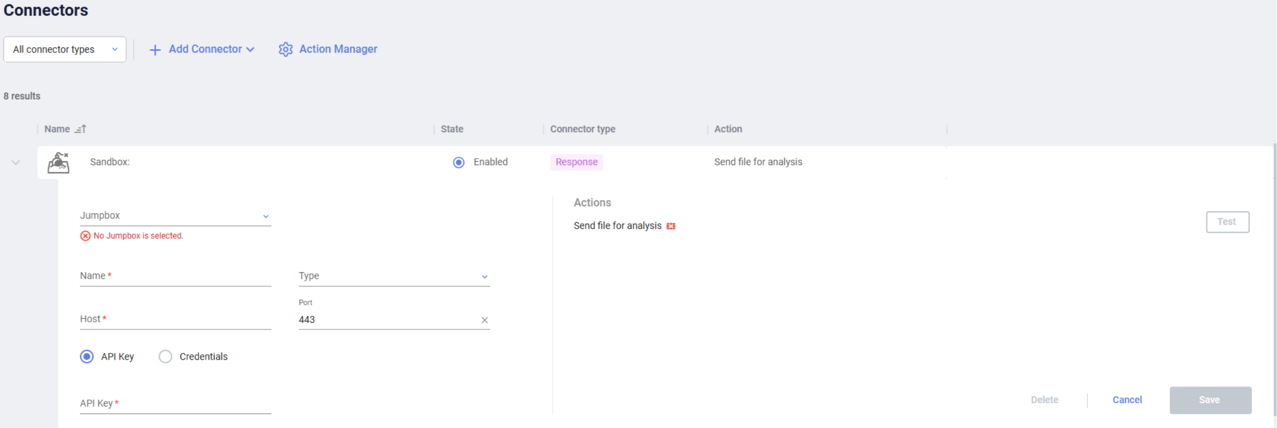
Before you start sandbox configuration, make sure that:

- Your FortiEDR deployment includes a Jumpbox that has connectivity to the sandbox.
  - Refer to Setting up the FortiEDR Core on page 511 for details about how to install a FortiEDR Core and configure it as a Jumpbox.
  - Refer to Cores on page 403 for more information about configuring a Jumpbox.
- The FortiEDR Central Manager has connectivity to Fortinet Cloud Services (FCS).
- **(FortiSandbox)** A FortiSandbox administrator account with JSON API access enabled. Refer to the FortiSandbox Integration Guide for detailed instructions.

- **(FortiSandbox Cloud)** A valid FortiCloud API user under a permission profile with read/write access to the FortiSandbox Cloud portal. See the FortiCloud IAM documentation for detailed instructions about creating a permission profile and an API user.

To set up a sandbox connector with FortiEDR:

1. Click the *Add Connector* button and select *Sandbox* in the *Connectors* dropdown list. The following displays:



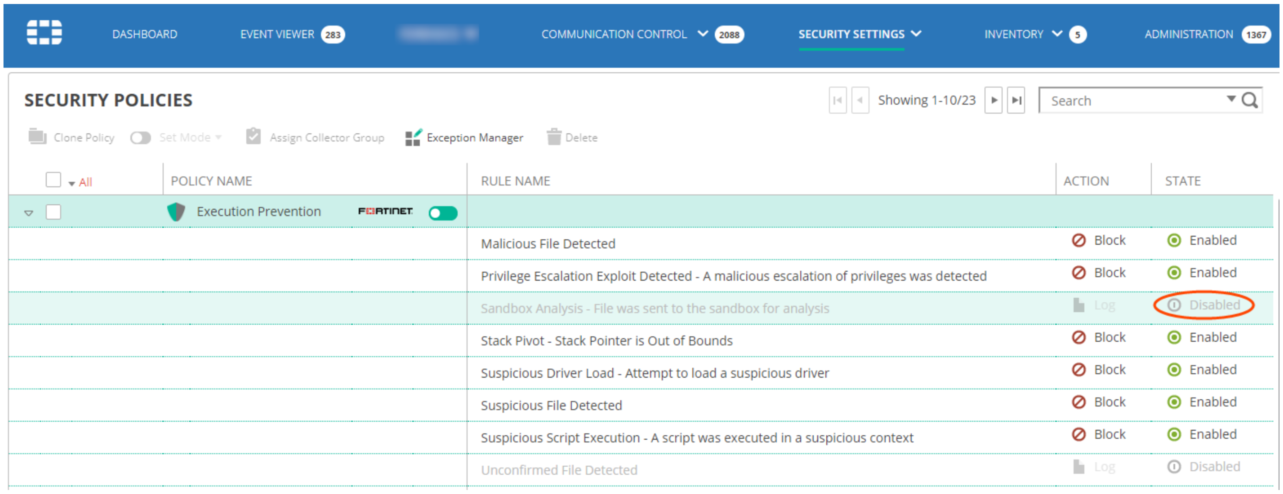
2. Fill in the following fields:

Field	Definition
Jumpbox	Select the FortiEDR Jumpbox that will communicate with this sandbox.
Name	Specify a name of your choice which will be used to identify this sandbox.
Type	Select the type of sandbox to be used in the dropdown list, for example: *FortiSandbox*.
Host	Specify the IP or DNS address of you sandbox.
Port	Specify the port that is used for API communication with your sandbox.
API Key / Credentials	Specify authentication details of the FortiSandbox or FortiSandbox Cloud. • **(FortiSandbox)** To use an API token, select *API Key* and copy the token value into the text box. To use credentials, select *Credentials* and fill in the FortiSandbox username and password. • **(FortiSandbox Cloud)** Select *API Key* and copy the token value into the text box.

3. Click *Save*.
In order to complete sandbox integration, the Sandbox Scan rule must be enabled with the FortiEDR Central Manager.

To enable the Sandbox scan rule:

1. Navigate to the *SECURITY SETTINGS > Security Policies* page.
2. Open the Execution Prevention policy that is applied on devices for which you want the sandbox scan to apply and click the *Disabled* button next to the Sandbox Analysis rule to enable it, as shown below:



☐ All	POLICY NAME	RULE NAME	ACTION	STATE
☐	Execution Prevention			
		Malicious File Detected	Block	Enabled
		Privilege Escalation Exploit Detected - A malicious escalation of privileges was detected	Block	Enabled
		Sandbox Analysis - File was sent to the sandbox for analysis	Log	Disabled
		Stack Pivot - Stack Pointer is Out of Bounds	Block	Enabled
		Suspicious Driver Load - Attempt to load a suspicious driver	Block	Enabled
		Suspicious File Detected	Block	Enabled
		Suspicious Script Execution - A script was executed in a suspicious context	Block	Enabled
		Unconfirmed File Detected	Log	Disabled

FortiEDR is now configured to send unknown files to the sandbox.

You can check file analysis on your sandbox console.

In addition, you can see sandbox analysis events in the*Overview* tab when you select the incident and click *Investigate* in the *Incidents* pane. Events of files that were found to be clean appear under the *Handled* filter and events of files that were found to be risky are displayed under the *All statuses* filter. A sandbox analysis digest is added to the security event's handling comment.

eXtended detection source integration

You can connect to external systems to collect activity log by adding a new connector for extended detection. The aggregated data is then being sent to Fortinet Cloud Services (FCS) where it is correlated and analyzed to detect malicious indications that will result in security events of eXtended Detection policy rule violations.

FortiEDR supports extended detection with the following external systems:

- FortiAnalyzer or FortiAnalyzer Cloud on page 358
- FortiSIEM or FortiSIEM Cloud
- Google Cloud Security Command Center (SCC) on page 361
- AWS GuardDuty on page 364
- Custom on page 367

FortiAnalyzer or FortiAnalyzer Cloud

You can integrate FortiEDR with FortiAnalyzer or FortiAnalyzer Cloud to correlate data between FortiEDR and the Fortinet Security Fabric and issue eXtended detection alerts. To complete the integration, you must configure an eXtended detection source connector for FortiAnalyzer or FortiAnalyzer Cloud and enable the eXtended detection rules and FortiEDR Threat Hunting events collection.

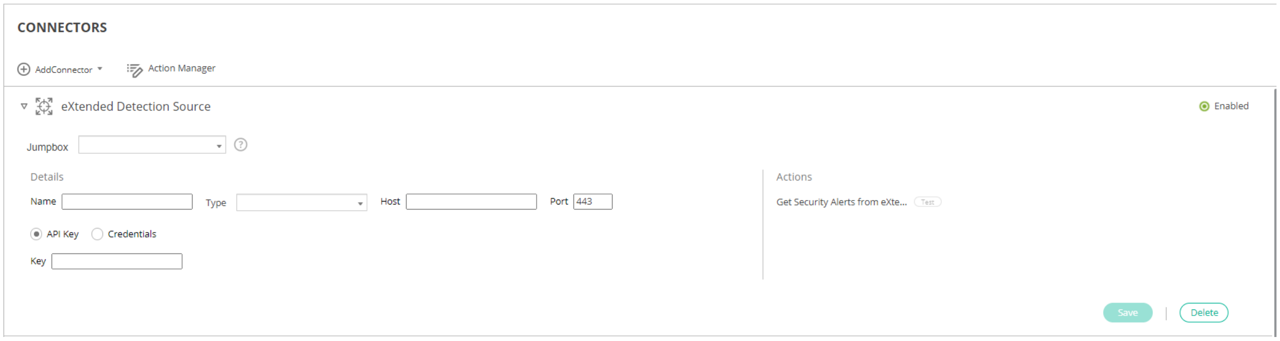
Prerequisites

Before you start integrating FortiEDR with FortiAnalyzer or FortiAnalyzer Cloud, verify you have the following:

- A valid license for eXtended Detection Response—While you can create an eXtended detection source connector without a valid license for eXtended Detection Response, the license is required for a successful XDR definition.
- A Jumpbox with connectivity to FortiAnalyzer:
  - Refer to Setting up the FortiEDR Core on page 511 for details about how to install a FortiEDR Core and configure it as a Jumpbox.
  - Refer to Cores on page 403 for more information about configuring a Jumpbox.
- Connectivity from the FortiEDR Central Manager to the Fortinet Cloud Services (FCS).
- **(FortiAnalyzer)** A FortiAnalyzer administrator account with JSON API access enabled. Refer to the FortiAnalyzer Administration Guide for more information.
- **(FortiAnalyzer Cloud)** A valid FortiCloud API user under a permission profile with read/write access to the FortiAnalyzer Cloud portal. See the FortiCloud IAM documentation for detailed instructions about creating a permission profile and an API user.

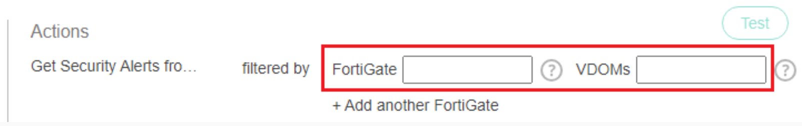
Setting up a connector for FortiAnalyzer or FortiAnalyzer Cloud

1. Click the *Add Connector* button and select *eXtended Detection Source* in the *Connectors* dropdown list. The following displays:



2. Fill in the following fields:

Field	Definition
Enabled	Check this checkbox to enable blocking of malicious IP addresses by the FortiAnalyzer or FortiAnalyzer Cloud.
Jumpbox	Select the FortiEDR Jumpbox that will communicate with the FortiAnalyzer or FortiAnalyzer Cloud.
Name	Specify a name of your choice to identify the connector.
Type	Select *FortiAnalyzer*.

Field	Definition
Host	Specify the IP or DNS address of the FortiAnalyzer or FortiAnalyzer Cloud.
Port	Specify the port that is used for API communication with the FortiAnalyzer or FortiAnalyzer Cloud.
API Key/Credentials/Authentication	Specify authentication details of the FortiAnalyzer or FortiAnalyzer Cloud. • **(FortiAnalyzer)** Select *Credentials* and fill in the FortiAnalyzer username and password. • **(FortiAnalyzer Cloud)** Specify the username and password of the FortiCloud API user with read/write access to the FortiAnalyzer Cloud portal.
Actions	Configure the FortiGate and VDOM logs to be correlated with FortiEDR data by specifying the FortiGate or VDOM name in the following fields. If both fields are empty, FortiEDR uses the default value, which is *All*.  Actions Test Get Security Alerts fro... filtered by FortiGate VDOMs + Add another FortiGate

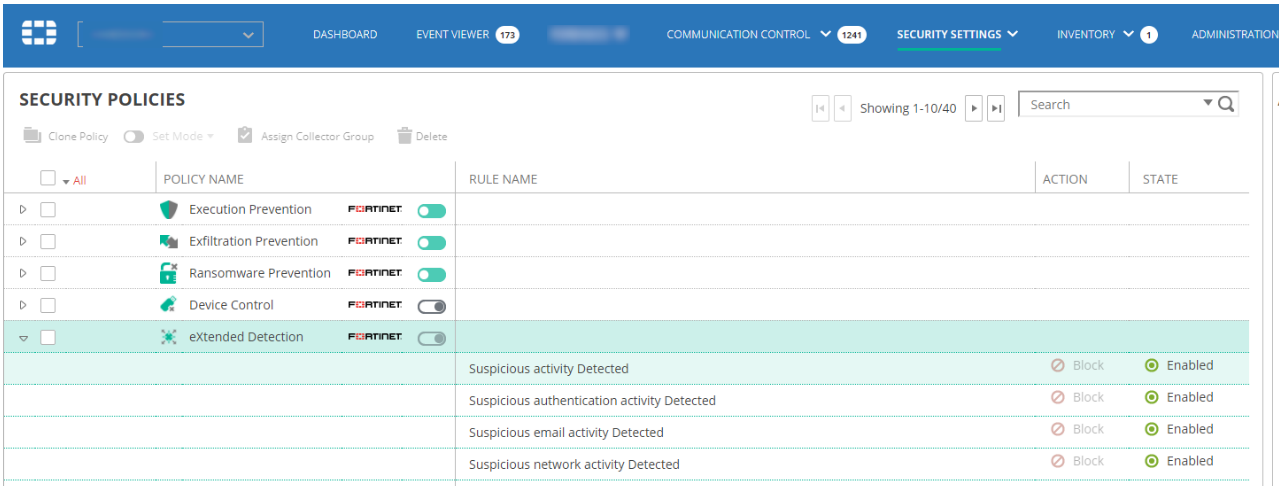
3. Click *Save*.

Setting up FortiEDR Central Manager

In order to complete the integration with FortiAnalyzer or FortiAnalyzer Cloud, the eXtended detection rules and FortiEDR Threat Hunting events collection must be enabled with the FortiEDR Central Manager, as follows.

To enable eXtended detection rules:

1. Navigate to the *SECURITY SETTINGS* > *Security Policies* page.
2. Open the eXtended detection policy that is applied on devices on which you want the eXtended detection policy to apply and click the *Disabled* button next to each of the underlying rules to enable it, as shown below:

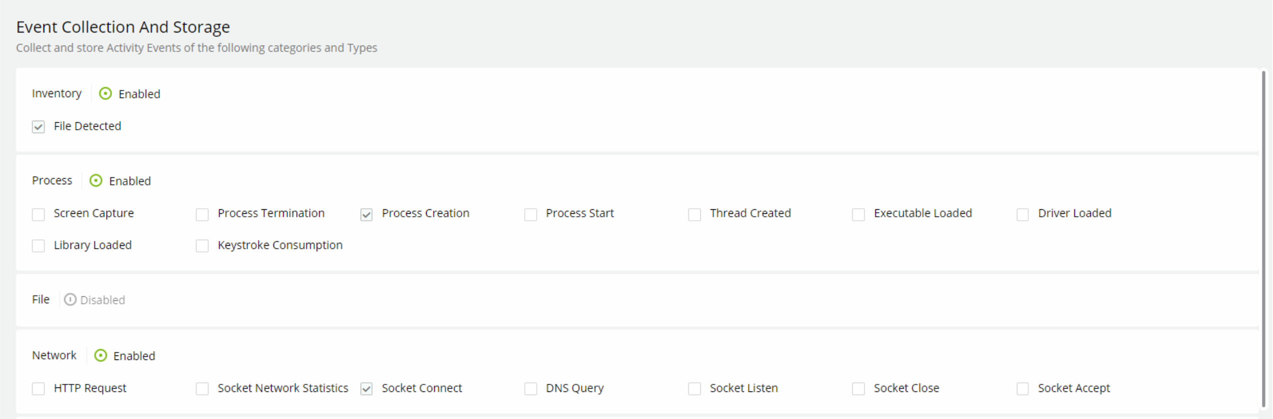


SECURITY POLICIES

□ All	POLICY NAME		RULE NAME	ACTION	STATE
▷ □	Execution Prevention	FORTINET			
▷ □	Exfiltration Prevention	FORTINET			
▷ □	Ransomware Prevention	FORTINET			
▷ □	Device Control	FORTINET			
▽ □	eXtended Detection	FORTINET			
			Suspicious activity Detected	Block	Enabled
			Suspicious authentication activity Detected	Block	Enabled
			Suspicious email activity Detected	Block	Enabled
			Suspicious network activity Detected	Block	Enabled

To enable FortiEDR Threat Hunting events collection:

1. Navigate to the *SECURITY SETTINGS > Threat Hunting > Collection Profiles* page.
2. Open the Threat Hunting collection profile that is applied on devices on which you want the eXtended detection policy to apply.
3. Select the following event types on that profile:
   - Socket Connect
   - Process Creation
   - File Create
   - File Detected



Event Collection And Storage

Collect and store Activity Events of the following categories and Types

Inventory ○ Enabled

☑ File Detected

Process ○ Enabled

□ Screen Capture □ Process Termination ☑ Process Creation □ Process Start □ Thread Created □ Executable Loaded □ Driver Loaded

□ Library Loaded □ Keystroke Consumption

File ○ Disabled

Network ○ Enabled

□ HTTP Request □ Socket Network Statistics ☑ Socket Connect □ DNS Query □ Socket Listen □ Socket Close □ Socket Accept

FortiEDR is now configured to issue eXtended detection alerts from FortiAnalyzer or FortiAnalyzer Cloud.

Google Cloud Security Command Center (SCC)

To integrate FortiEDR with Google Cloud Security Command Center (SCC) to collect activity log and issue eXtended detection alerts, you must configure Google SCC for threat logging and API access, configure an eXtended detection source connector with Google Cloud SCC in FortiEDR, and enable the eXtended detection rules and FortiEDR Threat Hunting events collection in FortiEDR.

Prerequisites

Before you start integrating FortiEDR with Google SCC, verify you have the following:

- Google Cloud licensing of Security Command Center Premium tier that has Event Threat Detection feature.
- A valid FortiEDR license for eXtended Detection Response—While you can create an eXtended detection source connector without a valid license for eXtended Detection Response, the license is required for a successful XDR definition.
- A Jumpbox with connectivity to Google SCC. Details about how to install a FortiEDR Core and configure it as a Jumpbox are provided in Setting up the FortiEDR Core on page 511. You may refer to Cores on page 403 for more information about configuring a Jumpbox.
- Connectivity from the FortiEDR Central Manager to the Fortinet Cloud Services (FCS).

Configuring Google SCC

Perform the following steps to configure Google SCC:

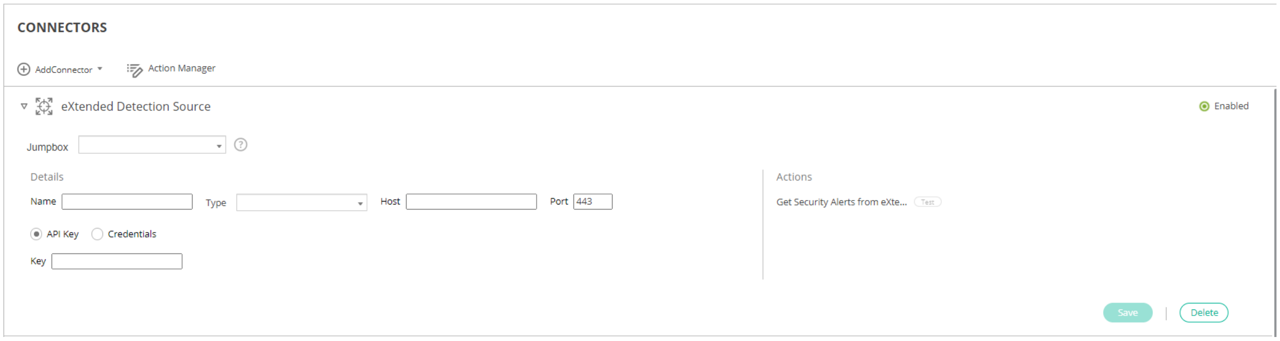
1. Enable threat logging in Google SCC:
   a. Enable Event Threat Detection per monitored project in the organization. The following Event Threat Detection rules are required:
      - Malware: bad IP
      - Malware: bad domain

      Make sure to enable all log source types that are needed for these rules detectors to work, such as Cloud DNS logs and Admin Activity log. For more details about Event Threat Detection rules and the required log sources, see Google Documentation.
   b. Verify that raw log items now show on Google's Logs Explorer and Event Threat Detection findings show on Security Command Center as described in Google Documentation.
2. Enable API access to Google for fetching threat logs:
   a. Set up a service account on Google, as described in Google Documentation.
   b. Download the json key file for this service account. This file should be uploaded via FortiEDR console as part of setting up the extended detection source connector (see section below).
   c. Grant the following permission to the service account to allow API access:
      - Organization Admin (resourcemanager.organizationAdmin)
      - Security Command Center Admin (securityCenter.admin)

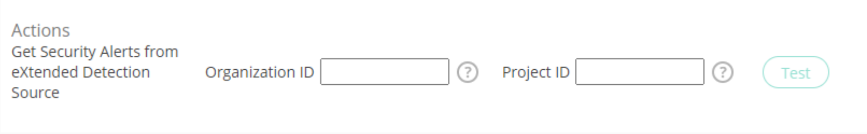
        See Google Documentation for more details about permissions.

Setting up a connector for Google SCC

1. Click the *Add Connector* button and select *eXtended Detection Source* in the *Connectors* dropdown list. The following displays:



2. Fill in the following fields:

Field	Definition
Enabled	Check this checkbox to enable blocking of malicious IP addresses by Google SCC.
Jumpbox	Select the FortiEDR Jumpbox that will communicate with Google SCC.
Name	Specify a name of your choice to identify the connector.
Type	Select *Google SCC*.
Authentication	Upload the JSON file that was created for your Google Service account.
Actions	Specify the unique organization resource identifier in Google cloud or ID of Google cloud project to use for fetching alerts.  Actions Get Security Alerts from eXtended Detection Source Organization ID Project ID Test

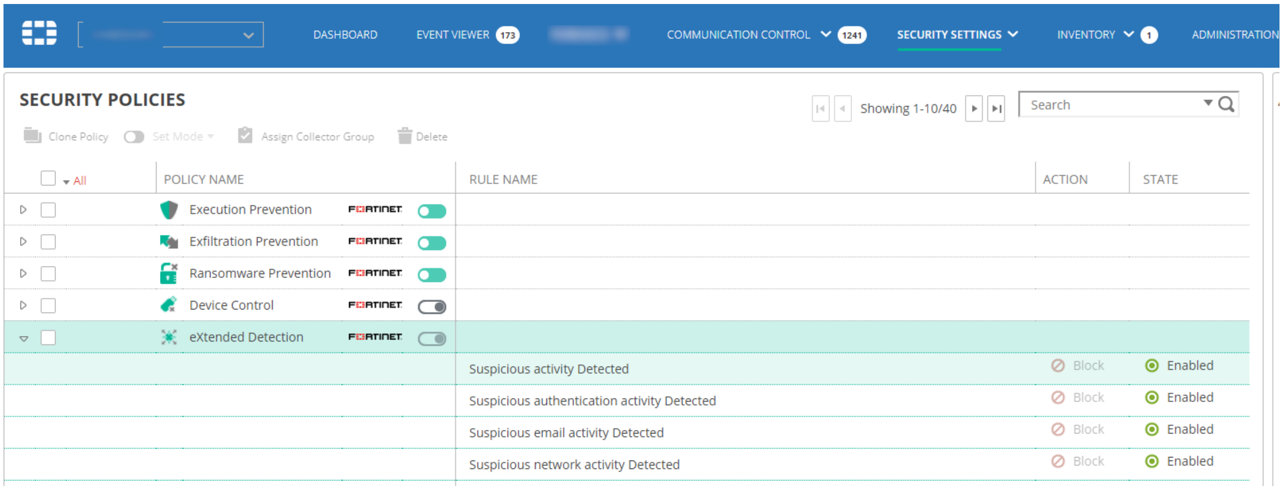
3. Click *Save*.

Setting up FortiEDR Central Manager

In order to complete the integration with Google SCC, the eXtended detection rules and FortiEDR Threat Hunting events collection must be enabled with the FortiEDR Central Manager, as follows.

To enable eXtended detection rules:

1. Navigate to the *SECURITY SETTINGS > Security Policies* page.
2. Open the eXtended detection policy that is applied on devices on which you want the eXtended detection policy to apply and click the *Disabled* button next to each of the underlying rules to enable it, as shown below:

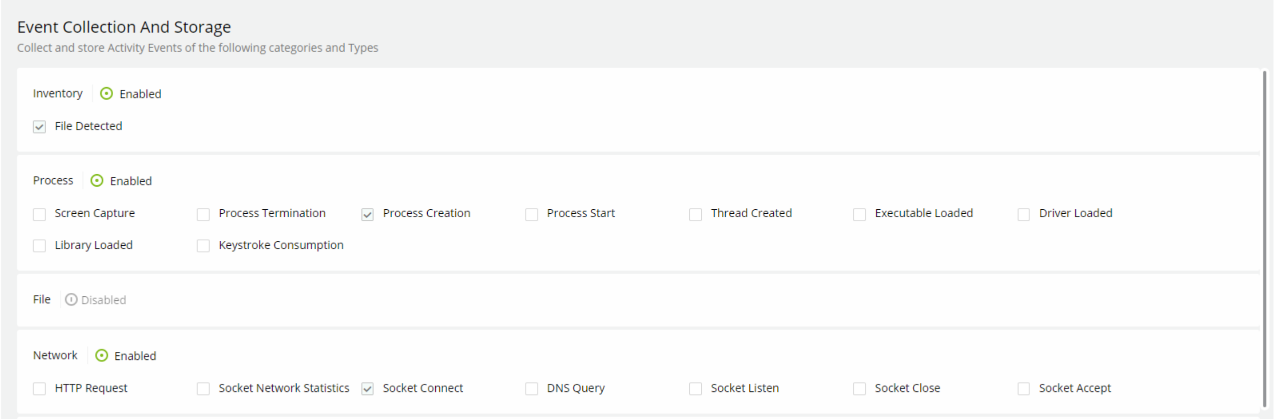


SECURITY POLICIES

□ All	POLICY NAME		RULE NAME	ACTION	STATE
▷ □	Execution Prevention	FORTINET			
▷ □	Exfiltration Prevention	FORTINET			
▷ □	Ransomware Prevention	FORTINET			
▷ □	Device Control	FORTINET			
▽ □	eXtended Detection	FORTINET			
			Suspicious activity Detected	Block	Enabled
			Suspicious authentication activity Detected	Block	Enabled
			Suspicious email activity Detected	Block	Enabled
			Suspicious network activity Detected	Block	Enabled

To enable FortiEDR Threat Hunting events collection:

1. Navigate to the *SECURITY SETTINGS > Threat Hunting > Collection Profiles* page.
2. Open the Threat Hunting collection profile that is applied on devices on which you want the eXtended detection policy to apply.
3. Select the following event types on that profile:
   - Socket Connect
   - Process Creation
   - File Create
   - File Detected



Event Collection And Storage

Collect and store Activity Events of the following categories and Types

Inventory ⊙ Enabled

☑ File Detected

Process ⊙ Enabled

□ Screen Capture □ Process Termination ☑ Process Creation □ Process Start □ Thread Created □ Executable Loaded □ Driver Loaded

□ Library Loaded □ Keystroke Consumption

File ⓘ Disabled

Network ⊙ Enabled

□ HTTP Request □ Socket Network Statistics ☑ Socket Connect □ DNS Query □ Socket Listen □ Socket Close □ Socket Accept

FortiEDR is now configured to issue eXtended detection alerts from Google SCC.

AWS GuardDuty

To integrate FortiEDR with AWS GuardDuty to collect activity log and issue eXtended detection alerts, you must configure AWS GuardDuty, configure an eXtended detection source connector with AWS GuardDuty in FortiEDR, and enable the eXtended detection rules and FortiEDR Threat Hunting events collection.

Prerequisites

Before you start integrating FortiEDR with AWS GuardDuty, verify you have the following:

- A valid license for eXtended Detection Response—While you can create an eXtended detection source connector without a valid license for eXtended Detection Response, the license is required for a successful XDR definition.
- A Jumpbox with connectivity to AWS GuardDuty. Details about how to install a FortiEDR Core and configure it as a Jumpbox are provided in Setting up the FortiEDR Core on page 511. You may refer to Cores on page 403 for more information about configuring a Jumpbox.
- Connectivity from the FortiEDR Central Manager to the Fortinet Cloud Services (FCS).

Configuring AWS GuardDuty

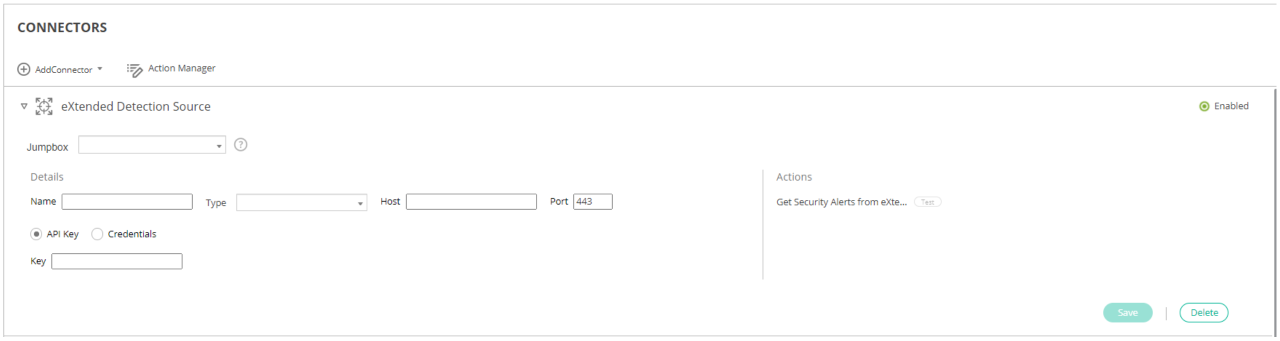
Perform the following steps to configure AWS GuardDuty:

1. Enable Amazon GuardDuty in your account as described in AWS Documentation.
   The following GuardDuty finding types are correlated with the FortiEDR events:
   - Backdoor:EC2/C&CActivity.B!DNS
   - Discovery:Kubernetes/MaliciousIPCaller

   You are encouraged to test that GuardDuty generates these findings as described on AWS documentation.
2. Create IAM user on AWS console as described here:
   a. Set Programmatic Access for this user to allow API calls.
   b. Set full permissions to access GuardDuty service.
   c. Show and copy access key ID and secret access key of this user, which will be used on FortiEDR console when you set up the extended detection source connector in the following section.

Setting up a connector for AWS GuardDuty

1. Click the *Add Connector* button and select *eXtended Detection Source* in the *Connectors* dropdown list. The following displays:



● Enabled

Jumpbox

Name

Type

Host

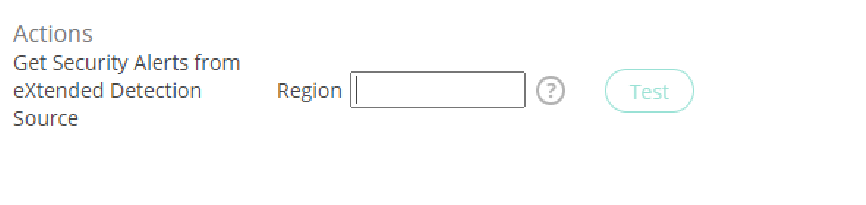
Port 443

● API Key ○ Credentials

Key

2. Fill in the following fields:

Field	Definition
Enabled	Check this checkbox to enable blocking of malicious IP addresses by AWS GuardDuty.

Field	Definition
Jumpbox	Select the FortiEDR Jumpbox that will communicate with AWS GuardDuty.
Name	Specify a name of your choice to identify the connector.
Type	Select *AWS GuardDuty*.
Authentication	Specify the access key ID and secret access key.
Actions	Specify the AWS region for API calls.  Actions Get Security Alerts from eXtended Detection Source Region Test

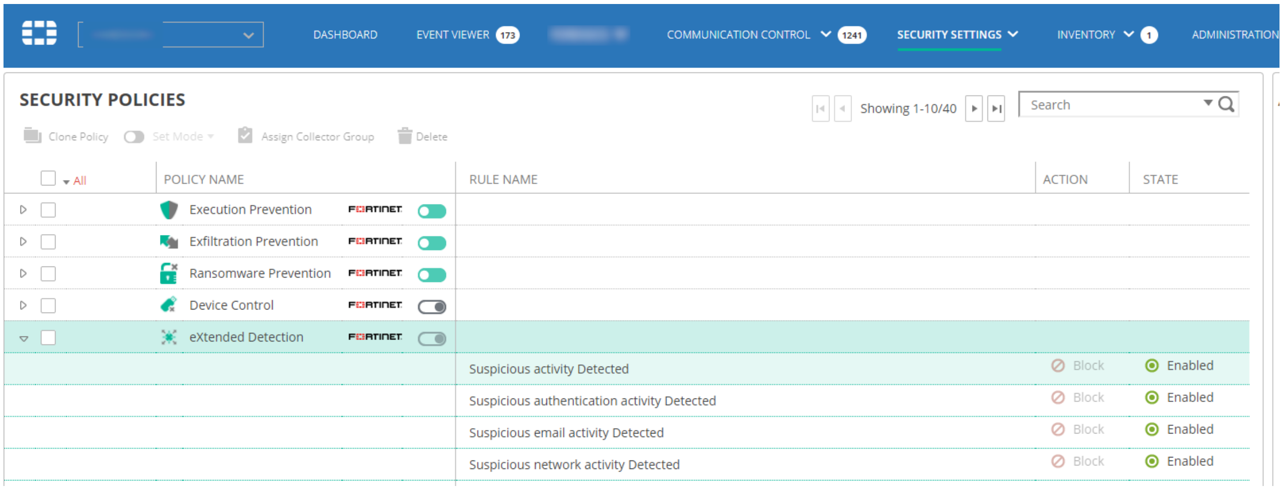
3. Click *Save*.

Setting up FortiEDR Central Manager

In order to complete the integration with AWS GuardDuty, the eXtended detection rules and FortiEDR Threat Hunting events collection must be enabled with the FortiEDR Central Manager, as follows.

To enable eXtended detection rules:

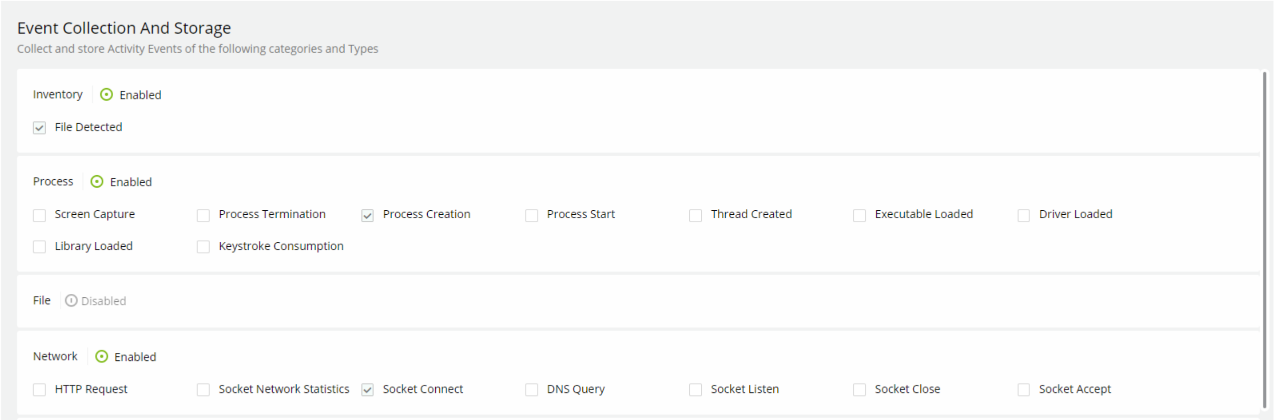
1. Navigate to the *SECURITY SETTINGS > Security Policies* page.
2. Open the eXtended detection policy that is applied on devices on which you want the eXtended detection policy to apply and click the *Disabled* button next to each of the underlying rules to enable it, as shown below:



☐ All	POLICY NAME		RULE NAME	ACTION	STATE
▷ ☐	Execution Prevention	FORTINET			
▷ ☐	Exfiltration Prevention	FORTINET			
▷ ☐	Ransomware Prevention	FORTINET			
▷ ☐	Device Control	FORTINET			
▽ ☐	eXtended Detection	FORTINET			
			Suspicious activity Detected	Block	Enabled
			Suspicious authentication activity Detected	Block	Enabled
			Suspicious email activity Detected	Block	Enabled
			Suspicious network activity Detected	Block	Enabled

To enable FortiEDR Threat Hunting events collection:

1. Navigate to the *SECURITY SETTINGS* > *Threat Hunting* > *Collection Profiles* page.
2. Open the Threat Hunting collection profile that is applied on devices on which you want the eXtended detection policy to apply.
3. Select the following event types on that profile:
   - Socket Connect
   - Process Creation
   - File Create
   - File Detected



Event Collection And Storage

Collect and store Activity Events of the following categories and Types

Inventory ○ Enabled

☑ File Detected

Process ○ Enabled

□ Screen Capture □ Process Termination ☑ Process Creation □ Process Start □ Thread Created □ Executable Loaded □ Driver Loaded

□ Library Loaded □ Keystroke Consumption

File ○ Disabled

Network ○ Enabled

□ HTTP Request □ Socket Network Statistics ☑ Socket Connect □ DNS Query □ Socket Listen □ Socket Close □ Socket Accept

FortiEDR is now configured to issue eXtended detection alerts from AWS GuardDuty.

Custom

To integrate FortiEDR with a custom system to collect activity log and issue eXtended detection alerts, you must configure an eXtended detection source connector with the custom system and enable the eXtended detection rules and FortiEDR Threat Hunting events collection.

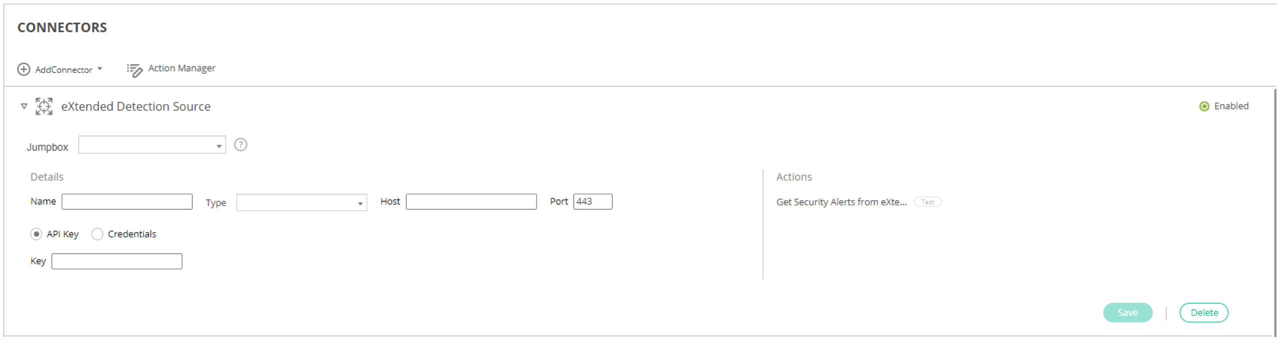
Prerequisites

Before you start integrating FortiEDR with a custom system, verify you have the following:

- A valid license for eXtended Detection Response—While you can create an eXtended detection source connector without a valid license for eXtended Detection Response, the license is required for a successful XDR definition.
- A Jumpbox with connectivity to the custom system. Details about how to install a FortiEDR Core and configure it as a Jumpbox are provided in Setting up the FortiEDR Core on page 511. You may refer to Cores on page 403 for more information about configuring a Jumpbox.
- Connectivity from the FortiEDR Central Manager to the Fortinet Cloud Services (FCS).

Setting up a connector for the custom system

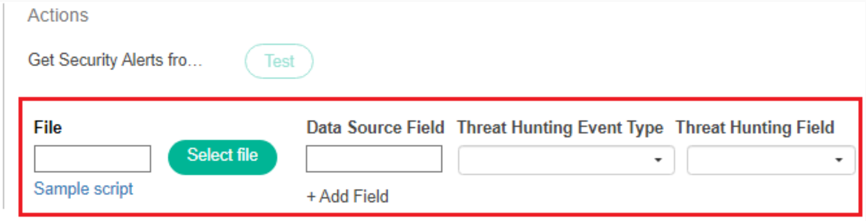
1. Click the *Add Connector* button and select *eXtended Detection Source* in the *Connectors* dropdown list. The following displays:



Port 443

● API Key ○ Credentials

2. Fill in the following fields:

Field	Definition
Enabled	Check this checkbox to enable blocking of malicious IP addresses by the custom system.
Jumpbox	Select the FortiEDR Jumpbox that will communicate with the custom system.
Name	Specify a name of your choice to identify the custom system.
Type	Select *Custom*.
Host	Specify the IP or DNS address of the custom system.
Port	Specify the port that is used for API communication with the custom system.
API Key/Credentials	Specify authentication details of the custom system.
Actions Parameters	1. Upload a script file that contains all the authentication details for the external system and the query for FortiEDR to pull data from the system. Use the sample script as a starting point to build your own script by replacing all the values with those for your system. 2. Specify the name of the data source field in the external system for FortiEDR to correlate with. You can add fields as needed. 3. For each data source field, select the corresponding *Threat Hunting Event Type* and *Threat Hunting Field* for FortiEDR to correlate data with.  Actions Get Security Alerts fro... Test File Select file Sample script Data Source Field Threat Hunting Event Type Threat Hunting Field + Add Field

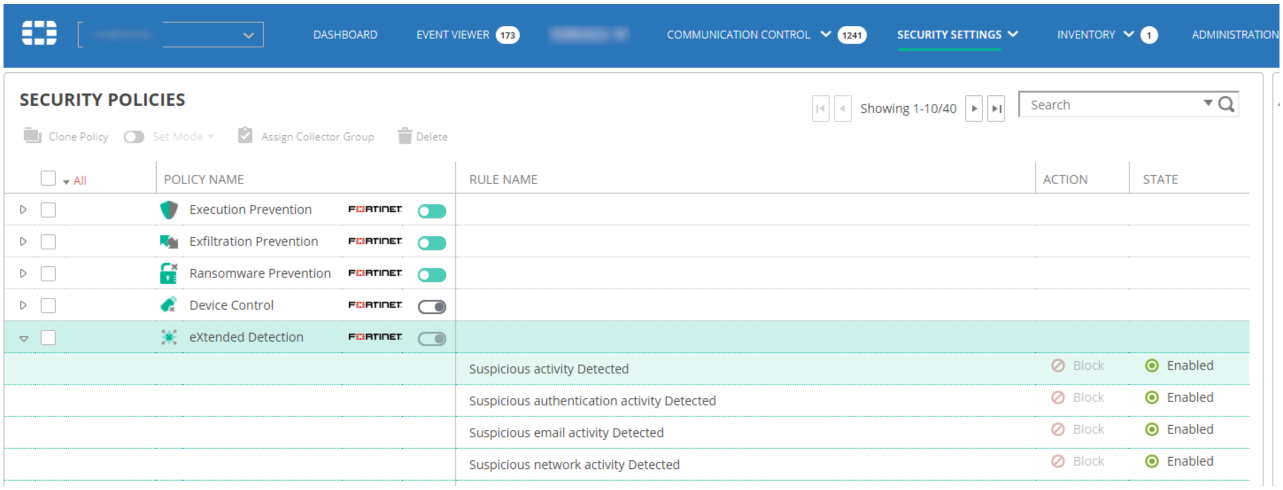
3. Click *Save*.

Setting up FortiEDR Central Manager

In order to complete the integration with the custom system, the eXtended detection rules and FortiEDR Threat Hunting events collection must be enabled with the FortiEDR Central Manager, as follows.

To enable eXtended detection rules:

1. Navigate to the *SECURITY SETTINGS* > *Security Policies* page.
2. Open the eXtended detection policy that is applied on devices on which you want the eXtended detection policy to apply and click the *Disabled* button next to each of the underlying rules to enable it, as shown below:

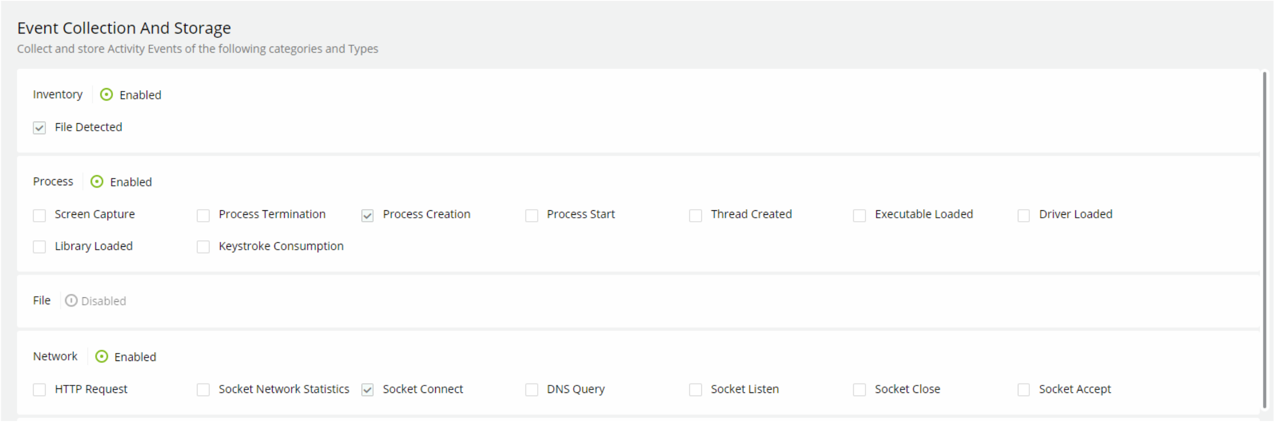


SECURITY POLICIES

All	POLICY NAME		RULE NAME	ACTION	STATE
▷ □	Execution Prevention	FORTINET			
▷ □	Exfiltration Prevention	FORTINET			
▷ □	Ransomware Prevention	FORTINET			
▷ □	Device Control	FORTINET			
▽ □	eXtended Detection	FORTINET			
			Suspicious activity Detected	Block	Enabled
			Suspicious authentication activity Detected	Block	Enabled
			Suspicious email activity Detected	Block	Enabled
			Suspicious network activity Detected	Block	Enabled

To enable FortiEDR Threat Hunting events collection:

1. Navigate to the *SECURITY SETTINGS* > *Threat Hunting* > *Collection Profiles* page.
2. Open the Threat Hunting collection profile that is applied on devices on which you want the eXtended detection policy to apply.
3. Select the following event types on that profile:
   - Socket Connect
   - Process Creation
   - File Create
   - File Detected



Event Collection And Storage

Collect and store Activity Events of the following categories and Types

Inventory ● Enabled

☑ File Detected

Process ● Enabled

□ Screen Capture □ Process Termination ☑ Process Creation □ Process Start □ Thread Created □ Executable Loaded □ Driver Loaded

□ Library Loaded □ Keystroke Consumption

File ○ Disabled

Network ● Enabled

□ HTTP Request □ Socket Network Statistics ☑ Socket Connect □ DNS Query □ Socket Listen □ Socket Close □ Socket Accept

FortiEDR is now configured to issue eXtended detection alerts from the custom system.

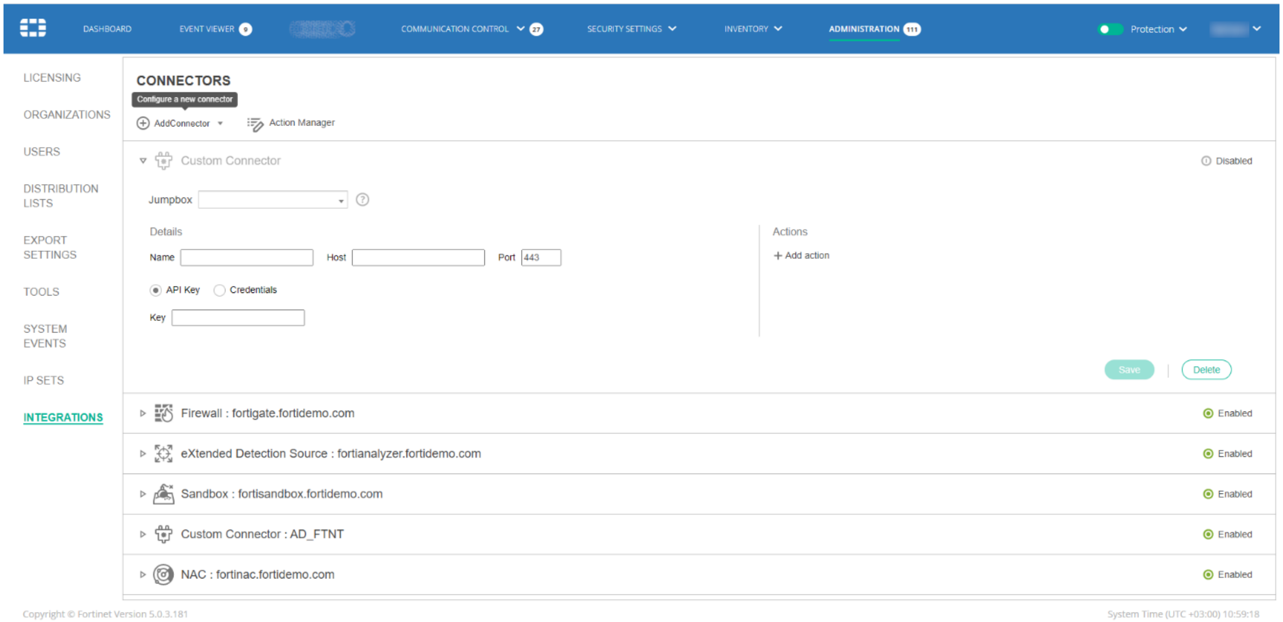
Custom integration

The *CUSTOM* section enables you to connect to any third-party system in order to automatically trigger an incident response in that third-party system as the result of a security event detected by FortiEDR. After you define a Custom Integration connector (and its actions) and configure a relevant Playbook policy, an automatic incident response action will be triggered in the third-party system upon the triggering of a security event.

Custom integration is only available to users with Admin or IT permissions and have the *Custom script* option enabled. For more information about user roles and permissions, see Users on page 277.

To set up a custom integration connector in FortiEDR:

1. Click the *Add Connector* button and select *Custom Connector* from the dropdown list. The following displays:



CONNECTORS

Custom Connector — Disabled

Jumpbox

Details

Name Host Port 443

● API Key ○ Credentials

Key

Actions

Firewall : fortigate.fortidemo.com — Enabled

eXtended Detection Source : fortianalyzer.fortidemo.com — Enabled

Sandbox : fortisandbox.fortidemo.com — Enabled

Custom Connector : AD_FTNT — Enabled

NAC : fortinac.fortidemo.com — Enabled

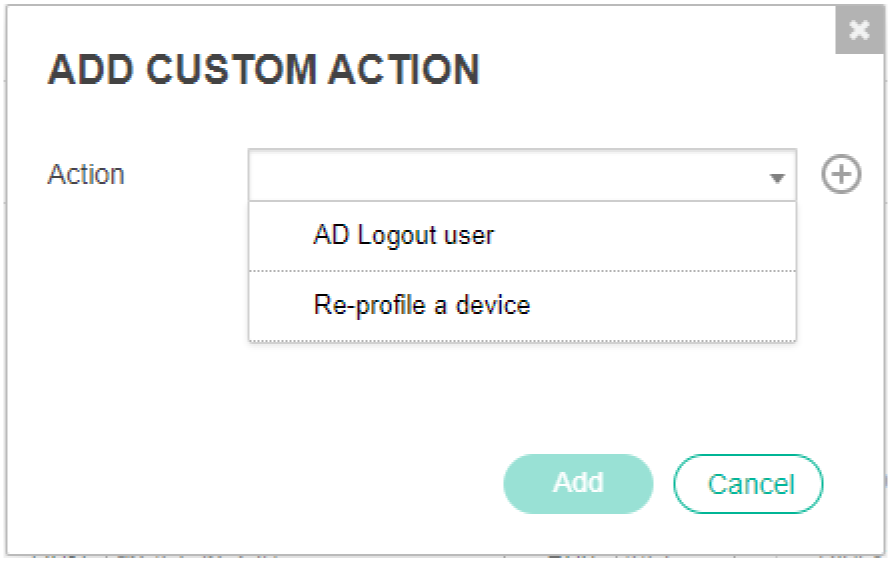
Copyright © Fortinet Version 5.0.3.181

System Time (UTC +03:00) 10:59:18

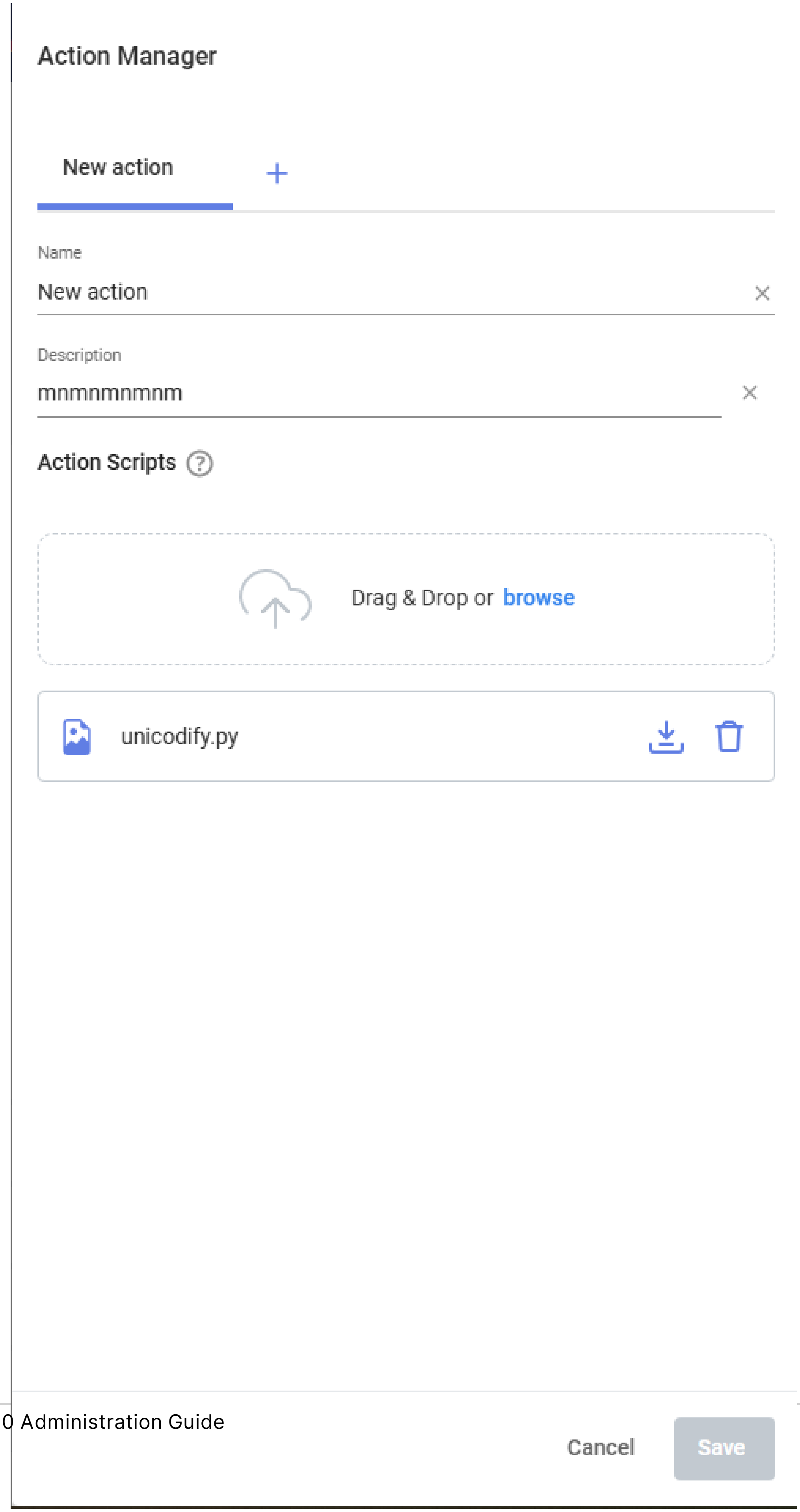
2. Fill in the following fields:

Field	Description
Jumpbox	Select the FortiEDR Jumpbox that will communicate with the third-party system. A FortiEDR deployment must include a Jumpbox that has connectivity to the external system of this custom integration connector. This Jumpbox must be exclusive to this organization and cannot function as a Core.
Name	Specify a name of your choice to be used to identify this custom connector.
Host	Specify the IP or DNS address of the relevant third-party application.
Port	Specify the port that is used for API communication with the relevant third-party application.
API Key/Credentials	Specify authentication details of the relevant third-party application. To use an API token, click the *API Key* radio button and copy the token value into the text box. To use API credentials, click the *Credentials* radio button and enter the relevant third-party application's API username and password.

3. In the *Actions* area on the right, define the action to be taken by this custom connector, as follows:
   - To trigger an action on a custom connected third-party system, click the **+ Add Action** button to display the following popup window:



1. In the *Action* dropdown menu, select one of the previously defined actions (which were defined in FortiEDR as described Custom integration on page 370).
   -OR-
2. Click the *Create New Action* button in this popup window to define a new action that can be triggered according to the definitions in the Playbook, as described in the next section below.
   The following displays:



Action Manager

Name: New action

Description: mnmnmnmnm

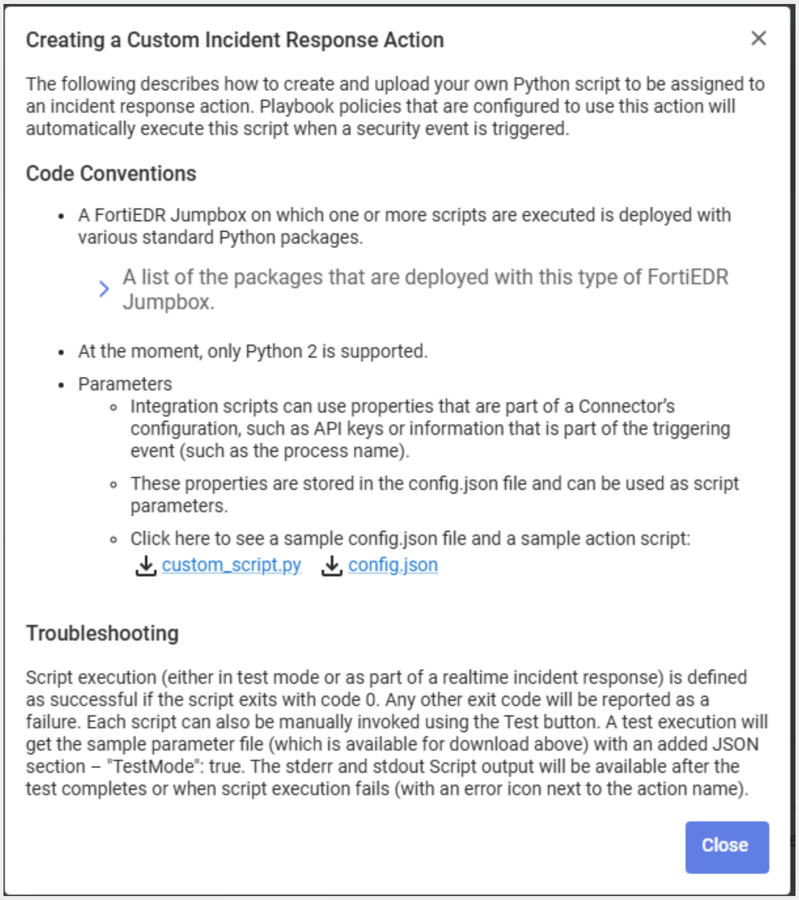
Action Scripts

unicodify.py

Fill out the fields of this window as follows in order to define a new action to be triggered in response to an incident.

In order to trigger this action, a Playbook policy must be defined that triggers this action to execute the script when a security event is triggered. The definition of this new action here automatically adds this action as an option in a Playbook policy. This action however, is not selected by default in the Playbook policy. Therefore, you must go to the Playbook policy and select it in order for it to be triggered when a security event is triggered.

Field	Definition
Name	Enter any name for this action.
Description	Enter a description of this action.
Upload	Upload a Python script that calls an API from the third-party system in order to perform the relevant action. Python 2.7 or later is supported. The Python script must be created according to the coding conventions that can be displayed by clicking the ? icon next to the *Action Scripts* field. The following displays providing an explanation of the coding conventions and provides various links that you can click to see more detail and/or to download sample files.

Field	Definition
	

Creating a Custom Incident Response Action ✕

The following describes how to create and upload your own Python script to be assigned to an incident response action. Playbook policies that are configured to use this action will automatically execute this script when a security event is triggered.

Code Conventions

- A FortiEDR Jumpbox on which one or more scripts are executed is deployed with various standard Python packages.

  › A list of the packages that are deployed with this type of FortiEDR Jumpbox.

- At the moment, only Python 2 is supported.
- Parameters
  - Integration scripts can use properties that are part of a Connector's configuration, such as API keys or information that is part of the triggering event (such as the process name).
  - These properties are stored in the config.json file and can be used as script parameters.
  - Click here to see a sample config.json file and a sample action script:
    custom_script.py config.json

Troubleshooting

Script execution (either in test mode or as part of a realtime incident response) is defined as successful if the script exits with code 0. Any other exit code will be reported as a failure. Each script can also be manually invoked using the Test button. A test execution will get the sample parameter file (which is available for download above) with an added JSON section – "TestMode": true. The stderr and stdout Script output will be available after the test completes or when script execution fails (with an error icon next to the action name).

3. Click *Save*. The new action is then listed in the Actions area.

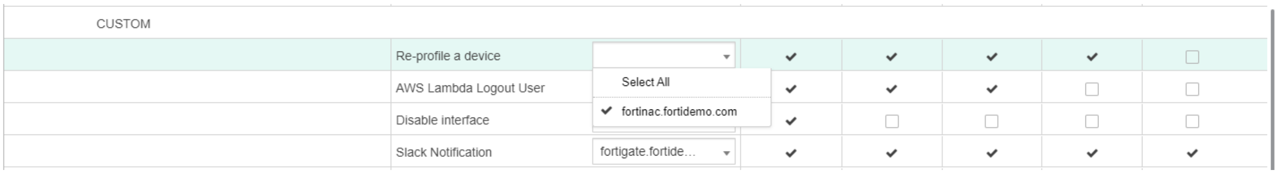
4. Select this action to associate it with the custom connector.
5. You can click the *Test* button next to it to execute this action.
   A new row is added to the *CUSTOM* section of the *Automated Incident Response – Playbooks* page. In order for this custom integration connector to trigger an action, you must define it in the Playbook, as described below.

The actions that you define here can also be selected as an action for a Firewall integration on page 341 connector or Network Access Control (NAC) integration on page 350 connector. These integration connectors might use the same API. Alternatively, you may need to upload a different script that will be used to perform the same action on different third-party products. You can associate several scripts with the same action and select the appropriate one per connector. For example, an IM notification action could have two scripts – one for notifications via Slack and the other for notifications via Teams.

Playbooks configuration

To configure an automated incident response that triggers an action using this custom integration connector upon the triggering of a security event:

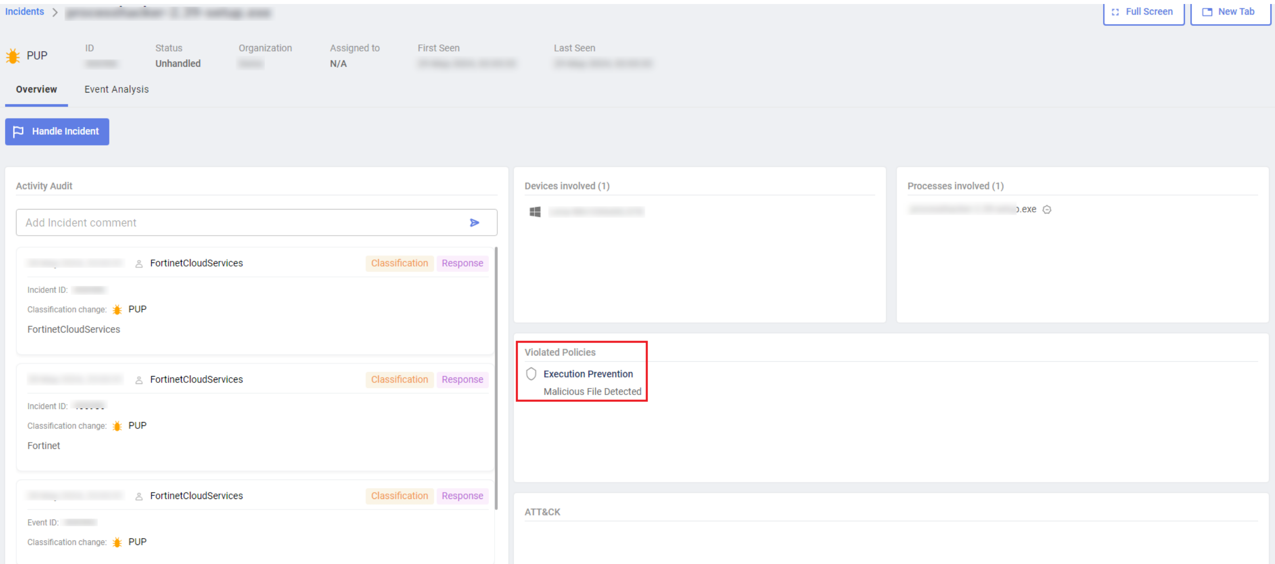
1. Navigate to the *SECURITY SETTINGS > Playbooks* page.
2. Open the Playbook policy that is applied on devices for which you want the custom action (defined above) to apply.
3. In the *CUSTOM* section, place a checkmark in the relevant Classification columns next to the row of that action.
4. In the dropdown menu next to the action, select the connector with which to perform the action or click *Select All*, as shown below:



CUSTOM						
Re-profile a device	▾ Select All ✓ fortinac.fortidemo.com	✓	✓	✓	✓	□
AWS Lambda Logout User		✓	✓	✓	□	□
Disable interface		✓	□	□	□	□
Slack Notification	fortigate.fortide... ▾	✓	✓	✓	✓	✓

The example above showed how to configure two custom connectors by using the same action named IM notification in the Playbook – one for notifications via Teams and the other for notifications via Slack.

FortiEDR is now configured to trigger this action in the third-party system upon the triggering of a security event. This automatic incident response action appears in the *Overview* tab when you select the incident and click *Investigate* in the *Incidents* pane.



Identity Management integration

When an Identity Management connector, such as FortiClient Endpoint Management Server (EMS), is set and Playbook policies are configured, automatic incident response actions can include ZeroTrust device tagging on FortiClient EMS upon security event triggering.

For more details about integrating FortiEDR with FortiClient EMS, refer to the FortiClient EMS Integration Guide.

Prerequisites

Before you start Identity Management configuration, verify the following:

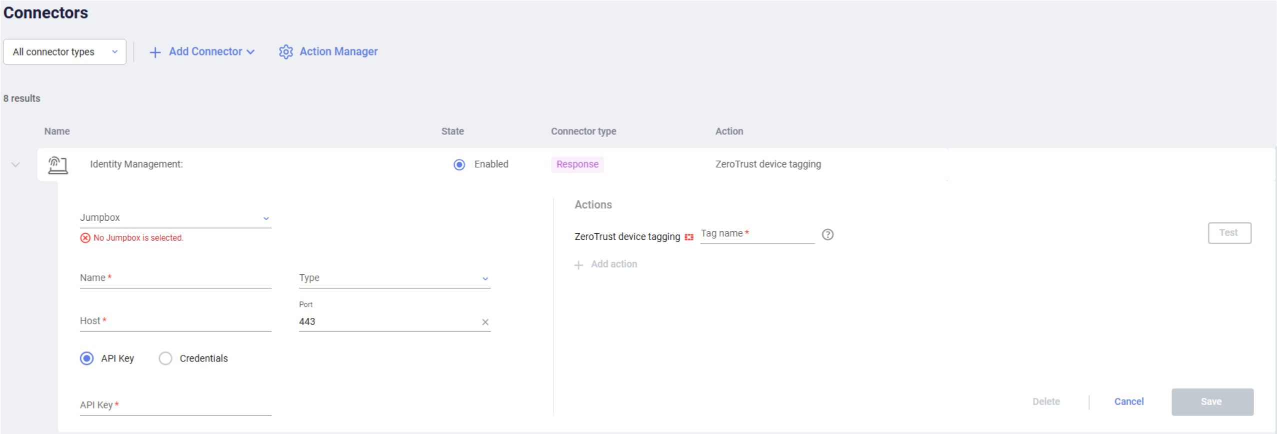
- Your FortiEDR deployment includes a Jumpbox that has connectivity to the identity management server.
  - Refer to Setting up the FortiEDR Core on page 511 for details about how to install a FortiEDR Core and configure it as a Jumpbox.
  - Refer to Cores on page 403 for more information about configuring a Jumpbox.
- The FortiEDR Central Manager has connectivity to the Fortinet Cloud Services (FCS).
- You have a valid user with access to the identity management system. For FortiClient EMS, the following type of user is required depending on the deployment type:
  - **FortiClient EMS On-Premise**—A valid API user. See the FortiClient EMS Integration Guide for detailed instructions.
  - **FortiClient EMS Cloud**— FortiCloud master user (e.g. email address) with read/write access to the FortiClient EMS Cloud portal. Sub user accounts cannot be used. See the FortiCloud IAM documentation for detailed instructions about creating a permission profile and an API user.

Follow the steps below to tag a device as non-trusted automatically upon the detection of a FortiEDR security event.

Configuring a FortiEDR Connector

To configure Identity Management integration:

1. Click the *Add Connector* button and select *Identity Management* from the dropdown list.
   The following displays:



8 results

Name	State	Connector type	Action
Identity Management:	● Enabled	Response	ZeroTrust device tagging

Jumpbox
No Jumpbox is selected.

Name *

Type

Host *

Port
443

● API Key ○ Credentials

API Key *

Actions

ZeroTrust device tagging Tag name *

2. Fill in the following fields:

Field	Description
Jumpbox	Select the FortiEDR Jumpbox that will communicate with this Identity Management system.
Name	Specify a name of your choice to be used to identify this Identity Management system.
Type	Select the type of Identity Management to be used in the dropdown list. For example, *FortiClient EMS*.

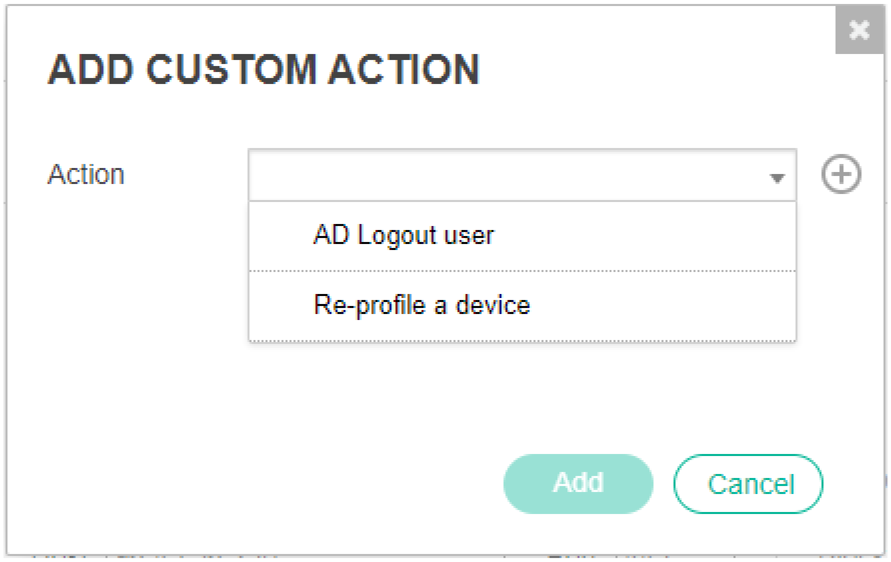
Field	Description
Host	Specify the IP or DNS address of the external Identity Management system.
Port	Specify the port that is used for communication with the external Identity Management system.
API Key/Credentials	Specify authentication details of the external Identity Management system. Fill in the external Identity Management system API username/Account and password/key. For FortiClient EMS, specify the following depending on your deployment type: • **(FortiClient EMS on-premise)** Specify the username and password of the FortiClient EMS Admin User. • **(FortiClient EMS cloud)** Specify the account (e.g. email address) and password of the FortiCloud master user with read/write access to the FortiClient EMS Cloud portal. Sub user accounts cannot be used.

3. In the *Actions* area on the right, define the action to be taken by this connector:
   - To use an action provided out-of-the-box with FortiEDR (for example, Zero Trust device tagging on FortiClient EMS), tag the device as non-trusted the Identity management system and specify the classification tag to apply on the device in the *Tag name* field.
     This step is optional for FortiClient EMS 7.2 or later as it has the following fabric tags predefined for FortiEDR. Both the predefined fabric tags and classification tags, if any, will be used by FortiClient EMS 7.2 or later to tag the device.
     - **FortiEDR_Malicious**: FortiEDR has classified this endpoint as malicious.
     - **FortiEDR_PUP**: FortiEDR has detected a potentially unwanted program on this endpoint.
     - **FortiEDR_Suspicious**: FortiEDR has detected suspicious activity on this endpoint.
     - **FortiEDR_Likely_Safe**: FortiEDR has detected this endpoint as likely to be safe.
     - **FortiEDR_Probably_Good**: FortiEDR has determined that this endpoint is not a safety risk.

     See the FortiClient EMS Administration Guide for more information about endpoint tagging in FortiClient EMS.

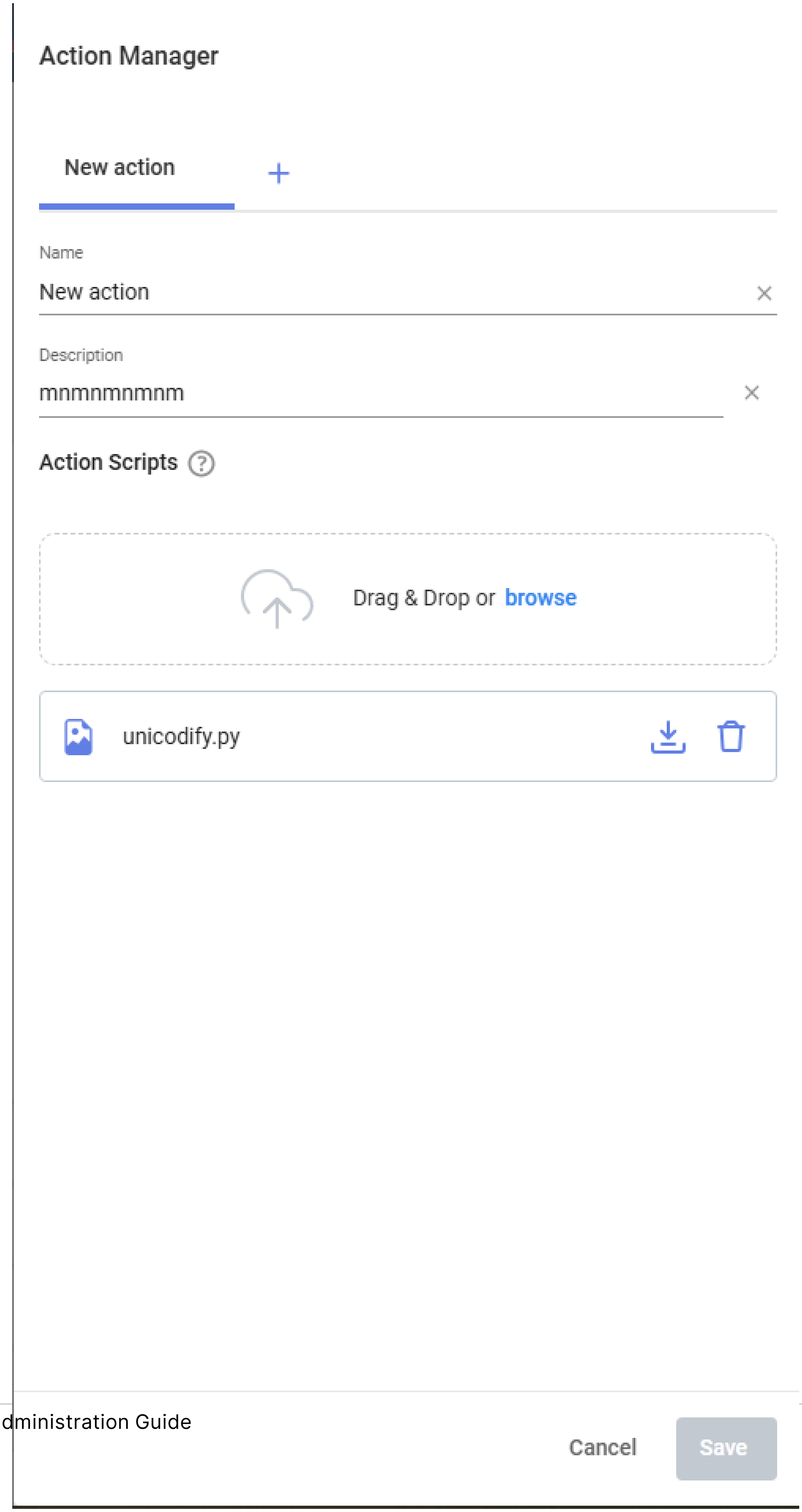
- To use a custom integration action:

  i. Click the *+ Add Action* button. The following popup window displays:



  ii. In the *Action* dropdown menu, select one of the previously defined actions (which were defined in FortiEDR as described in Custom integration on page 370), or define a new action that can be triggered according to the definitions in the Playbook:

i. Click the *Create New Action* button. The following displays:



Action Manager

Name: New action

Description: mnmnmnmnm

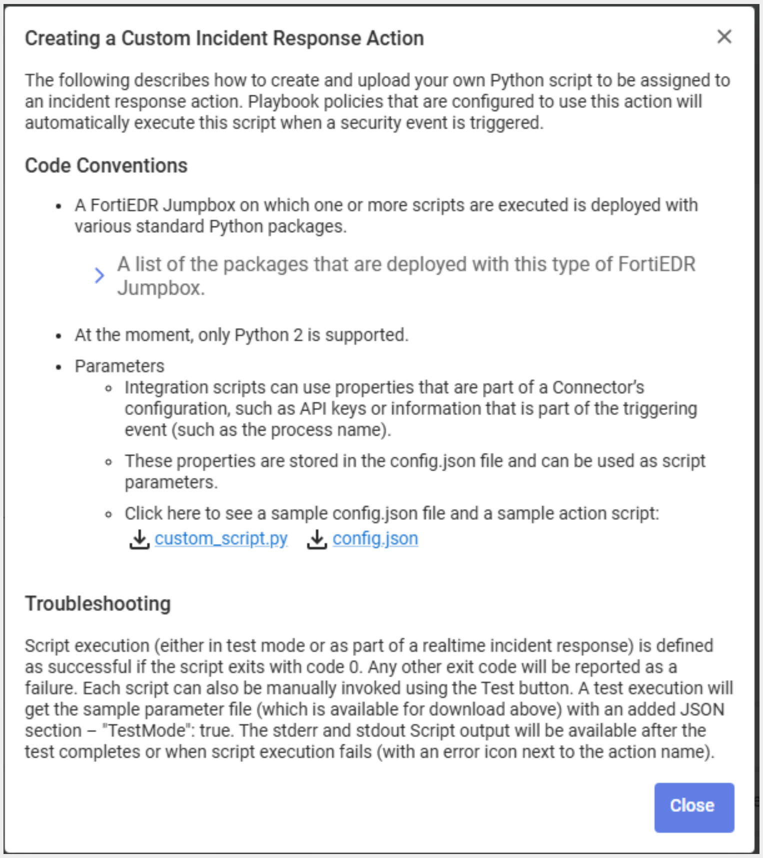
Action Scripts

unicodify.py

ii. Fill out the fields of this window as follows in order to define a new action to be triggered in response to an incident.

In order to trigger this action, a Playbook policy must be defined that triggers this action to execute the script when a security event is triggered. The definition of this new action here automatically adds this action as an option in a Playbook policy. However, this action is not selected by default in the Playbook policy. Therefore, you must go to the Playbook policy and select it in order for it to be triggered when a security event is triggered.

Field	Definition
Name	Enter any name for this action.
Description	Enter a description of this action.
Upload	Upload a Python script that calls an API from the third-party system in order to perform the relevant action. Python 2.7 or later is supported. The Python script must be created according to the coding conventions that can be displayed by clicking the ? icon next to the *Action Scripts* field. The following displays providing an explanation of the coding conventions and provides various links that you can click to see more detail and/or to download sample files.

Field	Definition
	

Creating a Custom Incident Response Action

The following describes how to create and upload your own Python script to be assigned to an incident response action. Playbook policies that are configured to use this action will automatically execute this script when a security event is triggered.

Code Conventions

- A FortiEDR Jumpbox on which one or more scripts are executed is deployed with various standard Python packages.
  - › A list of the packages that are deployed with this type of FortiEDR Jumpbox.
- At the moment, only Python 2 is supported.
- Parameters
  - Integration scripts can use properties that are part of a Connector's configuration, such as API keys or information that is part of the triggering event (such as the process name).
  - These properties are stored in the config.json file and can be used as script parameters.
  - Click here to see a sample config.json file and a sample action script: custom_script.py config.json

Troubleshooting

Script execution (either in test mode or as part of a realtime incident response) is defined as successful if the script exits with code 0. Any other exit code will be reported as a failure. Each script can also be manually invoked using the Test button. A test execution will get the sample parameter file (which is available for download above) with an added JSON section – "TestMode": true. The stderr and stdout Script output will be available after the test completes or when script execution fails (with an error icon next to the action name).

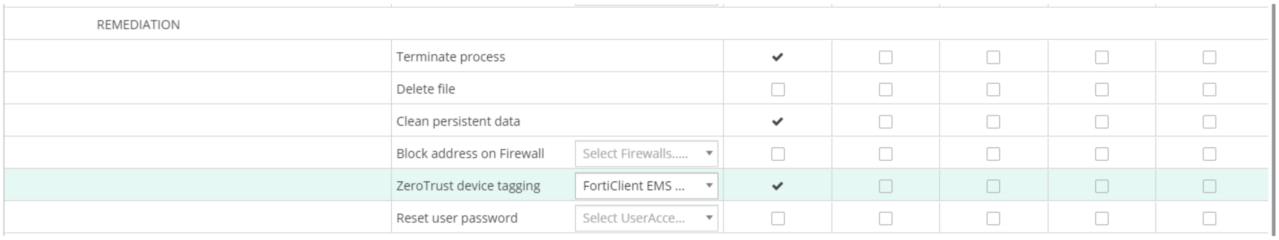
iii. Click *Save*. The new action is then listed in the *Actions* area.

4. You can click the *Test* button next to an action to execute that action.
5. Click *Save* to save the connector configuration.

Configuring Playbooks

To configure an automated incident response that uses an Identity Management connector to tag a device upon security event triggering:

1. Navigate to the *SECURITY SETTINGS* > *Playbooks* page.
2. Open the Playbook policy that is applied on devices for which you want the identity management response to apply.
3. Place a checkmark in the relevant *Classification* column next to the *Zero Trust device tagging* row under the *REMEDIATION* section.
   FortiEDR is now configured to automatically tag a device as non-trusted upon triggering of a security event.

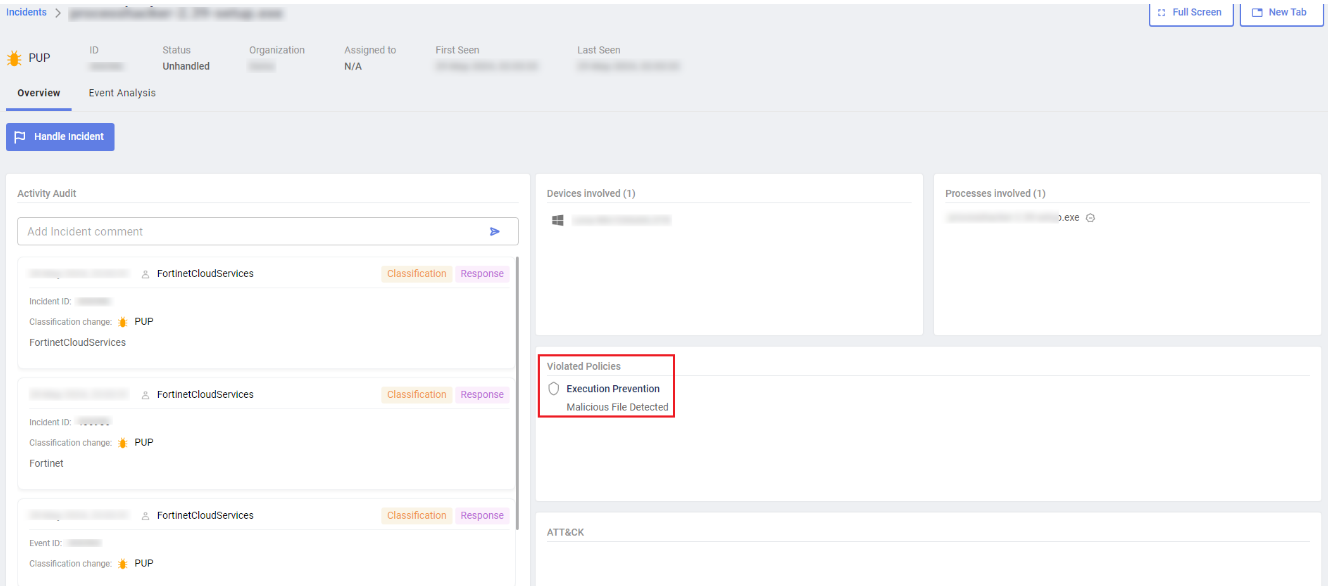


REMEDIATION							
	Terminate process		✓	□	□	□	□
	Delete file		□	□	□	□	□
	Clean persistent data		✓	□	□	□	□
	Block address on Firewall	Select Firewalls..... ▾	□	□	□	□	□
	ZeroTrust device tagging	FortiClient EMS ... ▾	✓	□	□	□	□
	Reset user password	Select UserAcce... ▾	□	□	□	□	□

To configure an automated incident response that uses an Identity Management connector to perform a custom action upon the triggering of a security event:

1. Navigate to the *SECURITY SETTINGS* > *Playbooks* page.
2. Open the Playbook policy that is applied on devices for which you want the custom action (defined above) to apply.
3. In the *CUSTOM* section, place a checkmark in the relevant *Classification* columns next to the row of the relevant custom action.
4. In the dropdown menu next to the relevant custom action, select the relevant Identity Management connector with which to perform the action.
   FortiEDR is now configured to trigger this action in the third-party system upon the triggering of a security event.

Automatic incident response actions are listed in the *Overview* tab when you select the incident and click *Investigate* in the *Incidents* pane, as shown below:



Incidents > [redacted]

PUP

ID	Status	Organization	Assigned to	First Seen	Last Seen
[redacted]	Unhandled	[redacted]	N/A	[redacted]	[redacted]

Activity Audit

Add Incident comment

[redacted] FortinetCloudServices Classification Response
Incident ID: [redacted]
Classification change: PUP
FortinetCloudServices

[redacted] FortinetCloudServices Classification Response
Incident ID: [redacted]
Classification change: PUP
Fortinet

[redacted] FortinetCloudServices Classification Response
Event ID: [redacted]
Classification change: PUP

Devices involved (1)
[redacted]

Processes involved (1)
[redacted].exe

Violated Policies
Execution Prevention
Malicious File Detected

ATT&CK

User Access integration

When a user access connector, such as Active Directory, is set and Playbook policies are configured, automatic incident response actions can include resetting user’s password or disabling user account on domain controller upon security event triggering.

For more details about integrating FortiEDR with Active Directory, refer to the Active Directory Integration Guide.

Prerequisites

Before you start User Access configuration, verify the following:

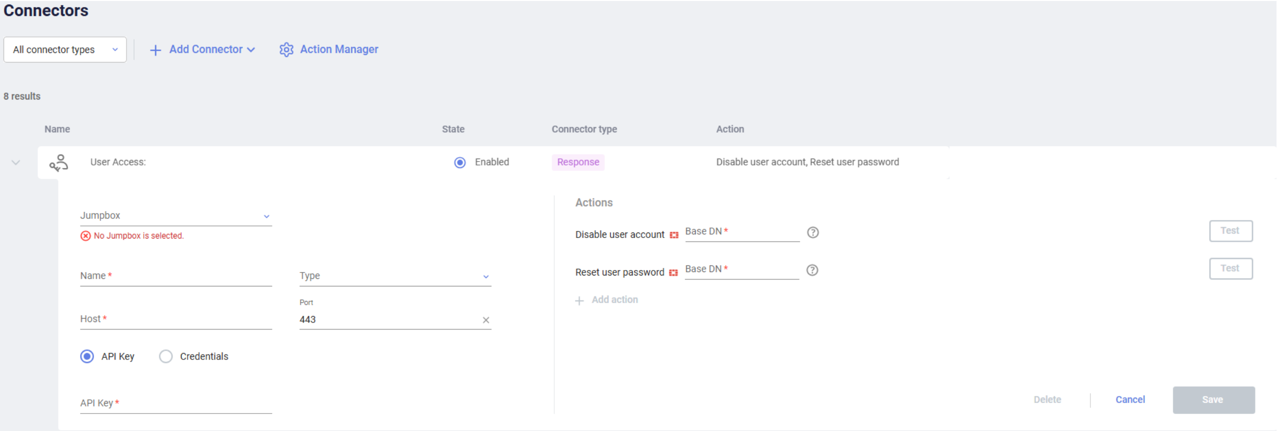
- Your FortiEDR deployment includes a Jumpbox that has connectivity to the domain controller server. Details about how to install a FortiEDR Core and configure it as a Jumpbox are described in Setting up the FortiEDR Core on page 511. You may refer to Cores on page 403 for more information about configuring a Jumpbox.
- The FortiEDR Central Manager has connectivity to the Fortinet Cloud Services (FCS).
- You have a valid API user with access to Active Directory or equivalent domain control system. See the Active Directory Integration Guide for detailed instructions about creating an Active Directory admin user.

Follow the steps below to perform user access actions automatically upon the detection of a FortiEDR security event.

Configuring a FortiEDR Connector

To configure User Access integration:

1. Click the *Add Connector* button and select *User Access* from the dropdown list.
   The following displays:



Connectors

All connector types | + Add Connector | Action Manager

8 results

Name	State	Connector type	Action
User Access:	● Enabled	Response	Disable user account, Reset user password

Jumpbox

No Jumpbox is selected.

Name *

Type

Host *

Port 443

● API Key ○ Credentials

API Key *

Actions

Disable user account Base DN * Test

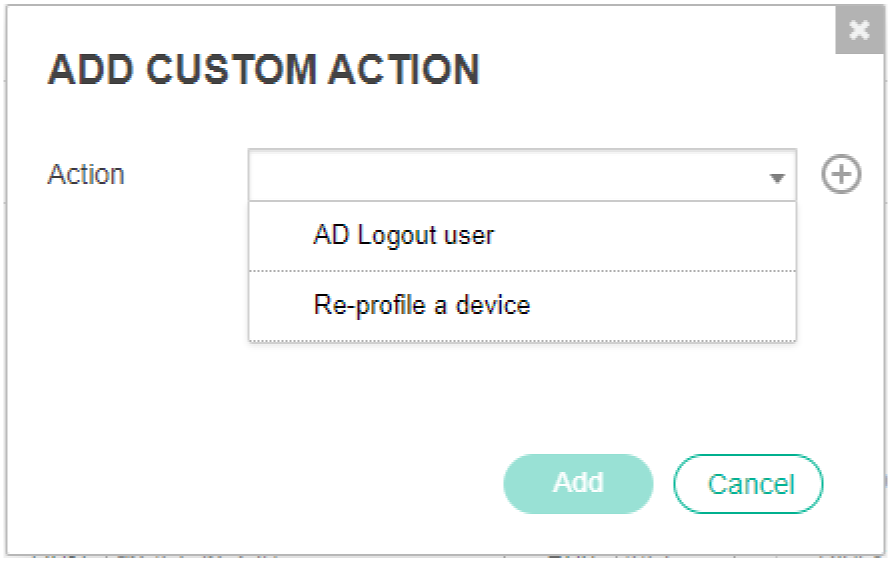
Reset user password Base DN * Test

2. Fill in the following fields:

Field	Description
Jumpbox	Select the FortiEDR Jumpbox that will communicate with this User Access system.
Name	Specify a name of your choice to be used to identify this User Access system.

Field	Description
Type	Select the type of user access to be used in the dropdown list. For example, *Active Directory*.
Host	Specify the IP or DNS address of the external User Access system.
Port	Specify the port that is used for communication with the external User Access system.
API Key/Credentials	Specify authentication details of the external user access system: • To use an API token , click the *API Key* radio button and copy the token value into the text box. • To use API credentials, click the *Credentials* radio button and fill in the external User Access system API username (or Bind User DN) and password.

3. In the *Actions* area on the right, define the action to be taken by this connector:
   - To use an action provided out-of-the-box with FortiEDR (for example, Disable user account on Active Directory), in the *baseDN* field of *Disable user account* or *Reset user password*, specify where FortiEDR starts searching for the user upon which actions are performed.
   - To use a custom integration action:
     i. Click the *+ Add Action* button. The following popup window displays:

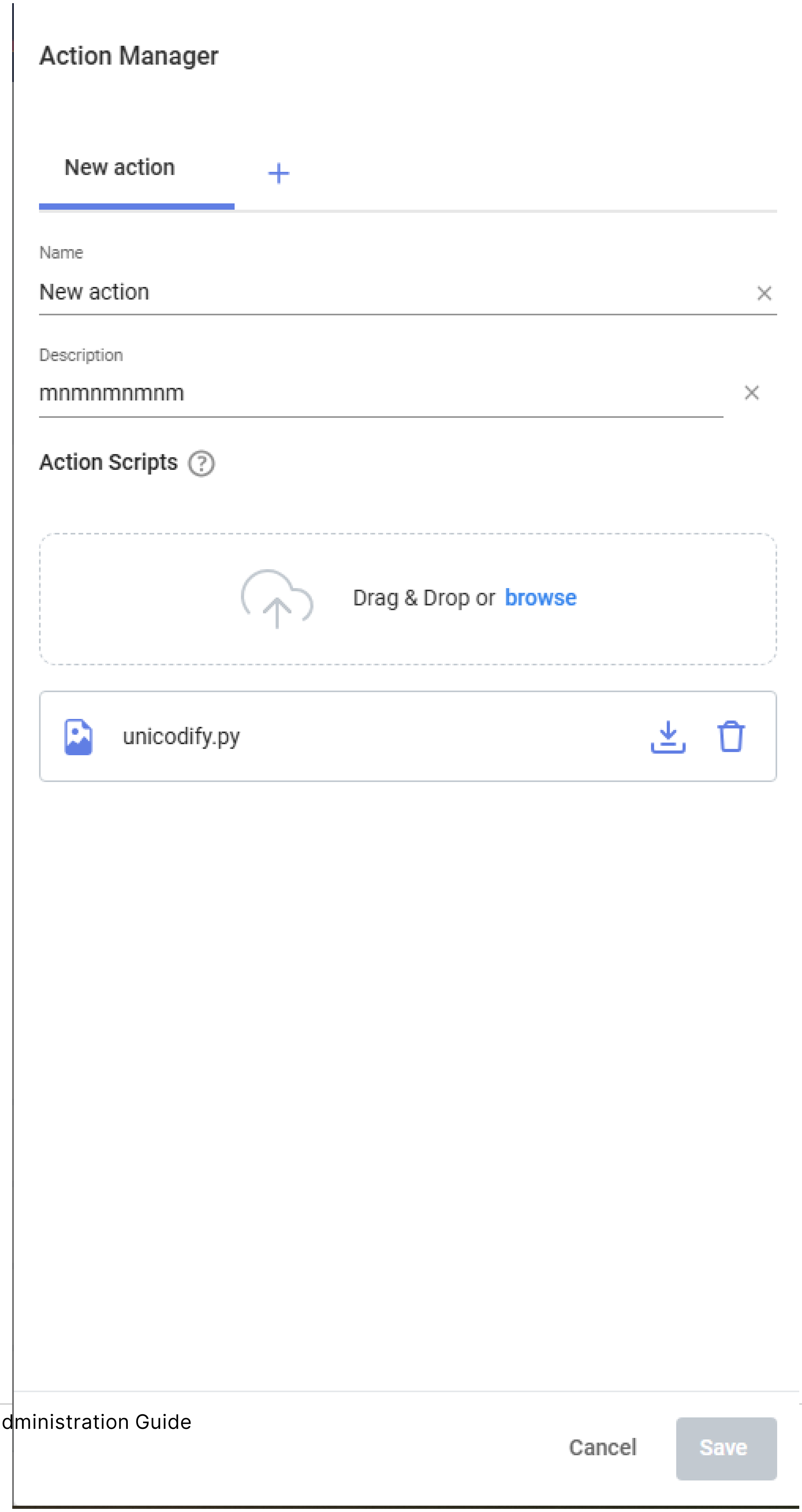


ADD CUSTOM ACTION

Action

     ii. In the *Action* dropdown menu, select one of the previously defined actions (which were defined in FortiEDR as described in Custom integration on page 370), or define a new action that can be triggered according to the definitions in the Playbook:

i. Click the *Create New Action* button. The following displays:



Action Manager

Name: New action

Description: mnmnmnmnm

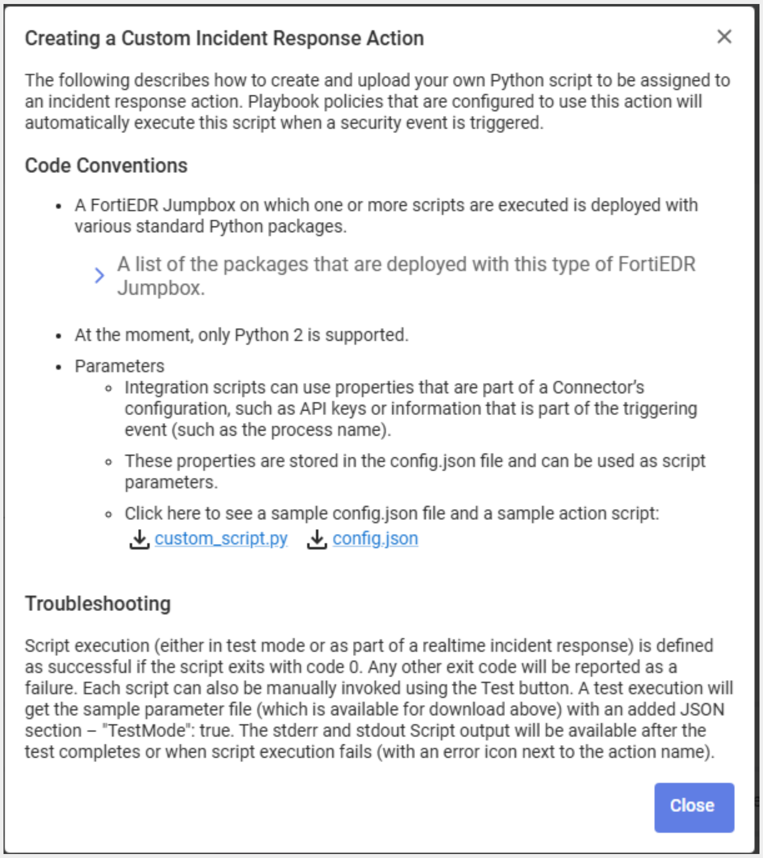
Action Scripts

unicodify.py

ii. Fill out the fields of this window as follows in order to define a new action to be triggered in response to an incident.

In order to trigger this action, a Playbook policy must be defined that triggers this action to execute the script when a security event is triggered. The definition of this new action here automatically adds this action as an option in a Playbook policy. However, this action is not selected by default in the Playbook policy. Therefore, you must go to the Playbook policy and select it in order for it to be triggered when a security event is triggered.

Field	Definition
Name	Enter any name for this action.
Description	Enter a description of this action.
Upload	Upload a Python script that calls an API from the third-party system in order to perform the relevant action. Python 2.7 or later is supported. The Python script must be created according to the coding conventions that can be displayed by clicking the ? icon next to the *Action Scripts* field. The following displays providing an explanation of the coding conventions and provides various links that you can click to see more detail and/or to download sample files.

Field	Definition
	

Creating a Custom Incident Response Action

The following describes how to create and upload your own Python script to be assigned to an incident response action. Playbook policies that are configured to use this action will automatically execute this script when a security event is triggered.

Code Conventions

- A FortiEDR Jumpbox on which one or more scripts are executed is deployed with various standard Python packages.
  - › A list of the packages that are deployed with this type of FortiEDR Jumpbox.
- At the moment, only Python 2 is supported.
- Parameters
  - Integration scripts can use properties that are part of a Connector's configuration, such as API keys or information that is part of the triggering event (such as the process name).
  - These properties are stored in the config.json file and can be used as script parameters.
  - Click here to see a sample config.json file and a sample action script:
    custom_script.py config.json

Troubleshooting

Script execution (either in test mode or as part of a realtime incident response) is defined as successful if the script exits with code 0. Any other exit code will be reported as a failure. Each script can also be manually invoked using the Test button. A test execution will get the sample parameter file (which is available for download above) with an added JSON section – "TestMode": true. The stderr and stdout Script output will be available after the test completes or when script execution fails (with an error icon next to the action name).

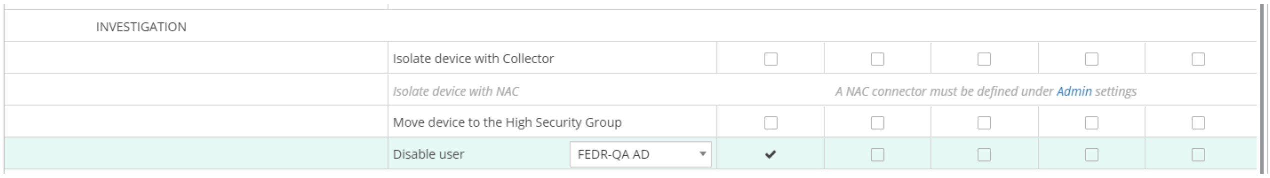
iii. Click *Save*. The new action is then listed in the *Actions* area.

4. You can click the *Test* button next to an action to execute that action.
5. Click *Save* to save the connector configuration.

Configuring Playbooks

To configure an automated incident response that uses a user access connector to reset user password or disable a user upon security event triggering:

1. Navigate to the *SECURITY SETTINGS* > *Playbooks* page.
2. Open the Playbook policy that is applied on devices for which you want the user access response to apply.
3. Place a checkmark in the relevant *Classification* column next to the *Disable user* row under the *INVESTIGATION* section or the *Reset user password* row under the *REMEDIATION* section.
   FortiEDR is now configured to automatically perform user access actions upon triggering of a security event.

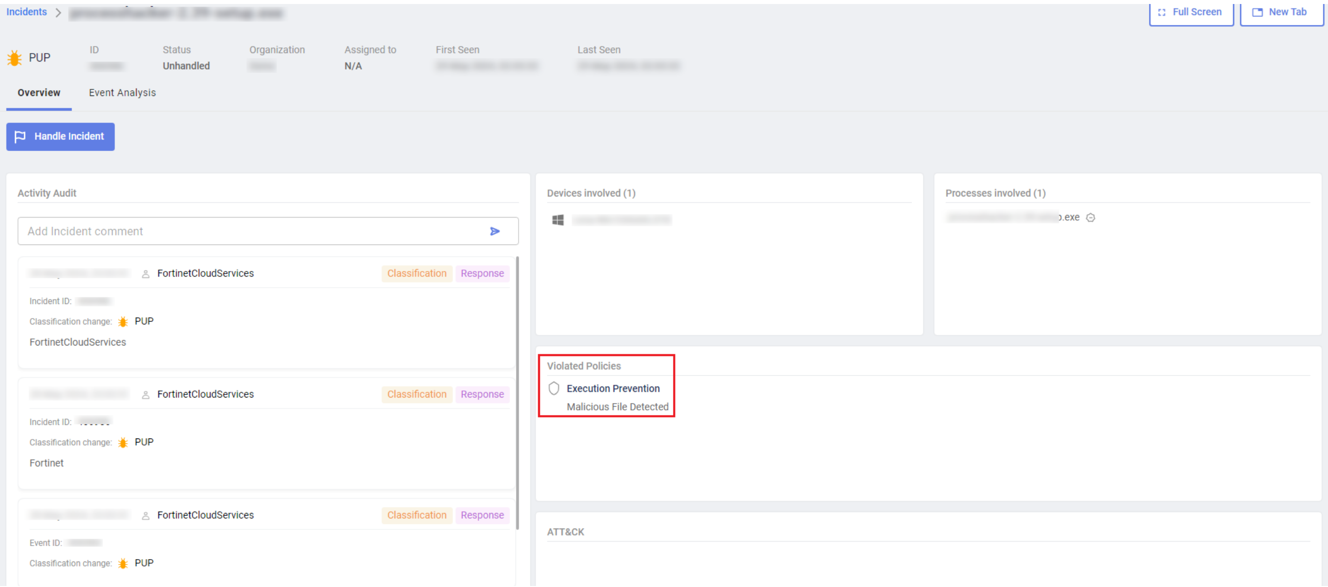


INVESTIGATION						
	Isolate device with Collector	☐	☐	☐	☐	☐
	Isolate device with NAC	*A NAC connector must be defined under Admin settings*				
	Move device to the High Security Group	☐	☐	☐	☐	☐
	Disable user FEDR-QA AD	✓	☐	☐	☐	☐

To configure an automated incident response that uses a User Access connector to perform a custom action upon the triggering of a security event:

1. Navigate to the *SECURITY SETTINGS > Playbooks* page.
2. Open the Playbook policy that is applied on devices for which you want the custom action (defined above) to apply.
3. In the *CUSTOM* section, place a checkmark in the relevant *Classification* columns next to the row of the relevant custom action.
4. In the dropdown menu next to the relevant custom action, select the relevant User Access connector with which to perform the action.
   FortiEDR is now configured to trigger this action in the third-party system upon the triggering of a security event.

Automatic incident response actions are listed in the*Overview* tab when you select the incident and click *Investigate* in the *Incidents* pane, as shown below:



PUP | ID [redacted] | Status Unhandled | Organization [redacted] | Assigned to N/A | First Seen [redacted] | Last Seen [redacted]

Activity Audit

Add Incident comment

[redacted] FortiNetCloudServices Classification Response
Incident ID: [redacted]
Classification change: PUP
FortinetCloudServices

[redacted] FortiNetCloudServices Classification Response
Incident ID: [redacted]
Classification change: PUP
Fortinet

[redacted] FortiNetCloudServices Classification Response
Event ID: [redacted]
Classification change: PUP

Devices involved (1)
[redacted]

Processes involved (1)
[redacted].exe

Violated Policies
Execution Prevention
Malicious File Detected

ATT&CK

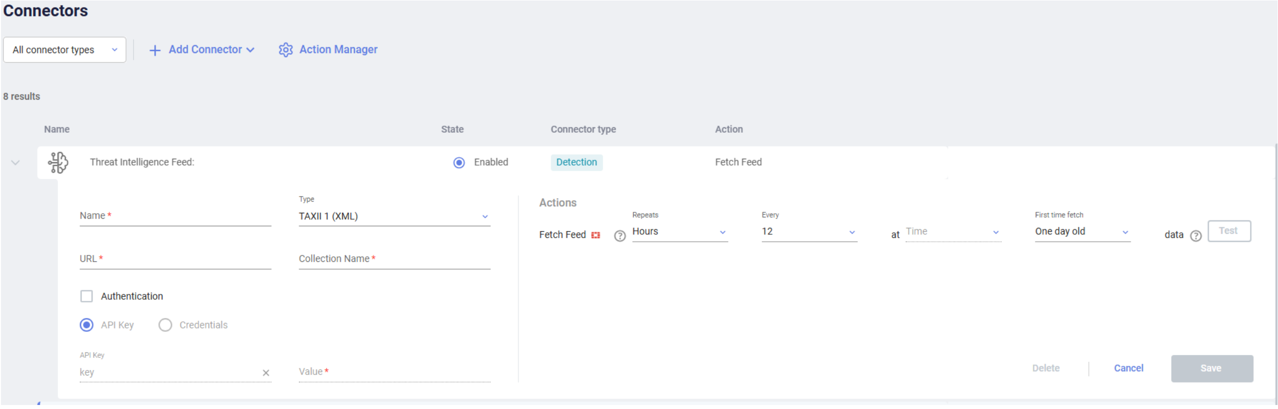
Threat Intelligence Feed integration

When a Threat Intelligence Feed connector is configured, FortiEDR creates a Threat Hunting query based on the data fetched from STIX/TAXII feed. The related query is updated upon each scheduled retrieval of collection data which covers the following indicators: hashes, file names, files size, paths, IPs, usernames, registry keys, URLs, and domain names. You can find the relevant queries under *Threat Hunting > Saved Queries*.

As one Threat Hunting query can include only 150 to 1000 conditions, depending on the indicator type, FortiEDR may create multiple query entries for the same collection.

To set up a Threat Intelligence Feed connector with FortiEDR:

1. Click the *Add Connector* button and select *Threat Intelligence Feed* in the *Connectors* dropdown list. The following displays:



Name	State	Connector type	Action
Threat Intelligence Feed:	● Enabled	Detection	Fetch Feed

Name *

Type: TAXII 1 (XML)

URL *

Collection Name *

□ Authentication

● API Key ○ Credentials

API Key: key

Value *

Actions

Fetch Feed — Repeats: Hours — Every: 12 — at Time — First time fetch: One day old data

2. In the *Details* section, fill in the following fields:

Field	Definition
Name	Specify a name of your choice which will be used to identify this Threat Intelligence Feed Collection.
Type	Select the syntax type of the original query, for example: *TAXII (JSON)* or *TAXII 1 (XML)*.
URL	Specify the IP or DNS address of the Threat Intelligence server.
Collection ID	Specify the collection name of the XML query or collection ID of the JSON query.
Authentication	Select this option to specify authentication details of your Threat Intelligence Feed. To use an API token, click the *API Key* radio button and copy the token value into the text box. To use API credentials, click the *Credentials* radio button and fill in the external system API username and password.
Enabled	Use this option to enable or disable FortiEDR integration with this Threat Intelligence Feed.

3. In the *Actions* section, specify the schedule for FortiEDR to retrieve the provided collection data, which covers the following indicators: hashes, file names, files size, paths, IPs, usernames, registry keys, URLs, and domain names.
4. Specify the age of collection data for the initial retrieval. For example, *One day old* means that only indicators that were added to the Collection during the last day will be retrieved for the initial retrieval.
5. Click the *Test* button to execute the action.

6. Click *Save*.
The Threat Intelligence Feed connector is set up and relevant queries will be created in Saved Queries under Threat Hunting on page 125.

Action Manager

The *Action Manager* button is only available to users with Admin or IT permissions and have the *Custom script* option enabled. For more information about user roles and permissions, see Users on page 277.

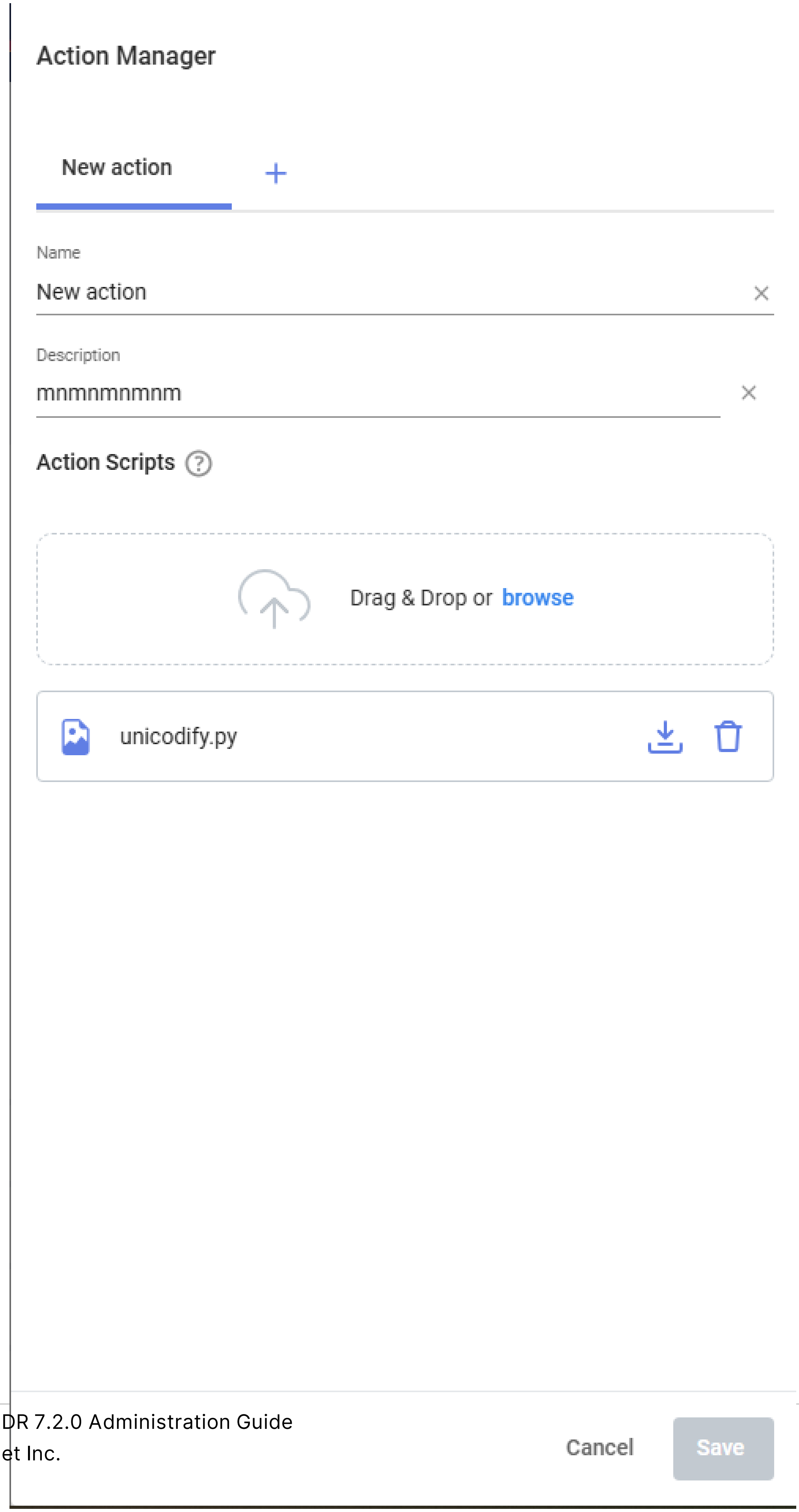
FortiEDR enables you to define connectors to external systems, so that FortiEDR will automatically trigger predefined actions when a security event is triggered in FortiEDR. You can define your own actions while defining a Custom integration connector, Firewall integration connector or NAC integration connector (as described above). Each action is comprised of a Python script (one or several ones) that calls an API from the third-party system in order to perform the relevant action.

The Action Manager enables you to upload and manage (add, modify and delete) these actions and the Python scripts that call third-party systems' APIs. Python 2.7 or later is supported.

To display the Action Manager:

1. In the *Administration* tab, select *Connectors*.

2. Click the *Action Manager* button. The following displays:



Action Manager

New action

Name

New action

Description

mnmnmnmnm

Action Scripts

Drag & Drop or browse

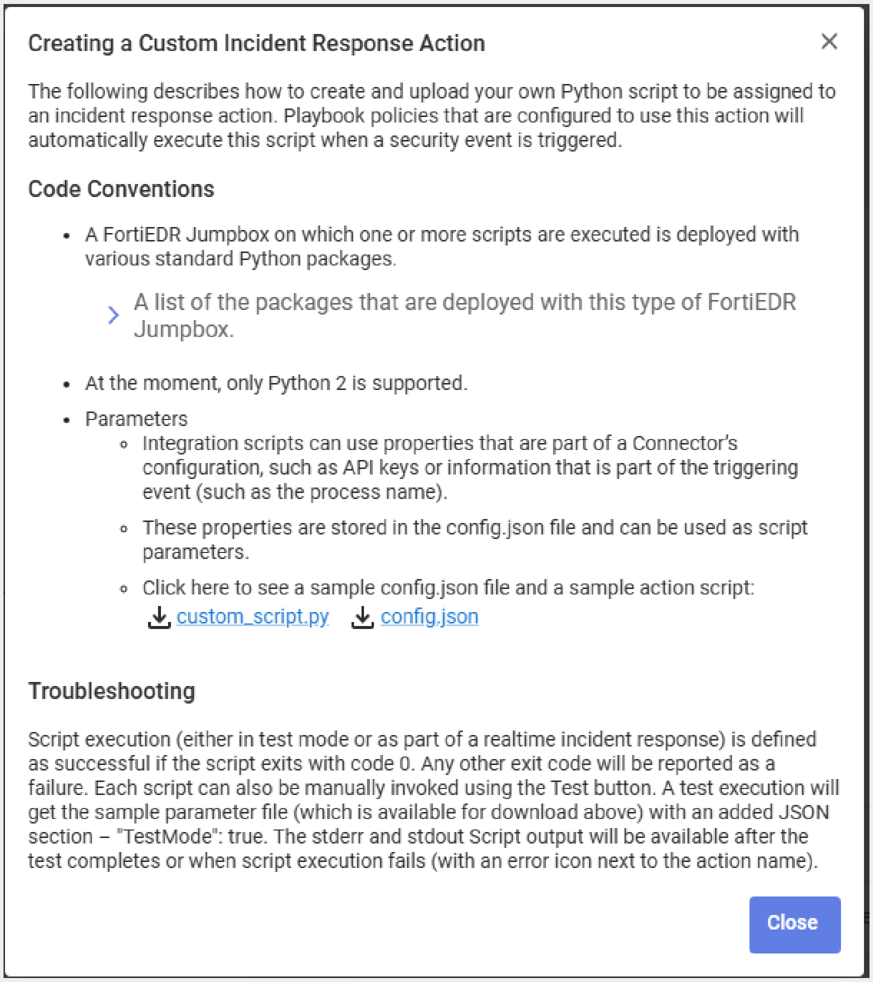
unicodify.py

To define a new action:

1. Click the *+ Add action* button.
2. Fill out the fields of this window as follows in order to define a new action to be triggered in response to an incident.

In order to trigger this action, a Playbook policy must be defined that triggers this action to execute the script when a security event is triggered. The definition of this new action here automatically adds this action as an option in a Playbook policy. This action however, is not selected by default in the Playbook policy. Therefore, you must go to the Playbook policy and select it in order for it to be triggered when a security event is triggered.

Field	Definition
Name	Enter any name for this action.
Description	Enter a description of this action.
Upload	Upload a Python script that calls an API from the third-party system in order to perform the relevant action. Python 2.7 or later is supported. This Python script must be created according to the coding conventions that can be displayed by clicking the icon next to the *Action Scripts* field. The following displays providing an explanation of these coding conventions and provides various links that you can click to see more detail and/or to download sample files.

Field	Definition
	 Creating a Custom Incident Response Action The following describes how to create and upload your own Python script to be assigned to an incident response action. Playbook policies that are configured to use this action will automatically execute this script when a security event is triggered. Code Conventions - A FortiEDR Jumpbox on which one or more scripts are executed is deployed with various standard Python packages. › A list of the packages that are deployed with this type of FortiEDR Jumpbox. - At the moment, only Python 2 is supported. - Parameters ∘ Integration scripts can use properties that are part of a Connector's configuration, such as API keys or information that is part of the triggering event (such as the process name). ∘ These properties are stored in the config.json file and can be used as script parameters. ∘ Click here to see a sample config.json file and a sample action script: custom_script.py config.json Troubleshooting Script execution (either in test mode or as part of a realtime incident response) is defined as successful if the script exits with code 0. Any other exit code will be reported as a failure. Each script can also be manually invoked using the Test button. A test execution will get the sample parameter file (which is available for download above) with an added JSON section – "TestMode": true. The stderr and stdout Script output will be available after the test completes or when script execution fails (with an error icon next to the action name).

3. Click *Save*.

To modify the script of an action:

1. In the *Administration* tab, select *Connectors*.
2. Click the *Action Manager* button.
3. Select the action of the script to be modified.
4. In the *Action Scripts* area, hover over the name of the script in order to display various tools, as follows:

Tool	Description
⤓	To download the action's current script. For example, so that you can edit it.
🗑	To delete the action's selected script.

Tool	Description
☁	To upload a new Python script that calls an API from the third-party system in order to perform the relevant action. Python 2.7 or later is supported.

5. Click *Save*.

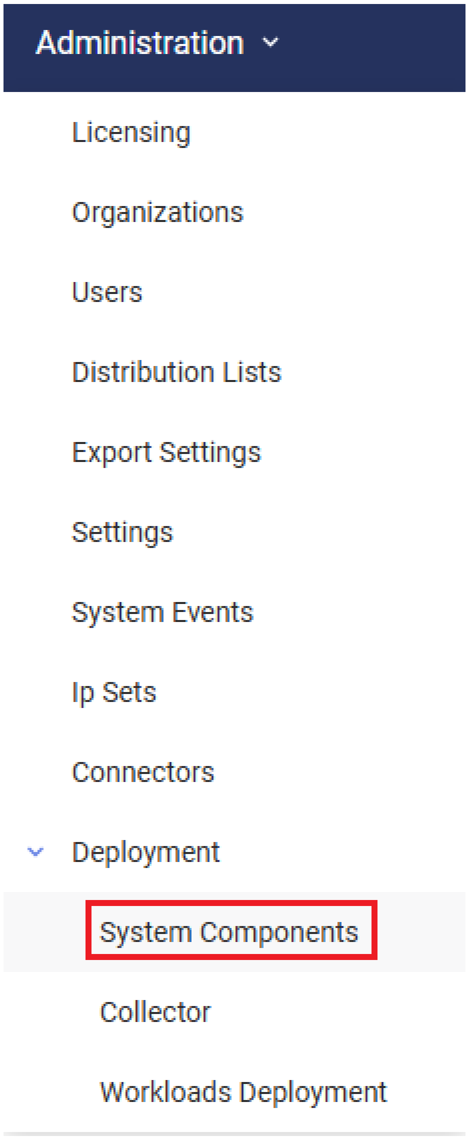
Deployment

The *Administration* > *Deployment* menu includes the following pages:

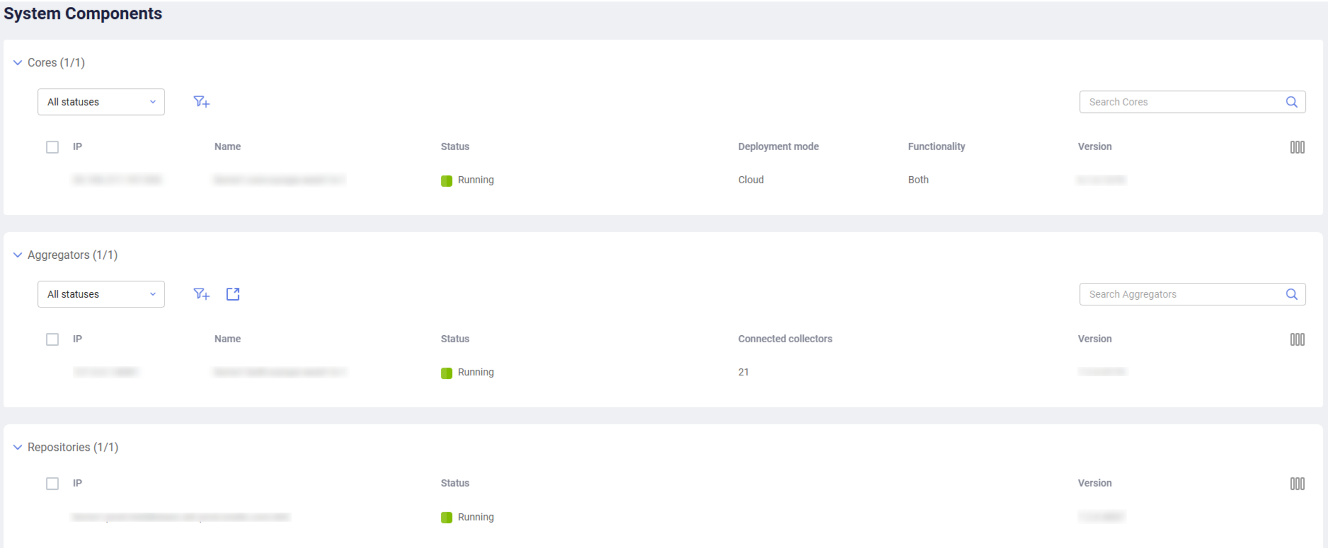
- System Components on page 400
- Collector on page 405

System Components

The *Administration* > *Deployment* > *System Components* page lists the FortiEDR Aggregators, Cores and Repositories.



The following displays:



System Components

Cores (1/1)

All statuses

Search Cores

□	IP	Name	Status	Deployment mode	Functionality	Version
	[redacted]	[redacted]	🟩 Running	Cloud	Both	[redacted]

Aggregators (1/1)

All statuses

Search Aggregators

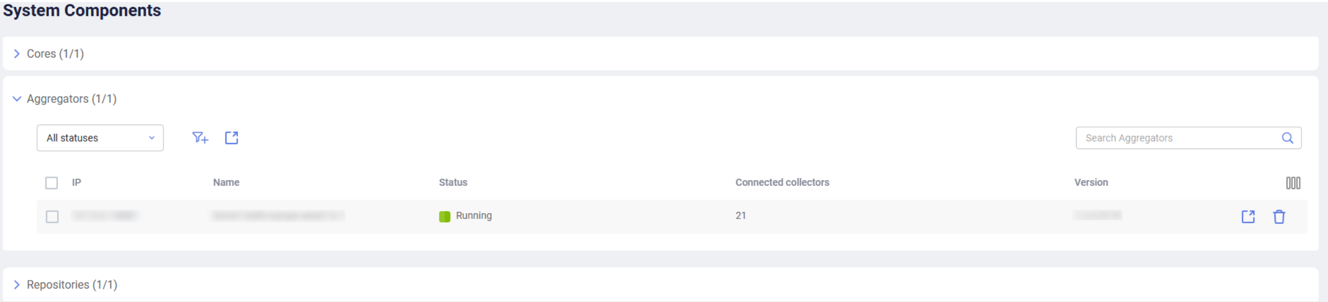
□	IP	Name	Status	Connected collectors	Version
	[redacted]	[redacted]	🟩 Running	21	[redacted]

Repositories (1/1)

□	IP	Status	Version
	[redacted]	🟩 Running	[redacted]

Aggregators

The *AGGREGATORS* area lists the FortiEDR Aggregators.



System Components

Cores (1/1)

Aggregators (1/1)

All statuses

Search Aggregators

□	IP	Name	Status	Connected collectors	Version
□	[redacted]	[redacted]	🟩 Running	21	[redacted]

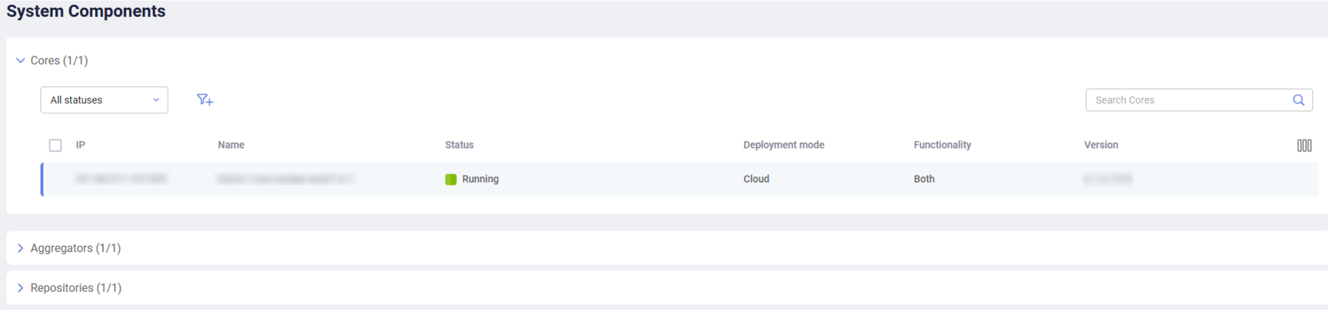
Repositories (1/1)

Click the *Expand* icon (›) to expand the list. The following information is provided for each FortiEDR Aggregator:

Information Field	Description
Checkbox	Check this checkbox to select the Aggregator. You can then use one of the buttons at the top left of the window, such as the *Delete* button.
IP	Specifies the IP address of the communicating device on which the FortiEDR Aggregator is installed.
Name	Specifies the Aggregator name entered during installation.
Connected Collectors	Specifies the number of FortiEDR Collectors that have been configured to operate with this Aggregator.
Version	Specifies the version of the Aggregator software.
State	Specifies the current state of the FortiEDR Aggregator.

Cores

The *CORES* area lists the FortiEDR Cores.



System Components

Cores (1/1)

All statuses

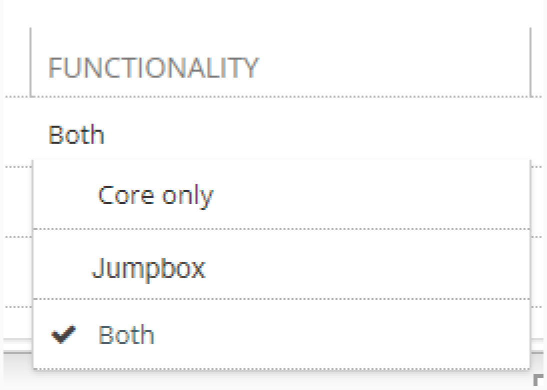
Search Cores

□	IP	Name	Status	Deployment mode	Functionality	Version
□	[redacted]	[redacted]	🟩 Running	Cloud	Both	[redacted]

Aggregators (1/1)

Repositories (1/1)

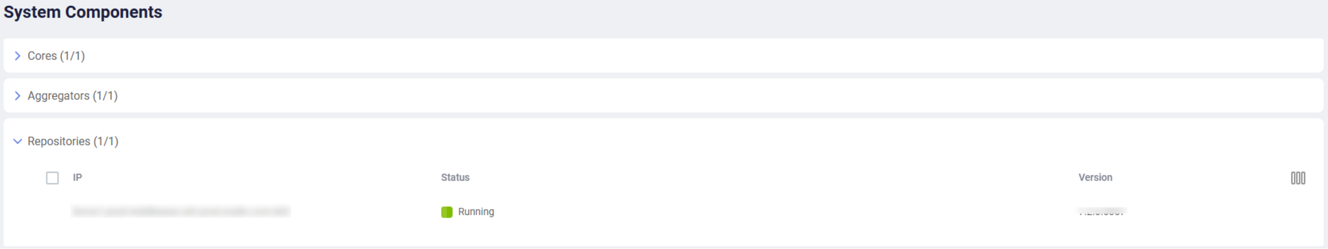
Click the *Expand* icon (>) to expand the list. The following information is provided for each FortiEDR Core:

Information Field	Description
Checkbox	Check this checkbox to select the Core. You can then use one of the buttons at the top left of the window, such as the *Delete* button.
Organization	Specifies the name of the organization in a multi-organization FortiEDR environment. In a single-organization FortiEDR system, this column does not appear.
IP	Specifies the IP address of the communicating device on which the FortiEDR Core is installed.
Name	Specifies the FortiEDR Core name entered during installation.
Deployment Mode	Specifies whether the FortiEDR Core is physically deployed on your organization's premises (On-Premise) or in the cloud provided by Fortinet (Cloud). The following deployment options are available: • Cloud • On-premise
Functionality	Specifies the core's functionality and enables you to modify it by selecting one of the following options:  • *Core only* – Specifies that the system provides basic FortiEDR Core

Information Field	Description
	functionality: events processing, communication control handling, activity events proxy to the Repository and so on. • *Jumpbox* – Specifies that the FortiEDR Core is used by the Central Manager (the central web user interface) as a Jumpbox, while the Jumpbox connects to the LDAP, sandbox or to the products. No basic Core functionalities are provided. The *Jumpbox* option is unavailable for cloud Cores. To configure a cloud Core to function as Jumpbox, please contact Fortinet Support. • *Both* – Provides both *Core* and *Jumpbox* functionality, as described above. It is not mandatory to have a Core with Jumpbox functionality. However, removing Jumpbox functionality (by selecting the Core only option) may affect previously defined connectors, thus causing them to be nonfunctional. In this case, an appropriate message is displayed.
Version	Specifies the version of the FortiEDR Core.
State	Specifies the current state of the FortiEDR Core.

Repositories

The *REPOSITORIES* area shows details about the FortiEDR Threat Hunting Repository server.



System Components

› Cores (1/1)

› Aggregators (1/1)

⌄ Repositories (1/1)

□ IP	Status	Version
[redacted]	🟩 Running	[redacted]

Click the *Expand* icon (›) to expand the list. The following information is provided for each FortiEDR Repository:

- *IP*: Specifies the IP and port address of the communicating device on which the FortiEDR Repository is installed.
- *STATE*: Specifies the current state of the FortiEDR Repository.

Collector

Perform the following tasks on the *Administration* > *Deployment* > *Collector* page:

- Updating the Collector version on page 405
- Loading a server certificate on page 408
- Requesting and obtaining a Collector installer on page 409
- Requesting and obtaining a mobile installer on page 412

Updating the Collector version

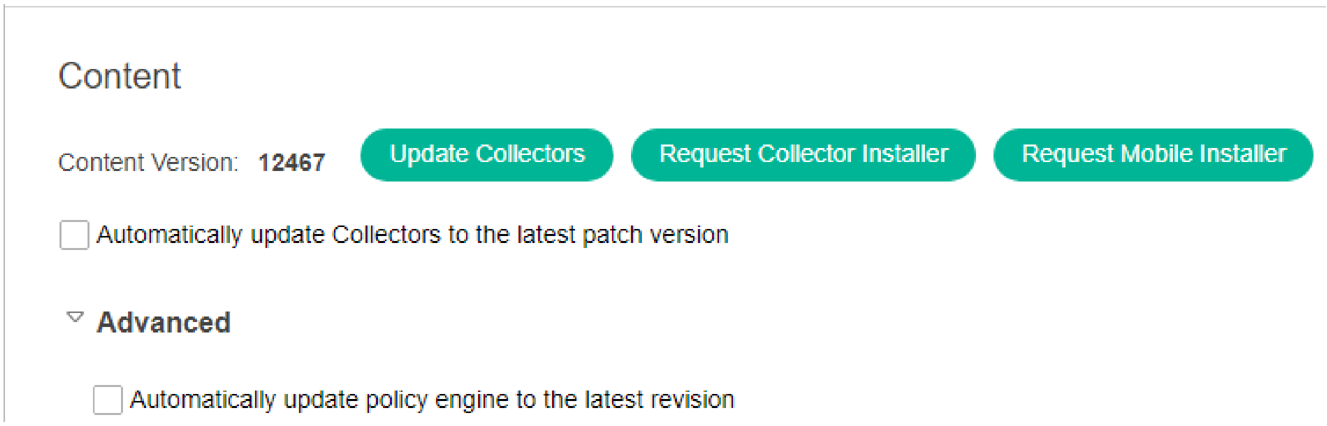
Use the Update Collector Version feature to update a FortiEDR Collector version, such as from 5.0.3 to 5.2.

This feature does not support upgrading a macOS Collector from 5.2 to 6.0, which can only be done via JAMF. See Installing FortiEDR on MacOS devices using Jamf PRO on page 58. Upgrading macOS Collector 6.0 to a later build using this option will work.

The Automatic Collector Updates feature updates the patch and revision for a given FortiEDR version upon the availability of a new Collector build. The patch and revision numbers are the third and fourth digits of the FortiEDR version number. For example, for FortiEDR version 3.1.*y*.*x*, *y* indicates the patch number and *x* indicates the revision number.

When the *Automatically update Collectors to the latest patch revision* checkbox is checked, whenever the content contains a new build (for example, 5.0.3.508 is a new build of 5.0.2.342), all Collectors are updated to that build. This means that all Collectors in all Collector Groups in all environments and operating systems are updated to the latest FortiEDR revision available (as provided by Fortinet using the Load Content feature). For more details about the Load Content feature, see Content Updates on page 477

In the *Advanced* section you can choose to disallow automatic updates of the Collector’s policy logic library. When the checkbox is checked, the engine library is updated on the Collector whenever new engine becomes generally available. Automatic Policy engine library update keeps the core detection functionality within the Collector up to date and as it does not enforce any downtime or restart of the device is recommended.



Content

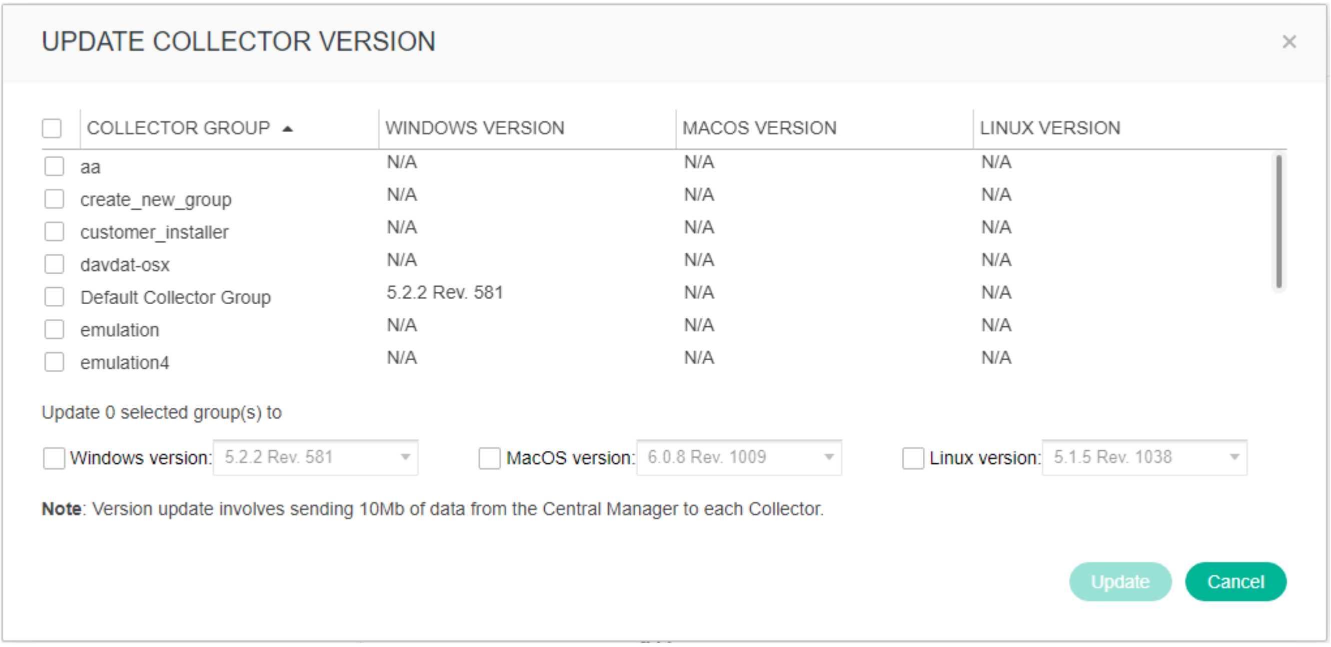
Content Version: 12467

□ Automatically update Collectors to the latest patch version

Advanced

□ Automatically update policy engine to the latest revision

When you click the *Update Collectors* button in the Licensing window, the *Update Collector Version* window displays. This window lists all available Collector Groups. The *Windows Version*, *macOS Version*, and *Linux Version* columns indicate the current FortiEDR version for the Collectors in a Collector Group.



UPDATE COLLECTOR VERSION

□ COLLECTOR GROUP ▲	WINDOWS VERSION	MACOS VERSION	LINUX VERSION
□ aa	N/A	N/A	N/A
□ create_new_group	N/A	N/A	N/A
□ customer_installer	N/A	N/A	N/A
□ davdat-osx	N/A	N/A	N/A
□ Default Collector Group	5.2.2 Rev. 581	N/A	N/A
□ emulation	N/A	N/A	N/A
□ emulation4	N/A	N/A	N/A

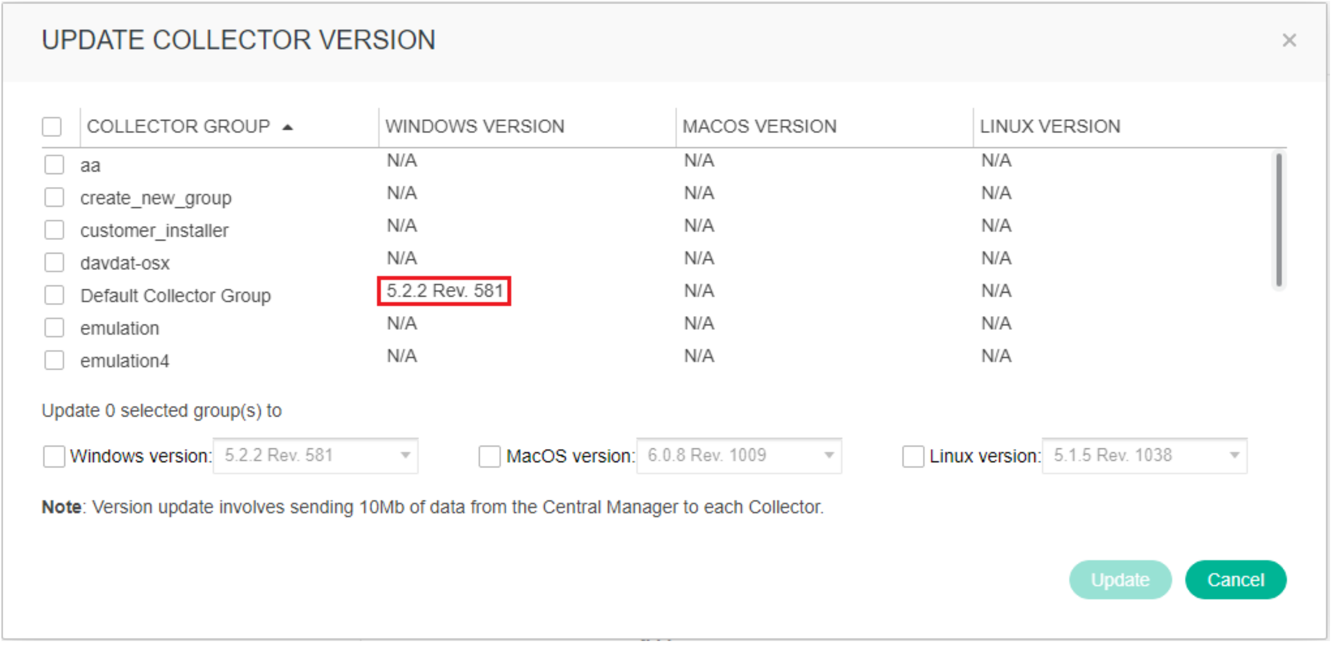
Update 0 selected group(s) to

□ Windows version: 5.2.2 Rev. 581 □ MacOS version: 6.0.8 Rev. 1009 □ Linux version: 5.1.5 Rev. 1038

Note: Version update involves sending 10Mb of data from the Central Manager to each Collector.

You can update the version for the Collectors in a Collector Group for each operating system.

If the *Automatically update Collectors to the latest patch version* checkbox is enabled on the *Administration > Deployment > Collector* page, then the *Update Collector Version* window does not display the revision number in the Windows Version, macOS Version and Linux Version columns, as the revision is automatically updated with the Automatic Updates feature.



UPDATE COLLECTOR VERSION

□ COLLECTOR GROUP ▲	WINDOWS VERSION	MACOS VERSION	LINUX VERSION
□ aa	N/A	N/A	N/A
□ create_new_group	N/A	N/A	N/A
□ customer_installer	N/A	N/A	N/A
□ davdat-osx	N/A	N/A	N/A
□ Default Collector Group	5.2.2 Rev. 581	N/A	N/A
□ emulation	N/A	N/A	N/A
□ emulation4	N/A	N/A	N/A

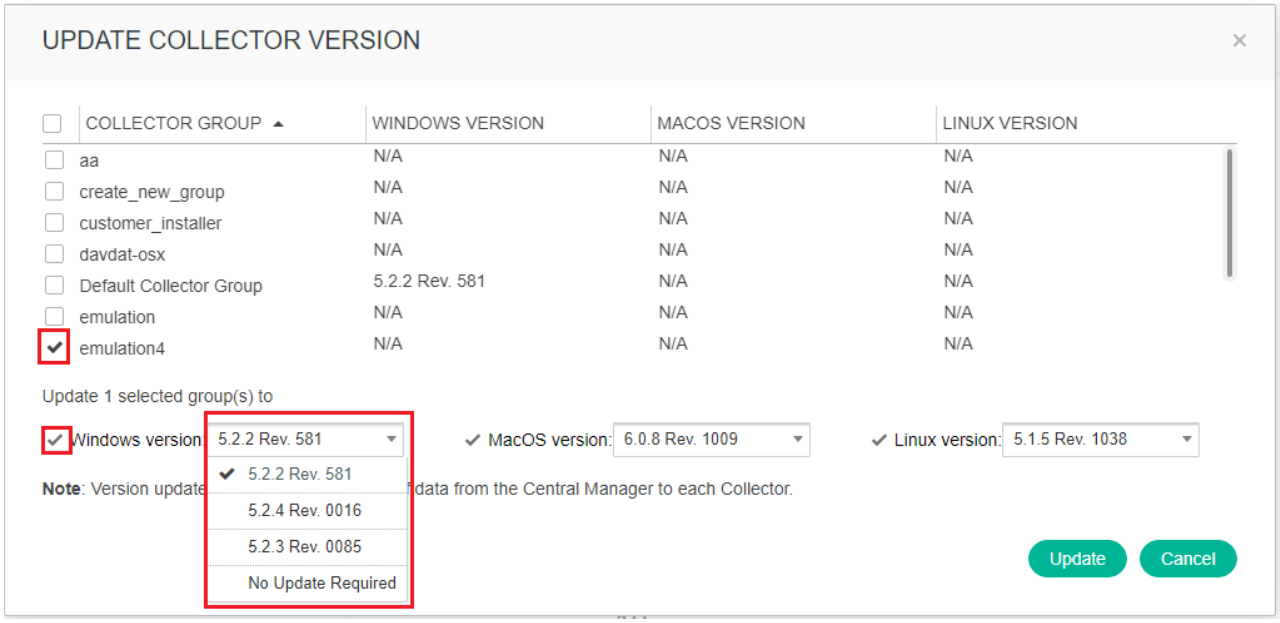
Update 0 selected group(s) to

□ Windows version: 5.2.2 Rev. 581 □ MacOS version: 6.0.8 Rev. 1009 □ Linux version: 5.1.5 Rev. 1038

Note: Version update involves sending 10Mb of data from the Central Manager to each Collector.

To update the version for the Collectors in a Collector Group:

1. Check the checkbox of the Collector Group(s) whose Collectors you want to update. You can select more than one Collector Group.
2. Select the checkbox of the operating system(s) to update and in its adjacent dropdown list, select the FortiEDR version for the Collectors in the designated Collector Group. You can select more than one operating system.



UPDATE COLLECTOR VERSION

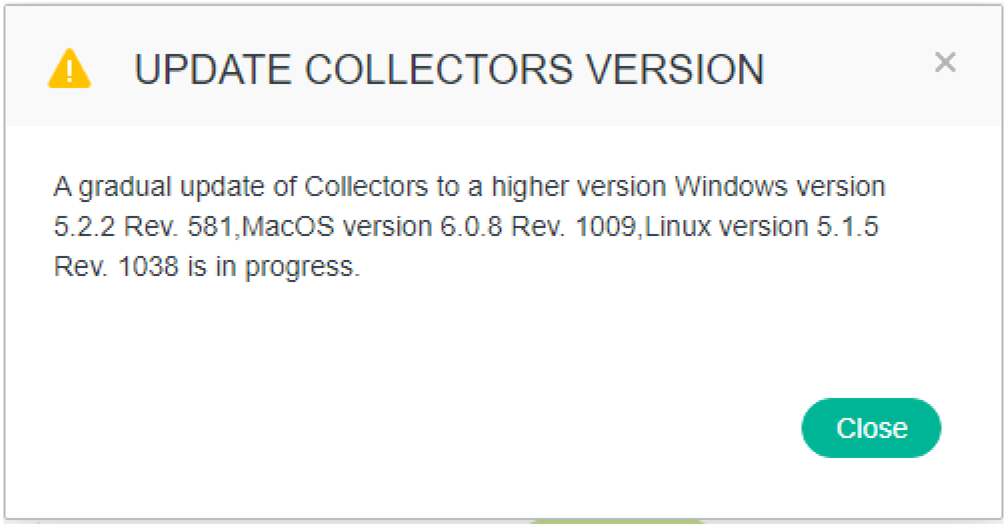
□	COLLECTOR GROUP ▲	WINDOWS VERSION	MACOS VERSION	LINUX VERSION
□	aa	N/A	N/A	N/A
□	create_new_group	N/A	N/A	N/A
□	customer_installer	N/A	N/A	N/A
□	davdat-osx	N/A	N/A	N/A
□	Default Collector Group	5.2.2 Rev. 581	N/A	N/A
□	emulation	N/A	N/A	N/A
☑	emulation4	N/A	N/A	N/A

Update 1 selected group(s) to

☑ Windows version: 5.2.2 Rev. 581 ✓ MacOS version: 6.0.8 Rev. 1009 ✓ Linux version: 5.1.5 Rev. 1038

Note: Version update data from the Central Manager to each Collector.

3. Click *Update*. FortiEDR gradually updates all the Collectors in the Collector Group(s) to the required version for the specified operating system(s), and displays the following window:



UPDATE COLLECTORS VERSION

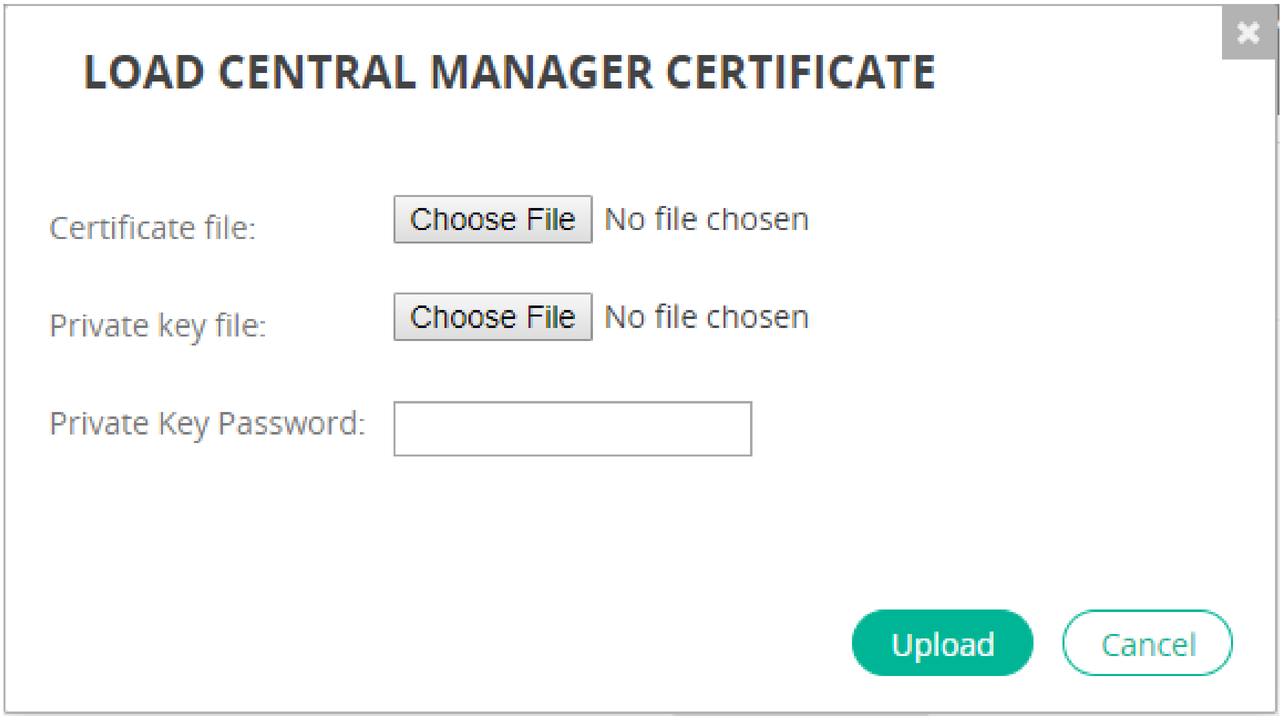
A gradual update of Collectors to a higher version Windows version 5.2.2 Rev. 581,MacOS version 6.0.8 Rev. 1009,Linux version 5.1.5 Rev. 1038 is in progress.

4. Click *Close*.

Loading a server certificate

To load a certificate:

1. Click *Central Manager Certificate* (Central Manager Certificate). The *Load Central Manager Certificate* dialog opens.



LOAD CENTRAL MANAGER CERTIFICATE

Certificate file: Choose File No file chosen

Private key file: Choose File No file chosen

Private Key Password:

2. Click *Choose File* to upload the certificate file. Only PEM certificates (`.pem`) are supported.

> The certificate common name (CN) must match the FQDN of the FortiEDR machine. Otherwise, an error will occur.

3. Click *Choose File* to upload the private key file.
4. Enter the certificate password in the *Private Key Password* field.
5. Click *Upload*.
6. Configure the certificate as follows:
   - For cloud deployment, please contact Fortinet Support.
   - For on-premise deployment, add or edit the following entries in the `/opt/FortiEDR/webapp/application-customer.properties` file on the FortiEDR Manager VM:
     - `connector.ssl.externalAddress={`*`certificate domain/DNS name of machine`*`}`
     - `smtp.template.server.login={`*`certificate domain/DNS name of machine`*`}`

   > The properties are case-sensitive and must be in lowercase. Space is not allowed.

7. Restart the FortiEDR Manager VM.

Requesting and obtaining a Collector installer

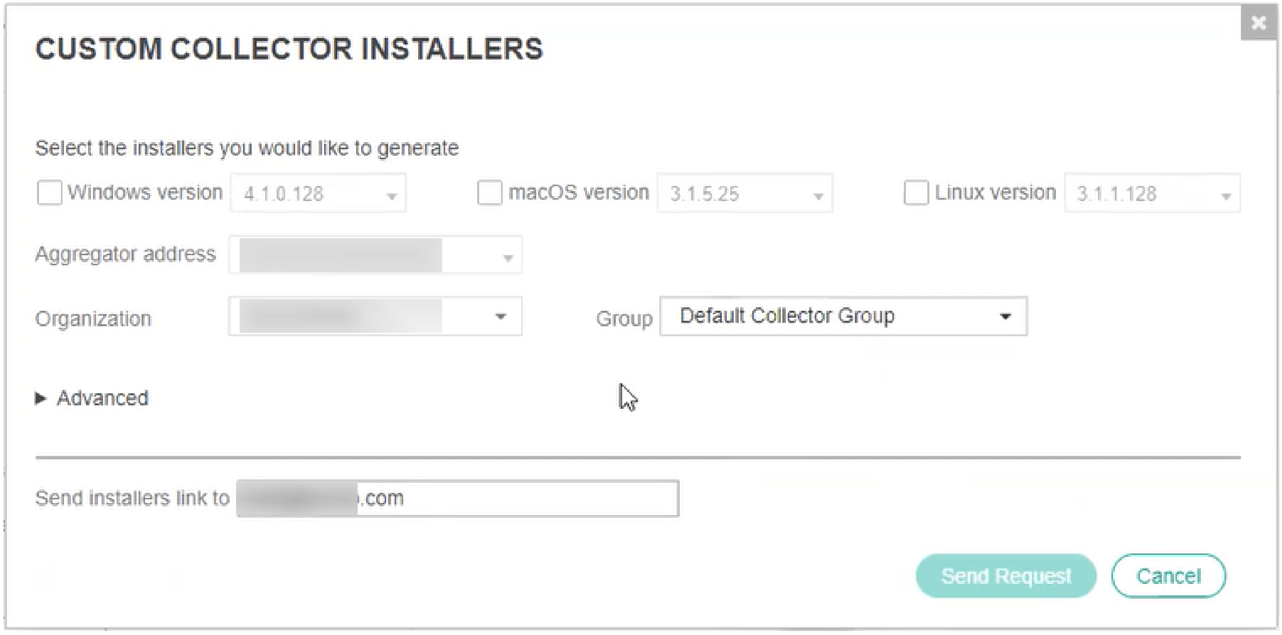
You can click the *Request Collector Installer* button (Request Collector Installer) to obtain a Collector installer file that can be used to install a Collector. This option enables you to request an installer for a particular operating system(s), such as Windows, MacOS, or Linux. This installer is similar to the standard wizard used to install a Collector, except that many of the fields in the wizard have already been filled in for you.

The requested Collector installer will then emailed to you. You can unzip it with 7-Zip using the registration password (available under *Administration* > *Settings* > *Component Authentication on page 316*) and install it by following the instructions in Installing FortiEDR Collectors on page 23, based on the operating system on which it is to be installed.

To minimize the risk of extraction failures and compatibility issues, we recommend using 7-Zip to extract the contents of the MSI package to ensure that all necessary files within the collector package are properly retrieved for further use or configuration. Using WinRAR or the Windows built-in extractor may cause errors or incomplete extractions.

To configure custom installer settings to determine the type of installer to request :

1. On the *Administration* > *Deployment* > *Collector* page, click the *Request Collector Installer* button (Request Collector Installer). The following displays:



CUSTOM COLLECTOR INSTALLERS

Select the installers you would like to generate

□ Windows version 4.1.0.128 □ macOS version 3.1.5.25 □ Linux version 3.1.1.128

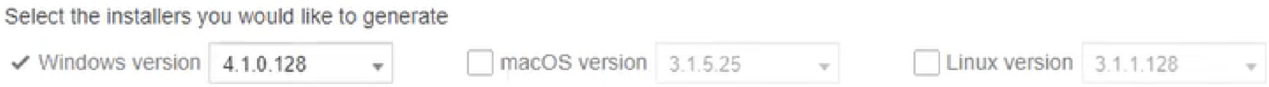
Aggregator address [redacted]

Organization [redacted] Group Default Collector Group

▸ Advanced

Send installers link to [redacted].com

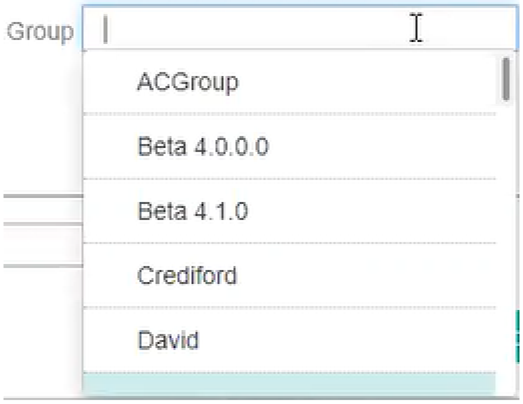
2. In the *Select the installer you would like to generate* area, select the checkbox of the installer(s) you want to request. Multiple installers can be requested at the same time.



Select the installers you would like to generate

✓ Windows version 4.1.0.128 ▾ □ macOS version 3.1.5.25 ▾ □ Linux version 3.1.1.128 ▾

3. In the adjacent dropdown list, select the installer version. When selecting installers for more than one operating system, you must specify the version for each of them. Specify the version in the same manner as described on Updating the Collector version on page 405
4. In the *Aggregator Address* dropdown list, select the aggregator to which this Collector is registered.
5. In a multi-tenant system, select the organization to which the installed Collector is registered in the *Organization* dropdown list.
6. In the *Group* dropdown list, select the Collector Group to which the installed Collector is assigned, or leave the field empty for the Collector to be assigned to the default Collector Group.



Group

ACGroup

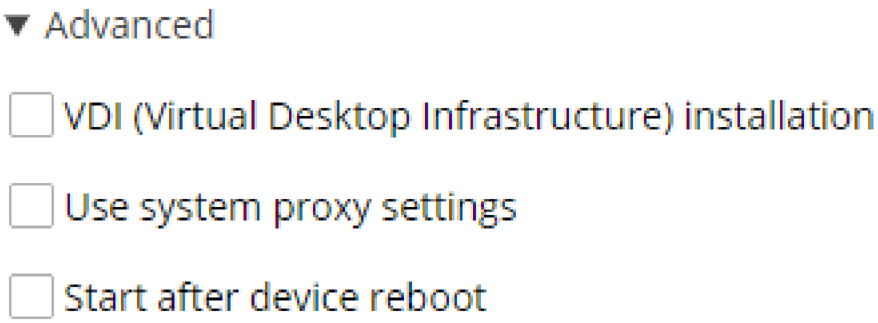
Beta 4.0.0.0

Beta 4.1.0

Crediford

David

7. In the *Advanced* area, specify the following:



▼ Advanced

□ VDI (Virtual Desktop Infrastructure) installation

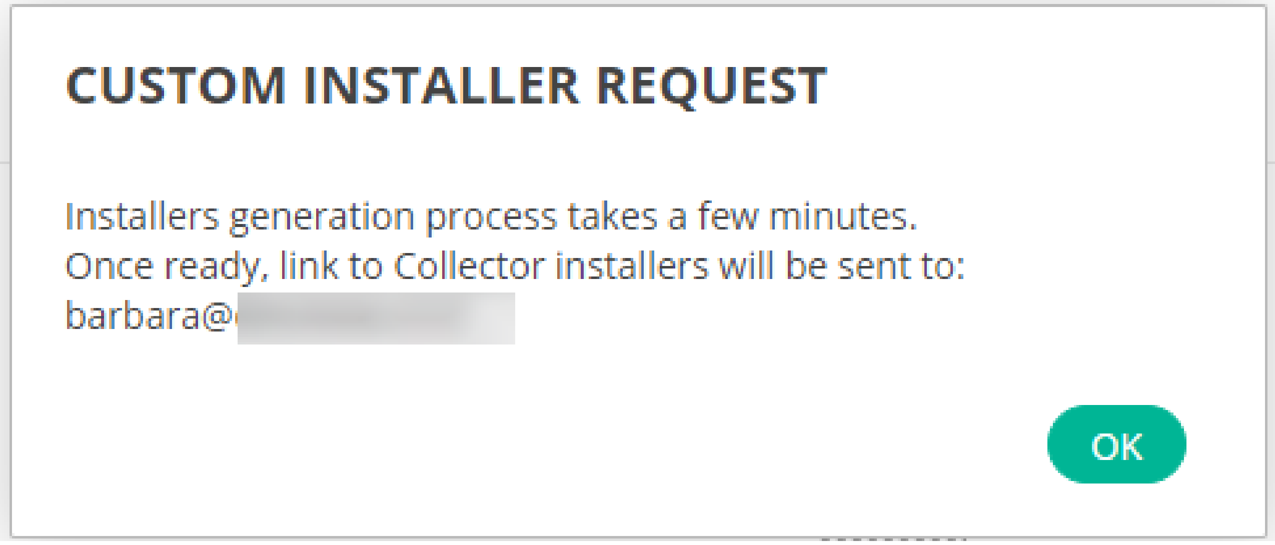
□ Use system proxy settings

□ Start after device reboot

- *VDI (Virtual Desktop Infrastructure) Installation*: If you are installing the Collector on a VDI environment, check this checkbox. For more details, you may refer to the Working with FortiEDR on VDI Environments section on page 54.
- *Use System Proxy Settings*: If you use a web proxy to filter requests in this device's network, then check the *Use System Proxy Settings* checkbox. Note that Windows must be configured to use a proxy and tunneling must be allowed from the Collector to the Aggregator on port 8081 and from the Collector to the Core on port 555. (Run as Administrator: netsh winhttp set proxy <proxy IP >).
- *Start After Device Reboot*: Check this checkbox in order to delay data collection until a device reboot is applied. This is only required in rare cases. Typically, this checkbox remains unchecked.

8. In the *Send Installers Link To* field, specify the email address to which the installer is to be sent.

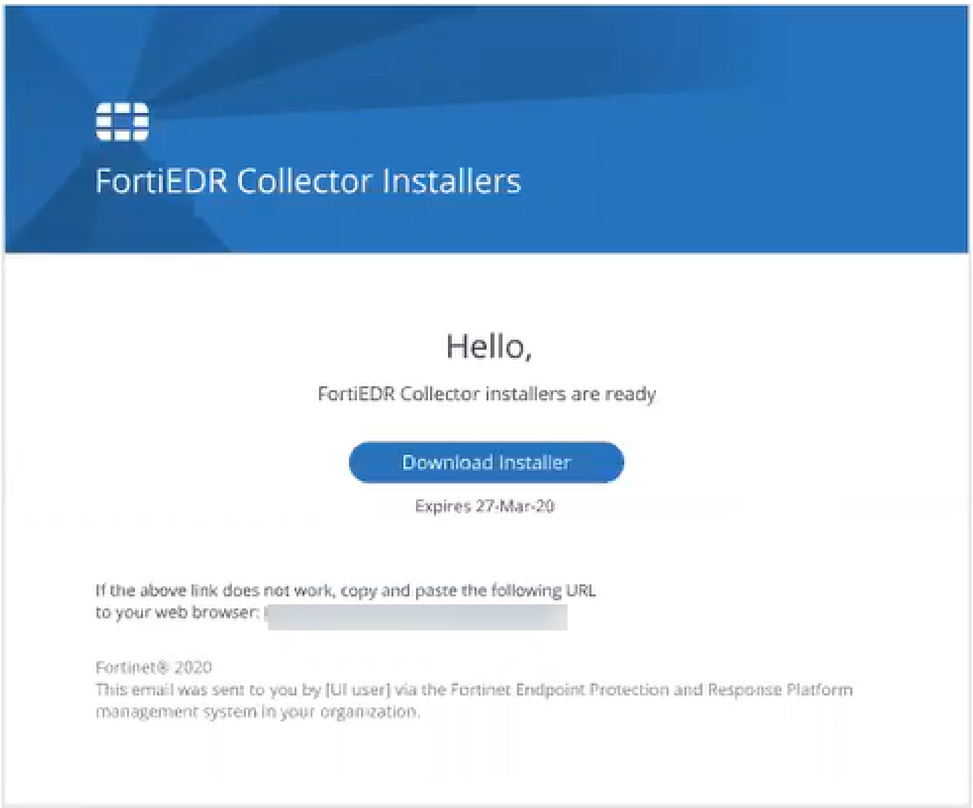
9. Click the *Send Request* (Send Request) button. A confirmation message displays.



CUSTOM INSTALLER REQUEST

Installers generation process takes a few minutes.
Once ready, link to Collector installers will be sent to:
barbara@[redacted]

10. Click *OK*. After the installer is generated by FortiEDR, it is emailed to the specified email address. Note that the link to download installers is only available for several hours. Be sure to download the installers within the required time period so that the link does not expire.



FortiEDR Collector Installers

Hello,

FortiEDR Collector installers are ready

Expires 27-Mar-20

If the above link does not work, copy and paste the following URL to your web browser: [redacted]

Fortinet® 2020
This email was sent to you by [UI user] via the Fortinet Endpoint Protection and Response Platform management system in your organization.

Note that in the presence of an email filtering system and/or a mail transfer agent that modifies the URL content, the installer download URL might include space(s) or %20s in it, that are added by the system/agent. In these cases, browsing directly to the URL will fail with a *signature* error message from the installer storage. In such cases, the URL should be amended to drop the redundant space/%20 before it can be used.

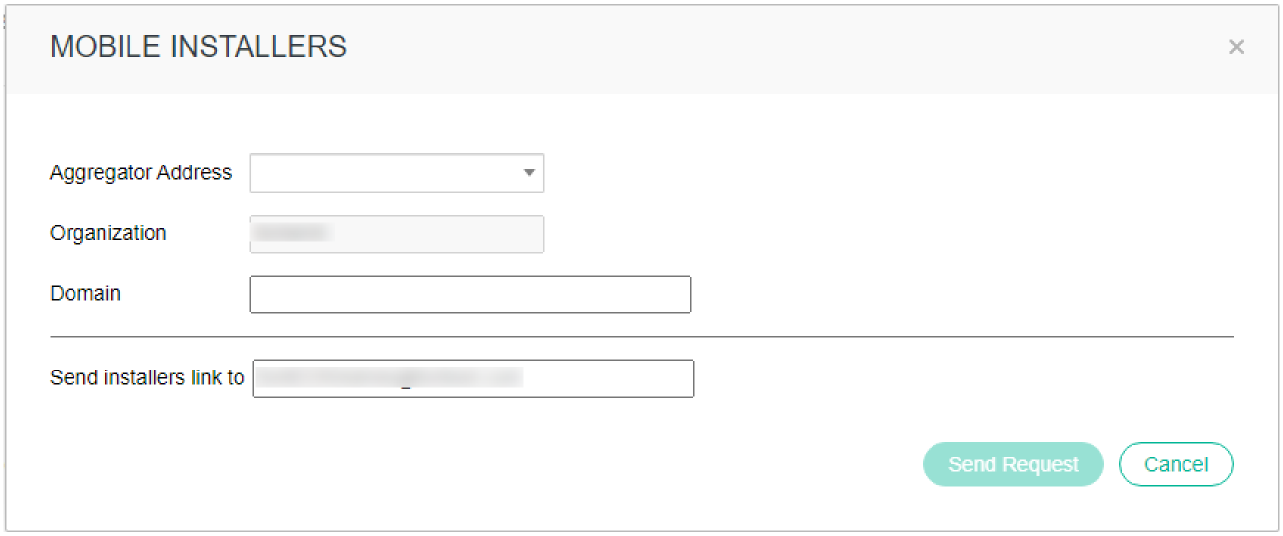
Requesting and obtaining a mobile installer

On the *Administration > Deployment > Collector* page, you can click the *Request Mobile Installer* button (Request Mobile Installer) to obtain a mobile Collector installer file that can be used to install on Android and iOS endpoints. The requested installer is then emailed to you. After you receive the installer file from FortiEDR, simply scan the QR code provided in the email using the mobile endpoint and follow the instructions attached in the email to install the mobile Collector.

The *Request Mobile Installer* option is available only if mobile is enabled in the organization setting. See Step 2 – Defining or importing an organization on page 419.

To request a mobile installer:

1. For multi-tenant systems, verify the correct organization (to which the mobile Collector will be registered) is selected at the top-left corner.
2. On the *Administration > Deployment > Collector* page, click *Request Mobile Installer* (Request Mobile Installer). The following displays:



MOBILE INSTALLERS

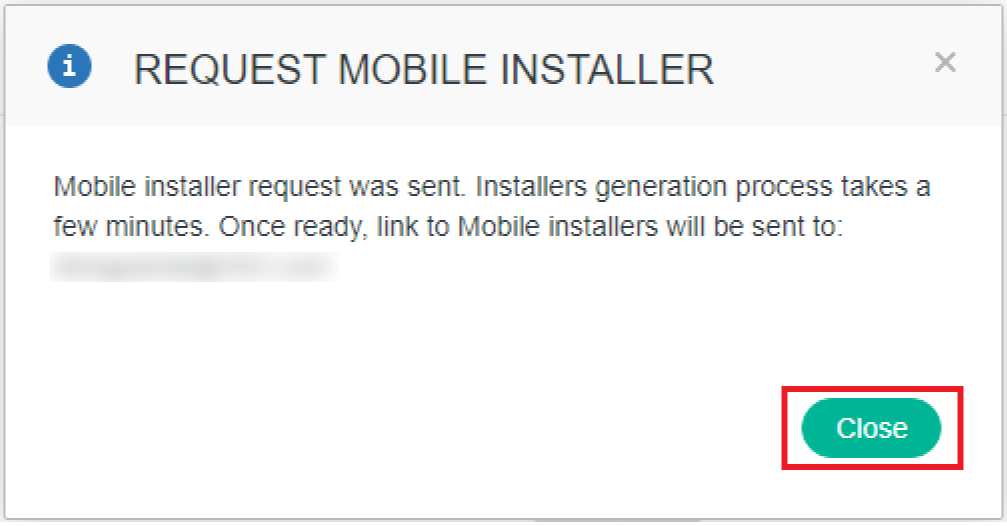
Aggregator Address

Organization [redacted]

Domain

Send installers link to [redacted]

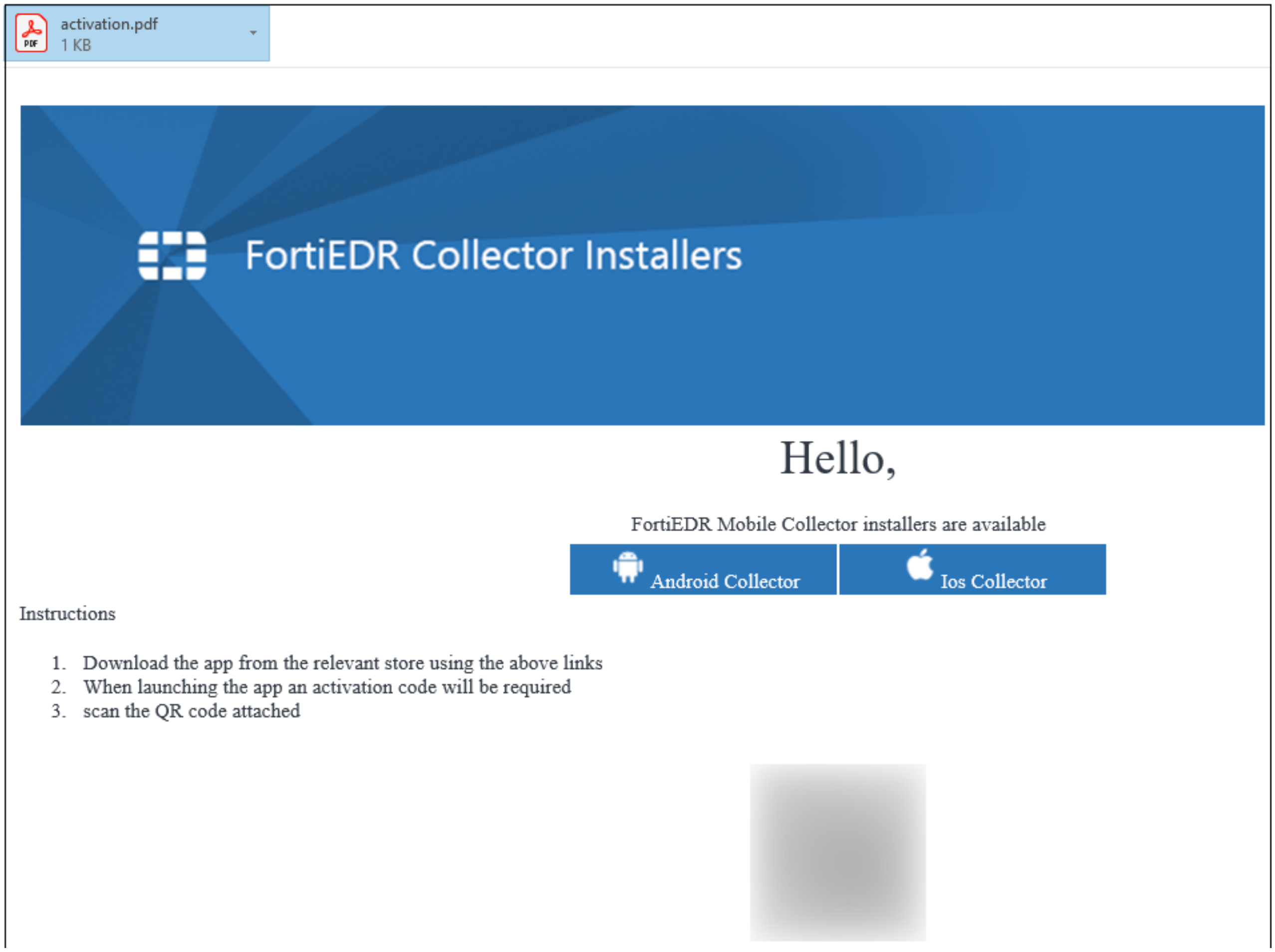
3. In the *Aggregator Address* dropdown list, select the aggregator to which this Collector is registered.
4. Confirm the organization for the Collector to register with, if applicable.
   To change the organization, you must exit the window and change it at the top-left corner of the Central Manager console.
5. Specify the domain, which will be used for validation during account activation (see the FortiEDR Android and iOS User Guide).
   For example, if the domain is set to `fortinet.com`, the user must specify a valid username with a matching Fortinet email address. Account activation will fail if the username fails the domain validation.
6. Specify the email of the recipient of the mobile Collector.
7. Click *Send Request*. The Android and iOS collector installers and instructions will be sent via email.
8. Click *Close* in the *REQUEST MOBILE INSTALLER* window.



REQUEST MOBILE INSTALLER

Mobile installer request was sent. Installers generation process takes a few minutes. Once ready, link to Mobile installers will be sent to: [redacted]

9. In the *Send Installers Link To* field, specify the email address to which the installer is to be sent.
10. Verify that the mobile Collector installers have been received in the specified email.
11. Follow the instructions to install the mobile Collector on desired Android or iOS devices.



FortiEDR Collector Installers

Hello,

FortiEDR Mobile Collector installers are available

Instructions

1. Download the app from the relevant store using the above links
2. When launching the app an activation code will be required
3. scan the QR code attached

12. After the mobile Collector is installed, activate it using the registration code attached in the email.

(Android only) After activation, the Collector automatically scans all files (including APKs) and applications on the mobile device for potential vulnerabilities. You can also trigger a scan anytime or schedule periodic scanning based on your needs (see File Scan on page 319). When a malicious application or file is detected, executed, or installed, the Collector sends a notification and prevents the execution or installation based on the policy setting. You can then view the details of the activity in the Incidents menu of the FortiEDR Central Manager console.

Multi-tenancy (organizations)

This chapter describes the operations that can be performed by an Administrator in a FortiEDR multi-organization system.

This chapter is only relevant for administrators in a multi-organization system. If you do not have Administrator rights, there is no need to read this chapter.

What is a multi-organization environment in FortiEDR?

Beginning with 3.0, the FortiEDR system can be set up as a single-organization or multi-organization environment. When set up as a single-organization system, the FortiEDR system and all its operations and infrastructure serve a single tenant, called an ***organization*** in the FortiEDR system, and work as described in all the previous chapters of this guide.

Prior to 3.0, the FortiEDR system only supported a single tenant (organization).

In a multi-organization FortiEDR system, someone with Administrator rights can perform operations and handle data for all organizations in the system. For example, think of a multi-organization environment like a hotel chain, which has a parent company along with hotels in various cities. In this scenario, the ABC Hotel corporate entity represents the *main organization*, and each ABC Hotel branch location represents a separate, discrete organization. For example, ABC Hotel Los Angeles, ABC Hotel New York, ABC Hotel Boston and so on.

FortiEDR uses *organizations* to distinguish between tenants in a multi-tenant environment. Each organization uses the same FortiEDR user interface and shares the same FortiEDR database.

Multi-organization and user roles

FortiEDR uses a series of predefined roles to control access to organizational data, as follows:

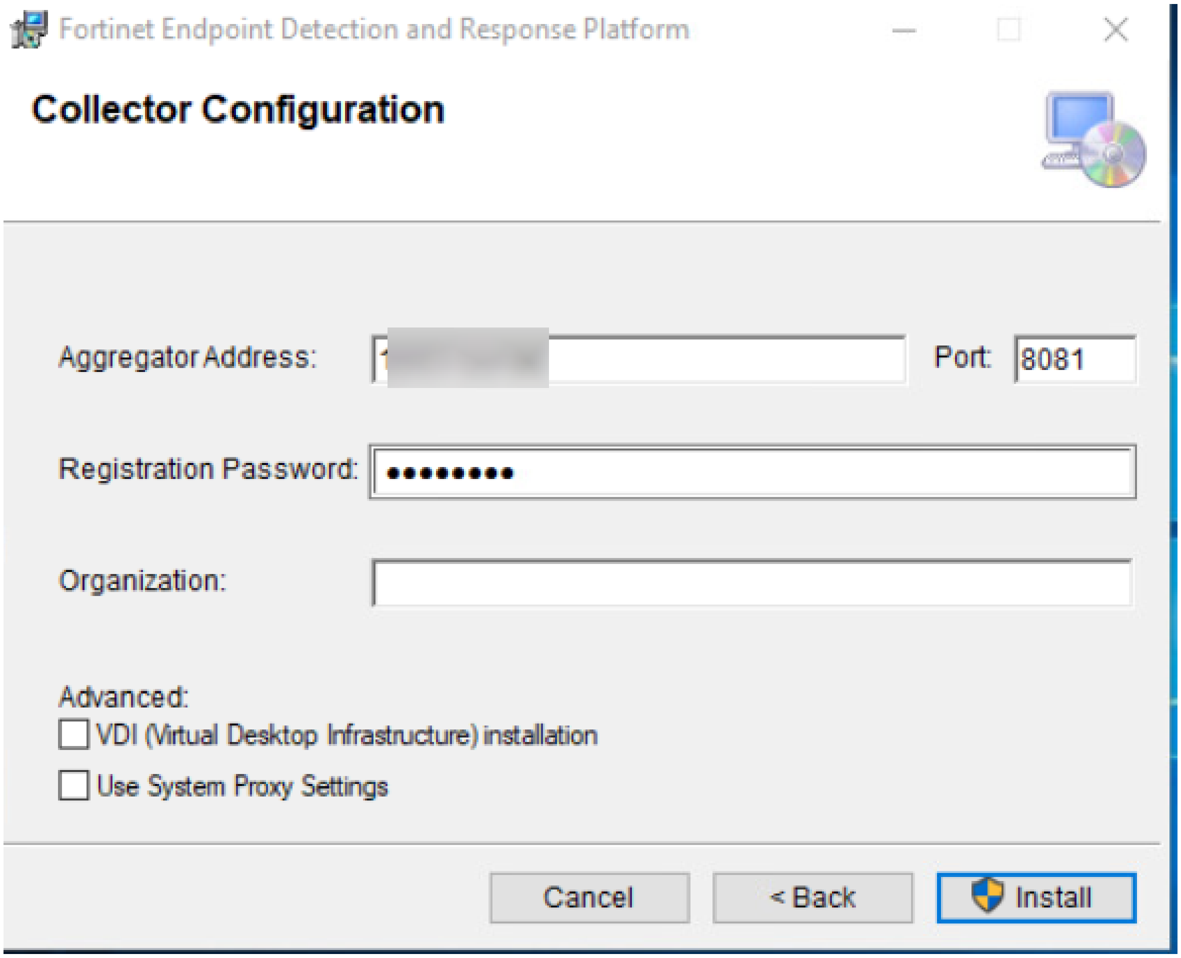
Role	Description
Admin	Highest-level super user that can access all data and perform all operations in the FortiEDR Central Manager console for one specific organization or all organizations, as defined in the user settings.

Role	Description
	In a FortiEDR multi-organization system, the system comes with one predefined Administrator user. More than one user with the Admin role is permitted. There must always be at least one Administrator in the system. Prior to 3.0, the FortiEDR system only supported a single tenant (organization).
Senior Analyst	Analysts supervisor who can define security policies in addition to all the actions that can be performed by an Analyst. Similar to admin users but without administration privileges. A senior analyst can view all information and perform actions, such as marking security events as handled, changing policies and defining exceptions, but cannot access the Administration on page 277 tab.
Analyst	SOC/MDR service analyst who can perform actions as required in the day-to-day activities of handling events. Similar to senior analyst users but without access to security configuration. An analyst can view all information and perform actions, such as marking security events as handled, but cannot access the *ADMINISTRATION* tab or define/change policies.
IT	IT staff who can define settings related to the FortiEDR integration with the customer ecosystem. This role has system configuration access only. They can deploy and upgrade system components and perform system integration with external systems using the *ADMINISTRATION* tab but do not have access to any security configuration, alert monitoring, or Forensics options.
Read-Only	Basic role with read-only access to all non-administrative functions.

Component registration in a multi-organization environment

Collector registration

Each organization has its own registration password. The Collector installer specifies the Collector organization name. If the *Organization* field is left empty during installation, the Collector is added to the default Hoster account, as shown below:



Fortinet Endpoint Detection and Response Platform

Collector Configuration

Aggregator Address: [redacted] Port: 8081

Registration Password: ●●●●●●●●●

Organization:

Advanced:

□ VDI (Virtual Desktop Infrastructure) installation

□ Use System Proxy Settings

After registration, the Collector receives the organization ID. You can rename the organization if preferred.

To specify the organization when installing from a command line, run the following command:

```
msiexec…\qn ORG=<organization name> AGG=
```

For more details about Collector installation, see Installing FortiEDR Collectors on page 23.

Core registration

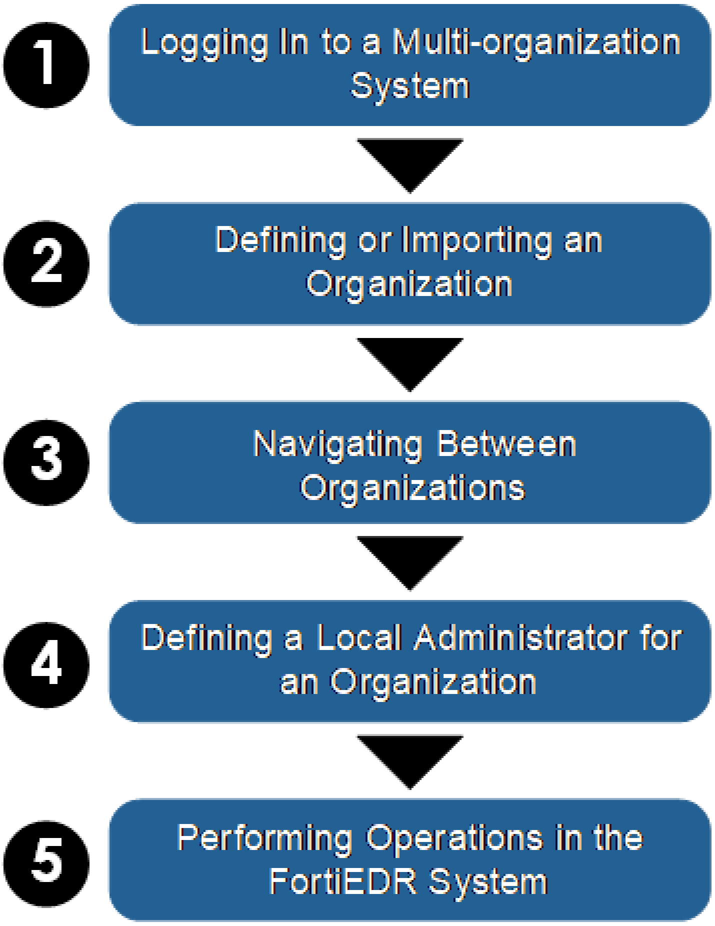
Most Cores are shared between organizations. It is possible to install a Core that belongs only to your organization by installing it on-premises. In this case, you must specify the organization during the Core installation process.

Collectors that do not belong to an organization cannot see that organization's organization-specific Core.

For more details about Core installation, see Setting up the FortiEDR Core on page 511.

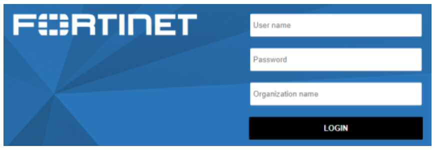
Workflow

The following general workflow applies for Administrators when working in a FortiEDR multi-organization system:


1
Logging In to a Multi-organization System
2
Defining or Importing an Organization
3
Navigating Between Organizations
4
Defining a Local Administrator for an Organization
5
Performing Operations in the FortiEDR System

Step 1 – Logging in to a multi-organization system

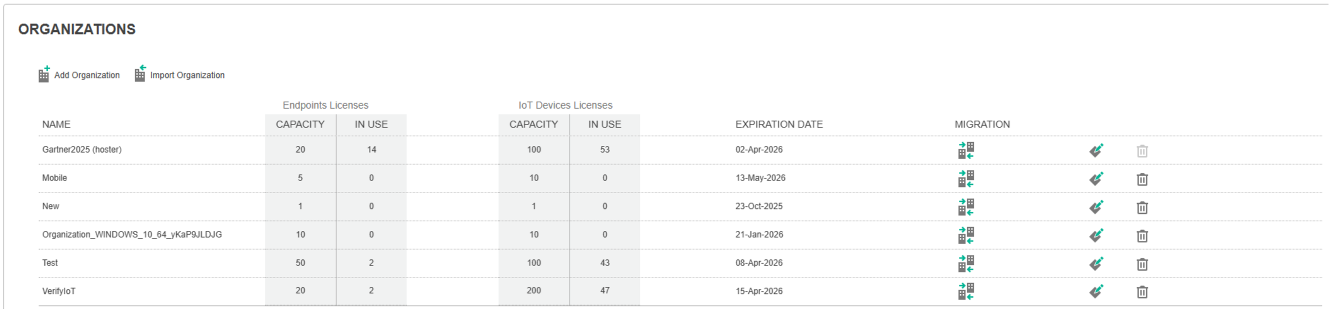
For a FortiEDR multi-organization system, a user must also specify the organization when logging in to the system.



A user must be defined for an organization in order to log in to that organization. When logging in, the user must specify the organization name in the *Organization Name* dropdown list unless he/she is an administrator with privileges to all organizations, in which case he/she is logged in to the main organization by default without the need to specify an organization.

Step 2 – Defining or importing an organization

The *ORGANIZATIONS* page lists all the organizations defined in the FortiEDR system.



ORGANIZATIONS

	Endpoints Licenses		IoT Devices Licenses			
NAME	CAPACITY	IN USE	CAPACITY	IN USE	EXPIRATION DATE	MIGRATION
Gartner2025 (hoster)	20	14	100	53	02-Apr-2026	
Mobile	5	0	10	0	13-May-2026	
New	1	0	1	0	23-Oct-2025	
Organization_WINDOWS_10_64_yKaP9JLDJG	10	0	10	0	21-Jan-2026	
Test	50	2	100	43	08-Apr-2026	
VerifyIoT	20	2	200	47	15-Apr-2026	

The *Default (hoster)* organization is predefined in the system. This organization represents the main organization in the system, such as the ABC Hotel chain described before. The *Default (hoster)* main organization cannot be deleted.

The default organization can be accessed by an Administrator with permissions to the default organization or to all organizations.

In a single-organization system, the Default (hoster) organization is the only organization. To set up a multi-organization system, see Moving from a single-organization to multi-organization structure in FortiEDR on page 423 in FortiEDR.

The *Organizations* window contains the following information:

Field	Definition
Name	Specifies the name of the organization.
Endpoint Licenses Capacity	For the organization, specifies the number of endpoint licenses (which includes workstations and servers) allocated to the organization.
Endpoint Licenses in Use	Specifies the number of endpoint licenses (which includes workstations and servers) in use (installed).
IoT Devices Capacity	For the organization, specifies the maximum number of IoT devices that can be detected in the organization.
IoT Devices in Use	Specifies the number of IoT devices detected in the organization.
Expiration Date	Specifies the expiration date of licenses for the organization.

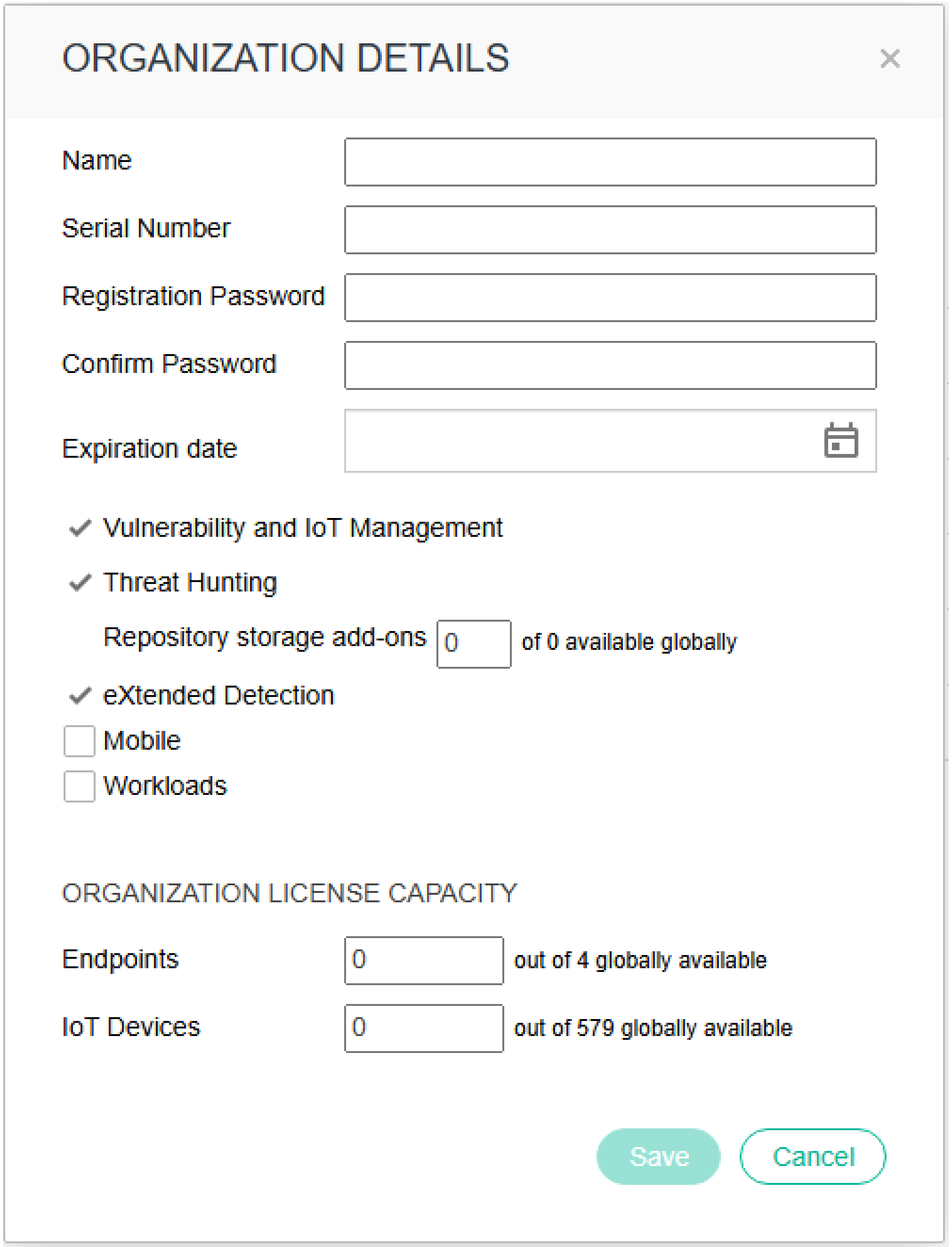
Click the *Edit* button in an organization row to edit the properties of that organization.

You can delete an organization as long as it does not have any workstations or servers in use. Click the *Delete* 🗑 button in an organization row to delete that organization.

Click the *Migrate Organization* ⇄ button in an organization row to migrate that organization. For more details, see Migrating an organization on page 425.

To define an organization:

1. Click the *ADMINISTRATION* tab and then click *ORGANIZATIONS* in the left pane. The *ORGANIZATIONS* page displays.
2. Click the *Add Organization* button. The following window displays:



ORGANIZATION DETAILS

Name	
Serial Number	
Registration Password	
Confirm Password	
Expiration date	

✓ Vulnerability and IoT Management

✓ Threat Hunting

Repository storage add-ons 0 of 0 available globally

✓ eXtended Detection

□ Mobile

□ Workloads

ORGANIZATION LICENSE CAPACITY

Endpoints	0	out of 4 globally available
IoT Devices	0	out of 579 globally available

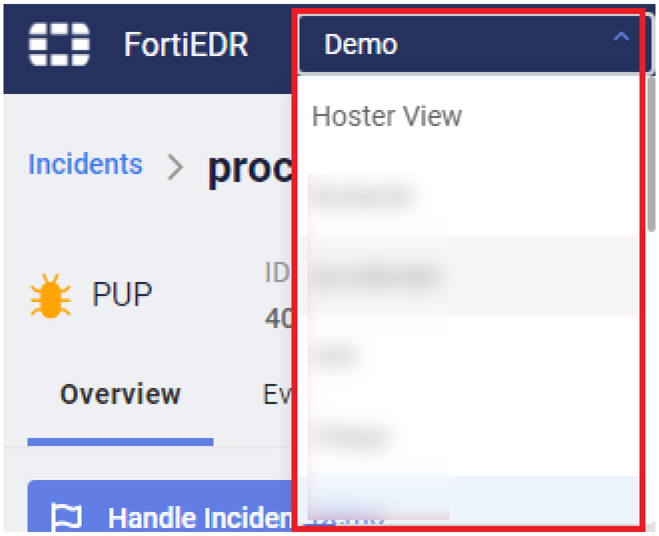
3. Fill in all fields in this window. All fields are mandatory.

Field	Definition
Name	Define the name of the organization. Supported characters in the

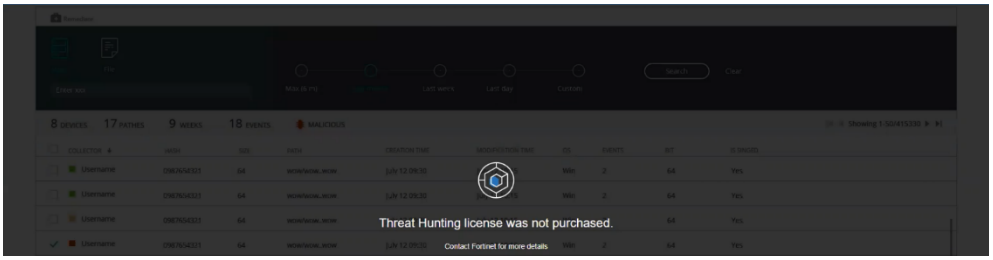
Field	Definition
	organization name: 0123456789:=@ABCDEFGHIJKLMNOPQRSTUVWXYZ_ abcdefghijklmnopqrstuvwxyz. Spaces are also allowed. For example, you can specify the organization name of a hotel branch as `ABC_Hotel@Los Angeles`.
Serial Number	Your FortiEDR unique identifier with Fortinet, which can be found at the top of the *Administration > Licensing* tab.
Registration Password	Specifies the registration password for the organization. Each organization can have a different registration password. You set the value for this password. Supported special characters in the password: !, #, %, &, +, -, ., /, :, <, =, >, ?, @, [, \,], ^, _, `, {, |, }, (,), ~, and , You can display the registration password for an organization by selecting *Administration> Settings> Component Authentication > Display*. If third-party software attempts to stop the FortiEDR Collector service, the system prompts for the registration password. This is the same password used when installing the Collector. If an incorrect password is supplied at the prompt, the message `Access Denied` displays on the Collector device. In this case, the FortiEDR Collector service is not stopped. For more details about the required password to supply in this situation, refer to Component Authentication on page 316.
Expiration Date	Specifies when this license expires. Notifications are sent to you beforehand. Each organization can have its own expiration date. If the Default (hoster) organization expiration date is earlier than that for the organization, then the expiration date for the Default (hoster)organization applies. Whenever there is an expiration date conflict, the earlier date always applies.
Vulnerability and IoT Management	Check this checkbox for the organization to have access to these features. This option is only available on setups that have purchased a Discover and Protect license or Discover, Protect and Response license.

Field	Definition
	The various license types in FortiEDR enable access to different FortiEDR features. The Administrator can configure the various organizations in a multi-tenant environment to each have access to different features in the product. For example, Organization A may have access to the Threat Hunting feature and Organization B may not.
Threat Hunting	Check this checkbox to provide the organization access to threat hunting. This option is only available on setups that have purchased a *Discover, Protect and Response* or *Protect and Response* license. • *Repository storage add-ons*: Specifies the number of repository add ons, out of the total number of add on purchases, to enable this organization to use.
eXtended Detection	Check this checkbox to give the organization access to this feature. This option is only available on setups that have purchased an eXtended Detection add on. See Licensing on page 277 for details on how to check the license type.
Mobile	Check this checkbox to enable mobile-related features. See Mobile on page 261.
Endpoint / IoT Devices License Capacity	Specifies the number of license seats for the organization, meaning the number of Collectors that can be installed in this organization. Before allocating licenses to an organization, you may need to verify the number of available licenses that can be distributed. All currently unallocated licenses are available for allocation to an organization. You cannot enter a number that is greater than the number of licenses available for allocation. The License Capacity field in the Licenses window shows the total number of license seats for the entire FortiEDR system, which are divided into endpoints (which includes workstations and servers) and IoT devices. The Default (hoster) organization initially receives the total allocation of licenses. The Administrator is responsible for allocating these licenses among organizations. In a single-organization FortiEDR system, licenses do not need to be allocated between organizations, as there is only one organization.

4. Click the *Save* button. Note that it may take a minute or so to create the organization.
   After creating the organization, the organization appears as a new row in the *Organization* dropdown list.



If a user attempts to use a feature that is not available with their license, a warning message displays. For example, as shown below.



Threat Hunting license was not purchased.

Contact Fortinet for more details

Moving from a single-organization to multi-organization structure in FortiEDR

In a single-organization system, the Default (hoster) organization is the only organization.

To create a multi-organization (multi-tenant) system, an Administrator simply needs to add one or more organizations to a single-organization system. When there are multiple organizations in the system, you can select the organization of interest in the *Organization* dropdown menu that appears at the top left of the window, as described below.

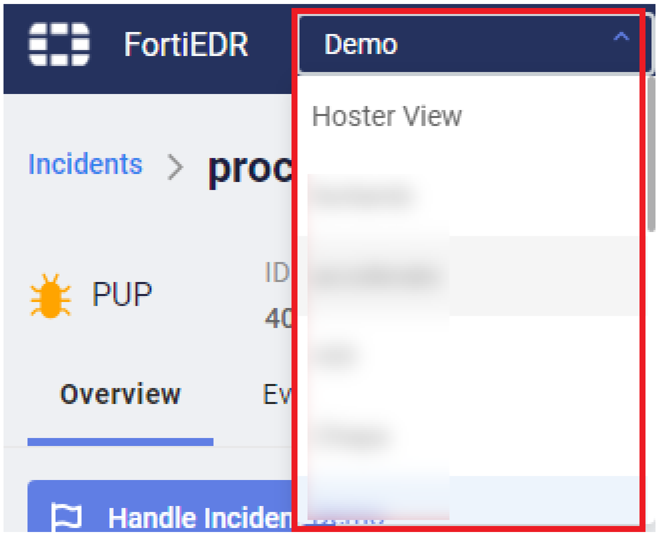
Step 3 - Navigating between organizations

In a multi-organization system, all types of information are now organized per organization.

Administrators can view information in the FortiEDR system for a specific organization or for all organizations together. To do so, use one of the following methods:

a. Select the *Hoster view* in the *Organization* dropdown menu at the top left of the window to display information for all organizations together. For more details about Hoster view, see Hoster view on page 434.

b. Select the organization of interest in the *Organization* dropdown list.



In Hoster view, each row in the *Organizations* pane represents a different organization. Note that after you select an organization, the entire user interface only shows information for that organization.

If that multiple web browser tabs or windows are opened on the same device and each of them navigates to a different organization on the FortiEDR Central Manager Console, they all show the data of the same organization, which is the last organization that was selected in the *Organization* dropdown list. In this case, the dropdown may look as if it points to Organization A however the data would be of Organization B.

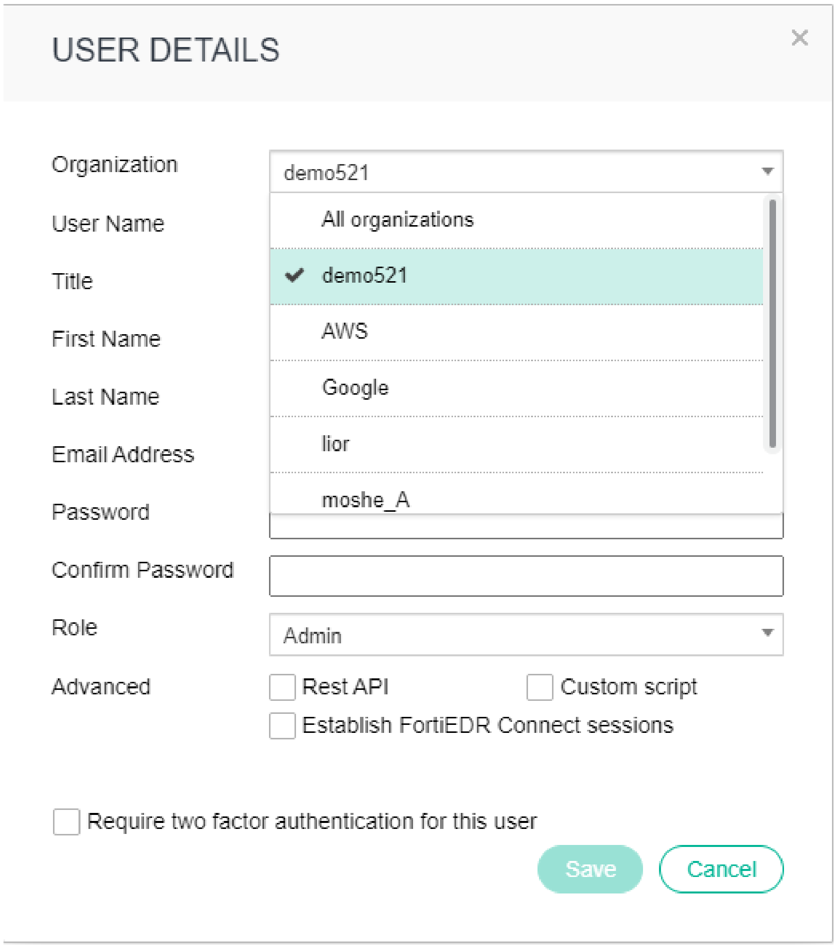
Step 4 – Defining an Administrator for an organization

Administrators can create one or more Administrators for an organization or for all organizations. You should define at least one Administrator for each organization.

To define an Administrator for an organization:

1. In Hoster view, click the *ADMINISTRATION* tab and then click *USERS* in the left pane.
2. Click the *Add User* button.

3. Select the organization in the *Organization* field, as shown below.



USER DETAILS

Organization	demo521
User Name	
Title	
First Name	
Last Name	
Email Address	
Password	
Confirm Password	
Role	Admin
Advanced	□ Rest API □ Custom script □ Establish FortiEDR Connect sessions

□ Require two factor authentication for this user

4. Fill in the displayed window, as described in Users on page 277.
5. Click *Save*.

Step 5 – Performing operations in the FortiEDR system

Administrators can perform all of the operations described from Security Settings on page 196 to Threat Hunting on page 125 in this guide using the user interface of the FortiEDR Central Manager for all organizations in the system.

Administrators can monitor the system per organization or using Hoster view, which shows data for all organizations together.

Migrating an organization

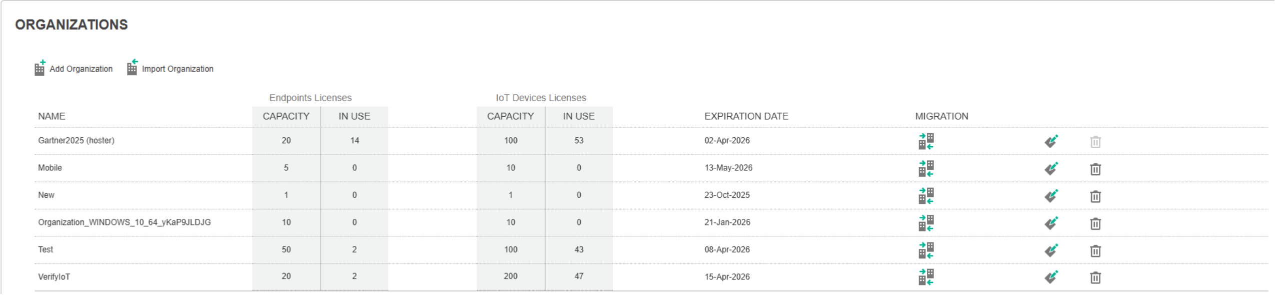
FortiEDR's Consolidation feature enables you to copy all the data and definitions within an organization from one environment to another environment. This feature copies an organization from one environment (`source setup/environment`) to another (`destination setup/environment`). The copy operation adds to the content in the destination environment, and does not replace the target's existing content.

This feature is only available to Administrators.

Organization migration involves three steps, which are described in detail in the procedure below.

To migrate an organization:

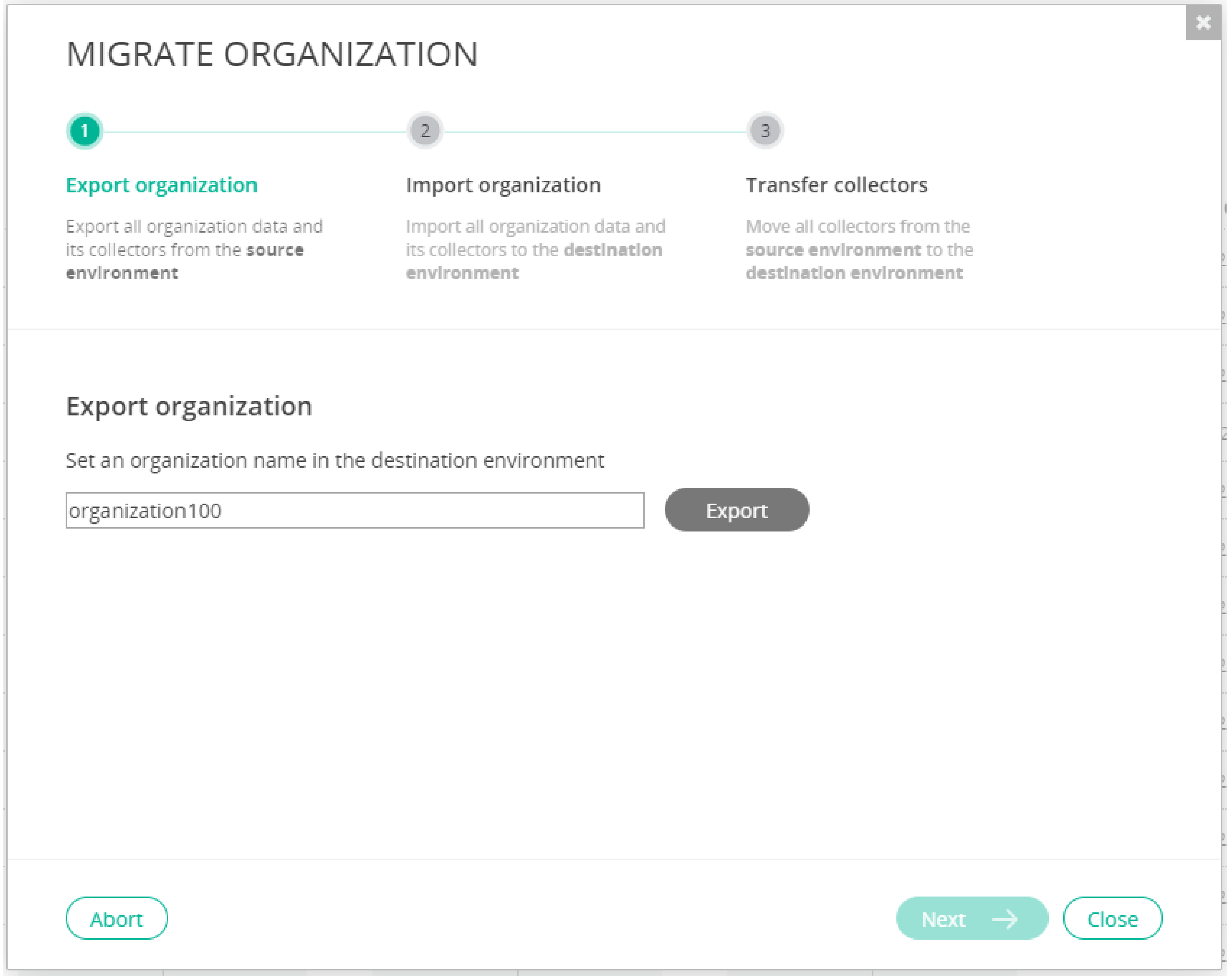
1. Click the *ADMINISTRATION* tab and then click *ORGANIZATIONS* in the left pane. The *Organizations* window displays.



ORGANIZATIONS

NAME	Endpoints Licenses CAPACITY	Endpoints Licenses IN USE	IoT Devices Licenses CAPACITY	IoT Devices Licenses IN USE	EXPIRATION DATE	MIGRATION		
Gartner2025 (hoster)	20	14	100	53	02-Apr-2026			
Mobile	5	0	10	0	13-May-2026			
New	1	0	1	0	23-Oct-2025			
Organization_WINDOWS_10_64_yKaP9JLDJG	10	0	10	0	21-Jan-2026			
Test	50	2	100	43	08-Apr-2026			
VerifyIoT	20	2	200	47	15-Apr-2026			

2. Click the *Migrate organization* button in the row of the source organization that you want to copy to another environment. The following window displays:



MIGRATE ORGANIZATION

1 Export organization
Export all organization data and its collectors from the **source environment**

2 Import organization
Import all organization data and its collectors to the **destination environment**

3 Transfer collectors
Move all collectors from the **source environment** to the **destination environment**

Export organization

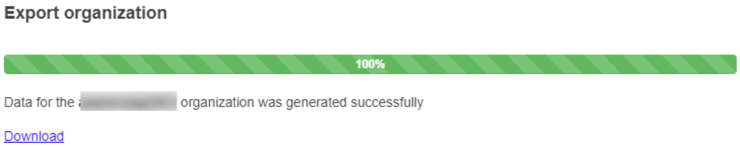
Set an organization name in the destination environment

organization100

From this window, you perform three steps to migrate the organization to another environment:

- **a.** Export the Organization: This step exports all the data of the selected organization to a zip file.
- **b.** This step imports all the organization’s data using the zip file exported in step 1. Note that this step is performed on the destination environment.
- **c.** This step moves all the Collectors of the selected organization from the source environment to the destination environment.

3. In the *Export organization* field, specify the name of the organization to appear for this data in the destination environment. Make sure that you assign an organization name that does not already exist in the destination environment.
4. Click the *Export* button. All the data and definitions for the organization are exported to a zip file. The zip file is named as follows: `<source organization name>_<environment name>_FortiEDR_<timestamp>_Export.zip`. For example, `ad_localhost.localdomain_enSilo_Feb.05.2019_Export.zip`.
   After the export completes, a *Download* link displays in the window:



Export organization

100%

Data for the [redacted] organization was generated successfully

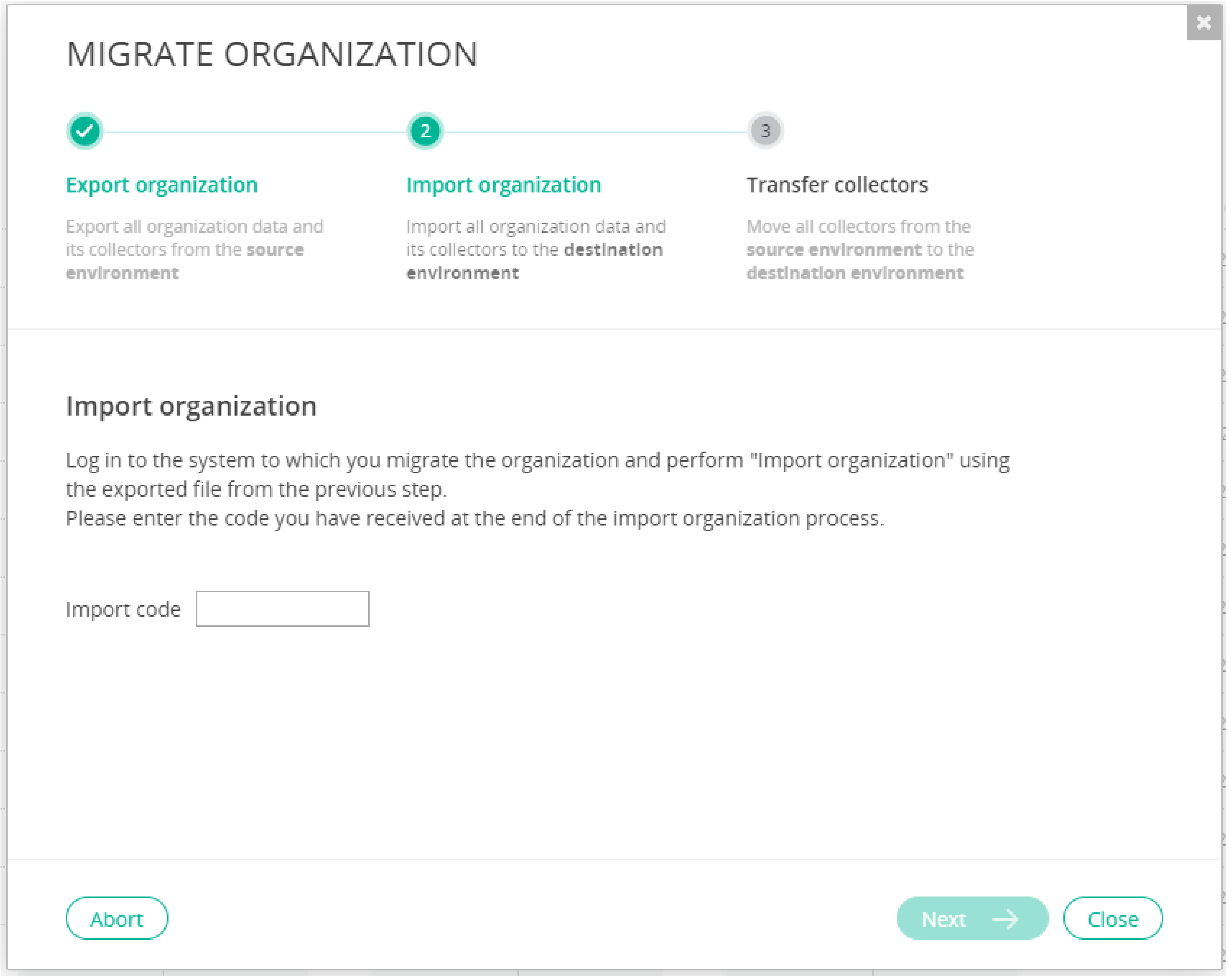
You can cancel the migration process at any time by clicking the *Abort* button.

5. Click the *Download* link to download the exported zip file.

Click the *Close* button if you want to close this window and continue the migration process at a later time. This action saves the relevant organizational data. You can later continue this migration process by using the *Continue Migration* Cont. button.

If you click the *Close* button before downloading the exported zip file, a warning displays. In this case, you must perform the migration process again from the beginning.

6. Click *Next*. The following window displays:



MIGRATE ORGANIZATION

✓ **Export organization** Export all organization data and its collectors from the **source environment**

2 **Import organization** Import all organization data and its collectors to the **destination environment**

3 **Transfer collectors** Move all collectors from the **source environment** to the **destination environment**

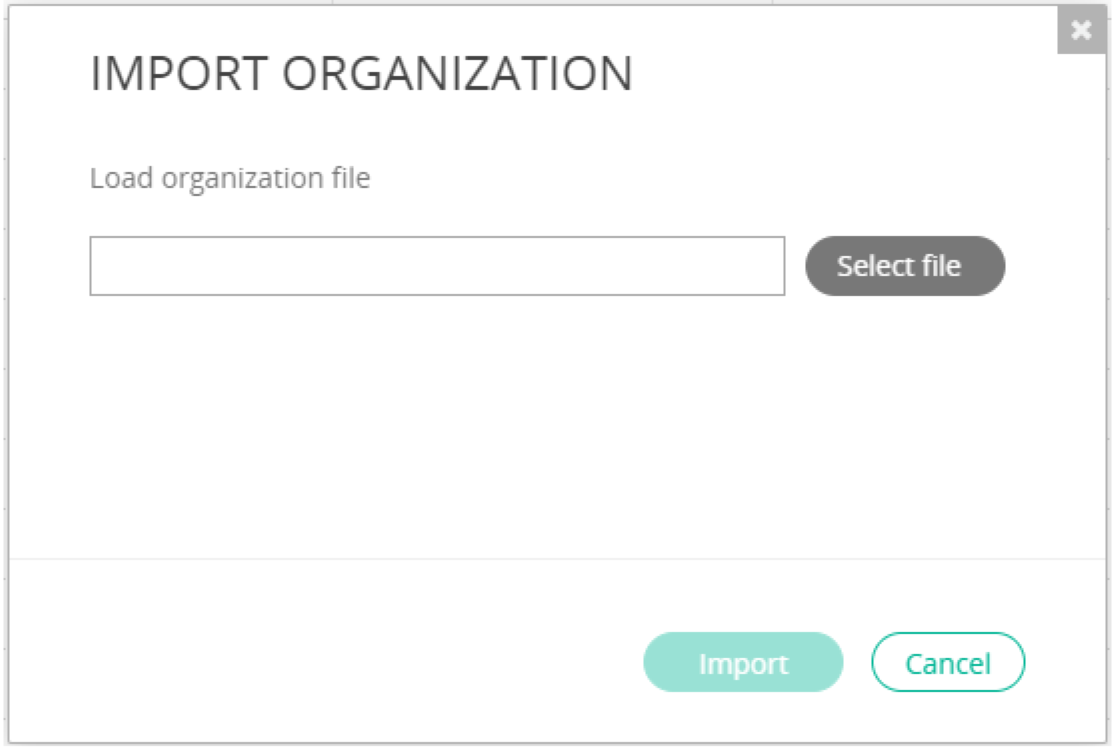
Import organization

Log in to the system to which you migrate the organization and perform "Import organization" using the exported file from the previous step.
Please enter the code you have received at the end of the import organization process.

Import code

7. Log in to the destination environment.
8. Click the *ADMINISTRATION* tab and then click *ORGANIZATIONS* in the left pane.

9. In the *ORGANIZATIONS* page, click the *Import Organization* button. The following window displays:



IMPORT ORGANIZATION

Load organization file

10. Select the exported zip file to load and then click *Import*. This step copies all the data and environment definitions of the exported organization.

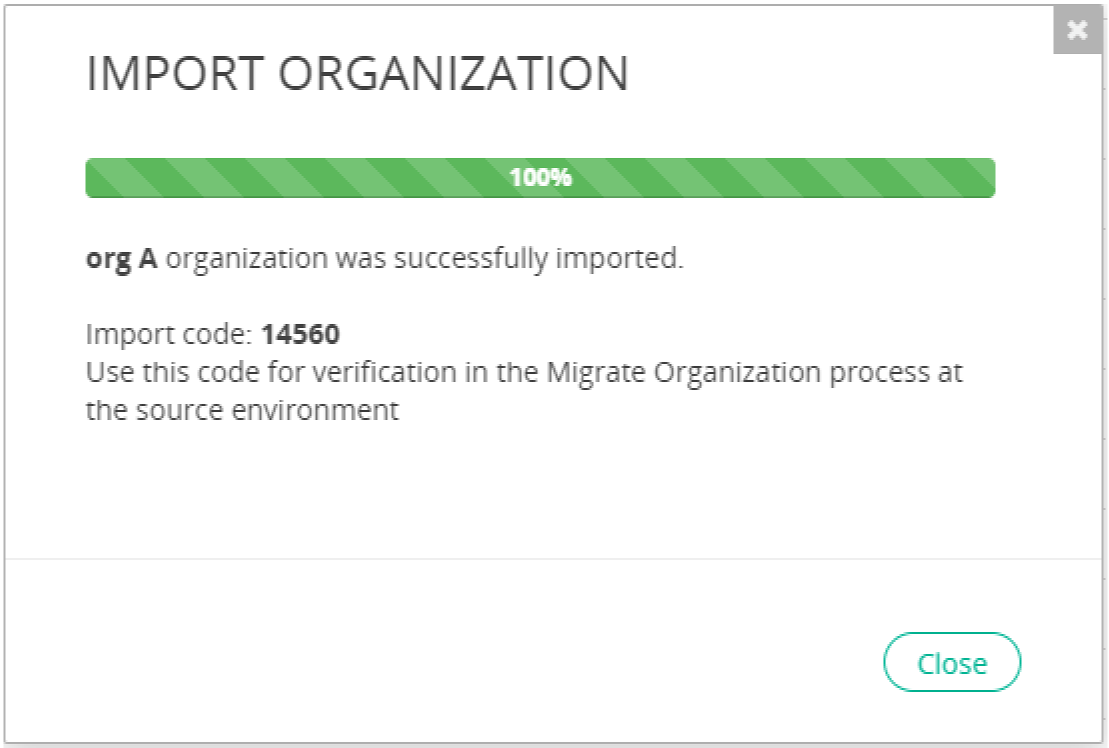
You cannot import an exported organization that has a name that already exists in the destination environment.

To import an organization, the FortiEDR platform version must be the same in both the source and destination environments.

The content version must be the same in both the source and destination environments. You can see the Content Version at the bottom of the Licensing on page 277 window.

You must have sufficient workstation and server licenses in the destination environment.

At the end of the import process, the *Import Organization* window displays a code. Write down this code, as it will be entered later as part of the migration process.

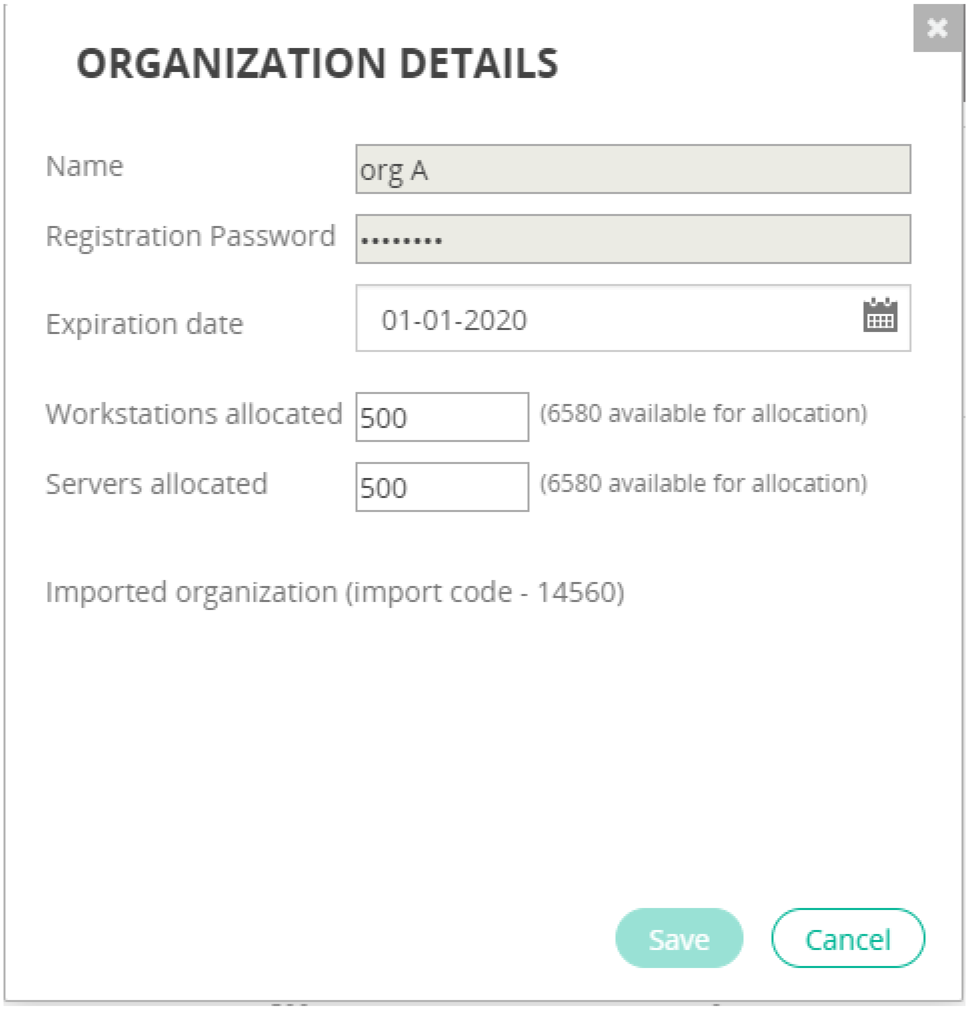


IMPORT ORGANIZATION

org A organization was successfully imported.

Import code: **14560**
Use this code for verification in the Migrate Organization process at the source environment

The *Import code* also displays in the *Organization Details* window, which you can display at any time by clicking the *Edit* button in an organization row in the *Organizations* window.



ORGANIZATION DETAILS

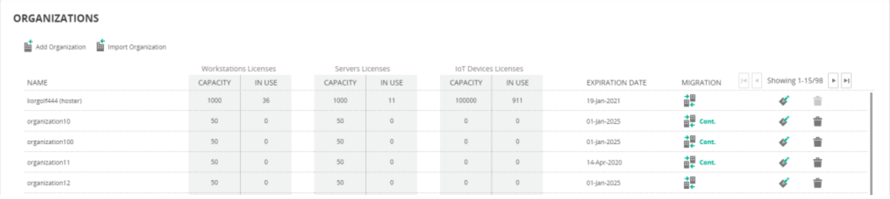
Name	org A
Registration Password	••••••••
Expiration date	01-01-2020
Workstations allocated	500 (6580 available for allocation)
Servers allocated	500 (6580 available for allocation)

Imported organization (import code - 14560)

Note that the name of the organization cannot be changed in this window, and is read-only.

11. In step 2 of the *Migrate Organization* window, enter or copy the import code into the *Import code* field.

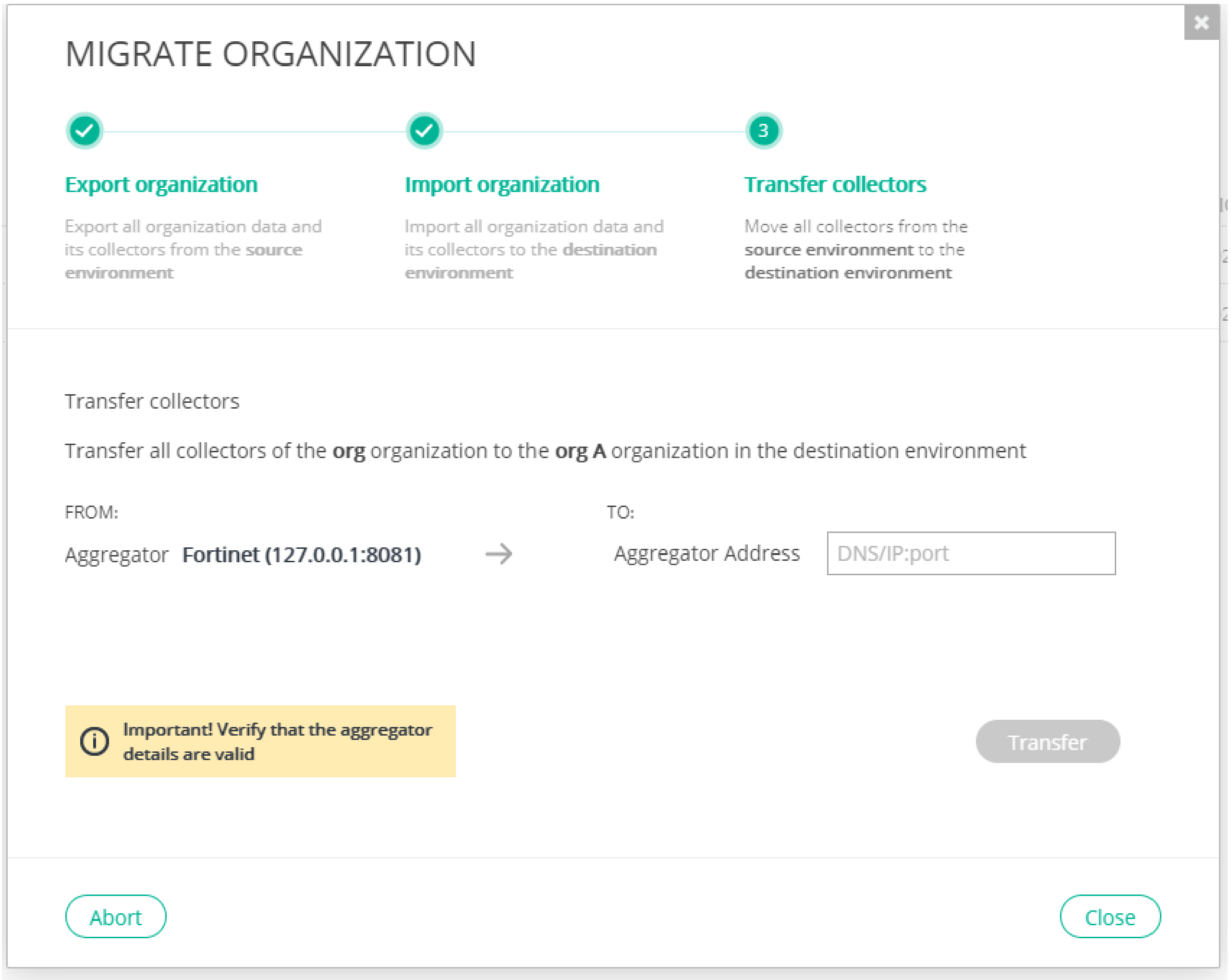
If you previously closed the *Migrate Organization* window, then click the *Continue Migration* Cont. button in the source organization row in the *ORGANIZATIONS* page.



ORGANIZATIONS

	Workstations Licenses		Servers Licenses		IoT Devices Licenses			
NAME	CAPACITY	IN USE	CAPACITY	IN USE	CAPACITY	IN USE	EXPIRATION DATE	MIGRATION
liorgolf444 (hoster)	1000	36	1000	11	100000	911	19-Jan-2021	
organization10	50	0	50	0	0	0	01-Jan-2025	Cont.
organization100	50	0	50	0	0	0	01-Jan-2025	Cont.
organization11	50	0	50	0	0	0	14-Apr-2020	Cont.
organization12	50	0	50	0	0	0	01-Jan-2025	

12. Click *Next*. The following window displays:



MIGRATE ORGANIZATION

✓
Export organization
Export all organization data and its collectors from the source environment
✓
Import organization
Import all organization data and its collectors to the destination environment
3
Transfer collectors
Move all collectors from the source environment to the destination environment

Transfer collectors

Transfer all collectors of the **org** organization to the **org A** organization in the destination environment

FROM:

Aggregator **Fortinet (127.0.0.1:8081)** →

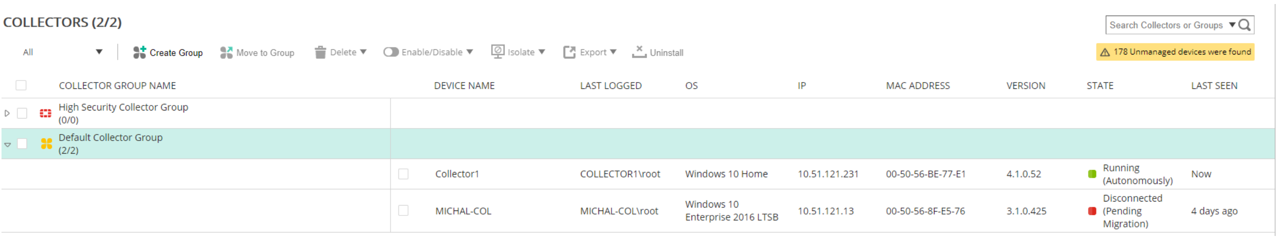
TO:

Aggregator Address DNS/IP:port

Important! Verify that the aggregator details are valid

In this window, you move the Collectors from the source environment to the destination environment. The Collectors cannot be registered to both environments at the same time.

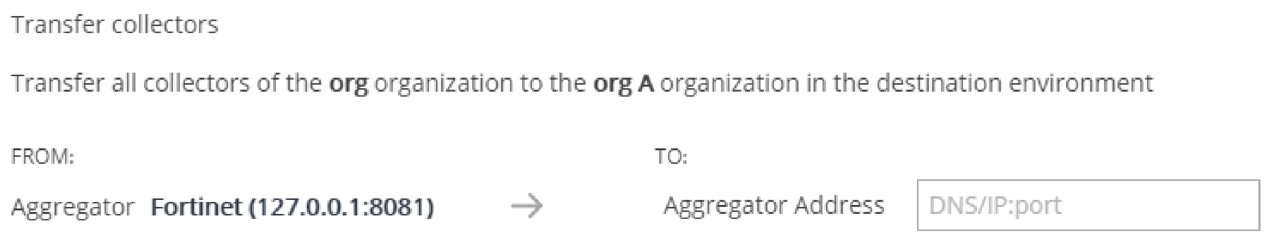
Note that until this step is completed, the Collectors are still registered to the organization in the source environment and their status and security events are displayed there. In the destination environment, Collectors are displayed with the *Pending Migration* state, as shown in the *Inventory* window. This state indicates that the Collector has not yet been transferred from the source environment to this environment. Collectors in the *Pending Migration* state are still registered to the source environment.



COLLECTORS (2/2)

COLLECTOR GROUP NAME	DEVICE NAME	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	STATE	LAST SEEN
High Security Collector Group (0/0)								
Default Collector Group (2/2)								
	Collector1	COLLECTOR1\root	Windows 10 Home	10.51.121.231	00-50-56-BE-77-E1	4.1.0.52	🟩 Running (Autonomously)	Now
	MICHAL-COL	MICHAL-COL\root	Windows 10 Enterprise 2016 LTSB	10.51.121.13	00-50-56-8F-E5-76	3.1.0.425	🟥 Disconnected (Pending Migration)	4 days ago

13. Specify the *Aggregator Address* in the *To* field. Each Collector is connected to one Aggregator. In this field, you specify the IP address or DNS name and the port of the Aggregator that will service the Collectors in the destination environment.



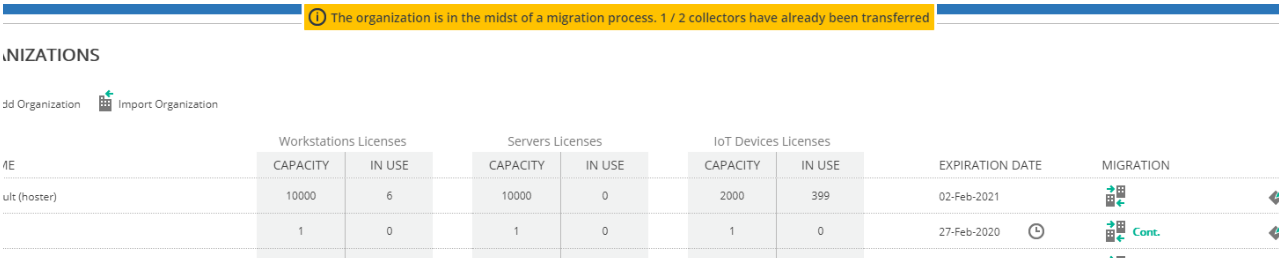
Transfer collectors

Transfer all collectors of the **org** organization to the **org A** organization in the destination environment

FROM: Aggregator **Fortinet (127.0.0.1:8081)** →

TO: Aggregator Address DNS/IP:port

14. Click the *Transfer* button. The Collectors are transferred from the organization in the source environment to the organization in the destination environment. A progress indicator counter displays as the Collectors are transferred.



The organization is in the midst of a migration process. 1 / 2 collectors have already been transferred

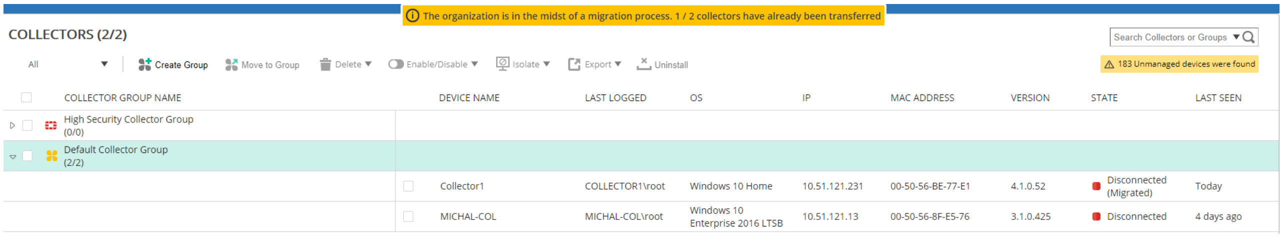
ANIZATIONS

	Workstations Licenses		Servers Licenses		IoT Devices Licenses			
ME	CAPACITY	IN USE	CAPACITY	IN USE	CAPACITY	IN USE	EXPIRATION DATE	MIGRATION
ult (hoster)	10000	6	10000	0	2000	399	02-Feb-2021	
	1	0	1	0	1	0	27-Feb-2020	Cont.

The progress indicator counter continues to display until the organization is deleted in the source environment, which is recommended after all Collectors have been transferred from the source environment to the destination environment. See step 16 below.

If you click the *Abort* button at this step, any Collectors already transferred from the source environment to the destination environment remain in the destination environment.

After a Collector has been transferred from the source environment to the destination environment, its state is *Migrated* in the source environment, and is *Running* (functional) in the destination environment.



The organization is in the midst of a migration process. 1 / 2 collectors have already been transferred

COLLECTORS (2/2)

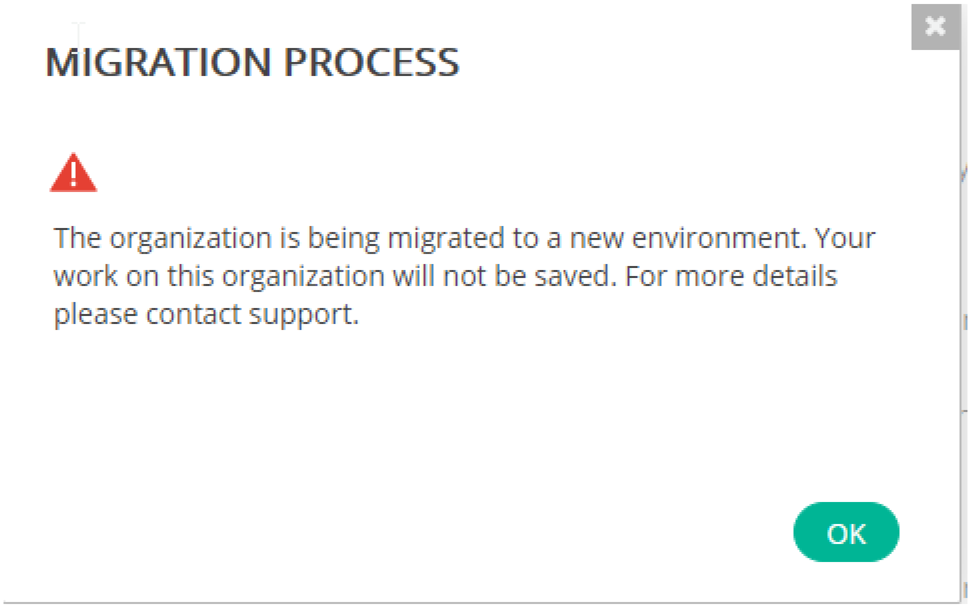
183 Unmanaged devices were found

COLLECTOR GROUP NAME	DEVICE NAME	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	STATE	LAST SEEN
High Security Collector Group (0/0)								
Default Collector Group (2/2)								
	Collector1	COLLECTOR1\root	Windows 10 Home	10.51.121.231	00-50-56-BE-77-E1	4.1.0.52	Disconnected (Migrated)	Today
	MICHAL-COL	MICHAL-COL\root	Windows 10 Enterprise 2016 LTSB	10.51.121.13	00-50-56-8F-E5-76	3.1.0.425	Disconnected	4 days ago

Collector protection remains in effect throughout the entire migration process.

15. (Optional) Click the *Stop Transfer* button to pause the Collector transfer process. You can resume the transfer process by clicking the *Transfer* button again.

If a user enters the source organization while a migration process is in progress for it, a warning displays. Any changes made by this user will not be migrated or included in the destination organization. Any changes made to an organization while it is being migrated are ultimately lost.



MIGRATION PROCESS

The organization is being migrated to a new environment. Your work on this organization will not be saved. For more details please contact support.

16. After all the Collectors were successfully migrated from the organization on the source environment to the organization on the destination environment, delete the source organization. To do so, select the *Administration* tab and then click *Organizations* in the left pane. In the *Organizations* window, click the *Delete* button in the row of the source organization to be removed.

Collector protection and functionality remain throughout the entire migration process.

Hoster view

When you select *Hoster* view in the *Organization* dropdown list, all windows in the user interface are affected. In general, this view shows aggregated data for all organizations.

However, some data is only available in Hoster view, such as the following:

- *Export Settings*: In a multi-organization system, SMTP-related information is only displayed in Hoster view.
- *Administration* > *Settings*: The *Session Time Out* setting is available only in Hoster view.

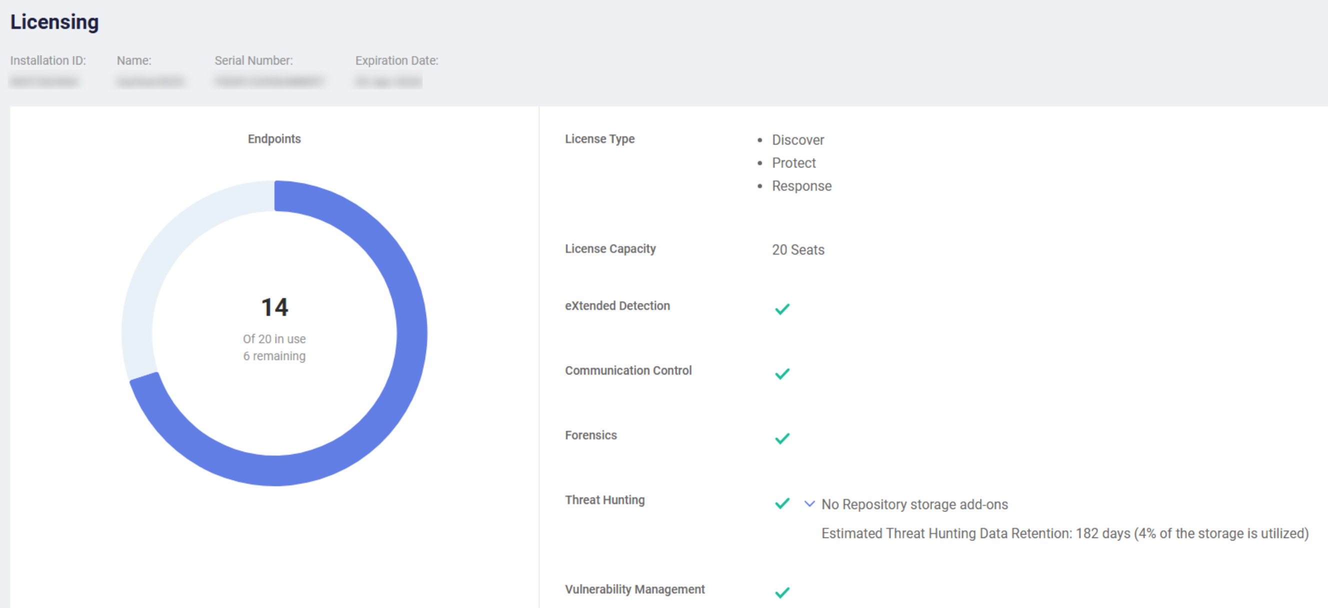
In addition, there are some special cases where you cannot view administration data in Hoster view, and can only view data for a specific organization, such as the following:

- Component Authentication
- Automatic Updates
- End User Notifications
- Periodic Scan

Many of the windows that display aggregated data for all organizations have some special features when displaying data in Hoster view. In general, in Hoster view, these windows have an additional column or field, and require that you specify the organization in order to add the item. Several examples are provided below. The examples below are not all-inclusive.

Licensing

When in Hoster view, the *Licensing* window shows aggregated information for all organizations.



Licensing

Installation ID: [redacted] Name: [redacted] Serial Number: [redacted] Expiration Date: [redacted]

Endpoints

14
Of 20 in use
6 remaining

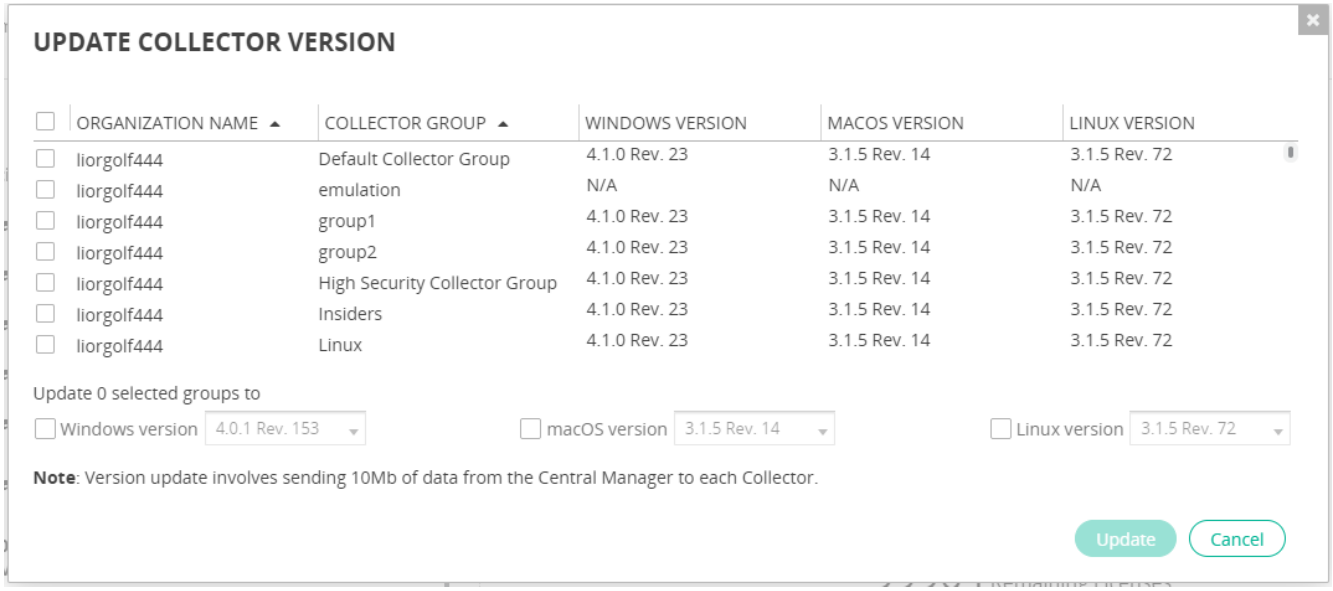
License Type	• Discover • Protect • Response
License Capacity	20 Seats
eXtended Detection	✓
Communication Control	✓
Forensics	✓
Threat Hunting	✓ No Repository storage add-ons Estimated Threat Hunting Data Retention: 182 days (4% of the storage is utilized)
Vulnerability Management	✓

For example, the Workstations and Servers diagrams indicate the number of allocated and available licenses for all workstations and servers, respectively, in the entire FortiEDR system. The *Licenses in Use* numbers represent the number of Collectors that have been installed out of the total permitted to be installed.

The *Load Content* option loads content to all organizations. Once loaded, the new configuration applies to all organizations, including new Collector installers. However, Collectors are not being updated yet.

When in this view, you cannot load content to a specific organization.

When you click the *Update Collectors* button in the *Licensing* window, the *Update Collector Version* window displays, and includes an *Organization Name* column. Use the checkboxes in this column to update the organization for a Collector Group. All other functionality in this window works in the standard manner.



UPDATE COLLECTOR VERSION

□	ORGANIZATION NAME ▲	COLLECTOR GROUP ▲	WINDOWS VERSION	MACOS VERSION	LINUX VERSION
□	liorgolf444	Default Collector Group	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
□	liorgolf444	emulation	N/A	N/A	N/A
□	liorgolf444	group1	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
□	liorgolf444	group2	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
□	liorgolf444	High Security Collector Group	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
□	liorgolf444	Insiders	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
□	liorgolf444	Linux	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72

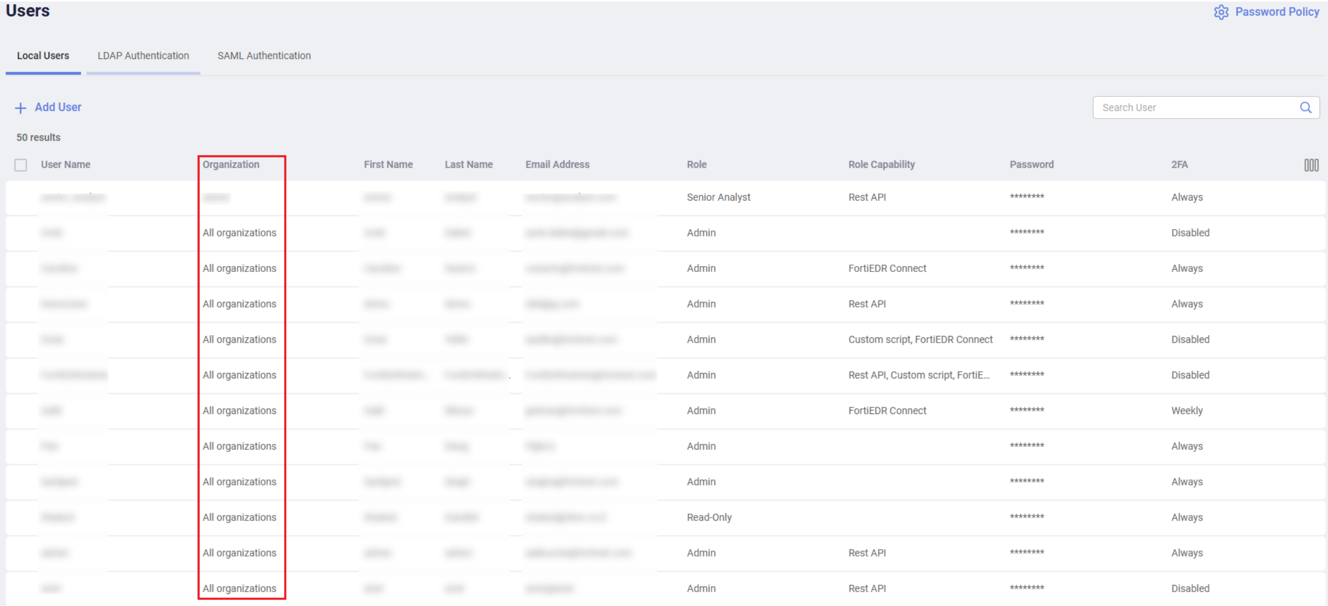
Update 0 selected groups to

□ Windows version 4.0.1 Rev. 153 □ macOS version 3.1.5 Rev. 14 □ Linux version 3.1.5 Rev. 72

Note: Version update involves sending 10Mb of data from the Central Manager to each Collector.

Users

In Hoster view, this window includes an *Organization* column.

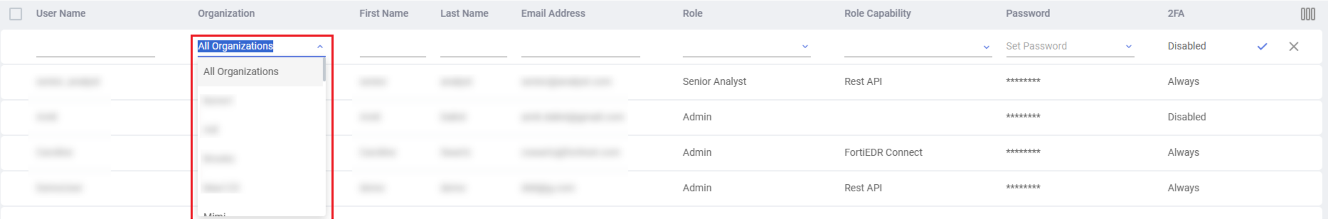


Users

50 results

□ User Name	Organization	First Name	Last Name	Email Address	Role	Role Capability	Password	2FA
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Senior Analyst	Rest API	********	Always
[redacted]	All organizations	[redacted]	[redacted]	[redacted]	Admin		********	Disabled
[redacted]	All organizations	[redacted]	[redacted]	[redacted]	Admin	FortiEDR Connect	********	Always
[redacted]	All organizations	[redacted]	[redacted]	[redacted]	Admin	Rest API	********	Always
[redacted]	All organizations	[redacted]	[redacted]	[redacted]	Admin	Custom script, FortiEDR Connect	********	Disabled
[redacted]	All organizations	[redacted]	[redacted]	[redacted]	Admin	Rest API, Custom script, FortiE...	********	Disabled
[redacted]	All organizations	[redacted]	[redacted]	[redacted]	Admin	FortiEDR Connect	********	Weekly
[redacted]	All organizations	[redacted]	[redacted]	[redacted]	Admin		********	Always
[redacted]	All organizations	[redacted]	[redacted]	[redacted]	Admin		********	Always
[redacted]	All organizations	[redacted]	[redacted]	[redacted]	Read-Only		********	Always
[redacted]	All organizations	[redacted]	[redacted]	[redacted]	Admin	Rest API	********	Always
[redacted]	All organizations	[redacted]	[redacted]	[redacted]	Admin	Rest API	********	Disabled

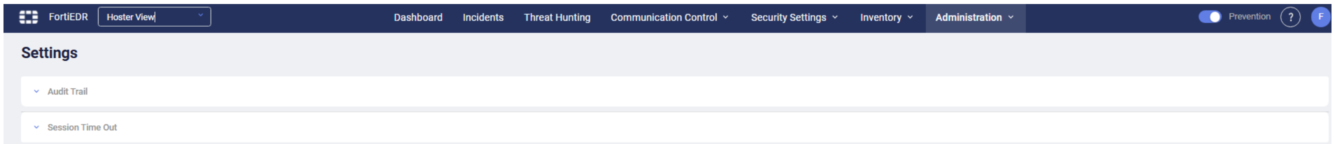
When you click the *Add User* button from this window, you must specify the *Organization* field . You can assign the user to one specific organization or *All organizations*.



User Name	Organization	First Name	Last Name	Email Address	Role	Role Capability	Password	2FA
	All Organizations						Set Password	Disabled
[redacted]		[redacted]	[redacted]	[redacted]	Senior Analyst	Rest API	********	Always
[redacted]		[redacted]	[redacted]	[redacted]	Admin		********	Disabled
[redacted]		[redacted]	[redacted]	[redacted]	Admin	FortiEDR Connect	********	Always
[redacted]		[redacted]	[redacted]	[redacted]	Admin	Rest API	********	Always

Settings

In Hoster view, the *Administration* > *Settings* page only includes the Audit Trail on page 314 and *Session Time Out* sections.



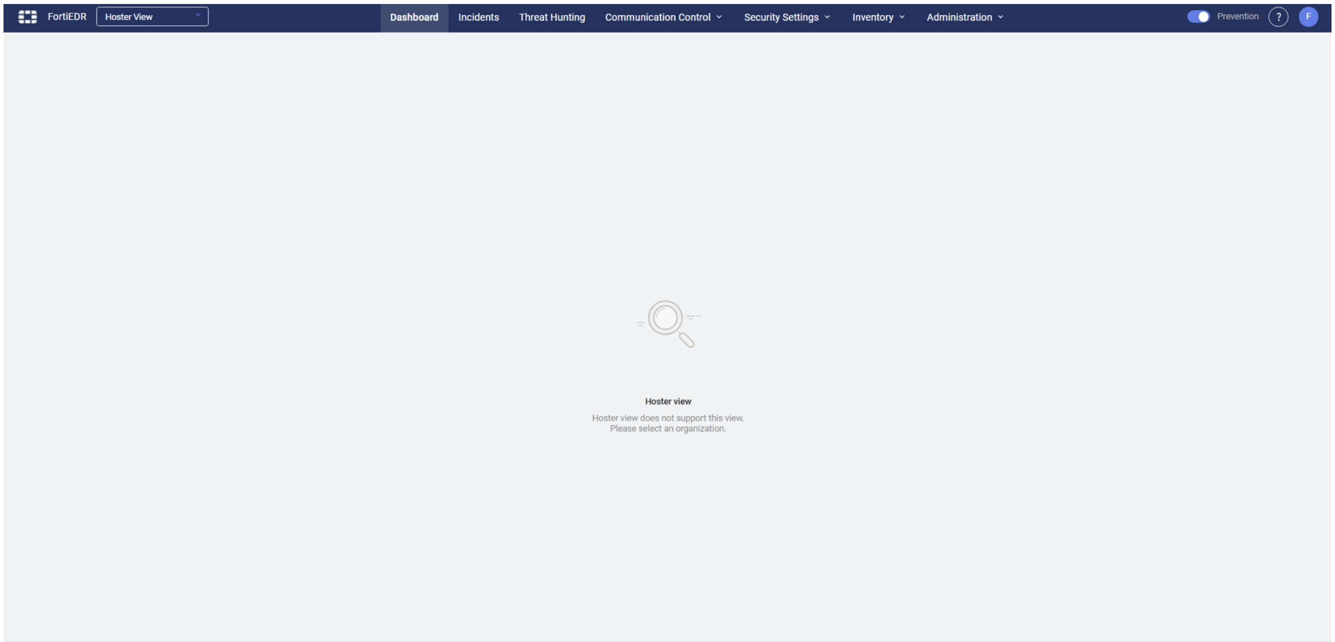
The *Session Time Out* section is specific to hoster view and can be used to configure the idle session timeout period, which is the duration (in minutes) before a session expires and users are prompted for credentials. The session timeout setting applies to all FortiEDR Console tabs except *Dashboard*. The default is 15 minutes. The acceptable value range is 1 - 1440.

The following sections are unavailable in the *Administration* > *Settings* page in Hoster view:

- Component Authentication on page 316
- File Scan on page 319
- End Users Notifications on page 320
- Personal Data Handling on page 325
- IoT Device Discovery on page 331
- Windows Security Center on page 333
- Application Control Manager on page 334
- FortiEDR Connect on page 334

Dashboard

In Hoster view, some information does not display in the Dashboard. The information that does display is aggregated for all organizations, such as Collectors, System Components, Repositories and so on, as shown below.



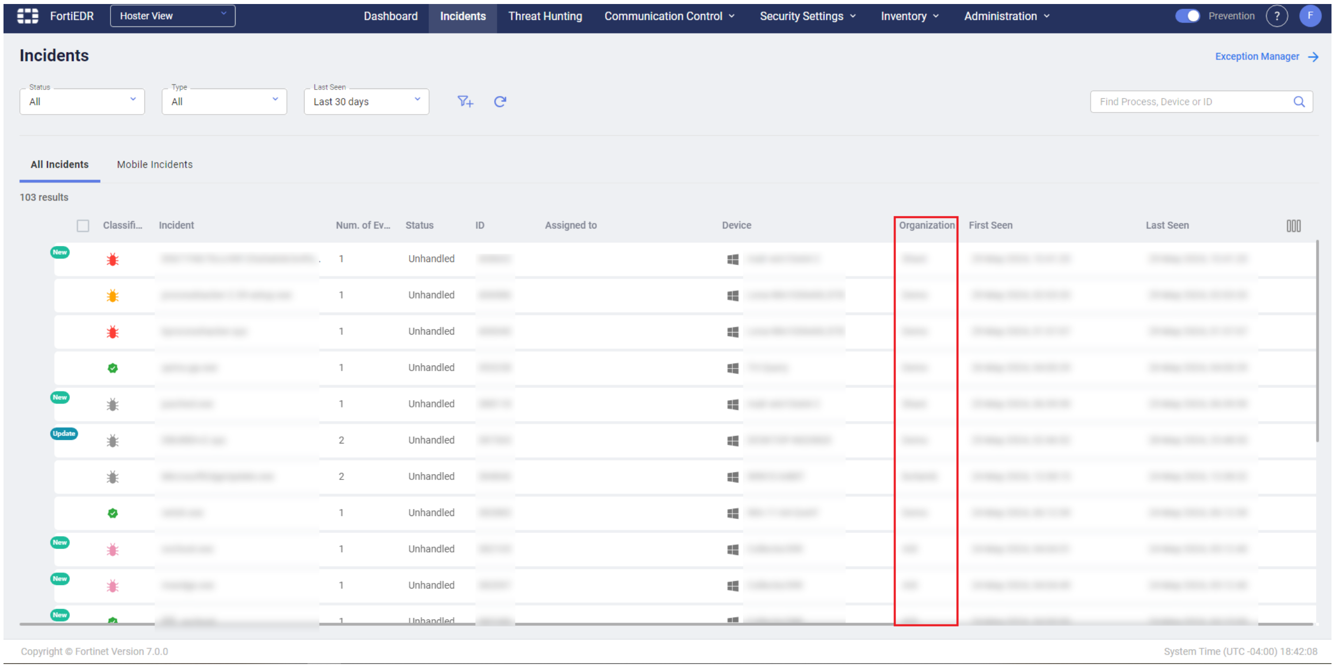
Hoster view

Hoster view does not support this view.
Please select an organization.

To view Dashboard information for a specific organization, you must select the organization of interest in the *Organization* dropdown list at the top left corner.

Incidents

In Hoster view, the *Incidents* tab displays the security events from all organizations. The *Organization* column indicates the organization in which the security event occurred.



Incidents

Status: All
Type: All
Last Seen: Last 30 days

All Incidents | Mobile Incidents

103 results

	Classifi...	Incident	Num. of Ev...	Status	ID	Assigned to	Device	Organization	First Seen	Last Seen
New	●	[redacted]	1	Unhandled	[redacted]		[redacted]	[redacted]	[redacted]	[redacted]
	●	[redacted]	1	Unhandled	[redacted]		[redacted]	[redacted]	[redacted]	[redacted]
	●	[redacted]	1	Unhandled	[redacted]		[redacted]	[redacted]	[redacted]	[redacted]
	✓	[redacted]	1	Unhandled	[redacted]		[redacted]	[redacted]	[redacted]	[redacted]
New	●	[redacted]	1	Unhandled	[redacted]		[redacted]	[redacted]	[redacted]	[redacted]
Update	●	[redacted]	2	Unhandled	[redacted]		[redacted]	[redacted]	[redacted]	[redacted]
	●	[redacted]	2	Unhandled	[redacted]		[redacted]	[redacted]	[redacted]	[redacted]
	✓	[redacted]	1	Unhandled	[redacted]		[redacted]	[redacted]	[redacted]	[redacted]
New	●	[redacted]	1	Unhandled	[redacted]		[redacted]	[redacted]	[redacted]	[redacted]
New	●	[redacted]	1	Unhandled	[redacted]		[redacted]	[redacted]	[redacted]	[redacted]
New	✓	[redacted]	1	Unhandled	[redacted]		[redacted]	[redacted]	[redacted]	[redacted]

Copyright © Fortinet Version 7.0.0

System Time (UTC -04:00) 18:42:08

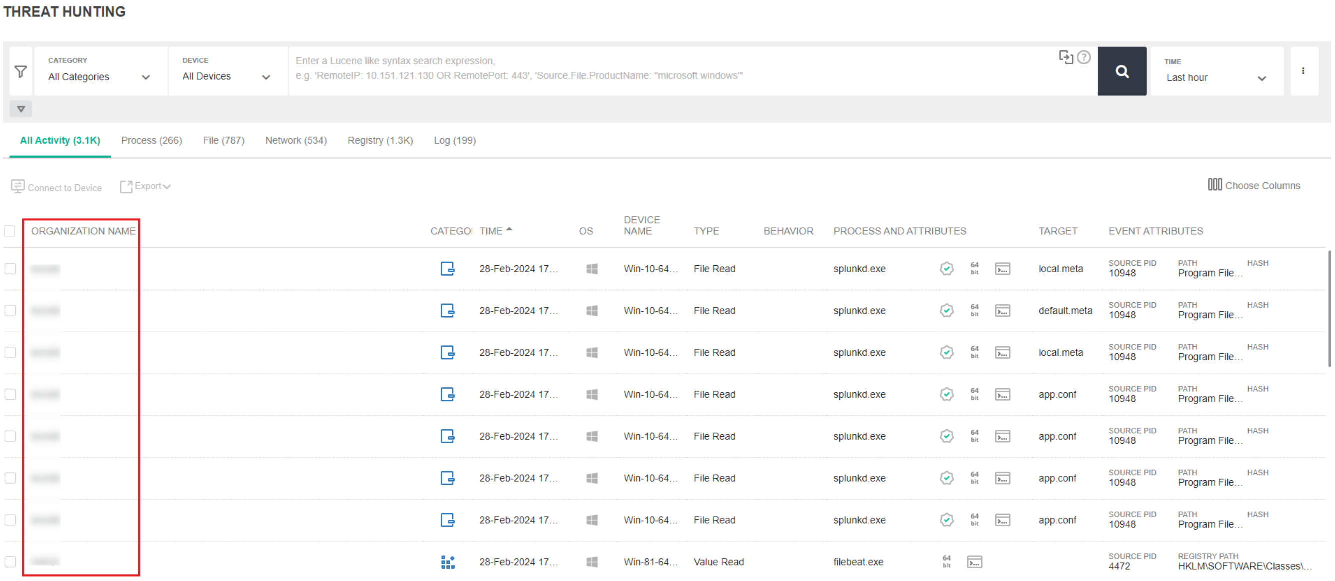
> The same security event can occur in multiple organizations. In this case, it is displayed in separate rows per organization.

The various options in the toolbar can be applied on multiple organizations simultaneously. For example, you can handle security events from different organizations at once using the *Handle Incident* button and you can export security events from different organizations using the *Export* button.

You can also use the *Handle Incident* button to handle security events from multiple organizations.

Threat Hunting

In Hoster view, this window includes an *Organization* column.



THREAT HUNTING

CATEGORY: All Categories
DEVICE: All Devices
Enter a Lucene like syntax search expression,
e.g. 'RemoteIP: 10.151.121.130 OR RemotePort: 443', 'Source.File.ProductName: "microsoft windows"'
TIME: Last hour

ORGANIZATION NAME	CATEGO	TIME	OS	DEVICE NAME	TYPE	BEHAVIOR	PROCESS AND ATTRIBUTES	TARGET	EVENT ATTRIBUTES
[redacted]		28-Feb-2024 17…		Win-10-64…	File Read		splunkd.exe	local.meta	SOURCE PID 10948 PATH Program File… HASH
[redacted]		28-Feb-2024 17…		Win-10-64…	File Read		splunkd.exe	default.meta	SOURCE PID 10948 PATH Program File… HASH
[redacted]		28-Feb-2024 17…		Win-10-64…	File Read		splunkd.exe	local.meta	SOURCE PID 10948 PATH Program File… HASH
[redacted]		28-Feb-2024 17…		Win-10-64…	File Read		splunkd.exe	app.conf	SOURCE PID 10948 PATH Program File… HASH
[redacted]		28-Feb-2024 17…		Win-10-64…	File Read		splunkd.exe	app.conf	SOURCE PID 10948 PATH Program File… HASH
[redacted]		28-Feb-2024 17…		Win-10-64…	File Read		splunkd.exe	app.conf	SOURCE PID 10948 PATH Program File… HASH
[redacted]		28-Feb-2024 17…		Win-10-64…	File Read		splunkd.exe	app.conf	SOURCE PID 10948 PATH Program File… HASH
[redacted]		28-Feb-2024 17…		Win-81-64…	Value Read		filebeat.exe		SOURCE PID 4472 REGISTRY PATH HKLM\SOFTWARE\Classes\…

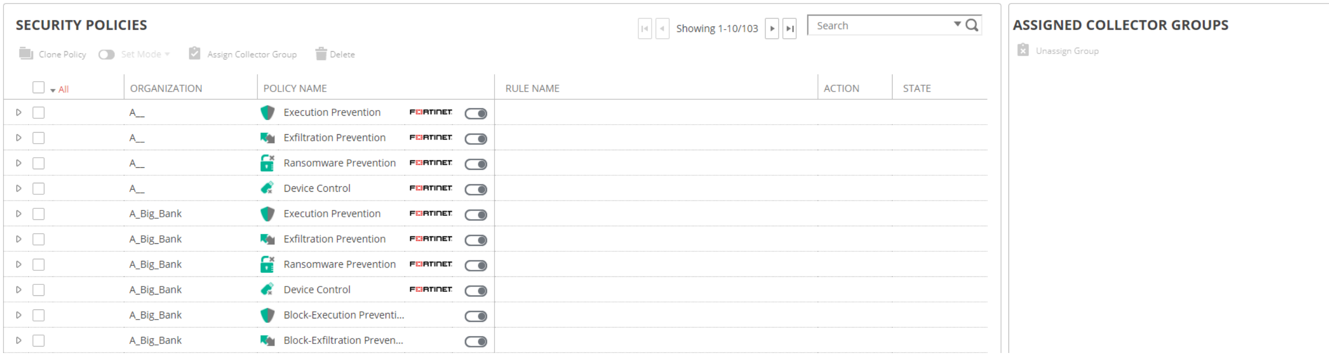
Communication Control

The *Communication Control* window is not available in Hoster view.

Security settings

SECURITY POLICIES page

In Hoster view, the *SECURITY POLICIES* page displays all policies from all organizations.



SECURITY POLICIES

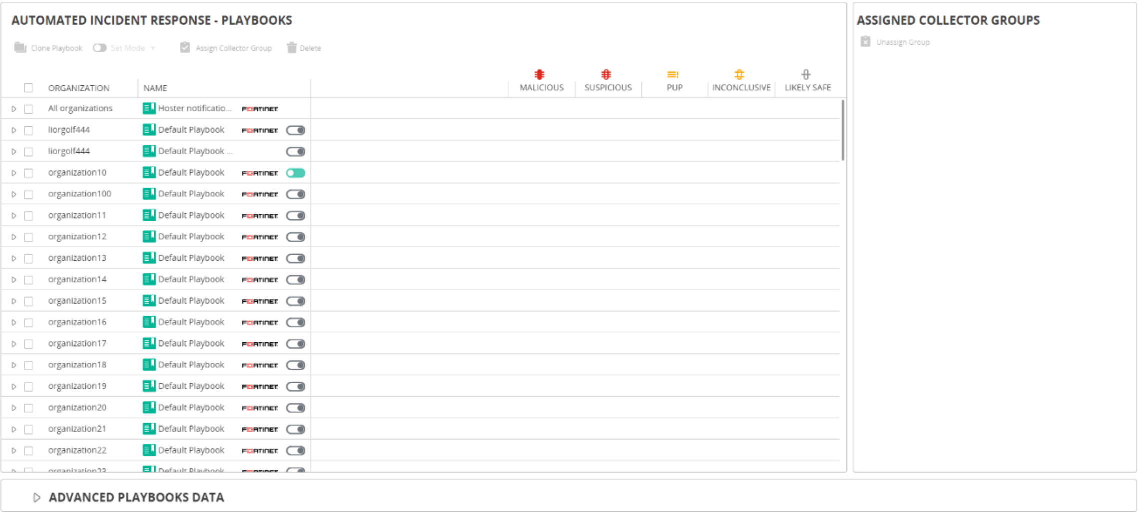
All	ORGANIZATION	POLICY NAME	RULE NAME	ACTION	STATE
▷ □	A__	Execution Prevention			
▷ □	A__	Exfiltration Prevention			
▷ □	A__	Ransomware Prevention			
▷ □	A__	Device Control			
▷ □	A_Big_Bank	Execution Prevention			
▷ □	A_Big_Bank	Exfiltration Prevention			
▷ □	A_Big_Bank	Ransomware Prevention			
▷ □	A_Big_Bank	Device Control			
▷ □	A_Big_Bank	Block-Execution Preventi...			
▷ □	A_Big_Bank	Block-Exfiltration Preven...			

ASSIGNED COLLECTOR GROUPS

FortiEDR's multi-organization feature enables you to clone a security policy from one organization to another. To do so, you must be in Hoster view. When not in Hoster view, you can only clone a policy within the same organization.

AUTOMATED INCIDENT RESPONSE - PLAYBOOKS page

In Hoster view, you can view all the notifications for the entire organization, based on the actions defined in the Hoster Notifications Playbook. This Playbook policy is only available in Hoster view.



AUTOMATED INCIDENT RESPONSE - PLAYBOOKS

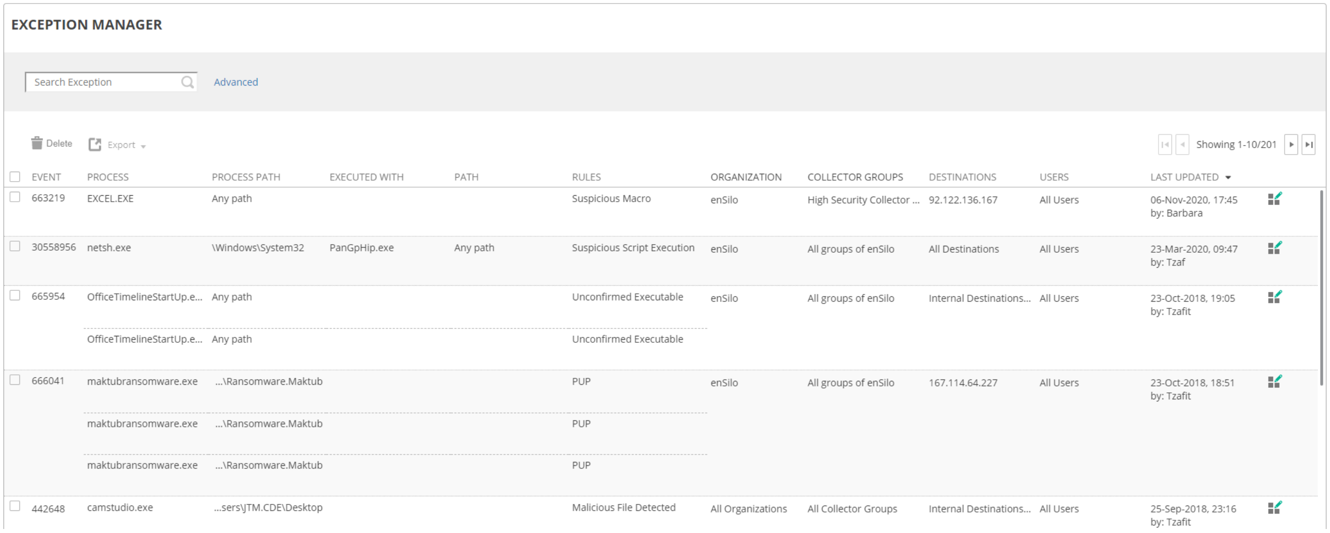
□	ORGANIZATION	NAME	MALICIOUS	SUSPICIOUS	PUP	INCONCLUSIVE	LIKELY SAFE
▷ □	All organizations	Hoster notificatio...					
▷ □	liorgolf444	Default Playbook					
▷ □	liorgolf444	Default Playbook ...					
▷ □	organization10	Default Playbook					
▷ □	organization100	Default Playbook					
▷ □	organization11	Default Playbook					
▷ □	organization12	Default Playbook					
▷ □	organization13	Default Playbook					
▷ □	organization14	Default Playbook					
▷ □	organization15	Default Playbook					
▷ □	organization16	Default Playbook					
▷ □	organization17	Default Playbook					
▷ □	organization18	Default Playbook					
▷ □	organization19	Default Playbook					
▷ □	organization20	Default Playbook					
▷ □	organization21	Default Playbook					
▷ □	organization22	Default Playbook					
▷ □	organization23	Default Playbook					

ASSIGNED COLLECTOR GROUPS

▷ ADVANCED PLAYBOOKS DATA

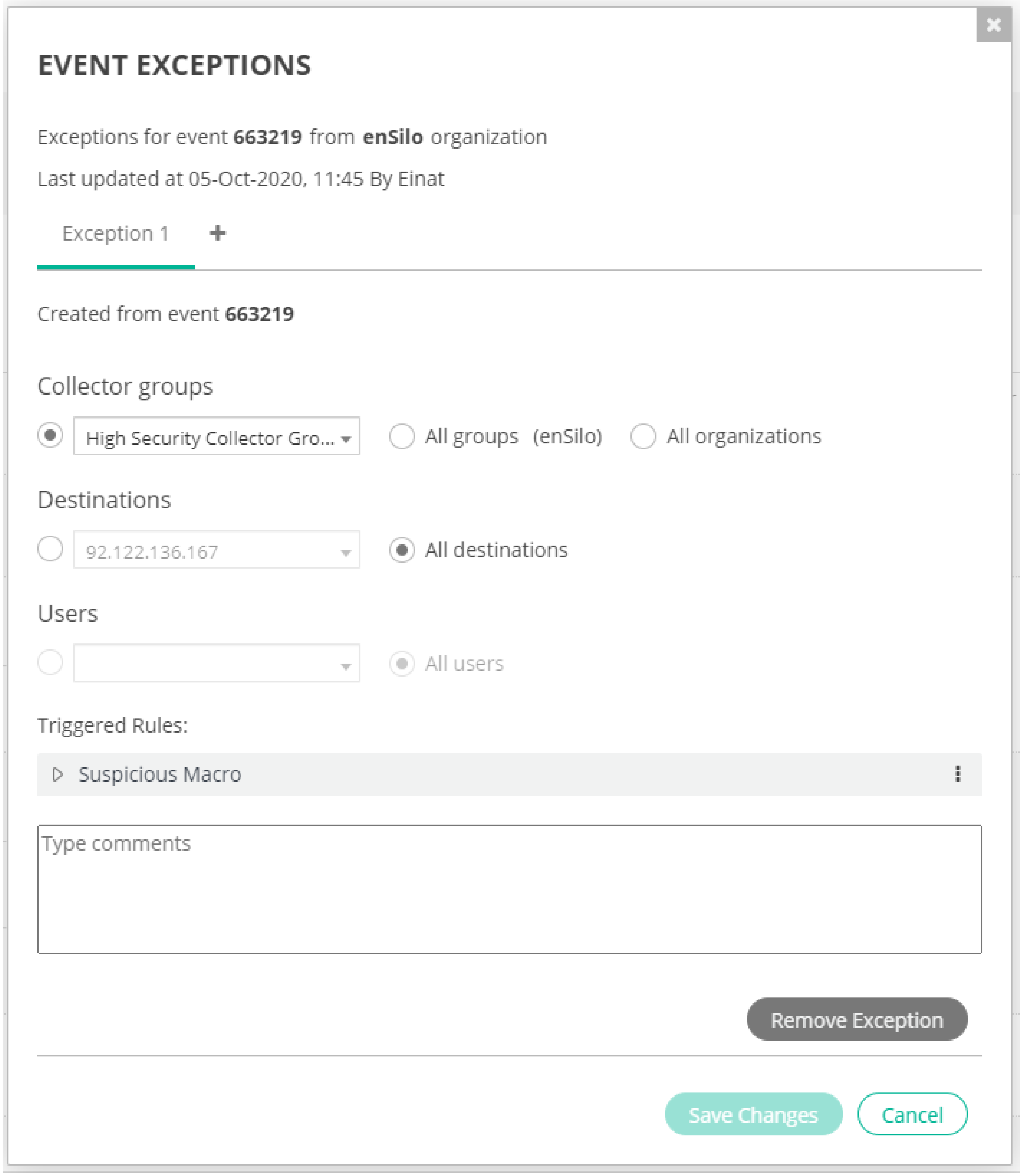
Exception Manager

In Hoster view, the *Exception Manager* page displays all exceptions from all organizations.



□	EVENT	PROCESS	PROCESS PATH	EXECUTED WITH	PATH	RULES	ORGANIZATION	COLLECTOR GROUPS	DESTINATIONS	USERS	LAST UPDATED
□	663219	EXCEL.EXE	Any path			Suspicious Macro	enSilo	High Security Collector ...	92.122.136.167	All Users	06-Nov-2020, 17:45 by: Barbara
□	30558956	netsh.exe	\Windows\System32	PanGpHip.exe	Any path	Suspicious Script Execution	enSilo	All groups of enSilo	All Destinations	All Users	23-Mar-2020, 09:47 by: Tzaf
□	665954	OfficeTimelineStartUp.e...	Any path			Unconfirmed Executable	enSilo	All groups of enSilo	Internal Destinations...	All Users	23-Oct-2018, 19:05 by: Tzafit
		OfficeTimelineStartUp.e...	Any path			Unconfirmed Executable					
□	666041	maktubransomware.exe	...\Ransomware.Maktub			PUP	enSilo	All groups of enSilo	167.114.64.227	All Users	23-Oct-2018, 18:51 by: Tzafit
		maktubransomware.exe	...\Ransomware.Maktub			PUP					
		maktubransomware.exe	...\Ransomware.Maktub			PUP					
□	442648	camstudio.exe	...sers\JTM.CDE\Desktop			Malicious File Detected	All Organizations	All Collector Groups	Internal Destinations...	All Users	25-Sep-2018, 23:16 by: Tzafit

When creating an exception in Hoster view, the organization in which the security event occurred is also shown in the *Exception Creation* window, as well as the event ID.



EVENT EXCEPTIONS

Exceptions for event **663219** from **enSilo** organization

Last updated at 05-Oct-2020, 11:45 By Einat

Created from event **663219**

Collector groups

● High Security Collector Gro... ○ All groups (enSilo) ○ All organizations

Destinations

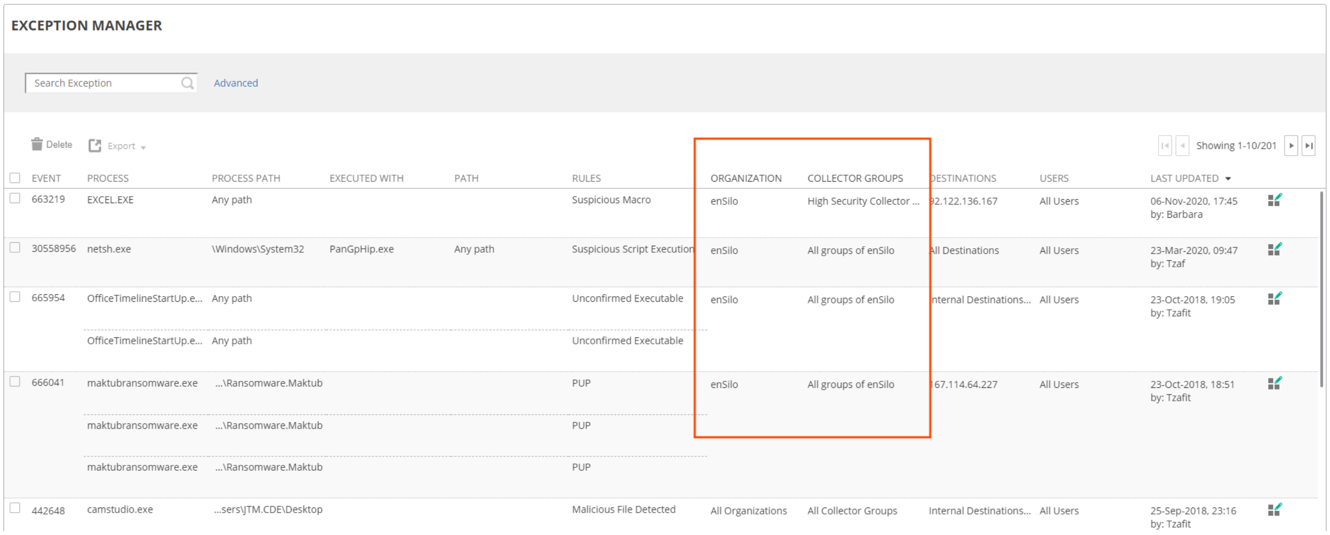
○ 92.122.136.167 ● All destinations

Users

○ ● All users

Triggered Rules:

The *Exception Manager* page also shows the organization to which the exception applies. In addition, the *Collector Groups* column indicates the Collector Groups to which the exception applies.

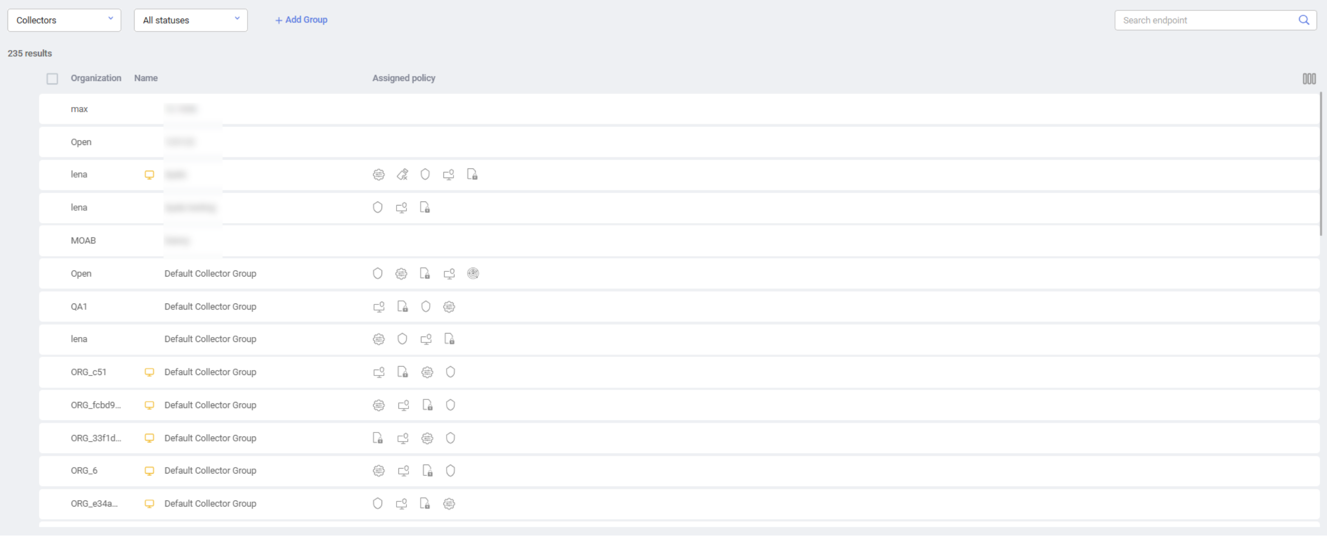


□	EVENT	PROCESS	PROCESS PATH	EXECUTED WITH	PATH	RULES	ORGANIZATION	COLLECTOR GROUPS	DESTINATIONS	USERS	LAST UPDATED
□	663219	EXCEL.EXE	Any path			Suspicious Macro	enSilo	High Security Collector ...	92.122.136.167	All Users	06-Nov-2020, 17:45 by: Barbara
□	30558956	netsh.exe	\Windows\System32	PanGpHip.exe	Any path	Suspicious Script Execution	enSilo	All groups of enSilo	All Destinations	All Users	23-Mar-2020, 09:47 by: Tzaf
□	665954	OfficeTimelineStartUp.e...	Any path			Unconfirmed Executable	enSilo	All groups of enSilo	nternal Destinations...	All Users	23-Oct-2018, 19:05 by: Tzafit
		OfficeTimelineStartUp.e...	Any path			Unconfirmed Executable					
□	666041	maktubransomware.exe	...\Ransomware.Maktub			PUP	enSilo	All groups of enSilo	167.114.64.227	All Users	23-Oct-2018, 18:51 by: Tzafit
		maktubransomware.exe	...\Ransomware.Maktub			PUP					
		maktubransomware.exe	...\Ransomware.Maktub			PUP					
□	442648	camstudio.exe	...sers\JTM.CDE\Desktop			Malicious File Detected	All Organizations	All Collector Groups	Internal Destinations...	All Users	25-Sep-2018, 23:16 by: Tzafit

Assets

Inventory page

In Hoster view, the *Assets* > *Inventory* page shows all the Collectors from all organizations.



235 results

□ Organization	Name	Assigned policy
max	[redacted]	
Open	[redacted]	
lena	[redacted]	
lena	[redacted]	
MOAB	[redacted]	
Open	Default Collector Group	
QA1	Default Collector Group	
lena	Default Collector Group	
ORG_c51	Default Collector Group	
ORG_fcbd9...	Default Collector Group	
ORG_33f1d...	Default Collector Group	
ORG_6	Default Collector Group	
ORG_e34a...	Default Collector Group	

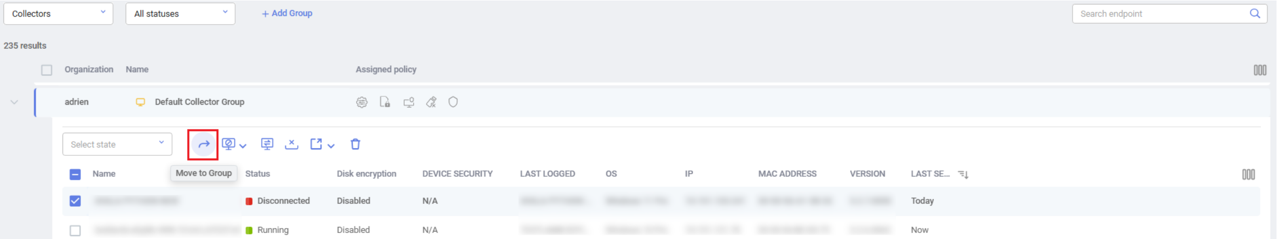
When in Hoster view, you can move Collectors between organizations using this window.

Only Collectors from 3.0 and above can be in the non-default organization. All older Collectors can only be installed in the default organization.

Only Collectors from 3.0 and above can be moved between organizations.

To move a Collector between organizations in Hoster view:

1. Check the checkbox of the Collector Group or check the checkbox(es) of one or more Collectors.

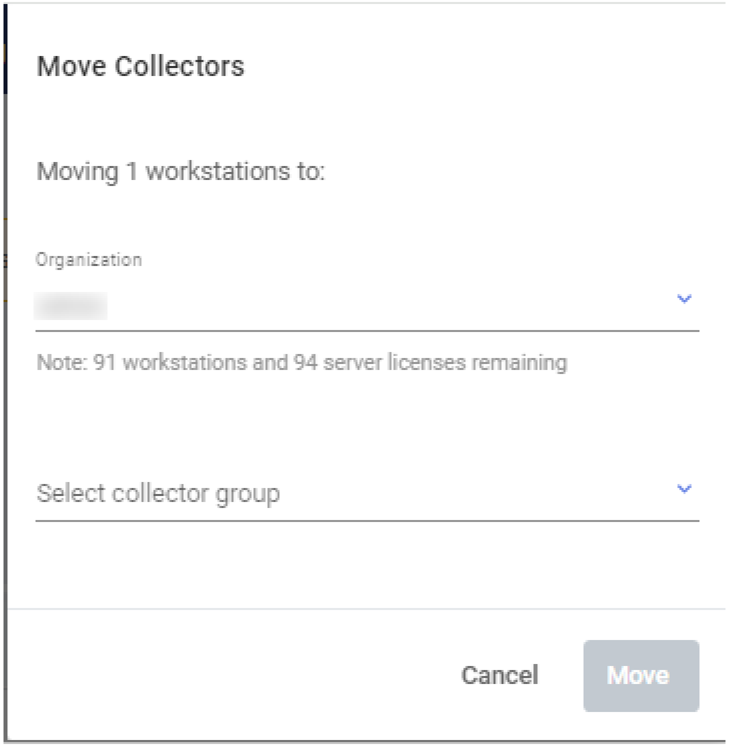


235 results

	Organization	Name	Assigned policy
□	adrien	Default Collector Group	

	Name	Status	Disk encryption	DEVICE SECURITY	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	LAST SE...
☑	[redacted]	🟥 Disconnected	Disabled	N/A	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Today
□	[redacted]	🟩 Running	Disabled	N/A	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Now

2. Click the *Move to group* button. The following window displays:



Move Collectors

Moving 1 workstations to:

Organization

[redacted]

Note: 91 workstations and 94 server licenses remaining

Select collector group

3. In the *Organization* field, select the organization to which to move the Collector(s).
4. Click *Move*.

Troubleshooting

This chapter describes how to troubleshoot various problems that you may encounter in the FortiEDR system.

For debugging and troubleshooting, Fortinet Support may request that you provide the logs for the FortiEDR devices deployed in your organization (Collectors, Cores, Aggregators). You may refer to Exporting logs on page 273 for details about how to do so.

If your system includes the Forensics add-on, you can use the Retrieve Memory function to retrieve memory related to a specific stack on a specific Collector. For more details, you may refer to Retrieving memory on page 100.

A FortiEDR Collector does not display in the INVENTORY tab

After a FortiEDR Collector is first launched, it registers with the FortiEDR Central Manager and is displayed in the *INVENTORY* tab. If it does not appear to have registered, then perform the following:

1. Check that the device on which the FortiEDR Collector is installed is powered on and has an Internet connection.
2. Validate that ports 8081 and 555 are available and that no other third-party product is blocking these ports.

No events on the FortiEDR Central Manager console

If no events are displayed in the FortiEDR Central manager console, then perform the following.

Validate that there is network connectivity between all the system components.

To do so, we recommend:

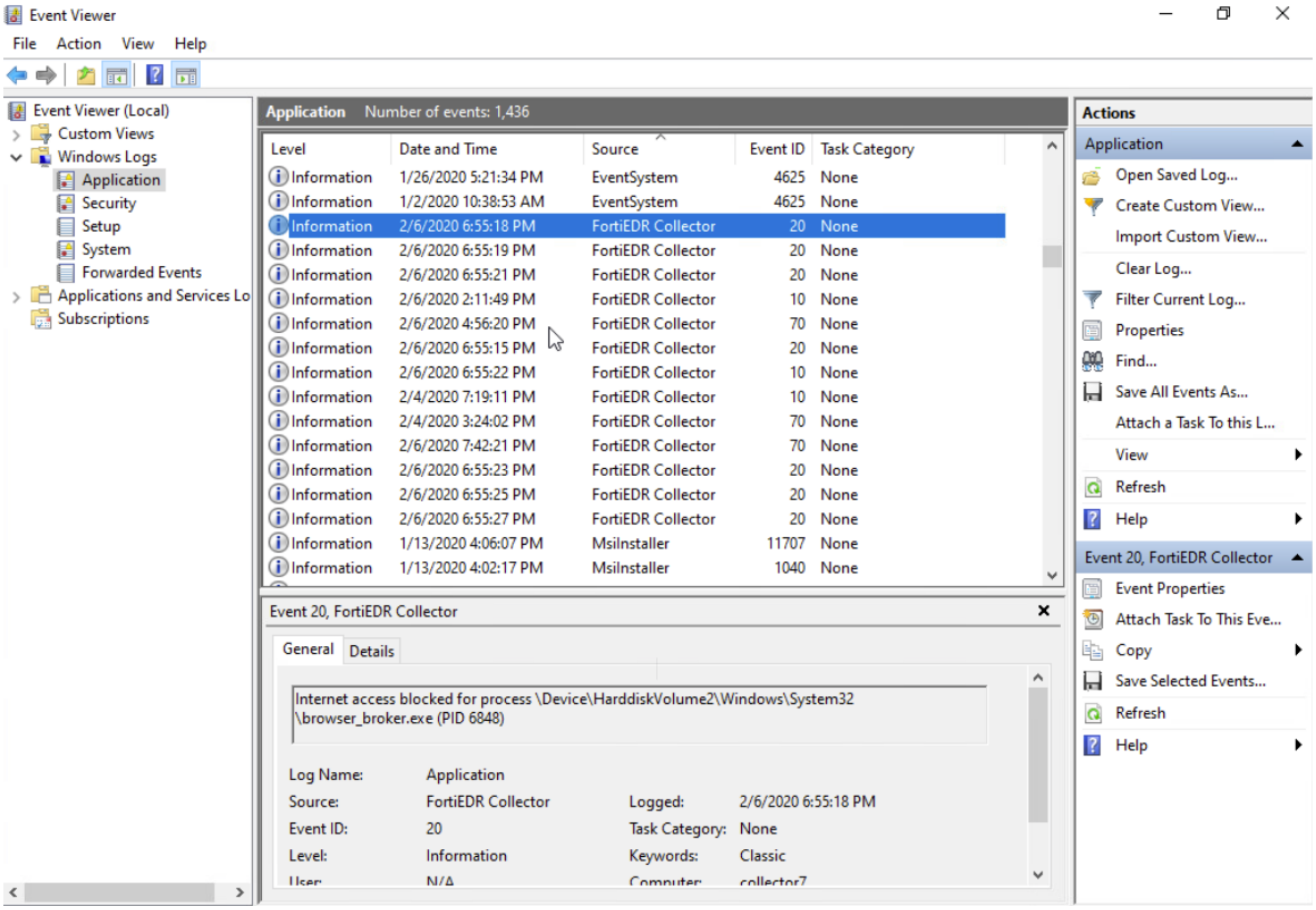
- Running Telnet on the FortiEDR Collector and connecting to the FortiEDR Core IP via port 555.
- Running Telnet on the FortiEDR Core and attempting to connect to the FortiEDR Aggregator IP on port 8081.

Make sure that Telnet is enabled on Windows.

User cannot communicate externally or files modification activity is blocked

Microsoft Windows-based devices

The Windows Event Viewer records whenever a FortiEDR Collector blocks communication from a device or file modification related to ransomware activity. This information is recorded in the Windows Event Viewer log located in the following location: *Event Viewer > Windows Logs > Application*.



Application Number of events: 1,436

Level	Date and Time	Source	Event ID	Task Category
Information	1/26/2020 5:21:34 PM	EventSystem	4625	None
Information	1/2/2020 10:38:53 AM	EventSystem	4625	None
Information	2/6/2020 6:55:18 PM	FortiEDR Collector	20	None
Information	2/6/2020 6:55:19 PM	FortiEDR Collector	20	None
Information	2/6/2020 6:55:21 PM	FortiEDR Collector	20	None
Information	2/6/2020 2:11:49 PM	FortiEDR Collector	10	None
Information	2/6/2020 4:56:20 PM	FortiEDR Collector	70	None
Information	2/6/2020 6:55:15 PM	FortiEDR Collector	20	None
Information	2/6/2020 6:55:22 PM	FortiEDR Collector	10	None
Information	2/4/2020 7:19:11 PM	FortiEDR Collector	10	None
Information	2/4/2020 3:24:02 PM	FortiEDR Collector	70	None
Information	2/6/2020 7:42:21 PM	FortiEDR Collector	70	None
Information	2/6/2020 6:55:23 PM	FortiEDR Collector	20	None
Information	2/6/2020 6:55:25 PM	FortiEDR Collector	20	None
Information	2/6/2020 6:55:27 PM	FortiEDR Collector	20	None
Information	1/13/2020 4:06:07 PM	MsiInstaller	11707	None
Information	1/13/2020 4:02:17 PM	MsiInstaller	1040	None

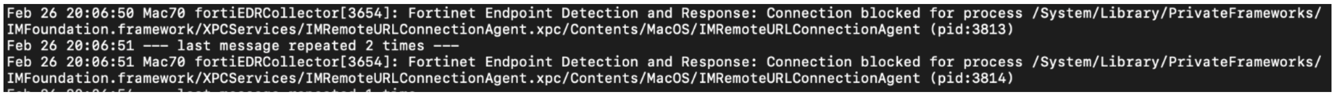
Event 20, FortiEDR Collector

Internet access blocked for process \Device\HarddiskVolume2\Windows\System32\browser_broker.exe (PID 6848)

Log Name:	Application		
Source:	FortiEDR Collector	Logged:	2/6/2020 6:55:18 PM
Event ID:	20	Task Category:	None
Level:	Information	Keywords:	Classic
User:	N/A	Computer:	collector7

macOS-based devices

The mconsole records whenever a FortiEDR Collector blocks communication from a device or file modification related to ransomware activity. This information is recorded in the macOS console log located in the following location: *Applications > Utilities > Console > All Messages*, as shown below:

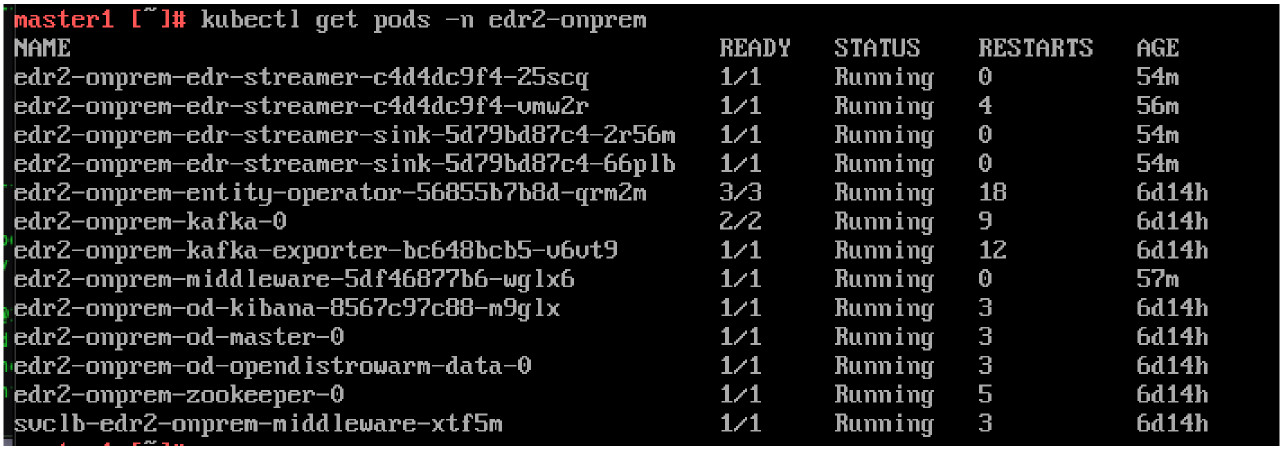


```
Feb 26 20:06:50 Mac70 fortiEDRCollector[3654]: Fortinet Endpoint Detection and Response: Connection blocked for process /System/Library/PrivateFrameworks/
IMFoundation.framework/XPCServices/IMRemoteURLConnectionAgent.xpc/Contents/MacOS/IMRemoteURLConnectionAgent (pid:3813)
Feb 26 20:06:51 --- last message repeated 2 times ---
Feb 26 20:06:51 Mac70 fortiEDRCollector[3654]: Fortinet Endpoint Detection and Response: Connection blocked for process /System/Library/PrivateFrameworks/
IMFoundation.framework/XPCServices/IMRemoteURLConnectionAgent.xpc/Contents/MacOS/IMRemoteURLConnectionAgent (pid:3814)
```

Threat Hunting tab does not show expected activity events

If the Threat Hunting tab does not show expected activity events after installation, perform the following troubleshooting steps:

1. Check which Collectors group the triggering device belongs to.
2. Check the Threat Hunting Collection profile assigned to this group and make sure the profile includes the activity events you are searching for in the Threat Hunting tab.
3. If the profile includes the activity events but the Threat Hunting tab still does not show them, check the installation status of the Threat Hunting repository by running the `kubectl get pods -n edr2-onprem` command in the Threat Hunting repository console.
4. Verify the status is *Running* for all entries. See example below. Otherwise, reinstall the Threat Hunting repository.



```
master1 [~]# kubectl get pods -n edr2-onprem
NAME                                          READY   STATUS    RESTARTS   AGE
edr2-onprem-edr-streamer-c4d4dc9f4-25scq      1/1     Running   0          54m
edr2-onprem-edr-streamer-c4d4dc9f4-vmw2r      1/1     Running   4          56m
edr2-onprem-edr-streamer-sink-5d79bd87c4-2r56m 1/1    Running   0          54m
edr2-onprem-edr-streamer-sink-5d79bd87c4-66plb 1/1    Running   0          54m
edr2-onprem-entity-operator-56855b7b8d-qrm2m  3/3     Running   18         6d14h
edr2-onprem-kafka-0                           2/2     Running   9          6d14h
edr2-onprem-kafka-exporter-bc648bcb5-v6vt9    1/1     Running   12         6d14h
edr2-onprem-middleware-5df46877b6-wglx6       1/1     Running   0          57m
edr2-onprem-od-kibana-8567c97c88-m9glx        1/1     Running   3          6d14h
edr2-onprem-od-master-0                       1/1     Running   3          6d14h
edr2-onprem-od-opendistrowarm-data-0          1/1     Running   3          6d14h
edr2-onprem-zookeeper-0                       1/1     Running   5          6d14h
svclb-edr2-onprem-middleware-xtf5m            1/1     Running   3          6d14h
```

Collector is slow or hangs

If an endpoint is slow or hangs, check the Collector logs. It might be caused by collision with another AV product that FortiEDR is running in parallel with. You can fix the collision by excluding AV exceptions in both FortiEDR and the other AV product.

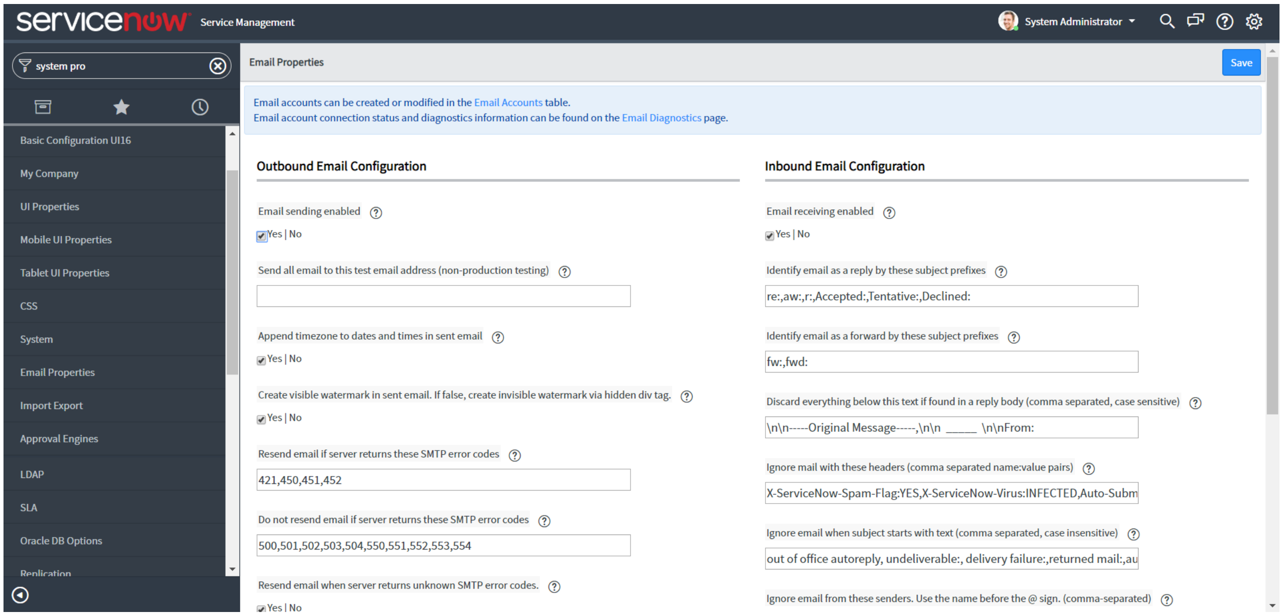
Appendix A – Setting up an email feed for open ticket

The Open Ticket feature enables you to send events to an event-management tool such as Jira or ServiceNow.

In order for the Open Ticket feature to work properly, you must set up a receiving email feed in the event-management tool to be used. This appendix provides an example that describes how to set up the required email feed in ServiceNow.

To set up an email feed in ServiceNow:

1. Launch ServiceNow.
2. In the window that opens, select *System Properties > Email Properties*. The following window displays:



Email Properties

Email accounts can be created or modified in the Email Accounts table.
Email account connection status and diagnostics information can be found on the Email Diagnostics page.

Outbound Email Configuration

Email sending enabled
☑ Yes | No

Send all email to this test email address (non-production testing)

Append timezone to dates and times in sent email
☑ Yes | No

Create visible watermark in sent email. If false, create invisible watermark via hidden div tag.
☑ Yes | No

Resend email if server returns these SMTP error codes
421,450,451,452

Do not resend email if server returns these SMTP error codes
500,501,502,503,504,550,551,552,553,554

Resend email when server returns unknown SMTP error codes.
☑ Yes | No

Inbound Email Configuration

Email receiving enabled
☑ Yes | No

Identify email as a reply by these subject prefixes
re:,aw:,r:,Accepted:,Tentative:,Declined:

Identify email as a forward by these subject prefixes
fw:,fwd:

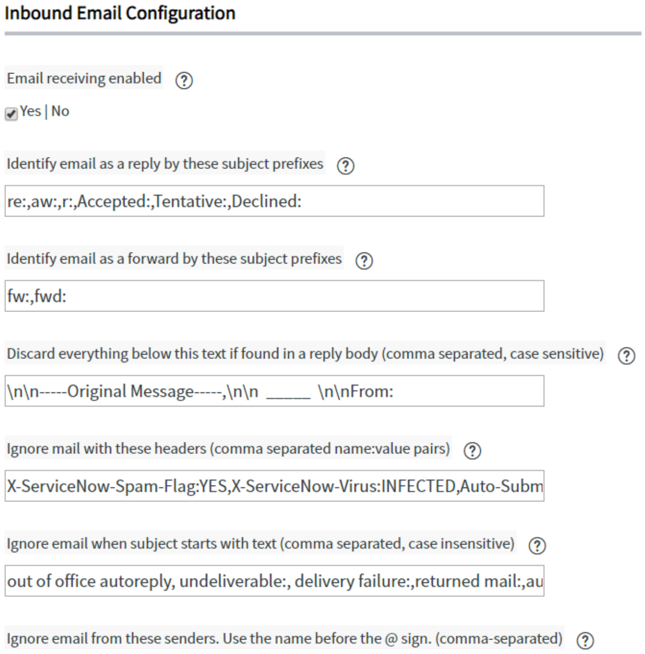
Discard everything below this text if found in a reply body (comma separated, case sensitive)
\n\n-----Original Message-----,\n\n _____ \n\nFrom:

Ignore mail with these headers (comma separated name:value pairs)
X-ServiceNow-Spam-Flag:YES,X-ServiceNow-Virus:INFECTED,Auto-Subm

Ignore email when subject starts with text (comma separated, case insensitive)
out of office autoreply, undeliverable:, delivery failure:,returned mail:,au

Ignore email from these senders. Use the name before the @ sign. (comma-separated)

3. In the *Inbound Email Configuration* area, check the *Email receiving enabled* checkbox.



Inbound Email Configuration

Email receiving enabled ?

☑ Yes | No

Identify email as a reply by these subject prefixes ?

re:,aw:,r:,Accepted:,Tentative:,Declined:

Identify email as a forward by these subject prefixes ?

fw:,fwd:

Discard everything below this text if found in a reply body (comma separated, case sensitive) ?

\n\n-----Original Message-----,\n\n _____ \n\nFrom:

Ignore mail with these headers (comma separated name:value pairs) ?

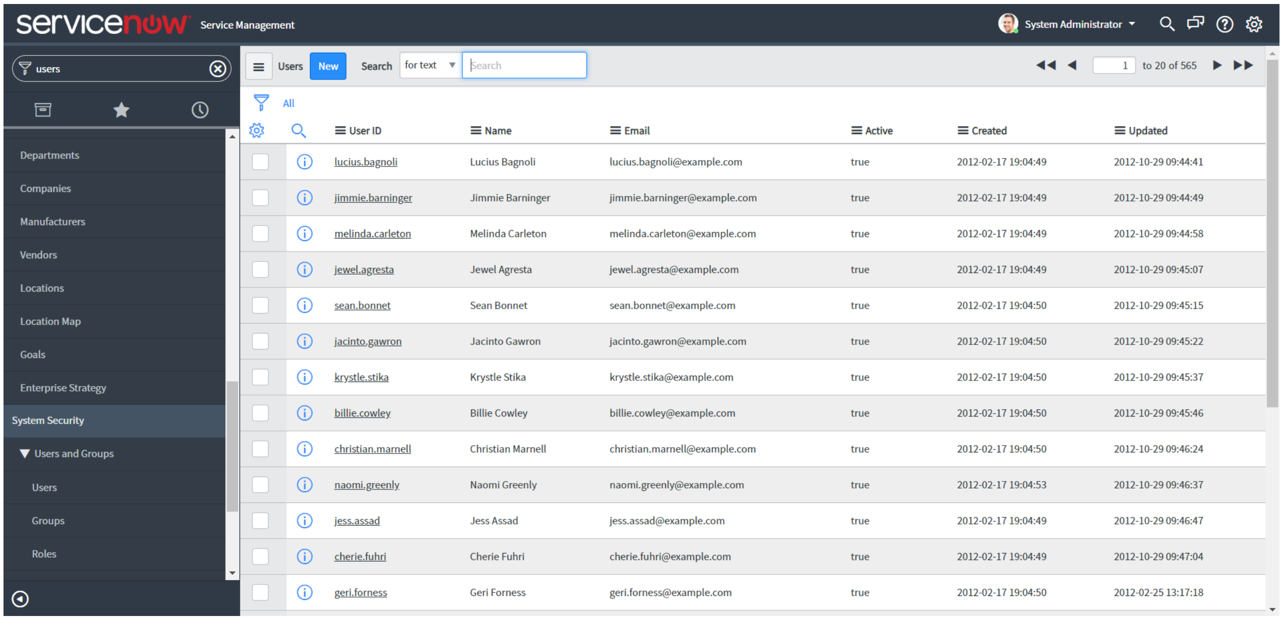
X-ServiceNow-Spam-Flag:YES,X-ServiceNow-Virus:INFECTED,Auto-Subm

Ignore email when subject starts with text (comma separated, case insensitive) ?

out of office autoreply, undeliverable:, delivery failure:,returned mail:,au

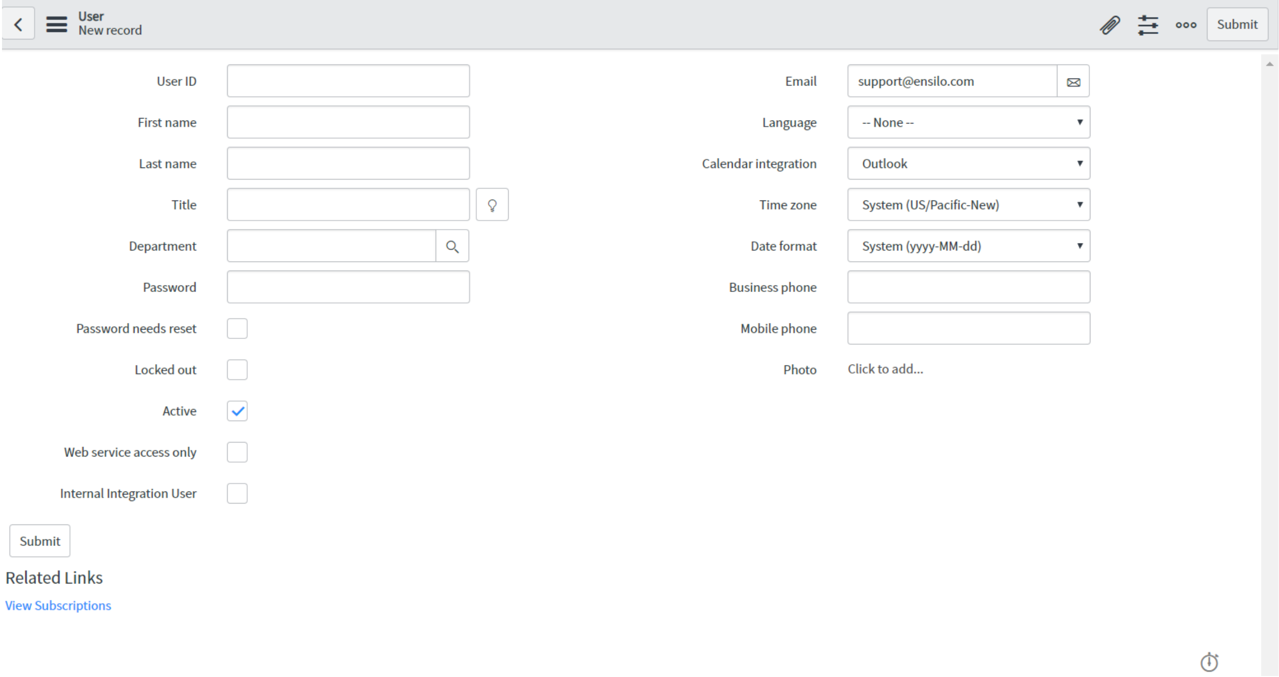
Ignore email from these senders. Use the name before the @ sign. (comma-separated) ?

4. In the left pane, select *System Security* > *Users and Groups* > *Users*. The following window displays:



User ID	Name	Email	Active	Created	Updated
lucius.bagnoli	Lucius Bagnoli	lucius.bagnoli@example.com	true	2012-02-17 19:04:49	2012-10-29 09:44:41
jimmie.barninger	Jimmie Barninger	jimmie.barninger@example.com	true	2012-02-17 19:04:49	2012-10-29 09:44:49
melinda.carleton	Melinda Carleton	melinda.carleton@example.com	true	2012-02-17 19:04:49	2012-10-29 09:44:58
jewel.agresta	Jewel Agresta	jewel.agresta@example.com	true	2012-02-17 19:04:49	2012-10-29 09:45:07
sean.bonnet	Sean Bonnet	sean.bonnet@example.com	true	2012-02-17 19:04:50	2012-10-29 09:45:15
jacinto.gawron	Jacinto Gawron	jacinto.gawron@example.com	true	2012-02-17 19:04:50	2012-10-29 09:45:22
krystle.stika	Krystle Stika	krystle.stika@example.com	true	2012-02-17 19:04:50	2012-10-29 09:45:37
billie.cowley	Billie Cowley	billie.cowley@example.com	true	2012-02-17 19:04:50	2012-10-29 09:45:46
christian.marnell	Christian Marnell	christian.marnell@example.com	true	2012-02-17 19:04:50	2012-10-29 09:46:24
naomi.greenly	Naomi Greenly	naomi.greenly@example.com	true	2012-02-17 19:04:53	2012-10-29 09:46:37
jess.assad	Jess Assad	jess.assad@example.com	true	2012-02-17 19:04:49	2012-10-29 09:46:47
cherie.fuhri	Cherie Fuhri	cherie.fuhri@example.com	true	2012-02-17 19:04:49	2012-10-29 09:47:04
geri.forness	Geri Forness	geri.forness@example.com	true	2012-02-17 19:04:50	2012-02-25 13:17:18

5. Click the *New* button to create a new user. The following window displays:



User
New record

User ID	
First name	
Last name	
Title	
Department	
Password	
Password needs reset	□
Locked out	□
Active	☑
Web service access only	□
Internal Integration User	□

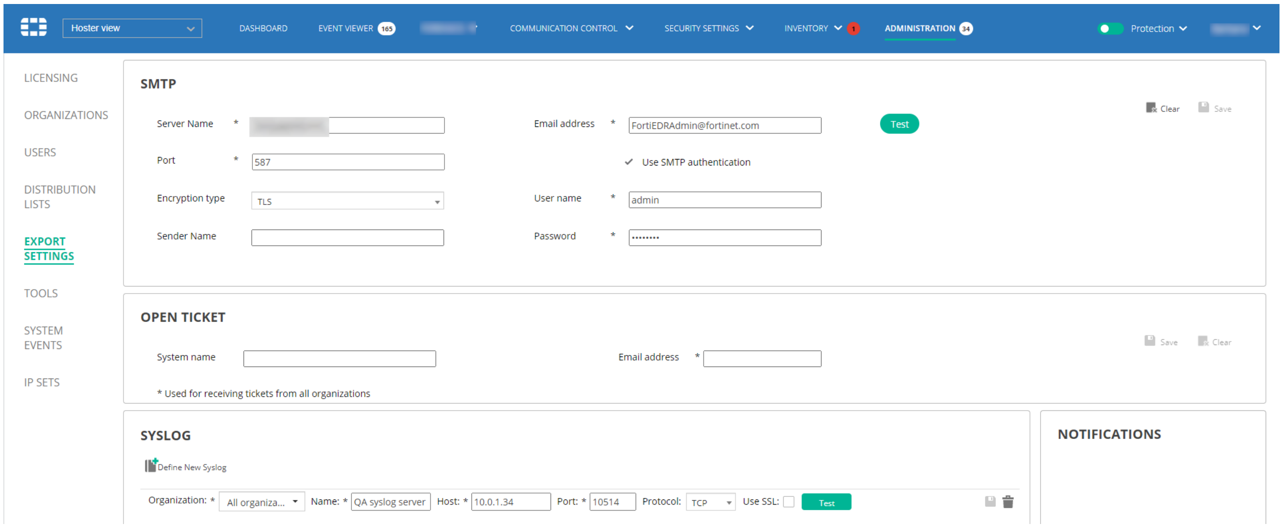
Email	support@ensilo.com
Language	-- None --
Calendar integration	Outlook
Time zone	System (US/Pacific-New)
Date format	System (yyyy-MM-dd)
Business phone	
Mobile phone	
Photo	Click to add...

Submit

Related Links

View Subscriptions

6. In the *Email* field, enter the email address of the FortiEDR messaging system. This email address is specified in the *Email Address* field of the FortiEDR Open Ticket settings, which can be accessed by selecting *Administration > Export Settings* in the FortiEDR user interface, as shown below:



SMTP

Server Name *	[redacted]
Port *	587
Encryption type	TLS
Sender Name	
Email address *	FortiEDRAdmin@fortinet.com
✓ Use SMTP authentication	
User name *	admin
Password *	••••••••

OPEN TICKET

System name	
Email address *	

* Used for receiving tickets from all organizations

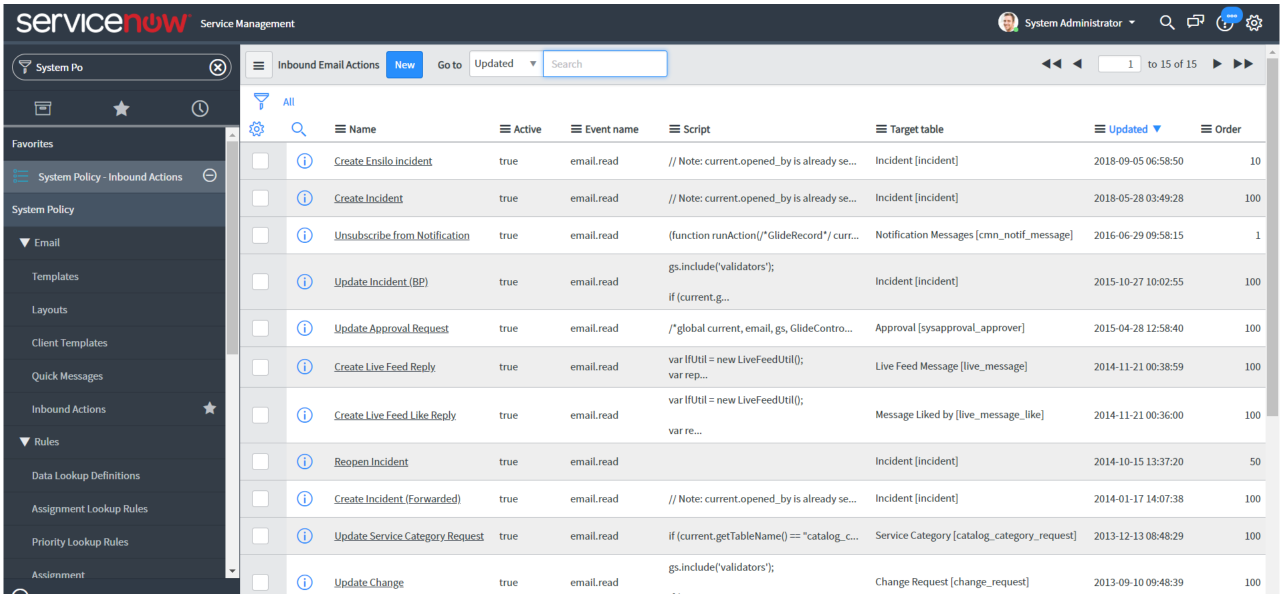
SYSLOG

Define New Syslog

Organization: * All organiza... Name: * QA syslog server Host: * 10.0.1.34 Port: * 10514 Protocol: TCP Use SSL: □

NOTIFICATIONS

7. In the left pane, select *System Policy > Email > Inboun Actions*. The following window displays:

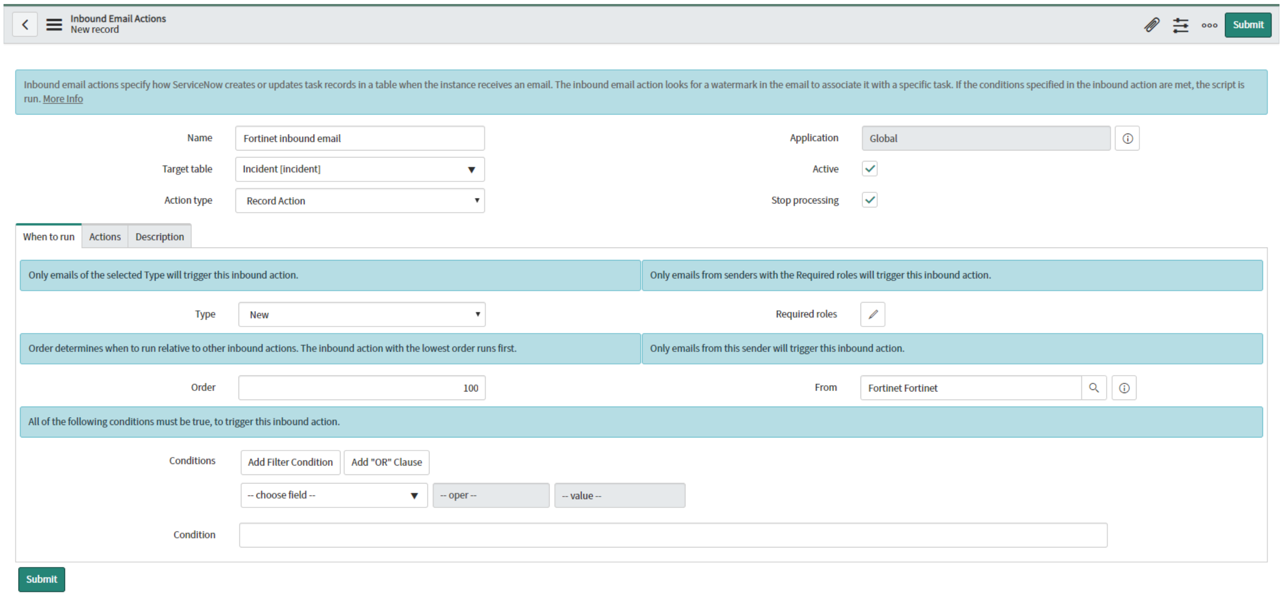


Name	Active	Event name	Script	Target table	Updated	Order
Create Ensilo incident	true	email.read	// Note: current.opened_by is already se...	Incident [incident]	2018-09-05 06:58:50	10
Create Incident	true	email.read	// Note: current.opened_by is already se...	Incident [incident]	2018-05-28 03:49:28	100
Unsubscribe from Notification	true	email.read	(function runAction(/*GlideRecord*/ curr...	Notification Messages [cmn_notif_message]	2016-06-29 09:58:15	1

Update Incident (BP)	true	email.read	gs.include('validators');
			if (current.g...
				Incident [incident]	2015-10-27 10:02:55	100

Update Approval Request	true	email.read	/*global current, email, gs, GlideContro...	Approval [sysapproval_approver]	2015-04-28 12:58:40	100
Create Live Feed Reply	true	email.read	var lfUtil = new LiveFeedUtil(); var rep...	Live Feed Message [live_message]	2014-11-21 00:38:59	100
Create Live Feed Like Reply	true	email.read	var lfUtil = new LiveFeedUtil(); var re...	Message Liked by [live_message_like]	2014-11-21 00:36:00	100
Reopen Incident	true	email.read		Incident [incident]	2014-10-15 13:37:20	50
Create Incident (Forwarded)	true	email.read	// Note: current.opened_by is already se...	Incident [incident]	2014-01-17 14:07:38	100
Update Service Category Request	true	email.read	if (current.getTableName() == "catalog_c...	Service Category [catalog_category_request]	2013-12-13 08:48:29	100
Update Change	true	email.read	gs.include('validators');	Change Request [change_request]	2013-09-10 09:48:39	100

8. Click the *New* blue button to create new inbound email actions. The following window displays:



Inbound email actions specify how ServiceNow creates or updates task records in a table when the instance receives an email. The inbound email action looks for a watermark in the email to associate it with a specific task. If the conditions specified in the inbound action are met, the script is run. More Info

Name	Fortinet inbound email	Application	Global
Target table	Incident [incident]	Active	☑
Action type	Record Action	Stop processing	☑

Only emails of the selected Type will trigger this inbound action.

Only emails from senders with the Required roles will trigger this inbound action.

Type: New

Required roles:

Order determines when to run relative to other inbound actions. The inbound action with the lowest order runs first.

Only emails from this sender will trigger this inbound action.

Order: 100

From: Fortinet Fortinet

All of the following conditions must be true, to trigger this inbound action.

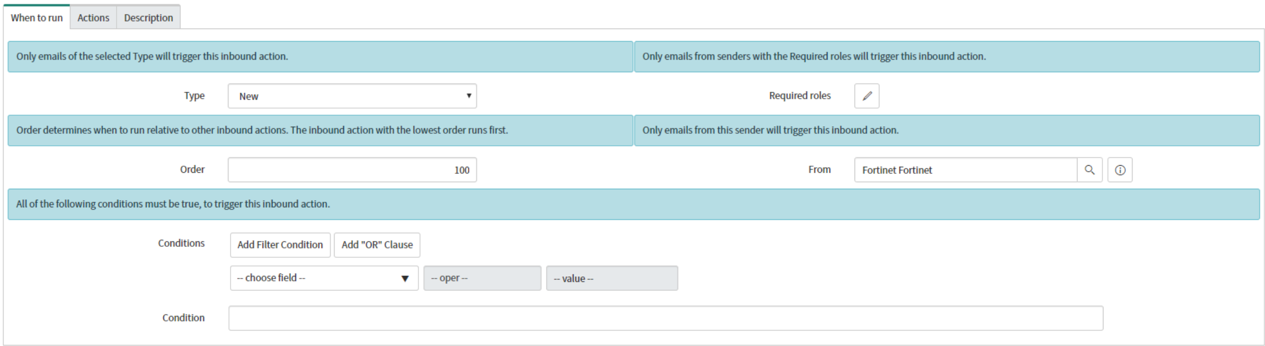
Conditions

Condition

9. Fill in the following fields in this window:

Field	Definition
Name	Enter a free-text name for the inbound email feed. For example, `Fortinet inbound email`.
Target table	Select *Incident [incident]* in the dropdown list.
Action type	Select *Record Action* in the dropdown list.
Active	Check this checkbox to select it.
Stop Processing	Check this checkbox to select it.

10. In this window, select the *When to run* tab and then in the *From* field, select the FortiEDR user created in step 6.



Only emails of the selected Type will trigger this inbound action.

Only emails from senders with the Required roles will trigger this inbound action.

Type: New

Required roles

Order determines when to run relative to other inbound actions. The inbound action with the lowest order runs first.

Only emails from this sender will trigger this inbound action.

Order: 100

From: Fortinet Fortinet

All of the following conditions must be true, to trigger this inbound action.

Conditions: -- choose field -- | -- oper -- | -- value --

Condition:

11. Select the *Actions* tab and then paste the provided JavaScript (see below) into the email body. You can modify this script, as needed.

```
//  Note: current.opened_by is already set to the first UserID that matches the From: email
address

current.caller_id = gs.getUserID();

current.comments = “received from: “ + email.origemail + “\n\n” + email.body_text;

current.short_description = email.subject;

current.category = “request”;

current.incident_state = 1;

current.notify = 2;

current.contact_type = “email”;


//set highest priority for emails from FortiEDR notification

if (email.origemail == "doNotReply@fortinet.com") {

    current.impact=1;


    current.urgency=1;

}


if (email.body.assign != undefined)

    current.assigned_to = email.body.assign;
```

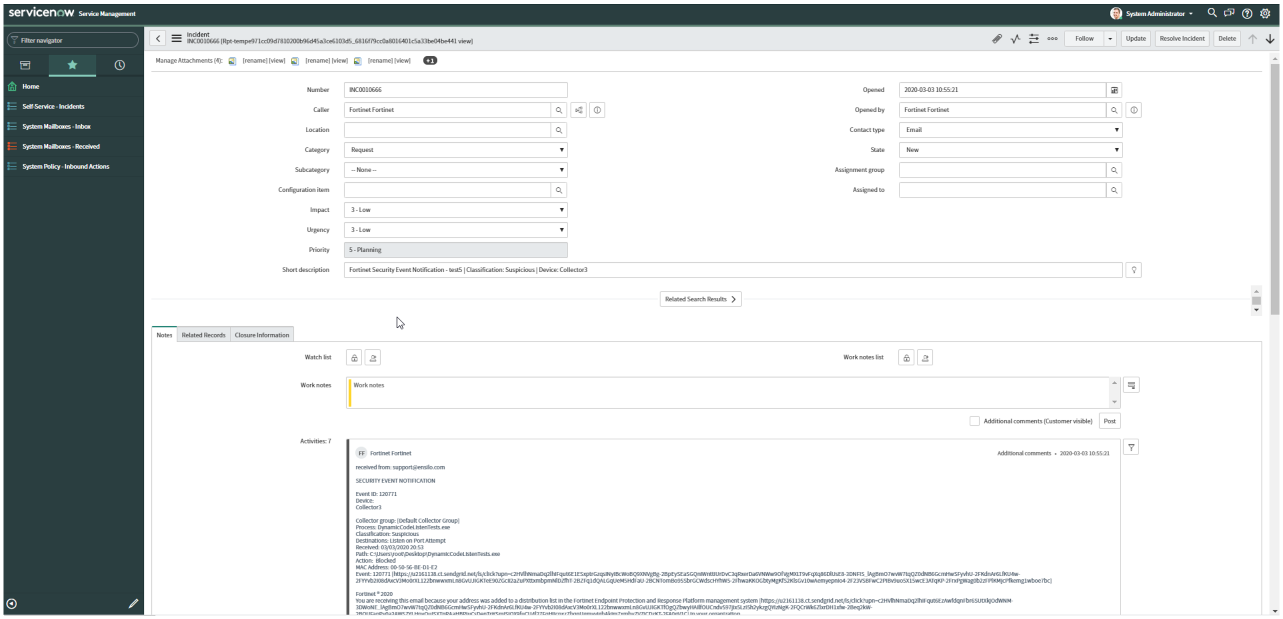
```
if (email.importance != undefined) {

    if (email.importance.toLowerCase() == "high")

        current.priority = 1;

}


if (email.body.priority != undefined)

    current.priority = email.body.priority;

//parsing fields from message body example

var severityStart = email.body_text.indexOf('Severity:') + 9;

var classificationStart = email.body_text.indexOf('Classification:') + 15;

var destinitionStart = email.body_text.indexOf('Destinations:');


var severity = email.body_text.slice(severityStart, classificationStart -15 );

var classification = email.body_text.slice(classificationStart, destinitionStart);

 current.insert();
```

12. When pasting in the JavaScript, make sure that:
    - The emails address on line 11(see above) is the same as that specified in Email Address field of the FortiEDR Open Ticket settings (see step 6).
    - You set the *current.impact* and *current.urgency* fields on lines 12 and 14 to specify the impact and urgency values for ServiceNow.
      Various types of information can be extracted from the email sent by FortiEDR. For example, the text on line 33 in the JavaScript (see above) is an example of how to extract the classification value of this event from the email.
13. Click the *Submit* button in the ServiceNow window. This completes the email feed setup.
    When FortiEDR sends an email to ServiceNow, a JSON file is attached to it. This JSON file contains the raw data for the event. Once received, you should save this raw data to the ticket.
    The following shows a sample JSON file:

```
//parsing fields from attachment example

if (sys_email.hasAttachments()){

    var att = new GlideRecord("sys_attachment");

    att.addEncodedQuery("table_name=sys_email^table_sys_id=" + sys_email.getValue("sys_
id"));
```

```
        att.query();

        while (att.next()){

            if (att.file_name == "event.json" ) {

                var sa = new GlideSysAttachment();


                var binData = sa.getBytes(att);

                var strData = Packages.java.lang.String(binData);

                var parser = new JSONParser();

                var parsed = parser.parse(strData);

                current.comments =("EventId from JSON: " + parsed.EventId);

                }

        }

    }
```

The following shows how an event appears when received in ServiceNow, after being sent from FortiEDR:



Incident
INC0010666 [Rpt-tempe971cc09d7810200b96d45a3ce6103d5_6816f79cc0a8016401c5a33be04be441 view]

Manage Attachments (4): [rename] [view] [rename] [view] [rename] [view] +1

Number	INC0010666	Opened	2020-03-03 10:55:21
Caller	Fortinet Fortinet	Opened by	Fortinet Fortinet
Location		Contact type	Email
Category	Request	State	New
Subcategory	-- None --	Assignment group	
Configuration item		Assigned to	
Impact	3 - Low		
Urgency	3 - Low		
Priority	5 - Planning		
Short description	Fortinet Security Event Notification - test5 | Classification: Suspicious | Device: Collector3		

Work notes: Work notes

□ Additional comments (Customer visible)

Activities: 7

FF Fortinet Fortinet — Additional comments • 2020-03-03 10:55:21

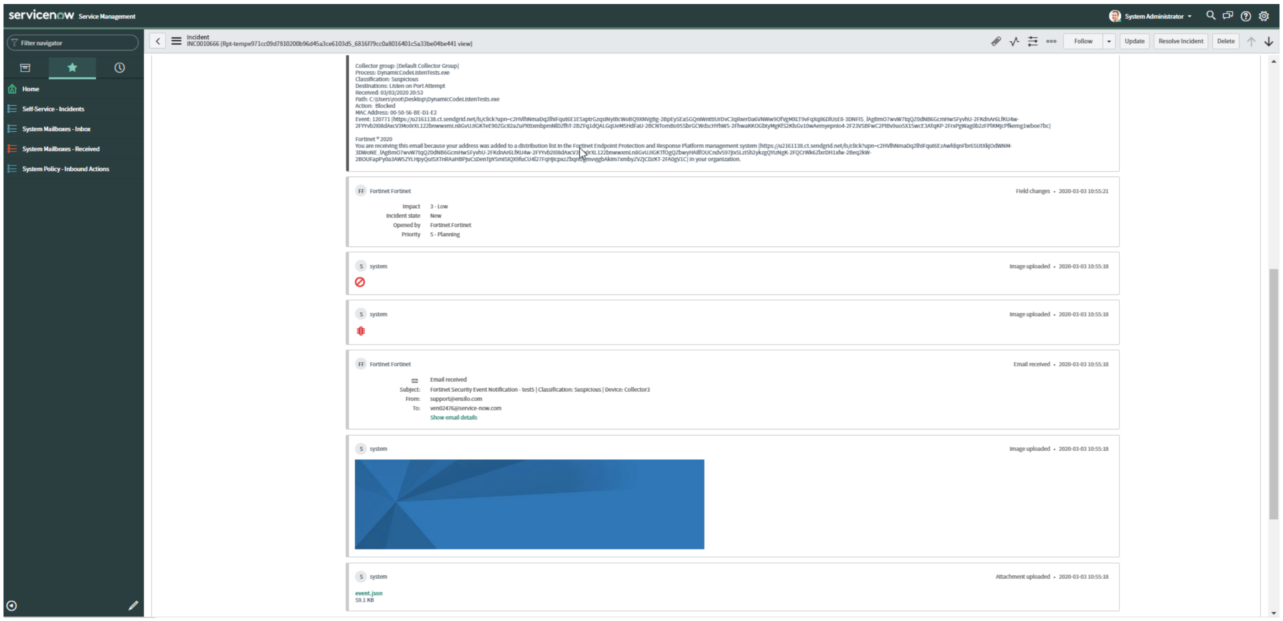
received from: support@ensilo.com

SECURITY EVENT NOTIFICATION

Event ID: 120771
Device:
Collector3

Collector group: [Default Collector Group]
Process: DynamicCodeListenTests.exe
Classification: Suspicious
Destinations: Listen on Port Attempt
Received: 03/03/2020 20:53
Path: C:\Users\root\Desktop\DynamicCodeListenTests.exe
Action: Blocked
MAC Address: 00-50-56-BE-D1-E2
Event: 120771 [https://u2161138.ct.sendgrid.net/ls/click?upn=c2HVlhNmaDq2lhIFqut6E1ESxptrGzqsINyIBcWoBQ9XNVgBg-2BpEySEaSGQnIWnttIUrDvC3qRxerDa6VNWw9OfVgMXLT9vFqXq86DlUsE8-3DNFIS_lAgBmO7wvW7tqQZ0dNB6GcmHwSFyvhU-2FKdnAr6LfKU4w-2FYYvb2I08dAxcV3Mo0rXL122bnwwxmLn8GvUJIGKTeE90ZGcII2aZuPXttxmbpmNlDZfhT-2BZFq1dQALGqUeM5HdFaU-2BCNTomBo95SbrGCWdscHYhW5-2FhwaKKOGbtyMgKfS2KlsGv10wAemyepnIo4-2F23VSBFwC2PIBv9uo5X15wcE3ATqKP-2FrxPgWag0b2zFPlKMJcPfkemg1wboe7bc]

Fortinet ® 2020
You are receiving this email because your address was added to a distribution list in the Fortinet Endpoint Protection and Response Platform management system [https://u2161138.ct.sendgrid.net/ls/click?upn=c2HVlhNmaDq2lhIFqut6EzAwfdqnFbr6SUtXkjOdWNM-3DWoNE_lAgBmO7wvW7tqQZ0dNB6GcmHwSFyvhU-2FKdnAr6LfKU4w-2FYYvb2I08dAxcV3Mo0rXL122bnwwxmLn8GvUJIGKTfOgQZbwyHAllfOUCndv597JIx5LzI5h2ykzgQYIzNgK-2FQCrWk6ZlxrDH1xfw-2Beq2kW-2BQUFanPv0a2AW5ZYLHnvQuISXTnPAaHBPluCsDenTnYSmISIQX9fuCU4l27FqHIlcnxzZbqnUgmvyighAkIm7xmbvZVZICDzKT-2FA0qV1C] in your organization.



Incident
INC0010666 [Rpt-tempe971cc09d7810200b96d45a3ce6103d5_6816f79cc0a8016401c5a33be04be441 view]

Collector group: [Default Collector Group]
Process: DynamicCodeListenTests.exe
Classification: Suspicious
Destinations: Listen on Port Attempt
Received: 03/03/2020 20:53
Path: C:\Users\root\Desktop\DynamicCodeListenTests.exe
Action: Blocked
MAC Address: 00-50-56-BE-D1-E2
Event: 120771 [https://u2161138.ct.sendgrid.net/ls/click?upn=c2HVlhNmaDq2lhIFqut6E1ESxptrGzqsINyIBcWoBQ9XNVgBg-2BpEySEaSGQnIWnttIUrDvC3qRxerDa6VNWw9OfVgMXLT9vFqXq86DlUsE8-3DNFIS_lAgBmO7wvW7tqQZ0dNB6GcmHwSFyvhU-2FKdnAr6LfKU4w-2FYYvb2I08dAxcV3Mo0rXL122bnwwxmLn8GvUJIGKTeE90ZGcII2aZuPXttxmbpmNlDZfhT-2BZFq1dQALGqUeM5HdFaU-2BCNTomBo95SbrGCWdscHYhW5-2FhwaKKOGbtyMgKfS2KlsGv10wAemyepnIo4-2F23VSBFwC2PIBv9uo5X15wcE3ATqKP-2FrxPgWag0b2zFPlKMJcPfkemg1wboe7bc]

Fortinet ® 2020
You are receiving this email because your address was added to a distribution list in the Fortinet Endpoint Protection and Response Platform management system [https://u2161138.ct.sendgrid.net/ls/click?upn=c2HVlhNmaDq2lhIFqut6EzAwfdqnFbr6SUtXkjOdWNM-3DWoNE_lAgBmO7wvW7tqQZ0dNB6GcmHwSFyvhU-2FKdnAr6LfKU4w-2FYYvb2I08dAxcV3Mo0rXL122bnwwxmLn8GvUJIGKTfOgQZbwyHAllfOUCndv597Jlx5Lzl5h2ykzgQYIzNgK-2FQCrWk6ZlxrDH1xfw-2Beq2kW-2BOUFapPy0a3AW5ZYLHpyQuISXTnRAaHBPJuCsDenTpYSmISIQX9fuCU4l27FqHjIcpxzZbqnUgmvvjgbAkim7xmbyZVZJCDzKT-2FA0gV1C] in your organization.

FF Fortinet Fortinet — Field changes • 2020-03-03 10:55:21

Impact	3 - Low
Incident state	New
Opened by	Fortinet Fortinet
Priority	5 - Planning

S system — Image uploaded • 2020-03-03 10:55:18

S system — Image uploaded • 2020-03-03 10:55:18

FF Fortinet Fortinet — Email received • 2020-03-03 10:55:18

✉	Email received
Subject:	Fortinet Security Event Notification - test5 | Classification: Suspicious | Device: Collector3
From:	support@ensilo.com
To:	ven02476@service-now.com
	Show email details

S system — Image uploaded • 2020-03-03 10:55:18

S system — Attachment uploaded • 2020-03-03 10:55:18

event.json
59.1 KB

Appendix B - Lucene syntax

The FortiEDR Threat Hunting free-text query is based on Lucene syntax. This syntax consists of terms and operators, as described below. For more details about the use of this query, see Threat Hunting on page 125.

You can convert JSON and XML syntax queries into Lucene syntax using the built-in *Convert Query* button in the *Free-text Query* filter.

Terms

A *free-text term* is a single word (for example NetworkService or CryptSvc) or a phrase surrounded by double quotes (for example, ”NetworkService -p -s CryptSvc”) that searches for all the words in a phrase (in the same order) regardless of the field in which the words appear.

A *Field: Value* term is a combination of a field and a value.

A list of available fields is provided in the query box, which is an automatically-complete dropdown list.

Examples

Where the Source command line contains the value NetworkService:

```
Source.CommandLine: NetworkService
```

Where the value of the remote IP is 10.151.121.130:

```
RemoteIP: 10.151.121.130
```

Operators

Operators enable you to customize the search and/or to create more complex queries.

Operators are case insensitive.

Operators	Definition
OR , ||	The query should match either one of the terms/values.
AND, &&	The query should match both of the terms/values.

Operators	Definition
NOT, !	The query should not match the term/value.
exists	The query should match when the field value is not null.
+ –	The term following this operator must be present.
•	The term following this operator must not be present.

Example

Where the Event includes either the RemoteIP field that contains 10.151.121.130 or the Remote Port field that contains 443

```
RemoteIP: 10.151.121.130 OR RemotePort: 443
```

Where the ProductName field contains both Microsoft and Windows

```
Source.Process.File.ProductName: (microsoft AND windows){}
```

Where the ProductName field contains Microsoft and does not include Windows

```
Source.File.ProductName: (microsoft -windows)
```

Where the Product Name field contains the exact phrase “Microsoft Windows”

```
Source.Process.File.ProductName: microsoft\ windows
```

Where the field Behavior has any non-null value

```
_exists_: Behavior
```

Where the field PID does not include the value 5292

```
Source.PID: (NOT 5292)
```

Where the Event does not include the value 5292 in any of the Event fields

```
NOT 5292
```

Wildcards

Wildcard searches can be run on individual terms using a **?** (question mark) to replace a single character, and an ***** (asterisk) to replace zero or more characters. For example: `Progr?m Fil*`.

If the value contains a space, escape it with a backslash. For example:

- `Source.Process.File.Path: Program\ Files*`
- `Source.Process.CompanyName: Microsoft\ Corporation`

Do not enclose wildcard search values with double quotes.

Wildcard queries may consume huge amounts of memory and perform poorly.

Ranges

Ranges can be specified for date, numeric or string fields. The inclusive ranges are specified with square brackets

[min TO max] and exclusive ranges with curly brackets {min TO max}.

Numbers 1..5

```
count:[1 TO 5]
```

Numbers from 10 upwards

```
count:[10 TO *]
```

Dates before 2012

```
date:{* TO 2012-01-01}
```

Ranges of IPs

```
RemoteIP: "140.100.100.0/24"
```

Reserved characters

Should you need to use any of the characters that function as operators in the query itself (and not as operators), then you should escape them with a leading backslash (\). For instance, to search for *c:\Windows\*, write the query as *c\:\\Windows\\*.

Reserved characters are +,-, =, &&, ||, >, <, !, ( ), { }, [ ], ^, ", ~, *, ?, :, \ and /.

Appendix C – ON PREMISE DEPLOYMENTS

This chapter describes how to set up the FortiEDR backend components for on-premise deployments. Before you start, make sure that on-premise deployment is the most suitable option for you.

System requirements

The following tables lists the system requirements of each backend component. Make sure that all devices, workstations, virtual machines and servers on which a FortiEDR backend component will be installed comply with those requirements.

Component	Central Manager	Aggregator[1]	Threat Hunting Repository	Core[2]	Reputation Server
Processor	Intel or AMD x86 (64-bit)				
Number of CPUs	4	4	Varies by number of seats and period of required Threat Hunting data retention. Refer to the Threat Hunting Repository CPU, Physical Memory, and Disk Space Requirements on page 463 section for requirements for one month of data retention for the extensive profile.	• 4 for Core • 2 for Core running as a Jumpbox 💡 The following CPUs are unsupported: • E5-2440 • E5-2650 • E5-2660 • E5-2690 • E5-2699	4
Physical Memory	16 GB	16 GB		• 16 GB for Core • 8 GB for Core running as a Jumpbox	16 GB
Disk Space	150 GB, SSD	80 GB		• 250 GB SSD for Core • 50 GB (non-SSD) for Core running as a Jumpbox	120 GB

Component	Central Manager	Aggregator[1]	Threat Hunting Repository	Core[2]	Reputation Server
				For a Threat Hunting license, each 1000 additional Collectors above the first 1000 require an additional 45 GB of disk space.	
ISO Image OS	Ubuntu 22.04		ESXi 7.0	Ubuntu 22.04	

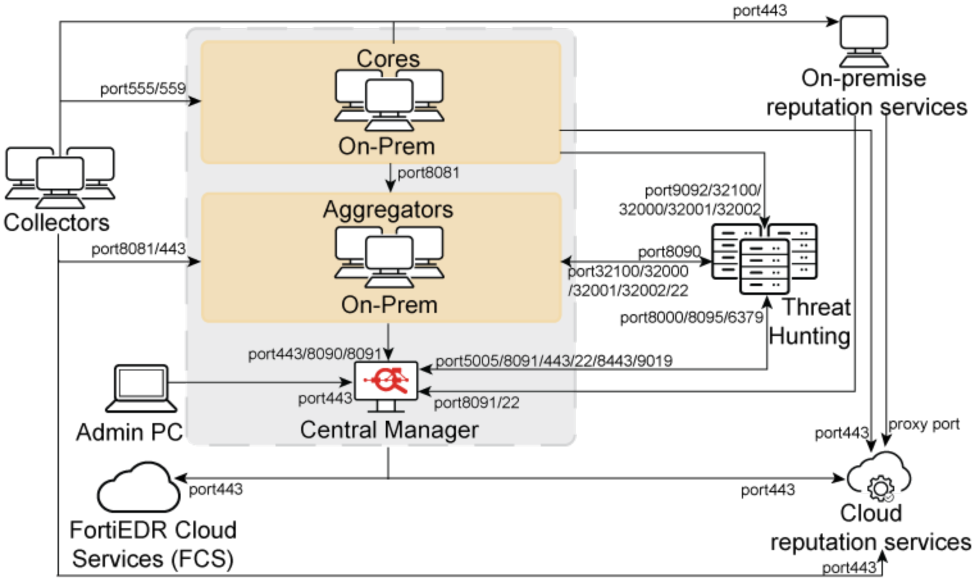
[1] If organizations will be defined and the number of Collectors exceeds 10000, set up an additional FortiEDR Aggregator VM on the top of the initial one.

[2] Refer to the following guidelines to determine the number of Cores you need to set up:

- Set up a separate Core for each Aggregator.
- For every additional 5000 Collectors, set up at least one additional Core. The number of additional Cores required depends on the amount of Threat Hunting events data, which relates to the Data Collection profile, number of servers, etc.
- You can set up a maximum of 50 Cores.

Network ports

Refer to the following image or table for the port information for communication between different components. Ensure that these ports or destination servers are not blocked by your firewall product (if one is deployed) and can be accessed by the corresponding component. You must also ensure that network ranges `10.42.x.x` and `10.43.x.x` are not used by any device.



Source	Destination	Port	Purpose
Collector	Aggregator	8081	Sending events, status, etc
		443	Sending events, status, etc, only when a custom port is used
	Core	555	Collector to Core communication without SSL
		(Core 5.2.2 or later) 559	Collector to Core communication with SSL enabled
	(Windows Collector 5.2.5.0052 or later) Reputation services (on-premise and/or cloud)	443	Sending requests for reputation data. When both on-premise and cloud reputation services are configured, FortiEDR Collectors prioritize the on-premise reputation server over the cloud. The cloud reputation services will be contacted only when the on-premise reputation server is unreachable.
Core	Aggregator	8081	Core registration
	Threat Hunting Repository	9092	Kafka topic
		32100, 32000, 32001, 32002	Kafka broker
	Reputation services (on-premise and/or cloud)	443	Sending requests for reputation data.
Aggregator	Central Manager and Threat Hunting Repository	8090	AV Signature updates
	Central Manager	8091	Aggregator communication
		443	Aggregator registration

Source	Destination	Port	Purpose
Central Manager	Threat Hunting Repository	8000	"FortiEDR Connect" related
		8095	Threat Hunting queries
		6379	Redis MS
	Syslog	**(Optional)** 6514	Syslog messages from Central Manager IP to syslog server via UDP/TCP/TCP SSL
	SMTP	**(Optional)** 587	SSLv3/TLS protocol to email server
	`rbq.cldsrv.ensilo.com`	5672	To RabbitMQ
	`cldsrv.ensilo.com`	443	Data sent to FCS (rest over RabbitMQ)

	`storage.googleapis.com`
	`oauth.googleapis.com`
	`oauth2.googleapis.com`
			Localization, scheduled queries, etc

	`fortiav.cloud.ensilo.com`		AV signatures updates
	Reputation service (cloud)	443	If proxy is not enabled, on-premise reputation service requests missing hashes from the cloud reputation service via the manager nginx.
Threat Hunting Repository	Central Manager	8091	Aggregator communication
		5005	"FortiEDR Connect" dedicated tunnel
		443	GUI access
		22	Communication with Central Manager during Threat Hunting Repository installation
		8443	Authentication service
		9019	Sink service
	Aggregator	22	Communication with Aggregator during Threat Hunting Repository installation
		32100, 32000, 32001, 32002	Secure browser connections to Kafka broker from Aggregator
Admin PC	Central Manager	443	FortiEDR console access

Source	Destination	Port	Purpose
Reputation service (on-premise)	Central Manager	8091	If proxy is not enabled, on-premise reputation service requests missing hashes from the cloud reputation service via the manager nginx.
		22	SSH application access
	Reputation service (cloud)	Proxy port	If proxy is enabled, on-premise reputation service requests missing hashes from the cloud reputation service via proxy.
Machines connecting to Grafana or Kibana	Threat Hunting Repository	3000	Grafana - monitoring
		5601	Kibana - logging
Machines accessing the Threat Hunting server via SSH	Central Manager	22	SSH access
	Aggregator		
	Threat Hunting Repository		

As a security best practice, it is recommended to update the firewall rules so that they only have a narrow opening. For example:

- Only open the TCP outbound port 555 to the Core IP address.
- Only open the TCP outbound port 8091 to the Central Manager IP address to be accessed by the Aggregator when the Aggregator is installed on premise while the Central Manager is in the cloud.

Threat Hunting Repository CPU, Physical Memory, and Disk Space Requirements

Number of Seats	Number of VMs (Nodes)	Number of CPUs per VM (Node)	Memory per VM (Node)	OS Disk per VM (Node)	Data Disk per VM (Node)
2000 or fewer	1	17	40 GB	100 GB, non-SSD	1500 GB SSD

Number of Seats	Number of VMs (Nodes)	Number of CPUs per VM (Node)	Memory per VM (Node)	OS Disk per VM (Node)	Data Disk per VM (Node)
				For Hyper-V VMs, the disk should be IDE with at least 30% of the physical disk space remaining free at all times. Do not use a Hyper-V checkpoint which consumes the entire disk size every few hours.	
4000		27	40 GB		2310 GB SSD
6000		37	41 GB		3410 GB SSD
8000		47	48 GB		4510 GB SSD
10000		57	55 GB		5610 GB SSD
12000		67	62 GB		6710 GB SSD
14000		77	69 GB		7810 GB SSD
15000	3	30	27 GB		3249 GB SSD
20000		40	35 GB		4318 GB SSD
25000		49	42 GB		5387 GB SSD
30000		58	47 GB		6456 GB SSD
For the Threat Hunting Repository specifications required for supporting more than 30000 Collectors, please contact Fortinet Support.					

Setting up FortiEDR components on-premise

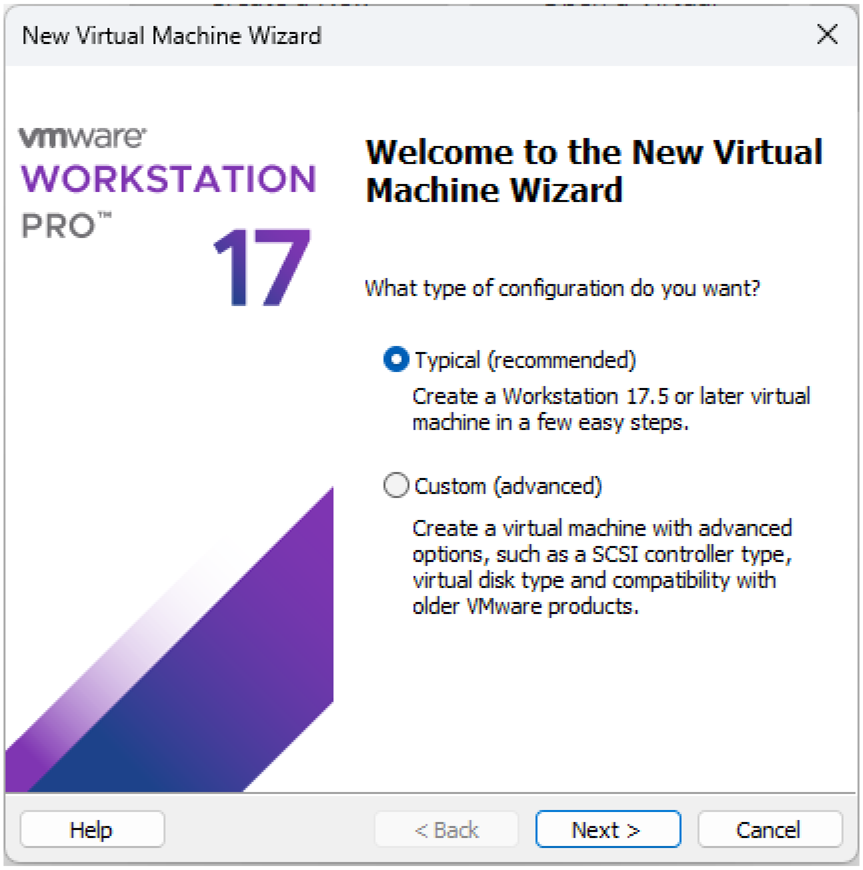
Set up the system components top-down in the following order:

1. Setting up a VM to be the FortiEDR Central Manager on page 465
2. Setting up a VM to be the FortiEDR Aggregator on page 481
3. Setting up the FortiEDR Threat Hunting Repository on page 490
4. Setting up the FortiEDR reputation server on page 508
5. Setting up the FortiEDR Core on page 511
6. Installing FortiEDR Collectors on page 23

Setting up a VM to be the FortiEDR Central Manager

To set up a VM to be the FortiEDR Central Manager:

1. Create a new virtual server by selecting *File > New Virtual Machine*.
2. Select *Typical* option and select *Next*.



New Virtual Machine Wizard

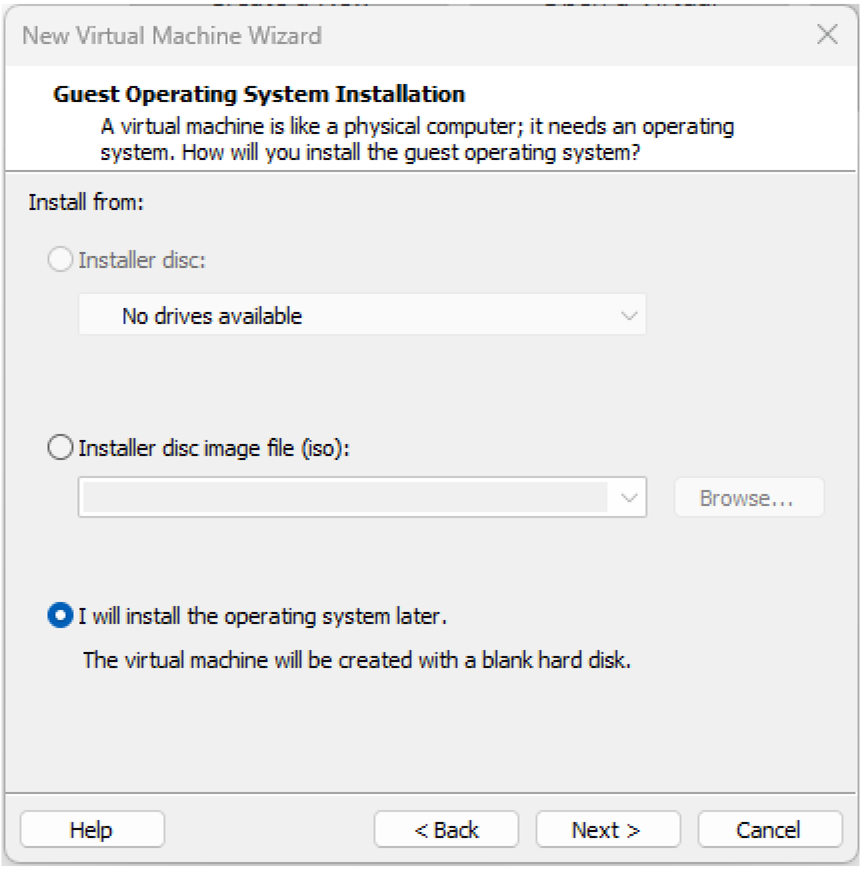
Welcome to the New Virtual Machine Wizard

What type of configuration do you want?

● Typical (recommended)
Create a Workstation 17.5 or later virtual machine in a few easy steps.

○ Custom (advanced)
Create a virtual machine with advanced options, such as a SCSI controller type, virtual disk type and compatibility with older VMware products.

3. Select the *I will install the operating system later* option and click *Next*.



New Virtual Machine Wizard

Guest Operating System Installation

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

○ Installer disc:

No drives available

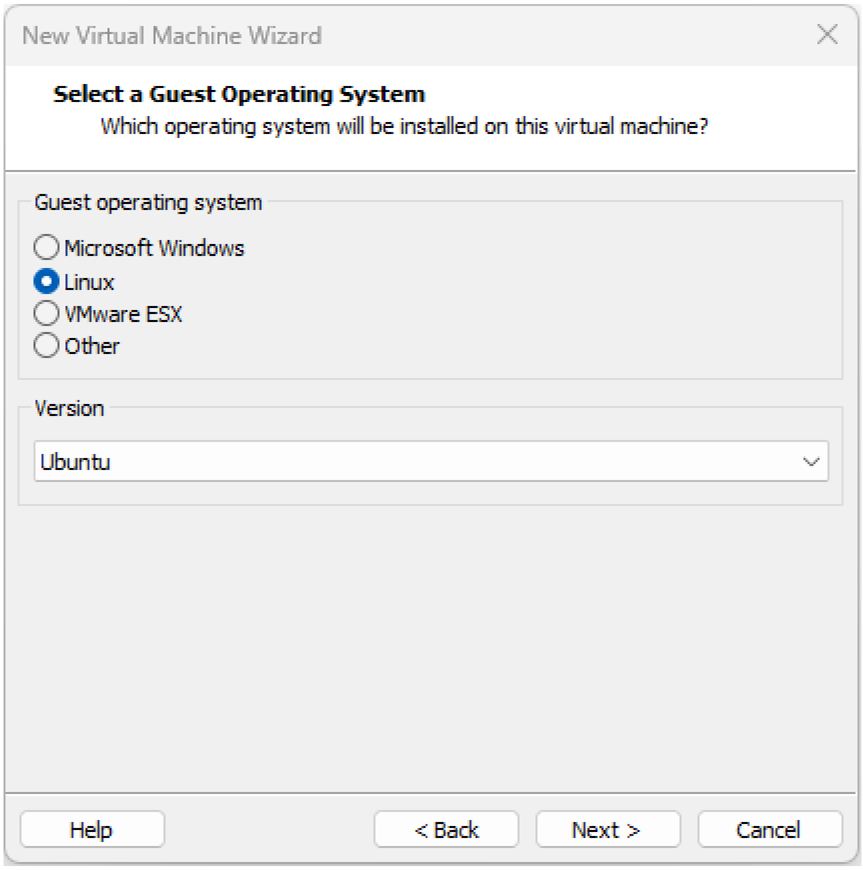
○ Installer disc image file (iso):

● I will install the operating system later.

The virtual machine will be created with a blank hard disk.

4. Select the *Linux* radio button. In the *Version* field, select *Ubuntu* and click *Next*.

In some VMware environments where the *Linux* radio button is unavailable, select a generic Linux type, such as *General Linux* or *Other Linux (for vSphere/ESXi)*. Do not select a specific Linux distribution.



New Virtual Machine Wizard

Select a Guest Operating System

Which operating system will be installed on this virtual machine?

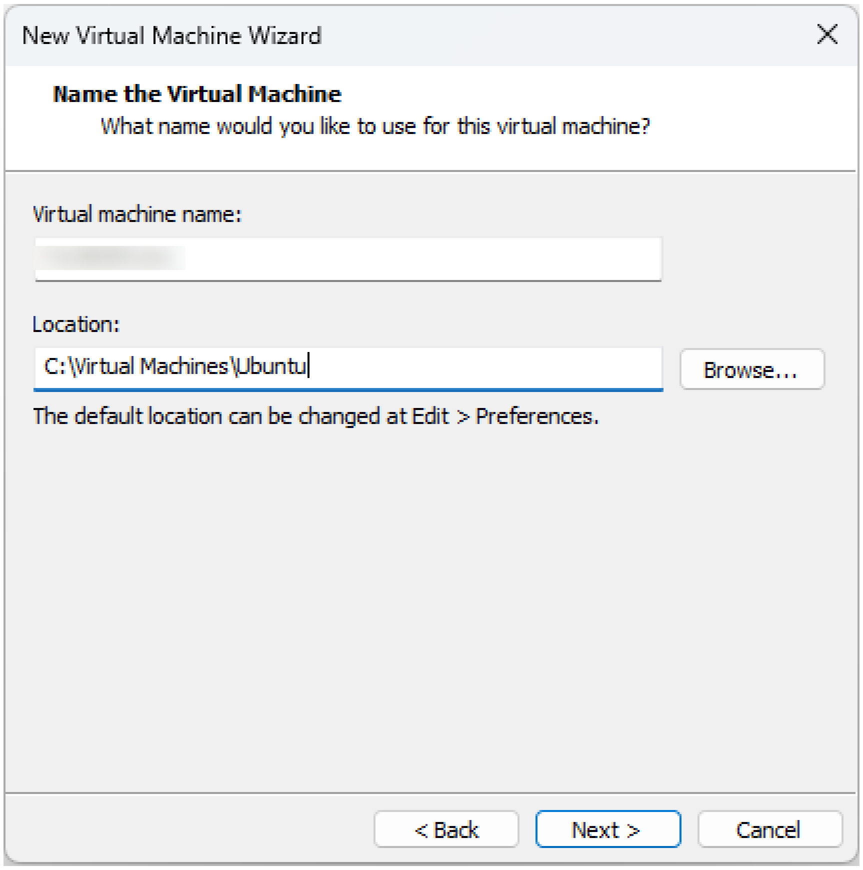
Guest operating system

○ Microsoft Windows
● Linux
○ VMware ESX
○ Other

Version

Ubuntu

5. Specify a name for the virtual machine and the location in which to store the provided ISO file and click *Next*.



New Virtual Machine Wizard

Name the Virtual Machine

What name would you like to use for this virtual machine?

Virtual machine name:

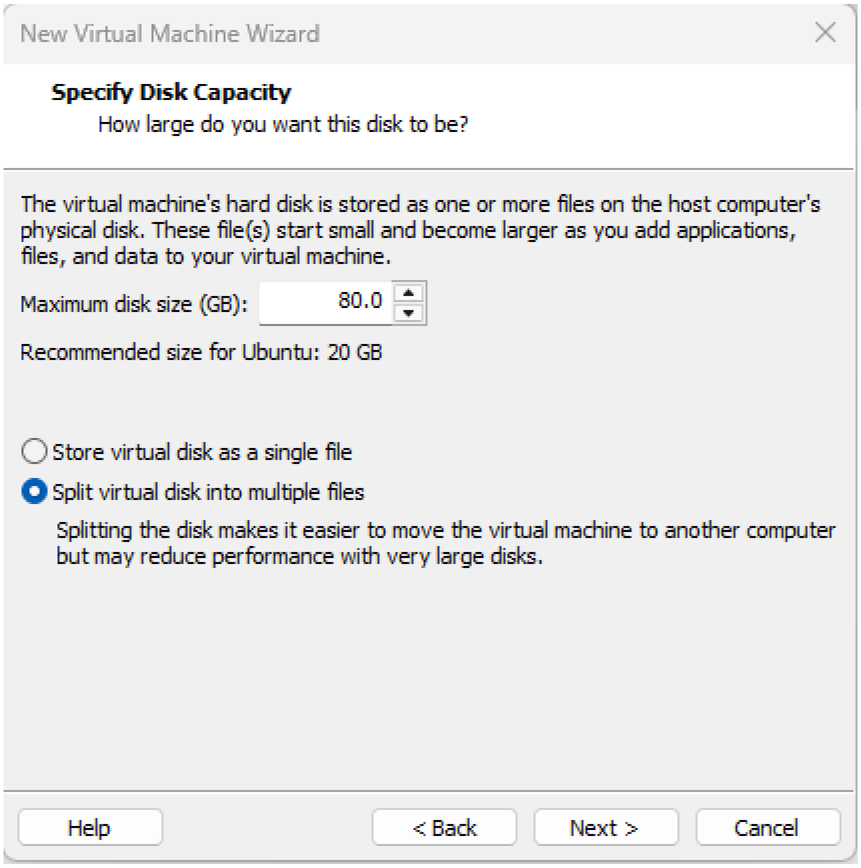
[redacted]

Location:

C:\Virtual Machines\Ubuntu

The default location can be changed at Edit > Preferences.

6. Change the *Maximum disk size* according to system requirements listed in Appendix C – ON PREMISE DEPLOYMENTS on page 459, leave the default option as *Split virtual disk into multiple files* and click *Next*.



Specify Disk Capacity

How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

Maximum disk size (GB): 80.0

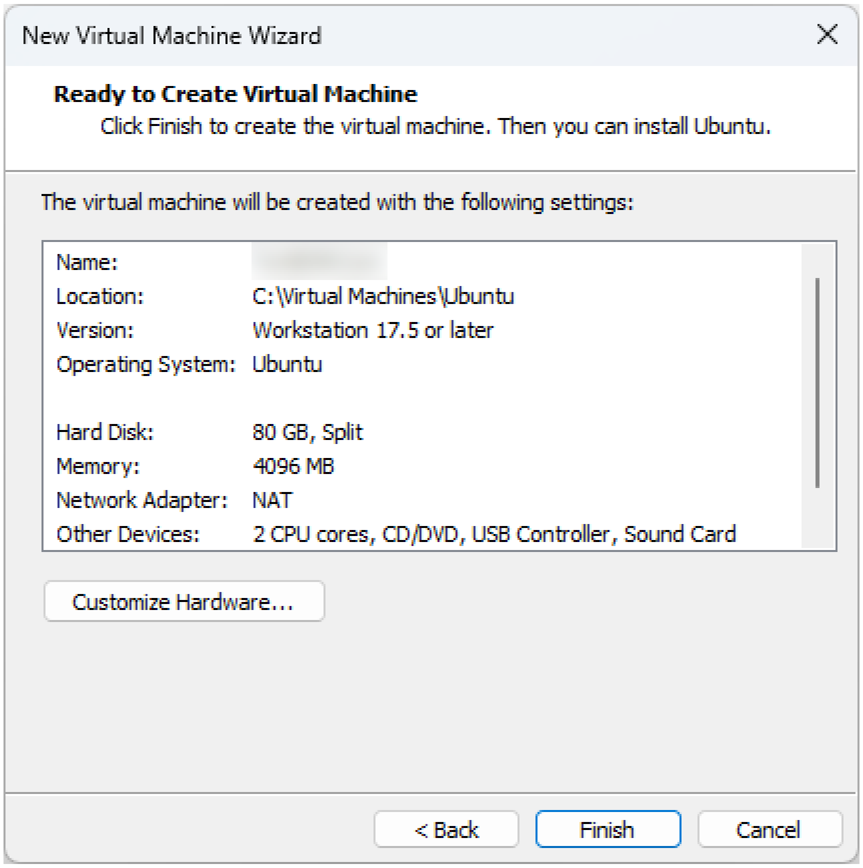
Recommended size for Ubuntu: 20 GB

○ Store virtual disk as a single file

● Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

7. Click *Finish*.



New Virtual Machine Wizard

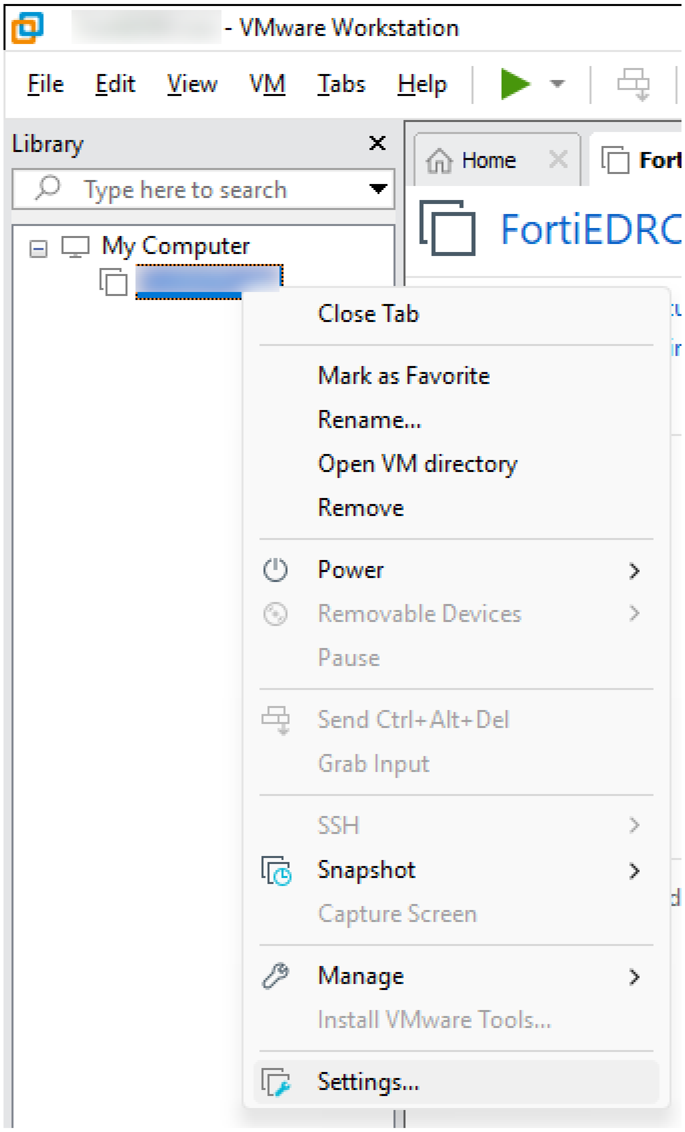
Ready to Create Virtual Machine

Click Finish to create the virtual machine. Then you can install Ubuntu.

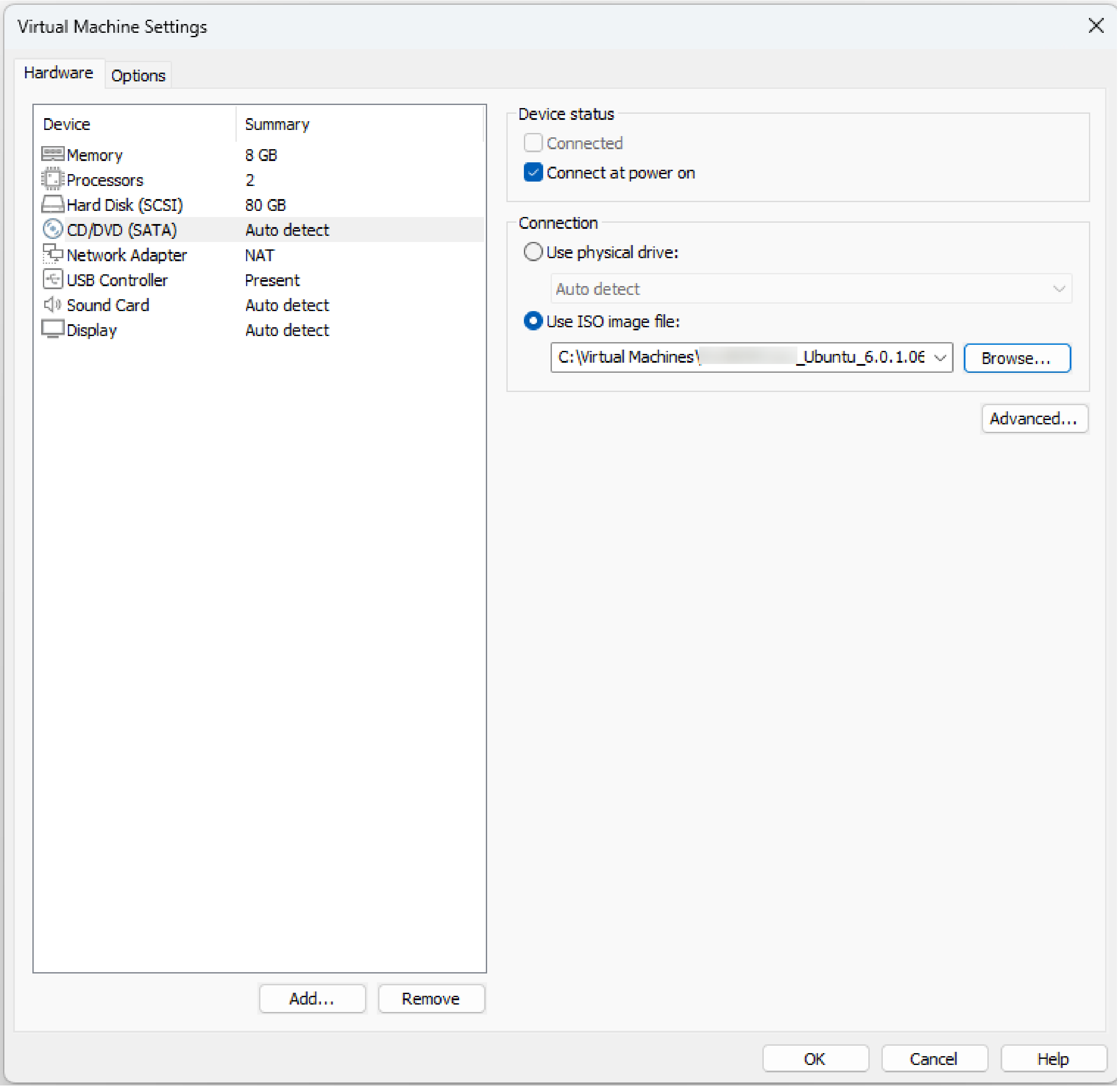
The virtual machine will be created with the following settings:

Name:	[redacted]
Location:	C:\Virtual Machines\Ubuntu
Version:	Workstation 17.5 or later
Operating System:	Ubuntu
Hard Disk:	80 GB, Split
Memory:	4096 MB
Network Adapter:	NAT
Other Devices:	2 CPU cores, CD/DVD, USB Controller, Sound Card

8. Right-click the new machine and select the *Settings* option



9. Select the *Memory* option and change the RAM according to the system requirements listed in Appendix C – ON PREMISE DEPLOYMENTS on page 459.



Virtual Machine Settings

Hardware | Options

Device	Summary
Memory	8 GB
Processors	2
Hard Disk (SCSI)	80 GB
CD/DVD (SATA)	Auto detect
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Device status

□ Connected

☑ Connect at power on

Connection

○ Use physical drive:

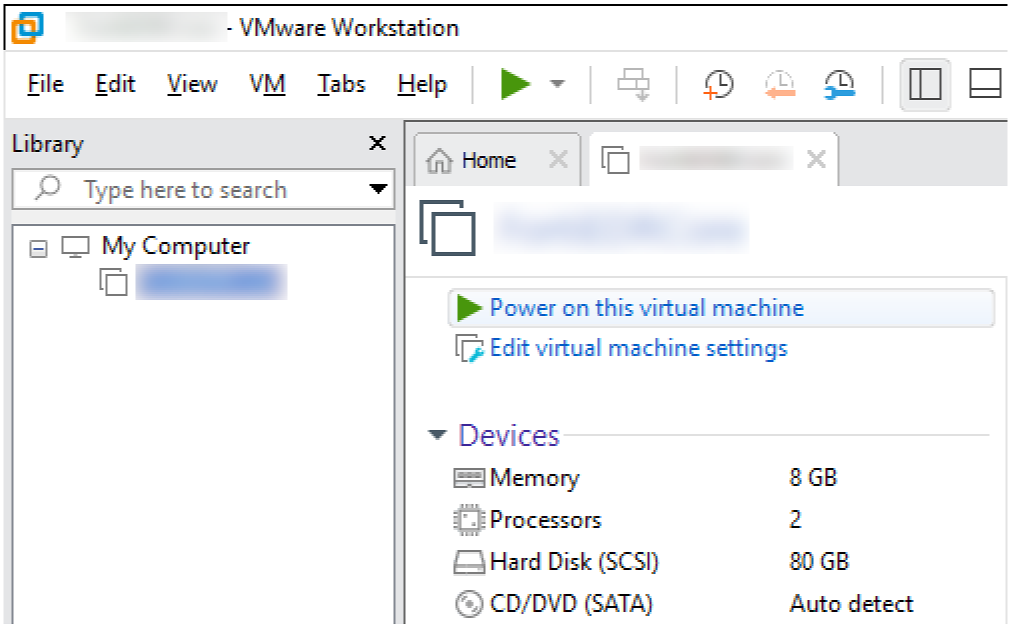
Auto detect

● Use ISO image file:

C:\Virtual Machines\ _Ubuntu_6.0.1.06

10. Select the *Processors* option and change the value according to the system requirements.
11. Select the *CD/DVD* option and then select the *Use ISO image file* option on the right.
12. Click the *Browse* button and select the ISO file provided by Fortinet for the FortiEDR Central Manager. Click *OK*.

13. Start the virtual machine.



Memory	8 GB
Processors	2
Hard Disk (SCSI)	80 GB
CD/DVD (SATA)	Auto detect

The virtual machine automatically starts the installation process, which may take a few minutes.

14. Wait until a success message is displayed requesting that you reboot.
15. Reboot the virtual machine.
16. Log into the virtual machine in order to continue the installation process.
    `Login: root`
    Change the root password, by entering any password you want. Then re-type it. The password must be strong enough according to Linux standards.
17. In the VM CLI, enter `fortiedr config`.
18. At the prompt, enter your `hostname` and click *Next*. (Note: This can be any hostname)
19. At the prompt, select *manager* to configure the VM as the Central Manager, and click *Next*.
20. A list of network interfaces on this virtual machine displays. At the *Pick your primary interface* prompt, select the interface to be used as the primary network interface through which all FortiEDR Cores and FortiEDR Collectors will reach this server, and click *Next*.
21. At the *Do you want to use DHCP* prompt, select *No* to configure the IP of this virtual machine manually, and then click *Next*.
22. At the prompt, enter the IP address of the machine that you are installing. Use the following format: `xxx.xxx.xxx.xxx/yy`, where yy is the routing prefix of the subnet.
23. At the prompt, enter the default gateway and click *Next*.
24. At the *Please set your DNS server* prompt, enter a valid IP address and click *Next*. Use the following format:
    `xxx.xxx.xxx.xxx/yy`, where yy is the routing prefix of the subnet.
25. At the prompt, select *No* for debug mode.
26. At the *Please set the date* prompt, verify the date and click *Next*. The installer automatically presents the current date. You can change this date, if necessary.
27. At the *Please set your Time* prompt, set the time and click *Next*.
28. At the prompt, select the timezone and country in which the server is being installed.

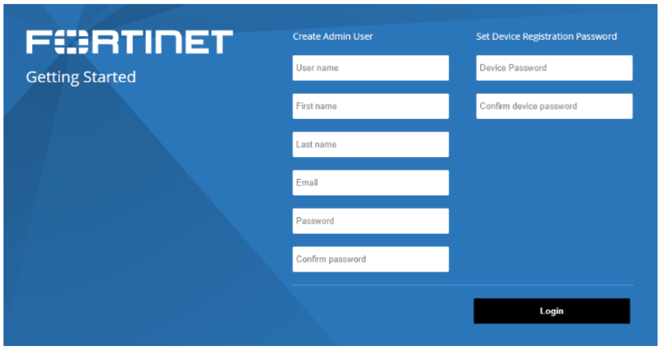
29. At the *Do you want to enable web-proxy for the Manager?* prompt, if the Central Manager will communicate via a proxy when accessing the web (such as the FortiEDR Cloud Service (FCS)), select *Yes* and then enter the IP and port of the proxy. Otherwise, select *No*.
30. At the *Do you want to enable FCS?* prompt, select *Yes*.
31. Wait a few moments while the installation processes, until you see the Installation completed successfully message.
32. Configuring the FortiEDR Central Manager server and console on page 474.

Configuring the FortiEDR Central Manager server and console

After you install the FortiEDR Central Manager, you must configure the FortiEDR Central Manager Server and console before setting up other components, such as Aggregators, Cores, and Collectors. The configuration includes creating an Admin user, setting up device registration password, loading your license, and optional MITM configuration.

To configure the FortiEDR Central Manager Server and console:

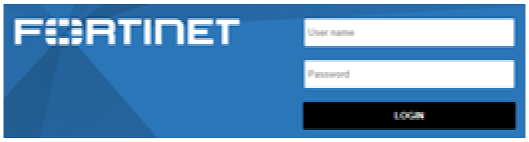
1. Use any standard Internet browser to connect securely (via https://) to the IP address and port of the machine on which the FortiEDR Central Manager is installed, as follows:
   a. `https://<machine_IP_addess>/`
   b. Default port is 443
2. Define the first administrator user to be allowed to log into the FortiEDR Manager by filling in the *First Name*, *Last Name*, *Email Address*, and *Define administrator user name* fields.



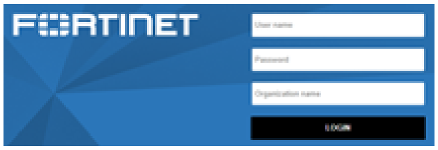
3. Enter and confirm the password to be used by this administrator user.
4. In the *Device Registration Password* fields, enter and confirm the password to be used to install all FortiEDR Collectors, FortiEDR Aggregators and FortiEDR Cores. This same password must be used by all. The following special characters are supported in the password: !, #, %, &, +, -, ., /, :, <, =, >, ?, @, [, \,], ^, _, `, {, |, }, (,), ~, and ,

Write this password down in a good place. This password will be needed each time a FortiEDR component is installed. If you forgot your user interface password, contact Fortinet Support to retrieve it.

5. Click the *Login* button. The regular FortiEDR Central Manager Login page is then displayed, as shown below. The page that displays varies, depending on whether the FortiEDR system is set up as a single-organization or multi-organization system.



Login Page in a Single-organization System

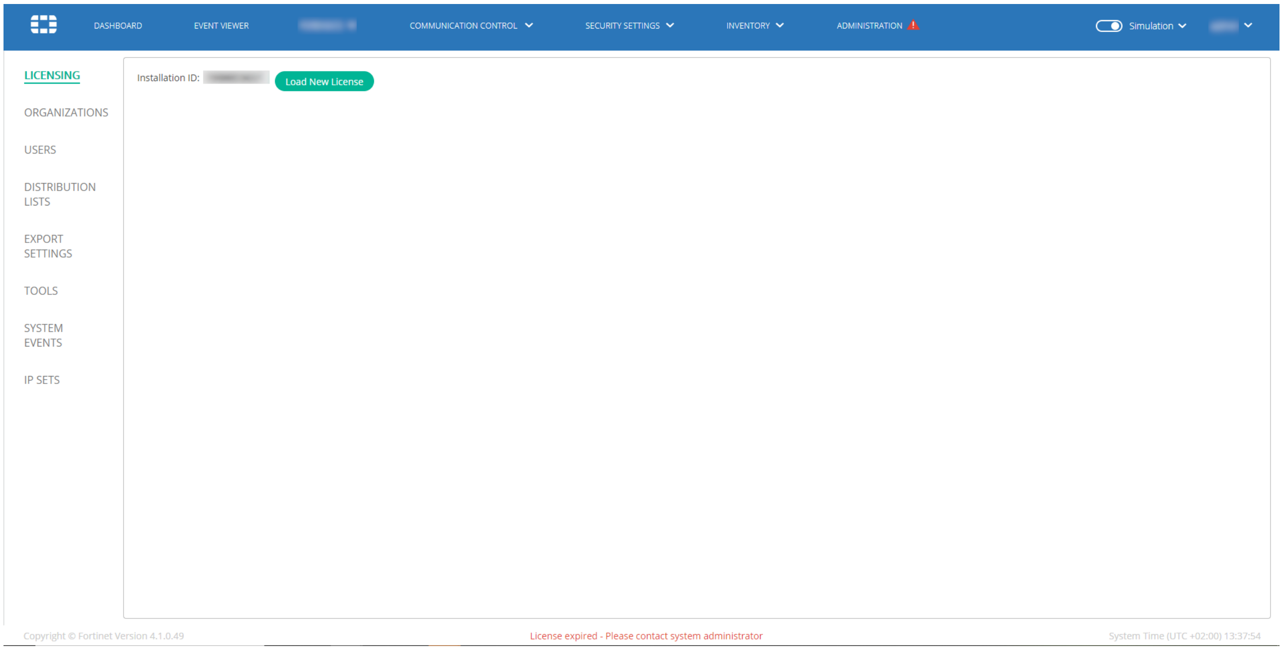


Login Page in a Multi-organization System

The FortiEDR system can be set up as a single-organization or multi-organization system. In a multi-organization system, all users except an Administrator user must specify the organization in the Organization Name dropdown list. If a user is defined for an organization, then he/she can log in to that organization. Otherwise, he/she cannot.

For more details about logging in to a multi-organization system, see Step 1 – Logging in to a multi-organization system on page 418.

6. Enter the administrator user name and password you have just defined and click *Login*. All fields are case sensitive. The following window displays automatically the first time you log into the FortiEDR Central Manager:



Installation ID: [redacted]

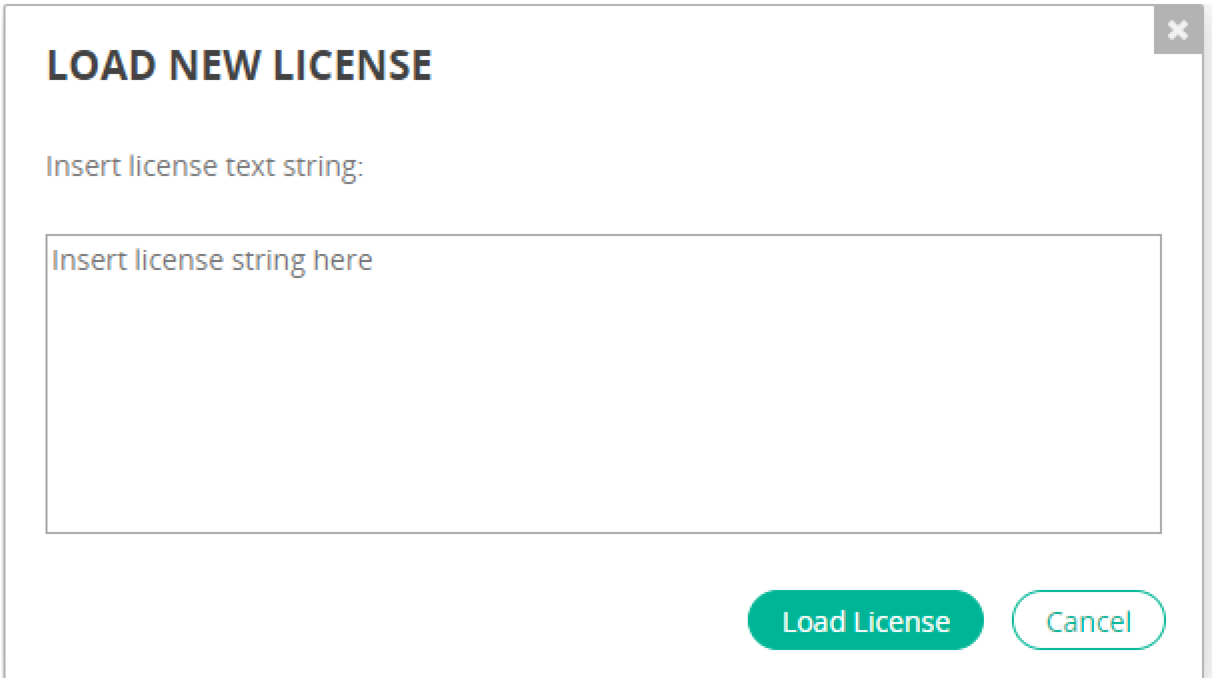
Copyright © Fortinet Version 4.1.0.49

License expired - Please contact system administrator

System Time (UTC +02:00) 13:37:54

7. Send the displayed Installation ID to FortiEDRAdmin@fortinet.com by email in order to receive a license string from Fortinet.

8. Click *Load New License*. The *LOAD NEW LICENSE* window opens.

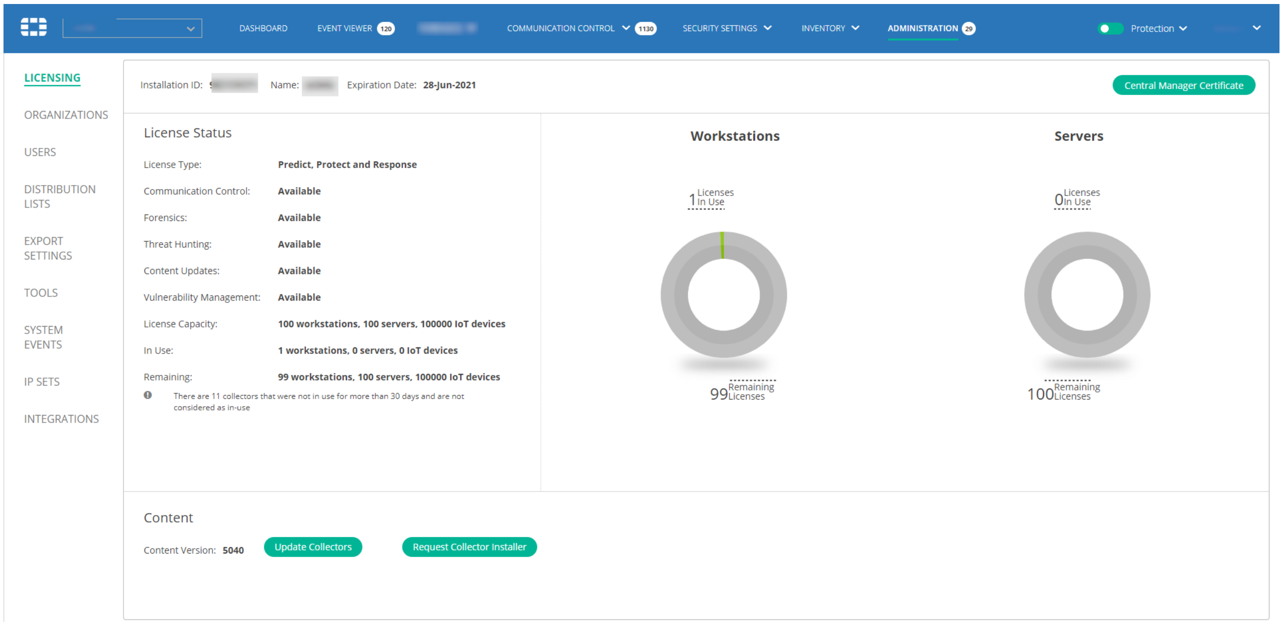


LOAD NEW LICENSE

Insert license text string:

Insert license string here

9. Copy/paste the license string that you received by email into the *LOAD NEW LICENSE* window and click *Load License*. The following displays showing the relevant licensed entitlements:



Installation ID: [redacted] Name: [redacted] Expiration Date: 28-Jun-2021

License Status

License Type:	Predict, Protect and Response
Communication Control:	Available
Forensics:	Available
Threat Hunting:	Available
Content Updates:	Available
Vulnerability Management:	Available
License Capacity:	100 workstations, 100 servers, 100000 IoT devices
In Use:	1 workstations, 0 servers, 0 IoT devices
Remaining:	99 workstations, 100 servers, 100000 IoT devices

There are 11 collectors that were not in use for more than 30 days and are not considered as in-use

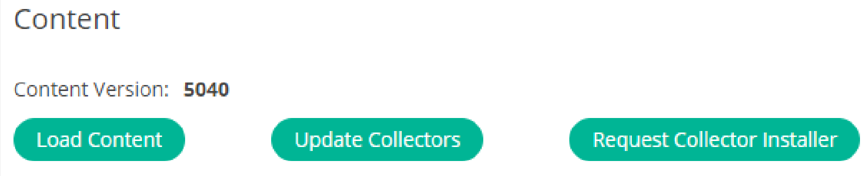
Workstations: 1 Licenses In Use; 99 Remaining Licenses

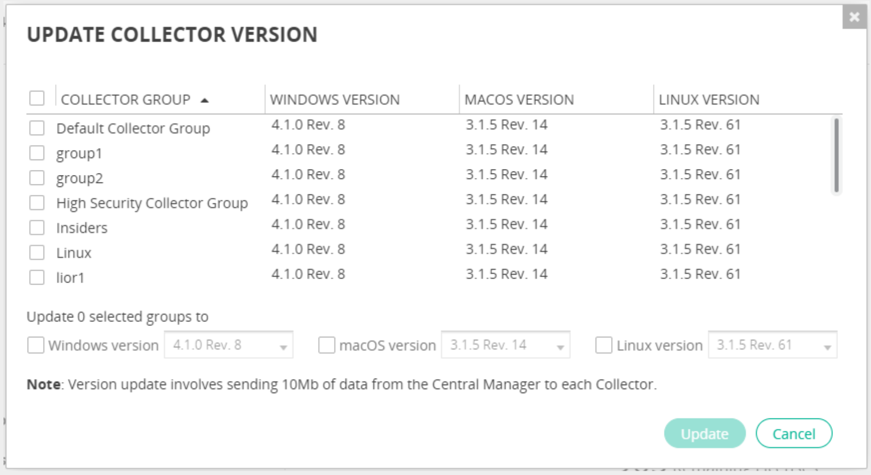
Servers: 0 Licenses In Use; 100 Remaining Licenses

Content

Content Version: 5040

Field	Description
Installation ID	Specifies the unique identifier that is automatically generated upon installation of the ForitEDR Management server. You may be asked to provide this ID and the *Name* field when contacting Fortinet for support.

Field	Description
Name	Specifies the name of the organization in a multi-organization FortiEDR system. For more details, see Multi-tenancy (organizations) on page 415.
Expiration Date	Specifies when this license expires. Notifications will be sent to you beforehand.
License Type	Specifies whether the *Discover, Protect and Response* license, *Discover and Protect* license, or *Protect and Response* license was purchased. The license type defines the availability of the relevant add-ons.
Communication Control	Specifies the word *Available* if the Communication Control add-on is included in the license.
eXtended Detection	Specifies the word *Available*, when the *eXtended Detection* add-on is included in the license.
Forensics	Specifies the word *Available* if the Forensics add-on is included in the license.
Threat Hunting	Specifies the word *Available* if the Threat hunting add-on (described in Threat Hunting on page 125) is included in the license. It also specifies whether Repository add-ons have been purchased and how many have been.
Content Updates	Specifies the word *Available* if the *Content Updates* add-on is included in the license. This add-on enables you to automatically receive the latest FortiEDR policy rule and built-in exception updates. The system arrives with the latest content pre-installed. There is no need to install content during the initial installation. The *Load Content* button enables you to update content, as well as to update the Collector version on any existing Collector.  Content Content Version: **5040** To load content updates on your FortiEDR system, click the *Load Content* button and then select the content file to load. In a multi-tenant environment, the *Load Content* button is available in Hoster View . If the content file contains a Collector update, you can update all Collectors with the new version at that time, or choose to do so later. Click the *Update Collectors* button to update the version for all Collectors.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>

UPDATE COLLECTOR VERSION
<table>
<tr><th>□ COLLECTOR GROUP ▲</th><th>WINDOWS VERSION</th><th>MACOS VERSION</th><th>LINUX VERSION</th></tr>
<tr><td>□ Default Collector Group</td><td>4.1.0 Rev. 8</td><td>3.1.5 Rev. 14</td><td>3.1.5 Rev. 61</td></tr>
<tr><td>□ group1</td><td>4.1.0 Rev. 8</td><td>3.1.5 Rev. 14</td><td>3.1.5 Rev. 61</td></tr>
<tr><td>□ group2</td><td>4.1.0 Rev. 8</td><td>3.1.5 Rev. 14</td><td>3.1.5 Rev. 61</td></tr>
<tr><td>□ High Security Collector Group</td><td>4.1.0 Rev. 8</td><td>3.1.5 Rev. 14</td><td>3.1.5 Rev. 61</td></tr>
<tr><td>□ Insiders</td><td>4.1.0 Rev. 8</td><td>3.1.5 Rev. 14</td><td>3.1.5 Rev. 61</td></tr>
<tr><td>□ Linux</td><td>4.1.0 Rev. 8</td><td>3.1.5 Rev. 14</td><td>3.1.5 Rev. 61</td></tr>
<tr><td>□ lior1</td><td>4.1.0 Rev. 8</td><td>3.1.5 Rev. 14</td><td>3.1.5 Rev. 61</td></tr>
</table>
Update 0 selected groups to
□ Windows version 4.1.0 Rev. 8 □ macOS version 3.1.5 Rev. 14 □ Linux version 3.1.5 Rev. 61
<b>Note</b>: Version update involves sending 10Mb of data from the Central Manager to each Collector.

</td></tr>
<tr><td><i>Vulnerability Management</i></td><td>Specifies the word <i>Available</i> if the Vulnerability Management add-on (described in Administration on page 277) is included in the license.</td></tr>
<tr><td><i>License Capacity</i></td><td>Specifies the number of available licenses for protection by FortiEDR Collectors (for workstations and servers). Only the number of FortiEDR Collectors allowed by the license can register with the FortiEDR Central Manager. Additional FortiEDR Collectors are not registered with the FortiEDR Central Manager. In addition, the number of IoT devices specified under the License Capacity determines whether or not IoT Discovery is available (zero number).</td></tr>
<tr><td><i>In Use</i></td><td>Specifies the number of FortiEDR licenses for workstations and servers that are currently in use. In addition, it specifies the number of IoT devices detected in the system thus far.</td></tr>
<tr><td><i>Remaining</i></td><td>Specifies the number of FortiEDR licenses for workstations and servers that are still available for use.</td></tr>
</table>

Regarding questions about the number of licenses purchased, please contact Fortinet Support.

10. **(Optional)** Configure the FortiEDR Central Manager to communicate with the Internet via a controlled MITM application (for example, FortiGate with SSL deep inspection enabled):

    a. Add the MITM CA certificate to the list of trusted certificates in the Central Manager Java application using the following API:

```
Method: POST
URL: /maintenance/upload-certificate
Body:
{
"alias": [custom_ca_name],
"certificateBlob": [CA certificate in pem format, encoded in base64]
}
```

Certificates signed by your custom MITM CA will not be trusted.

Example:

For the following certificate:

```
---BEGIN CERTIFICATE---

MIIDYzCCAkugAwIBAgIUXTs0sl6LZ3MNoiuy1+2QUOEqNqIwDQYJKoZIhvcNAQEL

BQAwUzELMAkGA1UEBhMCVVMxDjAMBgNVBAgMBVN0YXRlMQ0wCwYDVQQHDARDaXR5

MRUwEwYDVQQKDAxPcmdhbml6YXRpb24xDjAMBgNVBAMMBU15IENBMB4XDTI0MTAy

NzA4NDgxN1oXDTM0MTAyNTA4NDgxN1owUzELMAkGA1UEBhMCVVMxDjAMBgNVBAgM

BVN0YXRlMQ0wCwYDVQQHDARDaXR5MRUwEwYDVQQKDAxPcmdhbml6YXRpb24xDjAM

BgNVBAMMBU15IENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAua6l

NjX39F4T0MDozaENXHfnJ7qli/oK/M3SH6ZMFkOyAita31ri/JO2L2k7HS4qwHpJ

GGPnwsWEMsnwYJ8xuSi2Iz90KfRniDD5sgt/DFAjb+CRO4zbfERizO0qvQqCgqnU

24I2gCl31K7Frsky11B6db2s2I0LLpPVl7LMyaZ84yx4g1VFJSU1aYYXh8AU8oJa

ghW9LD6WFYMXjQIP0RQbUhqT0UK1CuEcl0ly/yVWmQ7edSyAV/YsIO7DpicPBuG9

fsLoY60tPhqj0pmfHcdMLDJoa03offAAhiqRDAQN5k5KnA6YcPxvDCoT88jTx823

8QQNd9gsVHr6uvLmpwIDAQABoy8wLTAMBgNVHRMEBTADAQH/MB0GA1UdDgQWBBQo

x7OwCDVpK1627HvgxMHNfAcp9TANBgkqhkiG9w0BAQsFAAOCAQEAL5u6LZQFLWVd

mQhkLWn9RuOR1vTnNHaARzURCH8k4VCfIliz93ruYXjJb/LWbJlMxR1nPjRbieI8

wAgUBfPV2cr4bXuP70W8Ftp/MYyw37G1sg1vzi9rvMl/h61I7aPn4JX9IRAaP+jO

7vT8hWP1DGf+TQKFBehHP5xJIEhCoWCESqPrOjF24YtDd4QYJWZm0IRtVIIVBnZ9

m6ZlHuRcZ3zLDpigtkyuLG3S/6BsQF0WOJQNQt90QU168026+7JlF7OSlH7EIl79

LaguuiA+PRXAN3ysNi4+/anp7Auy5ssIwjcZX7nAuPsUNGLUKH2LAELC0FxCZoO6

gC6bm+wRsg==

---END CERTIFICATE---
```

Encode the certificate in Base64 and use it in the API as follows:

```
{
```

```
"alias": "my_custom_MITM_ca",
```

```
"certificateBlob":
"LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSURZekNDQWt1Z0F3SUJBZ0lVWFRzMHNsNkxaM01Ob2l1eTErM
lFVT0VxTnFJd0RRWUpLb1pJaHZjTkFRRUwKQlFBd1V6RUxNQWtHQTFVRUJoTUNWVk14RGpBTUJnTlZCQWdNQlZOMFl
YUmxNUTB3Q3dZRFZRUUhEQVJEYVhSNQpNUlV3RXdZRFZRUUtEQXhQY21kaGJtbDZZWFJwYjI0eERqQU1CZ05WQkFNT
UJVMTVJRU5CTUI0WERUSTBNVEF5Ck56QTRORGd4TjFvWERUTTBNVEF5TlRBNE5EZ3hOMW93VXpFTE1Ba0dBMVVFQmh
NQ1ZWTXhEakFNQmdOVkJBZ00KQlZOMFlYUmxNUTB3Q3dZRFZRUUhEQVJEYVhSNU1SVXdFd1lEVlFRS0RBeFBjbWRoY
m1sNllYUnBiMjR4RGpBTQpCZ05WQkFNTUJVMTVJRU5CTUlJQklqQU5CZ2txaGtpRzl3MEJBUUVGQUFPQ0FROEFNSUl
CQ2dLQ0FRRUF1YTZsCk5qWDM5RjRUME1Eb3phRU5YSGZuSjdxbGkvb0svTTNTSDZaTUZrT3lBaXRhMzFyaS9KTzJMM
ms3SFM0cXdIcEoKR0dQbndzV0VNc253WUo4eHVTaTJJejkwS2ZSbmlERDVzZ3QvREZBamIrQ1JPNHpiZkVSaXpPMHF
2UXFDZ3FuVQoyNEkyZ0NsMzFLN0Zyc2t5MTFCNmRiMnMySTBMTHBQVmw3TE15YVo4NHl4NGcxVkZKU1UxYVlZWGg4Q
VU4b0phCmdoVzlMRDZXRllNWGpRSVAwUlFiVWhxVDBVSzFDdUVjbDBseS95VldtUTdlZFN5QVYvWXNJTzdEcGljUEJ
1RzkKZnNMb1k2MHRQaHFqMHBtZkhjZE1MREpvYTAzb2ZmQUFoaXFSREFRTjVrNUtuQTZZY1B4dkRDb1Q4OGpUeDgyM
wo4UVFOZDlnc1ZIcjZ1dkxtcHdJREFRQUJveTh3TFRBTUJnTlZIUk1FQlRBREFRSC9NQjBHQTFVZERnUVdCQlFvCng
3T3dDRFZwSzE2MjdIdmd4TUhOZkFjcDlUQU5CZ2txaGtpRzl3MEJBUXNGQUFPQ0FRRUFMNXU2TFpRRkxXVmQKbVFoa
0xXbjlSdU9SMXZUbk5IYUFSelVSQ0g4azRWQ2ZJbGl6OTNydVlYakpiL0xXYkpsTXhSMW5QalJiaWVJOAp3QWdVQmZ
QVjJjcjRiWHVQNzBXOEZ0cC9NWXl3MzdHMXNnMXZ6aTlydk1sL2g2MUk3YVBuNEpYOUlSQWFQK2pPCjd2VDhoV1AxR
EdmK1RRS0ZCZWhIUDV4SklFaENvV0NFU3FQck9qRjI0WXREZDRRWUpXWm0wSVJ0VklJVkJuWjkKbTZabEh1UmNaM3p
MRHBpZ3RreXVMRzNTLzZCc1FGMFdPSlFOUXQ5MFFVMTY4MDI2KzdKbEY3T1NsSDdFSWw3OQpMYWd1dWlBK1BSWEFOM
3lzTmk0Ky9hbnA3QXV5NXNzSXdqY1pYN25BdVBzVU5HTFVLSDJMQUVMQzBGeENNab082CmdDNmJtK3dSc2c9PQotLS0
tLUVORCBDRVJUSUZJQ0FURS0tLS0t"
```

```
}
```

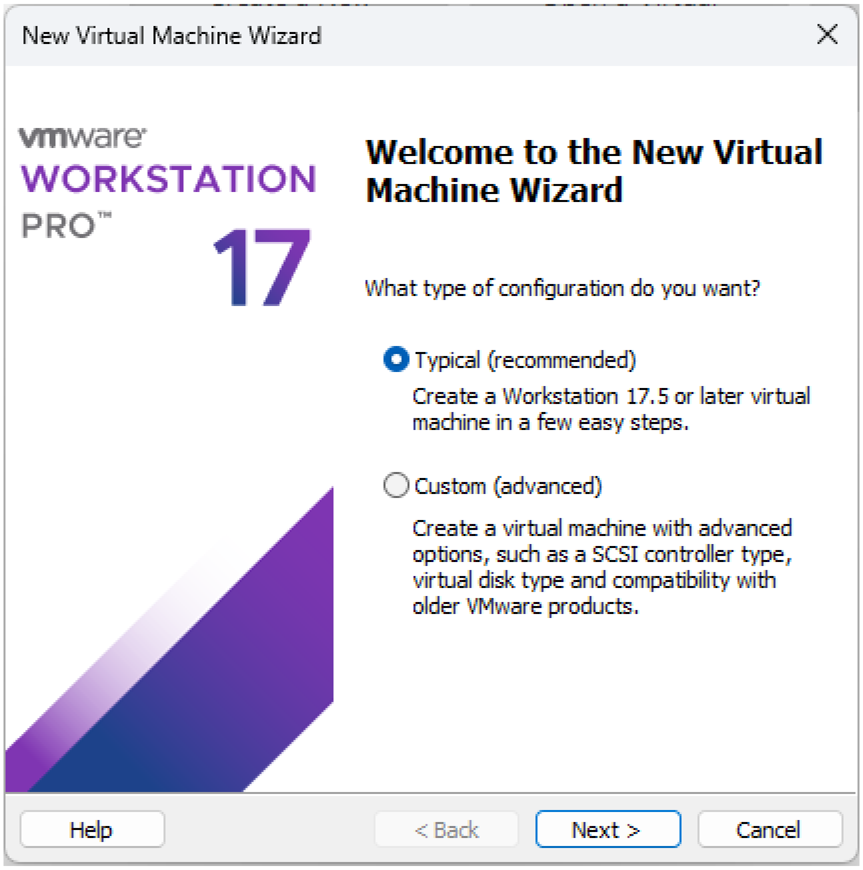
b. Add propery `ssl.truststore.enabled=true` to file `application-customer.properties`.

c. Restart the manager service using the following command: `exec command fortiedr manager restart`.

Setting up a VM to be the FortiEDR Aggregator

To set up a VM to be the FortiEDR Aggregator:

1. Create a new virtual server by selecting *File* > *New Virtual Machine*.
2. Select *Typical* option and select *Next*.


New Virtual Machine Wizard

Welcome to the New Virtual Machine Wizard

What type of configuration do you want?

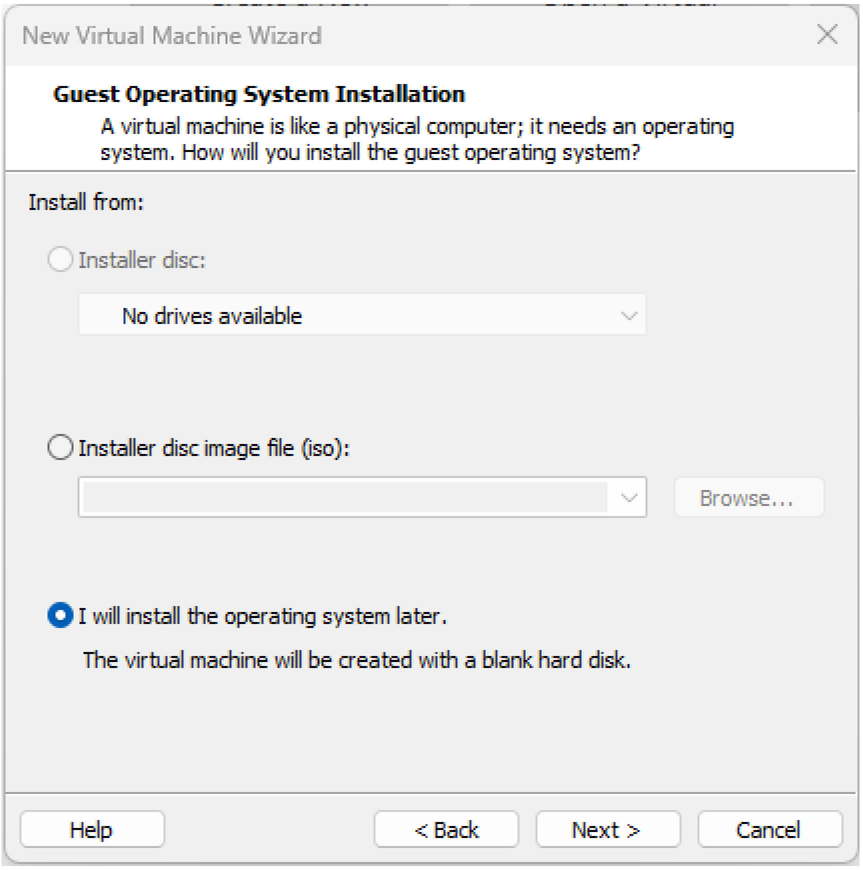
● Typical (recommended)

Create a Workstation 17.5 or later virtual machine in a few easy steps.

○ Custom (advanced)

Create a virtual machine with advanced options, such as a SCSI controller type, virtual disk type and compatibility with older VMware products.

3. Select the *I will install the operating system later* option and click *Next*.



New Virtual Machine Wizard

Guest Operating System Installation

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

○ Installer disc:

No drives available

○ Installer disc image file (iso):

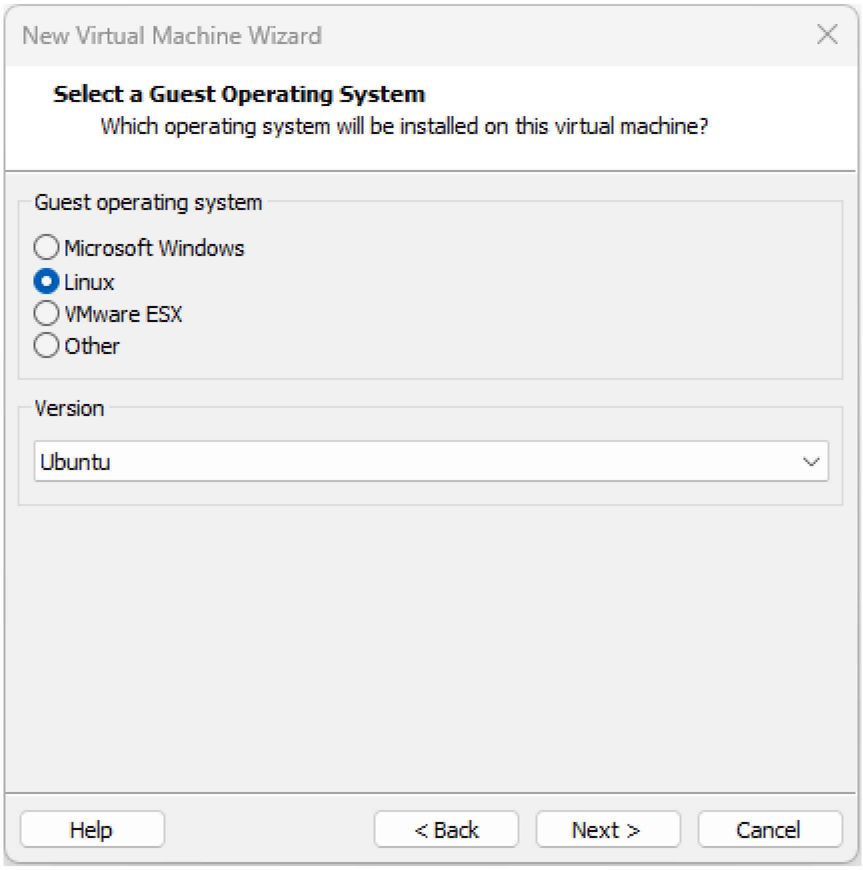
Browse...

● I will install the operating system later.

The virtual machine will be created with a blank hard disk.

4. Select the *Linux* radio button. In the *Version* field, select *Ubuntu* and click *Next*.

In some VMware environments where the *Linux* radio button is unavailable, select a generic Linux type, such as *General Linux* or *Other Linux (for vSphere/ESXi)*. Do not select a specific Linux distribution.



Select a Guest Operating System

Which operating system will be installed on this virtual machine?

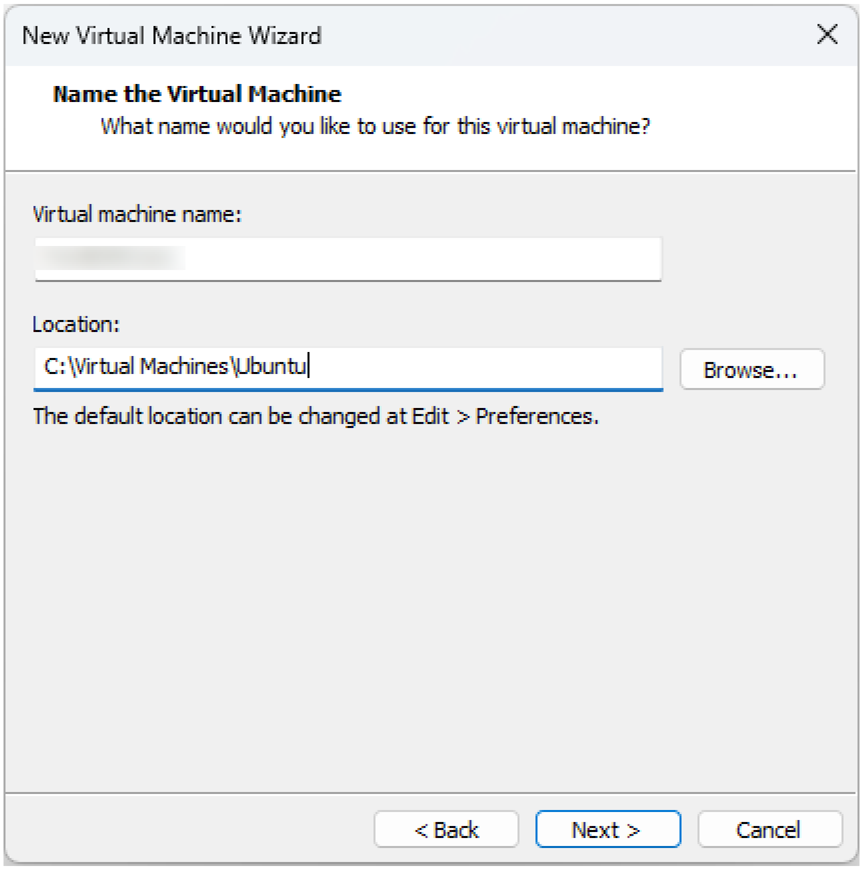
Guest operating system

○ Microsoft Windows
● Linux
○ VMware ESX
○ Other

Version

Ubuntu

5. Specify a name for the virtual machine and the location in which to store the provided ISO file and click *Next*.



New Virtual Machine Wizard

Name the Virtual Machine

What name would you like to use for this virtual machine?

Virtual machine name:

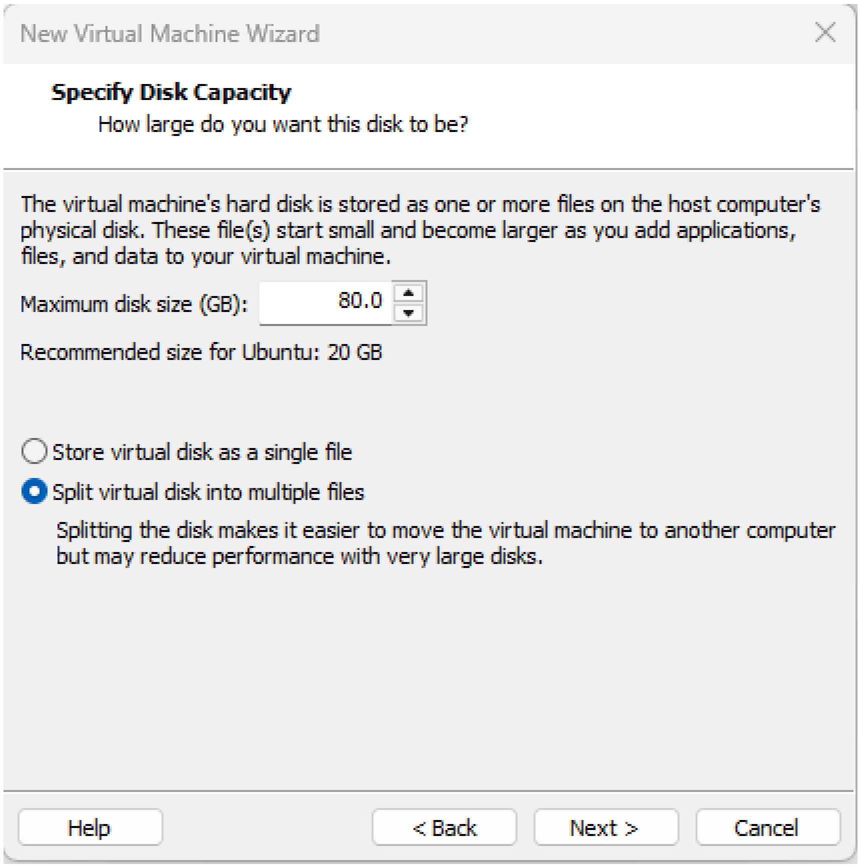
[redacted]

Location:

C:\Virtual Machines\Ubuntu

The default location can be changed at Edit > Preferences.

6. Change the *Maximum disk size* according to system requirements listed in Appendix C – ON PREMISE DEPLOYMENTS on page 459, leave the default option as *Split virtual disk into multiple files* and click *Next*.



New Virtual Machine Wizard

Specify Disk Capacity

How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

Maximum disk size (GB): 80.0

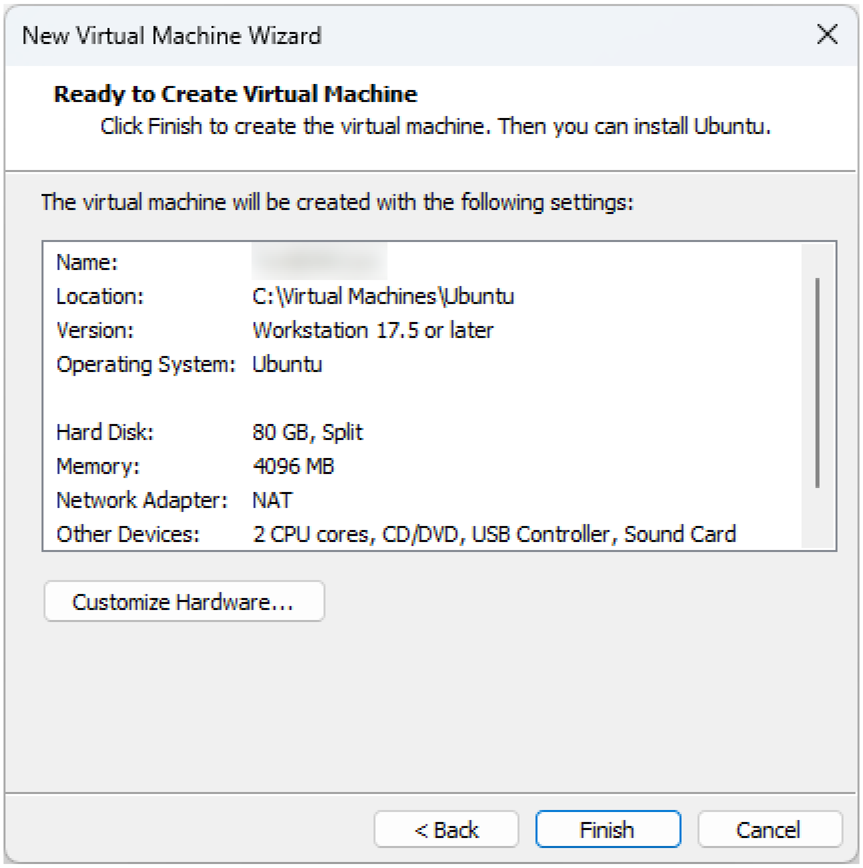
Recommended size for Ubuntu: 20 GB

○ Store virtual disk as a single file

● Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

7. Click *Finish*.



New Virtual Machine Wizard

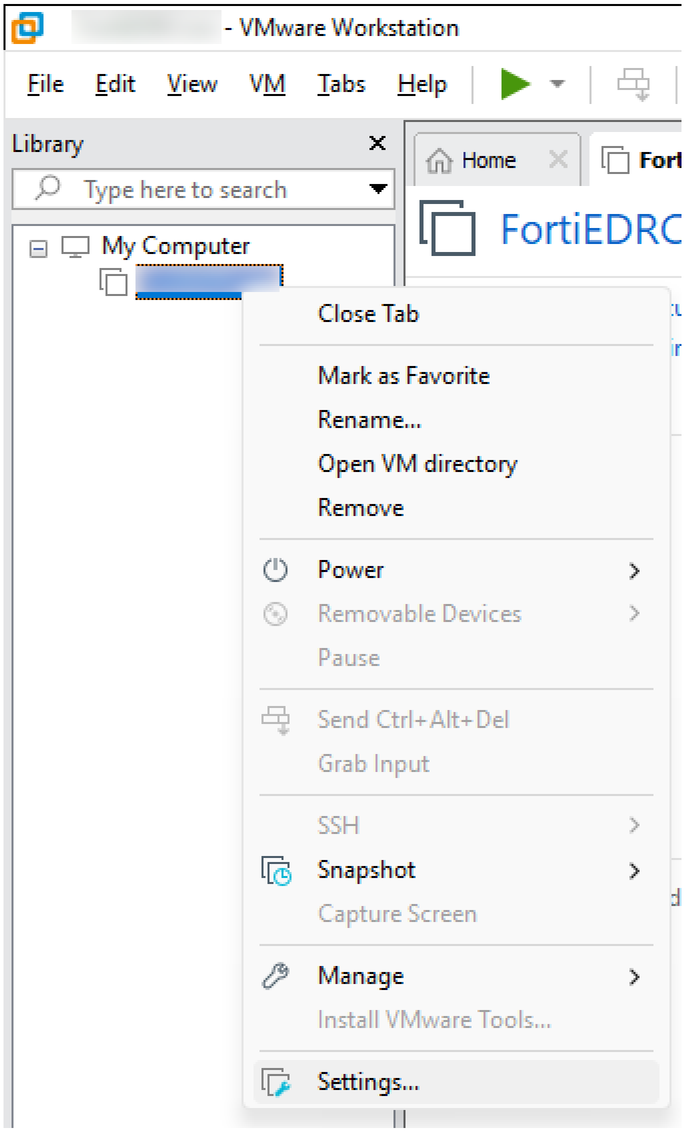
Ready to Create Virtual Machine

Click Finish to create the virtual machine. Then you can install Ubuntu.

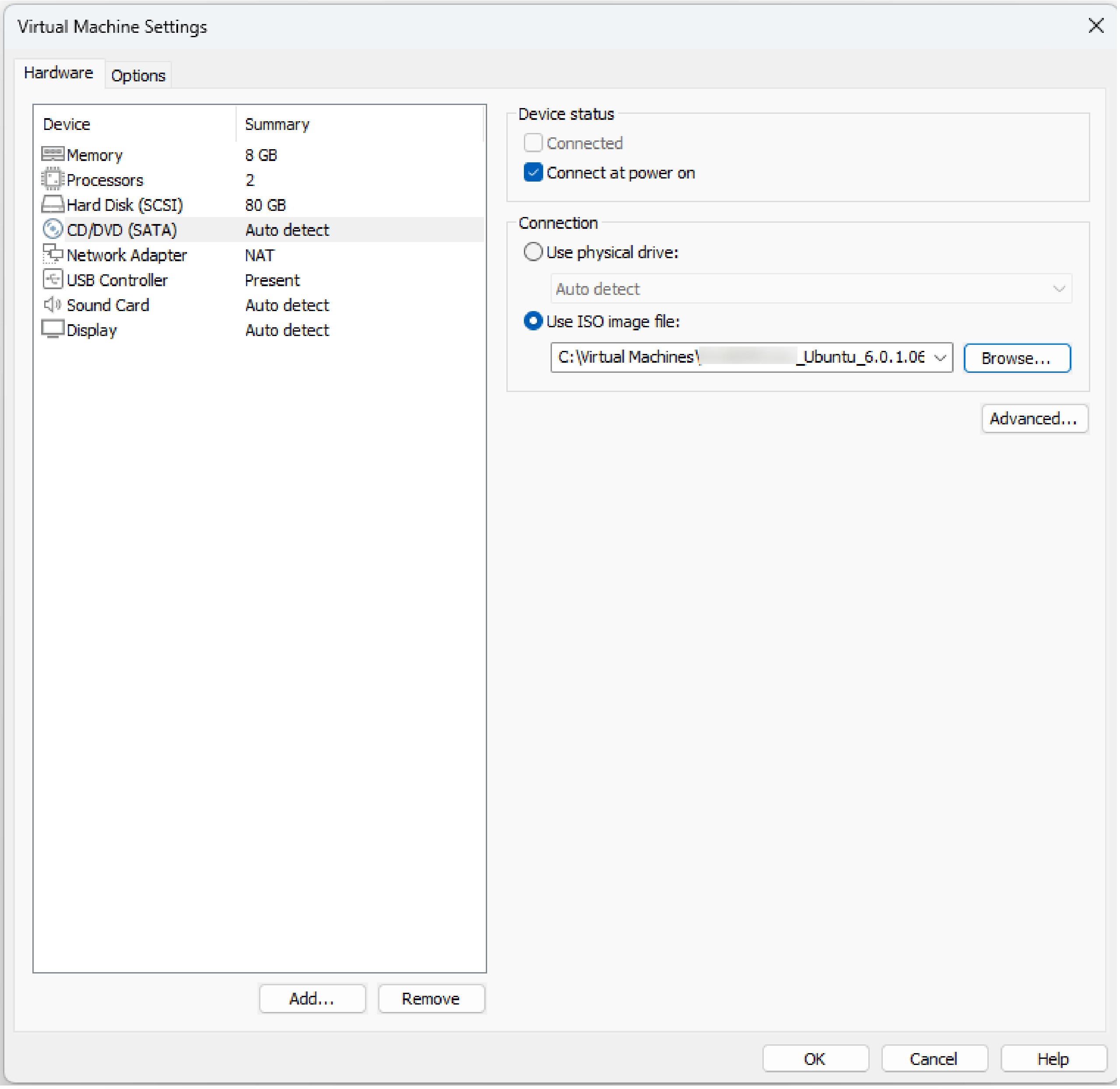
The virtual machine will be created with the following settings:

Name:	[redacted]
Location:	C:\Virtual Machines\Ubuntu
Version:	Workstation 17.5 or later
Operating System:	Ubuntu
Hard Disk:	80 GB, Split
Memory:	4096 MB
Network Adapter:	NAT
Other Devices:	2 CPU cores, CD/DVD, USB Controller, Sound Card

8. Right-click the new machine and select the *Settings* option



9. Select the *Memory* option and change the RAM according to the system requirements listed in Appendix C – ON PREMISE DEPLOYMENTS on page 459.



Virtual Machine Settings

Device	Summary
Memory	8 GB
Processors	2
Hard Disk (SCSI)	80 GB
CD/DVD (SATA)	Auto detect
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Device status

□ Connected

☑ Connect at power on

Connection

○ Use physical drive:

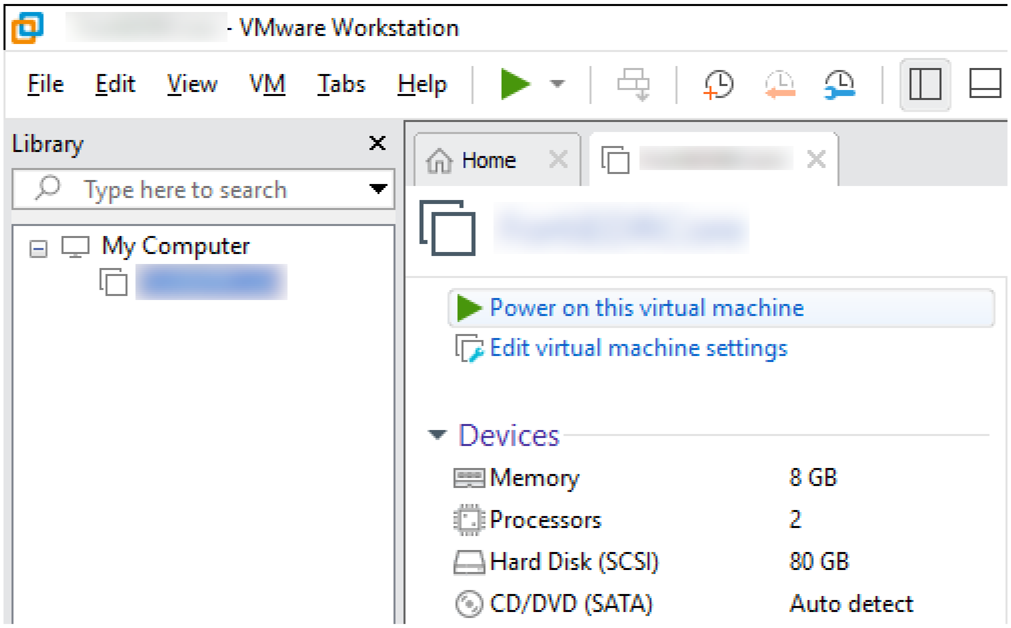
Auto detect

● Use ISO image file:

C:\Virtual Machines\[redacted]_Ubuntu_6.0.1.06

10. Select the *Processors* option and change the value according to the system requirements.
11. Select the *CD/DVD* option and then select the *Use ISO image file* option on the right.
12. Click the *Browse* button and select the ISO file provided by Fortinet for the FortiEDR Central Manager. Click *OK*.

13. Start the virtual machine.



Memory	8 GB
Processors	2
Hard Disk (SCSI)	80 GB
CD/DVD (SATA)	Auto detect

The virtual machine automatically starts the installation process, which may take a few minutes.

14. Wait until a success message is displayed requesting that you reboot.
15. Reboot the virtual machine.
16. Log into the virtual machine in order to continue the installation process.
`Login: root`
Change the root password, by entering any password you want. Then re-type it. The password must be strong enough according to Linux standards.
17. In the VM CLI, enter `fortiedr config`.
18. At the prompt, enter your `hostname` and click *Next*. (Note: This can be any hostname)
19. At the prompt, select *aggregator* to configure the VM as the Aggregator, and click *Next*.
20. At the *Please enter the management IP address* prompt, enter the IP address to be used for communicating with the FortiEDR Central Manager and click *Next*.
21. At the *Please enter your registration password* prompt, enter the user and password used to register the FortiEDR Aggregator with the FortiEDR Central Manager, which you configured in step 30 in the previous section, and click *Next*.
22. At the *Do you want to use DHCP* prompt, select *No* to configure the IP of this virtual machine manually, and then click *Next*.
23. At the prompt, enter the IP address of the machine that you are installing. Use the following format: `xxx.xxx.xxx.xxx/yy`, where yy is the routing prefix of the subnet.
24. At the prompt, enter the default gateway and click *Next*.
25. At the *Please set your DNS server* prompt, enter a valid IP address and click *Next*. Use the following format:
`xxx.xxx.xxx.xxx/yy`, where yy is the routing prefix of the subnet.
26. At the prompt, select *No* for debug mode.
27. At the *Please set the date* prompt, verify the date and click *Next*. The installer automatically presents the current date. You can change this date, if necessary.
28. At the *Please set your Time* prompt, set the time and click *Next*.
29. At the prompt, select the timezone and country in which the server is being installed.

30. Wait a few moments while the installation processes, until you see the Installation completed successfully message.
31. If organizations are defined and the number of Collectors exceeds 10000, set up additional Aggregators by repeating the previous steps for each additional Aggregator.
32. (Recommended) Define a DNS address for the Aggregator by following the steps below. Doing so avoids the need to reinstall all Collectors that are registered with the Aggregator IP when the Aggregator IP changes in some cases, such as when the Aggregator is migrated to a different data center.
    a. Define a DNS address for the Aggregator.
    b. Configure FortiEDR to disable the NAT IP and use the local IP of the Aggregator:
        i. Connnect to the FortiEDR Central Manager via `ssh`.
        ii. Open the `conf-customer.properties` configuration file using the following command: `vi/opt/FortiEDR/aggregator/conf-customer.properties`.
        iii. Comment out the `connection.dnsname = 10.10.80.201` line as follows: `#connection.dns-name = 10.10.80.201`.
        iv. Save the changes and restart the FortiEDR Aggregator service using the `fortiedr aggregator restart` command.
        v. Check the status of the Aggregator using the `fortiedr aggregator status` command.

Setting up the FortiEDR Threat Hunting Repository

The FortiEDR Threat Hunting feature (described in Threat Hunting on page 125) requires the set up of the Threat Hunting repository, which includes the following steps:

1. Creating a Virtual Machine on page 491
2. Installing an Operating System ISO on page 493
3. Installing a FortiEDR Repository software ISO on page 499
4. Configuring the Threat Hunting Repository Monitoring console on page 502
5. Backing up Threat Hunting Repository data on page 503
6. Activating the Threat Hunting Repository Monitoring console on page 504

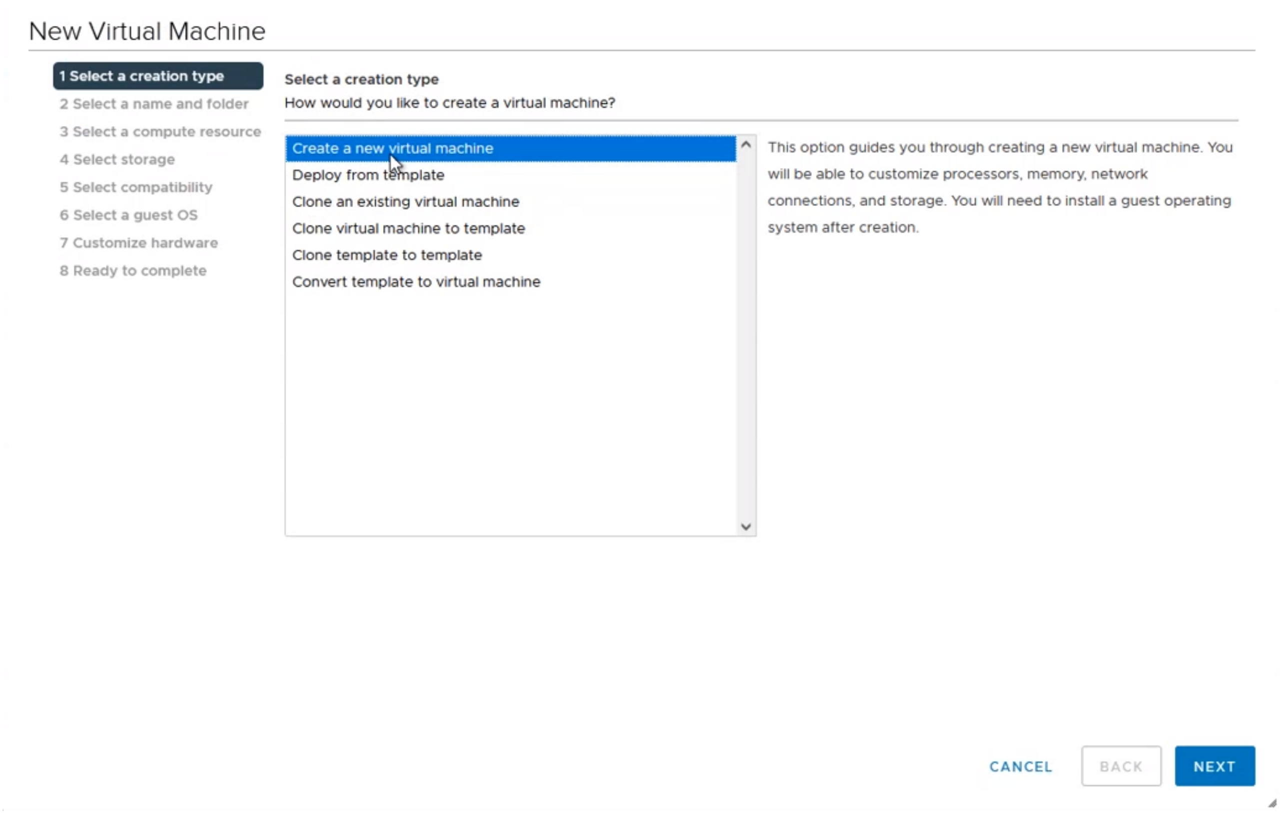
Prerequisites

- A license with access to the Threat Hunting feature.
- The FortiEDR Central Manager is installed.
- The system requirements listed in Appendix C – ON PREMISE DEPLOYMENTS on page 459 must be met.

Creating a Virtual Machine

To create a virtual machine:

1. Create a new virtual server. For example, by selecting *File > New Virtual Machine....*, then selecting *Create a new virtual machine* and clicking *NEXT*.



New Virtual Machine

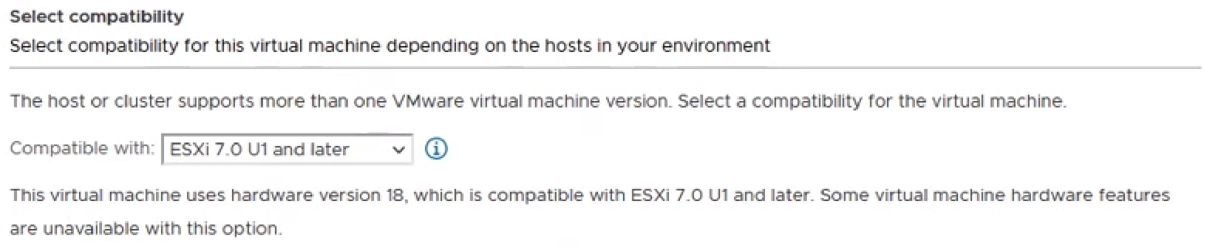
1 Select a creation type
2 Select a name and folder
3 Select a compute resource
4 Select storage
5 Select compatibility
6 Select a guest OS
7 Customize hardware
8 Ready to complete

Select a creation type
How would you like to create a virtual machine?

Create a new virtual machine
Deploy from template
Clone an existing virtual machine
Clone virtual machine to template
Clone template to template
Convert template to virtual machine

This option guides you through creating a new virtual machine. You will be able to customize processors, memory, network connections, and storage. You will need to install a guest operating system after creation.

2. Enter the desired *virtual machine name*. For example, *FortiEDR-TH-Repository* and click *NEXT*.
3. Enter the virtual machine settings, as follows:
   a. In the *Select storage* step, select the storage where the virtual machine disk should be stored on and click *NEXT*.
   b. In the *Select Compatibility* step, select *ESXi 7.0 U1 and later* and click *NEXT*.



Select compatibility
Select compatibility for this virtual machine depending on the hosts in your environment

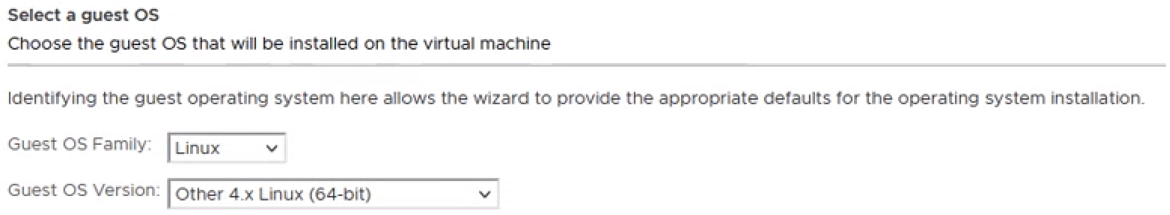
The host or cluster supports more than one VMware virtual machine version. Select a compatibility for the virtual machine.

Compatible with: ESXi 7.0 U1 and later

This virtual machine uses hardware version 18, which is compatible with ESXi 7.0 U1 and later. Some virtual machine hardware features are unavailable with this option.

   c. At the *Select a guest OS* step:
      i. In the *Guest OS family* field, select *Linux*.
      ii. In the *Guest OS version* field, select *Other 4.x Linux (64-bit)*.

iii. Click *Next*. The following displays:



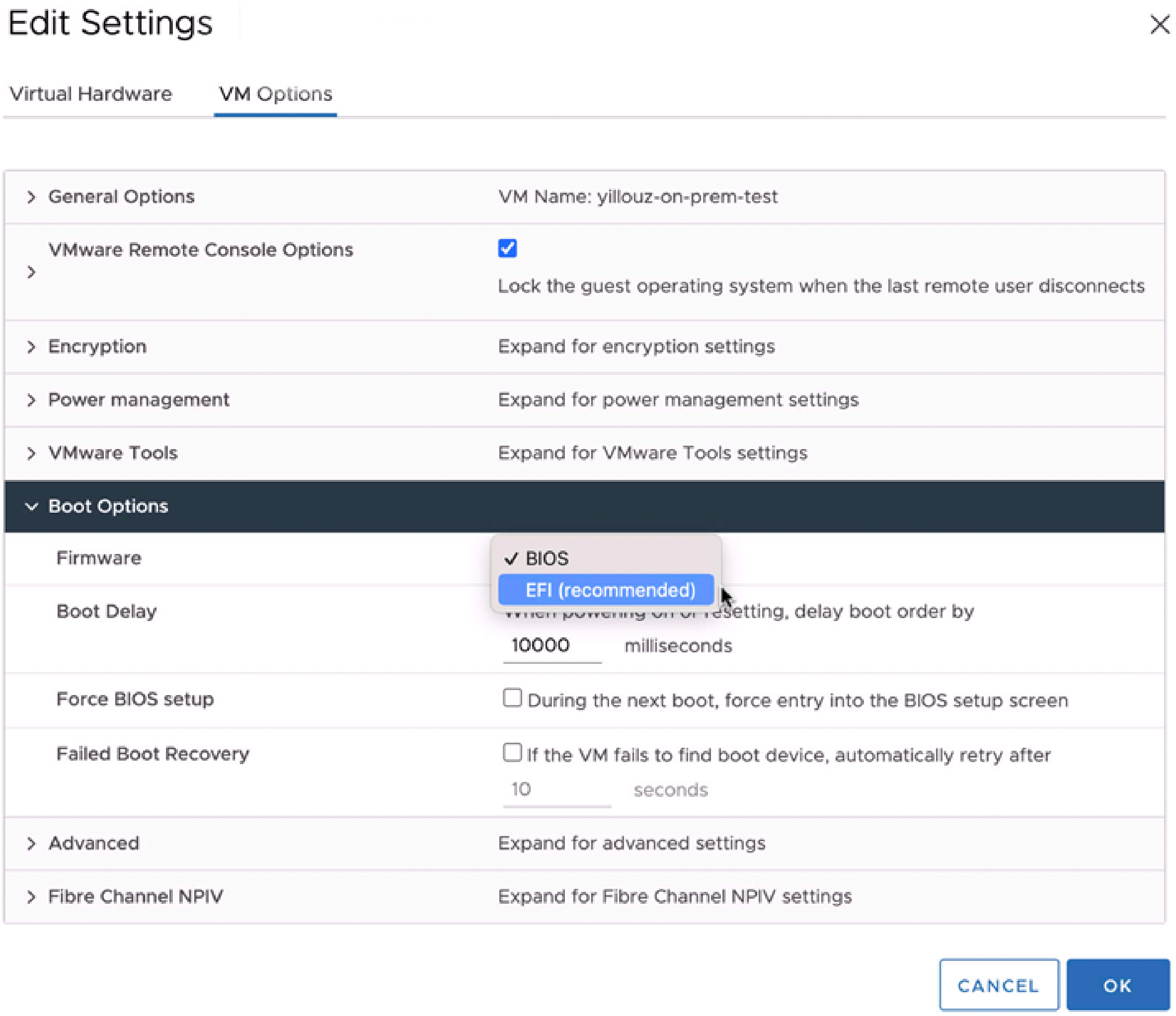
Select a guest OS
Choose the guest OS that will be installed on the virtual machine

Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.

Guest OS Family: Linux

Guest OS Version: Other 4.x Linux (64-bit)

d. In the Virtual Machine *Boot Options*, select *BIOS* under *Firmware*, and click *OK*.



Edit Settings

› General Options	VM Name: yillouz-on-prem-test
› VMware Remote Console Options	☑ Lock the guest operating system when the last remote user disconnects
› Encryption	Expand for encryption settings
› Power management	Expand for power management settings
› VMware Tools	Expand for VMware Tools settings
⌄ Boot Options	
Firmware	✓ BIOS EFI (recommended)
Boot Delay	When powering on or resetting, delay boot order by 10000 milliseconds
Force BIOS setup	□ During the next boot, force entry into the BIOS setup screen
Failed Boot Recovery	□ If the VM fails to find boot device, automatically retry after 10 seconds
› Advanced	Expand for advanced settings
› Fibre Channel NPIV	Expand for Fibre Channel NPIV settings

e. In the *Customize hardware* step, do the following:

a. Enter the values for *CPU*, *Memory*, and *New Hard disk* fields as specified in *Prerequisites*. It is highly recommended to use SSD for hard disk.

b. Add an OS disk in the *New Hard disk*:

a. Enter the OS disk size in GB, as specified in *Prerequisites*.

b. In the *Disk Provisioning* field, it is recommended to select *Thick Provision*.

c. Add a DATA disk in the *New Hard disk*:

a. Enter the DATA disk size in GB, as specified in *Prerequisites*.

b. In the *Disk Provisioning* field, it is recommended to select *Thick Provision*.

c. In case the previous disk hasn't been installed as SSD, define another SSD DATA disk of a size as specified in *Prerequisites*.

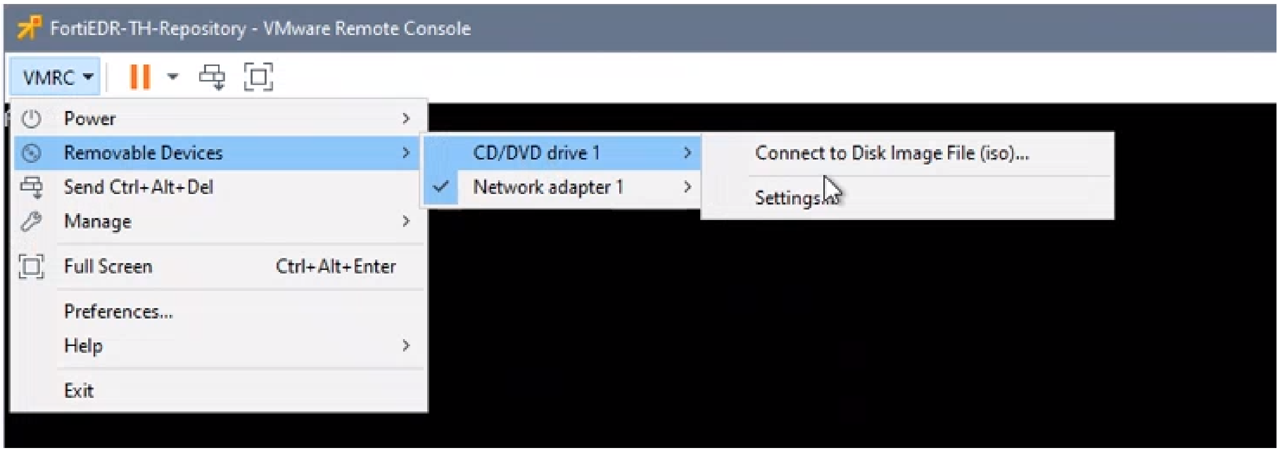
d. In the *New Network* field, choose *VMXNET3*.

4. Select *Finish* to complete the creation of the virtual machine.

Installing an Operating System ISO

To install an operating system ISO:

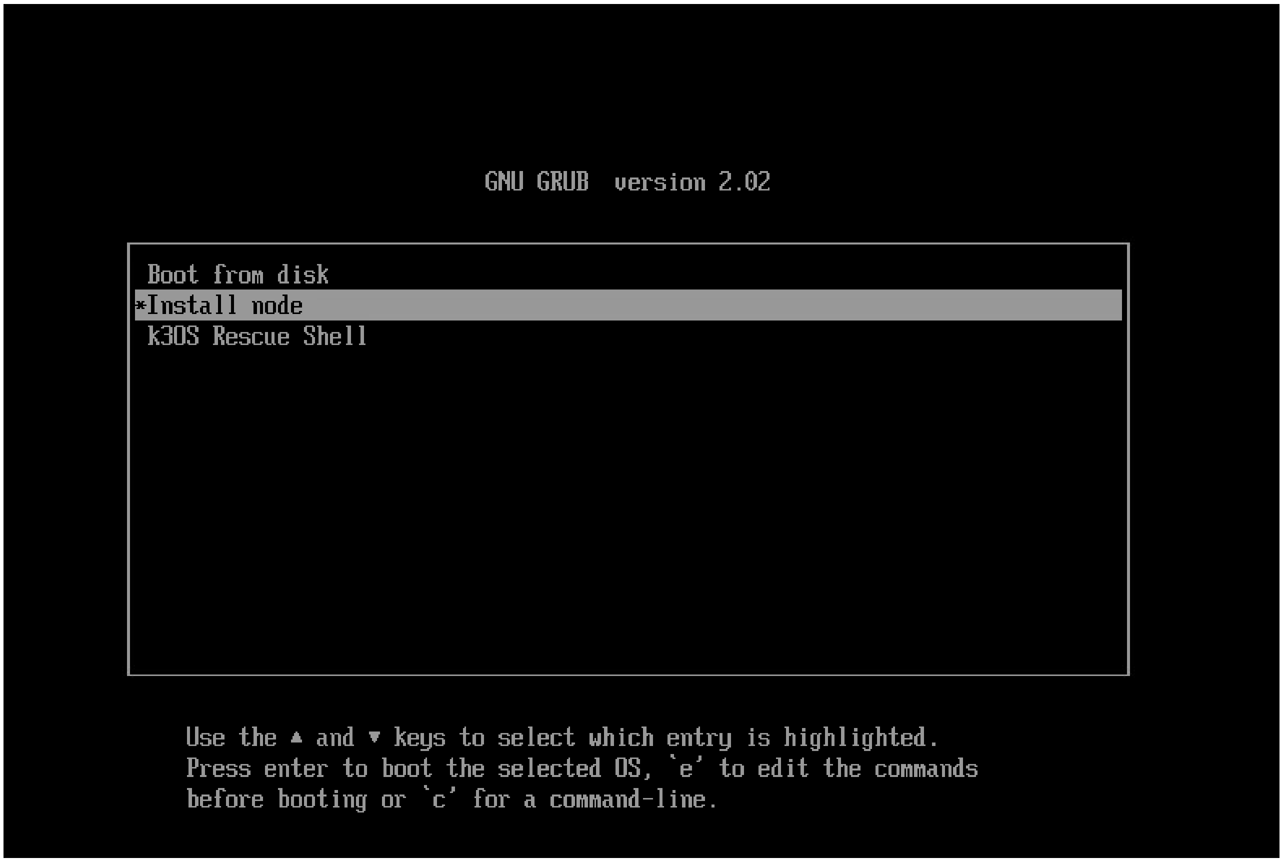
1. Select the newly created virtual machine and click **Launch Remote Console**.
2. In the *VMRC* menu, select *Removable Device > CD/DVE drive 1 > Connect to Disk Image File (iso)...*.



3. Select the *FortiEDR_Repository_OSInstaller* ISO file and click *Open*. Make sure that the ISO remains mounted.

Another option instead of completing the two steps described above is to upload the ISO from the VMWare datastore (this is possible if the ISO has already been uploaded there).

4. Restart the Virtual Machine. The virtual machine starts and the following menu is displayed:



```
GNU GRUB  version 2.02

 Boot from disk
*Install node
 k3OS Rescue Shell

Use the ▲ and ▼ keys to select which entry is highlighted.
Press enter to boot the selected OS, `e' to edit the commands
before booting or `c' for a command-line.
```

5. Select the *Install Node* option.
6. Configure the timezone of the VM using the following command:

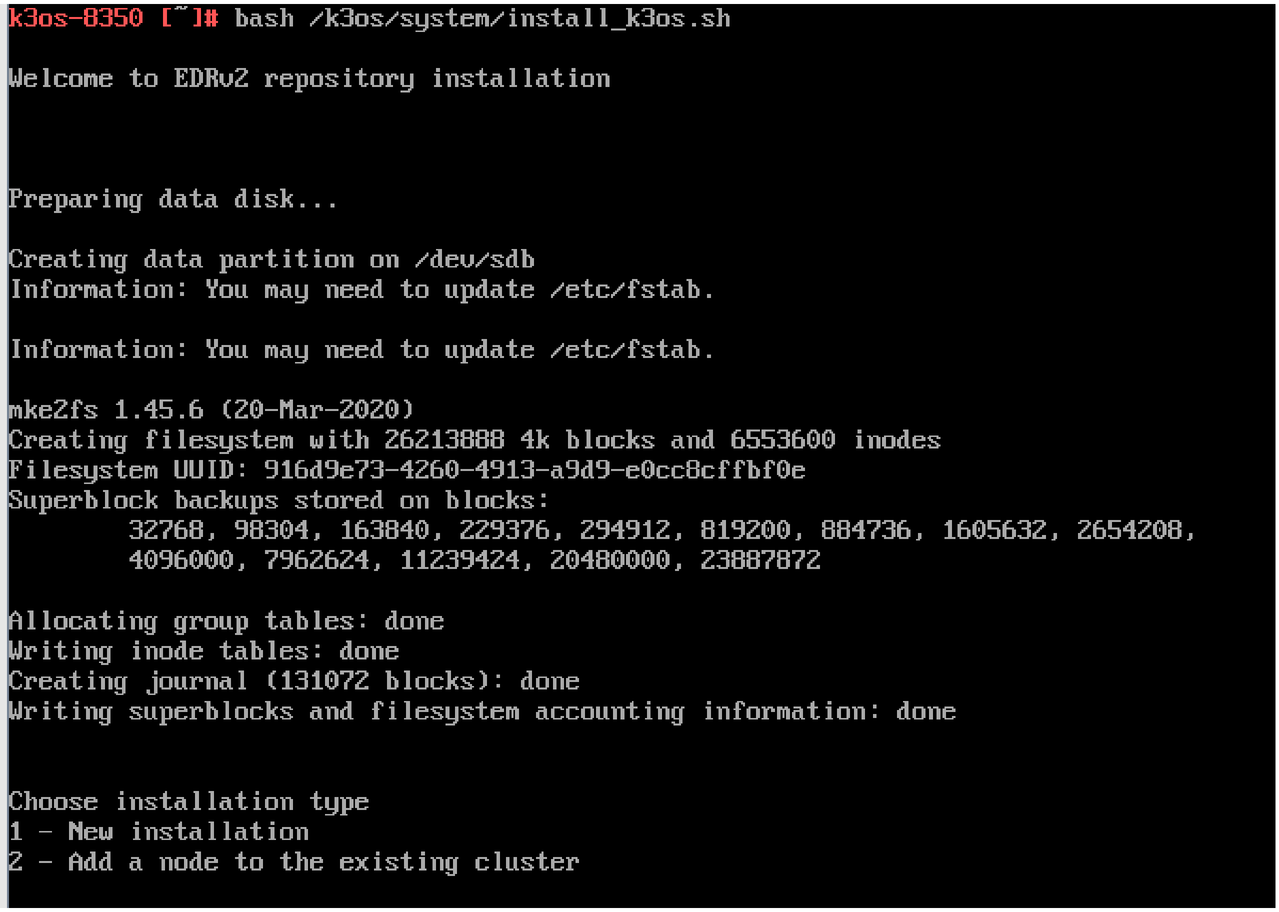
```
sudo su –

export TIMEZONE=Area/Location
```

Replace *Area/Location* with the time zone value from the tz (timezone) database used by Linux and other Unix systems.

The default timezone UTC will be used if you skip this step. The timezone can only be set here once and cannot be changed after the installation.

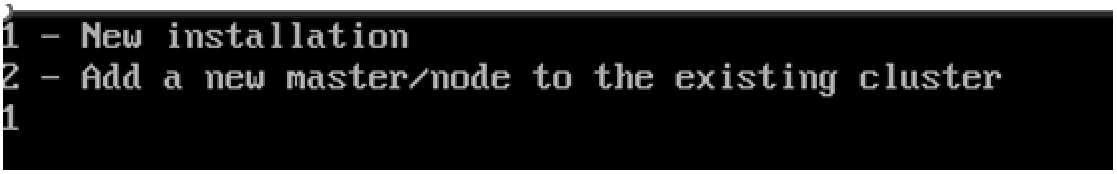
7. Log in using the *rancher* user (without the password) and run the following commands in order to start the K8S node installation:

```
sudo su –

bash /k3os/system/install_k3os.sh
```



```
k3os-8350 [~]# bash /k3os/system/install_k3os.sh

Welcome to EDRv2 repository installation



Preparing data disk...

Creating data partition on /dev/sdb
Information: You may need to update /etc/fstab.

Information: You may need to update /etc/fstab.

mke2fs 1.45.6 (20-Mar-2020)
Creating filesystem with 26213888 4k blocks and 6553600 inodes
Filesystem UUID: 916d9e73-4260-4913-a9d9-e0cc8cffbf0e
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
        4096000, 7962624, 11239424, 20480000, 23887872

Allocating group tables: done
Writing inode tables: done
Creating journal (131072 blocks): done
Writing superblocks and filesystem accounting information: done


Choose installation type
1 - New installation
2 - Add a node to the existing cluster
```

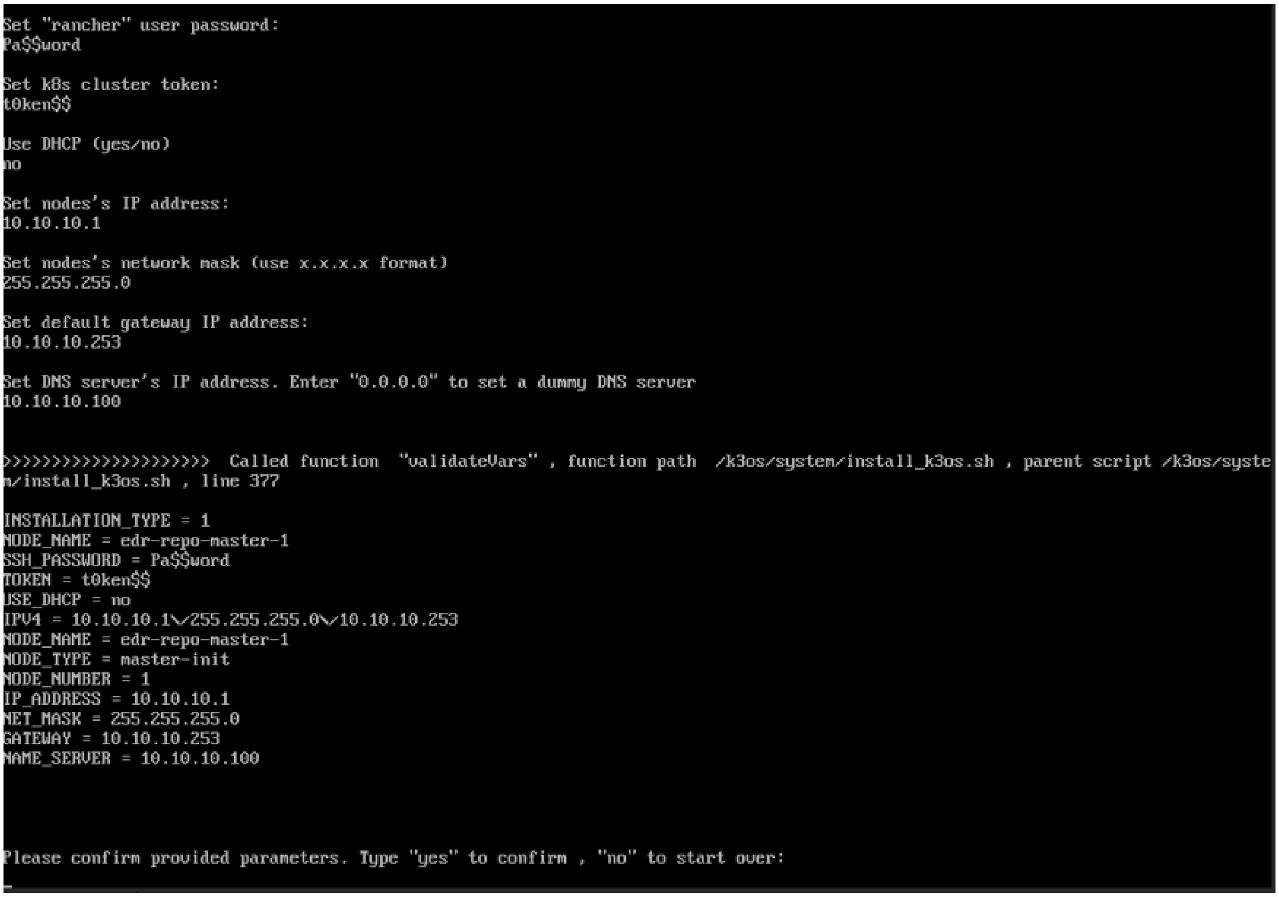
8. When prompted with the following, enter the number depending on the virtual machine (node) you are installing:



```
1 - New installation
2 - Add a new master/node to the existing cluster
1
```

- Enter 1 if you are installing one single virtual machine (node) with fewer than 15000 seats or if you are installing the first virtual machine (node) of the three for 15000 to 30000 seats.
- Enter 2 if you are installing the second or third virtual machine (node) of the three for 15000 to 30000 seats.

9. Complete the *k3os* installation by providing the following parameters:



```
Set "rancher" user password:
Pa$$word

Set k8s cluster token:
t0ken$$

Use DHCP (yes/no)
no

Set nodes's IP address:
10.10.10.1

Set nodes's network mask (use x.x.x.x format)
255.255.255.0

Set default gateway IP address:
10.10.10.253

Set DNS server's IP address. Enter "0.0.0.0" to set a dummy DNS server
10.10.10.100


>>>>>>>>>>>>>>>>>>>>>  Called function  "validateVars" , function path  /k3os/system/install_k3os.sh , parent script /k3os/syste
m/install_k3os.sh , line 377

INSTALLATION_TYPE = 1
NODE_NAME = edr-repo-master-1
SSH_PASSWORD = Pa$$word
TOKEN = t0ken$$
USE_DHCP = no
IPV4 = 10.10.10.1\/255.255.255.0\/10.10.10.253
NODE_NAME = edr-repo-master-1
NODE_TYPE = master-init
NODE_NUMBER = 1
IP_ADDRESS = 10.10.10.1
NET_MASK = 255.255.255.0
GATEWAY = 10.10.10.253
NAME_SERVER = 10.10.10.100



Please confirm provided parameters. Type "yes" to confirm , "no" to start over:
_
```

   a. When prompted to enter the *SSH password*, enter the password to be used for the rancher user. A strong password must be entered.
   b. At the *Use DHCP (yes/no)* prompt, enter *no*.

> Using DHCP causes a malfunction of the FortiEDR Repository server so that it is in an *Offline* state after the installation. When prompted, enter the IP, Mask and Gateway details of the virtual machine.

   c. At the *Do you want to change the default Pod network CIDR's* prompt, enter *yes* or *no* depending on your needs. The default Kubernetes internal Pod network is `10.42.0.0/16`.
      i. If you enter *yes*, provide the desired Pod network subnet in `x.x.0.0/16` format when prompted.
      ii. If you enter *no*, make sure the default Pod network CIDR does not overlap with your existing networks.
   d. At the *Do you want to change the default Service network CIDR's* prompt, enter *yes* or *no* depending on your needs. The default Kubernetes internal Service network is `10.43.0.0/16`.
      i. If you enter *yes*, provide the desired Service network subnet in `x.x.0.0/16` format when prompted.
      ii. If you enter *no*, make sure the default Service network CIDR does not overlap with your existing networks.
   e. When prompted to enter *node IP*, enter an IP depending on the virtual machine (node) you are installing:

- If you are installing one single virtual machine (node) with fewer than 15000 seats or if you are installing the first virtual machine (node) of the three for 15000 to 30000 seats, enter the virtual IP address.
- If you are installing the second or third virtual machine (node) of the three for 15000 to 30000 seats, enter the virtual IP address you defined for the first virtual machine (node).

f. When prompted to enter *subnet mask*, provide the virtual machine subnet mask.

g. When prompted to enter *DNS*, provide the DNS details.

h. When asked, read the settings provided and approve or reject them.

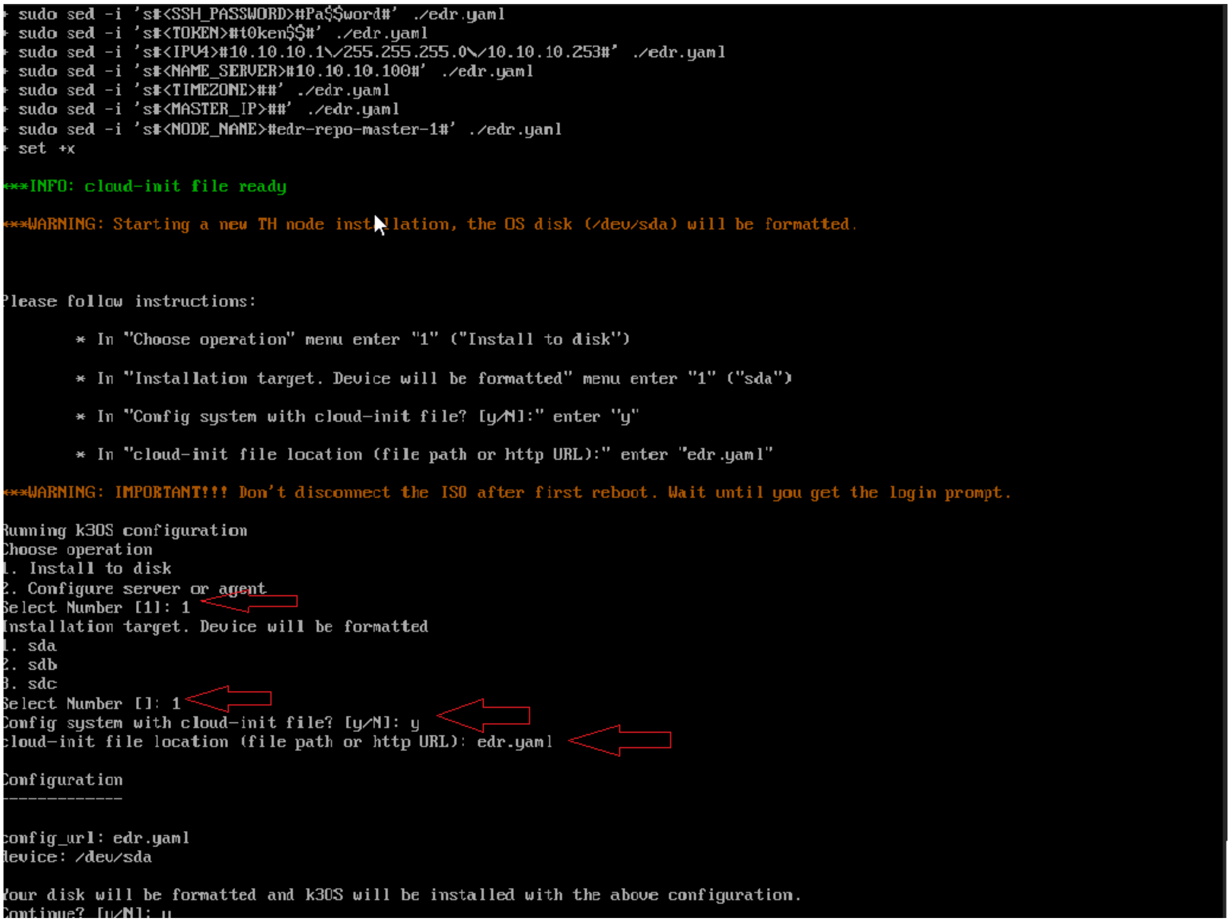
i. When prompted to select an operation, approve the default (*1. Install to disk*) by pressing `Enter`.

j. To select the *sda disk* as the *OS disk*, select *1*.

k. At the *Config system with cloud-init file* prompt, enter y.

l. When prompted to provide a *Cloud-init file location (file path or http URL)*, enter `edr.yaml`.

m. When prompted to continue, enter y.
The image below provides a preview of the parameters you entered for a master virtual machine (node).

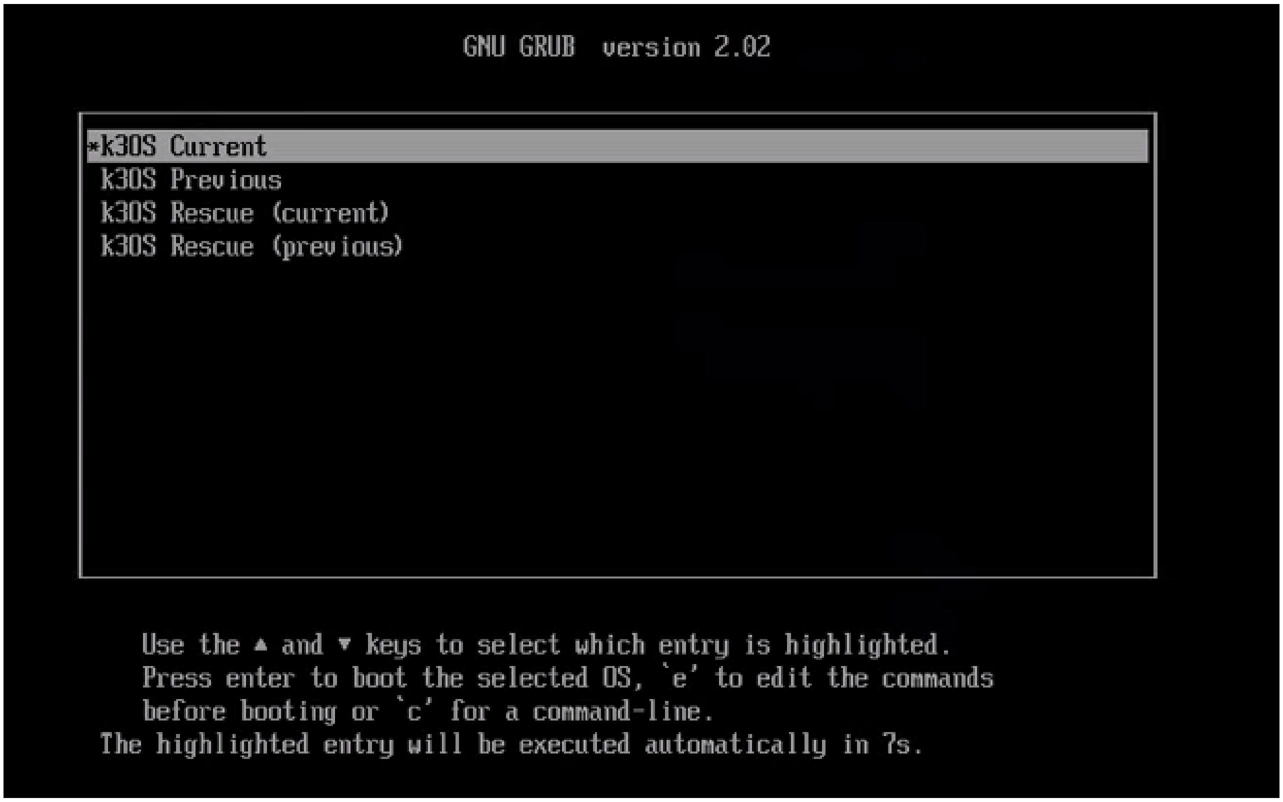


```
+ sudo sed -i 's#<SSH_PASSWORD>#Pa$$word#' ./edr.yaml
+ sudo sed -i 's#<TOKEN>#t0ken$$#' ./edr.yaml
+ sudo sed -i 's#<IPV4>#10.10.10.1\/255.255.255.0\/10.10.10.253#' ./edr.yaml
+ sudo sed -i 's#<NAME_SERVER>#10.10.10.100#' ./edr.yaml
+ sudo sed -i 's#<TIMEZONE>##' ./edr.yaml
+ sudo sed -i 's#<MASTER_IP>##' ./edr.yaml
+ sudo sed -i 's#<NODE_NAME>#edr-repo-master-1#' ./edr.yaml
+ set +x

***INFO: cloud-init file ready

***WARNING: Starting a new TH node installation, the OS disk (/dev/sda) will be formatted.


Please follow instructions:

        * In "Choose operation" menu enter "1" ("Install to disk")

        * In "Installation target. Device will be formatted" menu enter "1" ("sda")

        * In "Config system with cloud-init file? [y/N]:" enter "y"

        * In "cloud-init file location (file path or http URL):" enter "edr.yaml"

***WARNING: IMPORTANT!!! Don't disconnect the ISO after first reboot. Wait until you get the login prompt.

Running k3OS configuration
Choose operation
1. Install to disk
2. Configure server or agent
Select Number [1]: 1
Installation target. Device will be formatted
1. sda
2. sdb
3. sdc
Select Number []: 1
Config system with cloud-init file? [y/N]: y
cloud-init file location (file path or http URL): edr.yaml

Configuration
-------------

config_url: edr.yaml
device: /dev/sda

Your disk will be formatted and k3OS will be installed with the above configuration.
Continue? [y/N]: y
```

10. Wait for the installation to complete which may take a while. The Virtual Machine restarts automatically after the installation.

11. If you have 15000 to 30000 seats, define two additional virtual machines (nodes) by repeating the steps in *Creating a virtual machine* and the previous steps in *Installing an Operating System ISO* for each node. Otherwise, skip to the next step.

12. In the menu, select the default option *k30S Current* and press *Enter*.

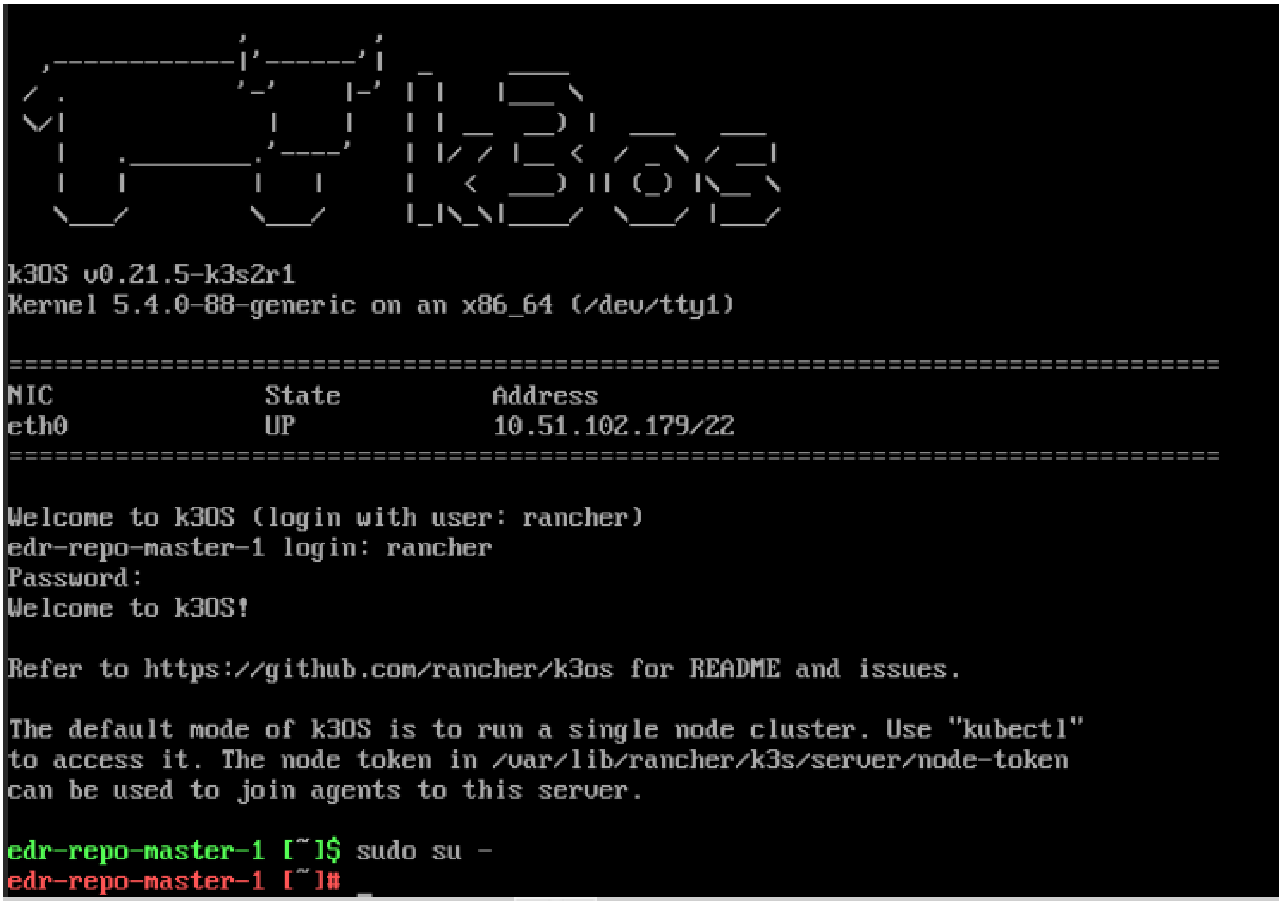


```
                      GNU GRUB  version 2.02

 *k3OS Current
  k3OS Previous
  k3OS Rescue (current)
  k3OS Rescue (previous)

      Use the ▲ and ▼ keys to select which entry is highlighted.
      Press enter to boot the selected OS, `e' to edit the commands
      before booting or `c' for a command-line.
   The highlighted entry will be executed automatically in 7s.
```

The system will start. This might take a few minutes while OS data is copied to the Virtual Machine.

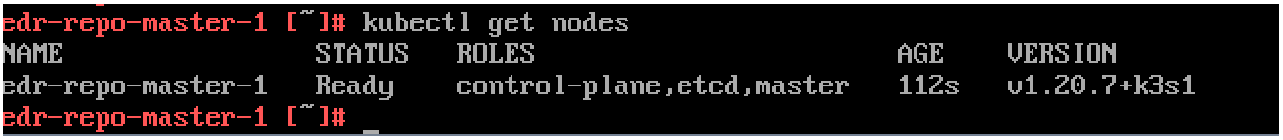
13. Log in with the `rancher` name and the password set previously.

14. Run the `sudo su -` command.



```
k3OS v0.21.5-k3s2r1
Kernel 5.4.0-88-generic on an x86_64 (/dev/tty1)

================================================================================
NIC               State          Address
eth0              UP             10.51.102.179/22
================================================================================

Welcome to k3OS (login with user: rancher)
edr-repo-master-1 login: rancher
Password:
Welcome to k3OS!

Refer to https://github.com/rancher/k3os for README and issues.

The default mode of k3OS is to run a single node cluster. Use "kubectl"
to access it. The node token in /var/lib/rancher/k3s/server/node-token
can be used to join agents to this server.

edr-repo-master-1 [~]$ sudo su -
edr-repo-master-1 [~]# _
```

15. Verify the installation is successful by running the `kubectl get nodes` command and checking that the status of *edr-repo-master1* is *Ready*, as shown below. If you installed three nodes, verify that the status of the other two nodes are *Ready* as well.

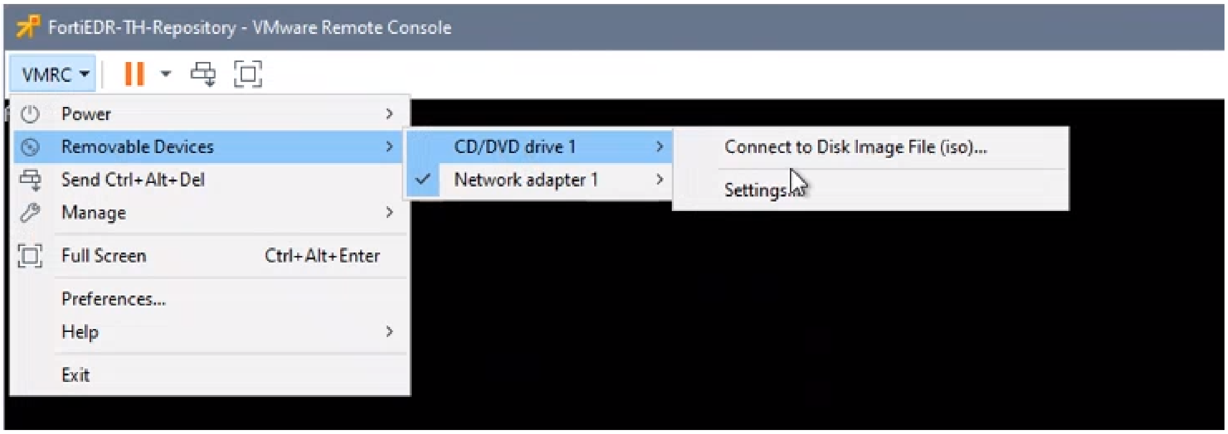


```
edr-repo-master-1 [~]# kubectl get nodes
NAME                STATUS   ROLES                       AGE    VERSION
edr-repo-master-1   Ready    control-plane,etcd,master   112s   v1.20.7+k3s1
edr-repo-master-1 [~]# _
```

Installing a FortiEDR Repository software ISO

To install the FortiEDR Repository Software ISO:

1. Launch the *FortiEDR_RepositoryInstaller* ISO file:
   a. From the *VMRC* menu, select *Removable Device > CD/DVD drive 1 > Connect to Disk Image File (iso)...*.



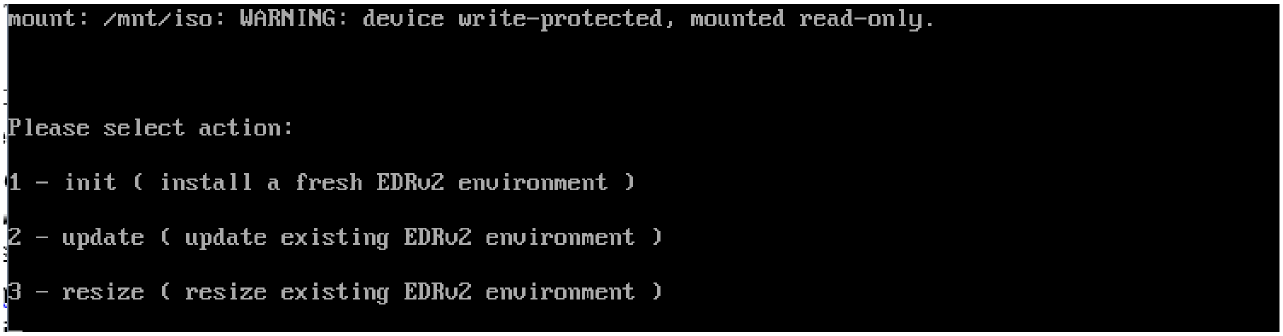
b. Select the *FortiEDR_RepositoryInstaller* ISO file and click on *Open*. If the ISO has already been uploaded to the VMware datastore, you can also upload the ISO from there.

If mounting the new ISO appears to freeze the system, check if there is a prompt to disconnect the existing ISO. If yes, select *yes* to disconnect the existing ISO and then try mounting the new ISO again by repeating steps a and b.

2. Run the following command:

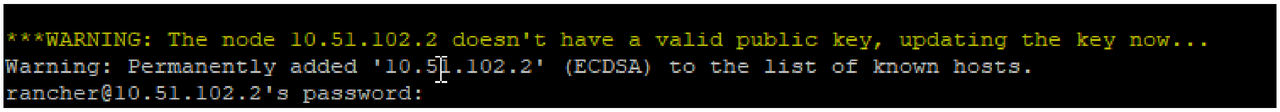
```
bash /k3os/system/install_edr2.sh
```

Select *init* (1) for a new installation.



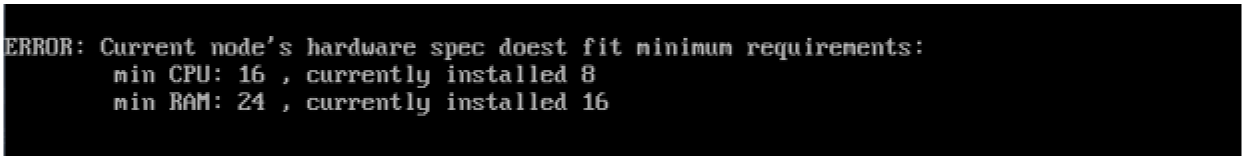
```
mount: /mnt/iso: WARNING: device write-protected, mounted read-only.


Please select action:

1 - init ( install a fresh EDRv2 environment )

2 - update ( update existing EDRv2 environment )

3 - resize ( resize existing EDRv2 environment )
```

The node is being synchronized, which might take 10 to 15 minutes. If you installed three nodes, you will be prompted for the SSH password for each node.



```
***WARNING: The node 10.51.102.2 doesn't have a valid public key, updating the key now...
Warning: Permanently added '10.51.102.2' (ECDSA) to the list of known hosts.
rancher@10.51.102.2's password:
```

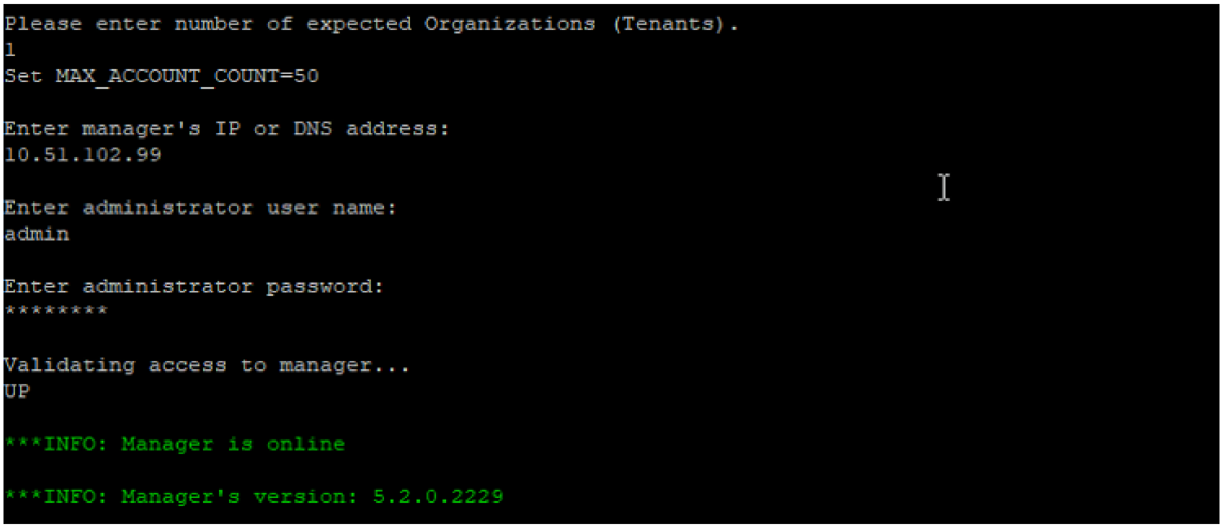
Existing virtual machine specifications (CPU and RAM) are being validated. If one is found to be lower than the minimum requirements for proper functioning of the FortiEDR Repository, the following warning appears:



```
ERROR: Current node's hardware spec doest fit minimum requirements:
       min CPU: 16 , currently installed 8
       min RAM: 24 , currently installed 16
```

Wait until the required container images are imported from ISO to the local image storage (might take few minutes).

3. Complete the FortiEDR Repository software installation by providing the following parameters:
   - When prompted to enter the *number of seats*, enter the number of seats of your FortiEDR License (workstations and servers).
   - When prompted to specify whether the repository will be used by a *Managed Security Service Provider (MSSP)*, enter yes if you are going to define organizations, or no if you are not.

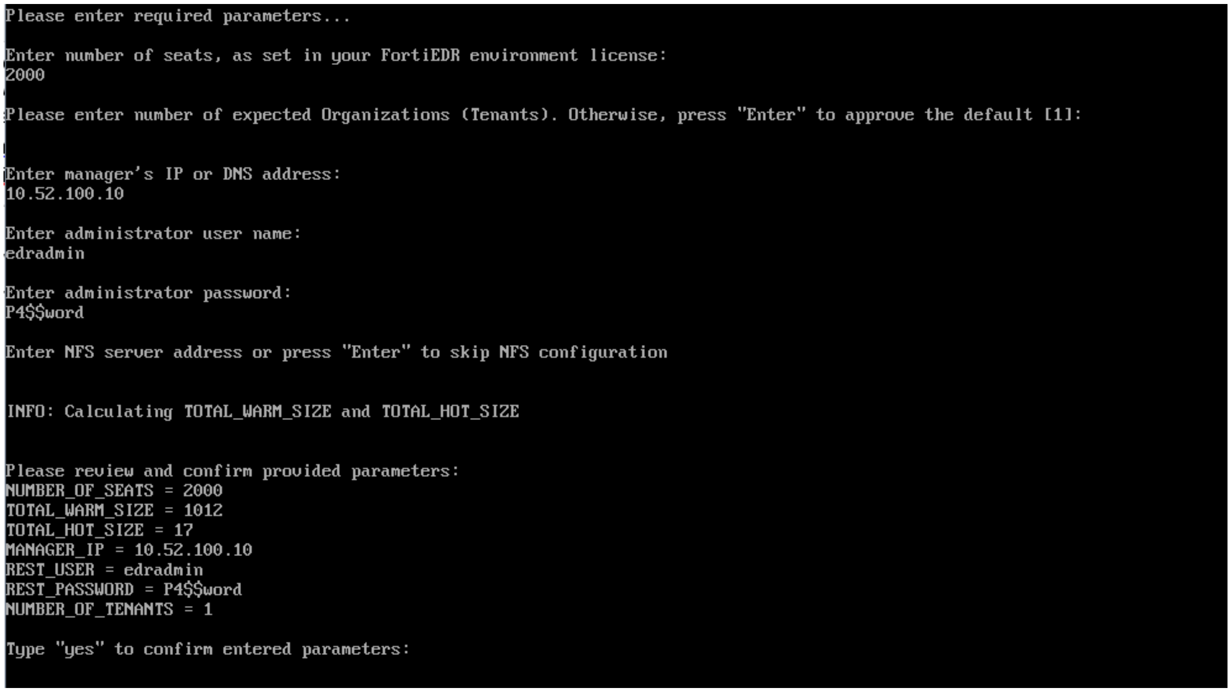


```
Please enter number of expected Organizations (Tenants).
1
Set MAX_ACCOUNT_COUNT=50

Enter manager's IP or DNS address:
10.51.102.99

Enter administrator user name:
admin

Enter administrator password:
********

Validating access to manager...
UP

***INFO: Manager is online

***INFO: Manager's version: 5.2.0.2229
```

   - If you entered yes in the previous question, provide the number of expected organizations (meaning Tenants).
   - When prompted for the FortiEDR Manager details, provide its IP and the credentials of one of the FortiEDR Console administrators that have Rest API permissions.

Make sure that the Threat Hunting repository does not block outbound traffic to port 443 on Central Manager.

   - Review the displayed configuration. Type *yes* to approve it or if the parameters are not correct, press *Enter* to restart the configuration process. The installation may take several minutes.



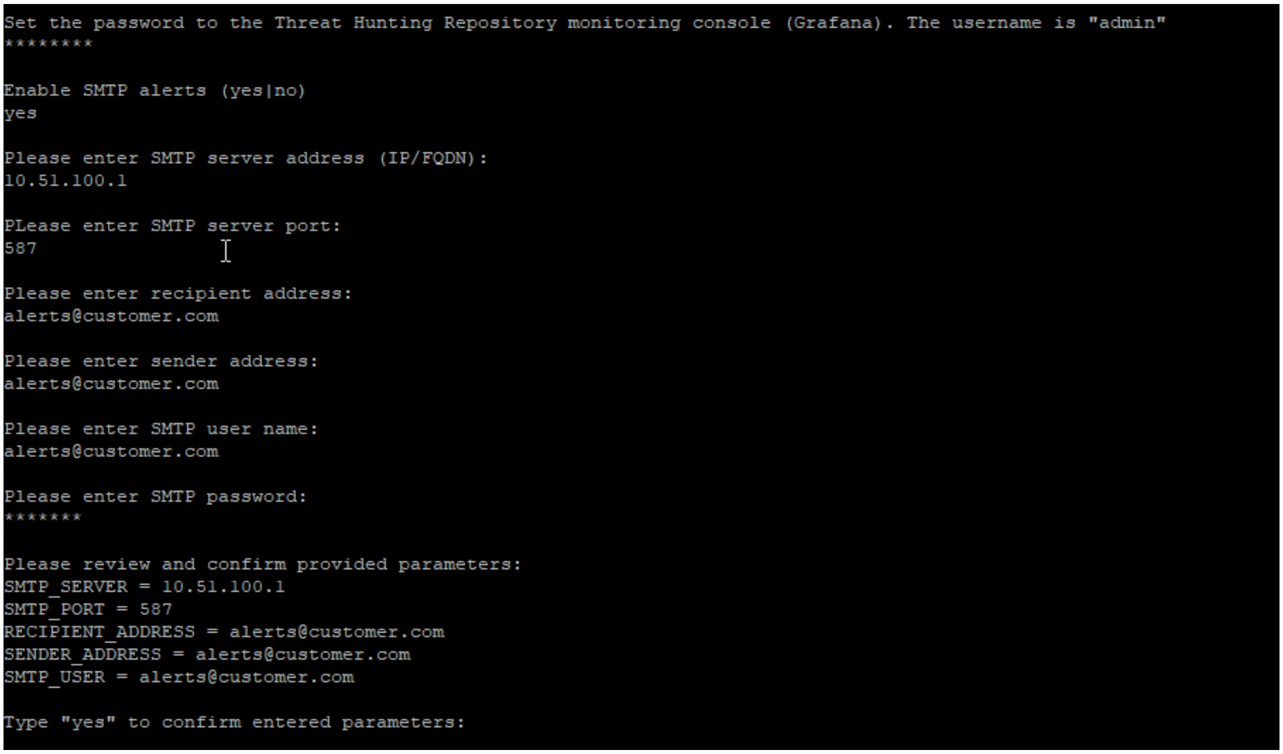
```
Please enter required parameters...

Enter number of seats, as set in your FortiEDR environment license:
2000

Please enter number of expected Organizations (Tenants). Otherwise, press "Enter" to approve the default [1]:


Enter manager's IP or DNS address:
10.52.100.10

Enter administrator user name:
edradmin

Enter administrator password:
P4$$word

Enter NFS server address or press "Enter" to skip NFS configuration


INFO: Calculating TOTAL_WARM_SIZE and TOTAL_HOT_SIZE


Please review and confirm provided parameters:
NUMBER_OF_SEATS = 2000
TOTAL_WARM_SIZE = 1012
TOTAL_HOT_SIZE = 17
MANAGER_IP = 10.52.100.10
REST_USER = edradmin
REST_PASSWORD = P4$$word
NUMBER_OF_TENANTS = 1

Type "yes" to confirm entered parameters:
```

Configuring the Threat Hunting Repository Monitoring console

To configure and access the Threat Hunting Repository Monitoring console:

1. When prompted, provide the password to be used for the Threat Hunting Repository monitoring console (Grafana) login. Note that the password should be a combination of letters and digits.
2. When asked whether to enable SMTP alerts, enter yes if you want to receive alert emails triggered by the Threat Hunting Repository monitoring. Otherwise, enter no and skip to step 7.
3. When prompted, provide the following information of the SMTP server:
   a. Details of the SMTP server (IP or FQDN, and port)
   b. Email address to send the alerts
   c. Email sender address
   d. Username and password required for the SMTP server access

4. When prompted, review the provided details and confirm.



```
Set the password to the Threat Hunting Repository monitoring console (Grafana). The username is "admin"
********

Enable SMTP alerts (yes|no)
yes

Please enter SMTP server address (IP/FQDN):
10.51.100.1

PLease enter SMTP server port:
587

Please enter recipient address:
alerts@customer.com

Please enter sender address:
alerts@customer.com

Please enter SMTP user name:
alerts@customer.com

Please enter SMTP password:
*******

Please review and confirm provided parameters:
SMTP_SERVER = 10.51.100.1
SMTP_PORT = 587
RECIPIENT_ADDRESS = alerts@customer.com
SENDER_ADDRESS = alerts@customer.com
SMTP_USER = alerts@customer.com

Type "yes" to confirm entered parameters:
```

Backing up Threat Hunting Repository data

Fortinet recommends that you back up the data stored in the Threat Hunting Repository database by replicating it to a NFS server, which can be used in for disaster recovery.

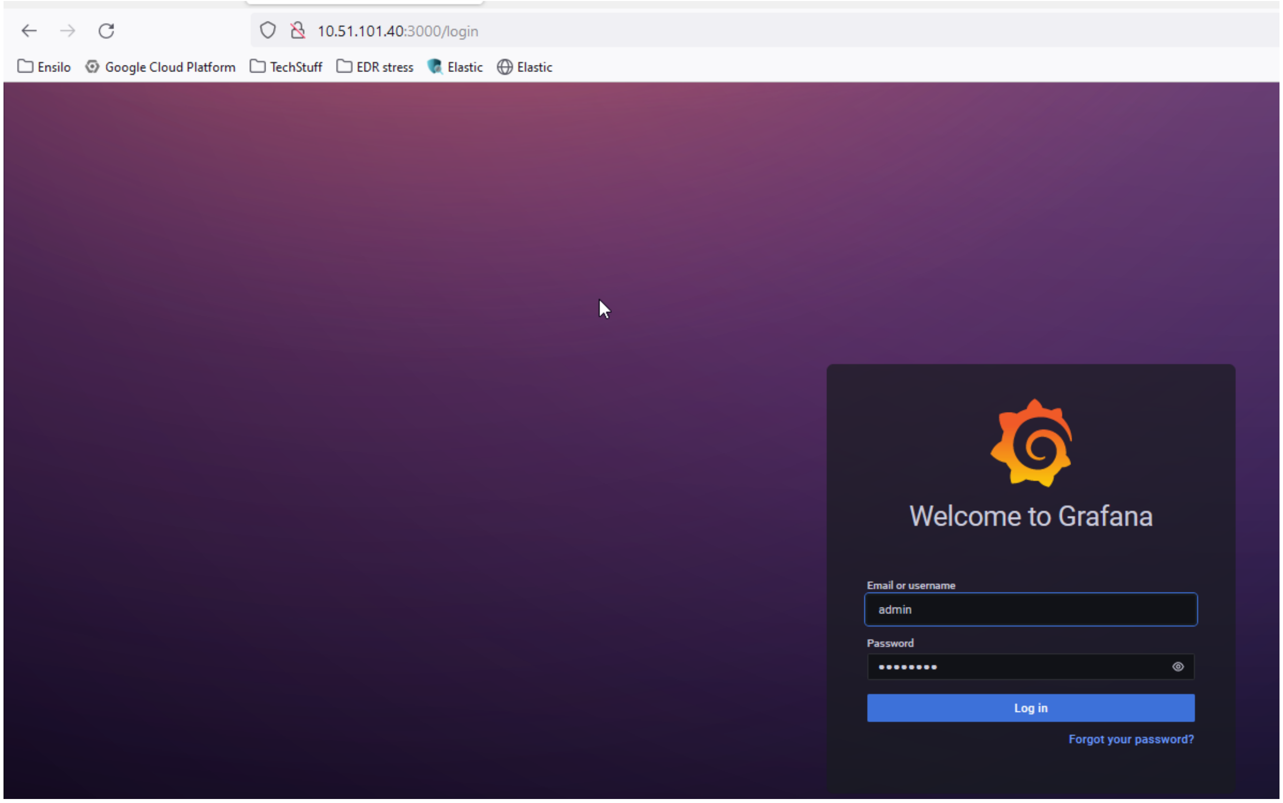
- The size of the NFS storage must be at least 55% of the total size of your Repository storage.
- The time to back up the data depends on the amount of data being copied over from the Repository database to the NFS server.
- When a piece of data is deleted from the Threat Hunting Repository storage due to retention, the backup copy of that piece of data, if exists, is deleted from the NFS server as well.

To enable backup of data, provide details about the backup storage in the CLI:

1. At the prompted question, enter yes.
2. When prompted, enter the NFS server address.
3. When prompted, enter the NFS share path to which the data will be replicated.

Activating the Threat Hunting Repository Monitoring console

1. Visit `http://<TH IP>:3000`.

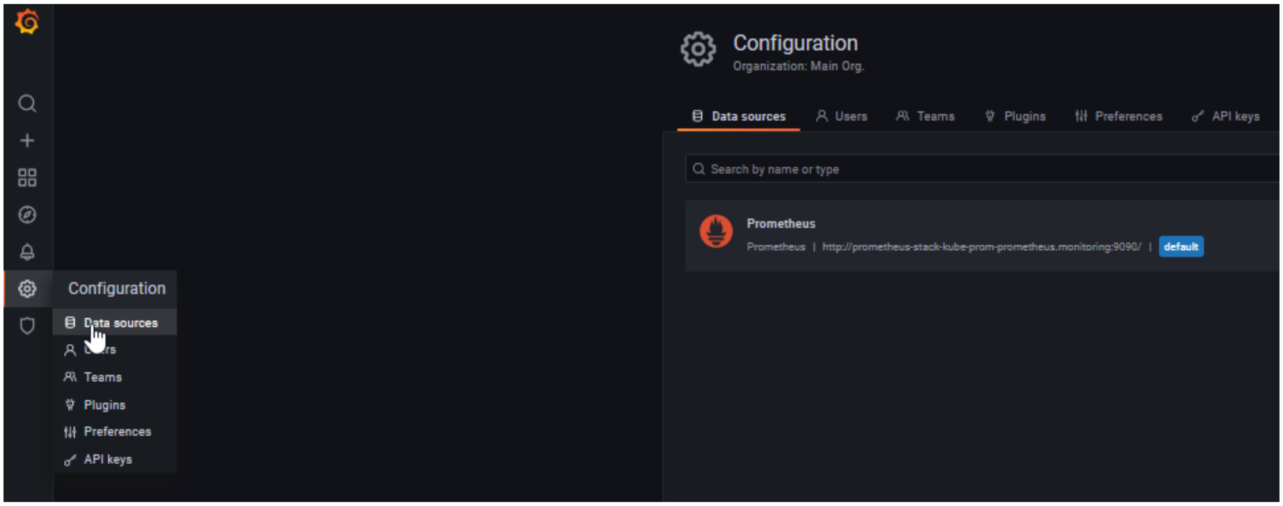


10.51.101.40:3000/login

Email or username: admin

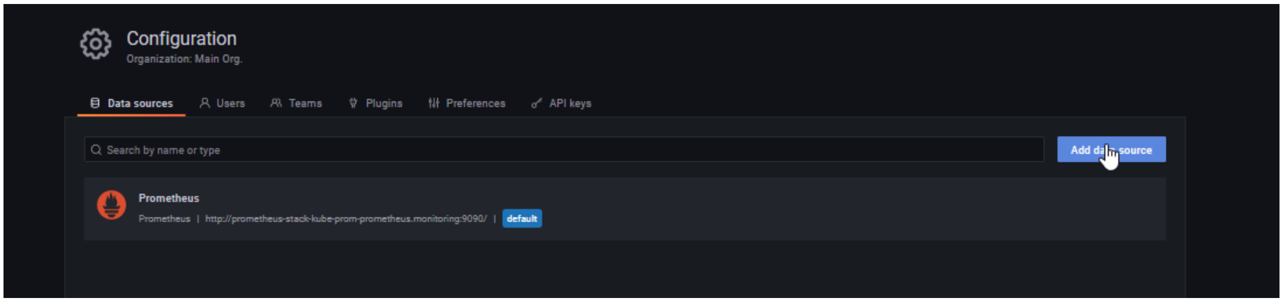
Password: ••••••••••

2. Enter the user and password that you provided during the initial installation setup.
3. Go to *Configuration* > *Data sources*.

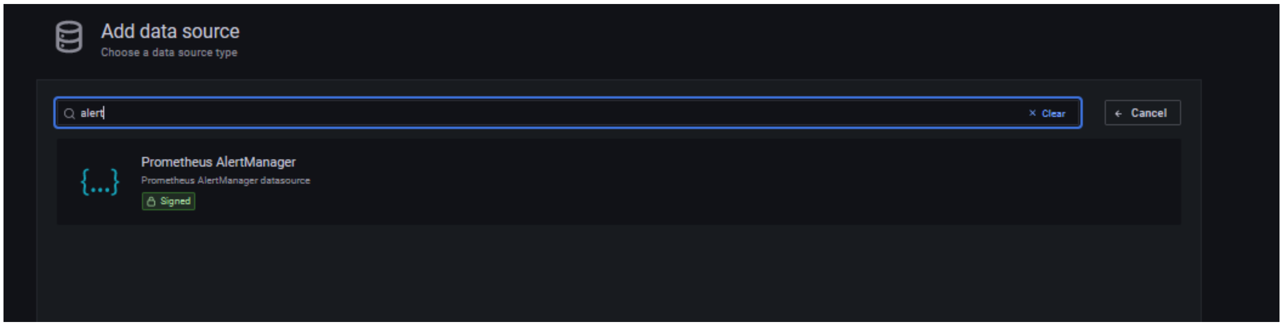


Prometheus
Prometheus | http://prometheus-stack-kube-prom-prometheus.monitoring:9090/ | default

4. Click *Add data source*.

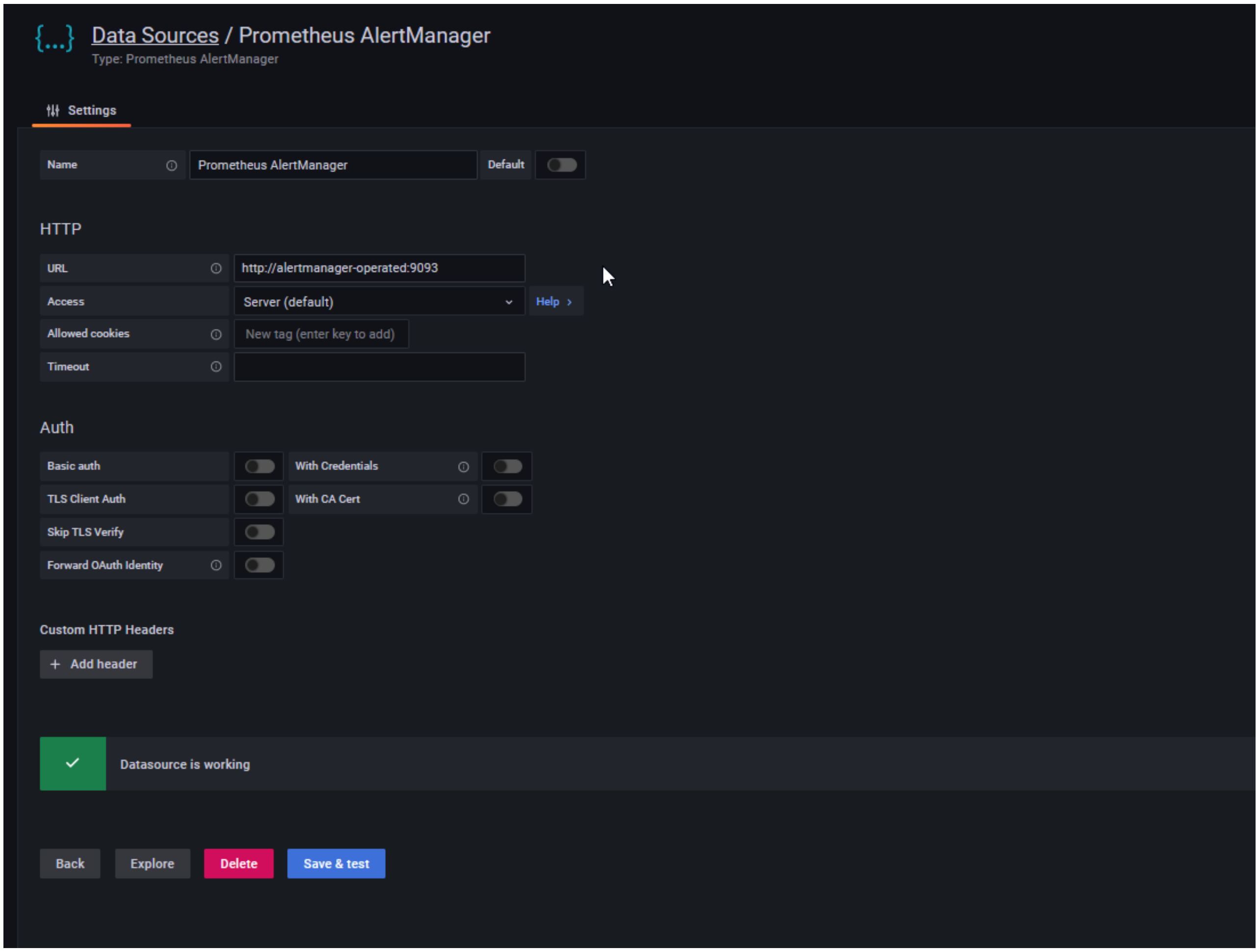


5. Select *Prometheus AlertManager*.



6. In the *URL* field, enter `http://alertmanager-operated:9093`.

7. Click *Save & test*.



Data Sources / Prometheus AlertManager

Type: Prometheus AlertManager

Name: Prometheus AlertManager

HTTP

URL: http://alertmanager-operated:9093

Access: Server (default)

Allowed cookies: New tag (enter key to add)

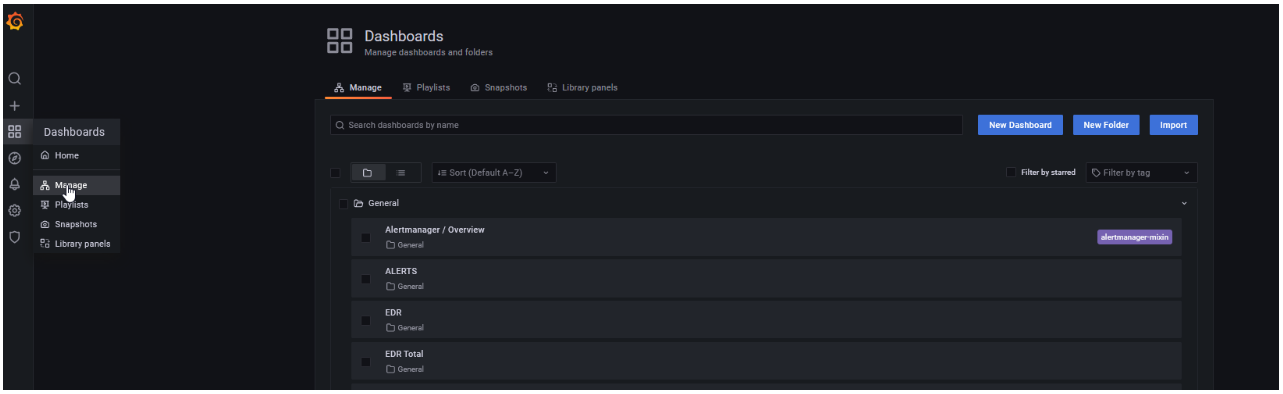
Timeout:

Auth

Custom HTTP Headers

Datasource is working

8. Under *Dashboards > Manage*:



Dashboards

Manage dashboards and folders

General

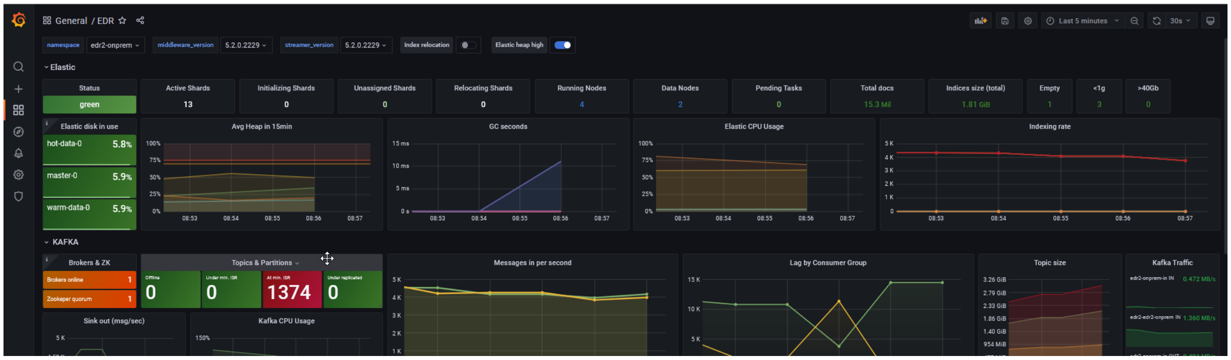
Alertmanager / Overview — General — alertmanager-mixin

ALERTS — General

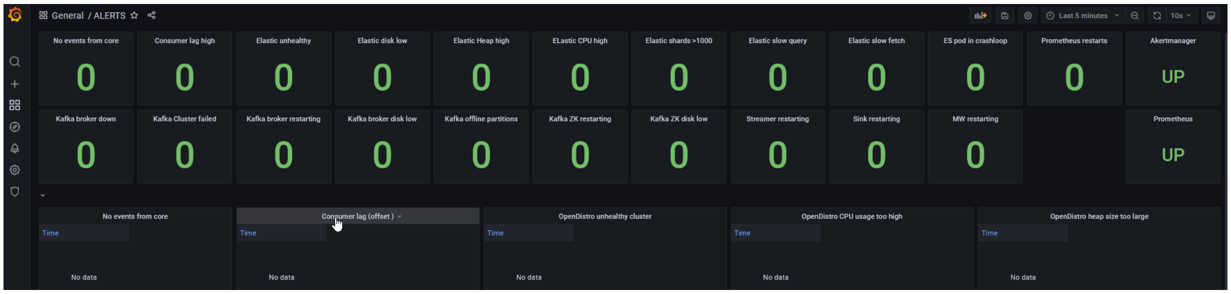
EDR — General

EDR Total — General

- Open the *EDR* dashboard to view the current status of threat hunting.



- Open the *Alerts* dashboard to view alerts triggered by the Threat Hunting Repository monitoring system.



The following table lists all the alerts and the mitigation methods.

Alert	Mitigation
No events from core	Verify that all Cores are an running by using the FortiEDR Manager.

Alert	Mitigation
Consumer Lag (offset)	Contact Fortinet Support.
OpenDistro Unhealthy Cluster	
OpenDistro CPU usage too high	
OpenDistro heap size too large	
OpenDistro too many shards per node	
OpenDistro slow search query	
OpenDistro slow search fetch	
OpenDistro disk usage	
ES pod in crashloop	
Kafka Offline Partitions	
Kafka broker is down	
Kafka cluster failed	
Kafaka broker restart rate high	
Kafka broker disk low	
ZooKeeper disk low	
Streamer restart rate high	
StreamerSink restart rate high	
ZooKeeper restart too often	
Streamer MAX HPA	
Streamer unreached desired HPA	
Middleware restart rate high	

Setting up the FortiEDR reputation server

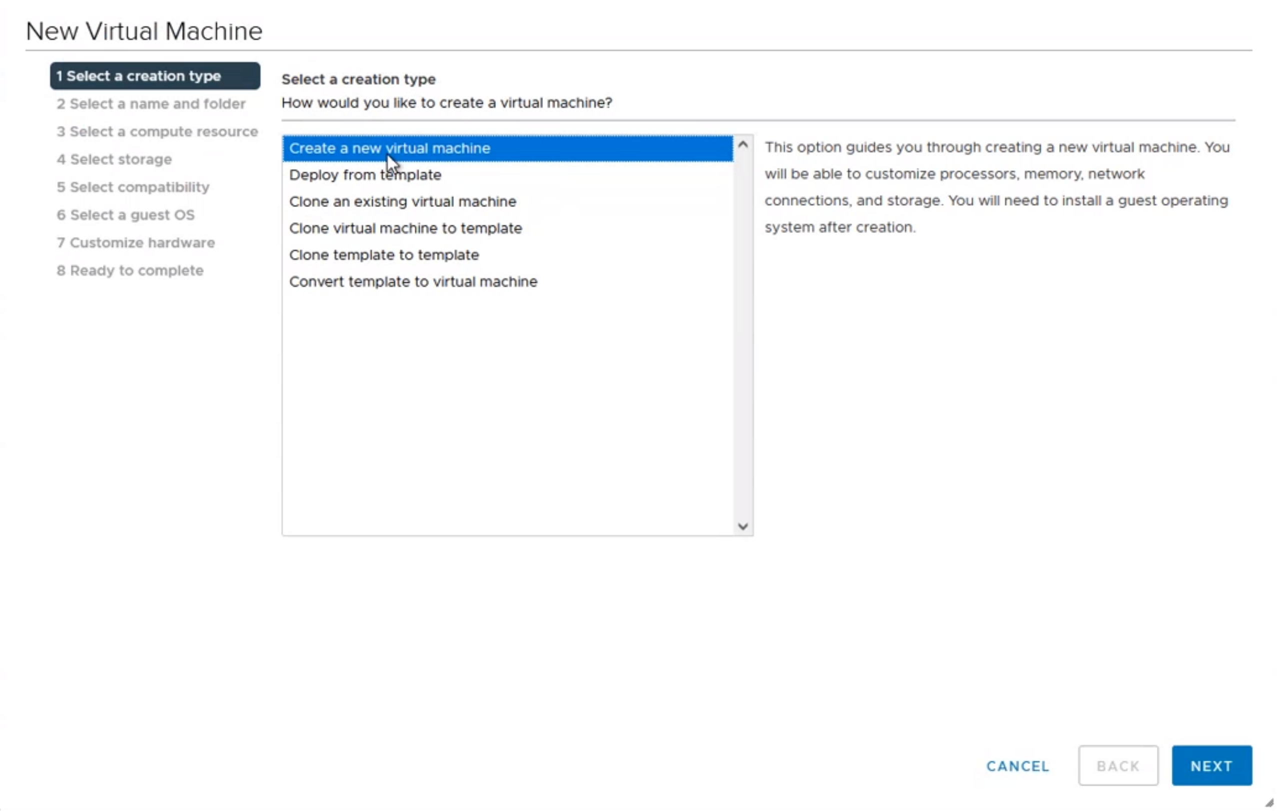
The installation of the reputation service includes the following steps:

1. Creating a Virtual Machine on page 509
2. Installing the reputation service on page 510
3. Configuring the reputation service on page 510

Creating a Virtual Machine

To create a virtual machine:

1. Create a new virtual server. For example, by selecting *File > New Virtual Machine...*., then selecting *Create a new virtual machine* and clicking *NEXT*.



New Virtual Machine

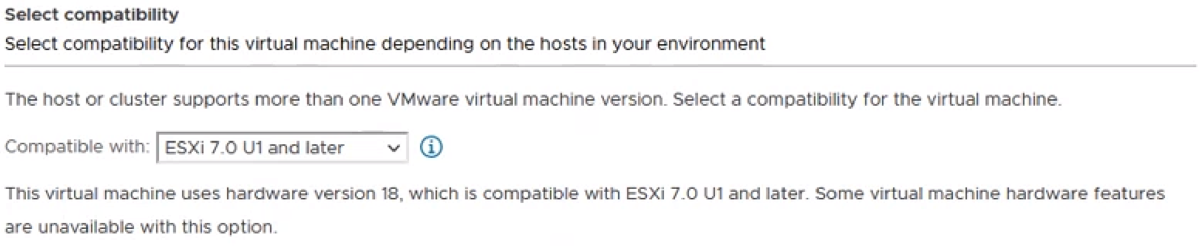
1 Select a creation type
2 Select a name and folder
3 Select a compute resource
4 Select storage
5 Select compatibility
6 Select a guest OS
7 Customize hardware
8 Ready to complete
Create a new virtual machine
Deploy from template
Clone an existing virtual machine
Clone virtual machine to template
Clone template to template
Convert template to virtual machine
CANCEL
BACK
NEXT

Select a creation type

How would you like to create a virtual machine?

This option guides you through creating a new virtual machine. You will be able to customize processors, memory, network connections, and storage. You will need to install a guest operating system after creation.

2. Enter the desired *virtual machine name*. For example, *fortiedr-reputation-service* and click *NEXT*.
3. Enter the virtual machine settings, as follows:
   - **a.** In the *Select a compute resource* step, select the resources as needed and click *NEXT*.
   - **b.** In the *Select storage* step, select the storage where the virtual machine disk should be stored on and click *NEXT*.
   - **c.** In the *Select Compatibility* step, select your ESXi version and click *NEXT*.



Select compatibility

Select compatibility for this virtual machine depending on the hosts in your environment

The host or cluster supports more than one VMware virtual machine version. Select a compatibility for the virtual machine.

Compatible with: ESXi 7.0 U1 and later

This virtual machine uses hardware version 18, which is compatible with ESXi 7.0 U1 and later. Some virtual machine hardware features are unavailable with this option.

   - **d.** At the *Select a guest OS* step, select *Linux* in the *Guest OS family* field and select *Ubuntu Linux (64-bit)* in the *Guest OS version* field.

   e. In the *Customize hardware* step, select the minimum requirements as specified in system requirements in Appendix C – ON PREMISE DEPLOYMENTS on page 459 and attach a network interface.

4. Select *Finish* to complete the creation of the virtual machine.

Installing the reputation service

To install the FortiEDR reputation service:

1. Right-click the new VM and select *Open Remote Console*.
2. Select *Manage > Virtual Machine Settings*.
3. In the *Hardware* tab, select the *CD/DVD* option and then select the *Use ISO image file* option on the right.
4. Click the *Browse* button and select the ISO file provided by Fortinet for the FortiEDR Reputation Server. Click *OK*.

Another option instead of completing the two steps described above is to upload the ISO from the VMWare datastore (this is possible if the ISO has already been uploaded there).

5. Start the virtual machine and wait until installation is complete.
6. Log into the virtual machine in order to continue the installation process.
   `Login: root`
   Change the root password, by entering any password you want. Then re-type it. The password must be strong enough according to Linux standards.

Configuring the reputation service

To configure the FortiEDR reputation service:

1. In the VM CLI, enter `fortiedr config`.
2. At the device role prompt, click *Next*.
3. At the prompt, enter your `hostname` and click *Next*. (Note: This can be any hostname)
4. A list of network interfaces on this virtual machine displays. At the *Pick your primary interface* prompt, select the primary interface to reach the Central Manager server, and click *Next*.
5. At the *Do you want to use DHCP* prompt, select *No* to configure the IP of this virtual machine manually, and then click *Next*.
6. At the prompt, enter the IP address of the machine that you are installing. Use the following format: `xxx.xxx.xxx.xxx/yy`, where yy is the routing prefix of the subnet.
7. At the prompt, enter the default gateway and click *Next*.
8. At the *Please set your DNS server* prompt, enter a valid IP address and click *Next*. Use the following format:
   `xxx.xxx.xxx.xxx/yy`, where yy is the routing prefix of the subnet.
9. At the management prompt, enter the Central Manager IP address, which must be reachable from the reputation server.

10. Enter the credentials of an admin user with REST API permissions in the FortiEDR Central Manager. If no such user exists, you must first create one by following the steps in Users on page 277.
11. Enter the Central Manager SSH port (default is 22).
12. Enter the Central Manager SSH credentials, which are the root username and password you created when Setting up a VM to be the FortiEDR Central Manager on page 465.
13. At the *Do you want to enable web-proxy ?* prompt, if the service will communicate via a proxy when accessing the web (such as the FortiEDR Cloud Service (FCS)), select *Yes* and then enter the IP and port of the proxy. Otherwise, select *No*.
14. At the *Please set the date* prompt, verify the date and click *Next*. The installer automatically presents the current date. You can change this date, if necessary.
15. At the *Please set your Time* prompt, set the time and click *Next*.
16. At the prompt, select the timezone and country in which the server is being installed.
17. Wait a few moments while the installation processes, until you see the Installation completed successfully message.
18. Run `fortiedr status` to validate that the reputation service is running.

Setting up the FortiEDR Core

This topic includes the following sections:

- Prerequisites on page 511
- Installing the FortiEDR Core on page 512

Prerequisites

The workstation, virtual machine or server on which the FortiEDR Core will be installed, must meet the following requirements:

- Complies with the requirements described in the *System Requirements* section in Appendix C – ON PREMISE DEPLOYMENTS on page 459.
- Has connectivity to a Local Area Network (for wired users) or a Wireless Network (for wireless users). If there is no connectivity, consult your IT support person.
- Has connectivity to the FortiEDR Aggregator. You can check this by browsing to the Aggregator's IP address. For problems connecting, see Troubleshooting on page 445.
- Has connectivity to the FortiEDR Reputation Server at `reputation.cloud.ensilo.com`.
- If the FortiEDR Core is deployed on your organization's premises (on-premises) and you use a web proxy to filter requests, then before running the installer, set the system proxy to work with an HTTPS connection, as follows:
  - Edit the file `/etc/environment` to have a proxy address configuration, https_proxy or PAC address. For example: `https_proxy=https://192.168.0.2:443`

    (for PAC): `https_proxy=pac+http://192.168.200.100/sample.pac`, where the `sample.pac` file contains an HTTPS address of the proxy.

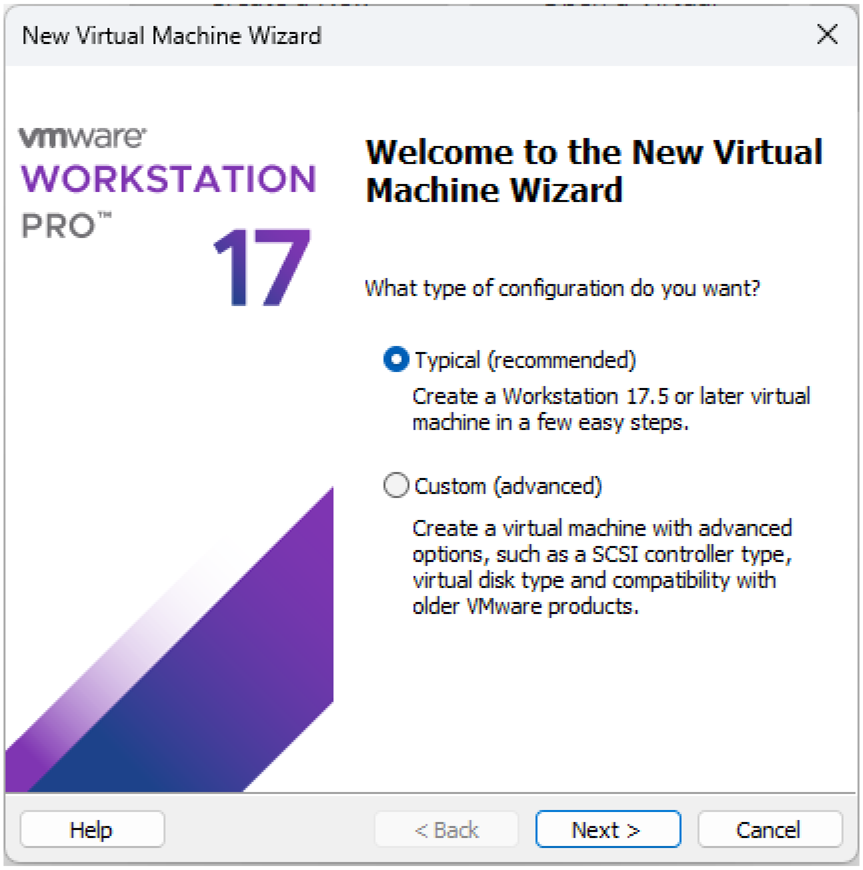
- If the definitions of the system proxy are placed somewhere other than `/etc/environment`, then:
  - Copy the definitions to the file `/etc/environment`. Note that this affects all processes on the Linux system.
  - Define a specific environment variable for the FortiEDR Linux Core with the name *nslo_https_proxy* at the file `/etc/environment`
    For example: `nslo_https_proxy=https://192.168.0.2:443`
    (for PAC): `nslo_https_proxy=pac+http://192.168.200.100/sample.pac`

For more details about installing a Core in a multi-organization environment, see the *Core Registration* section in Component registration in a multi-organization environment on page 416.

Installing the FortiEDR Core

The following describes how to install the FortiEDR Core:

1. Create a new virtual server by selecting *File > New Virtual Machine*.
2. Select the *Typical* option and click *Next*.



New Virtual Machine Wizard

Welcome to the New Virtual Machine Wizard

What type of configuration do you want?

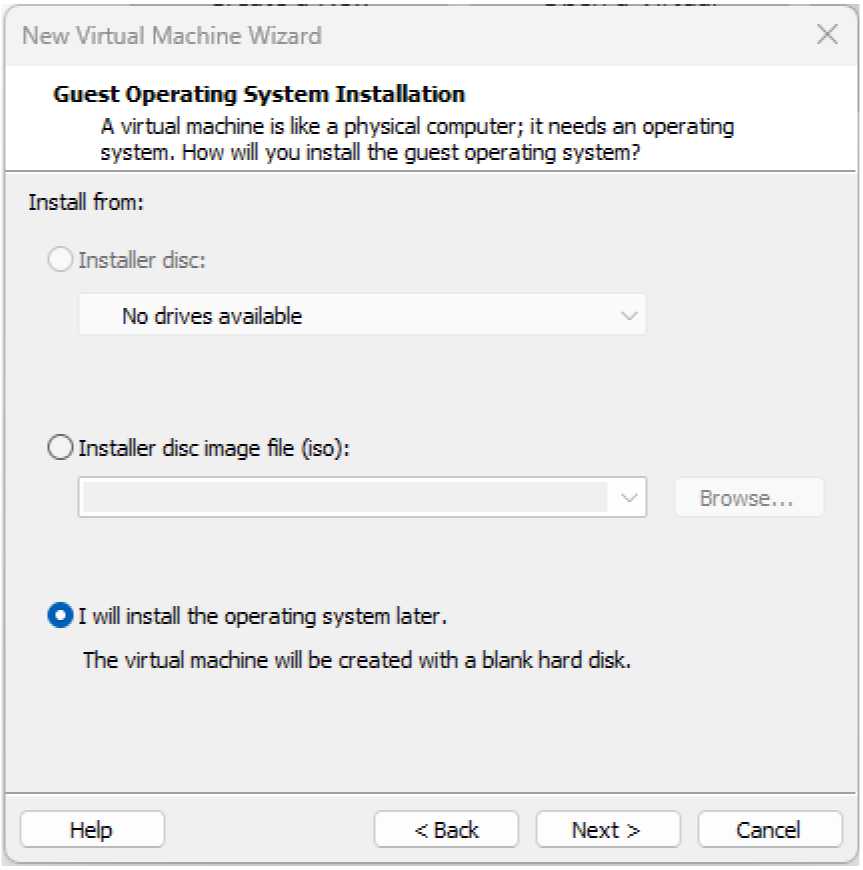
● Typical (recommended)

Create a Workstation 17.5 or later virtual machine in a few easy steps.

○ Custom (advanced)

Create a virtual machine with advanced options, such as a SCSI controller type, virtual disk type and compatibility with older VMware products.

3. Select the *I will install the operating system later* option and click *Next*.



New Virtual Machine Wizard

Guest Operating System Installation

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

○ Installer disc:

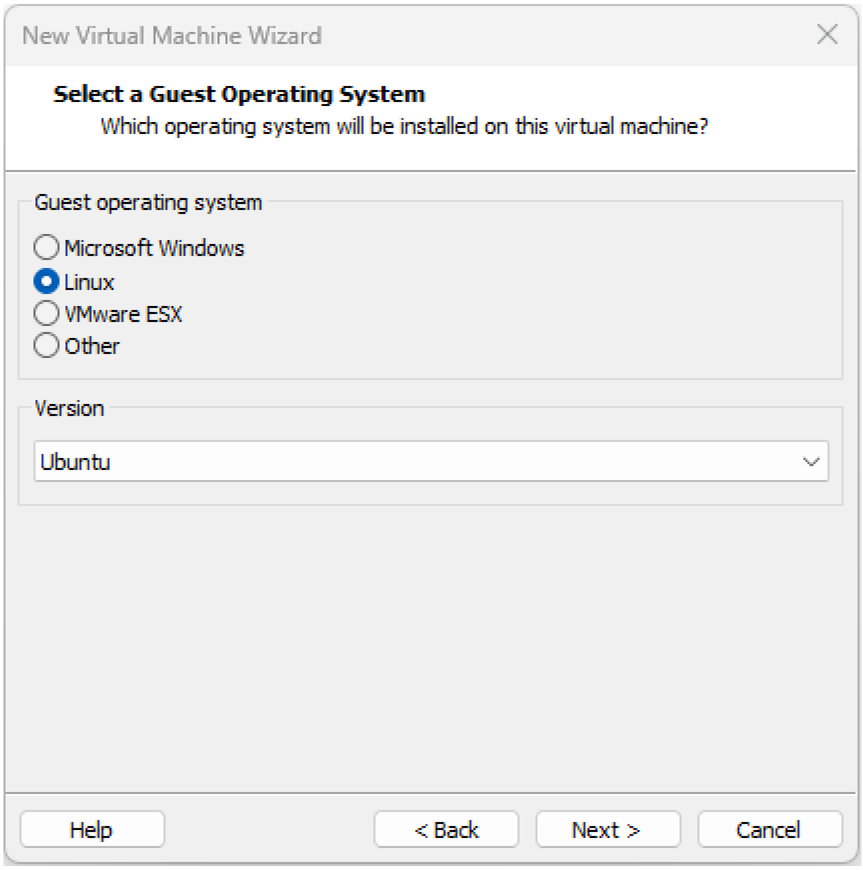
No drives available

○ Installer disc image file (iso):

● I will install the operating system later.

The virtual machine will be created with a blank hard disk.

4. Select the *Linux* radio button. In the *Version* field, select *Ubuntu* and click *Next*. Alternatively, you can select a different generic Linux 64-bit in the *Version* field.



New Virtual Machine Wizard

Select a Guest Operating System

Which operating system will be installed on this virtual machine?

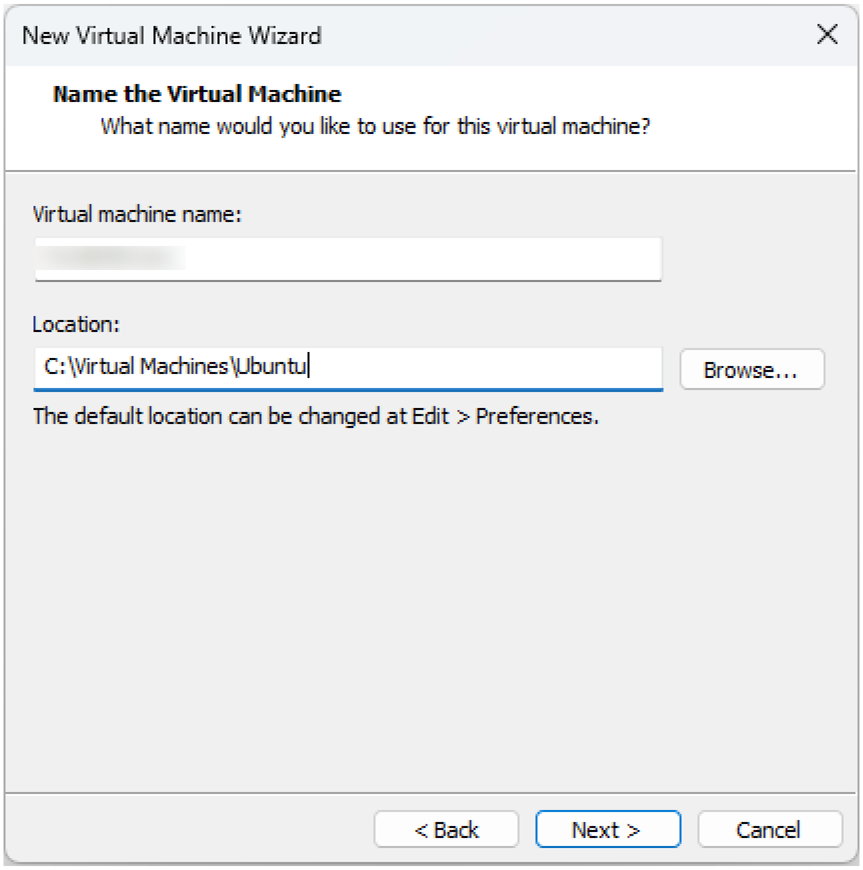
Guest operating system

○ Microsoft Windows
● Linux
○ VMware ESX
○ Other

Version

Ubuntu

5. Specify a name for the virtual machine such as *FortiEDRCore* and the location in which to store the provided ISO file and click *Next*.



New Virtual Machine Wizard

Name the Virtual Machine

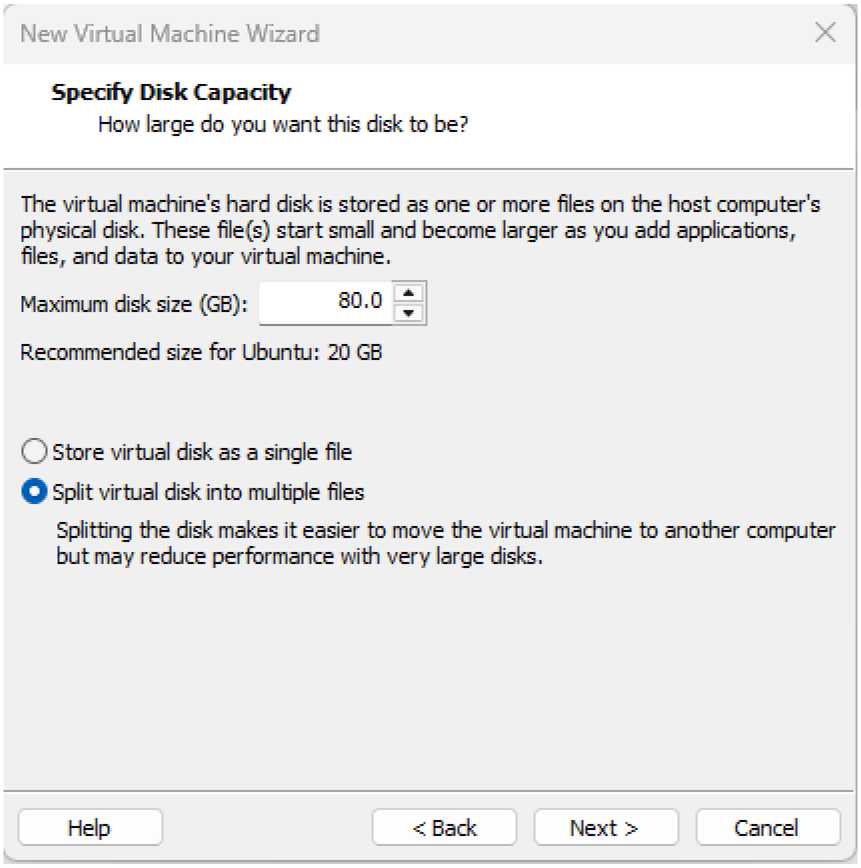
What name would you like to use for this virtual machine?

Virtual machine name: [redacted]

Location: C:\Virtual Machines\Ubuntu

The default location can be changed at Edit > Preferences.

6. Change the *Maximum disk size* to `80` GB, leave the default option as *Split virtual disk into multiple files* and click *Next*.



New Virtual Machine Wizard

Specify Disk Capacity

How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

Maximum disk size (GB): 80.0

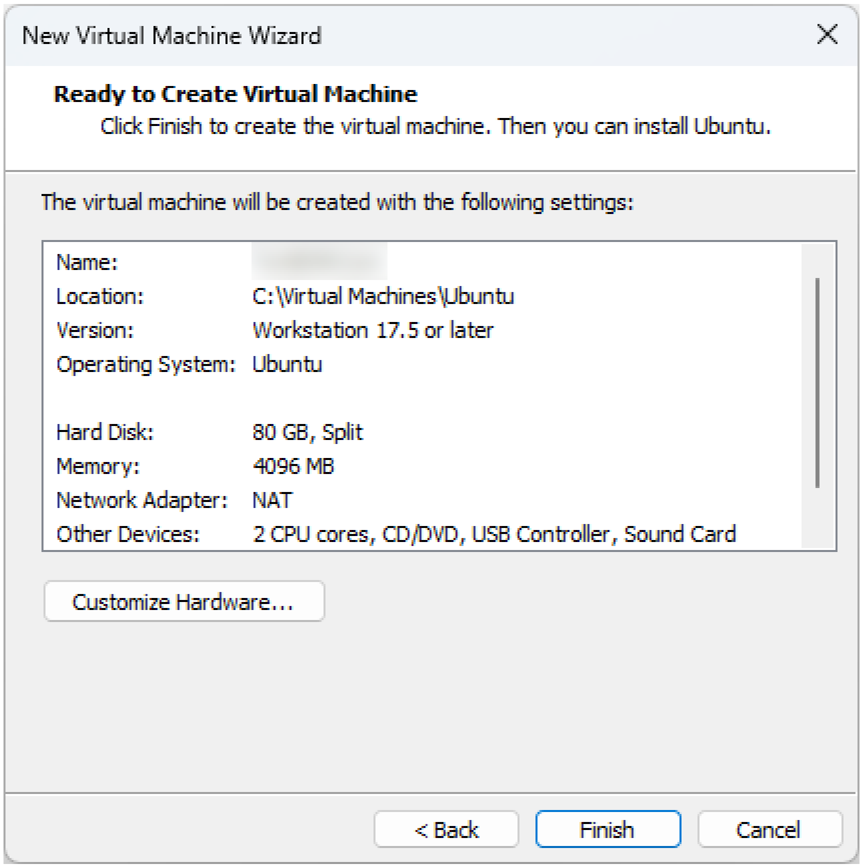
Recommended size for Ubuntu: 20 GB

○ Store virtual disk as a single file

● Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

7. Click *Finish*.



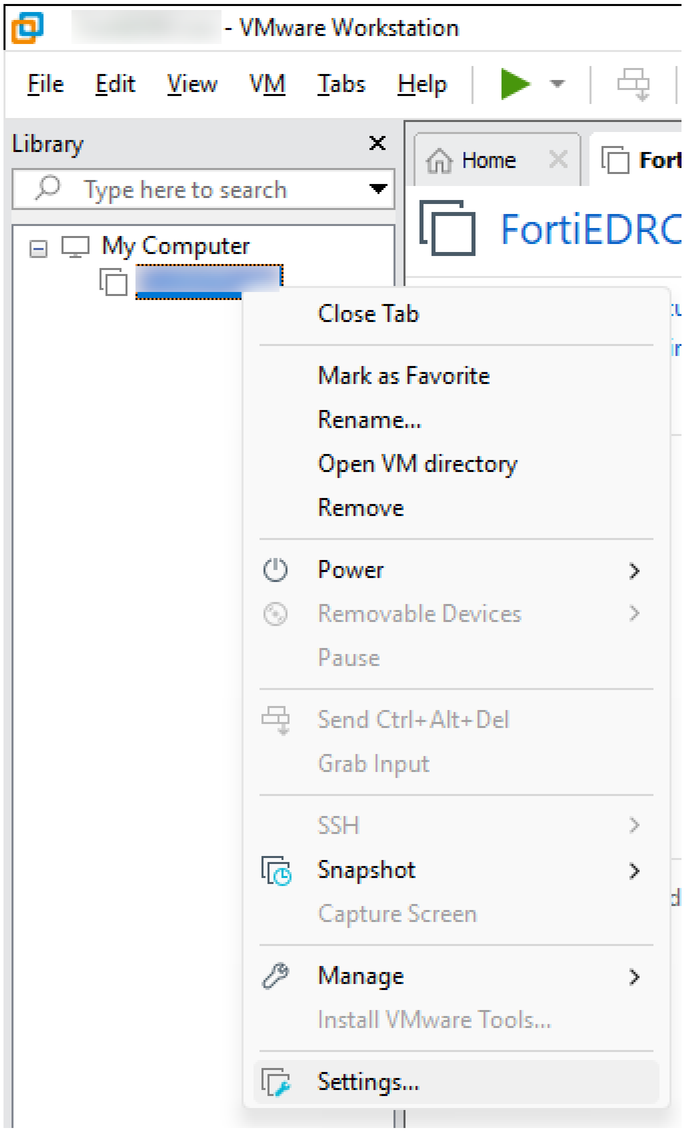
Ready to Create Virtual Machine

Click Finish to create the virtual machine. Then you can install Ubuntu.

The virtual machine will be created with the following settings:

Name:	[redacted]
Location:	C:\Virtual Machines\Ubuntu
Version:	Workstation 17.5 or later
Operating System:	Ubuntu
Hard Disk:	80 GB, Split
Memory:	4096 MB
Network Adapter:	NAT
Other Devices:	2 CPU cores, CD/DVD, USB Controller, Sound Card

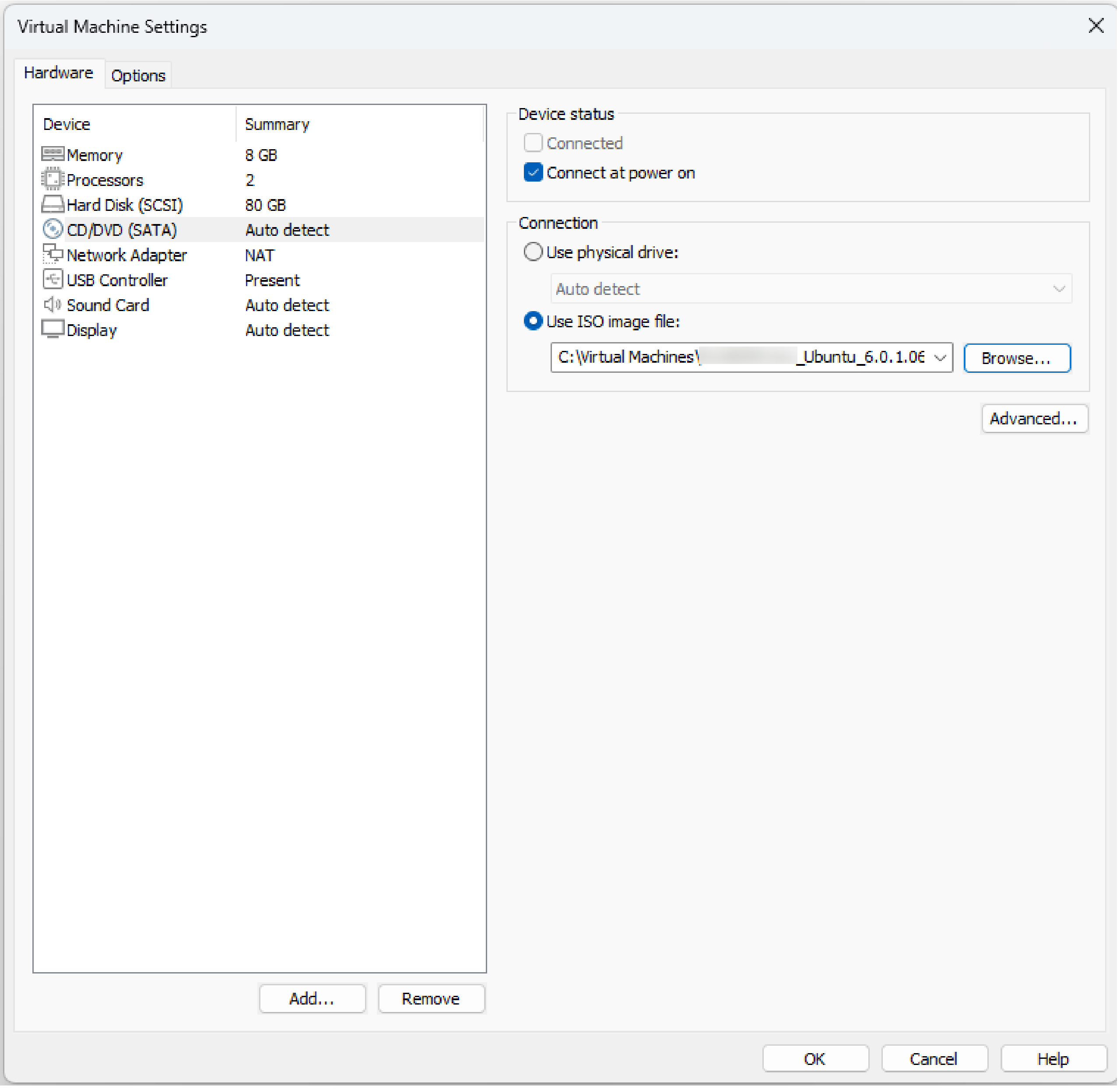
8. Right-click the new machine and select the *Settings* option.



9. Select the *Memory* option and change the RAM to at least 8 GB.

10. Select the *Processors* option and change the value to a total of at least two CPU Cores.

11. Select the *CD/DVD* option and then select the *Use ISO image* file option on the right.



Virtual Machine Settings

Device	Summary
Memory	8 GB
Processors	2
Hard Disk (SCSI)	80 GB
CD/DVD (SATA)	Auto detect
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Device status

□ Connected

☑ Connect at power on

Connection

○ Use physical drive:

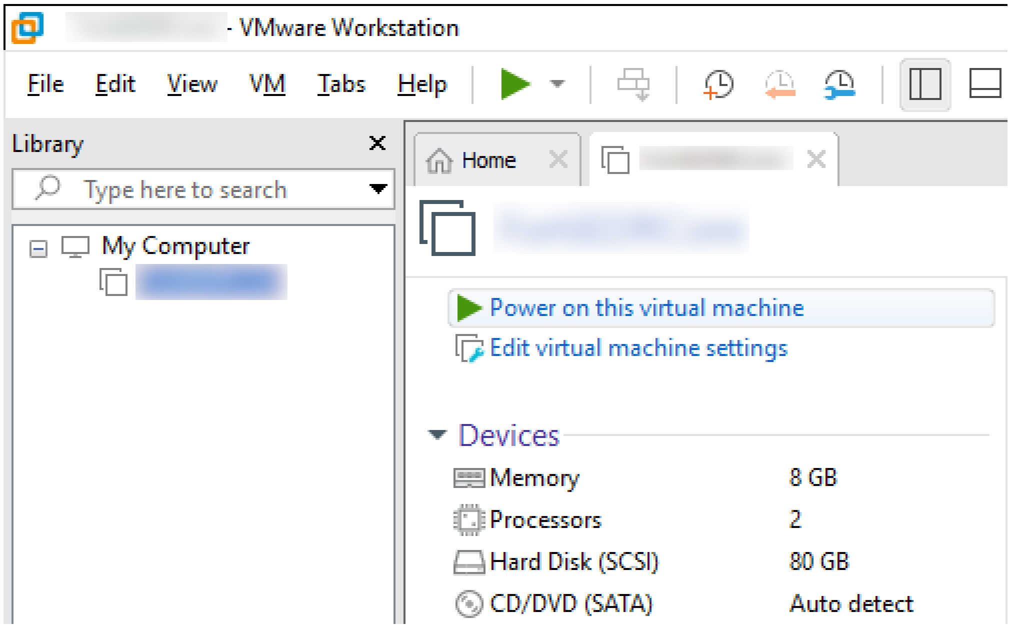
Auto detect

● Use ISO image file:

C:\Virtual Machines\[redacted]_Ubuntu_6.0.1.06

12. Click the *Browse* button and select the ISO file provided by Fortinet for the FortiEDR Core. Click *OK*.

13. Start the virtual machine. For example, by using the button shown below:



Memory	8 GB
Processors	2
Hard Disk (SCSI)	80 GB
CD/DVD (SATA)	Auto detect

The virtual machine automatically starts the installation process, which may take a few minutes.

14. Wait until a success message is displayed requesting that you reboot.
15. Reboot the virtual machine.
16. Log into the virtual machine in order to continue the installation process.
    `Login: root`
    Change the root password, by entering any password you want and then retype it. The password must be strong enough according to Linux standards.
17. Enter `fortiedr config`.
18. At the prompt, select the role of the virtual machine. For this installation, select *CORE* and click *Next*.

After the installation of the Core, you can configure the functionality of the Core as *Core only*, *Jumpbox*, or *Both* in the *INVENTORY > System Components* tab of the Central Manager.

19. At the prompt, enter your hostname (any hostname) and click *Next*.
20. At the prompt, enter the Organization name if this Core is added to a multi-tenant environment and should work only with one organization. For a non-multi-tenant setup, leave the organization name empty. Click *Next*.
21. At the prompt, enter the registration password.

If this is a multi-tenant setup and this Core is to belong only to a specific organization, then the password should match the registration password that was provided upon creating that organization (listed under *ADMINISTRATION > ORGANIZATIONS* tab of the FortiEDR Central Manager).

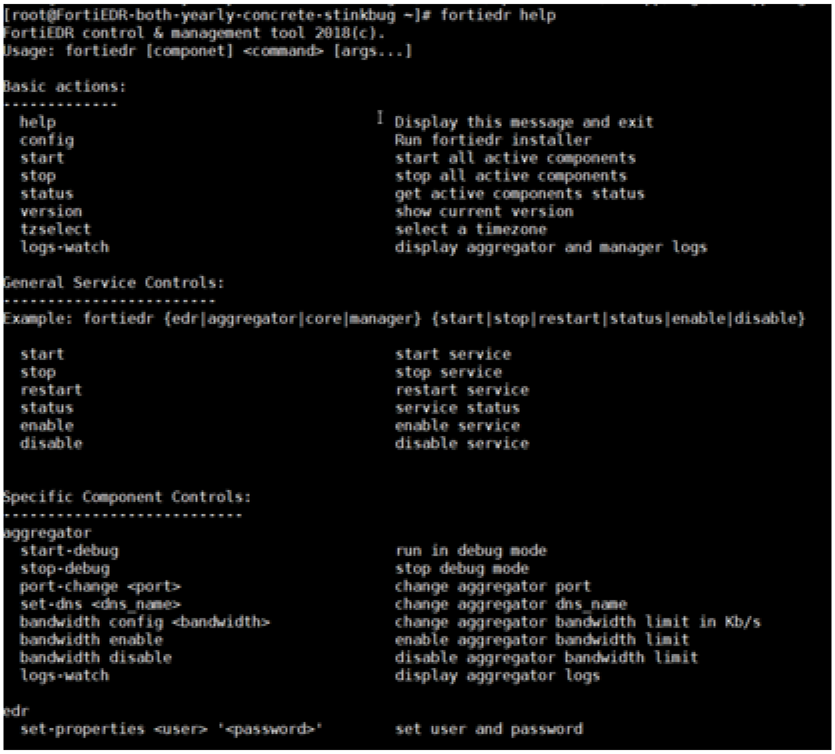
22. At the prompt, enter the Aggregator external IP address.
23. At the prompt, enter this Core machine’s external IP address without the port.

24. A list of network interfaces on this virtual machine displays. At the *Pick your primary interface* prompt, select the interface to be used as the primary network interface through which all FortiEDR Cores and FortiEDR Collectors will reach this server, and then click *Next*.
25. At the *Do you want to use DHCP* prompt, do one of the following:
    a. Select *yes* to use DHCP and click *Next*. Proceed to step 29 below.
    b. Select *no* to configure the IP of this virtual machine manually, and then click *Next*. Perform steps 26 through 35 below.
26. At the prompt, enter the IP address of the machine that you are installing.
    Use the following format: `xxx.xxx.xxx.xxx/yy`, where yy is the routing prefix of the subnet.
27. At the prompt, enter the default gateway and click *Next*.
28. At the *Please set your DNS server* prompt, enter a valid IP address and click *Next*.
    Use the following format: `xxx.xxx.xxx.xxx/yy`, where yy is the routing prefix of the subnet.
29. At the prompt, select *no* for debug mode.
30. At the *Please set the date* prompt, verify the date and click *Next*. The installer automatically presents the current date. You can change this date, if necessary.
31. At the *Please set your Time* prompt, set the time and click *Next*.
32. At the prompt, select the timezone and country in which the server is being installed.
33. At the *Do you want to enable Web proxy* prompt, select one of the following:
    - *yes*—If you select *yes*, you must manually edit the `/etc/environment` file to configure the proxy address, which can be https_proxy (such as `https_proxy=https://192.168.0.2:443`) or PAC address (such as `https_proxy=pac+http://192.168.200.100/`*`sample.pac`*, where `sample.pac` is the file that contains an HTTPS address of the proxy.
    - *no* (default)
34. If you selected *yes* in the previous step, at the *Do you want to exclude proxy configuration for Aggregator communication?* prompt, if the Aggregator is also installed on-premise, select *yes* to ignore the proxy for Core and Aggregator communication. Otherwise, select *no*.
35. Wait a few moments while the installation processes, until you see the *Installation completed successfully* message.
36. To verify that core installation succeeded, use the `fortiedr status` and `fortiedr version` commands.
37. In the *Administration > Deployment > System Components* tab of the Central Manager, verify that the FortiEDR Core details are listed and configure the functionality of the Core as *Core only*, *Jumpbox*, or *Both*.

FortiEDR CLI commands

The following describes additional commands that you can perform in the FortiEDR Core, Repository Server, FortiEDR Central Manager, or FortiEDR Aggregator CLI.

At the prompt, type `fortiedr` or `fortiedr help` to display them.



```
[root@FortiEDR-both-yearly-concrete-stinkbug ~]# fortiedr help
FortiEDR control & management tool 2018(c).
Usage: fortiedr [componet] <command> [args...]

Basic actions:
--------------
  help                                      Display this message and exit
  config                                    Run fortiedr installer
  start                                     start all active components
  stop                                      stop all active components
  status                                    get active components status
  version                                   show current version
  tzselect                                  select a timezone
  logs-watch                                display aggregator and manager logs

General Service Controls:
-------------------------
Example: fortiedr {edr|aggregator|core|manager} {start|stop|restart|status|enable|disable}

  start                                     start service
  stop                                      stop service
  restart                                   restart service
  status                                    service status
  enable                                    enable service
  disable                                   disable service


Specific Component Controls:
----------------------------
aggregator
  start-debug                               run in debug mode
  stop-debug                                stop debug mode
  port-change <port>                        change aggregator port
  set-dns <dns_name>                        change aggregator dns_name
  bandwidth config <bandwidth>              change aggregator bandwidth limit in Kb/s
  bandwidth enable                          enable aggregator bandwidth limit
  bandwidth disable                         disable aggregator bandwidth limit
  logs-watch                                display aggregator logs

edr
  set-properties <user> '<password>'        set user and password
```

Command	Description
Basic actions	
`help`	Display this message and exit.
`config`	Run FortiEDR installer.
`start`	Start all active components.
`stop`	Stop all active components.
`status`	Get active components status.
`version`	Show current version.
`tzselect`	Select a timezone.
`logs-watch`	Display Aggregator and Central Manager logs.
General service controls	
`start`	Start service.
`stop`	Stop service.
`restart`	Restart service.
`status`	Get service status.
`enable`	Enable service.

Command	Description
`disable`	Disable service.
Example: fortiedr {edr|aggregator|core|manager|activemq} {start|stop|restart|status|enable|disable}	
Specific component controls	
Aggregator	
`start-debug`	Run in debug mode.
`stop-debug`	Stop debug mode.
`port-change <port>`	Change Aggregator port.
`set-dns <dns_name>`	Change Aggregator DNS name.
`bandwidth config <bandwidth>`	Change aggregator bandwidth limit (in Kb/s).
`bandwidth enable`	Enable aggregator bandwidth limit.
`bandwidth disable`	Disable aggregator bandwidth limit.
`logs-watch`	Display Aggregator logs.
activemq	
`queue-stat <queue>`	Provides detailed metrics about the activemq queues (queue name is optional)
EDR	
`set-properties <user> '<password>'`	Set user and password.
`start-debug`	Run in debug mode.
`stop-debug`	Stop debug mode.
Central Manager	
`start-debug`	Run in debug mode.
`stop-debug`	Stop debug mode.
`load-content <password>`	Load dynamic content.
`load-extra-config <password>`	Load extra configuration.
`load-ssl-certificate <user> <password> <certificate-location> <privateKeyLocation> <privateKeyPassword>`	Load new SSL certificate.
`set-smtp-server <ip>`	Set SMTP server in `application-customer.properties`.
`reset-password <username>`	Reset web password for a specific user.
`disable-edr`	Disable FortiEDR in the Central Manager.
`enable-edr`	Enable FortiEDR in the Central Manager.

Command	Description
`set-edr-ip <ip>:<port>`	Set FortiEDR server IP address and port.
`set-edr-password <password>`	Set FortiEDR password.
`set-edr-user <user>`	Set FortiEDR user.
`logs-watch`	Display Central Manager logs.

Upgrading FortiEDR components

This section describes how to upgrade the components in the FortiEDR system.

Upgrading to a newer build number (major.minor.patch.build) can be done in any order. However, upgrading to newer major/minor versions (major.minor.patch.build) should be done top-down in the following order:

1. Upgrading the Central Manager on page 524
2. Upgrading the Aggregator on page 524
3. Upgrading the Threat Hunting Repository on page 525
4. Upgrading the Core on page 526
5. Upgrading the Collector on page 73

Upgrading the Central Manager

The required upgrade file is provided to you by Fortinet. Use it to perform the procedure below.

1. Copy the `FortiEDRInstaller_Ubuntu_7.2.0.xxxx.x` file to the Central Manager machine. You can place the file anywhere on the Linux machine. For example, `FortiEDRInstaller_Ubuntu_7.2.0.0097.x`.
2. Change the *chmod 755* permission and the *patch* name in order to enable you to run the upgrade, as shown below:
   ```
   [root@dan ~]# chmod 755 FortiEDRInstaller_Ubuntu_7.2.0.0097.x
   ```
3. Run the patch, as shown below:
   ```
   [root@dan ~]# ./FortiEDRInstaller_Ubuntu_7.2.0.0097.x
   ```
4. Wait for the upgrade to complete, as shown below:
   ```
   FortiEDR installation 7.2.0.0097.x finished successfully
   [root@dan ~]#
   ```

Upgrading the Aggregator

The required upgrade file is provided to you by Fortinet. Use it to perform the procedure below.

1. Copy the `FortiEDRInstaller_Ubuntu_7.2.0.xxxx.x` file to the Aggregator machine. You can place the file anywhere on the Linux machine. For example, `FortiEDRInstaller_Ubuntu_7.2.0.0097.x`.

2. Change the *chmod 755* permission and the *patch* name in order to enable you to run the upgrade, as shown below:

   ```
   [root@dan ~]# chmod 755 FortiEDRInstaller_Ubuntu_7.2.0.0097.x
   ```

3. Run the patch, as shown below:

   ```
   [root@dan ~]# ./FortiEDRInstaller_Ubuntu_7.2.0.0097.x
   ```

4. Wait for the upgrade to complete, as shown below:

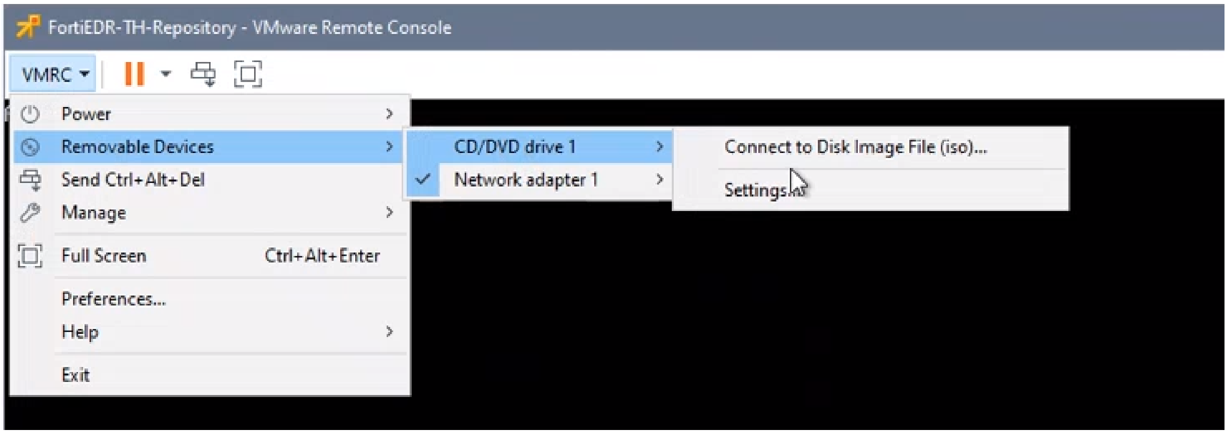
   ```
   FortiEDR installation 7.2.0.0097.x finished successfully
   [root@dan ~]#
   ```

Upgrading the Threat Hunting Repository

Before you begin, ensure the CPU and memory of the repository are at least 1.5 times of the defined Threat Hunting specifications in Appendix C – ON PREMISE DEPLOYMENTS on page 459. You can reduce the CPU and memory back to the specifications once the upgrade is completed.

To upgrade the Threat Hunting Repository:

1. Launch the *FortiEDR_RepositoryInstaller* ISO file of the new Threat Hunting Repository version:
   a. From the *VMRC* menu, select *Removable Device > CD/DVD drive 1 > Connect to Disk Image File (iso)....*



If an existing ISO is still connected, select *Removable Device > CD/DVD drive 1 > Disconnect [ISO path]* before connecting to the new ISO file.

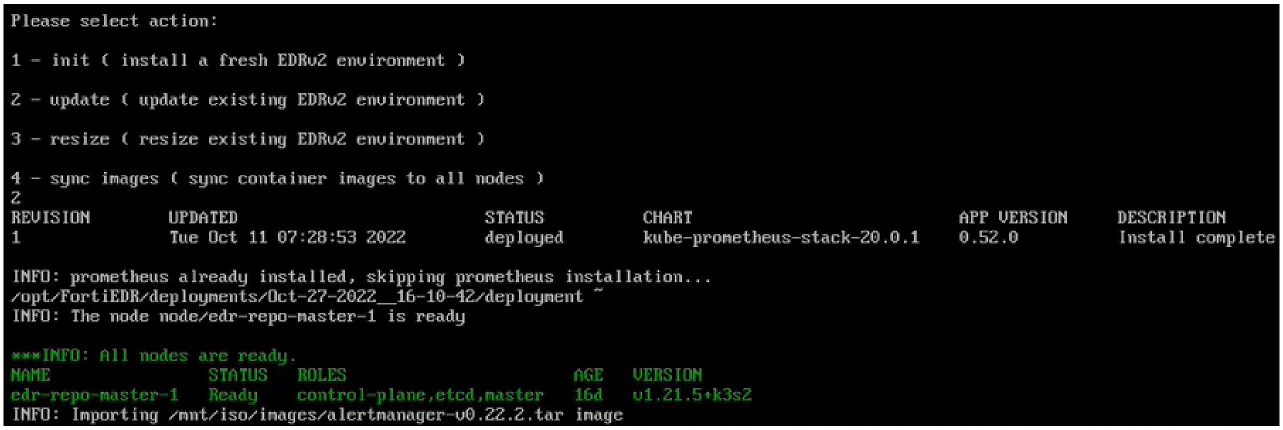
   b. Select the *FortiEDR_RepositoryInstaller* ISO file for the new version and click on *Open*.

Another option instead of the two steps described above is to upload the ISO from the VMWare datastore (this is possible if the ISO has already been uploaded there).

2. Start an SSH session to the repository machine, log in with user `rancher`, and run the following command:

```
sudo su -

bash /k3os/system/install_edr2.sh
```

Select *update* (2) to upgrade the Threat Hunting Repository.



```
Please select action:

1 - init ( install a fresh EDRv2 environment )

2 - update ( update existing EDRv2 environment )

3 - resize ( resize existing EDRv2 environment )

4 - sync images ( sync container images to all nodes )
2
REVISION        UPDATED                         STATUS          CHART                           APP VERSION     DESCRIPTION
1               Tue Oct 11 07:28:53 2022        deployed        kube-prometheus-stack-20.0.1    0.52.0          Install complete

INFO: prometheus already installed, skipping prometheus installation...
/opt/FortiEDR/deployments/Oct-27-2022__16-10-42/deployment ~
INFO: The node node/edr-repo-master-1 is ready

***INFO: All nodes are ready.
NAME                STATUS   ROLES                       AGE   VERSION
edr-repo-master-1   Ready    control-plane,etcd,master   16d   v1.21.5+k3s2
INFO: Importing /mnt/iso/images/alertmanager-v0.22.2.tar image
```

The node is being updated, which might take 8 to 10 minutes.

3. Complete the FortiEDR Repository software upgrade by providing the following parameters:
    - When prompted for the FortiEDR Manager details, provide its IP and the credentials of one of the FortiEDR Console administrators with Rest API permissions. See Users on page 277.
    - When prompted for the primary DNS server address, provide the primary DNS server address for the Threat Hunting Repository.
    - When asked whether to set additional DNS servers, enter yes and provide an alternative DNS address for the Threat Hunting Repository if needed. Otherwise, enter no to proceed.

    Fortinet recommends that you set up one additional DNS server in case the primary DNS server fails.

    - Enter the password of the FortiEDR Console administrator with Rest API permissions. See Users on page 277.
    - When asked if you have a dedicated Aggregator VM, enter yes if you installed the Aggregator on a separate VM than the Central Manager, and you will then be prompted to provide the Aggregator details. Otherwise, enter no to proceed.
4. Wait for the configuration to complete.
5. Repeat step 1-4 on each additional Threat Hunting Repository nodes you may have.
6. Verify the upgrade is successful by opening the Central Manager and checking the version information under the *INVENTORY* > *System Components* > *REPOSITORIES* tab.

Upgrading the Core

1. Copy the `FortiEDRCoreInstaller_x.x.x.x.x` file to the Core machine. You can place the file anywhere on the Linux machine. For example, `FortiEDRCoreInstaller_6.0.1.x.y.`

2. Change the *chmod 755* permission and the *patch* name in order to enable you to run the upgrade, as shown below:

   ```
   [root@dan ~]# chmod 755 FortiEDRCoreInstaller_6.0.1.x.y
   ```

3. Run the patch, as shown below:

   ```
   [root@dan ~]# ./FortiEDRCoreInstaller_6.0.1.x.y
   ```

4. Wait for the upgrade to complete, as shown below:

   ```
   FortiEDR patch 6.0.1.x.y finished
   [root@dan ~]#
   ```

FORTINET®

www.fortinet.com

Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.