FortiEDR Installation and Administration Guide

Version 4.2

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

FORTINET VIDEO GUIDE
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/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

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

FEEDBACK
Email: techdoc@fortinet.com

July 2020

FortiEDR Installation and Administration Guide

Table of Contents

Change Log

Date	Change Description
July 2020	Initial release

Chapter 1 – INTRODUCING FortiEDR

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

Introduction

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

Execution Prevention

Next-Generation Anti-Virus (NGAV) is a signature-less approach that can detect and mitigate zero-day attacks. FortiEDR stops both known and unknown malware types using machine-learning-based NGAV, which filters 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.

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

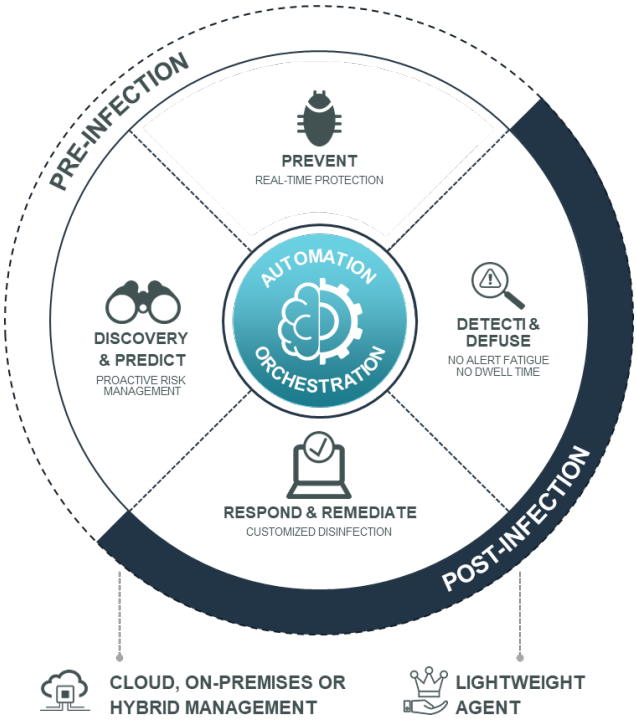
FortiEDR's threat-hunting capabilities features a set of software tools and information sources focused on detecting, investigating, containing and mitigating suspicious activities on end-user devices.

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 IOCs and delivers full attack-chain views – all while simultaneously enabling users to conduct further threat hunting, if and when needed.

FortiEDR's EDR capabilities provide realtime blocking to deliver a multi-layered defense strategy that can be managed from the cloud.

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.

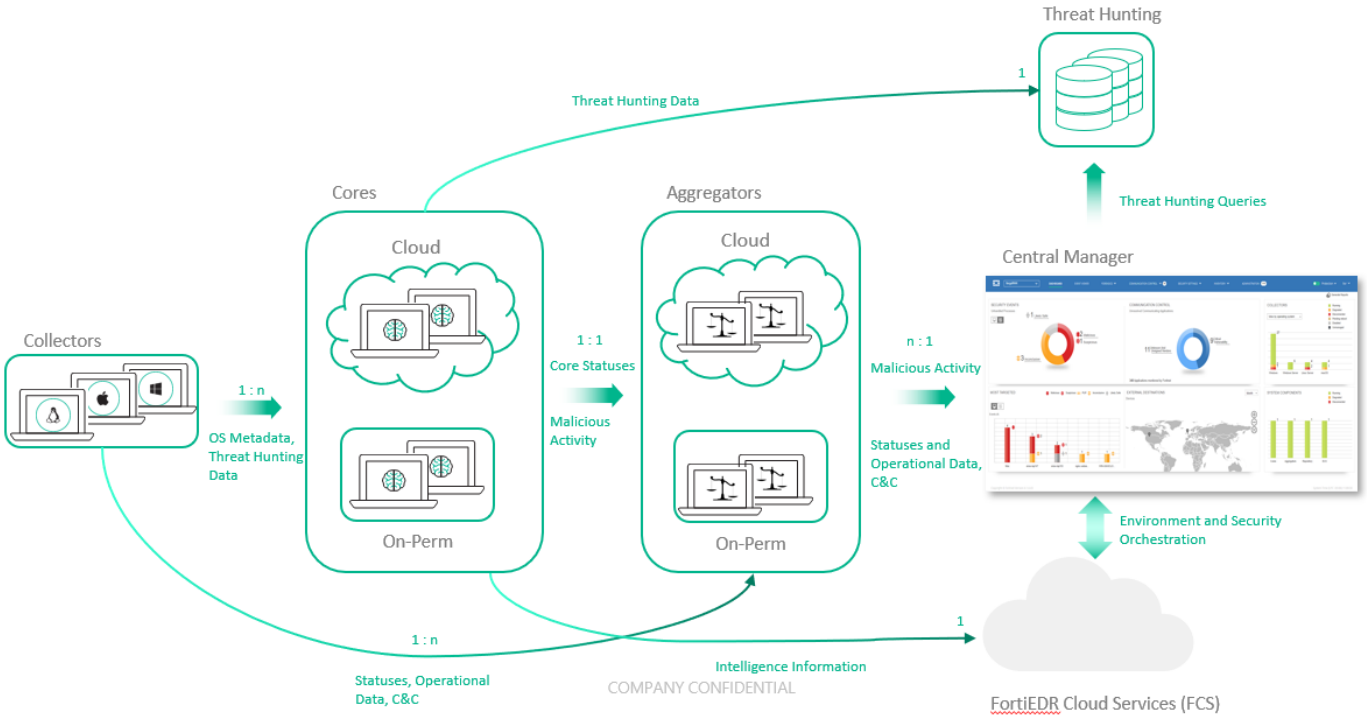
Our research revealed that all legitimate outgoing communications must pass through the operating system. Thus, by monitoring the operating system internals it is possible to verify that a connection was established in a valid manner. FortiEDR gathers OS stack data, thread and process related data and 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 a *brainless* collector that resides on every communicating device in your enterprise, including desktops, laptops and servers.

The FortiEDR Collector resides deep inside the communicating device's operating system.

Upon every attempt made by the communicating device to establish a network connection, the FortiEDR Collector collects all required metadata and sends it to the FortiEDR Core (described below) signed by a FortiEDR digital signature.

The FortiEDR Collector then holds the establishment of this connection until authorization is received from the FortiEDR Core.

- **Pass:** Legitimate requests are allowed out of your network with extremely negligible latency.
- **Block:** Malicious exfiltration attempts are blocked.

Note – 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 the *Component Authentication* section on page 164.

A FortiEDR Collector should be installed on each communicating device in your organization. The same FortiEDR Collector can be installed on all Windows systems, Mac systems 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 and status information.
- **From the FortiEDR Aggregator:** The FortiEDR Collector receives its configuration from the FortiEDR Aggregator.
- **To the FortiEDR Core:** The FortiEDR Collector sends compressed operating system metadata to the FortiEDR Core and then ongoing health and status information.
- **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 since FortiEDR only processes the initial connection establishment. The amount of metadata sent to the FortiEDR Core is so minimal that the latency on the Core's decision point is negligible. Additionally, FortiEDR uses message compression in order to further reduce the traffic sent to the network. You may refer to page 18 for the exact specifications of the system requirements.

Quick and Easy Installation

The FortiEDR Collector comes as a standard MSI 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 on page 182.

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). You may refer to page 18 for the exact specifications of the system requirements. The following are the connections established between the FortiEDR Core and other FortiEDR components:

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

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

FortiEDR Aggregator

The FortiEDR Aggregator is a software-only entity that acts as a proxy for the FortiEDR Central Manager and provides processing load handling services. All FortiEDR Collectors and FortiEDR Cores interact with the Aggregator for registration, configuration and monitoring purposes. The FortiEDR Aggregator aggregates this information for the FortiEDR Central Manager and distributes the configurations defined in the FortiEDR Central Manager 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 3 through 8 of this user guide described 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 an event. The FCS is a cloud-based, GDPR-compliant, software-only service that determines the exact classification of events and acts accordingly based on that classification – all with a high degree of accuracy.

The FCS 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 event exception (whitelisting). After a triggered 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 *Exceptions* on page 66.
- **Playbook Actions:** All Playbook policy actions are based on the final determination of the FCS. For more details, see *Playbook Policies* on page 59.

How Does FortiEDR Work?

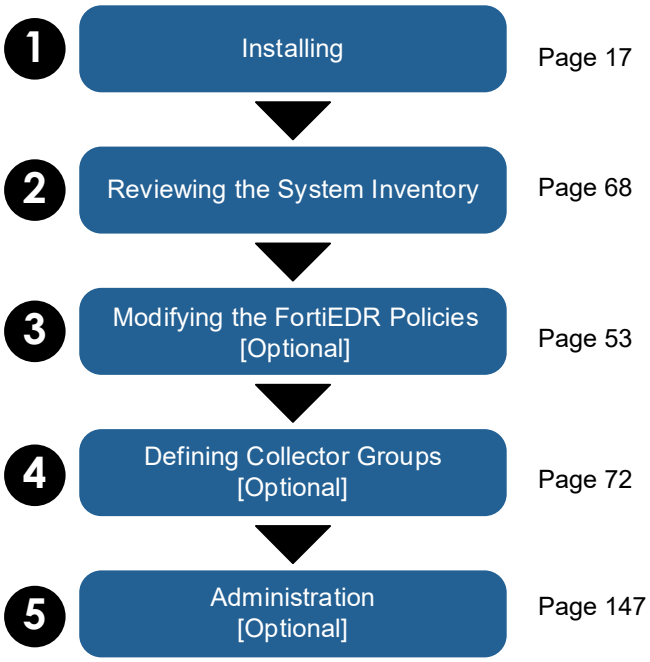
- **Step 1, The FortiEDR Collector Collects OS Metadata:** A FortiEDR Collector runs on each communicating device in the organization and transparently collects OS metadata on the computing device.
- **Step 2, Communicating Device Makes a Connection Establishment Request:** When any connection establishment 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.
- **Step 3, The FortiEDR Core Identifies Malicious Requests:** Using FortiEDR's patented technology, the FortiEDR Core analyzes the collected OS metadata and enforces the policies.
- **Step 4, Pass or Block:** Only legitimate connections are allowed outbound communication. Malicious outbound connection attempts are blocked.
- **Step 5, Event Generation:** Each FortiEDR policy violation generates a realtime 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 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.
- Step 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 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

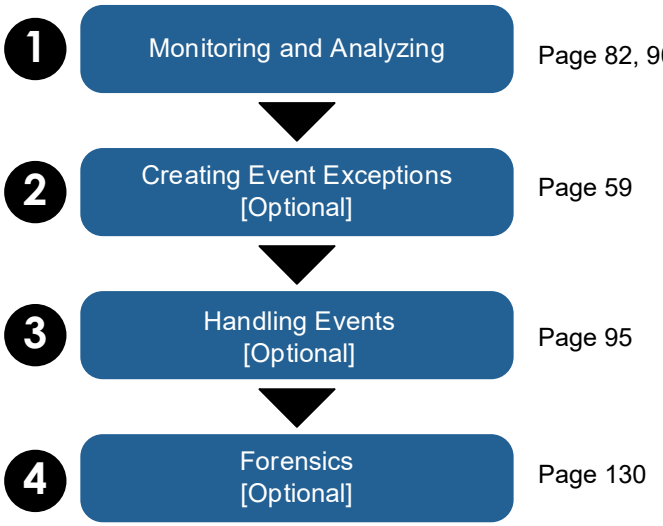
The following describes the workflow for getting FortiEDR up and running in your organization:



- **Step 1, Installing:** Install all FortiEDR components, as described in *Chapter 2, INSTALLING FortiEDR* on page 17 and launch the FortiEDR Central Manager for the first time (page 29).
- **Step 2, Reviewing the Inventory:** Review the health status and details of all the FortiEDR components in the **DASHBOARD** (page 82) and **INVENTORY** tab (page 68). FortiEDR Collectors are automatically assigned FortiEDR's default policies.
- **Step 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** tab (page 53) to modify the default policies for blocking and/or to create additional policies.
- **Step 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 the **INVENTORY** tab (page 72). You can then assign the required policy to each Collector Group (page 58).
- **Step 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 events on an ongoing basis:



- **Monitoring:** Monitor and analyze the events triggered by FortiEDR in the:
  - **Dashboard** (page 82)
  - **Event Viewer** (page 90)
  - **SIEM via Syslog** (page 159)
- **[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 (page 59).
- **[Optional] Handling Events:** Mark events that you have handled and optionally describe how they were handled (page 95).
- **[Optional] Forensics** (page 130): This licensed add-on enables deep investigation into an event, including the actual internals of the communicating devices' operating system.

Chapter 2 – INSTALLING FortiEDR

This chapter describes how to install each of the FortiEDR components.

Before You Start

Before you start the FortiEDR installation process, please make sure that:

- All devices, workstations, virtual machines and servers on which a FortiEDR component will be installed comply with the system requirements provided on page 18.
- You have read and selected the most suitable deployment option for you.
- FortiEDR Core, FortiEDR Aggregator and FortiEDR Central Manager use ports 555, 8081 and 443, respectively. Ensure that these ports 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.

Install the system components top-down in the following order:

- FortiEDR Threat-hunting Repository, page 19
- FortiEDR Central Manager Server and FortiEDR Aggregator, page 24
- FortiEDR Cores, page 33
- FortiEDR Collectors, page 38

System Requirements

Component	System Requirements
Processor	▪ The FortiEDR Collector runs on Intel or AMD x86 – both 32-bit and 64-bit. ▪ FortiEDR Core, FortiEDR Aggregator and FortiEDR Central Manager run on Intel or AMD x86 64-bit. ▪ Hypervisors-compatible. ▪ FortiEDR is designed to use less than 1% CPU for the FortiEDR Collector. ▪ FortiEDR Core, Aggregator and Central Manager require a minimum of two CPUs.
Physical Memory	▪ FortiEDR Collector requires at least 60 MB of RAM. ▪ FortiEDR Core requires at least 8 GB of RAM. ▪ FortiEDR Aggregator requires at least 16 GB of RAM. ▪ FortiEDR Central Manager requires at least 16 GB of RAM.
Disk Space	▪ FortiEDR Collector installation requires at least 20 MB of disk space. ▪ FortiEDR Core installation and log space requires at least 60 GB of disk space. ▪ FortiEDR Aggregator installation and logs space requires at least 80 GB of disk space. ▪ FortiEDR Central Manager installation and logs space requires at least 150 GB of disk space.

Component	System Requirements
Connectivity	▪ FortiEDR Core listens to communication on port 555. ▪ FortiEDR Aggregator listens to communication on port 8081. ▪ Browser connection to the FortiEDR Core is via port 443. ▪ FortiEDR Core, FortiEDR Aggregator and FortiEDR Central Manager components must be assigned a static IP address or domain name. The FortiEDR Aggregator and FortiEDR Central Manager can be installed on the same machine. ▪ Network connectivity between all system components is required. ▪ Allow up to 5 Mbps of additional network workload for each 1,000 Collectors.
Supported Operating Systems	The FortiEDR Collector can be installed on any of the following operating systems (both 32-bit and 64-bit versions): ▪ Windows XP SP2/SP3, 7, 8, 8.1and 10. ▪ Windows Server 2003 SP2, R2 SP2, 2008 SP2, 2008 R2 SP1, 2012, 2012 R2, 2016 and 2019. ▪ MacOS Versions: Yosemite (10.10), El Capitan (10.11), Sierra (10.12), High Sierra (10.13), Mojave (10.14) and Catalina (10.15). ▪ Linux Versions: RedHat Enterprise Linux and CentOS 6.8, 6.9, 6.10, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7 and 7.8 and Ubuntu LTS 16.04.5, 16.04.6, 18.04.1 and 18.04.2 server, 64-bit only. ▪ VDI Environments: VMware Horizons 6 and 7 and Citrix XenDesktop 7. ▪ The FortiEDR Core, Repository Server, FortiEDR Aggregator and FortiEDR Central Manager components are supplied in ISO format, which includes a CentOS 7 image. FortiEDR Core, FortiEDR Aggregator and FortiEDR Central Manager can be installed on a virtual machine or a dedicated workstation or server.
Supported Browsers	The FortiEDR Central Manager console can be accessed using the Google Chrome, Firefox Mozilla, Microsoft Edge and Apple Safari browsers.
Threat-hunting Repository	▪ The number of CPUs (Cores) depends on the number of FortiEDR Cores connected to the threat-hunting repository and the total number of CPUs on these Cores. A minimum of four CPUs is required. For example, if the customer has a Core with two CPUs, then the threat-hunting repository should have four CPUs. Similarly, if the Core has four CPUs, then the threat-hunting repository should have four CPUs. If the customer has two active Cores, each with two CPUs, then the threat-hunting repository should have four CPUs. ▪ Disk Size: Minimum of 200 GB of available space. ▪ Memory: At least 16 GB

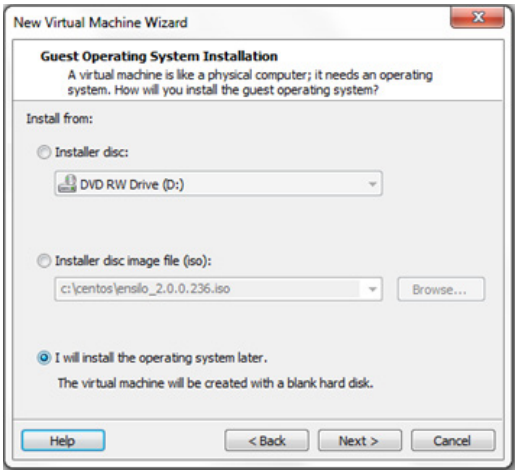
Installing the FortiEDR Threat-hunting Repository

The FortiEDR threat-hunting repository handles the FortiEDR threat-hunting feature, which is described on page 144. If you have a license for the threat-hunting feature, install this component first. The threat-hunting repository must be installed before installing the FortiEDR Central Manager.

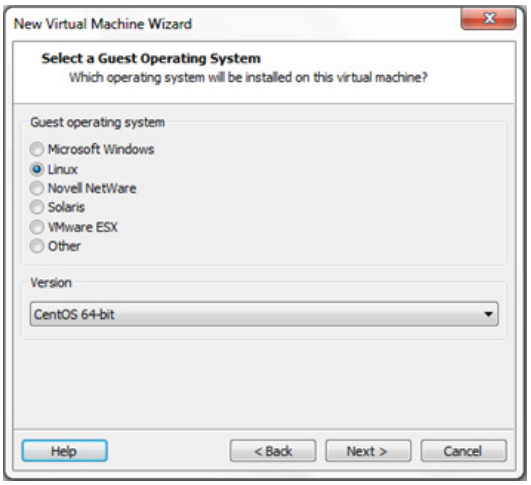
To install the FortiEDR threat-hunting repository:

1. Create a new virtual server. For example, by selecting **File ➔ New Virtual Machine….** The following window displays:

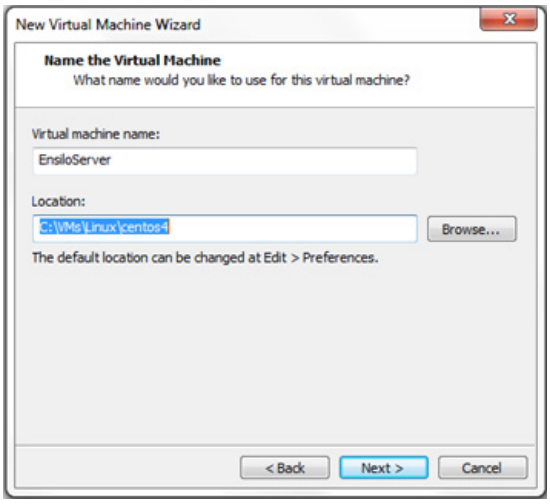
2. Select the **Typical** option and click **Next**. The following displays:



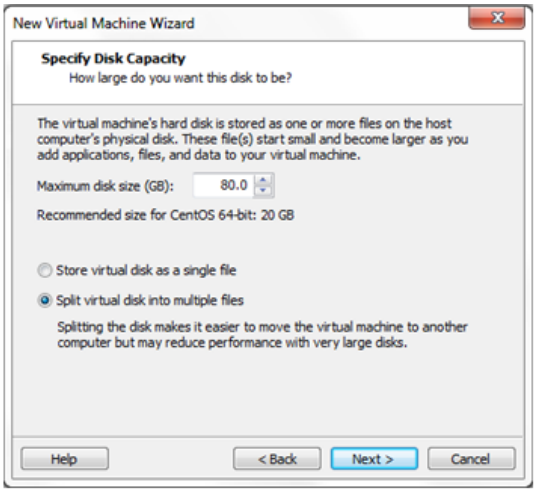
3. Select the **I will install the operating system later** option and click **Next**. The following displays:



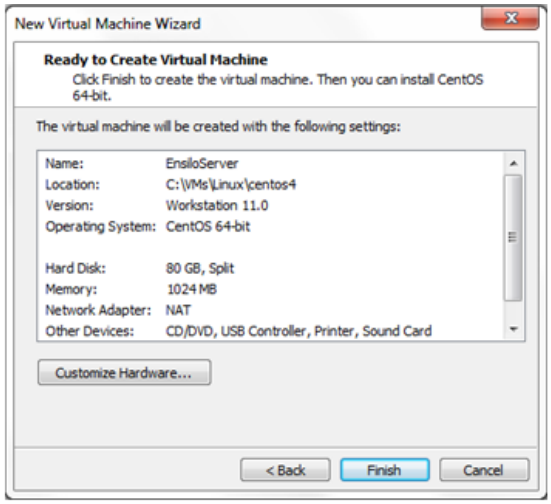
4. Select the **Linux** radio button. In the **Version** field, select **CentOS 7 64-bit** and click **Next**. Alternatively, you can select a different generic Linux 64-bit option in the **Version** field. The following displays:



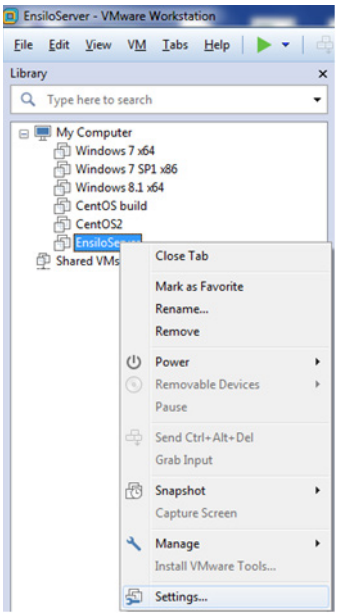
5. Specify a name such as *FortiEDRThreatHuntingRepository* for the virtual machine and the location in which to store the provided ISO file and click **Next**. The following displays:



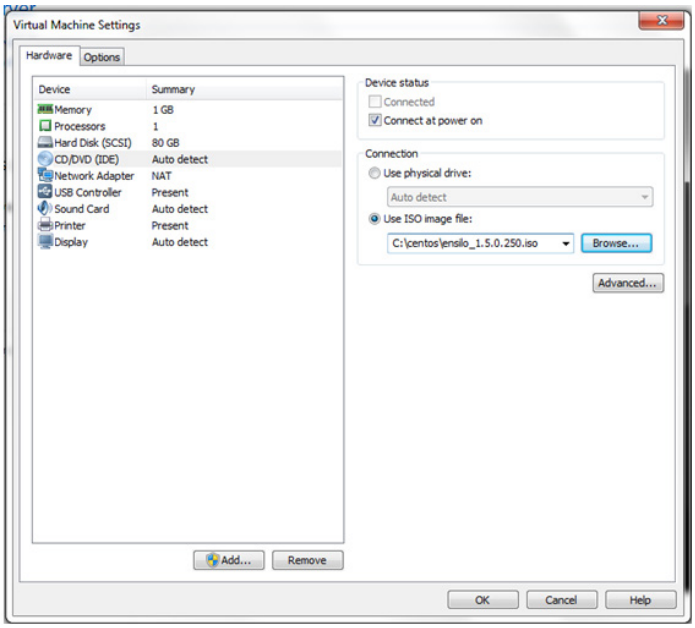
6. Change the **Maximum disk size** to **200 GB**, leave the default option as **Split virtual disk into multiple files** and click **Next**. The following displays:



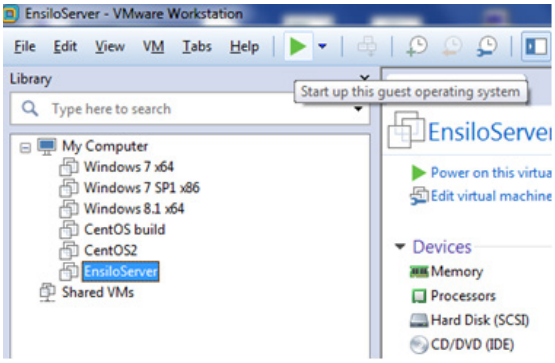
7. Click **Finish**.
8. Right-click the new machine and select the **Settings** option.



The following window displays:



9. Select the **Memory** option and change the RAM to at least 16 GB.
10. Select the **Processors** option and change the value to a total of at least four 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 Threat Hunting Repository. 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` and click **Next**.

Note – This can be any hostname.

19. At the prompt, select the role of the virtual machine. For this installation, select `EDR` and click **Next**.
20. At the `Please enter EDR user` prompt, enter the threat-hunting repository `user` and click **Next**.
21. At the `Please enter EDR password` prompt, enter the threat-hunting repository `password` and click **Next**.
22. 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**.
23. At the `Do you want to use DHCP` prompt, do one of the following:
    - Select `Yes` to use DHCP and click **Next**. Proceed to step 27 below.
    - Select `No` to configure the IP of this virtual machine manually, and then click **Next**. Perform steps 24 through 31 below.
24. At the prompt, enter the IP address of the machine that you are installing. Use the following format: xxx.xxx.xxx.xxx/yyyy, where yyyy is the routing prefix of the subnet.
25. At the prompt, enter the default gateway and click **Next**.
26. At the `Please set your DNS server` prompt, enter a valid IP address and click **Next**. Use the following format: xxx.xxx.xxx.xxx/yyyy, where yyyy is the routing prefix of the subnet.
27. At the prompt, select **No** for debug mode.
28. 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.

29. At the `Please set your Time` prompt, set the time and click **Next**.
30. At the prompt, select the `timezone` and `country` in which the server is being installed.
31. Wait a few moments while the installation processes, until you see the `Installation completed successfully` message.

Installing the FortiEDR Central Manager and FortiEDR Aggregator on the Same Machine

The following describes how to install both the FortiEDR Central Manager and the FortiEDR Aggregator on the same machine.

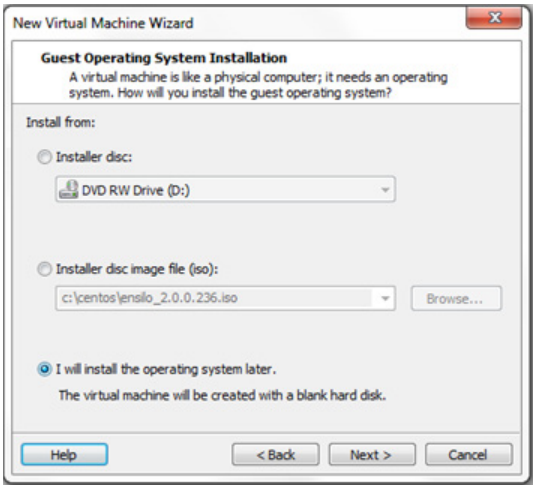
The same ISO file is provided for installing both the FortiEDR Central Manager and the FortiEDR Aggregator. Both of these can be installed on the same machine or separately. To install these components on different machines, see page 28.

The procedure below describes how to install the FortiEDR Central Manager on a virtual server.

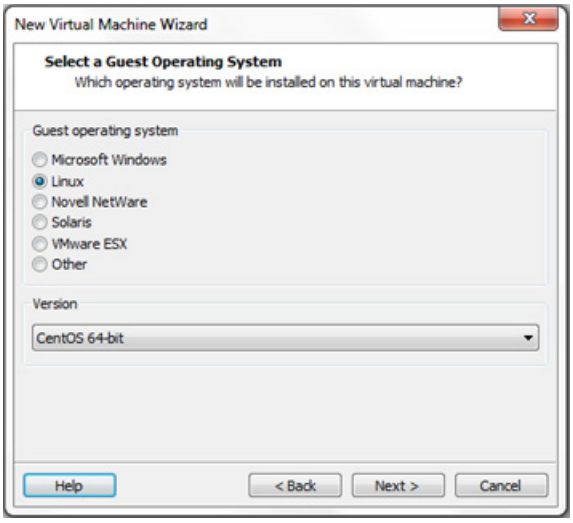
To install the FortiEDR Central Manager and/or FortiEDR Aggregator on the same machine:

1. Create a new virtual server. For example, by selecting **File ➔ New Virtual Machine….** The following window displays:

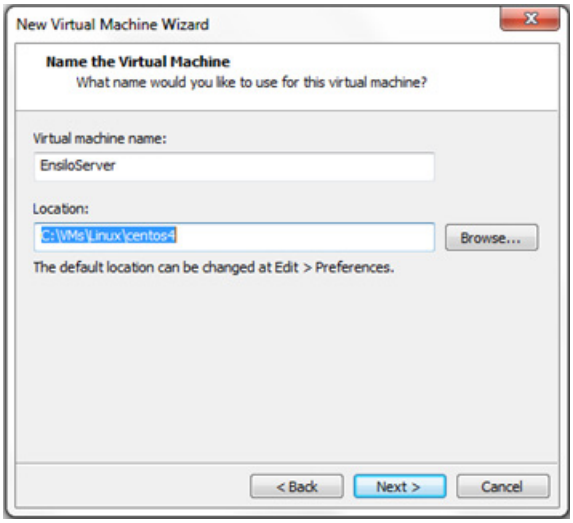
2. Select the **Typical** option and click **Next**. The following displays:



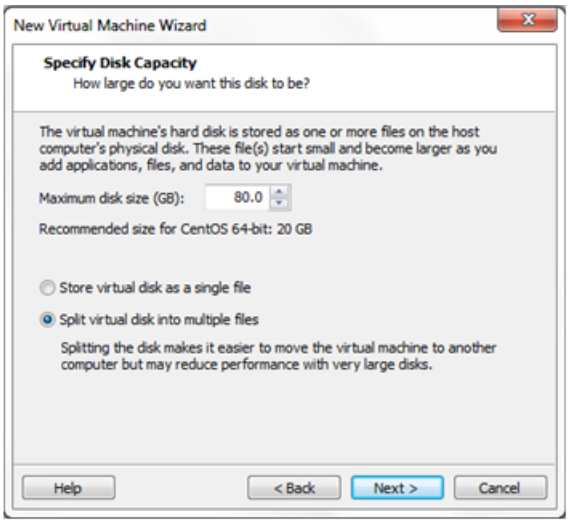
3. Select the **I will install the operating system later** option and click **Next**. The following displays:



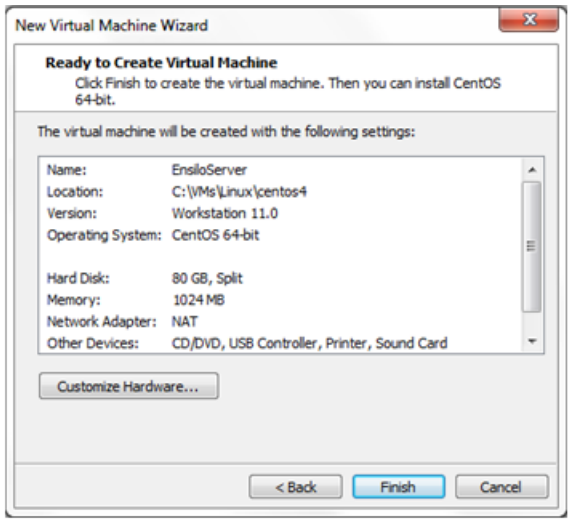
4. Select the **Linux** radio button. In the **Version** field, select **CentOS 7 64-bit** and click **Next**. Alternatively, you can select a different generic Linux 64-bit option in the **Version** field. The following displays:



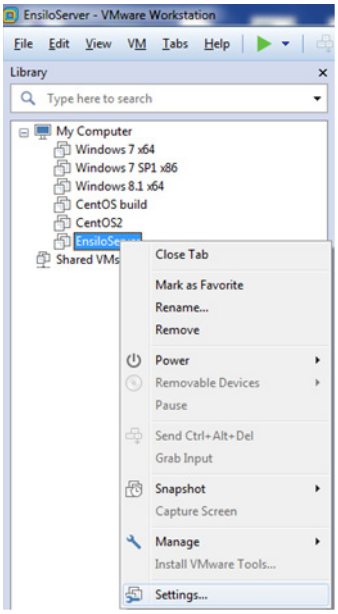
5. Specify a name such as *FortiEDRCentralManager* for the virtual machine and the location in which to store the provided ISO file and click **Next**. The following displays:



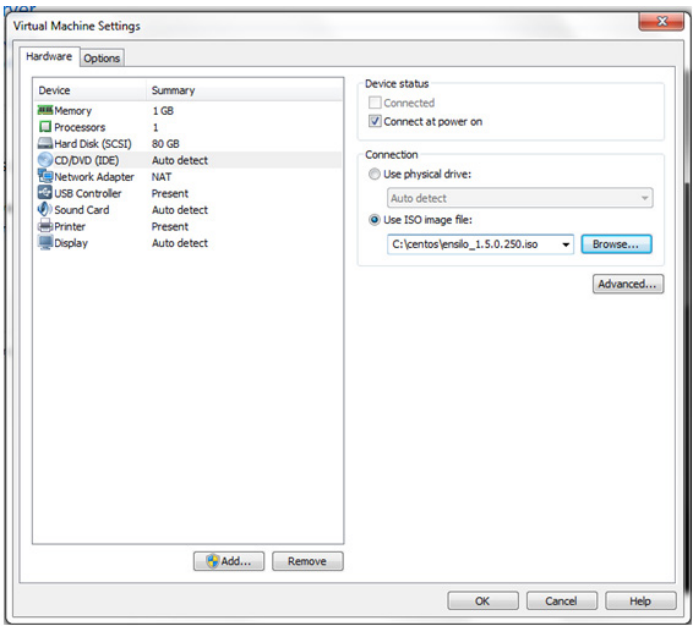
6. Change the **Maximum disk size** to **150** GB, leave the default option as **Split virtual disk into multiple files** and click **Next**. The following displays:



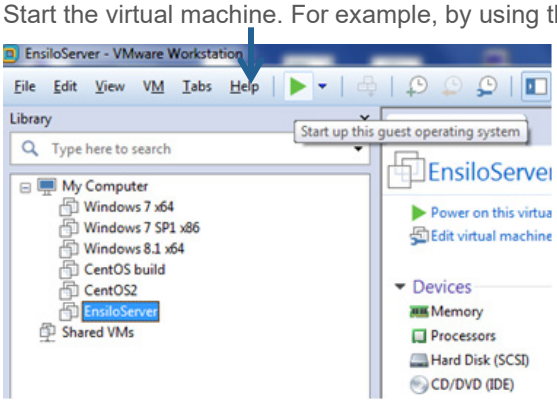
7. Click **Finish**.
8. Right-click the new machine and select the **Settings** option.



The following window displays:



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 Central Manager. 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` and click **Next**.

    Note – This can be any hostname.
19. At the prompt, select the role of the virtual machine. For this installation, which installs both the FortiEDR Central Manager and FortiEDR Aggregator on the same machine, select `(B)oth` and click **Next**.

20. At the `Do you want to connect to EDR server?` prompt, which relates to the FortiEDR threat-hunting feature, select one of the following options:
    - Select `Yes` if you have a threat-hunting license and then click **Next**. Perform steps 19 through 22 below.
    - Select `No` if you do not have a threat-hunting license and click **Next**. Proceed to step 23 below.

    Note –The threat-hunting repository must be installed before installing the FortiEDR Central Manager. For more details, see the *Installing the FortiEDR Threat-hunting Repository* section on page 19.
21. At the prompt, enter the threat-hunting repository `IP address` and click **Next**. This address is set during repository installation.
22. At the prompt, enter the threat-hunting repository `port` and click **Next**. The default port is 443. This port is set during repository installation.
23. At the prompt, enter the threat-hunting repository `user` and click **Next**. This user is set during repository installation.
24. At the prompt, enter the threat-hunting repository `password` and click **Next**. This password is set during repository installation.

    Note –The threat-hunting repository password can be different than the FortiEDR Central Manager registration password.
25. 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**.
26. At the `Do you want to use DHCP` prompt, do one of the following:
    - Select `Yes` to use DHCP and click **Next**. Proceed to step 30 below.
    - Select `No` to configure the IP of this virtual machine manually, and then click **Next**. Perform steps 27 through 29 below.
27. At the prompt, enter the IP address of the machine that you are installing. Use the following format: xxx.xxx.xxx.xxx/yyyy, where yyyy is the routing prefix of the subnet.
28. At the prompt, enter the default gateway and click **Next**.
29. At the `Please set your DNS server` prompt, enter a valid IP address and click **Next**. Use the following format: xxx.xxx.xxx.xxx/yyyy, where yyyy is the routing prefix of the subnet.
30. At the prompt, select **No** for debug mode.
31. 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.
32. At the `Please set your Time` prompt, set the time and click **Next**.
33. At the prompt, select the `timezone` and `country` in which the server is being installed.
34. Wait a few moments while the installation processes, until you see the `Installation completed successfully` message.
35. Log in for the first time, as described on page 29.

To install the FortiEDR Central Manager and FortiEDR Aggregator on different machines:

1. To install only the FortiEDR Central Manager component, perform the entire *To install the FortiEDR Central Manager and/or FortiEDR Aggregator on the same machine* procedure described on page 24.
2. To install only the FortiEDR Aggregator component, perform steps 1 through 22 in the *To install the FortiEDR Central Manager and/or FortiEDR Aggregator on the same machine* procedure described on page 24. Then, perform the steps described below.
3. At the `Please enter the management IP address` prompt, enter the IP address to be used for communicating with the FortiEDR Central Manager and click **Next**.
4. At the `Please enter your registration password` prompt, enter the user and password used to register the FortiEDR Aggregator with the FortiEDR Central Manager and click **Next**.
5. Perform steps 23 through 32 in the *To install the FortiEDR Central Manager and/or FortiEDR Aggregator on the same machine* procedure described on page 24.

FortiEDR CLI Commands

The following describes additional commands that you can perform in the FortiEDR Core, Repository Server, FortiEDR Central Manager or FortiEDR Aggregator CLI. At the prompt, type `fortiedr` or `fortiedr help` to display them.

```
[root@FortiEDR-both-yearly-concrete-stinkbug ~]# fortiedr help
FortiEDR control & management tool 2018(c).
Usage: fortiedr [componet] <command> [args...]

Basic actions:
--------------
  help                                  Display this message and exit
  config                                Run fortiedr installer
  start                                 start all active components
  stop                                  stop all active components
  status                                get active components status
  version                               show current version
  tzselect                              select a timezone
  logs-watch                            display aggregator and manager logs

General Service Controls:
-------------------------
Example: fortiedr {edr|aggregator|core|manager} {start|stop|restart|status|enable|disable}

  start                                 start service
  stop                                  stop service
  restart                               restart service
  status                                service status
  enable                                enable service
  disable                               disable service


Specific Component Controls:
----------------------------
aggregator
  start-debug                           run in debug mode
  stop-debug                            stop debug mode
  port-change <port>                    change aggregator port
  set-dns <dns_name>                    change aggregator dns_name
  bandwidth config <bandwidth>          change aggregator bandwidth limit in Kb/s
  bandwidth enable                      enable aggregator bandwidth limit
  bandwidth disable                     disable aggregator bandwidth limit
  logs-watch                            display aggregator logs

edr
  set-properties <user> '<password>'    set user and password
```

Launching the FortiEDR Central Manager for the First Time

Note –The procedure below enables you to define passwords. No passwords are provided by Fortinet.

To launch the FortiEDR Central Manager:

1. Use any standard Internet browser to connect securely (via https://) to the IP address and port of the machine on which the FortiEDR Central Manager is installed, as follows:

   https://<machine_IP_address>/

   The default port is 443.

   The FIRST TIME ADMINISTRATOR LOGIN window is displayed, as shown below:

2. Define the first administrator user to be allowed to log into the FortiEDR Manager by filling in the **First Name**, **Last Name**, **Email Address** and **Define administrator user name** fields.
3. Enter and confirm the password to be used by this administrator user.
4. In the **DEVICE REGISTRATION PASSWORD** fields, enter and confirm the password to be used to install all FortiEDR Collectors, FortiEDR Aggregators and FortiEDR Cores. This same password must be used by all.

Write this password down in a good place. This password will be needed each time a FortiEDR component is installed. If you forgot your registration password, contact Fortinet support. FortiEDR support can reset your password and provide you with a new one.

---

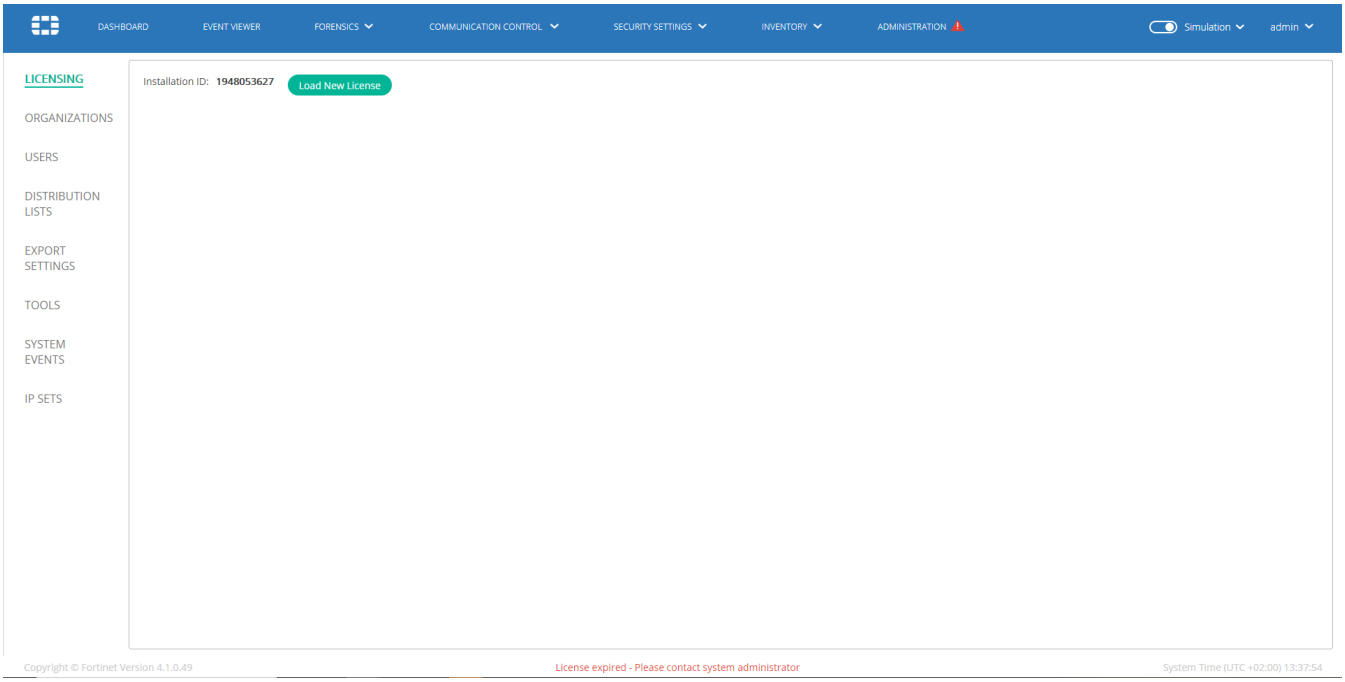
5. Click the **LOGIN** button. The regular FortiEDR Central Manager Login page is then displayed, as shown below. The page that displays varies, depending on whether the FortiEDR system is set up as a single-organization or multi-organization system.

Login Page in a Single-organization System

Login Page in a Multi-organization System

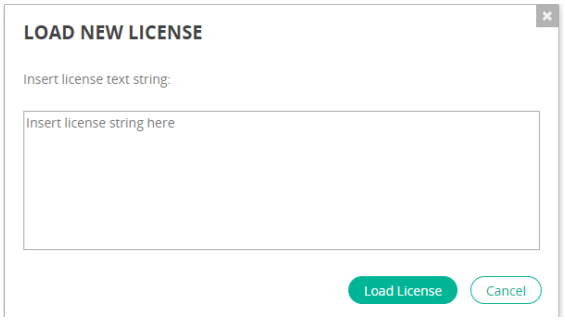
Note – The FortiEDR system can be set up as a single-organization or multi-organization system. In a multi-organization system, all users except an Administrator user must specify the organization in the **Organization Name** dropdown list. If a user is defined for an organization, then he/she can log in to that organization. Otherwise, he/she cannot.
For more details about logging in to a multi-organization system, see *Step 1 – Logging In to a Multi-organization System* on page 185.
Note – If you forgot your user interface password, contact Fortinet support. Fortinet support can reset your password and provide you with a new one.

6. Enter the administrator user name and password you have just defined and click the **LOGIN** button. All fields are case sensitive. The following window displays automatically the first time you log into the FortiEDR Central Manager:

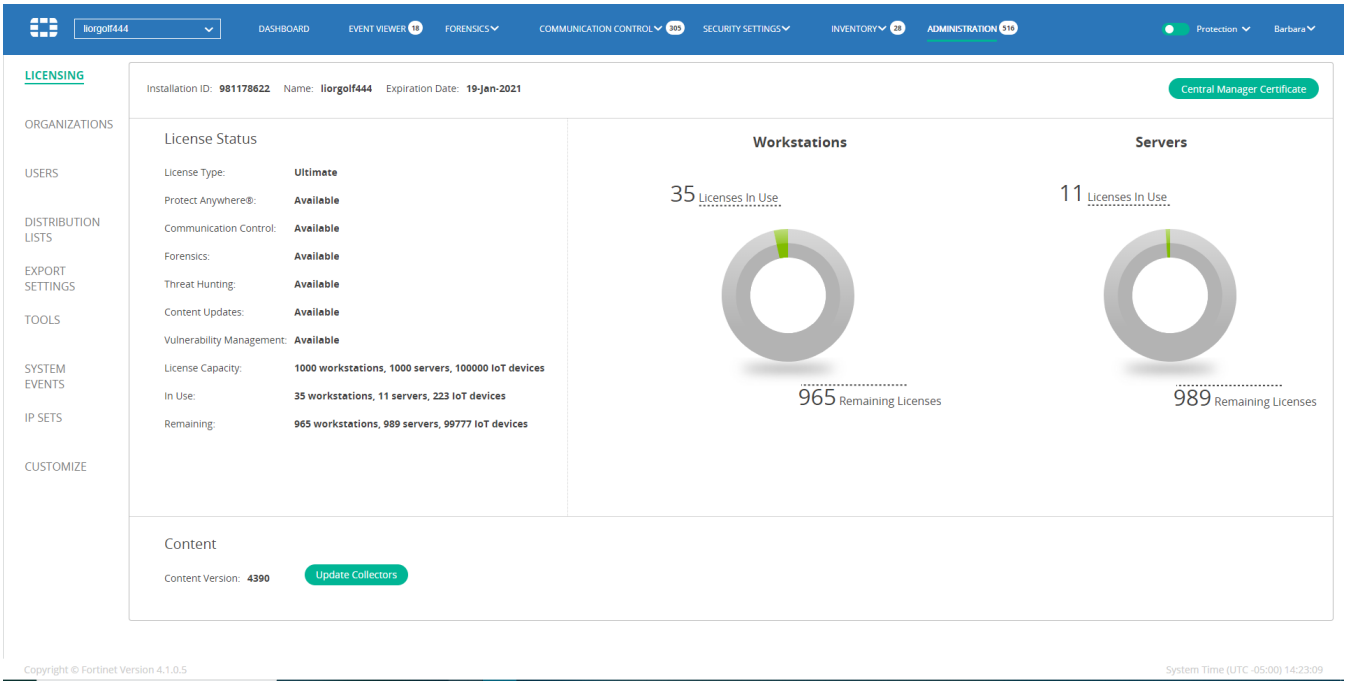


7. Send the displayed Installation ID to FortiEDRAdmin@fortinet.com by email in order to receive a license string from Fortinet.

8. Click the **Load New License** button. The following window displays:



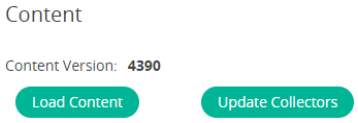
9. Copy/paste the license string that you received by email into the LOAD NEW LICENSE window and click the **Load License** button. The following displays showing the relevant licensed entitlements:



- **Installation ID:** 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 **Name** field when contacting Fortinet for support.
- **Name:** Specifies the name of the organization in a multi-organization FortiEDR system. For more details, see *Chapter 11*, *Multi-tenancy (Organizations)* on page 183.
- **Expiration Date:** Specifies when this license expires. Notifications will be sent to you beforehand.
- **License Type:** Specifies whether the **Predict, Protect and Response** license, **Predict, Protect and Response – Air-gapped** license, **Predict and Protect** license or **Protect and Response** license was purchased. The license type defines the availability of the relevant add-ons.
- **Communication Control:** Specifies the word **Available** if the **Communication Control** add-on is included in the license.
- **Forensics:** Specifies the word **Available** if the Forensics add-on (described on page 130) is included in the license.
- **Threat Hunting:** Specifies the word **Available** if the Threat hunting add-on (described on page 144) is included in the license.
- **Content Updates:** Specifies the word **Available** if the **Content Updates** add-on is included in the license. This add-on enables you to automatically receive the latest FortiEDR policy rule and built-in exception updates.

The system arrives with the latest content pre-installed. There is no need to install content during the initial installation.

The Load Content button enables you to update content, as well as to update the Collector version on any existing Collector.

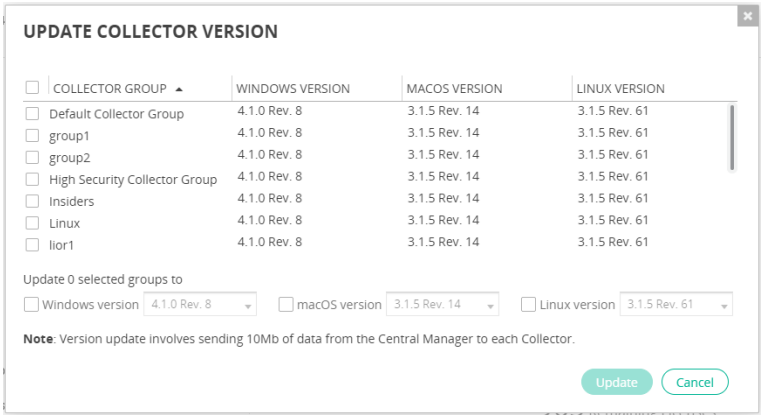


To load content updates on your FortiEDR system, click the Load Content button and then select the content file to load. In a multi-tenant environment, the Load Content button is available in Hoster View 

.

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.



- **Vulnerability Management:** Specifies the word **Available** if the Vulnerability Management add-on (described on page 147) is included in the license.
- **License Capacity:** 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).
- **In Use:** 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.
- **Remaining:** Specifies the number of FortiEDR licenses for workstations and servers that are still available for use.
- Regarding questions about the number of licenses purchased, you may contact Fortinet support.

The FortiEDR Central Manager Server and console are now fully installed.

Continue to install the other system components (as described below) before using the FortiEDR Central Manager to configure the system.

Installing the FortiEDR Core

Preparing for FortiEDR Core Installation

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

- Complies with the requirements described in the *System Requirements* section on page 18.
- 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 page 181.
- Has connectivity to the FortiEDR Reputation Server at **reputation.ensilo.com**. Connectivity is recommended for enhanced security.
- 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 , or 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 or for PAC: nslo_https_proxy=pac+http://192.168.200.100/sample.pac**

Note – For more details about installing a Core in a multi-organization environment, see the *Core Registration* section on page 184.

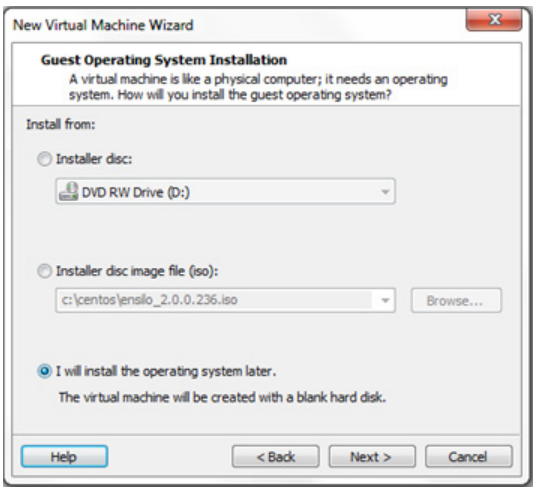
Installing the FortiEDR Core on Linux

The following describes how to install the FortiEDR Core on Linux.

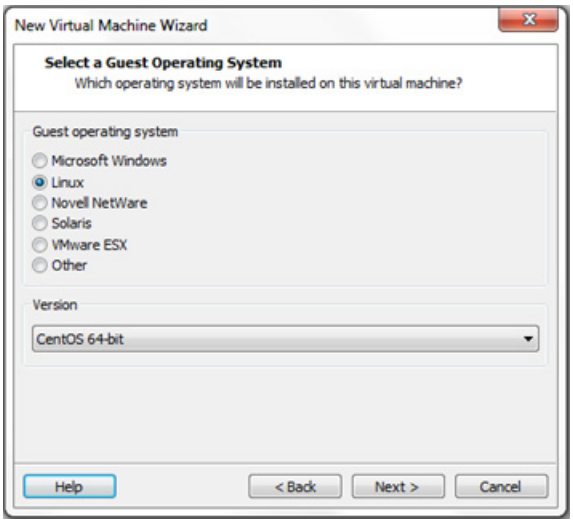
To install the FortiEDR Core on Linux:

1. Create a new virtual server. For example, by selecting **File ➔ New Virtual Machine….** The following window displays:

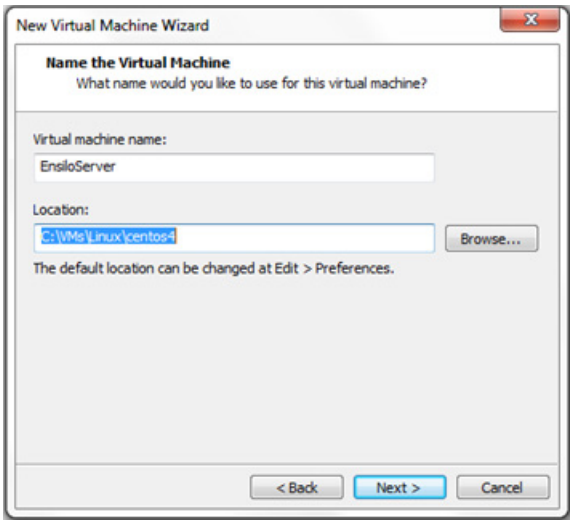
2. Select the **Typical** option and click **Next**. The following displays:



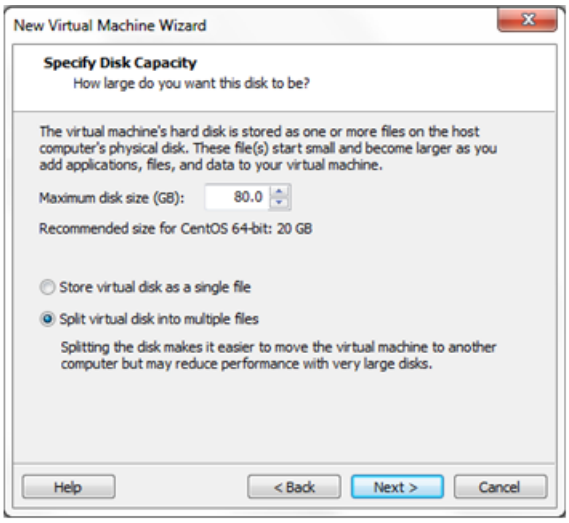
3. Select the **I will install the operating system later** option and click **Next**. The following displays:



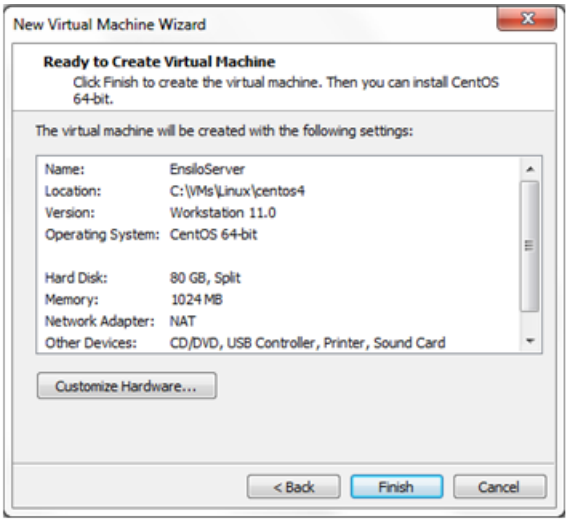
4. Select the **Linux** radio button. In the **Version** field, select **CentOS 64-bit** and click **Next**. Alternatively, you can select a different generic Linux 64-bit option in the **Version** field. The following displays:



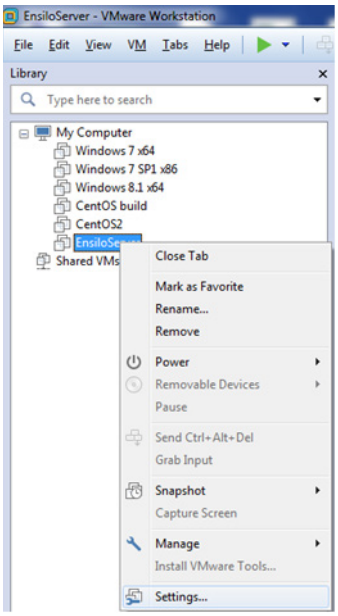
5. Specify a name for the virtual machine such as *FortiEDRCore* and the location in which to store the provided ISO file and click **Next**. The following displays:



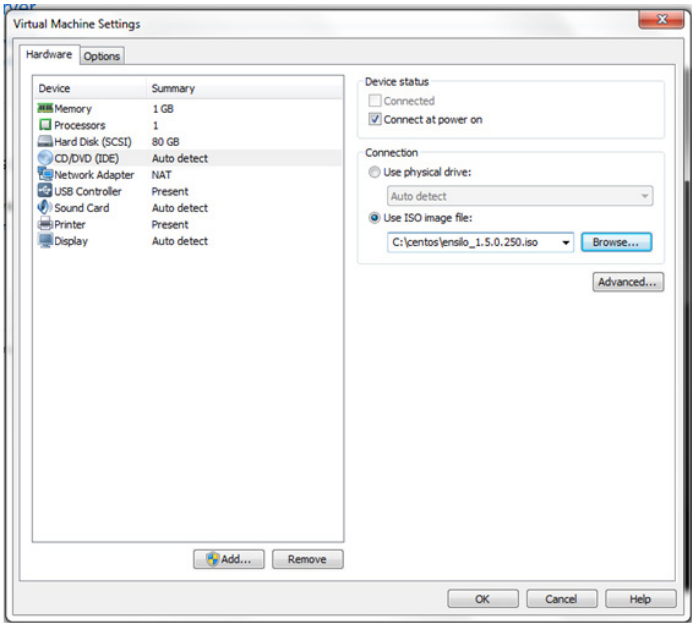
6. Change the **Maximum disk size** to **80** GB, leave the default option as **Split virtual disk into multiple files** and click **Next**. The following displays:



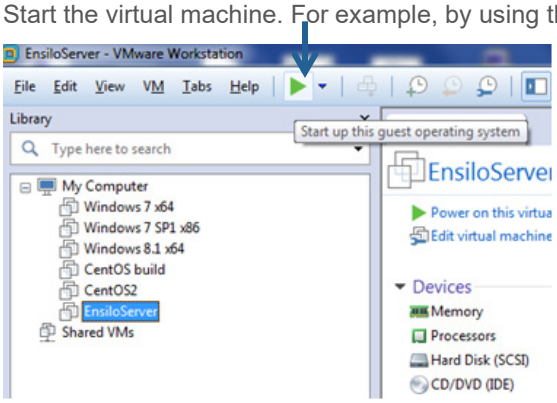
7. Click **Finish**.
8. Right-click the new machine and select the **Settings** option.



The following window displays:



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**.
20. At the prompt, enter the registration password, which is described on page 29.

    Note that 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:
    - Select `Yes` to use DHCP and click **Next**. Proceed to step **29** below.
    - 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/yyyy, where yyyy 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/yyyy, where yyyy 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. Verify that the FortiEDR Core details are listed in the **INVENTORY** tab of the FortiEDR Central Manager.

Installing FortiEDR Collectors

Preparing for FortiEDR Collector Installation

The communicating device on which the FortiEDR Collector will be installed, must meet the following requirements:

- Complies with the requirements described in the *System Requirements* section on page 18.
- 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 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 page 181.
- If the FortiEDR Collector 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 , or 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 Collector with the name **nslo_https_proxy** at the file **/etc/environment**.

    For example: nslo_https_proxy=https://192.168.0.2:443 or for PAC: nslo_https_proxy=pac+http://192.168.200.100/sample.pac

Note – For more details about installing a Collector in a multi-organization environment, see the *Collector Registration* section on page 184.

Installing a FortiEDR Collector

Only the number of FortiEDR Collectors allowed by the license can register with the FortiEDR Central Manager.

Additional FortiEDR Collectors cannot register with the FortiEDR Central Manager.

You can uninstall a FortiEDR Collector from a device and then delete it from the FortiEDR INVENTORY (page 73) if you would like to add another FortiEDR Collector.

When a user attempts to uninstall the Collector from a Windows OS device, he/she must supply the registration password.

In order to stop the FortiEDR service from running on a Windows OS device, enter the following command:

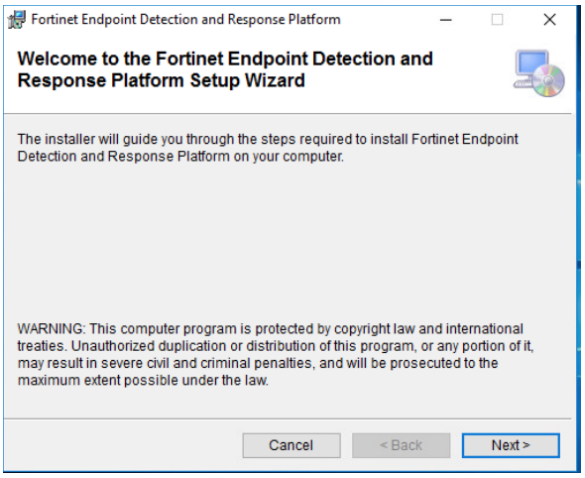
C:\Program Files\Fortinet\FortiEDR\ ➔ NsIoCollectorService.exe --stop and then provide the registration password in the pop-up windows.

Installing a FortiEDR Collector on Windows

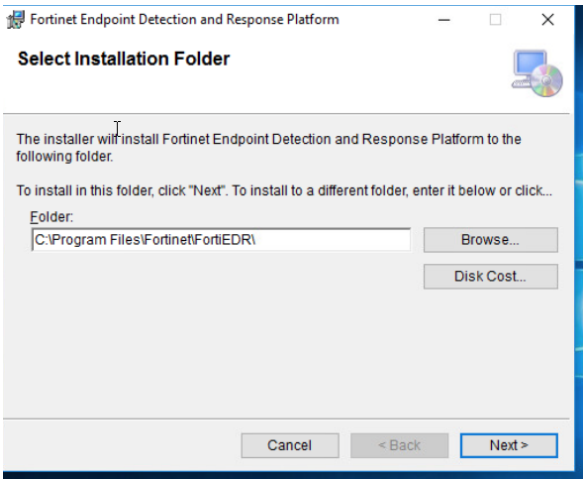
To install a FortiEDR Collector on Windows:

1. 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.

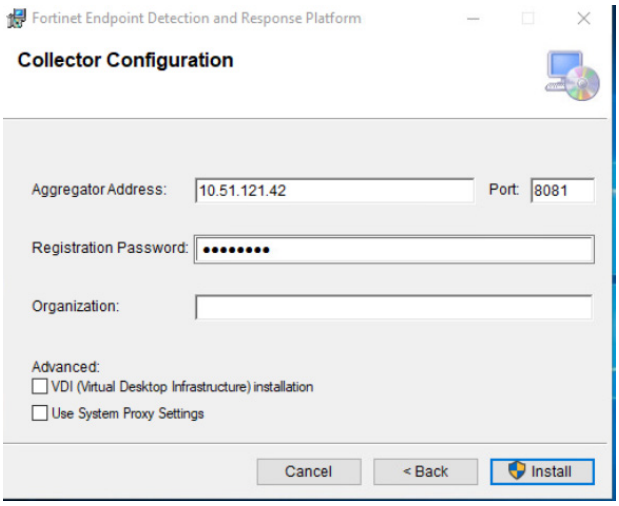
   The FortiEDR Collector setup wizard launches, as shown below:



2. Click **Next**. The following displays:



3. Leave the default FortiEDR Collector installation folder or change it as necessary. Click **Next**. The following displays:



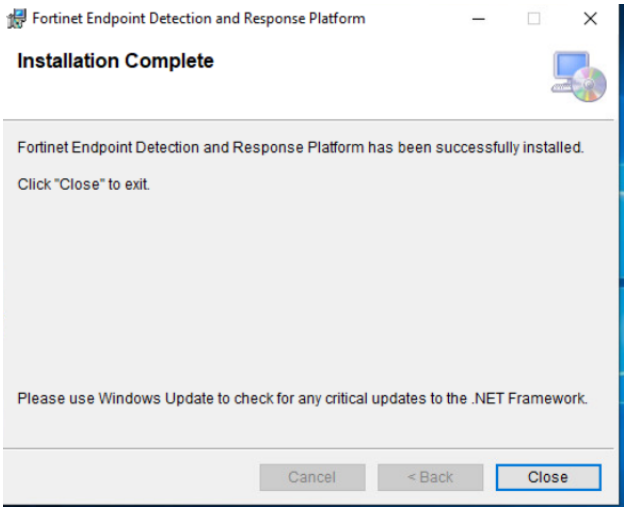
4. In the **Aggregator Address** field, specify the FortiEDR Aggregator domain name or IP address.
5. In the **Port** field, specify the FortiEDR Aggregator port (8081).

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

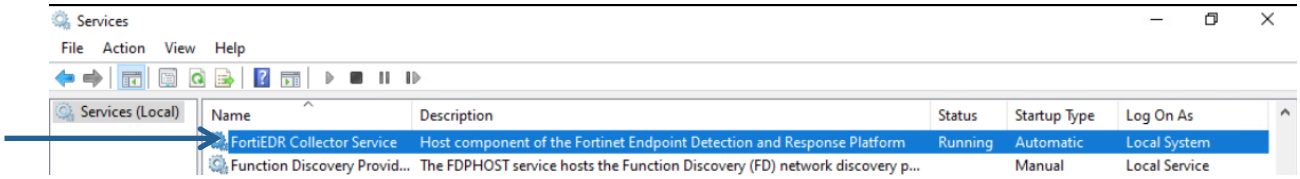
6. In the **Registration Password** field, enter the device registration password that you defined, as described on page 30.
7. For a multi-organization FortiEDR system, enter the name of the organization in the **Organization** field. For more details, see the *Collector Registration* section on page 184.

   If you are installing the Collector on a VDI environment, check the **VDI** checkbox. For more details, you may refer to the *Working with FortiEDR on VDI Environments* section on page 48.
8. 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 >**).
9. Click **Next** twice to start the installation. Windows may possibly display a message requesting that you confirm the installation. Please do so.

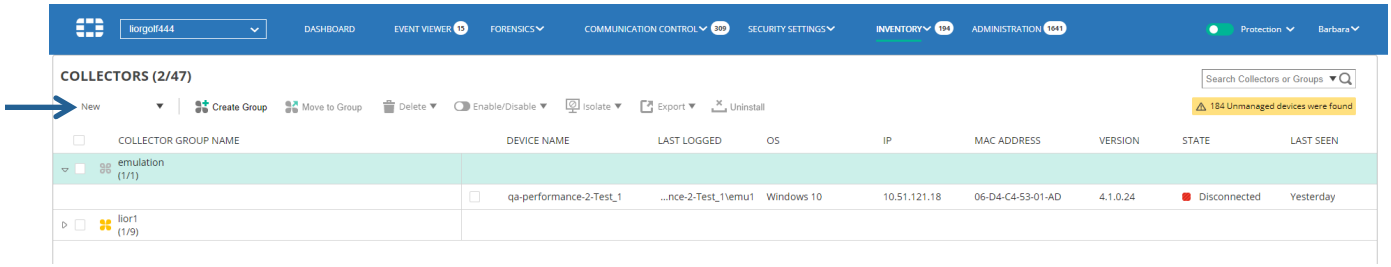
10. After the installation of the FortiEDR Collector has been successfully completed, the following window displays:



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



11. Verify that the FortiEDR Collector details are listed in the **INVENTORY** tab of the FortiEDR Central Manager console (page 68). Select the **New** filter to display a list of newly registered FortiEDR Collectors, as shown below:

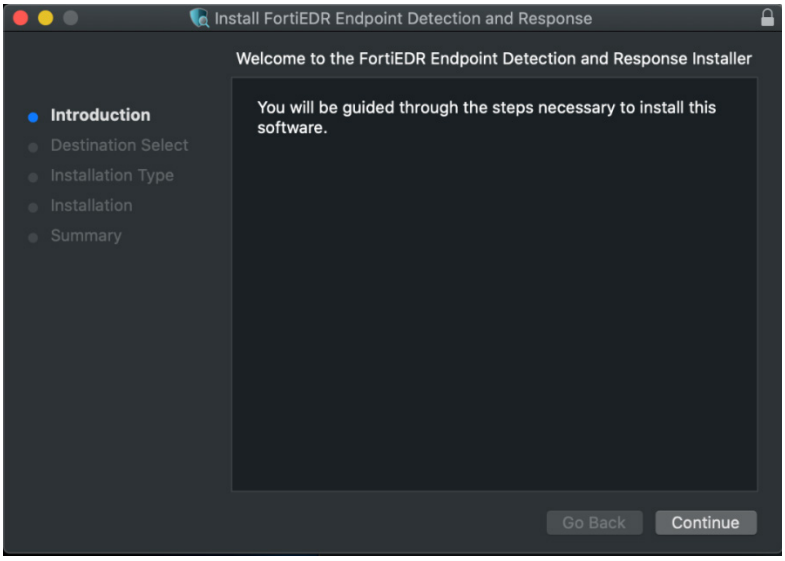


Installing a FortiEDR Collector on an Mac Operating System

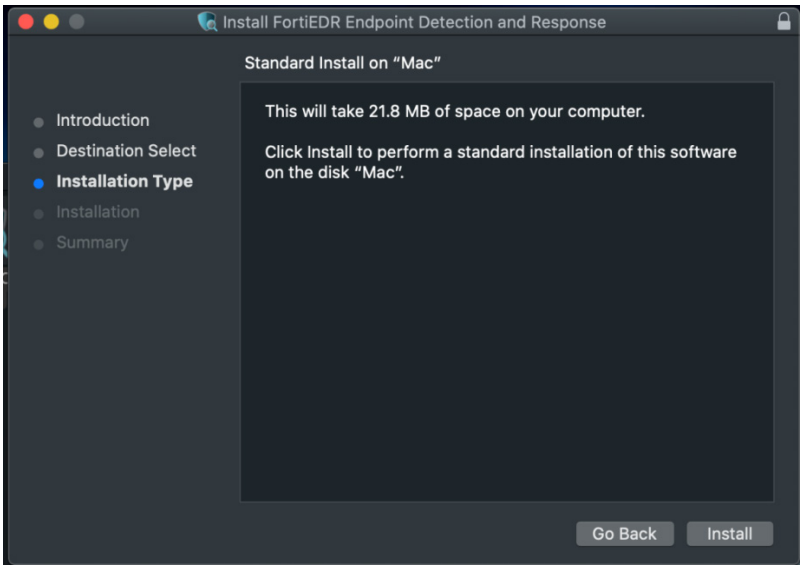
To install a FortiEDR Collector on an Mac operating system:

1. Double-click the *.dmg file named **FortiEDRCollectorInstallerOSX_1.3.0.xxx.dmg**. The following window displays:

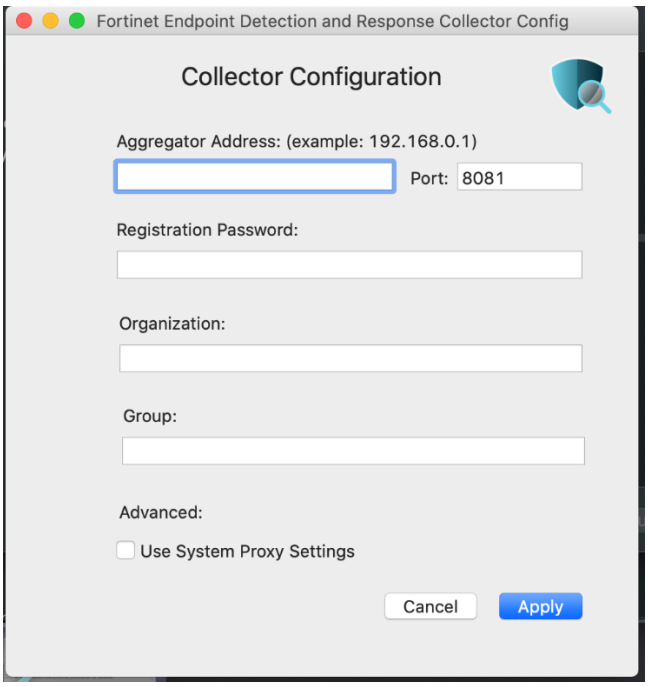
2. Double-click the *.pkg file named **FortiEDRCollectorInstallerOSX_1.3.0.xxx.pkg**. The following window displays:



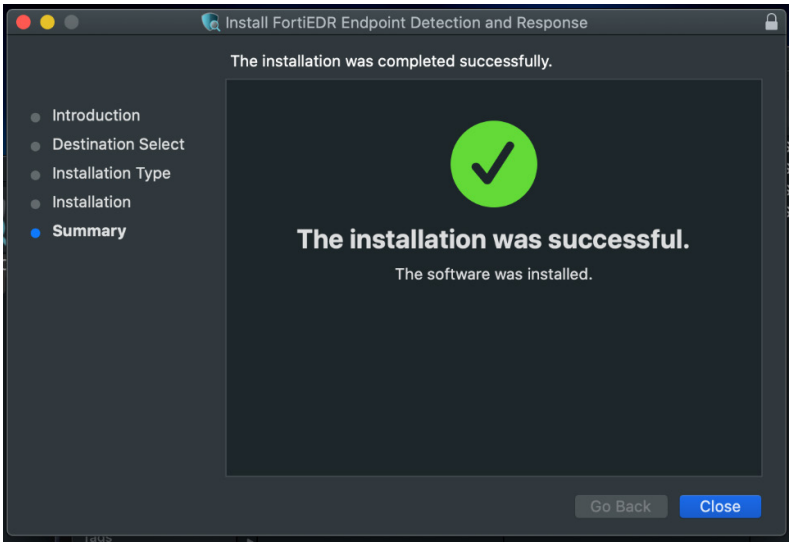
3. Click **Continue**.
4. Select the destination disk and click **Continue**. The following window displays:



5. Specify the installation location and click **Install**. The following window displays:



6. 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.
7. In the **Registration Password** field, enter the registration password, as described on page 30.
8. 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).
9. 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**).
10. Click **Apply**. The following window displays:



11. Click **Close**.

Installing a FortiEDR Collector on Linux

To install a FortiEDR Collector on Linux:

1. Run the FortiEDR Collector installation file for 64-bit servers using the following command:
   - CentOS:
     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 FortiEDRCollectorInstaller_Ubuntu-3.1.0-74.deb.
2. After the installation is completed, run the following:
   `sudo /opt/FortiEDRCollector/scripts/fortiedrconfig.sh`
3. Specify the FortiEDR Aggregator domain name or IP address.
4. Enter the FortiEDR Aggregator port information (usually 8081).
5. For a multi-tenant setup, enter the organization. Otherwise, leave the organization empty.
6. Enter Collector Group information or leave empty to be registered to the default Collector Group.
7. Enter the device registration password, which is described on page 30.
8. At the **Do you want to connect via proxy (Y/N)?** prompt, type `Y` if your setup includes a web proxy. For more details, see page 38.

Automated FortiEDR Collector Deployment on Windows

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

To deploy a FortiEDR 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
   ```

   Note –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 72) and will not start operating until the after the device is rebooted.

   Note – 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. If your software distribution system does not allow the addition of specific parameters to the command, you can use the provided **FortiEDRCollectorSilentInstallerGenerator** utility to create a custom FortiEDR Collector installation package with the required IP address and password already embedded inside. This file is located in the FortiEDR Collector installation folder. For more details, see the *Creating a Custom FortiEDR Installer* section on page 46.

Automated FortiEDR Collector Deployment on Mac

To deploy a FortiEDR Collector via a command line:

1. Run the following command line to generate the settings file:

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

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

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

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

   - If the Collector should be part of a designated Collector Group, use `--group '[GROUP]'`.
   - For a multi-tenant setup, the organization to which this device belongs to can be added using `--organization '[ORGANIZATION]'`.
   - If a web proxy is being used to filter requests in this device's network, use `--useProxy '1'`.

   The following is an example that includes all optional parameters:

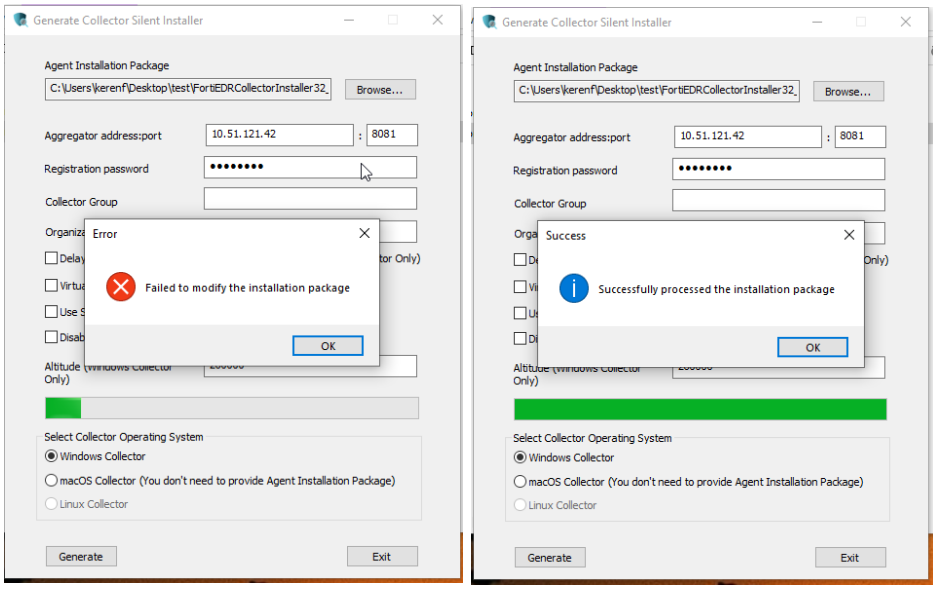
   ```
   ./CustomBootstrapGenerator --aggregator [IP] --password [PASSWORD] --useProxy
   '1' --organization '[ORGANIZATION]' --group '[GROUP]' > CustomerBootstrap.jsn
   ```

Creating a Custom FortiEDR Installer for Windows

Creating a custom installer for your customers enables the swift deployment of FortiEDR Collectors into your environment.

Before you create a custom installer, review the guidelines below:

- When creating a custom installation file, the Silent Installer Generator overwrites its source files. Therefore, be sure to create a copy of the MSI files **before** running the Silent Installer Generator.
- The Silent Installer Generator can create 32-bit and 64-bit MSI installers.
- The Silent Installer Generator requires empty fields. The target MSI files must not have been previously modified. An error displays if the configurator cannot set the parameters, as shown in the *Failed* message below:



Preparing the Files

Before you begin, verify that you have the following three files (version numbers may vary):

FortiEDRCollectorInstaller32_4.1.0.49.MSI
FortiEDRCollectorInstaller64_4.1.0.49.MSI
FortiEDRCollectorSilentInstallerGenerator_4.1.0.49.exe

It is important that these files remain unaltered so that you can create new custom installers in the future.

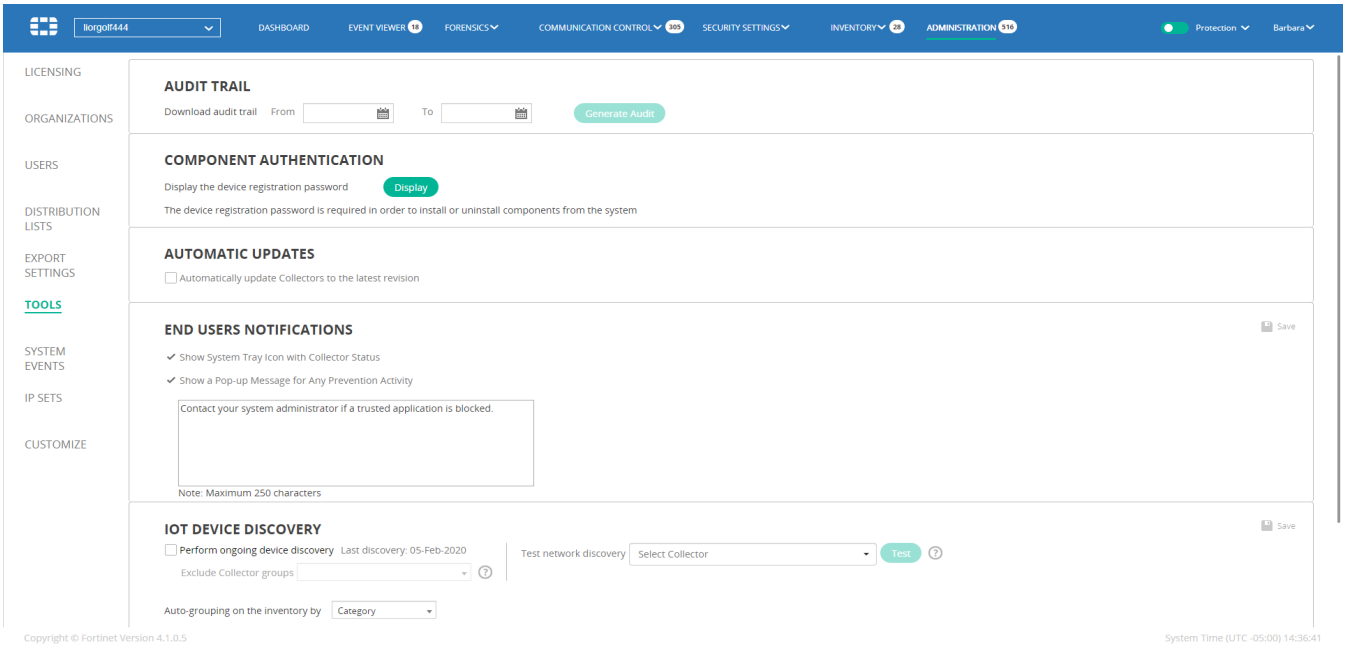
To prepare the files:

1. Create a new folder for the customer.
2. Copy the MSI files into this folder. Do **not** move the files into this folder.
3. Modify the name of the Collectors to include the organization's name, in order to easily locate the proper installer. For example, **ClientA_FortiEDRCollectorInstaller64_x.x.x.xxx.MSI**.

Creating Custom Installers

To create a customer FortiEDR installer for Windows:

1. Open the Silent Installer Generator file (FortiEDRCollectorSilentInstallerGenerator_#.#.#.###.exe).
2. Click the Browse… button.
3. In the browser window, locate the copied MSI files that you prepared.
4. Select the first MSI file (FortiEDRCollectorInstaller32_x.x.x.xxx.MSI) and click Open.
5. Fill in the Aggregator DNS/address:port fields, as follows:
   - The Aggregator address is the FQDN for your console. For example, **crptoblkr.console.ensilo.com**.
   - Keep the default port 8081 unless otherwise directed.
6. Fill in the **Registration Password**. This is the password created for your customer's organization within your console. To locate this password:
   - Open the FortiEDR Management Console.
   - Click the **Administration** tab.
   - In the left pane, select **Tools**.



   - Click the green **Display** button under Component Authentication. The Device Registration Password window displays:

   - Copy the password shown.
7. **[Optional]** If you want the installer to automatically place the device within a designated Collector Group and/or Organization, fill in the **Collector Group** and/or **Organization** fields, respectively.

   Note – The **Collector Group** field is case sensitive. If the name entered does not match an existing Collector Group at the time of device registration, the device is placed in the default Collector Group.

   If you are working with large groups of Collectors, you may want to create a custom installer for each group within the organization.

Alternatively, you can modify the default Collector Group before deployment so that all new Collectors go into the designated group, and then change the default to the next group. If you select this method, be aware that any Collectors that have been deleted, but not uninstalled from the device, are re-registered into the default group if they reconnect.

8. [Optional] If you want the installer to automatically place the device within a designated organization, fill in the Organization field.
9. [Optional] If you use a web proxy to filter requests in this device's network, then check the Use System Proxy Settings checkbox.
10. Disregard all other options unless directed to do so by Fortinet Support.
11. Repeat this procedure for the second MSI installer (**FortiEDRCollectorInstaller64_x.x.x.xxx.MSI**) in your customer folder.

Creating a Custom FortiEDR Installer for MAC

To create a custom installer for MAC, the same tool can be used.

To create a custom installer for MAC:

1. On a Windows system, run the FortiEDRCollectorSilentInstallerGenerator_3.1.0.159.exe file.
2. Click the MacOS Collector radio button.
3. Fill in the Aggregator IP or DNS Name and Port.
4. Fill in the registration password for the organization in which the Collector is to be installed.
5. (Optional) Fill in the Organization and Group.

   Note – This is case sensitive and must be spelled correctly. Leave blank is not installing in a custom organization.
6. Click Generate.

   Note – There is no need to browse and select the current installer, as is done for Windows.

   After clicking the **Generate** button, a browse window opens in which you select the location of the settings file.

When clicking **Save**, a *.jsn file is created in the specified location, which includes the preferred settings. At that point, you should:

1. Copy the settings file to the MacOS system you want to install in the following location: **/tmp/.CollectorBootstrap.jsn**.
2. Run the following command 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**, you should use the following command:

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

Working with FortiEDR on VDI Environments

The FortiEDR Collector should be installed on the VMware Horizon or Citrix XenDesktop master image only.

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 on page 40.

In installations on VMware Horizon-based environments, 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.

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.

IMPORTANT – 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.

Working with FortiEDR on VDI Environments for Citrix XenDesktop VDI or XenApp

The FortiEDR Collector should be installed on the Citrix XenDesktop/XenApp master images to ensure that the Citrix virtual environment is protected. It is also recommend to install the Collector on the Windows servers that runs 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 on page 40.

In installations on Citrix environments, there is no need to generate Collector groups in the user interface. Any newly generated virtual desktop or XenApp Server is automatically assigned to the default VDI Collectors group. Upon first user login to the virtual desktop/XenApp server, FortiEDR automatically generates a Collector group that corresponds with the respective pool name, as specified in Citrix delivery group configuration. Any Collector that is installed on a virtual desktop/XenApp server that is part of this pool is automatically assigned from the default VDI Collectors group to the corresponding Collector group. In effect, Collector groups in the FortiEDR user interface are a copy of the virtual machines' pool on Citrix delivery group configuration.

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/XenApp server is automatically and immediately protected by a unique instance of the FortiEDR Collector.

IMPORTANT – 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 a FortiEDR Collector

Uninstalling a FortiEDR Collector can be performed using the following methods:

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

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

Linux

The Collector should be stopped before running the uninstall command.

To start or stop the Collector:

- CentOS 6, CentOS 7 and Ubuntu:

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

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

  For example: `/ opt/FortiEDRCollector/control.sh --stop 12345678`

To check the status of the Collector:

- CentOS 6, CentOS 7 and Ubuntu:

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

To uninstall the Collector on Linux:

Before uninstalling, the Collector must first be stopped using its password. Then, run the following:

- CentOS:
  - rpm -qa | grep fortiedr | xargs rpm –e

    –OR–
  - yum remove <package name>
- Ubuntu:
  - dpkg --purge fortedricollectorinstaller

Mac (Version 2.6.3)

To uninstall the Collector on Mac:

- sudo /Library/FortiEDR/fortiedr_uninstaller.sh REGISTRATION PASSWORD

  Note – 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'.`

Windows

To uninstall the Collector on Windows:

- Run the following command as administrator:

  ```
  msiexec /x FortiEDRCollectorInstaller_X.msi /qn UPWD= REGPWD RMCONFIG=1
  ```

  Replace `REGPWD` with the correct registration password that was used for the install.

Upgrading FortiEDR Components

This section describes how to upgrade the components in the FortiEDR system.

Upgrading to a newer build number (major.minor.patch.build) can be done in any order. However, upgrading to newer major/minor versions (major.minor.patch.build) should be done top-down in the following order:

- FortiEDR Threat-hunting Repository
- FortiEDR Central Manager Server and FortiEDR Aggregator
- FortiEDR Cores
- FortiEDR Collectors

Upgrading the Central Manager

The required upgrade file is provided to you by Fortinet. Use it to perform the procedure below. If both the Central Manager and the Aggregator are installed on the same machine, you only need to perform this procedure once to upgrade both components.

To upgrade the Central Manager:

1. Copy the **FortiEDRInstaller_x.x.x.xxx.x** file to the Central Manager machine. You can place the file anywhere on the Linux machine. For example, **FortiEDRInstaller_2.0.0.330.x**.
2. Change the **chmod 755** permission and the **pathc** name in order to enable you to run the upgrade, as shown below:

   ```
   [root@dan ~]# chmod 755 FortiEDRPatch_2.0.0.330.x
   ```

3. Run the upgrade, as shown below:

   ```
   [root@dan ~]# ./FortiEDRPatch_2.0.0.330.x
   ```

4. Wait for the upgrade to complete, as shown below:

   ```
   FortiEDR patch 2.0.0.330 finished
   [root@dan ~]#
   ```

Upgrading the Aggregator

The procedure for upgrading the Aggregator is the same as that for updating the Central Manager. You only need to perform the procedure a second time if the Aggregator is installed on a different machine than the Central Manager.

For more details, you may refer to the *Upgrading the Central Manager* section on page 50.

Upgrading the Core

To upgrade 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_3.1.1.90.x**.
2. Change the **chmod 755** permission and the **patch** name in order to enable you to run the upgrade, as shown below:

   ```
   [root@dan ~]# chmod 755 FortiEDRCoreInstaller_3.1.1.90.x
   ```

3. Run the upgrade, as shown below:

   ```
   [root@dan ~]# ./ FortiEDRCoreInstaller_3.1.1.90.x
   ```

4. Wait for the upgrade to complete, as shown below:

   ```
   FortiEDR patch 3.1.1.90 finished
   [root@dan ~]#
   ```

Upgrading the Collector

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

- Using the **Load Content** option, as described on page 32.
- As described in the procedure below.

You can use whichever method you prefer.

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

Windows

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

Linux

1. Copy the installer file to the Collector machine (either CentOS FortiEDRCollectorInstaller_%Linux_distribution%-%version_number%.x86_64.rpm or Ubuntu FortiEDRCollectorInstaller_Ubuntu-%version_number%.deb).
2. Stop the Collector using its password.
3. Do one of the following:
   - CentOS: Run sudo yum install FortiEDRCollectorInstaller_%Linux_distribution%-%version_number%.x86_64.rpm.
   - Ubuntu: Run sudo apt-get install FortiEDRCollectorInstaller_Ubuntu-%version_number%.deb.
4. Answer **y** when asked if you want to upgrade.

Chapter 3 – SECURITY SETTINGS

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

Introducing FortiEDR Security Policies

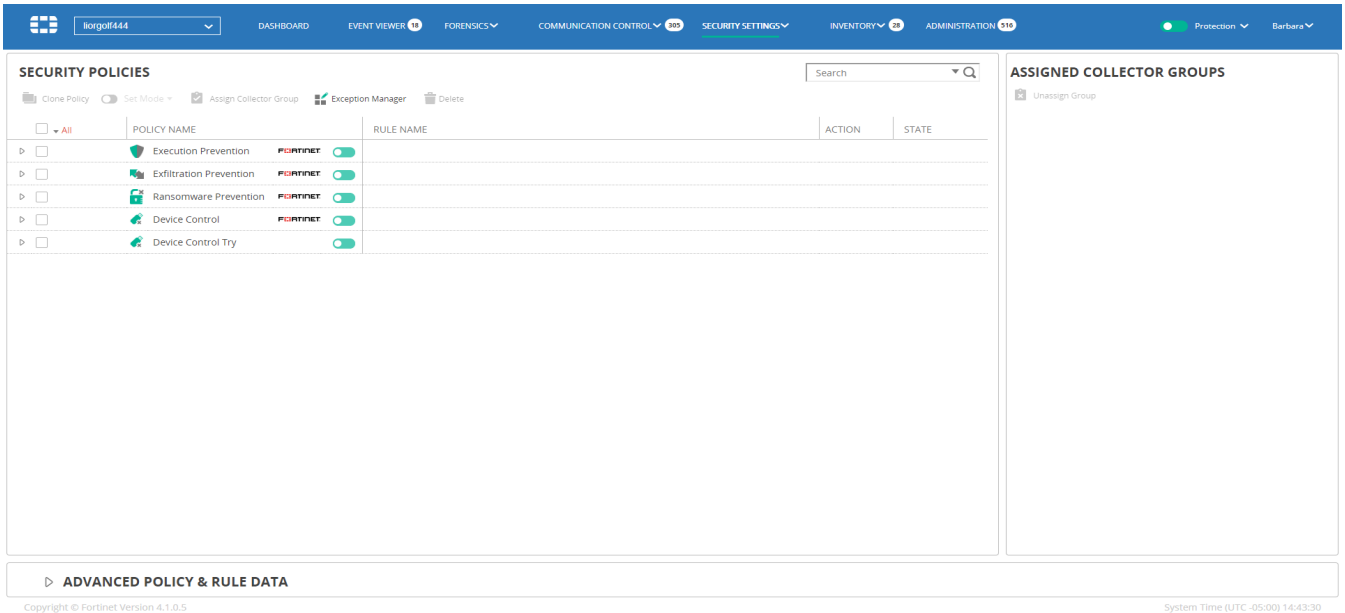
The most powerful proprietary feature of the FortiEDR platform is its predefined and configurable security policies.

Exfiltration Prevention/Ransomware Prevention/Execution Prevention/Device Control

FortiEDR provides the following out-of-the-box policies:

- **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.
- **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.

Note – You will receive one or all policies, depending on your FortiEDR license.



To access this page, click the down arrow next to **SECURITY SETTINGS** and then select **Security Policies**.

FortiEDR security policies come with multiple highly intelligent rules that enforce them.

The Exfiltration Prevention, Ransomware Prevention, Device Control and Execution Prevention security policies can run simultaneously.

Note – When multiple security policies are used, they do not generate duplicate events:

- Exfiltration Prevention rule violation is detected when there is a connection establishment attempt.
- Ransomware rule violation is detected when there is an attempt to lock files or access their data (for example, by encrypting the data).
- Execution Prevention rule violation is detected when a malicious file is being executed by the user or by the operation system.
- Device Control rule violation is detected when there is an attempt to use a USB device, such as a mass storage device.

Thus, these security policies detect rule violations at different places and points in time in the operating system. Device control events are displayed under a dedicated **Device Control** filter in the Events page and are not listed as part of the **All** filter.

Protection or Simulation Mode

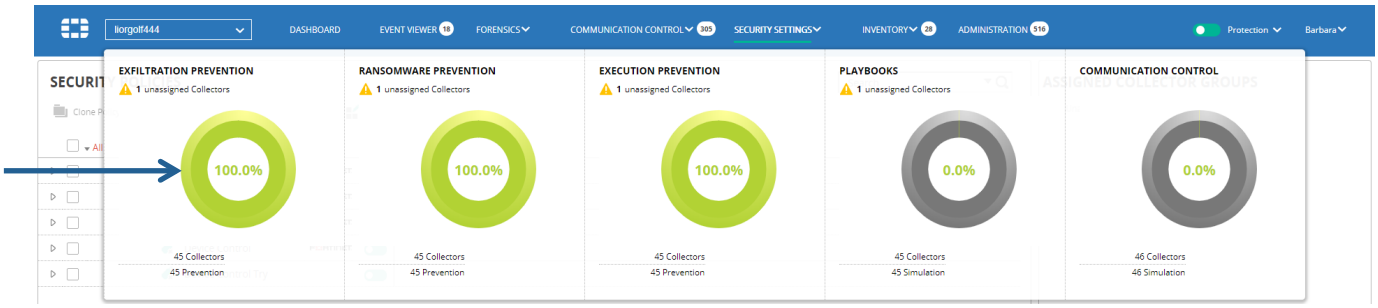
During an initial acquaintance period or at any time, you can decide that FortiEDR acts as either of the following:

- **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.

Note – 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.

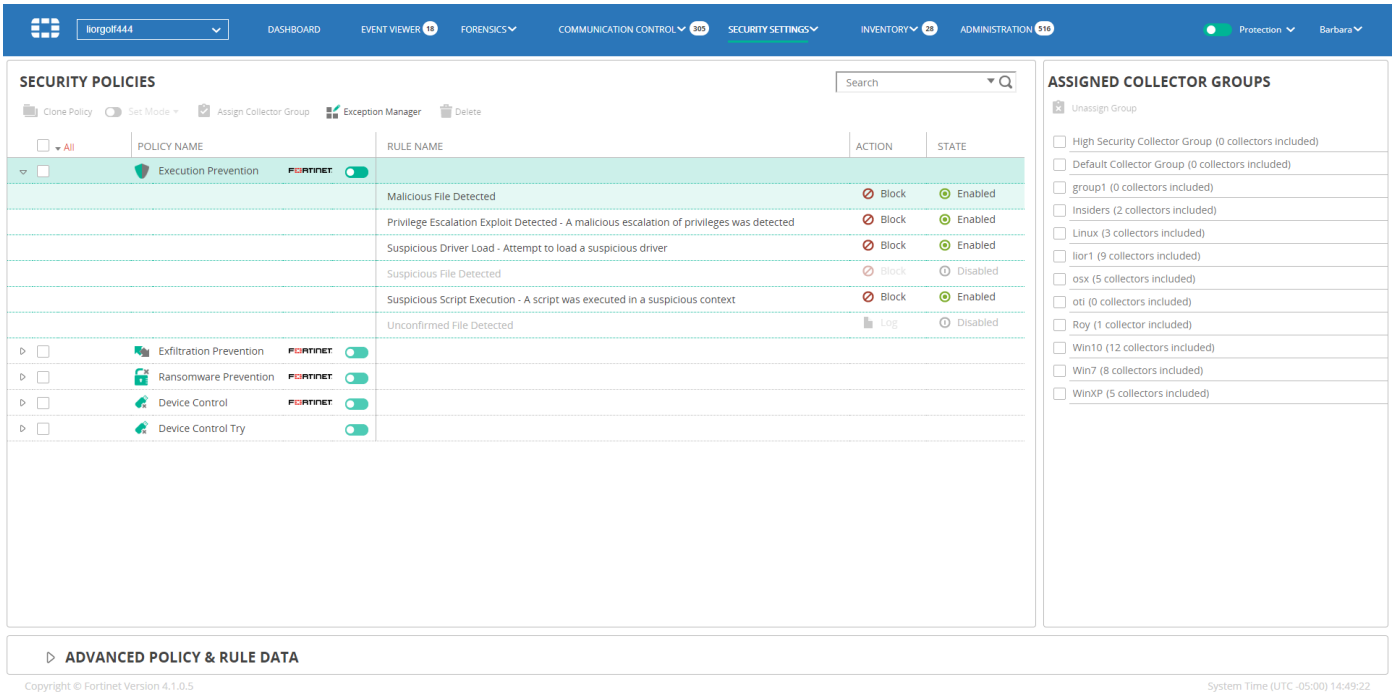
Use the **Protection/Simulation** slider at the far right of the window to enable the applicable mode, as shown below:

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**.



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.

Exfiltration prevention policies are marked with the icon, ransomware prevention policies are marked with the icon, execution prevention policies are marked with the icon and device control policies are marked with the icon.

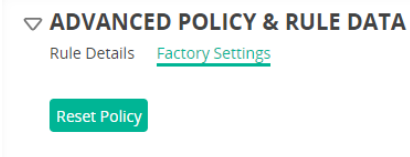
The following information is defined per security policy:

Note – Only the **ACTION** (described below) and the **STATE** (Enabled/Disabled) column of a rule can be changed by you.

- **POLICY NAME:** The policy name appears in the leftmost column. The policy name is defined when the policy is created. The name of the **Default Policy** cannot be changed.
- **RULE NAME:** FortiEDR's proprietary rules come predefined and are the primary component of FortiEDR's proprietary security solution. This column displays a short description for the purpose of this rule.

  Note – You can expand the **ADVANCED POLICY & RULES DATA** area at the bottom left of the window to display a more detailed description of what the rule does and how it works.
- **ACTION:** Specifies the action that is enforced when this rule is violated. You can change this field, as follows:
  - Block**:** When this policy is set to **Prevention** mode (page 56), the exfiltration attempt is blocked and a blocking event is generated. When this policy is set to **Simulation** mode, the outgoing connection attempt is **NOT** blocked and a simulated-blocking event is generated (this indicates that FortiEDR ***would have*** blocked the exfiltration if the policy had been set to **Prevention** mode).
  - Log**: Log.** The event is only logged regardless of whether the policy is set to Prevention or Simulation mode. The outgoing connection attempt is not blocked.
- **STATE:** (Enabled/Disabled) This option enables you to disable/enable this rule. FortiEDR's rules have been created as a result of extensive expertise and experience. Therefore, we do not recommend disabling any of them.

To reset a FortiEDR security policy to its out-of-the-box settings, click the **Reset Policy** button in the **ADVANCED POLICY & RULE DATA** section, as shown below:



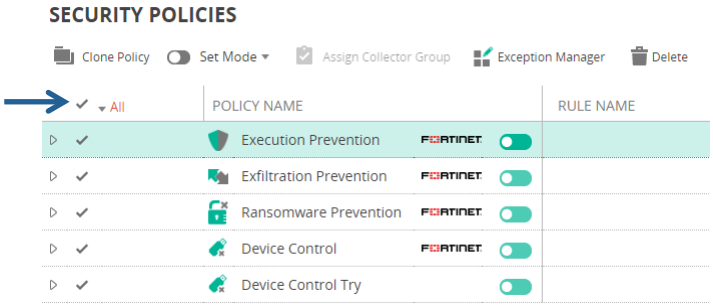
Setting a Security Policy's Prevention or Simulation Mode

Each FortiEDR security policy can be set to operate in one of the following modes:

- **Prevention:** FortiEDR enforces its active prevention policy that blocks all activity that violates relevant rules in the FortiEDR security policy.
- **Simulation/Notification Only:** FortiEDR logs and alerts only violations of FortiEDR security policy. The events are shown in the FortiEDR Central Manager. In this mode, FortiEDR does not block malicious activity. This is the default mode of all FortiEDR security policies out of the box. You can decide to use this mode during an initial acquaintance period or at any time.

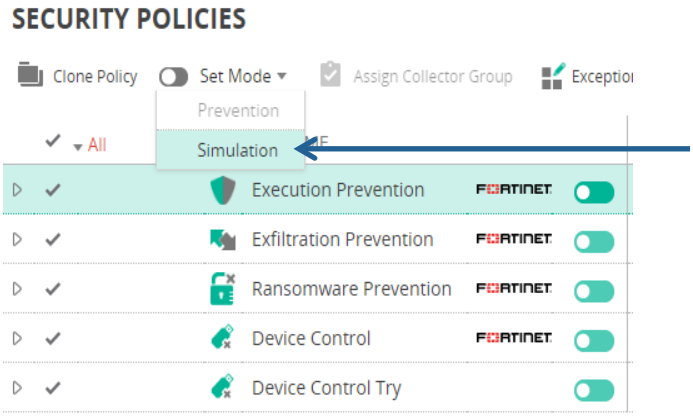
To set a security policy to Prevention or Simulation mode:

1. Select the checkbox of the security policy to be configured. Alternatively, you can select the top-left checkbox to configure all security policies at once.



2. You can now either:
   - Set mode **:** Click the **Set Mode** button 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:

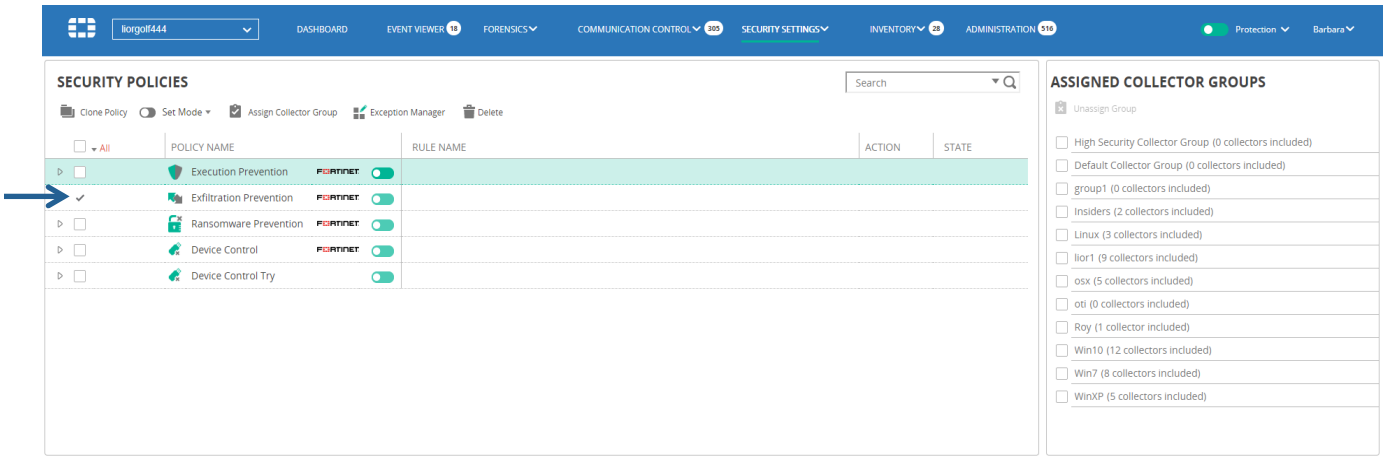


Creating a New Security Policy

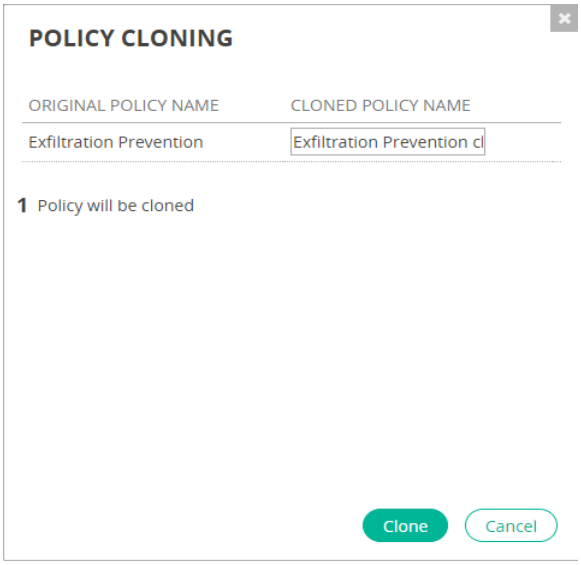
A new security policy can be created by cloning an existing policy, as described below. New security policies are only needed if you are going to assign different policies to different Collector Groups. Otherwise, you can simply modify one of the default policies that are provided out-of-the-box and 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.



2. Select the **Clone Policy** button. The following window displays:



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 below.

Assigning a Security Policy to a Collector Group

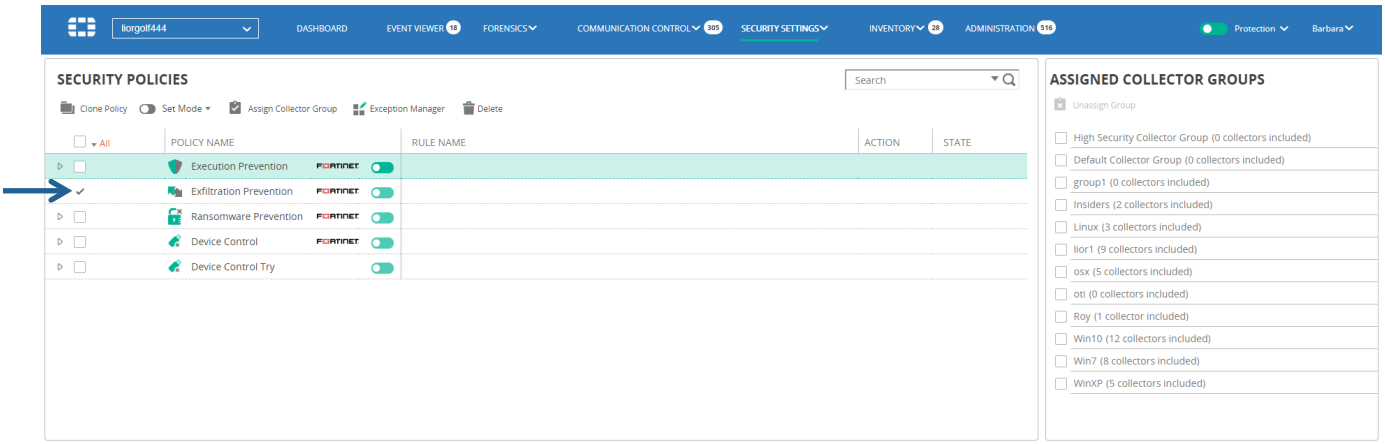
By default, a security policy protects the FortiEDR Collectors that belong to that Collector Group. A security policy can be assigned to more than one Collector Group. Multiple security policies can be assigned to each Collector Group.

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 events will be triggered in response to both policies, producing duplicated events.

You may refer to page 72 for a description of how to define a new Collector Group in the **INVENTORY** tab.

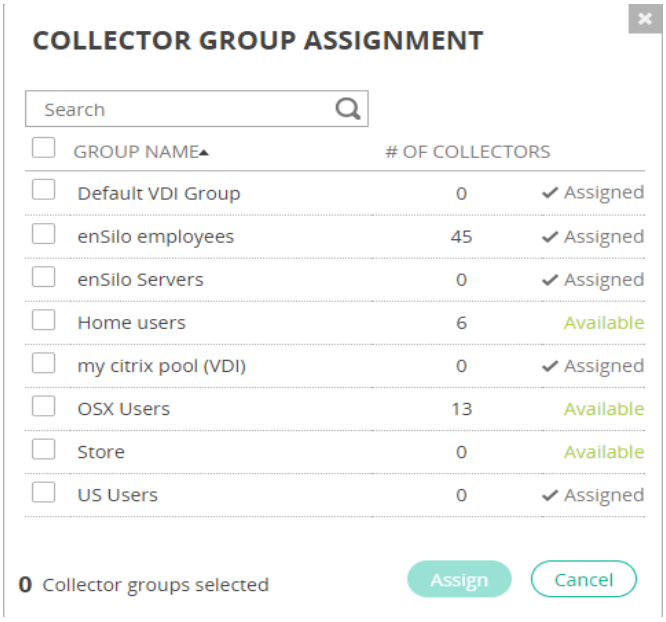
To assign a security policy to protect a Collector Group:

1. In the **SECURITY POLICIES** page, select the name of the security policy to be assigned by clicking its checkbox.



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.



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

To delete a security policy:

- Select the policy's checkbox and then click the Delete button.

  Note – The Exfiltration Prevention, Ransomware Prevention, Device Control and Execution Prevention FortiEDR security policies provided out-of-the-box (FORTINET) cannot be deleted.

Playbook Policies

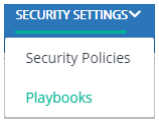
The FortiEDR Playbooks feature determines which automatic actions are triggered, based on the classification of an event (for details about event classification, see page 106). Playbook policies enable administrators to preconfigure the action(s) to be automatically executed according to an event's classification. Typically, Playbook policies only need be configured once, and can be modified thereafter, if needed. FortiEDR classifies each event into one of five categories described on page 93.

FortiEDR provides the following Playbook policy out of the box:

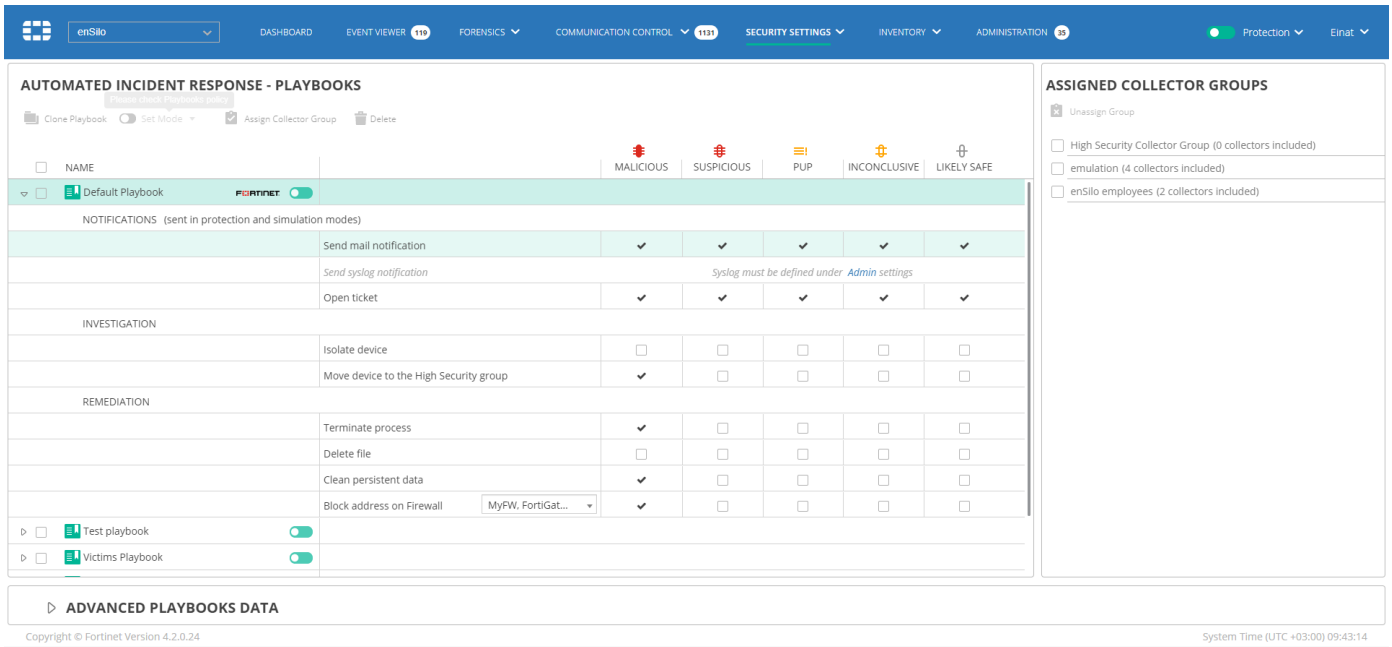
- **Default Playbook:** This Playbook policy specifies the default actions for the Collector Groups assigned to the policy. By default, all Collector Groups are assigned to this policy.

Automated Incident Response - Playbooks Page

The **AUTOMATED INCIDENT RESPONSE – PLAYBOOKS** page displays a row for each Playbook policy. To access this page, click the down arrow next to **SECURITY SETTINGS** and then select **Playbooks**.



Each Playbook policy row can be expanded to show the actions that it contains, as shown below:



You can drill down in a Playbook policy row to view the actions for that policy by clicking the ▷ icon.

Note – 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 FortiEDR support about how to add them.

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.

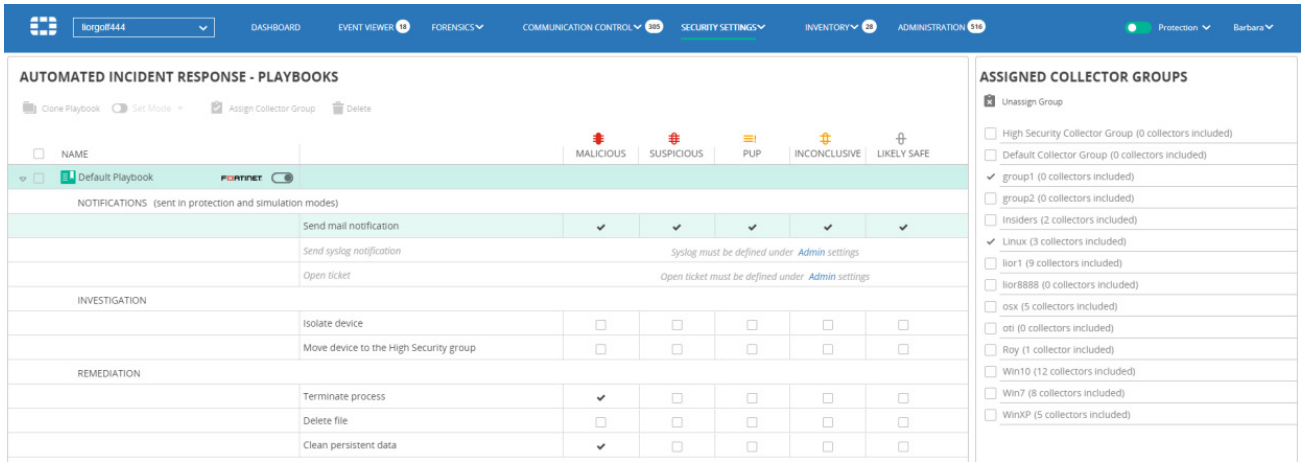
Note – When upgrading your FortiEDR system, all existing Collector Groups are automatically assigned to the Default Playbook policy.

Cloning a Playbook Policy

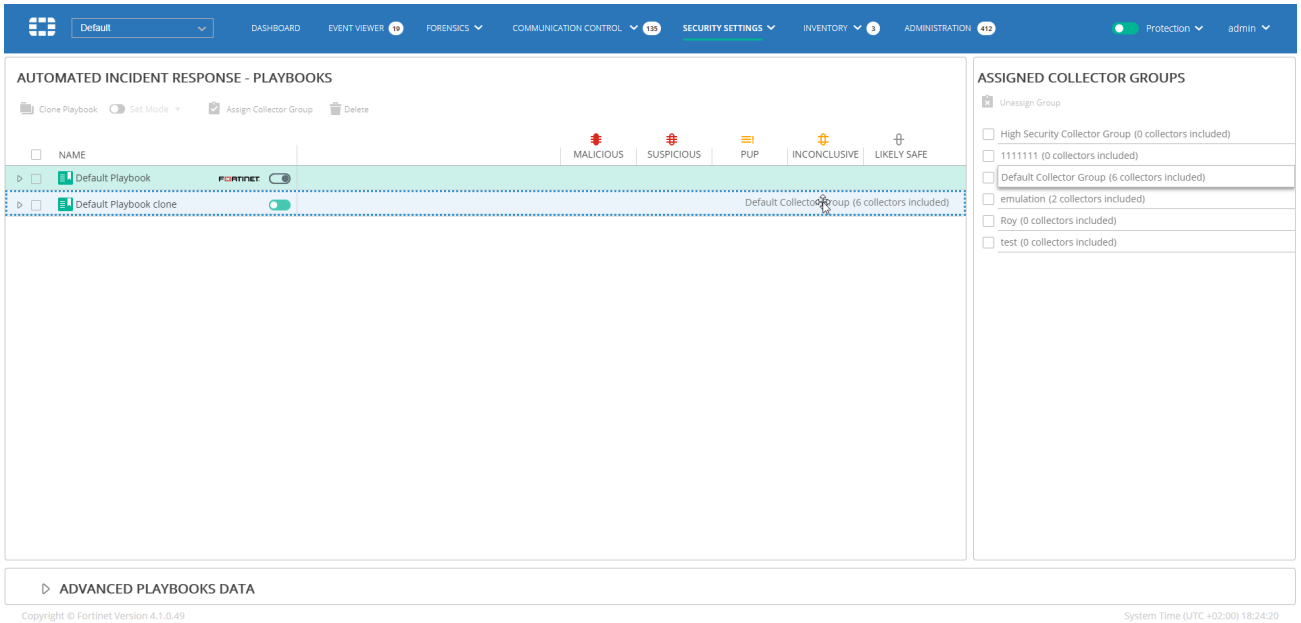
Cloning a Playbook policy unassigns the policy from one Collector Group and then reassigns it to a different Collector Group. A Collector Group can only be assigned to one Playbook policy.

To clone a 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:
   - 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.



- Click the 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:

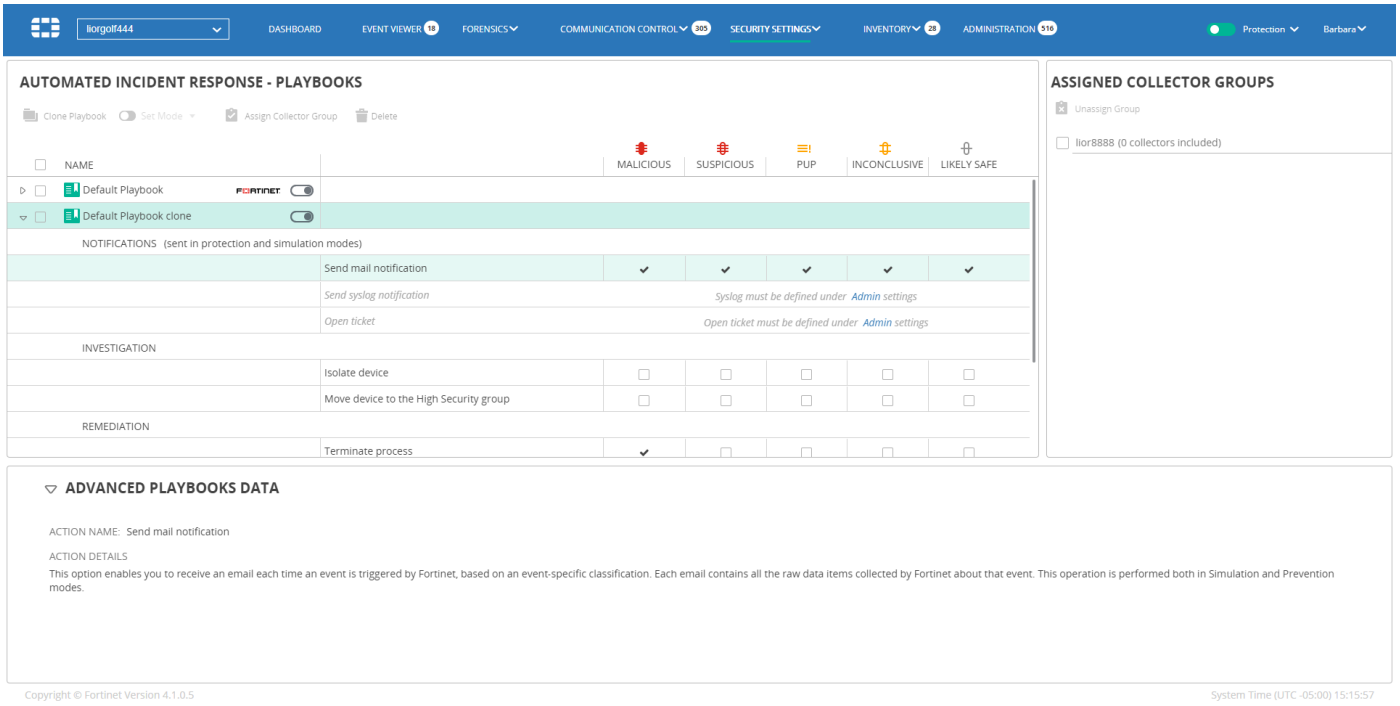


The following message displays.

Click **OK**.

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.



Playbook Policy Actions

Playbook policy actions are divided into the following types:

- **Notifications,** page 62
- **Investigation,** page 64
- **Remediation,** page 65

Each of these categories contains different types of actions that can be performed when an event is triggered.

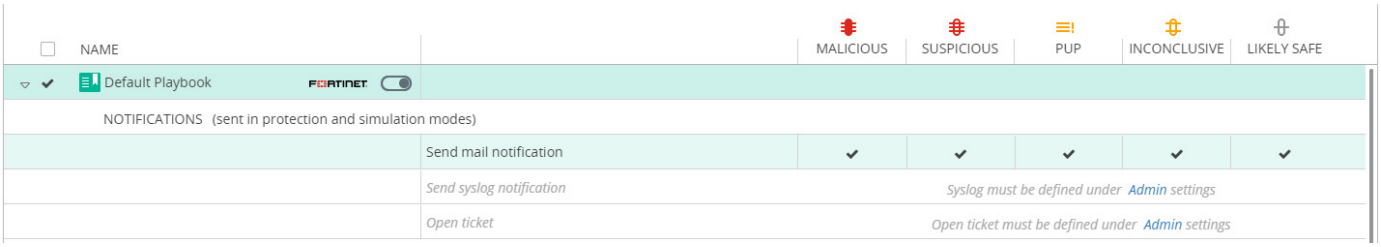
Notifications

Notification actions send a notification when a relevant 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

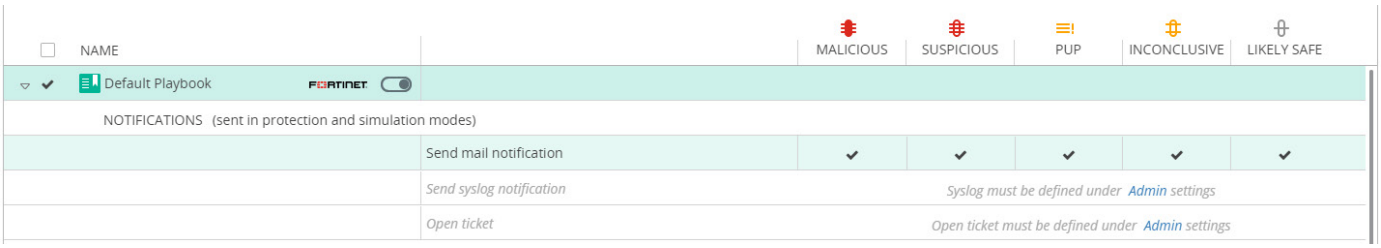
Each row under Notifications corresponds to a single type of notification (mail [email] notification, Syslog notification or Open Ticket notification). In the Notifications area, you configure each notification type to indicate whether or not it is to automatically send the relevant notification, once triggered by an event. By default, the Default Playbook policy is set to Simulation mode, and only email notifications are automatically enabled, as shown below:



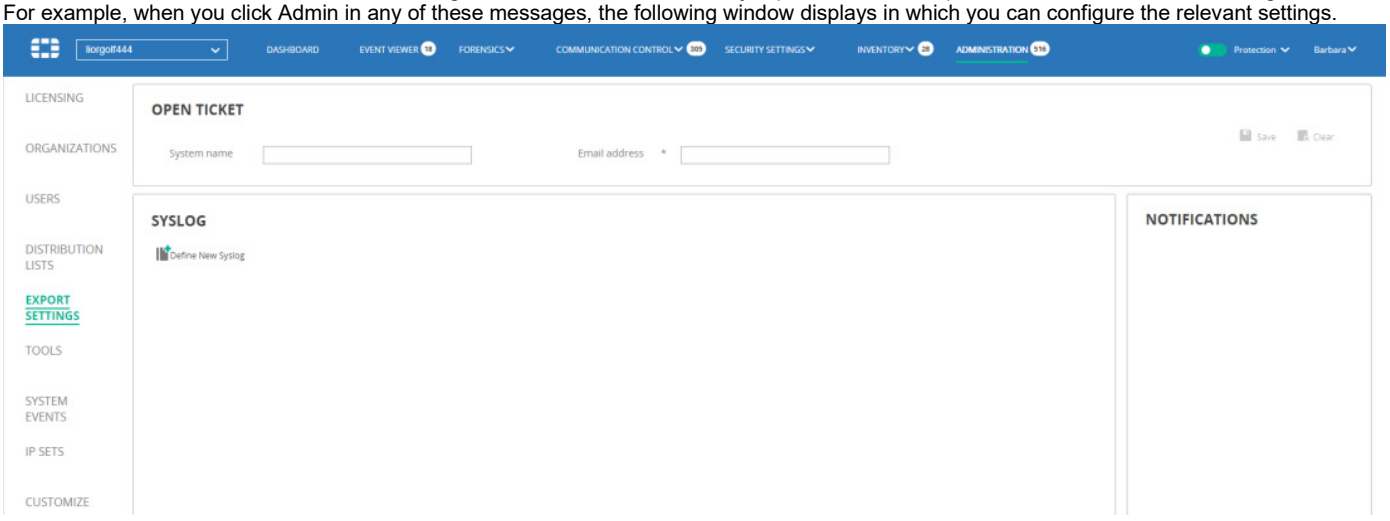
Note – Notification actions must be enabled in order to be implemented by a Playbook policy. If notifications are disabled, they are not implemented by the Playbook policy, even if that policy is configured to send notifications. See page 159 for more details.

The **Malicious**, **Suspicious**, **PUP**, **Inconclusive** and **Likely Safe** columns correspond to the possible classifications for an 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 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 event is triggered. **Syslog** and **Open Ticket** notifications work in the same way as Email notifications. For more details about classifications, see page 93.

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:



Note –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.



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.

Investigation actions can be one of the following types:

- Isolate Device, below
- Move Device to High Security Group, below

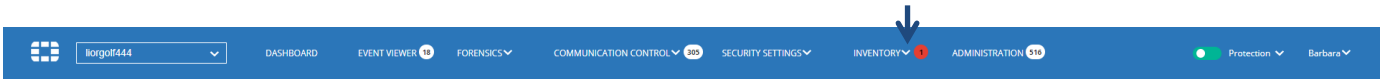
Isolate Device

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 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 incoming and outgoing communications.

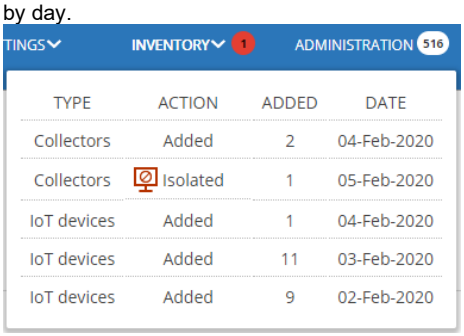
A checkmark ✔ in a classification column here means that the device is automatically isolated when an event is triggered with that classification.

Note – 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 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.



Move Device to High Security Group

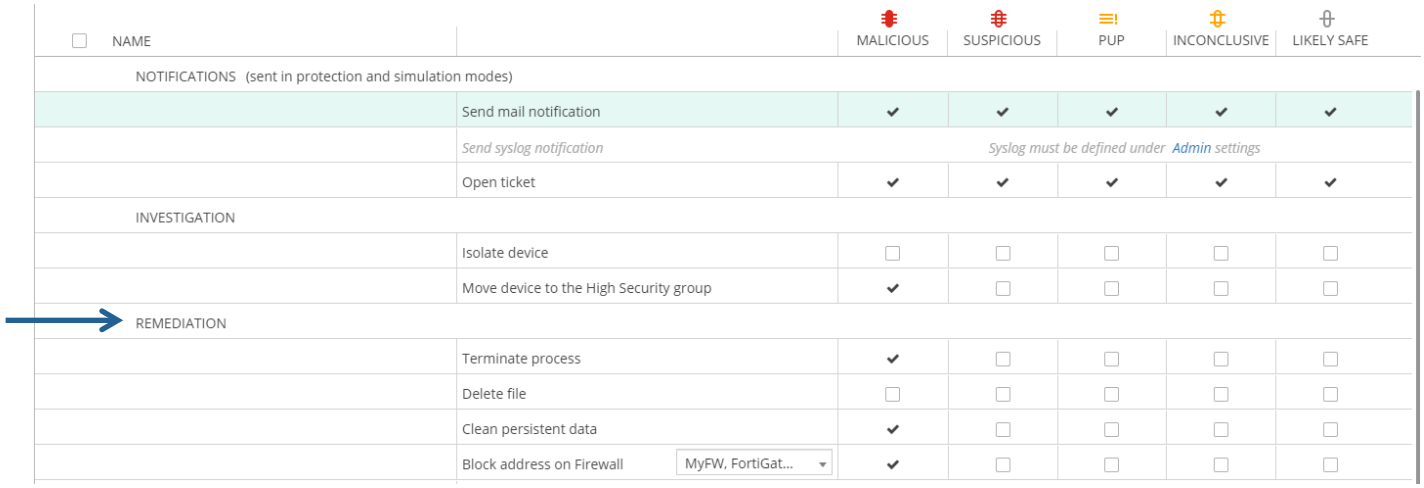
FortiEDR provides two default Collector Groups: the Default Collector Group and the High Security Collector Group. Both of these default Collector Groups are initially assigned to the Default Playbook policy, and cannot be deleted.

A checkmark ✔ in a classification column here means that the device is automatically moved (assigned) to the High Security Collector Group when an event is triggered that has that classification. This feature is useful when you want to mark Collectors that triggered malicious events.

Move device to High security group	✔	✔	✔	✔	☐

Remediation

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



Remediation actions can be one of the following types:

- Terminate Process, below
- Delete File, below
- Clean Persistent Data, below
- Block Address on Firewall, page 66

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 page 137.

A checkmark ✔ in a classification column here means that the affected process is automatically terminated on the device when an 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 page 137.

A checkmark ✔ in a classification column here means that the affected file is automatically removed on the device when an event is triggered that has that classification.

Clean Persistent Data

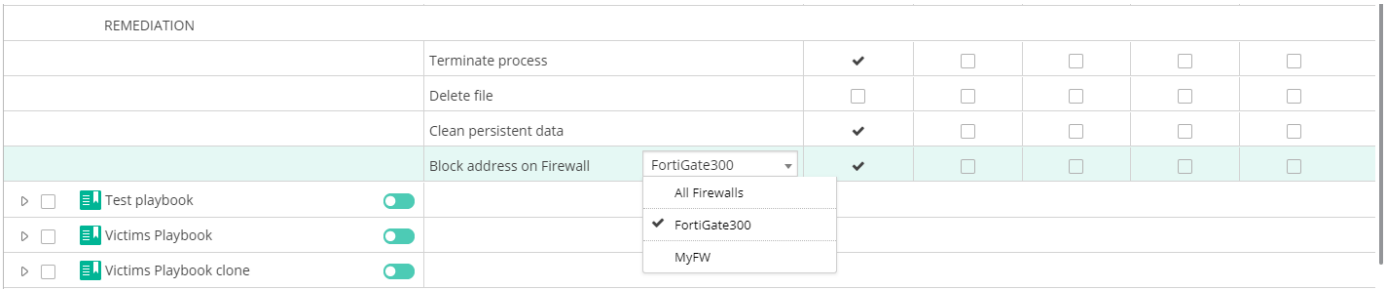
This action cleans the registry keys in Windows. This action can also be performed manually using the Forensics add-on, as described on page 137.

A checkmark ✔ in a classification column here means that the affected registry key is automatically cleaned on the device when an 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 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 page 175.

In the dropdown menu next to the action, you can specify which firewalls to block or select all of them, as shown below:



A checkmark ✔ in a **Classification** column means that communication with the affected destination is automatically blocked when an 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:

Note – 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).

Other Options in the Playbooks Tab

You can perform the following operations using the toolbar at the top of the tab:

- **Clone Policy:** Clones a Playbook policy, as described on page 60.
- **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 page 56.
- **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 page 58.
- **Delete:** Deletes a cloned Playbook policy. Default Playbook policies cannot be deleted.

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

Exceptions

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.

An exception can be made for a Collector Group (a specific one or for all) and a destination IP (specific or all). The event is then no longer triggered for that specific Collector Group or destination IP. This exception is added on 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 an 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.

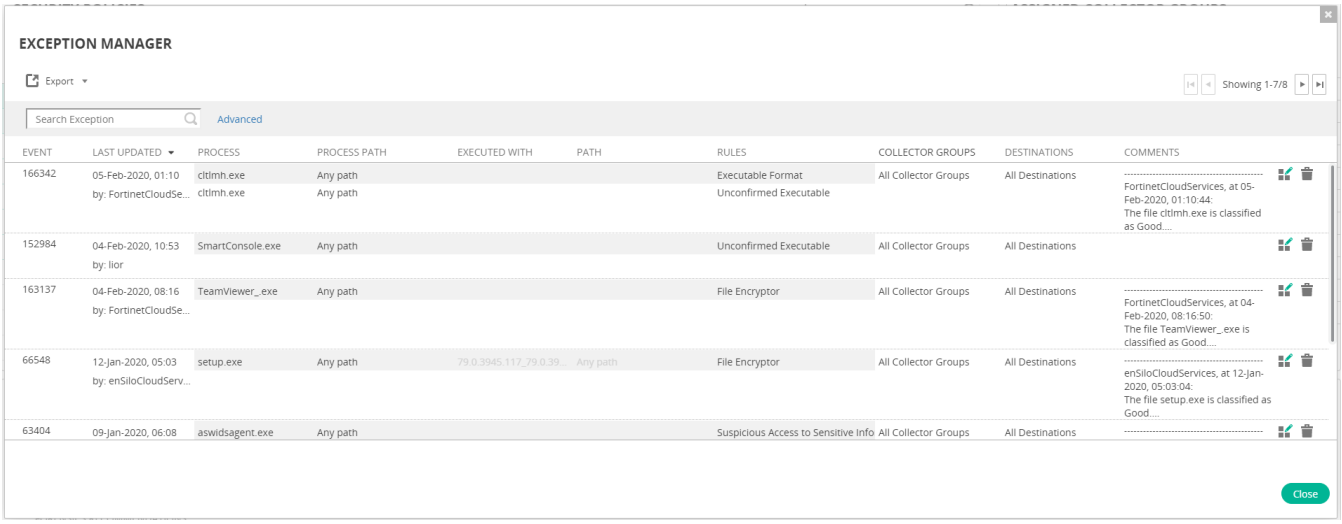
Any exception that you define applies to all policies.

Exceptions are created in the Event Viewer, as described on page 98.

Note –FCS may push an automated exception in cases where extended analysis and investigation of an event leads to its reclassification as Safe. This prevents the event from triggering again.
In such cases, the 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. In the **SECURITY POLICIES** page, click the Exception Manager button. The following window displays, showing the list of previously created exceptions:



2. To filter the exception list, click the **Advanced** button. The window displays various filter boxes at the top of the window, which you can use to filter the list by specific criteria.

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 Event Exceptions* on page 120.

Click the **Delete** button in an exception row to delete that exception.

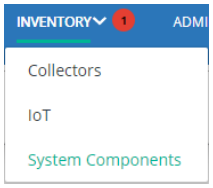
3. Click **Close** to exit the Exception Manager.

Chapter 4 – INVENTORY

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

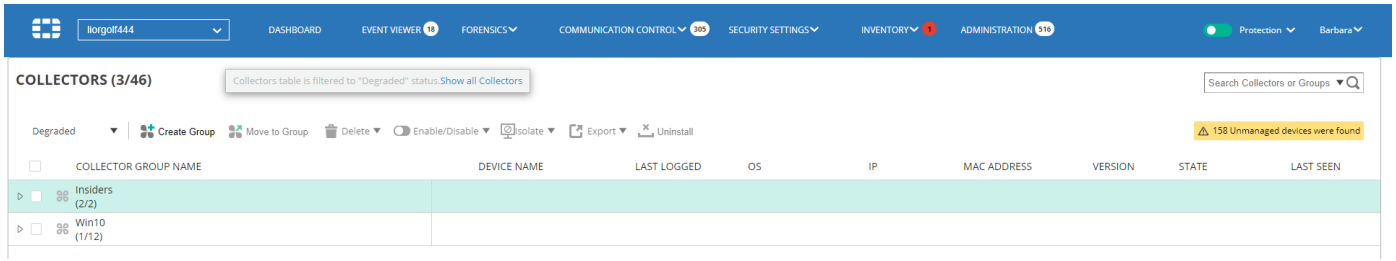
Introducing the Inventory

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.

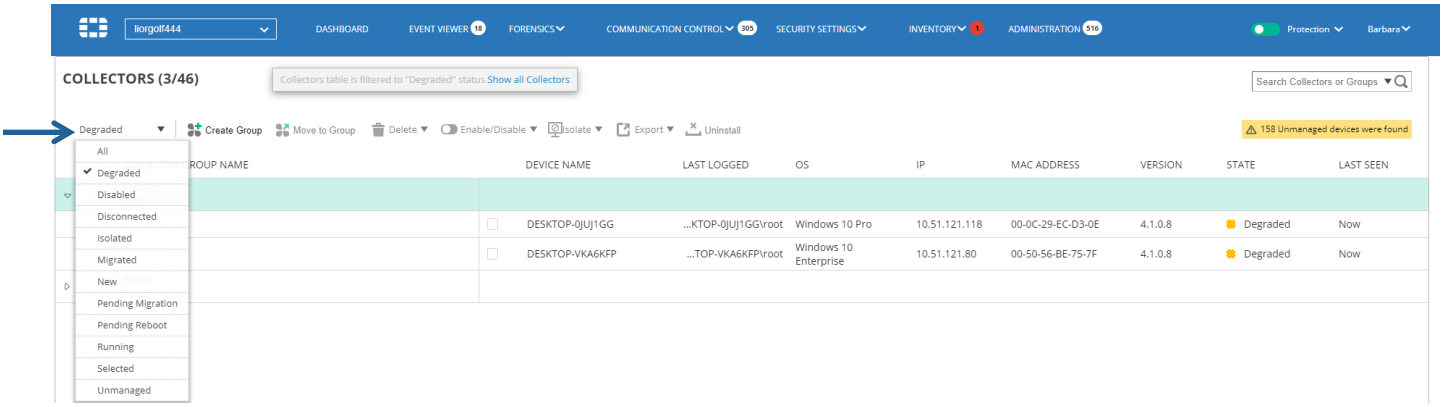


This view enables you to monitor system health and to define Collector Groups. If you have a large system with thousands of FortiEDR Collectors, it may take a few moments to populate this window.

By default, the **INVENTORY** tab and its various pages are filtered to display all the FortiEDR components that are degraded.



You can select to display all components that are 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:

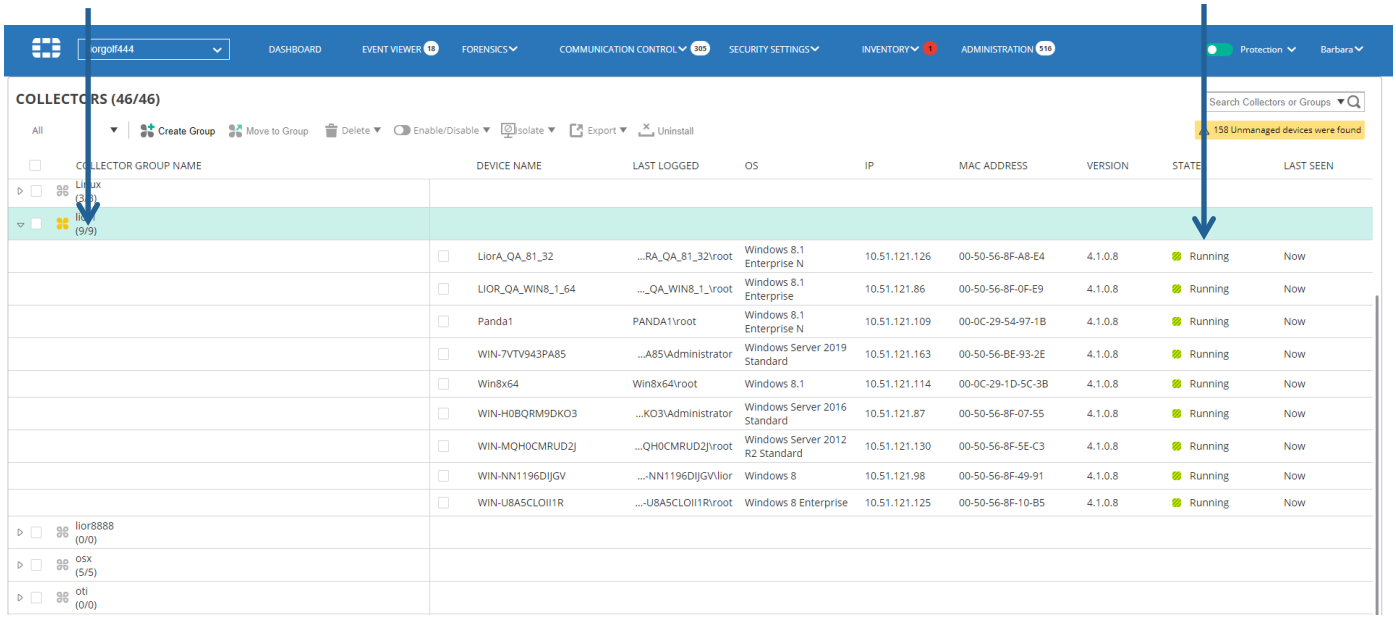


When a new FortiEDR Collector registers, an indicator displays on the **INVENTORY** tab.

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, 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 11/11, which means that there are 9 Collectors that are Running in a Collector Group containing **9** Collectors.



To export the list of FortiEDR components:

- Use the Export button and select Excel or **PDF**.

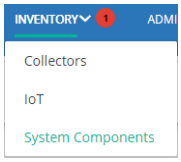
Uninstalling a Collector

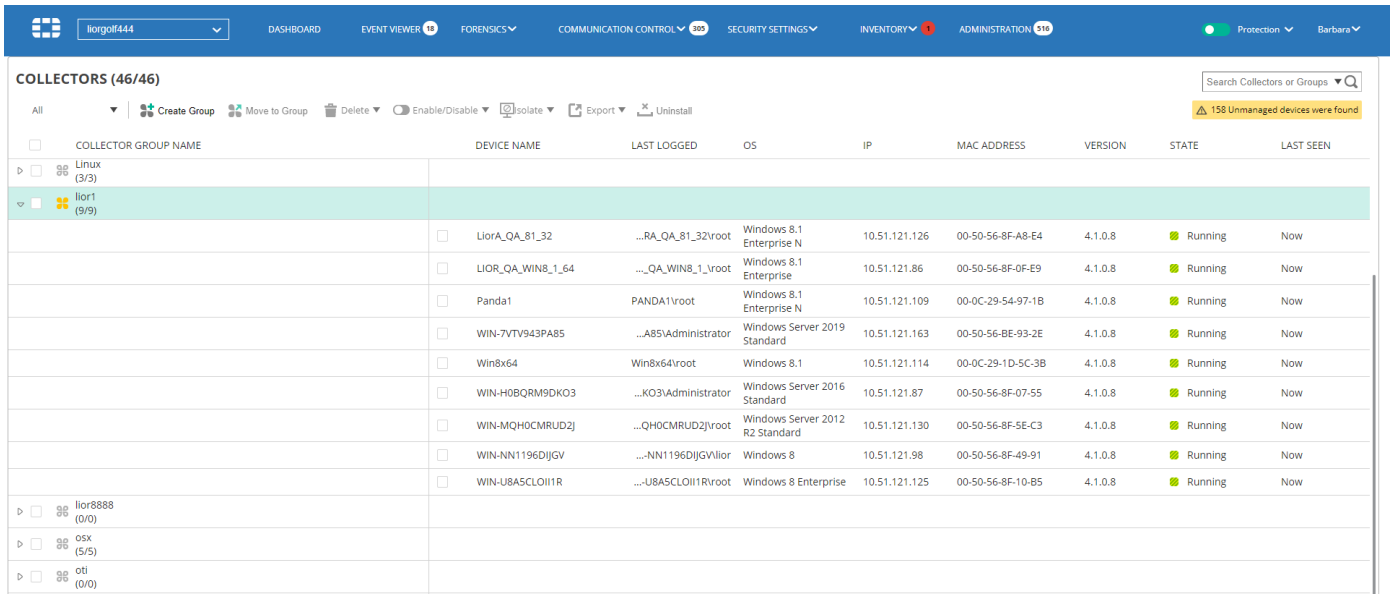
Use the Uninstall button to uninstall a Collector from a device. Use caution when using this option, as a Collector cannot be reinstalled after removal using the FortiEDR user interface. Therefore, it is recommended to disable a Collector using the **Enable/Disable** option rather than uninstalling it.

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 page 72. 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 page 73.

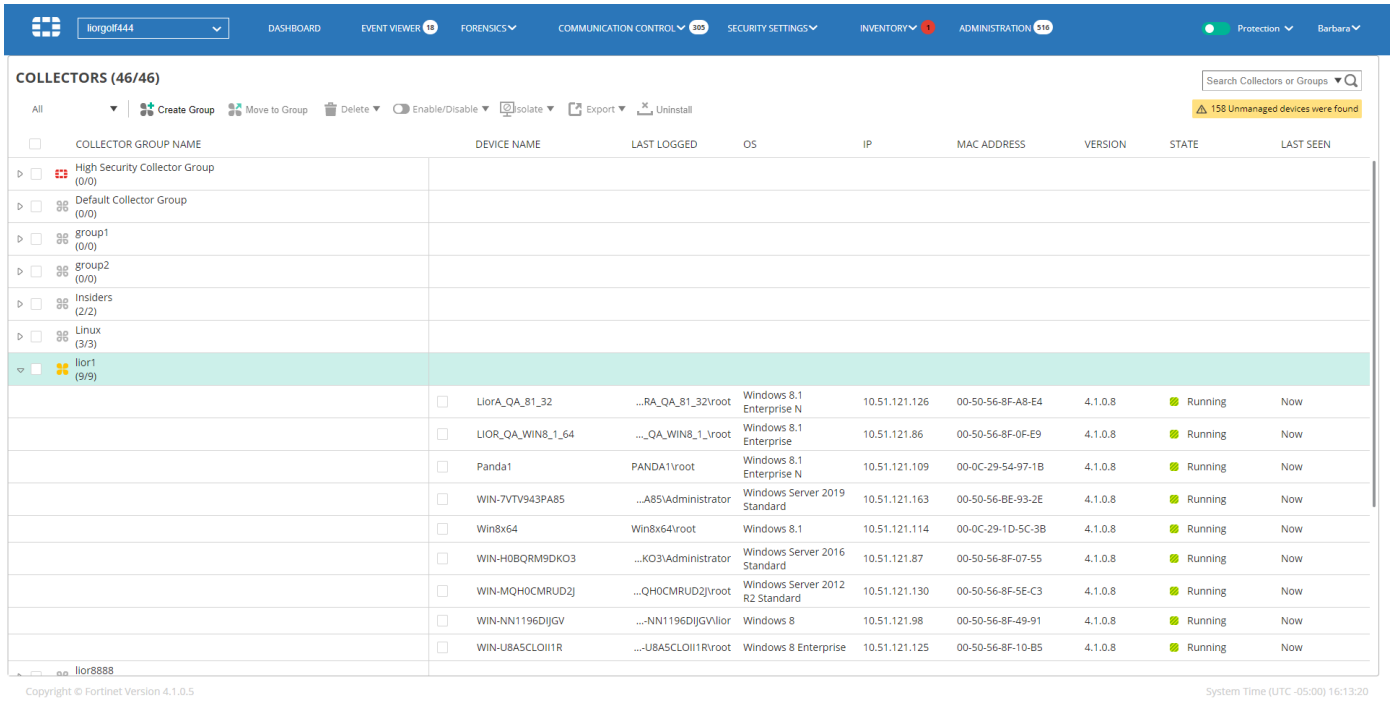
To access this page, click the down arrow next to **INVENTORY** and then select **Collectors**, as shown below.





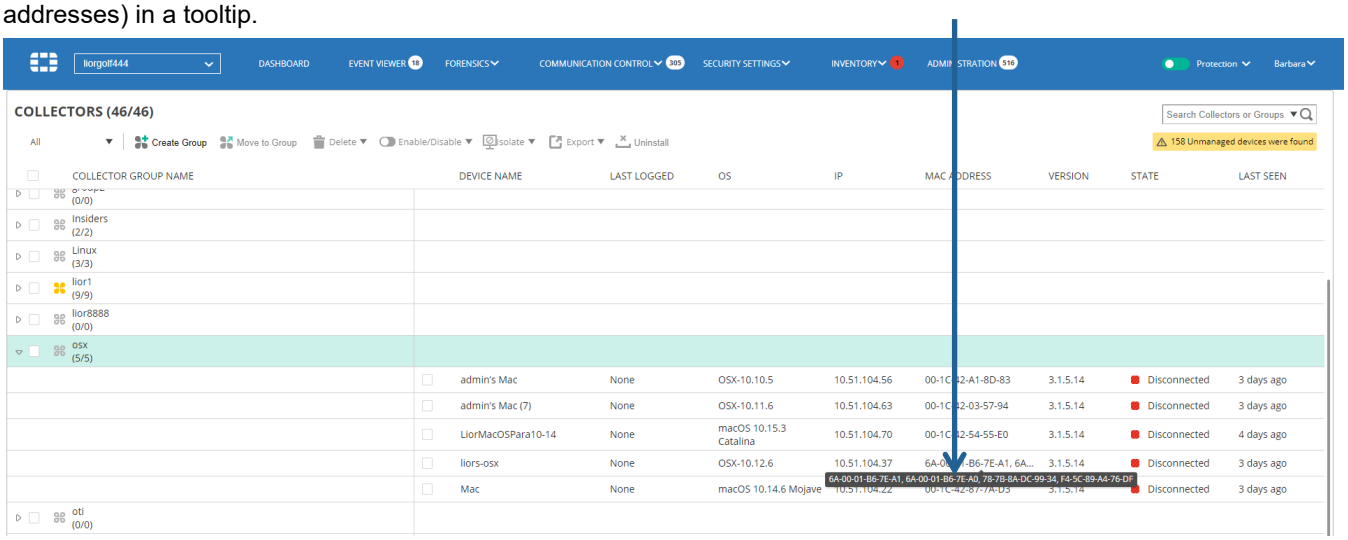
The default Collector Group (to which new Collectors are automatically added) is marked with a yellow group icon . You can change to a different default Collector Group by clicking the group icon of another Collector Group.

Click to expand the list and display the FortiEDR Collectors that the Collector Group contains.



The following information is provided for each Collector:

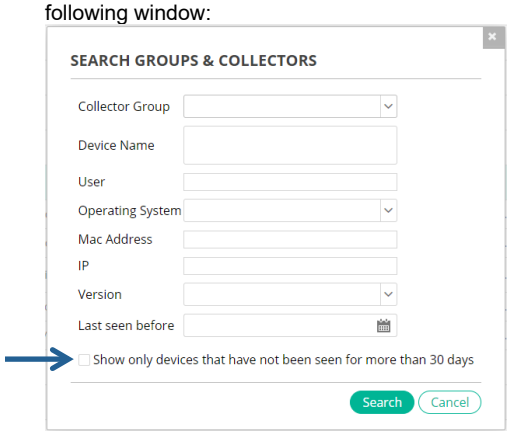
- **Checkbox:** Check this checkbox to select the Collector. You can then use one of the buttons at the top left of the window, such as the **Delete** button.
- **COLLECTOR GROUP NAME:** Specifies the name of the Collector Group to which the Collector is assigned.
- **DEVICE NAME:** Specifies the device 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 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:** 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:
  - **Running:** The FortiEDR Collector is up and all is well.
  - **Running (Autonomously):** The core is temporarily inaccessible. Therefore, policy enforcement is performed by the FortiEDR Collector.
  - **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.

  Note – To see the list of Collectors in this state, click the down arrow in the **Search** box at the top right of the window to display the following window:

  Then, check the **Show only devices that have not been seen for more than 30 days** checkbox, and click the **Search** button. The Collectors area then displays only devices in the Disconnected (Expired) state.

- **Pending Reboot:** 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.
- **Disabled:** Specifies that this FortiEDR Collector was disabled in the FortiEDR Central Manager. This feature is not yet available in version 1.2.
- **Degraded:** 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).

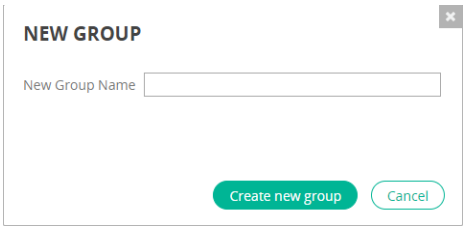
- **LAST SEEN:** Counts the number of days passed from the last time this Collector communicated with the Core.

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.

To define a new Collector Group:

1. Click the Create group button. The following window displays:

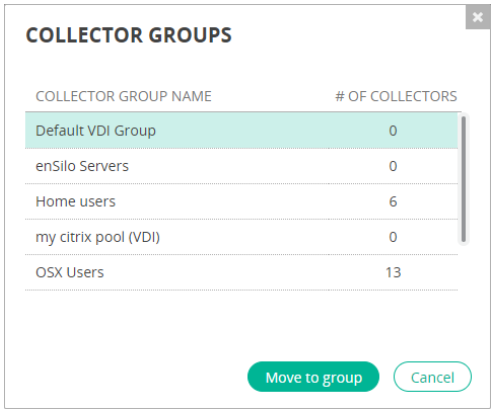
   

2. Enter any name for this group and click the **Create new group** button.

Assigning Collectors to a Collector Group

To assign a Collector 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 button. The following window displays showing the names of the current Collector Groups and how many Collectors each contains:



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:

- Select the Collector Group's/Collector's checkbox and then click the Delete button.

Enabling/Disabling a Collector

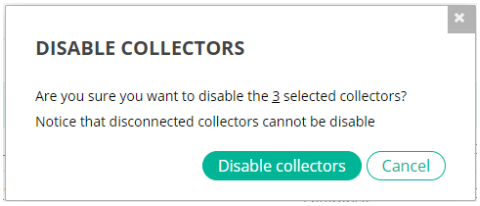
You can enable or disable one or more Collectors simultaneously.

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:



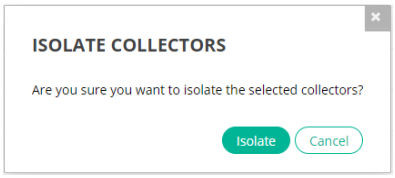
3. Click Disable collectors.

Device Isolation

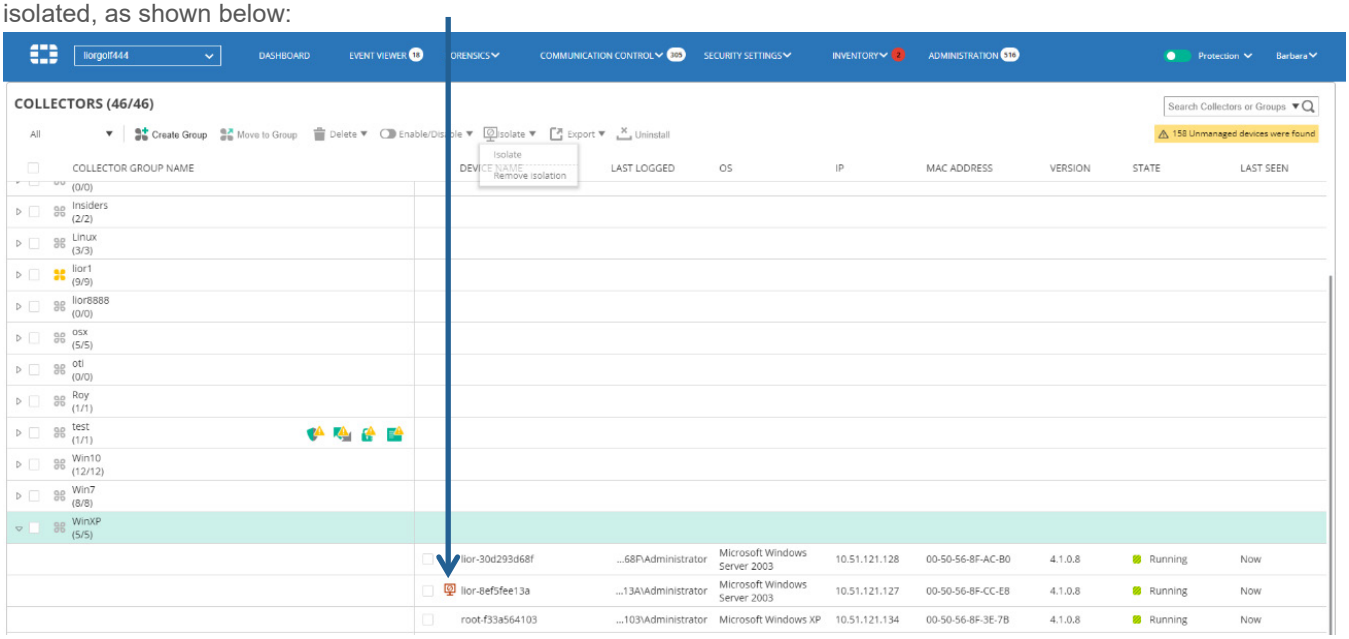
An isolated device is one that is blocked from communicating with the outside world (for both sending and receiving). A device can be isolated manually, as described below. For more details about device isolation, see page 64.

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:

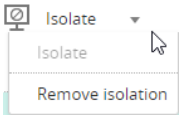


3. Click the **Isolate** button. A red icon appears next to the relevant Collector to indicate that the Collector has been isolated, as shown below:

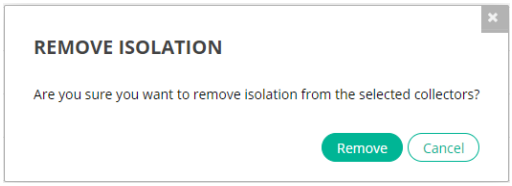


To remove isolation from a device:

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:

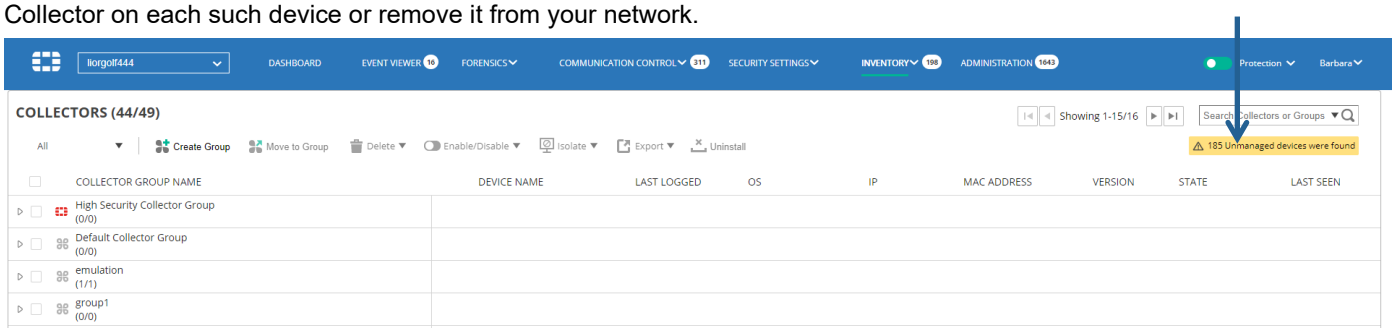


3. Click the **Remove** button.

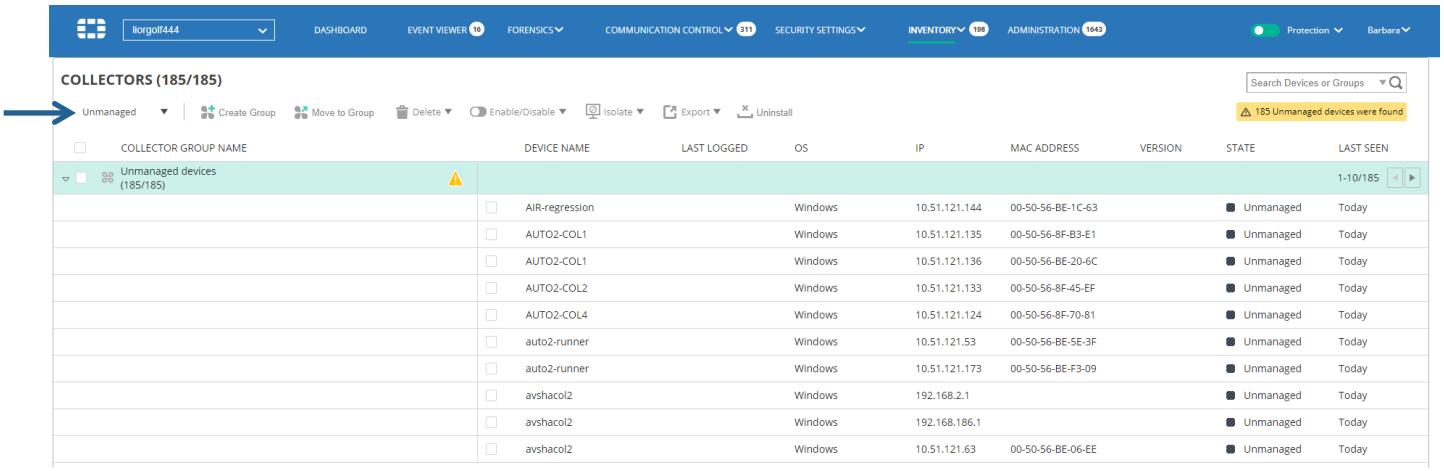
Unmanaged Devices

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.

Important – Unmanaged devices are not protected in the system. Therefore, it is recommended that you either install a Collector on each such device or remove it from your network.



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



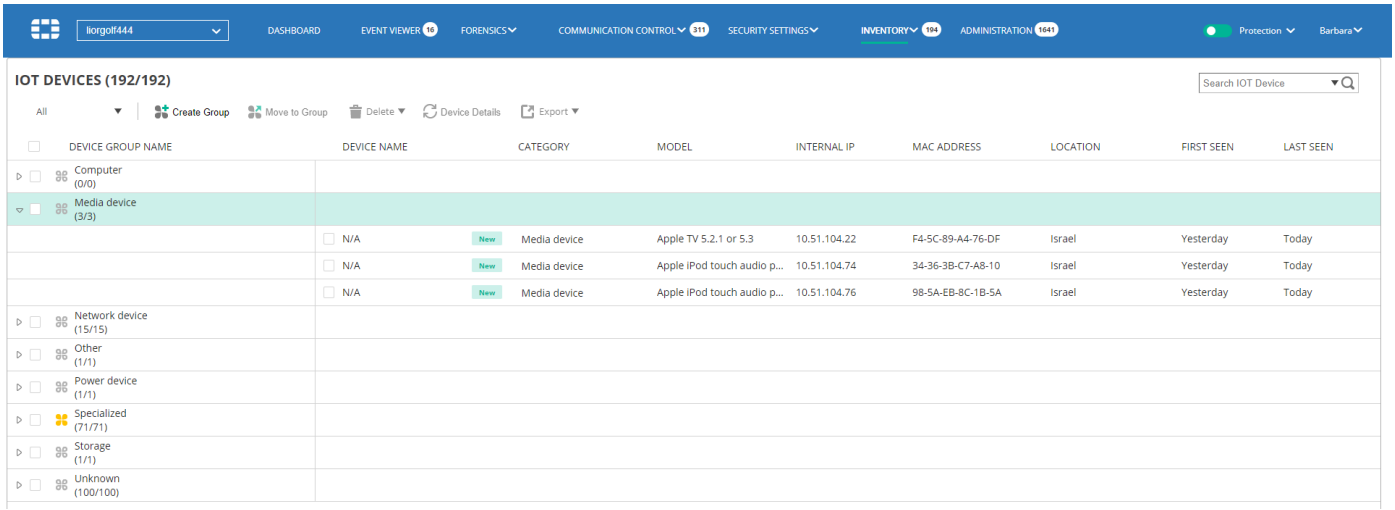
None of the action buttons at the top of the window are available for unmanaged devices, as there is no Collector installed on these devices.

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 **Predict and Protect** or the **Predict, 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 the *IoT Device Discovery* section on page 168.



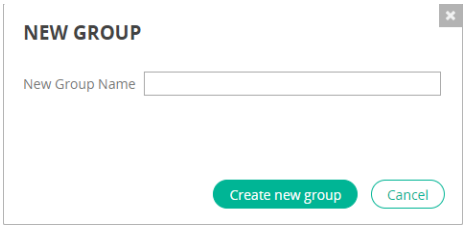
This page provides all the collected information about each discovered device, including its name, category (device type), model number, internal IP address, MAC address, the physical location where the device was detected (based on its external IP address) and when it was first and last seen. FortiEDR 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

To define a new IoT Group:

1. Click the Create group button. The following window displays:

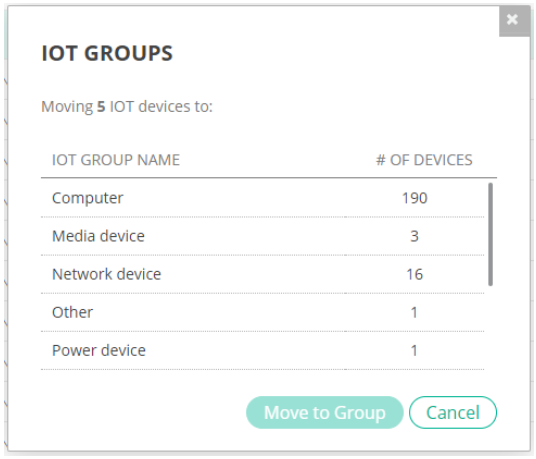


2. Enter any name for this group and click the **Create new group** button.

Assigning Devices to an IoT Group

To assign an IoT device 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:



3. Select the IoT Group to which to move the selected devices.
4. Click the **Move to group** button.

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:

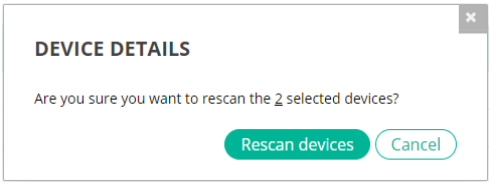
- Select the IoT Group's/IoT device's checkbox and then click the Delete button.

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 the **Rescan devices** button.

Exporting IoT Information

To export the list of IoT devices:

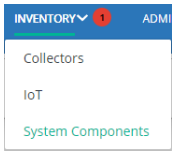
- Use the Export button and select **Excel** or **PDF**.

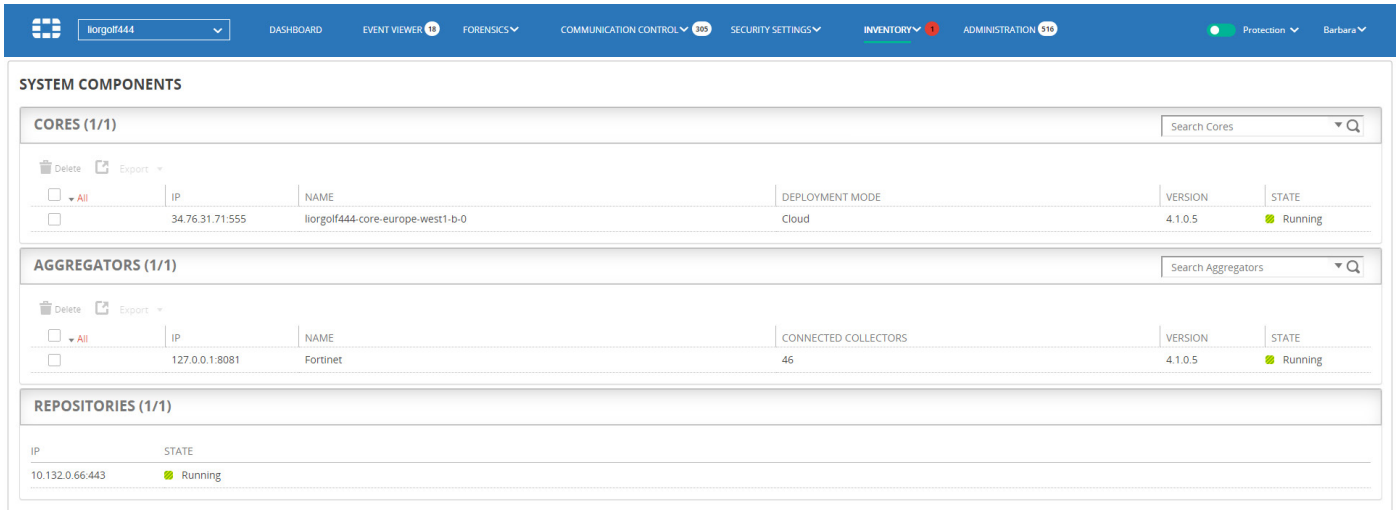
To export details for an IoT device:

- Check the checkbox of the device of interest and then 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

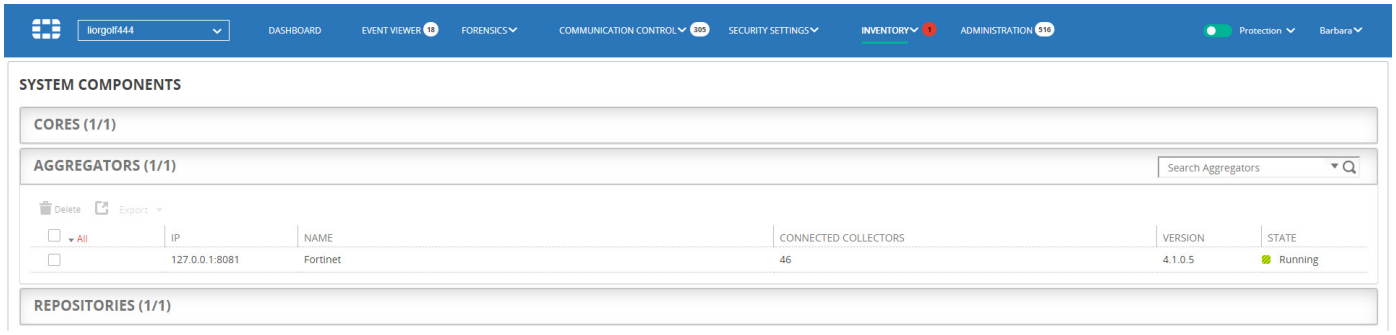
The SYSTEM COMPONENTS page lists the FortiEDR Aggregators, Cores and Repositories. To access this page, click the down arrow next to INVENTORY and then select System Components, as shown below.





Aggregators

The **AGGREGATORS** area lists the FortiEDR Aggregators.

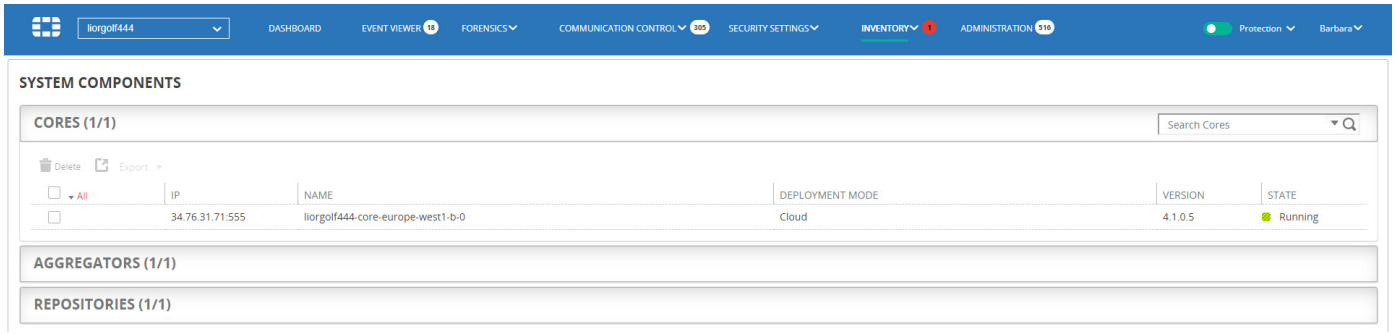


Click to expand the list. The following information is provided for each FortiEDR Aggregator:

- **Checkbox:** Check this checkbox to select the Aggregator. You can then use one of the buttons at the top left of the window, such as the **Delete** button
- **IP:** Specifies the IP address of the communicating device on which the FortiEDR Aggregator is installed.
- **NAME:** Specifies the Aggregator name entered during installation.
- **CONNECTED COLLECTORS:** Specifies the number of FortiEDR Collectors that have been configured to operate with this Aggregator.
- **VERSION:** Specifies the version of the Aggregator software.
- **STATE:** Specifies the current state of the FortiEDR Aggregator (page 71).

Cores

The **CORES** area lists the FortiEDR Cores.

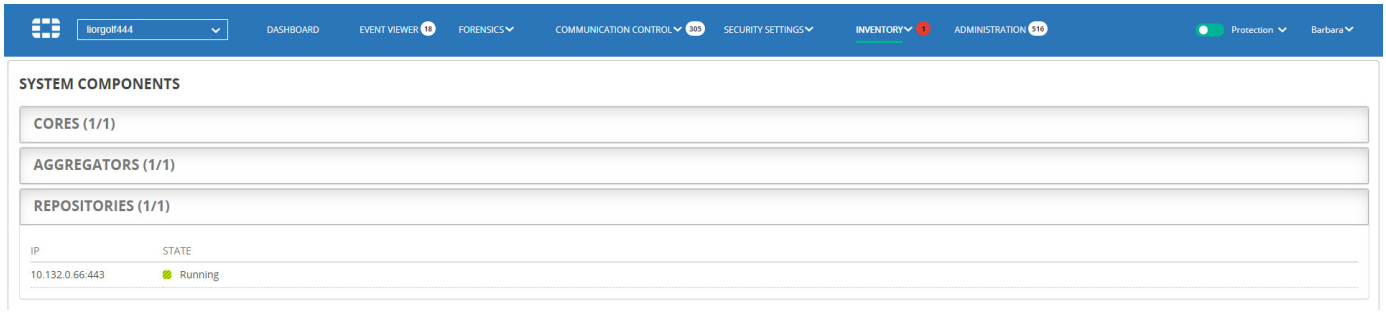


Click to expand the list. The following information is provided for each FortiEDR Core:

- **Checkbox:** Check this checkbox to select the Core. You can then use one of the buttons at the top left of the window, such as the **Delete** button
- **ORGANIZATION:** Specifies the name of the organization in a multi-organization FortiEDR environment. In a single-organization FortiEDR system, this column does not appear.
- **IP:** Specifies the IP address of the communicating device on which the FortiEDR Core is installed.
- **NAME:** Specifies the FortiEDR Core name entered during installation.
- **DEPLOYMENT MODE:** Specifies whether the FortiEDR Core is physically deployed on your organization's premises (On-Premise) or in the cloud provided by Fortinet (Cloud).
- **VERSION:** Specifies the version of the FortiEDR Core.
- **STATE:** Specifies the current state of the FortiEDR Core (page 71).

Repositories

The **REPOSITORIES** area shows details about the FortiEDR Threat Hunting Repository server.



Click ▷ to expand the list. The following information is provided for the FortiEDR Repository:

- **IP:** Specifies the IP 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**.

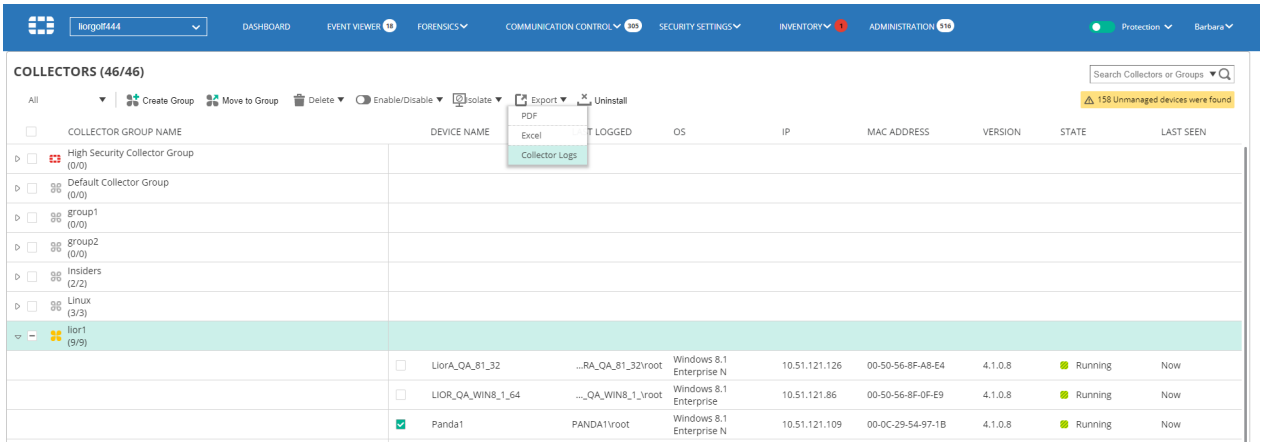
Logs only need to be retrieved when Fortinet technical support requests that you provide them. There is no need for you to analyze the data contained in the FortiEDR logs. You can retrieve logs for the following:

- **Exporting Logs for Collectors,** page 80
- **Exporting Logs for Cores,** page 81
- **Exporting Logs for Aggregators,** page 81

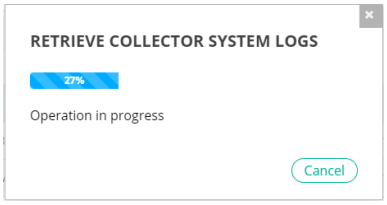
Exporting Logs for Collectors

To export Collector logs:

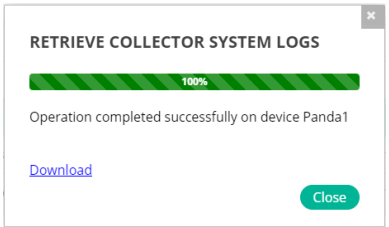
1. In the **COLLECTORS** page, select the checkboxes of the FortiEDR Collectors for which you want to export logs.



2. 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:



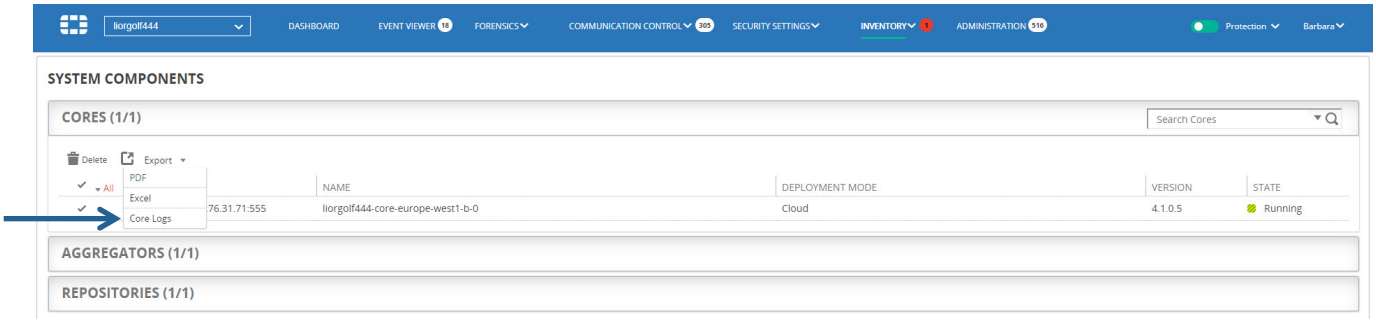
3. Click the **Download** link to automatically send the retrieved logs to Fortinet technical support.

Exporting Logs for Cores

The procedure for exporting logs for Cores is similar to that for exporting Collector logs.

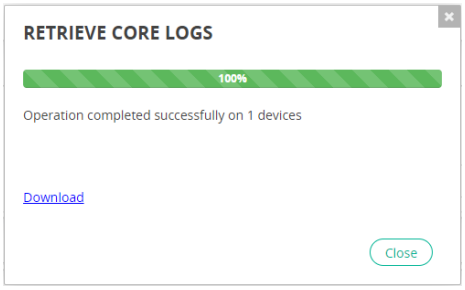
To export Core logs:

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:

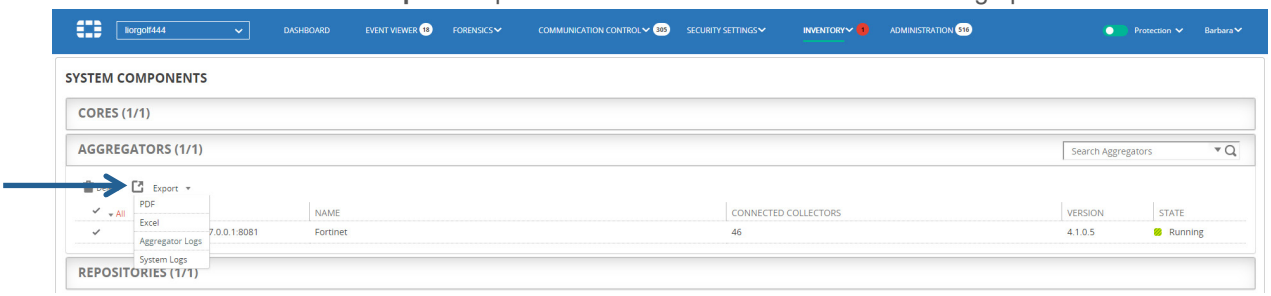


3. Click the **Download** link to automatically send the retrieved logs to Fortinet technical support.

Exporting Logs for Aggregators

To export Aggregator logs:

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:



- **Aggregator Logs:** Exports the log for the selected Aggregator(s).
- **System Logs:** Exports the logs of the central Manager.

A progress window displays.

After the retrieval process completes, a window displays.

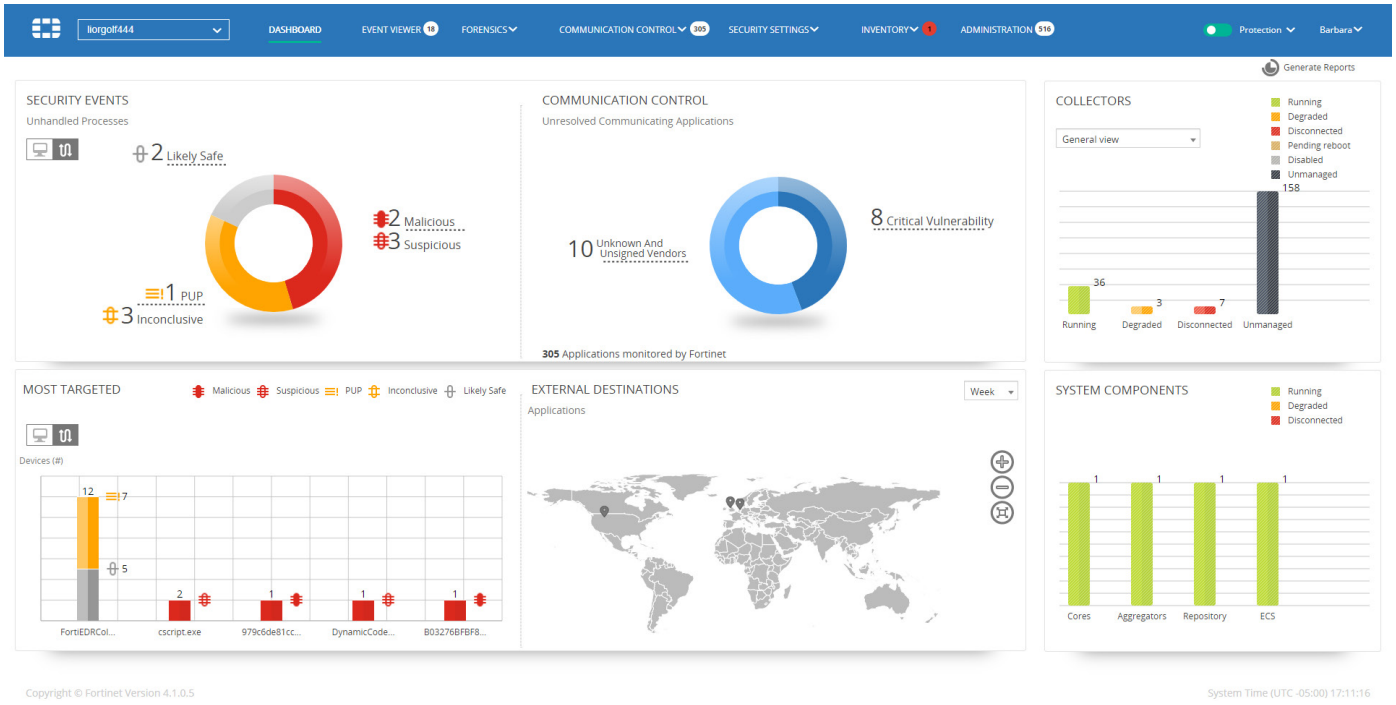
Click the **Download** link to automatically send the retrieved logs to Fortinet technical support.

Chapter 5 – 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.



Note – 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.

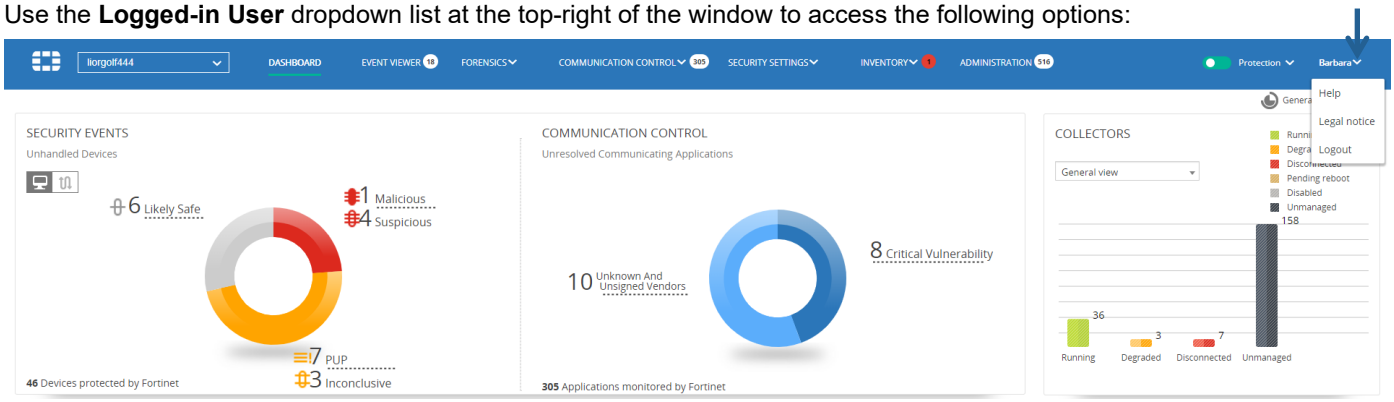
The Dashboard enables you to display two different slices or views of the data collected by FortiEDR:

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

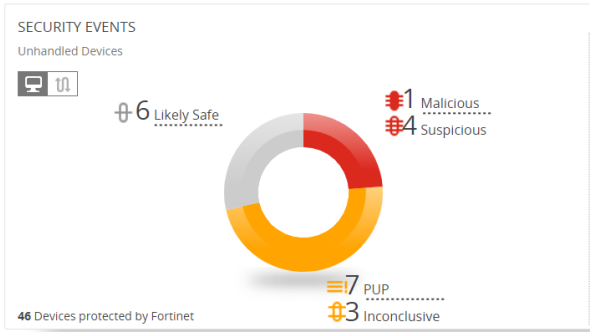
The information presented in the Dashboard represents an aggregation of events. For more details, you may refer to the *Event Aggregation* section on page 90. FortiEDR aggregates events in both the Device view and the Process view in the Dashboard.

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

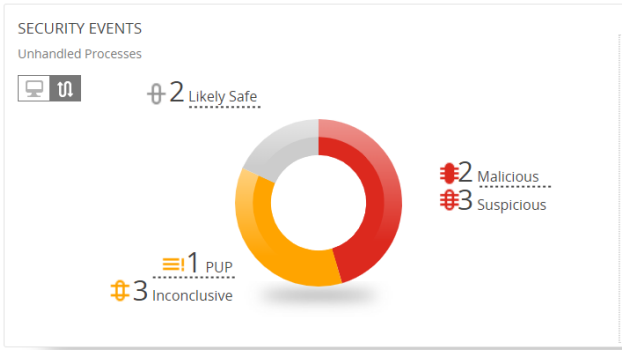


- **Help:** Enables you to download the latest version of the *FortiEDR Installation and Administration Guide*.
- **Legal Notice:** Downloads the FortiEDR legal notice.
- **Logout:** Exits the FortiEDR application.

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 severity of the FortiEDR events that have not yet been handled. The chart is color-coded according to event severity:

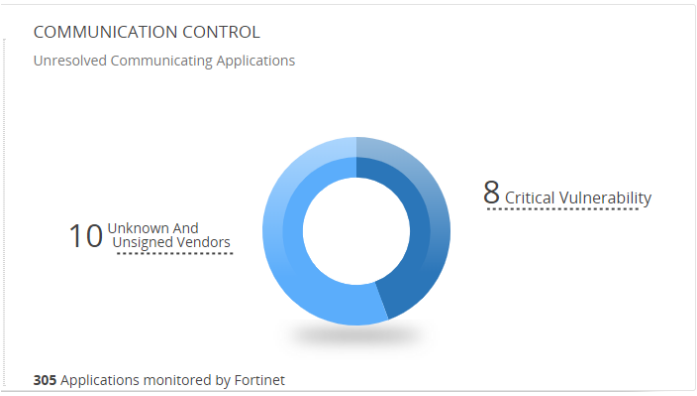
- **Red:** Critical
- **Yellow:** High
- **Grey:** Medium

Click this chart to drill down to the Event Viewer, which shows a filtered chart listing the unhandled events (page 95) according to the severity (color) that you clicked in this chart.

Each 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.



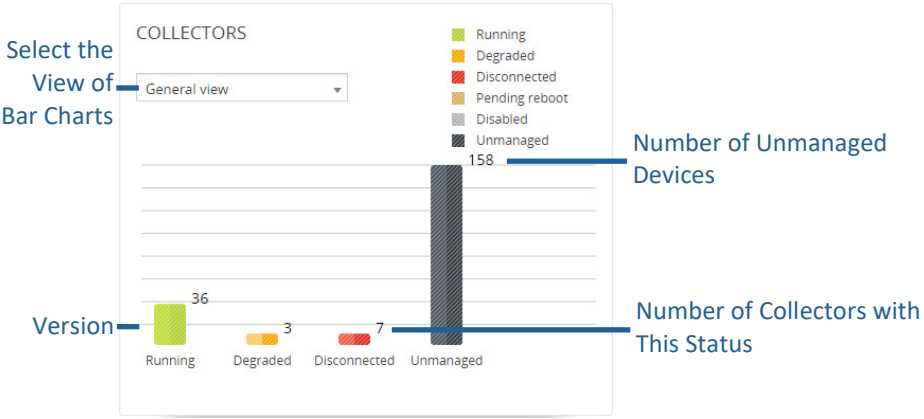
Click a box in the chart to drill down to the Communication Control.

Collectors Chart

The **COLLECTORS** chart provides an overview of FortiEDR Collectors. 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. For more information about unmanaged devices, see page 70.

The bar chart is color-coded and numbered to indicate the distribution of statuses (page 83) among the components within the operating system group.

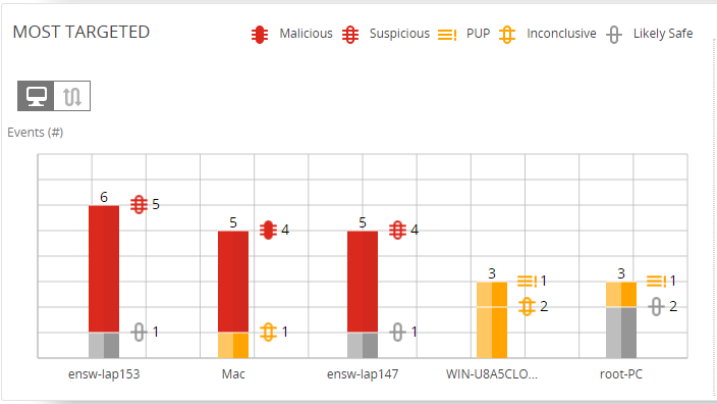
Each bar chart indicates the Version or the Operating System of that component, according to the option that you selected in the **View By** dropdown menu.



Click this chart to drill down to the relevant INVENTORY (page 68), 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

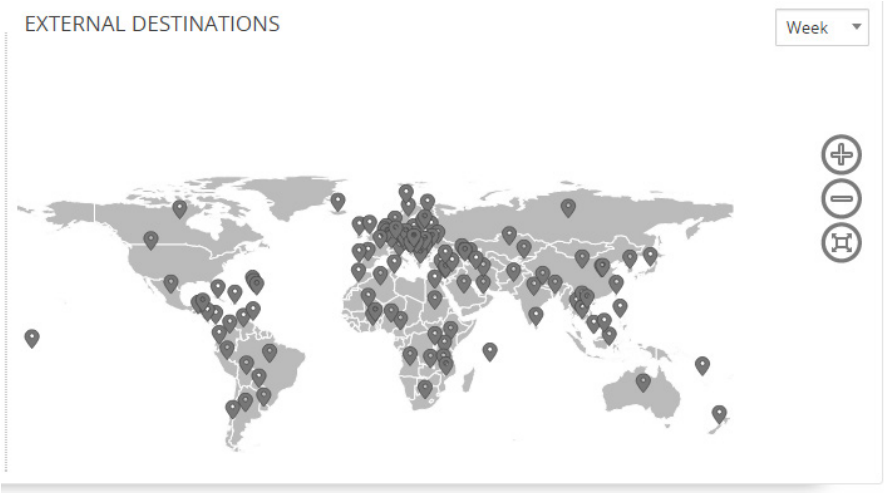


The **MOST TARGETED** chart displays the history of the most-infected and targeted processes, applications and devices. This chart is color-coded according to the severity of the attacks. The information is displayed per last day, last week or last month, according to your selection.

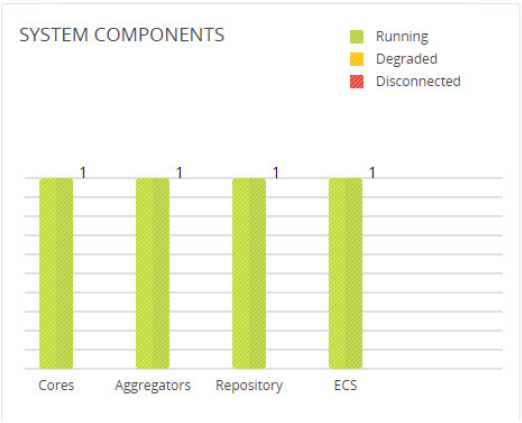
Click this chart to drill down to the Event Viewer (page 90), which shows a filtered chart listing the events for the selected process or device.

External Destinations

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



System Components



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

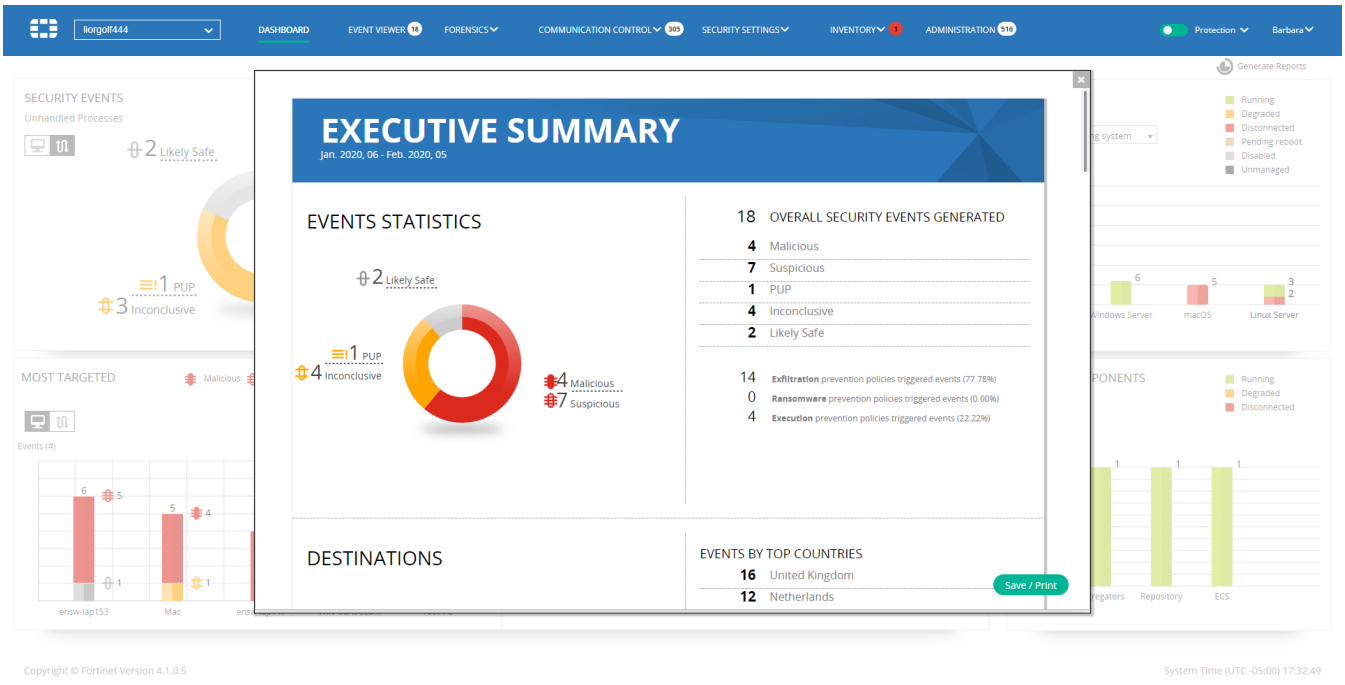
Executive Summary Report

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

To generate an Executive Summary report:

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

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.



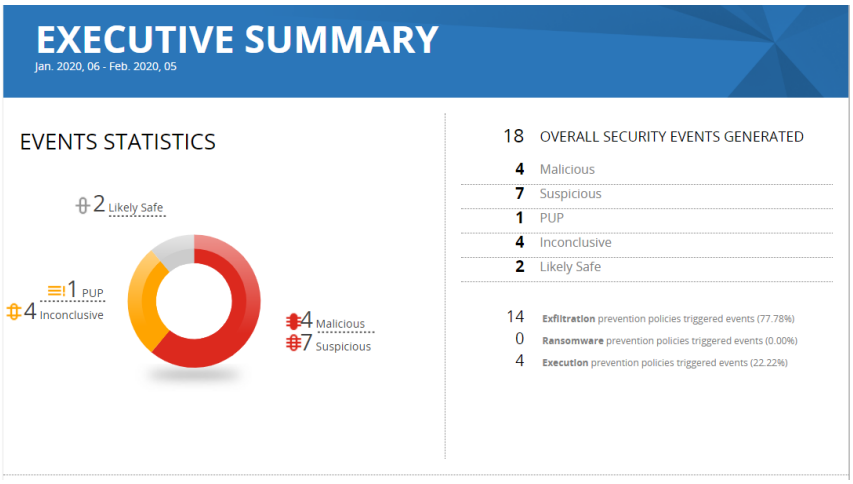
4. Click **Save/Print** to save or print the report.

   The report presents several sections of information, as follows:

   - **Event Statistics,** page 87
   - **Destinations,** page 87
   - **Most-targeted Devices,** page 88
   - **Communication Control,** page 88
   - **System Components,** page 89
   - **License Status,** page 89

Event Statistics

The Event Statistics section of the Executive Summary report displays a breakdown of the events created during the timeframe of the report. Events are classified by severity. The total number and percentage of events triggered by the Exfiltration and Ransomware policies are also displayed. For more details, see *Chapter 6*, *Event Viewer* on page 90.

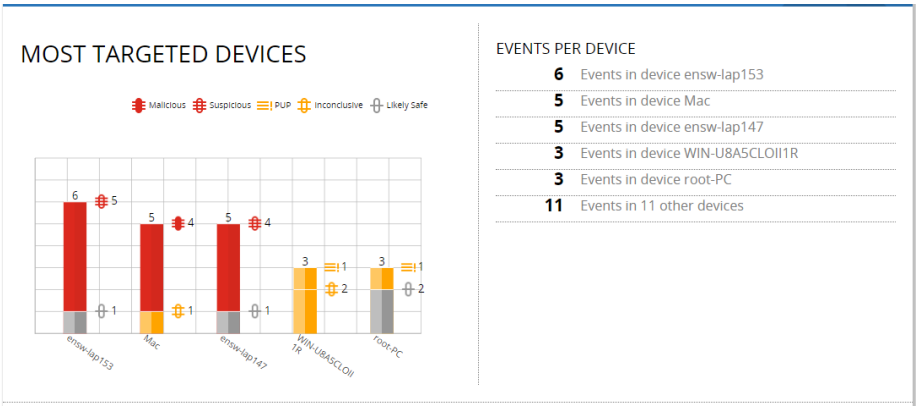


Destinations

The Destination section of the Executive Summary report displays a map of all the destinations for the events triggered during the timeframe of the report. The names of the top seven countries with the most events are shown. There is a pin on the map for each represented country. For more details, see the *External Destinations* section on page 85.

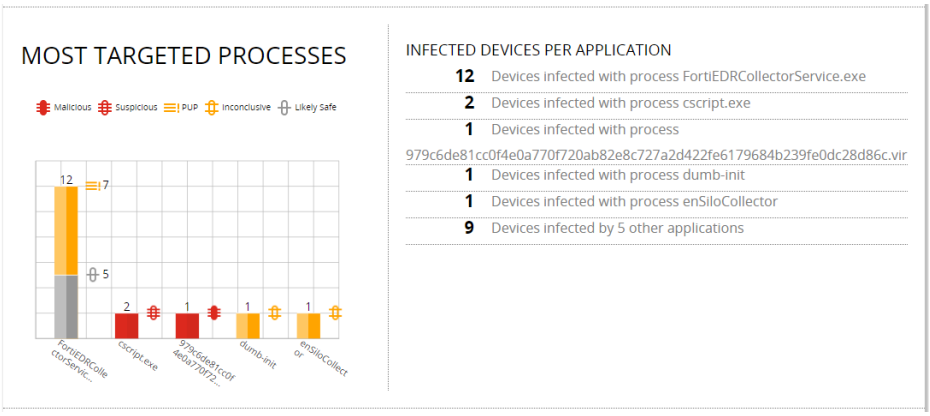
Most-targeted Devices

The Most Targeted Devices section of the Executive Summary report displays all the 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* section on page 85.



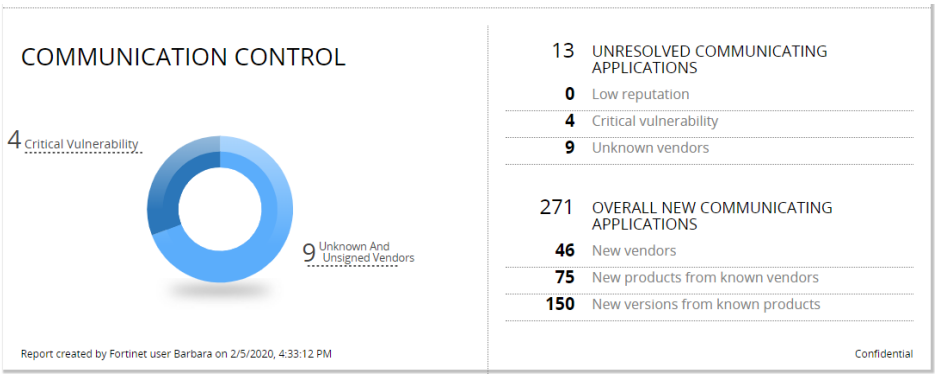
Most-targeted Processes

The Most Targeted Processes section of the Executive Summary report displays all the 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* section on page 85.



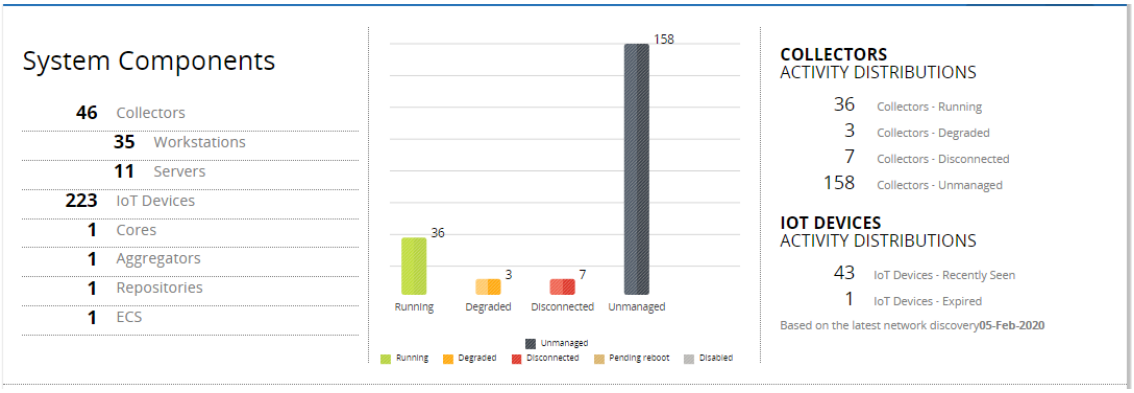
Communication Control

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 *Chapter 7*, *Communication Control* on page 110.



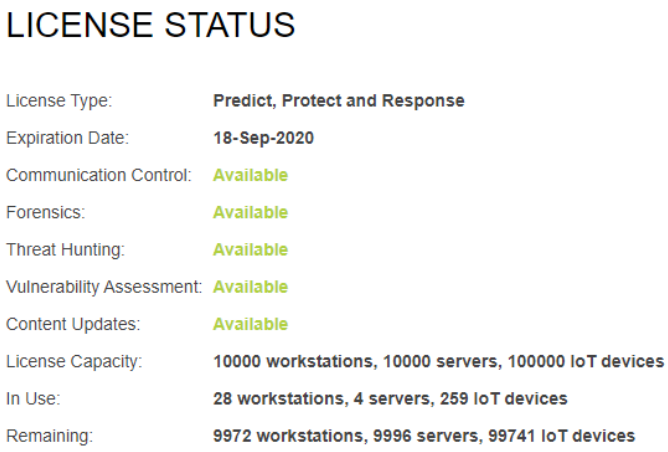
System Components

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* section on page 12. For more details about IoT devices, see page 76. For more details about unmanaged devices, see page 69.



License Status

The License Status section of the Executive Summary report displays a summary of license-related information. For more details, see the *Licensing* section on page 147.



Chapter 6 – EVENT VIEWER

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

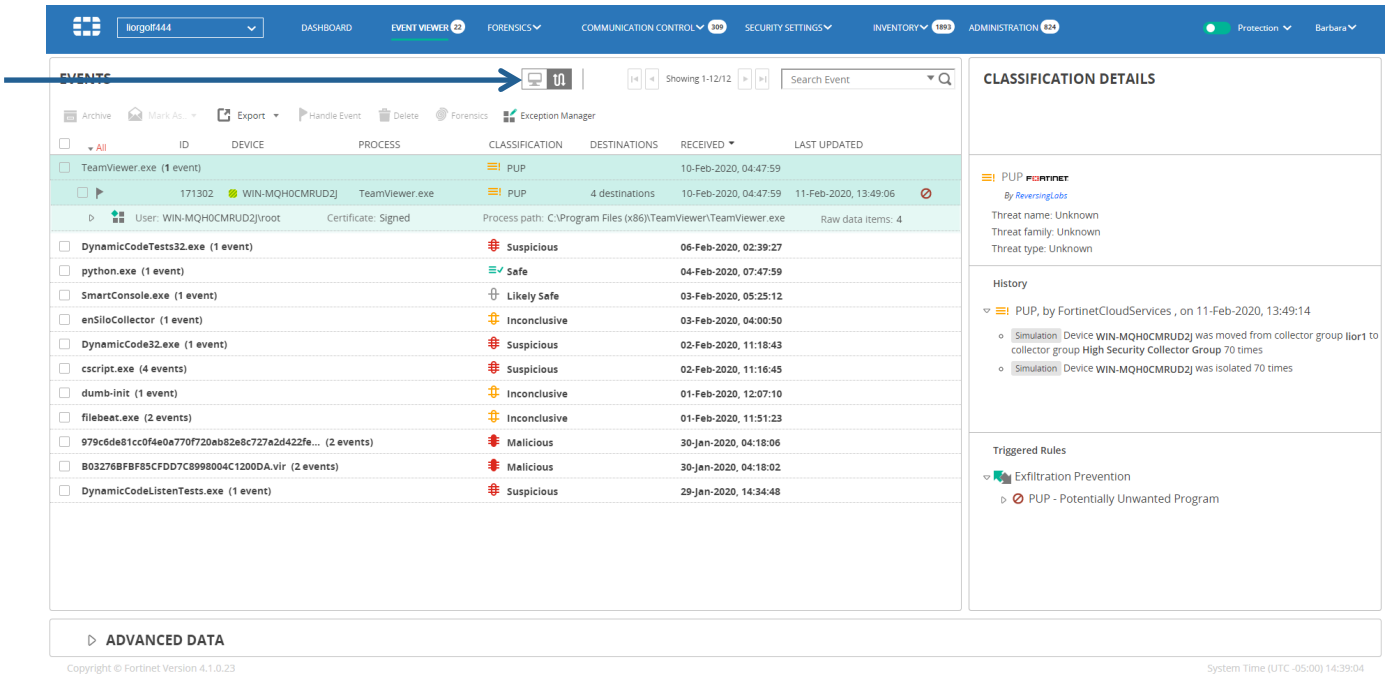
Introducing the Event Viewer

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

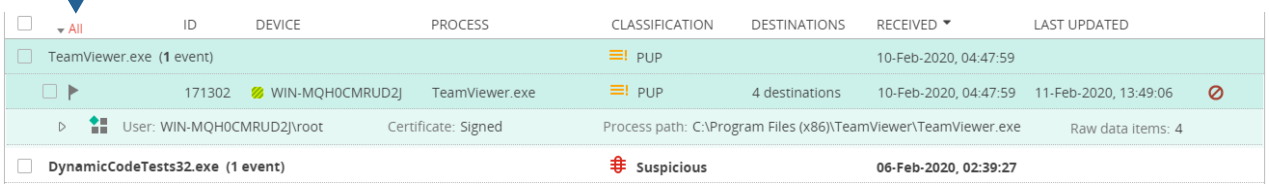
Click the applicable view button at the top center of the window to display that view.



Event Aggregation

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

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

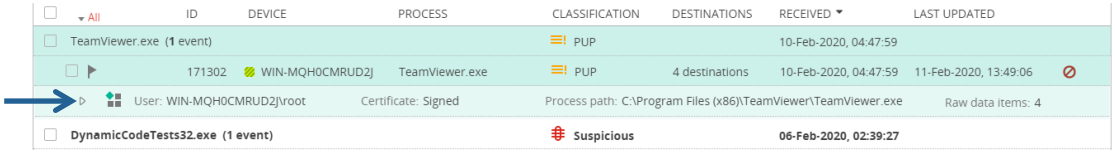


Note – The **All** filter also displays expired events.

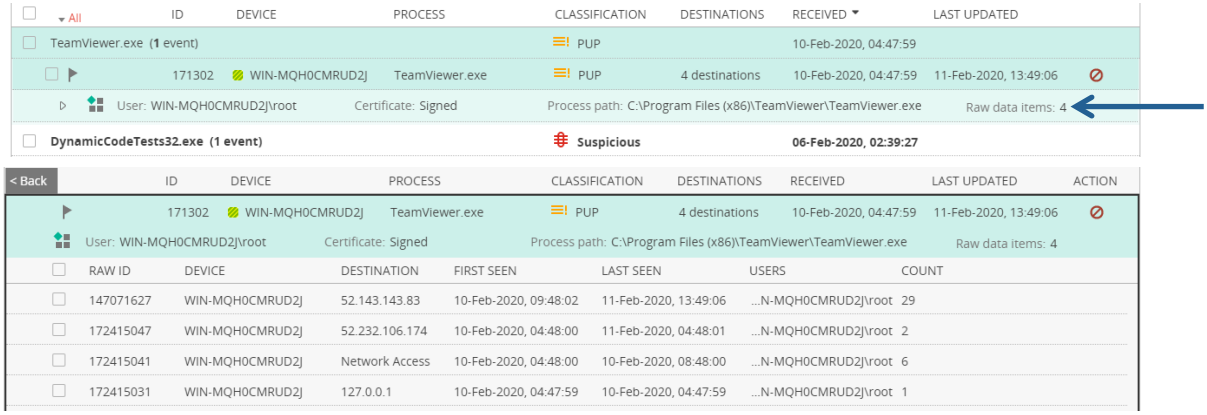
- You can drill down on a device/process to display the events for that device/process. Each event row is marked with a flag indicator.

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

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



- You can drill down further in an 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 event. For example, in the figure below, the event comprises 4 raw data items, coming from different devices and going to different destinations. You can click the < Back icon to return to the aggregated event view.



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.

An 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 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 events, each with one event under it.
- In the Process view, you see one event aggregation named **adobe.exe**. Under it, there is one event for the **adobe.exe** process. That 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:

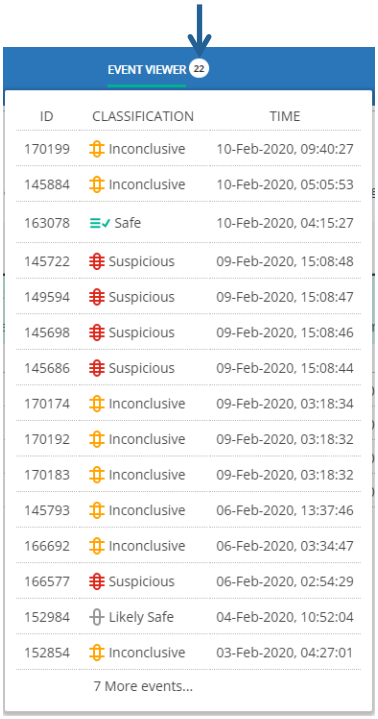
- **EVENTS,** page 92
- **ADVANCED DATA,** page 94
- **CLASSIFICATION DETAILS,** page 106

The following actions can be performed in the Event Viewer:

- **Marking an Event as Handled/Unhandled,** page 95
- **Defining Event Exceptions,** page 96
- **Marking an Event as Read/Unread,** page 104
- **Viewing Expired Events,** page 104
- **Viewing Device Control Events,** page 105
- **Other Event Viewer Options,** page 105

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

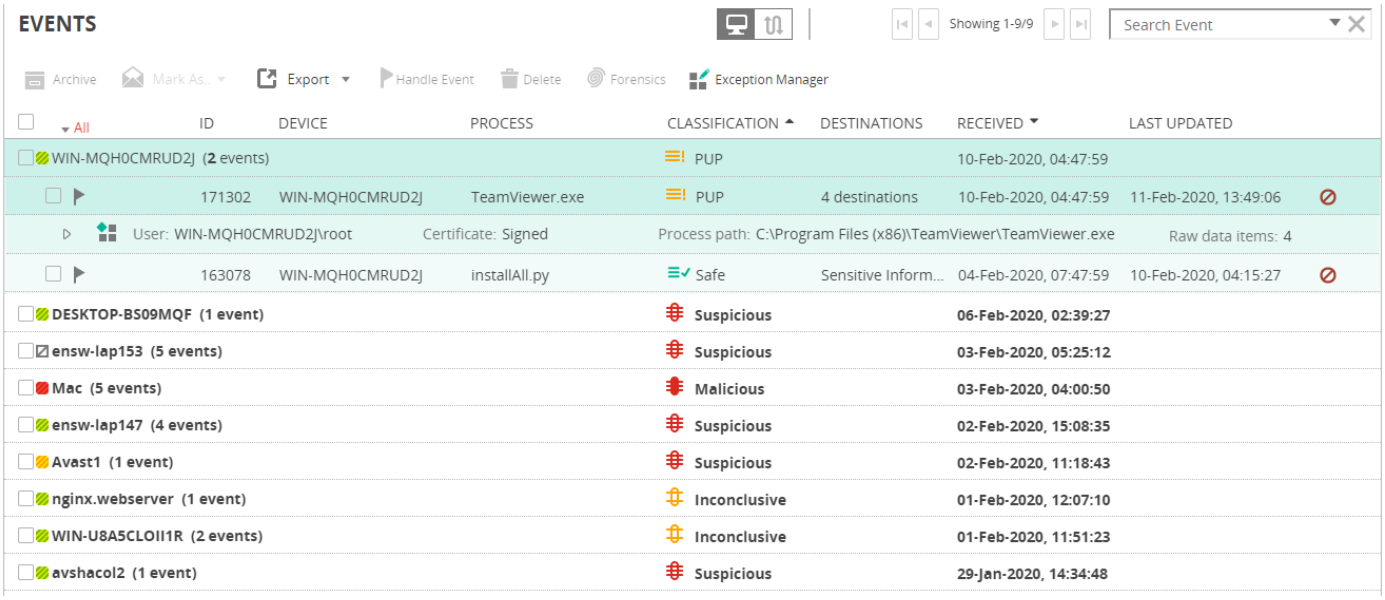
Hovering over this number indicates the number of new unread events, shown below:



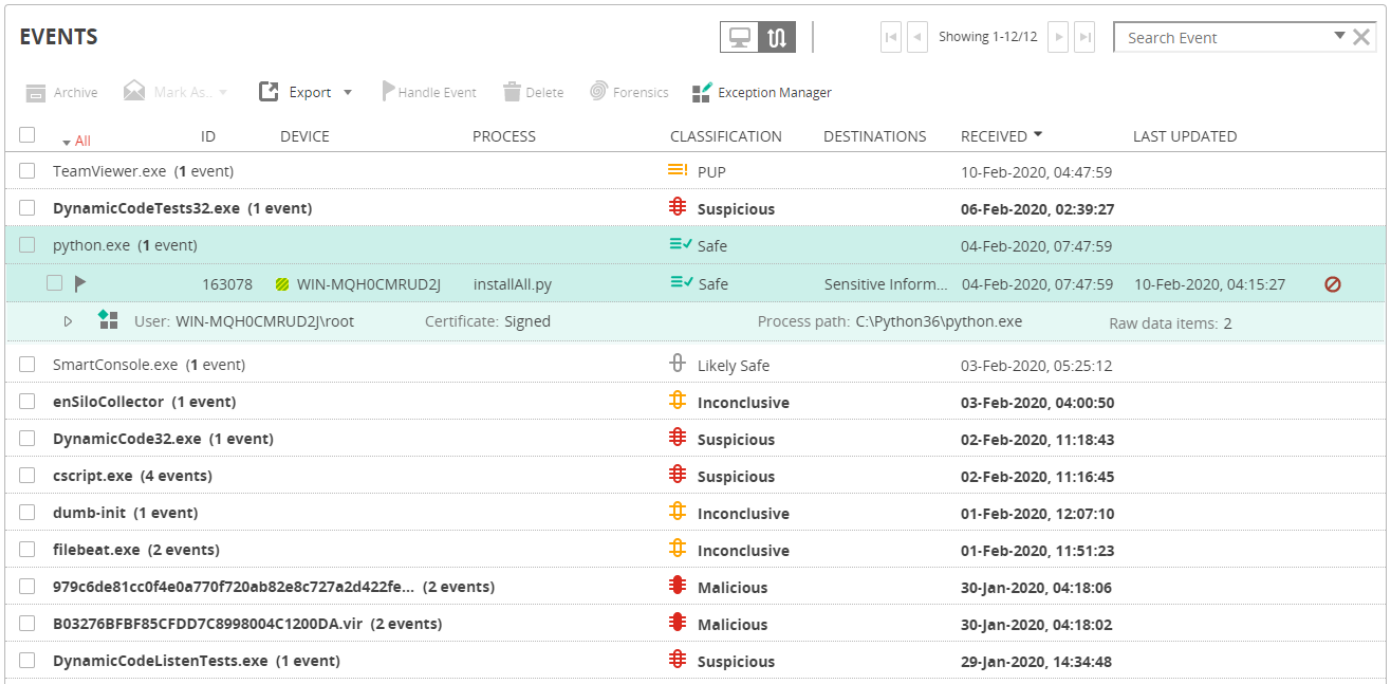
In some cases, **Updated** displays next to the number of new unread events indicator. Updated means that FortiEDR originally classified one of the unread events, but that classification was later changed by the user. After more data for this event was received, FortiEDR overrode the manual classification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

Events Pane

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



Device View



Process View

- **View Indicator:** Indicates the view context for the event aggregation. displays for a device and displays for a process.
- **Handled/Not Handled:** Specifies whether any FortiEDR Central Manager user handled this event, as described on page 95.
- **ID:** Specifies an automatically assigned unique identifier for each event generated by FortiEDR. This identifier is particularly useful for event tracking purposes when monitoring events using an external system, such as a SIEM.
- **DEVICE:** Specifies the communicating device name on which the FortiEDR Collector is installed.
- **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 event was triggered by a script, then the script name is specified.
- **SEVERITY:** Specifies the severity of the rule – **Critical**, **High** or **Medium**. The severity of the event that is triggered is determined by the most severe rule that is violated.
- **CLASSIFICATION:** Specifies how malicious the 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 FortiEDR Cloud Service (FCS) or manually. The FCS is a cloud-based, software-only service that determines the exact classification of 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 59.Classifications are:
  - Malicious
  - Suspicious
  - Inconclusive
  - Likely Safe
  - PUP (Potentially Unwanted Program)
  - Safe
- **DESTINATIONS:** Specifies the IP address to which the malicious entity requested to establish a connection.

  Note – For a violation of the Ransomware Prevention policy, this column may show **File Access** instead of an IP address. For more details about this policy, see page 53.
- **RECEIVED:** Specifies the first time that this event was triggered. For aggregations, the most-recent received time is displayed.

- **LAST UPDATED:** Specifies the last time that the event was triggered. For aggregations, the most-recent time is displayed.
- **ACTION:** Specifies the action that was enforced:
  - **: Block**: The exfiltration attempt was blocked and this blocking event was generated.
  - **Simulated Block:** The policy that protected this device was set to **Simulation** mode. Therefore, the exfiltration attempt was **NOT** blocked and this blocking event was generated. FortiEDR *would have* blocked his exfiltration event if the policy had been set to **Prevention** mode.
  - **: Log.** The event was only logged and was not blocked.
- FIRST SEEN: The Event Viewer aggregates the occurrences of the same events into a single row when it represents the same attack on the same device. This timestamp specifies the first time this event occurred. The row of this event pops to the top of the list in the Event Viewer each time it occurs again.

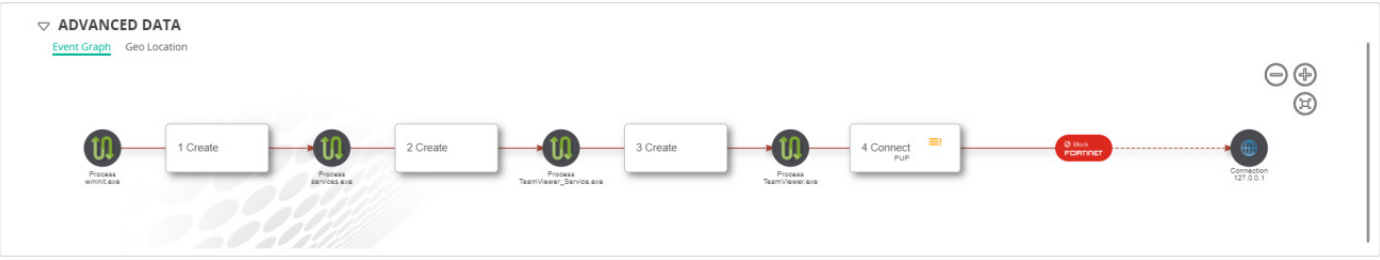
  Note – If a change is made to the FortiEDR policy used by a specific FortiEDR Collector, then the events before and after that change are not aggregated together.
- **LAST SEEN:** Specifies the most recent time this same event occurred. See **FIRST SEEN** described above.
- **Process Type:** Specifies whether the infected process is 32-bit or 64-bit.
- **User:** Specifies the domain of the computer/user of the device.
- **Certificate:** Specifies whether the process or application have certificate – **Signed** or **Unsigned**. You may refer to http://en.wikipedia.org/wiki/Authorization_certificate for general information about the subject.
- **Process Path:** Specifies the path of the infected process.
- **Count:** Specifies the number of occurrences of the same events on the same device.

  Note – Notification actions are not shown in the Event Viewer, but Investigation and Remediation actions are. For more details, see page 62, 64 and 65, respectively.

Advanced Data

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

In addition to textual information that is displayed (described above), a picture is provided 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.



A world map is also displayed showing the location of the event and indicating the country by its flag.

An abundance of additional investigative tools and information are provided by FortiEDR's Forensic add-on (page 130).

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.

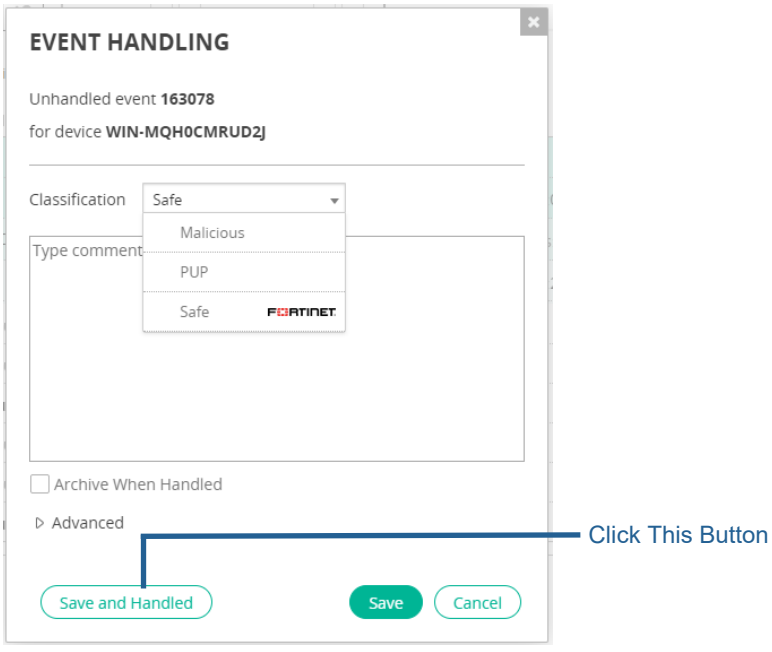
Marking an Event as Handled/Unhandled

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

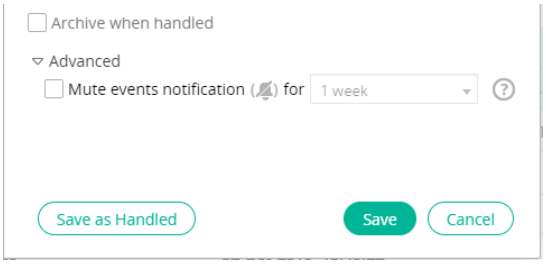
To mark an event as handled:

1. Select the rule's checkbox and then click the Handle event button or just click the flag icon of the event row. The Event Handling window displays.

   Note – If an exception was already defined for this 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 event, if needed. For more details, see page 96.
3. In the comments box, use free text to describe how you handled the event.
4. Click the **Save as Handled** button. The flag icon next to the event changes from dark gray to light gray to indicate to all users that it has been handled.



5. [Optional] Check the **Archive When Handled** checkbox to archive the event after handling it. When you select this option, the 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 event. In addition, specify how long to mute the event notifications. Notifications can be muted for **1 Week**, **1 Month**, **1 Year** or **Permanently**. When checked, you will not receive notifications whenever this event is triggered. When using this option, click the **Save as Handled** button, which indicates that the event has been both handled and saved.



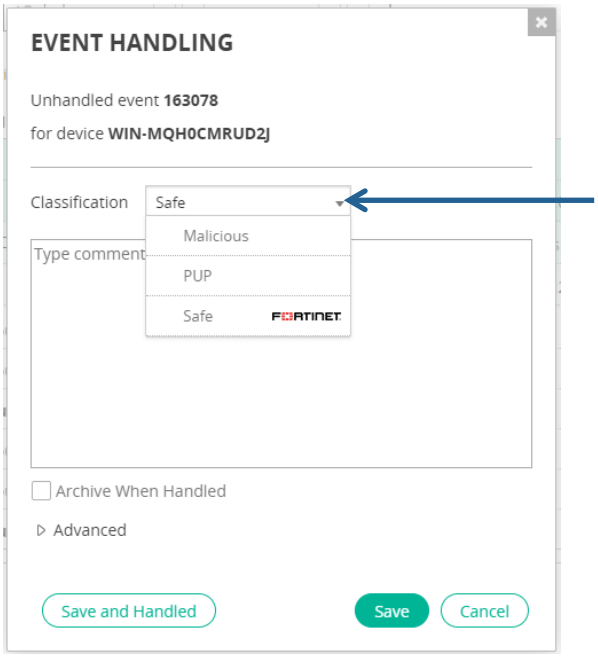
Note – Events with muted event notifications are indicated by the icon in the Event Viewer.

Manually Changing the Classification of an Event

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

To manually change the classification of an event:

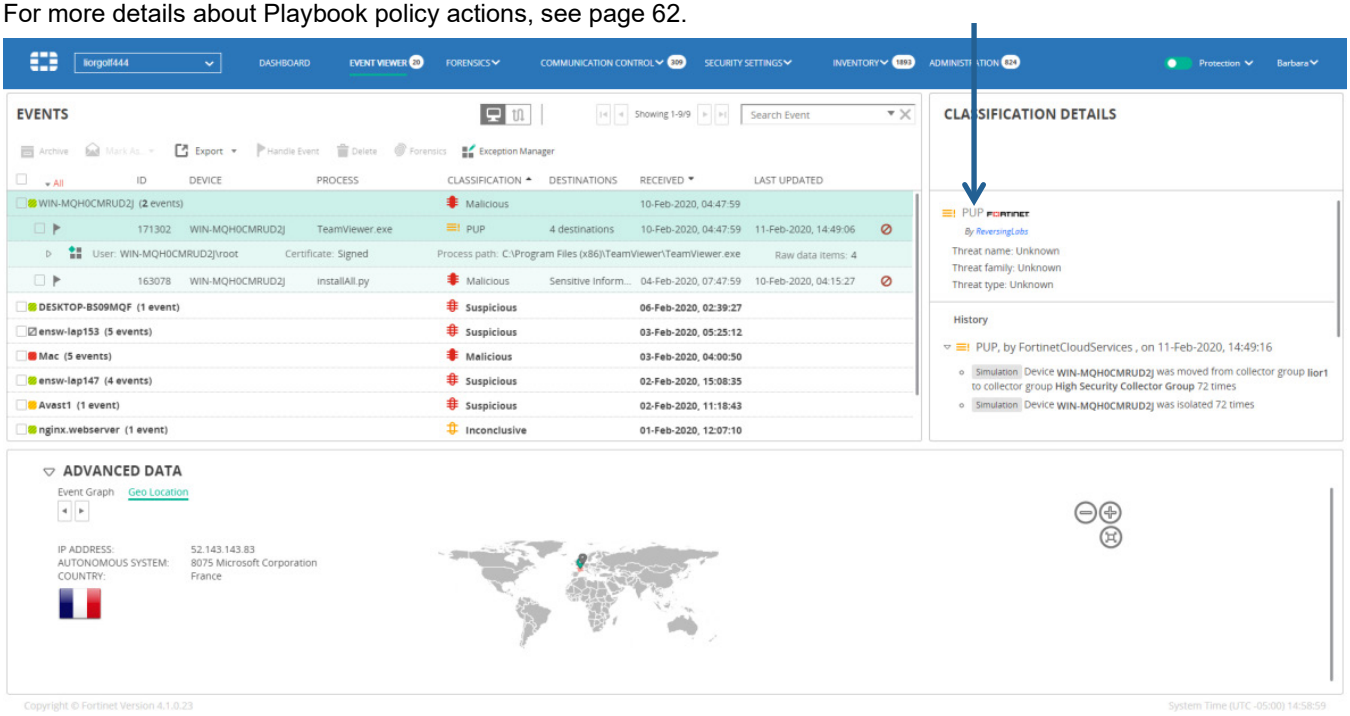
1. Select the rule's checkbox and then click the Handle event button or just click the flag icon of the event row. The Event Handling window displays.
2. In the **Classification** dropdown list, change the classification for the event, as needed.



3. Click the Save button.

[Optional] Click the Save and Handled button to mark the event as handled after saving the event.

After changing the classification of an event, the Classification Details area 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 page 62.



When the Fortinet logo appears next to an entry in the CLASSIFICATION DETAILS area, it indicates that the event was automatically classified by FortiEDR. Events that are manually classified do not display the Fortinet logo.

Note – Notifications for events are not shown in the Classification Details area.

Defining Event Exceptions

The following describes how to create a new exception and how to edit an existing one. Details describing how to edit an existing exception are described in the *Editing Event Exceptions* section on page 102. You can access the Exception Manager by clicking the Exception Manager button at the top of the Events pane. Additional options for managing exceptions are provided in the **POLICIES** tab, as described on page 66.

An exception that applies to an 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 page 59.

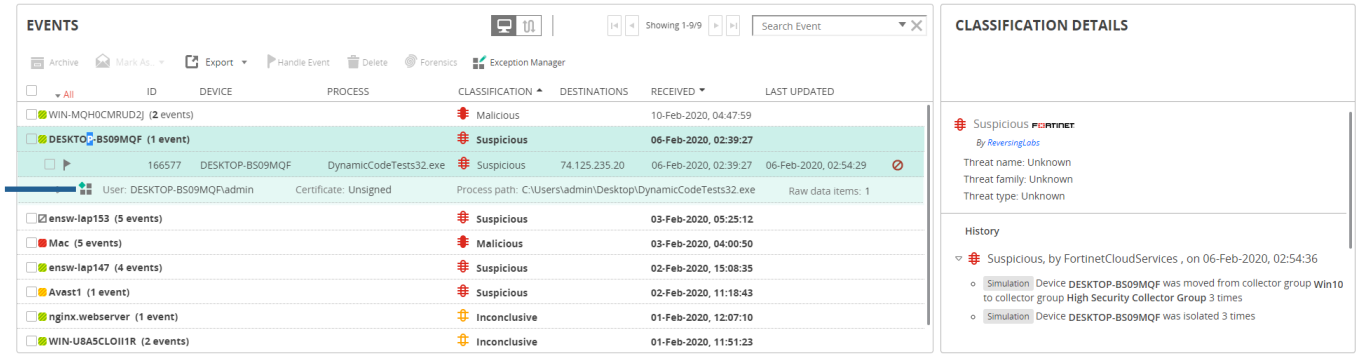
Note – After an exception is defined for an event, new **identical** events are not triggered.

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 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).

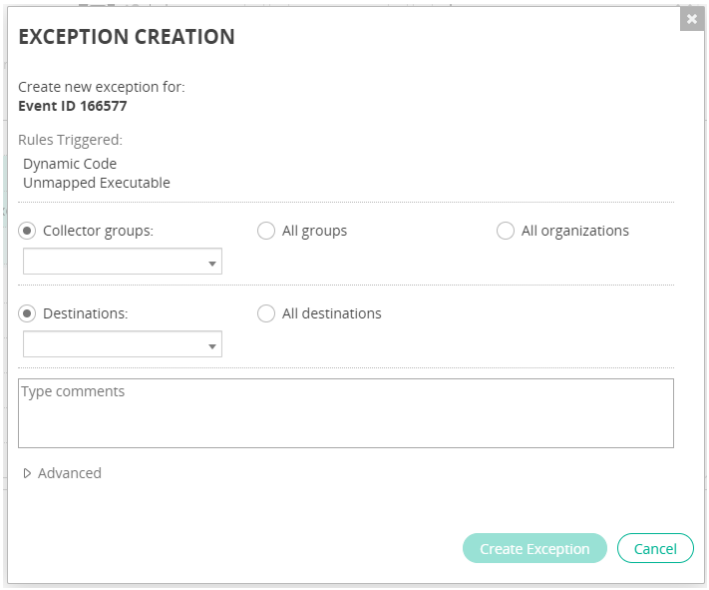
Note – When defining an exception for *Listen on Port Attempt* events, listening on 0.0.0.0 means listening on all interfaces. In such cases, you should use *All Destinations*.

To define an event as an exception:

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



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



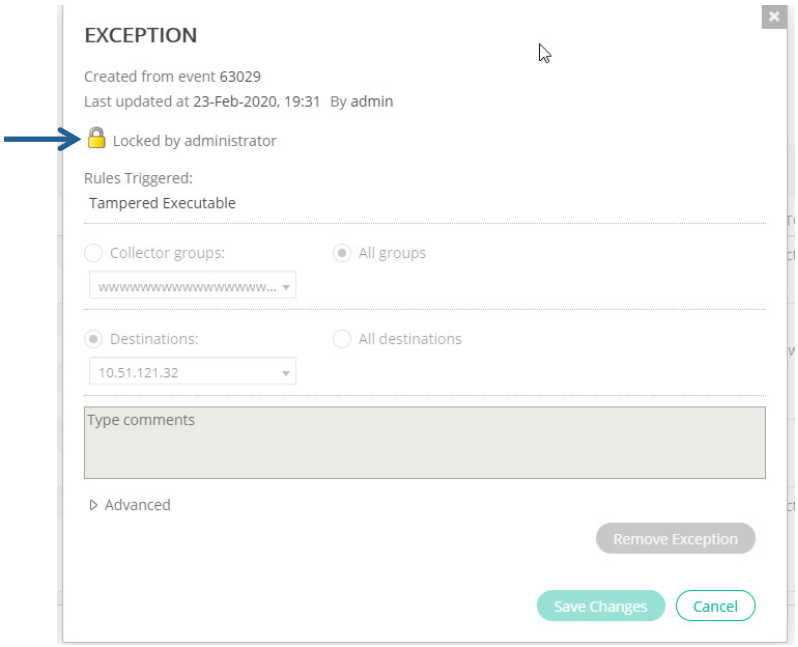
3. Specify whether this exception applies to all the Collector Groups or only to the Collectors in the same Collector Group as the one for which this event was triggered.

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

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 event already occurred.

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.

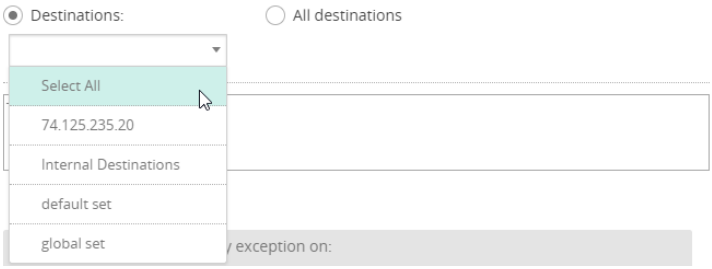
Exceptions defined by an Administrator (Hoster) that apply to all organizations display as *Locked by the administrator* to other users, and cannot be changed by a user other than the Administrator who created it, as shown below:



Note – The **All organizations** option does not display for Local Administrators or regular users. Only an Administrator can set the **All organizations** option.

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 IPs listed in the dropdown menu are those IPs that generated connections for this event. Use the dropdown menu to select the specific IPs to exclude that were triggered on this event, which can be either internal or external.

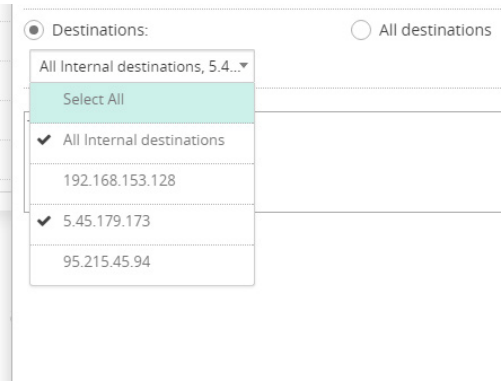


To apply the exception to a specific destination(s), select from the following options:

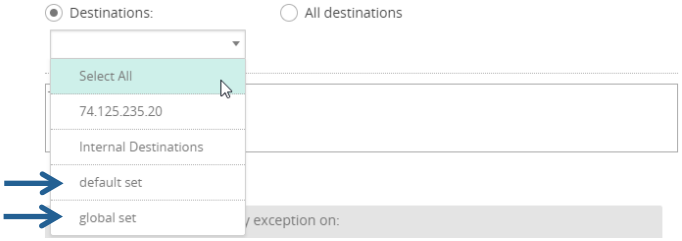
- **Select All:** Applies the exception on all destinations that were seen as part of this event. If there will be an identical violation (the same set of rules will be violated on this process) but the connection attempt will be to a different IP, than the event will be triggered. To exclude this event completely from being triggered in the future you can select the **All Destinations** radio button.

- **Internal** Destinations: 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:
  - Loopback addresses: 127.X.X.X, 0:0:0:0:0:0:0:1 and 0:0:0:0:0:FFFF:7f
  - 10.0.0.0 –10.255.255.255
  - 192.168.0.0–192.168.255.255
  - 169.254.0.0–169.254.255.255
  - 172.16.0.0 - 172.31.255.255
  -
  - IPV6: fc00:: – fd00:: :: or fe80

  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.
- **<IP Address>:** Applies the exception to the selected IP address. You can select multiple IP addresses.

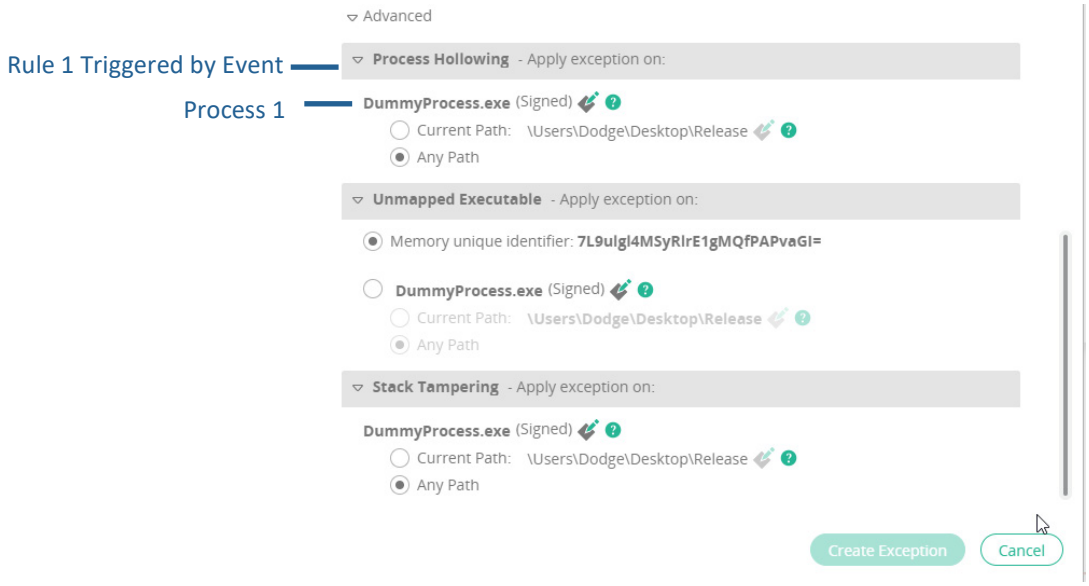


- **<IP Set>:** An IP set defines a set of IPs to be included or excluded from an event. When you select an IP set here, it means that an exception is applied only to a device that has one of the IPs specified in the IP set. IP sets can only be defined by an Administrator, as described on page 174.



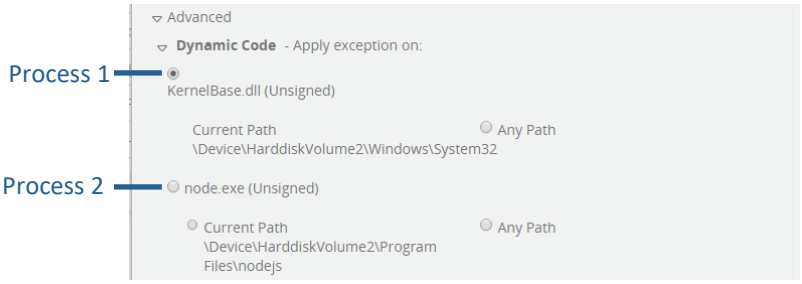
5. Fill in a description of the exception.

6. In the **Advanced** 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 event, as displayed in the window. When you select **Any Path**, the process triggers the exception no matter from where it is running.



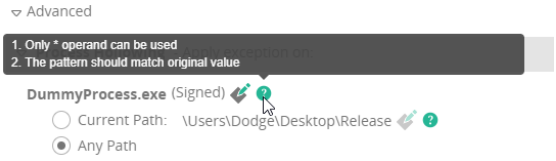
You can define an exception so that an event is triggered, based on a complex set of conditions. For example, you can define an exception so that an event is triggered when a specific process (B) is executed by another process (A). For example, you can limit an exception so that it applies only when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



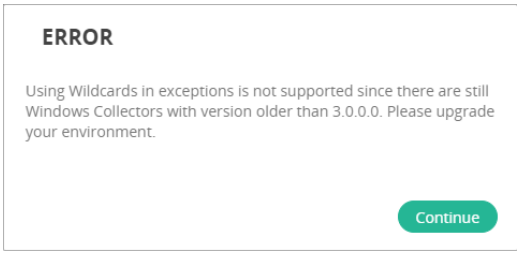
You can also define an exception specifying that an exception is triggered only when both processes are running.

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



Beginning with V3.0, you can edit the process path and file name. Wildcards can be used for this purpose.

Note – 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:

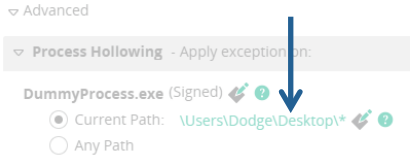


You can only edit the process path or file name when selecting the **Current Path** option. To do so, click the adjacent **Edit** button, and then edit the process/file name as needed. When doing so, the following conditions apply:

Path

- Only an asterisk (*) character(s) can be added.
- Do not change the displayed path. Otherwise, it will no longer match. However, you can replace a piece of the string with an asterisk (*).
- Only a single asterisk character (*) is permitted between two consecutive path separators (/).
- The number of separators (/) in the displayed path must remain the same.
- **File Name**
- Only an asterisk (*) character(s) can be added.
- Do not change the file name. Otherwise, it will no longer match. However, you can replace a piece of the string with an asterisk (*).
- Only a single asterisk character (*) is permitted.

When a wildcard is used as part of the process path or file name definition, the entry displays in green, as shown below:



7. Click the **Create Exception** button.

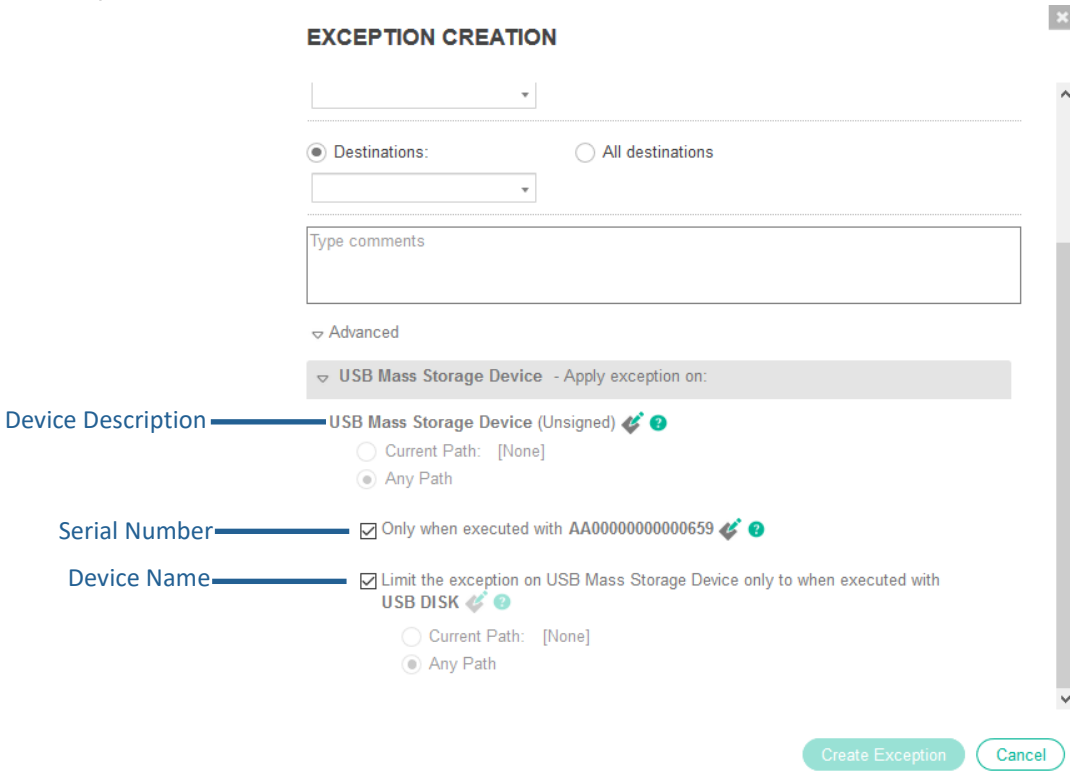
Note – If this exception was created previously, the **Remove Exception** button appears enabling you to delete the exception.

Device Control Exceptions

Exceptions on device control 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**.

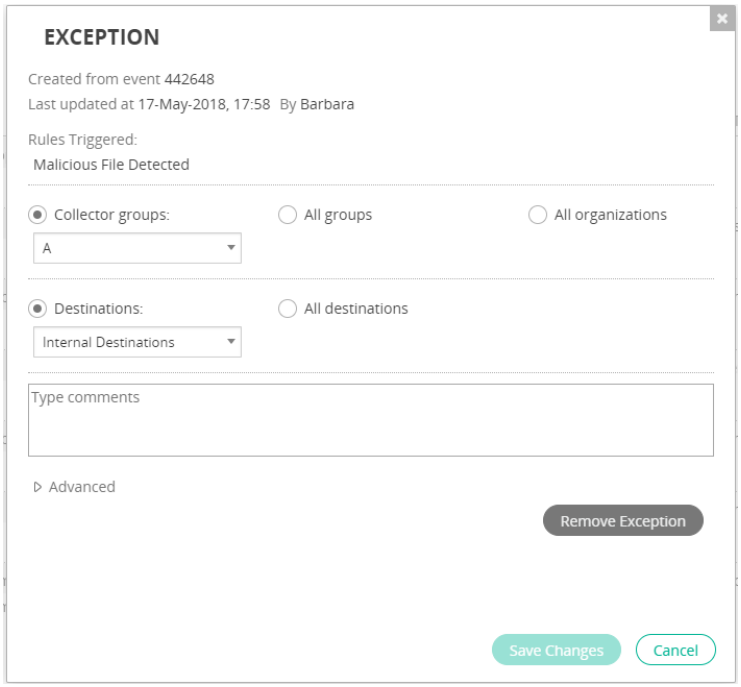
For example:



Editing Event Exceptions

To edit an event exception:

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



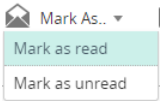
2. Modify the Collector Groups and Destinations to which the exception applies and the pairs of rules and processes that operate together to define an exception in the **Advanced** area, as needed. For more details, see page 98.

   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 event already occurred.
3. Click the **Save Changes** button.

Marking an Event as Read/Unread

The following describes how to specify that you have viewed an event. This does not mean that the event has been handled (page 95). When any FortiEDR Central Manager user marks an event as Read, all users see it as having been read. Unread events are displayed bold.

To mark an event as having been viewed:

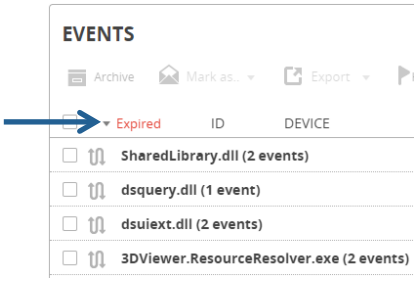
- Select the rule's checkbox and then click the 

button and then select **Mark as read**. The event row text is no longer displayed bold.

Viewing Expired Events

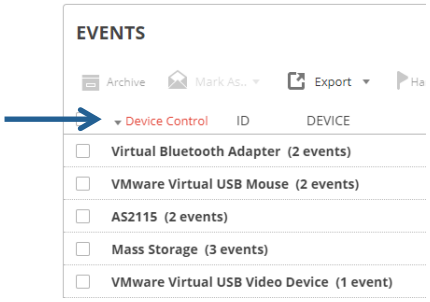
Events in the Event Viewer can be filtered to show only expired events. Expired events are events that the system has determined as *safe*. As such, these events are only triggered once and then saved internally in the system. There is no need to define an exception for them. Expired events cannot be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

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

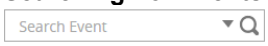


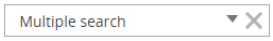
Viewing Device Control Events

Events in the Event Viewer can be filtered to show device control events. Device control 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 events are displayed separately from other security events. Defining an exception for them can be done in a similar manner as for other events. The exception can be set on the device name, vendor, serial number or a combination.

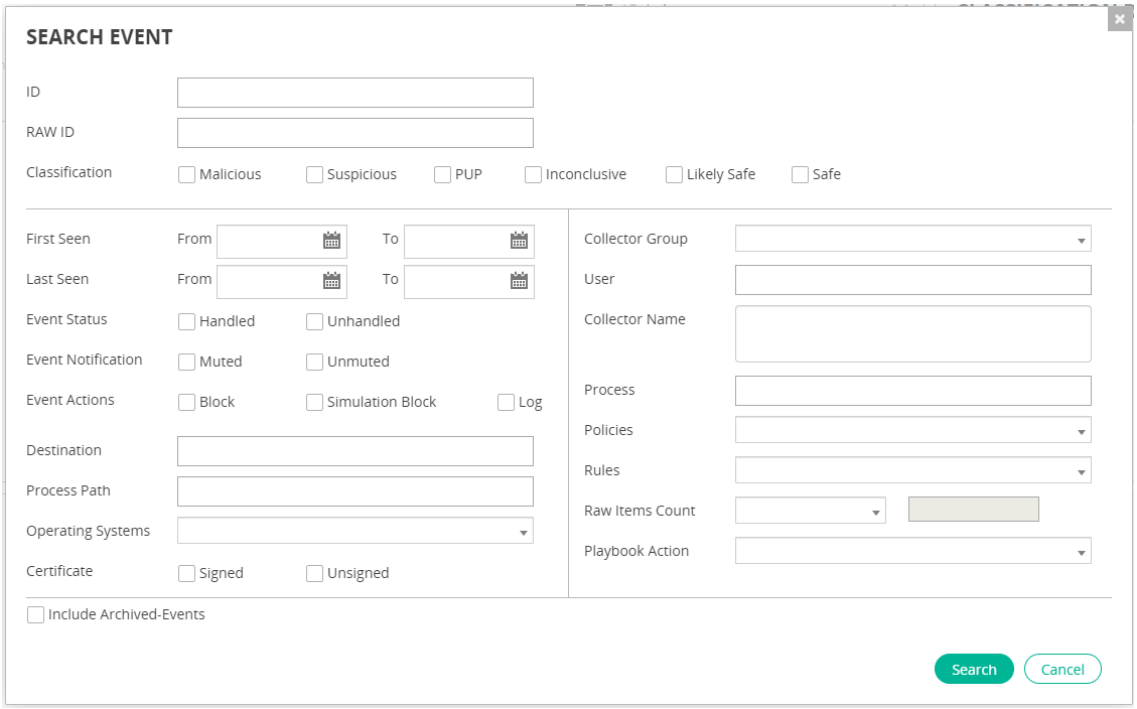


Other Options in the Event Viewer

- **Sorting Events:** Click any column name to sort 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.
- **Searching For Events:** Click the down arrow in the **Search Event** field to display a variety of search options 

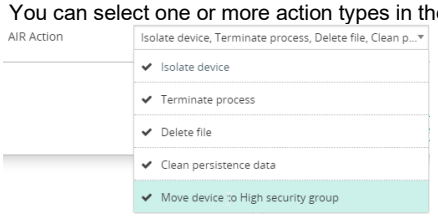
. When the Event Viewer display is filtered by a search, the **Search Event** field displays the words **Multiple search** 

. Click the ✕ to redisplay all the events (unfiltered).



Note – The **User** field refers to the employee's username on the computer and on the FortiEDR Manager.

You can select one or more action types in the **AIR Action** dropdown list.



- **Exporting Events:** Click the Export button to export the selected events to Excel or PDF.
- **Archiving Events:** Click the Archive button to archive the selected events. These events are not deleted. You can display them using the **Search** option (described above) and selecting the **Included Archived Events** option.

  Note – To unarchive an event, click the **Unarchive** button, and then confirm the unarchive action in the window that displays.
- **Deleting Events:** Click the Delete button to completely delete an event from the FortiEDR system.

  Note – A deleted event cannot be restored or retrieved. Unless you are having storage capacity issues, we highly recommend just hiding events and not deleting them.
- **Forensics:** The optional FortiEDR Forensics add-on enables you to perform deep analysis of security events, as described on page 130.
- **Exception Manager:** Click the Exception Manager button to access the Exception Manager, as described on page 59.

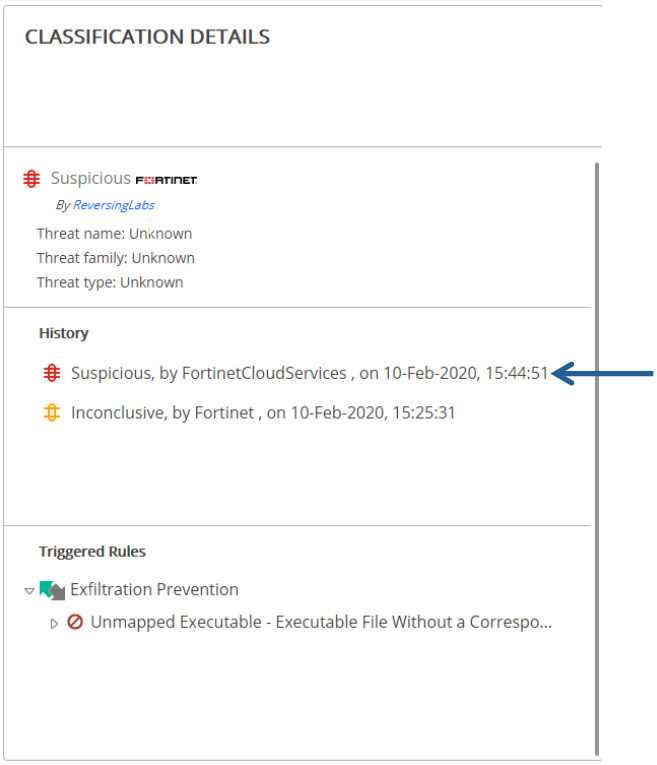
Classification Details

The Classification Details area displays the classification, policy and rules assigned to the FortiEDR Collector that triggered this event.

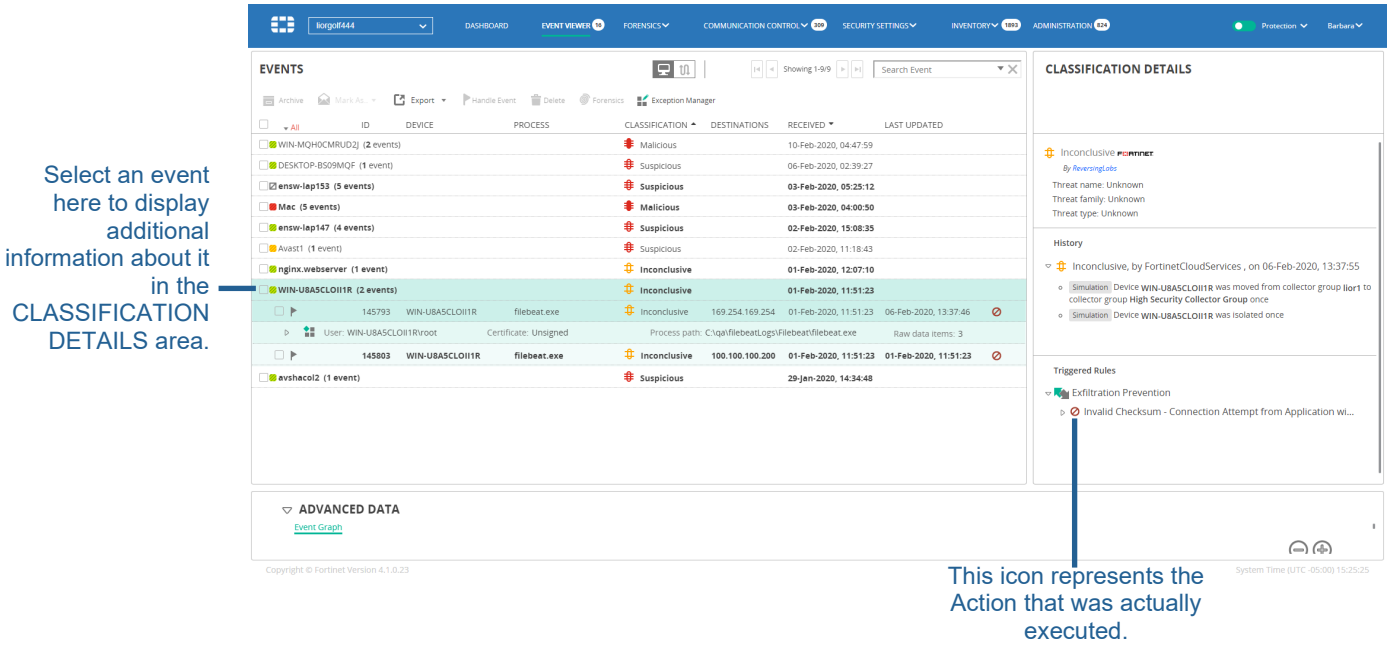
Click the **History** down arrow to display the classification history of an event. The classification history shows the chronology for classifying the event, and the actions performed by FortiEDR for that event. This area also displays relevant details when the FortiEDR Cloud Service (FCS) reclassifies an event after its initial classification by the Core.

All FortiEDR actions are based on the final classification of an event by the FCS. The FCS is a cloud-based, software-only service that determines the exact classification of 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 59.

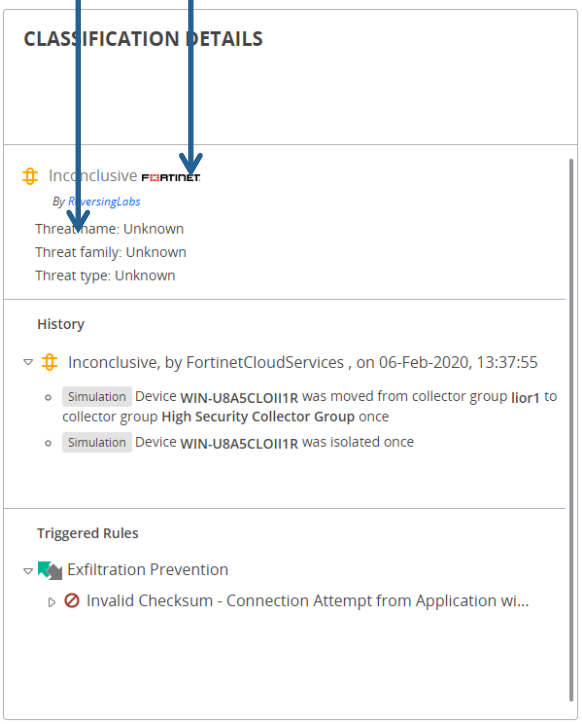
For example, the following example shows that the event was reclassified by the FCS and given a notification status of Suspicious at 15:44:51.



In the Triggered Rules area, 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.



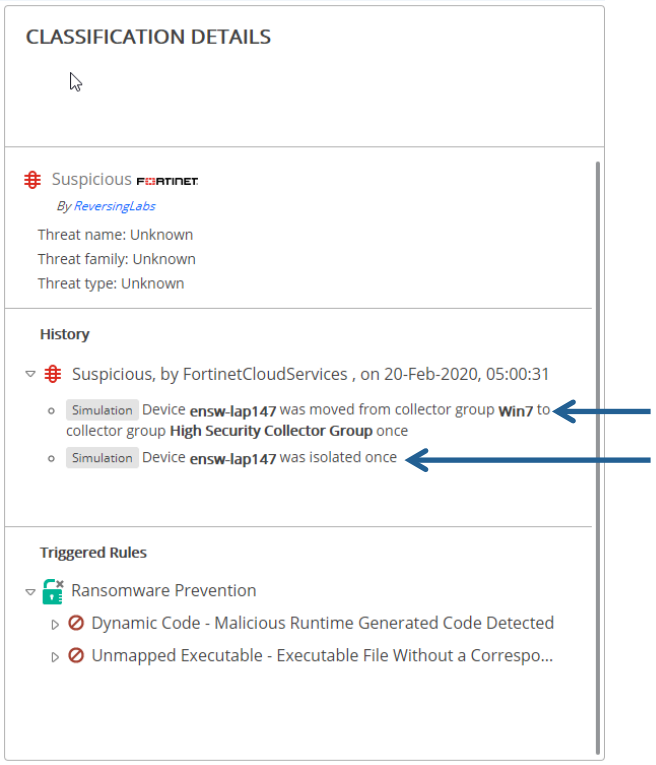
Each entry in the CLASSIFICATION DETAILS area displays the threat name, threat family and threat type. If threat intelligence data is available for the threat, it displays as well.



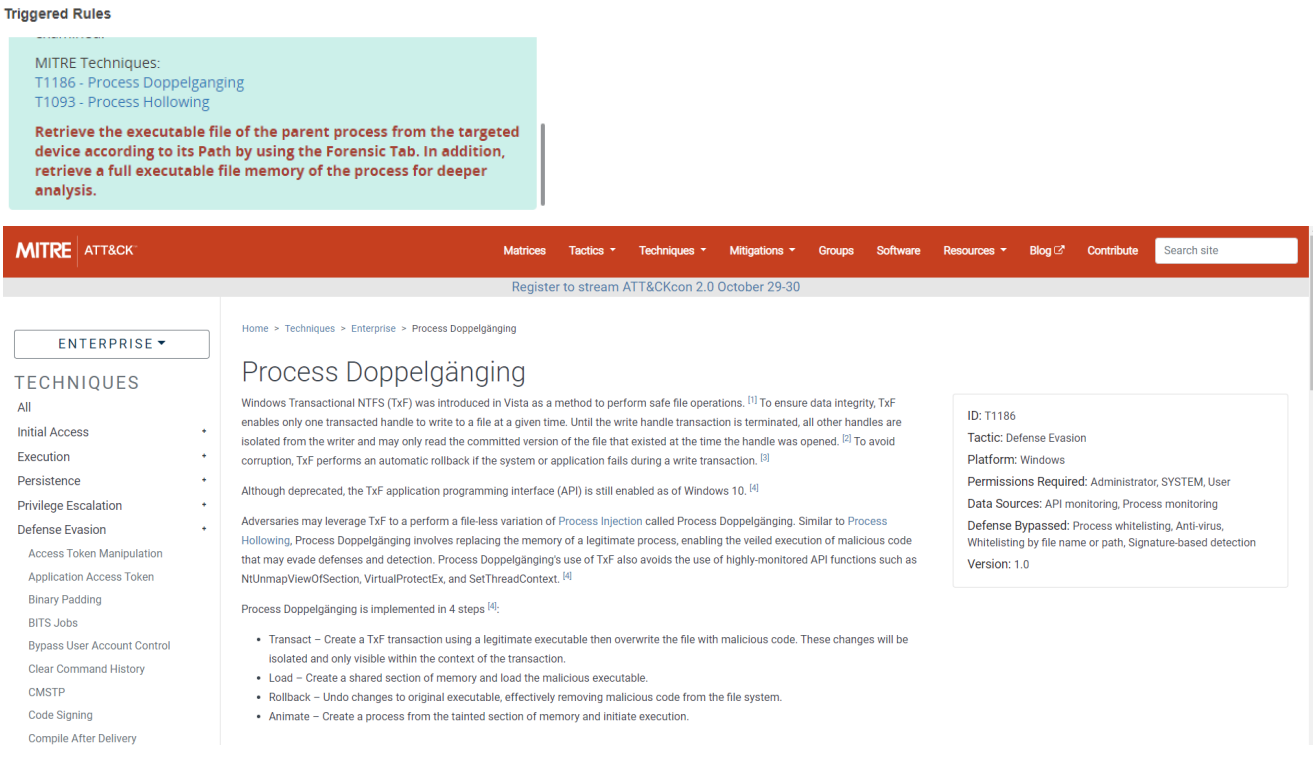
When the Fortinet logo appears next to an entry in the CLASSIFICATION DETAILS area, it indicates that the event classification is the one that was automatically added by FortiEDR. Events that were manually classified do not display the Fortinet logo.

Click the **Reversing labs** link to access an external site, which displays more details about the classification process. 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 an event is set to Simulation mode, then the event action is documented in the Event Viewer, but is not performed. Such events display (simulation) in the History section of the Classification Details area, as shown below:



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



Chapter 7 – 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 outside of the organization.

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 (whitelist). After the whitelist of communicating applications is defined, only applications in the whitelist can communicate externally. If an attacker abuses an application in the whitelist, FortiEDR's patented technology (Exfiltration and Ransomware prevention policies) blocks the communication and displays an 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 from communicating outside your organization.

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.

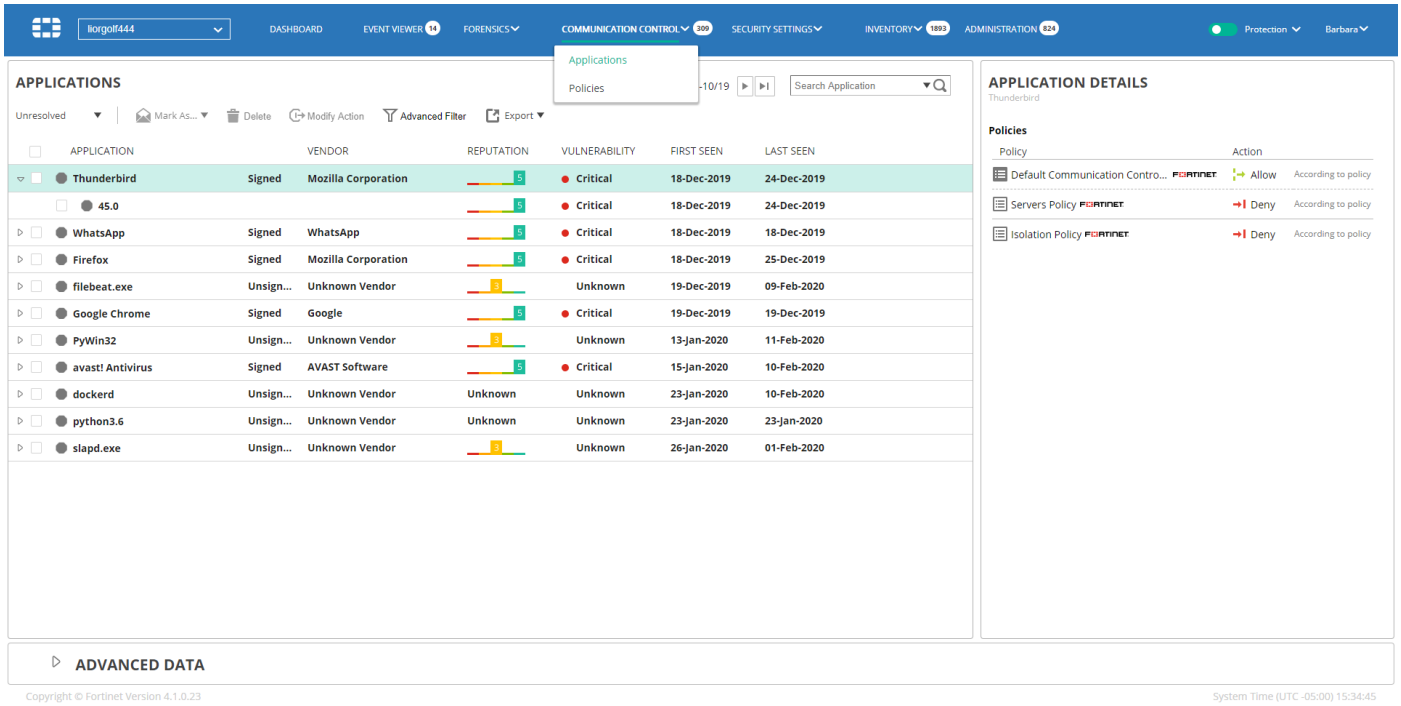
Moreover, FortiEDR Communication Control provides data and tools for efficient vulnerability assessment and control. Virtual patching is made possible with Communication Control policies that can be configured to automatically block connections from vulnerable applications.

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

- **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.

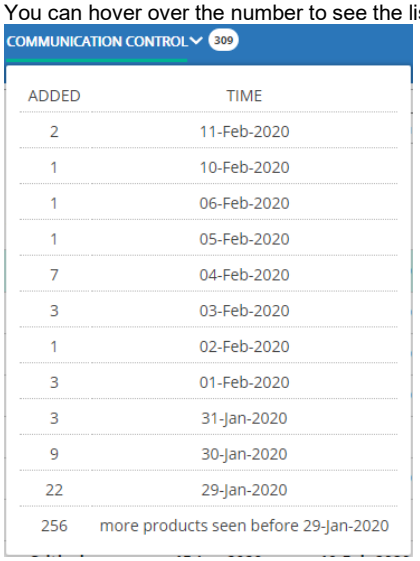
Introducing Communication Control

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**.



Note – 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.

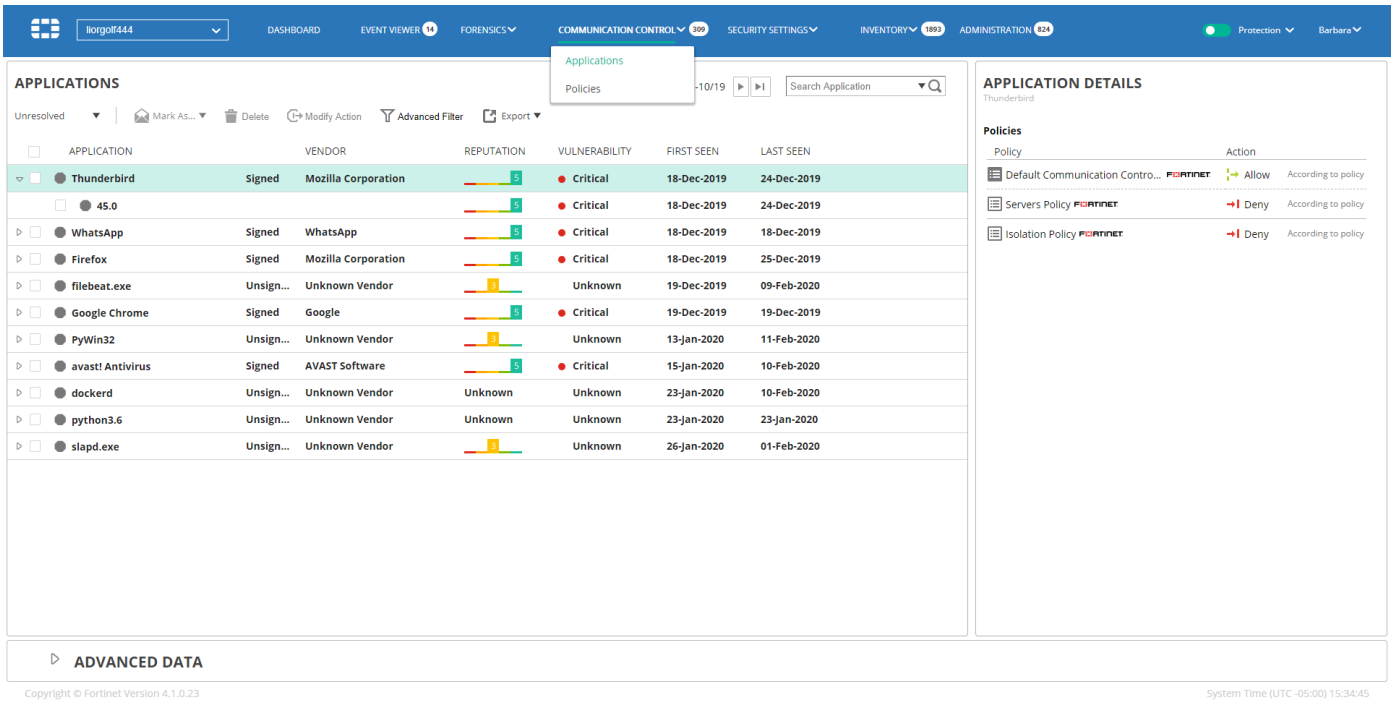


The **Communication Control** tab contains two main pages:

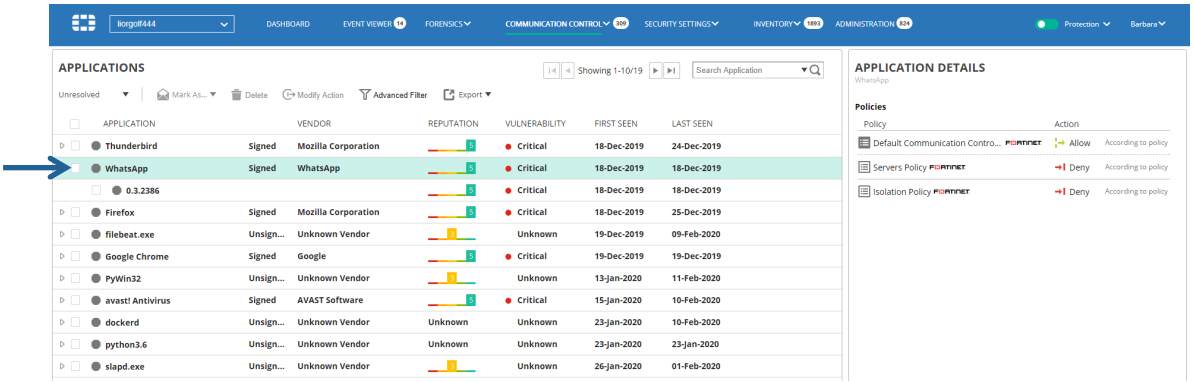
- **Applications,** page 112
- **Policies,** page 123

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.



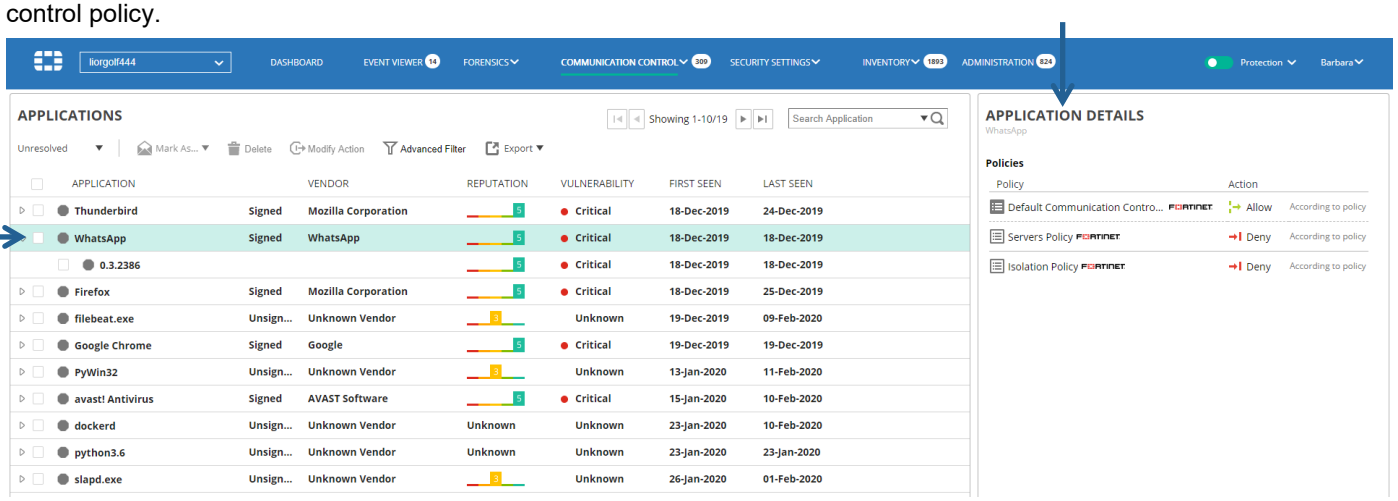
Information is organized hierarchically in a two-level tree. The first (top) level specifies the name of the application. The second level specifies the application **version**. For example, the figure below shows one version for the What'sApp application.



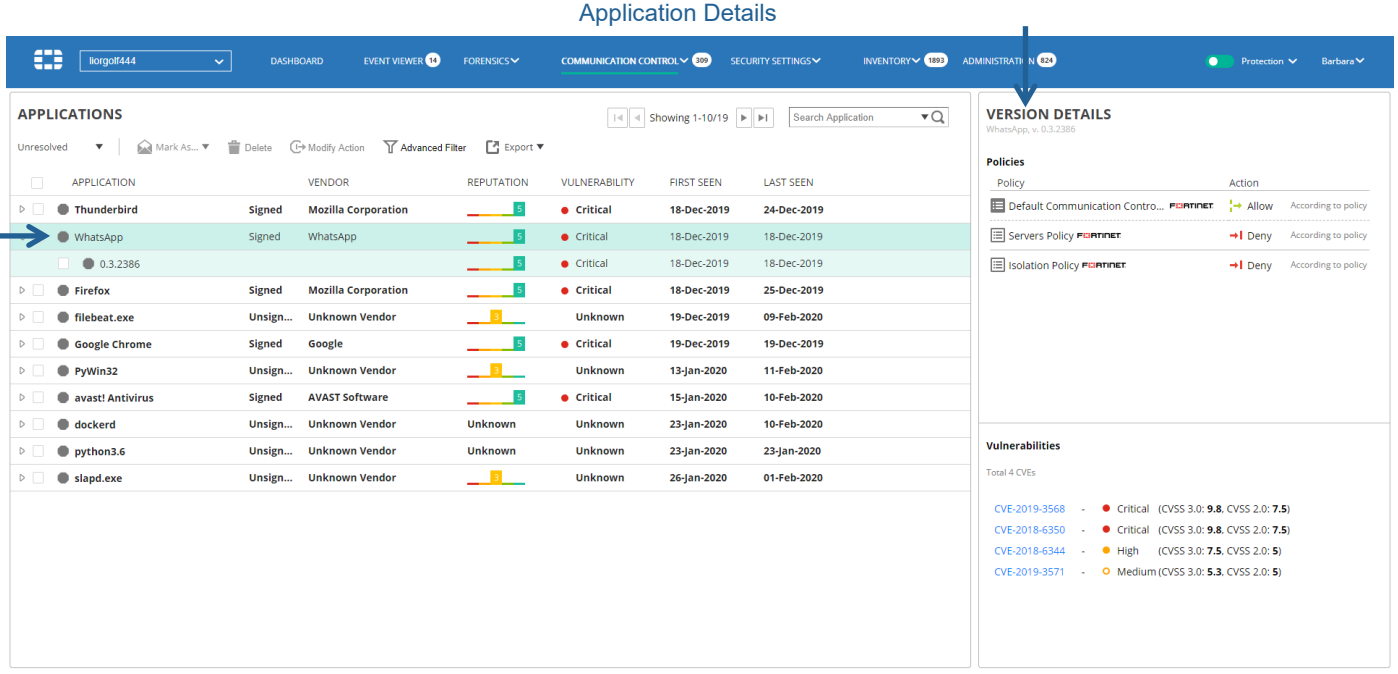
The following information displays for each application in the application list:

- Selection checkbox
- Resolving status icon
- **Application/Version:** The name of the application/version.
- Signed/Unsigned indication
- **Vendor:** The application's vendor and certificate details.
- **Reputation:** The reputation score of the application. For more details, see page 113.
- **Vulnerability:** The highest CVE vulnerability score for the application. For more details, see page 114.
- **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.



Application Details

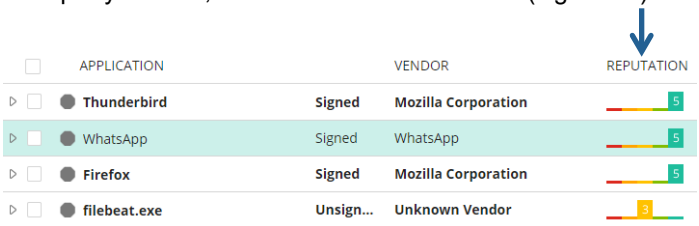


Version Details

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 page 119.

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.



Reputation scores use the following range to indicate the reputation for an application:

- **1:** Known as bad
- **2:** Assumed as bad
- **3:** Unclear, indicating a contradiction or inability to determine the reputation
- **4:** Assumed as good
- **5:** Known as good

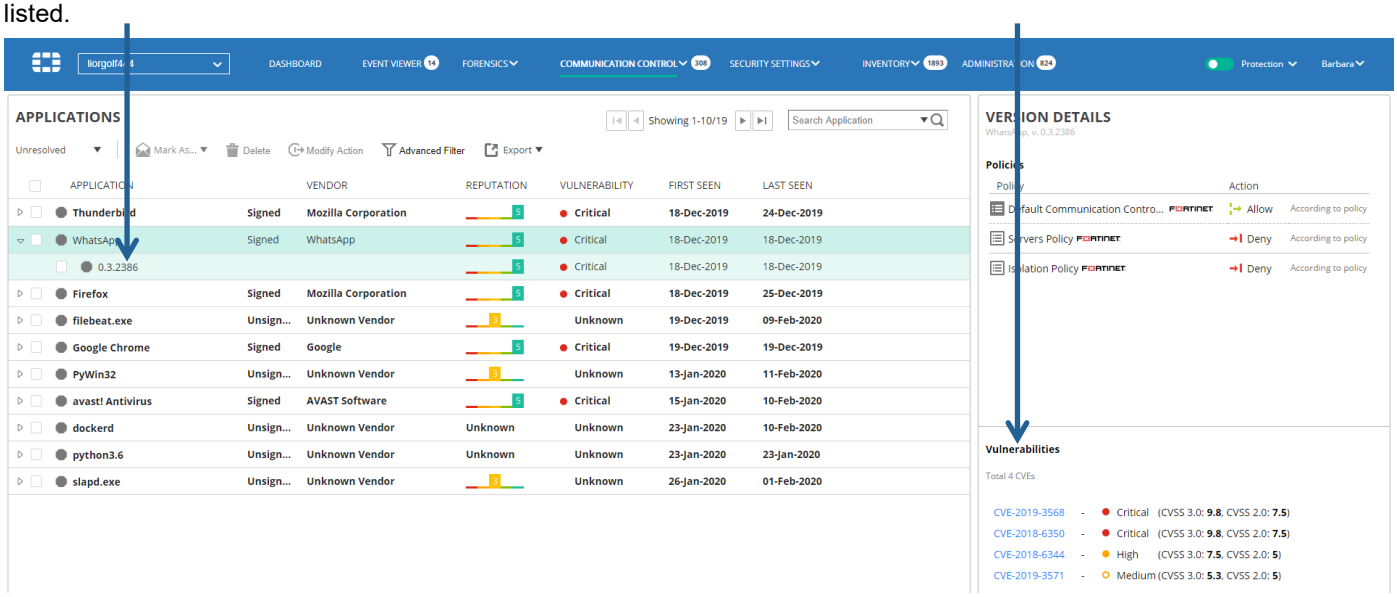
The Reputation indicator displays **Unknown** if the reputation score is unknown.

Vulnerability

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

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

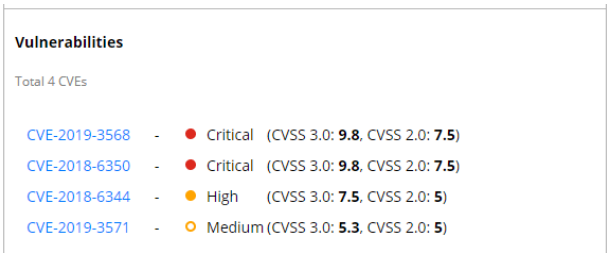
FortiEDR categorizes applications/versions based on the Common Vulnerability Scoring System (CVSS) CVE scheme, which is commonly used worldwide. FortiEDR's vulnerability scoring system provides a useful tool for vulnerability assessment, and enables you to review the weaknesses detected in your environment 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.



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

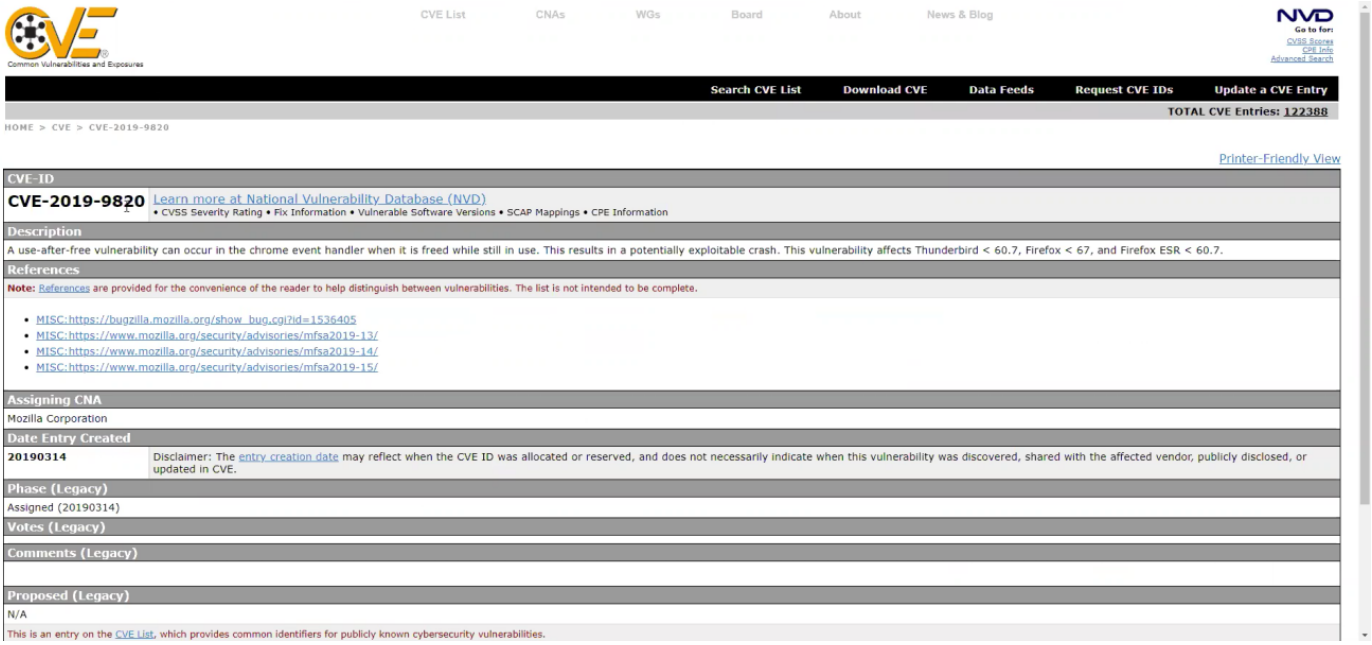
- Unknown
- Low
- Medium
- High
- Critical

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.



Note – 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.



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 page 123. The information presented in the Advanced Data area of the window also provides useful information to help protect against vulnerabilities. For more details, see page 119.

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. Applications can also be changed to the Resolved status by the user, as described on page 116.

Sorting the Application List

The application list can be sorted alphabetically by product, vendor, reputation score, vulnerability or arrival time (first seen or last seen). By default, the list is sorted by arrival time, with the most recent communication at the top.

Marking an Entry as Read/Unread

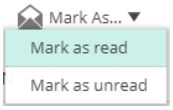
The following describes how to specify that you have viewed an entity in the application list. You can mark applications or versions as read/unread.

The first time that an application/version is detected in the application list, it is shown in **bold**. **Bold** indicates that the item is unread (see below).

APPLICATION		VENDOR	REPUTATION	VULNERABILITY	FIRST SEEN	LAST SEEN
Thunderbird	**Signed**	**Mozilla Corporation**	5	**Critical**	**18-Dec-2019**	**24-Dec-2019**
WhatsApp	Signed	WhatsApp	5	Critical	18-Dec-2019	18-Dec-2019
Firefox	**Signed**	**Mozilla Corporation**	5	**Critical**	**18-Dec-2019**	**25-Dec-2019**
filebeat.exe	**Unsign...**	**Unknown Vendor**	3	**Unknown**	**19-Dec-2019**	**09-Feb-2020**
Google Chrome	**Signed**	**Google**	5	**Critical**	**19-Dec-2019**	**19-Dec-2019**

To mark an entity as read:

- Select the entity's (application or version) checkbox and then click the down arrow on the Mark As... button and select **Mark as read**. The text no longer displays in bold.

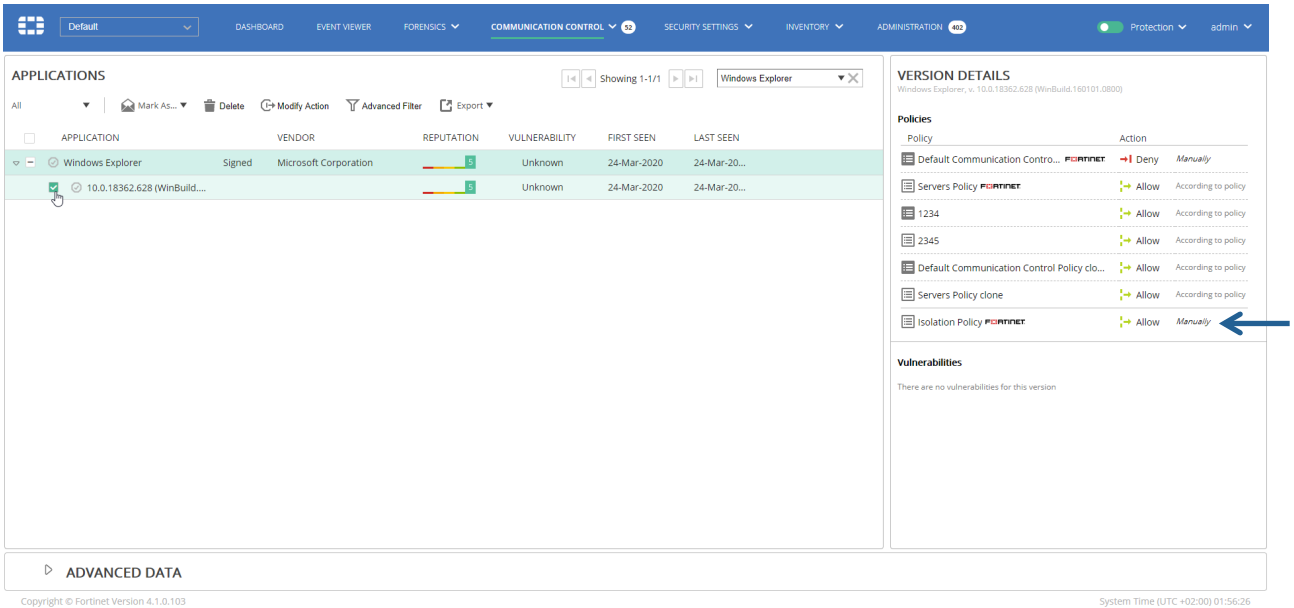


Note – If you mark an application version as read, all lower levels in the version hierarchy for that application are also marked as read.

Modifying a Policy Action

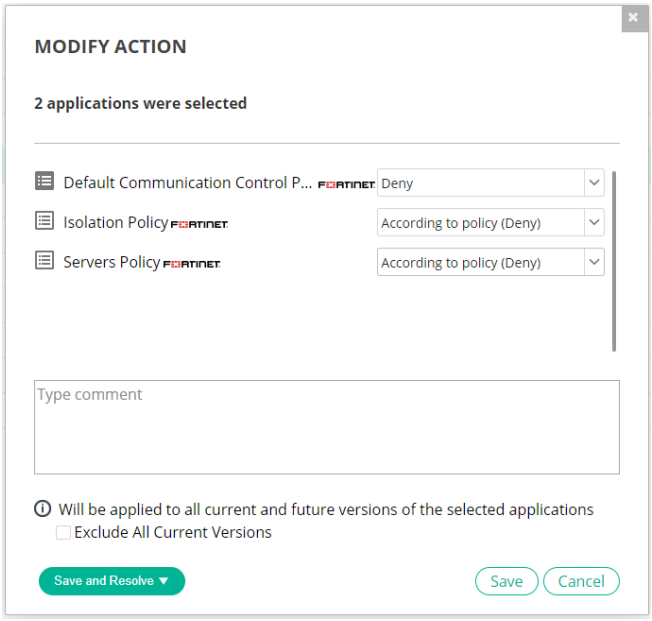
The following describes how to apply a different action to an application/version other than that specified in the current policy for that application/version. In this case, the application/version is excluded from the current action defined in the policy (Allow or Deny).

When modifying a policy action in this manner, the Application/Version Details area displays **Manually** to indicate that the action was modified manually, and is excluded from the action defined in the policy.

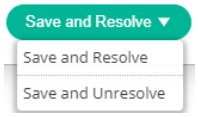


To modify a policy action:

1. Select the application/version checkbox and then click the Modify action button. The Modify Action window displays.



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.

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 

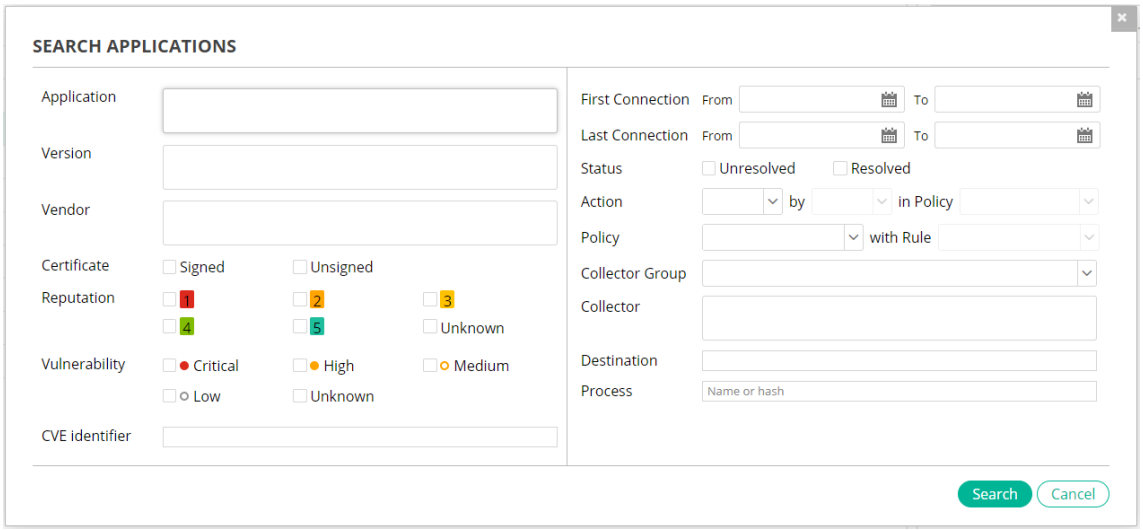
button to save the new communication control decision for the selected application(s).

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.

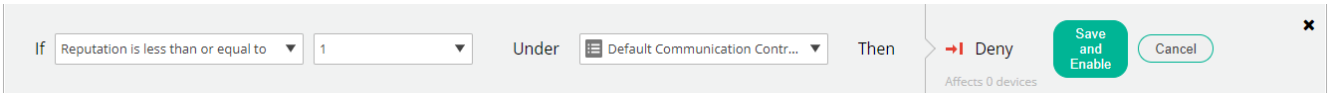


You can filter the application list by the following criteria:

- **Application:** Filters by application name application.
- **Version:** Filters by version. This is a free-text field.
- **Vendor:** Filters by vendor name.
- **Certificate:** Filters by signed or unsigned certificate.
- **Reputation:** Filters by reputation score. Check the checkbox(es) for the reputation score(s) of interest.
- **Reputation:** Filters by reputation score.
- **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 Applications Pane

- All : Click the down arrow in the All button and then select an option in the dropdown list to filter the application list accordingly. You can filter the list by:
  - **All:** Lists all applications for the organization.
  - **Unresolved:** Lists applications that have not been resolved by either the user or FortiEDR. Applications with this status are indicated by the icon in the application list. This is the default filter.
  - **Resolved:** Lists applications that have been resolved by either the user or FortiEDR. Applications with this status are indicated by the icon in the application list.
  - **Unknown Vendors:** Lists applications whose for which the vendor is not known in the system.
  - **Low Reputation:** Lists applications with a low reputation score.
  - **Critical CVE:** Lists applications with a Critical CVE score.
  - **Unread:** Lists applications that have not yet been viewed in the application list.
- Mark As... : Click the down arrow on the Mark As... button and then select **Mark as read** or **Mark as unread**. For more details, you may refer to the *Marking an Entry as Read/Unread* section on page 116.
- Delete: Click to delete the entity selected in the application list. Note that if the deleted entity attempts external communication again, it will be added back to the application list. In this case, any action defined in the policy for this entity must be redefined.
- Modify action: Click the button to change the current policy action to be applied for the selected entity, as described on page 116.
- Advanced filter: Click the advanced filter to review applications by suspicious characteristics, such as existing vulnerabilities or reputation score. This filter can be used to set up policy rules. See page 127 for more details.



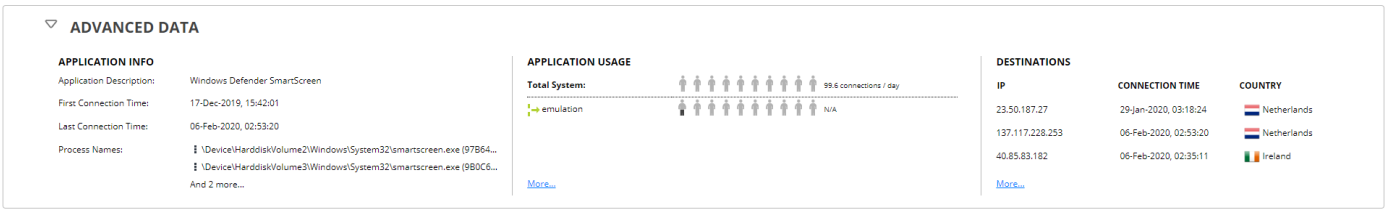
- Export : Click the down arrow in the Export button and select the format for exporting data. You can select **PDF**, **Excel** or **JSON**.
- Search Application : Use the **Search Application** field to perform an advanced search, as described in the *Searching the Application* List section on page 118.

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

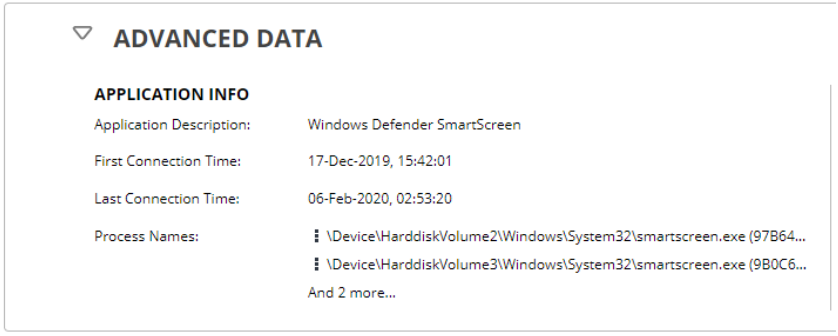
When an application is selected in the application list, the Advanced Data area displays the following information for it:



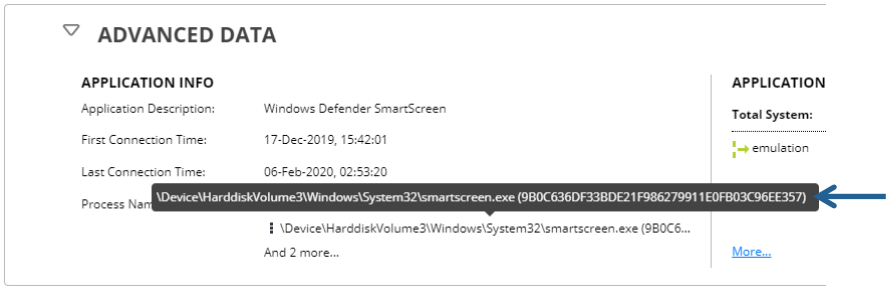
- **Application Information,** page 120
- **Application Usage,** page 120
- **Destinations,** page 121

Application Information

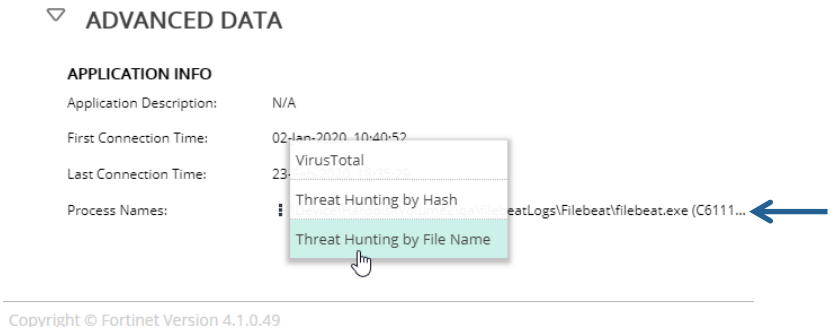
The Application Information area displays summary information about the selected application.



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.

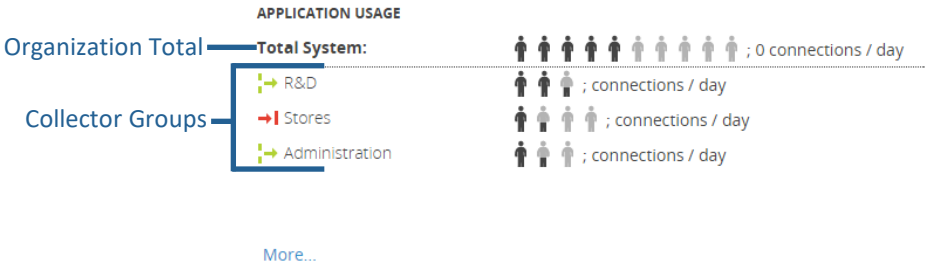


You can click the three dots next to the **Process names** field to navigate to the Threat Hunting window for that process name or hash, or to explore the hash in VirusTotal, as shown below:



Application Usage

The Application Usage area displays details about usage of the selected application.

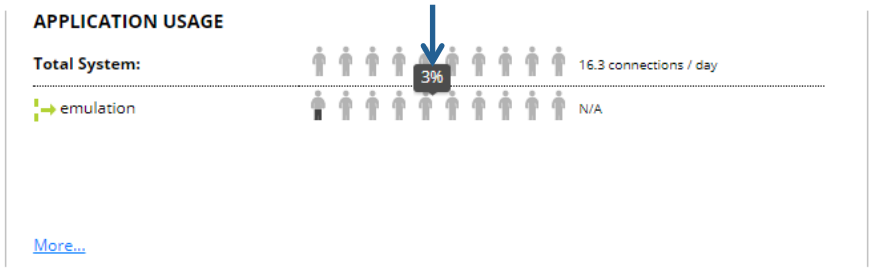


This area shows the number of connections (communication sessions) per day. The top line shows the total number of devices within the organization on which the selected application is installed.

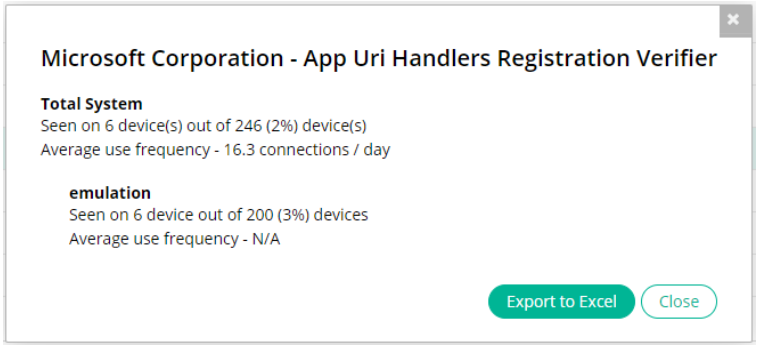
Each row below the underline represents a different Collector Group, and shows the number of devices in the organization in that Collector Group.

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.



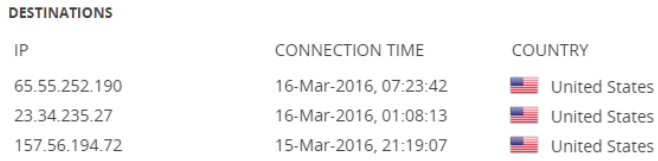
Click the **More…** link to open the following window, in which you can view additional details about the selected application.



Click the **Export to Excel** button in this window to export application usage information to Excel.

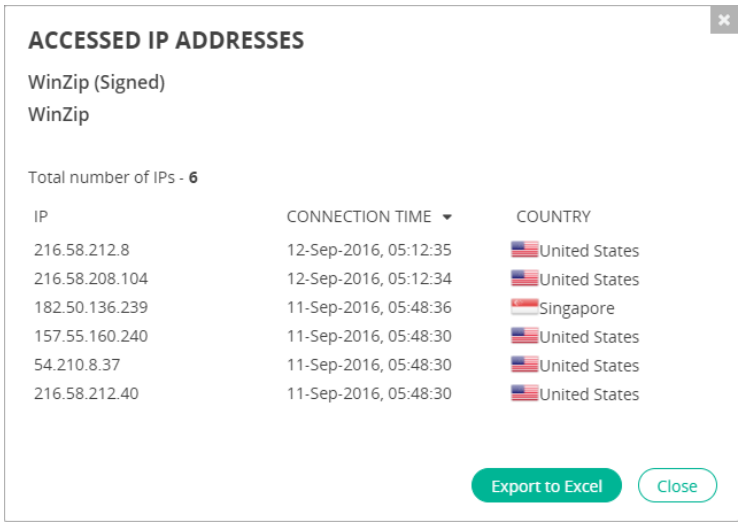
Destinations

The Destinations area shows the destinations to which the selected application communicated (Allowed) or attempted to communicate (Denied).



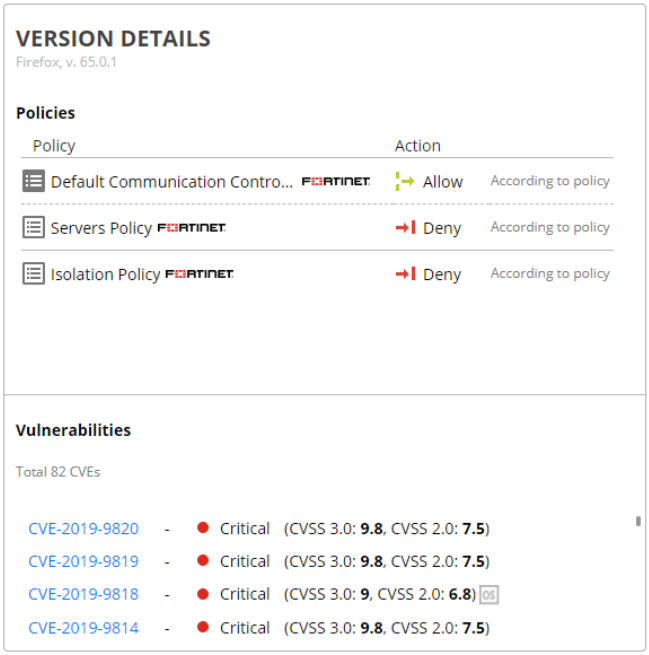
Each row shows the IP address, connection time and country of the destination.

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.



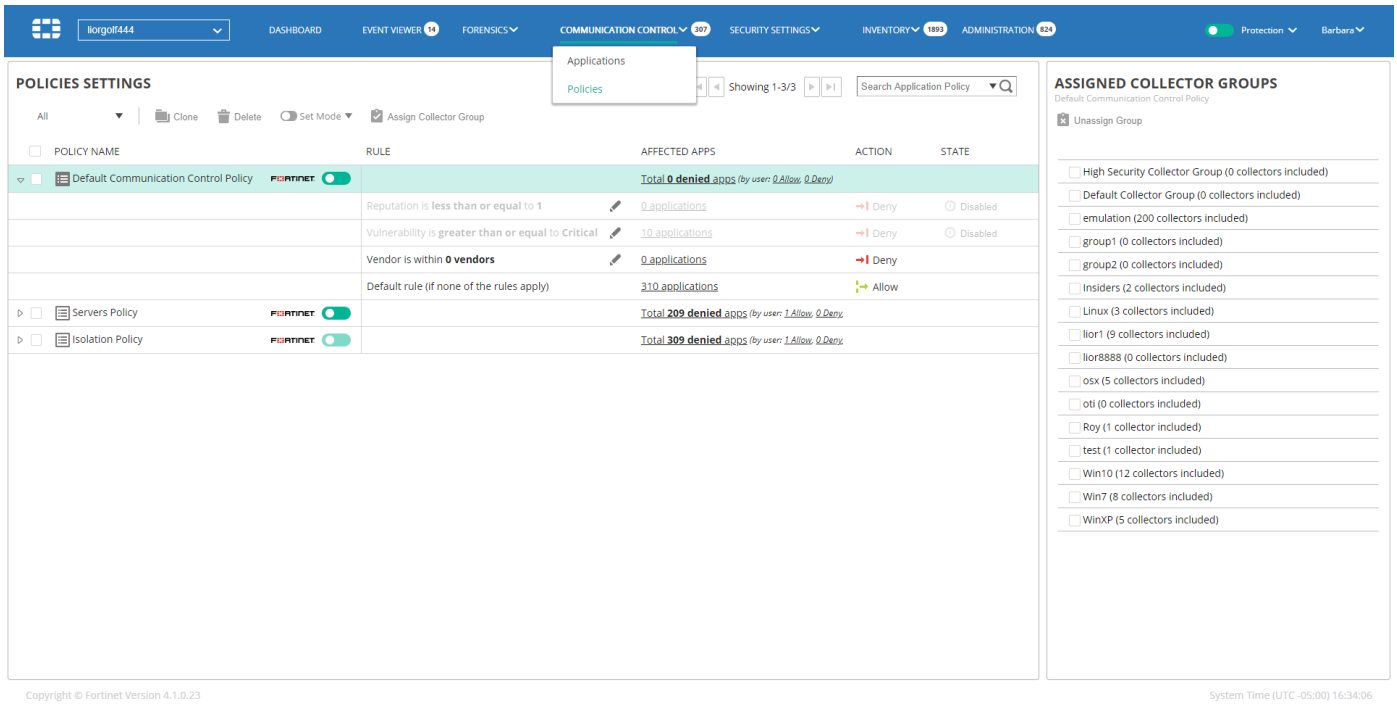
Version Details

The Version Details area displays the action defined for the application in each policy, plus its vulnerability details.



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**.

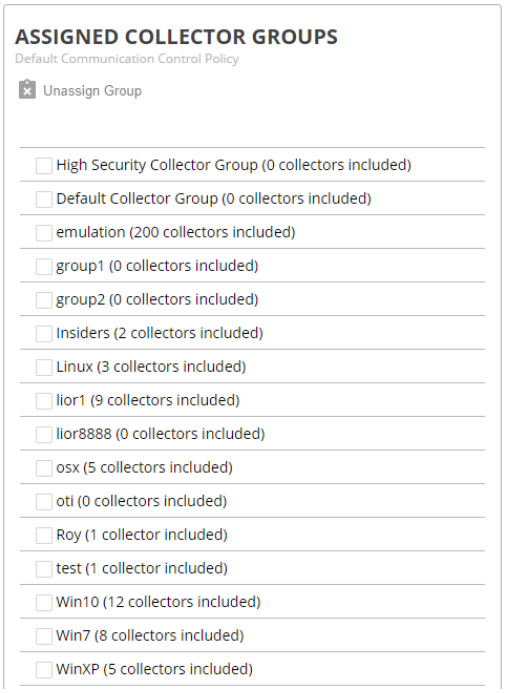


Communication Control policies define the actions to be taken for a given application or application version. Each policy applies to a different Collector Group(s), and all the devices that belong to that Collector Group(s). A Collector Group can only be assigned to one policy.

The following information is defined for each communication policy:

- **POLICY NAME:** The policy name appears in the leftmost column. The policy name is defined when the policy is created.
- **RULE:** The rule as it applies to the policy. The default action for the policy is displayed under the default rule of the policy. For more details, see the *Policy Rules* section on page 126.
- **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.



Predefined Policies

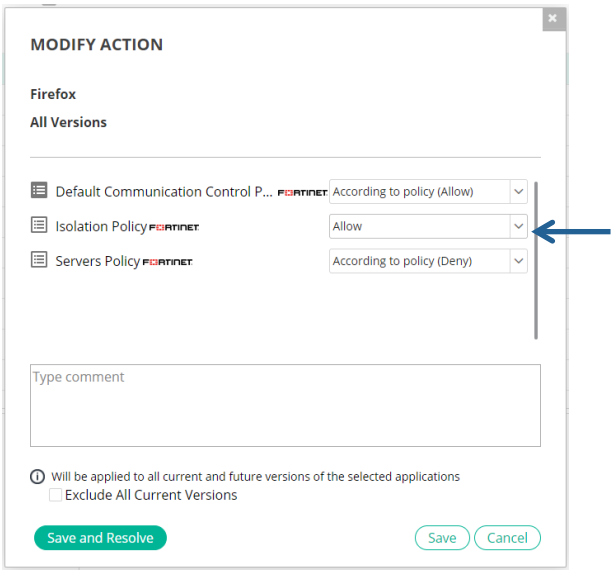
FortiEDR is provided out-of-the-box with several predefined policies, ready for you to get started. These policies are marked with the FORTINET logo. The **Default Communication Control** policy is one such policy, and is always listed first in the list of policies. The Default Communication Control policy is a blacklisting 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 a whitelisting policy that includes a list of known, recognized applications and a recommended action for each. FortiEDR identified these applications as legitimate and assigned an Allow action to them by default. 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:



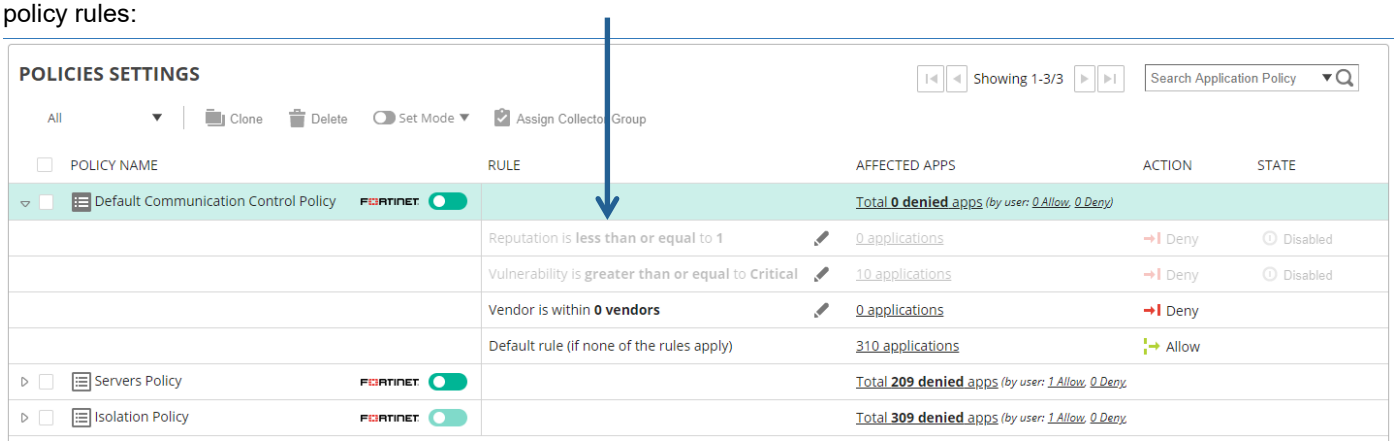
4. In the Isolation Policy row, select **Allow** in the dropdown menu.

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 button at the top of the Policies pane. For more details about these modes, you may refer to the *Protection or Simulation Mode* section on page 54.

Policy Rules

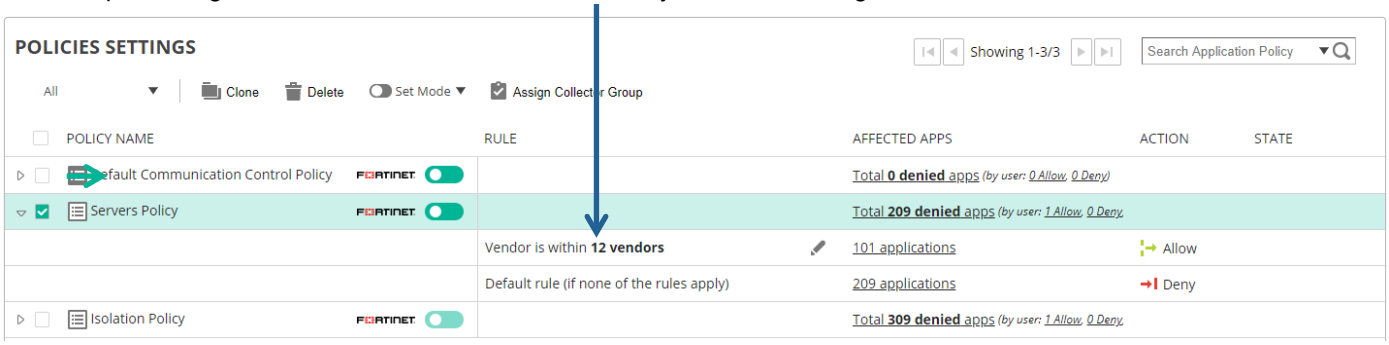
For each communication policy, FortiEDR provides four rules out of the box. These rules can be modified to specify the connections to be blocked/unblocked according to several parameters. FortiEDR provides the following communication policy rules:



- **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.

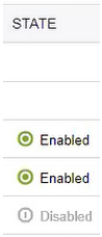
In the rules, X represents a user-defined value.

For example, the figure below shows that the Servers Policy has the following rules defined for it:



- 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**.

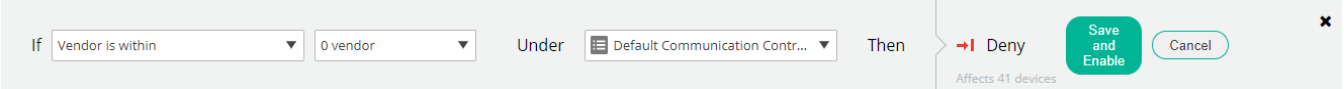


Editing a Policy Rule

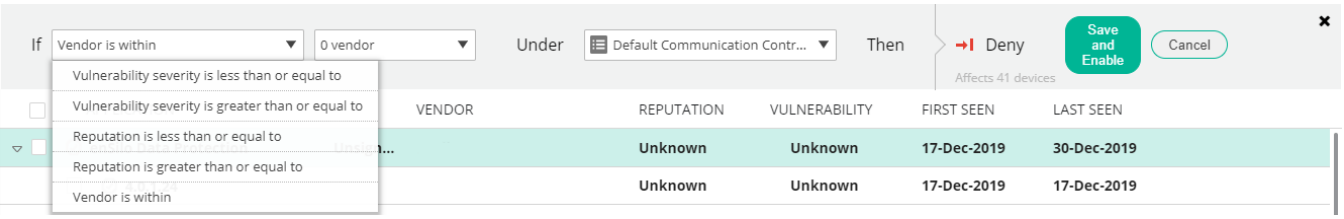
The four rules for a policy can be modified, as needed.

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:

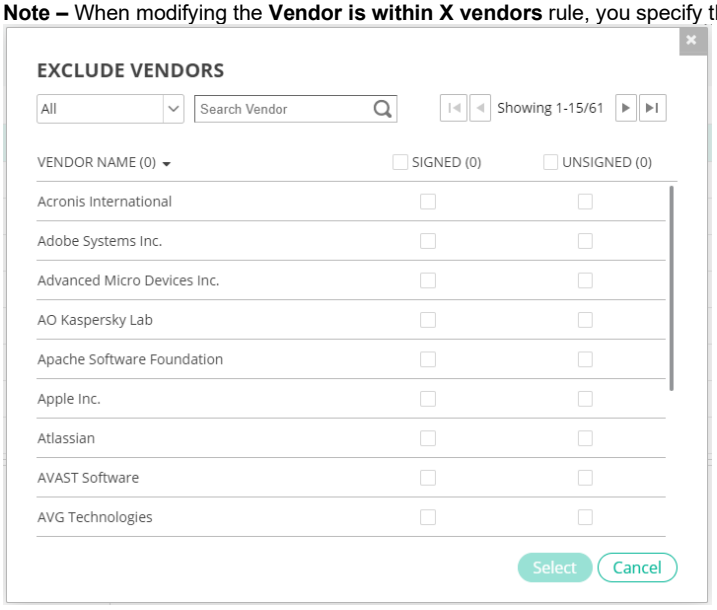


2. In the **If** dropdown list, select the parameter whose value you want to set in the rule. This dropdown list lists the parameters available to configure for the rule.

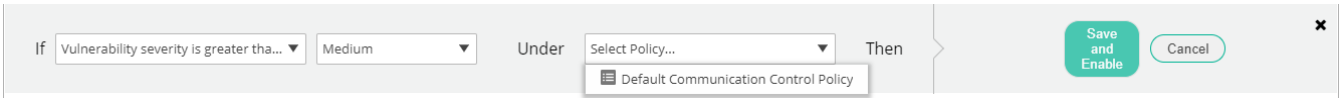


3. In the rightmost **Select** dropdown list, select the value for the parameter. This dropdown list lists the values available to configure for the parameter specified in step **2**.

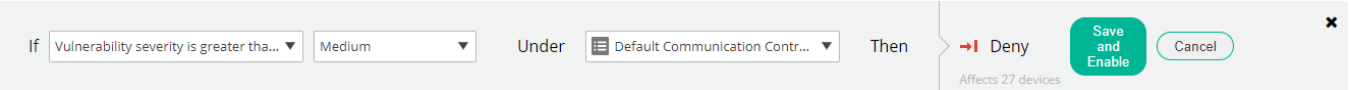
Note – When modifying the **Vendor is within X vendors** rule, you specify the vendor(s) to include and those to exclude for the rule.



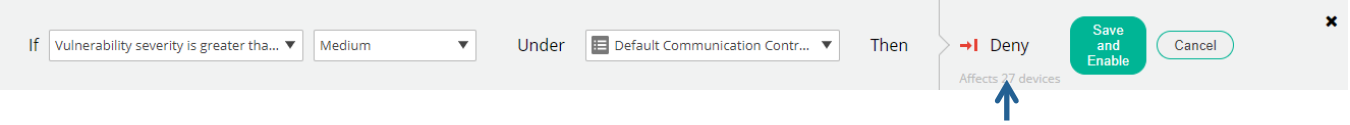
4. In the **Under** dropdown list, select the policy to which this rule applies.



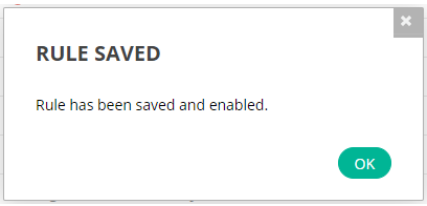
5. In the **Then** field, specify whether to **Allow** or **Deny** the application based on this rule.



The application list now shows the number of application(s) affected by the rule change.



6. Click the **Save and Enable** button to save and enable the changes to the rule. A confirmation window displays, confirming the rule change.

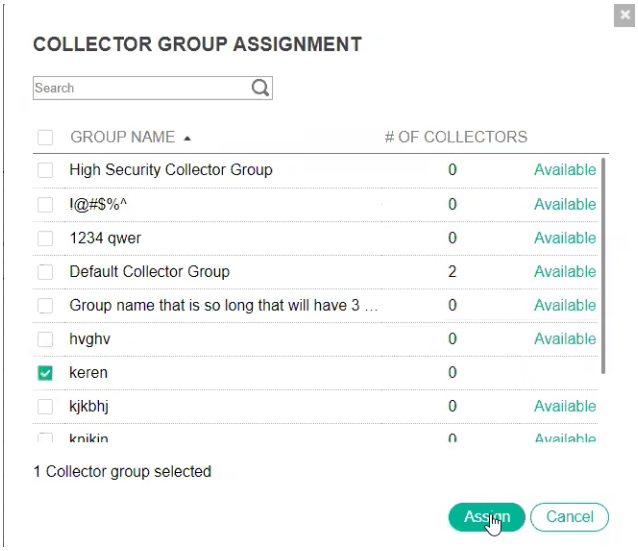


7. Click **OK**.

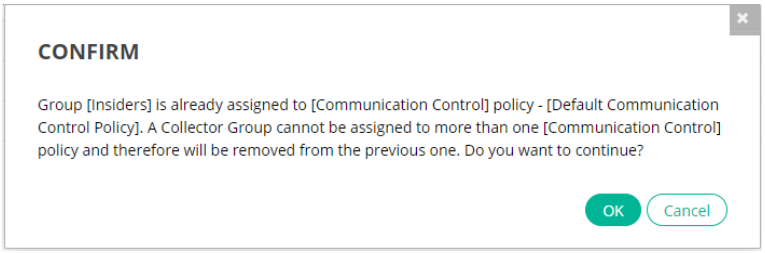
Assigning a Policy to a Collector Group

To assign a policy to a Collector Group:

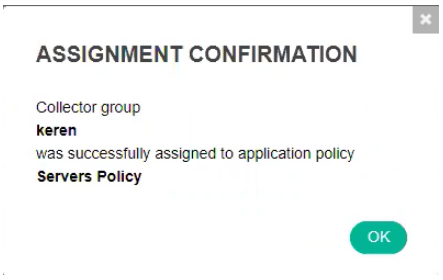
1. Check the policy that you want to change in the policy list and then click the **Assign Collector Group** button. The following displays:



2. Check the checkbox of the Collector Group you want to assign to the policy.
3. Click the **Assign** button. A window displays, prompting you to confirm the reassignment.



4. Click **OK**. The following displays:



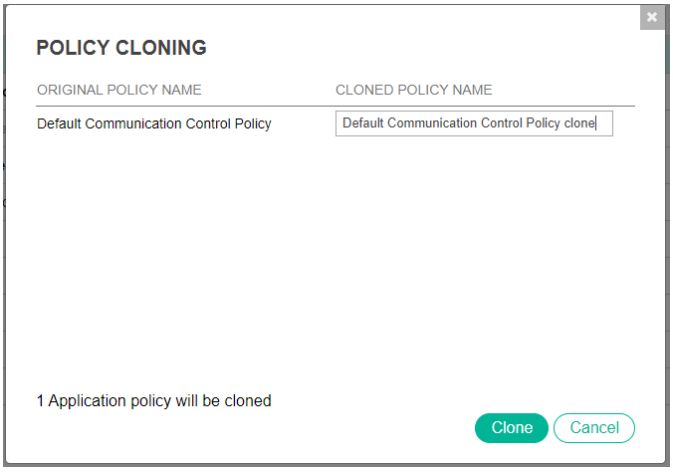
5. Click **OK**.

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.

To create a new Communication Control policy:

1. In the policy list, check the policy that you want to clone. There are two types of Communication Control policies: blacklisting policies ( ), such as the Default communication control policy, which allows any connection by default, and whitelisting policies ( ), such as the Servers policy, which denies any connection by default.
2. Click the **Clone** button. The following window displays:



3. In the **Cloned Policy Name** field, specify a name for the cloned policy.
4. Click the **Clone** button.

Other Options in the Policies Pane

- All : Click the down arrow in the All button and then select an option in the dropdown list to filter the policy list accordingly.
- Clone: Click this button to clone a policy.
- Delete: Click this button to delete a policy. Before deletion, a confirmation message displays, prompting you to confirm the deletion of the policy.
- Set mode : Click the down arrow in the Set mode button and then select the mode for the policy, as described in the *Policy Mode* section on page 125.

Chapter 8 – FORENSICS

This chapter describes the FortiEDR Forensics 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 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:

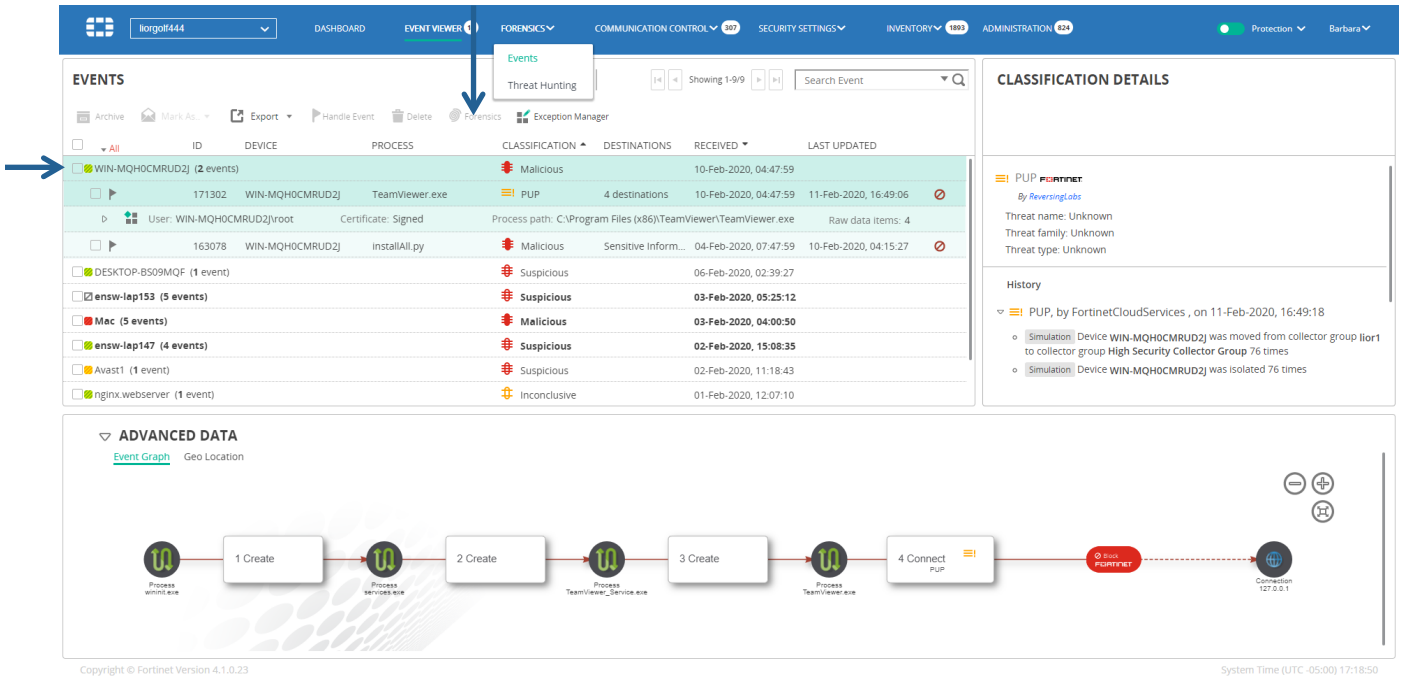
- Infected device and application details.
- Evidence path, which includes the process that the threat actor violated and which type of violation was executed.
- Side-by-side event comparisons.

This option is only available to users who have purchased the Forensics add-on license, which is part of the **Protect and Response** license or the **Predict, Protect and Response** license.

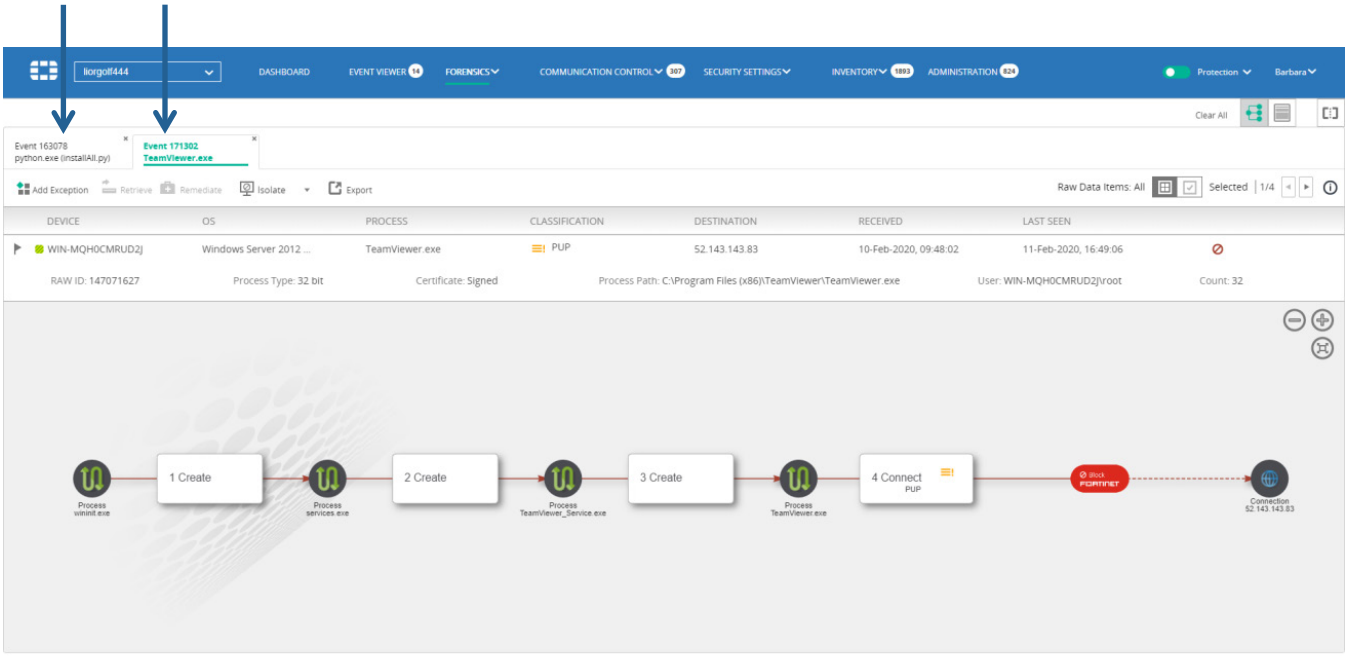
The Forensic Analysis add-on also enables you to search for malware across your entire environment, in order to remediate using its Thread Hunting feature. For more details, see the *Threat Hunting* section on page 144.

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

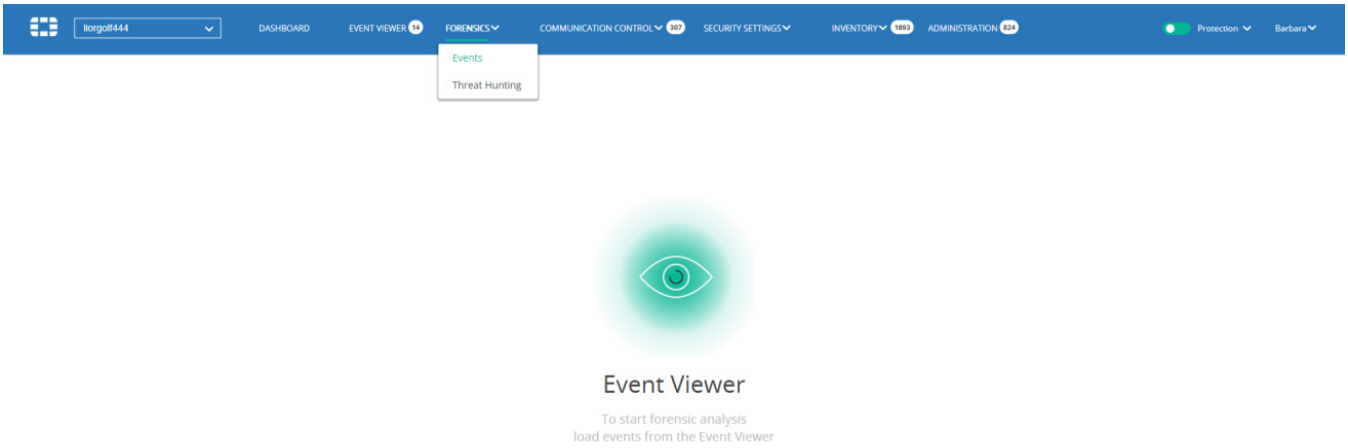
- In the Event Viewer, select an event aggregation and then click the Forensics button. Selecting an event aggregation lets you analyze the aggregation of events triggered on this process.



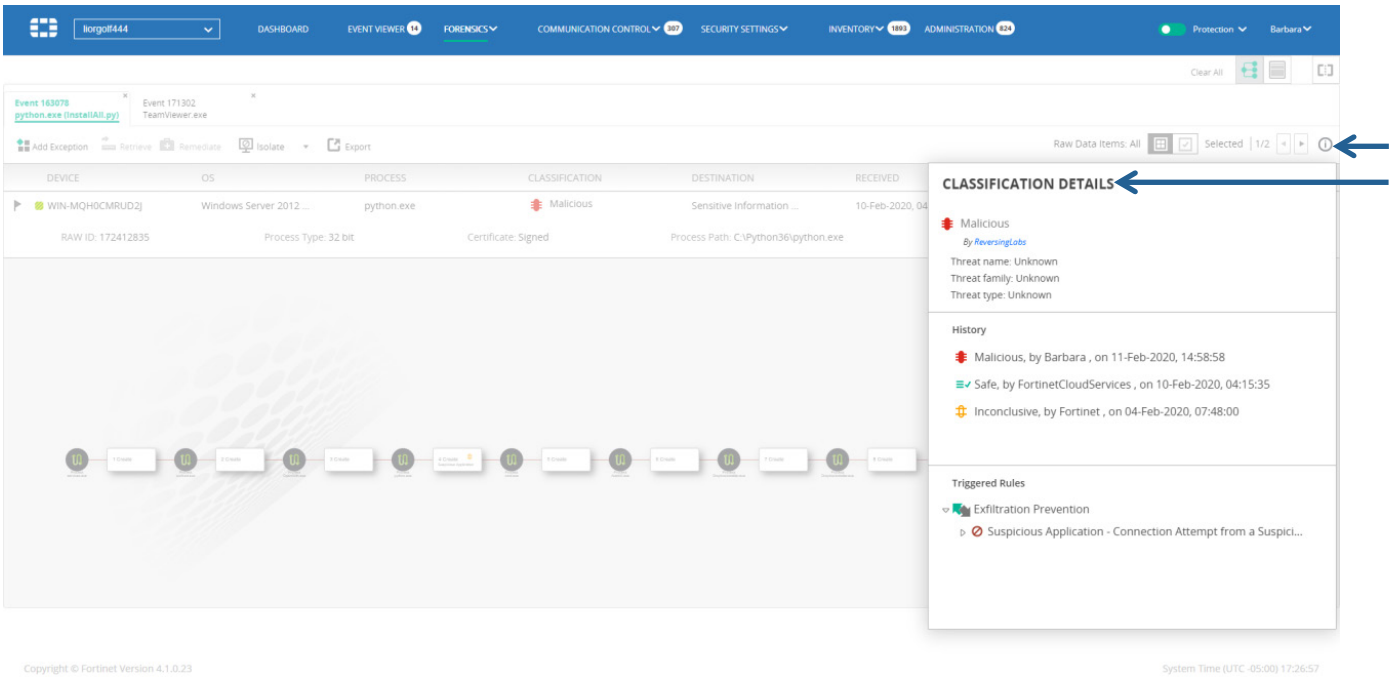
In this case, the Forensics add-on shows a separate tab for each event associated with the event aggregation. For example, the figure below shows seven tabs for an event aggregation containing two events.



- Select an individual event in the Event Viewer and then click the Forensics button. In this case, the Forensics add-on shows a single tab for the selected event, with all of its related raw data items.
- Select a raw data item when in drill down, and then click the Forensics button. In this case, the Forensics add-on shows a single tab for the selected 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 event of interest using any of the methods described above.

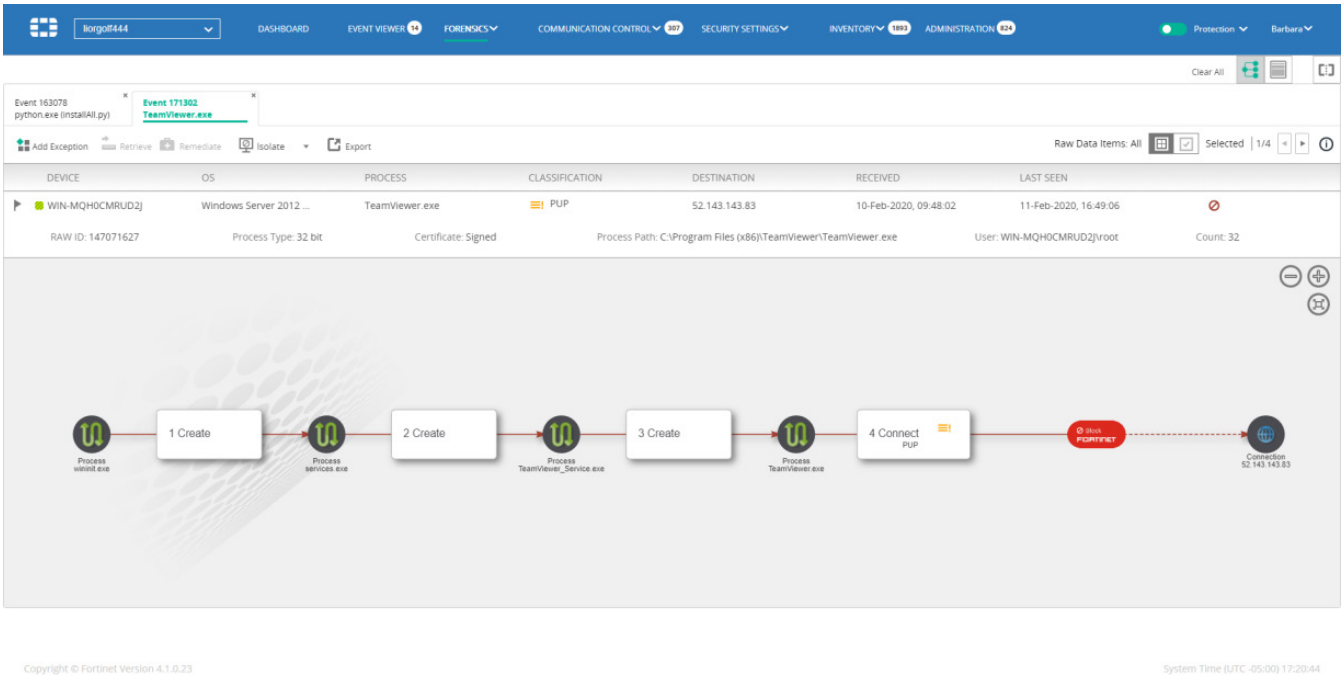


You can click the ⓘ button in the **FORENSICS** tab to display classification details, including the classification, policy and rules assigned to the FortiEDR Collector that triggered this event. For more details about classification details, see page 106.



To perform deep Forensic analysis:

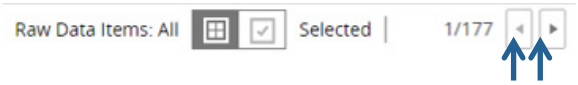
1. Select the events to analyze using one of the methods described on page 90.
   Selected events that are currently loaded to the **FORENSICS** tab are marked in the **Event Viewer** with a fingerprint icon.
2. Each selected event is then displayed in the Event Viewer as a separate tab:



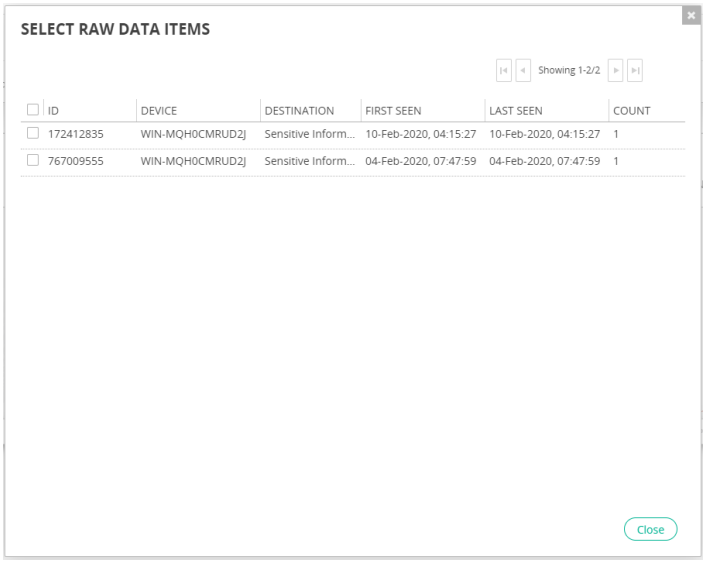
Each tab shows the same information as in the Event Viewer (page 90), with additional information as described below.

The following options for viewing more information are provided:

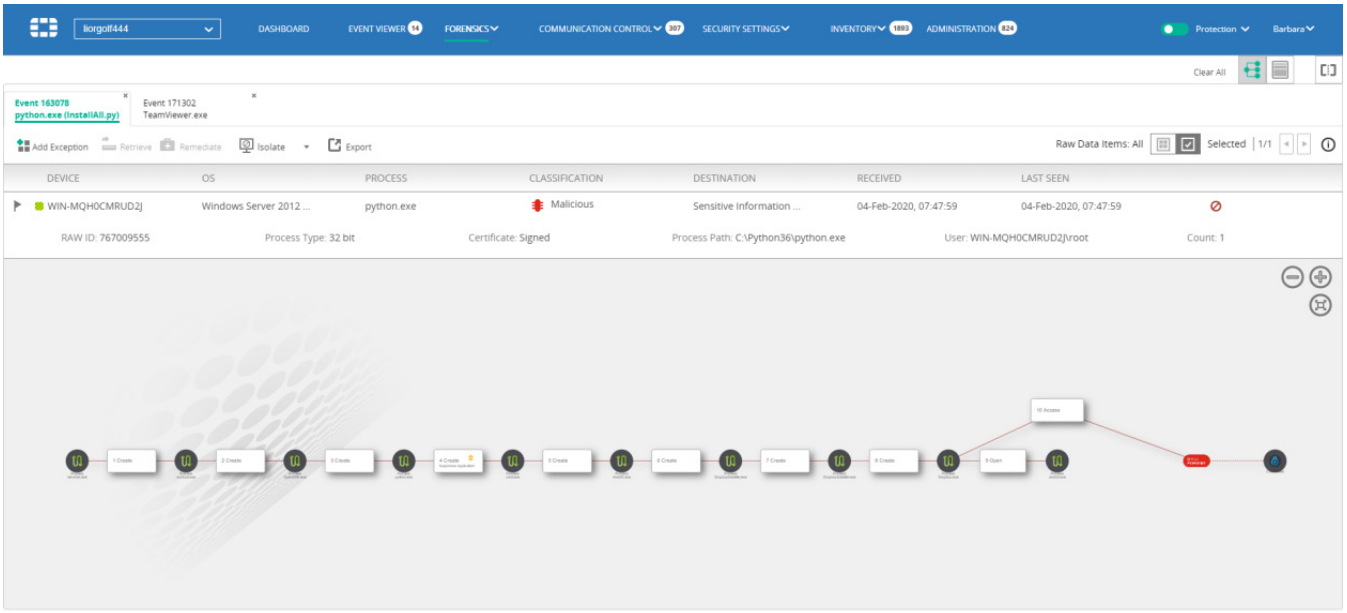
In the Raw Events area, use the right and left arrows to scroll through the raw data items for an event.



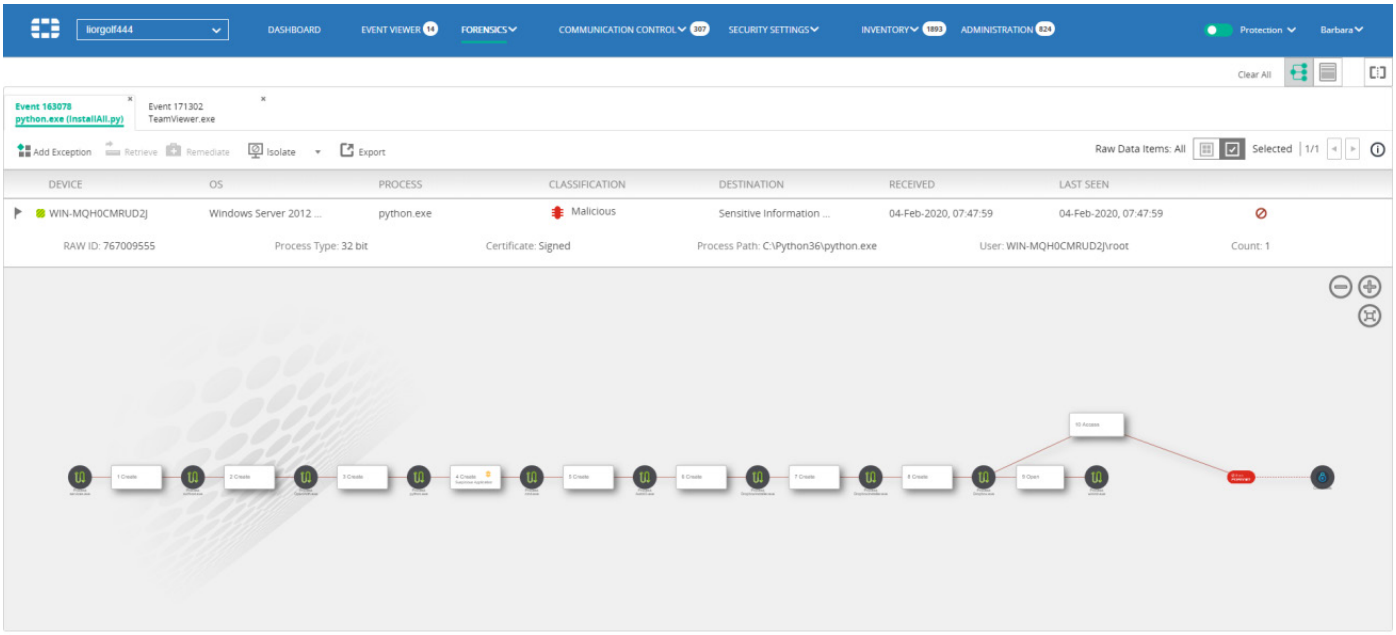
Click the All Raw Data Items button to display all raw data items. Click the Selected Raw Data Items button to select a specific raw data item. This action opens the following window, in which you specify the raw data item(s) to display.



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



Flow Analyzer View



This view shows a graphic flow diagram depicting the history of what happened before the 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 ----.

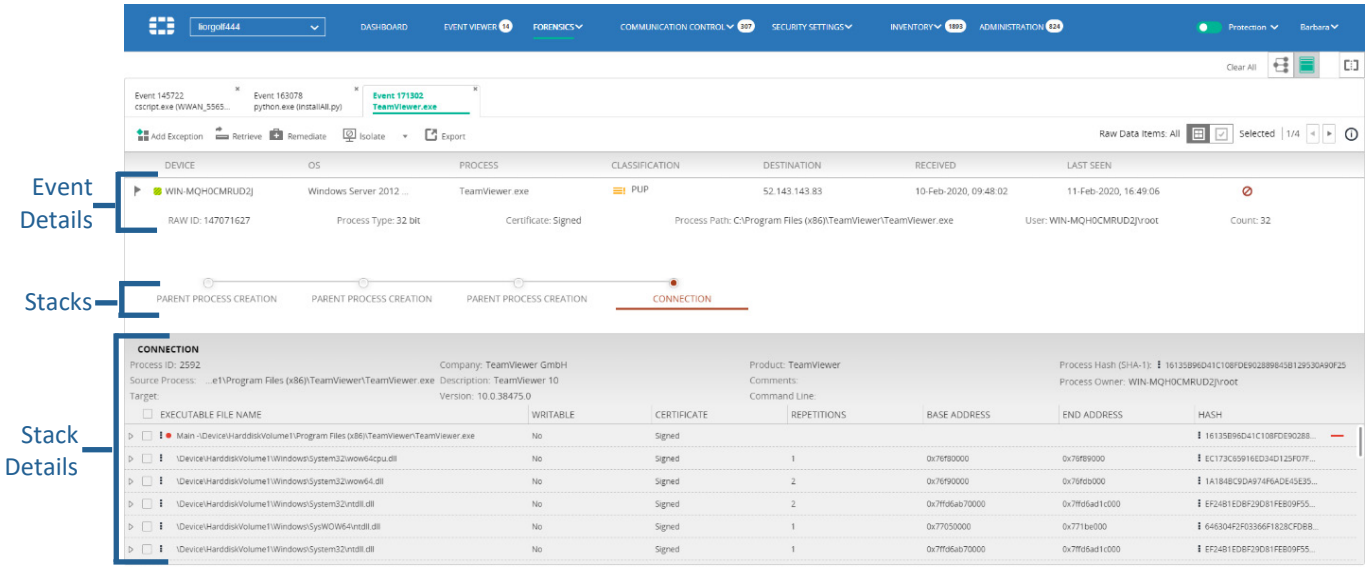
Typically, the next to last rightmost node represents a connection request 

and specifies the IP 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 **Block**, **Log** or **Simulated Block**.

The flow chart is interactive. Clicking on a specific node or arrow drills down to the Stack View (described below). This enables you to perform further investigation of the specific stack that was collected during that step.

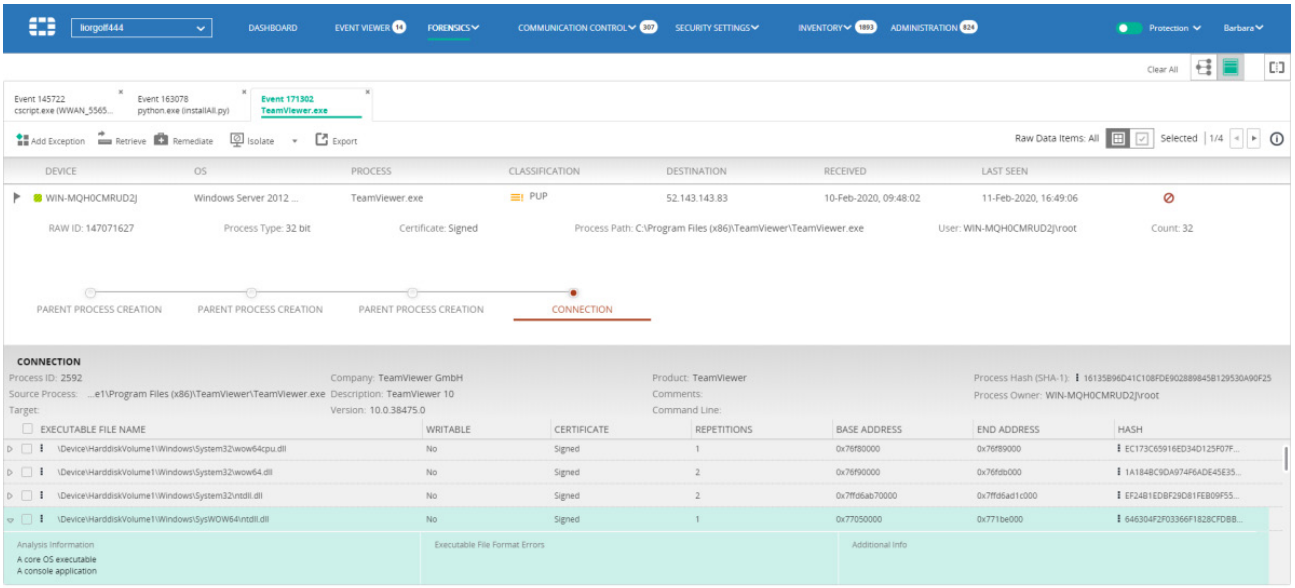
Stack View



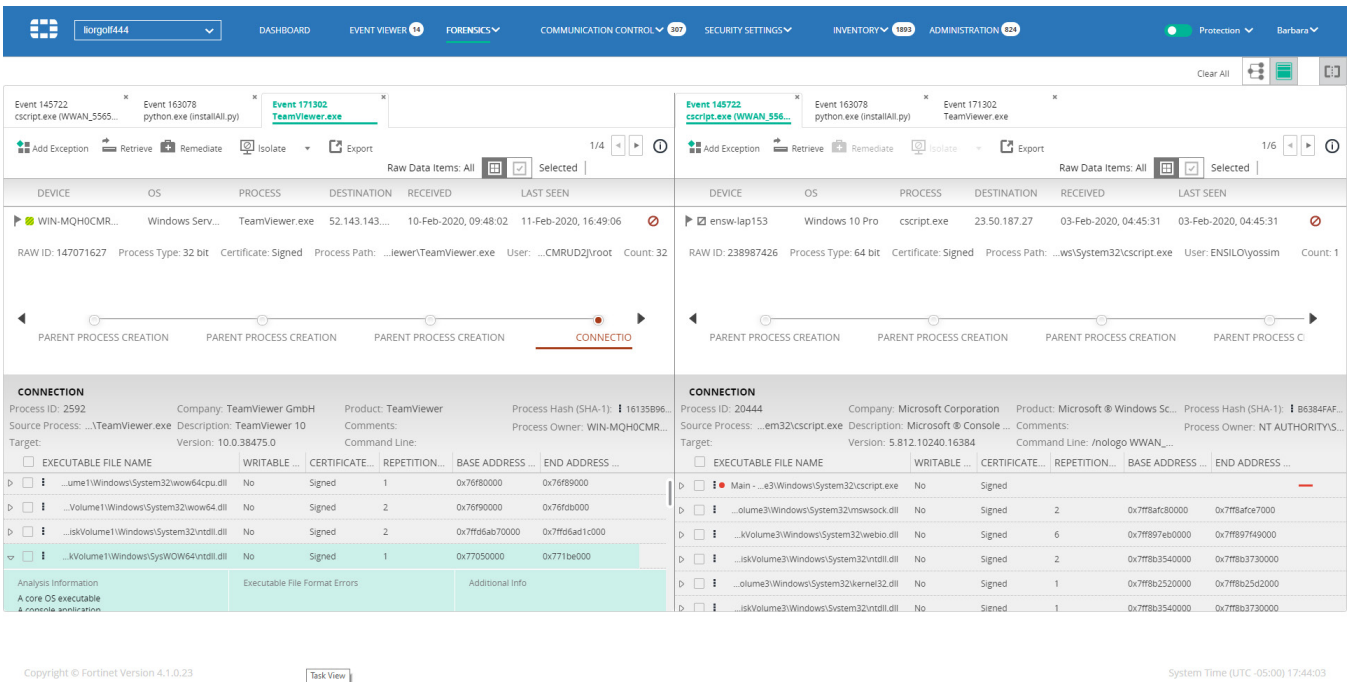
The **Stack View** displays the following sections of information:

- **Events:** Shows the same information as in the Event Viewer (page 90).
- **Stacks:** 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.
- **Stack Content Details:** 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.
  - Click the **Process Hash** link to check 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 www.virustotal.com, click the **Search** tab, paste the hash from FortiEDR and then click **Search It**.
  - For each executable, you can see the following information:
    - Executable File Name
    - Writeable: 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 event is highlighted with a red dot. This indicates the row that you may want to investigate further, as described below.

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



Compare View



The **Compare View** enables you to display two views side-by-side. They can both be either Flow Analyzer View or Stack View (described above).

Defining an Exception

After Forensic analysis, you may decide to create an exception for a specific event. To do so, you may refer to the *Defining Event Exceptions* section on page 98. You may refer to page 59 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:

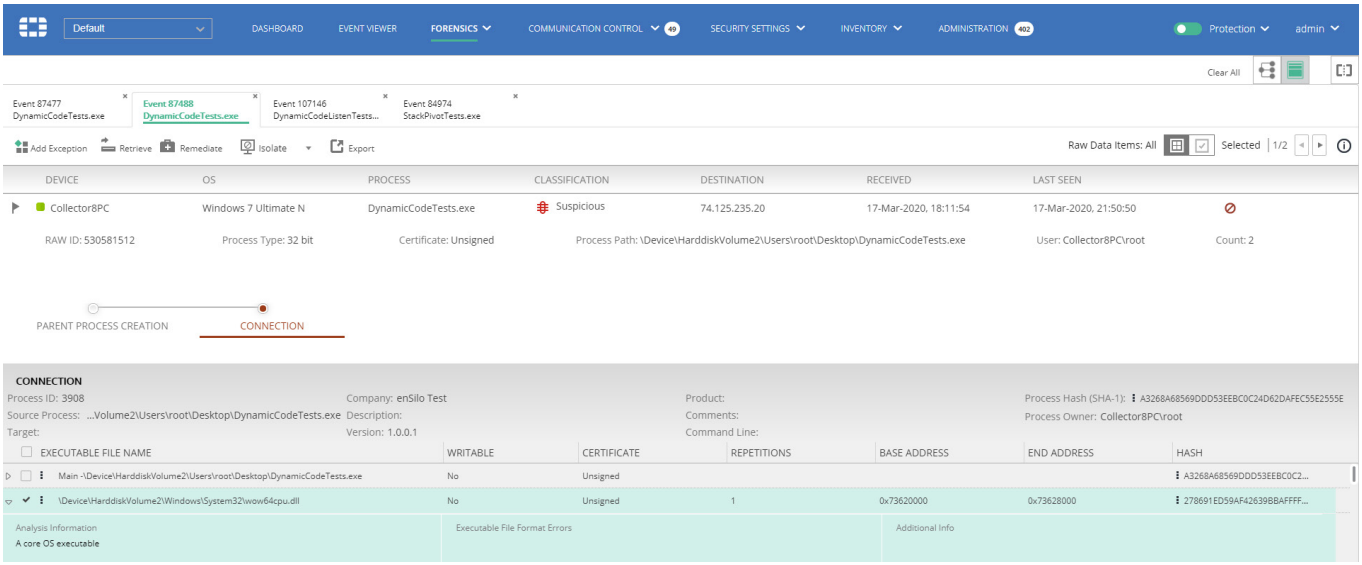
- **Terminate the Process:** This method does not guarantee that the affected process will not attempt to execute again.
- **Delete the Affected File from the Computer:** This method ensures that the file does not attempt to exfiltrate data again, as the file is permanently removed from the device. When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

Note – Some malware have persistency capabilities, which makes the infection appear again. In addition, in some rare cases, malware can cause the system to crash if you try to remove them.

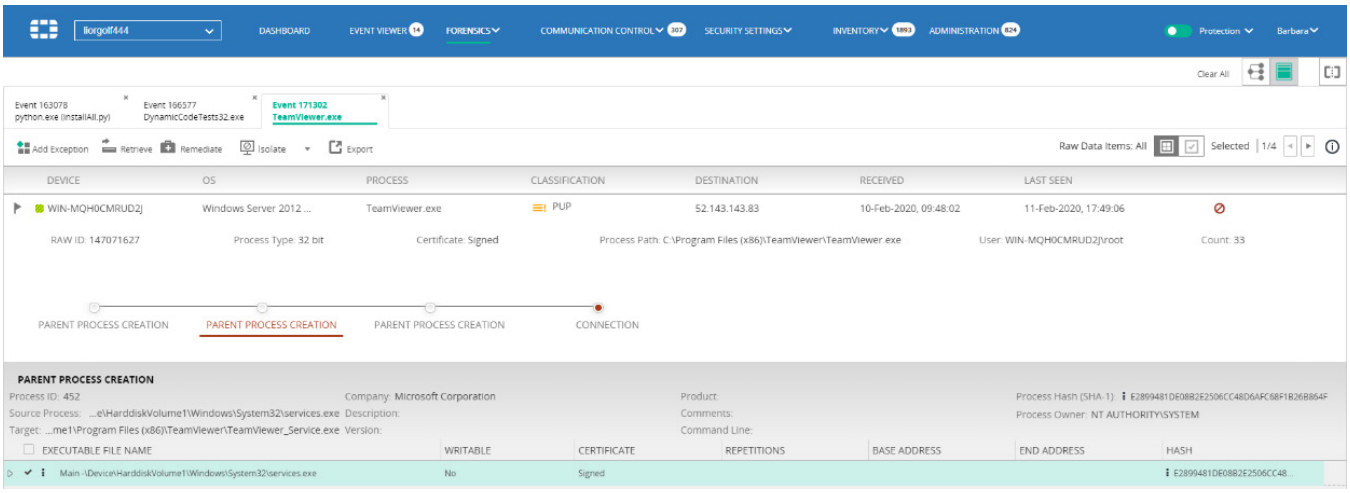
Both of these methods can be performed using the Forensics add-on.

To remediate a device on which malware was detected:

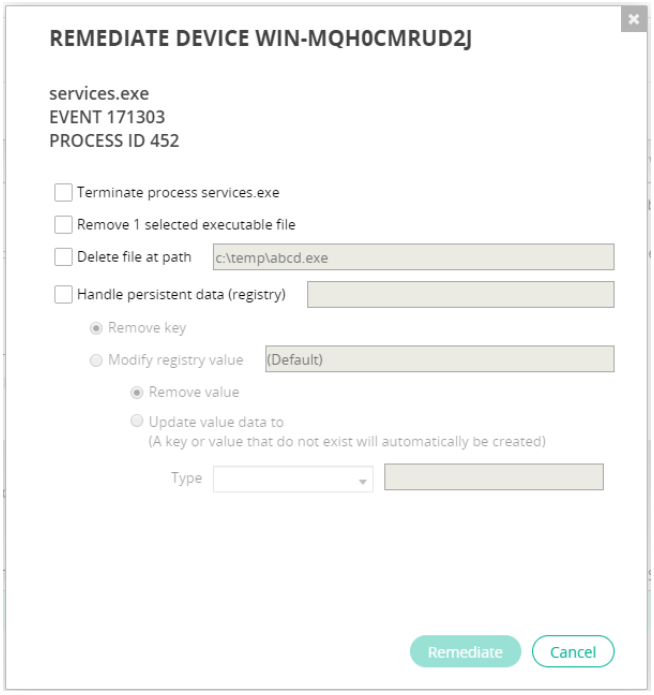
1. Select the event(s) to analyze using one of the following methods described on page 90.
2. In the Raw Events area, select the relevant process. Use the various forensic tools provided by FortiEDR to determine the process of interest.



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

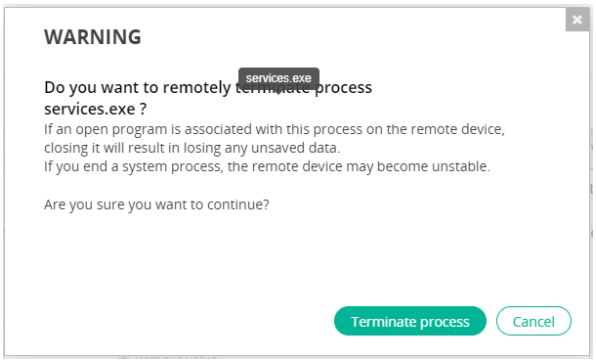


3. Check the checkbox of the relevant file and then click the Remediate button. The following window displays:



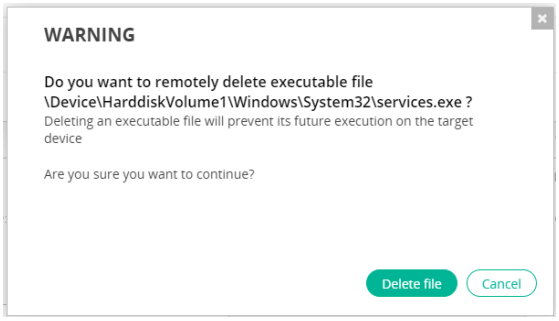
4. Do one of the following:

- Check the **Terminate process** checkbox to terminate the selected process. A warning message displays.



Click **Terminate process** to terminate the selected process.

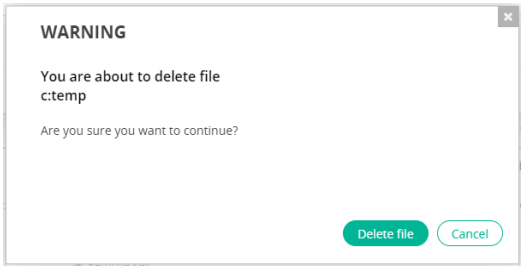
- Check the **Remove selected executable file** checkbox to delete the specified file from the device. A warning message displays.



  Click **Delete file** to remove the selected file.

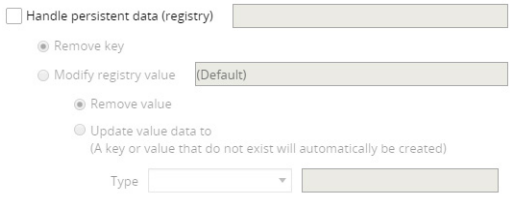
- Check the **Delete file at path** checkbox. In the adjacent field, enter the file path on the device that contains the file to be removed.

  A warning message displays.



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

- 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.



  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 the **Remediate** button.

Retrieving Memory

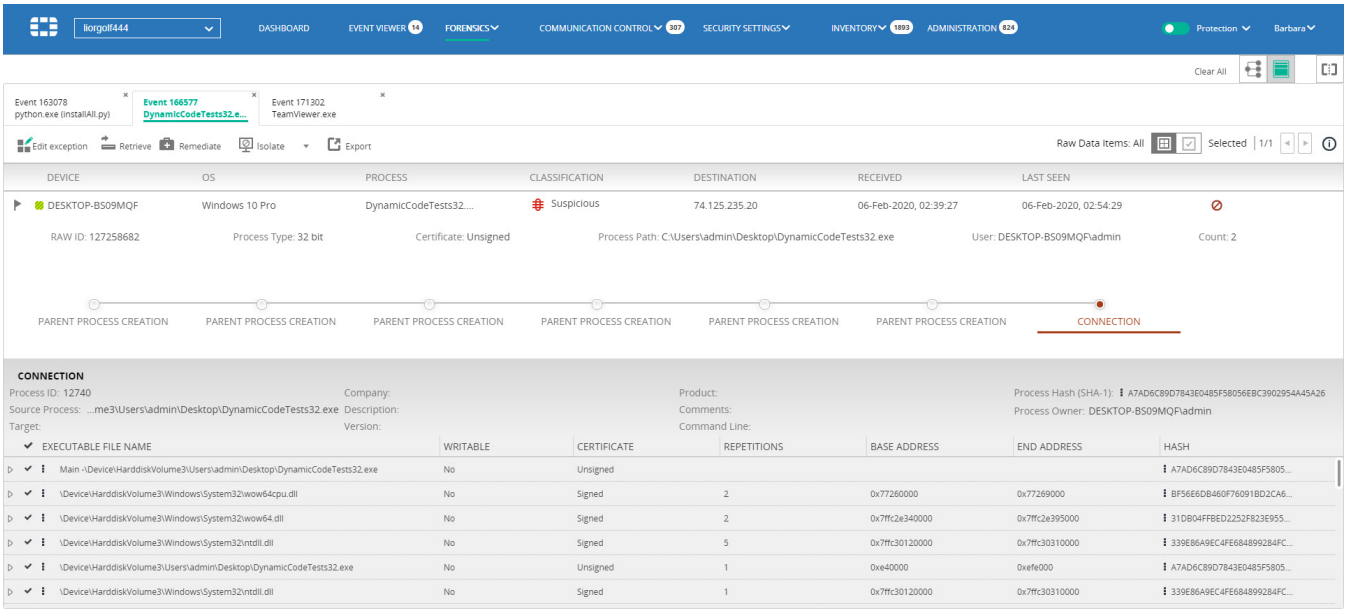
The **Retrieve Memory** function enables you to retrieve the stack-memory of a specific Collector. This option enables you to retrieve memory from a specific communicating device in order to perform deeper analysis by analyzing the actual memory from the device. This function is only accessible from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

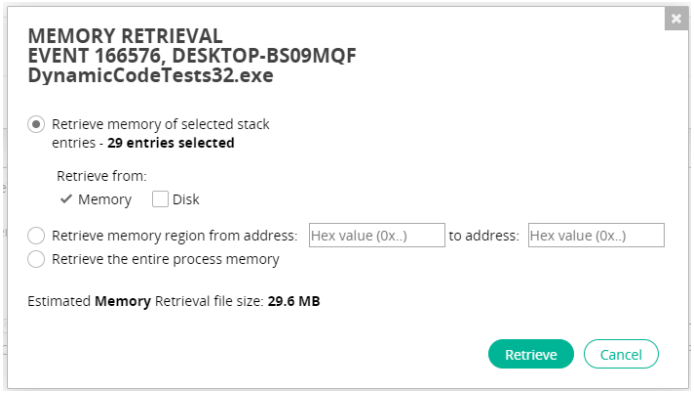
If the file cannot be sent, it is saved locally on the host by the Collector.

To retrieve memory for a Collector:

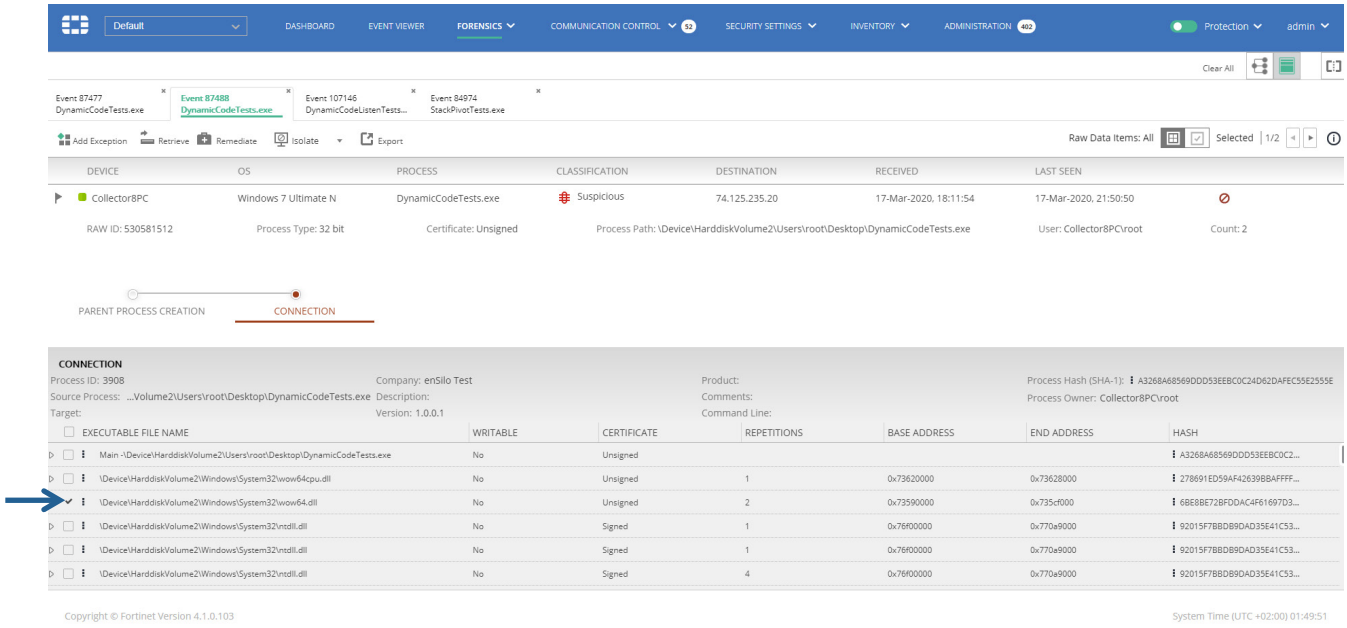
1. In the Stack View, select the stack(s) that you want to analyze by selecting its checkbox(es).



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

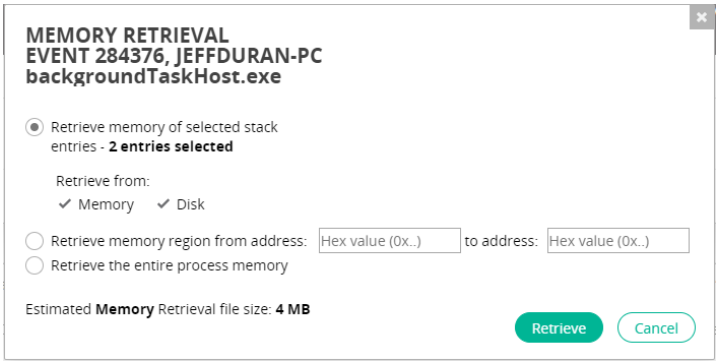


3. Select one of the following options:
   - Retrieve memory of selected stack entries: Select this radio button to retrieve memory for one or more specific stack entries. Then, select the stack entries you want to analyze by checking their checkboxes, as shown below:



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.



- **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 the entire process memory:** Select this option to retrieve memory for an entire process. This option retrieves all the stack entries comprising the process.

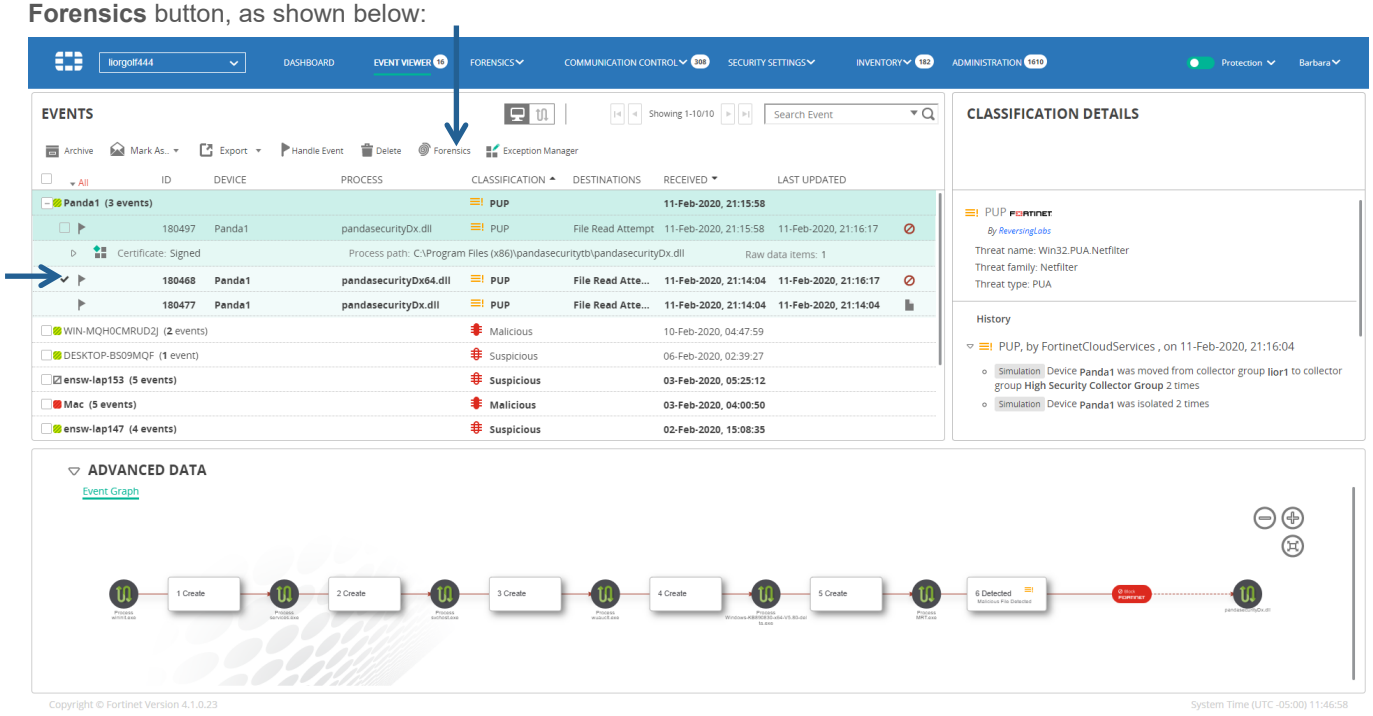
4. Click the **Retrieve** button.

Isolating a Device

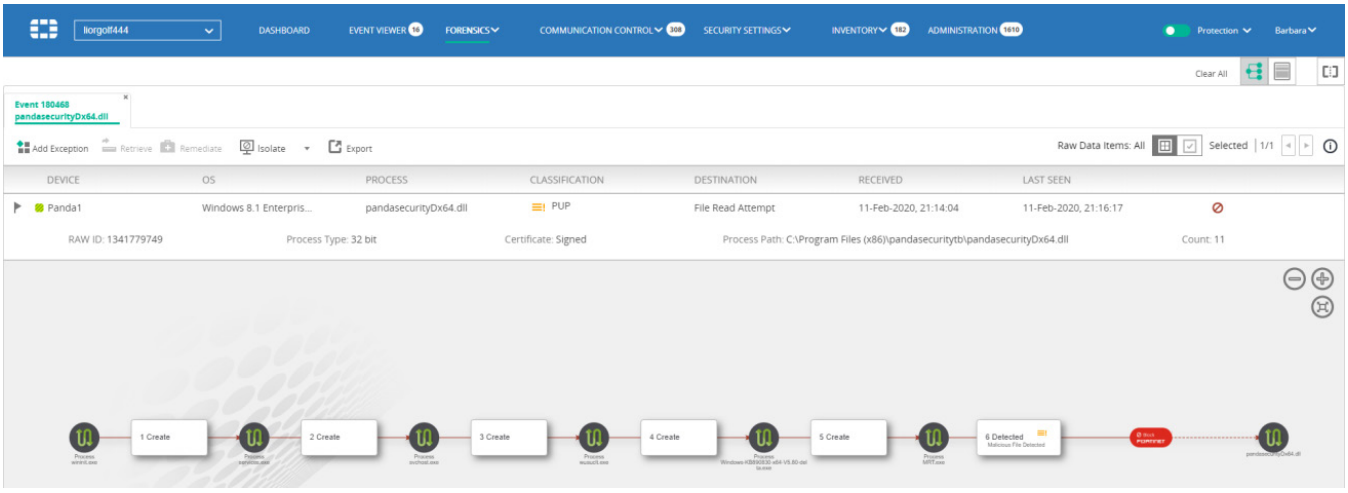
An isolated device is one that is blocked from communicating with the outside world (for both sending and receiving). For more details about device isolation, see page 64.

To isolate a device:

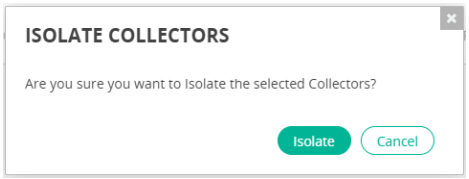
1. In the **EVENT VIEWER** tab, select the checkbox(es) of the event(s) that you want to isolate, and then click the **Forensics** button, as shown below:



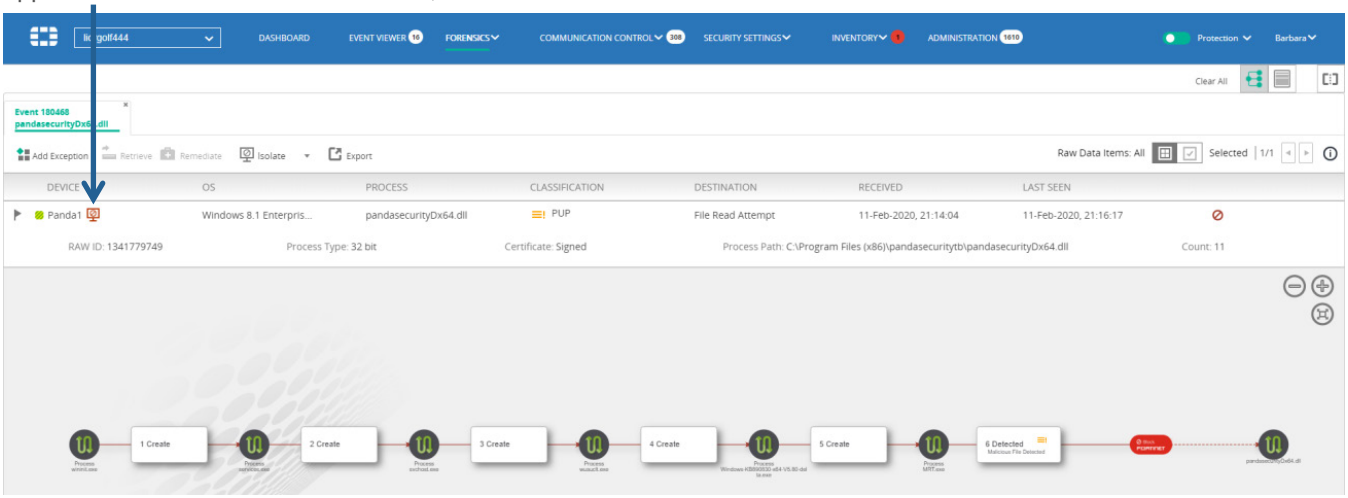
The following window displays:



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

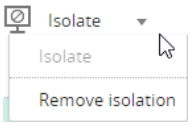


3. Click the **Isolate** button. A red icon appears next to the relevant event in the **Events** tab to indicate that the applicable Collector has been isolated, as shown below:

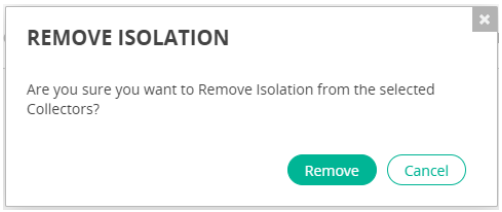


To remove isolation from a device:

1. In the **FORENSICS** tab, select the checkbox of the event 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:



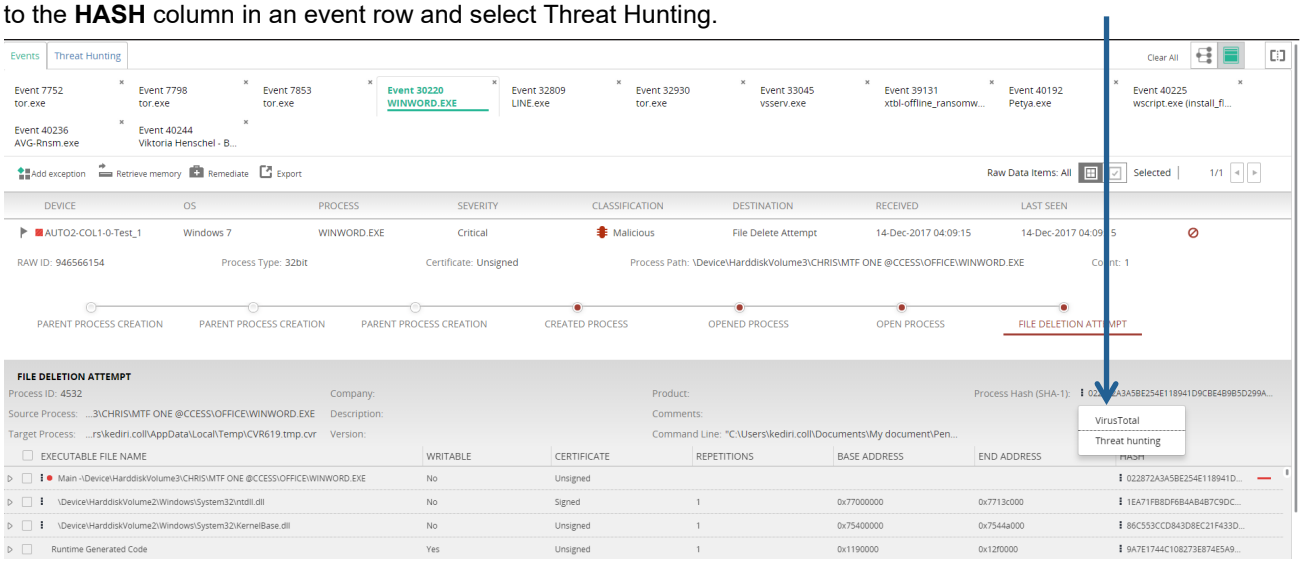
3. Click the **Remove** button.

Threat Hunting

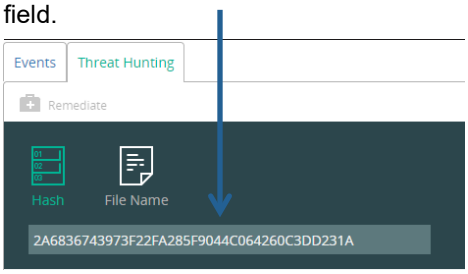
FortiEDR's *Threat Hunting* feature enables you to search for malware across your entire environment, in order to remediate it. Searching can be based on events or a free-text search. You can search for malware based on an event's process or HASH. The search operation only applies to files on the Windows operating system, and not to Linux or MacOS.

Access the **Threat Hunting** page under the **Forensics** tab using one of the following methods:

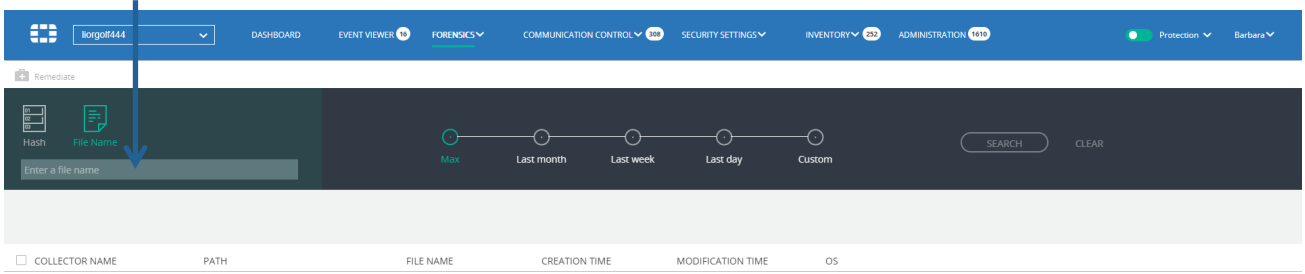
- Method 1 (Search from an Event): In the **Events** page under the **Forensics** tab, left-click the three dots ⋮ next to the **HASH** column in an event row and select Threat Hunting.



This action opens the **Threat Hunting** page and automatically enters the HASH value in the **Hash/Process** field.



- **Method 2 (Free-text Search):** Click the **Threat Hunting** option under the **Forensics** tab. This action opens the **Threat Hunting** page. In this case, the **Hash/Process** field is empty.



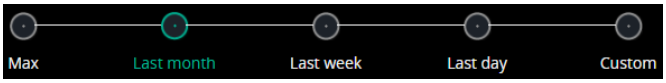
To search for malware:

1. 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 file names.

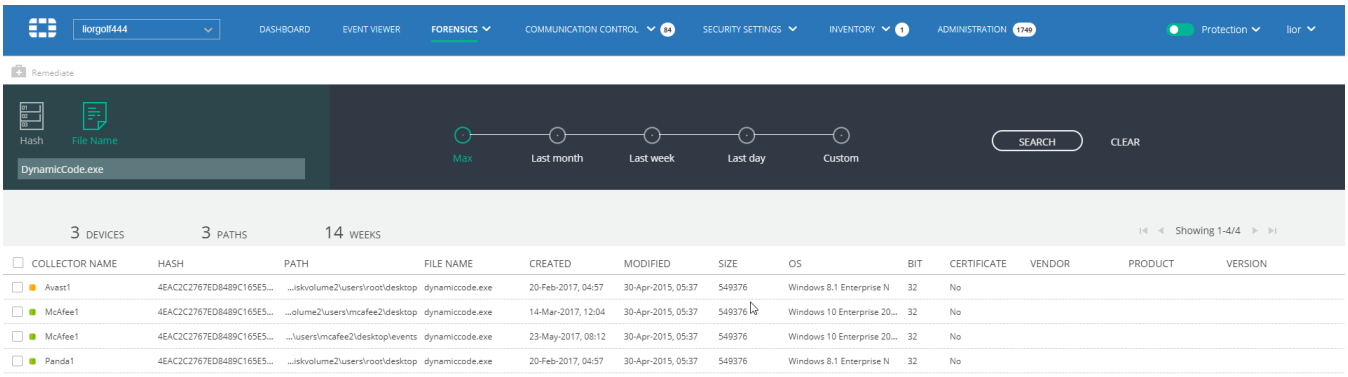
   When accessing the **Threat Hunting** page using Method 1 (described above), the relevant HASH value appears in the field adjacent to the Hash button, as shown below.

   When accessing the **Threat Hunting** page using Method 2 (described above), the field adjacent to the Hash and File Name buttons is empty.

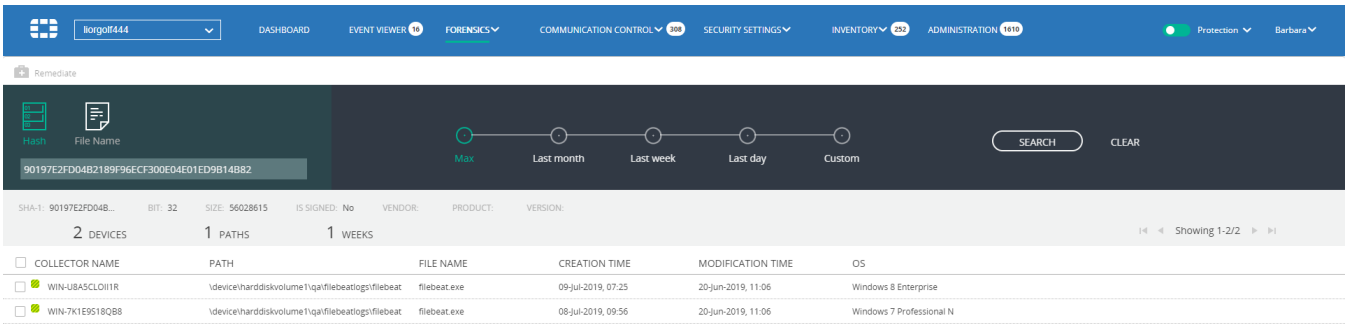
2. If the field adjacent to the Hash and File Name buttons is empty, copy and paste the applicable file name or HASH value into the empty field.
3. Specify the time range for the search using the timeline buttons at the top of the window.

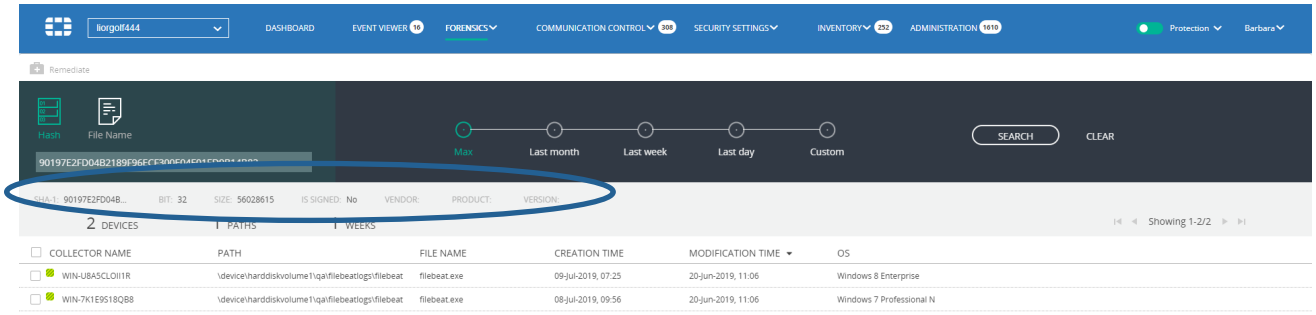
4. Click the **Search** button. The system searches for matching files in all devices in your environment. When the search completes, the search results display in the window. The example below shows a search by process.

   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.

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.



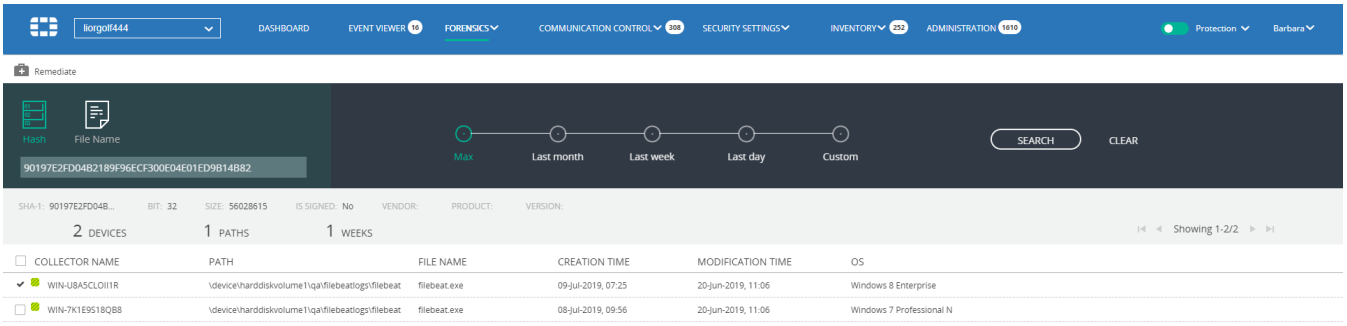
Remediating Devices upon Malware Detection

You can remediate detected malware from some or all devices at once using the Remediate button in the Threat Hunting page. This option enables you to delete detected malware across all the search results in the Threat Hunting page simultaneously. This is in contrast to the Remediate option described on page 137, which only deletes a specific file from a specific device.

To remediate one or more devices on which malware was detected:

1. Check the checkbox of the row(s) you want to remediate.

   Alternatively, you can click the **Collector** checkbox at the top of the window to select all devices on that page of the window simultaneously. Note that you need to repeat this action for each page of results, if you want to delete multiple pages of results.



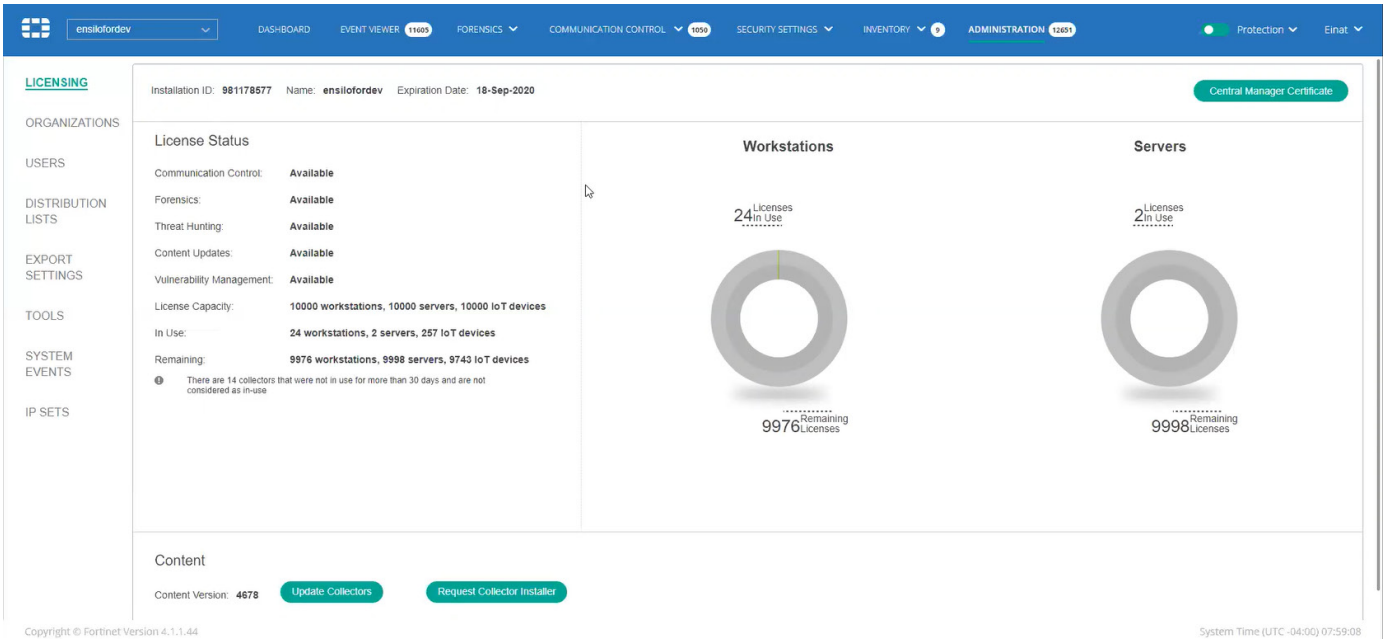
2. Click the Remediate button to delete the selected files from the relevant device(s).

Chapter 9 – ADMINISTRATION

This chapter describes the FortiEDR Administration options, which are only available to users with administration rights (Local Administrators and Administrators).

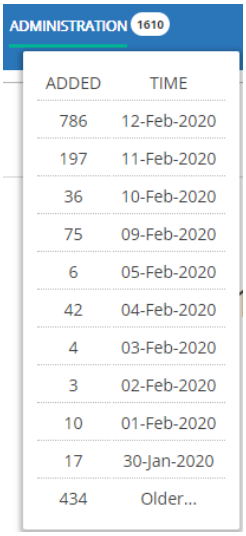
Licensing

Selecting **LICENSING** in the **ADMINISTRATION** tab displays all the entitlements provided by your license. You may refer to page 32 for more information.



Note – 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 events have not been read by the user. For **Administration**, the number represents the number of unread system events.

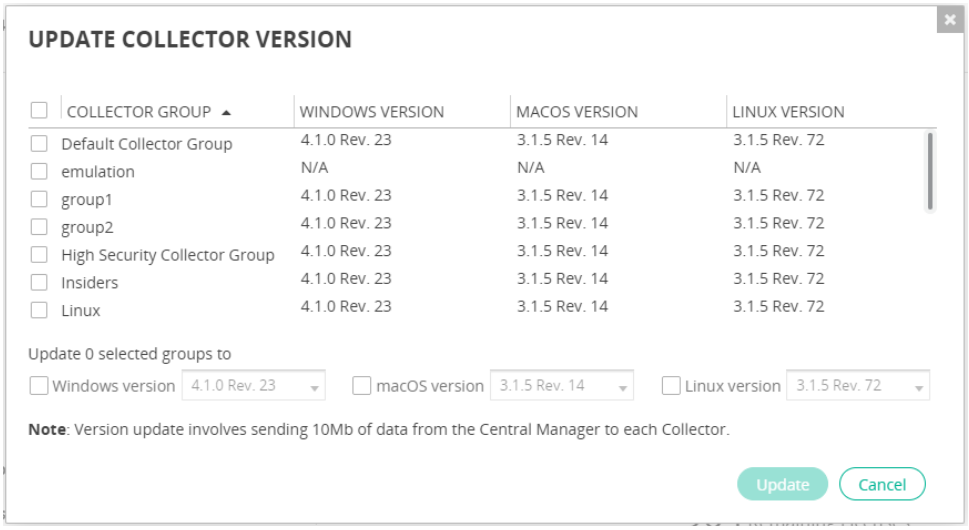
You can hover over the number to see the list of unread system events. Each row shows the number of system events added by day.



Updating the Collector Version

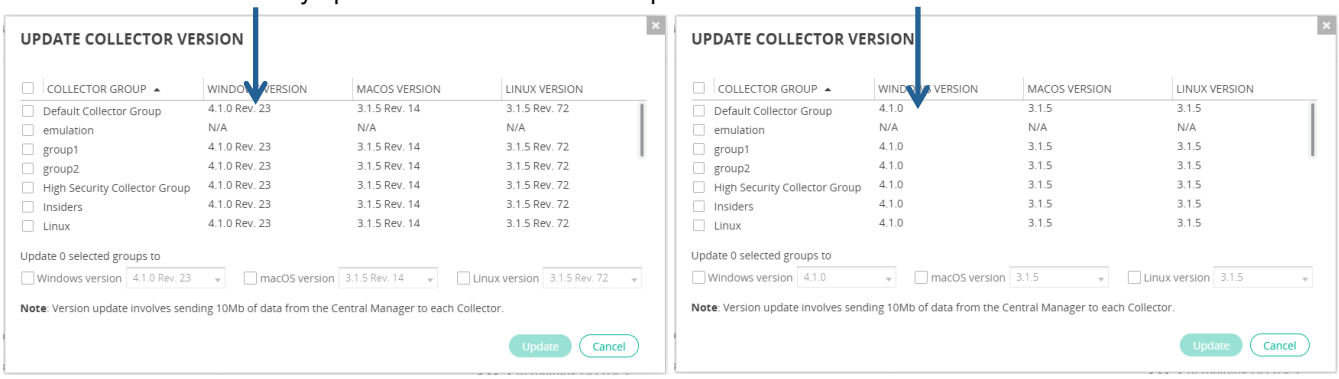
The Update Collector Version feature is used to update a FortiEDR version, such as from version 3.1.**0** to 3.1.**1**. To update a FortiEDR revision, use the Automatic Updates feature described on page 165.

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.



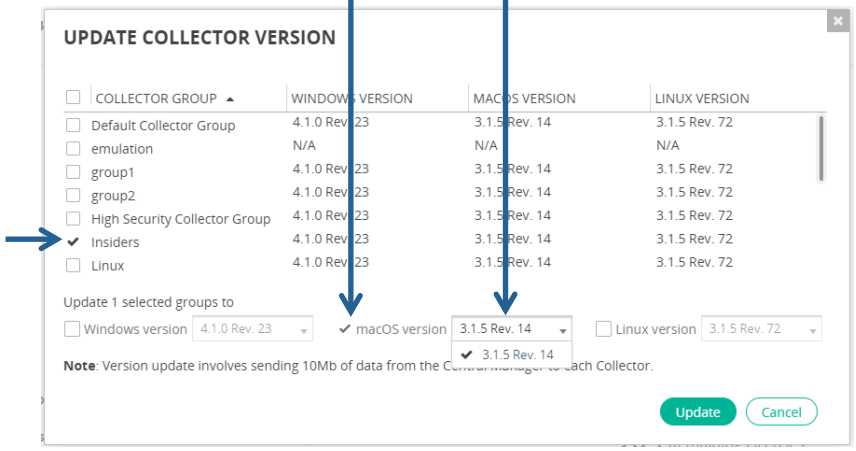
You can update the version for the Collectors in a Collector Group for each operating system.

Note that if the **Automatic Updates** checkbox is checked in the Tools 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.



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.

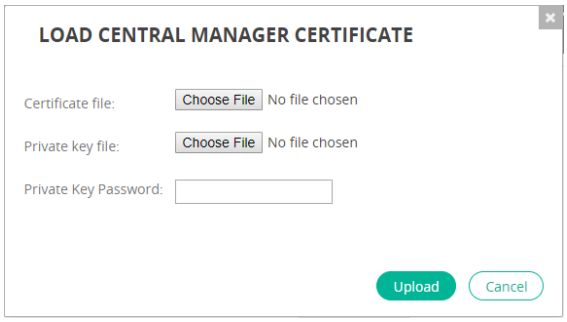


3. Click **Update**. FortiEDR gradually updates all the Collectors in the Collector Group(s) to the required version for the specified operating system(s), and displays the following window:

4. Click **OK**.

Loading a Server Certificate

You can click the Central Manager Certificate button to load a Central Manager certificate. To load a certificate, you must specify the certificate file, the private key file and the private key password, as shown below.



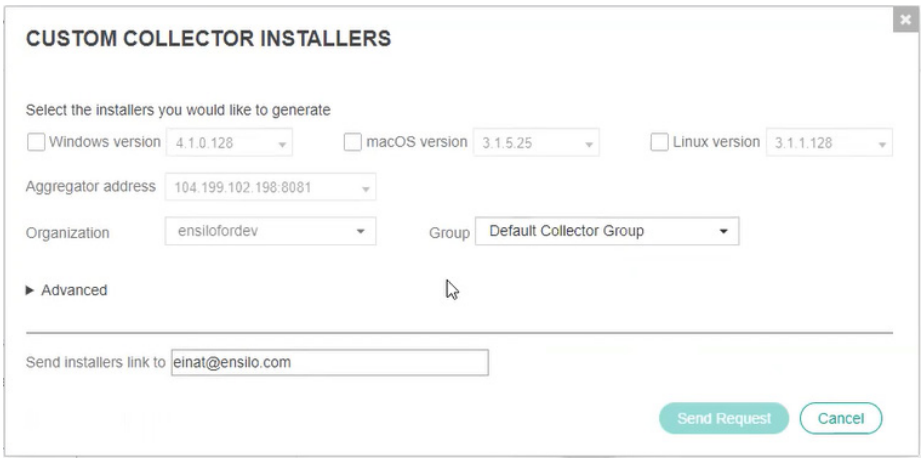
Requesting and Obtaining a Collector Installer

You can click the Request Collector Installer button 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 double-click it and then follow the instructions to install a Collector based on the operating system on which it is to be installed, as described in the *Installing a FortiEDR Collector on Windows* section on page 39, the *Installing a FortiEDR Collector on an Mac Operating System* section on page 41 and the *Installing a FortiEDR Collector on Linux* section on page 44.

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.

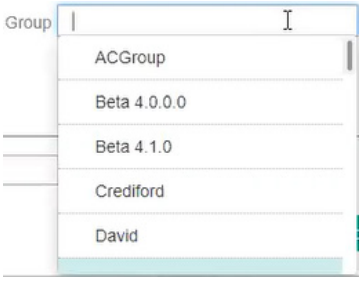
To configure custom installer settings:

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

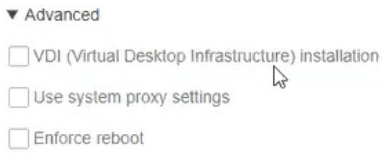


2. In the Select the installer you would like to generate area, select the checkbox of the installer(s) you want to request. Multiple installers can be requested at the same time.

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 page 149.
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.



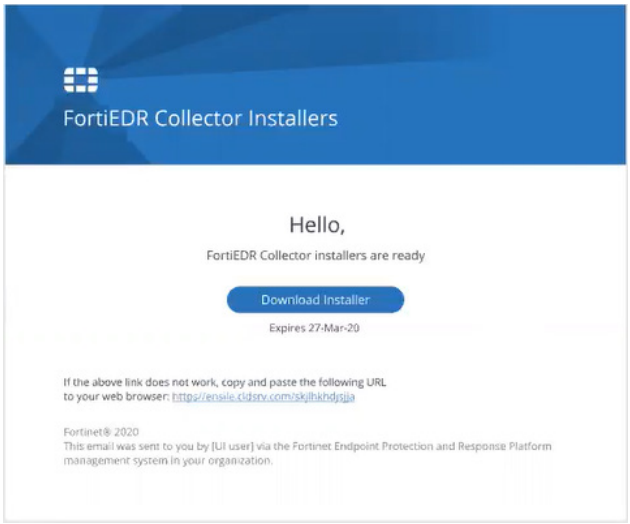
7. In the Advanced area, specify the following:



- **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 48.
- **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 >**).
- **Enforce 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.

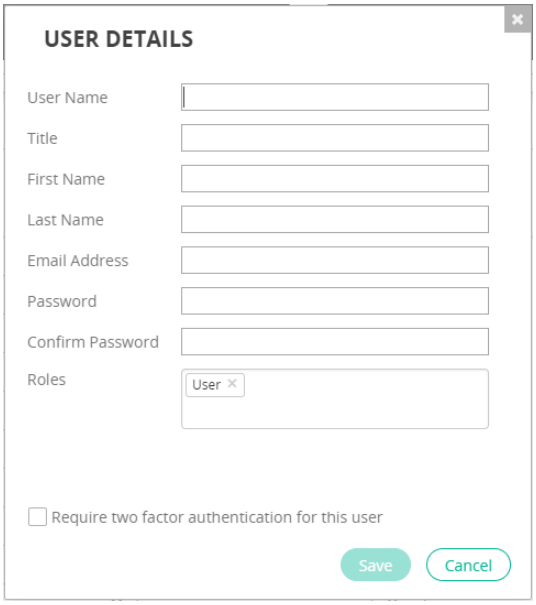


Users

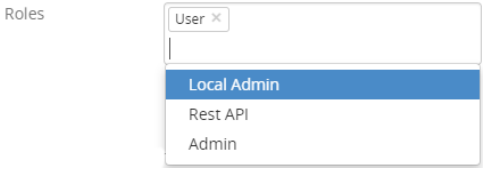
The USERS option specifies who is allowed to use the FortiEDR Central Manager console. During installation of the FortiEDR Central Manager, you must specify the user name and password of the first FortiEDR Central Manager console user. This is the only user who can log in to the FortiEDR Central Manager console for the first time.

To add a user:

1. Click the Add User button.
2. Fill in the displayed window.



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 three predefined user roles:
   - **Admin:** Is the highest-level super user that can perform all operations in the FortiEDR Central Manager console for all organizations. This role can create users for any organization. For more details, see *Chapter 11*, *Multi-tenancy* on page 183.
   - **Local Admin:** Is a super user that can perform all operations in the FortiEDR Central Manager console only for its own organization. Typically, the Local Administrator sets up the users for its organization. This role can only create users for its own organization.
   - **User:** This user is allowed to view all information and to perform actions, such as to mark events as handled, change policies and define Exceptions. This user is very similar to the Local Administrator. However, this user cannot access the **ADMINISTRATION** tab, which is described in this chapter.



Note – When upgrading FortiEDR from a version prior to V3.0, all administrators in the previous FortiEDR version are automatically assigned Administrator and Local Administrator privileges. You can decide whether to leave each such administrator with both sets of privileges, or to only assign them the Local Administrator role.

5. Check the **Require two-factor authentication for this user** checkbox if you want to require two-factor authentication for the user. When checked, this user must be authenticated using two-factor authentication in order to log in. For more details about two-factor authentication in FortiEDR, see the *Two-factor Authentication* section below.
6. 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 their user name and password whenever logging in to FortiEDR. In FortiEDR, two-factor authentication can be used with any third-party authentication application such as Google Authenticator, Microsoft Authenticator or Duo, in order to verify the user's identify.

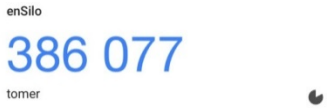
To designate that a user requires two-factor authentication, you must check the **Require two-factor authentication for this user** checkbox for that user, as described on page 152.

To log in using two-factor authentication (in this example we use the Google Authenticator app):

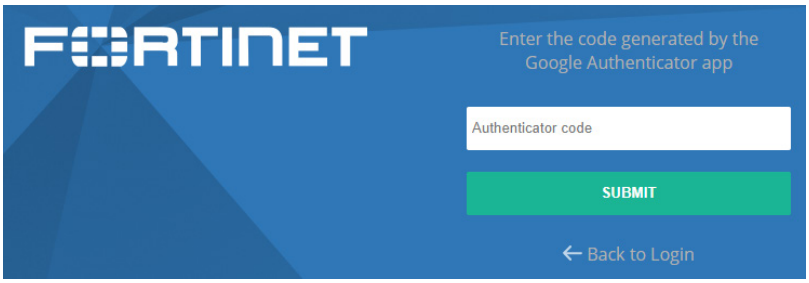
1. For a user who requires two-factor authentication to log in, the following window appears the first time that user attempts to log in.

2. Enter the user name and password and click **LOGIN**.
3. After clicking **LOGIN**, the user's identify must be verified using Google Authenticator. To do so, launch Google Authenticator by clicking the **Google Authenticator** icon on your mobile device. A QR code displays, as shown below:

4. Scan the QR code that displays in the FortiEDR window using your mobile device. After scanning, a FortiEDR token appears on the mobile device, as shown below. Note that this token (code) changes every 30 seconds.



5. In the FortiEDR login window, click the **INSERT AUTHENTICATOR CODE** button. The following window displays:



6. Enter the authentication token (code) you received in step **4**, and then click **SUBMIT**. Be sure to enter the latest code, as the code changes every 30 seconds.

   From this point on, the user can log in using the standard manner. Note that FortiEDR asks for a new token once every seven days. This means that you must repeat steps **1** through **6** when logging in to FortiEDR every seven days.

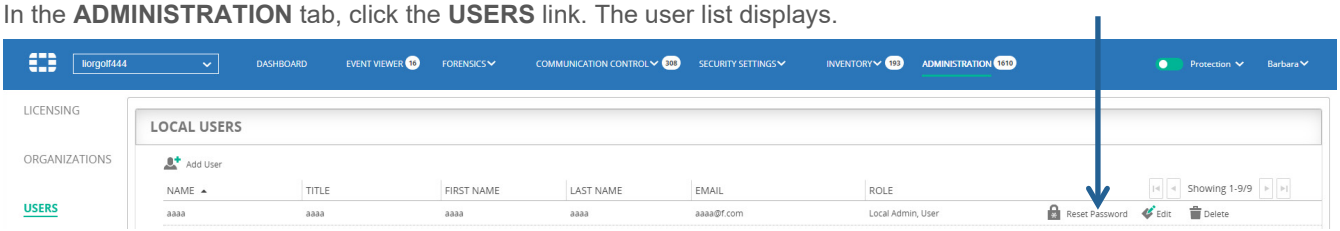
Resetting a User Password

Use the procedure described below to reset a user's password.

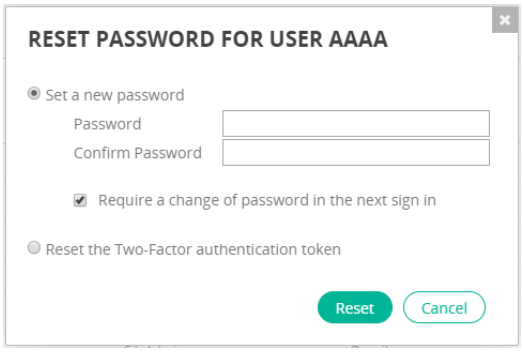
If a user who must use two-factor authentication cannot access the FortiEDR application because of a lost or replaced mobile device, that user must repeat the *To log in using two-factor authentication* procedure described on page 153 in order to log in. Before performing this procedure, you must first reset that user's password to accept a new two-factor authentication token, as described below.

To reset a user password:

1. In the **ADMINISTRATION** tab, click the **USERS** link. The user list displays.



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



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 *To log in using two-factor authentication* procedure described on page 153 in order to log in.
4. Click the **Reset** button.

LDAP Authentication

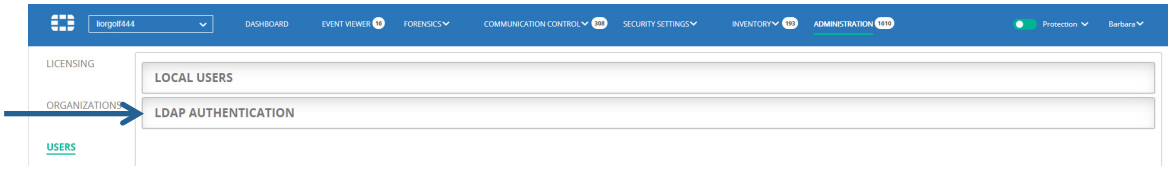
Lightweight Directory Access Protocol (LDAP) authentication is an open, industry-standard application protocol for accessing and maintaining distributed directory information services over an IP network. LDAP provides a central place to store usernames and passwords. This enables many different applications 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 **Admin ➔ User Settings**).

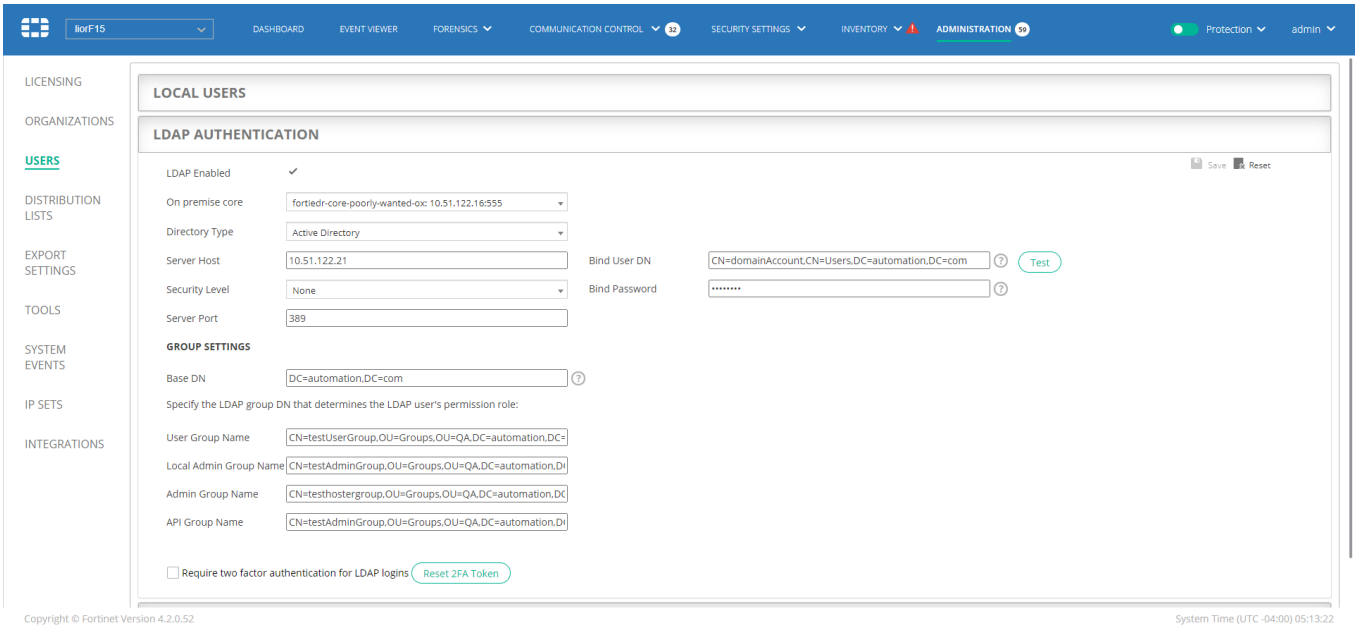
Before you start firewall configuration, make sure that your FortiEDR deployment includes an on-premise Core that has connectivity to the LDAP server. Details about how to install a FortiEDR on-premise Core can be found in *Installing the FortiEDR Core*.

To set up LDAP authentication in FortiEDR:

1. Click the LDAP AUTHENTICATION button.



The following window displays:



2. Fill in the following fields:
   - **LDAP Enabled:** Check this checkbox to enable LDAP authentication in FortiEDR.
   - **On Premise Core:** Select the on-premise FortiEDR Core that is to communicate with the LDAP server.

- **Directory Type:** Specify the type of central directory in use. FortiEDR supports **Active Directory** and **OpenLDAP**. The default is **Active Directory**.
- **Server Host:** Specify the IP address of your LDAP server.
- **Security Level:** Specify the protocol to be used for the secured connection – TLS, SSL or None.
- **Port:** This value is dependent on the security protocol that was selected.
- **Bind DN and Bind Password:** Specify the user and password for the authentication of FortiEDR in the Central Directory.
- **Base DN:** Specify the location in the Central Directory hierarchy where the Groups that are used for permission mapping can be found. For example, the DN for the root of the Domain should always work, but results in low performance.
- **User Group Name/Local Admin Group Name/Admin Group Name/API Group Name:** 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. Be sure to specify a name for the **User**, **Local Admin**, **Admin** and **API** groups. Each of these groups corresponds to a different role in FortiEDR.
- For example, to give the user **John** user permissions in FortiEDR (for both the FortiEDR application and the RESTful API), assign **John** to a **FortiEDRUsers** group that is defined in your Central Directory. Then, specify **FortiEDRUsers** in the text box next to the User Group Name in the LDAP configuration page of the FortiEDR management UI. Then, 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, matches the user role permissions.

3. If users must use two-factor authentication to log in, check the **Require two-factor authentication for LDAP logins** checkbox. For more details about two-factor login, see the *Two-factor Authentication* section on page 153.

   Note – Click the **Reset 2FA Token** button to reset the two-factor authentication token for a specific user. This process works in the same way as described in the *Resetting a User Password* section on page 154.

4. Click **Save**.

   Note – Users in Active Directory must not have a backslash (\) in the user name, in order for the name be supported by the FortiEDR console. In some cases in Active Directory, a backslash is added when there is a space between a user's first and last names. For example, "CN=Yell\, ".

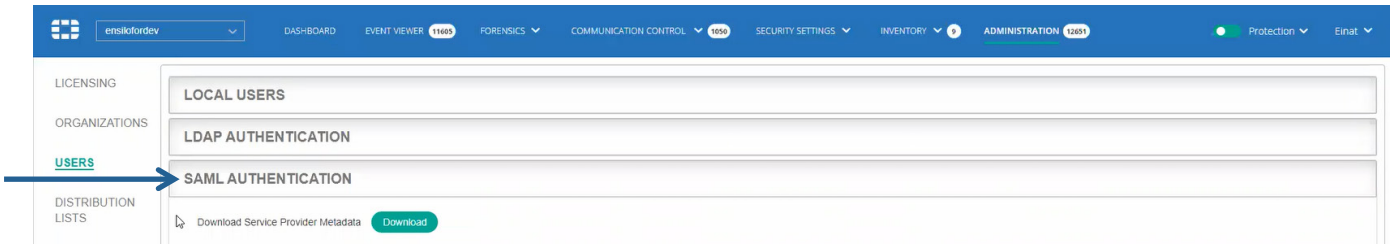
SAML Authentication

Security Assertion Markup Language (SAML) is an XML-based open standard for exchanging authentication and authorization data between parties, particularly between an identity provider (IdP) and a service provider (SP).

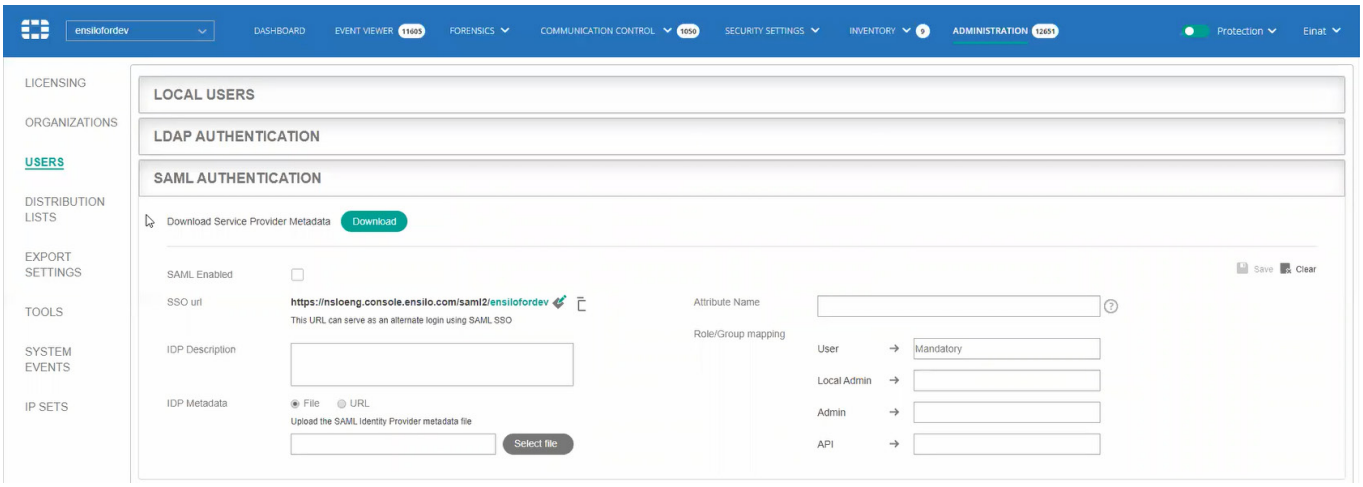
FortiEDR can act as an SP to authenticate users with a third-party IdP, enabling transparent user sign-in to the FortiEDR Central Manager Console.

To set up SAML authentication in FortiEDR:

1. 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:

   - **Entity ID:** Located under the **md:EntityDescriptor** tag, in the **entityID** attribute.
   - **Logout Address Value:** Located under the **md:SingleLogoutService** tag, in the **Location** attribute.
   - **Login Address Value:** Located under the **md:AssertionConsumerService** tag, in the **Location** attribute.
   - **Certificate Value(Public):** Located under the **ds:X509Certificate** tag.

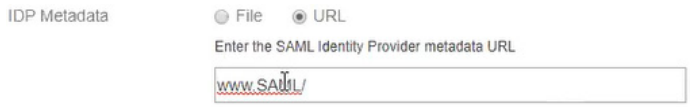
3. Fill in the following fields:

   - **SAML Enabled:** Check this checkbox to enable SAML authentication in FortiEDR.
   - **SSO URL:** Specify the URL to be used by users to log in to FortiEDR. If necessary, you can edit the suffix of this URL (shown in green) by clicking the **Edit** button and then modifying it as needed. You can also copy the URL to the clipboard using the **Copy** button (for example, in order to email the FortiEDR SAML login page to your users).

     Make sure that the suffix does not include any spaces.

   - **IDP Description:** Specify a free-text description. For example, you may want to specify the IdP server that you are using here.
   - **IDP Metadata:** Upload the IdP metadata to FortiEDR. You can either upload an *.XML file or a URL. To upload a file, click the **File** radio button and then click the **Select File** button to navigate to and select the applicable *.XML file. To upload a URL, click the **URL** radio button and then specify the requisite URL.

   - **Attribute Name:** Specify the name of the attribute to be read by FortiEDR, in order to determine the permissions and role to be assigned to that user in FortiEDR. This attribute must be included as part of the response from the identify provider server to FortiEDR when a user attempts to log in to FortiEDR.

- **Role/Group Mapping:** Specify an attribute value for the **User**, **Local Admin**, **Admin** and **API** groups. You must specify a value for at least one of these user roles. Each of these groups corresponds to a different role in FortiEDR.

Note that 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.

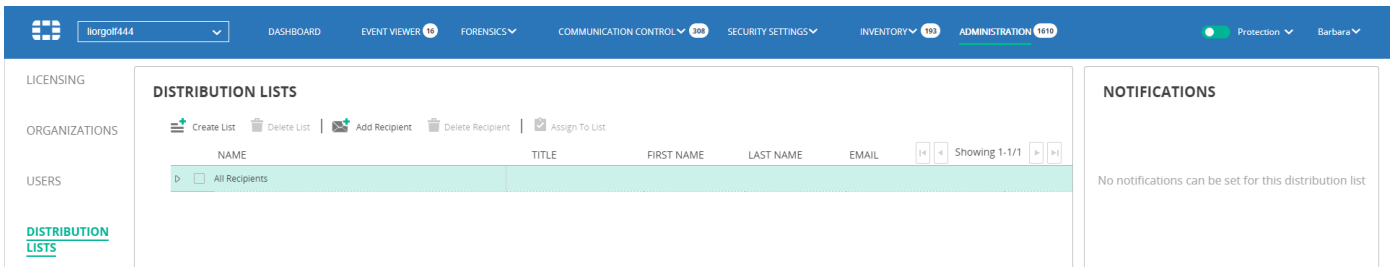
4. Click **Save**.

Distribution Lists

The **DISTRIBUTION LISTS** option enables you to specify recipients who will receive an email each time an event is triggered by FortiEDR.

Note – You must configure SMTP before using the Distribution List option. For more details, see page 159.
Note – Emails are only sent for 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.

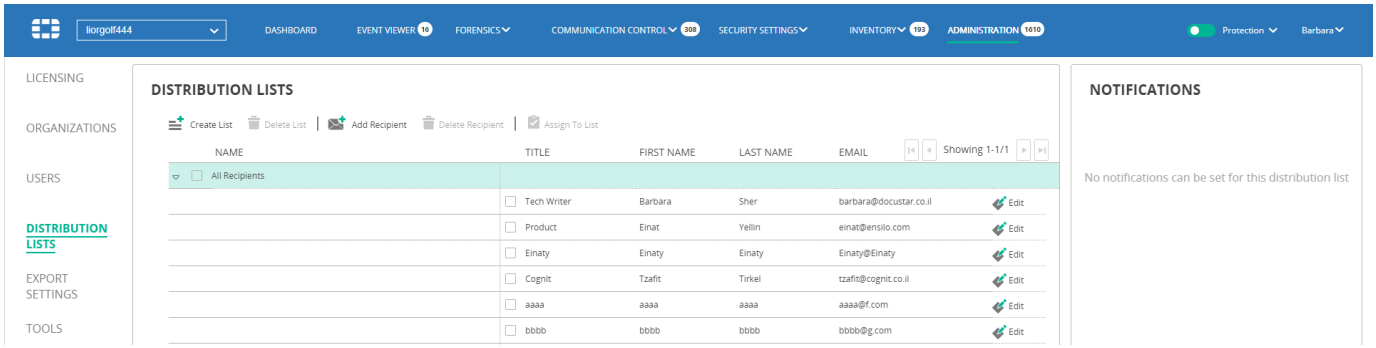
Each email contains all the raw data items collected by FortiEDR about that event. The system is provided with a Distribution List called All Recipients that contains all FortiEDR Central Manager users. All other recipients that are added to the system are also automatically added to the **All Recipients** list.



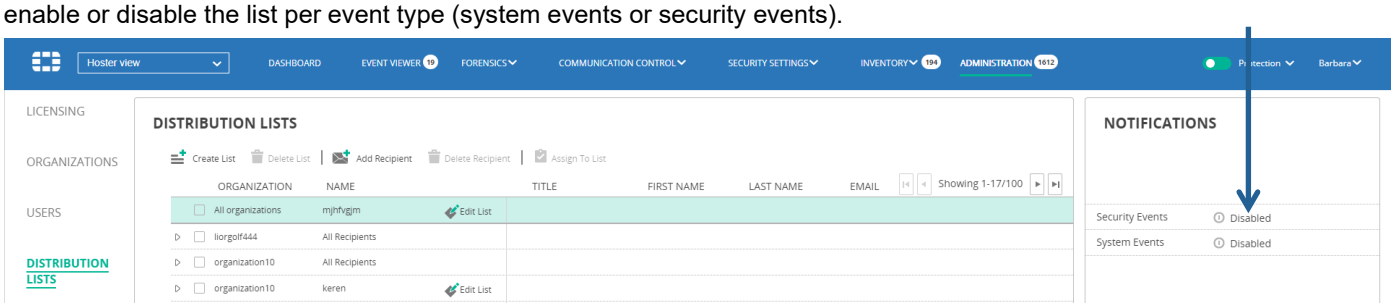
This window displays a row for each Distribution List. Click the button in a row to view the recipients assigned to that list.

Use the Create List button to create a new Distribution List.

Use the Add Recipient button to add a recipient/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).



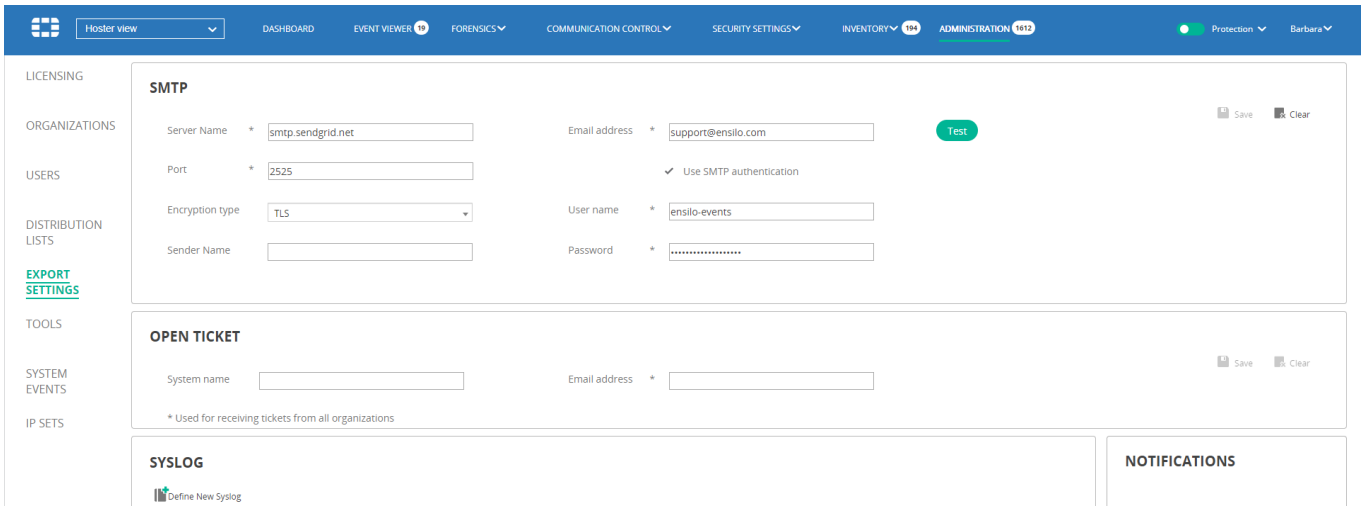
Export Settings

The **EXPORT SETTINGS** option provides access to the following options:

- **SMTP,** page 159
- **OPEN TICKET,** page 160
- **SYSLOG,** page 160

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.



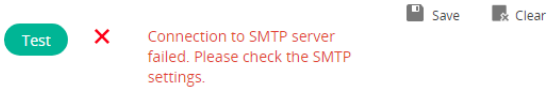
Note – In a single-organization system, SMTP settings are only accessible in Hoster view (for administrators), or to the local administrator of that organization.

To configure SMTP server settings:

- In the SMTP area, enter standard SMTP settings and then click **Save**.

To test SMTP server connectivity:

- In the SMTP area, click **Test**. An error message displays if there is no connectivity to the server.

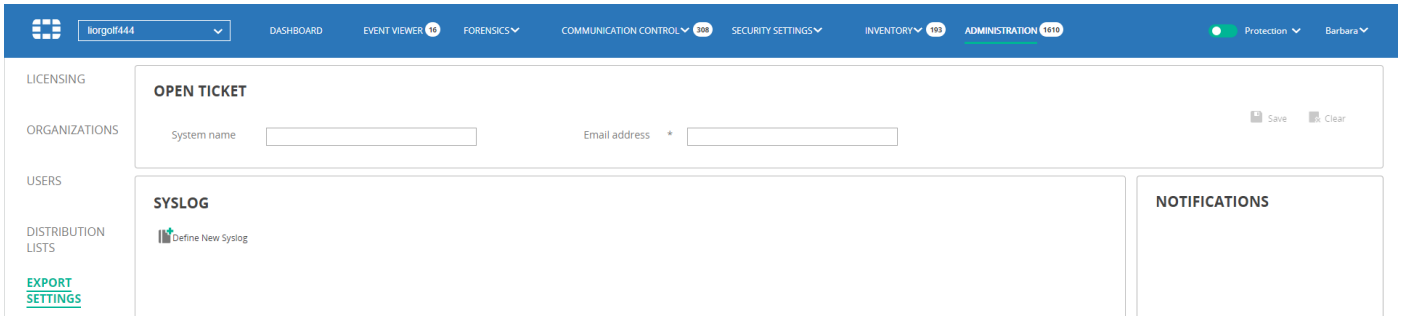


Open Ticket

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.

Note – 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 207.
Note – 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.



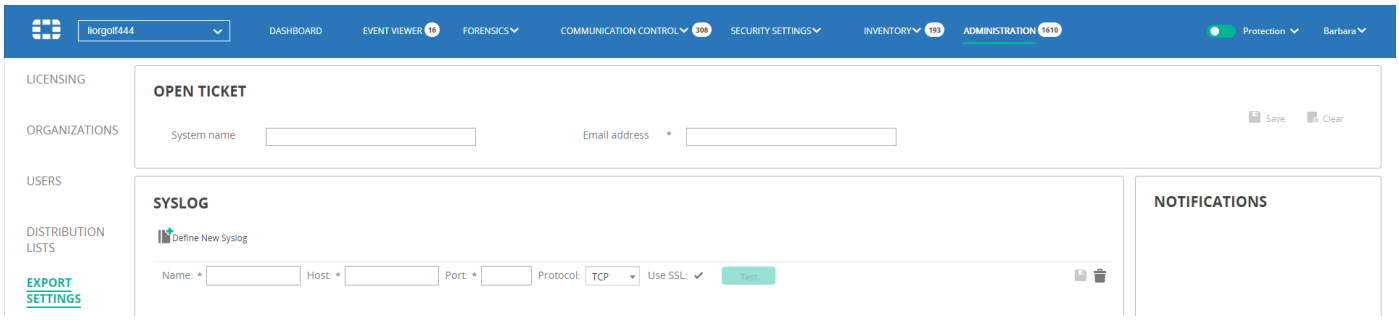
To configure Open Ticket settings:

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 event aggregations. Each entry contains a raw data ID and an event ID. Raw data items belonging to the same event aggregation share the same event ID, which enables the SIEM to combine them into one event on the SIEM side, in order to remain aligned with the FortiEDR system.



Use the Define New Syslog button to define a new Syslog destination. The **Syslog Name** is a free-text field that identifies this destination in the FortiEDR.

Note – Syslog messages are only sent for 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.

All other fields are standard Syslog parameters that the FortiEDR Central Manager is able to send. Check the checkbox of the fields that you want to be sent to your Syslog.

Select a syslog destination row and then 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).

Syslog Notifications

Syslog includes the following types of notifications:

- Security event with the following fields:
  - Event ID
  - Device Name
  - Process Path
  - Certificate
  - Last Seen
  - Severity
  - Count
  - MAC Address
  - Source IP
  - Raw Data ID
  - Process Name
  - Process Type
  - First Seen
  - Destination
  - Action
  - Rules List
  - Classification
  - Organization
  - Organization ID
  - Operating System
  - Script
  - Script Path
  - Country
  - Users
  - Device State
  - Autonomous System
  - Process Hash
- System event (see page 173) with the following fields:
  - Component Type
  - Component Name
  - Description
  - Date
- Audit trail event (see page 163) with the following fields:
  - Date
  - Module
  - Username
  - Action Description

Syslog Message

The order of the fields in the Syslog message is as follows:

1. Organization
2. Organization ID
3. Event ID
4. Raw Data ID
5. Device Name
6. Device State
7. Operating System
8. Process Name
9. Process Path
10. 1Process Type
11. 1Severity
12. Classification
13. Destination
14. First Seen
15. Last Seen
16. Action
17. Count
18. Certificate
19. Rules List
20. Users
21. MAC Address
22. Script
23. Script Path
24. Autonomous System
25. Country
26. Process Hash
27. Source IP

Syslog Message Format

The Syslog message contains the following sections:

1. **Facility Code:** All messages have the value 16 (Custom App).
2. **Severity:** All messages have the value 5 (Notice).
3. **MessageType:** Enables you to differentiate between syslog message categories – Security Event, System Event or Audit.
4. **Message Text:** Contains the name and value of all the selected fields.
   For example, Device name: Laptop123. Each field is separated by a semi-colon (;).

Tools

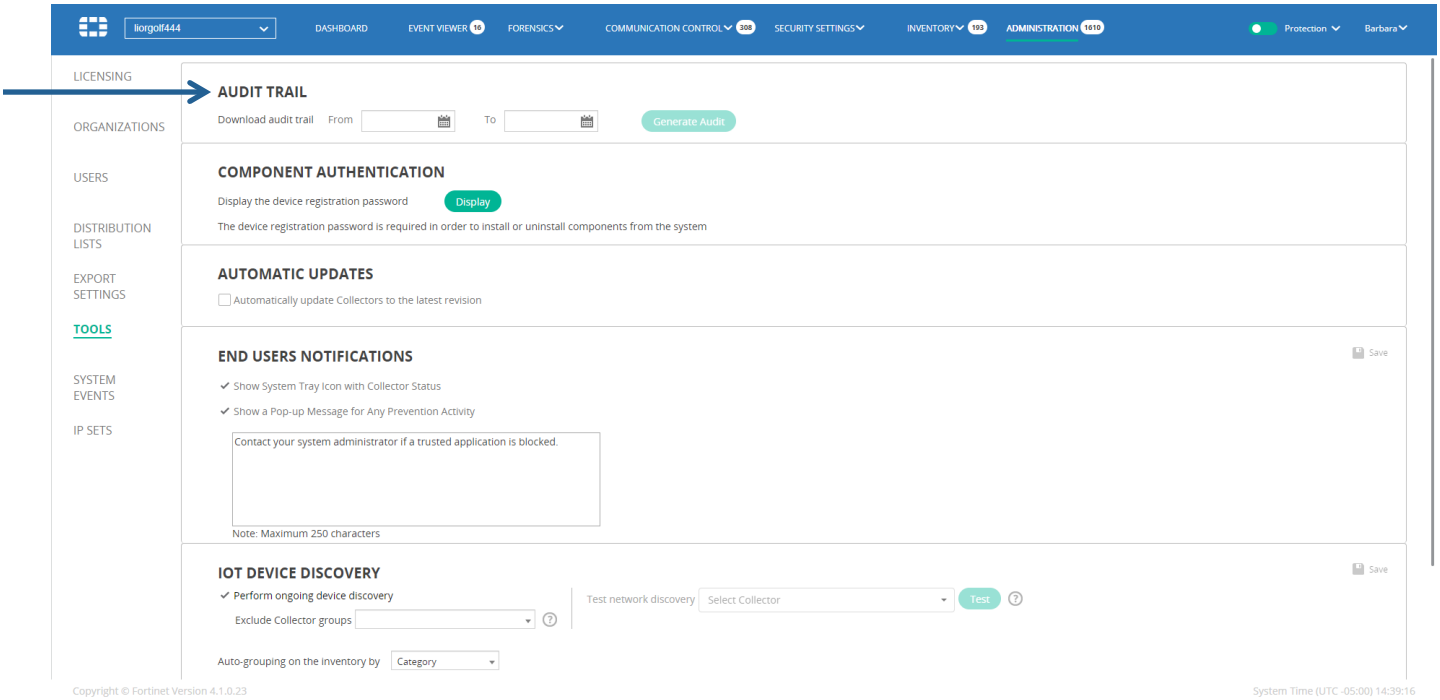
The **TOOLS** option provides access to the following options:

- **Audit Trail,** page 163
- **Component Authentication,** page 164
- **Automatic Updates,** page 165
- **File Scan,** page 165
- **End-user Notifications,** page 166
- **IoT Device Discovery,** page 168
- **Personal Data Handling,** page 169

Audit Trail

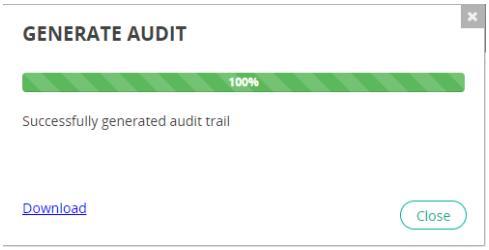
FortiEDR's audit mechanism records every user action in the FortiEDR system. System actions are not recorded. You can download the audit trail to a *.csv file for further analysis.

Each time a new audit trail is created, it can be sent through the Syslog.

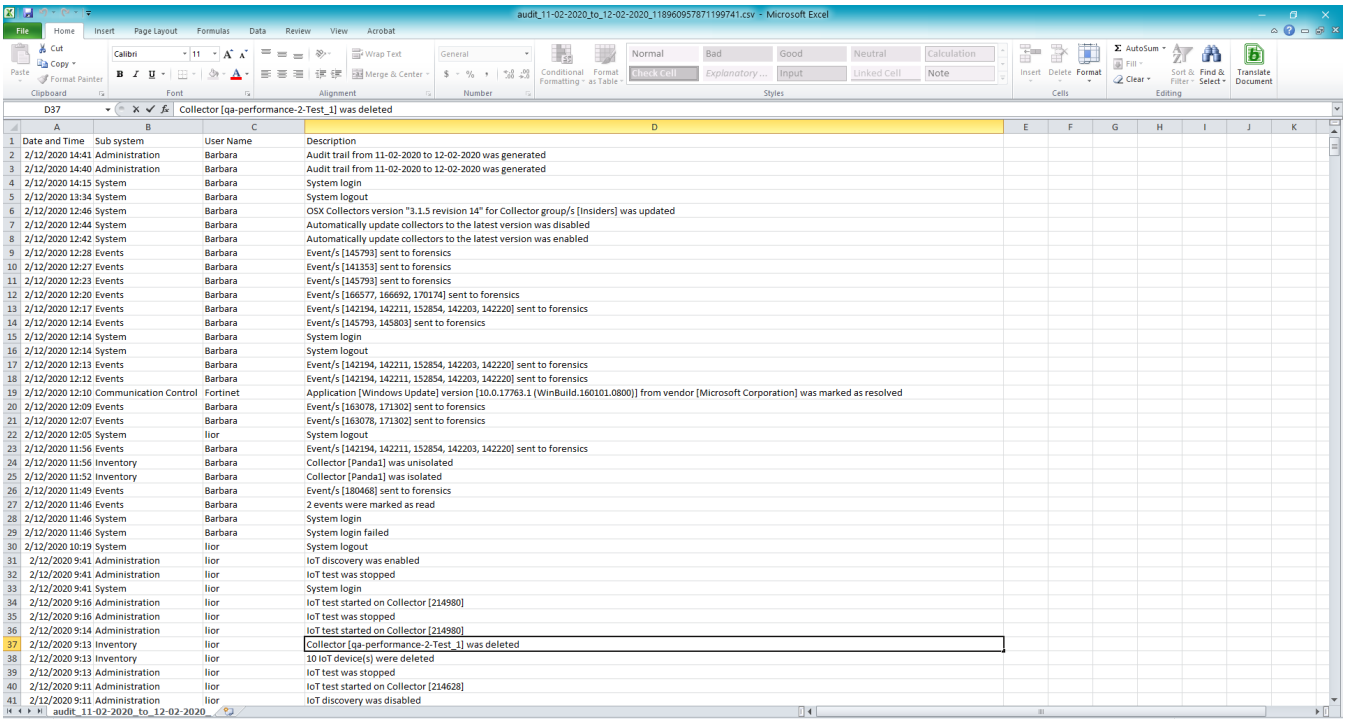


To generate the audit trail:

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. An Excel file, such as the example shown below, displays:



Date and Time	Sub system	User Name	Description
2/12/2020 14:41	Administration	Barbara	Audit trail from 11-02-2020 to 12-02-2020 was generated
2/12/2020 14:40	Administration	Barbara	Audit trail from 11-02-2020 to 12-02-2020 was generated
2/12/2020 14:15	System	Barbara	System login
2/12/2020 13:34	System	Barbara	System logout
2/12/2020 12:46	System	Barbara	OSX Collectors version "3.1.5 revision 14" for Collector group/s [Insiders] was updated
2/12/2020 12:44	System	Barbara	Automatically update collectors to the latest version was disabled
2/12/2020 12:42	System	Barbara	Automatically update collectors to the latest version was enabled
2/12/2020 12:28	Events	Barbara	Event/s [145793] sent to forensics
2/12/2020 12:27	Events	Barbara	Event/s [141353] sent to forensics
2/12/2020 12:23	Events	Barbara	Event/s [145793] sent to forensics
2/12/2020 12:20	Events	Barbara	Event/s [166577, 166692, 170174] sent to forensics
2/12/2020 12:17	Events	Barbara	Event/s [142194, 142211, 152854, 142203, 142220] sent to forensics
2/12/2020 12:14	Events	Barbara	Event/s [145793, 145803] sent to forensics
2/12/2020 12:14	System	Barbara	System login
2/12/2020 12:14	System	Barbara	System logout
2/12/2020 12:13	Events	Barbara	Event/s [142194, 142211, 152854, 142203, 142220] sent to forensics
2/12/2020 12:12	Events	Barbara	Event/s [142194, 142211, 152854, 142203, 142220] sent to forensics
2/12/2020 12:10	Communication Control	Fortinet	Application [Windows Update] version [10.0.17763.1 (WinBuild.160101.0800)] from vendor [Microsoft Corporation] was marked as resolved
2/12/2020 12:09	Events	Barbara	Event/s [163078, 171302] sent to forensics
2/12/2020 12:07	Events	Barbara	Event/s [163078, 171302] sent to forensics
2/12/2020 12:05	System	lior	System logout
2/12/2020 11:56	Events	Barbara	Event/s [142194, 142211, 152854, 142203, 142220] sent to forensics
2/12/2020 11:56	Inventory	Barbara	Collector [Panda1] was unisolated
2/12/2020 11:52	Inventory	Barbara	Collector [Panda1] was isolated
2/12/2020 11:49	Events	Barbara	Event/s [180468] sent to forensics
2/12/2020 11:46	Events	Barbara	2 events were marked as read
2/12/2020 11:46	System	Barbara	System login
2/12/2020 11:46	System	Barbara	System login failed
2/12/2020 10:19	System	lior	System logout
2/12/2020 9:41	Administration	lior	IoT discovery was enabled
2/12/2020 9:41	Administration	lior	IoT test was stopped
2/12/2020 9:41	System	lior	System login
2/12/2020 9:16	Administration	lior	IoT test started on Collector [214980]
2/12/2020 9:16	Administration	lior	IoT test was stopped
2/12/2020 9:14	Administration	lior	IoT test started on Collector [214980]
2/12/2020 9:13	Inventory	lior	Collector [qa-performance-2-Test_1] was deleted
2/12/2020 9:13	Inventory	lior	10 IoT device(s) were deleted
2/12/2020 9:13	Administration	lior	IoT test was stopped
2/12/2020 9:11	Administration	lior	IoT test started on Collector [214628]
2/12/2020 9:11	Administration	lior	IoT discovery was disabled

Each row in the audit trail file contains the following columns of information:

- **Date and Time:** Displays the date and time in the format yyyy-mm-dd hh:mm:ss.
- **Sub system:** Displays the change type, such as System, Configuration, Administration, Forensics, Events, Inventory, Communication Control or Health.
- **User Name:** Displays the name of the user.
- **Description:** Displays the action and/or a description.

The following actions can be audited:

- System actions
- Policy actions
- Forensic actions
- Administrative actions
- Events
- Inventory actions
- System health changes

Note – 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

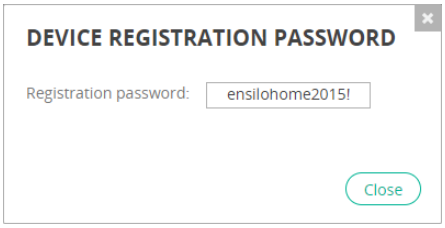
Component Authentication

In order to install, upgrade or uninstall a Collector, you must supply the Aggregator password. The Aggregator password is the same for all Collectors in the FortiEDR system. This password is defined during initial system installation. For more details, see the *Installing the FortiEDR Central Manager and FortiEDR Aggregator on the Same Machine* section on page 24.

If you forget the Aggregator 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.



Automatic Collector Updates

The Automatic Collector Updates feature updates the revision for a given FortiEDR version. The revision number is the fourth digit of the FortiEDR version number. For example, for FortiEDR version 3.1.0.**x**, **x** indicates the revision number.

When the **Automatically update Collectors to the latest revision** checkbox is checked, whenever the content contains a new build only (for example, 2.7.0.15 is a new build of 2.7.0.5), all Collectors are uploaded 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 page 32.

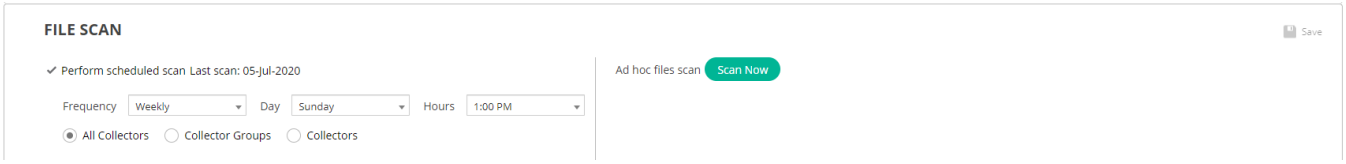
To update a FortiEDR version, use the Update Collector Version feature described on page 148.

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, an event is triggered.

To schedule a periodic scan:

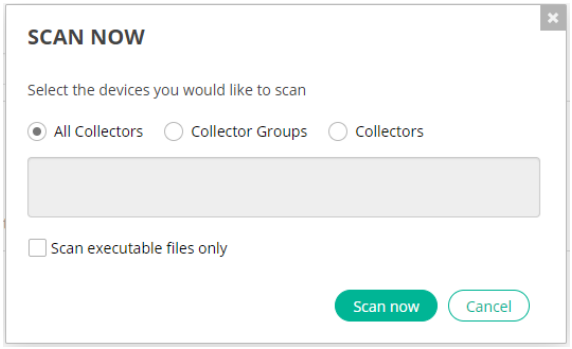
1. Click the **TOOLS** link in the left pane.
2. In the FILE SCAN area, check the **Perform Scheduled Scan** checkbox. This checkbox must be checked to perform the scan according to the designated schedule.



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 FILE SCAN area, click the **Scan Now** button. The following displays:



3. 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.
4. 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.
5. Click **Scan Now**. The scan is performed immediately.

End-user Notifications

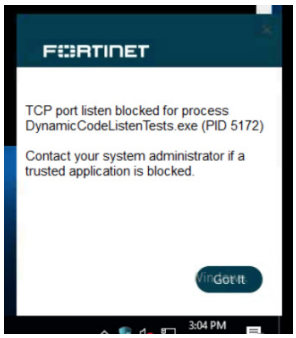
Each device protected by FortiEDR can display an icon in the system tray to indicate its state.

The FortiEDR icon indicates the current state of the device, as follows:

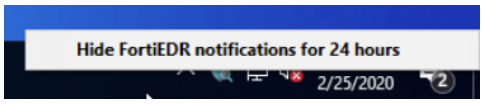
-  – Protection On
-  – Protection Off/Disabled
-  – Degraded
-  – Isolated

Note – 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...

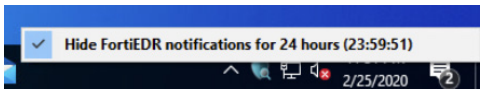
When the FortiEDR icon is configured to display on FortiEDR-protected devices, a popup message displays whenever something is blocked on a protected device (based on the blocking policy set for that device). File modifications (due to suspected ransomware), the exfiltration of external connections and execution prevention actions can be blocked. For example, the following shows that a TCP port listening action was blocked for the **DynamicCodeListenTests.exe** process.



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.



Hide Notifications



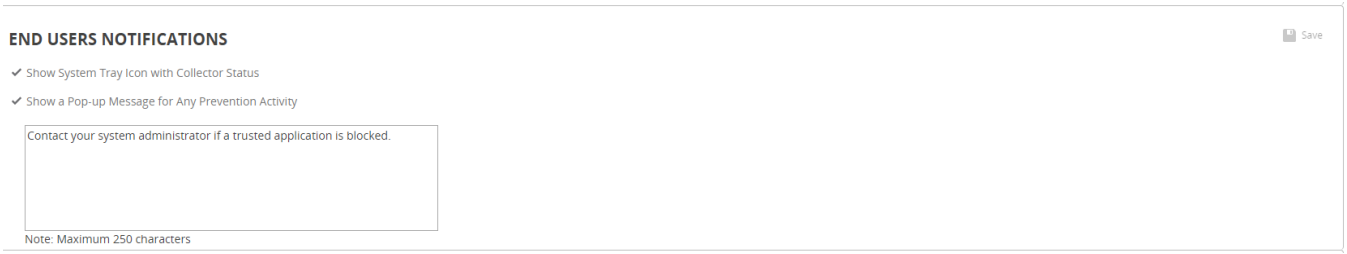
Display Notifications

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:

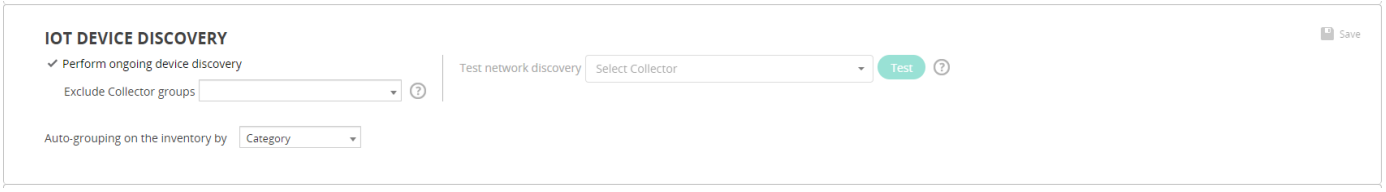


   - **Show System Tray Icon with Collector Status:** Check this checkbox to display the FortiEDR icon on each FortiEDR-protected device or leave the checkbox unchecked to hide the icon on each protected device. Your selection here is applied on all protected devices. The default is checked.
   - **Show 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.
3. 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 on page 76.



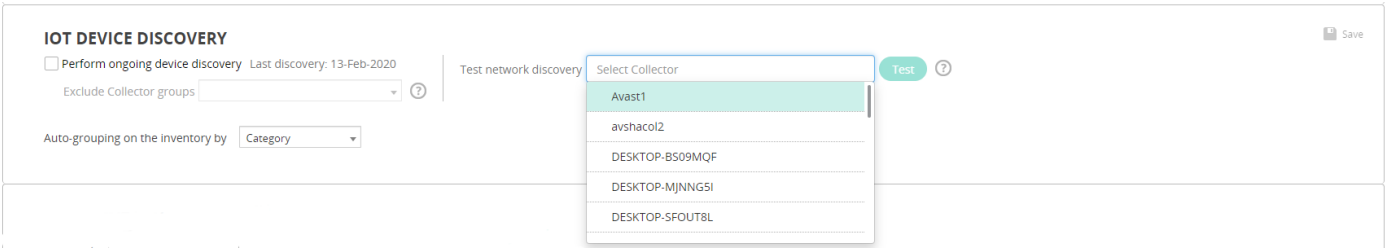
To enable IoT device discovery, check the **Perform ongoing device discovery** checkbox. Note that when doing so, all relevant Collectors in the system perform sniffing in order to identify new connected devices in the system. When performing this discovery process, FortiEDR uses only the most powerful 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.

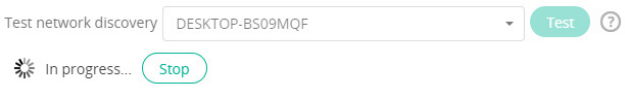
The **Auto-grouping on the inventory by** option enables you to group discovered devices by device type. For example, cameras, network devices, media devices, printers and so on. Select the **Category** option in the dropdown list to group discovered devices by device type or **None** not to. When you select Category, devices are auto-grouped in the **IOT DEVICES** page, as shown on page 76.

Click the **Save** button 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 **Test 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).

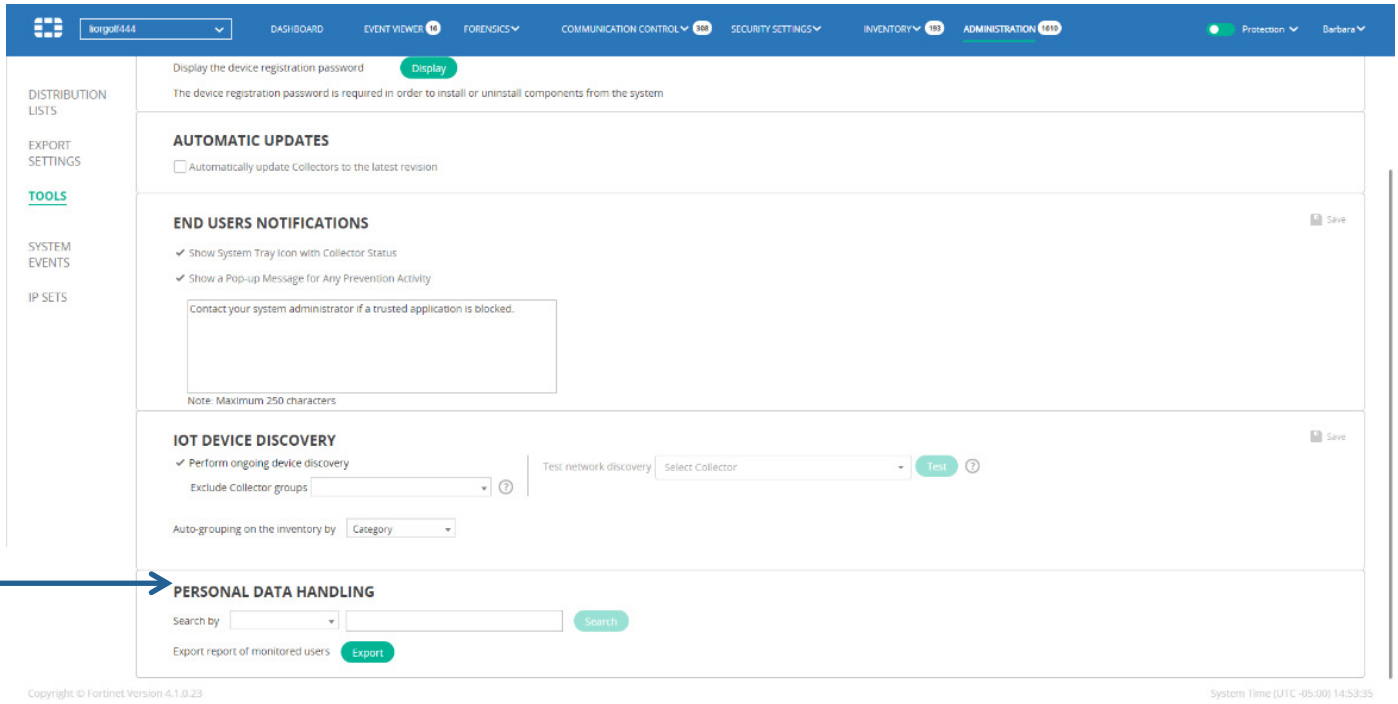


Personal Data Handling

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.

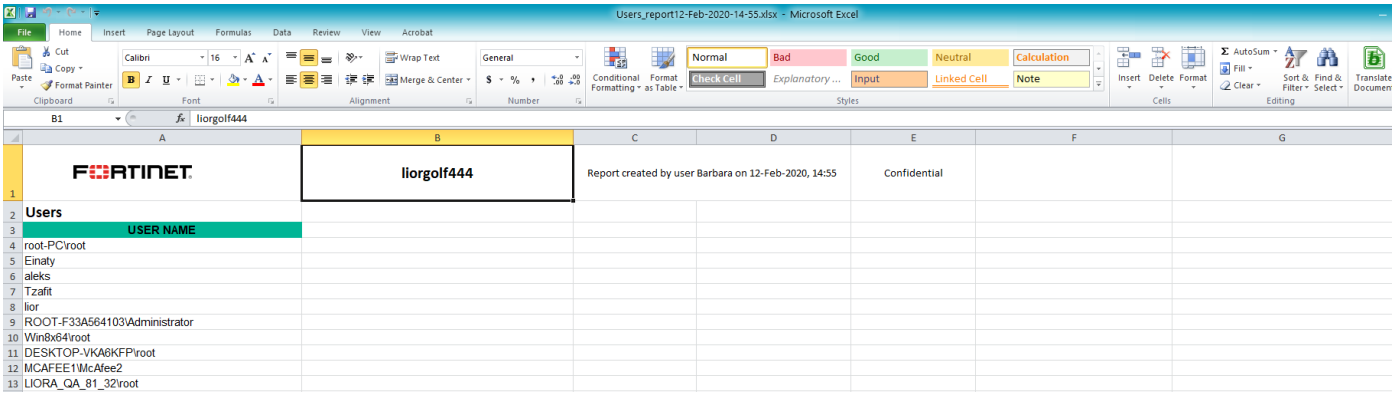
The GDPR standard requires that all relevant data for an employee of a company that is using the FortiEDR system or a FortiEDR user be removed from the FortiEDR system, once he/she no longer has access to or uses the FortiEDR system.

In FortiEDR, the GDPR feature is implemented in the Personal Data Handling area of the Tools window.



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:



To remove employee/user data from the FortiEDR system for GDPR compliance:

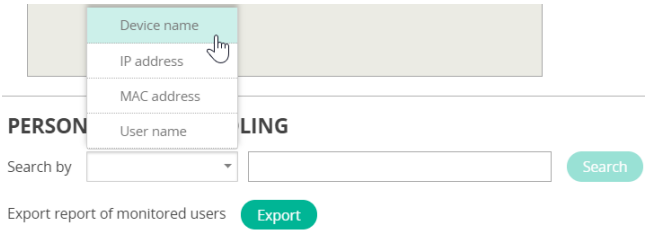
1. Uninstall the Collector from the employee's/user's computer. This step is important, so that no further data is collected from that Collector. For more details about uninstalling, see page 49.

   Note – 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.

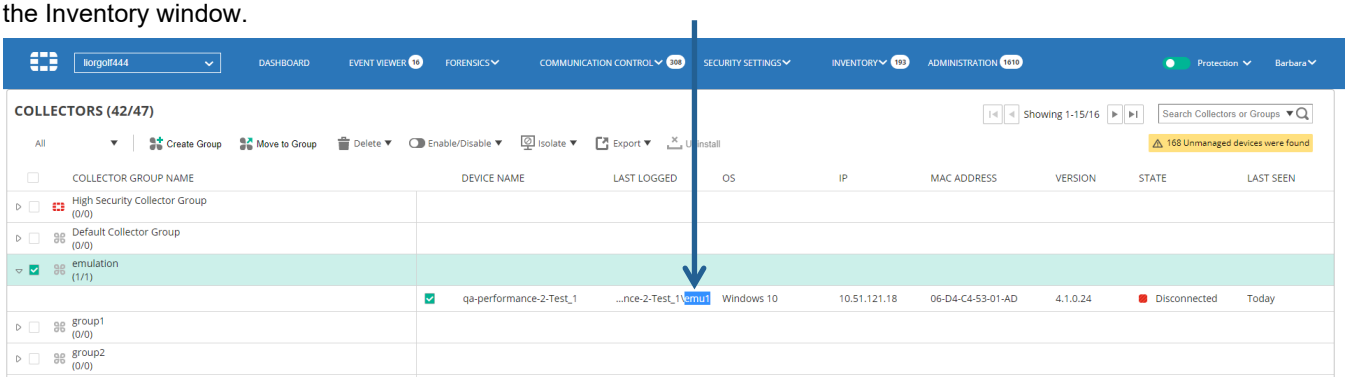
   Note – If the employee/user has multiple computers on which Collectors are installed, you must repeat the steps below for each of his/her computers.

   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.

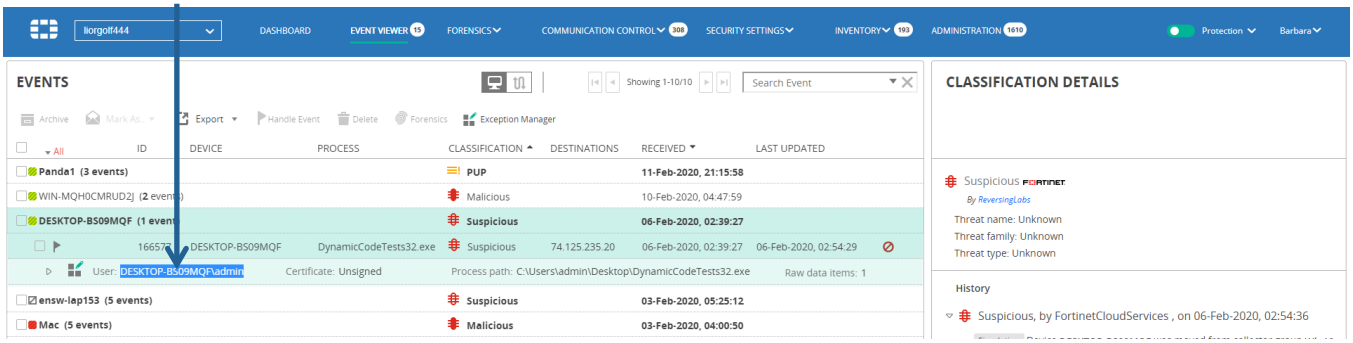
   IMPORTANT – You can remove the device name, IP address, MAC address and user name of the employee/user from FortiEDR in any order that you prefer. However, you **must** remove all device name, IP address, MAC address and user name data from FortiEDR in order to fully comply with the GDPR standard.
4. 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.



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.

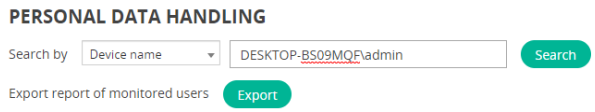


In a similar manner, you can locate the user name in the Event Viewer, and then copy/paste that information into the adjacent field in the Personal Data Handling area, as shown below:

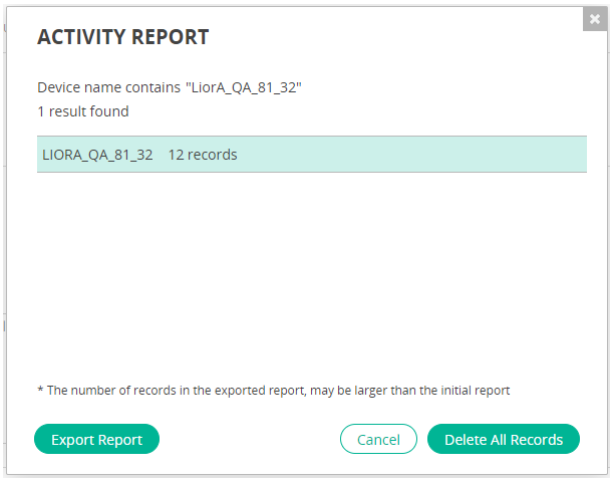


If you prefer, you can use another method of your choice to identify the device name.

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.



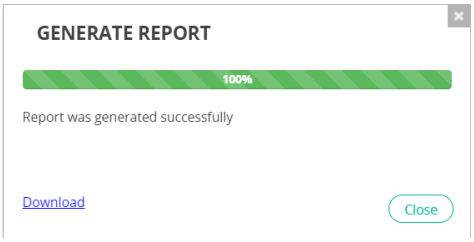
The following displays, listing all matching results:



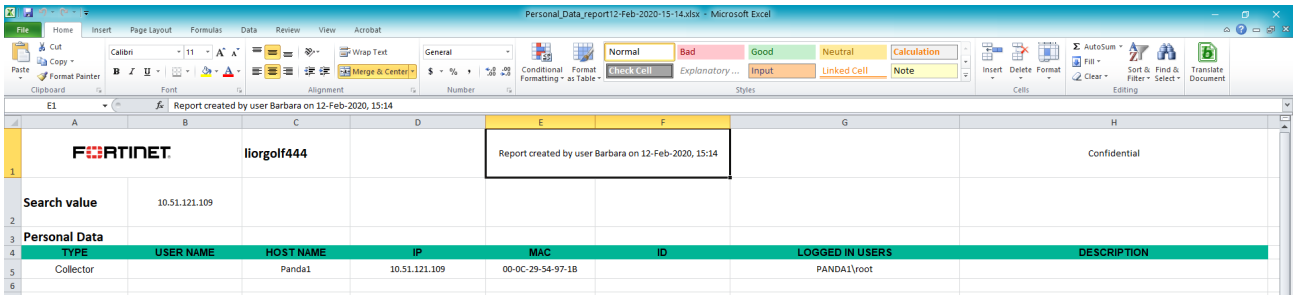
7. Do one of the following:

- 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:

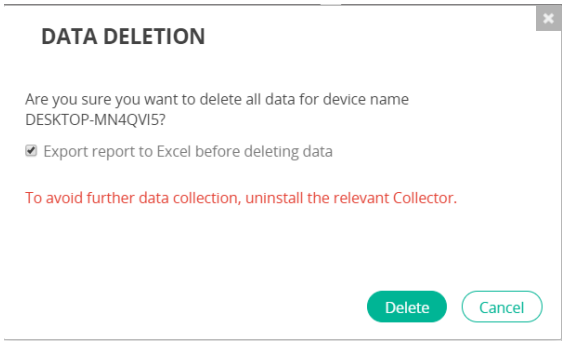


Click the **Download** link to download the Excel report. An example of the downloaded report is shown below:

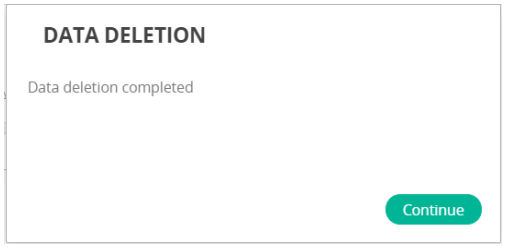


–OR–

- 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:

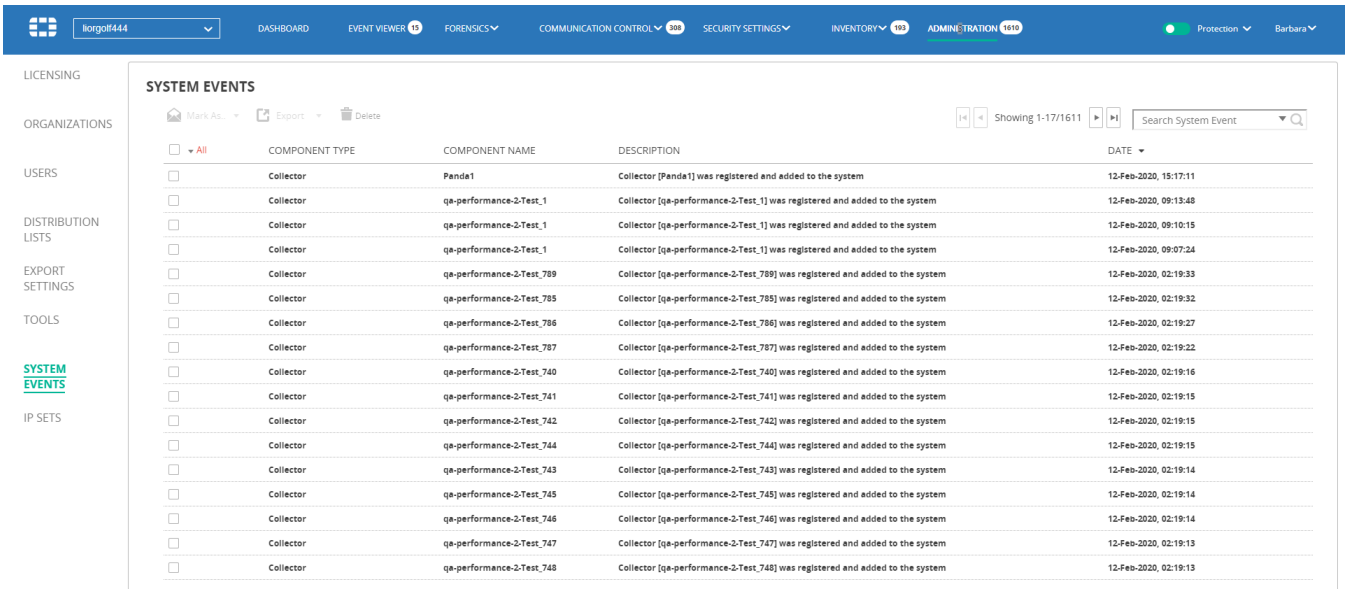


You can check the **Export report to Excel before deleting data** checkbox if you want to export the data before it is removed from FortiEDR.

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**.

System Events

Selecting **SYSTEM EVENTS** in the **ADMINISTRATION** tab displays all the events relevant to the FortiEDR system.



When a system event is triggered, it is sent via email to the defined distribution list. For more details, you may refer to the *Distribution Lists* section on page 158.

Note – System events can also be retrieved using an API command. For more details, refer to the *FortiEDR RESTful API Guide*.

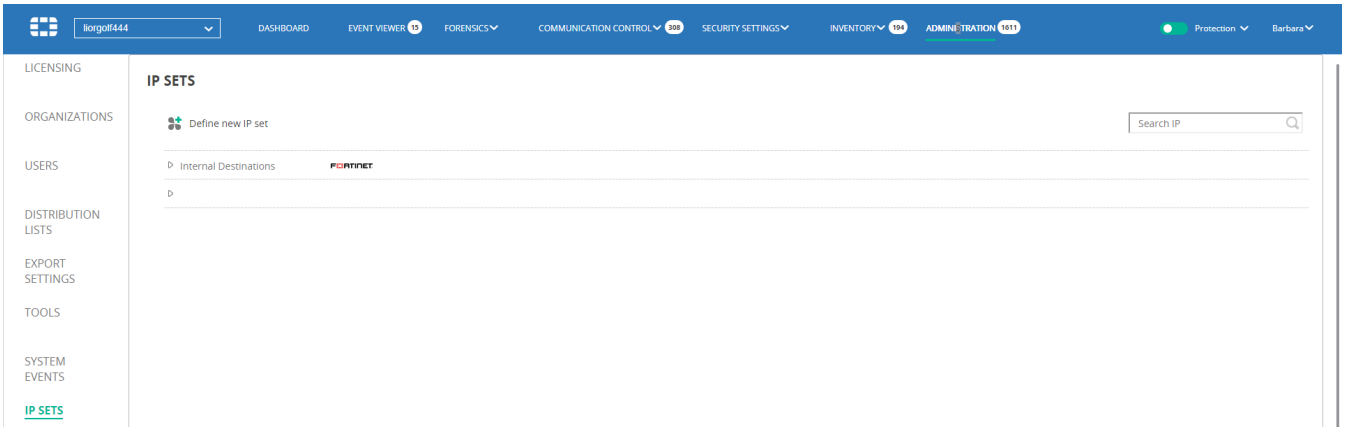
Each time a new system event is created, it can be sent through the Syslog.

The following events are defined as system events in the system. The user receives a notification for each of them:

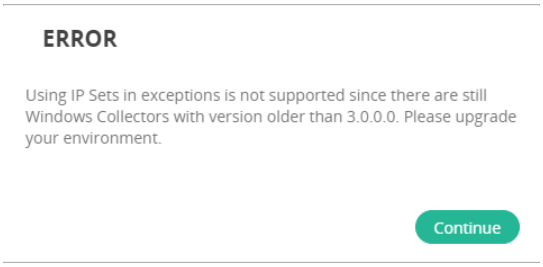
- Core state was changed to Disconnected (and another event when the Core state was returned to the Connected state immediately afterward)
- Core state was changed to Degraded (and another event when the Core state was returned to THE Connected state immediately afterward)
- Aggregator state was changed 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)
- Collector registered for the first time (only UI/API; is not sent by email/Syslog)
- Collector state was changed to Degraded (and another event when the Collector state was returned to the Connected state immediately afterward)
- Collector state was changed to Disabled (and another event when the Collector state was returned to the Connected state immediately afterward)
- 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 events. This feature is used when defining exceptions.



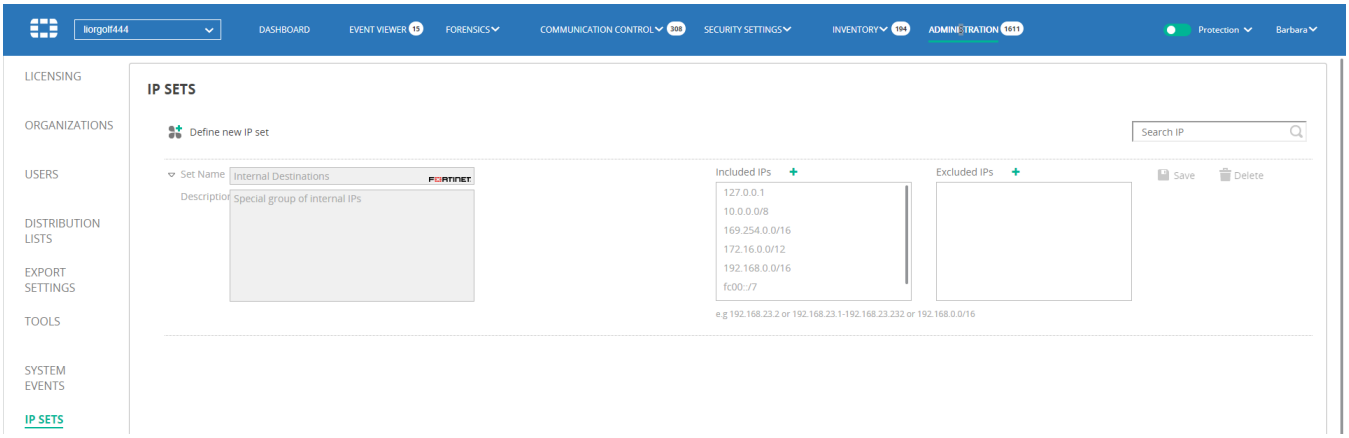
Note – IP Sets can only be defined if all Collectors are V3.0.0.0 and up. If you attempt to define an exception and all Collectors are not V3.0.0.0 or above, the following error message displays:



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.

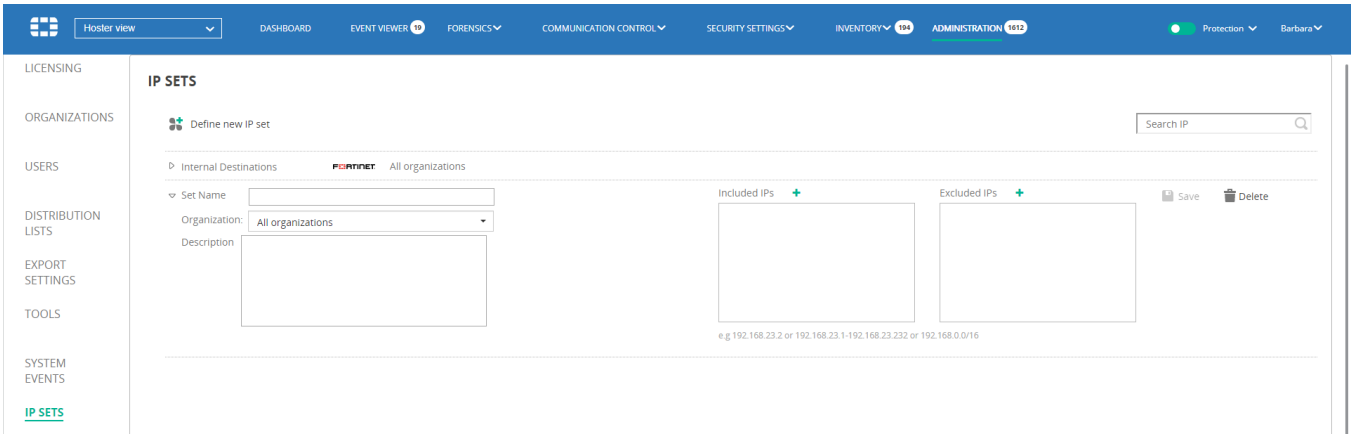
The IP Sets window lists all the IP sets created by the Administrator. A Local Administrator can edit an IP set that was specifically created for his/her organization. A Local Administrator cannot edit an IP set that applies to all organizations.

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. 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 + button to add an IP, IP range or IP mask to be included in the IP set's definition. Each click of the + 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 + button to add an IP, IP range or IP mask that is to be excluded.
6. Click the **Save** button.

The **Search IP** field at the top-right of the page enables you to search for a specific IP in all of the IP sets defined. The search option identifies matching IPs, even if they are part of a range in an IP set's definition.

To use an IP set:

- Select an IP set in the Destinations area when defining an exception, as described on pages 99 and 100.

Integrations

Integrations enable you to configure connectors to external systems. FortiEDR connectors utilize Fortinet products' APIs to automatically perform the required actions to extend its automatic Playbook actions.

You can set up an unlimited number of connectors for each type and use them by associating Playbook policies or Security policies to their actions, as specified below.

Firewall Integration

When a FortiGate connector is set and Playbook policies are configured, automatic incident response actions can include blocking of malicious IP addresses by FortiGate upon event triggering.

Before you start firewall configuration, make sure that:

- Your FortiEDR deployment includes an on-premise Core that has connectivity to the firewall.
  Details about how to install a FortiEDR on-premise Core are described in *Installing the FortiEDR Core*.
- The FortiEDR Central Manager has connectivity to the Fortinet Cloud Services (FCS).
- You have a valid API user with access to FortiGate.

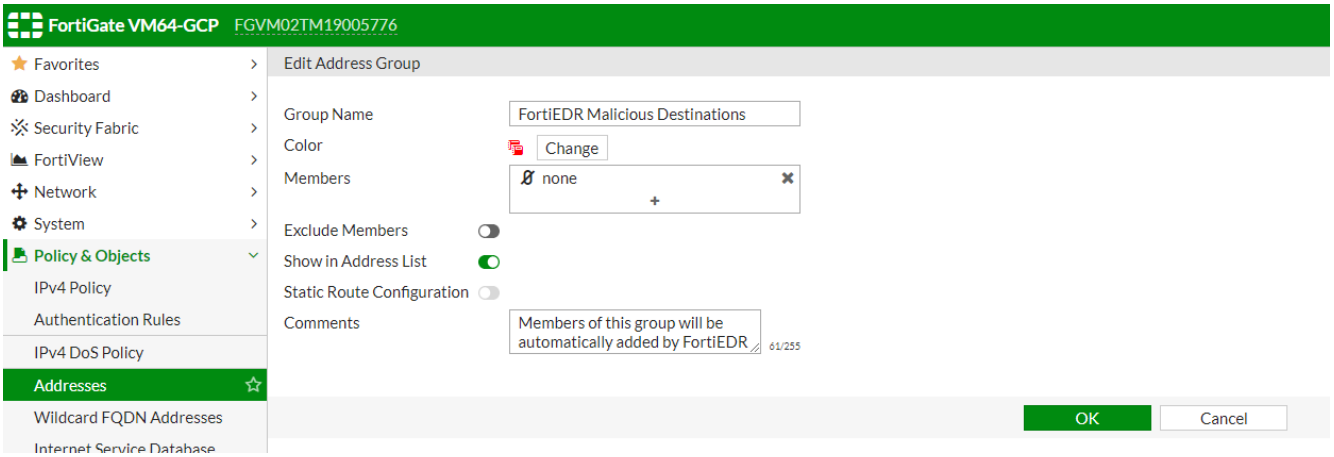
Follow the steps below to automatically deny access on FortiGate to malicious destination addresses detected by FortiEDR.

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.

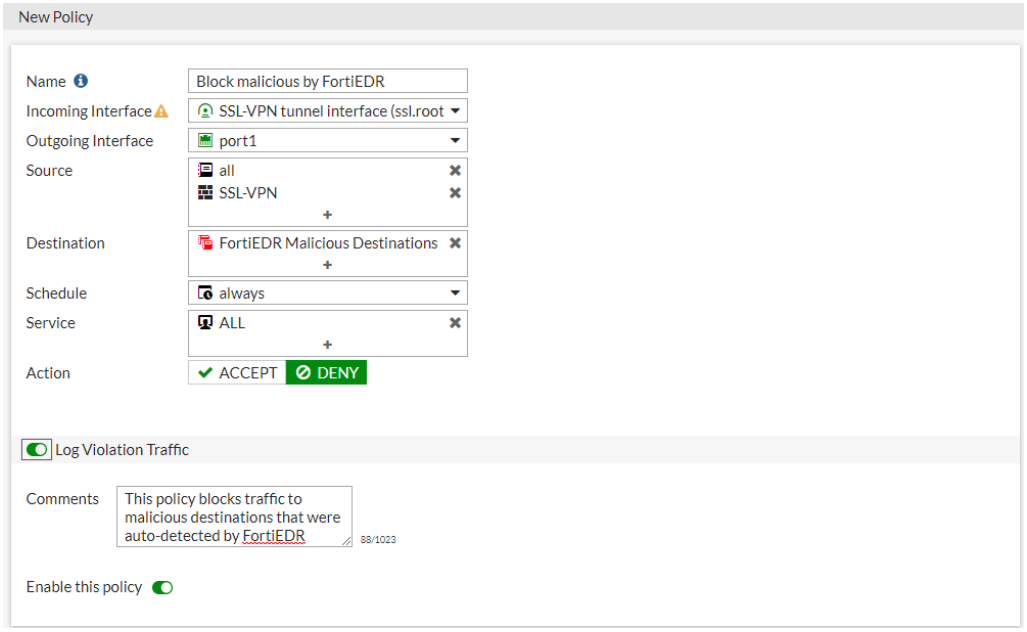
FortiGate Configuration

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.



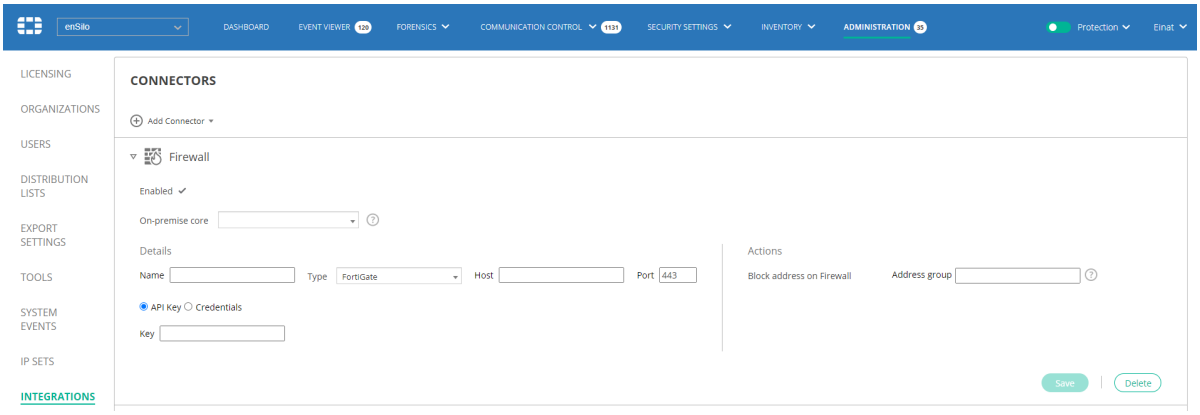
3. Go to **Policy & Objects ➔ IPv4 Policy**.
4. Create a new policy to deny traffic to any address in the address group that was created as part of step **2**. The new policy now appears in the FortiGate Policies table.



FortiEDR Connector Configuration

To set up FortiGate Connector with FortiEDR:

1. Click the Add Connector button and select **Firewall** in the **Connectors** dropdown list. The following displays:

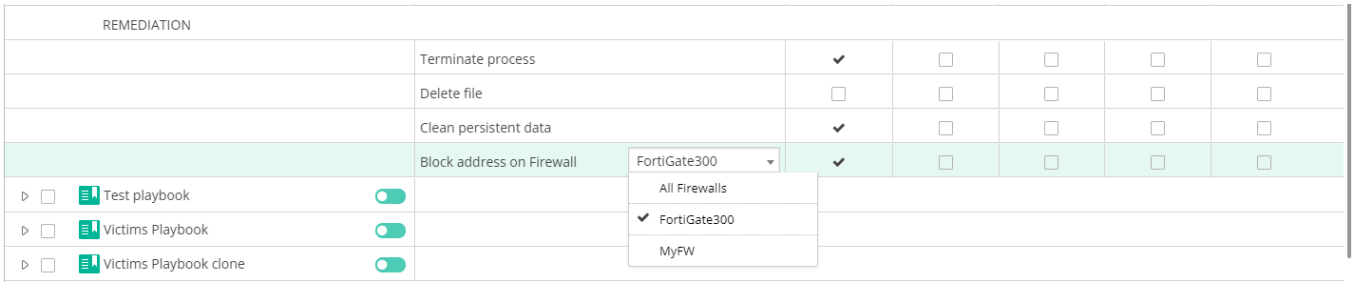


2. Fill in the following fields:
   - **Enabled:** Check this checkbox to enable blocking of malicious IP addresses by this firewall.
   - **On-premise Core:** Select the on-premise FortiEDR Core that will communicate with the firewall.
   - **Name:** Specify a name of your choice to be used to identify this firewall.
   - **Host:** Specify the IP or DNS address of your firewall.
   - **Port:** Specify the port that is used for API communication with your firewall.
   - **API Key/Credentials:** Specify authentication details of your firewall. To use an API token, click the **API Key** radio button and copy the token value into the text box. To use API credentials, click the **Credentials** radio button and enter the Firewall API username and password.
   - **Address Group:** Specify the name of the address group that was previously defined on the firewall.
3. Click **Save.**

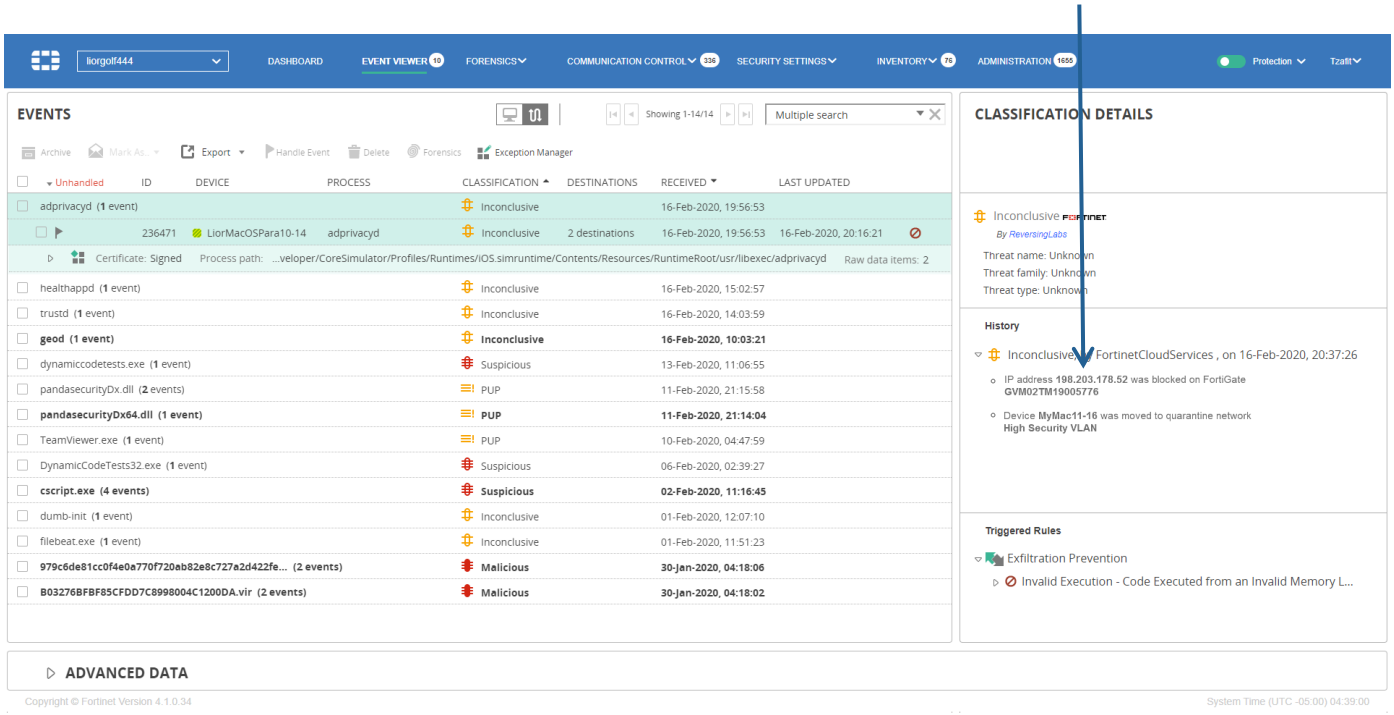
Playbooks Configuration

To configure an automated incident response that uses a firewall connector to block malicious destinations upon 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:



FortiEDR is now configured to add malicious IP addresses to the blocking policy on FortiGate 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. In addition, automatic incident response actions are listed in the CLASSIFICATION DETAILS area of the **Events** page of the FortiEDR Console, as shown below:



Sandbox Integration

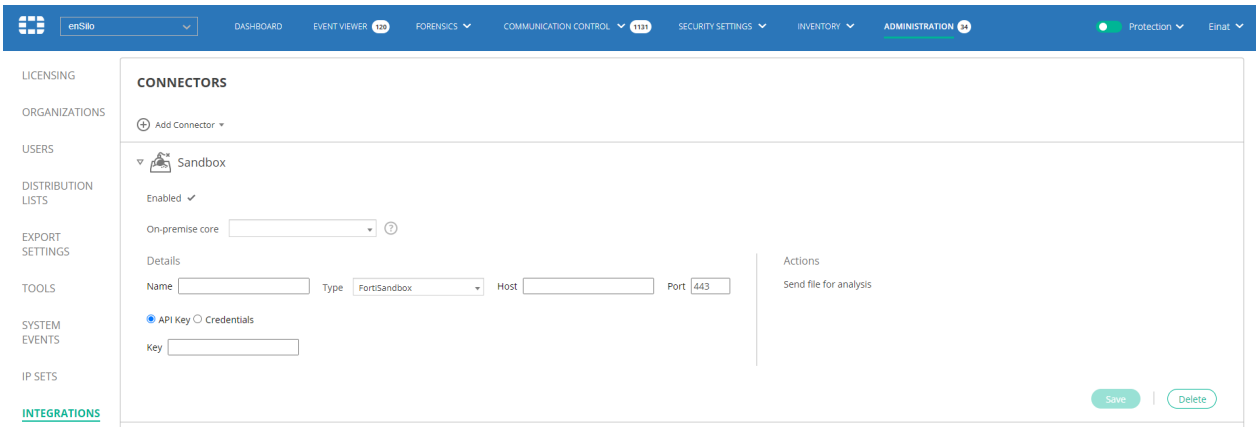
When FortiSandbox is configured and the Sandbox Analysis Policy rule is enabled, files that meet several conditions and that have not been previously analyzed trigger a sandbox analysis event on FortiEDR and are sent to FortiSandbox. The conditions are a combination of several items, such as the file 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 an on-premise Core that has connectivity to the sandbox.
  Details about how to install a FortiEDR on-premise Core are described in *Installing the FortiEDR Core*.
- The FortiEDR Central Manager has connectivity to Fortinet Cloud Services (FCS).
- You have a valid API user with access to FortiSandbox.

To set up FortiSandbox Connector with FortiEDR:

1. Click the Add Connector button and select **Sandbox** in the **Connectors** dropdown list. The following displays:

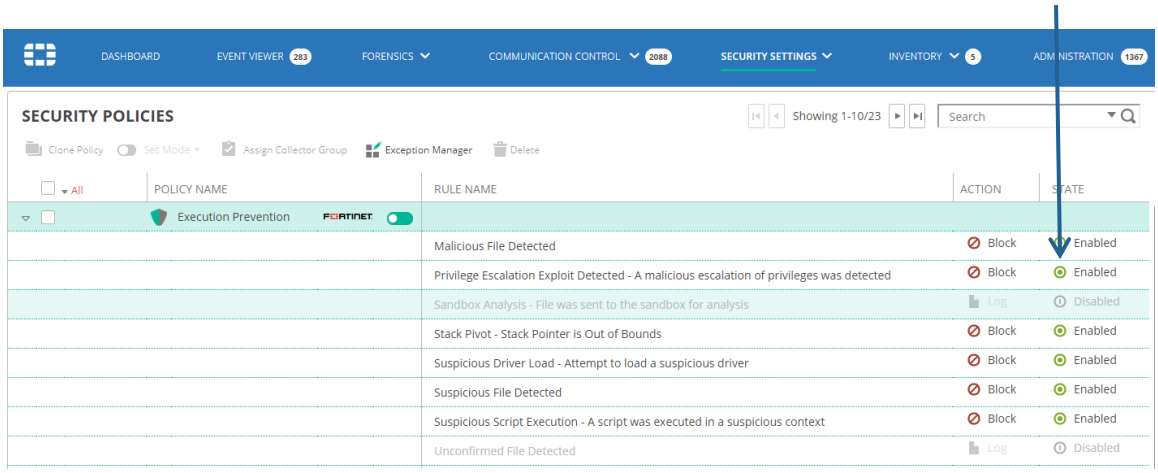


2. Fill in the following fields:
   - **Enabled:** Check this checkbox to enable file investigation with this sandbox.
   - **On-premise Core:** Select the on-premise FortiEDR Core that will communicate with the sandbox.
   - **Name:** Specify a name of your choice which will be used to identify this sandbox.
   - **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/Credentials:** Specify authentication details of your sandbox. To use an API token, click the **API Key** radio button and copy the token value into the text box. To use API credentials, click the **Credentials** radio button and fill in the sandbox 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:

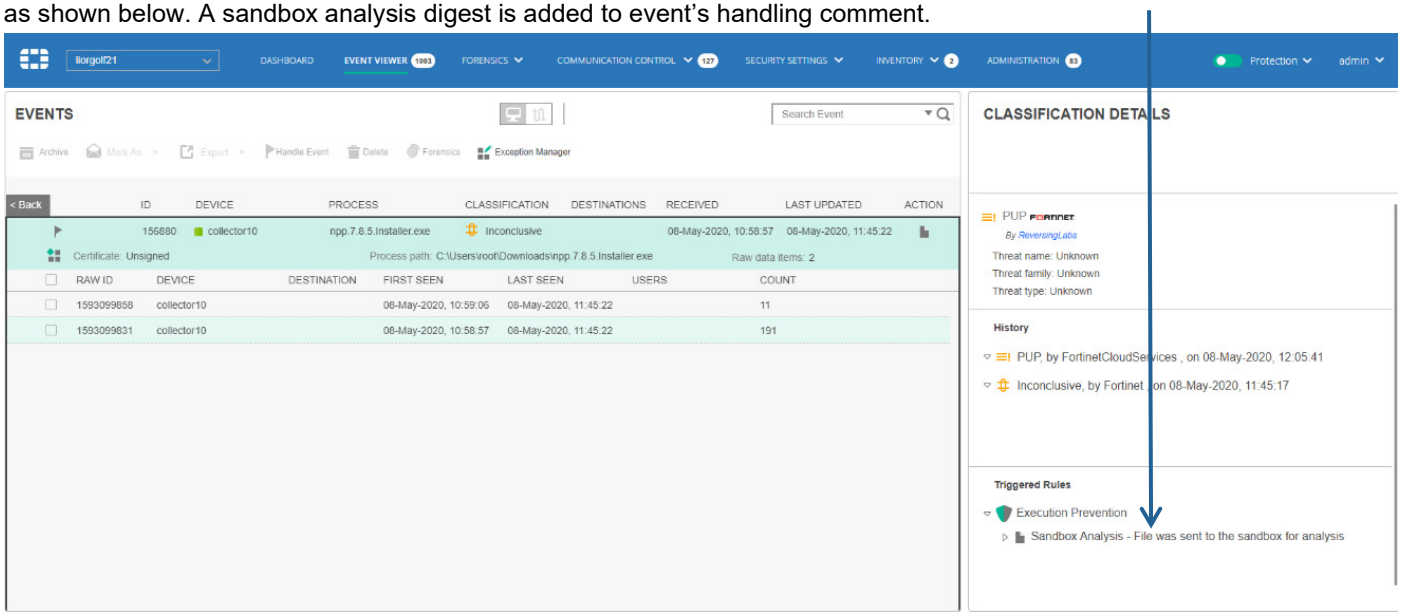
1. Navigate to the **SECURITY SETTINGS** ➔ **Security Policies** page.
2. Open the Execution Prevention policy that is applied on devices for which you want the sandbox scan to apply and click the **Disabled** button next to the Sandbox Analysis rule to enable it, as shown below:



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 event's handling comment.



Chapter 10 – TROUBLESHOOTING

This chapter describes how to troubleshoot various problems that you may encounter in the FortiEDR system.

Note – For debugging and troubleshooting, FortiEDR support may request that you provide the logs for the FortiEDR devices deployed in your organization (Collectors, Cores, Aggregators). You may refer to the *Exporting Logs* section on page 80 for details about how to do so.
Note – 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 the *Retrieving Memory* section on page 140.

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. Perform a connectivity test in order to validate connectivity between all of the FortiEDR components: **FortiEDR Collector ➔ FortiEDR Core ➔ FortiEDR Aggregator ➔ FortiEDR Central Manager** console.
   - Contact Fortinet support (at https://support.fortinet.com) to be provided with a connectivity test utility.
   - Place the provided ConnectivityTestApp.exe utility on the communicating device. This utility simulates a simple security event generated from the FortiEDR Collector.
   - Run it by double-clicking. This utility is available for both 32-bit and 64-bit operating systems. Upon activation of the utility, a security event should appear on the FortiEDR Central Manager.
3. 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:

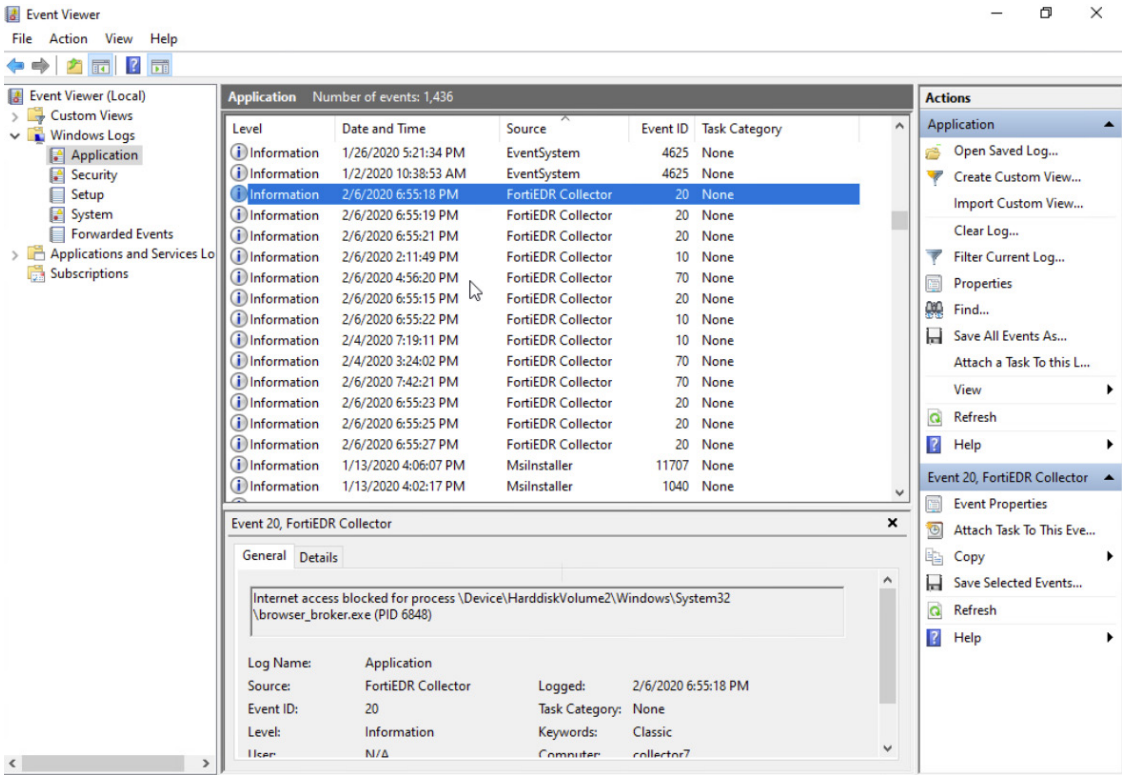
- Running Telnet on the FortiEDR Collector and connecting to the FortiEDR Core IP via port 555,
- Running Telnet on the FortiEDR Core and attempting to connect to the FortiEDR Aggregator IP on port 8081.

  Note – Make sure that Telnet is enabled in 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 MacOS console records whenever a FortiEDR Collector blocks communication from a device or file modification related to ransomware activity. This information is recorded in the MacOS console log located in the following location: Applications ➔ **Utilities ➔ Console ➔ All Messages**, as shown below:

```
Feb 26 20:06:50 Mac70 fortiEDRCollector[3654]: Fortinet Endpoint Detection and Response: Connection blocked for process /System/Library/PrivateFrameworks/
IMFoundation.framework/XPCServices/IMRemoteURLConnectionAgent.xpc/Contents/MacOS/IMRemoteURLConnectionAgent (pid:3813)
Feb 26 20:06:51 --- last message repeated 2 times ---
Feb 26 20:06:51 Mac70 fortiEDRCollector[3654]: Fortinet Endpoint Detection and Response: Connection blocked for process /System/Library/PrivateFrameworks/
IMFoundation.framework/XPCServices/IMRemoteURLConnectionAgent.xpc/Contents/MacOS/IMRemoteURLConnectionAgent (pid:3814)
```

Chapter 11 – 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 (see below), there is no need to read this chapter.

What is a Multi-organization Environment in FortiEDR?

Beginning with V3.0, 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.

Note – Prior to V3.0, 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:

- **Administrator:** Is the highest-level super user that can perform all operations in the FortiEDR Central Manager console for **all organizations**. This role can access all organizations in the system, and also includes the same privileges as the Local Administrator and User roles.

  In a FortiEDR multi-organization system, the system comes with one predefined Administrator user. More than one Administrator role is permitted.

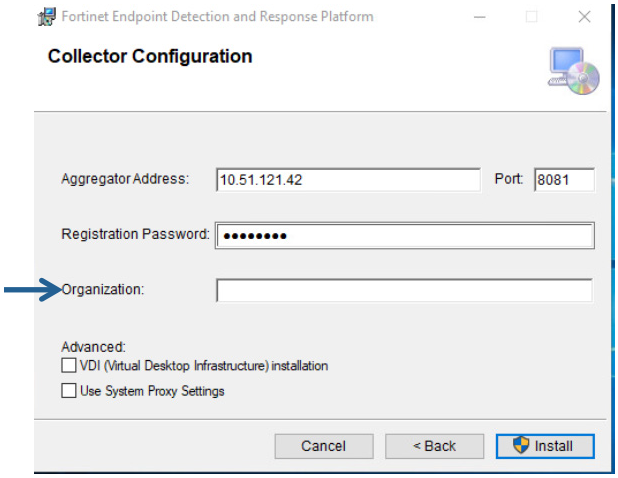
  Note – There must always be at least one Administrator in the system.

  - **Local Administrator:** Is a super user that can perform all operations in the FortiEDR Central Manager console for a **single organization**. This role can only access its own organization's data, and also includes the same privileges as the User role. More than one Local Administrator role is permitted per organization.
  - **User:** This user is allowed to view all information and to perform actions for its **own organization**, such as to mark events as handled, change policies and define Exceptions. This user is similar to the Local Administrator. However, this user cannot access the **ADMINISTRATION** tab, which is described in *Chapter 9*, *Administration* on page 147.

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:



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 the *Installing FortiEDR Collectors* section on page 38.

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 the *Installing the FortiEDR Core* section on page 33.

Workflow

The following general workflow applies for Administrators when working in a FortiEDR multi-organization system:

1. Logging In to a Multi-organization System Page 185
2. Defining or Importing an Organization Page 186
3. Navigating Between Organizations Page 190
4. Defining a Local Administrator for an Organization Page 190
5. Performing Operations in the FortiEDR System Page 191

Step 1 – Logging In to a Multi-organization System

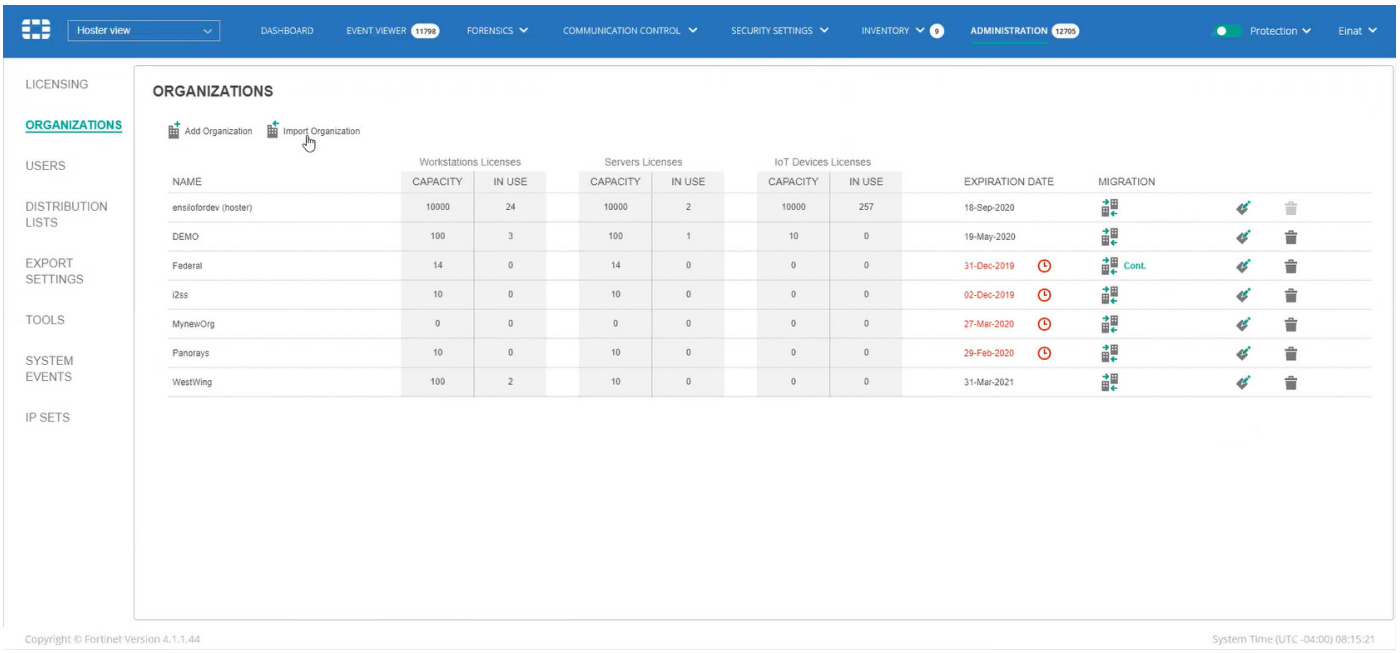
For a FortiEDR multi-organization system, a user must also specify the organization when logging in to the system.

By default, Administrators are logged in to the main organization, and do not need to specify an organization in the **Organization Name** dropdown list.

A Local Administrator or regular User must specify the organization when logging in. The user must be defined for an organization in order to log in to that organization.

Step 2 – Defining or Importing an Organization

The **ORGANIZATIONS** page lists all the organizations defined in the FortiEDR system.



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 (hoster) organization can be accessed by an Administrator and the Local Administrator that you define for it.

Note – In a single-organization system, the Default (hoster) organization is the only organization. To set up a multi-organization system, see page 189.

The Organizations window contains the following information:

- **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).
- **Workstation Licenses Remaining:** Specifies the number of workstation licenses remaining.
- **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).
- **Servers Licenses Remaining:** Specifies the number of server licenses remaining.
- **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.

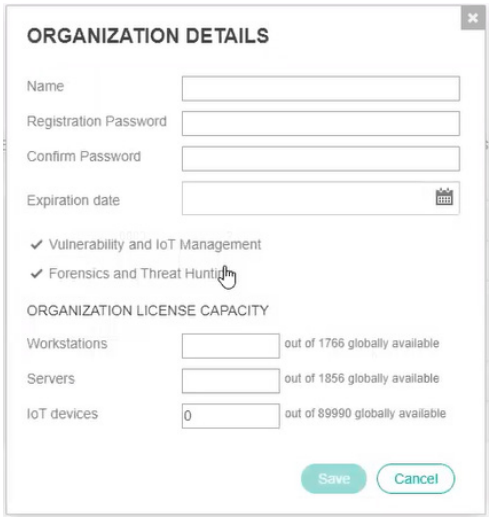
Click the Edit button in an organization row to edit the properties of that organization.

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 page 191.

To define an organization:

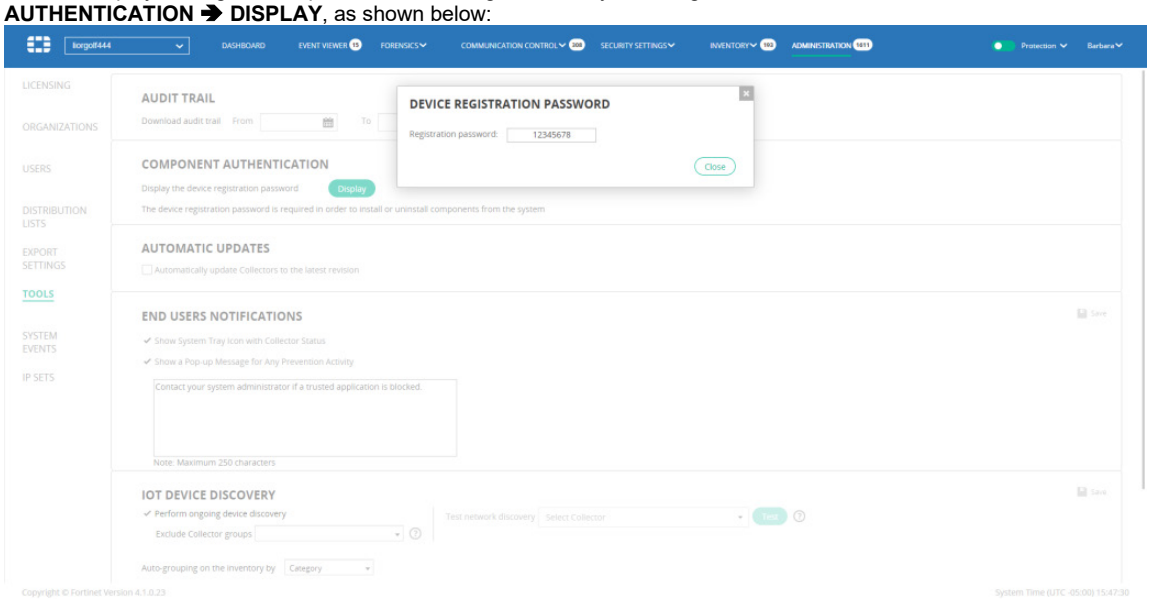
1. Click the **ADMINISTRATION** tab and then click **ORGANIZATIONS** in the left pane. The **ORGANIZATIONS** page displays.
2. Click the Add Organization button. The following window displays:



All fields in this window are mandatory.

3. Fill in all fields in this window, as follows:
   - **Name:** A free-text field that specifies the name of the organization. For example, a hotel branch location like ABC Hotel Los Angeles.
   - **Registration Password:** Specifies the registration password for the organization. Each organization can have a different registration password. You set the value for this password.

You can display the registration password for an organization by selecting **ADMINISTRATION ➔ TOOLS ➔ COMPONENT AUTHENTICATION ➔ DISPLAY**, as shown below:



Note – 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 the Component Authentication section on page 164.

- **Expiration date:** Specifies when this license expires. Notifications are sent to you beforehand. Each organization can have its own expiration date.

  Note – If the Default (hoster) organization expiration date is earlier than that for the organization, then the expiration date for the Default (hoster)organization applies. Whenever there is an expiration date conflict, the earlier date always applies.

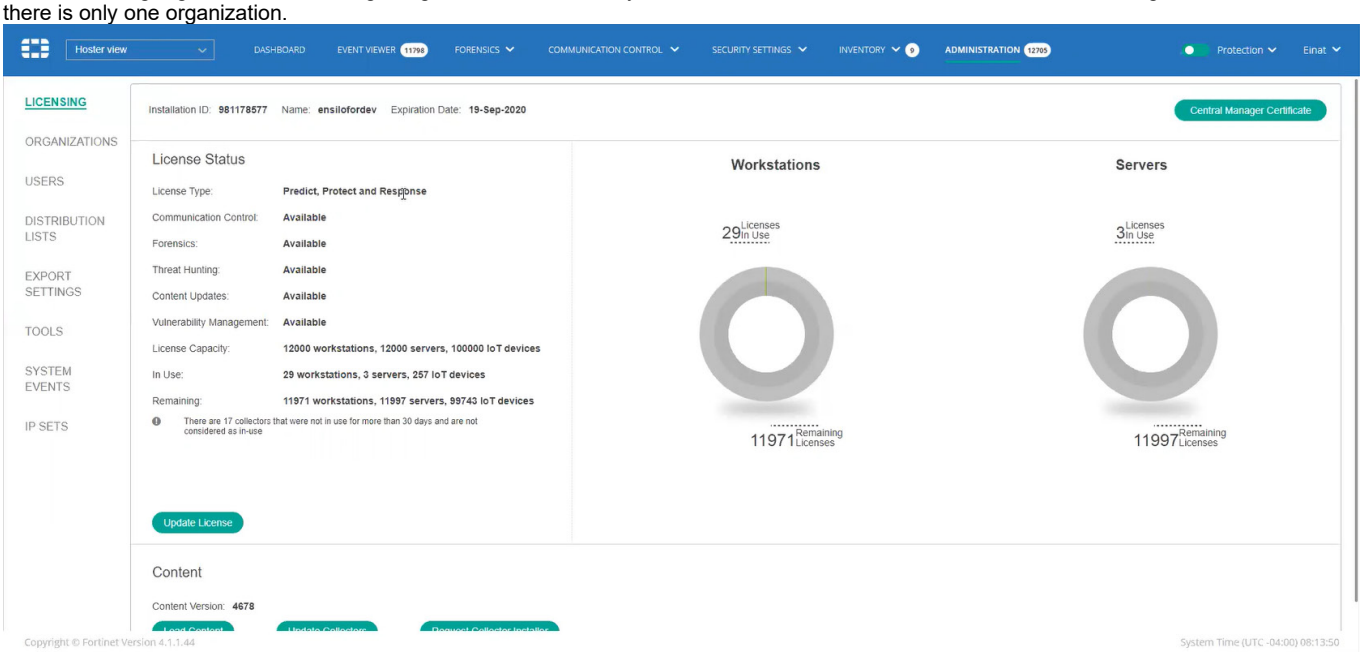
- **Vulnerability and IoT Management:** Check this checkbox for the organization to have access to these features. This option is only available on setups that have purchased a **Predict and Protect** license or **Predict, Protect and Response** license. See more details on license types on page 31.

  Note – 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.

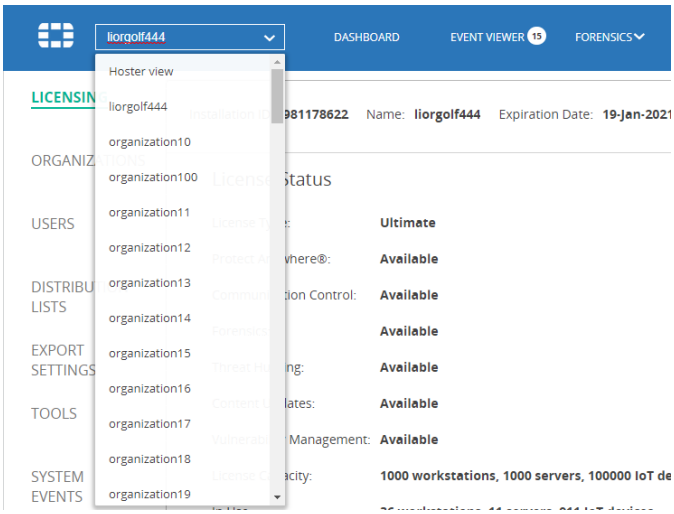
- **Forensics and Threat Hunting:** Check this checkbox for the organization to have access to these features. This option is only available on setups that have purchased a **Predict, Protect and Response** or **Protect and Response** license.
- **Workstations /Servers /IoT Devices License Capacity:** 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.

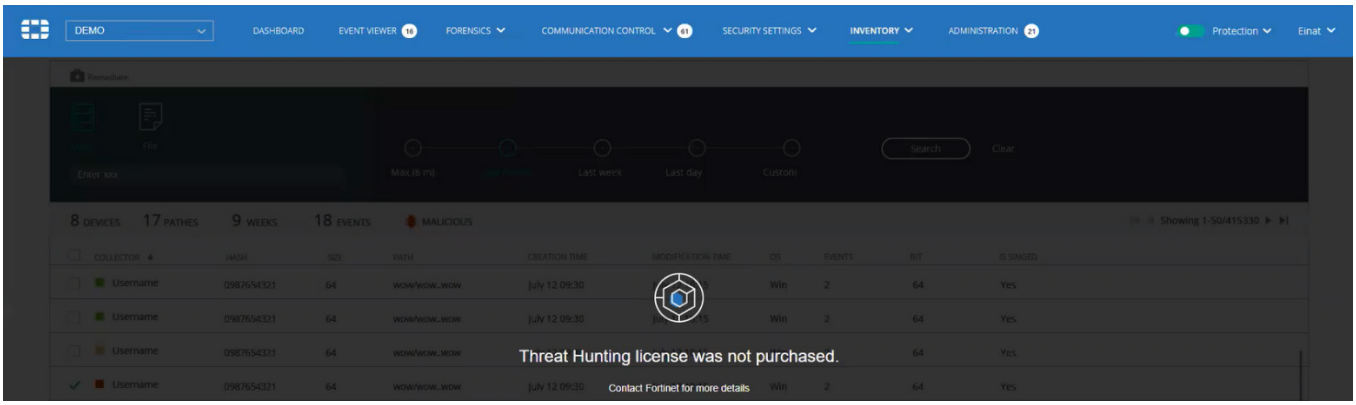
  Note – The **License Capacity** field in the Licenses window shows the total number of license seats for the entire FortiEDR system, which are divided into Workstations, Servers and IoT Devices.
  The Default (hoster) organization initially receives the total allocation of licenses. The Administrator 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.



4. Click the **Save** button. Note that it may take a minute or so to create the organization.
   After creating the organization, the organization appears as a new row in the **Organization** dropdown list.



Note – 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.

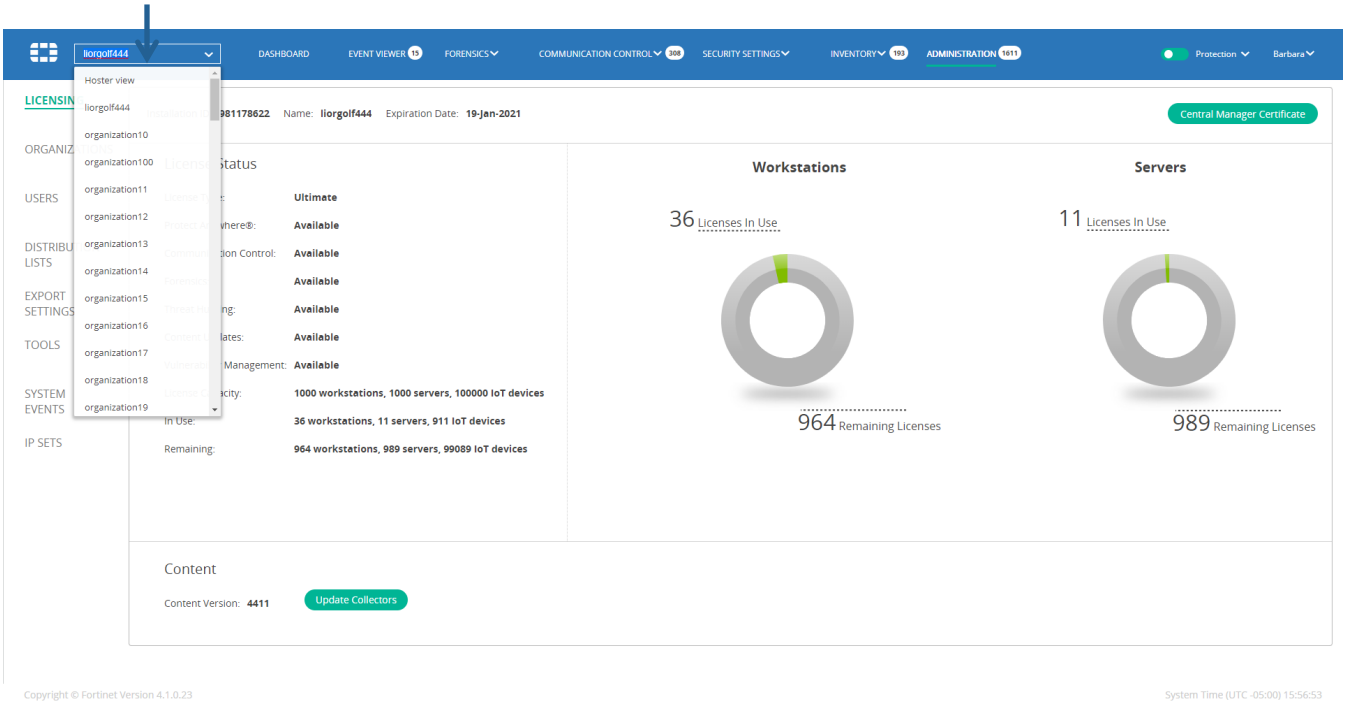
To create a multi-organization (multi-tenant) system, an Administrator simply needs to add one or more organizations to a single-organization system. When there are multiple organizations in the system, you can select the organization of interest in the **Organization** dropdown menu that appears at 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 page 197.
- Select the organization of interest in the **Organization** dropdown list.



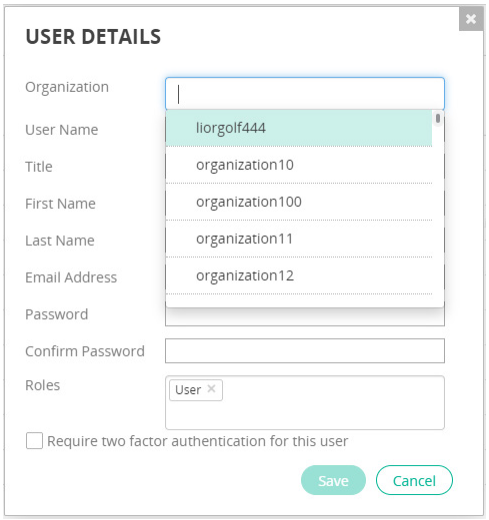
In Hoster view, each row in the Organizations pane represents a different organization. Note that after you select an organization, the entire user interface only shows information for that organization.

Step 4 – Defining a Local Administrator for an Organization

Administrators can create one or more Local Administrators for an organization. You should define at least one Local Administrator for each organization.

To define a Local Administrator:

1. Click the **ADMINISTRATION** tab and then click **USERS** in the left pane.
2. Click the Add User button.
3. Fill in the displayed window, as described on page 152, and then click **Save**. Be sure to select **Local** Administrator in the Roles field.
   In addition, you must specify the organization for the Local Administrator in the **Organization** field, as shown below.



Step 5 – Performing Operations in the FortiEDR System

Administrators can perform all of the operations described in Chapters 3 through 8 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

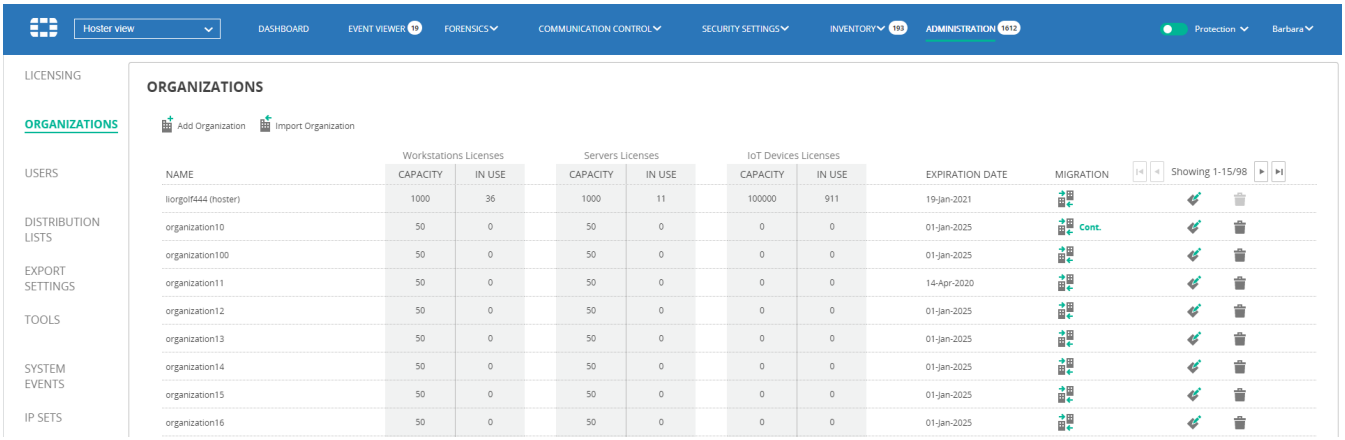
FortiEDR's Consolidation feature enables you to copy all the data and definitions within an organization from one environment to another environment. This feature copies an organization from one environment (source setup/environment) to another (destination setup/environment). The copy operation adds to the content in the destination environment, and does not replace the target's existing content.

Note that this feature is only available to Administrators.

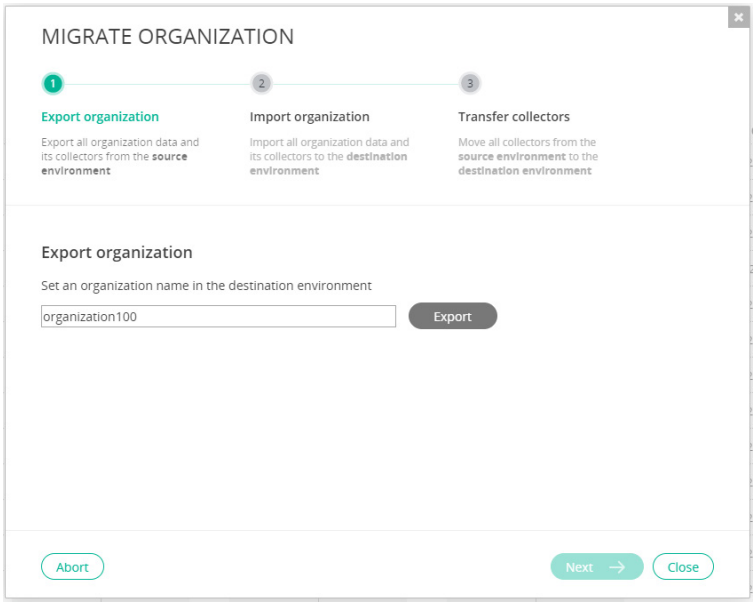
Organization migration involves three steps, which are described in detail in the procedure below.

To migrate an organization:

1. Click the **ADMINISTRATION** tab and then click **ORGANIZATIONS** in the left pane. The Organizations window displays.



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:



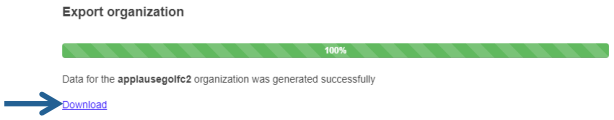
From this window, you perform three steps to migrate the organization to another environment:

- **Step 1, Export the Organization:** This step exports all the data of the selected organization to a zip file.
- **Step 2, Import the Organization:** 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.
- **Step 3, Transfer the Collectors:** This step moves all the Collectors of the selected organization from the source environment to the destination environment.

3. In the **Export organization** field, specify the name of the organization to appear for this data in the destination environment. Make sure that you assign an organization name that does not already exist in the destination environment.

4. Click the **Export** button. All the data and definitions for the organization are exported to a zip file. The zip file is named as follows: **source organization name_environment name_FortiEDR_timestamp_Export.zip**, as shown in the example below:
   ad_localhost.localdomain_enSilo_Feb.05.2019_Export.zip

   After the export completes, a **Download** link displays in the window:

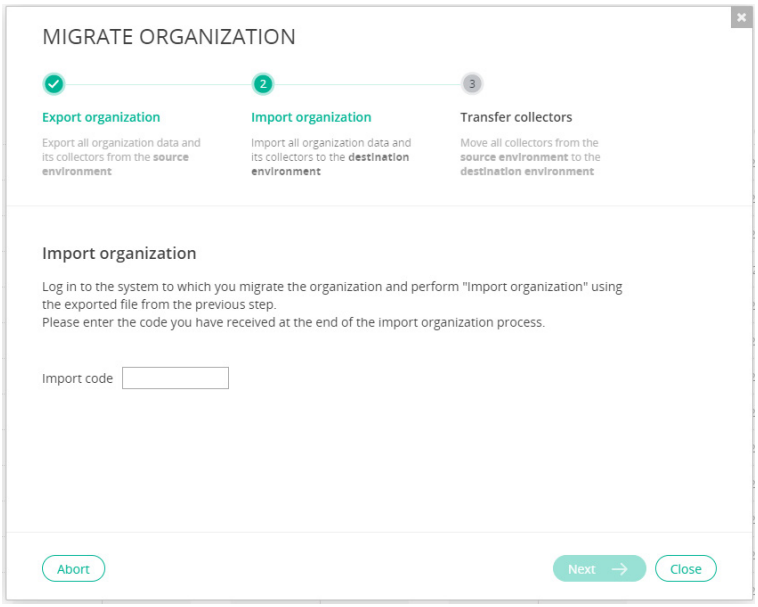


   Note – You can cancel the migration process at any time by clicking the **Abort** button.

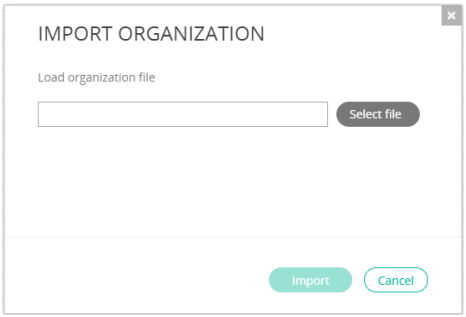
5. Click the **Download** link to download the exported zip file.

   Note – 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:



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:

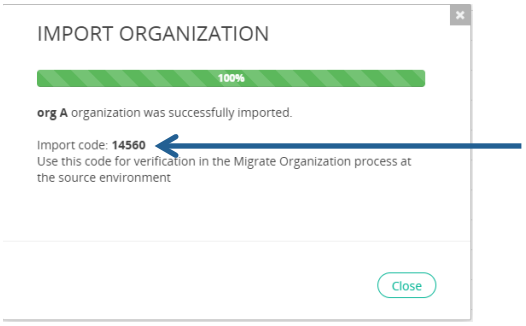


10. Select the exported zip file to load and then click **Import**. This step copies all the data and environment definitions of the exported organization.

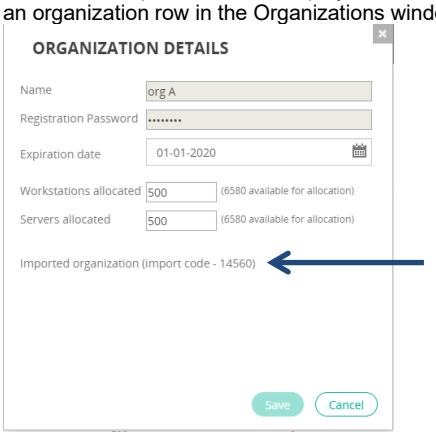
    Notes – You cannot import an exported organization that has a name that already exists in the destination environment.
    To import:
    The FortiEDR platform version must be the same in both the source and destination environments.

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 window (see page 147).
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.



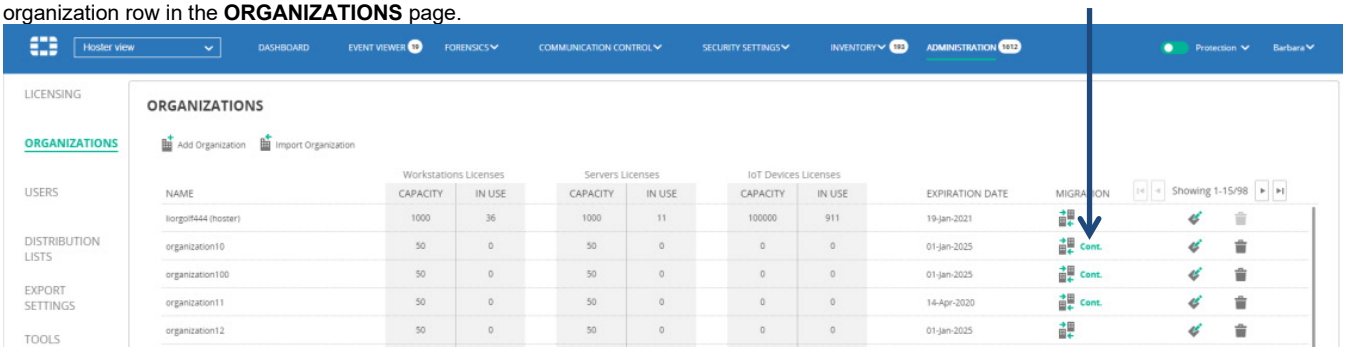
Note – The Import code also displays in the Organization Details window, which you can display at any time by clicking the **Edit** button in an organization row in the Organizations window.



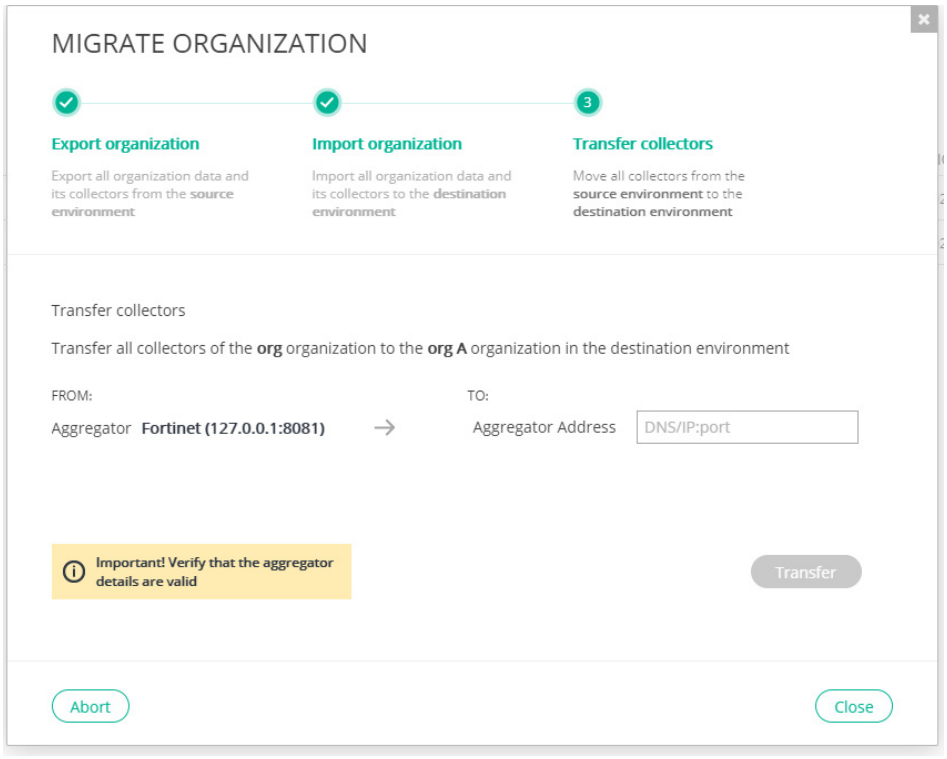
Note that the name of the organization cannot be changed in this window, and is read only.

11. In step 2 of the Migrate Organization window, enter or copy the import code into the **Import code** field.

Note – If you previously closed the Migrate Organization window, then click the **Continue Migration** Cont. button in the source organization row in the **ORGANIZATIONS** page.

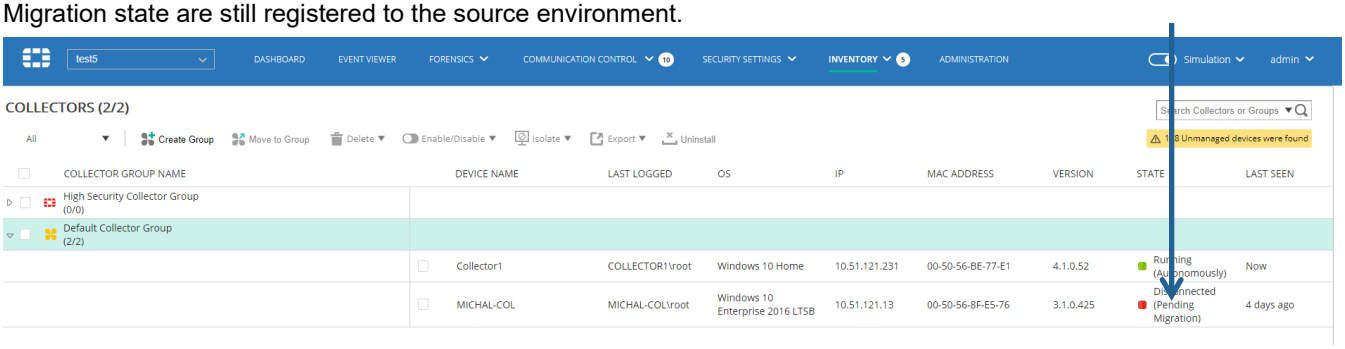


12. Click **Next**. The following window displays:

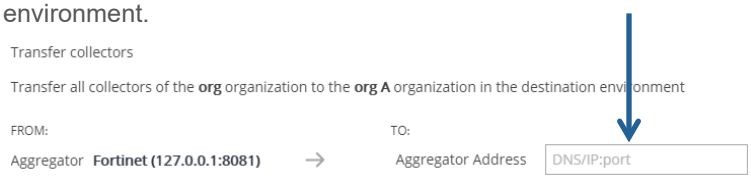


In this window, you move the Collectors from the source environment to the destination environment. The Collectors cannot be registered to both environments at the same time.

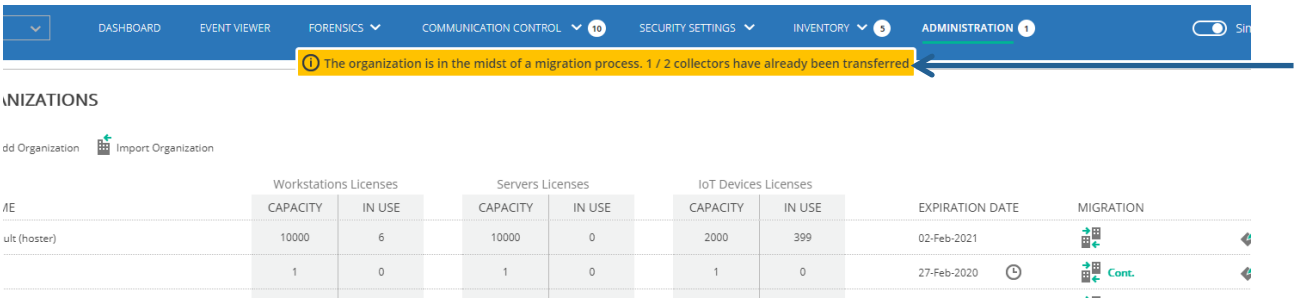
Note that until this step is completed, the Collectors are still registered to the organization in the source environment and their status and events are displayed there. In the destination environment, Collectors are displayed with the **Pending Migration** state, as shown in the Inventory window. This 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.



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.



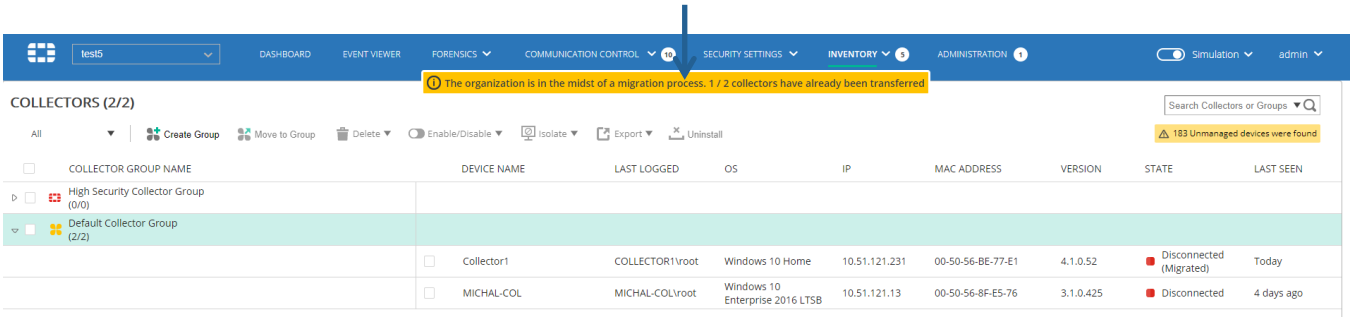
14. Click the **Transfer** button. The Collectors are transferred from the organization in the source environment to the organization in the destination environment. A progress indicator counter displays as the Collectors are transferred.



Note – 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.

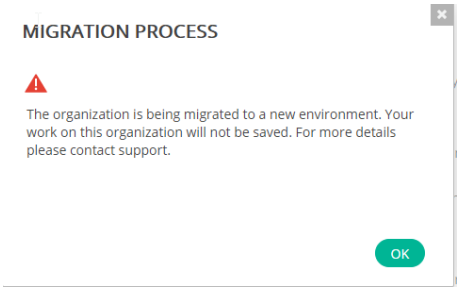
After a Collector has been transferred from the source environment to the destination environment, its state is **Migrated** in the source environment, and is **Running** (functional) in the destination environment.

Note – 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.

    IMPORTANT – 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.



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.

    Note – Collector protection and functionality remain throughout the entire migration process.

Hoster View

When you select **Hoster view** in the **Organization** dropdown list, all windows in the user interface are affected. In general, this view shows aggregated data for all organizations.

However, some data is only available in Hoster view, such as the following:

- **Export Settings:** In a multi-organization system, SMTP-related information is only displayed in Hoster view.
- Tools – Periodic Scan

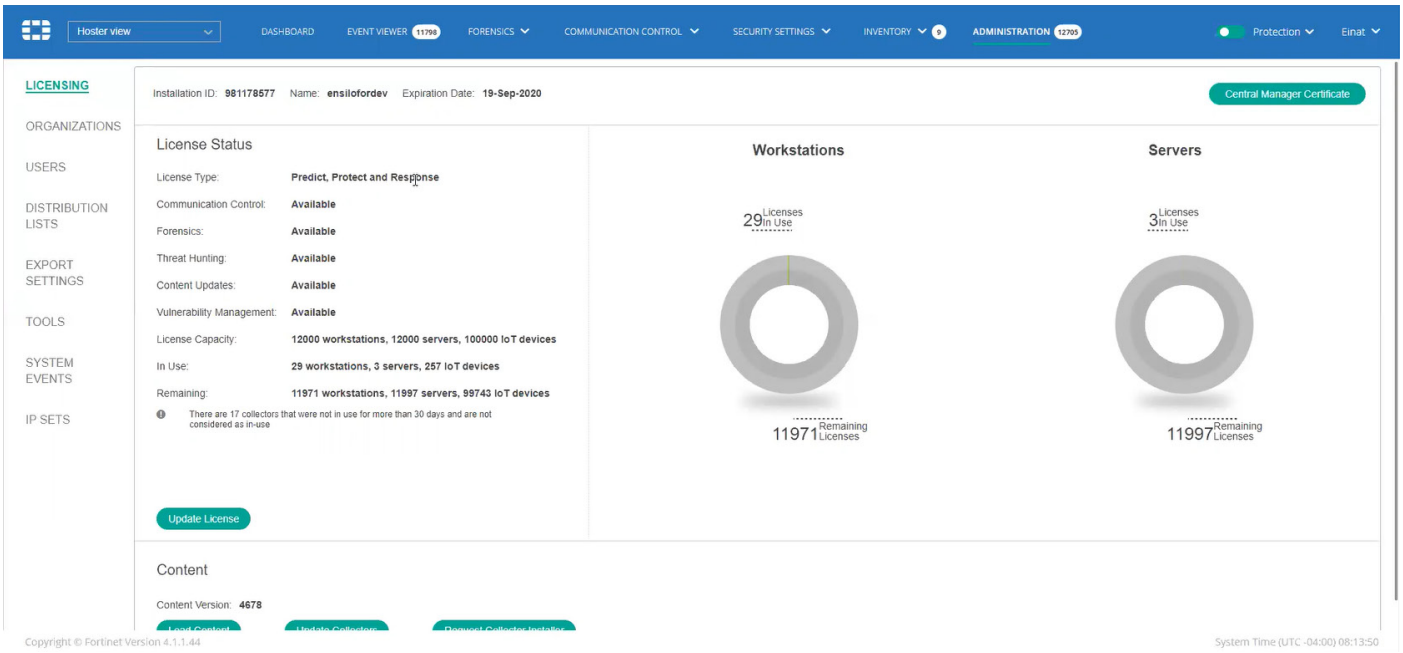
In addition, there are some special cases where you cannot view administration data in Hoster view, and can only view data for a specific organization, such as the following:

- Component Authentication
- Automatic Updates
- End User Notifications

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.

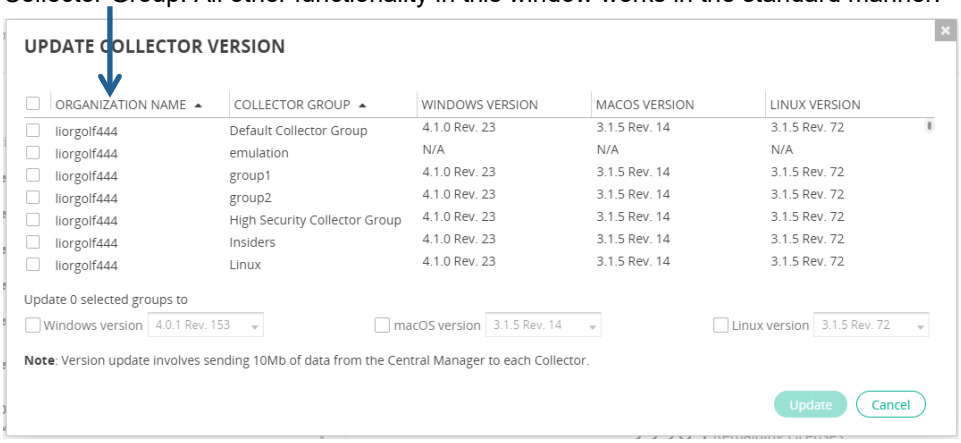


For example, the Workstations and Servers diagrams indicate the number of allocated and available licenses for all workstations and servers, respectively, in the entire FortiEDR system. The Licenses in Use numbers represent the number of Collectors that have been installed out of the total permitted 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. In order to select Collectors to update, see page 198.

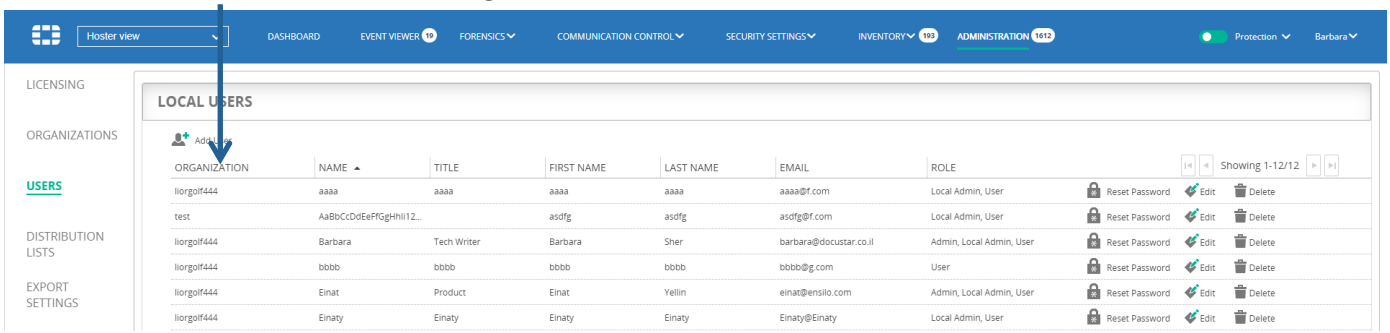
When in this view, you cannot load content to a specific organization.

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.

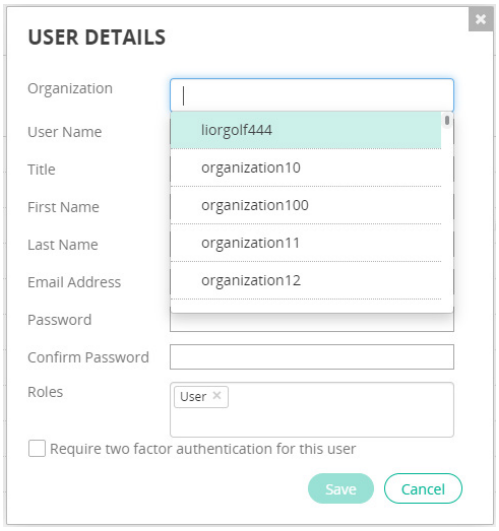


Users

In Hoster view, this window includes an **Organization** column.

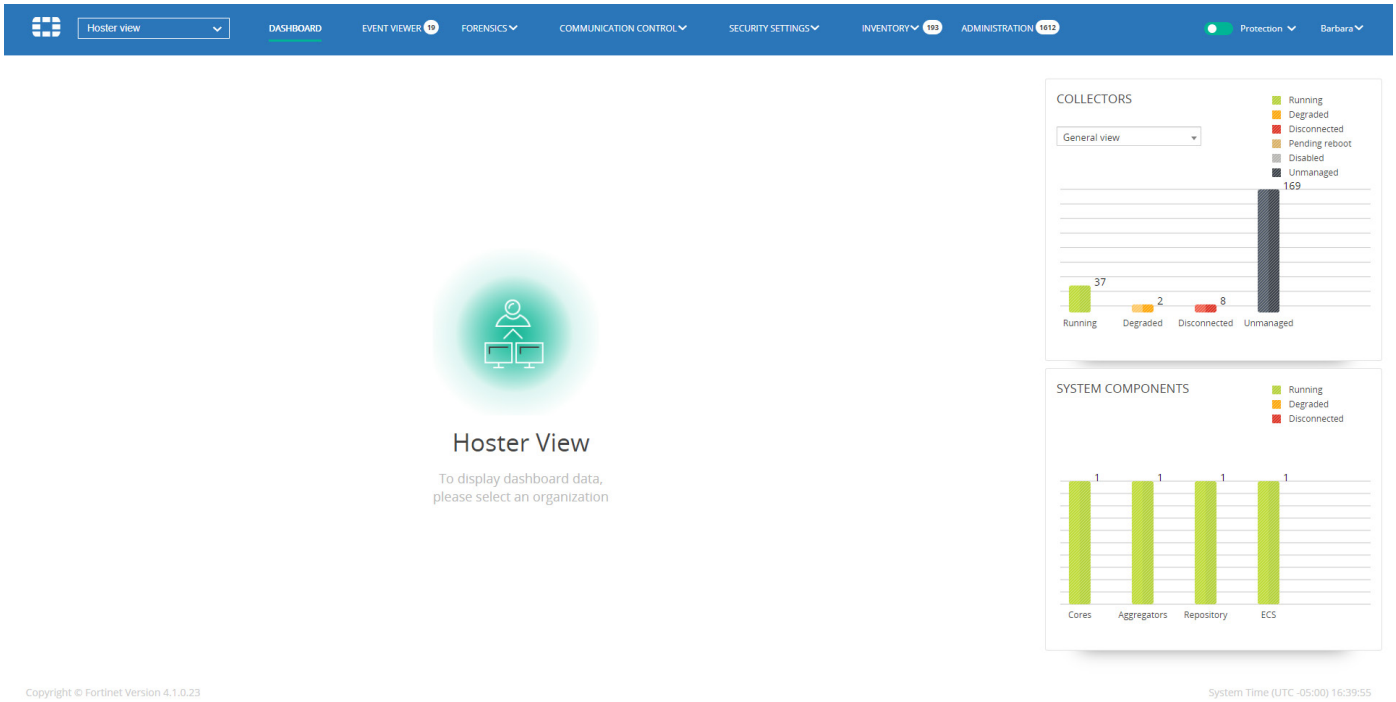


When you click the Add User button from this window, the User Details window displays. The User Details window includes an Organization field that you must specify to add the user.



Dashboard

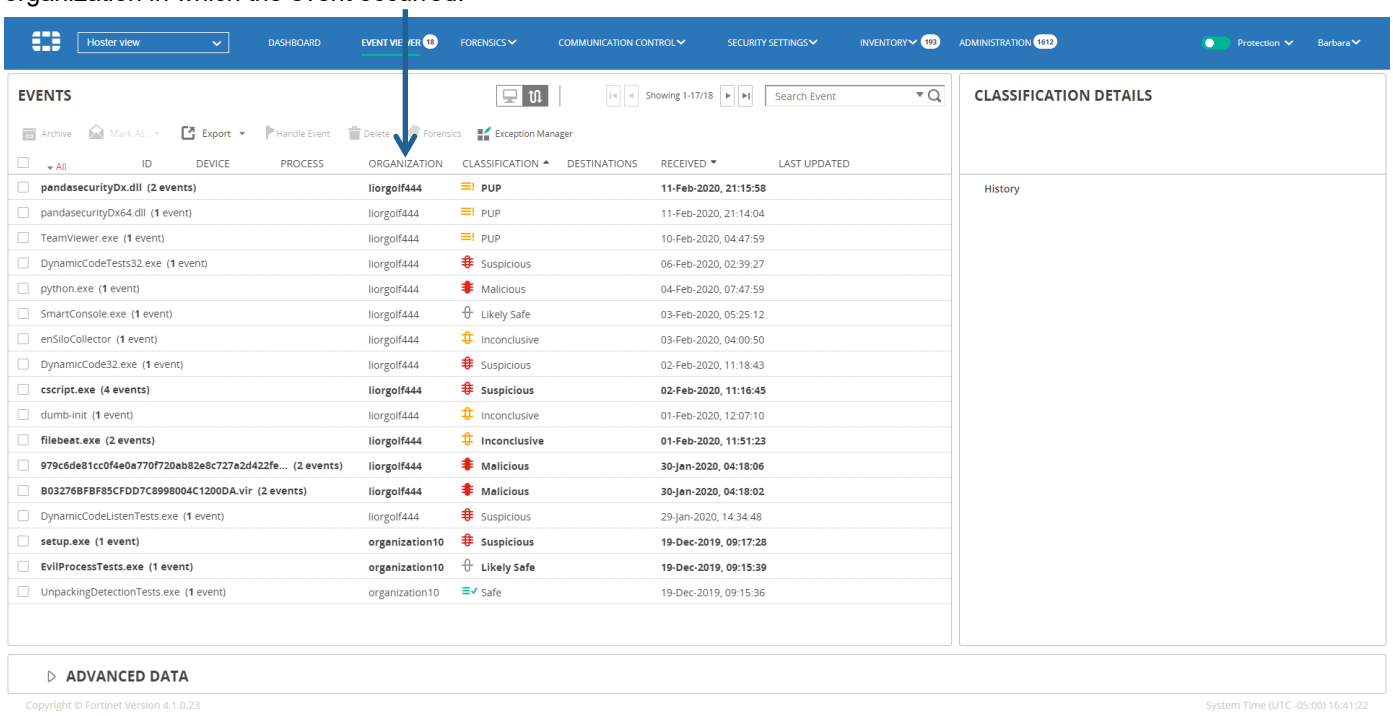
In Hoster view, some information does not display in the Dashboard. The information that does display is aggregated for all organizations, such as Collectors, System Components, Repositories and so on, as shown below.



To view Dashboard information for a specific organization, you must select the organization of interest in the Organization dropdown list.

Event Viewer

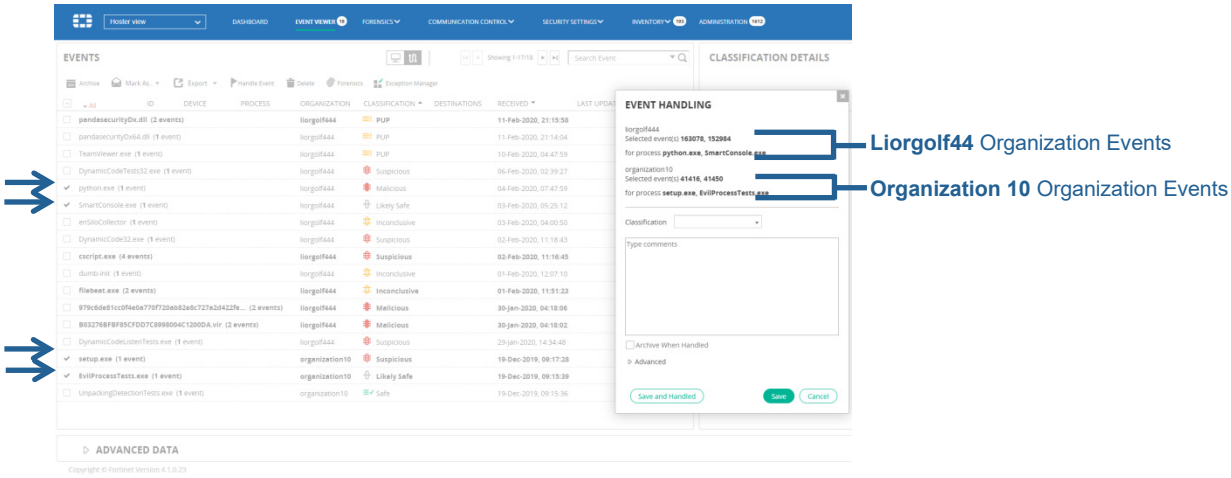
In Hoster view, the Event Viewer displays the events from all organizations. The **Organization** column indicates the organization in which the event occurred.



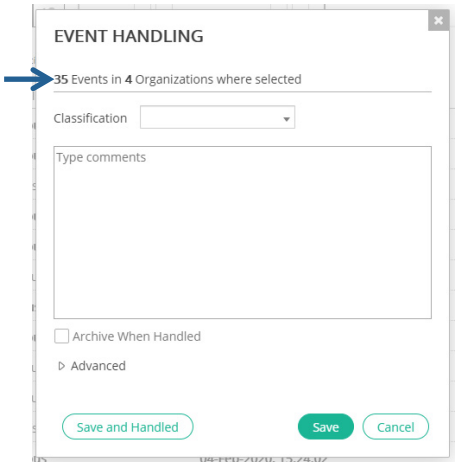
Note – The same event can occur in multiple organizations. In this case, it is displayed in separate rows per organization.

The various options in the toolbar can be applied on multiple organizations simultaneously. For example, you can archive events from different organizations at once using the **Archive** button and you can export events from different organizations using the **Export** button.

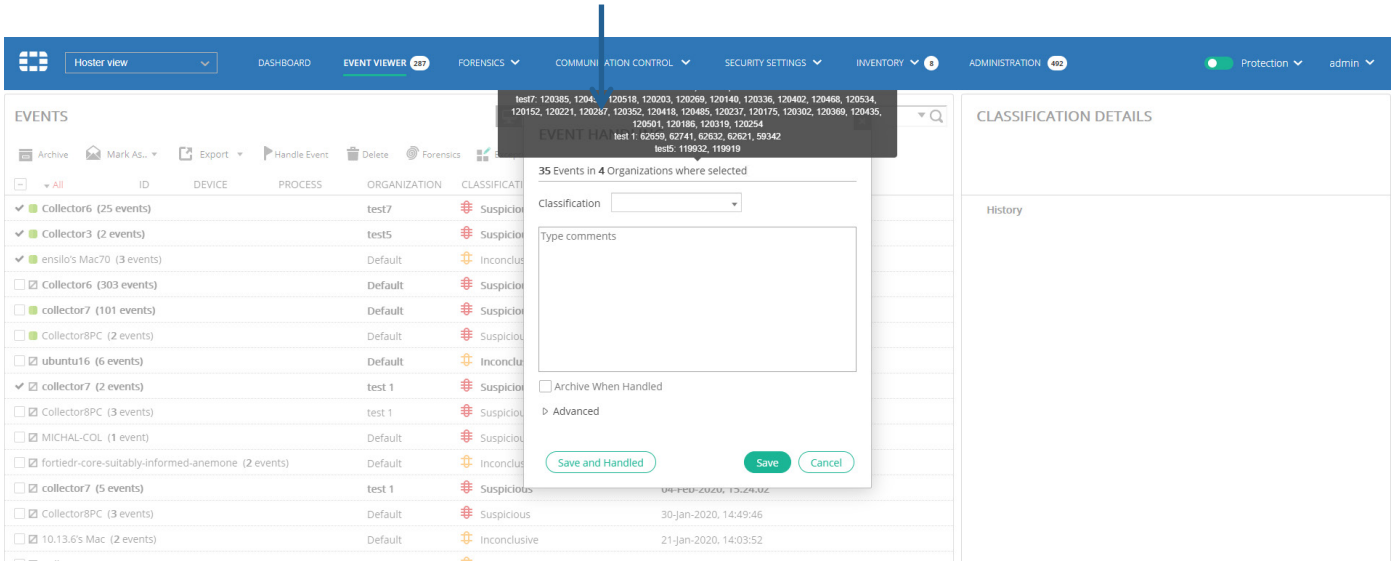
You can also use the **Handle Event** button to handle events from multiple organizations. In Hoster view, for each event selected in the Events window, the Event Handling window shows the organization name and events selected for that organization (when you select events in up to three organizations).



If you select events from more than three organizations, the Event Handling window displays the number of organizations and events you selected in a summary line at the top of the window.

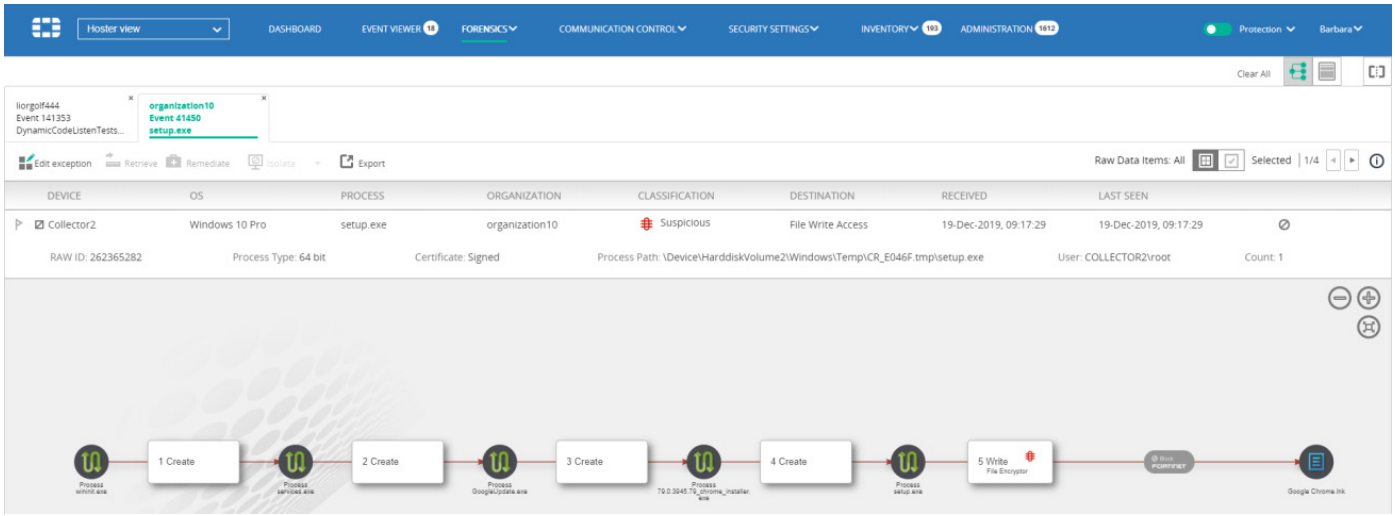


In this case, when you hover over the summary line, the details of the selected events display in a gray box. This box shows the name of the organization and its associated event IDs.



Forensics

You can select events from multiple organizations in the Event Viewer and then click the Forensics button in the Event Viewer to display these events in the Forensics window. Each event tab in the Forensics window shows the name of the organization in which the event occurred above the event ID.

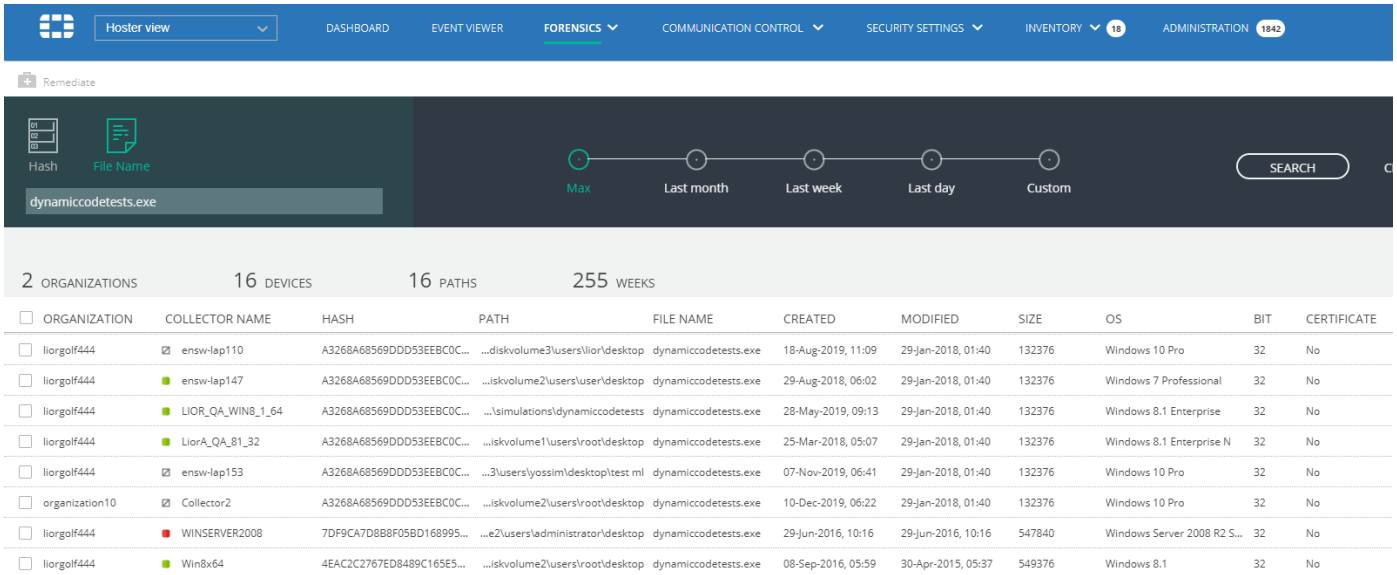


Communication Control

The Communication Control window is not available in Hoster view.

Threat Hunting

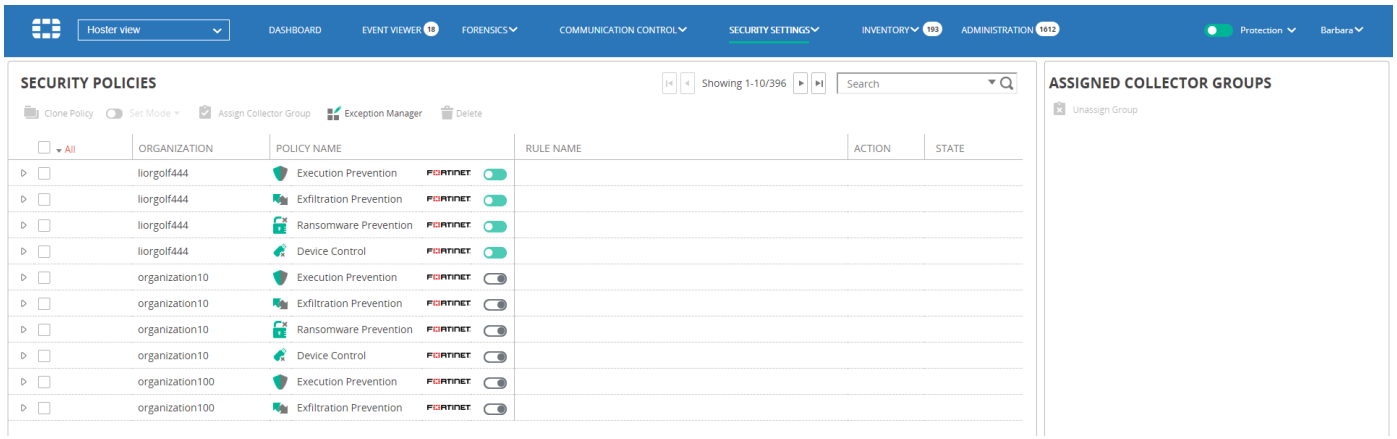
In Hoster view, this window includes an **Organization** column. In addition, you can hover over an entry in the **Product** column to display version information for the item.



Security Settings

SECURITY POLICIES Page

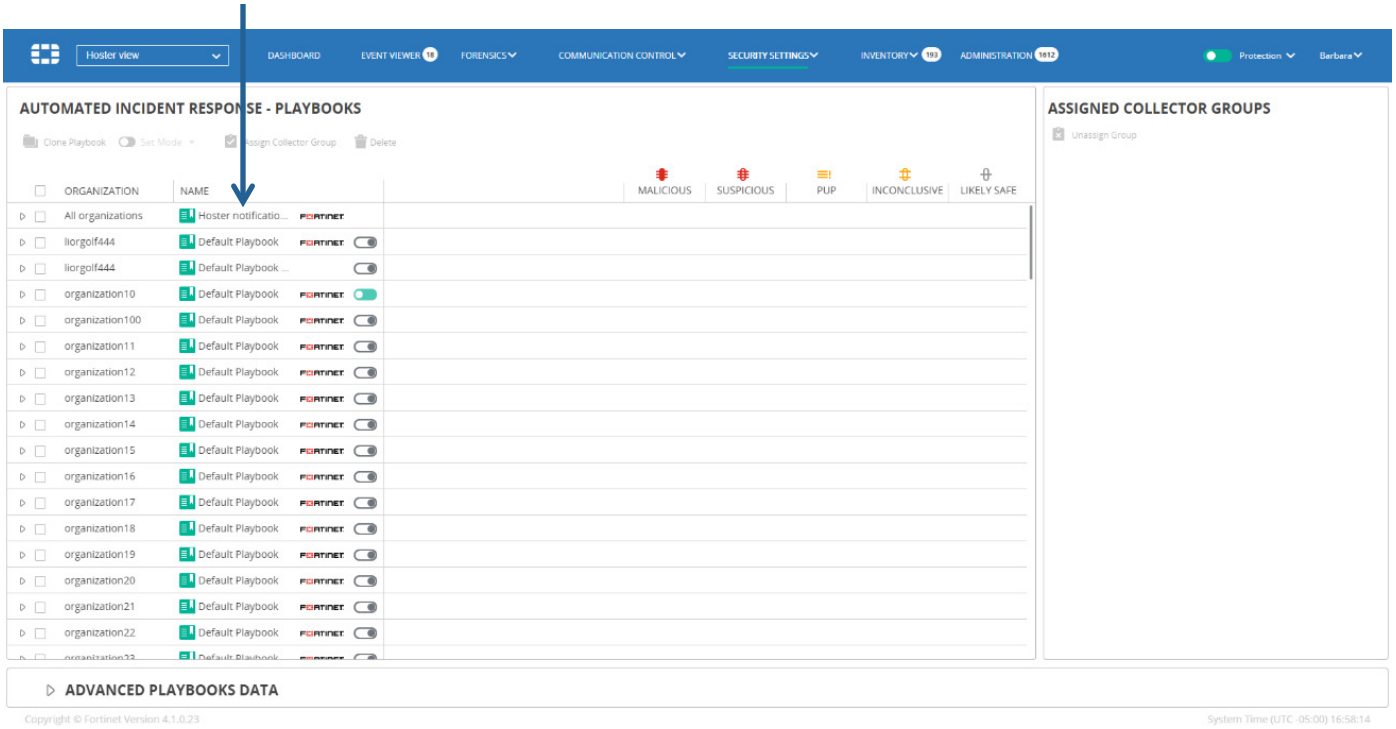
In Hoster view, the SECURITY POLICIES page displays all policies from all organizations.



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

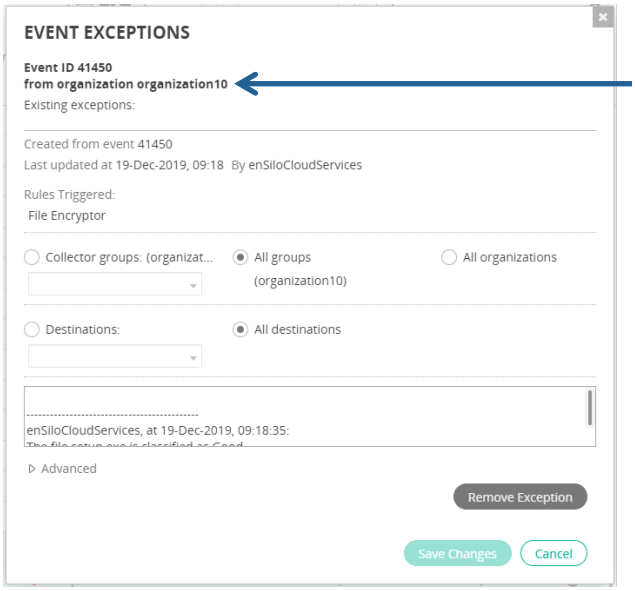
In Hoster view, you can view all the notifications for the entire organization, based on the actions defined in the Hoster Notifications Playbook. This Playbook policy is only available in Hoster view.



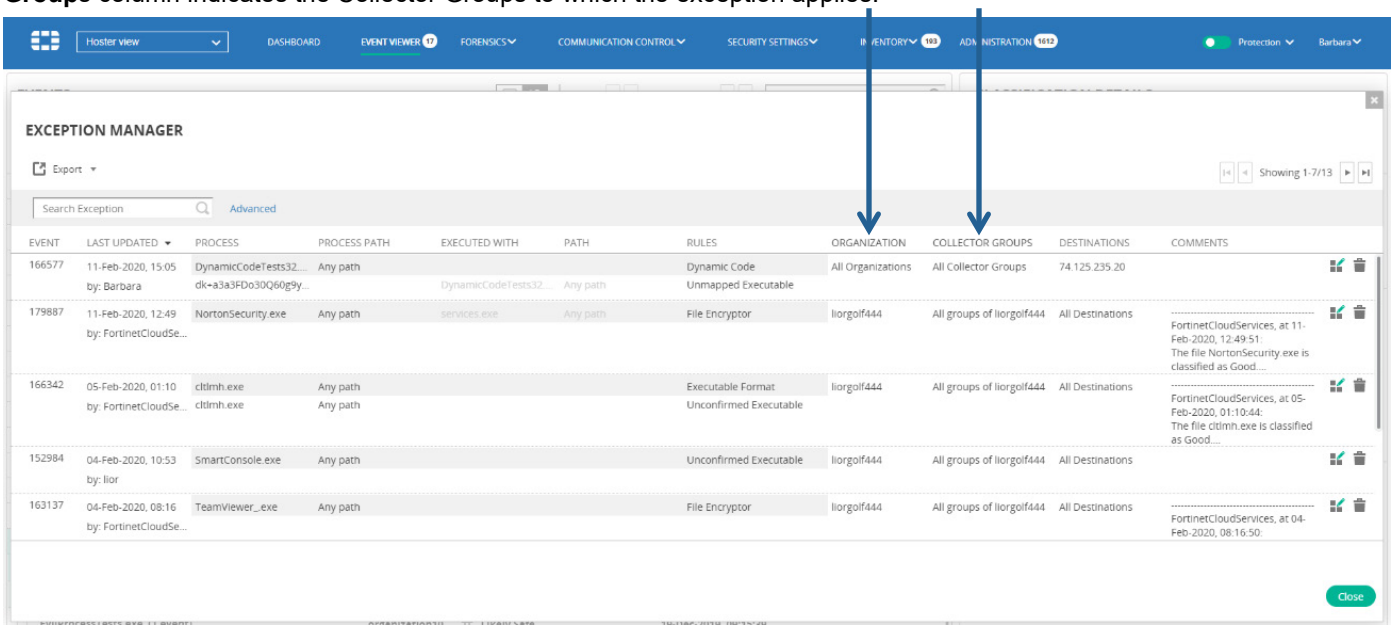
Exceptions Manager

In Hoster view, the Exceptions Manager window displays all exceptions from all organizations.

When creating an exception in Hoster view, the organization in which the event occurred is also shown in the Exception Creation window, as well as the event ID.



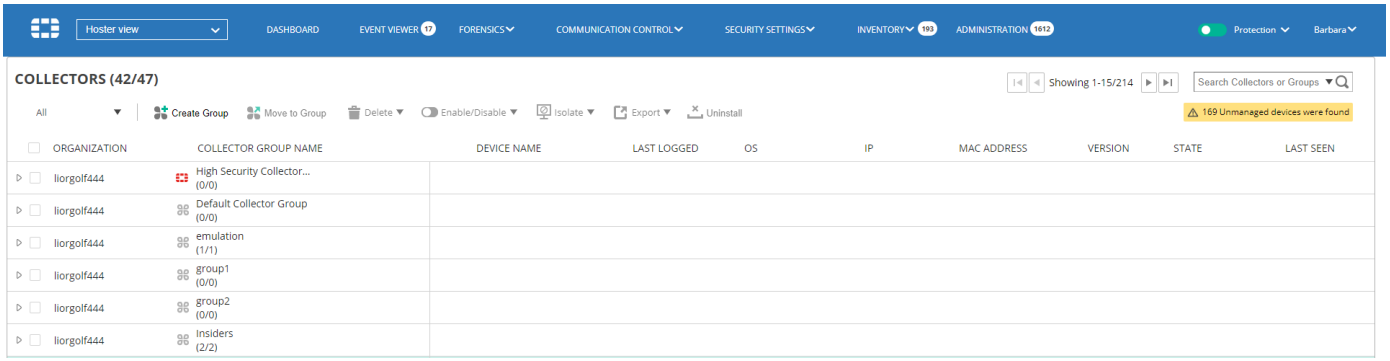
The Exception Manager window also shows the organization to which the exception applies. In addition, the **Collector Group**s column indicates the Collector Groups to which the exception applies.



Inventory

COLLECTORS Page

In Hoster view, the **COLLECTORS** page shows all the Collectors from all organizations.

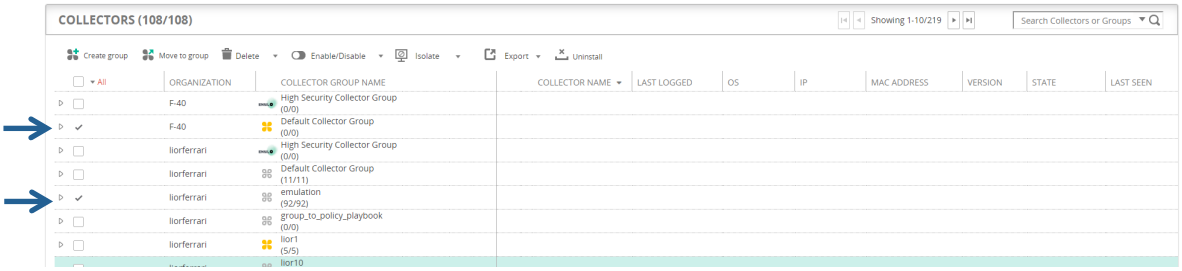


When in Hoster view, you can move Collectors between organizations using this window.

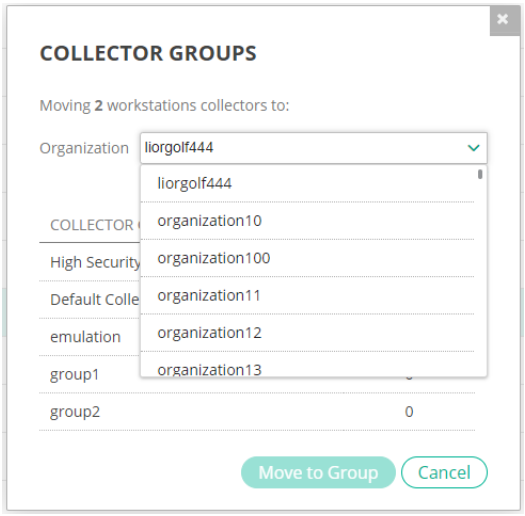
Note – Only Collectors from V3.0 and above can be in the non-default organization.
All older Collectors can only be installed in the default organization.
Only Collectors from V3.0 and above can be moved between organizations.

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.



2. Click the Move to group button. The following window displays:



3. In the **Organization** field, select the organization to which to move the Collector(s).
4. Click **Move to Group**.

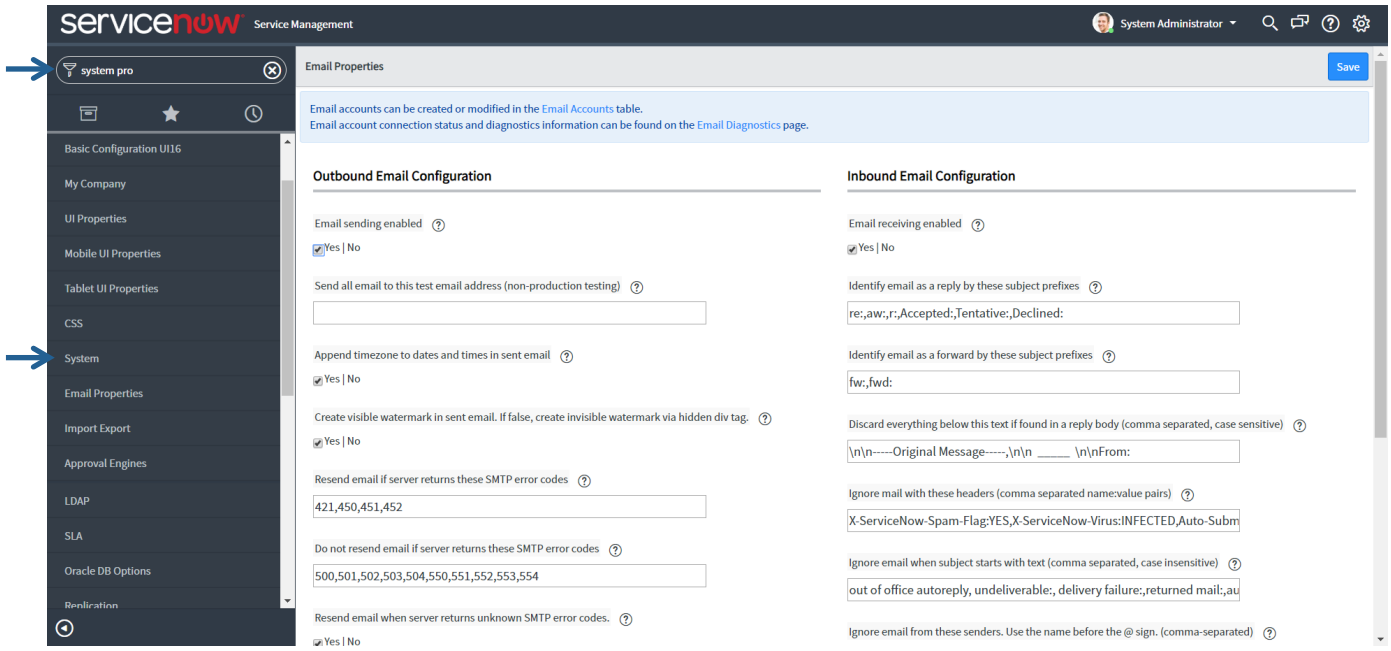
Appendix A – SETTING UP AN EMAIL FEED FOR OPEN TICKET

The Open Ticket feature enables you to send events to an event-management tool such as Jira or ServiceNow.

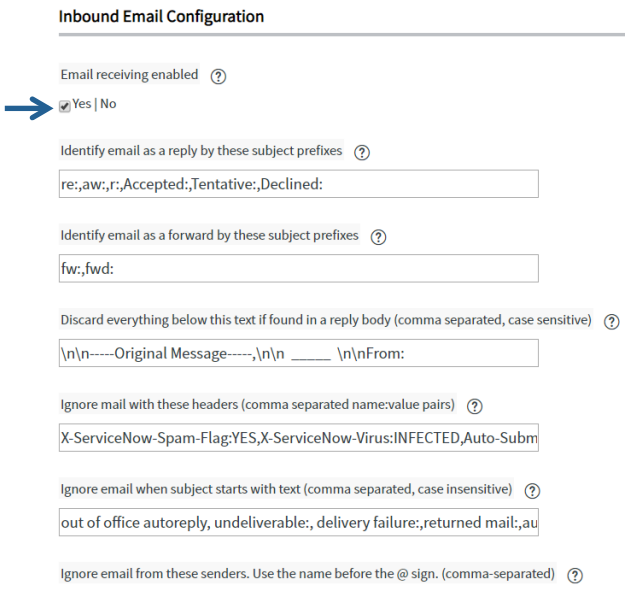
In order for the Open Ticket feature to work properly, you must set up a receiving email feed in the event-management tool to be used. This appendix provides an example that describes how to set up the required email feed in ServiceNow.

To set up an email feed in ServiceNow:

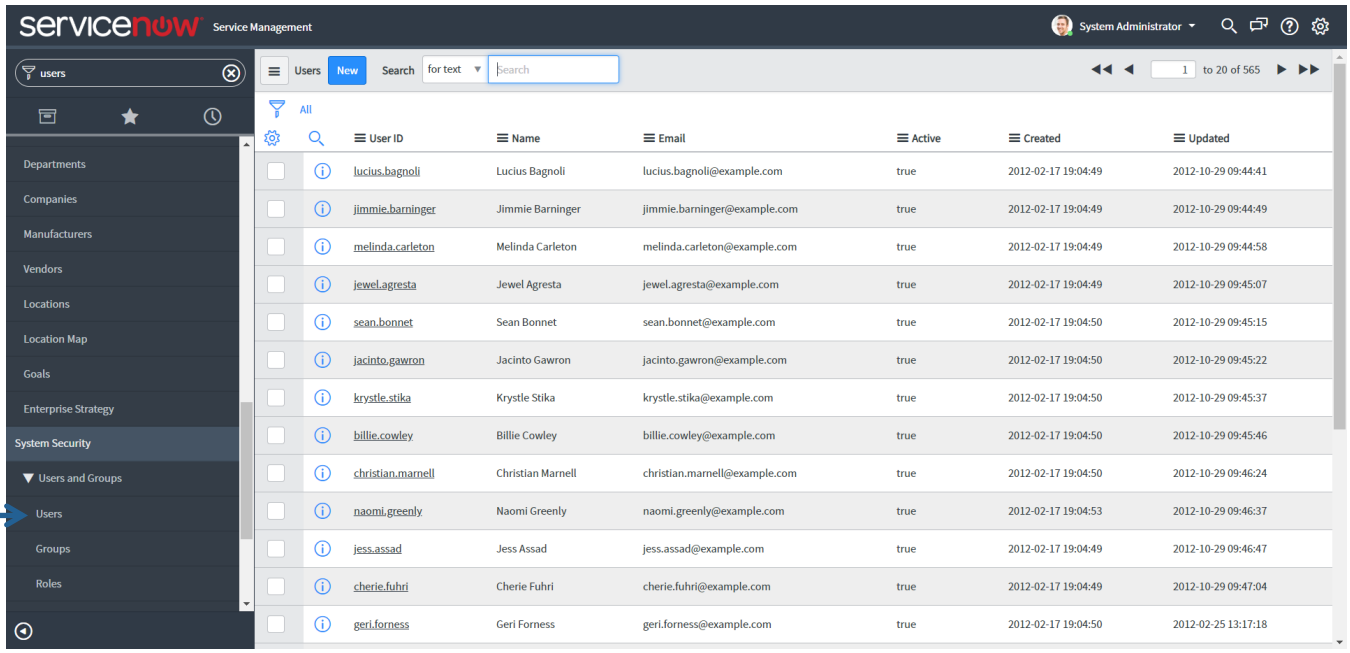
1. Launch ServiceNow.
2. In the window that opens, select **System Properties ➔ Email Properties**. The following window displays:



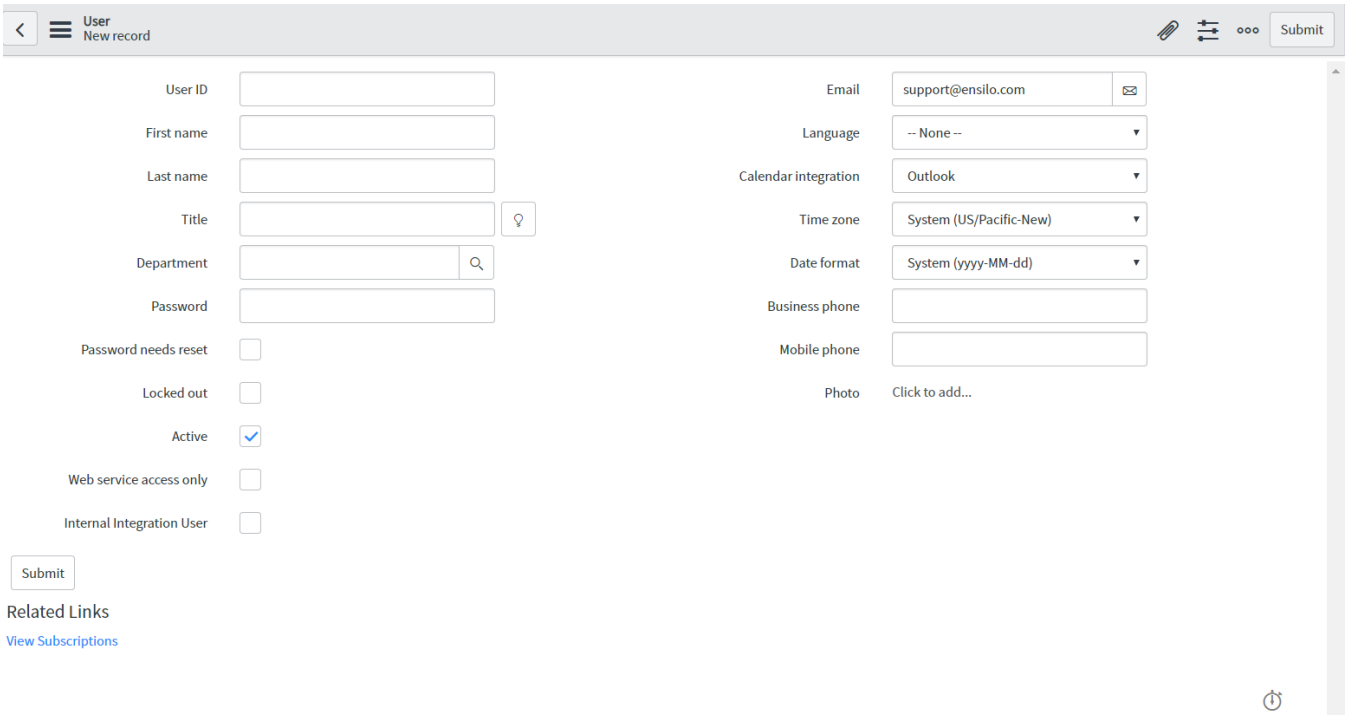
3. In the Inbound Email Configuration area, check the **Email receiving enabled** checkbox.



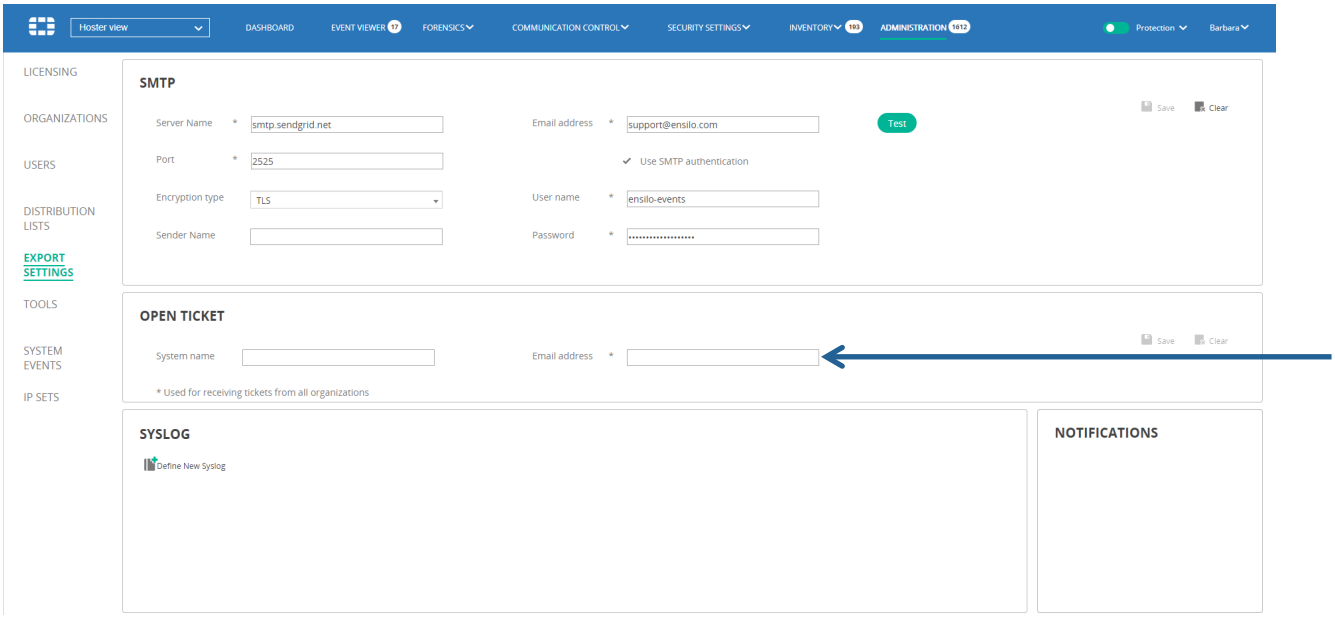
4. In the left pane, select **System Security ➔ Users and Groups ➔ Users**. The following window displays:



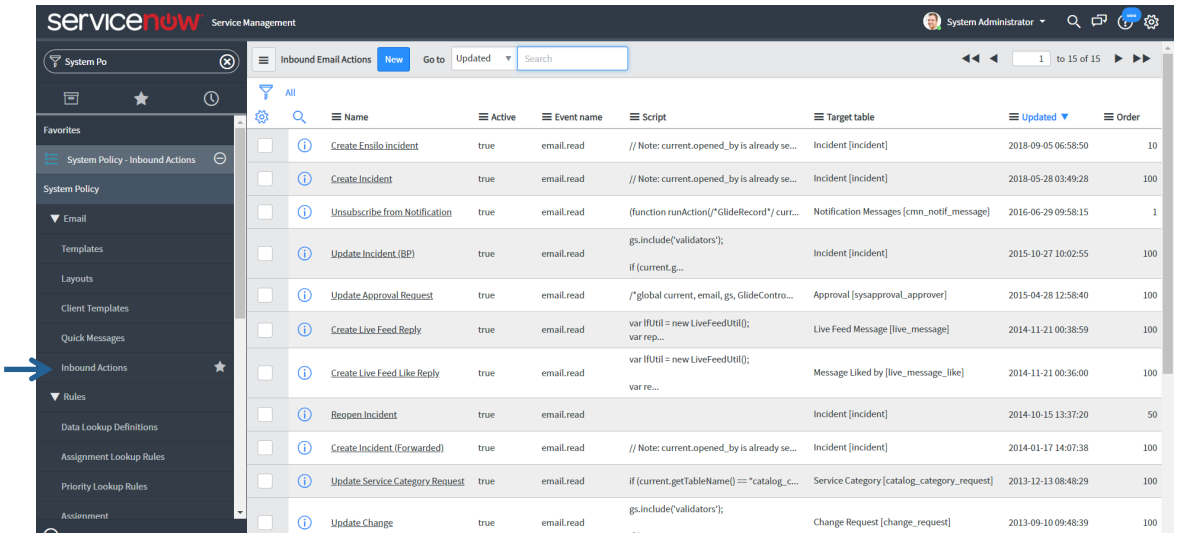
5. Click the New button to create a new user. The following window displays:



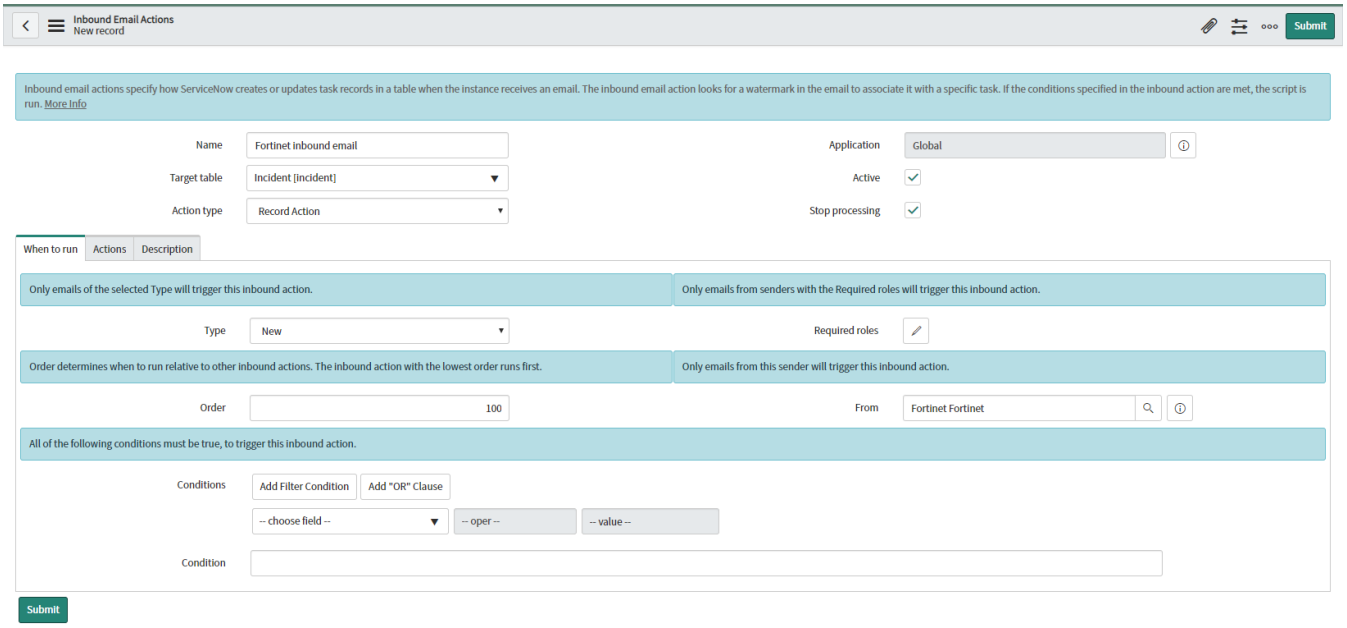
6. In the **Email** field, enter the email address of the FortiEDR messaging system. This email address is specified in the **Email Address** field of the FortiEDR Open Ticket settings, which can be accessed by selecting **Administration ➔ Export Settings** in the FortiEDR user interface, as shown below:



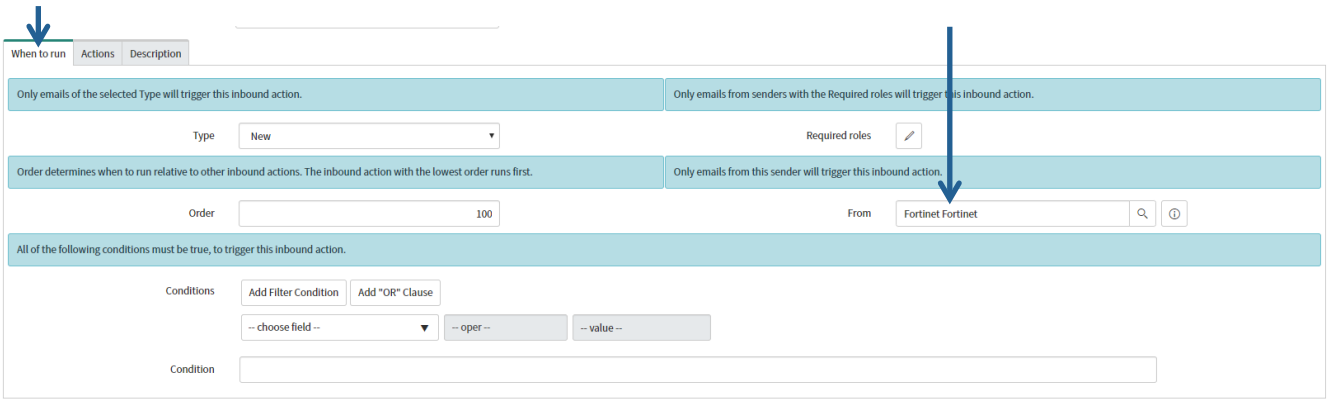
7. In the left pane, select **System Policy ➔ Email ➔ Inbound Actions**. The following window displays:



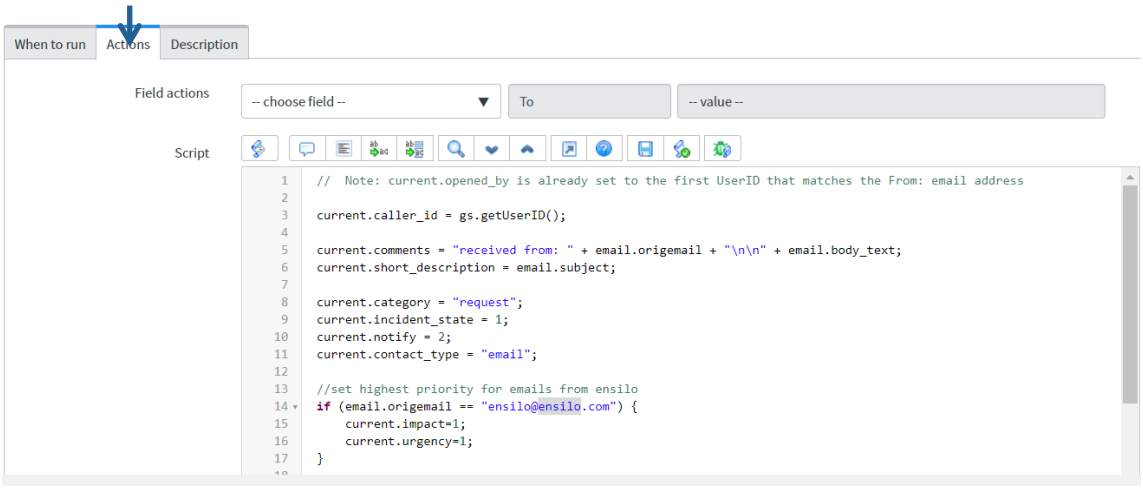
8. Click the New blue button to create new inbound email actions. The following window displays:



9. Fill in the following fields in this window:
   - **Name:** Enter a free-text name for the inbound email feed. For example, **Fortinet inbound email**.
   - **Target table:** Select **Incident [incident]** in the dropdown list.
   - **Action type:** Select **Record Action** in the dropdown list.
   - **Active:** Check this checkbox to select it.
   - **Stop processing:** Check this checkbox to select it.
10. In this window, select the **When to run** tab and then in the **From** field, select the FortiEDR user created in step **6**.



11. Select the **Actions** tab and then paste the provided JavaScript (see below) into the email body. You can modify this script, as needed.



The JavaScript includes the following code:

```
//  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 ensilo
if (email.origemail == "ensilo@ensilo.com") {
    current.impact=1;


    current.urgency=1;
}


if (email.body.assign != undefined)
    current.assigned_to = email.body.assign;


if (email.importance != undefined) {
    if (email.importance.toLowerCase() == "high")
```

```
        current.priority = 1;
}

if (email.body.priority != undefined)
    current.priority = email.body.priority;
//parsing fields from message body example
var severityStart = email.body_text.indexOf('Severity:') + 9;
var classificationStart = email.body_text.indexOf('Classification:') + 15;
var destinitionStart = email.body_text.indexOf('Destinations:');

var severity = email.body_text.slice(severityStart, classificationStart -15 );
var classification = email.body_text.slice(classificationStart,
destinitionStart);
 current.insert();
```

12. When pasting in the JavaScript, make sure that:
    - The emails address highlighted in yellow (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 highlighted in light blue 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 highlighted in pink 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: