FortiEDR Installation and Administration Guide

Version 5.0

Document Revision 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

December 2020

FortiEDR Installation and Administration Guide

Table of Contents

Change Log 9

Chapter 1 – INTRODUCING FortiEDR 10

Introduction 10

Execution Prevention 10

Data Exfiltration 10

Ransomware 10

Threat Hunting 11

FortiEDR Technology 11

FortiEDR Components 12

Overview 12

FortiEDR Collector 12

FortiEDR Core 13

FortiEDR Aggregator 14

FortiEDR Central Manager 14

FortiEDR Cloud Service 14

How Does FortiEDR Work? 15

Using FortiEDR – Workflow 16

Setup Workflow Overview 16

Ongoing Workflow Overview 17

Chapter 2 – INSTALLING FortiEDR 18

Before You Start 18

System Requirements 18

Installing the FortiEDR Threat-hunting Repository 19

Installing the FortiEDR Central Manager and FortiEDR Aggregator on the Same Machine 19

FortiEDR CLI Commands 25

Launching the FortiEDR Central Manager for the First Time 25

Installing the FortiEDR Core 29

Preparing for FortiEDR Core Installation 29

Installing the FortiEDR Core on Linux 29

Installing FortiEDR Collectors 34

Preparing for FortiEDR Collector Installation 34

Installing a FortiEDR Collector 35

Automated FortiEDR Collector Deployment on Windows 45

Automated FortiEDR Collector Deployment on Mac 46

Working with FortiEDR on VDI Environments 47

Working with FortiEDR on VDI Environments for Citrix XenDesktop VDI or XenApp 47

Uninstalling a FortiEDR Collector 47

Upgrading FortiEDR Components 48

Upgrading the Central Manager 49

Upgrading the Aggregator 49

Upgrading the Core 49

Upgrading the Collector 50

Chapter 3 – SECURITY SETTINGS 51

Introducing FortiEDR Security Policies 51

Out-of-the-box Policies 51

Protection or Simulation Mode 52

Security Policies Page 53

Setting a Security Policy’s Prevention or Simulation Mode 54

Creating a New Security Policy 55

Assigning a Security Policy to a Collector Group 56

Playbook Policies 58

Automated Incident Response - Playbooks Page 58

Assigned Collector Groups 59

Exception Manager 65

Threat Hunting Settings 67

Assigning a Collector Group to a Profile 68

Creating/Cloning a Profile 68

Exclusion Manager 69

Filters 69

Defining Exclusion Lists 70

Defining Exclusions 71

Chapter 4 – INVENTORY 74

Introducing the Inventory 74

Uninstalling a Collector 75

Collectors 75

Defining a New Collector Group 78

Assigning Collectors to a Collector Group 79

Deleting a Collector Group/Collector 79

Enabling/Disabling a Collector 79

Device Isolation 80

Unmanaged Devices 81

IoT Devices 82

Defining a New IoT Group 82

Assigning Devices to an IoT Group 83

Deleting an IoT Device/IoT Group 83

Refreshing IoT Device Data 83
Exporting IoT Information 84
System Components 84
Aggregators 85
Cores 85
Repositories 86
Exporting Logs 86
Exporting Logs for Collectors 87
Exporting Logs for Cores 88
Exporting Logs for Aggregators 88
Chapter 5 – DASHBOARD 89
Introduction 89
Security Events Chart 90
Communication Control Chart 91
Collectors Chart 91
Most Targeted Charts 92
External Destinations 92
System Components 93
Executive Summary Report 93
Event Statistics 94
Destinations 94
Most-targeted Devices 95
Most-targeted Processes 95
Communication Control 95
System Components 96
License Status 96
Chapter 6 – EVENT VIEWER 97
Introducing the Event Viewer 97
Events Pane 100
Advanced Data 102
Event Graph 102
Geo Location 102
Automated Analysis 103
Marking a Security Event as Handled/Unhandled 104
Manually Changing the Classification of a Security Event 105
Defining Security Event Exceptions 107
Defining the Scope of an Exception 107
Defining a Security Event as an Exception 109

Device Control Exceptions 115

Editing Security Event Exceptions 116

Marking a Security Event as Read/Unread 117

Viewing Relevant Activity Events 117

Viewing Expired Security Events 117

Viewing Device Control Security Events 118

Other Options in the Event Viewer 118

Classification Details 120

Chapter 7 – COMMUNICATION CONTROL 123

Application Communication Control – How Does It Work? 123

Introducing Communication Control 124

Applications 125

Reputation Score 126

Vulnerability 127

Resolved vs. Unresolved Applications 128

Sorting the Application List 129

Marking an Entry as Read/Unread 129

Modifying a Policy Action 129

Searching the Application List 131

Other Options in the Applications Pane 132

Advanced Data 132

Policies 136

Predefined Policies 138

Policy Mode 138

Policy Rules 139

Assigning a Policy to a Collector Group 141

Creating a New Communication Control Policy 142

Other Options in the Policies Pane 143

Chapter 8 – FORENSICS 144

Introduction 144

Flow Analyzer View 148

Stack View 149

Compare View 150

Defining an Exception 151

Remediating a Device upon Malware Detection 151

Retrieving Memory 154

Isolating a Device **156**

Threat Hunting **158**

Threat Hunting 158

Legacy Threat Hunting 175

Chapter 9 – ADMINISTRATION **178**

Licensing **178**

Updating the Collector Version 179

Loading a Server Certificate 180

Requesting and Obtaining a Collector Installer 181

Users **183**

Two-factor Authentication 184

Resetting a User Password 185

LDAP Authentication **186**

SAML Authentication **188**

SAML IdP configuration with Azure 190

SAML IdP Configuration with Okta 194

SAML IdP Configuration with FortiAuthenticator 199

FortiAuthenticator IdP Configuration 199

User Groups Management Settings on FortiAuthenticator 199

Service Provider Settings for FortiEDR on FortiAuthenticator 201

Distribution Lists **203**

Export Settings **204**

SMTP 204

Open Ticket 205

Syslog 206

Tools **208**

Audit Trail 208

Component Authentication 210

Automatic Collector Updates 210

File Scan 210

End-user Notifications 211

IoT Device Discovery 213

Personal Data Handling 214

Windows Security Center 218

System Events **219**

IP Sets **220**

Integrations **221**

Firewall Integration 221

Sandbox Integration 225

Network Access Control Integration 226

eXtended Detection Source Integration 229

Chapter 10 – TROUBLESHOOTING..231
A FortiEDR Collector Does Not Display in the INVENTORY Tab..231
No Events on the FortiEDR Central Manager Console...231
User Cannot Communicate Externally or Files Modification Activity Is Blocked.............................232
Microsoft Windows-based Devices..232
MacOS-based Devices...232
Chapter 11 – MULTI-TENANCY (ORGANIZATIONS)..233
What is a Multi-organization Environment in FortiEDR?..233
Multi-organization and User Roles..233
Component Registration in a Multi-organization Environment...234
Collector Registration..234
Core Registration..234
Workflow...235
Step 1 – Logging In to a Multi-organization System...235
Step 2 – Defining or Importing an Organization..236
Step 3 –Navigating Between Organizations..239
Step 4 – Defining a Local Administrator for an Organization...239
Step 5 – Performing Operations in the FortiEDR System...240
Migrating an Organization..241
Hoster View..247
Licensing...247
Users...248
Dashboard..249
Event Viewer..249
Forensics..251
Communication Control..251
Threat Hunting..252
Security Settings...252
Exception Manager...254
Inventory...255
Appendix A – SETTING UP AN EMAIL FEED FOR OPEN TICKET..................257
Appendix B – LUCENE SYNTAX..265
Terms...265
Operators..265
Wildcards..266
Ranges..266
Reserved Characters..266
Appendix C – CONTAINERS MANAGEMENT..267

Change Log

Date	Change Description
December 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.

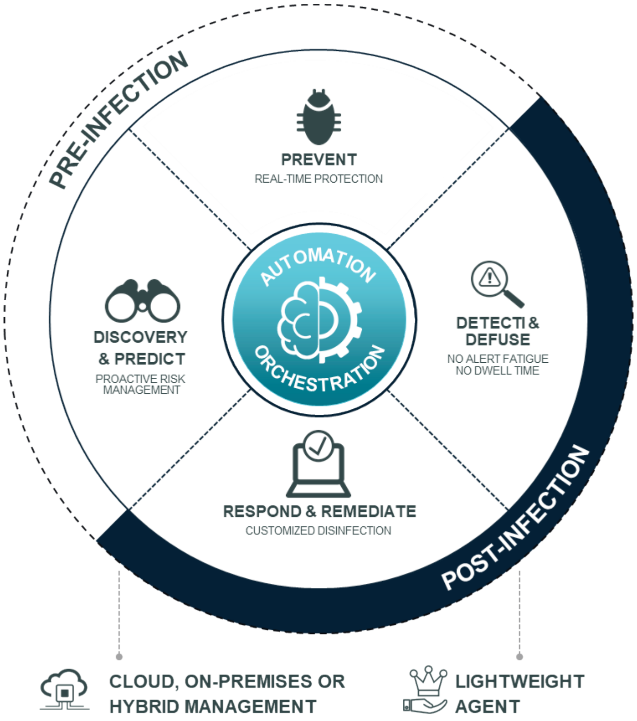
Threat Hunting

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

FortiEDR Technology



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

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

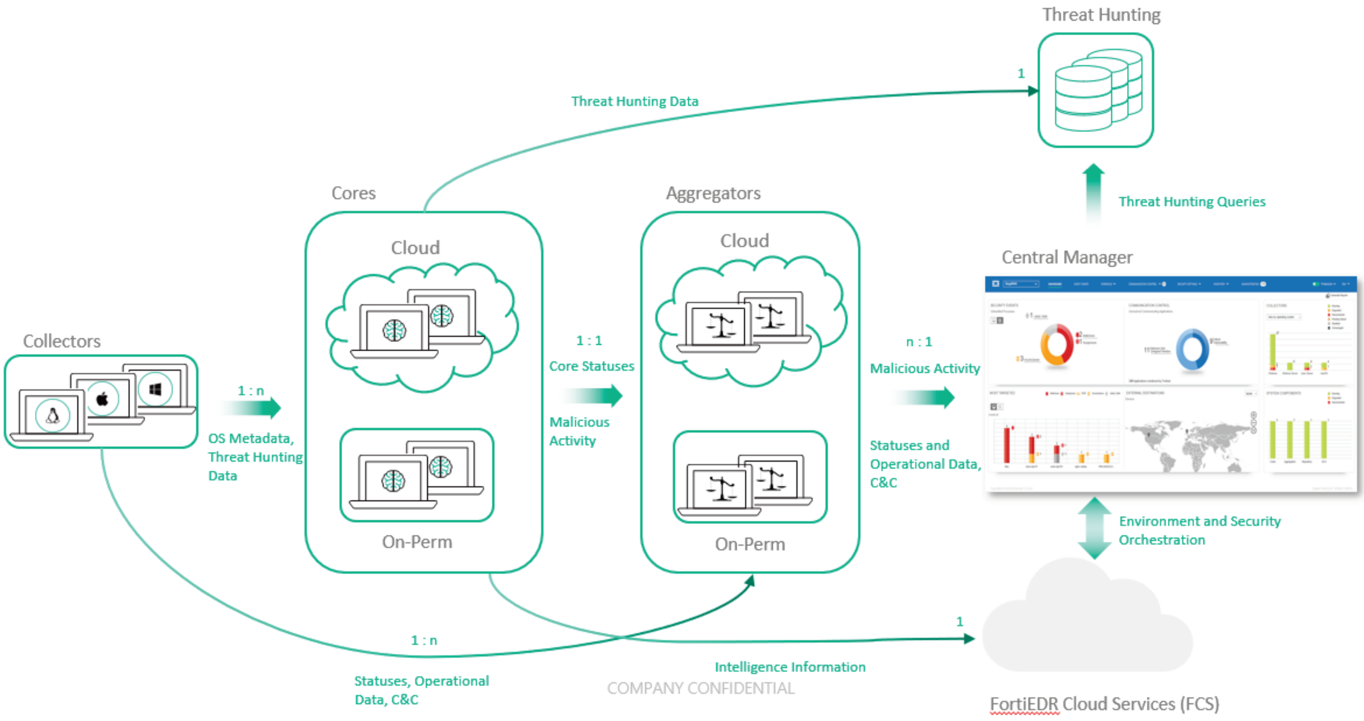
Our research revealed that all legitimate outgoing communications must pass through the operating system. Thus, by monitoring the operating system internals it is possible to verify that a connection was established in a valid manner. FortiEDR gathers OS stack data, thread and process related data and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

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

FortiEDR Components

Overview

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



FortiEDR Collector

The FortiEDR Collector is 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 210.

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 232.

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 a security event. The FCS is a cloud-based, GDPR-compliant, software-only service that determines the exact classification of security events and acts accordingly based on that classification – all with a high degree of accuracy.

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

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

- **Tuning:** Automated security event exception (whitelisting). After a triggered security event is reclassified as *Safe,* an automated cross-environment exception can be pushed downstream and expire the event, preventing it from triggering again. For more details, see *Exceptions* on page 65.
- **Playbook Actions:** All Playbook policy actions are based on the final determination of the FCS. For more details, see *Playbook Policies* on page 57.

How Does FortiEDR Work?

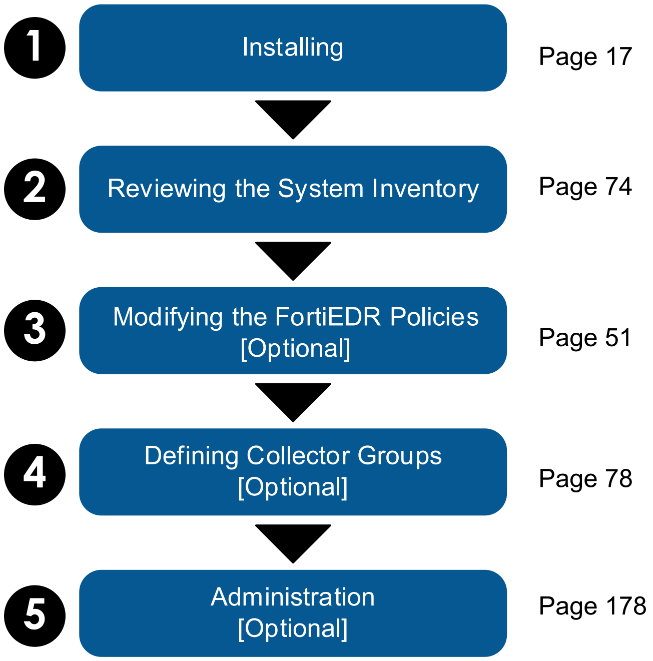
- **Step 1, The FortiEDR Collector Collects OS Metadata:** A FortiEDR Collector runs on each communicating device in the organization and transparently collects OS metadata on the computing device.
- **Step 2, Communicating Device Makes a Connection Establishment Request:** When any connection establishment 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 security event (alert) that is packaged with an abundance of device metadata describing the internals of the operating system leading up to the malicious connection establishment request. This security event is triggered by the FortiEDR Core and is viewable in the FortiEDR Central Manager console. FortiEDR can also send email alerts and/or be integrated with any standard Security Information and Event Management (SIEM) solution via Syslog.
- 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 security event and the internal stack data that led up to it.

Using FortiEDR – Workflow

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

Setup Workflow Overview

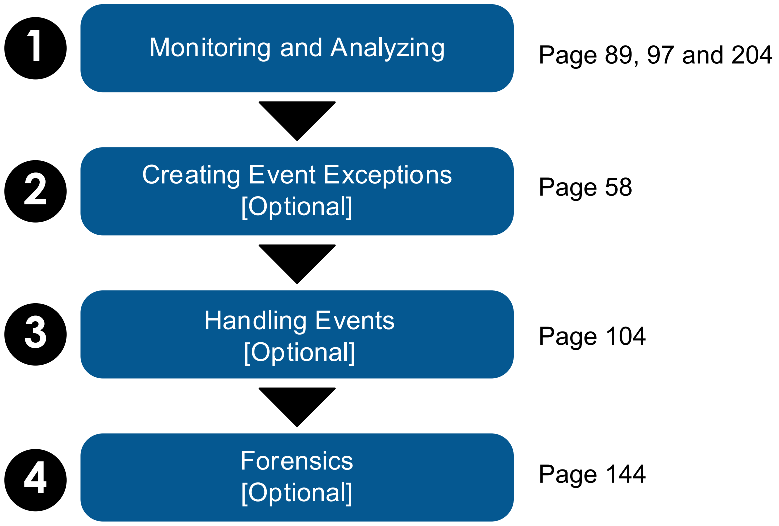
The following describes the workflow for getting FortiEDR up and running in your organization:


1
Installing
Page 17
2
Reviewing the System Inventory
Page 74
3
Modifying the FortiEDR Policies [Optional]
Page 51
4
Defining Collector Groups [Optional]
Page 78
5
Administration [Optional]
Page 178

- **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 25).
- **Step 2, Reviewing the Inventory:** Review the health status and details of all the FortiEDR components in the **DASHBOARD** (page 89) and **INVENTORY** tab (page 74). 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 51) 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 78). You can then assign the required policy to each Collector Group (page 56).
- **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 security events on an ongoing basis:



- **Monitoring:** Monitor and analyze the events triggered by FortiEDR in the:
  - **Dashboard** (page 89)
  - **Event Viewer** (page 97)
  - **SIEM via Syslog** (page 204)
- **[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 58).
- **[Optional] Handling Events:** Mark security events that you have handled and optionally describe how they were handled (page 104).
- **[Optional] Forensics** (page 144): This licensed add-on enables deep investigation into a security 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 19
- FortiEDR Cores, page 29
- FortiEDR Collectors, page 34

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 SP1, 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), Catalina (10.15) and Big Sur (11). ▪ Linux Versions: RedHat Enterprise Linux and CentOS 6.8+, 7.2+ and 8 and Ubuntu LTS 16.04.5+, 18.04 and 20.04 server, 64-bit only and Oracle Linux 8.2+. The complete list of supported Linux versions and kernels is updated regularly and can be provided upon request. ▪ 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.

Installing the FortiEDR Threat-hunting Repository

The FortiEDR threat-hunting repository handles the FortiEDR threat-hunting feature, which is described on page 158. 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.

On premise Threat Hunting Repository is currently not supported.

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

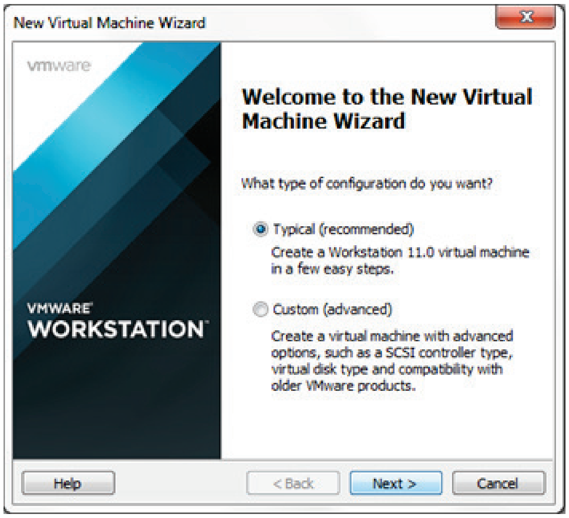
The following describes how to install both the FortiEDR Central Manager and the FortiEDR Aggregator on the same machine.

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 24.

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:


New Virtual Machine Wizard

Welcome to the New Virtual Machine Wizard

What type of configuration do you want?

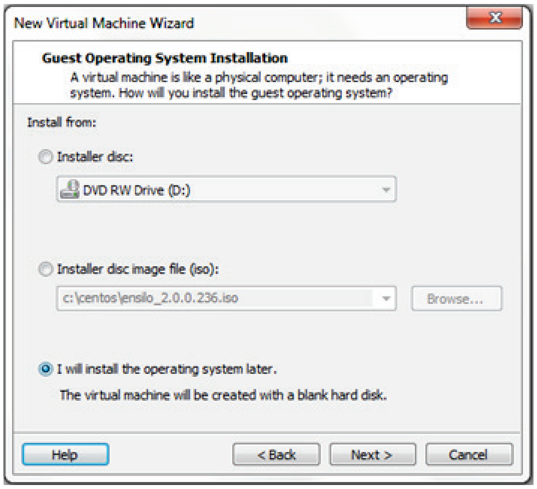
● Typical (recommended)

Create a Workstation 11.0 virtual machine in a few easy steps.

○ Custom (advanced)

Create a virtual machine with advanced options, such as a SCSI controller type, virtual disk type and compatibility with older VMware products.

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


New Virtual Machine Wizard

Guest Operating System Installation

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

○ Installer disc:

DVD RW Drive (D:)

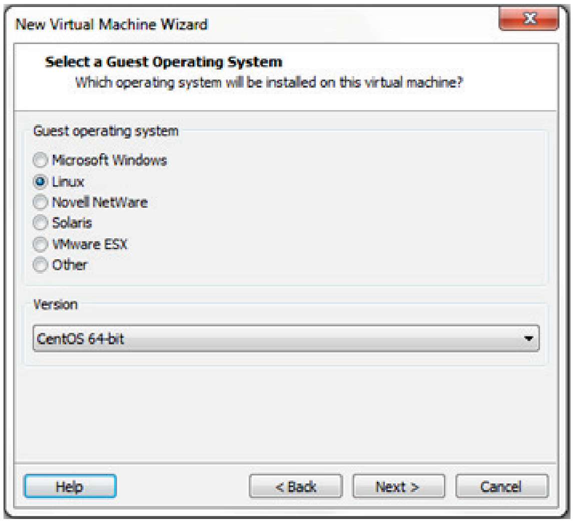
○ Installer disc image file (iso):

c:\centos\ensilo_2.0.0.236.iso

● I will install the operating system later.

The virtual machine will be created with a blank hard disk.

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


New Virtual Machine Wizard

Select a Guest Operating System

Which operating system will be installed on this virtual machine?

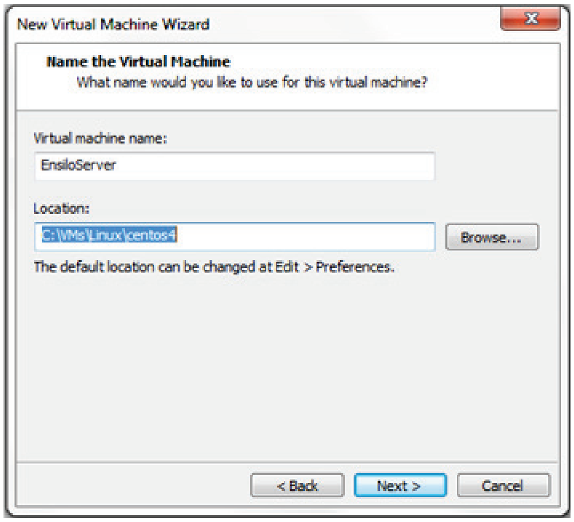
Guest operating system

○ Microsoft Windows
● Linux
○ Novell NetWare
○ Solaris
○ VMware ESX
○ Other

Version

CentOS 64-bit

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:



Name the Virtual Machine

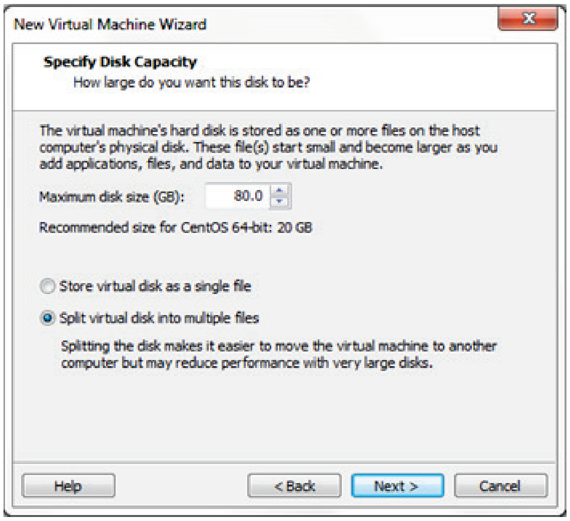
What name would you like to use for this virtual machine?

Virtual machine name: EnsiloServer

Location: C:\VMs\Linux\centos4

The default location can be changed at Edit > Preferences.

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:



Specify Disk Capacity

How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

Maximum disk size (GB): 80.0

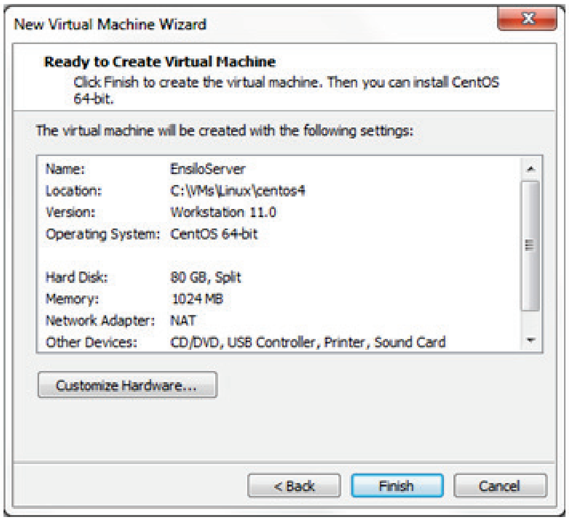
Recommended size for CentOS 64-bit: 20 GB

○ Store virtual disk as a single file

● Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

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:



New Virtual Machine Wizard

Ready to Create Virtual Machine

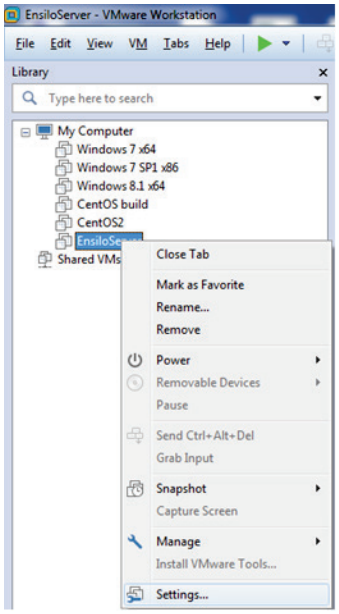
Click Finish to create the virtual machine. Then you can install CentOS 64-bit.

The virtual machine will be created with the following settings:

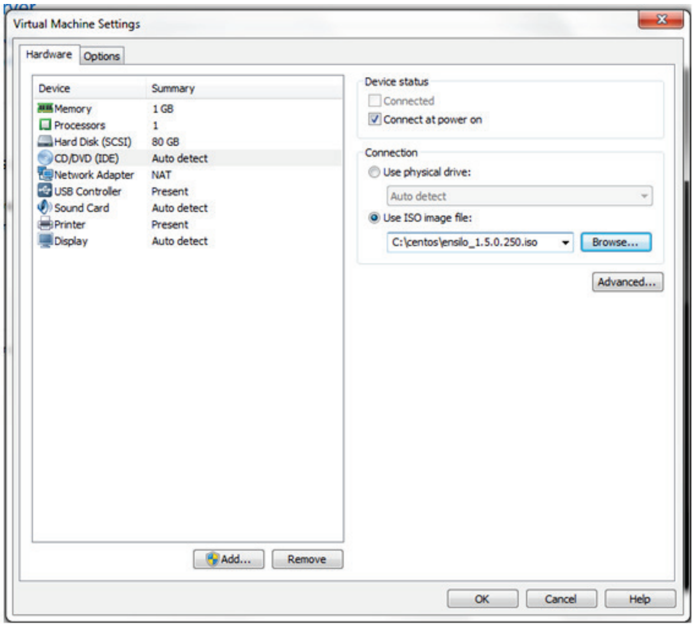
Name:	EnsiloServer
Location:	C:\VMs\Linux\centos4
Version:	Workstation 11.0
Operating System:	CentOS 64-bit
Hard Disk:	80 GB, Split
Memory:	1024 MB
Network Adapter:	NAT
Other Devices:	CD/DVD, USB Controller, Printer, Sound Card

7 Click **Finish**.

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



The following window displays:



Virtual Machine Settings

Hardware | Options

Device	Summary
Memory	1 GB
Processors	1
Hard Disk (SCSI)	80 GB
CD/DVD (IDE)	Auto detect
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Device status

□ Connected

☑ Connect at power on

Connection

○ Use physical drive:

Auto detect

● Use ISO image file:

C:\centos\ensilo_1.5.0.250.iso

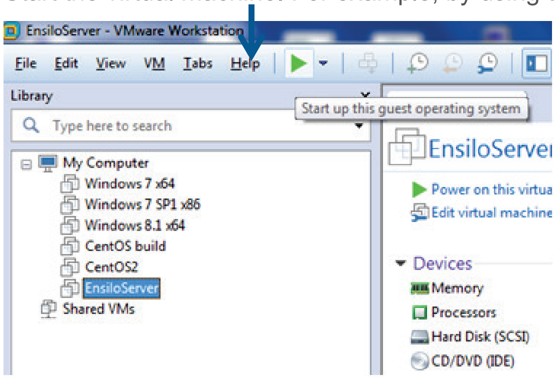
9 Select the **Memory** option and change the RAM to at least 8 GB.

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 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**.

21 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.

22 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.

23 At the prompt, enter the default gateway and click **Next**.

24 At the `Please set your DNS server` prompt, enter a valid IP address and click **Next**. Use the following format: xxx.xxx.xxx.xxx/yyyy, where yyyy is the routing prefix of the subnet.

25 At the prompt, select **No** for debug mode.

26 At the `Please set the date` prompt, verify the date and click **Next**. The installer automatically presents the current date. You can change this date, if necessary.

27 At the `Please set your Time` prompt, set the time and click **Next**.

28 At the prompt, select the `timezone` and `country` in which the server is being installed.

29 Wait a few moments while the installation processes, until you see the `Installation completed successfully` message.

30 Log in for the first time, as described on page 25.

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 20.

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 20. Then, perform the steps described below.

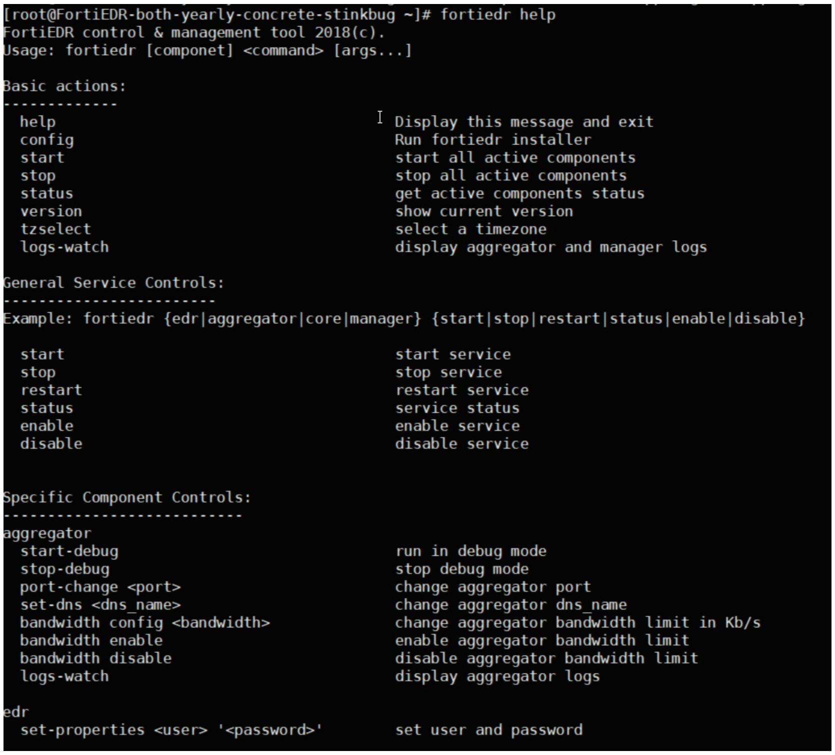
3 At the `Please enter the management IP address` prompt, enter the IP address to be used for communicating with the FortiEDR Central Manager and click **Next**.

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 20.

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.

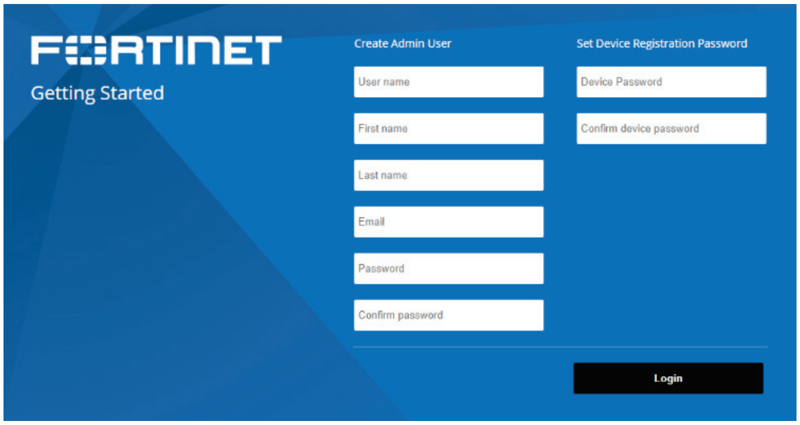
To launch the FortiEDR Central Manager:

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.

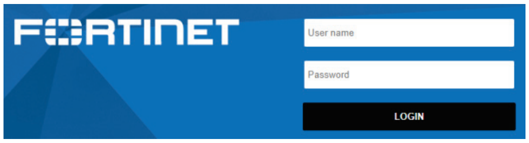
3 Enter and confirm the password to be used by this administrator user.

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.

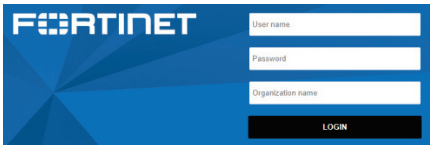
Write this password down in a good place. This password will be needed each time a FortiEDR component is installed. If you forgot your registration password, contact Fortinet support. FortiEDR support can reset your password and provide you with a new one.

---

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



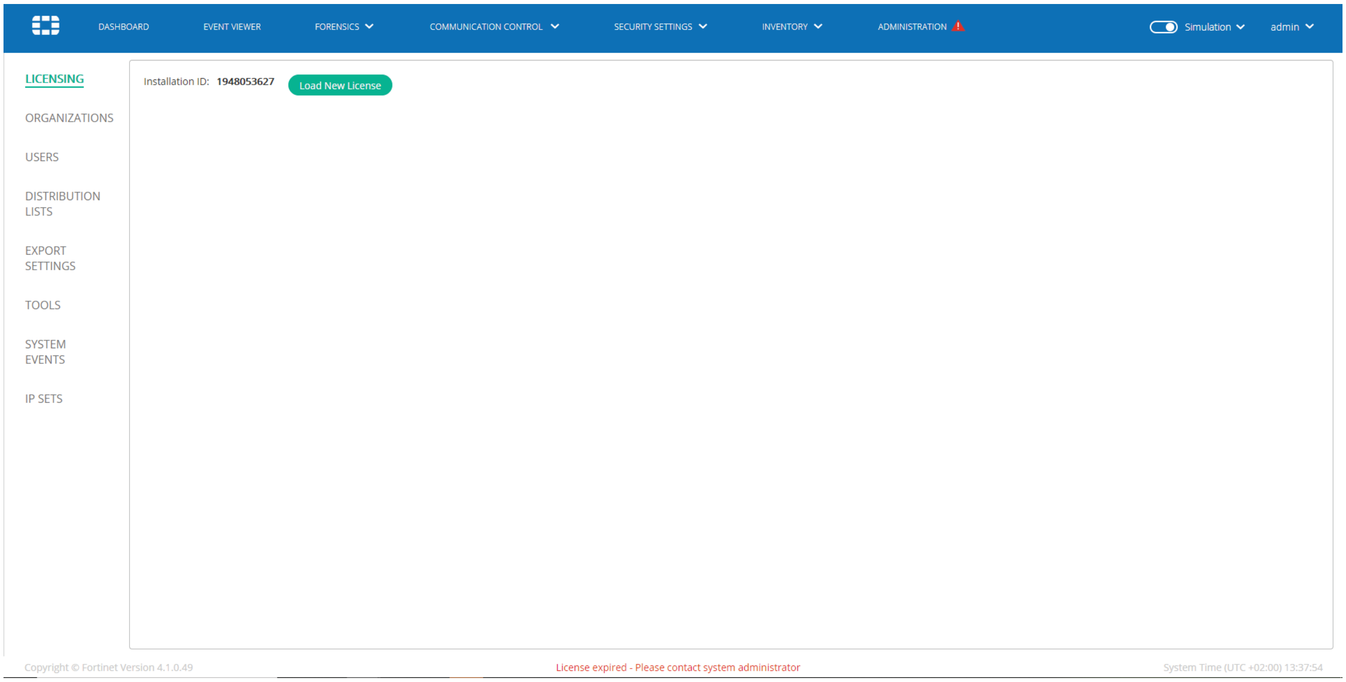
Login Page in a Multi-organization System

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 235.

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:



Installation ID: 1948053627

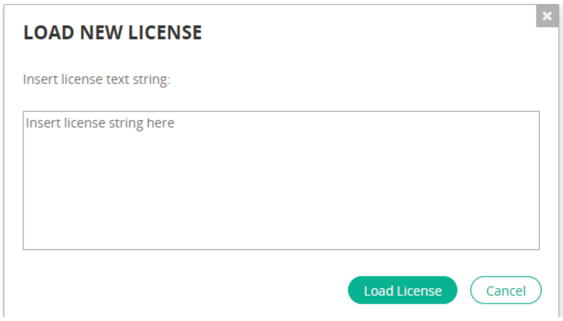
Copyright © Fortinet Version 4.1.0.49

License expired - Please contact system administrator

System Time (UTC +02:00) 13:37:54

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

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

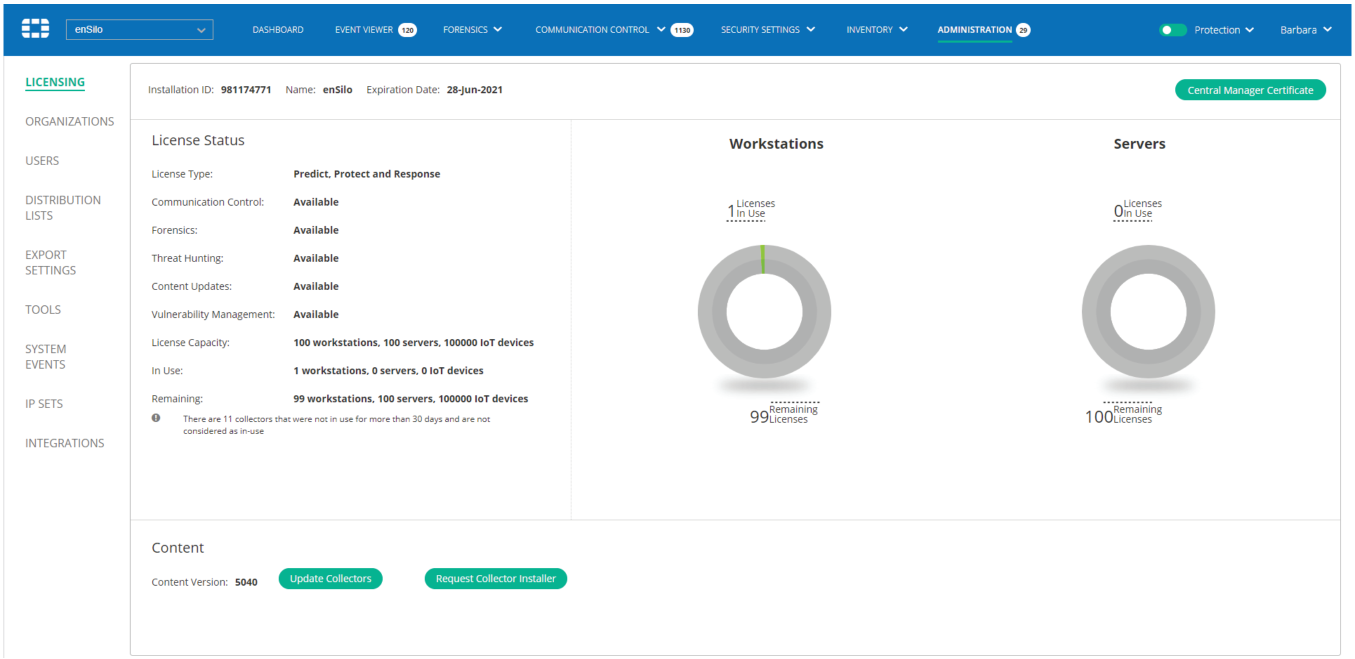


LOAD NEW LICENSE

Insert license text string:

Insert license string here

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



Installation ID: 981174771 Name: enSilo Expiration Date: 28-Jun-2021

License Status

License Type: Predict, Protect and Response

Communication Control: Available

Forensics: Available

Threat Hunting: Available

Content Updates: Available

Vulnerability Management: Available

License Capacity: 100 workstations, 100 servers, 100000 IoT devices

In Use: 1 workstations, 0 servers, 0 IoT devices

Remaining: 99 workstations, 100 servers, 100000 IoT devices

There are 11 collectors that were not in use for more than 30 days and are not considered as in-use

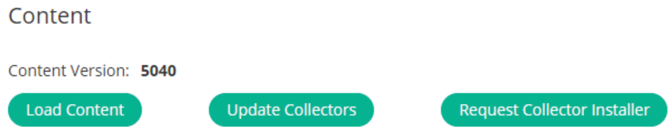
Content

Content Version: 5040

- **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 233.
- **Expiration Date:** Specifies when this license expires. Notifications will be sent to you beforehand.
- **License Type:** Specifies whether the **Discover, Protect and Response** license, **Discover, Protect and Response – Air-gapped** license, **Discover and Protect** license or **Protect and Response** license was purchased. The license type defines the availability of the relevant add-ons.
- **Communication Control:** Specifies the word **Available** if the **Communication Control** add-on is included in the license.
- **Forensics:** Specifies the word **Available** if the Forensics add-on (described on page 144) is included in the license.
- **Threat Hunting:** Specifies the word **Available** if the Threat hunting add-on (described on page 158) 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.



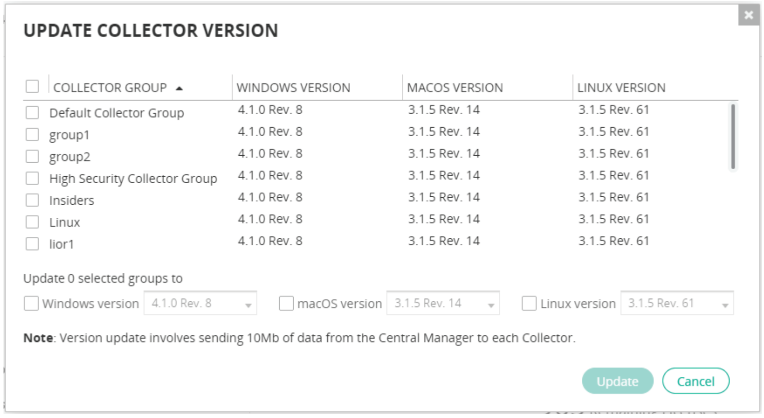
Content

Content Version: **5040**

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

If the content file contains a Collector update, you can update all Collectors with the new version at that time, or choose to do so later.

Click the Update Collectors button to update the version for all Collectors.



UPDATE COLLECTOR VERSION

□ COLLECTOR GROUP ▲	WINDOWS VERSION	MACOS VERSION	LINUX VERSION
□ Default Collector Group	4.1.0 Rev. 8	3.1.5 Rev. 14	3.1.5 Rev. 61
□ group1	4.1.0 Rev. 8	3.1.5 Rev. 14	3.1.5 Rev. 61
□ group2	4.1.0 Rev. 8	3.1.5 Rev. 14	3.1.5 Rev. 61
□ High Security Collector Group	4.1.0 Rev. 8	3.1.5 Rev. 14	3.1.5 Rev. 61
□ Insiders	4.1.0 Rev. 8	3.1.5 Rev. 14	3.1.5 Rev. 61
□ Linux	4.1.0 Rev. 8	3.1.5 Rev. 14	3.1.5 Rev. 61
□ lior1	4.1.0 Rev. 8	3.1.5 Rev. 14	3.1.5 Rev. 61

Update 0 selected groups to

□ Windows version 4.1.0 Rev. 8 □ macOS version 3.1.5 Rev. 14 □ Linux version 3.1.5 Rev. 61

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

- **Vulnerability Management:** Specifies the word **Available** if the Vulnerability Management add-on (described on page 178) 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 231.
- 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

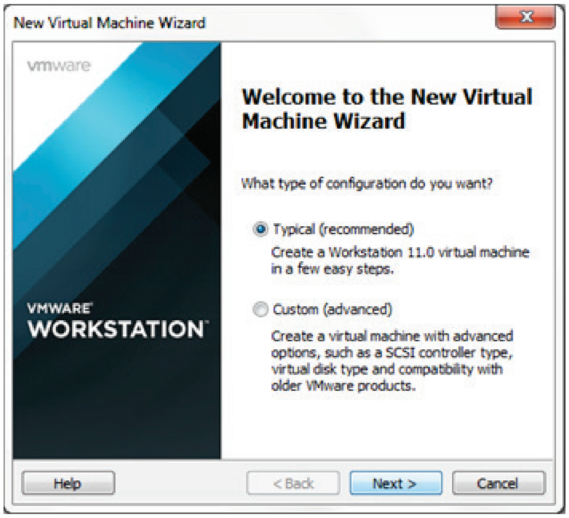
Note – For more details about installing a Core in a multi-organization environment, see the *Core Registration* section on page 234.

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:



New Virtual Machine Wizard

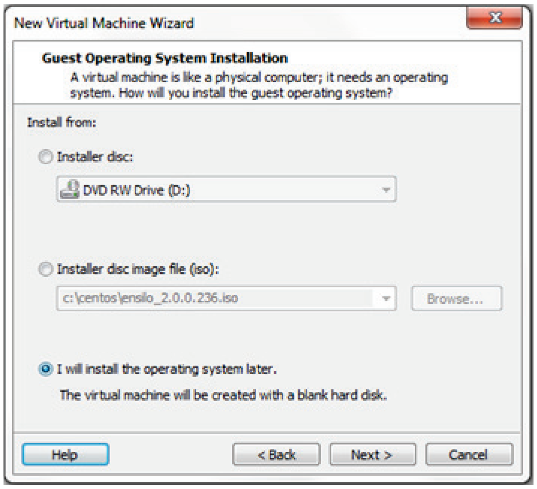
Welcome to the New Virtual Machine Wizard

What type of configuration do you want?

● Typical (recommended)
Create a Workstation 11.0 virtual machine in a few easy steps.

○ Custom (advanced)
Create a virtual machine with advanced options, such as a SCSI controller type, virtual disk type and compatibility with older VMware products.

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



Guest Operating System Installation
A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

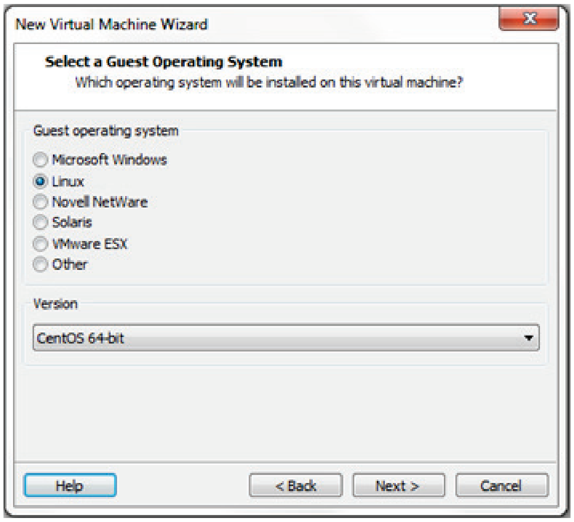
Install from:

○ Installer disc:
DVD RW Drive (D:)

○ Installer disc image file (iso):
c:\centos\ensilo_2.0.0.236.iso

● I will install the operating system later.
The virtual machine will be created with a blank hard disk.

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

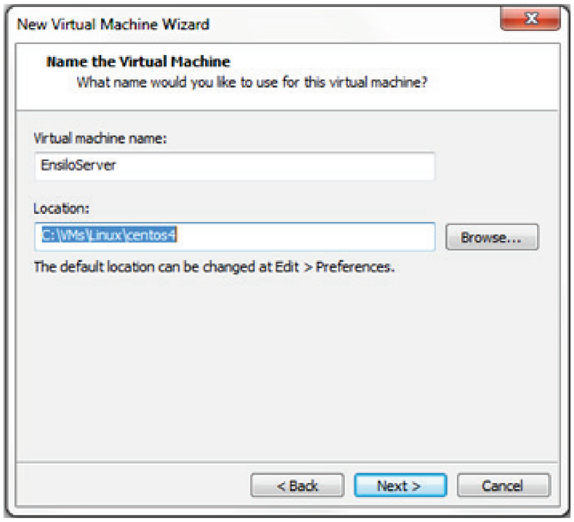


Select a Guest Operating System
Which operating system will be installed on this virtual machine?

Guest operating system
○ Microsoft Windows
● Linux
○ Novell NetWare
○ Solaris
○ VMware ESX
○ Other

Version
CentOS 64-bit

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:



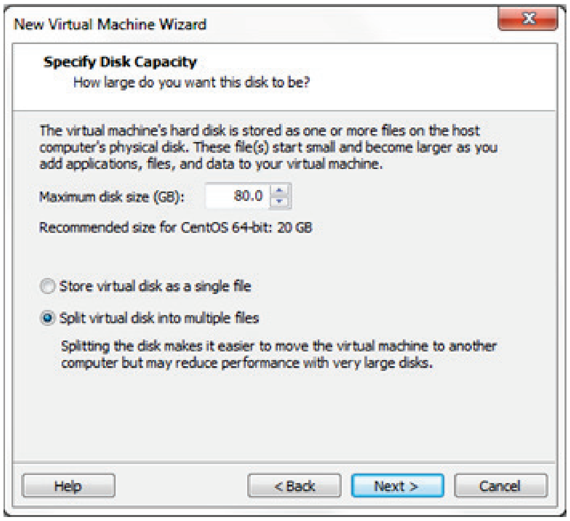
Name the Virtual Machine
What name would you like to use for this virtual machine?

Virtual machine name:
EnsiloServer

Location:
C:\VMs\Linux\centos4

The default location can be changed at Edit > Preferences.

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:



New Virtual Machine Wizard

Specify Disk Capacity
How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

Maximum disk size (GB): 80.0

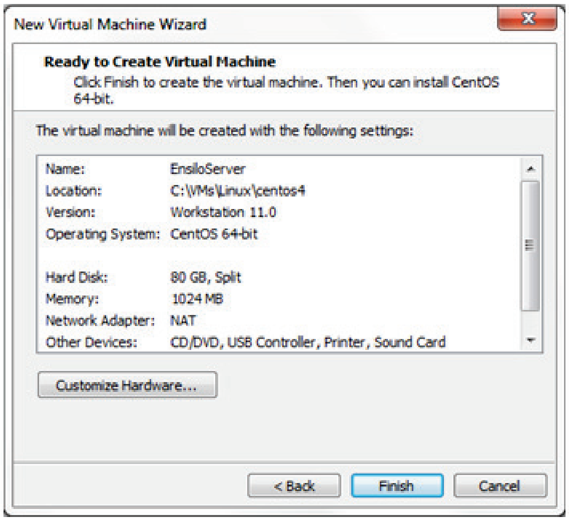
Recommended size for CentOS 64-bit: 20 GB

○ Store virtual disk as a single file

● Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

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:



New Virtual Machine Wizard

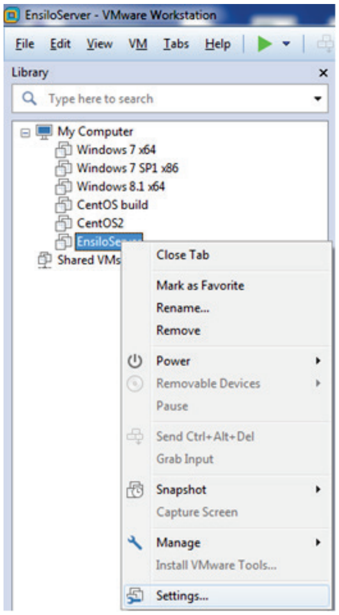
Ready to Create Virtual Machine
Click Finish to create the virtual machine. Then you can install CentOS 64-bit.

The virtual machine will be created with the following settings:

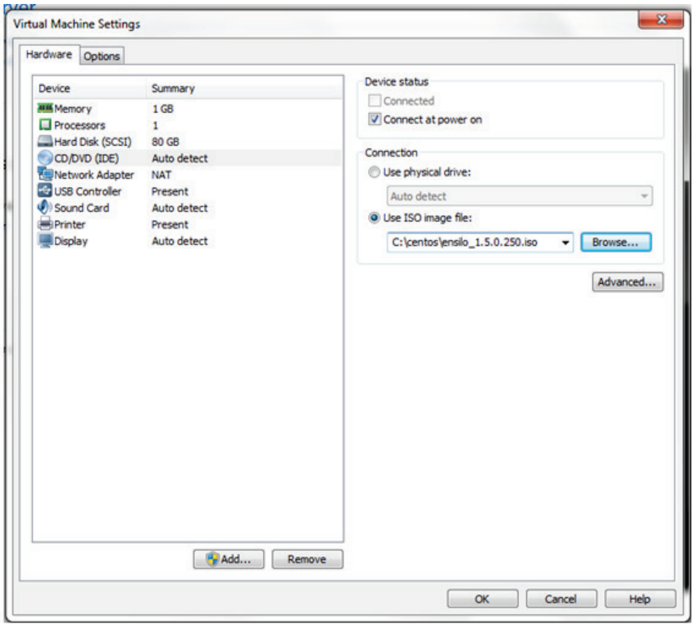
Name:	EnsiloServer
Location:	C:\VMs\Linux\centos4
Version:	Workstation 11.0
Operating System:	CentOS 64-bit
Hard Disk:	80 GB, Split
Memory:	1024 MB
Network Adapter:	NAT
Other Devices:	CD/DVD, USB Controller, Printer, Sound Card

7 Click **Finish**.

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



The following window displays:



Device	Summary
Memory	1 GB
Processors	1
Hard Disk (SCSI)	80 GB
CD/DVD (IDE)	Auto detect
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Device status

□ Connected

☑ Connect at power on

Connection

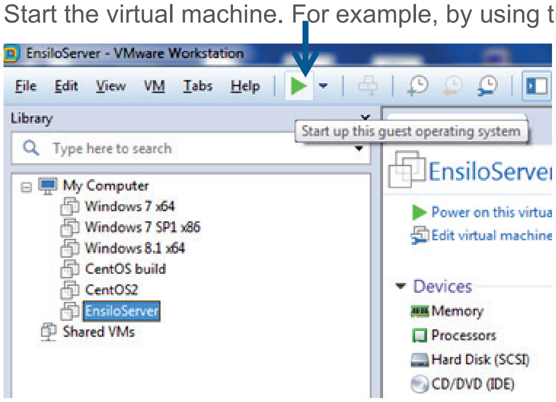
○ Use physical drive:

Auto detect

● Use ISO image file:

C:\centos\ensilo_1.5.0.250.iso

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 25.

    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 231.
- 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 234.
Note – You can get a Collector that is customized to your environment's settings, see the Requesting and Obtaining a Collector Installer section on page 181. If a custom Collector is used during the installation, all input fields such as Aggregator address and registration password are auto-filled.

Installing a FortiEDR Collector

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 79) 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:

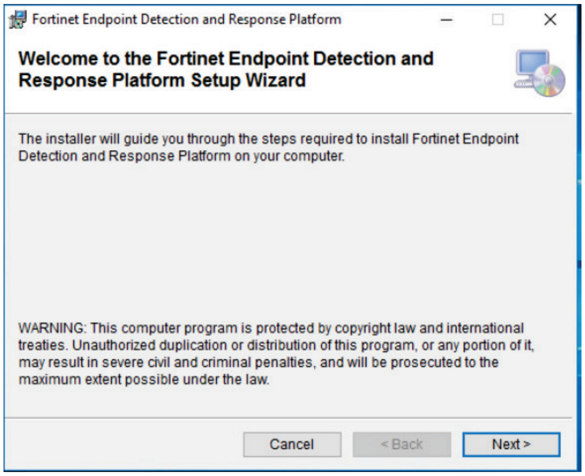
C:\Program Files\Fortinet\FortiEDR\ ➔ NsloCollectorService.exe—stop and then provide the registration password in the pop-up windows.

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:



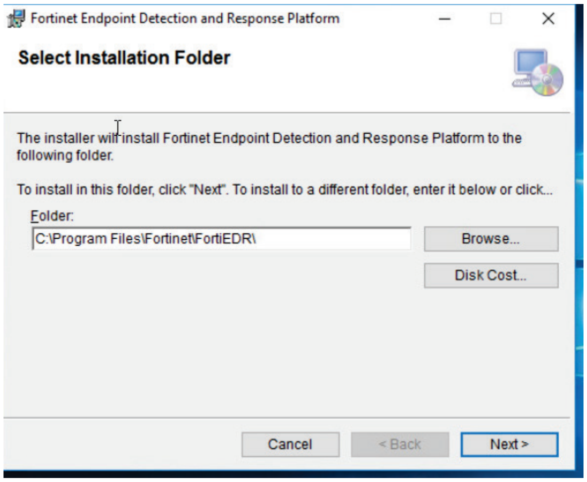
Fortinet Endpoint Detection and Response Platform

Welcome to the Fortinet Endpoint Detection and Response Platform Setup Wizard

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

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

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



Fortinet Endpoint Detection and Response Platform

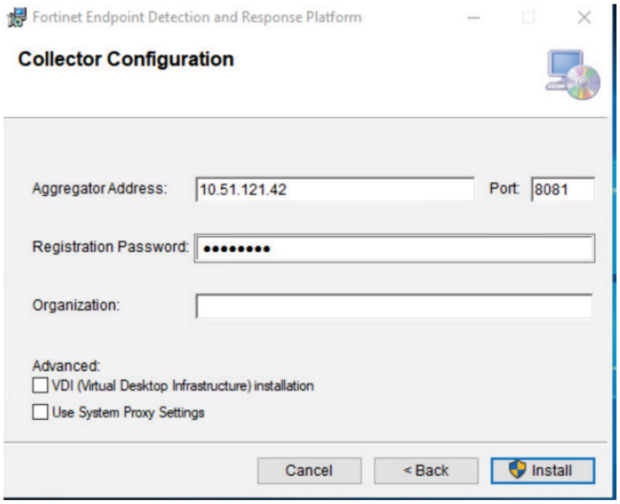
Select Installation Folder

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

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

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

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



Collector Configuration

Aggregator Address: 10.51.121.42 Port: 8081

Registration Password: ••••••••

Organization:

Advanced:

□ VDI (Virtual Desktop Infrastructure) installation

□ Use System Proxy Settings

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 26.

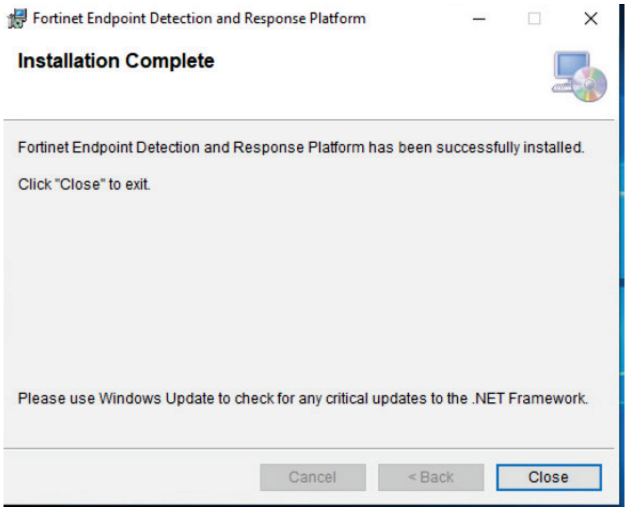
7 For a multi-organization FortiEDR system, enter the name of the organization in the **Organization** field. For more details, see the *Collector Registration* section on page 234.

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 47.

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:



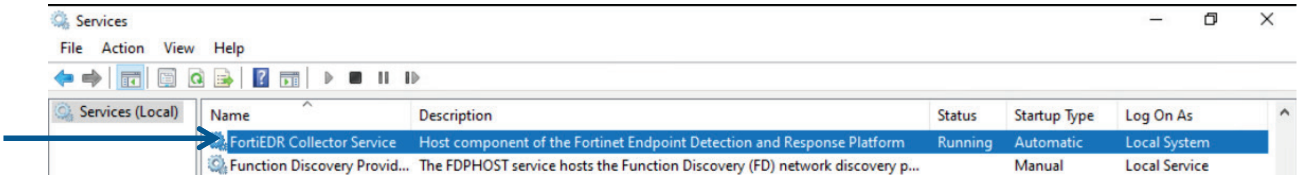
Installation Complete

Fortinet Endpoint Detection and Response Platform has been successfully installed.

Click "Close" to exit.

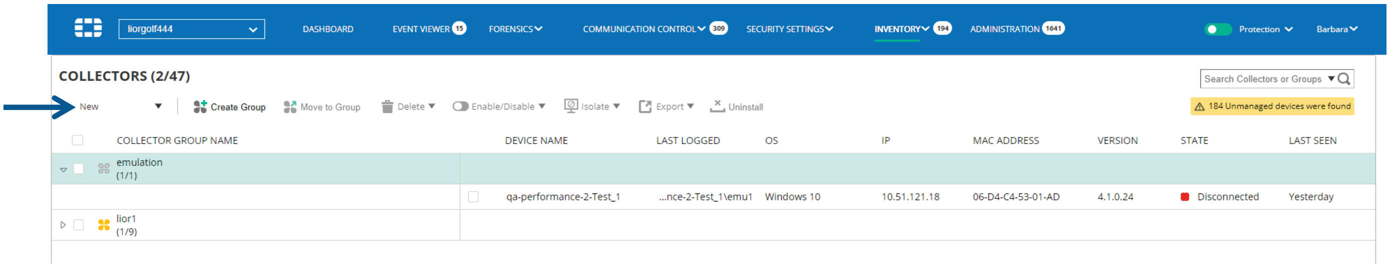
Please use Windows Update to check for any critical updates to the .NET Framework.

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



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

11 Verify that the FortiEDR Collector details are listed in the **INVENTORY** tab of the FortiEDR Central Manager console (page 74). Select the **New** filter to display a list of newly registered FortiEDR Collectors, as shown below:



COLLECTORS (2/47)

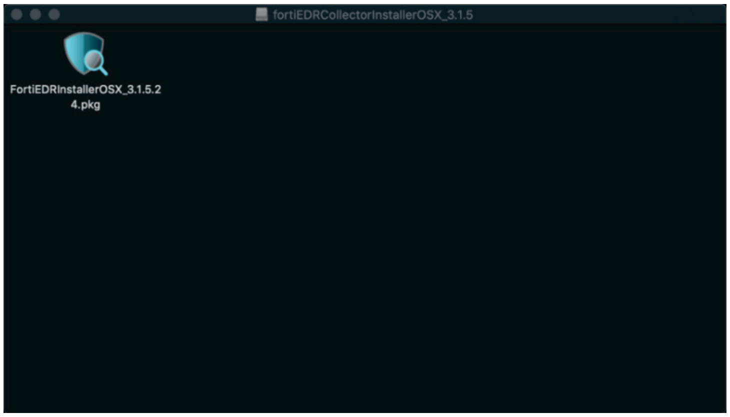
⚠ 184 Unmanaged devices were found

COLLECTOR GROUP NAME	DEVICE NAME	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	STATE	LAST SEEN
emulation (1/1)								
	qa-performance-2-Test_1	...nce-2-Test_1\emu1	Windows 10	10.51.121.18	06-D4-C4-53-01-AD	4.1.0.24	🟥 Disconnected	Yesterday
lior1 (1/9)								

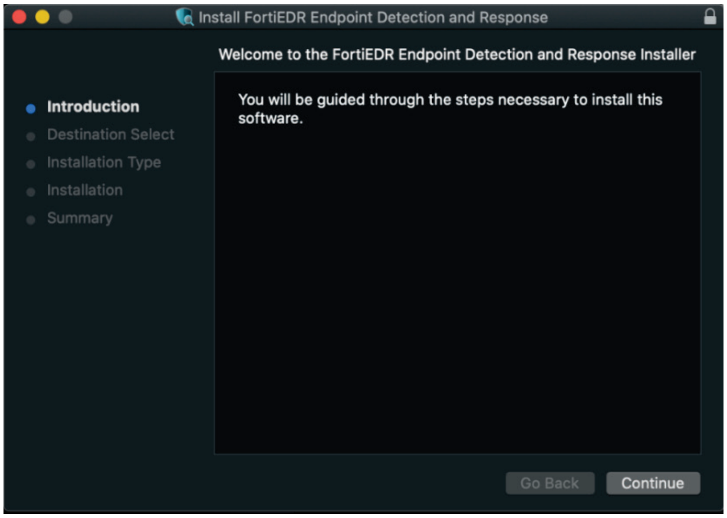
Installing a FortiEDR Collector on an Mac Operating System

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

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


fortiEDRCollectorInstallerOSX_3.1.5
FortiEDRInstallerOSX_3.1.5.2 4.pkg

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

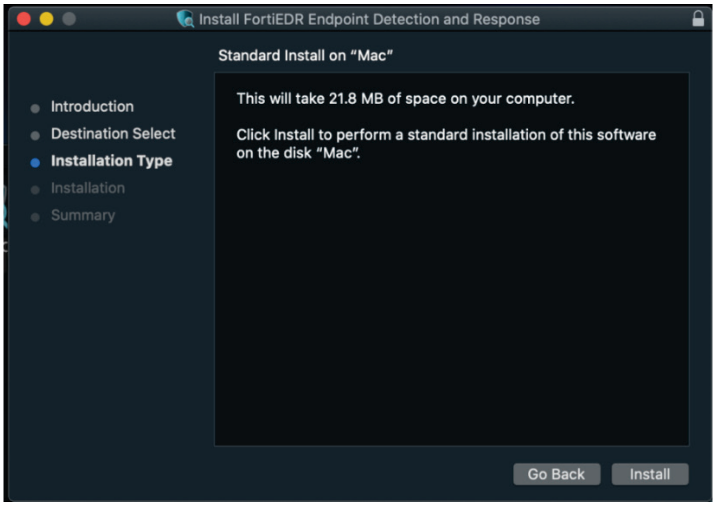


Welcome to the FortiEDR Endpoint Detection and Response Installer

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

3 Click **Continue**.

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

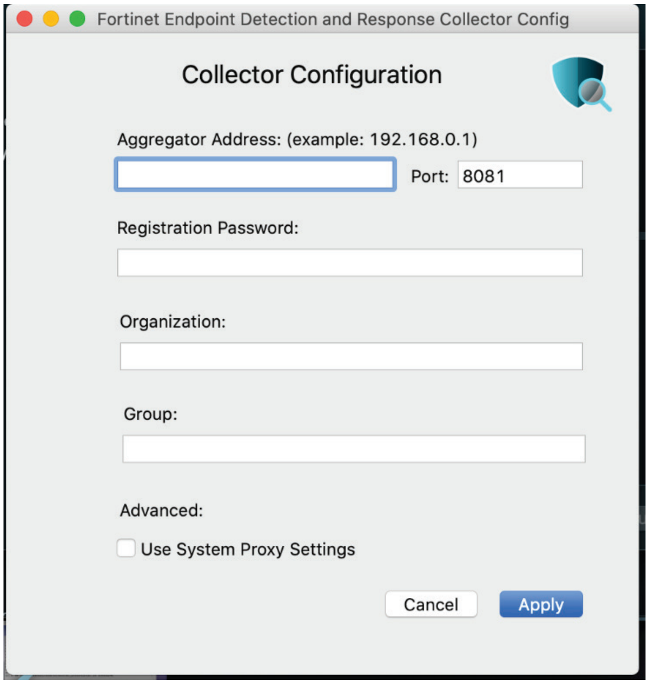


Standard Install on "Mac"

This will take 21.8 MB of space on your computer.

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

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



Fortinet Endpoint Detection and Response Collector Config

Collector Configuration

Aggregator Address: (example: 192.168.0.1)

Port: 8081

Registration Password:

Organization:

Group:

Advanced:

□ Use System Proxy Settings

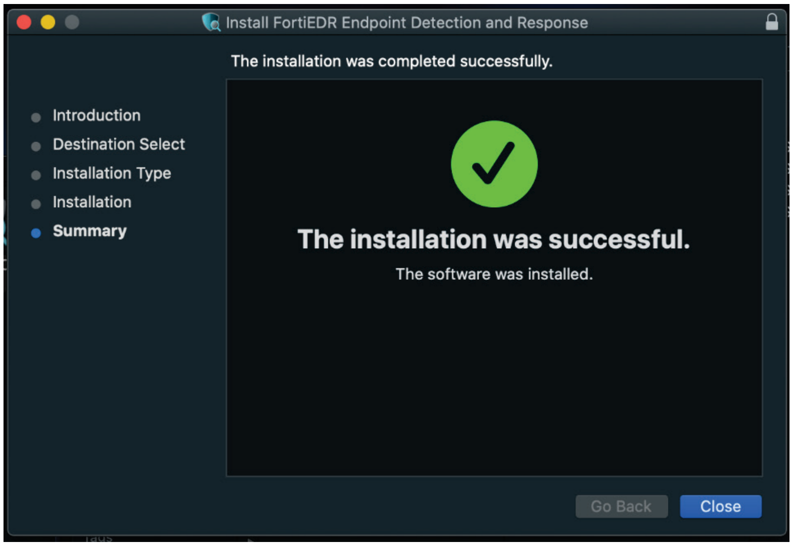
6 In the **Aggregator Address** field, enter the IP address of the Aggregator in the first box and the port of the Aggregator in the adjacent (**Port**) box.

7 In the **Registration Password** field, enter the registration password, as described on page 26.

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:



Install FortiEDR Endpoint Detection and Response

The installation was completed successfully.

The installation was successful.

The software was installed.

11 Click **Close**.

To install a FortiEDR Collector on a Mac operating system that is running with Big Sur (version 11) or above:

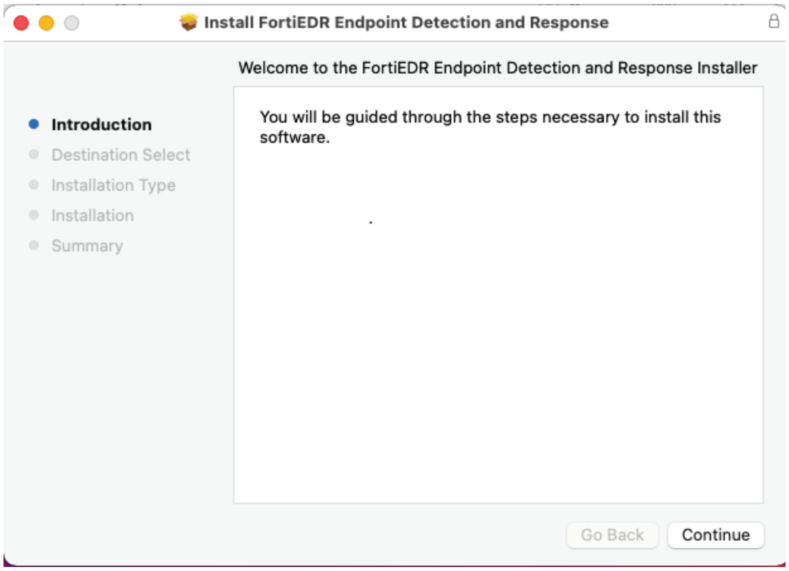
The process described below includes a description of how to allow the following upon first FortiEDR Collector installation:

- System Extensions
- Network Extensions
- Full Disk Access

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

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

1 Double-click the *.dmg file named **FortiEDRCollectorInstallerOSX_4.1.x**.dmg. The following window displays:

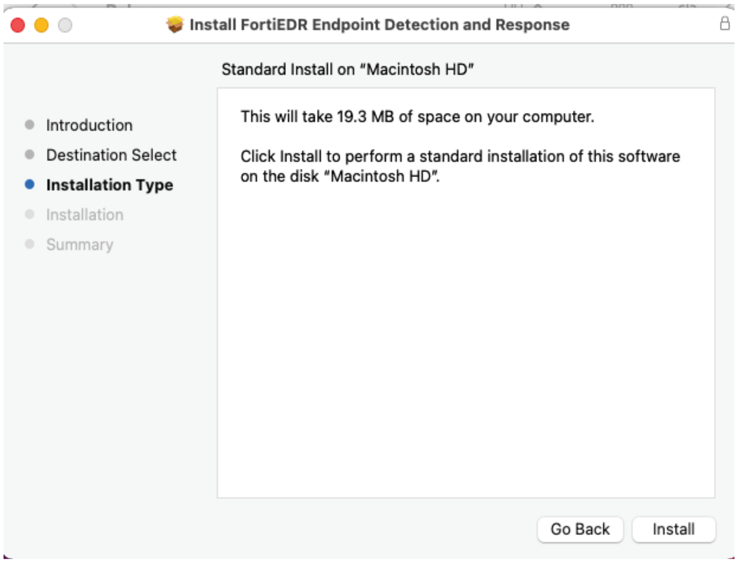


Install FortiEDR Endpoint Detection and Response

Welcome to the FortiEDR Endpoint Detection and Response Installer

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

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



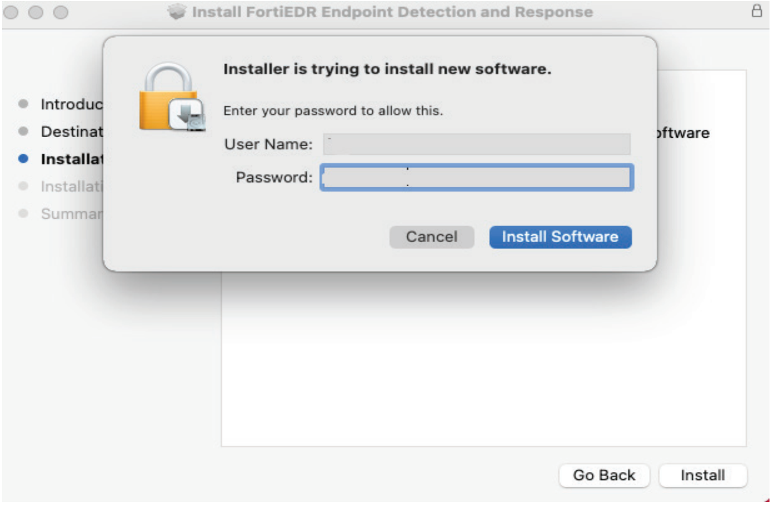
Install FortiEDR Endpoint Detection and Response

Standard Install on "Macintosh HD"

This will take 19.3 MB of space on your computer.

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

3 Click **Install**. Enter the Mac password at the prompt.



Install FortiEDR Endpoint Detection and Response

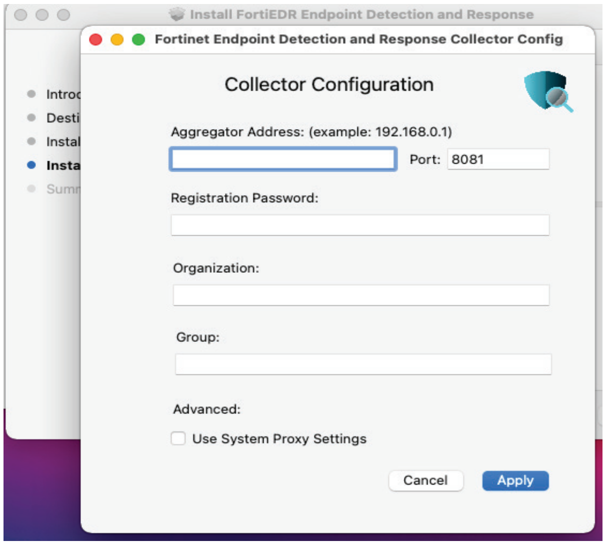
Installer is trying to install new software.

Enter your password to allow this.

User Name:

Password:

The following displays:



Install FortiEDR Endpoint Detection and Response

Fortinet Endpoint Detection and Response Collector Config

Collector Configuration

Aggregator Address: (example: 192.168.0.1)

Port: 8081

Registration Password:

Organization:

Group:

Advanced:

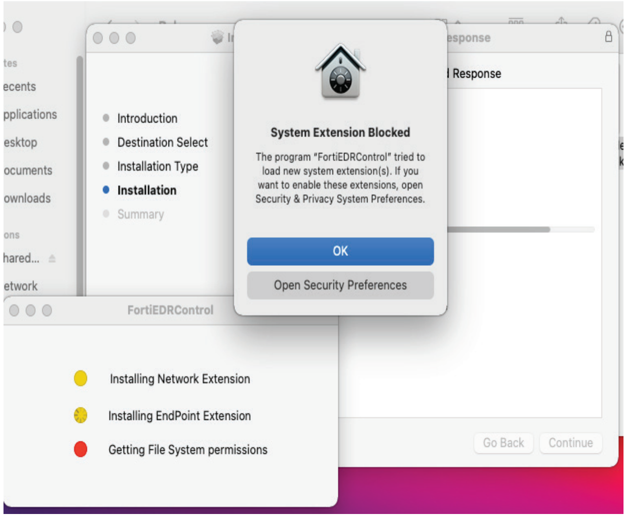
☐ Use System Proxy Settings

4 In the Collector Configuration page, specify the Aggregator’s address and FortiEDR registration password. Optionally, you can select a destination Organization and Collector Group and/or installation using a system proxy.

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

6 Perform the following during installation:

- Enable Network and System Extensions, shown below:



System Extension Blocked

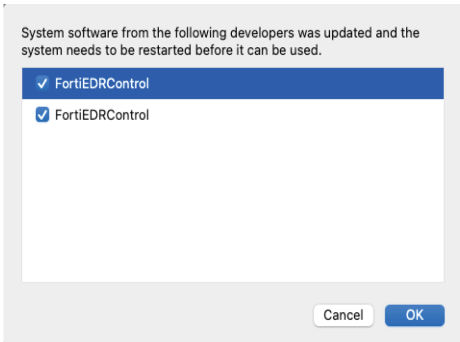
The program "FortiEDRControl" tried to load new system extension(s). If you want to enable these extensions, open Security & Privacy System Preferences.

Installing Network Extension

Installing EndPoint Extension

Getting File System permissions

  - Open Security Preferences.
  - Click the lock at the bottom of the window in order to make changes.
  - In the General tab, click Details. The following displays:



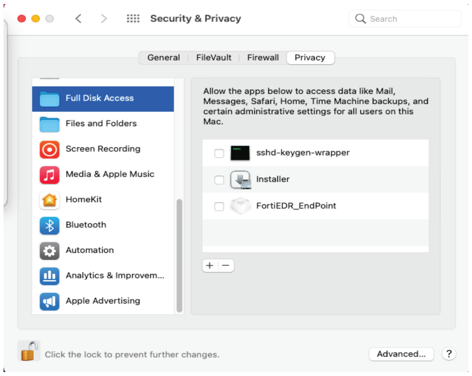
System software from the following developers was updated and the system needs to be restarted before it can be used.

☑ FortiEDRControl

☑ FortiEDRControl

  - Mark both checkboxes in order to allow FortiEDR to use Network and System Extensions.
  - Click **OK** in the System Extension Blocked window.

- Enable Full Disk Access by performing the following:
  - Open Security Preferences.
  - Click the lock at the bottom of the window in order to make changes.
  - In the **Privacy** tab, select **Full Disk Access** from the left pane.
  - Mark the checkboxes of all the applications that are displayed in the following window:



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

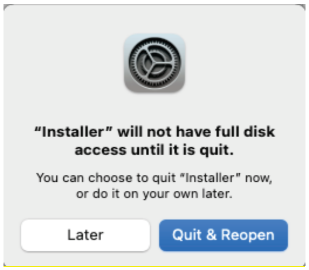
□ sshd-keygen-wrapper

□ Installer

□ FortiEDR_EndPoint

Click the lock to prevent further changes.

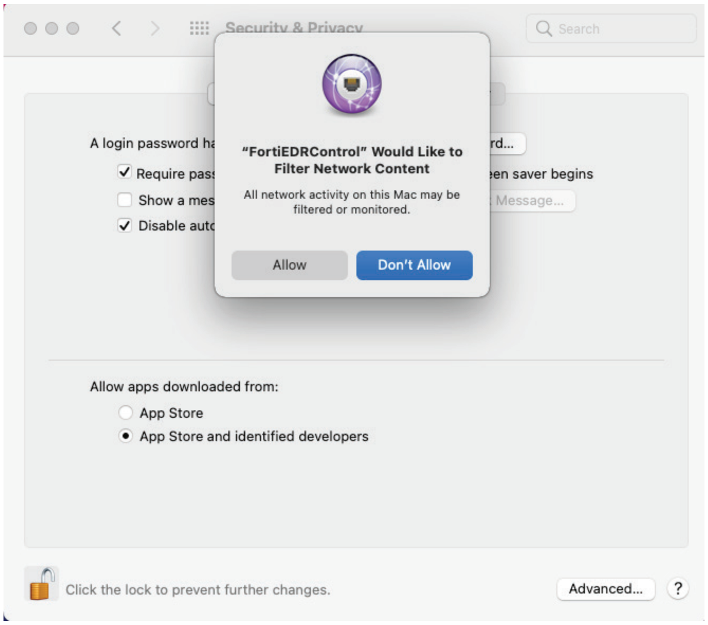
7 In the popup window, click **Later**.



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

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

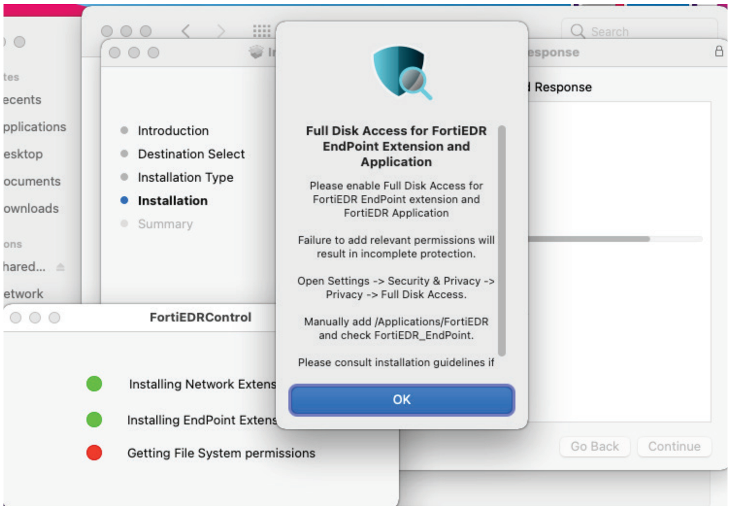
The following displays:



"FortiEDRControl" Would Like to Filter Network Content

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

8 Click **Allow**. The following displays:



Full Disk Access for FortiEDR EndPoint Extension and Application

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

Failure to add relevant permissions will result in incomplete protection.

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

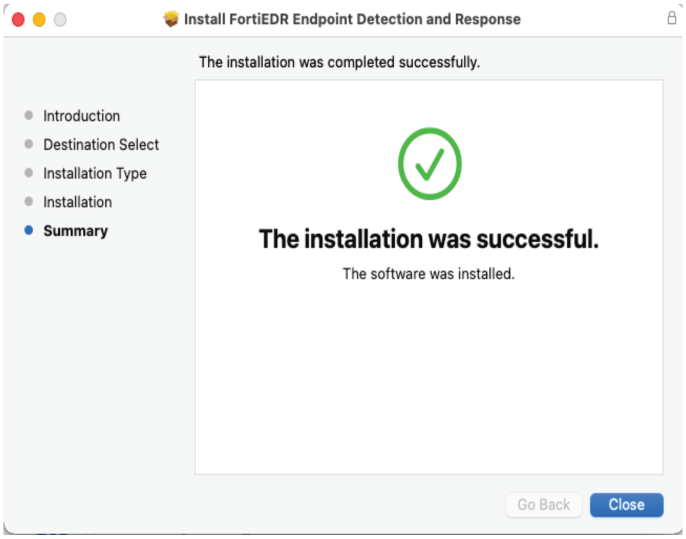
Manually add /Applications/FortiEDR and check FortiEDR_EndPoint.

Please consult installation guidelines if

FortiEDRControl

- Installing Network Extens
- Installing EndPoint Extens
- Getting File System permissions

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



Install FortiEDR Endpoint Detection and Response

The installation was completed successfully.

The installation was successful.

The software was installed.

10 Click **Close** to complete the process.

11 Reboot the device.

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 26.

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 34.

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 78) 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 custom FortiEDR Collector installer, which can be accessed via the Central Manager Console using the required DNS or IP address and password that is already embedded inside. For more details, see the *Requesting and Obtaining a Collector Installer* section on page 181.

Automated FortiEDR Collector Deployment on Mac

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

1 Get a pre-populated customized Collector installer for macOS as described on section Requesting and Obtaining a Collector Installer on page 181.

2 Run the following command in order to install using the specified settings:

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

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

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

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

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
```

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 36.

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 36.

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

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

- 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'`.

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

- /Applications/FortiEDR.app/fortiedr_uninstaller.sh REGISTRATION PASSWORD

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_Management_Agg__5.0.x.y.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 FortiEDRInstaller_Management_Agg__5.0.x.y.x
   ```

3. Run the upgrade, as shown below:

   ```
   [root@dan ~]# ./ FortiEDRInstaller_Management_Agg__5.0.x.y.x
   ```

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

   ```
   FortiEDR installation 5.0.x.y finished successfully
   [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 49.

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 28.
- 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.

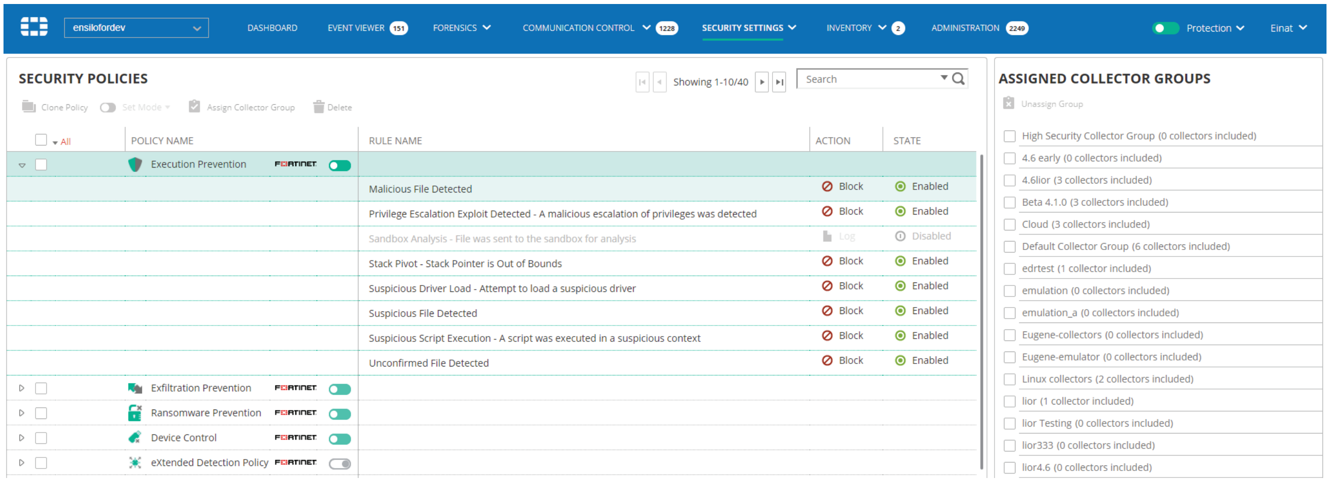
Out-of-the-box Policies

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.
- **Extended Detection Policy:** This policy provides visibility into data across multiple security systems and identifies abnormal or malicious activity by applying analytics and correlating data from various systems. This policy requires that you configure an XDR source connector in the **ADMINISTRATION ➔ INTEGRATIONS** section. This feature is a license-dependent add-on. You may contact Fortinet support for more information.

  Note – The Extended Detection policy provides detection features (meaning that events are logged and displayed in the Event Viewer). No blocking options are provided. The exceptions and forensics options are not available in the Event Viewer for security events triggered by the Extended Detection policy.
- **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.



SECURITY POLICIES

All	POLICY NAME	RULE NAME	ACTION	STATE
▽ □	Execution Prevention FORTINET			
		Malicious File Detected	Block	Enabled
		Privilege Escalation Exploit Detected - A malicious escalation of privileges was detected	Block	Enabled
		Sandbox Analysis - File was sent to the sandbox for analysis	Log	Disabled
		Stack Pivot - Stack Pointer is Out of Bounds	Block	Enabled
		Suspicious Driver Load - Attempt to load a suspicious driver	Block	Enabled
		Suspicious File Detected	Block	Enabled
		Suspicious Script Execution - A script was executed in a suspicious context	Block	Enabled
		Unconfirmed File Detected	Block	Enabled
▷ □	Exfiltration Prevention FORTINET			
▷ □	Ransomware Prevention FORTINET			
▷ □	Device Control FORTINET			
▷ □	eXtended Detection Policy FORTINET			

ASSIGNED COLLECTOR GROUPS

□ High Security Collector Group (0 collectors included)
□ 4.6 early (0 collectors included)
□ 4.6lior (3 collectors included)
□ Beta 4.1.0 (3 collectors included)
□ Cloud (3 collectors included)
□ Default Collector Group (6 collectors included)
□ edrtest (1 collector included)
□ emulation (0 collectors included)
□ emulation_a (0 collectors included)
□ Eugene-collectors (0 collectors included)
□ Eugene-emulator (0 collectors included)
□ Linux collectors (2 collectors included)
□ lior (1 collector included)
□ lior Testing (0 collectors included)
□ lior333 (0 collectors included)
□ lior4.6 (0 collectors included)

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, Execution Prevention and eXtended Detection security policies can run simultaneously.

Note – When multiple security policies are used, they do not generate duplicate security 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.
- An eXtended Detection rule violation is detected when malicious activity is identified across network, endpoints and cloud.

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

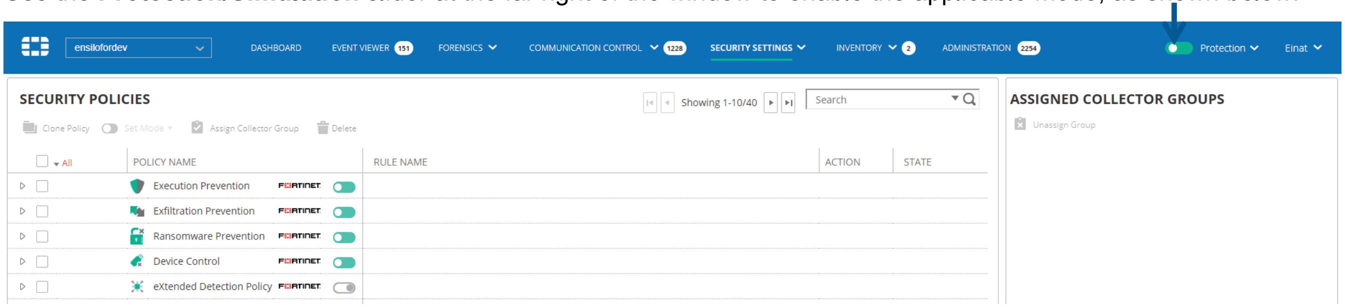
Protection or Simulation Mode

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:

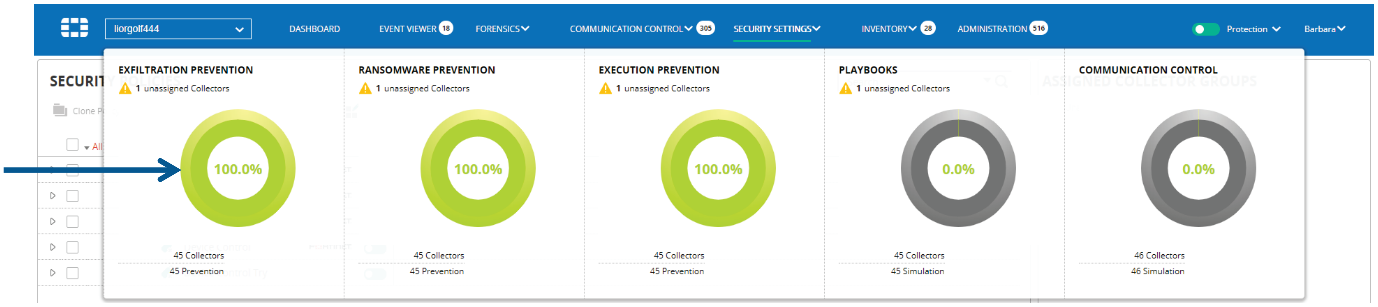


SECURITY POLICIES

All	POLICY NAME		RULE NAME	ACTION	STATE
▷ □	Execution Prevention	FORTINET			
▷ □	Exfiltration Prevention	FORTINET			
▷ □	Ransomware Prevention	FORTINET			
▷ □	Device Control	FORTINET			
▷ □	eXtended Detection Policy	FORTINET			

ASSIGNED COLLECTOR GROUPS

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



EXFILTRATION PREVENTION
1 unassigned Collectors
100.0%
45 Collectors
45 Prevention

RANSOMWARE PREVENTION
1 unassigned Collectors
100.0%
45 Collectors
45 Prevention

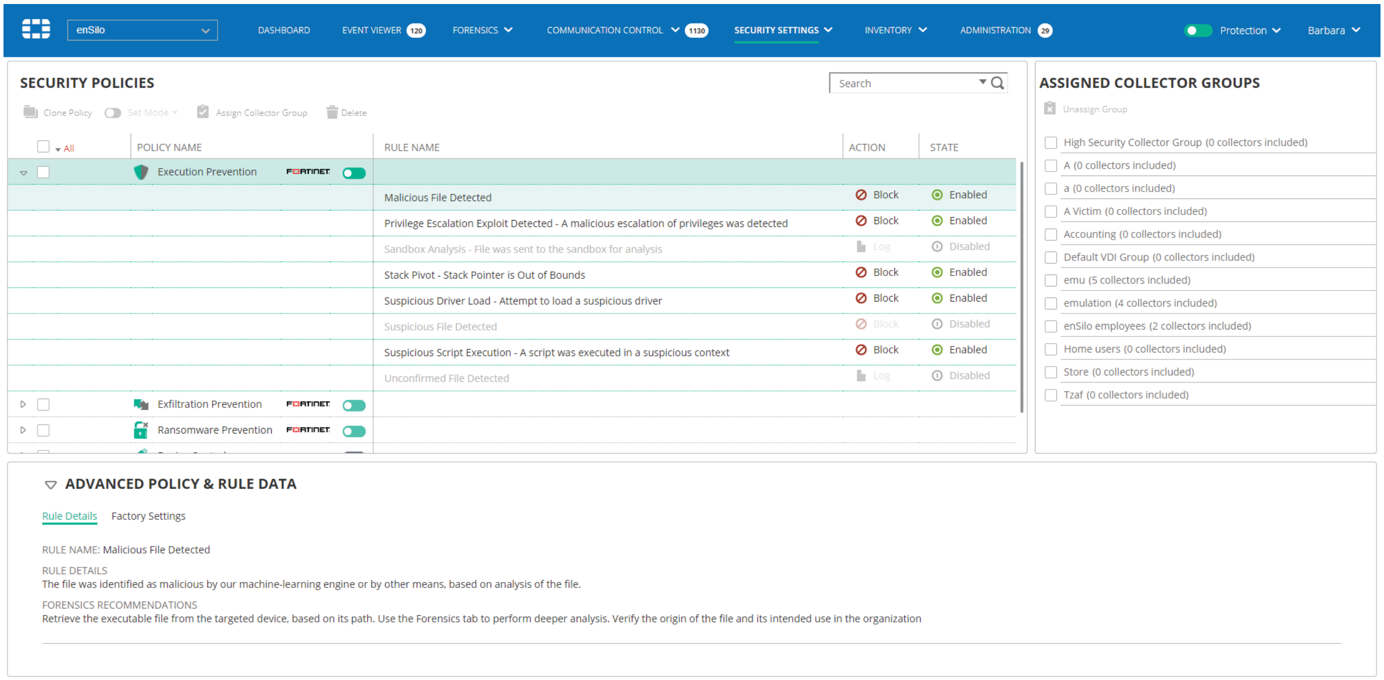
EXECUTION PREVENTION
1 unassigned Collectors
100.0%
45 Collectors
45 Prevention

PLAYBOOKS
1 unassigned Collectors
0.0%
45 Collectors
45 Simulation

COMMUNICATION CONTROL
0.0%
46 Collectors
46 Simulation

Security Policies Page

The **SECURITY POLICIES** page displays a row for each security policy. Each policy row can be expanded to show the rules that it contains, as shown below. To access this page, click the down arrow next to **SECURITY SETTINGS** and then select **Security Policies**.



SECURITY POLICIES

□ All	POLICY NAME	RULE NAME	ACTION	STATE
□	Execution Prevention FORTINET			
		Malicious File Detected	⊘ Block	◉ Enabled
		Privilege Escalation Exploit Detected - A malicious escalation of privileges was detected	⊘ Block	◉ Enabled
		Sandbox Analysis - File was sent to the sandbox for analysis	Log	ⓘ Disabled
		Stack Pivot - Stack Pointer is Out of Bounds	⊘ Block	◉ Enabled
		Suspicious Driver Load - Attempt to load a suspicious driver	⊘ Block	◉ Enabled
		Suspicious File Detected	⊘ Block	ⓘ Disabled
		Suspicious Script Execution - A script was executed in a suspicious context	⊘ Block	◉ Enabled
		Unconfirmed File Detected	Log	ⓘ Disabled
□	Exfiltration Prevention FORTINET			
□	Ransomware Prevention FORTINET			

ASSIGNED COLLECTOR GROUPS

- □ High Security Collector Group (0 collectors included)
- □ A (0 collectors included)
- □ a (0 collectors included)
- □ A Victim (0 collectors included)
- □ Accounting (0 collectors included)
- □ Default VDI Group (0 collectors included)
- □ emu (5 collectors included)
- □ emulation (4 collectors included)
- □ enSilo employees (2 collectors included)
- □ Home users (0 collectors included)
- □ Store (0 collectors included)
- □ Tzaf (0 collectors included)

ADVANCED POLICY & RULE DATA

Rule Details Factory Settings

RULE NAME: Malicious File Detected

RULE DETAILS
The file was identified as malicious by our machine-learning engine or by other means, based on analysis of the file.

FORENSICS RECOMMENDATIONS
Retrieve the executable file from the targeted device, based on its path. Use the Forensics tab to perform deeper analysis. Verify the origin of the file and its intended use in the organization

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, device control policies are marked with the icon and extended detection policies are marked with the icon.

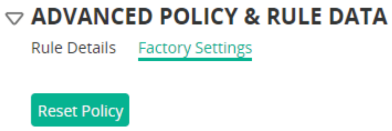
The following information is defined per security policy:

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 54), 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:



▽ ADVANCED POLICY & RULE DATA

Rule Details   Factory Settings

Reset Policy

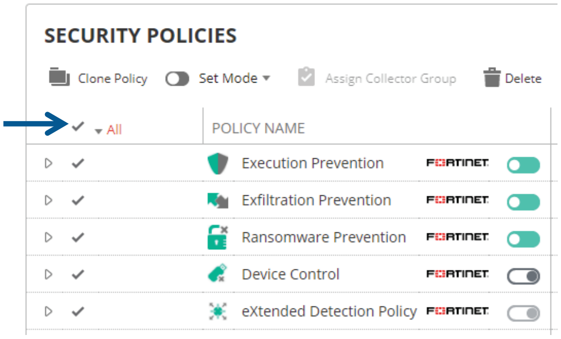
Setting a Security Policy's Prevention or Simulation Mode

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

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

To set a security policy to Prevention or Simulation mode:

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



SECURITY POLICIES

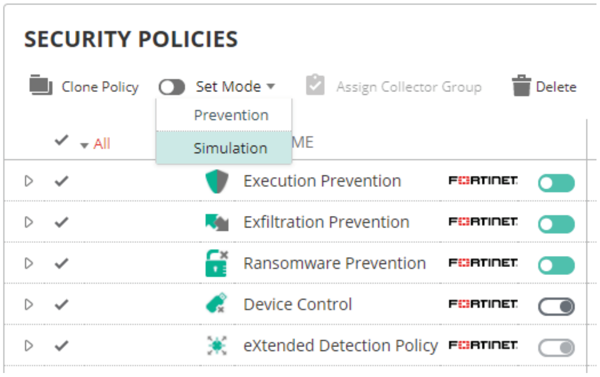
Clone Policy   Set Mode ▾   Assign Collector Group   Delete

	✓ ▾ All	POLICY NAME		
▷	✓	Execution Prevention	FORTINET	●
▷	✓	Exfiltration Prevention	FORTINET	●
▷	✓	Ransomware Prevention	FORTINET	●
▷	✓	Device Control	FORTINET	○
▷	✓	eXtended Detection Policy	FORTINET	○

2 You can now either:

- ○ Set mode : Click 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:



SECURITY POLICIES

Clone Policy   Set Mode ▾   Assign Collector Group   Delete

Prevention

Simulation

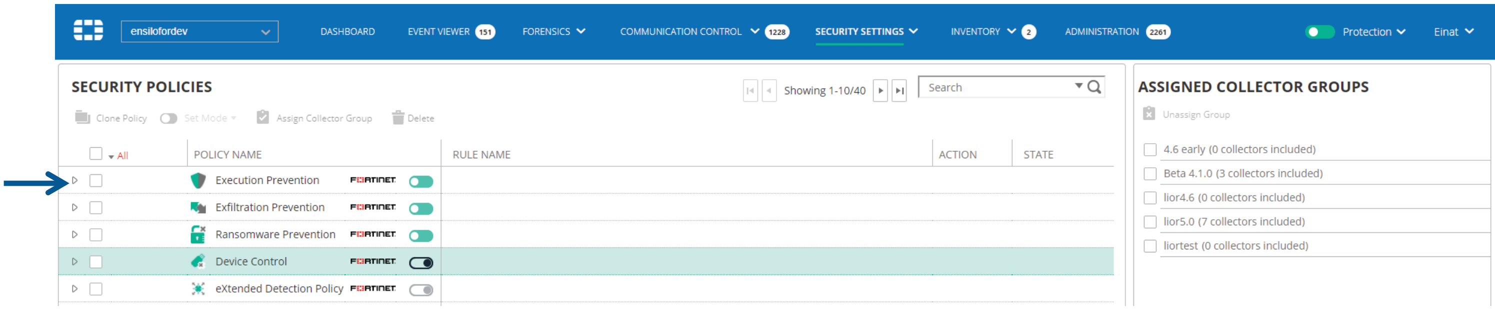
	✓ ▾ All	ME		
▷	✓	Execution Prevention	FORTINET	●
▷	✓	Exfiltration Prevention	FORTINET	●
▷	✓	Ransomware Prevention	FORTINET	●
▷	✓	Device Control	FORTINET	○
▷	✓	eXtended Detection Policy	FORTINET	○

Creating a New Security Policy

A new security policy can be created by cloning an existing policy, as described below. New security policies are only needed if you are going to assign different policies to different Collector Groups. Otherwise, you can simply modify one of the default policies that are provided out-of-the-box and apply it to all FortiEDR Collectors by default. Modifications made on one security policy do not affect any other policies

To create a new security policy:

1 In the **SECURITY POLICIES** page, check the checkbox of the security policy to be cloned. The buttons at the top of the window then become active.



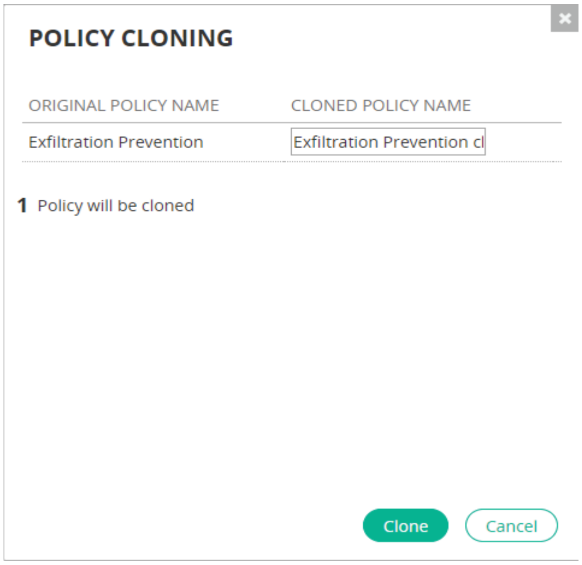
SECURITY POLICIES

□ All	POLICY NAME		RULE NAME	ACTION	STATE
▷ □	Execution Prevention	FORTINET			
▷ □	Exfiltration Prevention	FORTINET			
▷ □	Ransomware Prevention	FORTINET			
▷ □	Device Control	FORTINET			
▷ □	eXtended Detection Policy	FORTINET			

ASSIGNED COLLECTOR GROUPS

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

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



POLICY CLONING

ORIGINAL POLICY NAME	CLONED POLICY NAME
Exfiltration Prevention	Exfiltration Prevention cl

1 Policy will be cloned

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

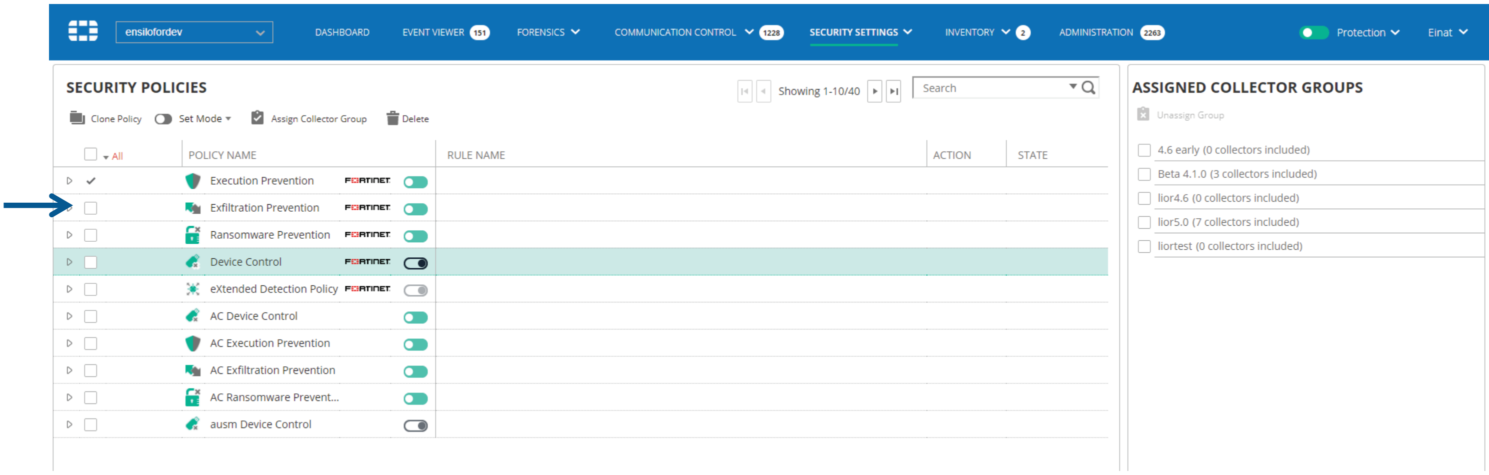
By default, a security policy protects the FortiEDR Collectors that belong to that Collector Group. A security policy can be assigned to more than one Collector Group. Multiple security policies can be assigned to each Collector Group.

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

You may refer to page 78 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.



SECURITY POLICIES

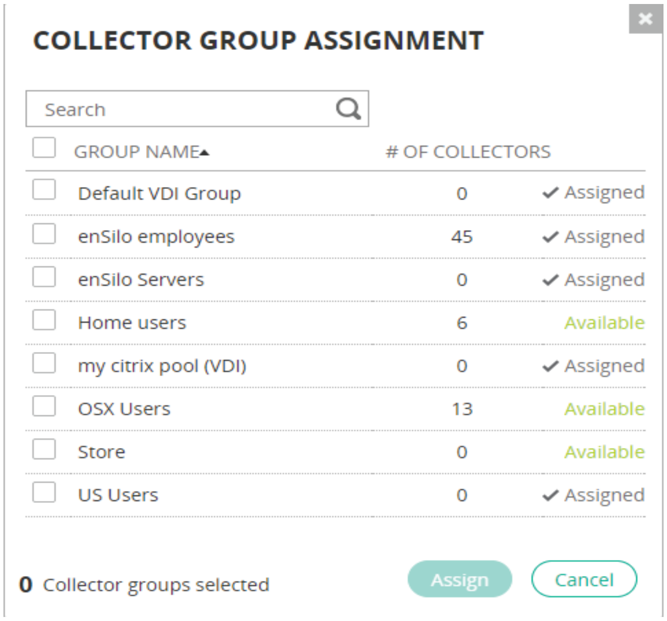
☐ All	POLICY NAME		RULE NAME	ACTION	STATE
✓	Execution Prevention	FORTINET			
☐	Exfiltration Prevention	FORTINET			
☐	Ransomware Prevention	FORTINET			
☐	Device Control	FORTINET			
☐	eXtended Detection Policy	FORTINET			
☐	AC Device Control				
☐	AC Execution Prevention				
☐	AC Exfiltration Prevention				
☐	AC Ransomware Prevent...				
☐	ausm Device Control				

ASSIGNED COLLECTOR GROUPS

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

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

Click the ☑ Assign Collector Group toolbar button, which displays the following window in which you can select the Collector Groups to which to assign this policy.



COLLECTOR GROUP ASSIGNMENT

☐	GROUP NAME▴	# OF COLLECTORS	
☐	Default VDI Group	0	✓ Assigned
☐	enSilo employees	45	✓ Assigned
☐	enSilo Servers	0	✓ Assigned
☐	Home users	6	Available
☐	my citrix pool (VDI)	0	✓ Assigned
☐	OSX Users	13	Available
☐	Store	0	Available
☐	US Users	0	✓ Assigned

0 Collector groups selected

The **ASSIGNED COLLECTORS GROUPS** area lists all the Collector Groups that have been assigned a security policy to protect them. You can also simply drag-and-drop a Collector Group from this list onto a policy in the left pane of this window to assign the Collector Group to be protected by that policy.

Deleting a Security Policy

To delete a security policy:

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

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

Playbook Policies

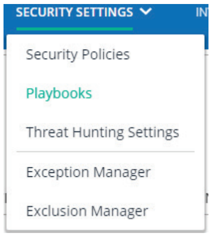
The FortiEDR Playbooks feature determines which automatic actions are triggered, based on the classification of a security event (for details about security event classification, see page 120). Playbook policies enable administrators to preconfigure the action(s) to be automatically executed according to a security event's classification. Typically, Playbook policies only need be configured once, and can be modified thereafter, if needed. FortiEDR classifies each security event into one of five Categories described on page 101.

FortiEDR provides the following Playbook policy out of the box:

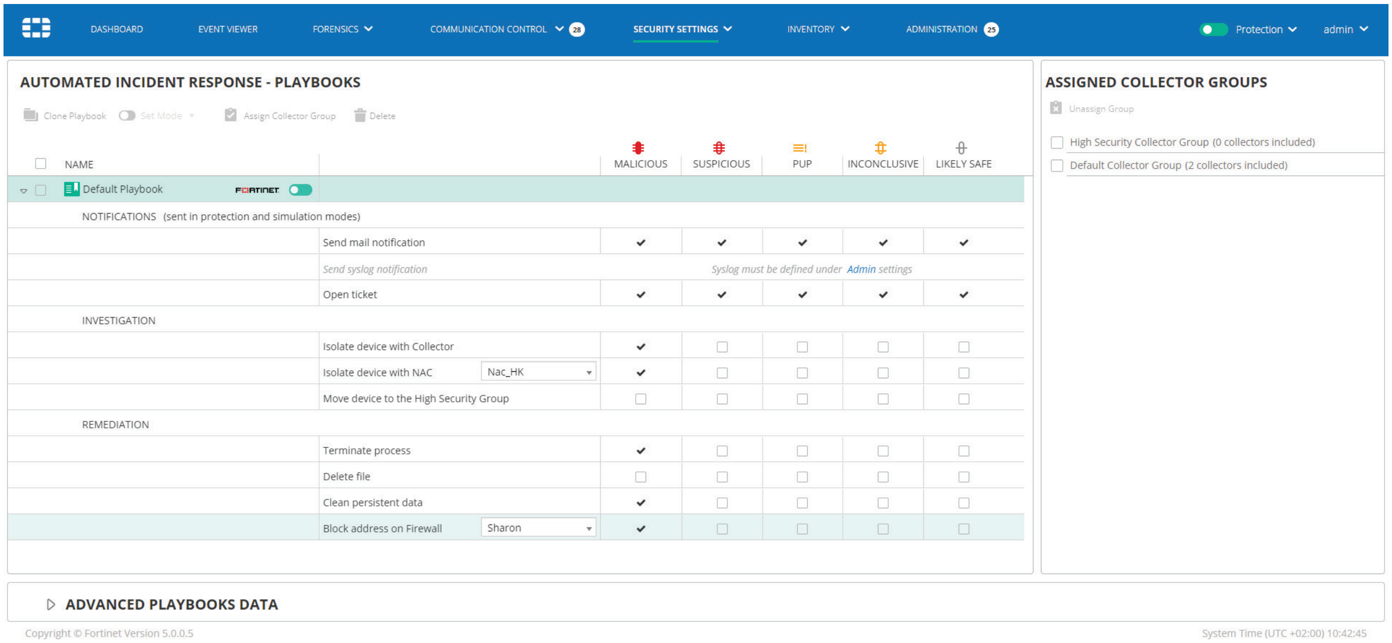
- **Default Playbook:** This Playbook policy specifies the default actions for the Collector Groups assigned to the policy. By default, all Collector Groups are assigned to this policy.

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:



AUTOMATED INCIDENT RESPONSE - PLAYBOOKS

NAME			MALICIOUS	SUSPICIOUS	PUP	INCONCLUSIVE	LIKELY SAFE
Default Playbook							
NOTIFICATIONS (sent in protection and simulation modes)							
	Send mail notification		✓	✓	✓	✓	✓
	Send syslog notification			*Syslog must be defined under Admin settings*			
	Open ticket		✓	✓	✓	✓	✓
INVESTIGATION							
	Isolate device with Collector		✓	□	□	□	□
	Isolate device with NAC	Nac_HK	✓	□	□	□	□
	Move device to the High Security Group		□	□	□	□	□
REMEDIATION							
	Terminate process		✓	□	□	□	□
	Delete file		□	□	□	□	□
	Clean persistent data		✓	□	□	□	□
	Block address on Firewall	Sharon	✓	□	□	□	□

ASSIGNED COLLECTOR GROUPS

□ High Security Collector Group (0 collectors included)

□ Default Collector Group (2 collectors included)

Copyright © Fortinet Version 5.0.0.5

System Time (UTC +02:00) 10:42:45

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

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.
Note – Automatic Incident Response Playbook features can also be triggered by extended detection events when follow-up actions are configured for the Collector Group of a device on which the event triggered. This enables the system to follow up upon the detection of such an event and execute a sequence of actions, such as to block an address on a firewall or to isolate the device in which part of the event occurred.

Assigned Collector Groups

The Assigned Collector Groups pane on the right lists the various Collector Groups in the system. By default, all Collector Groups are assigned to the Default Playbook policy. You can reassign one or more Collector Groups to different Playbook policies, if preferred.

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

Cloning a Playbook Policy

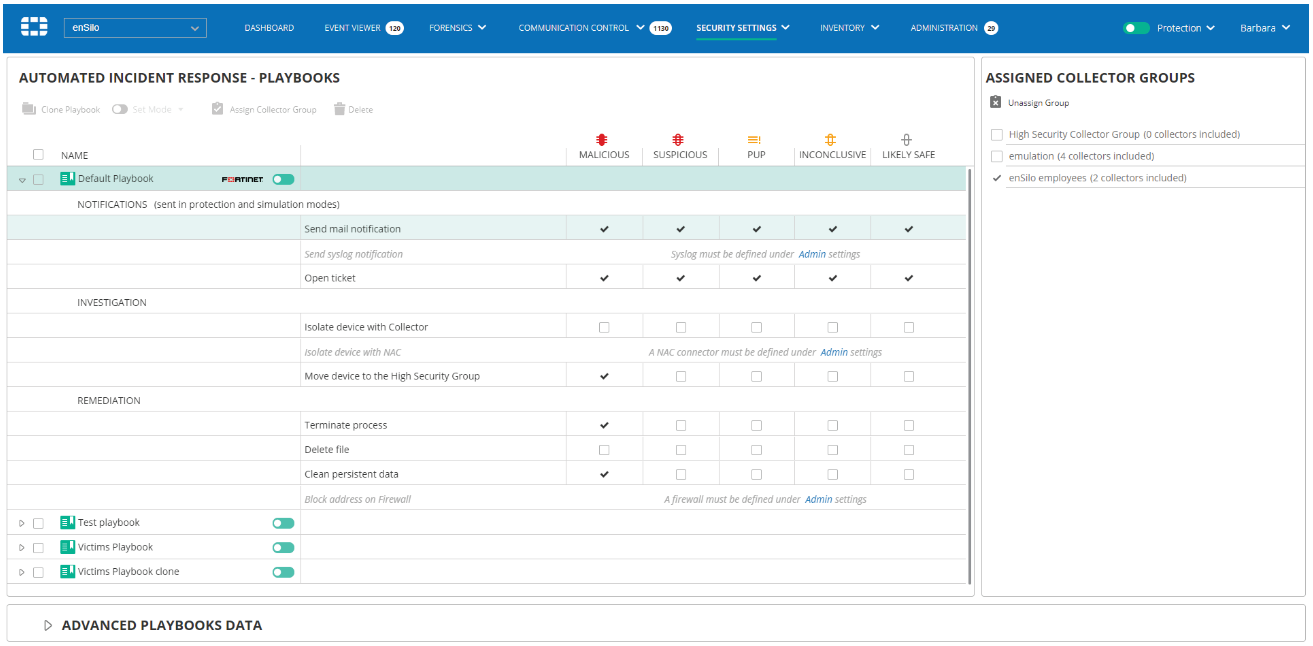
Cloning a Playbook policy unassigns the policy from one Collector Group and then reassigns it to a different Collector Group. A Collector Group can only be assigned to one Playbook policy.

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.



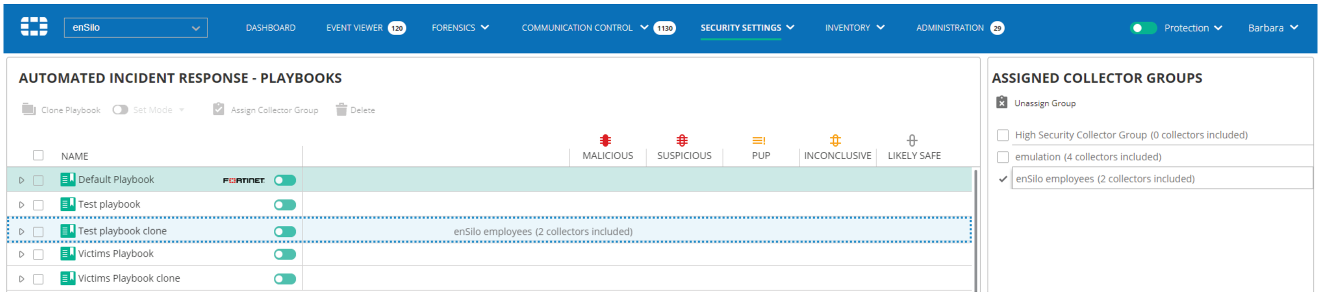
AUTOMATED INCIDENT RESPONSE - PLAYBOOKS

NAME		MALICIOUS	SUSPICIOUS	PUP	INCONCLUSIVE	LIKELY SAFE
▽ □ Default Playbook FORTINET						
NOTIFICATIONS (sent in protection and simulation modes)						
	Send mail notification	✓	✓	✓	✓	✓
	Send syslog notification	*Syslog must be defined under Admin settings*				
	Open ticket	✓	✓	✓	✓	✓
INVESTIGATION						
	Isolate device with Collector	□	□	□	□	□
	Isolate device with NAC	*A NAC connector must be defined under Admin settings*				
	Move device to the High Security Group	✓	□	□	□	□
REMEDIATION						
	Terminate process	✓	□	□	□	□
	Delete file	□	□	□	□	□
	Clean persistent data	✓	□	□	□	□
	Block address on Firewall	*A firewall must be defined under Admin settings*				
▷ □ Test playbook						
▷ □ Victims Playbook						
▷ □ Victims Playbook clone						

ASSIGNED COLLECTOR GROUPS

□ High Security Collector Group (0 collectors included)
□ emulation (4 collectors included)
✓ enSilo employees (2 collectors included)

- 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:



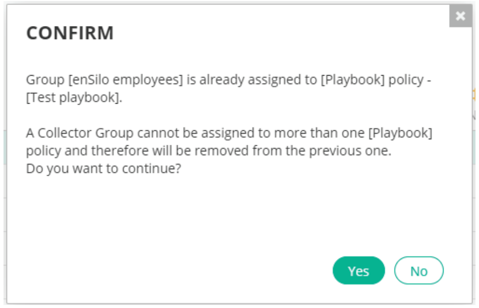
AUTOMATED INCIDENT RESPONSE - PLAYBOOKS

NAME		MALICIOUS	SUSPICIOUS	PUP	INCONCLUSIVE	LIKELY SAFE
▷ □ Default Playbook FORTINET						
▷ □ Test playbook						
▷ □ Test playbook clone	enSilo employees (2 collectors included)					
▷ □ Victims Playbook						
▷ □ Victims Playbook clone						

ASSIGNED COLLECTOR GROUPS

□ High Security Collector Group (0 collectors included)
□ emulation (4 collectors included)
✓ enSilo employees (2 collectors included)

The following message displays.



CONFIRM

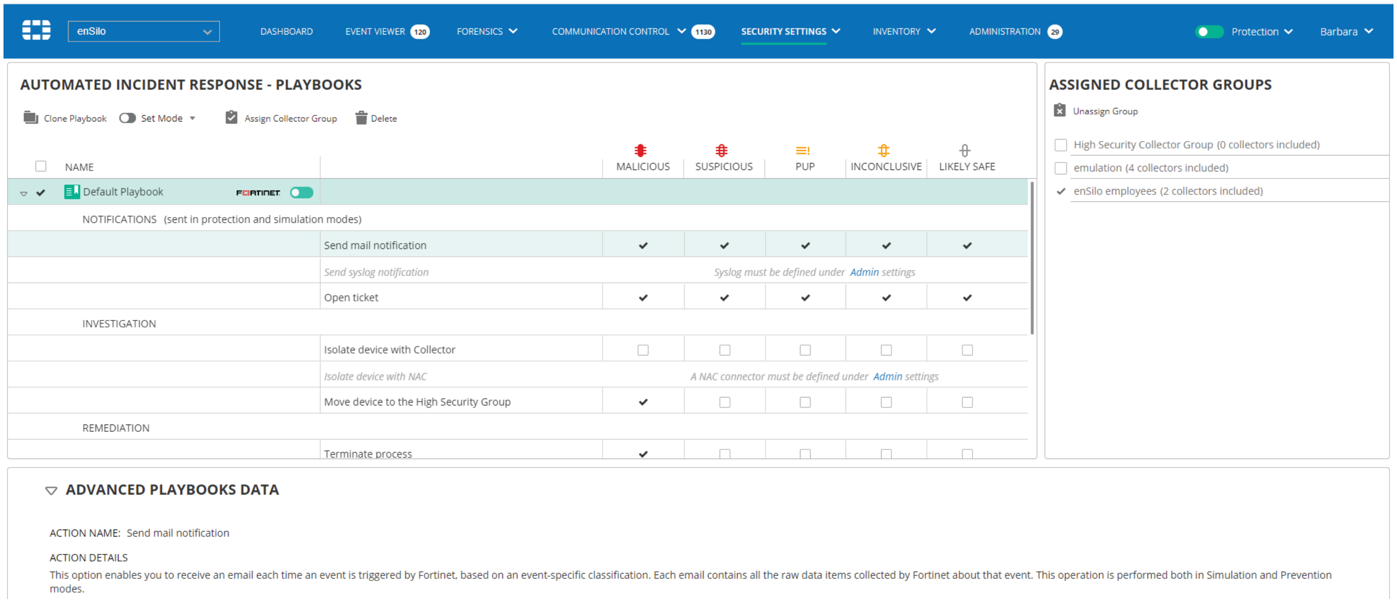
Group [enSilo employees] is already assigned to [Playbook] policy - [Test playbook].

A Collector Group cannot be assigned to more than one [Playbook] policy and therefore will be removed from the previous one.
Do you want to continue?

Click **Yes**.

Advanced Playbooks Data

The Advanced Playbooks Data area at the bottom of the **AUTOMATED INCIDENT RESPONSE – PLAYBOOKS** page displays more details about the action selected in the Playbook Policy list.



AUTOMATED INCIDENT RESPONSE - PLAYBOOKS

NAME		MALICIOUS	SUSPICIOUS	PUP	INCONCLUSIVE	LIKELY SAFE
Default Playbook						
NOTIFICATIONS (sent in protection and simulation modes)						
	Send mail notification	✓	✓	✓	✓	✓
	Send syslog notification	*Syslog must be defined under Admin settings*				
	Open ticket	✓	✓	✓	✓	✓
INVESTIGATION						
	Isolate device with Collector	□	□	□	□	□
	Isolate device with NAC	*A NAC connector must be defined under Admin settings*				
	Move device to the High Security Group	✓	□	□	□	□
REMEDIATION						
	Terminate process	✓	□	□	□	□

ASSIGNED COLLECTOR GROUPS

- □ High Security Collector Group (0 collectors included)
- □ emulation (4 collectors included)
- ✓ enSilo employees (2 collectors included)

ADVANCED PLAYBOOKS DATA

ACTION NAME: Send mail notification

ACTION DETAILS
This option enables you to receive an email each time an event is triggered by Fortinet, based on an event-specific classification. Each email contains all the raw data items collected by Fortinet about that event. This operation is performed both in Simulation and Prevention modes.

Playbook Policy Actions

Playbook policy actions are divided into the following types:

- **Notifications,** page 60
- **Investigation,** page 62
- **Remediation,** page 63

Each of these Categories contains different types of actions that can be performed when a security event is triggered.

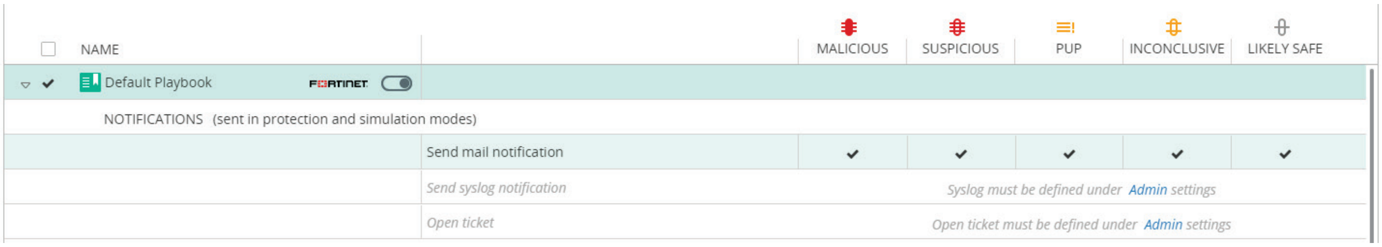
Notifications

Notification actions send a notification when a relevant security event is triggered. These actions are implemented in both FortiEDR modes (Simulation and Prevention).

Notifications can be one of the following types:

- Emails
- Syslog
- Open Ticket

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

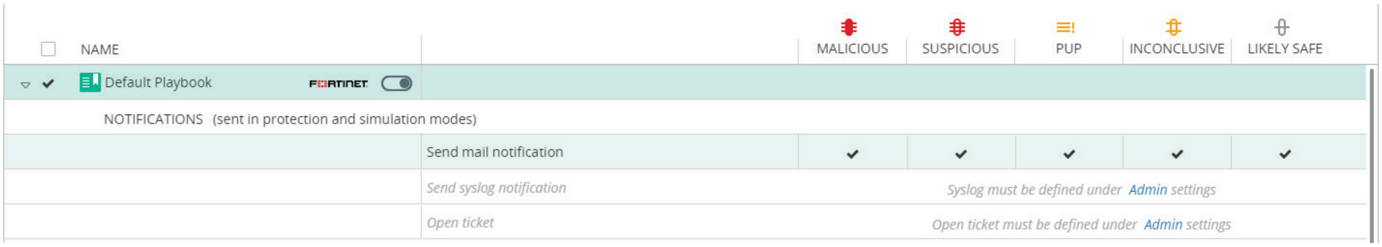


□ NAME		MALICIOUS	SUSPICIOUS	PUP	INCONCLUSIVE	LIKELY SAFE
✓ Default Playbook FORTINET						
NOTIFICATIONS (sent in protection and simulation modes)						
	Send mail notification	✓	✓	✓	✓	✓
	Send syslog notification	*Syslog must be defined under Admin settings*				
	Open ticket	*Open ticket must be defined under Admin settings*				

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 204 for more details.

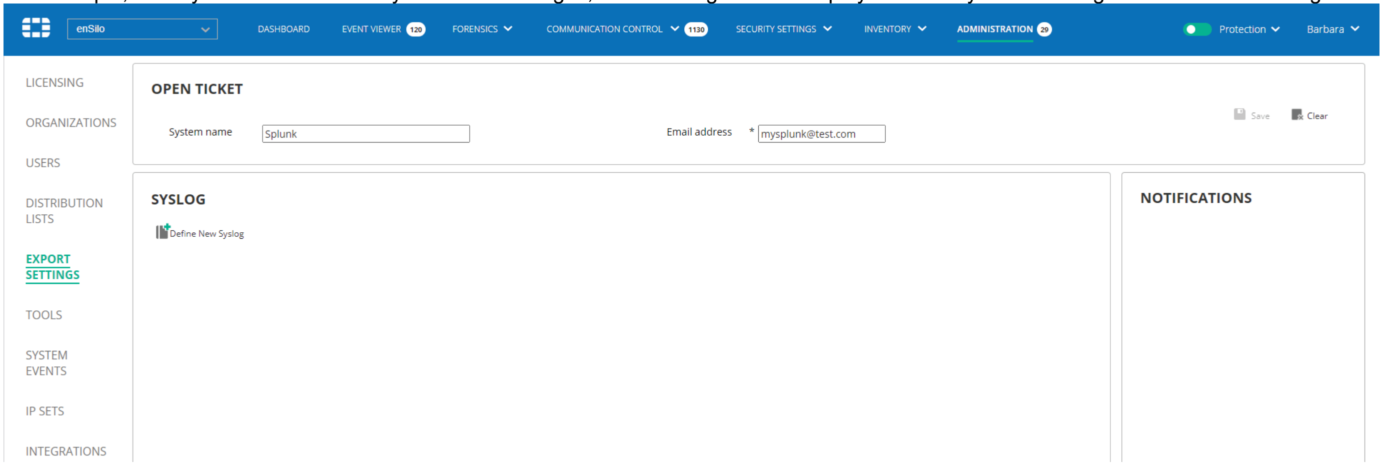
The **Malicious**, **Suspicious**, **PUP**, **Inconclusive** and **Likely Safe** columns correspond to the possible classifications for a security event. When a checkmark ✓ appears in one of these columns, it means that a notification of the specified type is sent when an event is triggered that has that classification. Notifications are sent for all security events except those classified as **Likely Safe**. For example, the figure below shows that an email notification is sent whenever a Malicious, Suspicious, PUP or Inconclusive security event is triggered. **Syslog** and **Open Ticket** notifications work in the same way as Email notifications. For more details about classifications, see page 101.

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:



□ NAME		MALICIOUS	SUSPICIOUS	PUP	INCONCLUSIVE	LIKELY SAFE
✓ Default Playbook FORTINET						
NOTIFICATIONS (sent in protection and simulation modes)						
	Send mail notification	✓	✓	✓	✓	✓
	Send syslog notification	*Syslog must be defined under Admin settings*				
	Open ticket	*Open ticket must be defined under Admin settings*				

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.



OPEN TICKET

System name: Splunk

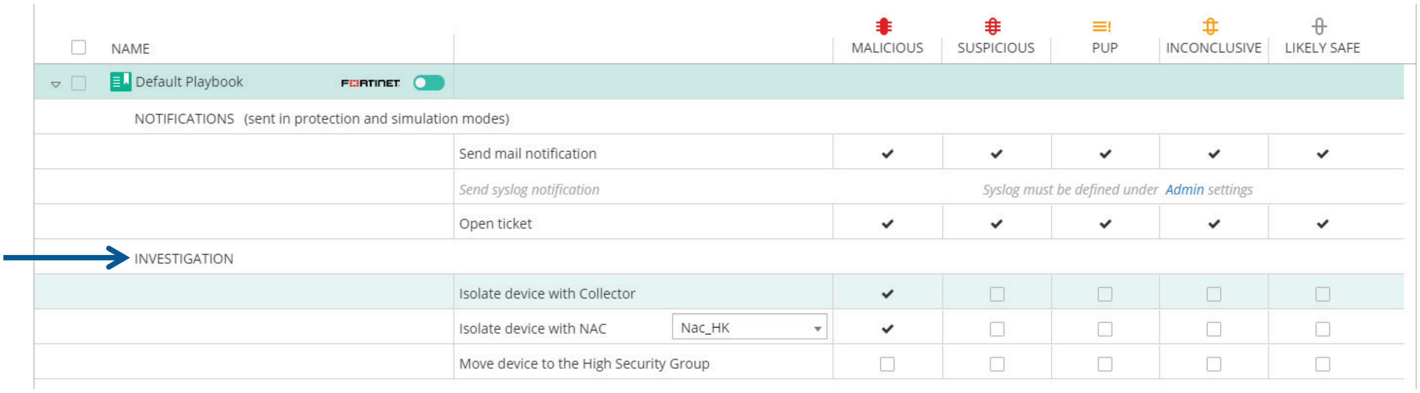
Email address *: mysplunk@test.com

SYSLOG

NOTIFICATIONS

Investigation

Investigation actions enable you to isolate a device or assign it to a high-security Collector Group, in order to further investigate the relevant device's activity.



NAME			MALICIOUS	SUSPICIOUS	PUP	INCONCLUSIVE	LIKELY SAFE
□ Default Playbook							
NOTIFICATIONS (sent in protection and simulation modes)							
	Send mail notification		✓	✓	✓	✓	✓
	Send syslog notification			*Syslog must be defined under Admin settings*			
	Open ticket		✓	✓	✓	✓	✓
INVESTIGATION							
	Isolate device with Collector		✓	□	□	□	□
	Isolate device with NAC	Nac_HK	✓	□	□	□	□
	Move device to the High Security Group		□	□	□	□	□

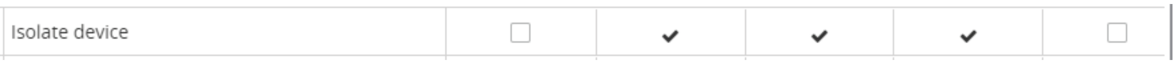
Investigation actions can be one of the following types:

- Isolate Device with Collector, below
- Isolate Device with NAC, page 63
- Move Device to High Security Group, page 63

Isolate Device with Collector

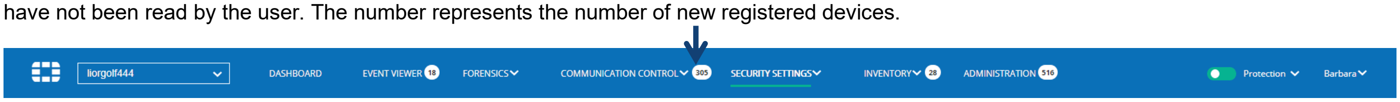
This action blocks the communication to/from the affected Collector. This action only applies for endpoint Collectors. For example, if the Playbook policy is configured to isolate the device for a malicious event, then whenever a maliciously classified security event is triggered from a device, then that device is isolated (blocked) from communicating with the outside world (for both sending and receiving). This means, for example, that applications that communicate with the outside world, such as Google Chrome, Firefox and so on, will be blocked for incoming and outgoing communications.

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

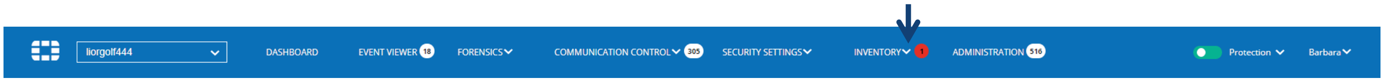


Isolate device	□	✓	✓	✓	□

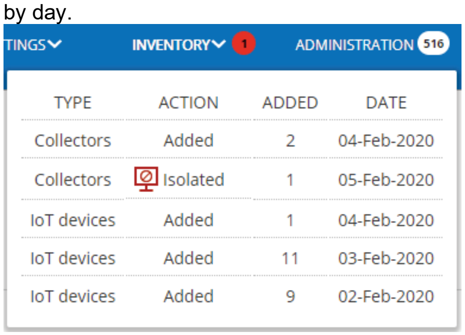
Note – The tab bar at the top of the window may display a white circle(s) with a number inside the circle to indicate that new security events have not been read by the user. The number represents the number of new registered devices.



When the circle is white, it means that there are no isolated devices and the number inside the circle represents the number of new registered devices in the last three days.
When the circle is red, it indicates that there are one or more isolated devices. In this case, the number inside the circle indicates only the number of isolated devices.



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



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

Isolate Device with NAC

This action blocks the communication to/from the affected device by disabling this host on an external Network Access Control system. A NAC connector must already be configured in order to perform this action. For details about how to configure NAC connectors, see *Network Access Control Integration* on page 226.

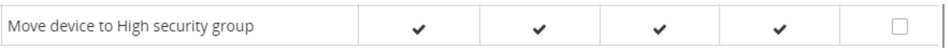
In the dropdown menu next to the action, you can specify which NAC to use for disabling the host or select all of them.

Note – Unlike devices that are isolated using the FortiEDR Collector for which there is an isolation indication on **Inventory** tab and un-isolation is available, devices that were isolated using an external system such as a NAC are not indicated as such on the FortiEDR Console and un-isolation is only possible on the external NAC system.

Move Device to High Security Group

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

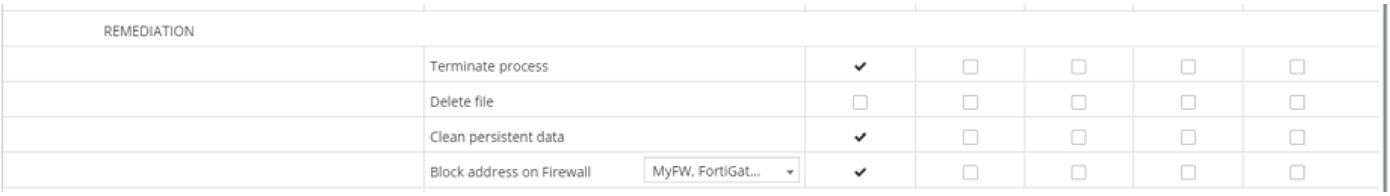
A checkmark ✓ in a classification column here means that the device is automatically moved (assigned) to the High Security Collector Group when a security event is triggered that has that classification. This feature is useful when you want to mark Collectors that triggered malicious events.



Move device to High security group	✓	✓	✓	✓	□

Remediation

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



REMEDIATION							
	Terminate process		✓	□	□	□	□
	Delete file		□	□	□	□	□
	Clean persistent data		✓	□	□	□	□
	Block address on Firewall	MyFW, FortiGat...	✓	□	□	□	□

Remediation actions can be one of the following types:

- Terminate Process, below
- Delete File, below
- Clean Persistent Data, below
- Block Address on Firewall, page 64

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 151.

A checkmark ✓ in a classification column here means that the affected process is automatically terminated on the device when a security event is triggered that has that classification.

Delete File

This action ensures that the file does not attempt to exfiltrate data again, as the file is permanently removed from the device. This action can also be performed manually using the Forensics add-on, as described on page 151.

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

Clean Persistent Data

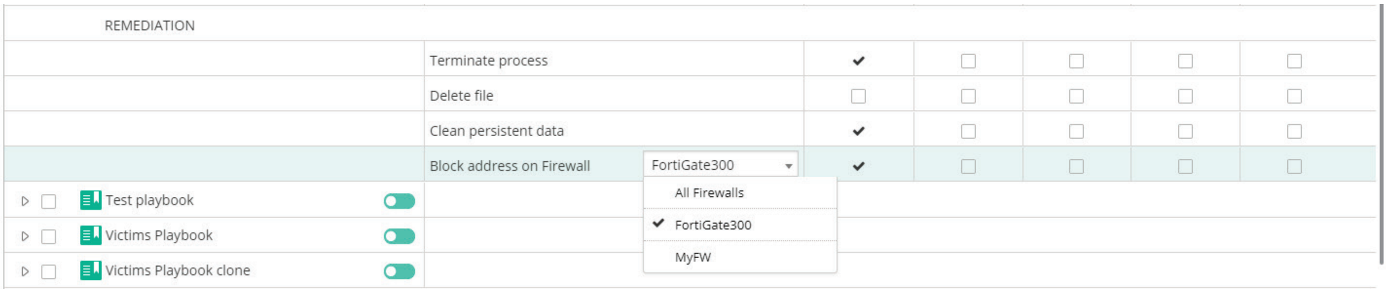
This action cleans the registry keys in Windows. This action can also be performed manually using the Forensics add-on, as described on page 151.

A checkmark ✓ in a classification column here means that the affected registry key is automatically cleaned on the device when a security event is triggered that has that classification.

Block Address on Firewall

This action ensures that connections to remote malicious addresses that are associated with the security event are blocked. A Firewall Connector must already be configured in order to perform this action. For details about how to configure firewall connectors, see Firewall Integration on page 221.

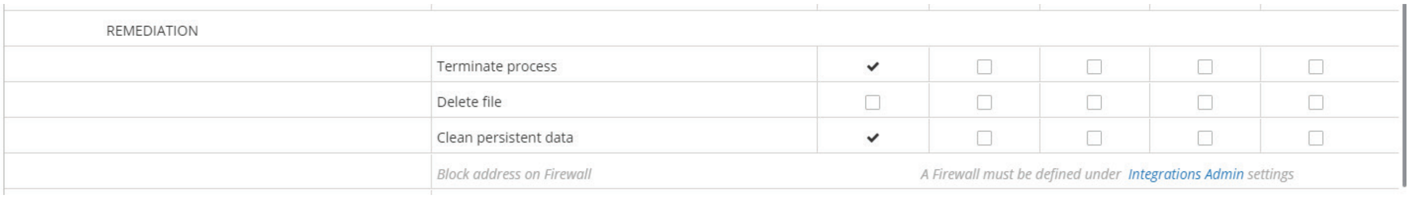
In the dropdown menu next to the action, you can specify which firewalls are used to perform the blocking or select all of them, as shown below:



REMEDIATION						
	Terminate process	✓	□	□	□	□
	Delete file	□	□	□	□	□
	Clean persistent data	✓	□	□	□	□
	Block address on Firewall FortiGate300 ▾	✓	□	□	□	□
▷ □ Test playbook						
▷ □ Victims Playbook						
▷ □ Victims Playbook clone						

A checkmark ✓ in a **Classification** column means that communication with the affected destination is automatically blocked when a security event is triggered that has that classification.

The firewall must already be configured in order to add malicious destinations to blocked addresses. If its settings are not already configured, the relevant row in the Remediation list displays a message indicating that you must first configure it, as shown below:



REMEDIATION						
	Terminate process	✓	□	□	□	□
	Delete file	□	□	□	□	□
	Clean persistent data	✓	□	□	□	□
	Block address on Firewall	*A Firewall must be defined under Integrations Admin settings*				

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 Playbook:** Clones a Playbook policy, as described on page 59.
- **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 54.
- **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 56.
- **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.

Exception Manager

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

An exception can be made for a Collector Group (several specific ones or for all) and a destination IP (a specific one, IP-set or all). The event is then no longer triggered for that specific Collector Group or destination IP. This exception can be added on part or the entire set of rules and the process that triggered this event.

When an exception is defined, it results in one or more *exception pairs*. An exception pair specifies the **rule** that was violated, and the **process** on which the violation occurred, including its entire location path. For example, the following shows several examples of exception pairs:

- **Rule** – File encryptor with **Process** – c:\users\root\Desktop\ransom\RnsmTOX.exe
- **Rule** – Process hollowing with **Process** – c:\users\root\AppData\Local\hipmiav.exe

An exception that applies to a security event can result in the creation of several exception pairs. Each exception is associated with a specific process path. You determine whether the exception pair can run from the event-specific path or whether to apply the exception for this process so that it can run from any path.

If the exception pair includes more than one process, you can include the other processes too, as well as determine whether they can run from the event-specific path or from any path.

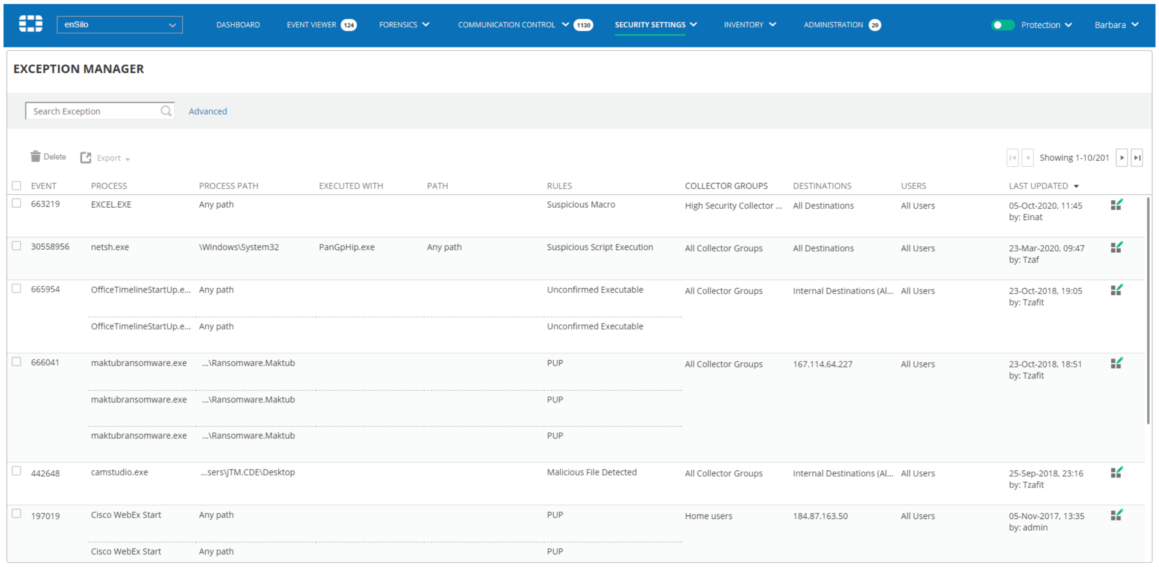
Any exception that you define applies to all policies.

Exceptions are created in the Event Viewer, as described on page 107.

Note – FCS may push an automated exception in cases where extended analysis and investigation of a security event leads to its reclassification as Safe. This prevents the security event from triggering again.
In such cases, the security event is moved under archived events and the exception that was set is added in the Exception Manager with FortiEDRCloudServices as the handling user.

To manage exceptions:

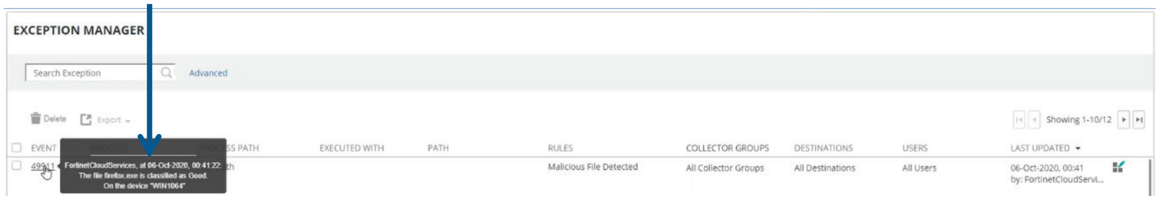
1 Select **SECURITY SETTINGS ➔ Exception Manager**. Alternatively, in the **EVENT VIEWER** page, click the Exception Manager button. The following window displays, showing the list of previously created exceptions:



EXCEPTION MANAGER

EVENT	PROCESS	PROCESS PATH	EXECUTED WITH	PATH	RULES	COLLECTOR GROUPS	DESTINATIONS	USERS	LAST UPDATED
663219	EXCEL.EXE	Any path			Suspicious Macro	High Security Collector ...	All Destinations	All Users	05-Oct-2020, 11:45 by: Einat
30558956	netsh.exe	\Windows\System32	PanGpHip.exe	Any path	Suspicious Script Execution	All Collector Groups	All Destinations	All Users	23-Mar-2020, 09:47 by: Tzaf
665954	OfficeTimelineStartUp.e...	Any path			Unconfirmed Executable	All Collector Groups	Internal Destinations (Al...	All Users	23-Oct-2018, 19:05 by: Tzafit
	OfficeTimelineStartUp.e...	Any path			Unconfirmed Executable				
666041	maktubransomware.exe	...\Ransomware.Maktub			PUP	All Collector Groups	167.114.64.227	All Users	23-Oct-2018, 18:51 by: Tzafit
	maktubransomware.exe	...\Ransomware.Maktub			PUP				
	maktubransomware.exe	...\Ransomware.Maktub			PUP				
442648	camstudio.exe	...sers\JTM.CDE\Desktop			Malicious File Detected	All Collector Groups	Internal Destinations (Al...	All Users	25-Sep-2018, 23:16 by: Tzafit
197019	Cisco WebEx Start	Any path			PUP	Home users	184.87.163.50	All Users	05-Nov-2017, 13:35 by: admin
	Cisco WebEx Start	Any path			PUP				

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



EXCEPTION MANAGER

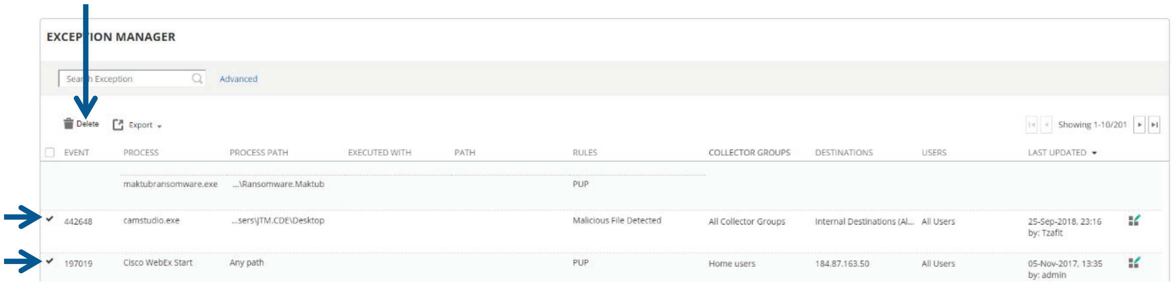
Search Exception | Advanced

Delete | Export | Showing 1-10/12

FortinetCloudServices, at 06-Oct-2020, 00:41:22:
The file firefox.exe is classified as Good.
On the device "WIN1064"

□	EVENT	PROCESS	PROCESS PATH	EXECUTED WITH	PATH	RULES	COLLECTOR GROUPS	DESTINATIONS	USERS	LAST UPDATED
□	49911		th			Malicious File Detected	All Collector Groups	All Destinations	All Users	06-Oct-2020, 00:41 by: FortinetCloudServi...

Tip – You can delete one or more exceptions simultaneously by selecting the checkbox at the beginning of its row and then clicking the **Delete** button.



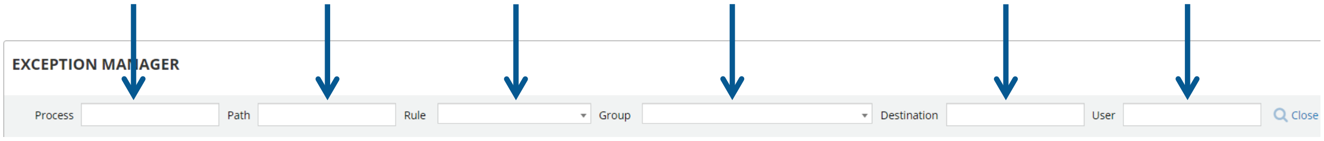
EXCEPTION MANAGER

Search Exception | Advanced

Delete | Export | Showing 1-10/201

□	EVENT	PROCESS	PROCESS PATH	EXECUTED WITH	PATH	RULES	COLLECTOR GROUPS	DESTINATIONS	USERS	LAST UPDATED
		maktubransomware.exe	...\Ransomware.Maktub			PUP				
✓	442648	camstudio.exe	...sers\JTM.CDE\Desktop			Malicious File Detected	All Collector Groups	Internal Destinations (Al...	All Users	25-Sep-2018, 23:16 by: Tzafit
✓	197019	Cisco WebEx Start	Any path			PUP	Home users	184.87.163.50	All Users	05-Nov-2017, 13:35 by: admin

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



EXCEPTION MANAGER

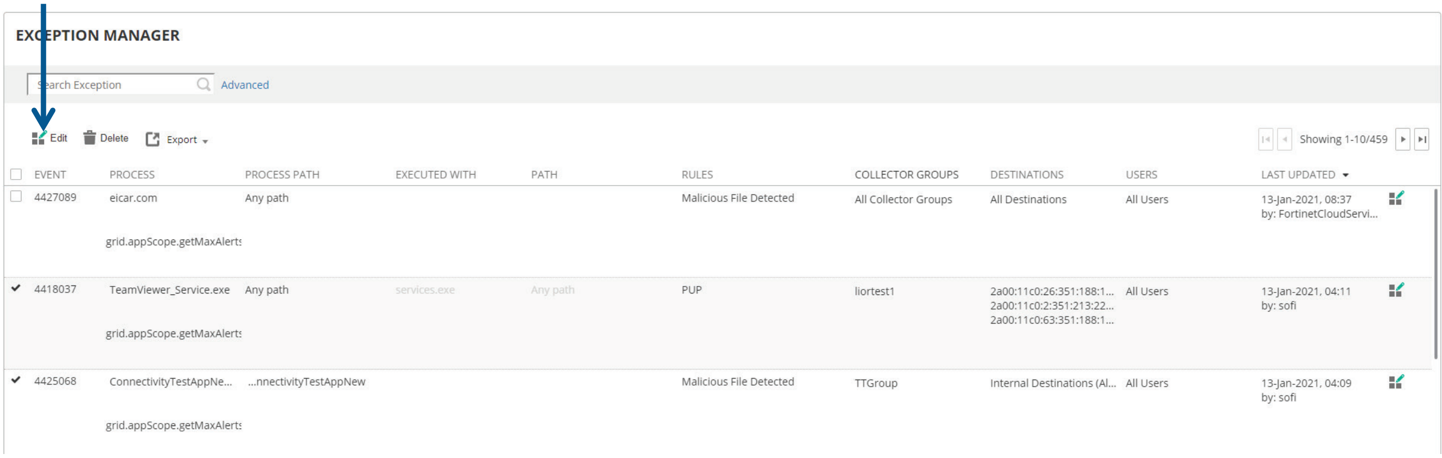
Process | Path | Rule | Group | Destination | User | Close

Click the **Basic search** button to access the standard search options.

Click the **Edit Exception** button in an exception row to edit that exception. For more details, see *Editing Security Event Exceptions* on page 116.

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

Changes can be made on multiple exceptions at the same time by checking the Exceptions that you would like to edit and then clicking on the **Edit** tool, as shown below:



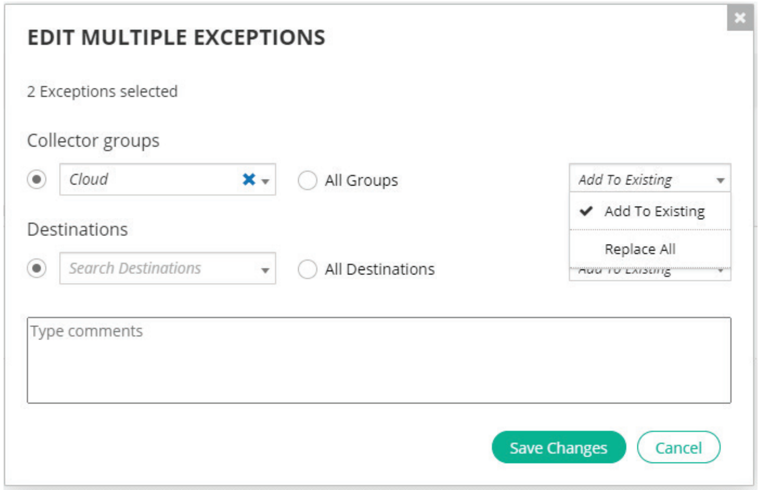
EXCEPTION MANAGER

Search Exception | Advanced

Edit | Delete | Export | Showing 1-10/459

□	EVENT	PROCESS	PROCESS PATH	EXECUTED WITH	PATH	RULES	COLLECTOR GROUPS	DESTINATIONS	USERS	LAST UPDATED
□	4427089	eicar.com grid.appScope.getMaxAlerts	Any path			Malicious File Detected	All Collector Groups	All Destinations	All Users	13-Jan-2021, 08:37 by: FortinetCloudServi...
✓	4418037	TeamViewer_Service.exe grid.appScope.getMaxAlerts	Any path	services.exe	Any path	PUP	liortest1	2a00:11c0:26:351:188:1... 2a00:11c0:2:351:213:22... 2a00:11c0:63:351:188:1...	All Users	13-Jan-2021, 04:11 by: sofi
✓	4425068	ConnectivityTestAppNe... grid.appScope.getMaxAlerts	...nnectivityTestAppNew			Malicious File Detected	TTGroup	Internal Destinations (Al...	All Users	13-Jan-2021, 04:09 by: sofi

The following window displays in the which you can choose to add new Collector Groups in addition to existing ones or to replace all Collector Groups with the new Collector Group values that you select:



EDIT MULTIPLE EXCEPTIONS

2 Exceptions selected

Collector groups

● Cloud ○ All Groups — Add To Existing

✓ Add To Existing

Replace All

Destinations

● Search Destinations ○ All Destinations

Type comments

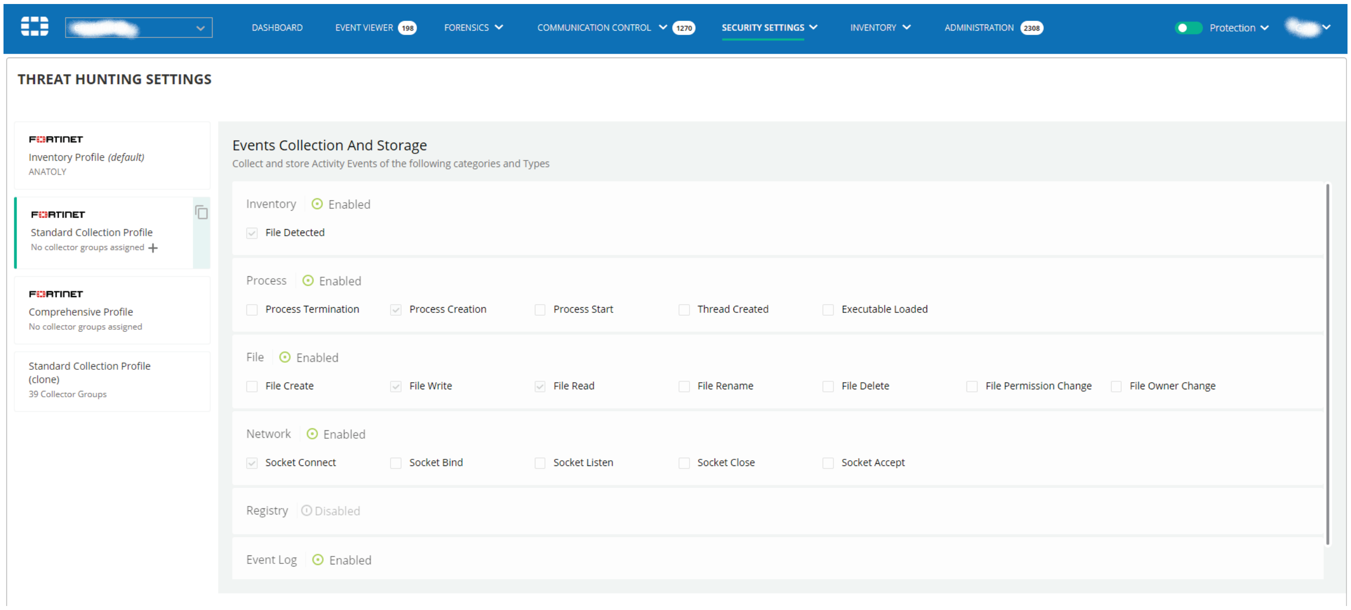
This same procedure can be used to edit the IP sets of the destination addresses of the selected exceptions.

Threat Hunting Settings

Note – Threat Hunting Settings is a license-dependent add-on. You may contact Fortinet support for more information.

Threat Hunting Settings control the type of activity data that is collected for the Threat Hunting feature (which is described in the *Threat Hunting* section on page 158). Activity data that is collected is stored on the Repository server.

To access Threat Hunting settings, select **SECURITY SETTINGS ➔ Threat Hunting Settings**. The following page displays:



THREAT HUNTING SETTINGS

FORTINET Inventory Profile *(default)* ANATOLY

FORTINET Standard Collection Profile — No collector groups assigned +

FORTINET Comprehensive Profile — No collector groups assigned

Standard Collection Profile (clone) — 39 Collector Groups

Events Collection And Storage

Collect and store Activity Events of the following categories and Types

Inventory ⊙ Enabled

☑ File Detected

Process ⊙ Enabled

□ Process Termination ☑ Process Creation □ Process Start □ Thread Created □ Executable Loaded

File ⊙ Enabled

□ File Create ☑ File Write ☑ File Read □ File Rename □ File Delete □ File Permission Change □ File Owner Change

Network ⊙ Enabled

☑ Socket Connect □ Socket Bind □ Socket Listen □ Socket Close □ Socket Accept

Registry ⓘ Disabled

Event Log ⊙ Enabled

The left side of the **Threat Hunting Settings** page shows a list of Profiles. A Profile defines the activity event categories and actions to be collected. FortiEDR comes with several predefined default Profiles, which cannot be modified.

In addition to the pre-defined Profiles, you can define your own custom Profiles by cloning an existing Profile.

The pane on the right side of the page lists all activity event categories and their associated actions. These categories are the same as those described on page 158.

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

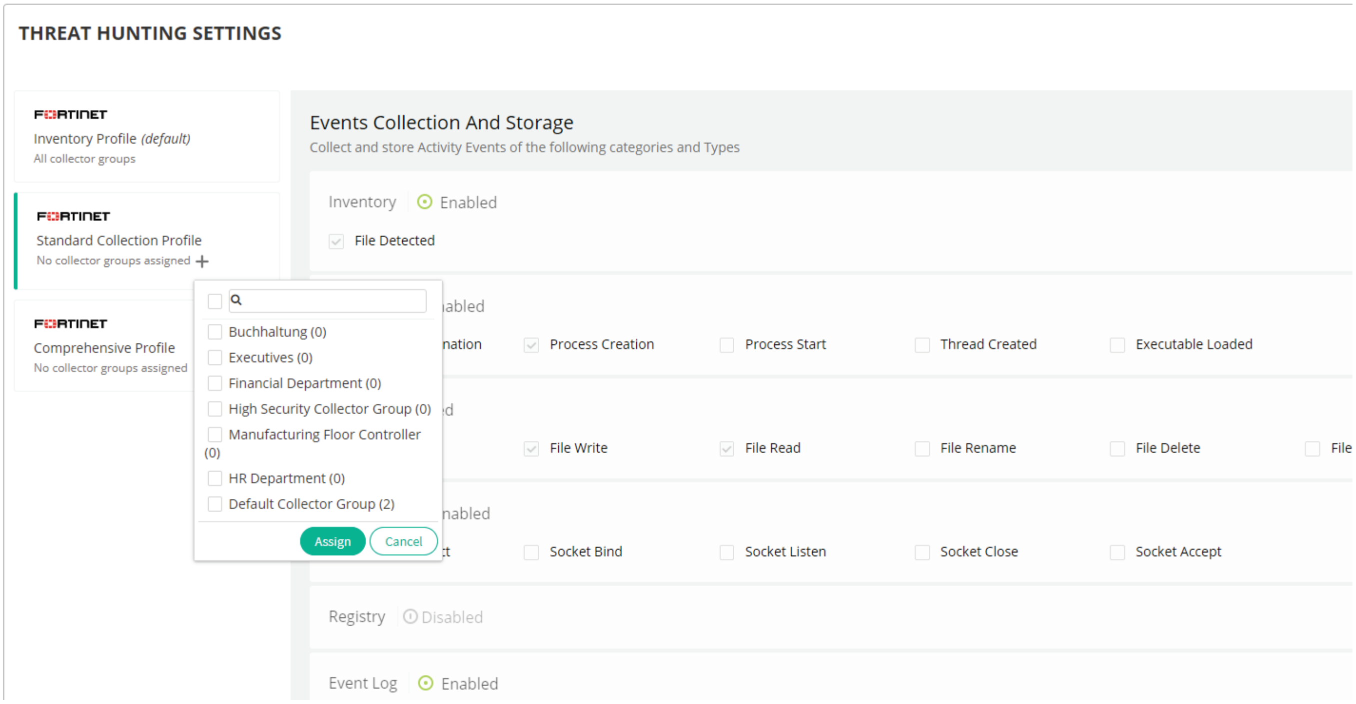
Check the checkboxes of the actions for which FortiEDR will collect activity data.

Assigning a Collector Group to a Profile

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

To assign a Collector Group to a Profile:

1 In the Profiles pane, click the **+** button of the Profile to which to assign a Collector Group. The following displays showing the list of all Collector Groups:



2 Select the checkbox(s) of the Collector Group(s) to assign to the Profile.

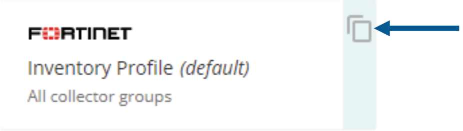
3 Click **Assign**. A message is displayed indicating that the selected groups are currently assigned to another Profile and they will be reassigned and asking for you approval. Please approve.

Creating/Cloning a Profile

In order to create a new Profile, you must first clone an existing Profile and then customize the clone.

To clone a Profile:

1 Click the **Clone** icon that appears on the right of the Profile to be cloned.



2 Enter the name of the new Profile.

3 On the right side, enable the activity events to be collected and disable the activity events that should not be collected.

4 Click **Save**.

5 Assign the Collector Group(s) on which to apply the newly created Profile.

Exclusion Manager

Exclusions enable you to define certain types of activity events to be excluded from being collected by Threat Hunting data (even though should be collected according to the Threat Hunting Profile assigned to a Collector group, which was described in the *Threat Hunting Settings* section on page 67). For example, if you know that a certain process is legitimate, but it creates many activity events that are not relevant to your Threat Hunting investigation, you can use the Exclusion Manager to define that these activities are not collected.

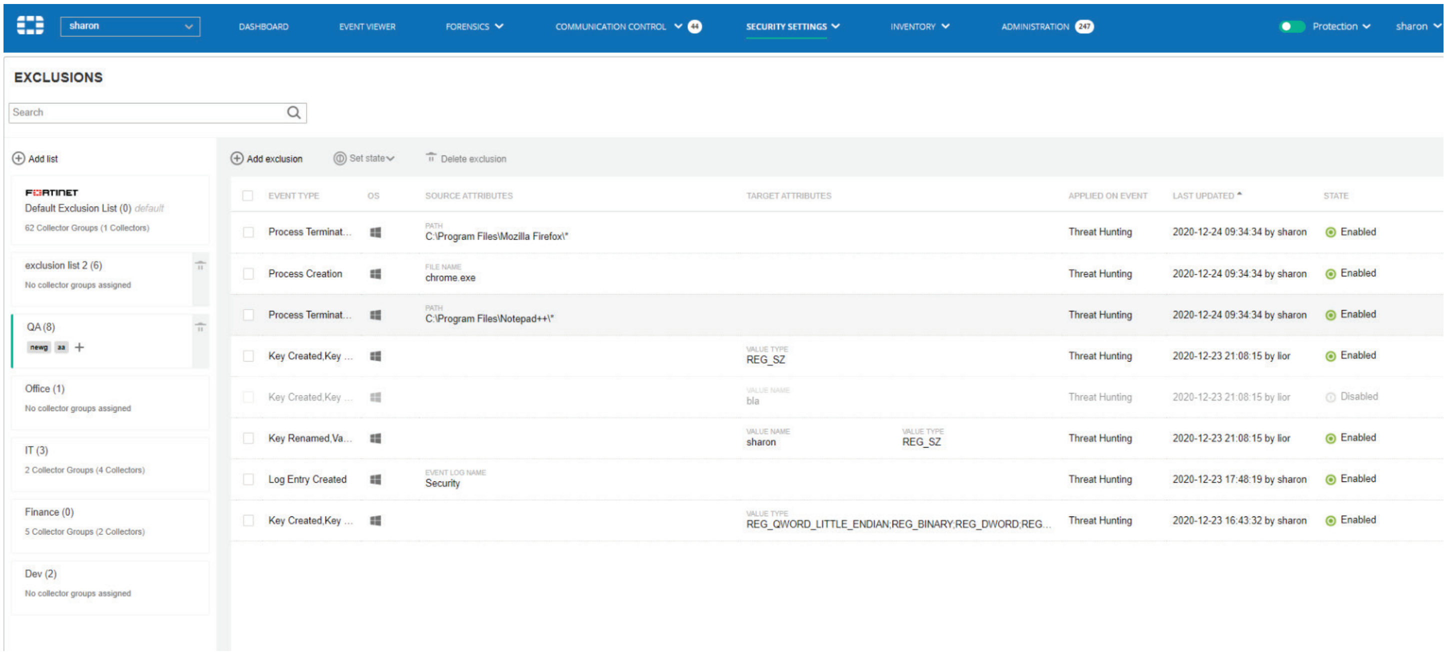
The Exclusion Manager enables you to define and manage exclusion lists and the exclusions that they contain.

Note – Exclusions are different than security event exceptions, as follows:

- Exclusions define which activity events should be collected. They are exclusions to the Threat Hunting Profile.
- Security event exceptions are defined after a particular security event has occurred. They are an exception to the assigned Security Policy

To access the Exclusion Manager, select **SECURITY SETTINGS ➔ Exclusion Manager**.

The **Exclusion Manager** page contains the following areas:



EXCLUSIONS

FORTINET
Default Exclusion List (0) *default*
62 Collector Groups (1 Collectors)

exclusion list 2 (6)
No collector groups assigned

QA (8)

Office (1)
No collector groups assigned

IT (3)
2 Collector Groups (4 Collectors)

Finance (0)
5 Collector Groups (2 Collectors)

Dev (2)
No collector groups assigned

□	EVENT TYPE	OS	SOURCE ATTRIBUTES	TARGET ATTRIBUTES		APPLIED ON EVENT	LAST UPDATED ^	STATE
□	Process Terminat...	⊞	PATH C:\Program Files\Mozilla Firefox*			Threat Hunting	2020-12-24 09:34:34 by sharon	● Enabled
□	Process Creation	⊞	FILE NAME chrome.exe			Threat Hunting	2020-12-24 09:34:34 by sharon	● Enabled
□	Process Terminat...	⊞	PATH C:\Program Files\Notepad++\*			Threat Hunting	2020-12-24 09:34:34 by sharon	● Enabled
□	Key Created,Key ...	⊞		VALUE TYPE REG_SZ		Threat Hunting	2020-12-23 21:08:15 by lior	● Enabled
□	Key Created,Key ...	⊞		VALUE NAME bla		Threat Hunting	2020-12-23 21:08:15 by lior	○ Disabled
□	Key Renamed,Va...	⊞		VALUE NAME sharon	VALUE TYPE REG_SZ	Threat Hunting	2020-12-23 21:08:15 by lior	● Enabled
□	Log Entry Created	⊞	EVENT LOG NAME Security			Threat Hunting	2020-12-23 17:48:19 by sharon	● Enabled
□	Key Created,Key ...	⊞		VALUE TYPE REG_QWORD_LITTLE_ENDIAN;REG_BINARY;REG_DWORD;REG...		Threat Hunting	2020-12-23 16:43:32 by sharon	● Enabled

- **Filters,** page 69
- **Exclusion Lists,** page 70
- **Exclusions,** page 71

Filters

To filter the Exclusion list names and its content, simply enter text in the **Search** field. Afterwards, only the Exclusion lists that match the provided text are displayed showing only the relevant exclusions.

Defining Exclusion Lists

An Exclusion List contains a list of exclusions. You can assign Collector Groups to an Exclusion List in order to specify that the exclusions in the Exclusion List apply to the Collectors in the Collector Groups assigned to it. Exclusion Lists enable you to logically organize, categorize and group exclusions based on the type of activity data they are to exclude. For example, let's say that you want to collect network activity data for your system, but a specific application generates quite a bit of uninteresting logistical network activity that you do not want to collect. In this case, you can define an Exclusion List named after that application that contains one or more exclusions that relate specifically to the network activity generated by that application. Exclusion Lists can be organize anyway you see fit. For example, you can create an Exclusion List for security products, a different one for PDF documents, a different one for HR-related software and so on.

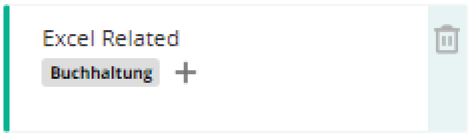
FortiEDR comes with a default General Exclusion List that includes important exclusions. The exclusions in this group are not editable.

Adding an Exclusion List

To define an Exclusion List:

1. Click the **+ Add List** option and provide a name to create a new Exclusion List.
2. Add (define) the exclusions of this Exclusion List (as described on the following page). Each exclusion that you add belongs to a specific Exclusion List.
3. Assign Collector Groups to this Exclusion List (as described below) in order to determine to which Collector Groups these exclusions apply. A Collector Group can be assigned to multiple Exclusion Lists.

Assigning a Collector Group to an Exclusion List



You can perform the following operations on an Exclusion List:

- **Assign a Collector Group:** Click the **+** button in the Exclusion List to which to assign a Collector Group. Then, select the Collectors groups to which to assign this list and approve it. Note that a Collector Group can be assigned to multiple Exclusion Lists.
- **Unassign a Collector Group:** Click the **+** button and uncheck the Collector Group to be removed from an Exclusion List.
- **Delete Exclusions List:** press on the **Delete** 🗑 button. Note that all Exclusions in this list will be removed and will no longer be applied to the assigned Collector groups.

Defining Exclusions

All exclusions must belong to an Exclusion List. Select an Exclusion List on the left to display the exclusions that are defined in it. Exclusions can be defined for a –

- **Source (process) –** Which is identified by a source attribute, such as a Signer.
- **Type/Action –** Activity event types, as described on page 72.
- **Target –** Which is identified by a target attribute, such as IP & Port

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

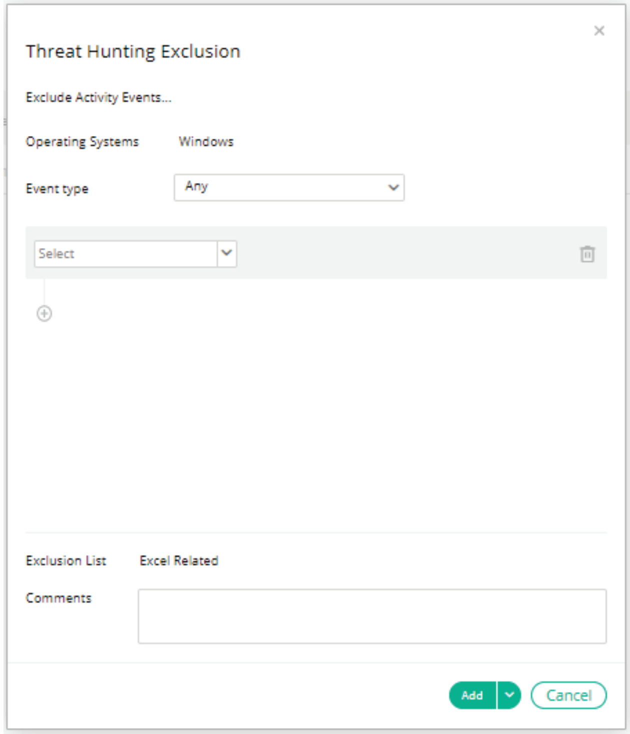
For example, you can define to exclude activity events of a specific Type that have a specific source and a specific target or to exclude (for example) activity events that have a specific source and any activity or target.

Adding an Exclusion

To add an exclusion:

1 In the left pane, click the Exclusion List to which to add the exclusion.

2 In the right pane, click the **+ Add Exclusion** button. The following displays:



Threat Hunting Exclusion

Exclude Activity Events...

Operating Systems Windows

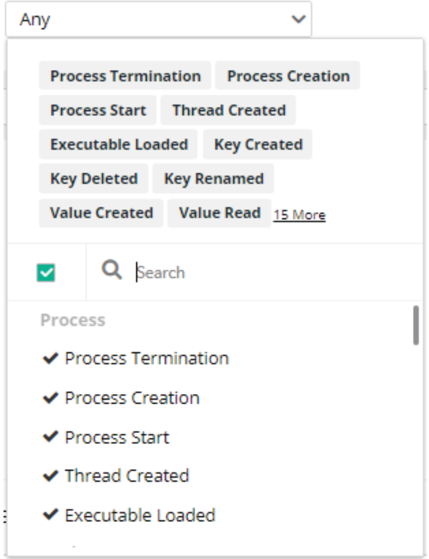
Event type Any

Exclusion List Excel Related

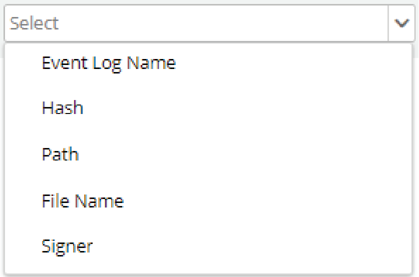
Comments

3 To define that an exclusion includes a specific **Activity Event Type**, select the type of action(s) to exclude from the displayed dropdown list. Alternatively, select the **Any** option (the default option), which means that you are not specifying a specific action type.

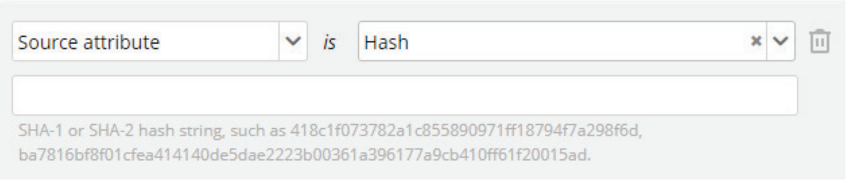
All action types for collection are listed according to Category. You can select one or more actions from a single Category. Actions cannot be selected from different categories. For example, you can select the **Process Termination** and the **Process Start** options from the **Process Category** in the same exclusion. However, you cannot select the **Key Created** option together and the **Thread Created** options in the same exclusion – to do this you must create two different exclusions.



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

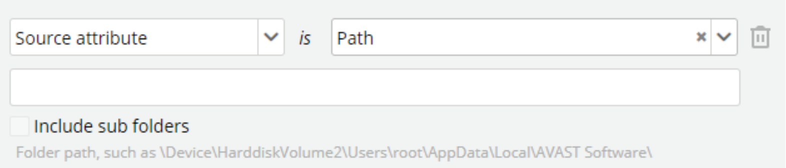


If you select **Hash**, then specify the hash, as shown below:



SHA-1 or SHA-2 hash string, such as 418c1f073782a1c855890971ff18794f7a298f6d, ba7816bf8f01cfea414140de5dae2223b00361a396177a9cb410ff61f20015ad.

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

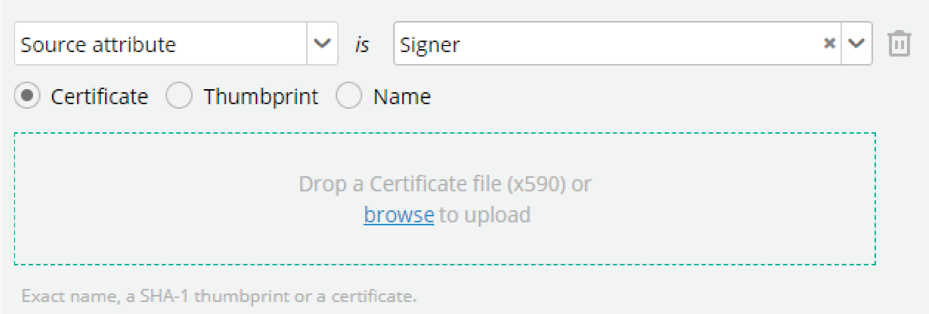


□ Include sub folders

Folder path, such as \Device\HarddiskVolume2\Users\root\AppData\Local\AVAST Software\

If you select **File Name**, then enter the file name.

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



Source attribute is Signer

● Certificate ○ Thumbprint ○ Name

Drop a Certificate file (x590) or browse to upload

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

5 To define that an exclusion includes a **Target** attribute condition, click the **+** button, select the target Attribute and then define the target criteria, as described below:

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

- A process Category event is identified by hash, path, file name or Signer.
- A network Category event is identified by network-related properties, such as a remote IP and port.
- A registry Category event is identified by a registry key path, value name, value type or value size.
- An Event log Category event is identified by the Event Log ID.

When defining an exclusion that contains multiple conditions, an AND relationship exists between the conditions.

Note – If an OR relationship is needed between the conditions that you define, simply create another exclusion.

Setting the State of an Exclusion

The **Set State** button enables you to enable or disable the selected exclusion(s). By default, an exclusion is enabled.

Deleting an Exclusion

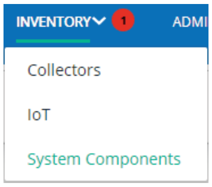
The **Delete** button enables you to delete the selected exclusion(s).

Chapter 4 – INVENTORY

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

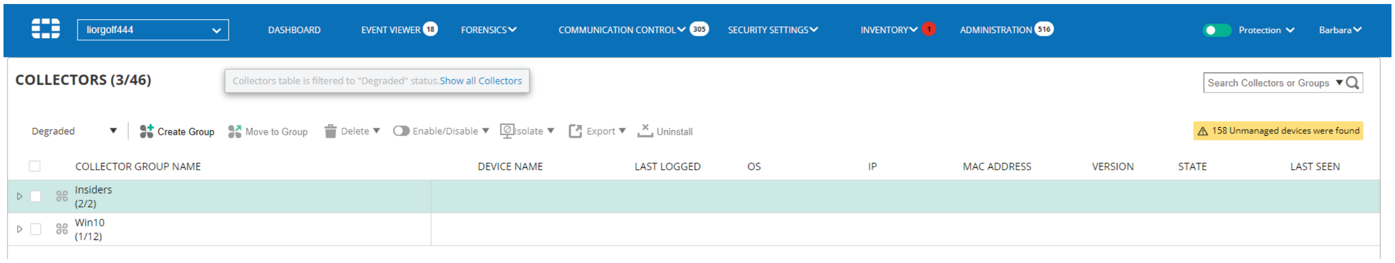
Introducing the Inventory

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.

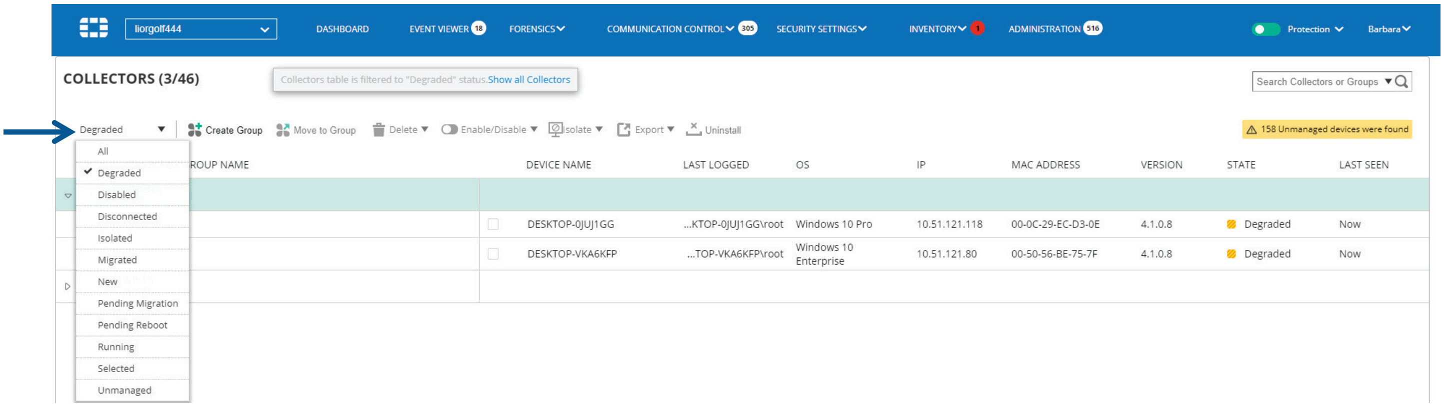


COLLECTORS (3/46)

Collectors table is filtered to "Degraded" status.Show all Collectors

COLLECTOR GROUP NAME	DEVICE NAME	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	STATE	LAST SEEN
Insiders (2/2)								
Win10 (1/12)								

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:

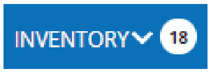


COLLECTORS (3/46)

Collectors table is filtered to "Degraded" status.Show all Collectors

ROUP NAME	DEVICE NAME	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	STATE	LAST SEEN
	DESKTOP-0JUJ1GG	...KTOP-0JUJ1GG\root	Windows 10 Pro	10.51.121.118	00-0C-29-EC-D3-0E	4.1.0.8	Degraded	Now
	DESKTOP-VKA6KFP	...TOP-VKA6KFP\root	Windows 10 Enterprise	10.51.121.80	00-50-56-BE-75-7F	4.1.0.8	Degraded	Now

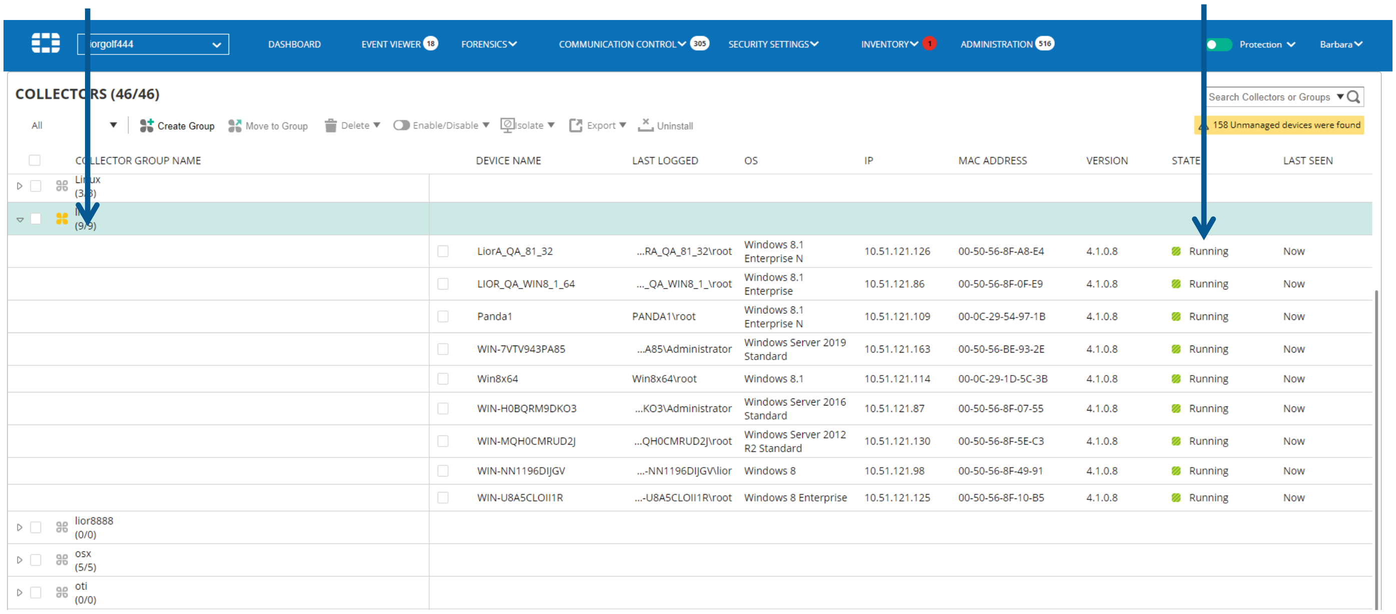
When a new FortiEDR Collector registers, an indicator displays on the **INVENTORY** tab.



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.



COLLECTORS (46/46)

158 Unmanaged devices were found

COLLECTOR GROUP NAME	DEVICE NAME	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	STATE	LAST SEEN
Linux (3/3)								
l (9/9)								
	LiorA_QA_81_32	...RA_QA_81_32\root	Windows 8.1 Enterprise N	10.51.121.126	00-50-56-8F-A8-E4	4.1.0.8	Running	Now
	LIOR_QA_WIN8_1_64	..._QA_WIN8_1_\root	Windows 8.1 Enterprise	10.51.121.86	00-50-56-8F-0F-E9	4.1.0.8	Running	Now
	Panda1	PANDA1\root	Windows 8.1 Enterprise N	10.51.121.109	00-0C-29-54-97-1B	4.1.0.8	Running	Now
	WIN-7VTV943PA85	...A85\Administrator	Windows Server 2019 Standard	10.51.121.163	00-50-56-BE-93-2E	4.1.0.8	Running	Now
	Win8x64	Win8x64\root	Windows 8.1	10.51.121.114	00-0C-29-1D-5C-3B	4.1.0.8	Running	Now
	WIN-H0BQRM9DKO3	...KO3\Administrator	Windows Server 2016 Standard	10.51.121.87	00-50-56-8F-07-55	4.1.0.8	Running	Now
	WIN-MQH0CMRUD2J	...QH0CMRUD2J\root	Windows Server 2012 R2 Standard	10.51.121.130	00-50-56-8F-5E-C3	4.1.0.8	Running	Now
	WIN-NN1196DIJGV	...-NN1196DIJGV\lior	Windows 8	10.51.121.98	00-50-56-8F-49-91	4.1.0.8	Running	Now
	WIN-U8A5CLOII1R	...-U8A5CLOII1R\root	Windows 8 Enterprise	10.51.121.125	00-50-56-8F-10-B5	4.1.0.8	Running	Now
lior8888 (0/0)								
osx (5/5)								
oti (0/0)								

To export the list of FortiEDR components:

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

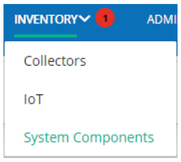
Uninstalling a Collector

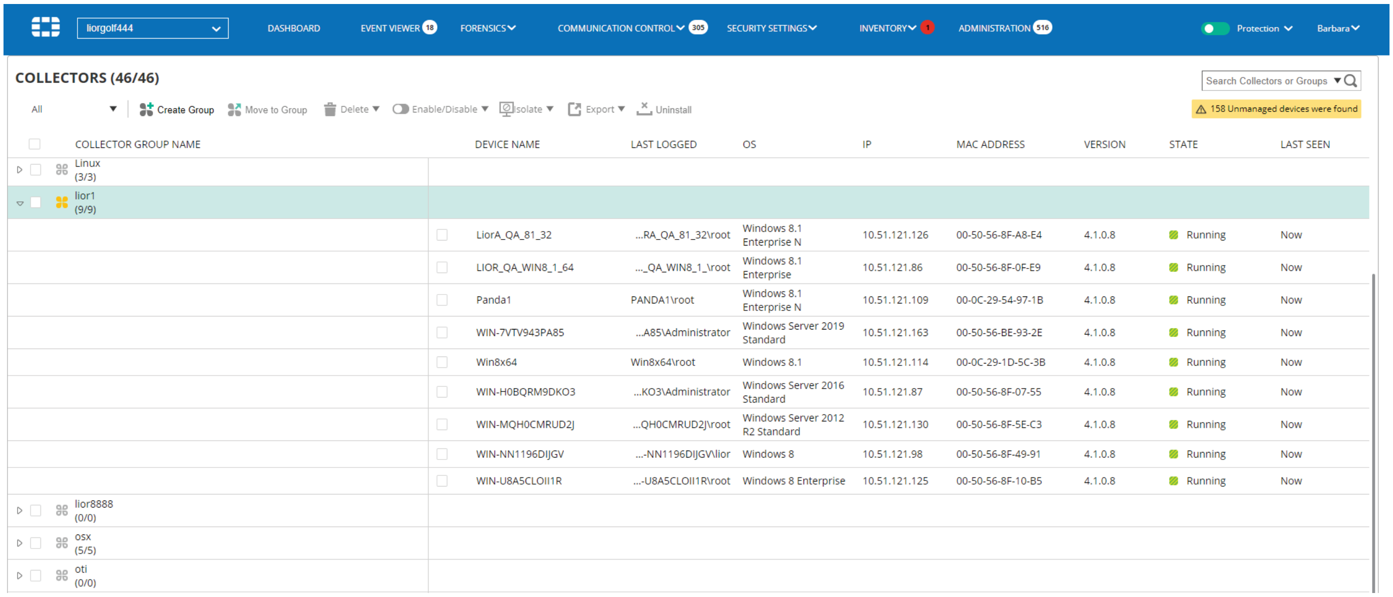
Use the Uninstall button to uninstall a Collector from a device. Use caution when using this option, as a Collector cannot be reinstalled after removal using the FortiEDR user interface. Therefore, it is recommended to disable a Collector using the **Enable/Disable** option rather than uninstalling it.

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 78. 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 79.

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





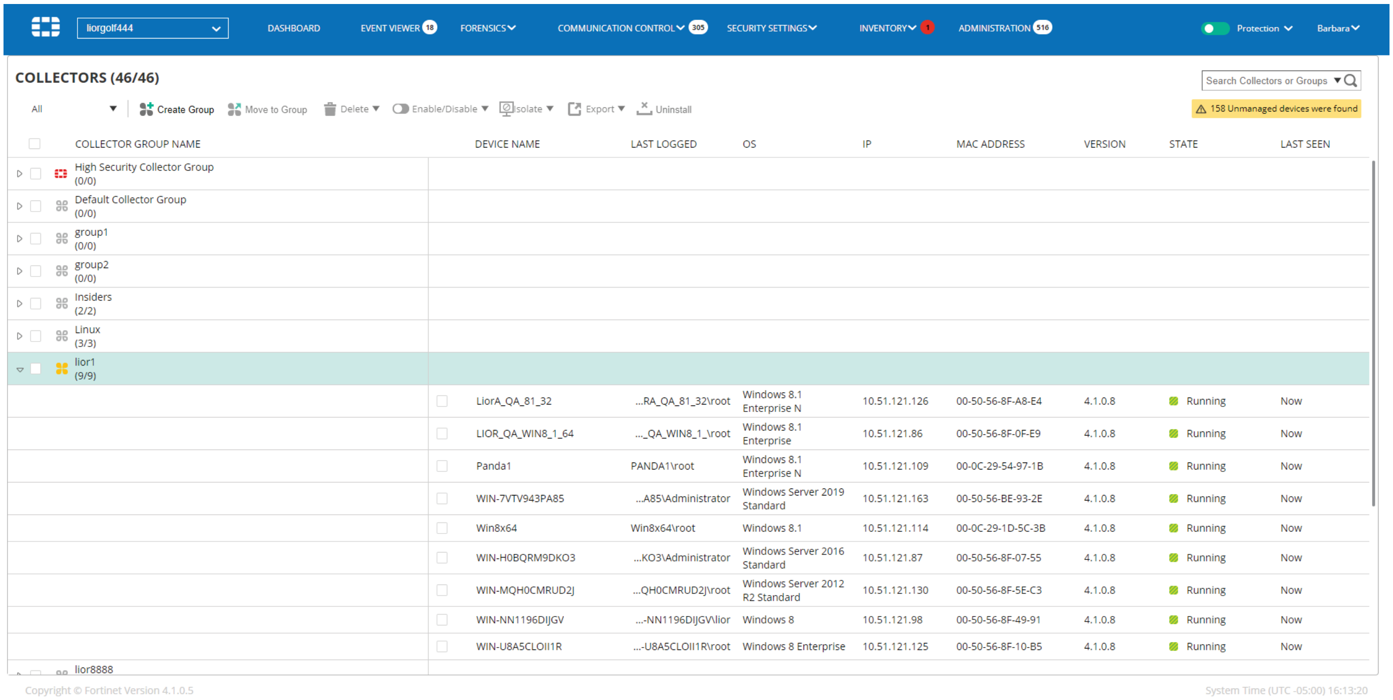
COLLECTORS (46/46)

⚠ 158 Unmanaged devices were found

COLLECTOR GROUP NAME	DEVICE NAME	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	STATE	LAST SEEN
Linux (3/3)								
lior1 (9/9)								
	LiorA_QA_81_32	...RA_QA_81_32\root	Windows 8.1 Enterprise N	10.51.121.126	00-50-56-8F-A8-E4	4.1.0.8	Running	Now
	LIOR_QA_WIN8_1_64	..._QA_WIN8_1_\root	Windows 8.1 Enterprise	10.51.121.86	00-50-56-8F-0F-E9	4.1.0.8	Running	Now
	Panda1	PANDA1\root	Windows 8.1 Enterprise N	10.51.121.109	00-0C-29-54-97-1B	4.1.0.8	Running	Now
	WIN-7VTV943PA85	...A85\Administrator	Windows Server 2019 Standard	10.51.121.163	00-50-56-BE-93-2E	4.1.0.8	Running	Now
	Win8x64	Win8x64\root	Windows 8.1	10.51.121.114	00-0C-29-1D-5C-3B	4.1.0.8	Running	Now
	WIN-H0BQRM9DKO3	...KO3\Administrator	Windows Server 2016 Standard	10.51.121.87	00-50-56-8F-07-55	4.1.0.8	Running	Now
	WIN-MQH0CMRUD2J	...QH0CMRUD2J\root	Windows Server 2012 R2 Standard	10.51.121.130	00-50-56-8F-5E-C3	4.1.0.8	Running	Now
	WIN-NN1196DIJGV	...-NN1196DIJGV\lior	Windows 8	10.51.121.98	00-50-56-8F-49-91	4.1.0.8	Running	Now
	WIN-U8A5CLOII1R	...-U8A5CLOII1R\root	Windows 8 Enterprise	10.51.121.125	00-50-56-8F-10-B5	4.1.0.8	Running	Now
lior8888 (0/0)								
osx (5/5)								
oti (0/0)								

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.



COLLECTORS (46/46)

⚠ 158 Unmanaged devices were found

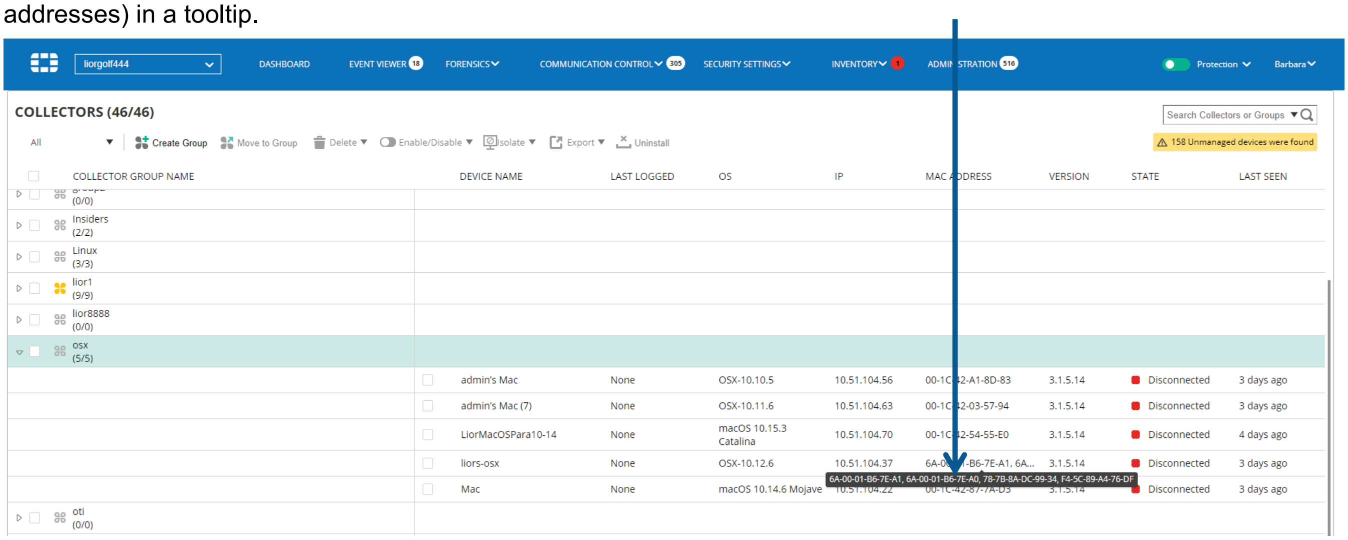
COLLECTOR GROUP NAME	DEVICE NAME	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	STATE	LAST SEEN
High Security Collector Group (0/0)								
Default Collector Group (0/0)								
group1 (0/0)								
group2 (0/0)								
Insiders (2/2)								
Linux (3/3)								
lior1 (9/9)								
	LiorA_QA_81_32	...RA_QA_81_32\root	Windows 8.1 Enterprise N	10.51.121.126	00-50-56-8F-A8-E4	4.1.0.8	Running	Now
	LIOR_QA_WIN8_1_64	..._QA_WIN8_1_\root	Windows 8.1 Enterprise	10.51.121.86	00-50-56-8F-0F-E9	4.1.0.8	Running	Now
	Panda1	PANDA1\root	Windows 8.1 Enterprise N	10.51.121.109	00-0C-29-54-97-1B	4.1.0.8	Running	Now
	WIN-7VTV943PA85	...A85\Administrator	Windows Server 2019 Standard	10.51.121.163	00-50-56-BE-93-2E	4.1.0.8	Running	Now
	Win8x64	Win8x64\root	Windows 8.1	10.51.121.114	00-0C-29-1D-5C-3B	4.1.0.8	Running	Now
	WIN-H0BQRM9DKO3	...KO3\Administrator	Windows Server 2016 Standard	10.51.121.87	00-50-56-8F-07-55	4.1.0.8	Running	Now
	WIN-MQH0CMRUD2J	...QH0CMRUD2J\root	Windows Server 2012 R2 Standard	10.51.121.130	00-50-56-8F-5E-C3	4.1.0.8	Running	Now
	WIN-NN1196DIJGV	...-NN1196DIJGV\lior	Windows 8	10.51.121.98	00-50-56-8F-49-91	4.1.0.8	Running	Now
	WIN-U8A5CLOII1R	...-U8A5CLOII1R\root	Windows 8 Enterprise	10.51.121.125	00-50-56-8F-10-B5	4.1.0.8	Running	Now
lior8888								

Copyright © Fortinet Version 4.1.0.5

System Time (UTC -05:00) 16:13:20

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 security event was triggered.
- **OS:** Specifies the operating system of the communicating device on which the FortiEDR Collector is installed.
- **IP:** Specifies the IP address of the communicating device on which the FortiEDR Collector is installed.
- **MAC Address:** Specifies the physical address of the device. If a device has multiple MAC addresses, three dots (…) display. You can hover over the MAC Address to display the value (or values, in case of multiple MAC addresses) in a tooltip.



COLLECTORS (46/46)

⚠ 158 Unmanaged devices were found

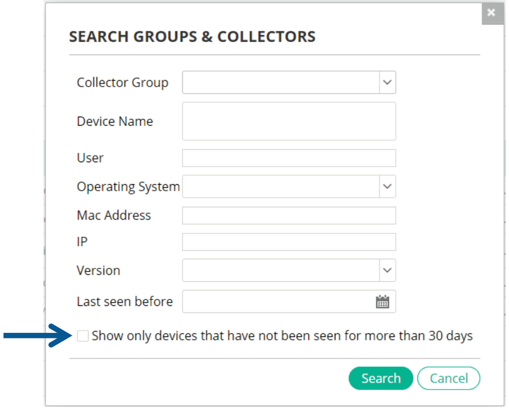
□ COLLECTOR GROUP NAME	DEVICE NAME	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	STATE	LAST SEEN
▷ □ group2 (0/0)								
▷ □ Insiders (2/2)								
▷ □ Linux (3/3)								
▷ □ lior1 (9/9)								
▷ □ lior8888 (0/0)								
▽ □ osx (5/5)								
	□ admin's Mac	None	OSX-10.10.5	10.51.104.56	00-1C-42-A1-8D-83	3.1.5.14	🟥 Disconnected	3 days ago
	□ admin's Mac (7)	None	OSX-10.11.6	10.51.104.63	00-1C-42-03-57-94	3.1.5.14	🟥 Disconnected	3 days ago
	□ LiorMacOSPara10-14	None	macOS 10.15.3 Catalina	10.51.104.70	00-1C-42-54-55-E0	3.1.5.14	🟥 Disconnected	4 days ago
	□ liors-osx	None	OSX-10.12.6	10.51.104.37	6A-00-01-B6-7E-A1, 6A...	3.1.5.14	🟥 Disconnected	3 days ago
	□ Mac	None	macOS 10.14.6 Mojave	10.51.104.22	00-1C-42-87-7A-D3	3.1.5.14	🟥 Disconnected	3 days ago
▷ □ oti (0/0)								

6A-00-01-B6-7E-A1, 6A-00-01-B6-7E-A0, 78-7B-8A-DC-99-34, F4-5C-89-A4-76-DF

- **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:

  SEARCH GROUPS & COLLECTORS

  Collector Group

  Device Name

  User

  Operating System

  Mac Address

  IP

  Version

  Last seen before

  □ Show only devices that have not been seen for more than 30 days

  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).

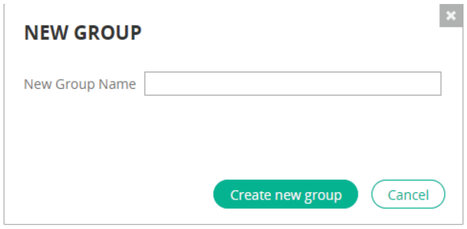
- **LAST SEEN:** Counts the number of days passed from the last time this Collector communicated with the Core.

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:



NEW GROUP

New Group Name

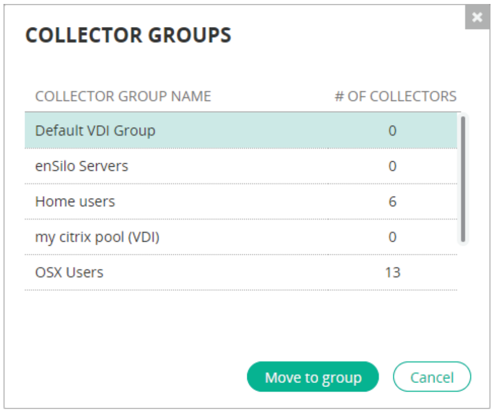
2 Enter any name for this group and click the **Create new group** button.

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:



COLLECTOR GROUPS

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

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:

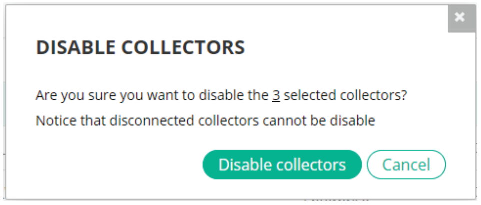
1 In the **COLLECTORS** page, select the checkboxes of the FortiEDR Collectors to be enabled. All selected Collectors must be in a Disabled (▨) state.

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:



DISABLE COLLECTORS

Are you sure you want to disable the 3 selected collectors?
Notice that disconnected collectors cannot be disable

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 62.

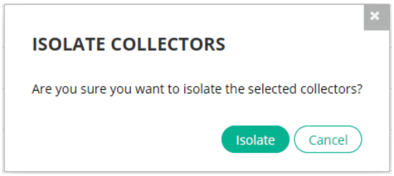
Note – Isolation mode takes effect upon any attempt to establish a network session after isolation mode has been initiated. Connections that were established before device isolation was initiated remain intact. The same applies for Communication Control denial configuration changes. Note that both Isolation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

To isolate a device:

1 In the **COLLECTORS** page, select the checkbox(es) of the FortiEDR Collector(s) that you want to isolate.

2 Click the down arrow on the Isolate ▾ button and select **Isolate**.

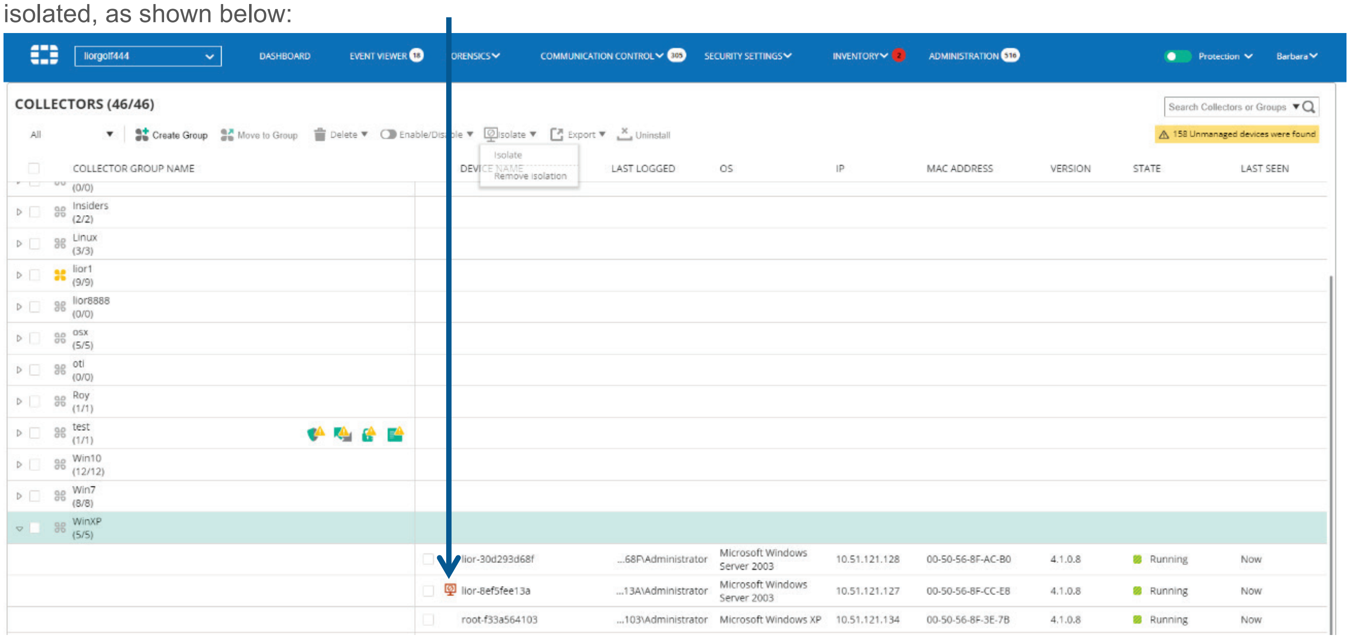
The following window displays:



ISOLATE COLLECTORS

Are you sure you want to isolate the selected collectors?

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:



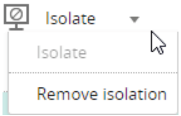
COLLECTORS (46/46)

⚠ 158 Unmanaged devices were found

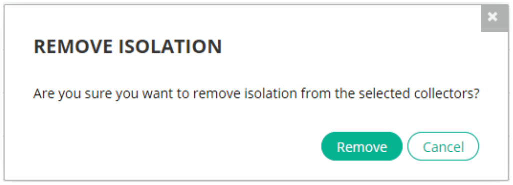
COLLECTOR GROUP NAME	DEVICE NAME	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	STATE	LAST SEEN
(0/0)								
Insiders (2/2)								
Linux (3/3)								
lior1 (9/9)								
lior8888 (0/0)								
osx (5/5)								
oti (0/0)								
Roy (1/1)								
test (1/1)								
Win10 (12/12)								
Win7 (8/8)								
WinXP (5/5)								
	lior-30d293d68f	...68F\Administrator	Microsoft Windows Server 2003	10.51.121.128	00-50-56-8F-AC-B0	4.1.0.8	🟩 Running	Now
	lior-8ef5fee13a	...13A\Administrator	Microsoft Windows Server 2003	10.51.121.127	00-50-56-8F-CC-E8	4.1.0.8	🟩 Running	Now
	root-f33a564103	...103\Administrator	Microsoft Windows XP	10.51.121.134	00-50-56-8F-3E-7B	4.1.0.8	🟩 Running	Now

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:



REMOVE ISOLATION

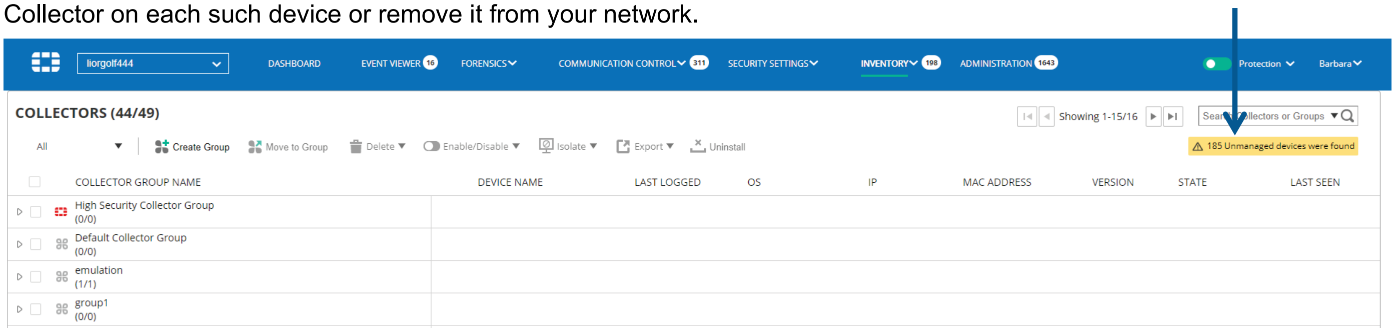
Are you sure you want to remove isolation from the selected collectors?

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.

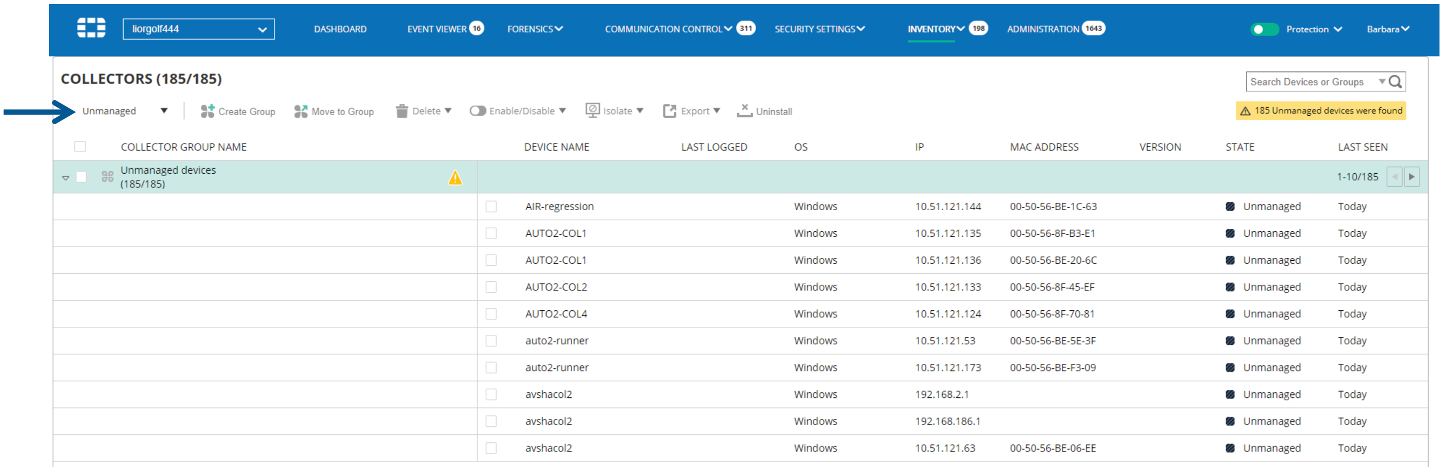


COLLECTORS (44/49)

⚠ 185 Unmanaged devices were found

COLLECTOR GROUP NAME	DEVICE NAME	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	STATE	LAST SEEN
High Security Collector Group (0/0)								
Default Collector Group (0/0)								
emulation (1/1)								
group1 (0/0)								

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



COLLECTORS (185/185)

⚠ 185 Unmanaged devices were found

COLLECTOR GROUP NAME	DEVICE NAME	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	STATE	LAST SEEN
Unmanaged devices (185/185) ⚠								
	AIR-regression		Windows	10.51.121.144	00-50-56-BE-1C-63		Unmanaged	Today
	AUTO2-COL1		Windows	10.51.121.135	00-50-56-8F-B3-E1		Unmanaged	Today
	AUTO2-COL1		Windows	10.51.121.136	00-50-56-BE-20-6C		Unmanaged	Today
	AUTO2-COL2		Windows	10.51.121.133	00-50-56-8F-45-EF		Unmanaged	Today
	AUTO2-COL4		Windows	10.51.121.124	00-50-56-8F-70-81		Unmanaged	Today
	auto2-runner		Windows	10.51.121.53	00-50-56-BE-5E-3F		Unmanaged	Today
	auto2-runner		Windows	10.51.121.173	00-50-56-BE-F3-09		Unmanaged	Today
	avshacol2		Windows	192.168.2.1			Unmanaged	Today
	avshacol2		Windows	192.168.186.1			Unmanaged	Today
	avshacol2		Windows	10.51.121.63	00-50-56-BE-06-EE		Unmanaged	Today

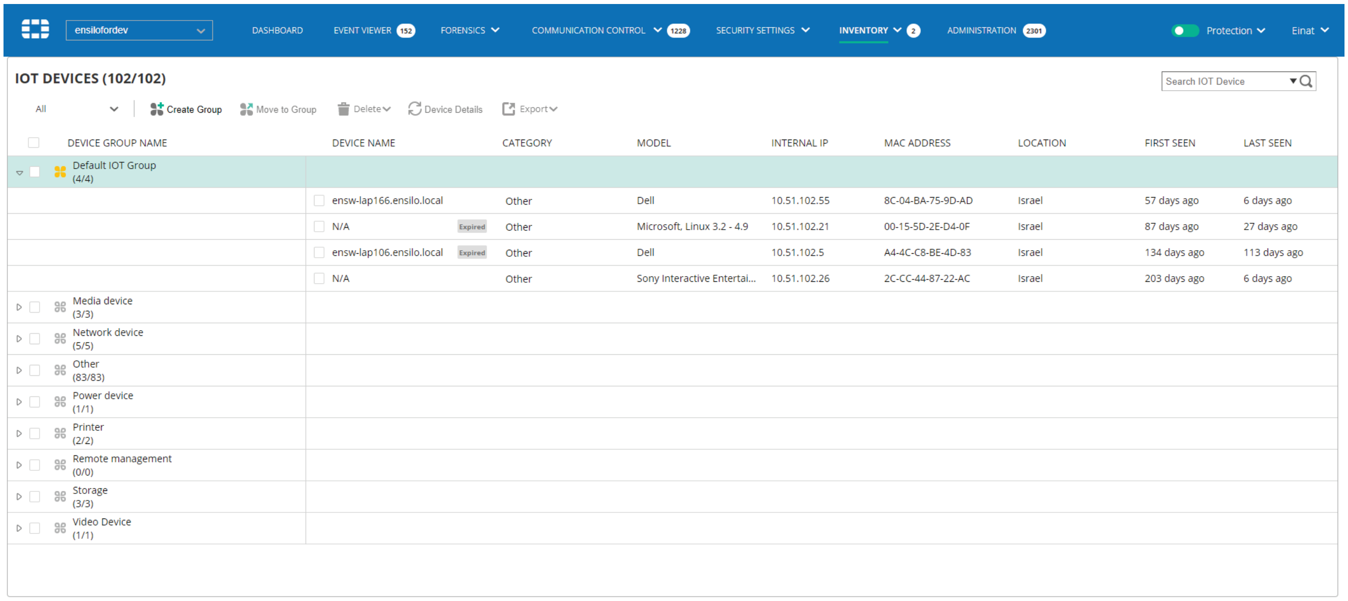
None of the action buttons at the top of the window are available for unmanaged devices, as there is no Collector installed on these devices.

IoT Devices

The **IOT DEVICES** page lists the non-workstation devices, such as printers, cameras and so on, that are part of your network. To access this page, click the down arrow next to **INVENTORY** and then select **IoT**.

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

FortiEDR provides you with visibility to any device in your network, including those on which FortiEDR components are not installed. IoTs are proactively discovered from existing FortiEDR Collectors. For more details, see the *IoT Device Discovery* section on page 213.



IOT DEVICES (102/102)

DEVICE GROUP NAME	DEVICE NAME	CATEGORY	MODEL	INTERNAL IP	MAC ADDRESS	LOCATION	FIRST SEEN	LAST SEEN
Default IOT Group (4/4)								
	ensw-lap166.ensilo.local	Other	Dell	10.51.102.55	8C-04-BA-75-9D-AD	Israel	57 days ago	6 days ago
	N/A Expired	Other	Microsoft, Linux 3.2 - 4.9	10.51.102.21	00-15-5D-2E-D4-0F	Israel	87 days ago	27 days ago
	ensw-lap106.ensilo.local Expired	Other	Dell	10.51.102.5	A4-4C-C8-BE-4D-83	Israel	134 days ago	113 days ago
	N/A	Other	Sony Interactive Entertai...	10.51.102.26	2C-CC-44-87-22-AC	Israel	203 days ago	6 days ago
Media device (3/3)								
Network device (5/5)								
Other (83/83)								
Power device (1/1)								
Printer (2/2)								
Remote management (0/0)								
Storage (3/3)								
Video Device (1/1)								

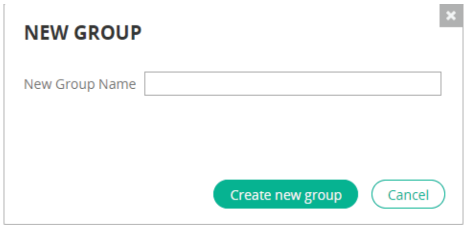
This page provides all the collected information about each discovered device, including its name, Category (device type), model number, internal IP address, MAC address, the physical location where the device was detected (based on its external IP address) and when it was first and last seen. FortiEDR presents all the information it collected for each device. Information that was not available for a device is marked as N/A in that device's row in the table. The New indication indicates that the device was discovered within the last three days. The Expired indication indicates that the device has not been seen for more than one week.

The default IoT Group to which new IoT devices are automatically added is marked with a yellow group icon ⁜. You can change to a different default IoT Group by clicking the group icon of another IoT Group. Alternatively, you can use Category-based grouping, where each new IoT device is automatically added to the group that represents its Category (for example, network devices, cameras, printers and so on).

Defining a New IoT Group

To define a new IoT Group:

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



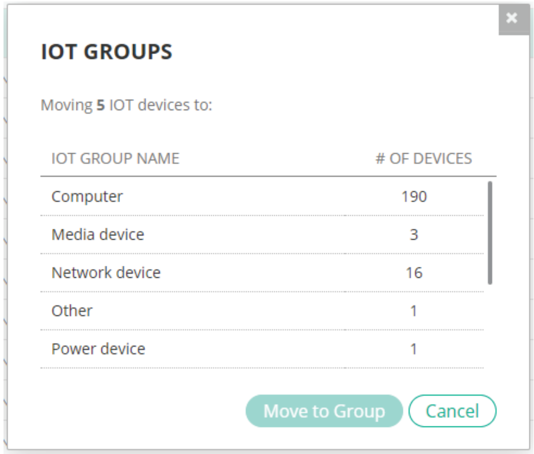
2 Enter any name for this group and click the **Create new group** button.

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:



IOT GROUPS

Moving **5** IOT devices to:

IOT GROUP NAME	# OF DEVICES
Computer	190
Media device	3
Network device	16
Other	1
Power device	1

3 Select the IoT Group to which to move the selected devices.

4 Click 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:

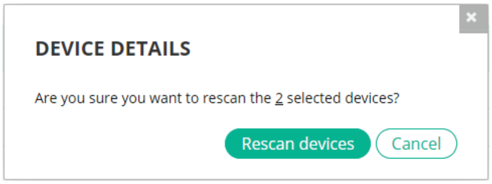
- Select the IoT Group’s/IoT device’s checkbox and then click the Delete button.

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.



DEVICE DETAILS

Are you sure you want to rescan the 2 selected devices?

2 Click the **Rescan devices** button.

Exporting IoT Information

To export the list of IoT devices:

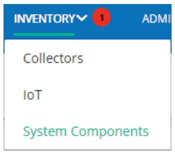
- Use the Export ▾ button and select **Excel** or **PDF**.

To export details for an IoT device:

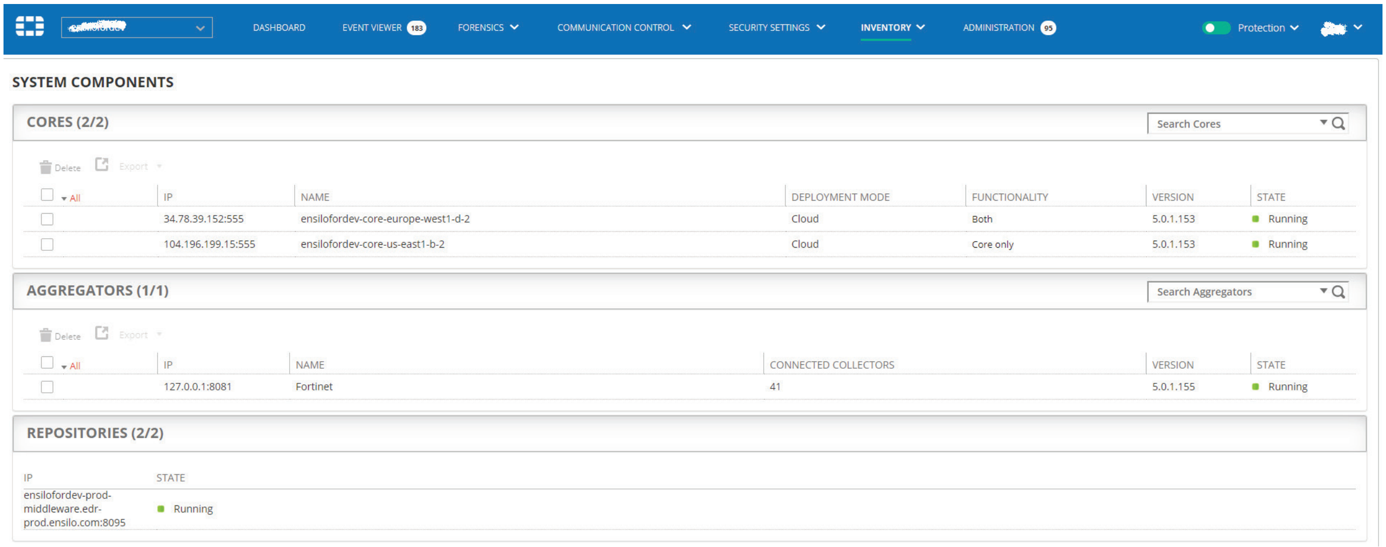
- Check the checkbox of the device of interest and then select Device Info under the **Export** button. You can only export details for one device at a time. This report exports all collected data for the IoT device of interest, including additional data beyond what is presented in the user interface.

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.



The following displays:



SYSTEM COMPONENTS

CORES (2/2)

□ All	IP	NAME	DEPLOYMENT MODE	FUNCTIONALITY	VERSION	STATE
□	34.78.39.152:555	ensilofordev-core-europe-west1-d-2	Cloud	Both	5.0.1.153	🟩 Running
□	104.196.199.15:555	ensilofordev-core-us-east1-b-2	Cloud	Core only	5.0.1.153	🟩 Running

AGGREGATORS (1/1)

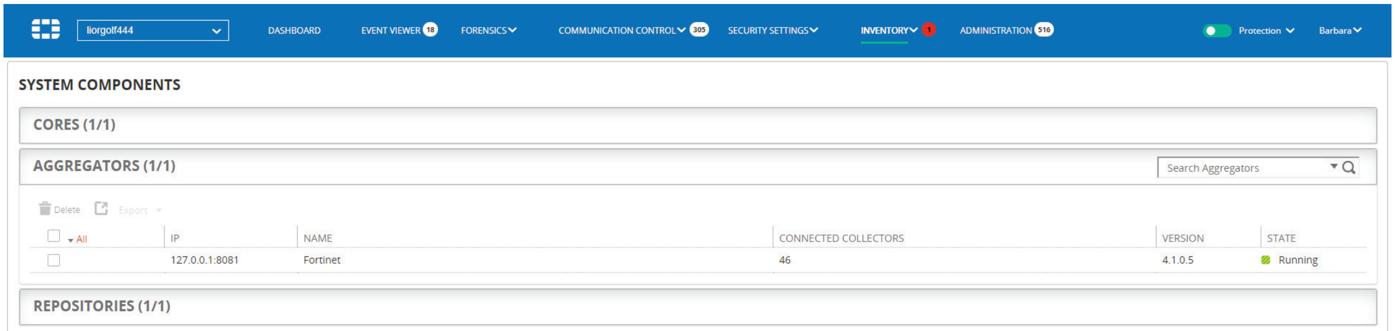
□ All	IP	NAME	CONNECTED COLLECTORS	VERSION	STATE
□	127.0.0.1:8081	Fortinet	41	5.0.1.155	🟩 Running

REPOSITORIES (2/2)

IP	STATE
ensilofordev-prod-middleware.edr-prod.ensilo.com:8095	🟩 Running

Aggregators

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



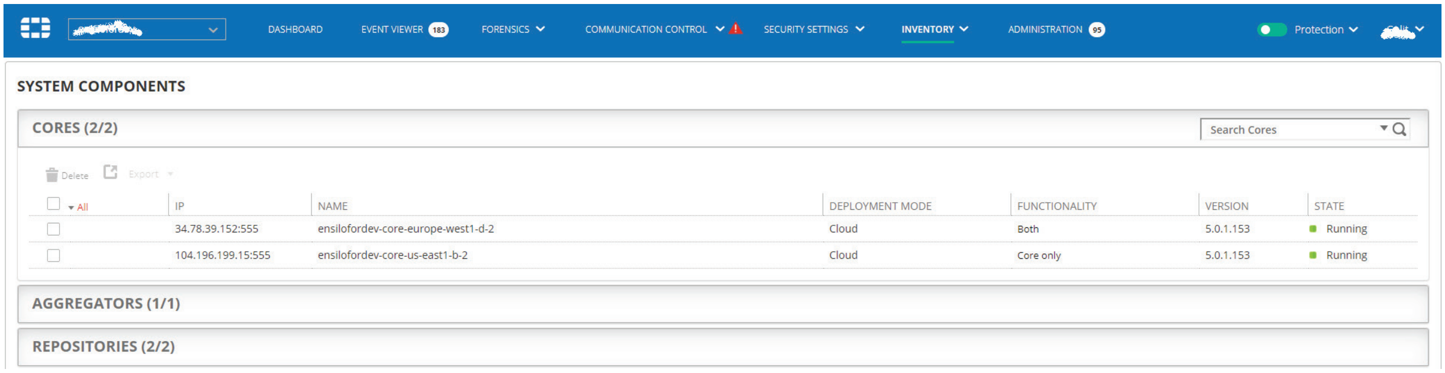
☐ All	IP	NAME	CONNECTED COLLECTORS	VERSION	STATE
☐	127.0.0.1:8081	Fortinet	46	4.1.0.5	🟩 Running

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 77).

Cores

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



☐ All	IP	NAME	DEPLOYMENT MODE	FUNCTIONALITY	VERSION	STATE
☐	34.78.39.152:555	ensilofordev-core-europe-west1-d-2	Cloud	Both	5.0.1.153	🟩 Running
☐	104.196.199.15:555	ensilofordev-core-us-east1-b-2	Cloud	Core only	5.0.1.153	🟩 Running

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). The following deployment options are available:
  - Cloud
  - On-premise

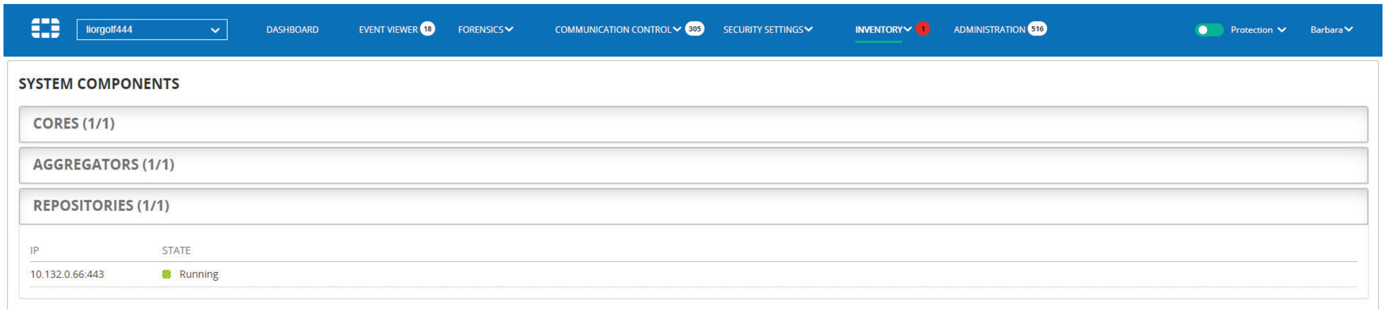
- **FUNCTIONALITY:** Specifies the core's functionality and enables you to modify it by selecting one of the following options –
  - **Core only –** Specifies that the system provides basic FortiEDR Core functionality: events processing, communication control handling, activity events proxy to the Repository and so on.
  - **JumpBox –** Specifies that the FortiEDR Core is used by the Central Manager (the central web user interface) as a JumpBox, while the JumpBox connects to the LDAP, sandbox or to the products. No basic Core functionalities are provided.

    Note – The jumpbox can also be used in the Cloud, not only when the Core is on-premise.
  - **Both –** Provides both **Core** and **JumpBox** functionality, as described above.

  Note – It is not mandatory to have a Core with JumpBox functionality. However, removing JumpBox functionality (by selecting the **Core only** option) may affect previously defined connectors, thus causing them to be nonfunctional. In this case, an appropriate message is displayed.
- **VERSION:** Specifies the version of the FortiEDR Core.
- **STATE:** Specifies the current state of the FortiEDR Core (page 77).

Repositories

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



SYSTEM COMPONENTS

CORES (1/1)

AGGREGATORS (1/1)

REPOSITORIES (1/1)

IP	STATE
10.132.0.66:443	🟩 Running

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

- **IP:** Specifies the IP and port address of the communicating device on which the FortiEDR Repository is installed.
- **STATE:** Specifies the current state of the FortiEDR Repository.

Exporting Logs

The Export Logs feature enables you to retrieve technical information from the FortiEDR devices deployed in the organization, such as from Collectors, Cores, Aggregators and the Management server. The retrievable technical content describes the activities of each FortiEDR device. Typically, the technical content contains logs and statistical information. The retrieved technical content is password-protected. The password is **enCrypted**.

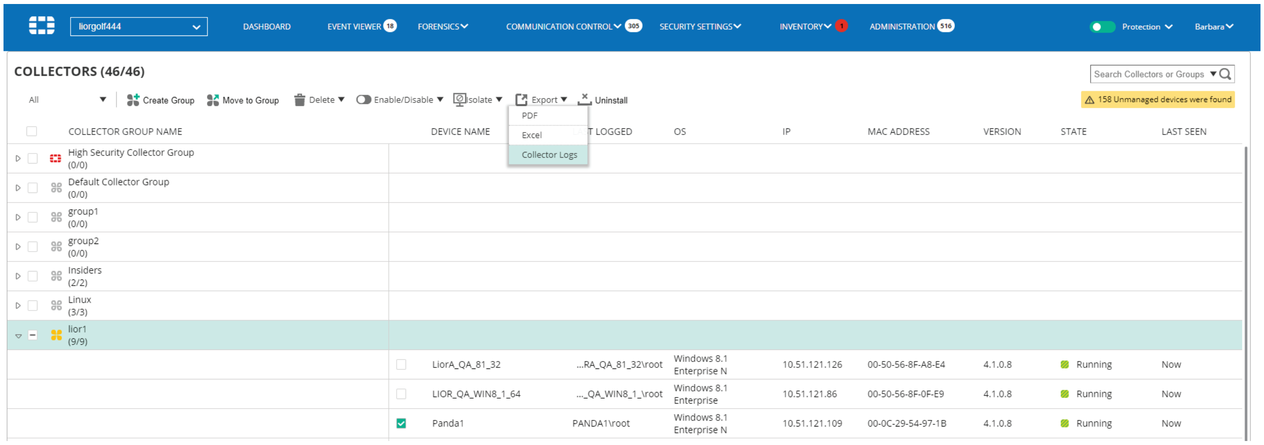
Logs only need to be retrieved when Fortinet technical support requests that you provide them. There is no need for you to analyze the data contained in the FortiEDR logs. You can retrieve logs for the following:

- **Exporting Logs for Collectors,** page 87
- **Exporting Logs for Cores,** page 88
- **Exporting Logs for Aggregators,** page 88

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.



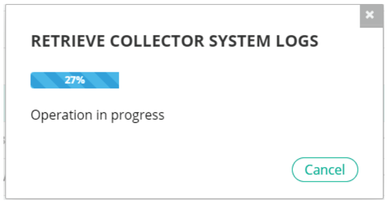
COLLECTORS (46/46)

⚠ 158 Unmanaged devices were found

	COLLECTOR GROUP NAME	DEVICE NAME	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	STATE	LAST SEEN
□	High Security Collector Group (0/0)								
□	Default Collector Group (0/0)								
□	group1 (0/0)								
□	group2 (0/0)								
□	Insiders (2/2)								
□	Linux (3/3)								
⊟	lior1 (9/9)								
□		LiorA_QA_81_32	...RA_QA_81_32\root	Windows 8.1 Enterprise N	10.51.121.126	00-50-56-8F-A8-E4	4.1.0.8	Running	Now
□		LIOR_QA_WIN8_1_64	..._QA_WIN8_1_\root	Windows 8.1 Enterprise	10.51.121.86	00-50-56-8F-0F-E9	4.1.0.8	Running	Now
☑		Panda1	PANDA1\root	Windows 8.1 Enterprise N	10.51.121.109	00-0C-29-54-97-1B	4.1.0.8	Running	Now

2 Click the down arrow on the **Export** dropdown menu and select **Collector Logs**.

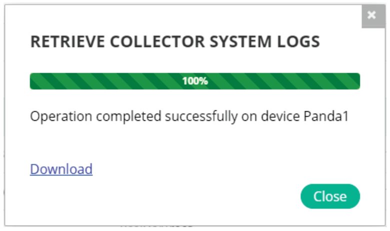
A progress window displays, showing the status of the Collector log retrieval process:



RETRIEVE COLLECTOR SYSTEM LOGS

Operation in progress

After the retrieval process completes, the following window displays:



RETRIEVE COLLECTOR SYSTEM LOGS

Operation completed successfully on device Panda1

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

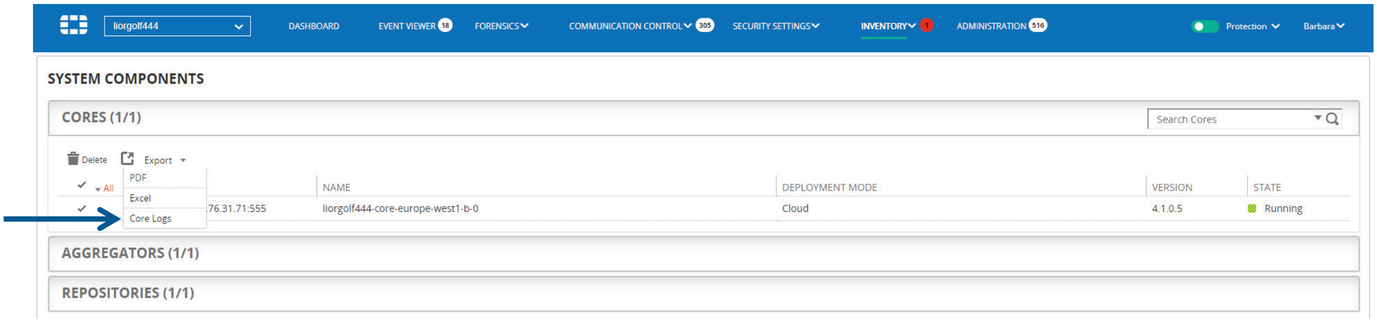
Exporting Logs for Cores

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.

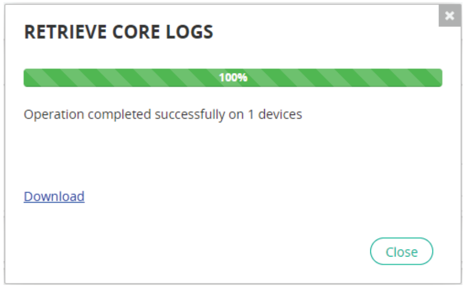
2 Click the down arrow on the **Export** dropdown menu and select **Core Logs**.



✓ All		NAME	DEPLOYMENT MODE	VERSION	STATE
✓	76.31.71:555	liorgolf444-core-europe-west1-b-0	Cloud	4.1.0.5	Running

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

After the retrieval process completes, the following window displays:


RETRIEVE CORE LOGS

Operation completed successfully on 1 devices

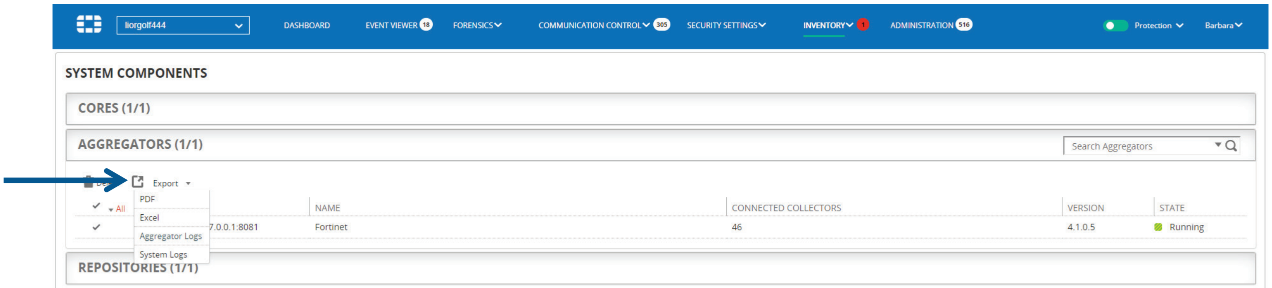
3 Click the **Download** link to automatically send the retrieved logs to Fortinet technical support.

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:



✓ All		NAME	CONNECTED COLLECTORS	VERSION	STATE
✓	7.0.0.1:8081	Fortinet	46	4.1.0.5	Running

- **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.

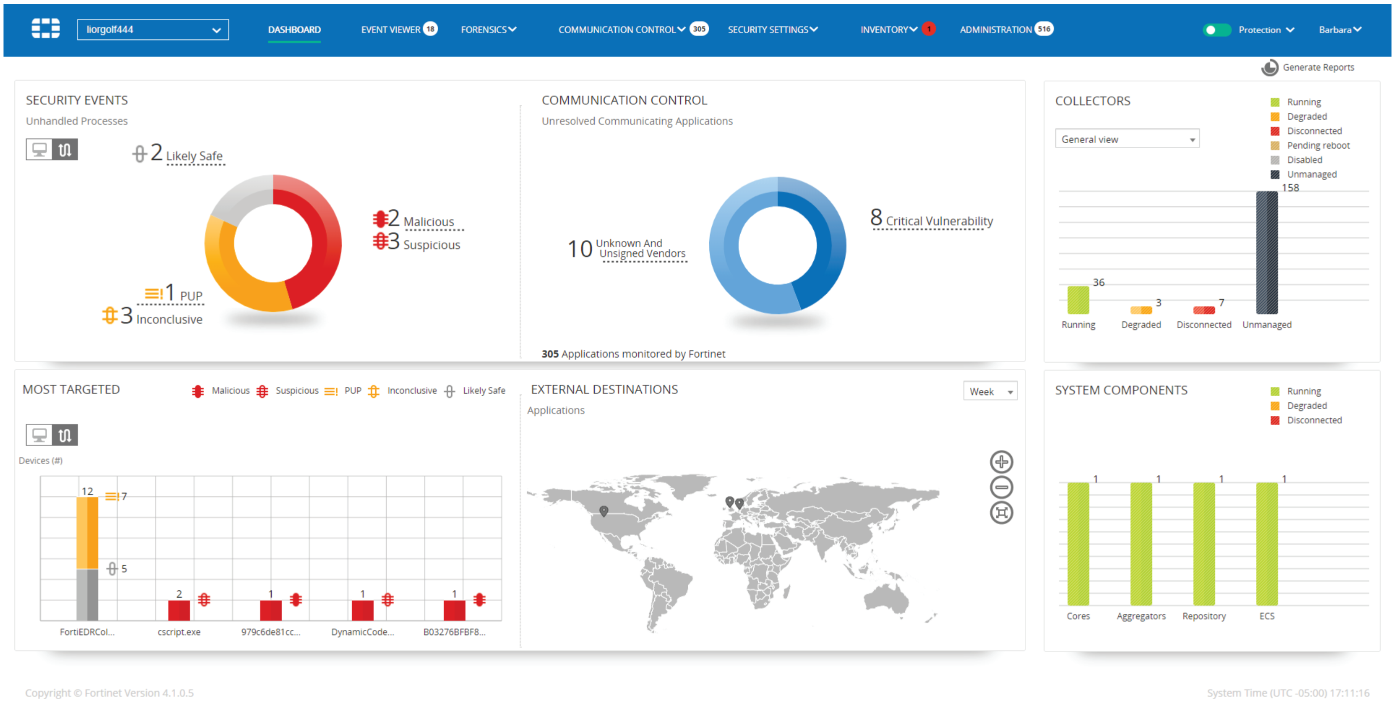
Click the **Download** link to automatically send the retrieved logs to Fortinet technical support.

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.

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

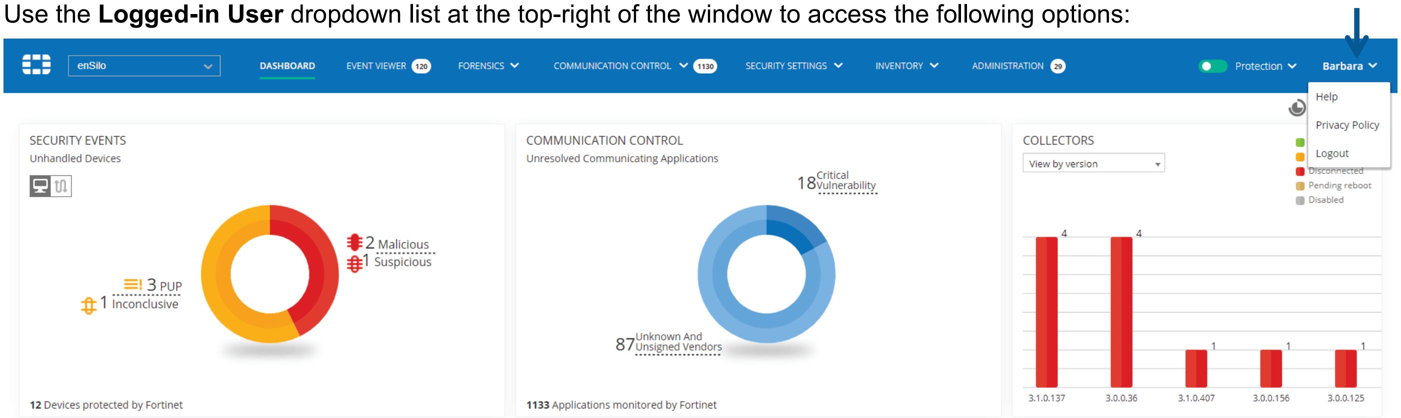
The Dashboard enables you to display two different slices or views of the data collected by FortiEDR:

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

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

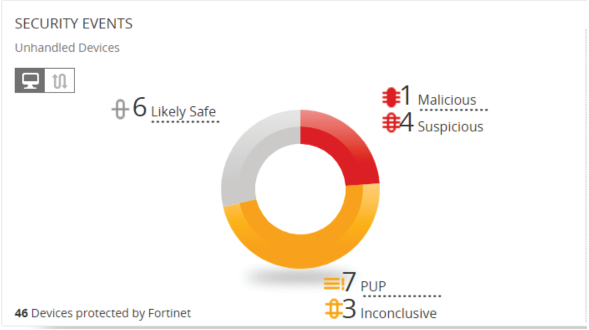
The information presented in the Dashboard represents an aggregation of events. For more details, you may refer to the *Event Aggregation* section on page 97. FortiEDR aggregates security events in both the Device view and the Process view in the Dashboard.

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

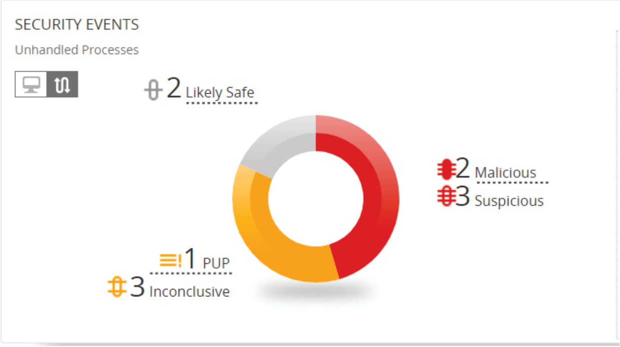


- **Help:** Enables you to download the latest version of the *FortiEDR Installation and Administration Guide*.
- **Privacy Policy:** Downloads the FortiEDR privacy policy.
- **Logout:** Exits the FortiEDR application.

Security Events Chart



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



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

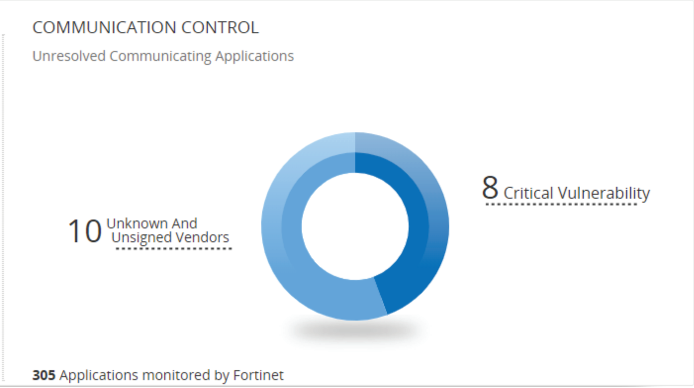
- **Red:** Critical
- **Yellow:** High
- **Grey:** Medium

Click this chart to drill down to the Event Viewer, which shows a filtered chart listing the unhandled security events (page 104) according to the classification (color) that you clicked in this chart.

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

Communication Control Chart

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


COMMUNICATION CONTROL
Unresolved Communicating Applications
10 Unknown And Unsigned Vendors
8 Critical Vulnerability
305 Applications monitored by Fortinet

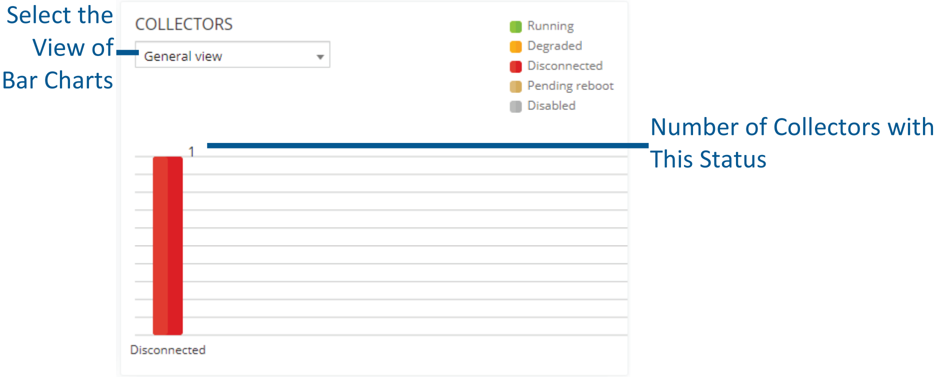
Click a box in the chart to drill down to the Communication Control.

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 76.

The bar chart is color-coded and numbered to indicate the distribution of statuses (page 90) among the components within the operating system group.

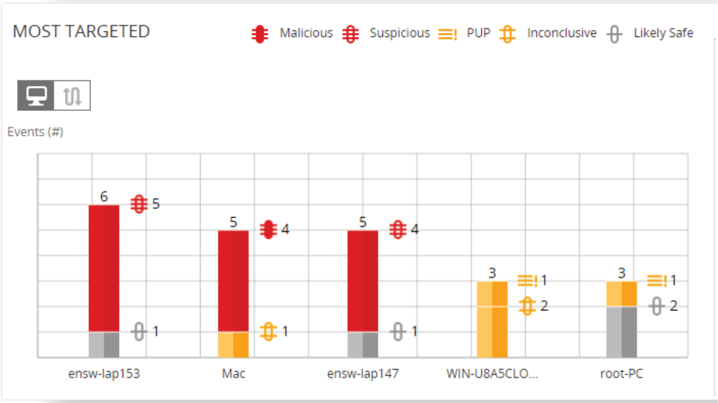
Each bar chart indicates the Version or the Operating System of that component, according to the option that you selected in the **View By** dropdown menu.



Click this chart to drill down to the relevant INVENTORY (page 74), which shows a filtered chart listing the Collectors with the selected Version or Operating System.

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

Most Targeted Charts

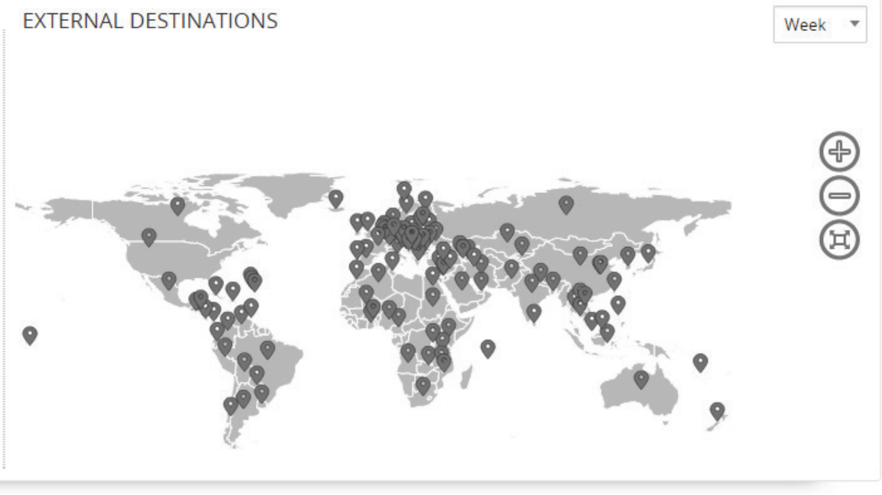


The **MOST TARGETED** chart displays the history of the most-infected and targeted processes, applications and devices. This chart is color-coded according to the classification of the attacks. The information is displayed per last day, last week or last month, according to your selection.

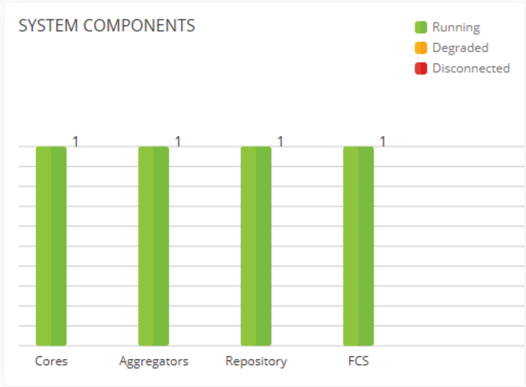
Click this chart to drill down to the Event Viewer (page 97), which shows a filtered chart listing the security events for the selected process or device.

External Destinations

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



System Components



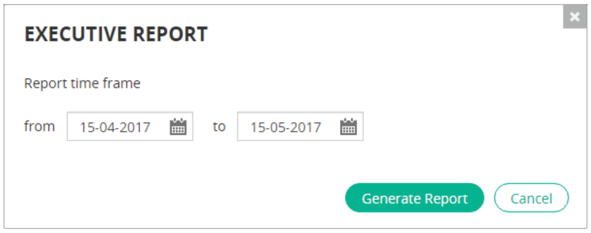
The **SYSTEM COMPONENTS** chart shows the status of the Cores, Aggregators, Threat Hunting Repository and FCS.

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:



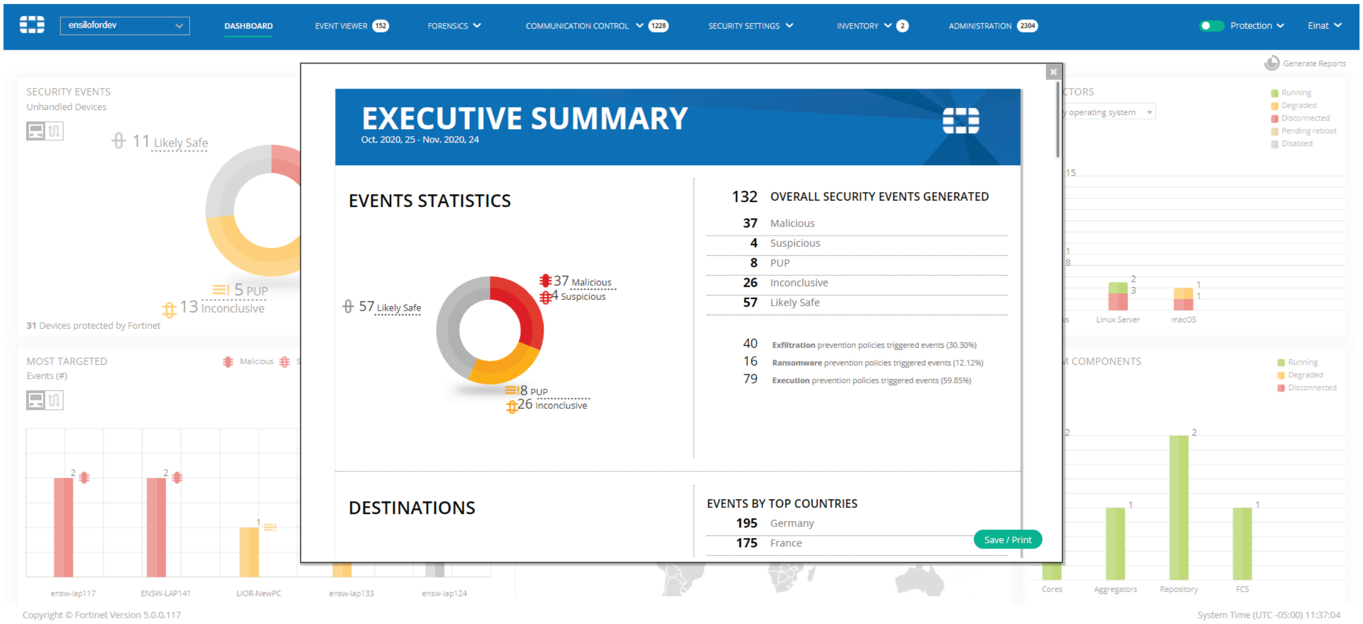
EXECUTIVE REPORT

Report time frame

from 15-04-2017 to 15-05-2017

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.



EXECUTIVE SUMMARY

Oct. 2020, 25 - Nov. 2020, 24

EVENTS STATISTICS

132	OVERALL SECURITY EVENTS GENERATED
37	Malicious
4	Suspicious
8	PUP
26	Inconclusive
57	Likely Safe

40	**Exfiltration** prevention policies triggered events (30.30%)
16	**Ransomware** prevention policies triggered events (12.12%)
79	**Execution** prevention policies triggered events (59.85%)

DESTINATIONS

EVENTS BY TOP COUNTRIES

195	Germany
175	France

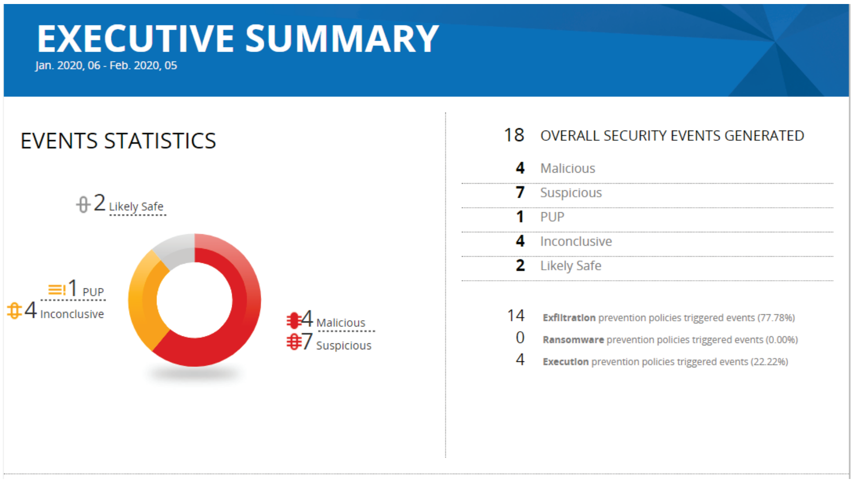
4 Click **Save/Print** to save or print the report.

The report presents several sections of information, as follows:

- **Event Statistics,** page 94
- **Destinations,** page 94
- **Most-targeted Devices,** page 95
- **Most-targeted Processes,** page 95
- **Communication Control,** page 95
- **System Components,** page 96
- **License Status,** page 96

Event Statistics

The Event Statistics section of the Executive Summary report displays a breakdown of the security events created during the timeframe of the report. Security events are classified by classification. The total number and percentage of events triggered by the Exfiltration and Ransomware policies are also displayed. For more details, see *Chapter 6*, *Event Viewer* on page 97.



EXECUTIVE SUMMARY

Jan. 2020, 06 - Feb. 2020, 05

EVENTS STATISTICS

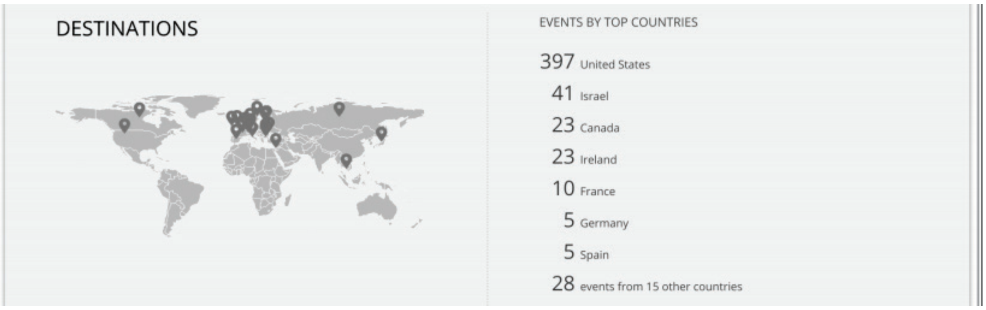
18 OVERALL SECURITY EVENTS GENERATED

4	Malicious
7	Suspicious
1	PUP
4	Inconclusive
2	Likely Safe

14 **Exfiltration** prevention policies triggered events (77.78%)
0 **Ransomware** prevention policies triggered events (0.00%)
4 **Execution** prevention policies triggered events (22.22%)

Destinations

The Destination section of the Executive Summary report displays a map of all the destinations for the security events triggered during the timeframe of the report. The names of the top seven countries with the most security events are shown. There is a pin on the map for each represented country. For more details, see the *External Destinations* section on page 92.



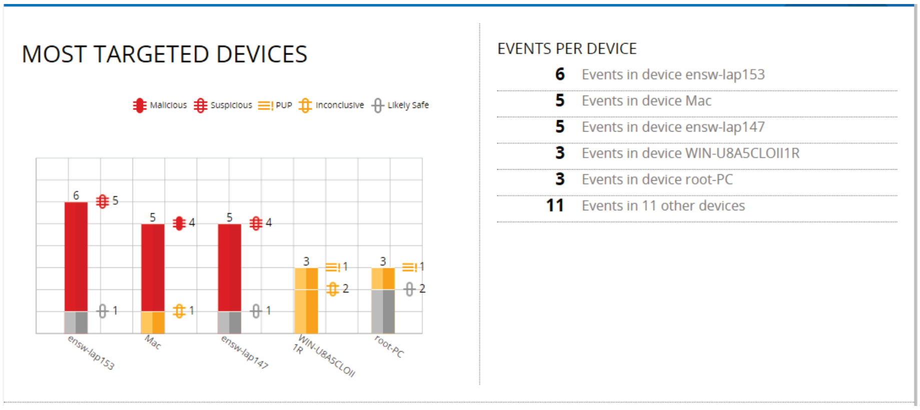
DESTINATIONS

EVENTS BY TOP COUNTRIES

397	United States
41	Israel
23	Canada
23	Ireland
10	France
5	Germany
5	Spain
28	events from 15 other countries

Most-targeted Devices

The Most Targeted Devices section of the Executive Summary report displays all the security events in the system during the timeframe of the report. A breakdown for the top-five most-targeted devices is shown. For more details, see the *Most Targeted Charts* section on page 92.



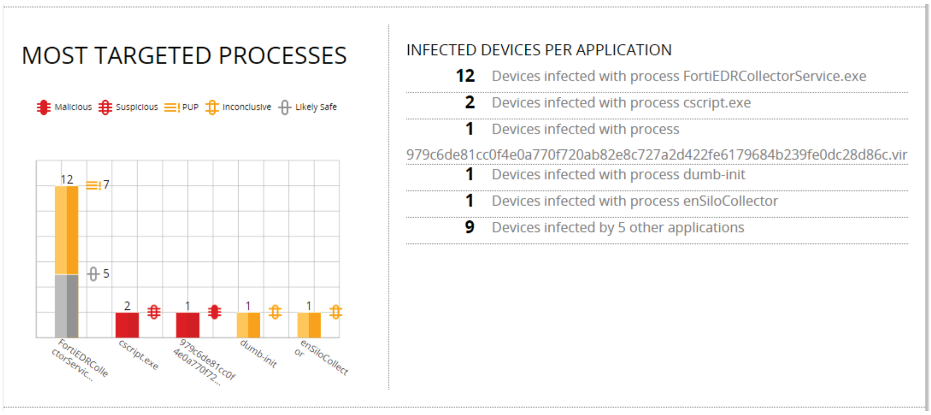
MOST TARGETED DEVICES

EVENTS PER DEVICE

6	Events in device ensw-lap153
5	Events in device Mac
5	Events in device ensw-lap147
3	Events in device WIN-U8A5CLOII1R
3	Events in device root-PC
11	Events in 11 other devices

Most-targeted Processes

The Most Targeted Processes section of the Executive Summary report displays all the security events in the system during the timeframe of the report. A breakdown for the top-five most-targeted processes is shown. For more details, see the *Most Targeted Charts* section on page 92.



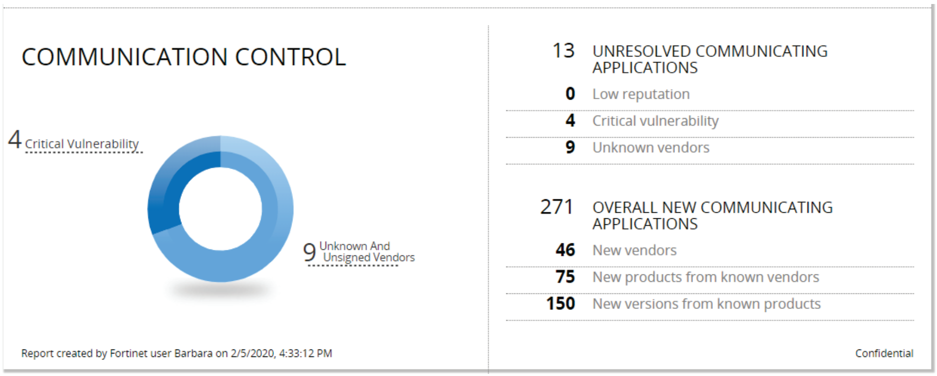
MOST TARGETED PROCESSES

INFECTED DEVICES PER APPLICATION

12	Devices infected with process FortiEDRCollectorService.exe
2	Devices infected with process cscript.exe
1	Devices infected with process 979c6de81cc0f4e0a770f720ab82e8c727a2d422fe6179684b239fe0dc28d86c.vir
1	Devices infected with process dumb-init
1	Devices infected with process enSiloCollector
9	Devices infected by 5 other applications

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 123.



COMMUNICATION CONTROL

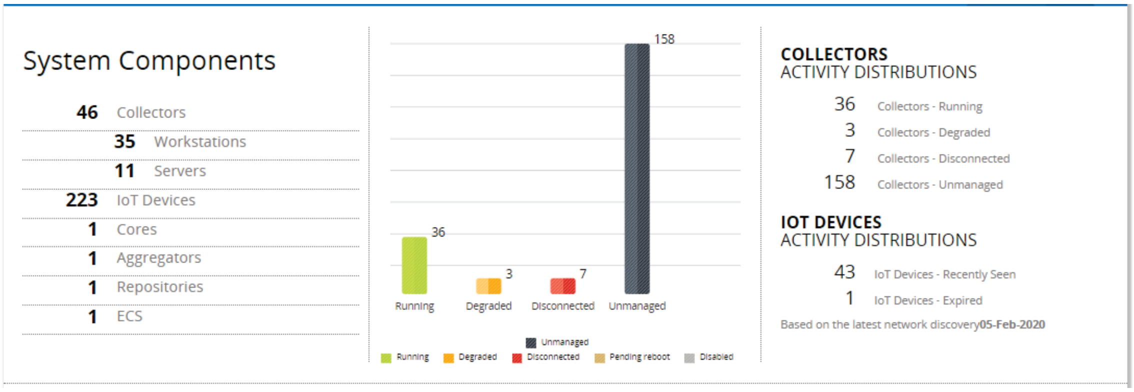
13	UNRESOLVED COMMUNICATING APPLICATIONS
0	Low reputation
4	Critical vulnerability
9	Unknown vendors
271	OVERALL NEW COMMUNICATING APPLICATIONS
46	New vendors
75	New products from known vendors
150	New versions from known products

Report created by Fortinet user Barbara on 2/5/2020, 4:33:12 PM

Confidential

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 82. For more details about unmanaged devices, see page 75.



System Components

46	Collectors
35	Workstations
11	Servers
223	IoT Devices
1	Cores
1	Aggregators
1	Repositories
1	ECS

COLLECTORS
ACTIVITY DISTRIBUTIONS

36	Collectors - Running
3	Collectors - Degraded
7	Collectors - Disconnected
158	Collectors - Unmanaged

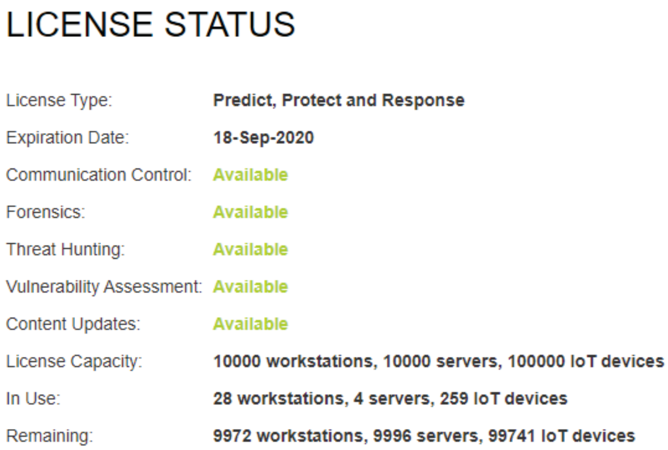
IOT DEVICES
ACTIVITY DISTRIBUTIONS

43	IoT Devices - Recently Seen
1	IoT Devices - Expired

Based on the latest network discovery**05-Feb-2020**

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 178.



LICENSE STATUS

License Type:	**Predict, Protect and Response**
Expiration Date:	**18-Sep-2020**
Communication Control:	**Available**
Forensics:	**Available**
Threat Hunting:	**Available**
Vulnerability Assessment:	**Available**
Content Updates:	**Available**
License Capacity:	**10000 workstations, 10000 servers, 100000 IoT devices**
In Use:	**28 workstations, 4 servers, 259 IoT devices**
Remaining:	**9972 workstations, 9996 servers, 99741 IoT devices**

Chapter 6 – EVENT VIEWER

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

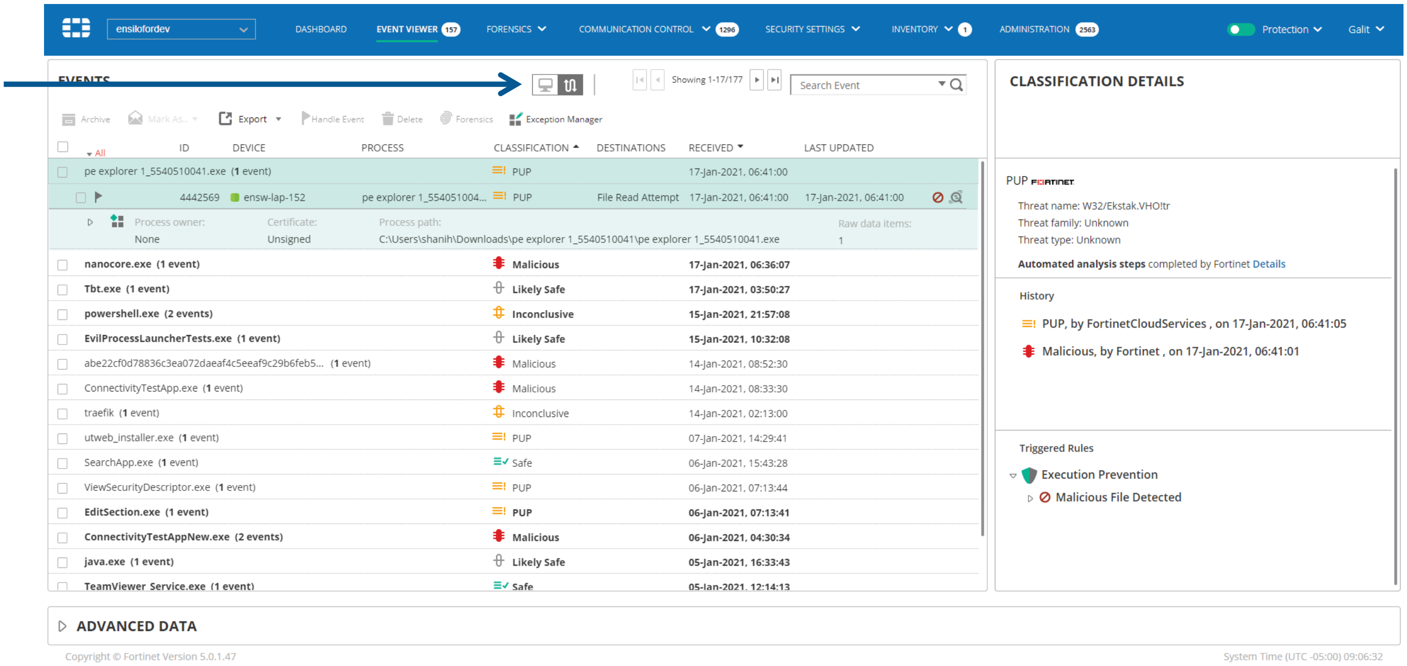
Introducing the Event Viewer

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 security event. A row is displayed for each event.

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

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

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



All	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
pe explorer 1_5540510041.exe (1 event)				PUP		17-Jan-2021, 06:41:00	
	4442569	ensw-lap-152	pe explorer 1_554051004...	PUP	File Read Attempt	17-Jan-2021, 06:41:00	17-Jan-2021, 06:41:00
nanocore.exe (1 event)				Malicious		17-Jan-2021, 06:36:07	
Tbt.exe (1 event)				Likely Safe		17-Jan-2021, 03:50:27	
powershell.exe (2 events)				Inconclusive		15-Jan-2021, 21:57:08	
EvilProcessLauncherTests.exe (1 event)				Likely Safe		15-Jan-2021, 10:32:08	
abe22cf0d78836c3ea072daeaf4c5eeaf9c29b6feb5... (1 event)				Malicious		14-Jan-2021, 08:52:30	
ConnectivityTestApp.exe (1 event)				Malicious		14-Jan-2021, 08:33:30	
traefik (1 event)				Inconclusive		14-Jan-2021, 02:13:00	
utweb_installer.exe (1 event)				PUP		07-Jan-2021, 14:29:41	
SearchApp.exe (1 event)				Safe		06-Jan-2021, 15:43:28	
ViewSecurityDescriptor.exe (1 event)				PUP		06-Jan-2021, 07:13:44	
EditSection.exe (1 event)				PUP		06-Jan-2021, 07:13:41	
ConnectivityTestAppNew.exe (2 events)				Malicious		06-Jan-2021, 04:30:34	
java.exe (1 event)				Likely Safe		05-Jan-2021, 16:33:43	
TeamViewer Service.exe (1 event)				Safe		05-Jan-2021, 12:14:13	

Process owner: None
Certificate: Unsigned
Process path: C:\Users\shanih\Downloads\pe explorer 1_5540510041\pe explorer 1_5540510041.exe
Raw data items: 1

PUP FORTINET
Threat name: W32/Ekstak.VHO!tr
Threat family: Unknown
Threat type: Unknown
Automated analysis steps completed by Fortinet Details

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

Triggered Rules
Execution Prevention
Malicious File Detected

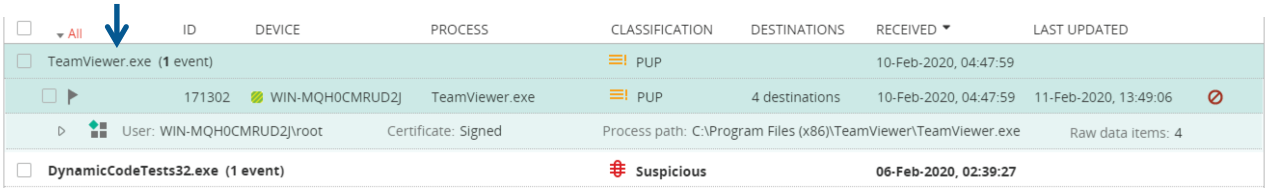
Copyright © Fortinet Version 5.0.1.47
System Time (UTC -05:00) 09:06:32

Note – Security events that were triggered by Saved Queries appear slightly different in the Event Viewer, as described page 161.

Event Aggregation

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

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



All	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
TeamViewer.exe (1 event)				PUP		10-Feb-2020, 04:47:59	
	171302	WIN-MQH0CMRUD2J	TeamViewer.exe	PUP	4 destinations	10-Feb-2020, 04:47:59	11-Feb-2020, 13:49:06
DynamicCodeTests32.exe (1 event)				Suspicious		06-Feb-2020, 02:39:27	

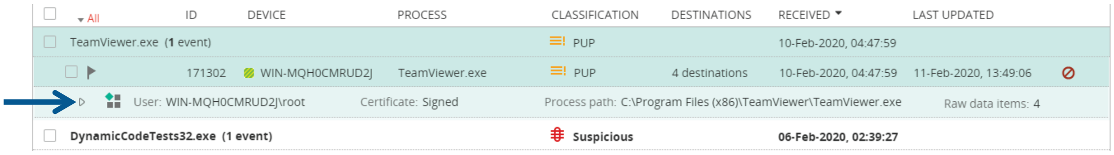
User: WIN-MQH0CMRUD2J\root
Certificate: Signed
Process path: C:\Program Files (x86)\TeamViewer\TeamViewer.exe
Raw data items: 4

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

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

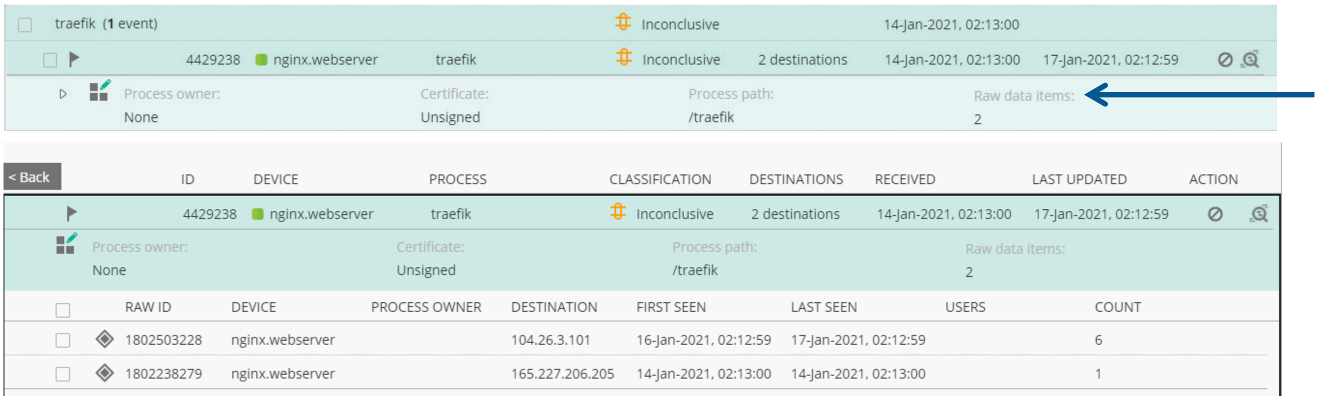
  In the Process view, the **Destinations** column indicates the number of destinations to which the process attempted to connect. If only one destination was accessed, its IP address is shown. If more than one destination was accessed, the number of destination IPs is shown in the **Destinations** column.

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



□ All	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED ▾	LAST UPDATED	
□ TeamViewer.exe (**1** event)				PUP		10-Feb-2020, 04:47:59		
□ ⚑	171302	WIN-MQH0CMRUD2J	TeamViewer.exe	PUP	4 destinations	10-Feb-2020, 04:47:59	11-Feb-2020, 13:49:06	⊘
▷ User: WIN-MQH0CMRUD2J\root		Certificate: Signed		Process path: C:\Program Files (x86)\TeamViewer\TeamViewer.exe			Raw data items: 4	
□ **DynamicCodeTests32.exe (1 event)**				**Suspicious**		**06-Feb-2020, 02:39:27**		

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



□ traefik (**1** event)				Inconclusive		14-Jan-2021, 02:13:00		
□ ⚑	4429238	nginx.webserver	traefik	Inconclusive	2 destinations	14-Jan-2021, 02:13:00	17-Jan-2021, 02:12:59	⊘
▷ Process owner: None		Certificate: Unsigned		Process path: /traefik			Raw data items: 2	

< Back	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED	ACTION
⚑	4429238	nginx.webserver	traefik	Inconclusive	2 destinations	14-Jan-2021, 02:13:00	17-Jan-2021, 02:12:59	⊘
Process owner: None		Certificate: Unsigned		Process path: /traefik			Raw data items: 2	

□	RAW ID	DEVICE	PROCESS OWNER	DESTINATION	FIRST SEEN	LAST SEEN	USERS	COUNT
□	1802503228	nginx.webserver		104.26.3.101	16-Jan-2021, 02:12:59	17-Jan-2021, 02:12:59		6
□	1802238279	nginx.webserver		165.227.206.205	14-Jan-2021, 02:13:00	14-Jan-2021, 02:13:00		1

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

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

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

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

- **EVENTS,** page 100
- **ADVANCED DATA,** page 102
- **CLASSIFICATION DETAILS,** page 120

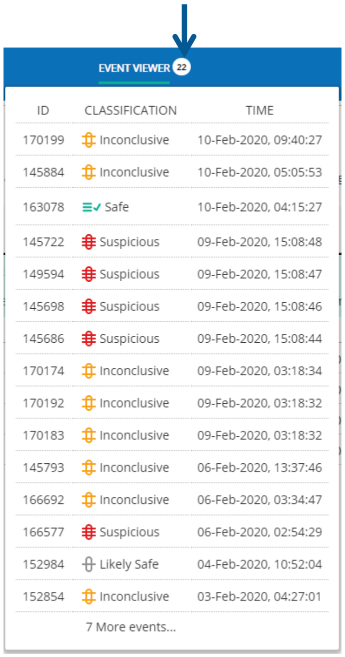
The following actions can be performed in the Event Viewer:

- **Marking an Event as Handled/Unhandled,** page 104
- **Defining Event Exceptions,** page 105
- **Marking an Event as Read/Unread,** page 117

- **Viewing Relevant Activity Events,** page 117
- **Viewing Expired Events,** page 117
- **Viewing Device Control Events,** page 118
- **Other Event Viewer Options,** page 118

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

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

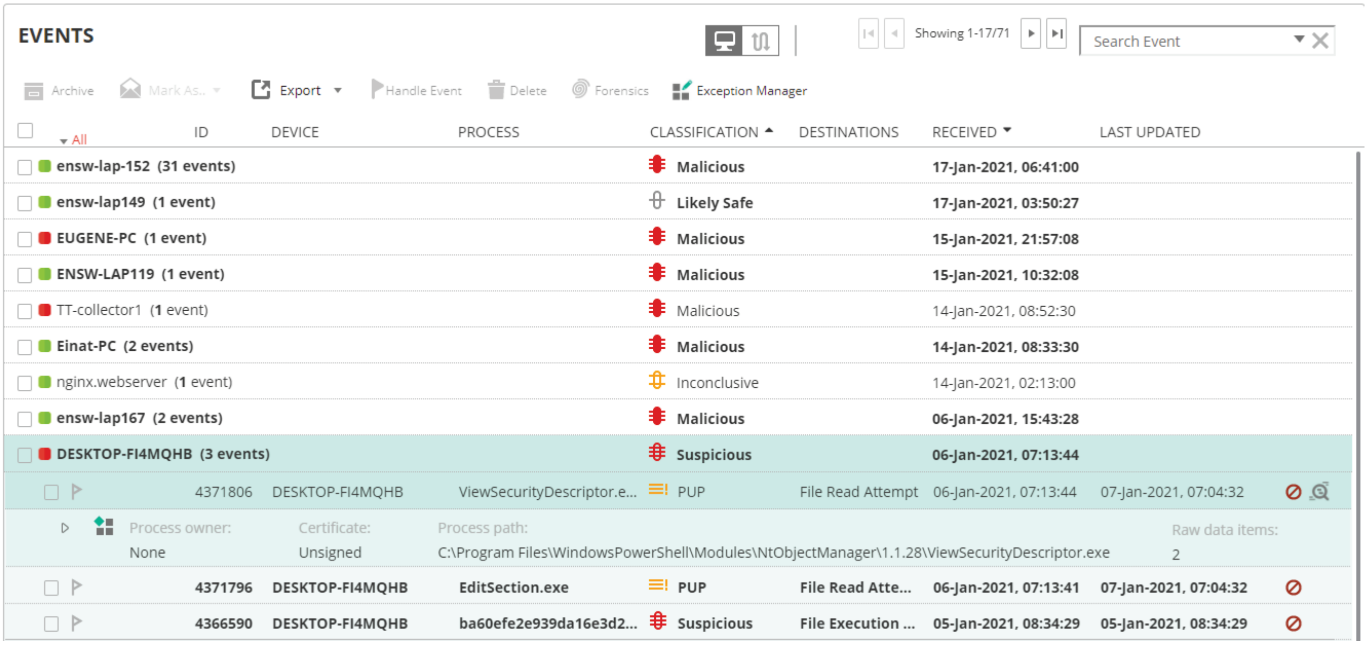


ID	CLASSIFICATION	TIME
170199	Inconclusive	10-Feb-2020, 09:40:27
145884	Inconclusive	10-Feb-2020, 05:05:53
163078	✓ Safe	10-Feb-2020, 04:15:27
145722	Suspicious	09-Feb-2020, 15:08:48
149594	Suspicious	09-Feb-2020, 15:08:47
145698	Suspicious	09-Feb-2020, 15:08:46
145686	Suspicious	09-Feb-2020, 15:08:44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

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

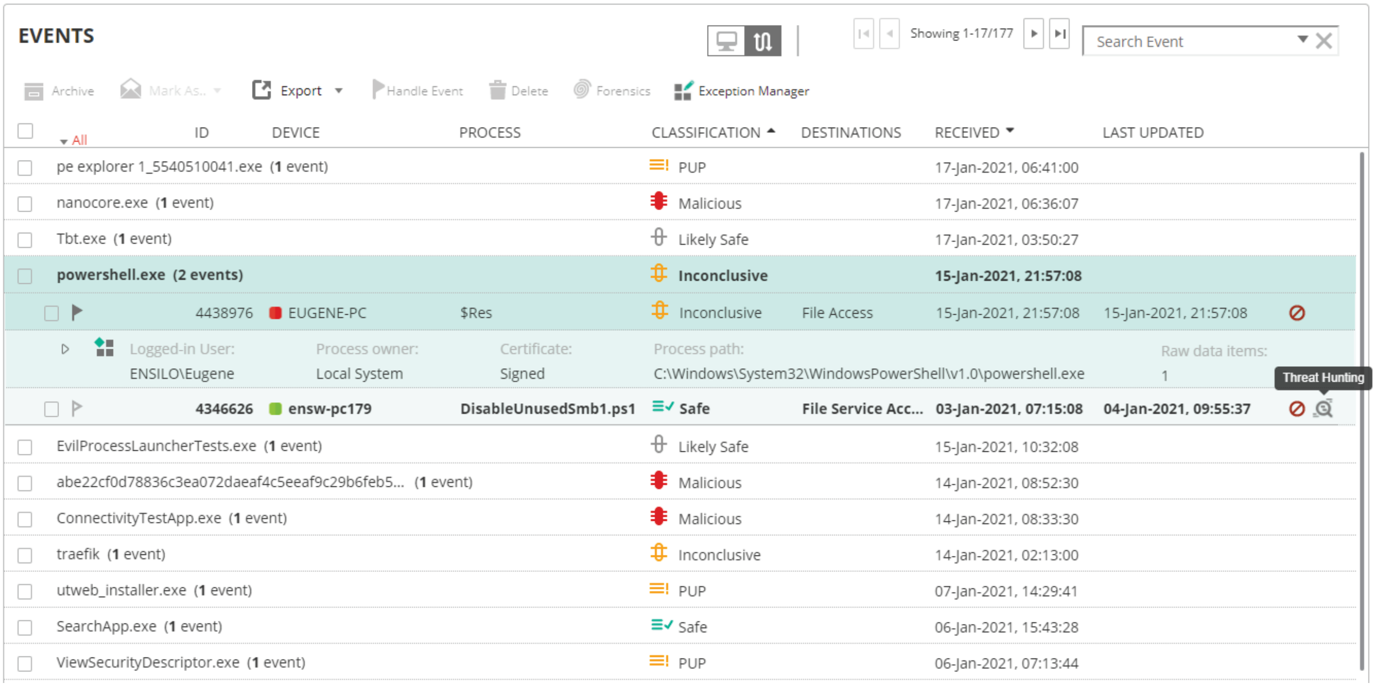
Events Pane

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



All	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
☐ 🟩 ensw-lap-152 (31 events)				Malicious		17-Jan-2021, 06:41:00	
☐ 🟩 ensw-lap149 (1 event)				Likely Safe		17-Jan-2021, 03:50:27	
☐ 🟥 EUGENE-PC (1 event)				Malicious		15-Jan-2021, 21:57:08	
☐ 🟩 ENSW-LAP119 (1 event)				Malicious		15-Jan-2021, 10:32:08	
☐ 🟥 TT-collector1 (1 event)				Malicious		14-Jan-2021, 08:52:30	
☐ 🟩 Einat-PC (2 events)				Malicious		14-Jan-2021, 08:33:30	
☐ 🟩 nginx.webserver (1 event)				Inconclusive		14-Jan-2021, 02:13:00	
☐ 🟩 ensw-lap167 (2 events)				Malicious		06-Jan-2021, 15:43:28	
☐ 🟥 DESKTOP-FI4MQHB (3 events)				Suspicious		06-Jan-2021, 07:13:44	
☐	4371806	DESKTOP-FI4MQHB	ViewSecurityDescriptor.e...	PUP	File Read Attempt	06-Jan-2021, 07:13:44	07-Jan-2021, 07:04:32
Process owner: None		Certificate: Unsigned	Process path: C:\Program Files\WindowsPowerShell\Modules\NtObjectManager\1.1.28\ViewSecurityDescriptor.exe				Raw data items: 2
☐	4371796	DESKTOP-FI4MQHB	EditSection.exe	PUP	File Read Atte...	06-Jan-2021, 07:13:41	07-Jan-2021, 07:04:32
☐	4366590	DESKTOP-FI4MQHB	ba60efe2e939da16e3d2...	Suspicious	File Execution ...	05-Jan-2021, 08:34:29	05-Jan-2021, 08:34:29

Device View



All	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
☐ pe explorer 1_5540510041.exe (1 event)				PUP		17-Jan-2021, 06:41:00	
☐ nanocore.exe (1 event)				Malicious		17-Jan-2021, 06:36:07	
☐ Tbt.exe (1 event)				Likely Safe		17-Jan-2021, 03:50:27	
☐ powershell.exe (2 events)				Inconclusive		15-Jan-2021, 21:57:08	
☐	4438976	🟥 EUGENE-PC	$Res	Inconclusive	File Access	15-Jan-2021, 21:57:08	15-Jan-2021, 21:57:08
Logged-in User: ENSILO\Eugene		Process owner: Local System	Certificate: Signed	Process path: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe			Raw data items: 1
☐	4346626	🟩 ensw-pc179	DisableUnusedSmb1.ps1	Safe	File Service Acc...	03-Jan-2021, 07:15:08	04-Jan-2021, 09:55:37
☐ EvilProcessLauncherTests.exe (1 event)				Likely Safe		15-Jan-2021, 10:32:08	
☐ abe22cf0d78836c3ea072daeaf4c5eeaf9c29b6feb5... (1 event)				Malicious		14-Jan-2021, 08:52:30	
☐ ConnectivityTestApp.exe (1 event)				Malicious		14-Jan-2021, 08:33:30	
☐ traefik (1 event)				Inconclusive		14-Jan-2021, 02:13:00	
☐ utweb_installer.exe (1 event)				PUP		07-Jan-2021, 14:29:41	
☐ SearchApp.exe (1 event)				Safe		06-Jan-2021, 15:43:28	
☐ ViewSecurityDescriptor.exe (1 event)				PUP		06-Jan-2021, 07:13:44	

Process View

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

- **View Indicator:** Indicates the view context for the security event aggregation. 🖥 displays for a device and ⇅ displays for a process.

- ⚑ **Handled/Not Handled:** Specifies whether any FortiEDR Central Manager user handled this security event, as described on page 104.
- **ID:** Specifies an automatically assigned unique identifier for each security event generated by FortiEDR. This identifier is particularly useful for security event tracking purposes when monitoring security events using an external system, such as a SIEM.
- **DEVICE:** Specifies the device name on which the security event has occurred.
- **PROCESS:** Specifies the process that is infected. This is not necessarily the process that made the connection establishment request (such as Firefox, which might be being controlled by the infected application). If the security event was triggered by a script, then the script name is specified.
- **CLASSIFICATION:** Specifies how malicious the security event is, if at all. Classifications are initially determined by FortiEDR. They can be changed either automatically as the result of additional post-processing, deep, thorough analysis and investigation by the FortiEDR Cloud Service (FCS) or manually. The FCS is a cloud-based, software-only service that determines the exact classification of security events and acts accordingly based on that classification – all with a high degree of accuracy. All Playbook policy actions are based on the final determination of the FCS. For more details, see *Playbook Policies* on page 57. 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 51.
- **RECEIVED:** Specifies the first time that this security event was triggered. For aggregations, the earliest received time is displayed.
- **LAST UPDATED:** Specifies the last time that the security event was triggered. For aggregations, the most-recent time is displayed.
- **ACTION:** 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 this exfiltration security event if the policy had been set to **Prevention** mode.
  - 🗎**: Log.** The security event was only logged and was not blocked.

For raw data items, the following information is available:

- **Device:** Specifies the device name on which the security event has occurred.
- **FIRST SEEN:** The Event Viewer aggregates the occurrences of the same security events into a single row when it represents the same attack on the same device. This timestamp specifies the first time this security event occurred. The row of this security event pops to the top of the list in the Event Viewer each time it occurs again.

  Note – If a change is made to the FortiEDR policy used by a specific FortiEDR Collector, then the security events before and after that change are not aggregated together.
- **LAST SEEN:** Specifies the most recent time this same security event occurred. See **FIRST SEEN** described above.
- **Destinations:** Specifies the external address for connection attempt security events.
- **Process Owner:** Specifies the user who ran the process that triggered the security event.
- **Process Type:** Specifies whether the infected process is 32-bit or 64-bit.
- **User:** Specifies the domain of the computer/user of the device.

- **Certificate:** Specifies whether the process or application have a 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 raw event on the same device.

Advanced Data

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

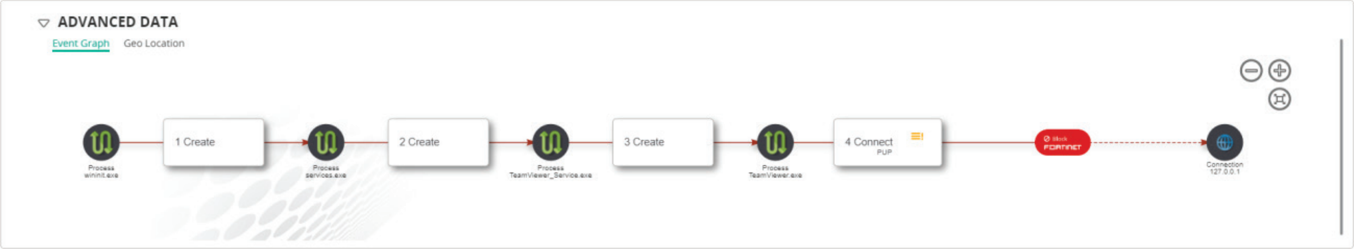
The **ADVANCED DATA** area contains three tabs, as follows:

- **Event Graph,** page 102
- **Geo Location,** page 102
- **Automated Analysis,** page 103

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

Event Graph

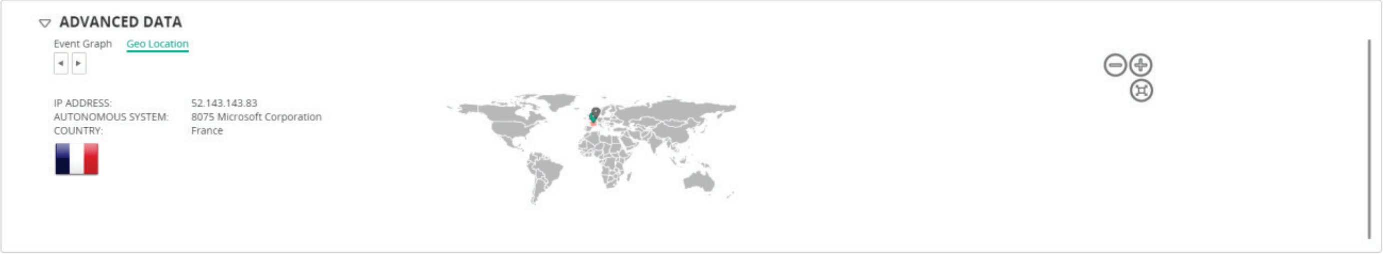
In addition to textual information that is displayed (described above), the **Event Graph** tab provides an image depicting the flow of operating system events that led up to the connection establishment request or the attempt to lock data. The picture is shown as a timeline from left to right (meaning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



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

Geo Location

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



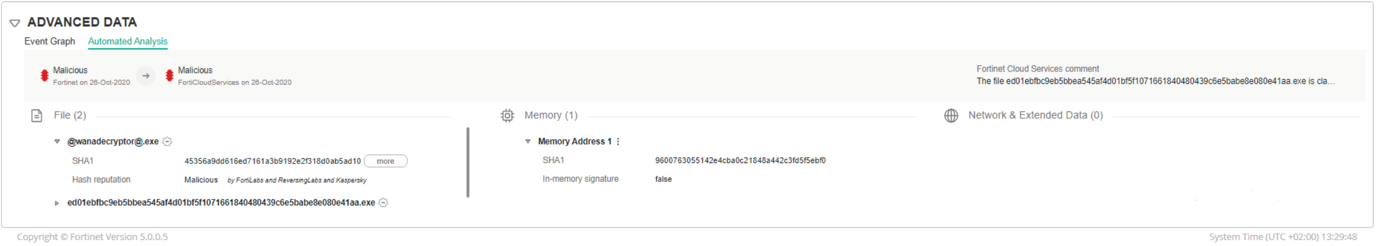
IP ADDRESS: 52.143.143.83
AUTONOMOUS SYSTEM: 8075 Microsoft Corporation
COUNTRY: France

An abundance of additional investigative tools and information are provided by FortiEDR's Forensic add-on (page 144).

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

Automated Analysis

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



ADVANCED DATA

Malicious
Fortinet on 26-Oct-2020

Malicious
FortiCloudServices on 26-Oct-2020

Fortinet Cloud Services comment
The file ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe is cla...

File (2)

@wanadecryptor@.exe

SHA1 45356a9dd616ed7161a3b9192e2f318d0ab5ad10 more
Hash reputation Malicious *by FortiLabs and ReversingLabs and Kaspersky*

ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe

Memory (1)

Memory Address 1

SHA1 9600763055142e4cba0c21848a442c3fd5f5ebf0
In-memory signature false

Network & Extended Data (0)

Copyright © Fortinet Version 5.0.0.5

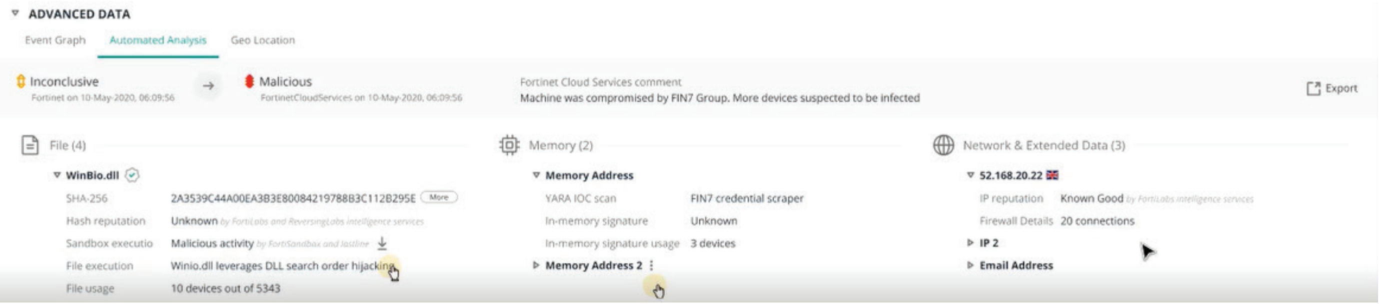
System Time (UTC +02:00) 13:29:48

The classification history of a security event is presented in the Classification Details area (see page 120) and shows the chronology for classifying a security event, as well as the automatic investigation and remediation actions performed by FortiEDR for that event.

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

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

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



ADVANCED DATA

Inconclusive
Fortinet on 10-May-2020, 06:09:56

Malicious
FortinetCloudServices on 10-May-2020, 06:09:56

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

File (4)

WinBio.dll

SHA-256 2A3539C44A00EA3B3E80084219788B3C112B295E More
Hash reputation Unknown *by FortiLabs and ReversingLabs intelligence services*
Sandbox executio Malicious activity *by FortiSandbox and Jostline*
File execution Winio.dll leverages DLL search order hijacking
File usage 10 devices out of 5343

Memory (2)

Memory Address

YARA IOC scan FIN7 credential scraper
In-memory signature Unknown
In-memory signature usage 3 devices

Memory Address 2

Network & Extended Data (3)

52.168.20.22

IP reputation Known Good *by FortiLabs intelligence services*
Firewall Details 20 connections

IP 2

Email Address

Marking a Security Event as Handled/Unhandled

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

To mark a security event as handled:

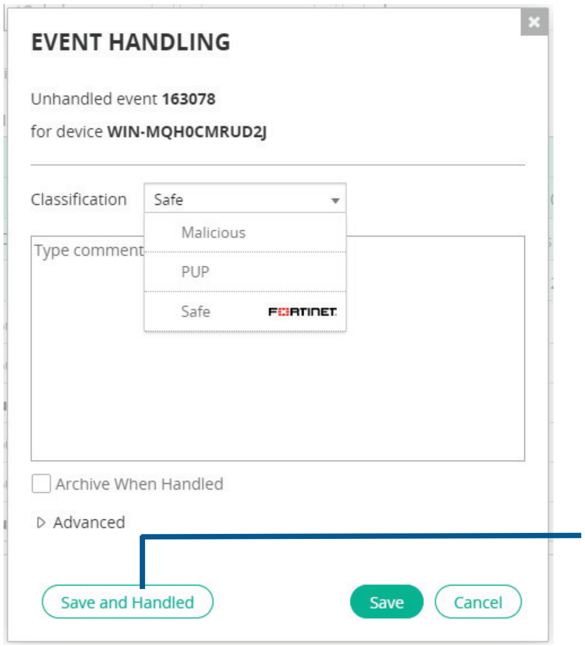
1 Select the rule's checkbox and then click the ⚑ Handle event button or just click the flag icon of the security event row. The Event Handling window displays.

Note – If an exception was already defined for this security event, then the words event includes exceptions are displayed at the top of the Event Handling window.

2 In the **Classification** dropdown list, change the classification for the security event, if needed. For more details, see page 105.

3 In the comments box, use free text to describe how you handled the security event.

4 Click the **Save as Handled** button. The flag icon next to the security event changes from dark gray ⚑ to light gray ⚐ to indicate to all users that it has been handled.



EVENT HANDLING

Unhandled event **163078**

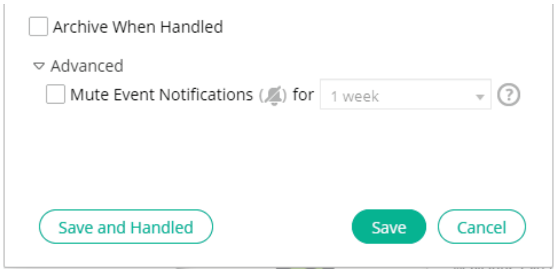
for device **WIN-MQHOCMRUD2J**

Classification: Safe

Click This Button

5 [Optional] Check the **Archive When Handled** checkbox to archive the security event after handling it. When you select this option, the security event is marked both as handled and as archived.

6 [Optional] Click the arrow to the left of **Advanced** to display the **Mute events notification** field. Select this checkbox if you want to mute the notifications for this security event. In addition, specify how long to mute the security event notifications. Notifications can be muted for **1 Week**, **1 Month**, **1 Year** or **Permanently**. When checked, you will not receive notifications whenever this security event is triggered. When using this option, click the **Save as Handled** button, which indicates that the security event has been both handled and saved.



Note – Security events with muted event notifications are indicated by the 🔕 icon in the Event Viewer.

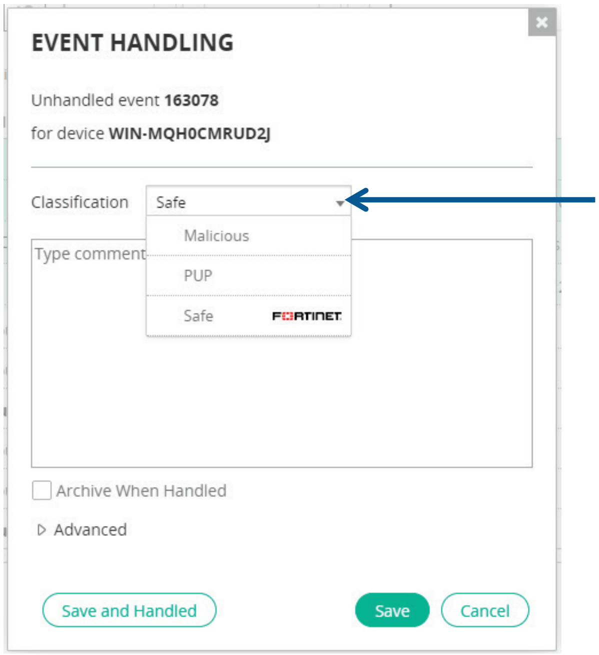
Manually Changing the Classification of a Security Event

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

To manually change the classification of a security event:

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

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



EVENT HANDLING

Unhandled event **163078**

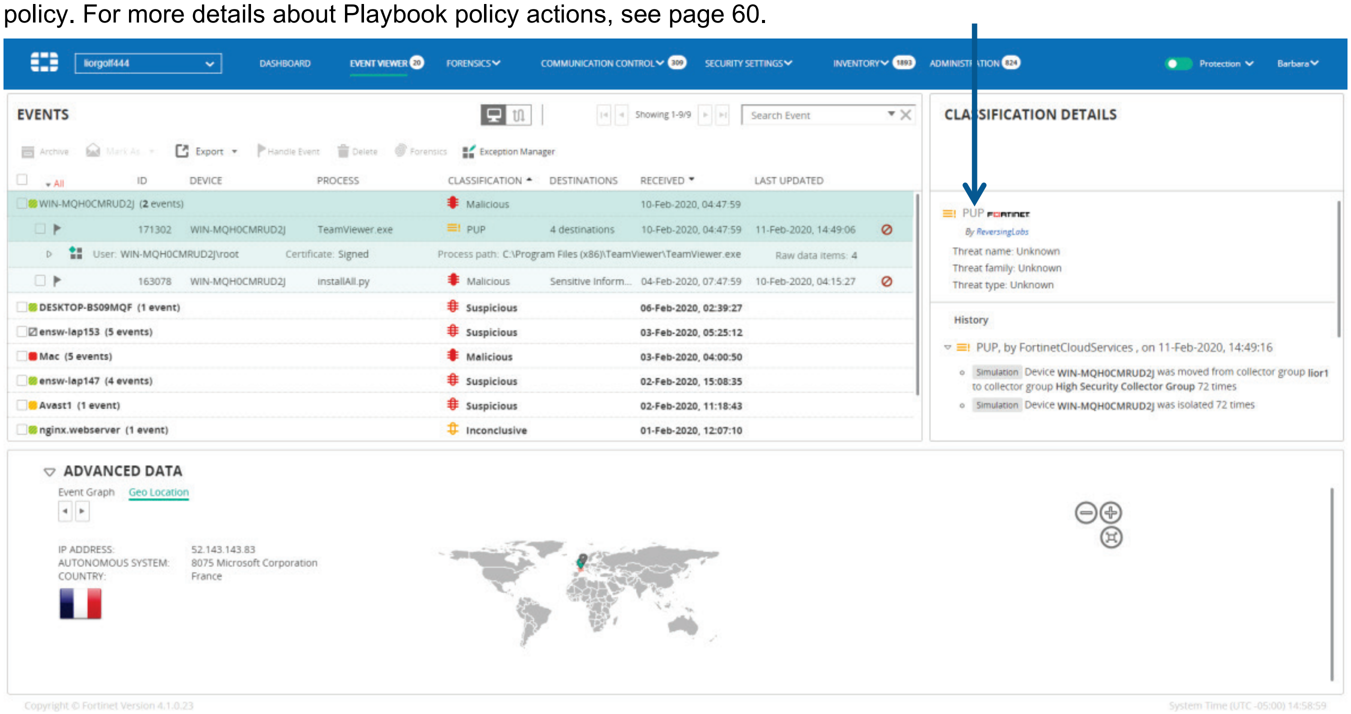
for device **WIN-MQH0CMRUD2J**

Classification: Safe

3 Click the Save button.

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

After changing the classification of a security 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 60.



All	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
WIN-MQHOCMRUD2J (2 events)				Malicious		10-Feb-2020, 04:47:59	
	171302	WIN-MQHOCMRUD2J	TeamViewer.exe	PUP	4 destinations	10-Feb-2020, 04:47:59	11-Feb-2020, 14:49:06
User: WIN-MQHOCMRUD2J\root			Certificate: Signed	Process path: C:\Program Files (x86)\TeamViewer\TeamViewer.exe			Raw data items: 4
	163078	WIN-MQHOCMRUD2J	installAll.py	Malicious	Sensitive Inform...	04-Feb-2020, 07:47:59	10-Feb-2020, 04:15:27
DESKTOP-BS09MQF (1 event)				Suspicious		06-Feb-2020, 02:39:27	
ensw-lap153 (5 events)				Suspicious		03-Feb-2020, 05:25:12	
Mac (5 events)				Malicious		03-Feb-2020, 04:00:50	
ensw-lap147 (4 events)				Suspicious		02-Feb-2020, 15:08:35	
Avast1 (1 event)				Suspicious		02-Feb-2020, 11:18:43	
nginx.webserver (1 event)				Inconclusive		01-Feb-2020, 12:07:10	

CLASSIFICATION DETAILS

PUP FORTINET

By ReversingLabs

Threat name: Unknown
Threat family: Unknown
Threat type: Unknown

History

PUP, by FortinetCloudServices , on 11-Feb-2020, 14:49:16

- Simulation Device WIN-MQHOCMRUD2J was moved from collector group lior1 to collector group High Security Collector Group 72 times
- Simulation Device WIN-MQHOCMRUD2J was isolated 72 times

IP ADDRESS: 52.143.143.83
AUTONOMOUS SYSTEM: 8075 Microsoft Corporation
COUNTRY: France

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

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

Defining Security Event Exceptions

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

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

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

Details describing how to edit an existing exception are described in the *Editing Security Event Exceptions* section on page 116. You can access the Exception Manager by clicking the Exception Manager button at the top of the Events pane or by selecting **SECURITY SETTINGS ➔ Exception Manager**. Additional options for managing exceptions are provided in the **SECURITY SETTINGS** tab, as described on page 65.

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

An exception pair specifies the **rule** that was violated and the **process** on which the violation occurred, including or excluding its entire location path. For more details, see page 58.

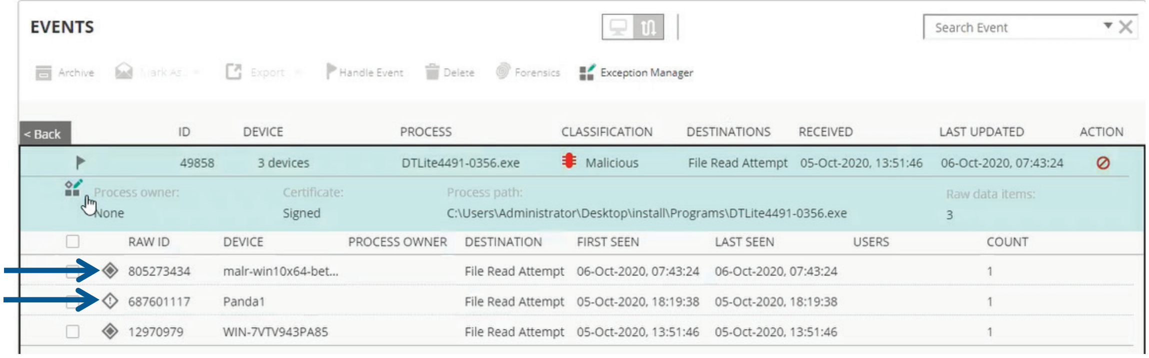
Note – After an exception is defined for a security event, new **identical** events are not triggered.

Security events that occurred in the past appear with an icon to indicate that an exception has been defined for them, even though at the time they were triggered, the exception did not exist. This icon on past security events serves as an indication to you that there is no need to create an exception for it, since one was already created (but after the event occurred).
In cases where an exception was defined for the security event but it does not fully cover all the existing occurrences or raw data items of this event, a slightly different icon is displayed, as described and shown below.
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 Destination*s.

Defining the Scope of an Exception

When defining an exception, it is important not to make it too broad or too narrow in scope, so that it properly identifies and *catches* the data items that you want. If an exception does not cover all the raw data items for a security event, the icon displays for that exception instead of the icon. This can happen, for example if the exception was defined only on part of the collector groups and the security event occurred on devices that are not part of the collector groups on which the exception was set.

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

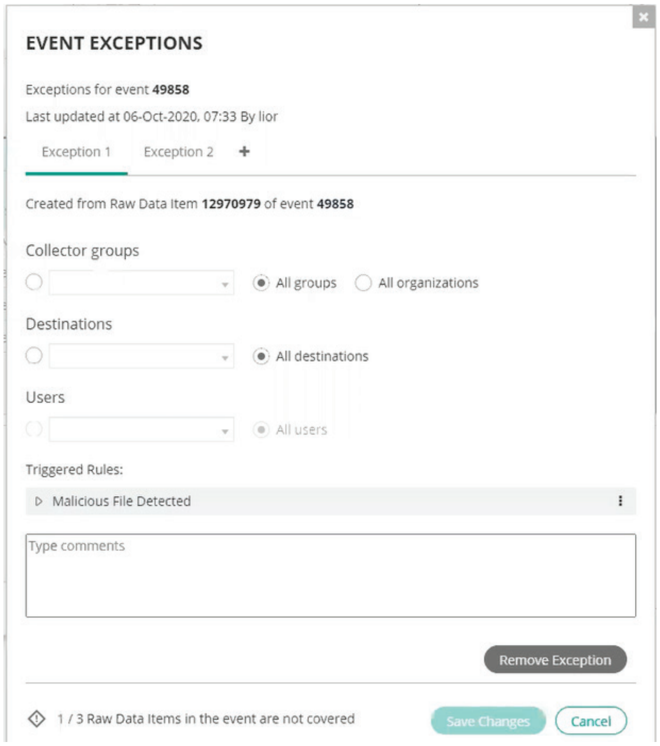


ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED	ACTION
49858	3 devices	DTLite4491-0356.exe	Malicious	File Read Attempt	05-Oct-2020, 13:51:46	06-Oct-2020, 07:43:24	⊘

Process owner:	Certificate:	Process path:	Raw data items:
None	Signed	C:\Users\Administrator\Desktop\install\Programs\DTLite4491-0356.exe	3

RAW ID	DEVICE	PROCESS OWNER	DESTINATION	FIRST SEEN	LAST SEEN	USERS	COUNT
◈ 805273434	malr-win10x64-bet...		File Read Attempt	06-Oct-2020, 07:43:24	06-Oct-2020, 07:43:24		1
◇ 687601117	Panda1		File Read Attempt	05-Oct-2020, 18:19:38	05-Oct-2020, 18:19:38		1
◈ 12970979	WIN-7VTV943PA85		File Read Attempt	05-Oct-2020, 13:51:46	05-Oct-2020, 13:51:46		1

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



EVENT EXCEPTIONS

Exceptions for event **49858**

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

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

Collector groups

○ ● All groups ○ All organizations

Destinations

○ ● All destinations

Users

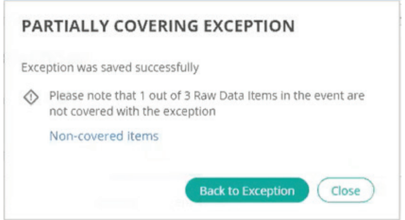
○ ● All users

Triggered Rules:

▷ Malicious File Detected

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

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



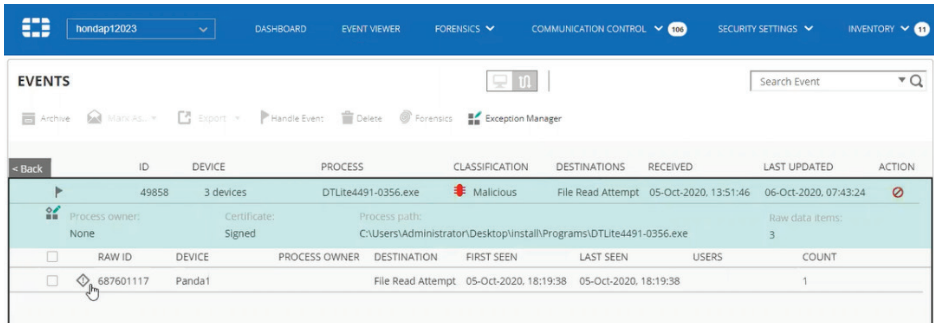
PARTIALLY COVERING EXCEPTION

Exception was saved successfully

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

Non-covered items

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



EVENTS

ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED	ACTION
49858	3 devices	DTLite4491-0356.exe	Malicious	File Read Attempt	05-Oct-2020, 13:51:46	06-Oct-2020, 07:43:24	⊘

Process owner: None

Certificate: Signed

Process path: C:\Users\Administrator\Desktop\install\Programs\DTLite4491-0356.exe

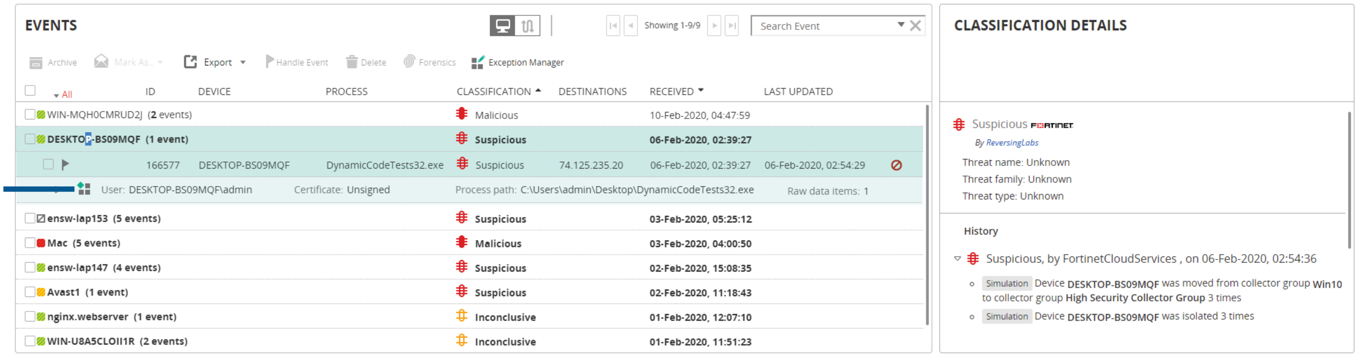
Raw data items: 3

□	RAW ID	DEVICE	PROCESS OWNER	DESTINATION	FIRST SEEN	LAST SEEN	USERS	COUNT
□	◇ 687601117	Panda1		File Read Attempt	05-Oct-2020, 18:19:38	05-Oct-2020, 18:19:38		1

Defining a Security Event as an Exception

To define a security event as an exception:

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



Click Here to Create an Exception

EVENTS

All	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
WIN-MQH0CMRUD2J (2 events)				Malicious		10-Feb-2020, 04:47:59	
DESKTOP-BS09MQF (1 event)				**Suspicious**		**06-Feb-2020, 02:39:27**	
	166577	DESKTOP-BS09MQF	DynamicCodeTests32.exe	Suspicious	74.125.235.20	06-Feb-2020, 02:39:27	06-Feb-2020, 02:54:29
ensw-lap153 (5 events)				**Suspicious**		**03-Feb-2020, 05:25:12**	
Mac (5 events)				**Malicious**		**03-Feb-2020, 04:00:50**	
ensw-lap147 (4 events)				**Suspicious**		**02-Feb-2020, 15:08:35**	
Avast1 (1 event)				**Suspicious**		**02-Feb-2020, 11:18:43**	
nginx.webserver (1 event)				**Inconclusive**		**01-Feb-2020, 12:07:10**	
WIN-U8A5CLOII1R (2 events)				**Inconclusive**		**01-Feb-2020, 11:51:23**	

User: DESKTOP-BS09MQF\admin Certificate: Unsigned Process path: C:\Users\admin\Desktop\DynamicCodeTests32.exe Raw data items: 1

CLASSIFICATION DETAILS

Suspicious FORTINET

By ReversingLabs

Threat name: Unknown

Threat family: Unknown

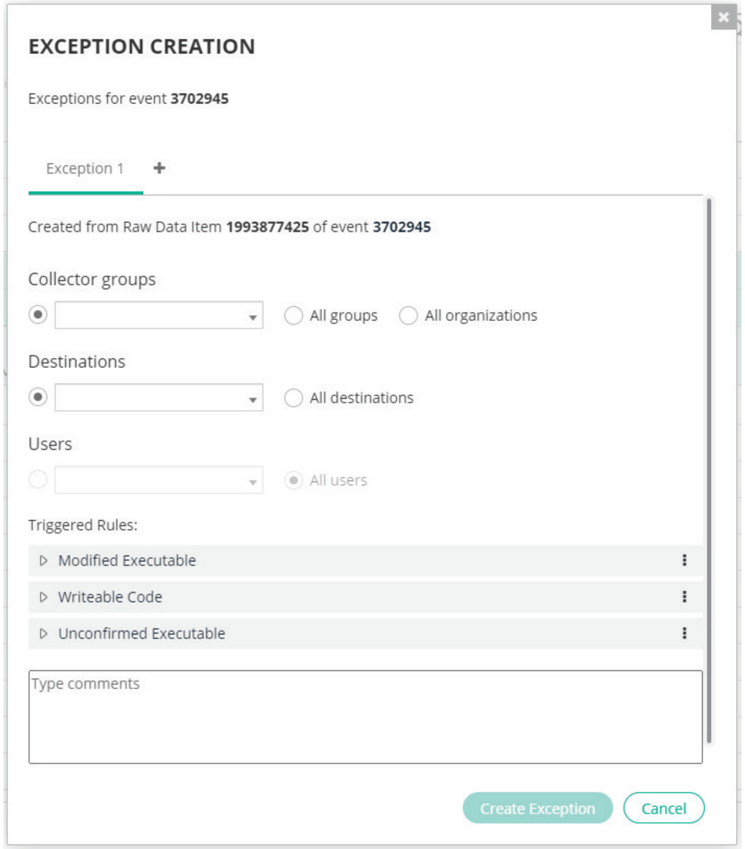
Threat type: Unknown

History

Suspicious, by FortinetCloudServices , on 06-Feb-2020, 02:54:36

- Simulation Device **DESKTOP-BS09MQF** was moved from collector group **Win10** to collector group **High Security Collector Group** 3 times
- Simulation Device **DESKTOP-BS09MQF** was isolated 3 times

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



EXCEPTION CREATION

Exceptions for event **3702945**

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

Collector groups

● [▾] ○ All groups ○ All organizations

Destinations

● [▾] ○ All destinations

Users

○ [▾] ● All users

Triggered Rules:

- Modified Executable
- Writeable Code
- Unconfirmed Executable

Type comments

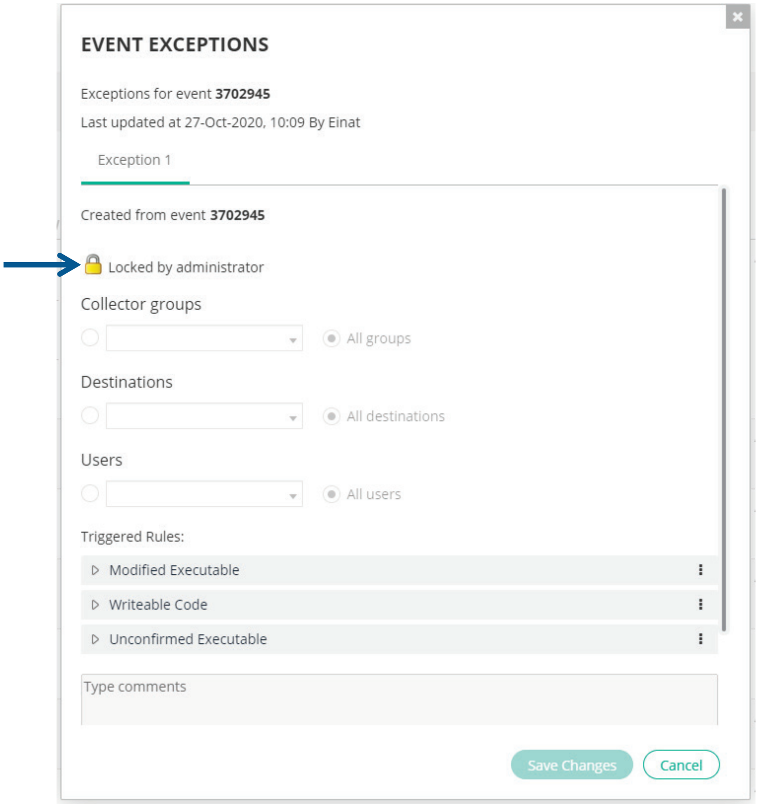
3 Specify whether this exception applies to all the Collector Groups or only to the Collectors in the same Collector Group as the one for which this security event was triggered.

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

For a multi-organization FortiEDR system, an Administrator can also specify whether the exception applies to all organizations. The All organizations option applies the exception to all organizations, regardless of whether or not the security event already occurred.

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

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



EVENT EXCEPTIONS

Exceptions for event **3702945**

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

Exception 1

Created from event **3702945**

🔒 Locked by administrator

Collector groups

○ ● All groups

Destinations

○ ● All destinations

Users

○ ● All users

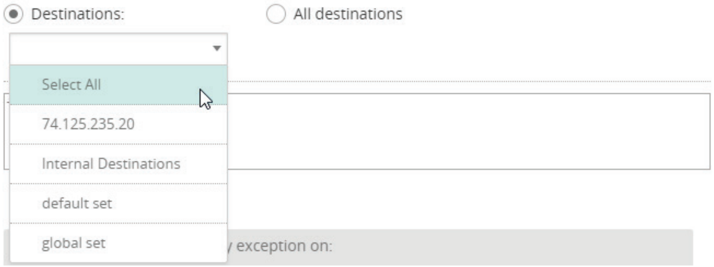
Triggered Rules:

- Modified Executable
- Writeable Code
- Unconfirmed Executable

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 security event. Use the dropdown menu to select the specific Ips to exclude that were triggered on this security event, which can be either internal or external.



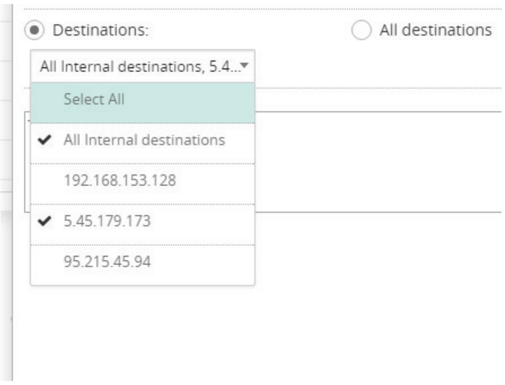
● Destinations: ○ All destinations

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

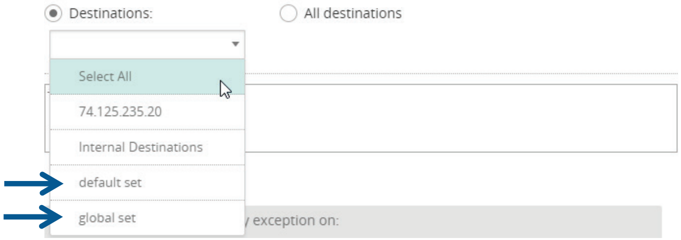
- **Select All:** Applies the exception on all destinations that were seen as part of this security event. If there will be an identical violation (the same set of rules will be violated on this process) but the connection attempt will be to a different IP, than the security event will be triggered.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

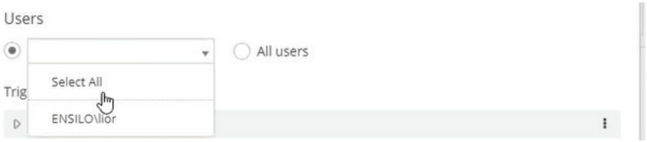
  This option is useful when an application is allowed for use within the organization, but you do not want it to be used for external communications. Using this option enables the application to communicate internally without triggering alerts. However, the application might still trigger alerts when attempting to connect to an external IP.
- **<IP Address>:** Applies the exception to the selected IP address. You can select multiple IP addresses.



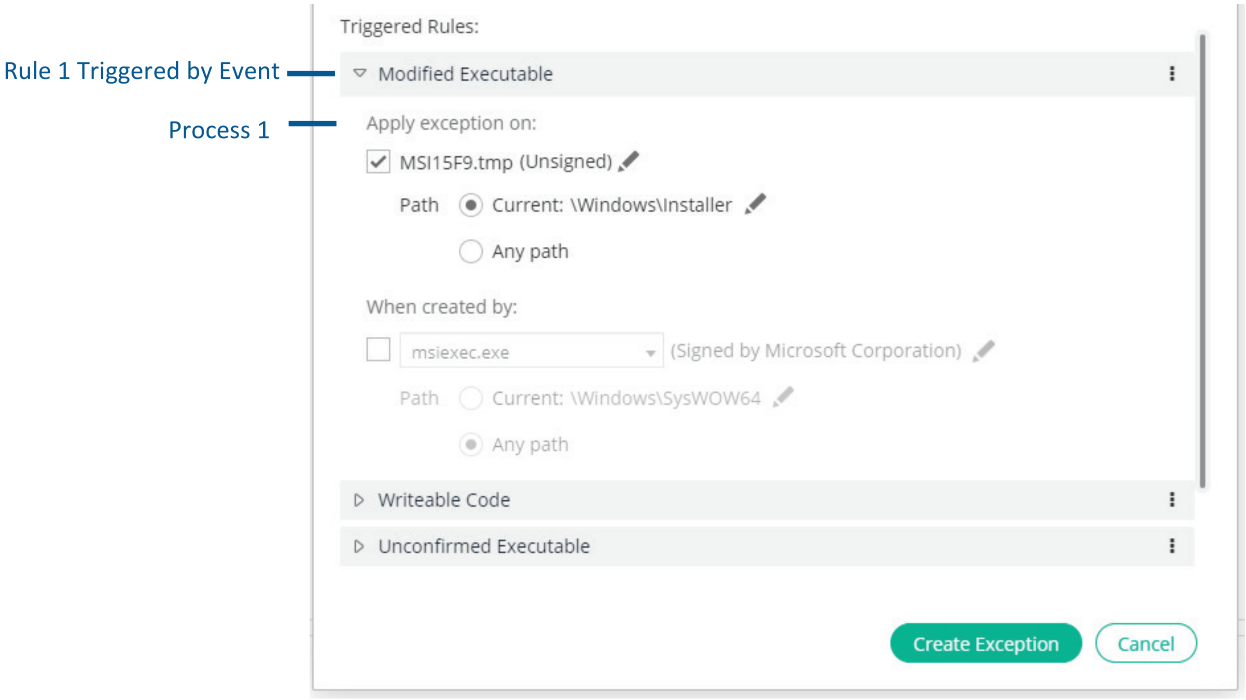
- **<IP Set>:** An IP set defines a set of Ips to be included or excluded from a security event. When you select an IP set here, it means that an exception is applied only to a device that has one of the Ips specified in the IP set. IP sets can only be defined by an Administrator, as described on page 220.



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



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



Rule 1 Triggered by Event

Process 1

Triggered Rules:

▽ Modified Executable

Apply exception on:

☑ MSI15F9.tmp (Unsigned)

Path ● Current: \Windows\Installer

○ Any path

When created by:

□ msiexec.exe (Signed by Microsoft Corporation)

Path ○ Current: \Windows\SysWOW64

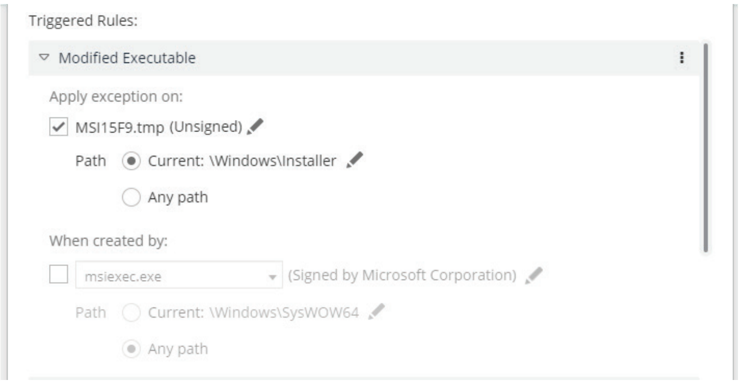
● Any path

▷ Writeable Code

▷ Unconfirmed Executable

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

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



Triggered Rules:

▽ Modified Executable

Apply exception on:

☑ MSI15F9.tmp (Unsigned)

Path ● Current: \Windows\Installer

○ Any path

When created by:

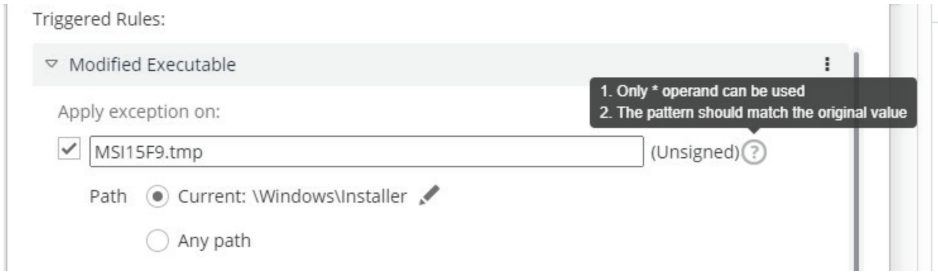
□ msiexec.exe (Signed by Microsoft Corporation)

Path ○ Current: \Windows\SysWOW64

● Any path

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

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



Triggered Rules:

▽ Modified Executable

1. Only * operand can be used
2. The pattern should match the original value

Apply exception on:

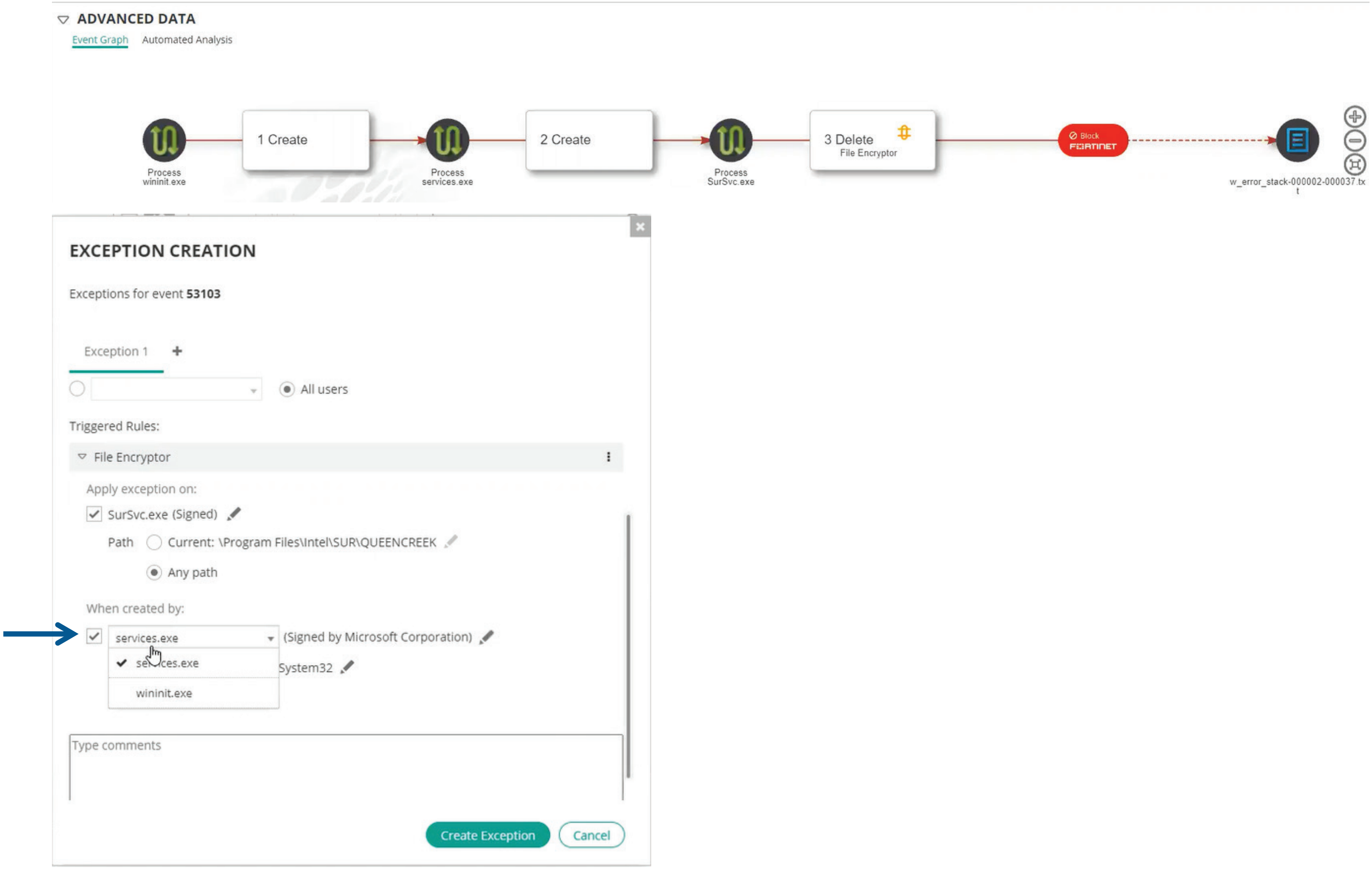
☑ MSI15F9.tmp (Unsigned)

Path ● Current: \Windows\Installer

○ Any path

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

Let's look at an example in more detail. Let's say that you want to define an exception that allows the **SurSvc.exe** executable to run, but only when it is created from the **services.exe** executable. Therefore, in order to define this exception, you would select the **SurSvc.exe** process in the **Apply exception on** field and select the **services.exe** process in the **When created by** field. Based on this security event's ancestry chain, **wininit.exe**, which is the grandparent of the **SurSvc.exe** executable, would not be selected in the **When created by** field. Note that the immediate parent of the **SurSvc.exe** executable is **services.exe** and that it is therefore listed at the top of the **When created by** field dropdown list and that the **SurSvc.exe** executable's grandparent is **wininit.exe**, which is listed at the bottom of the list. The order in which the processes run in a security event chain is always maintained. This means that the oldest ancestor is shown at the bottom of the list of processes in this window and the immediate parent is at the top.



EXCEPTION CREATION

Exceptions for event **53103**

Exception 1 +

○ ● All users

Triggered Rules:

▽ File Encryptor

Apply exception on:

☑ SurSvc.exe (Signed)

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

● Any path

When created by:

☑ services.exe (Signed by Microsoft Corporation)

✓ services.exe

wininit.exe

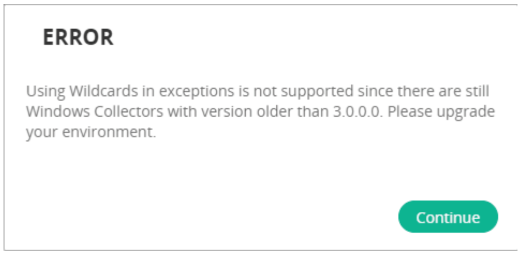
System32

Type comments

Create Exception | Cancel

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:



ERROR

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

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:

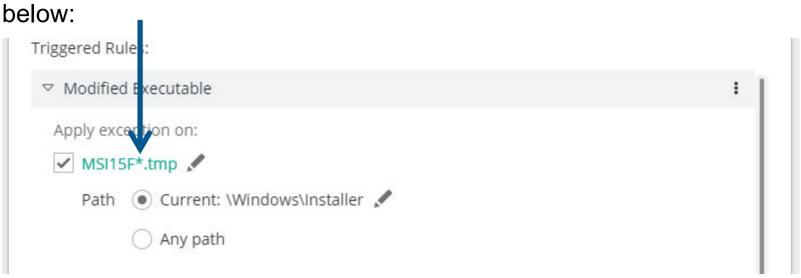
Path

- 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:



Triggered Rules:

Modified Executable

Apply exception on:

☑ MSI15F*.tmp

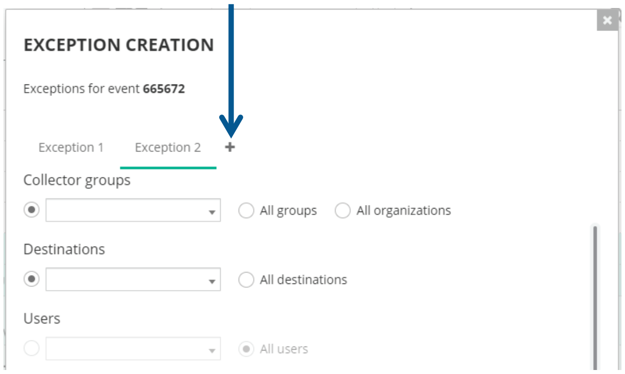
Path ● Current: \Windows\Installer

○ Any path

7 [Optional] Enter any comments in the **Comments** box.

8 Click the **Create Exception** button.

9 [Optional] You can define another exception for this same security event by clicking the **plus** button at the top of the window. Then, define the exception in the same manner as described above in steps **1**–**8**.



EXCEPTION CREATION

Exceptions for event **665672**

Collector groups

● ○ All groups ○ All organizations

Destinations

● ○ All destinations

Users

○ ● All users

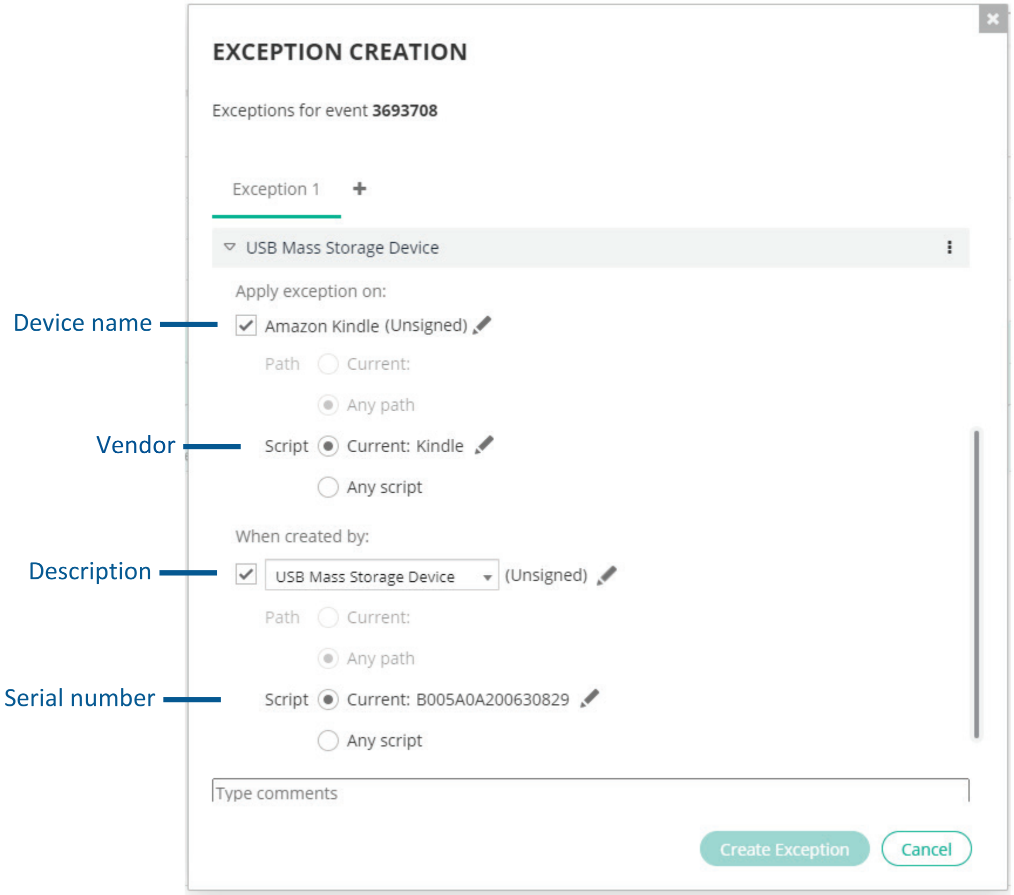
Note – If this exception was created previously, the **Remove Exception** button appears enabling you to delete the exception.

Device Control Exceptions

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

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

For example:



EXCEPTION CREATION

Exceptions for event **3693708**

Exception 1 +

USB Mass Storage Device

Apply exception on:

☑ Amazon Kindle (Unsigned)

Path ○ Current:
● Any path

Script ● Current: Kindle
○ Any script

When created by:

☑ USB Mass Storage Device (Unsigned)

Path ○ Current:
● Any path

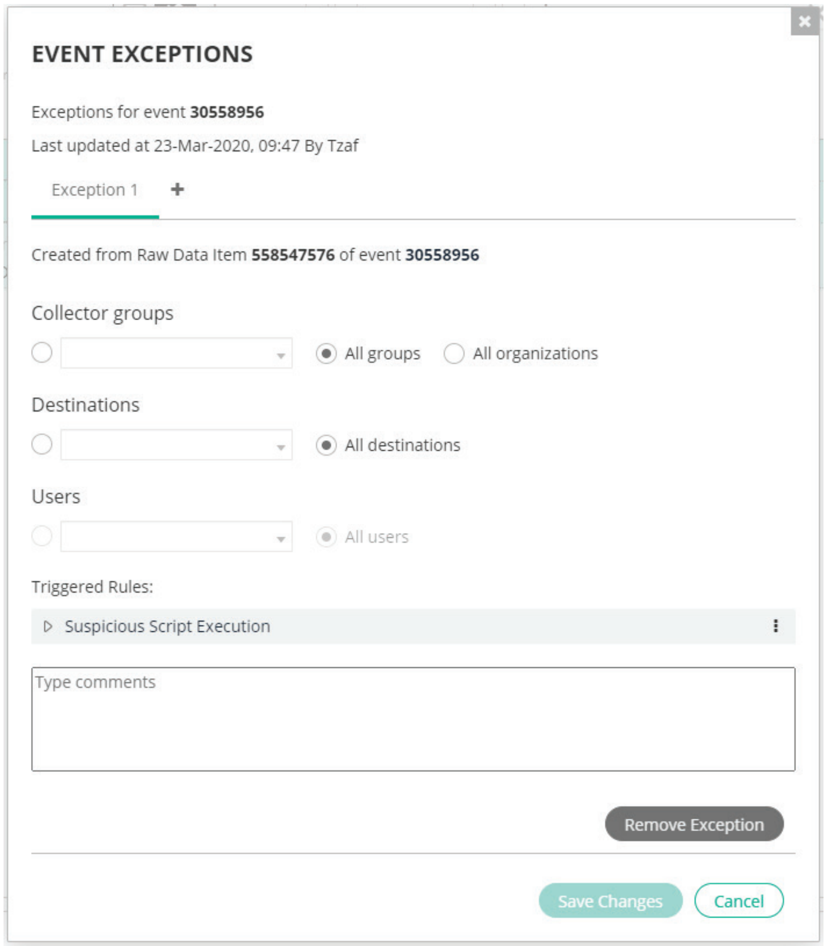
Script ● Current: B005A0A200630829
○ Any script

Type comments

Editing Security Event Exceptions

To edit a security event exception:

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



EVENT EXCEPTIONS

Exceptions for event **30558956**

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

Exception 1 +

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

Collector groups

○ ● All groups ○ All organizations

Destinations

○ ● All destinations

Users

○ ● All users

Triggered Rules:

▷ Suspicious Script Execution

Type comments

2 Modify the Collector Groups, Destinations and Users to which the exception applies and the pairs of rules and processes that operate together to define an exception in the **Triggered Rules** area, as needed. For more details, see page 109.

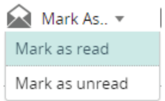
For a multi-organization FortiEDR system, an Administrator can also specify whether the exception applies to all organizations. The **All organizations** option applies the exception to all organizations, regardless of whether or not the security event already occurred.

3 Click the **Save Changes** button.

Marking a Security Event as Read/Unread

The following describes how to specify that you have viewed a security event. This does not mean that the security event has been handled (page 104). When any FortiEDR Central Manager user marks a security event as Read, all users see it as having been read. Unread security events are displayed bold.

To mark a security event as having been viewed:

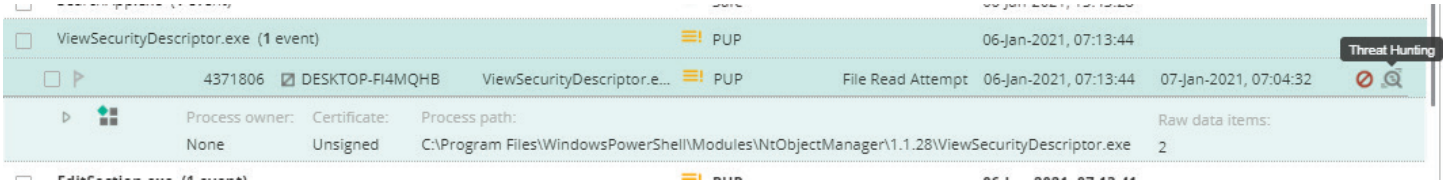
- Select the rule's checkbox and then click the **Mark As**  button and then select **Mark as read**. The security event row text is no longer displayed bold.

Viewing Relevant Activity Events

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

To view the related Activity event of a Security Event in the Event Viewer –

- Click on the **Threat Hunting** icon that is displayed when you hover over the event, as shown below. The Threat Hunting windows is then displayed.



ViewSecurityDescriptor.exe (1 event) PUP 06-Jan-2021, 07:13:44

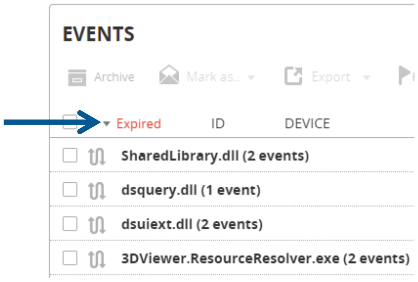
4371806 DESKTOP-FI4MQHB ViewSecurityDescriptor.e... PUP File Read Attempt 06-Jan-2021, 07:13:44 07-Jan-2021, 07:04:32

Process owner: None
Certificate: Unsigned
Process path: C:\Program Files\WindowsPowerShell\Modules\NtObjectManager\1.1.28\ViewSecurityDescriptor.exe
Raw data items: 2

Viewing Expired Security Events

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

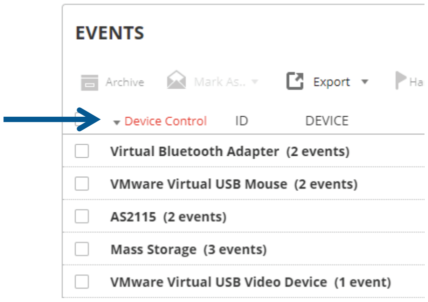
Expired security events can only occur when a Collector is connected to the Core, and do not occur when a Collector works autonomously.



SharedLibrary.dll (2 events)
dsquery.dll (1 event)
dsuiext.dll (2 events)
3DViewer.ResourceResolver.exe (2 events)

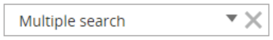
Viewing Device Control Security Events

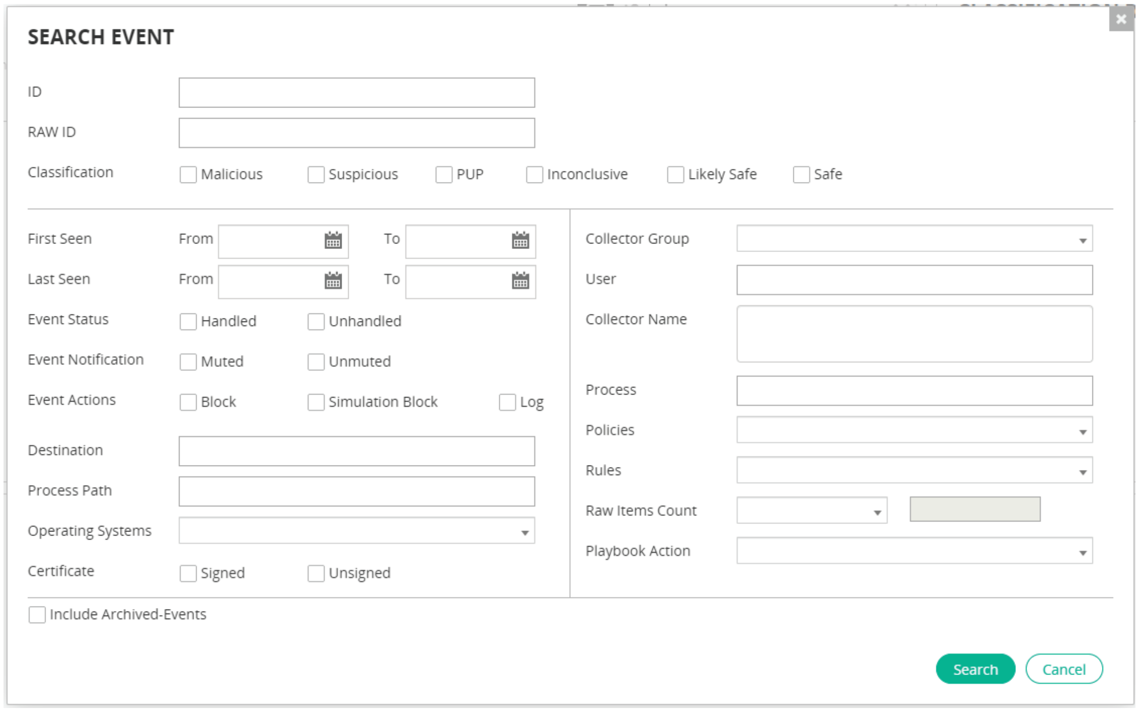
Security events in the Event Viewer can be filtered to show device control security events. Device control security events are events that were triggered on rules that are part of the Device Control policy. Such events do not necessarily mean that there was malicious activity but indicate USB peripheral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



□ Virtual Bluetooth Adapter (2 events)
□ VMware Virtual USB Mouse (2 events)
□ AS2115 (2 events)
□ Mass Storage (3 events)
□ VMware Virtual USB Video Device (1 event)

Other Options in the Event Viewer

- **Sorting Events:** Click any column name to sort security events. For example, you may want to sort by Process and Collector in order to see the history of everything that happened to that process on that device.
- **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 security events (unfiltered).



SEARCH EVENT

ID

RAW ID

Classification □ Malicious □ Suspicious □ PUP □ Inconclusive □ Likely Safe □ Safe

First Seen From To

Last Seen From To

Event Status □ Handled □ Unhandled

Event Notification □ Muted □ Unmuted

Event Actions □ Block □ Simulation Block □ Log

Destination

Process Path

Operating Systems

Certificate □ Signed □ Unsigned

Collector Group

User

Collector Name

Process

Policies

Rules

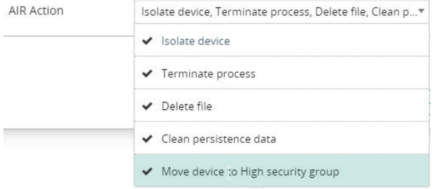
Raw Items Count

Playbook Action

□ Include Archived-Events

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.



AIR Action: Isolate device, Terminate process, Delete file, Clean p...

- ✓ Isolate device
- ✓ Terminate process
- ✓ Delete file
- ✓ Clean persistence data
- ✓ Move device to High security group

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

  Note – To unarchive a security 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 a security event from the FortiEDR system.

  Note – A deleted security event cannot be restored or retrieved. Unless you are having storage capacity issues, we highly recommend just hiding security events and not deleting them.
- **Forensics:** The optional FortiEDR Forensics add-on enables you to perform deep analysis of security events, as described on page 144.
- **Exception Manager:** Click the Exception Manager button to access the Exception Manager, as described on page 58.

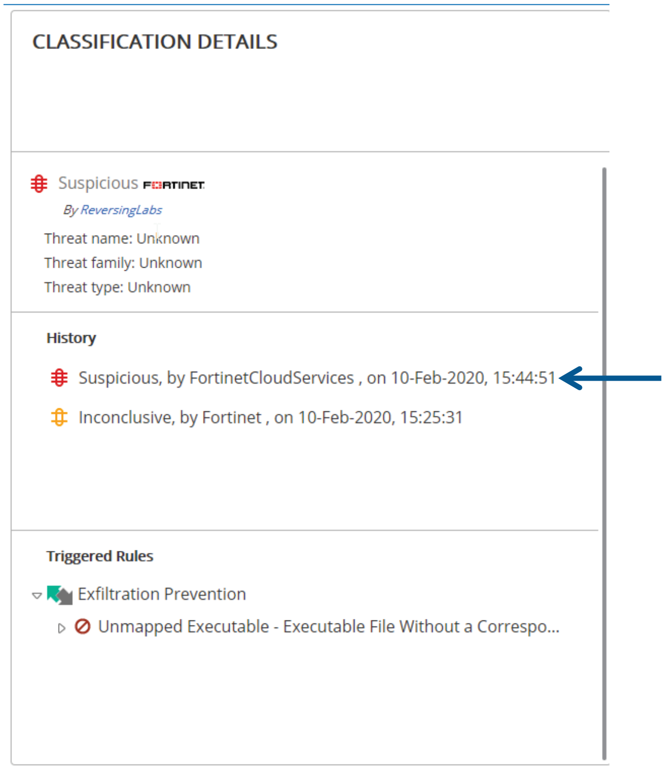
Classification Details

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

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

All FortiEDR actions are based on the final classification of a security event by the FCS. The FCS is a cloud-based, software-only service that determines the exact classification of security events and acts accordingly based on that classification – all with a high degree of accuracy. All Playbook policy actions are based on the final determination of the FCS. For more details, see *Playbook Policies* on page 57.

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



CLASSIFICATION DETAILS

Suspicious FORTINET
By ReversingLabs
Threat name: Unknown
Threat family: Unknown
Threat type: Unknown

History

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

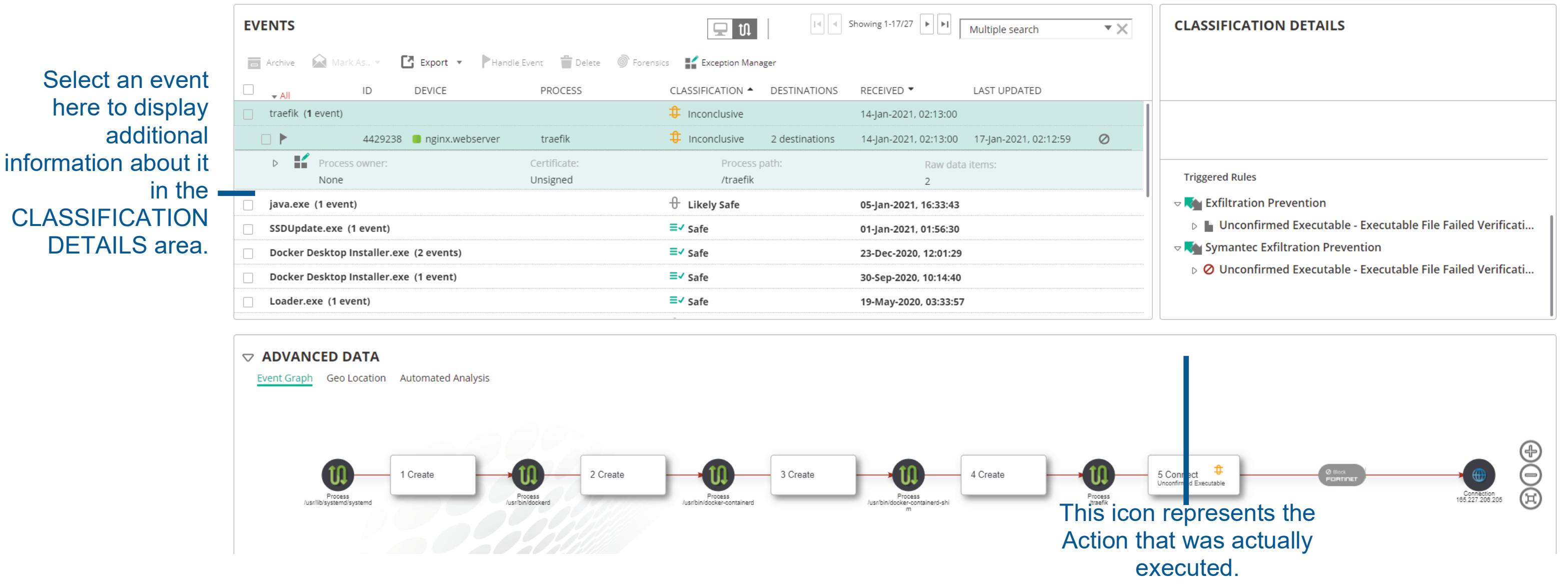
Inconclusive, by Fortinet , on 10-Feb-2020, 15:25:31

Triggered Rules

Exfiltration Prevention

Unmapped Executable - Executable File Without a Correspo...

In the Triggered Rules 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.



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

EVENTS

All	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
traefik (1 event)				Inconclusive		14-Jan-2021, 02:13:00	
	4429238	nginx.webserver	traefik	Inconclusive	2 destinations	14-Jan-2021, 02:13:00	17-Jan-2021, 02:12:59
java.exe (1 event)				Likely Safe		05-Jan-2021, 16:33:43	
SSDUpdate.exe (1 event)				Safe		01-Jan-2021, 01:56:30	
Docker Desktop Installer.exe (2 events)				Safe		23-Dec-2020, 12:01:29	
Docker Desktop Installer.exe (1 event)				Safe		30-Sep-2020, 10:14:40	
Loader.exe (1 event)				Safe		19-May-2020, 03:33:57	

Process owner: None
Certificate: Unsigned
Process path: /traefik
Raw data items: 2

CLASSIFICATION DETAILS

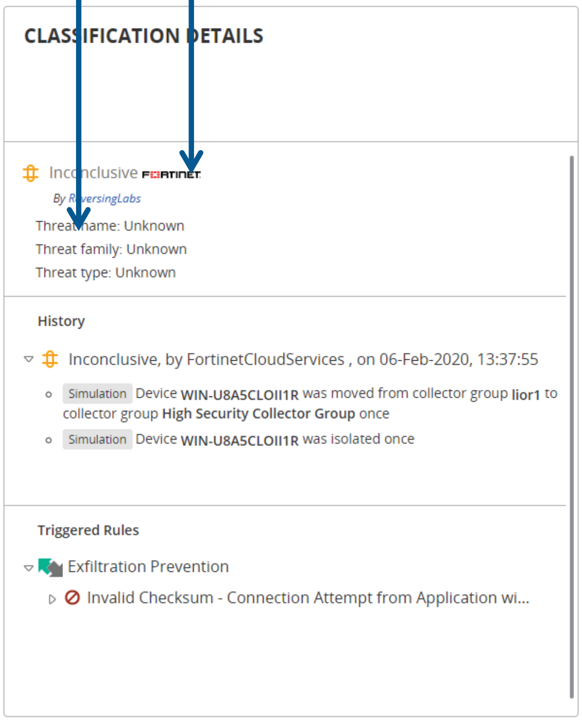
Triggered Rules

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

ADVANCED DATA

This icon represents the Action that was actually executed.

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.



CLASSIFICATION DETAILS

Inconclusive FORTINET
By ReversingLabs
Threat name: Unknown
Threat family: Unknown
Threat type: Unknown

History

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

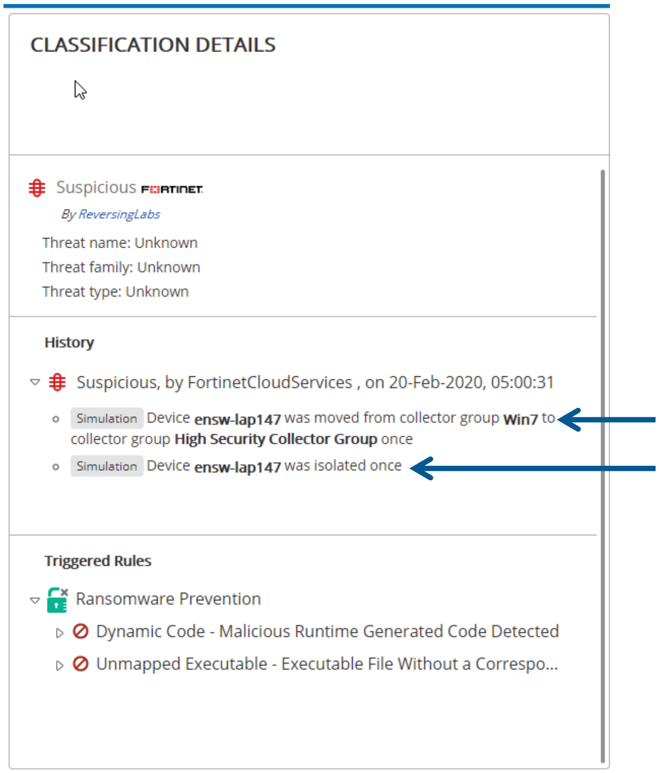
Triggered Rules

- Exfiltration Prevention
  - ⊘ Invalid Checksum - Connection Attempt from Application wi...

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

Contact Fortinet support for more details about the third-party tool used by Fortinet for the classification process.

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



CLASSIFICATION DETAILS

Suspicious FORTINET

By ReversingLabs

Threat name: Unknown
Threat family: Unknown
Threat type: Unknown

History

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

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

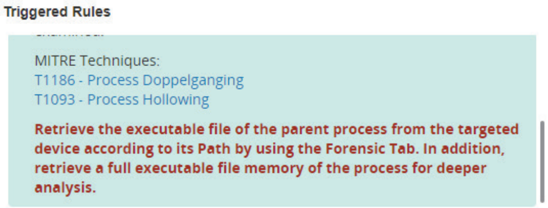
Triggered Rules

Ransomware Prevention

- Dynamic Code - Malicious Runtime Generated Code Detected
- Unmapped Executable - Executable File Without a Correspo...

> **Note –** Notification actions are not shown in the Event Viewer, but Investigation and Remediation actions are. For more details, see page 60, 62 and 63, respectively.

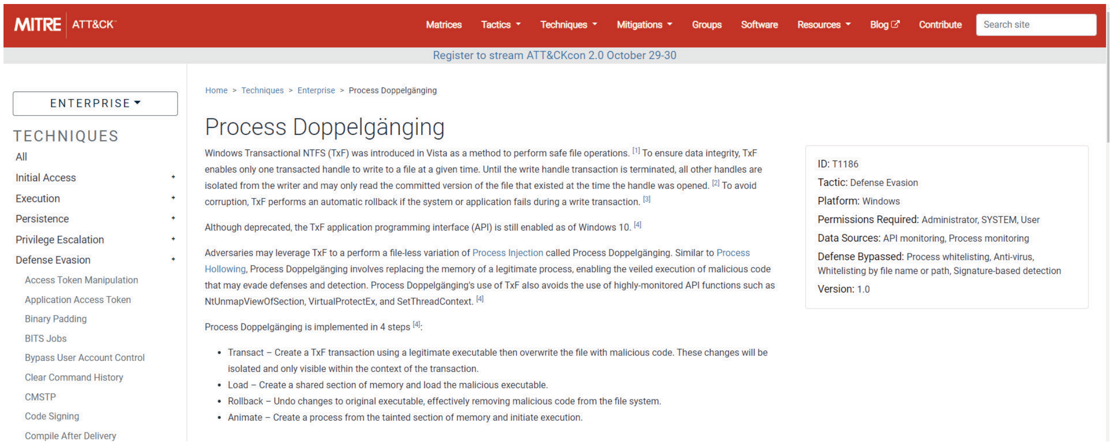
When expanding triggered rules, you can see the techniques that were used in this security event, based on the MITRE ATT&CK common techniques scheme. Clicking the technique opens the MITRE web page, providing additional details, as shown below.



Triggered Rules

MITRE Techniques:
T1186 - Process Doppelganging
T1093 - Process Hollowing

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



Register to stream ATT&CKcon 2.0 October 29-30

Home > Techniques > Enterprise > Process Doppelgänging

Process Doppelgänging

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

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

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

Process Doppelgänging is implemented in 4 steps [4]:

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

ID: T1186
Tactic: Defense Evasion
Platform: Windows
Permissions Required: Administrator, SYSTEM, User
Data Sources: API monitoring, Process monitoring
Defense Bypassed: Process whitelisting, Anti-virus, Whitelisting by file name or path, Signature-based detection
Version: 1.0

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 a security event in the **EVENTS** tab.

FortiEDR Communication Control uses a set of policies that contain recommendations about whether an application should be approved or denied 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.

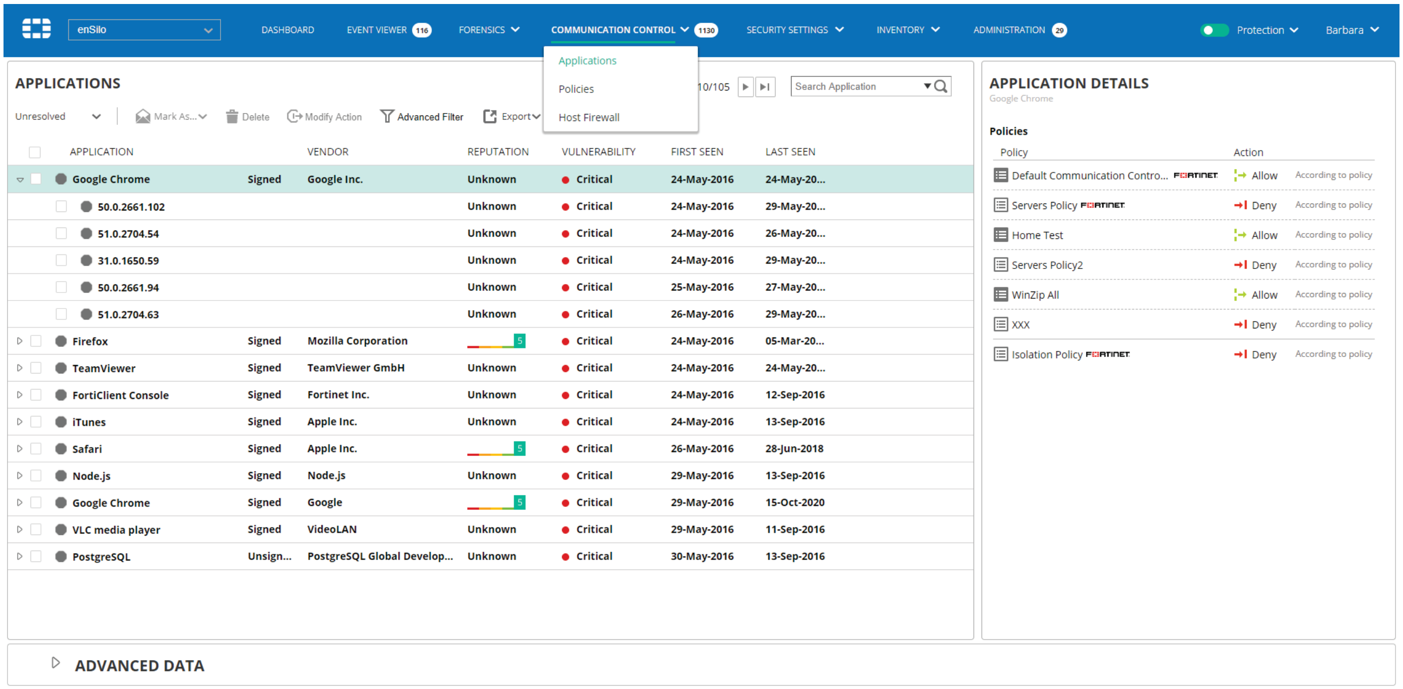
Moreover, FortiEDR Communication Control provides data and tools for efficient vulnerability assessment and control. Virtual patching is made possible with Communication Control policies that can be configured to automatically block connections from vulnerable applications.

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.**



APPLICATIONS

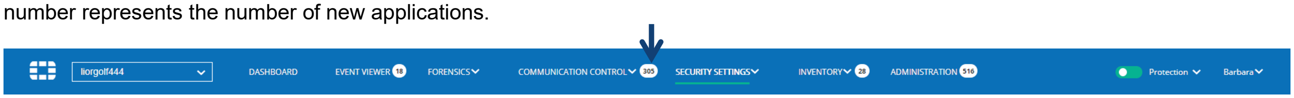
APPLICATION		VENDOR	REPUTATION	VULNERABILITY	FIRST SEEN	LAST SEEN
Google Chrome	Signed	Google Inc.	Unknown	● Critical	24-May-2016	24-May-20...
50.0.2661.102			Unknown	● Critical	24-May-2016	29-May-20...
51.0.2704.54			Unknown	● Critical	24-May-2016	26-May-20...
31.0.1650.59			Unknown	● Critical	24-May-2016	29-May-20...
50.0.2661.94			Unknown	● Critical	25-May-2016	27-May-20...
51.0.2704.63			Unknown	● Critical	26-May-2016	29-May-20...
Firefox	Signed	Mozilla Corporation	5	● Critical	24-May-2016	05-Mar-20...
TeamViewer	Signed	TeamViewer GmbH	Unknown	● Critical	24-May-2016	24-May-20...
FortiClient Console	Signed	Fortinet Inc.	Unknown	● Critical	24-May-2016	12-Sep-2016
iTunes	Signed	Apple Inc.	Unknown	● Critical	24-May-2016	13-Sep-2016
Safari	Signed	Apple Inc.	5	● Critical	26-May-2016	28-Jun-2018
Node.js	Signed	Node.js	Unknown	● Critical	29-May-2016	13-Sep-2016
Google Chrome	Signed	Google	5	● Critical	29-May-2016	15-Oct-2020
VLC media player	Signed	VideoLAN	Unknown	● Critical	29-May-2016	11-Sep-2016
PostgreSQL	Unsign...	PostgreSQL Global Develop...	Unknown	● Critical	30-May-2016	13-Sep-2016

APPLICATION DETAILS
Google Chrome

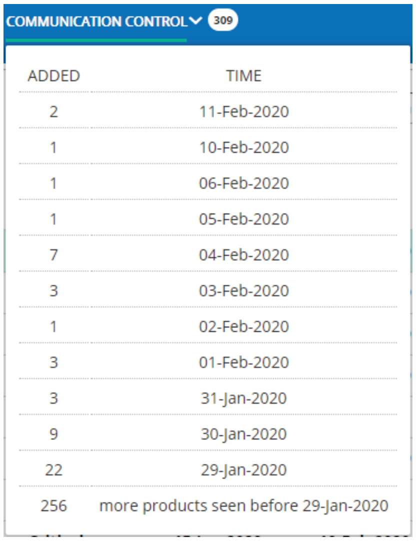
Policies

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

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.



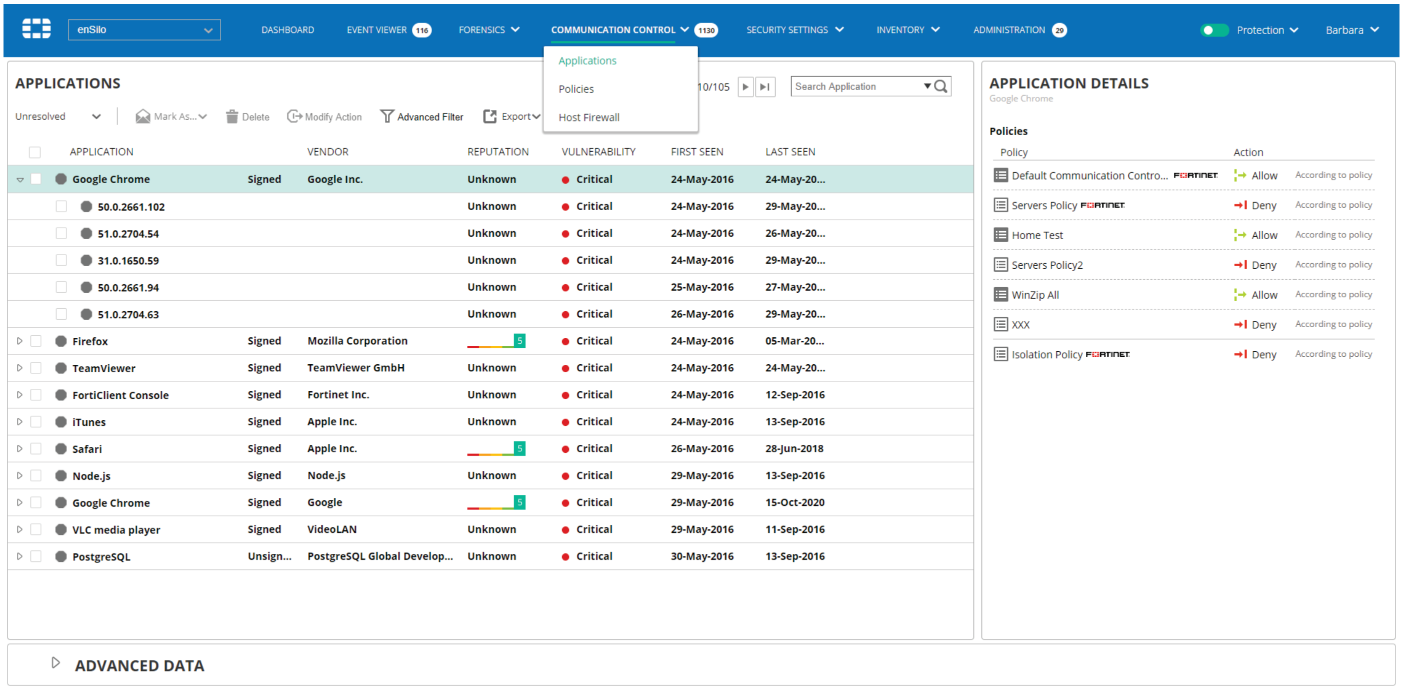
ADDED	TIME
2	11-Feb-2020
1	10-Feb-2020
1	06-Feb-2020
1	05-Feb-2020
7	04-Feb-2020
3	03-Feb-2020
1	02-Feb-2020
3	01-Feb-2020
3	31-Jan-2020
9	30-Jan-2020
22	29-Jan-2020
256	more products seen before 29-Jan-2020

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

- **Applications,** page 125
- **Policies,** page 136

Applications

The APPLICATIONS page lists all communicating applications detected in your organization that have ever attempted to communicate. By default, applications are sorted according to their first-seen indicator, placing new applications at the top. To access this page, click the down arrow next to COMMUNICATION CONTROL and then select Applications.



APPLICATIONS

APPLICATION		VENDOR	REPUTATION	VULNERABILITY	FIRST SEEN	LAST SEEN
Google Chrome	Signed	Google Inc.	Unknown	● Critical	24-May-2016	24-May-20...
50.0.2661.102			Unknown	● Critical	24-May-2016	29-May-20...
51.0.2704.54			Unknown	● Critical	24-May-2016	26-May-20...
31.0.1650.59			Unknown	● Critical	24-May-2016	29-May-20...
50.0.2661.94			Unknown	● Critical	25-May-2016	27-May-20...
51.0.2704.63			Unknown	● Critical	26-May-2016	29-May-20...
Firefox	Signed	Mozilla Corporation	5	● Critical	24-May-2016	05-Mar-20...
TeamViewer	Signed	TeamViewer GmbH	Unknown	● Critical	24-May-2016	24-May-20...
FortiClient Console	Signed	Fortinet Inc.	Unknown	● Critical	24-May-2016	12-Sep-2016
iTunes	Signed	Apple Inc.	Unknown	● Critical	24-May-2016	13-Sep-2016
Safari	Signed	Apple Inc.	5	● Critical	26-May-2016	28-Jun-2018
Node.js	Signed	Node.js	Unknown	● Critical	29-May-2016	13-Sep-2016
Google Chrome	Signed	Google	5	● Critical	29-May-2016	15-Oct-2020
VLC media player	Signed	VideoLAN	Unknown	● Critical	29-May-2016	11-Sep-2016
PostgreSQL	Unsign...	PostgreSQL Global Develop...	Unknown	● Critical	30-May-2016	13-Sep-2016

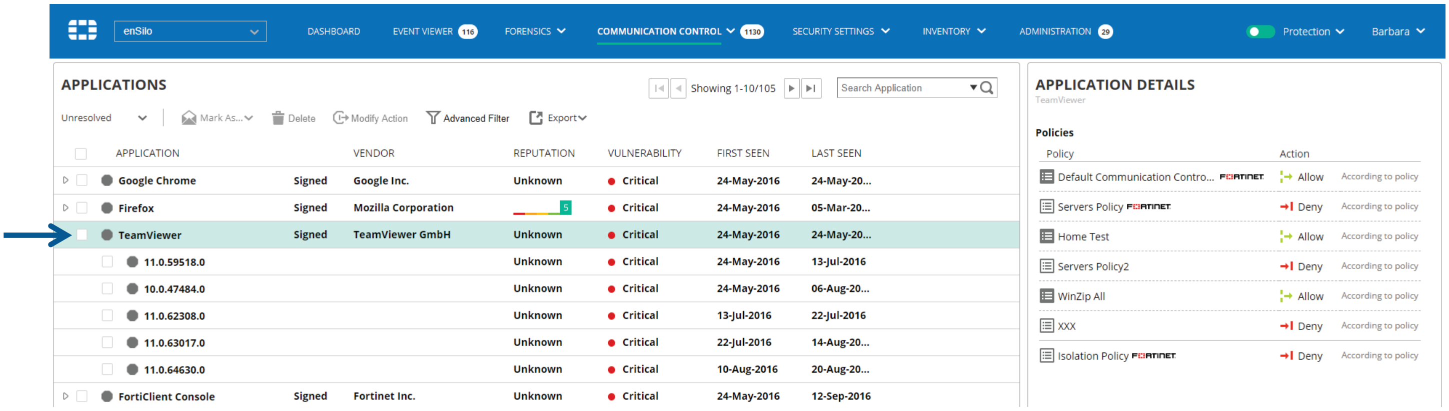
APPLICATION DETAILS

Google Chrome

Policies

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

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



APPLICATIONS

APPLICATION		VENDOR	REPUTATION	VULNERABILITY	FIRST SEEN	LAST SEEN
Google Chrome	Signed	Google Inc.	Unknown	● Critical	24-May-2016	24-May-20...
Firefox	Signed	Mozilla Corporation	5	● Critical	24-May-2016	05-Mar-20...
TeamViewer	Signed	TeamViewer GmbH	Unknown	● Critical	24-May-2016	24-May-20...
11.0.59518.0			Unknown	● Critical	24-May-2016	13-Jul-2016
10.0.47484.0			Unknown	● Critical	24-May-2016	06-Aug-20...
11.0.62308.0			Unknown	● Critical	13-Jul-2016	22-Jul-2016
11.0.63017.0			Unknown	● Critical	22-Jul-2016	14-Aug-20...
11.0.64630.0			Unknown	● Critical	10-Aug-2016	20-Aug-20...
FortiClient Console	Signed	Fortinet Inc.	Unknown	● Critical	24-May-2016	12-Sep-2016

APPLICATION DETAILS

TeamViewer

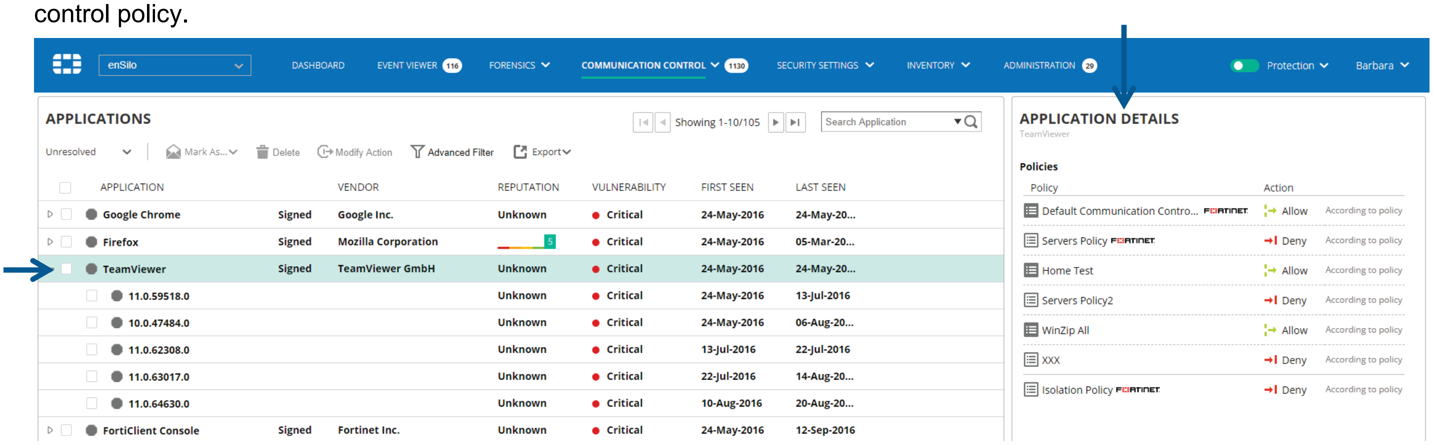
Policies

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

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

- Selection checkbox
- Resolving status icon
- Signed/Unsigned indication
- **Application/Version:** The name of the application/version.
- **Vendor:** The application's vendor and certificate details.
- **Reputation:** The reputation score of the application. For more details, see page 126.
- **Vulnerability:** The highest CVE vulnerability score for the application. For more details, see page 127.
- **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.



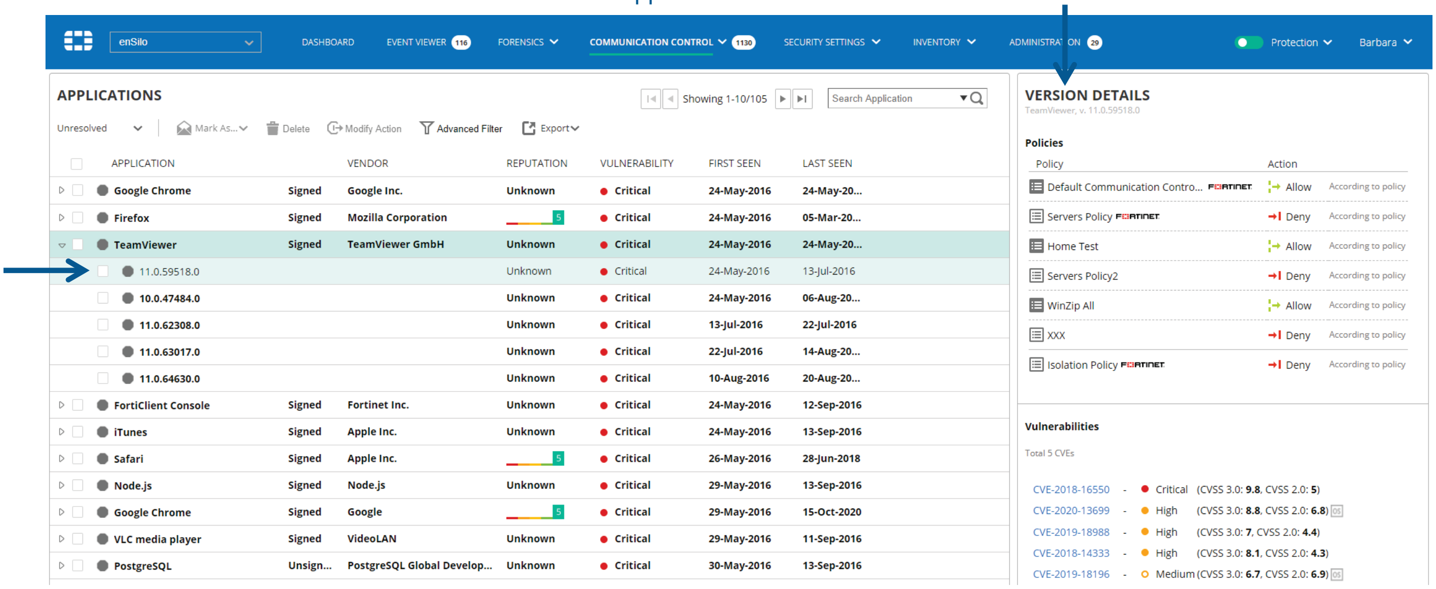
APPLICATION		VENDOR	REPUTATION	VULNERABILITY	FIRST SEEN	LAST SEEN
Google Chrome	Signed	Google Inc.	Unknown	● Critical	24-May-2016	24-May-20...
Firefox	Signed	Mozilla Corporation	5	● Critical	24-May-2016	05-Mar-20...
TeamViewer	Signed	TeamViewer GmbH	Unknown	● Critical	24-May-2016	24-May-20...
11.0.59518.0			Unknown	● Critical	24-May-2016	13-Jul-2016
10.0.47484.0			Unknown	● Critical	24-May-2016	06-Aug-20...
11.0.62308.0			Unknown	● Critical	13-Jul-2016	22-Jul-2016
11.0.63017.0			Unknown	● Critical	22-Jul-2016	14-Aug-20...
11.0.64630.0			Unknown	● Critical	10-Aug-2016	20-Aug-20...
FortiClient Console	Signed	Fortinet Inc.	Unknown	● Critical	24-May-2016	12-Sep-2016

APPLICATION DETAILS
TeamViewer

Policies

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

Application Details



APPLICATION		VENDOR	REPUTATION	VULNERABILITY	FIRST SEEN	LAST SEEN
Google Chrome	Signed	Google Inc.	Unknown	● Critical	24-May-2016	24-May-20...
Firefox	Signed	Mozilla Corporation	5	● Critical	24-May-2016	05-Mar-20...
TeamViewer	Signed	TeamViewer GmbH	Unknown	● Critical	24-May-2016	24-May-20...
11.0.59518.0			Unknown	● Critical	24-May-2016	13-Jul-2016
10.0.47484.0			Unknown	● Critical	24-May-2016	06-Aug-20...
11.0.62308.0			Unknown	● Critical	13-Jul-2016	22-Jul-2016
11.0.63017.0			Unknown	● Critical	22-Jul-2016	14-Aug-20...
11.0.64630.0			Unknown	● Critical	10-Aug-2016	20-Aug-20...
FortiClient Console	Signed	Fortinet Inc.	Unknown	● Critical	24-May-2016	12-Sep-2016
iTunes	Signed	Apple Inc.	Unknown	● Critical	24-May-2016	13-Sep-2016
Safari	Signed	Apple Inc.	5	● Critical	26-May-2016	28-Jun-2018
Node.js	Signed	Node.js	Unknown	● Critical	29-May-2016	13-Sep-2016
Google Chrome	Signed	Google	5	● Critical	29-May-2016	15-Oct-2020
VLC media player	Signed	VideoLAN	Unknown	● Critical	29-May-2016	11-Sep-2016
PostgreSQL	Unsign...	PostgreSQL Global Develop...	Unknown	● Critical	30-May-2016	13-Sep-2016

VERSION DETAILS
TeamViewer, v. 11.0.59518.0

Policies

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

Vulnerabilities

Total 5 CVEs

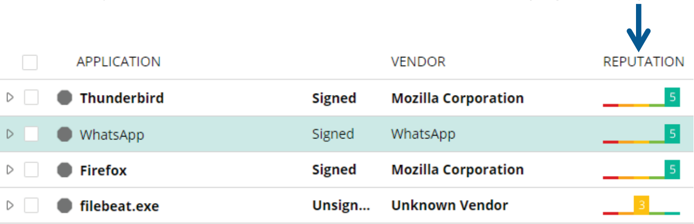
CVE-2018-16550 - ● Critical (CVSS 3.0: **9.8**, CVSS 2.0: **5**)
CVE-2020-13699 - ● High (CVSS 3.0: **8.8**, CVSS 2.0: **6.8**) OS
CVE-2019-18988 - ● High (CVSS 3.0: **7**, CVSS 2.0: **4.4**)
CVE-2018-14333 - ● High (CVSS 3.0: **8.1**, CVSS 2.0: **4.3**)
CVE-2019-18196 - ○ Medium (CVSS 3.0: **6.7**,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

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 132.

Reputation Score

Each application in the **APPLICATIONS** page shows a Reputation indicator. Reputation scores are determined by a third-party service, and are based on the hash (signature) of the file.



APPLICATION		VENDOR	REPUTATION
Thunderbird	Signed	Mozilla Corporation	5
WhatsApp	Signed	WhatsApp	5
Firefox	Signed	Mozilla Corporation	5
filebeat.exe	Unsign...	Unknown Vendor	3

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

- **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

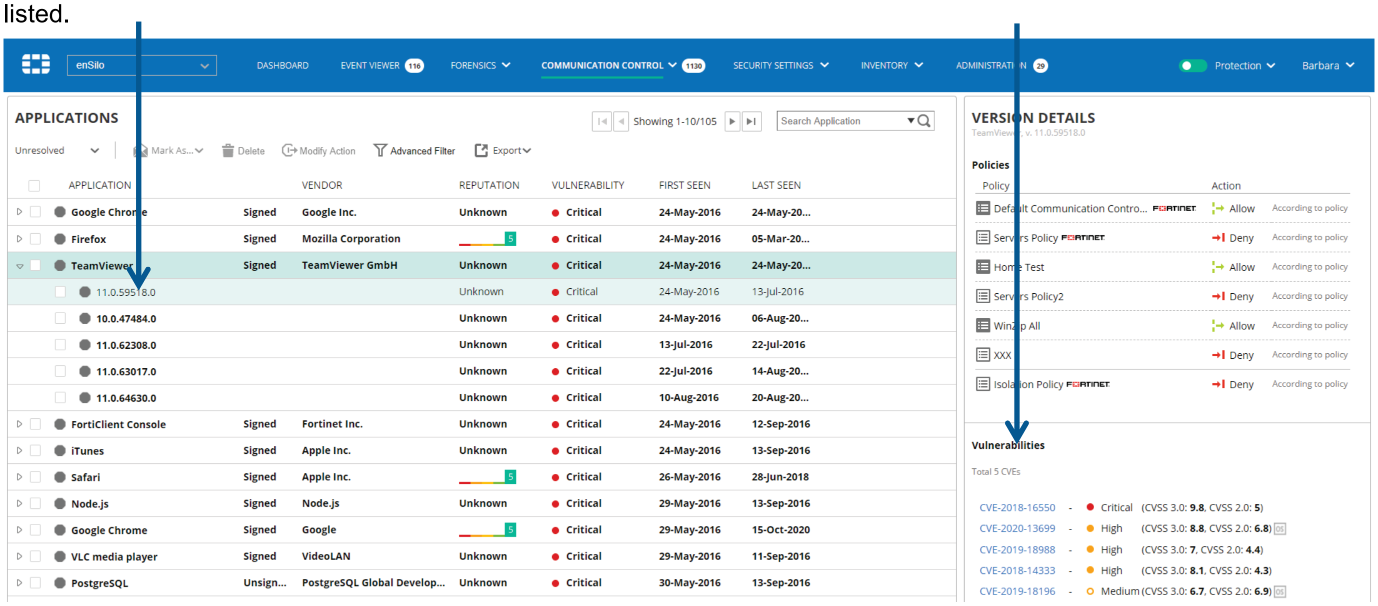
The Reputation indicator displays **Unknown** if the reputation score is unknown.

Vulnerability

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

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

FortiEDR categorizes applications/versions based on the Common Vulnerability Scoring System (CVSS) CVE scheme, which is commonly used worldwide. FortiEDR’s vulnerability scoring system provides a useful tool for vulnerability assessment, and enables you to review the weaknesses detected in your environment that could be exploited by attackers before they actually occur. Vulnerability assessment can be used together with virtual patching to block applications with known critical vulnerabilities, so that they cannot connect, until the system is patched for the CVEs listed.



APPLICATIONS

APPLICATION		VENDOR	REPUTATION	VULNERABILITY	FIRST SEEN	LAST SEEN
Google Chrome	Signed	Google Inc.	Unknown	● Critical	24-May-2016	24-May-20...
Firefox	Signed	Mozilla Corporation	5	● Critical	24-May-2016	05-Mar-20...
TeamViewer	Signed	TeamViewer GmbH	Unknown	● Critical	24-May-2016	24-May-20...
11.0.59518.0			Unknown	● Critical	24-May-2016	13-Jul-2016
10.0.47484.0			Unknown	● Critical	24-May-2016	06-Aug-20...
11.0.62308.0			Unknown	● Critical	13-Jul-2016	22-Jul-2016
11.0.63017.0			Unknown	● Critical	22-Jul-2016	14-Aug-20...
11.0.64630.0			Unknown	● Critical	10-Aug-2016	20-Aug-20...
FortiClient Console	Signed	Fortinet Inc.	Unknown	● Critical	24-May-2016	12-Sep-2016
iTunes	Signed	Apple Inc.	Unknown	● Critical	24-May-2016	13-Sep-2016
Safari	Signed	Apple Inc.	5	● Critical	26-May-2016	28-Jun-2018
Node.js	Signed	Node.js	Unknown	● Critical	29-May-2016	13-Sep-2016
Google Chrome	Signed	Google	5	● Critical	29-May-2016	15-Oct-2020
VLC media player	Signed	VideoLAN	Unknown	● Critical	29-May-2016	11-Sep-2016
PostgreSQL	Unsign...	PostgreSQL Global Develop...	Unknown	● Critical	30-May-2016	13-Sep-2016

VERSION DETAILS

TeamViewer, v. 11.0.59518.0

Policies

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

Vulnerabilities

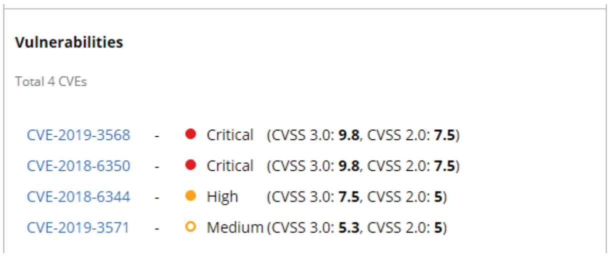
Total 5 CVEs

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

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

- Unknown
- Low
- Medium
- High
- Critical

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



Vulnerabilities

Total 4 CVEs

CVE-2019-3568 - ● Critical (CVSS 3.0: **9.8**, CVSS 2.0: **7.5**)

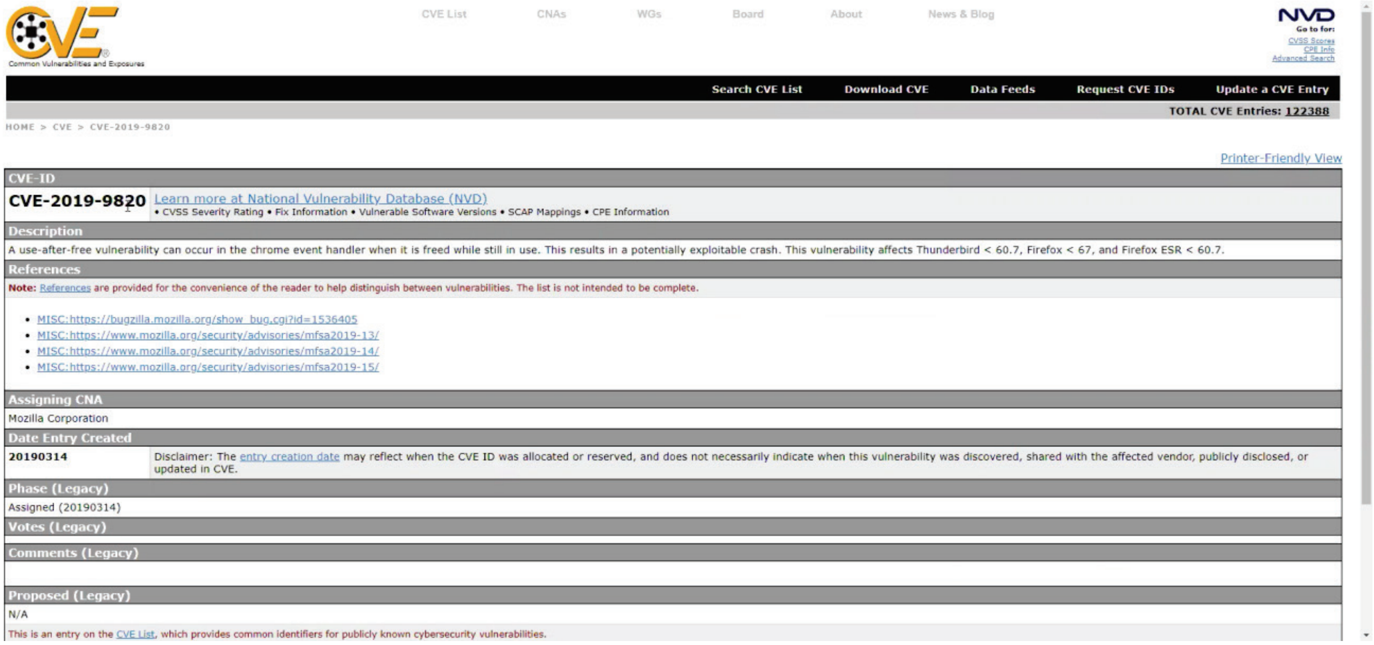
CVE-2018-6350 - ● Critical (CVSS 3.0: **9.8**, CVSS 2.0: **7.5**)

CVE-2018-6344 - ● High (CVSS 3.0: **7.5**, CVSS 2.0: **5**)

CVE-2019-3571 - ○ Medium (CVSS 3.0: **5.3**, CVSS 2.0: **5**)

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.



CVE-ID

CVE-2019-9820 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

A use-after-free vulnerability can occur in the chrome event handler when it is freed while still in use. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:https://bugzilla.mozilla.org/show_bug.cgi?id=1536405
- MISC:https://www.mozilla.org/security/advisories/mfsa2019-13/
- MISC:https://www.mozilla.org/security/advisories/mfsa2019-14/
- MISC:https://www.mozilla.org/security/advisories/mfsa2019-15/

Assigning CNA

Mozilla Corporation

Date Entry Created

20190314 Disclaimer: The entry creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20190314)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

N/A

This is an entry on the CVE List, which provides common identifiers for publicly known cybersecurity vulnerabilities.

After a vulnerability is detected in your system, you can decide the type of the action needed to address it. Typically, it is recommended to upgrade to a newer version of the application, meaning one that does not have the identified vulnerability. Alternatively, virtual patching can be applied with vulnerability-based policy that is configured to block communication of any application with known critical vulnerability. For more details, see page 136. 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 132.

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 129.

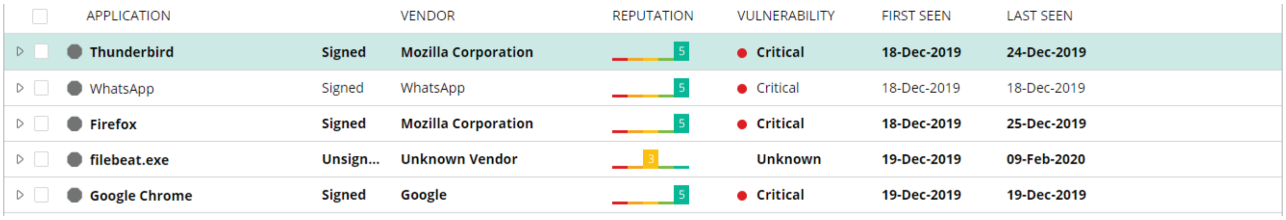
Sorting the Application List

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

Marking an Entry as Read/Unread

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

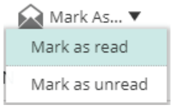
The first time that an application/version is detected in the application list, it is shown in **bold**. **Bold** indicates that the item is unread (see below).



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

To mark an entity as read:

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

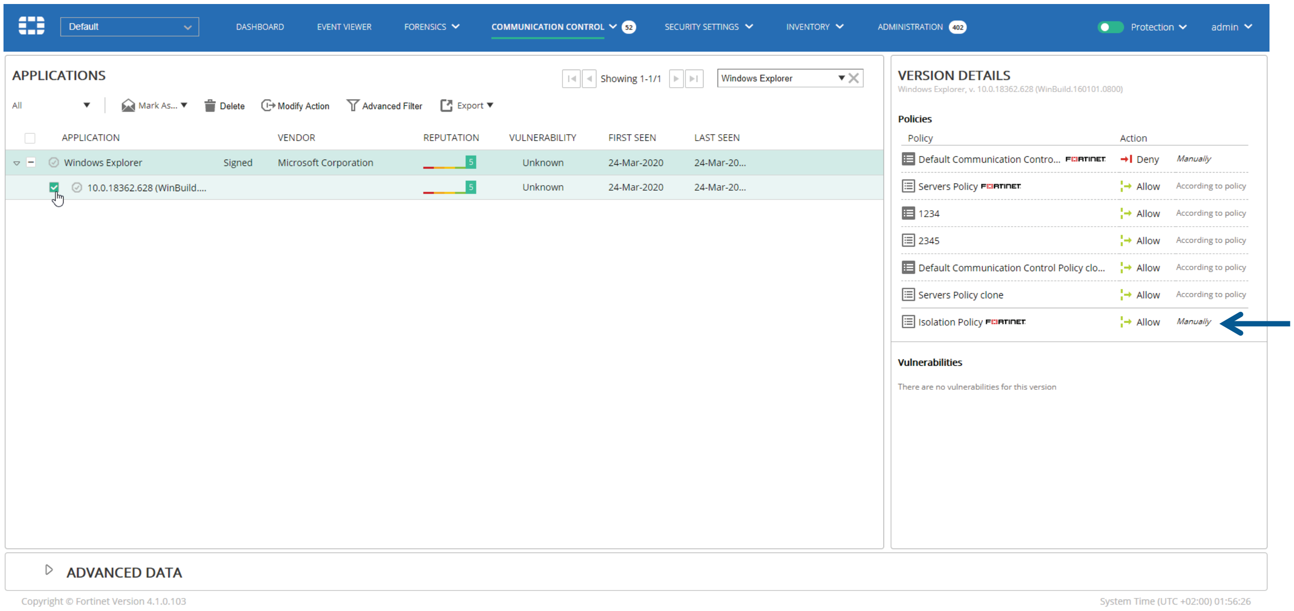
  

  Note – If you mark an application version as read, all lower levels in the version hierarchy for that application are also marked as read.

Modifying a Policy Action

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

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



□	APPLICATION		VENDOR	REPUTATION	VULNERABILITY	FIRST SEEN	LAST SEEN
▽ −	Windows Explorer	Signed	Microsoft Corporation	5	Unknown	24-Mar-2020	24-Mar-20...
☑	10.0.18362.628 (WinBuild....			5	Unknown	24-Mar-2020	24-Mar-20...

VERSION DETAILS

Windows Explorer, v. 10.0.18362.628 (WinBuild.160101.0800)

Policies

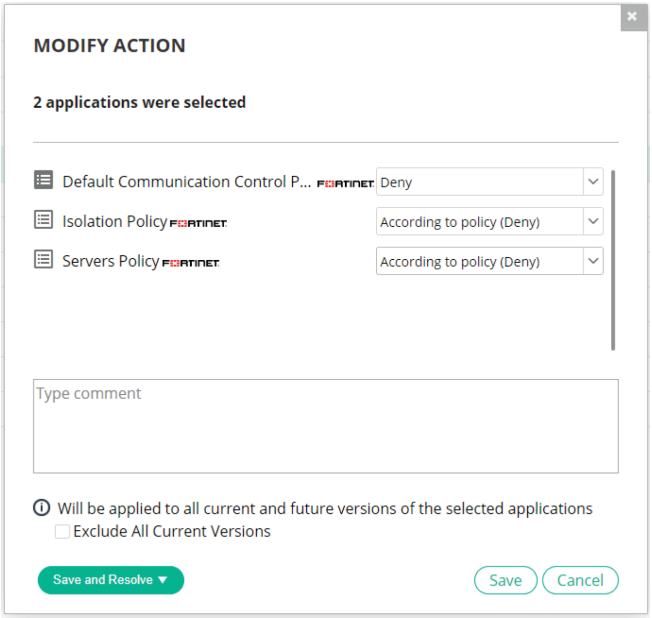
Policy	Action	
Default Communication Contro... FORTINET	Deny	*Manually*
Servers Policy FORTINET	Allow	According to policy
1234	Allow	According to policy
2345	Allow	According to policy
Default Communication Control Policy clo...	Allow	According to policy
Servers Policy clone	Allow	According to policy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

Vulnerabilities

There are no vulnerabilities for this version

To modify a policy action:

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



MODIFY ACTION

2 applications were selected

Default Communication Control P...	FORTINET	Deny
Isolation Policy	FORTINET	According to policy (Deny)
Servers Policy	FORTINET	According to policy (Deny)

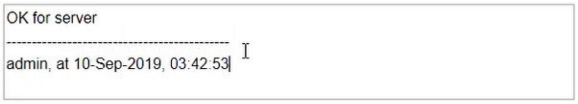
Type comment

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

□ Exclude All Current Versions

2 In the dropdown list on the right of the policy row whose action you want to change, click the down arrow and then select the action to apply to the selected entity. You can change the action for one or more policies.

3 [Optional] In the **Comment** field, enter a free-text comment describing the action change. By default, the date and time when the policy action was changed automatically displays.

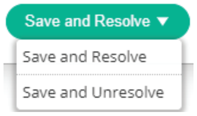


OK for server

----

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

4 [Optional] Check the **Exclude All Current Versions** checkbox if you want to exclude existing application versions from the decision. In this case, the new communication control decision only applies to a future version of the product. The application of the policy action change applies for current versions of the application. When this checkbox is not selected, the change is applied to all versions of the application.

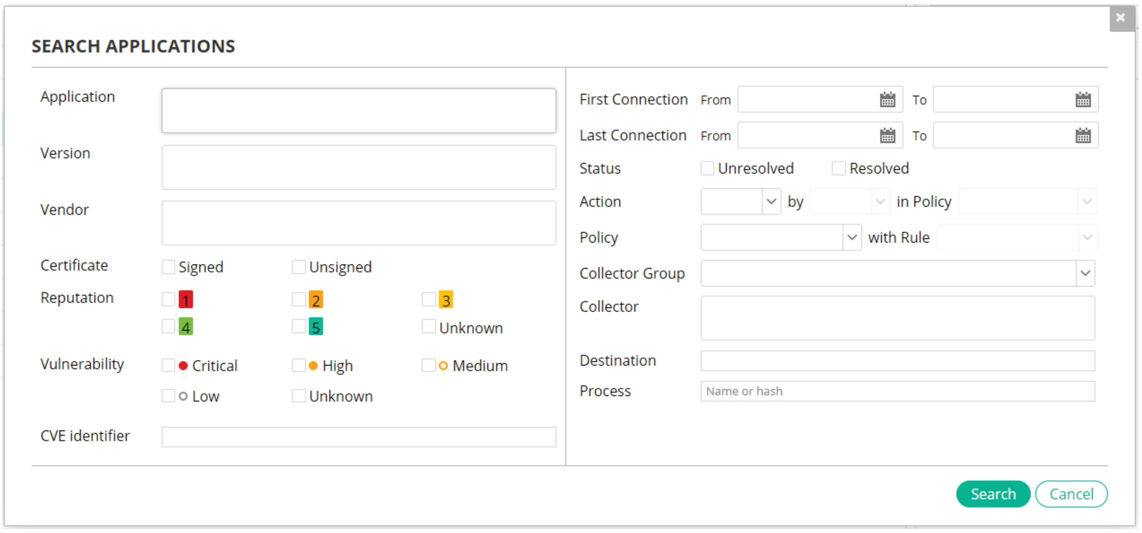


5 Click the arrow next to the button to save the new communication control decision for the selected application(s).

When any FortiEDR Central Manager user marks an application/version as **Resolved**, all users see it as having been resolved. You can also mark an application/version as resolved using the ✓ icon in its row in the application list.

Searching the Application List

You can use the field to perform an advanced search. Click the down arrow to open the Search Applications window, in which you specify your search criteria.

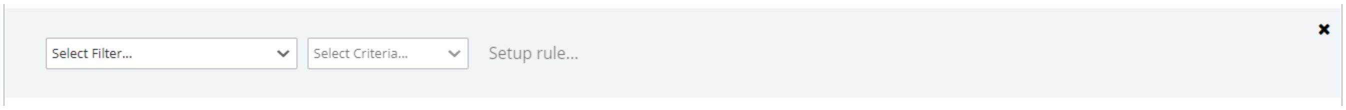


You can filter the application list by the following criteria:

- **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 129.
- 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 129.
- 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 140 for more details.

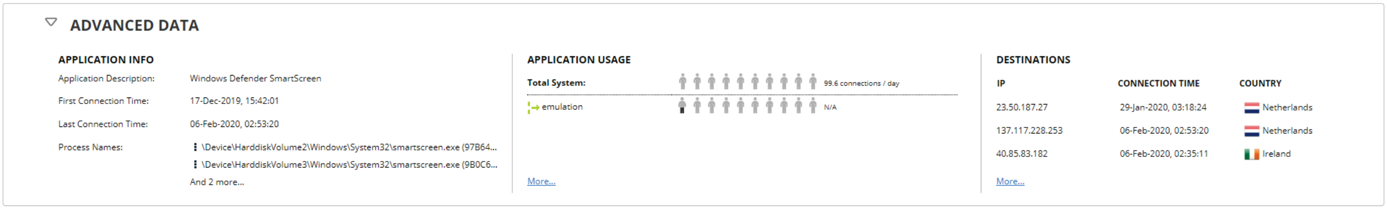
- Export ▼: Click the down arrow in the Export ▼ button and select the format for exporting data. You can select **PDF**, **Excel** or **JSON**.
- Search Application ▼ 🔍 : Use the **Search Application** field to perform an advanced search, as described in the *Searching the Application* List section on page 131.

Advanced Data

The Advanced Data area presents statistics about the selected entity in the application list. The information that displays varies, depending on the entity selected (application or version).

Application Advanced Data

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



ADVANCED DATA

APPLICATION INFO

Application Description: Windows Defender SmartScreen
First Connection Time: 17-Dec-2019, 15:42:01
Last Connection Time: 06-Feb-2020, 02:53:20
Process Names: \Device\HarddiskVolume2\Windows\System32\smartscreen.exe (97B64...
\Device\HarddiskVolume3\Windows\System32\smartscreen.exe (9B0C6...
And 2 more...

APPLICATION USAGE

Total System: 99.6 connections / day
emulation N/A
More...

DESTINATIONS

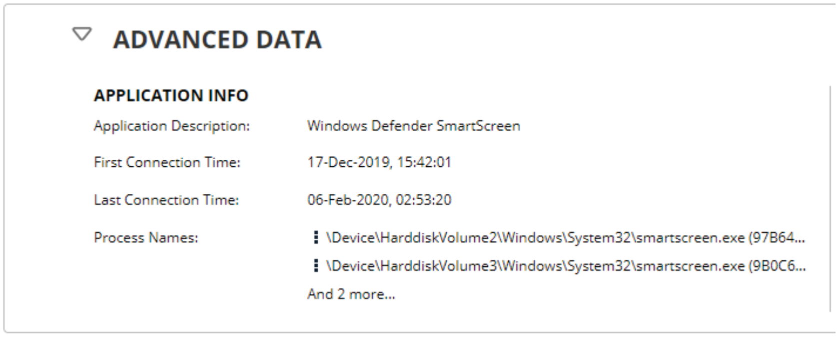
IP	CONNECTION TIME	COUNTRY
23.50.187.27	29-Jan-2020, 03:18:24	Netherlands
137.117.228.253	06-Feb-2020, 02:53:20	Netherlands
40.85.83.182	06-Feb-2020, 02:35:11	Ireland

More...

- **Application Information,** page 133
- **Application Usage,** page 133
- **Destinations,** page 134

Application Information

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



ADVANCED DATA

APPLICATION INFO

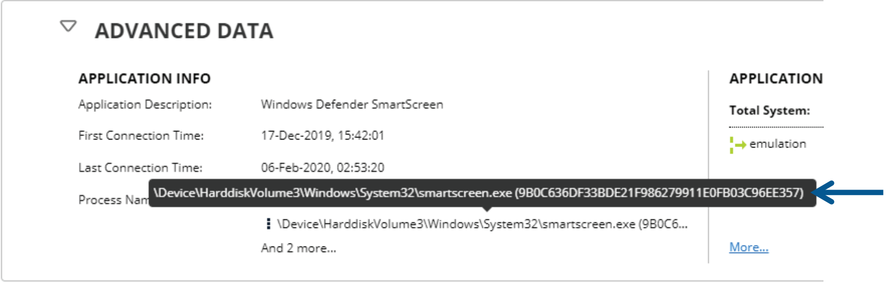
Application Description: Windows Defender SmartScreen

First Connection Time: 17-Dec-2019, 15:42:01

Last Connection Time: 06-Feb-2020, 02:53:20

Process Names:
⋮ \Device\HarddiskVolume2\Windows\System32\smartscreen.exe (97B64...
⋮ \Device\HarddiskVolume3\Windows\System32\smartscreen.exe (9B0C6...
And 2 more...

In the **Process names** field, a separate row appears for each application that shares the same vendor, product and version properties. The **Process names** field displays the full file path for each such application.



ADVANCED DATA

APPLICATION INFO

Application Description: Windows Defender SmartScreen

First Connection Time: 17-Dec-2019, 15:42:01

Last Connection Time: 06-Feb-2020, 02:53:20

Process Nam \Device\HarddiskVolume3\Windows\System32\smartscreen.exe (9B0C636DF33BDE21F986279911E0FB03C96EE357)
⋮ \Device\HarddiskVolume3\Windows\System32\smartscreen.exe (9B0C6...
And 2 more...

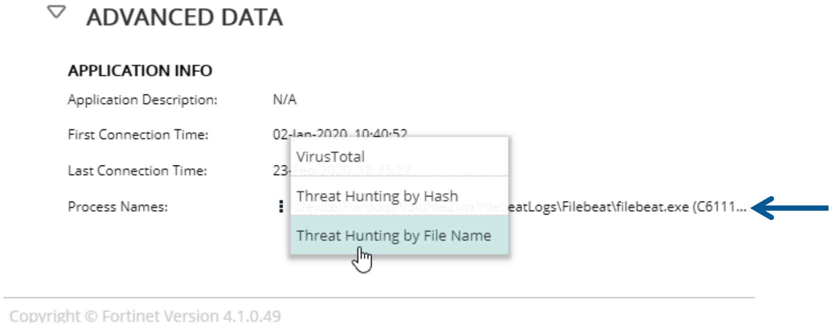
APPLICATION

Total System:

emulation

More...

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



ADVANCED DATA

APPLICATION INFO

Application Description: N/A

First Connection Time: 02-Jan-2020, 10:40:52

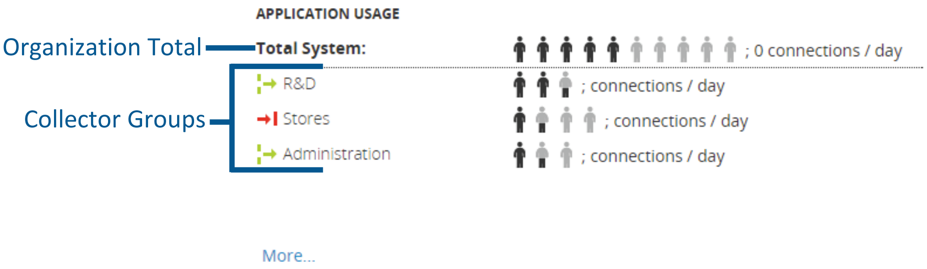
Last Connection Time: 23-

Process Names: ⋮ eatLogs\Filebeat\filebeat.exe (C6111...

Copyright © Fortinet Version 4.1.0.49

Application Usage

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



APPLICATION USAGE

Total System: ; 0 connections / day

R&D ; connections / day

Stores ; connections / day

Administration ; connections / day

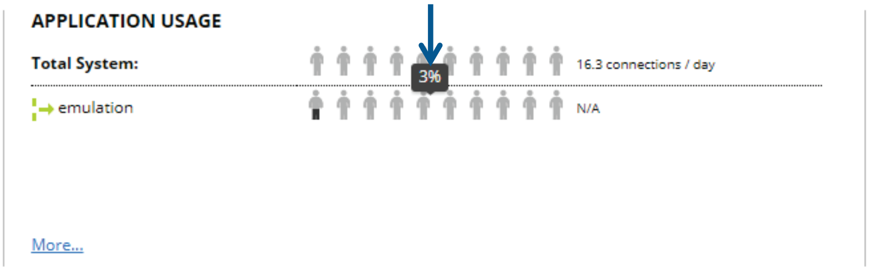
More...

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

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

Each person icon represents 10% of the total devices in the organization/Collector Group. Black icons represent devices that communicate externally using the selected application, and gray icons represent devices that did not communicate externally using the application.

You can hover over the people icons to see the percentage of devices that communicate externally per day using the selected application. For example, the figure below shows that only 3% of the devices in the organization have the selected application installed.

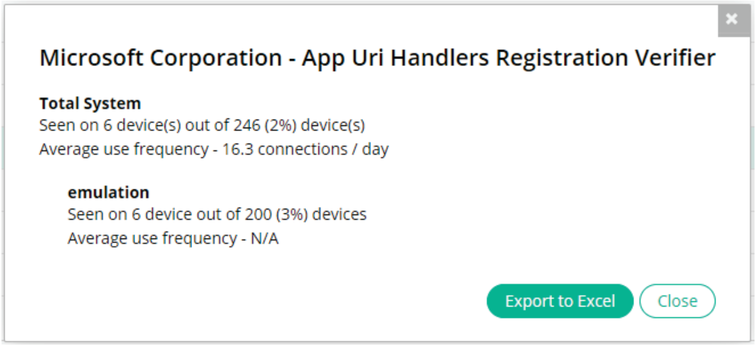


APPLICATION USAGE

Total System: 16.3 connections / day

emulation N/A

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



Microsoft Corporation - App Uri Handlers Registration Verifier

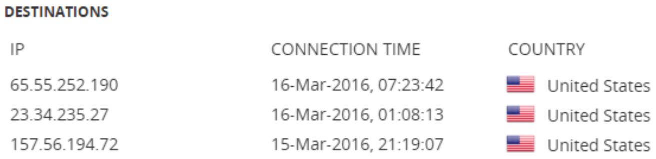
Total System
Seen on 6 device(s) out of 246 (2%) device(s)
Average use frequency - 16.3 connections / day

emulation
Seen on 6 device out of 200 (3%) devices
Average use frequency - N/A

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

Destinations

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

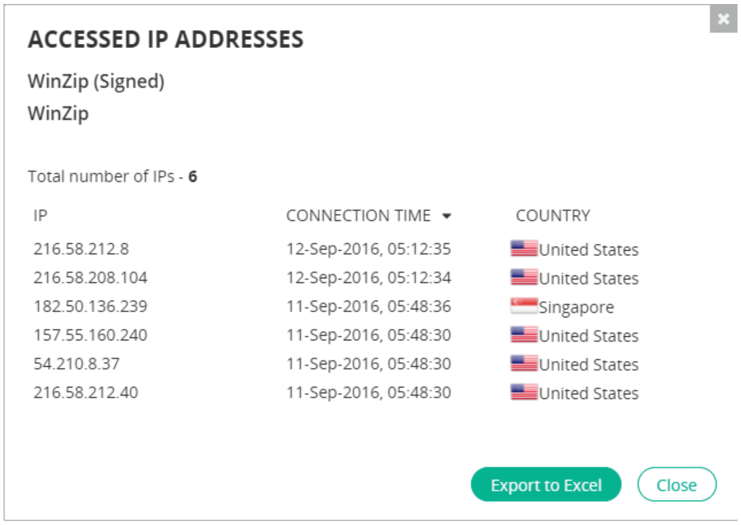


DESTINATIONS

IP	CONNECTION TIME	COUNTRY
65.55.252.190	16-Mar-2016, 07:23:42	United States
23.34.235.27	16-Mar-2016, 01:08:13	United States
157.56.194.72	15-Mar-2016, 21:19:07	United States

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

By default, this area displays the five most-recent destinations. Click the **More…** link to open the following window, which displays the last 50 destinations.



ACCESSED IP ADDRESSES

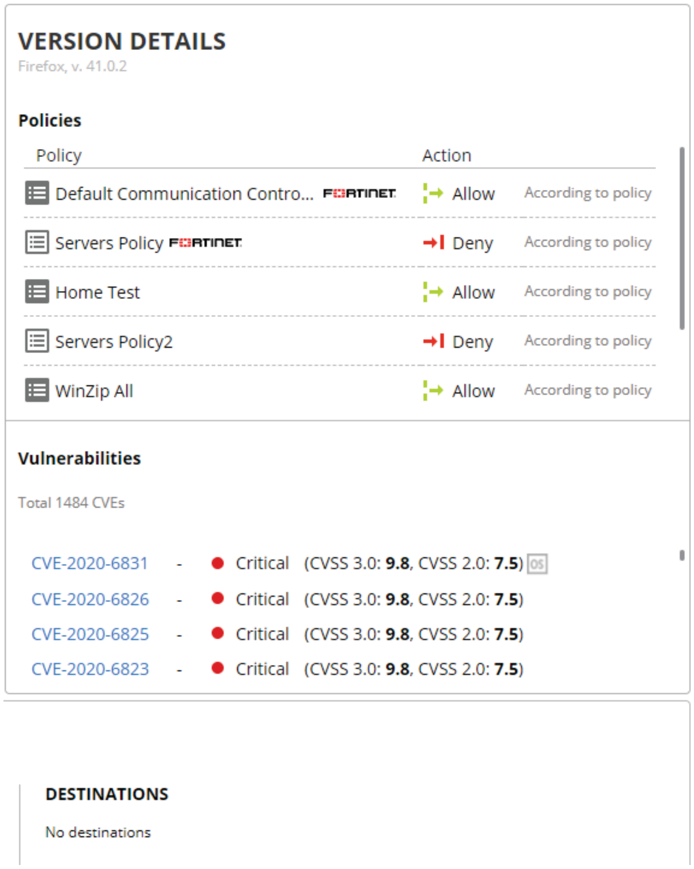
WinZip (Signed)
WinZip

Total number of IPs - **6**

IP	CONNECTION TIME ▾	COUNTRY
216.58.212.8	12-Sep-2016, 05:12:35	United States
216.58.208.104	12-Sep-2016, 05:12:34	United States
182.50.136.239	11-Sep-2016, 05:48:36	Singapore
157.55.160.240	11-Sep-2016, 05:48:30	United States
54.210.8.37	11-Sep-2016, 05:48:30	United States
216.58.212.40	11-Sep-2016, 05:48:30	United States

Version Details

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



VERSION DETAILS
Firefox, v. 41.0.2

Policies

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

Vulnerabilities

Total 1484 CVEs

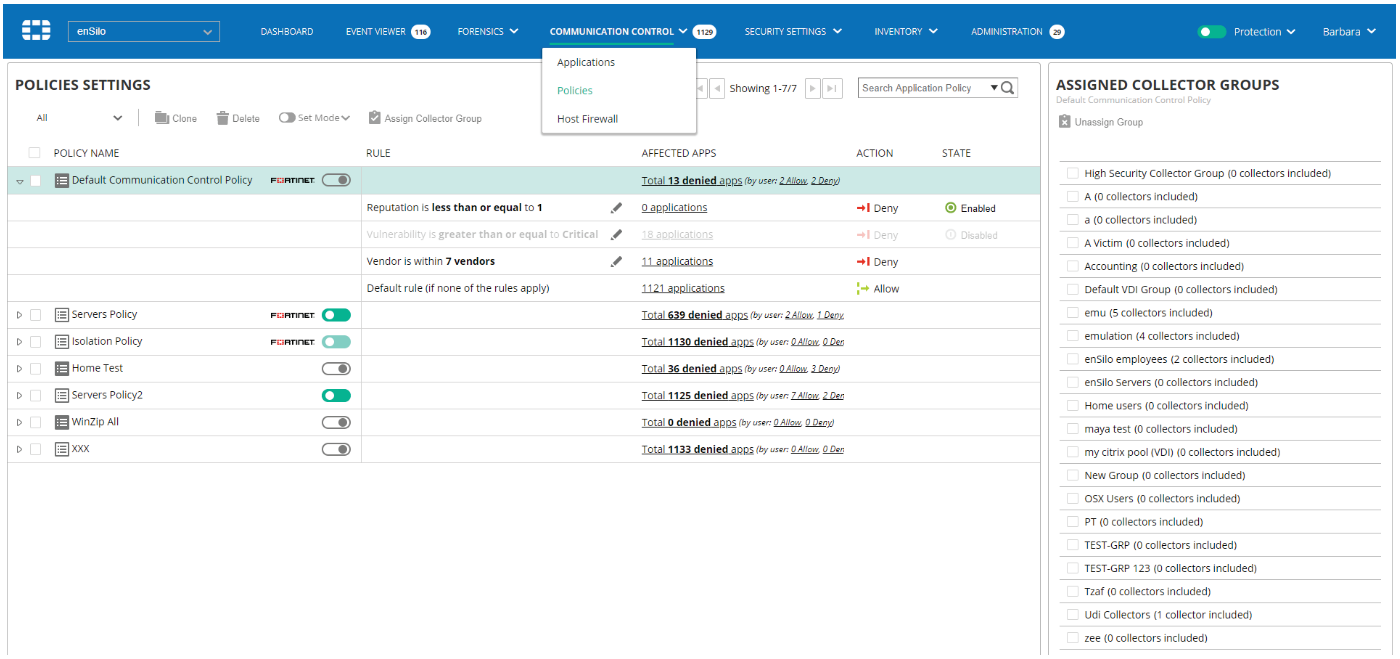
CVE-2020-6831	-	● Critical	(CVSS 3.0: **9.8**, CVSS 2.0: **7.5**) OS
CVE-2020-6826	-	● Critical	(CVSS 3.0: **9.8**, CVSS 2.0: **7.5**)
CVE-2020-6825	-	● Critical	(CVSS 3.0: **9.8**, CVSS 2.0: **7.5**)
CVE-2020-6823	-	● Critical	(CVSS 3.0: **9.8**, CVSS 2.0: **7.5**)

DESTINATIONS

No destinations

Policies

The **POLICY SETTINGS** page displays the Communication Control policies that can be applied to an application or version in the application list. Communication Control has its own policies. Each policy row can be expanded to show the rules for that policy. To access this page, click the down arrow next to **COMMUNICATION CONTROL** and then select the **Policies**.



POLICIES SETTINGS

POLICY NAME	RULE	AFFECTED APPS	ACTION	STATE
Default Communication Control Policy		Total **13 denied** apps *(by user: 2 Allow, 2 Deny)*		
	Reputation is **less than or equal** to **1**	0 applications	Deny	Enabled
	Vulnerability is **greater than or equal** to **Critical**	18 applications	Deny	Disabled
	Vendor is within **7 vendors**	11 applications	Deny	
	Default rule (if none of the rules apply)	1121 applications	Allow	
Servers Policy		Total **639 denied** apps *(by user: 2 Allow, 1 Deny*		
Isolation Policy		Total **1130 denied** apps *(by user: 0 Allow, 0 Den*		
Home Test		Total **36 denied** apps *(by user: 0 Allow, 3 Deny)*		
Servers Policy2		Total **1125 denied** apps *(by user: 7 Allow, 2 Den*		
WinZip All		Total **0 denied** apps *(by user: 0 Allow, 0 Deny)*		
XXX		Total **1133 denied** apps *(by user: 0 Allow, 0 Den*		

ASSIGNED COLLECTOR GROUPS

Default Communication Control Policy

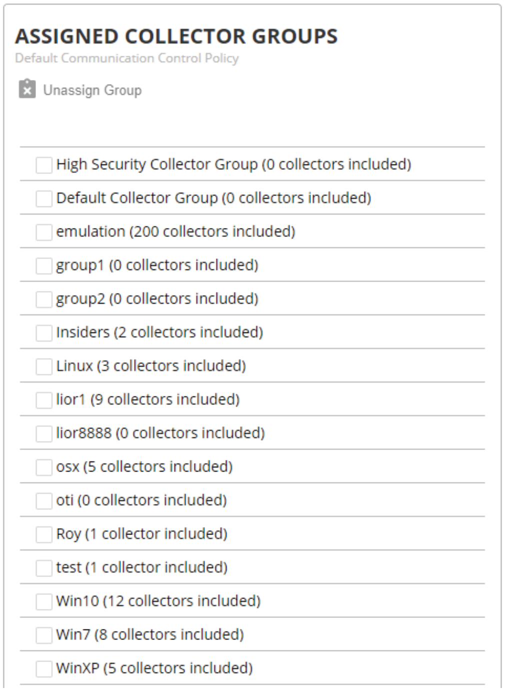
- □ High Security Collector Group (0 collectors included)
- □ A (0 collectors included)
- □ a (0 collectors included)
- □ A Victim (0 collectors included)
- □ Accounting (0 collectors included)
- □ Default VDI Group (0 collectors included)
- □ emu (5 collectors included)
- □ emulation (4 collectors included)
- □ enSilo employees (2 collectors included)
- □ enSilo Servers (0 collectors included)
- □ Home users (0 collectors included)
- □ maya test (0 collectors included)
- □ my citrix pool (VDI) (0 collectors included)
- □ New Group (0 collectors included)
- □ OSX Users (0 collectors included)
- □ PT (0 collectors included)
- □ TEST-GRP (0 collectors included)
- □ TEST-GRP 123 (0 collectors included)
- □ Tzaf (0 collectors included)
- □ Udi Collectors (1 collector included)
- □ zee (0 collectors included)

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 139.
- **AFFECTED APPS:** The number of applications affected by the policy.
- **ACTION:** Specifies the action that is enforced when this rule is violated (Allow or Deny).
- **STATE (Enabled/Disabled):** This option enables you to disable/enable this rule.

The Assigned Collector Groups area on the right lists the Collector Group(s) assigned to the policy.



ASSIGNED COLLECTOR GROUPS

Default Communication Control Policy

Unassign Group

- □ High Security Collector Group (0 collectors included)
- □ Default Collector Group (0 collectors included)
- □ emulation (200 collectors included)
- □ group1 (0 collectors included)
- □ group2 (0 collectors included)
- □ Insiders (2 collectors included)
- □ Linux (3 collectors included)
- □ lior1 (9 collectors included)
- □ lior8888 (0 collectors included)
- □ osx (5 collectors included)
- □ oti (0 collectors included)
- □ Roy (1 collector included)
- □ test (1 collector included)
- □ Win10 (12 collectors included)
- □ Win7 (8 collectors included)
- □ WinXP (5 collectors included)

Predefined Policies

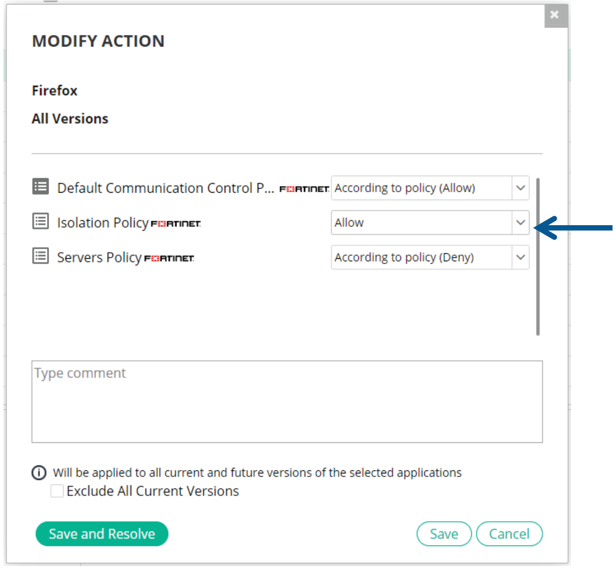
FortiEDR is provided out-of-the-box with several predefined policies, ready for you to get started. These policies are marked with the FORTINET logo. The **Default Communication Control** policy is one such policy, and is always listed first in the list of policies. The Default Communication Control policy is a 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:



MODIFY ACTION

Firefox

All Versions

Default Communication Control P... FORTINET	According to policy (Allow)
Isolation Policy FORTINET	Allow
Servers Policy FORTINET	According to policy (Deny)

Type comment
Will be applied to all current and future versions of the selected applications
□ Exclude All Current Versions
Save and Resolve
Save
Cancel

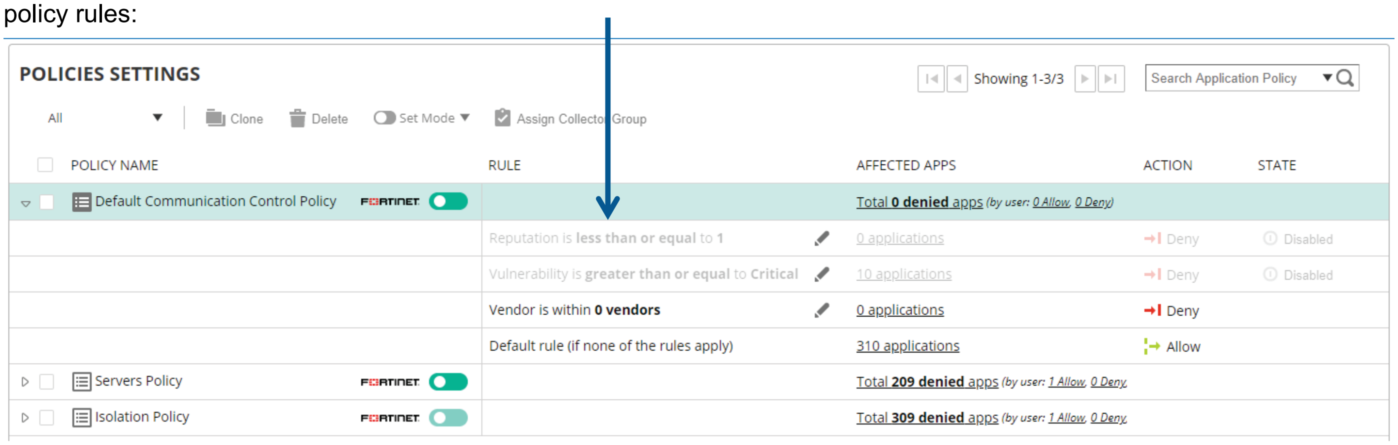
4. In the Isolation Policy row, select **Allow** in the dropdown menu.

Policy Mode

The slider for a policy indicates the current mode for the policy. A green slider indicates Prevention mode and a gray slider indicates Simulation mode. You can change the mode using the Set mode 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 52.

Policy Rules

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



POLICIES SETTINGS

Showing 1-3/3 | Search Application Policy

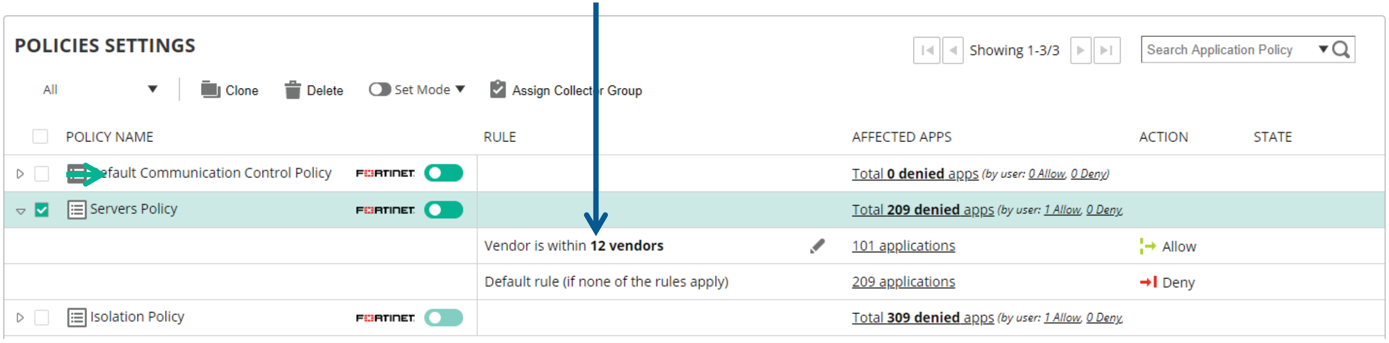
All ▼ | Clone | Delete | Set Mode ▼ | Assign Collector Group

□	POLICY NAME	RULE	AFFECTED APPS	ACTION	STATE
▽ □	Default Communication Control Policy FORTINET		Total **0 denied** apps (by user: 0 Allow, 0 Deny)		
		Reputation is **less than or equal** to **1**	0 applications	Deny	Disabled
		Vulnerability is **greater than or equal** to **Critical**	10 applications	Deny	Disabled
		Vendor is within **0 vendors**	0 applications	Deny	
		Default rule (if none of the rules apply)	310 applications	Allow	
▷ □	Servers Policy FORTINET		Total **209 denied** apps (by user: 1 Allow, 0 Deny)		
▷ □	Isolation Policy FORTINET		Total **309 denied** apps (by user: 1 Allow, 0 Deny)		

- **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:



POLICIES SETTINGS

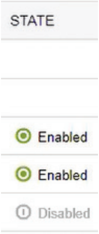
Showing 1-3/3 | Search Application Policy

All ▼ | Clone | Delete | Set Mode ▼ | Assign Collector Group

□	POLICY NAME	RULE	AFFECTED APPS	ACTION	STATE
▷ □	Default Communication Control Policy FORTINET		Total **0 denied** apps (by user: 0 Allow, 0 Deny)		
▽ ☑	Servers Policy FORTINET		Total **209 denied** apps (by user: 1 Allow, 0 Deny)		
		Vendor is within **12 vendors**	101 applications	Allow	
		Default rule (if none of the rules apply)	209 applications	Deny	
▷ □	Isolation Policy FORTINET		Total **309 denied** apps (by user: 1 Allow, 0 Deny)		

- Vendor is within 12 vendors. This rule is enabled for the policy. The action for this rule is Allow.
- Default rule (if none of the rules apply). This rule is always enabled.

You can enable or disable a rule for a policy by clicking the Enabled/Disabled button in the State column of the applicable rule. This button toggles between **Enabled/Disabled**.



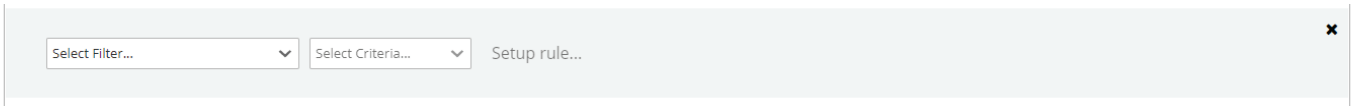
STATE
Enabled
Enabled
Disabled

Editing a Policy Rule

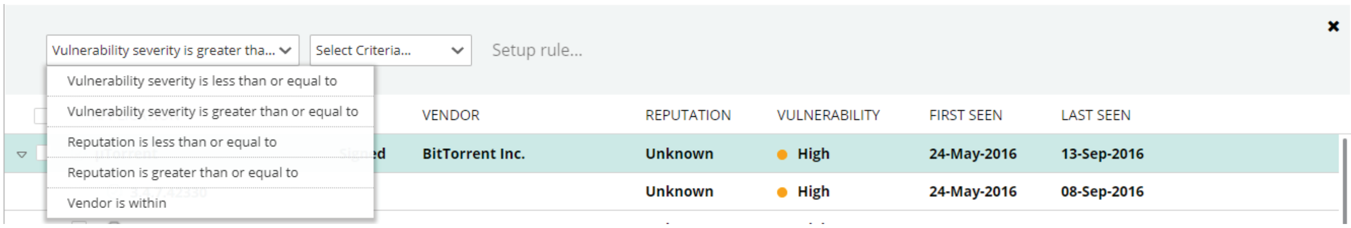
The four rules for a policy can be modified, as needed.

To edit a rule:

1 Click the **Edit** ✎ button for the rule of the policy that you want to modify. This switches the view to the **APPLICATIONS** page, enabling you to review the applications affected by this rule before saving it. The following displays:

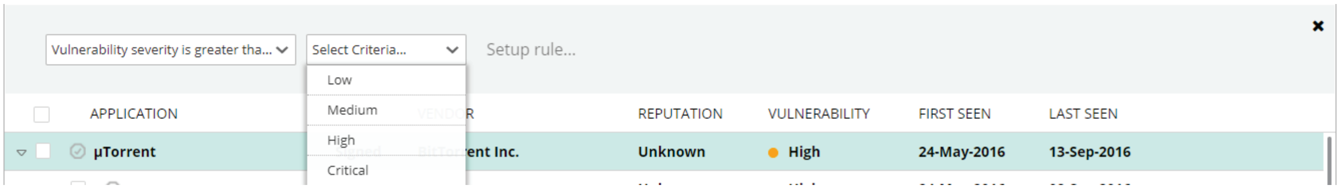


2 In the **Select Filter** dropdown list, select the parameter whose value you want to set in the rule. This dropdown list lists the parameters available to configure for the rule.


Vulnerability severity is greater tha...
Select Criteria...
Setup rule...
✖
Vulnerability severity is less than or equal to
Vulnerability severity is greater than or equal to
Reputation is less than or equal to
Reputation is greater than or equal to
Vendor is within

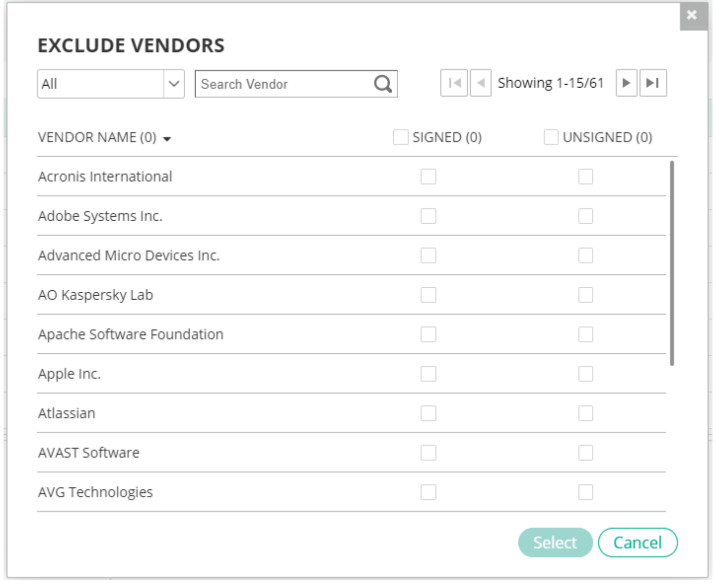
VENDOR	REPUTATION	VULNERABILITY	FIRST SEEN	LAST SEEN
BitTorrent Inc.	Unknown	● High	24-May-2016	13-Sep-2016
	Unknown	● High	24-May-2016	08-Sep-2016

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



APPLICATION	VENDOR	REPUTATION	VULNERABILITY	FIRST SEEN	LAST SEEN
µTorrent	BitTorrent Inc.	Unknown	● High	24-May-2016	13-Sep-2016

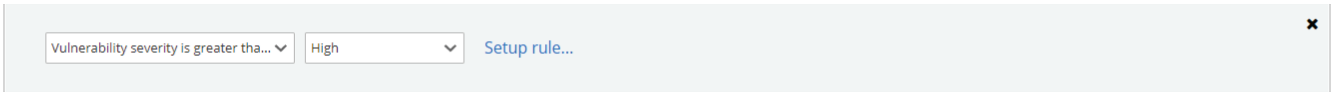
Note – When modifying the **Vendor is within X vendors** rule, you specify the vendor(s) to include and those to exclude for the rule.



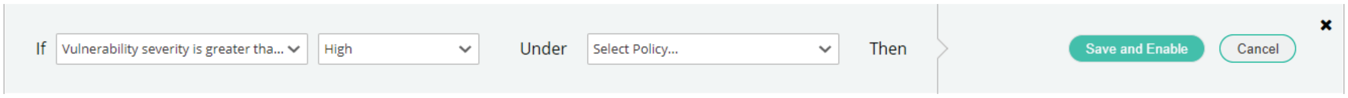
EXCLUDE VENDORS

VENDOR NAME (0)	□ SIGNED (0)	□ UNSIGNED (0)
Acronis International	□	□
Adobe Systems Inc.	□	□
Advanced Micro Devices Inc.	□	□
AO Kaspersky Lab	□	□
Apache Software Foundation	□	□
Apple Inc.	□	□
Atlassian	□	□
AVAST Software	□	□
AVG Technologies	□	□

4 Click the **Setup rule** link.

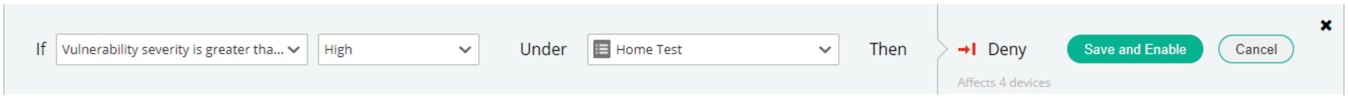


5 In the **Under** dropdown list, select the policy to which this rule applies.



If: Vulnerability severity is greater tha... | High | Under: Select Policy... | Then

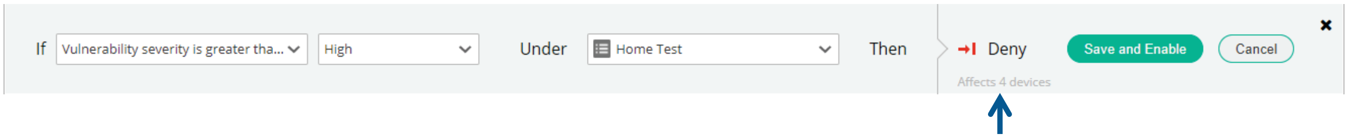
6 In the **Then** field, specify whether to **Allow** or **Deny** the application based on this rule.



If: Vulnerability severity is greater tha... | High | Under: Home Test | Then: Deny

Affects 4 devices

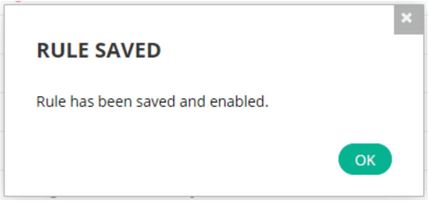
The application list now shows the number of application(s) affected by the rule change.



If: Vulnerability severity is greater tha... | High | Under: Home Test | Then: Deny

Affects 4 devices

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



RULE SAVED

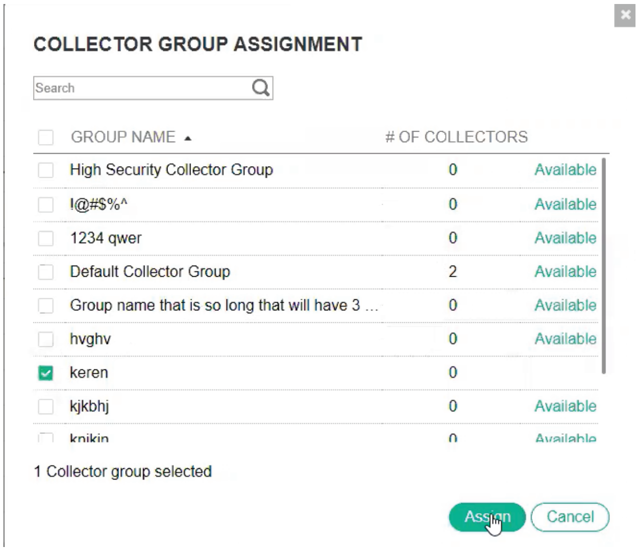
Rule has been saved and enabled.

8 Click **OK**.

Assigning a Policy to a Collector Group

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:



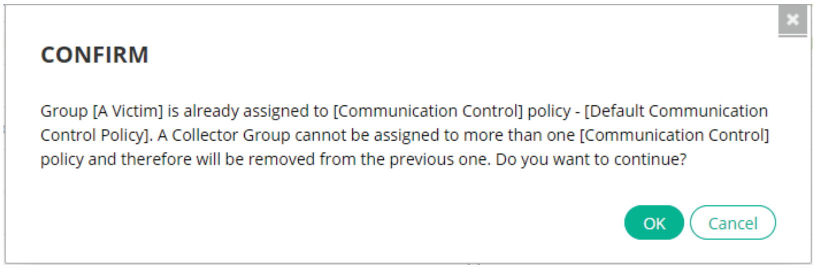
COLLECTOR GROUP ASSIGNMENT

	GROUP NAME ▲	# OF COLLECTORS	
□	High Security Collector Group	0	Available
□	!@#$%^	0	Available
□	1234 qwer	0	Available
□	Default Collector Group	2	Available
□	Group name that is so long that will have 3 ...	0	Available
□	hvghv	0	Available
☑	keren	0	
□	kjkbhj	0	Available
□	knikin	0	Available

1 Collector group selected

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

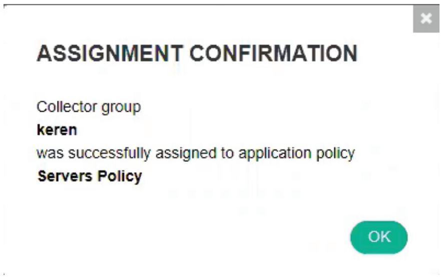
3 Click the **Assign** button. A window displays, prompting you to confirm the reassignment.



CONFIRM

Group [A Victim] is already assigned to [Communication Control] policy - [Default Communication Control Policy]. A Collector Group cannot be assigned to more than one [Communication Control] policy and therefore will be removed from the previous one. Do you want to continue?

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



ASSIGNMENT CONFIRMATION

Collector group
keren
was successfully assigned to application policy
Servers Policy

5 Click **OK**.

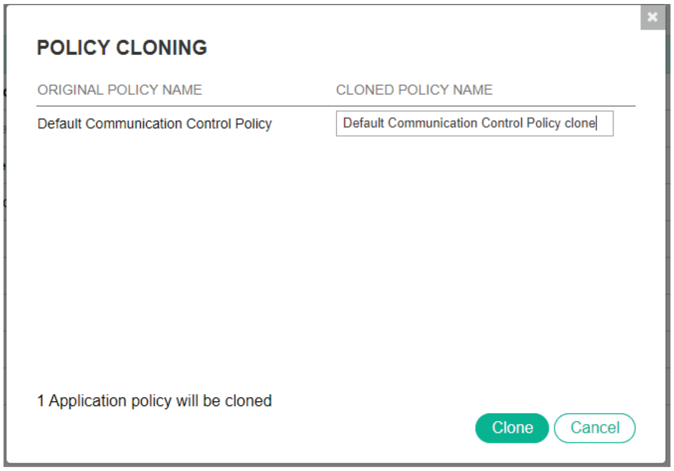
Creating a New Communication Control Policy

A new Communication Control policy can be created by cloning an existing policy, as described below. New policies are only needed if you are going to assign different policies to different Collector Groups. Otherwise, you can simply modify one of the default policies that come out-of-the-box and apply it to all FortiEDR Collector Groups by default. Modifications made on one policy do not affect any other policies.

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:



POLICY CLONING

ORIGINAL POLICY NAME	CLONED POLICY NAME
Default Communication Control Policy	Default Communication Control Policy clone

1 Application policy will be cloned

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

4 Click 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 138.

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 security event.

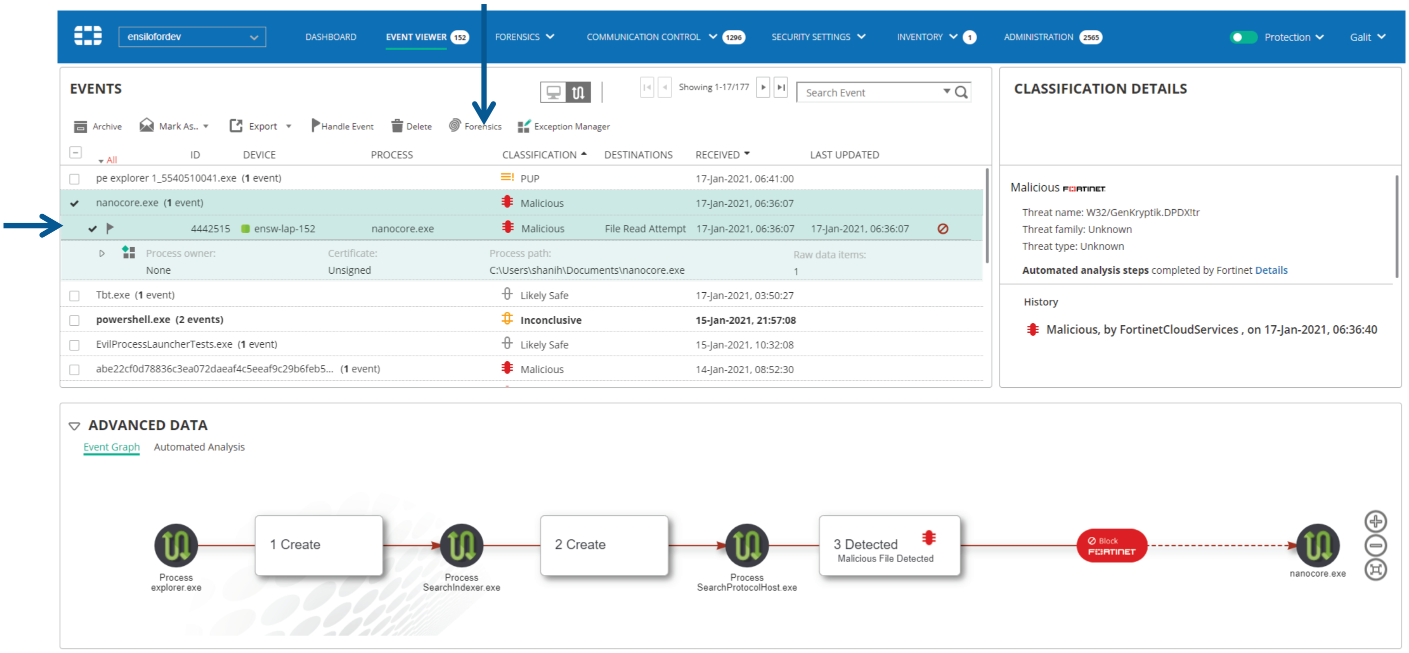
The Forensic Analysis add-on provides an abundance of deep analysis and drill-down options that reveal the process flows, memory stacks and a variety of operating system parameters in a graphic view, such as:

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

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 **Discover, Protect and Response** license.

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

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



EVENTS

All	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
□ pe explorer 1_5540510041.exe (**1** event)				PUP		17-Jan-2021, 06:41:00	
✓ nanocore.exe (**1** event)				Malicious		17-Jan-2021, 06:36:07	
✓	4442515	ensw-lap-152	nanocore.exe	Malicious	File Read Attempt	17-Jan-2021, 06:36:07	17-Jan-2021, 06:36:07
□ Tbt.exe (**1** event)				Likely Safe		17-Jan-2021, 03:50:27	
□ **powershell.exe (2 events)**				**Inconclusive**		**15-Jan-2021, 21:57:08**	
□ EvilProcessLauncherTests.exe (**1** event)				Likely Safe		15-Jan-2021, 10:32:08	
□ abe22cf0d78836c3ea072daeaf4c5eeaf9c29b6feb5... (**1** event)				Malicious		14-Jan-2021, 08:52:30	

Process owner: None
Certificate: Unsigned
Process path: C:\Users\shanih\Documents\nanocore.exe
Raw data items: 1

CLASSIFICATION DETAILS

Malicious FORTINET

Threat name: W32/GenKryptik.DPDX!tr

Threat family: Unknown

Threat type: Unknown

Automated analysis steps completed by Fortinet Details

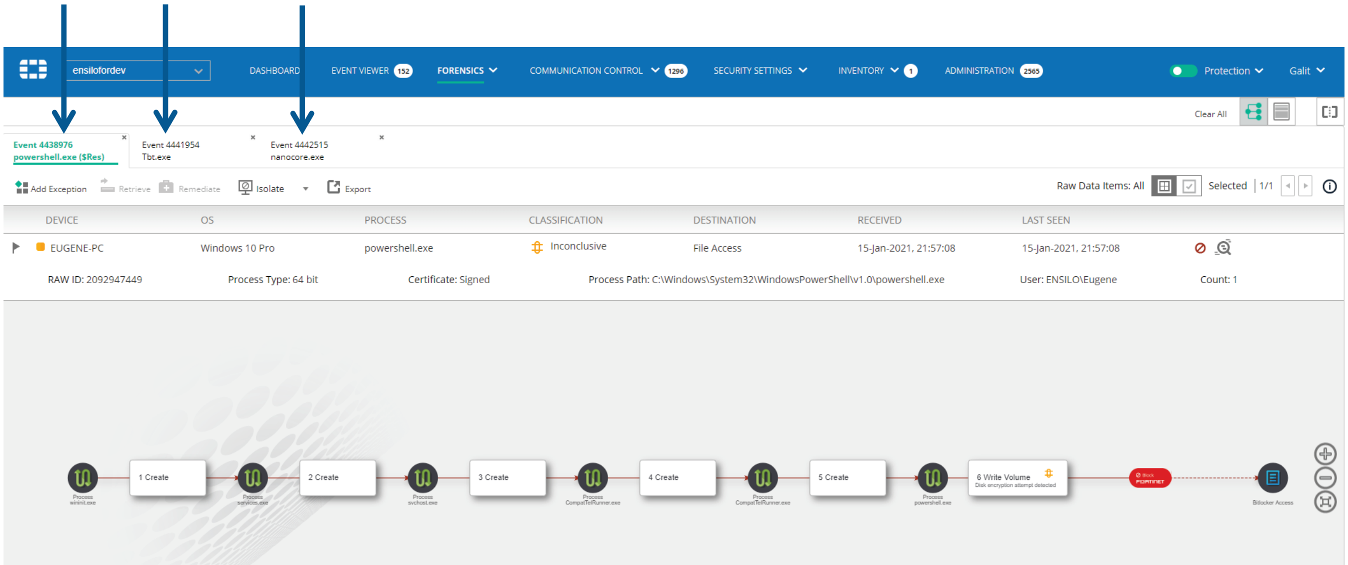
History

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

ADVANCED DATA

Event Graph Automated Analysis

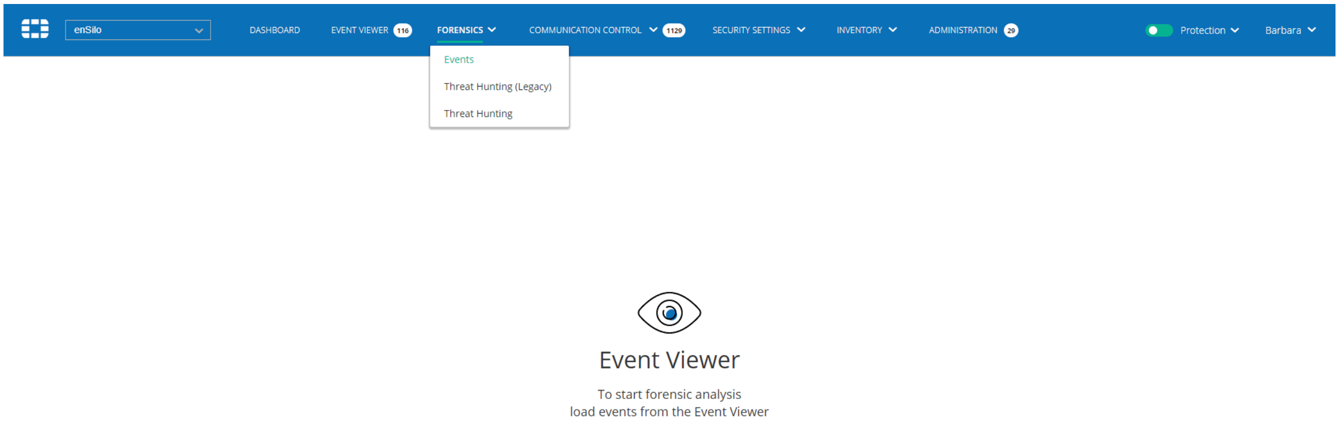
In this case, the Forensics add-on shows a separate tab for each security event associated with the security event aggregation. For example, the figure below shows seven tabs for a security event aggregation containing two events.



DEVICE	OS	PROCESS	CLASSIFICATION	DESTINATION	RECEIVED	LAST SEEN
EUGENE-PC	Windows 10 Pro	powershell.exe	Inconclusive	File Access	15-Jan-2021, 21:57:08	15-Jan-2021, 21:57:08

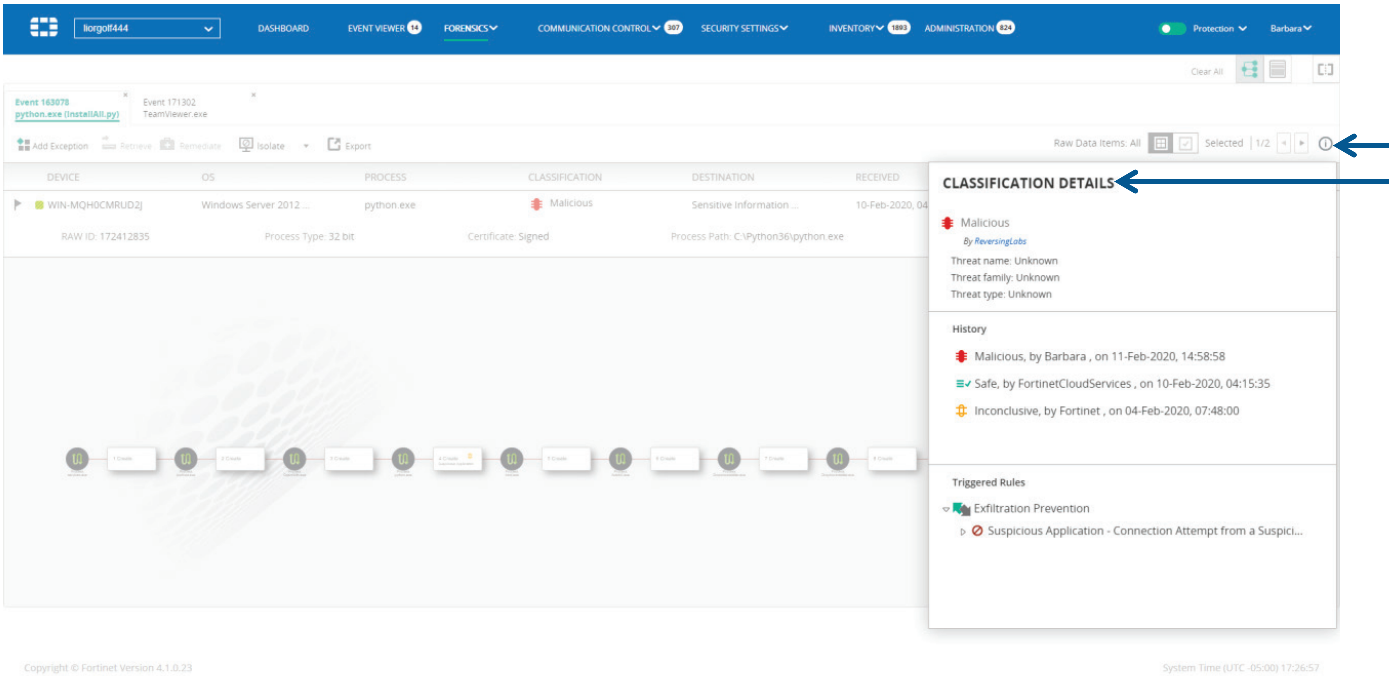
RAW ID: 2092947449 Process Type: 64 bit Certificate: Signed Process Path: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe User: ENSILO\Eugene Count: 1

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



To start forensic analysis
load events from the Event Viewer

You can click the ⓘ button in the **FORENSICS** tab to display classification details, including the classification, policy and rules assigned to the FortiEDR Collector that triggered this security event. For more details about classification details, see page 120.



DEVICE	OS	PROCESS	CLASSIFICATION	DESTINATION	RECEIVED
WIN-MQH0CMRUD2J	Windows Server 2012 ...	python.exe	Malicious	Sensitive Information ...	10-Feb-2020, 04

RAW ID: 172412835 Process Type: 32 bit Certificate: Signed Process Path: C:\Python36\python.exe

CLASSIFICATION DETAILS

Malicious
By ReversingLabs
Threat name: Unknown
Threat family: Unknown
Threat type: Unknown

History

Malicious, by Barbara , on 11-Feb-2020, 14:58:58
Safe, by FortinetCloudServices , on 10-Feb-2020, 04:15:35
Inconclusive, by Fortinet , on 04-Feb-2020, 07:48:00

Triggered Rules

Exfiltration Prevention
Suspicious Application - Connection Attempt from a Suspici...

Copyright © Fortinet Version 4.1.0.23

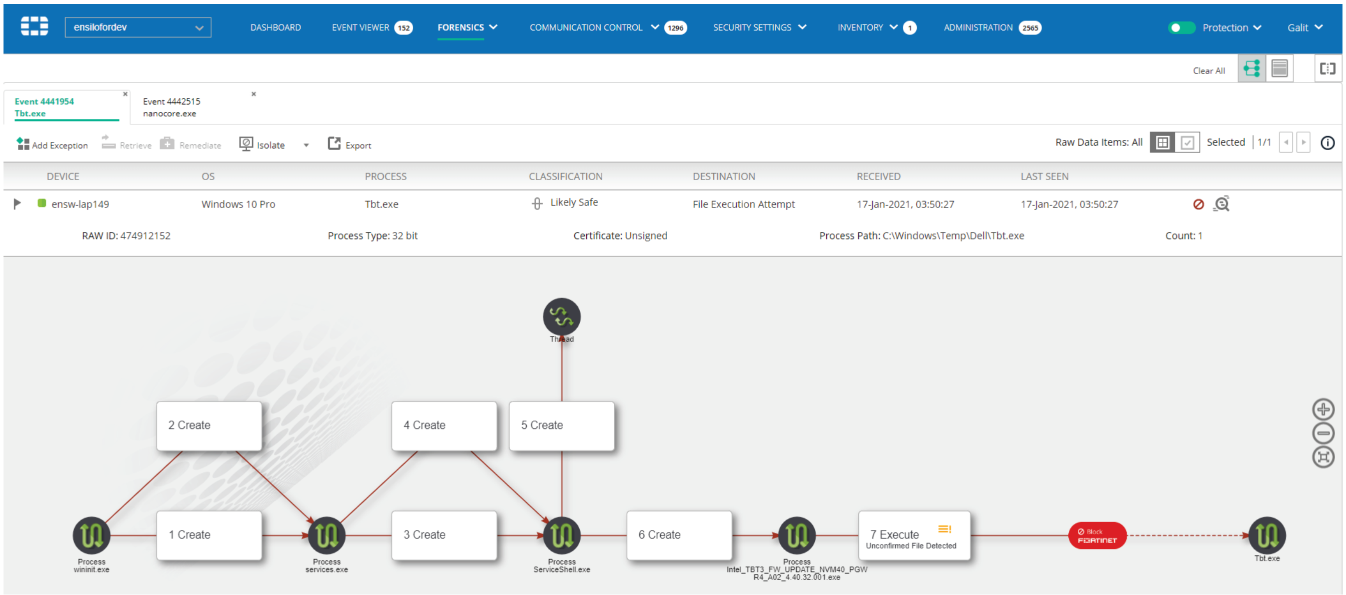
System Time (UTC -05:00) 17:26:57

To perform deep Forensic analysis:

1 Select the security events to analyze using one of the methods described on page 97.

Selected security events that are currently loaded to the **FORENSICS** tab are marked in the **Event Viewer** with a fingerprint icon.

2 Each selected security event is then displayed in the Event Viewer as a separate tab:

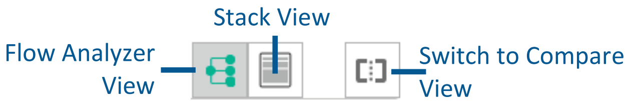


DEVICE	OS	PROCESS	CLASSIFICATION	DESTINATION	RECEIVED	LAST SEEN
ensw-lap149	Windows 10 Pro	Tbt.exe	Likely Safe	File Execution Attempt	17-Jan-2021, 03:50:27	17-Jan-2021, 03:50:27

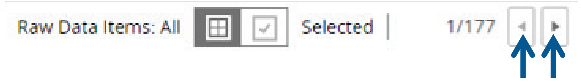
RAW ID: 474912152 Process Type: 32 bit Certificate: Unsigned Process Path: C:\Windows\Temp\Dell\Tbt.exe Count: 1

Each tab shows the same information as in the Event Viewer (page 97), with additional information as described below.

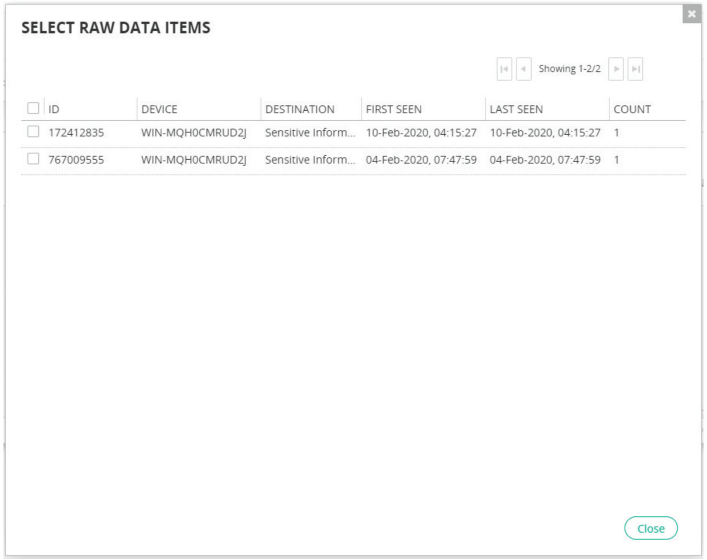
The following options for viewing more information are provided:



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



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

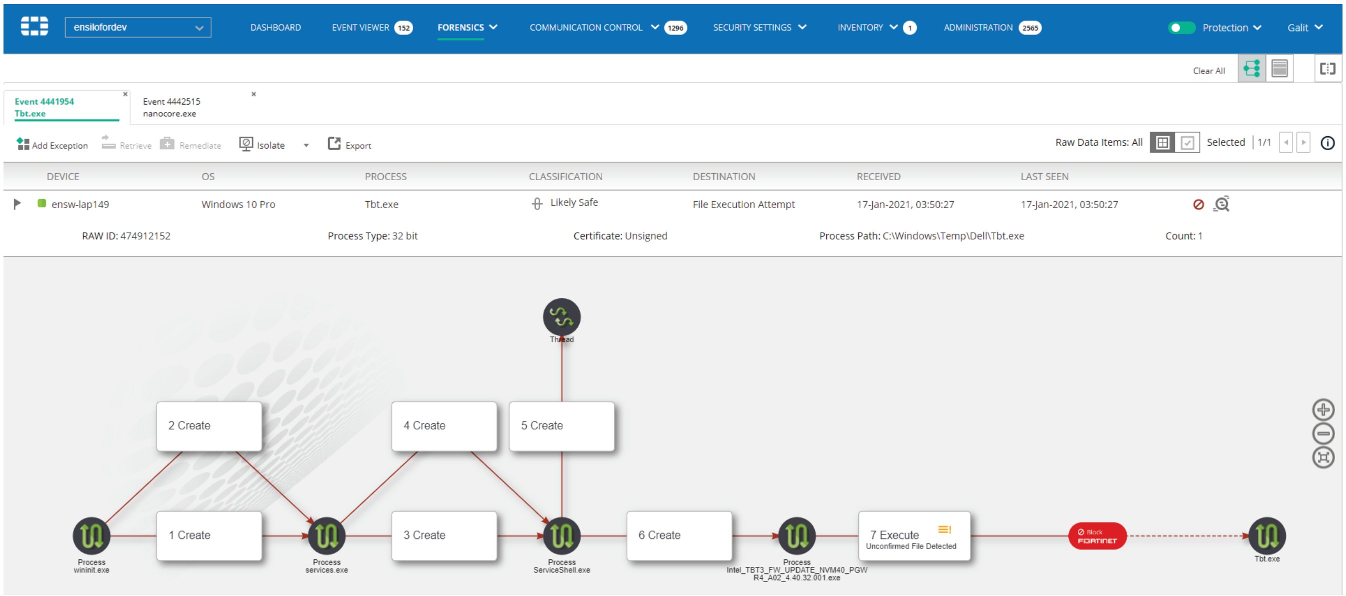


SELECT RAW DATA ITEMS

Showing 1-2/2

□ ID	DEVICE	DESTINATION	FIRST SEEN	LAST SEEN	COUNT
□ 172412835	WIN-MQHOCMRUD2J	Sensitive Inform...	10-Feb-2020, 04:15:27	10-Feb-2020, 04:15:27	1
□ 767009555	WIN-MQHOCMRUD2J	Sensitive Inform...	04-Feb-2020, 07:47:59	04-Feb-2020, 07:47:59	1

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

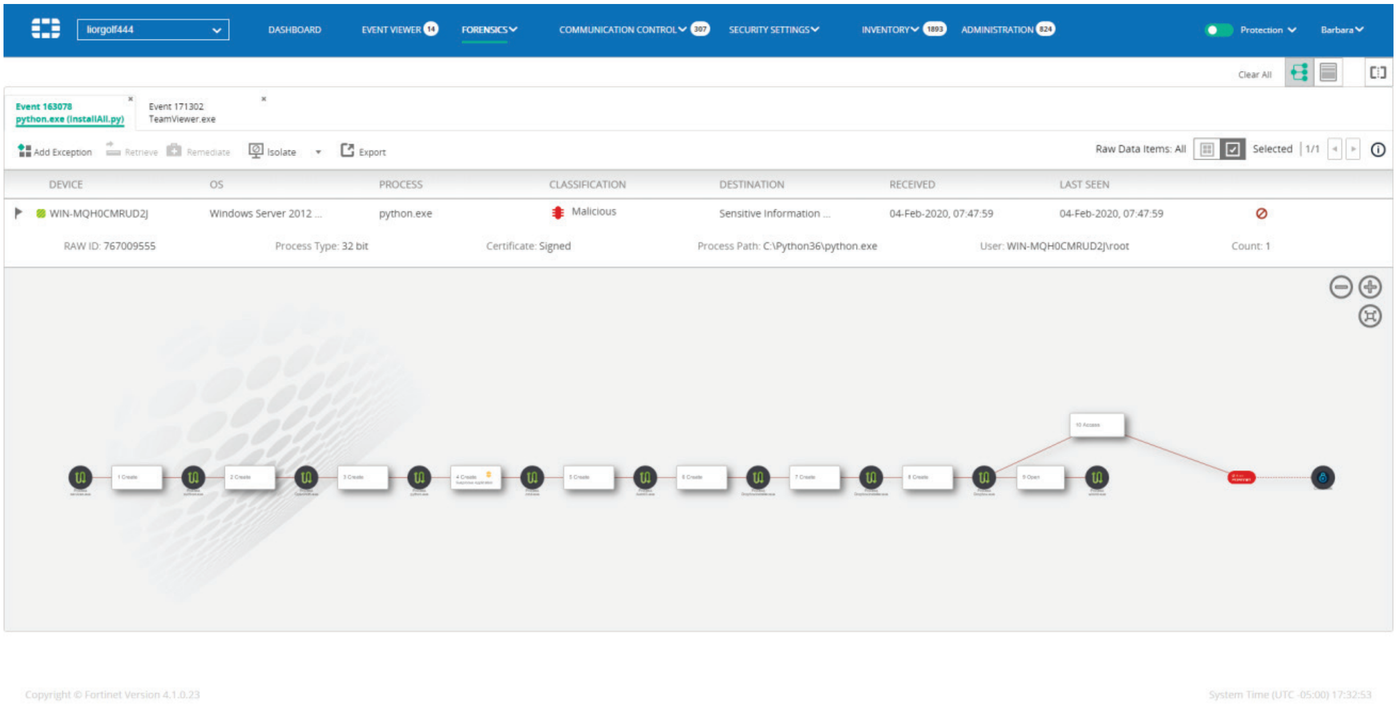


DEVICE	OS	PROCESS	CLASSIFICATION	DESTINATION	RECEIVED	LAST SEEN
ensw-lap149	Windows 10 Pro	Tbt.exe	Likely Safe	File Execution Attempt	17-Jan-2021, 03:50:27	17-Jan-2021, 03:50:27

RAW ID: 474912152 Process Type: 32 bit Certificate: Unsigned Process Path: C:\Windows\Temp\Dell\Tbt.exe Count: 1

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

Flow Analyzer View



liorgolf444 DASHBOARD EVENT VIEWER 14 FORENSICS COMMUNICATION CONTROL 307 SECURITY SETTINGS INVENTORY 1893 ADMINISTRATION 824 Protection Barbara

Clear All

Event 163078 python.exe (InstallAll.py) | Event 171302 TeamViewer.exe

Add Exception Retrieve Remediate Isolate Export | Raw Data Items: All Selected 1/1

DEVICE	OS	PROCESS	CLASSIFICATION	DESTINATION	RECEIVED	LAST SEEN
WIN-MQHOCMRUD2J	Windows Server 2012 ...	python.exe	Malicious	Sensitive Information ...	04-Feb-2020, 07:47:59	04-Feb-2020, 07:47:59

RAW ID: 767009555 Process Type: 32 bit Certificate: Signed Process Path: C:\Python36\python.exe User: WIN-MQHOCMRUD2J\root Count: 1

Copyright © Fortinet Version 4.1.0.23 System Time (UTC -05:00) 17:32:53

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

The arrows indicate the sequence of processes and specify the operation that was performed, such as **Create**, **Inject**, **Open** and so on. If multiple operations were performed between two processes, then multiple arrows are shown between them. If an operation repeated several times in the same segment, it is represented by a dashed line - - -.

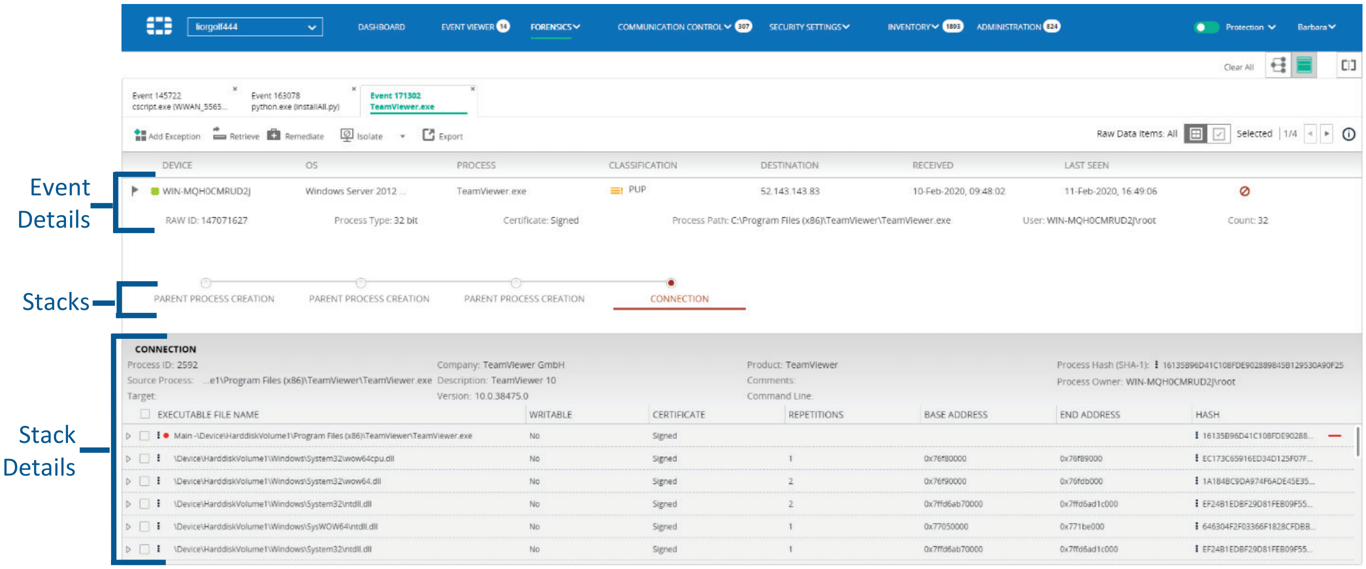
Typically, the next to last rightmost node represents a connection request Connection and specifies the IP to which it attempted to establish a connection. It can also represent an attempt to lock or encrypt a file by ransomware.

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

Log FORTINET | Block FORTINET | Block FORTINET

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



Event 145722 cscript.exe (WWAN_5565...
Event 163078 python.exe (installAll.py)
Event 171302 TeamViewer.exe

DEVICE	OS	PROCESS	CLASSIFICATION	DESTINATION	RECEIVED	LAST SEEN	
WIN-MQH0CMRUD2J	Windows Server 2012 ...	TeamViewer.exe	PUP	52.143.143.83	10-Feb-2020, 09:48:02	11-Feb-2020, 16:49:06	⊘

RAW ID: 147071627 Process Type: 32 bit Certificate: Signed Process Path: C:\Program Files (x86)\TeamViewer\TeamViewer.exe User: WIN-MQH0CMRUD2J\root Count: 32

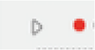
○ PARENT PROCESS CREATION ○ PARENT PROCESS CREATION ○ PARENT PROCESS CREATION ● CONNECTION

CONNECTION
Process ID: 2592
Source Process: ...e1\Program Files (x86)\TeamViewer\TeamViewer.exe
Target:
Company: TeamViewer GmbH
Description: TeamViewer 10
Version: 10.0.38475.0
Product: TeamViewer
Comments:
Command Line:
Process Hash (SHA-1): 16135B96D41C108FDE902889845B129530A90F25
Process Owner: WIN-MQH0CMRUD2J\root

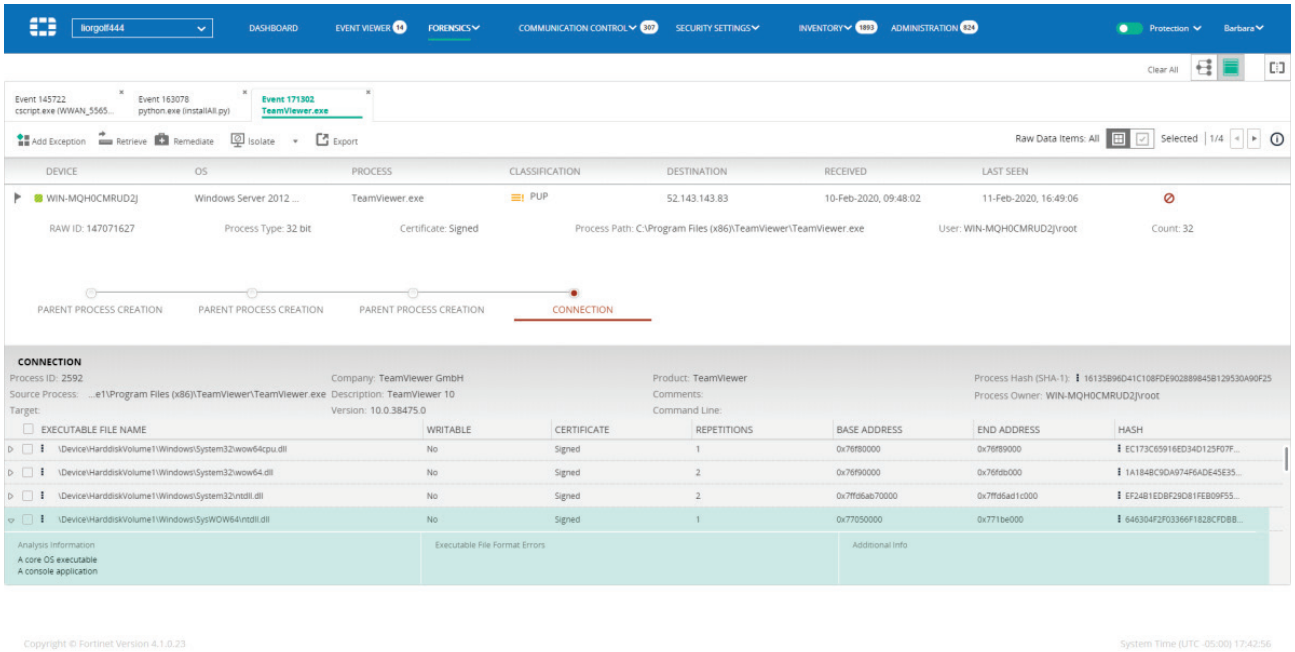
EXECUTABLE FILE NAME	WRITABLE	CERTIFICATE	REPETITIONS	BASE ADDRESS	END ADDRESS	HASH
● Main -\Device\HarddiskVolume1\Program Files (x86)\TeamViewer\TeamViewer.exe	No	Signed				16135B96D41C108FDE90288...
\Device\HarddiskVolume1\Windows\System32\wow64cpu.dll	No	Signed	1	0x76f80000	0x76f89000	EC173C65916ED34D125F07F...
\Device\HarddiskVolume1\Windows\System32\wow64.dll	No	Signed	2	0x76f90000	0x76fdb000	1A184BC9DA974F6ADE45E35...
\Device\HarddiskVolume1\Windows\System32\ntdll.dll	No	Signed	2	0x7ffd6ab70000	0x7ffd6ad1c000	EF24B1EDBF29D81FEB09F55...
\Device\HarddiskVolume1\Windows\SysWOW64\ntdll.dll	No	Signed	1	0x77050000	0x771be000	646304F2F03366F1828CFDBB...
\Device\HarddiskVolume1\Windows\System32\ntdll.dll	No	Signed	1	0x7ffd6ab70000	0x7ffd6ad1c000	EF24B1EDBF29D81FEB09F55...

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

- **Events:** Shows the same information as in the Event Viewer (page 97).
- **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 security 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:



DEVICE	OS	PROCESS	CLASSIFICATION	DESTINATION	RECEIVED	LAST SEEN
WIN-MQH0CMRUD2J	Windows Server 2012 ...	TeamViewer.exe	PUP	52.143.143.83	10-Feb-2020, 09:48:02	11-Feb-2020, 16:49:06

RAW ID: 147071627 Process Type: 32 bit Certificate: Signed Process Path: C:\Program Files (x86)\TeamViewer\TeamViewer.exe User: WIN-MQH0CMRUD2J\root Count: 32

CONNECTION

Process ID: 2592
Source Process: ...e1\Program Files (x86)\TeamViewer\TeamViewer.exe
Target:
Company: TeamViewer GmbH
Description: TeamViewer 10
Version: 10.0.38475.0
Product: TeamViewer
Comments:
Command Line:
Process Hash (SHA-1): 16135B96D41C108FDE902889845B129530A90F25
Process Owner: WIN-MQH0CMRUD2J\root

EXECUTABLE FILE NAME	WRITABLE	CERTIFICATE	REPETITIONS	BASE ADDRESS	END ADDRESS	HASH
\Device\HarddiskVolume1\Windows\System32\wow64cpu.dll	No	Signed	1	0x76f80000	0x76f89000	EC173C65916ED34D125F07F...
\Device\HarddiskVolume1\Windows\System32\wow64.dll	No	Signed	2	0x76f90000	0x76fdb000	1A184BC9DA974F6ADE45E35...
\Device\HarddiskVolume1\Windows\System32\ntdll.dll	No	Signed	2	0x7ffd6ab70000	0x7ffd6ad1c000	EF24B1EDBF29D81FEB09F55...
\Device\HarddiskVolume1\Windows\SysWOW64\ntdll.dll	No	Signed	1	0x77050000	0x771be000	646304F2F03366F1828CFDBB...

Analysis Information
A core OS executable
A console application

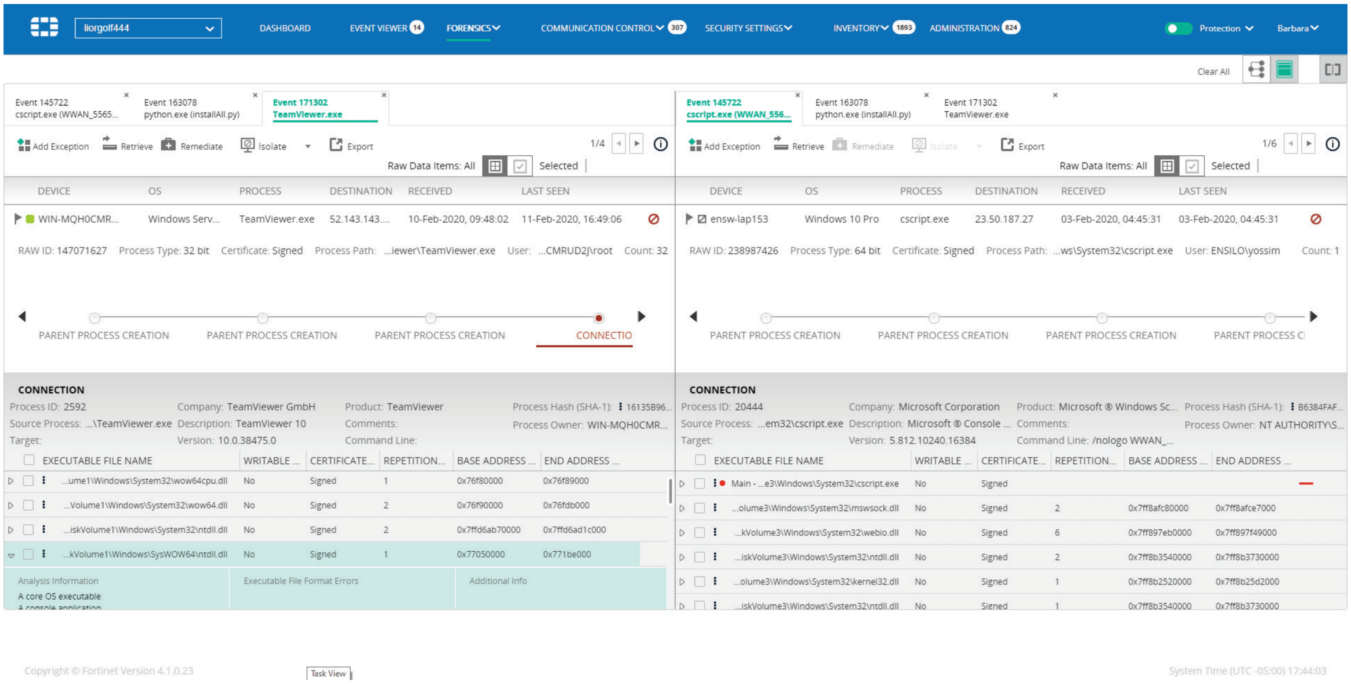
Executable File Format Errors

Additional Info

Copyright © Fortinet Version 4.1.0.23

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

Compare View



DEVICE	OS	PROCESS	DESTINATION	RECEIVED	LAST SEEN
WIN-MQH0CMR...	Windows Serv...	TeamViewer.exe	52.143.143....	10-Feb-2020, 09:48:02	11-Feb-2020, 16:49:06

RAW ID: 147071627 Process Type: 32 bit Certificate: Signed Process Path: ...iewer\TeamViewer.exe User: ...CMRUD2J\root Count: 32

CONNECTION

Process ID: 2592
Source Process: ...\TeamViewer.exe
Target:
Company: TeamViewer GmbH
Description: TeamViewer 10
Version: 10.0.38475.0
Product: TeamViewer
Comments:
Command Line:
Process Hash (SHA-1): 16135B96...
Process Owner: WIN-MQH0CMR...

EXECUTABLE FILE NAME	WRITABLE ...	CERTIFICATE...	REPETITION...	BASE ADDRESS ...	END ADDRESS ...
...ume1\Windows\System32\wow64cpu.dll	No	Signed	1	0x76f80000	0x76f89000
...Volume1\Windows\System32\wow64.dll	No	Signed	2	0x76f90000	0x76fdb000
...iskVolume1\Windows\System32\ntdll.dll	No	Signed	2	0x7ffd6ab70000	0x7ffd6ad1c000
...kVolume1\Windows\SysWOW64\ntdll.dll	No	Signed	1	0x77050000	0x771be000

Analysis Information
A core OS executable
A console application

Executable File Format Errors

Additional Info

DEVICE	OS	PROCESS	DESTINATION	RECEIVED	LAST SEEN
ensw-lap153	Windows 10 Pro	cscript.exe	23.50.187.27	03-Feb-2020, 04:45:31	03-Feb-2020, 04:45:31

RAW ID: 238987426 Process Type: 64 bit Certificate: Signed Process Path: ...ws\System32\cscript.exe User: ENSILO\yossim Count: 1

CONNECTION

Process ID: 20444
Source Process: ...em32\cscript.exe
Target:
Company: Microsoft Corporation
Description: Microsoft ® Console ...
Version: 5.812.10240.16384
Product: Microsoft ® Windows Sc...
Comments:
Command Line: /nologo WWAN_...
Process Hash (SHA-1): B6384FAF...
Process Owner: NT AUTHORITY\S...

EXECUTABLE FILE NAME	WRITABLE ...	CERTIFICATE...	REPETITION...	BASE ADDRESS ...	END ADDRESS ...
Main - ...e3\Windows\System32\cscript.exe	No	Signed			
...olume3\Windows\System32\mswsock.dll	No	Signed	2	0x7ff8afc80000	0x7ff8afce7000
...kVolume3\Windows\System32\webio.dll	No	Signed	6	0x7ff897eb0000	0x7ff897f49000
...iskVolume3\Windows\System32\ntdll.dll	No	Signed	2	0x7ff8b3540000	0x7ff8b3730000
...olume3\Windows\System32\kernel32.dll	No	Signed	1	0x7ff8b2520000	0x7ff8b25d2000
...iskVolume3\Windows\System32\ntdll.dll	No	Signed	1	0x7ff8b3540000	0x7ff8b3730000

Copyright © Fortinet Version 4.1.0.23

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

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

Defining an Exception

After Forensic analysis, you may decide to create an exception for a specific security event. To do so, you may refer to the *Defining Event Exceptions* section on page 107. You may refer to page 58 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.

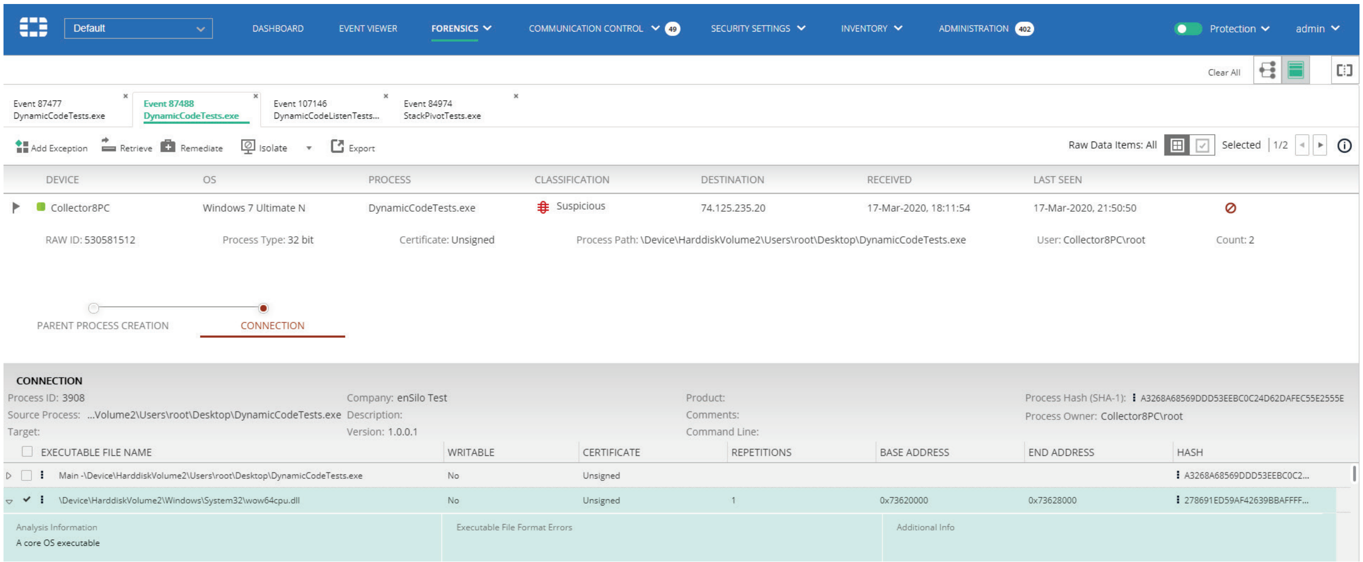
Note – Some malware have persistency capabilities, which makes the infection appear again. In addition, in some rare cases, malware can cause the system to crash if you try to remove them.

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

To remediate a device on which malware was detected:

1 Select the security event(s) to analyze using one of the following methods described on page 97.

2 In the Raw Events area, select the relevant process. Use the various forensic tools provided by FortiEDR to determine the process of interest.



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

RAW ID: 530581512 Process Type: 32 bit Certificate: Unsigned Process Path: \Device\HarddiskVolume2\Users\root\Desktop\DynamicCodeTests.exe User: Collector8PC\root Count: 2

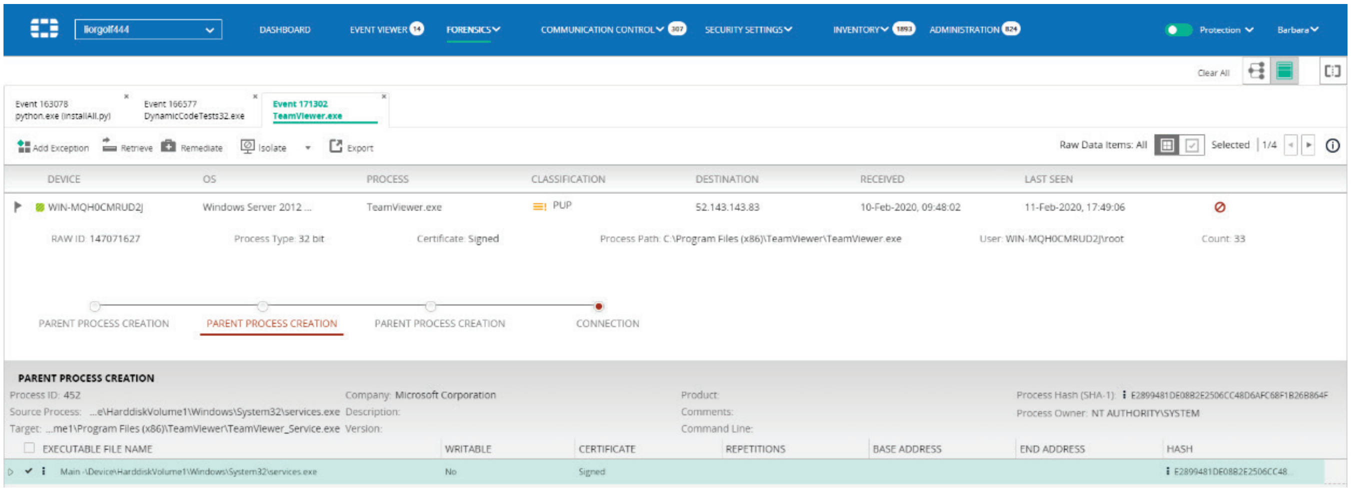
CONNECTION

Process ID: 3908
Source Process: ...Volume2\Users\root\Desktop\DynamicCodeTests.exe
Target:
Company: enSilo Test
Description:
Version: 1.0.0.1
Product:
Comments:
Command Line:
Process Hash (SHA-1): A3268A68569DDD53EEBC0C24D62DAFEC55E2555E
Process Owner: Collector8PC\root

EXECUTABLE FILE NAME	WRITABLE	CERTIFICATE	REPETITIONS	BASE ADDRESS	END ADDRESS	HASH
Main -\Device\HarddiskVolume2\Users\root\Desktop\DynamicCodeTests.exe	No	Unsigned				A3268A68569DDD53EEBC0C2...
\Device\HarddiskVolume2\Windows\System32\wow64cpu.dll	No	Unsigned	1	0x73620000	0x73628000	278691ED59AF42639BBAFFFF...

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

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



Event 163078 python.exe (installAll.py)

Event 166577 DynamicCodeTests32.exe

Event 171302 TeamViewer.exe

DEVICE	OS	PROCESS	CLASSIFICATION	DESTINATION	RECEIVED	LAST SEEN
WIN-MQH0CMRUD2J	Windows Server 2012 ...	TeamViewer.exe	PUP	52.143.143.83	10-Feb-2020, 09:48:02	11-Feb-2020, 17:49:06

RAW ID: 147071627 Process Type: 32 bit Certificate: Signed Process Path: C:\Program Files (x86)\TeamViewer\TeamViewer.exe User: WIN-MQH0CMRUD2J\root Count: 33

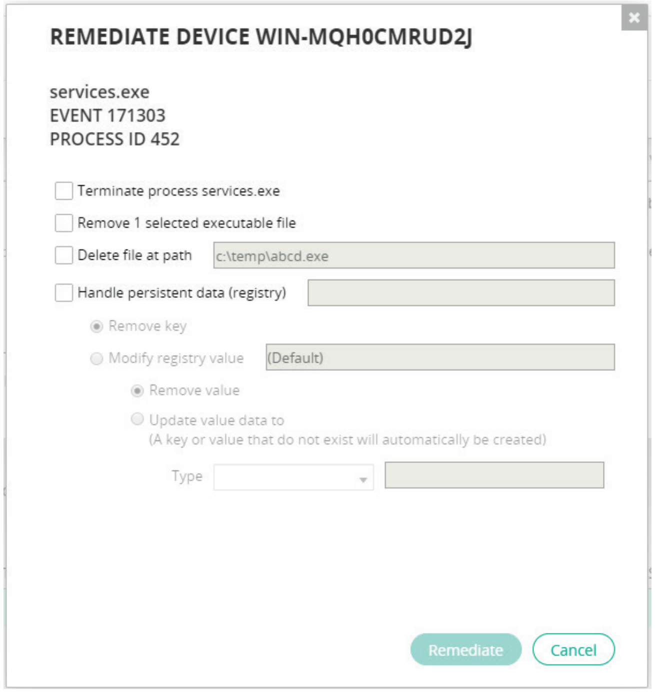
PARENT PROCESS CREATION — PARENT PROCESS CREATION — PARENT PROCESS CREATION — CONNECTION

PARENT PROCESS CREATION

Process ID: 452
Source Process: ...e\HarddiskVolume1\Windows\System32\services.exe
Target: ...me1\Program Files (x86)\TeamViewer\TeamViewer_Service.exe
Company: Microsoft Corporation
Description:
Version:
Product:
Comments:
Command Line:
Process Hash (SHA-1): E2899481DE0882E2506CC48D6AFC68F1B26B864F
Process Owner: NT AUTHORITY\SYSTEM

EXECUTABLE FILE NAME	WRITABLE	CERTIFICATE	REPETITIONS	BASE ADDRESS	END ADDRESS	HASH
✓ Main -\Device\HarddiskVolume1\Windows\System32\services.exe	No	Signed				E2899481DE0882E2506CC48...

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



REMEDIATE DEVICE WIN-MQH0CMRUD2J

services.exe
EVENT 171303
PROCESS ID 452

□ Terminate process services.exe

□ Remove 1 selected executable file

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

□ Handle persistent data (registry)

● Remove key

○ Modify registry value (Default)

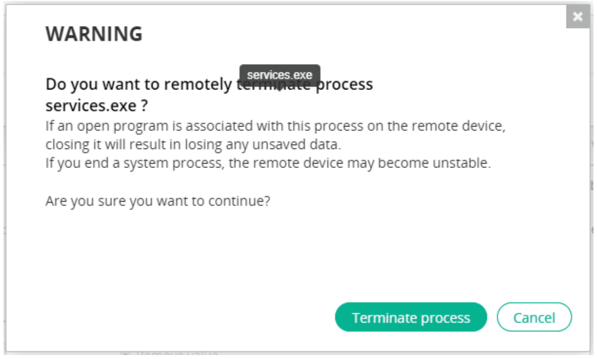
● Remove value

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

Type

4 Do one of the following:

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



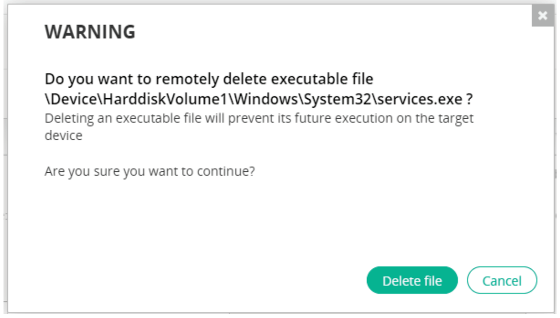
WARNING

Do you want to remotely terminate process services.exe ?
If an open program is associated with this process on the remote device, closing it will result in losing any unsaved data.
If you end a system process, the remote device may become unstable.

Are you sure you want to continue?

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

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

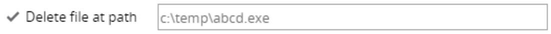
  WARNING

  Do you want to remotely delete executable file \Device\HarddiskVolume1\Windows\System32\services.exe ?
  Deleting an executable file will prevent its future execution on the target device

  Are you sure you want to continue?

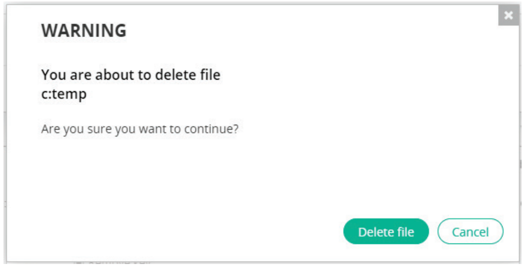
  Click **Delete file** to remove the selected file.

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

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

  A warning message displays.

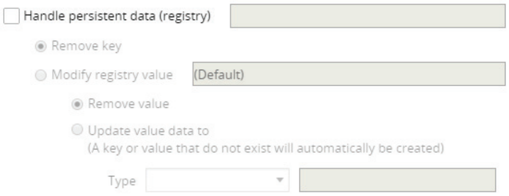
  WARNING

  You are about to delete file
  c:temp

  Are you sure you want to continue?

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

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

  □ Handle persistent data (registry)
  ● Remove key
  ○ Modify registry value (Default)
  ● Remove value
  ○ Update value data to
  (A key or value that do not exist will automatically be created)
  Type

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

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

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

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

5 Click the **Remediate** button.

Retrieving Memory

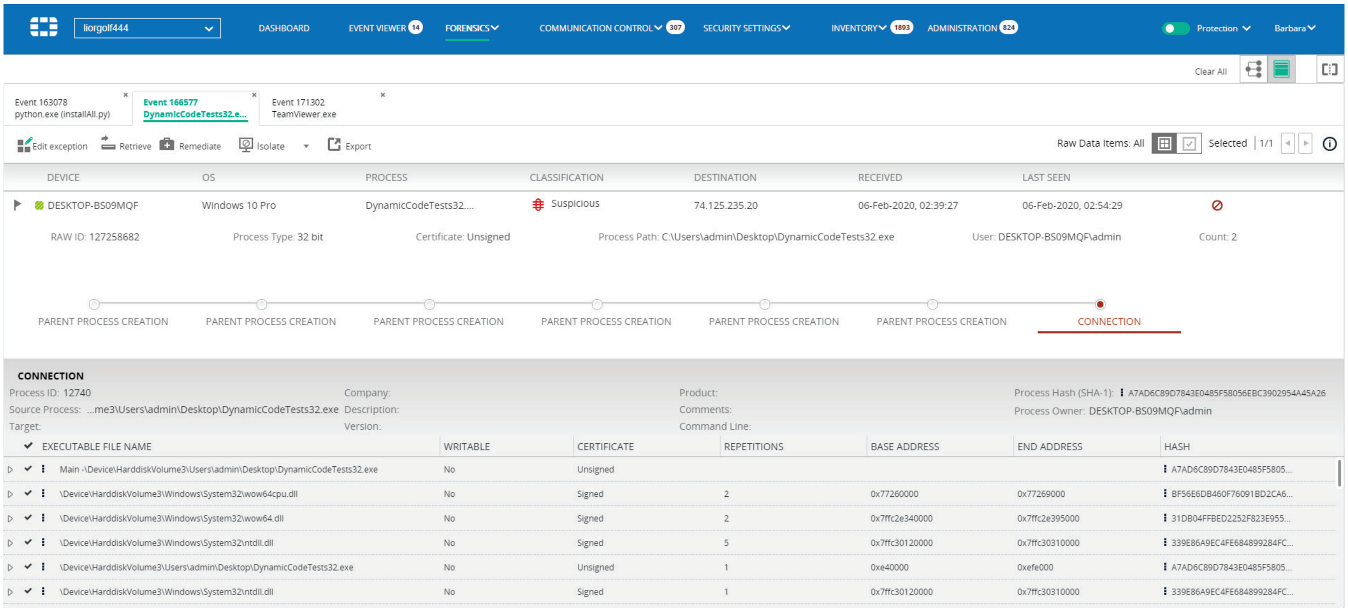
The **Retrieve Memory** function enables you to retrieve the stack-memory of a specific Collector. This option enables you to retrieve memory from a specific communicating device in order to perform deeper analysis by analyzing the actual memory from the device. This function is only accessible from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



DEVICE	OS	PROCESS	CLASSIFICATION	DESTINATION	RECEIVED	LAST SEEN
DESKTOP-BS09MQF	Windows 10 Pro	DynamicCodeTests32....	Suspicious	74.125.235.20	06-Feb-2020, 02:39:27	06-Feb-2020, 02:54:29

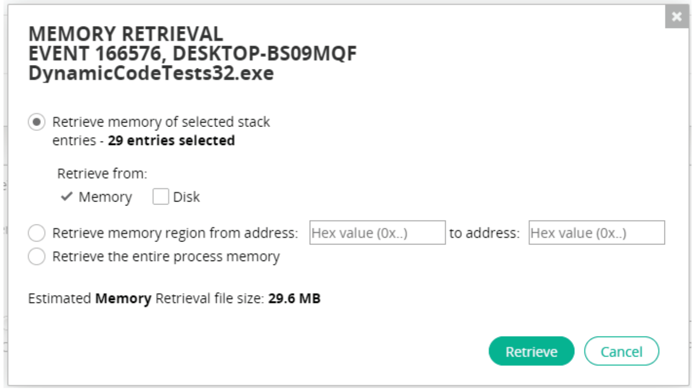
RAW ID: 127258682 Process Type: 32 bit Certificate: Unsigned Process Path: C:\Users\admin\Desktop\DynamicCodeTests32.exe User: DESKTOP-BS09MQF\admin Count: 2

CONNECTION

Process ID: 12740
Source Process: ...me3\Users\admin\Desktop\DynamicCodeTests32.exe
Target:
Company:
Description:
Version:
Product:
Comments:
Command Line:
Process Hash (SHA-1): A7AD6C89D7843E0485F58056EBC3902954A45A26
Process Owner: DESKTOP-BS09MQF\admin

✓	EXECUTABLE FILE NAME	WRITABLE	CERTIFICATE	REPETITIONS	BASE ADDRESS	END ADDRESS	HASH
✓	Main -\Device\HarddiskVolume3\Users\admin\Desktop\DynamicCodeTests32.exe	No	Unsigned				A7AD6C89D7843E0485F5805...
✓	\Device\HarddiskVolume3\Windows\System32\wow64cpu.dll	No	Signed	2	0x77260000	0x77269000	BF56E6DB460F76091BD2CA6...
✓	\Device\HarddiskVolume3\Windows\System32\wow64.dll	No	Signed	2	0x7ffc2e340000	0x7ffc2e395000	31DB04FFBED2252F823E955...
✓	\Device\HarddiskVolume3\Windows\System32\ntdll.dll	No	Signed	5	0x7ffc30120000	0x7ffc30310000	339E86A9EC4FE684899284FC...
✓	\Device\HarddiskVolume3\Users\admin\Desktop\DynamicCodeTests32.exe	No	Unsigned	1	0xe40000	0xefe000	A7AD6C89D7843E0485F5805...
✓	\Device\HarddiskVolume3\Windows\System32\ntdll.dll	No	Signed	1	0x7ffc30120000	0x7ffc30310000	339E86A9EC4FE684899284FC...

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



MEMORY RETRIEVAL
EVENT 166576, DESKTOP-BS09MQF
DynamicCodeTests32.exe

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

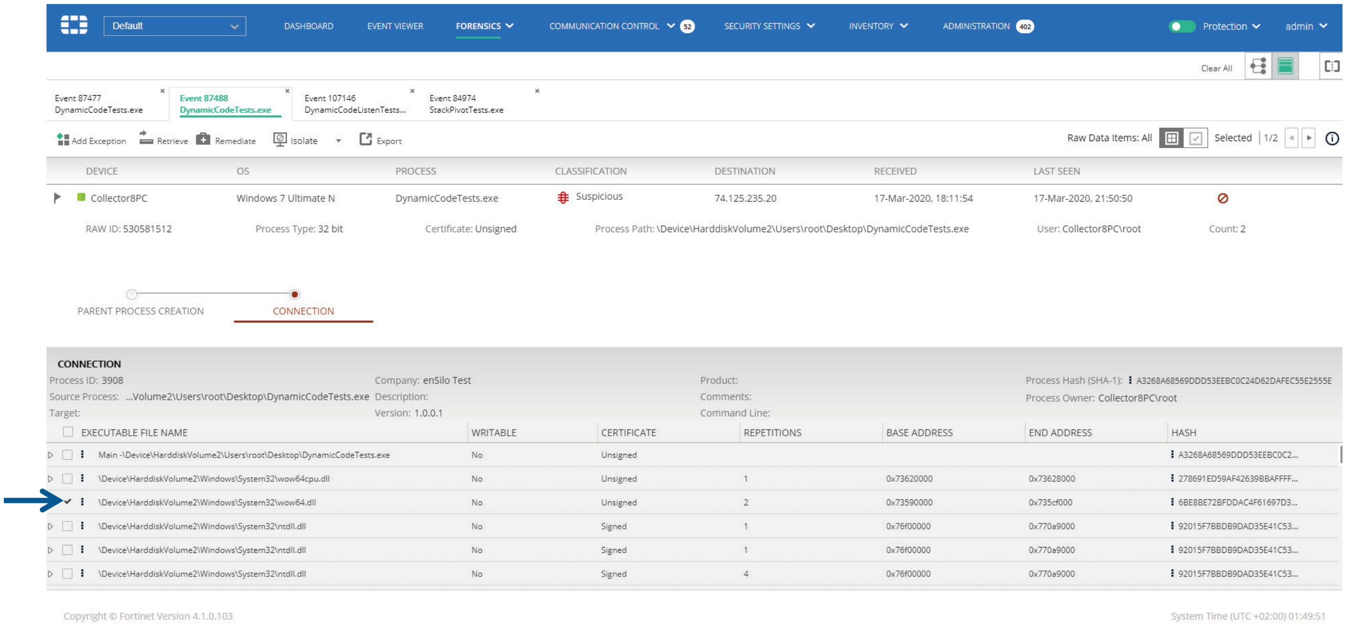
Retrieve from:
✓ Memory □ Disk

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

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

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:



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

RAW ID: 530581512 Process Type: 32 bit Certificate: Unsigned Process Path: \Device\HarddiskVolume2\Users\root\Desktop\DynamicCodeTests.exe User: Collector8PC\root Count: 2

CONNECTION

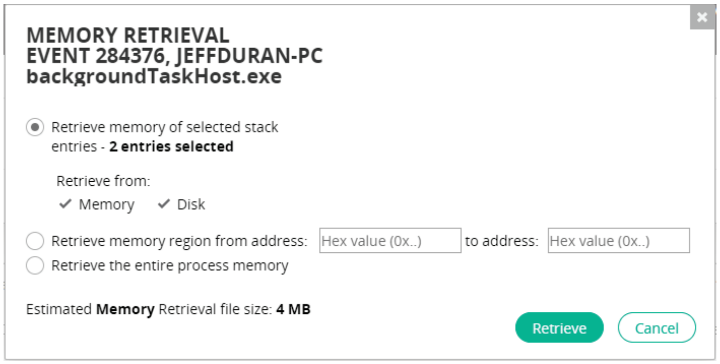
Process ID: 3908
Source Process: ...Volume2\Users\root\Desktop\DynamicCodeTests.exe
Target:
Company: enSilo Test
Description:
Version: 1.0.0.1
Product:
Comments:
Command Line:
Process Hash (SHA-1): A3268A68569DDD53EEBC0C24D62DAFEC55E2555E
Process Owner: Collector8PC\root

□	EXECUTABLE FILE NAME	WRITABLE	CERTIFICATE	REPETITIONS	BASE ADDRESS	END ADDRESS	HASH
□	Main -\Device\HarddiskVolume2\Users\root\Desktop\DynamicCodeTests.exe	No	Unsigned				A3268A68569DDD53EEBC0C2...
□	\Device\HarddiskVolume2\Windows\System32\wow64cpu.dll	No	Unsigned	1	0x73620000	0x73628000	278691ED59AF42639BBAFFFF...
✓	\Device\HarddiskVolume2\Windows\System32\wow64.dll	No	Unsigned	2	0x73590000	0x735cf000	6BE8BE72BFDDAC4F61697D3...
□	\Device\HarddiskVolume2\Windows\System32\ntdll.dll	No	Signed	1	0x76f00000	0x770a9000	92015F7BBDB9DAD35E41C53...
□	\Device\HarddiskVolume2\Windows\System32\ntdll.dll	No	Signed	1	0x76f00000	0x770a9000	92015F7BBDB9DAD35E41C53...
□	\Device\HarddiskVolume2\Windows\System32\ntdll.dll	No	Signed	4	0x76f00000	0x770a9000	92015F7BBDB9DAD35E41C53...

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

You must also specify whether to retrieve the memory from **Memory, Disk** or both by selecting the respective checkbox. The **Memory** option is the default. You can select either option or both options. It is important to remember that the retrievable data may be different in the memory and on disk. In addition, the stack entry may no longer reside in memory, for example, if the system was rebooted.

After you make your selection, the window indicates how many stack entries were selected, as shown below. For example, the figure below shows that three stack entries were selected for analysis.



MEMORY RETRIEVAL
EVENT 284376, JEFFDURAN-PC
backgroundTaskHost.exe

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

Retrieve from:
✓ Memory ✓ Disk

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

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

- **Retrieve memory region from address:** Select this option to retrieve memory from a specific memory region. Specify the **To** and **From** addresses for the region in the adjacent fields.

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

- **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.

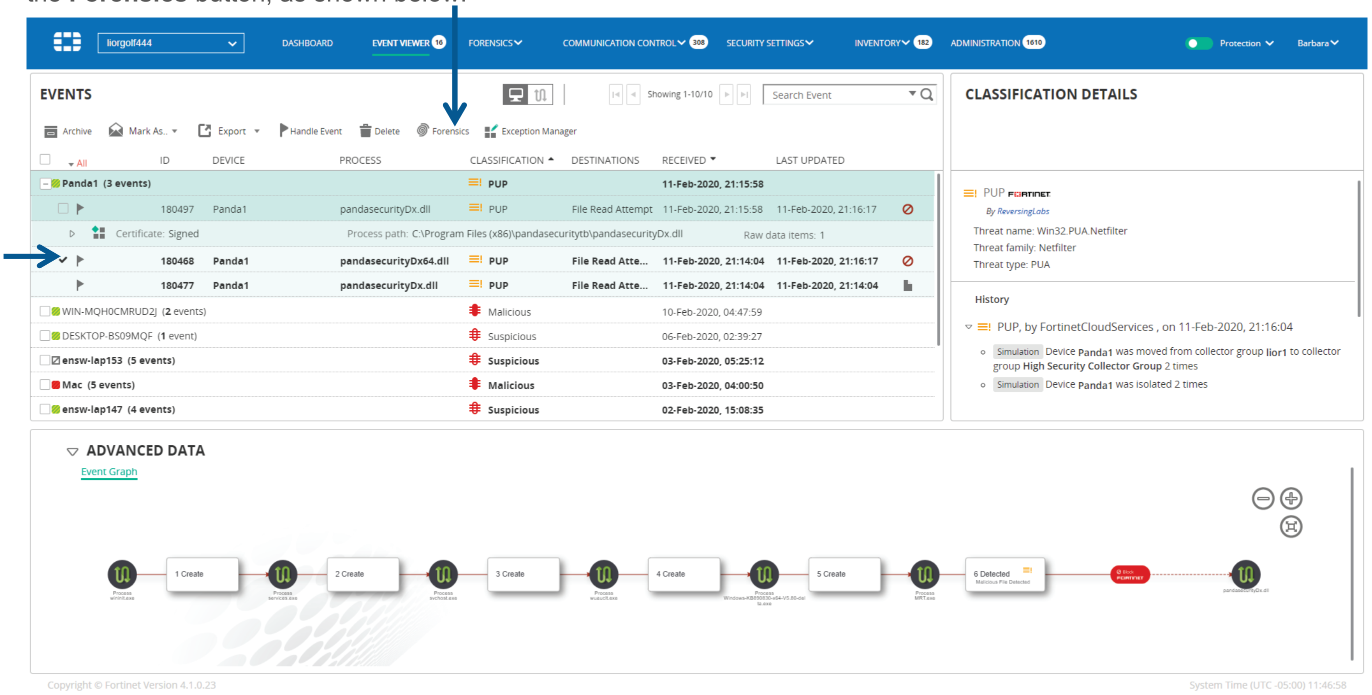
Isolating a Device

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 62.

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

To isolate a device using the FortiEDR Collector:

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



All	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
☐ Panda1 (3 events)				PUP		11-Feb-2020, 21:15:58	
☐	180497	Panda1	pandasecurityDx.dll	PUP	File Read Attempt	11-Feb-2020, 21:15:58	11-Feb-2020, 21:16:17
Certificate: Signed			Process path: C:\Program Files (x86)\pandasecuritytb\pandasecurityDx.dll			Raw data items: 1	
✓	180468	Panda1	pandasecurityDx64.dll	PUP	File Read Atte...	11-Feb-2020, 21:14:04	11-Feb-2020, 21:16:17
	180477	Panda1	pandasecurityDx.dll	PUP	File Read Atte...	11-Feb-2020, 21:14:04	11-Feb-2020, 21:14:04
☐ WIN-MQHOCMRUD2J (2 events)				Malicious		10-Feb-2020, 04:47:59	
☐ DESKTOP-BS09MQF (1 event)				Suspicious		06-Feb-2020, 02:39:27	
☐ ensw-lap153 (5 events)				Suspicious		03-Feb-2020, 05:25:12	
☐ Mac (5 events)				Malicious		03-Feb-2020, 04:00:50	
☐ ensw-lap147 (4 events)				Suspicious		02-Feb-2020, 15:08:35	

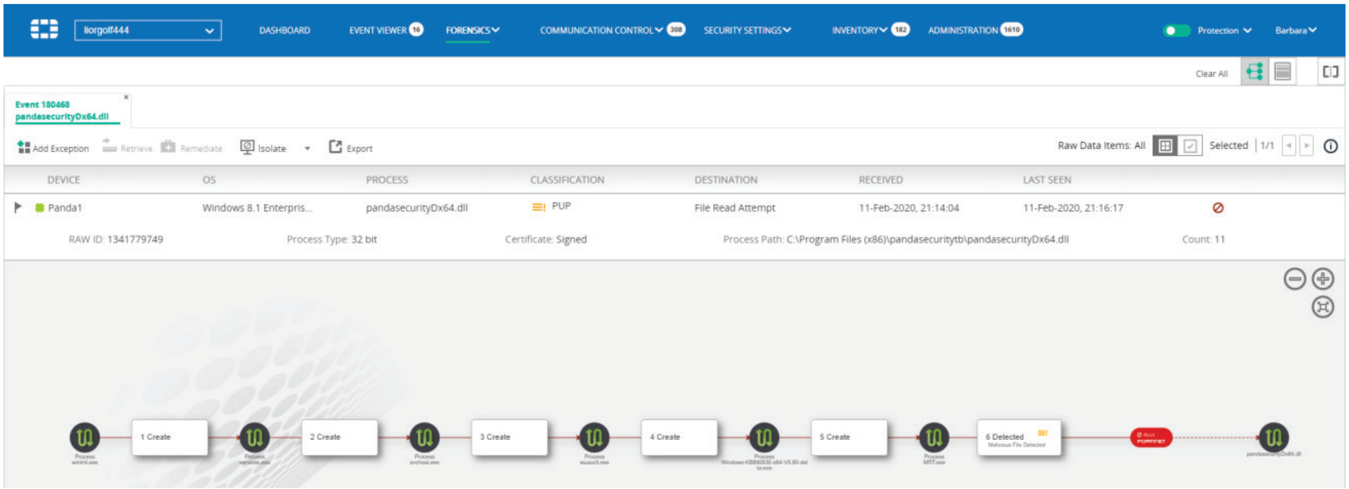
PUP
By ReversingLabs
Threat name: Win32.PUA.Netfilter
Threat family: Netfilter
Threat type: PUA

History

PUP, by FortinetCloudServices , on 11-Feb-2020, 21:16:04

- Simulation Device **Panda1** was moved from collector group **lior1** to collector group **High Security Collector Group** 2 times
- Simulation Device **Panda1** was isolated 2 times

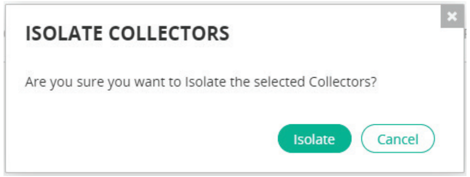
The following window displays:



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

RAW ID: 1341779749 Process Type: 32 bit Certificate: Signed Process Path: C:\Program Files (x86)\pandasecuritytb\pandasecurityDx64.dll Count: 11

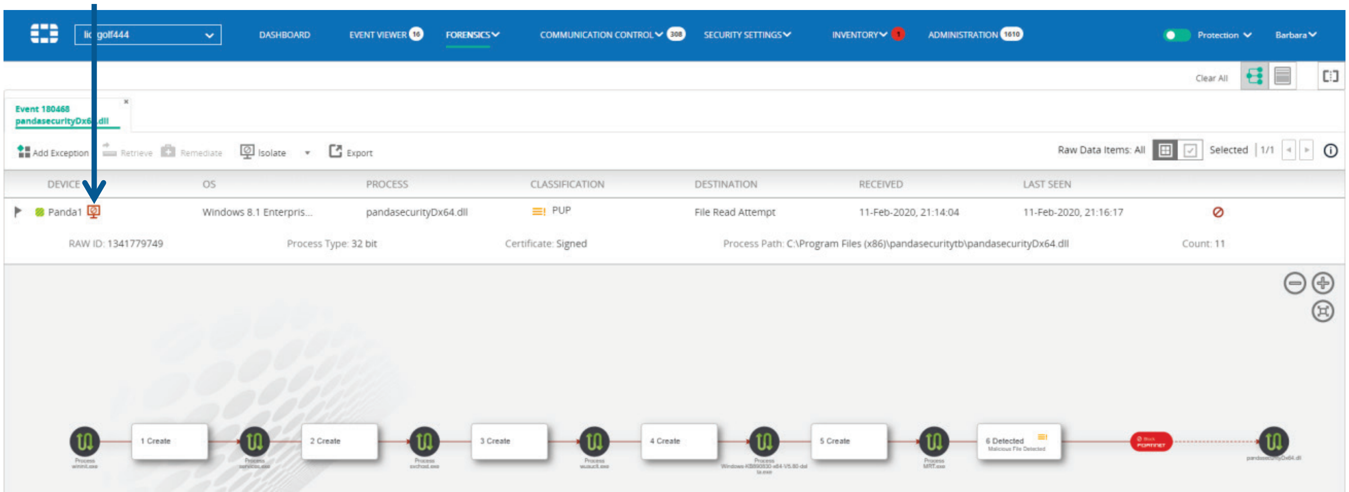
2 In the **Events** tab, click the security event that you want to isolate, click the Isolate ▾ button dropdown arrow and then select **Isolate**. The following window displays:



ISOLATE COLLECTORS

Are you sure you want to Isolate the selected Collectors?

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



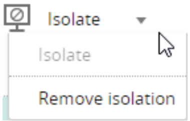
DEVICE	OS	PROCESS	CLASSIFICATION	DESTINATION	RECEIVED	LAST SEEN
Panda1	Windows 8.1 Enterpris...	pandasecurityDx64.dll	PUP	File Read Attempt	11-Feb-2020, 21:14:04	11-Feb-2020, 21:16:17

RAW ID: 1341779749 Process Type: 32 bit Certificate: Signed Process Path: C:\Program Files (x86)\pandasecuritytb\pandasecurityDx64.dll Count: 11

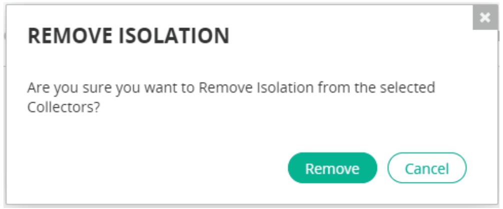
To remove isolation from a device:

1 In the **FORENSICS** tab, select the checkbox of the security 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:



REMOVE ISOLATION

Are you sure you want to Remove Isolation from the selected Collectors?

3 Click the **Remove** button.

Threat Hunting

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

Two versions of FortiEDR’s Threat Hunting feature are supported:

- **Threat Hunting,** page 158
- **Legacy Threat Hunting,** page 175

Note – Threat Hunting is a license-dependent add-on. You may contact Fortinet support for more information.

Threat Hunting

Threat Hunting significantly expands and enhances the capabilities of the Legacy Threat Hunting feature, which is described in the *Legacy Threat Hunting* section on page 175. In addition to searching for activities based on a security event’s process or HASH, you can also search for these activities based on a variety of activity types (such as Process Creation, File Deletion, Registry Value change, Socket Connect and so on), as well as by Process/File/Registry/Network or Event Log criteria.

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

Note – This **Threat Hunting** page automatically becomes the only option available after all Collectors are V5.0 or above.

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

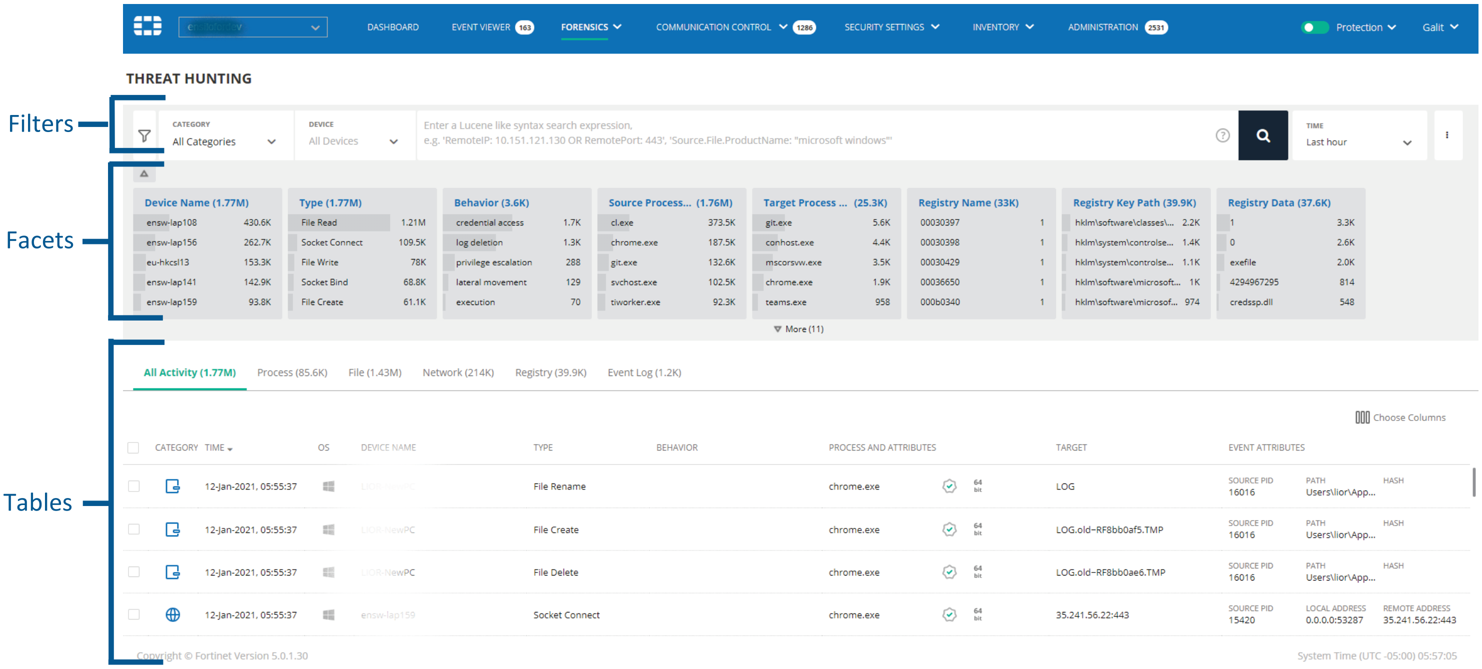
For example, when a process runs, it can perform various actions on files, such as File Open, File Read, File Delete and so on. In this case, the process is the source, and it performs an action such as File Open on a target File.

Note – Activity events are not the same as the security events identified in the Event Viewer. Unlike Event Viewer security events, which are only reported in the Event Viewer as they occur and are detected, activity events are continuously collected based on a wealth of data, activity and actions occurring in your system and the chosen Threat Hunting Profile. You may refer to the *Threat Hunting Settings* section on page 67 for more information.

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

- **Registry Key Actions:** All targets are either registry keys or registry values and all actions are registry-related, such as Key Created, Key Deleted, Value Set and so on.
- **File Actions:** All targets identify the target file on which the action was performed and all actions are file-related, such as File Create, File Delete, File Rename and so on.
- **Process Actions:** The target is another process and all actions are process related, such as Process Termination, Process Creation, Executable Loaded and so on.
- **Network Actions:** The target is a network item (such as connection or URL) and all actions are Network related, such as Socket Connect, Socket Close and Socket Bind.
- **Event Log Action:** Currently, only Windows logs are supported. The only action is Log Entry Created and relates to the logs of the operating system.

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



THREAT HUNTING

CATEGORY: All Categories

DEVICE: All Devices

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

TIME: Last hour

Device Name (1.77M)		Type (1.77M)		Behavior (3.6K)		Source Process... (1.76M)		Target Process ... (25.3K)		Registry Name (33K)		Registry Key Path (39.9K)		Registry Data (37.6K)	
ensw-lap108	430.6K	File Read	1.21M	credential access	1.7K	cl.exe	373.5K	git.exe	5.6K	00030397	1	hklm\software\classes\...	2.2K	1	3.3K
ensw-lap156	262.7K	Socket Connect	109.5K	log deletion	1.3K	chrome.exe	187.5K	conhost.exe	4.4K	00030398	1	hklm\system\controlse...	1.4K	0	2.6K
eu-hkcsl13	153.3K	File Write	78K	privilege escalation	288	git.exe	132.6K	mscorsvw.exe	3.5K	00030429	1	hklm\system\controlse...	1.1K	exefile	2.0K
ensw-lap141	142.9K	Socket Bind	68.8K	lateral movement	129	svchost.exe	102.5K	chrome.exe	1.9K	00036650	1	hklm\software\microsoft...	1K	4294967295	814
ensw-lap159	93.8K	File Create	61.1K	execution	70	tiworker.exe	92.3K	teams.exe	958	000b0340	1	hklm\software\microsof...	974	credssp.dll	548

All Activity (1.77M) | Process (85.6K) | File (1.43M) | Network (214K) | Registry (39.9K) | Event Log (1.2K)

CATEGORY	TIME	OS	DEVICE NAME	TYPE	BEHAVIOR	PROCESS AND ATTRIBUTES	TARGET	EVENT ATTRIBUTES		
	12-Jan-2021, 05:55:37		LIOR-NewPC	File Rename		chrome.exe 64 bit	LOG	SOURCE PID 16016	PATH Users\lior\App...	HASH
	12-Jan-2021, 05:55:37		LIOR-NewPC	File Create		chrome.exe 64 bit	LOG.old~RF8bb0af5.TMP	SOURCE PID 16016	PATH Users\lior\App...	HASH
	12-Jan-2021, 05:55:37		LIOR-NewPC	File Delete		chrome.exe 64 bit	LOG.old~RF8bb0ae6.TMP	SOURCE PID 16016	PATH Users\lior\App...	HASH
	12-Jan-2021, 05:55:37		ensw-lap159	Socket Connect		chrome.exe 64 bit	35.241.56.22:443	SOURCE PID 15420	LOCAL ADDRESS 0.0.0.0:53287	REMOTE ADDRESS 35.241.56.22:443

Copyright © Fortinet Version 5.0.1.30

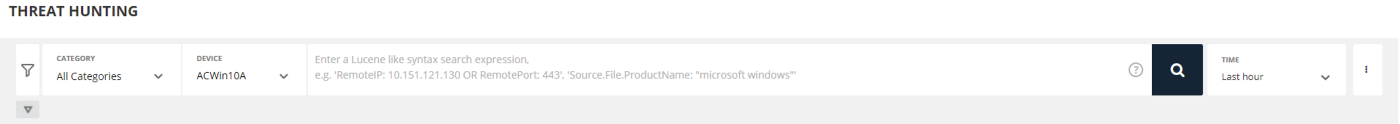
System Time (UTC -05:00) 05:57:05

The **Threat Hunting** page contains the following areas:

- **Filters,** page 159
- **Facets,** page 166
- **Activity Events Tables,** page 169
- **Details Pane,** page 172

Filters

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



THREAT HUNTING

CATEGORY: All Categories

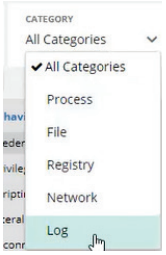
DEVICE: ACWin10A

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

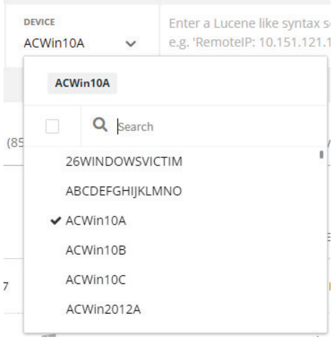
TIME: Last hour

Note – This area also enables you to save queries and to redisplay saved queries, as described on page 161.

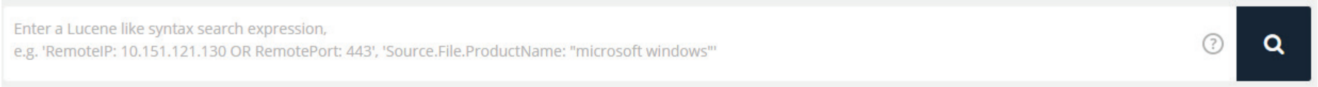
- **Category Filter:** The **Category** filter enables you to filter the activity events by their Category.



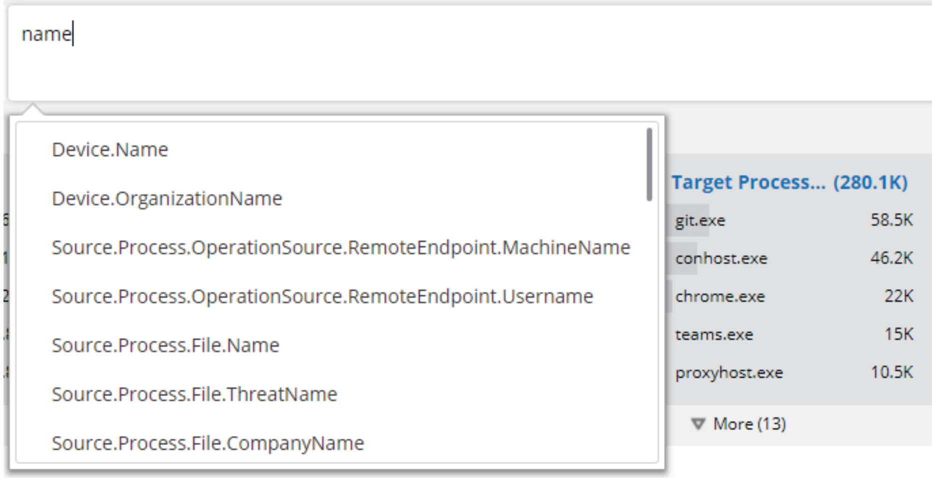
- **Device Filter:** The **Device** filter enables you to filter by a specific device\s.



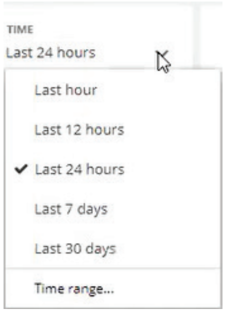
- **Free-text Query Filter:** This filter enables you to specify a free-text query to filter the results. This filter uses Lucene syntax. For details about the supported Lucene syntax features, see *Appendix B Lucene Syntax* on page 265.


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

To simply query definition, the free-text query filter has an auto-complete helper dropdown list that contains all the available activity event fields, as well as available syntax operators. Simply start typing to see a dropdown menu of options. The automatic-complete helper guides you through the process of creating a query by displaying appropriate options in the dropdown menus, such as fields and operators when appropriate.


name
Device.Name
Device.OrganizationName
Source.Process.OperationSource.RemoteEndpoint.MachineName
Source.Process.OperationSource.RemoteEndpoint.Username
Source.Process.File.Name
Source.Process.File.ThreatName
Source.Process.File.CompanyName
Target Process... (280.1K)
git.exe 58.5K
conhost.exe 46.2K
chrome.exe 22K
teams.exe 15K
proxyhost.exe 10.5K
More (13)

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



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

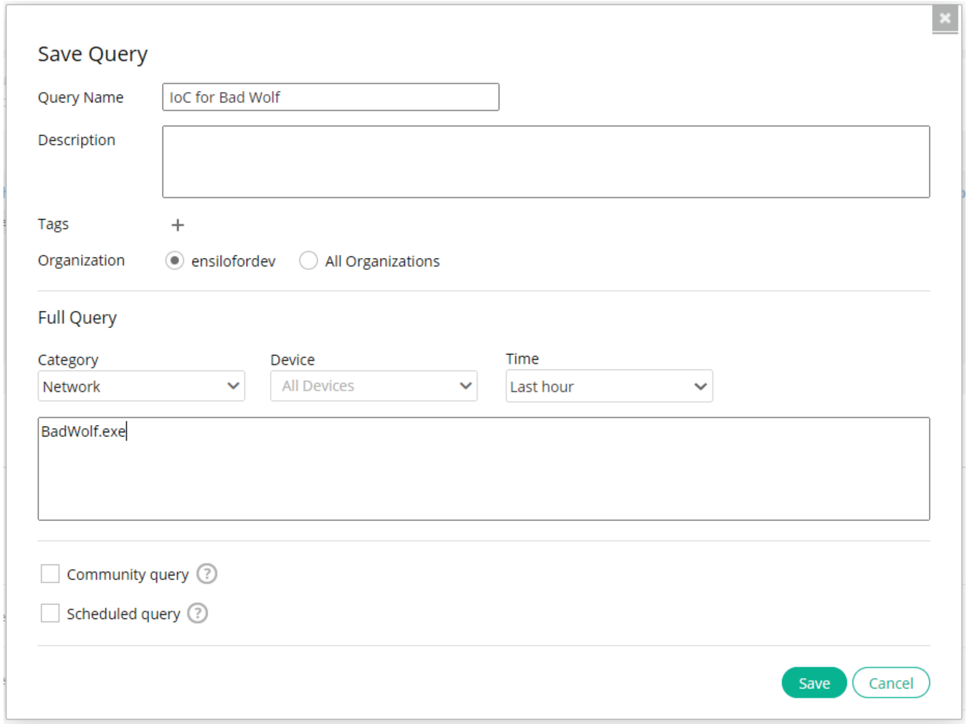
Saving Queries and Saved Queries

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

To save a query:

1 Use the filters (as described above) to display the desired filtered events in the result tables.

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



Save Query

Query Name: IoC for Bad Wolf

Description:

Tags +

Organization: ● ensilofordev ○ All Organizations

Full Query

Category: Network

Device: All Devices

Time: Last hour

BadWolf.exe

□ Community query ⓘ

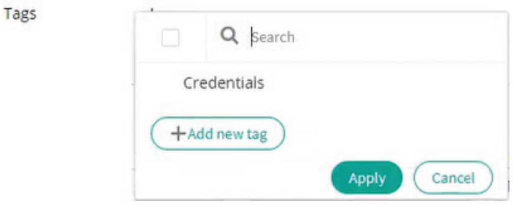
□ Scheduled query ⓘ

3 Fill in or modify the definitions of this saved query, as follows:

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

  Note – These tags only relate to saved queries.

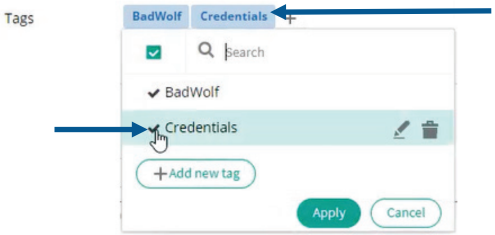
  Click the **+** to assign tag(s) to this query. The following displays:

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

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

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



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

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

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

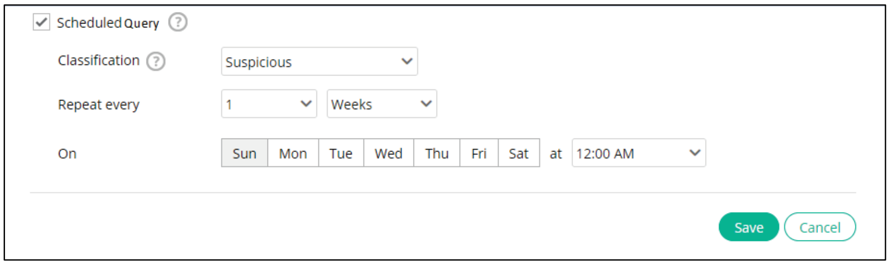
Click the **Apply** button to assign all the selected tags (with checkmarks) to this query.

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

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

- **Scheduled Query:** Mark this option to automate the process of detecting threats so that this query is run automatically according to the schedule that you define. A security event is automatically created in the Event Viewer upon detecting threats (query matches). Notifications are sent according to the security event's definition, such as via email, Syslog and so on.

  Marking this checkbox shows the following options:



☑ Scheduled Query

Classification: Suspicious

Repeat every: 1 Weeks

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

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

Define the scheduled query, as follows:

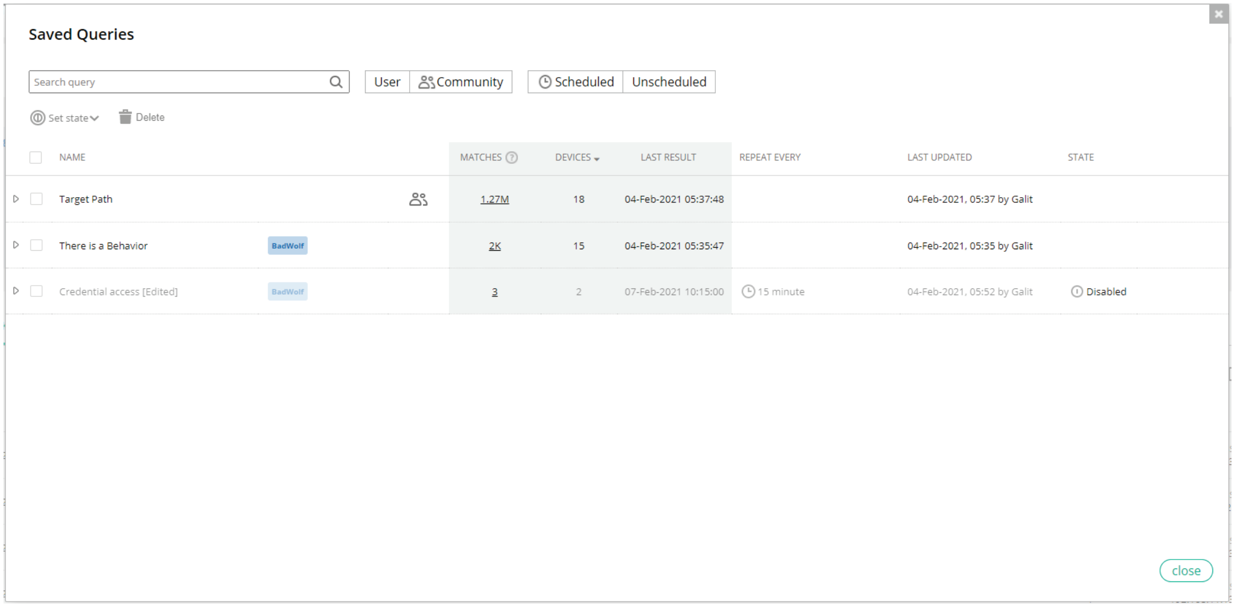
- **Classification:** Select the classification of the Security Event to be issued when the scheduled query has run and found matches. The Classification specifies how malicious the security event is, if at all. Classifications are initially determined by FortiEDR automatically or manually and are shown in the Event Viewer, as described on page 120. They can be:
  - Malicious
  - Suspicious
  - Inconclusive
  - Likely Safe
  - PUP (Potentially Unwanted Program)
  - Safe
- **Repeat Every/On:** These options enable you to define the frequency and schedule when this query will be run. For example, to repeat the query every week on Sunday, make the selections shown in the screen above.

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

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

To display a saved query –

1 In the Filters area, at the far right of the page, click the button ⋮ and select **Saved Queries**. The following displays listing all the queries that were saved using the **Save Query** option (described above), as shown below:

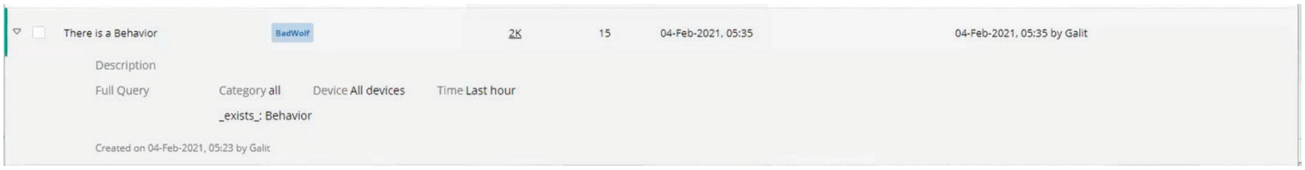


Saved Queries

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

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

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



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

Description

Full Query Category all Device All devices Time Last hour

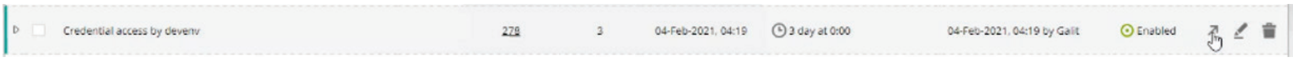
exists: Behavior

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

3 You can filter this list of saved queries by typing into the Search field and/or selecting one of the following options:

- **Scheduled/Unscheduled:** To specify that Scheduled Queries are listed in this window, click the **Scheduled** option. A Scheduled Query is one whose **Scheduled Query** field was marked when it was created/modified, as described above.
- **Community/User:** To specify that Community Queries are listed in this window, click the **Community** option. A Community Query is one whose **Community Query** field was marked when it was created/modified, as described above. 👥 appears in the list next to Community Queries. **User** refers to queries that are not Community Queries, meaning that each one is only available to the Organization for which it was created.

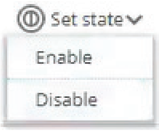
4 You can modify a Saved Query by hovering over it. The following tools are displayed on the right of the row:



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

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

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

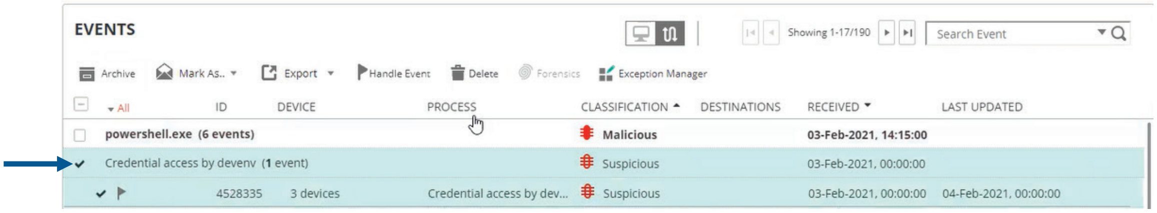


Scheduled Queries

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

The security event that is generated by a Scheduled Query in the Event Viewer is similar to a standard security event, except for the following:

- The following options are not available in the Event Viewer for Saved Query Security Events:
  - Forensics The **Forensics** option is not available because it is relevant.
  - An Exception cannot be defined for Saved Query Security Event.
- In the Process View of the Event Viewer, a Saved Query Security Event shows the name of the Saved Query instead of the process name, as shown below:

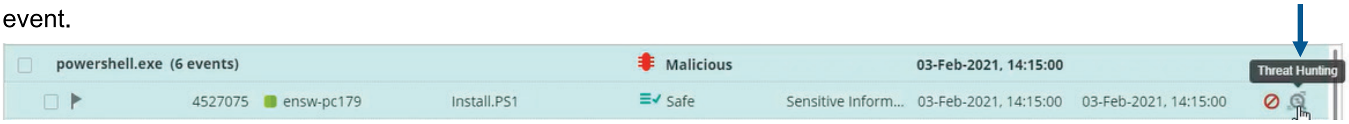


	All	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
□	powershell.exe (6 events)				Malicious		03-Feb-2021, 14:15:00	
✓	Credential access by devenv (1 event)				Suspicious		03-Feb-2021, 00:00:00	
✓		4528335	3 devices	Credential access by dev...	Suspicious		03-Feb-2021, 00:00:00	04-Feb-2021,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

The Classification (in the CLASSIFICATION column) is determined by the definition of the Saved Query.

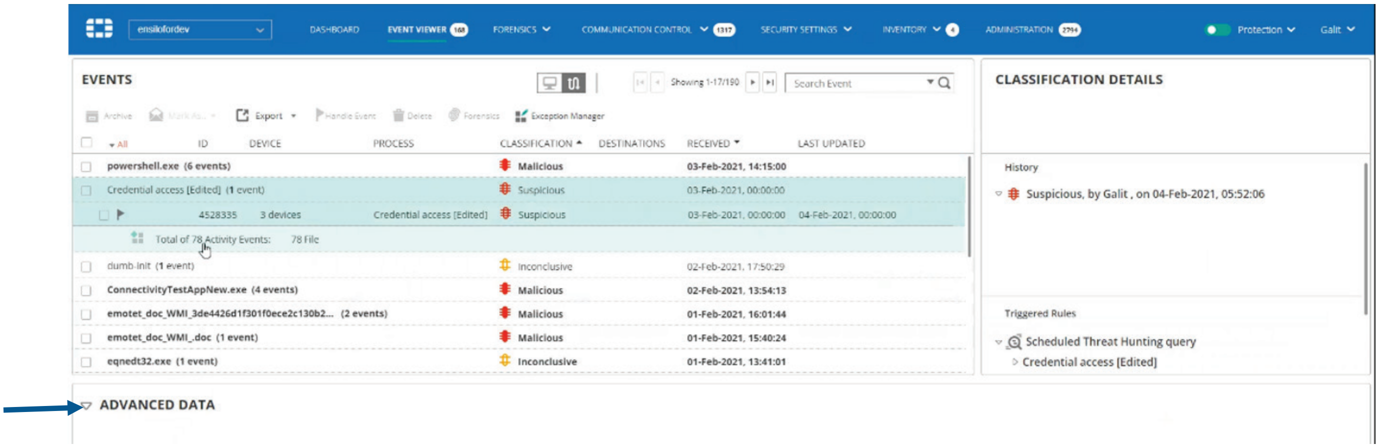
In the same manner as other security events it indicates the quantity of devices (in the DEVICE column) on which this type of activity events were found. All other aspects of a Saved Query Security Event are the same as other security events.

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



powershell.exe (6 events)			Malicious		03-Feb-2021, 14:15:00	
4527075	ensw-pc179	Install.PS1	Safe	Sensitive Inform...	03-Feb-2021, 14:15:00	03-Feb-2021, 14:15:00

- The Event Viewer does not show any **ADVANCED DATA** for a Saved Query Security Event.

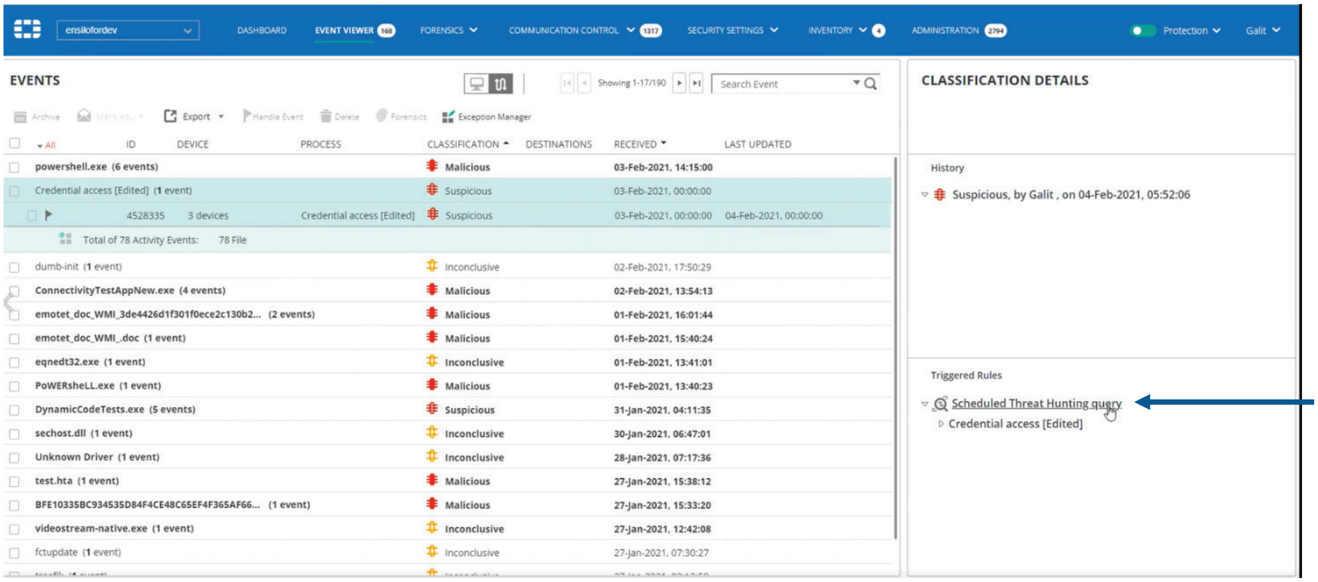


All	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
powershell.exe (6 events)				Malicious		03-Feb-2021, 14:15:00	
Credential access [Edited] (1 event)				Suspicious		03-Feb-2021, 00:00:00	
	4528335	3 devices	Credential access [Edited]	Suspicious		03-Feb-2021, 00:00:00	04-Feb-2021, 00:00:00
Total of 78 Activity Events: 78 File							
dumb-init (1 event)				Inconclusive		02-Feb-2021, 17:50:29	
ConnectivityTestAppNew.exe (4 events)				Malicious		02-Feb-2021, 13:54:13	
emotet_doc_WMI_3de4426d1f301f0ece2c130b2... (2 events)				Malicious		01-Feb-2021, 16:01:44	
emotet_doc_WMI_.doc (1 event)				Malicious		01-Feb-2021, 15:40:24	
eqnedt32.exe (1 event)				Inconclusive		01-Feb-2021, 13:41:01	

History
Suspicious, by Galit , on 04-Feb-2021, 05:52:06

Triggered Rules
Scheduled Threat Hunting query
Credential access [Edited]

- **Triggered Rules:** When a Saved Query Security Event is selected in the Event Viewer, the **Triggered Rules** pane on the bottom right of the page indicates that this security event was triggered by a **Scheduled Threat Hunting Query**, as shown below:

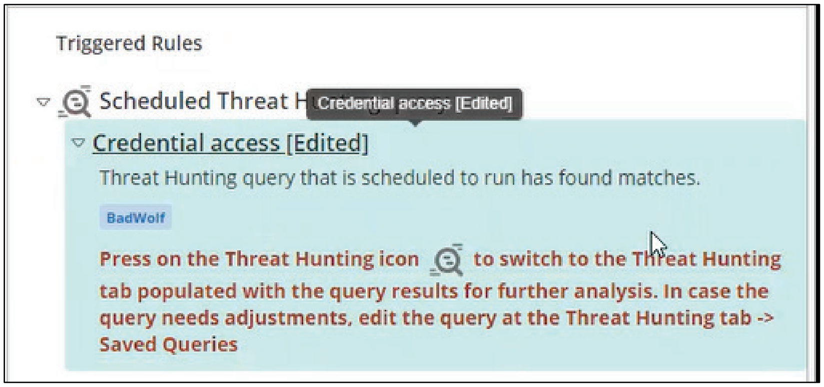


All	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
powershell.exe (6 events)				Malicious		03-Feb-2021, 14:15:00	
Credential access [Edited] (1 event)				Suspicious		03-Feb-2021, 00:00:00	
	4528335	3 devices	Credential access [Edited]	Suspicious		03-Feb-2021, 00:00:00	04-Feb-2021, 00:00:00
Total of 78 Activity Events: 78 File							
dumb-init (1 event)				Inconclusive		02-Feb-2021, 17:50:29	
ConnectivityTestAppNew.exe (4 events)				Malicious		02-Feb-2021, 13:54:13	
emotet_doc_WMI_3de4426d1f301f0ece2c130b2... (2 events)				Malicious		01-Feb-2021, 16:01:44	
emotet_doc_WMI_.doc (1 event)				Malicious		01-Feb-2021, 15:40:24	
eqnedt32.exe (1 event)				Inconclusive		01-Feb-2021, 13:41:01	
PoWERsheLL.exe (1 event)				Malicious		01-Feb-2021, 13:40:23	
DynamicCodeTests.exe (5 events)				Suspicious		31-Jan-2021, 04:11:35	
sechost.dll (1 event)				Inconclusive		30-Jan-2021, 06:47:01	
Unknown Driver (1 event)				Inconclusive		28-Jan-2021, 07:17:36	
test.hta (1 event)				Malicious		27-Jan-2021, 15:38:12	
BFE10335BC934535D84F4CE48C65EF4F365AF66... (1 event)				Malicious		27-Jan-2021, 15:33:20	
videostream-native.exe (1 event)				Inconclusive		27-Jan-2021, 12:42:08	
fctupdate (1 event)				Inconclusive		27-Jan-2021, 07:30:27	

History
Suspicious, by Galit , on 04-Feb-2021, 05:52:06

Triggered Rules
Scheduled Threat Hunting query
Credential access [Edited]

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



Triggered Rules

▿ Scheduled Threat H[unting] — Credential access [Edited]

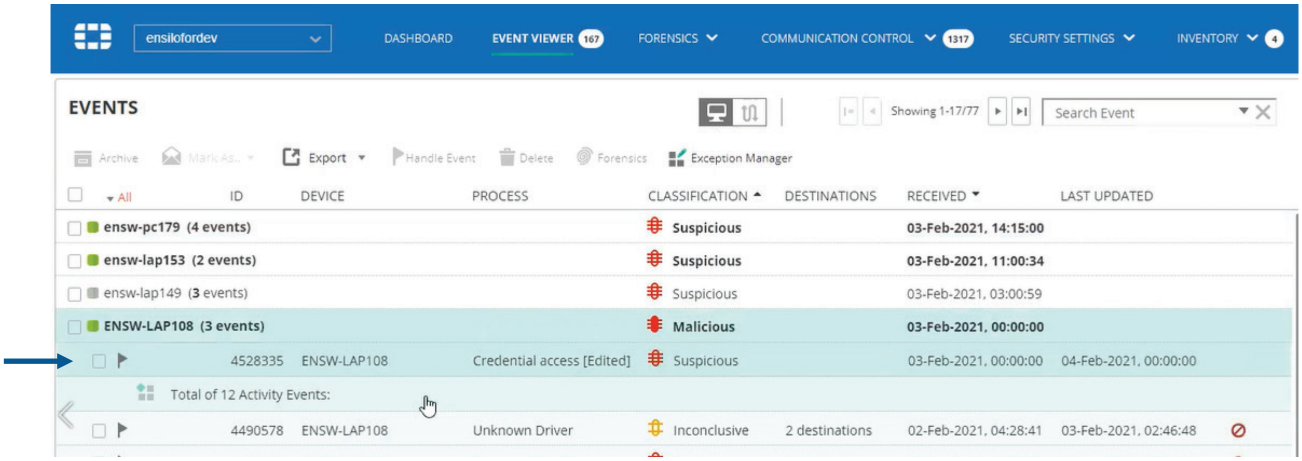
▿ Credential access [Edited]

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

BadWolf

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

- In the **Device View** of the Event Viewer, a Saved Query Security Event appears under the devices that were affected. It also shows the name of the Saved Query instead of the process name, as shown below:

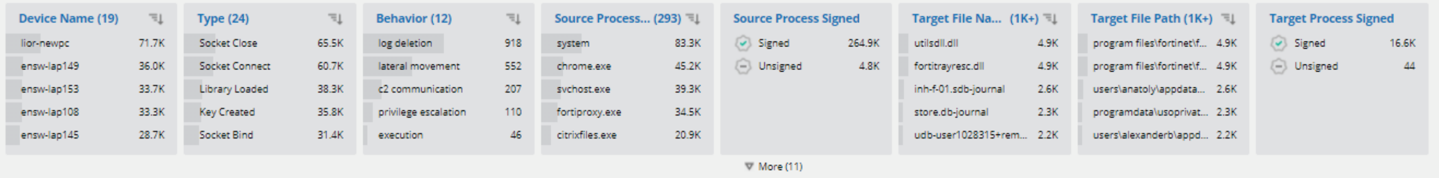


▾ All	ID	DEVICE	PROCESS	CLASSIFICATION ▴	DESTINATIONS	RECEIVED ▾	LAST UPDATED
ensw-pc179 (4 events)				Suspicious		03-Feb-2021, 14:15:00	
ensw-lap153 (2 events)				Suspicious		03-Feb-2021, 11:00:34	
ensw-lap149 (3 events)				Suspicious		03-Feb-2021, 03:00:59	
ENSW-LAP108 (3 events)				Malicious		03-Feb-2021, 00:00:00	
	4528335	ENSW-LAP108	Credential access [Edited]	Suspicious		03-Feb-2021, 00:00:00	04-Feb-2021, 00:00:00
Total of 12 Activity Events:							
	4490578	ENSW-LAP108	Unknown Driver	Inconclusive	2 destinations	02-Feb-2021, 04:28:41	03-Feb-2021, 02:46:48

If this security event was triggered for more than 100 devices, then this row shows a notification indicating that they are not all listed here and that you can use the Threat Hunting in option on the right of this event's row to investigate further.

Facets

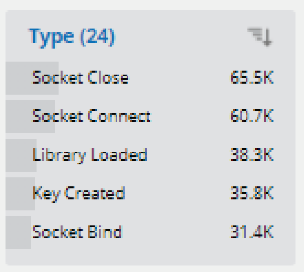
As expected, the continuous, realtime collection of Threat Hunting data produces numerous activity events. The sheer volume of activity data makes working directly with these activity events almost unmanageable. Therefore, FortiEDR uses **facets** to summarize the data displayed in the results tables.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



Device Name (19)		Type (24)		Behavior (12)		Source Process... (293)		Source Process Signed		Target File Na... (1K+)		Target File Path (1K+)		Target Process Signed	
lior-newpc	71.7K	Socket Close	65.5K	log deletion	918	system	83.3K	Signed	264.9K	utilsdll.dll	4.9K	program files\fortinet\f...	4.9K	Signed	16.6K
ensw-lap149	36.0K	Socket Connect	60.7K	lateral movement	552	chrome.exe	45.2K	Unsigned	4.8K	fortitrayresc.dll	4.9K	program files\fortinet\f...	4.9K	Unsigned	44
ensw-lap153	33.7K	Library Loaded	38.3K	c2 communication	207	svchost.exe	39.3K			inh-f-01.sdb-journal	2.6K	users\anatoly\appdata...	2.6K		
ensw-lap108	33.3K	Key Created	35.8K	privilege escalation	110	fortiproxy.exe	34.5K			store.db-journal	2.3K	programdata\usoprivat...	2.3K		
ensw-lap145	28.7K	Socket Bind	31.4K	execution	46	citrixfiles.exe	20.9K			udb-user1028315+rem...	2.2K	users\alexanderb\appd...	2.2K		

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

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

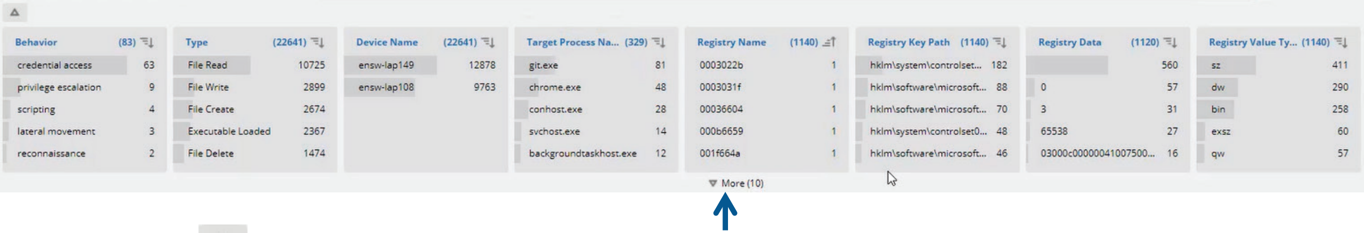


Type (24)	
Socket Close	65.5K
Socket Connect	60.7K
Library Loaded	38.3K
Key Created	35.8K
Socket Bind	31.4K

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

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

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

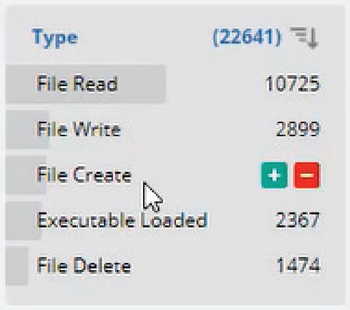


Behavior	(83)	Type	(22641)	Device Name	(22641)	Target Process Na...	(329)	Registry Name	(1140)	Registry Key Path	(1140)	Registry Data	(1120)	Registry Value Ty...	(1140)
credential access	63	File Read	10725	ensw-lap149	12878	git.exe	81	0003022b	1	hklm\system\controlset...	182		560	sz	411
privilege escalation	9	File Write	2899	ensw-lap108	9763	chrome.exe	48	0003031f	1	hklm\software\microsoft...	88	0	57	dw	290
scripting	4	File Create	2674			conhost.exe	28	00036604	1	hklm\software\microsoft...	70	3	31	bin	258
lateral movement	3	Executable Loaded	2367			svchost.exe	14	000b6659	1	hklm\system\controlset0...	48	65538	27	exsz	60
reconnaissance	2	File Delete	1474			backgroundtaskhost.exe	12	001f664a	1	hklm\software\microsoft...	46	03000c00000041007500...	16	qw	57

You can click the △ button to minimize the Facets area.

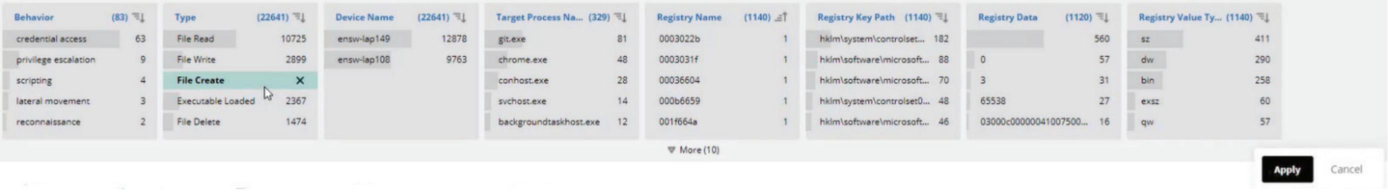
Filtering Using Facets

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



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

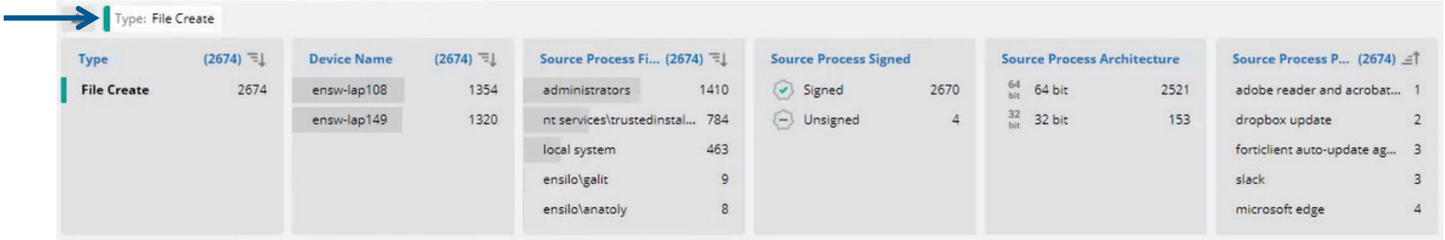
Then, click the **Apply** button.



Behavior	(83)	Type	(22641)	Device Name	(22641)	Target Process Na...	(329)	Registry Name	(1140)	Registry Key Path	(1140)	Registry Data	(1120)	Registry Value Ty...	(1140)
credential access	63	File Read	10725	ensw-lap149	12878	git.exe	81	0003022b	1	hklm\system\controlset...	182		560	sz	411
privilege escalation	9	File Write	2899	ensw-lap108	9763	chrome.exe	48	0003031f	1	hklm\software\microsoft...	88	0	57	dw	290
scripting	4	File Create	×			conhost.exe	28	00036604	1	hklm\software\microsoft...	70	3	31	bin	258
lateral movement	3	Executable Loaded	2367			svchost.exe	14	000b6659	1	hklm\system\controlset0...	48	65538	27	exsz	60
reconnaissance	2	File Delete	1474			backgroundtaskhost.exe	12	001f664a	1	hklm\software\microsoft...	46	03000c00000041007500...	16	qw	57

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

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

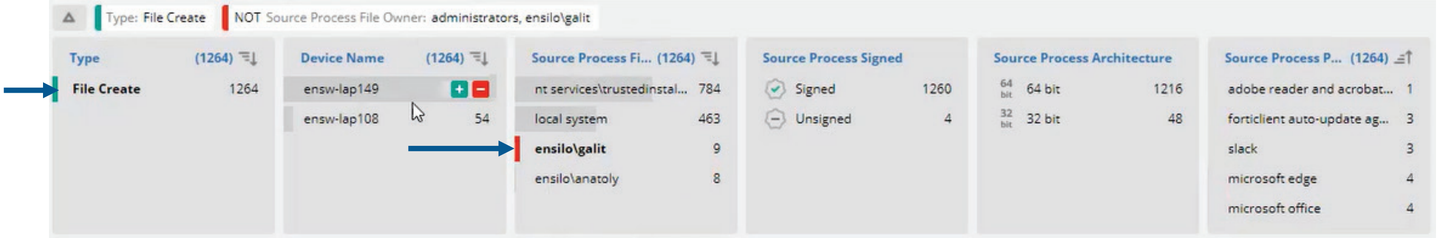


Type: File Create

Type (2674)		Device Name (2674)		Source Process Fi... (2674)		Source Process Signed		Source Process Architecture		Source Process P... (2674)	
File Create	2674	ensw-lap108	1354	administrators	1410	Signed	2670	64 bit	2521	adobe reader and acrobat...	1
		ensw-lap149	1320	nt services\trustedinstal...	784	Unsigned	4	32 bit	153	dropbox update	2
				local system	463					forticlient auto-update ag...	3
				ensilo\galit	9					slack	3
				ensilo\anatoly	8					microsoft edge	4

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

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

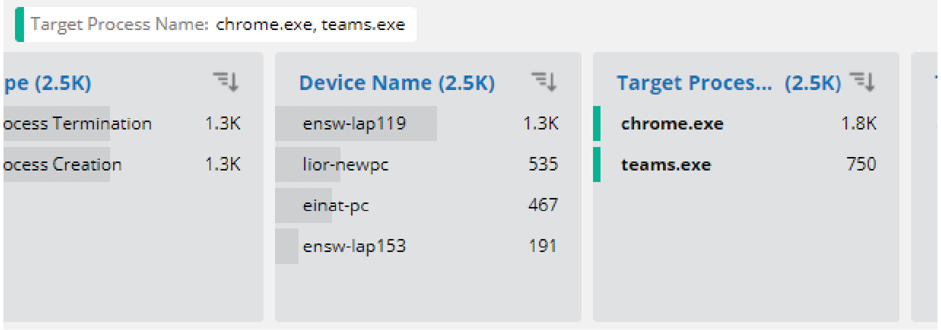


Type: File Create | NOT Source Process File Owner: administrators, ensilo\galit

Type (1264)		Device Name (1264)		Source Process Fi... (1264)		Source Process Signed		Source Process Architecture		Source Process P... (1264)	
File Create	1264	ensw-lap149	+ −	nt services\trustedinstal...	784	Signed	1260	64 bit	1216	adobe reader and acrobat...	1
		ensw-lap108	54	local system	463	Unsigned	4	32 bit	48	forticlient auto-update ag...	3
				ensilo\galit	9					slack	3
				ensilo\anatoly	8					microsoft edge	4
										microsoft office	4

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

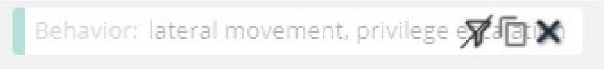
If two values have been added to the query from the same Facet pane, the relationship between the values in the chip is OR. The following example shows that the query includes activity events in which their Target Process Name is either **chrome.exe** or **teams.exe**, which is shown below in both the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



Target Process Name: chrome.exe, teams.exe

pe (2.5K)		Device Name (2.5K)		Target Proces... (2.5K)	
ocess Termination	1.3K	ensw-lap119	1.3K	**chrome.exe**	1.8K
ocess Creation	1.3K	lior-newpc	535	**teams.exe**	750
		einat-pc	467		
		ensw-lap153	191		

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



Behavior: lateral movement, privilege e

- **Remove –** The chip is removed and the Facets and Result tables are updated accordingly.

- **Disable –** A disabled chip no longer affects the results. The Facets and the Results tabs are updated as if the chip was removed and the chip appears as follows:

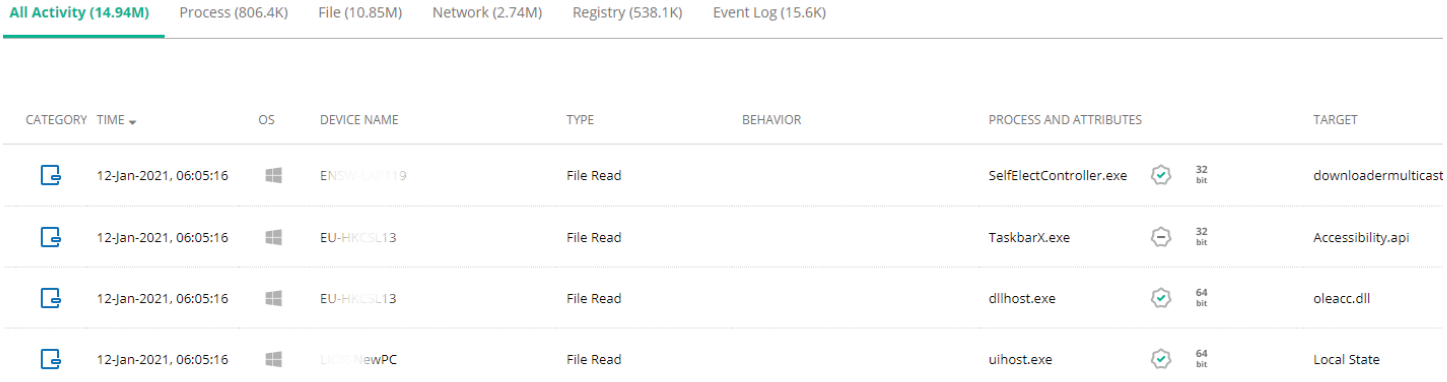
  Type: File Read, Socket Connect

- **Copy –** The chip content is copied to memory and can be pasted into the query for further editing.

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

Activity Events Tables

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

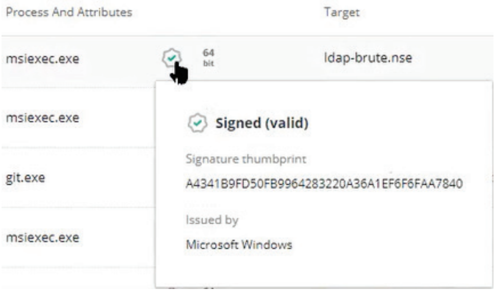


All Activity (14.94M) | Process (806.4K) | File (10.85M) | Network (2.74M) | Registry (538.1K) | Event Log (15.6K)

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

- **All Activity:** This tab (shown above) lists all activity events, based on the filters defined for the Threat Hunting query. The number in parentheses () specifies the total number of activity events, based on your query criteria. This total equals the sum of the activity events in the other five tabs. Each Category of activity events is represented by a different icon, as follows:
  - ⇅ – Process
  - 🗎 – File
  - ⠿ – Registry
  - 🌐 – Network
  - 🗋 – Log

  You can hover over the icon in the **Process and Attributes** column to temporarily display additional details about the source process, including whether it is signed, its signature, issuer and so on.

Process And Attributes			Target
msiexec.exe	✓	64 bit	ldap-brute.nse
msiexec.exe			
git.exe			
msiexec.exe			

  ✓ Signed (valid)

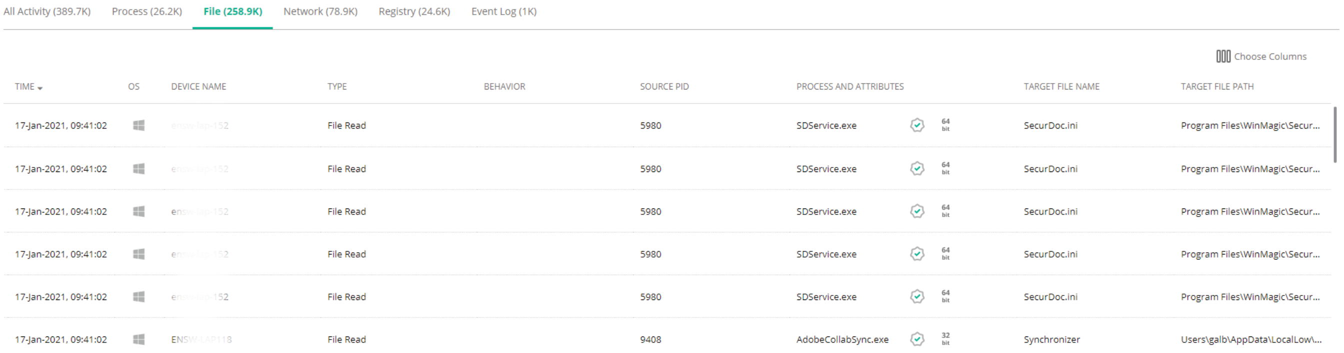
  Signature thumbprint
  A4341B9FD50FB9964283220A36A1EF6F6FAA7840

  Issued by
  Microsoft Windows

  Note – There are several types of attribute icons, such as Signed/Unsigned.

- **Process:** This tab shows all matching activity events of category Process.

- **File:** This tab shows all matching activity events of category File.



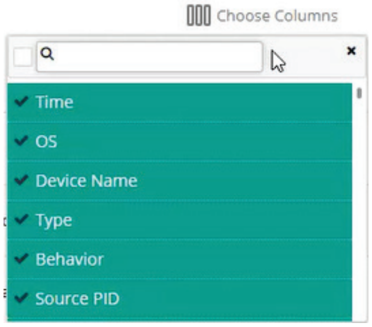
All Activity (389.7K) | Process (26.2K) | **File (258.9K)** | Network (78.9K) | Registry (24.6K) | Event Log (1K)

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

- **Network:** This tab shows all matching activity events of type Network.
- **Registry:** This tab shows all matching activity events of type Registry.
- **Event Log:** This tab shows all matching activity events of type Event Log.

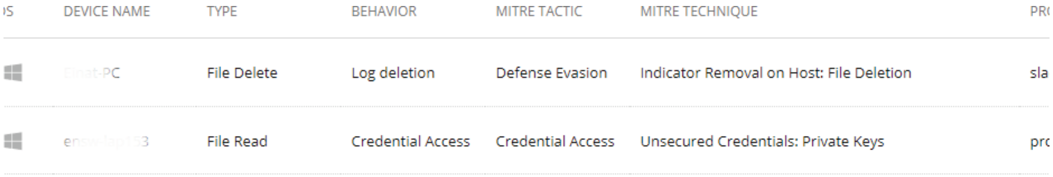
Each table contains a row for each matching activity event and each table includes different columns according to the Category.

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



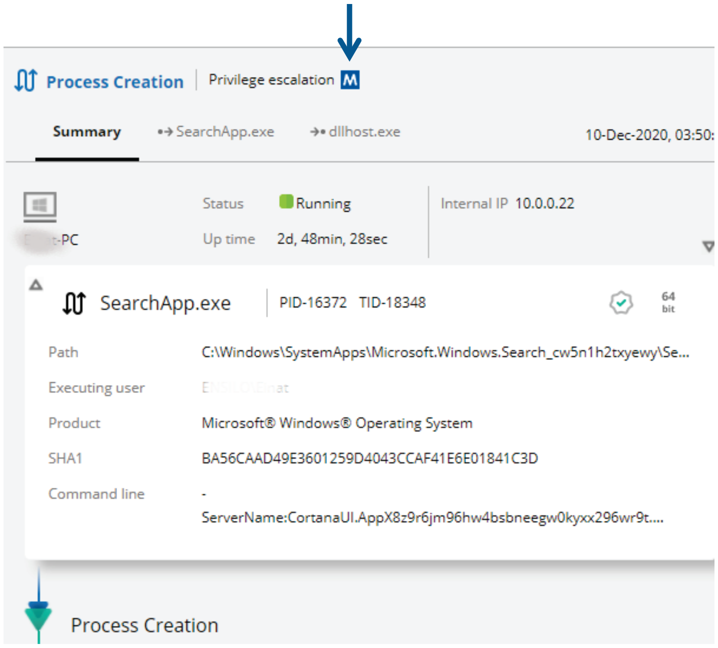
Each activity event may also be a part of a *behavior* and/or a MITRE Technique. A behavior indicates that this activity event is part of a specific behavior as determined by FortiEDR. A MITRE type (Technique or Tactic) indicates that the activity event is part of specification of a technique and tactic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

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



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

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



Process Creation | Privilege escalation M

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

[redacted]-PC

Status: Running

Up time: 2d, 48min, 28sec

Internal IP: 10.0.0.22

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

Path: C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\Se...

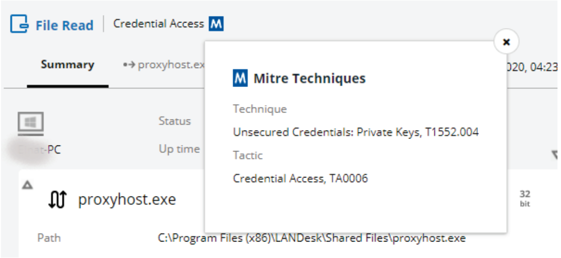
Executing user: [redacted]

Product: Microsoft® Windows® Operating System

SHA1: BA56CAAD49E3601259D4043CCAF41E6E01841C3D

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

Process Creation



File Read | Credential Access M

Summary | ••→ proxyhost.ex | 020, 04:23

[redacted]-PC

Status

Up time

proxyhost.exe | 32 bit

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

M Mitre Techniques

Technique

Unsecured Credentials: Private Keys, T1552.004

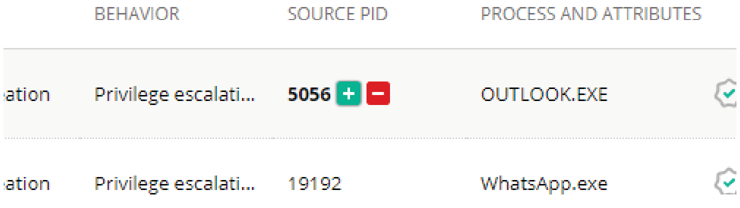
Tactic

Credential Access, TA0006

Filtering Using Activity Events Tables

The Activity Events Tables area can be used to add filters to the query in a similar manner as Facets.

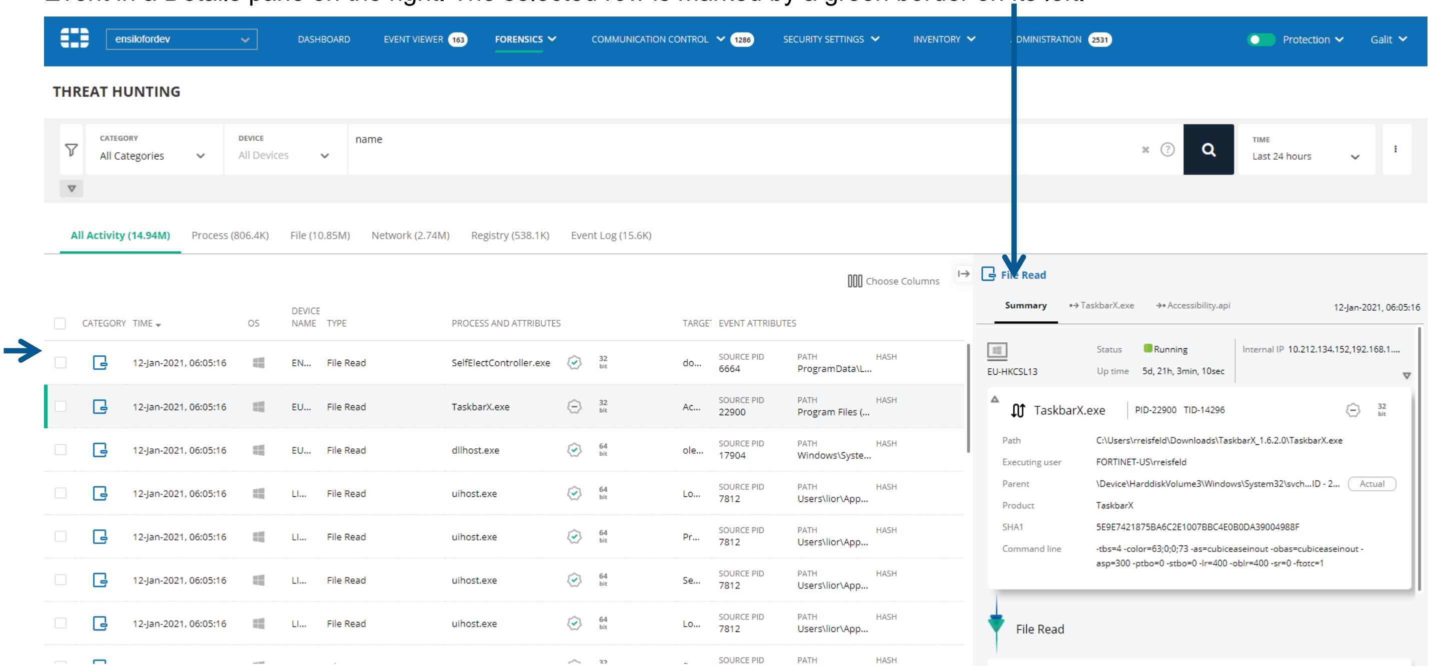
When you hover over an item in the table, a green and red button appear to its right. Click the green plus ➕ button to include that item as a filter or click the red minus ➖ button to exclude that item as a filter. For more details, see page 167.



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

Details Pane

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



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

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

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

File Read

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

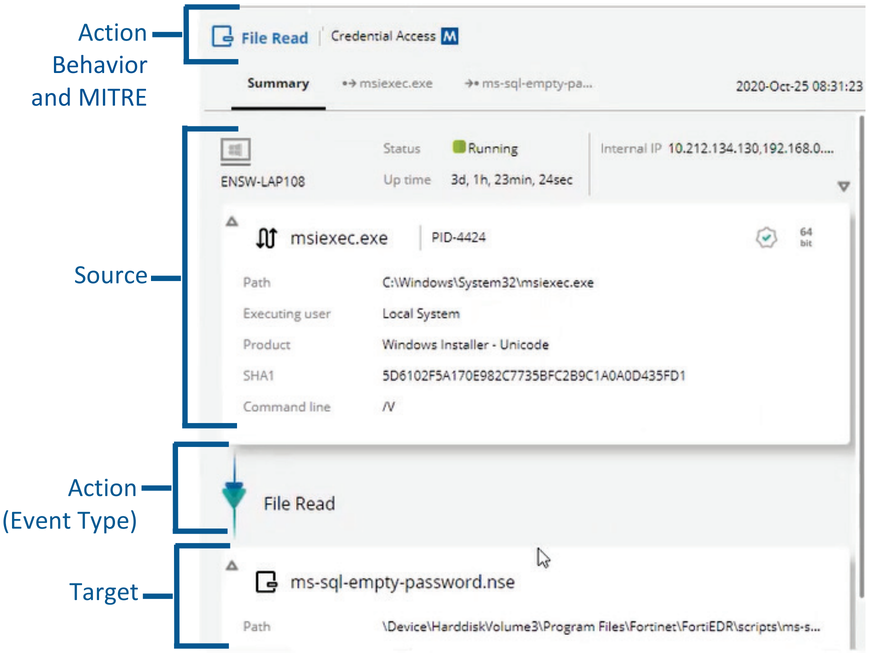
EU-HKCSL13 — Status: Running — Up time: 5d, 21h, 3min, 10sec — Internal IP: 10.212.134.152,192.168.1....

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

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

File Read

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



File Read | Credential Access

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

ENSW-LAP108 — Status: Running — Up time: 3d, 1h, 23min, 24sec — Internal IP: 10.212.134.130,192.168.0....

msiexec.exe — PID-4424 — 64 bit

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

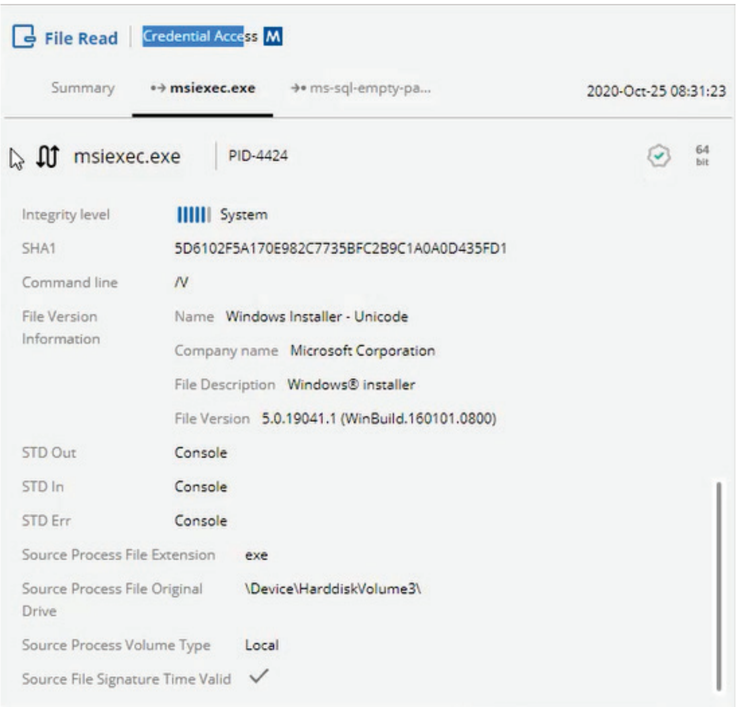
File Read

ms-sql-empty-password.nse

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

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

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



msiexec.exe | PID-4424

Integrity level: System

SHA1: 5D6102F5A170E982C7735BFC2B9C1A0A0D435FD1

Command line: /V

File Version Information:
Name: Windows Installer - Unicode
Company name: Microsoft Corporation
File Description: Windows® installer
File Version: 5.0.19041.1 (WinBuild.160101.0800)

STD Out: Console

STD In: Console

STD Err: Console

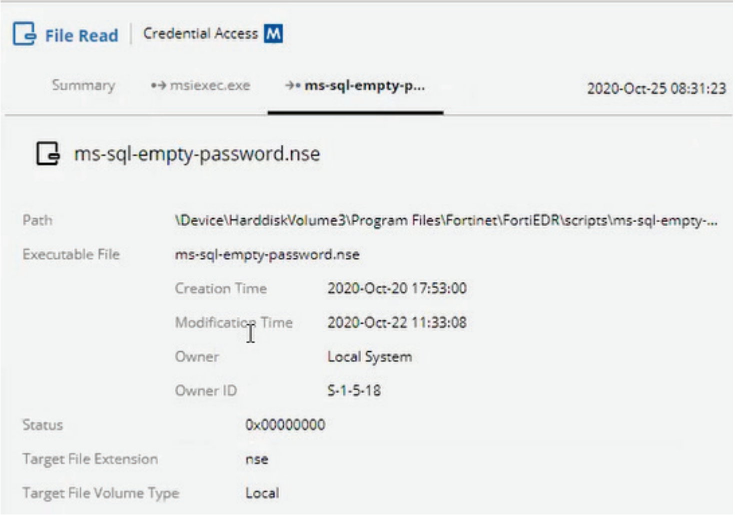
Source Process File Extension: exe

Source Process File Original Drive: \Device\HarddiskVolume3\

Source Process Volume Type: Local

Source File Signature Time Valid: ✓

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



ms-sql-empty-password.nse

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

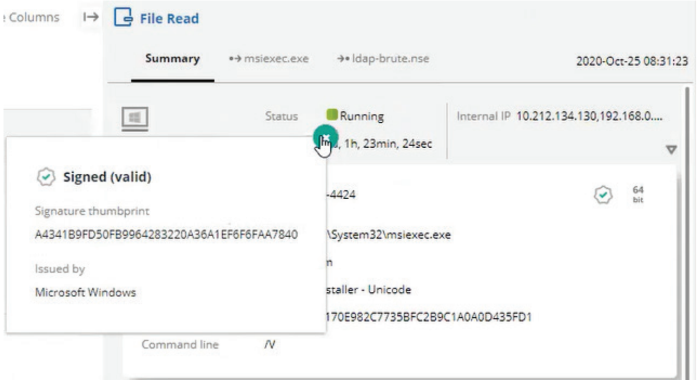
Executable File: ms-sql-empty-password.nse
Creation Time: 2020-Oct-20 17:53:00
Modification Time: 2020-Oct-22 11:33:08
Owner: Local System
Owner ID: S-1-5-18

Status: 0x00000000

Target File Extension: nse

Target File Volume Type: Local

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



Status: Running
, 1h, 23min, 24sec

Internal IP: 10.212.134.130,192.168.0....

Signed (valid)

Signature thumbprint: A4341B9FD50FB9964283220A36A1EF6F6FAA7840

Issued by: Microsoft Windows

-4424

\System32\msiexec.exe

n

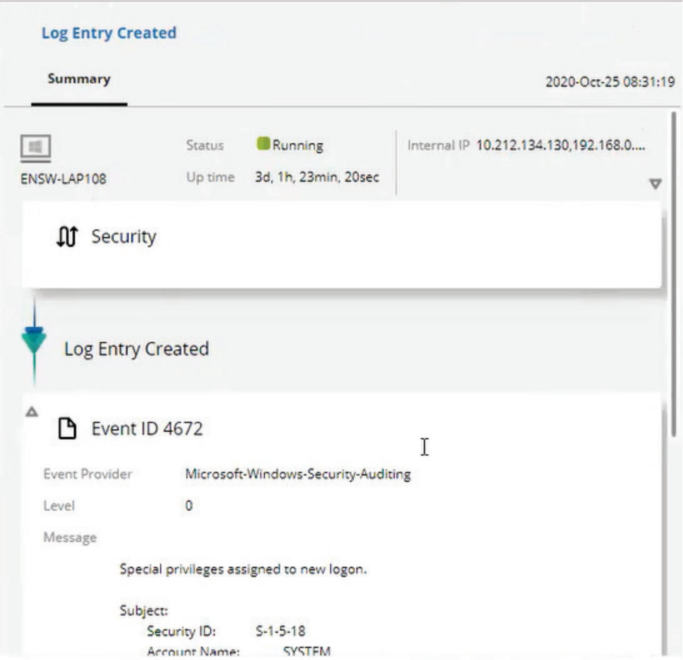
staller - Unicode

170E982C7735BFC2B9C1A0A0D435FD1

Command line: /V

Event Log Details Pane

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



Log Entry Created

Summary 2020-Oct-25 08:31:19

ENSW-LAP108 Status Running Up time 3d, 1h, 23min, 20sec Internal IP 10.212.134.130,192.168.0....

Security

Log Entry Created

Event ID 4672

Event Provider Microsoft-Windows-Security-Auditing

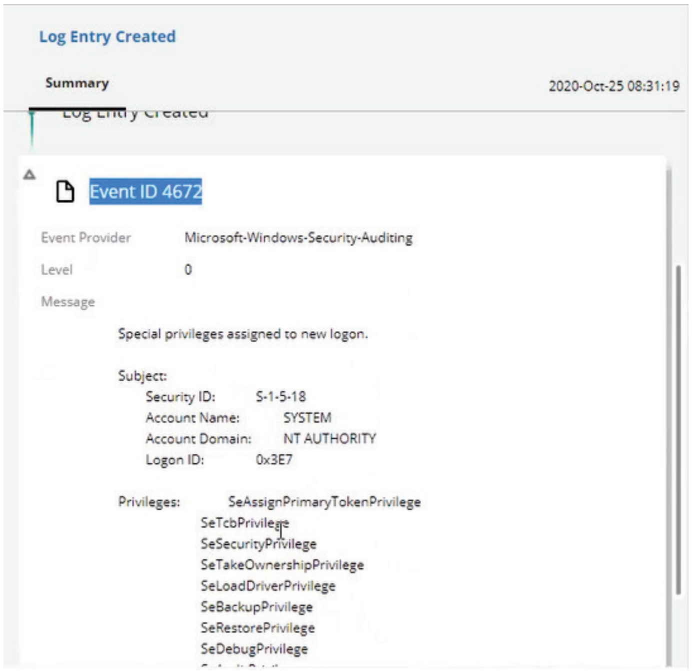
Level 0

Message

```
Special privileges assigned to new logon.

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

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



Log Entry Created

Summary 2020-Oct-25 08:31:19

Log Entry Created

Event ID 4672

Event Provider Microsoft-Windows-Security-Auditing

Level 0

Message

```
Special privileges assigned to new logon.

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

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

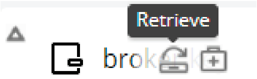
Retrieving a File / Remediating Devices upon Malware Detection

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

To retrieve a file or remediate the process:

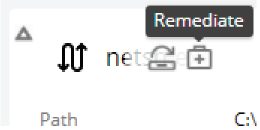
1. Select the relevant Activity Event and open its Details Pane.
2. When hovering over the file name, you can choose whether to –

   Retrieve the file, as shown below:

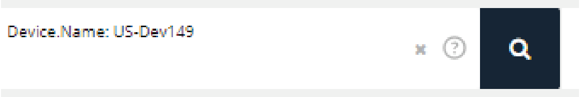
   – OR –

   Remediate it, as shown below:

GDPR and Activity Event Data

The FortiEDR system fully complies with the General Data Protection Regulation (GDPR) standard, as described in the *Personal Data Handling* section on page 214. When you use the Personal Data Handling feature to delete data, it also deletes activity event data. However, the Personal Data Handling Search option does not search for and display the activity data that it will delete. Just for your own knowledge, in order to see a list of the activity data that will be deleted you can view it here before you delete it. To do so, simply enter a query here that includes the chosen record from the Activity Report (that can be accessed by selecting **Administration ➔ Tools ➔ Personal Data Handling**) in order to find the data to be removed. For example, if you have provided the string **149** in **Personal Data Handling** for Search by **Device name**, then in the displayed Activity Report, select the record containing the Device name to be deleted. In this example, it is **US-Dev149**. Then, in order to display all the activity events that are related to this device, enter the query **Device.Name: US-Dev149**, as shown below in order to display the relevant records.



Device.Name: US-Dev149

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

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

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

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

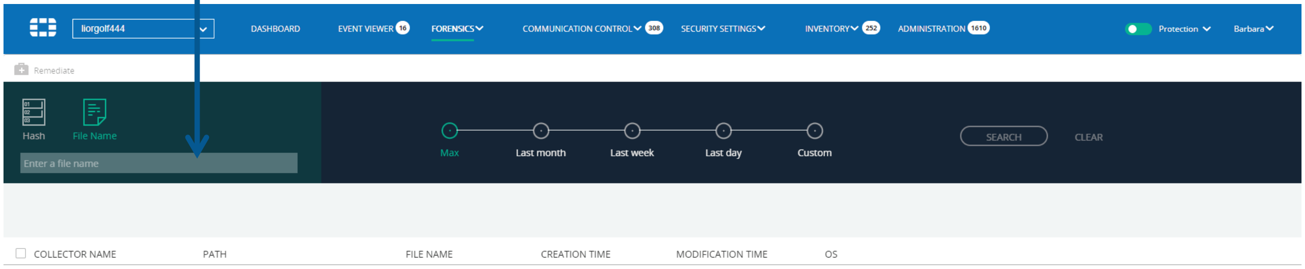
Legacy Threat Hunting

FortiEDR's Legacy Threat Hunting is available in FortiEDR environments that have been upgraded to v5.0 and above from previous versions. This feature enables you to hunt for files and hashes that were collected before the upgrade to v5.0.

Use the Legacy Threat Hunting feature when there are Collectors in your system that have not been upgraded to FortiEDR V5.0 in order to search for files/hashes on those Collectors. After all Collectors have been upgraded to V5.0 or above, you can use FortiEDR's Threat Hunting feature instead, which has more extensive collected data. For more details, see page 158.

Access the **Threat Hunting Legacy** page under the **Forensics** tab.

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 using Threat Hunting (Legacy):

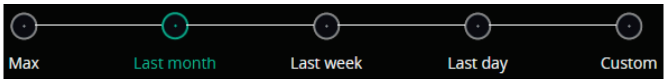
1 Select the basis for the search by clicking the Hash or File Name button. When you select the Hash button, the search results represent matching HASH values. When you select the File Name button, the search results represent matching file names.

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.

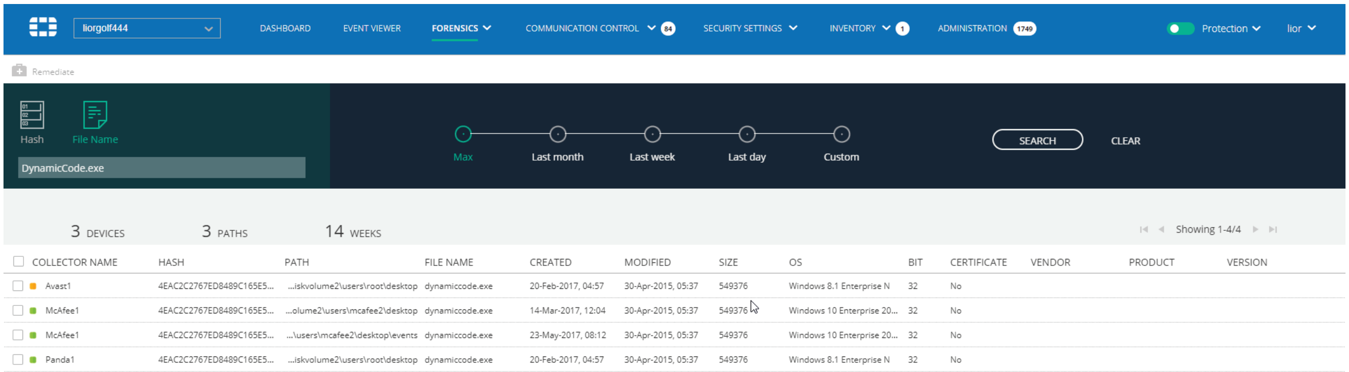
When accessing the **Threat Hunting** page using Method 2 (described above), the field adjacent to the Hash and File Name buttons is empty.

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.



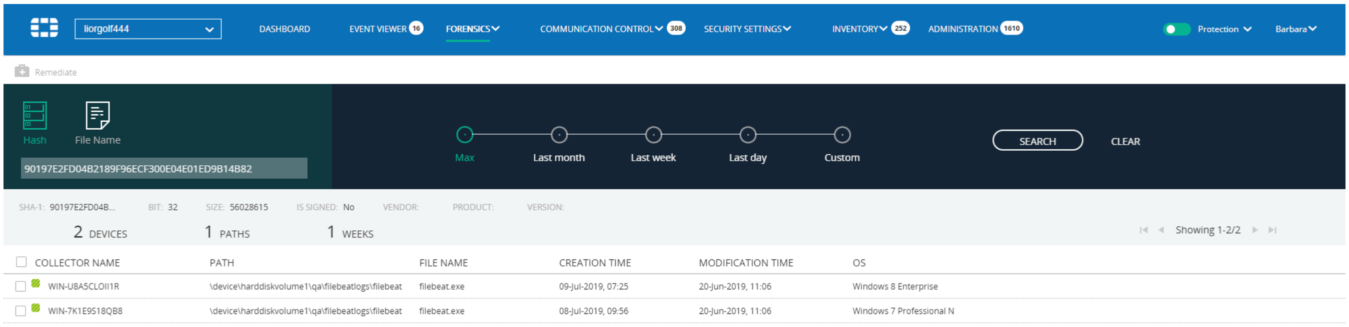
DynamicCode.exe

3 DEVICES 3 PATHS 14 WEEKS

Showing 1-4/4

□ COLLECTOR NAME	HASH	PATH	FILE NAME	CREATED	MODIFIED	SIZE	OS	BIT	CERTIFICATE	VENDOR	PRODUCT	VERSION
□ 🟧 Avast1	4EAC2C2767ED8489C165E5...	...iskvolume2\users\root\desktop	dynamiccode.exe	20-Feb-2017, 04:57	30-Apr-2015, 05:37	549376	Windows 8.1 Enterprise N	32	No			
□ 🟩 McAfee1	4EAC2C2767ED8489C165E5...	...olume2\users\mcafee2\desktop	dynamiccode.exe	14-Mar-2017, 12:04	30-Apr-2015, 05:37	549376	Windows 10 Enterprise 20...	32	No			
□ 🟩 McAfee1	4EAC2C2767ED8489C165E5...	...\users\mcafee2\desktop\events	dynamiccode.exe	23-May-2017, 08:12	30-Apr-2015, 05:37	549376	Windows 10 Enterprise 20...	32	No			
□ 🟩 Panda1	4EAC2C2767ED8489C165E5...	...iskvolume2\users\root\desktop	dynamiccode.exe	20-Feb-2017, 04:57	30-Apr-2015, 05:37	549376	Windows 8.1 Enterprise N	32	No			

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



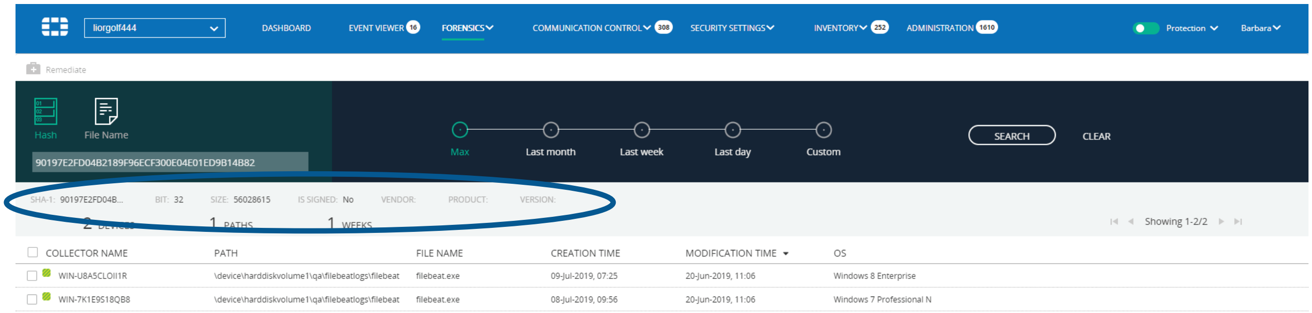
90197E2FD04B2189F96ECF300E04E01ED9B14B82

SHA-1: 90197E2FD04B... BIT: 32 SIZE: 56028615 IS SIGNED: No VENDOR: PRODUCT: VERSION:

2 DEVICES 1 PATHS 1 WEEKS Showing 1-2/2

□ COLLECTOR NAME	PATH	FILE NAME	CREATION TIME	MODIFICATION TIME	OS
□ WIN-U8A5CLOII1R	\device\harddiskvolume1\qa\filebeatlogs\filebeat	filebeat.exe	09-Jul-2019, 07:25	20-Jun-2019, 11:06	Windows 8 Enterprise
□ WIN-7K1E9S18QB8	\device\harddiskvolume1\qa\filebeatlogs\filebeat	filebeat.exe	08-Jul-2019, 09:56	20-Jun-2019, 11:06	Windows 7 Professional N

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



90197E2FD04B2189F96ECF300E04E01ED9B14B82

SHA-1: 90197E2FD04B... BIT: 32 SIZE: 56028615 IS SIGNED: No VENDOR: PRODUCT: VERSION:

2 DEVICES 1 PATHS 1 WEEKS Showing 1-2/2

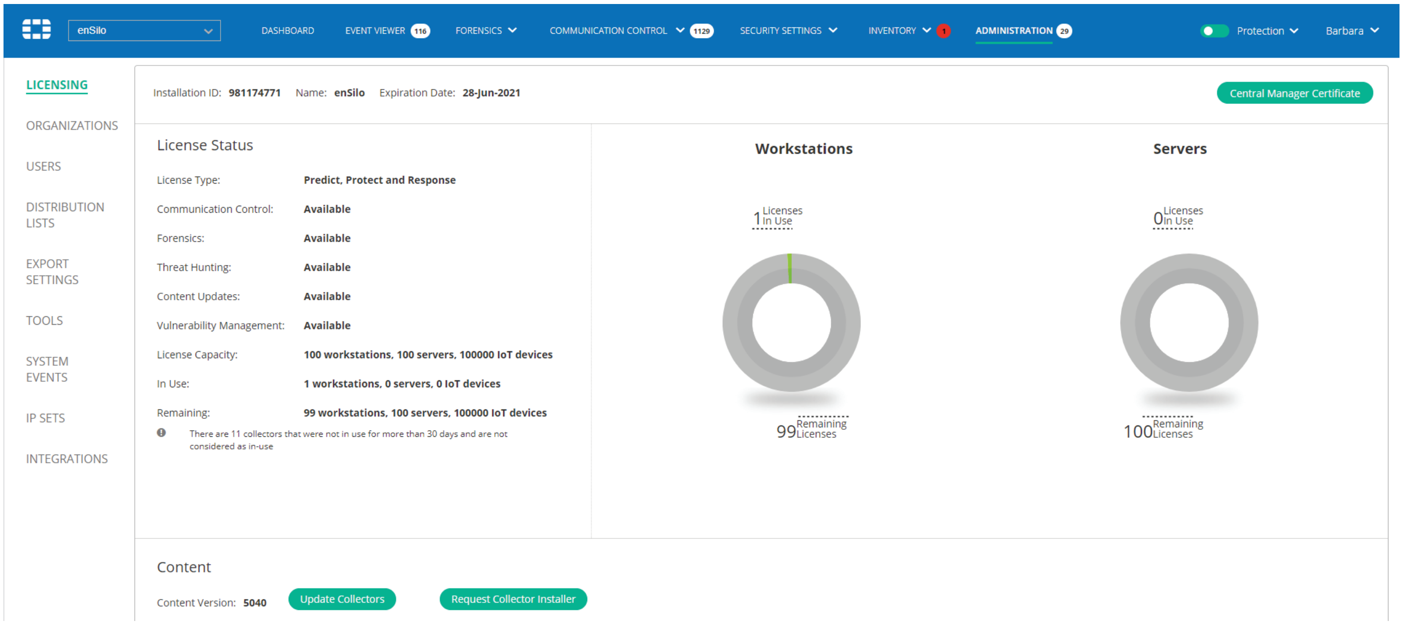
□ COLLECTOR NAME	PATH	FILE NAME	CREATION TIME	MODIFICATION TIME ▾	OS
□ WIN-U8A5CLOII1R	\device\harddiskvolume1\qa\filebeatlogs\filebeat	filebeat.exe	09-Jul-2019, 07:25	20-Jun-2019, 11:06	Windows 8 Enterprise
□ WIN-7K1E9S18QB8	\device\harddiskvolume1\qa\filebeatlogs\filebeat	filebeat.exe	08-Jul-2019, 09:56	20-Jun-2019, 11:06	Windows 7 Professional N

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 28 for more information.



Installation ID: **981174771** Name: **enSilo** Expiration Date: **28-Jun-2021**

License Status

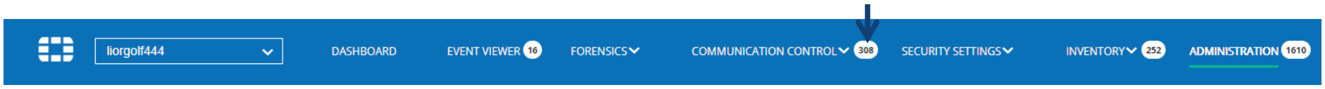
License Type:	**Predict, Protect and Response**
Communication Control:	**Available**
Forensics:	**Available**
Threat Hunting:	**Available**
Content Updates:	**Available**
Vulnerability Management:	**Available**
License Capacity:	**100 workstations, 100 servers, 100000 IoT devices**
In Use:	**1 workstations, 0 servers, 0 IoT devices**
Remaining:	**99 workstations, 100 servers, 100000 IoT devices**

There are 11 collectors that were not in use for more than 30 days and are not considered as in-use

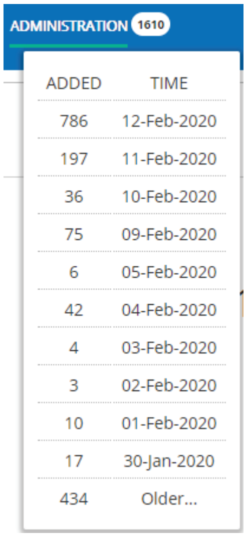
Content

Content Version: **5040**

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



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

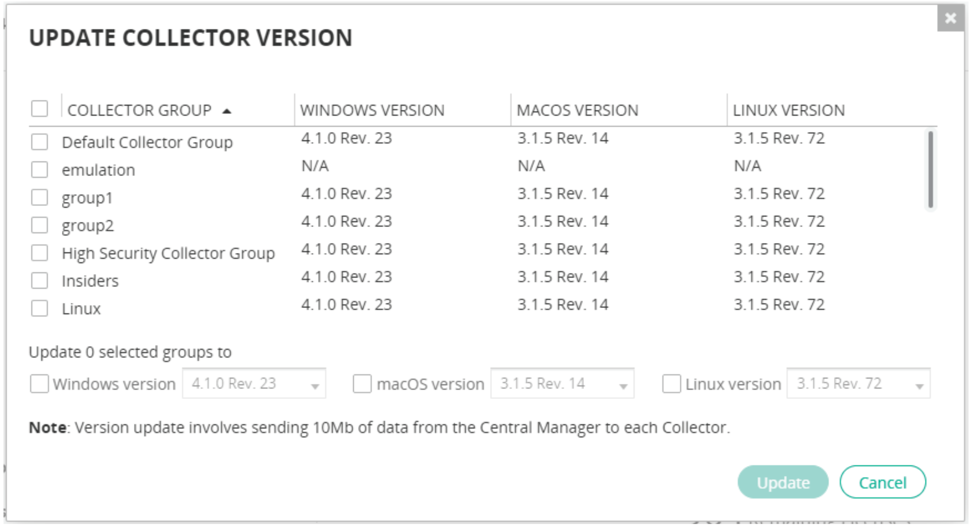


ADDED	TIME
786	12-Feb-2020
197	11-Feb-2020
36	10-Feb-2020
75	09-Feb-2020
6	05-Feb-2020
42	04-Feb-2020
4	03-Feb-2020
3	02-Feb-2020
10	01-Feb-2020
17	30-Jan-2020
434	Older...

Updating the Collector Version

The Update Collector Version feature is used to update a FortiEDR version, such as from version 3.1.**0** to 3.1.**1**. To update a FortiEDR revision, use the Automatic Updates feature described on page 210.

When you click the **Update Collectors** button in the Licensing window, the Update Collector Version window displays. This window lists all available Collector Groups. The **Windows Version**, **MacOS Version** and **Linux Version** columns indicate the current FortiEDR version for the Collectors in a Collector Group.



UPDATE COLLECTOR VERSION

□ COLLECTOR GROUP ▲	WINDOWS VERSION	MACOS VERSION	LINUX VERSION
□ Default Collector Group	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
□ emulation	N/A	N/A	N/A
□ group1	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
□ group2	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
□ High Security Collector Group	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
□ Insiders	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
□ Linux	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72

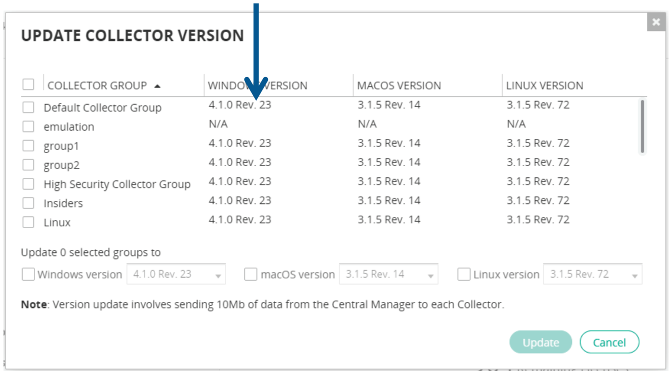
Update 0 selected groups to

□ Windows version 4.1.0 Rev. 23 □ macOS version 3.1.5 Rev. 14 □ Linux version 3.1.5 Rev. 72

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

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.



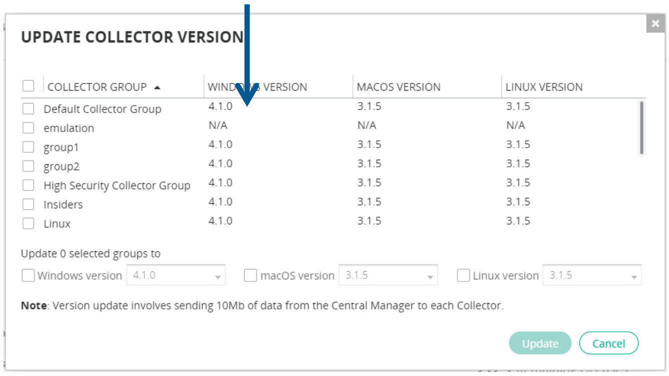
UPDATE COLLECTOR VERSION

□ COLLECTOR GROUP ▲	WINDOWS VERSION	MACOS VERSION	LINUX VERSION
□ Default Collector Group	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
□ emulation	N/A	N/A	N/A
□ group1	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
□ group2	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
□ High Security Collector Group	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
□ Insiders	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
□ Linux	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72

Update 0 selected groups to

□ Windows version 4.1.0 Rev. 23 □ macOS version 3.1.5 Rev. 14 □ Linux version 3.1.5 Rev. 72

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



UPDATE COLLECTOR VERSION

□ COLLECTOR GROUP ▲	WINDOWS VERSION	MACOS VERSION	LINUX VERSION
□ Default Collector Group	4.1.0	3.1.5	3.1.5
□ emulation	N/A	N/A	N/A
□ group1	4.1.0	3.1.5	3.1.5
□ group2	4.1.0	3.1.5	3.1.5
□ High Security Collector Group	4.1.0	3.1.5	3.1.5
□ Insiders	4.1.0	3.1.5	3.1.5
□ Linux	4.1.0	3.1.5	3.1.5

Update 0 selected groups to

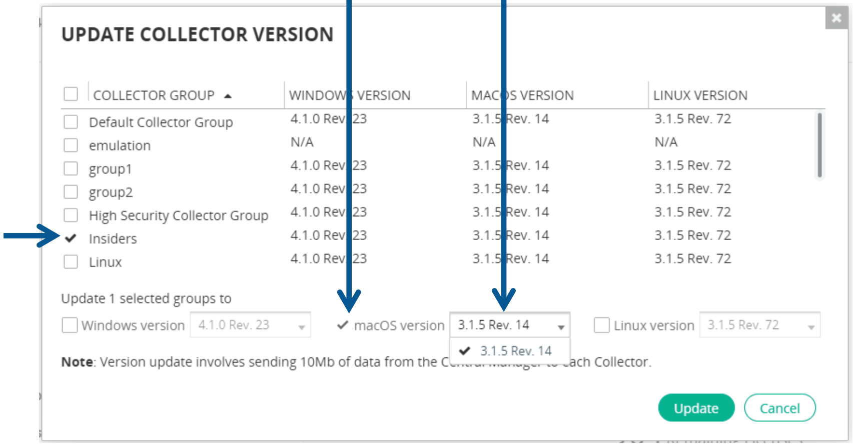
□ Windows version 4.1.0 □ macOS version 3.1.5 □ Linux version 3.1.5

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

To update the version for the Collectors in a Collector Group:

1 Check the checkbox of the Collector Group(s) whose Collectors you want to update. You can select more than one Collector Group.

2 Select the checkbox of the operating system(s) to update and in its adjacent dropdown list, select the FortiEDR version for the Collectors in the designated Collector Group. You can select more than one operating system.



UPDATE COLLECTOR VERSION

☐	COLLECTOR GROUP ▲	WINDOWS VERSION	MACOS VERSION	LINUX VERSION
☐	Default Collector Group	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
☐	emulation	N/A	N/A	N/A
☐	group1	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
☐	group2	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
☐	High Security Collector Group	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
✓	Insiders	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
☐	Linux	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72

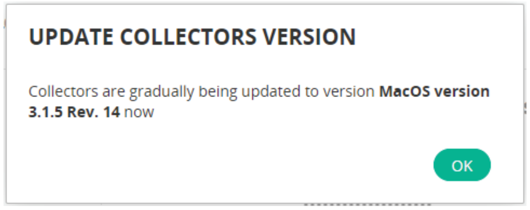
Update 1 selected groups to

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

✓ 3.1.5 Rev. 14

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

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



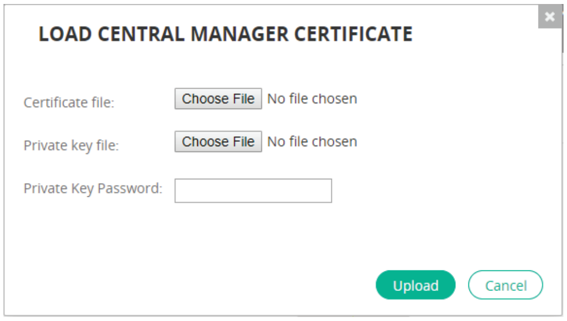
UPDATE COLLECTORS VERSION

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

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.



LOAD CENTRAL MANAGER CERTIFICATE

Certificate file: Choose File No file chosen

Private key file: Choose File No file chosen

Private Key Password:

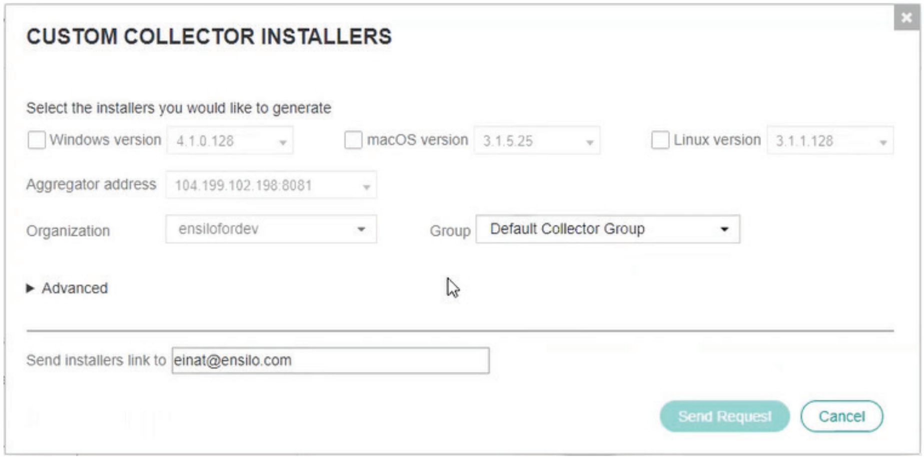
Requesting and Obtaining a Collector Installer

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 unzip it using the password provided in the email, double-click the installer and then follow the instructions to install a Collector based on the operating system on which it is to be installed, as described in the *Installing a FortiEDR Collector on Windows* section on page 35, the *Installing a FortiEDR Collector on an Mac Operating System* section on page 38 and the *Installing a FortiEDR Collector on Linux* section on page 45.

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:



CUSTOM COLLECTOR INSTALLERS

Select the installers you would like to generate

□ Windows version 4.1.0.128 □ macOS version 3.1.5.25 □ Linux version 3.1.1.128

Aggregator address 104.199.102.198:8081

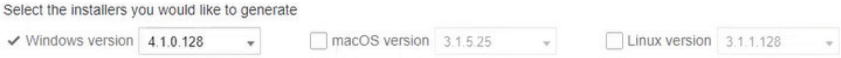
Organization ensilofordev Group Default Collector Group

▸ Advanced

Send installers link to einat@ensilo.com

Send Request Cancel

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



Select the installers you would like to generate

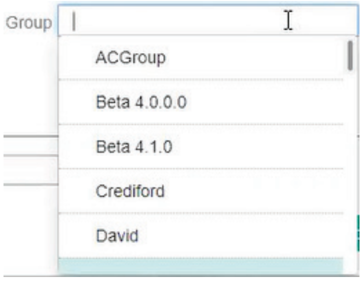
✓ Windows version 4.1.0.128 □ macOS version 3.1.5.25 □ Linux version 3.1.1.128

3 In the adjacent dropdown list, select the installer version. When selecting installers for more than one operating system, you must specify the version for each of them. Specify the version in the same manner as described on page 180.

4 In the **Aggregator Address** dropdown list, select the aggregator to which this Collector is registered.

5 In a multi-tenant system, select the organization to which the installed Collector is registered in the **Organization** dropdown list.

6 In the **Group** dropdown list, select the Collector Group to which the installed Collector is assigned, or leave the field empty for the Collector to be assigned to the default Collector Group.



Group

ACGroup

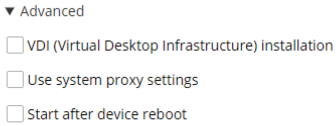
Beta 4.0.0.0

Beta 4.1.0

Crediford

David

7 In the Advanced area, specify the following:



▼ Advanced

□ VDI (Virtual Desktop Infrastructure) installation

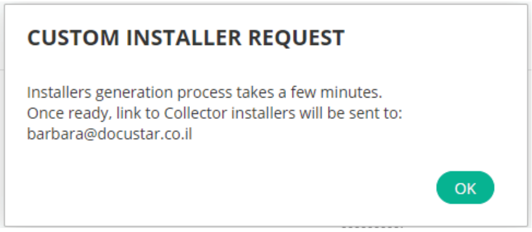
□ Use system proxy settings

□ Start after device reboot

- **VDI (Virtual Desktop Infrastructure) Installation:** If you are installing the Collector on a VDI environment, check this checkbox. For more details, you may refer to the *Working with FortiEDR on VDI Environments* section on page 47.
- **Use System Proxy Settings:** If you use a web proxy to filter requests in this device's network, then check the **Use System Proxy Settings** checkbox. Note that Windows must be configured to use a proxy and tunneling must be allowed from the Collector to the Aggregator on port 8081 and from the Collector to the Core on port 555. (Run as Administrator: **netsh winhttp set proxy <proxy IP >**).
- **Start After Device Reboot:** Check this checkbox in order to delay data collection until a device reboot is applied. This is only required in rare cases. Typically, this checkbox remains unchecked.

8 In the **Send Installers Link To** field, specify the email address to which the installer is to be sent.

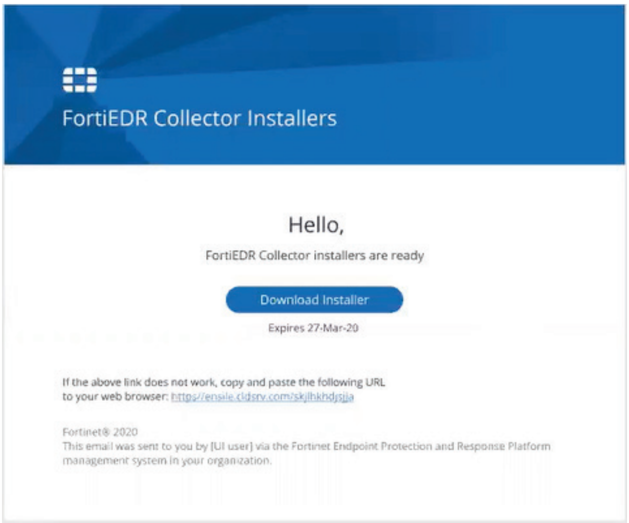
9 Click the Send Request button. A confirmation message displays.



CUSTOM INSTALLER REQUEST

Installers generation process takes a few minutes.
Once ready, link to Collector installers will be sent to:
barbara@docustar.co.il

10 Click **OK**. After the installer is generated by FortiEDR, it is emailed to the specified email address. Note that the link to download installers is only available for several hours. Be sure to download the installers within the required time period so that the link does not expire.



FortiEDR Collector Installers

Hello,

FortiEDR Collector installers are ready

Expires 27-Mar-20

If the above link does not work, copy and paste the following URL
to your web browser: https://ensile.cldsrv.com/skjlhkhdjsjja

Fortinet® 2020
This email was sent to you by [UI user] via the Fortinet Endpoint Protection and Response Platform management system in your organization.

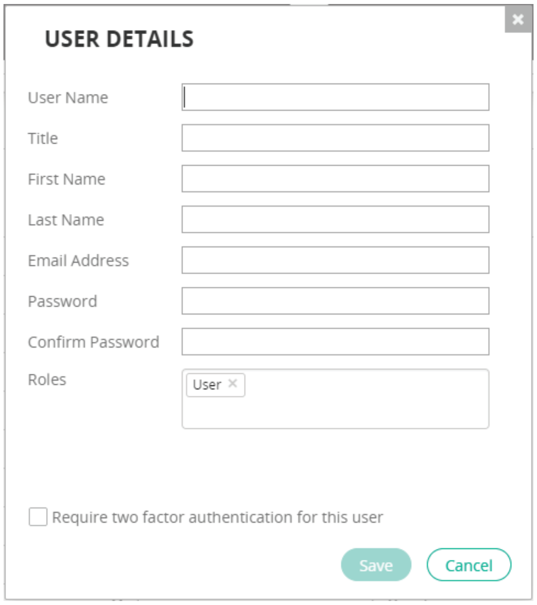
Users

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.



USER DETAILS

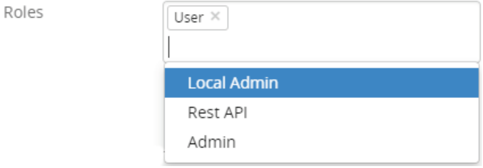
User Name	
Title	
First Name	
Last Name	
Email Address	
Password	
Confirm Password	
Roles	User ×

□ Require two factor authentication for this user

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 233.
- **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 security 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**.

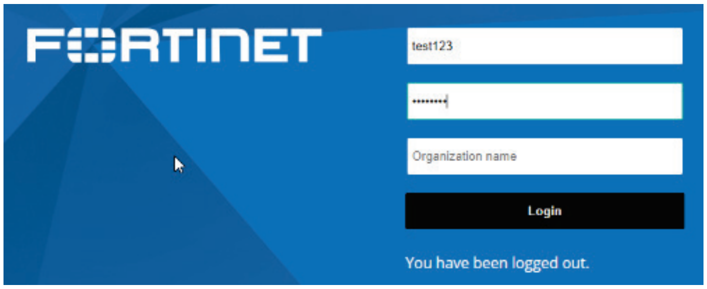
Two-factor Authentication

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 183.

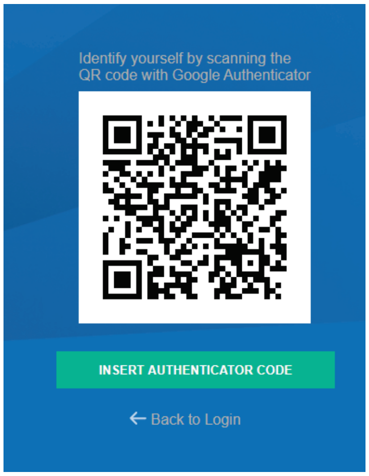
To log in using two-factor authentication (in this example we use the Google Authenticator app):

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.

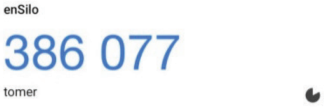


2 Enter the user name and password and click **LOGIN**.

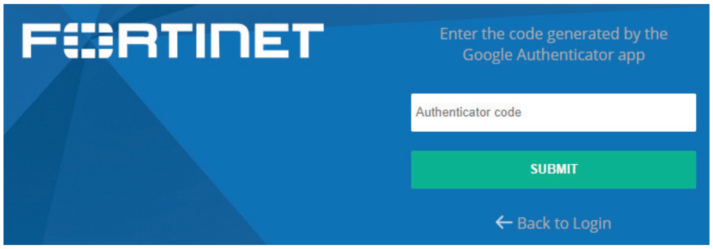
3 After clicking **LOGIN**, the user's identify must be verified using Google Authenticator. To do so, launch Google Authenticator by clicking the **Google Authenticator** icon on your mobile device. A QR code displays, as shown below:


Identify yourself by scanning the QR code with Google Authenticator
INSERT AUTHENTICATOR CODE
← Back to Login

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:



Enter the code generated by the Google Authenticator app

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.

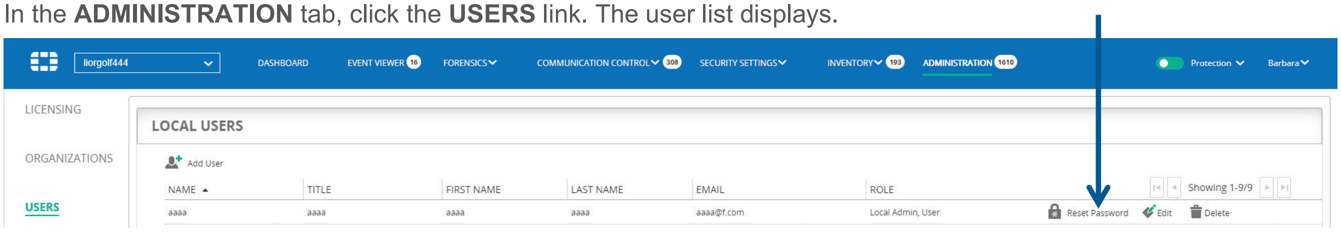
Resetting a User Password

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 184 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:

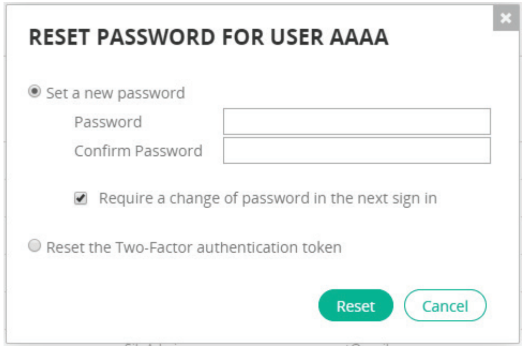
1 In the **ADMINISTRATION** tab, click the **USERS** link. The user list displays.



LOCAL USERS

NAME ▲	TITLE	FIRST NAME	LAST NAME	EMAIL	ROLE
aaaa	aaaa	aaaa	aaaa	aaaa@f.com	Local Admin, User

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



RESET PASSWORD FOR USER AAAA

● Set a new password

Password

Confirm Password

☑ Require a change of password in the next sign in

○ Reset the Two-Factor authentication token

3 Do one of the following:

- Click the **Set a New Password** radio button and define a new password for the user.
- For a user that must use two-factor authentication, click the **Reset the Two-Factor Authentication Token** radio button to force user identity verification using two-factor authentication during that user's next login. This means that the user must complete the *To log in using two-factor authentication* procedure described on page 184 in order to log in.

4 Click the **Reset** button.

LDAP Authentication

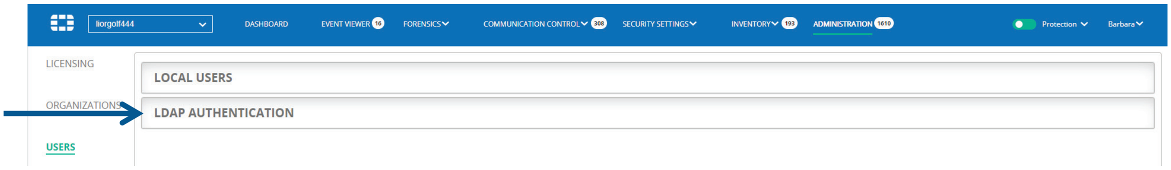
Lightweight Directory Access Protocol (LDAP) authentication is an open, industry-standard application protocol for accessing and maintaining distributed directory information services over an IP network. LDAP provides a central place to store usernames and passwords. This enables many different applications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

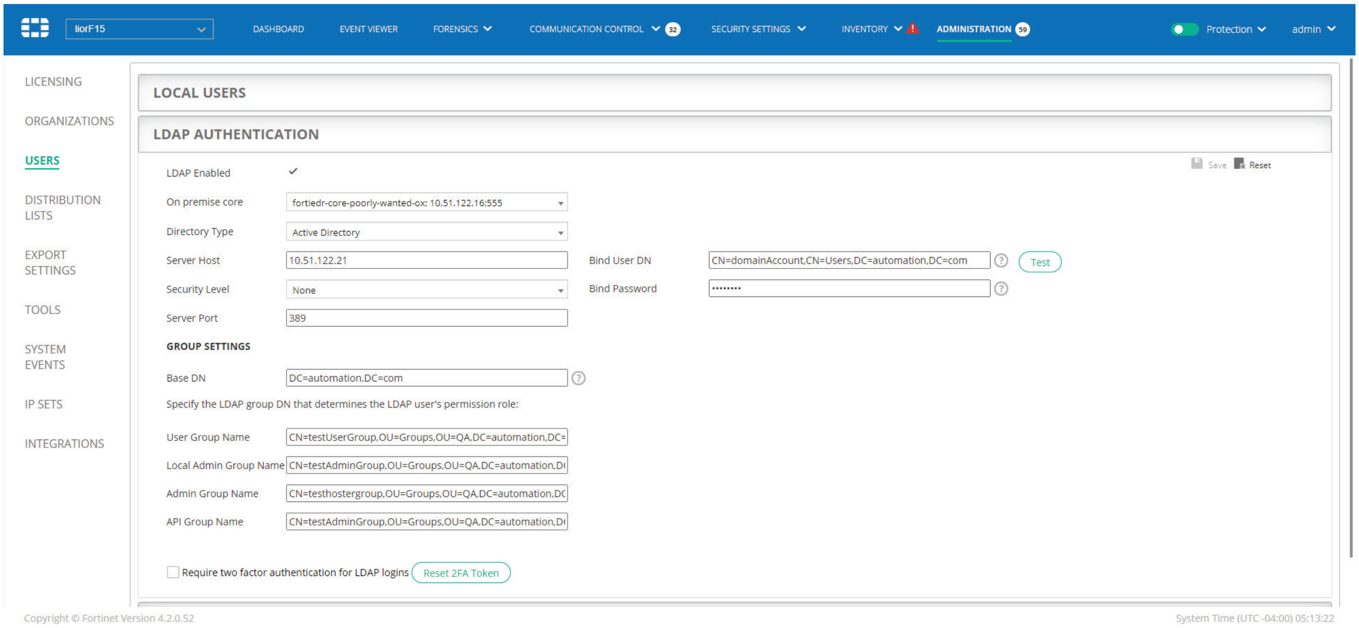
Before you start firewall configuration, make sure that your FortiEDR deployment includes an on-premise Core that has connectivity to the LDAP server. Details about how to install a FortiEDR on-premise Core can be found in *Installing the FortiEDR Core*.

To set up LDAP authentication in FortiEDR:

1 Click the LDAP AUTHENTICATION button.



The following window displays:



LDAP Enabled ✓

On premise core: fortiedr-core-poorly-wanted-ox: 10.51.122.16:555

Directory Type: Active Directory

Server Host: 10.51.122.21

Security Level: None

Server Port: 389

Bind User DN: CN=domainAccount,CN=Users,DC=automation,DC=com

Bind Password: ••••••••

GROUP SETTINGS

Base DN: DC=automation,DC=com

Specify the LDAP group DN that determines the LDAP user's permission role:

User Group Name: CN=testUserGroup,OU=Groups,OU=QA,DC=automation,DC=

Local Admin Group Name: CN=testAdminGroup,OU=Groups,OU=QA,DC=automation,D

Admin Group Name: CN=testhostergroup,OU=Groups,OU=QA,DC=automation,DC

API Group Name: CN=testAdminGroup,OU=Groups,OU=QA,DC=automation,D

☐ Require two factor authentication for LDAP logins

Copyright © Fortinet Version 4.2.0.52

System Time (UTC -04:00) 05:13:22

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 184.

   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 185.

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\, ".

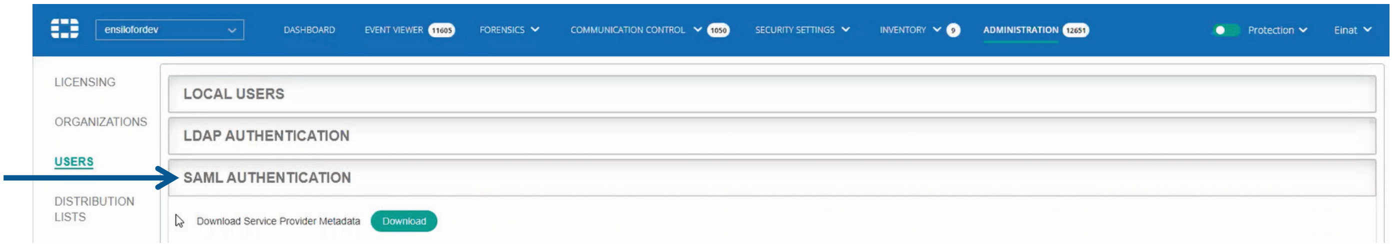
SAML Authentication

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).

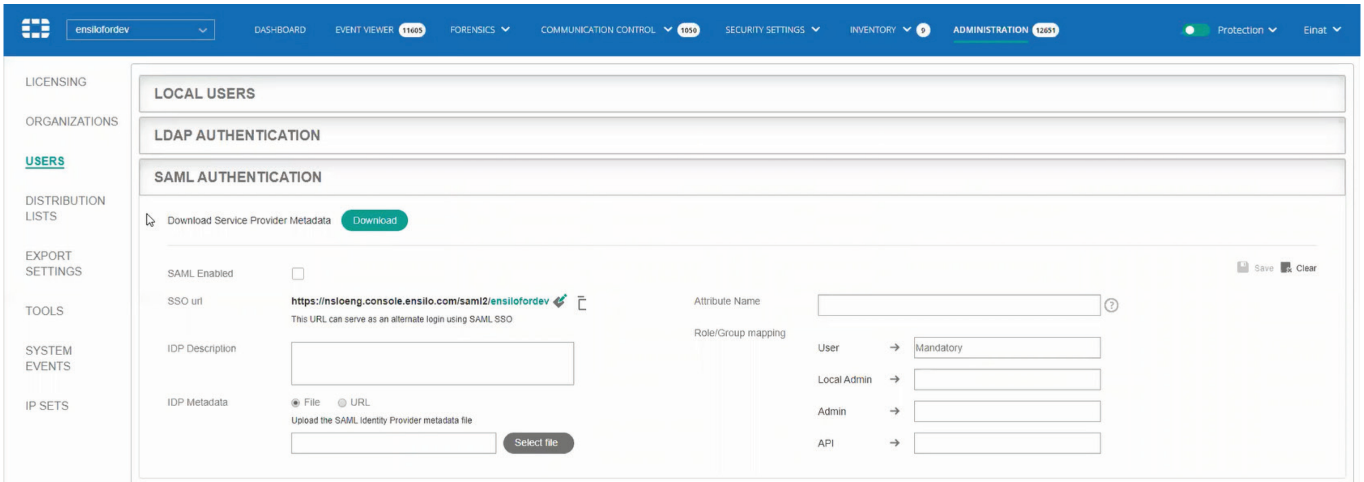
FortiEDR can act as an SP to authenticate users with a third-party IdP, enabling transparent user sign-in to the FortiEDR Central Manager Console.

To set up SAML authentication in FortiEDR:

1 Click the **SAML Authentication** button.



The following window displays:



SAML Enabled □

SSO url https://nsloeng.console.ensilo.com/saml2/ensilofordev

This URL can serve as an alternate login using SAML SSO

IDP Description

IDP Metadata ● File ○ URL

Upload the SAML Identity Provider metadata file

Attribute Name

Role/Group mapping

User → Mandatory

Local Admin →

Admin →

API →

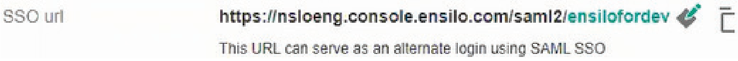
2 Click the **Download** button to download and save SP data from FortiEDR, which is used by your IdP server during SAML authentication. Then, upload this FortiEDR data as is to your IdP server using a standard method.

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).

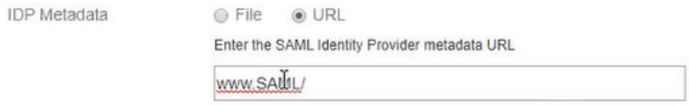


SSO url https://nsloeng.console.ensilo.com/saml2/ensilofordev

This URL can serve as an alternate login using SAML SSO

Make sure that the suffix does not include any spaces and is comprised of only letters, numbers and underscores

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



IDP Metadata ○ File ● URL

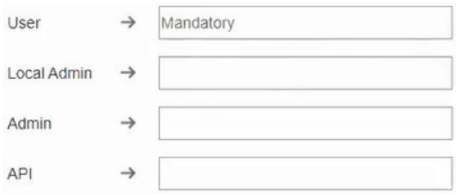
Enter the SAML Identity Provider metadata URL

www.SAML/

- **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.

Attribute Name: privileges

- **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.



User → Mandatory

Local Admin →

Admin →

API →

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**.

The examples below describe how the Azure, Okta or FortiAuthenticator SSO services can be used as an IdP that provides authorization and authentication for users attempting to access the FortiEDR Central Manager console. It demonstrates how to exchange metadata between the two entities, how to define group attributes and how to associate them with SAML users so that user permissions are dictated by the Group/Roles mapping in FortiEDR SAML configuration.

SAML IdP configuration with Azure

To configure general SAML IdP portal settings:

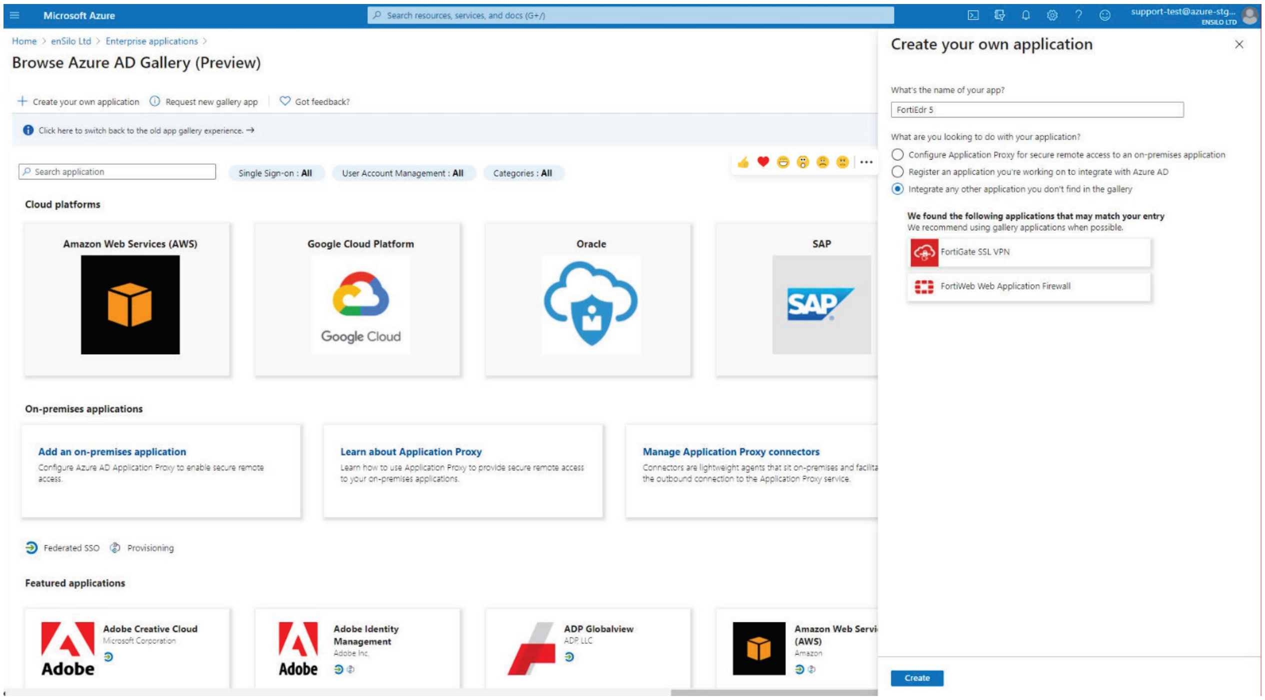
1 Before you start configuring SAML on Azure, download and save SP data from the FortiEDR SAML configuration page (fortiEDR.sp.metedata.id.1.xml), as described above on page 188.

2 Sign in to the Azure Dashboard.

3 In the Azure services, select and navigate to the Azure Active Directory.

4 From the left menu, select **Enterprise applications**.

5 Click **New Application** and then **Create your own application**. The following displays:



Create your own application

What's the name of your app?

FortiEdr 5

What are you looking to do with your application?

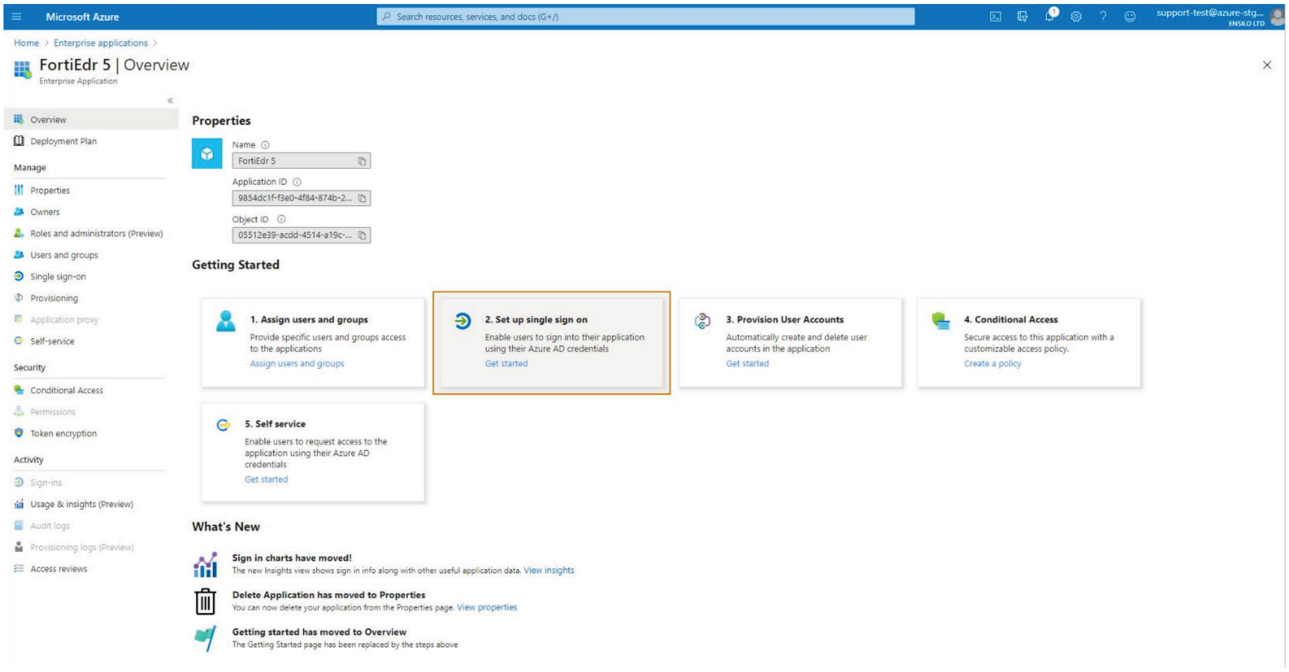
○ Configure Application Proxy for secure remote access to an on-premises application
○ Register an application you're working on to integrate with Azure AD
● Integrate any other application you don't find in the gallery

We found the following applications that may match your entry
We recommend using gallery applications when possible.

- FortiGate SSL VPN
- FortiWeb Web Application Firewall

Microsoft Azure
Search resources, services, and docs (G+/)
support-test@azure-stg...
ENSILO LTD
Home > enSilo Ltd > Enterprise applications >
Browse Azure AD Gallery (Preview)
Create your own application
Request new gallery app
Got feedback?
Click here to switch back to the old app gallery experience. →
Search application
Single Sign-on : All
User Account Management : All
Categories : All
Cloud platforms
Amazon Web Services (AWS)
Google Cloud Platform
Google Cloud
Oracle
SAP
On-premises applications
Add an on-premises application
Configure Azure AD Application Proxy to enable secure remote access.
Learn about Application Proxy
Learn how to use Application Proxy to provide secure remote access to your on-premises applications.
Manage Application Proxy connectors
Connectors are lightweight agents that sit on-premises and facilita the outbound connection to the Application Proxy service.
Federated SSO
Provisioning
Featured applications
Adobe Creative Cloud
Microsoft Corporation
Adobe Identity Management
Adobe Inc.
ADP Globalview
ADP LLC
Amazon Web Servi (AWS)
Amazon
Adobe
Create

6 Leave the default and click **Create**. The following displays:



FortiEdr 5 | Overview
Enterprise Application

Properties

Name: FortiEdr 5
Application ID: 9854dc1f-f3e0-4f84-874b-2...
Object ID: 05512e39-acdd-4514-a19c-...

Getting Started

1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

2. Set up single sign on
Enable users to sign into their application using their Azure AD credentials
Get started

3. Provision User Accounts
Automatically create and delete user accounts in the application
Get started

4. Conditional Access
Secure access to this application with a customizable access policy.
Create a policy

5. Self service
Enable users to request access to the application using their Azure AD credentials
Get started

What's New

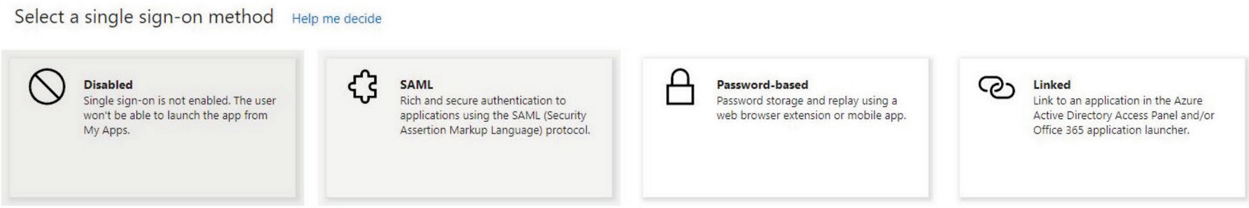
Sign in charts have moved!
The new Insights view shows sign in info along with other useful application data. View insights

Delete Application has moved to Properties
You can now delete your application from the Properties page. View properties

Getting started has moved to Overview
The Getting Started page has been replaced by the steps above

7 Click **Assign users and groups** and configure which users and groups to be provided with access to the FortiEDR application.

8 Click **Set up single sign on**. The following displays:



Select a single sign-on method Help me decide

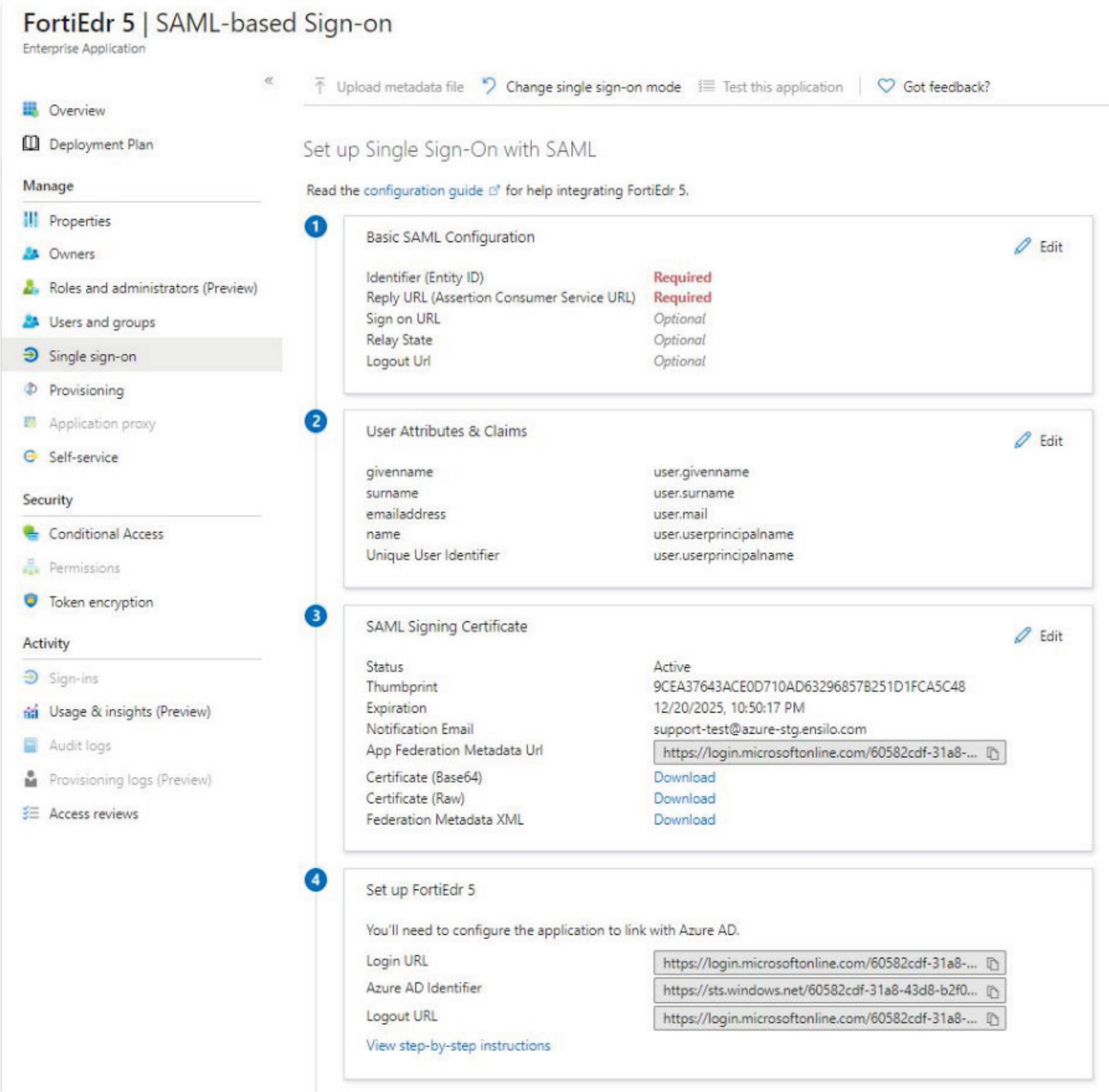
Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Password-based
Password storage and replay using a web browser extension or mobile app.

Linked
Link to an application in the Azure Active Directory Access Panel and/or Office 365 application launcher.

9 Click **SAML**. The following displays:



FortiEdr 5 | SAML-based Sign-on

Set up Single Sign-On with SAML

Read the configuration guide for help integrating FortiEdr 5.

1 Basic SAML Configuration

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Optional
Relay State	Optional
Logout Url	Optional

2 User Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

3 SAML Signing Certificate

Status	Active
Thumbprint	9CEA37643ACE0D710AD63296857B251D1FCA5C48
Expiration	12/20/2025, 10:50:17 PM
Notification Email	support-test@azure-stg.ensilo.com
App Federation Metadata Url	https://login.microsoftonline.com/60582cdf-31a8-...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

4 Set up FortiEdr 5

You'll need to configure the application to link with Azure AD.

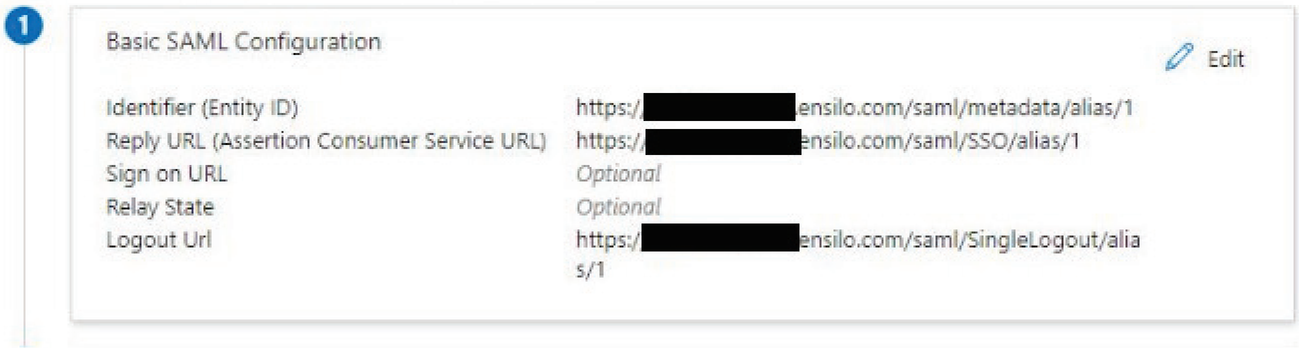
Login URL	https://login.microsoftonline.com/60582cdf-31a8-...
Azure AD Identifier	https://sts.windows.net/60582cdf-31a8-43d8-b2f0...
Logout URL	https://login.microsoftonline.com/60582cdf-31a8-...

View step-by-step instructions

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

11 Click **Upload metadata file** and browse in order to select the FortiEDR SP metadata file (fortiEDR.sp.metedata.id.1.xml) that was downloaded from FortiEDR SAML configuration page (as described on page 188). Alternatively, you can manually copy entityID and the Reply URL values from FortiEDR metadata file and paste it to the relevant input text boxes.

12 Click **Save**. The required SAML Configuration fields displays populated with details, as shown below:

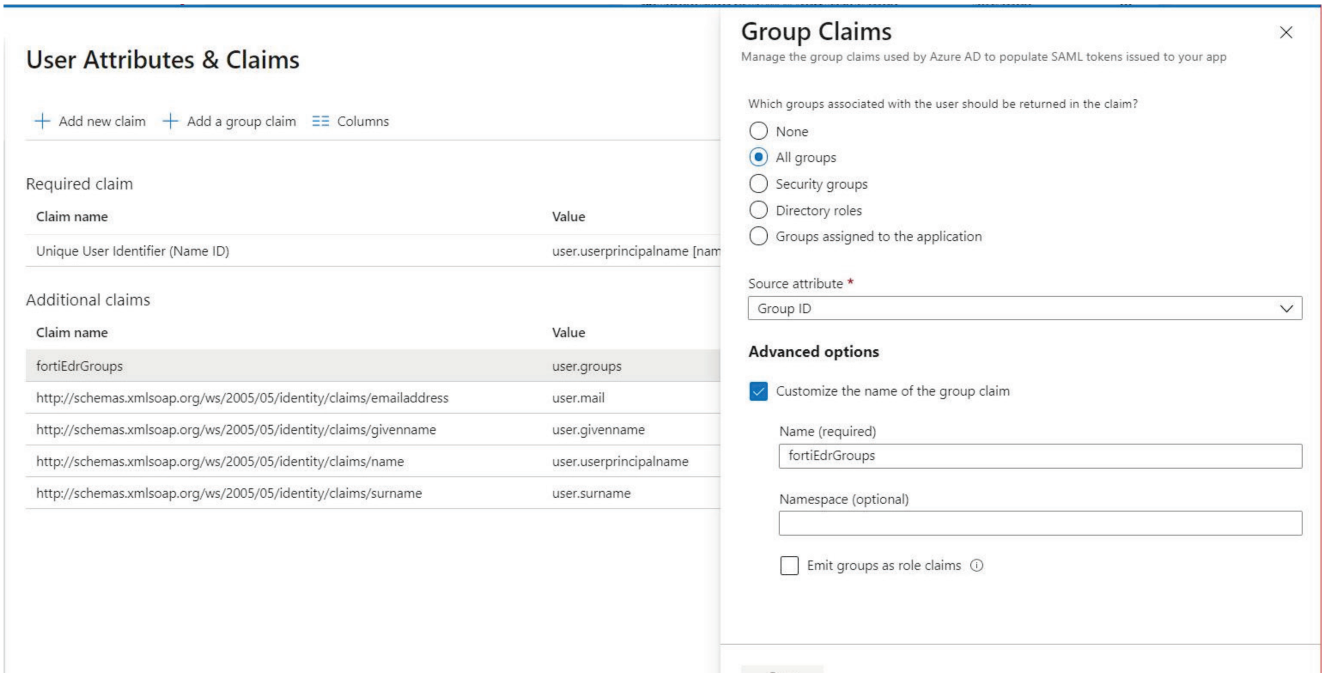


Basic SAML Configuration

Identifier (Entity ID)	https:/[redacted]ensilo.com/saml/metadata/alias/1
Reply URL (Assertion Consumer Service URL)	https:/[redacted]ensilo.com/saml/SSO/alias/1
Sign on URL	*Optional*
Relay State	*Optional*
Logout Url	https:/[redacted]ensilo.com/saml/SingleLogout/alias/1

13 Click **Edit** in the User Attributes & Claims box.

14 In the User Attributes & Claims window, click **Add a group claim**. The following window displays:



User Attributes & Claims

Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nam

Additional claims

Claim name	Value
fortiEdrGroups	user.groups
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname

Group Claims

Manage the group claims used by Azure AD to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

○ None
● All groups
○ Security groups
○ Directory roles
○ Groups assigned to the application

Source attribute *: Group ID

Advanced options

☑ Customize the name of the group claim

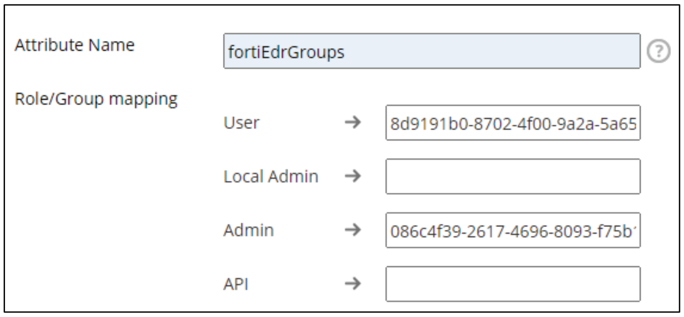
Name (required): fortiEdrGroups

Namespace (optional):

□ Emit groups as role claims ⓘ

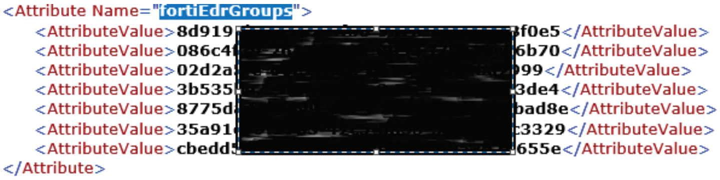
15 Select the groups to be added to the claim sent to the FortiEDR application. These specific groups should be specified in the Role/Group mapping on the SAML configuration page of the FortiEDR console in order to determine the permissions of the signed in user.

16 Check the **Customize the name of the group claim** checkbox, and in the **Name** field, enter the Attribute Name that was specified on the SAML configuration page of the FortiEDR console. In our example, it is **fortiEdrGroups**, as shown below:



Attribute Name	fortiEdrGroups	
Role/Group mapping		
	User →	8d9191b0-8702-4f00-9a2a-5a65
	Local Admin →	
	Admin →	086c4f39-2617-4696-8093-f75b
	API →	

17 Click **Save.** The newly defined attribute should now be included in the assertion, such as in the following example:



```
<Attribute Name="fortiEdrGroups">
    <AttributeValue>8d919[redacted]3f0e5</AttributeValue>
    <AttributeValue>086c4[redacted]6b70</AttributeValue>
    <AttributeValue>02d2a[redacted]99</AttributeValue>
    <AttributeValue>3b535[redacted]3de4</AttributeValue>
    <AttributeValue>8775d[redacted]bad8e</AttributeValue>
    <AttributeValue>35a91[redacted]3329</AttributeValue>
    <AttributeValue>cbedd[redacted]655e</AttributeValue>
</Attribute>
```

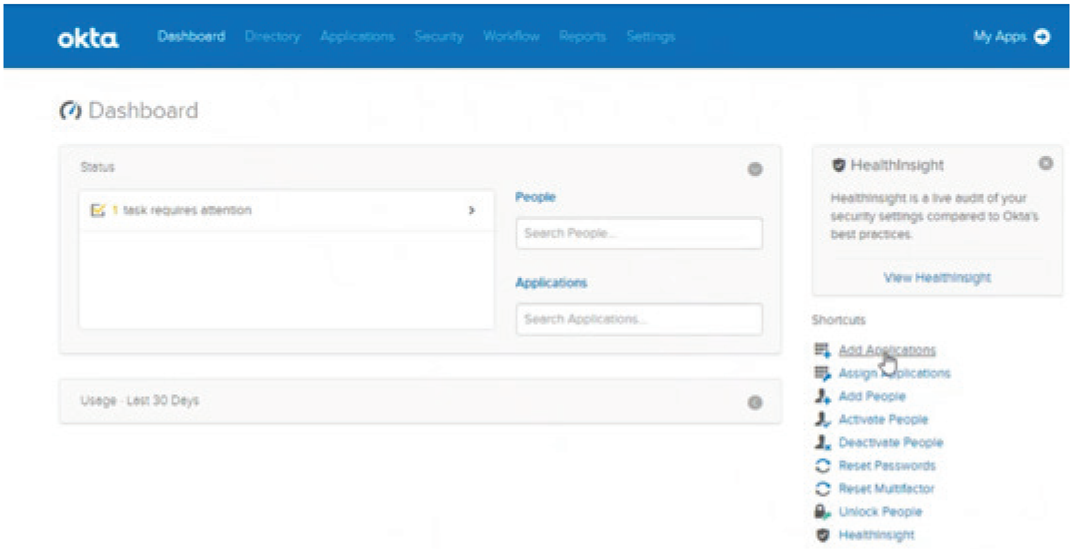
Azure can now be used as an IdP that awards authorization and authentication to users trying to access the FortiEDR Central Manager console. When logging into the FortiEDR console via an SSO URL that is specified under the SAML settings page, an Azure user is awarded access rights to the FortiEDR Central Manager according to the User Groups to which that user was added in Azure.

SAML IdP Configuration with Okta

To configure general SAML IdP portal settings:

1 Before starting to configure SAML on Okta, you must download and save SP data from the FortiEDR SAML configuration page (fortiEDR.sp.metedata.id.1.xml), as described above on page 188.

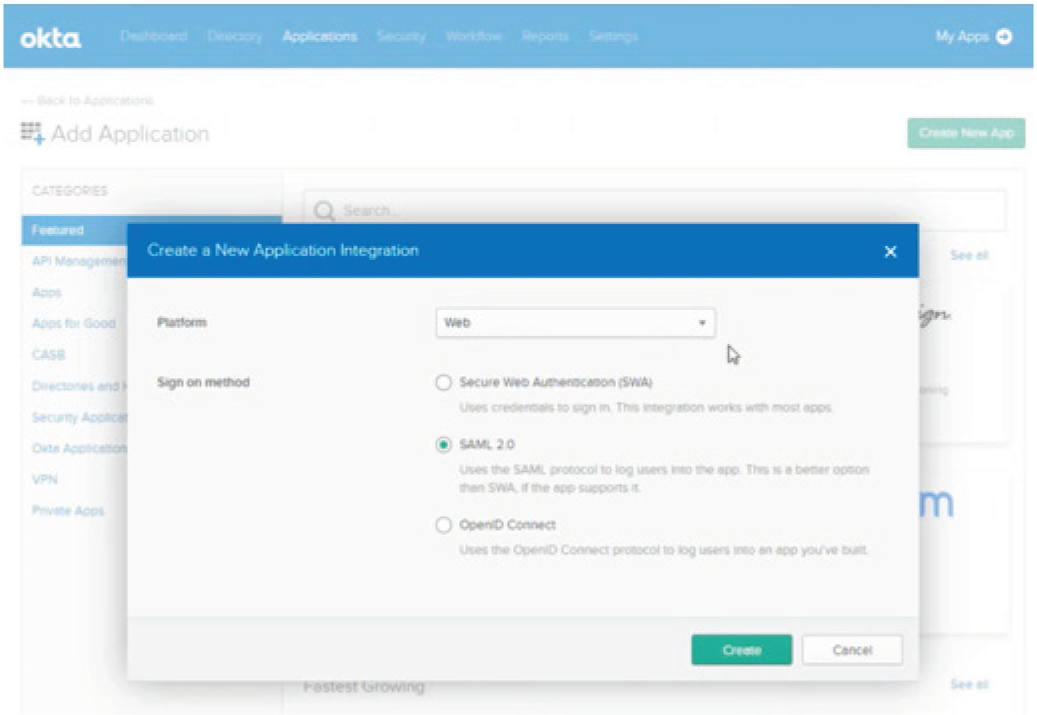
2 Sign in to the Okta Admin Dashboard. The following displays:



HealthInsight is a live audit of your security settings compared to Okta's best practices.

3 In your Okta org, click **Applications** and then **Add Applications**.

4 Click **Create New App** . The following displays:



Create a New Application Integration

Platform: Web

Sign on method

○ Secure Web Authentication (SWA)
Uses credentials to sign in. This integration works with most apps.

● SAML 2.0
Uses the SAML protocol to log users into the app. This is a better option than SWA, if the app supports it.

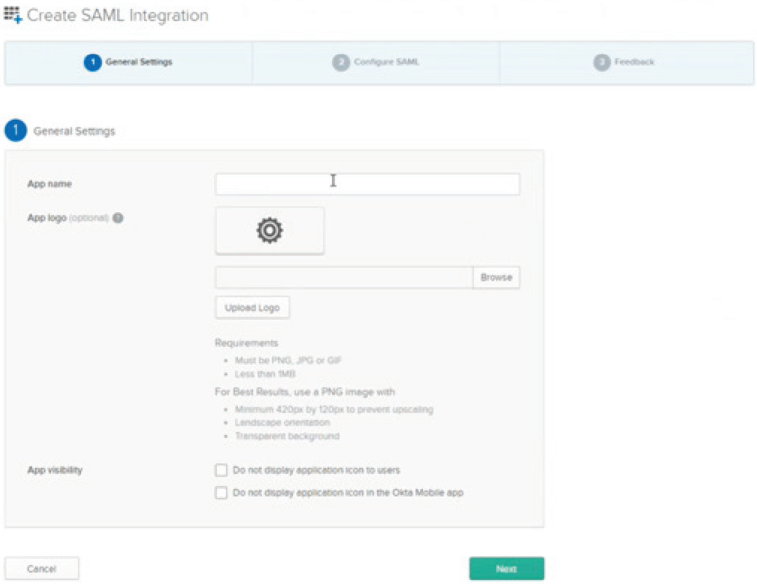
○ OpenID Connect
Uses the OpenID Connect protocol to log users into an app you've built.

5 In the **Platform** field, select **Web**.

6 In the **Sign on method** field, select **SAML 2.0**.

7 Click **Create**.

8 In the **General Settings** page, select a name for the application. For example, FortiEDRConsole. Optionally, you can also add the FortiEDR logo here.



1 General Settings

App name

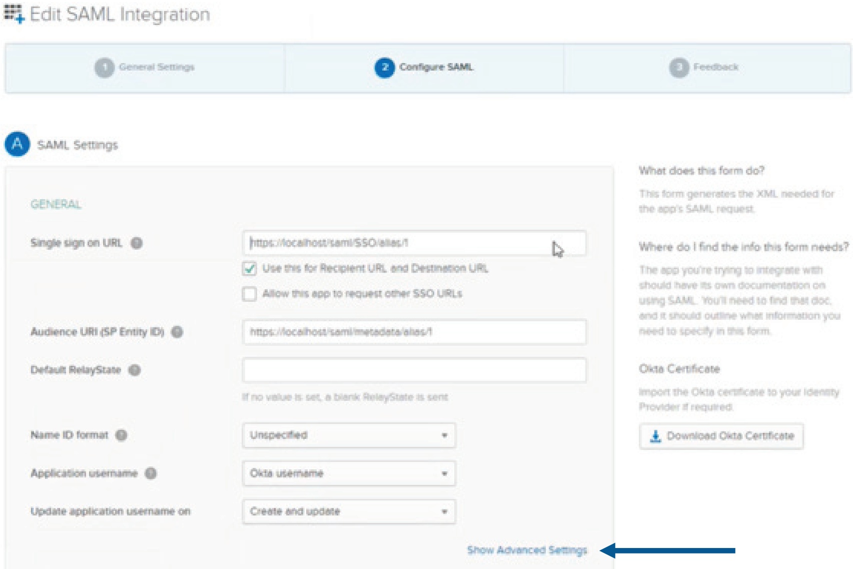
App logo (optional)

Requirements
- Must be PNG, JPG or GIF
- Less than 1MB

For Best Results, use a PNG image with
- Minimum 420px by 120px to prevent upscaling
- Landscape orientation
- Transparent background

App visibility
□ Do not display application icon to users
□ Do not display application icon in the Okta Mobile app

9 Click **Next**. The Configure SAML page displays –



Edit SAML Integration

A SAML Settings

GENERAL

Single sign on URL: https://localhost/saml/SSO/alias/1

☑ Use this for Recipient URL and Destination URL

□ Allow this app to request other SSO URLs

Audience URI (SP Entity ID): https://localhost/saml/metadata/alias/1

Default RelayState:

If no value is set, a blank RelayState is sent

Name ID format: Unspecified

Application username: Okta username

Update application username on: Create and update

What does this form do?

This form generates the XML needed for the app's SAML request.

Where do I find the info this form needs?

The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

Okta Certificate

Import the Okta certificate to your Identity Provider if required.

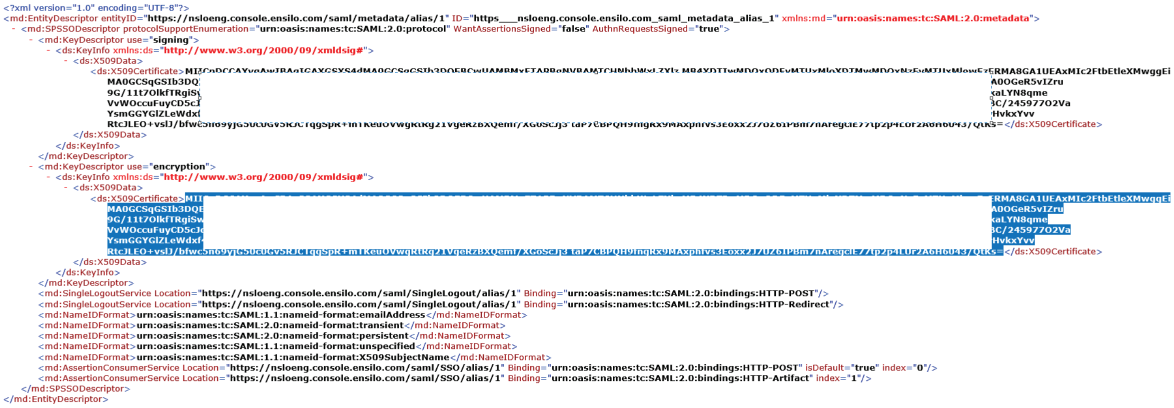
10 Copy the following values that are taken from the FortiEDR SP metadata file (fortiEDR.sp.metedata.id.1.xml) that was downloaded from FortiEDR SAML configuration page (as described on page 188):

- **Single sign on URL:** Under the 'md:AssertionConsumerService' tag, in the **Location** attribute (For example, https:// nsloeng.console.ensilo.com/saml/SSO/alias/1).
- **Audience URI (SP entity ID):** Under the 'md:EntityDescriptor' tag, in the 'entityID' attribute (For example, https://nsloeng.console.ensilo.com/saml/metadata/alias/1).

11 In **Advanced Settings** (shown above), in the **Assertion Encryption** field, select **Encrypted.**

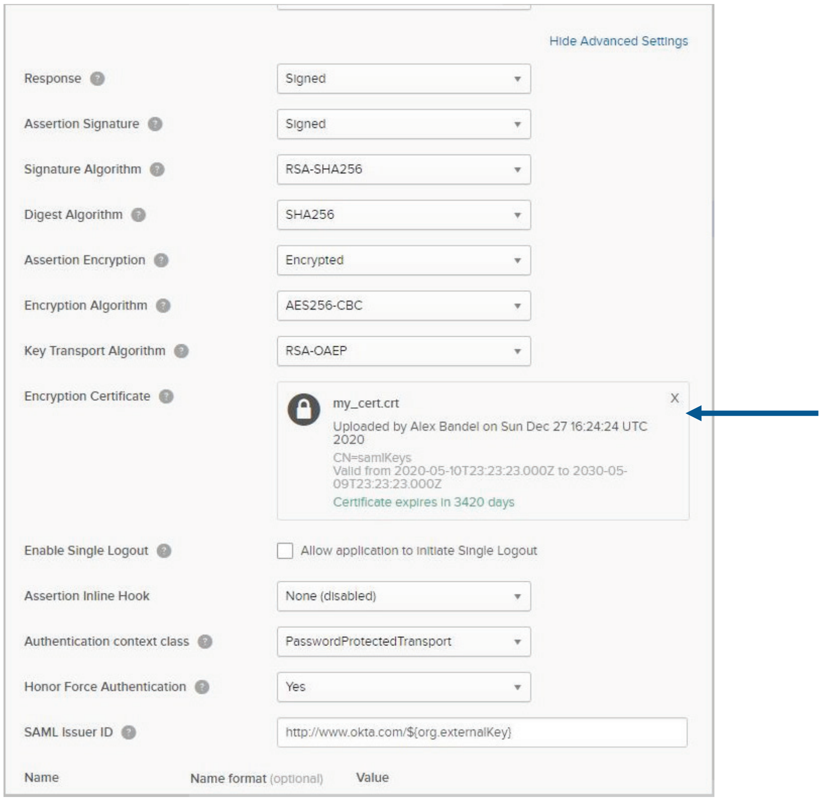
12 Use Notepad or another text editor to copy the entire attribute <ds:X509Certificate>XXX </ds:X509Certificate> from the FortiEDR SP metadata file (fortiEDR.sp.metedata.id.1.xml) that was downloaded from FortiEDR SAML configuration page. Then, save this attribute as a .crt file to be used as a certificate.

13 Upload this .crt file to the Encryption Certificate box on Okta, as shown below:



```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor entityID="https://nsloeng.console.ensilo.com/saml/metadata/alias/1" ID="https___nsloeng.console.ensilo.com_saml_metadata_alias_1" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
 - <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="false" AuthnRequestsSigned="true">
   - <md:KeyDescriptor use="signing">
     - <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
       - <ds:X509Data>
           <ds:X509Certificate>MI[redacted]ERMA8GA1UEAxMIc2FtbEtleXMwggEi
             MA0GCSqGSIb3DQ                                         A0OGeR5vIZru
             9G/11t7OlkfTRgiS                                       kaLYN8qme
             VvWOccuFuyCD5cJ                                        3C/24597702Va
             YsmGGYGlZLeWdx                                         HvkxYvv
             RtcJLEO+vslJ/bfw                                       =</ds:X509Certificate>
         </ds:X509Data>
       </ds:KeyInfo>
     </md:KeyDescriptor>
   - <md:KeyDescriptor use="encryption">
     - <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
       - <ds:X509Data>
           <ds:X509Certificate>MII[redacted]ERMA8GA1UEAxMIc2FtbEtleXMwggEi
             MA0GCSqGSIb3DQE                                        A0OGeR5vIZru
             9G/11t7OlkfTRgiSw                                      kaLYN8qme
             VvWOccuFuyCD5cJ                                        3C/24597702Va
             YsmGGYGlZLeWdxf                                        HvkxYvv
             RtcJLEO+vslJ/bfw                                       =</ds:X509Certificate>
         </ds:X509Data>
       </ds:KeyInfo>
     </md:KeyDescriptor>
     <md:SingleLogoutService Location="https://nsloeng.console.ensilo.com/saml/SingleLogout/alias/1" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
     <md:SingleLogoutService Location="https://nsloeng.console.ensilo.com/saml/SingleLogout/alias/1" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"/>
     <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
     <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
     <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat>
     <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>
     <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName</md:NameIDFormat>
     <md:AssertionConsumerService Location="https://nsloeng.console.ensilo.com/saml/SSO/alias/1" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" isDefault="true" index="0"/>
     <md:AssertionConsumerService Location="https://nsloeng.console.ensilo.com/saml/SSO/alias/1" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" index="1"/>
   </md:SPSSODescriptor>
</md:EntityDescriptor>
```

14 Leave the default values in the rest of the settings. For example, as shown below:

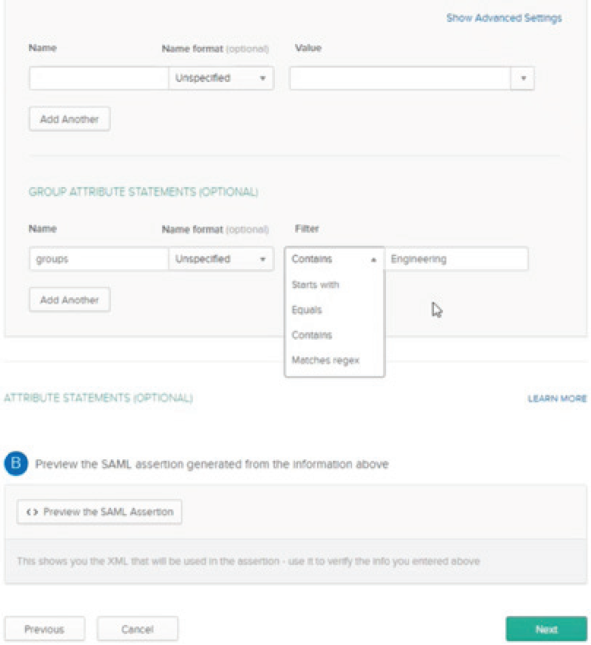


Hide Advanced Settings

Response	Signed
Assertion Signature	Signed
Signature Algorithm	RSA-SHA256
Digest Algorithm	SHA256
Assertion Encryption	Encrypted
Encryption Algorithm	AES256-CBC
Key Transport Algorithm	RSA-OAEP
Encryption Certificate	my_cert.crt Uploaded by Alex Bandel on Sun Dec 27 16:24:24 UTC 2020 CN=samlKeys Valid from 2020-05-10T23:23:23.000Z to 2030-05-09T23:23:23.000Z Certificate expires in 3420 days
Enable Single Logout	□ Allow application to initiate Single Logout
Assertion Inline Hook	None (disabled)
Authentication context class	PasswordProtectedTransport
Honor Force Authentication	Yes
SAML Issuer ID	http://www.okta.com/${org.externalKey}

Name Name format (optional) Value

15 Groups will be used in the assertion so that FortiEDR roles will be assigned according to the current groups in the Okta directory. For example, to assign the **Okta Engineering** group to have Admin roles on FortiEDR, add it to Okta as follows:



Show Advanced Settings

Name	Name format (optional)	Value
	Unspecified	

Add Another

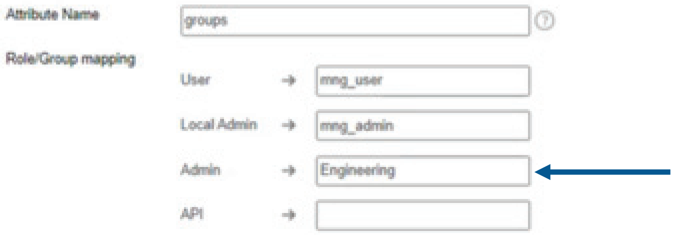
GROUP ATTRIBUTE STATEMENTS (OPTIONAL)

Name	Name format (optional)	Filter	
groups	Unspecified	Contains	Engineering

B Preview the SAML assertion generated from the information above

This shows you the XML that will be used in the assertion - use it to verify the info you entered above

The mapping of this group to the FortiEDR Admin role is then performed in the SAML settings page of the FortiEDR Central Manager console as follows:

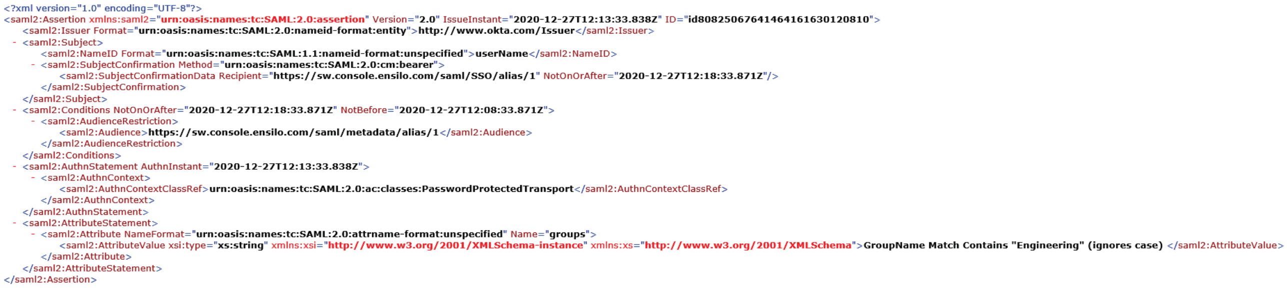


Attribute Name: groups

Role/Group mapping

User	→	mng_user
Local Admin	→	mng_admin
Admin	→	Engineering
API	→	

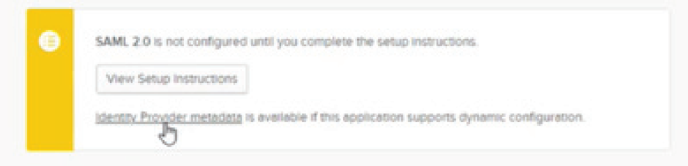
16 Previewing the assertion should appear similar to the following example:



```
<?xml version="1.0" encoding="UTF-8"?>
<saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" Version="2.0" IssueInstant="2020-12-27T12:13:33.838Z" ID="id8082506764146416163012081O">
    <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">http://www.okta.com/Issuer</saml2:Issuer>
  - <saml2:Subject>
        <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">userName</saml2:NameID>
      - <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml2:SubjectConfirmationData Recipient="https://sw.console.ensilo.com/saml/SSO/alias/1" NotOnOrAfter="2020-12-27T12:18:33.871Z"/>
        </saml2:SubjectConfirmation>
    </saml2:Subject>
  - <saml2:Conditions NotOnOrAfter="2020-12-27T12:18:33.871Z" NotBefore="2020-12-27T12:08:33.871Z">
      - <saml2:AudienceRestriction>
            <saml2:Audience>https://sw.console.ensilo.com/saml/metadata/alias/1</saml2:Audience>
        </saml2:AudienceRestriction>
    </saml2:Conditions>
  - <saml2:AuthnStatement AuthnInstant="2020-12-27T12:13:33.838Z">
      - <saml2:AuthnContext>
            <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml2:AuthnContextClassRef>
        </saml2:AuthnContext>
    </saml2:AuthnStatement>
  - <saml2:AttributeStatement>
      - <saml2:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified" Name="groups">
            <saml2:AttributeValue xsi:type="xs:string" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xs="http://www.w3.org/2001/XMLSchema">GroupName Match Contains "Engineering" (ignores case) </saml2:AttributeValue>
        </saml2:Attribute>
    </saml2:AttributeStatement>
</saml2:Assertion>
```

17 Click **Next** and then click **Finish.**

18 When you configure SAML SSO on the FortiEDR console, use the URL for **Identity Provide Metadata** from the application Sign On settings in Okta, as shown below:

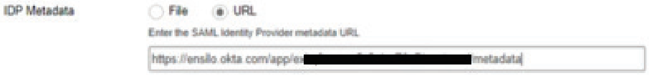


SAML 2.0 is not configured until you complete the setup instructions.

View Setup Instructions

Identity Provider metadata is available if this application supports dynamic configuration.

19 Paste it into the FortiEDR Central Manager as follows:



IDP Metadata ○ File ● URL

Enter the SAML Identity Provider metadata URL

https://ensilo.okta.com/app/ex[redacted]metadata

Okta can now be used as an IdP that awards authorization and authentication to users trying to access the FortiEDR Central Manager console. When logging into FortiEDR console via the SSO URL that is specified under the SAML settings page, an Okta user is awarded access rights to the FortiEDR Central Manager according to the User Groups to which that user was added in Okta.

SAML IdP Configuration with FortiAuthenticator

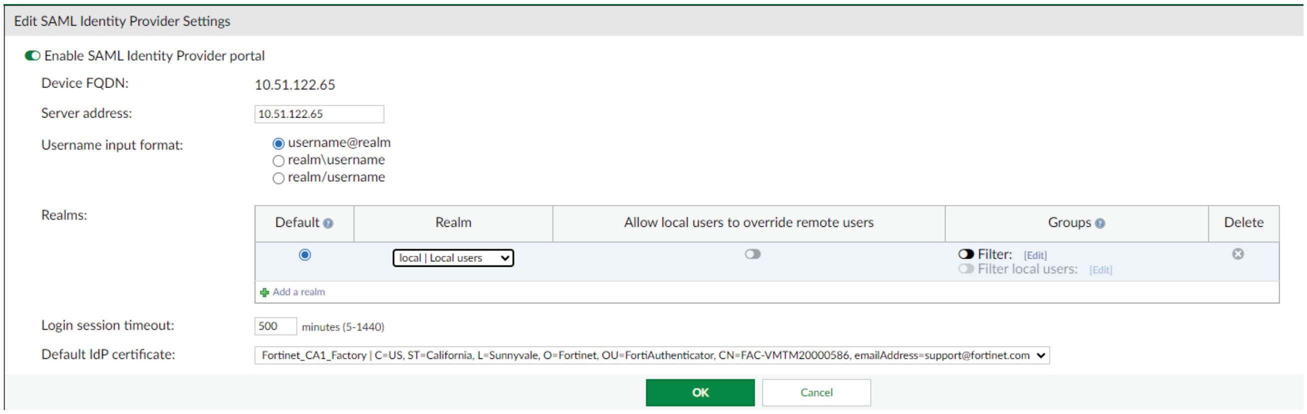
FortiAuthenticator configuration is comprised of the following steps:

1. Setting up FortiAuthenticator as an IdP.
2. Setting up user group management (if not configured already).
3. Setting up service provider settings for FortiEDR.

FortiAuthenticator IdP Configuration

To configure general SAML IdP portal settings:

1. Go to **Authentication ➔ SAML IdP ➔General** and select **Enable SAML Identity Provider portal**.
2. Configure the following settings:
   - **Device FQDN:** To configure this setting, you must enter a Device FQDN in the System Information widget in the Dashboard.
   - **Server address:** Enter the IP address or FQDN of the FortiAuthenticator device.
   - **Username input format:** Select one of the provided options. In our example, we used **username@realm**
   - **Realms:** Select **Add a realm** to add the default local realm to which the users will be associated.
   - **Login session timeout:** Set the user's login session timeout limit to between **5 – 1440** minutes (one day). In our example, we used **500** minutes.
   - **Default IdP certificate:** Select a default certificate the IdP uses to sign SAML assertions from the dropdown menu.



Edit SAML Identity Provider Settings

● Enable SAML Identity Provider portal

Device FQDN: 10.51.122.65

Server address: 10.51.122.65

Username input format:
● username@realm
○ realm\username
○ realm/username

Realms:

Default	Realm	Allow local users to override remote users	Groups	Delete
●	local | Local users	○	● Filter: [Edit] ○ Filter local users: [Edit]	⊗

Add a realm

Login session timeout: 500 minutes (5-1440)

Default IdP certificate: Fortinet_CA1_Factory | C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=FortiAuthenticator, CN=FAC-VMTM20000586, emailAddress=support@fortinet.com

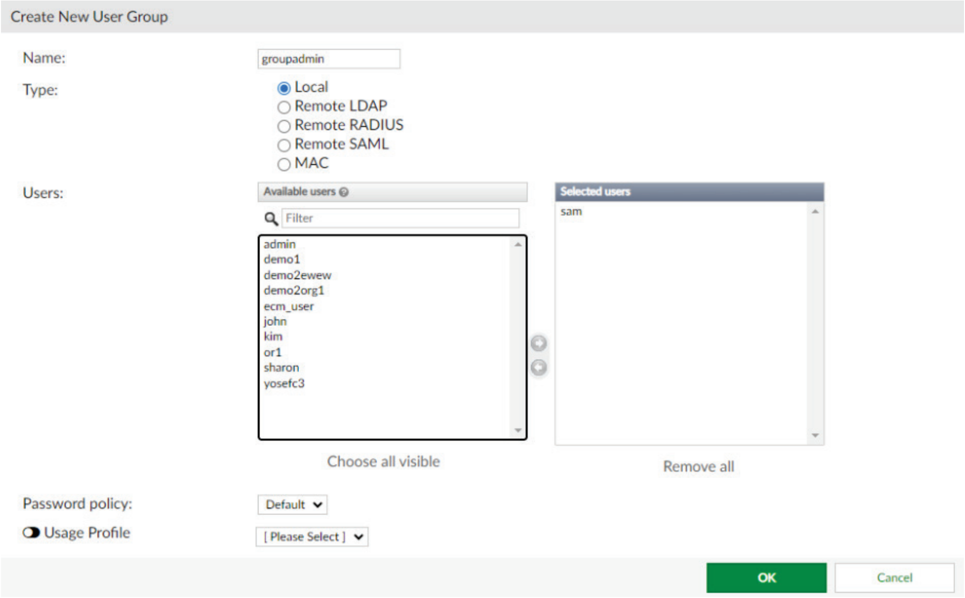
3. Click **OK** to apply these changes.

User Groups Management Settings on FortiAuthenticator

To configure on FortiAuthenticator the assertion attribute that will be used to map users' permissions to access FortiEDR:

1. Go to **Authentication ➔ User Management ➔ User Groups**.
2. Select **Create New**.
3. Specify a name for the group to be used for setting User access permissions for FortiEDR. In our example, we used **groupuser**.
4. In the **Users** section, select all the FortiAuthenticator users to be assigned with User permission to the FortiEDR Central Manager Console in order to add them to this User Group.
5. Click **OK** to save the configuration.
6. Repeat steps 1 – 5 above in order to also create Local Admin, Admin and API groups and in order to select the users to be assigned with these access permissions to the FortiEDR Central Manager Console.

In our example, we created a group named **groupadmin** and assigned this user the same Admin permissions to the FortiEDR Central Manager Console, as shown below:



Create New User Group

Name: groupadmin

Type:
● Local
○ Remote LDAP
○ Remote RADIUS
○ Remote SAML
○ MAC

Users:

Available users	Selected users
admin demo1 demo2ewew demo2org1 ecm_user john kim or1 sharon yosefc3	sam

Password policy: Default

Usage Profile: [Please Select]

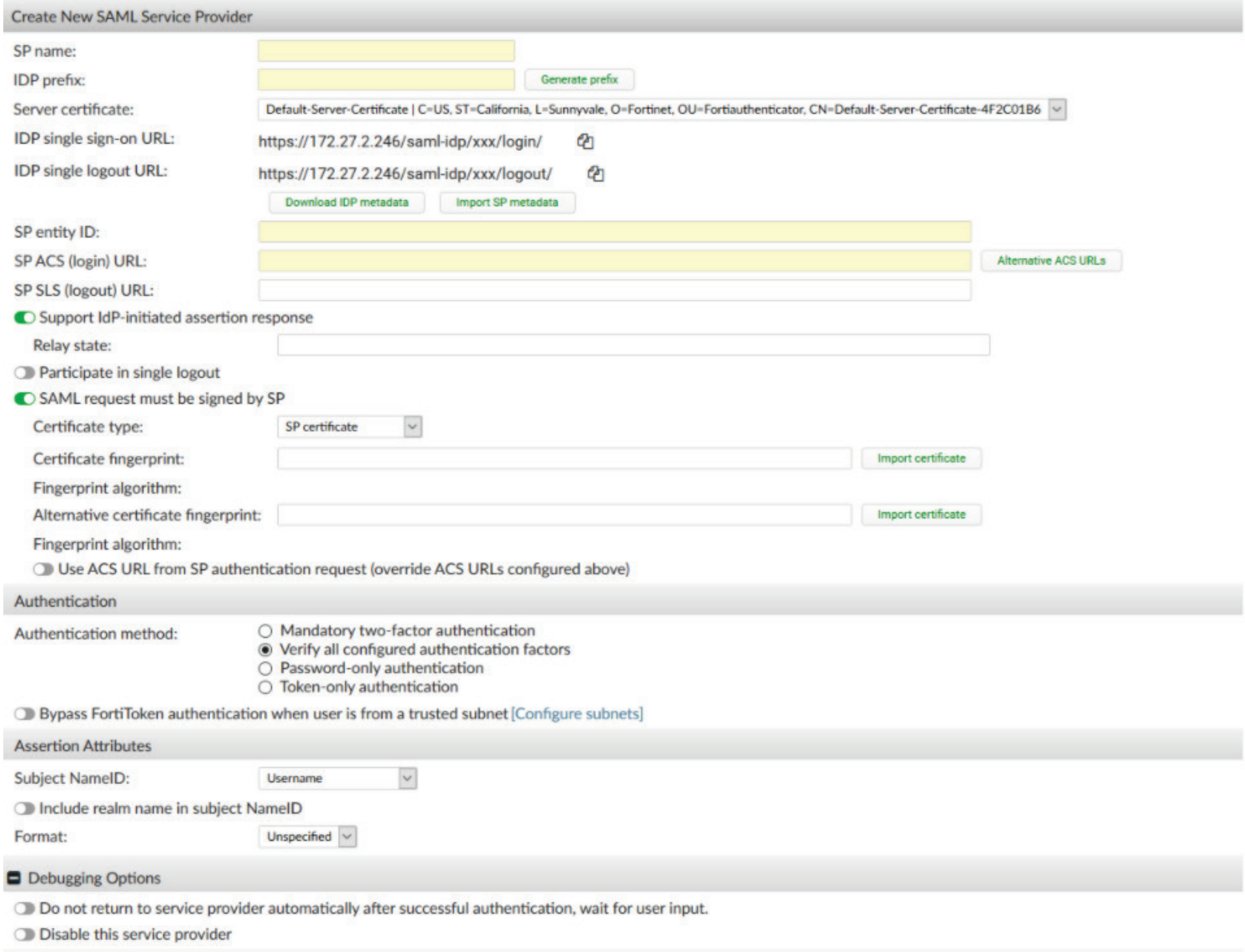
Note – New or existing FortiAuthenticator users can also be configured into groups on the Local Users create and edit page.

Service Provider Settings for FortiEDR on FortiAuthenticator

To configure FortiEDR as a SAML service provider on FortiAuthenticator:

1 Go to **Authentication ➔ SAML IdP ➔ Service Providers.**

2 Select **Create New.**



Create New SAML Service Provider

SP name:

IDP prefix: Generate prefix

Server certificate: Default-Server-Certificate | C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=Fortiauthenticator, CN=Default-Server-Certificate-4F2C01B6

IDP single sign-on URL: https://172.27.2.246/saml-idp/xxx/login/

IDP single logout URL: https://172.27.2.246/saml-idp/xxx/logout/

Download IDP metadata | Import SP metadata

SP entity ID:

SP ACS (login) URL: Alternative ACS URLs

SP SLS (logout) URL:

☑ Support IdP-initiated assertion response

Relay state:

☐ Participate in single logout

☑ SAML request must be signed by SP

Certificate type: SP certificate

Certificate fingerprint: Import certificate

Fingerprint algorithm:

Alternative certificate fingerprint: Import certificate

Fingerprint algorithm:

☐ Use ACS URL from SP authentication request (override ACS URLs configured above)

Authentication

Authentication method:

○ Mandatory two-factor authentication
● Verify all configured authentication factors
○ Password-only authentication
○ Token-only authentication

☐ Bypass FortiToken authentication when user is from a trusted subnet [Configure subnets]

Assertion Attributes

Subject NameID: Username

☐ Include realm name in subject NameID

Format: Unspecified

Debugging Options

☐ Do not return to service provider automatically after successful authentication, wait for user input.

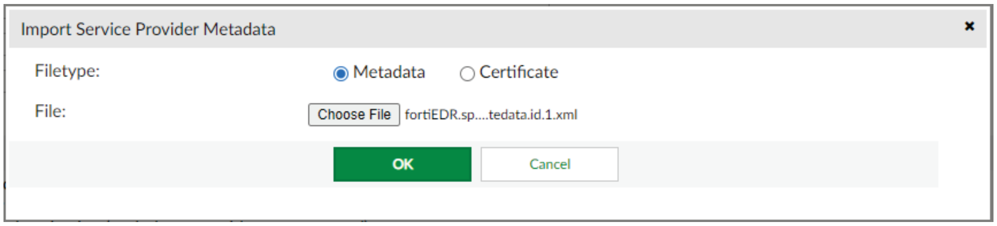
☐ Disable this service provider

3 Fill in the following fields:

- **SP name:** Enter a name for the FortiEDR SP.
- **IDP prefix:** Select **Generate prefix** in order to generate a random 16-digit alphanumeric string or alternatively enter a prefix for the IDP that is appended to the end of the IDP URLs.

4 Click **Download IDP metadata** to save the FortiAuthenticator IDP data file to be used for uploading into FortiEDR. You may refer to step 3 in the *To set up SAML authentication in FortiEDR* procedure on page 188 for more information.

5 Click **Import SP metadata** and select the SP data file that was downloaded from FortiEDR. You may refer to step 2 in the *To set up SAML authentication in FortiEDR* procedure on page 188 for more information.

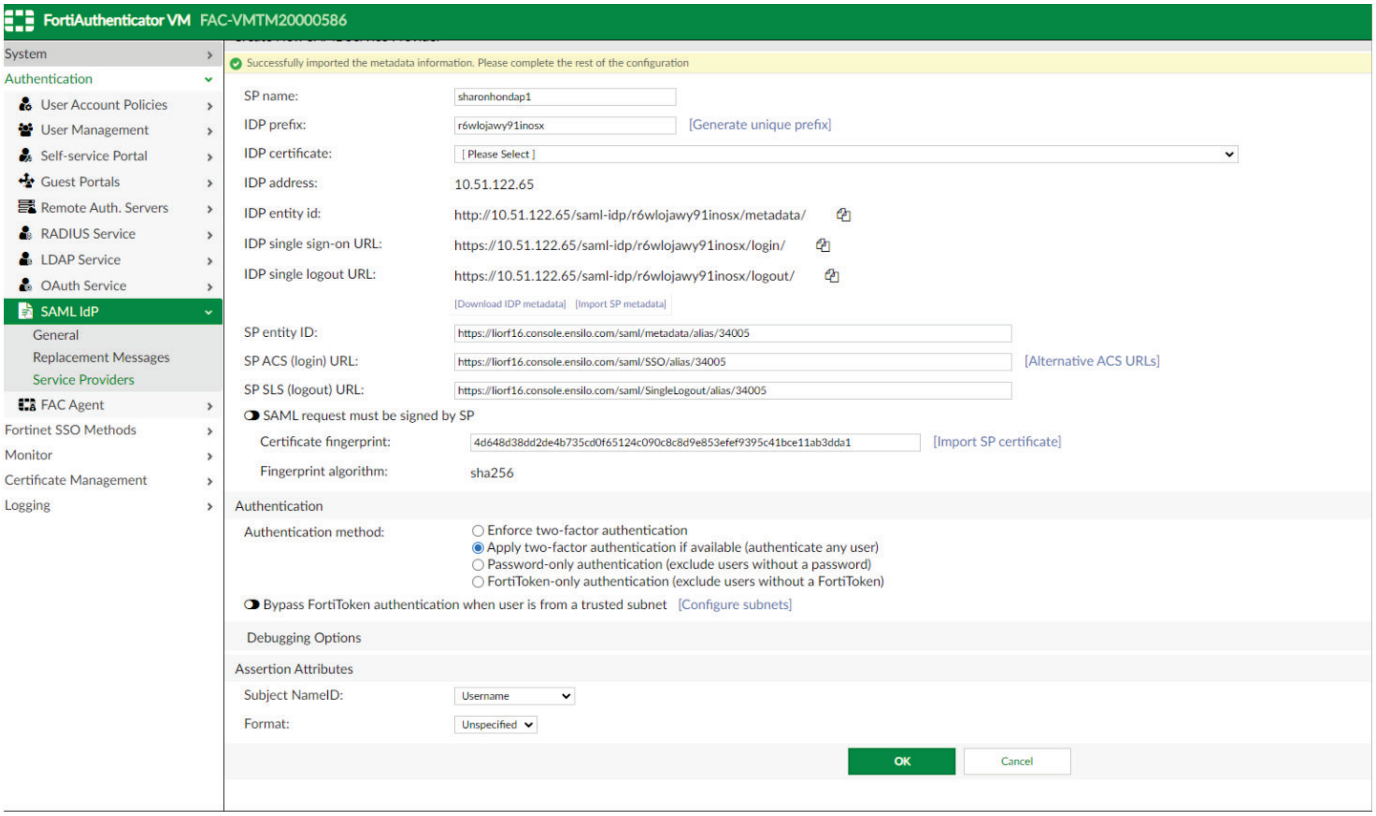


Import Service Provider Metadata

Filetype: ● Metadata ○ Certificate

File: fortiEDR.sp....tedata.id.1.xml

6 All other service provider configuration fields are auto-filled after the SP data file import:



Successfully imported the metadata information. Please complete the rest of the configuration

SP name: sharonhondap1

IDP prefix: r6wlojawy91inosx [Generate unique prefix]

IDP certificate: [Please Select]

IDP address: 10.51.122.65

IDP entity id: http://10.51.122.65/saml-idp/r6wlojawy91inosx/metadata/

IDP single sign-on URL: https://10.51.122.65/saml-idp/r6wlojawy91inosx/login/

IDP single logout URL: https://10.51.122.65/saml-idp/r6wlojawy91inosx/logout/

[Download IDP metadata] [Import SP metadata]

SP entity ID: https://liorf16.console.ensilo.com/saml/metadata/alias/34005

SP ACS (login) URL: https://liorf16.console.ensilo.com/saml/SSO/alias/34005 [Alternative ACS URLs]

SP SLS (logout) URL: https://liorf16.console.ensilo.com/saml/SingleLogout/alias/34005

SAML request must be signed by SP

Certificate fingerprint: 4d648d38dd2de4b735cd0f65124c090c8c8d9e853efef9395c41bce11ab3dda1 [Import SP certificate]

Fingerprint algorithm: sha256

Authentication

Authentication method:
○ Enforce two-factor authentication
● Apply two-factor authentication if available (authenticate any user)
○ Password-only authentication (exclude users without a password)
○ FortiToken-only authentication (exclude users without a FortiToken)

Bypass FortiToken authentication when user is from a trusted subnet [Configure subnets]

Debugging Options

Assertion Attributes

Subject NameID: Username

Format: Unspecified

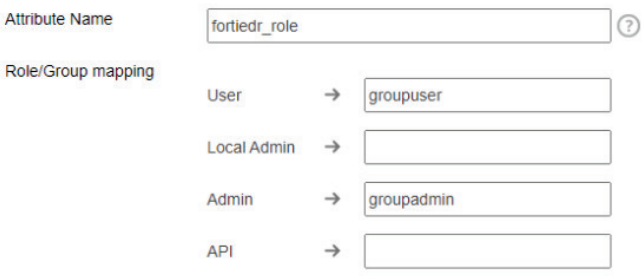
7 Click **OK** to apply the changes.

8 Go to **Authentication ➔ SAML IdP ➔ Service Providers** and double-click to open the Service Provider that you created in the previous step.

9 In the **SAML Attribute** section, click **Create New**.

10 In the popup window, enter the attribute name that was configured in the FortiEDR SAML Authentication settings and select **FortiAuthenticator Group** as the User Attribute.

In our example, we use **fortiedr_role** as an attribute name, as shown below:

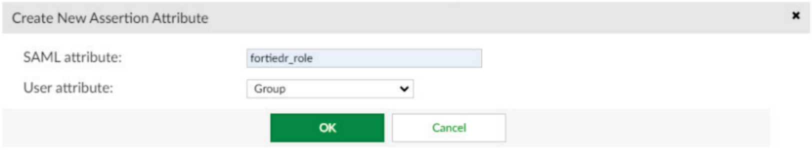


Attribute Name: fortiedr_role

Role/Group mapping

User	→	groupuser
Local Admin	→	
Admin	→	groupadmin
API	→	

And therefore the configuration on FortiAuthenticator appears as follows:



Create New Assertion Attribute

SAML attribute: fortiedr_role

User attribute: Group

11. Click **OK** to save the changes.

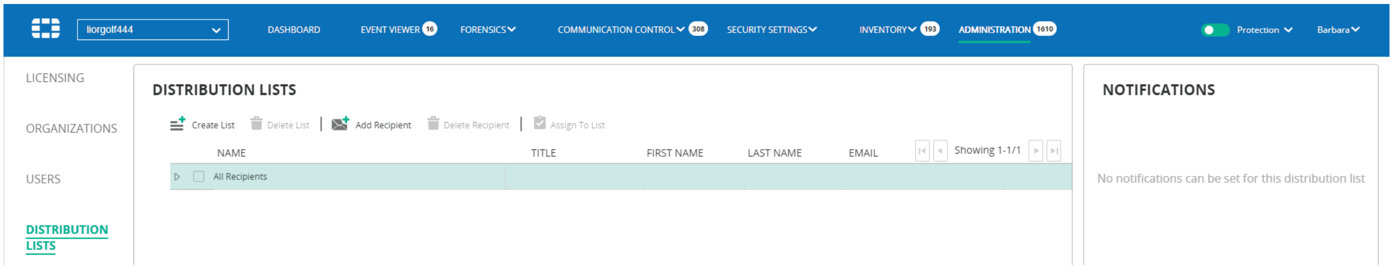
FortiAuthenticator can now be used as the IdP, which provides authorization and authentication for users trying to access the FortiEDR Central Manager Console. When logging into the FortiEDR Console via the SSO url that is specified in the SAML settings page, a FortiAuthenticator user is awarded access permissions to the FortiEDR Central Manager according to the User Groups into which he/she was added.

Distribution Lists

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

Note – You must configure SMTP before using the Distribution List option. For more details, see page 204.
Note – Emails are only sent for security events that occur on devices that are part of Collector Groups that are assigned to a Playbook policy in which the **Send Email Notification** option is checked.

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



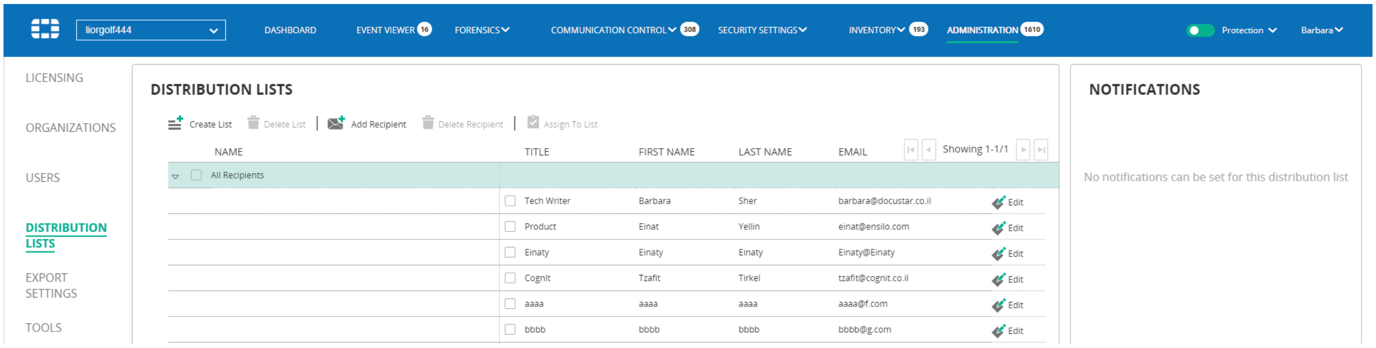
NAME	TITLE	FIRST NAME	LAST NAME	EMAIL
All Recipients				

No notifications can be set for this distribution 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.



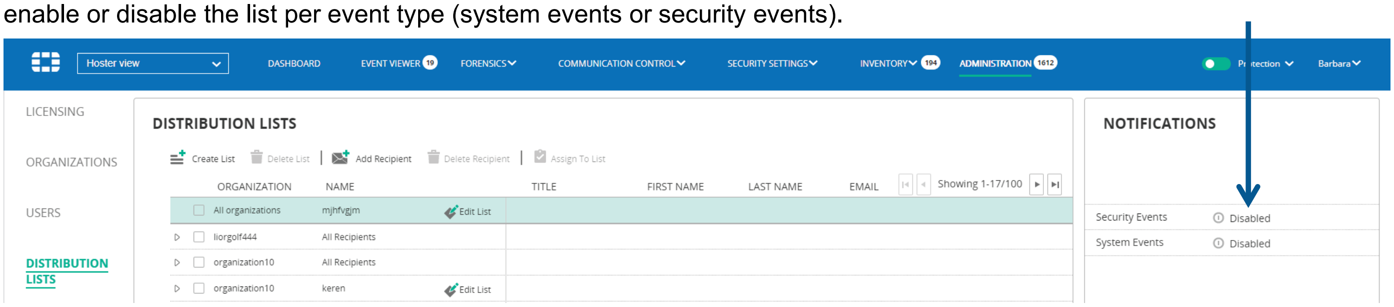
DISTRIBUTION LISTS

NAME	TITLE	FIRST NAME	LAST NAME	EMAIL	
All Recipients					
	Tech Writer	Barbara	Sher	barbara@docustar.co.il	Edit
	Product	Einat	Yellin	einat@ensilo.com	Edit
	Einaty	Einaty	Einaty	Einaty@Einaty	Edit
	CognIt	Tzafit	Tirkel	tzafit@cognit.co.il	Edit
	aaaa	aaaa	aaaa	aaaa@f.com	Edit
	bbbb	bbbb	bbbb	bbbb@g.com	Edit

NOTIFICATIONS

No notifications can be set for this distribution list

Select a distribution list row and then use the Enabled/Disabled option in the NOTIFICATIONS pane on the right to enable or disable the list per event type (system events or security events).



DISTRIBUTION LISTS

ORGANIZATION	NAME		TITLE	FIRST NAME	LAST NAME	EMAIL
All organizations	mjhfvgjm	Edit List				
liorgolf444	All Recipients					
organization10	All Recipients					
organization10	keren	Edit List				

NOTIFICATIONS

Security Events	Disabled
System Events	Disabled

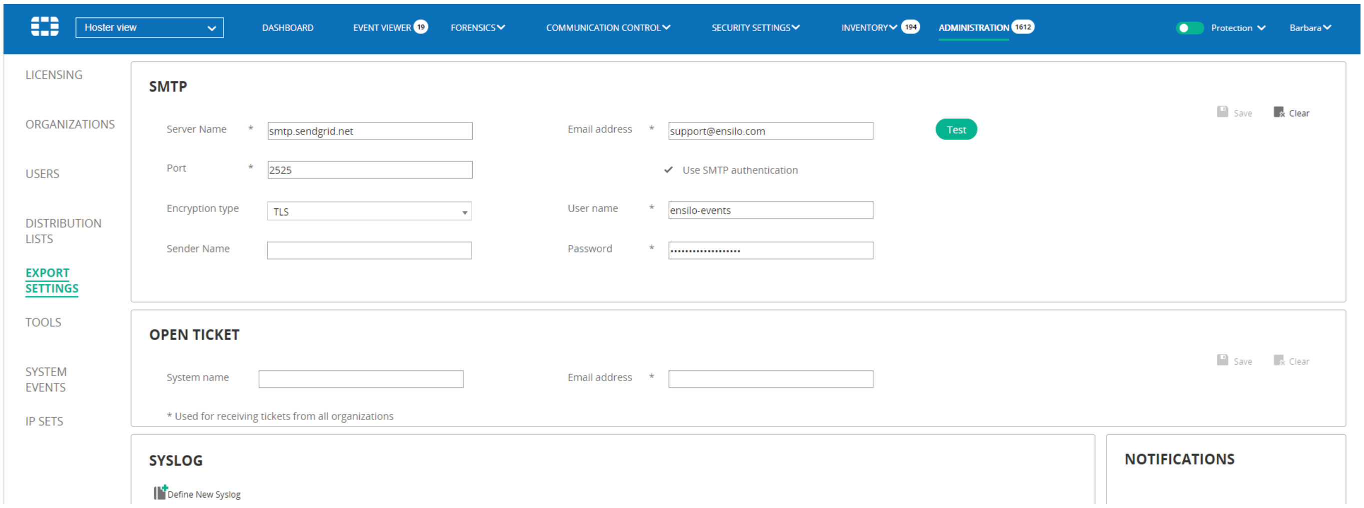
Export Settings

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

- **SMTP,** page 204
- **OPEN TICKET,** page 205
- **SYSLOG,** page 206

SMTP

The SMTP option enables you to configure the SMTP server to be used for sending emails. You can also check the connectivity to the SMTP server.



SMTP

Server Name *	smtp.sendgrid.net	Email address *	support@ensilo.com
Port *	2525	✓ Use SMTP authentication	
Encryption type	TLS	User name *	ensilo-events
Sender Name		Password *	....

OPEN TICKET

System name		Email address *	

* Used for receiving tickets from all organizations

SYSLOG

Define New Syslog

NOTIFICATIONS

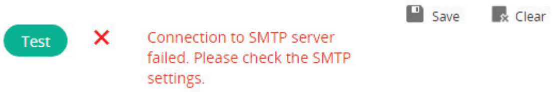
Note – In a single-organization system, SMTP settings are only accessible in Hoster view (for administrators), or to the local administrator of that organization.

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.



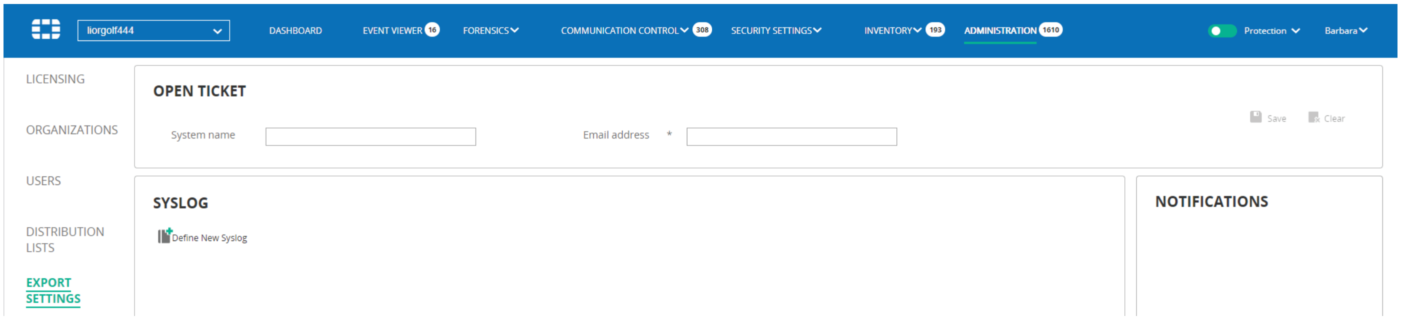
Connection to SMTP server failed. Please check the SMTP settings.

Open Ticket

The **Open Ticket** option enables you to send events to an event-management tool such as Jira or ServiceNow. Open Ticket automatically opens a ticket and attaches the relevant event to a ticket.

In order for the Open Ticket feature to work properly, you must set up an email feed in the event-management tool to be used.

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 257.
Note – Security events are only sent to a ticketing system when they occur on devices that are part of Collector Groups that are assigned to a Playbook policy in which the **Open Ticket** option is checked.



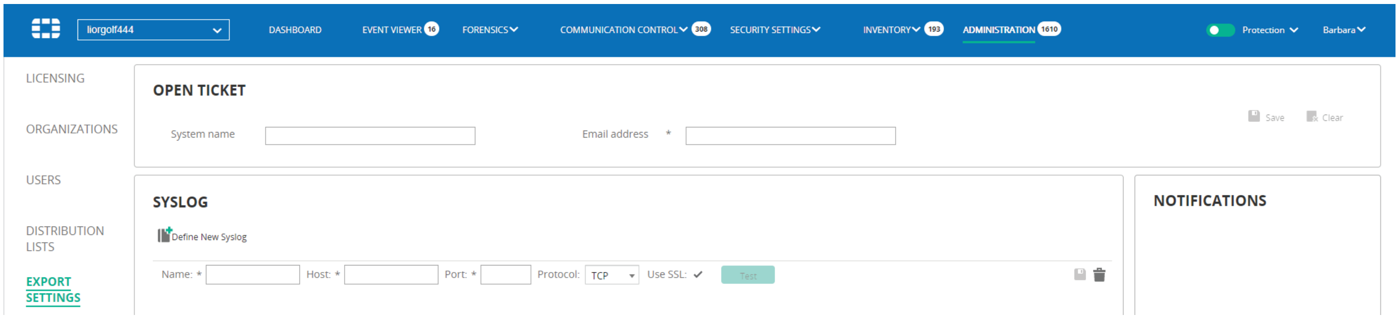
To configure Open Ticket settings:

1. In the Open Ticket area, in the **System name** field, enter the system name for the tool to be used for event management. This is a free-text field.
2. In the **Email address** field, enter the email address that is the destination to which all tickets are to be sent from FortiEDR. All tickets from all organizations are sent to this email.
3. Click **Save**.

Syslog

The **SYSLOG** option enables you to configure FortiEDR to automatically send FortiEDR events to one or more standard Security Information and Event Management (SIEM) solutions via Syslog.

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



Name: * Host: * Port: * Protocol: TCP Use SSL: ✓

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 security events that occur on devices that are part of Collector Groups that are assigned to a Playbook policy in which the **Send Syslog Notification** option is checked.

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 219) with the following fields:
  - Component Type
  - Component Name
  - Description
  - Date
- Audit trail event (see page 208) 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

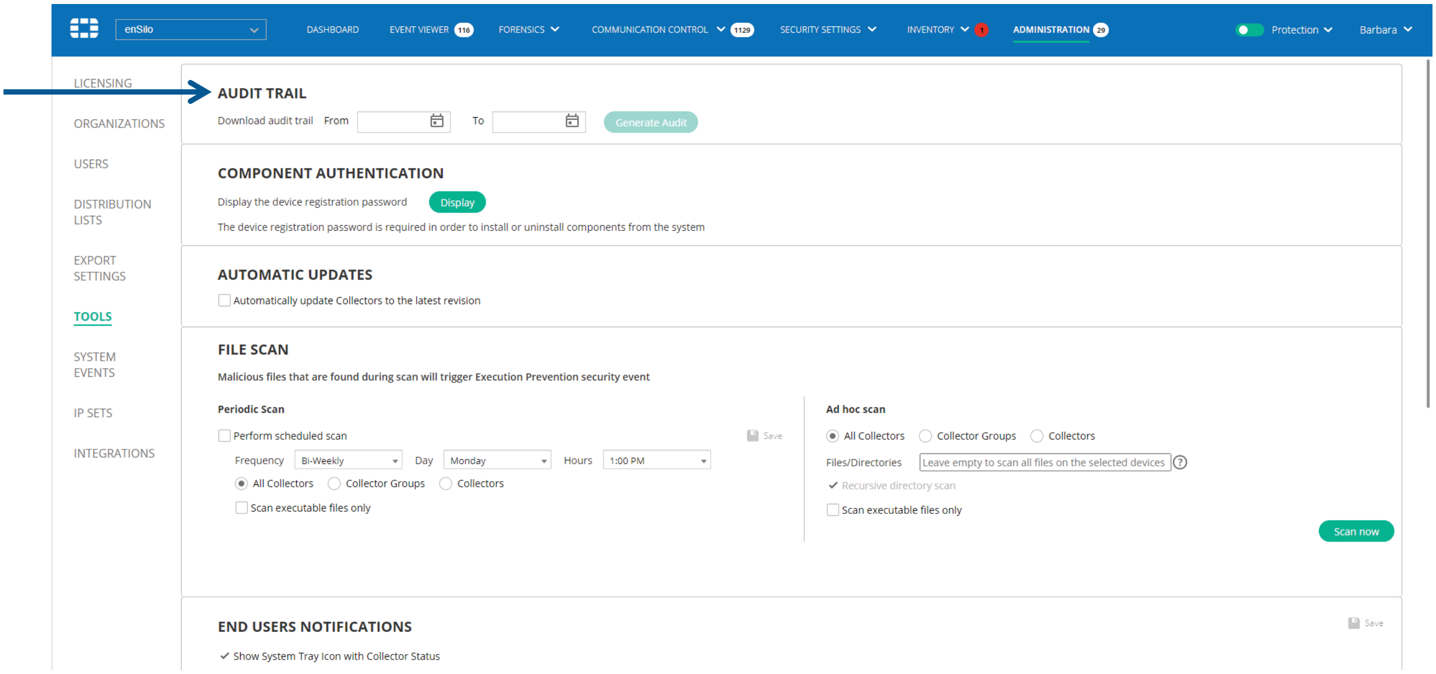
The **TOOLS** option provides access to the following options:

- **Audit Trail,** page 208
- **Component Authentication,** page 210
- **Automatic Updates,** page 210
- **File Scan,** page 210
- **End-user Notifications,** page 211
- **IoT Device Discovery,** page 213
- **Personal Data Handling,** page 214
- **Windows Security Center,** page 218

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.



AUDIT TRAIL

Download audit trail From To

COMPONENT AUTHENTICATION

Display the device registration password

The device registration password is required in order to install or uninstall components from the system

AUTOMATIC UPDATES

□ Automatically update Collectors to the latest revision

FILE SCAN

Malicious files that are found during scan will trigger Execution Prevention security event

Periodic Scan

□ Perform scheduled scan

Frequency: Bi-Weekly Day: Monday Hours: 1:00 PM

● All Collectors ○ Collector Groups ○ Collectors

□ Scan executable files only

Ad hoc scan

● All Collectors ○ Collector Groups ○ Collectors

Files/Directories: Leave empty to scan all files on the selected devices

✓ Recursive directory scan

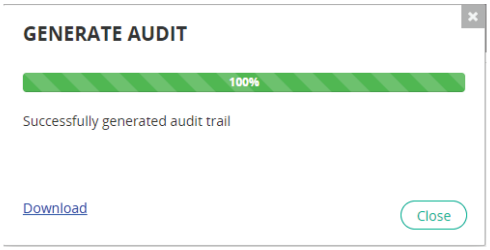
□ Scan executable files only

END USERS NOTIFICATIONS

✓ Show System Tray Icon with Collector Status

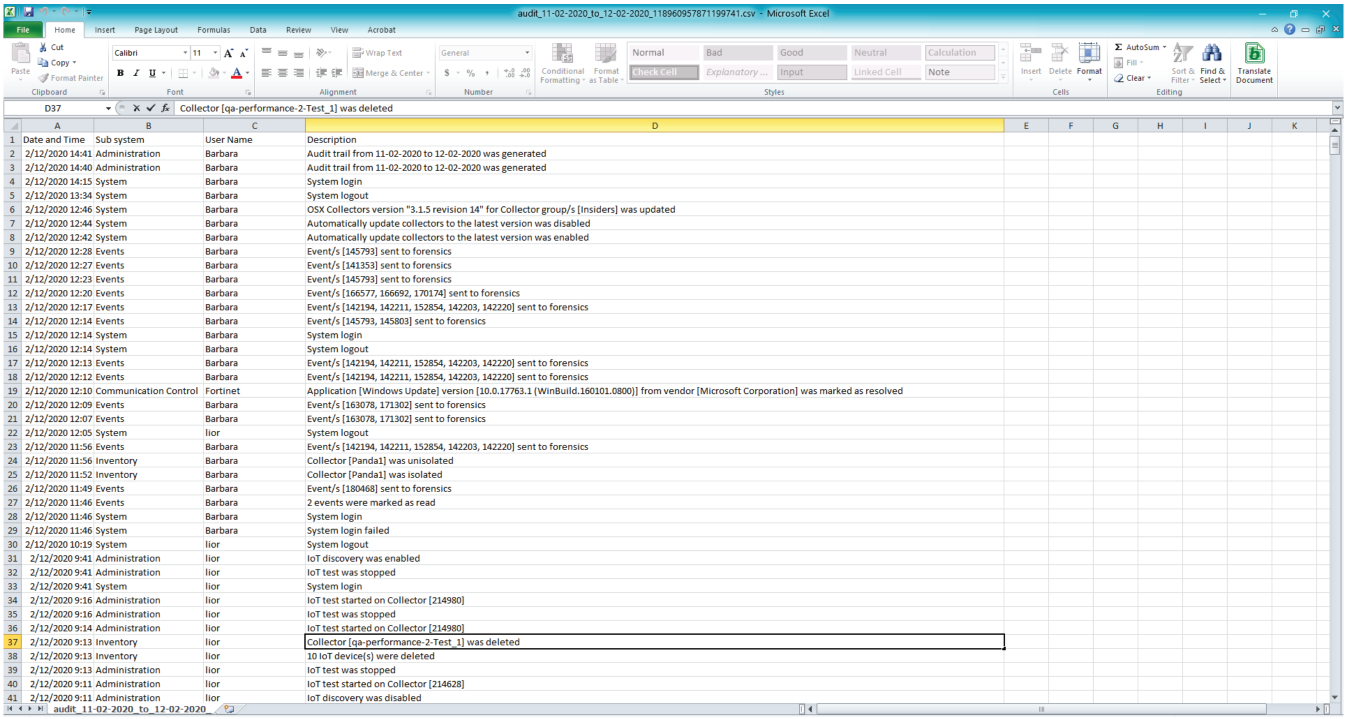
To generate the audit trail:

1. Click the **TOOLS** link in the left pane.
2. In the AUDIT TRAIL area, specify the **From** and **To** dates in the respective fields.
3. Click the **Generate Audit** button. A progress window displays:



Successfully generated audit trail

4. Click the **Download** link to download the audit trail to a *.csv file. An Excel file, such as the example shown below, displays:



D37 Collector [qa-performance-2-Test_1] was deleted

	A	B	C	D
1	Date and Time	Sub system	User Name	Description
2	2/12/2020 14:41	Administration	Barbara	Audit trail from 11-02-2020 to 12-02-2020 was generated
3	2/12/2020 14:40	Administration	Barbara	Audit trail from 11-02-2020 to 12-02-2020 was generated
4	2/12/2020 14:15	System	Barbara	System login
5	2/12/2020 13:34	System	Barbara	System logout
6	2/12/2020 12:46	System	Barbara	OSX Collectors version "3.1.5 revision 14" for Collector group/s [Insiders] was updated
7	2/12/2020 12:44	System	Barbara	Automatically update collectors to the latest version was disabled
8	2/12/2020 12:42	System	Barbara	Automatically update collectors to the latest version was enabled
9	2/12/2020 12:28	Events	Barbara	Event/s [145793] sent to forensics
10	2/12/2020 12:27	Events	Barbara	Event/s [141353] sent to forensics
11	2/12/2020 12:23	Events	Barbara	Event/s [145793] sent to forensics
12	2/12/2020 12:20	Events	Barbara	Event/s [166577, 166692, 170174] sent to forensics
13	2/12/2020 12:17	Events	Barbara	Event/s [142194, 142211, 152854, 142203, 142220] sent to forensics
14	2/12/2020 12:14	Events	Barbara	Event/s [145793, 145803] sent to forensics
15	2/12/2020 12:14	System	Barbara	System login
16	2/12/2020 12:14	System	Barbara	System logout
17	2/12/2020 12:13	Events	Barbara	Event/s [142194, 142211, 152854, 142203, 142220] sent to forensics
18	2/12/2020 12:12	Events	Barbara	Event/s [142194, 142211, 152854, 142203, 142220] sent to forensics
19	2/12/2020 12:10	Communication Control	Fortinet	Application [Windows Update] version [10.0.17763.1 (WinBuild.160101.0800)] from vendor [Microsoft Corporation] was marked as resolved
20	2/12/2020 12:09	Events	Barbara	Event/s [163078, 171302] sent to forensics
21	2/12/2020 12:07	Events	Barbara	Event/s [163078, 171302] sent to forensics
22	2/12/2020 12:05	System	lior	System logout
23	2/12/2020 11:56	Events	Barbara	Event/s [142194, 142211, 152854, 142203, 142220] sent to forensics
24	2/12/2020 11:56	Inventory	Barbara	Collector [Panda1] was unisolated
25	2/12/2020 11:52	Inventory	Barbara	Collector [Panda1] was isolated
26	2/12/2020 11:49	Events	Barbara	Event/s [180468] sent to forensics
27	2/12/2020 11:46	Events	Barbara	2 events were marked as read
28	2/12/2020 11:46	System	Barbara	System login
29	2/12/2020 11:46	System	Barbara	System login failed
30	2/12/2020 10:19	System	lior	System logout
31	2/12/2020 9:41	Administration	lior	IoT discovery was enabled
32	2/12/2020 9:41	Administration	lior	IoT test was stopped
33	2/12/2020 9:41	System	lior	System login
34	2/12/2020 9:16	Administration	lior	IoT test started on Collector [214980]
35	2/12/2020 9:16	Administration	lior	IoT test was stopped
36	2/12/2020 9:14	Administration	lior	IoT test started on Collector [214980]
37	2/12/2020 9:13	Inventory	lior	Collector [qa-performance-2-Test_1] was deleted
38	2/12/2020 9:13	Inventory	lior	10 IoT device(s) were deleted
39	2/12/2020 9:13	Administration	lior	IoT test was stopped
40	2/12/2020 9:11	Administration	lior	IoT test started on Collector [214628]
41	2/12/2020 9:11	Administration	lior	IoT discovery was disabled

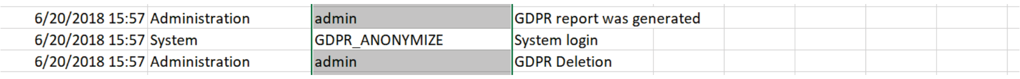
Each row in the audit trail file contains the following columns of information:

- **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

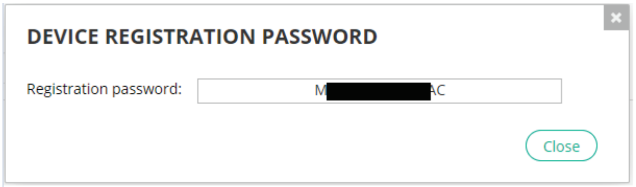
In order to install, upgrade or uninstall a Collector, you must supply the Aggregator password. The Aggregator password is the same for all Collectors in the FortiEDR system. This password is defined during initial system installation. For more details, see the *Installing the FortiEDR Central Manager and FortiEDR Aggregator on the Same Machine* section on page 19.

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.



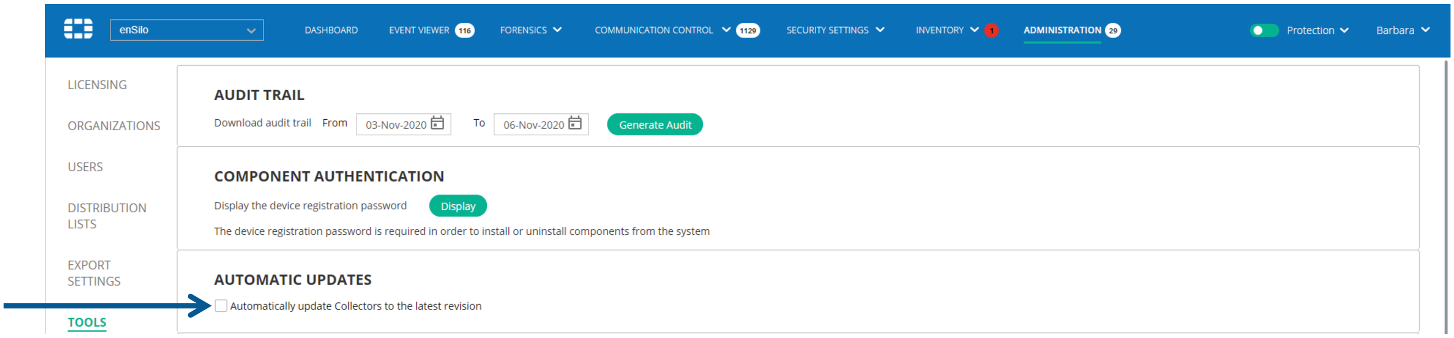
DEVICE REGISTRATION PASSWORD

Registration password: M[redacted]AC

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 28.



AUDIT TRAIL

Download audit trail From 03-Nov-2020 To 06-Nov-2020 Generate Audit

COMPONENT AUTHENTICATION

Display the device registration password Display

The device registration password is required in order to install or uninstall components from the system

AUTOMATIC UPDATES

□ Automatically update Collectors to the latest revision

To update a FortiEDR version, use the Update Collector Version feature described on page 179.

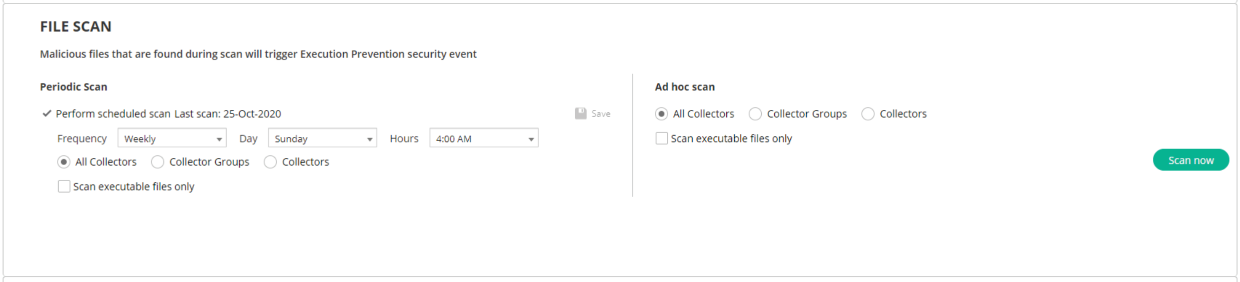
File Scan

FortiEDR can perform periodic scans of the files in the system on a scheduled or on-demand basis, based on its execution prevention policy. During a periodic scan, only the files on the hard drive are scanned and no memory scan is performed. For a periodic scan, each file on the hard drive is scanned. If a malicious file is identified during a scan, a security event is triggered.

To schedule a periodic scan:

1 Click the **TOOLS** link in the left pane.

2 In the FILE SCAN area, check the **Perform Scheduled Scan** checkbox. This checkbox must be checked to perform the scan according to the designated schedule.



FILE SCAN

Malicious files that are found during scan will trigger Execution Prevention security event

Periodic Scan

✓ Perform scheduled scan Last scan: 25-Oct-2020

Save

Frequency: Weekly Day: Sunday Hours: 4:00 AM

● All Collectors ○ Collector Groups ○ Collectors

□ Scan executable files only

Ad hoc scan

● All Collectors ○ Collector Groups ○ Collectors

□ Scan executable files only

Scan now

3 In the **Frequency** dropdown list, select how frequently to execute the scan. Options are **Weekly**, **Bi-Weekly** (every two weeks) or **Monthly**.

4 In the **Day** dropdown list, select the day of the week to execute the scan.

5 In the **Hours** dropdown list, select the hour of the day to execute the scan.

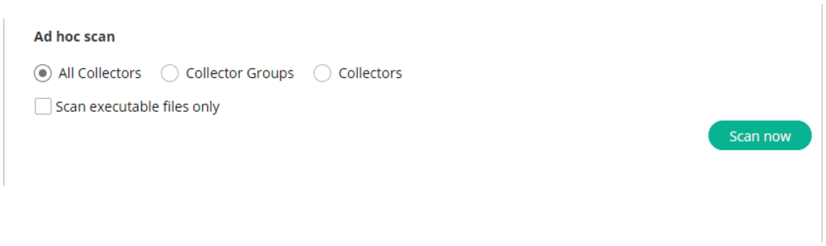
6 Use the radio button to select on which devices the scheduled scan should be performed. When selecting Collector Groups or Collectors, you should specify which Groups or Collectors should be included in the scan. Devices that are not listed here are not scanned.

7 Click the **Save** button. The scan is performed as scheduled.

To perform an on-demand file scan:

1 Click the **TOOLS** link in the left pane.

2 In the Ad hoc scan area, select which devices to scan by specifying one or more Collectors or Collector Groups, or selecting the **All Collectors** option to scan all devices with installed Collectors.



Ad hoc scan

● All Collectors ○ Collector Groups ○ Collectors

□ Scan executable files only

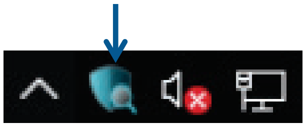
Scan now

3 Check the **Scan executable files only** checkbox to only scan executable files. This option enables a quicker scan, but neglects documents, scripts and other potentially malicious files.

4 Click **Scan now**. The scan is performed immediately.

End-user Notifications

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

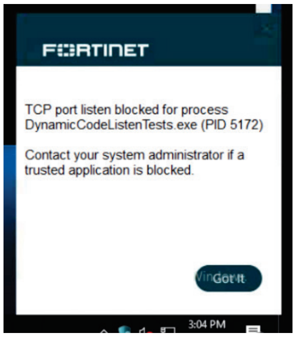


The FortiEDR icon indicates the current state of the device, as follows:

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

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.

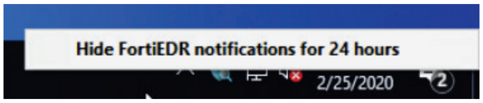


FORTINET

TCP port listen blocked for process DynamicCodeListenTests.exe (PID 5172)

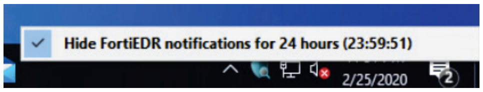
Contact your system administrator if a trusted application is blocked.

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 FortiEDR notifications for 24 hours

Hide Notifications



☑ Hide FortiEDR notifications for 24 hours (23:59:51)

Display Notifications

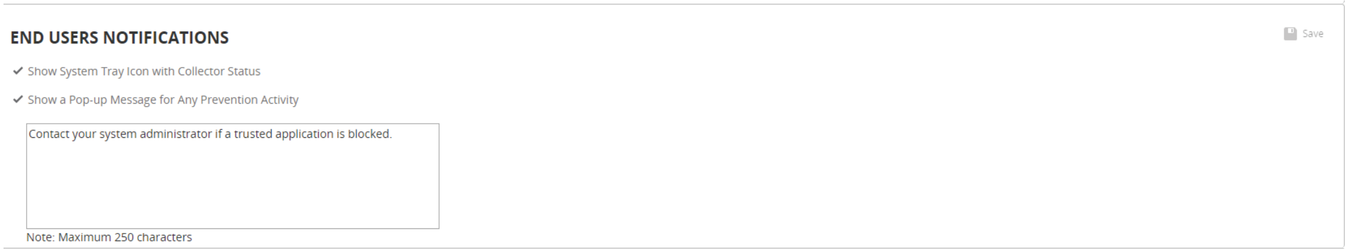
FortiEDR Icon Configuration

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:



END USERS NOTIFICATIONS

✓ Show System Tray Icon with Collector Status

✓ Show a Pop-up Message for Any Prevention Activity

Contact your system administrator if a trusted application is blocked.

Note: Maximum 250 characters

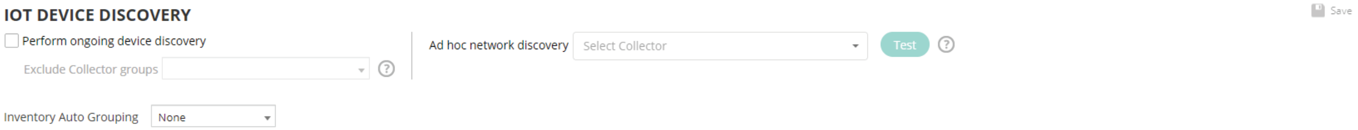
- **Show System Tray Icon with Collector Status:** Check this checkbox to display the FortiEDR icon on each FortiEDR-protected device or leave the checkbox unchecked to hide the icon on each protected device. Your selection here is applied on all protected devices. The default is checked.
- **Show a 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 82.



IOT DEVICE DISCOVERY

□ Perform ongoing device discovery

Exclude Collector groups

Ad hoc network discovery: Select Collector

Inventory Auto Grouping: None

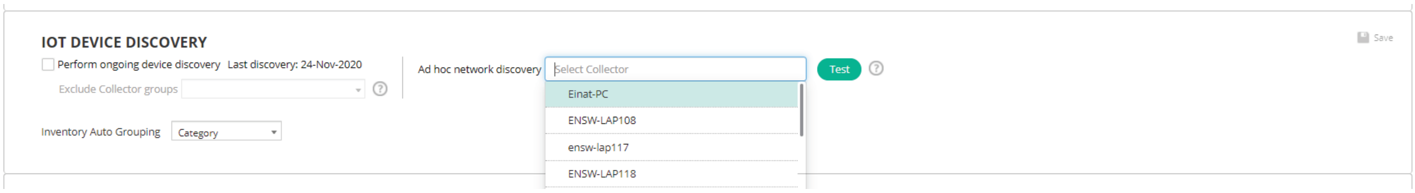
To enable IoT device discovery, check the **Perform ongoing device discovery** checkbox. Note that when doing so, all relevant Collectors in the system perform sniffing in order to identify new connected devices in the system. When performing this discovery process, FortiEDR uses only the most powerful Collectors in each sub-network to perform sniffing, and excludes weaker Collectors for this process (disabled and degraded Collectors). This means that FortiEDR collects all the required information in the most efficient manner possible.

You can exclude specific Collector Groups from this discovery process. To do so, select the relevant Collector Group(s) in the **Exclude Collector Groups** dropdown list.

The Inventory **Auto Grouping** option enables you to group discovered devices by device type. For example, cameras, network devices, media devices, printers and so on. Select the **Category** option in the dropdown list to group discovered devices by device type or **None**. When you select Category, devices are auto-grouped in the **IOT DEVICES** page, as shown on page 82.

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 **Ad Hoc Network Discovery** dropdown list and then click the **Test** button, as shown below.



IOT DEVICE DISCOVERY

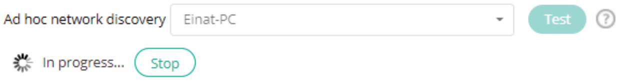
□ Perform ongoing device discovery Last discovery: 24-Nov-2020

Exclude Collector groups

Inventory Auto Grouping: Category

Ad hoc network discovery: Select Collector

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).



Ad hoc network discovery: Einat-PC

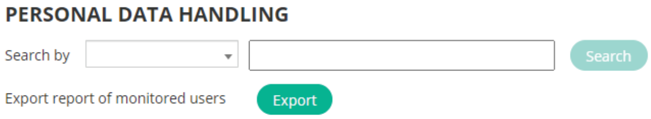
In progress...

Personal Data Handling

The FortiEDR system fully complies with the General Data Protection Regulation (GDPR) standard. The GDPR is a regulation in European Union (EU) law regarding data protection and privacy for all individuals within the EU and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA areas. The goal of the GDPR is primarily to give control to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

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

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



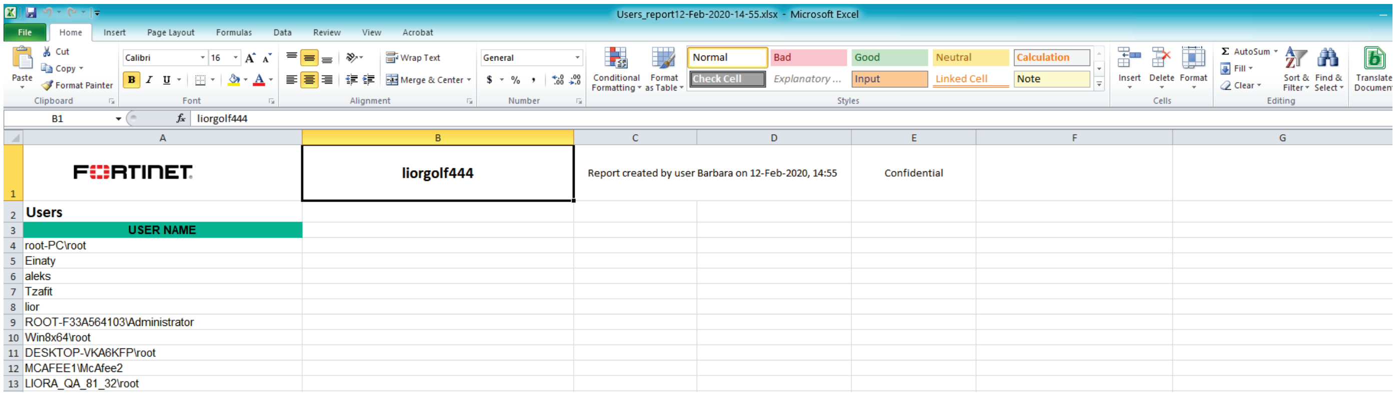
PERSONAL DATA HANDLING

Search by

Export report of monitored users

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:



Users_report12-Feb-2020-14-55.xlsx - Microsoft Excel

	A	B	C	D	E
1	FORTINET	liorgolf444	Report created by user Barbara on 12-Feb-2020, 14:55		Confidential
2	Users				
3	USER NAME				
4	root-PC\root				
5	Einaty				
6	aleks				
7	Tzafit				
8	lior				
9	ROOT-F33A564103\Administrator				
10	Win8x64\root				
11	DESKTOP-VKA6KFP\root				
12	MCAFEE1\McAfee2				
13	LIORA_QA_81_32\root				

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 47.

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.

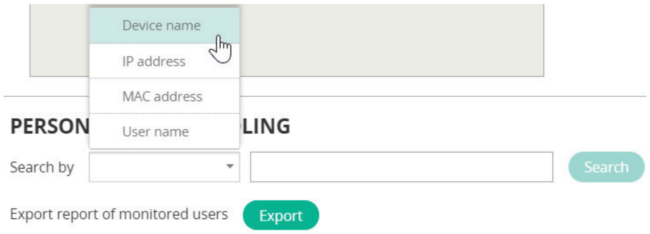
Note – If the employee/user has multiple computers on which Collectors are installed, you must repeat the steps below for each of his/her computers.

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.

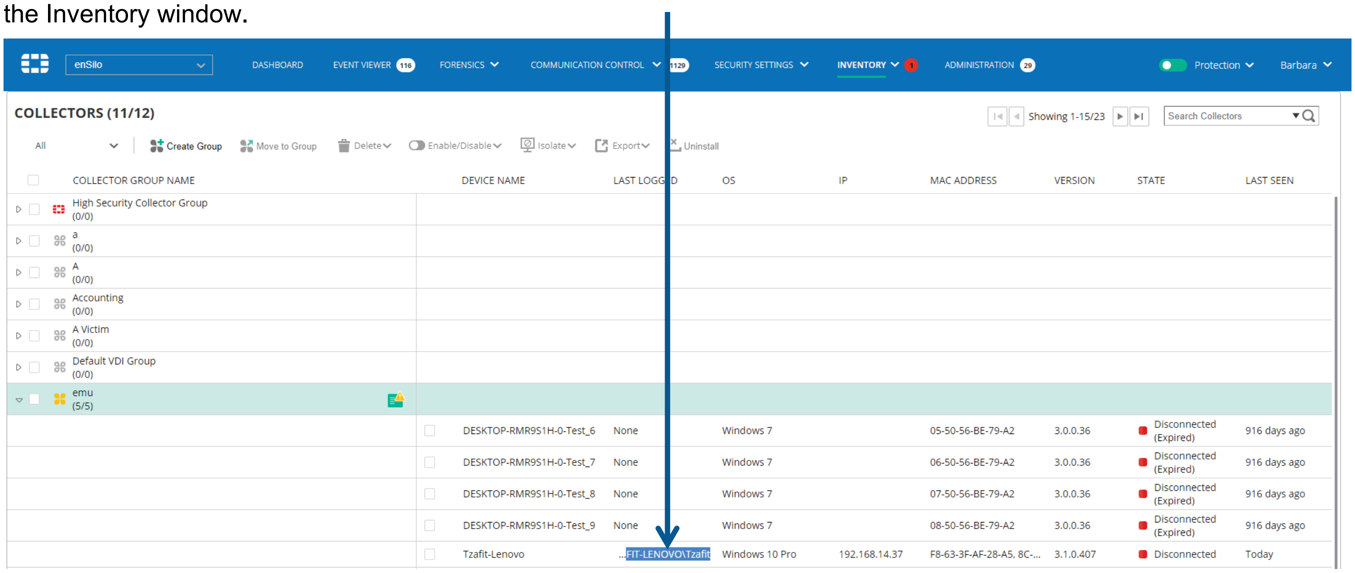
IMPORTANT – You can remove the device name, IP address, MAC address and user name of the employee/user from FortiEDR in any order that you prefer. However, you **must** remove all device name, IP address, MAC address and user name data from FortiEDR in order to fully comply with the GDPR standard.

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.



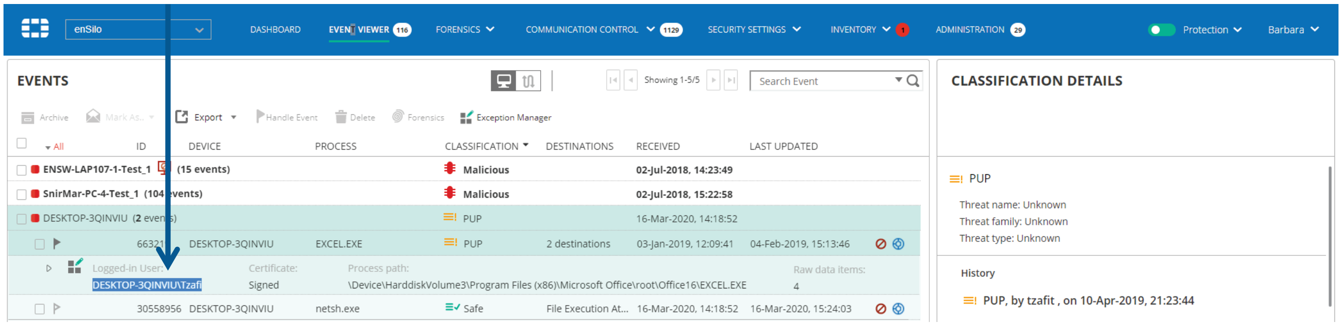
You can copy/paste this information into the adjacent field after locating it elsewhere in the FortiEDR user interface. For example, you can locate the relevant device name in the **Last Logged** column in the Collectors list in the Inventory window, such as shown below, and then copy that value into 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.



COLLECTORS (11/12)

☐	COLLECTOR GROUP NAME	DEVICE NAME	LAST LOGG D	OS	IP	MAC ADDRESS	VERSION	STATE	LAST SEEN
☐	High Security Collector Group (0/0)								
☐	a (0/0)								
☐	A (0/0)								
☐	Accounting (0/0)								
☐	A Victim (0/0)								
☐	Default VDI Group (0/0)								
☐	emu (5/5)								
☐		DESKTOP-RMR9S1H-0-Test_6	None	Windows 7		05-50-56-BE-79-A2	3.0.0.36	🟥 Disconnected (Expired)	916 days ago
☐		DESKTOP-RMR9S1H-0-Test_7	None	Windows 7		06-50-56-BE-79-A2	3.0.0.36	🟥 Disconnected (Expired)	916 days ago
☐		DESKTOP-RMR9S1H-0-Test_8	None	Windows 7		07-50-56-BE-79-A2	3.0.0.36	🟥 Disconnected (Expired)	916 days ago
☐		DESKTOP-RMR9S1H-0-Test_9	None	Windows 7		08-50-56-BE-79-A2	3.0.0.36	🟥 Disconnected (Expired)	916 days ago
☐		Tzafit-Lenovo	...FIT-LENOVO\Tzafit	Windows 10 Pro	192.168.14.37	F8-63-3F-AF-28-A5, 8C-...	3.1.0.407	🟥 Disconnected	Today

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



EVENTS

All	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
ENSW-LAP107-1-Test_1 (15 events)				Malicious		02-Jul-2018, 14:23:49	
SnirMar-PC-4-Test_1 (104 events)				Malicious		02-Jul-2018, 15:22:58	
DESKTOP-3QINVIU (2 events)				PUP		16-Mar-2020, 14:18:52	
	66321	DESKTOP-3QINVIU	EXCEL.EXE	PUP	2 destinations	03-Jan-2019, 12:09:41	04-Feb-2019, 15:13:46
	30558956	DESKTOP-3QINVIU	netsh.exe	Safe	File Execution At...	16-Mar-2020, 14:18:52	16-Mar-2020, 15:24:03

Logged-in User: DESKTOP-3QINVIU\Tzafi
Certificate: Signed
Process path: \Device\HarddiskVolume3\Program Files (x86)\Microsoft Office\root\Office16\EXCEL.EXE
Raw data items: 4

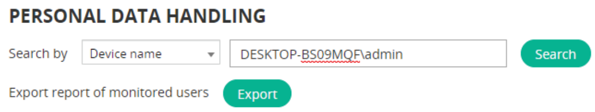
CLASSIFICATION DETAILS

PUP
Threat name: Unknown
Threat family: Unknown
Threat type: Unknown

History
PUP, by tzafit , on 10-Apr-2019, 21:23:44

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

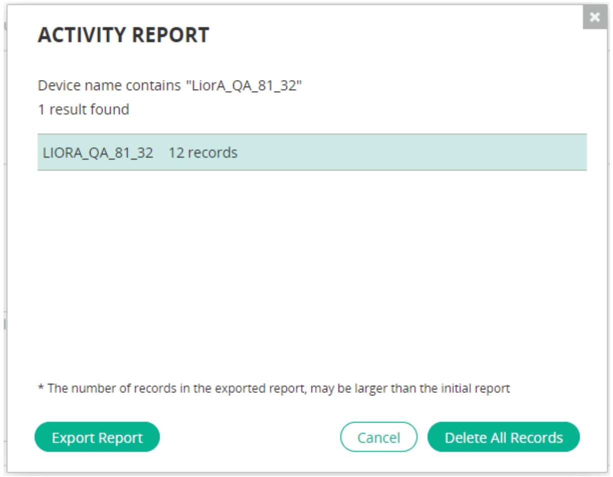
6 After entering the details for the device name, as shown below, click **Search** to search for all occurrences of the device name in the FortiEDR system.



PERSONAL DATA HANDLING

Search by: Device name — DESKTOP-BS09MQF\admin

The following displays, listing all matching results:



ACTIVITY REPORT

Device name contains "LiorA_QA_81_32"
1 result found

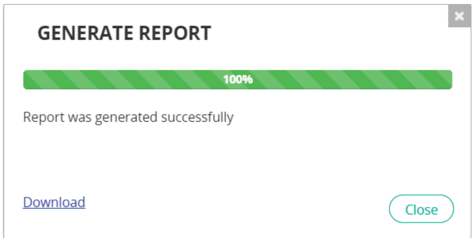
LIORA_QA_81_32 12 records

* The number of records in the exported report, may be larger than the initial report

7 Do one of the following:

- 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:

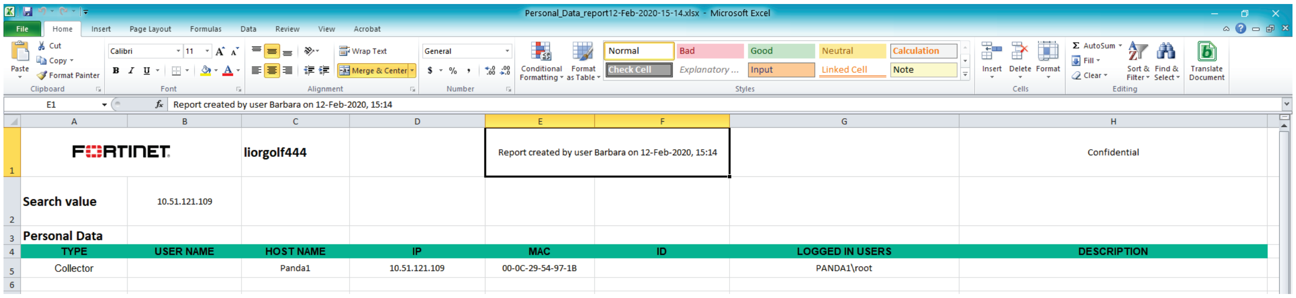


GENERATE REPORT

100%

Report was generated successfully

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



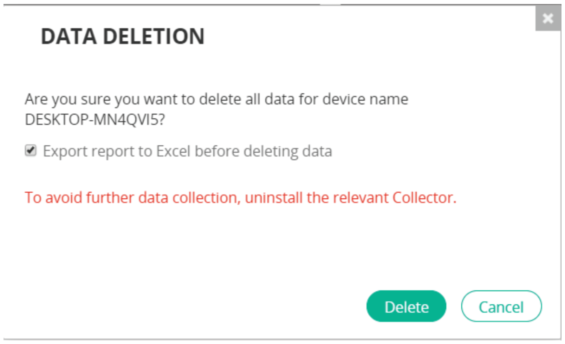
Personal_Data_report12-Feb-2020-15-14.xlsx - Microsoft Excel
File
Home
Insert
Page Layout
Formulas
Data
Review
View
Acrobat
E1

Report created by user Barbara on 12-Feb-2020, 15:14

FORTINET	liorgolf444			Report created by user Barbara on 12-Feb-2020, 15:14			Confidential
Search value	10.51.121.109						
Personal Data							
TYPE	USER NAME	HOST NAME	IP	MAC	ID	LOGGED IN USERS	DESCRIPTION
Collector		Panda1	10.51.121.109	00-0C-29-54-97-1B		PANDA1\root	

OR–

- Click the **Delete All Records** button to remove all device name data for the employee/user. The following displays:



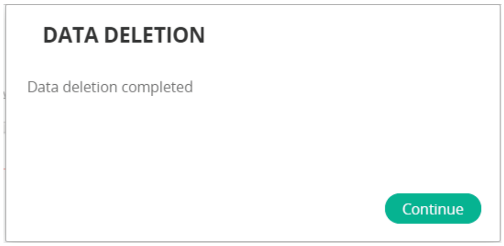
DATA DELETION

Are you sure you want to delete all data for device name DESKTOP-MN4QVI5?

☑ Export report to Excel before deleting data

To avoid further data collection, uninstall the relevant Collector.

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:



DATA DELETION

Data deletion completed

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

8 Click **Continue** to proceed with removing the other required data for the employee/user (IP address, MAC address and user name).

9 Repeat steps **4–8** to remove the relevant IP address from FortiEDR. Be sure to select **IP Address** in step **4**.

10 Repeat steps **4–8** to remove the relevant MAC address from FortiEDR. Be sure to select **MAC Address** in step **4**.

11 Repeat steps **4–8** to remove the relevant user name data from FortiEDR. Be sure to select **User Name** in step **4**.

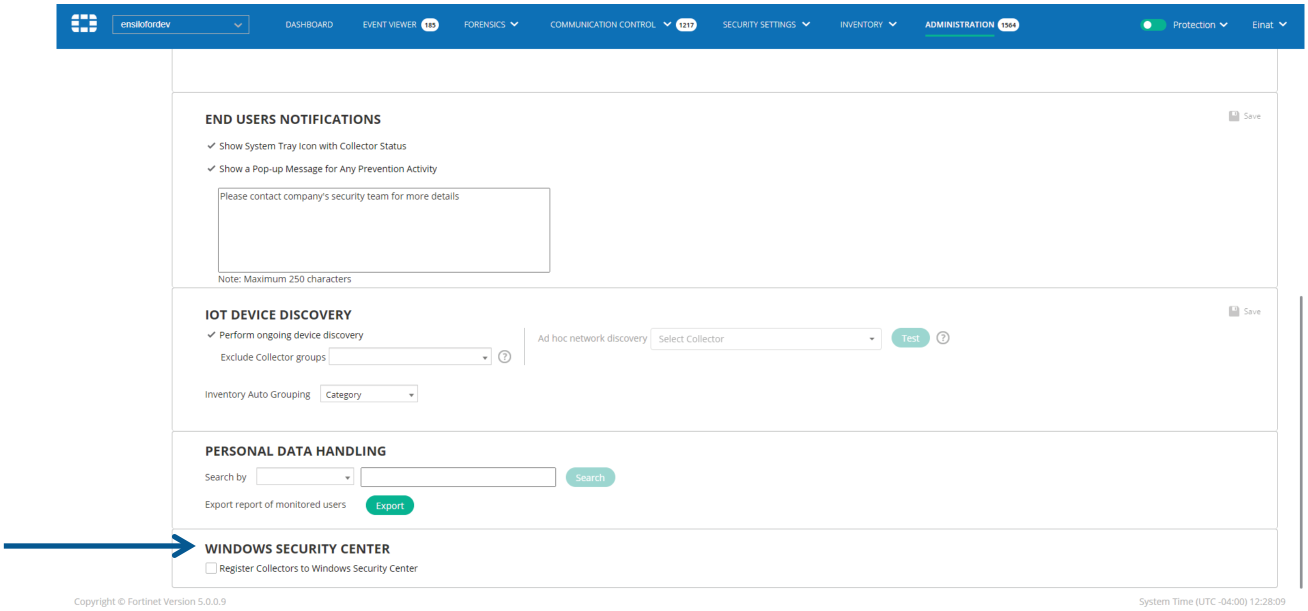
Personal Data Handling of Threat Hunting Data

The search performed by Personal Data Handling (described above) does not show activity event data. This data will be deleted in case you use the delete option (described above), even though it is not displayed in the search results. If you're interested in seeing the activity data that will be deleted, you can view it by using the Search option of the Threat Hunting feature, as described in page 160.

Windows Security Center

FortiEDR is fully integrated with Windows Security Center and has been certified by Microsoft as an anti-virus and threat protection application. You can choose whether to register FortiEDR Collectors as anti-virus and threat protection agents in Windows Security Center. When registering FortiEDR Collectors, Windows Security Center indicates that your system has anti-virus and threat protection provided by FortiEDR.

Note that in some cases, registering FortiEDR in Windows Security Center may prevent other vendors' products from installing or functioning properly. Therefore, you can choose whether or not to register FortiEDR Collectors. Your system is still fully protected, even if you do not choose to register FortiEDR Collectors with Windows Security Center.



END USERS NOTIFICATIONS

✓ Show System Tray Icon with Collector Status

✓ Show a Pop-up Message for Any Prevention Activity

Please contact company's security team for more details

Note: Maximum 250 characters

IOT DEVICE DISCOVERY

✓ Perform ongoing device discovery

Exclude Collector groups

Ad hoc network discovery: Select Collector

Inventory Auto Grouping: Category

PERSONAL DATA HANDLING

Search by

Export report of monitored users

WINDOWS SECURITY CENTER

□ Register Collectors to Windows Security Center

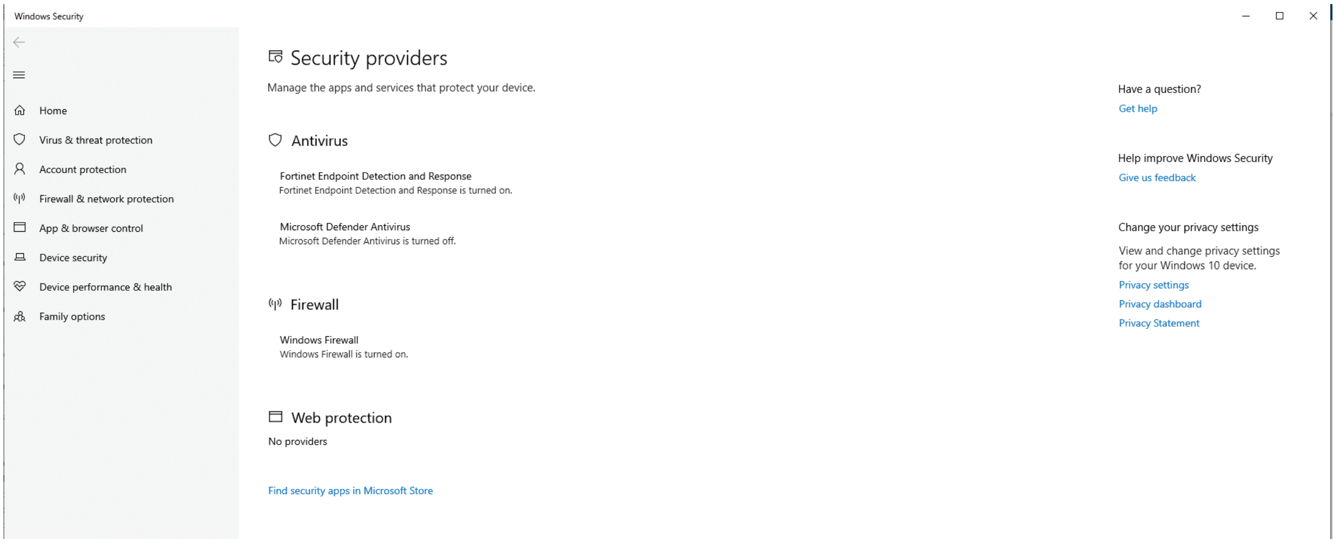
Copyright © Fortinet Version 5.0.0.9

System Time (UTC -04:00) 12:28:09

To register FortiEDR Collectors with Windows Security Center:

- In the **ADMINISTRATION** tab, navigate to the **Tools 🡺 Windows Security Center** area, and then check the **Register Collectors to Windows Security Center** checkbox, as shown above.

  When registered, FortiEDR is listed under Windows Security, as follows:



Security providers

Manage the apps and services that protect your device.

Antivirus

Fortinet Endpoint Detection and Response
Fortinet Endpoint Detection and Response is turned on.

Microsoft Defender Antivirus
Microsoft Defender Antivirus is turned off.

Firewall

Windows Firewall
Windows Firewall is turned on.

Web protection

No providers

Find security apps in Microsoft Store

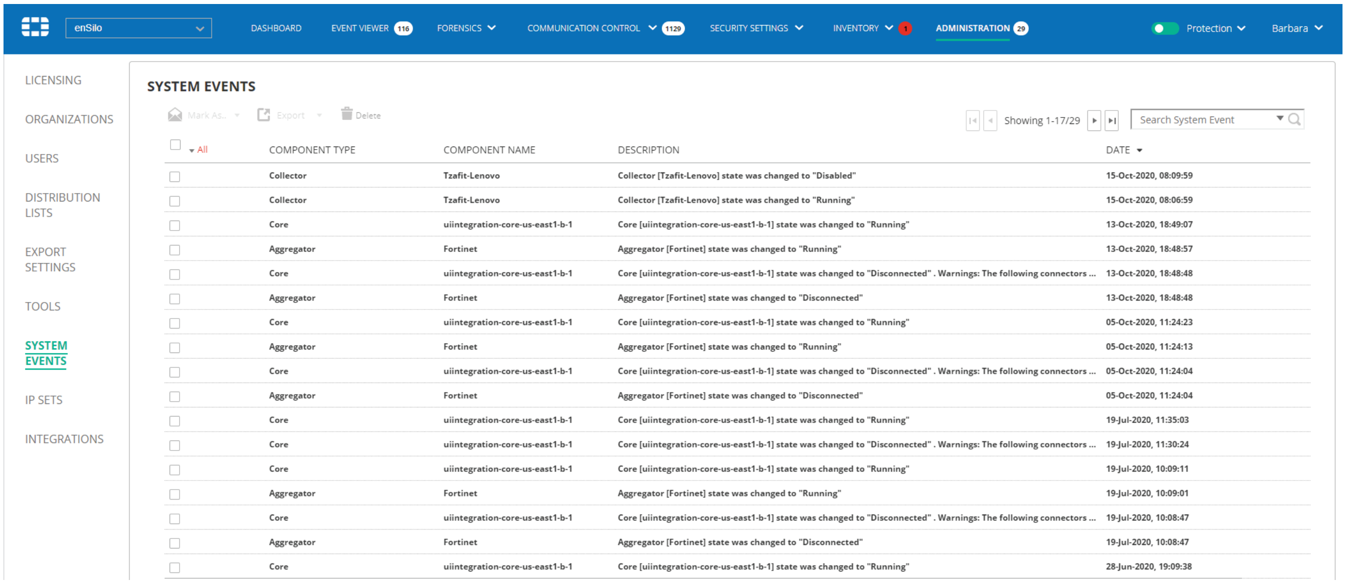
Have a question?
Get help

Help improve Windows Security
Give us feedback

Change your privacy settings
View and change privacy settings for your Windows 10 device.
Privacy settings
Privacy dashboard
Privacy Statement

System Events

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



SYSTEM EVENTS

□ All	COMPONENT TYPE	COMPONENT NAME	DESCRIPTION	DATE
□	Collector	Tzafit-Lenovo	Collector [Tzafit-Lenovo] state was changed to "Disabled"	15-Oct-2020, 08:09:59
□	Collector	Tzafit-Lenovo	Collector [Tzafit-Lenovo] state was changed to "Running"	15-Oct-2020, 08:06:59
□	Core	uiintegration-core-us-east1-b-1	Core [uiintegration-core-us-east1-b-1] state was changed to "Running"	13-Oct-2020, 18:49:07
□	Aggregator	Fortinet	Aggregator [Fortinet] state was changed to "Running"	13-Oct-2020, 18:48:57
□	Core	uiintegration-core-us-east1-b-1	Core [uiintegration-core-us-east1-b-1] state was changed to "Disconnected" . Warnings: The following connectors ...	13-Oct-2020, 18:48:48
□	Aggregator	Fortinet	Aggregator [Fortinet] state was changed to "Disconnected"	13-Oct-2020, 18:48:48
□	Core	uiintegration-core-us-east1-b-1	Core [uiintegration-core-us-east1-b-1] state was changed to "Running"	05-Oct-2020, 11:24:23
□	Aggregator	Fortinet	Aggregator [Fortinet] state was changed to "Running"	05-Oct-2020, 11:24:13
□	Core	uiintegration-core-us-east1-b-1	Core [uiintegration-core-us-east1-b-1] state was changed to "Disconnected" . Warnings: The following connectors ...	05-Oct-2020, 11:24:04
□	Aggregator	Fortinet	Aggregator [Fortinet] state was changed to "Disconnected"	05-Oct-2020, 11:24:04
□	Core	uiintegration-core-us-east1-b-1	Core [uiintegration-core-us-east1-b-1] state was changed to "Running"	19-Jul-2020, 11:35:03
□	Core	uiintegration-core-us-east1-b-1	Core [uiintegration-core-us-east1-b-1] state was changed to "Disconnected" . Warnings: The following connectors ...	19-Jul-2020, 11:30:24
□	Core	uiintegration-core-us-east1-b-1	Core [uiintegration-core-us-east1-b-1] state was changed to "Running"	19-Jul-2020, 10:09:11
□	Aggregator	Fortinet	Aggregator [Fortinet] state was changed to "Running"	19-Jul-2020, 10:09:01
□	Core	uiintegration-core-us-east1-b-1	Core [uiintegration-core-us-east1-b-1] state was changed to "Disconnected" . Warnings: The following connectors ...	19-Jul-2020, 10:08:47
□	Aggregator	Fortinet	Aggregator [Fortinet] state was changed to "Disconnected"	19-Jul-2020, 10:08:47
□	Core	uiintegration-core-us-east1-b-1	Core [uiintegration-core-us-east1-b-1] state was changed to "Running"	28-Jun-2020, 19:09:38

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 203.

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

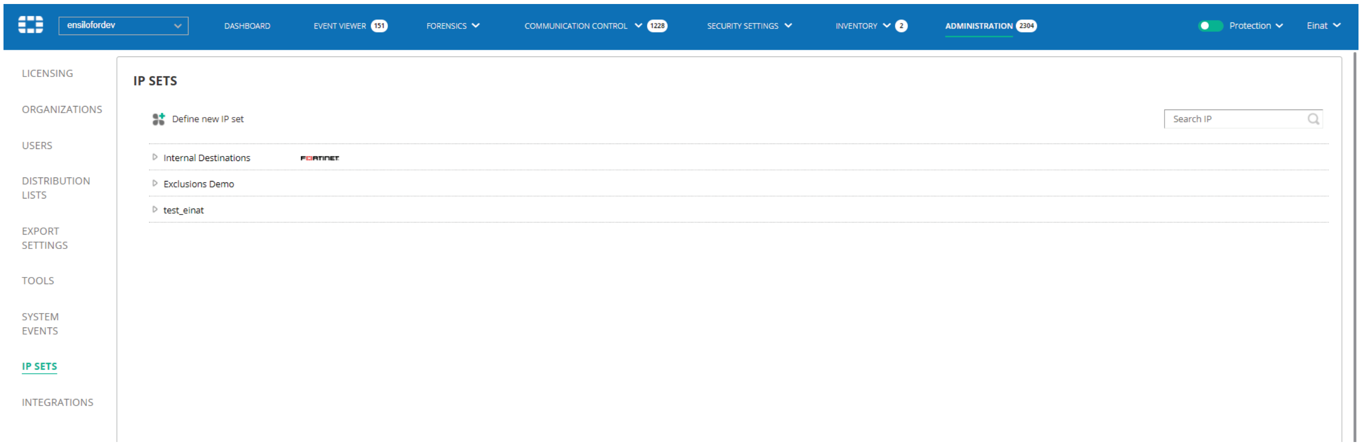
Each time a new system event is created, it can be sent through the Syslog.

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

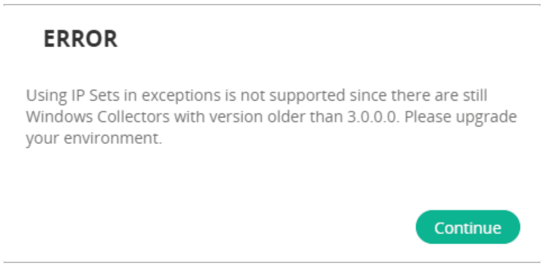
IP Sets enable you to define a set(s) of IPs to include or exclude for some security events. This feature is used when defining exceptions.



IP SETS

- Internal Destinations FORTINET
- Exclusions Demo
- test_einat

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:



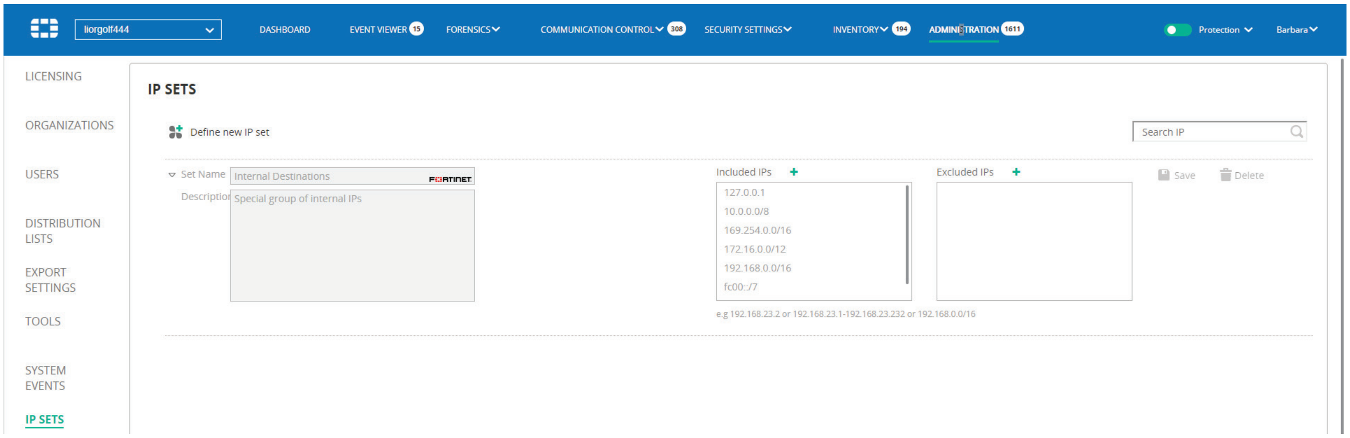
ERROR

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

Each row in the IP Sets window represents an IP inclusion/exclusion definition. The **Internal Destinations** row is provided by default (as indicated by the adjacent FortiEDR logo), which defines the default IPs that are included in and excluded from the FortiEDR system. All organizations in a multi-organization system are provided with this default IP set. In a single-organization system, the main organization is provided with it. The Internal Destinations IP set cannot be deleted. However, an Administrator can add Included IPs or Excluded IPs to it.

The IP Sets 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:



IP SETS

Set Name: Internal Destinations FORTINET

Descriptior: Special group of internal IPs

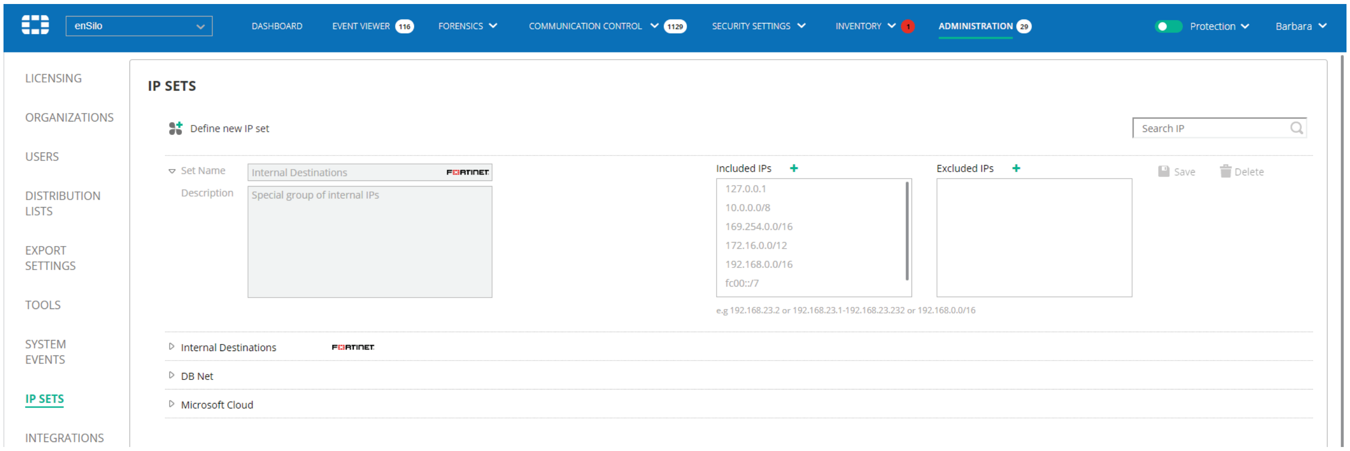
Included IPs:
127.0.0.1
10.0.0.0/8
169.254.0.0/16
172.16.0.0/12
192.168.0.0/16
fc00::/7

Excluded IPs:

e.g 192.168.23.2 or 192.168.23.1-192.168.23.232 or 192.168.0.0/16

To define an IP set:

1. Click the Define new IP set button. The following window displays:



IP SETS

Set Name: Internal Destinations

Description: Special group of internal IPs

Included IPs ✚

127.0.0.1
10.0.0.0/8
169.254.0.0/16
172.16.0.0/12
192.168.0.0/16
fc00::/7

Excluded IPs ✚

e.g 192.168.23.2 or 192.168.23.1-192.168.23.232 or 192.168.0.0/16

- Internal Destinations
- DB Net
- Microsoft Cloud

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 110 and 111.

Integrations

Integrations enable you to configure connectors to external systems. FortiEDR connectors utilize Fortinet products' APIs to automatically perform the required actions in order 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.

Note – The Integration menu is only available when the environment is connected to Fortinet Cloud Services (FCS).

Firewall Integration

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

Before you start firewall configuration, make sure that:

- Your FortiEDR deployment includes a JumpBox that has connectivity to the firewall.
  Details about how to install a FortiEDR Core and configure it as a JumpBox are described in *Installing the FortiEDR Core*. You may refer to page 86 for more information about configuring a JumpBox.
- The FortiEDR Central Manager has connectivity to the Fortinet Cloud Services (FCS).
- You have a valid API user with access to the external firewall.

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

The example below describes how to define an address group on FortiGate and associate it with a FortiGate policy rule, such that it blocks connections to the addresses in the group. The address group is then used when configuring the FortiEDR connector so that it is automatically populated with malicious destinations upon detection by FortiEDR.

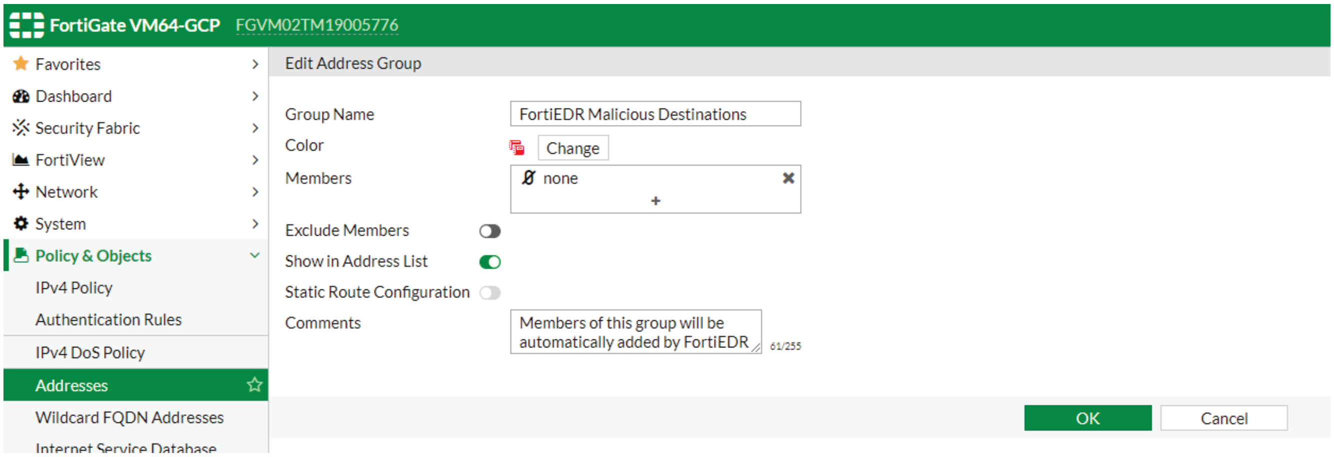
The same address group can obviously be used for multiple firewall policies in order to cover any VLAN-to-WAN interface in the network.

FortiGate Configuration

To set up an address group and policy on FortiGate:

1 Go to **Policy & Objects ➔ Addresses**.

2 Create a new address group to be populated by FortiEDR. The new address group now appears in the FortiGate Addresses table.

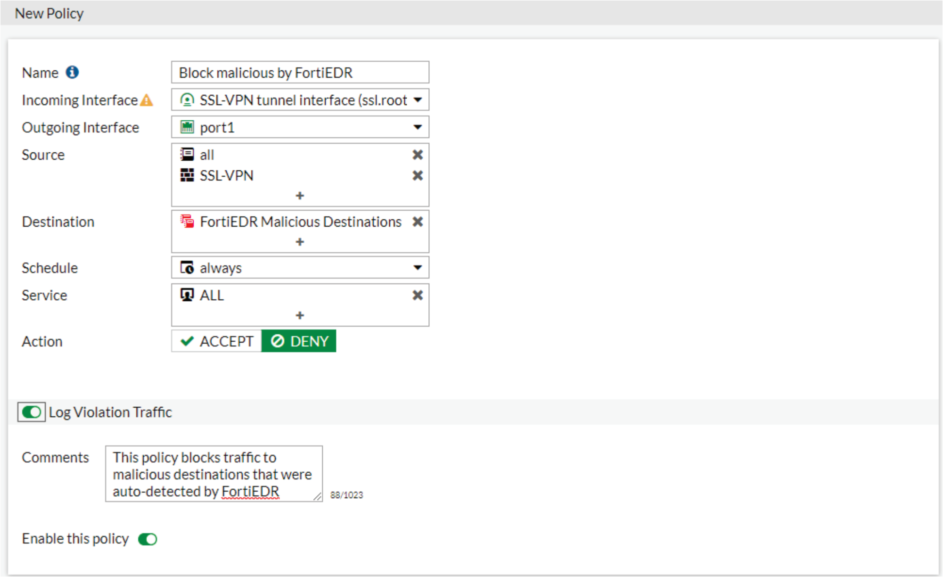


Edit Address Group

Group Name	FortiEDR Malicious Destinations
Color	Change
Members	none
Exclude Members	○
Show in Address List	●
Static Route Configuration	○
Comments	Members of this group will be automatically added by FortiEDR 61/255

3 Go to **Policy & Objects ➔ IPv4 Policy**.

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


New Policy

Name	Block malicious by FortiEDR
Incoming Interface	SSL-VPN tunnel interface (ssl.root
Outgoing Interface	port1
Source	all SSL-VPN
Destination	FortiEDR Malicious Destinations
Schedule	always
Service	ALL
Action	✓ ACCEPT [✓ DENY]

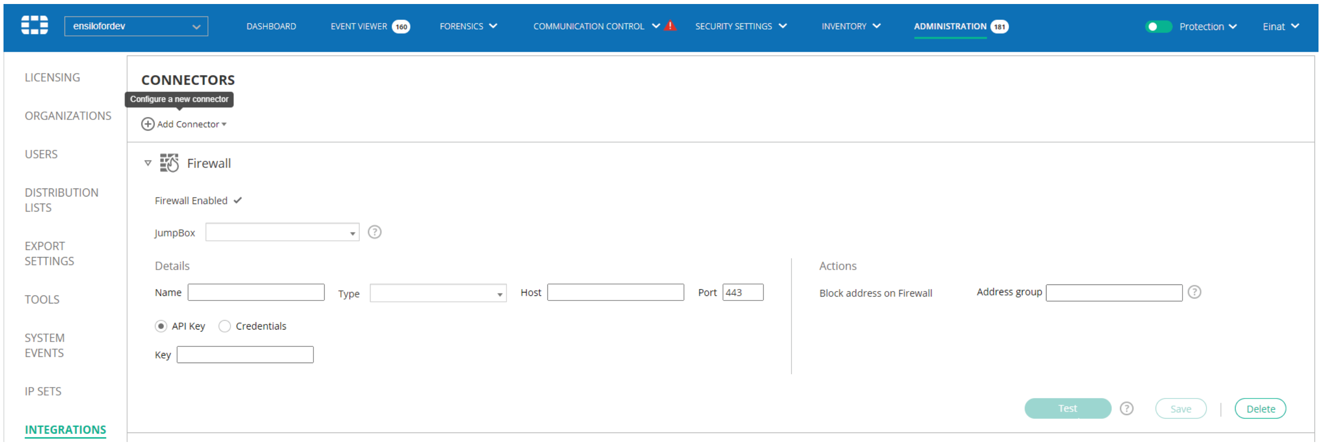
● Log Violation Traffic

Comments	This policy blocks traffic to malicious destinations that were auto-detected by FortiEDR 88/1023
Enable this policy	●

FortiEDR Connector Configuration

To set up a firewall connector with FortiEDR:

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



Firewall Enabled ✓

JumpBox

Name | Type | Host | Port 443

● API Key ○ Credentials

Key

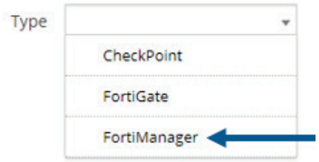
Block address on Firewall | Address group

2 Fill in the following fields:

- **Firewall Enabled:** Check this checkbox to enable blocking of malicious IP addresses by this firewall.
- **JumpBox:** Select the FortiEDR JumpBox to communicate with the firewall.
- **Name:** Specify a name of your choice to be used to identify this firewall.
- **Type:** Select the type of firewall to be used in the dropdown list.
- **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.**

Note – If you are working with a FortiManager in order to manage firewalls, use the same instructions to integrate with the firewall, but select **FortiManager** as the integrated device **Type** when configuring the FortiEDR Connector in the **Administration ➔ Integration** page, as follows:

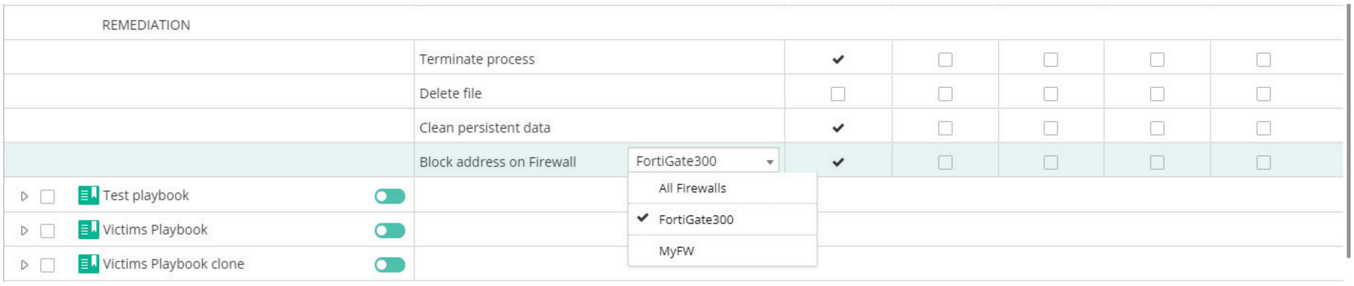


Playbooks Configuration

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

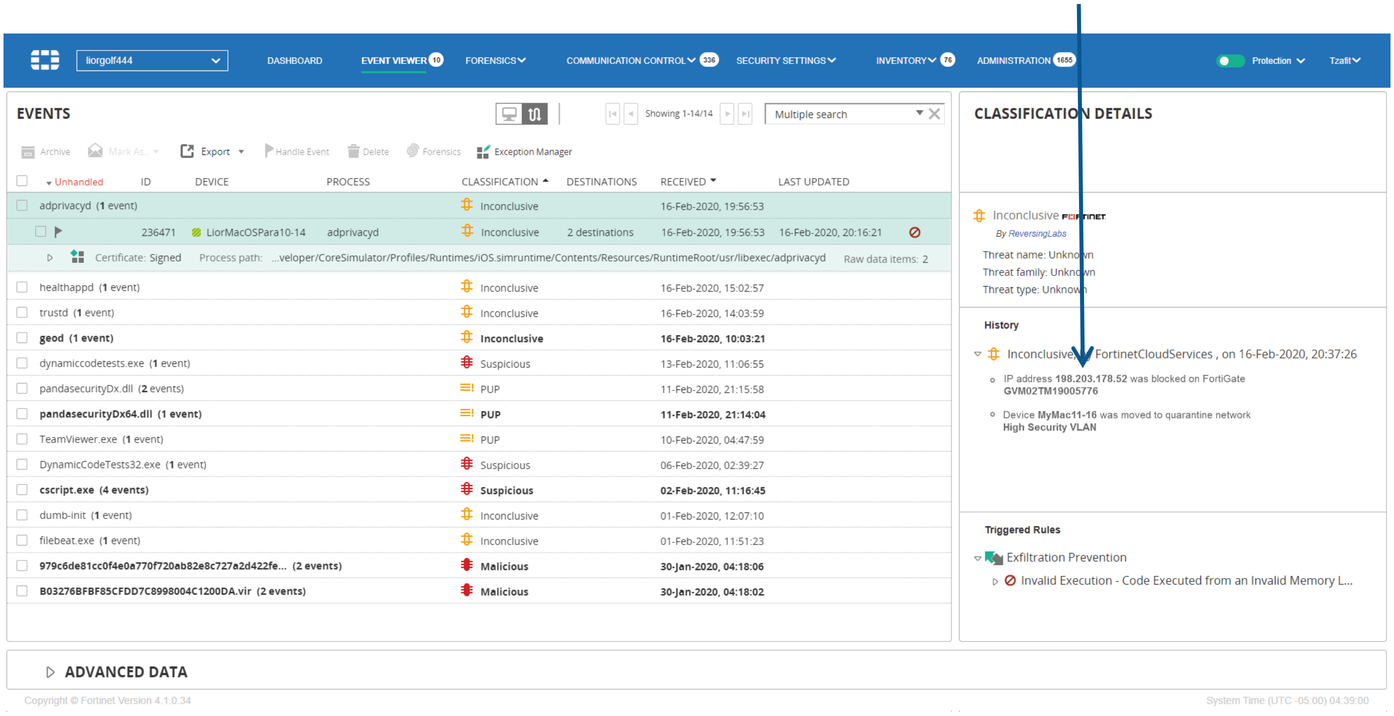
1 Navigate to the **SECURITY SETTINGS** ➔ **Playbooks** page.

2 Open the Playbook policy that is applied on devices for which you want the block IP incident response to apply and place a checkmark ✔ in the relevant **Classification** column next to the **Block address on Firewall** row that is under the REMEDIATION section. In the dropdown menu next to the action, you can specify which firewalls to use to perform the block or select all of them, as shown below:



REMEDIATION						
	Terminate process	✓	□	□	□	□
	Delete file	□	□	□	□	□
	Clean persistent data	✓	□	□	□	□
	Block address on Firewall FortiGate300 ▾	✓	□	□	□	□
▷ □ Test playbook	All Firewalls					
▷ □ Victims Playbook	✓ FortiGate300					
▷ □ Victims Playbook clone	MyFW					

FortiEDR is now configured to add malicious IP addresses to the blocking policy on the firewall upon triggering of a security event. You can check that malicious IP addresses are added to the address group that was configured on the firewall following FortiEDR security events. In addition, automatic incident response actions are listed in the CLASSIFICATION DETAILS area of the **Events** page of the FortiEDR Console, as shown below:



EVENTS

Unhandled	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
adprivacyd (1 event)				Inconclusive		16-Feb-2020, 19:56:53	
	236471	LiorMacOSPara10-14	adprivacyd	Inconclusive	2 destinations	16-Feb-2020, 19:56:53	16-Feb-2020, 20:16:21
Certificate: Signed	Process path: ...veloper/CoreSimulator/Profiles/Runtimes/iOS.simruntime/Contents/Resources/RuntimeRoot/usr/libexec/adprivacyd					Raw data items: 2	
healthappd (1 event)				Inconclusive		16-Feb-2020, 15:02:57	
trustd (1 event)				Inconclusive		16-Feb-2020, 14:03:59	
geod (1 event)				**Inconclusive**		**16-Feb-2020, 10:03:21**	
dynamiccodetests.exe (1 event)				Suspicious		13-Feb-2020, 11:06:55	
pandasecurityDx.dll (2 events)				PUP		11-Feb-2020, 21:15:58	
pandasecurityDx64.dll (1 event)				**PUP**		**11-Feb-2020, 21:14:04**	
TeamViewer.exe (1 event)				PUP		10-Feb-2020, 04:47:59	
DynamicCodeTests32.exe (1 event)				Suspicious		06-Feb-2020, 02:39:27	
cscript.exe (4 events)				**Suspicious**		**02-Feb-2020, 11:16:45**	
dumb-init (1 event)				Inconclusive		01-Feb-2020, 12:07:10	
filebeat.exe (1 event)				Inconclusive		01-Feb-2020, 11:51:23	
979c6de81cc0f4e0a770f720ab82e8c727a2d422fe... (2 events)				**Malicious**		**30-Jan-2020, 04:18:06**	
B03276BFBF85CFDD7C8998004C1200DA.vir (2 events)				**Malicious**		**30-Jan-2020, 04:18:02**	

CLASSIFICATION DETAILS

Inconclusive FORTINET
By ReversingLabs
Threat name: Unknown
Threat family: Unknown
Threat type: Unknown

History

Inconclusive, by FortinetCloudServices , on 16-Feb-2020, 20:37:26

- IP address **198.203.178.52** was blocked on FortiGate **GVM02TM19005776**
- Device **MyMac11-16** was moved to quarantine network **High Security VLAN**

Triggered Rules

Exfiltration Prevention
- Invalid Execution - Code Executed from an Invalid Memory L...

Copyright © Fortinet Version 4.1.0.34

System Time (UTC -05:00) 04:39:00

Sandbox Integration

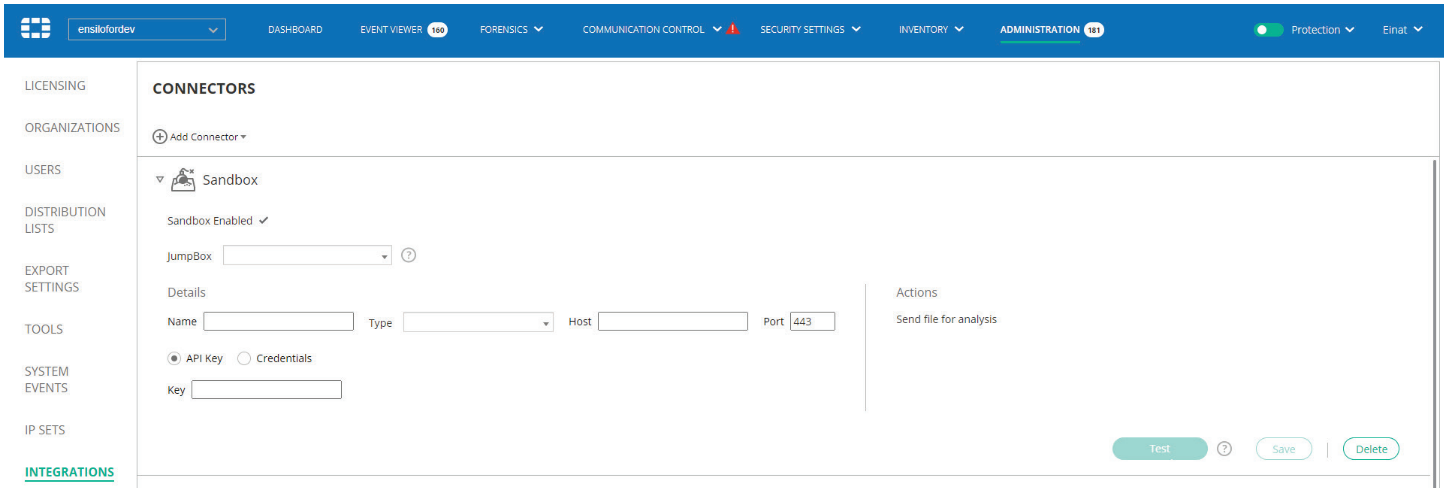
When a sandbox such as FortiSandbox is configured and the Sandbox Analysis Policy rule is enabled, files that meet several conditions and that have not been previously analyzed trigger a sandbox analysis event on FortiEDR and are sent to the sandbox. The conditions are a combination of several items, such as the file was downloaded from the Internet and was not signed by a known vendor. If the file is found to be clean, the event is automatically classified as safe and is archived. If the file is determined by the sandbox to be suspicious or malicious, then the event is classified as non-safe and any future execution attempt of the file in the environment is blocked by one of the Pre-execution (NGAV) Policy rules. Note that in all cases the first file execution is not delayed or blocked.

Before you start sandbox configuration, make sure that:

- Your FortiEDR deployment includes a JumpBox that has connectivity to the sandbox.
  Details about how to install a FortiEDR Core and configure it as a JumpBox are described in *Installing the FortiEDR Core*. You may refer to page 86 for more information about configuring a JumpBox.
- The FortiEDR Central Manager has connectivity to Fortinet Cloud Services (FCS).
- You have a valid API user with access to the sandbox.

To set up a sandbox connector with FortiEDR:

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



Sandbox Enabled ✓

JumpBox

Details

Name Type Host Port 443

● API Key ○ Credentials

Key

Actions

Send file for analysis

2 Fill in the following fields:

- **Enabled:** Check this checkbox to enable file investigation with this sandbox.
- **JumpBox:** Select the FortiEDR JumpBox that will communicate with the sandbox.
- **Name:** Specify a name of your choice which will be used to identify this sandbox.
- **Type:** Select the type of sandbox to be used in the dropdown list.
- **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.

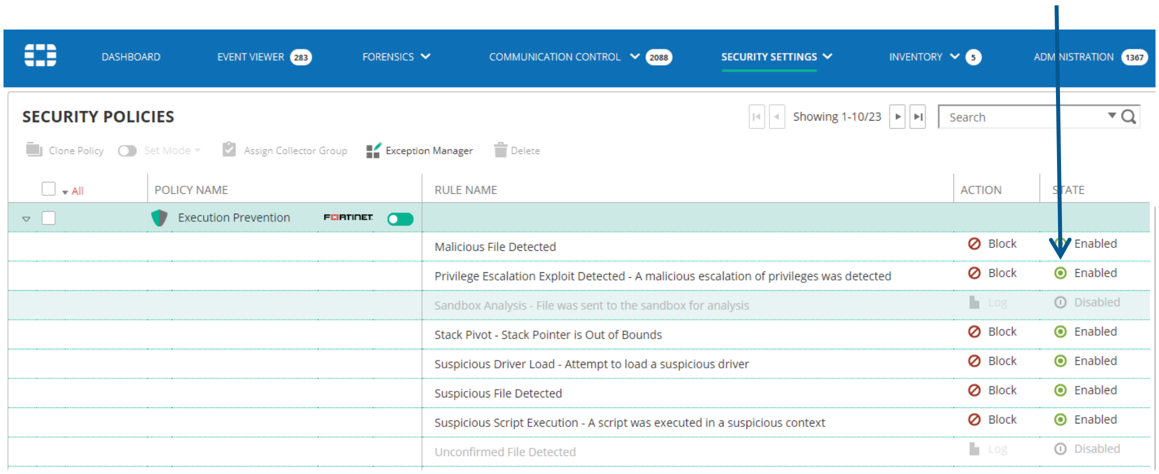
3 Click **Save**.

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:



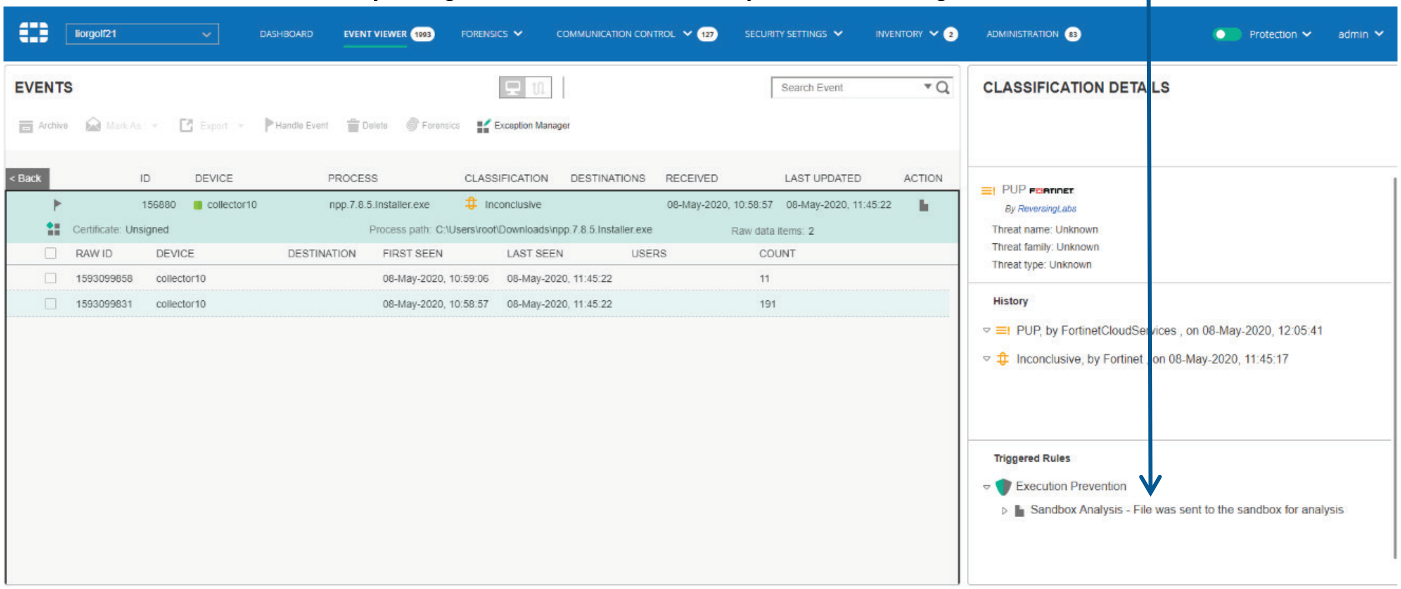
SECURITY POLICIES

☐ All	POLICY NAME	RULE NAME	ACTION	STATE
☐	Execution Prevention FORTINET			
		Malicious File Detected	Block	Enabled
		Privilege Escalation Exploit Detected - A malicious escalation of privileges was detected	Block	Enabled
		Sandbox Analysis - File was sent to the sandbox for analysis	Log	Disabled
		Stack Pivot - Stack Pointer is Out of Bounds	Block	Enabled
		Suspicious Driver Load - Attempt to load a suspicious driver	Block	Enabled
		Suspicious File Detected	Block	Enabled
		Suspicious Script Execution - A script was executed in a suspicious context	Block	Enabled
		Unconfirmed File Detected	Log	Disabled

FortiEDR is now configured to send unknown files to the sandbox.

You can check file analysis on your sandbox console.

In addition, you can see sandbox analysis events in the **Events** page. Events of files that were found to be clean appear under the **Archived Events** filter and events of files that were found to be risky are displayed under the **All** filter, such as shown below. A sandbox analysis digest is added to the security event's handling comment.



EVENTS

ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED	ACTION
156880	collector10	npp.7.8.5.Installer.exe	Inconclusive		08-May-2020, 10:58:57	08-May-2020, 11:45:22	

Certificate: Unsigned Process path: C:\Users\root\Downloads\npp.7.8.5.Installer.exe Raw data items: 2

☐	RAW ID	DEVICE	DESTINATION	FIRST SEEN	LAST SEEN	USERS	COUNT
☐	1593099858	collector10		08-May-2020, 10:59:06	08-May-2020, 11:45:22		11
☐	1593099831	collector10		08-May-2020, 10:58:57	08-May-2020, 11:45:22		191

CLASSIFICATION DETAILS

PUP FORTINET
By ReversingLabs
Threat name: Unknown
Threat family: Unknown
Threat type: Unknown

History
PUP, by FortinetCloudServices , on 08-May-2020, 12:05:41
Inconclusive, by Fortinet , on 08-May-2020, 11:45:17

Triggered Rules
Execution Prevention
Sandbox Analysis - File was sent to the sandbox for analysis

Network Access Control Integration

When a Network Access Control connector such as FortiNAC is set and Playbook policies are configured, automatic incident response actions can include isolating a device by a NAC system upon security event triggering.

Before you start NAC configuration, make sure that:

- Your FortiEDR deployment includes a JumpBox that has connectivity to the NAC server.
  Details about how to install a FortiEDR Core and configure it as a JumpBox are described in *Installing the FortiEDR Core*. You may refer to page 86 for more information about configuring a JumpBox.

- The FortiEDR Central Manager has connectivity to the Fortinet Cloud Services (FCS).
- You have a valid API user with access to FortiNAC or equivalent network access control system.

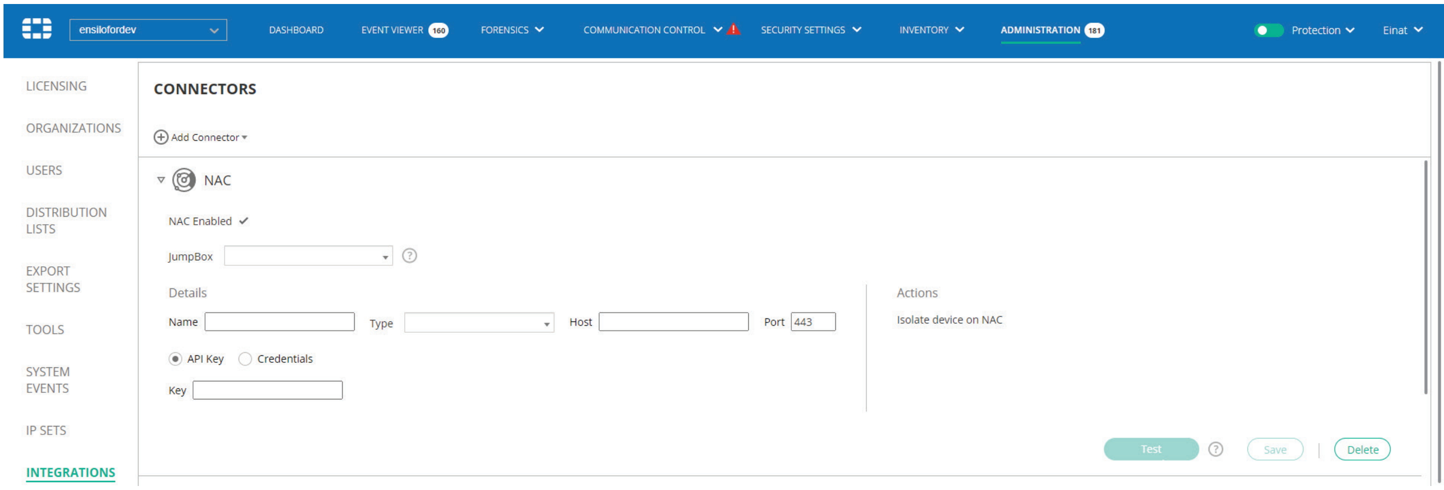
Follow the steps below in order to automatically isolate a device by NAC upon the detection of a FortiEDR security event. The example below describes how to define an API user on FortiNAC in order to enable FortiEDR to perform automatic device isolation after a FortiEDR security event.

Note: Make sure to add FortiEDR domains and/or IP addresses to the exclusion list on the VLAN that is being used for isolation on the FortiNAC system such that the FortiEDR Collector would still be able to communicate with its servers when the device is being isolated.

FortiEDR Connector Configuration

To configure NAC integration:

1 Click the ⊕ Add Connector ▾ button and select NAC in the Connectors dropdown list. The following displays:



NAC Enabled ✓

JumpBox

Details

Name | Type | Host | Port 443

● API Key ○ Credentials

Key

Actions

Isolate device on NAC

2 Fill in the following fields:

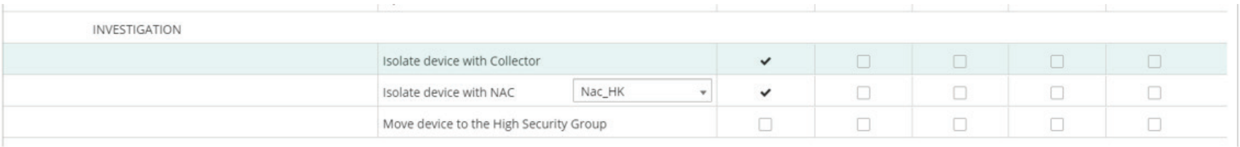
- NAC Enabled: Check this checkbox to enable FortiEDR integration with this external NAC system.
- JumpBox: Select the FortiEDR JumpBox that will communicate with this NAC system.
- Name: Specify a name of your choice which will be used to identify this NAC system.
- Type: Select the type of NAC to be used in the dropdown list, for example: FortiNAC.
- Host: Specify the IP or DNS address of the external NAC system.
- Port: Specify the port that is used for communication with the external NAC system.
- API Key / Credentials: Specify authentication details of the external NAC system. To use an API token, click the API Key radio button and copy the token value into the text box. To use API credentials, click the Credentials radio button and fill in the external NAC system API username and password.

3 Click **Save**.

Playbooks Configuration

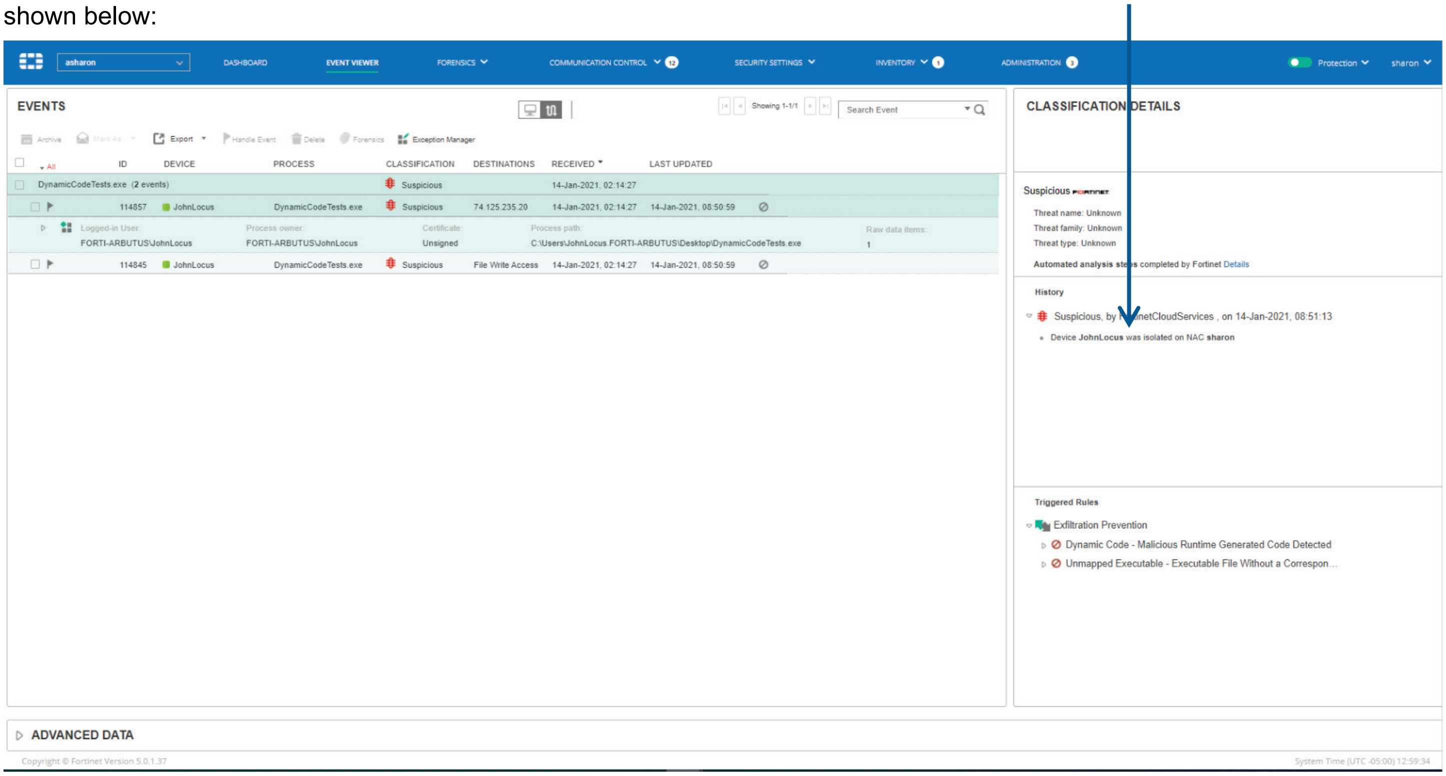
To configure an automated incident response that uses a NAC connector to isolate a device upon security event triggering:

1. Navigate to the **SECURITY SETTINGS** ➔ **Playbooks** page.
2. Open the Playbook policy that is applied on devices for which you want the isolation response to apply and place a checkmark ✔ in the relevant Classification column next to the Isolate device with NAC row that is under the INVESTIGATION section.



INVESTIGATION						
	Isolate device with Collector	✓	□	□	□	□
	Isolate device with NAC — Nac_HK	✓	□	□	□	□
	Move device to the High Security Group	□	□	□	□	□

FortiEDR is now configured to automatically isolate the device upon triggering of a security event. Automatic incident response actions are listed in the CLASSIFICATION DETAILS area of the Events page of the FortiEDR Console as shown below:



EVENTS

All	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
DynamicCodeTests.exe (2 events)				Suspicious		14-Jan-2021, 02:14:27	
	114857	JohnLocus	DynamicCodeTests.exe	Suspicious	74.125.235.20	14-Jan-2021, 02:14:27	14-Jan-2021, 08:50:59
	114845	JohnLocus	DynamicCodeTests.exe	Suspicious	File Write Access	14-Jan-2021, 02:14:27	14-Jan-2021, 08:50:59

Logged-in User: FORTI-ARBUTUS\JohnLocus
Process owner: FORTI-ARBUTUS\JohnLocus
Certificate: Unsigned
Process path: C:\Users\JohnLocus.FORTI-ARBUTUS\Desktop\DynamicCodeTests.exe
Raw data items: 1

CLASSIFICATION DETAILS

Suspicious FORTINET

Threat name: Unknown
Threat family: Unknown
Threat type: Unknown

Automated analysis steps completed by Fortinet Details

History

Suspicious, by FortinetCloudServices , on 14-Jan-2021, 08:51:13

- Device **JohnLocus** was isolated on NAC **sharon**

Triggered Rules

Exfiltration Prevention
- Dynamic Code - Malicious Runtime Generated Code Detected
- Unmapped Executable - Executable File Without a Correspon...

Copyright © Fortinet Version 5.0.1.37

System Time (UTC -05:00) 12:59:34

Note that isolation by NAC will only be done for devices that are managed on the specified NAC.

eXtended Detection Source Integration

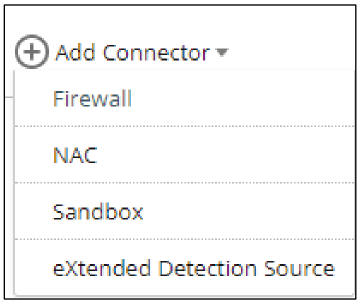
To connect to external systems in order to collect activity data, you must add a new connector for extended detection, which will automatically collect activity logs and activity data from external systems. Currently, this feature connects to a FortiAnalyzer device type, which collects the logs from other systems, such as firewalls, Active Directory and other security products. The aggregated data is then being sent to Fortinet Cloud Services (FCS) where it is correlated and analyzed to detect malicious indications that will result in security events of eXtended Detection policy rule violations.

Before you start configuring FortiAnalyzer configuration, verify that:

- Your FortiEDR deployment includes a JumpBox that has connectivity to FortiAnalyzer. Details about how to install a FortiEDR Core and configure it as a JumpBox are provided in *Installing the FortiEDR Core*. You may refer to page 86 for more information about configuring a JumpBox.
- The FortiEDR Central Manager has connectivity to the Fortinet Cloud Services (FCS).
- You have a valid API user that has access to FortiAnalyzer.

To set up an extended detection connector with FortiEDR:

1 Click the ⊕ Add Connector ▾ button and select eXtended Detection Source in the **Connectors** dropdown list



⊕ Add Connector ▾

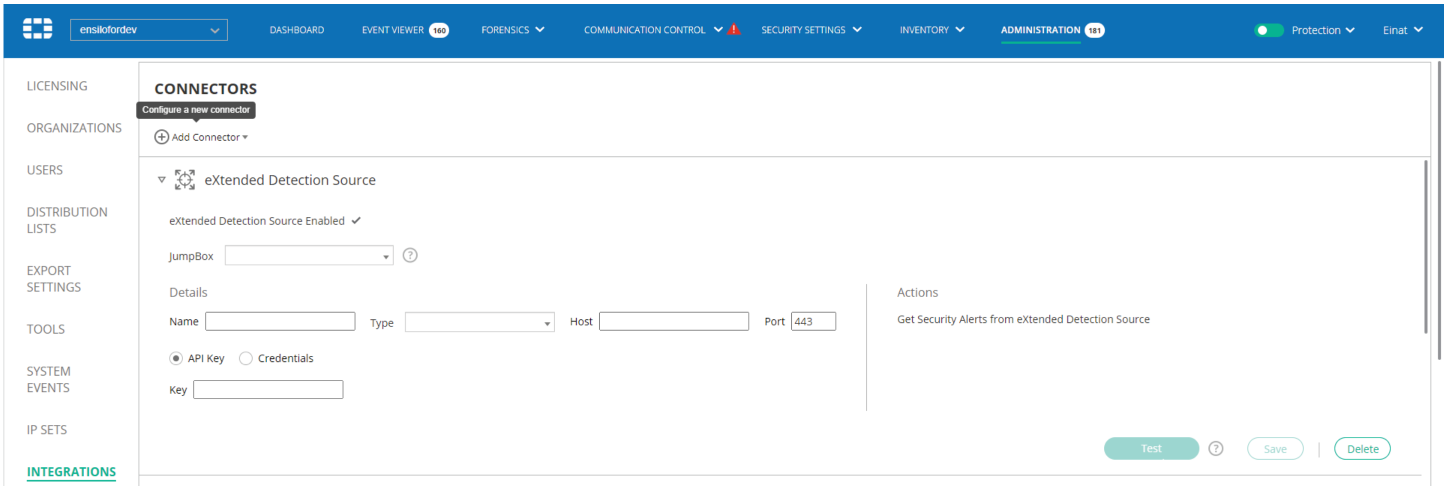
Firewall

NAC

Sandbox

eXtended Detection Source

The following displays:



CONNECTORS

eXtended Detection Source

eXtended Detection Source Enabled ✓

JumpBox

Details

Name Type Host Port 443

● API Key ○ Credentials

Key

Actions

Get Security Alerts from eXtended Detection Source

2 Fill in the following fields: **eXtended Detection Source Enabled:** Check this checkbox to enable blocking of malicious IP addresses by FortiAnalyzer.

- **JumpBox:** Select the FortiEDR JumpBox that will communicate with FortiAnalyzer.
- **Name:** Specify a name of your choice to be used to identify this connector.
- **Type:** Select the type of connector to be used in the dropdown list. Currently, only FortiAnalyzer is supported.
- **Host:** Specify the IP or DNS address of FortiAnalyzer.
- **Port:** Specify the port that is used for API communication with FortiAnalyzer.

- **API Key/Credentials:** Specify authentication details of FortiAnalyzer. 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 FortiAnalyzer API username and password.

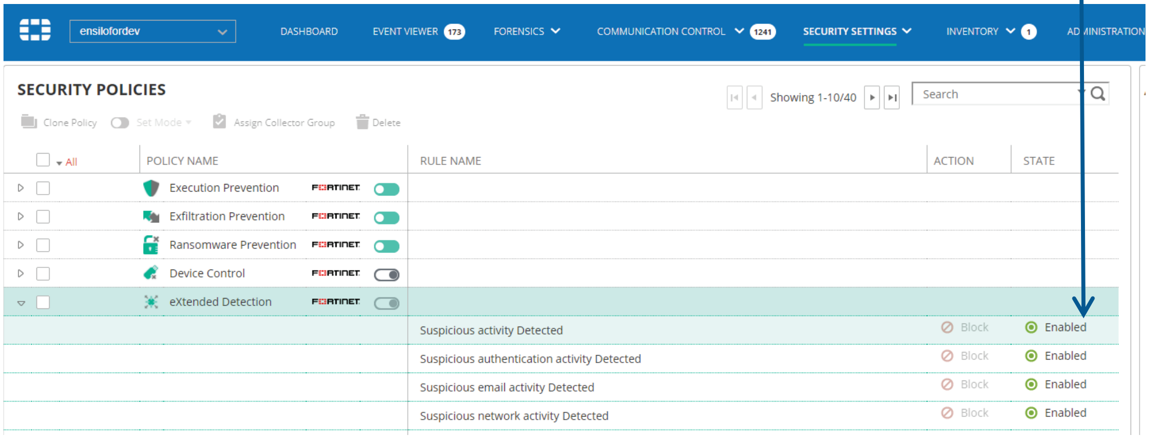
3 Click **Save.**

4 In order to complete eXtended Detection Source integration, the eXtended Detection rules must be enabled with the FortiEDR Central Manager, as follows.

To enable the eXtended Detection rules:

1 Navigate to the **SECURITY SETTINGS ➔ Security Policies** page.

2 Open the eXtended Detection policy that is applied on devices on which you want the eXtended detection policy to apply and click the **Disabled** button next to each of the underlying rules to enable it, as shown below:



SECURITY POLICIES

Showing 1-10/40

□ All	POLICY NAME	RULE NAME	ACTION	STATE
▷ □	Execution Prevention			
▷ □	Exfiltration Prevention			
▷ □	Ransomware Prevention			
▷ □	Device Control			
▽ □	eXtended Detection			
		Suspicious activity Detected	Block	Enabled
		Suspicious authentication activity Detected	Block	Enabled
		Suspicious email activity Detected	Block	Enabled
		Suspicious network activity Detected	Block	Enabled

FortiEDR is now configured to issue eXtended Detection alerts.

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 86 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 154.

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:

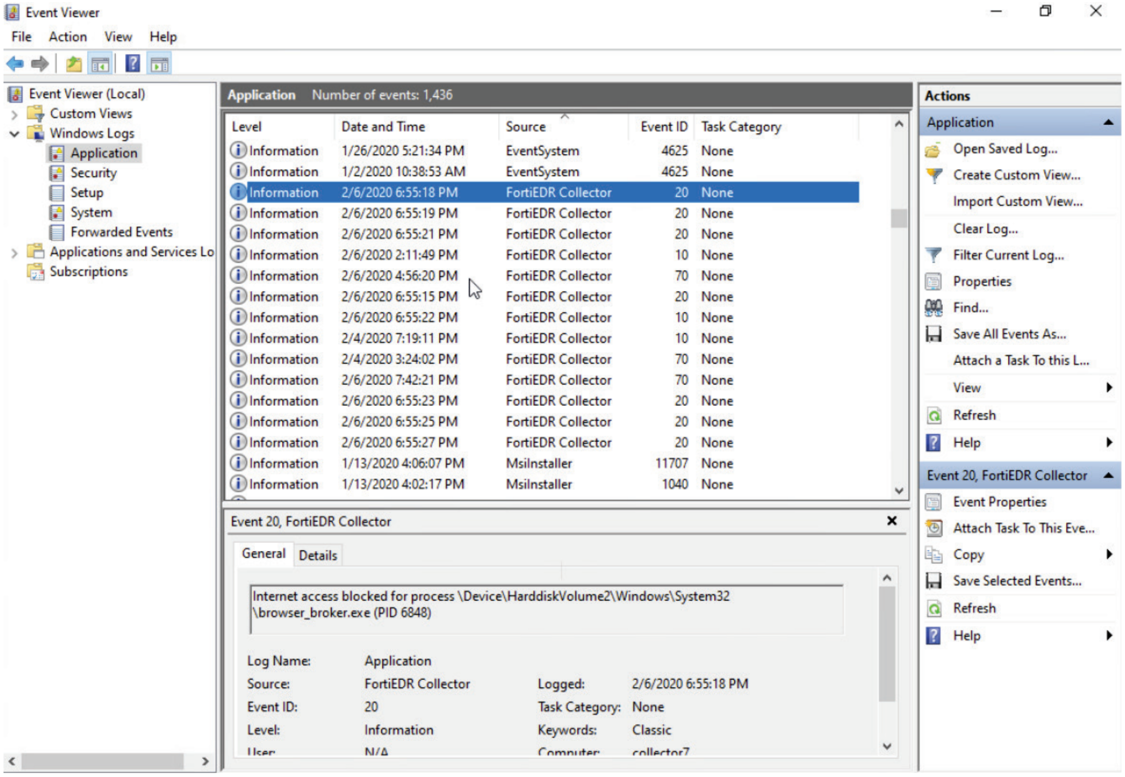
- Running Telnet on the FortiEDR Collector and connecting to the FortiEDR Core IP via port 555,
- Running Telnet on the FortiEDR Core and attempting to connect to the FortiEDR Aggregator IP on port 8081.

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**.



Application Number of events: 1,436

Level	Date and Time	Source	Event ID	Task Category
Information	1/26/2020 5:21:34 PM	EventSystem	4625	None
Information	1/2/2020 10:38:53 AM	EventSystem	4625	None
Information	2/6/2020 6:55:18 PM	FortiEDR Collector	20	None
Information	2/6/2020 6:55:19 PM	FortiEDR Collector	20	None
Information	2/6/2020 6:55:21 PM	FortiEDR Collector	20	None
Information	2/6/2020 2:11:49 PM	FortiEDR Collector	10	None
Information	2/6/2020 4:56:20 PM	FortiEDR Collector	70	None
Information	2/6/2020 6:55:15 PM	FortiEDR Collector	20	None
Information	2/6/2020 6:55:22 PM	FortiEDR Collector	10	None
Information	2/4/2020 7:19:11 PM	FortiEDR Collector	10	None
Information	2/4/2020 3:24:02 PM	FortiEDR Collector	70	None
Information	2/6/2020 7:42:21 PM	FortiEDR Collector	70	None
Information	2/6/2020 6:55:23 PM	FortiEDR Collector	20	None
Information	2/6/2020 6:55:25 PM	FortiEDR Collector	20	None
Information	2/6/2020 6:55:27 PM	FortiEDR Collector	20	None
Information	1/13/2020 4:06:07 PM	MsiInstaller	11707	None
Information	1/13/2020 4:02:17 PM	MsiInstaller	1040	None

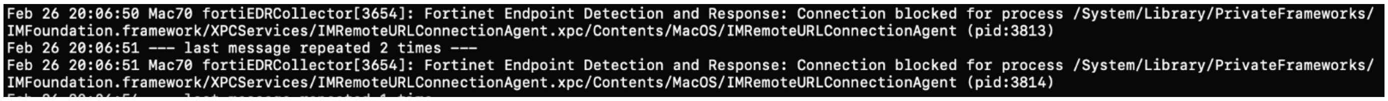
Event 20, FortiEDR Collector

Internet access blocked for process \Device\HarddiskVolume2\Windows\System32\browser_broker.exe (PID 6848)

Log Name:	Application		
Source:	FortiEDR Collector	Logged:	2/6/2020 6:55:18 PM
Event ID:	20	Task Category:	None
Level:	Information	Keywords:	Classic
User:	N/A	Computer:	collector7

MacOS-based Devices

The 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.

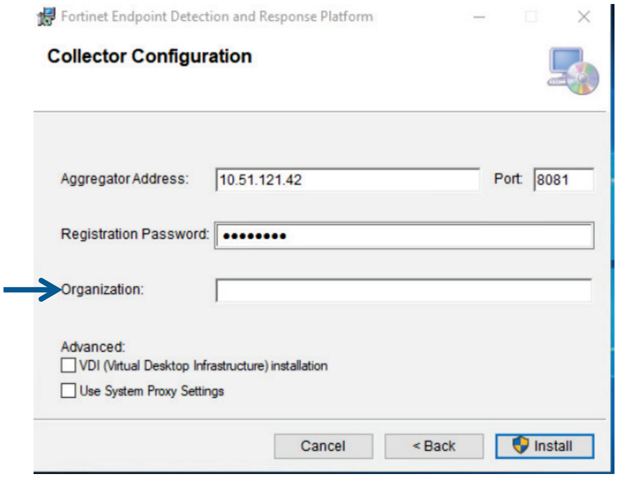
  Note – There must always be at least one Administrator in the system.

  - **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 security 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 178.

Component Registration in a Multi-organization Environment

Collector Registration

Each organization has its own registration password. The Collector installer specifies the Collector organization name. If the **Organization** field is left empty during installation, the Collector is added to the default Hoster account, as shown below:



Fortinet Endpoint Detection and Response Platform

Collector Configuration

Aggregator Address: 10.51.121.42 Port: 8081

Registration Password: ••••••••

Organization:

Advanced:

□ VDI (Virtual Desktop Infrastructure) installation

□ Use System Proxy Settings

After registration, the Collector receives the organization ID. You can rename the organization if preferred.

To specify the organization when installing from a command line, run the following command:

msiexec…\qn ORG=<organization name> AGG=

For more details about Collector installation, see the *Installing FortiEDR Collectors* section on page 34.

Core Registration

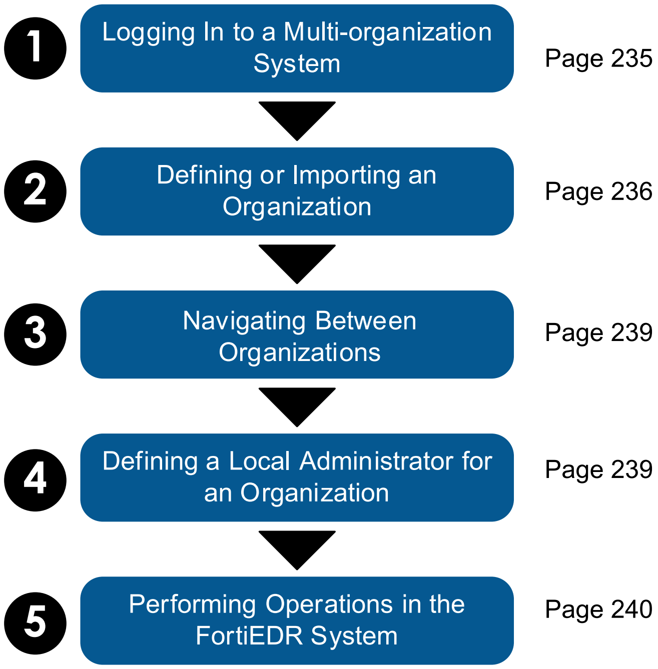
Most Cores are shared between organizations. It is possible to install a Core that belongs only to your organization by installing it on-premises. In this case, you must specify the organization during the Core installation process.

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 29.

Workflow

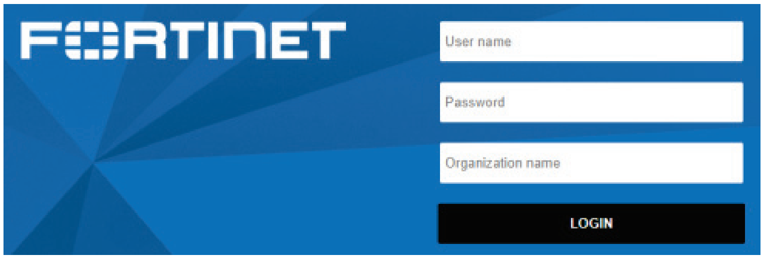
The following general workflow applies for Administrators when working in a FortiEDR multi-organization system:



1. Logging In to a Multi-organization System — Page 235
2. Defining or Importing an Organization — Page 236
3. Navigating Between Organizations — Page 239
4. Defining a Local Administrator for an Organization — Page 239
5. Performing Operations in the FortiEDR System — Page 240

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.

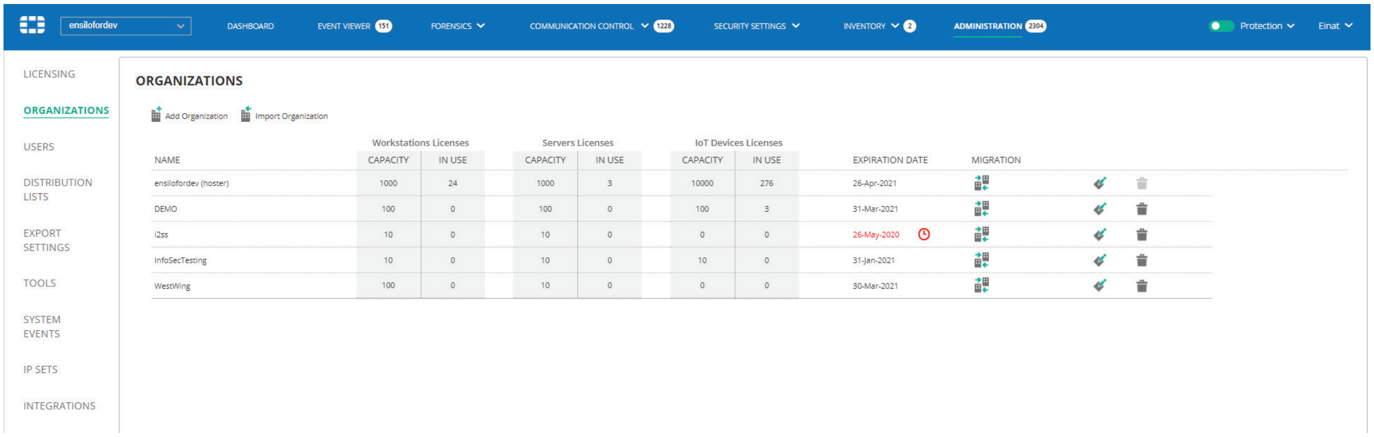


By default, Administrators are logged in to the main organization, and do not need to specify an organization in the **Organization Name** dropdown list.

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.



ORGANIZATIONS

	Workstations Licenses		Servers Licenses		IoT Devices Licenses			
NAME	CAPACITY	IN USE	CAPACITY	IN USE	CAPACITY	IN USE	EXPIRATION DATE	MIGRATION
ensilofordev (hoster)	1000	24	1000	3	10000	276	26-Apr-2021	
DEMO	100	0	100	0	100	3	31-Mar-2021	
i2ss	10	0	10	0	0	0	26-May-2020	
InfoSecTesting	10	0	10	0	10	0	31-Jan-2021	
WestWing	100	0	10	0	0	0	30-Mar-2021	

The **Default (hoster)** organization is predefined in the system. This organization represents the main organization in the system, such as the ABC Hotel chain described before. The Default (hoster) main organization cannot be deleted.

The Default (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 239.

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).
- **Servers Licenses Capacity:** For the organization, specifies the number of servers allocated to the organization.
- **Servers Licenses in Use:** Specifies the number of servers in use (installed).
- **IoT Devices Capacity:** For the organization, specifies the maximum number of IoT devices that can be detected in the organization.
- **IoT Devices in Use:** Specifies the number of IoT devices detected in the organization.
- **Expiration Date:** Specifies the expiration date of licenses for the organization.

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

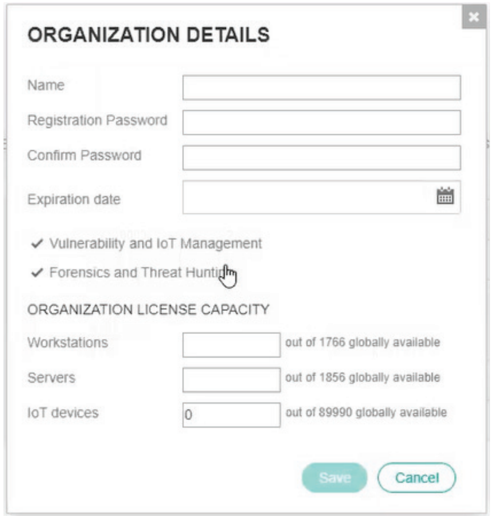
You can delete an organization as long as it does not have any workstations or servers in use. Click the **Delete** button in an organization row to delete that organization.

Click the **Migrate Organization** button in an organization row to migrate that organization. For more details, see page 241.

To define an organization:

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

2 Click the Add Organization button. The following window displays:



ORGANIZATION DETAILS

Name

Registration Password

Confirm Password

Expiration date

✓ Vulnerability and IoT Management

✓ Forensics and Threat Hunting

ORGANIZATION LICENSE CAPACITY

Workstations		out of 1766 globally available
Servers		out of 1856 globally available
IoT devices	0	out of 89990 globally available

Save Cancel

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.**

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 210.

- **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.

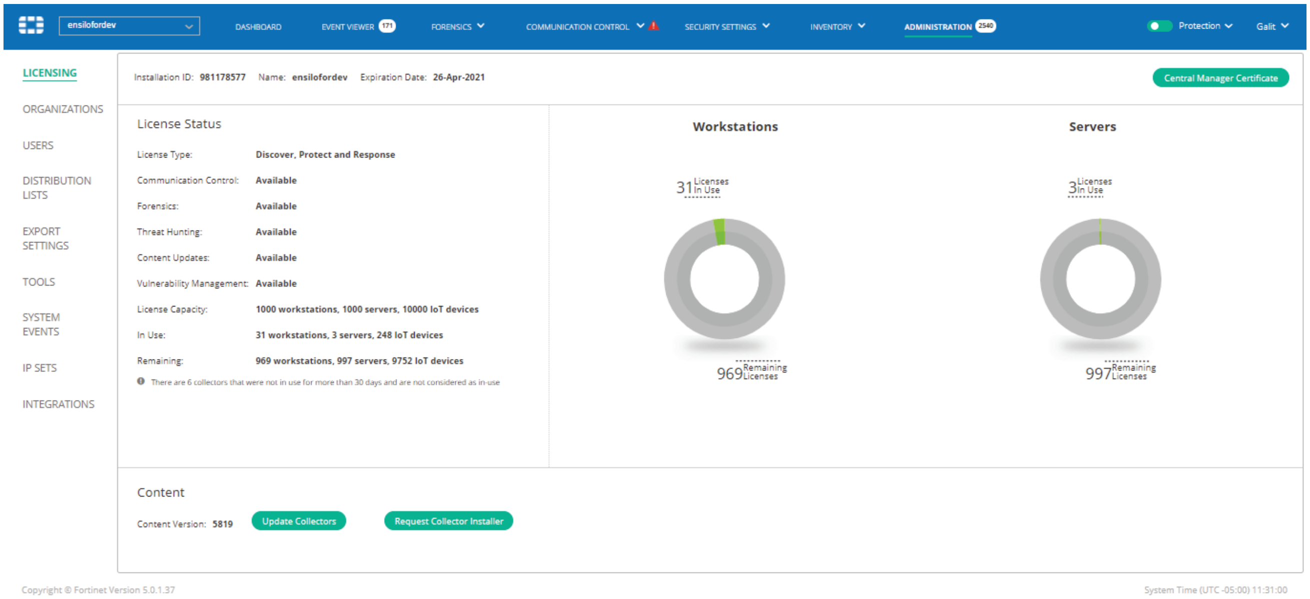
- **Vulnerability and IoT Management:** Check this checkbox for the organization to have access to these features. This option is only available on setups that have purchased a **Discover and Protect** license or **Discover, Protect and Response** license. See more details on license types on page 27.

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 **Discover, 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.



Installation ID: **981178577** Name: **ensilofordev** Expiration Date: **26-Apr-2021**

License Status

License Type:	**Discover, Protect and Response**
Communication Control:	**Available**
Forensics:	**Available**
Threat Hunting:	**Available**
Content Updates:	**Available**
Vulnerability Management:	**Available**
License Capacity:	**1000 workstations, 1000 servers, 10000 IoT devices**
In Use:	**31 workstations, 3 servers, 248 IoT devices**
Remaining:	**969 workstations, 997 servers, 9752 IoT devices**

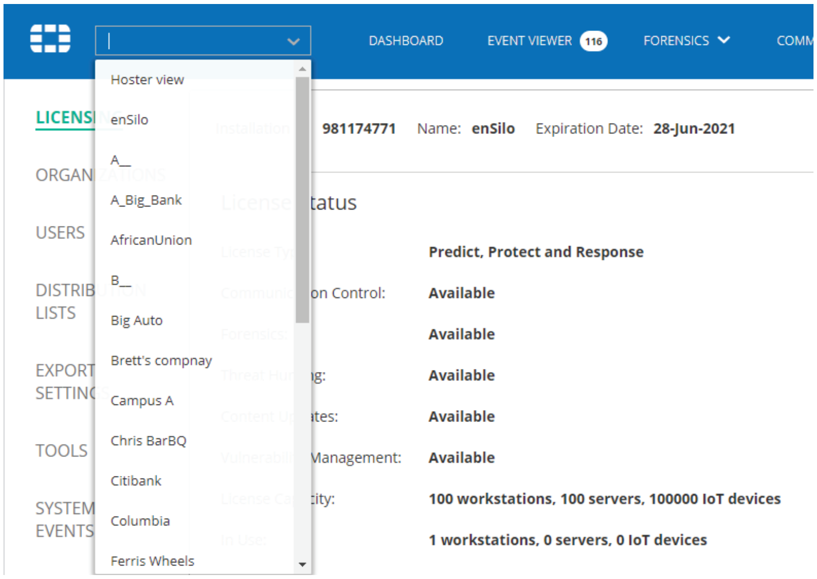
There are 6 collectors that were not in use for more than 30 days and are not considered as in-use

Content

Content Version: **5819**

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.

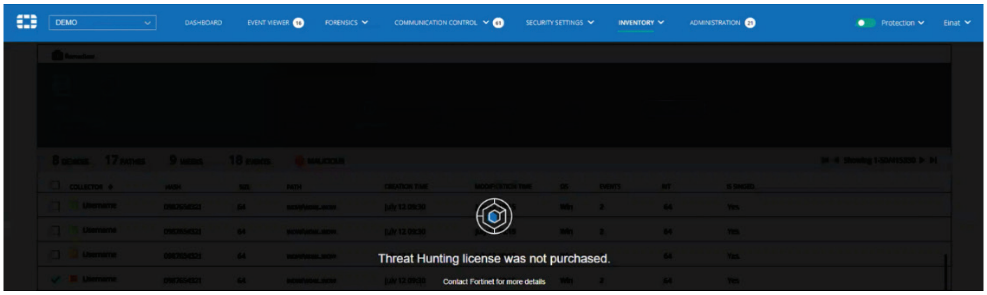


Installation 981174771 Name: **enSilo** Expiration Date: **28-Jun-2021**

License Status

License Type:	**Predict, Protect and Response**
Communication Control:	**Available**
Forensics:	**Available**
Threat Hunting:	**Available**
Content Updates:	**Available**
Vulnerability Management:	**Available**
License Capacity:	**100 workstations, 100 servers, 100000 IoT devices**
In Use:	**1 workstations, 0 servers, 0 IoT devices**

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.



Threat Hunting license was not purchased.

Contact Fortinet for more details

Moving from a Single-organization to Multi-organization Structure in FortiEDR

In a single-organization system, the Default (hoster) organization is the only organization.

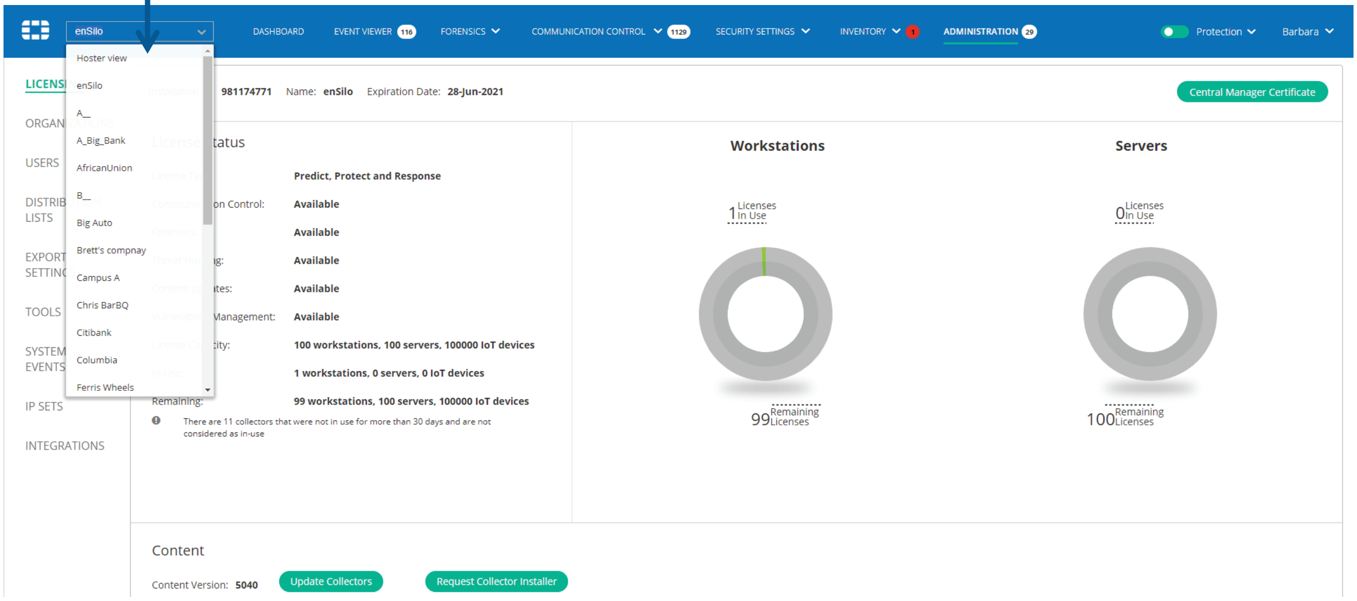
To create a multi-organization (multi-tenant) system, an Administrator simply needs to add one or more organizations to a single-organization system. When there are multiple organizations in the system, you can select the organization of interest in the **Organization** dropdown menu that appears at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

Step 3 –Navigating Between Organizations

In a multi-organization system, all types of information are now organized per organization.

Administrators can view information in the FortiEDR system for a specific organization or for all organizations together. To do so, use one of the following methods:

- 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 247.
- Select the organization of interest in the **Organization** dropdown list.



981174771 Name: enSilo Expiration Date: 28-Jun-2021

tatus

Predict, Protect and Response

on Control: Available

Available

g: Available

tes: Available

Management: Available

ity: 100 workstations, 100 servers, 100000 IoT devices

1 workstations, 0 servers, 0 IoT devices

Remaining: 99 workstations, 100 servers, 100000 IoT devices

There are 11 collectors that were not in use for more than 30 days and are not considered as in-use

Content

Content Version: 5040

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

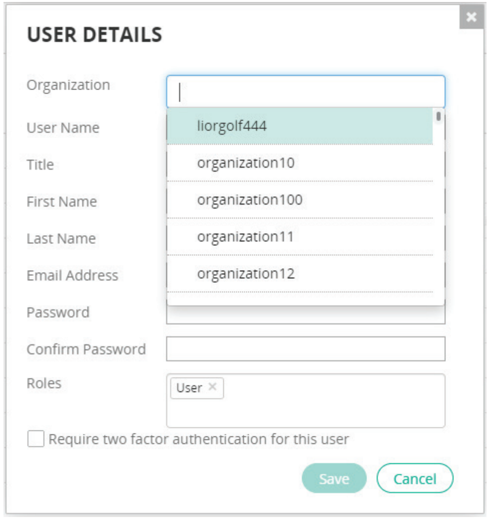
Administrators can create one or more Local Administrators for an organization. You should define at least one Local Administrator for each organization.

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 183, 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.



USER DETAILS

Organization
User Name
Title
First Name
Last Name
Email Address
Password
Confirm Password
Roles: User ×

☐ Require two factor authentication for this user

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

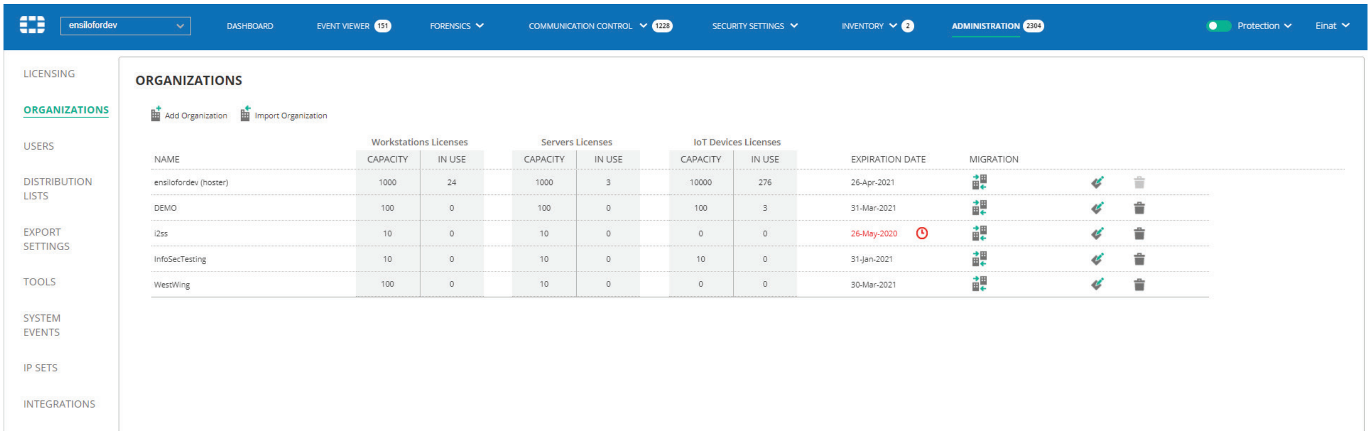
FortiEDR's Consolidation feature enables you to copy all the data and definitions within an organization from one environment to another environment. This feature copies an organization from one environment (source setup/environment) to another (destination setup/environment). The copy operation adds 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:

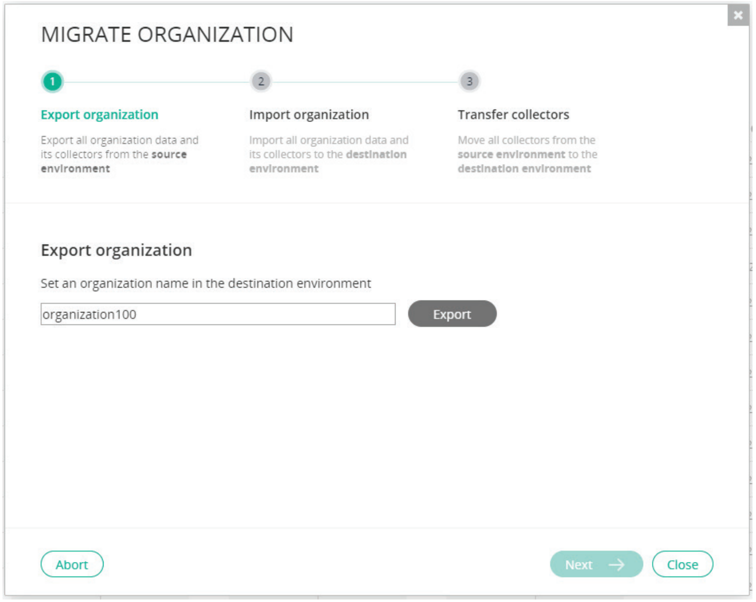
1 Click the **ADMINISTRATION** tab and then click **ORGANIZATIONS** in the left pane. The Organizations window displays.



ORGANIZATIONS

	Workstations Licenses		Servers Licenses		IoT Devices Licenses			
NAME	CAPACITY	IN USE	CAPACITY	IN USE	CAPACITY	IN USE	EXPIRATION DATE	MIGRATION
ensilofordev (hoster)	1000	24	1000	3	10000	276	26-Apr-2021	
DEMO	100	0	100	0	100	3	31-Mar-2021	
i2ss	10	0	10	0	0	0	26-May-2020	
InfoSecTesting	10	0	10	0	10	0	31-Jan-2021	
WestWing	100	0	10	0	0	0	30-Mar-2021	

2 Click the **Migrate organization** button in the row of the source organization that you want to copy to another environment. The following window displays:



MIGRATE ORGANIZATION

1 Export organization
Export all organization data and its collectors from the **source environment**

2 Import organization
Import all organization data and its collectors to the **destination environment**

3 Transfer collectors
Move all collectors from the **source environment** to the **destination environment**

Export organization

Set an organization name in the destination environment

organization100

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

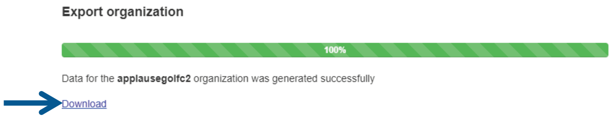
- **Step 1, Export the Organization:** This step exports all the data of the selected organization to a zip file.
- **Step 2, Import the Organization:** This step imports all the organization's data using the zip file exported in step 1. Note that this step is performed on the destination environment.
- **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:



Export organization

100%

Data for the **applausegolfc2** organization was generated successfully

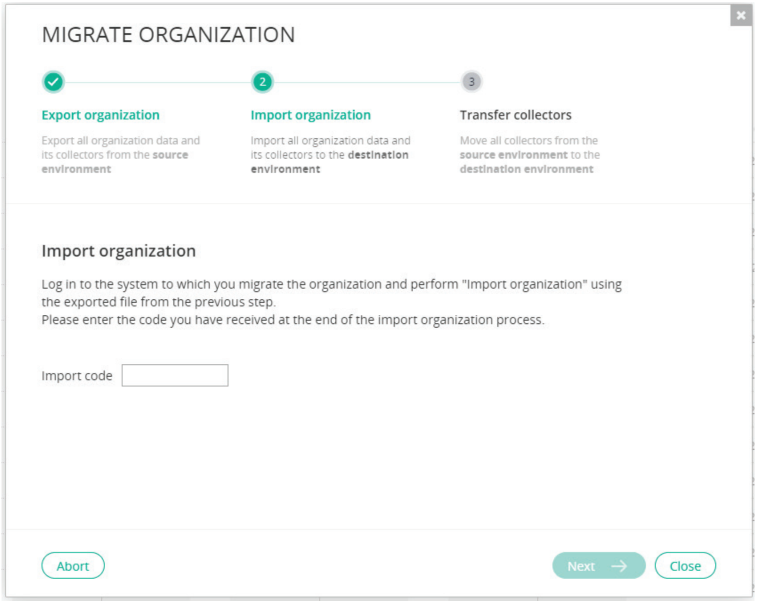
Download

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:



MIGRATE ORGANIZATION

✓ **Export organization**
Export all organization data and its collectors from the **source environment**

2 **Import organization**
Import all organization data and its collectors to the **destination environment**

3 **Transfer collectors**
Move all collectors from the **source environment** to the **destination environment**

Import organization

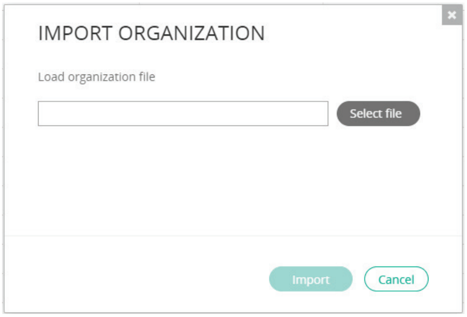
Log in to the system to which you migrate the organization and perform "Import organization" using the exported file from the previous step.
Please enter the code you have received at the end of the import organization process.

Import code

7 Log in to the destination environment.

8 Click the **ADMINISTRATION** tab and then click **ORGANIZATIONS** in the left pane.

9 In the **ORGANIZATIONS** page, click the **Import Organization** button. The following window displays:



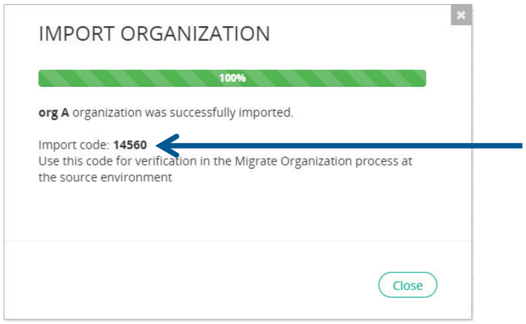
IMPORT ORGANIZATION

Load organization file

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

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 178).
You must have sufficient workstation and server licenses in the destination environment.

At the end of the import process, the Import Organization window displays a code. Write down this code, as it will be entered later as part of the migration process.

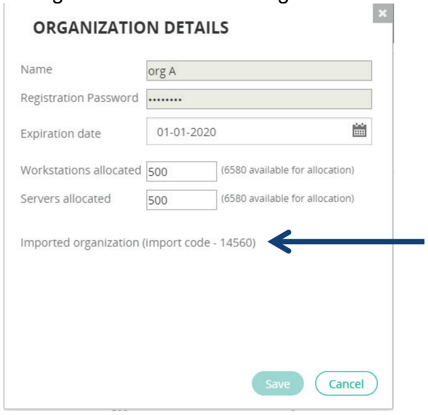

IMPORT ORGANIZATION

100%

org A organization was successfully imported.

Import code: **14560**
Use this code for verification in the Migrate Organization process at the source environment

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.


ORGANIZATION DETAILS

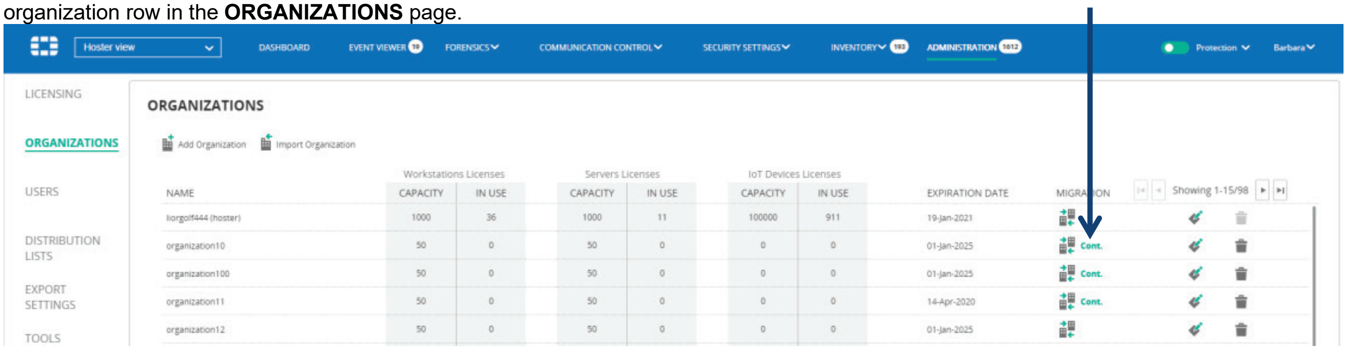
Name: org A
Registration Password: ••••••••
Expiration date: 01-01-2020
Workstations allocated: 500 (6580 available for allocation)
Servers allocated: 500 (6580 available for allocation)

Imported organization (import code - 14560)

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

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

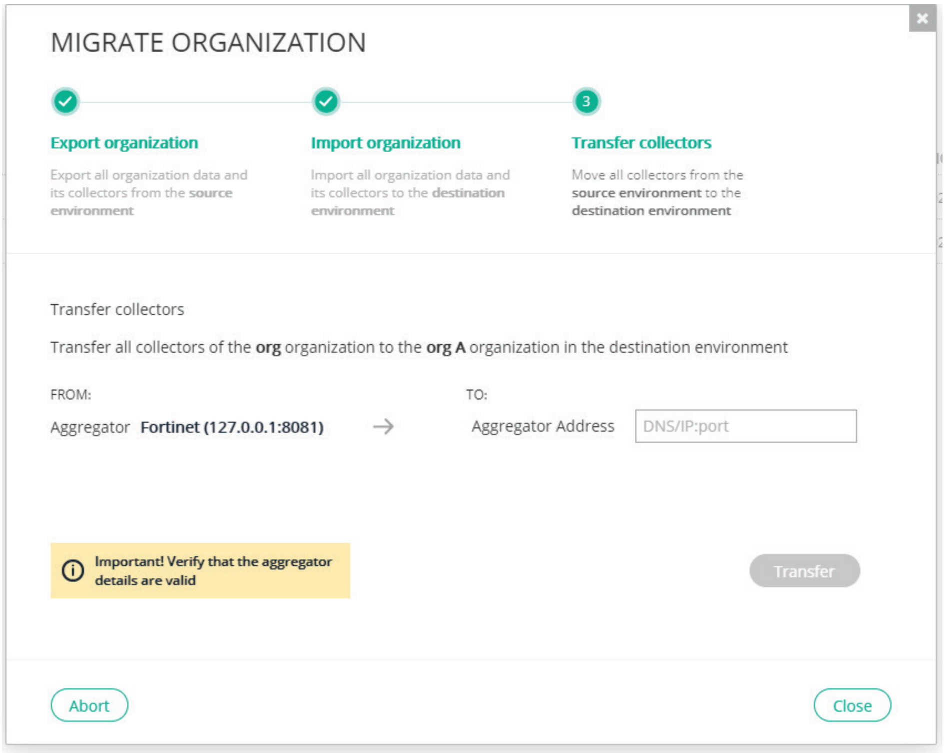
Note – If you previously closed the Migrate Organization window, then click the **Continue Migration** Cont. button in the source organization row in the **ORGANIZATIONS** page.



ORGANIZATIONS

	Workstations Licenses		Servers Licenses		IoT Devices Licenses			
NAME	CAPACITY	IN USE	CAPACITY	IN USE	CAPACITY	IN USE	EXPIRATION DATE	MIGRATION
liorgolf444 (hoster)	1000	36	1000	11	100000	911	19-Jan-2021	
organization10	50	0	50	0	0	0	01-Jan-2025	Cont.
organization100	50	0	50	0	0	0	01-Jan-2025	Cont.
organization11	50	0	50	0	0	0	14-Apr-2020	Cont.
organization12	50	0	50	0	0	0	01-Jan-2025	

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



MIGRATE ORGANIZATION

Export organization
Export all organization data and its collectors from the **source** environment

Import organization
Import all organization data and its collectors to the **destination** environment

3 Transfer collectors
Move all collectors from the **source environment** to the **destination environment**

Transfer collectors

Transfer all collectors of the **org** organization to the **org A** organization in the destination environment

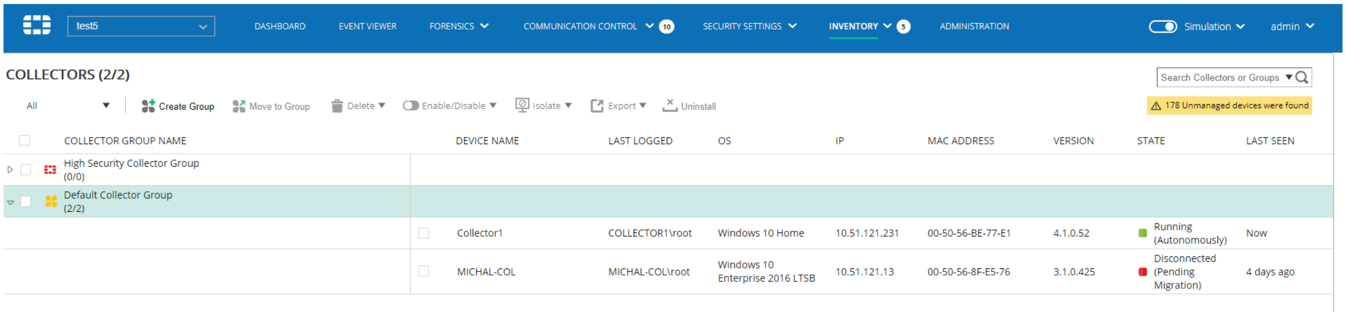
FROM:
Aggregator **Fortinet (127.0.0.1:8081)**

TO:
Aggregator Address DNS/IP:port

Important! Verify that the aggregator details are valid

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

Note that until this step is completed, the Collectors are still registered to the organization in the source environment and their status and security events are displayed there. In the destination environment, Collectors are displayed with the **Pending Migration** state, as shown in the Inventory window. This state indicates that the Collector has not yet been transferred from the source environment to this environment. Collectors in the Pending Migration state are still registered to the source environment.

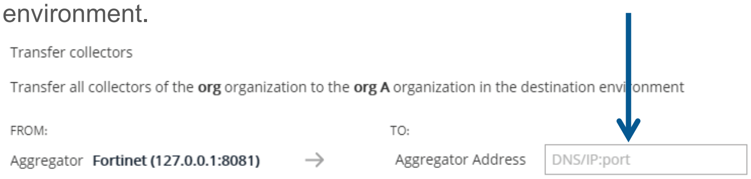


COLLECTORS (2/2)

⚠ 178 Unmanaged devices were found

COLLECTOR GROUP NAME	DEVICE NAME	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	STATE	LAST SEEN
High Security Collector Group (0/0)								
Default Collector Group (2/2)								
	Collector1	COLLECTOR1\root	Windows 10 Home	10.51.121.231	00-50-56-BE-77-E1	4.1.0.52	🟩 Running (Autonomously)	Now
	MICHAL-COL	MICHAL-COL\root	Windows 10 Enterprise 2016 LTSB	10.51.121.13	00-50-56-8F-E5-76	3.1.0.425	🟥 Disconnected (Pending Migration)	4 days ago

13 Specify the **Aggregator Address** in the **To** field. Each Collector is connected to one Aggregator. In this field, you specify the IP address or DNS name and the port of the Aggregator that will service the Collectors in the destination environment.


Transfer collectors

Transfer all collectors of the **org** organization to the **org A** organization in the destination environment

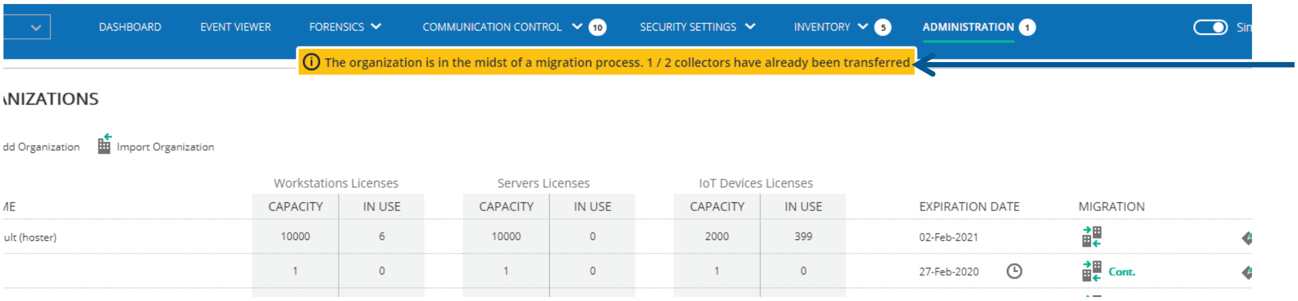
FROM:

Aggregator **Fortinet (127.0.0.1:8081)** →

TO:

Aggregator Address DNS/IP:port

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



ⓘ The organization is in the midst of a migration process. 1 / 2 collectors have already been transferred

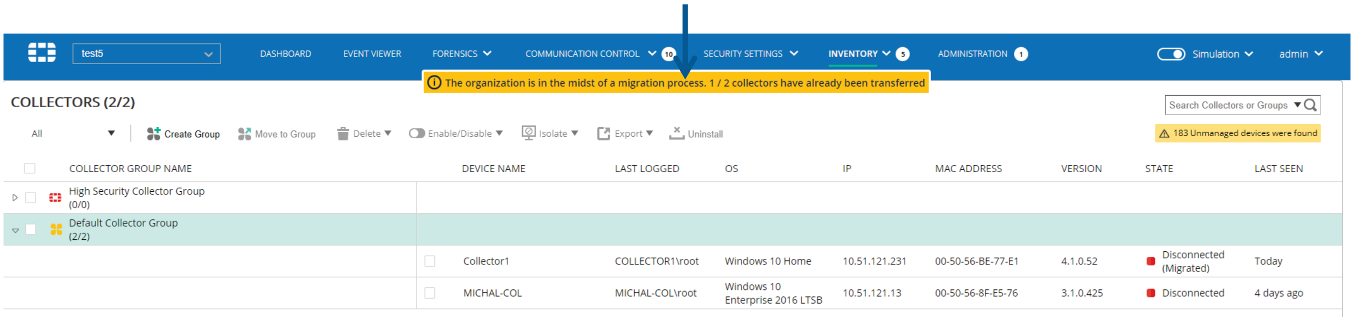
ɅNIZATIONS

	Workstations Licenses		Servers Licenses		IoT Devices Licenses			
ΛE	CAPACITY	IN USE	CAPACITY	IN USE	CAPACITY	IN USE	EXPIRATION DATE	MIGRATION
ult (hoster)	10000	6	10000	0	2000	399	02-Feb-2021	
	1	0	1	0	1	0	27-Feb-2020	Cont.

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.



ⓘ The organization is in the midst of a migration process. 1 / 2 collectors have already been transferred

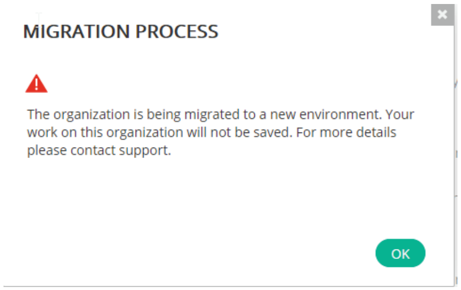
COLLECTORS (2/2)

⚠ 183 Unmanaged devices were found

COLLECTOR GROUP NAME	DEVICE NAME	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	STATE	LAST SEEN
High Security Collector Group (0/0)								
Default Collector Group (2/2)								
	Collector1	COLLECTOR1\root	Windows 10 Home	10.51.121.231	00-50-56-BE-77-E1	4.1.0.52	🟥 Disconnected (Migrated)	Today
	MICHAL-COL	MICHAL-COL\root	Windows 10 Enterprise 2016 LTSB	10.51.121.13	00-50-56-8F-E5-76	3.1.0.425	🟥 Disconnected	4 days ago

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.



MIGRATION PROCESS

The organization is being migrated to a new environment. Your work on this organization will not be saved. For more details please contact support.

16 After all the Collectors were successfully migrated from the organization on the source environment to the organization on the destination environment, delete the source organization. To do so, select the **Administration** tab and then click **Organizations** in the left pane. In the Organizations window, click the **Delete** button in the row of the source organization to be removed.

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

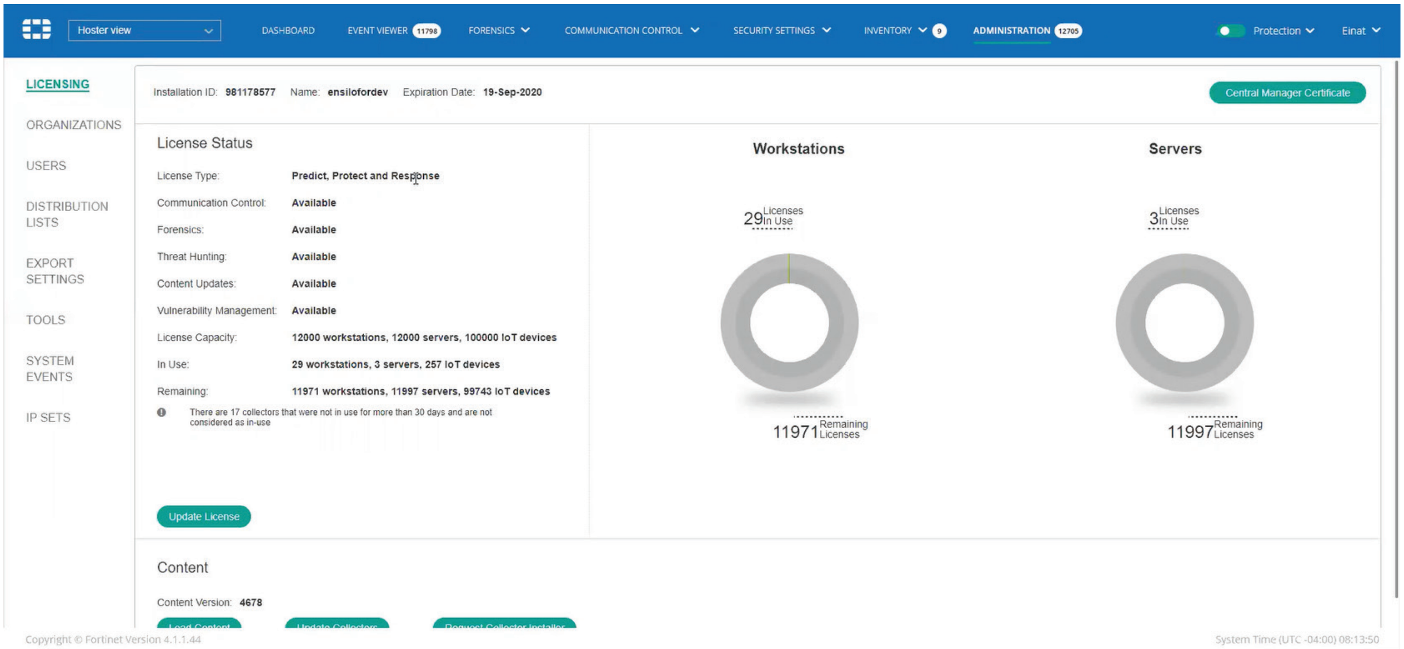
In addition, there are some special cases where you cannot view administration data in Hoster view, and can only view data for a specific organization, such as the following:

- 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.



Installation ID: **981178577** Name: **ensilofordev** Expiration Date: **19-Sep-2020**

License Status

License Type:	Predict, Protect and Response
Communication Control:	Available
Forensics:	Available
Threat Hunting:	Available
Content Updates:	Available
Vulnerability Management:	Available
License Capacity:	12000 workstations, 12000 servers, 100000 IoT devices
In Use:	29 workstations, 3 servers, 257 IoT devices
Remaining:	11971 workstations, 11997 servers, 99743 IoT devices

There are 17 collectors that were not in use for more than 30 days and are not considered as in-use

Content

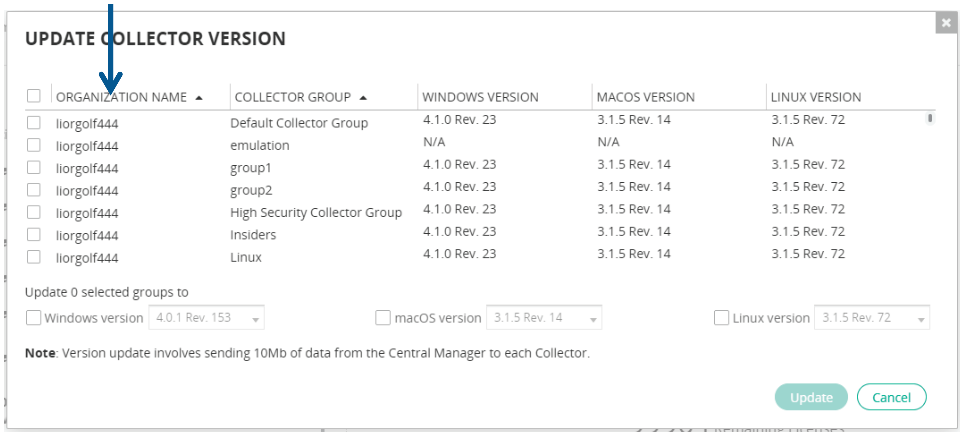
Content Version: **4678**

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 248.

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

When you click the **Update Collectors** button in the Licensing window, the Update Collector Version window displays, and includes an **Organization Name** column. Use the checkboxes in this column to update the organization for a Collector Group. All other functionality in this window works in the standard manner.



UPDATE COLLECTOR VERSION

□	ORGANIZATION NAME ▲	COLLECTOR GROUP ▲	WINDOWS VERSION	MACOS VERSION	LINUX VERSION
□	liorgolf444	Default Collector Group	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
□	liorgolf444	emulation	N/A	N/A	N/A
□	liorgolf444	group1	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
□	liorgolf444	group2	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
□	liorgolf444	High Security Collector Group	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
□	liorgolf444	Insiders	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72
□	liorgolf444	Linux	4.1.0 Rev. 23	3.1.5 Rev. 14	3.1.5 Rev. 72

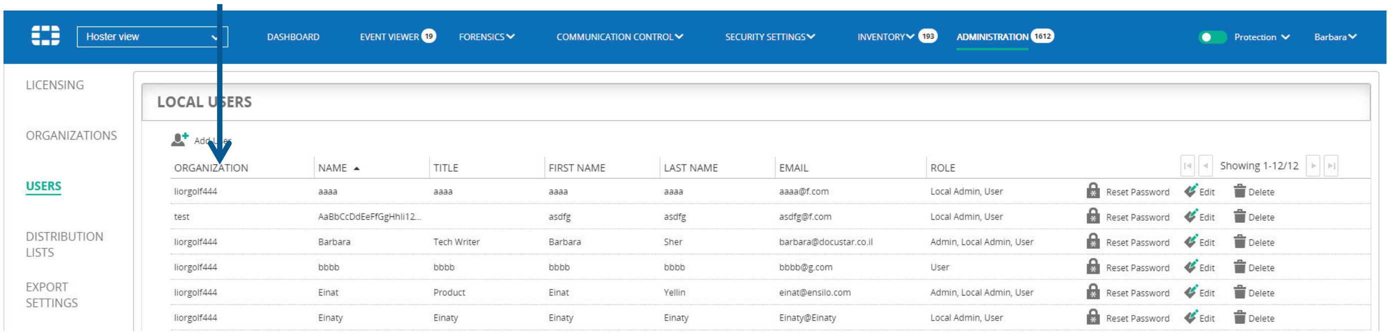
Update 0 selected groups to

□ Windows version 4.0.1 Rev. 153 □ macOS version 3.1.5 Rev. 14 □ Linux version 3.1.5 Rev. 72

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

Users

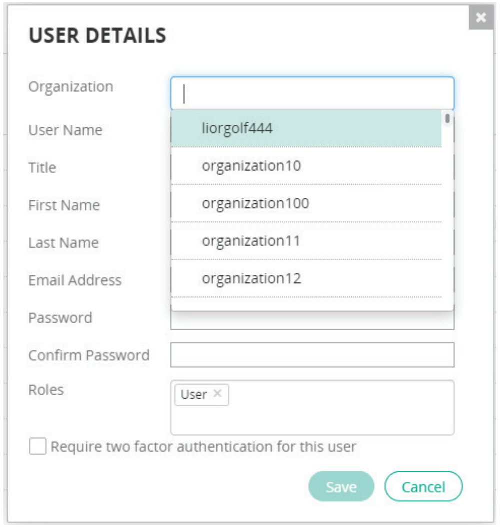
In Hoster view, this window includes an **Organization** column.



LOCAL USERS

ORGANIZATION	NAME ▲	TITLE	FIRST NAME	LAST NAME	EMAIL	ROLE			
liorgolf444	aaaa	aaaa	aaaa	aaaa	aaaa@f.com	Local Admin, User	Reset Password	Edit	Delete
test	AaBbCcDdEeFfGgHhIi12...		asdfg	asdfg	asdfg@f.com	Local Admin, User	Reset Password	Edit	Delete
liorgolf444	Barbara	Tech Writer	Barbara	Sher	barbara@docustar.co.il	Admin, Local Admin, User	Reset Password	Edit	Delete
liorgolf444	bbbb	bbbb	bbbb	bbbb	bbbb@g.com	User	Reset Password	Edit	Delete
liorgolf444	Einat	Product	Einat	Yellin	einat@ensilo.com	Admin, Local Admin, User	Reset Password	Edit	Delete
liorgolf444	Einaty	Einaty	Einaty	Einaty	Einaty@Einaty	Local Admin, User	Reset Password	Edit	Delete

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.



USER DETAILS

Organization

User Name

Title

First Name

Last Name

Email Address

Password

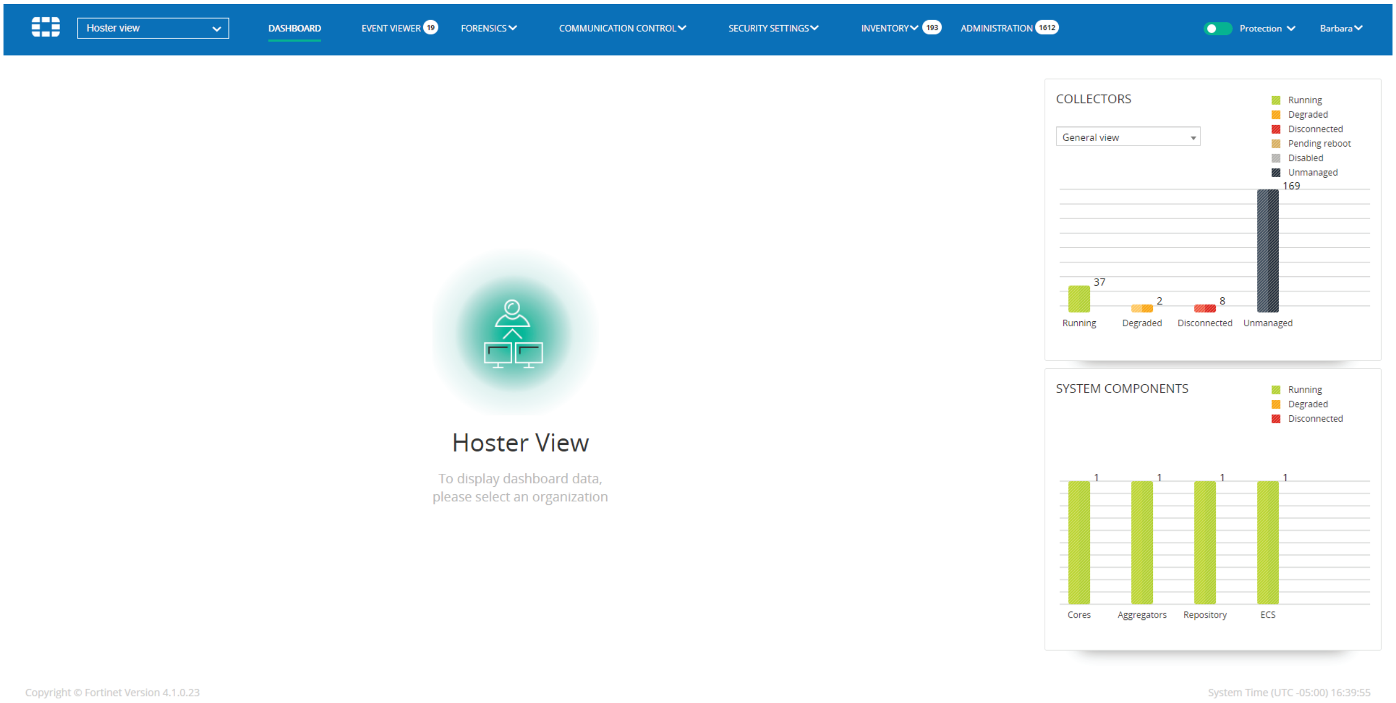
Confirm Password

Roles: User ×

□ Require two factor authentication for this 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.



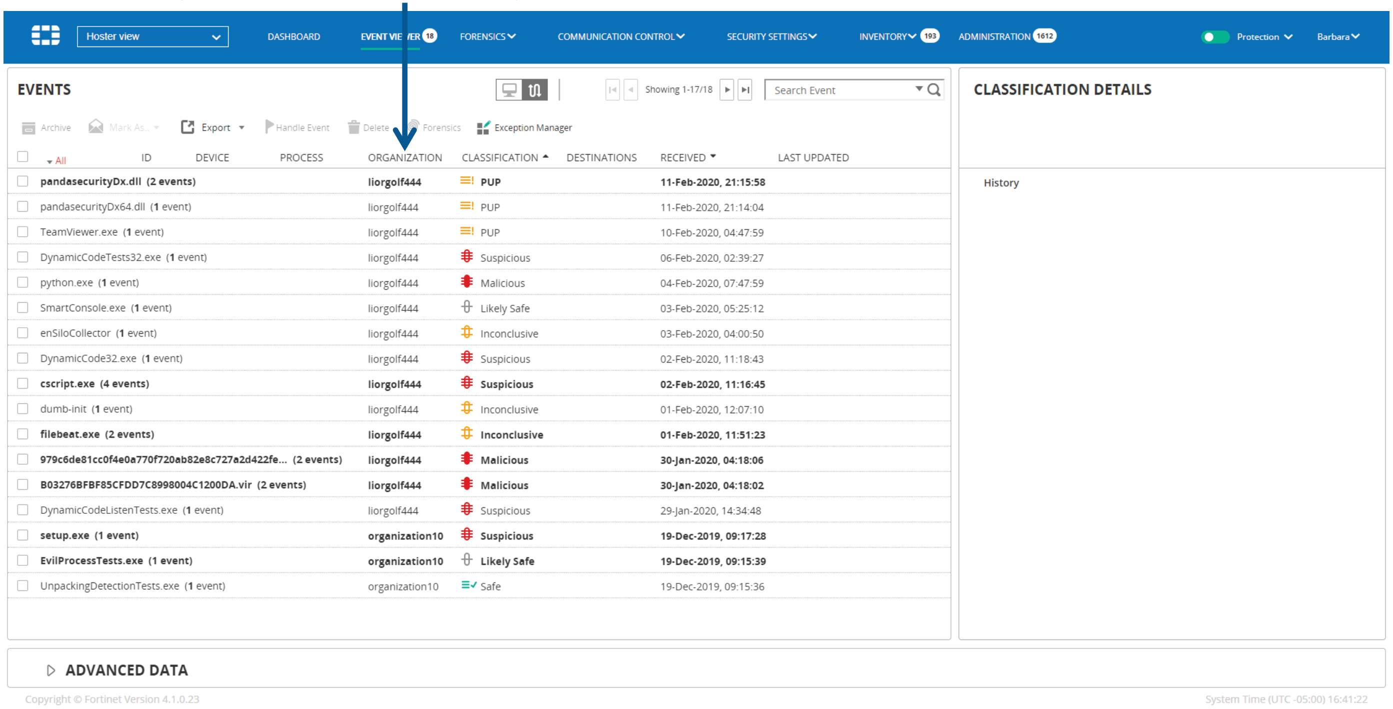
Hoster View

To display dashboard data, please select an organization

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

Event Viewer

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

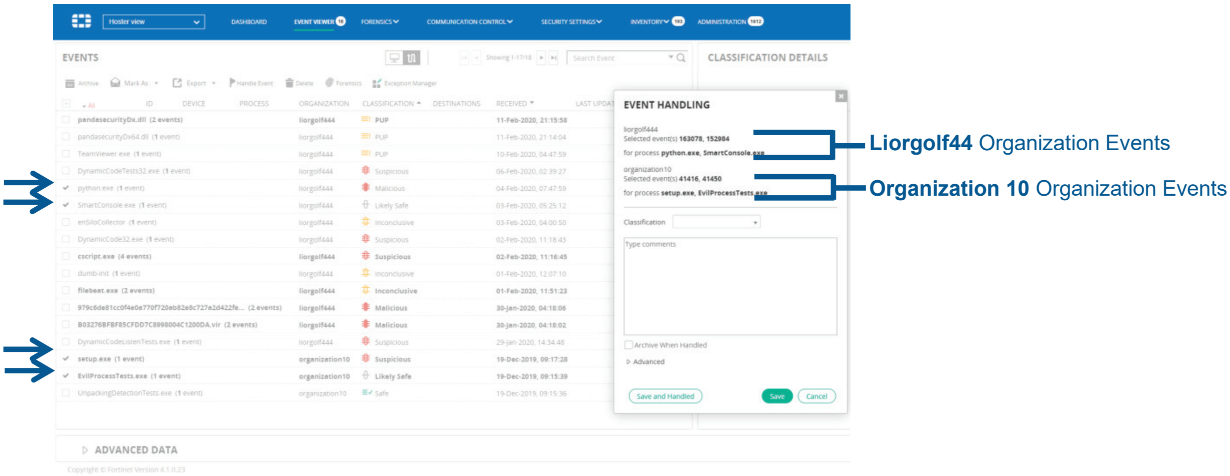


All	ID	DEVICE	PROCESS	ORGANIZATION	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
pandasecurityDx.dll (2 events)				**liorgolf444**	**PUP**		**11-Feb-2020, 21:15:58**	
pandasecurityDx64.dll (1 event)				liorgolf444	PUP		11-Feb-2020, 21:14:04	
TeamViewer.exe (1 event)				liorgolf444	PUP		10-Feb-2020, 04:47:59	
DynamicCodeTests32.exe (1 event)				liorgolf444	Suspicious		06-Feb-2020, 02:39:27	
python.exe (1 event)				liorgolf444	Malicious		04-Feb-2020, 07:47:59	
SmartConsole.exe (1 event)				liorgolf444	Likely Safe		03-Feb-2020, 05:25:12	
enSiloCollector (1 event)				liorgolf444	Inconclusive		03-Feb-2020, 04:00:50	
DynamicCode32.exe (1 event)				liorgolf444	Suspicious		02-Feb-2020, 11:18:43	
cscript.exe (4 events)				**liorgolf444**	**Suspicious**		**02-Feb-2020, 11:16:45**	
dumb-init (1 event)				liorgolf444	Inconclusive		01-Feb-2020, 12:07:10	
filebeat.exe (2 events)				**liorgolf444**	**Inconclusive**		**01-Feb-2020, 11:51:23**	
979c6de81cc0f4e0a770f720ab82e8c727a2d422fe... (2 events)				**liorgolf444**	**Malicious**		**30-Jan-2020, 04:18:06**	
B03276BFBF85CFDD7C8998004C1200DA.vir (2 events)				**liorgolf444**	**Malicious**		**30-Jan-2020, 04:18:02**	
DynamicCodeListenTests.exe (1 event)				liorgolf444	Suspicious		29-Jan-2020, 14:34:48	
setup.exe (1 event)				**organization10**	**Suspicious**		**19-Dec-2019, 09:17:28**	
EvilProcessTests.exe (1 event)				**organization10**	**Likely Safe**		**19-Dec-2019, 09:15:39**	
UnpackingDetectionTests.exe (1 event)				organization10	Safe		19-Dec-2019, 09:15:36	

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

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

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



	All	ID	DEVICE	PROCESS	ORGANIZATION	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDAT
☐	**pandasecurityDx.dll (2 events)**				**liorgolf444**	**PUP**		**11-Feb-2020, 21:15:58**	
☐	pandasecurityDx64.dll (1 event)				liorgolf444	PUP		11-Feb-2020, 21:14:04	
☐	TeamViewer.exe (1 event)				liorgolf444	PUP		10-Feb-2020, 04:47:59	
☐	DynamicCodeTests32.exe (1 event)				liorgolf444	Suspicious		06-Feb-2020, 02:39:27	
✓	python.exe (1 event)				liorgolf444	Malicious		04-Feb-2020, 07:47:59	
✓	SmartConsole.exe (1 event)				liorgolf444	Likely Safe		03-Feb-2020, 05:25:12	
☐	enSiloCollector (1 event)				liorgolf444	Inconclusive		03-Feb-2020, 04:00:50	
☐	DynamicCode32.exe (1 event)				liorgolf444	Suspicious		02-Feb-2020, 11:18:43	
☐	**cscript.exe (4 events)**				**liorgolf444**	**Suspicious**		**02-Feb-2020, 11:16:45**	
☐	dumb-init (1 event)				liorgolf444	Inconclusive		01-Feb-2020, 12:07:10	
☐	**filebeat.exe (2 events)**				**liorgolf444**	**Inconclusive**		**01-Feb-2020, 11:51:23**	
☐	**979c6de81cc0f4e0a770f720ab82e8c727a2d422fe... (2 events)**				**liorgolf444**	**Malicious**		**30-Jan-2020, 04:18:06**	
☐	**B03276BFBF85CFDD7C8998004C1200DA.vir (2 events)**				**liorgolf444**	**Malicious**		**30-Jan-2020, 04:18:02**	
☐	DynamicCodeListenTests.exe (1 event)				liorgolf444	Suspicious		29-Jan-2020, 14:34:48	
✓	**setup.exe (1 event)**				**organization10**	**Suspicious**		**19-Dec-2019, 09:17:28**	
✓	**EvilProcessTests.exe (1 event)**				**organization10**	**Likely Safe**		**19-Dec-2019, 09:15:39**	
☐	UnpackingDetectionTests.exe (1 event)				organization10	Safe		19-Dec-2019, 09:15:36	

EVENT HANDLING

liorgolf444
Selected event(s) **163078, 152984**
for process **python.exe, SmartConsole.exe**

organization10
Selected event(s) **41416, 41450**
for process **setup.exe, EvilProcessTests.exe**

Classification

Type comments

☐ Archive When Handled

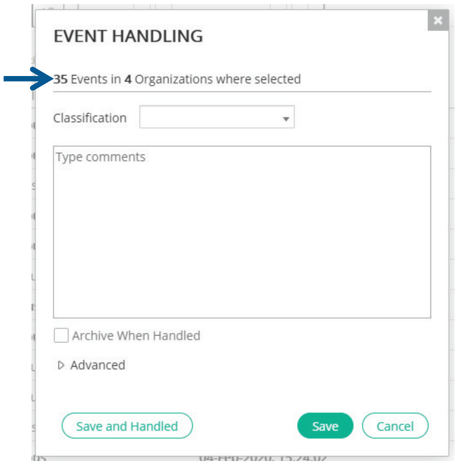
▷ Advanced

Save and Handled | Save | Cancel

Liorgolf44 Organization Events

Organization 10 Organization Events

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



EVENT HANDLING

35 Events in **4** Organizations where selected

Classification

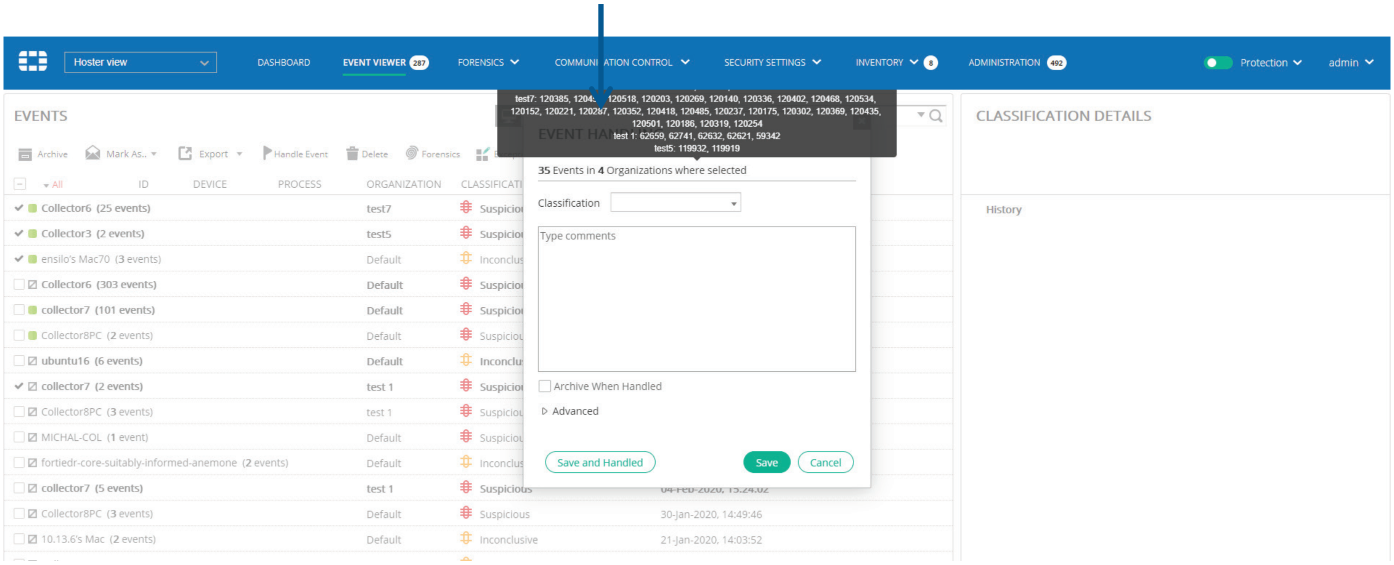
Type comments

☐ Archive When Handled

▷ Advanced

Save and Handled | Save | Cancel

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



test7: 120385, 1204■, 120518, 120203, 120269, 120140, 120336, 120402, 120468, 120534, 120152, 120221, 120287, 120352, 120418, 120485, 120237, 120175, 120302, 120369, 120435, 120501, 120186, 120319, 120254
test 1: 62659, 62741, 62632, 62621, 59342
test5: 119932, 119919

35 Events in **4** Organizations where selected

Classification

Type comments

□ Archive When Handled

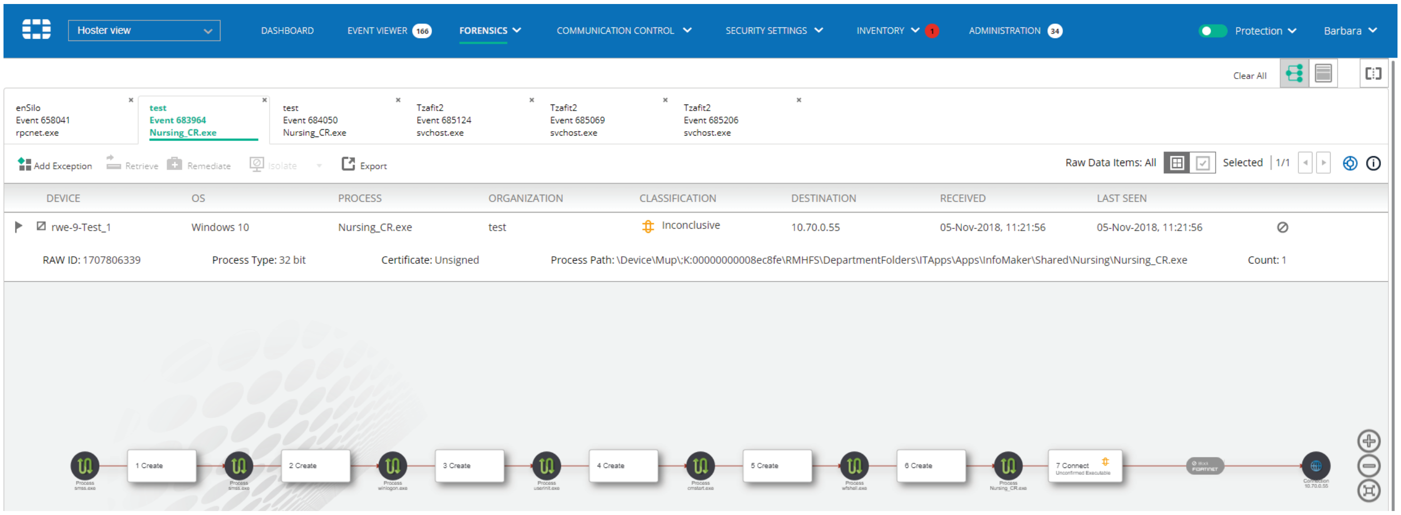
▷ Advanced

Save and Handled | Save | Cancel

	ID	DEVICE	PROCESS	ORGANIZATION	CLASSIFICATI	
✓		Collector6 (25 events)		test7	Suspicio	
✓		Collector3 (2 events)		test5	Suspicio	
✓		ensilo's Mac70 (3 events)		Default	Inconclus	
□		Collector6 (303 events)		Default	Suspicio	
□		collector7 (101 events)		Default	Suspicio	
□		Collector8PC (2 events)		Default	Suspiciou	
□		ubuntu16 (6 events)		Default	Inconclu	
✓		collector7 (2 events)		test 1	Suspicio	
□		Collector8PC (3 events)		test 1	Suspiciou	
□		MICHAL-COL (1 event)		Default	Suspiciou	
□		fortiedr-core-suitably-informed-anemone (2 events)		Default	Inconclus	
□		collector7 (5 events)		test 1	Suspicious	04-Feb-2020, 15:24:02
□		Collector8PC (3 events)		Default	Suspicious	30-Jan-2020, 14:49:46
□		10.13.6's Mac (2 events)		Default	Inconclusive	21-Jan-2020, 14:03:52

Forensics

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



enSilo	test	test	Tzafit2	Tzafit2	Tzafit2
Event 658041	Event 683964	Event 684050	Event 685124	Event 685069	Event 685206
rpcnet.exe	Nursing_CR.exe	Nursing_CR.exe	svchost.exe	svchost.exe	svchost.exe

DEVICE	OS	PROCESS	ORGANIZATION	CLASSIFICATION	DESTINATION	RECEIVED	LAST SEEN
rwe-9-Test_1	Windows 10	Nursing_CR.exe	test	Inconclusive	10.70.0.55	05-Nov-2018, 11:21:56	05-Nov-2018, 11:21:56

RAW ID: 1707806339 Process Type: 32 bit Certificate: Unsigned Process Path: \Device\Mup\;K:00000000008ec8fe\RMHFS\DepartmentFolders\ITApps\Apps\InfoMaker\Shared\Nursing\Nursing_CR.exe Count: 1

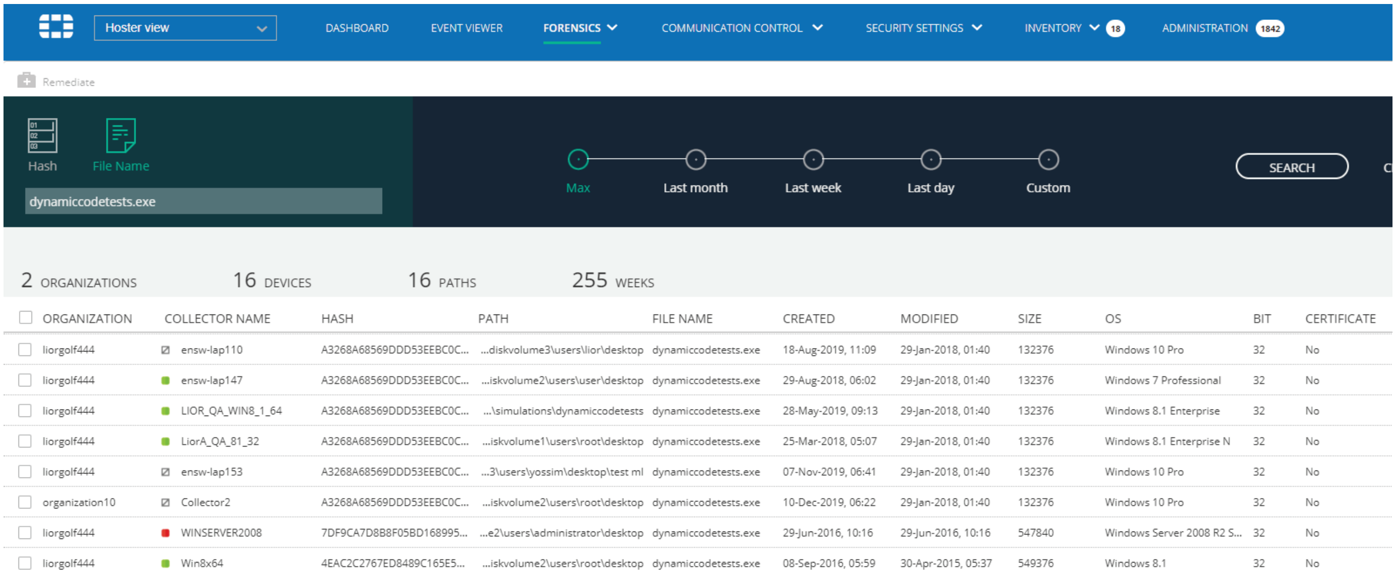
Communication Control

The Communication Control window is not available in Hoster view.

Threat Hunting

Threat Hunting (Legacy)

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



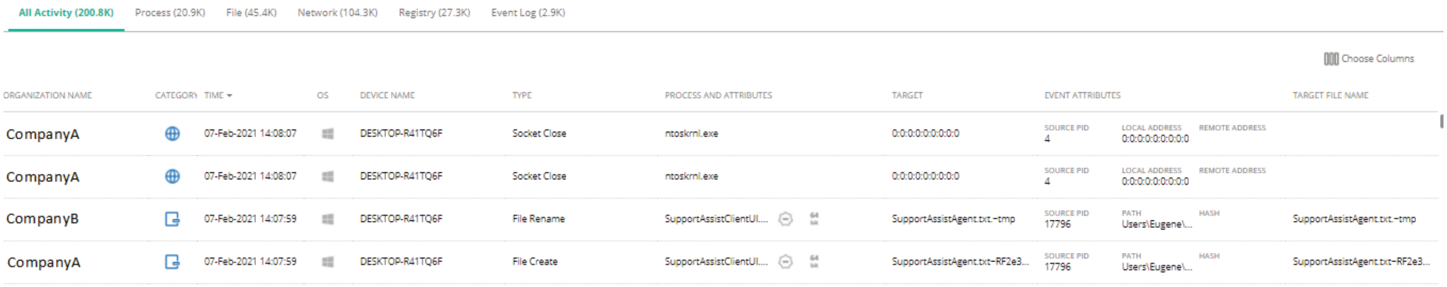
dynamiccodetests.exe

2 ORGANIZATIONS 16 DEVICES 16 PATHS 255 WEEKS

☐	ORGANIZATION		COLLECTOR NAME	HASH	PATH	FILE NAME	CREATED	MODIFIED	SIZE	OS	BIT	CERTIFICATE
☐	liorgolf444	☒	ensw-lap110	A3268A68569DDD53EEBC0C...	...diskvolume3\users\lior\desktop	dynamiccodetests.exe	18-Aug-2019, 11:09	29-Jan-2018, 01:40	132376	Windows 10 Pro	32	No
☐	liorgolf444	🟩	ensw-lap147	A3268A68569DDD53EEBC0C...	...iskvolume2\users\user\desktop	dynamiccodetests.exe	29-Aug-2018, 06:02	29-Jan-2018, 01:40	132376	Windows 7 Professional	32	No
☐	liorgolf444	🟩	LIOR_QA_WIN8_1_64	A3268A68569DDD53EEBC0C...	...\simulations\dynamiccodetests	dynamiccodetests.exe	28-May-2019, 09:13	29-Jan-2018, 01:40	132376	Windows 8.1 Enterprise	32	No
☐	liorgolf444	🟩	LiorA_QA_81_32	A3268A68569DDD53EEBC0C...	...iskvolume1\users\root\desktop	dynamiccodetests.exe	25-Mar-2018, 05:07	29-Jan-2018, 01:40	132376	Windows 8.1 Enterprise N	32	No
☐	liorgolf444	☒	ensw-lap153	A3268A68569DDD53EEBC0C...	...3\users\yossim\desktop\test ml	dynamiccodetests.exe	07-Nov-2019, 06:41	29-Jan-2018, 01:40	132376	Windows 10 Pro	32	No
☐	organization10	☒	Collector2	A3268A68569DDD53EEBC0C...	...iskvolume2\users\root\desktop	dynamiccodetests.exe	10-Dec-2019, 06:22	29-Jan-2018, 01:40	132376	Windows 10 Pro	32	No
☐	liorgolf444	🟥	WINSERVER2008	7DF9CA7D8B8F05BD168995...	...e2\users\administrator\desktop	dynamiccodetests.exe	29-Jun-2016, 10:16	29-Jun-2016, 10:16	547840	Windows Server 2008 R2 S...	32	No
☐	liorgolf444	🟩	Win8x64	4EAC2C2767ED8489C165E5...	...iskvolume2\users\root\desktop	dynamiccodetests.exe	08-Sep-2016, 05:59	30-Apr-2015, 05:37	549376	Windows 8.1	32	No

Threat Hunting

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

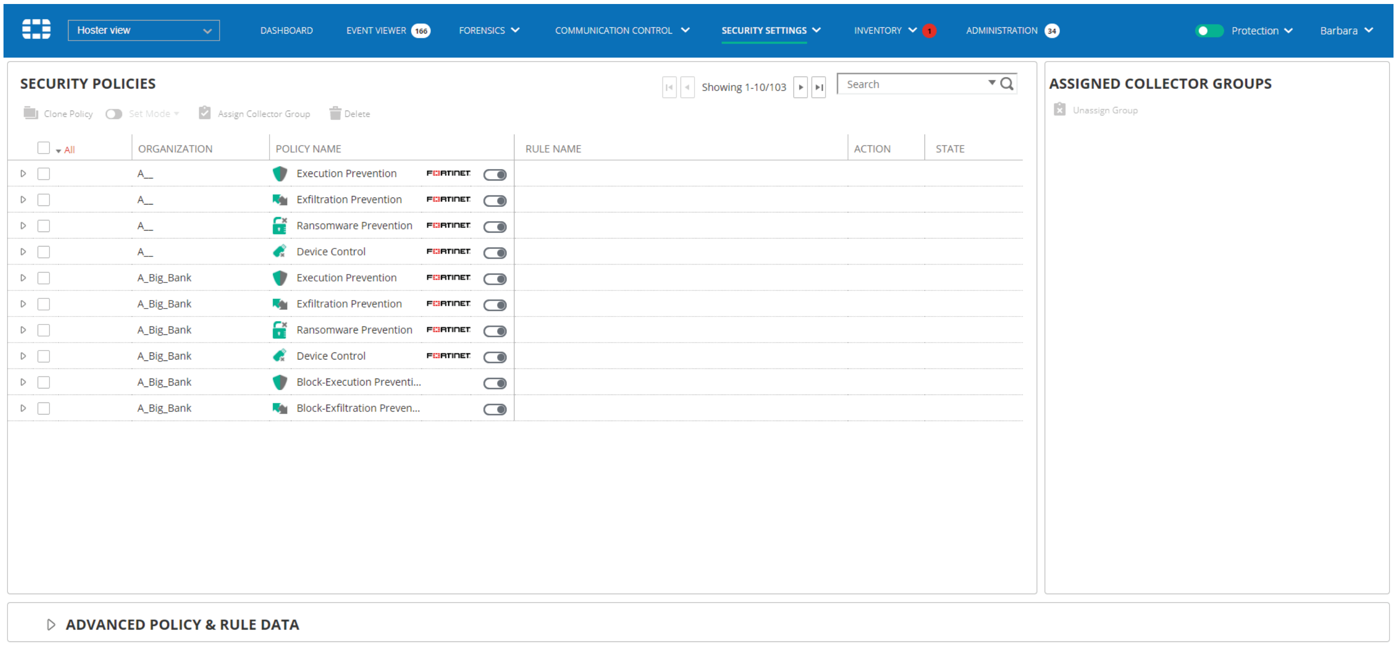


ORGANIZATION NAME	CATEGORY	TIME ▾	OS	DEVICE NAME	TYPE	PROCESS AND ATTRIBUTES	TARGET	EVENT ATTRIBUTES	TARGET FILE NAME
CompanyA	🌐	07-Feb-2021 14:08:07		DESKTOP-R41TQ6F	Socket Close	ntoskrnl.exe	0:0:0:0:0:0:0:0:0	SOURCE PID 4 LOCAL ADDRESS 0:0:0:0:0:0:0:0:0 REMOTE ADDRESS	
CompanyA	🌐	07-Feb-2021 14:08:07		DESKTOP-R41TQ6F	Socket Close	ntoskrnl.exe	0:0:0:0:0:0:0:0:0	SOURCE PID 4 LOCAL ADDRESS 0:0:0:0:0:0:0:0:0 REMOTE ADDRESS	
CompanyB		07-Feb-2021 14:07:59		DESKTOP-R41TQ6F	File Rename	SupportAssistClientUI.... 64 bit	SupportAssistAgent.txt.~tmp	SOURCE PID 17796 PATH Users\Eugene\... HASH	SupportAssistAgent.txt.~tmp
CompanyA		07-Feb-2021 14:07:59		DESKTOP-R41TQ6F	File Create	SupportAssistClientUI.... 64 bit	SupportAssistAgent.txt~RF2e3...	SOURCE PID 17796 PATH Users\Eugene\... HASH	SupportAssistAgent.txt~RF2e3...

Security Settings

SECURITY POLICIES Page

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



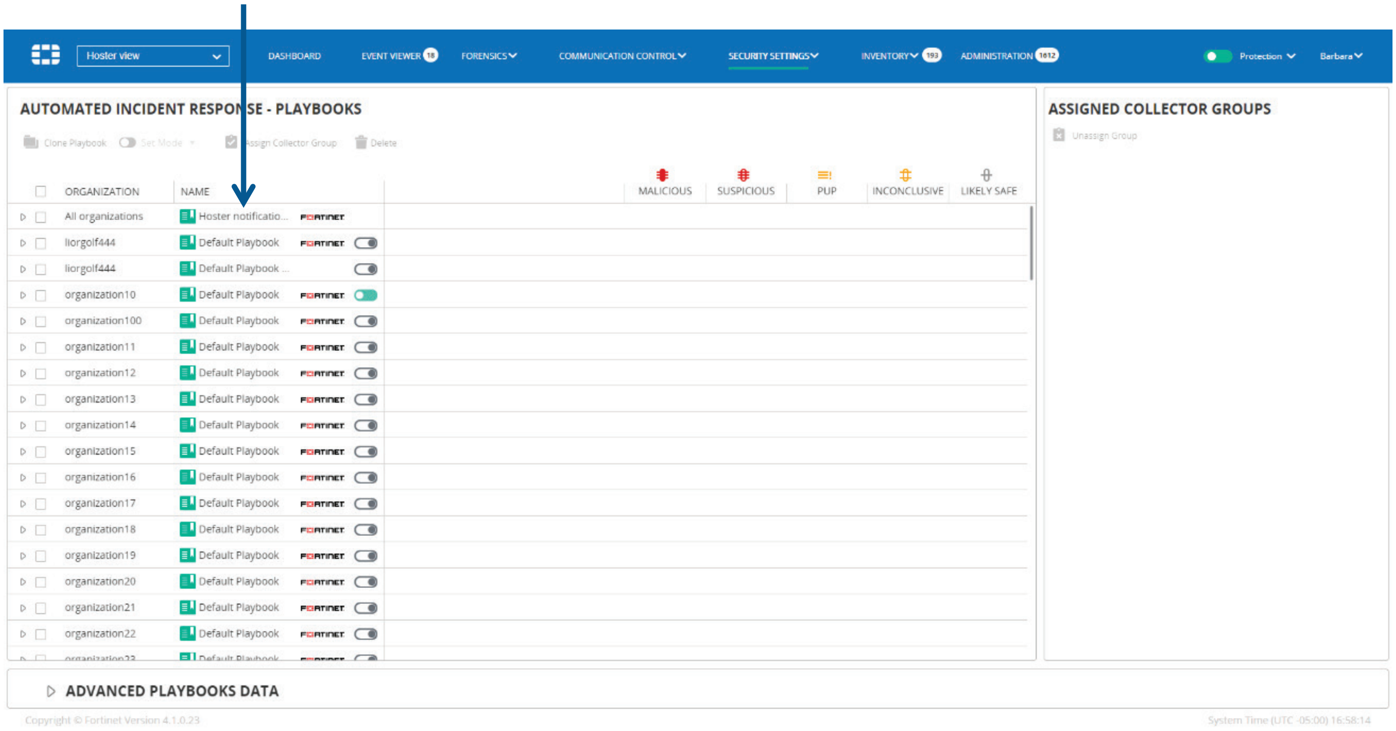
SECURITY POLICIES

All	ORGANIZATION	POLICY NAME	RULE NAME	ACTION	STATE
□	A_	Execution Prevention FORTINET			
□	A_	Exfiltration Prevention FORTINET			
□	A_	Ransomware Prevention FORTINET			
□	A_	Device Control FORTINET			
□	A_Big_Bank	Execution Prevention FORTINET			
□	A_Big_Bank	Exfiltration Prevention FORTINET			
□	A_Big_Bank	Ransomware Prevention FORTINET			
□	A_Big_Bank	Device Control FORTINET			
□	A_Big_Bank	Block-Execution Preventi...			
□	A_Big_Bank	Block-Exfiltration Preven...			

FortiEDR’s multi-organization feature enables you to clone a security policy from one organization to another. To do so, you must be in Hoster view. When not in Hoster view, you can only clone a policy within the same organization.

AUTOMATED INCIDENT RESPONSE - PLAYBOOKS Page

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

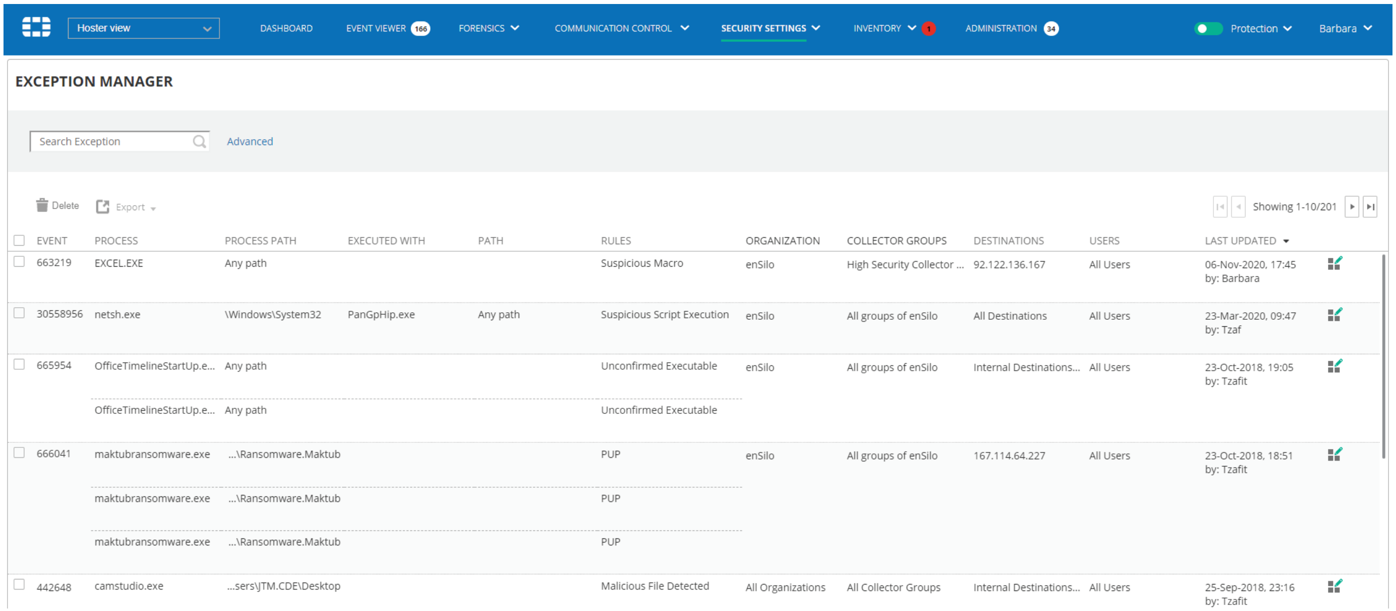


AUTOMATED INCIDENT RESPONSE - PLAYBOOKS

□	ORGANIZATION	NAME	MALICIOUS	SUSPICIOUS	PUP	INCONCLUSIVE	LIKELY SAFE
□	All organizations	Hoster notificatio... FORTINET					
□	liorgolf444	Default Playbook FORTINET					
□	liorgolf444	Default Playbook ...					
□	organization10	Default Playbook FORTINET					
□	organization100	Default Playbook FORTINET					
□	organization11	Default Playbook FORTINET					
□	organization12	Default Playbook FORTINET					
□	organization13	Default Playbook FORTINET					
□	organization14	Default Playbook FORTINET					
□	organization15	Default Playbook FORTINET					
□	organization16	Default Playbook FORTINET					
□	organization17	Default Playbook FORTINET					
□	organization18	Default Playbook FORTINET					
□	organization19	Default Playbook FORTINET					
□	organization20	Default Playbook FORTINET					
□	organization21	Default Playbook FORTINET					
□	organization22	Default Playbook FORTINET					
□	organization23	Default Playbook FORTINET					

Exception Manager

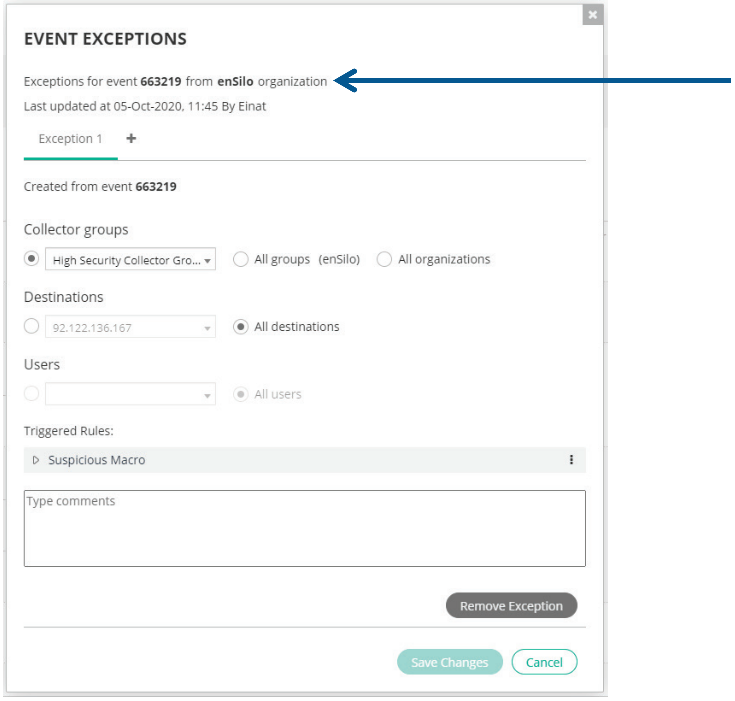
In Hoster view, the Exception Manager page displays all exceptions from all organizations.



EXCEPTION MANAGER

EVENT	PROCESS	PROCESS PATH	EXECUTED WITH	PATH	RULES	ORGANIZATION	COLLECTOR GROUPS	DESTINATIONS	USERS	LAST UPDATED
663219	EXCEL.EXE	Any path			Suspicious Macro	enSilo	High Security Collector ...	92.122.136.167	All Users	06-Nov-2020, 17:45 by: Barbara
30558956	netsh.exe	\Windows\System32	PanGpHip.exe	Any path	Suspicious Script Execution	enSilo	All groups of enSilo	All Destinations	All Users	23-Mar-2020, 09:47 by: Tzaf
665954	OfficeTimelineStartUp.e...	Any path			Unconfirmed Executable	enSilo	All groups of enSilo	Internal Destinations...	All Users	23-Oct-2018, 19:05 by: Tzafit
	OfficeTimelineStartUp.e...	Any path			Unconfirmed Executable					
666041	maktubransomware.exe	...\Ransomware.Maktub			PUP	enSilo	All groups of enSilo	167.114.64.227	All Users	23-Oct-2018, 18:51 by: Tzafit
	maktubransomware.exe	...\Ransomware.Maktub			PUP					
	maktubransomware.exe	...\Ransomware.Maktub			PUP					
442648	camstudio.exe	...sers\JTM.CDE\Desktop			Malicious File Detected	All Organizations	All Collector Groups	Internal Destinations...	All Users	25-Sep-2018, 23:16 by: Tzafit

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



EVENT EXCEPTIONS

Exceptions for event **663219** from **enSilo** organization

Last updated at 05-Oct-2020, 11:45 By Einat

Created from event **663219**

Collector groups

● High Security Collector Gro... ○ All groups (enSilo) ○ All organizations

Destinations

○ 92.122.136.167 ● All destinations

Users

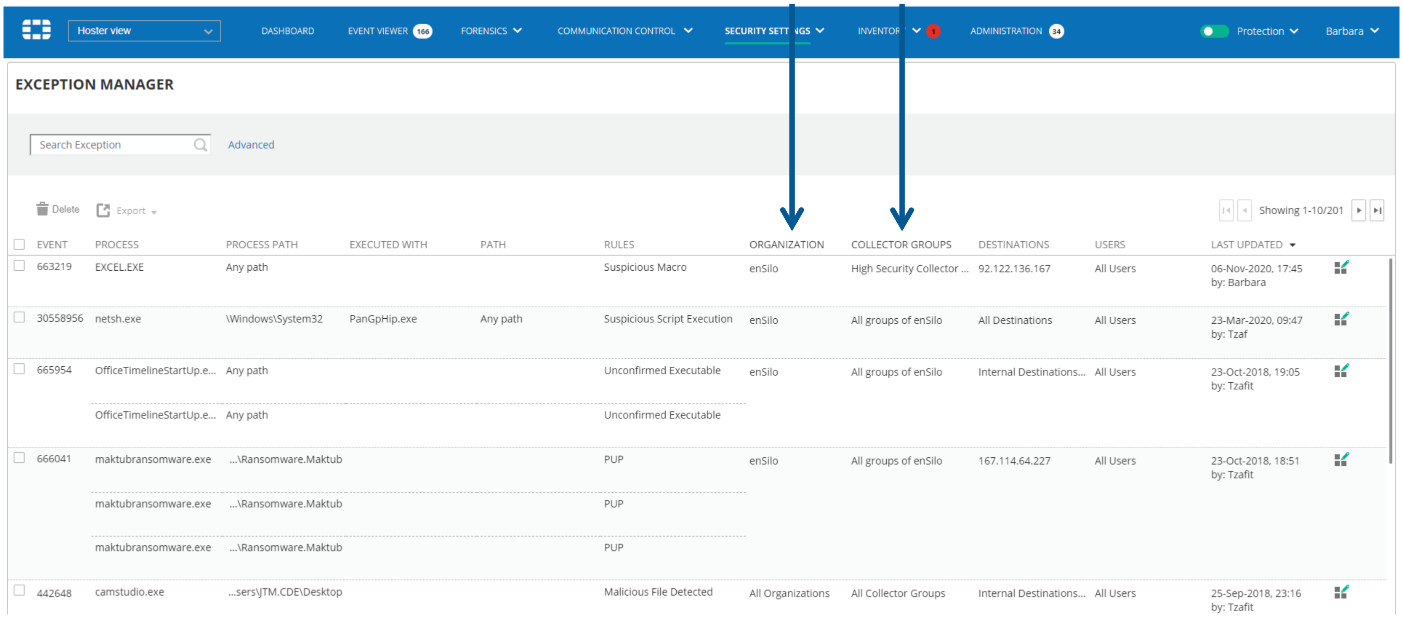
○ ● All users

Triggered Rules:

Suspicious Macro

Type comments

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



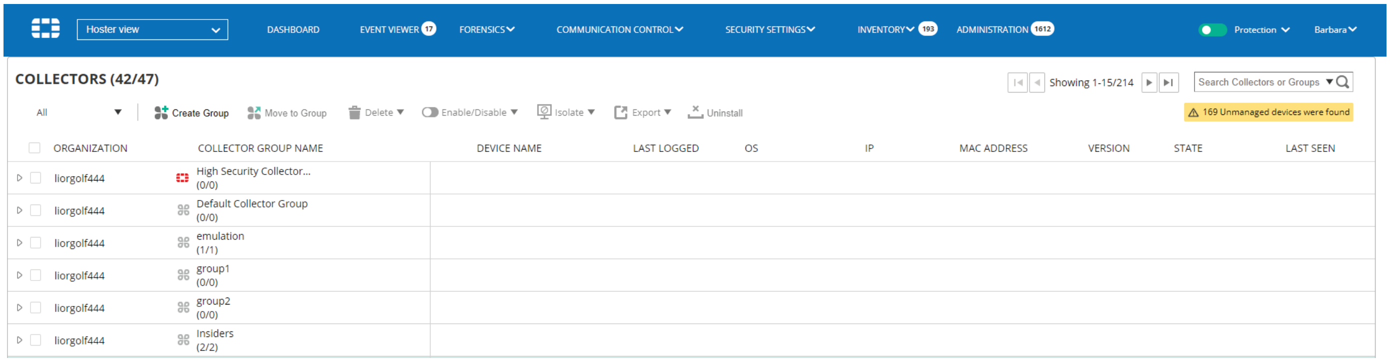
EXCEPTION MANAGER

EVENT	PROCESS	PROCESS PATH	EXECUTED WITH	PATH	RULES	ORGANIZATION	COLLECTOR GROUPS	DESTINATIONS	USERS	LAST UPDATED
663219	EXCEL.EXE	Any path			Suspicious Macro	enSilo	High Security Collector ...	92.122.136.167	All Users	06-Nov-2020, 17:45 by: Barbara
30558956	netsh.exe	\Windows\System32	PanGpHip.exe	Any path	Suspicious Script Execution	enSilo	All groups of enSilo	All Destinations	All Users	23-Mar-2020, 09:47 by: Tzaf
665954	OfficeTimelineStartUp.e...	Any path			Unconfirmed Executable	enSilo	All groups of enSilo	Internal Destinations...	All Users	23-Oct-2018, 19:05 by: Tzafit
	OfficeTimelineStartUp.e...	Any path			Unconfirmed Executable					
666041	maktubransomware.exe	...\Ransomware.Maktub			PUP	enSilo	All groups of enSilo	167.114.64.227	All Users	23-Oct-2018, 18:51 by: Tzafit
	maktubransomware.exe	...\Ransomware.Maktub			PUP					
	maktubransomware.exe	...\Ransomware.Maktub			PUP					
442648	camstudio.exe	...sers\JTM.CDE\Desktop			Malicious File Detected	All Organizations	All Collector Groups	Internal Destinations...	All Users	25-Sep-2018, 23:16 by: Tzafit

Inventory

COLLECTORS Page

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



COLLECTORS (42/47)

⚠ 169 Unmanaged devices were found

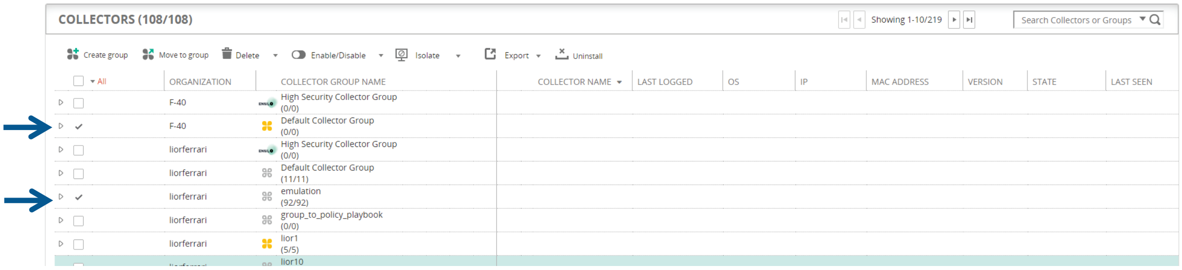
ORGANIZATION	COLLECTOR GROUP NAME	DEVICE NAME	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	STATE	LAST SEEN
liorgolf444	High Security Collector... (0/0)								
liorgolf444	Default Collector Group (0/0)								
liorgolf444	emulation (1/1)								
liorgolf444	group1 (0/0)								
liorgolf444	group2 (0/0)								
liorgolf444	Insiders (2/2)								

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.

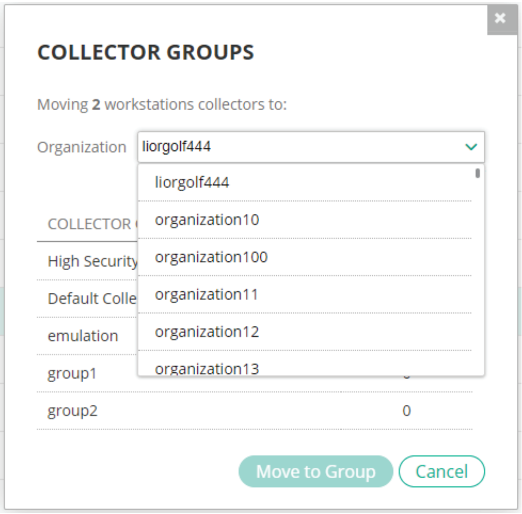
To move a Collector between organizations in Hoster view:

1 Check the checkbox of the Collector Group or check the checkbox(ex) of one or more Collectors.


COLLECTORS (108/108)

☐ All	ORGANIZATION	COLLECTOR GROUP NAME	COLLECTOR NAME	LAST LOGGED	OS	IP	MAC ADDRESS	VERSION	STATE	LAST SEEN
☐	F-40	High Security Collector Group (0/0)								
✓	F-40	Default Collector Group (0/0)								
☐	liorferrari	High Security Collector Group (0/0)								
☐	liorferrari	Default Collector Group (11/11)								
✓	liorferrari	emulation (92/92)								
☐	liorferrari	group_to_policy_playbook (0/0)								
☐	liorferrari	lior1 (5/5)								
☐	liorferrari	lior10								

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



COLLECTOR GROUPS

Moving **2** workstations collectors to:

Organization: liorgolf444

COLLECTOR	
High Security	
Default Colle	
emulation	
group1	
group2	0

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

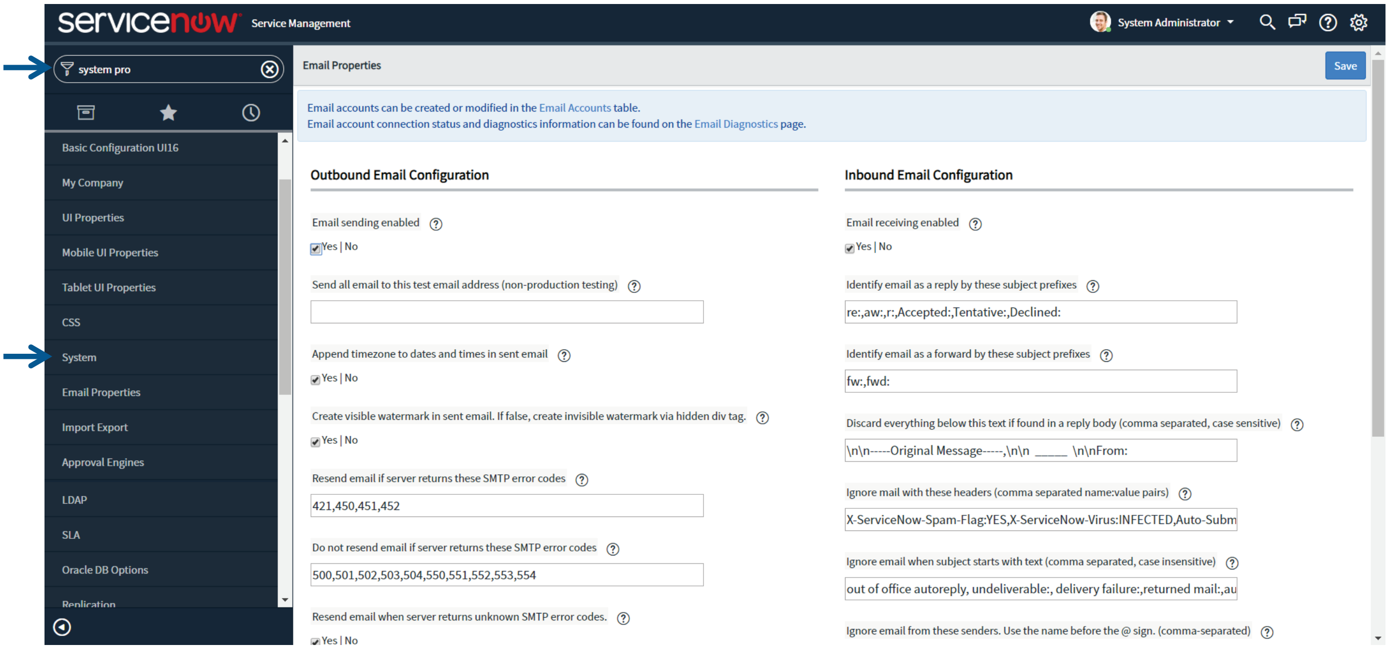
The Open Ticket feature enables you to send events to an event-management tool such as Jira or ServiceNow.

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:



Email Properties

Email accounts can be created or modified in the Email Accounts table.
Email account connection status and diagnostics information can be found on the Email Diagnostics page.

Outbound Email Configuration

Email sending enabled
☑ Yes | No

Send all email to this test email address (non-production testing)

Append timezone to dates and times in sent email
☑ Yes | No

Create visible watermark in sent email. If false, create invisible watermark via hidden div tag.
☑ Yes | No

Resend email if server returns these SMTP error codes
421,450,451,452

Do not resend email if server returns these SMTP error codes
500,501,502,503,504,550,551,552,553,554

Resend email when server returns unknown SMTP error codes.
☑ Yes | No

Inbound Email Configuration

Email receiving enabled
☑ Yes | No

Identify email as a reply by these subject prefixes
re:,aw:,r:,Accepted:,Tentative:,Declined:

Identify email as a forward by these subject prefixes
fw:,fwd:

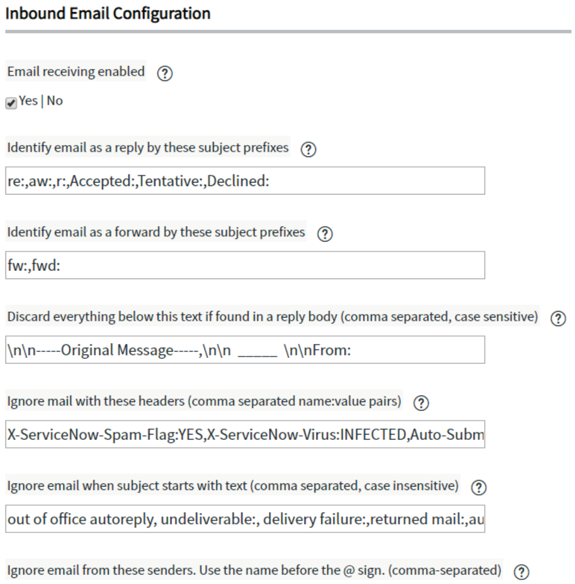
Discard everything below this text if found in a reply body (comma separated, case sensitive)
\n\n-----Original Message-----,\n\n _____ \n\nFrom:

Ignore mail with these headers (comma separated name:value pairs)
X-ServiceNow-Spam-Flag:YES,X-ServiceNow-Virus:INFECTED,Auto-Subm

Ignore email when subject starts with text (comma separated, case insensitive)
out of office autoreply, undeliverable:, delivery failure:,returned mail:,au

Ignore email from these senders. Use the name before the @ sign. (comma-separated)

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



Inbound Email Configuration

Email receiving enabled
☑ Yes | No

Identify email as a reply by these subject prefixes
re:,aw:,r:,Accepted:,Tentative:,Declined:

Identify email as a forward by these subject prefixes
fw:,fwd:

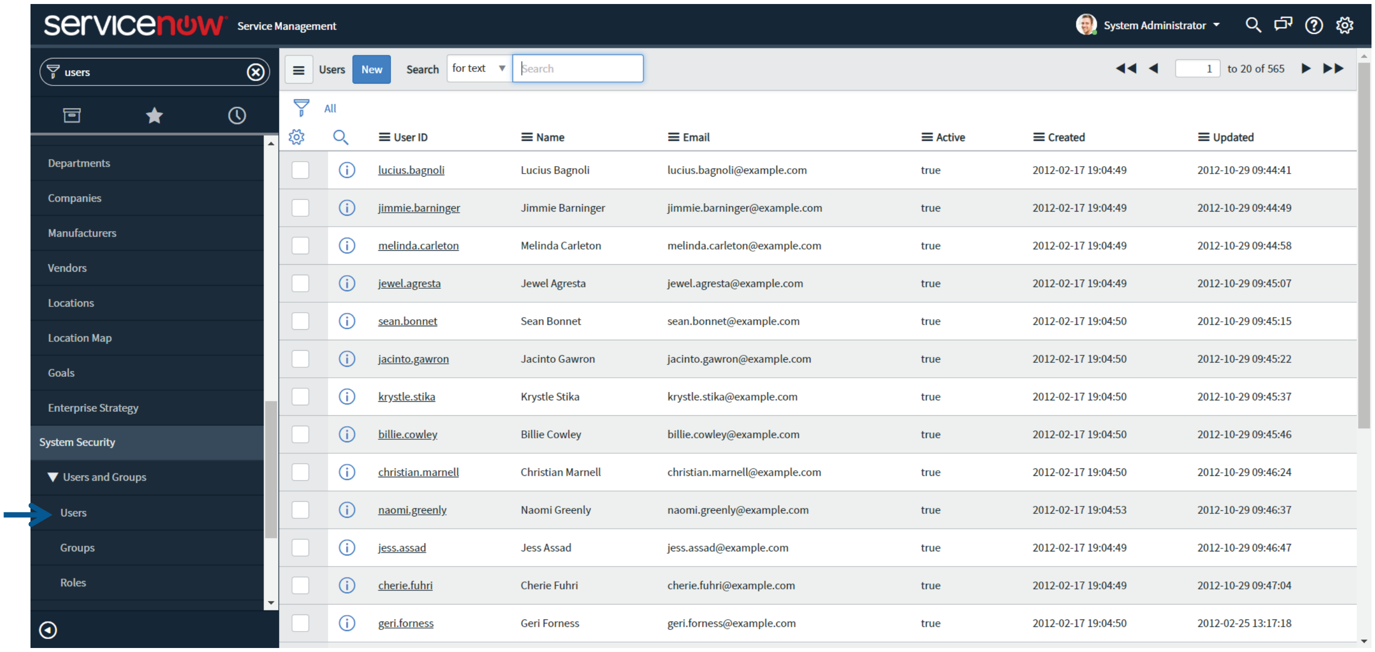
Discard everything below this text if found in a reply body (comma separated, case sensitive)
\n\n-----Original Message-----,\n\n _____ \n\nFrom:

Ignore mail with these headers (comma separated name:value pairs)
X-ServiceNow-Spam-Flag:YES,X-ServiceNow-Virus:INFECTED,Auto-Subm

Ignore email when subject starts with text (comma separated, case insensitive)
out of office autoreply, undeliverable:, delivery failure:,returned mail:,au

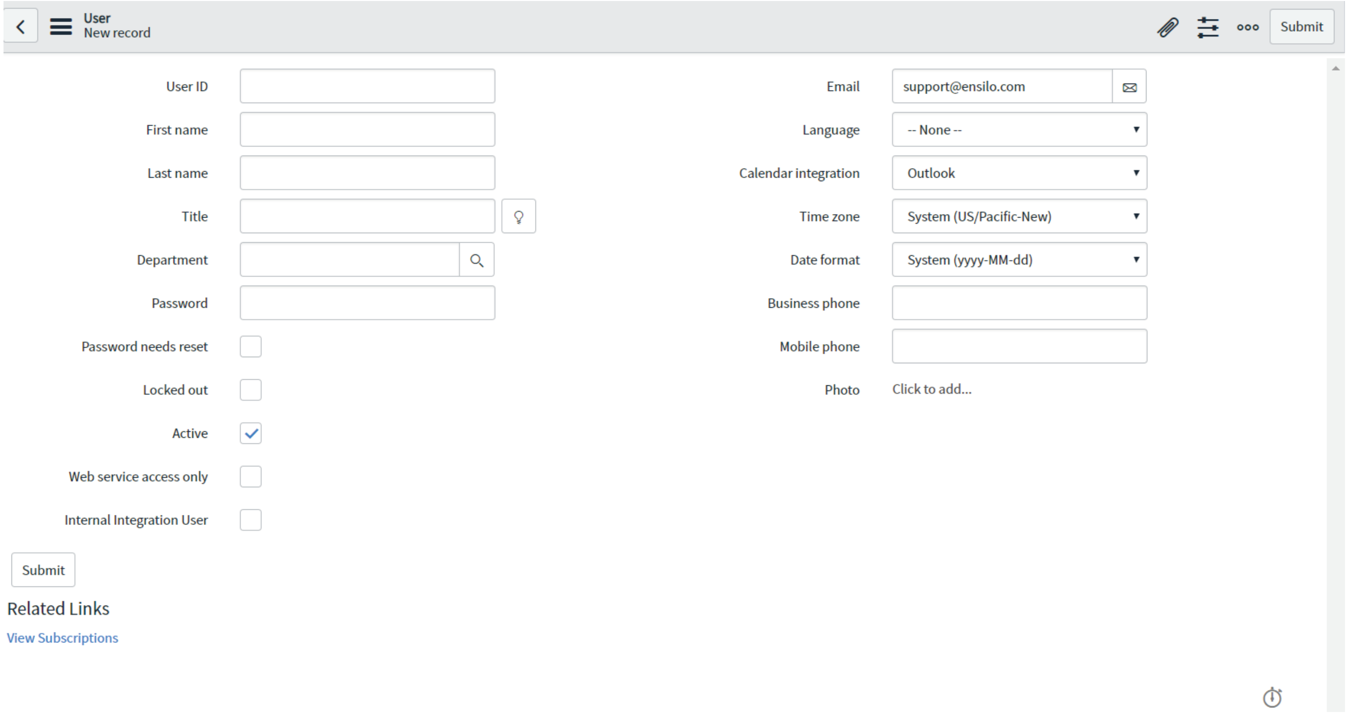
Ignore email from these senders. Use the name before the @ sign. (comma-separated)

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



User ID	Name	Email	Active	Created	Updated
lucius.bagnoli	Lucius Bagnoli	lucius.bagnoli@example.com	true	2012-02-17 19:04:49	2012-10-29 09:44:41
jimmie.barninger	Jimmie Barninger	jimmie.barninger@example.com	true	2012-02-17 19:04:49	2012-10-29 09:44:49
melinda.carleton	Melinda Carleton	melinda.carleton@example.com	true	2012-02-17 19:04:49	2012-10-29 09:44:58
jewel.agresta	Jewel Agresta	jewel.agresta@example.com	true	2012-02-17 19:04:49	2012-10-29 09:45:07
sean.bonnet	Sean Bonnet	sean.bonnet@example.com	true	2012-02-17 19:04:50	2012-10-29 09:45:15
jacinto.gawron	Jacinto Gawron	jacinto.gawron@example.com	true	2012-02-17 19:04:50	2012-10-29 09:45:22
krystle.stika	Krystle Stika	krystle.stika@example.com	true	2012-02-17 19:04:50	2012-10-29 09:45:37
billie.cowley	Billie Cowley	billie.cowley@example.com	true	2012-02-17 19:04:50	2012-10-29 09:45:46
christian.marnell	Christian Marnell	christian.marnell@example.com	true	2012-02-17 19:04:50	2012-10-29 09:46:24
naomi.greenly	Naomi Greenly	naomi.greenly@example.com	true	2012-02-17 19:04:53	2012-10-29 09:46:37
jess.assad	Jess Assad	jess.assad@example.com	true	2012-02-17 19:04:49	2012-10-29 09:46:47
cherie.fuhri	Cherie Fuhri	cherie.fuhri@example.com	true	2012-02-17 19:04:49	2012-10-29 09:47:04
geri.forness	Geri Forness	geri.forness@example.com	true	2012-02-17 19:04:50	2012-02-25 13:17:18

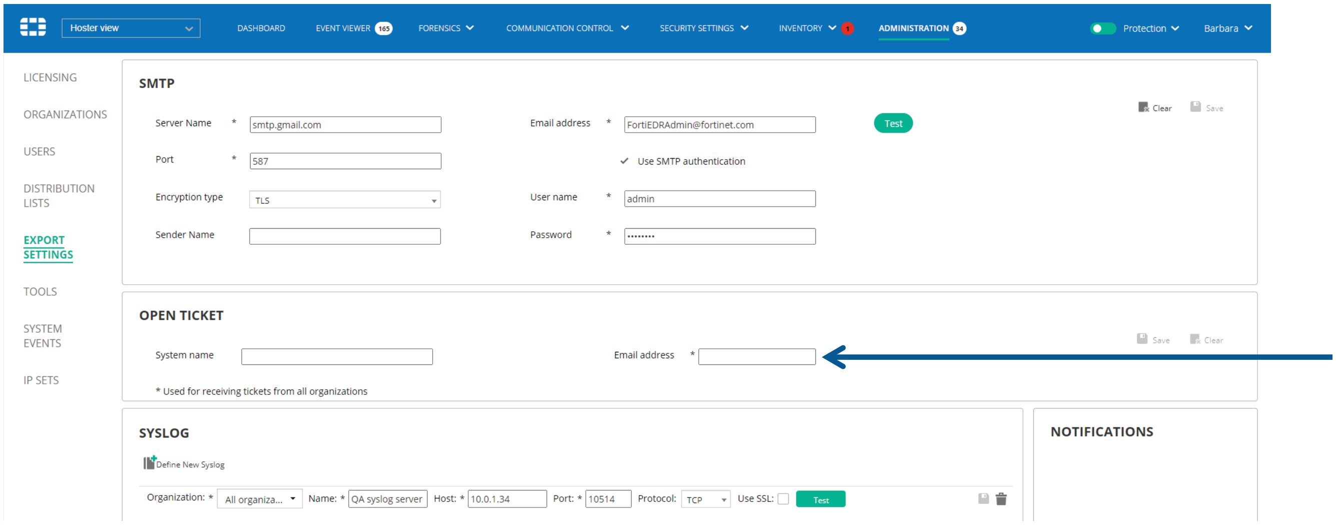
5 Click the New button to create a new user. The following window displays:



User ID	
First name	
Last name	
Title	
Department	
Password	
Password needs reset	□
Locked out	□
Active	☑
Web service access only	□
Internal Integration User	□

Email	support@ensilo.com
Language	-- None --
Calendar integration	Outlook
Time zone	System (US/Pacific-New)
Date format	System (yyyy-MM-dd)
Business phone	
Mobile phone	
Photo	Click to add...

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



SMTP

Server Name * smtp.gmail.com

Port * 587

Encryption type TLS

Sender Name

Email address * FortiEDRAdmin@fortinet.com

✓ Use SMTP authentication

User name * admin

Password * ••••••••

OPEN TICKET

System name

Email address *

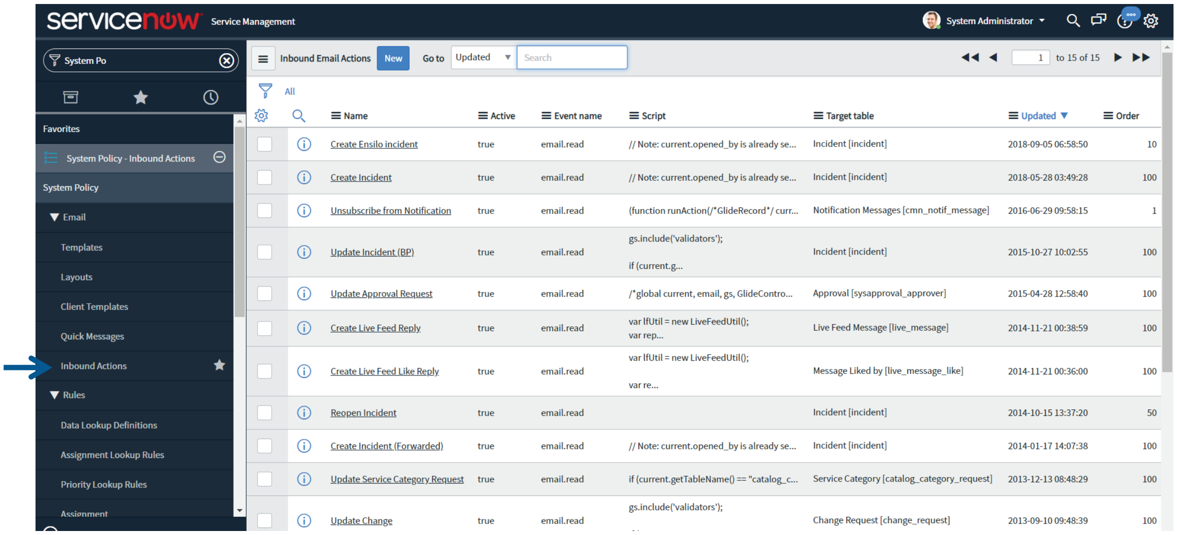
* Used for receiving tickets from all organizations

SYSLOG

Organization: * All organiza... Name: * QA syslog server Host: * 10.0.1.34 Port: * 10514 Protocol: TCP Use SSL: □

NOTIFICATIONS

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



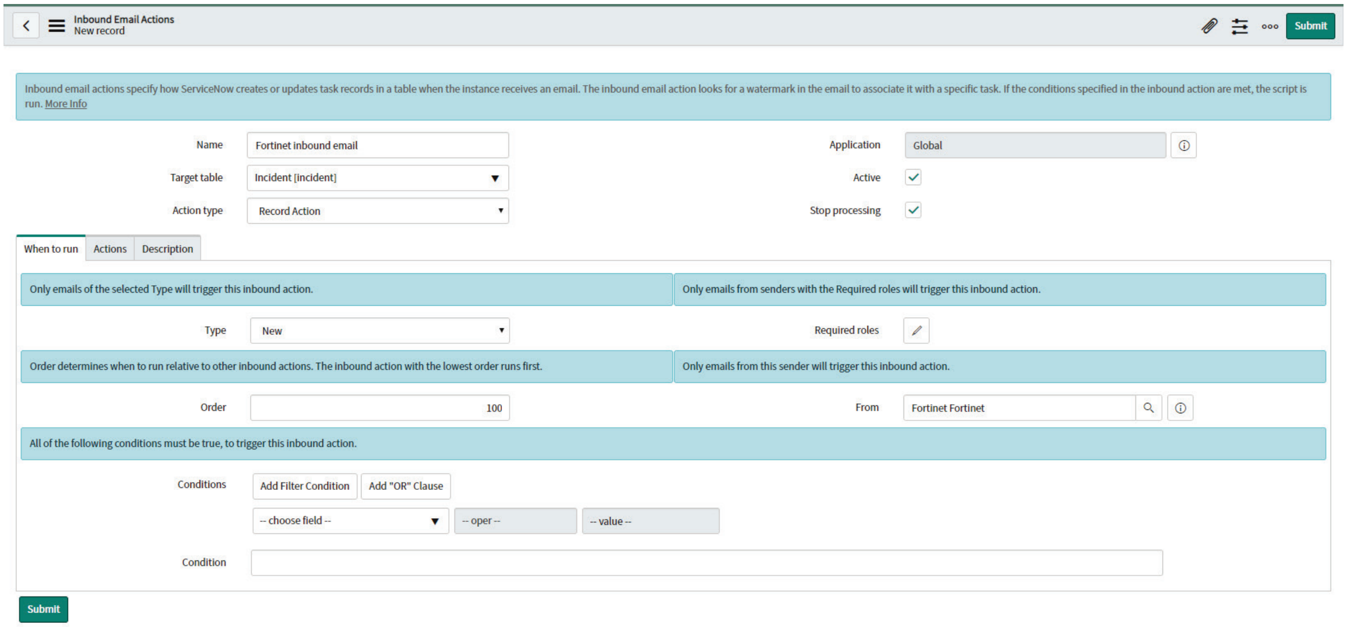
Inbound Email Actions

Name	Active	Event name	Script	Target table	Updated	Order
Create Ensilo incident	true	email.read	// Note: current.opened_by is already se...	Incident [incident]	2018-09-05 06:58:50	10
Create Incident	true	email.read	// Note: current.opened_by is already se...	Incident [incident]	2018-05-28 03:49:28	100
Unsubscribe from Notification	true	email.read	(function runAction(/*GlideRecord*/ curr...	Notification Messages [cmn_notif_message]	2016-06-29 09:58:15	1

Update Incident (BP)	true	email.read	gs.include('validators');
			if (current.g...
				Incident [incident]	2015-10-27 10:02:55	100

Update Approval Request	true	email.read	/*global current, email, gs, GlideContro...	Approval [sysapproval_approver]	2015-04-28 12:58:40	100
Create Live Feed Reply	true	email.read	var lfUtil = new LiveFeedUtil(); var rep...	Live Feed Message [live_message]	2014-11-21 00:38:59	100
Create Live Feed Like Reply	true	email.read	var lfUtil = new LiveFeedUtil(); var re...	Message Liked by [live_message_like]	2014-11-21 00:36:00	100
Reopen Incident	true	email.read		Incident [incident]	2014-10-15 13:37:20	50
Create Incident (Forwarded)	true	email.read	// Note: current.opened_by is already se...	Incident [incident]	2014-01-17 14:07:38	100
Update Service Category Request	true	email.read	if (current.getTableName() == "catalog_c...	Service Category [catalog_category_request]	2013-12-13 08:48:29	100
Update Change	true	email.read	gs.include('validators');	Change Request [change_request]	2013-09-10 09:48:39	100

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



Inbound Email Actions
New record

Submit

Inbound email actions specify how ServiceNow creates or updates task records in a table when the instance receives an email. The inbound email action looks for a watermark in the email to associate it with a specific task. If the conditions specified in the inbound action are met, the script is run. More Info

Name: Fortinet inbound email

Target table: Incident [incident]

Action type: Record Action

Application: Global

Active: ☑

Stop processing: ☑

When to run | Actions | Description

Only emails of the selected Type will trigger this inbound action.

Only emails from senders with the Required roles will trigger this inbound action.

Type: New

Required roles

Order determines when to run relative to other inbound actions. The inbound action with the lowest order runs first.

Only emails from this sender will trigger this inbound action.

Order: 100

From: Fortinet Fortinet

All of the following conditions must be true, to trigger this inbound action.

Conditions: Add Filter Condition | Add "OR" Clause

-- choose field -- | -- oper -- | -- value --

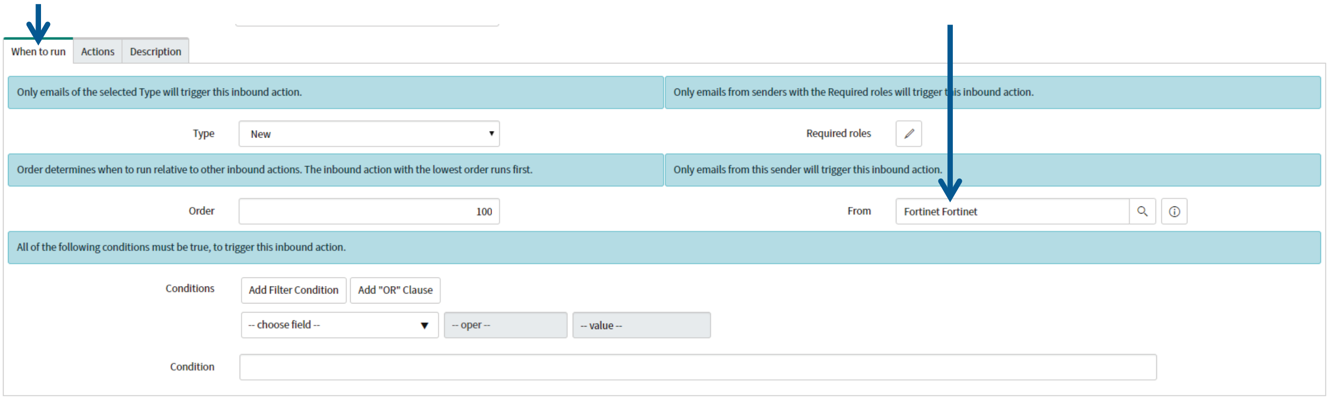
Condition

Submit

9 Fill in the following fields in this window:

- **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**.



When to run | Actions | Description

Only emails of the selected Type will trigger this inbound action.

Only emails from senders with the Required roles will trigger this inbound action.

Type: New

Required roles

Order determines when to run relative to other inbound actions. The inbound action with the lowest order runs first.

Only emails from this sender will trigger this inbound action.

Order: 100

From: Fortinet Fortinet

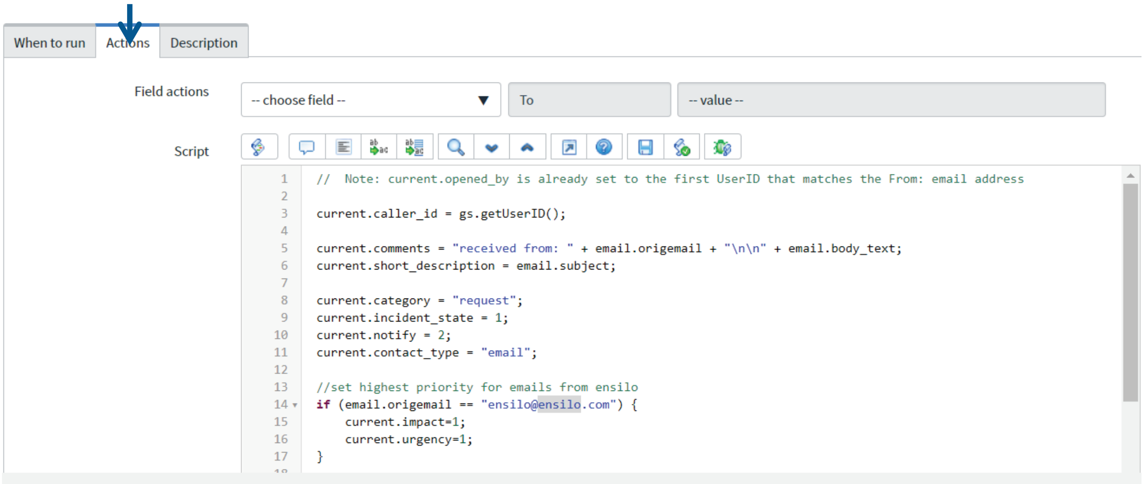
All of the following conditions must be true, to trigger this inbound action.

Conditions: Add Filter Condition | Add "OR" Clause

-- choose field -- | -- oper -- | -- value --

Condition

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



```
//  Note: current.opened_by is already set to the first UserID that matches the From: email address

current.caller_id = gs.getUserID();

current.comments = "received from: " + email.origemail + "\n\n" + email.body_text;
current.short_description = email.subject;

current.category = "request";
current.incident_state = 1;
current.notify = 2;
current.contact_type = "email";

//set highest priority for emails from ensilo
if (email.origemail == "ensilo@ensilo.com") {
    current.impact=1;
    current.urgency=1;
}
```

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 == DoNotReply@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.

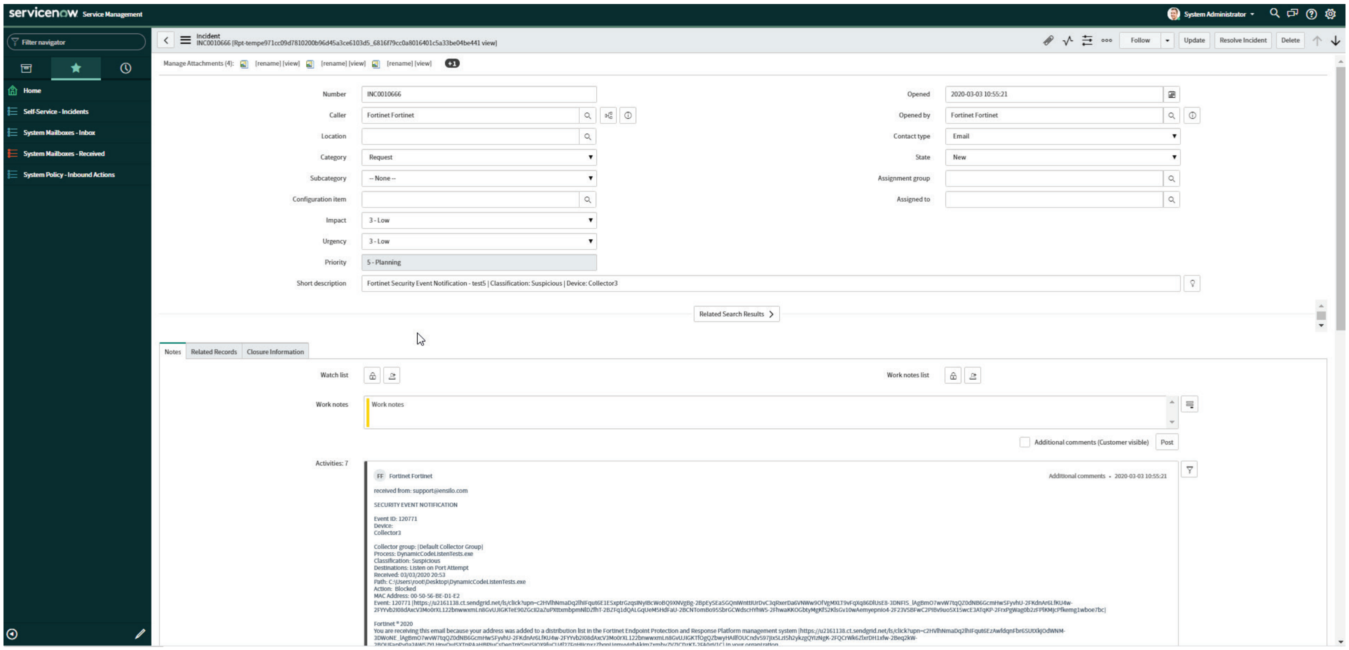
    When FortiEDR sends an email to ServiceNow, a JSON file is attached to it. This JSON file contains the raw data for the event. Once received, you should save this raw data to the ticket.

    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:



Incident
INC0010666 [Rpt-tempe971cc09d7810200b96d45a3ce6103d5_6816f79cc0a8016401c5a33be04be441 view]

Manage Attachments (4): [rename] [view] [rename] [view] [rename] [view] +1

Number	INC0010666	Opened	2020-03-03 10:55:21
Caller	Fortinet Fortinet	Opened by	Fortinet Fortinet
Location		Contact type	Email
Category	Request	State	New
Subcategory	-- None --	Assignment group	
Configuration item		Assigned to	
Impact	3 - Low		
Urgency	3 - Low		
Priority	5 - Planning		
Short description	Fortinet Security Event Notification - test5 | Classification: Suspicious | Device: Collector3		

Watch list

Work notes list

Work notes: Work notes

□ Additional comments (Customer visible)

Activities: 7

FF Fortinet Fortinet — Additional comments • 2020-03-03 10:55:21

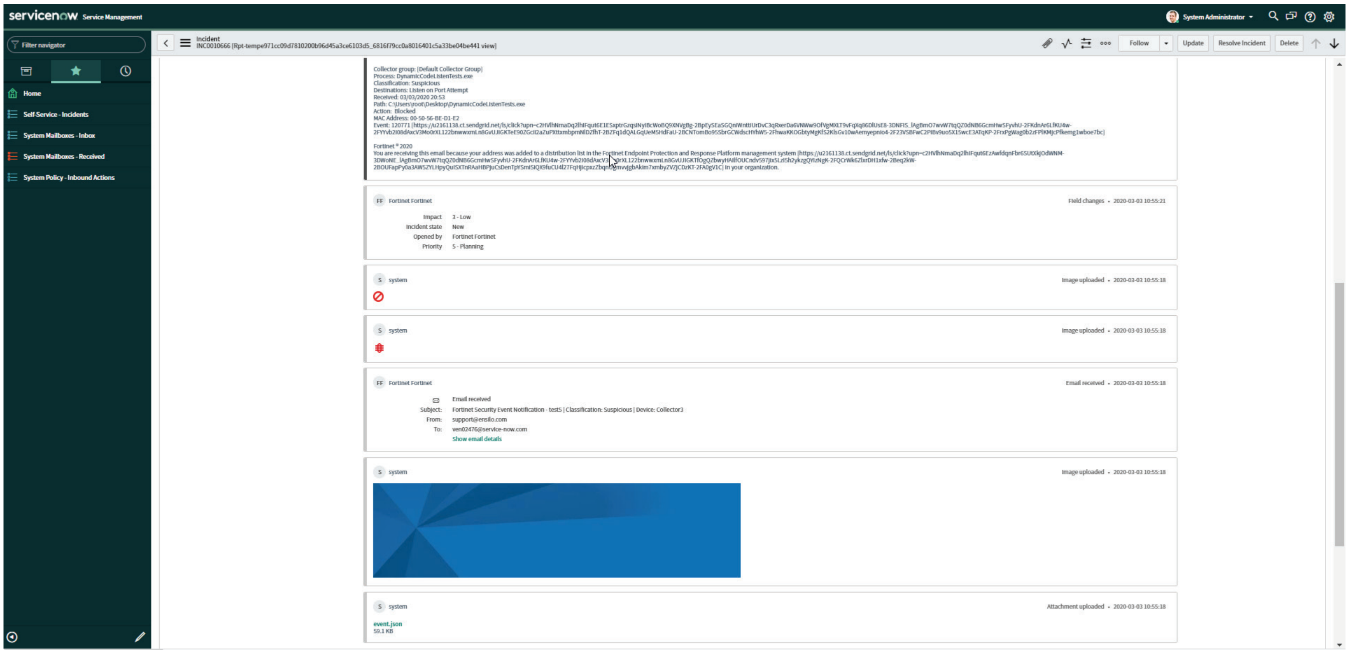
received from: support@ensilo.com

SECURITY EVENT NOTIFICATION

Event ID: 120771
Device:
Collector3

Collector group: [Default Collector Group]
Process: DynamicCodeListenTests.exe
Classification: Suspicious
Destinations: Listen on Port Attempt
Received: 03/03/2020 20:53
Path: C:\Users\root\Desktop\DynamicCodeListenTests.exe
Action: Blocked
MAC Address: 00-50-56-BE-D1-E2
Event: 120771 [https://u2161138.ct.sendgrid.net/ls/click?upn=c2HVlhNmaDq2lhIFqut6E1ESxptrGzqsINyIBcWoBQ9XNVgBg-2BpEySEaSGQnIWnttIUrDvC3qRxerDa6VNWw9OfVgMXLT9vFqXq86DlUsE8-3DNFIS_lAgBmO7wvW7tqQZ0dNB6GcmHwSFyvhU-2FKdnAr6LfKU4w-
2FYYvb2I08dAxcV3Mo0rXL122bnwwxmLn8GvUJIGKTeE90ZGcII2aZuPXttxmbpmNlDZfhT-2BZFq1dQALGqUeM5HdFaU-2BCNTomBo95SbrGCWdscHYhW5-2FhwaKKOGbtyMgKfS2KlsGv10wAemyepnIo4-2F23VSBFwC2PIBv9uo5X15wcE3ATqKP-2FrxPgWag0b2zFPlKMJcPfkemg1wboe7bc]

Fortinet ® 2020
You are receiving this email because your address was added to a distribution list in the Fortinet Endpoint Protection and Response Platform management system [https://u2161138.ct.sendgrid.net/ls/click?upn=c2HVlhNmaDq2lhIFqut6EzAwfdqnFbr6SUtXkJOdWNM-
3DWoNE_lAgBmO7wvW7tqQZ0dNB6GcmHwSFyvhU-2FKdnAr6LfKU4w-2FYYvb2I08dAxcV3Mo0rXL122bnwwxmLn8GvUJIGKTfOgQZbwyHAllfOUCndv597JIx5LzI5h2ykzgQYIzNgK-2FQCrWk6ZlxrDH1xfw-2Beq2kW-
2BOUFapPy0a3AW5ZYLHpyQuISXTnRAaHBPJuCsDenTpYSmISIQX9fuCU4l27FqHJIcpxzZbqn0gmvvjgbAkIm7xmbyZVZJCDzKT-2FA0gV1C] in your organization.



Incident
INC0010666 [Rpt-tempe971cc09d7810200b96d45a3ce6103d5_6816f79cc0a8016401c5a33be04be441 view]

Collector group: [Default Collector Group]
Process: DynamicCodeListenTests.exe
Classification: Suspicious
Destinations: Listen on Port Attempt
Received: 03/03/2020 20:53
Path: C:\Users\root\Desktop\DynamicCodeListenTests.exe
Action: Blocked
MAC Address: 00-50-56-BE-D1-E2
Event: 120771 [https://u2161138.ct.sendgrid.net/ls/click?upn=c2HVlhNmaDq2lhIFqut6E1ESxptrGzqsINyIBcWoBQ9XNVgBg-2BpEySEaSGQnIWnttIUrDvC3qRxerDa6VNWw9OfVgMXLT9vFqXq86DlUsE8-3DNFIS_lAgBmO7wvW7tqQZ0dNB6GcmHwSFyvhU-2FKdnAr6LfKU4w-
2FYYvb2I08dAxcV3Mo0rXL122bnwwxmLn8GvUJIGKTeE90ZGcII2aZuPXttxmbpmNlDZfhT-2BZFq1dQALGqUeM5HdFaU-2BCNTomBo95SbrGCWdscHYhW5-2FhwaKKOGbtyMgKfS2KlsGv10wAemyepnIo4-2F23VSBFwC2PIBv9uo5X15wcE3ATqKP-2FrxPgWag0b2zFPlKMJcPfkemg1wboe7bc]

Fortinet ® 2020
You are receiving this email because your address was added to a distribution list in the Fortinet Endpoint Protection and Response Platform management system [https://u2161138.ct.sendgrid.net/ls/click?upn=c2HVlhNmaDq2lhIFqut6EzAwfdqnFbr6SUtXkJOdWNM-
3DWoNE_lAgBmO7wvW7tqQZ0dNB6GcmHwSFyvhU-2FKdnAr6LfKU4w-2FYYvb2I08dAxcV3Mo0rXL122bnwwxmLn8GvUJIGKTfOgQZbwyHAllfOUCndv597JIx5LzI5h2ykzgQYIzNgK-2FQCrWk6ZlxrDH1xfw-2Beq2kW-
2BOUFapPy0a3AW5ZYLHpyQuISXTnRAaHBPJuCsDenTpYSmISIQX9fuCU4l27FqHJIcpxzZbqn0gmvvjgbAkIm7xmbyZVZJCDzKT-2FA0gV1C] in your organization.

FF Fortinet Fortinet — Field changes • 2020-03-03 10:55:21

Impact	3 - Low
Incident state	New
Opened by	Fortinet Fortinet
Priority	5 - Planning

S system — Image uploaded • 2020-03-03 10:55:18

⊘

S system — Image uploaded • 2020-03-03 10:55:18

FF Fortinet Fortinet — Email received • 2020-03-03 10:55:18

✉	Email received
Subject:	Fortinet Security Event Notification - test5 | Classification: Suspicious | Device: Collector3
From:	support@ensilo.com
To:	ven02476@service-now.com
	Show email details

S system — Image uploaded • 2020-03-03 10:55:18

S system — Attachment uploaded • 2020-03-03 10:55:18

event.json
59.1 KB

Appendix B – LUCENE SYNTAX

The FortiEDR Threat Hunting free-text query is based on Lucene syntax. This syntax consists of terms and operators, as described below. For more details about the use of this query, see page 158.

Terms

A *free-text term* is a single word (for example NetworkService or CryptSvc) or a phrase surrounded by double quotes (for example, "NetworkService -p -s CryptSvc") that searches for all the words in a phrase (in the same order) regardless of the field in which the words appear.

A *Field: Value* term is a combination of a *field* and a *value*.

A list of available fields is provided in the query box, which is an automatically-complete dropdown list.

Examples

Where the Source command line contains the value NetworkService –

```
Source.CommandLine: NetworkService
```

Where the value of the remote IP is 10.151.121.130 –

```
RemoteIP: 10.151.121.130
```

Operators

Operators enable you to customize the search and/or to create more complex queries.

Operators are case insensitive.

OR , || – The query should match either one of the terms/values.

AND, && – The query should match both of the terms/values.

NOT, ! – The query should not match the term/value.

exists – The query should match when the field value is not null.

+ – The term following this operator must be present.

- The term following this operator must not be present.

Example

Where the Event includes either the RemoteIP field that contains 10.151.121.130 or the Remote Port field that contains 443

```
RemoteIP: 10.151.121.130 OR RemotePort: 443
```

Where the ProductName field contains both Microsoft and Windows

```
Source.File.ProductName: (microsoft AND windows)
```

Where the ProductName field contains Microsoft and does not include Windows

```
Source.File.ProductName: (microsoft -windows)
```

Where the Product Name field contains the exact phrase "Microsoft Windows"

```
Source.File.ProductName: "microsoft windows"
```

Where the field Behavior has any non-null value

```
_exists_: Behavior
```

Where the field PID does not include the value 5292

```
Source.PID: (NOT 5292)
```

Where the Event does not include the value 5292 in any of the Event fields

```
NOT 5292
```

Wildcards

Wildcard searches can be run on individual terms using a **?** (question mark) to replace a single character, and an ***** (asterisk) to replace zero or more characters:

```
Progr?m Fil*
```

Note that wildcard queries may consume huge amounts of memory and perform poorly.

Ranges

Ranges can be specified for date, numeric or string fields. The inclusive ranges are specified with square brackets **[**min TO max**]** and exclusive ranges with curly brackets **{**min TO max**}**.

Numbers 1..5

```
count:[1 TO 5]
```

Numbers from 10 upwards

```
count:[10 TO *]
```

Dates before 2012

```
date:{* TO 2012-01-01}
```

Reserved Characters

Should you need to use any of the characters that function as operators in the query itself (and not as operators), then you should escape them with a leading backslash (\). For instance, to search for **c:\Windows\**, write the query as **c\:\\Windows\\**.

Reserved characters are +,-, =, &&, ||, >, <, !, ( ), { }, [ ], ^, ", ~, *, ?, :, \ and /.

Appendix C – CONTAINERS MANAGEMENT