

# Administration Guide

**FortiEDR 5.2.1**



**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](mailto:techdoc@fortinet.com)



March 6, 2024

FortiEDR 5.2.1 Administration Guide

63-521-833527-20240306

# TABLE OF CONTENTS

<b>Change log</b>	<b>8</b>
<b>Introducing FortiEDR</b>	<b>11</b>
Introduction	11
Execution prevention	11
Data exfiltration	11
Ransomware	12
Threat hunting	12
FortiEDR technology	13
FortiEDR components	14
Overview	14
FortiEDR Collector	14
FortiEDR Core	16
FortiEDR Aggregator	16
FortiEDR Central Manager	17
FortiEDR Cloud Service	17
How does FortiEDR work?	17
Using FortiEDR - workflow	18
Setup workflow overview	18
Ongoing workflow overview	19
<b>Deploying FortiEDR Collectors</b>	<b>21</b>
Installing FortiEDR Collectors	21
Before you start	21
Installing a FortiEDR Collector on Windows	23
Installing a FortiEDR Collector on macOS	28
Installing a FortiEDR Collector on Linux	43
Automated FortiEDR Collector deployment	45
Installing FortiEDR on Mac Big Sur devices using Jamf PRO	48
Setting up exclusions with other AV products	52
Working with FortiEDR on VDI environments	52
Uninstalling FortiEDR Collectors	53
Upgrading the Collector	55
<b>Setting up a FortiEDR Core as a Jumpbox</b>	<b>57</b>
Preparing for the FortiEDR Core installation	57
Installing the FortiEDR Core	57
Upgrading the Core	63
<b>Security Settings</b>	<b>64</b>
Security events	64
FortiEDR security policies	64
Protection or Simulation mode	66
Setting a security policy's Prevention or Simulation mode	69
Creating a new security policy	71
Assigning a security policy to a Collector Group	72
Exception Manager	75
Exclusion Manager	78

Filtering .....	79
Defining Exclusion Lists .....	79
Defining exclusions .....	80
Application Control Manager .....	85
Adding application(s) to be blocked .....	86
Exporting the list of applications to be blocked .....	90
Enabling/disabling application blocking .....	90
Changing the policy under which the application is blocked .....	91
Searching and filtering applications .....	92
Threat Hunting .....	92
Collection Profiles .....	92
Collection Exclusions .....	94
Threat Hunting data retention .....	101
Playbook policies .....	101
Automated Incident Response - Playbooks Page .....	102
Assigned Collector Groups .....	102
<b>Inventory .....</b>	<b>111</b>
Introducing the Inventory .....	111
Uninstalling a Collector .....	113
Collectors .....	113
Defining a new Collector Group .....	116
Assigning Collectors to a Collector Group .....	117
Deleting a Collector Group/Collector .....	118
Enabling/disabling a Collector .....	119
Device isolation .....	119
Unmanaged devices .....	121
IoT devices .....	122
Defining a new IoT group .....	123
Assigning devices to an IoT group .....	123
Deleting an IoT device/IoT group .....	124
Refreshing IoT device data .....	125
Exporting IoT information .....	125
System Components .....	125
Aggregators .....	126
Cores .....	127
Repositories .....	128
Exporting logs .....	129
Exporting logs for Collectors .....	129
Exporting logs for Cores .....	131
Exporting logs for Aggregators .....	131
<b>Dashboard .....</b>	<b>133</b>
Introduction .....	133
Security Events chart .....	134
Communication Control chart .....	135
Collectors chart .....	136
Most Targeted charts .....	138
External Destinations .....	138



System Components .....	140
Executive Summary Report .....	140
Event Statistics .....	142
Destinations .....	142
Most-targeted Devices .....	143
Most-targeted Processes .....	143
Communication Control .....	144
System Components .....	144
License Status .....	145
<b>Event Viewer .....</b>	<b>146</b>
Introducing the Event Viewer .....	146
Events pane .....	150
Advanced Data .....	154
Event Graph .....	154
Geo Location .....	155
Automated Analysis .....	155
Marking a security event as handled/unhandled .....	156
Manually changing the classification of a security event .....	158
Defining security event exceptions .....	160
Defining the scope of an exception .....	161
Defining a security event as an exception .....	164
Device Control exceptions .....	174
Editing security event exceptions .....	175
Marking a security event as read/unread .....	177
Viewing relevant activity events .....	177
Viewing expired security events .....	177
Viewing Application Control security events .....	178
Viewing Device Control security events .....	179
Other options in the Event Viewer .....	180
Classification Details .....	183
<b>Communication control .....</b>	<b>190</b>
Application communication control - how does it work? .....	190
Introducing communication control .....	191
Applications .....	193
Reputation score .....	194
Vulnerability .....	195
Resolved vs. unresolved applications .....	197
Sorting the Application List .....	197
Marking an Entry as Read/Unread .....	197
Modifying a Policy Action .....	198
Searching the Application List .....	201
Other options in the Application pane .....	202
Advanced Data .....	203
Policies .....	209
Predefined policies .....	211
Policy mode .....	212

Policy rules .....	213
Assigning a policy to a Collector Group .....	216
Creating a new Communication Control policy .....	217
Other options in the Policies pane .....	218
<b>Forensics .....</b>	<b>219</b>
Introduction .....	219
Flow Analyzer view .....	223
Stack view .....	224
Compare view .....	226
Defining an exception .....	227
Remediating a device upon malware detection .....	227
Retrieving memory .....	232
Isolating a device .....	234
Threat Hunting .....	237
Threat Hunting .....	237
Legacy Threat Hunting .....	265
FortiEDR Connect .....	267
Connecting to a FortiEDR-protected device .....	267
File Library pane .....	270
Disconnecting FortiEDR Connect session .....	272
<b>Administration .....</b>	<b>274</b>
Licensing .....	274
Updating the Collector version .....	277
Loading a server certificate .....	281
Requesting and obtaining a Collector installer .....	281
Users .....	285
Two-factor authentication .....	287
Resetting a user password .....	289
LDAP authentication .....	290
SAML authentication .....	292
Distribution lists .....	311
Export settings .....	312
SMTP .....	313
Open Ticket .....	313
Syslog .....	314
Tools .....	317
Audit trail .....	317
Component authentication .....	319
File scan .....	320
End-user notifications .....	321
IoT device discovery .....	324
Personal data handling .....	325
Windows Security Center .....	330
FortiEDR Connect .....	331
System events .....	332
IP sets .....	334

Integrations .....	336
Adding connectors .....	337
Action Manager .....	369
<b>Troubleshooting .....</b>	<b>374</b>
A FortiEDR Collector does not display in the INVENTORY tab .....	374
No events on the FortiEDR Central Manager console .....	374
User cannot communicate externally or files modification activity is blocked .....	375
Microsoft Windows-based devices .....	375
macOS-based devices .....	375
Collector is slow or hangs .....	376
<b>Multi-tenancy (organizations) .....</b>	<b>377</b>
What is a multi-organization environment in FortiEDR? .....	377
Multi-organization and user roles .....	377
Component registration in a multi-organization environment .....	378
Collector registration .....	378
Core registration .....	379
Workflow .....	380
Step 1 – Logging in to a multi-organization system .....	380
Step 2 – Defining or importing an organization .....	381
Step 3 - Navigating between organizations .....	386
Step 4 – Defining an Administrator for an organization .....	386
Step 5 – Performing operations in the FortiEDR system .....	387
Migrating an organization .....	387
Hoster view .....	397
Licensing .....	397
Users .....	398
Tools .....	399
Dashboard .....	400
Event Viewer .....	401
Forensics .....	403
Communication Control .....	403
Threat Hunting .....	404
Security settings .....	404
Exception Manager .....	405
Inventory .....	408
<b>Appendix A – Setting up an email feed for open ticket .....</b>	<b>411</b>
<b>Appendix B - Lucene syntax .....</b>	<b>418</b>
Terms .....	418
Operators .....	418
Wildcards .....	419
Ranges .....	419
Reserved characters .....	420

# Change log

Date	Change Description
2022-09-09	5.2.1 Initial release.
2022-09-14	Added the following topics: <ul style="list-style-type: none"><li>• <a href="#">Identity Management integration on page 350</a></li><li>• <a href="#">User Access integration on page 354</a></li></ul> Updated the following topics: <ul style="list-style-type: none"><li>• <a href="#">Events pane on page 150</a></li><li>• <a href="#">Classification Details on page 183</a></li></ul>
2022-09-19	Updated <a href="#">Installing FortiEDR Collectors on page 21</a> .
2022-09-28	Updated the following topics: <ul style="list-style-type: none"><li>• <a href="#">Installing FortiEDR Collectors on page 21</a></li><li>• <a href="#">Setting up a FortiEDR Core as a Jumpbox on page 57</a></li></ul>
2022-10-03	Updated the following topics: <ul style="list-style-type: none"><li>• <a href="#">Uninstalling FortiEDR Collectors on page 53</a></li><li>• <a href="#">SAML IdP configuration with Okta on page 301</a></li></ul>
2022-10-24	Updated <a href="#">Before you start on page 21</a> .
2022-11-02	Updated <a href="#">Before you start on page 21</a> .
2022-11-09	Updated the following topics: <ul style="list-style-type: none"><li>• <a href="#">Before you start on page 21</a>: Added "macOS Ventura (13)" to the supported OSes list</li><li>• <a href="#">Two-factor authentication on page 287</a></li></ul>
2022-11-14	Updated the following topics: <ul style="list-style-type: none"><li>• <a href="#">Loading a server certificate on page 281</a></li><li>• <a href="#">SAML IdP configuration with Azure on page 295</a></li></ul>
2022-11-23	Updated the following topics: <ul style="list-style-type: none"><li>• <a href="#">Setting up a FortiEDR Core as a Jumpbox on page 57</a></li><li>• <a href="#">SAML IdP configuration with Azure on page 295</a></li></ul>
2022-11-29	Updated <a href="#">Application communication control - how does it work? on page 190</a> .
2022-11-30	Updated the following topics: <ul style="list-style-type: none"><li>• <a href="#">FortiEDR components on page 14</a></li><li>• <a href="#">Exclusion Manager on page 78</a></li></ul>
2022-12-14	Reorganized the <a href="#">Deploying FortiEDR Collectors on page 21</a> chapter.
2022-12-16	<ul style="list-style-type: none"><li>• Deleted the <i>Appendix C – ON PREMISE DEPLOYMENTS</i> chapter because FortiEDR 5.2.1 does not support on-premise deployment.</li><li>• Updated <a href="#">Licensing on page 274</a>.</li></ul>

Date	Change Description
2022-12-21	Updated <a href="#">FortiEDR Connect</a> on page 267.
2022-12-29	Updated <a href="#">Setting up a FortiEDR Core as a Jumpbox</a> on page 57.
2023-01-03	Updated <a href="#">Cores</a> on page 127.
2023-01-23	Updated <a href="#">Appendix A – Setting up an email feed for open ticket</a> on page 411.
2023-02-07	Updated <a href="#">Playbook policy actions</a> on page 105.
2023-02-16	Updated <a href="#">Two-factor authentication</a> on page 287.
2023-03-16	Updated <a href="#">Component authentication</a> on page 319.
2023-03-21	<ul style="list-style-type: none"> <li>Added the following topics: <ul style="list-style-type: none"> <li><a href="#">Setting up exclusions with other AV products</a> on page 52</li> <li><a href="#">Collector is slow or hangs</a> on page 376</li> </ul> </li> <li>Updated the following topics: <ul style="list-style-type: none"> <li><a href="#">Installing FortiEDR Collectors</a> on page 21</li> <li><a href="#">Installing a FortiEDR Collector on Windows</a> on page 23</li> <li><a href="#">Installing a FortiEDR Collector on macOS</a> on page 28</li> <li><a href="#">Installing a FortiEDR Collector on Linux</a> on page 43</li> <li><a href="#">Automated FortiEDR Collector deployment</a> on page 45</li> <li><a href="#">Installing FortiEDR on Mac Big Sur devices using Jamf PRO</a> on page 48</li> <li><a href="#">Uninstalling FortiEDR Collectors</a> on page 53</li> <li><a href="#">System events</a> on page 332</li> </ul> </li> </ul>
2023-03-22	Updated the following topics: <ul style="list-style-type: none"> <li><a href="#">Setting up exclusions with other AV products</a> on page 52</li> <li><a href="#">Uninstalling FortiEDR Collectors</a> on page 53</li> </ul>
2023-03-29	Updated <a href="#">Step 2 – Defining or importing an organization</a> on page 381.
2023-04-24	Updated <a href="#">Before you start</a> on page 21.
2023-04-27	Updated <a href="#">Loading a server certificate</a> on page 281.
2023-05-26	Updated <a href="#">Hoster view</a> on page 397.
2023-05-29	Added <a href="#">Tools</a> on page 399.
2023-05-30	Updated the following topics: <ul style="list-style-type: none"> <li><a href="#">Introducing FortiEDR</a> on page 11</li> <li><a href="#">Two-factor authentication</a> on page 287</li> </ul>
2023-06-20	Updated <a href="#">Updating the Collector version</a> on page 277.
2023-07-28	Updated <a href="#">Installing a FortiEDR Collector on Linux</a> on page 43.
2023-08-15	Updated <a href="#">Installing a FortiEDR Collector on Linux</a> on page 43.
2023-08-30	Updated <a href="#">eXtended detection source integration</a> on page 361.



Date	Change Description
2023-09-06	Updated <a href="#">System events</a> on page 332.
2023-09-08	Updated <a href="#">Connecting to a FortiEDR-protected device</a> on page 267.
2023-09-13	Added supported Python version in the following topics: <ul style="list-style-type: none"><li>• <a href="#">Integrations</a> on page 336</li><li>• <a href="#">Firewall integration</a> on page 337</li><li>• <a href="#">Network Access Control (NAC) integration</a> on page 345</li><li>• <a href="#">Identity Management integration</a> on page 350</li><li>• <a href="#">User Access integration</a> on page 354</li><li>• <a href="#">Custom integration</a> on page 365</li><li>• <a href="#">Action Manager</a> on page 369</li></ul>
2023-09-20	Updated <a href="#">Two-factor authentication</a> on page 287.
2023-10-26	Updated <a href="#">Before you start</a> on page 21.
2023-10-30	Updated <a href="#">Flow Analyzer view</a> on page 223.
2023-11-07	Updated <a href="#">A FortiEDR Collector does not display in the INVENTORY tab</a> on page 374.
2023-11-14	Updated <a href="#">Before you start</a> on page 21.
2023-11-20	Updated <a href="#">Before you start</a> on page 21.
2023-11-24	Updated <a href="#">Before you start</a> on page 21.
2023-12-14	Updated <a href="#">Collectors</a> on page 113.
2023-12-18	Updated the following topics: <ul style="list-style-type: none"><li>• <a href="#">Defining exclusions</a> on page 80</li><li>• <a href="#">Step 2 – Defining or importing an organization</a> on page 381</li></ul>
2023-12-19	Updated <a href="#">Step 2 – Defining or importing an organization</a> on page 381.
2023-12-20	Updated <a href="#">Defining exclusions</a> on page 80.
2023-12-28	Updated <a href="#">eXtended detection source integration</a> on page 361.
2023-12-29	Updated <a href="#">Before you start</a> on page 21.
2024-01-03	Updated the following topics: <ul style="list-style-type: none"><li>• <a href="#">Upgrading the Collector</a> on page 55</li><li>• <a href="#">Uninstalling FortiEDR Collectors</a> on page 53</li></ul>
2024-01-04	Updated <a href="#">Uninstalling FortiEDR Collectors</a> on page 53.
2024-01-18	Updated <a href="#">Manually adding an application to be blocked</a> on page 87.
2024-02-21	Updated the following topics: <ul style="list-style-type: none"><li>• <a href="#">Installing a FortiEDR Collector on Linux</a> on page 43</li><li>• <a href="#">Audit trail</a> on page 317</li></ul>
2024-03-05	Updated <a href="#">Installing a FortiEDR Collector on macOS</a> on page 28.

# 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 ransomware 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.

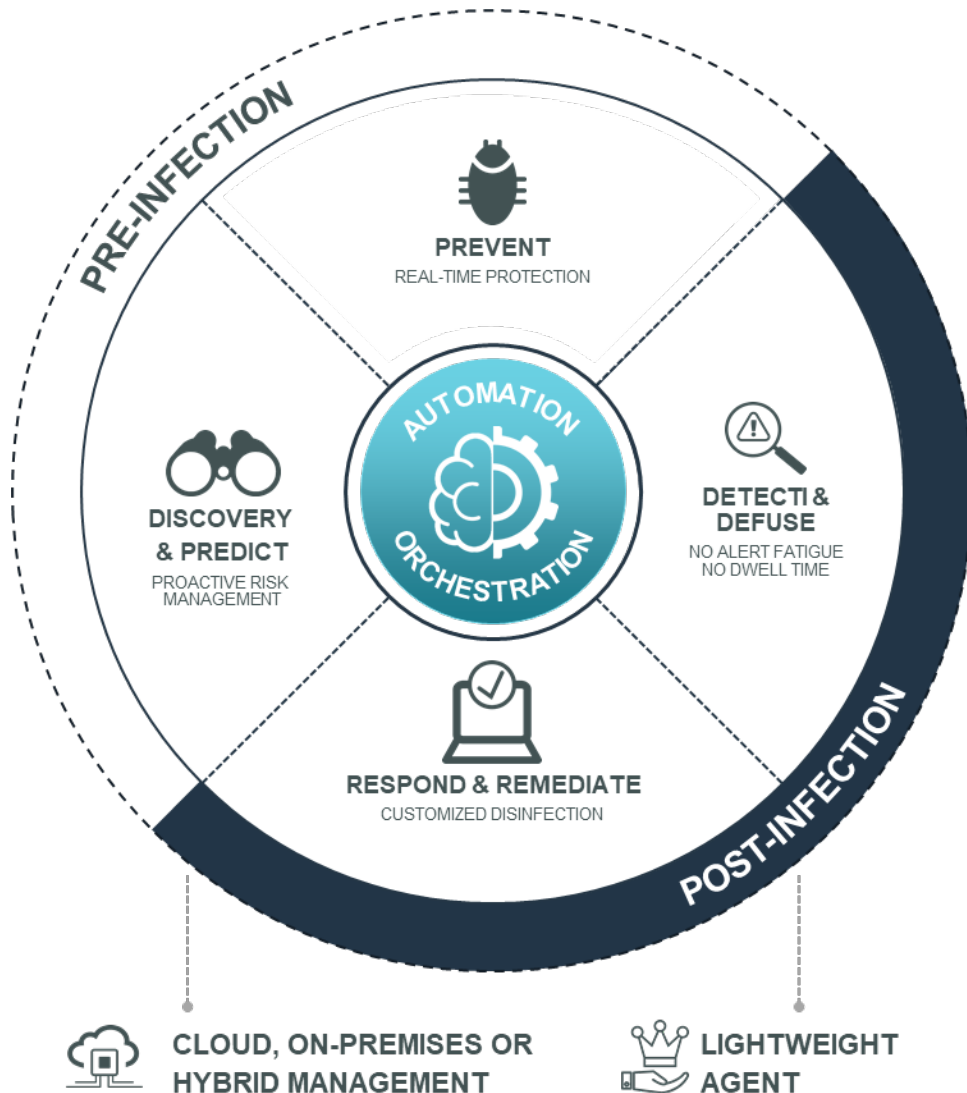
## Threat hunting

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.

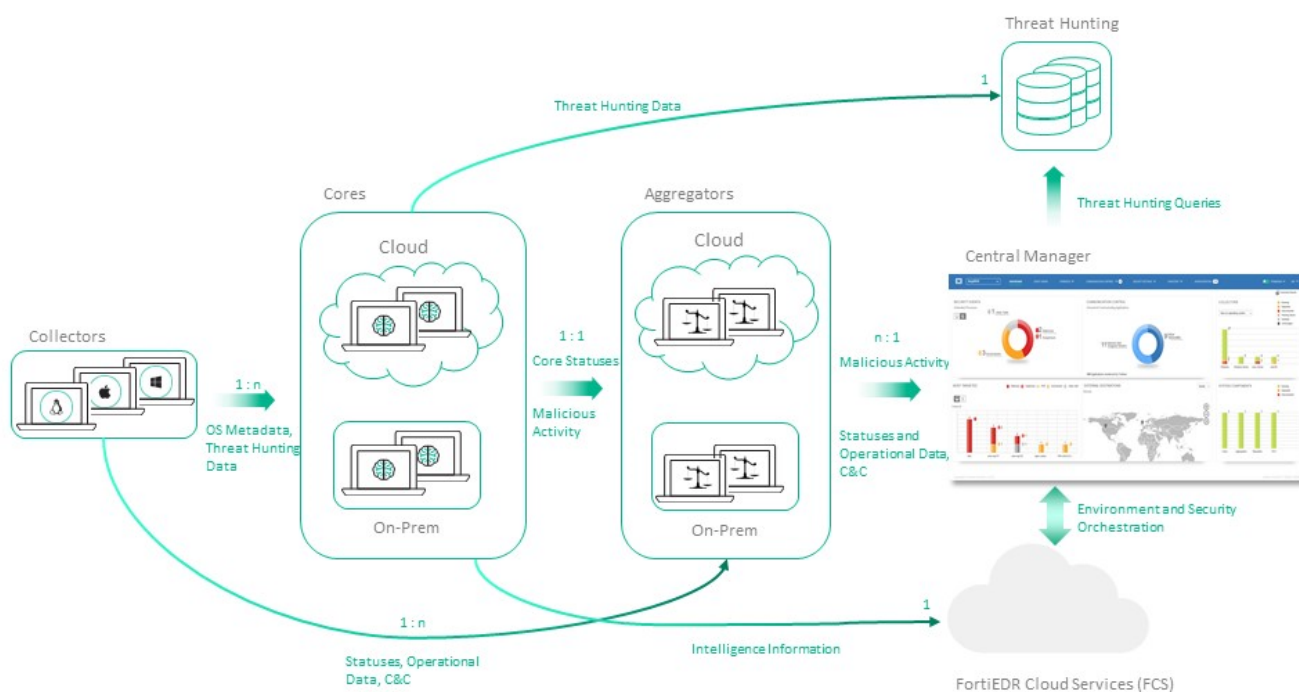
FortiEDR's technology prevents data exfiltration by identifying, in real time, malicious outgoing communications that were generated by external threat actors. Identification of malicious outgoing communications is the result of our research conducted on both operating system internals and malware operation 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 319](#).

---

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 [Before you start on page 21](#) 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.

### Event Viewer

The Windows Event Viewer records whenever a FortiEDR Collector blocks communication from a device, as described in [Event Viewer on page 146](#).

## 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). 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 to the FortiEDR Collectors and FortiEDR Cores.

Most deployments only require a single FortiEDR Aggregator that can be installed on the same server as the FortiEDR Central Manager. Additional FortiEDR Aggregators may be required for larger deployments of over 10,000 FortiEDR Collectors and can be installed on a different machine than the FortiEDR Central Manager.

## 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 64](#) to [Forensics on page 219](#) 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 75](#)
- **Playbook Actions:** All Playbook policy actions are based on the final determination of the FCS. For more details see [Playbook policies on page 101](#).

## 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.

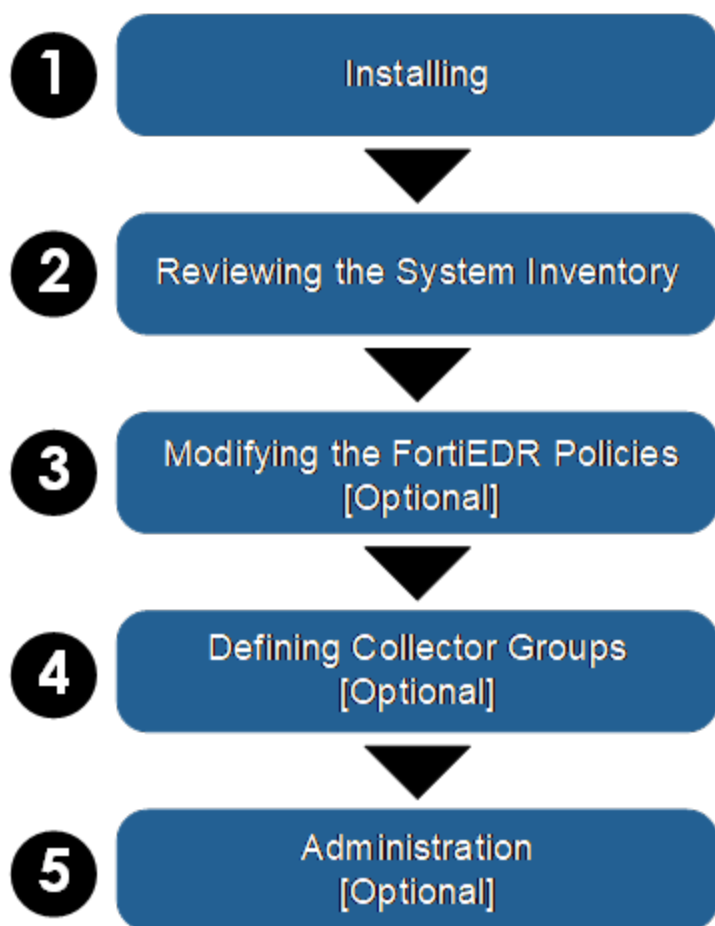
4. **Pass or block:** Only legitimate connections are allowed outbound communication. Malicious outbound connection attempts are blocked.
5. **Event Generation:** Each FortiEDR policy violation generates a realtime security event (alert) that is packaged with an abundance of device metadata describing 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:** Install all FortiEDR components, as described in [Deploying FortiEDR Collectors on page 21](#) and [Setting up a FortiEDR Core as a Jumpbox on page 57](#).
2. **Reviewing the Inventory:** Review the health status and details of all the FortiEDR components in the [Dashboard on page 133](#) and [Inventory on page 111](#). 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 64](#) 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 [Inventory on page 111](#). You can then assign the required policy to each Collector Group (see [Assigning a security policy to a Collector Group on page 72](#)).
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:
  - [Dashboard on page 133](#)
  - [Event Viewer on page 146](#)
  - [Syslog on page 314](#)



- **[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 101](#).
- **[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 156](#).
- **[Optional] Forensics (page 153):** This licensed add-on enables deep investigation into a security event, including the actual internals of the communicating devices' operating system.

# 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 21](#)
- [Uninstalling FortiEDR Collectors on page 53](#)
- [Upgrading the Collector on page 55](#)

Optionally you can install a Core to act as a jumpbox on your organization's premises (on-premises), see [Setting up a FortiEDR Core as a Jumpbox on page 57](#).

## Installing FortiEDR Collectors

You can install the FortiEDR Collector on any communicating device that meets the requirements in [Before you start on page 21](#). 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 281](#). If a custom Collector is used during the installation, all input fields such as Aggregator address and registration password are auto-filled.

---

- [Before you start on page 21](#)
- [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 43](#)
- [Automated FortiEDR Collector deployment on page 45](#)
- [Installing FortiEDR on Mac Big Sur devices using Jamf PRO on page 48](#)
- [Setting up exclusions with other AV products on page 52](#)
- [Working with FortiEDR on VDI environments on page 52](#)




For more details about installing a Collector in a multi-organization environment, see [Collector registration on page 378](#).

## Before you start

Before you start installing FortiEDR Collectors on the communicating device, make sure the device meets the following requirements:

- 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.

- Ports 555, 8081 and 443, which are used by FortiEDR Core, FortiEDR Aggregator and FortiEDR Central Manager respectively, are not blocked by your firewall product (if one is deployed). 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 8081 to the Aggregator IP address.
- Connectivity to the FortiEDR Core and the FortiEDR Aggregator. You can check this by browsing to the Core's IP address and the Aggregator's IP address. For problems connecting, see [Troubleshooting on page 374](#).
- System requirements:

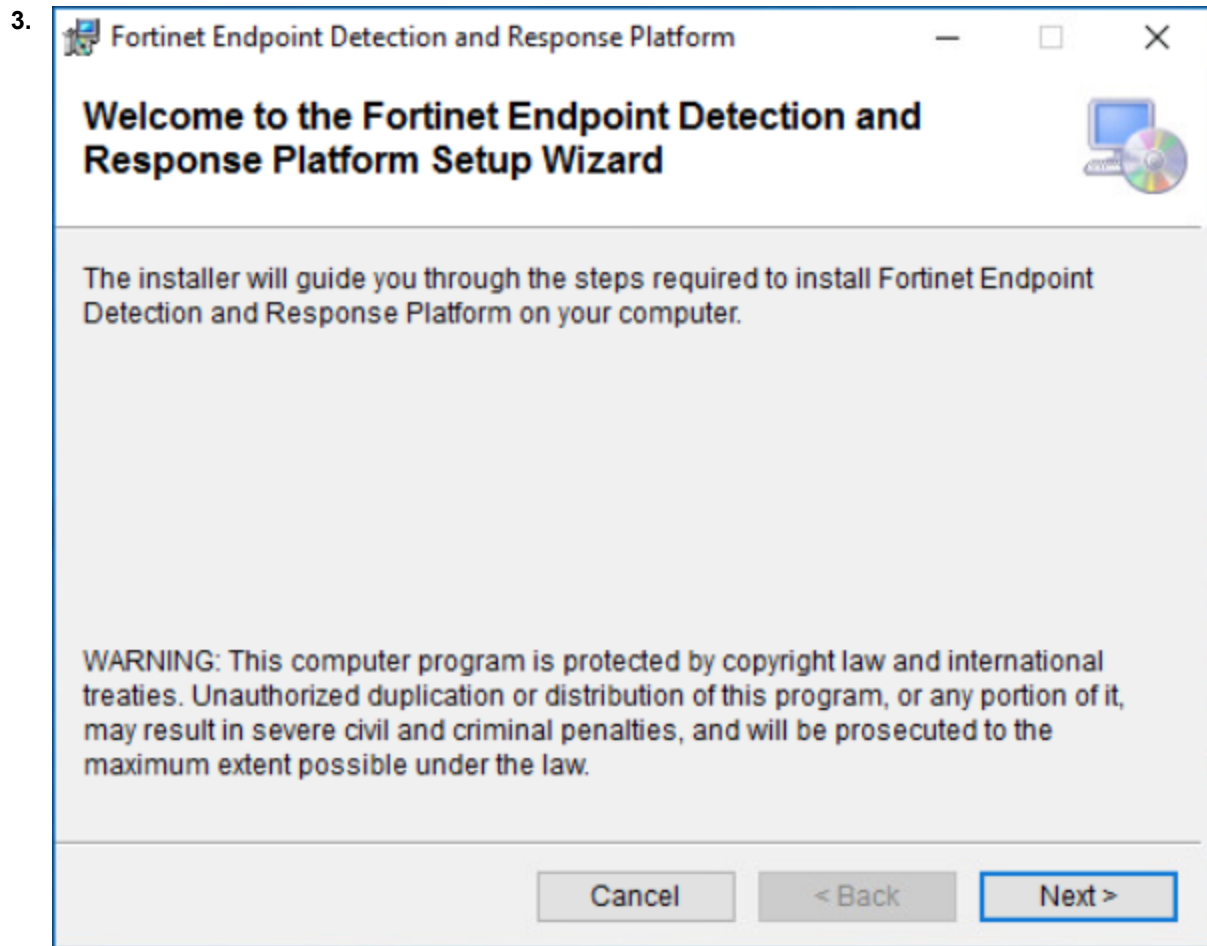
Component	System Requirements
Processor	<ul style="list-style-type: none"> <li>Intel or AMD x86 (32-bit and 64-bit)</li> <li>Apple M1 or M2 (ARM)</li> </ul>
Number of CPUs	1% to 2% CPU usage <div>  <p>FortiEDR Collector CPU consumption is highly dynamic by nature and varies depending on several factors:</p> <ul style="list-style-type: none"> <li>Variety of files and processes on the endpoint</li> <li>Activity on the endpoint</li> <li>Enabled features</li> </ul> </div>
Physical Memory	<ul style="list-style-type: none"> <li>200 MB to 250 MB without a Response (Threat Hunting) license</li> <li>300 MB to 350 MB with a Response (Threat Hunting) license</li> </ul>
Disk Space	<ul style="list-style-type: none"> <li>750 MB without a Response (Threat Hunting) license</li> <li>1 GB with a Response (Threat Hunting) license</li> </ul> <div>  <p>A Response (Threat Hunting) license results in more disk usage due to Threat Hunting audit activity data collection, such as activity on the device and the connection to the Core component status.</p> </div>
Connectivity	<ul style="list-style-type: none"> <li>Browser connection to the FortiEDR Central Manager is via port 443.</li> <li>Network connectivity between all system components is required.</li> <li>Allow up to 5 Mbps of additional network workload for each 1,000 Collectors.</li> </ul>
Supported Operating Systems	<p>The FortiEDR Collector can be installed on any of the following operating systems (both 32-bit and 64-bit versions):</p> <div>  <p>To avoid protection impact, please do not upgrade your devices to a new OS version (eg. Windows 11 23H1 or 23H2) before a compatible FortiEDR Collector version is available.</p> </div> <ul style="list-style-type: none"> <li>Windows Desktop:           <ul style="list-style-type: none"> <li>Windows 11</li> <li>Windows 10</li> <li>Windows 8.1</li> </ul> </li> </ul>

Component	System Requirements
	<ul style="list-style-type: none"> <li>• Windows 8</li> <li>• Windows 7 SP1</li> <li>• Windows XP SP2/SP3</li> <li>• Windows Server: <ul style="list-style-type: none"> <li>• Windows Server 2022</li> <li>• Windows Server 2019</li> <li>• Windows Server 2016</li> <li>• Windows Server 2012 R2</li> <li>• Windows Server 2012</li> <li>• Windows Server 2008 R2 SP2</li> <li>• Windows Server 2008 SP1</li> <li>• Windows Server R2 SP2</li> <li>• Windows Server 2003 SP2</li> </ul> </li> <li>• macOS: <ul style="list-style-type: none"> <li>• El Capitan (10.11)</li> <li>• Sierra (10.12)</li> <li>• High Sierra (10.13)</li> <li>• Mojave (10.14)</li> <li>• Catalina (10.15)</li> <li>• Big Sur (11)</li> <li>• Monterey (12)</li> <li>• Ventura (13)</li> <li>• Sonoma (14)</li> </ul> </li> <li>• Linux: <ul style="list-style-type: none"> <li>• RedHat Enterprise Linux (RHEL)</li> <li>• CentOS 6.8+, 7.2+ and 8+</li> <li>• Ubuntu LTS 16.04.5+, 18.04 and 20.04 server, 64-bit</li> <li>• Oracle Linux 6.10, 7.7+, and 8.2+</li> <li>• Amazon Linux AMI 2 2018</li> <li>• SUSE Linux Enterprise Server SLES v12 SP5 and v15</li> <li>• Open SUSE Leap 15.2</li> </ul> <p>The complete list of supported Linux versions and kernels is updated regularly and can be provided upon request.</p> </li> <li>• VDI Environments: <ul style="list-style-type: none"> <li>• VMware Horizons 6 and 7</li> <li>• Citrix XenDesktop 7</li> </ul> </li> </ul>

## Installing a FortiEDR Collector on Windows

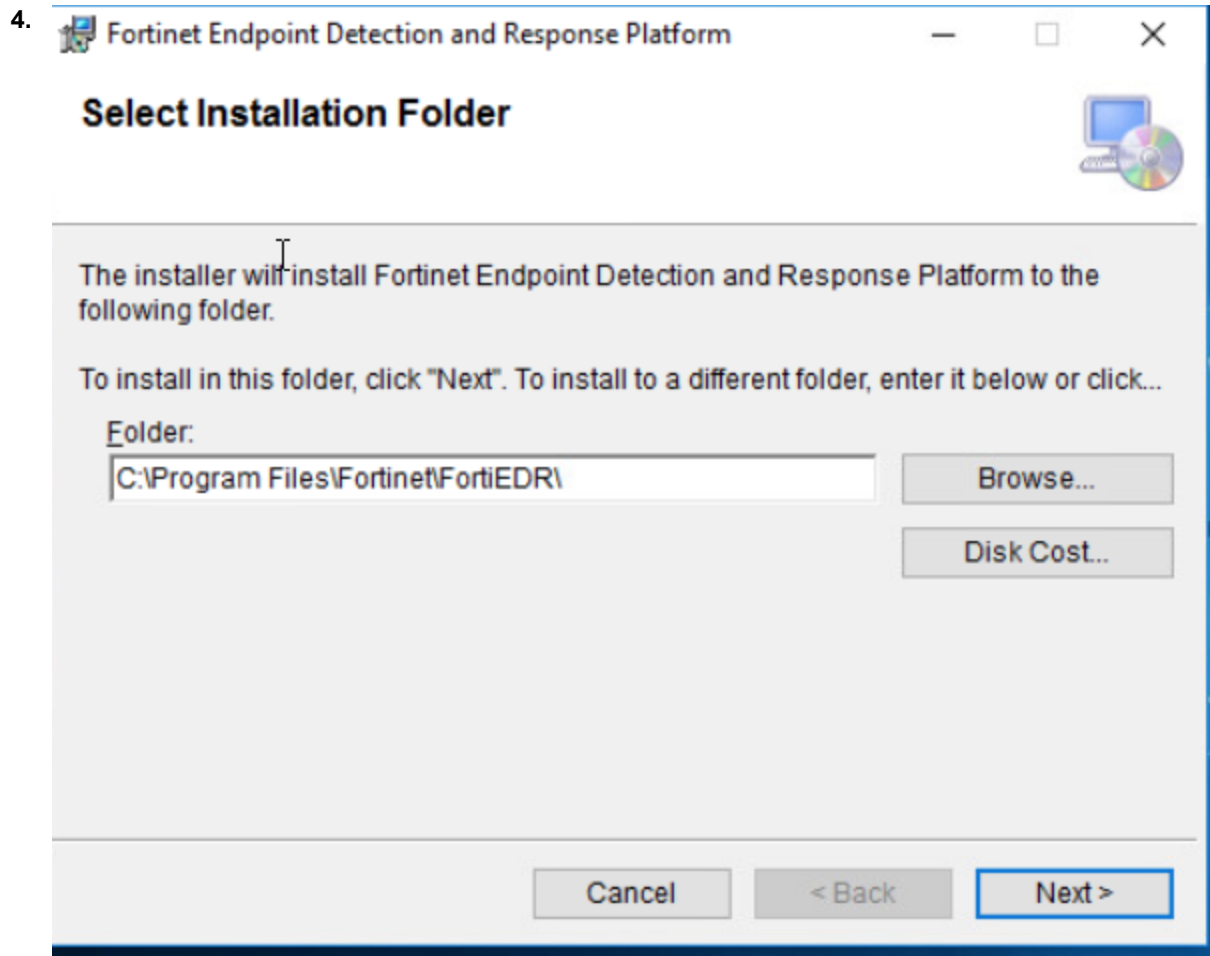
1. It is recommended to get a pre-populated customized Collector installer for Windows, as described in [Requesting and obtaining a Collector installer on page 281](#).

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.




Click *Next*.





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

5.  Fortinet Endpoint Detection and Response Platform

## Collector Configuration

Aggregator Address:  Port:

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.

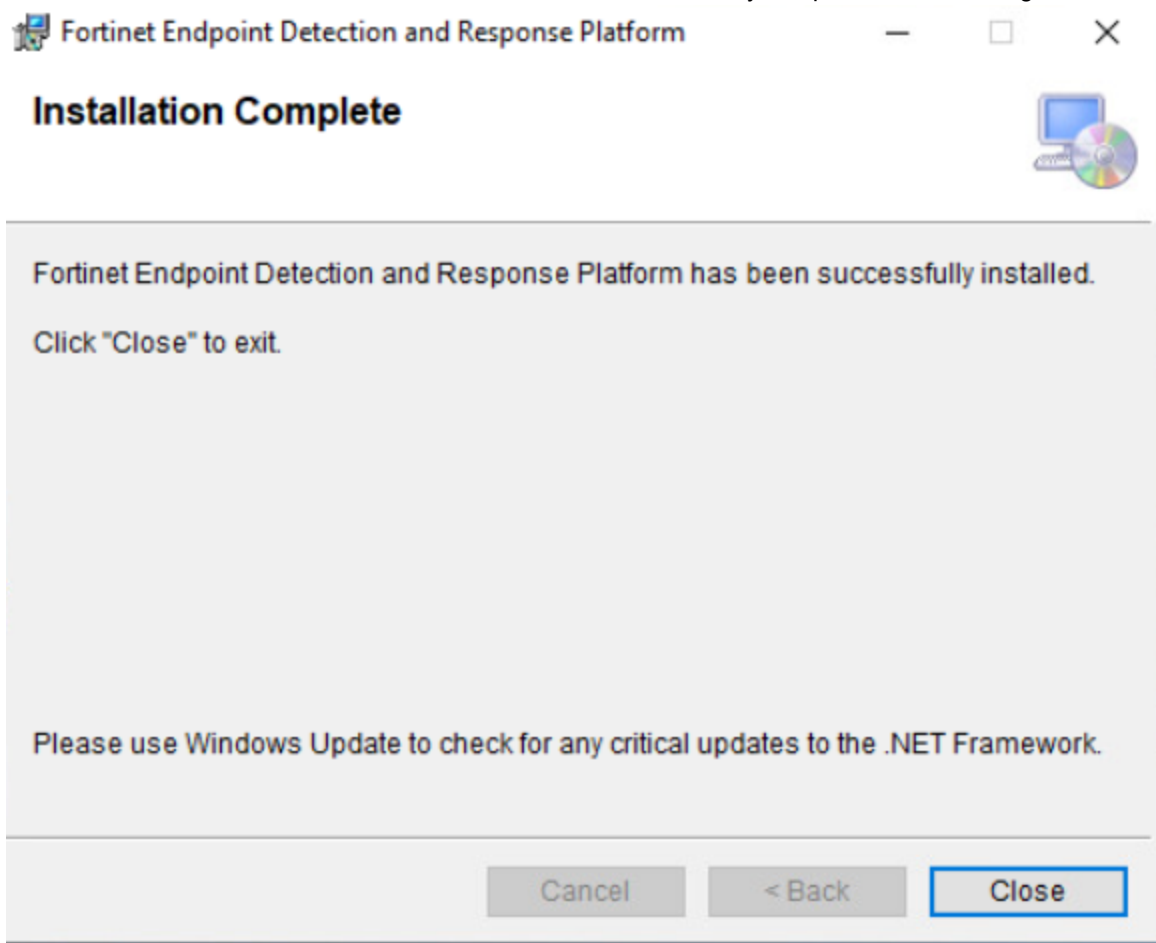
6. If a non-customized installer is used, in the *Port* field, specify the FortiEDR Aggregator port (8081).



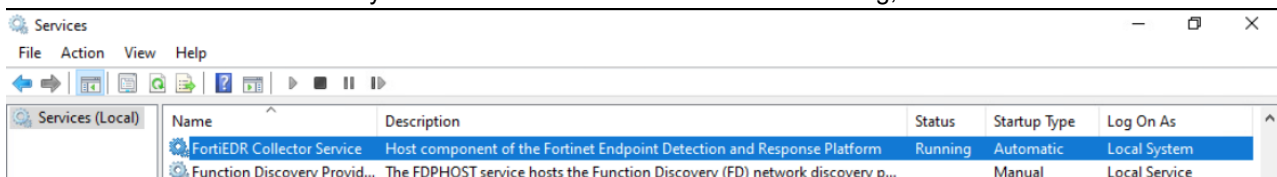
When upgrading a FortiEDR Collector, the Aggregator address field can be left empty – in order to retain the previously defined Aggregator address.

7. If a non-customized installer is used, in the *Registration Password* field, enter the device registration password that you received from Fortinet.
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 378](#).
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 52](#).
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.

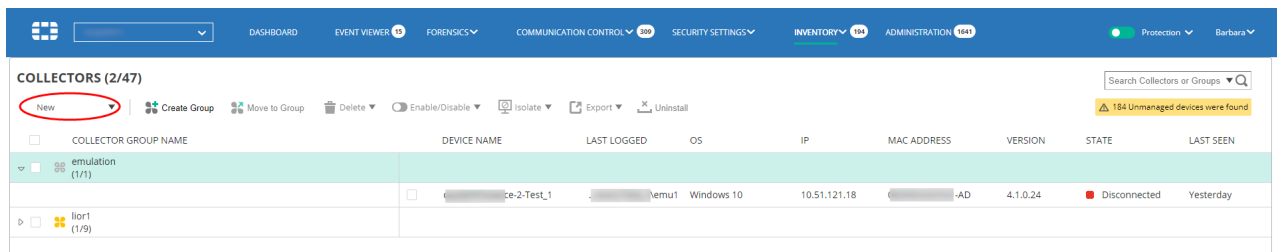
13. After the installation of the FortiEDR Collector has been successfully completed, the following window displays:



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



14. Verify that the FortiEDR Collector details are listed in the INVENTORY tab of the FortiEDR Central Manager console (see [Inventory on page 111](#)). Select the New filter to display a list of newly registered FortiEDR Collectors, as shown below:



15. 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 52](#).

## Installing a FortiEDR Collector on macOS

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

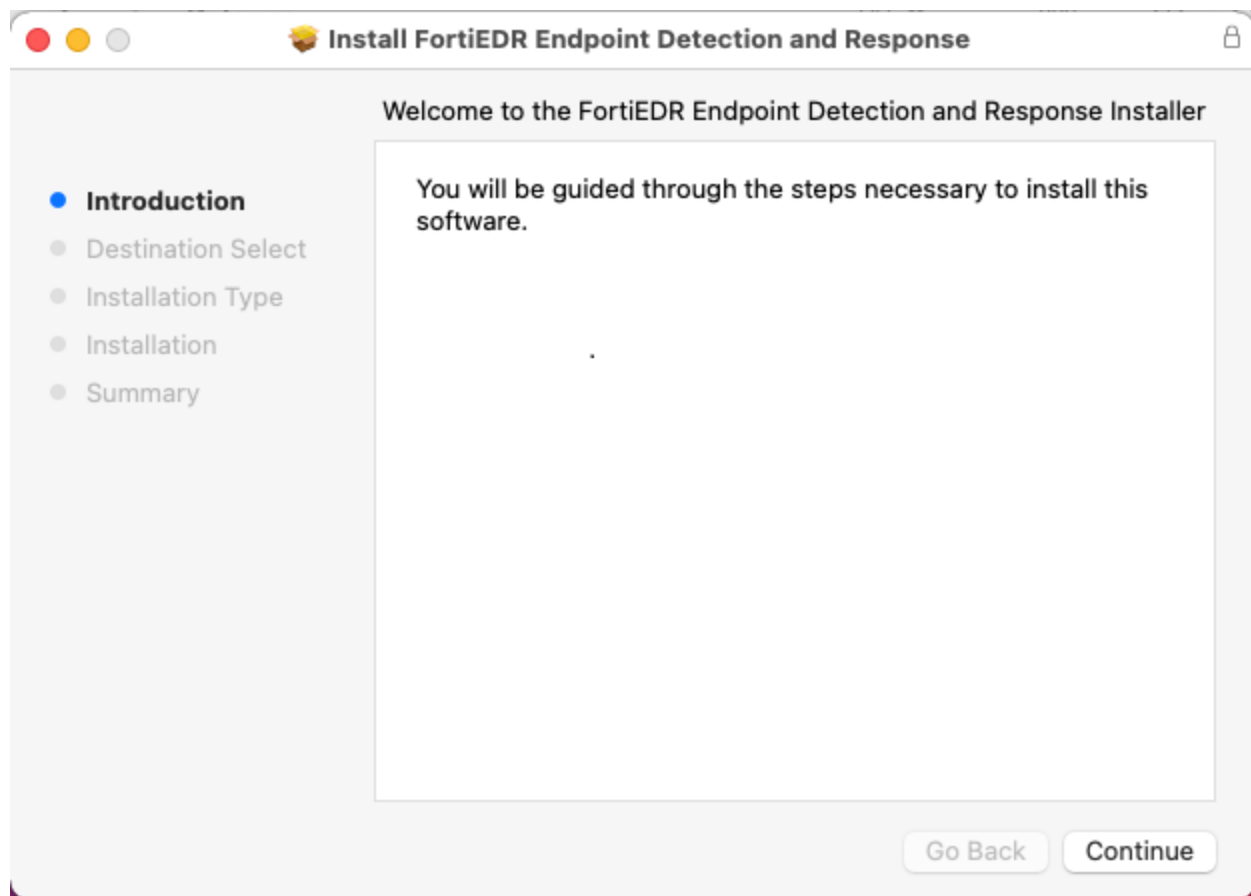
- System Extensions
- Network Extensions
- Full Disk Access

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

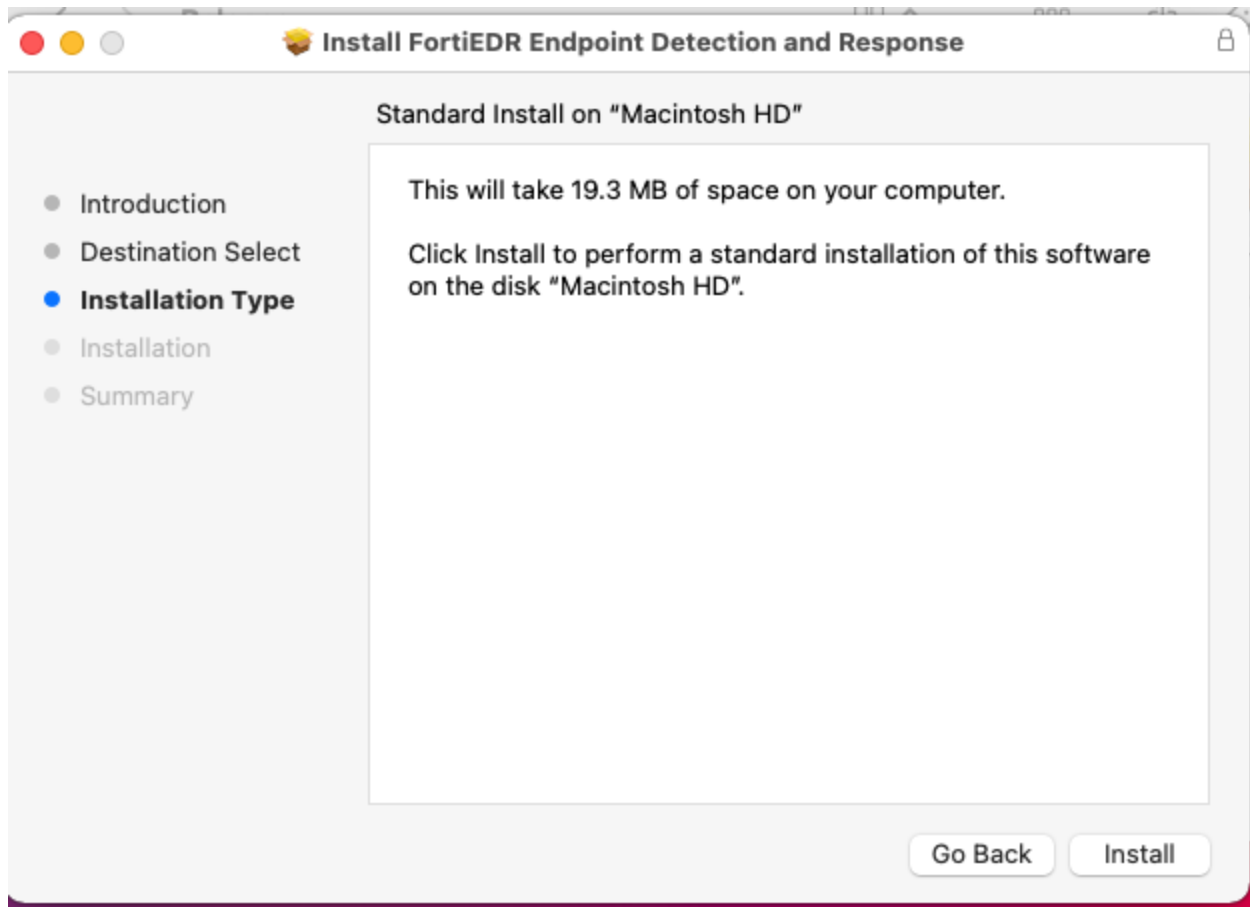
Deployment can also be managed using an MDM, such as Jamf.

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

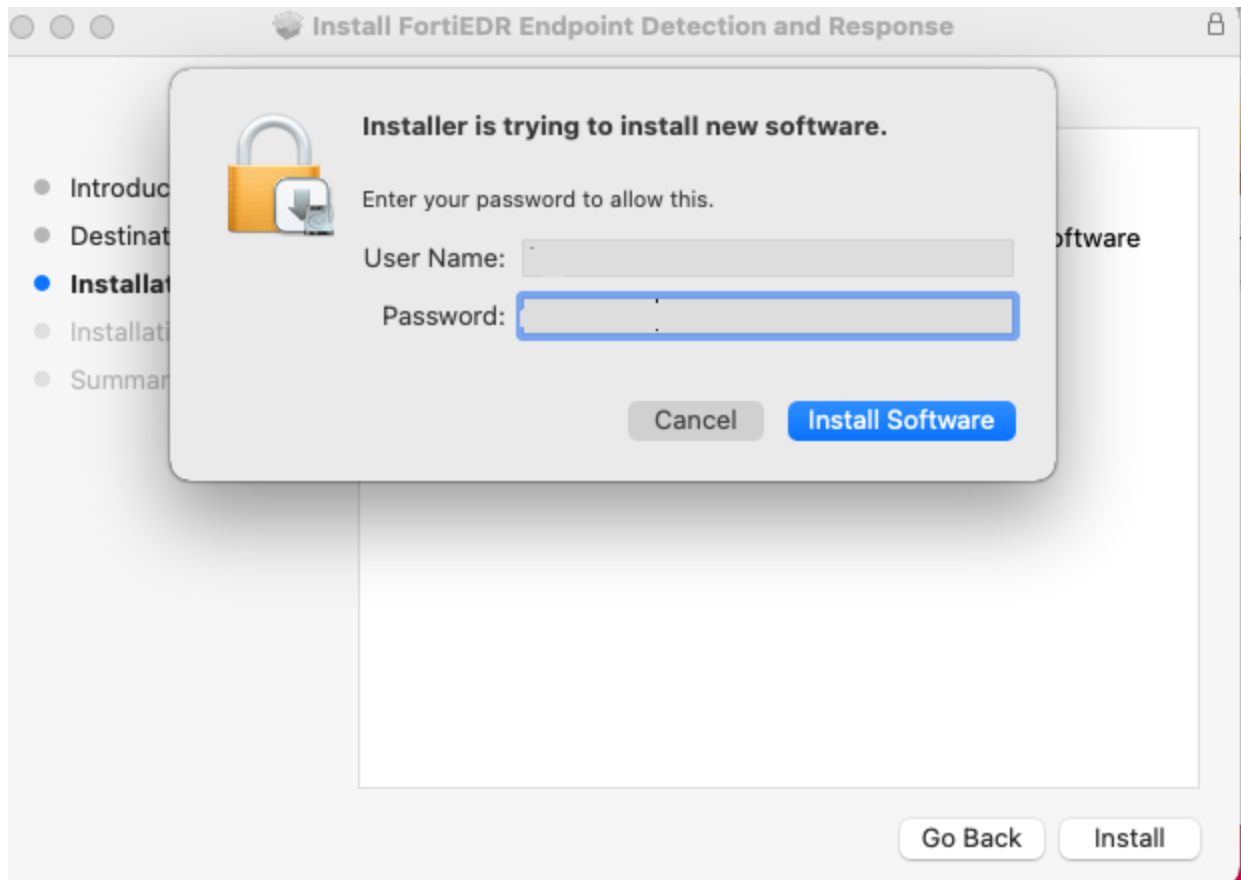
1. It is recommended to get a pre-populated customized Collector installer for macOS, as described in [Requesting and obtaining a Collector installer on page 281](#).
2. Double-click the \*.dmg file named `FortiEDRCollectorInstallerOSX_<version>.dmg`.
3. Click *Continue*.



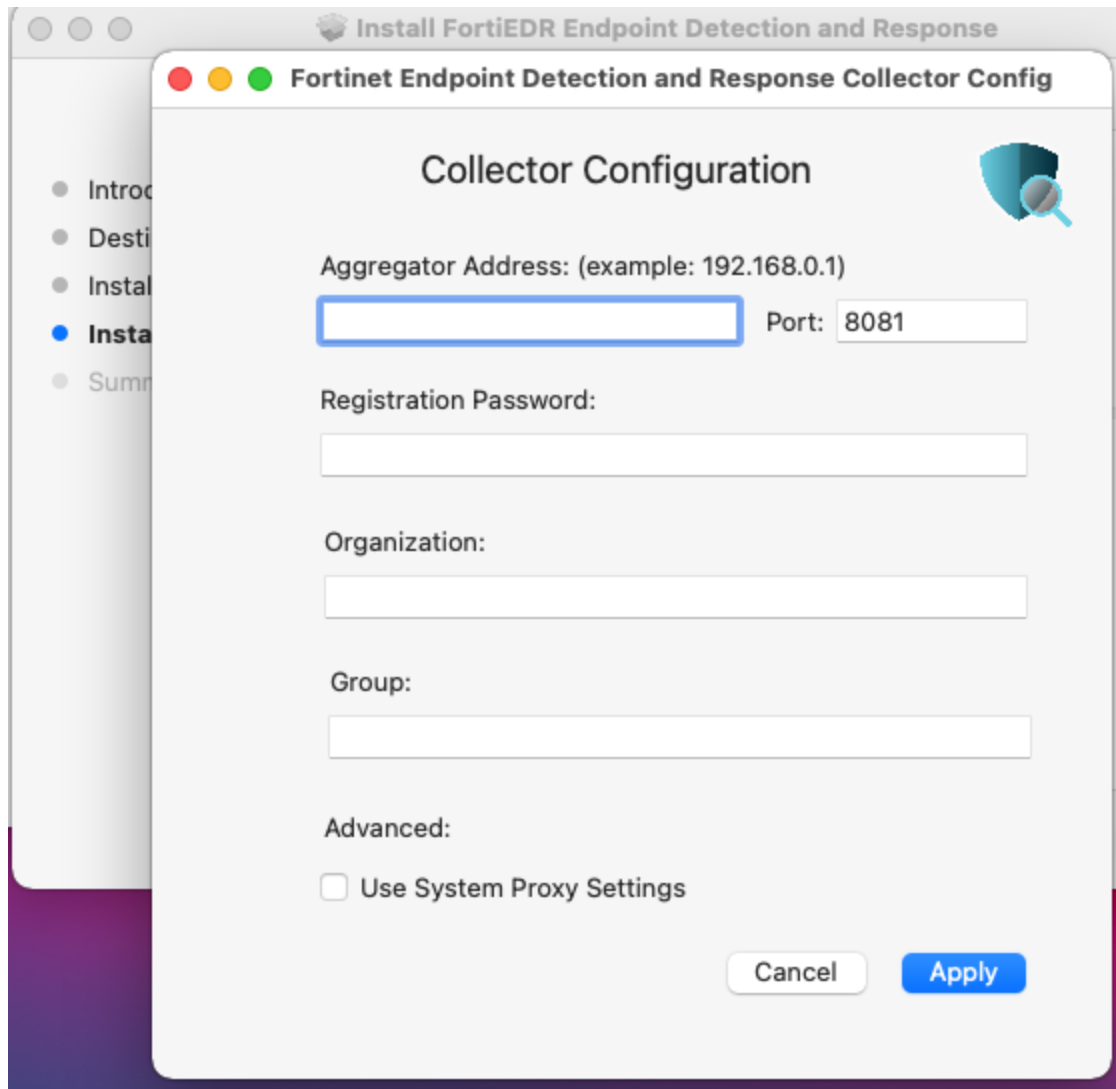
4. Click *Install*.



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



6. If a non-customized installer is used, in the *Collector Configuration* 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.



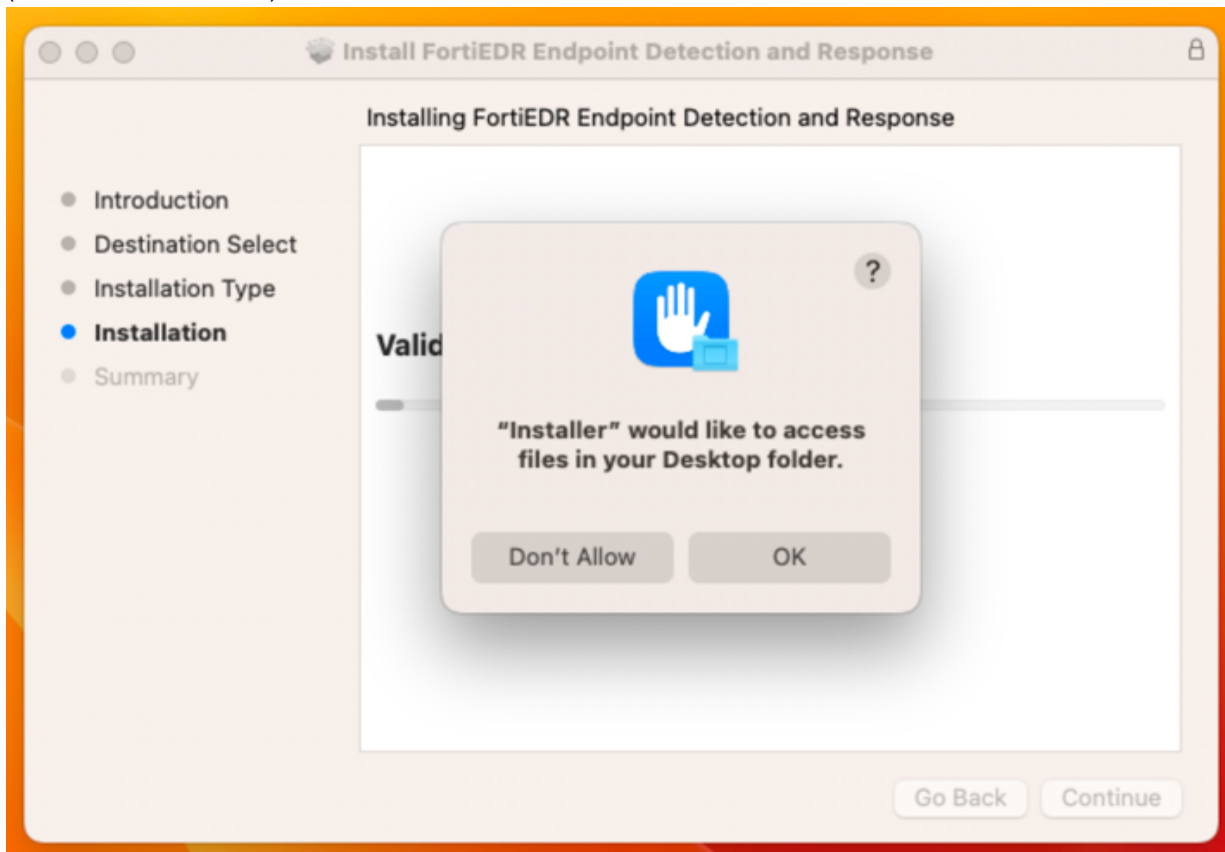
The screenshot shows a macOS window titled "Install FortiEDR Endpoint Detection and Response". Inside, there is a sub-window titled "Fortinet Endpoint Detection and Response Collector Config". The sub-window has a sidebar on the left with a list of steps: "Intro", "Desti", "Instal", "Insta" (highlighted with a blue dot), and "Summ". The main area of the sub-window is titled "Collector Configuration" and contains the following fields and options:

- Aggregator Address:** (example: 192.168.0.1) with a text input field.
- Port:** 8081 with a text input field.
- Registration Password:** with a text input field.
- Organization:** with a text input field.
- Group:** with a text input field.
- Advanced:**
  - ☐ Use System Proxy Settings

At the bottom right of the sub-window are two buttons: "Cancel" and "Apply".

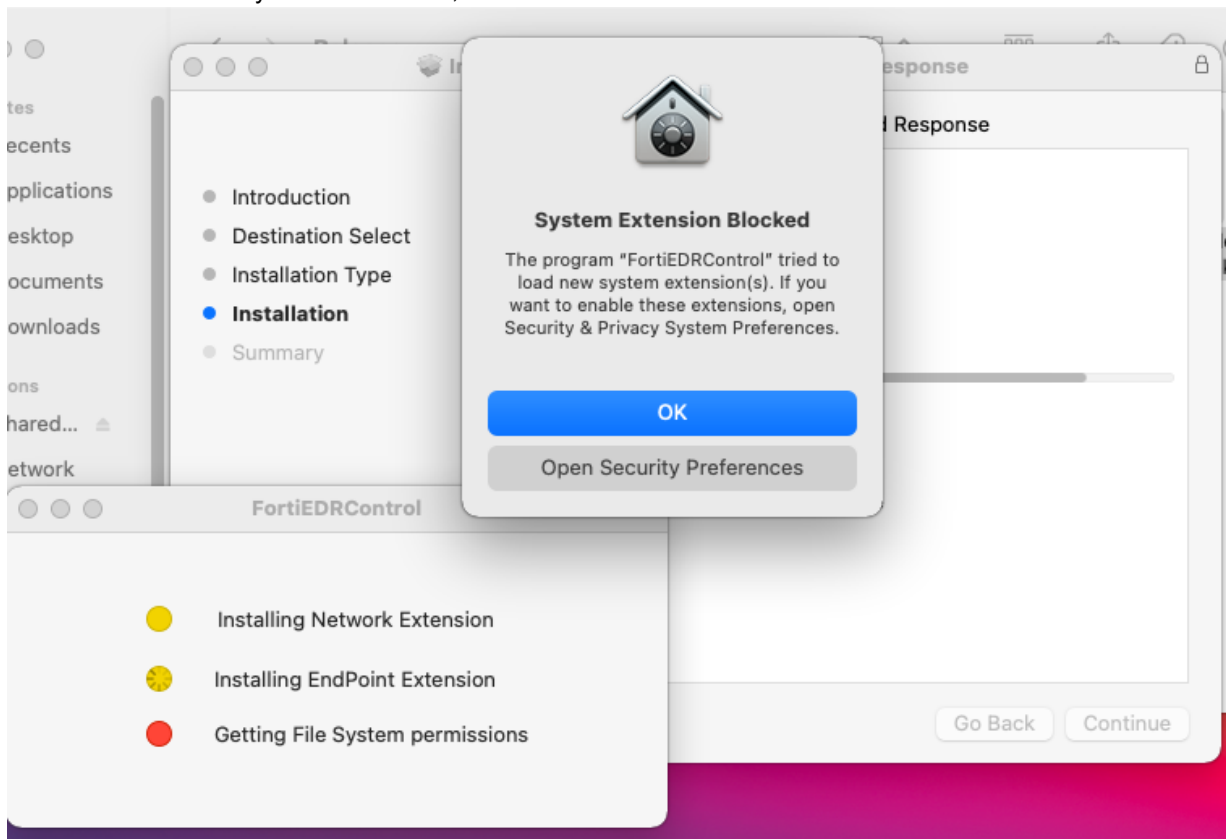
7. Click *Apply* to start the installation process.

8. Perform the following during installation:
  - a. (macOS v13.0 or above): Allow the installer to access files as shown below.



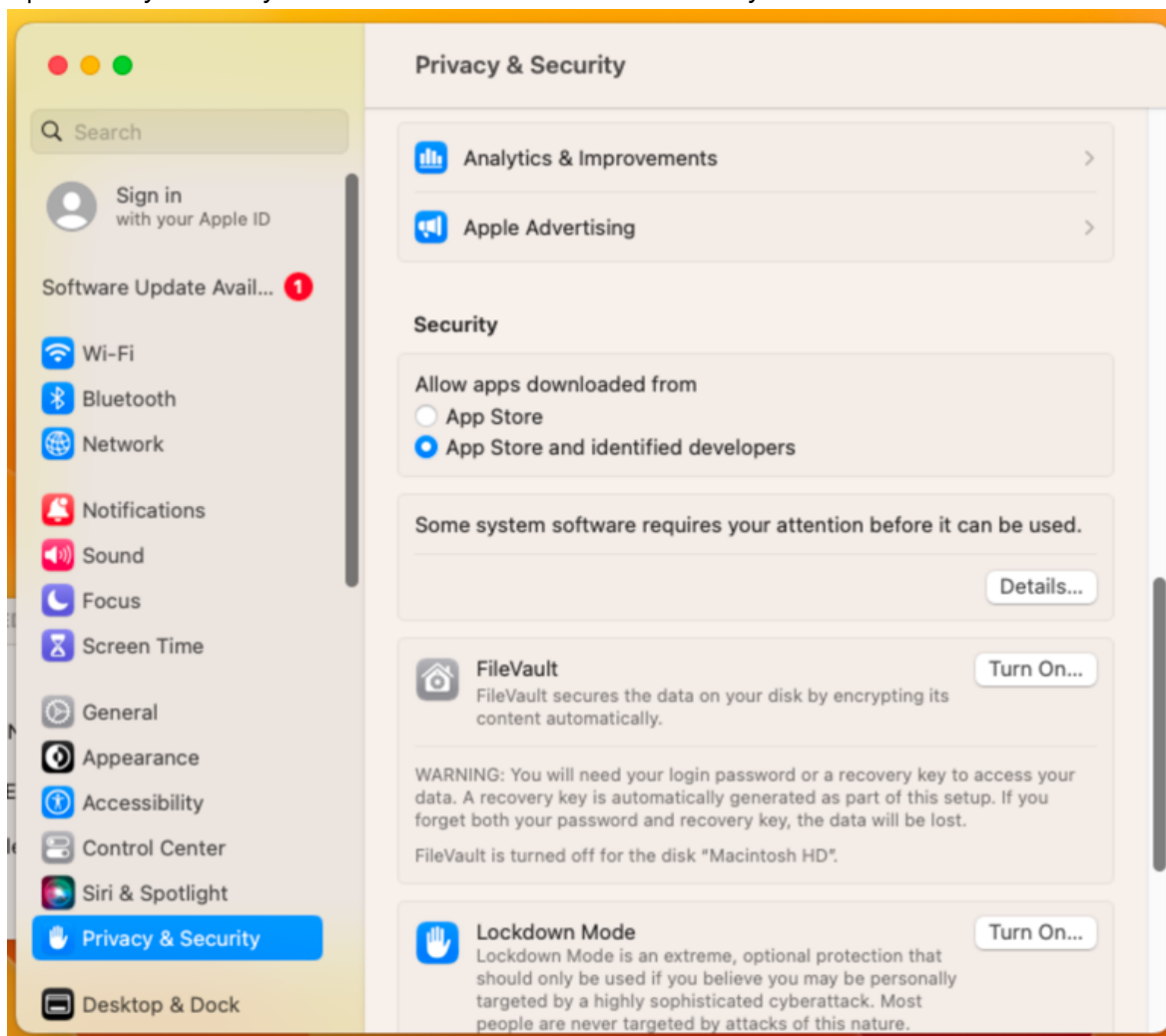


- b. Enable Network and System Extensions, shown below:



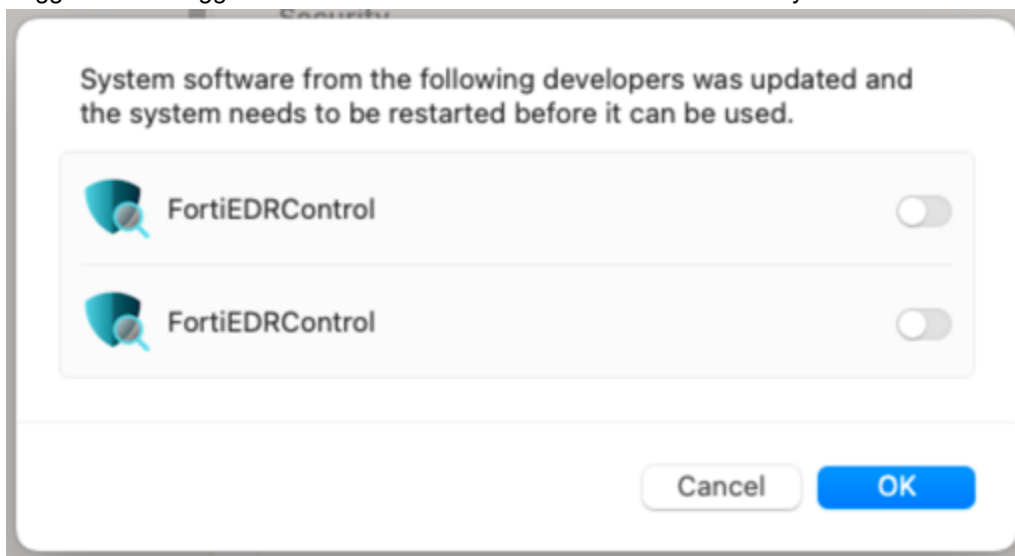
**macOS v13.0 or above:**

- i. Open *Privacy & Security Preferences* and scroll down to the *Security* section:



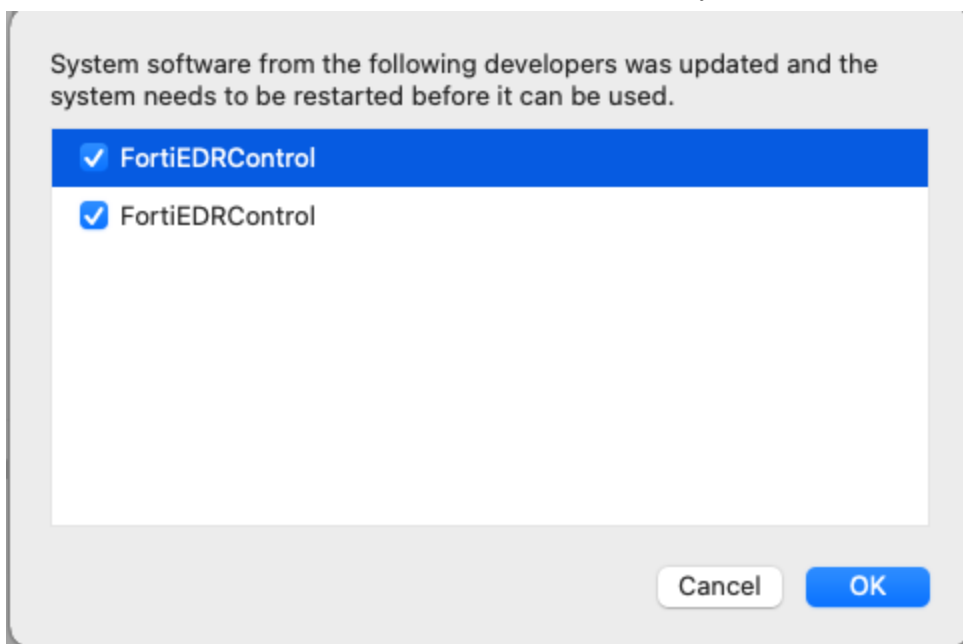
- ii. Under *Some system software requires your attention before it can be used*, Click *Details*.
- iii. Enter the Mac password at the prompt.

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



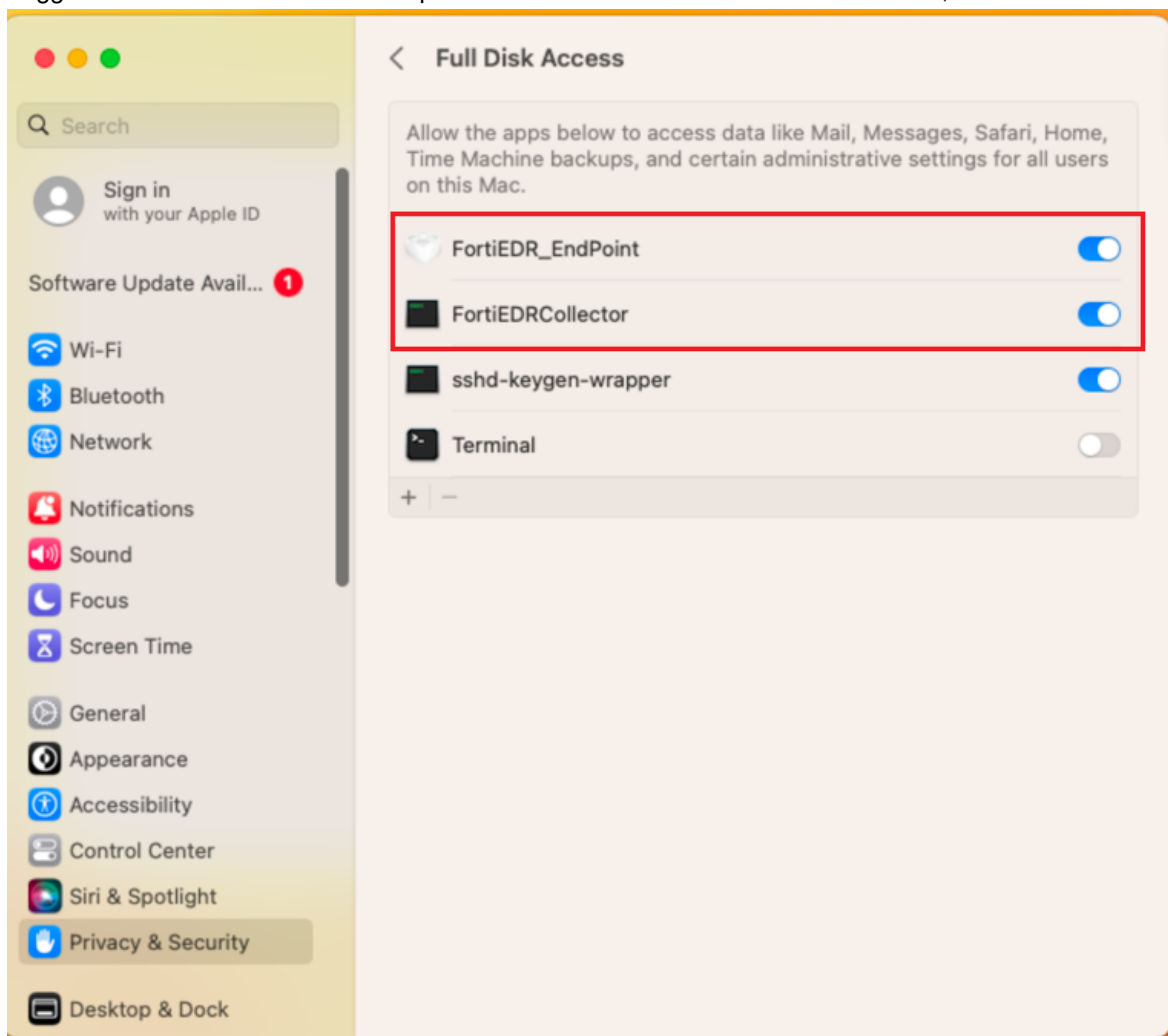
**macOS v11 or v12:**

- i. Open *Security Preferences*.
- ii. Click the lock at the bottom of the window in order to make changes.
- iii. In the *General* tab, click *Details*.
- iv. Mark both checkboxes to allow FortiEDR to use Network and System Extensions. Click *OK*.



- c. Enable Full Disk Access by performing the following:  
**macOS v13.0 or above:**

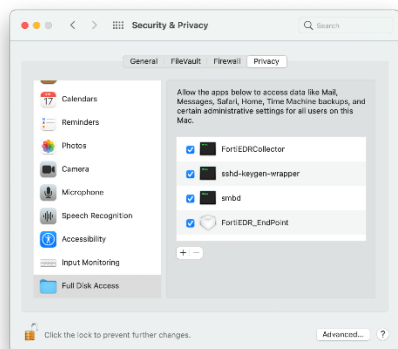
- i. Open Full Disk Access on *Security Preferences*.
- ii. Toggle on the two FortiEDR-related options to authorize full disk access for FortiEDR, as shown below.



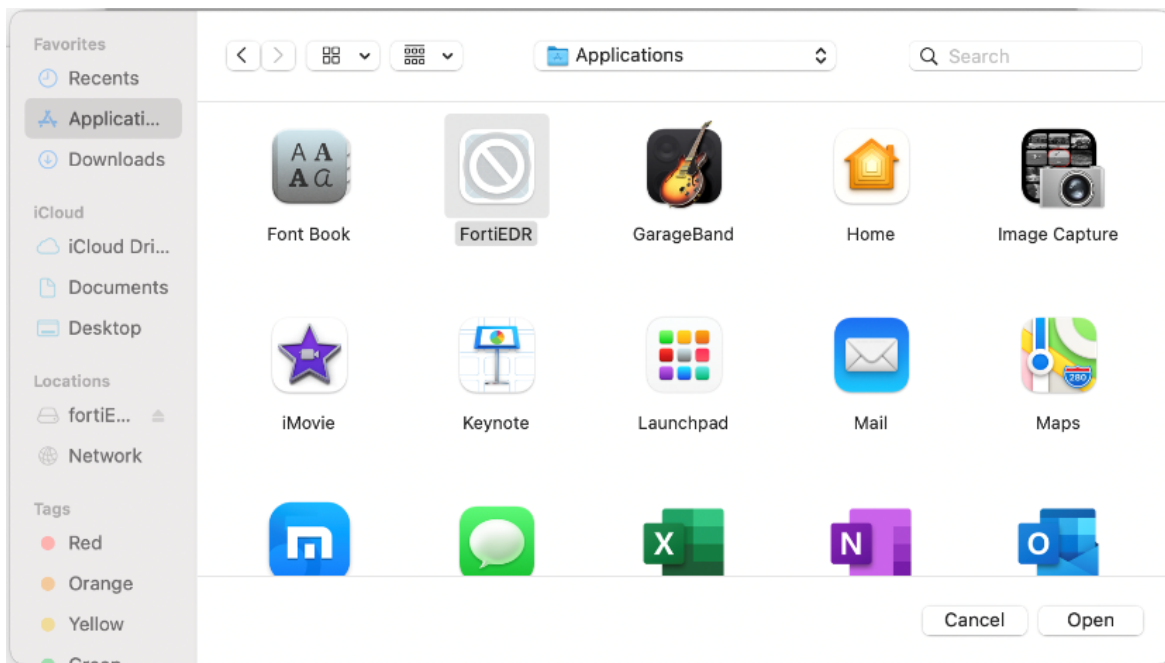
**macOS v11 or v12:**

- i. Open *Security Preferences*.
- ii. Click the lock at the bottom of the window in order to make changes.
- iii. In the *Privacy* tab, select *Full Disk Access* from the left pane.

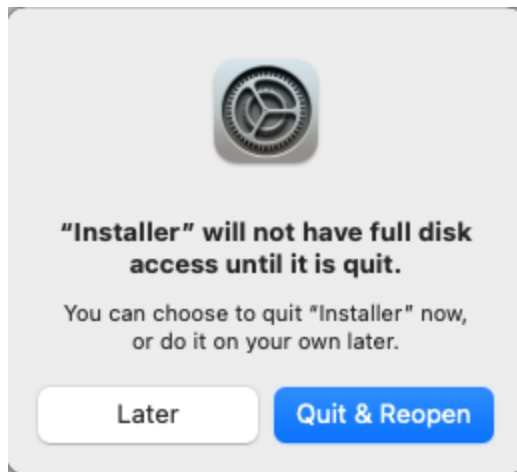
- iv. Select the checkboxes of both the *FortiEDRCollector* and the *FortiEDR\_EndPoint* applications:



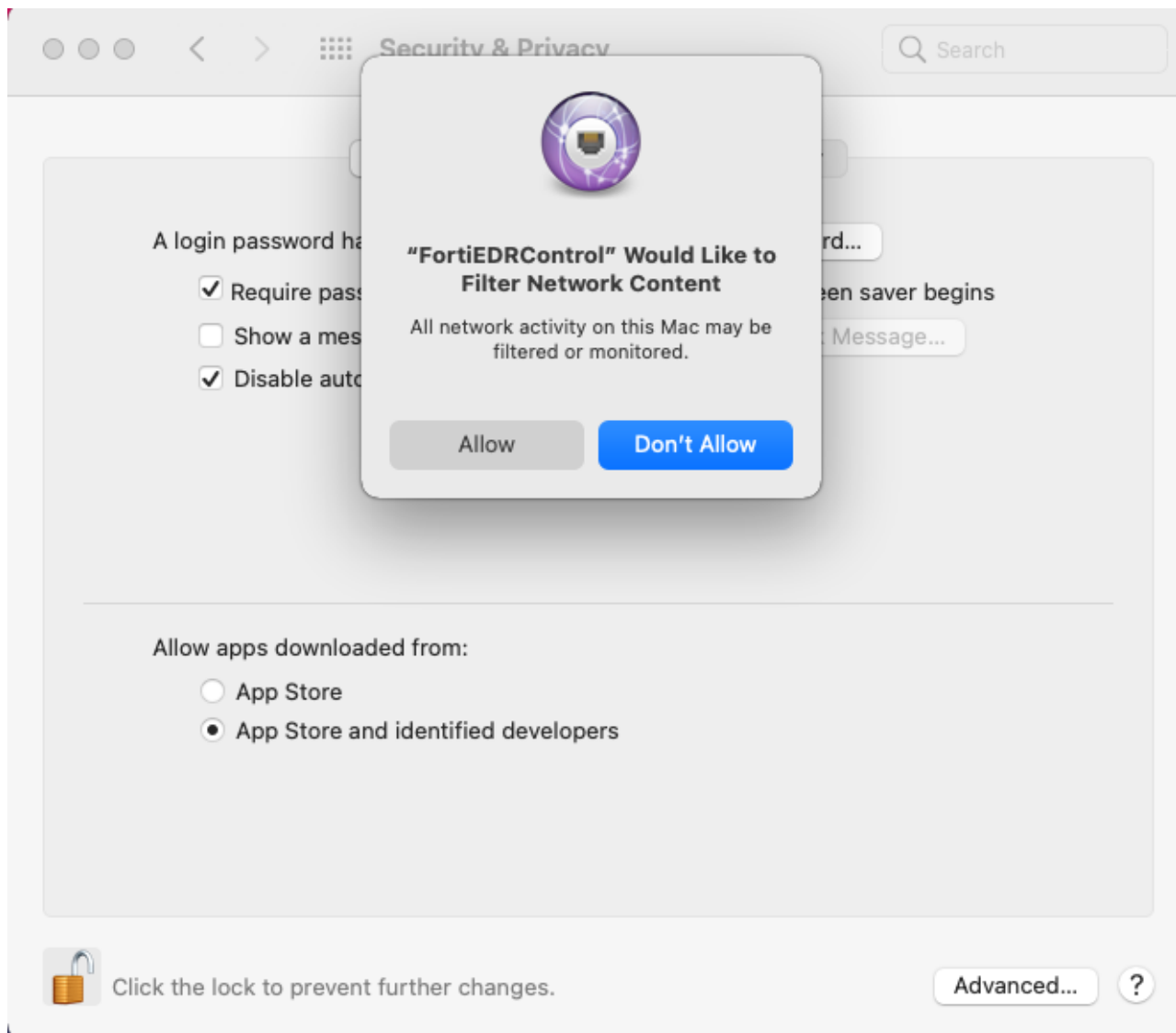
- v. If that FortiEDR application does not display on this page, click the + button.  
vi. Click *Applications*, select FortiEDR and then click *Open*.



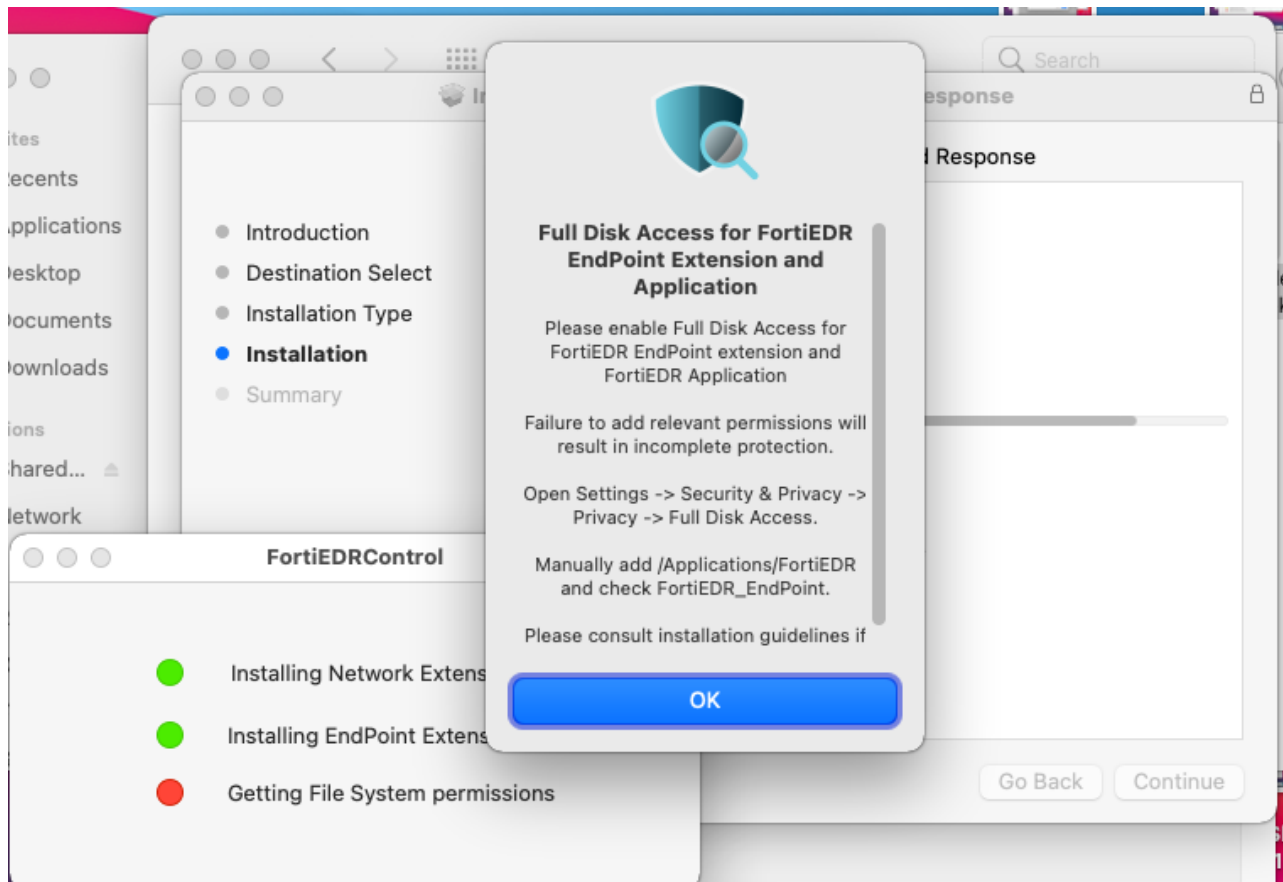
9. In the popup window, click *Later*.



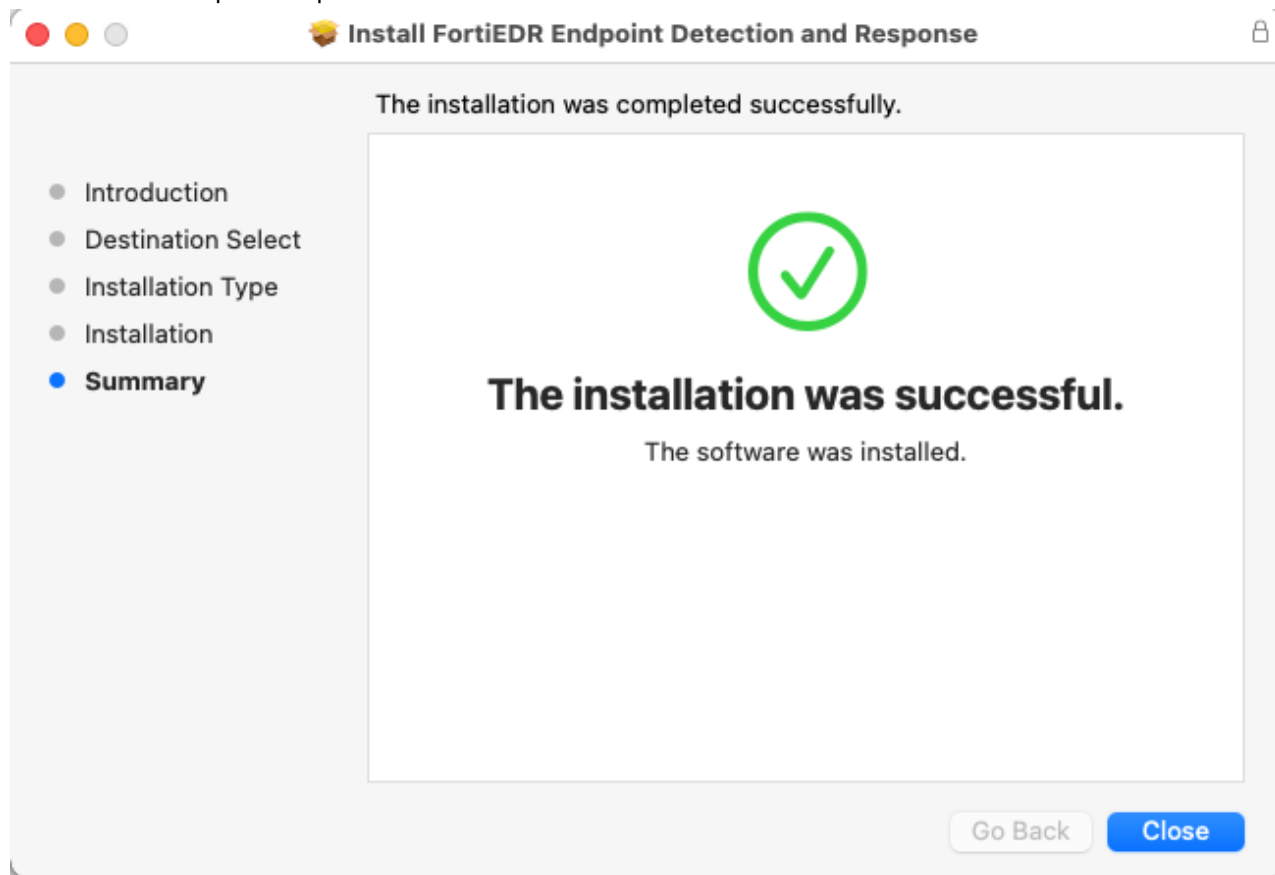
10. Click *Allow*.



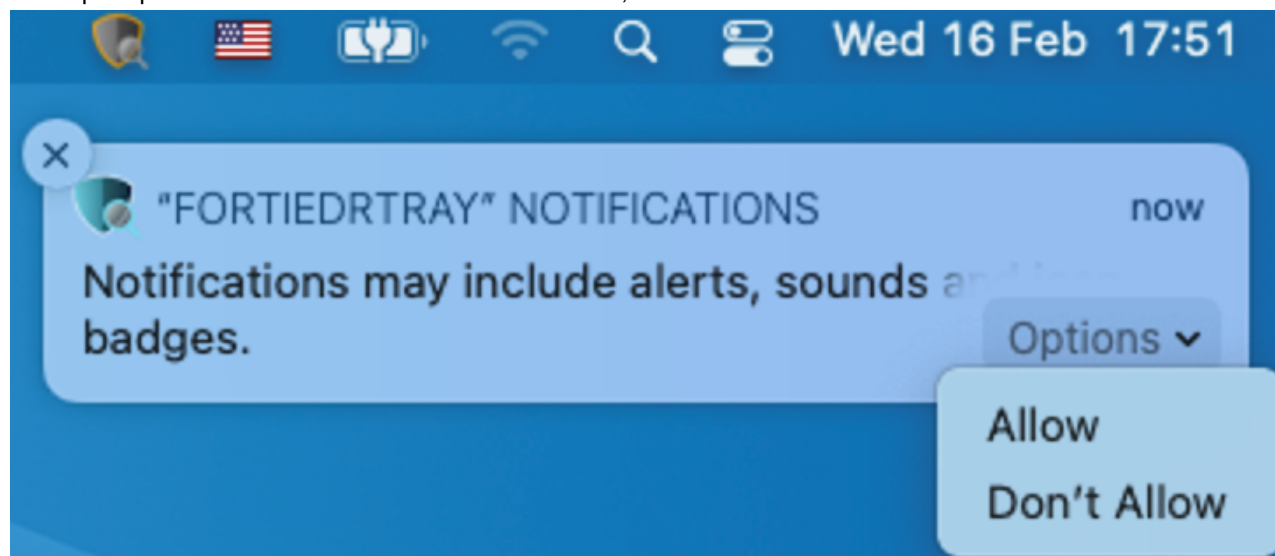
11. Click OK.



12. Click *Close* to complete the process.



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



14. Reboot the device.
15. You can run the following command to check the status of the Collector:

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



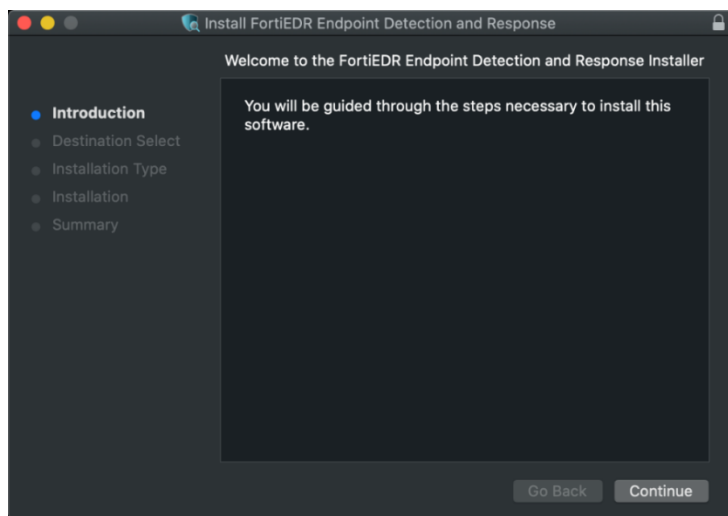
16. If another AV product is also installed on the machine, exclude AV exceptions by following the instructions in [Setting up exclusions with other AV products on page 52](#).

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

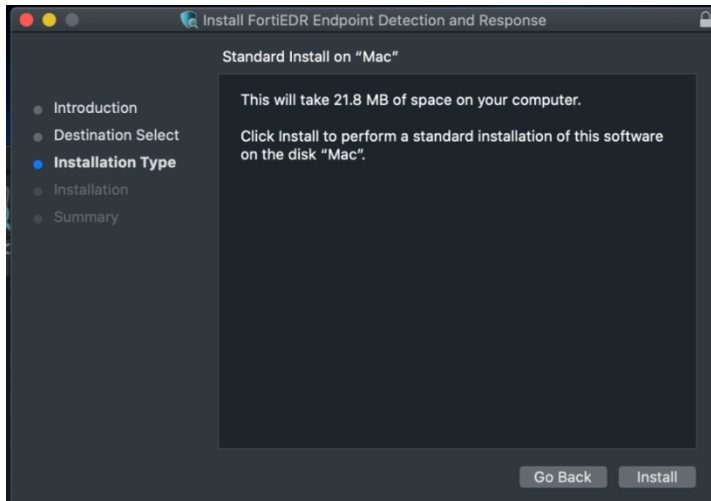
1. It is recommended to get a pre-populated customized Collector installer for macOS, as described in [Requesting and obtaining a Collector installer on page 281](#).
2. Double-click the \*.dmg file named FortiEDRCollectorInstallerOSX\_1.3.0.xxx.dmg.
3. Double-click the \*.pkg file named FortiEDRCollectorInstallerOSX\_1.3.0.xxx.pkg.



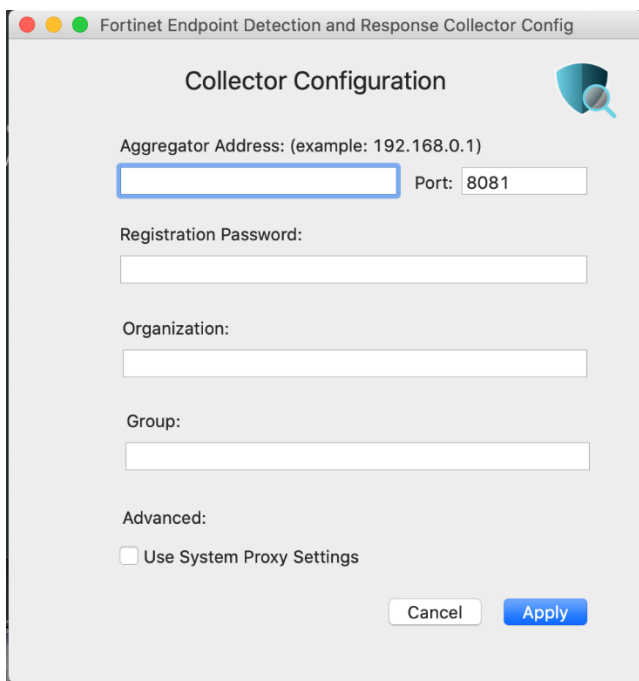
4. Click *Continue*.



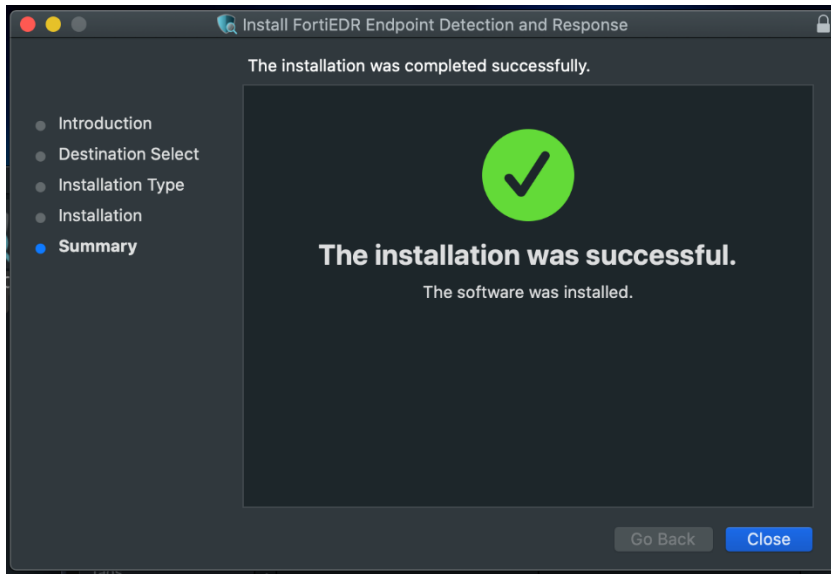
5. Select the destination disk and click *Continue*.
6. Specify the installation location and click *Install*.



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.



8. If a non-customized installer is used, in the *Registration Password* field, enter the registration password that you received from Fortinet.
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*.



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 52](#).

## Installing a FortiEDR Collector on Linux

### 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 281](#).
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 281](#).
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 [Setting up exclusions with other AV products on page 52](#).

### 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 281](#).

```
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
```

- Specify the FortiEDR Aggregator domain name or IP address.
- Enter the FortiEDR Aggregator port information (usually 8081).
- For a multi-tenant setup, enter the organization. Otherwise, leave the organization empty.
- Enter Collector Group information or leave empty to be registered to the default Collector Group.
- Enter the device registration password that you received from Fortinet.
- At the *Do you want to connect via proxy (Y/N)?* prompt, type *Y* if your setup includes a web proxy.
- 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.
- 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 281](#).
- 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 52](#).



Installation of the FortiEDR Linux Collector on a VM that is running other components of FortiEDR such as Core or Aggregator requires adding a special hidden configuration. Contact [Fortinet Support](#) for more assistance.

## 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 281](#).
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 52](#).

#### 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 Collector Group to assign this Collector to by adding the DEFGROUP parameter. This parameter is optional. When you specify this parameter, the first time that this Collector registers with the system, it is automatically assigned to the Collector Group specified by the DEFGROUP parameter.

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, use the device registration password 1234, use the DEFGROUP parameter and enter the following command:

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



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 281](#).
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 52](#).

## 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 281](#).
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.json
```

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.json
```

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.json
```

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 52](#).

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

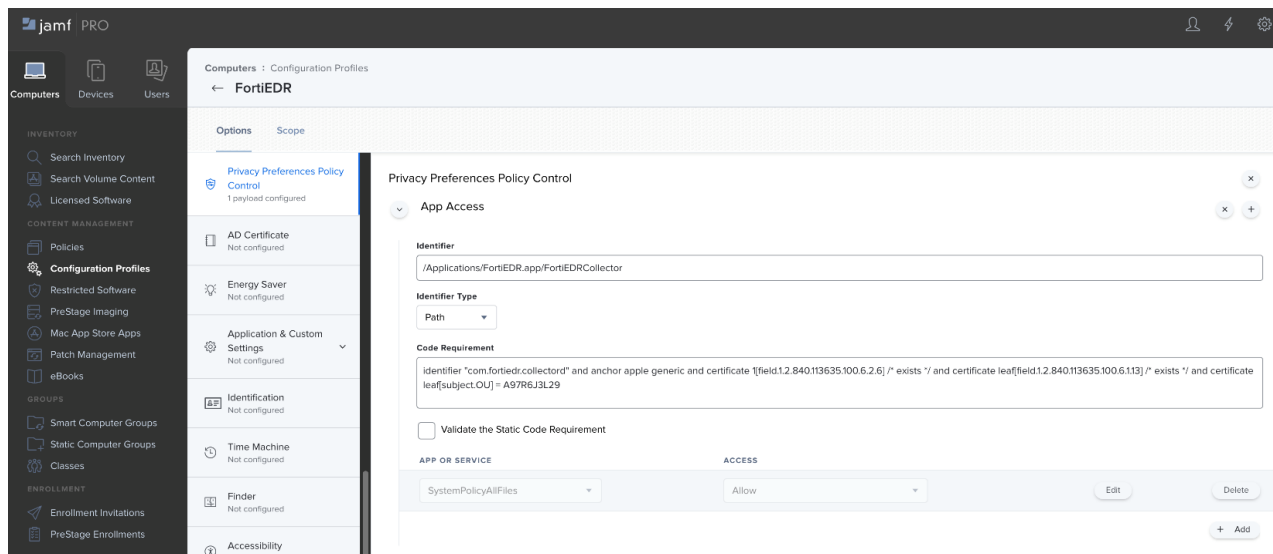
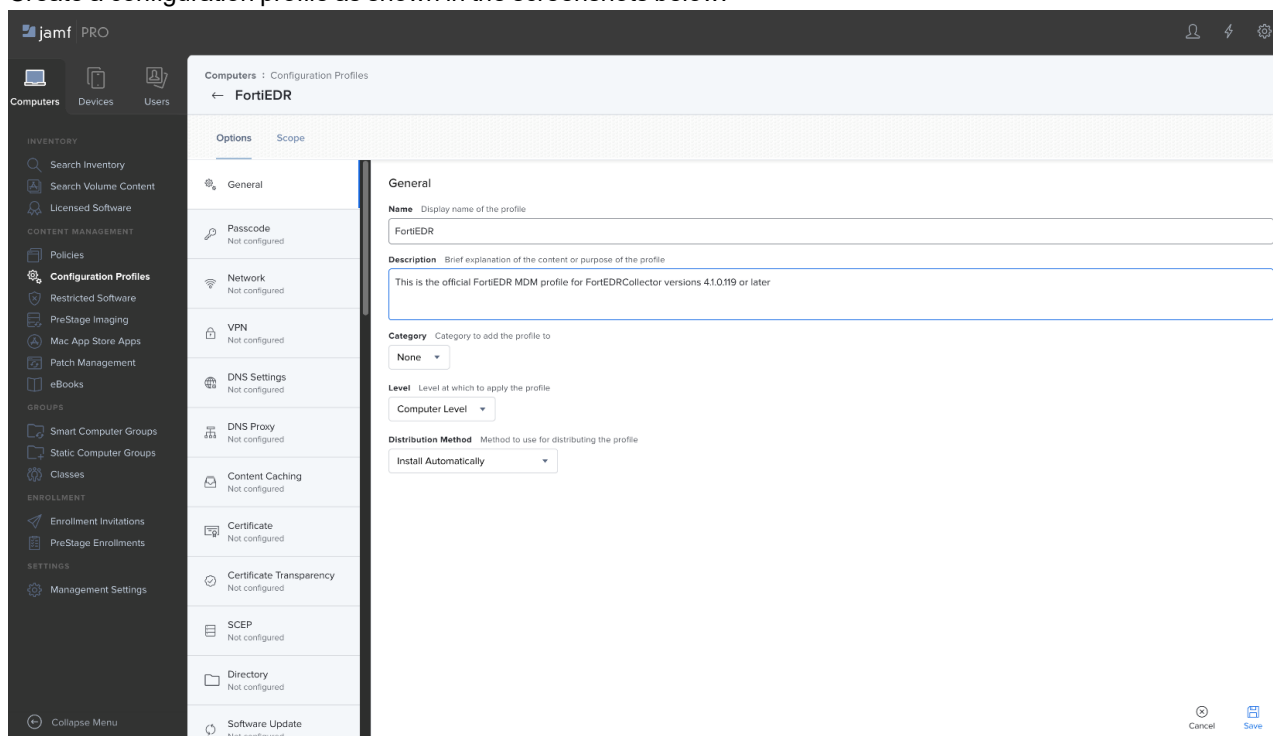
When distributed with MDM solutions such as Jamf, FortiEDR can be allowlisted with the following Team ID and Bundle ID identifiers:

- A97R6J3L29 com.ensilo.ftnt
- A97R6J3L29 com.ensilo.ftnt.sysex

## Installing FortiEDR on Mac Big Sur devices using Jamf PRO

### To install FortiEDR on Mac Big Sur devices using Jamf PRO:

1. In jamf PRO, navigate to *Computers > Configuration Profiles > New*.
2. Create a configuration profile as shown in the screenshots below:





The image displays two screenshots of the Jamf Pro interface, specifically the 'Computers > Configuration Profiles > FortiEDR' section.

**Top Screenshot: App Access Configuration**

- Options Tab:** Shows various configuration items like Privacy Preferences Policy, AD Certificate, Energy Saver, Application & Custom Settings, Identification, Time Machine, Finder, Accessibility, Proxies, and App-To-Per-App VPN.
- App Access Section:**
  - Identifier:** com.ensilo.fnt.sysext
  - Identifier Type:** Bundle ID
  - Code Requirement:** anchor apple generic and identifier "com.ensilo.fnt.sysext" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /\* exists \*/ or certificate leaf[field.1.2.840.113635.100.6.2.6] /\* exists \*/ and certificate leaf[field.1.2.840.113635.100.6.1.3] /\* exists \*/ and certificate leaf[subject.OU] = A97R6J3L29
  - Validate the Static Code Requirement:** (checkbox)
  - APP OR SERVICE:** SystemPolicyAllFiles
  - ACCESS:** Allow

**Bottom Screenshot: System Extensions Configuration**

- Options Tab:** Shows various configuration items like Proxies, App-To-Per-App VPN Mapping, Xsan, Smart Card, System Migration, Approved Kernel Extensions, Associated Domains, and Extensions.
- System Extensions Section:**
  - Allow users to approve system extensions:** (checked)
  - 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.fnt (Edit, Delete)
    - com.ensilo.fnt.sysext (Edit, Delete)

The screenshot shows the 'Content Filter' configuration page in the Jamf Pro interface. The left sidebar contains navigation menus for 'INVENTORY', 'CONTENT MANAGEMENT', 'GROUPS', 'ENROLLMENT', and 'SETTINGS'. The main content area is titled 'Computers : Configuration Profiles' and 'FortiEDR'. It features a 'Options' tab and a 'Scope' tab. The 'Options' tab is active, showing a list of configuration items on the left and a detailed configuration form on the right. The configuration form includes fields for 'Filter Name' (FortiEDR), 'Identifier' (com.ensilo.fnt), 'Service Address', 'Organization' (Fortinet Inc.), 'User Name', and 'Password'. Each field has a toggle switch on the right to enable or disable it. The 'Filter Name' and 'Identifier' fields are required. The 'Service Address' field is optional. The 'Organization' and 'User Name' fields are optional. The 'Password' field is optional and has a 'Required to authenticating to the service' note. The 'Filter Name' and 'Identifier' fields are required. The 'Service Address' field is optional. The 'Organization' and 'User Name' fields are optional. The 'Password' field is optional and has a 'Required to authenticating to the service' note. The 'Filter Name' and 'Identifier' fields are required. The 'Service Address' field is optional. The 'Organization' and 'User Name' fields are optional. The 'Password' field is optional and has a 'Required to authenticating to the service' note.

**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.fnt  
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**  
Required to authenticating to the service

Cancel Save

The screenshot shows the 'Options' tab of the 'FortiEDR' configuration page in the Jamf Pro interface. The left sidebar contains navigation menus for 'INVENTORY', 'CONTENT MANAGEMENT', 'GROUPS', 'ENROLLMENT', and 'SETTINGS'. The main content area is titled 'Computers : Configuration Profiles' and 'FortiEDR'. It features a 'Options' tab and a 'Scope' tab. The 'Options' tab is active, showing a list of configuration items on the left and a detailed configuration form on the right. The configuration form includes fields for 'User Name', 'Password', 'Certificate', 'Filter Order', 'Socket Filter', 'Socket Filter Bundle Identifier', 'Socket Filter Designated Requirement', and 'Network Filter'. Each field has a toggle switch on the right to enable or disable it. The 'Filter Order' and 'Socket Filter' fields are required. The 'Socket Filter Bundle Identifier' and 'Socket Filter Designated Requirement' fields are optional. The 'Network Filter' field is optional. The 'User Name' and 'Password' fields are optional. The 'Certificate' field is optional. The 'Filter Order' and 'Socket Filter' fields are required. The 'Socket Filter Bundle Identifier' and 'Socket Filter Designated Requirement' fields are optional. The 'Network Filter' field is optional. The 'User Name' and 'Password' fields are optional. The 'Certificate' field is optional.

**User Name**  
User name for authenticating to the service

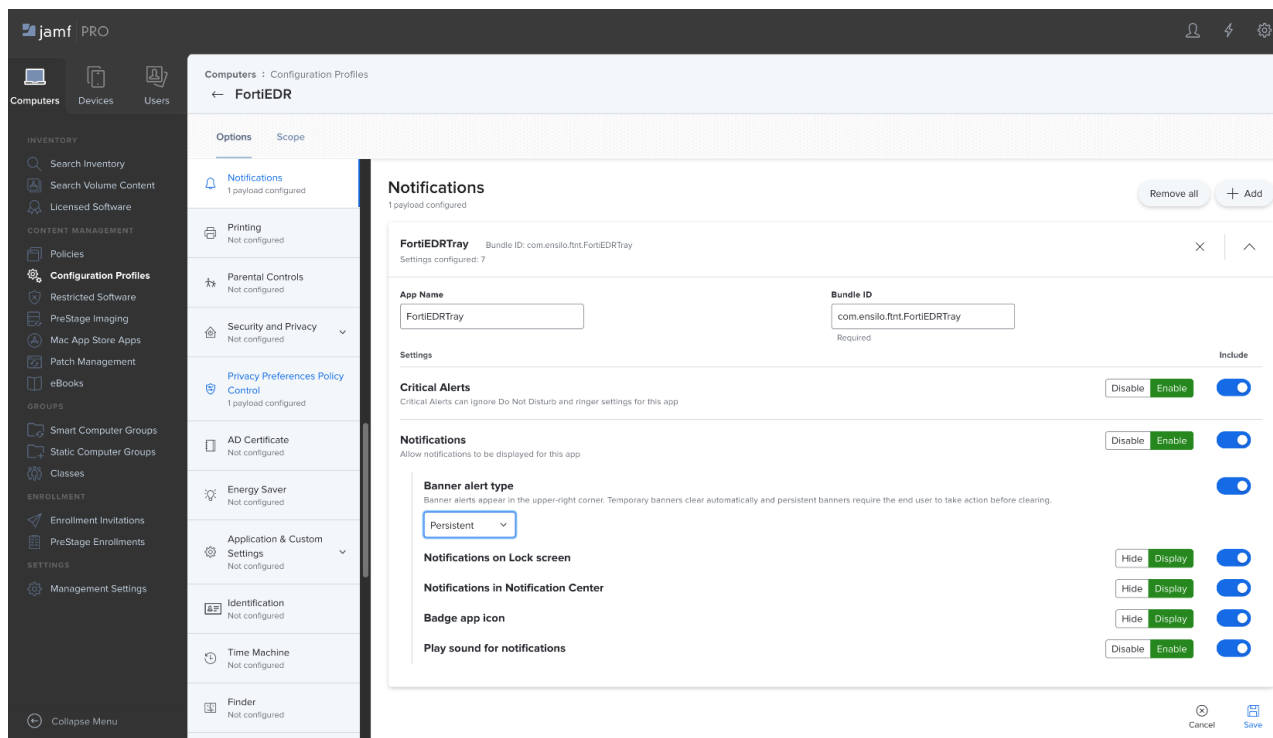
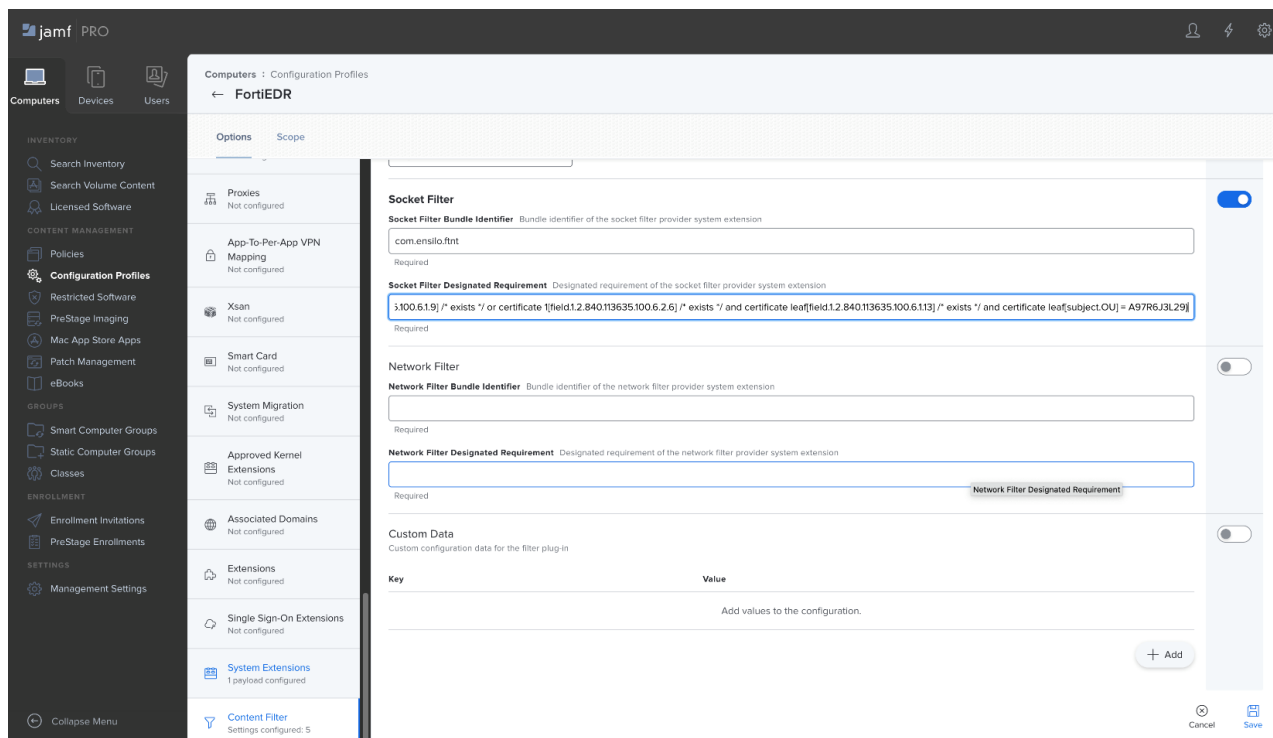
**Password**  
Password for authenticating to the service

**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: com.ensilo.fnt  
Socket Filter Designated Requirement: anchor apple generic and identifier "com.ensilo.fnt" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /\* exists \*/ or certificate /\*field.1.2.840.113635.100.6.2.6] /\* exists \*/ and certificate /\*

Cancel Save



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

- 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 52](#).

## Setting up exclusions with other AV products

If another AV product 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
<ul style="list-style-type: none"> <li>• %ProgramData%\FortiEDR\</li> <li>• %ProgramFiles%\Fortinet\FortiEDR</li> <li>• %ProgramFiles%\Fortinet\FortiEDR\FortiEDRCollector.exe</li> <li>• %ProgramFiles%\Fortinet\FortiEDR\FortiEDRCollectorService.exe</li> <li>• %ProgramFiles%\Fortinet\FortiEDR\FortiEDRAvScanner.exe</li> <li>• %ProgramFiles%\Fortinet\FortiEDR\FortiEDRInventoryScanner.exe</li> <li>• %ProgramFiles%\Fortinet\FortiEDR\FortiEDRIotDiscovery.exe</li> <li>• %windir%\System32\drivers\FortiEDRAvDriver_*.sys</li> <li>• %windir%\System32\drivers\FortiEDRBaseDriver_*.sys</li> <li>• %windir%\System32\drivers\FortiEDRElamDriver_*.sys</li> <li>• %windir%\System32\drivers\FortiEDRIotDriver_*.sys</li> <li>• %windir%\System32\drivers\FortiEDRWinDriver_*.sys</li> </ul>	<ul style="list-style-type: none"> <li>• /Library/FortiEDR</li> <li>• /Applications/FortiEDR.app</li> <li>• /Library/FortiEDR/FortiEDRCollector</li> <li>• /Library/FortiEDR/FortiEDRCollectorTray</li> <li>• /Library/FortiEDR/FortiEDRConfig</li> <li>• /Library/FortiEDR/FortiEDRDrive</li> <li>• /Library/Extensions/FortiEDRDriver.kext</li> </ul>	<ul style="list-style-type: none"> <li>• /sbin/FortiEDRCollector</li> <li>• /opt/FortiEDRCollector</li> </ul>

## 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 21](#).

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 319](#).

- `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:

- Select *Start >> Run*.
- Type `regedit` to open the *Registry Editor* window.
- 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:**

```
/Applications/FortiEDR.app/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, AML, SLES:

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

○

OR

```
rpm -qa | grep 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 277](#)
- As described in the procedure below.

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

### Windows

- Copy the `FortiEDRCollectorInstaller32_x.x.x.xxx.msi` or `FortiEDRCollectorInstaller64_x.x.x.xxx.msi` file (as appropriate) to the Collector machine. For example, `FortiEDRCollectorInstaller32_2.0.0.330.msi` or `FortiEDRCollectorInstaller64_2.0.0.330.msi`.
- Double-click the `FortiEDRCollectorInstaller32_x.x.x.xxx.msi` or `FortiEDRCollectorInstaller64_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
```



# Setting up a FortiEDR Core as a Jumpbox

While you do not need to set up any Cores for cloud deployment, you can optionally set up a Core as a Jumpbox on premise.

## Preparing for the FortiEDR Core installation

The workstation, virtual machine or server on which the FortiEDR Core will be installed, must meet the following requirements:

- System requirements: 2 CPUs, 4 GB of physical memory, 50 GB (non-SSD).
- 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 374](#).
- Has connectivity to the FortiEDR Reputation Server at 35.186.218.233.
- 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`

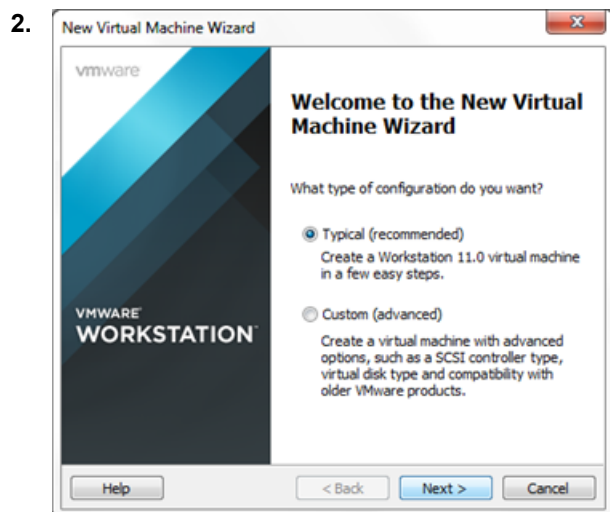


For more details about installing a Core in a multi-organization environment, see the *Core Registration* section in [Component registration in a multi-organization environment on page 378](#).

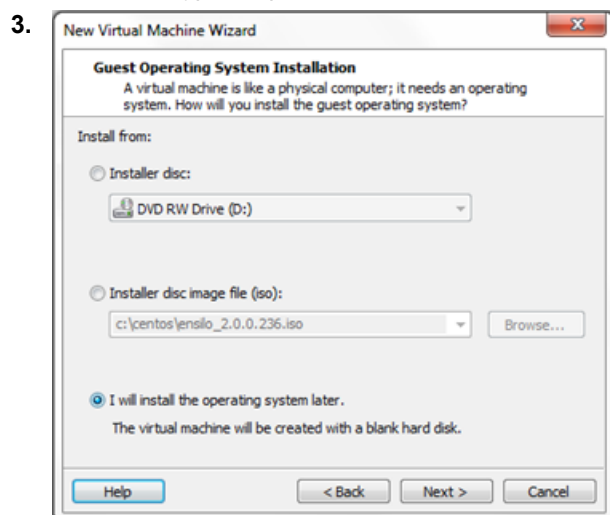
## Installing the FortiEDR Core

The following describes how to install the FortiEDR Core.

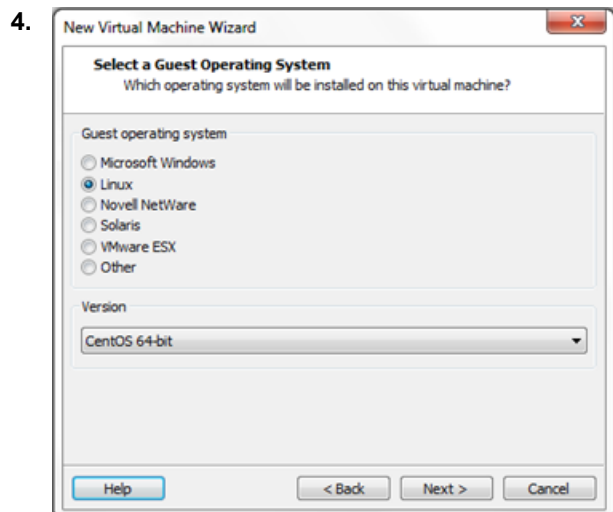
1. Create a new virtual serve by selecting *File > New Virtual Machine*.



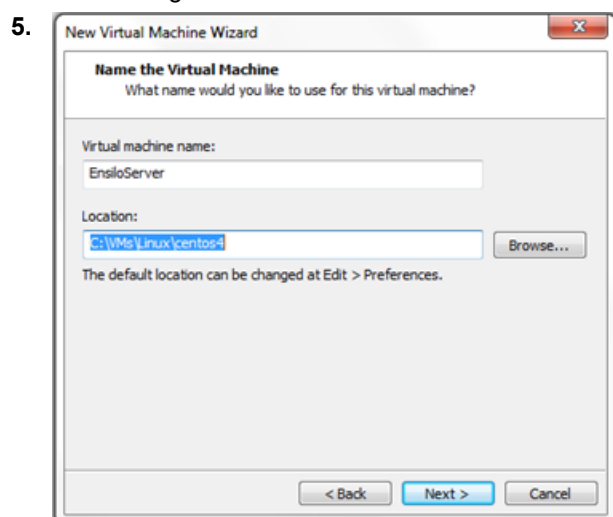
Select the *Typical* option and click *Next*.



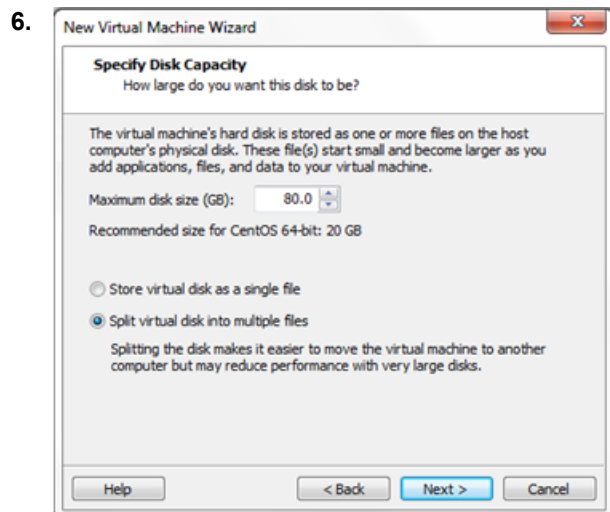
Select the *I will install the operating system later* option and click *Next*.



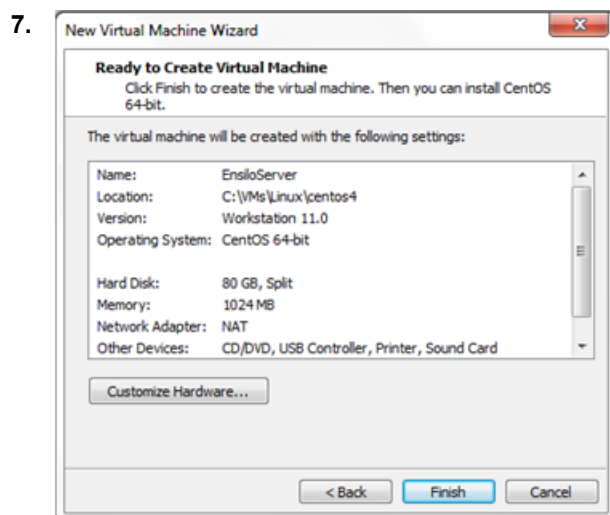
Select the *Linux* radio button. In the *Version* field, select *CentOS 64-bit* and click *Next*. Alternatively, you can select a different generic Linux 64-bit in the *Version* field.



Specify a name for the virtual machine such as *FortiEDRCore* and the location in which to store the provided ISO file and click *Next*.

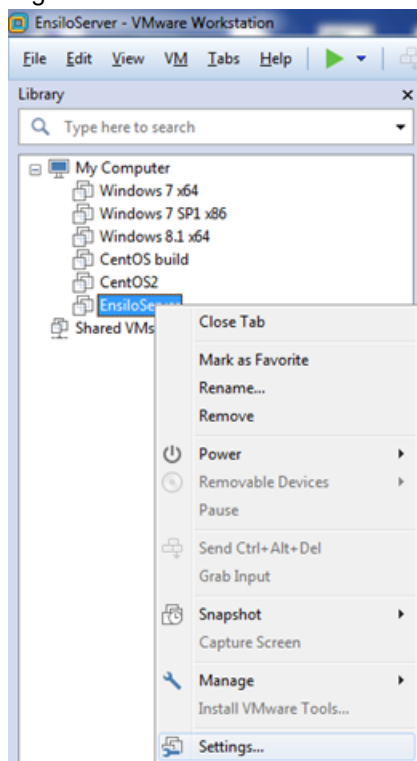


Change the *Maximum disk size* to 80 GB, leave the default option as *Split virtual disk into multiple files* and click *Next*.

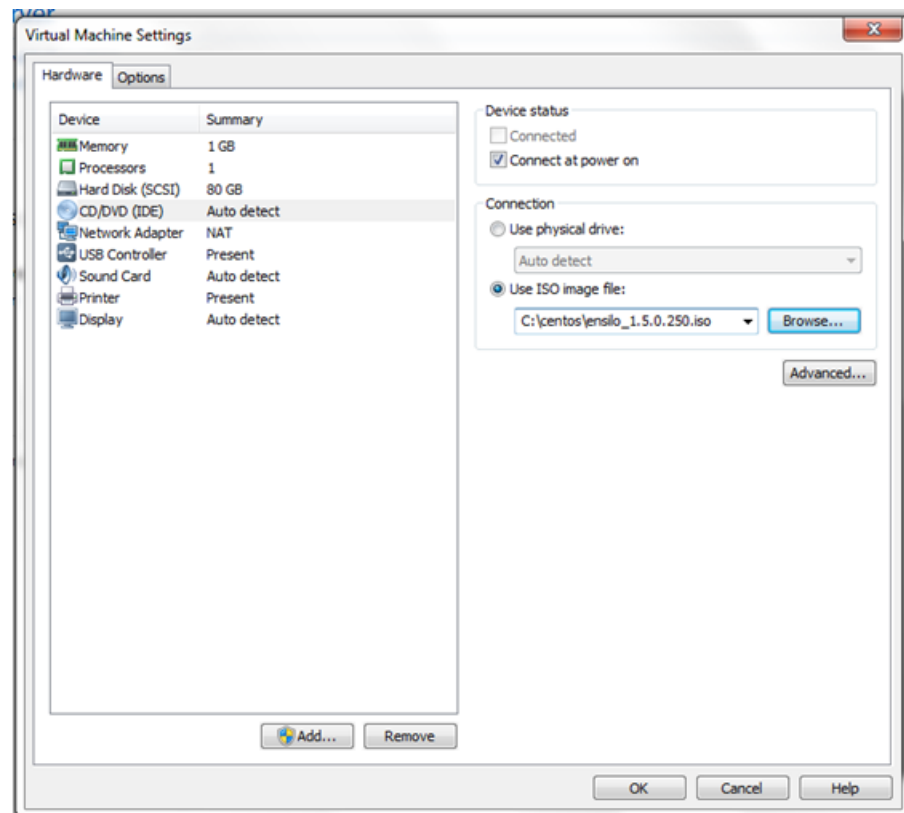


Click *Finish*.

8. Right-click the new machine and select the *Settings* option.



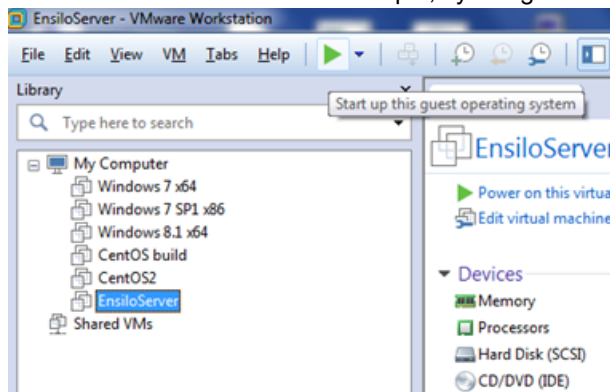
- 9.



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.
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:



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, enter your hostname (any hostname) and click *Next*.
19. 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 *JumpBox* in the *INVENTORY > System Components* tab of the Central Manager.

20. 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).

21. At the prompt, enter the Aggregator external IP address followed by the port (optional). If a port is not provided, the default port 8081 is used.
22. At the prompt, enter this machine's external IP address followed by the port (optional). If a port is not provided, the default port 555 is used.
23. At the prompt, enter the Organization name. For a non-multi-tenant setup, this must be left empty.
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 34 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:
  - *No* (the default)
  - *Yes* (only for an on-premises Core installation, which should be configured to pass a web proxy)
34. Wait a few moments while the installation processes, until you see the *Installation completed successfully* message.
35. To verify that core installation succeeded, use the `fortiedr status` and `fortiedr version` commands.
36. In the *INVENTORY > System Components* tab of the Central Manager, verify that the [FortiEDR Core details](#) are listed and configure the functionality of the Core as *JumpBox*.

## 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_5.2.1.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_5.2.1.x.y
```
3. Run the patch, as shown below:

```
[root@dan ~]# ./ ./ FortiEDRCoreInstaller_5.2.1.x.y
```
4. Wait for the upgrade to complete, as shown below:

```
FortiEDR patch 5.2.1.x.y finished
[root@dan ~]#
```

# Security Settings

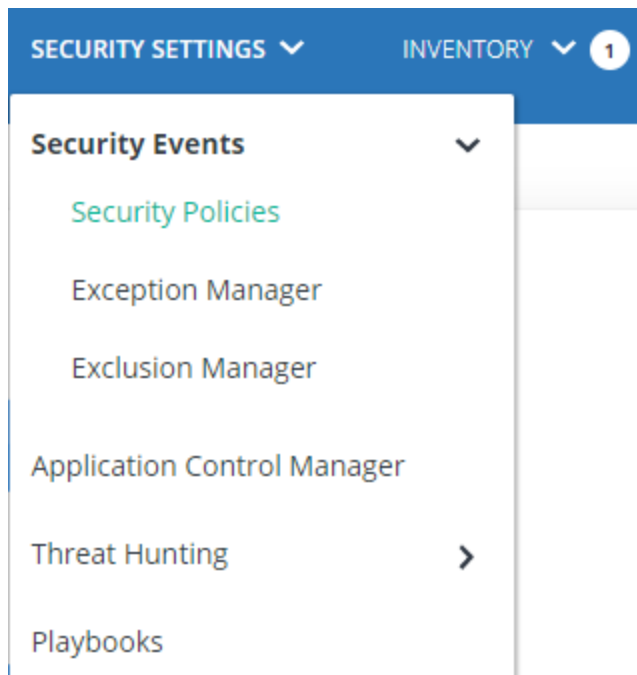
This chapter describes FortiEDR security policies and Playbook policies for defining, monitoring and handling FortiEDR security.

## 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.



- **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.
- **Ransomware Prevention:** This policy enables FortiEDR to detect and block malware that prevents or limits users from accessing their own system.
- **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 *Events* page and are not listed as part of the *All* filter.

- 
- **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 Manager on page 85](#) page.



Application Control security events are displayed under dedicated *Application Control* filter in the *Events* page and are not listed as part of the *All* filter.

- 
- **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 Event Viewer. No blocking options are provided. The exceptions and forensics options are not available in the Event Viewer for security events triggered by this policy.



This policy requires that you configure an XDR source connector in the **ADMINISTRATION > INTEGRATIONS** section. This feature is a license-dependent add-on. You may contact [Fortinet Support](#) for more information.

---

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:

The screenshot shows the 'SECURITY POLICIES' section of the FortiEDR interface. It features a table with columns for 'POLICY NAME', 'RULE NAME', 'ACTION', and 'STATE'. The policies listed are Execution Prevention, Exfiltration Prevention, Ransomware Prevention, Device Control, and extended Detection Policy. Each policy has a FortiNET logo and a status indicator (green for enabled, red for disabled). To the right, there is a section for 'ASSIGNED COLLECTOR GROUPS' with a search bar and a list of groups.

You can click the down arrow next to the *Protection/Simulation* slider to see an at-a-glance view of the system's various security policies and their impact on the Collectors in the system.









## 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*.

The screenshot shows a detailed view of the 'SECURITY POLICIES' page. It includes a table of policies and their rules. The 'Execution Prevention' policy is expanded, showing a list of rules such as 'Malicious File Detected', 'Privilege Escalation Exploit Detected', and 'Sandbox Analysis'. Each rule has an associated action (Block, Log) and state (Enabled, Disabled). To the right, there is a section for 'ASSIGNED COLLECTOR GROUPS' with a search bar and a list of groups. Below the table, there is an 'ADVANCED POLICY & RULE DATA' section with tabs for 'Rule Details' and 'Factory Settings'. The 'Rule Details' tab is selected, showing information about the 'Malicious File Detected' rule, including its name, details, and forensic recommendations.

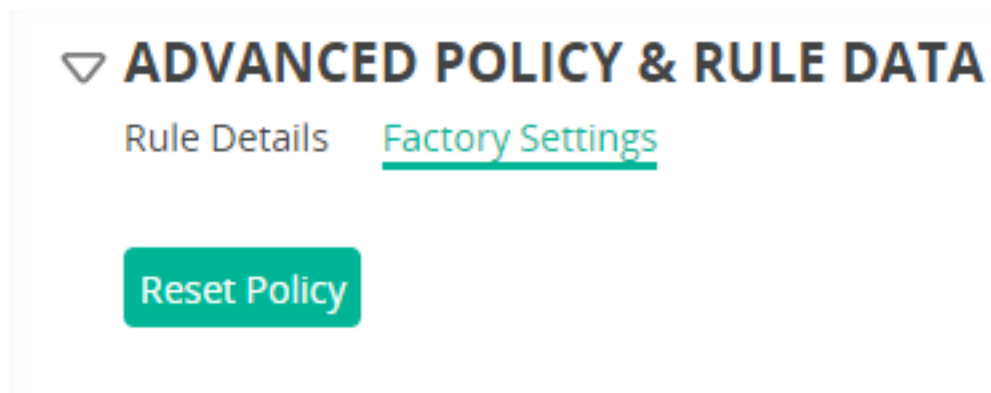
FortiEDR is provided out-of-the-box with several predefined security policies (depending on your license), ready for you to get started. By default, all policies are set to Simulation mode (meaning that they only log and do not block) and show the **Fortinet** logo. This page also enables you to define additional policies.

Security Policy	Icon
Exfiltration Prevention	
Ransomware Prevention	
Execution Prevention	
Device Control Policies	
Application Control Policies	
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 <i>Default Policy</i> cannot be changed.
Rule Name	<p>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.</p> <hr/> <div>  <p>You can expand the <i>ADVANCED POLICY &amp; RULES DATA</i> area at the bottom left of the window to display a more detailed description of what the rule does and how it works.</p> </div> <hr/>
Action	<p>Specifies the action that is enforced when this rule is violated. You can change this field, as follows:</p> <ul style="list-style-type: none"> <li>• <b>Block</b>  <b>Block</b>: When this policy is set to <i>Prevention</i> mode (<a href="#">Setting a security policy's Prevention or Simulation mode on page 69</a>), the exfiltration attempt is blocked and a blocking event is generated. When this policy is set to <i>Simulation</i> mode, the outgoing connection attempt is NOT blocked and a simulated-blocking event is generated (this indicates that FortiEDR <b>would have</b> blocked the exfiltration if the policy had been set to Prevention mode).</li> <li>• <b>Log</b>  <b>Log</b>: The event is only logged regardless of whether the policy is set to Prevention or Simulation mode. The outgoing connection attempt is not blocked.</li> </ul>
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.

## SECURITY POLICIES

Clone Policy
 Set Mode ▼
 Assign Collector Group
 Delete

	✓ All	POLICY NAME			
▶	✓	Execution Prevention	FORTINET		
▶	✓	Exfiltration Prevention	FORTINET		
▶	✓	Ransomware Prevention	FORTINET		
▶	✓	Device Control	FORTINET		
▶	✓	eXtended Detection Policy	FORTINET		

2. You can now either:

- Set mode : Click *Set Mode* and select either *Prevention* or *Simulation*, as shown above.
- : 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:



## SECURITY POLICIES

Clone Policy
 Set Mode ▼
 Assign Collector Group
 Delete

	✓ All	POLICY NAME			
▶	✓	Execution Prevention	FORTINET		
▶	✓	Exfiltration Prevention	FORTINET		
▶	✓	Ransomware Prevention	FORTINET		
▶	✓	Device Control	FORTINET		
▶	✓	eXtended Detection Policy	FORTINET		

## 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.

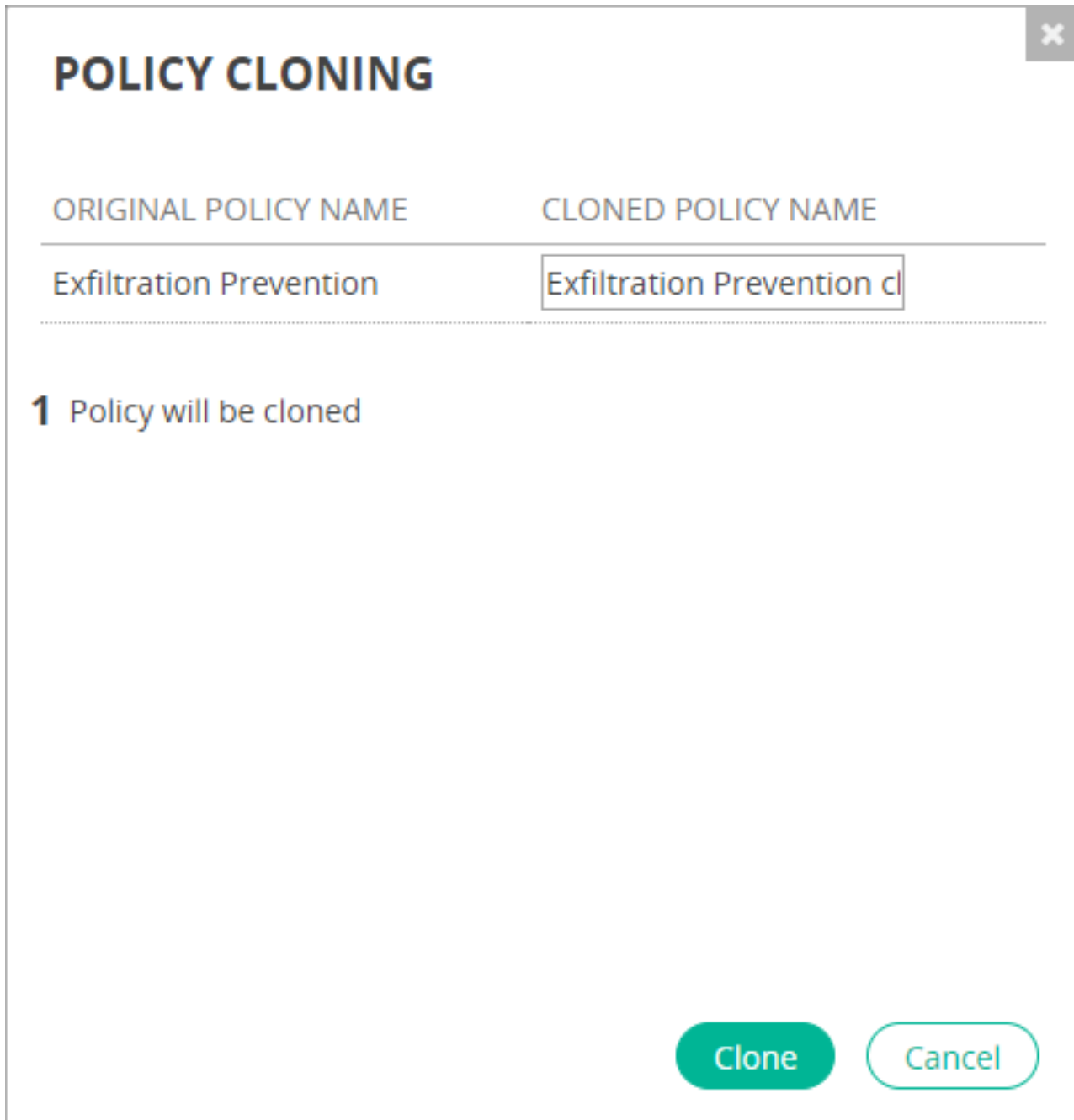
The screenshot shows the FortiEDR Security Settings interface. The top navigation bar includes Dashboard, Event Viewer (131), Forensics, Communication Control (1228), Security Settings (active), Inventory (2), and Administration (2281). The main content area is titled 'SECURITY POLICIES' and displays a table of policies. The 'Device Control' policy is selected, and the 'ASSIGNED COLLECTOR GROUPS' panel on the right shows the 'Unassign Group' button.

POLICY NAME	RULE NAME	ACTION	STATE
Execution Prevention		Fortinet	On
Exfiltration Prevention		Fortinet	On
Ransomware Prevention		Fortinet	On
Device Control		Fortinet	On
extended Detection Policy		Fortinet	Off

**ASSIGNED COLLECTOR GROUPS**

- Unassign Group
- 4.6 early (0 collectors included)
- Beta 4.1.0 (3 collectors included)
- lior4.6 (0 collectors included)
- lior5.0 (7 collectors included)
- liortest (0 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

Clone Cancel

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 72](#).

## 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 116](#) 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 screenshot shows the FortiEDR Security Settings interface. The top navigation bar includes tabs for DASHBOARD, EVENT VIEWER (151), FORENSICS, COMMUNICATION CONTROL (1228), SECURITY SETTINGS (active), INVENTORY (2), and ADMINISTRATION (2263). The 'SECURITY POLICIES' section is active, displaying a table of policies. The 'Device Control' policy is selected. The 'ASSIGNED COLLECTOR GROUPS' section on the right shows a list of collector groups with checkboxes.

POLICY NAME	RULE NAME	ACTION	STATE
Execution Prevention		FORNINET	ON
Exfiltration Prevention		FORNINET	ON
Ransomware Prevention		FORNINET	ON
Device Control		FORNINET	ON
extended Detection Policy		FORNINET	ON
AC Device Control			ON
AC Execution Prevention			ON
AC Exfiltration Prevention			ON
AC Ransomware Prevent...			ON
ausm Device Control			ON

**ASSIGNED COLLECTOR GROUPS**

- ☐ Unassign Group
- ☐ 4.6 early (0 collectors included)
- ☐ Beta 4.1.0 (3 collectors included)
- ☐ Ilor4.6 (0 collectors included)
- ☐ Ilor5.0 (7 collectors included)
- ☐ Iliortest (0 collectors included)

2. The right side of the window displays the Collector Groups to which this policy is assigned. 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

Q

<input type="checkbox"/>	GROUP NAME▲	# OF COLLECTORS	
<input type="checkbox"/>	Default VDI Group	0	✓ Assigned
<input type="checkbox"/>	enSilo employees	45	✓ Assigned
<input type="checkbox"/>	enSilo Servers	0	✓ Assigned
<input type="checkbox"/>	Home users	6	Available
<input type="checkbox"/>	my citrix pool (VDI)	0	✓ Assigned
<input type="checkbox"/>	OSX Users	13	Available
<input type="checkbox"/>	Store	0	Available
<input type="checkbox"/>	US Users	0	✓ Assigned

0 Collector groups selected

Assign
Cancel



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 Event Viewer, as described on [Defining security event exceptions on page 160](#)



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 archived 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 **EVENT VIEWER** page, click the *Exception Manager* button. The following window displays, showing the list of previously created exceptions:

EXCEPTION MANAGER										
<input type="text" value="Search Exception"/> <span>Advanced</span>										
<span>Delete</span> <span>Export</span> <span>Showing 1-10/201</span>										
<input type="checkbox"/>	EVENT	PROCESS	PROCESS PATH	EXECUTED WITH	PATH	RULES	COLLECTOR GROUPS	DESTINATIONS	USERS	LAST UPDATED
<input type="checkbox"/>	663219	EXCEL.EXE	Any path			Suspicious Macro	High Security Collector ...	All Destinations	All Users	05-Oct-2020, 11:45 by: Einat
<input type="checkbox"/>	30558956	netsh.exe	Windows\System32	PanGhlp.exe	Any path	Suspicious Script Execution	All Collector Groups	All Destinations	All Users	23-Mar-2020, 09:47 by: Tzaf
<input type="checkbox"/>	665954	OfficeTimelineStartUp.e...	Any path			Unconfirmed Executable	All Collector Groups	Internal Destinations (AL...	All Users	23-Oct-2018, 19:05 by: Tzafit
		OfficeTimelineStartUp.e...	Any path			Unconfirmed Executable				
<input type="checkbox"/>	666041	maktubransomware.exe	...\Ransomware.Maktub			PUP	All Collector Groups	167.114.64.227	All Users	23-Oct-2018, 18:51 by: Tzafit
		maktubransomware.exe	...\Ransomware.Maktub			PUP				
		maktubransomware.exe	...\Ransomware.Maktub			PUP				
<input type="checkbox"/>	442648	camstudio.exe	...ers\JTM.CDE\Desktop			Malicious File Detected	All Collector Groups	Internal Destinations (AL...	All Users	25-Sep-2018, 23:16 by: Tzafit
<input type="checkbox"/>	197019	Cisco WebEx Start	Any path			PUP	Home users	184.87.163.50	All Users	05-Nov-2017, 13:35 by: admin
		Cisco WebEx Start	Any path			PUP				



If the exception includes a free-text comment, you can hover over the Event ID in the Exception Manager to display it.

EXCEPTION MANAGER										
<input type="text" value="Search Exception"/> <span>Advanced</span>										
<span>Delete</span> <span>Export</span> <span>Showing 1-10/12</span>										
<input type="checkbox"/>	EVENT	PROCESS	PROCESS PATH	EXECUTED WITH	PATH	RULES	COLLECTOR GROUPS	DESTINATIONS	USERS	LAST UPDATED
<input type="checkbox"/>	659541	FortinetCloudServices...	at 05-Oct-2020, 00:41:22 (UTC)			Malicious File Detected	All Collector Groups	All Destinations	All Users	06-Oct-2020, 00:41 by: FortinetCloudServ...




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										
<input type="text" value="Search Exception"/> <span>Advanced</span>										
<span>Delete</span> <span>Export</span> <span>Showing 1-10/201</span>										
<input type="checkbox"/>	EVENT	PROCESS	PROCESS PATH	EXECUTED WITH	PATH	RULES	COLLECTOR GROUPS	DESTINATIONS	USERS	LAST UPDATED
<input type="checkbox"/>		maktubransomware.exe	...\Ransomware.Maktub			PUP				
<input checked="" type="checkbox"/>	442648	camstudio.exe	...ers\JTM.CDE\Desktop			Malicious File Detected	All Collector Groups	Internal Destinations (AL...	All Users	25-Sep-2018, 23:16 by: Tzafit
<input type="checkbox"/>	197019	Cisco WebEx Start	Any path			PUP	Home users	184.87.163.50	All Users	05-Nov-2017, 13:35 by: admin

- 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	<input type="text"/>	Path	<input type="text"/>	Rule	<input type="text"/>	Group	<input type="text"/>	Destination	<input type="text"/>	User <input type="text"/>
										<span>Close</span>

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 page 175](#).

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

<input type="checkbox"/>	EVENT	PROCESS	PROCESS PATH	EXECUTED WITH	PATH	RULES	COLLECTOR GROUPS	DESTINATIONS	USERS	LAST UPDATED
<input type="checkbox"/>	4427089	eicar.com	Any path			Malicious File Detected	All Collector Groups	All Destinations	All Users	13-Jan-2021, 08:37 by: FortinetCloudServi...
		grid.appScope.getMaxAlert:								
<input checked="" type="checkbox"/>	4418037	TeamViewer_Service.exe	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: soft
		grid.appScope.getMaxAlert:								
<input checked="" type="checkbox"/>	4425068	ConnectivityTestAppNe...	...nnectivityTestAppNew			Malicious File Detected	TTGroup	Internal Destinations (Al...	All Users	13-Jan-2021, 04:09 by: soft
		grid.appScope.getMaxAlert:								

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

Destinations

☒ Search Destinations ☐ All Destinations

Type comments

Add To Existing

✓ Add To Existing

Replace All

Add To Existing

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 or files are excluded from Security Policies monitoring. Two types of exclusions can be defined in the Exclusion Manager:

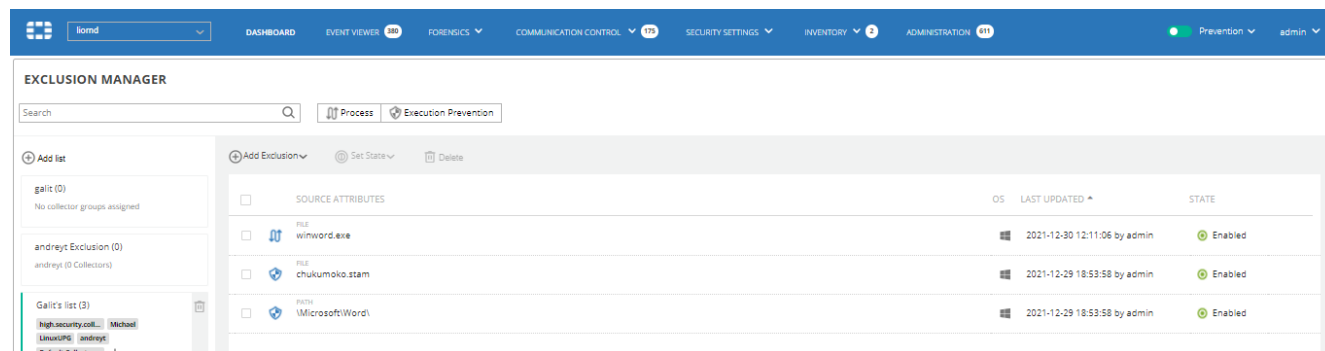
- Process Exclusions:** This type of exclusion specifies that FortiEDR does not inspect the actions that are performed by specific processes, so that these processes do not trigger security events. The processes that are excluded are identified by the attributes of the processes, according to your definitions.
 

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 64](#). 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.



### To manage exclusions:

Select **SECURITY SETTINGS > Security Events > Exclusion Manager**. The following window displays, showing the list of previously created exclusions:



The list of exclusions in the Collection Exclusions page contains the following columns:

Column	Description
Checkbox	Enables you to select multiple rows.
Icon	Represents the type of exclusion <ul style="list-style-type: none"> <li> - Process</li> <li> - Execution Prevention</li> </ul>
SOURCE ATTRIBUTES	Specifies the attributes that were defined in order to identify the Process/File, as described in <a href="#">Defining exclusions on page 80</a>

Column	Description
OS	Specifies the operating system to which this exclusion applies. Currently, only Windows is supported.
LAST UPDATED	Specifies when this exclusion was last updated and by whom.
STATE	Specifies whether this exclusion is enabled or disabled.
 	Edit and delete exclusion tools.

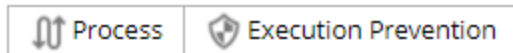
The following actions can be performed in the *Collection Exclusions* page:

- [Filtering on page 79](#)
- [Defining Exclusion Lists on page 79](#)
- [Defining exclusions on page 80](#)

## 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 comes with a default General Exclusion List that includes important exclusions. The exclusions in this group are not editable.

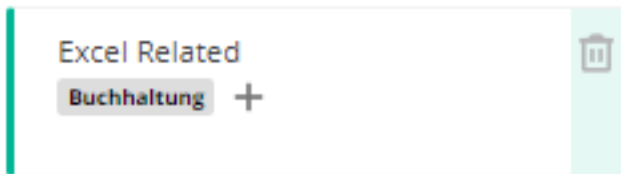
## Adding an Exclusion List

### 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 the <i>Delete</i>  button. Note that all Exclusions in this list will be removed and will no longer be applied to the assigned Collector groups.

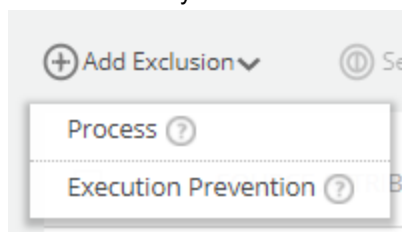
## Defining exclusions

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 and then how to define an Execution Prevention Exclusion.

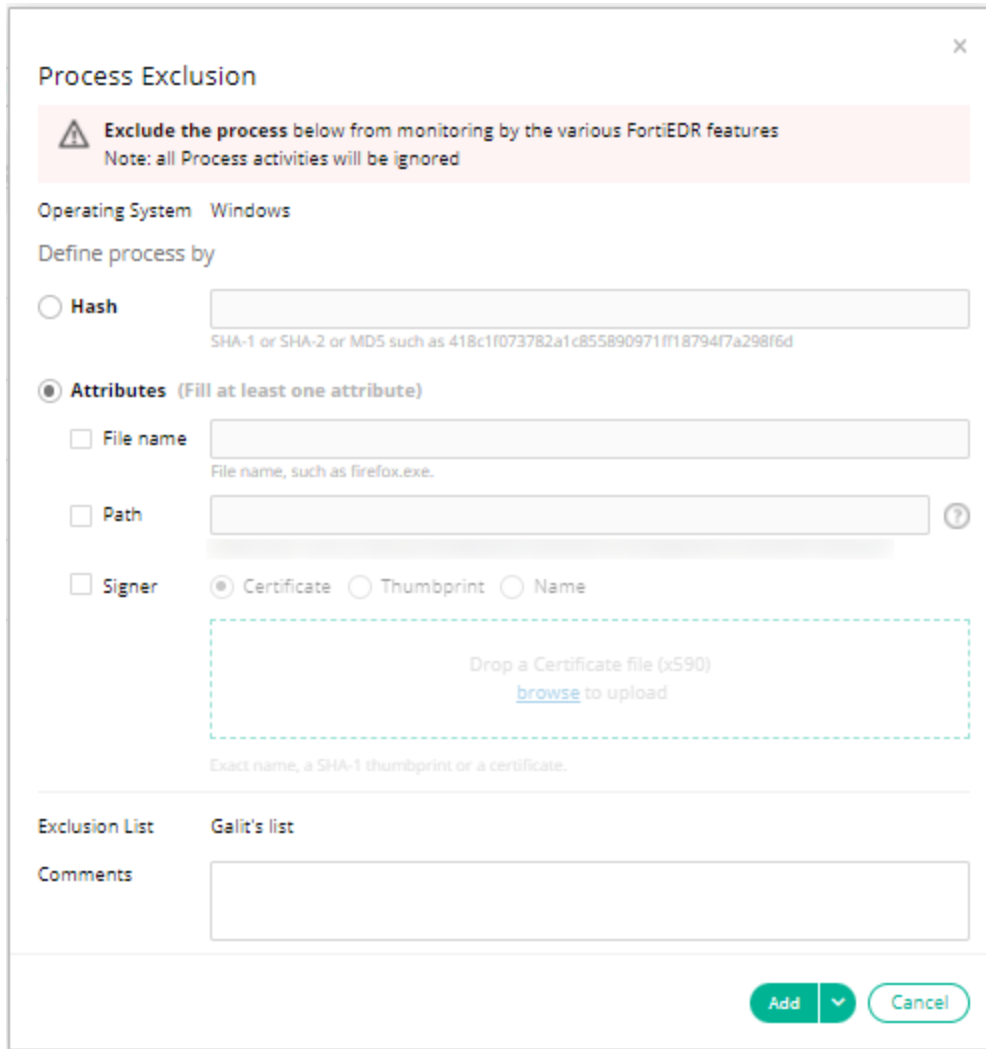
### Adding a Process Exclusion

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 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 such as 418c1f073782a1c855890971ff18794f7a298f6d

☒ **Attributes (Fill at least one attribute)**

☐ **File name**

File name, such as firefox.exe.

☐ **Path**

☐ **Signer**

☒ Certificate ☐ Thumbprint ☐ Name

Drop a Certificate file (x590)  
[browse](#) to upload

Exact name, a SHA-1 thumbprint or a certificate.

Exclusion List: Galit's list

Comments

**Add** **Cancel**

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.
  - **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:
    - 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 84](#) section for more details about defining an exclusion path.

☒ **Attributes** (Specify at least one attribute)

☐ File name   
File name, such as firefox.exe.

☐ Path  ?

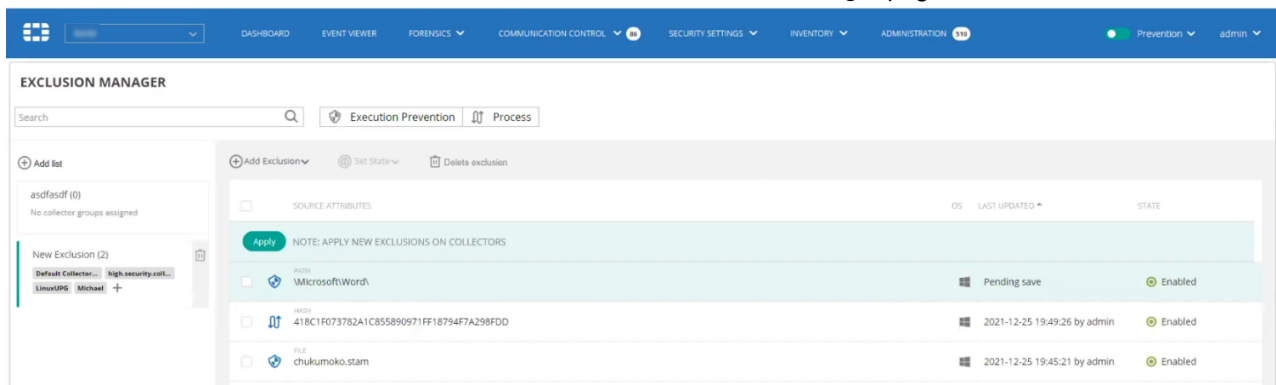
If you select *Signer*, then either upload the Signer's Certificate, provide its thumbprint or provide the Signer's name.

Signer ☒ Certificate ☐ Thumbprint ☐ Name

Drop a Certificate file (x590)  
[browse](#) to upload

Exact name, a SHA-1 thumbprint or a certificate.

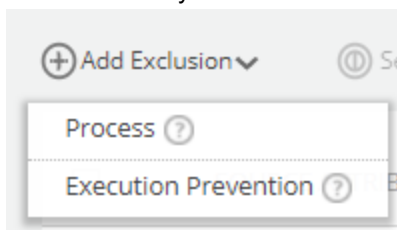
- The *Exclusion List* field specifies the Exclusion List that was selected, when the *Add Exclusion* option was selected. This field is not editable.
- Click the *Add* button. This new exclusion is then listed in the *Exclusion Manager* page, as shown below:



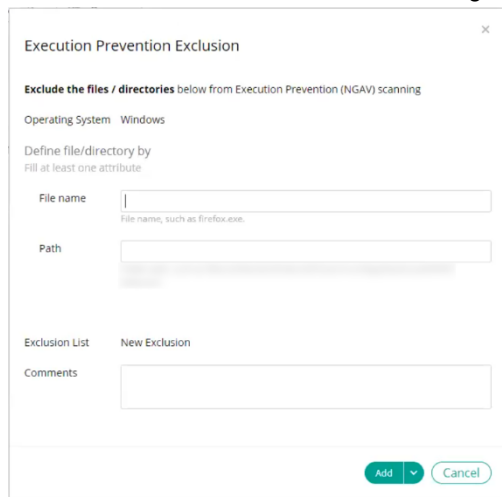
- The newly defined exclusions appear with a green background and the words *Pending save* appear in their *LAST UPDATED* column. To define that these exclusions take effect, you must click the *Apply* button and then click the *Save* button in the window that pops up. Their *LAST UPDATED* column then shows the timestamp when they were saved.

## Adding an Execution Prevention Exclusion

- In the left pane, click the Exclusion List to which to add the exclusion.
- 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 *Execution Prevention*. The following displays:



Execution Prevention Exclusion

Exclude the files / directories below from Execution Prevention (NGAV) scanning

Operating System: Windows

Define file/directory by  
Fill at least one attribute

File name:   
File name, such as firefox.exe.

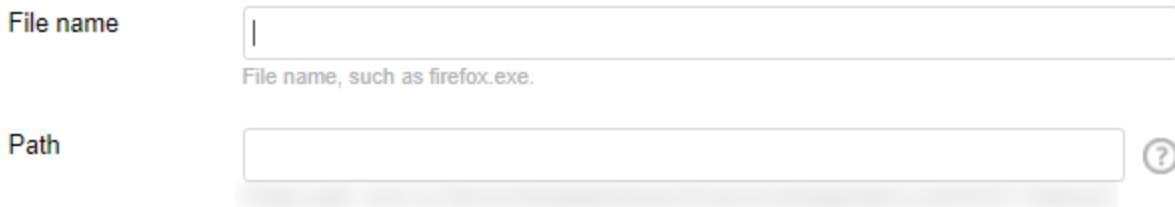
Path:

Exclusion List: New Exclusion

Comments:

4. The *Operating system* dropdown menu specifies *Windows*, which is currently the only operating system supported for exclusion prevention.
5. 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 84](#) section for more details about defining an exclusion path.

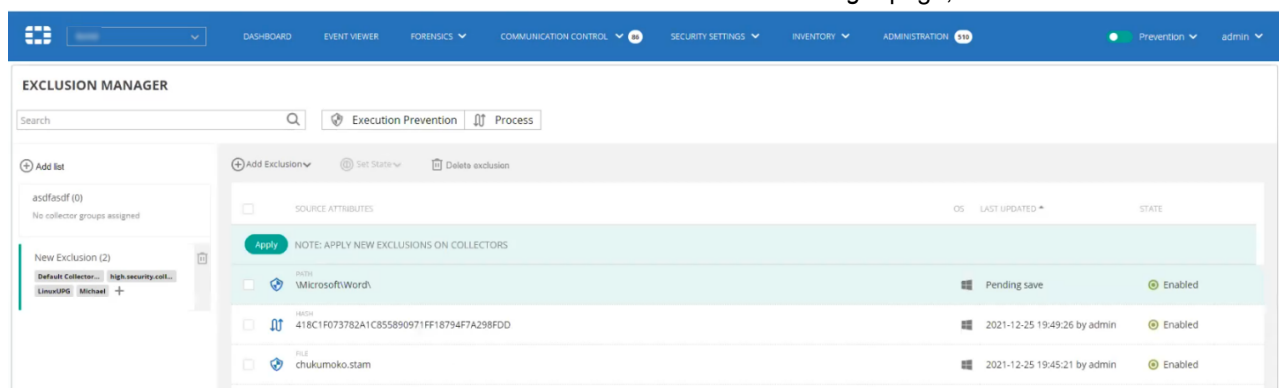
Define file/directory by  
Specify at least one attribute



File name:   
File name, such as firefox.exe.

Path:  ?

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:



EXCLUSION MANAGER

Search:

Execution Prevention | Process

+ Add list

asdfsdf (0)  
No collector groups assigned

New Exclusion (2)

SOURCE ATTRIBUTES	OS	LAST UPDATED *	STATE
NOTE: APPLY NEW EXCLUSIONS ON COLLECTORS			
Path: \Microsoft\Word\	Pending save	2021-12-25 19:49:26 by admin	Enabled
Hash: 418C1F073782A1C855890971FF18794F7A298FDD		2021-12-25 19:45:26 by admin	Enabled
File: chukumoko.stam		2021-12-25 19:45:21 by admin	Enabled

8. 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.

## 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	<ul style="list-style-type: none"> <li>• \Documents</li> <li>• \Documents\Personal\temp</li> </ul>
\Documents\Personal\*	<ul style="list-style-type: none"> <li>• \Documents\Personal\subfolder\</li> <li>• \Documents\Personal\subfolder\subfolder\etc\</li> </ul>	<ul style="list-style-type: none"> <li>• \Documents</li> <li>• \Documents\Personal</li> </ul>
\Documents\Personal*\	<ul style="list-style-type: none"> <li>• \Documents\Personal</li> <li>• \Documents\Personal2</li> <li>• \Documents\Personal\subfolder\</li> </ul>	\Documents
*\Documents\Personal\	<ul style="list-style-type: none"> <li>• \Documents\Personal</li> <li>• \Windows\Documents\Personal</li> </ul>	<ul style="list-style-type: none"> <li>• \Documents</li> <li>• \Documents\Personal\temp</li> </ul>
*\Documents\Personal\*	<ul style="list-style-type: none"> <li>• \Documents\Personal\subfolder\</li> <li>• \Parent\Documents\Personal\subfolder</li> </ul>	<ul style="list-style-type: none"> <li>• \Documents</li> <li>• \Documents\Personal</li> </ul>



- 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.

## Application Control Manager

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 193](#) under *Communication Control*, which enables you to control which applications can communicate outside of the organization, but does not stop them from launching.

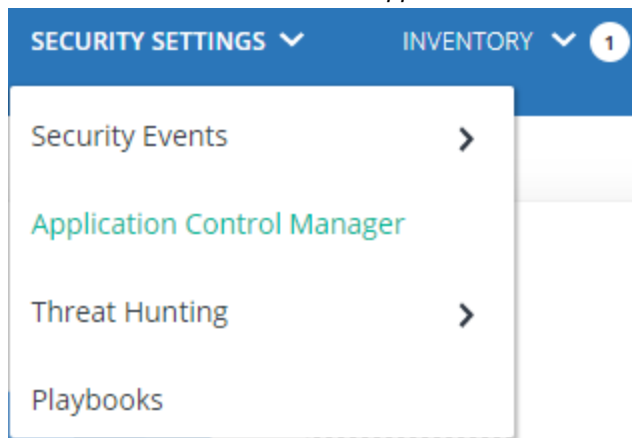
This section describes how to define the applications to be blocked by adding them in the Application Control Manager. In addition, applications can be added to the list of applications to be blocked by adding them from the Forensics window (as described in [Stack view on page 224](#)) and the Threat Hunting window (as described in [Threat Hunting 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 Policy
- 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 Manager*.





The following window displays, showing the list of all the applications that have been defined to be blocked by the Application Control policies. A row appears for each application to be blocked.

<div> <div> <div></div> <div>Galit</div> </div> <div> <div>DASHBOARD</div> <div>EVENT VIEWER</div> <div>FORENSICS</div> <div>COMMUNICATION CONTROL</div> <div>SECURITY SETTINGS</div> <div>INVENTORY</div> <div>ADMINISTRATION</div> </div> <div> <div>Simulation</div> <div>FortiEDRAdmin</div> </div> </div>									
APPLICATION CONTROL MANAGER									
<div> <div>Auto</div> <div>Search</div> <div>Policy All</div> <div>State Enabled Disabled</div> </div>									
<div> <div>+ Add Application</div> <div>Set State</div> <div>Policy Assignment</div> <div>Delete</div> <div>Export</div> </div>									
	APPLICATION ATTRIBUTES	POLICY	TAG	OS	LAST UPDATED	UPDATED BY	STATUS		
<input type="checkbox"/>	HASH: 518C1F073782A1C855890971FF18794F7A298F6D	Application Control	<a href="#">Flashshare</a>	Windows	14-jan-2022 10:24:04	FortiEDRAdmin	Enabled		
<input type="checkbox"/>	HASH: 318C1F073782A1C855890971FF18794F7A298F6D	Application Control	<a href="#">Flashshare</a>	Windows	14-jan-2022 10:23:38	FortiEDRAdmin	Enabled		
<input type="checkbox"/>	HASH: 418C1F073782A1C855890971FF18794F7A298F7D	Application Control	<a href="#">RemoteT...</a>	Windows	14-jan-2022 10:17:51	FortiEDRAdmin	Enabled		
<input type="checkbox"/>	HASH: 418C1F073782A1C855890971FF18794F7A298F6F	Application Control Snir	<a href="#">RemoteT...</a>	Windows	14-jan-2022 10:17:20	FortiEDRAdmin	Enabled		
<input type="checkbox"/>	HASH: 418C1F073782A1C855890971FF18794F7A298F6E	Application Control Snir, Application Control		Windows	14-jan-2022 10:16:33	FortiEDRAdmin	Enabled		
<input type="checkbox"/>	HASH: 418C1F073782A1C855890971FF18794F7A298F6D	Application Control Snir, Application Control		Windows	12-jan-2022 13:11:48	FortiEDRAdmin	Enabled		
<input type="checkbox"/>	HASH: BBEE5B6900164AE1C64F6042BE1BB2E14C3A2A0A446...	Application Control		Windows	10-jan-2022 11:53:22	FortiEDRAdmin	Enabled		

Copyright © Fortinet Version 5.1.0.304

System Time (UTC -05:00) 03:24:17

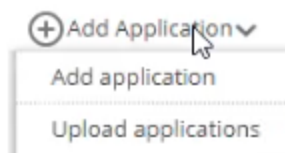
## 2. You can then perform any of the following actions:

- Adding application(s) to be blocked on page 86
- Exporting the list of applications to be blocked on page 90
- Enabling/disabling application blocking on page 90
- Changing the policy under which the application is blocked on page 91
- Searching and filtering applications on page 92
- 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.

## Adding application(s) to be blocked

### To add an application(s) to be blocked:

- 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 87
- Uploading application(s) to be blocked on page 89

## Manually adding an application to be blocked

### To manually add an application to be blocked:

1. Select the *Add application* option from the drop-down menu. The following displays:

2. 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.
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 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.

4. 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.

☐ **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.

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 than 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.

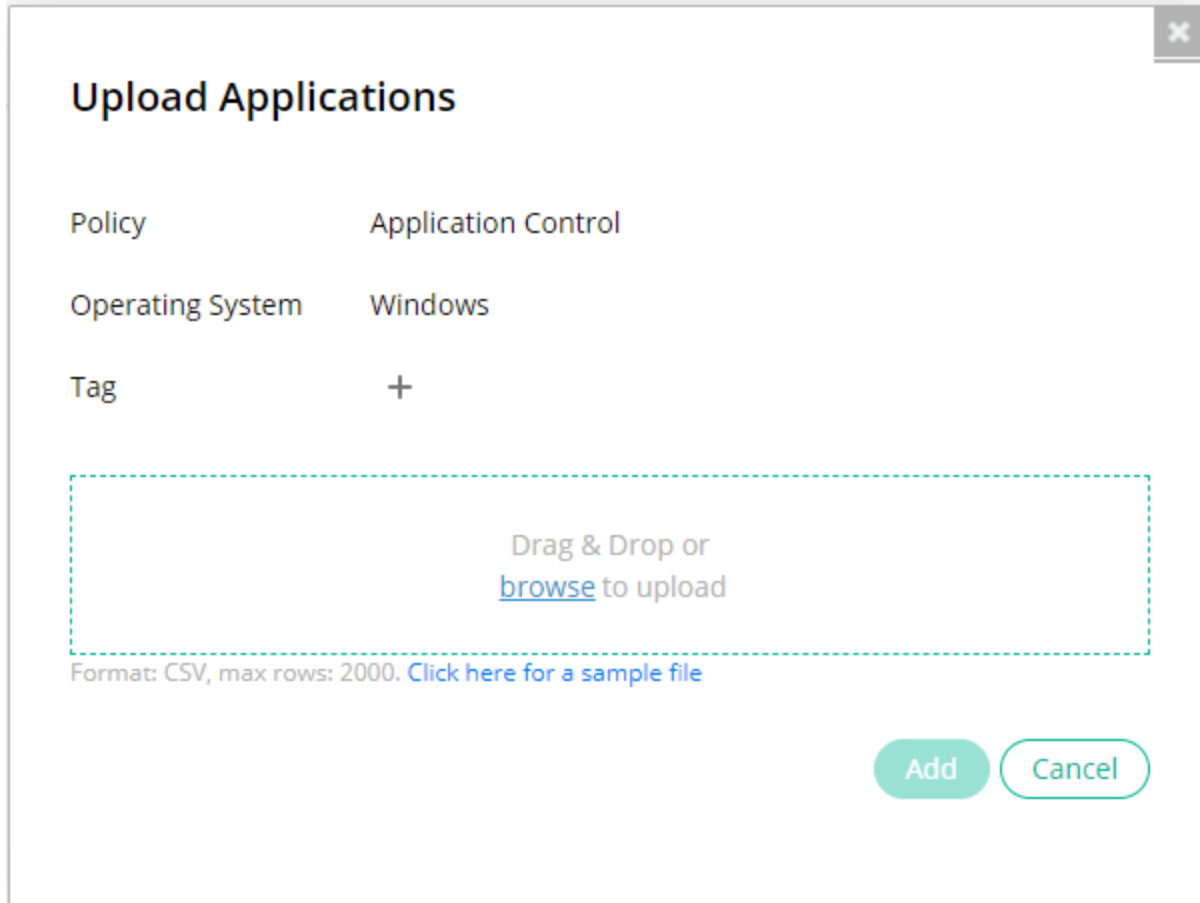
5. Click the *Add* button. The Application Control Manager then lists a row for each application. When a Collector Group is assigned to the application control policy (specify above), then all these applications are blocked and cannot be launched.



## Uploading application(s) to be blocked

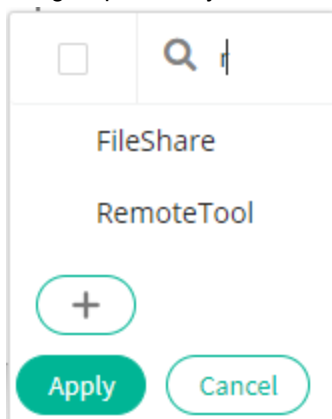
### To upload a list of applications to be blocked from a file:

1. Select the *Upload applications* option. The following displays:



The screenshot shows a dialog box titled "Upload Applications" with a close button in the top right corner. Inside the dialog, there are three fields: "Policy" with the value "Application Control", "Operating System" with the value "Windows", and "Tag" with a "+" icon. Below these fields is a large dashed green rectangle containing the text "Drag & Drop or [browse](#) to upload". At the bottom left of the dialog, there is a note: "Format: CSV, max rows: 2000. [Click here for a sample file](#)". At the bottom right, there are two buttons: "Add" and "Cancel".

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.



The screenshot shows a dropdown menu for selecting a tag. At the top, there is a search icon and a filter icon. Below them, the text "FileShare" and "RemoteTool" are listed. At the bottom, there is a "+" icon in a circle, and two buttons: "Apply" and "Cancel".

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 90](#).

A		B		C		D		E		F		G		H		I	
FORTINET				liornd6												Report created by u	
APPLICATIONS CONTROL																	
HASH		SIGNER THUMBPRINT		SIGNER NAME		PATH		FILE NAME		POLICY		TAG		OS		LAST	
⏵		CBFF86060F72047E8CAFE35AD96ACC836E895D2B								Danny Application Control clone, Application				Windows		2022-04-01	
				Azure Software Solutions, Inc						Danny Application Control clone, Application				Windows		2022-04-01	
				Test						Danny Application Control clone, Application				Windows		2022-04-01	
						\\Windows\System32\smartscreen.exe		smartscreen.exe		Danny Application Control clone				Windows		2022-04-01	
								terapad.exe		Japan-Application Control clone, CSE - Application				Windows		2022-04-01	
						\\Users\user1\Desktop\APPS\		TreeSizeFree.exe		Danny Application Control clone				Windows		2022-04-01	
								free-hex.exe		Danny Application Control clone				Windows		2022-04-01	

5. Click the *Add* button. The Application Control Manager then lists a row for each application in the uploaded file. 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:

Use the *Export* button to export 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:

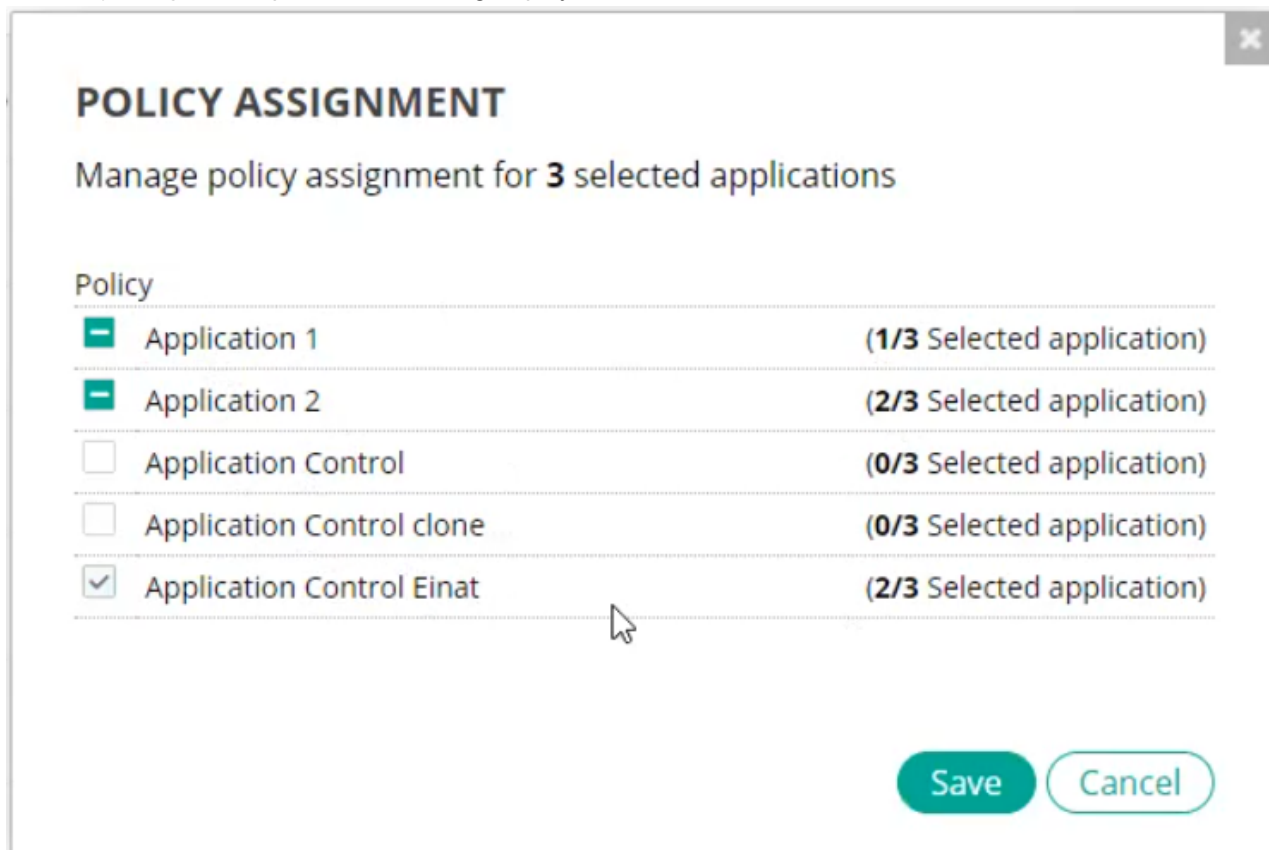
1. Select *SECURITY SETTINGS > Application Control* to display the Application Control Manager. Each row represents an application to be blocked.
2. In the *STATUS* column on the right, toggle the value between *Enabled* and *Disabled*. Alternatively, you can check the checkboxes of the desired application rows, and then select the *Enabled* or the *Disabled* option from the *Set State* dropdown.





## Changing the policy under which the application is blocked



To change the policy that blocks an application:

1. Select **SECURITY SETTINGS > Application Control Manager** to display the Application Control Manager. Each row represents an application to be blocked.
2. In the Application Control Manager window, check the checkboxes of the desired application rows, and then select 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)
<input type="checkbox"/> Application Control	(0/3 Selected application)
<input type="checkbox"/> Application Control clone	(0/3 Selected application)
<input checked="" type="checkbox"/> Application Control Einat	(2/3 Selected application)

Save Cancel

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.

3. In the **Policy Assignment** window, check (or uncheck) the checkboxes of the policies that should block the currently selected applications.
4. 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:

The screenshot shows a search interface for applications. A dropdown menu is open, displaying the following options: **System-defined** (with a checkmark), **Application**, **Creator**, **Updated by**, and **Tag**. The background interface includes a search bar with the text "Search" and a magnifying glass icon. Below the search bar, there are buttons for "Set State", "Delete", and "Export". A table with columns "Application", "Policy", and "State" is partially visible, along with a section titled "ATTRIBUTES".

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 92](#)
- [Collection Exclusions on page 94](#)
- [Threat Hunting data retention on page 101](#)

## Collection Profiles

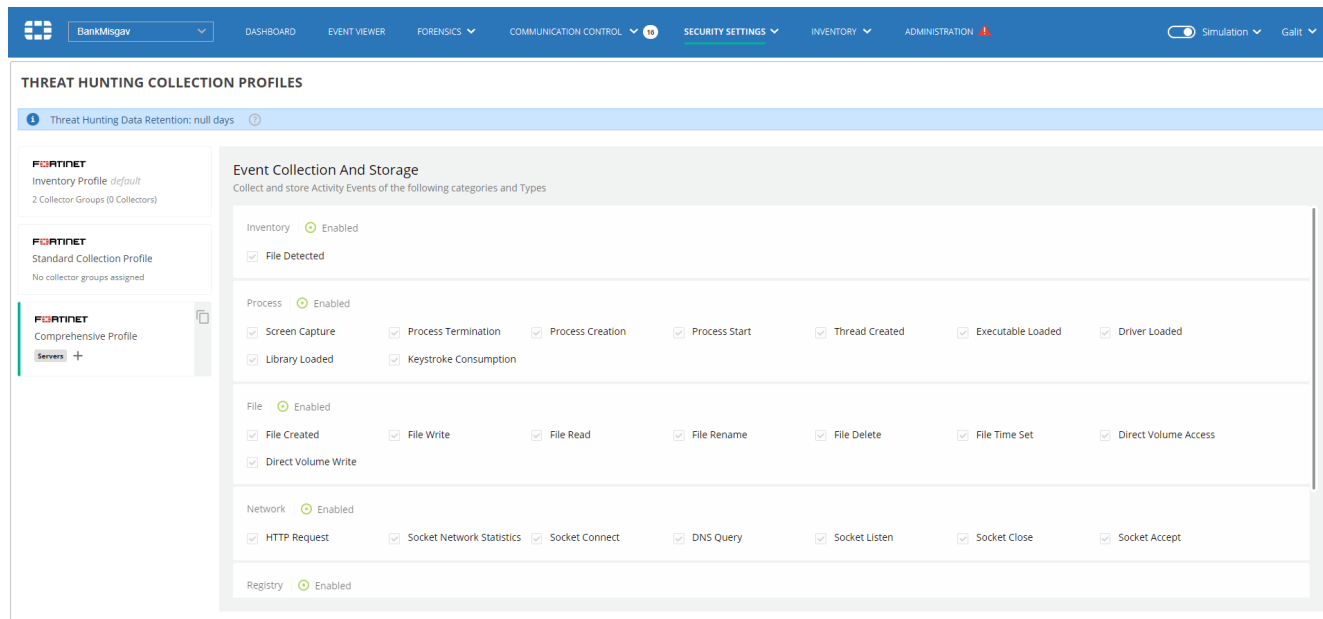


Threat Hunting Settings is a license-dependent add-on. You may contact [Fortinet Support](#) for more information.

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 237](#)). 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:



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 default 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 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 237](#)

Selecting a Profile on the left displays the categories and actions defined for that Profile in the right pane.

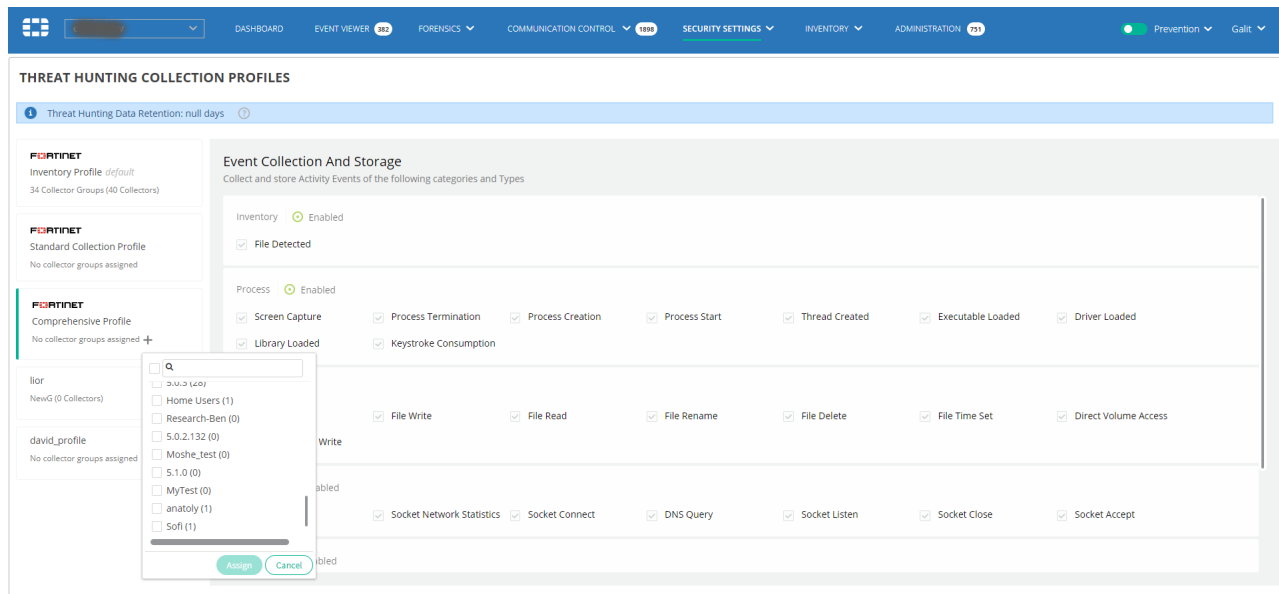
Check the checkboxes of the actions for which FortiEDR will collect activity data.

## Assigning a Collector Group to a Profile

Profiles are assigned to Collector Groups. Only a single Profile can be assigned to each Collector Group. New Collector Groups are automatically assigned to the default Inventory Scan Fortinet Profile, which is the first Profile listed in the Profiles pane.

### 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:

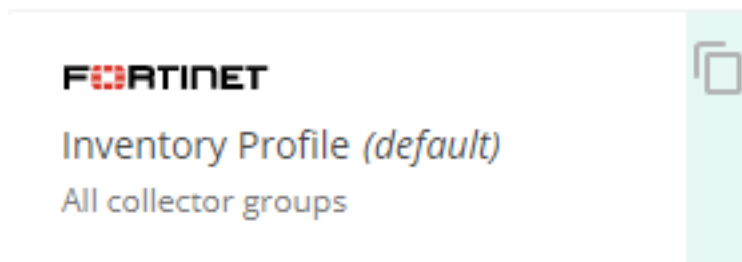


2. Select the checkbox(s) of the Collector Group(s) to assign to the Profile.
3. Click **Assign**. A message is displayed indicating that the selected groups are currently assigned to another Profile and they will be reassigned and asking for you approval. Please approve.

## 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.

## 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 92](#)). 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:

The screenshot displays the 'THREAT HUNTING COLLECTION EXCLUSIONS' page. On the left, there is a sidebar with a search bar and a list of exclusion lists. The main area shows a table of exclusions with columns for EVENT TYPE, SOURCE ATTRIBUTES, TARGET ATTRIBUTES, OS, LAST UPDATED, and STATE.

EVENT TYPE	SOURCE ATTRIBUTES	TARGET ATTRIBUTES	OS	LAST UPDATED	STATE
<input type="checkbox"/> Process Terminat...	SIGNER same		Windows	2022-01-06 11:04:49 by lior	Enabled
<input type="checkbox"/> Process Terminat...		SIGNER bla	Windows	2021-06-02 15:47:45 by lior	Enabled
<input type="checkbox"/> File Read/File Write	FILE NAME git.exe	FILE NAME HEAD	Windows	2021-01-14 15:41:34 by lior	Enabled
<input type="checkbox"/> Socket Connect	FILE NAME Teams.exe	REMOTE IP 13.79.26.107	Windows	2021-01-14 12:05:23 by lior	Enabled
<input type="checkbox"/> File Read	FILE NAME git.exe	FILE NAME gitconfig	Windows	2021-01-13 16:08:04 by lior	Enabled
<input type="checkbox"/> File Read	FILE NAME vcpkgshr.exe		Windows	2021-01-11 11:14:49 by lior	Enabled
<input type="checkbox"/> File Read	FILE NAME silhouette studio.exe		Windows	2021-01-05 12:32:10 by lior	Enabled
<input type="checkbox"/> File Read	FILE NAME ss_bluetooth.exe		Windows	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

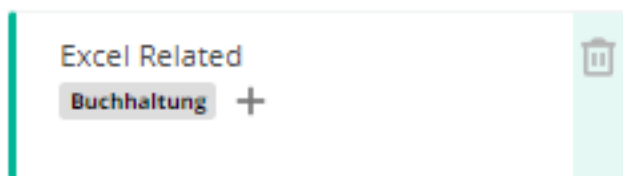
activity generated by that application. Exclusion Lists can be organized anyway you see fit. For example, you can create an Exclusion List for security products, a different one for PDF documents, a different one for HR-related software and so on.

## 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 <i>Delete</i>  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 237](#).
- **Target** – Which is identified by a target attribute, such as IP & Port.

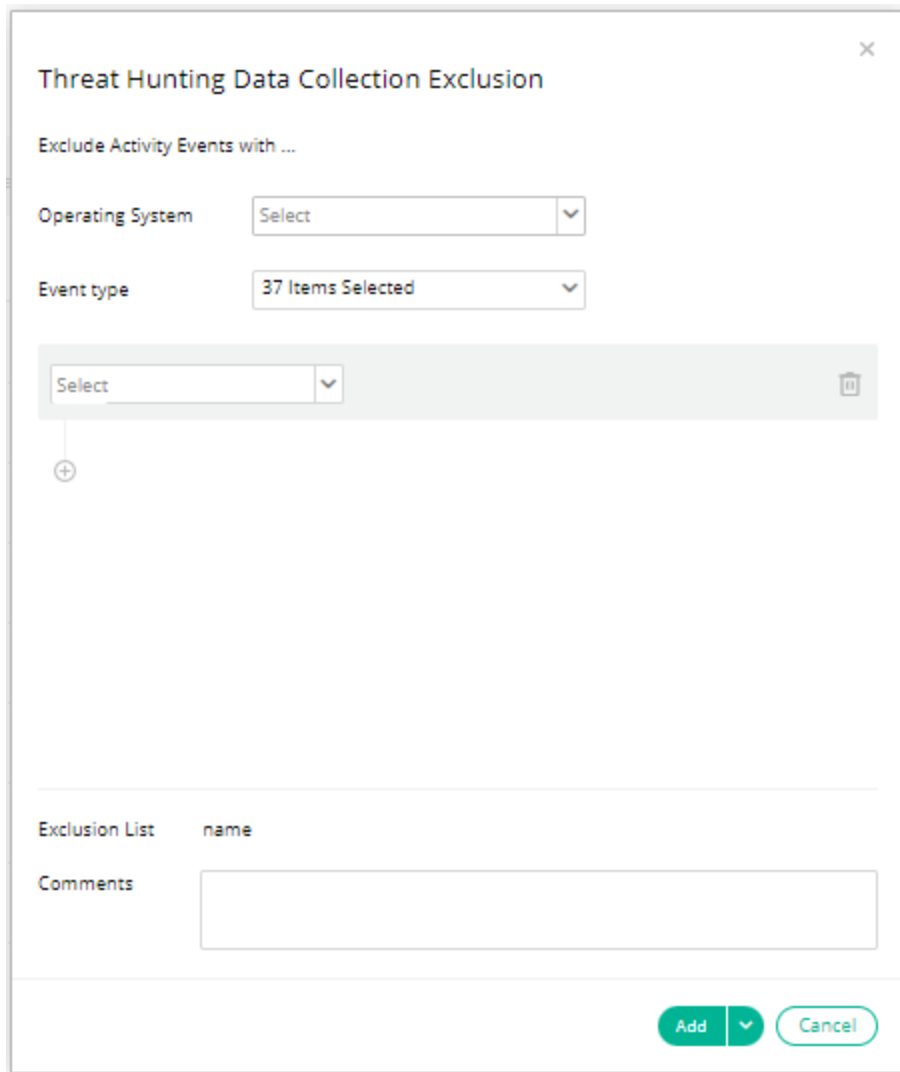
Exclusion can include all of these three or any combination. However, defining an exclusion that only contains a Type is not valid, because this kind of exclusion should be defined in a Threat Hunting Profile.



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:



The screenshot shows a dialog box titled "Threat Hunting Data Collection Exclusion". It contains the following fields and controls:

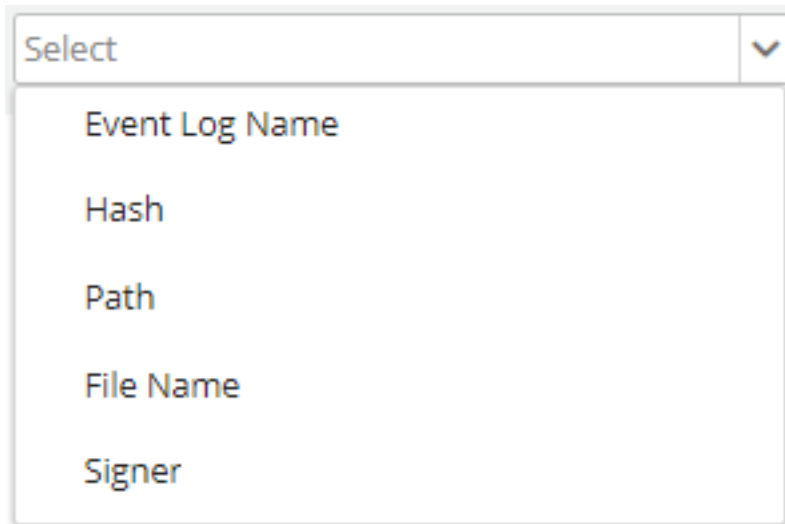
- Exclude Activity Events with ...**: A section header.
- Operating System**: A dropdown menu with "Select" as the current value.
- Event type**: A dropdown menu with "37 Items Selected" as the current value.
- A third dropdown menu with "Select" as the current value, located below the "Event type" dropdown.
- A trash icon to the right of the third dropdown menu.
- A plus icon (+) below the third dropdown menu.
- Exclusion List**: A table with one column labeled "name".
- Comments**: A text input field.
- Buttons**: "Add" and "Cancel" buttons at the bottom right.

3. From the *Operating system* dropdown menu, select either *Linux* or *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.

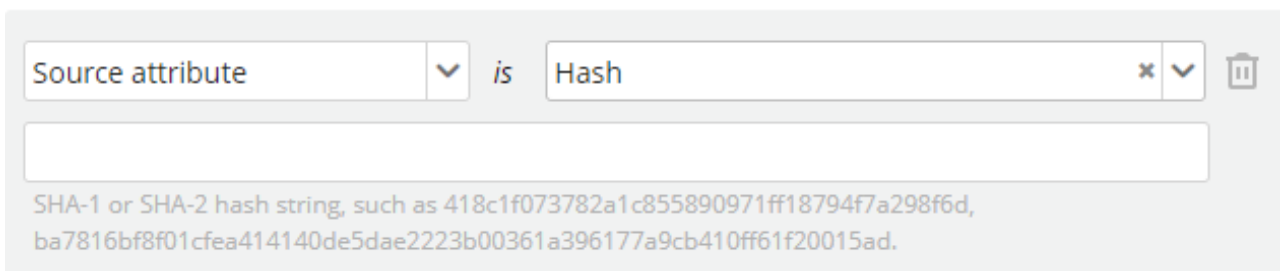
All action types to be collected are listed according to Category. You can select one or more actions from a single Category. Actions cannot be selected from different categories. For example, you can select the *Process Termination* and the *Process Start* options from the Process Category in the same 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.

The screenshot displays a configuration window for security settings. At the top, a dropdown menu is set to 'Any'. Below it, a grid of buttons lists various system events: 'Process Termination', 'Process Creation', 'Process Start', 'Thread Created', 'Executable Loaded', 'Key Created', 'Key Deleted', 'Key Renamed', 'Value Created', and 'Value Read'. A link labeled '15 More' is positioned to the right of the 'Value Read' button. Below the grid is a search bar with a magnifying glass icon and the text 'Search'. To the left of the search bar is a green checkmark icon. Below the search bar, a list titled 'Process' shows five items, each with a green checkmark: 'Process Termination', 'Process Creation', 'Process Start', 'Thread Created', and 'Executable Loaded'.

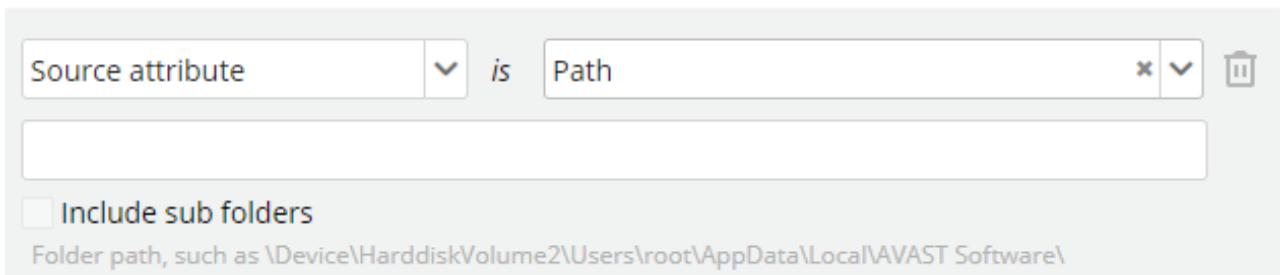
5. To define that an exclusion includes a *Source* attribute condition, from the *Select* box, select *Source attribute*, which can be identified by file name, path, hash and signer for Source Process or Event Log Name for event log related activity events, as shown below:



If you select *Hash*, then specify the hash, as shown below:

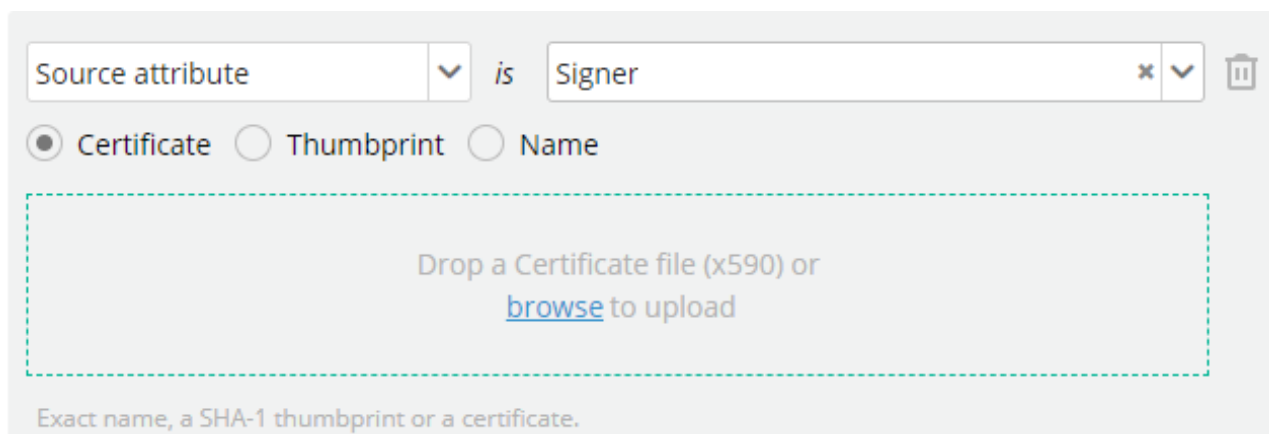


If you select *Path*, then specify the *Path*, as shown below. A path can include wild cards. If you wish to include sub-folders as well, check the *Select sub folders* checkbox.



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:

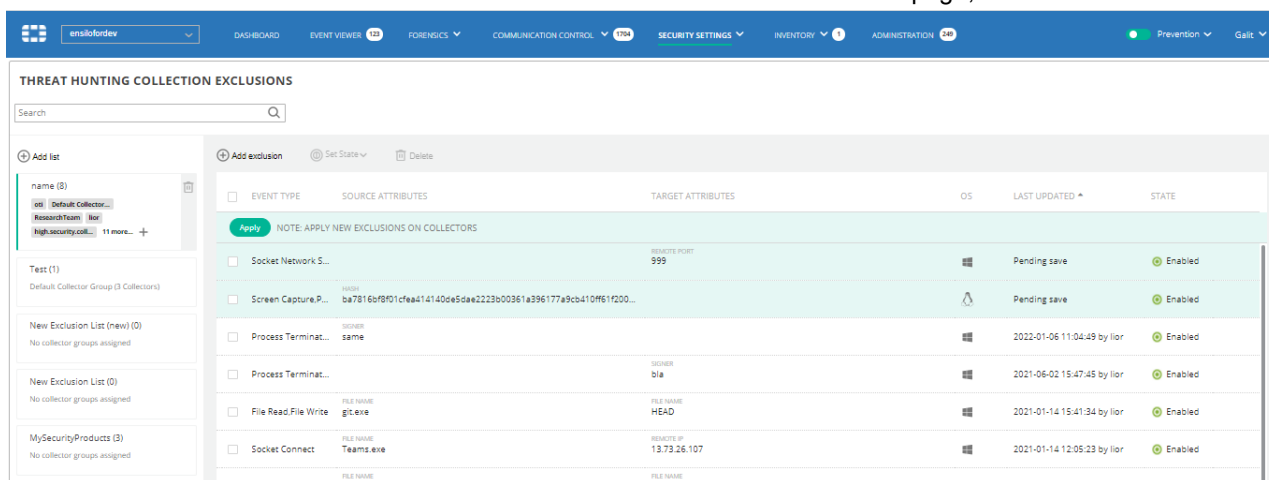
Targets can be identified by various criteria, depending on the selected Activity Event Category.

- 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 (3)  
☐ Default Collector...  
☐ ResearchTeam...  
☐ HighSecurity.com... 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

EVENT TYPE	SOURCE ATTRIBUTES	TARGET ATTRIBUTES	OS	LAST UPDATED	STATE
Apply NOTE: APPLY NEW EXCLUSIONS ON COLLECTORS					
<input type="checkbox"/>	Socket Network S...	REMOTE PORT 999		Pending save	Enabled
<input type="checkbox"/>	Screen Capture P...	HASH ba7816cf8f9f01cfad414140e5dae223b00361a396177a9cb410f61f200...		Pending save	Enabled
<input type="checkbox"/>	Process Terminat...	PROCESS same		2022-01-06 11:04:49 by Ior	Enabled
<input type="checkbox"/>	Process Terminat...	SIGNER bla		2021-06-02 15:47:45 by Ior	Enabled
<input type="checkbox"/>	File Read/File Write	FILE NAME git.exe		2021-01-14 15:41:34 by Ior	Enabled
<input type="checkbox"/>	Socket Connect	REMOTE IP 13.79.26.107		2021-01-14 12:05:23 by Ior	Enabled
<input type="checkbox"/>	File Read	FILE NAME mshta.exe		2021-01-14 12:05:23 by Ior	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**

Clone Playbook | Self Mode | Assign Collector Group | Delete

NAME	MALICIOUS	SUSPICIOUS	PUP	INCONCLUSIVE	LIKELY SAFE
Default Playbook	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>NOTIFICATIONS</b> (sent in protection and simulation modes)					
Send mail notification	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Send syslog notification	Syslog must be defined under Admin settings				
Open ticket	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>INVESTIGATION</b>					
Isolate device with Collector	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Isolate device with NAC	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Move device to the High Security Group	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>REMEDIATION</b>					
Terminate process	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Delete file	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Clean persistent data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Block address on Firewall	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**ASSIGNED COLLECTOR GROUPS**

Unassign Group

☐ 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.

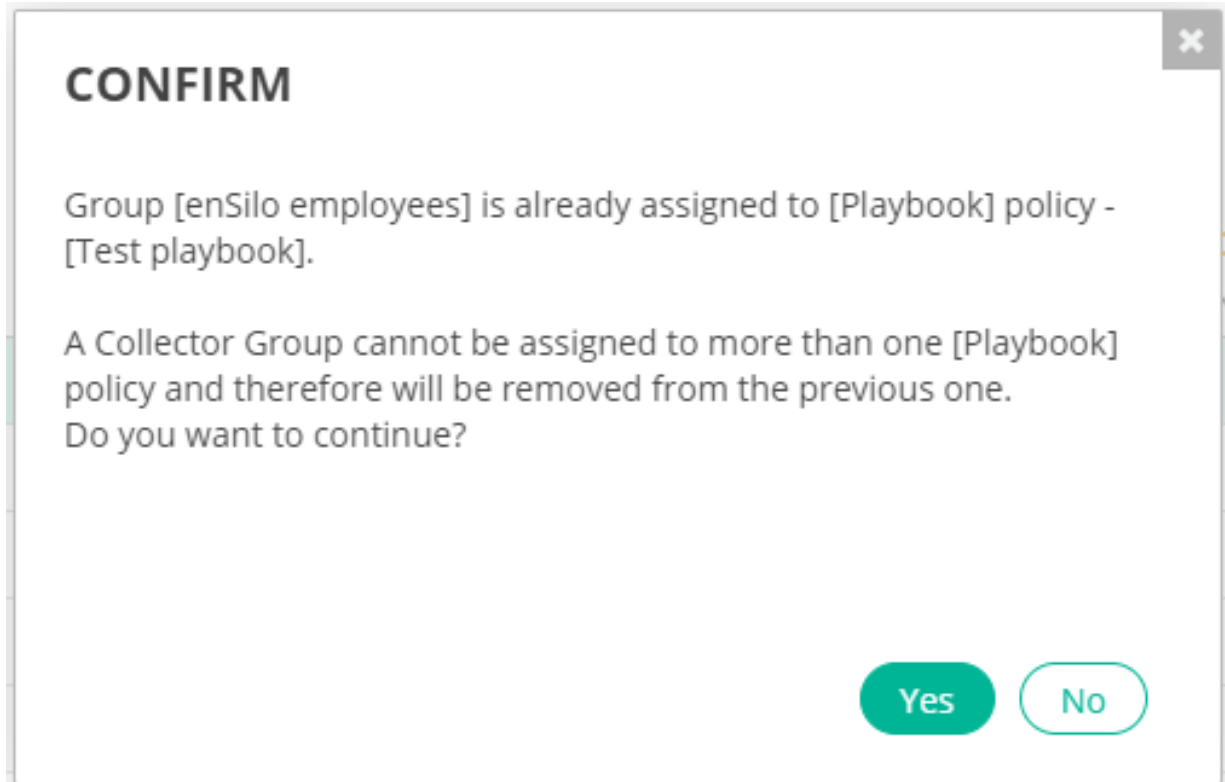
1. In the *AUTOMATED INCIDENT RESPONSE - PLAYBOOKS* page, select the Playbook policy row that you want to clone in the *Playbook Policies* list.
2. Do one of the following:
  - a. Select the checkbox(es) of the Collector Group(s) in the *Assigned Collector Groups* pane that you want to assign to the cloned Playbook policy. Then, click the *Unassign Group* button in the *Assigned Collector Groups* pane.

The screenshot shows the FortiEDR Security Settings interface. The main pane is titled 'AUTOMATED INCIDENT RESPONSE - PLAYBOOKS'. It contains a table of playbooks with columns for NAME, MALICIOUS, SUSPICIOUS, PUP, INCONCLUSIVE, and LIKELY SAFE. The 'Default Playbook' is selected. Below the table, there are sections for NOTIFICATIONS, INVESTIGATION, and REMEDIATION, each with a list of actions and checkboxes. On the right, the 'ASSIGNED COLLECTOR GROUPS' pane is visible, showing a list of collector groups: 'High Security Collector Group (0 collectors included)', 'emulation (4 collectors included)', and 'ensilo employees (2 collectors included)'. The 'ensilo employees' group is selected, and the 'Unassign Group' button is visible at the top of the pane.

- 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:

This screenshot is similar to the previous one, but it shows the 'Test playbook clone' selected in the 'PLAYBOOKS' list. The 'ASSIGNED COLLECTOR GROUPS' pane on the right remains the same, with 'ensilo employees (2 collectors included)' selected. The 'Unassign Group' button is still visible at the top of the pane.

The following message displays.



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.

Dashboard
Event Viewer 120
Forensics
Communication Control 130
Security Settings
Inventory
Administration 29
Protection
Barbara

### AUTOMATED INCIDENT RESPONSE - PLAYBOOKS

NAME	MALICIOUS	SUSPICIOUS	PUP	INCONCLUSIVE	LIKELY SAFE
<input checked="" type="checkbox"/> Default Playbook <span>Fortinet</span>					
NOTIFICATIONS (sent in protection and simulation modes)					
Send mail notification	✓	✓	✓	✓	✓
Send syslog notification	Syslog must be defined under <a href="#">Admin</a> settings				
Open ticket	✓	✓	✓	✓	✓
INVESTIGATION					
Isolate device with Collector	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Isolate device with NAC	A NAC connector must be defined under <a href="#">Admin</a> settings				
Move device to the High Security Group	✓	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
REMEDIATION					
Terminate process	✓	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

#### ASSIGNED COLLECTOR GROUPS

- ☐ Unassign Group
- ☐ 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 105](#)
- [Investigation on page 106](#)
- [Remediation on page 108](#)
- [Custom on page 110](#)

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

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. By default, the *Default Playbook* policy is set to Simulation mode, and only email notifications are automatically enabled, as shown below:

<input type="checkbox"/> NAME		 MALICIOUS	 SUSPICIOUS	 PUP	 INCONCLUSIVE	 LIKELY SAFE
<input checked="" type="checkbox"/>  Default Playbook 						
NOTIFICATIONS (sent in protection and simulation modes)						
	Send mail notification	✓	✓	✓	✓	✓
	Send syslog notification	Syslog must be defined under <a href="#">Admin settings</a>				
	Open ticket	Open ticket must be defined under <a href="#">Admin settings</a>				










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 313](#).

The *Malicious*, *Suspicious*, *PUP*, *Inconclusive*, and *Likely Safe* columns correspond to the possible classifications 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 that has that classification. Notifications are sent for all security events except those classified as *Likely Safe*. For example, the figure below shows that an email notification is sent whenever a Malicious, Suspicious, PUP or Inconclusive security event is triggered. *Syslog* and *Open Ticket* notifications work in the same way as Email notifications. For more details about classifications, see [Events pane on page 150](#).

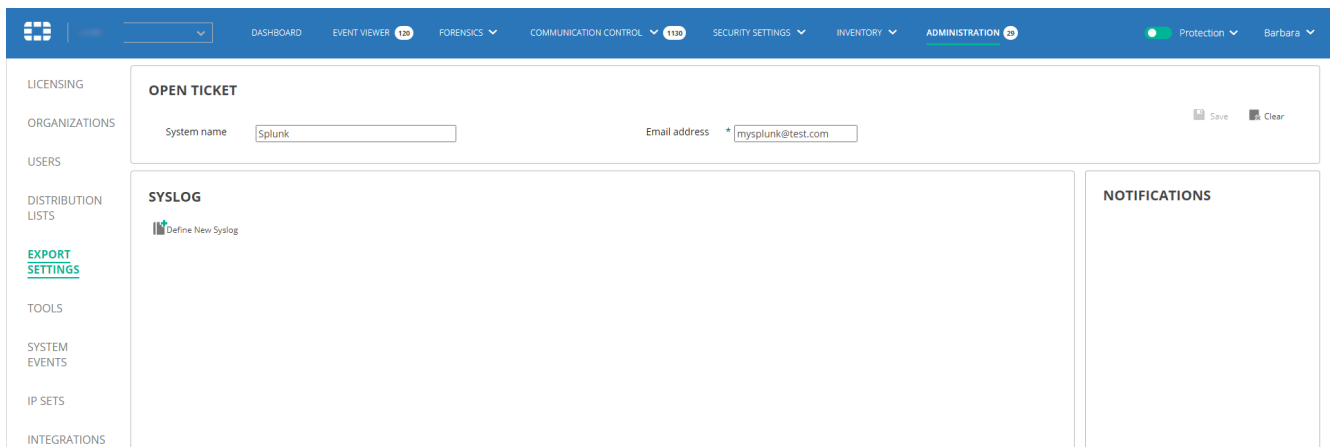
SMTP, Syslog and Open Ticket must already be configured in order to send their respective notifications. If their settings are not already configured, the relevant row in the Notifications list displays a message indicating that you must first configure it, as shown below:

## Security Settings

<input type="checkbox"/> NAME		 MALICIOUS	 SUSPICIOUS	 PUP	 INCONCLUSIVE	 LIKELY SAFE
▼  Default Playbook						
NOTIFICATIONS (sent in protection and simulation modes)						
	Send mail notification	✓	✓	✓	✓	✓
	Send syslog notification	Syslog must be defined under <a href="#">Admin settings</a>				
	Open ticket	Open ticket must be defined under <a href="#">Admin settings</a>				










The word Admin in each of these messages is a link that when clicked, jumps to the relevant place in the user interface to configure it. For example, when you click *Admin* in any of these messages, the following window displays in which you can configure the relevant settings.



The screenshot shows the FortiEDR Administration console. The top navigation bar includes links for DASHBOARD, EVENT VIEWER (120), FORENSICS, COMMUNICATION CONTROL (130), SECURITY SETTINGS, INVENTORY, and ADMINISTRATION (20). The left sidebar lists various settings categories: LICENSING, ORGANIZATIONS, USERS, DISTRIBUTION LISTS, EXPORT SETTINGS (highlighted), TOOLS, SYSTEM EVENTS, IP SETS, and INTEGRATIONS. The main content area is divided into two sections: 'OPEN TICKET' and 'SYSLOG'. The 'OPEN TICKET' section has a 'System name' field with 'Splunk' and an 'Email address' field with 'mysplunk@test.com'. The 'SYSLOG' section has a 'Define New Syslog' button. The 'NOTIFICATIONS' section is empty.

## 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.

<input type="checkbox"/> NAME		 MALICIOUS	 SUSPICIOUS	 PUP	 INCONCLUSIVE	 LIKELY SAFE
▼ <input type="checkbox"/>  Default Playbook						
NOTIFICATIONS (sent in protection and simulation modes)						
	Send mail notification	✓	✓	✓	✓	✓
	Send syslog notification	Syslog must be defined under <a href="#">Admin settings</a>				
	Open ticket	✓	✓	✓	✓	✓
INVESTIGATION						
	Isolate device with Collector	✓	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Isolate device with NAC	✓	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Move device to the High Security Group	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Investigation actions can be one of the following types:

- [Isolate device with Collector on page 107](#)
- [Isolate device with NAC on page 108](#)
- [Move device to High Security Group on page 108](#)

## Isolate device with Collector

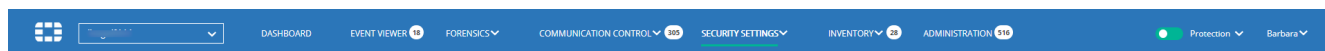
This action blocks the communication to/from the affected Collector. This action only applies for endpoint Collectors. For example, if the Playbook policy is configured to isolate the device for a malicious event, then whenever a maliciously classified security event is triggered from a device, then 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	<input type="checkbox"/>	✓	✓	✓	<input type="checkbox"/>
----------------	--------------------------	---	---	---	--------------------------

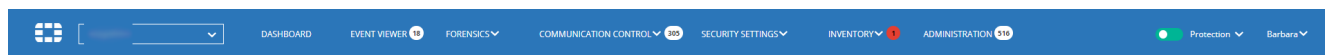


The tab bar at the top of the window may display a white circle(s) with a number inside the circle to indicate that new security events have not been read by the user. The number represents the number of new registered devices.




When the circle is white, it means that there are no isolated devices and the number inside the circle represents the number of new registered devices in the last three days.

When the circle is red, it indicates that there are one or more isolated devices. In this case, the number inside the circle indicates only the number of isolated devices.



You can hover over the number to see the list of new registered devices and isolated devices. Each row shows the number of devices added, by day.

TYPE	ACTION	ADDED	DATE
Collectors	Added	2	04-Feb-2020
Collectors	 Isolated	1	05-Feb-2020
IoT devices	Added	1	04-Feb-2020
IoT devices	Added	11	03-Feb-2020
IoT devices	Added	9	02-Feb-2020

## 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 345](#).

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	✓	✓	✓	✓	<input type="checkbox"/>
------------------------------------	---	---	---	---	--------------------------

## Remediation

Remediation actions enable you to remediate a situation in the FortiEDR system, should malware be detected on a device.

REMEDIATION						
Terminate process	✓	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Delete file	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Clean persistent data	✓	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Block address on Firewall	MyFW, FortiGat...	✓	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Remediation actions can be one of the following types:

- [Terminate process on page 108](#)
- [Delete file on page 109](#)
- [Clean persistent data on page 109](#)
- [Block address on Firewall on page 109](#)

## 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 227](#)

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 227](#)

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 227](#).

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 337](#).

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	✓	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Delete file	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Clean persistent data	✓	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Block address on Firewall	✓	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
▷ <input type="checkbox"/> 	Test playbook	<input type="checkbox"/>				
▷ <input type="checkbox"/> 	Victims Playbook	<input type="checkbox"/>				
▷ <input type="checkbox"/> 	Victims Playbook clone	<input type="checkbox"/>				

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	✓	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Delete file	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Clean persistent data	✓	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Block address on Firewall	A Firewall must be defined under <a href="#">Integrations Admin settings</a>				



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 *Admin* 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 365](#).



This list appears empty until at least one 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 101](#).
- *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 69](#).
- *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 72](#).
- *Delete*: Deletes a cloned Playbook policy. Default Playbook policies cannot be deleted.



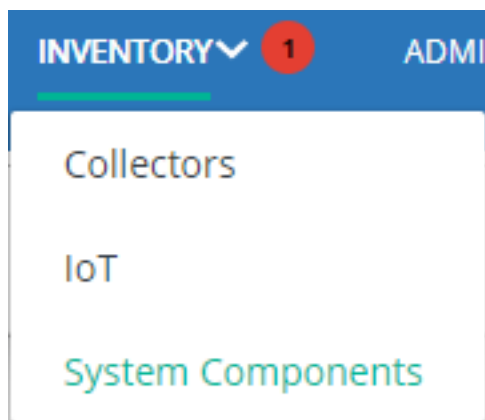
The default Playbook policy (named Default Playbook) is mandatory and cannot be deleted.

# Inventory

This chapter describes the FortiEDR Inventory, which enables you to monitor the health of FortiEDR components and to create Collector Groups.

## Introducing the Inventory

The *INVENTORY* tab displays separate pages for *COLLECTORS*, *IoT (devices)* and *System Components* (AGGREGATORS, CORES and REPOSITORIES). Click the down arrow next to *INVENTORY* and then select the relevant option to access its page, as shown below.

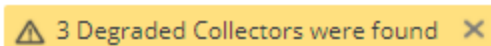


This view enables you to monitor system health and to define Collector Groups. If you have a large system with thousands of FortiEDR Collectors, it may take a few moments to populate this window.

By default, the *INVENTORY* tab and its various pages are filtered to display all the FortiEDR components that are degraded, except for FortiEDR Collectors, which are filtered to see all Collectors, regardless of their state.

COLLECTORS (19/42)									
<div> <span>All</span> <span>Create Group</span> <span>Move to Group</span> <span>Delete</span> <span>Enable/Disable</span> <span>Isolate</span> <span>Export</span> <span>Uninstall</span> </div>									
COLLECTOR GROUP NAME	DEVICE NAME	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	STATE	LAST SEEN	
High Security Collector Group (0/0)									
4.6.10r (0/0)									
5.0.1 (9/9)									
5.0.1.225 (0/0)									
5.0.1.71									

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.



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:

Collectors (3/46)

Collectors table is filtered to "Degraded" status. [Show all Collectors](#)

Search Collectors or Groups

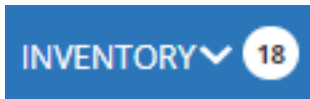
Degraded

- All
- ✓ Degraded
- Disabled
- Disconnected
- Isolated
- Migrated
- New
- Pending Migration
- Pending Reboot
- Running
- Selected
- Unmanaged

GROUP NAME	DEVICE NAME	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	STATE	LAST SEEN
			Windows 10 Pro	10.51.121.118	00-0C-29-EC-D3-0E	4.1.0.8	Degraded	Now
			Windows 10 Enterprise	10.51.121.80	00-50-56-BE-75-7F	4.1.0.8	Degraded	Now

158 Unmanaged devices were found

When a new FortiEDR Collector registers, an indicator displays on the *INVENTORY* tab.



The X/Y numbers in the *Collector Group Name* column indicate the following:

- X indicates the number of Collectors, based on the filter option selected (*New*, *Running*, *Disabled*, *Degraded*, *Disconnected*, *Isolated*, *Selected*, or *Pending Reboot*), as described on the preceding page.
- Y indicates the total number of Collectors in the Collector Group to which the Collector belongs.

For example, the figure below shows 4/4 for the Collector Group named 5.0.1, which means that there are 4 Collectors that are Running in a Collector Group containing 4 Collectors.

Collectors (37/47)

Showing 1-15/35

Search Collectors

7 Degraded Collectors were found

657 Unmanaged devices were found

All

Create Group Move to Group Delete Enable/Disable Isolate Connect to Device Export Uninstall

COLLECTOR GROUP NAME	DEVICE NAME	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	STATE	LAST SEEN
High Security Collector Group (0/0)								
5.0.1 (4/4)								
5.0.1.71 (0/0)								
5.0.2 (0/0)								
5.0.2.132 (0/0)								
5.0.3 (27/27)								1-10/27
	DESILO/R41TQ6F	ENSILO/eugene	Windows 10 Pro N	192.168.11.170	10-02-B5-42-A7-ED, FB-C...	5.2.0.2003	Running	Now
	ENSILO/ANM08	ENSILO/ianatoly	Windows 10 Pro	192.168.1.157	14-AB-C5-42-F3-F6	5.2.0.2003	Running	Now
	ENSILO/p121	ENSILO/khalifab	Windows 10 Pro	192.168.68.112	D4-81-D7-F9-9D-1A, FB-S...	5.2.0.2003	Running	Now
	ENSILO/p124	ENSILO/yinonm	Windows 10 Pro	192.168.68.101	A4-4C-C8-34-28-19, 90-6...	5.2.0.2003	Running	Now
	ENSILO/p127	ENSILO/lor	Windows 10 Pro	10.151.91.24	90-61-AE-76-FA-0C, A4-4...	5.2.0.2003	Running	Now
	ENSILO/p175	ENSILO/lor	Windows 10 Pro	10.151.91.60	34-48-ED-5E-C6-33, 34-4...	5.2.0.2003	Running	Now
	ENSILO/p195	ENSILO/leinat	Windows 10 Pro	10.51.102.105	18-DB-F2-46-23-61, 34-F...	5.2.0.2003	Running	Now
	ENSILO/p180	ENSILO/ianatoly	Windows 10 Pro	10.51.102.101	2C-F0-5D-14-08-36, CC-0...	5.2.0.2003	Running	Now
	...TINET-US/ldavidovits	Windows 10 Pro	10.51.102.156	AD-29-19-AC-E6-F4, AD-2...	5.2.0.2003	Running	Now	
	FORTINET-US/basapov	Windows 10 Pro	10.100.102.119	F0-9E-4A-29-9A-2D, 38-1...	5.2.0.2003	Running	Now	



The *Connect to Device* button opens a console that provides direct access to FortiEDR-protected devices. See [Administration](#) on page 274.



**To export the list of FortiEDR components:**

Use the *Export* button and select *Excel*.

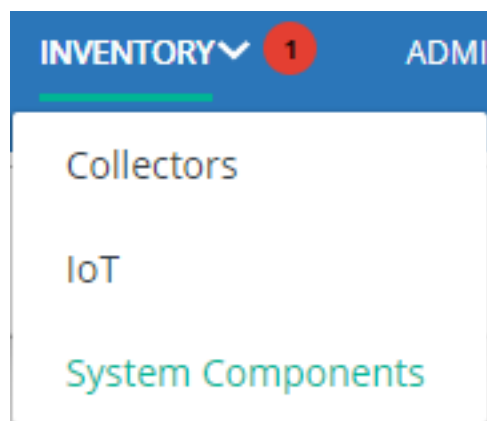
## Uninstalling a Collector

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.

## Collectors


The *COLLECTORS* 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 116](#). 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 117](#).

To access this page, click the down arrow next to *INVENTORY* and then select *Collectors*, as shown below.



[illegible]

The default Collector Group (to which new Collectors are automatically added) is marked with a yellow group icon . You can change to a different default Collector Group by clicking the group icon of another Collector Group.

Click the Expand icon (  ) to expand the list and display the FortiEDR Collectors that the Collector Group contains.

[Menu]
DASHBOARD
EVENT VIEWER (1)
FORENSICS ▼
COMMUNICATION CONTROL (10)
SECURITY SETTINGS ▼
INVENTORY (1)
ADMINISTRATION (10)
● Protection ▼
Barbara ▼

### COLLECTORS (46/46) Search Collectors or Groups ▼ 🔍

All ▼ | Create Group Move to Group Delete Enable/Disable Isolate Export Uninstall

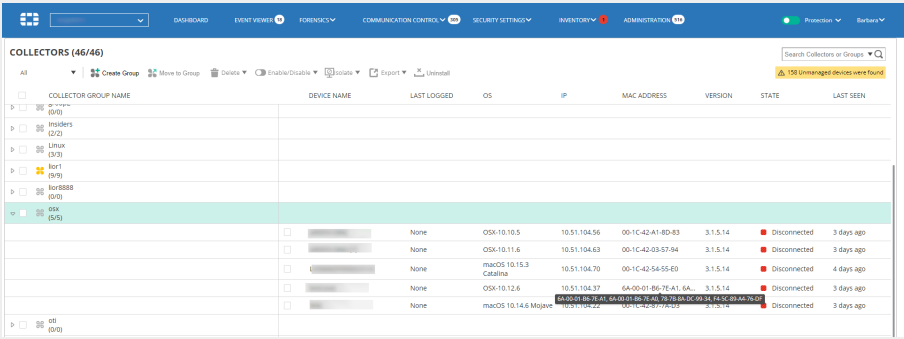
⚠️ 158 Unmanaged devices were found

COLLECTOR GROUP NAME	DEVICE NAME	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	STATE	LAST SEEN
High Security Collector Group (0/0)								
Default Collector Group (0/0)								
group1 (0/0)								
group2 (0/0)								
Insiders (2/2)								
Linux (3/3)								
lloer1 (9/9)								
	<input type="checkbox"/> [Device Name]	[Last Logged]	Windows 8.1 Enterprise N	10.51.121.126	00-50-56-8F-A8-E4	4.1.0.8	<span style="color: green;">●</span> Running	Now
	<input type="checkbox"/> [Device Name]	[Last Logged]	Windows 8.1 Enterprise	10.51.121.86	00-50-56-8F-0F-E9	4.1.0.8	<span style="color: green;">●</span> Running	Now
	<input type="checkbox"/> [Device Name]	[Last Logged]	Windows 8.1 Enterprise N	10.51.121.109	00-0C-29-54-97-1B	4.1.0.8	<span style="color: green;">●</span> Running	Now
	<input type="checkbox"/> [Device Name]	[Last Logged]	Windows Server 2019 Standard	10.51.121.163	00-50-56-8E-93-2E	4.1.0.8	<span style="color: green;">●</span> Running	Now
	<input type="checkbox"/> [Device Name]	[Last Logged]	Windows 8.1	10.51.121.114	00-0C-29-1D-5C-3B	4.1.0.8	<span style="color: green;">●</span> Running	Now
	<input type="checkbox"/> [Device Name]	[Last Logged]	Windows Server 2016 Standard	10.51.121.87	00-50-56-8F-07-55	4.1.0.8	<span style="color: green;">●</span> Running	Now
	<input type="checkbox"/> [Device Name]	[Last Logged]	Windows Server 2012 R2 Standard	10.51.121.130	00-50-56-8F-5E-C3	4.1.0.8	<span style="color: green;">●</span> Running	Now
	<input type="checkbox"/> [Device Name]	[Last Logged]	Windows 8	10.51.121.98	00-50-56-8F-49-91	4.1.0.8	<span style="color: green;">●</span> Running	Now
	<input type="checkbox"/> [Device Name]	[Last Logged]	Windows 8 Enterprise	10.51.121.125	00-50-56-8F-10-B5	4.1.0.8	<span style="color: green;">●</span> Running	Now

☐ ☒ lloer888

The following information is provided for each Collector:

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 <i>Delete</i> button.

Information Field	Description								
Collector Group Name	Specifies the name of the Collector Group to which the Collector is assigned.								
Device Name	Specifies the device name taken from the communicating device on which the FortiEDR Collector is installed.								
Last Logged	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.								
OS	Specifies the operating system of the communicating device on which the FortiEDR Collector is installed.								
IP	Specifies the IP address of the communicating device on which the FortiEDR Collector is installed.								
MAC Address	Specifies the 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.								
									
Version	Specifies the version of the FortiEDR Collectors installed on the communicating device.								
State	<p>Specifies the 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:</p> <table> <tr> <th>State</th><th>Description</th></tr> <tr> <td>Running</td><td>The FortiEDR 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>The device has not been connected for 30 or more consecutive days. Collectors in this state are not counted for licensing purposes. To see the list of Collectors in this state, click the down arrow in the <i>Search</i> box at the top right of the window to display the following window:</td></tr> </table>	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.	Disconnected (Expired)	The device has not been connected for 30 or more consecutive days. Collectors in this state are not counted for licensing purposes. To see the list of Collectors in this state, click the down arrow in the <i>Search</i> box at the top right of the window to display the following window:
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.								
Disconnected (Expired)	The device has not been connected for 30 or more consecutive days. Collectors in this state are not counted for licensing purposes. To see the list of Collectors in this state, click the down arrow in the <i>Search</i> box at the top right of the window to display the following window:								

Information Field	Description
	<div> <div> <div>SEARCH GROUPS &amp; COLLECTORS</div> <div> <div>Collector Group</div> <div>Device Name</div> <div>User</div> <div>Operating System</div> <div>Mac Address</div> <div>IP</div> <div>Version</div> <div>Last seen before</div> <div> <input type="checkbox"/> Show only devices that have not been seen for more than 30 days </div> <div>Search</div> <div>Cancel</div> </div> </div> <p>Then, check the <i>Show only devices that have not been seen for more than 30 days</i> checkbox, and click the <b>Search</b> button. The Collectors area then displays only devices in the Disconnected (Expired) state.</p> <p>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.</p> <p>Specifies that this FortiEDR Collector was disabled in the FortiEDR Central Manager. This feature is not yet available in version 1.2.</p> <p>Specifies that 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).</p> </div>
Last Seen	Counts the number of days passed from the last time this Collector communicated with the Core.

## 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 *Create group* button. The following window displays:

2. Enter any name for this group and click *Create new group*.

## Assigning Collectors to a Collector Group

1. In the *COLLECTORS* page, select the checkboxes of the FortiEDR Collectors to be moved to a different group.
2. Select the *Move to group*  *Move to group* button. The following window displays showing the names of the current Collector Groups and how many Collectors each contains:

×

## COLLECTOR GROUPS

COLLECTOR GROUP NAME	# OF COLLECTORS
Default VDI Group	0
enSilo Servers	0
Home users	6
my citrix pool (VDI)	0
OSX Users	13

Move to group

Cancel

3. Select the Collector Group to which to move the selected Collectors.
4. Click the *Move to group* 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

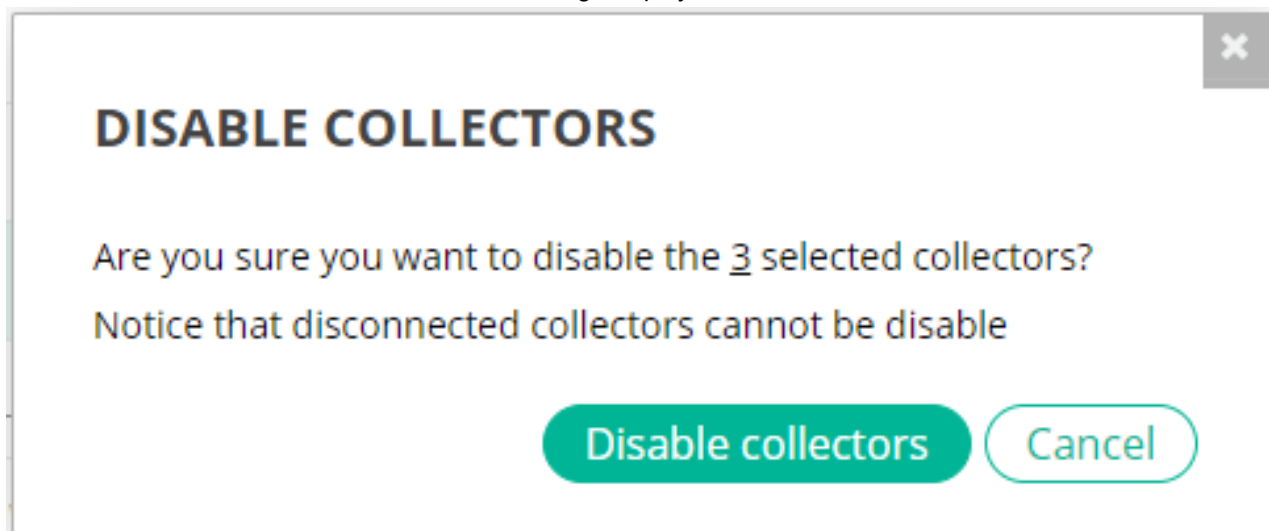
You can enable or disable one or more Collectors simultaneously.

### To enable one or more Collectors simultaneously:

1. In the *COLLECTORS* 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 on the *Enable/Disable* button and select *Enable*. This button is only enabled when one or more Collectors are selected.

### 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 on the *Enable/Disable* button and select *Disable*. This button is only enabled when one or more Collectors are selected. A confirmation message displays:



3. Click *Disable collectors*.

## 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, as described below. For more details see [Investigation on page 106](#)

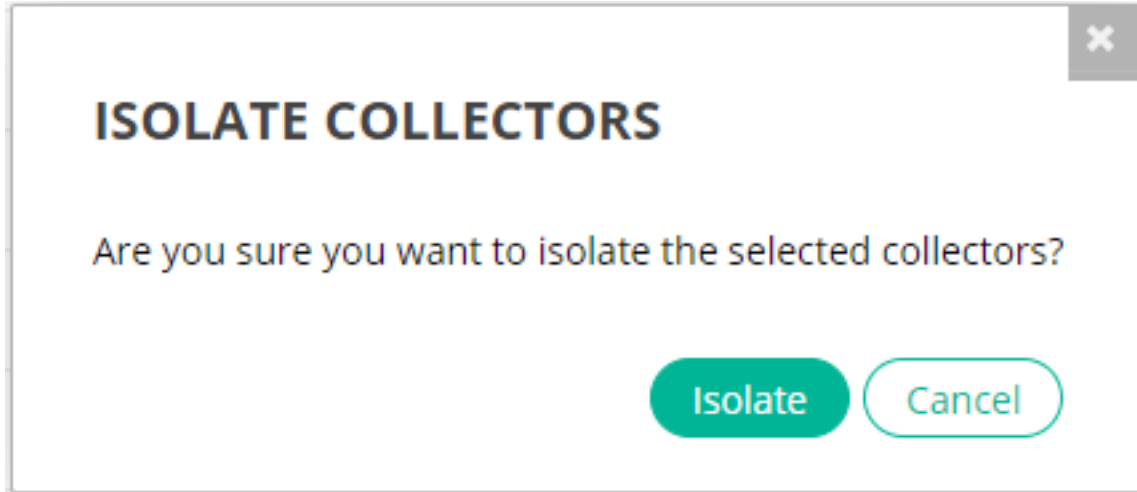



Isolation mode takes effect upon any attempt to establish a network session after isolation mode has been initiated. Connections that were established before device isolation was initiated remain intact. The same applies for Communication Control denial configuration changes. Note that both Isolation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

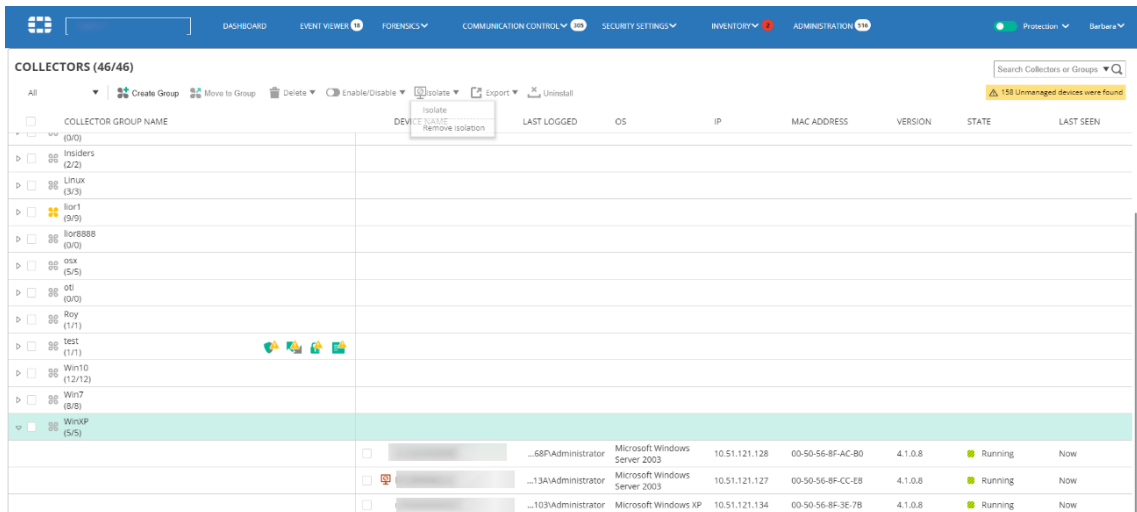
## To isolate a device:

1. In the *COLLECTORS* page, select the checkbox(es) of the FortiEDR Collector(s) that you want to isolate.
2. Click the down arrow on the *Isolate* button and select *Isolate*.

The following window displays:

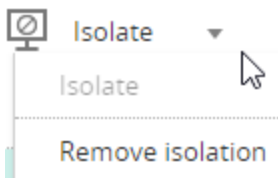


- Click the *Isolate* button. A red icon  appears next to the relevant Collector to indicate that the Collector has been isolated, as shown below:



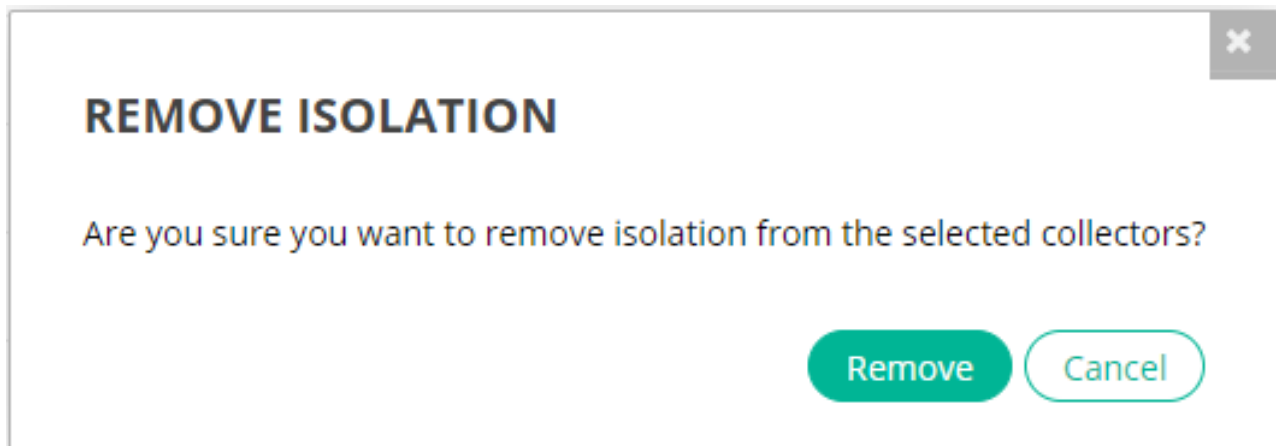
### To remove isolation from a device:

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.





The following window displays:



3. Click *Remove*.

## Unmanaged devices

The *COLLECTORS* page also indicates the number of unmanaged devices found in the system at the top right of the page, meaning those non-IoT devices on which no Collector is installed.



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.

COLLECTORS (44/49)									
<div> <span>All</span> <span>Create Group</span> <span>Move to Group</span> <span>Delete</span> <span>Enable/Disable</span> <span>Isolate</span> <span>Export</span> <span>Uninstall</span> </div>									
<input type="checkbox"/>	COLLECTOR GROUP NAME	DEVICE NAME	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	STATE	LAST SEEN
<input type="checkbox"/>	High Security Collector Group (0/0)								
<input type="checkbox"/>	Default Collector Group (0/0)								
<input type="checkbox"/>	emulation (1/1)								
<input type="checkbox"/>	group1 (0/0)								

To view the list of unmanaged devices, select *Unmanaged* in the filter at the top left of the page.

COLLECTORS (185/185)									
<div> <div>Unmanaged</div> <div>Create Group</div> <div>Move to Group</div> <div>Delete</div> <div>Enable/Disable</div> <div>Isolate</div> <div>Export</div> <div>Uninstall</div> </div> <div>Search Devices or Groups</div> <div>185 Unmanaged devices were found</div>									
COLLECTOR GROUP NAME	DEVICE NAME	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	STATE	LAST SEEN	
Unmanaged devices (185/185)								1-10/185	
			Windows	10.51.121.144	00-50-56-BE-1C-63		Unmanaged	Today	
			Windows	10.51.121.135	00-50-56-8F-B3-E1		Unmanaged	Today	
			Windows	10.51.121.136	00-50-56-BE-20-6C		Unmanaged	Today	
			Windows	10.51.121.133	00-50-56-8F-45-EF		Unmanaged	Today	
			Windows	10.51.121.124	00-50-56-8F-70-81		Unmanaged	Today	
			Windows	10.51.121.53	00-50-56-BE-5E-3F		Unmanaged	Today	
			Windows	10.51.121.173	00-50-56-BE-F3-09		Unmanaged	Today	
			Windows	192.168.2.1			Unmanaged	Today	
			Windows	192.168.186.1			Unmanaged	Today	
			Windows	10.51.121.63	00-50-56-BE-06-EE		Unmanaged	Today	

None of the action buttons at the top of the window are available for unmanaged devices, as there is no Collector installed on these devices.

## 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 324](#).

IOT DEVICES (102/102)									
<div> <div>All</div> <div>Create Group</div> <div>Move to Group</div> <div>Delete</div> <div>Device Details</div> <div>Export</div> </div> <div>Search IOT Device</div>									
DEVICE GROUP NAME	DEVICE NAME	CATEGORY	MODEL	INTERNAL IP	MAC ADDRESS	LOCATION	FIRST SEEN	LAST SEEN	
Default IOT Group (4/4)									
		Other	Dell	10.51.102.55	8C-04-BA-75-9D-AD	Israel	57 days ago	6 days ago	
		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	
		Expired Other	Dell	10.51.102.5	A4-4C-C8-BE-4D-83	Israel	134 days ago	113 days ago	
		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

Move to GroupCancel

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:

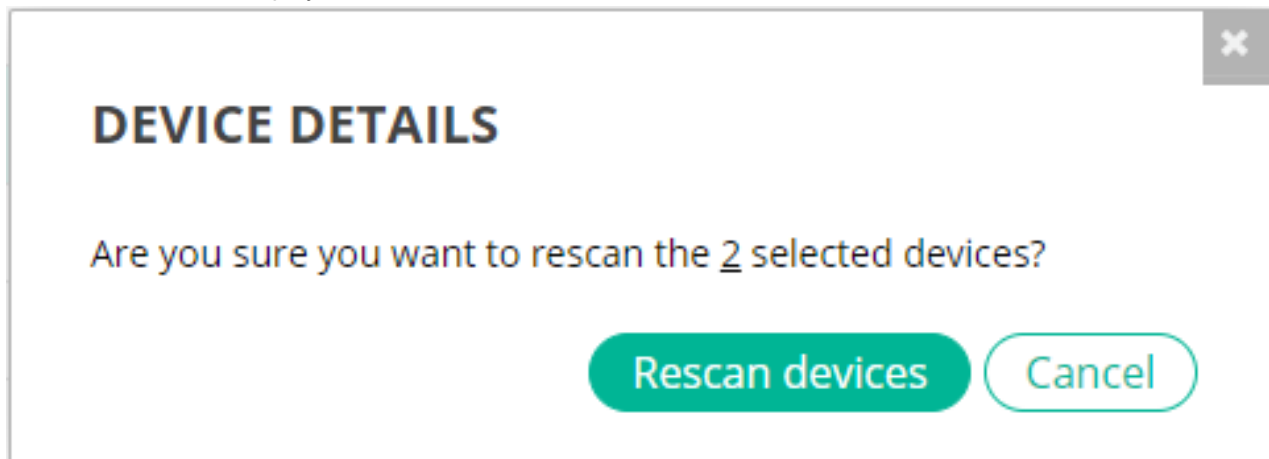
1. Select the IoT group's/IoT device's checkbox.
2. Click *Delete*.

## 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.



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:

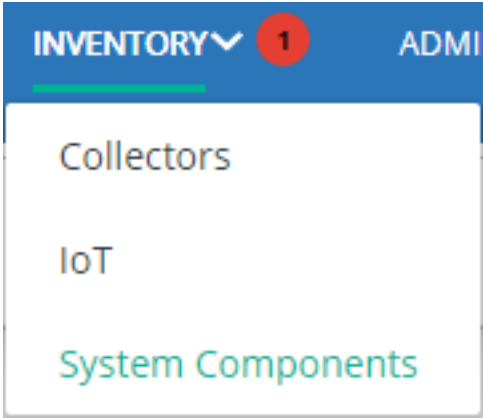
1. Check the checkbox of the device of interest.
2. Select *Device Info* under the *Export* button.



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.

## System Components

The *SYSTEM COMPONENTS* page lists the FortiEDR Aggregators, Cores and Repositories. To access this page, click the down arrow next to *INVENTORY* and then select *System Components*, as shown below.



The following displays:

A screenshot of the FortiEDR web interface showing the 'SYSTEM COMPONENTS' page. The page has a blue header with navigation tabs: DASHBOARD, EVENT VIEWER (183), FORENSICS, COMMUNICATION CONTROL, SECURITY SETTINGS, INVENTORY (selected), and ADMINISTRATION (55). The 'INVENTORY' tab is active, showing three sections: CORES (2/2), AGGREGATORS (1/1), and REPOSITORIES (2/2).  
**CORES (2/2)**  
Search Cores [Q]  
Delete Export  
All IP NAME DEPLOYMENT MODE FUNCTIONALITY VERSION STATE  
Cloud Both 5.0.1.153 Running  
Cloud Core only 5.0.1.153 Running  
**AGGREGATORS (1/1)**  
Search Aggregators [Q]  
Delete Export  
All IP NAME CONNECTED COLLECTORS VERSION STATE  
127.0.0.1:8081 Fortinet 41 5.0.1.155 Running  
**REPOSITORIES (2/2)**  
IP STATE  
ensiloford-ev-prod-middleware.edr-prod.ensilo.com:8095 Running

# Aggregators

The *AGGREGATORS* area lists the FortiEDR Aggregators.

A screenshot of the FortiEDR web interface showing the 'AGGREGATORS' section. The page has a blue header with navigation tabs: DASHBOARD, EVENT VIEWER (183), FORENSICS, COMMUNICATION CONTROL (305), SECURITY SETTINGS, INVENTORY (selected), and ADMINISTRATION (516). The 'INVENTORY' tab is active, showing three sections: CORES (1/1), AGGREGATORS (1/1), and REPOSITORIES (1/1).  
**AGGREGATORS (1/1)**  
Search Aggregators [Q]  
Delete Export  
All IP NAME CONNECTED COLLECTORS VERSION STATE  
127.0.0.1:8081 Fortinet 46 4.1.0.5 Running  
**REPOSITORIES (1/1)**

Click the *Expand* icon ( ) to expand the list. The following information is provided for each FortiEDR Aggregator:

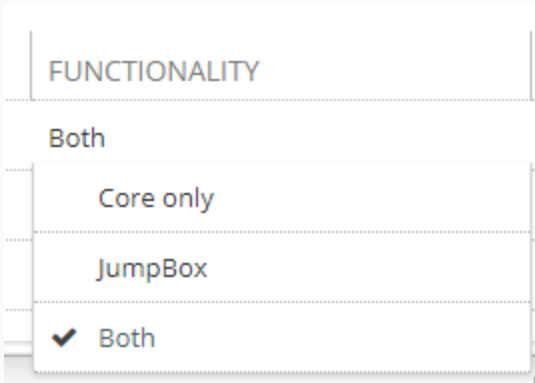


Information Field	Description
Checkbox	Check this checkbox to select the Aggregator. You can then use one of the buttons at the top left of the window, such as the <i>Delete</i> button.
IP	Specifies the IP address of the communicating device on which the FortiEDR Aggregator is installed.
Name	Specifies 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.

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 <i>Delete</i> 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. <ul style="list-style-type: none"> <li>• Cloud</li> <li>• On-premise</li> </ul>

Information Field	Description
Functionality	<p>Specifies the core's functionality and enables you to modify it by selecting one of the following options:</p>  <ul style="list-style-type: none"> <li>• <i>Core only</i> – Specifies that the system provides basic FortiEDR Core functionality: events processing, communication control handling, activity events proxy to the Repository and so on.</li> <li>• <i>JumpBox</i> – 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.</li> </ul> <hr/> <div>  <p>The <i>JumpBox</i> option is unavailable for cloud Cores. To configure a cloud Core to function as JumpBox, please contact <a href="#">Fortinet Support</a>.</p> </div> <hr/> <ul style="list-style-type: none"> <li>• <i>Both</i> – Provides both <i>Core</i> and <i>JumpBox</i> functionality, as described above.</li> </ul> <hr/> <div>  <p>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.</p> </div> <hr/>
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.





Dashboard

▼

DASHBOARD

EVENT VIEWER 11

FORENSICS ▼

COMMUNICATION CONTROL ▼ 305

SECURITY SETTINGS ▼

INVENTORY ▼ 1

ADMINISTRATION 510

Protection
▼

Barbara ▼

SYSTEM COMPONENTS

CORES (1/1)

AGGREGATORS (1/1)

REPOSITORIES (1/1)

IP	STATE
10.132.0.66:443	<span>Running</span>

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.

## 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 129
- Exporting logs for Cores on page 131
- Exporting logs for Aggregators on page 131

## Exporting logs for Collectors

## To export Collector logs:

1. In the *COLLECTORS* page, select the checkboxes of the FortiEDR Collectors for which you want to export logs.

Dashboard

Event Viewer18

Forensics

Communication Control202

Security Settings

InVENTORY1

ADMINISTRATION310

Protection

Barbara

COLLECTORS (46/46)

Search Collectors or Groups

All

Create Group

Move to Group

Delete

Enable/Disable

Isolate

Export

Uninstall

PDF

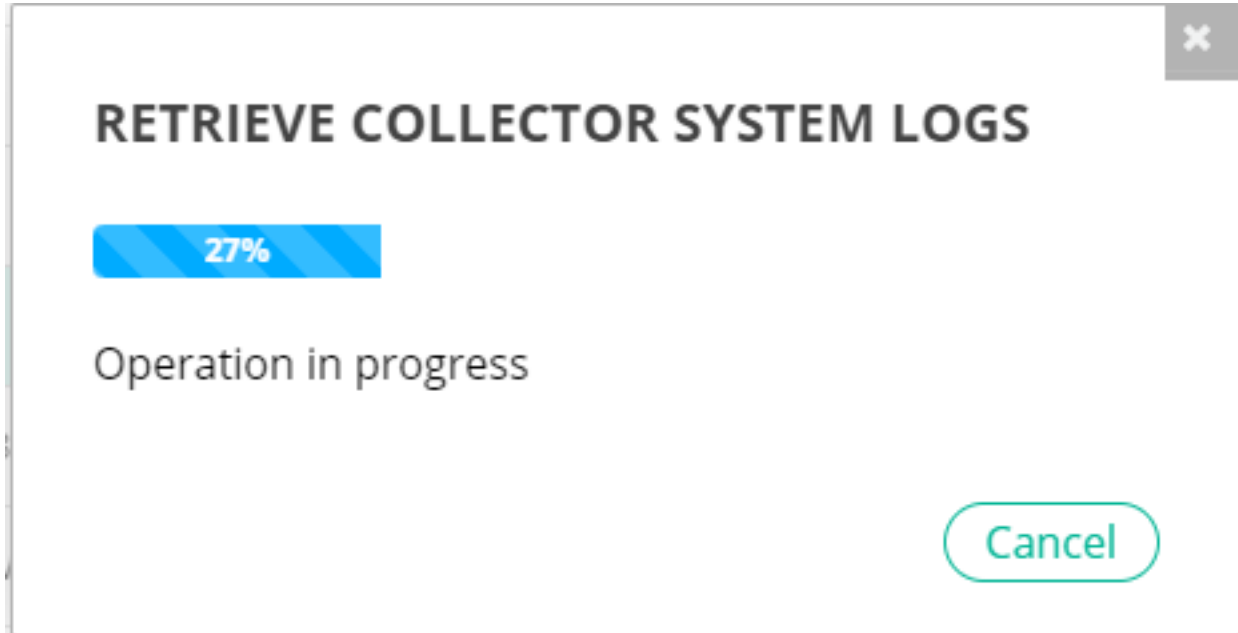
Excel

Collector Logs

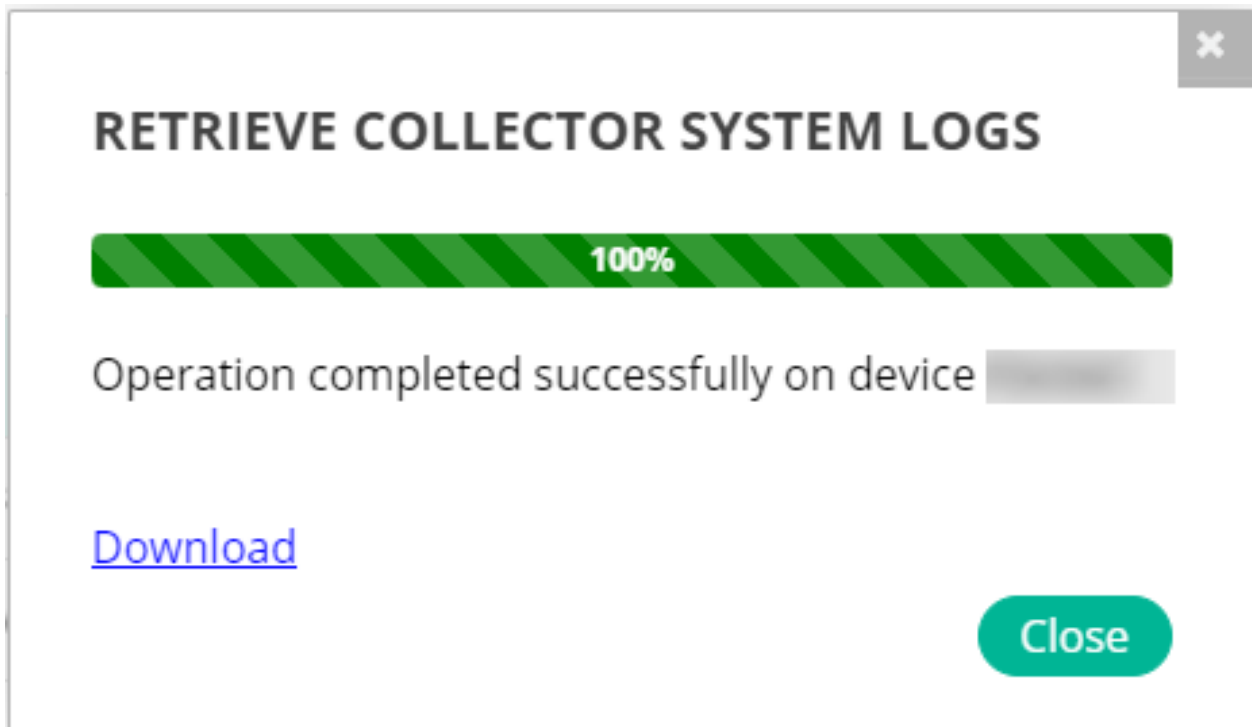
158 Unmanaged devices were found

COLLECTOR GROUP NAME	DEVICE NAME	LOGGED	OS	IP	MAC ADDRESS	VERSION	STATE	LAST SEEN
<div><div></div><div>High Security Collector Group (0/0)</div></div>								
<div><div></div><div>Default Collector Group (0/0)</div></div>								
<div><div></div><div>group1 (0/0)</div></div>								
<div><div></div><div>group2 (0/0)</div></div>								
<div><div></div><div>Insiders (2/2)</div></div>								
<div><div></div><div>Linux (3/3)</div></div>								
<div><div></div><div>llor1 (9/9)</div></div>								
	<div><div></div><div>...RA_QA_81_32root</div></div>	Windows 8.1 Enterprise N	10.51.121.126	00-50-56-8F-A8-E4	4.1.0.8	<div><div></div>Running</div>	Now	
	<div><div></div><div>...QA_WIN8_1_root</div></div>	Windows 8.1 Enterprise	10.51.121.86	00-50-56-8F-0F-E9	4.1.0.8	<div><div></div>Running</div>	Now	
	<div><div></div><div>PANDA1root</div></div>	Windows 8.1 Enterprise N	10.51.121.109	00-0C-29-54-97-1B	4.1.0.8	<div><div></div>Running</div>	Now	

- Click the down arrow on the *Export* dropdown menu and select *Collector Logs*.  
A progress window displays, showing the status of the Collector log retrieval process:



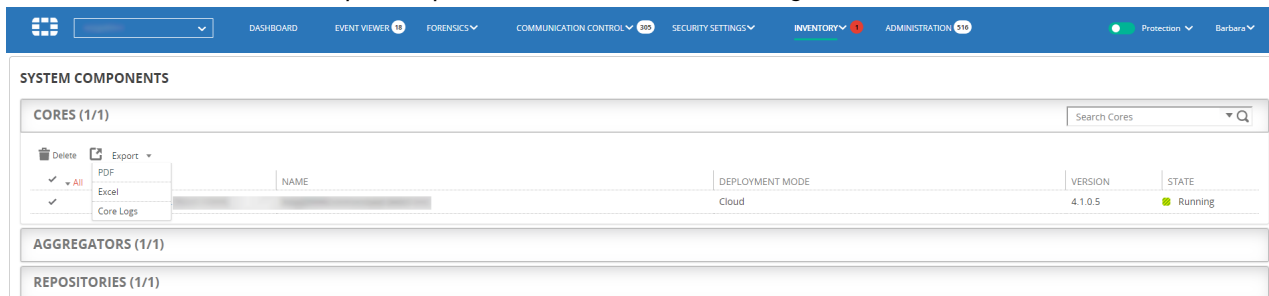
After the retrieval process completes, the following window displays:



- Click *Download* to automatically send the retrieved logs to Fortinet technical support.

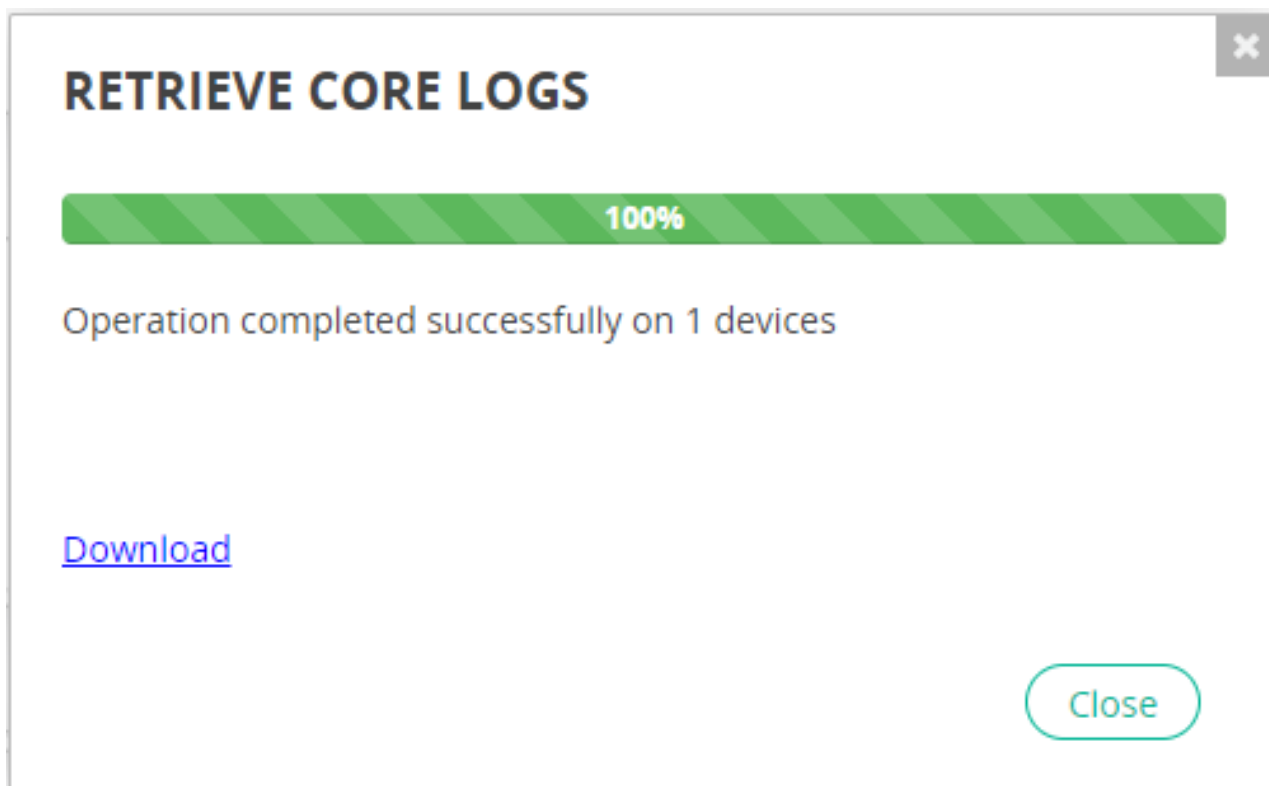
## Exporting logs for Cores

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*.



A progress window displays, showing the status of the log retrieval process:

After the retrieval process completes, the following window displays:

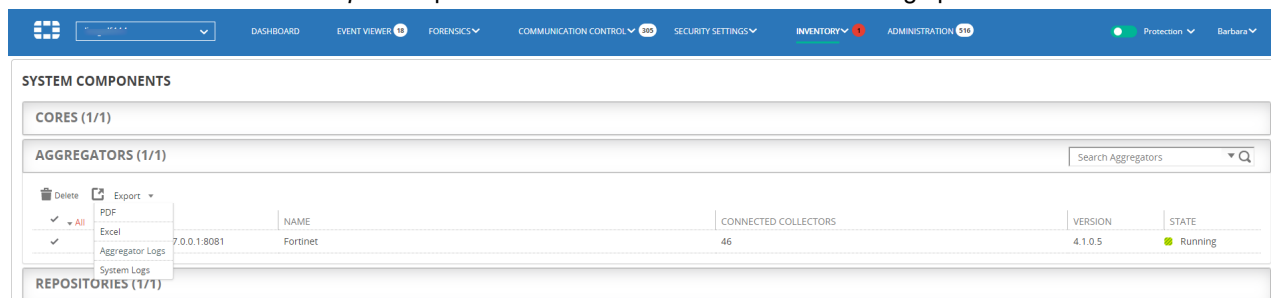


3. Click *Download* to automatically send the retrieved logs to Fortinet technical support.

## 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:



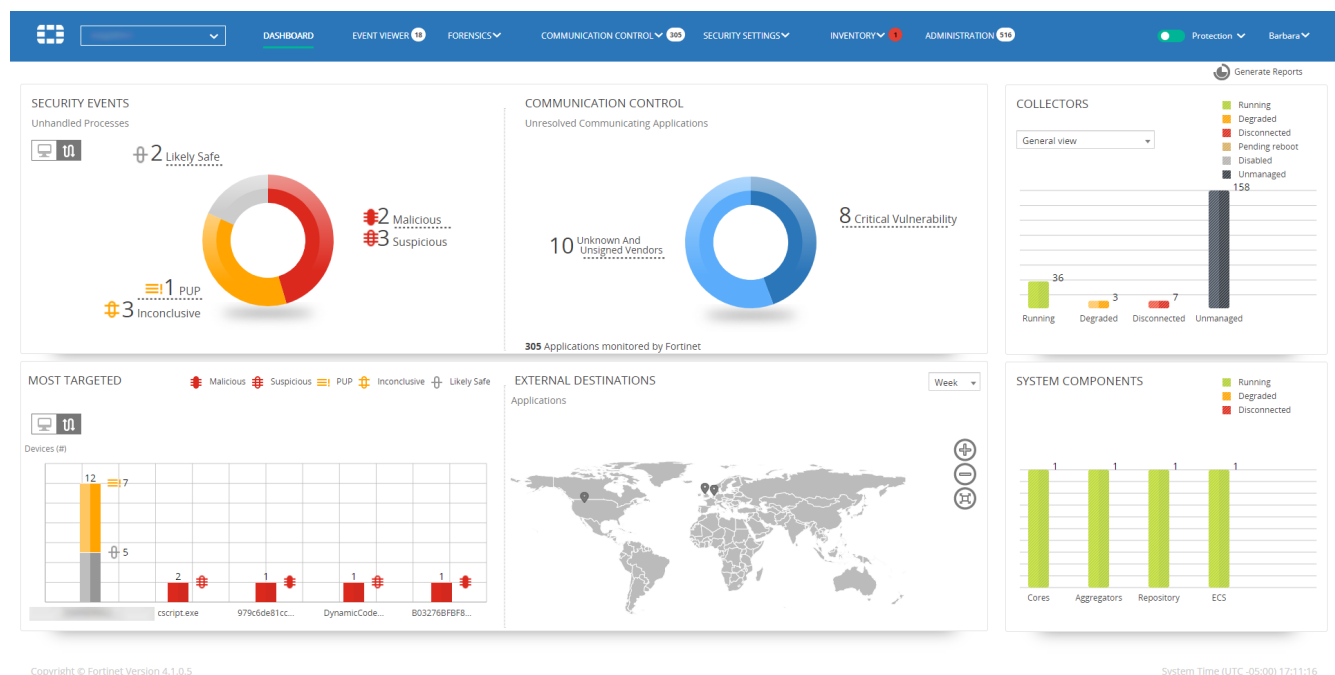
- a. *Aggregator Logs*: Exports the log for the selected Aggregator(s).
- b. *System Logs*: Exports the logs of the central Manager.  
A progress window displays.  
After the retrieval process completes, a window displays.  
Click *Download* to automatically send the retrieved logs to Fortinet technical support.

# 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 Dashboard is automatically displayed after installation 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**

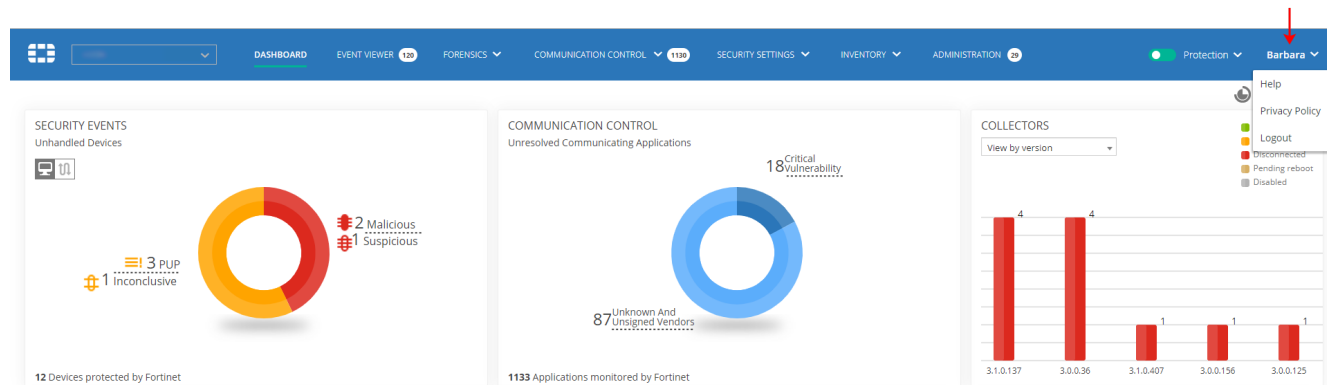
The Dashboard enables you to display two different slices or views of the data collected by FortiEDR:

- **Device View** (🖥️): This view presents information by device, and represents all the security events detected on a given device.
- **Process View** (🔍️): This view presents information by process, and represents all the security events detected for a given process.

Click the applicable view button at the top left of the window to display that view in the *DASHBOARD* tab.

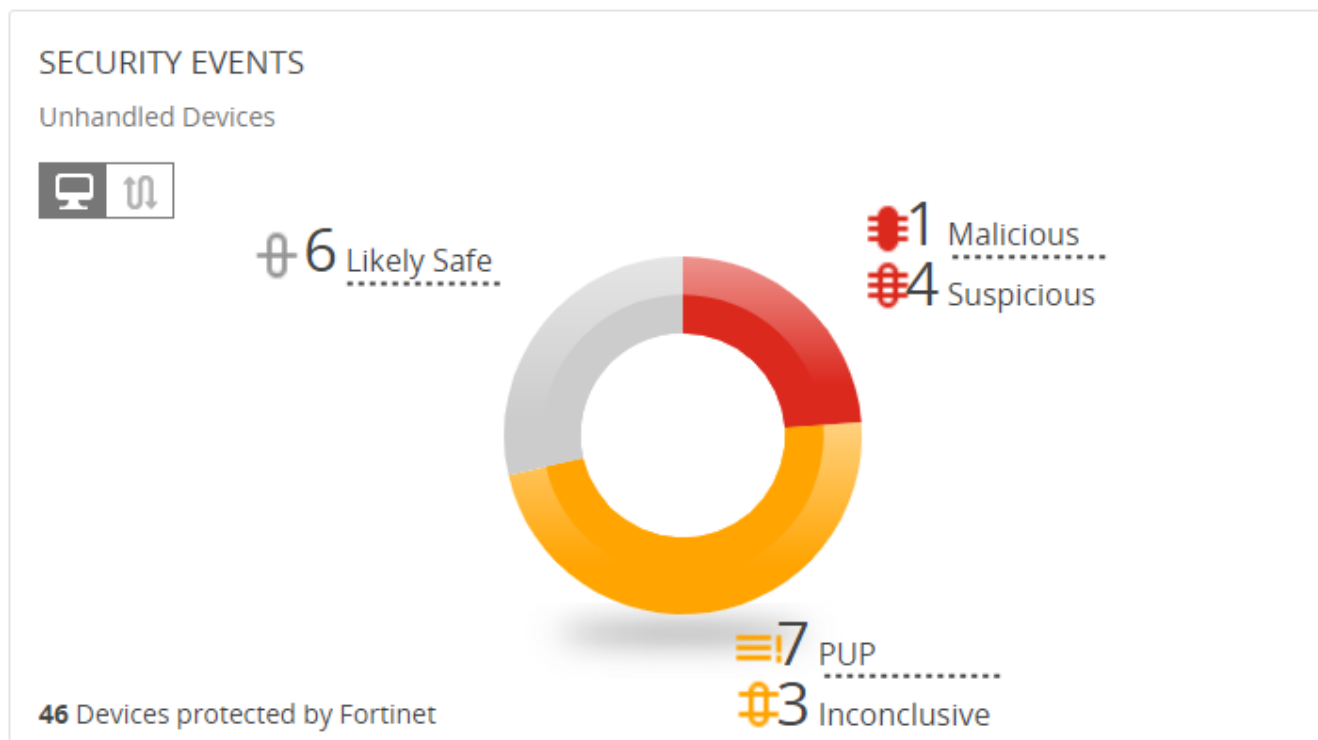
The information presented in the Dashboard represents an aggregation of events. For more details, you may refer to the [Event Aggregation on page 147](#). FortiEDR aggregates security events in both the Device view and the Process view in the Dashboard.

Use the *Logged-in User* dropdown list at the top-right of the window to access the following options:

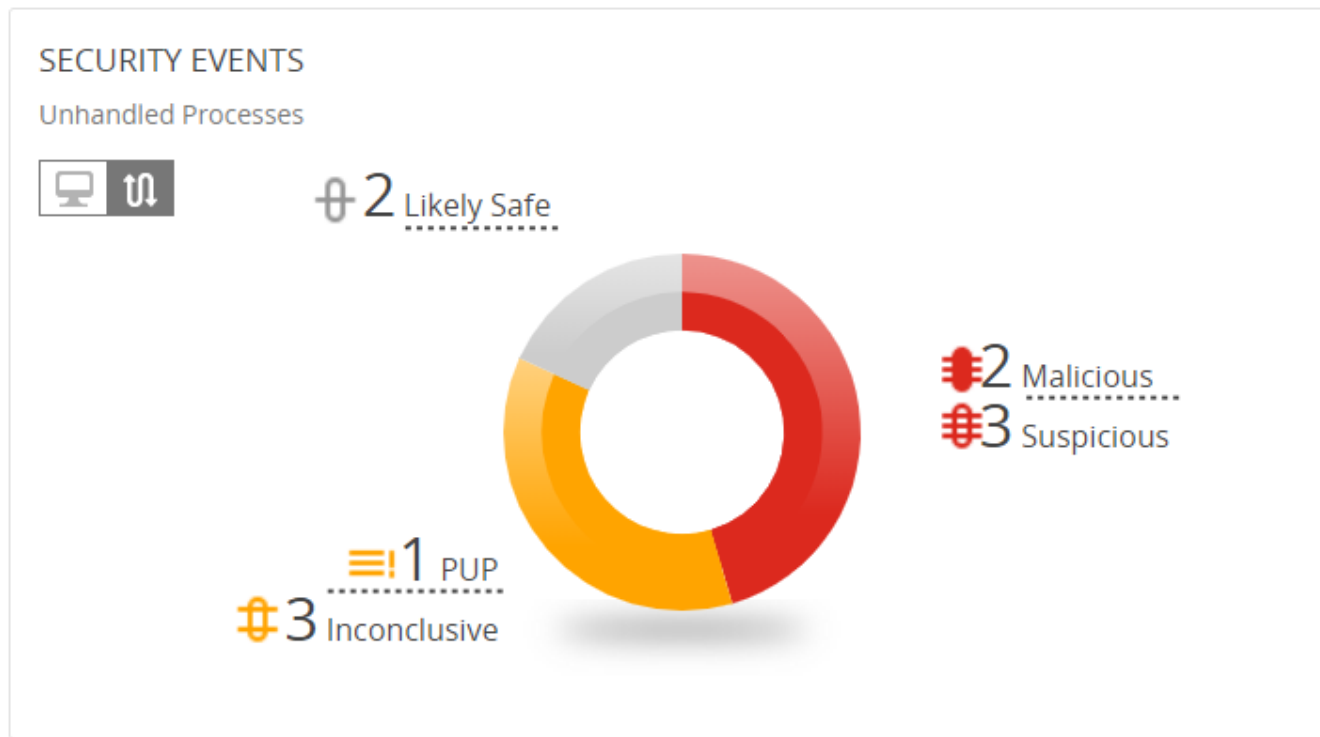


- **Help**: Enables you to download the latest version of the *FortiEDR Installation and Administration Guide*.
- **Privacy Policy**: Downloads the FortiEDR privacy policy.
- **Logout**: Exits the FortiEDR application.

## Security Events chart



The *SECURITY EVENTS* chart for the Device view shows the number of protected devices in the system at the bottom of the pane.



The *SECURITY EVENTS* chart shows the number and classification of the FortiEDR security events that have not yet been handled. The chart is color-coded according to security event classification:

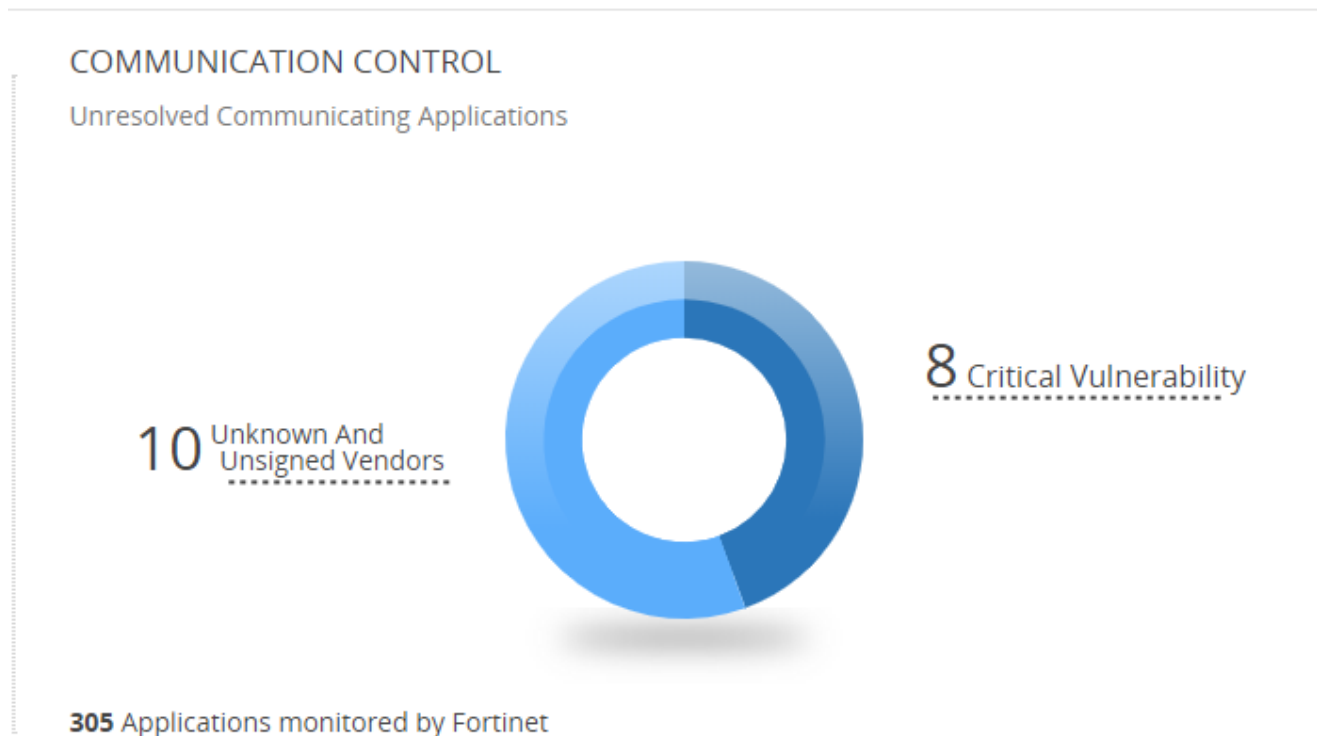
- **Red:** Critical
- **Yellow:** High
- **Grey:** Medium

Click this chart to drill down to the Event Viewer, which shows a filtered chart listing the unhandled security events ([Marking a security event as handled/unhandled on page 156](#)) according to the classification (color) that you clicked in this chart.

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.

## Communication Control chart

The *COMMUNICATION CONTROL* chart displays a breakdown of the applications with an Unresolved status detected in your organization.



Click a box in the chart to drill down to the Communication Control.

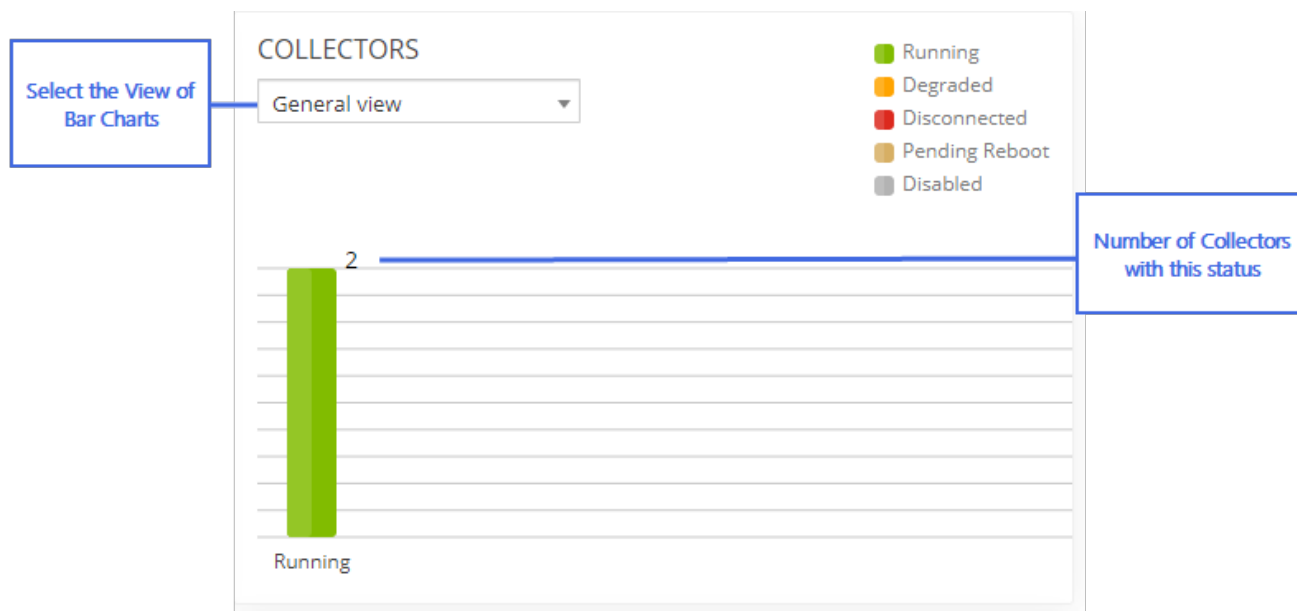
## Collectors chart

The *COLLECTORS* chart provides an overview of FortiEDR Collectors. When in operating system view, each bar in this chart represents a different operating system: Windows, Windows Server and MacOS. In addition, when in General View mode, the window shows the number of unmanaged devices in the system.

The bar chart is color-coded and numbered to indicate the distribution of statuses among the components within the operating system group.

Each bar chart indicates the version or the Operating System of that component, according to the option that you selected in the *View By* dropdown menu.



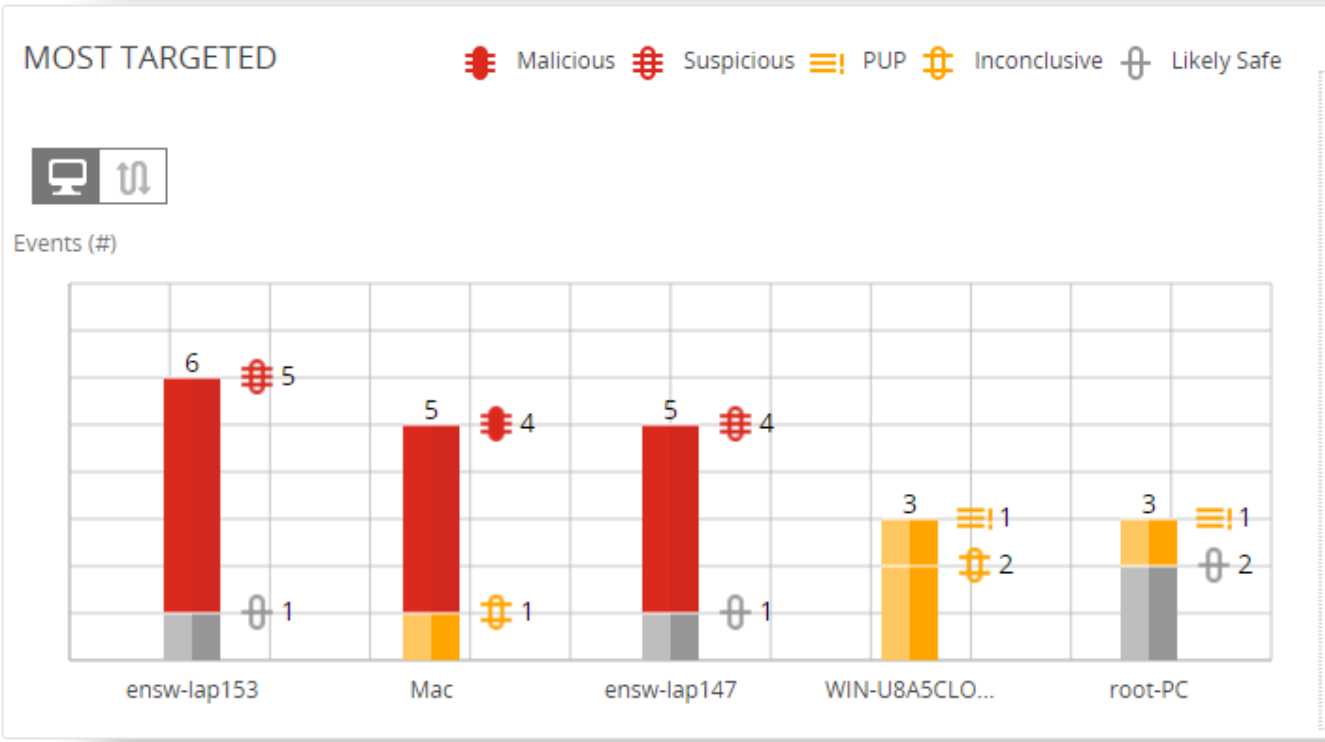


Click this chart to drill down to the relevant [Inventory on page 111](#), which shows a filtered chart listing the Collectors with the selected version or Operating System.



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.

## Most Targeted charts



The *MOST TARGETED* 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.

Click this chart to drill down to the [Event Viewer on page 146](#), which shows a filtered chart listing the security events for the selected process or device.

## External Destinations

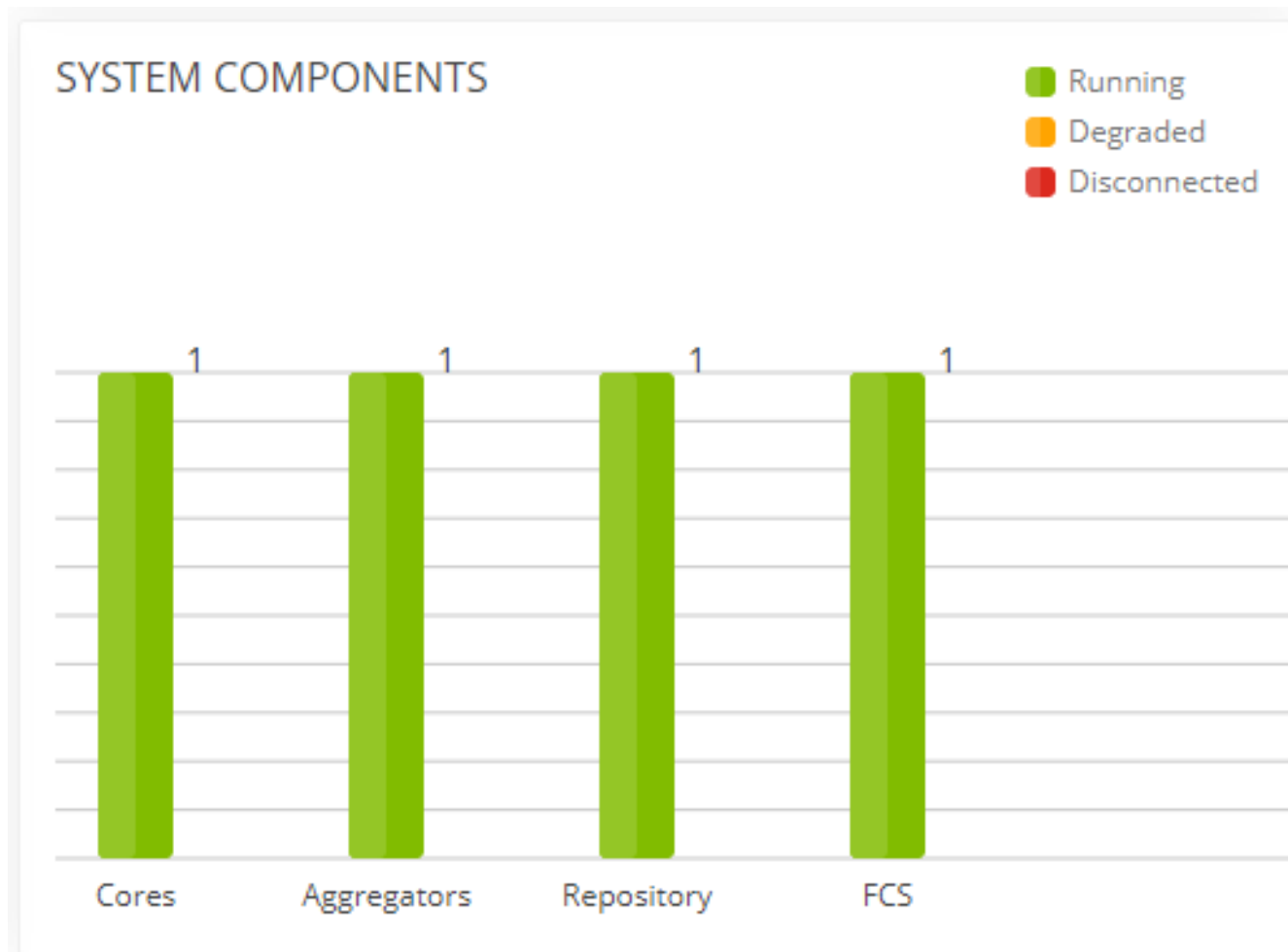
The *EXTERNAL DESTINATIONS* map displays the locations of the destinations for the security event for the past day, week, or month. Select the timeframe for displaying data in the dropdown menu at the top of the pane.

## EXTERNAL DESTINATIONS

Week ▼



## System Components

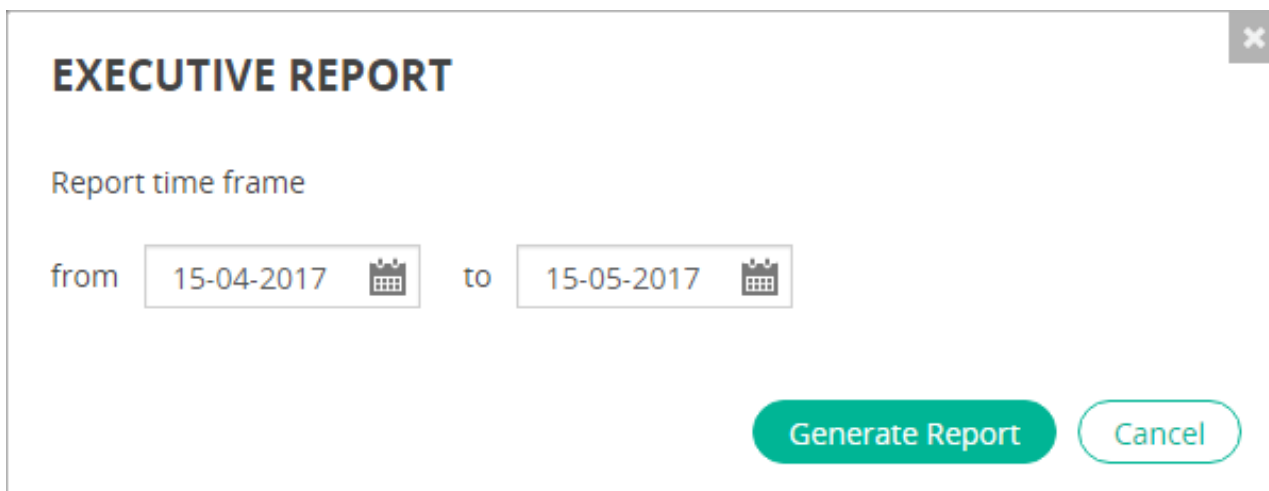


The *SYSTEM COMPONENTS* chart shows the status of the Cores, Aggregators, Threat Hunting Repository, and FCS.

## Executive Summary Report



The Executive Summary report provides a comprehensive summary describing security events and system health.

- 1 Click the  **Generate Reports** button at the top-right of the Dashboard window. The following window displays:



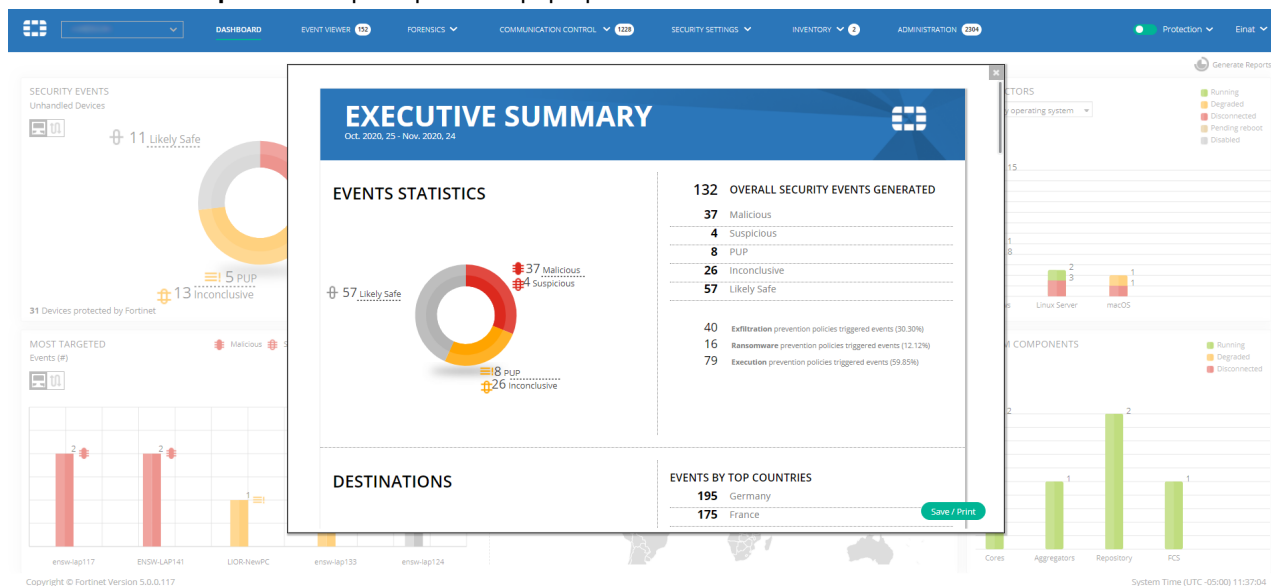
**EXECUTIVE REPORT**

Report time frame

from   to  

**Generate Report** **Cancel**

2. Specify the timeframe for the report in the **From/To** fields. The default period for the report is one month.
3. Click **Generate Report**. The report opens in a pop-up window.

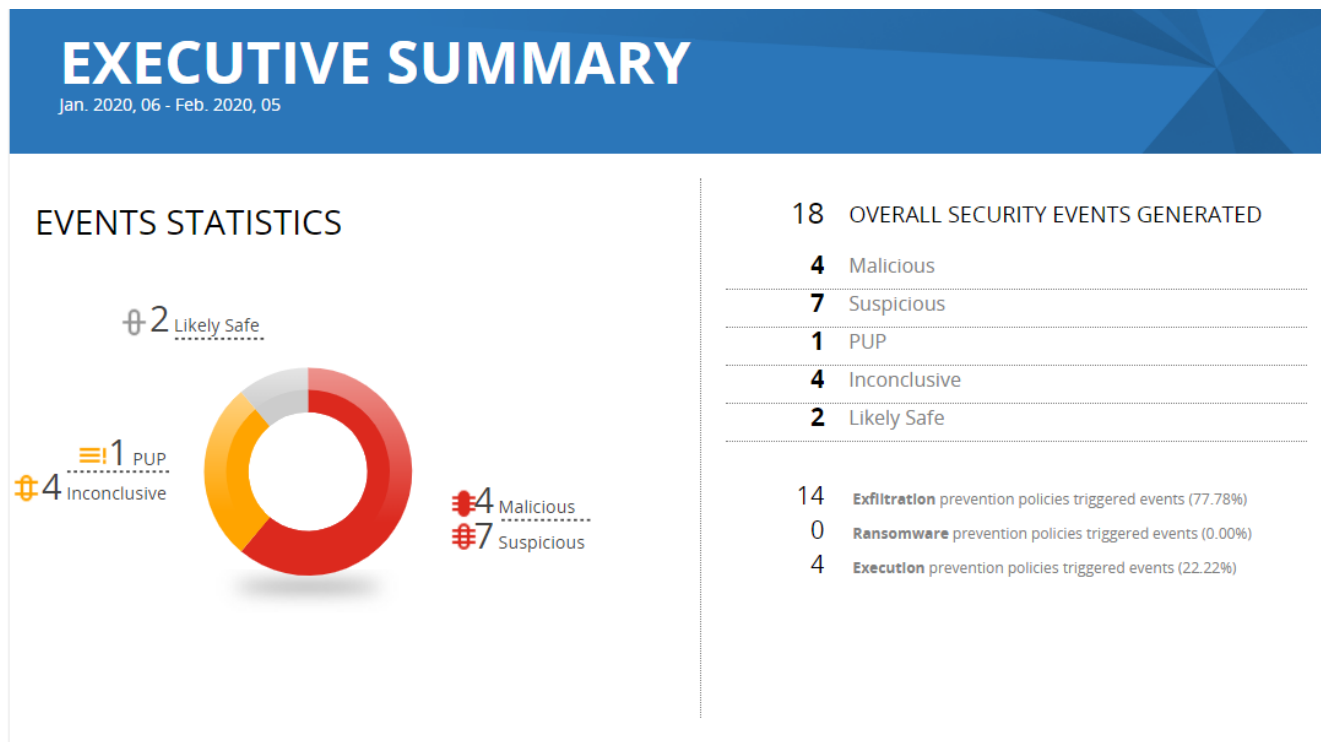


4. 4 Click **Save/Print** to save or print the report.
- The report presents several sections of information, as follows:

- [Event Statistics on page 142](#)
- [Destinations on page 142](#)
- [Most-targeted Devices on page 143](#)
- [Most-targeted Processes on page 143](#)
- [Communication Control on page 144](#)
- [System Components on page 144](#)
- [License Status on page 145](#)

## Event Statistics

The Event Statistics section of the Executive Summary report displays a breakdown of the security events created during the timeframe of the report. Security events are classified by classification. The total number and percentage of events triggered by the Exfiltration and Ransomware policies are also displayed. For more details, see [Event Viewer on page 146](#).



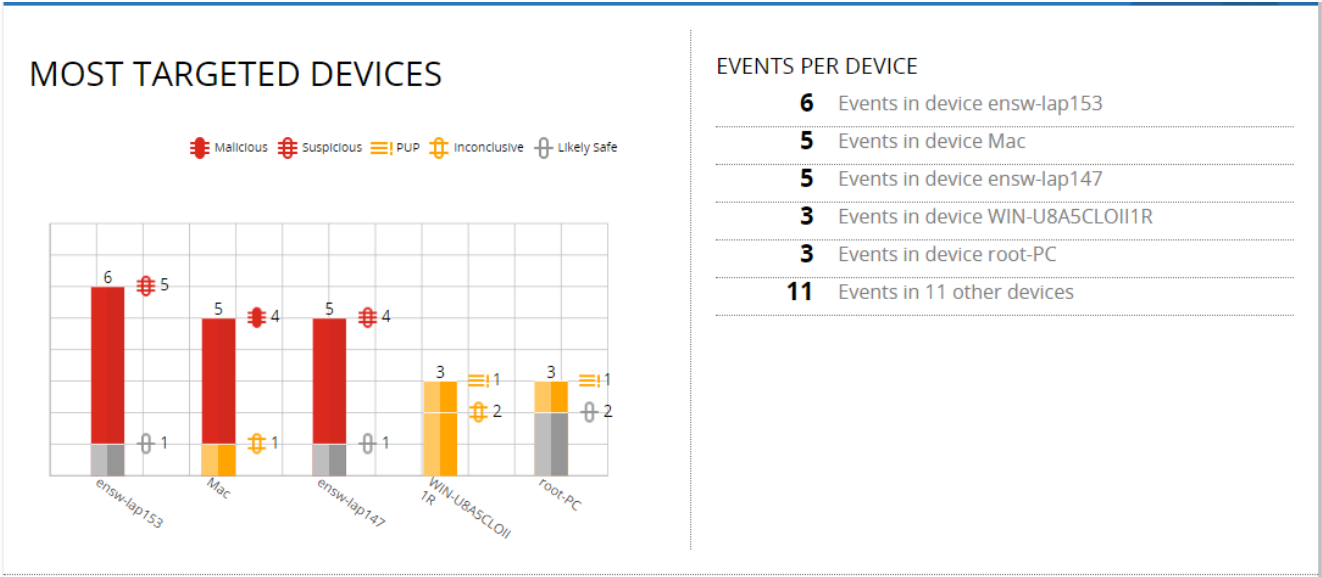
## Destinations

The Destination section of the Executive Summary report displays a map of all the destinations for the security events triggered during the timeframe of the report. The names of the top seven countries with the most security events are shown. There is a pin on the map for each represented country. For more details, see [External Destinations on page 138](#).



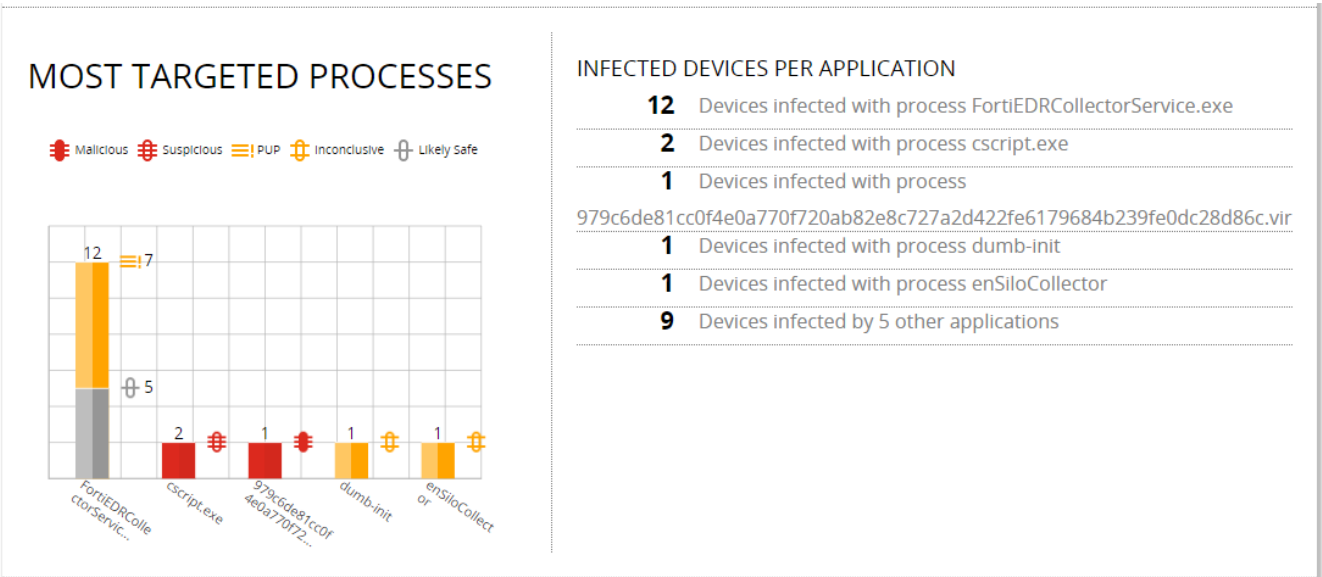
## Most-targeted Devices

The Most Targeted Devices section of the Executive Summary report displays all the security events in the system during the timeframe of the report. A breakdown for the top-five most-targeted devices is shown. For more details, see the [Most Targeted charts on page 138](#).



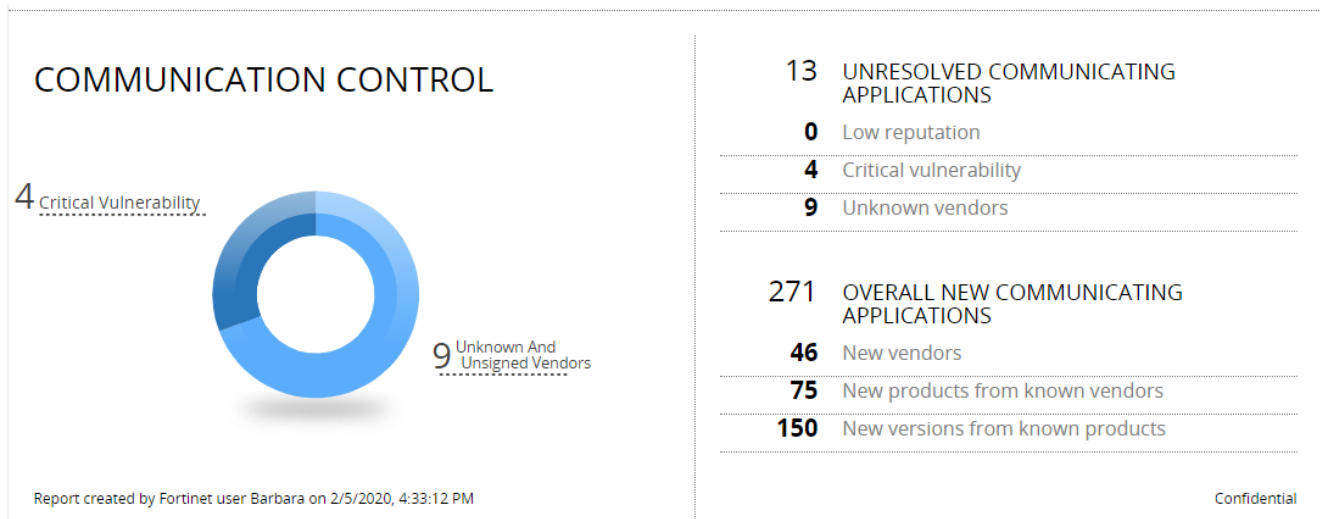
## Most-targeted Processes

The Most Targeted Processes section of the Executive Summary report displays all the security events in the system during the timeframe of the report. A breakdown for the top-five most-targeted processes is shown. For more details, see the [Most Targeted charts on page 138](#).



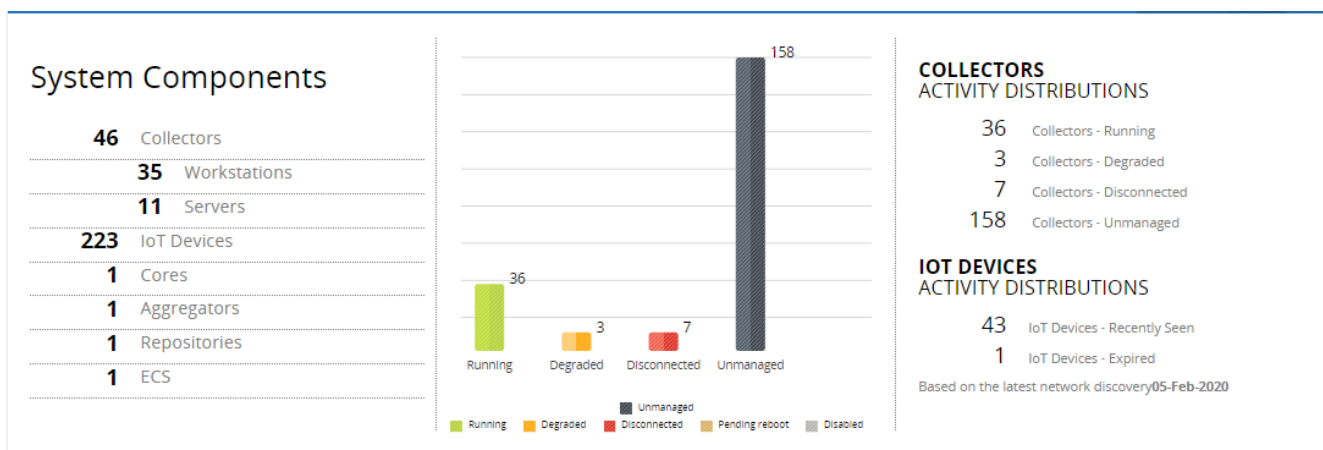
## Communication Control

The Communication Control section of the Executive Summary report displays the number of applications detected for the first time during the timeframe of the report. In addition, it shows how many of these applications have suspicious characteristics, such as low reputation or critical vulnerabilities. For more details, see [Communication control on page 190](#).



## System Components

The System Components section of the Executive Summary report displays a bar chart showing the Collectors in the system by their state. In addition, it shows a breakdown of the components in the system, the number of detected IoT devices and the number of unmanaged devices (non-IoT devices on which no Collector is installed). For more details, see the [FortiEDR components on page 14](#). For more details about IoT devices, see [IoT devices on page 122](#). For more details about unmanaged devices, [Unmanaged devices on page 121](#).





## License Status

The License Status section of the Executive Summary report displays a summary of license-related information. For more details, see [Licensing on page 274](#).

### LICENSE STATUS

License Type:	Discover, Protect and Response
Expiration Date:	12-Aug-2023
Communication Control:	Available
eXtended Detection	Available
Forensics:	Available
Threat Hunting:	Available
Vulnerability Assessment:	Available
Content Updates:	Available
License Capacity:	10 workstations, 10 servers, 10 IoT devices
In Use:	3 workstations, 0 servers, 0 IoT devices
Remaining:	7 workstations, 10 servers, 10 IoT devices

# Event Viewer

This chapter describes the FortiEDR Event Viewer for monitoring and handling security events.

## Introducing the Event Viewer

Upon connection establishment attempt, each FortiEDR Collectors 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 Event Viewer. The Event Viewer enables you to view, investigate, and acknowledge handling of each such security event. A row is displayed for each event.

The Event Viewer enables you to display two different slices or views of the event data collected by FortiEDR:

- **Device View** (🖨️): This view presents information by device, and shows all the security events detected on a given device.
- **Process View** (🔍): This view presents information by process, and shows all the security events detected for a given process.

Click the applicable view button at the top center of the window to display that view.

The screenshot displays the FortiEDR Event Viewer interface. The top navigation bar includes tabs for DASHBOARD, EVENT VIEWER (127), FORENSICS, COMMUNICATION CONTROL (126), SECURITY SETTINGS, INVENTORY (1), and ADMINISTRATION (203). The main content area is divided into two panels. The left panel, titled 'EVENTS', shows a list of events with columns for ID, DEVICE, PROCESS, CLASSIFICATION, DESTINATIONS, RECEIVED, and LAST UPDATED. The right panel, titled 'CLASSIFICATION DETAILS', provides information about the selected event, including the threat name, family, and type, as well as automated analysis steps and triggered rules.

EVENTS	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
pe explorer_1_5540510041.exe (1 event)				PUP		17-Jan-2021, 06:41:00	
4442569 ensow-lap-152		pe explorer_1_554051004...	PUP	File Read Attempt	17-Jan-2021, 06:41:00	17-Jan-2021, 06:41:00	
nanocore.exe (1 event)				Malicious		17-Jan-2021, 06:36:07	
Tbt.exe (1 event)				Likely Safe		17-Jan-2021, 03:50:27	
powershell.exe (2 events)				Inconclusive		15-Jan-2021, 21:57:08	
EvilProcessLauncherTests.exe (1 event)				Likely Safe		15-Jan-2021, 10:32:08	
abe22cf0d78836c3ea072daef4c5eaf9c29b6feb5... (1 event)				Malicious		14-Jan-2021, 08:52:30	
ConnectivityTestApp.exe (1 event)				Malicious		14-Jan-2021, 08:33:30	
traefik (1 event)				Inconclusive		14-Jan-2021, 02:13:00	
utweb_installer.exe (1 event)				PUP		07-Jan-2021, 14:29:41	
SearchApp.exe (1 event)				Safe		06-Jan-2021, 15:43:28	
ViewSecurityDescriptor.exe (1 event)				PUP		06-Jan-2021, 07:13:44	
EditSection.exe (1 event)				PUP		06-Jan-2021, 07:13:41	
ConnectivityTestAppNew.exe (2 events)				Malicious		06-Jan-2021, 04:30:34	
java.exe (1 event)				Likely Safe		05-Jan-2021, 16:33:43	
TeamViewer.Service.exe (1 event)				Safe		05-Jan-2021, 12:14:13	

**CLASSIFICATION DETAILS**

**PUP** **Fortinet**

Threat name: W32/Ekstak.VH0tr  
 Threat family: Unknown  
 Threat type: Unknown

Automated analysis steps completed by Fortinet [Details](#)

**History**

- PUP, by FortinetCloudServices, on 17-Jan-2021, 06:41:05
- Malicious, by Fortinet, on 17-Jan-2021, 06:41:01

**Triggered Rules**

- Execution Prevention
  - Malicious File Detected

**ADVANCED DATA**

Copyright © Fortinet Version 5.0.1.47

System Time (UTC -05:00) 09:06:32




Security events that were triggered by Saved Queries appear slightly different in the Event Viewer, as [Event Viewer on page 146](#)

## Event Aggregation

For convenience and easier navigation, FortiEDR aggregates security events in both the Device view and the Process view in the Event Viewer, as follows:


- Each primary-level row represents a device/process.



<input type="checkbox"/> All	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
<input type="checkbox"/> TeamViewer.exe (1 event)				PUP		10-Feb-2020, 04:47:59	
<input type="checkbox"/> 171302	WIN-MQH0CMRUD2J	TeamViewer.exe	PUP	4 destinations	10-Feb-2020, 04:47:59	11-Feb-2020, 13:49:06	
User: WIN-MQH0CMRUD2Jroot		Certificate: Signed	Process path: C:\Program Files (x86)\TeamViewer\TeamViewer.exe		Raw data items: 4		
<input type="checkbox"/> DynamicCodeTests32.exe (1 event)				Suspicious		06-Feb-2020, 02:39:27	




The All filter also displays expired security events.



- 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.



<input type="checkbox"/> All	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
<input type="checkbox"/> TeamViewer.exe (1 event)				PUP		10-Feb-2020, 04:47:59	
<input type="checkbox"/> 171302	WIN-MQH0CMRUD2J	TeamViewer.exe	PUP	4 destinations	10-Feb-2020, 04:47:59	11-Feb-2020, 13:49:06	
User: WIN-MQH0CMRUD2Jroot		Certificate: Signed	Process path: C:\Program Files (x86)\TeamViewer\TeamViewer.exe		Raw data items: 4		
<input type="checkbox"/> DynamicCodeTests32.exe (1 event)				Suspicious		06-Feb-2020, 02:39:27	

- 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  icon to return to the aggregated security event view.

<input type="checkbox"/> traefik (1 event)				Inconclusive		14-Jan-2021, 02:13:00	
<input type="checkbox"/> 4429238	nginx.webserver	traefik	Inconclusive	2 destinations	14-Jan-2021, 02:13:00	17-Jan-2021, 02:12:59	
Process owner: None		Certificate: Unsigned	Process path: /traefik		Raw data items: 2		

< Back	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED	ACTION
	4429238	nginx.webserver	traefik	Inconclusive	2 destinations	14-Jan-2021, 02:13:00	17-Jan-2021, 02:12:59	
Process owner: None		Certificate: Unsigned	Process path: /traefik		Raw data items: 2			
	RAW ID	DEVICE	PROCESS OWNER	DESTINATION	FIRST SEEN	LAST SEEN	USERS	COUNT
<input type="checkbox"/>	1802503228	nginx.webserver		104.26.3.101	16-Jan-2021, 02:12:59	17-Jan-2021, 02:12:59		6
<input type="checkbox"/>	1802238279	nginx.webserver		165.227.206.205	14-Jan-2021, 02:13:00	14-Jan-2021, 02:13:00		1



Examine the data in both the Device view and the Process view to identify the source of a problem. In this way, you can determine whether the issue is organization-wide or if only specific devices are infected.

---

A security event is triggered when one or more rules in a policy are violated. For example, let's assume that people in your organization using the Adobe PDF application modified this application to meet their individual needs, and that FortiEDR detected this as malware that appeared on 1,000 devices in the organization. In this case, when the same security event occurs on multiple devices for the same process, you see the following in the Event Viewer:

- In the Device view, you see 1,000 aggregation security events, each with one security event under it.
- In the Process view, you see one security event aggregation named `adobe.exe`. Under it, there is one security event for the `adobe.exe` process. That security event shows the number 1000 in the *Devices* column and 1,000 raw data items.

The Event Viewer is divided into the following areas of information:

- [Events pane on page 150](#)
- [Advanced Data on page 154](#)
- [Classification Details on page 183](#)
















The following actions can be performed in the Event Viewer:

- [Marking a security event as handled/unhandled on page 156](#)
- [Manually changing the classification of a security event on page 158](#)
- [Marking a security event as read/unread on page 177](#)
- [Viewing relevant activity events on page 177](#)
- [Viewing expired security events on page 177](#)
- [Viewing Application Control security events on page 178](#)
- [Viewing Device Control security events on page 179](#)
- [Other options in the Event Viewer on page 180](#)

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, shown below:

## EVENT VIEWER 22

ID	CLASSIFICATION	TIME
170199	 Inconclusive	10-Feb-2020, 09:40:27
145884	 Inconclusive	10-Feb-2020, 05:05:53
163078	 Safe	10-Feb-2020, 04:15:27
145722	 Suspicious	09-Feb-2020, 15:08:48
149594	 Suspicious	09-Feb-2020, 15:08:47
145698	 Suspicious	09-Feb-2020, 15:08:46
145686	 Suspicious	09-Feb-2020, 15:08:44
170174	 Inconclusive	09-Feb-2020, 03:18:34
170192	 Inconclusive	09-Feb-2020, 03:18:32
170183	 Inconclusive	09-Feb-2020, 03:18:32
145793	 Inconclusive	06-Feb-2020, 13:37:46
166692	 Inconclusive	06-Feb-2020, 03:34:47
166577	 Suspicious	06-Feb-2020, 02:54:29
152984	 Likely Safe	04-Feb-2020, 10:52:04
152854	 Inconclusive	03-Feb-2020, 04:27:01

[7 More 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.

## Events 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:

EVENTS							
<div> <span>Archive</span> <span>Mark As...</span> <span>Export</span> <span>Handle Event</span> <span>Delete</span> <span>Forensics</span> <span>Exception Manager</span> </div> <div> <span>Showing 1-17/71</span> <input type="text" value="Search Event"/> </div>							
<input type="checkbox"/>	All	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED
<input type="checkbox"/>	ensw-lap-152 (31 events)				Malicious		17-Jan-2021, 06:41:00
<input type="checkbox"/>	ensw-lap149 (1 event)				Likely Safe		17-Jan-2021, 03:50:27
<input type="checkbox"/>	EUGENE-PC (1 event)				Malicious		15-Jan-2021, 21:57:08
<input type="checkbox"/>	ENSW-LAP119 (1 event)				Malicious		15-Jan-2021, 10:32:08
<input type="checkbox"/>	TT-collector1 (1 event)				Malicious		14-Jan-2021, 08:52:30
<input type="checkbox"/>	Einat-PC (2 events)				Malicious		14-Jan-2021, 08:33:30
<input type="checkbox"/>	nginx.webserver (1 event)				Inconclusive		14-Jan-2021, 02:13:00
<input type="checkbox"/>	ensw-lap167 (2 events)				Malicious		06-Jan-2021, 15:43:28
<input type="checkbox"/>	DESKTOP-FI4MQHB (3 events)				Suspicious		06-Jan-2021, 07:13:44
<input type="checkbox"/>	4371806	DESKTOP-FI4MQHB	ViewSecurityDescriptor.e...	PUP	File Read Attempt	06-Jan-2021, 07:13:44	07-Jan-2021, 07:04:32
	Process owner: None	Certificate: Unsigned	Process path: C:\Program Files\WindowsPowerShell\Modules\NtObjectManager\1.1.28\ViewSecurityDescriptor.exe	Raw data items: 2			
<input type="checkbox"/>	4371796	DESKTOP-FI4MQHB	EditSection.exe	PUP	File Read Atte...	06-Jan-2021, 07:13:41	07-Jan-2021, 07:04:32
<input type="checkbox"/>	4366590	DESKTOP-FI4MQHB	ba60efe2e939da16e3d2...	Suspicious	File Execution ...	05-Jan-2021, 08:34:29	05-Jan-2021, 08:34:29

Device View



















EVENTS							
<div>  Archive            Mark As...            Export            Handle Event            Delete            Forensics            Exception Manager         </div>							
<input type="checkbox"/> All	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
<input type="checkbox"/>	pe explorer 1_5540510041.exe (1 event)			PUP		17-Jan-2021, 06:41:00	
<input type="checkbox"/>	nanocore.exe (1 event)			Malicious		17-Jan-2021, 06:36:07	
<input type="checkbox"/>	Tbt.exe (1 event)			Likely Safe		17-Jan-2021, 03:50:27	
<input type="checkbox"/>	powershell.exe (2 events)			Inconclusive		15-Jan-2021, 21:57:08	
<input type="checkbox"/>	4438976	EUGENE-PC	\$Res	Inconclusive	File Access	15-Jan-2021, 21:57:08	15-Jan-2021, 21:57:08
<div> <div>  Logged-in User:           <div></div> </div> <div>  Process owner:           Local System         </div> <div>  Certificate:           Signed         </div> <div>  Process path:           C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe         </div> <div>  Raw data items:           1         </div> </div>							
<input type="checkbox"/>	4346626	ensw-pc179	DisableUnusedSmb1.ps1	Safe	File Service Acc...	03-Jan-2021, 07:15:08	04-Jan-2021, 09:55:37
<input type="checkbox"/>	EvilProcessLauncherTests.exe (1 event)			Likely Safe		15-Jan-2021, 10:32:08	
<input type="checkbox"/>	abe22cf0d78836c3ea072daef4c5eeaf9c29b6feb5... (1 event)			Malicious		14-Jan-2021, 08:52:30	
<input type="checkbox"/>	ConnectivityTestApp.exe (1 event)			Malicious		14-Jan-2021, 08:33:30	
<input type="checkbox"/>	traefik (1 event)			Inconclusive		14-Jan-2021, 02:13:00	
<input type="checkbox"/>	utweb_installer.exe (1 event)			PUP		07-Jan-2021, 14:29:41	
<input type="checkbox"/>	SearchApp.exe (1 event)			Safe		06-Jan-2021, 15:43:28	
<input type="checkbox"/>	ViewSecurityDescriptor.exe (1 event)			PUP		06-Jan-2021, 07:13:44	

Process View






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


Information Field	Description
View Indicator	Indicates the view context for the security event aggregation.  displays for a device and  displays for a process.
Handled/Not Handled	Specifies whether any FortiEDR Central Manager user handled this security event, as described on <a href="#">Marking a security event as handled/unhandled on page 156</a>
ID	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.
Device	Specifies the device name on which the security event has occurred.
Process	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.

Information Field	Description																												
Classification	<p>Specifies how malicious the security event is, if at all. Classifications are initially determined by FortiEDR. They can be changed either automatically as the result of additional post-processing, deep, thorough analysis and investigation by the <a href="#">FortiEDR Cloud Service (FCS)</a> or manually. See <a href="#">Classification Details on page 183</a> for more detailed information about the classification of the event, such as the classification history. Classifications are as follows:</p> <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:<ul style="list-style-type: none"><li>• Verified to have malicious capability</li><li>• Intended to harm the infected device</li><li>• Have no commercially viable use</li></ul></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 if the event is malicious.</td><td>Administrator review</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>	Icon	Classification	Definition	Recommended Action		Malicious	Events with the following characteristics: <ul style="list-style-type: none"><li>• Verified to have malicious capability</li><li>• Intended to harm the infected device</li><li>• Have no commercially viable use</li></ul>	Remediate		Suspicious	Events that behave in ways that strongly indicate malware, but are not verified malware.	Review and remediate		Inconclusive	Further investigation needed to determine if the event is malicious.	Administrator review		PUP (Potentially Unwanted Program)	Events triggered by programs that are bundled with legitimate software or commercial software that may be used for malicious purposes, for example, torrents.	Administrator to review whether the program should be removed (recommended) or allowed		Likely Safe	Events that probably carry no risk, and are most likely legitimate.	Administrator review		Safe (Confirmed Safe Software)	Events triggered by legitimate software that was intended for use by the customer, for example, security software.	No action necessary
Icon	Classification	Definition	Recommended Action																										
	Malicious	Events with the following characteristics: <ul style="list-style-type: none"><li>• Verified to have malicious capability</li><li>• Intended to harm the infected device</li><li>• Have no commercially viable use</li></ul>	Remediate																										
	Suspicious	Events that behave in ways that strongly indicate malware, but are not verified malware.	Review and remediate																										
	Inconclusive	Further investigation needed to determine if the event is malicious.	Administrator review																										
	PUP (Potentially Unwanted Program)	Events triggered by programs that are bundled with legitimate software or commercial software that may be used for malicious purposes, for example, torrents.	Administrator to review whether the program should be removed (recommended) or allowed																										
	Likely Safe	Events that probably carry no risk, and are most likely legitimate.	Administrator review																										
	Safe (Confirmed Safe Software)	Events triggered by legitimate software that was intended for use by the customer, for example, security software.	No action necessary																										



Information Field	Description
Destinations	Specifies the IP address to which the malicious entity requested to establish a connection.
Received	Specifies the first time that this security event was triggered. For aggregations, the earliest received time is displayed.
Last Updated	Specifies the last time that the security event was triggered. For aggregations, the most-recent time is displayed.
Action	<p>Specifies the action that was enforced:</p> <ul style="list-style-type: none"> <li>• <i>Block</i>  : The exfiltration attempt was blocked and this blocking event was generated.</li> <li>• <i>Simulated Block</i>  : 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.</li> <li>• <i>Log</i>  . The security event was only logged and was not blocked.</li> </ul>

For raw data items, the following information is available:

Information	Description
Device	Specifies the device name on which the security event has occurred.
First Seen	<p>The Event Viewer 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 Event Viewer each time it occurs again.</p> <hr/> <div>  <p>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.</p> </div> <hr/>
Last Seen	Specifies the most recent time this same security event occurred. See FIRST SEEN described above.
Destinations	Specifies the external address for connection attempt security events.
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.
Certificate	Specifies whether the process or application have a certificate – <b>Signed</b> or <b>Unsigned</b> . You may refer to <a href="http://en.wikipedia.org/wiki/Authorization_certificate">http://en.wikipedia.org/wiki/Authorization_certificate</a> for general information about the subject.

Information	Description
Process Path	Specifies the path of the infected process.
Count	Specifies the number of occurrences of the same raw event on the same device.

## Advanced Data

The *ADVANCED DATA* area displays a graphic representation of what occurred that led to the security event. This information shows operating system metadata that occurred immediately preceding and at the time the connection establishment request was issued.

The *ADVANCED DATA* area contains three tabs.

- [Event Graph on page 154](#)
- [Geo Location on page 155](#)
- [Automated Analysis on page 155](#)



The events graph tabs are always available. The other two tabs may be missing when there is no data available for the security event.

## Event Graph

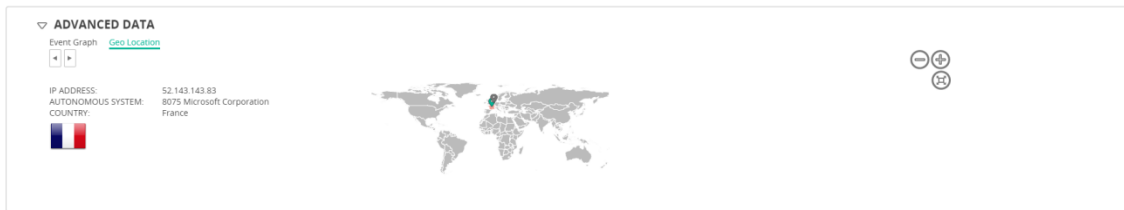
In addition to textual information that is displayed (described above), the *Event Graph* tab provides an image depicting the flow of operating system events that led up to the connection establishment request or the attempt to lock data. The picture is shown as a timeline from left to right (meaning that the left process happened before the others). A circle can represent an operating system entity such as a process, a thread, a service, a file and so on. The white boxes represent the operation that was done between the operating system entities, such as create, open, inject, connect and so on. Typically, the last circle (rightmost) is a connection establishment request or a file access. Each white box has a number attached to it, representing the sequence of operations, and also the rules that were violated during that operation, along with the worst classification associated with that operation.



You can zoom in and zoom out using the buttons at the top right. The button fits the picture to the size of the window.

## Geo Location

The *Geo Location* tab displays a world map showing the locations of the destinations of the security event and indicating the country by its flag.



An abundance of additional investigative tools and information are provided by FortiEDR's [Introduction on page 219](#).

You can zoom in and zoom out using the buttons at the top right. The button fits the picture to the size of the window.

## Automated Analysis

The *Automated Analysis* tab provides additional information about the investigation done automatically on Fortinet Cloud Services (FCS) per the security event to help you understand FortiEDR's rationale when classifying an item with a specific classification.



The classification history of a security event is presented in the [Classification Details on page 183](#) area and shows the chronology for classifying a security event, as well as the automatic investigation and remediation actions performed by FortiEDR for that event.

The information shown in the *Automated Analysis* tab supplements this analysis, providing even more information about how and why a given security event was classified as it was. This tab shows the actions that were performed for the analysis plus a categorized summary of what was analyzed. For example, the analyzed files, memory segments, the IP address involved in the communication, the email address associated with the security event and so on. A Fortinet Cloud Services comment is available at the top of this area that summarizes the analysis verdict and conclusion in text.

For example, the following shows a security event that was initially classified as *Inconclusive* by FortiEDR Core, but after FCS automatic analysis was reclassified as *Malicious*. In this case, four files were analyzed. You can click the name of the file to display more details about it, including its metadata along with several properties of the file (signature, certificate, hash and so on).

You can click the down arrow next to an item to view all the investigation actions performed and analysis results related to that item.

▼ ADVANCED DATA

Event Graph Automated Analysis Geo Location

**Inconclusive** Fortinet on 10-May-2020, 06:09:56 → **Malicious** FortinetCloudServices on 10-May-2020, 06:09:56

Fortinet Cloud Services comment  
Machine was compromised by FIN7 Group. More devices suspected to be infected

Export

File (4)

▼ WinBio.dll

SHA-256 2A3539C44A00EA3B3E80084219788B3C112B295E [More](#)

Hash reputation Unknown by FortiLab and ReversingLabs intelligence services

Sandbox execution Malicious activity by FortiSandbox and Isotime

File execution Winio.dll leverages DLL search order hijacking

File usage 10 devices out of 5343

Memory (2)

▼ Memory Address

YARA IOC scan FIN7 credential scraper

In-memory signature Unknown

In-memory signature usage 3 devices

▶ Memory Address 2

Network & Extended Data (3)

▼ 52.168.20.22

IP reputation Known Good by FortiLab intelligence services

Firewall Details 20 connections

▶ IP 2

▶ Email Address



## 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 event* button or just click the flag icon of the security event row. The *Event Handling* window displays.



If an exception was already defined for this security event, then the words event includes exceptions are displayed at the top of the *Event 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 158](#).
3. In the comments box, use free text to describe how you handled the security event.
4. Click the *Save as Handled* button. The flag icon next to the security event changes from dark gray  to light gray  to indicate to all users that it has been handled.

**EVENT HANDLING**

Unhandled event **163078**  
for device **WIN-MQH0CMRUD2J**

Classification: Safe

Type comment

☐ Archive When Handled

Advanced

Save and Handled Save Cancel

5. (Optional) Check the *Archive When Handled* checkbox to archive the security event after handling it. When you select this option, the security event is marked both as handled and as archived.
6. (Optional) Click the arrow to the left of *Advanced* to display the *Mute events notification* field. Select this checkbox if you want to mute the notifications for this security event. In addition, specify how long to mute the security event notifications. Notifications can be muted for any of the following periods: *1 Week*, *1 Month*, *1 Year*, or *Permanently*. When checked, you will not receive notifications whenever this security event is triggered. When using this option, click the *Save as Handled* button, which indicates that the security event has been both handled and saved.

☐ Archive When Handled

▼ Advanced

☐ Mute Event Notifications (🔔) for 1 week ?

Save and Handled

Save

Cancel



Security events with muted event notifications are indicated by the 🔔 icon in the *Event Viewer*.

## 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 event* button or just click the flag icon of the security event row. The *EVENT HANDLING* window displays.

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

**EVENT HANDLING**

Unhandled event **163078**  
for device **WIN-MQH0CMRUD2J**

Classification: Safe ▼

Type comment

Malicious

PUP

Safe **FORTINET**

☐ Archive When Handled

► Advanced

Save and Handled Save Cancel

3. Click *Save*.
4. (Optional) Click *Save and Handled* to mark the security event as handled after saving the event.
5. (Optional) Once the event is handled, it is advised to archive the event. To do so, click the *Archive* button in the actions area. See [Introducing communication control on page 191](#).

After changing the classification of a security event, the *CLASSIFICATION DETAILS* pane displays the history of any actions (Playbook policy-related actions and others) that were made automatically by FortiEDR, as shown below. 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 101](#).

The screenshot displays the FortiEDR Event Viewer interface. The top navigation bar includes tabs for DASHBOARD, EVENT VIEWER (active), FORENSICS, COMMUNICATION CONTROL, SECURITY SETTINGS, INVENTORY, and ADMINISTRATION. The main area is divided into three panes. The left pane, titled 'EVENTS', shows a table of security events with columns: ID, DEVICE, PROCESS, CLASSIFICATION, DESTINATIONS, RECEIVED, and LAST UPDATED. The middle pane, titled 'CLASSIFICATION DETAILS', provides information about the selected event, including the threat name, threat family, threat type, and a history of actions. The right pane, titled 'ADVANCED DATA', shows event graph and geo location information, including IP address, autonomous system, and a world map.

When the Fortinet logo appears next to an entry in the *CLASSIFICATION DETAILS* 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 *CLASSIFICATION DETAILS* 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 175](#). You can access the Exception Manager by clicking the *Exception Manager* button at the top of the *Events* 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 75](#).


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 101](#).



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.

EVENTS								
<div> <span>Archive</span> <span>Mark As...</span> <span>Export</span> <span>Handle Event</span> <span>Delete</span> <span>Forensics</span> <span>Exception Manager</span> </div>								
< Back	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED	ACTION
	49858	3 devices	DTLite4491-0356.exe	Malicious	File Read Attempt	05-Oct-2020, 13:51:46	06-Oct-2020, 07:43:24	
Process owner: None		Certificate: Signed		Process path: C:\Users\Administrator\Desktop\install\Programs\DTLite4491-0356.exe		Raw data items: 3		
<input type="checkbox"/>	RAW ID	DEVICE	PROCESS OWNER	DESTINATION	FIRST SEEN	LAST SEEN	USERS	COUNT
<input type="checkbox"/>		805273434	malr-win10x64-bet...	File Read Attempt	06-Oct-2020, 07:43:24	06-Oct-2020, 07:43:24		1
<input type="checkbox"/>		687601117	Panda1	File Read Attempt	05-Oct-2020, 18:19:38	05-Oct-2020, 18:19:38		1
<input type="checkbox"/>		12970979	WIN-7VTV943PA85	File Read Attempt	05-Oct-2020, 13:51:46	05-Oct-2020, 13:51:46		1

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

Exception 1    Exception 2    +

---

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

Collector groups

☐   
☒ All groups    ☐ All organizations

Destinations

☐   
☒ All destinations

Users


☐   
☒ All users

Triggered Rules:

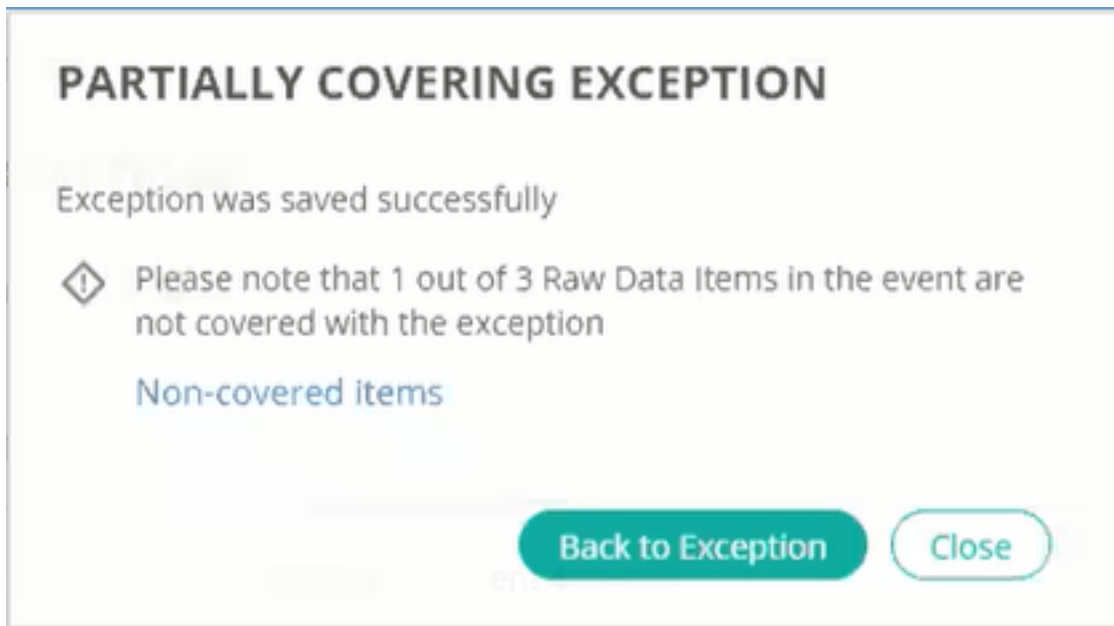
▶ Malicious File Detected ⋮

Type comments

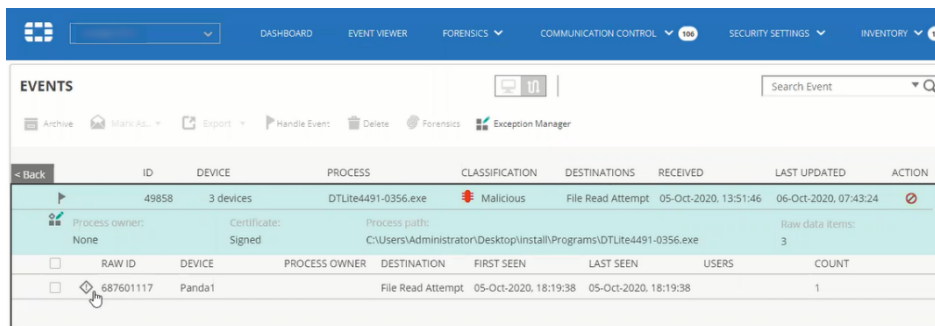
---

 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.

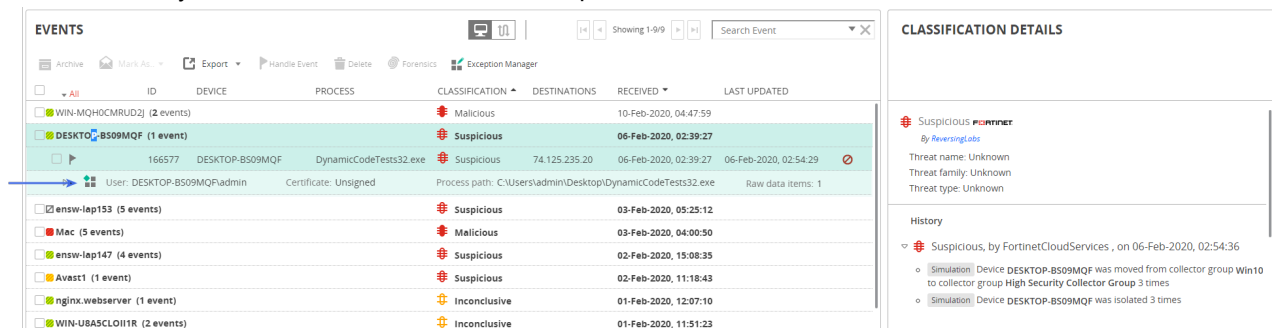


You can click the *Non-covered items* link in this message to open the Event Viewer in a new window, and display only not-covered raw data items, as shown below:

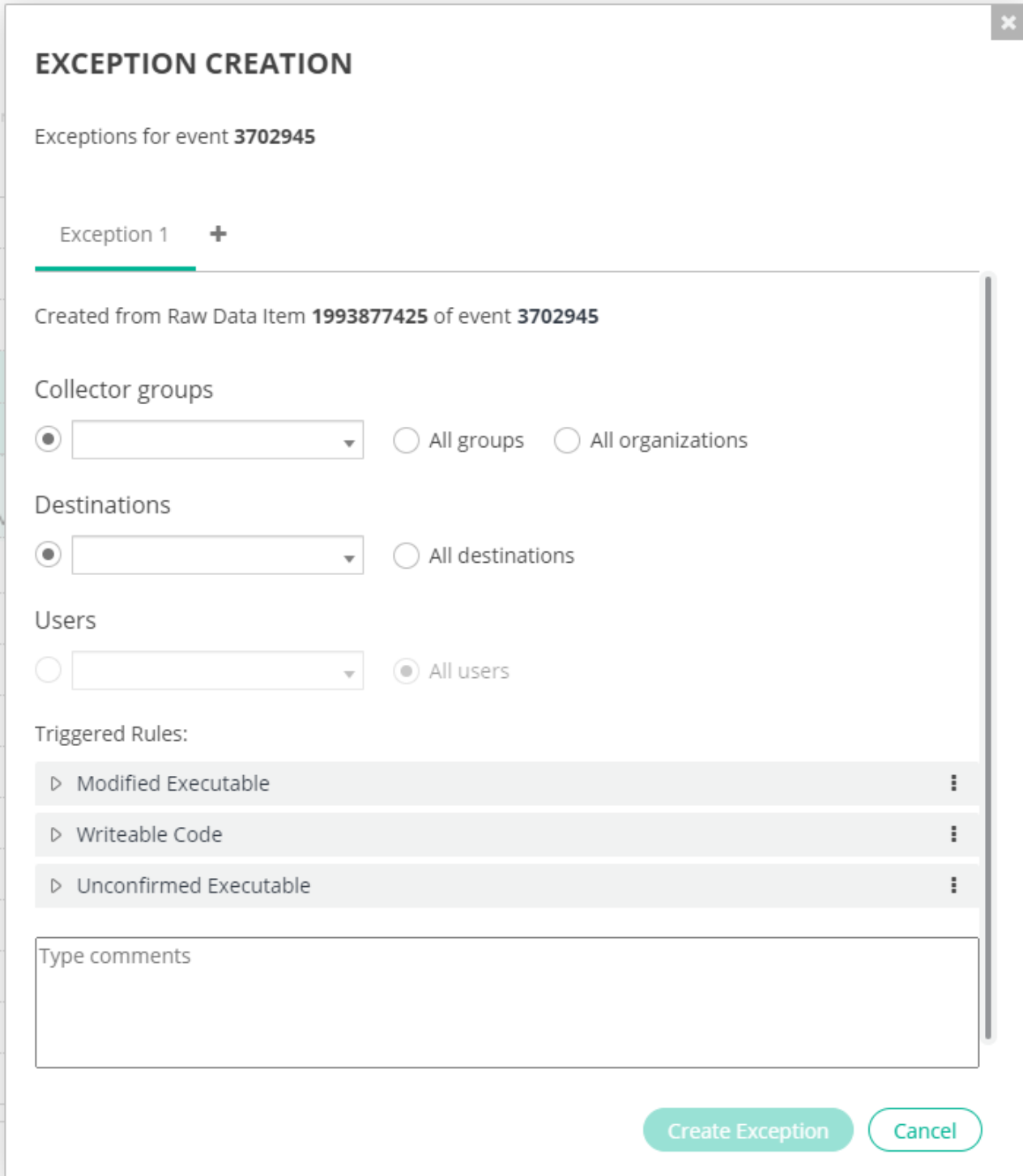


## Defining a security event as an exception

1. Click the security event row to be defined as an exception.



2. Click the *Create Exception*  button. The following window displays:



**EXCEPTION CREATION**

Exceptions for event **3702945**

Exception 1 +

Created from Raw Data Item **1993877425** of event **3702945**

**Collector groups**

☒  ☐ All groups ☐ All organizations

**Destinations**

☒  ☐ All destinations

**Users**

☐  ☒ All users

**Triggered Rules:**

- ▷ Modified Executable ⋮
- ▷ Writeable Code ⋮
- ▷ Unconfirmed Executable ⋮

Type comments

Create Exception Cancel

3. Specify whether this exception applies to all the Collector Groups or only to the Collectors in the same Collector Group as the one for which this security event was triggered.



The *All groups* and *Collector groups* options only apply to the current organization in which the security event occurred.

---

For a [multi-organization FortiEDR system](#), an Administrator who is assigned to *All organizations* (see [Users on page 398](#)) 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.

---



The *All organizations* option is available only for Admins assigned to *All organizations*. Admins not assigned to *All organizations* or other non-admin roles cannot set the *All organizations* option.

---

If an Administrator wants to define an exception that applies to one or more, but not all organizations, then he/she must define the exception separately for each organization.

Exceptions defined by an Administrator (Hoster) that apply to all organizations display as *Locked by the administrator* to other users, and cannot be changed by a user other than the Administrator who created it, as shown below:

×

## EVENT EXCEPTIONS


Exceptions for event **3702945**

Last updated at 27-Oct-2020, 10:09 By Einat

Exception 1

---

Created from event **3702945**

 Locked by administrator

Collector groups

☐

☒ All groups

Destinations

☐

☒ All destinations

Users

☐

☒ All users

Triggered Rules:

- ▷ Modified Executable ⋮
- ▷ Writeable Code ⋮
- ▷ Unconfirmed Executable ⋮

Type comments



Exceptions can only be defined for Collector Groups. If you would like to define an exception for a specific Collector, then create a Collector Group that only contains that Collector.

4. Specify whether this exception applies to all Destinations or only to specific destinations. The IP addresses listed in the dropdown menu are those IP addresses that generated connections for this security event. Use the dropdown menu to select the specific IP addresses to exclude that were triggered on this security event, which can be either internal or external.

☒ Destinations:
 ☐ All destinations

Select All

74.125.235.20

Internal Destinations

default set

global set

/ exception on:

To apply the exception to a specific destination(s), select from the following options:

Option	Description
Select All	Applies the exception on all destinations that were seen as part of this security event. If there will be an identical violation (the same set of rules will be violated on this process) but the connection attempt will be to a different IP, than the security event will be triggered. To exclude this security event completely from being triggered in the future you can select the <i>All Destinations</i> radio button.
Internal Destinations	<p>Applies the exception on all internal destinations. Internal destinations are internal IP addresses that are defined in TCP/IP standard definitions for internal networks. These IP addresses include the following:</p> <ul style="list-style-type: none"> <li>• Loopback addresses: 127.X.X.X, 0:0:0:0:0:0:1 and 0:0:0:0:0:0:FFFF:7f</li> <li>• 10.0.0.0–10.255.255.255</li> <li>• 192.168.0.0–192.168.255.255</li> <li>• 169.254.0.0–169.254.255.255</li> <li>• 172.16.0.0 - 172.31.255.255</li> <li>• IPV6: fc00:: – fd00:: :: or fe80</li> </ul> <p>This option is useful when an application is allowed for use within the organization, but you do not want it to be used for external communications. Using this option enables the application to communicate internally without triggering alerts. However, the application might still trigger alerts when attempting to connect to an external IP.</p>
<IP Address>	Applies the exception to the selected IP address. You can select multiple IP addresses.



Option	Description
<input checked="" type="radio"/> Destinations: <input type="radio"/> All destinations	<div> <div>All Internal destinations, 5.4...</div> <div>Select All</div> <div>✓ All Internal destinations</div> <div>192.168.153.128</div> <div>✓ 5.45.179.173</div> <div>95.215.45.94</div> </div>

&lt;IP Set&gt;

An IP set defines a set of IP addresses to be included or excluded from a security event. When you select an IP set here, it means that an exception is applied only to a device that has one of the IP addresses specified in the IP set. IP sets can only be defined by an Administrator, as described in [IP sets on page 334](#).

☒ Destinations:
 ☐ All destinations

Select All

74.125.235.20

Internal Destinations

default set

global set

exception on:

5. Specify whether this exception applies to all users or to a specific user.

Users

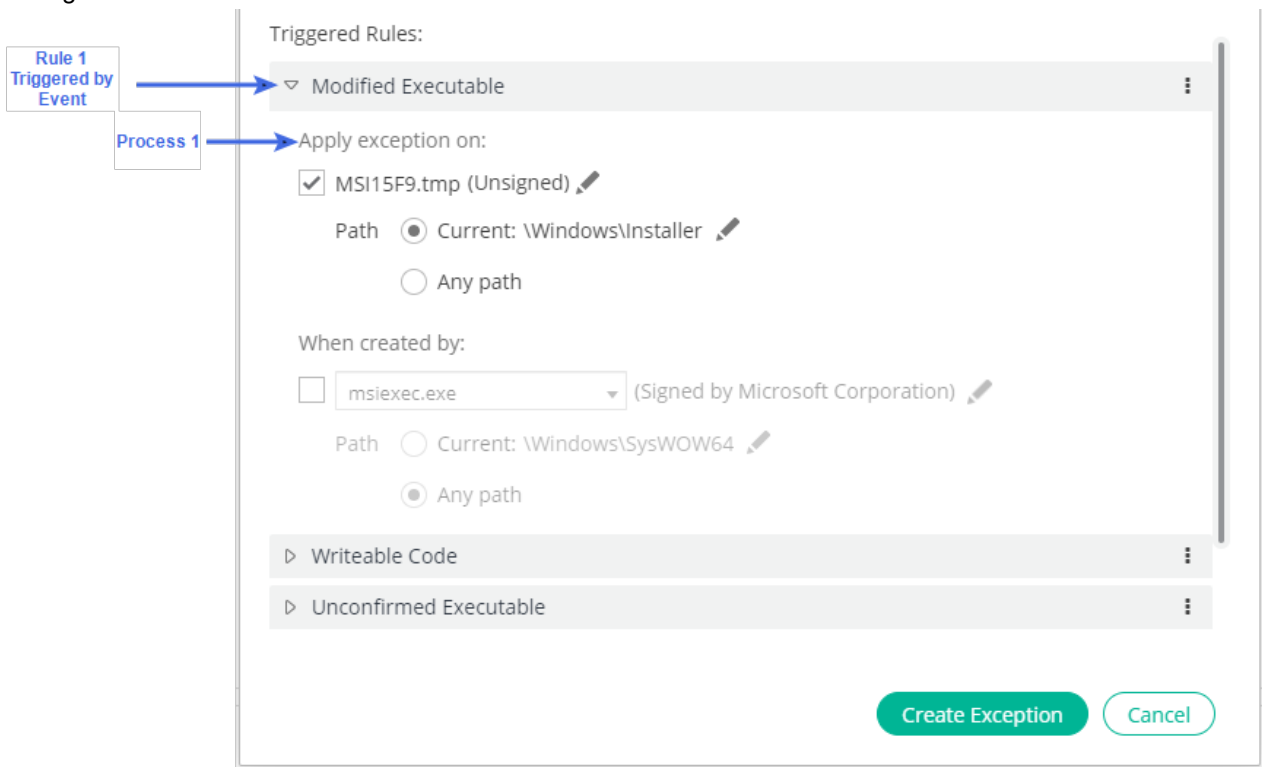
☒
☐ All users

Select All

ENSILO\lor

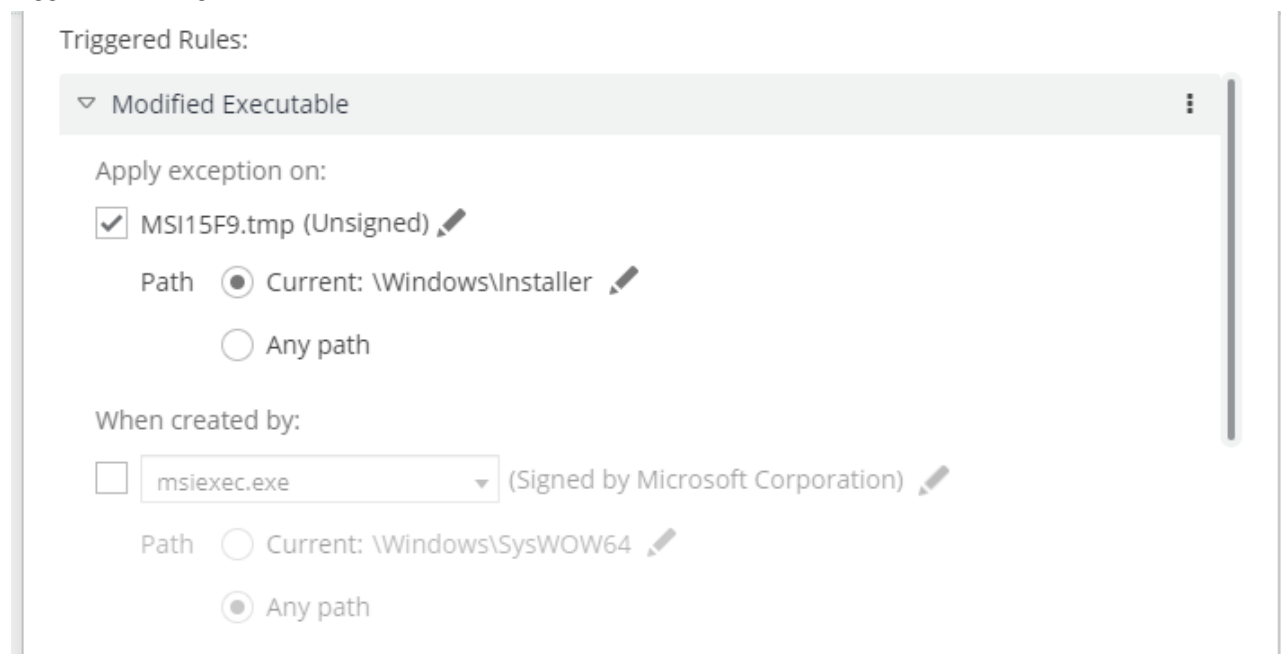
6. In the *Triggered Rules* area, specify the path on which to apply the exception. You can select either the *Current Path* or *Any Path*. By default, all options are set to *Any Path*. In this context, the path indicates the entire path of the [folder name] in which the process's file is located. The *Current Path* is the path used in this security event, as displayed in the window. When you select *Any Path*, the process triggers the exception no matter from where it is

running.




You can define an exception so that a security event is triggered, based on a complex set of conditions. For example, you can define an exception so that a security event is triggered when a specific process (B) is executed by another process (A). For example, you can limit an exception so that it applies only when process B is executed by process A, or every time that process B is executed.

You can also define an exception that specifies that an exception is triggered only when one of the two process triggers is running, as shown below:




You can also define an exception specifying that it is triggered only when both processes are running.

You can click the Help  button to view relevant help information, as shown below:


Triggered Rules:

▼ Modified Executable

Apply exception on:

☒ MSI15F9.tmp (Unsigned) 

Path

☒ Current: \Windows\Installer 

☐ Any path

1. Only \* operand can be used

2. The pattern should match the original value

FortiEDR enables you any to specify any of the processes in a security event's stack when defining an exception.

Let's look at an example in more detail. Let's say that you want to define an exception that allows the `SurSvc.exe` executable to run, but only when it is created from the `services.exe` executable. Therefore, in order to define this exception, you would select the `SurSvc.exe` process in the *Apply exception* field and select the `services.exe` process in the *When created by* field. Based on this security event's ancestry chain, `wininit.exe`, which is the grandparent of the `SurSvc.exe` executable, would not be selected in the *When created by* field.

The immediate parent of the `SurSvc.exe` executable is `services.exe` and that it is therefore listed at the top of the *When created by* field dropdown list and that the `SurSvc.exe` executable's grandparent is `wininit.exe`, which is listed at the bottom of the list. The order in which the processes run in a security event chain is always maintained. This means that the oldest ancestor is shown at the bottom of the list of processes in this window and the immediate parent is at the top.

ADVANCED DATA

Event Graph Automated Analysis

```

graph LR
    A[Process wininit.exe] -- "1 Create" --> B[Process services.exe]
    B -- "2 Create" --> C[Process SurSvc.exe]
    C -- "3 Delete File Encryptor" --> D[Block Fortinet]
    D -.-> E[w_erron_stack-000002-000037 tx]
  
```

FortiEDR 5.2.1 Administration Guide  
Fortinet Inc.

171

**EXCEPTION CREATION**

Exceptions for event **53103**

Exception 1 +

☐  ☒ All users

Triggered Rules:

▼ File Encryptor

Apply exception on:

☒ SurSvc.exe (Signed)

Path ☐ Current: \Program Files\Intel\SUR\QUEENCREEK

☒ Any path

When created by:

☒ services.exe (Signed by Microsoft Corporation)

☒ services.exe System32

wininit.exe

Type comments

**Create Exception** Cancel

You can edit the process path and file name. Wildcards can be used for this purpose.


To use wildcards as part of a process path or file name definition, all Collectors must be V3.0.0.0 or above. If you attempt to use wildcards with older Collectors, the following error message displays:






## ERROR

Using Wildcards in exceptions is not supported since there are still Windows Collectors with version older than 3.0.0.0. Please upgrade your environment.

Continue

You can only edit the process path or file name when selecting the *Current Path* option. To do so, click the adjacent *Edit*  button, and then edit the process/file name as needed. When doing so, the following conditions apply:

Field	Condition
Path	<ul style="list-style-type: none"> <li>Only an asterisk (*) character(s) can be added.</li> <li>Do not change the displayed path. Otherwise, it will no longer match. However, you can replace a piece of the string with an asterisk (*).</li> <li>Only a single asterisk character (*) is permitted between two consecutive path separators (/).</li> <li>The number of separators (/) in the displayed path must remain the same.</li> </ul>
File Name	<ul style="list-style-type: none"> <li>Only an asterisk (*) character(s) can be added.</li> <li>Do not change the file name. Otherwise, it will no longer match. However, you can replace a piece of the string with an asterisk (*).</li> <li>Only a single asterisk character (*) is permitted.</li> </ul> <p>When a wildcard is used as part of the process path or file name definition, the entry displays in green, as shown below:</p> <div> <p>Triggered Rules:</p> <ul style="list-style-type: none"> <li>Modified Executable           <ul style="list-style-type: none"> <li>Apply exception on:               <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> MSI15F*.tmp </li> </ul> </li> <li>Path                   <ul style="list-style-type: none"> <li><input checked="" type="radio"/> Current: \Windows\Installer </li> <li><input type="radio"/> Any path</li> </ul> </li> </ul> </li> </ul> </div>

- (Optional) Enter any comments in the *Comments* box.
- Click the *Create Exception* button.
- (Optional) You can define another exception for this same security event by clicking the *plus*  button at the top of the window. Then, define the exception in the same manner as described in the previous steps.

×

## EXCEPTION CREATION

Exceptions for event **665672**

Exception 1

Exception 2

+

Collector groups

☒ 
☐ All groups
☐ All organizations

Destinations

☒ 
☐ All destinations

Users

☐ 
☒ All users



If this exception was created previously, the *Remove Exception* button appears enabling you to delete the exception.

## Device Control exceptions



Device Control capabilities are license-dependent. You may contact [Fortinet Support](#) for more information.

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*.

For example:

**EXCEPTION CREATION**

Exceptions for event **3693708**

Exception 1 +

▼ USB Mass Storage Device

Apply exception on:

☒ Amazon Kindle (Unsigned)

Path ☐ Current:

☒ Any path

Script ☒ Current: Kindle

☐ Any script

When created by:

☒ USB Mass Storage Device (Unsigned)

Path ☐ Current:

☒ Any path


Script ☒ Current: B005A0A200630829

☐ Any script

Type comments

Create Exception Cancel

## 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

Exception 1 +

---

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 ⋮

Type comments

Remove Exception

Save Changes Cancel

- 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 more details, see [Defining a security event as an exception on page 164](#).  
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.



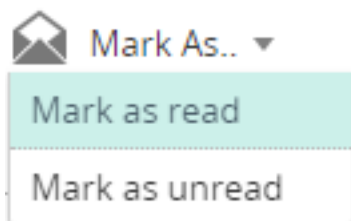
3. Click *Save Changes*.

## Marking a security event as read/unread

The following describes how to specify that you have viewed a security event. This does not mean that the security event has been handled ([Marking a security event as handled/unhandled on page 156](#)). When any FortiEDR Central Manager user marks a security event as read, all users see it as having been read. Unread security events are displayed in bold.

### To mark a security event as having been viewed:

1. Select the rule's checkbox.
2. Click *Mark As* and select *Mark as read* from the dropdown menu.



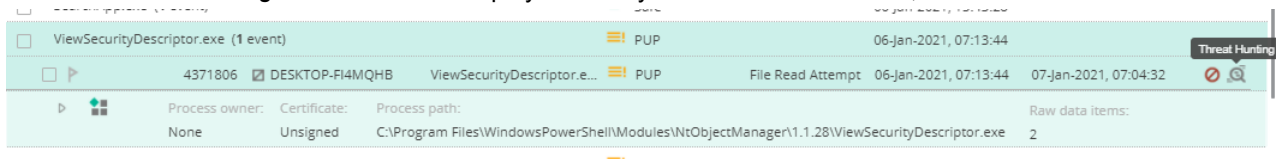
The security event row text is no longer displayed in bold.

## Viewing relevant activity events

Security events may have related activity events that can be viewed in the *Threat Hunting* tab.

### To view the related activity event of a security Event in the Event Viewer

1. Click the *Threat Hunting*  icon that is displayed when you hover over the event, as shown below.

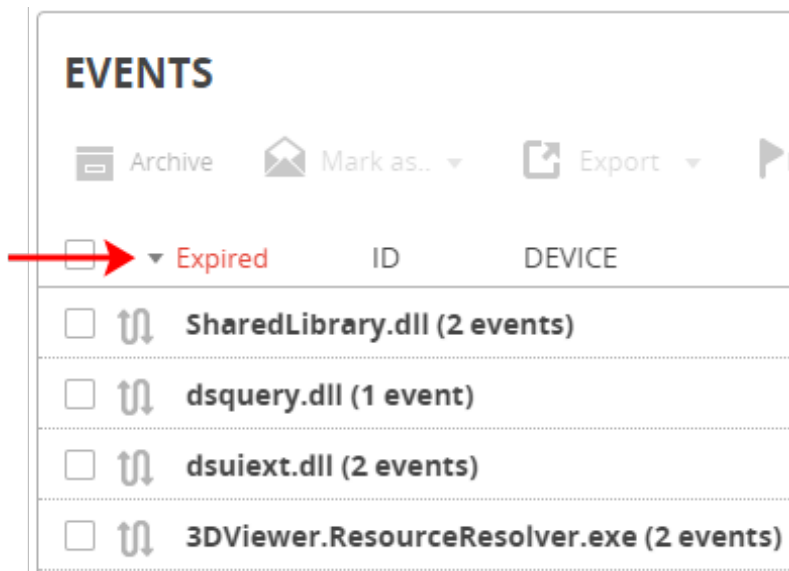


The *Threat Hunting* window then opens.

## Viewing expired security events

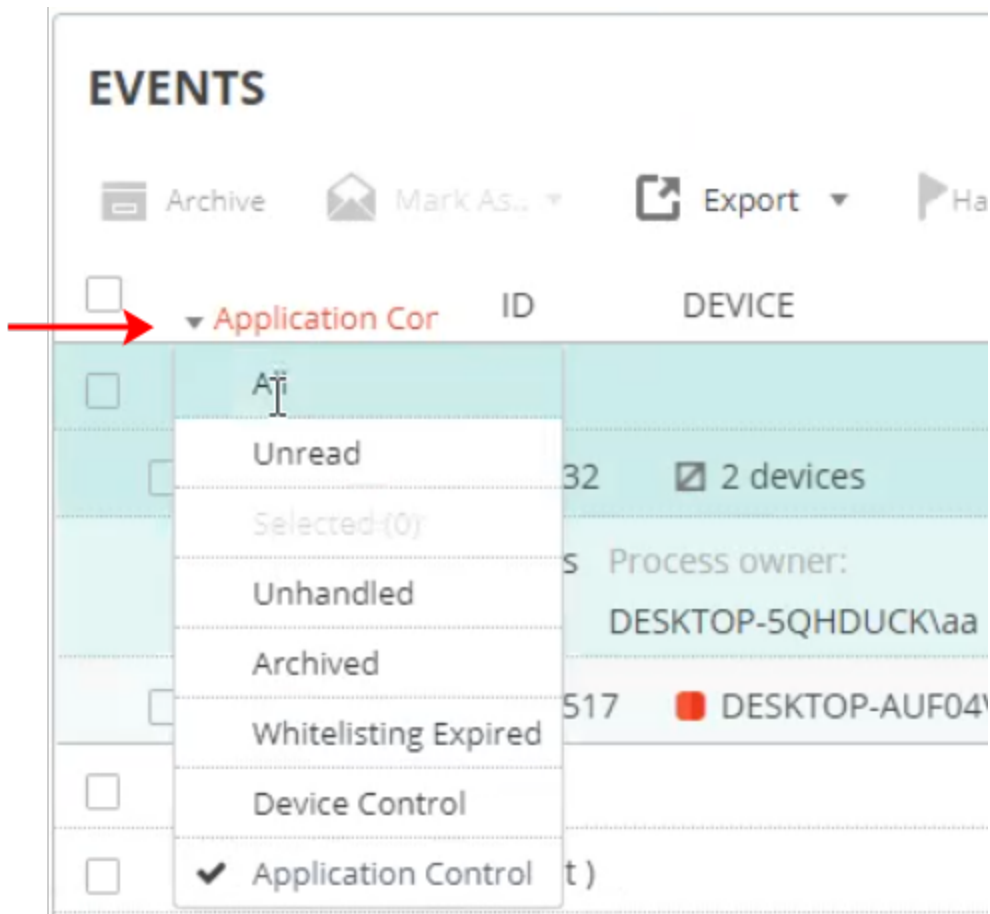
Security events in the *Event Viewer* can be filtered to show only expired events. Expired security events are events that the system has determined as safe. As such, these security events are only triggered once and then saved internally in the system. There is no need to define an exception for them. Expired security events cannot be handled in the system in any way, such as marking them as read/unread, defining an exception for them and so on.

Expired security events can only occur when a Collector is connected to the Core, and do not occur when a Collector works autonomously.



## Viewing Application Control security events

Security events in the *Event Viewer* 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.

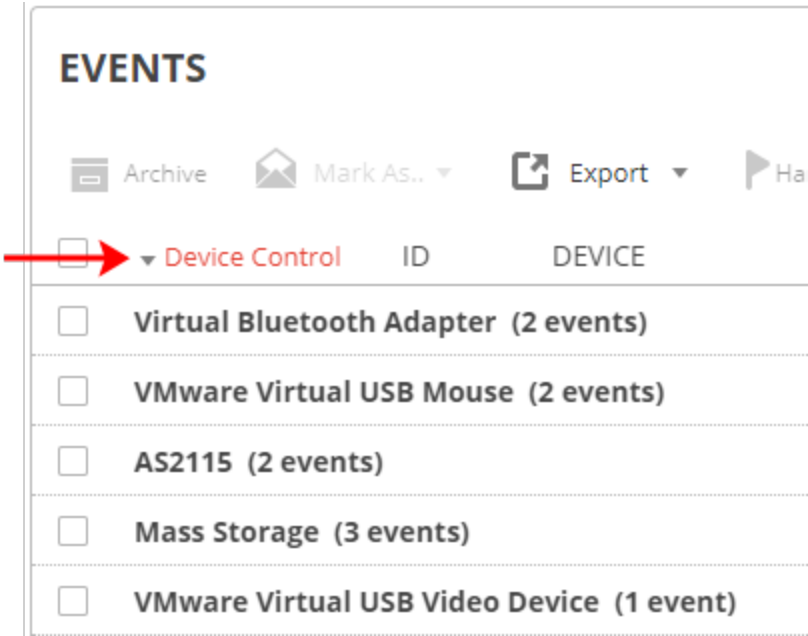


## Viewing Device Control security events



Device Control capabilities are license-dependent. You may contact [Fortinet Support](#) for more information.

Security events in the *Event Viewer* 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.



Other options in the Event Viewer

Option	Description
Sorting Events	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. By default, the <i>System Defined</i> option is selected, which specifies that the search is performed on the most relevant fields and then the event list is filtered accordingly. Alternatively, from this dropdown menu, you can select the field(s) that are searched, as follows:

Option	Description
--------	-------------

▼

✓ System Defined

ID

Raw ID

Device

Process

Remote IP/URL

Logged Users




Search Event

▼ 🔍

LAST UPDATED

Select a specific field when you know what you are searching (meaning whether it is ID, Process name or so on) in order to get results faster.

## Searching For Events

Click the down arrow in the *Search Event* field to display a variety of search options . When the *Event Viewer* display is filtered by a search, the *Search Event* field displays the words *Multiple search* . To redisplay all the security events (unfiltered), click .

## SEARCH EVENT

ID

RAW ID

Classification
☐ Malicious
☐ Suspicious
☐ PUP
☐ Inconclusive
☐ Likely Safe
☐ Safe

First Seen
From
To

Last Seen
From
To

Event Status
☐ Handled
☐ Unhandled

Event Notification
☐ Muted
☐ Unmuted

Event Actions
☐ Block
☐ Simulation Block
☐ Log

Destination

Process Path

Operating Systems

Certificate
☐ Signed
☐ Unsigned

Collector Group

User

Collector Name

Process

Policies

Rules









Raw Items Count

Playbook Action

☐ Include Archived-Events

Search

Cancel

Option	Description
	<ul style="list-style-type: none"> <li>The <i>User</i> field refers to the employee's username on the computer and on the FortiEDR Manager.</li> <li>You can select one or more action types in the AIR Action dropdown list.</li> </ul> <div>  <div> <div>AIR Action</div> <div>Isolate device, Terminate process, Delete file, Clean p...</div> <div> <div>✓ Isolate device</div> <div>✓ Terminate process</div> <div>✓ Delete file</div> <div>✓ Clean persistence data</div> <div>✓ Move device to High security group</div> </div> </div> </div>
Time Filter	Click the down arrow in the Time Filter to display a list of time period options. The default is <i>Last 30 days</i> .
Archiving Events	<p>Click the <i>Archive</i> button (  <i>Archive</i> ) to archive the selected security events. These security events are not deleted. You can display them using the <i>Search</i> option (described above) and selecting the included <i>Archived Events</i> option.</p> <hr/> <div>  <p>To unarchive a security event, click the <i>Unarchive</i> button (  ), and then confirm the unarchive action in the window that displays.</p> </div>
Exporting Events	Click the <i>Export</i> button (  <i>Export</i> ) to export the selected security events to Excel.
Deleting Events	<p>Click the <i>Delete</i> button (  <i>Delete</i> ) to completely delete a security event from the FortiEDR system.</p> <hr/> <div>  <p>A deleted security event cannot be restored or retrieved. Unless you are having storage capacity issues, we highly recommend just hiding security events and not deleting them.</p> </div>
Forensics	The optional FortiEDR Forensics add-on enables you to perform deep analysis of security events, as described on <a href="#">Forensics on page 219</a> .
Exception Manager	Click the <i>Exception Manager</i> button (  <i>Exception Manager</i> ) to access the <a href="#">Exception Manager on page 75</a> .

## Classification Details

After you click a security event in the [Events pane on page 150](#), the *CLASSIFICATION DETAILS* pane displays detailed information about the classification, policy, and rules assigned to the FortiEDR Collector that triggered this security event.

Click the *History* down arrow to display the classification history of a security event. The classification 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.

All FortiEDR actions are based on the final classification of a security event by the FCS. The FCS is a cloud-based, 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. All Playbook policy actions are based on the final determination of the FCS. For more details, see [Playbook policies on page 101](#).

For example, the following example shows that the security event was reclassified by the FCS and given a notification status of *Suspicious* at 15:44:51.

## CLASSIFICATION DETAILS

 Suspicious **FORTINET**


*By ReversingLabs*

Threat name: Unknown

Threat family: Unknown

Threat type: Unknown

### History

 Suspicious, by FortinetCloudServices , on 10-Feb-2020, 15:44:51

 Inconclusive, by Fortinet , on 10-Feb-2020, 15:25:31

### Triggered Rules

▼  Exfiltration Prevention

▶  Unmapped Executable - Executable File Without a Correspo...

In the *Triggered Rules* pane, only rules 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 *EVENTS* pane of this window. The action taken is determined by the rule with the highest priority.



Select an event here to display additional information about it in the CLASSIFICATION DETAILS area.

**EVENTS**

ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
traefik (1 event)			Inconclusive		14-Jan-2021, 02:13:00	
4429238	nginx.webserver	traefik	Inconclusive	2 destinations	14-Jan-2021, 02:13:00	17-Jan-2021, 02:12:59
Process owner: None Certificate: Unsigned Process path: /traefik Raw data items: 2						
java.exe (1 event)			Likely Safe		05-Jan-2021, 16:33:43	
SSDUpdate.exe (1 event)			Safe		01-Jan-2021, 01:56:30	
Docker Desktop installer.exe (2 events)			Safe		23-Dec-2020, 12:01:29	
Docker Desktop installer.exe (1 event)			Safe		30-Sep-2020, 10:14:40	
Loader.exe (1 event)			Safe		19-May-2020, 03:33:57	

**CLASSIFICATION DETAILS**

Triggered Rules

- Exfiltration Prevention
  - Unconfirmed Executable - Executable File Failed Verificati...
- Symantec Exfiltration Prevention
  - Unconfirmed Executable - Executable File Failed Verificati...

**ADVANCED DATA**

Event Graph Geo Location Automated Analysis

Process (win10\system\system) 1 Create Process (win10\system) 2 Create Process (win10\system\docker-container) 3 Create Process (win10\system\docker-container) 4 Create Process (traefik) 5 Connect Unconfirmed Executable 6 Process (193.227.209.208)

Each entry in the *CLASSIFICATION DETAILS* pane displays the threat name, threat family, and threat type. If threat intelligence data is available for the threat, it displays as well.

## CLASSIFICATION DETAILS

 Inconclusive **FORTINET**


By [ReversingLabs](#)

Threat name: Unknown



Threat family: Unknown

Threat type: Unknown

### History

- ▼  Inconclusive, by FortinetCloudServices , on 06-Feb-2020, 13:37:55
  - **Simulation** Device WIN-U8A5CLOII1R was moved from collector group lior1 to collector group High Security Collector Group once
  - **Simulation** Device WIN-U8A5CLOII1R was isolated once

### Triggered Rules

- ▼  Exfiltration Prevention
  - ▷  Invalid Checksum - Connection Attempt from Application wi...

When the Fortinet logo appears next to an entry in the *CLASSIFICATION DETAILS* pane, it indicates that the security event classification is the one that was automatically added by FortiEDR. Security events that were manually classified do not display the Fortinet logo.

Contact [Fortinet Support](#) for more details about the third-party tool used by Fortinet for the classification process.

Note that when the Playbook policy that relates to a security event is set to *Simulation* mode, then the event action is documented in the *Event Viewer*, but is not performed. Such security events display (simulation) in the *History* section of the *CLASSIFICATION DETAILS* pane, as shown below:

## CLASSIFICATION DETAILS



 Suspicious **FORTINET**

By *ReversingLabs*

Threat name: Unknown

Threat family: Unknown




Threat type: Unknown

### History

▼  Suspicious, by FortinetCloudServices , on 20-Feb-2020, 05:00:31

- Simulation Device **ensw-lap147** was moved from collector group **Win7** to collector group **High Security Collector Group** once
- Simulation Device **ensw-lap147** was isolated once

### Triggered Rules

- ▼  Ransomware Prevention
- ▷  Dynamic Code - Malicious Runtime Generated Code Detected
  - ▷  Unmapped Executable - Executable File Without a Correspo...



Notification actions are not shown in the *Event Viewer*, but Investigation and Remediation actions are. For more details, see [Playbook policy actions on page 105](#).

When expanding triggered rules, you can see the techniques that were used in this security event, based on the MITRE ATT&CK common techniques scheme. Clicking the technique opens the MITRE web page, providing additional details, as shown below.

### Triggered Rules

MITRE Techniques:

[T1186 - Process Doppelganging](#)

[T1093 - Process Hollowing](#)

**Retrieve the executable file of the parent process from the targeted device according to its Path by using the Forensic Tab. In addition, retrieve a full executable file memory of the process for deeper analysis.**

MITRE

ATT&CK

MatricesTacticsTechniquesMitigationsGroupsSoftwareResourcesBlogContribute

Search site

Register to stream ATT&CKcon 2.0 October 29-30

ENTERPRISE

TECHNIQUES

All

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
  - Access Token Manipulation
  - Application Access Token
  - Binary Padding
  - BITS Jobs
  - Bypass User Account Control
  - Clear Command History
  - CMSTP
  - Code Signing
  - Compile After Delivery

Home > Techniques > Enterprise > Process Doppelganging

## Process Doppelganging

Windows Transactional NTFS (TxF) was introduced in Vista as a method to perform safe file operations.<sup>[1]</sup> 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.<sup>[2]</sup> To avoid corruption, TxF performs an automatic rollback if the system or application fails during a write transaction.<sup>[3]</sup>

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

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

Process Doppelganging is implemented in 4 steps<sup>[4]</sup>:

- **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

# 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 *EVENTS* 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.

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**

Unresolved | Mark As... | Delete | Modify Action | Advanced Filter | Export

Applications | Policies | Host Firewall

APPLICATION	VENDOR	REPUTATION	VULNERABILITY	FIRST SEEN	LAST SEEN
Google Chrome	Signed Google Inc.	Unknown	Critical	24-May-2016	24-May-20...
50.0.2661.102		Unknown	Critical	24-May-2016	29-May-20...
51.0.2704.54		Unknown	Critical	24-May-2016	26-May-20...
31.0.1650.59		Unknown	Critical	24-May-2016	29-May-20...
50.0.2661.94		Unknown	Critical	25-May-2016	27-May-20...
51.0.2704.63		Unknown	Critical	26-May-2016	29-May-20...
Firefox	Signed Mozilla Corporation	Unknown	Critical	24-May-2016	05-Mar-20...
TeamViewer	Signed TeamViewer GmbH	Unknown	Critical	24-May-2016	24-May-20...
FortiClient Console	Signed Fortinet Inc.	Unknown	Critical	24-May-2016	12-Sep-2016
iTunes	Signed Apple Inc.	Unknown	Critical	24-May-2016	13-Sep-2016
Safari	Signed Apple Inc.	Unknown	Critical	26-May-2016	28-Jun-2018
Node.js	Signed Node.js	Unknown	Critical	29-May-2016	13-Sep-2016
Google Chrome	Signed Google	Unknown	Critical	29-May-2016	15-Oct-2020
VLC media player	Signed VideoLAN	Unknown	Critical	29-May-2016	11-Sep-2016
PostgreSQL	Unsign... PostgreSQL Global Develop...	Unknown	Critical	30-May-2016	13-Sep-2016

ADVANCED DATA

**APPLICATION DETAILS**

Google Chrome

**Policies**

Policy	Action
Default Communication Contro...	Allow According to policy
Servers Policy	Deny According to policy
Home Test	Allow According to policy
Servers Policy2	Deny According to policy
WinZip All	Allow According to policy
XXX	Deny According to policy
Isolation Policy	Deny According to policy

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 applications. The number represents the number of new applications.



You can hover over the number to see the list of new products. Each row shows the number of new products, by day.



COMMUNICATION CONTROL 309	
ADDED	TIME
2	11-Feb-2020
1	10-Feb-2020
1	06-Feb-2020
1	05-Feb-2020
7	04-Feb-2020
3	03-Feb-2020
1	02-Feb-2020
3	01-Feb-2020
3	31-Jan-2020
9	30-Jan-2020
22	29-Jan-2020
256	more products seen before 29-Jan-2020

The *COMMUNICATION CONTROL* tab contains two main pages:

- [Applications on page 193](#)
- [Policies on page 209](#)



## 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**.

The screenshot shows the FortiEDR interface with the **APPLICATIONS** page selected. The top navigation bar includes **DASHBOARD**, **EVENT VIEWER** (116), **FORENSICS**, **COMMUNICATION CONTROL** (130), **SECURITY SETTINGS**, **INVENTORY**, and **ADMINISTRATION** (29). The **COMMUNICATION CONTROL** dropdown menu is open, showing **Applications**, **Policies**, and **Host Firewall**.

The **APPLICATIONS** table lists the following applications:

APPLICATION	VENDOR	REPUTATION	VULNERABILITY	FIRST SEEN	LAST SEEN
Google Chrome	Signed Google Inc.	Unknown	Critical	24-May-2016	24-May-20...
50.0.2661.102		Unknown	Critical	24-May-2016	29-May-20...
51.0.2704.54		Unknown	Critical	24-May-2016	26-May-20...
31.0.1650.59		Unknown	Critical	24-May-2016	29-May-20...
50.0.2661.94		Unknown	Critical	25-May-2016	27-May-20...
51.0.2704.63		Unknown	Critical	26-May-2016	29-May-20...
Firefox	Signed Mozilla Corporation	Unknown	Critical	24-May-2016	05-Mar-20...
TeamViewer	Signed TeamViewer GmbH	Unknown	Critical	24-May-2016	24-May-20...
FortiClient Console	Signed Fortinet Inc.	Unknown	Critical	24-May-2016	12-Sep-2016
iTunes	Signed Apple Inc.	Unknown	Critical	24-May-2016	13-Sep-2016
Safari	Signed Apple Inc.	Unknown	Critical	26-May-2016	28-Jun-2018
Node.js	Signed Node.js	Unknown	Critical	29-May-2016	13-Sep-2016
Google Chrome	Signed Google	Unknown	Critical	29-May-2016	15-Oct-2020
VLC media player	Signed VideoLAN	Unknown	Critical	29-May-2016	11-Sep-2016
PostgreSQL	Unsign... PostgreSQL Global Develop...	Unknown	Critical	30-May-2016	13-Sep-2016

The **APPLICATION DETAILS** panel on the right shows the **Policies** for the selected application (Google Chrome):

Policy	Action
Default Communication Control...	Allow According to policy
Servers Policy	Deny According to policy
Home Test	Allow According to policy
Servers Policy2	Deny According to policy
WinZip All	Allow According to policy
XXX	Deny According to policy
Isolation Policy	Deny According to policy

Below the table is an **ADVANCED DATA** section.

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. For example, the figure below shows five versions for the *TeamViewer* application.

The screenshot shows the FortiEDR interface with the **APPLICATIONS** page selected. The **TeamViewer** application is highlighted in the list. The **APPLICATION DETAILS** panel on the right shows the **Policies** for the selected application (TeamViewer):

Policy	Action
Default Communication Control...	Allow According to policy
Servers Policy	Deny According to policy
Home Test	Allow According to policy
Servers Policy2	Deny According to policy
WinZip All	Allow According to policy
XXX	Deny According to policy
Isolation Policy	Deny According to policy

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 194](#)

- **VULNERABILITY:** The highest CVE vulnerability score for the application. For more details, see [Vulnerability on page 195](#)
- **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.

**APPLICATIONS**

APPLICATION	VENDOR	REPUTATION	VULNERABILITY	FIRST SEEN	LAST SEEN
Google Chrome	Signed Google Inc.	Unknown	Critical	24-May-2016	24-May-20...
Firefox	Signed Mozilla Corporation	Unknown	Critical	24-May-2016	05-Mar-20...
TeamViewer	Signed TeamViewer GmbH	Unknown	Critical	24-May-2016	24-May-20...
11.0.59518.0		Unknown	Critical	24-May-2016	13-Jul-2016
10.0.47484.0		Unknown	Critical	24-May-2016	06-Aug-20...
11.0.62308.0		Unknown	Critical	13-Jul-2016	22-Jul-2016
11.0.63017.0		Unknown	Critical	22-Jul-2016	14-Aug-20...
11.0.64630.0		Unknown	Critical	10-Aug-2016	20-Aug-20...
FortiClient Console	Signed Fortinet Inc.	Unknown	Critical	24-May-2016	12-Sep-2016

**APPLICATION DETAILS**

**Policies**

Policy	Action
Default Communication Control...	Allow
Servers Policy	Deny
Home Test	Allow
Servers Policy2	Deny
WinZip All	Allow
XXX	Deny
Isolation Policy	Deny

**APPLICATIONS**

APPLICATION	VENDOR	REPUTATION	VULNERABILITY	FIRST SEEN	LAST SEEN
Google Chrome	Signed Google Inc.	Unknown	Critical	24-May-2016	24-May-20...
Firefox	Signed Mozilla Corporation	Unknown	Critical	24-May-2016	05-Mar-20...
TeamViewer	Signed TeamViewer GmbH	Unknown	Critical	24-May-2016	24-May-20...
11.0.59518.0		Unknown	Critical	24-May-2016	13-Jul-2016
10.0.47484.0		Unknown	Critical	24-May-2016	06-Aug-20...
11.0.62308.0		Unknown	Critical	13-Jul-2016	22-Jul-2016
11.0.63017.0		Unknown	Critical	22-Jul-2016	14-Aug-20...
11.0.64630.0		Unknown	Critical	10-Aug-2016	20-Aug-20...
FortiClient Console	Signed Fortinet Inc.	Unknown	Critical	24-May-2016	12-Sep-2016
iTunes	Signed Apple Inc.	Unknown	Critical	24-May-2016	13-Sep-2016
Safari	Signed Apple Inc.	Unknown	Critical	26-May-2016	28-Jun-2018
Node.js	Signed Node.js	Unknown	Critical	29-May-2016	13-Sep-2016
Google Chrome	Signed Google	Unknown	Critical	29-May-2016	15-Oct-2020
VLC media player	Signed VideoLAN	Unknown	Critical	29-May-2016	11-Sep-2016
PostgreSQL	Unsign... PostgreSQL Global Develop...	Unknown	Critical	30-May-2016	13-Sep-2016

**VERSION DETAILS**

**Policies**

Policy	Action
Default Communication Control...	Allow
Servers Policy	Deny
Home Test	Allow
Servers Policy2	Deny
WinZip All	Allow
XXX	Deny
Isolation Policy	Deny

**Vulnerabilities**


Total 5 CVEs









- CVE-2018-16550 - Critical (CVSS 3.0: 9.8, CVSS 2.0: 5)
- CVE-2020-13699 - High (CVSS 3.0: 8.8, CVSS 2.0: 6.8)
- CVE-2019-18988 - High (CVSS 3.0: 7, CVSS 2.0: 4.4)
- CVE-2018-14333 - High (CVSS 3.0: 8.1, CVSS 2.0: 4.3)
- CVE-2019-18196 - Medium (CVSS 3.0: 6.7, CVSS 2.0: 6.9)

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 203](#).

## 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.



<input type="checkbox"/>	APPLICATION		VENDOR	REPUTATION
▶ <input type="checkbox"/>	 <b>Thunderbird</b>	Signed	Mozilla Corporation	 5
▶ <input type="checkbox"/>	 WhatsApp	Signed	WhatsApp	 5
▶ <input type="checkbox"/>	 <b>Firefox</b>	Signed	Mozilla Corporation	 5
▶ <input type="checkbox"/>	 <b>filebeat.exe</b>	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.

## Vulnerability

This option is only available to users who have purchased the *Discover and Protect* license or the *Discover, Protect and Response* license.

Each application in the application list also shows a vulnerability score.

FortiEDR categorizes applications/versions based on the Common Vulnerability Scoring System (CVSS) CVE scheme, which is commonly used worldwide. FortiEDR's vulnerability 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. Vulnerability assessment can be used together with virtual patching to block applications with known critical vulnerabilities, so that they cannot connect, until the system is patched for the CVEs listed.

**APPLICATIONS**

APPLICATION	VENDOR	REPUTATION	VULNERABILITY	FIRST SEEN	LAST SEEN
Google Chrome	Signed Google Inc.	Unknown	Critical	24-May-2016	24-May-20...
Firefox	Signed Mozilla Corporation	Unknown	Critical	24-May-2016	05-Mar-20...
TeamViewer	Signed TeamViewer GmbH	Unknown	Critical	24-May-2016	24-May-20...
11.0.59518.0		Unknown	Critical	24-May-2016	13-Jul-2016
10.0.47484.0		Unknown	Critical	24-May-2016	06-Aug-20...
11.0.62308.0		Unknown	Critical	13-Jul-2016	22-Jul-2016
11.0.63017.0		Unknown	Critical	22-Jul-2016	14-Aug-20...
11.0.64630.0		Unknown	Critical	10-Aug-2016	20-Aug-20...
FortiClient Console	Signed Fortinet Inc.	Unknown	Critical	24-May-2016	12-Sep-2016
iTunes	Signed Apple Inc.	Unknown	Critical	24-May-2016	13-Sep-2016
Safari	Signed Apple Inc.	Unknown	Critical	26-May-2016	28-Jun-2018
Node.js	Signed Node.js	Unknown	Critical	29-May-2016	13-Sep-2016
Google Chrome	Signed Google	Unknown	Critical	29-May-2016	15-Oct-2020
VLC media player	Signed VideoLAN	Unknown	Critical	29-May-2016	11-Sep-2016
PostgreSQL	Unsign... PostgreSQL Global Develop...	Unknown	Critical	30-May-2016	13-Sep-2016

**VERSION DETAILS**  
TeamViewer 11.0.59518.0

**Policies**

Policy	Action
Default Communication Contro...	Allow
Servers Policy	Deny
Home Test	Allow
Servers Policy2	Deny
WinZip All	Allow
XXX	Deny
Isolation Policy	Deny

**Vulnerabilities**  
Total 5 CVEs

- CVE-2018-16550 - Critical (CVSS 3.0: 9.8, CVSS 2.0: 5)
- CVE-2020-13699 - High (CVSS 3.0: 8.8, CVSS 2.0: 6.8)
- CVE-2019-18988 - High (CVSS 3.0: 7, CVSS 2.0: 4.4)
- CVE-2018-14333 - High (CVSS 3.0: 8.1, CVSS 2.0: 4.3)
- CVE-2019-18196 - Medium (CVSS 3.0: 6.7, CVSS 2.0: 6.9)

FortiEDR categories vulnerabilities into the following categories based on National Vulnerability Database (NVD) severity ratings:

- Unknown
- Low
- Medium
- High
- Critical

The Vulnerabilities area at the bottom right of the window lists the CVE-identified vulnerabilities for the selected application/version. Each CVE row includes the CVE identifier, the FortiEDR-assigned vulnerability Category and the CVSS vulnerability scores.

**Vulnerabilities**

Total 4 CVEs

CVE-2019-3568	-	Critical	(CVSS 3.0: 9.8, CVSS 2.0: 7.5)
CVE-2018-6350	-	Critical	(CVSS 3.0: 9.8, CVSS 2.0: 7.5)
CVE-2018-6344	-	High	(CVSS 3.0: 7.5, CVSS 2.0: 5)
CVE-2019-3571	-	Medium	(CVSS 3.0: 5.3, CVSS 2.0: 5)



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.

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.

**CVE-2019-9820** [Learn more at National Vulnerability Database \(NVD\)](#)

**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](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

**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 209](#). The information presented in the *Advanced Data* area of the window also provides useful information to help protect against vulnerabilities. For more details, [Advanced Data on page 203](#).

## 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

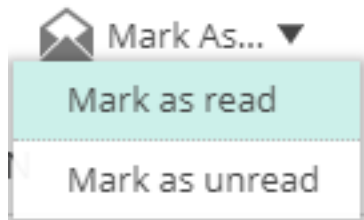
The following describes how to specify that you have viewed an entity in the application list. You can mark applications or versions as read/unread.

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).

<input type="checkbox"/>	APPLICATION		VENDOR	REPUTATION	VULNERABILITY	FIRST SEEN	LAST SEEN
▶ <input type="checkbox"/>	<b>Thunderbird</b>	Signed	Mozilla Corporation	<div><div></div><div></div><div></div><div></div><div></div></div> 5	<span>●</span> Critical	18-Dec-2019	<b>24-Dec-2019</b>
▶ <input type="checkbox"/>	WhatsApp	Signed	WhatsApp	<div><div></div><div></div><div></div><div></div><div></div></div> 5	<span>●</span> Critical	18-Dec-2019	18-Dec-2019
▶ <input type="checkbox"/>	Firefox	Signed	Mozilla Corporation	<div><div></div><div></div><div></div><div></div><div></div></div> 5	<span>●</span> Critical	18-Dec-2019	25-Dec-2019
▶ <input type="checkbox"/>	filebeat.exe	Unsign...	Unknown Vendor	<div><div></div><div></div><div></div><div></div><div></div></div> 3	Unknown	19-Dec-2019	09-Feb-2020
▶ <input type="checkbox"/>	Google Chrome	Signed	Google	<div><div></div><div></div><div></div><div></div><div></div></div> 5	<span>●</span> 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.

DASHBOARD

EVENT VIEWER

FORENSICS

COMMUNICATION CONTROL 22

SECURITY SETTINGS

INVENTORY

ADMINISTRATION 403

Protection

admin

APPLICATIONS

All

Mark As...

Delete

Modify Action

Advanced Filter

Export

Showing 1-1/1

Windows Explorer

	APPLICATION	VENDOR	REPUTATION	VULNERABILITY	FIRST SEEN	LAST SEEN
<input type="checkbox"/>	Windows Explorer	Signed	Microsoft Corporation	<div><div></div></div> 5 Unknown	24-Mar-2020	24-Mar-20...
<input checked="" type="checkbox"/>	10.0.18362.628 (WinBuild...		<div><div></div></div> 5 Unknown	24-Mar-2020	24-Mar-20...	

VERSION DETAILS

Windows Explorer, v. 10.0.18362.628 (WinBuild.160101.0000)

Policies

Policy	Action
Default Communication Contro... <b>FORTINET</b>	<b>Deny</b> <b>Manually</b>
Servers Policy <b>FORTINET</b>	<b>Allow</b> According to policy
1234	<b>Allow</b> According to policy
2345	<b>Allow</b> According to policy
Default Communication Control Policy clo...	<b>Allow</b> According to policy
Servers Policy clone	<b>Allow</b> According to policy
Isolation Policy <b>FORTINET</b>	<b>Allow</b> <b>Manually</b>

Vulnerabilities


There are no vulnerabilities for this version

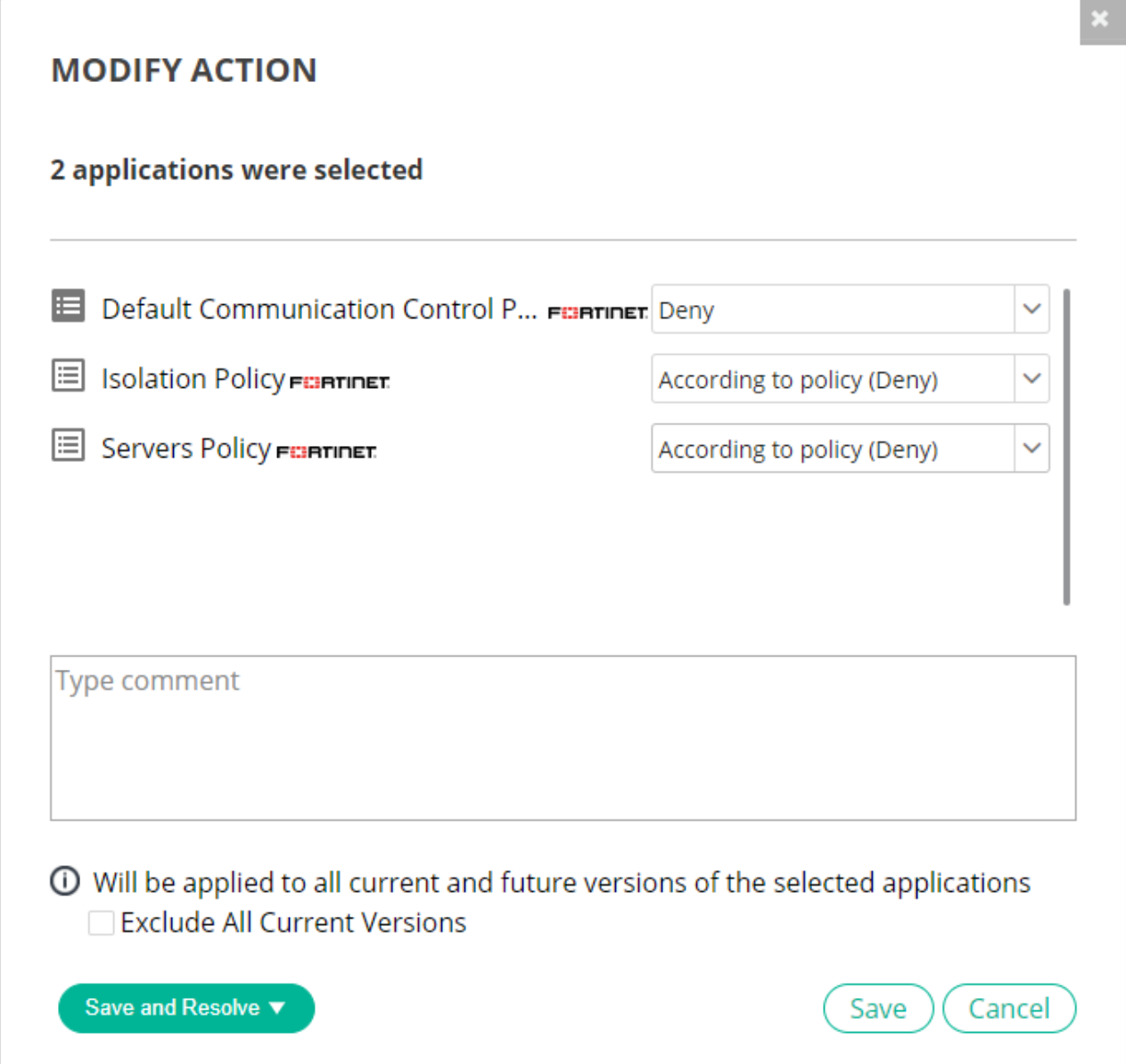
ADVANCED DATA

Copyright © Fortinet Version 4.1.0.103

System Time (UTC +02:00) 01:56:28




## 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... 	Deny
Isolation Policy 	According to policy (Deny)
Servers Policy 	According to policy (Deny)

Type comment

 Will be applied to all current and future versions of the selected applications

☐ Exclude All Current Versions

Save and Resolve Save Cancel

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

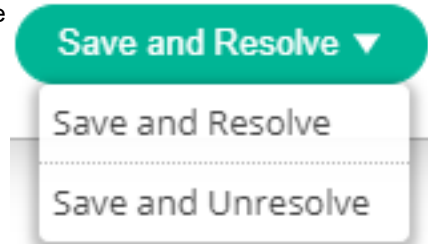
admin, at 10-Sep-2019, 03:42:53

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

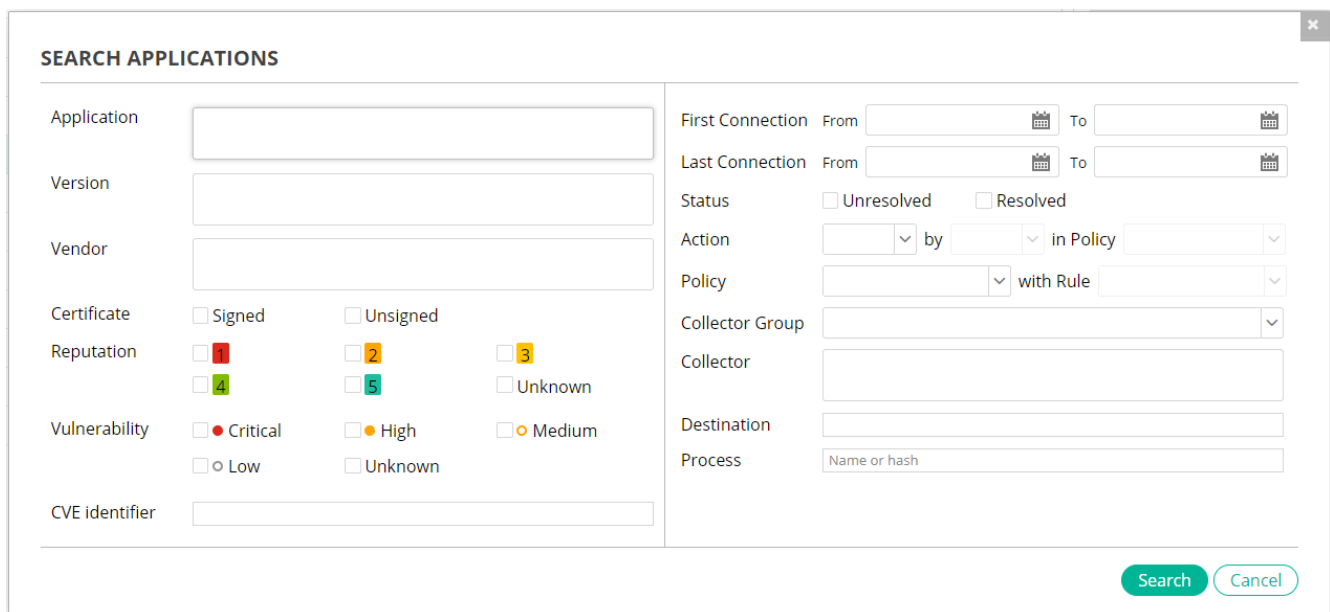


decision for the selected application(s).

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.












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.

Filter	Criteria
Reputation	Filters by reputation score. Check the checkbox(es) for the reputation 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
	Click the down arrow in the  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.
Critical CVE	Lists applications with a Critical CVE score.

Option	Function
 Mark As... ▼	<p>Lists applications that have not yet been viewed in the application list.</p> <p>Click the down arrow on the  button and then select <i>Mark as read</i> or <i>Mark as unread</i>. For more details, you may refer to the <a href="#">Marking an Entry as Read/Unread on page 197</a>.</p>
 Delete	<p>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.</p>
 Modify action	<p>Click the button to change the current policy action to be applied for the selected entity, as described in <a href="#">Modifying a Policy Action on page 198</a></p>
 Advanced filter	<p>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 <a href="#">Policy rules on page 213</a>.</p> <div> <input type="text" value="Select Filter..."/> <input type="text" value="Select Criteria..."/> <input type="text" value="Setup rule..."/> <span>✕</span> </div>
 Export ▼	<p>Click the down arrow in the <i>Export</i> button ( <i>Export</i> ▼) and select the format for exporting data. You can select <i>Excel</i> or <i>JSON</i>.</p>
<input type="text" value="Search Application"/>	<p>Use the <i>Search Application</i> field to perform an advanced search, as described in <a href="#">Searching the Application List on page 201</a>.</p>

## 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														
<b>APPLICATION INFO</b> 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: <ul style="list-style-type: none"> <li>I:\Device\HarddiskVolume2\Windows\System32\smartscreen.exe (97B64...)</li> <li>I:\Device\HarddiskVolume3\Windows\System32\smartscreen.exe (9B0C6...)</li> <li>And 2 more...</li> </ul>	<b>APPLICATION USAGE</b> Total System:  99.6 connections / day emulation  N/A <a href="#">More...</a>	<b>DESTINATIONS</b> <table border="1"> <thead> <tr> <th>IP</th><th>CONNECTION TIME</th><th>COUNTRY</th></tr> </thead> <tbody> <tr> <td>23.50.187.27</td><td>29-Jan-2020, 03:18:24</td><td> Netherlands</td></tr> <tr> <td>137.117.228.253</td><td>06-Feb-2020, 02:53:20</td><td> Netherlands</td></tr> <tr> <td>40.85.83.182</td><td>06-Feb-2020, 02:35:11</td><td> Ireland</td></tr> </tbody> </table> <a href="#">More...</a>	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
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												

- Application information on page 204
- Application Usage on page 205
- Destinations on page 206

## Application information

The *APPLICATION INFO* area displays summary information about the selected application.

**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...

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.

**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\HarddiskVolume3\Windows\System32\smartscreen.exe (9B0C636DF33BDE21F986279911E0FB03C96EE357)
- \Device\HarddiskVolume3\Windows\System32\smartscreen.exe (9B0C6...
- And 2 more...

**APPLICATION**

**Total System:**

emulation

[More...](#)

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 12:35:29

Process Names: VirusTotal

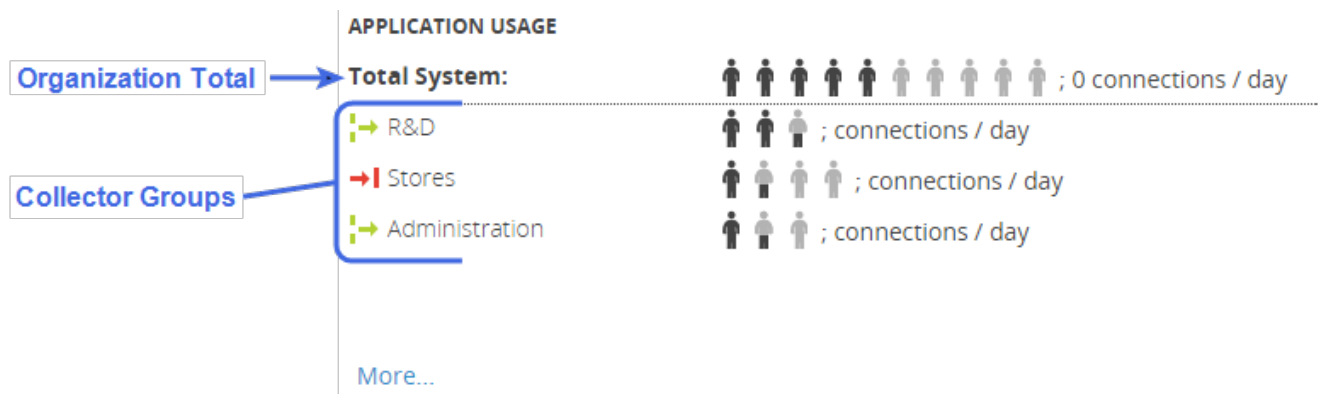
Threat Hunting by Hash

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.

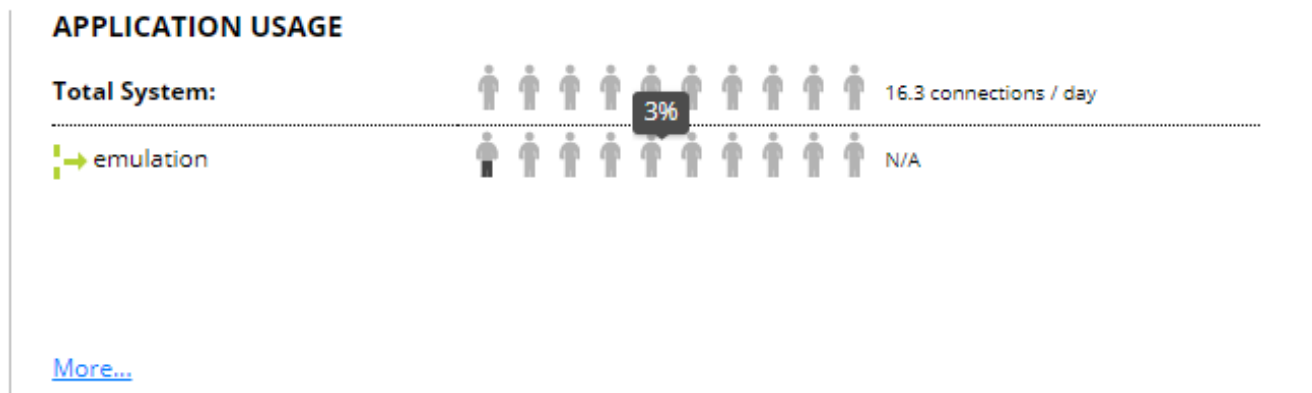


This area shows the number of connections (communication sessions) per day. The top line shows the total number of devices within the organization on which the selected application is installed.

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.



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

Export to Excel

Close

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

Export to Excel

Close











## 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... <b>FORTINET</b>	 Allow According to policy
 Servers Policy <b>FORTINET</b>	 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**) 
- [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.

The screenshot shows the FortiEDR interface. The top navigation bar includes Dashboard, Event Viewer (116), Forensics, Communication Control (126), Security Settings, Inventory, and Administration. The 'Communication Control' dropdown is open, showing 'Applications', 'Policies', and 'Host Firewall'. The 'POLICIES SETTINGS' section shows a table of policies. The 'Default Communication Control Policy' is expanded, showing rules like 'Reputation is less than or equal to 1' and 'Vendor is within 7 vendors'. The 'ASSIGNED COLLECTOR GROUPS' section on the right lists various groups like 'High Security Collector Group', 'A', 'a', 'A Victim', 'Accounting', 'Default VDI Group', 'emu', 'emulation', 'ensilo employees', 'ensilo Servers', 'Home users', 'maya test', 'my citrix pool (VDI)', 'New Group', 'OSX Users', 'PT', 'TEST-GRP', 'TEST-GRP 123', 'Tzaaf', 'Udi Collectors', and 'zee'.

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 <a href="#">Policy rules on page 213</a> .
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...	According to policy (Allow)
Isolation Policy	Allow
Servers Policy	According to policy (Deny)

Type comment




☐ Will be applied to all current and future versions of the selected applications

☐ Exclude All Current Versions

Save and Resolve Save Cancel

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 66](#).

## 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				
<div> <div>All</div> <div>Clone Delete Set Mode Assign Collector Group</div> </div>				
POLICY NAME	RULE	AFFECTED APPS	ACTION	STATE
<input type="checkbox"/> Default Communication Control Policy <div> <div>FORTINET</div> <div>Enabled</div> </div>		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	
<input type="checkbox"/> Servers Policy <div> <div>FORTINET</div> <div>Enabled</div> </div>		Total 209 denied apps (by user: 1 Allow, 0 Deny)		
<input type="checkbox"/> Isolation Policy <div> <div>FORTINET</div> <div>Enabled</div> </div>		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				
<div> <div>All</div> <div>Clone Delete Set Mode Assign Collector Group</div> </div>				
POLICY NAME	RULE	AFFECTED APPS	ACTION	STATE
<input type="checkbox"/> Default Communication Control Policy <div> <div>FORTINET</div> <div>Enabled</div> </div>		Total 0 denied apps (by user: 0 Allow, 0 Deny)		
<input checked="" type="checkbox"/> Servers Policy <div> <div>FORTINET</div> <div>Enabled</div> </div>		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	
<input type="checkbox"/> Isolation Policy <div> <div>FORTINET</div> <div>Enabled</div> </div>		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.

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.

VENDOR	REPUTATION	VULNERABILITY	FIRST SEEN	LAST SEEN
BitTorrent 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)	<input type="checkbox"/> SIGNED (0)	<input type="checkbox"/> UNSIGNED (0)
Acronis International	<input type="checkbox"/>	<input type="checkbox"/>
Adobe Systems Inc.	<input type="checkbox"/>	<input type="checkbox"/>
Advanced Micro Devices Inc.	<input type="checkbox"/>	<input type="checkbox"/>
AO Kaspersky Lab	<input type="checkbox"/>	<input type="checkbox"/>
Apache Software Foundation	<input type="checkbox"/>	<input type="checkbox"/>
Apple Inc.	<input type="checkbox"/>	<input type="checkbox"/>
Atlassian	<input type="checkbox"/>	<input type="checkbox"/>
AVAST Software	<input type="checkbox"/>	<input type="checkbox"/>
AVG Technologies	<input type="checkbox"/>	<input type="checkbox"/>

Select
Cancel

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
Save and Enable
Cancel

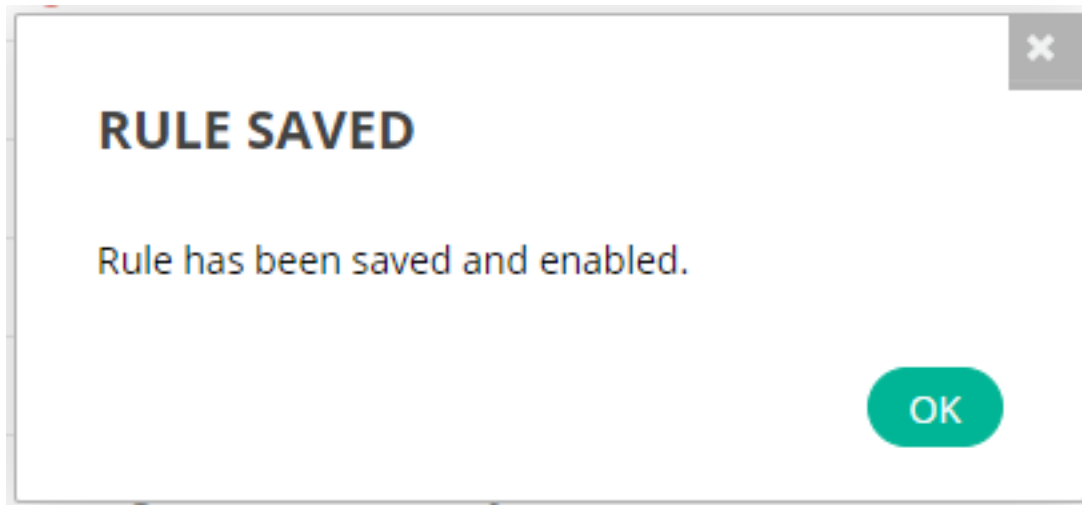
6. In the **Then** field, specify whether to Allow or Deny the application based on this rule.

If Vulnerability severity is greater tha...
High
Under Home Test
Then
Deny
Save and Enable
Cancel
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
Save and Enable
Cancel
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.



- Click OK.

## Assigning a policy to a Collector Group

- 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**

Search

<input type="checkbox"/> GROUP NAME ▲	# OF COLLECTORS	
<input type="checkbox"/> High Security Collector Group	0	Available
<input type="checkbox"/> l@#\$%^	0	Available
<input type="checkbox"/> 1234 qwer	0	Available
<input type="checkbox"/> Default Collector Group	2	Available
<input type="checkbox"/> Group name that is so long that will have 3 ...	0	Available
<input type="checkbox"/> hvghv	0	Available
<input checked="" type="checkbox"/> keren	0	
<input type="checkbox"/> kjkbhj	0	Available
<input type="checkbox"/> knikin	0	Available

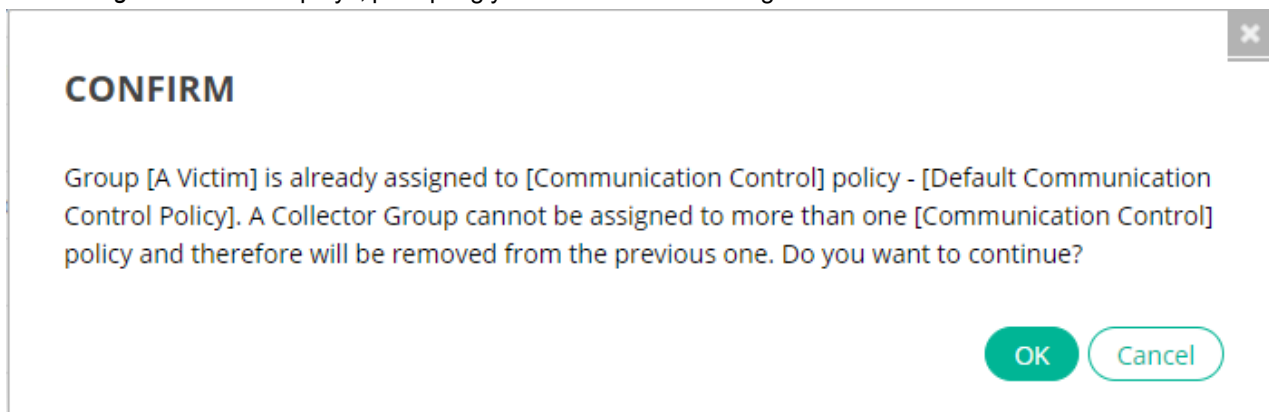
1 Collector group selected

Assign Cancel

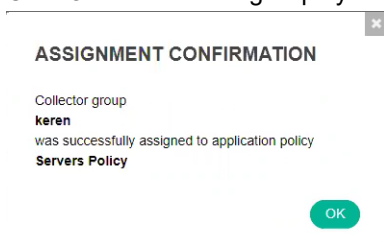
- Check the checkbox of the Collector Group you want to assign to the policy.



3. Click *Assign*. A window displays, prompting you to confirm the reassignment.





4. Click *OK*. The following displays:



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

Clone

Cancel

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
<div>All</div>	Click the down arrow in the <div>All</div> button and then select an option in the dropdown list to filter the policy list accordingly.
<div><div></div> Clone</div>	Click this button to clone a policy.
<div><div></div> Delete</div>	Click this button to delete a policy. Before deletion, a confirmation message displays, prompting you to confirm the deletion of the policy.
<div><div></div> Set mode</div>	Click the down arrow in the <div></div> Set mode button and then select the mode for the policy, as described in <a href="#">Policy mode on page 212</a>

# Forensics

This chapter describes the FortiEDR Forensics Analysis add-on option for deep analysis of security events.


## Introduction

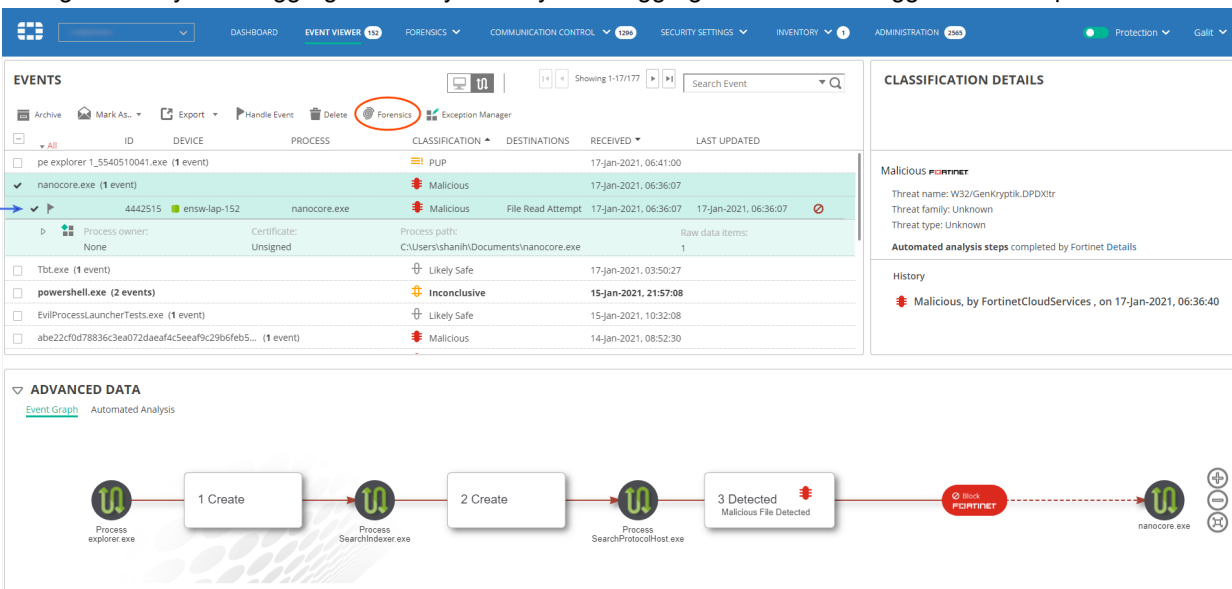
The Forensic Analysis add-on enables a security team (or anyone else) to delve deeply into the actual internals of the communicating devices' operating system that led up to the security event.

The Forensic Analysis add-on provides an abundance of deep analysis and drill-down options that reveal the process flows, memory stacks and a variety of operating system parameters in a graphic view, such as:

- Infected device and application details.
- Evidence path, which includes the process that the threat actor violated and which type of violation was executed.
- Side-by-side security event comparisons.

The first stage of working with Forensics is to select one or more security event aggregations or security events to analyze. To do so, use one of the methods below:

- In the *Event Viewer*, select a security event aggregation and then click the *Forensics* button (  **Forensics** ). Selecting a security event aggregation lets you analyze the aggregation of events triggered on this process.




The screenshot displays the FortiEDR Forensics interface. The top navigation bar includes tabs for DASHBOARD, EVENT VIEWER (152), FORENSICS, COMMUNICATION CONTROL (1296), SECURITY SETTINGS, INVENTORY (1), and ADMINISTRATION (2569). The main content area is divided into two sections: EVENTS and CLASSIFICATION DETAILS.

**EVENTS**

ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
pe explorer_1_5540510041.exe (1 event)			PUP		17-Jan-2021, 06:41:00	
nanocore.exe (1 event)			Malicious		17-Jan-2021, 06:36:07	
4442515	ensw-lap-152	nanocore.exe	Malicious	File Read Attempt	17-Jan-2021, 06:36:07	17-Jan-2021, 06:36:07
<p>Process owner: None   Certificate: Unsigned   Process path: C:\Users\shanih\Documents\nanocore.exe   Raw data items: 1</p>						
Tbt.exe (1 event)			Likely Safe		17-Jan-2021, 03:50:27	
powershell.exe (2 events)			Inconclusive		15-Jan-2021, 21:57:08	
EvilProcessLauncherTests.exe (1 event)			Likely Safe		15-Jan-2021, 10:32:08	
abe22cf0d78836c3ea072daef4c5eaf9c29b6feb5... (1 event)			Malicious		14-Jan-2021, 08:52:30	

**CLASSIFICATION DETAILS**

**Malicious** 

Threat name: W32/GenKryptik.DPDxtr  
Threat family: Unknown  
Threat type: Unknown

Automated analysis steps completed by Fortinet Details

**History**

- Malicious, by FortinetCloudServices, on 17-Jan-2021, 06:36:40

**ADVANCED DATA**

Event Graph | Automated Analysis

The Event Graph shows a sequence of events:

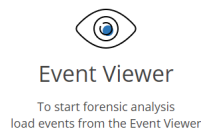
```

graph LR
    A[Process explorer.exe] --> B[1 Create]
    B --> C[Process SearchIndexer.exe]
    C --> D[2 Create]
    D --> E[Process SearchProtocolHost.exe]
    E --> F[3 Detected Malicious File Detected]
    F --> G[Malicious File Detected]
    G --> H[nanocore.exe]
  
```

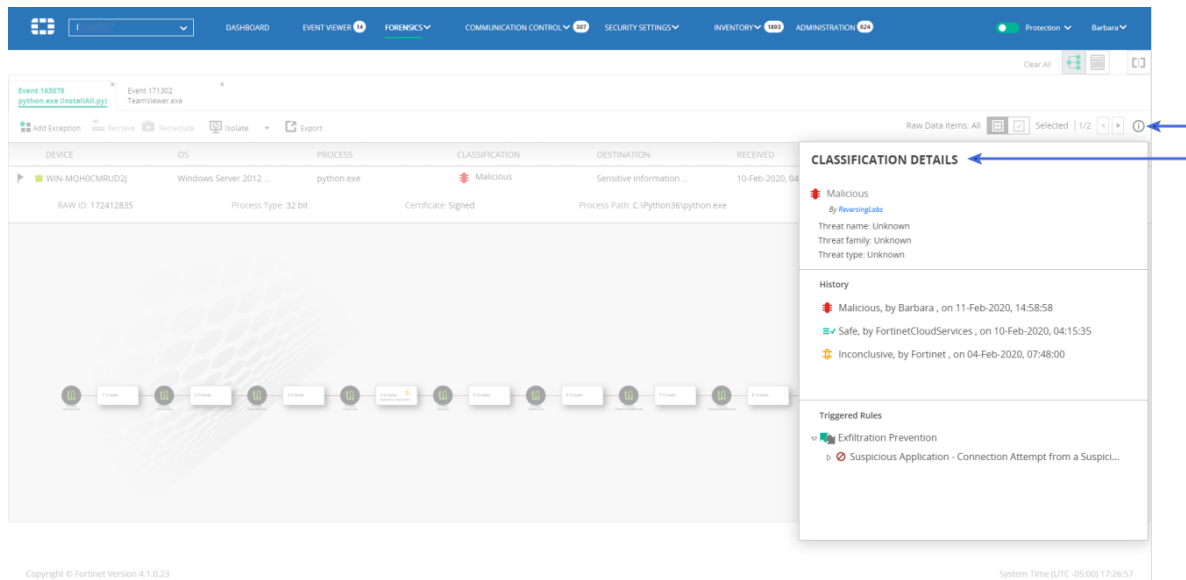
In this case, the Forensics add-on shows a separate tab for each security event associated with the security event aggregation. For example, the figure below shows seven tabs for a security event aggregation containing two events.

DEVICE	OS	PROCESS	CLASSIFICATION	DESTINATION	RECEIVED	LAST SEEN
EUGENE-PC	Windows 10 Pro	powershell.exe	Inconclusive	File Access	15-Jan-2021, 21:57:08	15-Jan-2021, 21:57:08
RAW ID: 2092947449	Process Type: 64 bit	Certificate: Signed	Process Path: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe		User: ENSILO\Eugene	Count: 1

- Select an individual security event in the Event Viewer and then click the *Forensics* button ( **Forensics** ). In this case, the Forensics add-on shows a single tab for the selected security event, with all of its related raw data items.
- Select a raw data item when in drill down, and then click the *Forensics* button ( **Forensics** ). In this case, the Forensics add-on shows a single tab for the selected security event with a single raw data item.
- In the *FORENSICS* tab, select *Events*. In the page that displays, click the *Event Viewer* link, shown below, and then select the security event of interest using any of the methods described above.

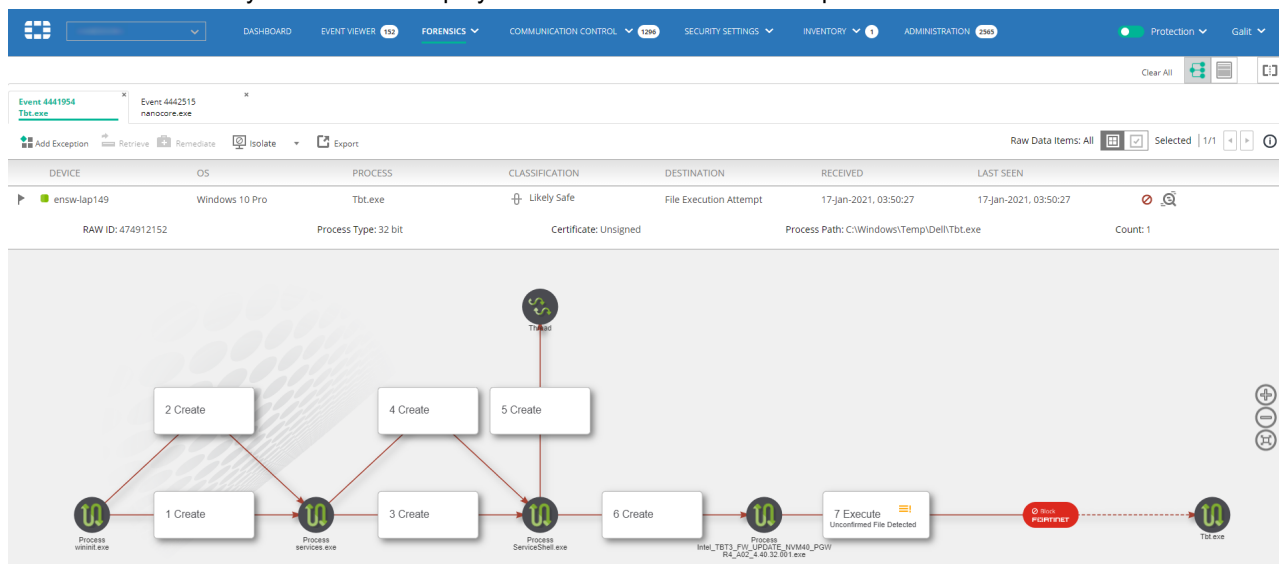


You can click the ⓘ button in the *FORENSICS* tab to display classification details, including the classification, policy and rules assigned to the FortiEDR Collector that triggered this security event. For more details about classification details, see [Classification Details on page 183](#).



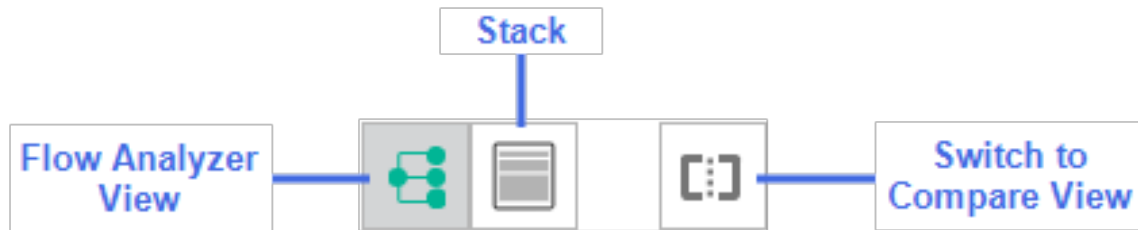
## To perform deep Forensic analysis:

1. Select the security events to analyze using one of the methods described on [Event Viewer on page 146](#). Selected security events that are currently loaded to the *FORENSICS* tab are marked in the *Event Viewer* with a fingerprint icon.
2. Each selected security event is then displayed in the *Event Viewer* as a separate tab:

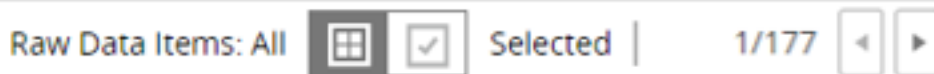




Each tab shows the same information as in the [Event Viewer on page 146](#), with additional information as described below.

The following options for viewing more information are provided:



In the *Raw Events* area, use the right and left arrows to scroll through the raw data items for a security event.



Click the *All Raw Data Items*  button to display all raw data items. Click the *Selected Raw Data Items*  button to select a specific raw data item. This action opens the following window, in which you specify the raw data item(s) to display.

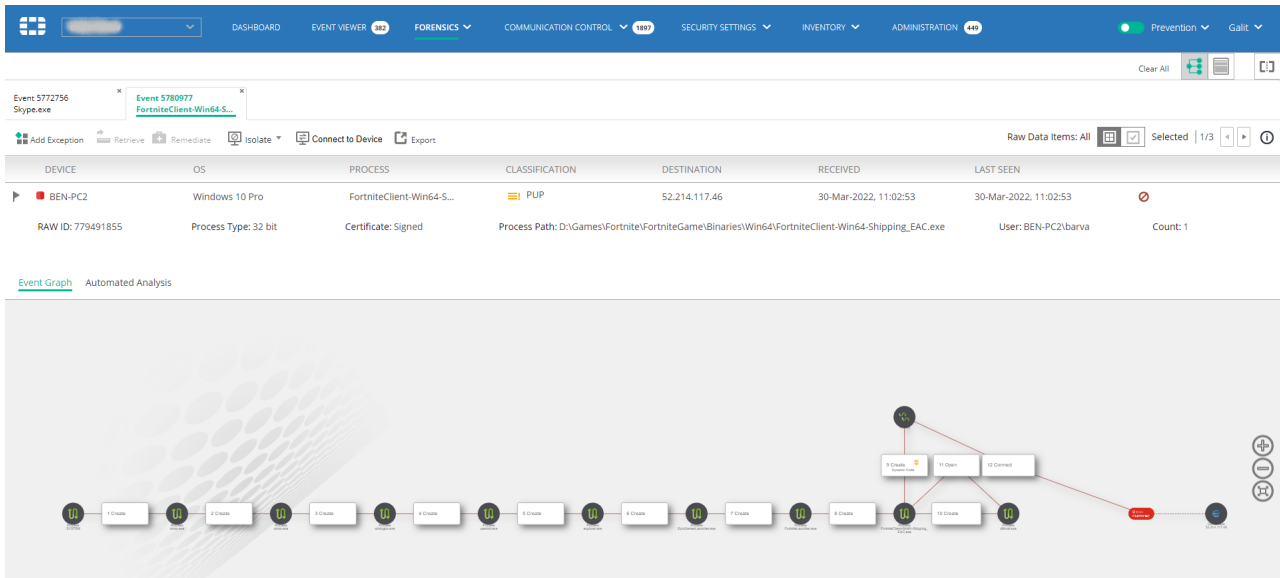
SELECT RAW DATA ITEMS

Showing 1-2/2

<input type="checkbox"/>	ID	DEVICE	DESTINATION	FIRST SEEN	LAST SEEN	COUNT
<input type="checkbox"/>	172412835	WIN-MQH0CMRUD2J	Sensitive Inform...	10-Feb-2020, 04:15:27	10-Feb-2020, 04:15:27	1
<input type="checkbox"/>	767009555	WIN-MQH0CMRUD2J	Sensitive Inform...	04-Feb-2020, 07:47:59	04-Feb-2020, 07:47:59	1

Close

Click *Close* in the *SELECT RAW DATA ITEMS* window. The *Events* page displays only those raw data items you selected in the view.

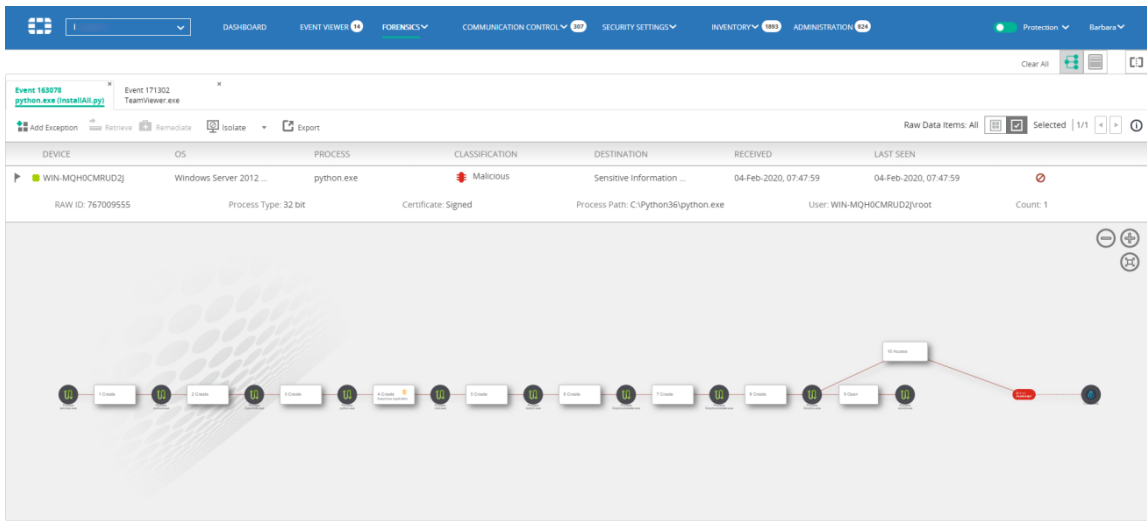


Click the *Threat Hunting*  button to review relevant Activity Events in the *Threat Hunting* tab.




The *Connect to Device* button opens a console that provides direct access to FortiEDR-protected devices. See [Administration on page 274](#).


## Flow Analyzer view





The *Flow Analyzer* view (  ) shows a graphic flow diagram depicting the history of what happened before the security event was triggered, from left to right. Each node can represent a process, a thread or a service.

The arrows indicate the sequence of processes and specify the operation that was performed, such as *Create*, *Inject*, *Open* and so on. If multiple operations were performed between two processes, then multiple arrows are shown between

them. If an operation repeated several times in the same segment, it is represented by a dashed line .



Typically, the next to last rightmost node represents a connection request and specifies the IP address to which it attempted to establish a connection. It can also represent an attempt to lock or encrypt a file by ransomware



The rightmost node represents the action performed by FortiEDR, such as *Log*, *Block*, or *Simulated Block*.



The flow chart is interactive. Clicking on a specific node or arrow drills down to the *Stack View* (described in [Stack view on page 224](#)). This enables you to perform further investigation of the specific stack that was collected during that step.

## Stack view

The screenshot displays the FortiEDR interface with the **Stack view** selected. The main pane shows a detailed view of a connection event. The left sidebar has tabs for **Event Details**, **Stacks**, and **Stack Details**.

**Event Details:**

- Event 145722: cscript.exe (WINAN\_5565...)
- Event 163078: python.exe (install.py)
- Event 171302: TeamViewer.exe

**Stacks:**

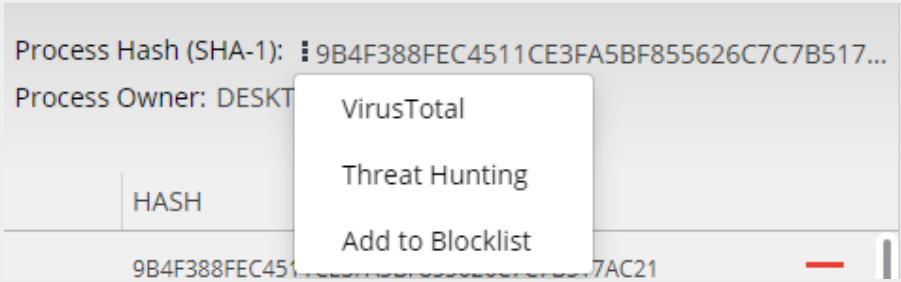
- PARENT PROCESS CREATION
- PARENT PROCESS CREATION
- PARENT PROCESS CREATION
- CONNECTION

**Stack Details:**

EXECUTABLE FILE NAME	WRITABLE	CERTIFICATE	REPETITIONS	BASE ADDRESS	END ADDRESS	HASH
\\Device\\Harddisk\\Volume1\\Program Files (x86)\\TeamViewer\\TeamViewer.exe	No	Signed				16135B96D41C108FCE902B8...
\\Device\\Harddisk\\Volume1\\Windows\\System32\\wow64cpu.dll	No	Signed	1	0x7f950000	0x7f959000	EC173C50816E234D123F07...
\\Device\\Harddisk\\Volume1\\Windows\\System32\\wow64.dll	No	Signed	2	0x7f950000	0x7f959000	1A1B4BCD4974F6A2E43E35...
\\Device\\Harddisk\\Volume1\\Windows\\System32\\ntdll.dll	No	Signed	2	0x7f95a07000	0x7f95a1c000	EF2481EDBF20D81F8B09F55...
\\Device\\Harddisk\\Volume1\\Windows\\System32\\WOW64cpu.dll	No	Signed	1	0x7f950000	0x7f959000	646304F2F3366F1828CFD8B...
\\Device\\Harddisk\\Volume1\\Windows\\System32\\ntdll.dll	No	Signed	1	0x7f95a07000	0x7f95a1c000	FF2481EDBF20D81F8B09F55...


The Stack view displays the following sections of information:



Field	Description
<b>Events</b>	Shows the same information as in the <a href="#">Event Viewer on page 146</a> .
<b>Stacks</b>	A control toolbar that depicts the stacks that were collected in each step prior to the connection establishment requestor file access. A red dot means that a rule violation was observed in this stack. You can click the different stack names to see the collected stack data.
<b>Stack Content Details</b>	<p>The bottom of the window displays each stack in the flow of the selected step. The stack entries represent the executable files that resided in the stack upon collecting the stack data. Click the stack node to filter the display to show that stack. The selected stack appears with a red line below it.</p> <p>Click the <i>Process Hash</i> link display a dropdown menu with the following options:</p>  <ul style="list-style-type: none"> <li>• <i>VirusTotal</i>: Checks whether this hash was seen elsewhere. This involves searching another external website (VirusTotal). Clicking the link runs the query in VirusTotal. Alternatively, you can go to <a href="http://www.virustotal.com">www.virustotal.com</a>, click the <i>Search</i> tab, paste the hash from FortiEDR and then click <i>Search It</i>.</li> <li>• <i>Threat Hunting</i>: Checks the activity events that are relevant to this hash. Clicking this option takes you to the <i>Threat Hunting</i> page.</li> <li>• <i>Add to Blocklist</i>: Adds this hash to the Application Control block list, as described in <a href="#">Application Control Manager on page 85</a>. Clicking this option opens up the <i>Add Application</i> Window with this hash specified.</li> </ul>

For each executable, you can see the following information:

- Executable File Name
- Writable: Specifies whether the executable code can be modified.
- Certificate: Specifies whether or not the certificate was signed.
- Repetitions: Specifies how many times this executable was detected in the stack.
- Base Address of this entry in memory.
- End Address of this entry in memory.
- Hash: Specifies the file hash.

The row of the executable that triggered the FortiEDR security event is highlighted with a red dot . This indicates the row that you may want to investigate further.

You can click an executable row to display an even deeper level of information describing that process, as shown below:

Copyright © Fortinet Version 4.1.0.23

System Time (UTC -05:00) 17:42:56

## Compare view

Copyright © Fortinet Version 4.1.0.23

Task View

System Time (UTC -05:00) 17:44:03


The Compare view enables you to display two views side-by-side. They can both be either [Flow Analyzer view on page 223](#) or [Stack view on page 224](#)

## Defining an exception

After Forensic analysis, you may decide to create an exception for a specific security event. To do so, you may refer to the [Defining security event exceptions on page 160](#). You may refer to [Playbook policies on page 101](#) for general information about exceptions.

## Remediating a device upon malware detection

After malware is detected on a device, you can use one of the following methods to 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	<p>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.</p> <hr/> <div>  <p>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.</p> </div> <hr/> <p>Both of these methods can be performed using the Forensics add-on.</p>

### To remediate a device on which malware was detected:

1. Select the security event(s) to analyze using one of the following methods described in [Event Viewer on page 146](#)
2. In the *Raw Events* area, select the relevant process. Use the various forensic tools provided by FortiEDR to determine the process of interest.

The screenshot shows the FortiEDR Forensics interface. The top navigation bar includes Dashboard, Event Viewer, Forensics (selected), Communication Control, Security Settings, Inventory, and Administration. The main window displays a list of events, with 'Event 87488 DynamicCodeTests.exe' selected. Below the event list, a table shows process details:

DEVICE	OS	PROCESS	CLASSIFICATION	DESTINATION	RECEIVED	LAST SEEN
Collector8PC	Windows 7 Ultimate N	DynamicCodeTests.exe	Suspicious	74.125.235.20	17-Mar-2020, 18:11:54	17-Mar-2020, 21:50:50

Below the table, a timeline shows 'PARENT PROCESS CREATION' and 'CONNECTION'. The 'CONNECTION' section provides details for Process ID: 3908, Source Process: ...Volume2\Users\root\Desktop\DynamicCodeTests.exe, Target: ..., Company: enSilo Test, Product: ..., Process Hash (SHA-1): A3268A8856900D53EEBC0C24D62DAFEC55E2555E, Process Owner: Collector8PCroot. A table lists associated files:

EXECUTABLE FILE NAME	WRITABLE	CERTIFICATE	REPETITIONS	BASE ADDRESS	END ADDRESS	HASH
Main -> Device\HarddiskVolume2\Users\root\Desktop\DynamicCodeTests.exe	No	Unsigned				A3268A8856900D53EEBC0C2...
Device\HarddiskVolume2\Windows\System32\wow64cpu.dll	No	Unsigned	1	0x73620000	0x73628000	278691ED59AF426398BAFFFF...

Analysis Information: A core OS executable. Executable File Format Errors. Additional Info.

After selecting the process of interest, the bottom pane of the window displays the list of files associated with that process.

The screenshot shows the FortiEDR Forensics interface. The top navigation bar includes Dashboard, Event Viewer, Forensics (selected), Communication Control, Security Settings, Inventory, and Administration. The main window displays a list of events, with 'Event 171302 TeamViewer.exe' selected. Below the event list, a table shows process details:

DEVICE	OS	PROCESS	CLASSIFICATION	DESTINATION	RECEIVED	LAST SEEN
WIN-MQH0CMRUDQ2	Windows Server 2012 ...	TeamViewer.exe	PUP	52.143.143.83	10-Feb-2020, 09:48:02	11-Feb-2020, 17:49:06

Below the table, a timeline shows 'PARENT PROCESS CREATION' and 'CONNECTION'. The 'PARENT PROCESS CREATION' section provides details for Process ID: 492, Source Process: ...e\HarddiskVolume1\Windows\System32\services.exe, Target: ...me1\Program Files (x86)\TeamViewer\TeamViewer\_Service.exe, Version: ..., Company: Microsoft Corporation, Product: ..., Process Hash (SHA-1): E289481D0682E250CC4BD6AFC6F1B26B86AF, Process Owner: NT AUTHORITY\SYSTEM. A table lists associated files:

EXECUTABLE FILE NAME	WRITABLE	CERTIFICATE	REPETITIONS	BASE ADDRESS	END ADDRESS	HASH
Main -> Device\HarddiskVolume1\Windows\System32\services.exe	No	Signed				E289481D0682E250CC4B...

3. Check the checkbox of the relevant file and then click the *Remediate* button. 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

☐ Handle persistent data (registry)

☒ Remove key

☐ Modify registry value

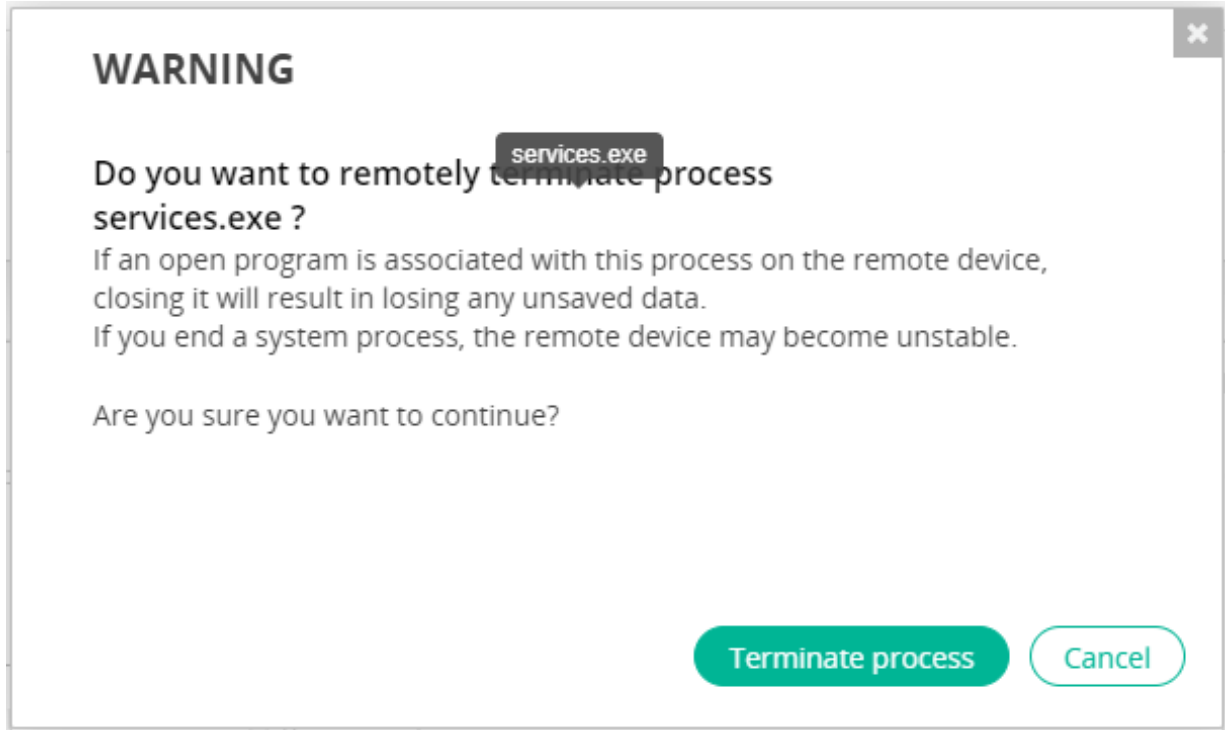
☒ Remove value

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

Type

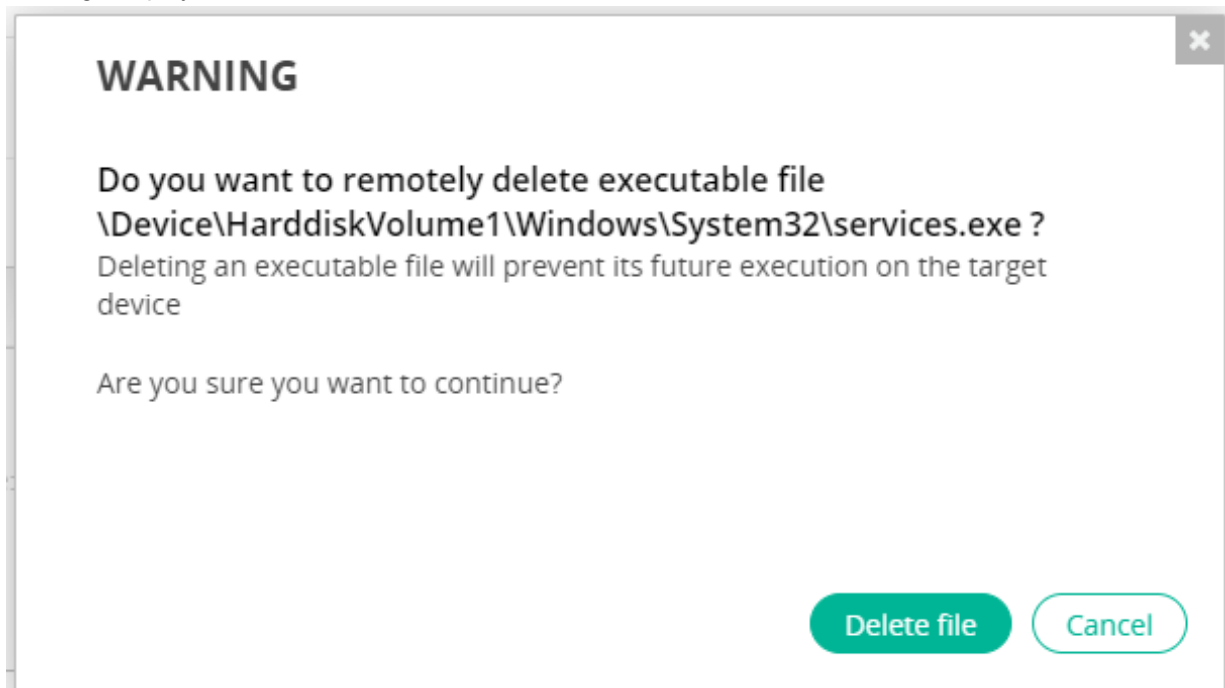
**Remediate** **Cancel**

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



Click *Terminate process* to terminate the selected process.

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

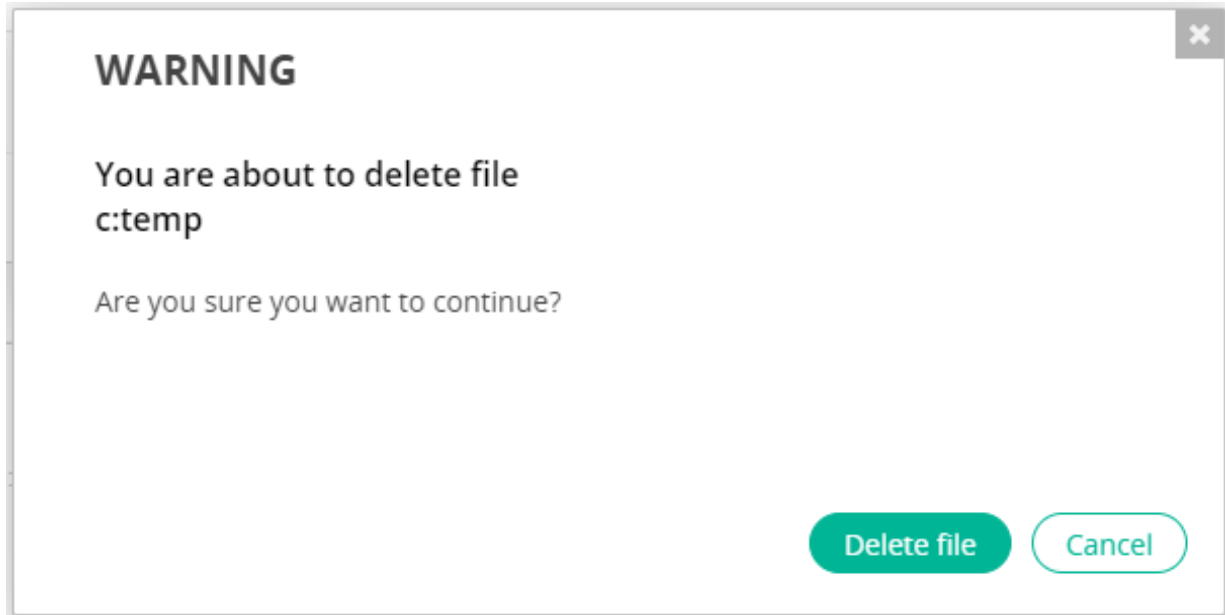


Click *Delete file* to remove the selected file.

- 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

A warning message displays.



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

☒ 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).

5. Click *Remediate*.

## Retrieving memory

The Retrieve Memory function enables you to retrieve the stack-memory of a specific Collector. This option enables you to retrieve memory from a specific communicating device in order to perform deeper analysis by analyzing the actual memory from the device. This function is only accessible from the Stack view.

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. The password is `enCrypted`.

If the file cannot be sent, it is saved locally on the host by the Collector.

### To retrieve memory for a Collector:

1. In the Stack view, select the stack(s) that you want to analyze by selecting its checkbox(es).

The screenshot shows the FortiEDR interface with the 'Stack view' selected. The main table lists process stacks with the following columns: DEVICE, OS, PROCESS, CLASSIFICATION, DESTINATION, RECEIVED, and LAST SEEN. The selected process is 'DynamicCodeTests32.exe' on 'DESKTOP-B509MQF' (Windows 10 Pro). Below the table, a detailed view of the selected process is shown, including a timeline of parent process creations and a connection table.

EXECUTABLE FILE NAME	WRITABLE	CERTIFICATE	REPETITIONS	BASE ADDRESS	END ADDRESS	HASH
Main ->Device\HarddiskVolume3\Users\admin\Desktop\DynamicCodeTests32.exe	No	Unsigned				A7AD6C89D7843E0485F5805...
Device\HarddiskVolume3\Windows\System32\wow64cpu.dll	No	Signed	2	0x77269000	0x77269000	8F56E5D8460F76091B02CA6...
Device\HarddiskVolume3\Windows\System32\wow64.dll	No	Signed	2	0x77c2e34000	0x77c2e395000	31D804FFB8D2252F823E955...
Device\HarddiskVolume3\Windows\System32\ntdll.dll	No	Signed	5	0x77c3012000	0x77c30130000	339E86A9EC4FE684899284FC...
Device\HarddiskVolume3\Users\admin\Desktop\DynamicCodeTests32.exe	No	Unsigned	1	0x400000	0xefe000	A7AD6C89D7843E0485F5805...
Device\HarddiskVolume3\Windows\System32\ntdll.dll	No	Signed	1	0x77c3012000	0x77c30130000	339E86A9EC4FE684899284FC...



2. Click *Retrieve*. The following window displays:

**MEMORY RETRIEVAL**  
**EVENT 166576, DESKTOP-BS09MQF**  
**DynamicCodeTests32.exe**

☒ Retrieve memory of selected stack entries - **29 entries selected**

Retrieve from:  
☒ Memory ☐ Disk

☐ Retrieve memory region from address:  to address:

☐ Retrieve the entire process memory

Estimated **Memory** Retrieval file size: **29.6 MB**

**Retrieve** **Cancel**

3. Select one of the following options:

- a. *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, as shown below:

Event 87477  
DynamicCodeTests.exe

Event 87488  
DynamicCodeTests.exe

Event 107146  
DynamicCodeTests.exe

Event 84974  
StackPivotTests.exe

Raw Data Items: All Selected 1/2

DEVICE	OS	PROCESS	CLASSIFICATION	DESTINATION	RECEIVED	LAST SEEN
CollectorBPC	Windows 7 Ultimate N	DynamicCodeTests.exe	Suspicious	74.125.235.20	17-Mar-2020, 18:11:54	17-Mar-2020, 21:50:50
RAW ID: 530581512	Process Type: 32 bit	Certificate: Unsigned	Process Path: \Device\HarddiskVolume2\Users\root\Desktop\DynamicCodeTests.exe	User: CollectorBPCroot	Count: 2	

PARENT PROCESS CREATION CONNECTION

**CONNECTION**

Process ID: 3908 Company: enSilo Test Product: Process Hash (SHA-1): A3268A6856900D53EEBC0C24D6DAFEC35E2355E  
Source Process: ...Volume2\Users\root\Desktop\DynamicCodeTests.exe Description: Command Line: Process Owner: CollectorBPCroot  
Target: Version: 1.0.0.1

EXECUTABLE FILE NAME	WRITABLE	CERTIFICATE	REPETITIONS	BASE ADDRESS	END ADDRESS	HASH
Main - \Device\HarddiskVolume2\Users\root\Desktop\DynamicCodeTests.exe	No	Unsigned				A3268A6856900D53EEBC0C2...
\Device\HarddiskVolume2\Windows\System32\wow64cpu.dll	No	Unsigned	1	0x73620000	0x73628000	278691ED59A42639B8AFFFF...
\Device\HarddiskVolume2\Windows\System32\wow64.dll	No	Unsigned	2	0x73590000	0x735c0000	68E88E72BFD0AC4F61697D3...
\Device\HarddiskVolume2\Windows\System32\ntdll.dll	No	Signed	1	0x76F00000	0x770a9000	92015F78BDB8D8AD035E41C33...
\Device\HarddiskVolume2\Windows\System32\ntdll.dll	No	Signed	1	0x76F00000	0x770a9000	92015F78BDB8D8AD035E41C33...
\Device\HarddiskVolume2\Windows\System32\ntdll.dll	No	Signed	4	0x76F00000	0x770a9000	92015F78BDB8D8AD035E41C33...

Copyright © Fortinet Version 4.1.0.103 System Time (UTC +02:00) 01:49:51

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, as shown below. For example, the figure below shows that three stack entries were selected for analysis.

**MEMORY RETRIEVAL**  
**EVENT 284376, JEFFDURAN-PC**  
**backgroundTaskHost.exe**

☒ Retrieve memory of selected stack entries - **2 entries selected**

Retrieve from:  
☒ Memory ☒ Disk

☐ Retrieve memory region from address:  to address:

☐ Retrieve the entire process memory

Estimated **Memory** Retrieval file size: **4 MB**

**Retrieve** **Cancel**

- b. *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.

☒ Retrieve memory region from address:  to address:

- c. *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). For more details about device isolation, see [Investigation on page 106](#).



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.

### To isolate a device using the FortiEDR Collector:

1. In the *EVENT VIEWER* tab, select the checkbox(es) of the security event(s) that you want to isolate, and then click the *Forensics* button, as shown below:

**EVENTS**

ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
180497	Panda1	pandasecurityDx.dll	PUP	File Read Attempt	11-Feb-2020, 21:15:58	11-Feb-2020, 21:16:17
180468	Panda1	pandasecurityDx64.dll	PUP	File Read Attempt	11-Feb-2020, 21:14:04	11-Feb-2020, 21:16:17
180477	Panda1	pandasecurityDx.dll	PUP	File Read Attempt	11-Feb-2020, 21:14:04	11-Feb-2020, 21:14:04

**CLASSIFICATION DETAILS**

**PUP**  
By ReversingLabs  
Threat name: Win32.PUA.Netfilter  
Threat family: Netfilter  
Threat type: PUA

**History**

- PUP, by FortinetCloudServices, on 11-Feb-2020, 21:16:04
  - Simulation Device Panda1 was moved from collector group High Security Collector Group 2 times
  - Simulation Device Panda1 was isolated 2 times

**ADVANCED DATA**

Event Graph

Copyright © Fortinet Version 4.1.0.23 System Time (UTC -05:00) 11:46:58

The following window displays:

**Event 180468**  
pandasecurityDx64.dll

Raw Data Items: All Selected 1/1

DEVICE	OS	PROCESS	CLASSIFICATION	DESTINATION	RECEIVED	LAST SEEN
Panda1	Windows 8.1 Enterpris...	pandasecurityDx64.dll	PUP	File Read Attempt	11-Feb-2020, 21:14:04	11-Feb-2020, 21:16:17


RAW ID: 134177949 Process Type: 32 bit Certificate: Signed Process Path: C:\Program Files (x86)\pandasecurity\pandasecurityDx64.dll Count: 11

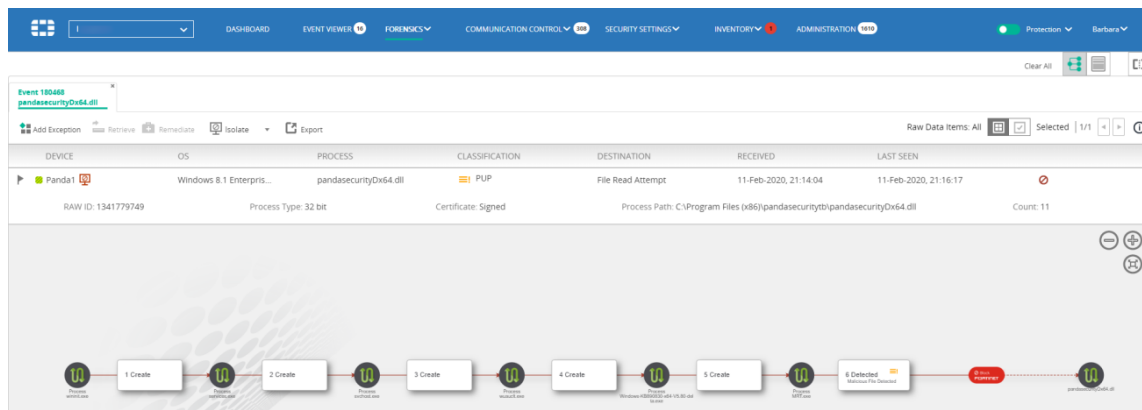
- In the *Events* tab, click the security event that you want to isolate, click the *Isolate* button dropdown arrow and then select *Isolate*. The following window displays:

**ISOLATE COLLECTORS**

Are you sure you want to isolate the selected collectors?

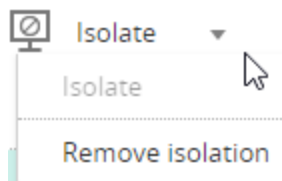
Isolate Cancel

- Click *Isolate*. A red icon  appears next to the relevant security event in the *Events* tab to indicate that the applicable Collector has been isolated, as shown below:

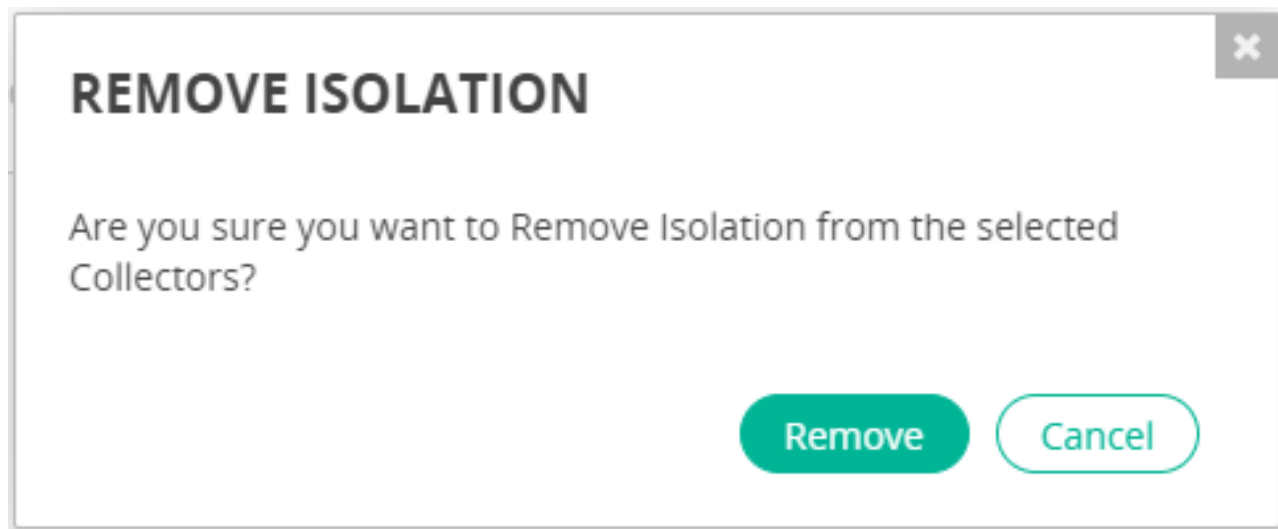


### To remove isolation from a device:

- In the *FORENSICS* tab, select the checkbox of the security event whose isolation you want to remove.
- Click the down arrow on the *Isolate* button and select *Remove isolation*, as shown below.



The following window displays:



- Click *Remove*.

## 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.

Select from the following FortiEDR's Threat Hunting options:

- [Threat Hunting on page 237](#)—Search for activities based on a security event's process or HASH, activity types, Process/File/Registry/Network or Event Log criteria. Use this option for a wide range of threat hunting capabilities for Collectors that run FortiEDR 5.0 or later.
- [Legacy Threat Hunting on page 265](#)—Hunt for files and hashes collected before the upgrade to 5.0 on Collectors that runs a FortiEDR version earlier than 5.0. This functionality is unavailable if all Collectors in your system run FortiEDR 5.0 or later.



Threat Hunting is a license-dependent add-on. You may contact [Fortinet Support](#) for more information.

---

## Threat Hunting

Threat Hunting significantly expands and enhances the capabilities of the Legacy Threat Hunting feature, which is described in [Legacy Threat Hunting on page 265](#). In addition to searching for activities based on a security event's process or HASH, you can also search for these activities based on a variety of activity types (such as Process Creation, File Deletion, Registry Value change, Socket Connect, and so on), as well as by Process/File/Registry/Network or Event Log criteria.

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 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 *Event Viewer*. Unlike Event Viewer security events, which are only reported in *Event Viewer* 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 92](#) 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 Bind.
Event Log Actions	The only action is Log Entry Created and relates to the logs of the operating system - Windows and Linux.

Access the *Threat Hunting* page under the *Forensics* tab by selecting the *Threat Hunting* option under the *Forensics* tab. The following page displays:

**THREAT HUNTING**

Category: All Categories | Device: All Devices | Search: 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

**All Activity (851.4K)** | Process (86.3K) | File (140.9K) | Network (5.7K) | Registry (592.9K) | Log (25.5K)

CATEGORY	TIME	OS	DEVICE NAME	TYPE	BEHAVIOR	PROCESS AND ATTRIBUTES	TARGET	EVENT ATTRIBUTES
File	15-May-2022 03:16:25	Windows	emc-100-117	Trace Entry Crea...		svchost.exe	Event ID 11	CHANNEL: Microsoft-Windows... LEVEL: 4 MESSAGE: Correlationid = {000...
File	15-May-2022 03:16:25	Windows	emc-100-117	Trace Entry Crea...		svchost.exe	Event ID 11	CHANNEL: Microsoft-Windows... LEVEL: 4 MESSAGE: Correlationid = ; Gro...
File	15-May-2022 03:16:25	Windows	emc-100-117	Trace Entry Crea...		svchost.exe	Event ID 11	CHANNEL: Microsoft-Windows... LEVEL: 4 MESSAGE: Correlationid = {000...
File	15-May-2022 03:16:25	Windows	emc-100-117	Trace Entry Crea...		svchost.exe	Event ID 11	CHANNEL: Microsoft-Windows... LEVEL: 4 MESSAGE: Correlationid = ; Gro...
Registry	15-May-2022 03:16:24	Windows	emc-100-117	Value Read		ngentask.exe	SOURCE PID: 11876	EDR.ATTRIBUTE.REGISTRY.PATH: HKLM\SOFTWARE\Classes\CLSID\{CF4CC4...
Registry	15-May-2022 03:16:24	Windows	emc-100-117	Value Read		ngentask.exe	SOURCE PID: 11876	EDR.ATTRIBUTE.REGISTRY.PATH: HKLM\SOFTWARE\Classes\CLSID\{CF4CC4...
Registry	15-May-2022 03:16:24	Windows	emc-100-117	Value Read		ngentask.exe	SOURCE PID: 11876	EDR.ATTRIBUTE.REGISTRY.PATH: HKLM\SOFTWARE\Classes\CLSID\{CF4CC4...
Registry	15-May-2022 03:16:24	Windows	emc-100-117	Value Read		ngentask.exe	SOURCE PID: 11876	EDR.ATTRIBUTE.REGISTRY.PATH: HKLM\SOFTWARE\Classes\CLSID\{CF4CC4...

The *Threat Hunting* page contains the following areas:

- [Filters on page 238](#)
- [Facets on page 249](#)
- [Activity events tables on page 252](#)
- [Details pane on page 256](#)
- The *Connect to Device* button opens a FortiEDR Connect (remote shell) session that provides direct access to the FortiEDR-protected device. See [Administration on page 274](#).

## 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:

THREAT HUNTING

CATEGORY

All Categories

DEVICE

ACWin10A

Enter a Lucene like syntax search expression,  
e.g. "RemoteIP: 10.151.121.130 OR RemotePort: 443"; "Source.File.ProductName: 'microsoft windows'"

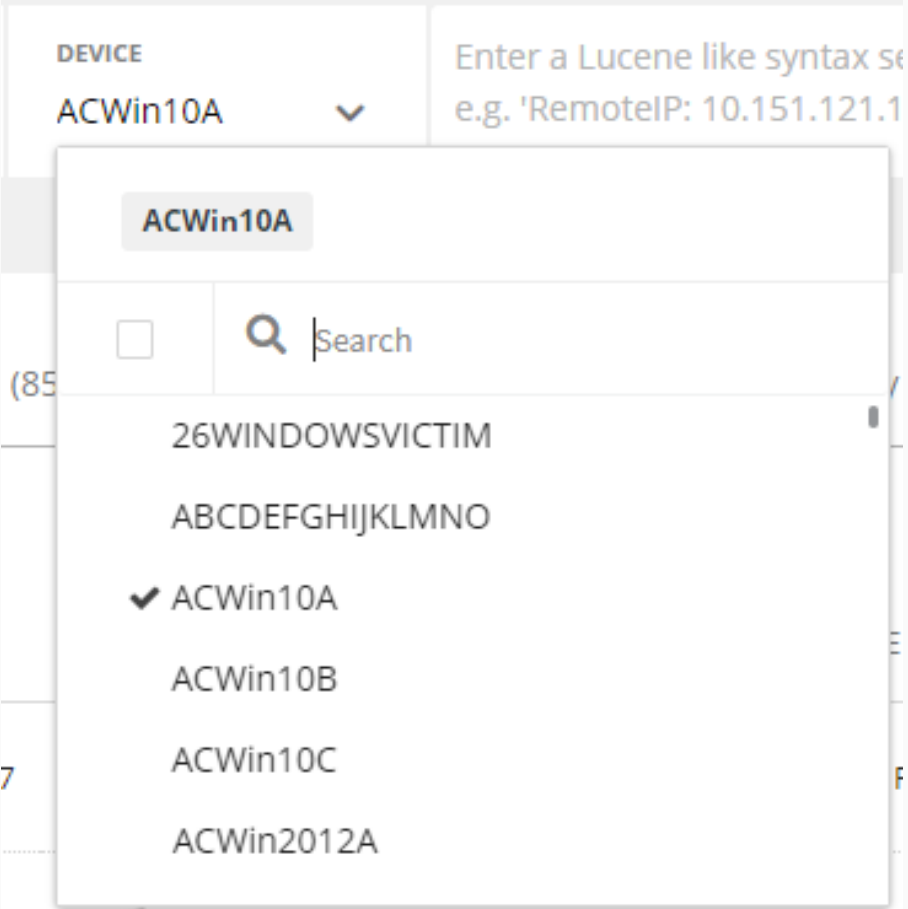
TIME

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 241](#).

Filter	Description
Category	<div>The <i>Category</i> filter enables you to filter the activity events by their category.</div> <div><div><div>CATEGORY</div><div>All Categories</div><div></div></div><div><div>✓ All Categories</div><div>Process</div><div>File</div><div>Registry</div><div>Network</div><div>Log</div></div></div>

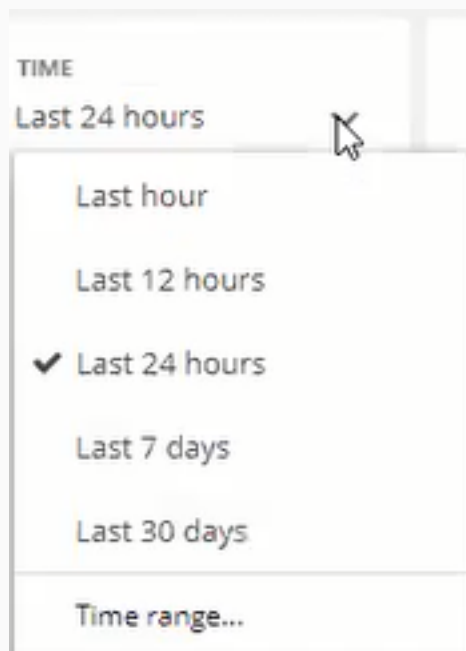
Filter	Description
	
Free-text Query	<p>This filter enables you to specify a free-text query to filter the results. This filter uses Lucene syntax. For details about the supported Lucene syntax features, see <a href="#">Appendix B - Lucene syntax on page 418</a>.</p> <div data-bbox="561 1314 1455 1367"> <p>Enter a Lucene like syntax search expression, e.g. 'RemoteIP: 10.151.121.130 OR RemotePort: 443'; 'Source.File.ProductName: "microsoft windows"'</p> </div> <p>To simplify query 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.</p>




Filter	Description
	<div> <input type="text" value="name"/> <div> 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 </div> </div> <div> <b>Target Process... (280.1K)</b>  git.exe 58.5K  conhost.exe 46.2K  chrome.exe 22K  teams.exe 15K  proxyhost.exe 10.5K  More (13) </div>

### Time

The *Time* filter enables you to filter for a specific time period. The default is the last hour.



To clear the contents of all the filters in the *Filters* area, at the far right of the page, click the eclipis 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:

Description:

Tags: +

Organization: ☒ ensllofordev ☐ All Organizations

Full Query

Category:  Device:  Time:

☐ 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 Event Viewer.



These tags only relate to saved queries.

Tags



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

Tags

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:

Tags

To unassign 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:

Tags

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 *Event Viewer* 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

Save Cancel

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	<p>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 Event Viewer, as described in <a href="#">Classification Details on page 183</a>. They can be:</p> <ul style="list-style-type: none"> <li>• Malicious</li> <li>• Suspicious</li> <li>• Inconclusive</li> <li>• Likely Safe</li> <li>• PUP (Potentially Unwanted Program)</li> <li>• Safe</li> </ul>
Repeat Every/On	<p>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.</p>

Field	Definition
Trigger Playbook Actions	<p>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.</p> <p>Configure the following options:</p> <ul style="list-style-type: none"> <li>• <i>Terminate Process</i>—Specifies which process in the Activity Event, which resulted from the execution of the saved query, should be terminated: <ul style="list-style-type: none"> <li>• <i>Source Process</i></li> <li>• <i>Source Process Parent</i></li> <li>• <i>Target Process</i></li> </ul> </li> <li>• <i>Delete File</i>—Specifies which file in the Activity Event, which resulted from the execution of the saved query, should be deleted: <ul style="list-style-type: none"> <li>• <i>Source Process File</i></li> <li>• <i>Target File</i></li> <li>• <i>Target Process File</i></li> <li>• <i>Target Executable Image File</i></li> </ul> </li> </ul>

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	Community	Scheduled	Unscheduled	
Set state		Delete				
NAME		MATCHES	DEVICES	LAST RESULT	REPEAT EVERY	LAST UPDATED
Target Path		1.27M	18	04-Feb-2021 05:37:48		04-Feb-2021, 05:37 by Galit
There is a Behavior	BadWolf	2K	15	04-Feb-2021 05:35:47		04-Feb-2021, 05:35 by Galit
Credential access [Edited]	BadWolf	3	2	07-Feb-2021 10:15:00	15 minute	04-Feb-2021, 05:52 by Galit
						Disabled




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**.



- 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					

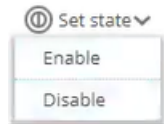
- You can filter this list of saved queries by typing into the *Search* field and/or selecting one of the following options:
  - FORTINET**/User: To select **FORTINET** defined queries. Selecting *User* filters by saved queries that were created by a user.
  - Scheduled/Unscheduled*: To specify that 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.
  - 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.
- You can modify a saved query by hovering over it. The following tools are displayed on the right of the row:

Credential access by	228	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 <i>Saved Query</i> definition.

Tool	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 <b>Delete</b>  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.

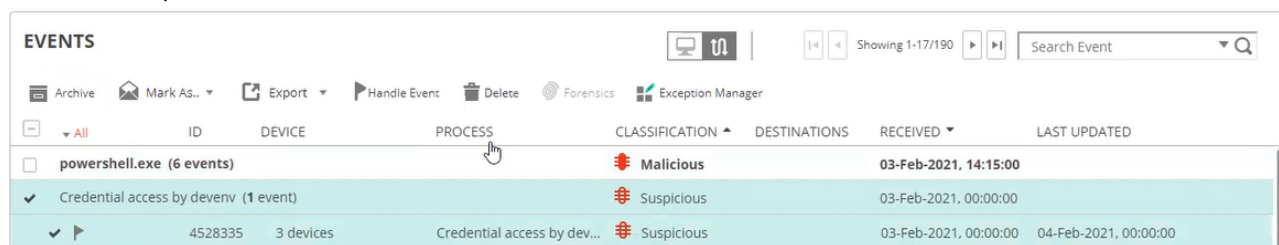


## Scheduled queries

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 *Event Viewer*, 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 *Event Viewer* is similar to a standard security event, except for the following:

- The following options are not available in the *Event Viewer* for saved query security events:
  -  **Forensics** The Forensics option is not available because it is irrelevant.
  -  **Exception Manager** An exception cannot be defined for saved query security events.
- In the Process View  of the *Event Viewer*, a saved query security event shows the name of the saved query instead of the process name, as shown below:

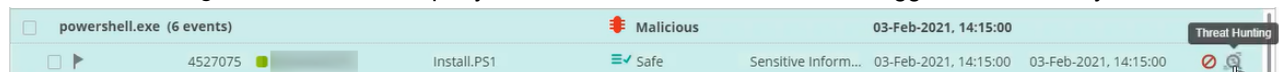


ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
powershell.exe (6 events)			Malicious		03-Feb-2021, 14:15:00	
Credential access by devenv (1 event)			Suspicious		03-Feb-2021, 00:00:00	
4528335	3 devices	Credential access by dev...	Suspicious		03-Feb-2021, 00:00:00	04-Feb-2021, 00:00:00

The classification (in the *CLASSIFICATION* column) is determined by the definition of the saved query.

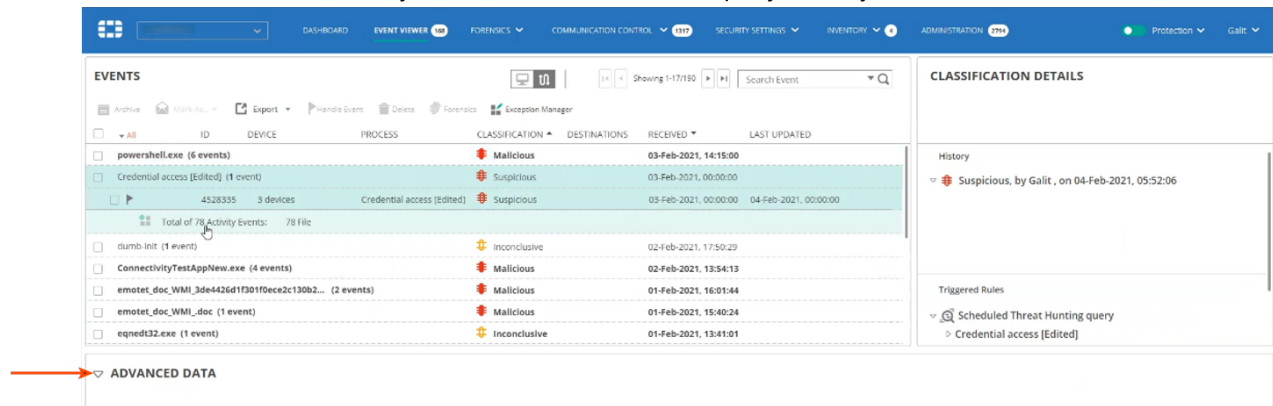
In the same manner as other security events it indicates the quantity of devices (in the *DEVICE* column) on which this type of activity events were found. All other aspects of a saved query security event are the same as other security events.

- Clicking the **Threat Hunting** option on the right side of the saved query security event in the *Event Viewer* displays the **Threat Hunting** tab and the saved query that was run, because that is what triggered the security event.

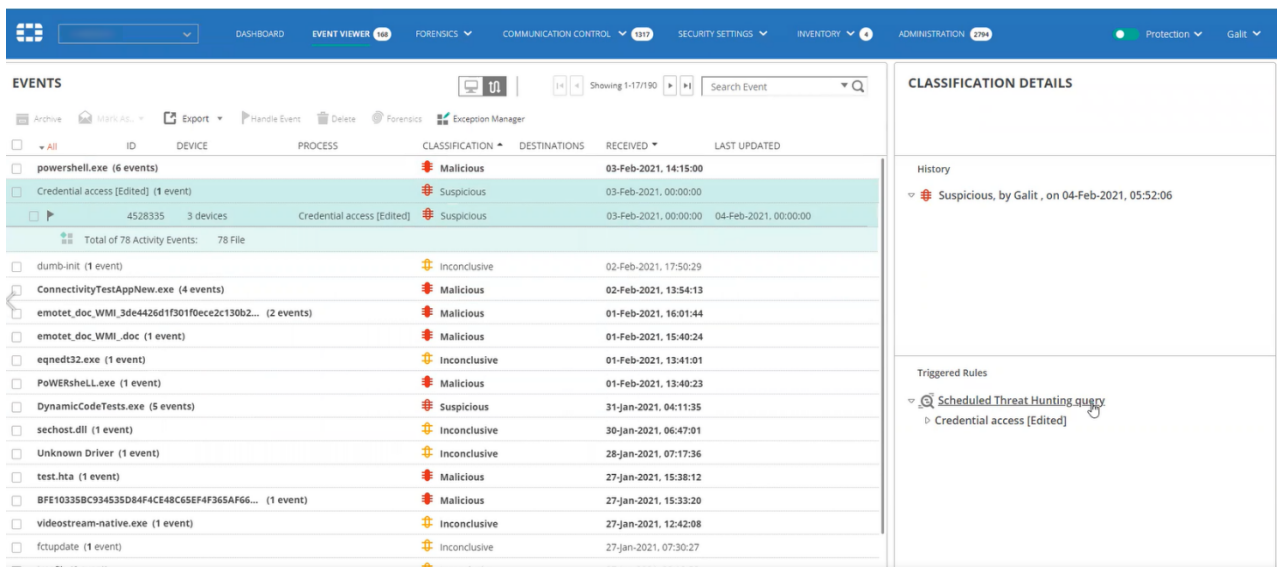


ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
powershell.exe (6 events)			Malicious		03-Feb-2021, 14:15:00	
4527075	3 devices	Install.PS1	Safe	Sensitive Inform...	03-Feb-2021, 14:15:00	03-Feb-2021, 14:15:00

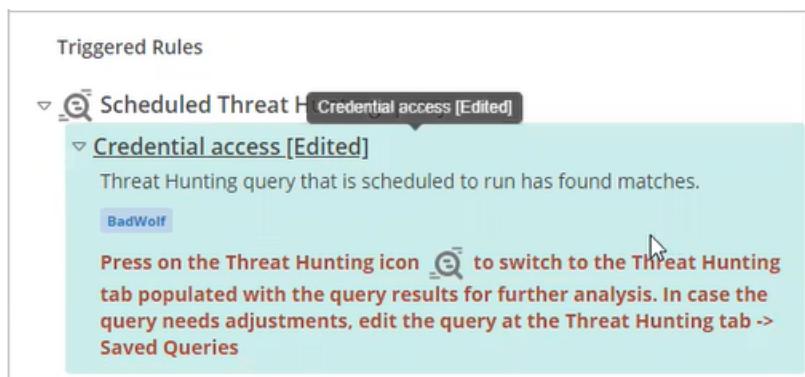
- The *Event Viewer* does not show any advanced data for a saved query security event.




- Triggered Rules:** When a saved query security event is selected in the *Event Viewer*, 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:

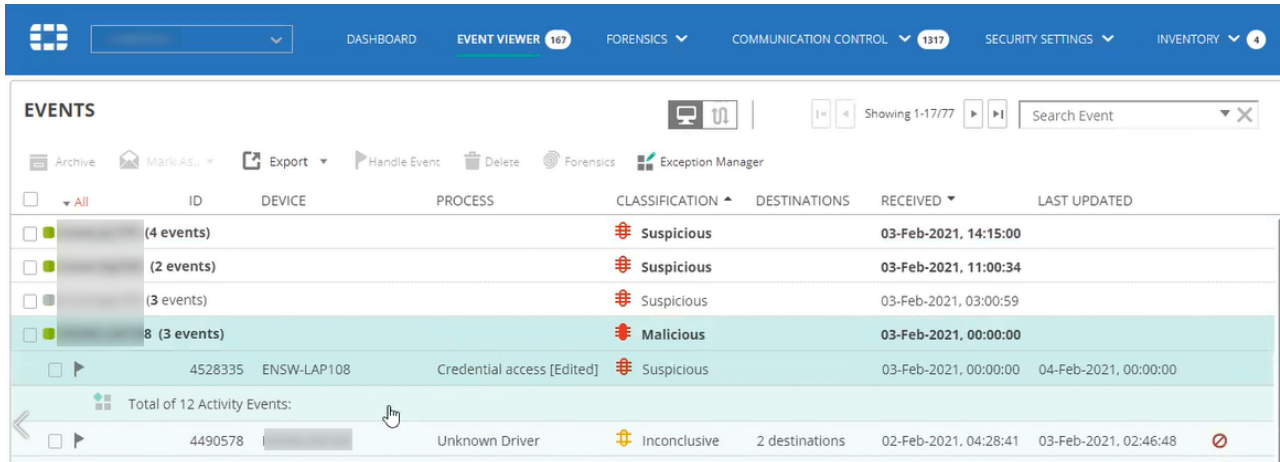


The name of the saved query is listed below it. Click that saved query's name (for example, *Credential Access (Edited)*) to display additional details about this saved query, such as its description and the tags that were defined when it was created/modified, as shown below:





- In the **Device View**  of the **Event Viewer**, 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, as shown below:



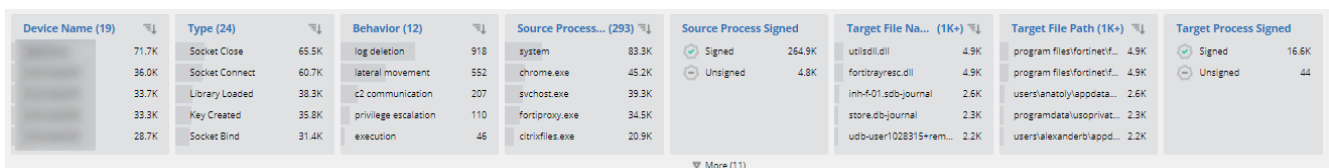
ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
(4 events)			Suspicious		03-Feb-2021, 14:15:00	
(2 events)			Suspicious		03-Feb-2021, 11:00:34	
(3 events)			Suspicious		03-Feb-2021, 03:00:59	
8 (3 events)			Malicious		03-Feb-2021, 00:00:00	
4528335	ENSW-LAP108	Credential access [Edited]	Suspicious		03-Feb-2021, 00:00:00	04-Feb-2021, 00:00:00
Total of 12 Activity Events:						
4490578		Unknown Driver	Inconclusive	2 destinations	02-Feb-2021, 04:28:41	03-Feb-2021, 02:46:48

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
71.7K	Socket Close 65.5K	log deletion 918	system 83.3K	Signed 264.9K	utilsdll.dll 4.9K	program files\fortinet\... 4.9K	Signed 16.6K
36.0K	Socket Connect 60.7K	lateral movement 552	chrome.exe 45.2K	Unsigned 4.8K	fortitrayres.dll 4.9K	program files\fortinet\... 4.9K	Unsigned 44
33.7K	Library Loaded 38.3K	c2 communication 207	svchost.exe 39.3K		inh-f01.sob-journal 2.6K	users\lanetoly\appdata... 2.6K	
33.3K	Key Created 35.8K	privilege escalation 110	fortiproxy.exe 34.5K		store.ob-journal 2.3K	programdata\usoprivat... 2.3K	
28.7K	Socket Bind 31.4K	execution 46	ctbtfilx.exe 20.9K		udb-user1028315+rem... 2.2K	users\alexanderblappd... 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		git.exe 81	0003022b 1	hkim\system\controlset... 182		sz 411
privilege escalation 9	File Write 2899		chrome.exe 48	0003031f 1	hkim\software\microsoft... 88	0	dw 290
scripting 4	File Create 2674		conhost.exe 28	00036604 1	hkim\software\microsoft... 70	3	bin 258
lateral movement 3	Executable Loaded 2367		svchost.exe 14	000b6659 1	hkim\system\controlset0... 48	65538	exsz 60
reconnaissance 2	File Delete 1474		backgroundtaskhost.exe 12	001f664a 1	hkim\software\microsoft... 46	03000c0000041007500... 16	qw 57
<div>More (10)</div>							

▼ 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	12878	git.exe 81	0003022b 1	hkim\system\controlset... 182	560	sz 411
privilege escalation 9	File Write 2899	9763	chrome.exe 48	0003031f 1	hkim\software\microsof... 88	0	dw 290
scripting 4	<b>File Create</b> X		conhost.exe 28	00036604 1	hkim\software\microsof... 70	3	bin 258
lateral movement 3	Executable Loaded 2367		svchost.exe 14	0006659 1	hkim\system\controlset0... 48	65538	exsz 60
reconnaissance 2	File Delete 1474		backgroundtaskhost.exe 12	001f664a 1	hkim\software\microsof... 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.

Type: File Create						
Type (2674) ▾	Device Name (2674) ▾	Source Process Fi... (2674) ▾	Source Process Signed	Source Process Architecture	Source Process P... (2674) ▴	
File Create 2674	1354	1410	✓ Signed 2670	64 bit 64 bit 2521	adobe reader and acrobat... 1	
	1320	784	✗ Unsigned 4	32 bit 32 bit 153	dropbox update 2	
		463			forticlient auto-update ag... 3	
		9			slack 3	
		8			microsoft edge 4	

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.

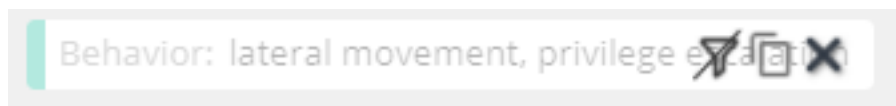
Type: File Create										NOT Source Process File Owner: administrators, ensilo\galit									
Type	(1264)	Device Name	(1264)	Source Process Fi...	(1264)	Source Process Signed	Source Process Architecture	Source Process P...	(1264)										
File Create	1264		54		784	Signed	64 bit 64 bit 1216	adobe reader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

Target Process Name: chrome.exe, teams.exe		
Process (2.5K)	Device Name (2.5K)	Target Process... (2.5K)
Process Termination 1.3K		chrome.exe 1.8K
Process Creation 1.3K		teams.exe 750

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




















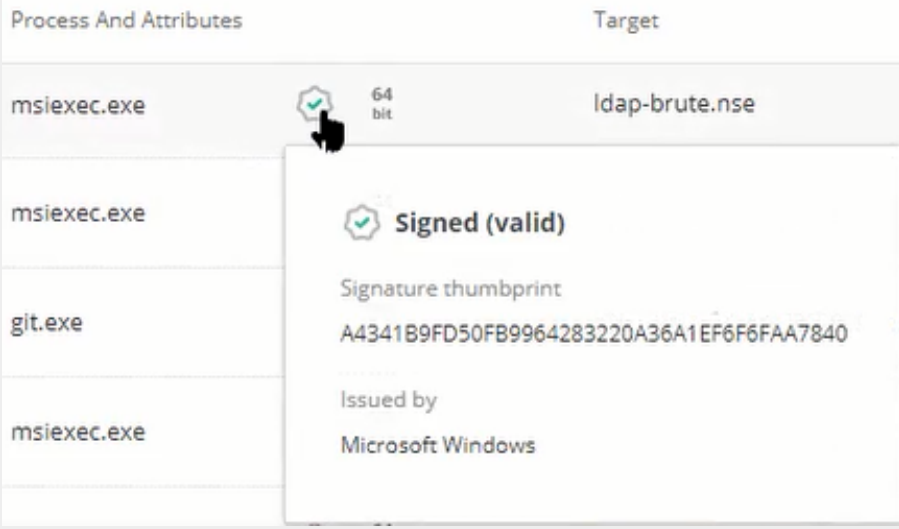

Tool	Definition
Remove	The chip is removed and the Facets and Result tables are updated accordingly.
Disable	A disabled chip no longer affects the results. The Facets and the Results tabs are updated as if the chip was removed and the chip appears as follows: <div> Type: File Read, Socket Connect </div>
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		ENDW-LAP119	File Read		SelfElectController.exe  32 bit	downloadermulticast
	12-Jan-2021, 06:05:16		EU-HKCSL13	File Read		TaskbarX.exe  32 bit	Accessibility.api
	12-Jan-2021, 06:05:16		EU-HKCSL13	File Read		dllhost.exe  64 bit	oleacc.dll
	12-Jan-2021, 06:05:16		LIGD-NewPC	File Read		uihost.exe  64 bit	Local State

Category	Definition
All Activity	<p>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:</p> <ul style="list-style-type: none"> <li>•  Process</li> <li>•  File</li> <li>•  Registry</li> <li>•  Network</li> <li>•  Log</li> </ul> <p>You can hover over the icon in the <i>Process and Attributes</i> column to temporarily display additional details about the source process, including whether it is signed, its signature, issuer and so on.</p>  <p>The screenshot shows a table with two columns: 'Process And Attributes' and 'Target'. The first row shows 'msiexec.exe' with a green checkmark icon and '64 bit' next to it, and 'ldap-brute.nse' in the target column. A tooltip is displayed over the green checkmark icon, showing 'Signed (valid)', 'Signature thumbprint: A4341B9FD50FB9964283220A36A1EF6F6FAA7840', and 'Issued by: Microsoft Windows'.</p> <p> There are several types of attribute icons, such as Signed/Unsigned.</p>
Process	This tab shows all matching activity events of category Process.
File	This tab shows all matching activity events of category File.

Category

Definition

All Activity (389,76)Process (26,29)File (258,96)Network (78,96)Registry (24,66)Event Log (76)

TIME

OS

DEVICE NAME

TYPE

BEHAVIOR

SOURCE PID

PROCESS AND ATTRIBUTES

TARGET FILE NAME

TARGET FILE PATH

17-Jan-2021, 09:41:02

Windows 10

WIN-10-01

File Read

5980

SService.exe

64 bit

SecurDoc.H

Program Files\WinMagiSecur...

17-Jan-2021, 09:41:02

Windows 10

WIN-10-01

File Read

5980

SService.exe

64 bit

SecurDoc.H

Program Files\WinMagiSecur...

17-Jan-2021, 09:41:02

Windows 10

WIN-10-01

File Read

5980

SService.exe

64 bit

SecurDoc.H

Program Files\WinMagiSecur...

17-Jan-2021, 09:41:02

Windows 10

WIN-10-01

File Read

5980

SService.exe

64 bit

SecurDoc.H

Program Files\WinMagiSecur...

17-Jan-2021, 09:41:02

Windows 10

WIN-10-01

File Read

5980

SService.exe

64 bit

SecurDoc.H

Program Files\WinMagiSecur...

17-Jan-2021, 09:41:02

Windows 10

WIN-10-01

File Read

9408

AdobeCollabSync.exe

32 bit

Synchronizer

Users\gato\AppData\LocalLow...

Choose Columns

Network

This tab shows all matching activity events of type Network.

Registry

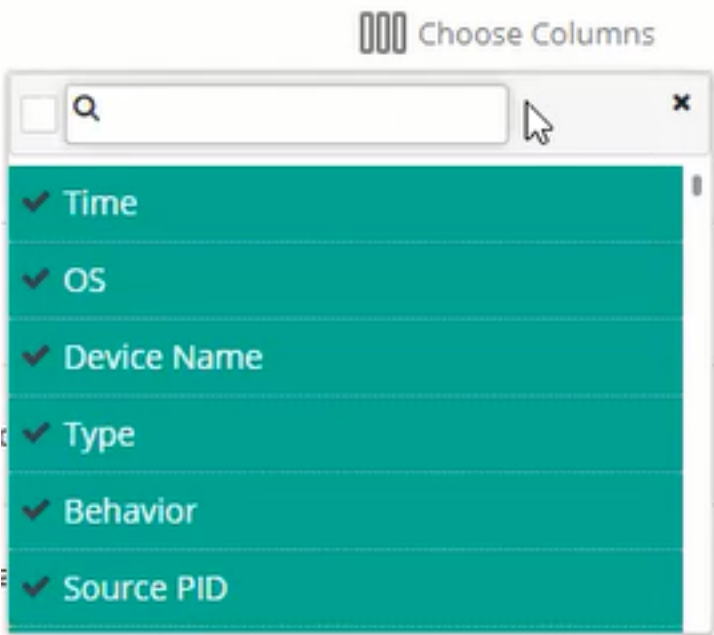
This tab shows all matching activity events of type Registry.

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.



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:

IS	DEVICE NAME	TYPE	BEHAVIOR	MITRE TACTIC	MITRE TECHNIQUE	PRI
	Ensat-PC	File Delete	Log deletion	Defense Evasion	Indicator Removal on Host: File Deletion	sla
	ensat-lap183	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 256](#) (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:

Ensat-PC

Status Running
Internal IP 10.0.0.22

Up time 2d, 48min, 28sec

**SearchApp.exe**

PID-16372 TID-18348
64 bit

Path C:\Windows\SystemApps\Microsoft.Windows.Search\_cw5n1h2txyewy\Se...

Executing user ENSLO\Ensat

Product Microsoft® Windows® Operating System

SHA1 BA56CAAD49E3601259D4043CCAF41E6E01841C3D

Command line -
ServerName:CortanaUI.AppX8z9r6jm96hw4bsbneegw0kyxx296wr9t....

**Process Creation**

**File Read**

Credential Access

Summary
→ proxyhost.exe
2020, 04:23

Ensat-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 250](#).

BEHAVIOR	SOURCE PID	PROCESS AND ATTRIBUTES
Privilege escalati...	5056 + -	OUTLOOK.EXE
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.

The screenshot displays the FortiEDR interface. At the top, there's a navigation bar with tabs like DASHBOARD, EVENT VIEWER, FORENSICS, COMMUNICATION CONTROL, SECURITY SETTINGS, INVENTORY, and ADMINISTRATION. Below this, the 'THREAT HUNTING' section is active, showing a table of activity events. The table has columns for CATEGORY, TIME, OS, DEVICE NAME, TYPE, PROCESS AND ATTRIBUTES, TARGET, and EVENT ATTRIBUTES. A row for 'TaskbarX.exe' is selected, highlighted with a green border on its left. To the right of the table, the 'Details pane' is open, showing a 'Summary' tab with information about the selected event, including its status (Running), up time, and command line.

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 ProgramDataL...
12-Jan-2021, 06:05:16	EU...	File Read	TaskbarX.exe	32 bit	Ac...	SOURCE PID 22900	PATH Program Files (...)
12-Jan-2021, 06:05:16	EU...	File Read	dllhost.exe	64 bit	ole...	SOURCE PID 17904	PATH Windows/Syste...
12-Jan-2021, 06:05:16	LI...	File Read	uihost.exe	64 bit	Lo...	SOURCE PID 7812	PATH ...
12-Jan-2021, 06:05:16	LI...	File Read	uihost.exe	64 bit	Pr...	SOURCE PID 7812	PATH ...
12-Jan-2021, 06:05:16	LI...	File Read	uihost.exe	64 bit	Se...	SOURCE PID 7812	PATH ...
12-Jan-2021, 06:05:16	LI...	File Read	uihost.exe	64 bit	Lo...	SOURCE PID 7812	PATH ...

**Details pane - Summary**

- Status: Running
- Up time: 5d, 21h, 3min, 10sec
- Internal IP: 1...
- Path: C:\Downloads\TaskbarX\_1.6.2.0\TaskbarX.exe
- Executing user: ...
- Parent: \Device\HarddiskVolume3\Windows\System32\svchost.exe
- Product: TaskbarX
- SHA1: 5E9E7421875B46C2E1007B8C4E0B00A3900498BF
- Command line: dba=4 -color=63,0,0,73 -as=cubiceaseinout -obas=cubiceaseinout -asp=300 -pbo=0 -sbo=0 -lr=400 -olr=400 -ar=0 -fotcc=1

The Details pane for an activity event contains a *Summary* tab and one or two other tabs, as follows:



**Action Behavior and MITRE**

File Read | Credential Access **M**

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

Status **Running** Internal IP 10.212.134.130,192.168.0....

Up time 3d, 1h, 23min, 24sec

**Source**

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

**Action (Event Type)**

File Read

**Target**

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.

File Read

Credential Access

M

Summary

→ **msiexec.exe**

→ ms-sql-empty-pa...

2020-Oct-25 08:31:23

---

msiexec.exe

PID-4424

64 bit

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.

The screenshot shows the 'File Read' tab in the FortiEDR interface. The breadcrumb trail is 'Summary' → 'msiexec.exe' → 'ms-sql-empty-p...'. The timestamp is '2020-Oct-25 08:31:23'. The main title is 'ms-sql-empty-password.nse'. Below this, a table lists file details:

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:

This screenshot shows the 'File Read' tab with the breadcrumb trail 'Summary' → 'msiexec.exe' → 'ldap-brute.nse'. The timestamp is '2020-Oct-25 08:31:23'. A process is shown as 'Running' with a duration of '1h, 23min, 24sec' and an 'Internal IP' of '10.212.134.130,192.168.0....'. A popup window displays details for a 'Signed (valid)' file:

<b>Signed (valid)</b>	-4424	64 bit
Signature thumbprint	A4341B9FD50FB9964283220A36A1EF6F6FAA7840	
Issued by	Microsoft Windows	
Command line	/V	

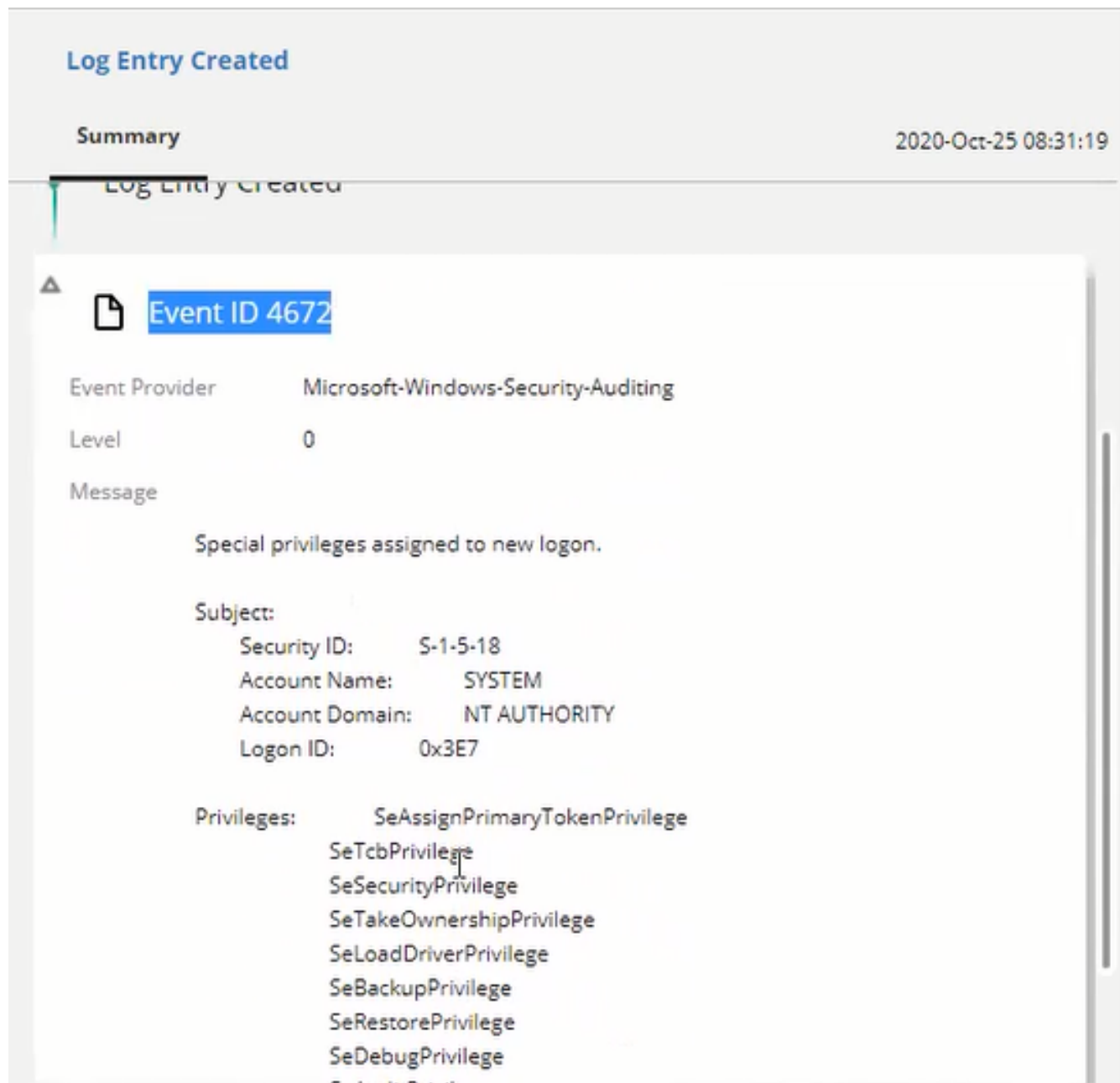
## Event Log Details pane

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.

The screenshot shows the 'Log Entry Created' details pane. At the top, the title 'Log Entry Created' is displayed in blue. Below it, the 'Summary' tab is selected, showing a status of 'Running' (indicated by a green dot) and an 'Up time' of '3d, 1h, 23min, 20sec'. The 'Internal IP' is listed as '10.212.134.130, 192.168.0...'. A 'Security' icon is visible. The main event is 'Log Entry Created', with a file icon and 'Event ID 4672'. The event details are as follows:

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.

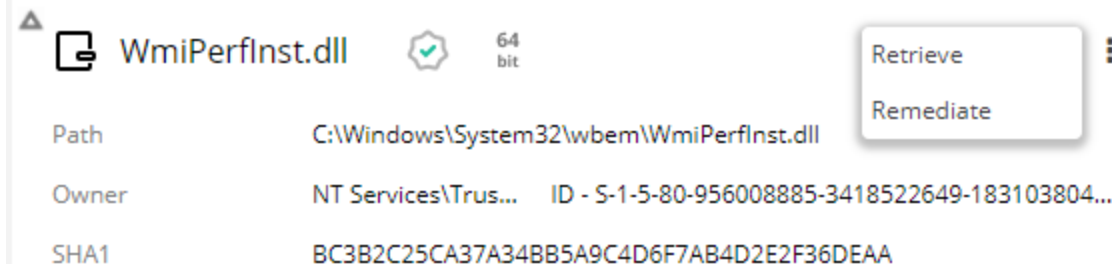


### Retrieving a file / Remediating devices upon malware detection

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.

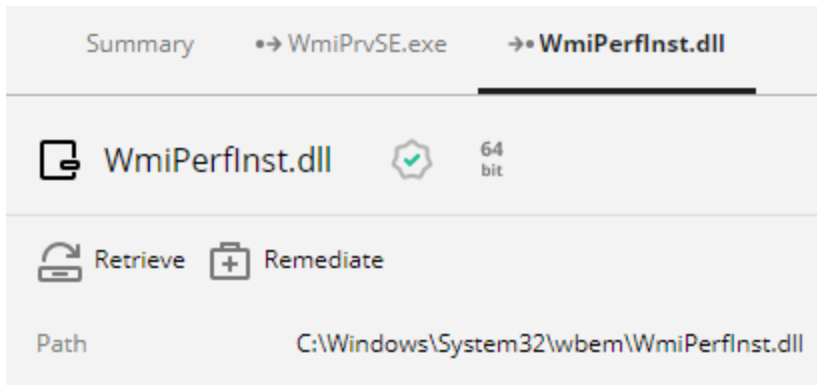
**To retrieve a file or remediate the process:**

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* or *Remediate* the file, as shown below:



– OR –

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

**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:

The screenshot displays the 'File Create' window in FortiEDR. At the top, there's a 'Summary' tab and navigation links for 'Adobe CEF He...' and 'ACC 2022-1-1...'. The date and time '14-Jan-2022 03:54:17' are shown in the top right. Below the summary, a process card for 'Adobe CEF Helper.exe' is visible. It shows the status as 'Running' with a green dot, an internal IP of '10.100.102.6', and an uptime of '3d, 1h, 27min, 43sec'. A detailed view of the process is expanded below, showing fields like Path, Executing user, Parent, Product, SHA1, and Command line. The 'Add to Blocklist' button is highlighted in the top right of the process details panel.

**File Create**

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

ens...    Status **Running**    Internal IP 10.100.102.6

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

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

Path C:\Program Files\Common Files\Adobe\Adobe Desktop Comm...

Executing user ENSILO\yc

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:

**File Create**

Summary
→ Adobe Desk...
→ longpoll[9].json
24-Jan-2022 16:38:02

---

Adobe Desktop Service.exe
PID-13868 TID-10764

32 bit

---

Add to Blocklist

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
EI O\

Executing User ID
S-1-5-21-4952-3892803170-2759984830-2235

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 > Tools > 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>"

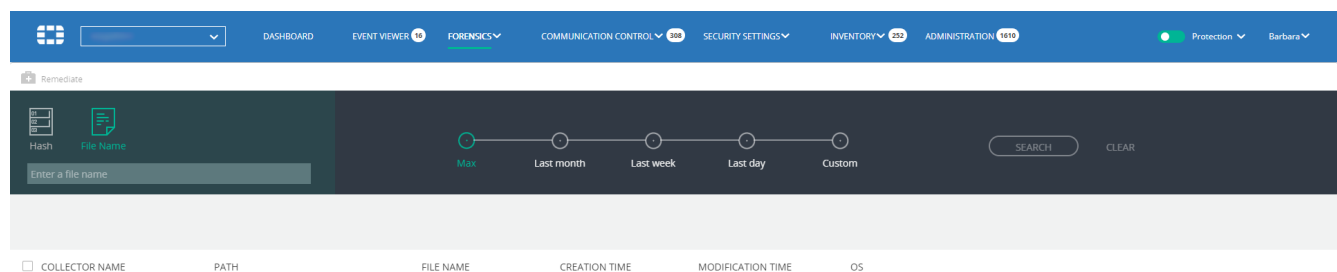
Similarly, to find all activity related to an IP chosen from a Personal Data Handling Activity Report, enter the following query:

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



## Legacy Threat Hunting

If your FortiEDR environment has recently upgraded and one or more Collectors in your system run a FortiEDR version earlier than 5.0, Legacy Threat Hunting allows you to hunt for files and hashes on those Collectors that were collected before you upgrade to 5.0 from earlier versions. Access the *Threat Hunting Legacy* page by clicking *Forensics > Threat Hunting Legacy*. If all Collectors run FortiEDR 5.0 or later, the *Legacy Threat Hunting* option is unavailable. Use the FortiEDR's [Threat Hunting on page 237](#) feature instead in this case, which has more extensive collected data.

The following shows the *Legacy Threat Hunting* page. In this case, the *Hash/Process* field is empty.



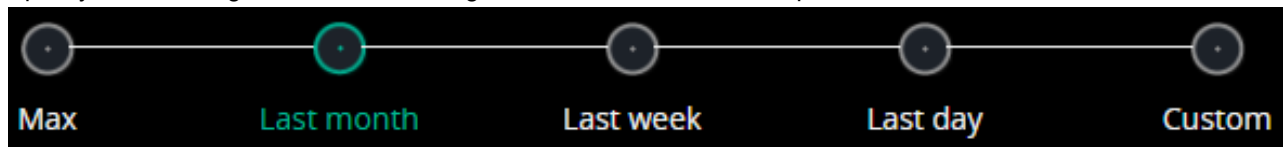
### To search for malware using Threat Hunting (legacy):

- Select the basis for the search by clicking the *Hash* () or *File Name* () button. When you select the *Hash* button, the search results represent matching HASH values. When you select the *File Name* button, the search results represent matching filenames.

When accessing the *Threat Hunting* page using Method 1, the relevant HASH value appears in the field adjacent to the *Hash* button, as shown below.

When accessing the *Threat Hunting* page using Method 2, the field adjacent to the *Hash* and *File Name* buttons is empty.
- If the field adjacent to the *Hash* and *File Name* buttons is empty, copy and paste the applicable filename or HASH value into the empty field.

3. Specify the time range for the search using the timeline buttons at the top of the window.



4. Click the **Search** button. The system searches for matching files in all devices in your environment. When the search completes, the search results display in the window. The example below shows a search by process.

COLLECTOR NAME	HASH	PATH	FILE NAME	CREATED	MODIFIED	SIZE	OS	BIT	CERTIFICATE	VENDOR	PRODUCT	VERSION
Avast1	4EAC2C767ED8489C165E5...	...iskvolume2\users\root\desktop	dynamiccode.exe	20-Feb-2017, 04:57	30-Apr-2015, 05:37	549376	Windows 8.1 Enterprise N	32	No			
McAfee1	4EAC2C767ED8489C165E5...	...olume2\users\mcafee2\desktop	dynamiccode.exe	14-Mar-2017, 12:04	30-Apr-2015, 05:37	549376	Windows 10 Enterprise 20...	32	No			
McAfee1	4EAC2C767ED8489C165E5...	...users\mcafee2\desktop\events	dynamiccode.exe	23-May-2017, 08:12	30-Apr-2015, 05:37	549376	Windows 10 Enterprise 20...	32	No			
Panda1	4EAC2C767ED8489C165E5...	...iskvolume2\users\root\desktop	dynamiccode.exe	20-Feb-2017, 04:57	30-Apr-2015, 05:37	549376	Windows 8.1 Enterprise N	32	No			

The row directly above the results table summarizes the results of the search. For example, in the window above, the system found 2 unique devices and one unique path created in the same one week. The example below shows the results of a search by HASH.

SHA-1	BIT	SIZE	IS SIGNED	VENDOR	PRODUCT	VERSION
90197E2FD04B2189F96ECF300E04E01ED9B14B82	32	56028615	No			

COLLECTOR NAME	PATH	FILE NAME	CREATION TIME	MODIFICATION TIME	OS
WIN-UBASCL011R	\\device\\harddiskvolume1\\qat\\filebeatlogs\\filebeat	filebeat.exe	09-jul-2019, 07:25	20-jun-2019, 11:06	Windows 8 Enterprise
WIN-7K1E9518QB8	\\device\\harddiskvolume1\\qat\\filebeatlogs\\filebeat	filebeat.exe	08-jul-2019, 09:56	20-jun-2019, 11:06	Windows 7 Professional N

The labels row directly above the summary row identifies common, shared data elements. For example, Sha-1, vendor, and so on. The identified elements are shared by all files. Note that typically you see more common data elements when searching by HASH than by process.

SHA-1	BIT	SIZE	IS SIGNED	VENDOR	PRODUCT	VERSION
90197E2FD04B2189F96ECF300E04E01ED9B14B82	32	56028615	No			

COLLECTOR NAME	PATH	FILE NAME	CREATION TIME	MODIFICATION TIME	OS
WIN-UBASCL011R	\\device\\harddiskvolume1\\qat\\filebeatlogs\\filebeat	filebeat.exe	09-jul-2019, 07:25	20-jun-2019, 11:06	Windows 8 Enterprise
WIN-7K1E9518QB8	\\device\\harddiskvolume1\\qat\\filebeatlogs\\filebeat	filebeat.exe	08-jul-2019, 09:56	20-jun-2019, 11:06	Windows 7 Professional N

## 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 the *INVENTORY* tab, the *FORENSICS* tab, and the *Threat Hunting* page under the *FORENSICS* tab.

- 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 267](#).
- 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 > Tools*, ensure that the *Allow FortiEDR Connect – Remote Shell Connection* checkbox is selected, which enables the FortiEDR Connect functionality for the organization. See [Tools on page 317](#).



- Select the *Establish FortiEDR Connect sessions* checkbox in the user profile to grant the user access to the FortiEDR Connect functionality. See [Users on page 285](#).



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:

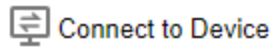
1. A FortiEDR Connect console can be accessed from various FortiEDR pages that list devices, such as the *INVENTORY* tab, the *FORENSICS* tab, and the *Threat Hunting* page under the *FORENSICS* tab. The operation of the FortiEDR Connect console is the same regardless of where it was accessed from.
2. 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.

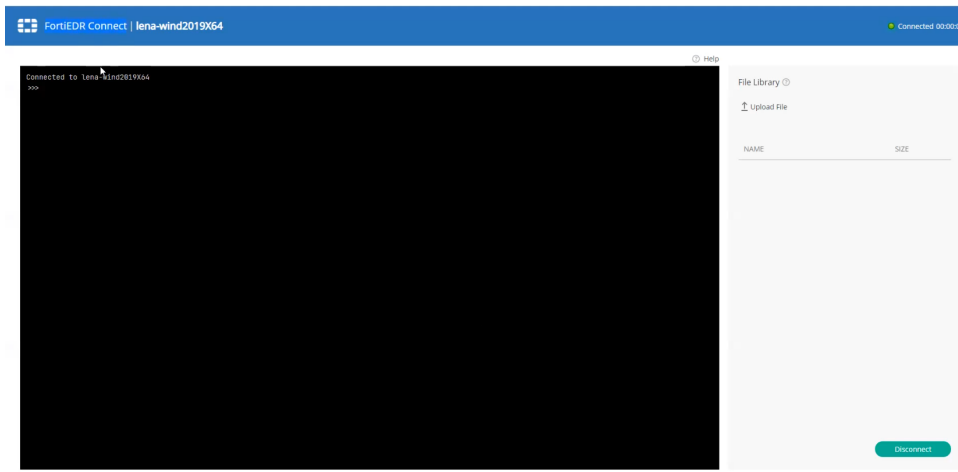


If the list only displays a single device, then the *Connect to Device* button automatically applies to that device without you needing to select it.

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



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:



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			X
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.	

Close

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 317](#) feature records the connection of a FortiEDR Connect session, but not 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 272](#). 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

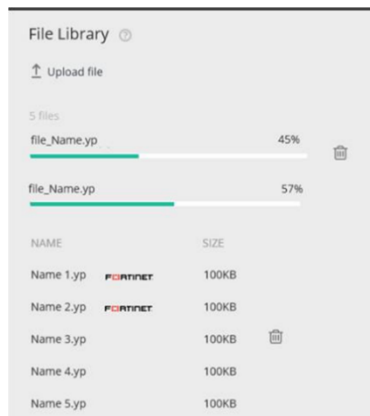
The *File Library* page lists the files that you have uploaded to the FortiEDR file library on the FortiEDR Manager during the current FortiEDR Connect sessions, and that are available to be uploaded on the devices.



## 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 277](#).
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.



- 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 267](#).
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 270](#). 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.
```

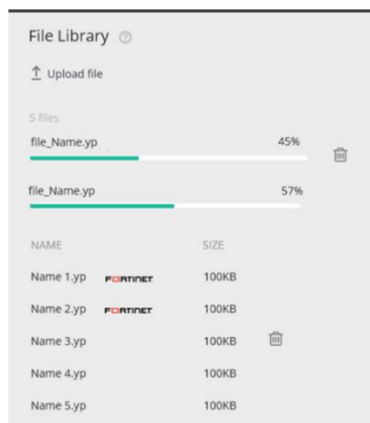
## Download a file from a FortiEDR-protected device

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 267](#). 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.



## Disconnecting FortiEDR Connect session

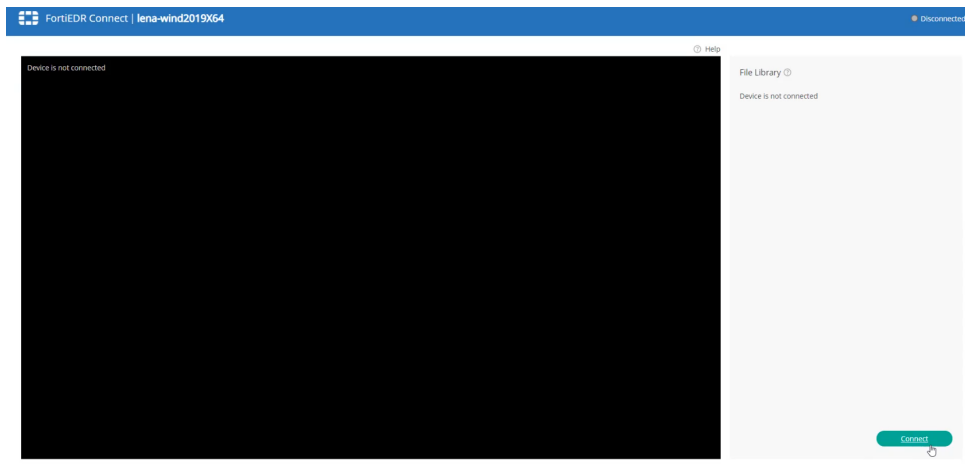
### Disconnect a FortiEDR Connect session in one of the following ways:

- 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:





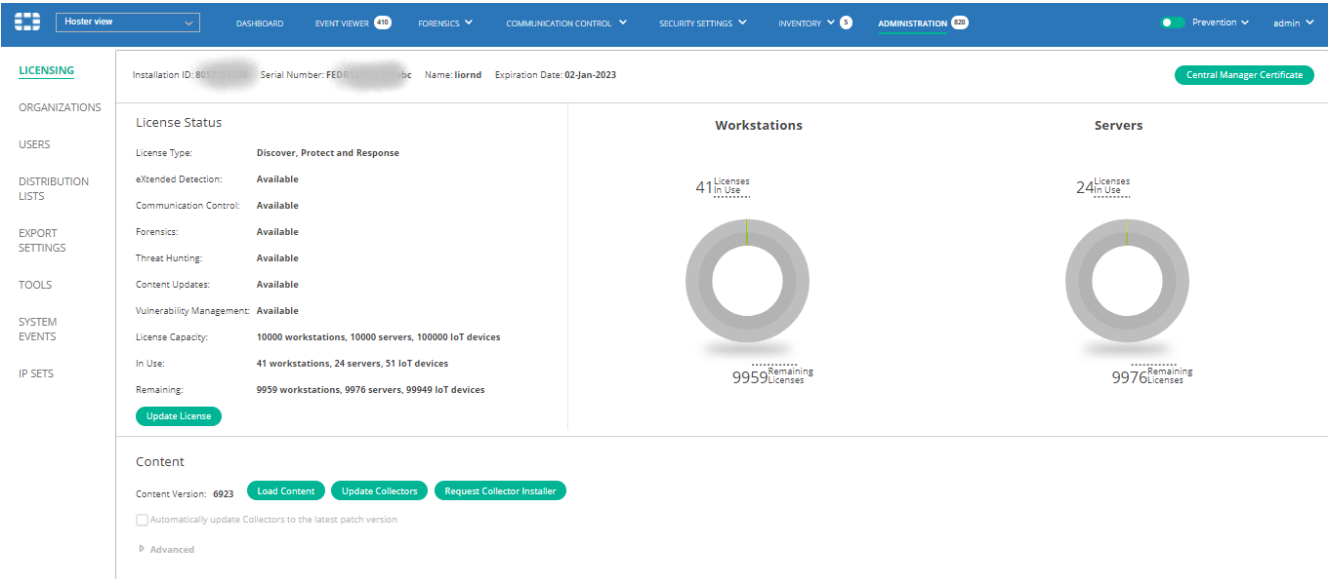
# Administration

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.



Field	Description
<i>Installation ID</i>	Specifies the unique identifier that is automatically generated upon installation of the FortiEDR Management server. You may be asked to provide this ID and the <i>Name</i> field when contacting Fortinet for support.
<i>Name</i>	Specifies the name of the organization in a multi-organization FortiEDR system. For more details, see <a href="#">Multi-tenancy (organizations)</a> on page 377.
<i>Expiration Date</i>	Specifies when this license expires. Notifications will be sent to you beforehand.
<i>License Type</i>	Specifies whether the <i>Discover, Protect and Response</i> license, <i>Discover and Protect</i> license, or <i>Protect and Response</i> license was purchased. The license type defines the availability of the relevant add-ons.
<i>Communication Control</i>	Specifies the word <i>Available</i> if the Communication Control add-on is included in the license.

Field	Description
<i>eXtended Detection</i>	Specifies the word <i>Available</i> , when the <i>eXtended Detection</i> add-on is included in the license.
<i>Forensics</i>	Specifies the word <i>Available</i> if the Forensics add-on (described in <a href="#">Forensics on page 219</a> ) is included in the license.
<i>Threat Hunting</i>	Specifies the word <i>Available</i> if the Threat hunting add-on (described in <a href="#">Threat Hunting on page 237</a> ) is included in the license. It also specifies whether Repository add-ons have been purchased and how many have been.
<b>Content Updates</b>	Specifies the word <i>Available</i> if the <i>Content Updates</i> 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**

Load Content

Update Collectors

Request Collector Installer

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.

UPDATE COLLECTOR VERSION

<input type="checkbox"/> COLLECTOR GROUP ▲	WINDOWS VERSION	MACOS VERSION	LINUX VERSION
<input type="checkbox"/> Default Collector Group	4.1.0 Rev. 8	3.1.5 Rev. 14	3.1.5 Rev. 61
<input type="checkbox"/> group1	4.1.0 Rev. 8	3.1.5 Rev. 14	3.1.5 Rev. 61
<input type="checkbox"/> group2	4.1.0 Rev. 8	3.1.5 Rev. 14	3.1.5 Rev. 61
<input type="checkbox"/> High Security Collector Group	4.1.0 Rev. 8	3.1.5 Rev. 14	3.1.5 Rev. 61
<input type="checkbox"/> Insiders	4.1.0 Rev. 8	3.1.5 Rev. 14	3.1.5 Rev. 61
<input type="checkbox"/> Linux	4.1.0 Rev. 8	3.1.5 Rev. 14	3.1.5 Rev. 61
<input type="checkbox"/> lior1	4.1.0 Rev. 8	3.1.5 Rev. 14	3.1.5 Rev. 61

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

**Note:** Version update involves sending 10Mb of data from the Central Manager to each Collector.

Update Cancel

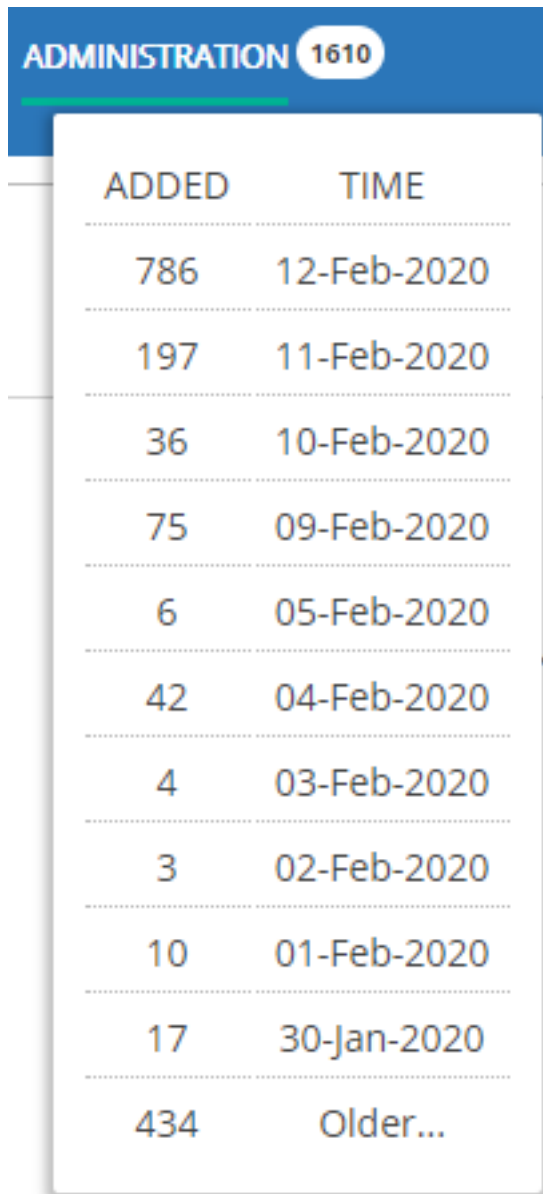
Field	Description
<i>Vulnerability Management</i>	Specifies the word <i>Available</i> if the Vulnerability Management add-on (described in <a href="#">Administration on page 274</a> ) is included in the license.
<i>License Capacity</i>	Specifies the number of available licenses for protection by FortiEDR 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).
<i>In Use</i>	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.
<i>Remaining</i>	Specifies the number of FortiEDR licenses for workstations and servers that are still available for use.



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.



You can hover over the number to see the list of unread system events. Each row shows the number of system events added by day.



The screenshot shows the 'ADMINISTRATION' tab in the FortiEDR interface, with a sub-tab labeled '1610'. Below the header, there is a table with two columns: 'ADDED' and 'TIME'. The table lists collector versions and their corresponding dates, ordered from newest to oldest. The last entry is '434 Older...'. Each row is separated by a horizontal dashed line.

ADDED	TIME
786	12-Feb-2020
197	11-Feb-2020
36	10-Feb-2020
75	09-Feb-2020
6	05-Feb-2020
42	04-Feb-2020
4	03-Feb-2020
3	02-Feb-2020
10	01-Feb-2020
17	30-Jan-2020
434	Older...

## Updating the Collector version

The Update Collector Version feature is used to update a FortiEDR version, such as from version 5.2 to 5.2.1.

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 [Licensing on page 274](#).

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: **7174** Update Collectors Request Collector Installer

☐ 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

<input type="checkbox"/> COLLECTOR GROUP ▲	WINDOWS VERSION	MACOS VERSION	LINUX VERSION
<input type="checkbox"/> Default Collector Group	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
<input type="checkbox"/> emulation	N/A	N/A	N/A
<input type="checkbox"/> group1	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
<input type="checkbox"/> group2	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
<input type="checkbox"/> High Security Collector Group	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
<input type="checkbox"/> Insiders	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
<input type="checkbox"/> Linux	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72

Update 0 selected groups to

☐ Windows version 4.1.0 Rev. 23 ▼
 ☐ 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.

Update Cancel

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 in the *LICENSING* window, 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

<input type="checkbox"/> COLLECTOR GROUP ▲	WINDOWS VERSION	MACOS VERSION	LINUX VERSION
<input type="checkbox"/> Default Collector Group	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
<input type="checkbox"/> emulation	N/A	N/A	N/A
<input type="checkbox"/> group1	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
<input type="checkbox"/> group2	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
<input type="checkbox"/> High Security Collector Group	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
<input type="checkbox"/> Insiders	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
<input type="checkbox"/> Linux	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72

Update 0 selected groups to

☐ Windows version 4.1.0 Rev. 23
 ☐ 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.

Update Cancel

### UPDATE COLLECTOR VERSION

<input type="checkbox"/> COLLECTOR GROUP ▲	WINDOWS VERSION	MACOS VERSION	LINUX VERSION
<input type="checkbox"/> Default Collector Group	4.1.0	3.1.5	3.1.5
<input type="checkbox"/> emulation	N/A	N/A	N/A
<input type="checkbox"/> group1	4.1.0	3.1.5	3.1.5
<input type="checkbox"/> group2	4.1.0	3.1.5	3.1.5
<input type="checkbox"/> High Security Collector Group	4.1.0	3.1.5	3.1.5
<input type="checkbox"/> Insiders	4.1.0	3.1.5	3.1.5
<input type="checkbox"/> Linux	4.1.0	3.1.5	3.1.5

Update 0 selected groups to

☐ Windows version 4.1.0
 ☐ macOS version 3.1.5
 ☐ Linux version 3.1.5

**Note:** Version update involves sending 10Mb of data from the Central Manager to each Collector.

Update Cancel

### 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.

<input type="checkbox"/> COLLECTOR GROUP ▲	WINDOWS VERSION	MACOS VERSION	LINUX VERSION
<input type="checkbox"/> Default Collector Group	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
<input type="checkbox"/> emulation	N/A	N/A	N/A
<input type="checkbox"/> group1	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
<input type="checkbox"/> group2	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
<input type="checkbox"/> High Security Collector Group	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
<input checked="" type="checkbox"/> Insiders	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
<input type="checkbox"/> Linux	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72

Update 1 selected groups to

☐ Windows version 4.1.0 Rev. 23 ☒ macOS version 3.1.5 Rev. 14 ☐ Linux version 3.1.5 Rev. 72

**Note:** Version update involves sending 10Mb of data from the Center management to each Collector.

**Update** **Cancel**

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

Collectors are gradually being updated to version **MacOS version 3.1.5 Rev. 14** now

**OK**

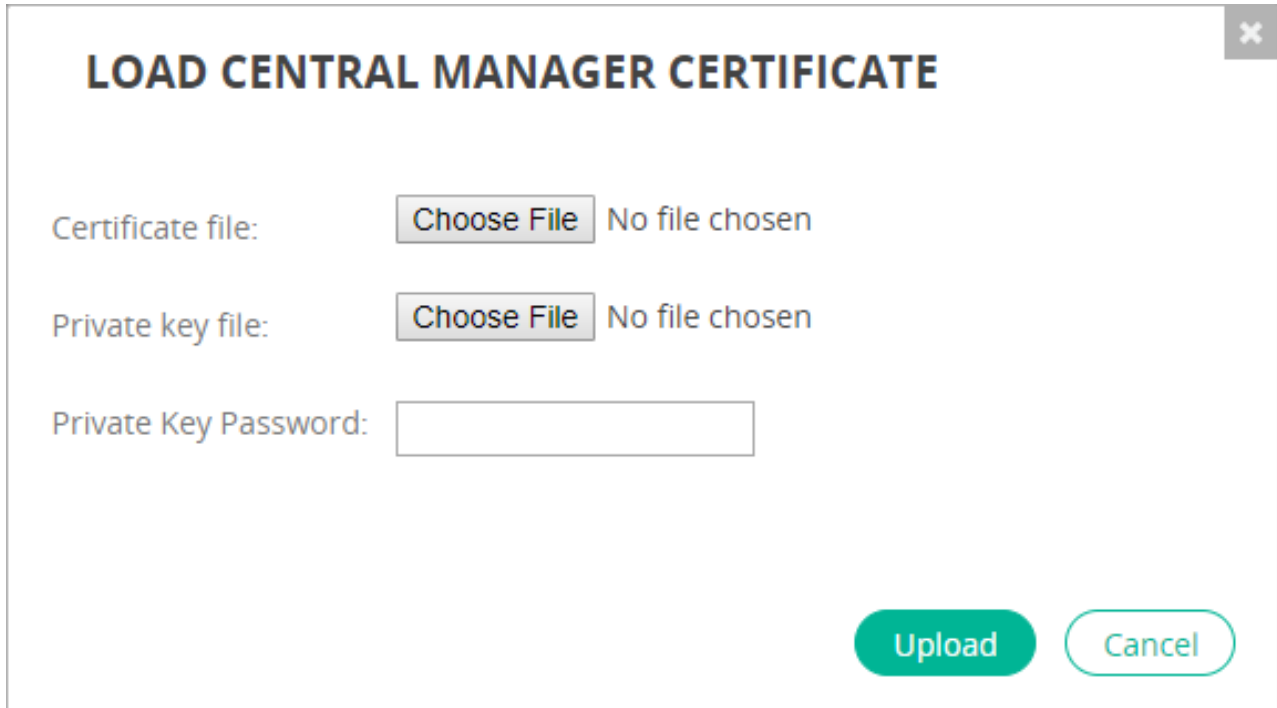
4. Click **OK**.



## Loading a server certificate

To load a certificate:

1. Click *Central Manager Certificate* ( **Central Manager Certificate** ). The *Load Central Manager Certificate* dialog opens.



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. Contact [Fortinet Support](#) to configure the certificate.


## Requesting and obtaining a Collector installer

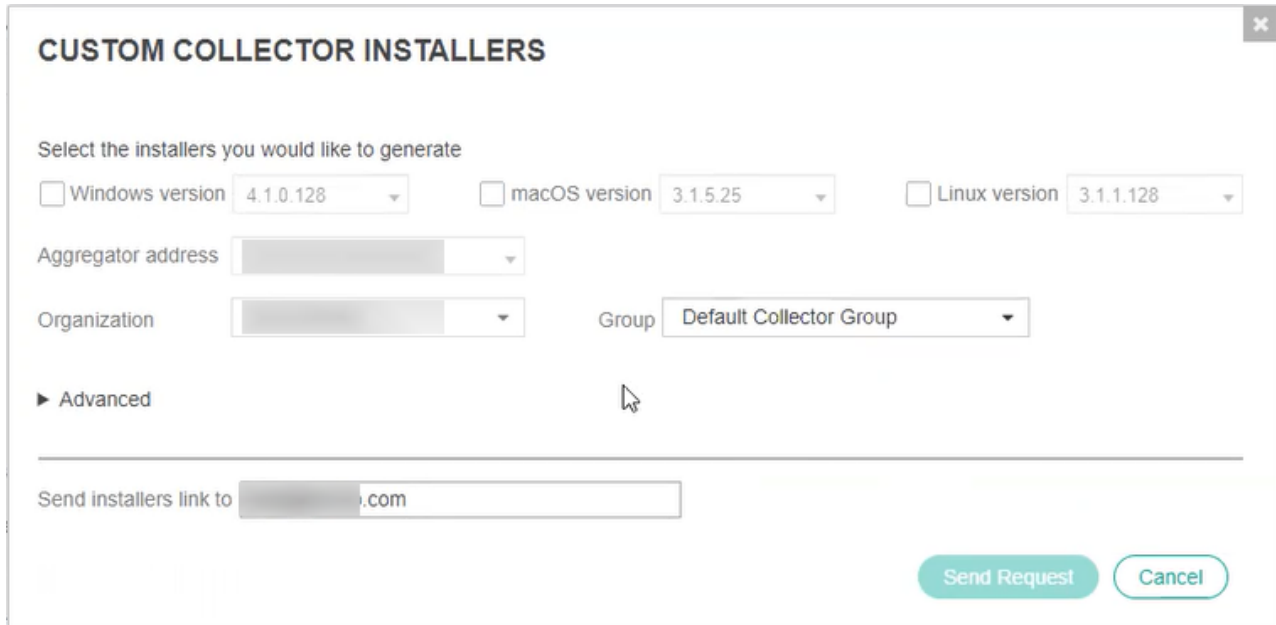
You can click the *Request Collector Installer* button ( **Request Collector Installer** ) to obtain a Collector installer file that can be used to install a Collector. This option enables you to request an installer for a particular operating system(s), such as Windows, MacOS, or Linux. This installer 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 installer is then emailed to you. After you receive the installer file from FortiEDR, simply unzip it using the password provided in the email, double-click the installer

and then follow the instructions to install a Collector based on the operating system on which it is to be installed, as described in [Installing FortiEDR Collectors on page 21](#).

In order to determine the type of installer to request (according to the operating system), configure the settings in the *Custom Collector Installers* window, as described below.

### To configure custom installer settings:

1. In the *Licensing* window, click the *Request Collector Installer* button (  ). The following displays:

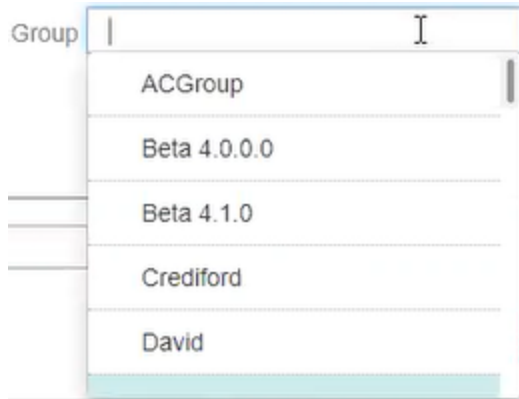


2. In the *Select the installer you would like to generate* area, select the checkbox of the installer(s) you want to request. Multiple installers can be requested at the same time.

Select the installers you would like to generate



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 277](#)
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.



7. In the *Advanced* area, specify the following:

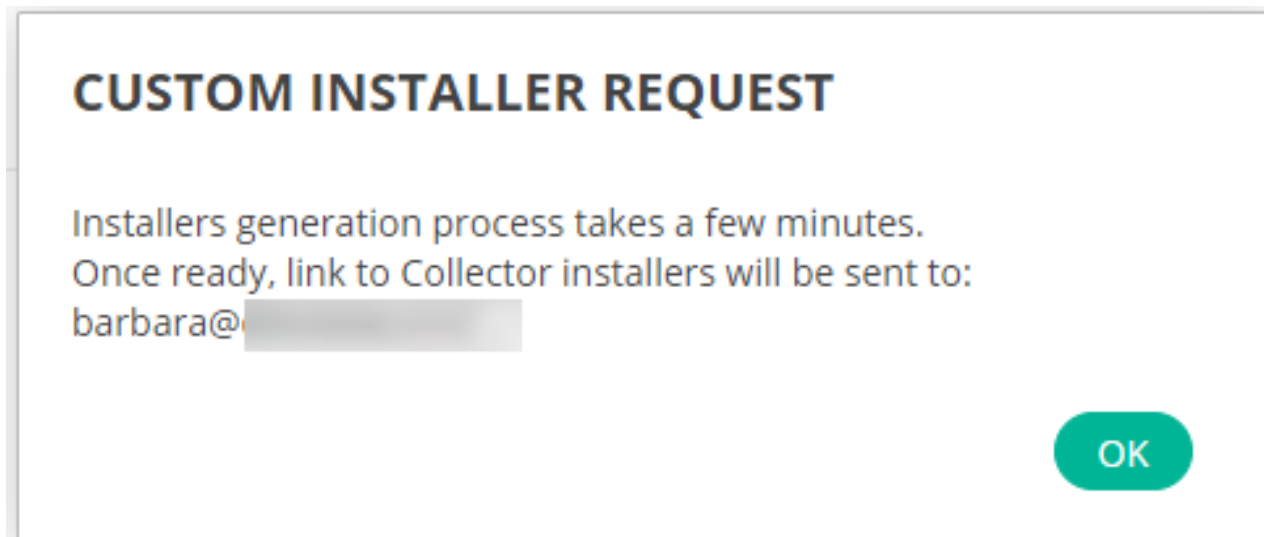
▼ **Advanced**

- ☐ **VDI (Virtual Desktop Infrastructure) installation**
- ☐ **Use system proxy settings**
- ☐ **Start after device reboot**

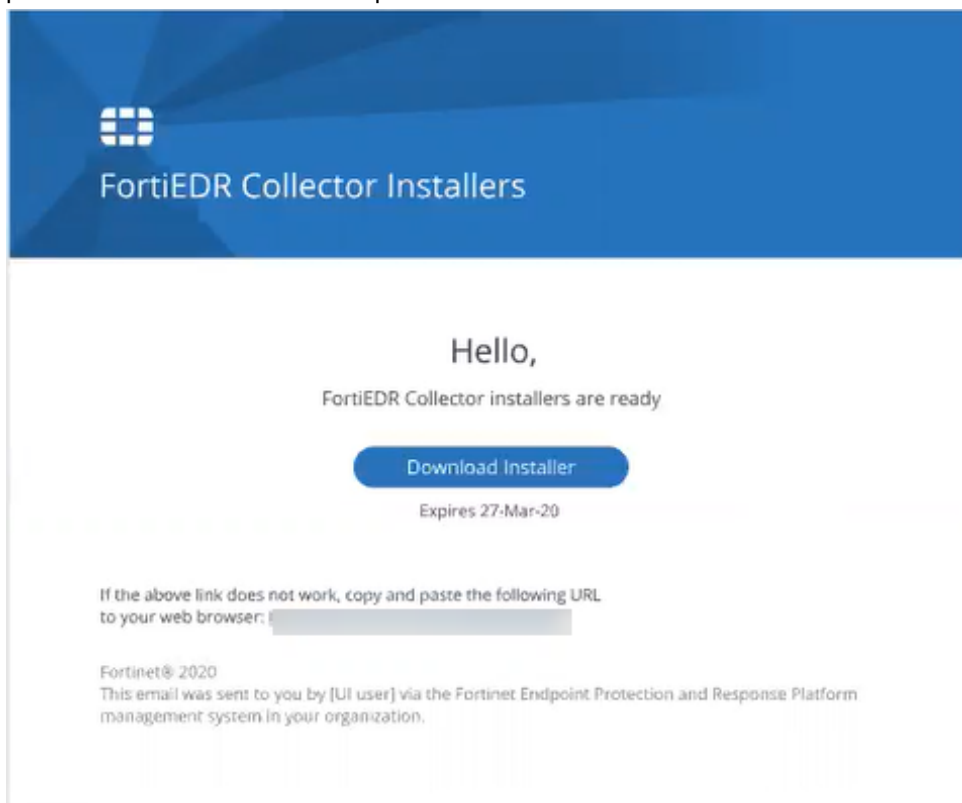
- *VDI (Virtual Desktop Infrastructure) Installation:* If you are installing the Collector on a VDI environment, check this checkbox. For more details, you may refer to the Working with FortiEDR on VDI Environments section on page 54.
- *Use System Proxy Settings:* If you use a web proxy to filter requests 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* (  ) button. A confirmation message displays.



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.




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.

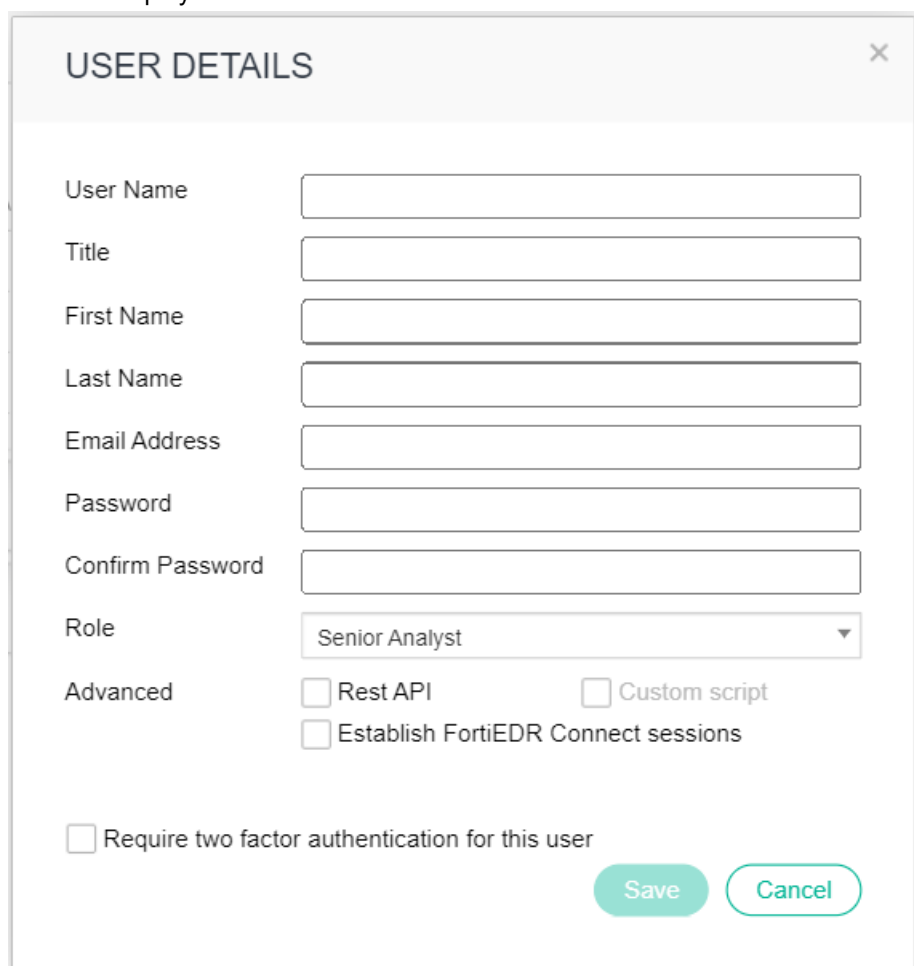
In such cases the URL should be amended to drop the redundant space/%20 before it can be used.

## 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.



The screenshot shows a 'USER DETAILS' dialog box with a close button (X) in the top right corner. The dialog contains the following fields and options:

- User Name: Text input field
- Title: Text input field
- First Name: Text input field
- Last Name: Text input field
- Email Address: Text input field
- Password: Text input field
- Confirm Password: Text input field
- Role: Dropdown menu with 'Senior Analyst' selected
- Advanced section with three checkboxes:
  - ☐ Rest API
  - ☐ Custom script
  - ☐ Establish FortiEDR Connect sessions
- ☐ Require two factor authentication for this user
- Buttons: 'Save' and 'Cancel' (both in teal rounded rectangles)

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
<i>Admin</i>	Highest-level super user that can perform all operations in the FortiEDR Central Manager console for the organization.
<i>Senior Analyst</i>	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 <i>ADMINISTRATION</i> 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 <i>ADMINISTRATION</i> tab.
<i>Analyst</i>	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 <i>ADMINISTRATION</i> tab or define/change policies.
<i>IT</i>	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 <i>ADMINISTRATION</i> tab but do not have access to other areas, such as security configuration, alert monitoring, or Forensics options.
<i>Read-Only</i>	Basic role with read-only access to all functions except system configuration.



For [Multi-tenancy \(organizations\) on page 377](#) 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
<i>Rest API</i>	Specifies whether to allow the user to access the FortiEDR Central Manager through API calls.  <div>  <p>For more information about APIs, see the <a href="#">FortiEDR RESTful API Guide</a>. You must log in to the Fortinet Developer Network to access the guide.</p> </div>
<i>Custom script</i>	Specifies whether to allow the user to upload and manage (add, modify and delete) Python scripts that call third-party system APIs (see <a href="#">Integrations on page 336</a> ). Those scripts will then be automatically triggered by FortiEDR as incident responses.

Option	Description
	 <p>This option is only available to users with Admin and IT permissions.</p>
<i>Establish FortiEDR Connect sessions</i>	<p>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 <a href="#">FortiEDR Connect on page 267</a>.</p>
	 <p>This option is only available to users with Admin, Analyst, and Senior Analyst permissions. This option takes effect only when the <i>Allow FortiEDR Connect - Remote Shell Connection</i> checkbox is selected under <i>Administration &gt; Tools</i>, which means the FortiEDR Connect functionality is enabled at the organization level.</p>

6. Select the *Require two-factor authentication for this user* checkbox if you want to require [two-factor authentication](#) for the user.
7. Click **Save**.

## Two-factor authentication


You can require two-factor authentication for a specific FortiEDR user. In this case, that user 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.

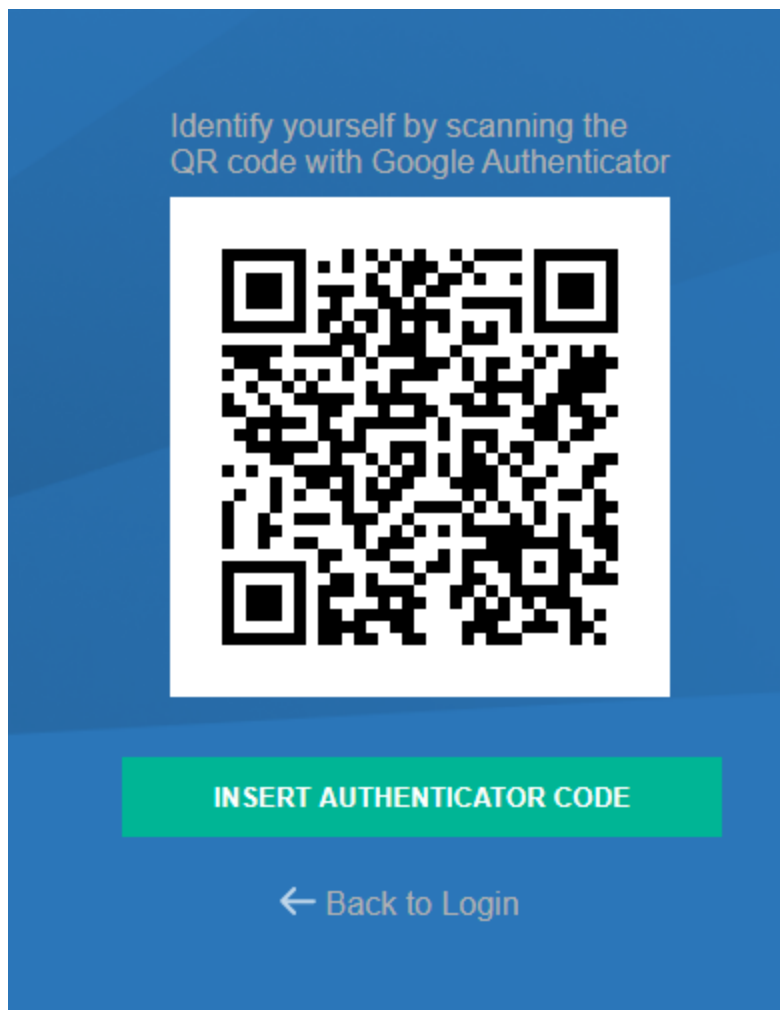
To require two-factor authentication on a user, check the *Require two-factor authentication for this user* checkbox for that user, as described in [Users on page 285](#).

**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**.



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:



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.

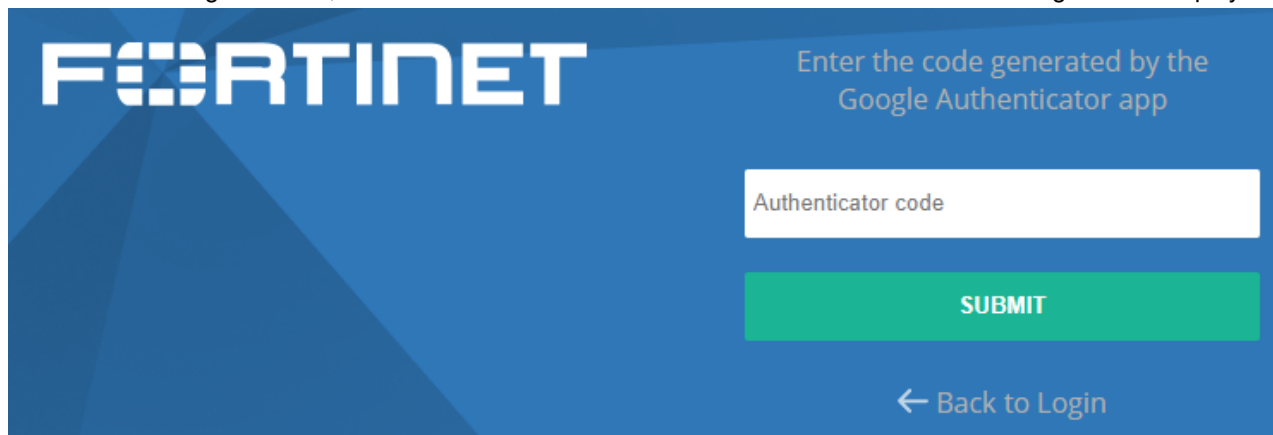
enSilo

386 077

tomor



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.

You can then log in FortiEDR without two-factor authentication for seven days. FortiEDR verifies your identity every seven days by asking you for a new token. After each seven-day cycle, repeat steps 1 through 5 to authenticate yourself again. To set a different cycle on a standalone environment, please contact [Fortinet Support](#).




## Resetting a user password

Use the procedure described below to reset a user's 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 287](#) 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.

NAME	TITLE	FIRST NAME	LAST NAME	EMAIL ADDRESS	ROLE	ADVANCED
chris		chris	001 sample	chris@sample.com	Read-Only	  
fxy		fxy	001 sample	fxy@sample.com	Admin	
wslwlmn		wslwlmn	wslwlmn	wslwlmn@sample.com	Admin	Rest API, FortiEDR Connect, Custom ...

2. Click the **Reset Password** button for the user whose password you want to reset. The following window displays:

## RESET PASSWORD FOR USER AAAA

☒ Set a new password

Password

Confirm Password

☒ Require a change of password in the next sign in

☐ Reset the Two-Factor authentication token

3. Do one of the following:

- Click the *Set a New Password* radio button and define a new password for the user.
- 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 287](#) in order to log in.

4. Click the *Reset* button.

## LDAP authentication

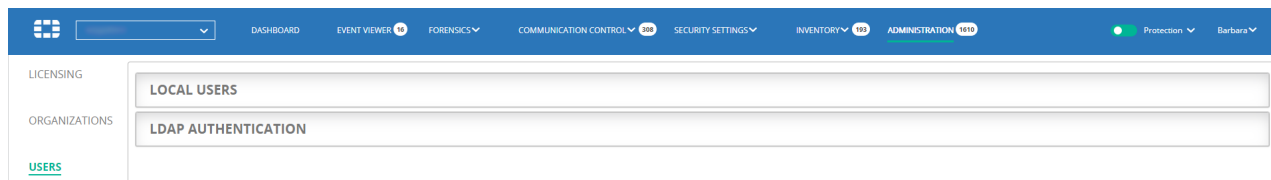
Lightweight Directory Access Protocol (LDAP) authentication is an open, industry-standard application protocol for accessing and maintaining distributed directory information services over an IP network. LDAP provides a central place to store usernames and passwords. This enables many different applications 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 a FortiEDR Core as a Jumpbox on page 57](#).

### To set up LDAP authentication in FortiEDR:

1. Click the *LDAP AUTHENTICATION* button.








The following window displays:

 This screenshot displays the 'LDAP AUTHENTICATION' configuration window. The window is divided into two main sections: 'LOCAL USERS' and 'LDAP AUTHENTICATION'. The 'LDAP AUTHENTICATION' section contains the following fields and options:
 

- LDAP Enabled:** A checkbox that is currently unchecked.
- JumpBox:** A dropdown menu.
- Directory Type:** A dropdown menu set to 'Active Directory'.
- Server Host:** A text input field.
- Security Level:** A dropdown menu set to 'None'.
- Server Port:** A text input field set to '389'.
- Bind User DN:** A text input field containing 'CN=username,OU=Users,DC=xxx,DC=yyy,DC=domain,DC=co'.
- Bind Password:** A text input field.
- Test:** A button next to the Bind User DN field.
- Role/Group mapping:** A section containing:
  - Base DN:** A text input field containing 'CN=username,OU=Users,DC=xxx,DC=yyy,DC=domain,DC=co'.
  - Specify the LDAP group DN that determines the LDAP user's permission role:** A text input field.
  - Add group:** A button with a plus icon.
- Require two factor authentication for LDAP logins:** A checkbox that is unchecked.
- Reset 2FA Token:** A button next to the checkbox.

## 2. 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 127 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.
Directory Type	Specify the type of central directory in use. FortiEDR supports Active Directory and OpenLDAP. The default is <i>Active Directory</i> .
Server Host	Specify the IP address of your LDAP server.
Security Level	Specify the protocol to be used for the secured connection: <i>TLS</i> , <i>SSL</i> , or <i>None</i> .
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	<p>Specify the base DN and define group/role mapping and permissions of the group:</p> <p><b>Role/Group mapping</b></p> <p>Base DN <input type="text" value="CN=username,OU=Users,DC=xxx,DC=yyy,DC=domain,DC=co"/> ?</p> <p>Specify the LDAP group DN that determines the LDAP user's permission role:</p> <p> Add group</p> <ol style="list-style-type: none"> <li>In <i>Base DN</i>, 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.</li> <li>Click <i>Add group</i>.</li> <li>Define group/role mapping and permissions of the group: <div> <p>Specify the LDAP group DN that determines the LDAP user's permission role:</p> <p>Group <input type="text"/> Role <input type="text"/> Advanced <input type="checkbox"/> Rest API <input type="checkbox"/> Custom script </p> <p> Add group</p> <ol style="list-style-type: none"> <li>In the <i>Group</i> field, specify the name of the group, as it is defined in your central directory (Active Directory or OpenLDAP), that is to be granted FortiEDR permissions. You can specify multiple groups in this field by separating them with commas. For example, <code>group_name1, group_name2</code>.</li> <li>Under <i>Role</i>, select a role from the list. See <a href="#">Users on page 285</a> for more information about the roles.</li> <li>Under <i>Advanced</i>, enable any additional privileges for the group. Some options are role-dependent.</li> </ol> </div> </li> </ol>

Field	Definition
	<p>4. Click <i>Add group</i> and repeat step 2 for each role you want to map to a group or multiple groups.</p> <p><b>For example:</b></p> <p>To give the user John Admin permissions in FortiEDR (for both the FortiEDR application and the RESTful APIs), assign John to a FortiEDRUsers group that is defined in your Central Directory:</p> <ol style="list-style-type: none"> <li>1. Specify <code>FortiEDRUsers</code> under <i>Group</i>.</li> <li>2. Select <i>Admin</i> under <i>Role</i>.</li> <li>3. Check the <i>Rest API</i> checkbox under <i>Advanced</i>.</li> </ol> <p>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, then FortiEDR checks the FortiEDRUsers group to which John is assigned and in this case, and matches the user role permissions.</p>
3.	<p>If users must use two-factor authentication to log in, check the <i>Require two-factor authentication for LDAP logins</i> checkbox. For more details about two-factor login, see the Two-factor Authentication section in <a href="#">Two-factor authentication on page 287</a>.</p>
	<div>  <p>Click the <i>Reset 2FA Token</i> button to reset the two-factor authentication token for a specific user. This process works in the same way as described in <a href="#">Resetting a user password on page 289</a>.</p> </div>
4.	<p>Click <i>Save</i>.</p>
	<div>  <p>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, <code>CN=Yell\,</code>.</p> </div>

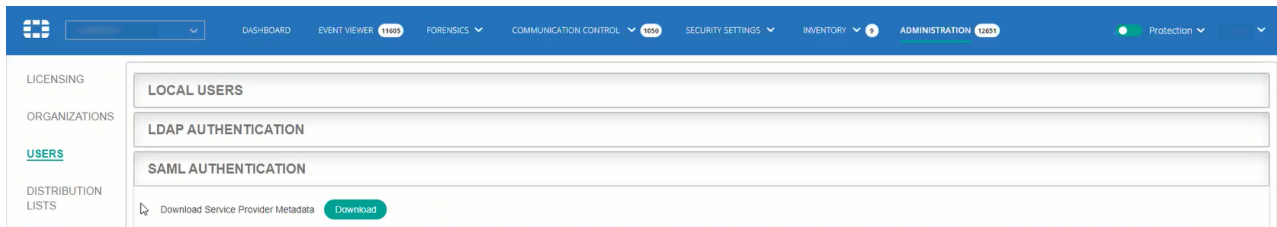
## SAML authentication

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. Click the *SAML Authentication* button.




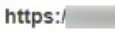




The following window displays:

2. 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 <code>md:EntityDescriptor</code> tag, in the <code>entityID</code> attribute.
Logout Address Value	Located under the <code>md:SingleLogoutService</code> tag, in the <code>Location</code> attribute.
Login Address Value	Located under the <code>md:AssertionConsumerService</code> tag, in the <code>Location</code>

Field	Description
	attribute.
Certificate Value (Public)	Located under the <code>ds:X509Certificate</code> tag.

3. Fill in the following fields:

Field	Definition
SAML Enabled	Check this checkbox to enable SAML authentication in FortiEDR.
SSO url	<p>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 <i>Edit</i> button and then modifying it as needed. You can also copy the URL to the clipboard</p> <p>using the <i>Copy</i> button  (for example, in order to email the FortiEDR SAML login page to your users).</p> <p>SSO url <code>https://.console.</code>  </p> <p><small>This URL can serve as an alternate login using SAML SSO</small></p> <p>Make sure that the suffix does not include any spaces and is comprised of only letters, numbers and underscores.</p>
IDP Description	Specify a free-text description. For example, you may want to specify the IdP server that you are using here.
IDP Metadata	<p>Upload the IdP metadata to FortiEDR. You can either upload an XML file or a URL. To upload a file, click the <i>File</i> radio button and then click the <i>Select File</i> button to navigate to and select the applicable *.XML file. To upload a URL, click the <i>URL</i> radio button and then specify the requisite URL.</p> <p>IDP Metadata <input type="radio"/> File <input checked="" type="radio"/> URL</p> <p>Enter the SAML Identity Provider metadata URL</p> <p><code>www.SAML/</code></p>
Role/Group mapping	<p>Specify the attribute name and define group/role mapping and permissions of the group:</p> <p><b>Role/Group mapping</b></p> <p>Attribute Name</p> <p><input type="text"/></p> <p>Specify name of the SAML attribute containing the groups information:</p> <p> Add group</p> <ol style="list-style-type: none"> <li>1. In <i>Attribute Name</i>, 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.</li> <li>2. Click <i>Add group</i>.</li> </ol>

Field	Definition
	<p><b>3. Define group/role mapping and permissions of the group:</b></p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>Specify name of the SAML attribute containing the groups information:</p> <div style="display: flex; justify-content: space-between;"> <div> <p>Group</p> <input type="text"/> </div> <div> <p>Role</p> <div style="border: 1px solid #ccc; padding: 2px;"> <div></div> </div> </div> <div> <p>Advanced</p> <div style="display: flex; gap: 10px;"> <input type="checkbox"/> Rest API           <input type="checkbox"/> Custom script            </div> </div> </div> </div>
	<ol style="list-style-type: none"> <li>a. In the <i>Group</i> field, specify an attribute value to be granted FortiEDR permissions.</li> <li>b. Under <i>Role</i>, select a role from the list. See <a href="#">Users on page 285</a> for more information about the roles.</li> <li>c. Under <i>Advanced</i>, enable any additional privileges for the group. Some options are role-dependent.</li> </ol> <p><b>4. Click <i>Add group</i> and repeat step 2 for each role you want to map to an attribute value.</b></p>
	<div style="display: flex; align-items: center; border-top: 1px solid #ccc; padding-top: 10px;"> <p>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.</p> </div>

**4. 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

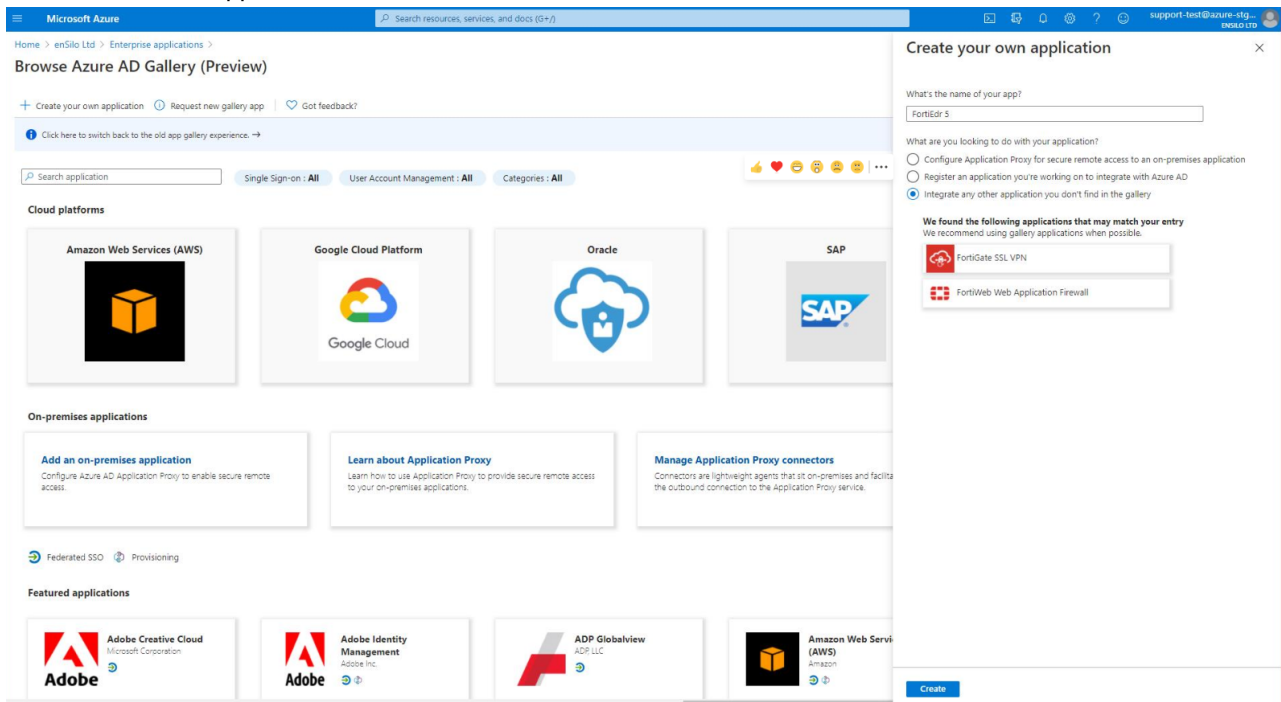


Azure may require a license to support SAML integration with their Enterprise Application. Contact Microsoft's support for further information.

### To configure general SAML IdP portal settings:

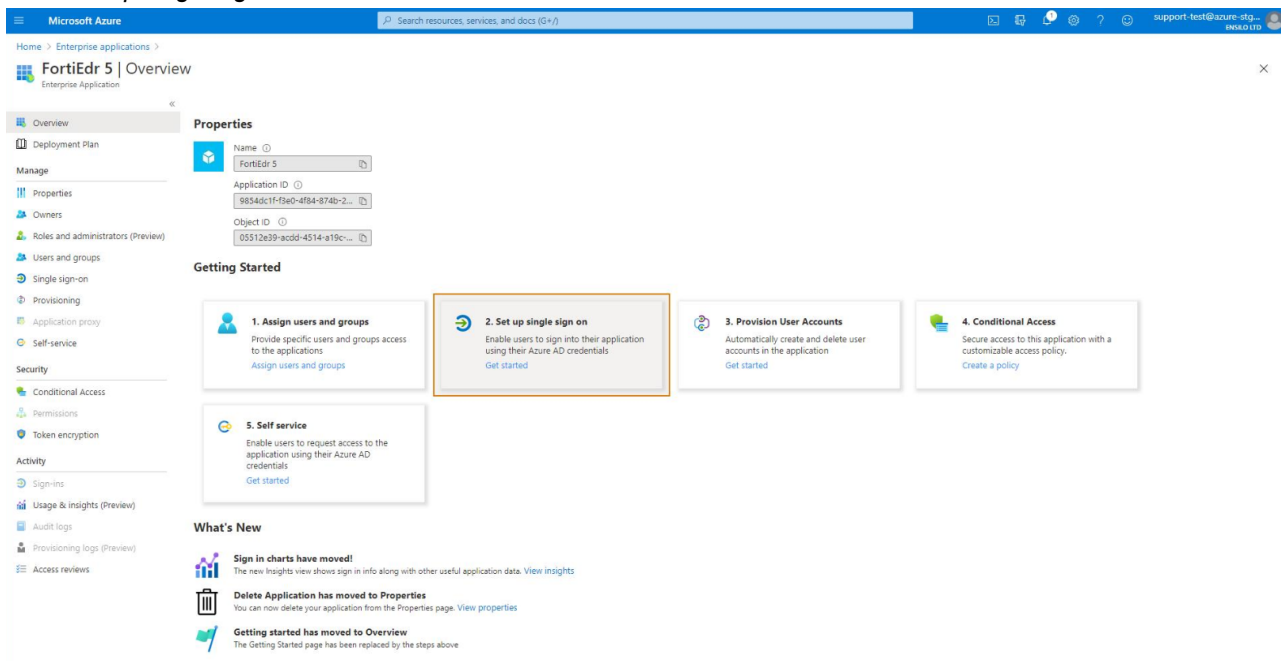
1. Before you start configuring SAML on Azure, download and save SP data from the FortiEDR SAML configuration page (`fortiEDR.sp.metadata.id.1.xml`), as described in [SAML authentication on page 292](#).
2. Sign in to the Azure Dashboard.
3. In the Azure services, select and navigate to the Azure Active 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**.



7. Click **Assign users and groups** to configure the users and groups to grant access to the FortiEDR application.

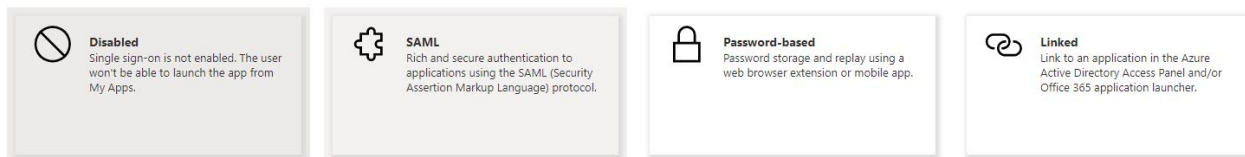
8. Click **Set up single sign on**.





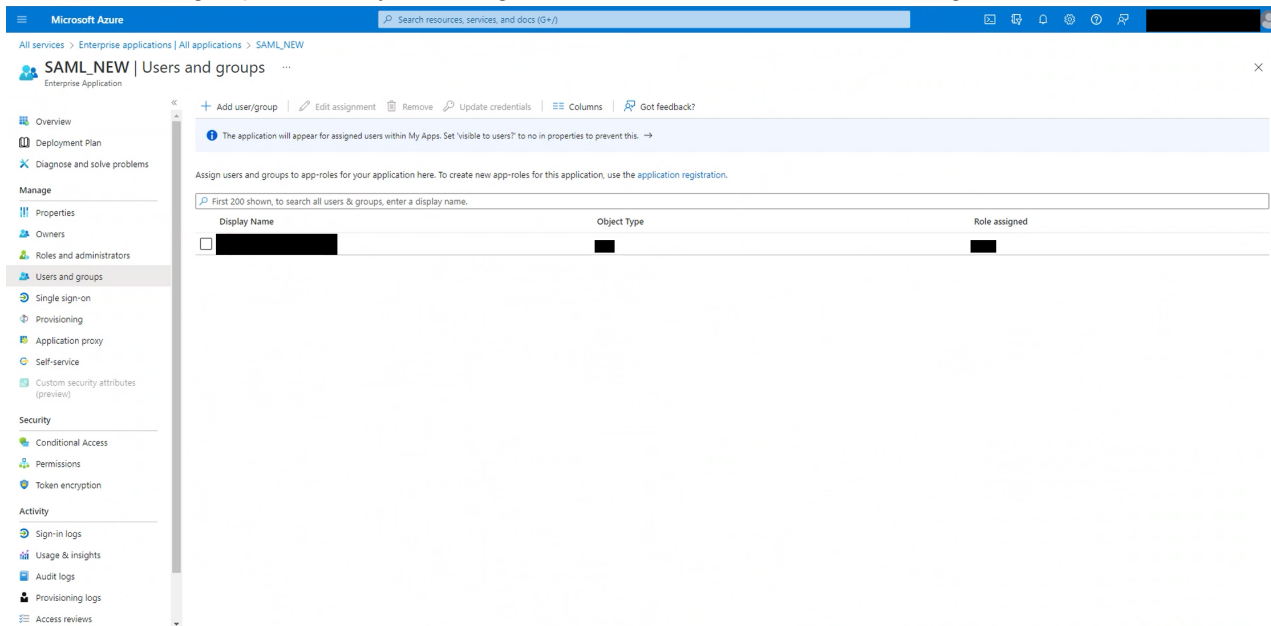
9. When prompted to select a single sign-on method, select **SAML**.

Select a single sign-on method [Help me decide](#)



10. Select **Users and groups** and then **+ Add user/group** to create a new user group.

11. Add users to the group so that they will be eligible to authenticate with FortiEDR Manager.



12. Go to the groups properties and note down the object Id which will be used in later steps.

13. Click *Edit* in the *Basic SAML Configuration* box.

**FortiEDR 5 | SAML-based Sign-on**  
Enterprise Application

Overview | Deployment Plan | Manage | Security | Activity

Manage: Properties, Owners, Roles and administrators (Preview), Users and groups, **Single sign-on**, Provisioning, Application proxy, Self-service

Security: Conditional Access, Permissions, Token encryption

Activity: Sign-ins, Usage & insights (Preview), Audit logs, Provisioning logs (Preview), Access reviews

Set up Single Sign-On with SAML

Read the [configuration guide](#) for help integrating FortiEDR 5.

- 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
- User Attributes & Claims** [Edit](#)

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
- 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)	<a href="#">Download</a>
Certificate (Raw)	<a href="#">Download</a>
Federation Metadata XML	<a href="#">Download</a>
- 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.metadata.id.1.xml`) that was downloaded from FortiEDR SAML configuration page during [SAML authentication on page 292](#). 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:

**1**

Basic SAML Configuration

Edit

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 *User Attributes & Claims* box.
17. In the *User Attributes & Claims* window, click **Add a group claim**.
18. In the window that appears, select the groups to be added to the claim sent to the FortiEDR application. 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

+ Add new claim + Add a group claim Columns

Required claim	
Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [name]
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 ⓘ

19. Select the *Customize the name of the group claim* checkbox.
20. In the *Name* field, enter the attribute name that was specified on the SAML configuration page of the FortiEDR console during [SAML authentication on page 292](#). In our example, it is *fortiEdrGroups*, as shown below:

**Role/Group mapping**

Attribute Name

fortiEdrGroups

Specify name of the SAML attribute containing the groups information:

Group



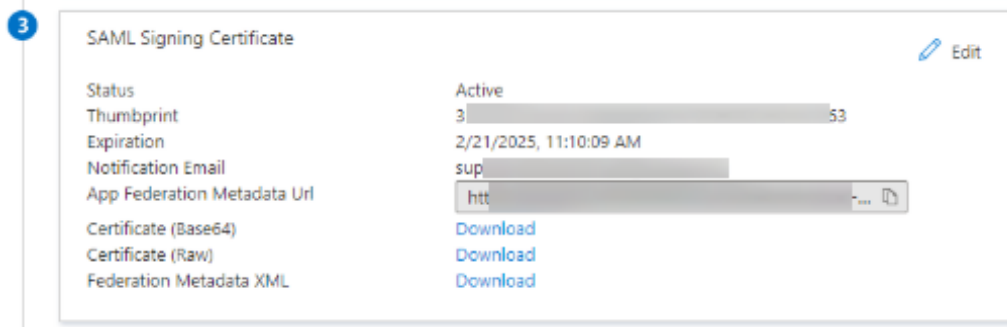
⊕ Add group

Role

Senior Analyst

Admin

Advanced

☐ Rest API☐ Custom script☐ Rest API☐ Custom script**21.** Click **Save**.**22.** Download the Federation Metadata XML file from the *SAML Signing Certificate* section on Azure, as shown below:**23.** Verify that the newly defined attribute is included in the assertion of the Federation Metadata XML file, as shown in the following example:

```
<Attribute Name="fortiEdrGroups">
  <AttributeValue>8d919f5e-3362-4f68-9a24-3605453f0e5</AttributeValue>
  <AttributeValue>086c4b39-2617-4869-8093-175b16c06b70</AttributeValue>
  <AttributeValue>02d2a9e-8015-400f-b656-6cfd9ba2099</AttributeValue>
  <AttributeValue>3b535fe7-9f06-4de8-8c5a-1a9a13013de4</AttributeValue>
  <AttributeValue>8775d4e-0899-4e24-a05e-00d915bad8e</AttributeValue>
  <AttributeValue>35a9179-2765-42c5-b855-5a0496c3329</AttributeValue>
  <AttributeValue>cbedd5e-0000-0000-0000-000000000000</AttributeValue>
</Attribute>
```

**24.** Select and upload the XML file into the FortiEDR Central Manager, as follows:

IDP Metadata

☒ File☐ URL

Upload the SAML Identity Provider metadata file

Select file

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

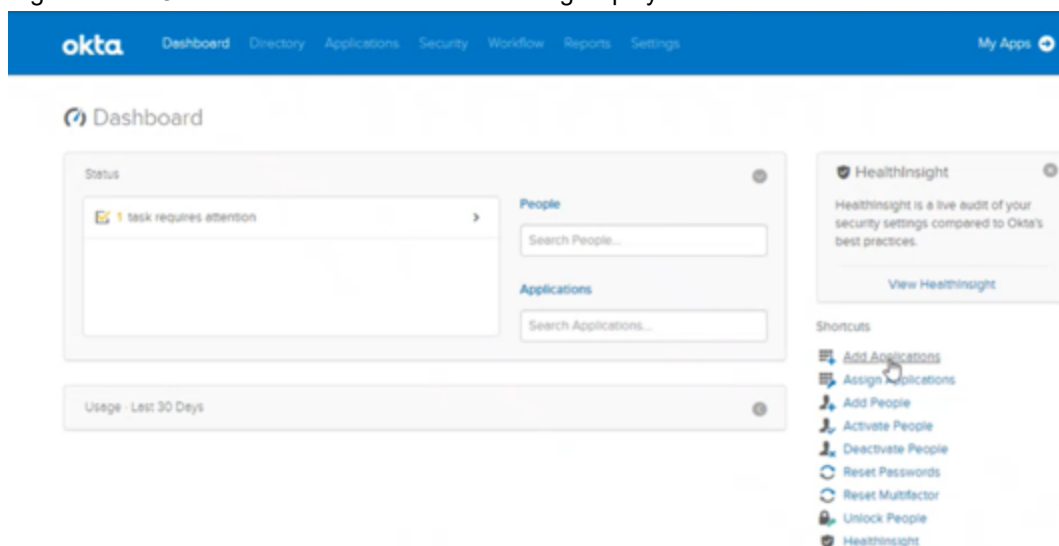
Enter the SAML Identity Provider metadata URL

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

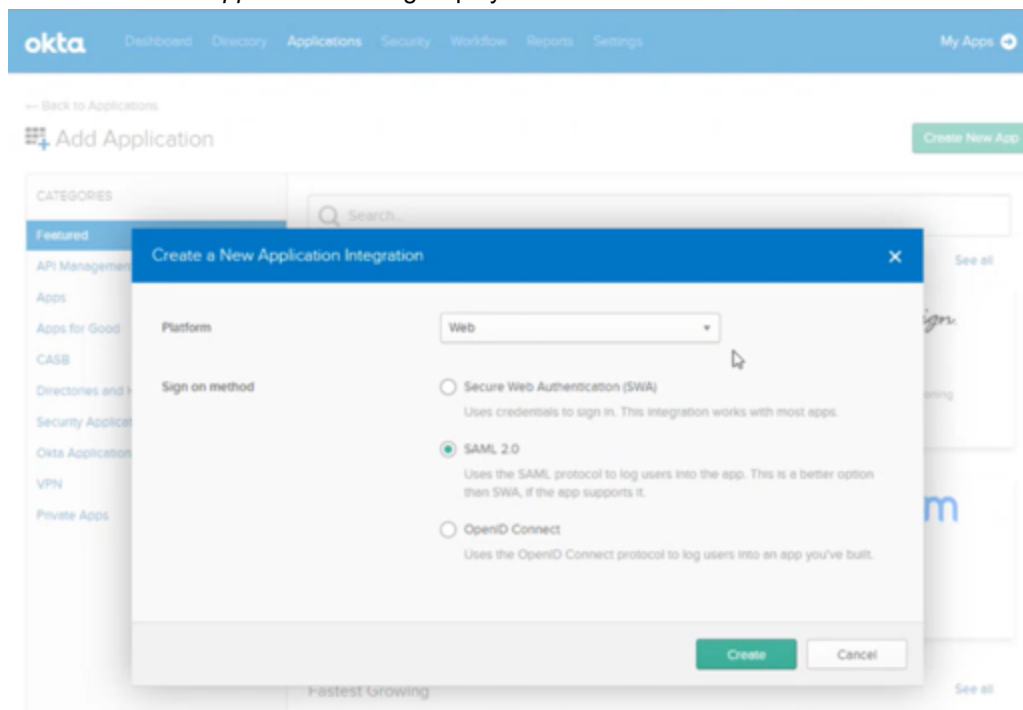
### To configure general SAML IdP portal settings:

1. Before starting to configure SAML on Okta, you must download and save SP data from the FortiEDR SAML configuration page (`fortiEDR.sp.metadata.id.1.xml`), as described in [SAML authentication on page 292](#)
2. Sign in to the Okta Admin dashboard. The following displays:



3. In your Okta org, click *Applications* and then *Add Applications*.

4. Click *Create New App* . The following displays:




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.

**Create SAML Integration**

1 General Settings    2 Configure SAML    3 Feedback

**1 General Settings**

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**

1 General Settings    2 Configure SAML    3 Feedback

**SAML Settings**

**GENERAL**

Single sign on URL

☒ Use this for Recipient URL and Destination URL

☐ Allow this app to request other SSO URLs

Audience URI (SP Entity ID)

Default RelayState

If no value is set, a blank RelayState is sent

Name ID format

Application username

Update application username on

[Show Advanced Settings](#)

**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.metadata.id.1.xml`) that was downloaded from FortiEDR SAML configuration page, as described in [SAML authentication on page 292](#).

- **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.metadata.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.enilo.com/saml/metadata/alias/1' ID='https_____nsloeng_console_enilo_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>MIITCDBGAIAUFAAATAACXCSYK4MAOCGSGSIIBDQF6G/11I7OlkfTRgISyVW0ccufuyCD5cJYsmMGVGIZLeWdxdtRtCLLEO+vsIJ/bfwcn0nyqjzucvscvckrqqspk+n1mu0vwkykguziyekzxazem/rAGuSx3/ar7BSpqhmgjcayagpiusvEoXXZ/zOLPBR/naregcj/vzpzcOTzhonouys/qUS</ds:X509Certificate>  
        </ds:X509Data>  
      </md:keyDescriptor>  
    <- md:keyDescriptor use='encryption'>  
      <- ds:KeyInfo xmlns:ds='http://www.w3.org/2000/09/xmldsig#'>  
        <- ds:X509Data>  
          <- ds:X509Certificate>MIITCDBGAIAUFAAATAACXCSYK4MAOCGSGSIIBDQF6G/11I7OlkfTRgISyVW0ccufuyCD5cJYsmMGVGIZLeWdxdtRtCLLEO+vsIJ/bfwcn0nyqjzucvscvckrqqspk+n1mu0vwkykguziyekzxazem/rAGuSx3/ar7BSpqhmgjcayagpiusvEoXXZ/PZQJHMY/fALegwT/hTPZ/pLUP/AJOIUAS/KULic</ds:X509Certificate>  
        </ds:X509Data>  
      </md:keyDescriptor>  
    <md:singleLogoutService Location='https://nsloeng.console.enilo.com/saml/SingletLogout/alias/1' Binding='urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST'/>  
    <md:singleLogoutService Location='https://nsloeng.console.enilo.com/saml/SingletLogout/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.enilo.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.enilo.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 ?	<div>Signed ▼</div>
Assertion Signature ?	<div>Signed ▼</div>
Signature Algorithm ?	<div>RSA-SHA256 ▼</div>
Digest Algorithm ?	<div>SHA256 ▼</div>
Assertion Encryption ?	<div>Encrypted ▼</div>
Encryption Algorithm ?	<div>AES256-CBC ▼</div>
Key Transport Algorithm ?	<div>RSA-OAEP ▼</div>
Encryption Certificate ?	<div> <div>🔒</div> <div> <b>my_cert.crt</b> <span style="float: right;">X</span>            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         </div> </div>
Enable Single Logout ?	<input type="checkbox"/> Allow application to initiate Single Logout
Assertion Inline Hook	<div>None (disabled) ▼</div>
Authentication context class ?	<div>PasswordProtectedTransport ▼</div>
Honor Force Authentication ?	<div>Yes ▼</div>
SAML Issuer ID ?	<div>http://www.okta.com/\${org.externalKey}</div>

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:

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

groups

Specify name of the SAML attribute containing the groups information:

Group	Role	Advanced
	Senior Analyst	<input type="checkbox"/> Rest API <input type="checkbox"/> Custom script
	Admin	<input type="checkbox"/> Rest API <input type="checkbox"/> Custom script

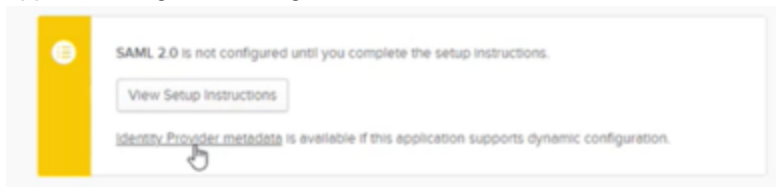
Add group

#### 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="Id808925067641464161630120810">
  <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" 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:



#### 19. Paste it into the FortiEDR Central Manager as follows:

IDP Metadata ☐ File ☒ URL

Enter the SAML Identity Provider metadata URL

<https://ensilo.okta.com/app/ensilo/1234567890/metadata>

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 307](#)
2. [Setting up user group management on page 308](#) (if not configured already)
3. [Setting up service provider for FortiEDR on page 309](#)

### 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 <i>username@realm</i> .
Realms	Select <i>Add a realm</i> 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	Allow local users to override remote users	Groups	Delete
<input checked="" type="radio"/>	local   local users	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Filter: (0)"/>
<input type="button" value="Add a realm"/>				

 Login session timeout: 500 minutes (5-1440)  
 Default IdP certificate: Fortinet\_CA3\_Factory | C=US, ST=California, L=San Jose, 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

Choose all visible

Selected users

sam

Remove all

Password policy:

Default

Usage Profile

[ Please Select ]

OK

Cancel



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:  [Generate prefix](#)

Server certificate:

IDP single sign-on URL:  [Copy](#)

IDP single logout URL:  [Copy](#)

[Download IDP metadata](#) [Import SP metadata](#)

SP entity ID:

SP ACS (login) URL:  [Alternative ACS URLs](#)

SP SLS (logout) URL:

☒ Support IdP-initiated assertion response

Relay state:

☐ Participate in single logout

☒ SAML request must be signed by SP

Certificate type:

Certificate fingerprint:  [Import certificate](#)

Fingerprint algorithm:

Alternative certificate fingerprint:  [Import certificate](#)

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:

☐ Include realm name in subject NameID

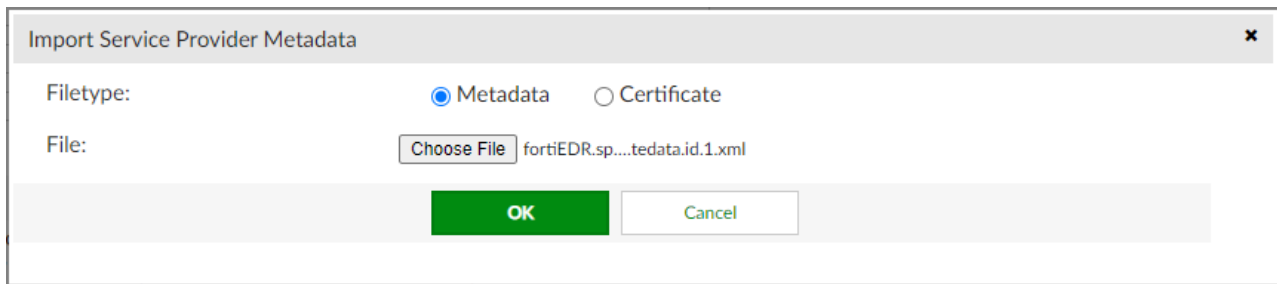
Format:

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 292](#) 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 292](#) for more information.

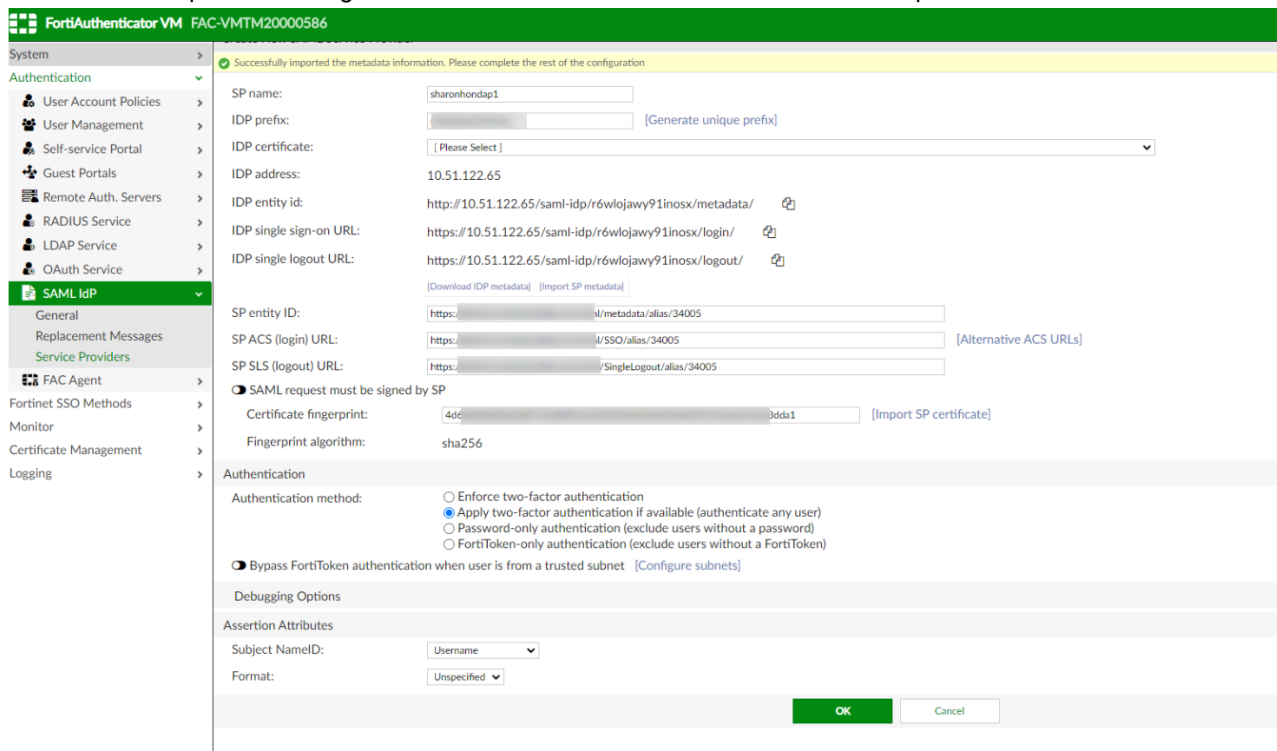


**Import Service Provider Metadata**

Filetype: ☒ Metadata ☐ Certificate

File:  fortiEDR.sp....tedata.id.1.xml

6. All other service provider configuration fields are auto-filled after the SP data file import:



**FortiAuthenticator VM** FAC-VMTM20000586

System > Authentication > SAML IdP

Successfully imported the metadata information. Please complete the rest of the configuration

SP name: sharonhondap1

IDP prefix:  [Generate unique prefix]

IDP certificate:  [Please Select]

IDP address: 10.51.122.65

IDP entity id: http://10.51.122.65/saml-idp/r6wlojavy91inosx/metadata/

IDP single sign-on URL: https://10.51.122.65/saml-idp/r6wlojavy91inosx/login/

IDP single logout URL: https://10.51.122.65/saml-idp/r6wlojavy91inosx/logout/

[Download IDP metadata] [Import SP metadata]

SP entity ID: https://10.51.122.65/saml-idp/r6wlojavy91inosx/metadata/alias/34005

SP ACS (login) URL: https://10.51.122.65/saml-idp/r6wlojavy91inosx/login/ [Alternative ACS URLs]

SP SLS (logout) URL: https://10.51.122.65/saml-idp/r6wlojavy91inosx/logout/

☒ SAML request must be signed by SP

Certificate fingerprint: 4dc...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**

Attribute Name

fortiedr\_role

Specify name of the SAML attribute containing the groups information:

Group



Add group

Role

Senior Analyst

Admin

Advanced

☐ Rest API☐ Custom script☐ Rest API☐ Custom script

And therefore the configuration on FortiAuthenticator appears as follows:

**Create New Assertion Attribute**

SAML attribute:

fortiedr\_role

User attribute:

Group

OK

Cancel

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.

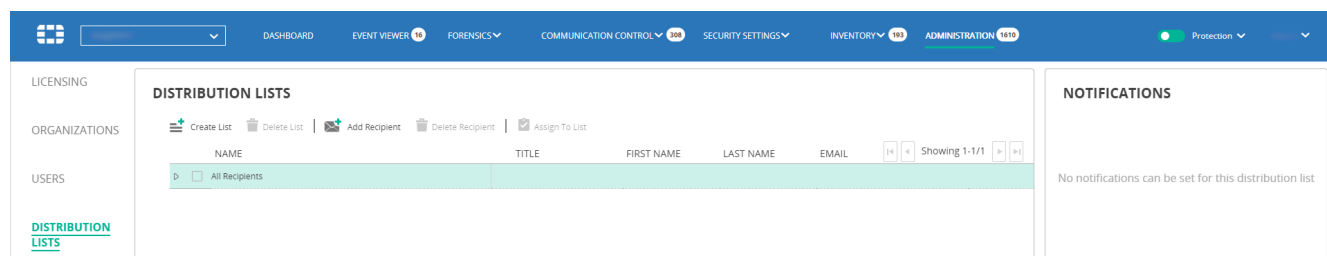



You must configure SMTP before using the *Distribution List* option. For more details, see [SMTP on page 313](#).




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.

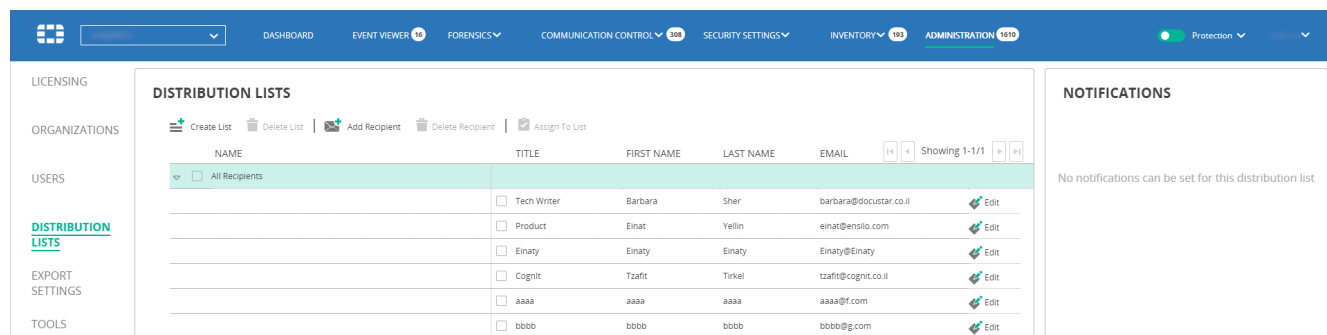
Each email contains all the raw data items collected by FortiEDR about that security event. The system is provided with a Distribution List called All Recipients that contains all FortiEDR Central Manager users. All other recipients that are added to the system are also automatically added to the *All Recipients* list.



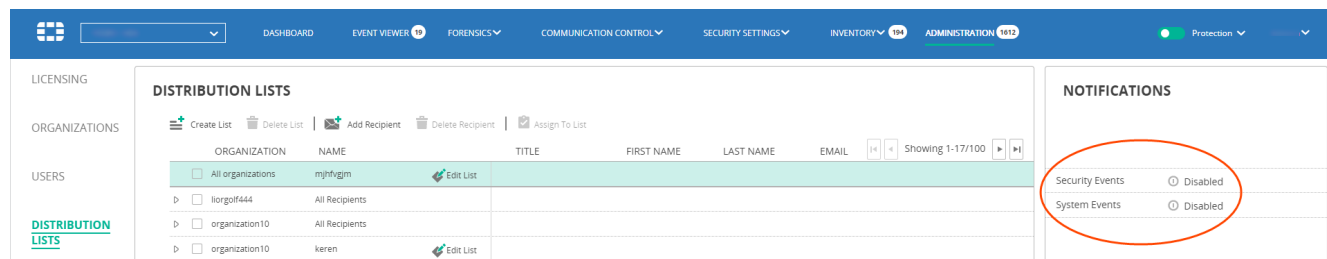
This window displays a row for each Distribution List. Click the *Expand* button (  ) in a row to view the recipients assigned to that list.

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.



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).



## Export settings

The *EXPORT SETTINGS* option provides access to the following options:

- SMTP on page 313
- Open Ticket on page 313
- Syslog on page 314



## 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.



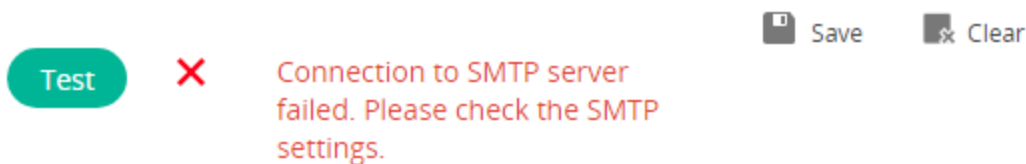
In a single-organization system, SMTP settings are only accessible in Hoster view (for administrators of all organization), or to the administrator of that organization.

### 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.



## 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 411](#).



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 via Syslog.

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.


Use the *Define New Syslog* button (  **Define New Syslog** ) to define a new Syslog destination. The *Syslog Name* is a free-text field that identifies this destination in the FortiEDR.



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 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	<input checked="" type="checkbox"/> Enabled	
System Events	<input checked="" type="checkbox"/> Enabled	
Audit trail	<input checked="" type="checkbox"/> Enabled	

### To select which fields will be included in the syslog messages:

Check the checkbox of the fields that you want to be sent to your Syslog.

### SECURITY EVENTS NOTIFICATIONS ×

<input checked="" type="checkbox"/> Organization	<input checked="" type="checkbox"/> Organization ID
<input checked="" type="checkbox"/> Event ID	<input checked="" type="checkbox"/> Raw Data ID
<input checked="" type="checkbox"/> Device Name	<input checked="" type="checkbox"/> Device State
<input checked="" type="checkbox"/> MAC Address	<input checked="" type="checkbox"/> Operating System
<input checked="" type="checkbox"/> Source IP	<input checked="" type="checkbox"/> Process Name
<input checked="" type="checkbox"/> Process Path	<input checked="" type="checkbox"/> Process Type
<input checked="" type="checkbox"/> Severity	<input checked="" type="checkbox"/> Classification
<input checked="" type="checkbox"/> Destination	<input checked="" type="checkbox"/> First Seen
<input checked="" type="checkbox"/> Last Seen	<input checked="" type="checkbox"/> Action
<input checked="" type="checkbox"/> Count	<input checked="" type="checkbox"/> Certificate
<input checked="" type="checkbox"/> Rules List	<input checked="" type="checkbox"/> Users
<input checked="" type="checkbox"/> Script	<input checked="" type="checkbox"/> Script Path
<input checked="" type="checkbox"/> Autonomous System	<input checked="" type="checkbox"/> Country
<input checked="" type="checkbox"/> Process Hash	<input checked="" type="checkbox"/> Threat Name
<input checked="" type="checkbox"/> Threat Family	<input checked="" type="checkbox"/> Threat Type

Save Cancel



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](#).

## Tools

The **TOOLS** option provides access to the following options:



Some options are only available to specific roles. For more information about user roles and permissions, see [Users on page 285](#).

- [Audit trail on page 317](#)
- [Component authentication on page 319](#)
- [File scan on page 320](#)
- [End-user notifications on page 321](#)
- [IoT device discovery on page 324](#)
- [Personal data handling on page 325](#)
- [Windows Security Center on page 330](#)
- [FortiEDR Connect on page 331](#)

## Audit trail

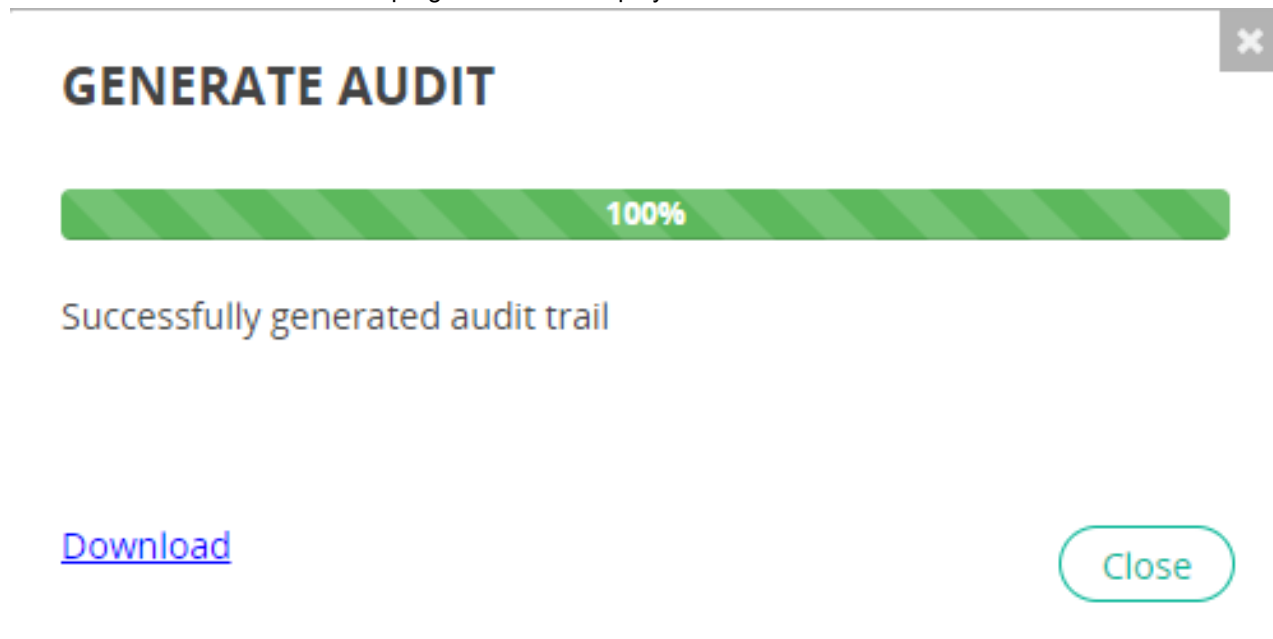
FortiEDR's audit mechanism records every user action in the FortiEDR system. System actions are not recorded. You can download the audit trail to a CSV file for further analysis.

Each time a new audit trail is created, it can be sent through the Syslog.

The screenshot shows the FortiEDR Administration console interface. The top navigation bar includes links to Dashboard, Event Viewer, Forensics, Communication Control, Security Settings, Inventory, and Administration. The left sidebar lists various system components: Licensing, Organizations, Users, Distribution Lists, Export Settings, **TOOLS** (highlighted), System Events, IP Sets, and Integrations. The main content area displays the 'AUDIT TRAIL' configuration page. It includes a 'Download audit trail' button with 'From' and 'To' date pickers, and a 'Generate Audit' button. Below this is the 'COMPONENT AUTHENTICATION' section with a 'Display' button. The 'AUTOMATIC UPDATES' section has a checkbox for 'Automatically update Collectors to the latest revision'. The 'FILE SCAN' section contains two tabs: 'Periodic Scan' and 'Ad hoc scan'. The 'Periodic Scan' tab is active, showing options for 'Perform scheduled scan', 'Frequency' (Bi-Weekly), 'Day' (Monday), 'Hours' (1:00 PM), and 'Scan executable files only'. The 'Ad hoc scan' tab shows options for 'All Collectors', 'Collector Groups', 'Collectors', 'Files/Directories', 'Recursive directory scan', and 'Scan executable files only'. A 'Scan now' button is located at the bottom right of the 'FILE SCAN' section. The 'END USERS NOTIFICATIONS' section at the bottom has a checkbox for 'Show System Tray Icon with Collector Status'.

### To generate the audit trail:

1. Click the **TOOLS** link in the left pane.
2. In the **AUDIT TRAIL** area, specify the *From* and *To* dates in the respective fields.
3. Click the **Generate Audit** button. A progress window displays:



4. Click the **Download** link to download the audit trail to a CSV file or spreadsheet, such as the example shown below, displays:

A	B	C	D	E	F	G	H	I	J	K
1	Date and Time	Sub System	User Name	Description						
2	2/12/2020 14:41	Administration	Barbara	Audit trail from 11-02-2020 to 12-02-2020 was generated						
3	2/12/2020 14:40	Administration	Barbara	Audit trail from 11-02-2020 to 12-02-2020 was generated						
4	2/12/2020 14:15	System	Barbara	System login						
5	2/12/2020 13:34	System	Barbara	System logout						
6	2/12/2020 12:46	System	Barbara	OSX Collectors version "3.1.5 revision 14" for Collector group/s [Insiders] was updated						
7	2/12/2020 12:44	System	Barbara	Automatically update collectors to the latest version was disabled						
8	2/12/2020 12:42	System	Barbara	Automatically update collectors to the latest version was enabled						
9	2/12/2020 12:28	Events	Barbara	Event/s [145793] sent to forensics						
10	2/12/2020 12:27	Events	Barbara	Event/s [141353] sent to forensics						
11	2/12/2020 12:23	Events	Barbara	Event/s [145793] sent to forensics						
12	2/12/2020 12:20	Events	Barbara	Event/s [166577, 166992, 170174] sent to forensics						
13	2/12/2020 12:17	Events	Barbara	Event/s [142194, 142211, 152854, 142203, 142220] sent to forensics						
14	2/12/2020 12:14	Events	Barbara	Event/s [145793, 145803] sent to forensics						
15	2/12/2020 12:14	System	Barbara	System login						
16	2/12/2020 12:14	System	Barbara	System logout						
17	2/12/2020 12:13	Events	Barbara	Event/s [142194, 142211, 152854, 142203, 142220] sent to forensics						
18	2/12/2020 12:12	Events	Barbara	Event/s [142194, 142211, 152854, 142203, 142220] sent to forensics						
19	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						
20	2/12/2020 12:09	Events	Barbara	Event/s [163078, 171302] sent to forensics						
21	2/12/2020 12:07	Events	Barbara	Event/s [163078, 171302] sent to forensics						
22	2/12/2020 12:05	System	lior	System logout						
23	2/12/2020 11:56	Events	Barbara	Event/s [142194, 142211, 152854, 142203, 142220] sent to forensics						
24	2/12/2020 11:56	Inventory	Barbara	Collector [Panda] was unisolated						
25	2/12/2020 11:52	Inventory	Barbara	Collector [Panda] was isolated						
26	2/12/2020 11:49	Events	Barbara	Event/s [180468] sent to forensics						
27	2/12/2020 11:46	Events	Barbara	2 events were marked as read						
28	2/12/2020 11:46	System	Barbara	System login						
29	2/12/2020 11:46	System	Barbara	System login failed						
30	2/12/2020 10:19	System	lior	System logout						
31	2/12/2020 9:41	Administration	lior	IoT discovery was enabled						
32	2/12/2020 9:41	Administration	lior	IoT test was stopped						
33	2/12/2020 9:41	System	lior	System login						
34	2/12/2020 9:16	Administration	lior	IoT test started on Collector [214980]						
35	2/12/2020 9:16	Administration	lior	IoT test was stopped						
36	2/12/2020 9:14	Administration	lior	IoT test started on Collector [214980]						
37	2/12/2020 9:13	Inventory	lior	Collector [qa-performance-2-Test_1] was deleted						
38	2/12/2020 9:13	Inventory	lior	10 IoT device(s) were deleted						
39	2/12/2020 9:13	Administration	lior	IoT test was stopped						
40	2/12/2020 9:11	Administration	lior	IoT test started on Collector [214628]						
41	2/12/2020 9:11	Administration	lior	IoT discovery was disabled						

Each row in the audit trail file contains the following columns of information:

Field	Definition
<i>Date and Time</i>	Displays the date and time in the format <i>yyyy-mm-dd hh:mm:ss</i> .
<i>Sub system</i>	Displays the change type, such as System, Configuration, Administration, Forensics, Events, Inventory, Communication Control or Health.
<i>User Name</i>	Displays the name of the user.
<i>Description</i>	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					

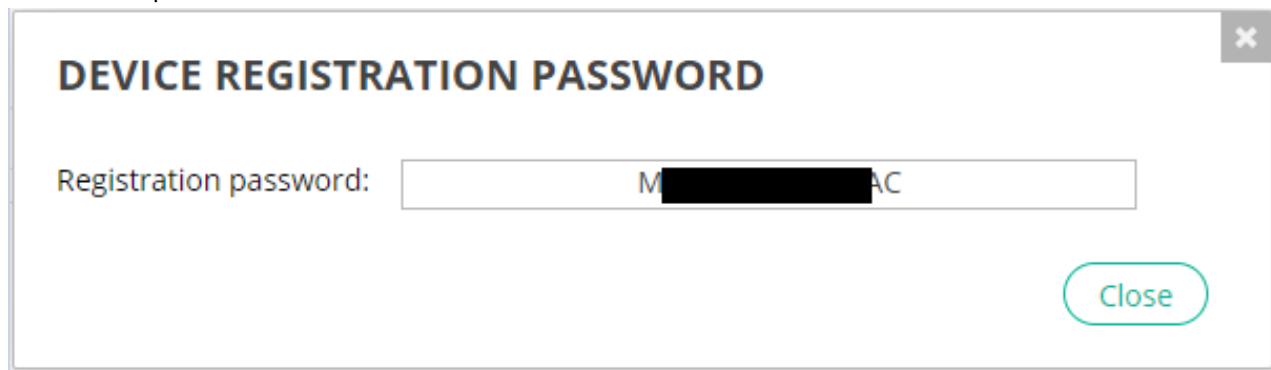
## Component authentication

In order to install, upgrade or uninstall a Collector, you must supply the registration password that you received from Fortinet. The registration password is the same for all Collectors in the FortiEDR system.

If you forget the registration password, you can use the *COMPONENT AUTHENTICATION* option to retrieve it.

**To retrieve the Aggregator password:**

1. Click the *TOOLS* link in the left pane.
2. In the *COMPONENT AUTHENTICATION* area, click the *Display* button. The following window displays, showing the retrieved 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. Click the **TOOLS** link in the left pane.
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.

The screenshot shows the 'FILE SCAN' configuration window. At the top, it states: 'Malicious files that are found during scan will trigger Execution Prevention security event'. Below this, there are two main sections: 'Periodic Scan' and 'Ad hoc scan'. In the 'Periodic Scan' section, the 'Perform scheduled scan' checkbox is checked, with a note 'Last scan: 25-Oct-2020'. There is a 'Save' button. Below the checkbox, there are dropdown menus for 'Frequency' (set to 'Weekly'), 'Day' (set to 'Sunday'), and 'Hours' (set to '4:00 AM'). There are also radio buttons for 'All Collectors' (selected), 'Collector Groups', and 'Collectors'. A checkbox for 'Scan executable files only' is present and unchecked. In the 'Ad hoc scan' section, there are radio buttons for 'All Collectors' (selected), 'Collector Groups', and 'Collectors'. A checkbox for 'Scan executable files only' is present and unchecked. A green 'Scan now' button is located at the bottom right of the 'Ad hoc scan' section.

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. Click the **TOOLS** link in the left pane.
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.

The screenshot shows the 'Ad hoc scan' configuration section. It has a title 'Ad hoc scan'. Below the title, there are radio buttons for 'All Collectors' (selected), 'Collector Groups', and 'Collectors'. A checkbox for 'Scan executable files only' is present and unchecked. A green 'Scan now' button is located at the bottom right of the section.

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 now**. The scan is performed immediately.







## End-user notifications

Each device protected by FortiEDR can display an icon in the system tray to indicate its state.



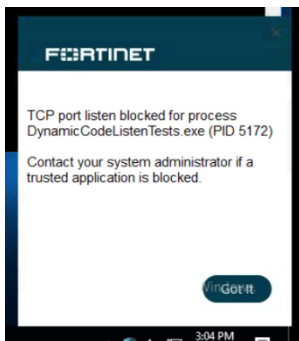
The FortiEDR icon indicates the current state of the device, as follows:

-  Protection On
-  Protection Off/Disabled
-  Degraded
-  Isolated



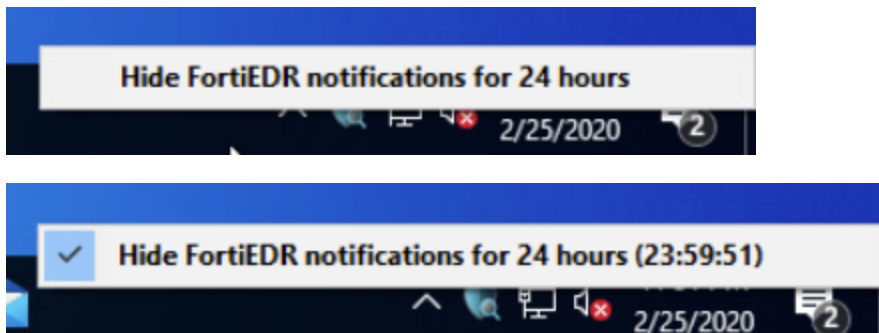
Terminating a FortiEDR process ends this process and stops the display of the FortiEDR icon in the system tray, but does not stop FortiEDR protection.

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.



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:

The screenshot shows the FortiEDR Protection interface. At the top, it says "FORTINET" and "FortiEDR Protection ON Version 5.0.3.206". Below this is the "Activity Log" section. It contains a table with columns: Policy, Process, First Seen, Last Seen, PID, and an expand/collapse icon. There are three entries in the log:

Policy	Process	First Seen	Last Seen	PID	Expand/Collapse
Security	msedge.exe	7/1/2021 10:31:01	7/1/2021 10:31:54	2296	^
Network connection blocked Path: \Device\HarddiskVolume4\Program Files (x86)\Microsoft\Edge\Application\msedge.exe Count: 7					
Security	firefox.exe	7/1/2021 10:30:12	7/1/2021 10:30:12	10388	v
Security	DynamicCodeListenTests.exe	5/23/2021 11:40:18	5/23/2021 11:40:18	4208	v

At the bottom of the log, there is a checkbox labeled "Hide notifications for 24 hours".

## FortiEDR icon configuration

The behavior of the FortiEDR icon in the system tray must be configured in the *Administration* tab.

### To configure FortiEDR icon behavior:

- 1 Click the *TOOLS* link in the left pane.
- 2 In the *END USERS NOTIFICATION* area, configure the following settings:

END USERS NOTIFICATIONS

☒ Show System Tray Icon with Collector Status
 ☒ Show a Pop-up Message for Any Prevention Activity

Note: Maximum 250 characters

Save

Setting	Definition
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

Setting	Definition
	device. Your selection here is applied on all protected devices. The default is checked.
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 these two 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.

- Click the **Save** button.

## 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 122](#).



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.

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 122](#).

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.

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).

## 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.

The GDPR standard requires that all relevant data for an employee of a company that is using the FortiEDR system or a FortiEDR user be removed from the FortiEDR system, once he/she no longer has access to or uses the FortiEDR system.

In FortiEDR, the GDPR feature is implemented in the *Personal Data Handling* area of the *Tools* window.

## PERSONAL DATA HANDLING

Search by


## Export report of monitored users

Export

To fully comply with the GDPR standard, the employee's/user's device name, IP address, MAC address, and user name must all be totally removed from the FortiEDR system. This data is deleted from FortiEDR in real time, from everywhere that it appears in the FortiEDR system (for example, from the Inventory, Event Viewer, Audit Trail and so on).

The GDPR regulation obligates you to notify your users, should the FortiEDR system be hacked. You can use the *Export report of monitored users* button to export the list of monitored users in the FortiEDR system. This action exports a report such as the one shown below:

The screenshot shows a Microsoft Excel spreadsheet with the following content:

	A	B	C	D	E	F	G
1		liorgolf444	Report created by user Barbara on 12-Feb-2020, 14:55		Confidential		
2	Users						
3	USER NAME						
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							

**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 page 55.



Be sure to do this for all the employee's/user's computers on which Collectors are installed.

2. Click the *TOOLS* link in the left pane.
3. In the *Personal Data Handling* area you must specify the device name, IP address, MAC address, and user name of the employee/user to be removed from FortiEDR.



If the employee/user has multiple computers on which Collectors are installed, you must repeat the steps below for each of his/her computers.

Removing an employee/user for GDPR compliance requires an iterative process in FortiEDR 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. For the purpose of example, we will start by removing all Device name data for the employee/user.

**IMPORTANT** – You can remove the device name, IP address, MAC address, and user name of the employee/user from FortiEDR in any order that you prefer. However, 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.

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.

Device name  
IP address  
MAC address  
User name

PERSONAL DATA HANDLING

Search by

Export report of monitored users

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)									
<input type="button" value="Create Group"/> <input type="button" value="Move to Group"/> <input type="button" value="Delete"/> <input type="button" value="Enable/Disable"/> <input type="button" value="Isolate"/> <input type="button" value="Export"/> <input type="button" value="Uninstall"/>									
<input type="checkbox"/>	COLLECTOR GROUP NAME	DEVICE NAME	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	STATE	LAST SEEN
<input type="checkbox"/>	High Security Collector Group (0/0)								
<input type="checkbox"/>	a (0/0)								
<input type="checkbox"/>	A (0/0)								
<input type="checkbox"/>	Accounting (0/0)								
<input type="checkbox"/>	A Victim (0/0)								
<input type="checkbox"/>	Default VDI Group (0/0)								
<input type="checkbox"/>	emu (5/5)								
<input type="checkbox"/>		DESKTOP-RMR951H-0-Test_6	None	Windows 7		05-50-56-BE-79-A2	3.0.0.36	Disconnected (Expired)	916 days ago
<input type="checkbox"/>		DESKTOP-RMR951H-0-Test_7	None	Windows 7		06-50-56-BE-79-A2	3.0.0.36	Disconnected (Expired)	916 days ago
<input type="checkbox"/>		DESKTOP-RMR951H-0-Test_8	None	Windows 7		07-50-56-BE-79-A2	3.0.0.36	Disconnected (Expired)	916 days ago
<input type="checkbox"/>		DESKTOP-RMR951H-0-Test_9	None	Windows 7		08-50-56-BE-79-A2	3.0.0.36	Disconnected (Expired)	916 days ago
<input type="checkbox"/>		Tzafit-Lenovo	...	Windows 10 Pro	192.168.14.37	F8-63-3F-AF-28-A5, 8C...	3.1.0.407	Disconnected	Today

In a similar manner, you can locate the user name in the Event Viewer, and then copy/paste that information into the adjacent field in the *Personal Data Handling* area, as shown below:

EVENTS									
<input type="button" value="Archive"/> <input type="button" value="Mark All"/> <input type="button" value="Export"/> <input type="button" value="Handle Event"/> <input type="button" value="Delete"/> <input type="button" value="Forensics"/> <input type="button" value="Exception Manager"/>									
<input type="checkbox"/>	All	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED	
<input type="checkbox"/>		ENSW-LAP107-1-Test_1 (15 events)			Malicious		02-Jul-2018, 14:23:49		
<input type="checkbox"/>		SnirMar-PC-4-Test_1 (104 events)			Malicious		02-Jul-2018, 15:22:58		
<input type="checkbox"/>		DESKTOP-3QINVIU (2 events)			PUP		16-Mar-2020, 14:18:52		
<input type="checkbox"/>		663219	DESKTOP-3QINVIU	EXCEL.EXE	PUP	2 destinations	03-Jan-2019, 12:09:41	04-Feb-2019, 15:13:46	
<input type="checkbox"/>		Logged-in User: <u>DESKTOP-3QINVIU\Tzafit</u> Certificate: Signed Process path: \Device\HarddiskVolume3\Program Files (x86)\Microsoft Office\root\Office16\EXCEL.EXE Raw data items: 4							
<input type="checkbox"/>		30558956	DESKTOP-3QINVIU	netsh.exe	Safe	File Execution AL...	16-Mar-2020, 14:18:52	16-Mar-2020, 15:24:03	

**CLASSIFICATION DETAILS**

PUP

Threat name: Unknown  
Threat family: Unknown  
Threat type: Unknown

**History**

PUP, by tzafit , on 10-Apr-2019, 21:23:44

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, as shown below, click *Search* to search for all occurrences of the device name in the FortiEDR system.

## PERSONAL DATA HANDLING

Search by

Export report of monitored users

The following displays, listing all matching results:

### ACTIVITY REPORT

Device name contains "DESKTOP-81\_32"

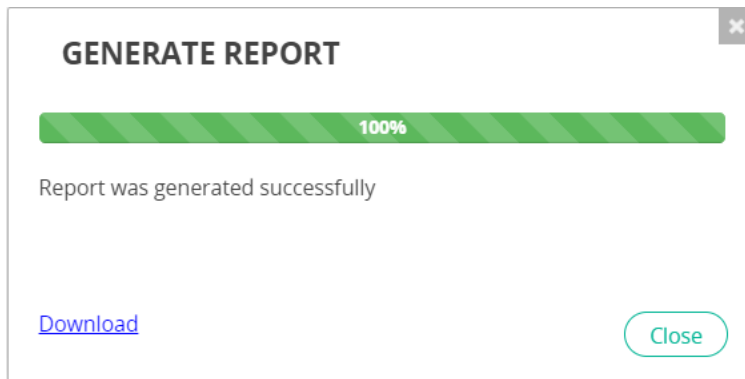
1 result found

DESKTOP-81_32	12 records
---------------	------------

\* The number of records in the exported report, may be larger than the initial report

7. Do one of the following:
  - a. Click the *Export Report* button to export a report of the data to be removed for the employee/user. This option enables you to keep a record of what will be deleted. However, use of this option is not recommended, as all traces of the employee's/user's data are to be permanently removed, including this report.  
The following displays after the report has been exported:

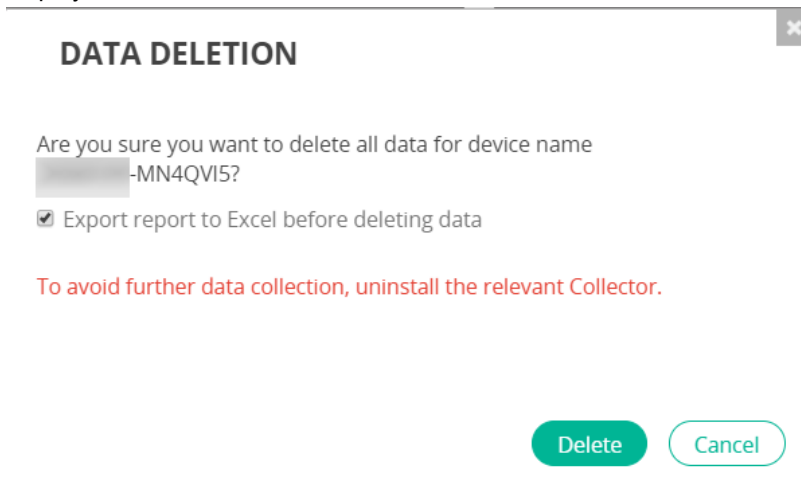




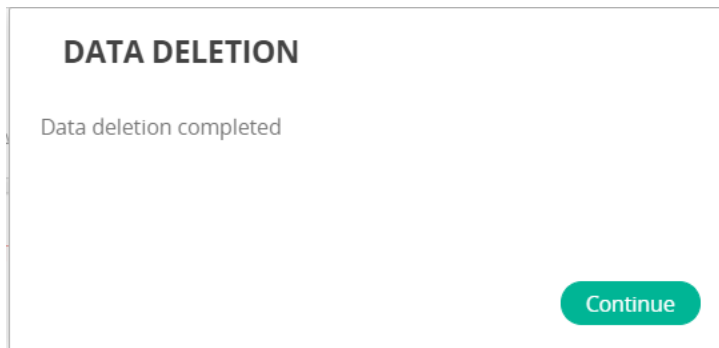
Click the *Download* link to download the Excel report. An example of the downloaded report is shown below:

Report created by user Barbara on 12-Feb-2020, 15:14							
<b>FORTINET</b>		liorgolf444		Report created by user Barbara on 12-Feb-2020, 15:14		Confidential	
Search value	10.51.121.109						
<b>Personal Data</b>							
TYPE	USER NAME	HOST NAME	IP	MAC	ID	LOGGED IN USERS	DESCRIPTION
Collector		Panda1	10.51.121.109	00-0C-29-34-97-1B		PANDA1\root	

- b. Click the *Delete All Records* button to remove all device name data for the employee/user. The following displays:



Click *Delete* to remove all device name data for the employee/user from FortiEDR. After several moments, the following displays, indicating that the data has been removed:



You can check the *Export report to Excel before deleting data* checkbox if you want to export the data before it is removed from FortiEDR.

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.

### Personal Data Handling of Threat Hunting Data

The search performed by Personal Data Handling (described above) does not show activity event data. This data will be deleted in case you use the delete option (described above), even though it is not displayed in the search results. If you're interested in seeing the activity data that will be deleted, you can view it by using the *Search* option of the Threat Hunting feature, as described in [Threat Hunting on page 237](#).

## 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. When registering FortiEDR Collectors, Windows Security Center indicates that your system has anti-virus and threat protection provided by FortiEDR.

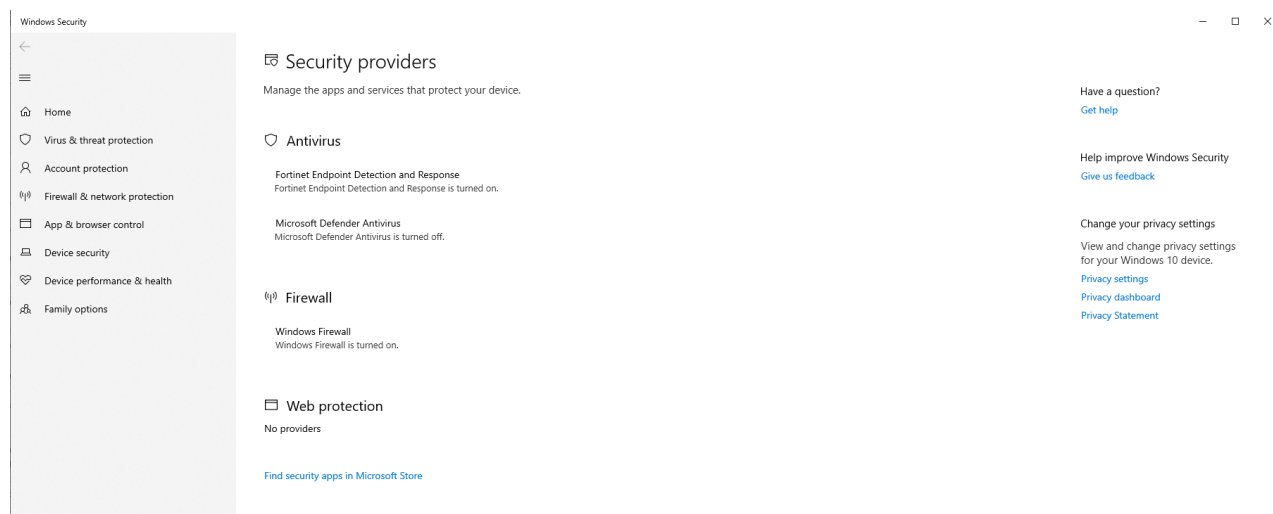
Note that in some cases, registering FortiEDR in Windows Security Center may prevent other vendors' products from installing or functioning properly. Therefore, you can choose whether or not to register FortiEDR Collectors. Your system is still fully protected, even if you do not choose to register FortiEDR Collectors with Windows Security Center.

The screenshot shows the FortiEDR Administration console with the 'ADMINISTRATION' tab selected. The 'WINDOWS SECURITY CENTER' section is highlighted, showing a checkbox labeled 'Register Collectors to Windows Security Center'. A blue arrow points to this checkbox. Other sections visible include 'END USERS NOTIFICATIONS', 'IOT DEVICE DISCOVERY', and 'PERSONAL DATA HANDLING'.

### To register FortiEDR Collectors with Windows Security Center:

- In the **ADMINISTRATION** tab, navigate to the **Tools > Windows Security Center** area, and then check the **Register Collectors to Windows Security Center** checkbox.

When registered, FortiEDR is listed under Windows Security, as follows:



## 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 267](#). 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 285](#).



The *Establish FortiEDR Connect sessions* checkbox is available for Admin, Analyst, and Senior Analyst users only.

## System events

Selecting *SYSTEM EVENTS* in the *ADMINISTRATION* tab displays all the system events relevant to the FortiEDR system.

SYSTEM EVENTS				
<input type="checkbox"/> Mark As... <input type="checkbox"/> Export <input type="checkbox"/> Delete		Showing 1-17/3998		Search System Event (syst... <input type="text"/> )
<input type="checkbox"/> All	COMPONENT TYPE	COMPONENT NAME	DESCRIPTION	DATE
<input type="checkbox"/>	Collector	Collector [redacted]	Collector [redacted] state was changed to "Running".	20-Mar-2023, 18:34:19
<input type="checkbox"/>	Collector	Collector [redacted]	Collector [redacted] state was changed to "Degraded". Warnings: The Core is not accessible. Please check netw...	20-Mar-2023, 18:34:00
<input type="checkbox"/>	Manager	Manager [redacted]	Connection to Syslog failed. mysyslog [redacted]	20-Mar-2023, 03:52:11
<input type="checkbox"/>	Manager	Manager [redacted]	Connection to Syslog failed. mysyslog [redacted]	20-Mar-2023, 03:52:02
<input type="checkbox"/>	Core	Core [redacted]	Core [redacted] state was changed to "Running"	20-Mar-2023, 03:49:00
<input type="checkbox"/>	Aggregator	Aggregator [redacted]	Aggregator [redacted] state was changed to "Running"	20-Mar-2023, 03:48:39
<input type="checkbox"/>	Repository	Repository [redacted]	Threat-hunting state was changed to "Running"	20-Mar-2023, 03:48:39
<input type="checkbox"/>	Manager	Manager [redacted]	Server was restarted	20-Mar-2023, 03:48:39
<input type="checkbox"/>	Core	Core [redacted]	Core [redacted] state was changed to "Disconnected". Warnings: The following connectors will ...	20-Mar-2023, 03:45:38
<input type="checkbox"/>	Aggregator	Aggregator [redacted]	Aggregator [redacted] state was changed to "Disconnected"	20-Mar-2023, 03:45:37
<input type="checkbox"/>	Collector	Collector [redacted]	Collector [redacted] state was changed to "Degraded". Warnings: Unknown error .	19-Mar-2023, 06:00:11
<input type="checkbox"/>	Collector	Collector [redacted]	Collector [redacted] was registered and added to the system	19-Mar-2023, 05:59:30
<input type="checkbox"/>	Collector	Collector [redacted]	Collector [redacted] state was changed to "Running".	15-Mar-2023, 03:57:01
<input type="checkbox"/>	Collector	Collector [redacted]	Collector [redacted] state was changed to "Degraded". Warnings: The Core is not accessible. Please check networ...	15-Mar-2023, 03:56:51
<input type="checkbox"/>	Collector	Collector [redacted]	Collector [redacted] state was changed to "disconnected (expired)"	14-Mar-2023, 20:00:00
<input type="checkbox"/>	Collector	Collector [redacted]	Collector [redacted] state was changed to "Running".	14-Mar-2023, 10:42:21
<input type="checkbox"/>	Collector	Collector [redacted]	Collector [redacted] state was changed to "Degraded". Warnings: There is no available configuration. Please conta...	14-Mar-2023, 10:42:11

Use the search bar on the top right corner to filter system events by keywords.

Search System Event (syst...


Use the *Advanced search* button to filter system events by component with a date range, which you can specify in the *SEARCH SYSTEM EVENT* window.


Search System Event (syst...

Advanced search

### SEARCH SYSTEM EVENT ×

Date

From  

To  

Component Type

Component Name

Search

Cancel



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 311](#). You can also configure [Syslog on page 314](#) 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.
- License will expire in 21/7 days/1 day
- License expired

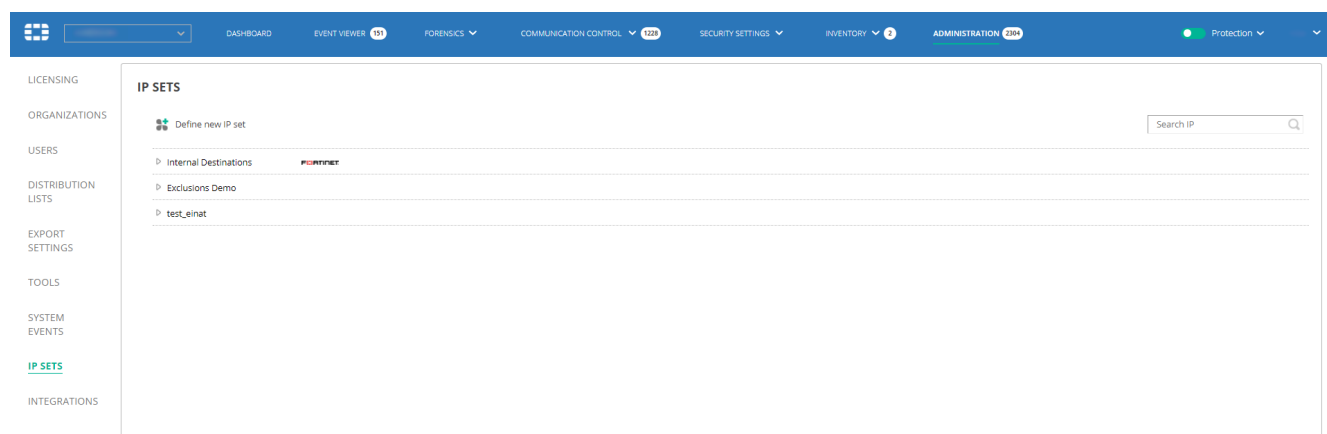
- License capacity of workstations has reached 90/95/100%
- License capacity of servers has reached 90/95/100%
- System mode was changed from Prevention to Simulation or vice versa
- FortiEDR Cloud Service (FCS) connectivity is down

## 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 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



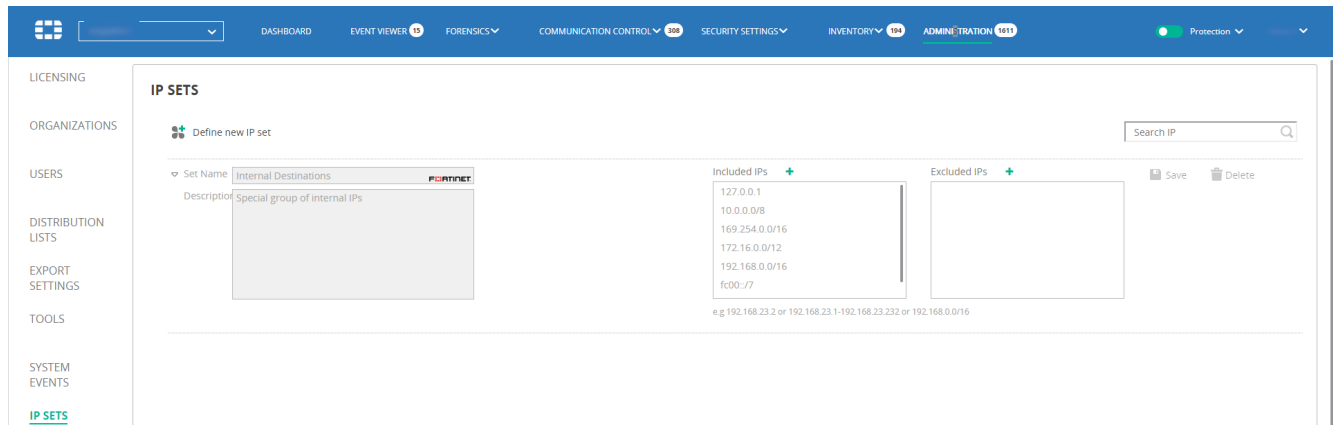
Using IP Sets in exceptions is not supported since there are still Windows Collectors with version older than 3.0.0.0. Please upgrade your environment.

Continue

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.

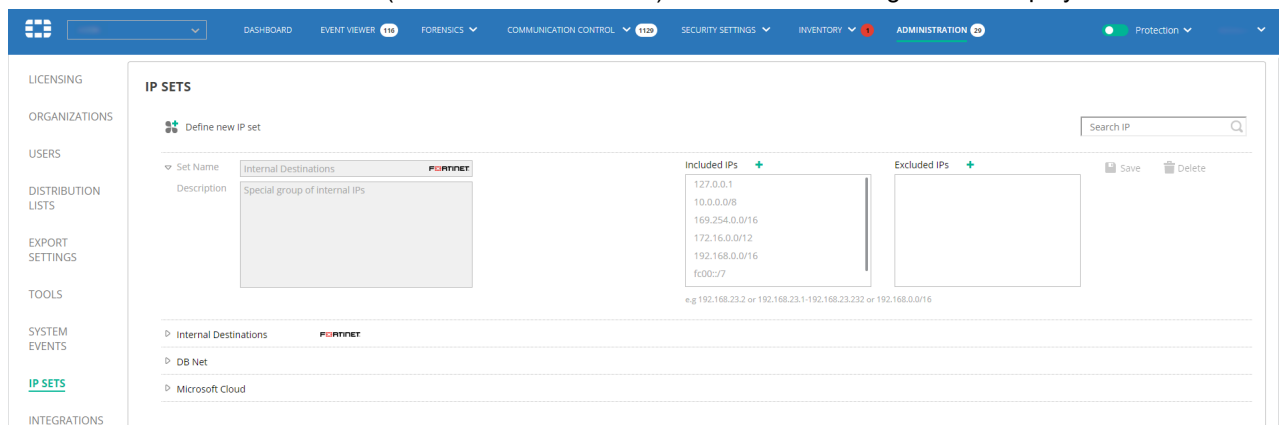
The *IP Sets* page lists all the IP sets. Users can only edit an IP set that was specifically created for his/her organization. For example, if the administrator is assigned to only organization A, he/she can edit an IP set create for organization A but not an IP set that applies to all organizations.

Click the **FORTINET** logo in the Internal Destinations row to view its definition, as shown below:



## To define an IP set:

1. Click the *Define new IP set* button ( **Define new IP set** ) button. The following window displays:



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.

- 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, as described in [Defining a security event as an exception on page 164](#).

## Integrations

Integrations 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 285](#).

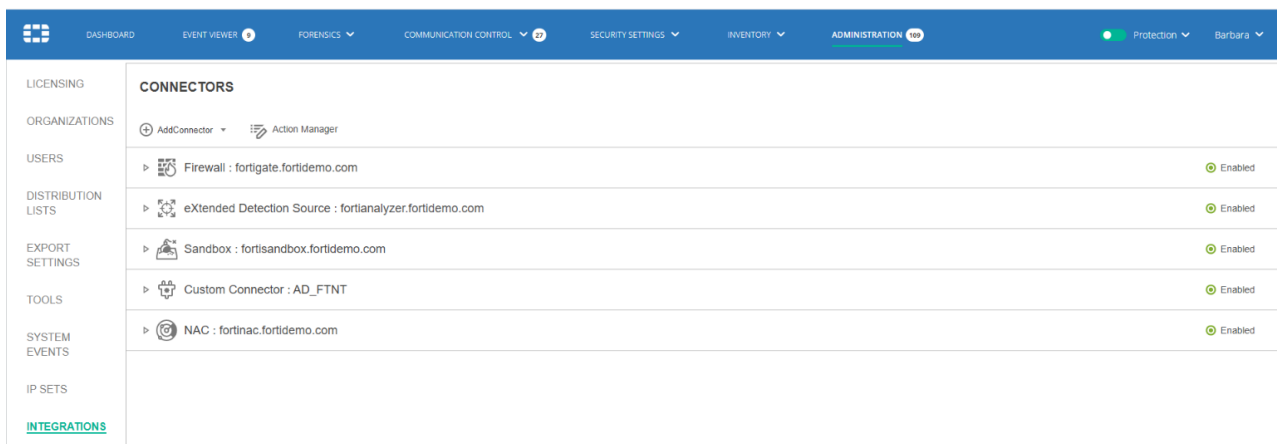
You can set up an unlimited number of connectors for each type and use them by associating Playbook policies or Security policies to the actions defined for these integration connectors, as described below.



The **Integration** menu is only available when the environment is connected to Fortinet Cloud Services (FCS).

To display the **INTEGRATIONS** page:

- Select **ADMINISTRATION > INTEGRATIONS**.



The top left of this page provides two buttons, as shown below:





- [Adding connectors on page 337](#) enables you to add and configure connectors for integration with FortiEDR.
- [Action Manager on page 369](#) 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 285](#).

## Adding connectors

The following types of integration connectors are provided to be configured:

- [Firewall integration on page 337](#)
- [Network Access Control \(NAC\) integration on page 345](#)
- [Identity Management integration on page 350](#)
- [User Access integration on page 354](#)
- [Sandbox integration on page 359](#)
- [eXtended detection source integration on page 361](#)
- [Custom integration on page 365](#)



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 285](#).

You can enable or disable a connector by clicking the *Enabled/Disabled* button next to the connector name. This button toggles between *Enabled/Disabled*.

CONNECTORS	
<div> <span>+</span> Add Connector           <span>⚙️</span> Action Manager         </div>	
<div> <span>▶</span>  Firewall : UK office FGT         </div>	<div> <span>●</span> Enabled         </div>
<div> <span>▶</span>  Firewall : MyFW         </div>	<div> <span>○</span> Disabled         </div>

## 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.

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 a FortiEDR Core as a Jumpbox on page 57](#). You may refer to [Cores on page 127](#) 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. Please refer to FortiGate documentation at <https://docs.fortinet.com/> for details about how an API user can be added.

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.

FortiGate VM64-GCP FGVMD0

★ Favorites > Edit Address Group

Dashboard >

Security Fabric >

FortiView >

Network >

System >

Policy & Objects > ✓

IPv4 Policy

Authentication Rules

IPv4 DoS Policy

Addresses ☆

Wildcard FQDN Addresses

Internet Service Database

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

OK Cancel

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:

**CONNECTORS**

+ AddConnector Action Manager

eXtended Detection Source : fortianalyzer.fortidemo.com	Enabled
Sandbox : fortisandbox.fortidemo.com	Enabled
Firewall : fortigate.fortidemo.com	Enabled

JumpBox: core-europe-west

Details

Name: fortigate.fortidemo.com Type: FortiGate Host: Port: 443

API Key Credentials

Username: Password:

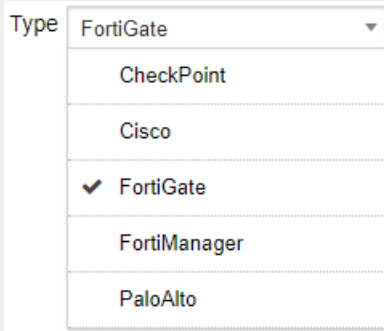
Actions

Block address on Firewall Assign NSX tag Add MAC Quarantine + Add action

Address group: FortiEDR\_Malicious\_Destinati

Save Cancel Delete

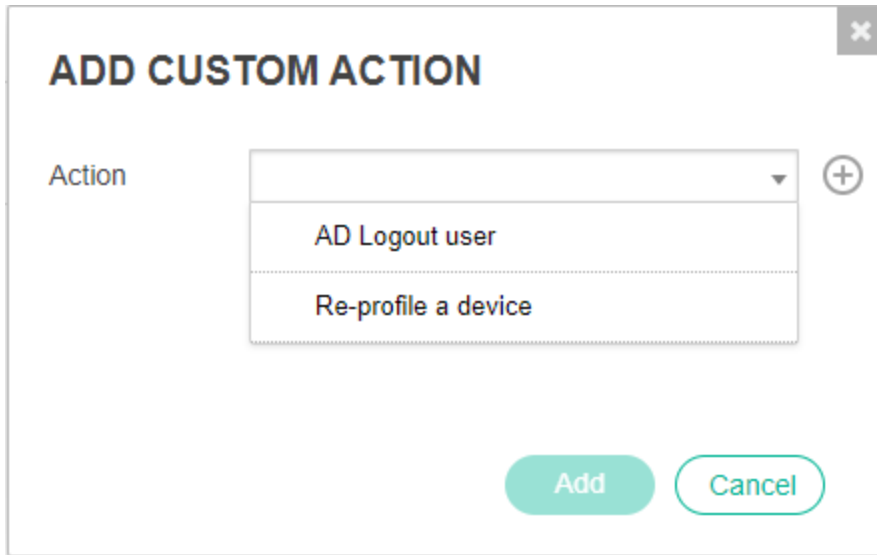
## 2. Fill in the following fields:

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	<p>Select the type of firewall to be used in the dropdown list.</p> 
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 <i>API Key</i> radio button and copy the token value into the text box. To use API credentials, click the <i>Credentials</i> 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.  
– 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

+ Add action

New action

Add Policy Block

Add MAC Quarantine

Disable interface

Assign NSX tag

Slack Notification

Teams Notification

AWS Lambda Logout User

Name

New action

Description

Action Scripts ?

Upload

Please upload a script

Save

Cancel


Close

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.

Field	Definition
Upload	<p>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 <i>Action Scripts</i> 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.</p> <div data-bbox="649 531 1433 1150"> <p><b>Creating A Custom Incident Response Action</b></p> <p>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.</p> <p><b>Code Conventions</b></p> <ul style="list-style-type: none"> <li>• A FortiEDR JumpBox on which one or more scripts are executed is deployed with various standard Python packages. <a href="#">Click here</a> to see a list of the packages that are deployed with this type of FortiEDR JumpBox.</li> <li>• At the moment, only Python 2 is supported.</li> <li>• Parameters <ul style="list-style-type: none"> <li>◦ 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).</li> <li>◦ These properties are stored in the config.json file and can be used as script parameters.</li> <li>◦ <a href="#">Click here</a> to see a sample config.json file and a sample action script:</li> </ul> </li> </ul> <p><a href="#">↓ custom_script.py</a>   <a href="#">↓ config.json</a></p> <p><b>Troubleshooting</b></p> <p>Script execution (either in test mode or as part of a realtime incident response) is defined as</p> <p><a href="#">Close</a></p> </div>

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	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Delete file	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Clean persistent data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Block address on Firewall	FortiGate300 <input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	 Test playbook	<input checked="" type="checkbox"/>				
<input type="checkbox"/>	 Victims Playbook	<input checked="" type="checkbox"/>				
<input type="checkbox"/>	 Victims Playbook clone	<input checked="" type="checkbox"/>				

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	<div><div></div></div>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	AWS Lambda Logout User	<div><div>Select All</div></div>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Disable Interface	<div><div>fortinac.fortidemo.com</div></div>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Slack Notification	<div><div>fortigate.fortide...</div></div>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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 *CLASSIFICATION DETAILS* area of the *Events* page of the FortiEDR Console, as shown below:

[Dashboard](#)
[Event Viewer](#)
[Forensics](#)
[Communication Control](#)
[Security Settings](#)
[Inventory](#)
[Administration](#)

● Protection
Tzafit

---

### EVENTS

Archive
 Mark As ...
 Export ▾
 Handle Event
 Delete
 Forensics
 Exception Manager

<input type="checkbox"/>	Unhandled	ID	DEVICE	PROCESS	CLASSIFICATION ▾	DESTINATIONS	RECEIVED ▾	LAST UPDATED
<input checked="" type="checkbox"/>		<b>adprivacyd (1 event)</b>						
<input type="checkbox"/>		236471	LiorMacOSPara10-14	adprivacyd	Inconclusive	2 destinations	16-Feb-2020, 19:56:53	16-Feb-2020, 20:16:21
<p> Certificate: Signed    Process path: ...veloper\CoreSimulator\Profiles\RuntimeMes\IOS.simruntime\Contents\Resources\RuntimeRoot\usr\libexec\adprivacyd    Raw data items: 2</p>								
<input type="checkbox"/>		<b>healthappd (1 event)</b>						
<input type="checkbox"/>		<b>trustd (1 event)</b>						
<input type="checkbox"/>		<b>geod (1 event)</b>						
<input type="checkbox"/>		<b>dynamiccodetests.exe (1 event)</b>						
<input type="checkbox"/>		<b>pandasecurityDx.dll (2 events)</b>						
<input type="checkbox"/>		<b>pandasecurityDx64.dll (1 event)</b>						
<input type="checkbox"/>		<b>TeamViewer.exe (1 event)</b>						
<input type="checkbox"/>		<b>DynamicCodeTests32.exe (1 event)</b>						
<input type="checkbox"/>		<b>cscript.exe (4 events)</b>						
<input type="checkbox"/>		<b>dumb-init (1 event)</b>						
<input type="checkbox"/>		<b>filebeat.exe (1 event)</b>						
<input type="checkbox"/>		<b>979c6de81cc0f4e0e770f720eb8c728a2d422fe... (2 events)</b>						
<input type="checkbox"/>		<b>B03276BFBF85CFDD7C8998004C1200DA.vir (2 events)</b>						

### CLASSIFICATION DETAILS

Inconclusive **Fortinet**
By ReversingLabs

Threat name: Unknown  
Threat family: Unknown  
Threat type: Unknown

---

#### History

- Inconclusive, by FortinetCloudServices , on 16-Feb-2020, 20:37:26
  - IP address 198.203.178.52 was blocked on FortiGate GVM02TM19005776
  - Device MyMac11-16 was moved to quarantine network High Security VLAN

---

#### Triggered Rules

- Exfiltration Prevention
  - Invalid Execution - Code Executed from an Invalid Memory L...

### ADVANCED DATA



## 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 a FortiEDR Core as a Jumpbox on page 57](#). You may refer to [Cores on page 127](#) 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:

**CONNECTORS**

+ Add Connector | Action Manager

▼ NAC Enabled

JumpBox

Details

Name  Type  Host  Port

☒ API Key ☐ Credentials

Key

Actions

Isolate device on NAC

+ Add action

2. Fill in the following fields:

Field	Definition
JumpBox	Select the FortiEDR JumpBox that will communicate with this NAC system.
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.

Field	Definition
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 <i>Credentials</i> 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 365](#)).

- 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 365](#)).

- 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:

Action Manager

+ Add action

New action

Add Policy Block

Add MAC Quarantine

Disable interface

Assign NSX tag

Slack Notification

Teams Notification

AWS Lambda Logout User

Name

New action

Description

Action Scripts ?

Upload

Please upload a script

Save

Cancel


Close

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

Field	Definition
	<p>displayed by clicking the icon  next to the <i>Action Scripts</i> 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.</p>

### 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. Click [here](#) to see 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

[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.

## 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		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Isolate device with NAC	Nac_HK	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Move device to the High Security Group		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

FortiEDR is now configured to automatically isolate the device upon triggering of a security event. Automatic incident response actions are listed in the **CLASSIFICATION DETAILS** area of the **Events** page of the FortiEDR Console as shown below:

The screenshot shows the FortiEDR Console interface. The top navigation bar includes tabs for DASHBOARD, EVENT VIEWER, FORENSICS, COMMUNICATION CONTROL, SECURITY SETTINGS, INVENTORY, and ADMINISTRATION. The main content area is divided into two sections: **EVENTS** and **CLASSIFICATION DETAILS**.

The **EVENTS** section displays a table with columns: ID, DEVICE, PROCESS, CLASSIFICATION, DESTINATIONS, RECEIVED, and LAST UPDATED. The table shows three events related to 'DynamicCodeTests.exe'. The first event (ID 114857) is classified as 'Suspicious' and occurred on 14-Jan-2021 at 02:14:27. The second event (ID 114845) is also classified as 'Suspicious' and occurred on 14-Jan-2021 at 02:14:27. The third event (ID 114845) is classified as 'Suspicious' and occurred on 14-Jan-2021 at 08:50:59.

The **CLASSIFICATION DETAILS** sidebar on the right provides more information about the selected event. It shows the threat name as 'Unknown', the threat family as 'Unknown', and the threat type as 'Unknown'. It also lists the history of the event, showing that it was triggered by 'FortinetCloudServices' on 14-Jan-2021 at 08:51:13. The sidebar also lists the triggered rules, including 'Exfiltration Prevention', 'Dynamic Code - Malicious Runtime Generated Code Detected', and 'Unmapped Executable - Executable File Without a Correspon...'. At the bottom of the sidebar, there is a section for 'ADVANCED DATA'.

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		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	AWS Lambda Logout User	Select All	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Disable interface	fortinac.fortidemo.com	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Slack Notification	fortigate.fortide...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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 **CLASSIFICATION DETAILS** area of the **Events** page of the FortiEDR Console.

The screenshot displays the FortiEDR console interface. On the left, the 'EVENTS' section shows a table of security events. The first event is 'DynamicCodeTests\_1.exe' (1 event) with ID 96879, classified as 'Suspicious'. It was received on 30-Jun-2021 at 10:36:28. The event details show it was logged by user 'er1' on a 'WIN10-64BIT-120/user1' device. The process path is 'C:\Users\user1\Desktop\Tudo boomboom\_folder\DynamicCodeTests\_1.exe' and it has 2 raw data items. On the right, the 'CLASSIFICATION DETAILS' section shows the threat name as 'Unknown', threat family as 'Unknown', and threat type as 'Unknown'. It also lists automated analysis steps completed by Fortinet Details, a history of the event being suspicious by FortinetCloudServices, and triggered rules including 'Exfiltration Prevention' and 'Dynamic Code - Malicious Runtime Generated Code Detected'.

## 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.

### Prerequisites

Before you start Identity Management configuration, verify the following:

- Your FortiEDR deployment includes a JumpBox that has connectivity to the identity management server. Details about how to install a FortiEDR Core and configure it as a JumpBox are described in [Setting up a FortiEDR Core as a Jumpbox on page 57](#). You may refer to [Cores on page 127](#) 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 FortiClient EMS or equivalent identity management system.

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:

The screenshot shows the 'CONNECTORS' configuration page in the FortiEDR console. The 'Identity Management' connector is selected and is currently 'Enabled'. The configuration details include a 'JumpBox' dropdown menu, a 'Name' field, a 'Type' dropdown menu, a 'Host' field, and a 'Port' field set to '443'. There are radio buttons for 'API Key' (selected) and 'Credentials', and a 'Key' field. The 'Actions' section shows 'ZeroTrust device tagging' as the selected action, with a 'Tag name' field and a 'Test' button. There are 'Save' and 'Delete' buttons at the bottom right.

## 2. Fill in the following fields:

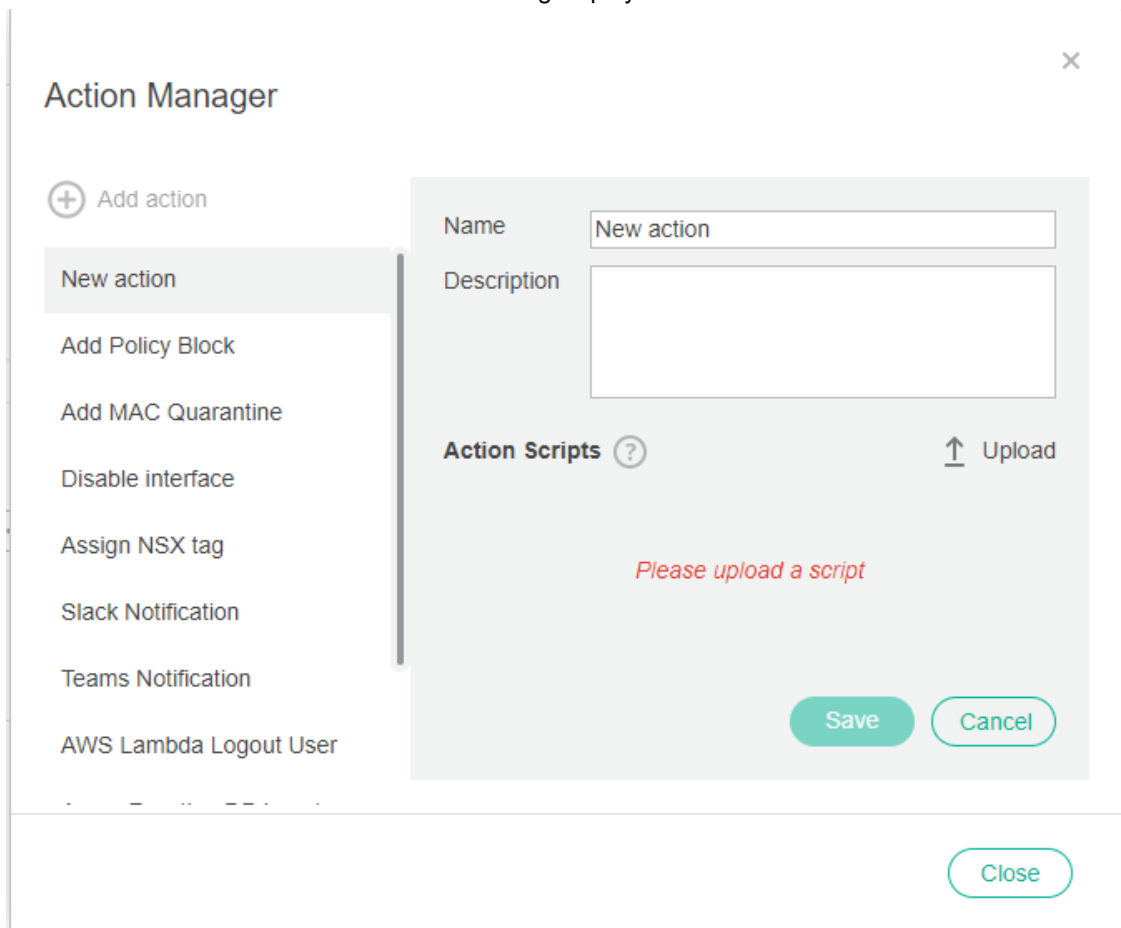
Field	Description
JumpBox	Select the FortiEDR JumpBox that will communicate with this Identity Management system.
Name	Specify a name of your choice to be used to identify this Identity Management system.
Type	Select the type of Identity Management to be used in the dropdown list. For example, <i>FortiClient EMS</i> .
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.

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 what tag to apply on the device in the *Tag name* field.
- To use a custom integration action:
  - Click the + *Add Action* button. The following popup window displays:

- In the *Action* dropdown menu, select one of the previously defined actions (which were defined in FortiEDR as described in [Identity Management integration on page 350](#)), 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:



The screenshot shows the 'Action Manager' window. On the left is a sidebar with a list of actions: 'New action' (highlighted), 'Add Policy Block', 'Add MAC Quarantine', 'Disable interface', 'Assign NSX tag', 'Slack Notification', 'Teams Notification', and 'AWS Lambda Logout User'. The main area contains a form with fields for 'Name' (containing 'New action') and 'Description'. Below these is a section for 'Action Scripts' with a question mark icon and an 'Upload' button. A red message 'Please upload a script' is displayed. At the bottom right of the form are 'Save' and 'Cancel' buttons. A 'Close' button is located at the bottom right of the entire window.


- 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.



Field	Definition
Upload	<p>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 <i>Action Scripts</i> 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.</p> <div> <p><b>Creating A Custom Incident Response Action</b></p> <p>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.</p> <p><b>Code Conventions</b></p> <ul style="list-style-type: none"> <li>A FortiEDR JumpBox on which one or more scripts are executed is deployed with various standard Python packages. <a href="#">Click here</a> to see a list of the packages that are deployed with this type of FortiEDR JumpBox.</li> <li>At the moment, only Python 2 is supported.</li> <li>Parameters           <ul style="list-style-type: none"> <li>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).</li> <li>These properties are stored in the config.json file and can be used as script parameters.</li> <li><a href="#">Click here</a> to see a sample config.json file and a sample action script:</li> </ul> </li> </ul> <p><a href="#">↓ custom_script.py</a>   <a href="#">↓ config.json</a></p> <p><b>Troubleshooting</b></p> <p>Script execution (either in test mode or as part of a realtime incident response) is defined as</p> <p><a href="#">Close</a></p> </div>

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 *INVESTIGATION* section.

FortiEDR is now configured to automatically tag a device as non-trusted upon triggering of a security event.

REMEDIATION						
	Terminate process	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Delete file	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Clean persistent data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Block address on Firewall <span>Select Firewalls.....</span>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	ZeroTrust device tagging <span>FortiClient EMS ...</span>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Reset user password <span>Select UserAcce...</span>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## 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 **CLASSIFICATION DETAILS** area of the **Events** page of the FortiEDR Console, as shown below:

The screenshot displays the FortiEDR Console interface. The main panel shows a table of security events with columns: ID, DEVICE, PROCESS, CLASSIFICATION, DESTINATIONS, RECEIVED, and LAST UPDATED. The table lists several events, including those from DESKTOP-52GG7K5, DESKTOP-6AV68KU, DESKTOP-K3EL7HF, DESKTOP-RR8JDDG, and DESKTOP-PSOR95V. The classification for most events is 'Malicious', while one is 'Inconclusive'. The right sidebar, titled 'CLASSIFICATION DETAILS', provides information for a selected 'Malicious' event, including threat name, family, type, and a history of automated analysis steps.

ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
DESKTOP-52GG7K5 (11 events)			Malicious		20-Sep-2022, 17:00:00	21-Sep-2022, 22:00:00
DESKTOP-6AV68KU (5 events)			Malicious		14-Sep-2022, 19:15:36	23-Sep-2022, 16:29:51
DESKTOP-K3EL7HF (6 events)			Malicious		11-Sep-2022, 00:00:00	18-Sep-2022, 00:00:00
DESKTOP-RR8JDDG (3 events)			Malicious		11-Sep-2022, 00:00:00	18-Sep-2022, 00:00:00
DESKTOP-PSOR95V (6 events)			Malicious		07-Sep-2022, 11:38:36	23-Sep-2022, 07:14:33
50347	DESKTOP-PSOR95V	firefox.exe	Inconclusive	Service Access	30-Aug-2022, 15:30:57	30-Aug-2022, 15:30:57
68825	DESKTOP-PSOR95V	ConnectivityTestApp.exe	Malicious	8.8.8.8	07-Sep-2022, 11:38:36	14-Sep-2022, 12:08:01
51153	DESKTOP-PSOR95V	ConnectivityTestApp.exe	Malicious	File Read Attempt	31-Aug-2022, 15:22:33	23-Sep-2022, 07:14:33
46108	DESKTOP-PSOR95V	ConnectivityTestApp.exe	Malicious	8.8.8.8	29-Aug-2022, 13:05:44	31-Aug-2022, 15:42:12
46091	DESKTOP-PSOR95V	ConnectivityTestApp.exe	Malicious	2 destinations	29-Aug-2022, 13:05:44	23-Sep-2022, 07:14:33
46066	DESKTOP-PSOR95V	ConnectivityTestApp.exe	Malicious	File Read Attempt	29-Aug-2022, 13:01:05	29-Aug-2022, 13:01:05

**CLASSIFICATION DETAILS**

**Malicious runner**

Threat name: Unknown  
Threat family: Unknown  
Threat type: Unknown

Automated analysis steps completed by Fortinet Details

**History**

- Process ...ctivityTestApp.exe with PID 7660 was terminated at device DESKTOP-PSOR95V 2 times
- Device DESKTOP-PSOR95V was tagged as untrusted on FortiClient EMS FortiClient EMS CL... 9 times
- Process ...ctivityTestApp.exe with PID 1180 was terminated at device DESKTOP-PSOR95V 2 times

**Triggered Rules**

- [Chris] Exfiltration Prevention
  - Invalid Checksum - Connection Attempt from Application with In...
  - Malicious File Detected
  - Suspicious Packer - Activity by an Application packed by a Sus...
  - Writable Code - Identified an Executable with Writable Code

## 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.

## 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 a FortiEDR Core as a Jumpbox on page 57](#). You may refer to [Cores on page 127](#) 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.

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:

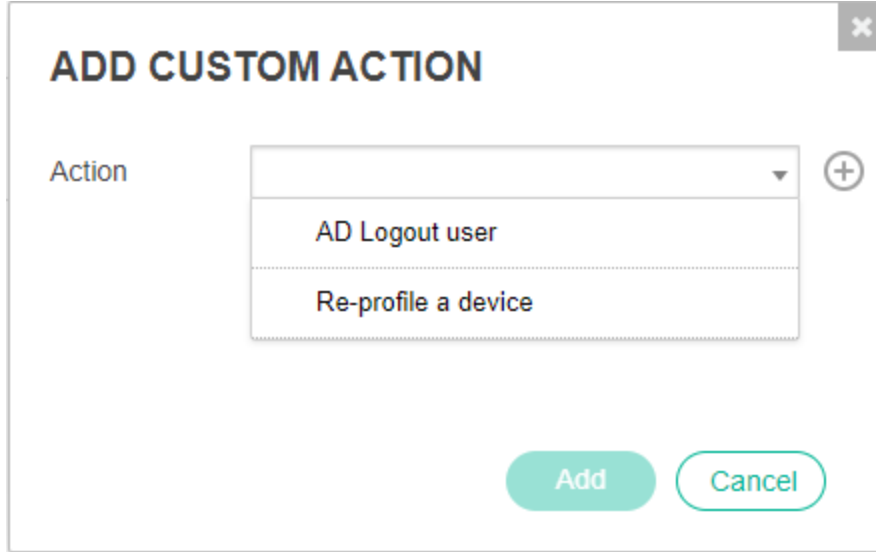
1. Click the *Add Connector* button and select *User Access* from the dropdown list.  
The following displays:

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.
Type	Select the type of user access to be used in the dropdown list. For example, <i>Active Directory</i> .
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 <i>API Key</i> radio button and copy the token value into the text box. To use API credentials, click the <i>Credentials</i> 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

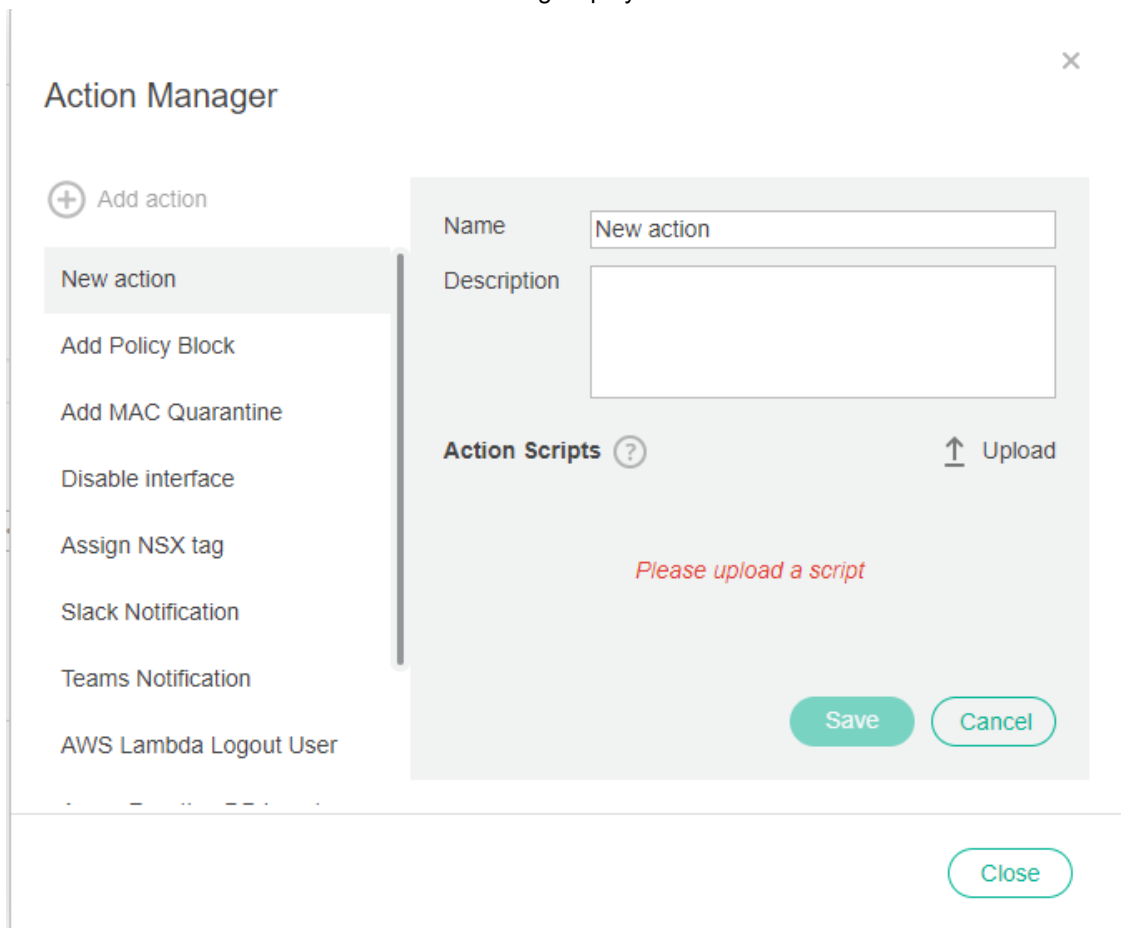
AD Logout user

Re-profile a device

Add Cancel

- ii. In the *Action* dropdown menu, select one of the previously defined actions (which were defined in FortiEDR as described in [User Access integration on page 354](#)), 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:




The screenshot shows the 'Action Manager' window. On the left is a sidebar with a list of actions: 'New action' (highlighted), 'Add Policy Block', 'Add MAC Quarantine', 'Disable interface', 'Assign NSX tag', 'Slack Notification', 'Teams Notification', and 'AWS Lambda Logout User'. The main area contains a form for creating a new action. The 'Name' field is filled with 'New action'. The 'Description' field is empty. Below these fields is a section for 'Action Scripts' with a help icon and an 'Upload' button. A red message 'Please upload a script' is displayed. At the bottom right of the form are 'Save' and 'Cancel' buttons. A 'Close' button is located at the bottom right of the entire window.

- 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.

Field	Definition
Upload	<p>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 <i>Action Scripts</i> 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.</p> <div> <p><b>Creating A Custom Incident Response Action</b></p> <p>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.</p> <p><b>Code Conventions</b></p> <ul style="list-style-type: none"> <li>A FortiEDR JumpBox on which one or more scripts are executed is deployed with various standard Python packages. <a href="#">Click here</a> to see a list of the packages that are deployed with this type of FortiEDR JumpBox.</li> <li>At the moment, only Python 2 is supported.</li> <li>Parameters <ul style="list-style-type: none"> <li>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).</li> <li>These properties are stored in the config.json file and can be used as script parameters.</li> <li><a href="#">Click here</a> to see a sample config.json file and a sample action script.</li> </ul> </li> </ul> <p><a href="#">↓ custom_script.py</a>   <a href="#">↓ config.json</a></p> <p><b>Troubleshooting</b></p> <p>Script execution (either in test mode or as part of a realtime incident response) is defined as</p> <p><a href="#">Close</a></p> </div>

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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Isolate device with NAC	A NAC connector must be defined under <a href="#">Admin settings</a>				
	Move device to the High Security Group	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Disable user	FEDR-QA AD	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## 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 **CLASSIFICATION DETAILS** area of the **Events** page of the FortiEDR Console, as shown below:

The screenshot displays the FortiEDR Console interface. The top navigation bar includes sections like DASHBOARD, EVENT VIEWER, FORENSICS, COMMUNICATION CONTROL, SECURITY SETTINGS, INVENTORY, and ADMINISTRATION. The main content area is divided into two panels. The left panel, titled 'EVENTS', shows a table of security events with columns for ID, DEVICE, PROCESS, CLASSIFICATION, DESTINATIONS, RECEIVED, and LAST UPDATED. The right panel, titled 'CLASSIFICATION DETAILS', provides a detailed view of a selected event, including threat information, history, and triggered rules.

ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
DESKTOP-52GG7K5 (11 events)			Malicious		20-Sep-2022, 17:00:00	21-Sep-2022, 22:00:00
DESKTOP-6AV6KU (5 events)			Malicious		14-Sep-2022, 19:15:36	23-Sep-2022, 15:58:49
DESKTOP-KJEL7HF (6 events)			Malicious		11-Sep-2022, 00:00:00	18-Sep-2022, 00:00:00
DESKTOP-RR8J3DG (3 events)			Malicious		11-Sep-2022, 00:00:00	18-Sep-2022, 00:00:00
DESKTOP-PSOR95V (6 events)			Malicious		07-Sep-2022, 11:38:36	23-Sep-2022, 07:14:33
50347	DESKTOP-PSOR95V	firefox.exe	Inconclusive	Service Access	30-Aug-2022, 15:30:57	30-Aug-2022, 15:30:57
68625	DESKTOP-PSOR95V	ConnectivityTestApp.exe	Malicious	8.8.8.8	07-Sep-2022, 11:38:36	14-Sep-2022, 12:08:01
51153	DESKTOP-PSOR95V	ConnectivityTestApp.exe	Malicious	File Read Attempt	31-Aug-2022, 15:22:33	23-Sep-2022, 07:14:33
46108	DESKTOP-PSOR95V	ConnectivityTestApp.exe	Malicious	8.8.8.8	29-Aug-2022, 13:05:44	31-Aug-2022, 15:42:12
46091	DESKTOP-PSOR95V	ConnectivityTestApp.exe	Malicious	2 destinations	29-Aug-2022, 13:05:44	23-Sep-2022, 07:14:33
46066	DESKTOP-PSOR95V	ConnectivityTestApp.exe	Malicious	File Read Attempt	29-Aug-2022, 13:01:05	29-Aug-2022, 13:01:05

**CLASSIFICATION DETAILS**

**Malicious runner**

Threat name: Unknown  
Threat family: Unknown  
Threat type: Unknown

Automated analysis steps completed by Fortinet Details

**History**

- Process ...ctivityTestApp.exe with PID 4964 was terminated at device DESKTOP-PSOR95V 2 times
- A request to reset the password of user FEDR-QA/QA Admin was sent to Active Directory FEDR-QA AD once
- Malicious, by FortinetCloudServices, on 14-Sep-2022, 12:28:40

**Triggered Rules**

- [Chris] Exfiltration Prevention
  - Invalid Checksum - Connection Attempt from Application with In...
  - Malicious File Detected
  - Suspicious Packer - Activity by an Application packed by a Sus...
  - Writable Code - Identified an Executable with Writable Code

## 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 is archived. 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.

Before you start sandbox configuration, make sure that:

- Your FortiEDR deployment includes a JumpBox that has connectivity to the sandbox.  
Details about how to install a FortiEDR Core and configure it as a JumpBox are described in [Setting up a FortiEDR Core as a Jumpbox on page 57](#). You may refer to [Cores on page 127](#) for more information about configuring a JumpBox.
- The FortiEDR Central Manager has connectivity to Fortinet Cloud Services (FCS).
- You have a valid API user with access to the sandbox.

**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:

The screenshot shows the 'CONNECTORS' section in the FortiEDR interface. At the top, there is a '+ Add Connector' button and an 'Action Manager' icon. Below this, the 'Sandbox' connector is selected and expanded. It shows a 'JumpBox' dropdown menu, a 'Details' section with fields for 'Name', 'Type', 'Host', and 'Port' (set to 443), and radio buttons for 'API Key' (selected) and 'Credentials'. A 'Key' text box is also present. On the right, there is an 'Actions' section with a 'Send file for analysis' button and a 'Test' button. At the bottom right, there are 'Save' and 'Delete' buttons. The status 'Enabled' is shown in the top right corner of the connector details.

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: <i>FortiSandbox</i> .
Host	Specify the IP or DNS address of your sandbox.
Port	Specify the port that is used for API communication with your sandbox.
API Key	Specify authentication details of your sandbox. To use an API token, click the <i>API Key</i> radio button and copy the token value into the text box. To use API credentials, click the <i>Credentials</i> radio button and fill in the external NAC system API username and password.

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:

**SECURITY POLICIES**

Showing 1-10/23

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 *Events* page. Events of files that were found to be clean appear under the *Archived Events* filter and events of files that were found to be risky are displayed under the All filter, such as shown below. A sandbox analysis digest is added to the security event's handling comment.

Dashboard
Event Viewer 393
Forensics ▾
Communication Control ▾ 117
Security Settings ▾
Inventory ▾ 2
Administration 3
● Protection ▾ admin ▾

## EVENTS

[Archive](#)
[Mark As... ▾](#)
[Export ▾](#)
[Handle Event](#)
[Delete](#)
[Forensic](#)
[Exception Manager](#)

Search Event ▾ 🔍

< Back	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED	ACTION
 Certificate: Unsigned  <input type="checkbox"/> RAW ID    DEVICE    DESTINATION    FIRST SEEN    LAST SEEN    USERS    COUNT	15680	collector10	rpp.7.8.5.Installer.exe	Inconclusive		06-May-2020, 10:58:57	06-May-2020, 11:45:22	
	Process path: C:\Users\roof\Downloads\rpp.7.8.5.Installer.exe						Raw data items: 2	
	1593099659	collector10		06-May-2020, 10:59:06	06-May-2020, 11:45:22		11	
	1593099631	collector10		06-May-2020, 10:58:57	06-May-2020, 11:45:22		191	

## CLASSIFICATION DETAILS

PUP **punner**  
By [Renswagelabs](#)

Threat name: Unknown  
Threat family: Unknown  
Threat type: Unknown

---

**History**

- PUP by FortinetCloudServices , on 06-May-2020, 12:05:41
- Inconclusive, by Fortinet , on 06 May 2020, 11:45:17

---

**Triggered Rules**

- Execution Prevention
  - Sandbox Analysis - File was sent to the sandbox for analysis

## 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 device type, which collects the logs from other systems, such as firewalls, Active Directory and other security products
- Google Cloud Security Command Center (SCC) and its built-in Event Threat Detection service
- AWS GuardDuty

## Prerequisites

Before you start configuring an eXtended detection source connector, 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 external detection source, such as FortiAnalyzer. Details about how to install a FortiEDR Core and configure it as a JumpBox are provided in [Setting up a FortiEDR Core as a Jumpbox on page 57](#). You may refer to [Cores on page 127](#) for more information about configuring a JumpBox.
- Connectivity from the FortiEDR Central Manager to the Fortinet Cloud Services (FCS).
- Valid permissions to perform API calls on the eXternal detection source:
  - **(FortiAnalyzer)** You have a FortiAnalyzer administrator account with JSON API access enabled. Refer to the [FortiAnalyzer Administration Guide](#) for more information.
  - **(Google Cloud SCC)** The following roles are required per account:
    - Organization Admin (resourceManager.organizationAdmin)
    - Security Center Admin (securityCenter.admin)See Google Documentation for more details about permissions.
  - **(AWS GuardDuty)** An IAM user with *Programmatic* access type and full permissions to access GuardDuty service.

## Configuring Google SCC

### To enable threat logging on Google:

1. To use Google Cloud SCC as an eXtended detection source, licensing of Security Command Center Premium tier that has Event Threat Detection feature is required.
2. Enable [Event Threat Detection](#) per monitored project in the organization. The following Event Threat Detection rules are required:
  - Malware: bad IP
  - Malware: bad domainMake 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.
3. 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.

### To enable API access to Google for fetching threat logs:

1. Set up a service account on Google, as described in [Google Documentation](#).
2. 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).
3. Grant Security Command Center admin permission to the service account (securityCenter.admin) to allow API access.

## Configuring 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&CAActivity.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](#):

- Set Programmatic Access for this user to allow API calls
- Set full permissions to access GuardDuty service
- 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 an extended detection connector with FortiEDR

1. Click the *Add Connector* button and select *eXtended Detection Source* in the *Connectors* dropdown list. The following displays:

The screenshot shows the 'CONNECTORS' section in the FortiEDR console. The 'AddConnector' button is visible. The selected connector is 'eXtended Detection Source', which is currently 'Enabled'. The configuration fields include:
 

- JumpBox:** A dropdown menu with a help icon.
- Details:**
  - Name:** A text input field.
  - Type:** A dropdown menu.
  - Host:** A text input field.
  - Port:** A text input field with '443' pre-filled.
  - API Key / Credentials:** Radio buttons to select 'API Key' (selected) or 'Credentials'.
  - Key:** A text input field.
- Actions:** A section with the text 'Get Security Alerts from eXte...' and a 'Test' button.

 At the bottom right, there are 'Save' and 'Delete' buttons.

2. Fill in the following fields: eXtended Detection Source Enabled: Check this checkbox to enable blocking of malicious IP addresses by FortiAnalyzer.

Field	Definition
JumpBox	Select the FortiEDR JumpBox that will communicate with the external system.
Name	Specify a name of your choice which will be used to identify the external system.
Type	Select the type of external system to be used in the dropdown list.
Host	Specify the IP or DNS address of the external system.
Port	Specify the port that is used for API communication with the external system.
API Key/Credentials	Specify authentication details of your external system. To use an API token, click the <i>API Key</i> radio button and copy the token value into the text box. To use API credentials, click the <i>Credentials</i> radio button and fill in the external system API username/password or Access key ID/Secret access key. To use Service Account key file, upload the JSON file that was created for your Google Service Account.
Actions Parameters	<ul style="list-style-type: none"> <li>• <b>(Google SCC)</b> Specify the unique organization resource identifier in Google cloud or ID of Google cloud project to use for fetching alerts.</li> </ul>

Actions  
Get Security Alerts from  
eXtended Detection  
Source

Organization ID  ? Project ID  ? Test

Field	Definition
	<ul style="list-style-type: none"> <li><b>(AWS GuardDuty)</b> Specify AWS region for API calls.</li> </ul> <div> <div>Actions</div> <div>Get Security Alerts from eXtended Detection Source</div> <div>Region <input type="text"/></div> <div>?</div> <div>Test</div> </div>

3. Click **Save**.

## Setting up FortiEDR Central Manager

In order to complete eXtended detection source integration, 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				
<div> <div>Clone Policy</div> <div>Set Mode</div> <div>Assign Collector Group</div> <div>Delete</div> </div> <div>Showing 1-10/40</div> <div>Search</div>				
<input type="checkbox"/> All	POLICY NAME	RULE NAME	ACTION	STATE
<input type="checkbox"/>	Execution Prevention	Fortinet	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	Exfiltration Prevention	Fortinet	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	Ransomware Prevention	Fortinet	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	Device Control	Fortinet	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	eXtended Detection	Fortinet	<input type="checkbox"/>	
		Suspicious activity Detected	<input type="radio"/> Block	<input checked="" type="radio"/> Enabled
		Suspicious authentication activity Detected	<input type="radio"/> Block	<input checked="" type="radio"/> Enabled
		Suspicious email activity Detected	<input type="radio"/> Block	<input checked="" type="radio"/> Enabled
		Suspicious network activity Detected	<input type="radio"/> Block	<input checked="" type="radio"/> 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

<b>Inventory</b> <span>Enabled</span> <input checked="" type="checkbox"/> File Detected
<b>Process</b> <span>Enabled</span> <input type="checkbox"/> Screen Capture <input type="checkbox"/> Process Termination <input checked="" type="checkbox"/> Process Creation <input type="checkbox"/> Process Start <input type="checkbox"/> Thread Created <input type="checkbox"/> Executable Loaded <input type="checkbox"/> Driver Loaded <input type="checkbox"/> Library Loaded <input type="checkbox"/> Keystroke Consumption
<b>File</b> <span>Disabled</span>
<b>Network</b> <span>Enabled</span> <input type="checkbox"/> HTTP Request <input type="checkbox"/> Socket Network Statistics <input checked="" type="checkbox"/> Socket Connect <input type="checkbox"/> DNS Query <input type="checkbox"/> Socket Listen <input type="checkbox"/> Socket Close <input type="checkbox"/> Socket Accept

FortiEDR is now configured to issue eXtended detection alerts.

## 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 users and have the *Custom script* option enabled. For more information about user roles and permissions, see [Users on page 285](#).

### 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**  
Configure a new connector

[Add Connector](#) [Action Manager](#)

▼ Custom Connector Disabled

JumpBox

Details

Name  Host  Port

☒ API Key ☐ Credentials

Key

Actions  
[+ Add action](#)

[Save](#) [Delete](#)

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 FortiAnalyzer. 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 <i>API Key</i> radio button and copy the token value into the text box. To use API credentials, click the <i>Credentials</i> 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:

- In the *Action* dropdown menu, select one of the previously defined actions (which were defined in FortiEDR as described [Custom integration on page 365](#)).
- OR-
- 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

+ Add action

New action

Add Policy Block

Add MAC Quarantine

Disable interface

Assign NSX tag

Slack Notification

Teams Notification

AWS Lambda Logout User

Name

New action

Description

Action Scripts ?

Please upload a script

Save

Cancel

Upload


Close

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.

Field	Definition
Upload	<p>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 <i>Action Scripts</i> 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.</p> <div data-bbox="649 525 1429 1144"> <p>Creating A Custom Incident Response Action <span>×</span></p> <p>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.</p> <p><b>Code Conventions</b></p> <ul style="list-style-type: none"> <li>• A FortiEDR JumpBox on which one or more scripts are executed is deployed with various standard Python packages. <a href="#">Click here</a> to see a list of the packages that are deployed with this type of FortiEDR JumpBox.</li> <li>• At the moment, only Python 2 is supported.</li> <li>• Parameters <ul style="list-style-type: none"> <li>◦ 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).</li> <li>◦ These properties are stored in the config.json file and can be used as script parameters.</li> <li>◦ <a href="#">Click here</a> to see a sample config.json file and a sample action script:</li> </ul> </li> </ul> <p><a href="#">↓ custom_script.py</a>   <a href="#">↓ config.json</a></p> <p><b>Troubleshooting</b></p> <p>Script execution (either in test mode or as part of a realtime incident response) is defined as</p> <p><a href="#">Close</a></p> </div>

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 337](#) connector or [Network Access Control \(NAC\) integration on page 345](#) 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		✓	✓	✓	✓	□
	AWS Lambda Logout User	Select All	✓	✓	✓	□	□
	Disable interface	✓ fortinac.fortidemo.com	✓	□	□	□	□
	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 *CLASSIFICATION DETAILS* area of the *Events* page of the FortiEDR Console.

EVENTS

Showing 103-104/104

Search Event

Archive

Mark As...

Export

Handle Event

Delete

Forensics

Exception Manager

ALL	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
□	DynamicCodeTests_1.exe (1 event)			Suspicious		30-Jun-2021, 10:36:28	
□	96879	Win10-64BIT-120-180	DynamicCodeTests_1.exe	Suspicious	2 destinations	30-Jun-2021, 10:36:28	30-Jun-2021, 10:36:28
▶	<div> <div>Logged-in User</div> <div>Process owner: WIN10-64BIT-120\user1</div> <div>Certificate: Signed</div> <div>Process path: C:\Users\user1\Desktop\tudo boomboom_folder\DynamicCodeTests_1.exe</div> <div>Raw data items: 2</div> </div>						
□	DynamicCodeTests_20.exe (1 event)			Suspicious		30-Jun-2021, 10:36:28	

CLASSIFICATION DETAILS

Suspicious **malware**

Threat name: Unknown

Threat family: Unknown

Threat type: Unknown

Automated analysis steps completed by Fortinet Details

History

Suspicious, by FortinetCloudServices, on 30-Jun-2021, 10:36:50

loop was executed on Connector Custom 7 using Jumpbox

domain 2 times

Triggered Rules

Exfiltration Prevention

Dynamic Code - Malicious Runtime Generated Code Detected

Unmapped Executable - Executable File Without a Correspon...

Writable Code - Identified an Executable with Writable Code

## 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 285.

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 *INTEGRATIONS*.
2. Click the *Action Manager* button. The following displays:

**Action Manager**

+ Add action

New action

Add Policy Block

Add MAC Quarantine

Disable interface

Assign NSX tag

Slack Notification

Teams Notification

AWS Lambda Logout User

Name: New action

Description:

Action Scripts ?

Upload

Please upload a script

Save Cancel

Close

**To define a new action:**

1. Click the + *Add action* button in the top left corner of the window.
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	<p>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 <i>Action Scripts</i> 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.</p> <div> <p><b>Creating A Custom Incident Response Action</b></p> <p>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.</p> <p><b>Code Conventions</b></p> <ul style="list-style-type: none"> <li>A FortiEDR JumpBox on which one or more scripts are executed is deployed with various standard Python packages. Click <a href="#">here</a> to see a list of the packages that are deployed with this type of FortiEDR JumpBox.</li> <li>At the moment, only Python 2 is supported.</li> <li>Parameters <ul style="list-style-type: none"> <li>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).</li> <li>These properties are stored in the config.json file and can be used as script parameters.</li> <li>Click <a href="#">here</a> to see a sample config.json file and a sample action script:</li> </ul> </li> </ul> <p><a href="#">↓ custom_script.py</a>   <a href="#">↓ config.json</a></p> <p><b>Troubleshooting</b></p> <p>Script execution (either in test mode or as part of a realtime incident response) is defined as</p> <p><a href="#">Close</a></p> </div>

3. Click **Save**.

### To modify the script of an action:

1. In the **ADMINISTRATION** tab, select **INTEGRATIONS**.
2. Click the **Action Manager** button.

3. Select the action of the script to be modified. The following displays:

4. In the *Action Scripts* area, hover over the name of the script in order to display various tools, as follows:

Tool	Description
	To overwrite the current script by uploading a different script instead of it.
	To download the action's current script. For example, so that you can edit it.
	To delete the action's selected script.
Upload	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.



To delete an action entirely, hover over its name in the list on the left and click the *Trashcan* icon.

5. Click Save.

# 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 129](#) 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 232](#).

## 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.

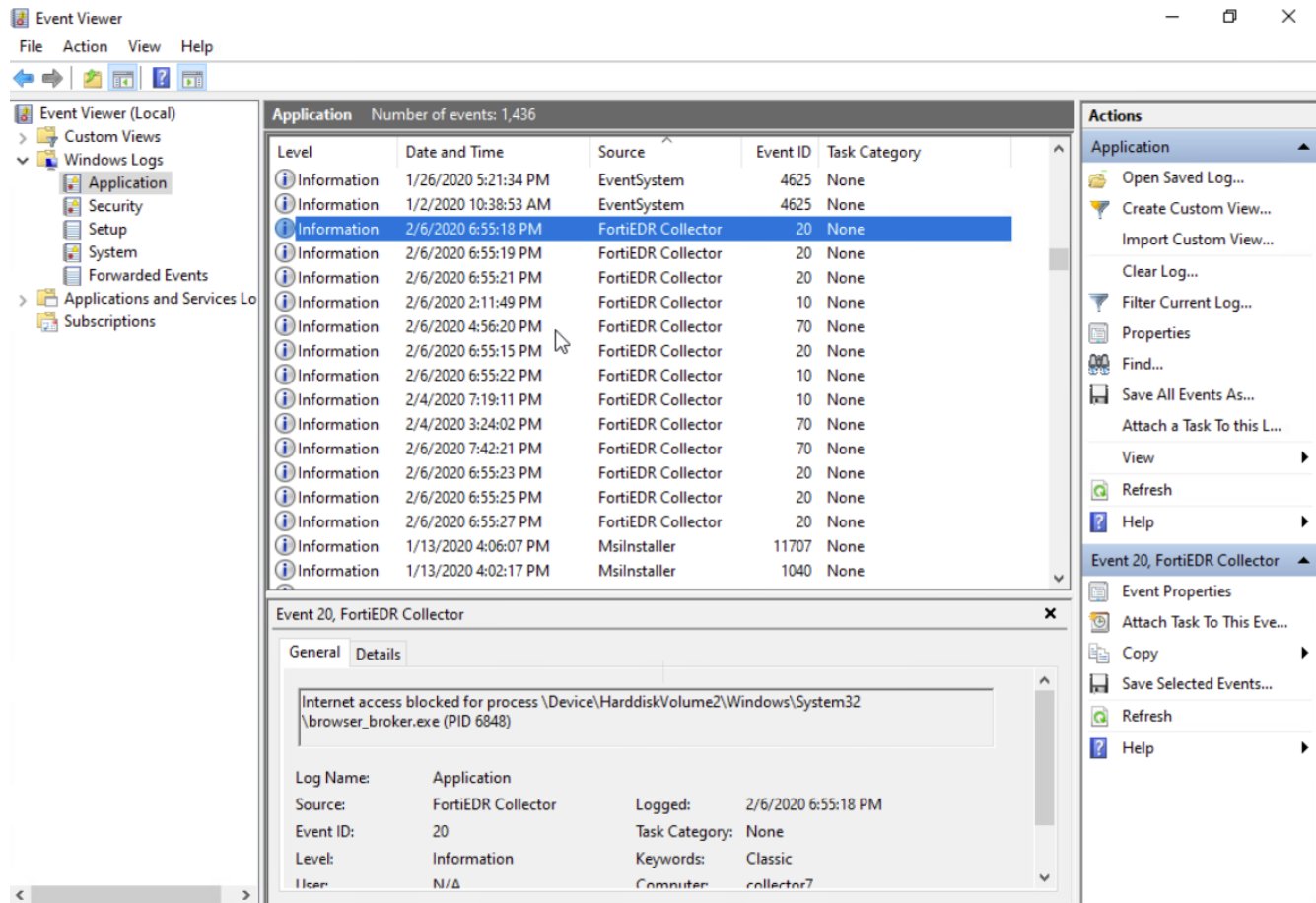


Make sure that Telnet is enabled on Windows.

## 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*.



### 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 fortiEDRColl[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 fortiEDRColl[3654]: Fortinet Endpoint Detection and Response: Connection blocked for process /System/Library/PrivateFrameworks/IMFoundation.framework/XPCServices/IMRemoteURLConnectionAgent.xpc/Contents/MacOS/IMRemoteURLConnectionAgent (pid:3814)
```

## 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.



## 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:

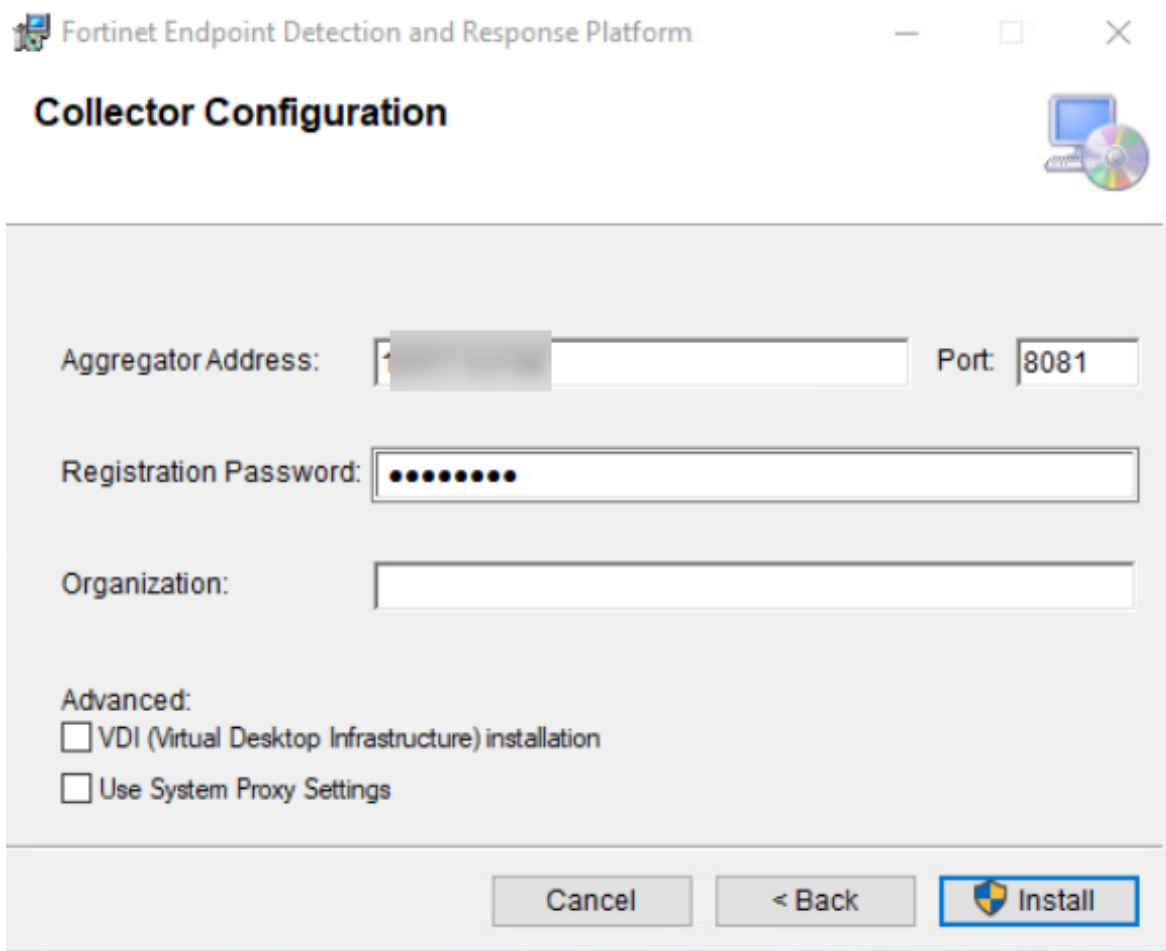
Role	Description
<i>Admin</i>	<p>Highest-level super user that can access all data and perform all operations in the FortiEDR Central Manager console for one specific organization or all organizations, as defined in the user settings.</p> <p>In a FortiEDR multi-organization system, the system comes with one predefined Administrator user. More than one user with the Admin role is permitted.</p>
	 <p>There must always be at least one Administrator in the system. Prior to 3.0, the FortiEDR system only supported a single tenant (organization).</p>

Role	Description
<i>Senior Analyst</i>	<p>Analysts supervisor who can define security policies in addition to all the actions that can be performed by an Analyst.</p> <p>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 <a href="#">Administration on page 274</a> tab.</p>
<i>Analyst</i>	<p>SOC/MDR service analyst who can perform actions as required in the day-to-day activities of handling events.</p> <p>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 <i>ADMINISTRATION</i> tab or define/change policies.</p>
<i>IT</i>	<p>IT staff who can define settings related to the FortiEDR integration with the customer ecosystem.</p> <p>This role has system configuration access only. They can deploy and upgrade system components and perform system integration with external systems using the <i>ADMINISTRATION</i> tab but do not have access to any security configuration, alert monitoring, or Forensics options.</p>
<i>Read-Only</i>	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:



The screenshot shows the 'Collector Configuration' window of the Fortinet Endpoint Detection and Response Platform. The window has a title bar with the Fortinet logo and the text 'Fortinet Endpoint Detection and Response Platform'. Below the title bar, the title 'Collector Configuration' is displayed in a large, bold font. To the right of the title is a small icon of a computer monitor and a CD. The main area of the window contains several input fields and checkboxes. The 'Aggregator Address' field is followed by a 'Port' field containing the value '8081'. Below these is a 'Registration Password' field with a masked password of ten dots. Underneath is an 'Organization' field. At the bottom left, under the heading 'Advanced:', there are two checkboxes: 'VDI (Virtual Desktop Infrastructure) installation' and 'Use System Proxy Settings'. At the bottom right, there are three buttons: 'Cancel', '< Back', and 'Install' (which is highlighted with a blue border and a shield icon).

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 21](#).

## Core registration

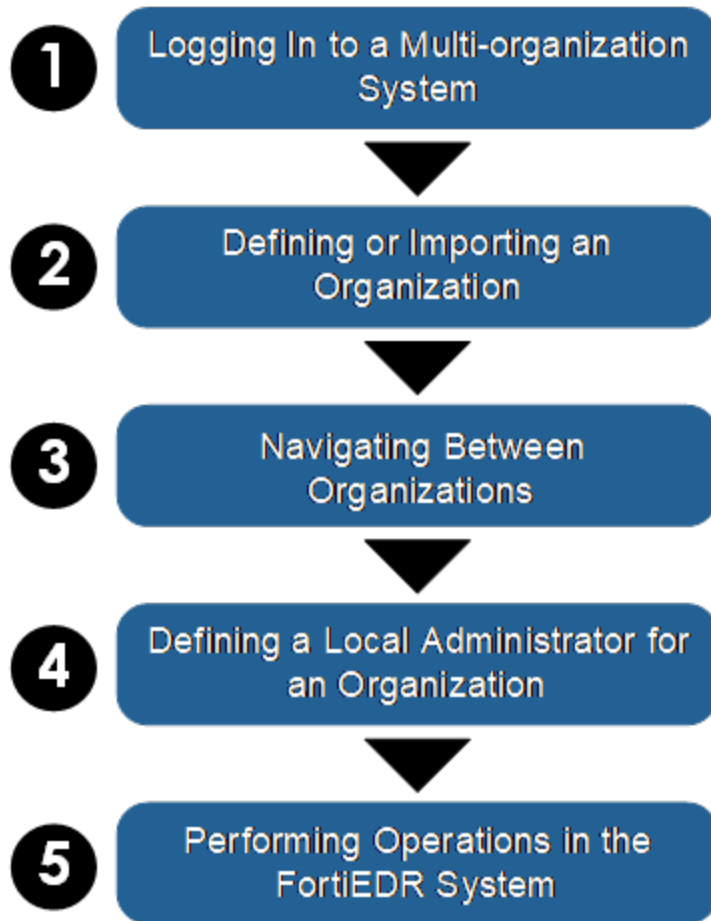
Most Cores are shared between organizations. It is possible to install a Core that belongs only to your organization by installing it on-premises. In this case, you must specify the organization during the Core installation process.

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 a FortiEDR Core as a Jumpbox on page 57](#).

## Workflow

The following general workflow applies for Administrators when working in a FortiEDR multi-organization system:



### Step 1 – Logging in to a multi-organization system

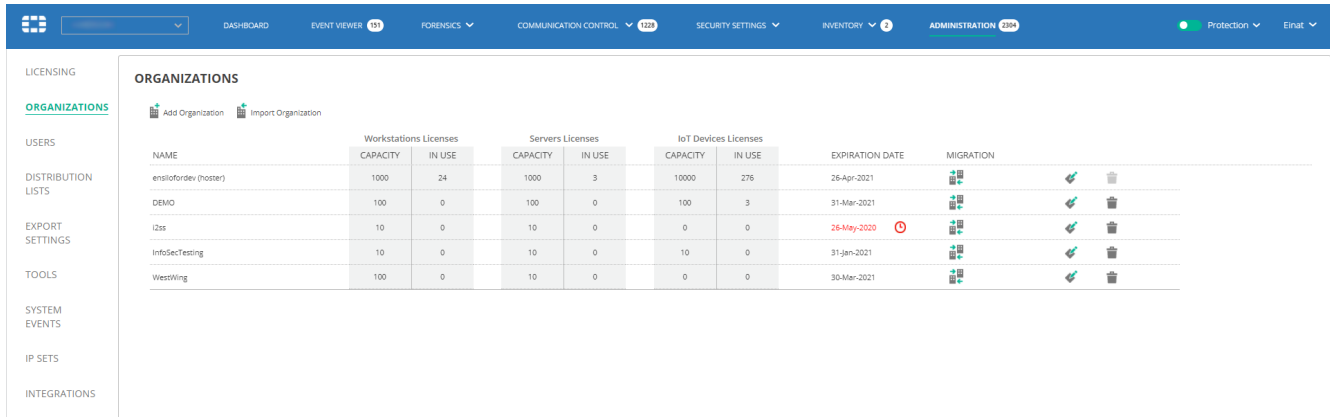
For a FortiEDR multi-organization system, a user must also specify the organization when logging in to the system.

The screenshot shows the Fortinet login page. On the left is the Fortinet logo. On the right, there are three input fields: 'User name', 'Password', and 'Organization name'. Below these fields is a 'LOGIN' button.

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.



NAME	Workstations Licenses		Servers Licenses		IoT Devices Licenses		EXPIRATION DATE	MIGRATION
	CAPACITY	IN USE	CAPACITY	IN USE	CAPACITY	IN USE		
ensiofordev (hoster)	1000	24	1000	3	10000	276	26-Apr-2021	
DEMO	100	0	100	0	100	3	31-Mar-2021	
i2ss	10	0	10	0	0	0	26-May-2020	
InfoSecTesting	10	0	10	0	10	0	31-Jan-2021	
Westring	100	0	10	0	0	0	30-Mar-2021	

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 385 in FortiEDR](#).

The *Organizations* window contains the following information:

Field	Definition
Name	Specifies the name of the organization.
Workstation Licenses Capacity	For the organization, specifies the number of workstation licenses allocated to the organization.
Workstation Licenses in Use	Specifies the number of workstation licenses in use (installed).
Servers Licenses Capacity	For the organization, specifies the number of servers allocated to the organization.
Servers Licenses in Use	Specifies the number of 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.

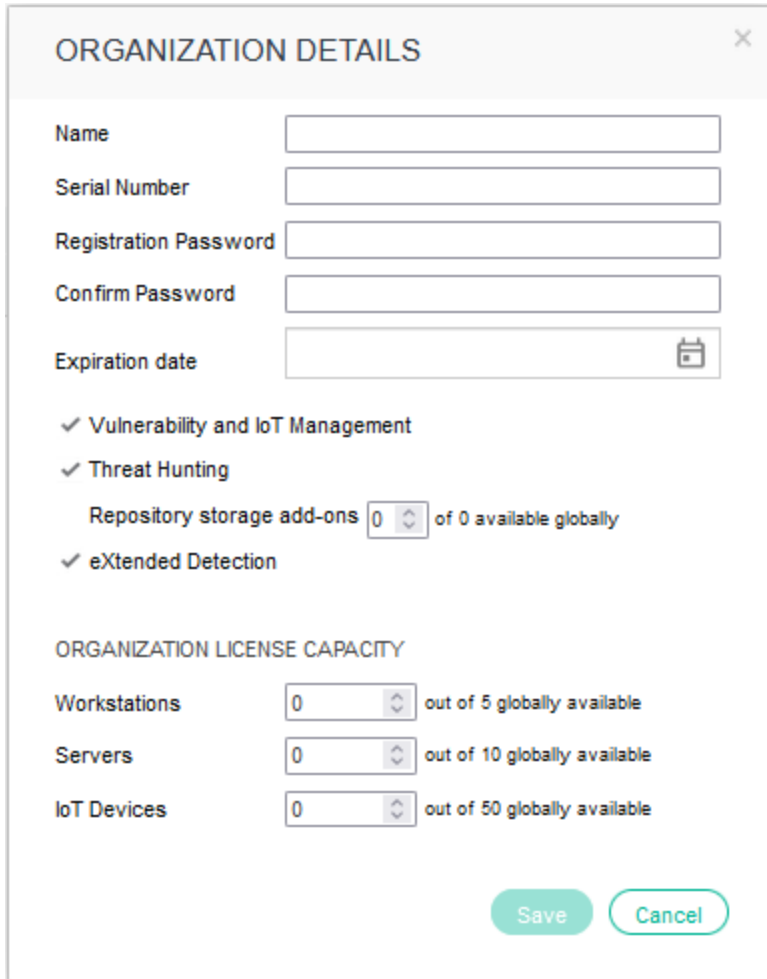
Click the *Edit* button in an organization row to edit the properties of that organization.

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 387](#).





### 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:



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 organization name: 0123456789:=-@ABCDEFGHIJKLMNOPQRSTUVWXYZ_abcdefghijklmnopqrstuvwxyz. Spaces are also allowed. For example, you can

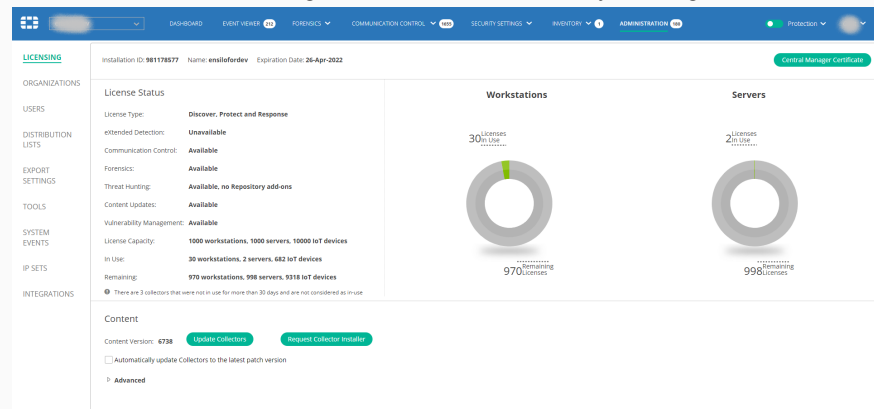
Field	Definition
	specify the organization name of a hotel branch as ABC_Hotel@Los Angeles.
Serial Number	Your FortiEDR unique identifier with Fortinet, which can be found at the top of the <a href="#">Administration &gt; Licensing</a> tab.
Registration Password	<p>Specifies the registration password for the organization. Each organization can have a different registration password. You set the value for this password.</p> <p>Supported special characters in the password: !, #, %, &amp;, ', +, -, ., /, :, &lt;, =, &gt;, ?, @, [, \, ], ^, _ ` , {,  , }, ~, and ,</p> <hr/> <div>  <p>You can display the registration password for an organization by selecting <b>ADMINISTRATION &gt; TOOLS &gt; COMPONENT AUTHENTICATION &gt; DISPLAY</b>.</p> </div> <hr/> <div>  <p>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 <b>Access Denied</b> 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 <a href="#">Component authentication on page 319</a>.</p> </div>
Expiration Date	<p>Specifies when this license expires. Notifications are sent to you beforehand. Each organization can have its own expiration date.</p> <hr/> <div>  <p>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.</p> </div>
Vulnerability and IoT Management	<p>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.</p> <hr/> <div>  <p>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.</p> </div>

Field	Definition
Threat Hunting	Check this checkbox to provide the organization access to threat hunting. This option is only available on setups that have purchased a <i>Discover, Protect and Response</i> or <i>Protect and Response</i> license. <ul style="list-style-type: none"> <li><i>Repository storage add-ons</i>: Specifies the number of repository add ons, out of the total number of add on purchases, to enable this organization to use.</li> </ul>
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 <a href="#">Licensing on page 274</a> for details on how to check the license type.
Workstations / Servers / 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.



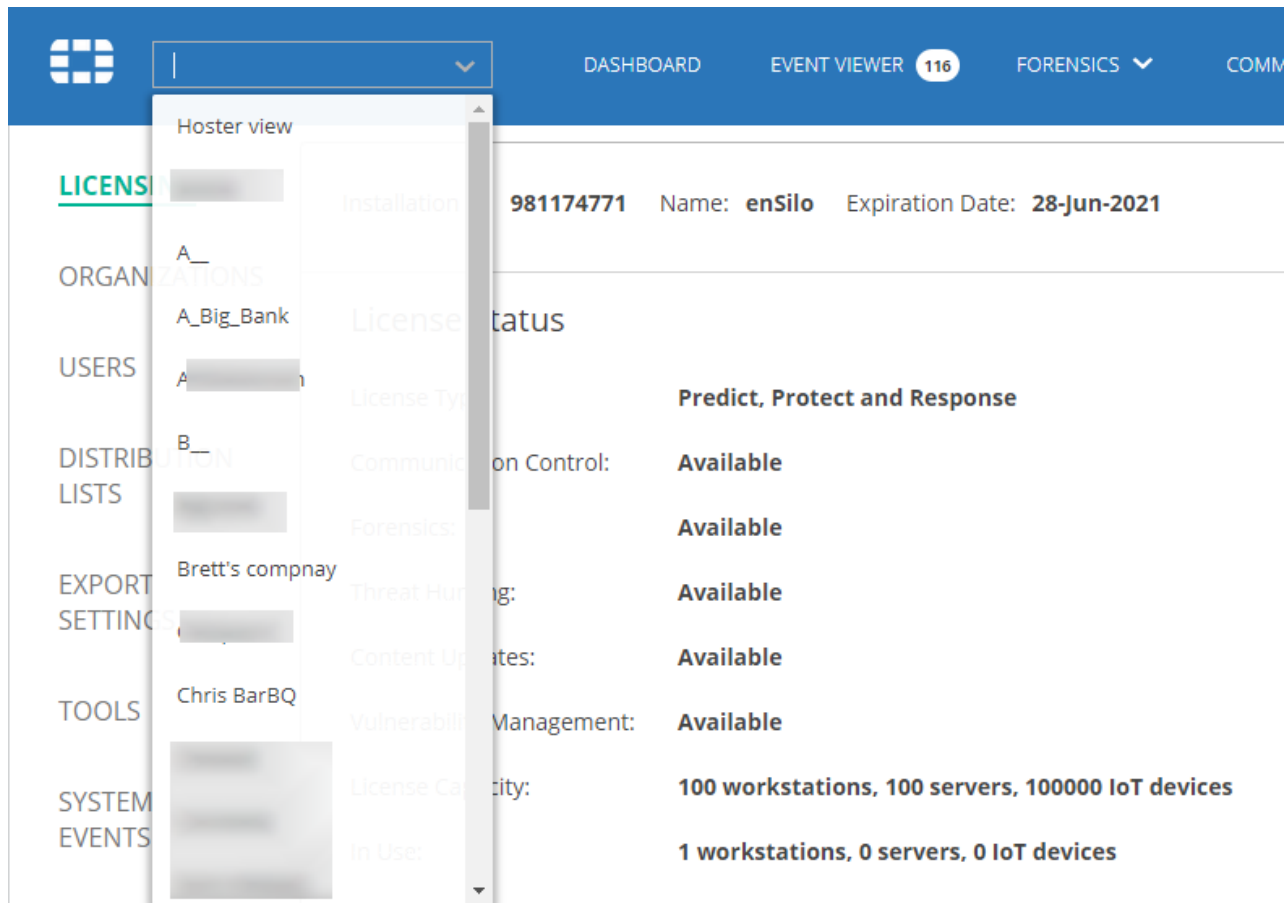
The License Capacity field in the Licenses window shows the total number of license seats for the entire FortiEDR system, which are divided into Workstations, Servers and IoT Devices.

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.

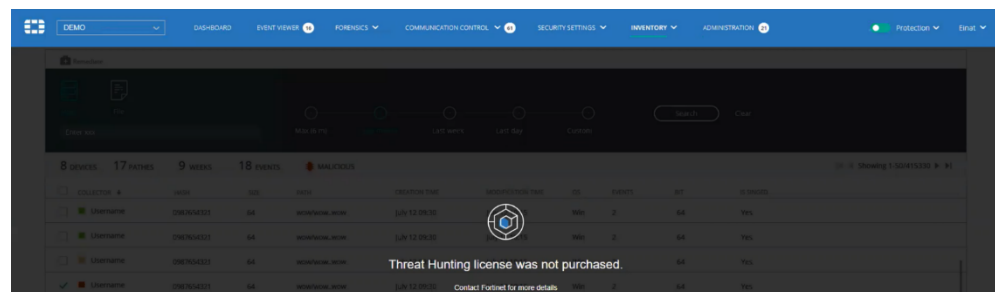


- Click the **Save** button. Note that it may take a minute or so to create the organization. After creating the organization, the organization appears as a new row in the *Organization* dropdown list.





If a user attempts to use a feature that is not available with their license, a warning message displays. For example, as shown below.



## Moving from a single-organization to multi-organization structure in FortiEDR

In a single-organization system, the Default (hoster) organization is the only organization.

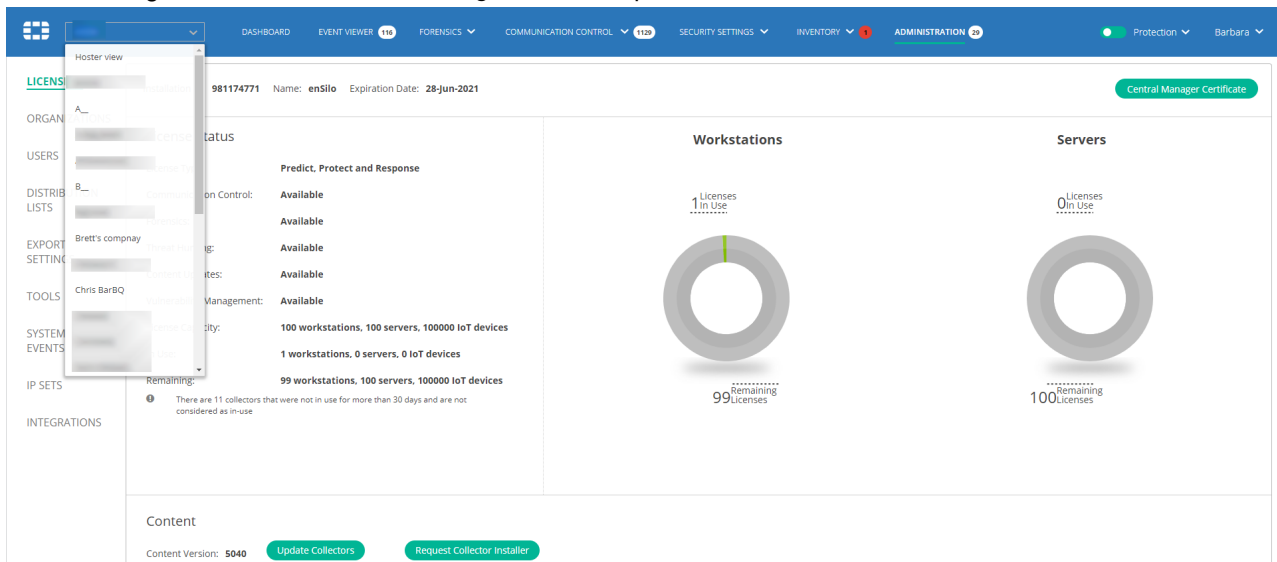
To create a multi-organization (multi-tenant) system, an Administrator simply needs to add one or more organizations to a single-organization system. When there are multiple organizations in the system, you can select the organization of interest in the *Organization* dropdown menu that appears at the 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:

- 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 397](#).
- 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:**

- In Hoster view, click the *ADMINISTRATION* tab and then click *USERS* in the left pane.
- Click the *Add User* button.

3. Select the organization in the *Organization* field, as shown below.

4. Fill in the displayed window, as described in [Users on page 285](#).  
 5. Click Save.

## Step 5 – Performing operations in the FortiEDR system

Administrators can perform all of the operations described from [Security Settings on page 64](#) to [Forensics on page 219](#) 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.

NAME	Workstations Licenses		Servers Licenses		IoT Devices Licenses		EXPIRATION DATE	MIGRATION
	CAPACITY	IN USE	CAPACITY	IN USE	CAPACITY	IN USE		
ensiloforddev (hoster)	1000	24	1000	3	10000	276	26-Apr-2021	[Icons]
DEMO	100	0	100	0	100	3	31-Mar-2021	[Icons]
i2s	10	0	10	0	0	0	26-May-2020	[Icons]
InfoSecTesting	10	0	10	0	10	0	31-Jan-2021	[Icons]
WestWing	100	0	10	0	0	0	30-Mar-2021	[Icons]

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

Export

Abort

Next →

Close

From this window, you perform three steps to migrate the organization to another environment:

- Export the Organization:** This step exports all the data of the selected organization to a zip file.
  - 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.
  - This step moves all the Collectors of the selected organization from the source environment to the destination environment.
- 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.
  - 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



Data for the [redacted] organization was generated successfully


[Download](#)



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

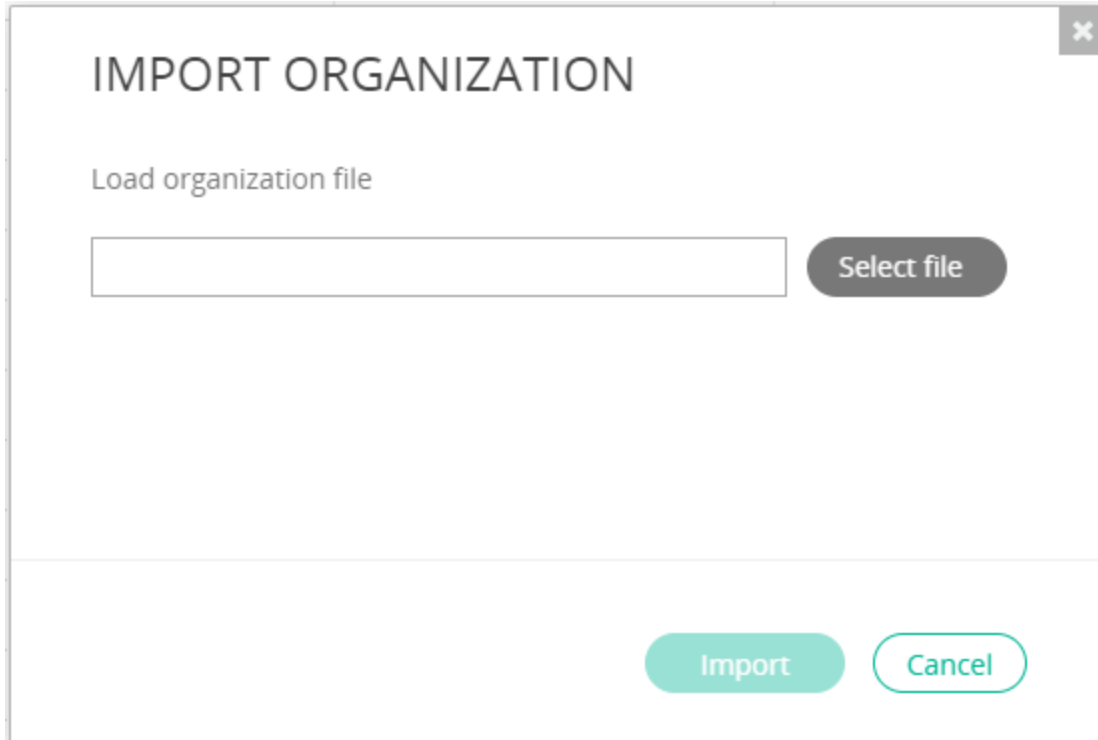
Abort

Next →

Close

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:



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.



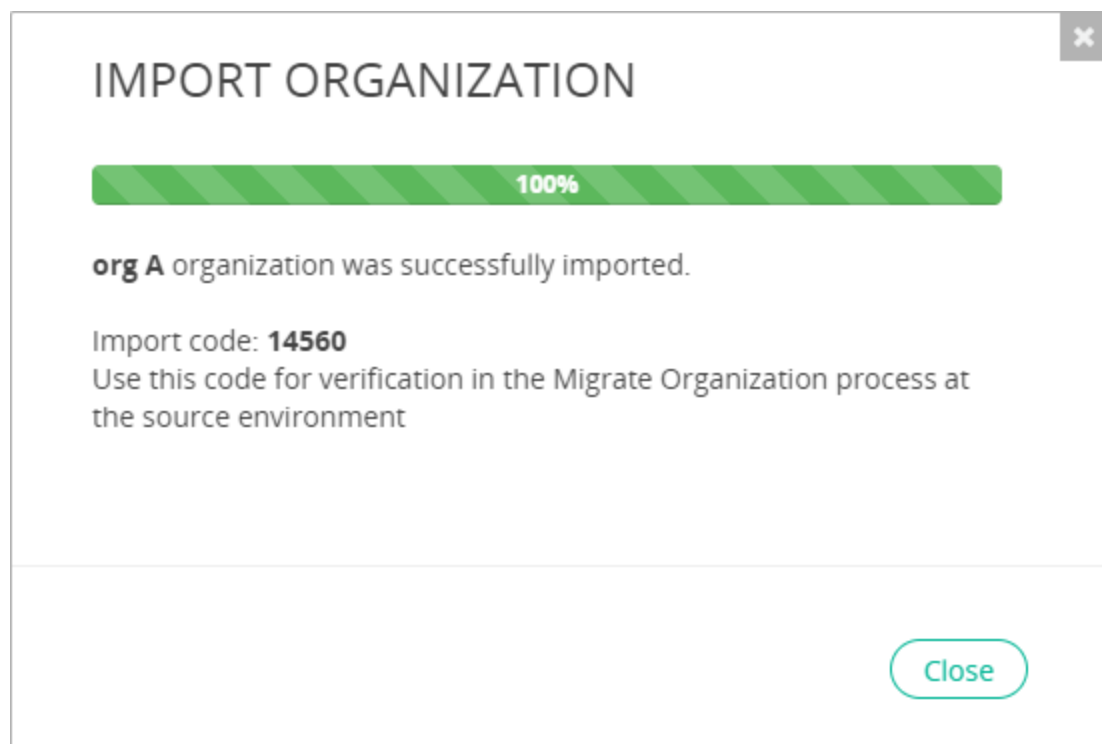
You cannot import an exported organization that has a name that already exists in the destination environment.

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 274](#) 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.





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

Registration Password

Expiration date

📅

Workstations allocated

(6580 available for allocation)

Servers allocated

(6580 available for allocation)

Imported organization (import code - 14560)

Save
Cancel

Note that the name of the organization cannot be changed in this window, and is read-only.

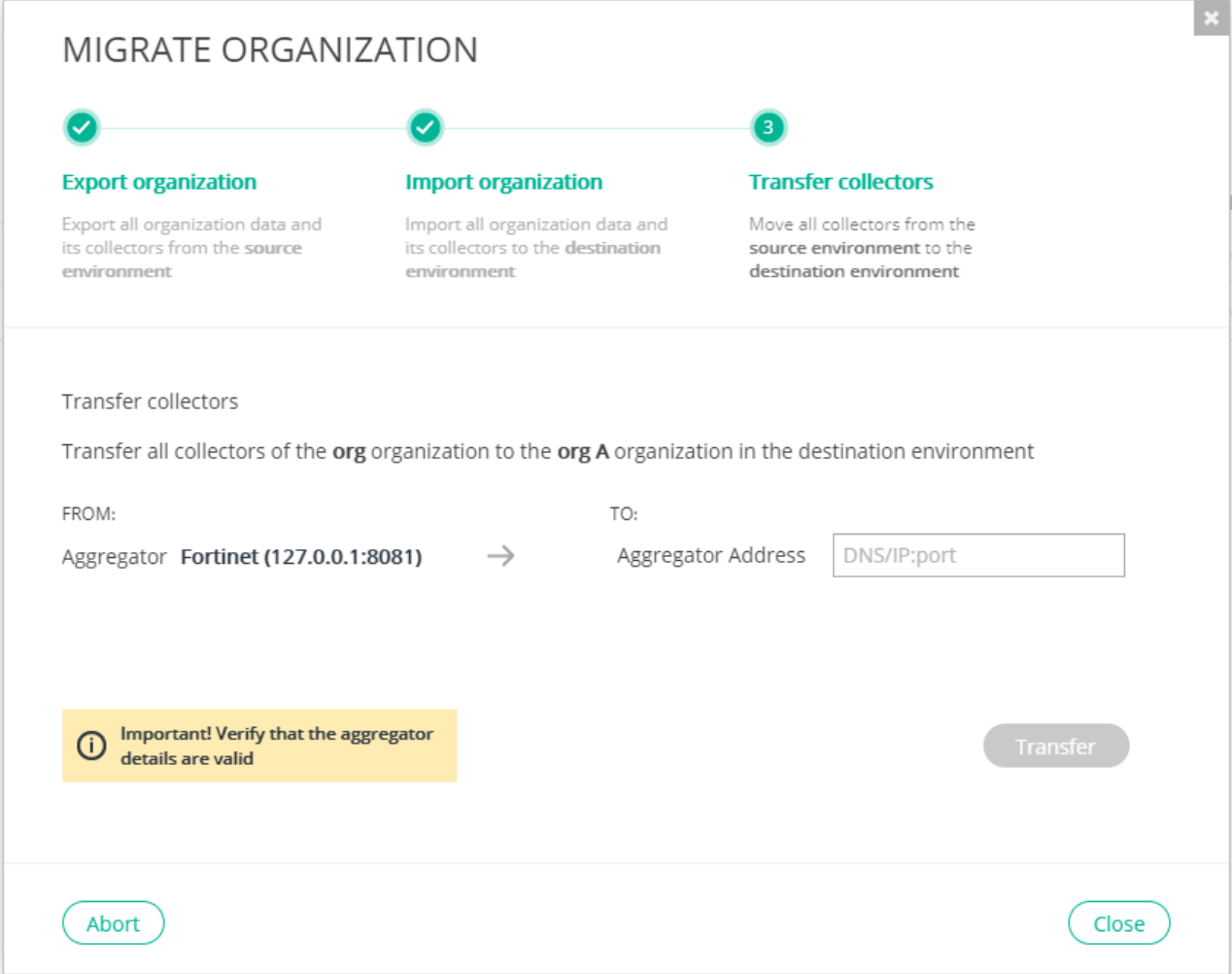
11. In step 2 of the *Migrate Organization* window, enter or copy the import code into the *Import code* field.

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										
Add Organization Import Organization										
NAME	Workstations Licenses		Servers Licenses		IoT Devices Licenses		EXPIRATION DATE	MIGRATION		
	CAPACITY	IN USE	CAPACITY	IN USE	CAPACITY	IN USE				
torgm44 (test)	1000	36	1000	11	10000	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-2023	Cont.		
organization12	50	0	50	0	0	0	01-Jan-2025			

12. Click *Next*. 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**

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

**Important!** Verify that the aggregator details are valid

**Transfer**

**Abort** **Close**

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)								
<div> <div>All</div> <div>Create Group</div> <div>Move to Group</div> <div>Delete</div> <div>Enable/Disable</div> <div>Isolate</div> <div>Export</div> <div>Uninstall</div> </div> <div>Search Collectors or Groups</div> <div>178 Unmanaged devices were found</div>								
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 LTSC	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:

TO:

Aggregator **Fortinet (127.0.0.1:8081)**



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.

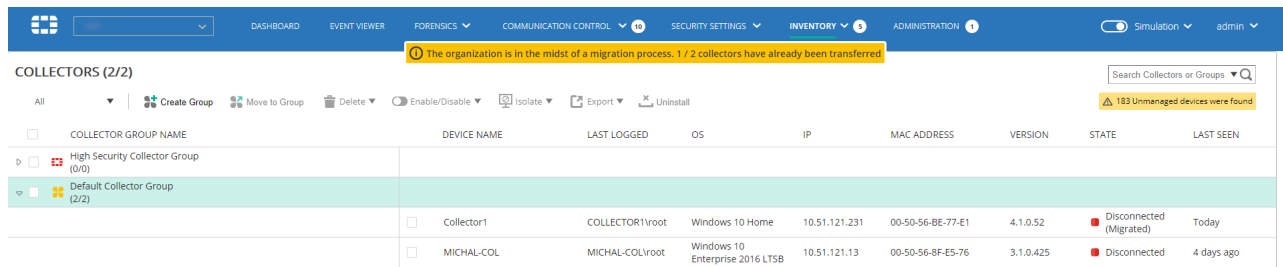
The organization is in the midst of a migration process. 1 / 2 collectors have already been transferred								
ORGANIZATIONS								
dd Organization								
/AE	Workstations Licenses		Servers Licenses		IoT Devices Licenses		EXPIRATION DATE	MIGRATION
	CAPACITY	IN USE	CAPACITY	IN USE	CAPACITY	IN USE		
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.



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 LTSC	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.

OK

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 SMTP-related information under *Administration > Export Settings* in a multi-organization system.

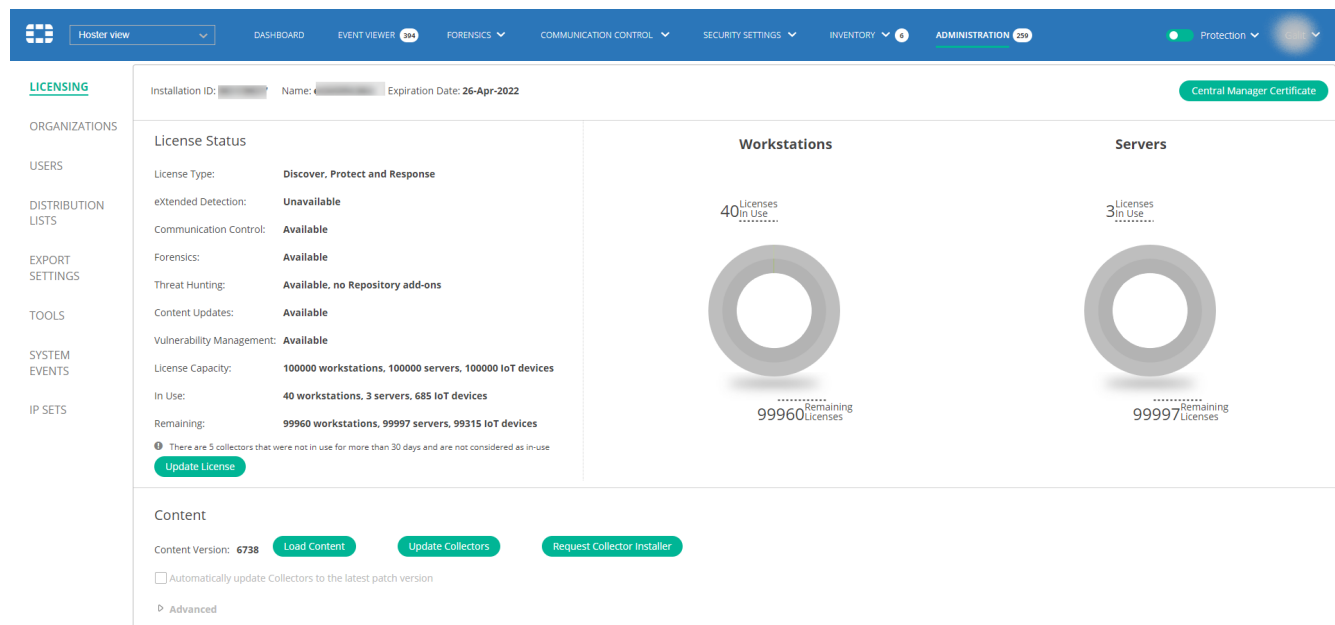
In addition, there are some special cases where you cannot view administration data in Hoster view, and can only view data for a specific organization, such as the following:

- 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.



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.

<input type="checkbox"/>	ORGANIZATION NAME ▲	COLLECTOR GROUP ▲	WINDOWS VERSION	MACOS VERSION	LINUX VERSION
<input type="checkbox"/>	liorgolf444	Default Collector Group	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
<input type="checkbox"/>	liorgolf444	emulation	N/A	N/A	N/A
<input type="checkbox"/>	liorgolf444	group1	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
<input type="checkbox"/>	liorgolf444	group2	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
<input type="checkbox"/>	liorgolf444	High Security Collector Group	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
<input type="checkbox"/>	liorgolf444	Insiders	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
<input type="checkbox"/>	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.

Update Cancel

## Users

In Hoster view, this window includes an *Organization* column.

NAME ▲	ORGANIZATION	TITLE	FIRST NAME	LAST NAME	EMAILADDRESS	ROLE	ADVANCED
demo521	All organizations	Admin	demo	521	demo521@demo.com	Admin	Rest API, FortiEDR Connect, Custom ...
demo521	demo521	Read-Only	demo	521	demo521@demo.com	Read-Only	FortiEDR Connect, Custom script
demo521	All organizations	Admin	demo	521	demo521@demo.com	Admin	FortiEDR Connect, Custom script
demo521	All organizations	Admin	demo	521	demo521@demo.com	Admin	FortiEDR Connect, Custom script
demo521	All organizations	Admin	demo	521	demo521@demo.com	Admin	Rest API, FortiEDR Connect, Custom ...
demo521	All organizations	Admin	demo	521	demo521@demo.com	Admin	Rest API, FortiEDR Connect, Custom ...
demo521	All organizations	Admin	demo	521	demo521@demo.com	Admin	Rest API, FortiEDR Connect, Custom ...
demo521	demo521	Senior Analyst	demo	521	demo521@demo.com	Senior Analyst	FortiEDR Connect, Custom script
demo521	val	Admin	val	val	val@demo.com	Admin	Rest API, FortiEDR Connect, Custom ...
demo521	demo521	Admin	demo	521	demo521@demo.com	Admin	Rest API, FortiEDR Connect, Custom ...

When you click the *Add User* button from this window, the *User Details* window displays. The *User Details* window includes an *Organization* field that you must specify to add the user. You can assign the user to one specific organization or *All organizations*.

USER DETAILS

Organization

All organizations

User Name

✓ All organizations

Title

demo521

First Name

AWS

Last Name

Google

Email Address

lior

Role

moshe\_A  
Admin

Advanced

✓ Rest API

✓ Custom script

✓ Establish FortiEDR Connect sessions

☐ Require two factor authentication for this user

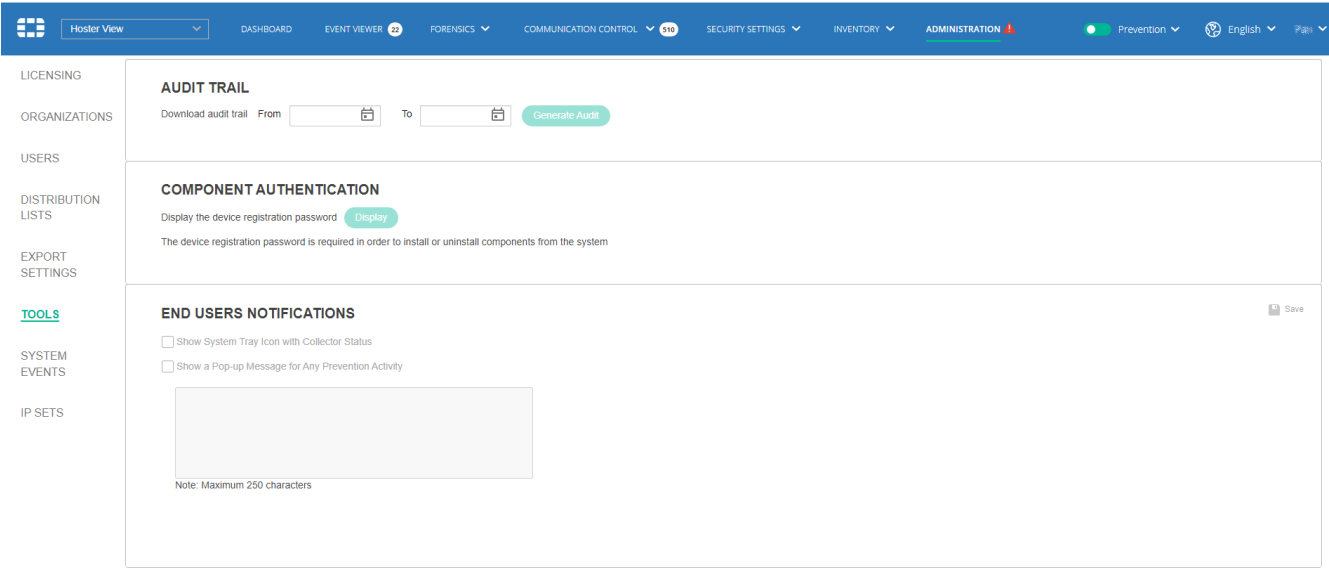
Save

Cancel

## Tools

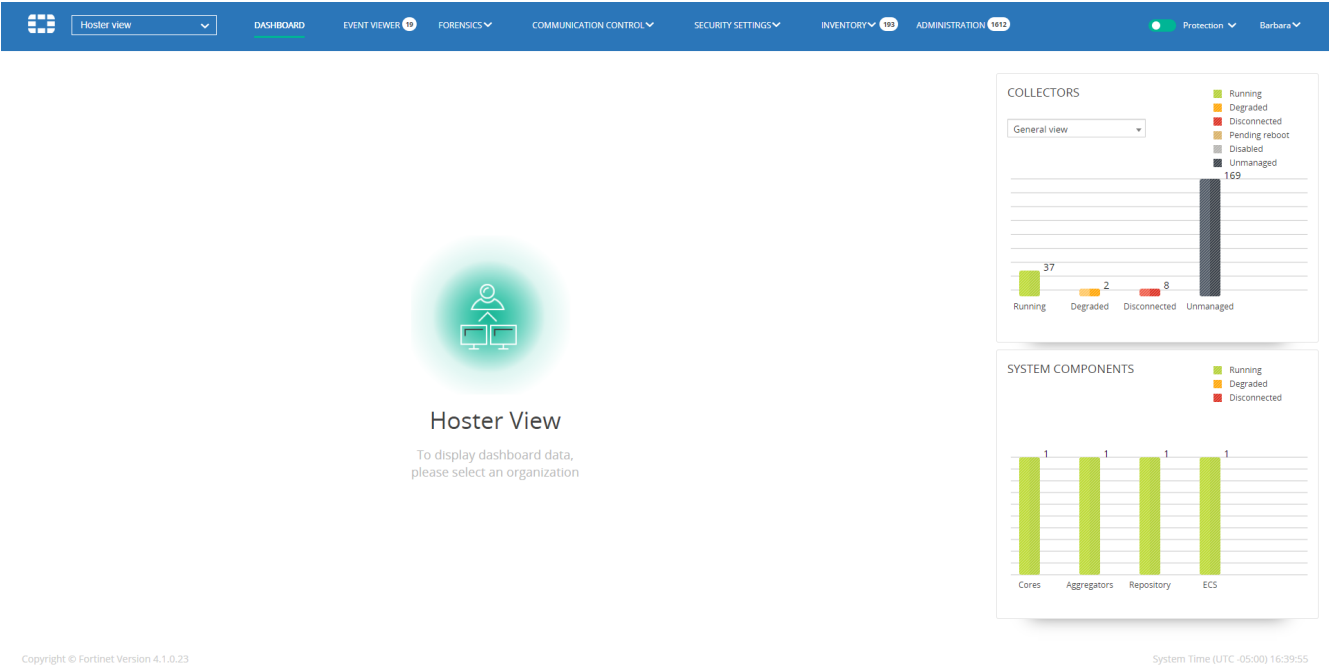
In Hoster view, the following sections are either view-only or unavailable in the *Administration > Tools* page:

- [Component authentication on page 319](#) (view-only)
- [File scan on page 320](#) (unavailable)
- [End-user notifications on page 321](#) (view-only)
- [IoT device discovery on page 324](#) (unavailable)
- [Personal data handling on page 325](#) (unavailable)
- [Windows Security Center on page 330](#) (unavailable)
- [FortiEDR Connect on page 331](#) (unavailable)



## 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.



To view Dashboard information for a specific organization, you must select the organization of interest in the *Organization* dropdown list.



## Event Viewer

In Hoster view, the Event Viewer displays the security events from all organizations. The *Organization* column indicates the organization in which the security event occurred.

The screenshot shows the FortiEDR Event Viewer interface in Hoster view. The main window displays a table of security events. The table has columns for ID, Device, Process, Organization, Classification, Destinations, Received, and Last Updated. The Organization column lists various organizations, including liorgolf444 and organization10. The Classification column shows various event types, such as PUP, Suspicious, Malicious, Inconclusive, and Safe. The Received column shows the date and time of the event. The interface also includes a toolbar with buttons for Archive, Mark As, Export, Handle Event, Delete, Forensics, and Exception Manager. A sidebar on the right shows Classification Details and History. The bottom of the interface displays Copyright © Fortinet Version 4.1.0.23 and System Time (UTC -05:00) 16:41:22.

ID	DEVICE	PROCESS	ORGANIZATION	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
pandasecurityDx.dll (2 events)			liorgolf444	PUP		11-Feb-2020, 21:15:58	
pandasecurityDx64.dll (1 event)			liorgolf444	PUP		11-Feb-2020, 21:14:04	
TeamViewer.exe (1 event)			liorgolf444	PUP		10-Feb-2020, 04:47:59	
DynamicCodeTests32.exe (1 event)			liorgolf444	Suspicious		06-Feb-2020, 02:39:27	
python.exe (1 event)			liorgolf444	Malicious		04-Feb-2020, 07:47:59	
SmartConsole.exe (1 event)			liorgolf444	Likely Safe		03-Feb-2020, 05:25:12	
enSiloCollector (1 event)			liorgolf444	Inconclusive		03-Feb-2020, 04:00:50	
DynamicCode32.exe (1 event)			liorgolf444	Suspicious		02-Feb-2020, 11:18:43	
cscript.exe (4 events)			liorgolf444	Suspicious		02-Feb-2020, 11:16:45	
dumb-init (1 event)			liorgolf444	Inconclusive		01-Feb-2020, 12:07:10	
filebeat.exe (2 events)			liorgolf444	Inconclusive		01-Feb-2020, 11:51:23	
979c6de81cc0f4e0e770f720eb82e8c727a2d422fe... (2 events)			liorgolf444	Malicious		30-Jan-2020, 04:18:06	
B03276BFBF85CFDD7C8998004C1200DA.vlr (2 events)			liorgolf444	Malicious		30-Jan-2020, 04:18:02	
DynamicCodeListenTests.exe (1 event)			liorgolf444	Suspicious		29-Jan-2020, 14:34:48	
setup.exe (1 event)			organization10	Suspicious		19-Dec-2019, 09:17:28	
EvilProcessTests.exe (1 event)			organization10	Likely Safe		19-Dec-2019, 09:15:39	
UnpackingDetectionTests.exe (1 event)			organization10	Safe		19-Dec-2019, 09:15:36	



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 archive security events from different organizations at once using the *Archive* button and you can export security events from different organizations using the *Export* button.

You can also use the *Handle Event* button to handle security events from multiple organizations. In Hoster view, for each security event selected in the *Events* window, the *Event Handling* window shows the organization name and security events selected for that organization (when you select security events in up to three organizations).

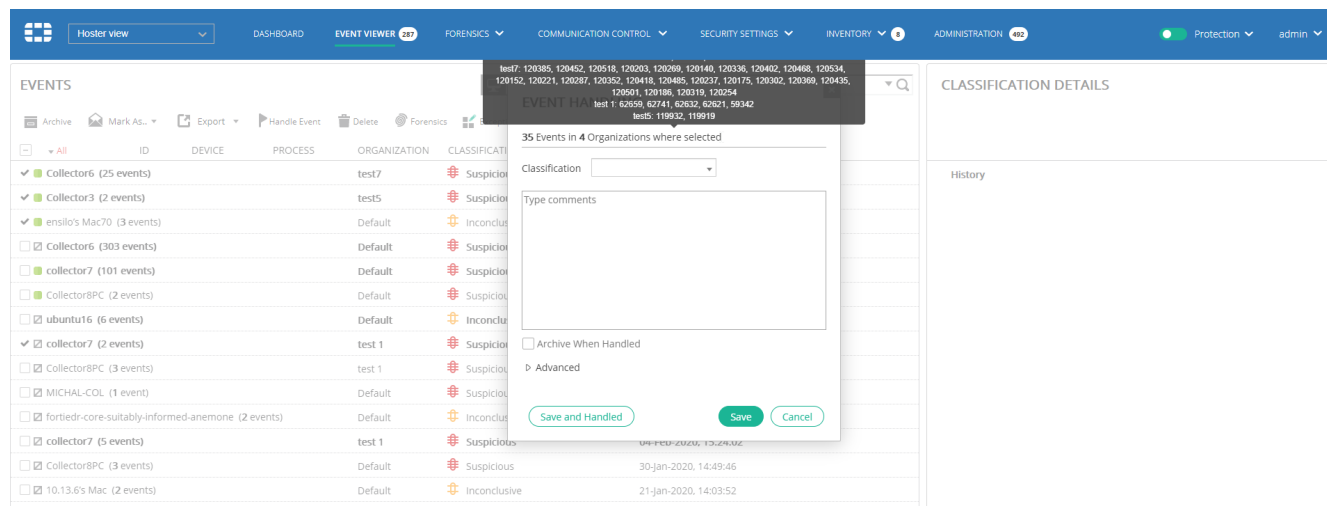
## Multi-tenancy (organizations)

The screenshot shows the FortiEDR 'EVENTS' page. The table lists events with columns for ID, DEVICE, PROCESS, ORGANIZATION, CLASSIFICATION, DESTINATIONS, RECEIVED, and LAST UPDATE. An 'EVENT HANDLING' modal is open, displaying a summary of the selected events: 'liorgol44 Organization Events' (Selected events: 163078, 152864 for process python.exe, SmartConsole.exe) and 'organization10 Organization Events' (Selected events: 41416, 41450 for process setup.exe, EvilProcessTests.exe). The modal also includes a 'Classification' dropdown, a 'Type comments' text area, an 'Archive When Handled' checkbox, and buttons for 'Save and Handled', 'Save', and 'Cancel'.

If you select security events from more than three organizations, the *Event Handling* window displays the number of organizations and security events you selected in a summary line at the top of the window.

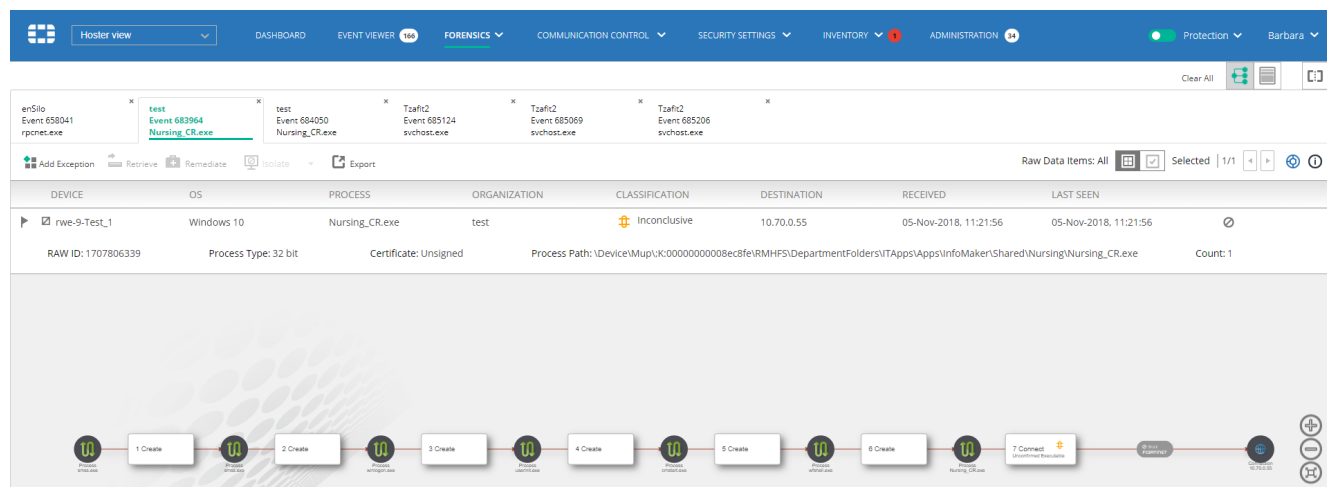
The 'EVENT HANDLING' modal displays a summary line: '35 Events in 4 Organizations where selected'. Below this is a 'Classification' dropdown menu. A large text area labeled 'Type comments' is provided for user input. At the bottom, there is an 'Archive When Handled' checkbox, an 'Advanced' expandable section, and three buttons: 'Save and Handled', 'Save', and 'Cancel'.

In this case, when you hover over the summary line, the details of the selected security events display in a gray box. This box shows the name of the organization and its associated event IDs.



## Forensics

You can select security events from multiple organizations in the Event Viewer and then click the *Forensics* button in the Event Viewer to display these security events in the *Forensics* window. Each security event tab in the *Forensics* window shows the name of the organization in which the security event occurred above the event ID.



## Communication Control

The *Communication Control* window is not available in Hoster view.

## Threat Hunting

### Threat Hunting (Legacy)

In Hoster view, this window includes an *Organization* column. In addition, you can hover over an entry in the Product column to display version information for the item.

ORGANIZATION	COLLECTOR NAME	HASH	PATH	FILE NAME	CREATED	MODIFIED	SIZE	OS	BIT	CERTIFICATE
liorgolf444		A3268A68569DD53EEBC0C...	...diskvolume3\users\lior\desktop	dynamiccode.exe	18-Aug-2019, 11:09	29-Jan-2018, 01:40	132376	Windows 10 Pro	32	No
liorgolf444		A3268A68569DD53EEBC0C...	...iskvolume2\users\user\desktop	dynamiccode.exe	29-Aug-2018, 06:02	29-Jan-2018, 01:40	132376	Windows 7 Professional	32	No
liorgolf444		A3268A68569DD53EEBC0C...	...simulations\dynamiccode.exe	dynamiccode.exe	28-May-2019, 09:13	29-Jan-2018, 01:40	132376	Windows 8.1 Enterprise	32	No
liorgolf444		A3268A68569DD53EEBC0C...	...iskvolume1\users\root\desktop	dynamiccode.exe	25-Mar-2018, 05:07	29-Jan-2018, 01:40	132376	Windows 8.1 Enterprise N	32	No
liorgolf444		A3268A68569DD53EEBC0C...	...3\users\yossim\desktop\test ml	dynamiccode.exe	07-Nov-2019, 06:41	29-Jan-2018, 01:40	132376	Windows 10 Pro	32	No
organization10		A3268A68569DD53EEBC0C...	...iskvolume2\users\root\desktop	dynamiccode.exe	10-Dec-2019, 06:22	29-Jan-2018, 01:40	132376	Windows 10 Pro	32	No
liorgolf444		7DF9CA7D8B8F05BD168995...	...e2\users\administrator\desktop	dynamiccode.exe	29-Jun-2016, 10:16	29-Jun-2016, 10:16	547840	Windows Server 2008 R2 S...	32	No
liorgolf444		4EAC2C2767ED8489C165E5...	...iskvolume2\users\root\desktop	dynamiccode.exe	08-Sep-2016, 05:59	30-Apr-2015, 05:37	549376	Windows 8.1	32	No

## Threat Hunting

In Hoster view, this window includes an *Organization* column.

ORGANIZATION NAME	CATEGORY	TIME	OS	DEVICE NAME	TYPE	PROCESS AND ATTRIBUTES	TARGET	EVENT ATTRIBUTES	TARGET FILE NAME
CompanyA		07-Feb-2021 14:08:07		DESKTOP-R41TQ6F	Socket Close	ntoskrnl.exe	0.0.0.0:0.0.0.0	SOURCE PID: 4 LOCAL ADDRESS: 0.0.0.0:0.0.0.0 REMOTE ADDRESS: 0.0.0.0:0.0.0.0	
CompanyA		07-Feb-2021 14:08:07		DESKTOP-R41TQ6F	Socket Close	ntoskrnl.exe	0.0.0.0:0.0.0.0	SOURCE PID: 4 LOCAL ADDRESS: 0.0.0.0:0.0.0.0 REMOTE ADDRESS: 0.0.0.0:0.0.0.0	
CompanyB		07-Feb-2021 14:07:59		DESKTOP-R41TQ6F	File Rename	SupportAssistClientUL...	SupportAssistAgent.txt-tmp	SOURCE PID: 17796 PATH: Users\EugeneL... HASH: SupportAssistAgent.txt-tmp	
CompanyA		07-Feb-2021 14:07:59		DESKTOP-R41TQ6F	File Create	SupportAssistClientUL...	SupportAssistAgent.txt-RF2e3...	SOURCE PID: 17796 PATH: Users\EugeneL... HASH: SupportAssistAgent.txt-RF2e3...	

## Security settings

### SECURITY POLICIES page

In Hoster view, the *SECURITY POLICIES* page displays all policies from all organizations.

Hoster view

DASHBOARD

EVENT VIEWER166

FORENSICS

COMMUNICATION CONTROL

SECURITY SETTINGS

INVENTORY1

ADMINISTRATION14

Protection

Barbara

SECURITY POLICIES

Showing 1-10/103

Search

Clone Policy

Set Mode

Assign Collector Group

Delete

	ORGANIZATION	POLICY NAME	RULE NAME	ACTION	STATE
<input type="checkbox"/>	All				
<input type="checkbox"/>	A_	Execution Prevention	Fortinet		
<input type="checkbox"/>	A_	Exfiltration Prevention	Fortinet		
<input type="checkbox"/>	A_	Ransomware Prevention	Fortinet		
<input type="checkbox"/>	A_	Device Control	Fortinet		
<input type="checkbox"/>	A_Big_Bank	Execution Prevention	Fortinet		
<input type="checkbox"/>	A_Big_Bank	Exfiltration Prevention	Fortinet		
<input type="checkbox"/>	A_Big_Bank	Ransomware Prevention	Fortinet		
<input type="checkbox"/>	A_Big_Bank	Device Control	Fortinet		
<input type="checkbox"/>	A_Big_Bank	Block-Execution Preventi...			
<input type="checkbox"/>	A_Big_Bank	Block-Exfiltration Preven...			

ADVANCED POLICY & RULE DATA

ASSIGNED COLLECTOR GROUPS

Unassign Group

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.

Hoster view

DASHBOARD

EVENT VIEWER166

FORENSICS

COMMUNICATION CONTROL

SECURITY SETTINGS

INVENTORY166

ADMINISTRATION1012

Protection

Barbara

AUTOMATED INCIDENT RESPONSE - PLAYBOOKS

Showing 1-10/103

Search

Clone Policy

Set Mode

Assign Collector Group

Delete

	ORGANIZATION	NAME		MALICIOUS	SUSPICIOUS	PUP	INCONCLUSIVE	LIKELY SAFE
<input type="checkbox"/>	All organizations	Hoster notification...	Fortinet					
<input type="checkbox"/>	ilorgof444	Default Playbook	Fortinet					
<input type="checkbox"/>	ilorgof444	Default Playbook ...						
<input type="checkbox"/>	organization10	Default Playbook	Fortinet					
<input type="checkbox"/>	organization100	Default Playbook	Fortinet					
<input type="checkbox"/>	organization11	Default Playbook	Fortinet					
<input type="checkbox"/>	organization12	Default Playbook	Fortinet					
<input type="checkbox"/>	organization13	Default Playbook	Fortinet					
<input type="checkbox"/>	organization14	Default Playbook	Fortinet					
<input type="checkbox"/>	organization15	Default Playbook	Fortinet					
<input type="checkbox"/>	organization16	Default Playbook	Fortinet					
<input type="checkbox"/>	organization17	Default Playbook	Fortinet					
<input type="checkbox"/>	organization18	Default Playbook	Fortinet					
<input type="checkbox"/>	organization19	Default Playbook	Fortinet					
<input type="checkbox"/>	organization20	Default Playbook	Fortinet					
<input type="checkbox"/>	organization21	Default Playbook	Fortinet					
<input type="checkbox"/>	organization22	Default Playbook	Fortinet					
<input type="checkbox"/>	organization23	Default Playbook	Fortinet					

ADVANCED PLAYBOOKS DATA

ASSIGNED COLLECTOR GROUPS

Unassign Group

Exception Manager

In Hoster view, the *Exception Manager* page displays all exceptions from all organizations.

## Multi-tenancy (organizations)

Hoster view										
DASHBOARD EVENT VIEWER 186 FORENSICS COMMUNICATION CONTROL SECURITY SETTINGS INVENTORY 1 ADMINISTRATION 11 Protection Barbara										
EXCEPTION MANAGER										
Search Exception Advanced										
Delete Export Showing 1-10/201										
EVENT	PROCESS	PROCESS PATH	EXECUTED WITH	PATH	RULES	ORGANIZATION	COLLECTOR GROUPS	DESTINATIONS	USERS	LAST UPDATED
663219	EXCELEXE	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
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	...ers\\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

Exception 1 +

---

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:

☒ Suspicious Macro
 ⋮

Type comments

Remove Exception

Save Changes Cancel

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	EXCELEXE	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
666041	maktubransomware.exe	...\\Ransomware.Maktub			PUP	enSilo	All groups of enSilo	67.114.64.227	All Users	23-Oct-2018, 18:51 by: Tzafit
442648	camstudio.exe	...ers\\JTM.CDE\\Desktop			Malicious File Detected	All Organizations	All Collector Groups	Internal Destinations...	All Users	25-Sep-2018, 23:16 by: Tzafit

## Inventory

### COLLECTORS page

In Hoster view, the *COLLECTORS* page shows all the Collectors from all organizations.

ORGANIZATION	COLLECTOR GROUP NAME	DEVICE NAME	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	STATE	LAST SEEN
liorgolf444	High Security Collector...								
liorgolf444	Default Collector Group								
liorgolf444	emulation								
liorgolf444	group1								
liorgolf444	group2								
liorgolf444	Insiders								

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(ex) of one or more Collectors.

COLLECTORS (108/108)										
Showing 1-10/219										
Search Collectors or Groups										
Create group Move to group Delete Enable/Disable Isolate Export Uninstall										
<input type="checkbox"/> All	ORGANIZATION	COLLECTOR GROUP NAME	COLLECTOR NAME	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	STATE	LAST SEEN
<input type="checkbox"/>	F-40	High Security Collector Group (0/0)								
<input checked="" type="checkbox"/>	F-40	Default Collector Group (0/0)								
<input type="checkbox"/>	liorferrari	High Security Collector Group (0/0)								
<input type="checkbox"/>	liorferrari	Default Collector Group (11/11)								
<input checked="" type="checkbox"/>	liorferrari	emulation (92/92)								
<input type="checkbox"/>	liorferrari	group_to_policy_playbook (0/0)								
<input type="checkbox"/>	liorferrari	lior1 (5/5)								
<input type="checkbox"/>	liorferrari	lior10								

2. Click the *Move to group* button. The following window displays:

## COLLECTOR GROUPS

Moving 2 workstations collectors to:

Organization

COLLECTOR GROUP

High Security

Default Collector Group

emulation

group1

group2

organization10

organization100

organization11

organization12

organization13

0

Move to Group

Cancel

3. In the *Organization* field, select the organization to which to move the Collector(s).
4. Click *Move to Group*.

## 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:

**serviceNow** Service Management

System Administrator

**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 ⓘ

Do not resend email if server returns these SMTP error codes ⓘ

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 ⓘ

Identify email as a forward by these subject prefixes ⓘ

Discard everything below this text if found in a reply body (comma separated, case sensitive) ⓘ

Ignore mail with these headers (comma separated name:value pairs) ⓘ

Ignore email when subject starts with text (comma separated, case insensitive) ⓘ

Ignore email from these senders. Use the name before the @ sign. (comma-separated) ⓘ

Save

### 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:

ServiceNow

Service Management

System Administrator

users

5. Click the **New** button to create a new user. The following window displays:

The screenshot shows the 'User New record' form in the FortiEDR interface. The form is organized into two main columns. The left column contains text input fields for 'User ID', 'First name', 'Last name', 'Title', and 'Department', followed by a 'Password' field and several checkboxes for 'Password needs reset', 'Locked out', 'Active' (checked), 'Web service access only', and 'Internal Integration User'. The right column contains dropdown menus for 'Email' (support@ensilo.com), 'Language' (None), 'Calendar integration' (Outlook), 'Time zone' (System (US/Pacific-New)), and 'Date format' (System (yyyy-MM-dd)), along with text input fields for 'Business phone' and 'Mobile phone'. A 'Photo' field with a 'Click to add...' button is also present. A 'Submit' button is located at the bottom left of the form. Below the form, there are 'Related Links' including '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:

The screenshot displays the 'Administration > Export Settings' page in the FortiEDR interface. The page has a blue header with navigation tabs: 'Hoster view', 'DASHBOARD', 'EVENT VIEWER', 'FORENSICS', 'COMMUNICATION CONTROL', 'SECURITY SETTINGS', 'INVENTORY', and 'ADMINISTRATION'. The left sidebar contains a list of settings categories: 'LICENSING', 'ORGANIZATIONS', 'USERS', 'DISTRIBUTION LISTS', 'EXPORT SETTINGS' (highlighted), 'TOOLS', 'SYSTEM EVENTS', and 'IP SETS'. The main content area is divided into three sections: 'SMTP', 'OPEN TICKET', and 'SYSLOG'. The 'SMTP' section includes fields for 'Server Name', 'Email address', 'Port', 'Encryption type', 'Sender Name', 'User name', and 'Password', along with a 'Test' button. The 'OPEN TICKET' section has fields for 'System name' and 'Email address'. The 'SYSLOG' section includes a 'Define New Syslog' button and fields for 'Organization', 'Name', 'Host', 'Port', 'Protocol', and 'Use SSL'. A 'NOTIFICATIONS' section is visible on the right side of the page.

7. In the left pane, select **System Policy > Email > Inbound Actions**. The following window displays:

	Name	Active	Event name	Script	Target table	Updated	Order
<input type="checkbox"/>	Create Incident	true	email.read	// Note: current.opened_by is already se...	Incident [incident]	2018-09-05 06:58:50	10
<input type="checkbox"/>	Create Incident	true	email.read	// Note: current.opened_by is already se...	Incident [incident]	2018-05-28 03:49:28	100
<input type="checkbox"/>	Unsubscribe from Notification	true	email.read	(function runAction("/ GlideRecord"/ curr...	Notification Messages [cmn_notif_message]	2016-06-29 09:58:15	1
<input type="checkbox"/>	Update Incident (BP)	true	email.read	gs.include('validators'); if (current.g...	Incident [incident]	2015-10-27 10:02:55	100
<input type="checkbox"/>	Update Approval Request	true	email.read	/* global current, email, gs, GlideContro...	Approval [sysapproval_approver]	2015-04-28 12:58:40	100
<input type="checkbox"/>	Create Live Feed Reply	true	email.read	var l[Util = new LiveFeedUtil(); var rep...	Live Feed Message [live_message]	2014-11-21 00:38:59	100
<input type="checkbox"/>	Create Live Feed Like Reply	true	email.read	var l[Util = new LiveFeedUtil(); var re...	Message Liked by [live_message_like]	2014-11-21 00:36:00	100
<input type="checkbox"/>	Reopen Incident	true	email.read		Incident [incident]	2014-10-15 13:37:20	50
<input type="checkbox"/>	Create Incident (Forwarded)	true	email.read	// Note: current.opened_by is already se...	Incident [incident]	2014-01-17 14:07:38	100
<input type="checkbox"/>	Update Service Category Request	true	email.read	if (current.getTable() == "catalog_c...	Service Category [catalog_category_request]	2013-12-13 08:48:29	100
<input type="checkbox"/>	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      Active: ☒      Stop processing: ☒

Target table: Incident [incident]      Action type: Record Action

When to run: Actions | Description

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: [Add](#)

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: [Add Filter Condition](#)      Add "OR" Clause

-- choose field --      -- oper --      -- value --

Condition:

[Submit](#)

9. Fill in the following fields in this window:

Field	Definition
Name	Enter a free-text name for the inbound email feed. For example, <i>Fortinet inbound email</i> .
Target table	Select <i>Incident [incident]</i> in the dropdown list.
Action type	Select <i>Record Action</i> 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.

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 destinationStart = email.body_text.indexOf('Destinations:');
```

```
var severity = email.body_text.slice(severityStart, classificationStart -15 );
var classification = email.body_text.slice(classificationStart, destinationStart);
current.insert();
```

**12.** When pasting in the JavaScript, make sure that:

- The email 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:

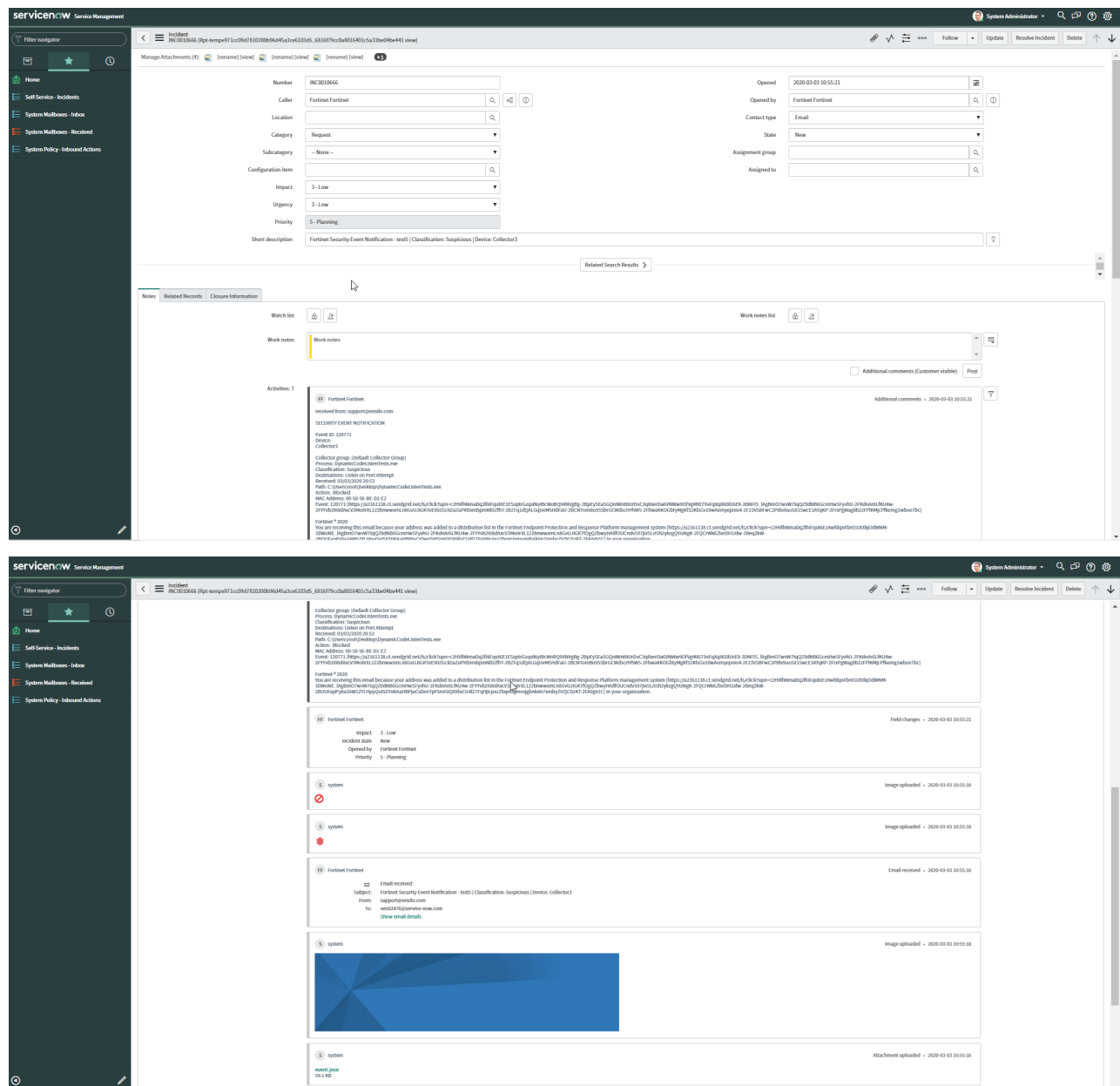
```
//parsing fields from attachment example
if (sys_email.hasAttachments()){
    var att = new GlideRecord("sys_attachment");
    att.addEncodedQuery("table_name=sys_email^table_sys_id=" + sys_email.getValue("sys_
id"));
    att.query();
    while (att.next()){
        if (att.file_name == "event.json" ) {
            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:



FortiEDR 5.2.1 Administration Guide  
Fortinet Inc.



## 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 237](#).

### 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.
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.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.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:

```
Progr?m Fil*
```

Note that 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 TO 140.100.100.255]

## 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 /.



[www.fortinet.com](http://www.fortinet.com)

Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. 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.