Administration Guide

FortiEndpoint 26.1.b

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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

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

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com



March 06, 2026
FortiEndpoint 26.1.b Administration Guide
94-252-1134987-20260306

TABLE OF CONTENTS

Introduction **7**
Deploying the FortiEndpoint platform **8**
Installing FortiEndpoint on endpoints **10**
Creating a unified FortiClient installer 10
Installing FortiEndpoint on an endpoint and registering to FortiEndpoint EMS 16
Connecting an endpoint to FortiEndpoint 21
Adding a new invitation for a deployment package 24
Customizing invitation code email content 25
Managing Chromebooks with FortiEndpoint 26
Managing endpoints using FortiEndpoint EMS **27**
GUI 28
Banner 28
Left pane 29
Content pane 31
Open Source Licensing Requirements 31
Dashboard 34
Viewing the Status 34
Viewing the Vulnerability Scan dashboard 39
Viewing the Forensics Analysis dashboard 49
Viewing the PUA dashboard 51
Viewing Chromebook Status 52
Endpoint management 53
Windows, macOS, and Linux endpoints 53
All Events 89
Group assignment rules 92
Google Domains 96
Deployment & Installers 101
Manage Deployment 101
FortiClient Installer 106
Endpoint Policy & Components 116
Manage Policies 116
CA Certificates 122
On-fabric Detection Rules 124
Chromebook Policy 130
Endpoint Profiles 131
Editing a default profile 131
Creating a new profile 131
Adding a new Chromebook profile 132
Managing profiles 132
Remote Access 134
ZTNA Destinations 307
Web Filter 320
Video Filter 343
Vulnerability Scan 344

Malware Protection 347
Sandbox 357
Firewall 361
Data Protection 366
FortiDeceptor Campaign 374
System Settings 378
XML Configuration 404
Security Posture Tags 408
Tags 408
Tag Monitor 420
FortiOS dynamic policies using EMS dynamic tags 421
Fabric Device Monitor 425
Fabric & Connectors 427
Fabric Devices 427
Troubleshooting 441
ZTNA Applications Catalog 446
FortiGuard Outbreak Alerts 448
Software Inventory 450
Applications 450
Hosts 473
Quarantine Management 475
Files 475
Allowlist 478
Administration 480
Admin Users 480
Admin roles 480
Authentication Servers 485
Log Viewer 496
User Management 498
Authorized User Groups 498
Verified Users 499
Unverified Users 501
Local users 501
SAML Configuration 502
Invitations 503
Configuring user verification with an LDAP server for authentication 504
Configuring user verification with SAML authentication and an LDAP domain user account 506
Configuring user verification with Entra ID authentication 514
Configuring user verification with SAML authentication and an Entra ID server user account 517
Configuring user verification with SAML authentication and an Okta user account 523
Troubleshooting SAML user verification failure 524
System Settings 532
Configuring EMS settings 533
Uninstalling all endpoints 542
Configuring Logs settings 542

Configuring FortiGuard Services settings 546
Alerts 548
Custom Messages 552
Invitation Email Template 553
Feature Select 555
MDM Integration 558
Endpoint detection and response (EDR) 561
Concepts and workflow 561
EDR terminology 561
FortiEndpoint EDR components 564
How does FortiEndpoint EDR work? 567
Using FortiEndpoint EDR - workflow 567
Incidents 569
Incidents pane 571
Overview 575
Investigation View 576
EDR Connect 592
Marking a security event as handled/unhandled 597
Manually changing the classification of a security event 598
Defining security event exceptions 600
Viewing Application Control security events 600
Viewing Device Control security events 601
Other options in the Incidents viewer 602
Forensics 602
Flow Analyzer view 605
Stack view 606
Compare view 607
Threat Hunting 608
Communication control 647
Applications 647
Policies 662
Host Firewall 672
Profiles 673
Security policies 674
Exception Manager 683
Exclusion Manager 686
Security Content Update 699
Application Control 701
Secure Browser 710
Disk Encryption 712
IP sets 714
EDR 716
Integrations 725
Playbooks 784
Export settings 792
Troubleshooting 797
An EDR Collector does not display in the EMS Endpoints > All Endpoints tab 797
User cannot communicate externally or files modification activity is blocked 798

Threat Hunting tab does not show expected activity events ... 799
Collector is slow or hangs ... 799
Appendix A – Setting up an email feed for open ticket ... 799
Appendix B - Lucene syntax ... 807
Terms ... 807
Operators ... 807
Wildcards ... 808
Ranges ... 808
Reserved characters ... 809
Platform administration ... 810
Accounts ... 811
Adding a secondary admin account ... 811
IAM users ... 812
API access keys ... 813
Upgrading FortiEndpoint ... 815
Allowlisting the FortiEndpoint IP addresses ... 817
Communication from endpoints to FortiEndpoint ... 817
Communication from FortiEndpoint to endpoints ... 818
Notifications ... 819
System maintenance ... 819
Targeted notifications ... 820
Managing notifications in the FortiEndpoint portal ... 821
Using the Fortinet email server for sending alerts ... 823

Introduction

FortiEndpoint is Fortinet's unified endpoint security platform that integrates secure remote access, ZTNA, EPP, EDR, and Data Protection into a single agent with centralized management and simplified licensing—providing end-to-end visibility, prevention, detection, and response for today's modern enterprise.

Deploying the FortiEndpoint platform

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



To migrate from FortiClient Cloud to FortiEndpoint, contact Fortinet Support. Direct in-place migration of standalone FortiEDR Cloud deployments to FortiEndpoint is not currently supported.

To deploy FortiEndpoint:

1. Register the FortiEndpoint subscription contract to your FortiCloud account:

   FortiEndpoint does not support enabling Organization Units (OUs) or registering it under existing OUs. You must log in as an IAM user without OUs enabled or a FortiCloud email user. You can create only one FortiEndpoint instance per FortiCloud account.

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

   You may need to wait a few minutes for the cloud instance to initialize before you can proceed to step 2 or 3.

2. Register the FortiEndpoint endpoint licenses for management by FortiEndpoint:
   a. On the Customer Service & Support site, go to *Asset Management* > *Register Now*.
   b. In the *Registration Code* field, enter your license activation code and select *Next* to continue registering the product.
   c. Select the *Used for Cloud Purpose* checkbox.
   d. Enter your details in the other fields and complete the registration.
3. Access FortiEndpoint in one of the following ways:

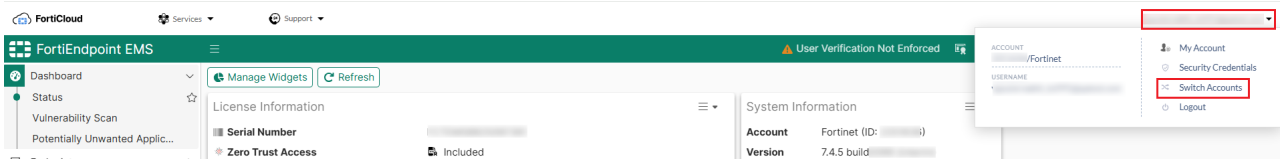
   You must log in as an IAM user without OUs enabled or a FortiCloud email user.

- Access FortiEndpoint from FortiCloud.
- Access FortiEndpoint from the FortiEndpoint portal:
  i. In a browser, go to the FortiEndpoint portal.
  ii. Log in with your FortiCloud credentials.
- Access FortiEndpoint from the link in the welcome email.



If you cannot access the FortiEndpoint portal, ensure that you enable access to `forticlient.forticloud.com:443`. See Allowlisting the FortiEndpoint IP addresses on page 817.

4. When you first log in to FortiEndpoint, you can select the region to store your FortiEndpoint data. Select North America, EMEA, U.K., or APAC.
5. To switch to other accounts that you belong to as a subuser, select your account in the upper right corner of the GUI and then select *Switch Accounts*.



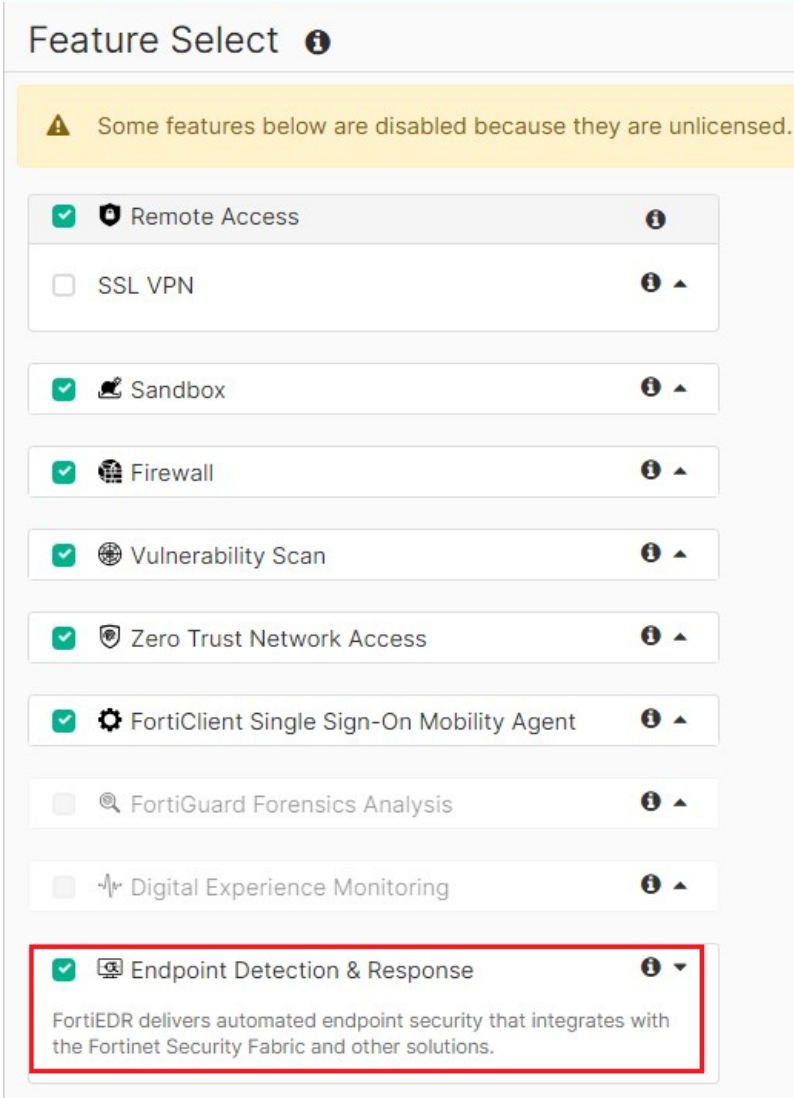
Installing FortiEndpoint on endpoints

Creating a unified FortiClient installer

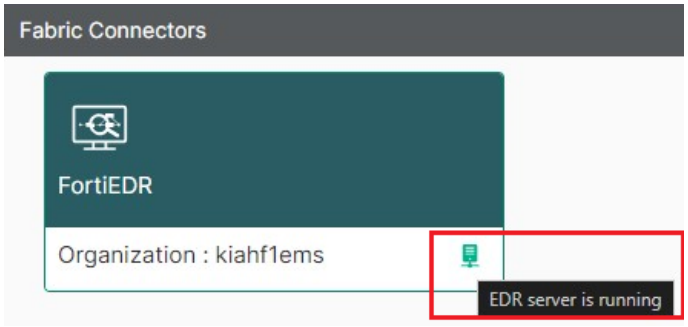
To deploy the FortiEndpoint platform, you first create a unified installer in FortiEndpoint EMS with the endpoint detection and response (EDR) feature enabled to deploy and manage EDR software updates.

To create a FortiClient installer for FortiEndpoint deployment:

1. In FortiEndpoint EMS, go to *System Settings* > *Feature Select* and verify that the *Endpoint Detection & Response* (EDR) feature is available and enabled, which indicates that you have a valid FortiEndpoint EDR Essentials or XDR license.



2. Go to *Fabric & Connectors* > *Fabric Connectors* and verify the EDR server status is running:



3. Go to *Deployment & Installers* > *FortiClient Installer* and click *Add*.
4. On the *General* tab, configure the options depending on the type of FortiClient installer you are using:
   - To use an official FortiClient installer, keep the *Create a manual installer* option disabled under *Advanced Options* at the bottom and set the following options:

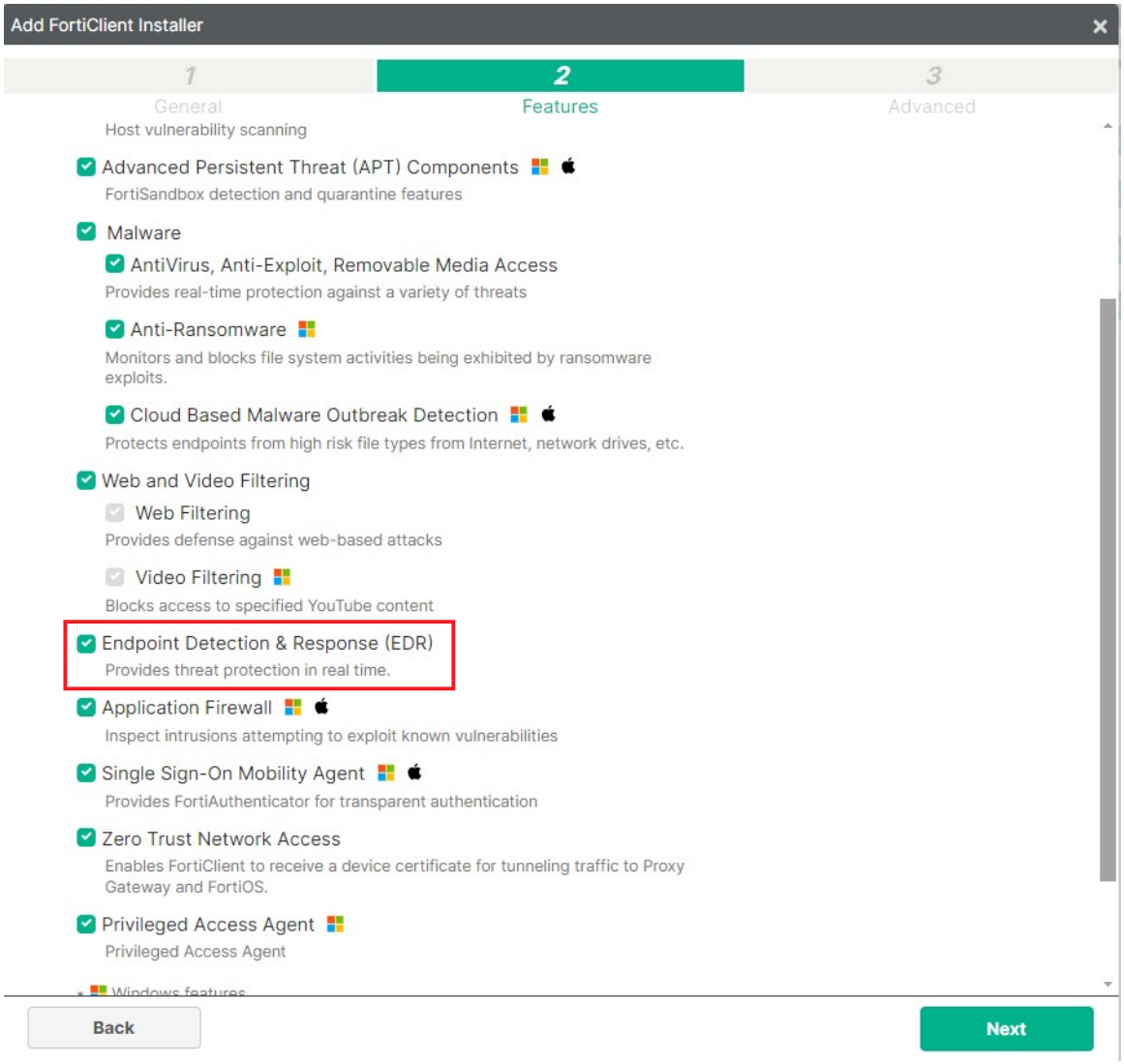
Option	Description
Online Installer Name	Enter the desired installer name.
Add Note	Click to add a note to the installer. In the *Notes* field, enter any details about the installer.
Release	Select the FortiClient release version to install.
Patch	Select the specific FortiClient patch version to install.
Hotfix	If a hotfix is available for the selected patch, the *Hotfix* dropdown list appears. See Adding a FortiClient hotfix installer on page 113.
Auto update to the Latest Patch	Select to enable FortiClient to automatically update to the latest patch release when FortiClient is installed on an endpoint. For more information about the FortiClient upgrade process on the endpoint, see Upgrading FortiClient.
Repackaged Installer Files	Configure which installer files to include.

   - To manually create a FortiClient installer, enable the *Create a manual installer* option under *Advanced Options* at the bottom and set the following options:

Option	Description
Release	Select from the following options: • *Upload packaged installer*—Manually upload a repackaged installer provided by TAC. • *Use custom installer*—Select from a list of previously uploaded custom installers or upload a new custom installer as follows: **a.** Click *Add*. **b.** Specify the custom installer name. **c.** Browse to select 64-bit/32-bit Window and/or Linux/macOS custom installers in ZIP format (FortiEndpoint does not support MSI installers).

Option	Description
	You can download FortiClient installers (in ZIP format) from Fortinet Customer Service & Support., which requires a support account with a valid support contract. **d.** For Windows and Linux, you can also select *Include ARM* and browse to select the ARM installer files. **e.** Click *Upload*.
Manual Installer Name	Enter the desired custom installer name.

5. Click *Next* and select *Endpoint Detection & Response (EDR)* on the *Features* tab.



6. Select other features as n

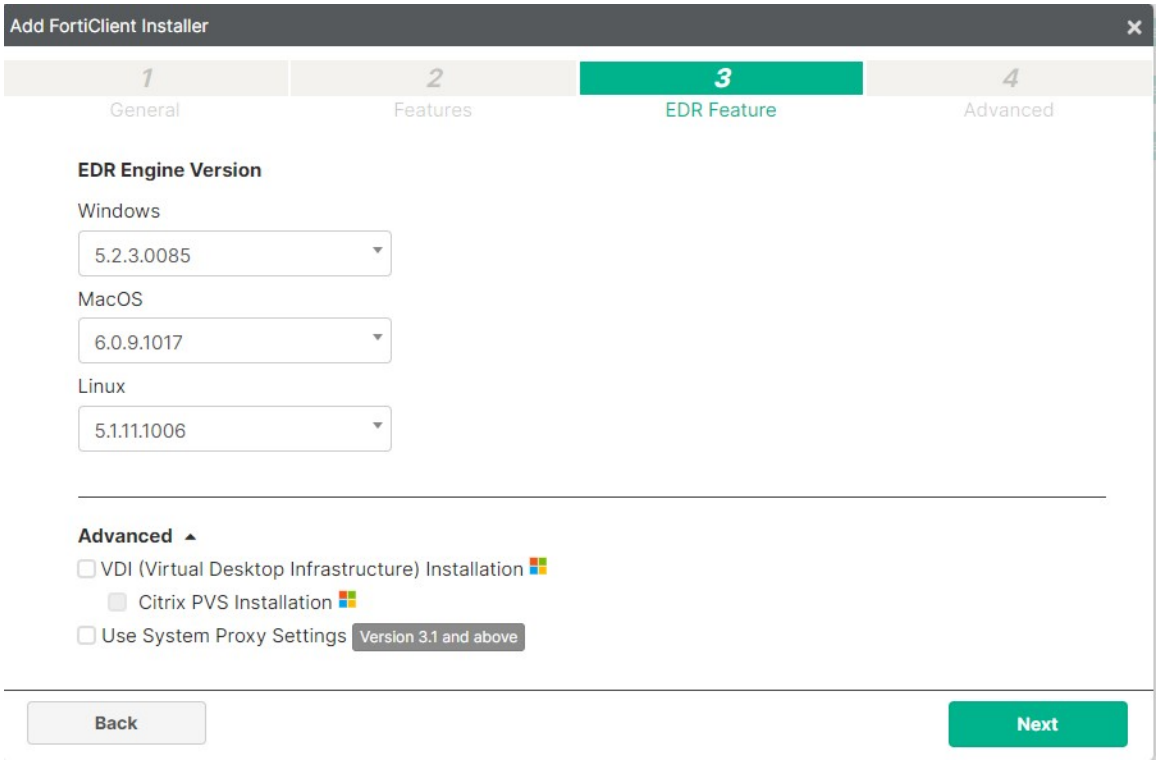


Available options may differ depending on the features you have enabled or disabled in *System Settings > Feature Select*.

Option	Description
Zero Trust Telemetry	Enabled by default and cannot be disabled. Installs FortiClient with Telemetry enabled.
Secure Access Architecture Components	Install FortiClient with SSL and IPsec VPN enabled. Disable to omit SSL and IPsec VPN support from the FortiClient deployment package. If you enable this feature for a deployment package and include a preconfigured VPN tunnel in the included endpoint profile, users who use this deployment package to install FortiClient can connect to this preconfigured VPN tunnel for three days after their initial FortiClient installation. This is useful for remote users, as it allows them to connect to the corporate network to activate their FortiClient license. If the user does not activate their FortiClient license within the three days, all FortiClient features, including VPN, stop working on their device. See Remote Access on page 134 for details on configuring a VPN tunnel.
Vulnerability Scan	Enabled by default and cannot be disabled. Installs FortiClient with Vulnerability Scan enabled.
Advanced Persistent Threat (APT) Components	Install FortiClient with APT components enabled. Disable to omit APT components from the FortiClient deployment package. Includes FortiSandbox detection and quarantine features.
Malware	Enable any of the following features: • AntiVirus, Anti-Exploit, Removable Media Access • Anti-Ransomware • Cloud Based Malware Outbreak Detection Disable to exclude features from the FortiClient installer.
Web and Video Filtering	Enable any of the following features: • Web Filtering • Video Filtering Disable to exclude features from the FortiClient installer.
Application Firewall	Enable or disable Application Firewall in the FortiClient installer.
Single Sign-On Mobility Agent	Enable or disable single sign-on mobility agent in the FortiClient installer.

Option	Description
Zero Trust Network Access	Enable or disable zero trust network access (ZTNA) in the FortiClient installer. The ZTNA feature is always installed on a macOS endpoint, regardless of whether this option is enabled or disabled.
Privileged Access Agent	Enable or disable privileged access agent in the FortiClient installer.

7. On the *EDR Feature* tab, select the desired engine versions under *EDR Engine Version*. By default, the latest versions are selected.



8. Configure the options in the *Advanced* section as needed and click *Finish*.

Option	Description
Enable desktop shortcut	Configure the FortiClient deployment package to create a desktop shortcut on the endpoint.
Enable start menu shortcut	Configure the FortiClient deployment package to create a Start menu shortcut on the endpoint.
Include MSI installer files	Disable this option as FortiEndpoint does not support MSI installers.
Enable Installer ID	Configure an installer ID. Select an existing installer ID or enter a new installer ID. If creating an installer ID, select a group path or create a new group in the *Group Path* field. FortiEndpoint EMS automatically groups endpoints according to installer ID group assignment rules. See Group assignment rules on page 92.

Option	Description
	If you manually move the endpoint to another group after FortiEndpoint EMS places it into the group defined by the installer ID group assignment rule, FortiEndpoint EMS returns the endpoint to the group defined by the installer ID group assignment rule. In an environment with a large number of endpoints, since you can configure each deployment package with only one installer ID, it may be inefficient to create a deployment package for each installer ID. See Deploying different installer IDs to endpoints using the same deployment package on page 105.
Enable Endpoint VPN Profile	Select an endpoint VPN profile to include in the installer. FortiEndpoint EMS applies the VPN profile to the endpoint once it has installed FortiClient. This option is necessary if users require VPN connection to connect to FortiEndpoint EMS.
Enable Endpoint System Profile	Select an endpoint system profile to include in the installer. FortiEndpoint EMS applies the system profile to the endpoint once it has installed FortiClient. This option is necessary if it is required to have certain security features enabled prior to contact with FortiEndpoint EMS.
Invalid Certificate Action	Select the action to take when FortiClient attempts to connect to FortiEndpoint EMS with an invalid certificate: • **Warn**: warn the user about the invalid server certificate. Ask the user whether to proceed with connecting to FortiEndpoint EMS, or terminate the connection attempt. FortiClient remembers the user's decision for this FortiEndpoint EMS, but displays the warning prompt if FortiClient attempts to connect to another FortiEndpoint EMS (using a different FortiEndpoint EMS FQDN/IP address and certificate) with an invalid certificate. • **Allow**: allows FortiClient to connect to FortiEndpoint EMS with an invalid certificate. • **Deny**: block FortiClient from connecting to FortiEndpoint EMS with an invalid certificate.

The unified installer will be added to FortiEndpoint EMS and displayed on the *Manage Installers* > *Deployment Packages* pane.

You can then deploy the unified installer to applicable endpoints just as you deploy any other FortiClient installer. The unified installer will install FortiClient and the EDR Collector on the endpoint if it is not already installed. See Installing FortiEndpoint on an endpoint and registering to FortiEndpoint EMS on page 16.

Installing FortiEndpoint on an endpoint and registering to FortiEndpoint EMS

After Creating a unified FortiClient installer on page 10, you must push the FortiClient installer to applicable endpoints which will install FortiClient and the EDR Collector on the endpoint if they are not already installed.

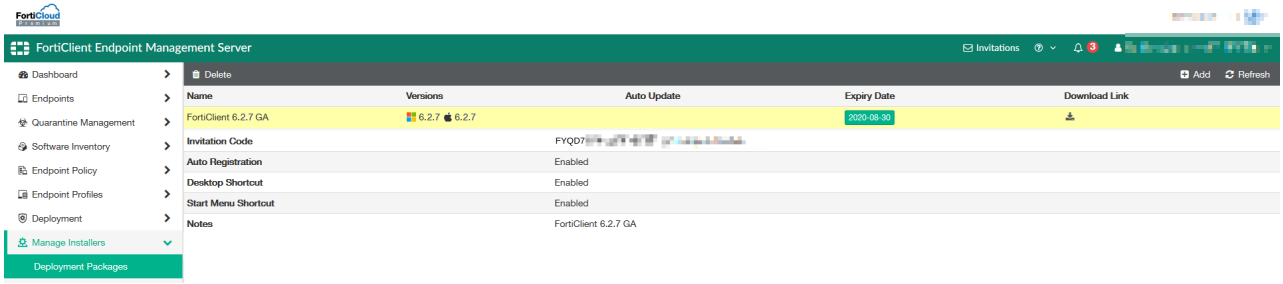
To deploy FortiEndpoint to Windows and macOS endpoints:

See Initially deploying FortiEndpoint software to endpoints.

To install FortiEndpoint on an endpoint:

When installing FortiEndpoint on an endpoint from a deployment package created in FortiEndpoint, the administrator carries out some actions, while the endpoint user carries out others.

1. (Administrator) In FortiEndpoint EMS, go to *Manage Installers* > *Deployment Packages*. Note the invitation code for the desired deployment package.

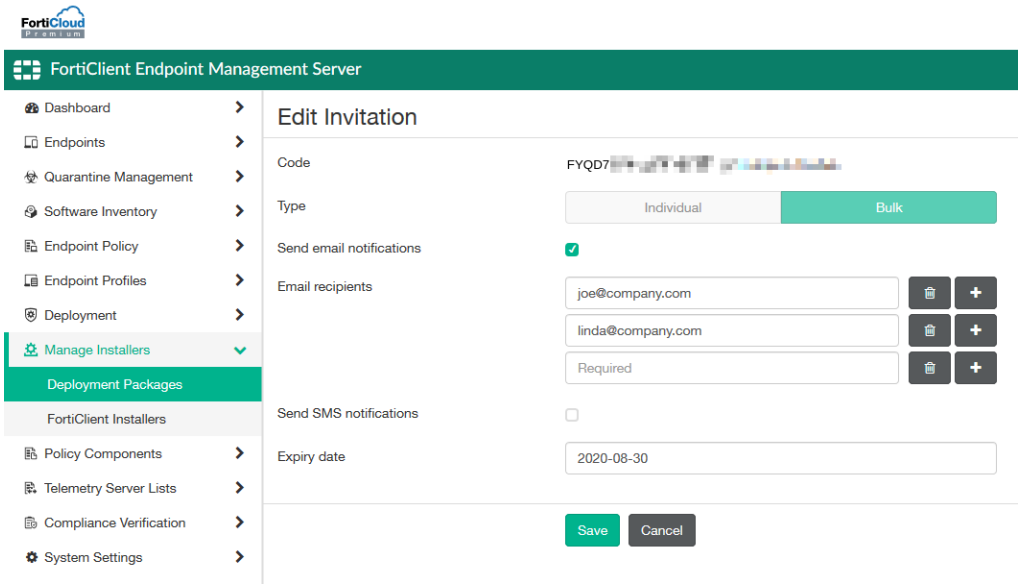


2. (Administrator) Go to *Invitations* in the upper right corner or in *Endpoints* > *Invitations*.
3. (Administrator) Select the invitation code that was noted in step 2. Click *Edit*.
4. (Administrator) Configure the invitation code:
   a. (Administrator) To send the code to a single recipient, select *Individual*. Otherwise, select *Bulk*.

   Sending individual invitation codes is considered best practice, as it can limit unexpected endpoints from connecting to FortiEndpoint.

   b. (Administrator) In the *Email recipients* field, enter the email addresses of the desired end users.
   c. (Administrator) If desired, enable *Send SMS notifications*.
   d. (Administrator) In the *SMS recipients* field, enter the phone numbers of the desired end users.

e. (Administrator) In the *Expiry date* field, set the expiry date. Click *Save*.

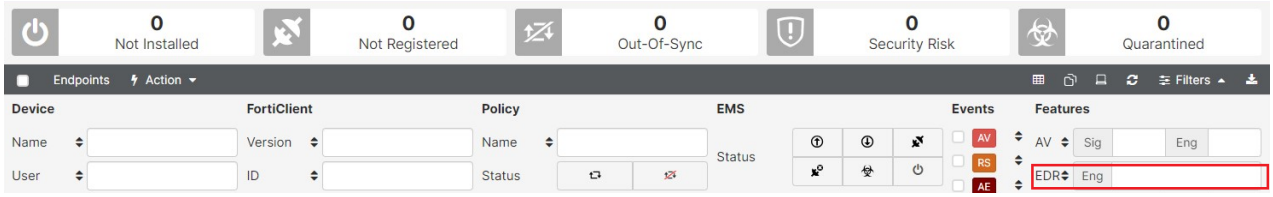


5. (Administrator) The email that users receive for an individual invitation code does not include a FortiEndpoint download link. You must share the installer files with users, or send them the link to FortiClient.com, from where they can download the installer files.
6. (End user) Install FortiEndpoint on your device. The FortiEndpoint invitation email or text message that you received may include a FortiEndpoint download link. Otherwise, your administrator should have provided the installer files or a link where you can download them.
7. (End user) Your FortiEndpoint may automatically register to FortiEndpoint after installation. If not, use the instructions in Connecting an endpoint to FortiEndpoint on page 21 to register to FortiEndpoint.

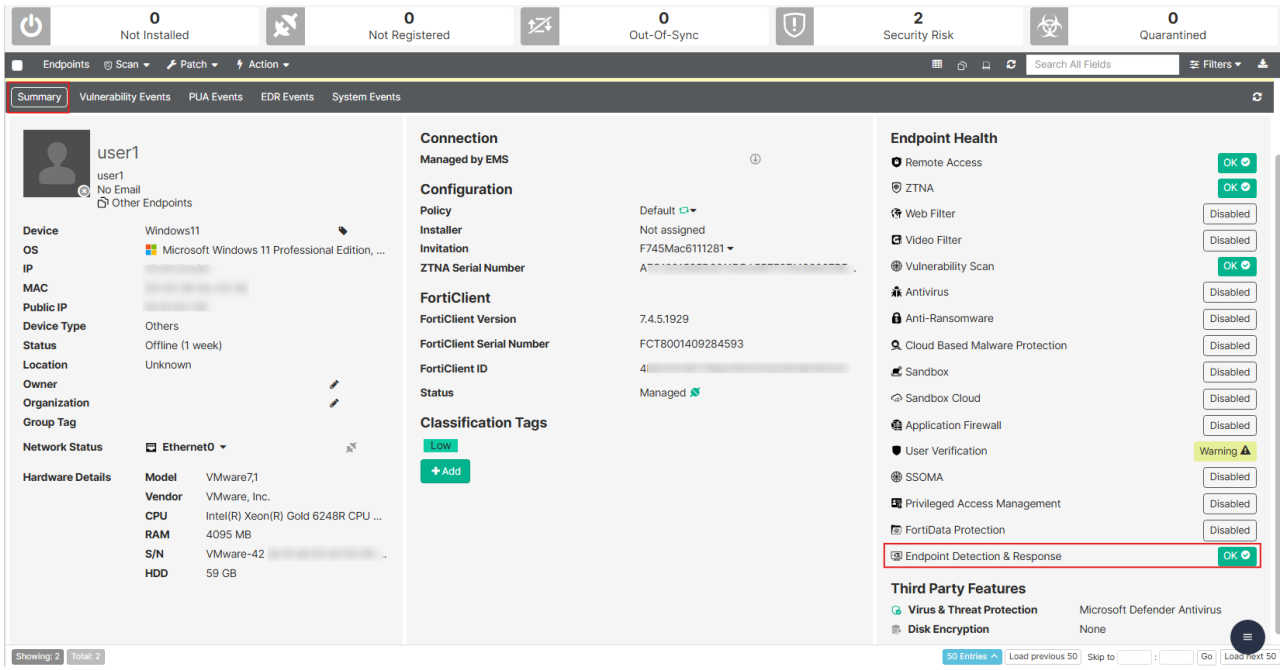
FortiEndpoint creates a Collector group with the same name as the deployment using the EDR connector. When you assign endpoints to the deployment, the EDR connector assigns the same endpoints to the associated EDR Collector group.

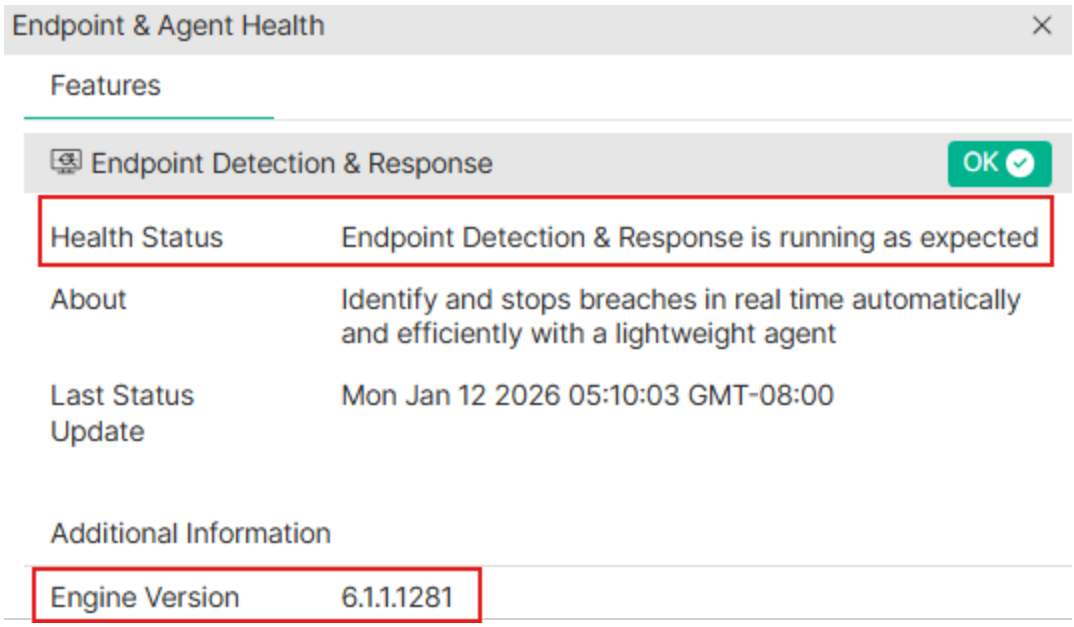
To verify the FortiEndpoint deployment is successful:

1. In FortiEndpoint EMS, go to the *Endpoints > All Endpoints* page (see Endpoint management on page 53) and verify that a new *EDR - Eng* filter is available for filtering endpoints based on their EDR engine version:

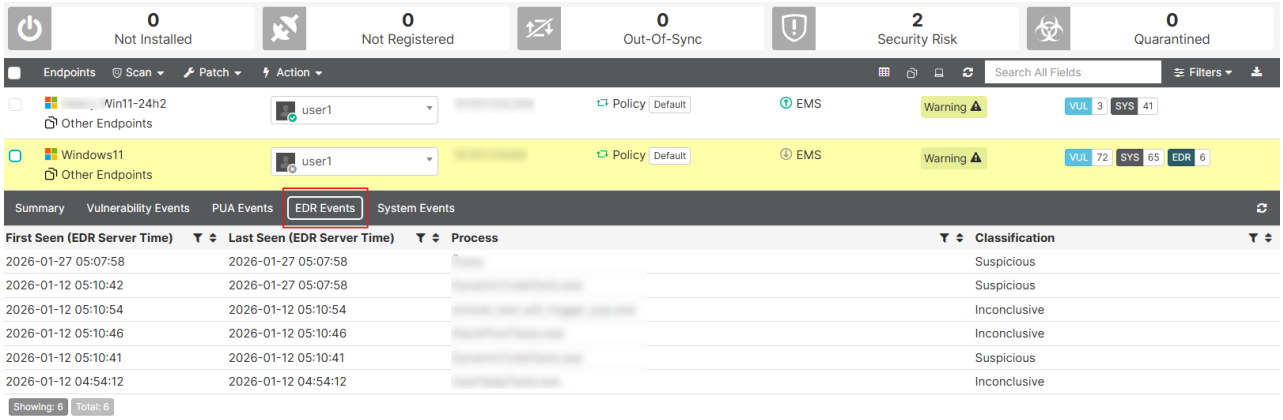


2. Go to the details page of an endpoint with the unified installer deployed. Verify that *Endpoint Detection & Response* is enabled in the *Summary* tab. Click *OK* to view more details about Endpoint & Agent Health status and the EDR engine version.

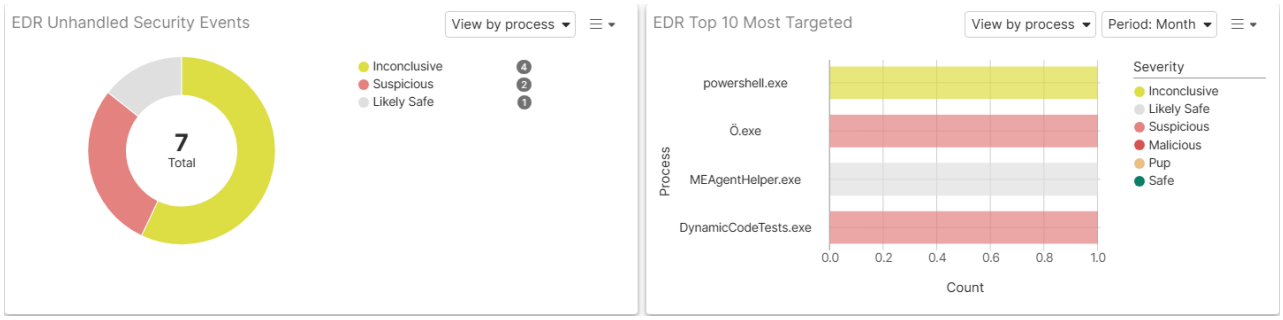




If EDR detects an event, you can view the details in the *EDR Events* tab.



3. Go to the FortiEndpoint EMS dashboard and verify the *EDR Unhandled Security Events* and *EDR Top 10 Most Targeted* widgets are displayed.



4. On the endpoint, open FortiClient and confirm that the *Detection & Response* tab is displayed.

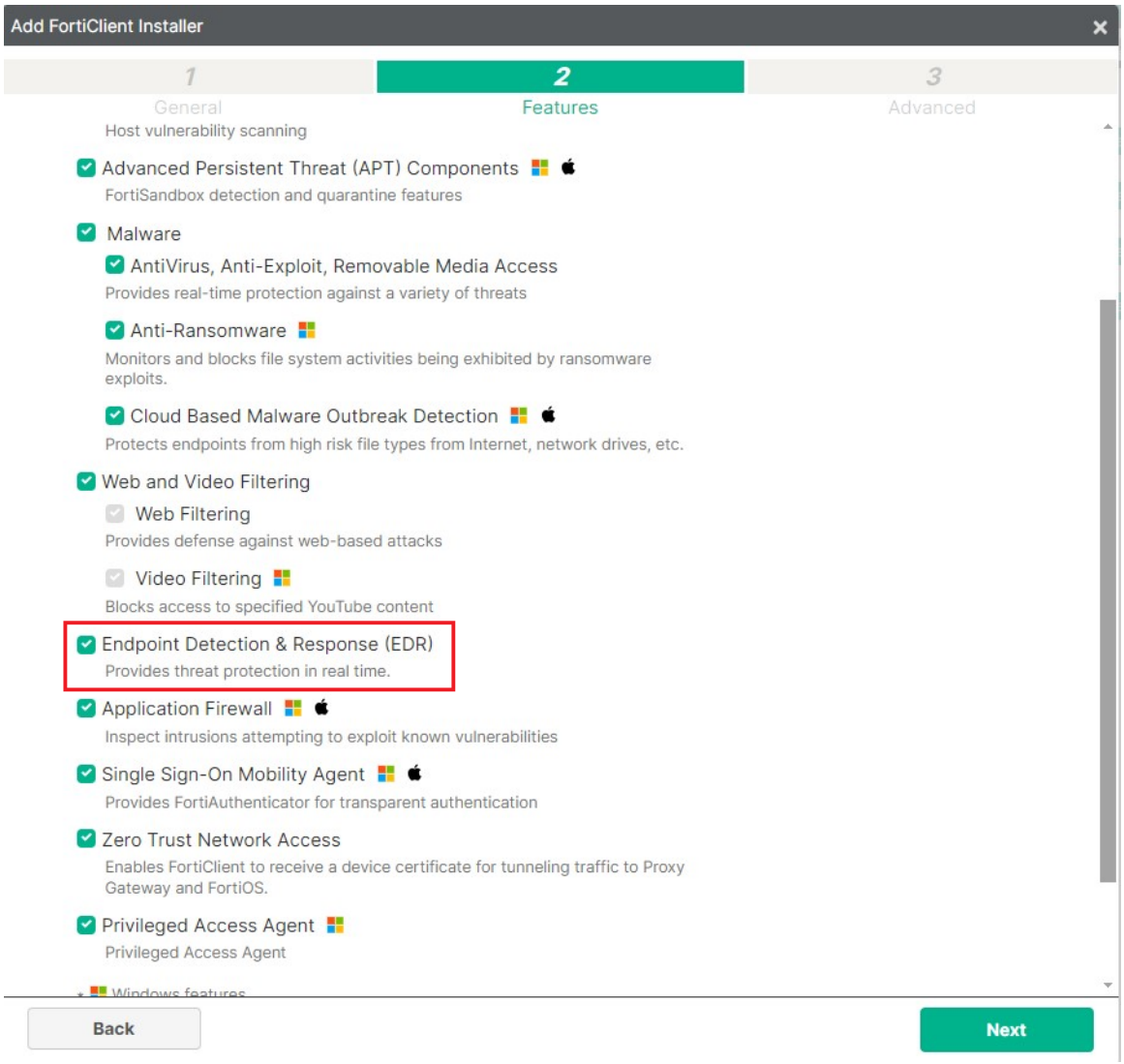


To uninstall the EDR Collector on endpoints after deploying FortiEndpoint, change the configuration of the FortiClient unified installer to exclude the EDR feature:

Users cannot uninstall the EDR Collector (installed through a FortiEndpoint deployment) locally on the endpoint, which may cause issues.

1. Go to *Deployment & Installers* > *FortiClient Installer*.
2. Select the unified installer for the FortiEndpoint deployment and click *Edit*.
3. Configure the *General* tab as desired, then click *Next*.

4. On the *Features* tab, disable *Endpoint Detection & Response (EDR)* and click *Next*.

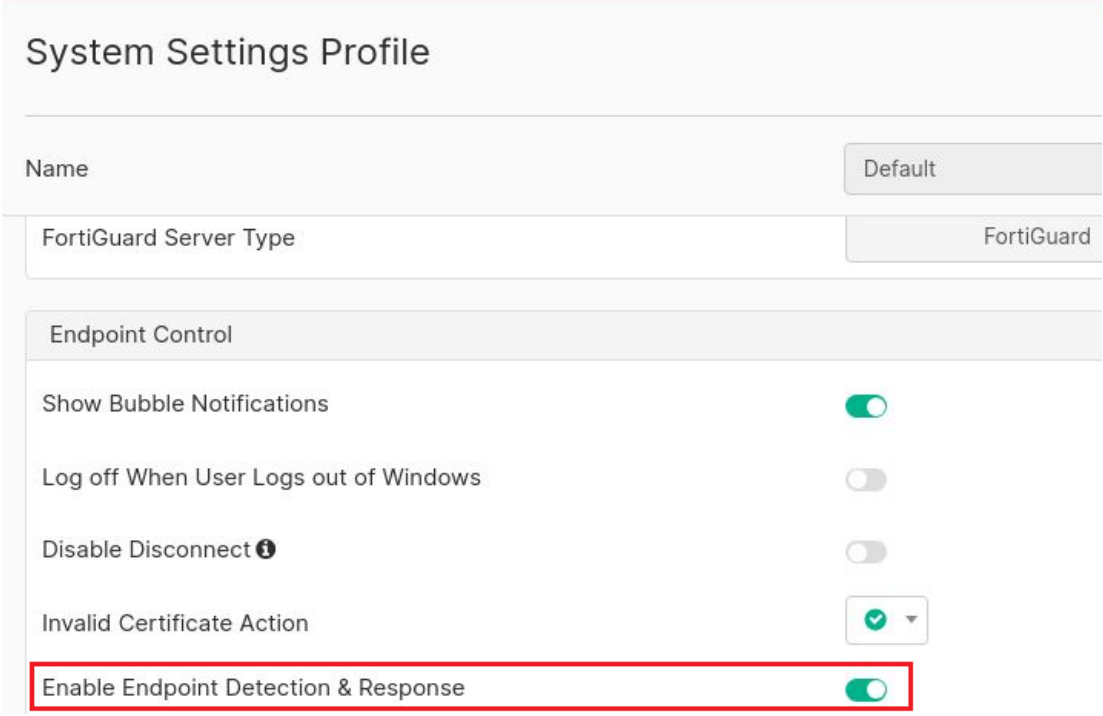


5. Click *Next* and complete the installer configuration.

   The FortiClient unified installer is updated to exclude the EDR feature and will be pushed to the endpoints with the EDR Collector uninstalled.

To disable the EDR feature without uninstalling the EDR Collector on some endpoints:

1. In FortiEndpoint EMS, go to *Endpoint Profiles > System Settings*.
2. Select the applicable profile for the endpoints and click *Edit*.
3. Disable the *Enable Endpoint Detection & Response* option under *Endpoint Control*.



4. Click *Save*.
   This will de-register the EDR Collector on the endpoints (with the profile applied) to the EDR management console without uninstalling the EDR Collectors from those endpoints.

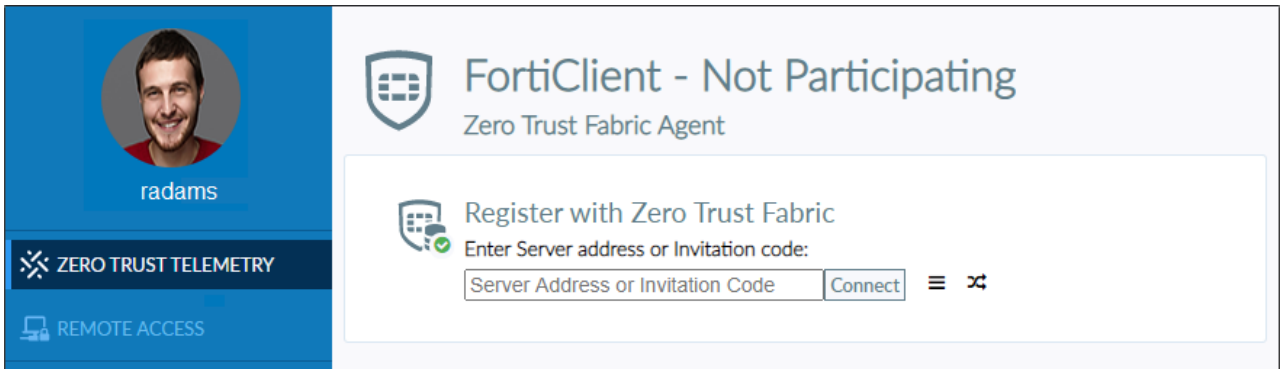
Connecting an endpoint to FortiEndpoint

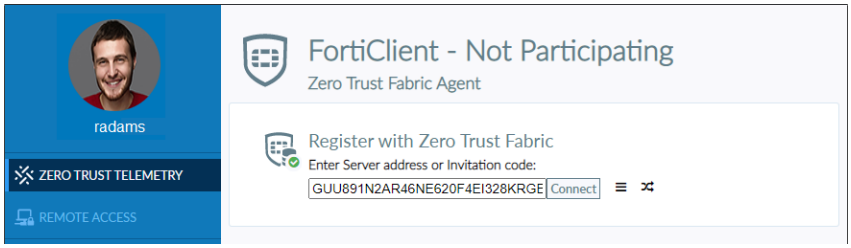
You can use the following instructions to connect to FortiEndpoint in one of the following scenarios:

- If you want to connect a Linux, iOS, or Android endpoint to FortiEndpoint. Since you cannot create a deployment package for these operating systems in FortiEndpoint, this is the only way to register these endpoints to FortiEndpoint.
- If an endpoint did not automatically register to FortiEndpoint after FortiEndpoint installation.

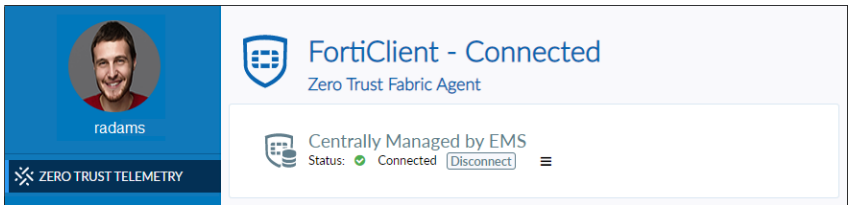
To register Windows, macOS, or Linux endpoints to FortiEndpoint:

1. If your administrator is using FortiEndpoint, you should receive an invitation email. Use the link in the invitation email to download FortiEndpoint to your device.
2. Run the downloaded installer to install FortiEndpoint.
3. After initial installation, FortiEndpoint should automatically register to FortiEndpoint EMS. If FortiEndpoint does not automatically register to FortiEndpoint EMS, enter the invitation code in the *Join FortiEndpoint* field on the *Zero Trust Telemetry* tab in FortiEndpoint.



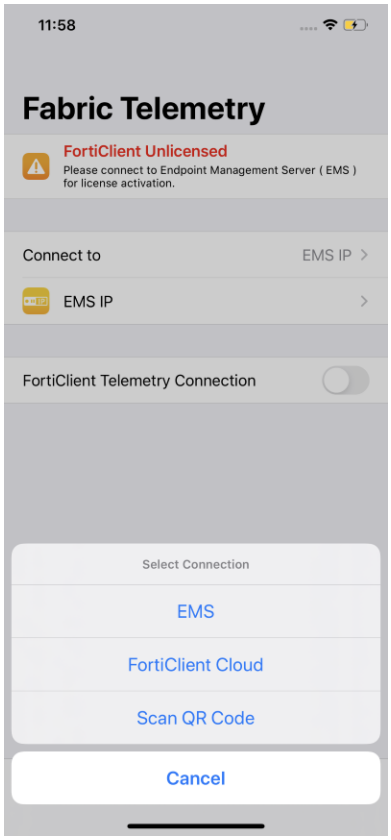


4. Click *Connect*. Ensure that the *Status* displays as *Connected*. FortiClient software is now licensed and activated.

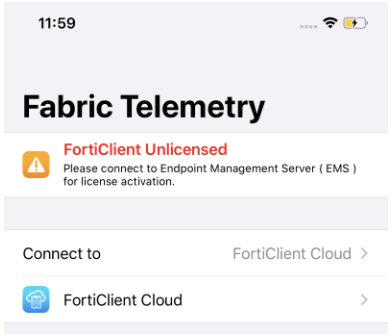


To register iOS or Android endpoints to FortiEndpoint:

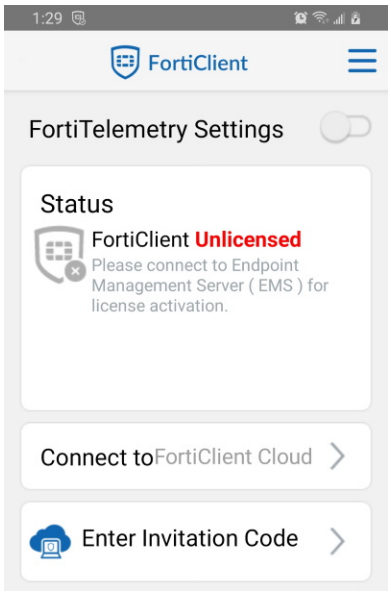
1. Tap *Connect to*, then select *FortiEndpoint*.



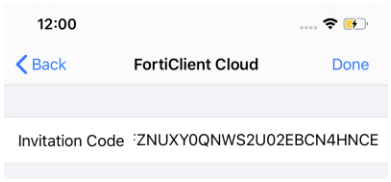
2. Do one of the following:
   a. For iOS, tap *FortiEndpoint*.



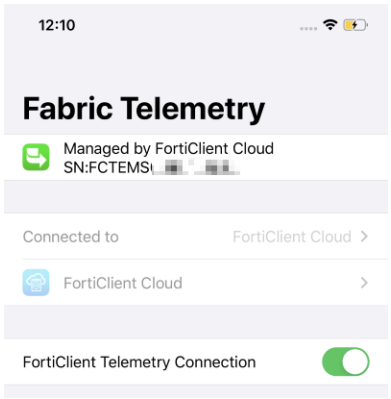
b. For Android, tap *Enter Invitation Code*.



3. Enter the invitation code.



FortiEndpoint is now managing FortiEndpoint.



Adding a new invitation for a deployment package

To add a new invitation for a deployment package:

1. Go to *Invitations* in the upper right corner or in *Endpoints* > *Invitations*.
2. Select an existing invitation code for the desired deployment package.
3. Click *Add*.

4. Configure the invitation:
   a. To send the code to a single recipient, select *Individual*. Otherwise, select *Bulk*.

   Sending individual invitation codes is considered best practice, as it can limit unexpected endpoints from connecting to FortiEndpoint.

   b. If desired, select *Send Email Notifications*.
   c. In the *Email Recipients* field, enter the desired end users' email addresses.
   d. If desired, enable *Send SMS Notifications*.
   e. In the *SMS Recipients* field, enter the desired end users' phone numbers.
   f. If desired, enable Expiring.
   g. In the *Expiry Date* field, set the expiry date.
   h. For *Verification Type*, select one of the following:

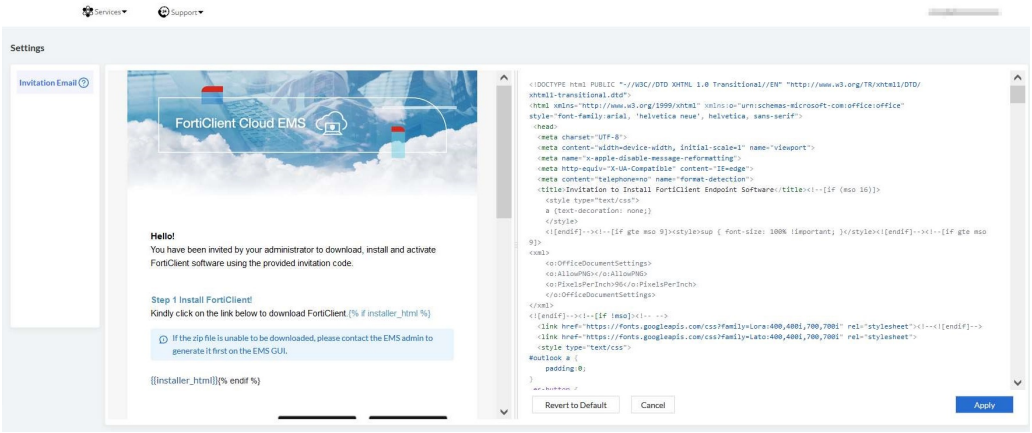
Verification type	Description
None	End user does not need to provide any credentials to connect to FortiEndpoint.
Local	End user must provide credentials that match a local user configured in *User Management > Local Users* to connect to EMS. You must create a local user to configure this option.
LDAP	End user must provide their domain credentials to connect to FortiEndpoint. You must configure an LDAP domain to configure this option.
SAML	End user must provide their credentials for an SAML identity provider, such as Azure Active Directory, to connect to EMS. You must configure SAML settings to configure this option.

5. Click *Save*. You see a new invitation code for the deployment package.

Customizing invitation code email content

To customize invitation code email content:

1. Log in to FortiEndpoint using your primary account credentials.
2. Go to *Settings*.
3. Edit and preview email content. You can edit email content on the right pane and preview your changes on the left pane. Click *Apply* to save your changes or click *Revert to Default* to get revert content to the default email template. Ensure that your email content contains {{invitation_code}} since it is used to render the invitation code in the email.



If you log in as a non-primary user, such as a subuser or Identity & Access Management user, you have read-only permissions and cannot edit the email content.

Managing Chromebooks with FortiEndpoint

You can use FortiEndpoint to manage Chromebooks. After you deploy and configure FortiEndpoint, the Google Admin console, and the FortiEndpoint Web Filter extension, the products work together to provide web filtering security for Google Chromebook users logged into the Google domain.

For a new deployment, ensure that you select FortiClient 7.2.1 or later. This section only provides instructions for 7.2.1 or a later version.

To configure FortiEndpoint for Chromebook management:

You can configure FortiEndpoint for Chromebook management by following the instructions in Installation and setup for managing Chromebooks. While these topics are for on-premise EMS, they also apply to FortiEndpoint, except for one difference. In step 2 of Configuring the FortiClient Web Filter extension, instead of `ProfileServerUrl`, the text file must contain the following text:

```
{
"InvitationCode": { "Value": "<FortiEndpoint invitation code>"}
}
```

The following provides an example:

```
{
"InvitationCode": { "Value": "6LY209RIP8NE6J1JR0FIF97LEVJVBKT2"}
}
```

You do not need to create an SSL certificate as a public certificate is used.

Managing endpoints using FortiEndpoint EMS

FortiEndpoint EMS is a security management tool that enables scalable and centralized management of multiple endpoints (computers). FortiEndpoint EMS provides efficient and effective administration of endpoints running FortiClient and EDR agents. It provides visibility across the network to securely share information and assign security policies to endpoints. It is designed to maximize operational efficiency and includes automated capabilities for device management and troubleshooting. FortiEndpoint EMS also works with the FortiClient Web Filter extension to provide web filtering for Google Chromebook users.

Use the FortiEndpoint EMS console for the following tasks:

- Remotely deploying FortiClient and EDR agents to Windows PCs
- Updating profiles for endpoint users regardless of access location
- Administering FortiClient and EDR endpoint connections, such as accepting, disconnecting, and blocking connections
- Managing and monitoring endpoints, such as status, system, and signature information
- Identifying outdated FortiClient and EDR agent versions
- Defining web filtering rules in a profile and remotely deploying the profile to the FortiClient Web Filter extension on Google Chromebook endpoints

You can manage endpoint security for Windows and macOS platforms using a unified organizational security policy. An organizational security policy provides a full understandable view of the security policies defined in the organization. You can see all policy rules, assignments, and exceptions in a single unified view. FortiEndpoint EMS is part of the Fortinet Endpoint Security Management suite, which ensures comprehensive policy administration and enforcement for an enterprise network.

GUI

The FortiEndpoint GUI consists of the following areas:

Banner

Option		Description
Activate License to Enable Features		Displays if you have not applied a license to FortiEndpoint. Click the link to access *Configure License*, where you can apply a license by logging in to your FortiCloud account or uploading a license file.
SSL Certificate is not secure		Displays if a secure SSL certificate has not been imported to FortiEndpoint. Click the link to go to the *EMS Settings* page, where you can import a license. See Configuring EMS settings on page 533.
Download icon		Displays if a new version of FortiEndpoint is available on FDS.
Invitations		You can configure invitation codes that endpoints users can use to connect to EMS. See Invitations on page 503.
Help icon		
	Getting Started	Provides access to links to the FortiEndpoint *Release Notes* and other resources.
	Technical Documentation	Link to the FortiEndpoint documentation.
	How-To Videos	Link to the Fortinet Video Library.
	Forums	Link to Fortinet Customer Service and Support forum.
	Product Videos	Links to the following FortiEndpoint videos: • Introduction to FortiEndpoint: introductory video for FortiEndpoint, which gives an overview of features, modes, and system requirements for FortiEndpoint 1.0. • How to License FortiEndpoint: shows how to license or renew FortiEndpoint 1.0 with more endpoints. • Adding a Domain to FortiEndpoint: shows how to add an AD domain to FortiEndpoint
	Create Support Package	Create a support package to provide to the Fortinet technical support team for troubleshooting.
	FortiGuard	View list of engine and signature versions for this version of FortiEndpoint.

Option	Description
Bell icon	Click the bell icon to display all alert logs.
<Logged in username>	Click the dropdown list beside the <logged in username> to do one of the following: • Change the password for this user. Enter a new password that complies with the displayed rules. • Log out of FortiEndpoint. • Go to *System > Legal Third Party* for a list of open source libraries used in EMS and a copy of their respective licenses. Click on any license source will direct you to the corresponding URL.

Left pane

The left navigation pane displays content in the right pane.

Option		Description
Dashboard		
	Status	Displays a dashboard of information about all managed endpoints.
	Vulnerability Scan	Displays the Current Vulnerabilities Summary chart that provides a centralized vulnerability summary for all managed endpoints. You can observe high-risk hosts and critical vulnerabilities existing on endpoints. You can also access links on how to fix or repair the vulnerabilities.
	Performance	Monitor EMS system resource utilization, such as CPU usage, network bandwidth usage, and disk usage.
	Chromebook Status	Displays a dashboard of information about all managed Chromebooks. Only available if the *EMS for Chromebooks Settings* option is enabled in *System Settings > EMS Settings*.
Endpoints		
	All Endpoints	Manage all endpoints.
	Manage Domains	Add and manage AD domains.
	Domains	Manage endpoints from AD domains. You can also add an AD domain if none exist.
	Workgroups	Manage endpoints from workgroups.
	Group Assignment Rules	Configure rules to automatically place endpoints into custom groups based on their installer ID, IP address, or OS.
Google Domains		Only available if the *EMS for Chromebooks Settings* option is enabled in *System Settings > EMS Settings*.

Option		Description
	All Users	Manage users from all Google domains.
	Manage Domains	Add and manage Google domains.
	Domains	Manage users from specific Google domains. You can also add a Google domain if none exist.
Deployment & Installers		
	Manage Deployment	Create deployment configurations to deploy FortiClient to endpoints.
	FortiClient Installers	Add and manage FortiClient deployment packages.
Endpoint Policy & Components		
	Manage Policies	Create endpoint policies and manage policy updates for Windows, macOS, and Linux endpoints.
	CA Certificates	Upload and import CA certificates into FortiEndpoint.
	On-fabric Detection Rules	Configure on-fabric detection rules for endpoints.
Chromebook Policy		Create endpoint policies and manage policy updates for Chromebook endpoints. Only available if the *EMS for Chromebooks Settings* option is enabled in *System Settings > EMS Settings*.
Endpoint Profiles		
	Manage Profiles	Create profiles and manage profile updates for all profiles.
	Import from FortiGate/FortiManager	Import Web Filter profiles from FortiOS or FortiManager.
Security Posture Tags		
	Security Posture Tagging Rules	Define security posture tagging rules.
	Security Posture Tag Monitor	View tagged endpoints.
Software Inventory		
	Applications	View applications installed on endpoints. Display applications by application or application vendor name.
	Hosts	View applications installed on endpoints, sorted by endpoint.
Quarantine Management		
	Files	View and allowlist files on endpoints that Sandbox or AV has quarantined.
	Allowlist	View and delete allowlisted files from the *Allowlist* pane.

Option		Description
Administration		
	Administrators	Add and manage FortiEndpoint administrators.
	Admin Roles	Add and manage FortiEndpoint admin roles and permissions.
	User Settings	Configure the inactivity timeout and other user settings.
	Fabric Devices	View Fabric devices connected to EMS.
	SAML SSO	Configure SAML SSO authentication.
	Configure License	Upgrade or renew the FortiEndpoint license.
	Log Viewer	View log messages generated by FortiEndpoint and download raw logs.
System Settings		
	EMS Settings	Change the IP address and port and configure other EMS settings for FortiEndpoint, including enabling Chromebook management.
	Log Settings	Specify what level of log messages to capture in FortiEndpoint logs and when to automatically delete logs and alerts.
	FortiGuard Services	Configure the FortiGuard server location. Configure FortiManager to use for client software/signature updates and configure FortiCloud settings.
	EMS Alerts	Enable alerts for FortiEndpoint events.
	Endpoint Alerts	Enable alerts for endpoint events.
	SMTP Server	Set up an SMTP server to enable email alerts.
	Custom Messages	Customize the message that displays on an endpoint when it has been quarantined by FortiEndpoint
	Feature Select	Choose which features to show and hide in EMS.

Content pane

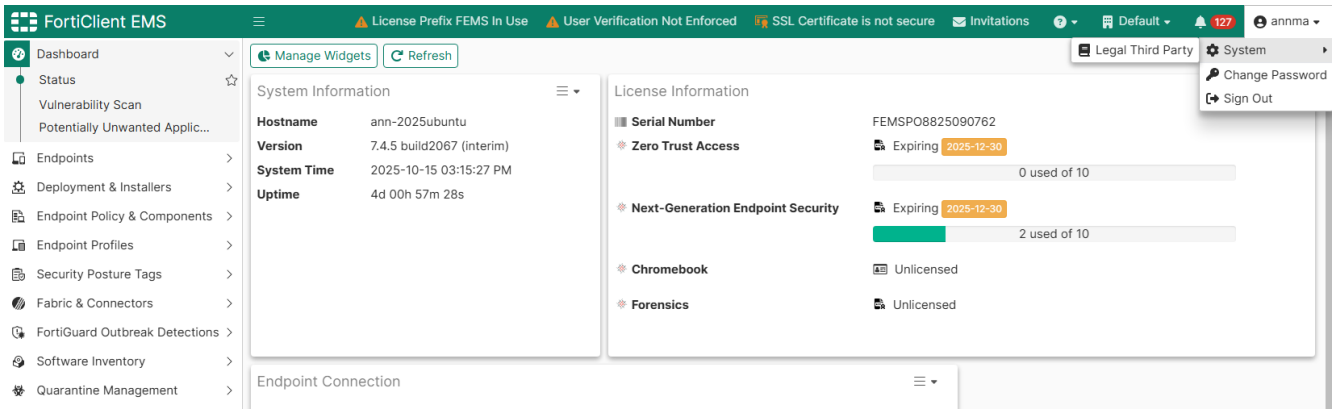
The right pane displays the user interface controls that correspond to the selection made in the left pane. The status and menu icons in the top-right display controls what you can use to configure additional settings for user management and each individual endpoint.

Open Source Licensing Requirements

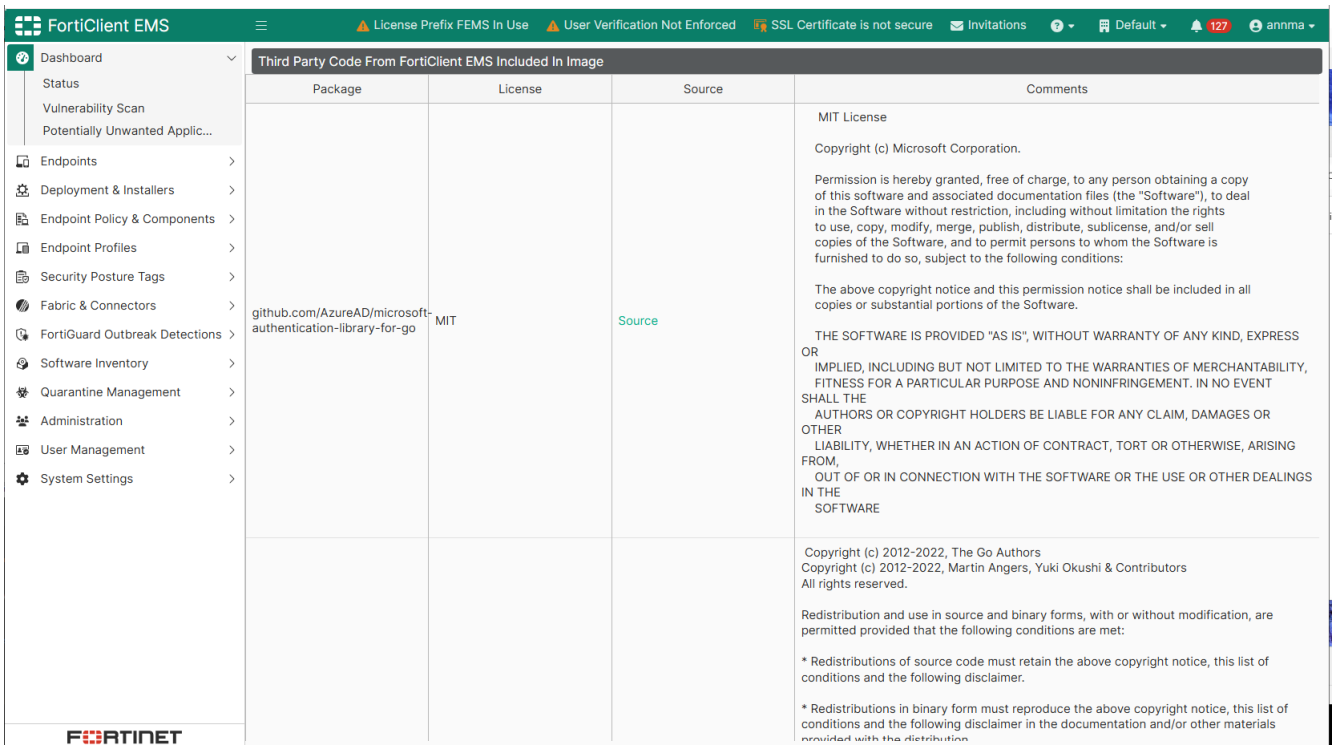
The *Legal Third Party* page includes a list of open source libraries used in EMS and a copy of their respective licenses. For example:

- Rijndael (AES) Decryption License
- MIT License
- BSD
- GPL v2

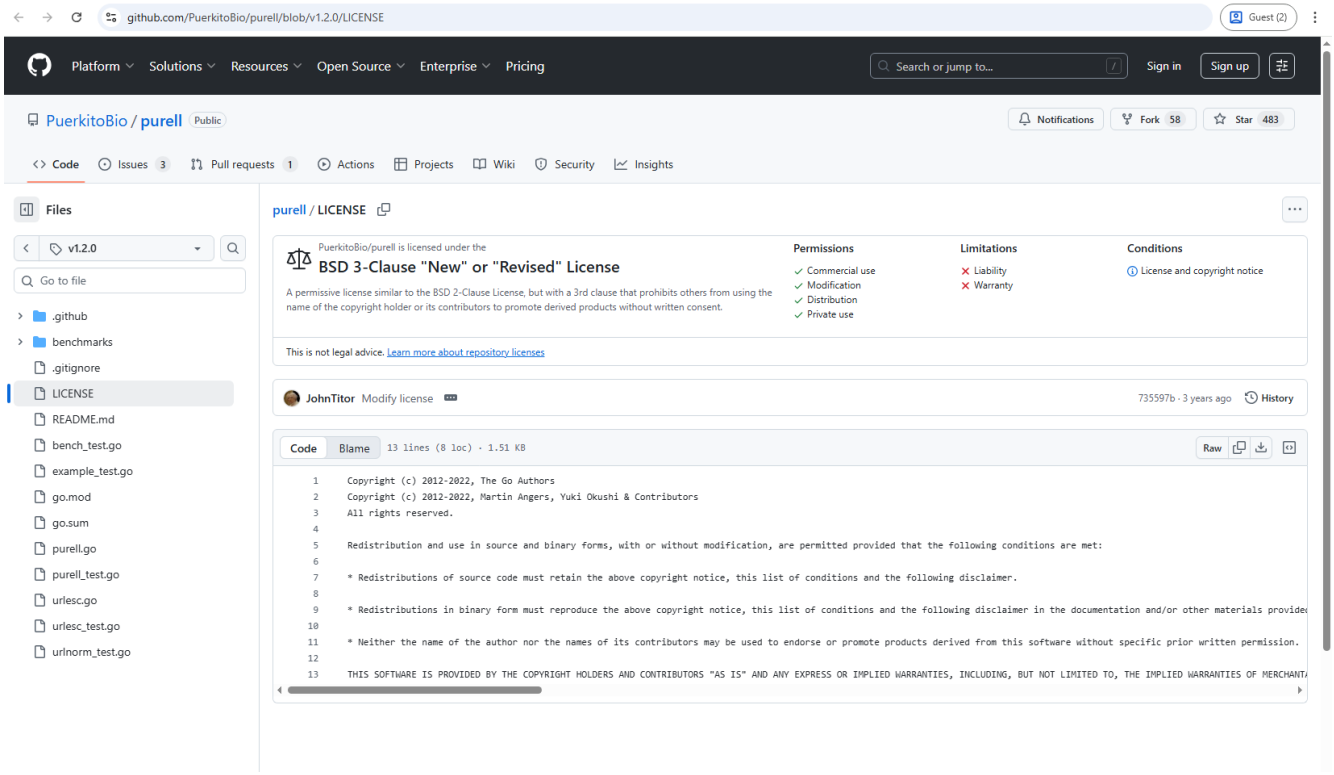
In FortiEndpoint EMS, click the admin username and select *System > Legal Third Party*.



A page opens with the list of open source libraries used in EMS and a copy of their respective licenses.



Click on any license source will direct you to the corresponding URL. For example, BSD-3-Clause:


github.com/PuerkitoBio/purell/blob/v1.2.0/LICENSE
Guest (2)
Platform
Solutions
Resources
Open Source
Enterprise
Pricing
Search or jump to...
Sign in
Sign up
PuerkitoBio / purell
Public
Notifications
Fork 58
Star 483
Code
Issues 3
Pull requests 1
Actions
Projects
Wiki
Security
Insights
Files
v1.2.0
Go to file
.github
benchmarks
.gitignore
LICENSE
README.md
bench_test.go
example_test.go
go.mod
go.sum
purell.go
purell_test.go
urlesc.go
urlesc_test.go
urlnorm_test.go
purell / LICENSE
PuerkitoBio/purell is licensed under the
BSD 3-Clause "New" or "Revised" License
A permissive license similar to the BSD 2-Clause License, but with a 3rd clause that prohibits others from using the name of the copyright holder or its contributors to promote derived products without written consent.
Permissions
Commercial use
Modification
Distribution
Private use
Limitations
Liability
Warranty
Conditions
License and copyright notice
This is not legal advice. Learn more about repository licenses
JohnTitor Modify license
735597b · 3 years ago
History
Code
Blame
13 lines (8 loc) · 1.51 KB
Raw
Copyright (c) 2012-2022, The Go Authors
Copyright (c) 2012-2022, Martin Angers, Yuki Okushi & Contributors
All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provide
* Neither the name of the author nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANT

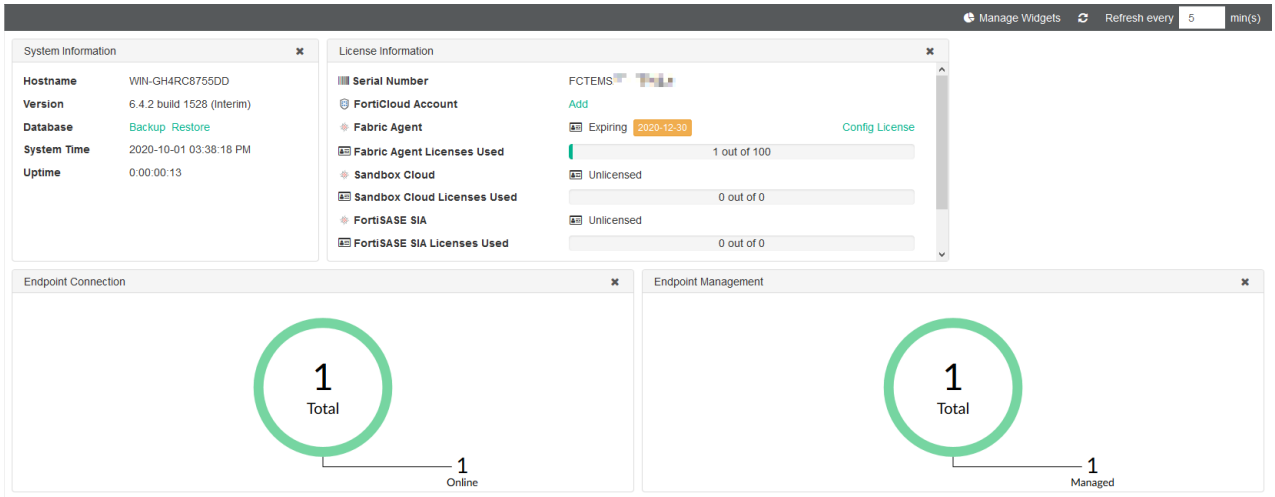
Dashboard

You can use the Dashboard to view summary information about the system and endpoints. You can view summary information about vulnerability scans on endpoints.

Viewing the Status

To view the Status:

1. In the left pane, click *Dashboard* > *Status*.
   A *System Information* widget and charts and widgets of summary information display. See System Information widget on page 34 and Status charts and widgets on page 37.



2. For most *Status* widgets, clicking a donut chart section leads to the *Endpoints* pane. The *Endpoints* pane displays with more details about the endpoints that belong to the selected donut chart section. See Viewing the Endpoints pane on page 57.
3. Click a section of the *Endpoint Alerts* widget. The *Endpoint Event Summary* displays with more details about the endpoints that belong to that chart section. The endpoint details that display on this page depend on the endpoint alert type. In the example, the selected alert was that the AV signature on the endpoint is out-of-date. Therefore, *Endpoint Event Summary* displays the current installed AV signature version and the latest available AV signature version that you can upgrade the endpoint to.



System Information widget

The following information displays in the *System Information* widget.

Field	Description
Hostname	Name of the computer where you installed FortiEndpoint.
Version	Version number for FortiEndpoint. Also displays the build number. If the build is an interim build, also displays *(Interim)* beside the build number.
Database	Options to back up and restore the database (DB). See To back up the DB: on page 35 and To restore the DB: on page 35.
System Time	Time and date that the computer where you installed FortiEndpoint uses.
Uptime	Number of days, hours, minutes, and seconds FortiEndpoint has been running.
Mode	Displays if the EMS is a standalone node or part of a high availability (HA) cluster.

To back up the DB:

1. Go to *Dashboard* > *Status*.
2. In the *System Information* widget, beside *Database*, click *Backup*.
3. Set the following options:

Option	Description
Password	Enter a password for backing up and restoring the DB.
Confirm Password	Reenter the password to confirm it.
Compression Type	Select one of the following: • *Database*: download the backup as a db.enc file • *Zip*: download the backup as a zip archive

4. Click *Back Up*. FortiEndpoint backs up the DB.

To restore the DB:

1. Go to *Dashboard* > *Status*.
2. In the *System Information* widget, beside *Database*, click *Restore*.
3. Click *Upload File*.
4. Locate and select the DB backup file.
   You can restore the DB across different deployment models, such as from a standalone EMS to an EMS HA setup or vice versa.
5. In the *Password* field, enter the password used to back up the database.
6. Click *Restore*. When the DB is restored, a message appears. The message instructs you to wait for the restored DB to reload.
7. Wait for the restored DB to be reloaded.

License Information widget

The following information displays in the *License Information* widget:

Option	Description
Serial Number	Serial number for FortiEndpoint.
FortiCloud Account	FortiCloud account that this EMS server is registered to. If EMS is not registered to a FortiCloud account, you can log into an existing FortiCloud account or create a new FortiCloud account from this widget.
Zero Trust Access	Zero Trust Network Access (ZTNA) device-based license status. You can use this license for managing Windows, macOS, Linux, iOS, Android, and Chromebook endpoints. When licensed, displays number of licenses used out of the total number of available licenses and the expiry date.
Next-Generation Endpoint Security	Endpoint Protection Platform (EPP) device-based license status. You can use this license for managing Windows, macOS, Linux, iOS, Android, and Chromebook endpoints. This license all features included in the ZTNA license as well as more advanced features. When licensed, displays number of licenses used out of the total number of available licenses and the expiry date.
FortiSASE	FortiSASE device-based license status. When licensed, displays number of licenses used out of the total number of available licenses and the expiry date.
Zero Trust Access User	ZTNA user-based license status. When licensed, displays number of licenses used out of the total number of available licenses and the expiry date.
Next-Generation Endpoint Security User	EPP user-based license status. This license all features included in the ZTNA license as well as more advanced features. When licensed, displays number of licenses used out of the total number of available licenses and the expiry date.
FortiSASE User	FortiSASE user-based license status. When licensed, displays number of licenses used out of the total number of available licenses and the expiry date.
Chromebook	Status of the Chromebook license for FortiEndpoint. You can use this license for managing Chromebook endpoints. When licensed, displays number of licenses used out of the total number of available licenses and the expiry date.
Remote Access	VPN-only license status. When licensed, displays number of licenses used out of the total number of available licenses and the expiry date.

If you have just installed EMS, click *Add* beside *FortiCloud Account* to license by logging in to your FortiCloud account.

Status charts and widgets

Status displays a number of pie charts. Each pie chart provides a summary of endpoint information. The sections in each chart are links. You can click any section of the pie charts or any row in the table to display more details.



Available options may differ depending on the features you have enabled or disabled in *Feature Select*. See Feature Select on page 555. See Feature Select.

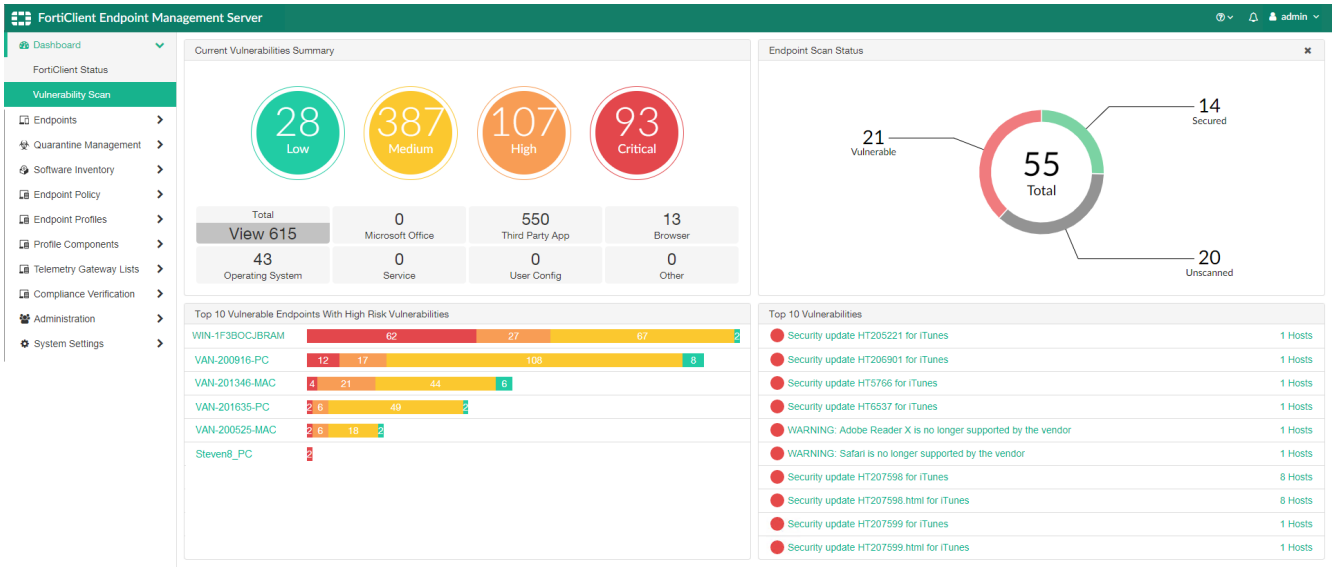
Option	Description
Endpoint Charts	
Endpoint Activity	Shows a summary of endpoint activity information. Categories are: • EMS On-fabric • EMS Off-fabric
Endpoint Alerts	Shows the number of endpoints with alerts, including pending software updates, out-of-date protection, and out-of-sync profiles.
Endpoint Connection	Shows the number of endpoints that are: • Online • Offline for less than one hour • Offline • Offline for 30 days or more
Managed Mac FortiClient Versions	This chart indicates the percentage of macOS endpoints with each version of FortiClient installed. Sorting by version lists FortiClient versions from most recent to least recent. For example, FortiClient 6.2.0 is listed first, then FortiClient 6.0.0, and so on. Sorting by count lists FortiClient versions from the version with the largest number of endpoints to the version with the smallest number of endpoints. For example, if there are 600 endpoints with FortiClient 6.0.0 installed and 40 endpoints with FortiClient 6.2.0 installed, FortiClient 6.0.0 is listed first.
Managed Windows FortiClient Versions	This chart indicates the percentage of Windows endpoints with each version of FortiClient installed. You can sort the data by version or count. Sorting by version lists FortiClient versions from most recent to least recent. For example, FortiClient 6.2.0 is listed first, then FortiClient 6.0.0, and so on. Sorting by count lists FortiClient versions from the version with the largest number of endpoints to the version with the smallest number of endpoints. For example, if there are 600 endpoints with FortiClient 6.0.0 installed and 40 endpoints with FortiClient 6.2.0 installed, FortiClient 6.0.0 is listed first.
Managed Linux FortiClient Versions	This chart indicates the percentage of Linux endpoints with each version of FortiClient installed. You can sort the data by version or count.

Option	Description
Endpoint Management	This chart indicates how many endpoints are disconnected and connected.
Mac Operating Systems	This chart indicates the number of endpoints running each version of the macOS operating system. You can sort the data by version or count. Sorting by version lists macOS versions from most recent to least recent. For example, macOS 10.13 High Sierra is listed first, then macOS 10.12 Sierra, OS X 10.11 El Capitan, and so on. Sorting by count lists FortiClient versions from the version with the largest number of endpoints to the version with the smallest number of endpoints. For example, if there are 600 endpoints with macOS 10.12 Sierra installed and 40 endpoints with macOS 10.13 High Sierra installed, macOS 10.12 Sierra is listed first.
Windows Operating Systems	This chart indicates the number of endpoints running each version of the Windows operating system. You can sort the data by version or count. Sorting by version lists Windows versions from most recent to least recent. For example, Windows 10 is listed first, then Windows 8, Windows 7, and so on. Sorting by count lists FortiClient versions from the version with the largest number of endpoints to the version with the smallest number of endpoints. For example, if there are 600 endpoints with Windows 7 installed and 40 endpoints with Windows 10 installed, Windows 7 is listed first.
Linux Operating Systems	This chart indicates the number of endpoints running each version of the Linux operating system. You can sort the data by version or count. Sorting by version lists Linux versions from most recent to least recent. For example, Ubuntu 18.10 is listed first, then Ubuntu 17.10, Ubuntu 16.04, and so on. Sorting by count lists FortiClient versions from the version with the largest number of endpoints to the version with the smallest number of endpoints. For example, if there are 600 endpoints with Ubuntu 16.04 installed and 40 endpoints with Ubuntu 18.10 installed, Ubuntu 16.04 is listed first.
iPhone Operating Systems	This chart indicates the number of endpoints running each version of the iOS operating system. You can sort the data by version or count. Sorting by version lists iOS versions from most recent to least recent. For example, iOS 15 is listed first, then iOS 14, iOS 13, and so on. Sorting by count lists FortiClient versions from the version with the largest number of endpoints to the version with the smallest number of endpoints. For example, if there are 600 endpoints with iOS 9 installed and 40 endpoints with iOS 10 installed, iOS 9 is listed first.
Android Operating Systems	This chart indicates the number of endpoints running each version of the Android operating system. You can sort the data by version or count. Sorting by version lists Android versions from most recent to least recent. For example, Android 12 is listed first, then Android 11, Android 10, and so on. Sorting by count lists FortiClient versions from the version with the largest number of endpoints to the version with the smallest number of endpoints. For example, if there are 600 endpoints with Android 10 installed and 40 endpoints with Android 11 installed, Android 10 is listed first.

Option	Description
FortiGuard Outbreak Alerts Service	This chart displays endpoints that are considered suspicious or compromised according to the outbreak alert rules that FortiEndpoint has received from FortiGuard. The chart displays the number of endpoints that are vulnerable to each outbreak. See FortiGuard Outbreak Alerts on page 448. You can drill down by clicking the outbreak bar. From here, you can quarantine the endpoint if desired.
Top 3 Lists	
Antivirus Detection	This chart indicates the top three endpoints with AV alerts, including the number of AV alerts for each endpoint.
Sandbox Detection	This chart indicates the top three endpoints with FortiSandbox alerts, including the number of FortiSandbox alerts for each endpoint.
Vulnerability Detection	This chart indicates the top three endpoints with vulnerability alerts, including the number of vulnerabilities detected for each endpoint.
Web Filter Detection	This chart indicates the top three endpoints with web filter alerts, including the number of web filter alerts for each endpoint.

Viewing the Vulnerability Scan dashboard

Go to *Dashboard* > *Vulnerability Scan*. Here you can view a variety of charts and widgets containing a summary of vulnerability scan information from endpoints.



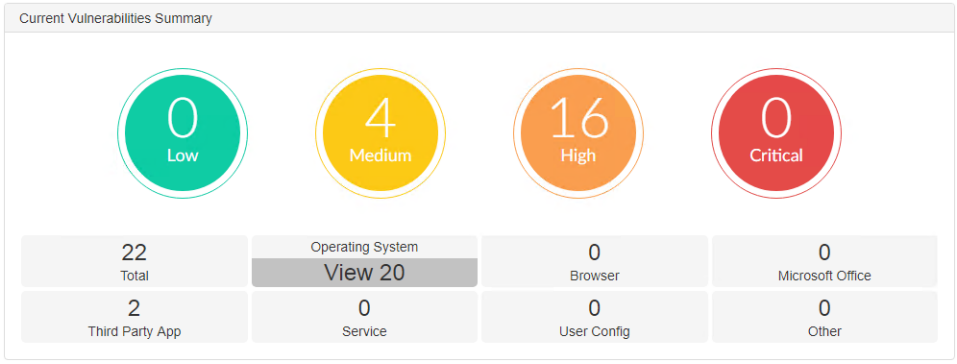
The *Vulnerability Scan* dashboard displays a number of charts. Each chart provides a summary of endpoint information. The sections in each chart are links. You can click sections of the charts or any row in the table to display more details.

Chart	Description
Current Vulnerabilities Summary	Displays the following summaries of current vulnerabilities: • Total (total number of vulnerabilities) • Operating System (number of operating system vulnerabilities) • Browser (number of browser vulnerabilities) • Microsoft Office (number of Microsoft Office vulnerabilities) • Third Party App (number of third-party application vulnerabilities) • Service (number of service vulnerabilities) • User Config (number of user configuration vulnerabilities) • Other (number of other vulnerabilities that do not fit any of the above categories) When you click a vulnerability tile, the colored circles update to display the number of vulnerabilities that correspond to each severity level in the selected category.
Endpoint Scan Status	Displays the following summaries about endpoints: • Vulnerable Endpoints • Un-Scanned Endpoints • Secured Endpoints • Scanning Endpoints
Top 10 Vulnerable Endpoints With High Risk Vulnerabilities	Displays the top ten vulnerable endpoints and the number of vulnerabilities detected on those endpoints, with associated severity levels.
Top 10 Vulnerabilities	Displays the top ten vulnerabilities and the number of hosts where the vulnerabilities have been detected. Click the vulnerability name to see information about the vulnerability on FortiGuard.

Viewing current vulnerabilities

To view current vulnerabilities:

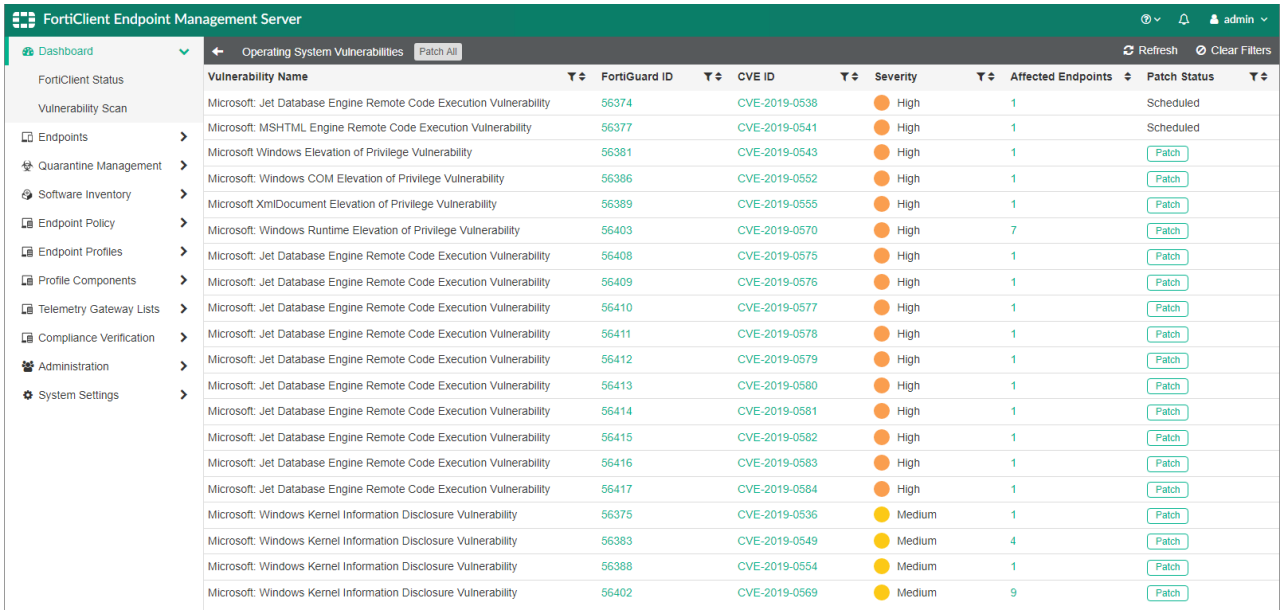
1. Go to *Dashboard > Vulnerability Scan*.
2. Under *Current Vulnerabilities Summary*, click a vulnerability tile.
3. When you click a vulnerability tile, the colored circles update to display the number of vulnerabilities that correspond to each severity level in the selected category.
   In this example, there are 22 total vulnerabilities, 20 of which are OS vulnerabilities. Click the *Operating System* tile.



The OS vulnerabilities are organized by severity:

- 0/20 are low risk (green circle)
- 4/20 are medium risk (yellow circle)
- 16/20 are high risk (orange circle)
- 0/20 are critical risk (red circle)

4. You can click any tile to display details for vulnerabilities of that type. In this example, click *View 20* on the *Operating System* tile to display all OS vulnerabilities and details:



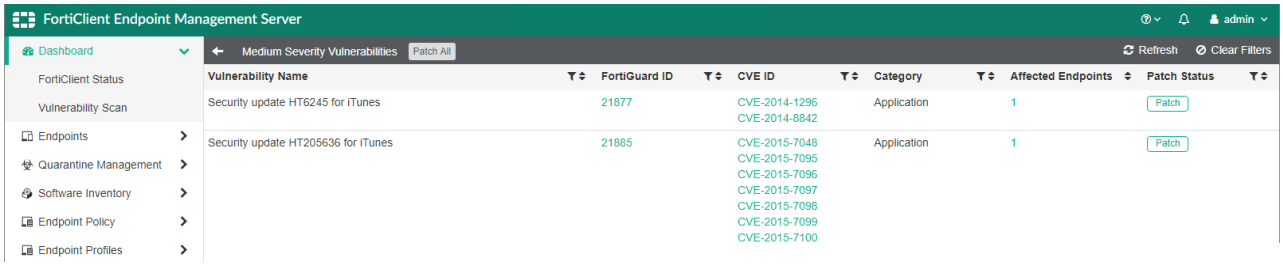
Patch All	Click this button to patch all vulnerabilities currently displayed on the content pane. The vulnerabilities are patched with the next Telemetry communication between FortiEndpoint and the endpoint.
Refresh	Click to refresh the list of vulnerabilities in the content pane.
Clear Filters	Click to clear all filters applied to the list of vulnerabilities.
Vulnerability Name	Name of the vulnerability.
FortiGuard ID	Displays the FortiGuard ID. Click the link to see information about the vulnerability on FortiGuard.

CVE ID	Displays the vulnerability ID as determined by the Common Vulnerabilities and Exposures (CVE) system. If available, you can click the link to see more information about the vulnerability. Depending on the vulnerability, there may be multiple CVE IDs listed.
Severity	Displays the severity of the vulnerability.
Affected Endpoints	Displays the number of endpoints that are affected by this vulnerability.
Patch Status	You can click the *Patch* button to patch the selected vulnerability with the next Telemetry communication between FortiEndpoint and the endpoint. If a patch is already scheduled for the vulnerability, this column displays *Scheduled*. If the vulnerability must be patched manually, this column displays *Manual Patch*. FortiClient may be unable to automatically patch the vulnerability due to one of the following reasons: • **Third-party application vulnerabilities**: incorrect or missing installation paths • **OS vulnerabilities**: Windows update service is disabled In these cases, EMS may incorrectly display the status of these vulnerabilities that were selected to be automatically patched as *Scheduled* instead of *Failed*.

You can filter the list of vulnerabilities by any column by clicking the filter icon beside the desired heading. Enter the value to include in the filter. You can toggle the *All/Any/Not* button for the following options:

- *All:* Display all files that match the set filter.
- *Any:* Display any file that matches the set filter.
- *Not:* Display only files that do not match the set filter.

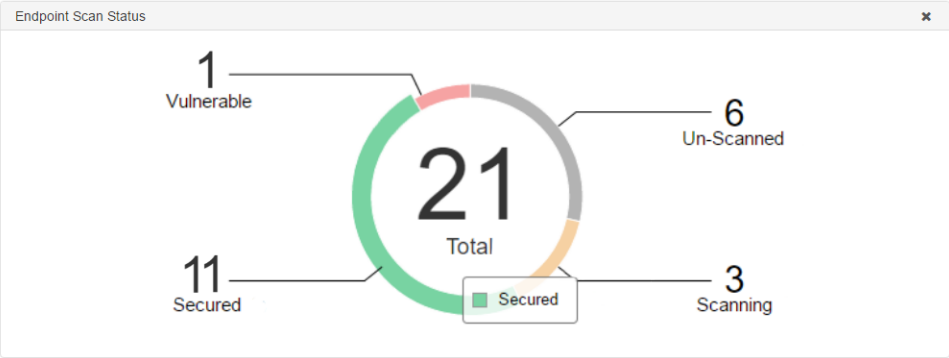
5. Return to *Dashboard > Vulnerability Scan*. You can also click a colored circle to view all vulnerabilities of the selected severity level. The following shows all medium severity third party application vulnerabilities:



Viewing the Endpoint Scan Status

To view the Endpoint Scan Status:

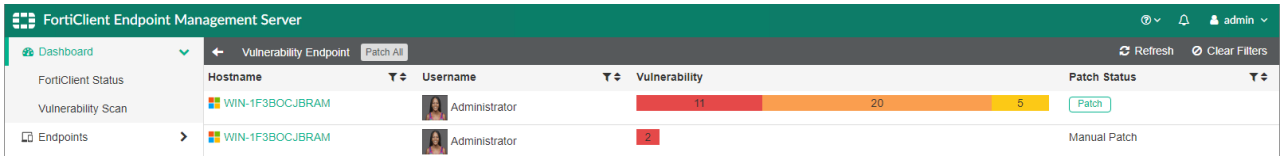
1. Go to *Dashboard* > *Vulnerability Scan*.



On the Endpoint Scan Status chart, endpoints are organized by type:

- 11/21 are *Secured* (green section)
- 1/21 is *Vulnerable* (red section)
- 6/21 are *Un-Scanned* (yellow section)
- 3/21 are *Scanning* (grey section)

2. Click the *Vulnerable* section to view all vulnerabilities detected on vulnerable endpoints:



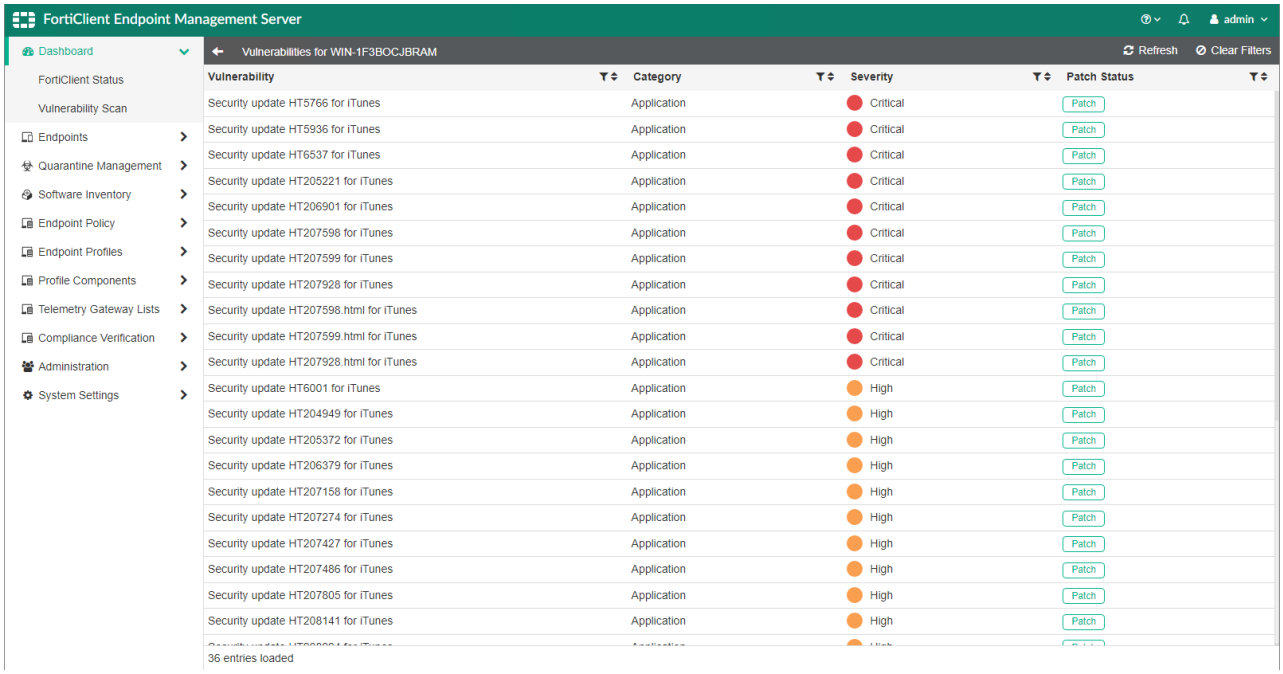
Patch All	Click this button to patch all vulnerabilities currently displayed on the content pane. The vulnerabilities are patched with the next Telemetry communication between FortiEndpoint and the endpoint.
Refresh	Click to refresh the list of vulnerabilities in the content pane.
Clear Filters	Click to clear all filters applied to the list of vulnerabilities.
Hostname	Hostname of the endpoint where the vulnerability was detected.
Username	User that is currently logged into the endpoint where the vulnerability was detected.
Vulnerability	Displays the number of vulnerabilities detected on the endpoint at each severity level. In this example, the endpoint has 11 critical vulnerabilities, 20 high risk vulnerabilities, and 5 medium risk vulnerabilities that can be patched using FortiClient. The same endpoint also has 2 critical vulnerabilities that must be manually patched.

Patch Status	You can click the *Patch* button to patch the selected vulnerability with the next Telemetry communication between FortiEndpoint and the endpoint. If a patch is already scheduled for the vulnerability, this column displays *Scheduled*. If the vulnerability must be patched manually, this column displays *Manual Patch*. FortiClient may be unable to automatically patch the vulnerability due to one of the following reasons: • **Third-party application vulnerabilities**: incorrect or missing installation paths • **OS vulnerabilities**: Windows update service is disabled In these cases, EMS may incorrectly display the status of these vulnerabilities that were selected to be automatically patched as *Scheduled* instead of *Failed*.

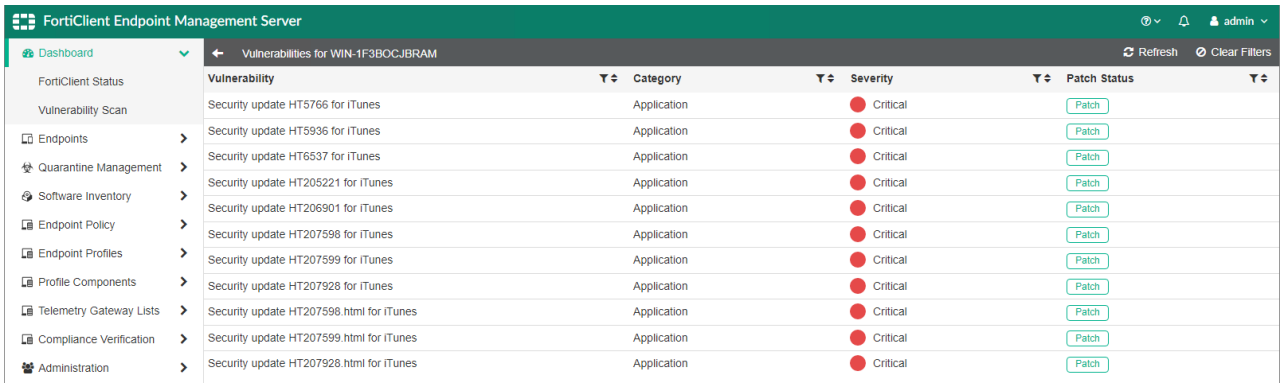
You can filter the list of vulnerable endpoints by any column by clicking the filter icon beside the desired heading. Enter the value to include in the filter. You can toggle the *All/Any/Not* button for the following options:

- *All:* Display all files that match the set filter.
- *Any:* Display any file that matches the set filter.
- *Not:* Display only files that do not match the set filter.

3. Click a hostname. You can view all vulnerabilities detected on that endpoint. You can filter the list of vulnerabilities in the same way that you can filter the list of vulnerable endpoints in step 2.



4. Go back, then click one of the sections under the *Vulnerability* column to view all vulnerabilities detected on the selected endpoint at the selected severity. The example displays all critical vulnerabilities for the selected endpoint. You can filter the list of vulnerabilities in the same way that you can filter the list of vulnerable endpoints in step 2.

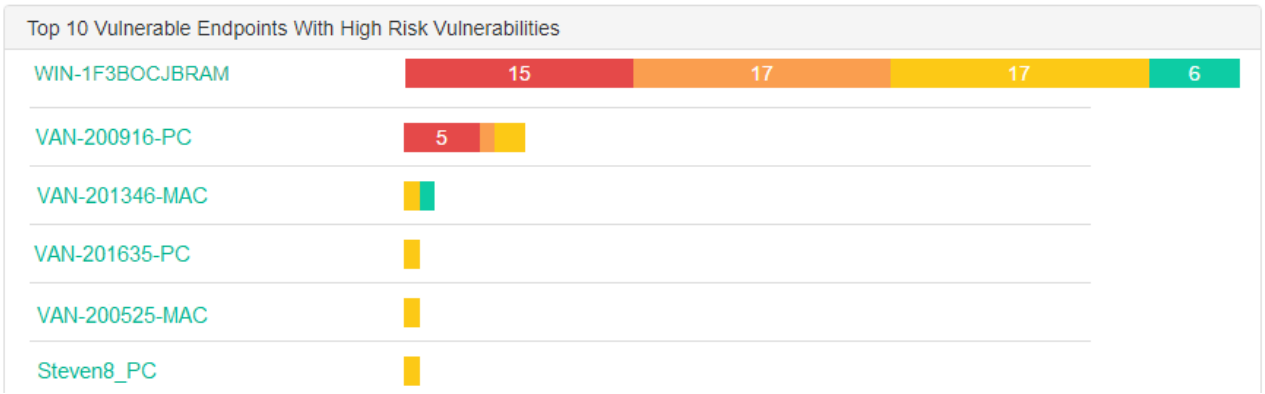


Vulnerability	Name of the vulnerability.
Category	Category of the vulnerability.
Severity	Severity level of the vulnerability.
Patch Status	You can click the *Patch* button to patch the selected vulnerability with the next Telemetry communication between FortiEndpoint and the endpoint. If a patch is already scheduled for the vulnerability, this column displays *Scheduled*. If the vulnerability must be patched manually, this column displays *Manual Patch*.

Viewing the top 10 vulnerable endpoints with high risk vulnerabilities

To view the top 10 vulnerable endpoints with high risk vulnerabilities:

1. Go to *Dashboard* > *Vulnerability Scan*. The *Top 10 Vulnerable Endpoints With High Risk Vulnerabilities* chart displays vulnerabilities per endpoint in a segmented bar graph and organized by severity.

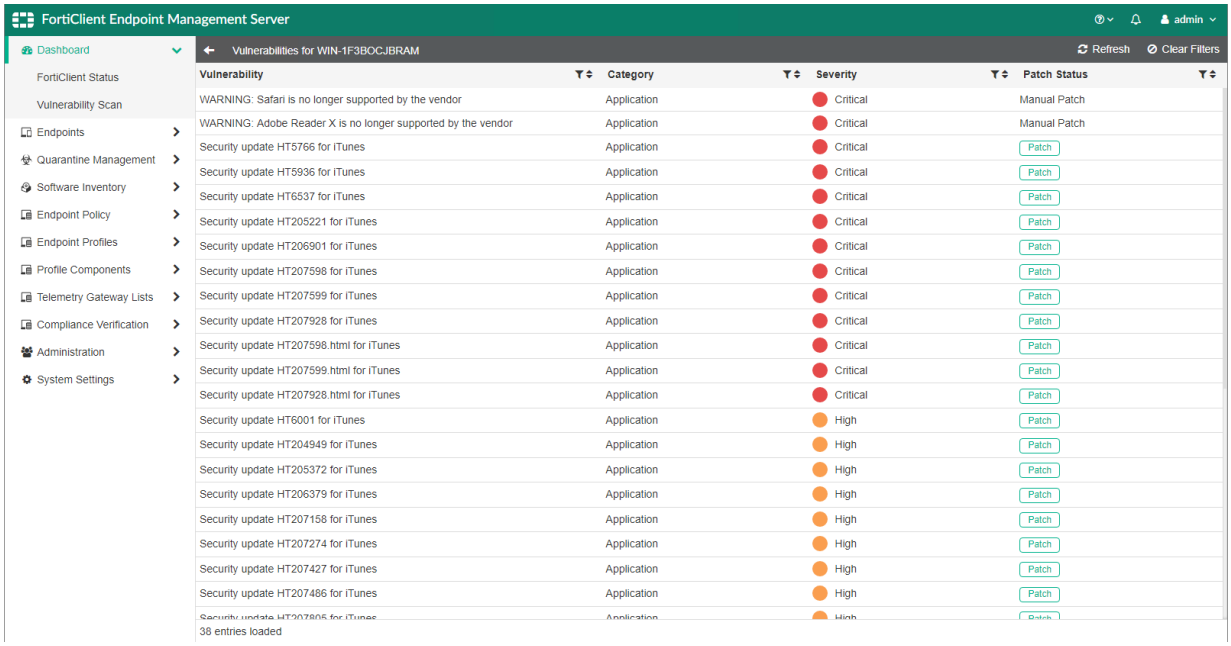


WIN-1F3BOCJBRAM has the following:

- 15 *Critical Vulnerabilities* (red bar)
- 17 *High Risk Vulnerabilities* (orange bar)

- 17 *Medium Risk Vulnerabilities* (yellow bar)
- 6 *Low Risk Vulnerabilities* (green bar)

2. Do one of the following:
   a. Click the endpoint hostname. You can view a list of all vulnerabilities detected on that endpoint.

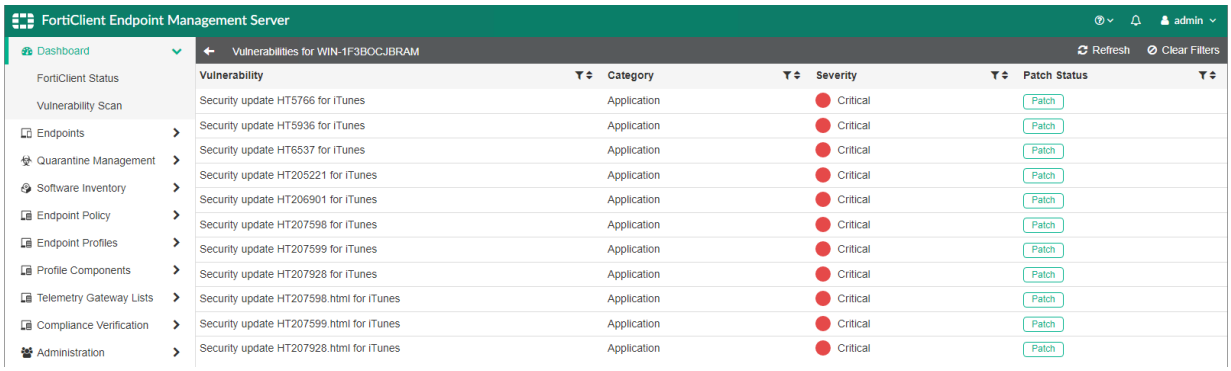


Vulnerability	Name of the vulnerability.
Category	Category of the vulnerability.
Severity	Severity level of the vulnerability.
Patch Status	You can click the *Patch* button to patch the selected vulnerability with the next Telemetry communication between FortiEndpoint and the endpoint. If a patch is already scheduled for the vulnerability, this column displays *Scheduled*. If the vulnerability must be patched manually, this column displays *Manual Patch*. FortiClient may be unable to automatically patch the vulnerability due to one of the following reasons: • **Third-party application vulnerabilities**: incorrect or missing installation paths • **OS vulnerabilities**: Windows update service is disabled In these cases, EMS may incorrectly display the status of these vulnerabilities that were selected to be automatically patched as *Scheduled* instead of *Failed*.

You can filter the list of vulnerable endpoints by any column by clicking the filter icon beside the desired heading. Enter the value to include in the filter. You can toggle the *All/Any/Not* button for the following options:

- *All:* Display all files that match the set filter.
- *Any:* Display any file that matches the set filter.
- *Not:* Display only files that do not match the set filter.

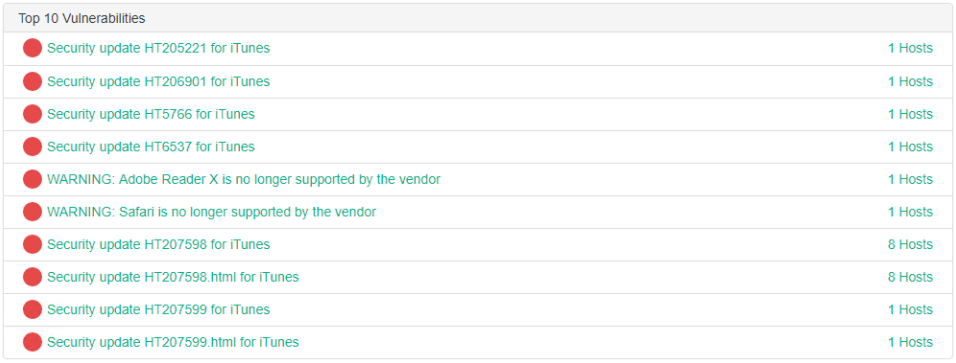
b. Click one of the sections of the vulnerability bar graph to view all vulnerabilities detected on the selected endpoint at the selected severity. The example displays all critical vulnerabilities for the selected endpoint. You can filter the list of vulnerabilities in the same way that you can filter the list of vulnerabilities in option a.



Viewing top ten vulnerabilities on endpoints

To view top ten vulnerabilities on endpoints:

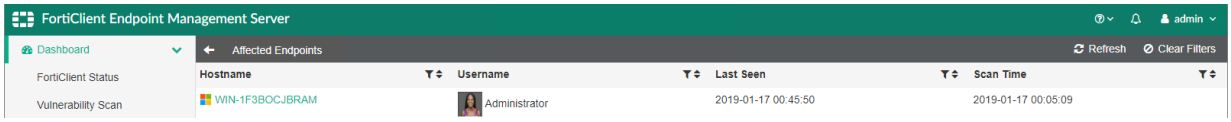
1. Go to *Dashboard* > *Vulnerability Scan*. The *Top 10 Vulnerabilities* widget displays the type of vulnerability and how many hosts the vulnerability has been detected on.



2. Do one of the following:
   a. Click the vulnerability name. You can view the vulnerability on FortiGuard.



   b. Click the number of hosts that are affected by a vulnerability. You can view a list of endpoints where the vulnerability has been detected.

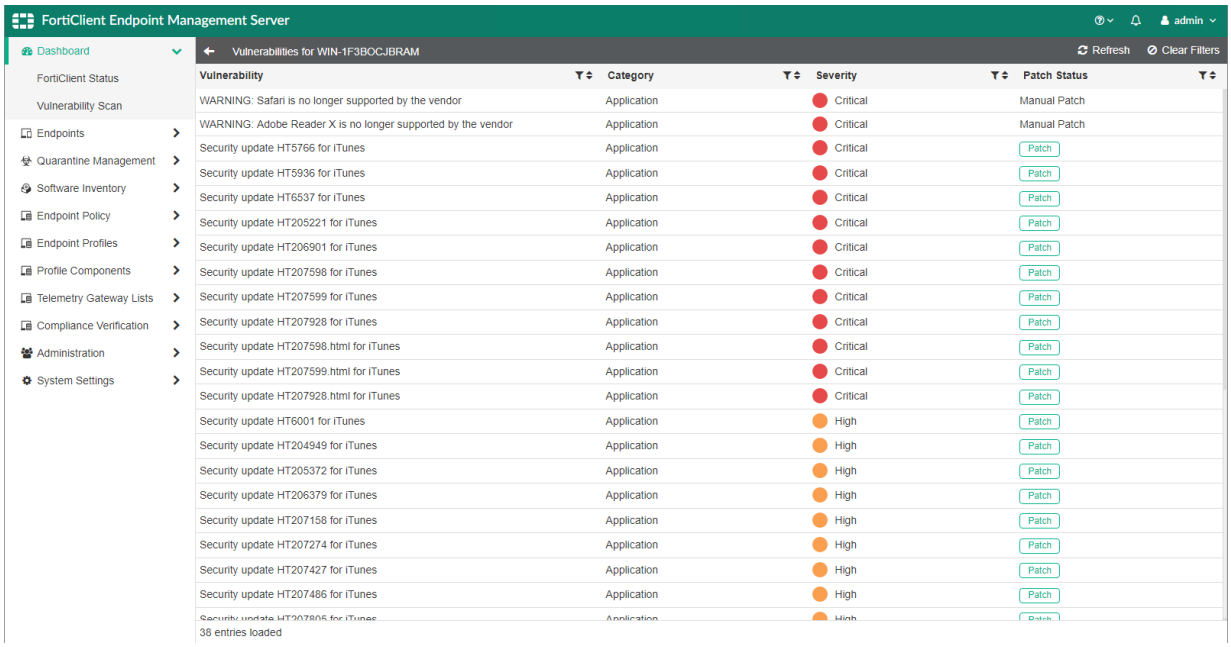


Refresh	Click to refresh the list of vulnerabilities in the content pane.
Clear Filters	Click to clear all filters applied to the list of vulnerabilities.
Hostname	Hostname of the endpoint where the vulnerability was detected.
Username	User that is currently logged into the endpoint where the vulnerability was detected.
Last Seen	Time of the last Telemetry communication between FortiEndpoint and the endpoint.
Scan Time	Time of the last Vulnerability Scan on the endpoint.

You can filter the list of vulnerable endpoints by any column by clicking the filter icon beside the desired heading. Enter the value to include in the filter. You can toggle the *All/Any/Not* button for the following options:

- *All:* Display all files that match the set filter.
- *Any:* Display any file that matches the set filter.
- *Not:* Display only files that do not match the set filter.

Here, you can also click the hostname to view all detected vulnerabilities on that endpoint. You can filter the list of vulnerabilities in the same way that you can filter the list of endpoints above.

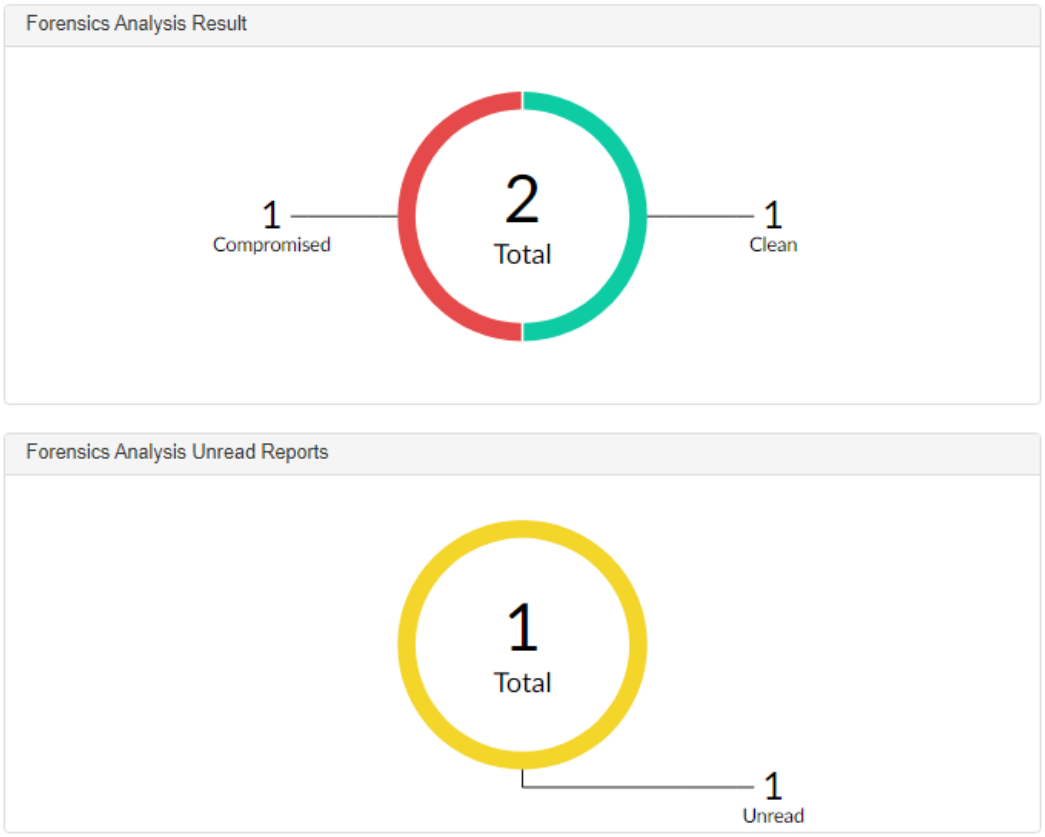


Vulnerability	Name of the vulnerability.
Category	Category of the vulnerability.
Severity	Severity level of the vulnerability.
Patch Status	You can click the *Patch* button to patch the selected vulnerability with the next Telemetry communication between FortiEndpoint and the endpoint. If a patch is already scheduled for the vulnerability, this column displays *Scheduled*. If the vulnerability must be patched manually, this column displays *Manual Patch*. FortiClient may be unable to automatically patch the vulnerability due to one of the following reasons: • **Third-party application vulnerabilities**: incorrect or missing installation paths • **OS vulnerabilities**: Windows update service is disabled In these cases, EMS may incorrectly display the status of these vulnerabilities that were selected to be automatically patched as *Scheduled* instead of *Failed*.

Viewing the Forensics Analysis dashboard

Go to *Dashboard* > *Forensics Analysis*. Here you can view a variety of charts and widgets containing a summary of Forensics analysis information from endpoints.

This feature requires the FortiGuard Endpoint Forensics Analysis license and for the FortiGuard Forensics Analysis feature to be enabled.



You can view forensics information in the following widgets:

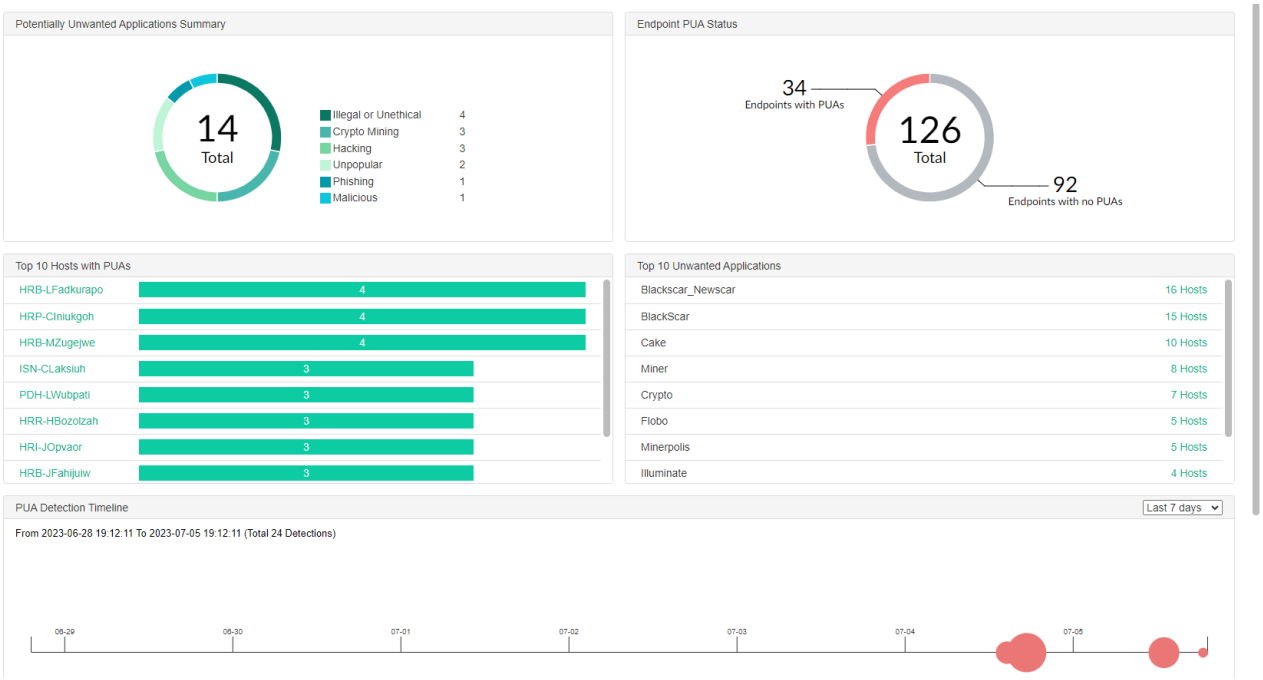
Widget	Information shown
Active Concurrent Forensics Analysis Requests	Number of active requests and available requests. You can only have five concurrent requests.
Forensics Analysis Status	Ticket status of each endpoint's forensics analysis task.
Forensics Analysis Result	Forensics verdict for analyzed endpoints: • Clean • Compromised • Suspicious
Forensics Analysis Unread Reports	Number of endpoints for which report are unread or not downloaded.
Top 10 Latest Forensics Analysis Reports	Analysis report, the time that it was updated, and the verdict.
Widget	Information shown

You can drill down on the *Forensics Analysis Status*, *Forensics Analysis Result*, and *Forensics Analysis Unread Reports* widgets by clicking into the charts.

Viewing the PUA dashboard

Go to *Dashboard* > *Vulnerability Scan*. Here you can view a variety of charts and widgets containing a summary of potentially unwanted application (PUA) information from endpoints.

This feature requires the Endpoint Protection Platform license and for the Software Inventory feature to be enabled.



You can view PUA information in the following widgets:

Widget	Description
Potentially Unwanted Applications Summary	Shows all detected PUAs categorized into the following: • Illegal or unethical • Cryptomining • Hacking • Unpopular • Phishing • Malicious
Endpoint PUA Status	Shows how many endpoints have PUAs and how many do not.
PUA Detection Timeline	Shows historical events related to PUA detection on a timeline. Hover over the red circles to see a popup with PUA detection count and the PUAs detected during that time period.
PUA Total Timeline	Shows line chart of PUA detection and uninstall events. Hover over the green icircles to see a popup with PUA totals, PUA detection count, and three events in that time period.

Widget	Description
Top 10 Hosts with PUAs	Displays the ten endpoints that have the most PUAs and the number of PUAs detected on those endpoints.
Top 10 Unwanted Applications	Displays the top ten most common PUAs and the number of hosts where the PUAs have been detected. Click the vulnerability name to see information about the vulnerability on FortiGuard.

You can drill down on information in the widgets. For example, for the Potentially Unwanted Applications Summary widget, you can click the Unpopular section of the chart to view all unpopular PUAs detected on endpoints. From there, you can further click a PUA to view all endpoints that have that PUA currently installed.

Viewing Chromebook Status

Chromebook Status displays a number of charts. Each chart provides a summary of Chromebook information. The sections in each chart are links. You can click any chart section or table row to display details. Chromebook Status is only available if you enabled *System Settings > EMS Settings > EMS for Chromebooks Settings*.

Option	Description
User Charts	
Active Users	Displays active and inactive users.
Managed Users	Displays managed and unmanaged users.
Webfilter Charts	
Top 10 Violations by Category	Displays the top ten web filter violations by category in the past few days. You can configure the number of days. Go to *System Settings > Logs*.
Top 10 Violations by User	Displays the top web filter violations by user in the past few days. You can configure the number of days. Go to *System Settings > Logs*.
Most Searched Monitored Words	Displays the top terms that users have searched that you have configured Web Filter to monitor. See Web Filter on page 320.
Most Searched Blocked Words	Displays the top terms that users have searched that you have configured Web Filter to block. See Web Filter on page 320.
Others	
System Information	See System Information widget on page 34.
License Information	See License Information widget on page 36.

Endpoint management

FortiEndpoint needs to determine which devices to manage. For Windows, macOS, and Linux endpoints, device information can come from an Active Directory server, Windows workgroup, or manual FortiClient connection.

For Chromebooks, device information comes from the Google Admin console.

Windows, macOS, and Linux endpoints

Device information can come from an AD server, Windows workgroup, or manual FortiClient connection. You can create groups to organize endpoints.

Managing groups

You can create groups to organize endpoints. You can also rename and delete groups.

The LDAP connection is read-only. These groups are local to EMS and are not seen in your Active Directory.

To create groups:

1. Go to *Endpoints*.
2. Right-click a domain or workgroup and select *Create group*. The *Create group* dialog displays.
3. In the *Required* field, enter a name for the group, and click *Confirm*.

To rename groups:

1. Go to *Endpoints*.
2. Right-click the group, and select *Rename group*. The *Rename the group* dialog displays.
3. In the *Required* field, enter the new name, and click *Confirm*.

To delete groups:

1. Go to *Endpoints*.
2. Right-click the group, and select *Delete group*. A confirmation dialog displays.
3. Click *Yes*.

Adding endpoints

You can add endpoints to EMS in one of the following ways:

Adding endpoints using an AD domain server

To add endpoints using an Active Directory (AD) domain server, you must add an AD server to EMS in *Administration > Authentication Servers*. See Adding an ADDS server on page 485.

To add endpoints using an AD domain server:

1. Go to *Endpoints > Manage Domains > Add*
2. From the *Authentication Server* dropdown list, select the desired AD server.
3. In the *Sync every* field, enter the desired sync schedule for the server.
4. Under *Select Base DN*, select the desired DNs to import. You can also add specific organizational units (OUs) and containers from the AD server to EMS. The *Changes to Selected Base DN* pane summarizes the changes to your selected base DNs.
   EMS does not support adding individual groups from an AD server. EMS allows importing users, devices, and subgroup members of a group that are contained in an imported OU. Review EMS import logic example on page 54, which provides an example of the EMS import logic, to ensure that you are able to import all desired endpoints to your EMS.

   EMS supports adding individual groups from Microsoft Entra ID. See Adding endpoints using an Entra ID server on page 55.
5. Click *Save*.

EMS import logic example

The following provides an example of EMS import logic using an example AD server with the following OU structure:

```
Root: myAD
├── OU: Premium
│   ├── Sub-OU: Department 1
│   │    ├── Sub-OU: Region-Americas
│   │          ├── Group A
│   │                  ├── Group B
│   │                  ├── Group C
│   ├── Sub-OU: Department 2
│       ├──  Group B
│              ├── Group D
├── OU: Basic
│   ├── Group C
```

Consider that on EMS, you only explicitly select the *Premium OU* and *Sub-OU: Region-Americas* to import. The OU structure shows these in bold. In this case, EMS imports the following:

Item	Reason imported
OU: Premium	Explicitly imported
Sub-OU: Region-Americas	

Item	Reason imported
Sub-OU: Department 1	Sub-OUs of *OU: Premium*, which you explicitly imported
Sub-OU: Department 2	
Group A	Contained by *Sub-OU: Region-Americas*, which you explicitly imported
Group B	Contained by *Group A*,which is contained by *Sub-OU: Region-Americas*, which you explicitly imported
Group C	

EMS does not import the following:

Item	Reason not imported
Group D	Although EMS imports Group B, since EMS does not import based on group membership, it does not import Group D, which is a member of Group B.
OU: Basic	Not selected to import

The following shows the OU tree with all items that EMS imports when you explicitly import *OU: Premium* and *Sub-OU: Region-Americas* bolded. *Group C* is shown bolded where *Group A* contains it:

```
Root: myAD
├── OU: Premium
│   ├── Sub-OU: Department 1
│   │    ├── Sub-OU: Region-Americas
│   │          ├── Group A
│   │                ├── Group B
│   │                ├── Group C
│   ├── Sub-OU: Department 2
│       ├──  Group B
│              ├── Group D
├── OU: Basic
│   ├── Group C
```

If you remove *Sub-OU: Region-Americas* from *OU: Premium*'s subtree, EMS still imports *Sub-OU: Region-Americas*. This is because you explicitly imported *Sub-OU: Region-Americas*.

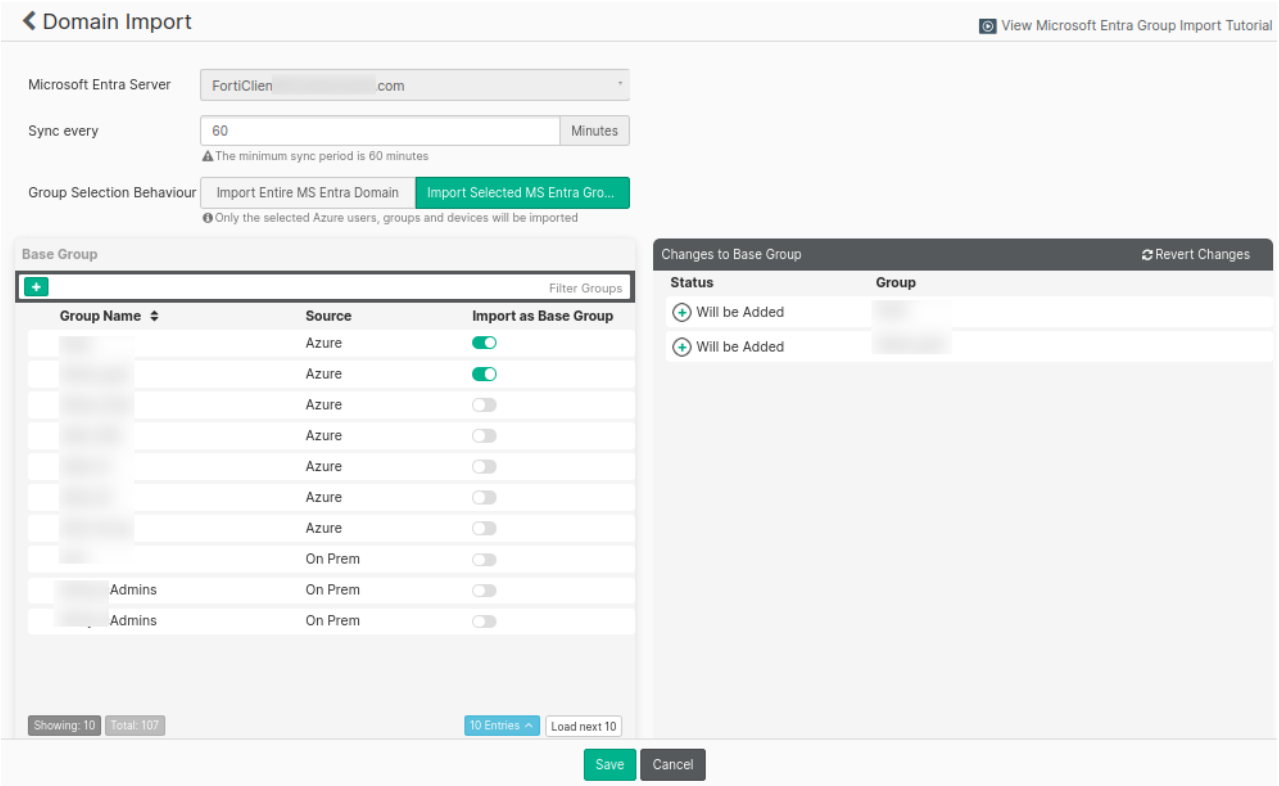
If you remove *Sub-OU: Department 2* from *OU: Premium*'s subtree, EMS does not import *Sub-OU: Department 2*. This is because you did not explicitly import *Sub-OU: Department 2*. EMS only imported it because it was in *OU: Premium*'s subtree.

Adding endpoints using an Entra ID server

To add endpoints using a Microsoft Entra ID (formerly known as Azure Active Directory (AD)) domain server, you must configure add an Entra ID server to EMS in *Administration > Authentication Servers*. See Adding an Entra ID server on page 487.

To add endpoints using an Entra ID server:

1. Go to *Endpoints* > *Manage Domains*.
2. Click *Add*, then *Azure*.
3. From the *Azure Server* dropdown list, select the desired server.
4. In the *Sync every* field, enter the number of minutes after which EMS syncs with the Azure server.
5. For *Group Selection Behaviour*, select *Import Entire Azure Domain* or *Import Selected Azure Groups*.
6. Enable *Import as Base Group* for the desired groups, then click *Save*.



Endpoints > *Domains* lists the Entra ID server domain groups and subgroups. It lists subgroups as a flat list and does not preserve the hierarchy from the Entra ID server.

Connecting manually from FortiClient

Endpoint users can manually connect FortiClient Telemetry to FortiEndpoint by specifying the IP address for FortiEndpoint in FortiClient. This process is sometimes called registering FortiClient to FortiEndpoint.

To manually connect to EMS from FortiClient:

1. In FortiClient on the endpoint, go to the *Fabric Telemetry* tab.
2. In *EMS IP* field, enter the EMS IP address, and click *Connect*. FortiClient connects to FortiClient EMS.

For information about FortiClient, see the *FortiClient Administration Guide*.

The FortiClient Telemetry gateway port may be appended to the gateway list address on FortiClient and separated by a colon. When the port is not provided, FortiClient attempts to connect to the IP address given using the default port. The default connection port in FortiClient 6.0 and 6.2 is 8013. By default, FortiClient EMS listens for connection on port 8013.

Adding endpoints using an AD domain server is considered best practice. Connecting FortiClient to FortiClient EMS manually is only recommended for troubleshooting purposes.

Viewing endpoints

After you add endpoints to FortiEndpoint, you can view the list of endpoints in a domain or workgroup in the *Endpoints* pane. You can also view details about each endpoint and use filters to access endpoints with specific qualities.

Viewing the Endpoints pane

You can view information about endpoints in *Endpoints*.

To view the *Endpoints* pane:

1. Go to *Endpoints*, and select *All Endpoints*, a domain, or workgroup. The list of endpoints, a quick status bar, and a toolbar display in the content pane.

Not Installed	Number of endpoints that do not have FortiClient installed. Click to display the list of endpoints without FortiClient installed.
Not Registered	Number of endpoints that are not connected to FortiEndpoint. Click to display the list of disconnected endpoints.
Out-Of-Sync	Number of endpoints with an out-of-sync profile. Click to display the list of endpoints with out-of-sync profiles.
Security Risk	Number of endpoints that are security risks. Click to display the list of endpoints that are security risks.
Quarantined	Number of endpoints that EMS has quarantined. Click to display the list of quarantined endpoints.
Endpoints	Click the checkbox to select all endpoints displayed in the content pane.
Show/Hide Heading	Click to hide or display the following column headings: *Device*, *User*, *IP*, *Configurations*, *Connections*, and *Alerts and Events*.
Show/Hide Full Group Path	Click to hide or display the full path for the group that the endpoint belongs to.

Refresh	Click to refresh the list of endpoints.
Search All Fields	Enter a value and press *Enter* to search for the value in the list of endpoints.
Filters	Click to display and hide filters you can use to filter the list of endpoints.
Device	Visible when headings are displayed. Displays an icon to represent the OS on the endpoint, the hostname, and the endpoint group.
User	Visible when headings are displayed. Displays the name and icon of the user logged into the endpoint. Also displays the endpoint status: • **Online**: endpoint has been seen within less than three keep alive timeouts. • **Away**: endpoint has been offline for less than eight hours. • **Offline**: endpoint has been offline for more than eight hours. • **Never Seen**: endpoint has never been registered to EMS. When using user-based licensing, you can use the dropdown list to view all registered users for this endpoint. The dropdown list displays the verified user and device username.
IP	Visible when headings are displayed. Displays the endpoint IP address.
Configurations	Visible when headings are displayed. Displays the name of the policy assigned to the endpoint and its synchronization status.
Connections	Visible when headings are displayed. Displays the connection status between FortiClient and FortiEndpoint. If the endpoint is connected to a FortiGate, displays the FortiGate hostname.
Alerts and Events	Visible when headings are displayed. Displays FortiClient alerts and events for the endpoint.  For Web Filter on page 320 events, only events of the *Block* and *Warn* categories are displayed here. Events of the *Allow* and *Monitor* categories are not displayed.

2. Click an endpoint to display its details in the content pane. The following dropdown lists display in the toolbar for the selected endpoint:

Scan	Click to start a Vulnerability or AV scan on the selected endpoint.
Patch	Click to patch all critical and high vulnerabilities on the selected endpoint. Choose one of the following options: • Selected Vulnerabilities on Selected Clients • Selected Vulnerabilities on All Affected Clients • All Critical and High Vulnerabilities
Move to	Move the endpoint to a different group.

Action	Click to perform one of the following actions on the selected endpoint: • Request FortiClient Logs • Request Diagnostic Results • Update Signatures • Download Available FortiClient Logs • Download Available Diagnostic Results • Deregister • Quarantine • *Un-quarantine* • *Exclude from Management* • *Revoke Client Certificate*: only available if the ZTNA or EPP license is applied. Revoke the certificate that FortiClient is using to securely encrypt and tunnel TCP traffic through HTTPS to the FortiGate. You may want to revoke a certificate if it becomes compromised and can no longer be trusted. When a certificate is revoked, EMS prompts FortiOS and FortiClient with a new certificate signing request. • Clear Events • Mark as Uninstalled • Set Importance • Set Custom Tags. This option is only available if you have already created a custom tag. • Delete Stale Verified Users. This option deletes stale verified users and only keeps the last seen record for each machine user on an endpoint. For example, if two users onboarded on FortiClient on an endpoint, this option removes the user who onboarded earlier one. This option does not affect license seats. • Delete Device • Send Message. See Sending endpoints one-way message on page 66.

The following tabs are available in the content pane toolbar when you select an endpoint, depending on which FortiClient features are installed on the endpoint and enabled via the assigned profile:

Summary		
	<user name>	Displays the name of the user logged into the selected endpoint. Also displays the user's avatar, email address, and phone number if these are provided to FortiClient on the endpoint. If the user's LinkedIn, Google, Salesforce, or other cloud app account is linked in FortiClient, the username from the cloud application displays. Also displays the group that the endpoint belongs to in EMS.
	Device	Displays the selected endpoint's hostname. You can enter an alias if desired.

	OS	Displays the selected endpoint's operating system and version number.
	IP	Displays the selected endpoint's IP address.
	MAC	Displays the selected endpoint's MAC address.
	Last Seen	Displays the last date and time that FortiClient sent a keepalive (KA) message to EMS. This information is useful if FortiClient is offline because it indicates when the last KA message occurred.
	Location	Displays whether the selected endpoint is on- or off-fabric. You can also view any on-fabric detection rules that the endpoint is applicable for. See On-fabric Detection Rules on page 124.
	Network Status	Displays the following information for the networks that the endpoint is connected to: • MAC address • IP address • Gateway IP address • Gateway MAC address • SSID for Wi-Fi connections
	Hardware Details	Displays the hardware model, vendor, CPU, RAM, and serial number information for the endpoint device, if available.
	Security Posture Tags	Displays which tags have been applied to the endpoint based on the security posture tagging rules. See Security Posture Tags on page 408.
	FortiGuard Outbreak Detections	Displays which FortiGuard Outbreak tags have been applied to the endpoint based on the FortiGuard Outbreak Alerts service rules. See FortiGuard Outbreak Alerts on page 448.
	Connection	Displays the connection status between the selected endpoint and FortiEndpoint.
	Configuration	Displays the following information for the selected endpoint: • Policy: Endpoint policy assigned to the selected endpoint • Installer: FortiClient installer used for the selected endpoint. • FortiClient Version: FortiClient version installed on the selected endpoint. • FortiClient Serial Number: Serial number for the selected endpoint's FortiClient license. • FortiClient ID • ZTNA Serial Number: serial number for the zero trust network access certificate provisioned to the endpoint. • MDM Enrolled: whether the endpoint is enrolled on a mobile device management (MDM) platform. • MDM Deployment Status: whether a ZTNA certificate provisioned through MDM has been installed on the endpoint.

	Classification Tags	Displays classification tags that are assigned to the endpoint. You can also assign a classification tag to the endpoint. Classification tags include the default importance level tags (low, medium, high, or critical), and custom tags. An endpoint can only have one default importance tag assigned, but can have multiple custom tags assigned. You can also unassign a tag from the endpoint, and create, assign, or delete a custom tag. To create a new custom tag, click *Add*, enter the desired tag, then click the *+* button. When you create a tag, it is available for assignment to all endpoints in the site. You can assign a classification tag to multiple endpoints by selecting the endpoints, then selecting *Action > Set Importance* or *Set Custom Tags*. Tags that FortiEndpoint receives from FortiAnalyzer also display under *Classification Tags*. Configuring a maximum of eight custom tags is recommended. Configuring more than eight custom tags may result in performance or management issues. See Sending endpoint classification tags to FortiAnalyzer on page 72.
	Classification Tags - Fabric	Displays Fabric classification tags that are currently assigned to the endpoint. In a Fabric deployment, FortiEDR can detect suspicious or compromised endpoint behavior, share that endpoint's security status with EMS, and tag the affected endpoint on EMS. You can view these tags under *Classification Tags - Fabric*. You can also unassign a tag from the endpoint. The following lists the predefined tags for FortiEDR use: • **FortiEDR_Malicious**: FortiEDR has classified this endpoint as malicious. • **FortiEDR_PUP**: FortiEDR has detected a potentially unwanted program on this endpoint. • **FortiEDR_Suspicious**: FortiEDR has detected suspicious activity on this endpoint. • **FortiEDR_Likely_Safe**: FortiEDR has detected this endpoint as likely to be safe. • **FortiEDR_Probably_Good**: FortiEDR has determined that this endpoint is not a safety risk. See Identity Management integration.

	Forensic Analysis	Displays statuses for forensic analysis tasks:
		• **Ticket Status**: status of the ticket. Possible statuses are:
		  • **Request Submitted**
		  • **Pending**: Forensic analysis request has been initiated. The Forensics team has not yet assigned it to an analyst.
		  • **Running**
		  • **In Progress**: Forensics team has assigned the request to an analyst, who has begun working on it.
		  • **Failed**: analyst could not connect to the endpoint.

		• **Cancelled**: indicates one of the following:
		  • The analyst needed more information about the endpoint to perform the analysis.
		  • The EMS administrator canceled the request.
		 • **Completed**: analyst has completed analysis on the endpoint and shared the result in a PDF document. You can download the report from the endpoint summary's *Forensic Analysis* section.
		• **Agent Status**: status of the forensic agent collecting logs on the endpoint. Possible statuses are:
		 • **Pending**: EMS has notified FortiClient that a forensic analysis request is submitted, but the forensic agent is not running yet.
		 • **Running**: forensics agent starts collecting forensics logs.
		 • **Collection Completed**: forensics agent has completed collecting forensics logs.
		 • **Upload Started**: FortiClient has started to upload the logs to the cloud.
		 • **Upload Completed**: FortiClient has completed uploading the logs to the cloud.
		 • **Upload Failed**: FortiClient failed to upload the logs to the cloud.
		• **Verdict**: forensic analysis verdict as determined by the FortiGuard analyst.
		• **Task ID**: Request ID in the FortiGuard forensics system.
		• **Request Analysis**: request forensic analysis on the endpoint. See Requesting forensic analysis on an endpoint on page 83.
		• **Download Report**: download the forensic analysis report.

	Status	Displays one of the following statuses: • Managed: Endpoint is managed by EMS. • Quarantined: If quarantined, displays access code. The user can enter this access code in the affected endpoint's FortiClient to remove the endpoint from quarantine. • Excluded: Endpoint is excluded from management by EMS.
	FortiDeceptor Campaign Deployment	Displays the status of the FortiDeception token if enabled on the endpoint: • When the token is deployed to FortiClient, the field progresses from *Pending* to *Notified* to *Deployed*. • When the token is removed from FortiClient, the field progresses from *Pending to uninstall* to *Notified to uninstall* to *Clean*. The *FortiDeceptor Campaign Deployment* field will eventually no longer be visible for the endpoint. See FortiDeceptor Campaign on page 374.

	Endpoint Health	Provides a comprehensive view of feature statuses, such as whether a feature is installed, not installed, enabled, or disabled. It also reports any warnings or error messages associated with a feature. For example, if FortiClient cannot connect to VPN, an error displays under *Remote Access*. This enhanced visibility significantly improves the ability to diagnose and troubleshoot feature-related issues. You can effectively identify and resolve problems specifically linked to endpoint feature configurations and statuses. A feature may have one of the following statuses: • *OK* • *Warning* • *Error* • *Disabled* • *Not Installed* Clicking the status opens a slide-in with detailed information about the status. For the *Warning* and *Error* statuses, the *Description* may provide details to explain the cause, which you can investigate.
	Third Party Features	Displays which third party features are installed and running on the endpoint. This section includes the status of FortiEDR on the endpoint. This information is only available for Windows endpoints.
Antivirus Events		
	Date	Displays the antivirus (AV) event date and time.
	Count	Displays the number of occurrences for this event.
	Message	Displays the AV event's message.
	Actions	Mark the event as read or delete it.
Cloud Scan Events		
	Date	Displays the cloud-based malware detection event's date and time.
	Count	Displays the number of occurrences for this event.
	Message	Displays the cloud-based malware detection event's message.
	Actions	Mark the event as read or delete it.
Anti-Ransomware Events		
	Date	Displays the anti-ransomware event's date and time.
	Count	Displays the number of occurrences for this event.
	Message	Displays the anti-ransomware event's message. The message may say that FortiClient detected ransomware on the endpoint, or that FortiClient restored a file that the detected ransomware encrypted.
	Actions	Mark the event as read or delete it.
AntiExploit Events		

	Date	Displays the AntiExploit event's date and time.
	Count	Displays the number of occurrences for this event.
	Message	Displays the AntiExploit event's message.
	Actions	Mark the event as read or delete it.
USB Device Events		
	Date	Displays the USB device event's date and time.
	Count	Displays the number of occurrences for this event.
	Message	Displays the USB device event's message.
	Actions	Mark the event as read or delete it.
Sandbox Events		
	Date	Displays the sandbox event's date and time.
	Message	Displays the sandbox event's message.
	Rating	Displays the file's risk rating as retrieved from FortiSandbox.
	Checksum	Displays the checksum for the file.
	Download	Download a PDF version of the detailed report.
	Magnifying glass	Click to view a more detailed report. See Viewing Sandbox event details on page 70.
Firewall Events		
	Date	Displays the firewall event's date and time.
	Count	Displays the number of occurrences for this event.
	Message	Displays the firewall event's message.
	Actions	Mark the event as read or delete it.
Web Filter Events		
	Date	Displays the web filter event's date and time.
	Count	Displays the number of occurrences for this event.
	Message	Displays the web filter event's message.
	Actions	Mark the event as read or delete it.
Videofilter Events		
	Date	Displays the video filter event's date and time.
	Count	Displays the number of occurrences for this event.
	Message	Displays the video filter event's message.

	Actions	Mark the event as read or delete it.
Vulnerability Events		
	Vulnerability	Displays the vulnerability's name. For example, *Security update available for Adobe Reader*.
	Category	Displays the vulnerability's category. For example, *Third Party App*.
	Application	Displays the name of the application with the vulnerability.
	Severity	Displays the vulnerability's severity.
	Patch Type	Displays the patch type for this vulnerability: *Auto* or *Manual*.
	FortiGuard	Displays the FortiGuard ID number. If you click the FortiGuard ID number, it redirects you to FortiGuard where further information is provided if available.
PUA Events		
	Name	Displays the potentially unwanted application (PUA) name.
	Vendor	Displays the PUA vendor name.
	Version	Displays the PUA version number.
	Category	Displays the PUA category that the application belongs to. PUA categories are as follows: • Illegal or unethical • Cryptomining • Hacking • Unpopular • Phishing • Malicious
	Date	Displays the date that EMS detected the PUA. This column is available in *Events* view.
	Event Type	Displays the event type, such as *Detected* (EMS detected the PUA) or *Uninstalled* (the PUA was uninstalled from the endpoint). This column is available in *Events* view.
Data Protection Events		
	Date	Displays the date the end user triggered the data protection event.
	Count	Displays the number of occurrences for this event.
	Message	Displays the event message.
	Actions	Mark the event as read or delete it.
System Events		
	Date	Displays the system event's date and time.
	Count	Displays the number of occurrences for this event.

	Message	Displays the system event's message.
	Actions	Mark the event as read.

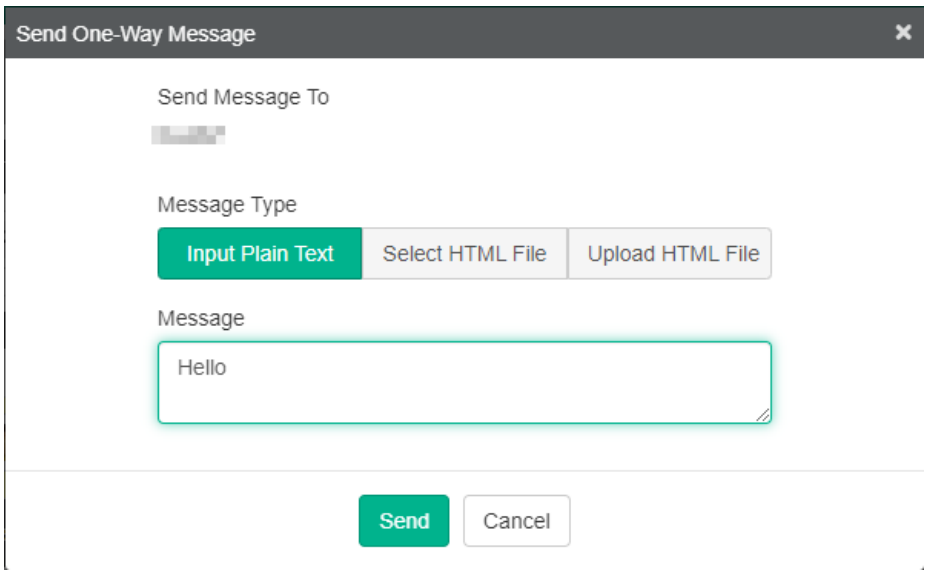
Sending endpoints one-way message

The EMS administrator can send a one-way message to endpoints in a tagged group, endpoint group, or one endpoint. For example, you may want to send a message to remind a user to upload an avatar to FortiClient. EMS sends the message at the next keepalive interval. By default, this is 60 seconds.

The message can be in plain text or HTML format.

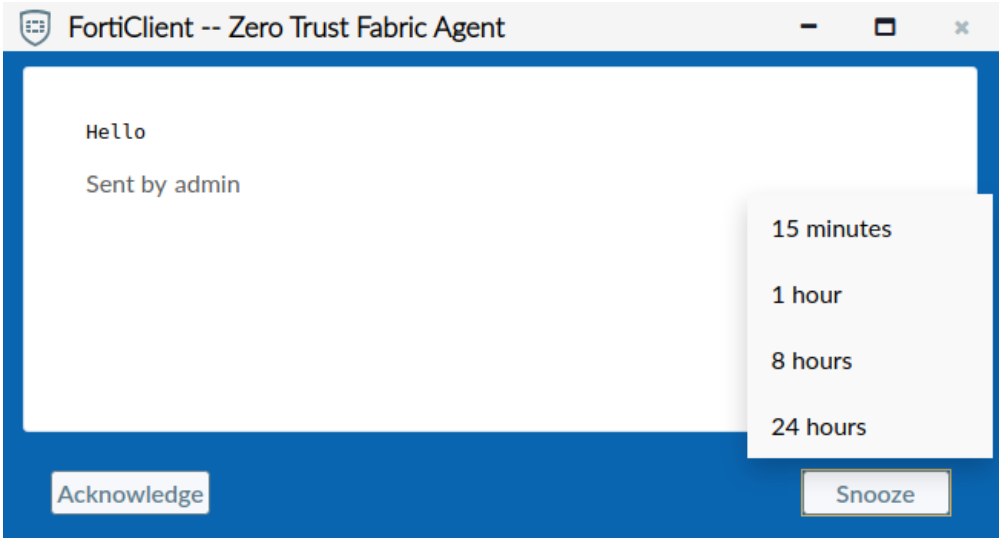
To send an endpoint a message:

1. In EMS, go to *Endpoints* > *All Endpoints*.
2. Select the desired endpoint(s).
3. Click *Action* > *Send Message*.
4. Do one of the following:
   a. To send a plain text message, select *Input Plain Text*. In the *Message* field, enter the desired text. Click *Send*.



   b. To send an HTML message, do the following:
      i. Click *Upload HTML File*.
      ii. Click *Browse*.
      iii. Navigate to and select the desired HTML file.
      iv. Click *Send*.

When the message appears on the endpoint, the user can acknowledge or snooze the message for their desired amount of time.



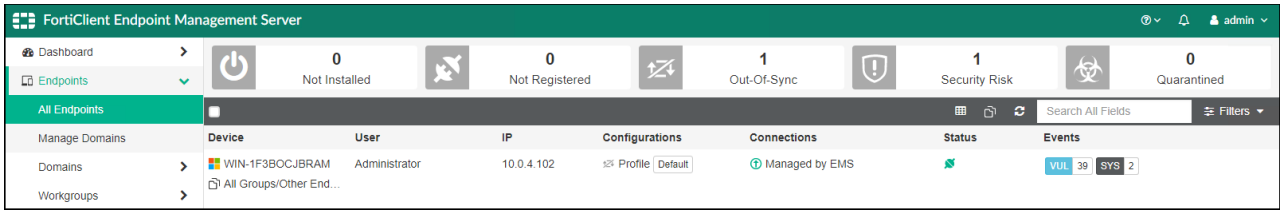
FortiClient logs a system event for when the user snoozes the message and when they acknowledge it.

Using the quick status bar

You can use the quick status bar to quickly display filtered lists of endpoints on the *Endpoints* content pane.

To use the quick status bar:

1. Go to *Endpoints*.
2. Click *All Endpoints*, a domain, or workgroup.
   The list of endpoints and quick status bar display.



3. Click one of the following buttons in the quick status bar:
   - Not Installed
   - Not Registered
   - Out-Of-Sync
   - Security Risk
   - Quarantined

   The list of affected endpoints displays.
4. Click an endpoint to display its details.
5. In the *Events* column, click the *AV <number>*, *SB <number>*, *FW <number>*, *VUL<number>*, *WEB <number>* and *SYS<number>* buttons to display the associated tab of details for the selected endpoint.
6. Click the *Total* button to clear the filters. The unfiltered list of endpoints displays.

Viewing endpoint details

You can view each endpoint's details on the *Endpoints* content pane. For a description of the options on the *Endpoints* content pane, see Viewing the Endpoints pane on page 57.

To view endpoint details:

1. Go to *Endpoints*, and select *All Domains*, a domain, or workgroup. The list of endpoints for the selected domain or workgroup displays.
2. Click an endpoint to display details about it in the content pane. Details about the endpoint display in the content pane.

Filtering the list of endpoints

You can filter the list of endpoints displayed on the *Endpoints* content pane.

To filter the list of endpoints:

1. Go to *Endpoints*.
2. Click *All Domains*, a domain, or workgroup. The list of endpoints displays.
3. Click the *Filters* menu, and set filters. The filter options display. For text values, you can use a comma (,) to separate values and an exclamation mark (!) to exclude a value. For buttons, hover the mouse over each button to view its tooltip.

Device		Lists the filter options for devices.
	Name	Enter the name(s) to include in the filter.
	User	Enter the name of the user(s) to include in the filter.
	Group	Enter the name of the group(s) to include in the filter.
	IP	Enter the IP address to include in the filter.
	OS	Enter the name of the operating system(s) to include in the filter.
	Tag	Enter the tag(s) to include in the filter. This includes security posture tagging and classification tags. See Security Posture Tags on page 408 and Viewing the Endpoints pane on page 57.
FortiClient		Lists the filter options for FortiClient version numbers.
	Version	Enter the FortiClient version number to include in the filter.
Deployment Package		Lists the filter options for deployment.
	Name	Enter the name(s) of the deployment package to include in the filter.
	Status	Click one or more deployment status buttons to include in the filter. Selected status buttons are green. Hover the mouse over each button to view its tooltip. Clear the status button to exclude the status from the filter. Excluded status buttons are gray.

	More States	Click to display additional statuses to include in the filter.
Policy		
	Name	Enter the name(s) of the policy to include in the filter.
	Status	Click the policy status to include in the filter. Selected status buttons are green. Choose between *Synced* and *Out-Of-Sync*. Clear the status button to exclude the status from the filter. Excluded status buttons are gray.
Profile		
	Name	Enter the name(s) of the profile to include in the filter.
Forensics		
	Enabled	Click whether to filter the list by endpoints where the Forensics feature is enabled or disabled.
	Status	Click one or more forensic analysis statuses to include in the filter. Selected status buttons are green. Clear the status button to exclude the status from the filter. Excluded status buttons are gray.
	Verdict	Click one or more forensic analysis verdicts to include in the filter. Selected status buttons are green. Clear the verdict button to exclude the status from the filter. Excluded verdict buttons are gray.
EMS		
	Status	Click the status for FortiClient Telemetry connection to EMS to include in the filter. Selected status buttons are green. Clear the status button to exclude the status from the filter. Excluded status buttons are gray.
User Verification		
	Status	Filter the list by endpoints depending on their user verification status. See User Management on page 498.
FortiGate		
	Serial	Filter the list by a FortiGate serial number that the endpoint is connected to. If desired, click *Exact match* to filter by only a FortiGate with a serial number that exactly matches the input.
Invitation		
	Name	Filter the list by the name of the invitation assigned to the endpoint
	Code	Filter the list by the name of the invitation code assigned to the endpoint
FortiDeceptor Campaign Deployment		

	Status	Filter the list by the status of the FortiDeception token deployment on the endpoint. See FortiDeceptor Campaign on page 374.
Events		Select the events to include in the filter. The selected checkboxes beside the events are included in the filter. Clear the checkbox beside the event to exclude the event from the filter.
Features		Enter the AV, Firewall, and/or vulnerability signature and/or engine to filter for.
Bookmarks		Displays the list of saved filter settings. Displays only after you have saved a bookmark. Click the *Bookmark* button to name and save filter settings. Click a bookmark to use the saved settings. Click the *x* beside a bookmark to delete it.
Search		Click the *Search* button to apply the filter setting.
Reset		Click the *Reset* button to clear the filter settings.
Bookmark		Click the *Bookmark* button to save the filter settings as a bookmark.

4. Click *Search*. The filtered list of endpoints displays.
5. Click *Reset* to clear the filter settings.

Using bookmarks to filter the list of endpoints

You can save filter settings as bookmarks, then select the bookmarks to use them.

To create bookmarks to filter endpoints:

1. Go to *Endpoints*.
2. Click *All Endpoints*, a domain, or workgroup. The list of endpoints displays.
3. Click the *Filters* menu, and set filters.
4. Click the *Bookmark* button.
5. In the *New Bookmark* field, enter a name for the filter settings, and press *Enter*.The bookmark displays under *Bookmarks*.

To use bookmarks to filter the list of endpoints:

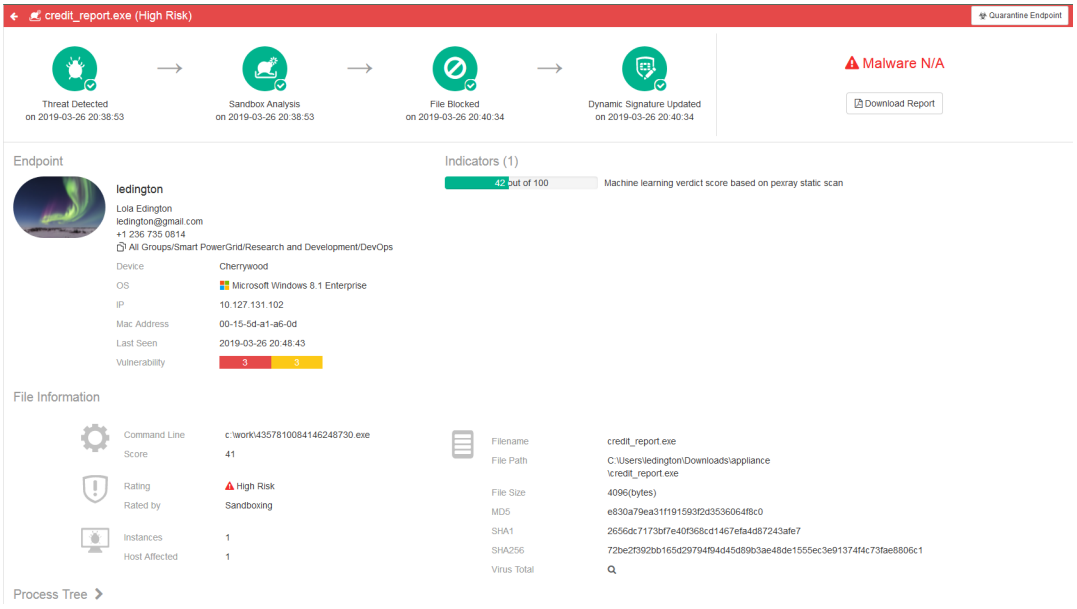
1. Go to *Endpoints*.
2. Click *All Endpoints*, a domain, or workgroup. The list of endpoints displays.
3. Click the *Filters* menu.
4. In the *Bookmarks* list, click a bookmark. The bookmark settings are used to filter the list of endpoints.

Viewing Sandbox event details

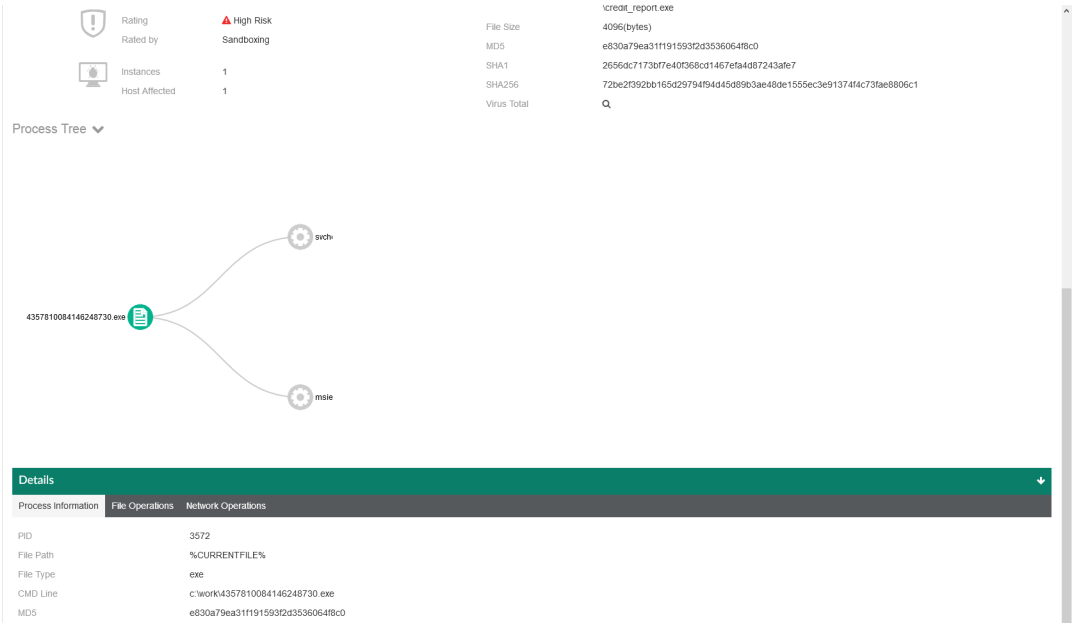
You can view a detailed report about a Sandbox event. EMS retrieves the report from FortiSandbox.

To view Sandbox event details:

1. Go to *Endpoints*, and select *All Domains*, a domain, or workgroup. The list of endpoints for the selected domain or workgroup displays.
2. Click an endpoint to display details about it in the content pane. Details about the endpoint display in the content pane.
3. On the *Sandbox Events* tab, click the magnifying glass icon beside the desired Sandbox event. EMS displays a detailed report about the Sandbox event.



4. Click *Process Tree*. For some events, you can see a graphical representation of the processes that the malware created on FortiSandbox.



Sending endpoint classification tags to FortiAnalyzer

You can use tags for grouping and classifying endpoints, which can help with assessing incident impact and prioritizing incidents by SOC analysts or SOAR playbooks.

You can assign a classification tag to an endpoint. Classification tags include the following:

- Default importance level tags (low, medium, high, or critical) to specify an endpoint's importance in the organization. You can tag critical endpoints accordingly and monitor them for security incidents.
- Custom tags. Configuring a maximum of eight custom tags is recommended. Configuring more than eight custom tags may result in performance or management issues. You can assign multiple custom tags to an endpoint or group of endpoints.

FortiAnalyzer Fabric View shows tags for each endpoint. FortiAnalyzer FortiSoC playbook pulls endpoint information from EMS using an EMS connector.

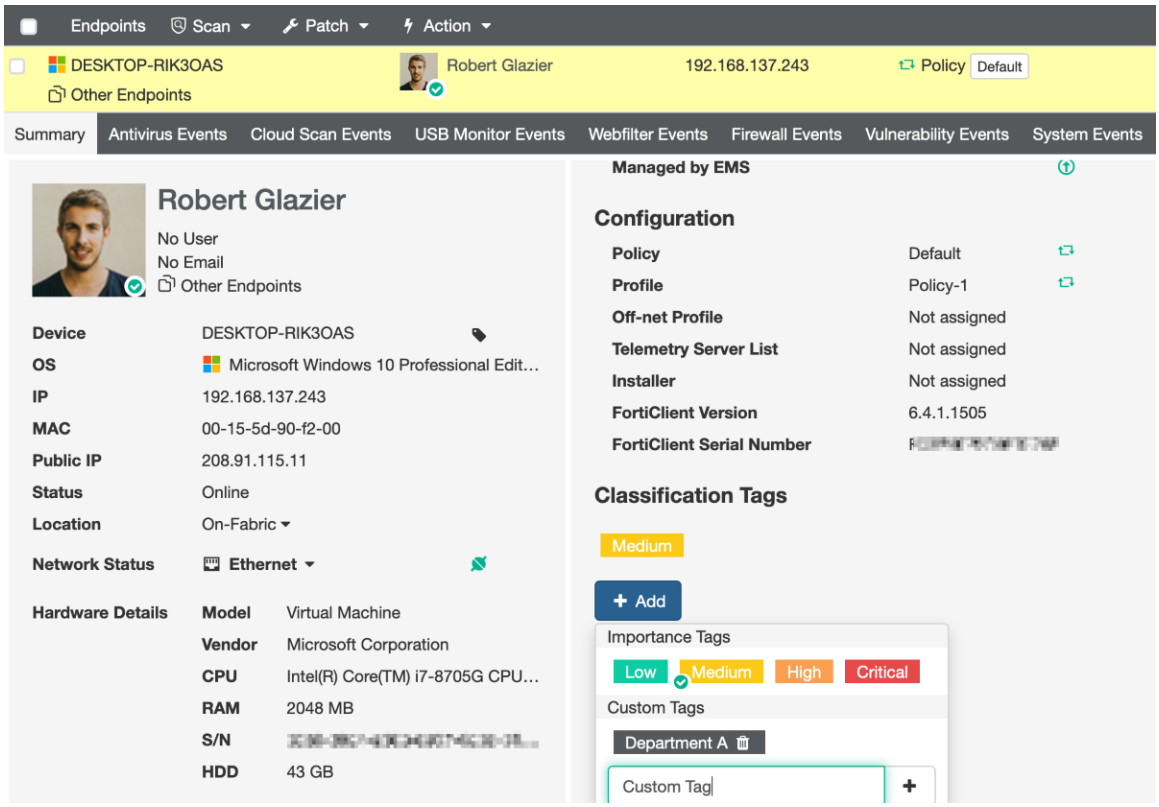
The following describes the process for configuring a classification tag and viewing the data in FortiAnalyzer:

1. Configure and apply classification tags to endpoints in EMS.
2. Configure FortiAnalyzer to receive the tags:
   a. Configure the EMS-FortiAnalyzer Fabric connection.
   b. Run the FortiSoC playbook to retrieve endpoint information from EMS.

To configure and apply classification tags to endpoints in EMS:

By default, EMS tags all newly registered endpoints with the Low default importance tag.

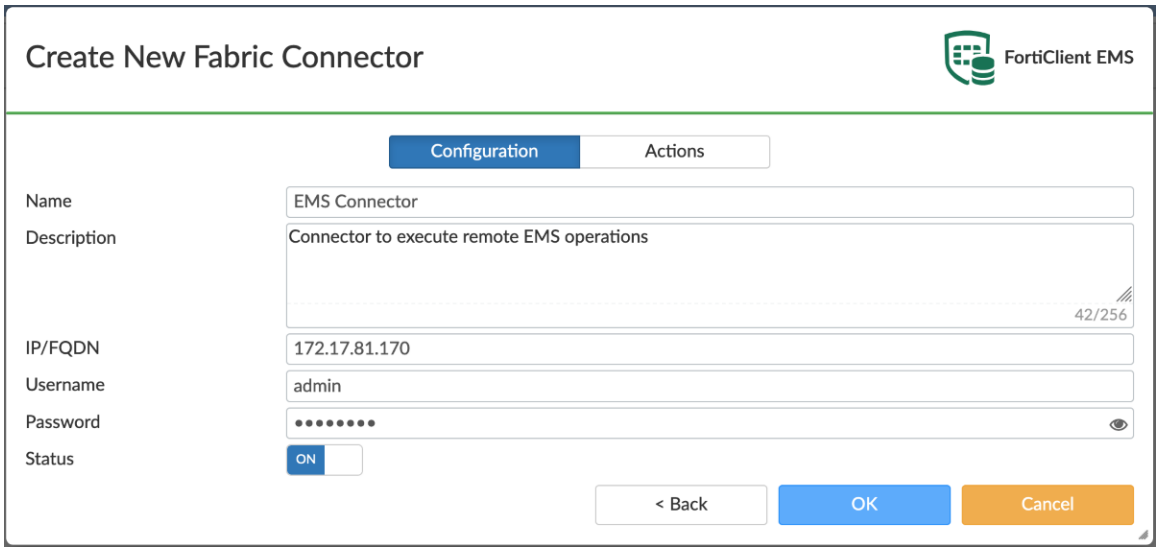
1. In EMS, go to *Endpoints*.
2. To apply tags to a single endpoint, go to the desired endpoint. Under *Classification Tags*, to create a new custom tag, click the *Add* button, enter the desired tag, the click the + button. You can also assign a new importance tag to the endpoint.



3. To apply tags to multiple endpoints, select all desired endpoints, then select *Action* > *Set Importance* or *Set Custom Tags*.

To configure the EMS-FortiAnalyzer Fabric connection:

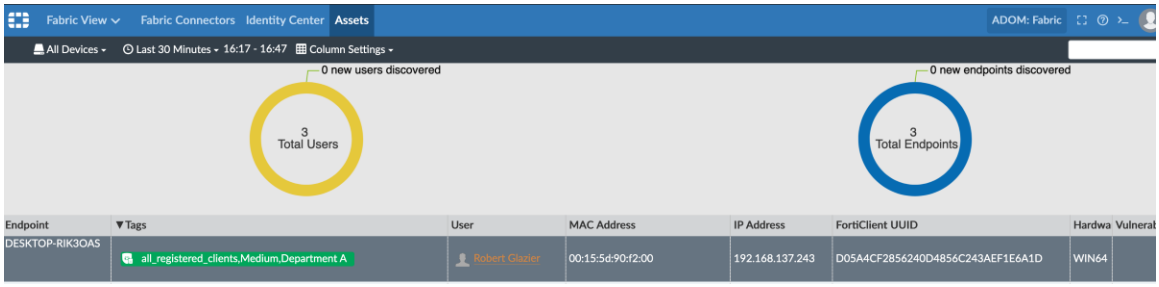
1. In FortiAnalyzer, go to *Fabric View*.
2. Click the *Fabric Connectors* tab, then click *Create New*.
3. Click the *FortiClient EMS* tile. The *Create New Fabric Connector* dialog opens.
4. In the *Configuration* tab, configure the connector settings, enter the EMS IP address and administrator credentials.



5. On the *Actions* tab, leave the default settings.
6. Click *OK*.

To run the FortiSoC playbook to retrieve endpoint information from EMS:

1. In FortiAnalyzer, in the Fabric ADOM, go to *FortiSoC > Automation > Playbook*.
2. Click *Create New*, then *New Playbook created from scratch*.
3. Add an on-demand playbook with two tasks:
```
* FabricView--FortiSoC--Playbook
-- EMS_GET_ENDPOINTS (no parameters)
-- LOCALHOST_UPDATE_ASSET_AND_IDENTITY (use parameter ems_endpoints = previous_task_id.ems_
     endpoints)
```
4. Click *Save*.
5. Click *Run*. Accept the *Manually Run Playbook* prompt.
6. Go to *Automation > Playbook Monitor*. You can view the running playbook status.
7. Once the corresponding playbook job finishes running, go to *Fabric View > Assets*. The endpoint and its tags display.



Exporting endpoint information

You can export endpoint information from EMS as a CSV file. You can use this data for compliance, software auditing, and so on.

To export endpoint information:

1. In EMS, go to *Endpoints > All Endpoints*.
2. Go to the desired endpoint group.
3. In the top right corner, click *Export CSV*.
4. In the confirmation dialog, click *Export*. This downloads a .zip file to the device which contains endpoint information in .csv format. The following shows an example:

```
device_id,name,ip_addr,os_version,cpu,manufacturer,sn,mem,hdd,model,ipv6_addr,mac_
addr,host,remote_ip,network_interfaces,group_id,group_name,group_path,orig_group_
name,domain_id,installer_name,deployment_state,fgt_sn,forticlient_id,uid,fct_
version,diskenc,av_product,is_installed,is_managed,is_migrating,is_ems_registered,is_ems_
online,is_ems_onnet,is_excluded,is_quarantined,quarantine_access_code,comparable_fct_
version,assigned_tags,last_seen,last_seen_fct_user_id,fct_users,endpoint_policy_
name,endpoint_policy_id,ip_list_name,av_enabled,rtp_enabled,ae_enabled,cs_enabled,rm_
enabled,fw_enabled,wf_enabled,vpn_enabled,vuln_enabled,ssoma_enabled,sb_enabled,sb_cloud_
enabled,rs_enabled,onboarding_supported,client_version_up_to_date,client_av_sig_version_
up_to_date,client_policy_synced,client_policy_primary_synced,client_policy_offnet_
synced,client_policy_iplist_synced,client_policy_onnet_rule_synced,client_policy_
verification_rule_synced,client_policy_certs_synced,av_events_count,wf_events_count,fw_
events_count,sb_events_count,ae_events_count,rm_events_count,cs_events_count,unreg_
events_count,rs_events_count,nwifsc_events_count,vuln_events_count,vuln_events_max_
severity,profile_components,off_net_profile_components
"""4""","""Boromir""","""192.168.0.10""","""Microsoft Windows 10 Enterprise Edition, 32-
bit (build 19044)""","""Intel(R) Core(TM) i9-9980HK CPU @ 2.40GHz""","""Microsoft
Corporation""","""...""","""2047""","""99""","""Virtual
Machine""","""""""","""...""","""Boromir""","""192.168.0.10""","""[intf_
name:Ethernet%203,mac:...,ip:192.168.0.10, gw_ip:192.168.0.100, gw_mac:..., ssid:,
route:0]""","""2""","""Other Endpoints""","""All Groups/Other
Endpoints""",,,,,,"""1""","""...""","""7.2.0.0690""","""""","""""","""True""","""True""",
"""False""","""True""","""True""","""True""","""0""","""0""",,"""7002000""","""[all_
registered_clients]|[Low]""","""2023-06-15 20:50:37""","""1""","""
[brando]""","""Policy01""","""2""",,"""True""","""True""","""False""","""False""","""Fals
e""","""True""","""True""","""True""","""True""","""False""","""False""","""True""","""Tr
ue""","""1""","""True""","""1""","""True""","""True""","""True""","""True""","""True""","
""True""","""True""","""2""","""2""","""0""","""0""","""0""","""0""","""0""","""1""","""0
""","""1""","""0""",,"""{'malware': {'id': 2, 'name': 'Profile01'}, 'sandbox': {'id': 2,
'name': 'Profile01'}, 'webfilter': {'id': 3, 'name': 'Profile01', 'fp_name': ''},
'firewall': {'id': 2, 'name': 'Profile01'}, 'vpn': {'id': 2, 'name': 'Profile01'},
'vulnerability_scan': {'id': 2, 'name': 'Profile01'}, 'system': {'id': 3, 'name':
'Profile01'}, 'ztna': {'id': 2, 'name': 'Profile01'}, 'videofilter': {'id': 2, 'name':
'Profile01'}}""","""{}"""
"""6""","""Legolas""","""192.168.0.15""","""Microsoft Windows 11 Professional Edition,
64-bit (build 22621)""","""Intel(R) Core(TM) i9-9980HK CPU @ 2.40GHz""","""Microsoft
Corporation""","""...""","""4094""","""69""","""Virtual
Machine""","""""""","""...""","""Legolas""","""192.168.0.15""","""[intf_
name:Ethernet,mac:...,ip:192.168.0.15, gw_ip:192.168.0.100, gw_mac:..., ssid:,
route:0]""","""2""","""Other Endpoints""","""All Groups/Other
```

```
Endpoints""",,,,,,"""2""","""...""","""7.2.1.0779""","""""""","""""""","""True""","""True""",
"""False""","""True""","""True""","""True""","""0""","""0""",,"""7002001""","""[all_
registered_clients]|[Low]""","""2023-06-15 20:50:37""","""2""","""
[Administrator]""","""Policy01""","""2""",,"""True""","""True""","""False""","""False""",
"""False""","""True""","""True""","""True""","""True""","""False""","""False""","""True""
","""True""","""1""","""True""","""1""","""True""","""True""","""True""","""True""","""Tr
ue""","""True""","""True""","""1""","""0""","""0""","""0""","""0""","""0""","""0""","""0"
"","""0""","""1""","""2""","""0.0""","""{'malware': {'id': 2, 'name': 'Profile01'},
'sandbox': {'id': 2, 'name': 'Profile01'}, 'webfilter': {'id': 3, 'name': 'Profile01',
'fp_name': ''}, 'firewall': {'id': 2, 'name': 'Profile01'}, 'vpn': {'id': 2, 'name':
'Profile01'}, 'vulnerability_scan': {'id': 2, 'name': 'Profile01'}, 'system': {'id': 3,
'name': 'Profile01'}, 'ztna': {'id': 2, 'name': 'Profile01'}, 'videofilter': {'id': 2,
'name': 'Profile01'}}""","""{}"""
```


Managing endpoints

You can manage endpoints from the *Endpoints* pane.

Running AV scans on endpoints

You can run a full or quick AV scan on endpoints. Scanning starts on the endpoints with the next FortiClient Telemetry communication.

For the difference between full and quick AV scans, see AntiVirus Protection on page 347.

To run AV scans on endpoints:

1. Go to *Endpoints*.
2. Right-click a domain or workgroup, and select *Start full antivirus scan* or *Start quick antivirus scan*.

To run AV scans on an endpoint:

1. Go to *Endpoints*.
2. Select *All Endpoints*, a domain, or workgroup.
3. Click an endpoint, and from the *Scan* menu, select *Quick AV Scan* or *Full AV Scan*.

Running vulnerability scans on endpoints

You can run a vulnerability scan on endpoints.

To run vulnerability scans on endpoints:

1. Go to *Endpoints*.
2. Right-click a domain or workgroup, and select *Start vulnerability scan*. Vulnerability scanning starts on the endpoints with the next FortiClient Telemetry communication.

To run vulnerability scans on an endpoint:

1. Go to *Endpoints*.
2. Select *All Endpoints*, a domain, or workgroup.
3. Click an endpoint, and from the *Scan* menu, select *Vulnerability Scan*. Vulnerability scanning starts on the endpoint with the next FortiClient Telemetry communication.

Patching vulnerabilities on endpoints

You can request FortiClient patch detected critical and high vulnerabilities on endpoints.

FortiClient can automatically patch many software. However, the endpoint user must manually patch some detected software vulnerabilities. If a vulnerability requires the endpoint user to download and install software to patch a vulnerability, FortiClient displays the information.

To patch vulnerabilities on a domain or group of endpoints:

1. Go to *Endpoints*.
2. Right-click a domain or workgroup, and select *Patch critical/high vulnerabilities*. FortiClient initiates automatic vulnerability patching with the next FortiClient Telemetry communication.

To patch vulnerabilities on an endpoint:

1. Go to *Endpoints*.
2. Select *All Endpoints*, a domain, or workgroup.
3. Click an endpoint, and from the *Patch* menu, select one of the following options:
   - *Selected Vulnerabilities on Selected Clients*
   - *Selected Vulnerabilities on All Affected Clients*
   - *All Critical and High Vulnerabilities*

   FortiClient initiates automatic vulnerability patching with the next FortiClient Telemetry communication.

Uploading FortiClient logs

You can upload a FortiClient log file from one or several endpoints to FortiEndpoint. The log file is uploaded to the hard drive on the computer on which you are running EMS. The uploaded log file is not visible in the FortiEndpoint GUI.

1. Go to *Endpoints*.
2. Select *All Endpoints*, a domain, or workgroup.
3. Click one or multiple endpoints, and from the *Action* menu, select *Upload FortiClient logs*. The `<Endpoint serial number>_<Endpoint hostname>_log` file is uploaded to the following location on your computer: `<drive>\Program Files (x86)\Fortinet\FortiClientEMS\logs`

Running the FortiClient diagnostic tool

You can use EMS to run the FortiClient diagnostic tool on one or multiple endpoints and export the results to the hard drive on the computer on which you are running FortiEndpoint. The exported information is not visible in the FortiEndpoint GUI.

1. Go to *Endpoints*.
2. Select *All Endpoints*, a domain, or workgroup.
3. Click one or multiple endpoints, and from the *Action* menu, select *Request Diagnostic Results*.
   The `<Endpoint serial number>_<Endpoint hostname>_Diagnostic_Result.cab` file is uploaded to the following location on your computer: `<drive>:\Program Files (x86)\Fortinet\FortiClientEMS\logs`.

Updating signatures

You can use EMS to request FortiClient update signatures on the endpoints.

1. Go to *Endpoints*.
2. Select *All Endpoints*, a domain, or workgroup. The list of endpoints displays in the content pane.
3. Click an endpoint, and from the *Action* menu, select *Update Signatures*. FortiClient receives the request to update signatures and downloads the signatures from the Internet.

Downloading available FortiClient logs

To download available FortiClient logs:

1. Go to *Endpoints*.
2. Select *All Endpoints*, a domain, or workgroup. The list of endpoints displays in the content pane.
3. Click an endpoint, and from the *Action* menu, select *Download Available FortiClient Logs*. If you recently requested FortiClient logs, you must wait at least five minutes before you can download them.
4. A confirmation dialog appears. Click *Download*.
5. Browse to the desired directory to download the logs to. Click *Save*. The logs are saved to your selected directory as a .zip file.

Downloading available diagnostic results

To download available diagnostic results:

1. Go to *Endpoints*.
2. Select *All Endpoints*, a domain, or workgroup. The list of endpoints displays in the content pane.
3. Click an endpoint, and from the *Action* menu, select *Download Available Diagnostic Results*. If you recently requested diagnostic results, you must wait at least twenty minutes before you can download them.
4. A confirmation dialog appears. Click *Download*.
5. Browse to the desired directory to download the logs to. Click *Save*. The logs are saved to your selected directory as a .zip file.

Disconnecting and connecting endpoints

You can manually disconnect endpoints using EMS.

To disconnect endpoints:

1. Go to *Endpoints*.
2. Click *All Endpoints*, a domain, or workgroup.
3. Click an endpoint, and from the *Action* menu, select *Deregister*. EMS disconnects the endpoint with the next FortiClient Telemetry communication. After the endpoint is disconnected from EMS, you can reconnect the endpoint to EMS manually.

Quarantining an endpoint

You can quarantine an endpoint using EMS. Quarantined endpoints cannot access the network.

You must enable Application Firewall for this feature to function. See Feature Select on page 555.

If FortiDeceptor integration is enabled, FortiDeceptor may automatically quarantine an endpoint. See FortiDeceptor Campaign on page 374.

To quarantine an endpoint:

1. Go to *Endpoints*.
2. Click *All Endpoints*, a domain, or workgroup. A list of endpoints displays.
3. Click an endpoint, and from the *Action* menu, select *Quarantine*.
   The endpoint status changes to *Quarantined*, and EMS quarantines the endpoint with the next FortiClient Telemetry communication.

   You can remove an endpoint from quarantine by right-clicking the endpoint and selecting *Unquarantine*. EMS removes the endpoint from quarantine with the next FortiClient Telemetry communication and restores network access.

   You can also provide the endpoint user with a one-time access code. The user can enter the code to access FortiClient on a quarantined endpoint, then remove the endpoint from quarantine in FortiClient. The code is available under *Quarantine Access Code* after selecting a quarantined endpoint.

Quarantining an endpoint from FortiOS using EMS

The Fortinet Security Fabric offers endpoint visibility at various monitoring levels. When the Security Fabric includes the following network devices, you can configure the system to automatically quarantine an endpoint on which an Indicator of Compromise (IoC) is detected. This requires the following network components:

- FortiGate
- FortiAnalyzer
- FortiEndpoint
- FortiClient

The following must be true:

- FortiAnalyzer must have both FortiGate and EMS as approved logging devices.
- FortiGate and FortiAnalyzer must have a valid Security Fabric connection.
- FortiGate and EMS must have a valid Security Fabric connection.
- FortiClient must have logging to FortiAnalyzer configured in the assigned endpoint profile.

This process functions as follows:

1. FortiClient sends logs to the FortiAnalyzer.
2. FortiAnalyzer discovers IoCs in the logs and notifies the FortiGate.
3. FortiGate determines if the FortiClient is among its connected endpoints and if it has a Fabric connection to the EMS that the FortiClient is connected to. With this information, FortiGate sends a notification to EMS to quarantine the endpoint.
4. EMS searches for the endpoint and sends a quarantine message to it.
5. The endpoint receives the quarantine message and quarantines itself, blocking all network traffic. The endpoint notifies the FortiGate and EMS of the status change.



FortiClient (Linux) does not support this feature.

Prerequisites

The following lists the prerequisites that must be met for FortiClient, EMS, and the FortiGate.

FortiClient

FortiClient must be installed on the endpoint and connected to EMS as part of a Security Fabric.

EMS

- This feature requires the endpoint protection platform or managed service license.
- You must create a profile for the endpoint. See Creating a new profile on page 131. The profile must:
  - Be configured to log to FortiAnalyzer
  - Include a unified threat management feature, such as *Malware Protection > AntiVirus Protection > Real-Time Protection*
- You must create and configure an endpoint policy that is configured with the desired profile and Telemetry gateway list for the desired endpoint group. See Adding an endpoint policy on page 116.
- Enable *Remote HTTPS access*. See Configuring EMS settings on page 533.

FortiGate

Before automation can be triggered, you must configure the following:

1. Configure an automation trigger.
2. Configure an automation object.
3. Configure an automation stitch.
4. Configure an EMS fabric connector

You may also elect to enable a pre-defined automation stitch instead of completing 1-3 above.

CLI

To create an automation trigger:

```
config system automation-trigger
```

```
   edit "trigger01"
      set trigger-type event-based
      set event-type ioc
   next
end
```

To create an automation action:

```
config system automation-action
   edit "action01"
      set action-type quarantine-forticlient
   next
end
```

To create an automation stitch:

```
config system automation-stitch
   edit "stitch01"
      set status enable
      set trigger "trigger01"
      config actions
         edit 1
            set action “action01”
         next
      end
   next
end
```

GUI

To enable an existing quarantine automation stitch:

1. Go to *Security Fabric > Automation*.
2. Under *Compromised Host*, right-click *Compromised Host Quarantine*, hover over *Set Status*, then select *Enable*.

To create a custom quarantine stitch:

1. Go to *Security Fabric > Automation*.
2. At the top of the page, select *Create New*.
3. Provide a name for the stitch.
4. Click the *Add Trigger* button to select *Compromised Host Quarantine* from the slide in menu, then click *Apply*.
5. Click the *Add Action* button to select *FortiClient Quarantine_quarantine-forticlient* from the slide in menu, then click *Apply*.
6. Click *OK* to save the automation stitch.

To configure EMS Fabric Connector:

1. Go to *Security Fabric > Fabric Connectors*.
2. Click the *FortiClient EMS* tile, then select *Edit*.
3. Enable EMS 1, then provide the EMS name and IP address or domain.
4. Click *OK*.
5. On the *Verify EMS Server Certificate* slide in, review the details and accept the certificate once verified.
6. You may authorize the FortiGate on the EMS using the new slide in menu, or you may do so from the EMS using the popup when you login to the EMS, or by navigating to *Fabric & Connectors > Fabric Devices*.

To verify the configuration:

The following occurs if the configuration has been performed correctly.

1. FortiClient sends logs to FortiAnalyzer. If the FortiClient profile is configured and connectivity is possible, FortiClient will send logs to FortiAnalyzer.



You can generate logs that will be flagged as an IOC by visiting http://195.22.28.198 from the test endpoint.

2. FortiAnalyzer receives the logs from FortiClient and determines there is an IOC
3. FortiAnalyzer notifies the FortiGate using the Fabric Connector
4. FortiGate triggers the automation stitch.
5. You can also review *Security Fabric > Automation > Stitch*, to see the *Trigger Count* for the configured stitch.
6. On the EMS, go to *Endpoints > All Endpoints*, then select the *Quarantined* tile in the top right.
7. Select the endpoint to view more details, such as the status in the top right.
8. The endpoint will also display a quarantine warning from the FortiClient:

Excluding endpoints from management

You can exclude endpoints from management.

To exclude endpoints from management:

1. Right-click a domain or workgroup.
2. Select *Exclude from management*.

To exclude an endpoint from management:

1. Go to *Endpoints*.
2. Click *All Endpoints*, a domain, or workgroup. A list of endpoints displays.
3. Click an endpoint, and from the *Action* menu, select *Exclude from Management*.

Deleting endpoints

You can delete disconnected endpoints from EMS. This option is only available for non-domain devices.

1. Go to *Endpoints*.
2. Click *All Endpoints* or a workgroup. A list of endpoints displays.
3. If the endpoint has a status of *Registered*, disconnect the endpoint.
4. Click an endpoint, and from the *Action* menu, select *Delete Device*.
5. In the dialog, click *Yes*. The endpoint is deleted from FortiEndpoint.

Requesting forensic analysis on an endpoint

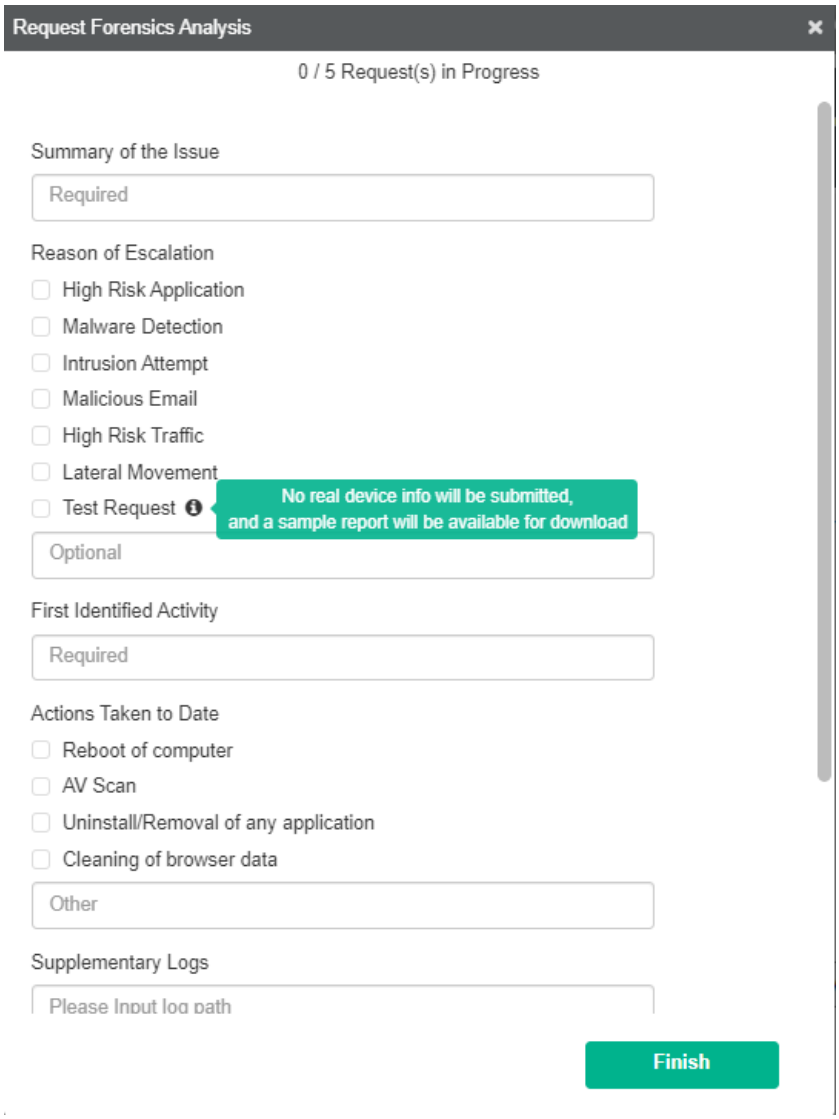
You can request forensic analysis on a suspected device from EMS. The Fortinet forensics team investigates the logs and provides a detailed report with their verdict. You can download the report from EMS.

You can only request forensic analysis for Windows or macOS endpoints. FortiClient (macOS) 7.4.1 and later versions support forensic analysis.

You must apply the Forensics license to EMS to access this feature. The following assumes that you have acquired and applied the license as necessary.

To request forensic analysis for an endpoint:

1. Enable the forensic analysis feature:
   a. In EMS, go to *System Settings > Feature Select*.
   b. Enable *FortiGuard Forensics Analysis*.
   c. Click *Save*.
2. Configure forensic analysis in a profile:
   a. Go to *Endpoint Profiles > System Settings*.
   b. Create a new profile or edit an existing one.
   c. Under *Endpoint Control*, toggle *Enable Forensics Feature* on.
   d. Click *Save*.
   e. Include this profile in a policy, and apply the policy to the desired endpoint.
3. Request analysis:
   a. Go to *Endpoints > All Endpoints*.
   b. Select the desired endpoint.
   c. Under *Forensics Analysis*, click *Request Analysis*.
4. Complete the questionnaire:
   a. In the *Summary of the Issue* field, enter a description of the issue that you are observing on the endpoint.
   b. In the *Reason of Escalation* field, select the reason that you are escalating this issue to the forensics team. If you are submitting a request to test that the forensics feature is functioning correctly on your EMS or FortiClient Cloud instance, select *Test Request*.



c. In the *First Identified Activity* field, enter the date that you first observed the issue.

d. In the *Actions Taken to Date* field, select any actions you took to resolve this issue.

e. In the *Supplementary Logs* field, enter the path to logs that you would like the analyst to review.

f. If desired, provide details in the *Comment* field.

Click *Finish*. Once you submit the request, EMS notifies FortiClient and the forensics agent on the endpoint starts collecting forensics logs. FortiClient uploads the logs to the cloud and shares a link with the analyst. In EMS, you can see status of the analysis request in the endpoint summary:

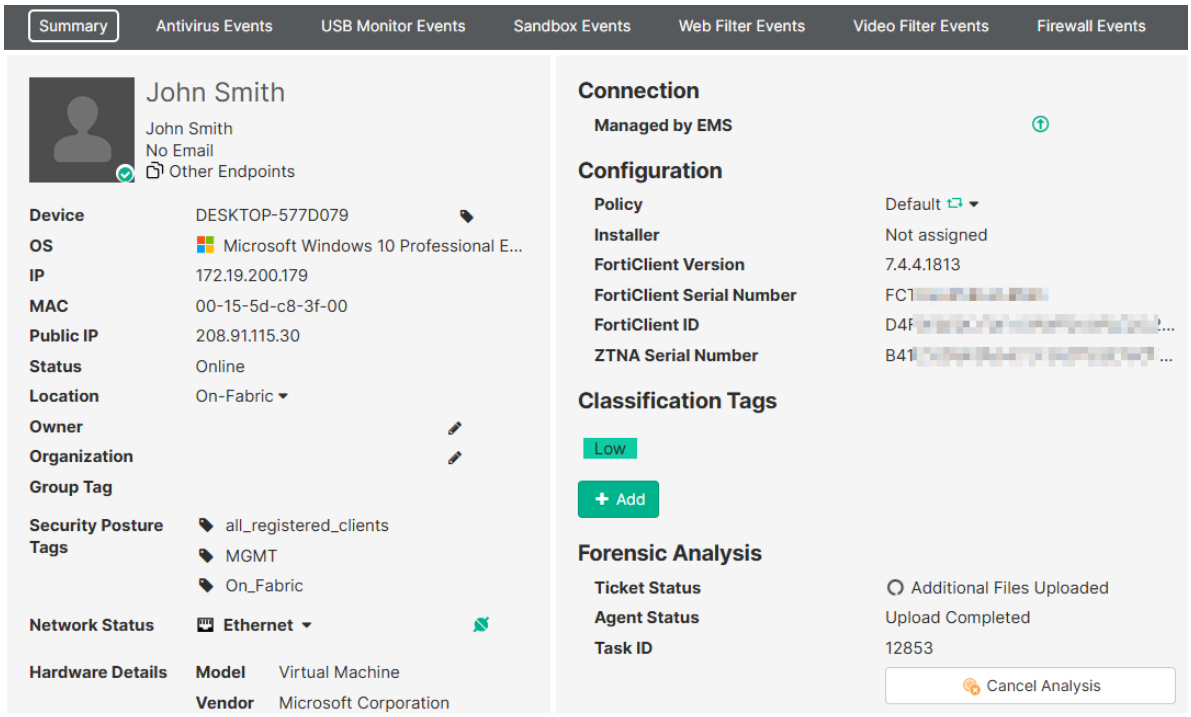
Status	Description
Ticket Status	Status of the ticket. Possible statuses are: • **Request Submitted**: EMS is creating the forensics analysis request and sending the information to the team. • **Pending**: Forensic analysis request has been initiated. The Forensics team has not yet assigned it to an analyst. • **In Progress**: Forensics team has assigned the request to an

Status	Description

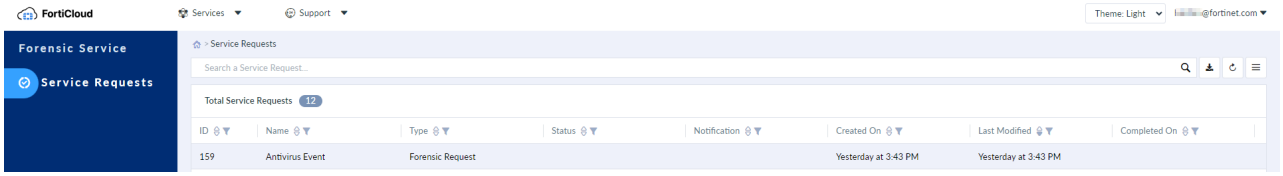
	analyst, who has begun working on it.
	• **Failed**: request is in a failed state. This can be due to a variety of reasons, for example, the analyst may not be able to connect to the endpoint. The analyst may contact you regarding the reason for the failure. See the remaining steps in this procedure for how to contact the analyst.
	• **Cancelled**: indicates one of the following:
	  • The analyst needed more information about the endpoint to perform the analysis.
	  • The EMS administrator canceled the request.
	• **Completed**: analyst has completed analysis on the endpoint and shared the result in a PDF document. You can download the report from the endpoint summary's *Forensic Analysis* section.
	• **Additional Files Requested**: analyst has requested more files from the endpoint via EMS.
	• **Additional Files Uploaded**: FortiClient has uploaded the additional files requested by analyst.

Agent Status	Status of the forensic agent collecting logs on the endpoint. Possible statuses are: • **Pending**: EMS has notified FortiClient that a forensic analysis request is submitted, but the forensic agent is not running yet. • **Running**: forensics agent starts collecting forensics logs. • **Collection Completed**: forensics agent has completed collecting forensics logs. • **Upload Started**: FortiClient has started to upload the logs to the cloud. • **Upload Completed**: FortiClient has completed uploading the logs to the cloud. • **Upload Failed**: FortiClient failed to upload the logs to the cloud. • **Add. Files Unsupported**: FortiClient failed to collect additional files as requested because this feature is unsupported in the current FortiClient version. Consider upgrading FortiClient to 7.4.4 or later so analyst can collect additional files.
Task ID	Request ID in the FortiGuard forensics system.

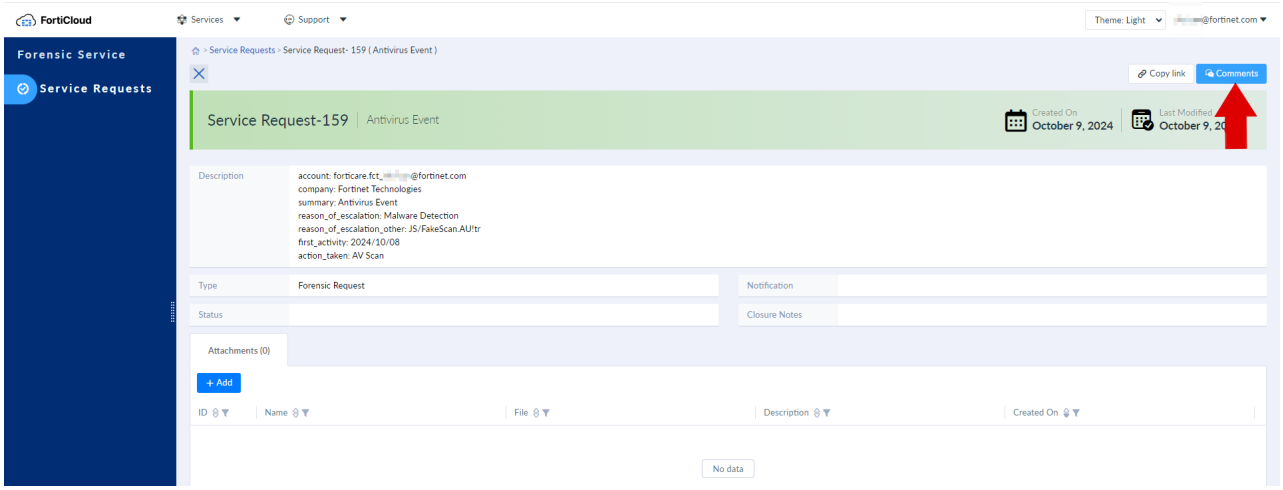
5. The forensic analyst verifies the files attached to your ticket. If they require additional files for analysis, they will request more and the *Ticket Status* changes to *Additional Files Requested* in EMS. The status may take up to an hour to update after the analyst submits the request on their end. Once EMS receives the request, it uses the forensics agent to collect the requested files and submits them to the analysis service. The *Ticket Status* updates to *Additional Files Uploaded*.



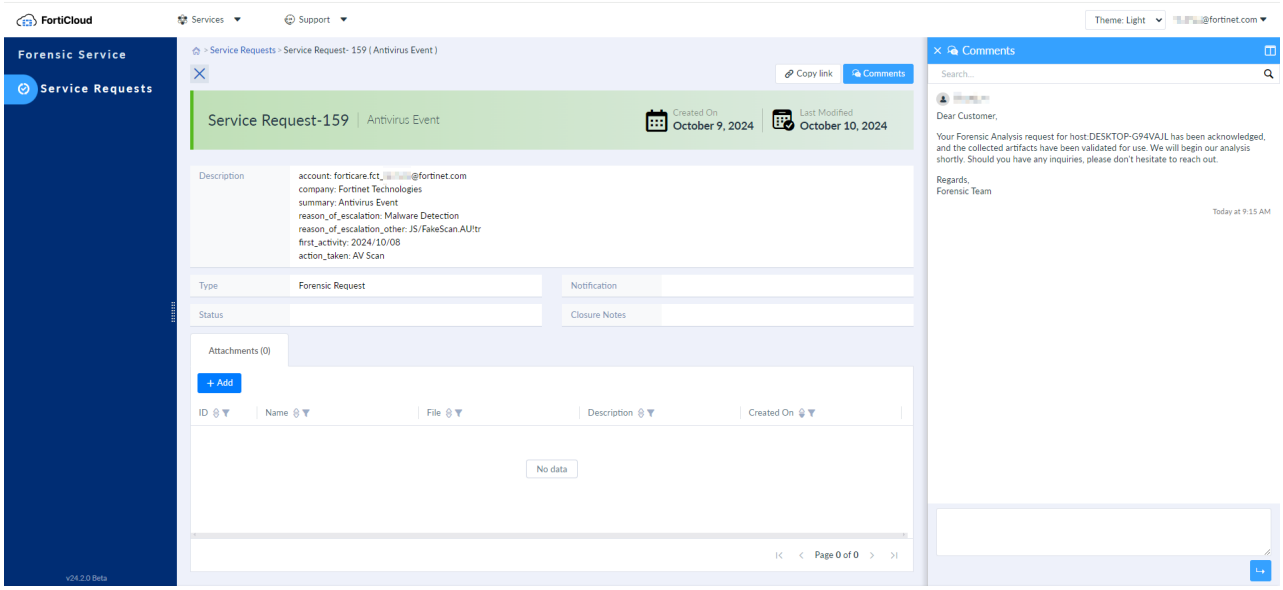
6. Do one of the following:
   - Log in to the Forensic Service portal using your FortiCloud credentials.
   - If using FortiClient Cloud, go to the *Forensics Analysis* tab on the left, then click the link to the Forensics Service portal. The link may not be available if the analyst has not created a service request for your analysis request.
7. The *Service Requests* dashboard shows your service requests. Select the current request, in this example, *Antivirus Event*.



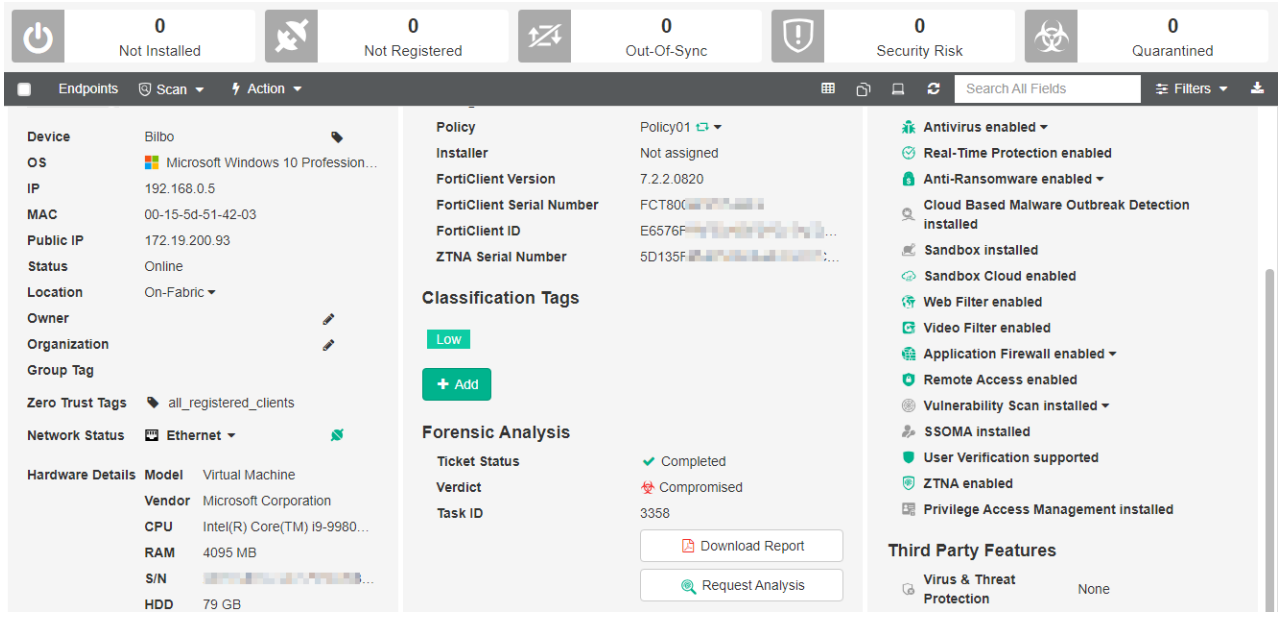
8. The service request page displays information about your request. Click *Comments* in the upper right corner.



9. The *Comments* pane displays messages from the Fortinet forensics team. You can also send the team messages to clarify details of your request. While your forensics analysis request is in progress, ensure that you monitor panel to provide the team details of your request as needed. You will also receive an email when the forensics team sends a message via this *Comments* pane.



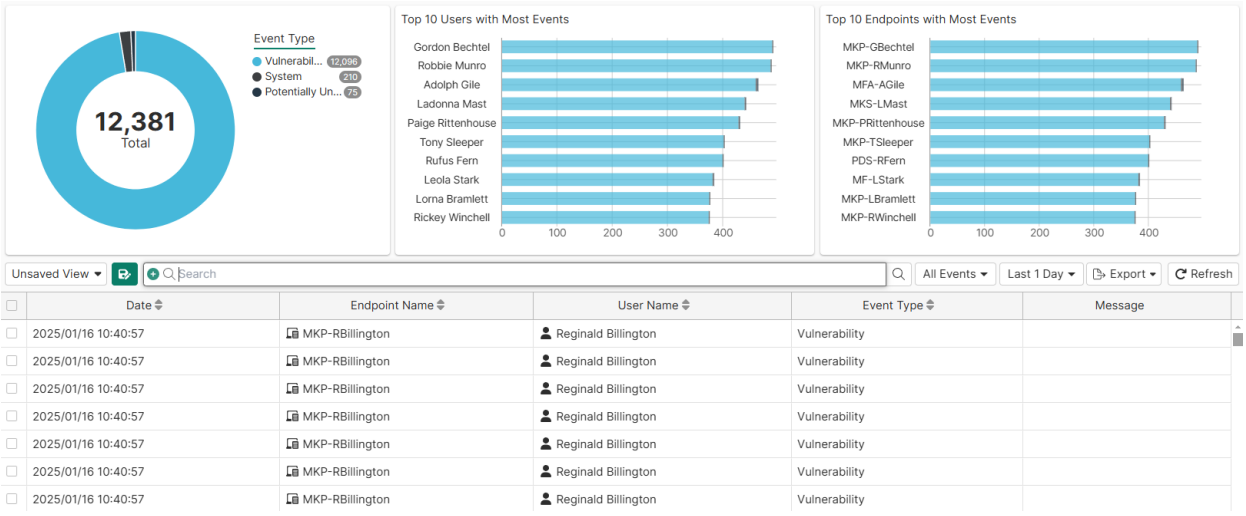
10. Once the analysis is complete, you can click *Download Report* in the endpoint summary to view the details. You can also view the verdict that the analyst arrived at. You can also filter the endpoint list based on whether the forensics service is enabled, the status, and verdict.


0
Not Installed
0
Not Registered
0
Out-Of-Sync
0
Security Risk
0
Quarantined
Endpoints
Scan
Action
Search All Fields
Filters
Device
Bilbo
OS
Microsoft Windows 10 Profession...
IP
192.168.0.5
MAC
00-15-5d-51-42-03
Public IP
172.19.200.93
Status
Online
Location
On-Fabric
Owner
Organization
Group Tag
Zero Trust Tags
all_registered_clients
Network Status
Ethernet
Hardware Details
Model
Virtual Machine
Vendor
Microsoft Corporation
CPU
Intel(R) Core(TM) i9-9980...
RAM
4095 MB
S/N
HDD
79 GB
Policy
Policy01
Installer
Not assigned
FortiClient Version
7.2.2.0820
FortiClient Serial Number
FortiClient ID
ZTNA Serial Number
Classification Tags
Low
Add
Forensic Analysis
Ticket Status
Completed
Verdict
Compromised
Task ID
3358
Download Report
Request Analysis
Antivirus enabled
Real-Time Protection enabled
Anti-Ransomware enabled
Cloud Based Malware Outbreak Detection installed
Sandbox installed
Sandbox Cloud enabled
Web Filter enabled
Video Filter enabled
Application Firewall enabled
Remote Access enabled
Vulnerability Scan installed
SSOMA installed
User Verification supported
ZTNA enabled
Privilege Access Management installed
Third Party Features
Virus & Threat Protection
None

All Events

There is an *Endpoints* > *All Events* page available where you can view all events from all endpoints and take actions as necessary.

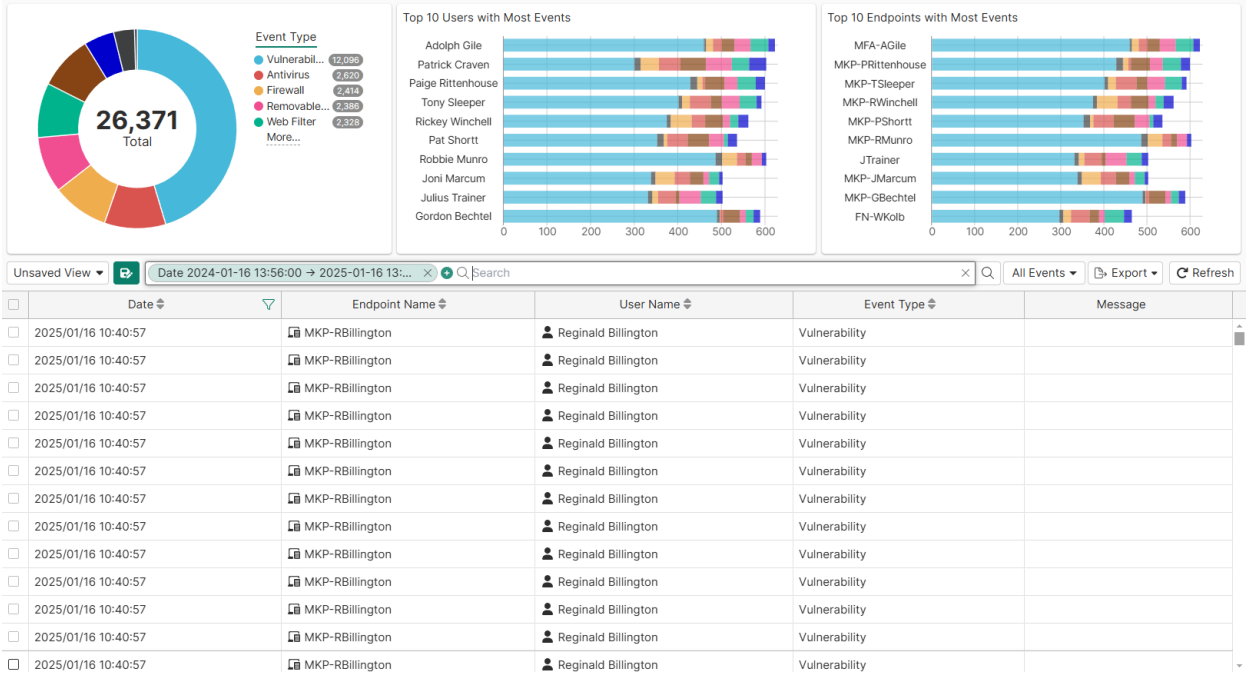
For Web Filter on page 320 events, only events of the *Block* and *Warn* categories are displayed here. Events of the *Allow* and *Monitor* categories are not displayed.



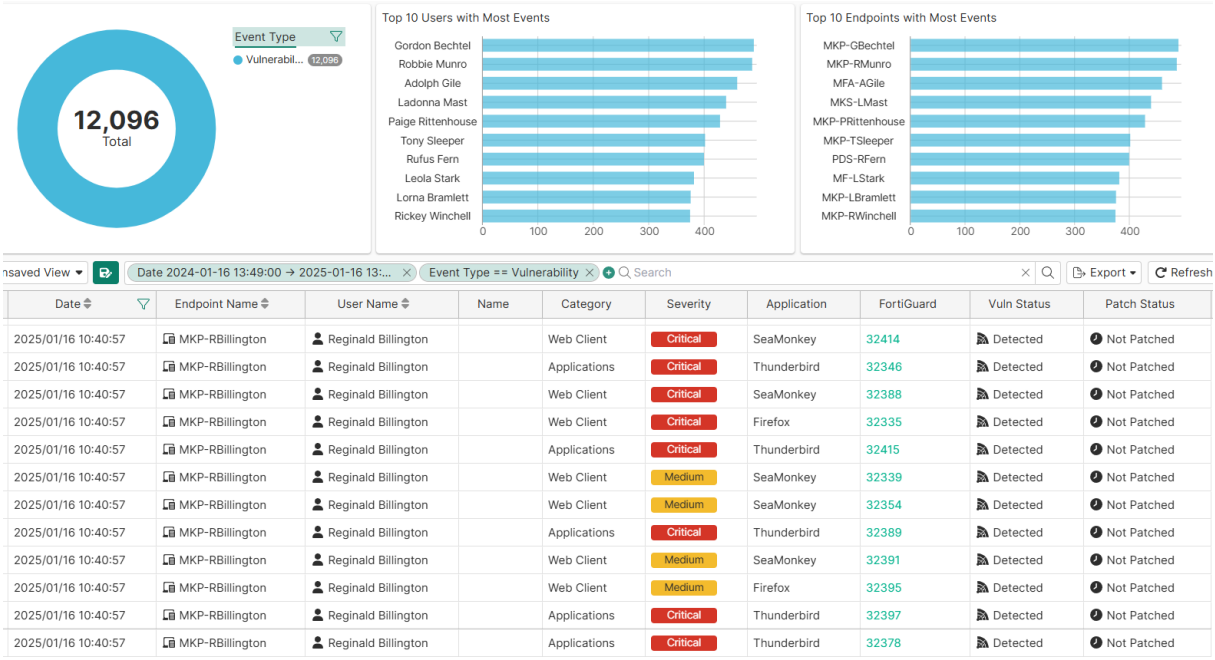
The top of the page contains the following charts:

Chart	Description
Event Type	Donut chart that shows the ratio of events by type, the total number of events, and total number of each event type. You can click into a chart section to filter only for the selected event type.
Top 10 Users with Most Events	Bar chart that displays the endpoint users with the most endpoint events.
Top 10 Endpoints with Most Events	Bar chart that displays the endpoints with the most events.

The bottom of the page displays the endpoint event list. You can filter the list by the columns. For example, you can filter the list for a specific start and end date to only view events that occurred during that time range.



Clicking a donut chart section filters the endpoint list by that event type. The following shows only endpoint Vulnerability events for the selected time range:



You can also select the desired event type from the *All Events* dropdown menu on the right.

You can create, update, or delete an event view. An event view is a saved combination of filters for the endpoint event list. When you save a view, you can simply select it later instead of reconfiguring the desired filters.

To create an event view:

1. In *Endpoints* > *All Events*, configure the desired filters.
2. Beside *Unsaved View*, click the save icon.
3. In the *Create View* pane, for *Action*, select *Create View*.
4. Configure other fields as desired, then click *OK*.

To export an event list:

1. In *Endpoints* > *All Events*, in the upper right corner, click *Export*.
2. Select *CSV* or *JSON*.
3. Export the file as desired.

When you select events in the event list, you can use the *Actions* dropdown list to apply actions to the endpoints with the selected events. For descriptions of these actions, see Viewing the Endpoints pane on page 57.

Index lifecycle

EMS enforces index lifecycle management (ILM) policies. EMS associates each index with a lifecycle policy to optimize data retention and storage performance:

Data age	Phase	Description
Up to 45 days	Hot	Data is actively indexed and queried. Index rolls over after 45 days or 50 GB, whichever is reached first.
Between 45 to 120 days	Warm	Data is still available to be queried but moved to less resource-intensive storage.
More than 120 days	Cold	Data is deleted automatically.

EMS assigns each index a specific ILM policy:

Index	Lifecycle policy
forticlientems_alerts-745-000001	forticlientems_alerts-policy
forticlientems_pua-745-000001	forticlientems_pua-policy
forticlientems_sysevs-745-000001	forticlientems_sysevs-policy
forticlientems_vulns-745-000001	forticlientems_vulns-policy

EMS is limited to querying data for up to 30 days from the used indexes but internally uses data of up to 45 days to determine status changes.

Group assignment rules

You can use group assignment rules to automatically place endpoints into custom groups.

EMS does not apply group assignment rules to a domain-joined endpoint if it belongs to an imported Active Directory (AD) domain in EMS. The endpoint stays in the organization unit to which it belongs in the AD domain tree, even if it matches a group assignment rule.

Group assignment rules only apply for endpoint in workgroups. EMS automatically places endpoints that do not apply for any group assignment rule into the *Other Endpoints* group.

Group assignment rule types

You can use group assignment rules to automatically place endpoints into custom groups based on certain traits.

Installer ID group assignment rules

Creating a FortiClient deployment package includes an option to specify an installer ID. For example, you may want to place all endpoints located in your company's headquarters in the same endpoint group. You can configure a FortiClient deployment package with an "HQ" installer ID, then deploy this deployment package to the desired endpoints. When the endpoints' FortiClient connects to FortiEndpoint, FortiEndpoint places them in the desired group. In this situation, the process is as follows:

1. In FortiEndpoint, create an installer ID group assignment rule that requires EMS to place endpoints with the installer ID "HQ" into the HQ group. The installer ID and group name do not need to match. See Adding a group assignment rule on page 94.
2. Create a FortiClient deployment package. Specify the "HQ" installer ID when creating or uploading the installer. See Adding a FortiClient installer on page 106.
3. Deploy the deployment package to the desired endpoints or send the download link to the desired users.
4. The endpoints install FortiClient. When FortiClient connects to FortiEndpoint, EMS places the endpoint in the HQ group.

If you manually move the endpoint to another group after EMS places it into the group defined by the installer ID group assignment rule, EMS returns the endpoint to the group defined by the installer ID group assignment rule.

IP address group assignment rules

You can create a group assignment rule to automatically place all endpoints within a specified subnet or IP address range into the same custom group. In this situation, the process is as follows:

1. In FortiEndpoint, create an IP address group assignment rule that requires endpoints within a certain subnet or IP address range to be placed into the desired group. See Adding a group assignment rule on page 94.
2. With the next FortiClient Telemetry communication, endpoints within the specified subnet or IP address range are placed in the specified group.

OS group assignment rules

You can create a group assignment rule to automatically place all endpoints that have a specific OS installed into the same custom group. In this situation, the process is as follows:

1. In FortiEndpoint, create an OS group assignment rule that requires endpoints with a certain OS installed to be placed into the desired group. See Adding a group assignment rule on page 94.
2. With the next FortiClient Telemetry communication, endpoints with the specified OS installed are placed in the specified group.

Invitation group assignment rules

You can create a group assignment rule to automatically place all endpoints that connected to EMS using a specific invitation code into the same custom group. In this situation, the process is as follows:

1. In FortiEndpoint, create an invitation group assignment rule that requires endpoints that connected to EMS using a specific invitation code to be placed into the desired group. See Adding a group assignment rule on page 94.
2. With the next FortiClient Telemetry communication, endpoints with the specified invitation code are placed in the specified group.

Managing group assignment rule priority levels

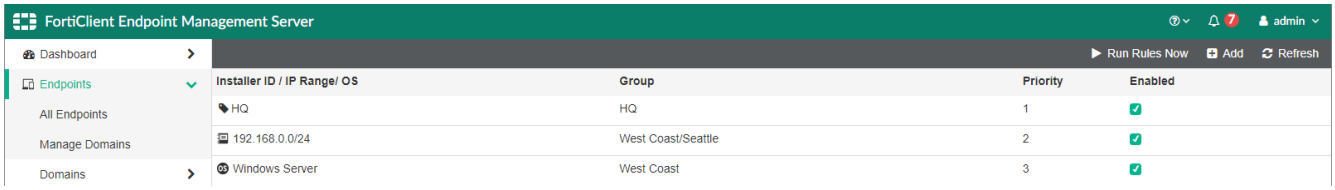
An endpoint may be eligible for multiple group assignment rules. When an endpoint is eligible for multiple endpoint group assignment rules, two factors determine which rule EMS applies to the endpoint:

1. EMS applies group assignment rules to endpoints only if the rules are enabled on the *Endpoints > Group Assignment Rules* page.
2. If an endpoint is eligible for multiple enabled rules, the EMS applies the rule with the first priority level to the endpoint.

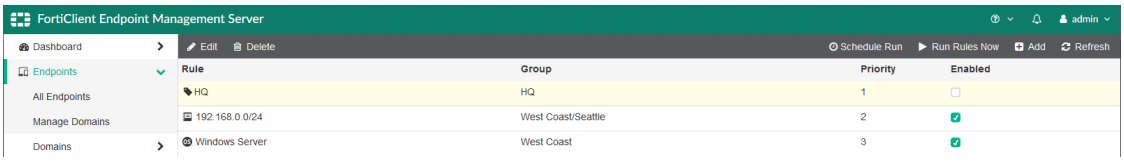
To change rule priority levels:

1. Go to *Endpoints > Group Assignment Rules*.
2. Click and hold the rule, then drag to the desired position.

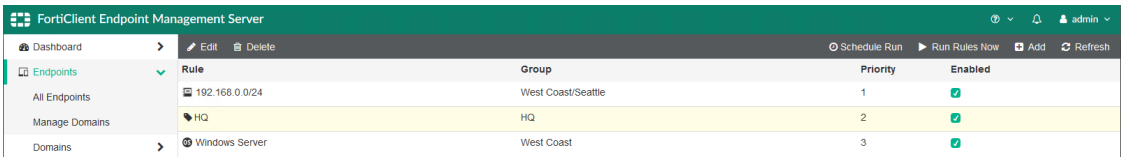
In the example, consider an endpoint where FortiClient was deployed using the "HQ" installer ID and has an IP address that belongs to the 192.168.0.0/24 subnet. The endpoint applies for two rules. In this case, the endpoint is placed in the HQ group, since the HQ rule has a higher priority level than the 192.168.0.0/24 subnet rule.



However, if you disable the HQ rule, EMS places the endpoint in the West Coast/Seattle group, as per the 192.168.0.0/24 subnet rule.



You can reenable the HQ rule, then change the rule priority levels sot hat the 192.168.0.0/24 rule has priority level 1. In this case, EMS places the endpoint in the West Coast/Seattle group.



Adding a group assignment rule

To add an installer ID group assignment rule:

An installer ID group assignment rule automatically places endpoints with the specified installer ID into the specified endpoint group.

1. Go to *Endpoints* > *Group Assignment Rules*.
2. Click *Create new*.
3. From the *Type* dropdown list, select *Installer ID*.
4. In the *Installer ID* field, enter the desired installer ID.
5. In the *Group* field, do one of the following:
   - To place the endpoints into an existing group, enable *Use existing groups*, then select the desired group from the dropdown list.
   - To place the endpoints into a new group, disable *Use existing groups*. In the *Group* field, enter the desired group name. FortiEndpoint creates the new group. To create a new nested group, enter the desired group hierarchy. For example, to create a *Seattle* group nested under a *West Coast* group, enter *West Coast/Seattle*. FortiEndpoint then dynamically creates any group that does not exist. For example, if both the *West Coast* and *Seattle* groups do not exist, FortiEndpoint creates both groups with the desired hierarchy. If the *West Coast* group exists, FortiEndpoint creates a new *Seattle* group nested under it.
6. Enable or disable the rule by toggling *Enable Rule* on or off.
7. Click *OK*.

To add an IP address group assignment rule:

An IP address group assignment rule automatically places all endpoints with an IP address in the specified subnet or IP address range into the specified endpoint group.

1. Go to *Endpoints* > *Group Assignment Rules*.
2. Click *Add*.
3. Under *Type*, select *IP Address*.
4. In the *Subnet/IP Range* field, enter the desired subnet or IP address range. You must enter an IPv4 range, such as 192.168.1.1-192.168.1.5, or an IPv4 subnet with subnet mask, such as 192.168.0.0/28.

You cannot enter an IPv6 range or subnet. EMS automatically places endpoints whose IP addresses belong to the specified subnet or IP address range into the specified group.

5. In the *Group* field, do one of the following:
   - To place the endpoints into an existing group, enable *Use existing groups*, then select the desired group from the dropdown list.
   - To place the endpoints into a new group, disable *Use existing groups*. In the *Group* field, enter the desired group name. FortiEndpoint creates the new group. To create a new nested group, enter the desired group hierarchy. For example, to create a *Seattle* group nested under a *West Coast* group, enter *West Coast/Seattle*. FortiEndpoint then dynamically creates any group that does not exist. For example, if both the *West Coast* and *Seattle* groups do not exist, FortiEndpoint creates both groups with the desired hierarchy. If the *West Coast* group exists, FortiEndpoint creates a new *Seattle* group nested under it.
6. Enable or disable the rule by toggling *Enable Rule* on or off.
7. Click *Save*.

To add an OS group assignment rule:

An OS group assignment rule automatically places all endpoints with the specified OS installed into the specified endpoint group.

1. Go to *Endpoints > Group Assignment Rules*.
2. Click *Add*.
3. Under *Type*, select *OS*.
4. In the *OS* field, enter the OS. EMS automatically places endpoints that have the specified OS installed into the specified group. You can enter only the OS name or specify a version number. For example, you can enter "Windows" to place endpoints with any version of Windows installed into the specified endpoint group. You can also specify "Windows Server 2019" to only place endpoints that have Windows Server 2019 installed into the specified endpoint group.
5. In the *Group* field, do one of the following:
   - To place the endpoints into an existing group, enable *Use existing groups*, then select the desired group from the dropdown list.
   - To place the endpoints into a new group, disable *Use existing groups*. In the *Group* field, enter the desired group name. FortiEndpoint creates the new group. To create a new nested group, enter the desired group hierarchy. For example, to create a *Seattle* group nested under a *West Coast* group, enter *West Coast/Seattle*. FortiEndpoint then dynamically creates any group that does not exist. For example, if both the *West Coast* and *Seattle* groups do not exist, FortiEndpoint creates both groups with the desired hierarchy. If the *West Coast* group exists, FortiEndpoint creates a new *Seattle* group nested under it.
6. Enable or disable the rule by toggling *Enable Rule* on or off.
7. Click *Save*.

To add an invitation group assignment rule:

An invitation group assignment rule automatically places all endpoints that connected to EMS using the specified invitation code into the specified endpoint group.

1. Go to *Endpoints > Group Assignment Rules*.
2. Click *Add*.
3. Under *Type*, select *Invitation*.

4. From the *Invitation* dropdown list, select the desired invitation. You must have previously configured invitations for this option to be available. See Invitations on page 503. EMS automatically places endpoints that connected to EMS using that invitation code into the specified group.
5. In the *Group* field, do one of the following:
   - To place the endpoints into an existing group, enable *Use existing groups*, then select the desired group from the dropdown list.
   - To place the endpoints into a new group, disable *Use existing groups*. In the *Group* field, enter the desired group name. FortiEndpoint creates the new group. To create a new nested group, enter the desired group hierarchy. For example, to create a *Seattle* group nested under a *West Coast* group, enter *West Coast/Seattle*. FortiEndpoint then dynamically creates any group that does not exist. For example, if both the *West Coast* and *Seattle* groups do not exist, FortiEndpoint creates both groups with the desired hierarchy. If the *West Coast* group exists, FortiEndpoint creates a new *Seattle* group nested under it.
6. Enable or disable the rule by toggling *Enable Rule* on or off.
7. Click *Save*.

Enabling/disabling a group assignment rule

To enable/disable a group assignment rule:

1. Go to *Endpoints* > *Group Assignment Rules*.
2. Select or deselect the *Enabled* checkbox for the desired group assignment rule.

Deleting a group assignment rule

To delete a group assignment rule:

1. Go to *Endpoints* > *Group Assignment Rules*.
2. Click the desired group assignment rule.
3. Click *Delete*.
4. In the confirmation dialog, click *Yes*.

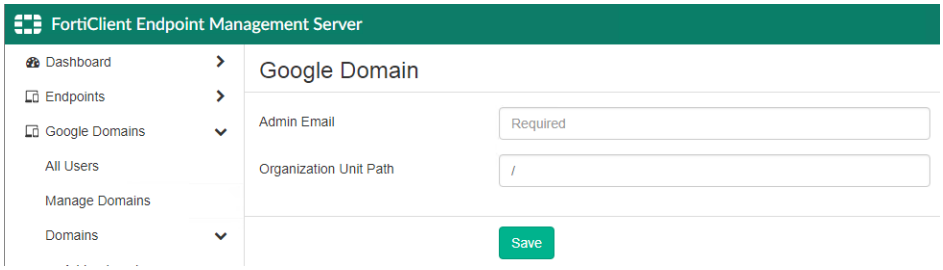
Google Domains

FortiEndpoint needs to determine which Chromebooks to manage. Device information comes from the Google Admin console. *Google Domains* is only available if you enabled *System Settings* > *EMS Settings* > *EMS for Chromebooks Settings*. This section only applies if you are using FortiEndpoint to manage Google Chromebooks.

Adding a Google domain

To add a Google domain:

1. Go to *Google Domains* > *Manage Domains*, and click the *Add* button. The *Google Domain* pane displays.



2. In the *Admin Email* field, enter your Google domain admin email.
3. In the *Organization Unit Path* field, enter the domain organization unit path.

> / stands for the root of the domain.

4. Click *Save*. EMS imports the Google domain information and users.

Viewing domains

Viewing domains

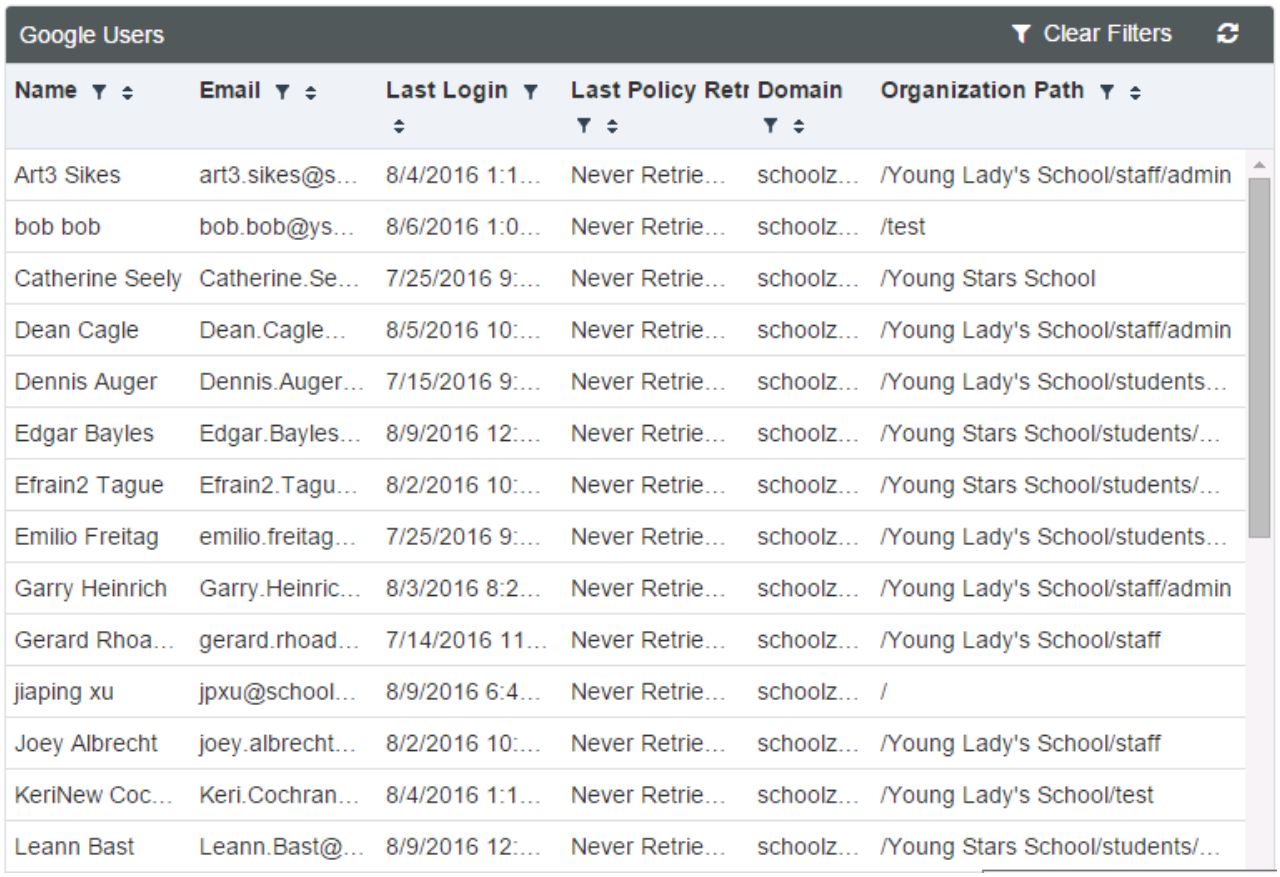
After you add domains to FortiEndpoint, you can view the list of domains in *Google Domains*. You can also view the list of Google users in each domain and details about each Google user in the *User Details*, *Client Statistics*, and *Blocked Sites* panes.

Viewing the Google Users pane

To view the Google Users pane:

You can view Google user information in FortiEndpoint.

1. Go to *Google Domains* > *Domains* and click a domain. The list of Google users displays.



The following options are available in the toolbar:

Clear Filters	Clear the currently used filter(s).
Refresh	Refresh the page.

The following columns of information display for Google users:

Name	Chromebook user's name.
Email	Chromebook user's email address.
Last Login	Date and time the user last logged into the domain.
Last Policy Retrieval	Date and time that the Google Chromebook last retrieved the endpoint profile.
Domain	Name of the domain to which the user belongs.
Organization Path	Organization path in the domain.

Viewing user details

You can view details about each user in a Google domain.

To view user details:

1. Go to *Google Domains* > *Domains*. The list of domains displays.
2. Click a domain. The list of Google users displays.
3. Click a Google user and scroll to the bottom of the content pane. The *User Details*, *Client Statistics*, and *Blocked Sites* panes display.

User Details

Field	Information
Name	Username.
Email	User's email address.
Last Login	Date and time the user last logged into the domain.
Last Policy Retrieval	Date and time that the Google Chromebook last retrieved the endpoint profile.
Organization Path	Organization path of the user in the domain.
Effective Policy	Name of the Chromebook policy assigned to the user in the domain.

Client Statistics

Charts	Information
Blocked Sites Distribution (past <number> days)	Displays the distribution of blocked sites in the past number of days. You can configure the number of days for which to display information. Go to *System Settings* > *Logs*.
Top 10 Site Categories by Distribution (Past <number> Days)	Displays the distribution of top ten site categories in the past number of days. You can configure the number of days for which to display information. Go to *System Settings* > *Logs*.

Blocked Sites (Past <number> Days)

Fields	Information
Time	Time that the user visited the blocked site.
Threat	Threat type that FortiClient detected.
Client Version	Chromebook user's current version.
OS	Type of OS that the Chromebook user used.
URL	Blocked site's URL.
Port	Port number currently listening.
User Initiated	Whether the user initiated visitation to the blocked site.

Editing a domain

To edit a domain:

1. Go to *Google Domains* > *Domains* and select a domain.
2. Click the *Edit* button.
3. Edit the options and click *Save Changes*.

Deleting a domain

To delete a domain:

1. Go to *Google Domains* > *Domains*, and select a domain.
2. Click the *Delete* button. A confirmation dialog displays.
3. Click *Yes*.

Deployment & Installers

You can use FortiEndpoint to deploy FortiClient upgrades on endpoints that already have FortiClient installed.

The following sections do not describe how to initially deploy FortiClient to endpoints. See Installing FortiEndpoint on endpoints on page 10.

Manage Deployment

Creating a deployment configuration



EMS may not deploy certain FortiClient versions to the selected endpoints.

EMS can download a signature, the *EMS/FCT upgrade & compatibility matrix* signature, from FortiGuard. This signature provides operating system support information for FortiClient versions. EMS uses this information and only pushes deployment to endpoints with an OS that supports the FortiClient version deployed.

For example, consider that you have an endpoint running Windows 7, which FortiClient 7.4.4 does not support. If your EMS has the EMS/FCT upgrade & compatibility matrix and you create a deployment configuration to deploy FortiClient 7.4.4 to the endpoint, EMS does not deploy FortiClient 7.4.4 to that endpoint.

To create a deployment configuration:

1. Go to *Deployment & Installers* > *Manage Deployment*.
2. Click *Add*.
3. Configure the fields as desired:

Field	Description
Name	Required. Enter the desired name.
Endpoint Groups	Optional. Select the desired endpoint group. The list includes device groups for all imported domains and workgroups. If you are selecting a security group from a Microsoft Entra ID server, it must include a device object. If you are selecting a security group from an Active Directory server, it must include a computer object. If you select a security group that only has user objects as members, EMS does not assign the installer to the users.
Action	Select *Install* or *Uninstall*.

Field	Description
	When EMS pushes an uninstall to FortiClient (macOS), the uninstall does not remove FortiClient system extensions from the device. A user can run the uninstaller manually to remove system extensions as part of the uninstall.
Deployment Package	Select the desired deployment package from the dropdown list.
Start at a Scheduled Time	If this feature is enabled, FortiClient displays a notification to users that there is a newer FortiClient version that they are expected to upgrade to. The time that you specify in this field displays to users as the default scheduled time for the installation to take place. The notification also allows users to configure a custom install time or to install the update immediately. If this feature is disabled, the FortiClient installation starts immediately without user interaction.
Unattended Installation	When enabled, the end user cannot modify the installation schedule. If needed, the device reboots without warning logged-in users.
Reboot When Needed	Reboot the endpoint to install FortiClient when needed. This option is supported on FortiClient Windows 7.2.0-7.2.5 and 7.4.0 only.
Reboot When No Users Are Logged In	Allow the endpoint to reboot without prompt if no endpoint user is logged into FortiClient.
Notify Users and Let Them Decide When To Reboot When Users Are Logged In	Notify the end user if a reboot of the endpoint is needed and allow the user to decide what time to reboot the endpoint. Disable to reboot the endpoint without notifying the user. This option is supported on FortiClient Windows 7.2.0-7.2.5 and 7.4.0 only.
Priority	The default priority for a new deployment configuration is the lowest priority. You cannot edit the priority while creating the deployment configuration. You can edit change the priority level after creating the deployment configuration. See Managing deployment configuration priority levels on page 102.
Enable the Deployment	Enable or disable.

4. Click *Save*.

Managing deployment configuration priority levels

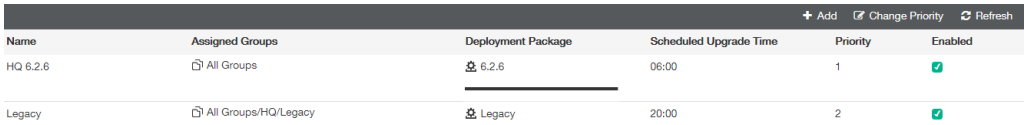
An endpoint may be eligible for multiple deployment configurations. When an endpoint is eligible for multiple endpoint deployment configurations, the following factors determine which configuration EMS applies to the endpoint:

1. EMS applies deployment configurations to endpoints only if the configurations are enabled on the *Deployment & Installers > Manage Deployment* page.
2. If an endpoint is eligible for multiple enabled configurations, EMS applies the configuration with the first priority level to the endpoint.

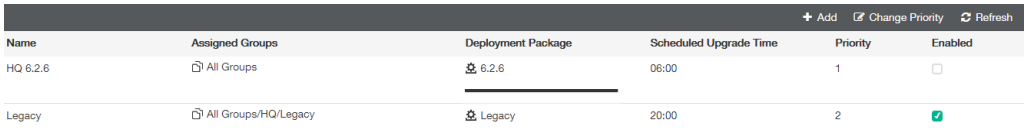
To change configuration priority levels in the GUI:

1. Go to *Deployment & Installers* > *Manage Deployment*.
2. Click *Change Priority*.
3. Click and hold the configuration, then drag to the desired position.
4. Click *Save Priority*.

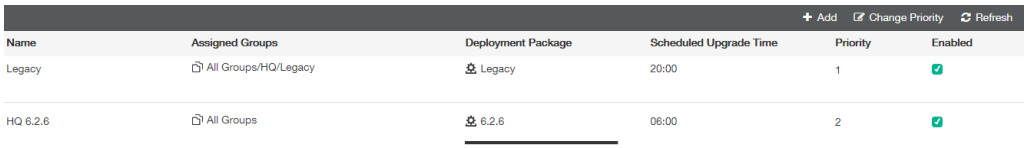
In the example, consider an endpoint that belongs to the Legacy group. The endpoint applies for two configurations. In this case, EMS applies the HQ deployment configuration to the endpoint, since the HQ configuration has a higher priority level than the Legacy configuration.



However, if you disable the HQ configuration, EMS applies the Legacy deployment configuration to the endpoint in the Legacy group.



You can reenable the HQ rule, then change the configuration priority levels so that the Legacy configuration has priority level 1. In this case, EMS applies the Legacy configuration to the endpoint.



To change configuration priority levels via a text file:

1. Go to *Deployment & Installers* > *Manage Deployment*.
2. Click *Change Priority*.
3. Click *Bulk Policy Order Update*. This option is only available if you have multiple deployment configurations configured.
4. Click *Export*.
5. Open the downloaded text file. The file lists the deployment configurations in their configured priority levels. Edit the order as desired and save.
6. Click *Next*.
7. Browse to and import the updated text file. The priority levels update in EMS.

Enabling or disabling a deployment configuration

To enable or disable a deployment configuration:

1. Go to *Deployment & Installers* > *Manage Deployment*.
2. Select or deselect *Enabled* for the desired deployment configuration.

Deleting a deployment configuration

To delete a deployment configuration:

1. Go to *Deployment & Installers* > *Manage Deployment*.
2. Click the desired configuration.
3. Click *Delete*.
4. In the confirmation dialog, click *Yes*.

Deploying FortiClient upgrades from FortiEndpoint

You can deploy a FortiClient software update from FortiEndpoint. A prompt appears on the FortiClient endpoint when a deployment package requests deployment. The prompt requests the user to do one of the following.

For the following options, if there are driver version changes due to the upgrade, the upgrade process also automatically reboots your computer. Otherwise, a reboot does not occur.

Prompt option	Description
Suggested install time	The dialog displays the time that you configured in *Start at a Scheduled Time* when you created the deployment configuration. See Creating a deployment configuration on page 101. If selected, FortiClient performs the upgrade at this time.
Select a time	Indicate the time to start the upgrade. The default is the same as the suggested install time.
Install now	Perform the upgrade now.
No option	If the user does not select an option, the upgrade occurs by default at the suggested install time. After the previous version is uninstalled, it asks if the user wants to reboot. The prompt requests the user to do one of the following: • *Reboot*: have the reboot occur immediately. • *Reboot later*: reboot the computer later. You cannot select a specific reboot time. Use this option at your discretion.



As initially installing FortiClient usually requires administrator privileges on the endpoint, upgrades does not require any additional privilege changes. See the following:

- Microsoft Windows
- macOS
- Linux

EMS may not deploy certain FortiClient versions to the selected endpoints.

EMS can download a signature, the *EMS/FCT upgrade & compatibility matrix* signature, from FortiGuard. This signature provides operating system support information for FortiClient versions. EMS uses this information and only pushes deployment to endpoints with an OS that supports the FortiClient version deployed.

For example, consider that you have an endpoint running Windows 7, which FortiClient 7.4.4 does not support. If your EMS has the EMS/FCT upgrade & compatibility matrix and you create a deployment configuration to deploy FortiClient 7.4.4 to the endpoint, EMS does not deploy FortiClient 7.4.4 to that endpoint.

Deploying different installer IDs to endpoints using the same deployment package

As Installer ID group assignment rules on page 92 describes, you can include an installer ID in a FortiClient deployment package. After FortiClient installation, the endpoint connects to EMS and EMS groups the endpoint according to the installer ID group assignment rule. You can configure one installer ID for each deployment package.

In an environment with a large number of endpoints, you may have dozens of installer IDs that you want to use to group endpoints automatically in EMS after installation. Since you can configure each deployment package with only one installer ID, it may be inefficient to create a deployment package for each installer ID.

Instead, you can create a deployment package without an installer ID in EMS, then install FortiClient on the endpoint using the CLI, providing the installer ID as one of the CLI options. You can use the same deployment package on multiple endpoints, providing different installer IDs in the CLI depending on which group you want EMS to place the endpoint in. When these endpoints connect to EMS, EMS groups them according to the installer ID provided in the CLI.

This process consists of the following:

1. Create a deployment package in EMS. Do not configure an installer ID. See Adding a FortiClient installer on page 106.
2. Create installer ID group assignment rules to automatically move endpoints into the desired groups. See To add an installer ID group assignment rule: on page 94.
3. Install FortiClient on endpoints using the following CLI commands:

Installer	CLI command

.msi	`msiexec /i forticlient.msi GROUP_TAG="<installer_ID>"`
	If the .msi file name includes a space, you must also enclose it in quotes. For example, if the .msi file name is "FortiClient Setup.msi", the command is as follows:
	`msiexec /i "FortiClient Setup.msi" GROUP_TAG="<installer_ID>"`

.exe	`FortiClientSetup_26.1.b_x64.exe /v"GROUP_TAG=<installer_ID>"`

For example, consider that you want to deploy the same deployment package but different installer IDs for the HR, Marketing, and Office Management teams at your organization. In this scenario, you would use EMS to create an deployment package without an installer ID and an installer ID group assignment rule for

each endpoint group. Then, you can install FortiClient on the HR, Marketing, and Office Management endpoints using the same deployment package and the following CLI commands, respectively:

```
FortiClientSetup_26.1.b_x64.exe /v"GROUP_TAG=HR"
FortiClientSetup_26.1.b_x64.exe /v"GROUP_TAG=Marketing"
FortiClientSetup_26.1.b_x64.exe /v"GROUP_TAG=OM"
```

After the endpoints connect to EMS, EMS automatically places them into groups based on their different installer IDs (HR, Marketing, and OM).

FortiClient Installer

You can create deployment packages to deploy FortiClient to endpoints. Deployment packages include the FortiClient installer, which determines the FortiClient release and patch to install on the endpoint. Deployment packages can also include a Telemetry gateway list for connection to a FortiGate.

See Installing FortiClient using the CLI.

Adding a FortiClient installer



After you add a FortiClient installer to FortiEndpoint, you cannot edit it. You can delete the deployment package from FortiEndpoint, and edit the installer outside of FortiEndpoint. You can then add the edited installer to FortiEndpoint.

You can create an installer or installer config file, or upload a packaged installer to add a FortiClient deployment package.



If the *Sign software packages* option is enabled in *System Settings > EMS Settings*, Windows deployment packages display as being from the publisher specified in the certificate file. See Configuring EMS settings on page 533. the*FortiEndpoint Administration Guide*.

To create an installer or install config file:

1. Go to *Deployment & Installers > FortiClient Installer* and click *Add*.
2. On the *General* tab, configure the options depending on the type of FortiClient installer you are using:
   - To use an official FortiClient installer, keep the *Create a manual installer* option disabled under *Advanced Options* at the bottom and set the following options:

Option	Description
Online Installer Name	Enter the desired installer name.
Add Note	Click to add a note to the installer. In the *Notes* field, enter any details about the installer.
Release	Select the FortiClient release version to install.

Option	Description
Patch	Select the specific FortiClient patch version to install.
Hotfix	If a hotfix is available for the selected patch, the *Hotfix* dropdown list appears. See Adding a FortiClient hotfix installer on page 113.
Auto update to the Latest Patch	If a hot fix is not available for the selected patch, this field displays *Auto update to the Latest Patch*. Enable to repackage the installer to the latest patch release. If a hotfix is available for the selected patch, you can select several options. See Adding a FortiClient hotfix installer on page 113.
Repackaged Installer Files	Configure which installer files to include.

- To manually create a FortiClient installer, enable the *Create a manual installer* option under *Advanced Options* at the bottom and set the following options:

Option	Description
Release	Select from the following options: • *Upload packaged installer*—Manually upload a repackaged installer provided by TAC. • *Use custom installer*—Select from a list of previously uploaded custom installers or upload a new custom installer as follows: **a.** Click *Add*. **b.** Specify the custom installer name. **c.** Browse to select 64-bit/32-bit Window and/or Linux/macOS custom installers in ZIP or MSI format. You can download FortiClient installers (in ZIP format) from Fortinet Customer Service & Support., which requires a support account with a valid support contract. To upload an `.msi` file, you must package the installer as an `.msi` file. **d.** For Windows and Linux, you can also select *Include ARM* and browse to select the ARM installer files. **e.** Click *Upload*.
Manual Installer Name	Enter the desired custom installer name.

3. Click *Next*. On the *Features* tab, set the following options. For features that are not available for all operating systems, the dialog displays the icons for the operating systems that the feature is available:



Available options may differ depending on the features you have enabled or disabled in *Feature Select*. See Feature Select on page 555. See Feature Select.

Option	Description
Zero Trust Telemetry	Enabled by default and cannot be disabled. Installs FortiClient with Telemetry enabled.

Option	Description
Secure Access Architecture Components	Install FortiClient with SSL and IPsec VPN enabled. Disable to omit SSL and IPsec VPN support from the FortiClient deployment package. If you enable this feature for a deployment package and include a preconfigured VPN tunnel in the included endpoint profile, users who use this deployment package to install FortiClient can connect to this preconfigured VPN tunnel for three days after their initial FortiClient installation. This is useful for remote users, as it allows them to connect to the corporate network to activate their FortiClient license. If the user does not activate their FortiClient license within the three days, all FortiClient features, including VPN, stop working on their device. See Remote Access on page 134 for details on configuring a VPN tunnel.
Vulnerability Scan	Enabled by default and cannot be disabled. Installs FortiClient with Vulnerability Scan enabled.
Advanced Persistent Threat (APT) Components	Install FortiClient with APT components enabled. Disable to omit APT components from the FortiClient deployment package. Includes FortiSandbox detection and quarantine features.
Malware	Enable any of the following features: • AntiVirus, Anti-Exploit, Removable Media Access • Anti-Ransomware • Cloud Based Malware Outbreak Detection Disable to exclude features from the FortiClient installer.
Web and Video Filtering	Enable any of the following features: • Web Filtering • Video Filtering Disable to exclude features from the FortiClient installer.
Application Firewall	Enable or disable Application Firewall in the FortiClient installer.
Single Sign-On Mobility Agent	Enable or disable single sign-on mobility agent in the FortiClient installer.
Zero Trust Network Access	Enable or disable zero trust network access (ZTNA) in the FortiClient installer. The ZTNA feature is always installed on a macOS endpoint, regardless of whether this option is enabled or disabled.

Option	Description
Privileged Access Agent	Enable or disable privileged access agent in the FortiClient installer.

If you enable a feature in the deployment package that is disabled in Feature Select, the feature is installed on the endpoint, but is disabled and does not appear in the FortiClient GUI. For example, when Web Filter is disabled in Feature Select, if you enable Web Filtering in a deployment package, the deployment package installs Web Filter on the endpoint. However, the Web Filter feature is disabled on the endpoint and does not appear in the FortiClient GUI.

4. Click *Next*. On the *Advanced* tab, set the following options:

Option	Description
Enable desktop shortcut	Configure the FortiClient deployment package to create a desktop shortcut on the endpoint.
Enable start menu shortcut	Configure the FortiClient deployment package to create a Start menu shortcut on the endpoint.
Include MSI installer files	Enable to include MSI installer files for FortiClient (Windows).
Enable Installer ID	Configure an installer ID. Select an existing installer ID or enter a new installer ID. If creating an installer ID, select a group path or create a new group in the *Group Path* field. FortiEndpoint automatically groups endpoints according to installer ID group assignment rules. See Group assignment rules on page 92. If you manually move the endpoint to another group after EMS places it into the group defined by the installer ID group assignment rule, EMS returns the endpoint to the group defined by the installer ID group assignment rule. In an environment with a large number of endpoints, since you can configure each deployment package with only one installer ID, it may be inefficient to create a deployment package for each installer ID. See Deploying different installer IDs to endpoints using the same deployment package on page 105.
Enable Endpoint VPN Profile	Select an endpoint VPN profile to include in the installer. EMS applies the VPN profile to the endpoint once it has installed FortiClient. This option is necessary if users require VPN connection to connect to EMS.
Enable Endpoint System Profile	Select an endpoint system profile to include in the installer. EMS applies the system profile to the endpoint once it has installed FortiClient. This option is necessary if it is required to have certain security features enabled prior to contact with EMS.
Invalid Certificate Action	Select the action to take when FortiClient attempts to connect to EMS with an invalid certificate: • **Warn**: warn the user about the invalid server certificate. Ask the user whether to proceed with connecting to EMS, or terminate the connection attempt. FortiClient remembers the user's decision for

Option	Description
	this EMS, but displays the warning prompt if FortiClient attempts to connect to another EMS (using a different EMS FQDN/IP address and certificate) with an invalid certificate. • **Allow**: allows FortiClient to connect to EMS with an invalid certificate. • **Deny**: block FortiClient from connecting to EMS with an invalid certificate.

5. Click *Next*. The *Telemetry* tab displays the hostname and IP address of the FortiEndpoint server, which manage FortiClient once it is installed on the endpoint.
6. Do one of the following:
   - If you selected *Create* installer, Click *Finish*. The FortiClient deployment package is added to FortiEndpoint and displays on the *Deployment Installers > FortiClient Installer* pane. The deployment package may include .exe (64-bit), .msi, .dmg, .rpm, and .deb files depending on the configuration. The end user can download these files to install FortiClient on their machine with the desired configuration.
   - If you selected *Create installer config* file, click *Download*. This downloads a config.json file to your device. You can upload this file to a cloud server to create a custom deployment package.

To upload packaged installers:

1. Go to *Deployment & Installers > FortiClient Installer*.
2. Click *Add*.
3. On the *General* tab, set the following options:

Option	Description
Online Installer Name	Enter the desired installer name.
Add Note	Click to add a note to the installer. In the *Notes* field, enter any details about the installer.
Release	Select *Upload packaged installer*.
Repackaged installer	Browse to and select the installer file.

4. Click *Next*. On the *Features* tab, set the following options. For features that are not available for all operating systems, the dialog displays the icons for the operating systems that the feature is available:



Available options may differ depending on the features you have enabled or disabled in *Feature Select*. See Feature Select on page 555. See Feature Select.

Option	Description
Zero Trust Telemetry	Enabled by default and cannot be disabled. Installs FortiClient with Telemetry enabled.

Option	Description
Secure Access Architecture Components	Install FortiClient with SSL and IPsec VPN enabled. Disable to omit SSL and IPsec VPN support from the FortiClient deployment package. If you enable this feature for a deployment package and include a preconfigured VPN tunnel in the included endpoint profile, users who use this deployment package to install FortiClient can connect to this preconfigured VPN tunnel for three days after their initial FortiClient installation. This is useful for remote users, as it allows them to connect to the corporate network to activate their FortiClient license. If the user does not activate their FortiClient license within the three days, all FortiClient features, including VPN, stop working on their device. See Remote Access on page 134 for details on configuring a VPN tunnel.
Vulnerability Scan	Enabled by default and cannot be disabled. Installs FortiClient with Vulnerability Scan enabled.
Advanced Persistent Threat (APT) Components	Install FortiClient with APT components enabled. Disable to omit APT components from the FortiClient deployment package. Includes FortiSandbox detection and quarantine features.
Malware	Enable any of the following features: • AntiVirus, Anti-Exploit, Removable Media Access • Anti-Ransomware • Cloud Based Malware Outbreak Detection Disable to exclude features from the FortiClient installer.
Web and Video Filtering	Enable any of the following features: • Web Filtering • Video Filtering Disable to exclude features from the FortiClient installer.
Application Firewall	Enable or disable Application Firewall in the FortiClient installer.
Single Sign-On Mobility Agent	Enable or disable single sign-on mobility agent in the FortiClient installer.
Zero Trust Network Access	Enable or disable zero trust network access (ZTNA) in the FortiClient installer. The ZTNA feature is always installed on a macOS endpoint, regardless of whether this option is enabled or disabled.

Option	Description
Privileged Access Agent	Enable or disable privileged access agent in the FortiClient installer.

If you enable a feature in the deployment package that is disabled in Feature Select, the feature is installed on the endpoint, but is disabled and does not appear in the FortiClient GUI. For example, when Web Filter is disabled in Feature Select, if you enable Web Filtering in a deployment package, the deployment package installs Web Filter on the endpoint. However, the Web Filter feature is disabled on the endpoint and does not appear in the FortiClient GUI.

5. Click *Next*. On the *Advanced* tab, set the following options:

Option	Description
Enable desktop shortcut	Configure the FortiClient deployment package to create a desktop shortcut on the endpoint.
Enable start menu shortcut	Configure the FortiClient deployment package to create a Start menu shortcut on the endpoint.
Installer Files	Enable to include MSI installer files for FortiClient (Windows).
Enable Installer ID	Configure an installer ID. Select an existing installer ID or enter a new installer ID. If creating an installer ID, select a group path or create a new group in the *Group Path* field. FortiEndpoint automatically groups endpoints according to installer ID group assignment rules. See Group assignment rules on page 92. If you manually move the endpoint to another group after EMS places it into the group defined by the installer ID group assignment rule, EMS returns the endpoint to the group defined by the installer ID group assignment rule. In an environment with a large number of endpoints, since you can configure each deployment package with only one installer ID, it may be inefficient to create a deployment package for each installer ID. See Deploying different installer IDs to endpoints using the same deployment package on page 105.
Enable Endpoint VPN Profile	Select an endpoint VPN profile to include in the installer. EMS applies the VPN profile to the endpoint once it has installed FortiClient. This option is necessary if users require VPN connection to connect to EMS.
Enable Endpoint System Profile	Select an endpoint system profile to include in the installer. EMS applies the system profile to the endpoint once it has installed FortiClient. This option is necessary if it is required to have certain security features enabled prior to contact with EMS.
Invalid Certificate Action	Select the action to take when FortiClient attempts to connect to EMS with an invalid certificate: • **Warn**: warn the user about the invalid server certificate. Ask the user whether to proceed with connecting to EMS, or terminate the connection attempt. FortiClient remembers the user's decision for

Option	Description
	this EMS, but displays the warning prompt if FortiClient attempts to connect to another EMS (using a different EMS FQDN/IP address and certificate) with an invalid certificate. • **Allow**: allows FortiClient to connect to EMS with an invalid certificate. • **Deny**: block FortiClient from connecting to EMS with an invalid certificate.
Invitation	Select an invitation to include in the deployment package. If you have not created an invitation, you can create one by clicking *Create Invitation*. See Invitations on page 503.

6. Click *Next*. The *Telemetry* tab displays the hostname and IP address of the FortiEndpoint server, which manage FortiClient once it is installed on the endpoint.
7. Do one of the following:
   - If you selected *Create* installer, Click *Finish*. The FortiClient deployment package is added to FortiEndpoint and displays on the *Deployment Installers > FortiClient Installer* pane. The deployment package may include .exe (64-bit), .msi, .dmg, .rpm, and .deb files depending on the configuration. The end user can download these files to install FortiClient on their machine with the desired configuration.
   - If you selected *Create installer config* file, click *Download*. This downloads a config.json file to your device. You can upload this file to a cloud server to create a custom deployment package.

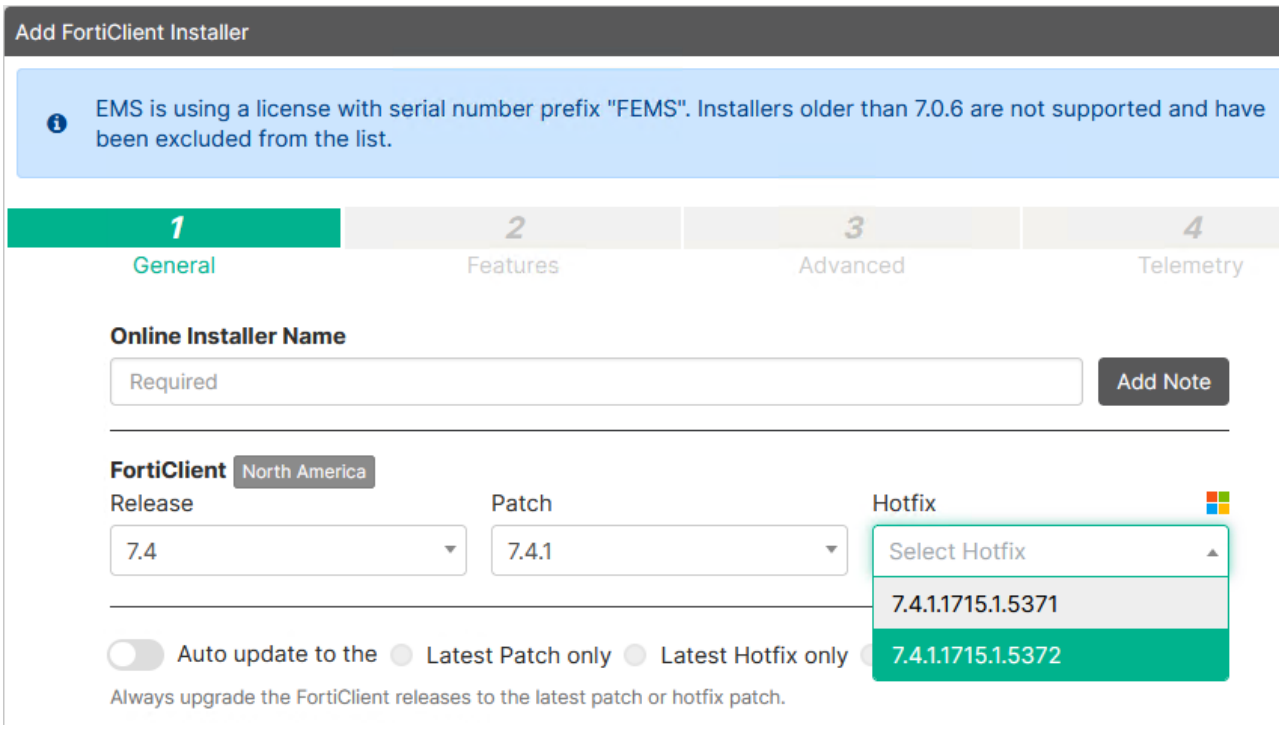
Adding a FortiClient hotfix installer

You can deploy FortiClient hotfix installers from EMS. A hotfix contains a subset of the FortiClient binaries to address a specific issue and reduces the risk of unintended side effects. Creating a hotfix installer follows the same EMS process as creating any other installer.

Prior to this implementation, EMS was restricted to deploying only major and minor FortiClient versions, such as 7.4.0 and 7.4.1. With this enhancement, if a bug is identified in any version, Fortinet can promptly address it by deploying a hotfix, rather than waiting for the release of the next major or minor builds.

To create a hotfix installer:

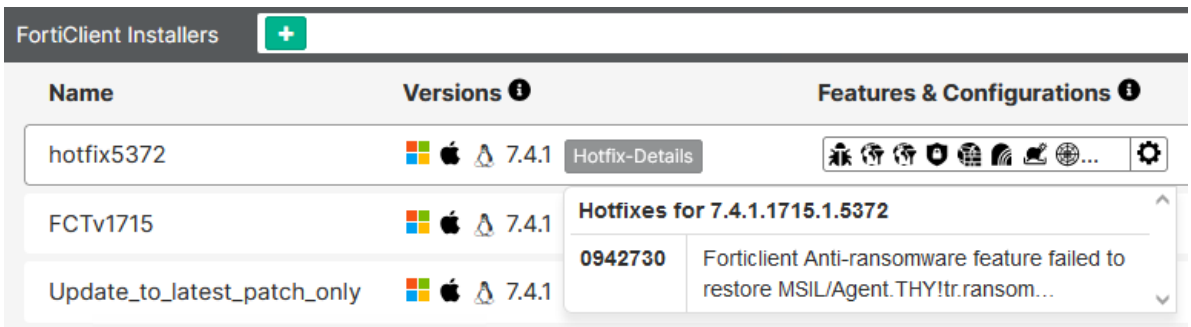
1. In EMS, go to *Deployment & Installers > FortiClient Installer*.
2. Click *Add*.
3. From the *Release* dropdown list, select the desired FortiClient version.
4. From the *Patch* release dropdown list, select the desired patch version.
5. If a hotfix is available for the selected patch, the *Hotfix* dropdown list appears. In the following example, there are two hotfixes available for the selected version, 7.4.1.



6. If desired, enable *Auto update to the*. When you select any of the following options, the installer automatically updates. For example, consider that you create the installer with *Latest Patch only* selected. When a new patch, 7.4.2, becomes available, EMS automatically updates the installer to install 7.4.2. If the installer is configured in a deployment configuration, the configuration is updated with the new installer, and if the configuration is enabled, EMS automatically deploys the updated installer. The following options are available:
   - *Latest Patch only*
   - *Latest Hotfix only*
   - *Latest Patch and Hotfix*

   Select *Latest Hotfix only* or *Latest Patch and Hotfix*.

   Hotfixes are specific to particular versions. You can only deploy a hotfix to an endpoint if it has the base FortiClient already installed. For example, you can only deploy or install hotfix 1715:5372 on an endpoint where FortiClient 7.4.1 build 1715 is installed. If an installer with *Latest Patch and Hotfix* selected is deployed to an endpoint with FortiClient 7.4.0 installed and the latest hotfix available is 1715:5372, the deployment first installs FortiClient 7.4.1 build 1715 on the endpoint, the installs the hotfix.
7. Continue configuring the installer as desired. After creation, you can view the installer in *Deployment & Installers > FortiClient Installer*. Click *Hotfix-Details* to see the details of the bug or issue that this hotfix addresses.



Viewing deployment packages

After you add FortiClient deployment packages to FortiEndpoint, you can view them on the *Deployment & Installers > FortiClient Installer* pane.

The *Deployment Packages* pane displays the following information about each deployment package:

- Name of the FortiClient deployment package
- Operating system (Windows and/or macOS)
- Version of FortiClient software for each OS
- Whether Auto Update is enabled or disabled
- Location of the FortiClient deployment package FortiEndpoint. Endpoint users can access this location to download and install FortiClient on endpoints.

Selecting a deployment package displays the following additional information:

- Enabled FortiClient features
- Configured endpoint profile
- Connection to FortiEndpoint
- Auto registration enabled/disabled
- Desktop shortcut enabled/disabled
- Start menu shortcut enabled/disabled
- Configured installer ID
- Notes included when creating the deployment package

You can also create or delete a deployment package and refresh the deployment package list.

Deleting a FortiClient deployment package

To delete a FortiClient deployment package:

1. Go to *Deployment & Installers > FortiClient Installer*.
2. Click the desired deployment package, then click *Delete*. A confirmation dialog displays.
3. Click *Yes*. FortiEndpoint deletes the FortiClient deployment package.

Endpoint Policy & Components

You can create endpoint policies to assign endpoint profiles and on-fabric detection rules to groups of Windows, macOS, and Linux endpoints. The *Endpoint Policy & Components* > *Manage Policies* page provides a comprehensive summary of which endpoint policies are applied to which endpoint groups.

Manage Policies

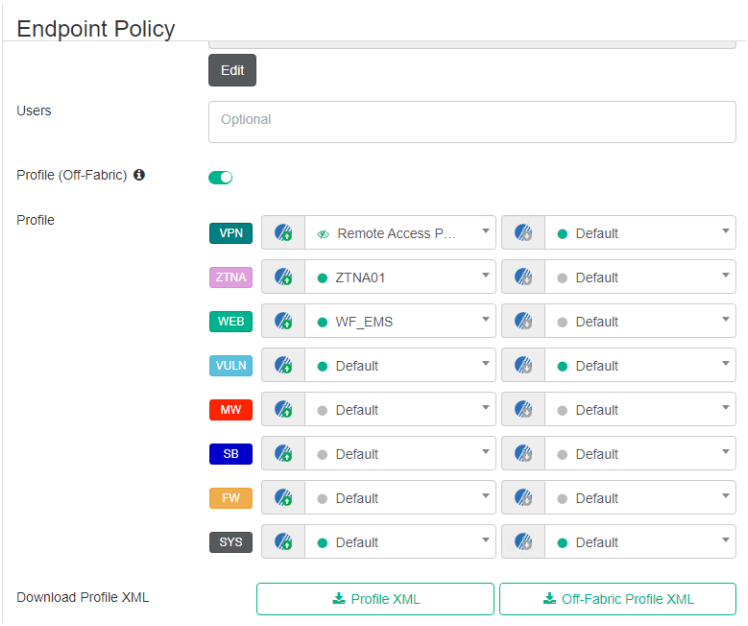
Adding an endpoint policy

To add an endpoint policy:

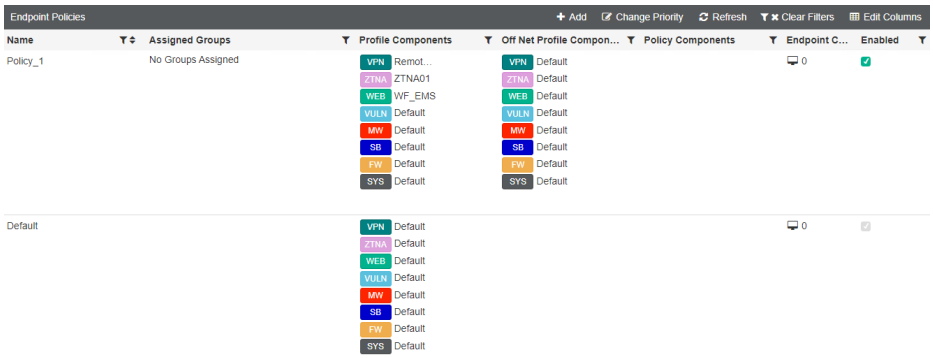
1. Go to *Endpoint Policy & Components* > *Manage Policies*.
2. Click *Add*.
3. Complete the following fields:

Option	Description
Endpoint Policy Name	Enter the desired name for the endpoint policy.
Endpoint Groups	Select the device and/or user group to apply the policy to. You can select a group from all imported domains and workgroups.
Users	Search for and select desired domain users to apply the policy to. If an endpoint is applicable for both a user-based and a group-based policy, EMS applies the user-based policy, which takes precedence, to the endpoint. When using a user-based policy, disabling the Windows switch users option is recommended to ensure EMS applies the policy correctly.
Profile (Off-Fabric)	Configure the desired endpoint profiles to apply to the endpoint when it is off-fabric according to the on-fabric detection rules configured in this policy. For example, you may want to apply more restrictive profiles to the endpoint when it is determined to be off-fabric. From the dropdown list, select the desired endpoint profiles. If including an off-fabric profile in a policy, also including on-fabric detection rules in the policy is recommended. Otherwise, EMS may not apply on-fabric and off-fabric profiles as desired. When you enable this toggle, the *Profile* field displays two sets of endpoint profile dropdown lists. You can configure the desired endpoint profiles for an off-fabric endpoint using the dropdown lists on the right.

Option	Description
Profile	From the dropdown lists, configure the desired endpoint profiles to apply to endpoints that EMS has applied the policy to. FortiEndpoint displays enabled endpoint profiles with a green circle and disabled endpoint profiles with a gray circle.
Download Profile XML	Download the XML configuration file for the profiles by clicking the *Profile XML* button. This downloads one XML file that contains the XML configuration for all selected endpoint profiles. If *Profile (Off-Fabric)* is enabled, you can use the *Off-Fabric Profile XML* button to download an XML file that contains the XML configuration for all selected endpoint profiles for off-fabric endpoints.
On-Fabric Detection Rules	Select the on-fabric detection rules to include in the policy. You can select multiple rules. If you select multiple rules, EMS considers the endpoint as on-fabric if it satisfies one of the selected rules. You must have already created on-fabric detection rules to include them in an endpoint policy. See On-fabric Detection Rules on page 124.
Comments	Enter any comments desired for the endpoint policy.
Enable the Policy	Toggle to enable or disable the endpoint policy. You can enable or disable the policy at a later time from *Endpoint Policy & Components > Manage Policies*.



4. Click *Save*. You can view the newly created policy in *Endpoint Policy & Components > Manage Policies*.



EMS pushes these settings to the endpoint with the next Telemetry communication.

Editing an endpoint policy

To edit an endpoint policy:

1. Go to *Endpoint Policy & Components Manage Policies*.
2. Select the endpoint policy.
3. Click *Edit*.
4. Edit as desired.
5. Click *Save*.

Deleting an endpoint policy

1. Go to *Endpoint Policy & Components Manage Policies*.
2. Click the desired endpoint policy.
3. Click *Delete*.
4. In the confirmation dialog, click *Yes*.

Enabling/disabling an endpoint policy

1. Go to *Endpoint Policy & Components Manage Policies*.
2. Select or deselect the *Enabled* checkbox for the desired endpoint policy.

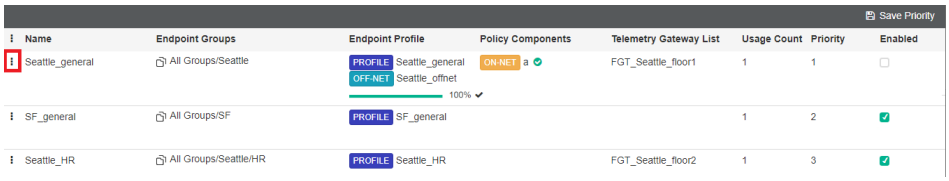
Managing endpoint policy priority levels

An endpoint may be eligible for multiple endpoint policies. When an endpoint is eligible for multiple endpoint policies, the following factors determine which endpoint policy EMS applies to the endpoint:

1. EMS only applies endpoint policies to endpoints if they are enabled on the *Endpoint Policy & Components Manage Policies* page.
2. If an endpoint is eligible for multiple enabled endpoint policies, EMS applies the policy with the highest priority to the endpoint.

To change endpoint policy priority levels:

1. Go to *Endpoint Policy & Components Manage Policies*.
2. Click *Change Priority*.
3. Click and hold the policy name, then drag to the desired position.

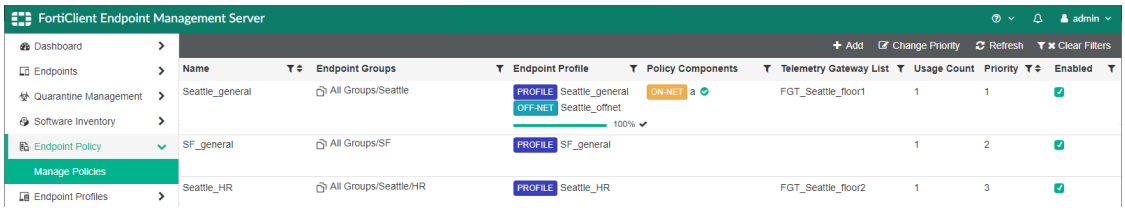


4. Click *Save Priority*.

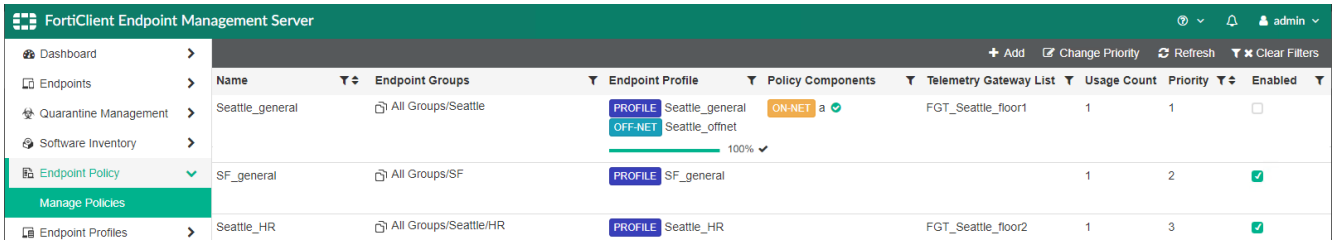
In the examples, there are three endpoint policies:

Name	Endpoint groups	Priority level
Seattle_general	All Groups/Seattle	1
SF_general	All Groups/SF	2
Seattle_HR	All Groups/Seattle/HR	3

In this example, all three policies are enabled. The All Groups/Seattle/HR subgroup is eligible for both the Seattle_general and Seattle_HR policies. In this scenario, EMS applies the first eligible endpoint policy, Seattle_general, to the All Groups/Seattle/HR subgroup.



In this example, the Seattle_general endpoint policy has been disabled. The All Groups/Seattle/HR group is still eligible for both policies. Since the Seattle_general policy is disabled, EMS applies Seattle_HR to the All Groups/Seattle/HR group.

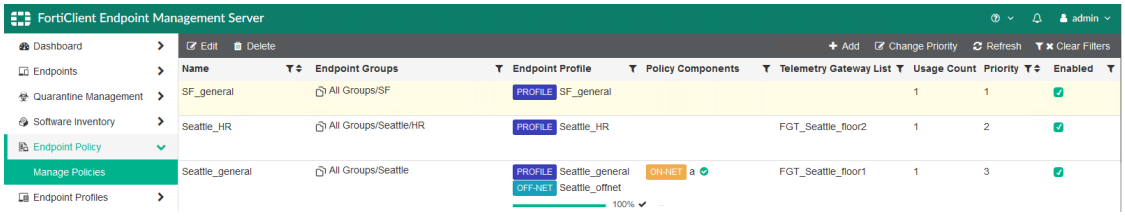


Consider that you then make the following changes:

- Enable Seattle_general
- Move policies so that they have the following priorities:
  - SF_general: 1
  - Seattle_HR: 2
  - Seattle_general: 3

In this example, the All Groups/Seattle/HR group is eligible for two policies: Seattle_HR and Seattle_general. Since Seattle_HR comes before Seattle_general in the priority list, EMS applies Seattle_HR to All Groups/Seattle/HR.

Even though SF_general is set to priority 1, EMS does not apply it to All Groups/Seattle/HR, since All Groups/Seattle/HR is not eligible for that policy.



To change policy priority levels via a text file:

1. Go to *Endpoint Policy & Components > Manage Policies*.
2. Click *Change Priority*.
3. Click *Bulk Policy Order Update*. This option is only available if you have multiple non-default policies configured.
4. Click *Export*.
5. Open the downloaded text file. The file lists the policies in their configured priority levels. Edit the order as desired and save.
6. Click *Next*.
7. Browse to and import the updated text file. The priority levels update in EMS.

Editing endpoint policy view

You can select columns to display in *Endpoint Policy & Components Manage Policies*.

To edit endpoint policy view:

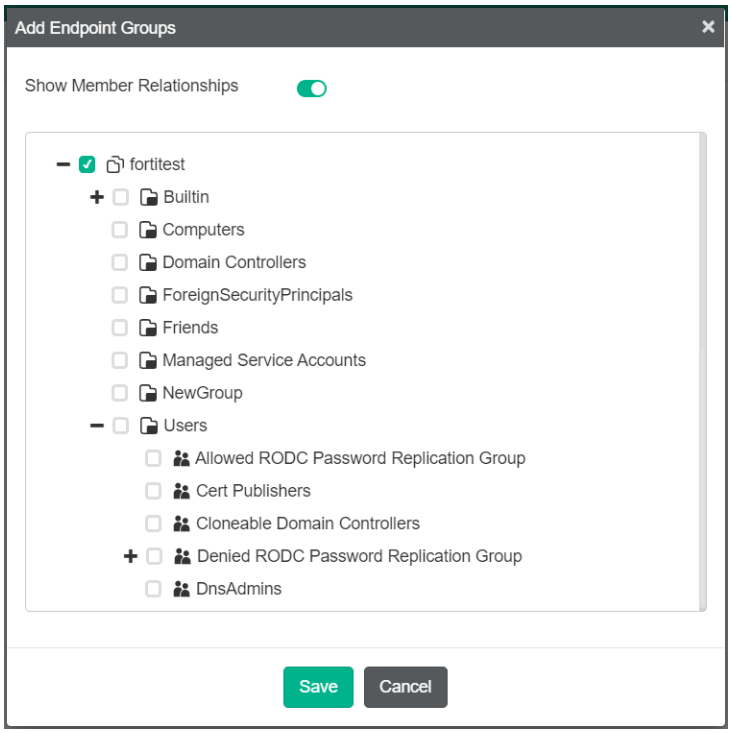
1. Go to *Endpoint Policy & Components Manage Policies*.
2. Click *Edit Columns*.
3. Enable or disable the columns as desired.
4. Click *Save*.

FortiClient management based on Active Directory user/user groups

You can assign FortiClient policies based on endpoint devices in organizational units.

To assign device groups, user groups, and users to a policy:

1. Go to *Endpoint Policy*. Create a new policy or select an existing one.
2. In the *Endpoint Groups* field, click *Edit*. In the *Add Endpoint Groups* dialog, select the desired device and/or user groups. Click *Save*.



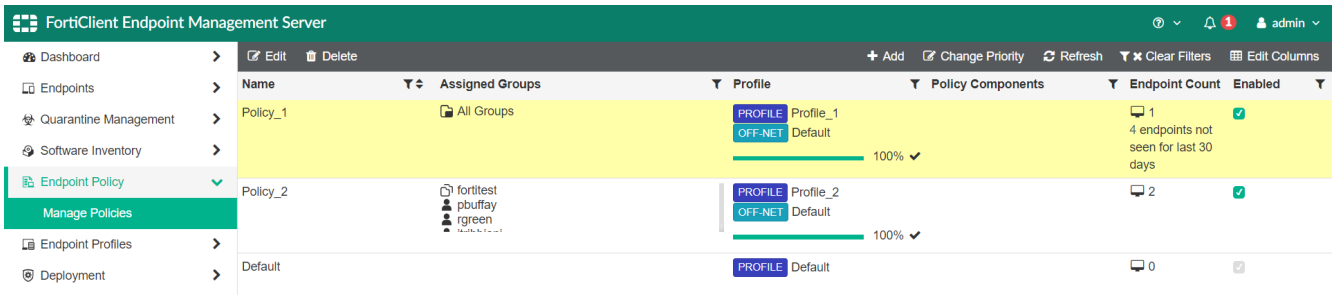
3. In the *Users* field, select the desired users.
4. Click *Save*.

When FortiClient connects to EMS, the following occurs:

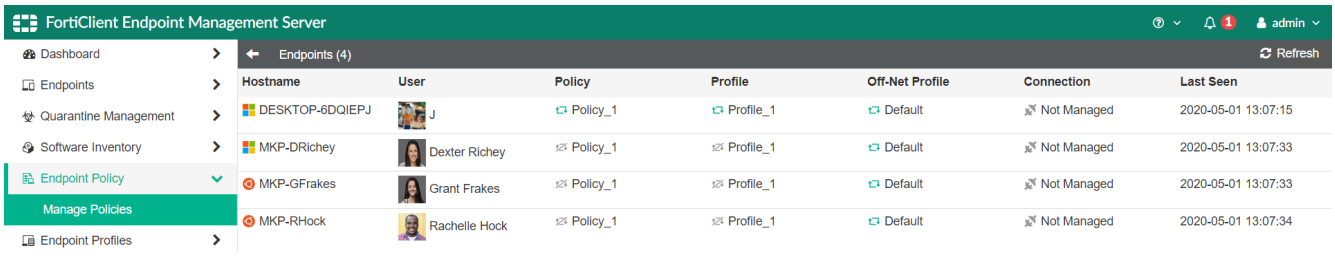
1. If a policy is assigned to the FortiClient user, EMS assigns that policy to the endpoint.
2. If there are policies for the FortiClient group container and/or user groups, EMS assigns the policy with the highest global priority.
3. If there are inherited policies for group containers and/or user groups, EMS assigns the inherited policy with the highest global priority.

In *Endpoint Policy & Components Manage Policies*, you can click *Edit Columns* to select which columns to display.

The *Manage Policies* page displays a progress line that indicates each policy's FortiClient synchronization status. The *Endpoint Count* column shows the number of FortiClient endpoints with the policy assigned and the number of endpoints that have not been seen for the past 30 days.



Click the endpoint count to see the endpoint list.

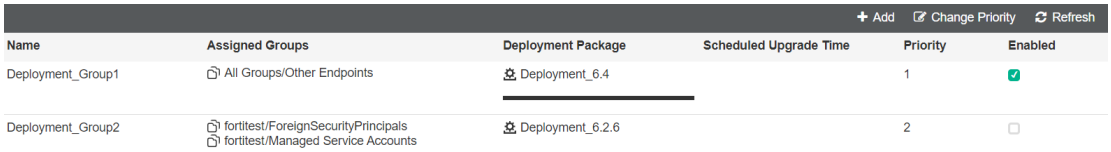


To deploy FortiClient to endpoints with user-based management:

1. (Optional) Create a custom installer.
2. Go to *System Settings* > *Feature Select*. Select the features to globally show and hide. In 6.4.0, you no longer select available features for each deployment package.
3. Create a deployment package.
4. Create a deployment configuration.

For details on this deployment process, see Manage Deployment on page 101.

In *Deployment & Installers* > *Management Deployment*, the *Deployment Package* column displays a progress line indicating each deployment package's deployment state.



CA Certificates

If FortiOS is connected to EMS using the EMS API, deep inspection is enabled, and the Fortinet Security Fabric connection between FortiOS and FortiEndpoint is configured, EMS automatically imports the FortiOS CA certificate. You then only need to apply the certificate in the desired endpoint profile. See System Settings on page 378. In this scenario, you do not need to manually upload or import CA certificates to EMS.

If you manually delete the imported certificate from EMS, EMS does not automatically reimport the certificate from FortiOS, even when EMS and FortiOS remain connected via the Fabric connector. EMS also does not automatically delete an already imported certificate if the Fabric connection between FortiOS and EMS is removed.

If FortiOS is not sending the CA certificate to EMS, you can manually upload or import CA certificates as the following describes.

After uploading or importing a certificate, you must configure it in a profile using the *Install CA Certificate on Client* option to provision it to endpoints. See System Settings on page 378.

To upload a CA certificate:

You can locally upload a CA certificate.

1. Go to *Endpoint Policy & Components > CA Certificates*.
2. Select *Upload*.
3. In the *Upload Local Certificate* window, click *Browse* and locate the certificate.
4. Click *Upload*.

To import a CA certificate:

1. Go to *Endpoint Policy & Components > CA Certificates*.
2. Select *Import*.
3. In the *Import Certificates from FortiGate* window, enter the following information:

IP address/Hostname	Enter the server IP/hostname in the following format: `<ip address> : <port>`.
VDOM	Enter the VDOM name.
Username	Enter the username.
Password	Enter the password.

4. Click *Import* to import the certificate.

On-fabric Detection Rules

You can configure on-fabric detection rules for endpoints. EMS uses the rules to determine if the endpoint is on- or off-fabric. Depending on the endpoint's on-fabric status, EMS may apply a different profile to the endpoint, as configured in the applied endpoint policy. See Adding an endpoint policy on page 116.

When a user switches accounts between a local non-domain account and a domain account on the same machine, FortiClient EMS may not apply the correct policy to the endpoint.

To add an on-fabric detection rule set:

1. Go to *Endpoint Policy & Components* > *On-fabric Detection Rules*.
2. Click *Add*.
3. In the *Name* field, enter the desired name.
4. Enable or disable the rule set by toggling *Enabled* on or off.
5. Click *Add Rule*.
6. In the *Add New Rule* dialog, from the *Detection Type* dropdown list, select and configure the desired rule detection type. If you configure rules of multiple detection types for a rule set, the endpoint must satisfy all configured rules to satisfy the entire rule set:

Detection type	OS	Description
Connection Media	• Windows • macOS • Linux	From the *Ethernet* and/or *Wi-Fi* dropdown lists, select *Connected* or *Not Connected*. EMS considers the endpoint as satisfying the rule if its network settings match all configured fields.
Default Gateway	• Windows • macOS • Linux • iOS (IP address only) • Android (IP address only)	In the *IP Address* field, enter the default gateway IP address. In the *MAC Address* field, optionally enter the default gateway MAC address. EMS considers the endpoint as satisfying the rule if its default gateway configuration matches the IP address specified and MAC address, if it is configured. Configuring the MAC address is optional. You can configure multiple addresses using the + button.
DHCP Server	• Windows • macOS • Linux	On the *IP/MAC Address* tab, configure the IP and/or MAC address for the desired DHCP server. On the *DHCP Code* tab, configure the DHCP code for the desired DHCP server. You can configure just the *IP/MAC Address* tab, just the *DHCP Code* tab, or both tabs. If configuring the *IP/Mac Address* tab, the MAC Address field is optional.

Detection type	OS	Description
		The DHCP code is synonymous with the old option 224, which FortiClient would read from the DHCP server and send to the FortiGate in FortiOS 6.0. It used to be the FortiGate serial number. Now, it can be any string configured in the DHCP server as option 224. You may still use FortiGate serial number as the DHCP code if desired. See To configure the DHCP code: on page 127. This rule type only supports local DHCP servers. EMS considers the endpoint as satisfying the rule if it is connected to a DHCP server that matches the specified configuration. You can configure multiple IP and MAC addresses and DHCP codes using the *+* button on each tab.
DNS Request	• Windows • macOS • Linux	In the *IP address* and *Hostname* fields, enter the IP address and hostname for the desired internal DNS server. EMS considers the endpoint as satisfying the rule if it can make a DNS request to the DNS server that matches the specified configuration and receive a successful DNS response. You can configure multiple servers using the *+* button.
DNS Server	• Windows • macOS • Linux • iOS • Android	Configure at least one IP address for the desired DNS server. EMS considers the endpoint as satisfying the rule if it is connected to a DNS server that matches the specified configuration. You can configure multiple IP addresses using the *+* button.
EMS Connection	• Windows • macOS • Linux • iOS • Android	The only available option for this detection type is that EMS considers the endpoint as satisfying the rule if it is online with EMS.
Local IP/Subnet	• Windows • macOS • Linux • iOS (IP address only) • Android (IP address only)	In the *IP Range* field, enter a range of IP addresses. Optionally, enter the default gateway MAC address in the *Default Gateway MAC Address* field. EMS considers the endpoint as satisfying the rule if its Ethernet or wireless IP address (not VPN IP address) is within the range specified and its default gateway MAC address matches the one specified, if it is configured. You can configure multiple addresses using the *+* button.

Detection type	OS	Description
		 This is the only detection type that applies to endpoints running FortiClient 6.4.0 and earlier versions. Other detection types do not apply to these endpoints.
Ping Server	• Windows • macOS • Linux	In the *IP Address* field, enter the server IP address. EMS considers the endpoint as satisfying the rule if it can access the server at the specified IP address. You can configure multiple addresses using the + button.
Public IP	• Windows • macOS • Linux • iOS • Android	In the *IP Address* field, enter the desired IP address. EMS considers the endpoint as satisfying the rule if its public (WAN) IP address matches the one specified. You can configure multiple addresses using the + button.
VPN Tunnel	• Windows • macOS • Linux • iOS • Android	In the *Name* field, enter an SSL or IPsec VPN tunnel name. EMS considers the endpoint as satisfying the rule if it is connected to a VPN tunnel with a matching name. You can configure tunnels using the + button.
HTTP Web Request	• Windows • macOS • Linux	Configure at least one internal IP address. EMS considers the endpoint as satisfying the rule if it can make an HTTP GET request to the IP address and receive a 200 OK response. You can configure multiple IP addresses using the + button.
HTTPS Web Request	• Windows • macOS • Linux	Configure at least one internal IP address and the certificate common name (CN) or SNI. EMS considers the endpoint as satisfying the rule if it can make an HTTPS GET request to the IP address and receive a server certificate with the specified SNI or CN. You can configure multiple IP addresses using the + button.

7. Click *Add Rule*.
8. Click *Save*.

To edit an on-fabric detection rule set:

1. Go to *Endpoint Policy & Components* > *On-fabric Detection Rules*.
2. Select the rule set.
3. Click *Edit*.
4. Edit as desired.

5. Click *Save*.

To delete an on-fabric detection rule set:

1. Go to *Endpoint Policy & Components* > *On-fabric Detection Rules*.
2. Click the desired rule set.
3. Click *Delete*.
4. In the confirmation dialog, click *Yes*.

To delete an on-fabric detection rule from a rule set:

1. Go to *Endpoint Policy & Components* > *On-fabric Detection Rules*.
2. Click the desired rule set.
3. Under *Rules*, select the desired rule.
4. Click *Delete Rule*.
5. Click *Save*.

To enable/disable an on-fabric detection rule:

1. Go to *Endpoint Policy & Components* > *On-fabric Detection Rules*.
2. Select or deselect the *Enabled* checkbox for the desired rule set.

An endpoint has an offline off-fabric status when it cannot connect FortiClient Telemetry to EMS and is outside any of the on-fabric networks.

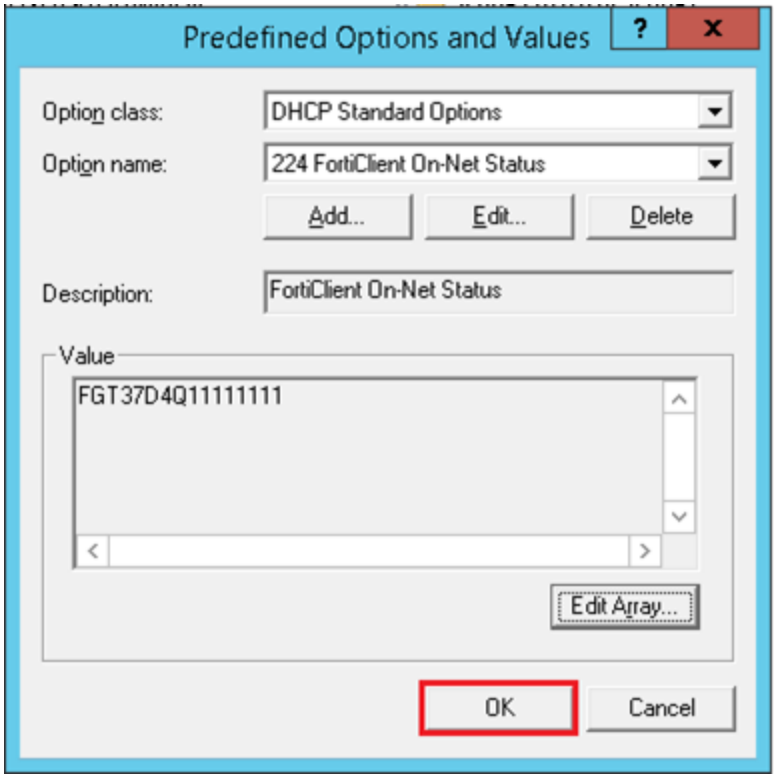
An endpoint has an offline on-fabric status when it cannot connect FortiClient Telemetry to EMS but is inside one of the on-fabric networks, or if no on-fabric rules are configured within the assigned policy.

To configure the DHCP code:

FortiClient can use a DHCP code/option 224 to determine on-/off-net status. A FortiGate automatically includes this option when used as a DHCP server. The following describes how to configure the option 224 when using a Windows server to handle DHCP.

1. On the Windows server, open DHCP settings.
2. Right-click *IPv4*, then select *Set Predefined Options*.
3. In the *Option name* dropdown list, confirm that option 224 has not been created.
4. Click *Add*.
5. In the *Code* field, enter 224.
6. Complete other fields as desired, then click *OK*.
7. Click *Edit Array*.
8. Click *Add*.

9. Enter the desired FortiGate serial number. Click *OK*.



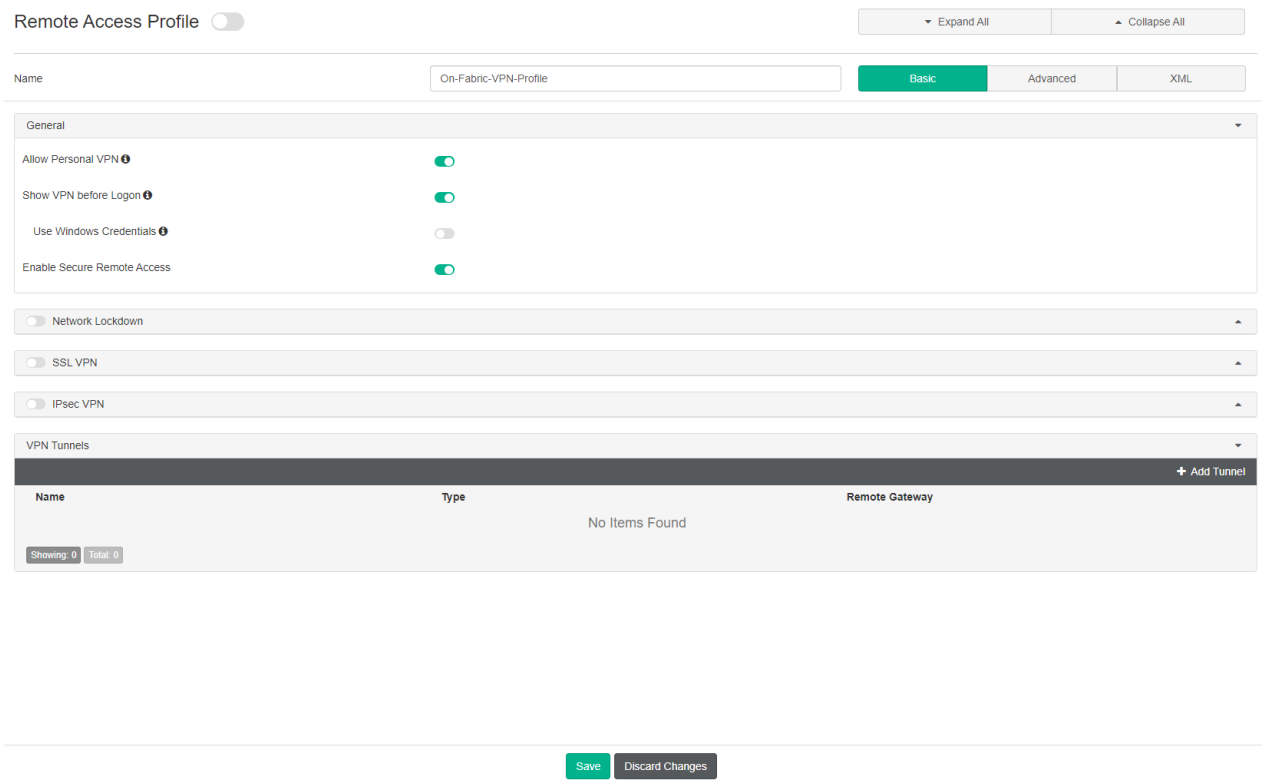
Source IP address anchoring for IPsec VPN

FortiOS requires endpoints' public IP addresses to achieve source IP address anchoring for IPsec VPN. FortiClient includes an enhancement to ensure that FortiClient provides a correct and reliable public IP address. You can then use the IP address in an on-Fabric detection rule in EMS.

This example configures an on-Fabric detection rule using the public IP address 208.91.115.30. The rule causes FortiClient to become on-Fabric or off-Fabric depending on if its public IP address is 208.91.115.30.

To configure an on-Fabric detection rule using a public IP address:

1. Add an on-Fabric rule:
   a. In EMS, go to *Endpoint Policy & Components > On-fabric Detection Rules*.
   b. Click *Add*.
   c. Click *Add Rule*.
   d. From the *Detection Type* dropdown list, select *Public IP*.
   e. In the *IP Address* field, enter the desired IP address.
   f. Click *Add Rule*.
   g. Click *Save*.
2. Go to *Endpoint Profiles > Remote Access*.
3. Create two Remote Access profiles, one for off-Fabric endpoints and one for on-Fabric endpoints. The profile for on-Fabric endpoints is disabled, while the profile for off-Fabric endpoints is enabled.



4. Go to *Endpoint Policy & Components* > *Manage Policies*.
5. Click *Add*.
6. Enable *Profile (Off-Fabric)*.
7. Configure the on- and off-Fabric VPN profiles as you configured.
8. Configure other fields as desired, then click *Save*. Once FortiClient receives the configuration, since it is on-Fabric, the *Remote Access* tab is not visible in FortiClient. If the FortiClient IP address does not match the one defined in the on-Fabric detection rule, the endpoint is considered off-Fabric and the *Remote Access* tab appears in FortiClient.

Chromebook Policy

You can create Chromebook policies to assign endpoint profiles to domains of Chromebook endpoints. The *Chromebook Policy > Manage Chromebook Policies* page provides a comprehensive summary of which policies are applied to which groups within the Google domain.

This option is only available if you enable the *EMS for Chromebooks Settings* option in *System Settings > EMS Settings*.

Chromebook policies function identically to Windows, macOS, and Linux endpoint policies except that you apply them to Chromebook endpoints and can only include a Chromebook profile. For details on configuring a Chromebook policy, refer to the equivalent sections in Endpoint Policy & Components on page 116.

Endpoint Profiles

FortiEndpoint has separate endpoint profiles for the following features:

- Remote Access on page 134
- ZTNA Destinations on page 307
- Web Filter on page 320
- Video Filter on page 343
- Vulnerability Scan on page 344
- Malware Protection on page 347
- Sandbox on page 357
- Firewall on page 361
- System Settings on page 378

For each endpoint profile type, you can use the default profile or create various profiles for different configurations and situations. You can then configure the desired combination of profiles in an endpoint policy and apply the policy to endpoints. See Adding an endpoint policy on page 116.

You can also import profiles to EMS.

Editing a default profile

You can edit a default profile to add or remove settings.

To edit a default profile:

1. Go to *Endpoint Profiles*, then select the desired profile type.
2. Click the desired default profile, then click Edit.
3. Configure the settings on the tabs.
4. Click *Save* to save the profile.

Creating a new profile

This section describes how to create a profile. You can use this profile to configure FortiClient software on endpoints by including it in an endpoint policy and deploying the policy to endpoints.

To create a profile to configure FortiClient:

1. Go to *Endpoint Profiles*.
2. Select the desired profile type.
3. Click the *Add* button.

4. Do one of the following:
   a. To create a Windows, macOS, and Linux profile, click *Add Profile*.
   b. To create a Chromebook profile, click *Add Chrome Profile*.
5. Configure the settings as desired.
6. Click *Save* to save the profile.

Adding a new Chromebook profile

When you enable Chromebook management on EMS, EMS creates default Web Filter and System Settings profiles for Chromebooks. By default, EMS includes these profiles in the default Chromebook policy, which it applies to any Google domains you add to FortiEndpoint.

You can add new Chromebook profiles to deploy different settings to Chomebook endpoints.



Adding Yandex search engine to the blocklist in the profile is recommended.

To add a new profile:

1. Go to *Endpoint Profiles*.
2. Go to *Web Filter* or *System Settings*.
3. Click *Add*, then click *Add Chrome Profile*.
4. Configure the profile as desired.
5. Click *Save*.

Managing profiles

You can manage profiles from the *Endpoint Profiles* pane.

Editing a profile

When you edit a profile that is assigned to endpoints or domains as part of an endpoint policy, FortiEndpoint automatically pushes the changes to the endpoints or Chromebooks with the next Telemetry communication after you save the profile.

To edit a profile:

1. Go to *Endpoint Profiles*, and select a profile.
2. Click *Edit*. The profile settings display in the content pane.
3. Edit the settings.
4. Click *Save*.

Cloning a profile

To clone a profile:

1. Go to *Endpoint Profiles* > *Manage Profiles*.
2. Select a profile, and click the *Clone* button. The cloned profile displays in the content pane.
3. In the *Profile Name* field, enter a name for the profile.
4. Configure the settings on the tabs.
5. Click *Save*.

Syncing profile changes

For profiles imported from FortiGate or FortiManager, you can manually sync profiles so that they are updated with the latest changes from the FortiGate or FortiManager that you imported them from.

1. Go to *Endpoint Profiles* > *Import from FortiGate / FortiManager*.
2. Select the desired profile.
3. Click *Sync Now*.

Editing sync schedules

For profiles imported from FortiGate or FortiManager, you can edit the sync schedule.

1. Go to *Endpoint Profiles* > *Manage Profiles*.
2. Select the desired profile.
3. Click *Edit Sync Schedule*.
4. In the *Synchronization Settings* window, configure the following options:
   a. *One Time Pull*: If selected, FortiEndpoint does not automatically sync profile changes from the FortiGate or FortiManager. You can manually sync profile changes after importing the profile. See Syncing profile changes on page 133.
   b. *Group Schedule*: Select to configure a group synchronization schedule for all selected profiles. Select the next date and time to automatically update the profiles, and the profile update interval in days, hours, or seconds.
   c. *Individual Schedule*: Select to configure an individual synchronization schedule for each selected profile. Select the next date and time to automatically update each profile, and the profile update interval in days, hours, or seconds.

Exporting a profile

You can export FortiClient endpoint profiles from EMS. When exporting the profile, all configured components are included. Profiles are exported as their XML configuration.

To export a profile:

1. Go to *Endpoint Policy & Components* > *Manage policies*.
2. Select the desired profile to export, then select *Edit*.
3. Select the button next to *Download Profile XML*. Your browser downloads a file named "profile.conf". Renaming this file to reflect the profile name is recommended.

Importing a profile

You can import a profile to EMS. When importing a profile, you can choose which components to import. After importing a profile, you can edit and include it in an endpoint policy.

To import a profile:

1. Go to *Endpoint Profiles*.
2. Select the desired profile type.
3. Do one of the following:
   a. If you selected *Web Filter*, go to *Import* > *Import from File*.
   b. If you selected another profile type, click *Import from File*.
4. In the *Name* field, enter the desired name.
5. In the *XML* field, browse to and upload the desired profile.
6. If desired, enable *Chrome Profile*. This is only available for Web Filter and System Settings profiles.
7. Do one of the following:
   a. Enable *Import All Components*.
   b. From the *Components* dropdown list, select the desired components to import from the profile. If *Chrome Profile* is enabled, only *Web Filter* and *System Settings* are available for selection.
8. Click *Upload*.

Deleting profiles

You cannot delete the default profiles.

1. Go to *Endpoint Profiles* > *Manage Profiles*.
2. Click desired profile, then click the *Delete* button. A popup displays.
3. Click *Yes*. EMS deletes the profile.

Remote Access

This topic contains general remote access settings descriptions:

Configuration	Description
Remote Access	Enable or disable the eye icon to show or hide the remote access feature from the end user in FortiClient.

Configuration	Description
	This option has no effect on FortiClient Android and iOS where the remote access feature is always enabled regardless of the EMS configuration.
General	
Allow Personal VPN	Allow users to create, modify, and use personal VPN configurations.
Disable Connect/Disconnect	Disable the *Connect/Disconnect* button when using *Auto Connect* with VPN.
Show VPN before Logon	Allow users to select a VPN connection before logging into the system.
Use Windows Credentials	If allowing users to select a VPN connection before logging into the system, enable this option to allow them to use their current Windows username and password.
After Logon SAML Authentication Framework	For VPN connections requiring SAML authentication, configure one of FortiClient's embedded browsers. A different engine powers each browser: • WebBrowser (Internet Explorer) • Electron (Chromium) • WebView2 (Microsoft Edge) Using Microsoft Edge WebView2 or Electron is recommended as they provide enhanced security and align with modern web standards. When Microsoft Entra ID is used as an identity provider and the endpoint is Azure-joined or added to an Azure account, if the SAML authentication framework is set to WebBrowser, the VPN connection establishes seamlessly without prompting for Azure credentials. In this case, disabling *Save Password* has no effect.
Minimize FortiClient Console on Connect	If FortiEndpoint is connected to one VPN tunnel, the FortiEndpoint console minimizes automatically after the tunnel is successfully established. This setting has no effect when FortiEndpoint is connected to multiple concurrent IKEv2 VPN tunnels, in which case the console window does not minimize automatically after the tunnel is successfully established even if this option is enabled.
Suppress VPN Notifications	Block FortiClient from displaying any VPN connection or error notifications.
Disable Internet Check	When you disable this setting, VPN autoconnect only starts FortiClient can access the internet. When enabled, VPN autoconnect starts even if FortiClient cannot access the internet.

Configuration		Description
Use Vendor ID		Use vendor ID. Enter the vendor ID in the *Vendor ID* field.
Enable Secure Remote Access		FortiClient denies or allows the endpoint to connect to a VPN tunnel based on the tunnel's *Tags* configuration. See the *Tags* field description in SSL VPN on page 139 and IPsec VPN on page 145.  This option does not work for FortiClient Android or iOS.
Prelogon Auto Connect Tunnel		Select the VPN tunnel that FortiClient starts when the OS boots up. If using a certificate, the certificate must exist in the computer certificate store. If the stored tunnel credentials are incorrect, FortiClient prompts the user for credentials to establish the tunnel connection. This feature may not work for IPsec VPN tunnels using certificates when per-user autoconnect is configured.
	Prelogon Auto Connect Priority	This option is available only if a tunnel is selected in *Prelogon Auto Connect Tunnel*. • When enabled, the selected tunnel (in *Prelogon Auto Connect Tunnel*) takes priority over any per-user tunnel and remains connected after user logon. • When disabled, FortiClient connects to a per-user VPN tunnel after user logon. If FortiClient was previously connected to any *Prelogon Auto Connect Tunnel*, it disconnects from that tunnel to connect to the per-user tunnel.
Current Connection		Select the current VPN tunnel.
	Auto Connect	Select a VPN tunnel for endpoints to automatically connect to when the end user logs into the endpoint. The end user must have established VPN connection manually at least once from FortiClient GUI.
	Disable Connect/Disconnect	Disable *Connect/Disconnect* button when using autoconnect VPN.
	Auto Connect Only When Off-Fabric	Autoconnect to the selected VPN tunnel only when EMS considers the endpoint off-fabric. See On-fabric Detection Rules on page 124.
	Auto Connect on Install	When enabled, the endpoint automatically connects to the VPN tunnel specified in *Auto Connect* after FortiClient receives an endpoint profile update.

Configuration	Description
Always Up Max Tries	Maximum number of attempts to retry a VPN connection lost due to network issues. If set to 0, it retries indefinitely.
Disconnect Password	Configure the password for users to disconnect FortiClient from FortiOS. The password will be encrypted using the PBKDF2 method. The default is no password. When a disconnect password is set, the *Disconnect* option will remain visible to end users using autoconnect VPN even if *Disable Connect/Disconnect* is selected.
Enforce Disabling Smart Multi-Homed Name Resolution	This field changes the status of the following registry key: *Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient\DisableSmartNameResolution* or in a group policy, *Computer Configuration > Administrative Templates > Network > DNS Client > Turn off smart multi-homed name resolution*. When using IPsec or SSL VPN split DNS, if this field is enabled, it may prevent the client from sending simultaneous DNS queries on multiple network interfaces. However, in cases where DNS queries via the FortiClient VPN virtual network interface are slow or fail, Windows may still attempt to resolve DNS queries through the physical network adapter. If you want to route DNS queries primarily through the FortiClient VPN interface, enabling the element helps ensure that queries are typically restricted to a single interface, though this behavior cannot be fully guaranteed.
Enable Multi-Connect on Eligible Tunnels	Enable FortiClient to connect to multiple tunnels concurrently. This feature is in beta and only supports IPsec VPN IKEv2 tunnels.
DNS Priority	When you enable *Enable Multi-Connect on Eligible Tunnels*, DNS Priority lists all IPsec VPN IKEv2 tunnels configured on this profile. There can be a maximum of 50 such tunnels configured per profile. Drag and drop the tunnels to configure the list in order of DNS priority. The priority list determines which tunnel interface has higher priority for DNS queries on Windows. When performing a DNS query, Windows queries the DNS server from the tunnel with the highest priority. If the query fails, then Windows queries the DNS server from the tunnel with the next highest priority, and so on. The DNS priority is the same as the VPN tunnel interface metric.
Enable View Selected VPNs	Enable for FortiClient to display pinned tunnels by default.

Configuration	Description
	If disabled, the FortiClient GUI displays all configured VPN tunnels. The user can select *View* > *Selected VPNs* to only display pinned tunnels. FortiClient remembers this setting and only shows pinned tunnels for that user when they open the FortiClient console in the future. FortiClient respects the local setting over the EMS setting in this case.
Network Lockdown	Configure network lockdown for off-fabric endpoints when they are not connected to VPN. When network lockdown is configured, when an endpoint goes off-fabric, a grace period that the EMS administrator configured comes into effect. During the grace period, an endpoint can continue to access LAN and the internet without restrictions. If the endpoint does not connect to VPN by the end of the grace period, the endpoint cannot access LAN and the internet. It can still access IP addresses and applications that the EMS administrator has configured as exceptions. FortiClient blocks both incoming and outgoing connection traffic unless the EMS administrator has configured it as an exception. After the end of the grace period, the endpoint can connect to VPN to regain internet access. For a full tunnel VPN, LAN is only accessible if exclusive routing is disabled. The administrator configures a limited number of attempts for the end user to enter valid VPN credentials. Once the user reaches the limit, the endpoint is in network lockdown. This feature only supports FortiClient (Windows) and (macOS).
`<detect_captive_portal>`	Configure captive portal detection options, which are XML-only (see VPN options). A captive portal is a webpage that users must interact with before gaining broader access to the network. Captive portals are commonly used in public or semi-public networks, such as those in hotels, where users must authenticate, accept terms of service, or log in before they can access the internet or other network resources.
Grace Period	Configure a grace period in seconds during which an off-fabric endpoint that is not connected to VPN can continue to access LAN and the internet without restrictions before network lockdown. Enter a value between 20 and 3600.

Configuration	Description
	 When `<detect_captive_portal>` is enabled (see VPN options), the grace period setting does not affect access to the captive portal login page. Users will always be redirect to the captive portal login page even if the grace period has passed.
Maximum Connection Attempts	Configure the maximum number of attempts for the end user of an off-fabric endpoint to enter valid VPN credentials.
Paths to Excluded Applications	Enter the path to applications that an off-Fabric endpoint that is not connected to VPN can still access.
Excluded IPs	Enter IP addresses that an off-Fabric endpoint that is not connected to VPN can still access.
Excluded Domains	Enter domains or the fully qualified domain names (FQDN) that an off-Fabric endpoint that is not connected to VPN can still access. Ensure to enter the FQDN correctly. Options that include protocols (such as *https://*) are not part of the FQDN and are therefore incorrect, as are entries with extra / added to the URL (such as *fortinet.com/*). Adding an entry like *example.com* matches both *.example.com* and *example.com* and an entry such as *www.example.com* matches *.www.example.com* and *www.example.com*. Moreover, network lockdown allows or blocks traffic based on the IP address extracted from the DNS response, so it does not rely on the top-level domain (TLD) or full URL. For instance, if we have added *www.fortinet.com* and then, in a lockdown state, attempt to access the site but are redirected to *www.fortinet.com/subscription*, access will still be allowed, and the client can reach the redirected page as well.
Excluded Saas Applications	Select SaaS applications that an off-Fabric endpoint that is not connected to VPN can still access.

SSL VPN

This topic contains descriptions of SSL VPN settings.



To view and configure SSL VPN settings, you must enable SSL VPN visibility in *System Settings* > *Feature Select*. See Feature Select on page 555.

In FortiOS 7.6.3 and later versions, SSL VPN tunnel mode is no longer supported and SSL VPN web mode is renamed to "agentless VPN". See Migration from SSL VPN tunnel mode to IPsec VPN and Agentless VPN.

You can continue to use FortiClient SSL VPN with FortiOS 7.6.2 and earlier versions.

Configuration	Description
SSL VPN	Enable SSL VPN.
DNS Cache Service Control	FortiClient disables Windows DNS cache when it establishes an SSL VPN tunnel. The DNS cache is restored after FortiClient disconnects from the SSL VPN tunnel. If you observe that Fortinet single sign on clients do not function correctly when an SSL VPN tunnel is up, use *Prefer SSL VPN DNS* to control the DNS cache.
Prefer SSL VPN DNS	When disabled, EMS does not add the custom DNS server from SSL VPN to the physical interface. When enabled, EMS prepends the custom DNS server from SSL VPN to the physical interface.
Do Not Accept Invalid Server Certificate	FortiClient does not complete the requested VPN connection when an invalid VPN server certificate is used.
Enable Invalid Server Certificate Warning	FortiClient displays a warning to the user when an invalid SSL VPN certificate is used.
Register the Address in DNS	Configure one of the following: • FortiClient registers the VPN adapter's address in the Active Directory (AD) DNS server. • FortiClient does not register the VPN adapter's address in the AD DNS server. • FortiClient registers only its own tunnel interface IP address in the AD DNS server.
Preferred DTLS Tunnel	DTLS tunnel uses UDP instead of TCP and can increase throughput over VPN. Only FortiClient (Windows) supports DTLS. • When enabled, FortiClient uses DTLS if it is enabled on the FortiGate and tunnel establishment succeeds. If dtls-tunnel is disabled on the FortiGate, or tunnel establishment does not succeed, FortiClient uses TLS. • When disabled, FortiClient uses TLS, even if dtls-tunnel is enabled on the FortiGate.
Split Tunnel Route Metric	Set route metric for certain subnet as needed. For example, you may want to set negative split routes with a higher metric, so these routes can be deactivated when another VPN product is being used and sets the same routes as FortiClient negatives split routes but with a lower metric. This configuration is not recommended for most use cases. This element only takes effect when you enable negative split tunnel.

Configuration	Description
Show Auth Certificates Only	Suppress dialogs from displaying certificates that do not bear OID "1.3.6.1.5.5.7.3.2" (client authentication).
Block IPv6	Blocks IPv6 when connected to an IPv4 tunnel. This option is unsupported on FortiClient (Linux).

When you click the *Add Tunnel* button in the *VPN Tunnels* section, you can create an SSL VPN tunnel using manual configuration or XML. For details on configuring a VPN tunnel using XML, see VPN. The following options are available for manual SSL VPN tunnel creation:

Basic Settings	
Name	Enter a VPN name. Use only standard alphanumeric characters. Do not use symbols or accented characters.
Type	Select *SSL VPN*.
Remote Gateway	Enter the remote gateway IP address/hostname. You can configure multiple remote gateways by clicking the + button. If one gateway is not available, the tunnel connects to the next configured gateway.
Port	Enter the access port. The default port is 443.
Linux Smart Card Certificate	Enter the name or path of a shared library on a Linux machine where FortiClient can find a smart card certificate to authenticate the connection. For example, you could enter `/usr/lib/sample.so`.
Require Certificate	Require a certificate.
Android Certificate Location	Configure a certificate location for FortiClient (Android) to automatically go to when doing the following: • When selecting a certificate • When the user clicks *Connect* to connect to this tunnel See Certificate path configuration for automated certificate selection on page 191.
Prompt for Username	Prompt for the username when accessing VPN.
Pinned Tunnel	When a tunnel is pinned, the end user cannot manually unpin it from the FortiClient GUI. All pinned tunnels display in the *Remote Access* tab in FortiClient. In the *VPN Tunnels* list on the *Remote Access* profile, pinned tunnels display with a thumbtack icon. The EMS administrator can pin a maximum of three tunnels per profile. The end user may pin an additional tunnel in FortiClient. FortiClient therefore supports pinning a maximum of four tunnels.
Persistent Connection	Enable to allow the VPN tunnel to remain connected if it is already connected. This is useful when there is a temporary network disconnection that causes the tunnel to drop the connection. An EMS-pushed tunnel with *Persistent Connection* enabled displays with *Save Password* and *Always Up* enabled and grayed out in the FortiClient GUI.
Split Tunnel	

Application Based		Enable application-based split tunnel. FortiClient (Windows) supports source application-based split tunnel, where you can specify which application traffic to exclude from or include in the VPN tunnel. You can exclude high bandwidth-consuming applications for improved performance. For example, you can exclude applications like the following from the VPN tunnel: • Microsoft Office 365 • Microsoft Teams • Skype • GoToMeeting • Zoom • WebEx • YouTube Once the VPN tunnel is up, FortiClient binds the specified excluded applications to the physical interface.
	Type	Select *Include* or *Exclude* to configure whether to include or exclude certain application traffic from the VPN tunnel.
	Local Applications	You can only exclude local applications from the VPN tunnel. Click *Add*. In the *Add Application(s)* field, specify which application traffic to exclude from the VPN tunnel and redirect to the endpoint physical interface. You can specify an application using its process name, full path, or the directory where it is installed. When entering the directory, you must end the value with \. You can enter file and directory paths using environment variables, such as %LOCALAPPDATA%, %programfiles%, and %appdata%. Do not use spaces in the tail or head, or add double quotes to full paths with spaces. You can add multiple entries by separating them with a semicolon. For example, to exclude Microsoft Teams and Firefox from the VPN tunnel, you can enter any of the following combinations: • Application Name: teams.exe;firefox.exe • Full Path: C:\Users\<username>appData\Local\Microsoft\Teams\current\Teams.exe;C:\Program Files\Mozilla Firefox\firefox.exe • Directory: C:\Users\<username>appData\Local\Microsoft\Teams\current\;C:\Program Files\Mozilla Firefox\ To find a running application's full path, on the *Details* tab in Task Manager, add the *Image path name* column. Select the application checkbox, then click *Remove* to remove it from the list.
	Cloud Applications	You can exclude or include cloud applications. Click *Add*. In the list, select the desired applications, then click *Add*. Select the application checkbox, then click *Remove* to remove it from the list.
	Domain	You can exclude or include domains. After you exclude a domain, any associated traffic does not go through the VPN tunnel when accessed through a popular browser such as Chrome, Edge, or Firefox. Click *Add*. In the *Add Domain(s)* field, enter the desired domains, using ; to configure multiple entries.

	For example, if you configure the VPN tunnel to exclude youtube.com, youtube.com and *.youtube.com are excluded from the tunnel. Select the application checkbox, then click *Remove* to remove it from the list.
Advanced Settings	
Enable Single User Mode	Enable single user mode.
Save Username	Save your username.
Allow Non-Administrators to Use Machine Certificates	Allow non-administrator users to use local machine certificates.
Enforce Acceptance of Disclaimer Message	Enable and enter a disclaimer message that appears when the user attempts VPN connection. The user must accept the message to allow connection.
Single Sign On Settings	Enable single sign on login for this VPN tunnel. FortiClient provides an option to the end user to save their VPN login password with or without SAML configured. When using SAML, this feature relies on persistent sessions being configured in the identity provider (IdP), discussed as follows: • Azure • Okta If the IdP does not support persistent sessions, FortiClient cannot save the SAML password. The end user must provide the password to the IdP for each VPN connection attempt. The FortiClient save password feature is commonly used along with autoconnect and always-up features as well. Configure one of the following: • *Use Internal Browser as User-Agent*, *Use External Browser as User-Agent*: Select whether to use the FortiClient internal browser or an external browser to authenticate the user. FortiClient can use a browser as an external user-agent to perform SAML authentication for VPN tunnel mode instead of the FortiClient embedded login window. If a user already authenticated using SAML in the default browser, they do not need to reauthenticate in the FortiClient built-in browser. Available if you enable *Enable Single Sign On (SSO) for VPN Tunnel*. See Using a browser as an external user-agent for SAML authentication in an SSL VPN connection. On FortiClient (macOS), if *Non-Secure site connections > Warn before connecting to a website over HTTP* is enabled in Safari and using an external browser for SAML authentication is configured, VPN connection may fail. • *Auto Login with Azure Active Directory*: configure FortiClient to automatically connect to a specified VPN tunnel immediately after it installs and receives its configuration from EMS, authenticating the connection using Microsoft Entra ID credentials. Configure the Entra ID tenant name and client ID as required. See Autoconnect on logging in as an Entra ID user on page 172.

	The <before_logon_saml_auth> and <after_logon_saml_auth> XML options affect how FortiClient presents SAML authentication in the GUI. See VPN options.
FQDN Resolution Persistence	Enable FortiClient to remember the IP address with which it contacts the FortiGate and reuse it throughout the connection phase. This feature helps support load balancing SSL VPN gateways with one FQDN. This feature is only available for FortiClient (Windows). See Load balancing SSL VPN gateways with one FQDN on page 187.
Resolve to IPv4 Only	If the SSL VPN gateway FQDN resolves to both IPv4 and IPv6 addresses, this option forces FortiClient to use the IPv4 address to access the SSL VPN gateway. When this option is disabled, FortiClient may use the IPv4 or IPv6 address to access the SSL VPN gateway.
Redundant Sort Method	How FortiClient determines the order in which to try connection to the SSL VPN servers when more than one is defined. FortiClient calculates the order before each SSL VPN connection attempt. When *Server* is selected, FortiClient tries the order explicitly defined in the server settings. When *Ping Speed* is selected, FortiClient determines the order by the ping response speed. When *TCP Round Trip Time* is selected, FortiClient determines the order by the TCP round trip time.
Tags	Select *Allow* or *Prohibit*, then select the desired security posture tag from the *Select a Tag* dropdown list. Tags only display in the list if they are already configured. See Security Posture Tags on page 408. You can use this feature to prohibit endpoints from connecting to the VPN tunnel when they do not meet certain criteria. For example, if you want to prohibit endpoints without up-to-date antivirus signatures from connecting to the VPN tunnel, you would do the following: 1. Configure a security posture tagging rule that tags all endpoints without up-to-date AV signatures. See Adding a security posture tag on page 408. 2. For the VPN tunnel settings, select *Prohibit*, then select the configured tag from the *Select a Tag* dropdown list. Endpoints without up-to-date AV signatures are prohibited from connecting to the VPN tunnel.
Customize Host Check Fail Warning	Enable and configure a custom message to display to the user when EMS prohibits the endpoint from connecting to the VPN tunnel due to its applied security posture tag. For the example configuration described in the *Host Tag* field description, you could configure a custom message to direct the user to update their AV signature, so that they can connect to the VPN tunnel afterward.
Show "Remember Password" Option	Show option to have the VPN tunnel remember the password. You must also enable this option on the FortiGate.

Show "Always Up" Option	Show option to have the VPN tunnel always up. You must also enable this option on the FortiGate.
Show "Auto Connect" Option	Automatically connect the VPN tunnel. You must also enable this option on the FortiGate. Automatic connection to the VPN tunnel may fail if the endpoint boots up with a user profile set to automatic logon.
On Connect Script	Enable the on connect script. Enter your script.
On Disconnect Script	Enable the disconnect script. Enter your script.

IPsec VPN



FortiClient 7.4.4 and later versions do not support IPsec VPN IKEv1. Configure IPsec VPN IKEv2 if using FortiClient 7.4.4 and later versions.

This topic contains descriptions of IPsec VPN settings:

Configuration	Description
VPN If you enable SSL VPN, this pane displays as *IPsec VPN*.	Enable IPsec VPN.
Beep If Connection Fails	Device beeps if connection to the IPsec VPN tunnel fails.
Use Windows Store Certificates	Enable using Windows store certificates.
Current User Windows Store Certificates	Certificates from the user store display.
Local Computer Windows Store Certificates	Certificates from the computer store display.
Use Smart Card Certificates	Shows certificates on smartcards.
Show Auth Certificates Only	Only shows certificates with authentication in certificate features.
Block IPv6	Blocks IPv6 traffic sent outside of VPN interface when connected to an IPv4 full tunnel.

Configuration	Description
	 This option does not support the following: • FortiClient (Linux) • FortiClient 7.4.4 and 7.4.5 (due to lack of IPv6 support for IPsec VPN)
Enable UDP Checksum	Add checksum to UDP packets.
Disable Default Route	Disable default route to gateway.
Check for Certificate Private Key	Does not show certificates if the private key is not directly accessible, such as for smartcards.
Enhanced Key Usage Mandatory	Lists only certificates with private keys that allow enhanced key usage.
Register the Address in DNS	Configure one of the following: • FortiClient registers the VPN adapter's address in the Active Directory (AD) DNS server. • FortiClient does not register the VPN adapter's address in the AD DNS server. • FortiClient registers only its own tunnel interface IP address in the AD DNS server.
Do Not Accept Invalid Server Certificate for SAML auth	FortiClient does not complete the requested VPN connection when an invalid VPN server certificate is used for SAML authentication. To perform a certificate check on an IPsec tunnel using authmethod signature, use the *Validate IKE Phase1 cert hostname* option or `<cert_subjectcheck>` XML tag (see IKE settings).

When you click *Add Tunnel* in *VPN Tunnels*, you can create an IPsec VPN tunnel using manual configuration or XML. For details on configuring a VPN tunnel using XML, see VPN. The following options are available for manual IPsec VPN tunnel creation:

Field	Description
Basic Settings	
Name	Enter a VPN tunnel name. Use only standard alphanumeric characters. Do not use symbols or accented characters.
Type	Displays if you enabled SSL VPN on EMS. Select *IPsec VPN*.
Remote Gateway	Enter the remote gateway IP address or hostname. You can configure multiple remote gateways by clicking *+*. If a gateway is unavailable, the tunnel connects to the next configured gateway.
Authentication Method	Select the authentication method for the tunnel.

Field	Description
Android Certificate Location	Configure a certificate location for FortiClient (Android) to automatically go to when selecting a certificate. Available if you selected *Smart Card Certificate* or *System Store Certificate* for *Authentication Method*. See Certificate path configuration for automated certificate selection on page 191.
Pre-Shared Key	Enter the preshared key required. Available if you selected *Pre-Shared Key* for *Authentication Method*.
Prompt for Username	Prompt for the username when accessing VPN.
Pinned Tunnel	When a tunnel is pinned, the end user cannot manually unpin it from the FortiClient GUI. All pinned tunnels display in the *Remote Access* tab in FortiClient. In the *VPN Tunnels* list on the *Remote Access* profile, pinned tunnels display with a thumbtack icon. The EMS administrator can pin a maximum of three tunnels per profile. The end user may pin an additional tunnel in FortiClient. FortiClient therefore supports pinning a maximum of four tunnels.
Persistent Connection	Enable to allow the VPN tunnel to remain connected if it is already connected. This is useful when there is a temporary network disconnection that causes the tunnel to drop the connection. An EMS-pushed tunnel with *Persistent Connection* enabled displays with *Save Password* and *Always Up* enabled and grayed out in the FortiClient GUI.

Validate IKE Phase1 cert hostname	When enabled, if the CN type of the server certificate is FQDN (see FortiOS documentation), FortiClient validates the remote gateway hostname to match the CN in the subject field of the server certificate of the IPsec phase1 interface, which is configured on the FortiGate under the following command:
	`config vpn ipsec phase1-interface`
	`edit "<interface>"`
	`set authmethod signature`
	`set certificate "<certificate>"`
	`next`
	`end`
	If there is no match, the VPN connection does not succeed.
	This option is available only if *Authentication Method* is not *Pre Shared Key*.

Split Tunnel	

Field		Description
Application Based		Enable application-based split tunnel. FortiClient (Windows) supports source application-based split tunnel, where you can specify which application traffic to exclude from or include in the VPN tunnel. You can exclude high bandwidth-consuming applications for improved performance. For example, you can exclude applications like the following from the VPN tunnel: • Microsoft Office 365 • Microsoft Teams • Skype • GoToMeeting • Zoom • WebEx • YouTube Once the VPN tunnel is up, FortiClient binds the specified excluded applications to the physical interface.
	Type	Select *Include* or *Exclude* to configure whether to include or exclude certain application traffic from the VPN tunnel.
	Local Applications	You can only exclude local applications from the VPN tunnel. Click *Add*. In the *Add Application(s)* field, specify which application traffic to exclude from the VPN tunnel and redirect to the endpoint physical interface. You can specify an application using its process name, full path, or the directory where it is installed. When entering the directory, you must end the value with \. You can enter file and directory paths using environment variables, such as %LOCALAPPDATA%, %programfiles%, and %appdata%. Do not use spaces in the tail or head, or add double quotes to full paths with spaces. You can add multiple entries by separating them with a semicolon. For example, to exclude Microsoft Teams and Firefox from the VPN tunnel, you can enter any of the following combinations: • Application Name: teams.exe;firefox.exe • Full Path: C:\Users\<username>appData\Local\Microsoft\Teams\current\Teams.exe;C:\Program Files\Mozilla Firefox\firefox.exe • Directory: C:\Users\<username>appData\Local\Microsoft\Teams\current\;C:\Program Files\Mozilla Firefox\ To find a running application's full path, on the *Details* tab in Task Manager, add the *Image path name* column. Select the application checkbox, then click *Remove* to remove it from the list.
	Cloud Applications	You can exclude or include cloud applications. Click *Add*. In the list, select the desired applications, then click *Add*. Select the application checkbox, then click *Remove* to remove it from the list.

Field	Description
Domain	You can exclude or include domains. After you exclude a domain, any associated traffic does not go through the VPN tunnel when accessed through a popular browser such as Chrome, Edge, or Firefox. Click *Add*. In the *Add Domain(s)* field, enter the desired domains, using ; to configure multiple entries. For example, if you configure the VPN tunnel to exclude youtube.com, youtube.com and *.youtube.com are excluded from the tunnel. Select the application checkbox, then click *Remove* to remove it from the list.
VPN Settings	
IKE	Select *Version 1* or *Version 2*. FortiClient 7.4.4 and later versions do not support IPsec VPN IKEv1. Configure IPsec VPN IKEv2 if using FortiClient 7.4.4 and later versions.
Mode	Select *Main* or *Aggressive*.
Address Assignment	Select *Mode Config*, *Manual Set*, or *DHCP over IPsec*.

Encapsulation	Available if you select *Version 2* for *IKE*. Configure one of the following for the encapsulation (or transport) mode:
	• *IKE UDP Port*: UDP encapsulation (transport) mode. This is the default and used for most VPN connections. Configure a custom port number if desired. If you select this option, you only need to configure the *IKE UDP Port* field and do not need to configure *IKE TCP Port*. The value for *IKE UDP Port* should match the port number configured on FortiOS via the following command:
	`config system settings`
	`  set ike-port 500`
	`end`
	After IKE packets are negotiated over UDP on the configured port, if no NAT is detected and ESP packets are allowed to pass through the internet, ESP packets do not need to be encapsulated inside UDP headers. In this scenario, the recommended setting on FortiOS is `set nattraversal disable`, as disabling NAT-T avoids the additional overhead of encapsulating and decapsulating ESP packets. This typically provides optimal VPN performance on the endpoint and FortiGate when NAT-T is unneeded. The implicitly configured XML tags for this mode are as follows:
	  • `<nat_traversal>0</nat_traversal>`
	  • `<transport_mode>0</transport_mode>`
	  • `<udp_port>500</udp_port>`
	If NAT is detected and you prefer NAT-T with ESP encapsulation over UDP, consider using *Auto* mode as the following describes. In auto mode, once the IKE negotiation completes, ESP packets are transferred over UDP on the default port (UDP/4500).
	• *IPsec over TCP*: TCP transport mode. This is recommended for use in

Field	Description

	restrictive networks. Configure a custom port number if desired. If you select this mode, you only need to configure the *IKE TCP Port* field and do not need to configure *IKE UDP Port*. The value for *IKE TCP Port* should match the port number configured on FortiOS via the following command:
	`config system settings`
	`set ike-tcp-port 443`
	`end`
	Use this mode when NAT is detected or if both UDP and ESP are blocked. In this scenario, IKE and ESP packets are encapsulated inside TCP, typically on port 443, to ensure the traffic can pass through strict network environments. The implicitly configured XML tags for this mode are as follows:
	• `<nat_traversal>1</nat_traversal>`
	• `<transport_mode>1</transport_mode>`
	• `<tcp_port>443</tcp_port>`
	• *Auto*: if you select *Auto*, you must configure both the *IKE UDP Port* and *IKE TCP Port* fields. The values must match those set on FortiOS using the following commands:
	`config system settings`
	`set ike-port 500`
	`set ike-tcp-port 443`
	`end`
	You must also configure the following phase 1 settings on FortiOS 7.4.2 and later versions:
	`config vpn ipsec phase1`
	`edit`
	`set nattraversal forced`
	`set transport udp-fallback-tcp`
	`next`
	`end`
	On FortiOS 7.6, you can configure the following phase 1 settings:
	`config vpn ipsec phase1`
	`edit`
	`set nattraversal forced`
	`set transport auto`
	`next`
	`end`
	If using FortiOS 7.4.1 or an earlier version, FortiClient will connect to IPsec VPN using UDP mode as `udp-fallback-tcp` and `auto` are not available.
	This mode dynamically uses UDP or TCP based on network conditions and NAT detection, automatically falling back to TCP/443 if UDP or ESP traffic is blocked. The implicitly configured XML tags for this mode are as follows:
	• `<nat_traversal>1</nat_traversal>`
	• `<transport_mode>2</transport_mode>`

Field		Description
		• `<tcp_port>443</tcp_port>` • `<udp_port>443</udp_port>`
	IKE TCP Port	Available if you select *Auto* for *Encapsulation*. Configure a custom port number if desired.
	IKE UDP Port	Available if you select *Auto* for *Encapsulation*. Configure a custom port number if desired.
Specify DNS Server (IPv4)		Specify the DNS server for the VPN tunnel. Available if you selected *Manual Set*.
Assign IP Address (IPv4)		Enter the IP address to assign for the VPN tunnel. Available if you selected *Manual Set*.
Split Table		Enter the IP address and subnet mask for the VPN tunnel. Available if you selected *Manual Set* or *DHCP over IPsec*.
Phase 1		Select the encryption and authentication algorithms used to generate keys for protecting negotiations and add encryption and authentication algorithms as required. You need to select a minimum of one and a maximum of two combinations. The remote peer or client must be configured to use at least one of the proposals that you define.
Encryption		Select the encryption standard.  FortiClient macOS does not support the DES encryption. If the DES encryption selected, FortiClient macOS uses AES-256 instead.
Authentication		Select the authentication method.
DH Groups		Select one or more Diffie-Hellman (DH) groups from groups 1, 2, 5, 14, 15, 16, 17, 18, 19, 20, and 21. At least one of the selected groups on the remote peer or client must match one of the selections on the FortiGate. Failure to match one or more DH groups results in failed negotiations.
Key Life		Enter the time (in seconds) that must pass before the IKE encryption key expires. When the key expires, a new key is generated without interrupting service. The key life can be from 120 to 172,800 seconds.
Local ID		Enter the local ID.
Network ID		Configure a network ID value between 0 to 255 to differentiate between multiple IKEv2 certificate-based phase 1 tunnels. See FortiOS documentation for more details. The network ID is a Fortinet proprietary attribute used to select the correct phase 1 between IPsec peers, so that multiple IKEv2 tunnels can be established between the same local/remote gateway pairs.

Field	Description
	In a dial-up VPN, network-id is in the first initiator message of an IKEv2 phase 1 negotiation. The responder (hub) uses the network-id to match a phase 1 configuration with a matching network-id. The hub can then differentiate multiple dial-up phase 1s that are bound to the same underlay interface and IP address. Without a network-id, the hub cannot have multiple phase 1 dialup tunnels on the same interface. In static phase 1 configurations, network-id is used with the pair of gateway IPs to negotiate the correct tunnel with a matching network-id. This allows IPsec peers to use the same pair of underlay IPs to establish multiple IPsec tunnels. Without it, only a single tunnel can be established over the same pair of underlay IPs.  The *Network ID* attribute is not supported on FortiClient iOS or Android.
EAP Authentication Method	Select one of the following EAP authentication methods: • *EAP-MSCHAPv2* (default) • *EAP-TTLS*—For LDAP-based user authentication using IKEv2, the EAP-TTLS authentication method allows credentials to be securely transmitted to FortiGate over a TLS tunnel and ensures secure user authentication. FortiClient (iOS) and (Android) do not support EAP-TTLS/PAP authentication.
Enable Implied SPDO	Enable implied SPDO. Enter the timeout in seconds.
Dead Peer Detection	Select this checkbox to reestablish VPN tunnels on idle connections and clean up dead IKE peers if required.
NAT Traversal	Select the checkbox if a NAT device exists between the client and the local FortiGate. The client and the local FortiGate must have the same NAT traversal setting (both selected or both cleared) to connect reliably.
Enable Local LAN	Enable local LAN.
Enable IKE Fragmentation	Enable support of fragmented IKE packets to avoid packet loss and ensure reliable IPsec VPN tunnel establishment. See the following for more details: • IKE fragmentation example • *IKEv1 fragmentation* and *IKEv2 fragmentation* sections in FortiOS documentation for more details.
Allow non-administrators to use machine certificates	Allow non-administrator users to use local machine certificates to connect IPsec VPN.

Field	Description
Phase 2	Select the encryption and authentication algorithms that to propose to the remote VPN peer. You can specify up to two proposals. To establish a VPN connection, at least one of the proposals that you specify must match configuration on the remote peer.
Encryption	Select the encryption standard.
Authentication	Select the authentication method.
DH Group	Select one DH group (1, 2, 5, 14, 15, 16, 17, 18, 19, 20, or 21). This must match the DH group that the remote peer or dialup client uses.
Key Life	Set a limit on the length of time that a phase 2 key can be used. The default units are seconds. Alternatively, you can set a limit on the number of kilobytes (KB) of processed data, or both. If you select both, the key expires when the time has passed or the number of KB have been processed. When the phase 2 key expires, a new key is generated without interrupting service.
Enable Replay Detection	Replay detection enables the unit to check all IPsec packets to see if they have been received before. If any encrypted packets arrive out of order, the unit discards them.
Enable Perfect Forward Secrecy (PFS)	Enable PFS. PFS forces a new DH exchange when the tunnel starts and whenever the phase 2 key life expires, causing a new key to be generated each time.
Negative Split Tunnel or Network Exclusion	Configure negative split tunnel or network exclusion for IPsec VPN. You can specify one or multiple subnets or FQDNs resolved from the client and expanded into a list of networks. For example: • 10.10.10.0/255.255.255.0 • 13.106.56.0/25 • `teams.microsoft.com` If negative split tunnel configuration is also received from FortiOS, FortiEndpoint uses the settings from FortiOS and ignores this setting. See Configure VPN remote gateway.
Advanced Settings	
Enable One-Time Password	Enable one-time password.
Enable XAuth	When IKEv1 is selected, enable IKE Extended Authentication (xAuth). When IKEv2 is selected, enable Extensible Authentication Protocol (EAP).
XAuth Timeout	Only available if *Enable XAuth* is enabled. Configure the timeout in seconds. Default value is two minutes if not configured. Enter a value between 120 and 300 seconds.
Prompt for Certificate	Prompt the user for the certificate.
Enable Single User Mode	Enable single user mode.

Field	Description
Show Passcode	Display Passcode instead of Password in the *VPN* tab in FortiClient.
Save Username	Save your username.
Enforce Acceptance of Disclaimer Message	Enable and enter a disclaimer message that appears when the user attempts VPN connection. The user must accept the message to allow connection.
Single Sign On Settings	Enable single sign on login for this VPN tunnel. FortiClient provides an option to the end user to save their VPN login password with or without SAML configured. When using SAML, this feature relies on persistent sessions being configured in the identity provider (IdP), discussed as follows: • Azure • Okta If the IdP does not support persistent sessions, FortiClient cannot save the SAML password. The end user must provide the password to the IdP for each VPN connection attempt. The FortiClient save password feature is commonly used along with autoconnect and always-up features as well. Configure one of the following: • *Use Internal Browser as User-Agent*, *Use External Browser as User-Agent*: Select whether to use the FortiClient internal browser or an external browser to authenticate the user. Using an external browser is only available for IKEv2 tunnels. FortiClient can use a browser as an external user-agent to perform SAML authentication for VPN tunnel mode instead of the FortiClient embedded login window. If a user already authenticated using SAML in the default browser, they do not need to reauthenticate in the FortiClient built-in browser. Available if you enable *Enable Single Sign On (SSO) for VPN Tunnel*. See Using a browser as an external user-agent for SAML authentication in an SSL VPN connection. On FortiClient (macOS), if *Non-Secure site connections > Warn before connecting to a website over HTTP* is enabled in Safari and using an external browser for SAML authentication is configured, VPN connection may fail. • *Auto Login with Azure Active Directory*: configure FortiClient to automatically connect to a specified VPN tunnel immediately after it installs and receives its configuration from EMS, authenticating the connection using Microsoft Entra ID credentials. Configure the Entra ID tenant name and client ID as required. Enter the port number that FortiClient uses to communicate with the FortiGate, which acts as the SAML service provider. See Autoconnect on logging in as an Entra ID user on page 172.

Field	Description
FQDN Resolution Persistence	Enable FortiClient to remember the IP address with which it contacts the FortiGate and reuse it throughout the connection phase. This feature helps support load balancing gateways with one FQDN. This feature is only available for FortiClient (Windows). See Load balancing SSL VPN gateways with one FQDN on page 187.
Failover SSL VPN Connection	If the IPsec VPN connection fails, FortiClient attempts to connect to the specified SSL VPN tunnel.
Redundant Sort Method	How FortiClient determines the order in which to try connection to the IPsec VPN servers when more than one is defined. FortiClient calculates the order before each IPsec VPN connection attempt. When *Server* is selected, FortiClient tries the order explicitly defined in the server settings. When *Ping Speed* is selected, FortiClient determines the order by the ping response speed. When *TCP Round Trip Time* is selected, FortiClient determines the order by the TCP round trip time.
Tags	Select *Allow* or *Prohibit*, then select the desired security posture tag from the *Select a Tag* dropdown list. Tags only display in the list if they are already configured. See Security Posture Tags on page 408. You can use this feature to prohibit endpoints from connecting to the VPN tunnel when they do not meet certain criteria. For example, if you want to prohibit endpoints without up-to-date antivirus signatures from connecting to the VPN tunnel, you would do the following: 1. Configure a security posture tagging rule that tags all endpoints without up-to-date AV signatures. See Adding a security posture tag on page 408. 2. For the VPN tunnel settings, select *Prohibit*, then select the configured tag from the *Select a Tag* dropdown list. Endpoints without up-to-date AV signatures are prohibited from connecting to the VPN tunnel.
Customize Host Check Fail Warning	Enable and configure a custom message to display to the user when EMS prohibits the endpoint from connecting to the VPN tunnel due to its applied security posture tag. For the example configuration described in the *Host Tag* field description, you could configure a custom message to direct the user to update their AV signature, so that they can connect to the VPN tunnel afterward.
Show "Remember Password" Option	Show option to have the VPN tunnel remember the password. You must also enable this option on the FortiGate.
Show "Always Up" Option	Show option to have the VPN tunnel always up. You must also enable this option on the FortiGate.

Field	Description
Show "Auto Connect" Option	Automatically connect the VPN tunnel. You must also enable this option on the FortiGate. Automatic connection to the VPN tunnel may fail if the endpoint boots up with a user profile set to automatic logon.
On Connect Script	Enable the on connect script. Enter your script.
On Disconnect Script	Enable the disconnect script. Enter your script.

Configuring a profile with application-based split tunnel

FortiClient (Windows) supports source application-based split tunnel, where you can specify which application traffic to exclude from the VPN tunnel. For example, you can exclude high bandwidth-consuming applications like the following from the VPN tunnel:

- Microsoft Office 365
- Microsoft Teams
- Skype
- GoToMeeting
- Zoom
- WebEx
- YouTube



- Source application-based split tunnel does not support IPv6 or explicitly including traffic in the VPN tunnel.
- FortiClient (macOS) and (Linux) do not support source application-based split tunnel.

You must configure these settings in the endpoint profile in EMS. The following instructions assume that you have already configured a remote IPsec or SSL VPN server in FortiOS. See the FortiOS documentation.

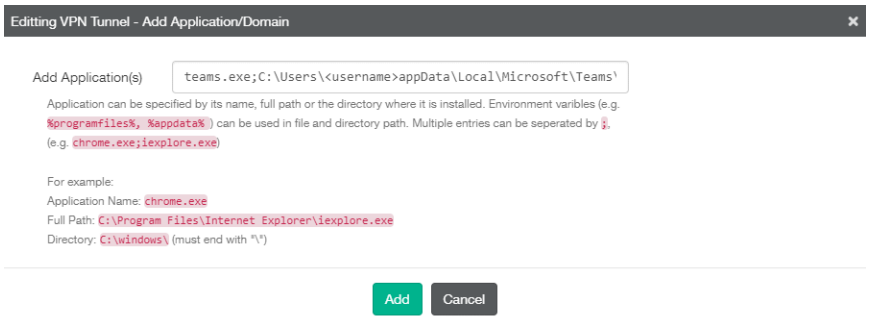
To configure application-based split tunnel using the GUI:

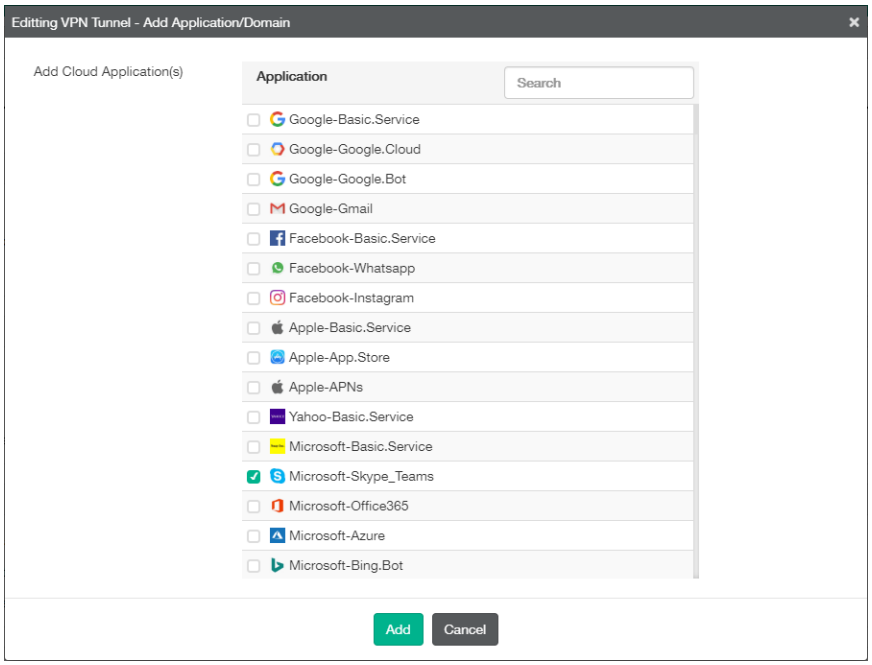
1. In EMS, go to *Endpoint Profiles*, and select the desired profile.
2. On the *VPN* tab, select an existing tunnel or create a new tunnel.
3. Under *Split Tunnel > Application Based*, configure the following fields:

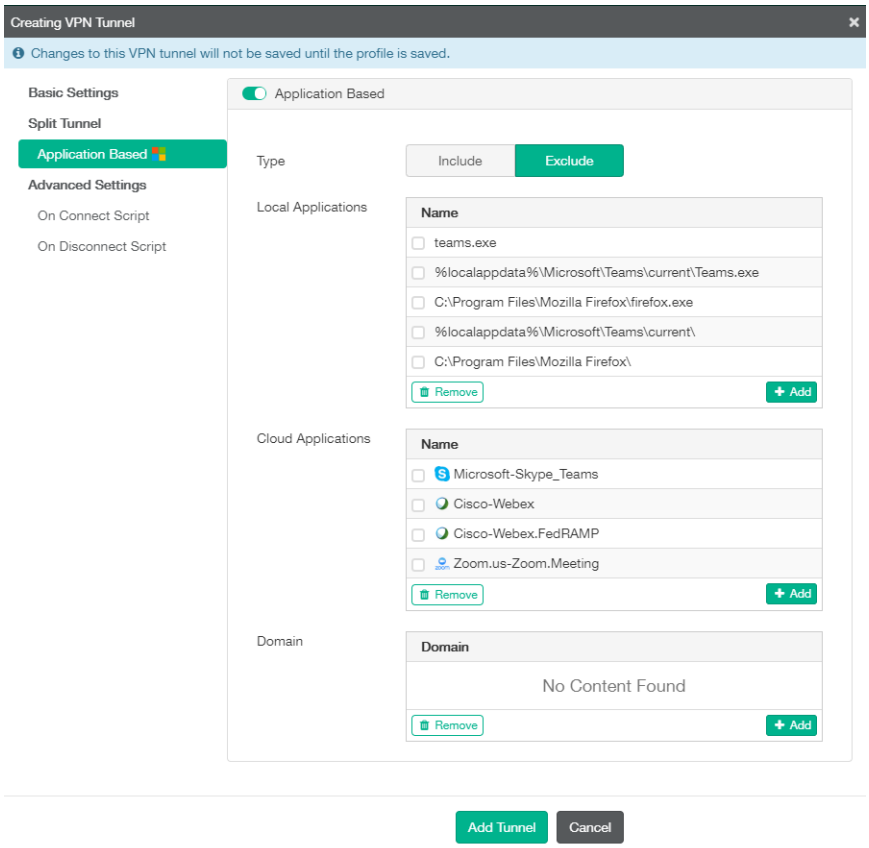
Configuration	Description
Application Based	Enable application-based split tunnel. FortiClient (Windows) supports source application-based split tunnel, where you can specify which application traffic to exclude from the VPN tunnel. You can exclude high bandwidth-consuming applications for improved performance. For example, you can exclude applications like the following from the VPN tunnel: • Microsoft Office 365 • Microsoft Teams

Configuration		Description
		• Skype • GoToMeeting • Zoom • WebEx • YouTube Once the VPN tunnel is up, FortiClient binds the specified excluded applications to the physical interface.
	Type	Select *Exclude* to configure whether to exclude certain application traffic from the VPN tunnel.
	Local Applications	You can only exclude local applications from the VPN tunnel. Click *Add*. In the *Add Application(s)* field, specify which application traffic to exclude from the VPN tunnel and redirect to the endpoint physical interface. You can specify an application using its process name, full path, or the directory where it is installed. When entering the directory, you must end the value with \. You can enter file and directory paths using environment variables, such as %LOCALAPPDATA%, %programfiles%, and %appdata%. Do not use spaces in the tail or head, or add double quotes to full paths with spaces. You can add multiple entries by separating them with a semicolon. For example, to exclude Microsoft Teams and Firefox from the VPN tunnel, you can enter any of the following combinations: • Application Name: teams.exe;firefox.exe • Full Path: %localappdata%\Microsoft\Teams\current\Teams.exe;C:\Program Files\Mozilla Firefox\firefox.exe • Directory: %localappdata%\Microsoft\Teams\current\;C:\Program Files\Mozilla Firefox\ To find a running application's full path, on the *Details* tab in Task Manager, add the *Image path name* column. Select the application checkbox, then click *Remove* to remove it from the list.
	Cloud Applications	You can exclude cloud applications. Click *Add*. In the list, select the desired applications, then click *Add*. Select the application checkbox, then click *Remove* to remove it from the list.
	Domain	You can exclude domains. After you exclude a domain, any associated traffic does not go through the VPN tunnel when accessed through a popular browser such as Chrome, Edge, or Firefox. Click *Add*. In the *Add Domain(s)* field, enter the desired domains, using ; to configure multiple entries. For example, if you configure the VPN tunnel to exclude youtube.com, youtube.com and *.youtube.com are excluded from the tunnel. Select the application checkbox, then click *Remove* to remove it from the list.

This example shows excluding the Microsoft Teams using the application name, full path, and directory. It also excludes Teams and other web conferencing cloud applications, such as Zoom and Cisco WebEx:







4. Assign the profile to the desired endpoints. When VPN is up on those endpoints, FortiClient excludes the application traffic specified in the profile from the VPN tunnel as configured.

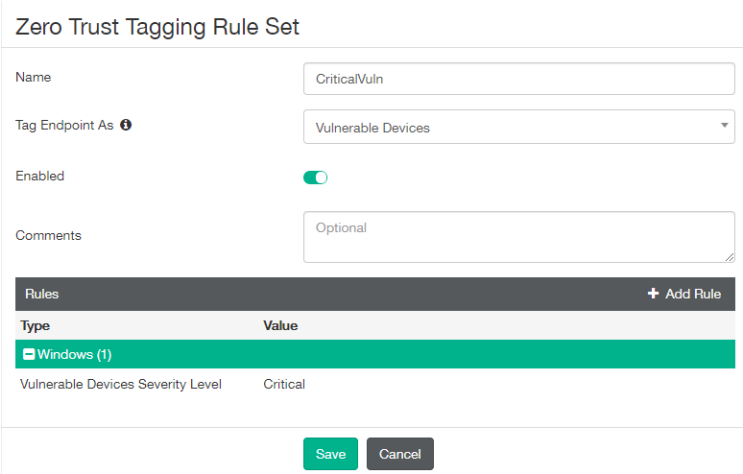
Configuring a profile to allow or block endpoint from VPN tunnel connection based on the applied security posture tag

You can configure a profile to allow or block an endpoint from connecting to a VPN tunnel based on its applied security posture tag. This example describes configuring an endpoint profile to prohibit Windows endpoints with critical vulnerabilities from connecting to VPN.

To configure an endpoint profile to prohibit endpoints with critical vulnerabilities from connecting to VPN:

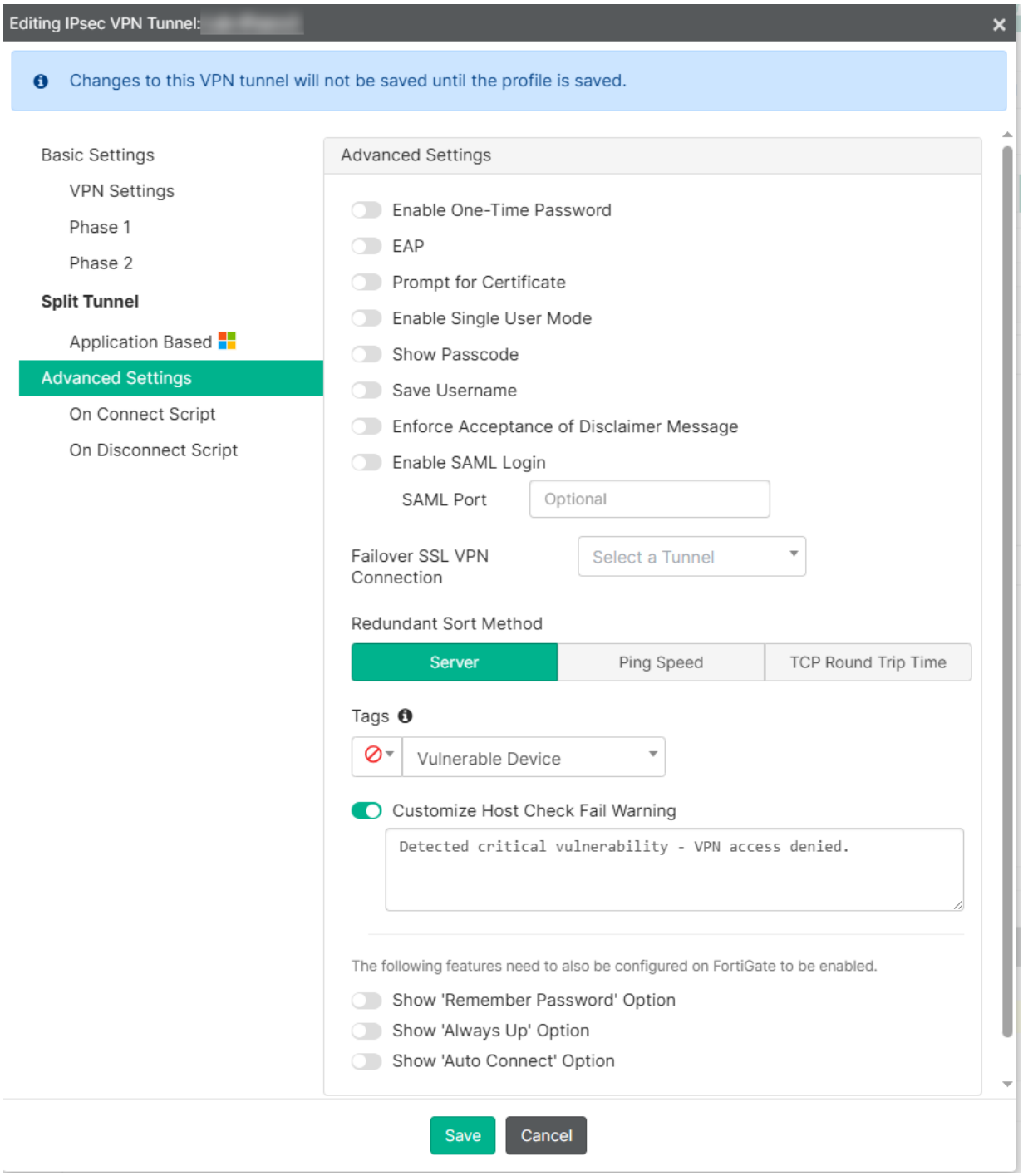
1. Create a security posture tagging rule set that tags endpoints with critical vulnerabilities with the "Vulnerable Devices" tag:
   a. Go to *Security Posture Tags* > *Security Posture Tagging Rules*.
   b. Click *Add*.
   c. In the *Tag Endpoint As* field, create a new "Vulnerable Devices" tag.
   d. Toggle *Enabled* to on.
   e. Click *Add Rule*.
   f. For Windows devices, from the *Rule Type* dropdown list, select *Vulnerable Devices*.
   g. From the *Severity Level* dropdown list, select *Critical*.

h. Click *Save*.
i. Click *Save* again.

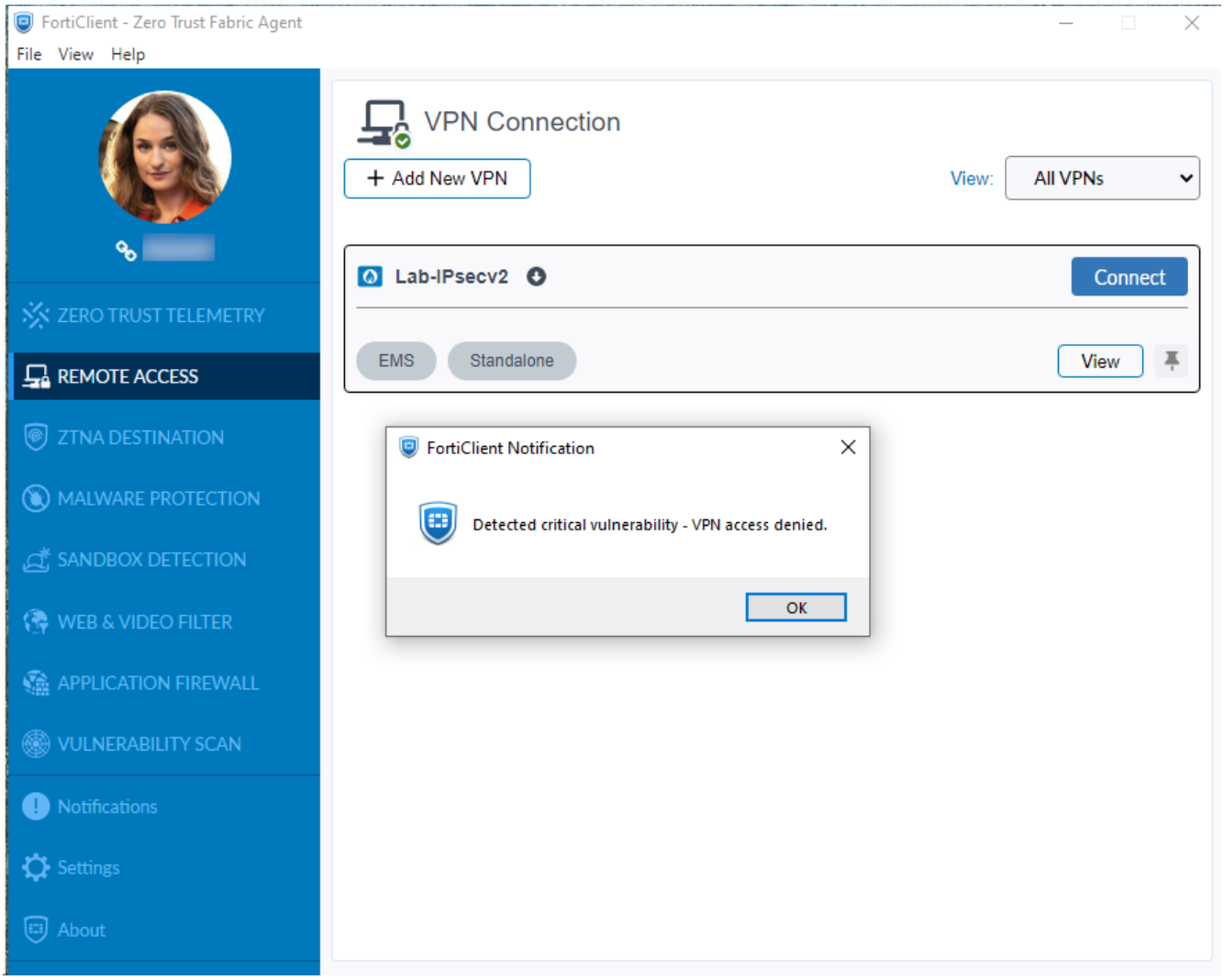


2. Configure the options on the endpoint profile:
   a. Go to *Endpoint Profiles* > *Remote Access*.
   b. Edit the desired profile, or create a new one.
   c. Under *General*, enable *Enable Secure Remote Access*.
   d. Select an existing VPN tunnel, or create a new one by clicking *Add Tunnel*, then *Manual*.
   e. In *Advanced Settings*, for *Tags*, select *Prohibit*.
   f. From the *Select a Tag* dropdown list, select *Vulnerable Device*.
   g. Enable *Customize Host Check Fail Warning*.
   h. Enter a message to display to users when their connection to the VPN tunnel is prohibited due to critical vulnerabilities on their device.
   i. Configure other fields as desired.

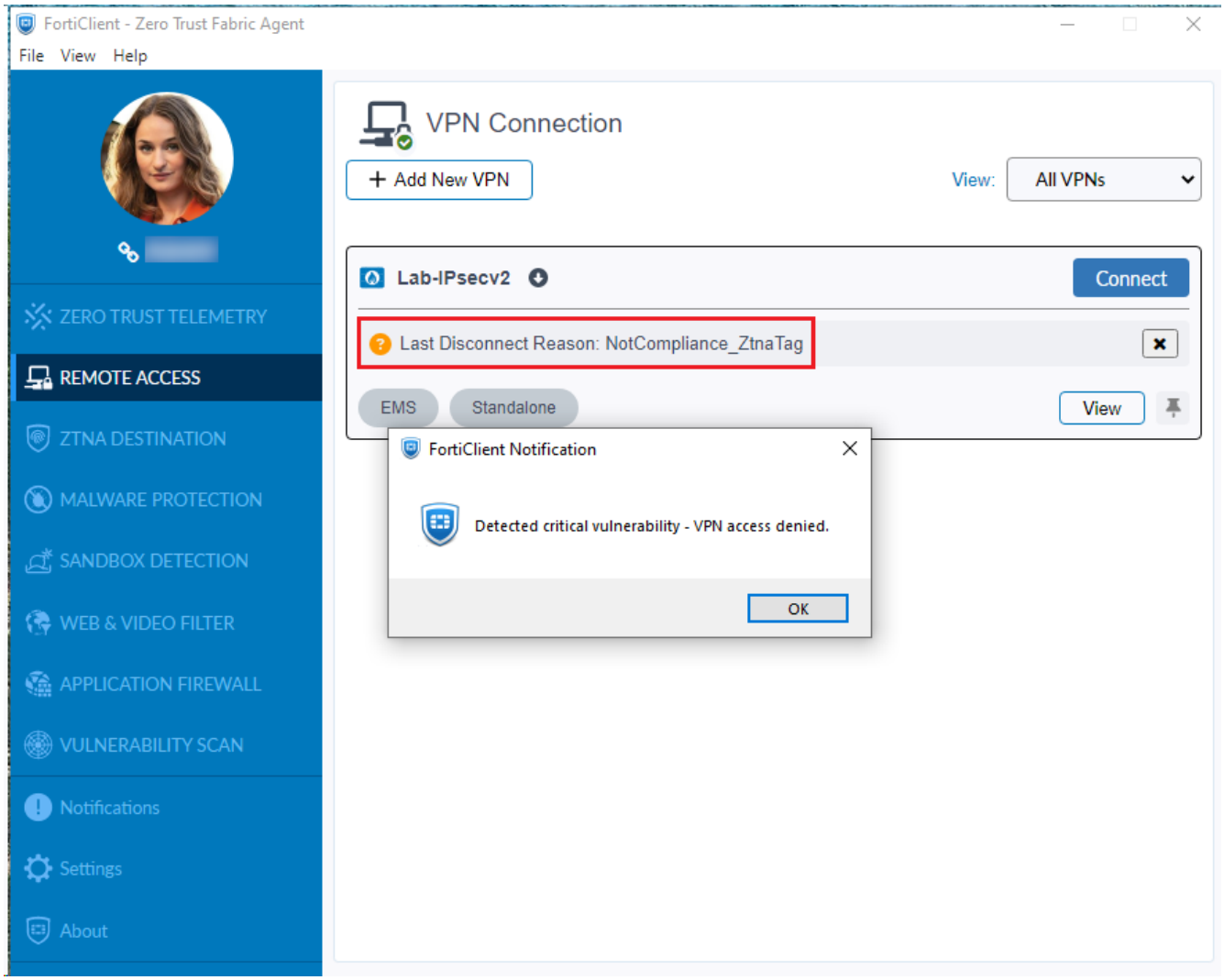
j. Save the configuration.



After the next communication between EMS and FortiClient, endpoints with this profile applied are unable to connect to this VPN tunnel if they have critical vulnerabilities. The following shows the notification that the end user sees when their connection to the VPN tunnel is prohibited due to critical vulnerabilities on their device.



After the end user fixes the vulnerabilities and connects to the VPN successfully, FortiClient periodically checks the tag compliance status of the endpoint to ensure security. If the endpoint has critical vulnerabilities again, FortiClient terminates the VPN connection with the same error and a warning message with the reason of the VPN disconnection:



Configuring a backup VPN connection

You can configure FortiClient to connect to a preconfigured SSL VPN tunnel instead when connection to a configured IPsec VPN tunnel fails. This feature is convenient for connecting to VPN when the IPsec VPN tunnel is blocked or if a public router or gateway is not preforming IPsec VPN NAT correctly.

This guide assumes that the EMS administrator has already configured an SSL VPN tunnel and IPsec VPN tunnel on the desired endpoint profile.

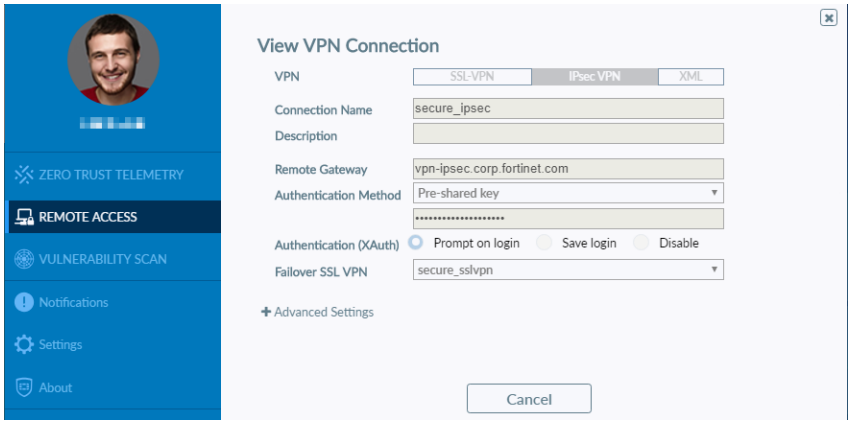
To view and configure SSL VPN settings, you must enable SSL VPN visibility in *System Settings* > *Feature Select*. See Feature Select on page 555.

To configure a backup VPN connection:

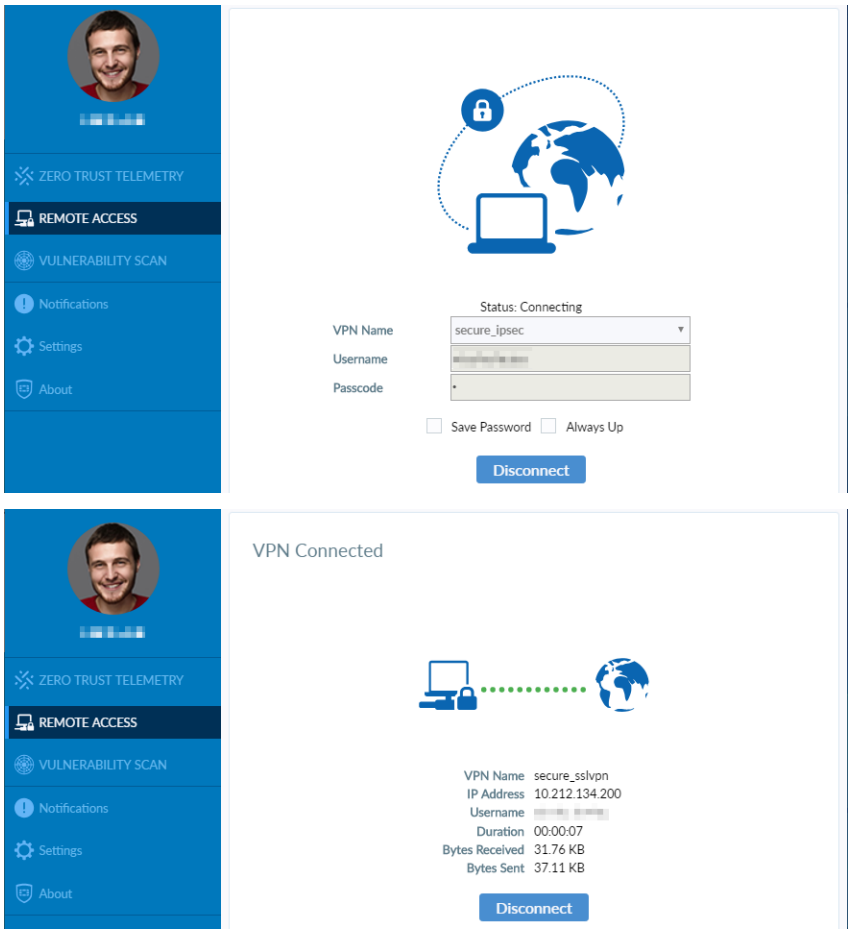
1. Go to *Endpoint Profiles* > *Manage Profiles*.
2. Edit the desired profile, then do one of the following:
   a. Configure this feature from the GUI. Do the following:
      i. Edit the desired IPsec VPN tunnel.
      ii. In *Advanced Settings*, from the *Failover SSL VPN Connection* dropdown list, select the desired SSL VPN connection.
      iii. Click *Save*.
   b. Configure this feature using XML. On the *XML Configuration* tab, configure the following for the desired IPsec VPN tunnel. The following configures the secure_sslvpn tunnel as the backup tunnel:

```
<forticlient_configuration>
   <vpn>
      <ipsecvpn>
         <connections>
            <connection>
               <ike_settings>
                  <failover_sslvpn_connection>SSLVPN HQ</failover_sslvpn_connection>
               <ike_settings>
            <connection>
         <connections>
      <ipsecvpn>
   <vpn>
<forticlient_configuration>
```

      This is a balanced but incomplete XML configuration fragment. It includes all closing tags but omits some important elements to complete the IPsec VPN configuration.
3. After FortiClient receives the next update from EMS, on the *Remote Access* tab, from the *VPN Name* dropdown list, select the IPsec VPN tunnel.
4. Select *View the selected connection*.
5. Verify that the *Failover SSL VPN* field specifies the SSL VPN tunnel configured in step 2.



6. Attempt connection to the IPsec VPN tunnel when you know that it fails. FortiClient automatically connects to the configured SSL VPN tunnel instead.



Using a browser as an external user-agent for SAML authentication in an SSL VPN connection

When establishing an SSL VPN tunnel connection, FortiClient can present a SAML authentication request to the end user in a web browser.

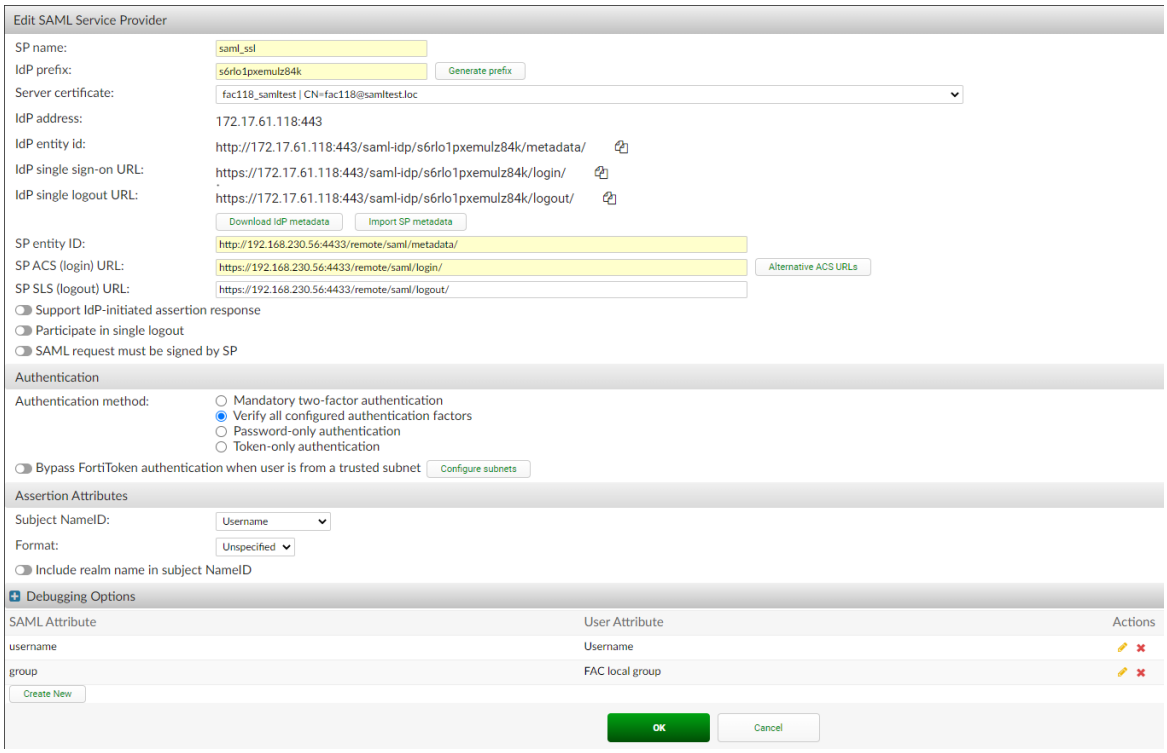
This feature is not supported when SSL VPN realms are configured. When SSL VPN realms are configured and the user provides their SAML authentication credentials in an external browser, FortiClient fails to establish the SSL VPN connection.

The `<before_logon_saml_auth>` and `<after_logon_saml_auth>` XML options affect how FortiClient presents SAML authentication in the GUI. See VPN options.

When using SAML with external browser authentication, VPN before logon is not supported.

To configure FortiAuthenticator as the identity provider (IdP):

1. In FortiAuthenticator, go to *Authentication > SAML IdP > Service Providers*.
2. Configure a new service provider (SP) for SAML.



3. Go to *Authentication > User Management > Local Users*.
4. Create a new user.

To configure FortiGate as a SAML SP:

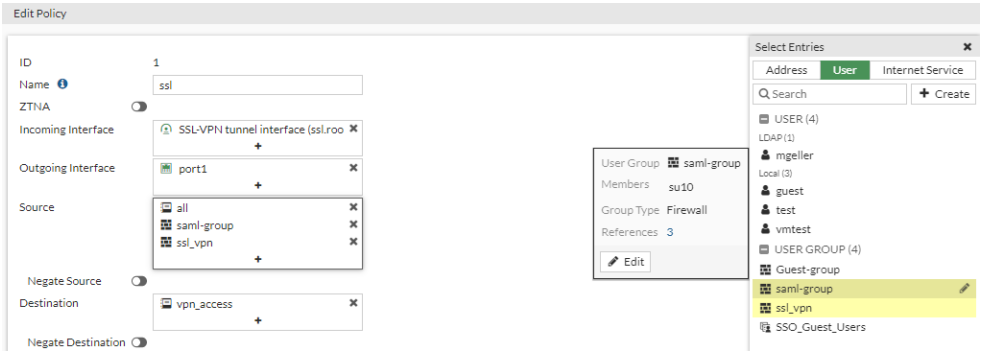
1. In the FortiOS CLI, create a SAML user. Ensure that the SP and IdP details match the details provided by FortiAuthenticator:

```
config user saml
   edit "su10"
      set cert "Fortinet_Factory"
      set entity-id "http://192.168.230.56:4433/remote/saml/metadata/"
      set single-sign-on-url "https://192.168.230.56:4433/remote/saml/login/"
      set single-logout-url "https://192.168.230.56:4433/remote/saml/logout/"
      set idp-entity-id "http://172.17.61.118:443/saml-idp/s6rlo1pxemulz84k/metadata/"
      set idp-single-sign-on-url "https://172.17.61.118:443/saml-idp/s6rlo1pxemulz84k/login/"
      set idp-single-logout-url "https://172.17.61.118:443/saml-idp/s6rlo1pxemulz84k/logout/"
      set idp-cert "REMOTE_Cert_1"
      set user-name "username"
      set group-name "group"
      set digest-method sha1
   next
end
```

2. Ensure that the SAML redirect port is set to 8020. SAML external browser authentication uses port 8020 by default. If another service or application is occupying this port, FortiClient displays a message showing that the SAML redirect port is unavailable.:

```
config vpn ssl setting
   show full-configuration | grep 8020
      set saml-redirect-port 8020
   next
end
```

3. Create a user group by going to *User & Authentication > User Groups > Create New*. Provide the required details and add the user that you created in step 1 to this group.
4. Go to *VPN > SSL-VPN Settings*. Under *Authentication/Portal Mapping*, create a mapping with the user group that you created in step 3. From the *Portal* dropdown list, select *full-access*. Click *OK*.
5. Go to *Policy & Objects > Firewall Policy*. Select the SSL VPN firewall policy. Ensure that the *Source* field includes the SAML user group.

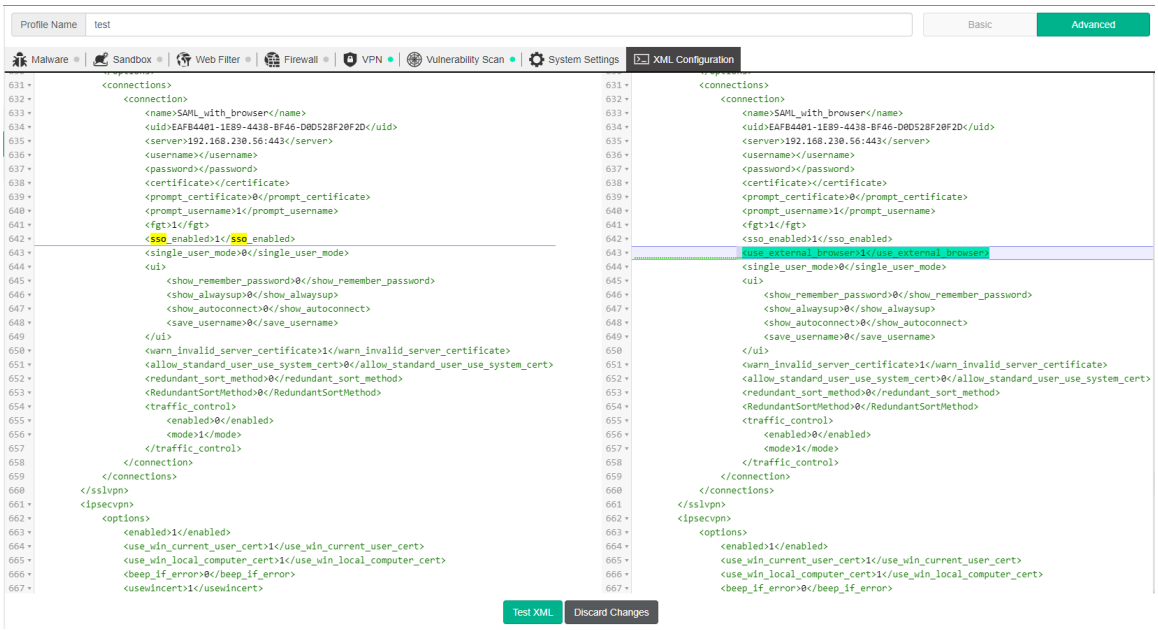


To configure external browser for authentication in EMS:



To view and configure SSL VPN settings, you must enable SSL VPN visibility in *System Settings > Feature Select*. See Feature Select on page 555.

1. In EMS, go to *Endpoint Profiles > Manage Profiles*, and edit the desired profile.
2. On the *VPN* tab, click *Add Tunnel*. Provide the correct gateway information. In *Advanced Settings*, enable *Enable SAML Login*. Configure other fields as desired. Save the tunnel.
3. On the *XML Configuration* tab, under the `<sso_enabled>` element for the tunnel, add `<use_external_browser>1</use_external_browser>`.



4. Click *Test XML*, then save the configuration.

To test the connection in FortiClient:

1. After FortiClient receives the latest configuration update from EMS, go to the *Remote Access* tab.
2. View the tunnel to verify that the *Use external browser as user-agent for saml user authentication field* is enabled.
3. Connect to the tunnel by clicking *SAML Login*. Verify that FortiClient opens your default browser to prompt for authentication. Provide your credentials and click *Login* to establish the connection.

Per-machine prelogon VPN connection without user interaction

You can configure per-machine SSL and IPsec VPN tunnels that connect before user logon without user interaction using XML configuration. The following describes the XML tags required:

XML tag	Description	Default value
`<show_vpn_before_logon>`	Show VPN before logon tile when logging in to Windows. Per-machine autoconnect depends on this tag being enabled to work. Boolean: `[1|0]`	1
`<on_os_start_connect>`	Enter the tunnel name for VPN to connect to when the OS starts. For per machine autoconnect to work, you must define a tunnel as the tunnel for per-machine autoconnect. See the `<machine>` tag.	
`<on_os_start_connect_ has_priority>`	When per-user and per-machine autoconnect configurations both exist, the following occurs: • If this tag is set to 1, the per-machine	1

XML tag	Description	Default value
	autoconnect configuration remains connected. • If this tag is set to `0`, after logging into Windows, the per-machine autoconnect configuration drops, and the per-user autoconnect configuration connects.	
`<machine>`	Enabling this tag indicates that FortiClient should use this tunnel for per-machine autoconnect. This tag must be enabled for per-machine autoconnect to start to connect. Boolean: `[1|0]`	`0`
`<username>`	Enter the remote gateway authentication username if xAuth is enabled. If using public key infrastructure (PKI) authentication, do not configure this tag.	
`<password>`	Enter the password for the remote gateway authentication username if xAuth is enabled. If using PKI authentication, do not configure this tag.	
`<keep_running>`	When this tag is enabled and the network status changes from up to down to up again, the tunnel autoconnects when the network status is up again. This tag applies whether before or after logging in to Windows. Boolean: `[1|0]`	`0`

The following show example XML configurations for SSL and IPsec VPN for per-machine autoconnect. Elements of note have been bolded for emphasis. Both examples are balanced but incomplete XML configuration fragments. The fragments include all closing tags, but omits some important elements to complete the configuration.

SSL VPN example

```
<vpn>
   <options>
      <on_os_start_connect>myfgt-ssl</on_os_start_connect>
      <show_vpn_before_logon>1</show_vpn_before_logon>
      <on_os_start_connect_has_priority>0</on_os_start_connect_has_priority>
   </options>
   <sslvpn>
      <options>
         <enabled>1</enabled>
         <disallow_invalid_server_certificate>0</disallow_invalid_server_certificate>
      </options>
      <connections>
         <connection>
            <name>myfgt-ssl</name>
            <description />
            <server>172.17.61.39:10439</server>
            <ui>
```

```
            <show_alwaysup>1</show_alwaysup>
            <show_autoconnect>1</show_autoconnect>
            <save_username>0</save_username>
            <show_remember_password>1</show_remember_password>
         </ui>
         <machine>1</machine>
         <password>11111111</password>
         <username>t1</username>
         <keep_running>0</keep_running >
         <certificate>
            <common_name>
               <match_type>simple</match_type>
               <pattern>
                  <![CDATA[ems.loc]]>
               </pattern>
            </common_name>
            <issuer>
               <match_type>simple</match_type>
               <pattern>
                  <![CDATA[L4RTP-AD4-EMS-LAB-CA]]>
               </pattern>
            </issuer>
         </certificate>
         <warn_invalid_server_certificate>0</warn_invalid_server_certificate>
         <prompt_certificate>1</prompt_certificate>
         <prompt_username>1</prompt_username>
      </connection>
   </connections>
</sslvpn>
</vpn>
```

IPsec VPN example

```
<ipsecvpn>
   <connections>
      <connection>
         <name>myfgt-ipsec</name>
         <type>manual</type>
         <ui>
            <show_remember_password>1</show_remember_password>
            <show_alwaysup>1</show_alwaysup>
            <show_autoconnect>1</show_autoconnect>
            <show_passcode>0</show_passcode>
            <save_username>0</save_username>
         </ui>
         <ike_settings>
            <server>fgt28.com</server>
            <authentication_method>System Store X509 Certificate</authentication_method>
            <fgt>1</fgt>
            <prompt_certificate>1</prompt_certificate>
            <xauth_timeout>120</xauth_timeout>
            <xauth>
            <use_otp>0</use_otp>
            <enabled>1</enabled>
            <prompt_username>1</prompt_username>
            <username>t1</username>
            <password>1</password>
```

```
            </xauth>
            <run_fcauth_system>1</run_fcauth_system>
            <auth_data>
               <certificate>
                  <common_name>
                     <match_type>wildcard</match_type>
                     <pattern>*</pattern>
                  </common_name>
                  <issuer>
                     <match_type>simple</match_type>
                     <pattern>L4RTP-AD4-EMS-LABCA</pattern>
                  </issuer>
               </certificate>
            </auth_data>
         </ike_settings>
         <ipsec_settings>
         </ipsec_settings>
         <host_check_fail_warning></host_check_fail_warning>
         <keep_running>0</keep_running>
         <machine>1</machine>
      </connection>
   </connections>
</ipsecvpn>
```

Use cases

In addition to per-machine autoconnect VPN tunnels, you can also configure per-user autoconnect VPN tunnels. The following describes the expected behavior for different scenarios involving these VPN tunnels:

Scenario	Behavior
Only a per-user autoconnect tunnel with <keep_running> disabled is configured.	• The per-user tunnel only connects after the user logs in to the device. • The per-user tunnel does not disconnect unless the user manually disconnects it. • When the user manually disconnects the per-user tunnel, the tunnel does not automatically reconnect.
Only a per-user autoconnect tunnel with <keep_running> enabled is configured.	• The per-user tunnel only connects after the user logs in to the device. • The per-user tunnel does not disconnect. • When the device disconnects from the network, the per-user tunnel disconnects. • When the device reconnects to the network, the per-user tunnel reconnects. • When the user manually disconnects the per-user tunnel, the tunnel does not automatically reconnect.
Only a per-machine autoconnect tunnel with <keep_running> disabled is configured.	• The per-machine tunnel connects before the user logs in to the device. • After the user logs in to the device, the per-machine tunnel remains connected and does not disconnect.

Scenario	Behavior
	• When the user manually disconnects the per-machine tunnel, the tunnel does not automatically reconnect.
Only a per-machine autoconnect tunnel with <keep_running> enabled is configured.	• The per-machine tunnel connects before the user logs in to the device. • After the user logs in to the device, the per-machine tunnel remains connected and does not disconnect. • When the device disconnects from the network, the per-machine tunnel disconnects. • When the device reconnects to the network, the per-machine tunnel reconnects. • When the user manually disconnects the per-machine tunnel, the tunnel does not automatically reconnect.

The following tunnels are configured:
• A per-machine autoconnect tunnel with <keep_running> disabled
• A per-user autoconnect tunnel with:
  • <keep_running> disabled
  • <show_remember_password> enabled
  • <show_autoconnect> enabled
	• The per-machine tunnel connects before the user logs in to the device.
	• After the user logs in to the device, the per-machine tunnel disconnects, and the per-user tunnel connects.
	• When the user manually disconnects the per-user tunnel, the tunnel does not automatically reconnect.

The following tunnels are configured: • A per-machine autoconnect tunnel with <keep_running> enabled • A per-user autoconnect tunnel with <keep_running> enabled	• The per-machine tunnel connects beforethe user logs in to the device. • After the user logs in to the device, the per-machine tunnel disconnects, and the per-user tunnel connects. • When the device disconnects from the network, the per-user tunnel disconnects. • When the device reconnects to the network, the per-user tunnel reconnects. • When the user manually disconnects the per-user tunnel, the tunnel does not automatically reconnect.

This document is not intended to cover all possible VPN tunnel configuration combinations.

Autoconnect on logging in as an Entra ID user

You can configure FortiClient to automatically connect to a specified VPN tunnel using Microsoft Entra ID credentials.

FortiClient supports two autoconnect methods with Entra ID SAML VPN:

- FortiClient can establish the VPN tunnel seamlessly without manual authentication if the user is already logged in to an Entra ID domain-joined endpoint. See Method 1: Autoconnect with Entra ID domain-joined FortiClient endpoint on page 173.
- The user establishes the VPN tunnel using manual authentication for the first time that they establish that VPN tunnel. Afterward, FortiClient can seamlessly establish the VPN tunnel without manual authentication. See Method 2: Autoconnect with non Entra ID-joined FortiClient endpoint on page 174.

The following describes configuration for both methods.

The following instructions assume that you have already configured your Entra ID environment, that your FortiEndpoint and FortiGate are part of a Fortinet Security Fabric, and that the FortiGate has been configured in Azure as an enterprise application for SAML single sign on. See Tutorial: Azure AD SSO integration with FortiGate SSL VPN.

The `<before_logon_saml_auth>` and `<after_logon_saml_auth>` XML options affect how FortiClient presents SAML authentication in the GUI. See VPN options.

The following configuration requires FortiOS 7.2.1 or a later version.

Method 1: Autoconnect with Entra ID domain-joined FortiClient endpoint

To join the endpoint to an Entra ID domain:

1. On the Windows machine, go to *Settings* > *Accounts* > *Access work or school* > *Join this device to Microsoft ID*.
2. Enter the Entra ID domain account credentials.
3. Reboot the endpoint.
4. Log in with the configured Entra ID credentials.

To configure EMS:

1. Go to *Endpoint Profiles* > *Remote Access*.
2. Select the desired profile.
3. Specify the desired tunnel as the autoconnect tunnel:

```
<vpn>
   <options>
      <autoconnect_tunnel>SSL VPN HQ</autoconnect_tunnel>
      <autoconnect_on_install>1</autoconnect_on_install>
   <options>
<vpn>
```

After the endpoint receives the updated configuration, when the user is logged in as the Entra ID domain user on the endpoint, FortiClient seamlessly connects to the VPN tunnel without displaying a prompt for credentials. The user does not need to manually authenticate the VPN tunnel connection.

To configure FortiOS:

FortiOS 7.2.8+ and 7.4.2+	FortiOS 7.2.1-7.2.8 and 7.4.0-7.4.2

`config user external-identity-provider`
`edit "msgragh"`
`set type ms-graph`
	`conf user saml`
	`edit "azure_saml"`

FortiOS 7.2.8+ and 7.4.2+	FortiOS 7.2.1-7.2.8 and 7.4.0-7.4.2

<pre>set version v1.0
next
end</pre>
	<pre>set auth-url
	"https://graph.microsoft.com/v1.0/me"
	next
	end</pre>

Method 2: Autoconnect with non Entra ID-joined FortiClient endpoint

To create and configure app registration in Azure:

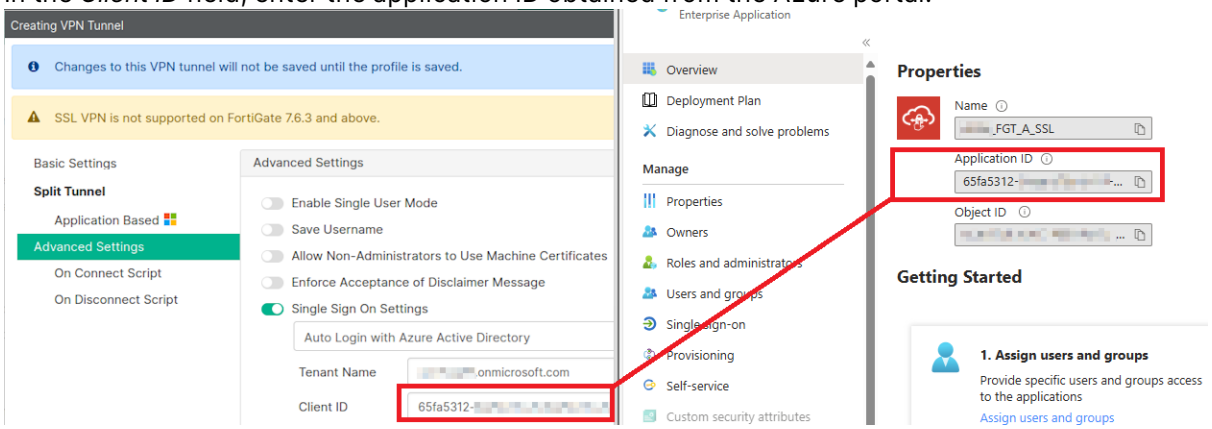
1. In the Azure portal, go to *Microsoft Entra ID > Enterprise applications*.
2. Select the FortiGate SSL VPN enterprise application.
3. Note down the application ID and Azure domain.
4. Go to *Microsoft Entra ID > App registrations > All applications*.
5. Click the application that you selected in step 2.
6. Go to *Manage > Authentication > Add a platform > Mobile and desktop applications*.
7. In the *Custom redirect URIs* field, enter ms-appx-web://microsoft.aad.brokerplugin/, followed by the application ID that you noted. For example, if your application ID is 123456, enter ms-appx-web://microsoft.aad.brokerplugin/123456.
8. Save the configuration.

To configure EMS:

1. Go to *Endpoint Profiles > Remote Access*.
2. Select the desired profile.
3. Configure the following for the desired tunnel for FortiClient to automatically connect to. This example configures an SSL VPN tunnel as the tunnel that FortiClient automatically connects to. You can configure the autoconnect tunnel to be an IPsec VPN tunnel if desired. For details on how to find the tenant domain name and application ID from the Azure portal, see the following:
   - Find the Microsoft Entra tenant ID and primary domain name
   - Quickstart: View enterprise applications

   Configure the following in *Advanced Settings*:
   a. Toggle on *Single Sign On Settings*.
   b. From the dropdown list, select *Auto Login with Azure Active Directory*.
   c. In the *Tenant Name* field, enter the domain name obtained from the Azure portal.

d. In the *Client ID* field, enter the application ID obtained from the Azure portal.



4. Save the tunnel.
5. In general VPN settings, specify the desired tunnel as the autoconnect tunnel:

```
<vpn>
   <options>
      <autoconnect_tunnel>SSL VPN HQ</autoconnect_tunnel>
      <autoconnect_on_install>1</autoconnect_on_install>
   <options>
<vpn>
```

To configure FortiOS:

You must define a user, msgraph, and use it as a member of *User & Authentication > User Groups*. The following shows the relevant CLI commands:

FortiOS 7.2.8+ and 7.4.2+	FortiOS 7.2.1-7.2.8 and 7.4.0-7.4.2

`config user external-identity-provider`
`  edit "msgragh"`
`  set type ms-graph`
`  set version v1.0`
`  next`
`end`
 	
`config user group`
`  edit "SSLVPN_SAML_Entra_ID"`
`  set authtimeout 60`
`  set member "msgragh"`
`  next`
`end`
	`conf user saml`
	`  edit "azure_saml"`
	`  set auth-url`
	`  "https://graph.microsoft.com/v1.0/me"`
	`  next`
	`end`
	
	`config user group`
	`  edit "SSLVPN_SAML_Entra_ID"`
	`  set authtimeout 60`
	`  set member "msgragh"`
	`  next`
	`end`

To configure EMS:

1. Go to *Endpoint Profiles > Remote Access*.
2. Select the desired profile.
3. In XML view, configure the following for the desired tunnel for FortiClient to automatically connect to. This example configures an SSL VPN tunnel as the tunnel that FortiClient automatically connects to. You can configure the autoconnect tunnel to be an IPsec VPN tunnel if desired. For details on how to

find the tenant domain name and application ID from the Azure portal, see the following:

- Find the Microsoft Entra tenant ID and primary domain name
- Quickstart: View enterprise applications

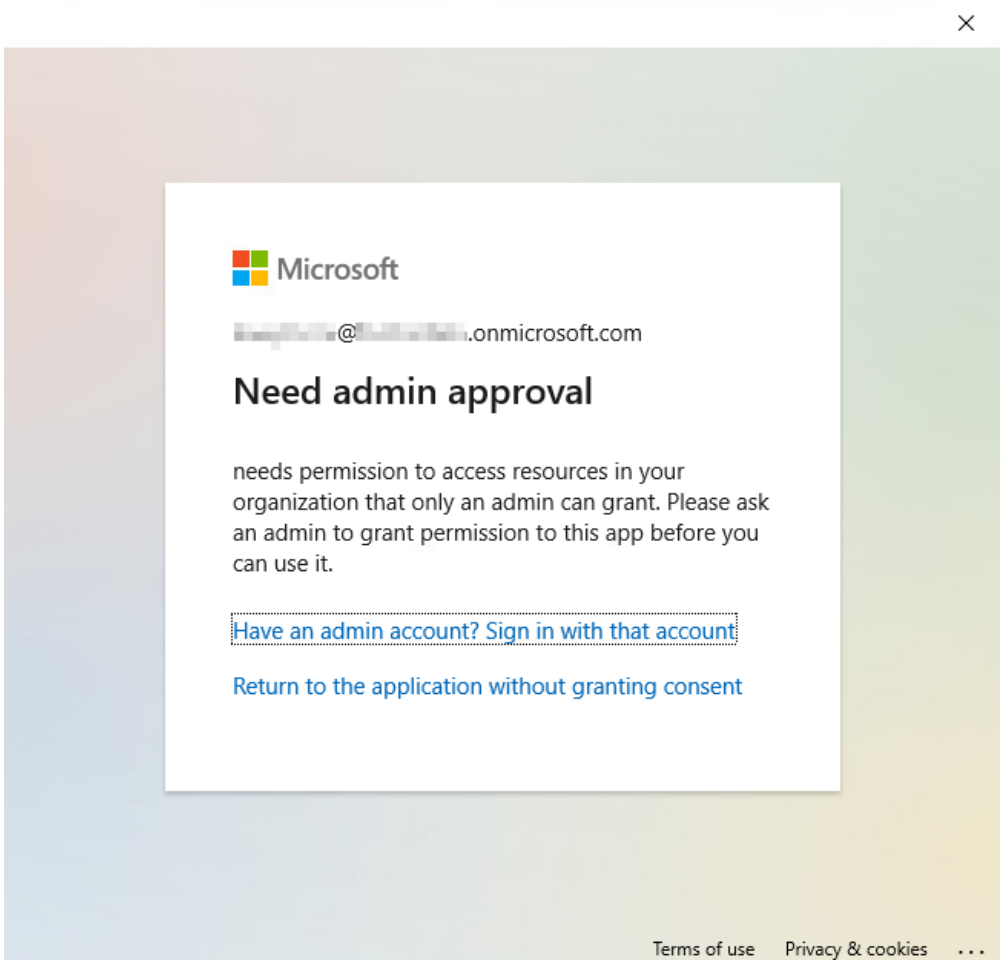
```
<vpn>
   <sslvpn>
      <connections>
         <connection>
            <name>SSL VPN HQ</name>
            <sso_enabled>1</sso_enabled>
            <azure_auto_login>
               <enabled>1</enabled>
               <azure_app>
                  <tenant_name>Domain name obtained from the Azure portal.</tenant_name>
                  <client_id>Application ID obtained from the Azure portal</client_id>
               </azure_app>
            </azure_auto_login>
         <connection>
      <connections>
   <sslvpn>
<vpn>
```

4. In general VPN settings, specify the desired tunnel as the autoconnect tunnel:

```
<vpn>
   <options>
      <autoconnect_tunnel>SSL VPN HQ</autoconnect_tunnel>
      <autoconnect_on_install>1</autoconnect_on_install>
   <options>
<vpn>
```

To manage application permissions:

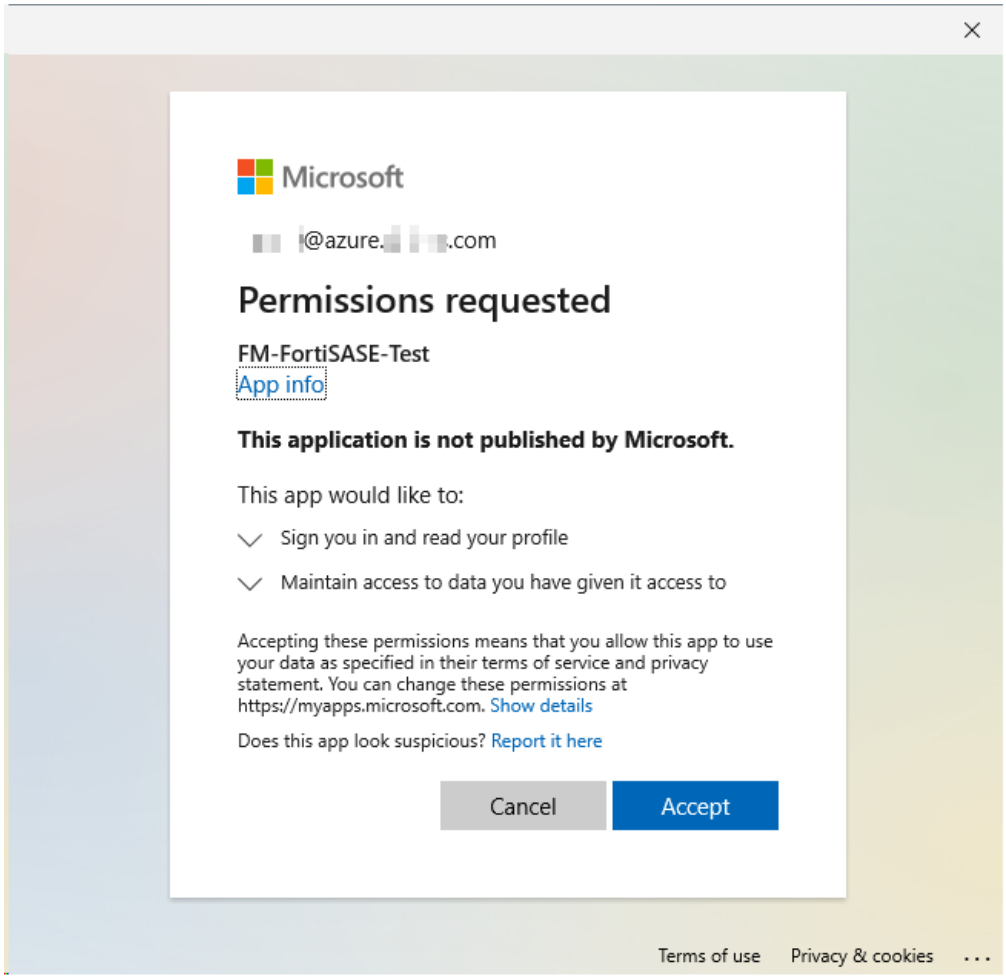
1. As an end user, log in to an endpoint that has the profile configured in To configure EMS: on page 175 applied.
2. FortiClient automatically attempts to connect to the specified VPN tunnel. If this is the initial attempt to connect to this VPN tunnel, Windows displays a prompt to select the desired Entra ID account. Select the desired account.
   You should now configure one of the following permission options. These steps assume that you have already configured Azure SAML SSL/IPsec VPN autoconnect as this document describes and you are signed in as a global administrator of the same tenant.
3. To have *Need admin approval* shown to users, do the following:
   a. In the Azure portal, go to *Enterprise Application > <Your VPN application> > (sidebar) Manage > Properties*.
   b. Set *Assignment required?* to *Yes*.
   c. Add the desired users to *Users & Groups*.
   d. Remove any permissions in *App Registration*.
   e. Go to *Home > App Registration > <Your VPN application> > (sidebar) Manage > API permissions*.
   f. Right-click and remove permission.
   g. If you want to disallow user consent for all applications, you can disable this by doing the following:
      i. Go to *Home > Enterprise Application > <Your VPN application> > (sidebar) Security > Consent and permissions > Manage > User consent settings*.
      ii. For *User consent for applications*, select *Do not allow user consent*.



4. To have users consent per a permissions request but avoid admin approval, do the following:
   a. Go to *Enterprise Application > <Your VPN application> > (sidebar) Manage > Properties*.
   b. Set *Assignment required?* to *No*. This allows any valid user from this tenant to use the app. You no longer need to add users to *Users and groups* to have access to this app. As per Microsoft documentation, when an application requires assignment, user consent for that application is not allowed. This is true even if users consent for that app would have otherwise been allowed.
   c. Remove any permissions in *App Registration*.
   d. Go to *Home > App Registration > <Your VPN application> > (sidebar) Manage > API permissions*.
   e. Right-click and remove permission.
   f. Allow users to consent:
      i. Go to *Home > Enterprise Application > <Your VPN application> > (sidebar) Security > Consent and permissions > Manage > User consent settings*.
      ii. Select *User consent for applications > Allow user consent for apps from verified publishers* for selected permissions.
      iii. Go to *Manage > Permission classifications*.
      iv. Ensure the following are listed under *Low-risk permissions > Microsoft Graph*:
         - *email*
         - *User.Read*
         - *offline_access*

- *profile*
- *openid*

The next time that the Entra ID user signs in with FortiClient Entra ID autoconnect triggered, the user should see a popup requesting permissions.



5. To grant admin consent to an enterprise application such that a user does not need to request consent, do one of the following:
   a. To grant this consent through the standard permission UI as a global administrator, do the following:
      i. Connect to the VPN. You are prompted as usual to grant permissions for your user account to the enterprise application.
      ii. As a global administrator, there is an extra *Consent on behalf of your organization* checkbox. Select it to grant admin consent to the application. Other users do not need to grant consent.
   b. To grant this consent in the Azure portal, do the following:
      i. Go to *Enterprise Application > <Your VPN application> > (sidebar) Security > Permissions*.
      ii. Click *app registration* in the sentence *To configure requested permissions for apps you own, use the app registration*.
      iii. Go to *API Permissions > Configured permissions > Add a permission > Request API permissions > Microsoft APIs > Microsoft Graph > Delegated Permissions*.

iv. Select the following:
   - openID permissions:
     - *offline_access*
     - *openid*
     - *profile*
     - *email*
   - *User > User.Read*

v. Add the permissions.

vi. After the permissions are added, they appear in the table on the same screen. Click *Grant admin consent for <Tenant name>*.

vii. Return to *Enterprise Applications Permissions* by clicking *Enterprise applications* in the sentence *To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try Enterprise applications*.

viii. The *Grant admin consent for <Tenant name>* button is blue instead of being grayed out. Click the button. A popup opens that requires you to sign in as a global administrator and to allow the application permissions. The permissions that you used in *App Permissions* fill in the following table.

After you complete either step, users no longer need to request consent and can autoconnect to VPN without having to give consent.



The prompt to grant permissions does not appear if the Azure domain or tenant administrator has already granted permission on behalf of the organization.

Load balancing IPsec VPN gateways with a single FQDN

FortiClient supports load balancing IPsec VPN gateways with a single fully qualified domain name (FQDN). This feature simplifies configuration management, reducing the need for users to manually select specific VPN gateway IP addresses.

Before IPsec VPN authentication, FortiClient resolves the FQDN to an IP address and saves it in the hosts file to ensure it remains connected to the same FortiGate throughout the tunnel establishment process, including authentication and tunnel creation. However, since DNS servers may return IP addresses using round robin, FortiClient may resolve the FQDN to a different FortiGate during login, leading to connection inconsistencies and IPsec VPN connection failure. This feature enables FortiClient to connect to different FortiGate IP addresses under a single FQDN. If a FortiGate is down, FortiClient can attempt to connect to it until the next DNS resolution provides an alternative IP address.

The example deployment consists of the following components:

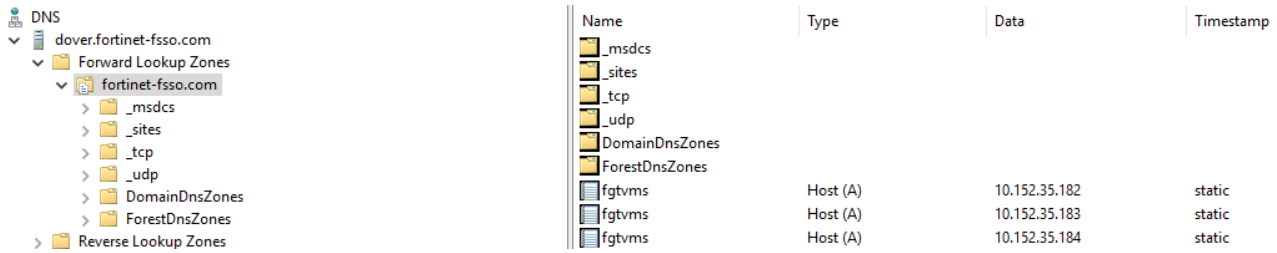
- **Three FortiGates acting as remote gateways, with the following IP addresses**:

Remote gateway	IP address
FGTVM_0_182	10.152.35.182
FGTVM_1_183	10.152.35.183
FGTVM_2_184	10.152.35.184

- **Single FQDN mapping the three FortiGates on the DNS server**: fgtvms.fortinet-fsso.com
- Microsoft Entra ID user to support SAML login for FortiClient VPN

To configure the DNS server:

1. Create three A records on the DNS server to map a single FQDN to three different IP addresses, each corresponding to a remote VPN gateway.



2. Run `nslookup` to confirm that the FQDN resolves to the three IP addresses.

```
C:\Windows\system32>nslookup fgtvms.fortinet-fsso.com
Server:         dover.fortinet-fsso.com
Address:        10.152.35.196

Name:           fgtvms.fortinet-fsso.com
Addresses:      10.152.35.182
                10.152.35.183
                10.152.35.184
```

To configure FortiOS:

1. Configure a user for Entra ID SAML login:

```
config user saml
    edit "saml_azure"
        set entity-id "https://fgtvms.fortinet-fsso.com:1234/remote/saml/metadata"
        set single-sign-on-url "https://fgtvms.fortinet-fsso.com:1234/remote/saml/login"
        set single-logout-url "https://fgtvms.fortinet-fsso.com:1234/remote/saml/logout"
        set idp-entity-id "https://sts.windows.net/f1a72219-bba3-4f6e-93b8-ce3b341b7cf4/"
        set idp-single-sign-on-url "https://login.microsoftonline.com/f1a72219-bba3-4f6e-93b8-
ce3b341b7cf4/saml2"
        set idp-single-logout-url "https://login.microsoftonline.com/f1a72219-bba3-4f6e-93b8-
ce3b341b7cf4/saml2"
        set idp-cert "REMOTE_Cert_1"
        set user-name "http://schemas.microsoft.com/identity/claims/displayname"
```

```
        set group-name "user.groups"
        set digest-method sha1
    next
end
```

2. Configure a VPN authentication user group that includes the user that you created in step 1:

```
config user group
    edit "saml_grp"
        set member "saml_azure"
    next
end
```

3. Configure an IPsec VPN IKEv2 tunnel:

```
config vpn ipsec phase1-interface
    edit "IKEV2-SAML-AZ"
        set type dynamic
        set interface "port1"
        set ike-version 2
        set peertype any
        set net-device disable
        set mode-cfg enable
        set ipv4-dns-server1 10.152.35.196
        set proposal aes128-sha256 aes256-sha256
        set comments "VPN: IKEV2_SAML_AZ (Created by VPN wizard)"
        set dhgrp 5
        set eap enable
        set eap-identity send-request
        set wizard-type dialup-forticlient
        set authusrgrp "saml_grp"
        set network-overlay enable
        set network-id 20
        set transport tcp
        set ipv4-start-ip 10.10.182.100 ## <<< or 10.10.183.100 or 10.10.184.100
        set ipv4-end-ip 10.10.182.200
        set save-password enable
        set client-auto-negotiate enable
        set client-keep-alive enable
        set psksecret ENC
y77chAtwvT25RPgnZTM5Xq51TzPpGjVKQ53r3kFUE5eQQmp1t8gxFSgXBth5nHCGChzcNB7VJhSUxmfCVOuz1c7qlS+n6e
RSs73jOGxUH++k3FgzVmFMmzidFW9nIA5/AqvUpPDL8tddMPsItRmtW/TLU355pYFHYa9RFB1UVuqTxZXlnJGqG51S54fb
ZF2C5lvptVlmMjY3dkVA
    next
end
config vpn ipsec phase2-interface
    edit "IKEV2_SAML_AZ"
        set phase1name "IKEV2-SAML-AZ"
        set proposal aes128-sha256 aes256-sha256
        set comments "VPN: IKEV2_SAML_AZ (Created by VPN wizard)"
    next
end
```

To configure EMS:

1. In EMS, go to *Endpoint Profiles > Remote Access*.
2. Create a new profile or edit an existing one.
3. Under *VPN Tunnels*, click *Add*.
4. For *Type*, select *IPsec VPN*.
5. In the *Remote Gateway* field, enter the FQDN. In this example, it is fgtvms.fortinet-fsso.com.
6. In *Advanced Settings*, toggle on *Enable SAML Login*.
7. Configure other fields as desired, then save.

The following shows example XML configuration:

```
<forticlient_configuration>
	<vpn>
		<enabled>1</enabled>
		<ipsecvpn>
			<connections>
				<connection>
					<name>IPSec-SAML-IntWeb</name>
					<uid>19527DD4-406D-48E1-9070-2FA86EB30254</uid>
					<machine>0</machine>
					<keep_running>0</keep_running>
					<keep_fqdn_resolution_consistency>1</keep_fqdn_resolution_
consistency>
					<disclaimer_msg/>
					<single_user_mode>0</single_user_mode>
					<type>manual</type>
					<ui>
						<show_remember_password>1</show_remember_password>
						<show_alwaysup>1</show_alwaysup>
						<show_autoconnect>1</show_autoconnect>
						<show_passcode>0</show_passcode>
						<save_username>0</save_username>
					</ui>
					<redundant_sort_method>0</redundant_sort_method>
					<tags>
						<allowed/>
						<prohibited/>
					</tags>
					<host_check_fail_warning/>
					<ike_settings>
						<server>fgtvms.fortinet-fsso.com</server>
						<authentication_method>Preshared Key</authentication_
method>
						<transport_mode>1</transport_mode>
						<session_resume>1</session_resume>
						<tcp_port>4500</tcp_port>
						<udp_port>500</udp_port>
						<fgt>1</fgt>
						<prompt_certificate>0</prompt_certificate>
						<xauth>
							<use_otp>0</use_otp>
```

```
                                        <enabled>1</enabled>
                                        <prompt_username>1</prompt_username>
                                </xauth>
                                <version>2</version>
                                <mode>aggressive</mode>
                                <key_life>86400</key_life>
                                <localid/>
                                <networkid>20</networkid>
                                <implied_SPDO>0</implied_SPDO>
                                <implied_SPDO_timeout>0</implied_SPDO_timeout>
                                <nat_traversal>1</nat_traversal>
                                <nat_alive_freq>5</nat_alive_freq>
                                <enable_local_lan>0</enable_local_lan>
                                <enable_ike_fragmentation>0</enable_ike_fragmentation>
                                <mode_config>1</mode_config>
                                <dpd>1</dpd>
                                <run_fcauth_system>0</run_fcauth_system>
                                <sso_enabled>1</sso_enabled>
                                <use_external_browser>0</use_external_browser>
                                <ike_saml_port>1234</ike_saml_port>
                                <dpd_retry_count>3</dpd_retry_count>
                                <dpd_retry_interval>5</dpd_retry_interval>
                                <auth_data>
                                        <preshared_key>Enc
41ea469c65f8ab068dc4ccf7f5f2544133fd01262b6d0e3536b2c17ccb8d</preshared_key>
                                </auth_data>
                                <xauth_timeout>120</xauth_timeout>
                                <dhgroup>5</dhgroup>
                                <proposals>
                                        <proposal>AES128|SHA256</proposal>
                                        <proposal>AES256|SHA256</proposal>
                                </proposals>
                        </ike_settings>
                        <ipsec_settings>
                                <remote_networks>
                                        <network>
                                                <addr>0.0.0.0</addr>
                                                <mask>0.0.0.0</mask>
                                        </network>
                                        <network>
                                                <addr>::/0</addr>
                                                <mask>::/0</mask>
                                        </network>
                                </remote_networks>
                                <dhgroup>5</dhgroup>
                                <key_life_type>seconds</key_life_type>
                                <key_life_seconds>43200</key_life_seconds>
                                <key_life_Kbytes>5200</key_life_Kbytes>
                                <replay_detection>1</replay_detection>
                                <pfs>1</pfs>
                                <use_vip>1</use_vip>
                                <virtualip>
```

```
                                        <type>modeconfig</type>
                                        <ip>0.0.0.0</ip>
                                        <mask>0.0.0.0</mask>
                                        <dnsserver>0.0.0.0</dnsserver>
                                        <winserver>0.0.0.0</winserver>
                                </virtualip>
                                <proposals>
                                        <proposal>AES128|SHA256</proposal>
                                        <proposal>AES256|SHA256</proposal>
                                </proposals>
                        </ipsec_settings>
                        <android_cert_path/>
                        <warn_invalid_server_certificate>1</warn_invalid_server_
certificate>
                        <on_connect>
                                <script>
                                        <os>windows</os>
                                        <script/>
                                </script>
                                <script>
                                        <os>MacOSX</os>
                                        <script/>
                                </script>
                                <script>
                                        <os>linux</os>
                                        <script/>
                                </script>
                        </on_connect>
                        <on_disconnect>
                                <script>
                                        <os>windows</os>
                                        <script/>
                                </script>
                                 <script>
                                        <os>MacOSX</os>
                                        <script/>
                                </script>
                                <script>
                                        <os>linux</os>
                                        <script/>
                                </script>
                        </on_disconnect>
                        <traffic_control>
                                <enabled>0</enabled>
                                <mode>1</mode>
                        </traffic_control>
                </connection>
        </connections>
        <options>
                <use_win_current_user_cert>1</use_win_current_user_cert>
                <enabled>1</enabled>
                <enable_udp_checksum>0</enable_udp_checksum>
```

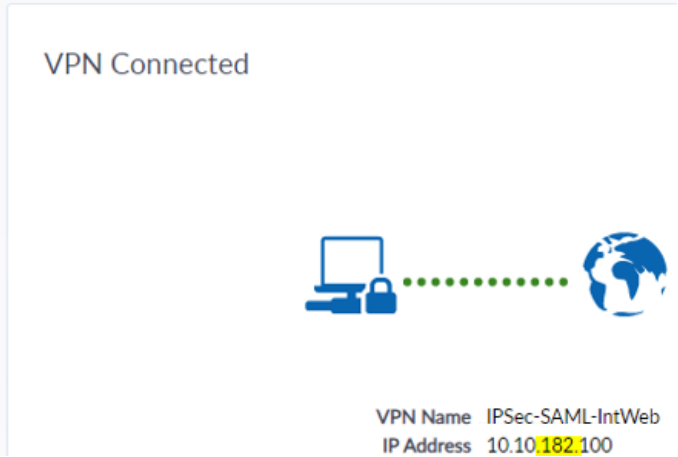
```
                        <usewincert>1</usewincert>
                        <check_for_cert_private_key>0</check_for_cert_private_key>
                        <block_ipv6>1</block_ipv6>
                        <use_win_local_computer_cert>1</use_win_local_computer_cert>
                        <disable_default_route>0</disable_default_route>
                        <enhanced_key_usage_mandatory>0</enhanced_key_usage_mandatory>
                        <uselocalcert>0</uselocalcert>
                        <usesmcardcert>1</usesmcardcert>
                        <show_auth_cert_only>0</show_auth_cert_only>
                        <no_dns_registration>0</no_dns_registration>
                        <beep_if_error>0</beep_if_error>
                         <disallow_invalid_server_certificate>0</disallow_invalid_server_
certificate>
                </options>
            </ipsecvpn>
            <options>
                <show_negotiation_wnd>0</show_negotiation_wnd>
                <use_legacy_vpn_before_logon>0</use_legacy_vpn_before_logon>
                <use_windows_credentials>0</use_windows_credentials>
                <show_vpn_before_logon>1</show_vpn_before_logon>
                <autoconnect_on_install>0</autoconnect_on_install>
                <secure_remote_access>0</secure_remote_access>
                <on_os_start_connect/>
                <certs_require_keyspec>0</certs_require_keyspec>
                <suppress_vpn_notification>0</suppress_vpn_notification>
                <allow_personal_vpns>1</allow_personal_vpns>
                <keep_running_max_tries>0</keep_running_max_tries>
                <autoconnect_only_when_offnet>0</autoconnect_only_when_offnet>
                <minimize_window_on_connect>0</minimize_window_on_connect>
                <disable_connect_disconnect>0</disable_connect_disconnect>
                <on_os_start_connect_has_priority>0</on_os_start_connect_has_priority>
                <after_logon_saml_auth>2</after_logon_saml_auth>
                <disable_internet_check>1</disable_internet_check>
                <current_connection_name>IPSec-SAML-IntWeb</current_connection_name>
                <current_connection_type>ipsec</current_connection_type>
            </options>
        </vpn>
</forticlient_configuration>
```

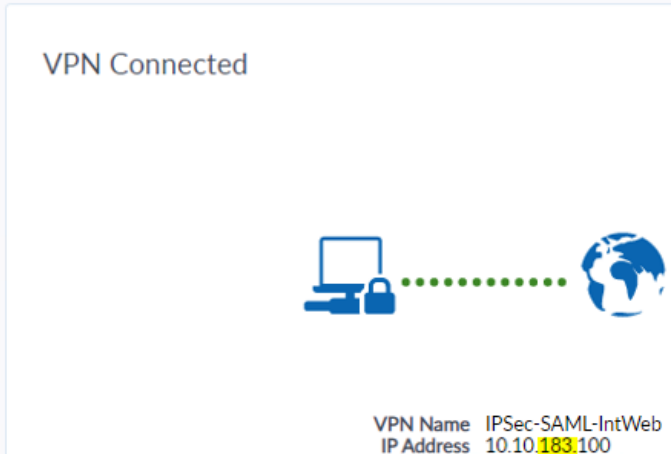
To verify the configuration using FortiClient:

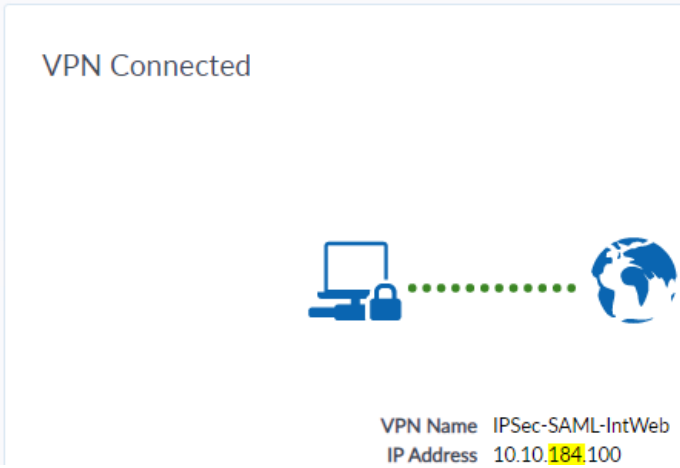
1. On three endpoints that received the profile updates, open FortiClient.
2. On the *Remote Access* tab, from the *VPN Name* dropdown list, select the configured IPsec VPN tunnel.
3. Click *Connect*.
4. FortiClient displays an authentication dialog. Enter the Entra ID credentials. If configured, you may also perform multifactor authentication.

The endpoints connect to the VPN gateways using the configured FQDN, fgtvm.fortinet-fsso.com. On the *Remote Access* tab, you can confirm in the *IP Address* field that the endpoints have connected to different IP addresses as corresponds to the three remote gateways:

Remote gateway	IP address
FGTVM_0_182	10.152.35.182
FGTVM_1_183	10.152.35.183
FGTVM_2_184	10.152.35.184









Round robin DNS does not ensure even distribution, as DNS caching and query timing may result in some clients resolving to the same IP address rather than a perfectly balanced spread. If one gateway goes offline, an endpoint that previously resolved to that gateway randomly selects one of the available gateways based o the round robin DNS response.

Load balancing SSL VPN gateways with one FQDN

When connecting to SSL VPN with an FQDN, FortiClient remembers the IP address with which it contacts the FortiGate and reuses it throughout the connection phase. This feature is available for FortiClient (Windows) and unavailable for FortiClient (macOS) or (Linux).

Prior to this enhancement, users experienced failed connections when load balancing SSL VPN gateways with one FQDN. The failed connections were due to the DNS server returning results using round robin while FortiClient tried to establish the SSL VPN connection during the login phase, leading to the connections going to different FortiGates.

With this enhancement, before SSL VPN authentication, FortiClient resolves the FQDN to an IP address and saves it to the hosts file. This keeps FortiClient connected to the same FortiGate during the entire tunnel establish process, including authentication and tunnel creation.

To support this feature, the DNS server must return the same IP addresss to multiple name lookup requests (sticky session).

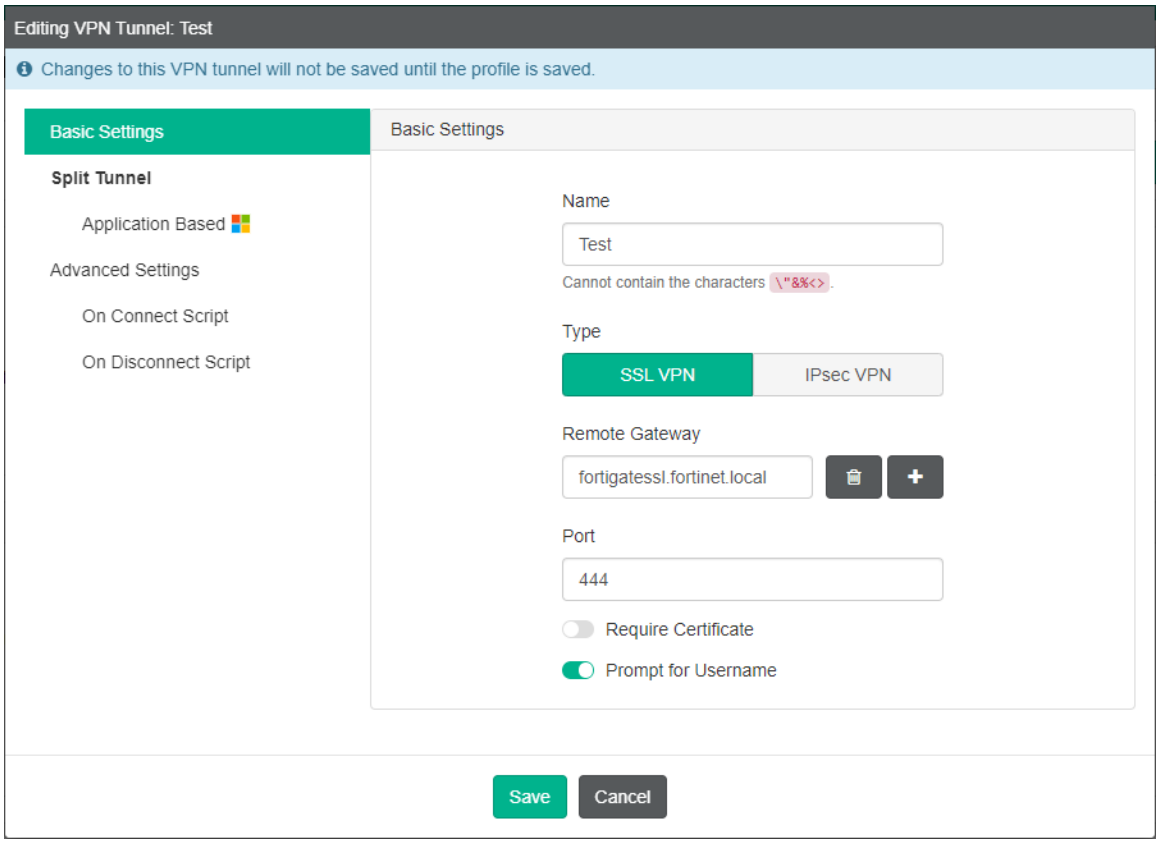
To configure load balancing SSL VPN gateways with one FQDN:



To view and configure SSL VPN settings, you must enable SSL VPN visibility in *System Settings* > *Feature Select*. See Feature Select on page 555.

1. Configure multiple remote gateways and map them to one FQDN on the DNS server. In this example, the remote gateways are 172.17.161.168 and 172.17.162.10. The FQDN is fortigatessl.fortinet.local.
2. In EMS, go to *Endpoint Profiles* > *Remote Access*.
3. Edit an existing profile or create a new one.
4. Create a VPN tunnel with the following settings:
   a. In *Basic Settings*, for *Type*, select *SSL VPN*.
   b. In the *Remote Gateway* field, enter the FQDN. In this example, it is fortigatessl.fortinet.local.

c. In the *Port* field, enter the port number for SSL VPN tunnel establishment.



d. In *Advanced Settings*, enable *Enable SAML Login* and *FQDN Resolution Persistence*.

e. Configure other settings as desired, and save the profile.

The following shows the XML configuration for this tunnel:

```
<forticlient_configuration>
    <vpn>
        <enabled>1</enabled>
        <options>
            <use_legacy_vpn_before_logon>0</use_legacy_vpn_before_logon>
            <autoconnect_only_when_offnet>0</autoconnect_only_when_offnet>
            <minimize_window_on_connect>1</minimize_window_on_connect>
            <disable_connect_disconnect>0</disable_connect_disconnect>
            <autoconnect_on_install>0</autoconnect_on_install>
            <suppress_vpn_notification>0</suppress_vpn_notification>
            <on_os_start_connect_has_priority>0</on_os_start_connect_has_priority>
            <show_negotiation_wnd>0</show_negotiation_wnd>
            <keep_running_max_tries>1</keep_running_max_tries>
            <use_windows_credentials>0</use_windows_credentials>
            <secure_remote_access>0</secure_remote_access>
            <on_os_start_connect/>
            <allow_personal_vpns>1</allow_personal_vpns>
            <show_vpn_before_logon>0</show_vpn_before_logon>
        </options>
        <sslvpn>
```

```
            <connections>
                <connection>
                    <name>Test</name>
                    <uid>EC71C6B4-8C6D-460F-A141-F8982338867B</uid>
                    <machine>0</machine>
                    <keep_running>0</keep_running>
                    <username/>
                    <password/>
                    <certificate/>
                    <prompt_certificate>0</prompt_certificate>
                    <prompt_username>1</prompt_username>
                    <fgt>1</fgt>
                    <is_fgd_cloud>0</is_fgd_cloud>
                    <disclaimer_msg/>
                    <sso_enabled>1</sso_enabled>
                    <keep_fqdn_resolution_consistency>1</keep_fqdn_resolution_consistency>
                    <azure_auto_login>
                        <enabled>0</enabled>
                        <azure_app>
                            <tenant_name/>
                            <client_id/>
                        </azure_app>
                    </azure_auto_login>
                    <single_user_mode>0</single_user_mode>
                    <ui>
                        <show_remember_password>1</show_remember_password>
                        <show_alwaysup>1</show_alwaysup>
                        <show_autoconnect>1</show_autoconnect>
                        <save_username>0</save_username>
                    </ui>
                    <warn_invalid_server_certificate>0</warn_invalid_server_certificate>
                    <redundant_sort_method>0</redundant_sort_method>
                    <RedundantSortMethod>0</RedundantSortMethod>
                    <tags>
                        <allowed/>
                        <prohibited/>
                    </tags>
                    <host_check_fail_warning/>
                    <server>fortigatessl.fortinet.local:444</server>
                    <on_connect>
                        <script>
                            <os>windows</os>
                            <script/>
                        </script>
                    </on_connect>
                    <on_disconnect>
                        <script>
                            <os>windows</os>
                            <script/>
                        </script>
                    </on_disconnect>
                    <traffic_control>
```

```
                        <enabled>0</enabled>
                        <mode>1</mode>
                    </traffic_control>
                </connection>
            </connections>
            <options>
                <enabled>1</enabled>
                <warn_invalid_server_certificate>0</warn_invalid_server_certificate>
                <dnscache_service_control>0</dnscache_service_control>
                <prefer_sslvpn_dns>1</prefer_sslvpn_dns>
                <disallow_invalid_server_certificate>0</disallow_invalid_server_certificate>
                <no_dns_registration>0</no_dns_registration>
            </options>
        </sslvpn>
    </vpn>
</forticlient_configuration>
```

To verify the configuration:

1. In FortiClient, on the *Remote Access* tab, select the desired tunnel from the *VPN Name* dropdown list.
2. Click *SAML Login*.
3. Open the hosts file. Confirm that an entry was added to resolve the SSL VPN tunnel FQDN:

```
# Copyright (c) 1993-2009 Microsoft Corp.
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host
# localhost name resolution is handled within DNS itself.
#    127.0.0.1       localhost
#    ::1             localhost
172.17.161.168 fortigatessl.fortinet.local
```

4. Enter valid SAML credentials to successfully establish the SSL VPN tunnel.
5. Confirm that the entry in the hosts file was removed after FortiClient established the SSL VPN tunnel connection:

```
# Copyright (c) 1993-2009 Microsoft Corp.
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
```

```
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host
# localhost name resolution is handled within DNS itself.
#    127.0.0.1       localhost
#    ::1             localhost
```

6. Disconnect from the VPN tunnel.
7. Start a new connection to the same VPN tunnel.
8. Confirm that an entry was added to resolve the SSL VPN tunnel FQDN to a different remote gateway:

```
# Copyright (c) 1993-2009 Microsoft Corp.
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host
# localhost name resolution is handled within DNS itself.
#    127.0.0.1       localhost
#    ::1             localhost
172.17.162.20 fortigatessl.fortinet.local
```

9. Confirm that the entry in the hosts file was removed after FortiClient established the SSL VPN tunnel connection.

Certificate path configuration for automated certificate selection

You can configure a certificate location in a Remote Access profile for IPsec and SSL VPN. FortiClient (Android) automatically goes to the certificate location when doing the following:

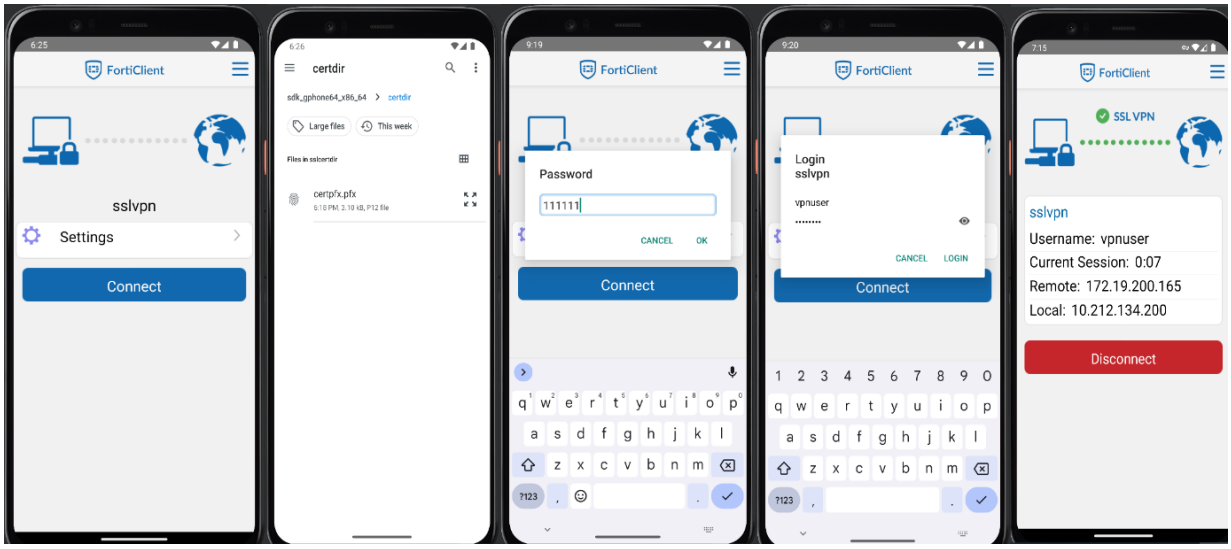
- When selecting a certificate
- When the user clicks *Connect* to connect to SSL VPN

To configure certificate path for automated certificate selection:

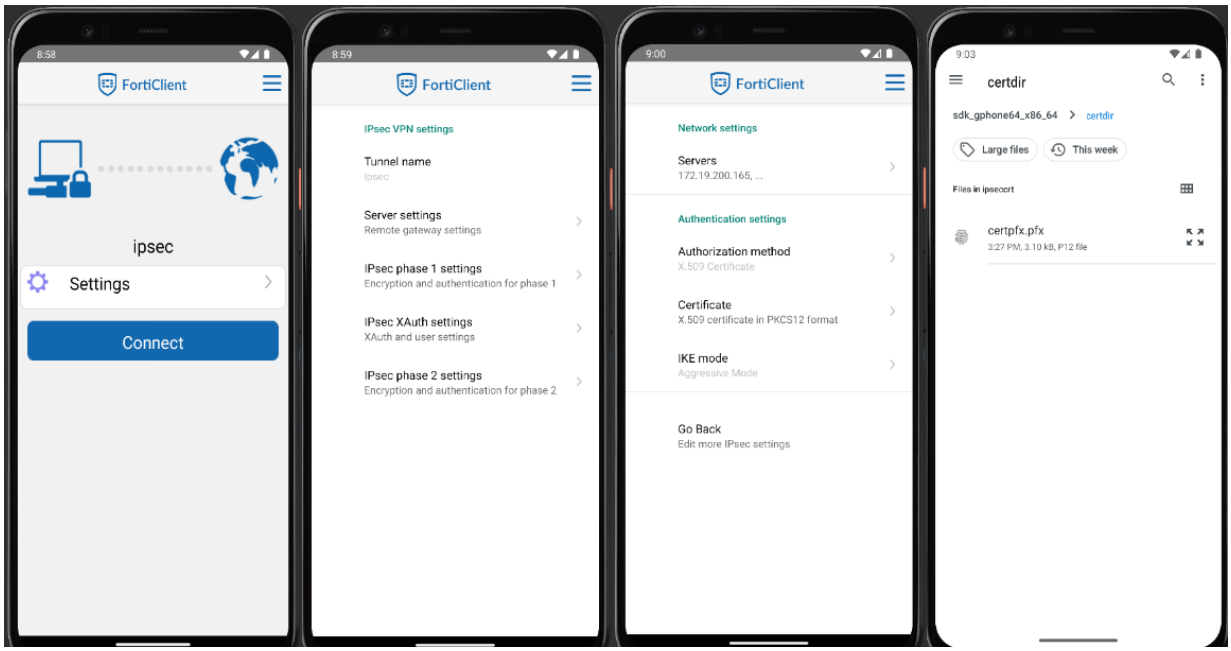
1. In EMS, go to *Endpoint Profiles* > *Remote Access*.
2. Create a new profile or edit an existing one.
3. Click *Add VPN Tunnel*.
4. Do one of the following:
   - For an SSL VPN tunnel, enable *Require Certificate*.

     To view and configure SSL VPN settings, you must enable SSL VPN visibility in *System Settings* > *Feature Select*. See Feature Select on page 555.

   - For an IPsec VPN tunnel, from the *Authentication Method* dropdown list, select *Smart Card Certificate* or *System Store Certificate*.
5. In the *Android Certificate Location* field, enter the certificate location for the Android device. In this example, the location is certdir/. You should already have created this directory in the Android device internal storage. The certificate path can be only one level deep. For example, you could configure this field as Folder/clientcert.p12.
6. Connect FortiClient (Android) to EMS.
7. After FortiClient (Android) receives the configuration changes, do one of the following:
   - For SSL VPN, connect to VPN. Clicking *Connect* automatically goes to certdir, the configured certificate location. Clicking the certificate options in *Settings* for the VPN tunnel also goes to certdir.



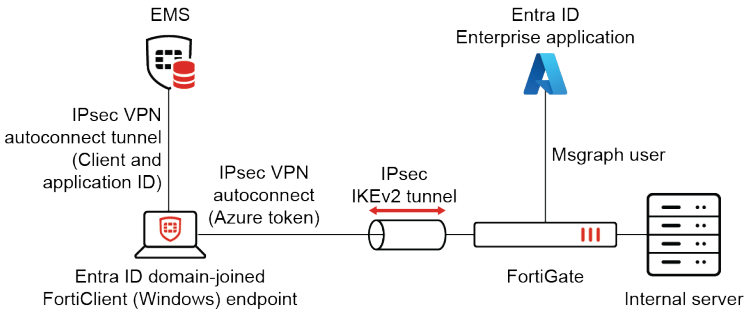
   - For IPsec VPN, go to the tunnel, then *Settings* > *Server settings* > *Certificate*. FortiClient (Android) automatically goes to certdir, the configured certificate location. Select the certificate, enter the password, then click *Connect*. The tunnel establishes successfully.



Autoconnect to IPsec VPN using Entra ID logon session information

This feature enables seamless and secure connectivity for users accessing corporate resources by automatically establishing IPsec VPN connections based on Microsoft Entra ID (formerly known as Azure Active Directory or AD) logon session information.

In the example use case, an organization has implemented a comprehensive security strategy that includes using IPsec VPN for securing communications between its network resources. To enhance user experience and streamline the connectivity process, the organization wants to implement IPsec VPN autoconnect, leveraging Entra ID logon session information. With automated IPsec VPN connections, users can focus on their tasks without the burden of manual VPN setup processes. Leveraging Entra ID logon session information ensures that only compliant and authenticated users can establish IPsec VPN connection.



The following instructions assume the following:

- You have configured an enterprise application on your Entra ID domain.
- The FortiClient (Windows) endpoint is connected to that Entra ID domain.

To configure FortiOS for this use case:

1. Configure the msgraph user:

```
config user external-identity-provider
    edit "msgraph"
        set type ms-graph
        set version v1.0
    next
end
```

2. Assign the msgraph user to the msgraphgrp group:

```
config user group
    edit "msgraphgrp"
        set member "msgraph"
    next
end
```

3. Create an IPsec VPN tunnel that uses IKEv2. This example uses childless IKE authentication. Ensure that you enable the `azure-ad-autoconnect` option:

```
config vpn ipsec phase1-interface
    edit "Azure"
        set type dynamic
        set interface "port1"
        set ike-version 2
        set peertype any
        set net-device disable
        set mode-cfg enable
        set proposal aes128-sha256 aes256-sha256 aes128gcm-prfsha256 aes256gcm-prfsha384
chacha20poly1305-prfsha256
        set comments "VPN: Azure (Created by VPN wizard)"
        set dhgrp 5
        set authusrgrp "msgraphgrp"
        set childless-ike enable
        set azure-ad-autoconnect enable
        set ipv4-start-ip 192.168.1.1
        set ipv4-end-ip 192.168.1.255
        set dns-mode auto
        set ipv4-split-include "Azure_split"
        set save-password enable
        set client-auto-negotiate enable
        set client-keep-alive enable
        set psksecret ENC
IdtpOOstic/GXm0KwTMjMVlhWoZIcHWPCM5RMfvk9Q7jLbgSwhHhkdyo35bMrNzdUglsq8saXNGM5fcnczNC1X9Yn
1E3F3THUE5U+g1XoIgXJt98VoEs4ROYGZaCOQTBusqMgBmtmRGSY3kZVzgk+Ym+lCpEPaPvTLxmzXT5h7xl4MFMuO
T+6v3cmb6Rz/xoq1zXFg==
    next
end
```

To configure EMS for this use case:

1. Go to *Endpoint Profiles > Remote Access*.
2. Select the desired profile.
3. In XML view, configure the following for the desired tunnel for FortiClient to automatically connect to. This example configures an IPsec VPN tunnel as the tunnel that FortiClient automatically connects to. For `<client_id>`, enter the Entra ID application ID. For `<tenant_name>`, enter the Entra ID tenant ID. You can find these values in the Entra ID portal:

```
<forticlient_configuration>
    <vpn>
        <enabled>1</enabled>
        <sslvpn>
            <connections/>
            <options>
                <dnscache_service_control>0</dnscache_service_control>
                <enabled>1</enabled>
                <disallow_invalid_server_certificate>0</disallow_invalid_server_certificate>
                <warn_invalid_server_certificate>1</warn_invalid_server_certificate>
                <negative_split_tunnel_metric/>
                <preferred_dtls_tunnel>0</preferred_dtls_tunnel>
                <prefer_sslvpn_dns>1</prefer_sslvpn_dns>
                <no_dns_registration>0</no_dns_registration>
            </options>
        </sslvpn>
        <ipsecvpn>
            <connections>
                <connection>
                    <name>IPSEC</name>
                    <uid>AECD683C-310E-4747-815A-B53C86983CFB</uid>
                    <machine>0</machine>
                    <keep_running>0</keep_running>
                    <disclaimer_msg/>
                    <sso_enabled>0</sso_enabled>
                    <single_user_mode>0</single_user_mode>
                    <type>manual</type>
                    <ui>
                        <show_remember_password>1</show_remember_password>
                        <show_alwaysup>1</show_alwaysup>
                        <show_autoconnect>1</show_autoconnect>
                        <show_passcode>0</show_passcode>
                        <save_username>0</save_username>
                    </ui>
                    <redundant_sort_method>0</redundant_sort_method>
                    <tags>
                        <allowed/>
                        <prohibited/>
                    </tags>
                    <host_check_fail_warning/>
                    <ike_settings>
                        <server>172.19.200.113</server>
                        <authentication_method>Preshared Key</authentication_method>
```

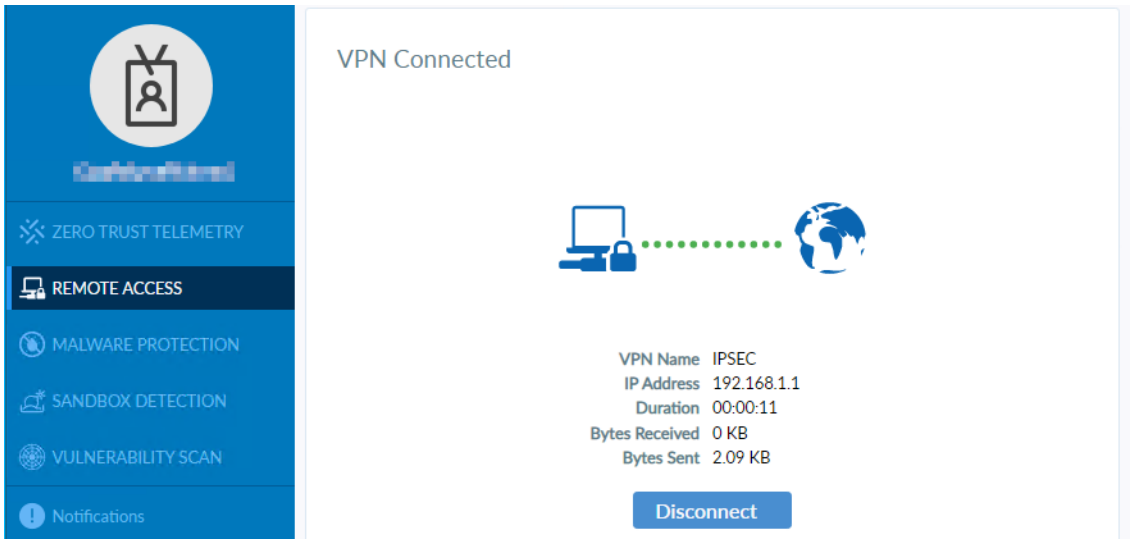
```
                        <fgt>1</fgt>
                        <prompt_certificate>0</prompt_certificate>
                        <xauth>
                            <use_otp>0</use_otp>
                            <enabled>0</enabled>
                            <prompt_username>0</prompt_username>
                        </xauth>
                        <version>2</version>
                        <mode>aggressive</mode>
                        <key_life>86400</key_life>
                        <localid/>
                        <implied_SPDO>0</implied_SPDO>
                        <implied_SPDO_timeout>96</implied_SPDO_timeout>
                        <nat_traversal>1</nat_traversal>
                        <nat_alive_freq>5</nat_alive_freq>
                        <enable_local_lan>0</enable_local_lan>
                        <enable_ike_fragmentation>0</enable_ike_fragmentation>
                        <mode_config>1</mode_config>
                        <dpd>1</dpd>
                        <dpd_retry_count>3</dpd_retry_count>
                        <dpd_retry_interval>5</dpd_retry_interval>
                        <run_fcauth_system>0</run_fcauth_system>
                        <auth_data>
                            <preshared_key>Enc
8000cad35ca0ce889e17d2f949042781fd02a57a1ae7afb13be95840b7e4</preshared_key>
                        </auth_data>
                        <dhgroup>5;14</dhgroup>
                        <proposals>
                            <proposal>AES128|SHA1</proposal>
                            <proposal>AES256|SHA256</proposal>
                        </proposals>
                        <azure_auto_login>
                         <enabled>1</enabled>
                         <azure_app>
                           <client_id>Example client ID</client_id>
                           <tenant_name>Example tenant ID</tenant_name>
                         </azure_app>
                      </azure_auto_login>
                    </ike_settings>
                    <ipsec_settings>
                        <remote_networks>
                            <network>
                                <addr>0.0.0.0</addr>
                                <mask>0.0.0.0</mask>
                            </network>
                            <network>
                                <addr>::/0</addr>
                                <mask>::/0</mask>
                            </network>
                        </remote_networks>
                        <dhgroup>5</dhgroup>
```

```
            <key_life_type>seconds</key_life_type>
            <key_life_seconds>43200</key_life_seconds>
            <key_life_Kbytes>5200</key_life_Kbytes>
            <replay_detection>1</replay_detection>
            <pfs>1</pfs>
            <use_vip>1</use_vip>
            <virtualip>
                <type>modeconfig</type>
                <ip>0.0.0.0</ip>
                <mask>0.0.0.0</mask>
                <dnsserver>0.0.0.0</dnsserver>
                <winserver>0.0.0.0</winserver>
            </virtualip>
            <proposals>
                <proposal>AES128|SHA1</proposal>
                <proposal>AES256|SHA256</proposal>
            </proposals>
        </ipsec_settings>
        <android_cert_path/>
        <warn_invalid_server_certificate>1</warn_invalid_server_certificate>
        <on_connect>
            <script>
                <os>windows</os>
                <script/>
            </script>
            <script>
                <os>MacOSX</os>
                <script/>
            </script>
            <script>
                <os>linux</os>
                <script/>
            </script>
        </on_connect>
        <on_disconnect>
            <script>
                <os>windows</os>
                <script/>
            </script>
            <script>
                <os>MacOSX</os>
                <script/>
            </script>
            <script>
                <os>linux</os>
                <script/>
            </script>
        </on_disconnect>
        <traffic_control>
            <enabled>0</enabled>
            <mode>1</mode>
```

```
                </traffic_control>
            </connection>
        </connections>
        <options>
            <enhanced_key_usage_mandatory>0</enhanced_key_usage_mandatory>
            <use_win_local_computer_cert>1</use_win_local_computer_cert>
            <disable_default_route>0</disable_default_route>
            <enabled>1</enabled>
            <usesmcardcert>1</usesmcardcert>
            <disallow_invalid_server_certificate>0</disallow_invalid_server_certificate>
            <block_ipv6>1</block_ipv6>
            <usewincert>1</usewincert>
            <use_win_current_user_cert>1</use_win_current_user_cert>
            <show_auth_cert_only>0</show_auth_cert_only>
            <check_for_cert_private_key>0</check_for_cert_private_key>
            <uselocalcert>0</uselocalcert>
            <beep_if_error>0</beep_if_error>
            <no_dns_registration>0</no_dns_registration>
            <enable_udp_checksum>0</enable_udp_checksum>
        </options>
    </ipsecvpn>
    <lockdown>
        <enabled>0</enabled>
        <exceptions>
            <apps/>
            <ips/>
        </exceptions>
        <max_attempts>3</max_attempts>
        <grace_period>120</grace_period>
    </lockdown>
    <options>
        <on_os_start_connect/>
        <on_os_start_connect_has_priority>0</on_os_start_connect_has_priority>
        <autoconnect_only_when_offnet>0</autoconnect_only_when_offnet>
        <autoconnect_on_install>0</autoconnect_on_install>
        <keep_running_max_tries>0</keep_running_max_tries>
        <suppress_vpn_notification>0</suppress_vpn_notification>
        <secure_remote_access>0</secure_remote_access>
        <minimize_window_on_connect>1</minimize_window_on_connect>
        <allow_sslvpn>0</allow_sslvpn>
        <show_negotiation_wnd>0</show_negotiation_wnd>
        <use_legacy_vpn_before_logon>0</use_legacy_vpn_before_logon>
        <show_vpn_before_logon>0</show_vpn_before_logon>
        <use_windows_credentials>0</use_windows_credentials>
        <disable_connect_disconnect>0</disable_connect_disconnect>
        <allow_personal_vpns>1</allow_personal_vpns>
        <autoconnect_tunnel>IPSEC</autoconnect_tunnel>
    </options>
</vpn>
<endpoint_control>
    <ui>
```

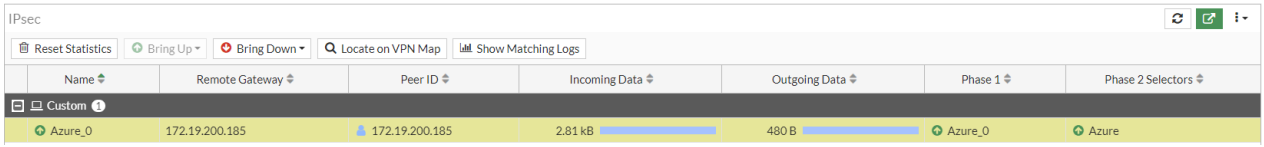
```
            <display_vpn>1</display_vpn>
        </ui>
    </endpoint_control>
</forticlient_configuration>
```

After the profile changes sync to the endpoint, it autoconnects to the IPsec VPN tunnel.



To verify the connection:

1. From the endpoint, ping the internal server located behind the edge FortiGate. The ping succeeds.
2. In FortiOS, go to *Dashboard* > *Network* and expand the *IPsec* widget. Observe that the tunnel is up.



3. View debug logs on FortiOS by running `diagnose debug enable` and `diagnose debug application ike-1` commands. The following shows the example output, which includes the endpoint IP address, hostname, and serial number:

```
Debug messages will be on for 30 minutes.
(root) # 2023-11-28 15:52:07.878432 ike 0: comes
172.19.200.185:500>172.19.200.113:500,ifindex=3,vrf=0....
2023-11-28 15:52:07.878511 ike 0: IKEv2 exchange=SA_INIT
id=d9ae37737ffaa01f/0000000000000000 len=468
2023-11-28 15:52:07.878517 ike 0: in
D9AE37737FFAA01F0000000000000000212022080000000000000001D42200006C020000340101000503000000C0
100000C800E008003000008020000020300000803

000002030000080400000E000000080400000500000034020100050300000C0100000C800E010003000008020
000050300000803000000C030000080400000E000000080400000528000C80005000029C52815C
```

```
D2472B215CE446B390FE2DF7C6F052B8D7944B839A10FCF82153A4B45D3B643A6E1780214D599926C29C343BE
E53AFA1E9E5E2D21E8E50A2401E36EC5C50C087E8BEB44C42E63AE180B6AD200B7C9D0CC383071

2BFBFE094239F2D8DDD688CCF47ACFEC2E6BF0AA12741D464C3DB27B281D592D6380E8D7B0CFB5EDEA3AD2C70
8EF3DF586208F6FD4546D5C2BA940B753D85B167F1B579189E4799963B0A52D5F25715F7FADA4A

374429CDA00A47867F430F12BE423EB60FB026B762B000014B8CC569F7DF724021D79F462613E502E2B000014
4C53427B6D465D1B337BB755A37A7FEF29000014B4F01CA951E9DA8D0BAFBBD34AD3044E290000

1C00004004E899574FF8046F347253D49303195705324AB60F2900001C000040051601420DB7DE78D205377D3
EC86A5AC8FBE790D6290000080100F1060000000801004022
2023-11-28 15:52:07.878529 ike 0:d9ae37737ffaa01f/0000000000000000:31: responder received
SA_INIT msg
2023-11-28 15:52:07.878533 ike 0:d9ae37737ffaa01f/0000000000000000:31: VID forticlient
connect license 4C53427B6D465D1B337BB755A37A7FEF
2023-11-28 15:52:07.878538 ike 0:d9ae37737ffaa01f/0000000000000000:31: VID Fortinet
Endpoint Control B4F01CA951E9DA8D0BAFBBD34AD3044E
2023-11-28 15:52:07.878541 ike 0:d9ae37737ffaa01f/0000000000000000:31: received notify
type NAT_DETECTION_SOURCE_IP
2023-11-28 15:52:07.878545 ike 0:d9ae37737ffaa01f/0000000000000000:31: received notify
type NAT_DETECTION_DESTINATION_IP
2023-11-28 15:52:07.878763 ike 0:d9ae37737ffaa01f/0000000000000000:31: received notify
type AZURE_AD_AUTOCONNECT
2023-11-28 15:52:07.878767 ike 0:d9ae37737ffaa01f/0000000000000000:31: received notify
type CHILDLESS_IKEV2_SUPPORTED
2023-11-28 15:52:07.878771 ike 0:d9ae37737ffaa01f/0000000000000000:31: ignoring
unauthenticated notify payload (CHILDLESS_IKEV2_SUPPORTED)
2023-11-28 15:52:07.878983 ike 0:d9ae37737ffaa01f/0000000000000000:31: incoming proposal:
2023-11-28 15:52:07.878987 ike 0:d9ae37737ffaa01f/0000000000000000:31: proposal id = 1:
2023-11-28 15:52:07.879196 ike 0:d9ae37737ffaa01f/0000000000000000:31:   protocol =
IKEv2:
2023-11-28 15:52:07.879199 ike 0:d9ae37737ffaa01f/0000000000000000:31:      encapsulation
= IKEv2/none
2023-11-28 15:52:07.879203 ike 0:d9ae37737ffaa01f/0000000000000000:31:         type=ENCR,
val=AES_CBC (key_len = 128)
2023-11-28 15:52:07.879205 ike 0:d9ae37737ffaa01f/0000000000000000:31:
type=INTEGR, val=AUTH_HMAC_SHA_96
2023-11-28 15:52:07.879419 ike 0:d9ae37737ffaa01f/0000000000000000:31:         type=PRF,
val=PRF_HMAC_SHA
2023-11-28 15:52:07.879423 ike 0:d9ae37737ffaa01f/0000000000000000:31:         type=DH_
GROUP, val=MODP1536.
2023-11-28 15:52:07.879426 ike 0:d9ae37737ffaa01f/0000000000000000:31:         type=DH_
GROUP, val=MODP2048.
2023-11-28 15:52:07.879430 ike 0:d9ae37737ffaa01f/0000000000000000:31: proposal id = 2:
2023-11-28 15:52:07.879640 ike 0:d9ae37737ffaa01f/0000000000000000:31:   protocol =
IKEv2:
2023-11-28 15:52:07.879643 ike 0:d9ae37737ffaa01f/0000000000000000:31:      encapsulation
= IKEv2/none
```

```
2023-11-28 15:52:07.879646 ike 0:d9ae37737ffaa01f/0000000000000000:31:         type=ENCR,
val=AES_CBC (key_len = 256)
2023-11-28 15:52:07.879649 ike 0:d9ae37737ffaa01f/0000000000000000:31:
type=INTEGR, val=AUTH_HMAC_SHA2_256_128
2023-11-28 15:52:07.879860 ike 0:d9ae37737ffaa01f/0000000000000000:31:         type=PRF,
val=PRF_HMAC_SHA2_256
2023-11-28 15:52:07.879863 ike 0:d9ae37737ffaa01f/0000000000000000:31:         type=DH_
GROUP, val=MODP1536.
2023-11-28 15:52:07.879866 ike 0:d9ae37737ffaa01f/0000000000000000:31:         type=DH_
GROUP, val=MODP2048.
2023-11-28 15:52:07.879874 ike 0:d9ae37737ffaa01f/0000000000000000:31: matched proposal
id 2
2023-11-28 15:52:07.880080 ike 0:d9ae37737ffaa01f/0000000000000000:31: proposal id = 2:
2023-11-28 15:52:07.880083 ike 0:d9ae37737ffaa01f/0000000000000000:31:   protocol =
IKEv2:
2023-11-28 15:52:07.880336 ike 0:d9ae37737ffaa01f/0000000000000000:31:      encapsulation
= IKEv2/none
2023-11-28 15:52:07.880339 ike 0:d9ae37737ffaa01f/0000000000000000:31:         type=ENCR,
val=AES_CBC (key_len = 256)
2023-11-28 15:52:07.880342 ike 0:d9ae37737ffaa01f/0000000000000000:31:
type=INTEGR, val=AUTH_HMAC_SHA2_256_128
2023-11-28 15:52:07.880344 ike 0:d9ae37737ffaa01f/0000000000000000:31:         type=PRF,
val=PRF_HMAC_SHA2_256
2023-11-28 15:52:07.880345 ike 0:d9ae37737ffaa01f/0000000000000000:31:         type=DH_
GROUP, val=MODP1536.
2023-11-28 15:52:07.880347 ike 0:d9ae37737ffaa01f/0000000000000000:31: lifetime=86400
2023-11-28 15:52:07.880351 ike 0:d9ae37737ffaa01f/0000000000000000:31: SA proposal
chosen, matched gateway Azure
2023-11-28 15:52:07.880369 ike 0:Azure: created connection: 0x10bdc0b0 3 172.19.200.113-
>172.19.200.185:500.
2023-11-28 15:52:07.880375 ike 0:Azure:31: processing notify type NAT_DETECTION_SOURCE_IP
2023-11-28 15:52:07.880391 ike 0:Azure:31: processing NAT-D payload
2023-11-28 15:52:07.880396 ike 0:Azure:31: NAT not detected
2023-11-28 15:52:07.880398 ike 0:Azure:31: process NAT-D
2023-11-28 15:52:07.880400 ike 0:Azure:31: processing notify type NAT_DETECTION_
DESTINATION_IP
2023-11-28 15:52:07.880407 ike 0:Azure:31: processing NAT-D payload
2023-11-28 15:52:07.880409 ike 0:Azure:31: NAT not detected
2023-11-28 15:52:07.880411 ike 0:Azure:31: process NAT-D
2023-11-28 15:52:07.880413 ike 0:Azure:31: processing notify type AZURE_AD_AUTOCONNECT
2023-11-28 15:52:07.880425 ike 0:Azure:31: enable FortiClient endpoint compliance check,
use 169.254.1.1
2023-11-28 15:52:07.880436 ike 0:Azure:31: responder preparing SA_INIT msg
2023-11-28 15:52:07.880460 ike 0:Azure:31: generate DH public value request queued
2023-11-28 15:52:07.880467 ike 0:Azure:31: responder preparing SA_INIT msg
2023-11-28 15:52:07.880660 ike 0:Azure:31: compute DH shared secret request queued
2023-11-28 15:52:07.880665 ike 0:Azure:31: responder preparing SA_INIT msg
2023-11-28 15:52:07.880668 ike 0:Azure:31: create NAT-D hash local 172.19.200.113/500
```

```
remote 172.19.200.185/500
2023-11-28 15:52:07.880674 ike 0:Azure:31: out
D9AE37737FFAA01FE0E51AE3ED77F208212022200000000000000168220000300000002C020100040300000C0
100000C800E0100030000080200000 5

03000008030000C000000080400000 5280000C80005000019215B62D25A7F7A5E7B358E5B2C1C3C70084FD3A
606A456015CF1A74314BCD7B5372C2CFBA2AB3F4DEA7A5531C27B59CC043D3BAE9002875A64966

DFA7E6A953742D24719C5E3D8D5D45D50A46C700DB099C0D7A0C719CAD5E0D6B061FE75CF3B1E5E492E9AFDC8
D5E0020FA2E93A4208BE12604E8E1EE4A6B68C6131164DE13D03DF19214F9685C2ADAA3CE8768D

0E47654EBA43016F0E61C5FEE550FA44A822334501F56199BD0DDD7BB19C0D8BF5AC626D6D9F7069ECE2F9321
91A0D30E22900001456BC1469291826AE59A604D454BFF2BF2900001C00004004F6DBD029D92D8

03928AE0CE23033027A9C20CAE92900001C000040054F8EE7A0730C99FD82681C8CAF9D7F488C6EE751000000
0801004022
2023-11-28 15:52:07.880692 ike 0:Azure:31: sent IKE msg (SA_INIT_RESPONSE):
172.19.200.113:500->172.19.200.185:500, len=360, vrf=0,
id=d9ae37737ffaa01f/e0e51ae3ed77f20
8
2023-11-28 15:52:07.880725 ike 0:Azure:31: IKE SA d9ae37737ffaa01f/e0e51ae3ed77f208 SK_ei
32:021F8486C8956677F0B0F1F2BA452F75DD9833DA841D47DA772126AFE49CBF1B
2023-11-28 15:52:07.880728 ike 0:Azure:31: IKE SA d9ae37737ffaa01f/e0e51ae3ed77f208 SK_er
32:A5EF924BD16BCE20AE70FE0FD61EAF70781D575E6EFA8F788A666B6700EA2DED
2023-11-28 15:52:07.880731 ike 0:Azure:31: IKE SA d9ae37737ffaa01f/e0e51ae3ed77f208 SK_ai
32:382A41BB8F3AD7A75964AA0E686052E71E63E3CC2C932EF15987A44DB3F5911A
2023-11-28 15:52:07.880738 ike 0:Azure:31: IKE SA d9ae37737ffaa01f/e0e51ae3ed77f208 SK_ar
32:4C1FC87AE6A0912DAA2636F2A81FBA793E702DA73FBEEAA3504EEAB68B32F193
2023-11-28 15:52:07.993013 ike 0: comes 172.19.200.185:500-
>172.19.200.113:500,ifindex=3,vrf=0....
2023-11-28 15:52:07.993062 ike 0: IKEv2 exchange=AUTH
id=d9ae37737ffaa01f/e0e51ae3ed77f208:00000001 len=464
2023-11-28 15:52:07.993290 ike 0: in
D9AE37737FFAA01FE0E51AE3ED77F2082E202308000000010000001D0230001B4E7B1C9245F45F810624FFD12C
9F2A28B2F2C08E9401A2AA912E7A53BE340A62EF5

5B7617F3B1EA24AAC418B700B79127C1763D611430D75C12D7AAF4AB48289536DF9812D23A742255846E785CA
1F93405BBD31240155DED929C1AA9AEB2C6E4DE29DE2B305EC3B4ADFDB2ECD31FEF13A5B20C9AB

5FE18E83F3A5A8A8FB9826512545661675ED918D7687429FDFCA7156FECD7E95DFEF9FE399A760167F0292EAA
7601FE9E02BF4265EE6A3291747029E483D4C5C319F4885C2A5C4E1AA74BFF38857285E4B9128F

6BD7875A193D27C63692C6A082B2E3AF4C97ECE69486688397470A7160AF07604F168298F44EE433FDD91A23A
6746B4A34232D0C60EDCE3A869F46D00340FD314E3A19E23813DCD55D6F001C9A461A9151FC434

7212AE54D139BFBD95072184D6BCD96BFE91A77484A14EF21A510947AF72004E73188BDCA2D90B99B26C6ADAE
0DED61096A5A9033250DB16CAFB8330F8B86374EE426F22A37F1B5E4B4C03B785064601CD9D786
```

```
B97F1A5915AE1FF0AAB9548C0AB645E8817AA421E16F2190F38F708FDA1ED0FB8E242B1251D36A4AEF3B84CDF
858D6CA30118400B7DE7CD32AB86E5BCBFEAFA38E
2023-11-28 15:52:07.993602 ike 0:Azure:31: dec
D9AE37737FFAA01FE0E51AE3ED77F2082E2023080000000100000 1A9230000042900000C01000000AC13C8B92
900000800004000270001010000F100

5645523D310A4643545645523D372E322E332E303931380A5549443D434643363241413233463334343233354
2354438413631383535453746463644 0A49503D3137322E31392E3230302E3138350A4D41433D3

0302D31352D35642D35312D30332D30343B0A484F53543D4445534B544F502D3043444F4633560A555345523D
476F70696368616E644D75726172690A4F535645523D4D6963726F736F66742057696E646F7773

20313020456E7465727072697365204564697 4696F6E2C2036342D62697420286275696C64203139303435290
A5245475F5354415455533D300A454D53534E3D464354454D533838323330393137303 20A002F0

0002802000000A5C200F5D13E654044C91714F1EC7BBC77964528DB2A56F03CBD82F7EECCEBEF290000440100
0000000700104643543830303035333230323530333000010000000200000003000000040000000
0D000070010000540A0000540B0000700000000019000000000008000040 22
2023-11-28 15:52:07.993807 ike 0:Azure:31: responder received AUTH msg
2023-11-28 15:52:07.994029 ike 0:Azure:31: processing notify type INITIAL_CONTACT
2023-11-28 15:52:07.994083 ike 0:Azure:31: processing notify type FORTICLIENT_CONNECT
2023-11-28 15:52:07.994277 ike 0:Azure:31: received FCT data len = 249, data = 'VER=1
FCTVER=7.2.3.0918
UID=CFC62AA23F344235B5D8A61855E7FF6D
IP=172.19.200.185
MAC=00-15-5d-51-03-04;
HOST=DESKTOP-0CDOF3V
USER=MCarey
OSVER=Microsoft Windows 10 Enterprise Edition, 64-bit (build 19045)
REG_STATUS=0
EMSSN=FCTEMS123456
'
2023-11-28 15:52:07.994510 ike 0:Azure:31: received FCT-UID :
CFC62AA23F344235B5D8A61855E7FF6D
2023-11-28 15:52:07.994714 ike 0:Azure:31: received EMS SN : FCTEMS123456
2023-11-28 15:52:07.994736 ike 0:Azure:31: EMS SN check passed
2023-11-28 15:52:07.994939 ike 0:Azure:31: processing notify type CHILDLESS_IKEV2_
SUPPORTED
2023-11-28 15:52:07.994965 ike 0:Azure:31: peer identifier IPV4_ADDR 172.19.200.185
2023-11-28 15:52:07.995168 ike 0:Azure:31: re-validate gw ID
2023-11-28 15:52:07.995178 ike 0:Azure:31: gw validation OK
2023-11-28 15:52:07.995413 ike 0:Azure:31: auth verify done
2023-11-28 15:52:07.995628 ike 0:Azure:31: responder AUTH continuation
2023-11-28 15:52:07.995634 ike 0:Azure:31: authentication succeeded
2023-11-28 15:52:07.995874 ike 0:Azure:31: mode-cfg type 7 request
16:'46435438303030353332303235303330'
2023-11-28 15:52:07.996080 ike 0:Azure:31: mode-cfg received APPLICATION_VERSION
'FCT8000532025030'
```

```
2023-11-28 15:52:07.996086 ike 0:Azure:31: mode-cfg type 1 request 0:''
2023-11-28 15:52:07.996312 ike 0:Azure: mode-cfg allocate 192.168.1.1/0.0.0.0
2023-11-28 15:52:07.996319 ike 0:Azure:31: mode-cfg using allocated IPv4 192.168.1.1
2023-11-28 15:52:07.996535 ike 0:Azure:31: mode-cfg type 2 request 0:''
2023-11-28 15:52:07.996540 ike 0:Azure:31: mode-cfg type 3 request 0:''
2023-11-28 15:52:07.996763 ike 0:Azure:31: mode-cfg type 4 request 0:''
2023-11-28 15:52:07.996769 ike 0:Azure:31: mode-cfg WINS ignored, no WINS servers
configured
2023-11-28 15:52:07.996989 ike 0:Azure:31: mode-cfg type 13 request 0:''
2023-11-28 15:52:07.996995 ike 0:Azure:31: mode-cfg type 28673 request 0:''
2023-11-28 15:52:07.997215 ike 0:Azure:31: mode-cfg UNITY type 28673 requested
2023-11-28 15:52:07.997446 ike 0:Azure:31: mode-cfg type 21514 request 0:''
2023-11-28 15:52:07.997451 ike 0:Azure:31: mode-cfg type 21514 requested
2023-11-28 15:52:07.997455 ike 0:Azure:31: mode-cfg type 21515 request 0:''
2023-11-28 15:52:07.997460 ike 0:Azure:31: mode-cfg type 21515 requested
2023-11-28 15:52:07.997464 ike 0:Azure:31: mode-cfg type 28672 request 0:''
2023-11-28 15:52:07.997468 ike 0:Azure:31: mode-cfg UNITY type 28672 requested
2023-11-28 15:52:07.997472 ike 0:Azure:31: mode-cfg no banner configured, ignoring
2023-11-28 15:52:07.997476 ike 0:Azure:31: mode-cfg type 25 request 0:''
2023-11-28 15:52:07.997483 ike 0:Azure:31: responder preparing AUTH msg
2023-11-28 15:52:07.997489 ike 0:Azure: IPv6 pool is not configured
2023-11-28 15:52:07.997494 ike 0:Azure: adding new dynamic tunnel for 172.19.200.185:500
2023-11-28 15:52:07.997513 ike 0:Azure_0: tunnel created tun_id 192.168.1.1/::10.0.0.11
remote_location 0.0.0.0
2023-11-28 15:52:07.997592 ike 0:Azure_0: added new dynamic tunnel for 172.19.200.185:500
2023-11-28 15:52:07.997598 ike 0:Azure_0:31: established IKE SA
d9ae37737ffaa01f/e0e51ae3ed77f208
2023-11-28 15:52:07.997606 ike 0:Azure_0:31: check peer route: if_addr4_rcvd=0, if_addr6_
rcvd=0, mode_cfg=1
2023-11-28 15:52:07.997614 ike 0:Azure_0:31: processing INITIAL-CONTACT
2023-11-28 15:52:07.997617 ike 0:Azure_0: flushing
2023-11-28 15:52:07.997635 ike 0:Azure_0: flushed
2023-11-28 15:52:07.997638 ike 0:Azure_0:31: processed INITIAL-CONTACT
2023-11-28 15:52:07.997655 ike 0:Azure_0:31: mode-cfg assigned (1) IPv4 address
192.168.1.1
2023-11-28 15:52:07.997658 ike 0:Azure_0:31: mode-cfg assigned (2) IPv4 netmask
255.255.255.255
2023-11-28 15:52:07.997662 ike 0:Azure_0:31: mode-cfg send (13)
0:192.168.150.0/255.255.255.0:0
2023-11-28 15:52:07.997664 ike 0:Azure_0:31: mode-cfg send (3) IPv4 DNS(1) 96.45.45.45
2023-11-28 15:52:07.997667 ike 0:Azure_0:31: mode-cfg send (3) IPv4 DNS(2) 96.45.46.46
2023-11-28 15:52:07.997669 ike 0:Azure_0:31: mode-cfg send APPLICATION_VERSION
'FortiGate-VM64-HV v7.2.5,build8347,230829 (GA)'
2023-11-28 15:52:07.997671 ike 0:Azure_0:31: mode-cfg send (28673) UNITY_SAVE_PASSWD
2023-11-28 15:52:07.997674 ike 0:Azure_0:31: mode-cfg send (21514) FNT_AUTO_NEGOTIATE
2023-11-28 15:52:07.997676 ike 0:Azure_0:31: mode-cfg send (21515) FNT_KEEP_ALIVE
2023-11-28 15:52:07.997678 ike 0:Azure_0:31: add INTERFACE-ADDR4 169.254.1.1
2023-11-28 15:52:07.997685 ike 0:Azure_0:31: enc
```

```
2700000C01000000AC13C8712F00002802000000032B2600E754DD686A012B0F6F15B5AACF188C6E360430E08
2BCDFDA0C720EC129000078020000

0000010004C0A8010100020004FFFFFFFF000D0008C0A89600FFFFFF0000030004602D2D2D00030004602D2E2
E0007002E466F727469476174652D564D36342D48562076372E322E352C6275696C64383334372

C3233303832392028474129700100020001540A00020001540B00020001000000C0000F0F9A9FE0101070605
0403020107
2023-11-28 15:52:07.997699 ike 0:Azure_0:31: out
D9AE37737FFAA01FE0E51AE3ED77F2082E2023200000000100000100240000E4F3993F243D0F8263A8437BAE5
FA374BDCCB76F12A529CF6D140BDB

7D16F4A31BCF8A01BF7FF565745E7A34CEF5DA87D60248CE37ECC09215900856FFD63450E0051F599310EAF79
9FB34362432B731B6A1CFD33A47923089B4989C08F2E8ADB97CB6DC62FE3D5B8A2F556B9A9F7B2

1455AF2B117804AEFFAB89332A0CEAFF6C1D45AFDAB9C8158074F8D9F1440500FA0BEB08B873C299BD9E55468
8D9A5BD986DD42974E0F247CC80DA4025BF026C05CEB1248A95C86483ECB765FBA232F6E07D0E6
7FBAEB45416899D51C253077D91C4E9D8BD7DDACDC5425510CAC1BC0B1CF
2023-11-28 15:52:07.997721 ike 0:Azure_0:31: sent IKE msg (AUTH_RESPONSE):
172.19.200.113:500->172.19.200.185:500, len=256, vrf=0,
id=d9ae37737ffaa01f/e0e51ae3ed77f208
:00000001
2023-11-28 15:52:08.110149 ike 0: comes 172.19.200.185:500-
>172.19.200.113:500,ifindex=3,vrf=0....
2023-11-28 15:52:08.110199 ike 0: IKEv2 exchange=INFORMATIONAL
id=d9ae37737ffaa01f/e0e51ae3ed77f208:00000002 len=2240
2023-11-28 15:52:08.110432 ike 0: in
D9AE37737FFAA01FE0E51AE3ED77F2082E2025080000000200000 8C0290008A49B6A9D7BD4E662F6667AF723F
93D5160ED6B11316EEA6DF7D75902415CD63031EF

F10A6D97A8409055084EB77803F990D01B2156EF6465F3087AE50297634090 3689A8D9D4ED842DBA99E4321FF
23844FA93051D39987C5AAB2D1376805066E44D318566A0A1AAFB8443C9E53B04B0BEF5519A6E3

4FF0351BAAB2343987A9845665B4A4B902C6F684284C156A5FC0F71D8B32D2F8A8C6BD0C1780723915CD9ABC3
6299EFF3D7FAF9EEB8C05BEFDB0396241E37AC740E9B37EFA80849FA5F610E34D315A9B6800EB9

EE7D6264772E78FF2A1E829B183DF08BCCB5F6FE7EF97E3DFD7721416E587584AE570BDA90F51B854FBE49126
9323A8B2769092658EFF3603786B4D6F9A42BDDA28ADA53FB57ACE83A002F8E22C73B1BAAAB95C

13843E0F13E0BB38A35E134276DBA0028775D43D9E63626FA740CD2ADE5B1E044FB136498C1391E13180A878A
011D1EAFEF705959F04EDAAFB1F4D0B4D7BE32595BF0626B48A8B4A4FE60BF3E3F258D07EA4474

2F763EA6021A209BE7026F3B694D078B4D083B0AB5E018D8FDD4E236E0428CC22A6A5E3F14D01E0D0E574DB9C
D058ADCDBA705E3A3FA9E445BFEB9015B367C458AF0510072C3B7FCF59346FDA3D9B90D69FA283

E553773E6F9C8CCC17630F33DCA445D5847DF9F5599CD8A9E1E65F99113F3BC18D88A70BB11D7EAAA9858DA28
4B488F58B49EC7E879FE1FE7126BDCCCFFB2CD62447203DE15485F957A602160D739B38F57EB18
```

```
023F4023C1C8C30729D87EF932701E69BA474478222FA4A427F38EA36B314F452CCD29C57F75A7BD1596AA430
0C42714BEF3E3A538786F30668B714880F2A2715C6B18AAA61DBFAA98C22302319917BEB5219A1

70B7250B69402A84697685055CDCE5B276B047FB172501DEA4FC7EF51A4B3FE06B590F212C9DCBB6AEF859A8F
D3E4A5118B603E75218294C3DF97A009F2CDD5D31CA9E28CB9C5A1D5CA56B3B6C0DF9BA7DED12E

0A44CE3A2C8B0101B2812B8FD3EC43A0AF07F3701AC6B0F5EA182C9797DCFF215207238A9DC5F3F544A919B6E
147C20847F20AD9CFD602734224EBB3E18A7200DFA06FA9EE6A4F665AE6559587F963C1116A43E

6D673601ABEA502DC789085D9537AC26DCB75A582AD12962C858910EF7AA42E9E04742B80483B02870CB600AE
F9F050A84A44213FDF23B283F73F7E064C9167FCFC63C9DBBBBB8DC8727E27EB62A2B412CF7989

665E248B5514E87264EAE9BE7E870D8243558548706092E2F2FB7B69307808CAA903BCE0B0EDACE95FCE7BD5D
D6D93EEB901BD4C541999D7E16A8ABF7B3FA99B163119CC27D851D42E7820659EBDA3E1649062A

3DE4544F7DC568665A5D5A52D6A62E252D9C6240AB32930B0066ECFBF9E4845768F8708E89A8A699786237D74
1659FB7F36E45F649F860C04523820584F0A668519DC200A16A9AE6F94714A5C9AFAA9CEA3B159

8836482ADA061F3E6BC73CDF18B441E3939F938A407E2FAB66563F32EFDE4EA1D26756B4983CDA332825B6CC7
1A64B3A2790CED7156AE0C7A9D684BBAF50095283C23ADF9882E4901C6DDA7E8132B632B9D33B6

961D1558323FAB4447CC6C1B6E0A543CF289566955CD045D42B3853934E98575FF0EB4F9DDCCD33E16EE39891
85CBD4C536CBEB55F2DE760AD87D0D0896952425F6099EC3775DABEC43669B3060371818B55CB1

09420BC54D6819785BE1D4380878ACA24502D20B8552E035B3FA728340CEC7114D557E9AFE7C6051053E4CF70
2D9C9CEB88F066EDC7C41ED7A2C331EAF1331DBEB965988F564515A11AD7023C4F5EECF73C870A

6B41C9006ADDA326377969F7309E42BEB220F6B8BB0DC4581304B5A26EFBFC91A3E6AF4B5E25DBDEA2AB79EF7
00948B05677B7B613D7C45D273B7A9F1E14809D90154C0B7E57E3144063DECEC730EC22D4AE450

FA064F428DBDAD2E7225AE832C66C4A79CA327EF8DE1B9DC1325CC5D7891A4F3619E813374306AA1379836A4B
7CD50A826E709D33FF24BF4E311DBB960732269470EBCA42F5A68A7038352B0C7DA6454541B3F3

348CED47D7FEFE7131FB3610D7D884B4E71BFEF414235CB6AC577F3D5B4EC816682CDA2480B8D232894AEEF9D
8578A97197D9C33A9D2C4E524A59FA0167D8759D3C2B089D715B005F5FB9403E822A1B5723531A

DD1527A4BEEC54C673470017057E7D6C0A64D1F4463E7453F61A1FA5C60BAD683E11F57ADF8C4147DE337897F
D913FF451A663E511515A1EEF1B64BC66125E310F729712CCBAF97316874986C52D96AB16C7587

31171EEBDAC8948D173532A92473AB990F853657A6E2F299C3C32C534D6560FDAF66C3C2E5CE690C3E0381E28
83E09C9E8F2E039B2403526419A810E048C9BFFB863EB00D4EEA8C2980799AF8FFE4D0FDA92C2E

8AEB30AB1D044CF5E806414B8BF4F630DD54274235295540A230B1E58CBBE6642A0D91AD0DE920B4DE385975A
10F97AB58C01508D43F40531F04EF403E626C06F1D70E6A5649721F60F9CED9ACB70997A265110

83E1E2F373049A1CB0012C181244F90DF3B917B7D337679F4EA3E4F5781929793E57DCE57426DE306E1C7348B
05FF5412AD20CBD323C9ACD9B381462F428EFB084DE2DF4AAA39F3A2498EBE0903E190C89B3CB6
```

```
9FE70EF451C17C337F2965F0F2FCEA63036DAC1735305113720441A040920DE11C76E597D2346766AC231966E
200FB6908954B049B57E077C8F9FF1E43019D22DCB75839C0BE084385510FE6CC225A84E8AE56D

9854C739545EB19DA193E031D59D58270E12D9A5F6E86E4870DD775F1C3C4DB80F5138B20521E7463045E48EF
1C1BE55D40F7AACC65BFA78B2D7C50832A08CAEE1534C9EF0D9309321D685102EA34BC45A62BEB

A927141839B4756BC3D33B33DD6F829762D9FEC37E8C5F6C28D3E0D513967D3E878D597A0F262263D47E696C4
43B3AD33742944F1EA8094AA1147E189EA3DC2E1838C12186A9ADA2534485D026E8456996E9815

0675B20DC5F337A0A90BDFE5516668AD234AF0FA4F0141F8145BF7F931E80C2B62E5517900CBAE94B37748E71
3A895CBB415319FA485C69C4CBE89F689DA9926597548CD5FC1F509F584330B07686F0EDE7EE1B
FCD55949
2023-11-28 15:52:08.110903 ike 0:Azure_0:31: dec
D9AE37737FFAA01FE0E51AE3ED77F2082E2025080000000020000089F290000040000087F0000F10765794A306
55841694F694A4B563151694C434A

756232356A5A534936496D704B4D314A6B55304A7653484A4B4F4570574D6B5A54646A687A595646596246683
36457773357484D325A4656786347307A5A316F74616C45694C434A68624763694F694A53557A4

9314E694973496E673164434936496C5178553351745A457855646E6C58556D6434516C38324E7A5A314F4774
7957464D7453534973496D74705A434936496C5178553351745A457855646E6C58556D6434516C

38324E7A5A314F47747957464D7453534A392E65794A68645751694F6949774D4441774D4441774D7930774D4
441774C5441774D444174597A41774D4330774D4441774D4441774D4441774D4441694C434A706

3334D694F694A6F64485277637A6F764C334E306379353361573 56B6233647A4C6D356C644338315A446B324D
4463335A4330794F47566D4C5451774E5749744F474A6A4E53307A5A6A6333595452695A47526B

5A6D597649697769615746304 96A6F784E7A41784D6A45794E546B794C434A75596D59694F6A45334D4445794
D5449314F544973496D5634634349364D5463774D5449784F4445344F53776959574E6A6443493

64D43776959574E79496A6F694D534973496D467062794936496B4657555546784C7A68575155464251545A48
64446376523064755354525951 6D566C615538356343394C654549315632354 34E46553363474E

6B596D4A4B546B7036626E5252593152305247 4E545158526B54445A3254334E32536D30304B323172656B383
562797435544534315755 6C715169397454304A59626B783365577451526A67334F53745162556

877636E6C6D616E45324D465259636B5646505349734 96D467463694936577 4A7764325169 4C434A79633245
694C434A745A6D4569585377695958427758325270633342735 9586C755957316C496A6F696447

567A6447647663476B694C434A68634842705A434936496A59334D574978597A5A684C5464694E6A4D744E474
E6C595330344F4463334C544D304D544A695A5463344E546B7A59794973496D467763476C6B595

74E79496A6F694D434973496D526C646D6C6A5A576C6B496A6F694D7A41355954526D4D7A4574593249345969
30305A6D4A6D4C546B785A6A67744F474E6B4D324E6D4D574D7759325669496977696157523065

5841694F694A31633256794969776961584268 5A475279496A6F694D6A41344C6A6B784C6A45784E53347A4D4
34973496D3568625755694F694A4862334270593268686 6D5167545856795958 4A70496977696
```

```
2326C6B496A6F694E4467324E4451324E6D45744F546B774F4330305A6A49324C546C6C4D7A41744F5755344D
3249344D6A49305A47526D4969776963477868644759694F69497A4969776963485670 5A434936

496A45774D444D794D4441794E445133516A45314D5463694C434A776432526664584A73496A6F69614852306
3484D364C79397762334A305957777562576C6A636D397A62325A3062323573615735 6C4C6D4E7

662533944614746755A32565159584E7A643239795A4335686333423449697769636D67694F6949774C6B4657
6130466D555756585747553462316377513078345644 6B7A6345777A5A4639335455464251554 6

425155464251586442515546425155464251554642515546445A45464F627934694C434A7A593341694F694A765A6D5A7
36157356C5832466A5932567A6379427663475675615751676348 4A765A6D6C735A53425663325

6794C6C4A6C595751675A573168615777694C434A7A615764756157356663335268644755694F6C7369613231
7A61534A644C434A7A645749694F694A61596D4D7964546C7955486C57636C4A4F6154464F5A31

524A65484E4352575A44566C6C4D52304A72615667795A3168324D6B354A4D325A4A4969776964475675595 73
53058334A6C5A326C76626C397A593239775A534936496B3542496977696476 4C6B496A6F694E5

751354E6A41334E3251744D6A686C5A6930304D4456694C546869597A55744D3259334E324530596D526B5A47
5A6D4969776964573570635856 6C583235686257556 94F694A6E6258567959584A7051455A7663

6E5270513278705A5735304D6A41756232357461574E7962334E765A6E5175593239744969776964584275496
A6F695A323131636D46796155424762334A3061554E7361575675644449774C6D397562576C6A6

36D397A62325A304C6D4E7662534973496E5630615349364964 6A457864484A365447397A4D6A4174636D553455
6D4E6D64463951515763694C434A325A5849694F6949784C6A41694C434A336157527A496A7062

496A59795A546B774D7A6B304C5459355A6A55744E44497A4E7930354D546B774C5441784D6A45334E7A45304
E5755784D434973496D49334F575A695A6A526B4C544E6C5A6A6B744E4459344F5330344D54517

A4C546332596A45354E4755344E5455774F534A644C434A3462584E6664474E6B644349364D5459324E7A4578
4D4451794D33302E4C5173624B7A695A52504F39505971495071754B4C316B39704F477A54776B

35376E3854676B4A616C79327362325333635A7635413137364265395 4A5A4D7978424F366F6349677731324
663304B4841316E354A474E5A36526E74674D73574457476F6968506E756B503474725F5549766

74A567A4578516D67554D6C3545723361635A7849577A41766E3353383259306E6F624573346152686541723 1
387A6271364D435F6137344C7668307332367263435A473675755767656D457A5F523768665039

3473586D4A68506F42564A427175357372662D3366766758615647525559456A6F746441496E744A485241426
3784B5647654E506C7276696C4F6B454D7577694A753544312D4F465064696C7A63686A644A343

2576B5A7A4D6F583250645849706938416F4565784D55435F49425A5A696379514F6A67307776724650537531
464A675539364F3637424841464C2D77
2023-11-28 15:52:08.110922 ike 0:Azure_0:31: received informational request
2023-11-28 15:52:08.110925 ike 0:Azure_0:31: processing notify type AZURE_AD_TOKEN
2023-11-28 15:52:08.110948 ike 0:Azure_0:31: received Azure AD token (len=2167)
```

```
2023-11-28 15:52:08.110949 ike 0:Azure_0:31: initiating Azure AD token authentication
2023-11-28 15:52:08.110951 ike 0:Azure_0: Azure AD token (len=2167)
2023-11-28 15:52:08.110953 ike 0:Azure: auth group msgraphgrp
2023-11-28 15:52:08.111007 ike 0:Azure_0: Azure AD auth 1975011919 pending
2023-11-28 15:52:08.111012 ike 0:Azure_0:31: enc 0F0E0D0C0B0A09080706050403020100F
2023-11-28 15:52:08.111021 ike 0:Azure_0:31: out
D9AE37737FFAA01FE0E51AE3ED77F2082E2025200000000200000050000000034ABDA11BFF7F1B3E0DE37C51CC
74D97E9E750351C4C59506A84CEC1
E9D726613718F6C5928D05641F3BA20B17F06A0E39
2023-11-28 15:52:08.111037 ike 0:Azure_0:31: sent IKE msg (INFORMATIONAL_RESPONSE):
172.19.200.113:500->172.19.200.185:500, len=80, vrf=0, id=d9ae37737ffaa01f/e0e51ae3
ed77f208:00000002
2023-11-28 15:52:08.506195 ike 0:Azure_0:31: Azure AD auth 1975011919 result FNBAM_
SUCCESS
2023-11-28 15:52:08.507752 ike 0:Azure_0: FNBAM_SUCCESS
2023-11-28 15:52:08.508794 ike 0:Azure_0: Azure AD auth succeeded (msgraphgrp)
2023-11-28 15:52:08.510216 ike 0:Azure_0:31: send AD_AUTH_SUCCESS
2023-11-28 15:52:08.511426 ike 0:Azure_0:15: sending NOTIFY msg
2023-11-28 15:52:08.512857 ike 0:Azure_0:31:15: send informational
2023-11-28 15:52:08.514534 ike 0:Azure_0:31: enc 000000080000F1080706050403020107
2023-11-28 15:52:08.516395 ike 0:Azure_0:31: out
D9AE37737FFAA01FE0E51AE3ED77F2082E2025000000000000000050290000 3413256E2704001DC9F80EBD2A7
35175246557478164D30E355013BC
69A0BDED148E2E2A603EF6D28DD13A932FAF61EC74
2023-11-28 15:52:08.519714 ike 0:Azure_0:31: sent IKE msg (INFORMATIONAL):
172.19.200.113:500->172.19.200.185:500, len=80, vrf=0,
id=d9ae37737ffaa01f/e0e51ae3ed77f208
2023-11-28 15:52:08.522490 ike 0: comes 172.19.200.185:500-
>172.19.200.113:500,ifindex=3,vrf=0....
2023-11-28 15:52:08.524446 ike 0: IKEv2 exchange=INFORMATIONAL_RESPONSE
id=d9ae37737ffaa01f/e0e51ae3ed77f208 len=80
2023-11-28 15:52:08.526370 ike 0: in
D9AE37737FFAA01FE0E51AE3ED77F2082E2025280000000000000050000000034925EA6E305C033FBF32AEB540
3FF3390A6AA68943E6E95FFD42F9A9DB5F2211EA2
E5030A8DCDCC68A0D952C49B7C104C
2023-11-28 15:52:08.529516 ike 0:Azure_0:31: dec
D9AE37737FFAA01FE0E51AE3ED77F2082E2025280000000000000002000000004
2023-11-28 15:52:08.531826 ike 0:Azure_0:31: received informational response
2023-11-28 15:52:08.533168 ike 0:Azure_0:15: received NOTIFY acknowledgement
2023-11-28 15:52:08.534569 ike 0:Azure_0:31:15: processing informational acknowledgement
2023-11-28 15:52:09.446751 ike 0: comes 172.19.200.185:500-
>172.19.200.113:500,ifindex=3,vrf=0....
2023-11-28 15:52:09.448432 ike 0: IKEv2 exchange=CREATE_CHILD
id=d9ae37737ffaa01f/e0e51ae3ed77f208:00000003 len=448
2023-11-28 15:52:09.450319 ike 0: in
D9AE37737FFAA01FE0E51AE3ED77F2082E2024080000000 3000001C0210001A4D1C2C49AECAEBA124A5DE2DF9
44A81ECC42E35F47089131AAAA1D089F60E74845C
```

```
A77B0F46616B3946EC1DB6386B95B3E4AAD48624AD098716B7C09377070A34A4A8FA29C5205A53FB705FB95FB
1196320A24E54F123C45E7EAA07DA2F7E5C73D5D68FCC29711163372CC0601061A1629C10D4B4D

29240FEB22BF758E73A0BF47D3EF2311B547683FBED69DE40960A30FDCACEFA83C5B002C117EF1849D9EFCBF5
D5C594424160C6DDAE59D72CA0FE69109D677B36A3E52251B12E609EBC39105228F03821F52DCC

A8F48FFCD2B1E467EFD6D22C944A2FE1668F52111B863790EAB4B70AC111BBBEA1BD4E400920E6002F541DBBF
A5B1270DB7F9A8E17DB837A55A161A848FBD3CEE545C59673114BC6C7192CB8FC3A22226647769

A47C5EC14F9A927A2DC22D3AEC869F7D22728EA36AE72C79BCAEC678F832D868F4AF4A9F11316AB525EE29E83
D7FE4B36B4C907FD695FC958F391CC53A55BA3D70768458374E0DEB496B4EE2C764259816EB4A5

1C500F83A98A8E134A7E5287057AC06D0DFB99A6403EB711B5ED4A0AD431D342BDF4E9674B614C0EA63AD879B
E72F0F6FB
2023-11-28 15:52:09.463679 ike 0:Azure_0:31: dec
D9AE37737FFAA01FE0E51AE3ED77F2082E2024080000000300000190210000042800006402000030010304 04B
6309E870300000C0100000C800E00

800300000803000002030000080400000500000008050000000000003002030404B6309E870300000C0100000
C800E0100030000080300000C0300000804000005000000080500000022000014B152C3DB9D7C4

DCB76B245B1B1E537752C0000C80005000013FC512EBBD59D5EE5926D399D13FE2811F9D965F6489E6727340F
15F2588D0B37347D70C4DB2A056AEDE07A0B83D0BC6C124CFBEFD8B8EC28E3BE927E3ADDCB5855

6010430E13A03A123A11C1A1F5F603093844ED7CA9CA65C97BF77689456F933584C0D706024321EB1BA2DEAB6
C7CDBF9D8C6B3CAEF02B8D98F10B8EF0B7F975EB3F922360B21B419E71D91DC8A86BF7361500BE

FD67B0AB19F0F89423D8E9229B2A71FD283FEAC4845F4DB2092A48ECECCD84C12CA552C234A2B6614FAF02D00
0018010000000700001000 00FFFF00000000FFFFFFFF0000001801000000070000100000FFFF00
000000FFFFFFFF
2023-11-28 15:52:09.476082 ike 0:Azure_0:31: received create-child request
2023-11-28 15:52:09.477573 ike 0:Azure_0:31: responder received CREATE_CHILD exchange
2023-11-28 15:52:09.479026 ike 0:Azure_0:31: responder creating new child
2023-11-28 15:52:09.480311 ike 0:Azure_0:31:16: peer proposal:
2023-11-28 15:52:09.481643 ike 0:Azure_0:31:16: TSi_0 0:0.0.0.0-255.255.255.255:0
2023-11-28 15:52:09.483041 ike 0:Azure_0:31:16: TSr_0 0:0.0.0.0-255.255.255.255:0
2023-11-28 15:52:09.484917 ike 0:Azure_0:31:Azure:16: comparing selectors
2023-11-28 15:52:09.486431 ike 0:Azure_0:31:Azure:16: matched by rfc-rule-2
2023-11-28 15:52:09.488240 ike 0:Azure_0:31:Azure:16: phase2 matched by subset
2023-11-28 15:52:09.489819 ike 0:Azure_0:31:Azure:16: using mode-cfg override
0:192.168.1.1-192.168.1.1:0
2023-11-28 15:52:09.493018 ike 0:Azure_0:31:Azure:16: accepted proposal:
2023-11-28 15:52:09.494773 ike 0:Azure_0:31:Azure:16: TSi_0 0:192.168.1.1-192.168.1.1:0
2023-11-28 15:52:09.496728 ike 0:Azure_0:31:Azure:16: TSr_0 0:0.0.0.0-255.255.255.255:0
2023-11-28 15:52:09.498785 ike 0:Azure_0:31:Azure:16: dialup
2023-11-28 15:52:09.500228 ike 0:Azure_0:31:Azure:16: incoming child SA proposal:
2023-11-28 15:52:09.502191 ike 0:Azure_0:31:Azure:16: proposal id = 1:
2023-11-28 15:52:09.504280 ike 0:Azure_0:31:Azure:16:   protocol = ESP:
```

```
2023-11-28 15:52:09.506390 ike 0:Azure_0:31:Azure:16:      encapsulation = TUNNEL
2023-11-28 15:52:09.508479 ike 0:Azure_0:31:Azure:16:         type=ENCR, val=AES_CBC
(key_len = 128)
2023-11-28 15:52:09.510929 ike 0:Azure_0:31:Azure:16:         type=INTEGR, val=SHA
2023-11-28 15:52:09.513041 ike 0:Azure_0:31:Azure:16:         type=DH_GROUP, val=MODP1536
2023-11-28 15:52:09.514921 ike 0:Azure_0:31:Azure:16:         type=ESN, val=NO
2023-11-28 15:52:09.517047 ike 0:Azure_0:31:Azure:16: matched proposal id 1
2023-11-28 15:52:09.518363 ike 0:Azure_0:31:Azure:16: proposal id = 1:
2023-11-28 15:52:09.519673 ike 0:Azure_0:31:Azure:16:   protocol = ESP:
2023-11-28 15:52:09.521199 ike 0:Azure_0:31:Azure:16:      encapsulation = TUNNEL
2023-11-28 15:52:09.522991 ike 0:Azure_0:31:Azure:16:         type=ENCR, val=AES_CBC
(key_len = 128)
2023-11-28 15:52:09.524846 ike 0:Azure_0:31:Azure:16:         type=INTEGR, val=SHA
2023-11-28 15:52:09.526296 ike 0:Azure_0:31:Azure:16:         type=DH_GROUP, val=MODP1536
2023-11-28 15:52:09.527909 ike 0:Azure_0:31:Azure:16:         type=ESN, val=NO
2023-11-28 15:52:09.529345 ike 0:Azure_0:31:Azure:16: lifetime=43200
2023-11-28 15:52:09.531065 ike 0:Azure_0:31:Azure:16: PFS enabled, group=5
2023-11-28 15:52:09.532636 ike 0:Azure_0:31:Azure:16: generate DH public value request
queued
2023-11-28 15:52:09.535270 ike 0:Azure_0:31:Azure:16: compute DH shared secret request
queued
2023-11-28 15:52:09.538204 ike 0:Azure_0:31:Azure:16: replay protection enabled
2023-11-28 15:52:09.540564 ike 0:Azure_0:31:Azure:16: set sa life soft seconds=43185.
2023-11-28 15:52:09.543517 ike 0:Azure_0:31:Azure:16: set sa life hard seconds=43200.
2023-11-28 15:52:09.545940 ike 0:Azure_0:31:Azure:16: IPsec SA selectors #src=1 #dst=1
2023-11-28 15:52:09.548329 ike 0:Azure_0:31:Azure:16: src 0 7 0:0.0.0.0-255.255.255.255:0
2023-11-28 15:52:09.549967 ike 0:Azure_0:31:Azure:16: dst 0 7 0:192.168.1.1-192.168.1.1:0
2023-11-28 15:52:09.551724 ike 0:Azure_0:31:Azure:16: add dynamic IPsec SA selectors
2023-11-28 15:52:09.553656 ike 0:Azure_0:31:Azure:16: added dynamic IPsec SA proxyids,
new serial 1
2023-11-28 15:52:09.555661 ike 0:Azure:16: add route 192.168.1.1/255.255.255.255 gw
192.168.1.1 oif Azure(17) metric 15 priority 1
2023-11-28 15:52:09.558385 ike 0:Azure_0:31:Azure:16: tunnel 1 of VDOM limit 0/0
2023-11-28 15:52:09.559849 ike 0:Azure_0:31:Azure:16: add IPsec SA:
SPIs=089ed054/b6309e87
2023-11-28 15:52:09.559855 ike 0:Azure_0:31:Azure:16: IPsec SA dec spi 089ed054 key
16:7266651ABA6DF54EA23C5F16ACA4323A auth 20:E5DE2B49D803AD657613D5E7A217019449E172E
D
2023-11-28 15:52:09.559859 ike 0:Azure_0:31:Azure:16: IPsec SA enc spi b6309e87 key
16:E5FC462D5B45E3D2D2CDBE80354F766A auth 20:B4FD4EC142626C58359AAC6278370986E4B9C4F
8
2023-11-28 15:52:09.559883 ike 0:Azure_0:31:Azure:16: added IPsec SA:
SPIs=089ed054/b6309e87
2023-11-28 15:52:09.560126 ike 0:Azure_0: tunnel up event assigned address 192.168.1.1
2023-11-28 15:52:09.560352 ike 0:Azure_0:31:Azure:16: sending SNMP tunnel UP trap
2023-11-28 15:52:09.560772 ike 0:Azure_0: sent tunnel-up message to EMS: (fct-
uid=CFC62AA23F344235B5D8A61855E7FF6D, intf=Azure_0, addr=192.168.1.1, vdom=root)
2023-11-28 15:52:09.561092 ike 0:Azure_0:31:Azure:16: responder preparing CREATE_CHILD
```

```
message
2023-11-28 15:52:09.561320 ike 0:Azure_0:31: enc
2800003400000030010304040 89ED0540300000C0100000C800E008003000008030000020300000804000005000000080500000022000014806 26D

7A23F5008349B6CC4289825B292C0000C800050000C26CB6DC83F23198EFB6B595A44AD7A2D4506D048F7E3BA27ED14CB47FF12B2C20ED2F7C59022E698A8EEB22AC1269DE785F4E4D674261E2268E6D5219EA8

DBCD598D59CE007D831420E3654A93ED0733AA1AC51B2908611CA39D64B17ABA6E3EFC338A700480CC5CB65549BDA2B527FDAC9B68A4CAFBFE90ACEE70333451F31BA79FFA53B7028879E38682E2A2E74E692D6

03B41ACA394E5EAEBEDAD923ADF8DF6E5B60C19A17860A9F72079F2A9B162244DA2ED48931DA94505F8A9784C6AE2D0000180100000007000010000 0FFFFC0A80101C0A80101000000180100000007000010000 0FFFF00000000FFFFFFFF0F0E0D0C0B0A0908070605040302010F
2023-11-28 15:52:09.561585 ike 0:Azure_0:31: out
D9AE37737FFAA01FE0E51AE3ED77F2082E2024200000000300000190210001747521BEB5752BC8166B870187B8184577A936B1617899657B3F61B0

ACE844FACE72E945DEC6A91FC5AB1001D8120A73ED5732605FE6D0DD57CDDFD2EB624A38490841A638172E86FAD3C27C255DF6508AE96D3C127C2FF9B479FD8007EE12B1E59227220F4A817A0BF29D9695C420F

5C0B9F5D74F910345D843AD638946098D38C7F2C5C19FD854F2BE128DD336328DBF1072308F4AAFD103AEE529495D8D7A48233F6565104F277EFC9E8371A81A6B9EB59CA9AF66AD93332F3F767585522A750AD9

1B124CD84C903BE6A64B3D63BA3E6D212E73C744D59DED2AE2580A12EB0550AD140F7CDB7587A5312910586972D01A39110DBF639CDF077B9B66799AA1C0F2A39C0106887F1D7E43B135B170A478A9DBF01B187

C20E21A04A953B0BDC4E71A00BCED1C0B2F95C5188F701EB0372CFF5FD0DD347BD7765540E45AB0E6419EC8EB139099561E1A95F7C5056AB3B18E023338A23B26C32421BD7D5CB1C1308CA9EBAE191A87E5025683811AB0C5E644
2023-11-28 15:52:09.561966 ike 0:Azure_0:31: sent IKE msg (CREATE_CHILD_RESPONSE):
172.19.200.113:500->172.19.200.185:500, len=400, vrf=0, id=d9ae37737ffaa01f/e0e51ae3ed77f208:00000003
2023-11-28 15:52:13.239889 ike 0: comes 172.19.200.185:500-
>172.19.200.113:500,ifindex=3,vrf=0....
2023-11-28 15:52:13.239970 ike 0: IKEv2 exchange=INFORMATIONAL
id=d9ae37737ffaa01f/e0e51ae3ed77f208:00000004 len=80
2023-11-28 15:52:13.239976 ike 0: in
D9AE37737FFAA01FE0E51AE3ED77F2082E2025080000000400000050000000034BFA2DC51F014978F5F695462630406B37D7311206880F4BA747BA1E786092E7F6F34C63B6D3B48A8E6531AABAA72FE55
2023-11-28 15:52:13.240004 ike 0:Azure_0:31: dec
D9AE37737FFAA01FE0E51AE3ED77F2082E2025080000000400000020000000004
2023-11-28 15:52:13.240222 ike 0:Azure_0:31: received informational request
2023-11-28 15:52:13.240230 ike 0:Azure_0:31: enc 0F0E0D0C0B0A0908070605040302010F
2023-11-28 15:52:13.240443 ike 0:Azure_0:31: out
D9AE37737FFAA01FE0E51AE3ED77F2082E2025200000000400000050000000349815B795B19825052A1CEB3BFBDF0890035F90BFBAB8D3DC8B2D24
```

```
3C0F347C253853573C4692A2FAB41271E0935FD0BE
2023-11-28 15:52:13.240670 ike 0:Azure_0:31: sent IKE msg (INFORMATIONAL_RESPONSE):
172.19.200.113:500->172.19.200.185:500, len=80, vrf=0, id=d9ae37737ffaa01f/e0e51ae3
ed77f208:00000004
2023-11-28 15:52:17.875738 ike shrank heap by 344064 bytes
```

IPsec VPN SAML-based authentication

FortiClient IPsec VPN IKEv2 supports SAML authentication with identity providers (IdP) such as Microsoft Entra ID, Okta, and FortiAuthenticator. This configuration also supports pushing authentication tokens. This provides a similar experience as using SAML-based authentication for SSL VPN.

The following instructions assume that you have already configured your Entra ID environment, that your EMS and FortiGate are part of a Fortinet Security Fabric, and that the FortiGate has been configured in Azure as an enterprise application for SAML single sign on (SSO).

You must enable XAuth for an IPsec VPN IKEv2 tunnel with SAML authentication. Note that when XAuth is enabled, user authentication is handled using EAP.

The following provide configuration examples for Entra ID, Okta, and FortiAuthenticator:

- Use case 1: SAML authentication with Entra ID as IdP on page 213
- Use case 2: SAML authentication with Okta as IdP on page 218
- Use case 3: SAML authentication with FortiAuthenticator as IdP on page 221

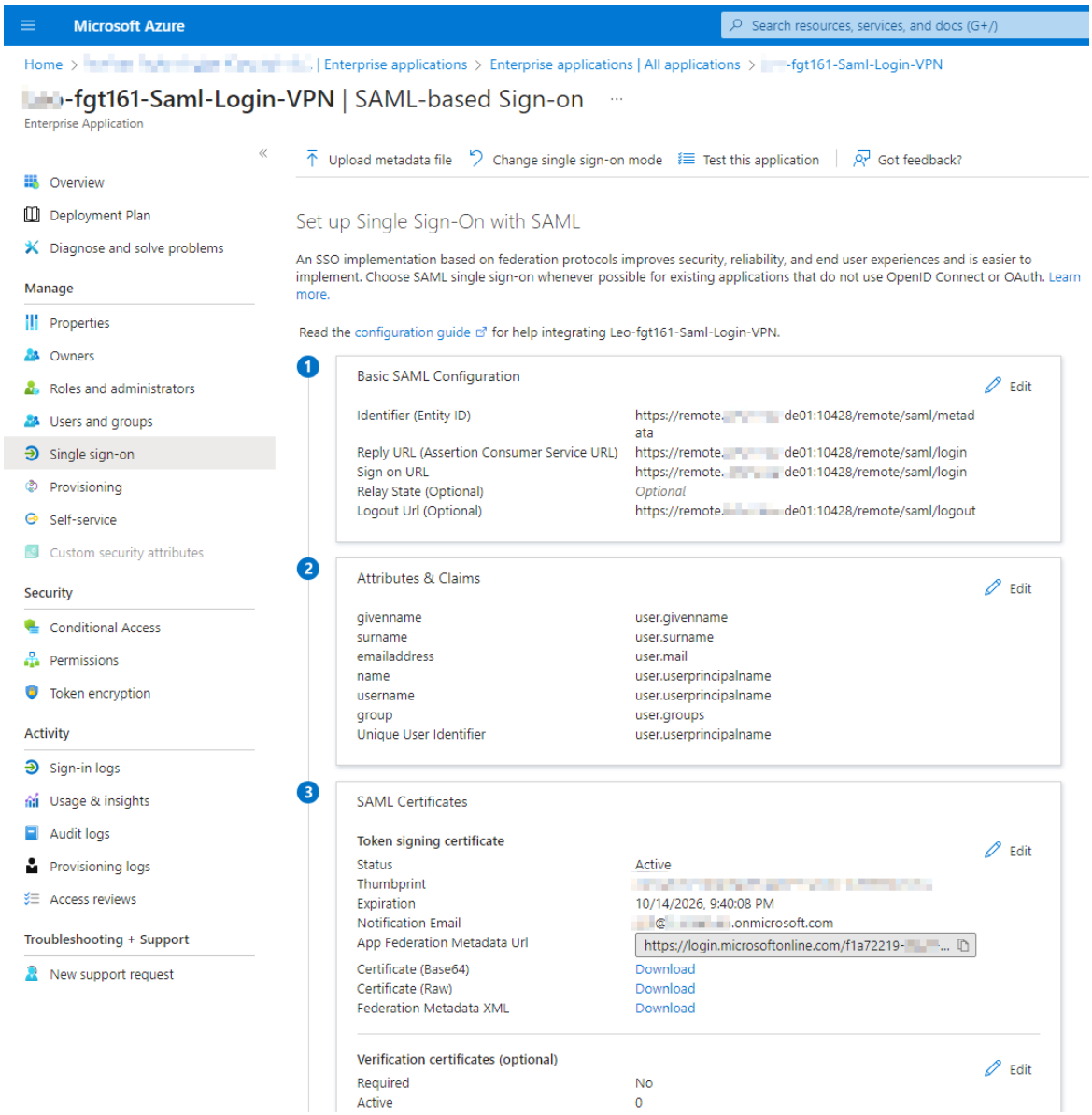
The examples use the following product versions:

Product	Version
FortiClient	7.2.4
FortiClient EMS	
FortiGate	7.4.3
FortiAuthenticator	6.5.3

Use case 1: SAML authentication with Entra ID as IdP

To configure SAML authentication with Entra ID as IdP:

1. The following shows an example enterprise application for SAML SSO in Azure. Key to this configuration is that the endpoint can resolve the FortiGate fully qualified domain name (FQDN) (in this example, it is remote...de01). Note the port number, which in this example is 10428. Under *SAML Certificates*, beside *Certificate (Base64)*, click *Download*.



2. Configure FortiOS:
   a. Import the certificate that you downloaded from the Azure portal to FortiOS by going to *System > Certificates > Create/Import > Remote Certificate* and selecting the desired certificate.
   b. Define a user IKE SAML authentication port:
   ```
   config system global
      set auth-ike-saml-port 10428
   end
   ```
   c. Configure SAML user settings. In this example, remote...de01 is the remote gateway. Port 10428 is the IKE SAML authentication port that you defined earlier:
      i. Configure a SAML user:
      ```
      config user saml
         edit "IPSec-SAML-FAC"
            set cert "Fortinet_Factory"
            set entity-id "https://remote...de01:10428/remote/saml/metadata"
            set single-sign-on-url "https://remote...de01:10428/remote/saml/login"
      ```

```
        set single-logout-url "https://remote...de01:10428/remote/saml/logout"
        set idp-entity-id "https://sts.windows.net/f1a72219-.../"
        set idp-single-sign-on-url "https://login.microsoftonline.com/f1a72219-.../saml2"
        set idp-single-logout-url "https://login.microsoftonline.com/f1a72219-.../saml2"
        set idp-cert "REMOTE_Cert_2"
        set user-name "username"
        set group-name "saml-group"
        set digest-method sha1
    next
end
```

ii. Configure a user group. The example user group is ipsec-saml-group, which includes the SAML user that you configured. You use this group in a FortiOS firewall policy to control access permission to protected resources:

```
config user group
    edit "ipsec-saml-group"
        set member "IPSec-SAML-FAC"
    next
end
```

d. Configure the IKE SAML server for the FortiOS interface used for VPN connection. This example uses port1 as the WAN interface, which the configuration uses for IPsec VPN IKEv2 connection:

```
config system interface
    edit "port1"
        set ike-saml-server IPSec-SAML-FAC
    next
end
```

e. Configure the IPsec VPN IKEv2 tunnel:

i. Configure an IP address range for the IPsec VPN tunnel to use. In this example, there is a file server with IP address 192.168.235.180 sitting on the FortiOS LAN network 192.168.235.0/24. Substitute your own values as needed.

```
config firewall address
    edit "IPSec_Tunnel_Addr1"
        set type iprange
        set start-ip 192.168.1.100
        set end-ip 192.168.1.108
    next
end
config firewall address
    edit "LAN2-192.168.235.0"
        set subnet 192.168.235.0 255.255.255.0
    next
end
```

ii. Create an IPsec VPN IKEv2 tunnel. This example uses a preshared key as the authentication method. Ensure that you `set eap enable` and `eap-identity send-request` correctly:

```
config vpn ipsec phase1-interface
    edit "v4-PSK-IKEv2"
        set type dynamic
        set interface "port1"
        set ike-version 2
        set peertype any
        set net-device disable
        set mode-cfg enable
        set ipv4-dns-server1 172.17.60.6
        set ipv4-dns-server2 8.8.8.8
        set proposal aes128-sha1 aes256-sha256
```

```
      set dpd on-idle
      set dhgrp 5
      set eap enable
      set eap-identity send-request
      set assign-ip-from name
      set ipv4-split-include "LAN2-192.168.235.0"
      set ipv4-name "IPSec_Tunnel_Addr1"
      set save-password enable
      set client-auto-negotiate enable
      set client-keep-alive enable
      set psksecret 11111111
      set dpd-retryinterval 60
   next
end
config vpn ipsec phase2-interface
   edit "v4-PSK-IKEv2"
      set phase1name "v4-PSK-IKEv2"
      set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256
      set dhgrp 5
   next
end
```

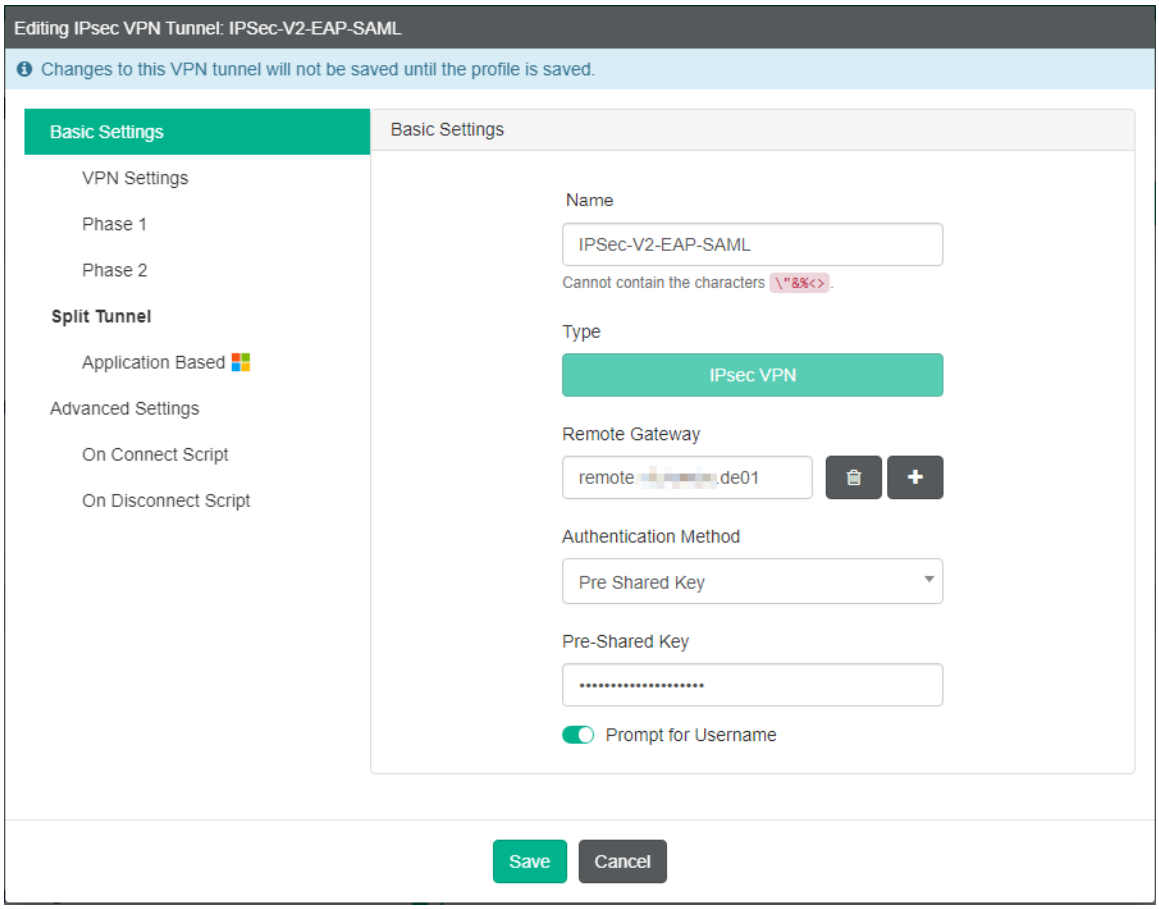
iii. Add the SAML group to the firewall policy for the VPN tunnel. In this example, ipsec-saml-group is the SAML group name, and port3 is the FortiGate LAN interface. Modify the commands to fit your environment:

```
config firewall address
   edit "LAN2_port3 address"
      set type interface-subnet
      set subnet 192.168.235.0 255.255.255.0
      set interface "port3"
   next
end
config firewall policy
   edit 117
      set name "v4-PSK-IKEv2 -> LAN"
      set srcintf "v4-PSK-IKEv2"
      set dstintf "port3"
      set action accept
      set srcaddr "IPSec_Tunnel_Addr1"
      set dstaddr "LAN2_port3 address"
      set schedule "always"
      set service "ALL"
      set nat enable
      set groups "ipsec-saml-group"
   next
end
```

iv. (Optional) FortiClient validates the certificate configured in FortiOS. To prevent an invalid server certificate prompt, the certificate common name (CN) should match the VPN remote gateway FQDN (remote...de01 in this example) and you should import the certificate authority (CA) as a trusted root CA authority. FortiClient also verifies certificates for IdPs such as FortiAuthenciator, Azure, and Okta.

```
config user setting
   set auth-cert "remote...de01-oldca"
end
```

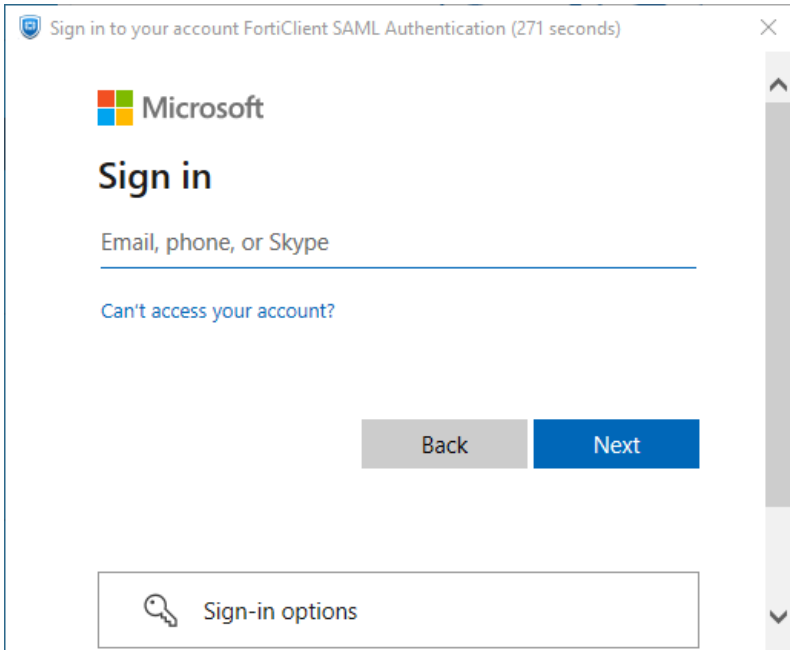
3. Configure a new IPsec VPN IKEv2 tunnel in EMS:
   a. In EMS, go to *Endpoint Profiles* > *Remote Access*.
   b. Create a new profile or edit an existing one.
   c. Under *VPN Tunnels*, click *Add Tunnel*.
   d. Select *Manual*.
   e. Configure *Basic Settings*:
      i. In the *Name* field, configure the desired tunnel name.
      ii. For *Type*, select *IPsec VPN*.
      iii. In the *Remote Gateway* field, enter the remote gateway. In this example it is remote...de01.
      iv. From the *Authentication Method* dropdown list, select *Pre Shared Key*.
      v. In the *Pre-Shared Key* field, enter the same key that you configured in step 2.e.ii.



   f. Configure *Advanced Settings*:
      i. Disable *Prompt for Certificate*.
      ii. Toggle on *Enable SAML Login*.
      iii. In the *SAML Port* field, enter the port that you noted from the Azure portal. In this example, it is 10428.
      iv. Enable *Show "Remember Password" Option*.
      v. Enable *Show "Always Up" Option*.
      vi. Enable *Show "Auto Connect" Option*.

g. Leave other fields at their default values, and save. For the XML configuration for the tunnel, see IPsec VPN tunnel XML configuration on page 221.

4. After FortiClient receives the configuration changes from EMS, connect to the tunnel:
   a. In FortiClient, go to the *Remote Access* tab.
   b. From the *VPN Name* dropdown list, select the IPsec VPN tunnel.
   c. Click *Connect*.
   d. An authentication dialog appears. Enter the Entra ID credentials to establish the VPN connection.



5. After the VPN tunnel is up, attempt access to a resource that a FortiOS firewall policy protects. The following shows `diagnose firewall auth list` output for such access:

```
192.168.1.100, user@example.onmicrosoft.com
        type: fw, id: 0, duration: 74, idled: 74
        server: IPSec-SAML-FAC
        packets: in 0 out 0, bytes: in 0 out 0
        group_id: 6
        group_name: ipsec-saml-group

----- 1 listed, 0 filtered ------
```

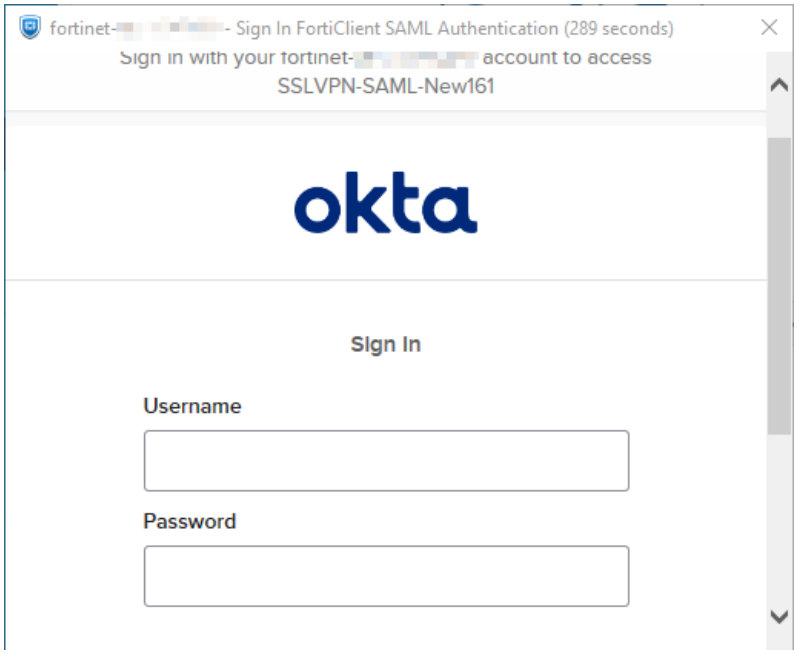
To view IKE debug log output for this access, see IKE debug log reference on page 227.

Use case 2: SAML authentication with Okta as IdP

Configuring IPsec VPN SAML authentication using Okta as the IdP is similar to Use case 1: SAML authentication with Entra ID as IdP on page 213. The following shows an example configuring the SAML user for Okta (step 2.c.i):

```
config user saml
   edit "IPSec-SAML-FAC"
      set cert "Fortinet_Factory"
      set entity-id "https://remote...de01:10428/remote/saml/metadata/"
      set single-sign-on-url "https://remote...de01:10428/remote/saml/login/"
```

```
      set single-logout-url "https://remote...de01:10428/remote/saml/logout/"
      set idp-entity-id "http://www.okta.com/exk5v..."
      set idp-single-sign-on-url "https://dev-....okta.com/app/dev-..._samlloginfgt39_
           1/exk5v.../sso/saml"
      set idp-single-logout-url "https://dev-....okta.com/app/dev-..._samlloginfgt39_
           1/exk5v.../slo/saml"
      set idp-cert "REMOTE_Cert_4"
      set user-name "username"
      set group-name "saml-group"
      set digest-method sha1
   next
end
```



To verify the configuration:

1. After the VPN tunnel is up, attempt access to a resource that a FortiOS firewall policy protects. Run `get ipsec vpn tunnel details` in the FortiOS CLI. Following is the expected output:

```
gateway
name: 'v4-PSK-IKEv2_0'
local-gateway: 10.152.35.161:0 (static)
remote-gateway: 10.152.35.170:0 (dynamic)
dpd-link: on
mode: ike-v2
interface: 'port1' (3) vrf:0
rx packets: 18 bytes: 2259 errors: 13
tx packets: 0 bytes: 0 errors: 0
dpd: on-idle/negotiated idle: 60000ms retry: 3 count: 0
selectors
name: 'v4-PSK-IKEv2'
auto-negotiate: disable
```

```
mode: tunnel
src: 0:0.0.0.0-255.255.255.255:0
dst: 0:192.168.1.100-192.168.1.100:0
SA
lifetime/rekey: 43200/43101
mtu: 1438
tx-esp-seq: 1
replay: enabled
qat: 0
inbound
spi: 758626b4
enc: aes-cb 37491f896e23475bcbc98cb98fe6511c
auth: sha1 01cfde3affa4edcca94626c9fcc474fe55113e36
outbound
spi: 80b1a046
enc: aes-cb 88c755eec85f512ca31ce65b687932bb
auth: sha1 d2953b6376c145b82e88a05983dfec180e33dbc4
NPU acceleration: none
```

2. Run `diagnose sniffer packet <gateway name>` to view the packet sniffer information. Following is the expected output:

```
Using Original Sniffing Mode
interfaces=[v4-PSK-IKEv2]
filters=[none]
pcap_lookupnet: v4-PSK-IKEv2: no IPv4 address assigned
8.902304 192.168.1.100 -> 192.168.235.180: icmp: echo request
8.902770 192.168.235.180 -> 192.168.1.100: icmp: echo reply
9.910247 192.168.1.100 -> 192.168.235.180: icmp: echo request
9.910518 192.168.235.180 -> 192.168.1.100: icmp: echo reply
10.925738 192.168.1.100 -> 192.168.235.180: icmp: echo request
10.926070 192.168.235.180 -> 192.168.1.100: icmp: echo reply
11.941364 192.168.1.100 -> 192.168.235.180: icmp: echo request
11.942012 192.168.235.180 -> 192.168.1.100: icmp: echo reply
49.060511 192.168.1.100 -> 192.168.235.180: icmp: echo request
49.061039 192.168.235.180 -> 192.168.1.100: icmp: echo reply
50.066813 192.168.1.100 -> 192.168.235.180: icmp: echo request
50.067084 192.168.235.180 -> 192.168.1.100: icmp: echo reply
51.082305 192.168.1.100 -> 192.168.235.180: icmp: echo request
51.082633 192.168.235.180 -> 192.168.1.100: icmp: echo reply
52.097539 192.168.1.100 -> 192.168.235.180: icmp: echo request
52.097898 192.168.235.180 -> 192.168.1.100: icmp: echo reply
```

3. Run `diagnose firewall auth list`. Following is the expected output:

```
192.168.1.100, example@fortinet.com
type: fw, id: 0, duration: 664, idled: 458
server: IPSec-SAML-FAC
packets: in 8 out 8, bytes: in 480 out 480
```

```
group_id: 6
group_name: ipsec-saml-group

----- 1 listed, 0 filtered ------
```

Use case 3: SAML authentication with FortiAuthenticator as IdP

Configuring IPsec VPN SAML authentication using FortiAuthenticator as the IdP is similar to Use case 1: SAML authentication with Entra ID as IdP on page 213. The following shows an example configuring the SAML user for FortiAuthenticator (step 2.c.i). Ensure the endpoint can resolve the remote gateway FQDN (in this example remote...de01) and the FortiAuthenticator FQDN (in this example fac.example.fct.local):

```
config user saml
   edit "IPSec-SAML-FAC"
      set cert "Fortinet_Factory"
      set entity-id "https://remote...de01:10428/remote/saml/metadata/"
      set single-sign-on-url "https://remote...de01:10428/remote/saml/login/"
      set single-logout-url "https://remote...de01:10428/remote/saml/logout/"
      set idp-entity-id "http://fac.example.fct.local/saml-idp/lxat.../metadata/"
      set idp-single-sign-on-url "https://fac.example.fct.local/saml-idp/lxat.../login/"
      set idp-single-logout-url "https://fac.example.fct.local/saml-idp/lxat.../logout/"
      set idp-cert "REMOTE_Cert_3"
      set user-name "username"
      set group-name "saml-group"
      set digest-method sha1
   next
end
```

IPsec VPN tunnel XML configuration

The following shows the XML configuration for the IPsec VPN tunnel configured in Use case 1: SAML authentication with Entra ID as IdP on page 213 step 3. Note the <sso_enabled> and <ike_saml_port> elements:

```
<?xml version="1.0" ?>
<forticlient_configuration>
    <vpn>
        <enabled>1</enabled>
        <sslvpn>
            <options>
                <negative_split_tunnel_metric/>
                <dnscache_service_control>0</dnscache_service_control>
                <warn_invalid_server_certificate>1</warn_invalid_server_certificate>
                <no_dns_registration>0</no_dns_registration>
                <use_gui_saml_auth>0</use_gui_saml_auth>
                <preferred_dtls_tunnel>0</preferred_dtls_tunnel>
                <prefer_sslvpn_dns>1</prefer_sslvpn_dns>
                <disallow_invalid_server_certificate>0</disallow_invalid_server_certificate>
                <enabled>1</enabled>
            </options>
            <connections/>
        </sslvpn>
```

```
        <ipsecvpn>
            <options>
                <use_win_local_computer_cert>1</use_win_local_computer_cert>
                <disallow_invalid_server_certificate>1</disallow_invalid_server_certificate>
                <usesmcardcert>1</usesmcardcert>
                <show_auth_cert_only>0</show_auth_cert_only>
                <no_dns_registration>0</no_dns_registration>
                <enable_udp_checksum>0</enable_udp_checksum>
                <beep_if_error>0</beep_if_error>
                <disable_default_route>0</disable_default_route>
                <block_ipv6>1</block_ipv6>
                <check_for_cert_private_key>0</check_for_cert_private_key>
                <enhanced_key_usage_mandatory>0</enhanced_key_usage_mandatory>
                <usewincert>1</usewincert>
                <uselocalcert>0</uselocalcert>
                <use_win_current_user_cert>1</use_win_current_user_cert>
                <enabled>1</enabled>
            </options>
            <connections>
                <connection>
                    <name>IPSec-V2-EAP-SAML</name>
                    <uid>BA387F1D-E421-4753-AAA4-657C4C8202AF</uid>
                    <machine>0</machine>
                    <keep_running>0</keep_running>
                    <disclaimer_msg/>
                    <sso_enabled>1</sso_enabled>
                    <single_user_mode>0</single_user_mode>
                    <type>manual</type>
                    <ui>
                        <show_remember_password>1</show_remember_password>
                        <show_alwaysup>1</show_alwaysup>
                        <show_autoconnect>1</show_autoconnect>
                        <show_passcode>0</show_passcode>
                        <save_username>0</save_username>
                    </ui>
                    <redundant_sort_method>0</redundant_sort_method>
                    <tags>
                        <allowed/>
                        <prohibited/>
                    </tags>
                    <host_check_fail_warning/>
                    <ike_settings>
                        <server>remote...de01</server>
                        <authentication_method>Preshared Key</authentication_method>
                        <fgt>1</fgt>
                        <prompt_certificate>0</prompt_certificate>
                        <xauth>
                            <use_otp>0</use_otp>
                            <enabled>1</enabled>
                            <prompt_username>1</prompt_username>
                        </xauth>
                        <version>2</version>
```

```
                        <mode>aggressive</mode>
                        <key_life>86400</key_life>
                        <localid/>
                        <implied_SPDO>0</implied_SPDO>
                        <implied_SPDO_timeout>0</implied_SPDO_timeout>
                        <nat_traversal>1</nat_traversal>
                        <nat_alive_freq>5</nat_alive_freq>
                        <enable_local_lan>0</enable_local_lan>
                        <enable_ike_fragmentation>0</enable_ike_fragmentation>
                        <mode_config>1</mode_config>
                        <dpd>1</dpd>
                        <run_fcauth_system>0</run_fcauth_system>
                        <sso_enabled>1</sso_enabled>
                        <ike_saml_port>10428</ike_saml_port>
                        <dpd_retry_count>3</dpd_retry_count>
                        <dpd_retry_interval>5</dpd_retry_interval>
                        <auth_data>
                            <preshared_key>Enc
380ffd71e1570436106bf459ff8fc41e43a7279260bec9b01e7dd3bfc3c8dfc0</preshared_key>
                        </auth_data>
                        <xauth_timeout>120</xauth_timeout>
                        <dhgroup>5</dhgroup>
                        <proposals>
                            <proposal>AES128|SHA1</proposal>
                            <proposal>AES256|SHA256</proposal>
                        </proposals>
                    </ike_settings>
                    <ipsec_settings>
                        <remote_networks>
                            <network>
                                <addr>0.0.0.0</addr>
                                <mask>0.0.0.0</mask>
                            </network>
                            <network>
                                <addr>::/0</addr>
                                <mask>::/0</mask>
                            </network>
                        </remote_networks>
                        <dhgroup>5</dhgroup>
                        <key_life_type>seconds</key_life_type>
                        <key_life_seconds>43200</key_life_seconds>
                        <key_life_Kbytes>5200</key_life_Kbytes>
                        <replay_detection>1</replay_detection>
                        <pfs>1</pfs>
                        <use_vip>1</use_vip>
                        <virtualip>
                            <type>modeconfig</type>
                            <ip>0.0.0.0</ip>
                            <mask>0.0.0.0</mask>
                            <dnsserver>0.0.0.0</dnsserver>
                            <winserver>0.0.0.0</winserver>
                        </virtualip>
```

```
                    <proposals>
                        <proposal>AES128|SHA1</proposal>
                        <proposal>AES256|SHA256</proposal>
                    </proposals>
                </ipsec_settings>
                <android_cert_path/>
                <warn_invalid_server_certificate>1</warn_invalid_server_certificate>
                <on_connect>
                    <script>
                        <os>windows</os>
                        <script/>
                    </script>
                    <script>
                        <os>MacOSX</os>
                        <script/>
                    </script>
                    <script>
                        <os>linux</os>
                        <script/>
                    </script>
                </on_connect>
                <on_disconnect>
                    <script>
                        <os>windows</os>
                        <script/>
                    </script>
                    <script>
                        <os>MacOSX</os>
                        <script/>
                    </script>
                    <script>
                        <os>linux</os>
                        <script/>
                    </script>
                </on_disconnect>
                <traffic_control>
                    <enabled>0</enabled>
                    <mode>1</mode>
                </traffic_control>
            </connection>
            <connection>
                <name>IPSec-V2-SAML-LM0</name>
                <uid>186A1714-E2EA-44D1-AC8D-60B21922C48A</uid>
                <machine>0</machine>
                <keep_running>0</keep_running>
                <disclaimer_msg/>
                <sso_enabled>1</sso_enabled>
                <single_user_mode>0</single_user_mode>
                <type>manual</type>
                <ui>
                    <show_remember_password>1</show_remember_password>
                    <show_alwaysup>1</show_alwaysup>
```

```
                        <show_autoconnect>1</show_autoconnect>
                        <show_passcode>0</show_passcode>
                        <save_username>0</save_username>
                    </ui>
                    <redundant_sort_method>0</redundant_sort_method>
                    <tags>
                        <allowed/>
                        <prohibited/>
                    </tags>
                    <host_check_fail_warning/>
                    <ike_settings>
                        <server>remote...de01</server>
                        <authentication_method>System Store X509 Certificate</authentication_
method>
                        <fgt>1</fgt>
                        <prompt_certificate>1</prompt_certificate>
                        <xauth>
                            <use_otp>0</use_otp>
                            <enabled>1</enabled>
                            <prompt_username>1</prompt_username>
                        </xauth>
                        <version>2</version>
                        <mode>aggressive</mode>
                        <key_life>86400</key_life>
                        <localid/>
                        <implied_SPDO>0</implied_SPDO>
                        <implied_SPDO_timeout>0</implied_SPDO_timeout>
                        <nat_traversal>1</nat_traversal>
                        <nat_alive_freq>5</nat_alive_freq>
                        <enable_local_lan>0</enable_local_lan>
                        <enable_ike_fragmentation>0</enable_ike_fragmentation>
                        <mode_config>1</mode_config>
                        <dpd>1</dpd>
                        <run_fcauth_system>0</run_fcauth_system>
                        <sso_enabled>1</sso_enabled>
                        <ike_saml_port>10428</ike_saml_port>
                        <dpd_retry_count>3</dpd_retry_count>
                        <dpd_retry_interval>5</dpd_retry_interval>
                        <xauth_timeout>120</xauth_timeout>
                        <dhgroup>5</dhgroup>
                        <proposals>
                            <proposal>AES128|SHA1</proposal>
                            <proposal>AES256|SHA256</proposal>
                        </proposals>
                        <auth_data/>
                    </ike_settings>
                    <ipsec_settings>
                        <remote_networks>
                            <network>
                                <addr>0.0.0.0</addr>
                                <mask>0.0.0.0</mask>
                            </network>
```

```
                        <network>
                            <addr>::/0</addr>
                            <mask>::/0</mask>
                        </network>
                    </remote_networks>
                    <dhgroup>5</dhgroup>
                    <key_life_type>seconds</key_life_type>
                    <key_life_seconds>43200</key_life_seconds>
                    <key_life_Kbytes>5200</key_life_Kbytes>
                    <replay_detection>1</replay_detection>
                    <pfs>1</pfs>
                    <use_vip>1</use_vip>
                    <virtualip>
                        <type>modeconfig</type>
                        <ip>0.0.0.0</ip>
                        <mask>0.0.0.0</mask>
                        <dnsserver>0.0.0.0</dnsserver>
                        <winserver>0.0.0.0</winserver>
                    </virtualip>
                    <proposals>
                        <proposal>AES128|SHA1</proposal>
                        <proposal>AES256|SHA256</proposal>
                    </proposals>
                </ipsec_settings>
                <android_cert_path/>
                <warn_invalid_server_certificate>1</warn_invalid_server_certificate>
                <on_connect>
                    <script>
                        <os>windows</os>
                        <script/>
                    </script>
                    <script>
                        <os>MacOSX</os>
                        <script/>
                    </script>
                    <script>
                        <os>linux</os>
                        <script/>
                    </script>
                </on_connect>
                <on_disconnect>
                    <script>
                        <os>windows</os>
                        <script/>
                    </script>
                    <script>
                        <os>MacOSX</os>
                        <script/>
                    </script>
                    <script>
                        <os>linux</os>
                        <script/>
```

```
                    </script>
                </on_disconnect>
                <traffic_control>
                    <enabled>0</enabled>
                    <mode>1</mode>
                </traffic_control>
            </connection>
        </connections>
    </ipsecvpn>
    <lockdown>
        <exceptions>
            <ips/>
            <apps/>
        </exceptions>
        <max_attempts>3</max_attempts>
        <grace_period>120</grace_period>
        <enabled>0</enabled>
    </lockdown>
    <options>
        <show_vpn_before_logon>1</show_vpn_before_logon>
        <keep_running_max_tries>0</keep_running_max_tries>
        <on_os_start_connect_has_priority>0</on_os_start_connect_has_priority>
        <autoconnect_only_when_offnet>0</autoconnect_only_when_offnet>
        <secure_remote_access>1</secure_remote_access>
        <minimize_window_on_connect>1</minimize_window_on_connect>
        <show_negotiation_wnd>0</show_negotiation_wnd>
        <allow_personal_vpns>1</allow_personal_vpns>
        <on_os_start_connect/>
        <autoconnect_on_install>0</autoconnect_on_install>
        <suppress_vpn_notification>1</suppress_vpn_notification>
        <disable_connect_disconnect>0</disable_connect_disconnect>
        <use_windows_credentials>0</use_windows_credentials>
        <use_legacy_vpn_before_logon>0</use_legacy_vpn_before_logon>
    </options>
</vpn>
<endpoint_control>
    <ui>
        <display_vpn>1</display_vpn>
    </ui>
</endpoint_control>
</forticlient_configuration>
```

IKE debug log reference

Following is a FortiOS IKE debug log as reference:

```
VPN-ZTNA-FGT1 # diagnose debug reset

VPN-ZTNA-FGT1 # diagnose debug application ike -1
Debug messages will be on for 30 minutes.
```

```
VPN-ZTNA-FGT1 # diagnose debug application samld -1

VPN-ZTNA-FGT1 # diagnose debug enable

VPN-ZTNA-FGT1 # ike :config update start
ike :ike_embryonic_conn_limit = 10000
ike :ikecrypt DH multi-process enabled
ike V=root:0: sync=no FGCP:disabled role:master, FGSP:disabled id:0 slave-add-routes:disabled
ike V=root:0:V4-PSK: local-addr 10.152.35.161
ike V=root:0:V4-PSK: oif 3, vrf 0
ike V=root:0:v4-Cert: local-addr 10.152.35.161
ike V=root:0:v4-Cert: oif 3, vrf 0
ike V=root:0:v4-PSK-IKEv2: local-addr 10.152.35.161
ike V=root:0:v4-PSK-IKEv2: oif 3, vrf 0
ike V=root:0:port3: add addr 192.168.235.0-192.168.235.255
ike V=root:0:ipsec-saml-group:6: update auth group
ike config clean start 10
ike config clean done 10
ike :config update done
samld_process_request [145]: len=453, cmd=0, pid=2293, job_id=563454
samld_process_request [162]: Received 453, 0x1272e30
__samld_sp_create_auth_req [433]: SAML SP algo: 0 -> lasso=1. Binding Method:
urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST

__samld_sp_create_auth_req [453]:
**** AuthnRequest URL ****

https://login.microsoftonline.com/f1a72219-.../saml2?SAMLRequest=lZJBb9swDIX%2FiqG7bcl2EkdIAt
jxigXoNqNJd9hlkGW6FSBLmSh327%2Bf4nRrd1iBHUW%2B

R%2FF74AbFqM%2B8mvyjuYNvE6CPfozaIJ8bWzI5w61AhdyIEZB7yY%2FVh1ueJZSfnfVWWk1eWd52CERwXllDokOzJV9
ZUZdlnjf7Zbmu6HpRsTqvbqqGvqsXjNYFiT6Dw6DfkmAPJsQJDga9MD6UaFbENI%2Fp8kR

zvljxrPxCoiYwKCP87Hr0%2Fow8TbV9UCYZlXQW7eCt0cpAIu2YDkyssoyt464TeVwMS4jXeVfGEvIuL1i3kkORXsgyEt
1YJ2HOaksGoREuG7UBSj3Bn0r7nEqtTK%2FMw9uBdFcR8venUxu3n44nElW%2FQ9pbg9MI

7gjuSUm4v7t9AXIwWh8IlHfKoNXCJT1QxhktsvK5O699RSe7zeXB5wDd7v%2BnjOBFL7zYpK%2FnbK7n8zFwHZrWaiV%2
FXkIahf83NkvYXFF9PMxSPhk8g1SDgj7Qa22%2F7x0IHyL1bgKS7q6f%2Fn2mu18%3D&Re
layState=magic%3D060806859681f2ed&SigAlg=http%3A%2F%2Fwww.w3.org%2F2000%2F09%2Fxmldsig%23rsa-
sha1&Signature=RkHlyfm3PThl8ei43dJ%2BERS%2B42ngKeo%2FQGxdcbl7pfcuipF%2

B0tt%2FctYzOQYMXmai3zBrmOWL%2FT6UHdySEPB3xy1puf%2BxwPfBYh%2BWnR6S6OQKwkYpsBwUsXWbgrENrQxRFv1R
Rxm9TFiORyyWJCSCf94THDC0Uu%2BNmG2lyfoDXnmWUfy3hpBdMAKAQL3DJs2l2cKotLmS

pPRvK9%2BG%2BYxDcUwDDXyfTzIW7pvo57qmO3L9DRDF1woftJ4Psn4p44LTxvV7bcW4WdhSfji7Z%2F%2FyXzcg7TGnF
C1pAw%2FsSXfzp%2FdHSym3TT%2FMIWtpa8JuKrmRWhBMzCP5IIUVxNQr5WiaIA%3D%3D
**********
__samld_sp_create_auth_req [467]:
```

```
**** AuthnRequest ****
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="_14B8833DC689A095A1B3AFAD0EB510B4" Ve
rsion="2.0" IssueInstant="2024-03-06T03:57:28Z"
Destination="https://login.microsoftonline.com/f1a72219-.../saml2" SignType="0" SignMethod=
"0" ForceAuthn="false" IsPassive="false"
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
AssertionConsumerServiceURL="https://remote...d

e01:10428/remote/saml/login"><saml:Issuer>https://remote...de01:10428/remote/saml/metadata</s
aml:Issuer><samlp:NameIDPolicy Format="urn:oasis:names:tc:SA
ML:1.1:nameid-format:unspecified" AllowCreate="true"/></samlp:AuthnRequest>
**********
__samld_sp_create_auth_req [472]:
**** SP Login Dump ****
<lasso:Login xmlns:lasso="http://www.entrouvert.org/namespaces/lasso/0.0"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:saml="urn:oasis:names:tc:SAML:2.
0:assertion" LoginDumpVersion="2"><lasso:Request><samlp:AuthnRequest ID="_
14B8833DC689A095A1B3AFAD0EB510B4" Version="2.0" IssueInstant="2024-03-06T03:57:28Z" Desti
nation="https://login.microsoftonline.com/f1a72219-.../saml2" SignType="0" SignMethod="0"
ForceAuthn="false" IsPassive="false" ProtocolBind
ing="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
AssertionConsumerServiceURL="https://remote...de01:10428/remote/saml/login"><saml:Issuer>http
s://rem
ote...de01:10428/remote/saml/metadata</saml:Issuer><samlp:NameIDPolicy
Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified" AllowCreate="true"/

></samlp:AuthnRequest></lasso:Request><lasso:RemoteProviderID>https://sts.windows.net/f1a7221
9-.../</lasso:RemoteProviderID><lasso:MsgUrl>h

ttps://login.microsoftonline.com/f1a72219-.../saml2?SAMLRequest=lZJBb9swDIX%2FiqG7bcl2EkdIAtj
xigXoNqNJd9hlkGW6FSBLmSh327%2Bf4nRrd1iBHUW%2BR

%2FF74AbFqM%2B8mvyjuYNvE6CPfozaIJ8bWzI5w61AhdyIEZB7yY%2FVh1ueJZSfnfVWWk1eWd52CERwXllDokOzJV9Z
UZdlnjf7Zbmu6HpRsTqvbqqGvqsXjNYFiT6Dw6DfkmAPJsQJDga9MD6UaFbENI%2Fp8kRz

vljxrPxCoiYwKCP87Hr0%2Fow8TbV9UCYZlXQW7eCt0cpAIu2YDkyssoyt464TeVwMS4jXeVfGEvIuL1i3kkORXsgyEt1
YJ2HOaksGoREuG7UBSj3Bn0r7nEqtTK%2FMw9uBdFcR8venUxu3n44nElW%2FQ9pbg9MI7

gjuSUm4v7t9AXIwWh8IlHfKoNXCJT1QxhktsvK5O699RSe7zeXB5wDd7v%2BnjOBFL7zYpK%2FnbK7n8zFwHZrWaiV%2F
XkIahf83NkvYXFF9PMxSPhk8g1SDgj7Qa22%2F7x0IHyL1bgKS7q6f%2Fn2mu18%3D&amp

;RelayState=magic%3D060806859681f2ed&amp;SigAlg=http%3A%2F%2Fwww.w3.org%2F2000%2F09%2Fxmldsig
%23rsa-sha1&amp;Signature=RkHlyfm3PThl8ei43dJ%2BERS%2B42ngKeo%2FQGxdcb

l7pfcuipF%2B0tt%2FctYzOQYMXmai3zBrmOWL%2FT6UHdySEPB3xy1puf%2BxwPfBYh%2BWnR6S6OQKwkYpsBwUsXWbg
rENrQxRFv1RRxm9TFiORyyWJCSCf94THDC0Uu%2BNmG2lyfoDXnmWUfy3hpBdMAKAQL3DJ
```

```
s2l2cKotLmSpPRvK9%2BG%2BYxDcUwDDXyfTzIW7pvo57qmO3L9DRDF1woftJ4Psn4p44LTxvV7bcW4WdhSfji7Z%2F%2
FyXzcg7TGnFC1pAw%2FsSXfzp%2FdHSym3TT%2FMIWtpa8JuKrmRWhBMzCP5IIUVxNQr5W

iaIA%3D%3D</lasso:MsgUrl><lasso:MsgRelayState>magic=060806859681f2ed</lasso:MsgRelayState><la
sso:HttpRequestMethod>4</lasso:HttpRequestMethod><lasso:RequestID>_14B
8833DC689A095A1B3AFAD0EB510B4</lasso:RequestID></lasso:Login>
**********************
samld_send_common_reply [91]: Code: 0, id: 563454, pid: 2293, len: 3517, data_len 3501
samld_send_common_reply [99]: Attr: 14, 2352, <lasso:Login
xmlns:lasso="http://www.entrouvert.org/namespaces/lasso/0.0"
xmlns:samlp="urn:oasis:names:tc:SAML:2.
0:protocol" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
LoginDumpVersion="2"><lasso:Request><samlp:AuthnRequest ID="_
14B8833DC689A095A1B3AFAD0EB510B4" Versi
on="2.0" IssueInstant="2024-03-06T03:57:28Z"
Destination="https://login.microsoftonline.com/f1a72219-.../saml2" SignType="0"
SignMethod="0"
ForceAuthn="false" IsPassive="false"
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
AssertionConsumerServiceURL="https://remote...de01

:10428/remote/saml/login"><saml:Issuer>https://remote...de01:10428/remote/saml/metadata</saml
:Issuer><samlp:NameIDPolicy Format="urn:oasis:names:tc:SAML:
1.1:nameid-format:unspecified"
AllowCreate="true"/></samlp:AuthnRequest></lasso:Request><lasso:RemoteProviderID>https://sts.
windows.net/f1a72219-.../</lasso:RemoteProviderID><lasso:MsgUrl>https://login.microsoftonline
.com/f1a72219-.../saml2?SAMLRequest=lZJBb9swDIX%2FiqG7bcl2Ekd

IAtjxigXoNqNJd9hlkGW6FSBLmSh327%2Bf4nRrd1iBHUW%2BR%2FF74AbFqM%2B8mvyjuYNvE6CPfozaIJ8bWzI5w61A
hdyIEZB7yY%2FVh1ueJZSfnfVWWk1eWd52CERwXllDokOzJV9ZUZdlnjf7Zbmu6HpRsTqv

bqqGvqsXjNYFiT6Dw6DfkmAPJsQJDga9MD6UaFbENI%2Fp8kRzvljxrPxCoiYwKCP87Hr0%2Fow8TbV9UCYZlXQW7eCt0
cpAIu2YDkyssoyt464TeVwMS4jXeVfGEvIuL1i3kkORXsgyEt1YJ2HOaksGoREuG7UBSj3

Bn0r7nEqtTK%2FMw9uBdFcR8venUxu3n44nElW%2FQ9pbg9MI7gjuSUm4v7t9AXIwWh8IlHfKoNXCJT1QxhktsvK5O699
RSe7zeXB5wDd7v%2BnjOBFL7zYpK%2FnbK7n8zFwHZrWaiV%2FXkIahf83NkvYXFF9PMxS

Phk8g1SDgj7Qa22%2F7x0IHyL1bgKS7q6f%2Fn2mu18%3D&amp;RelayState=magic%3D060806859681f2ed&amp;Si
gAlg=http%3A%2F%2Fwww.w3.org%2F2000%2F09%2Fxmldsig%23rsa-sha1&amp;Sign

ature=RkHlyfm3PThl8ei43dJ%2BERS%2B42ngKeo%2FQGxdcbl7pfcuipF%2B0tt%2FctYzOQYMXmai3zBrmOWL%2FT6
UHdySEPB3xy1puf%2BxwPfBYh%2BWnR6S6OQKwkYpsBwUsXWbgrENrQxRFv1RRxm9TFiOR

yyWJCSCf94THDC0Uu%2BNmG2lyfoDXnmWUfy3hpBdMAKAQL3DJs2l2cKotLmSpPRvK9%2BG%2BYxDcUwDDXyfTzIW7pvo
57qmO3L9DRDF1woftJ4Psn4p44LTxvV7bcW4WdhSfji7Z%2F%2FyXzcg7TGnFC1pAw%2Fs

SXfzp%2FdHSym3TT%2FMIWtpa8JuKrmRWhBMzCP5IIUVxNQr5WiaIA%3D%3D</lasso:MsgUrl><lasso:MsgRelaySta
te>magic=060806859681f2ed</lasso:MsgRelayState><lasso:HttpRequestMetho
```

```
d>4</lasso:HttpRequestMethod><lasso:RequestID>_
14B8833DC689A095A1B3AFAD0EB510B4</lasso:RequestID></lasso:Login>
samld_send_common_reply [99]: Attr: 11, 1149,
https://login.microsoftonline.com/f1a72219-.../saml2?SAMLRequest=lZJBb9swDIX%2FiqG7bcl2Ek

dIAtjxigXoNqNJd9hlkGW6FSBLmSh327%2Bf4nRrd1iBHUW%2BR%2FF74AbFqM%2B8mvyjuYNvE6CPfozaIJ8bWzI5w61
AhdyIEZB7yY%2FVh1ueJZSfnfVWWk1eWd52CERwXllDokOzJV9ZUZdlnjf7Zbmu6HpRsTq

vbqqGvqsXjNYFiT6Dw6DfkmAPJsQJDga9MD6UaFbENI%2Fp8kRzvljxrPxCoiYwKCP87Hr0%2Fow8TbV9UCYZlXQW7eCt
0cpAIu2YDkyssoyt464TeVwMS4jXeVfGEvIuL1i3kkORXsgyEt1YJ2HOaksGoREuG7UBSj

3Bn0r7nEqtTK%2FMw9uBdFcR8venUxu3n44nElW%2FQ9pbg9MI7gjuSUm4v7t9AXIwWh8IlHfKoNXCJT1QxhktsvK5O69
9RSe7zeXB5wDd7v%2BnjOBFL7zYpK%2FnbK7n8zFwHZrWaiV%2FXkIahf83NkvYXFF9PMx

SPhk8g1SDgj7Qa22%2F7x0IHyL1bgKS7q6f%2Fn2mu18%3D&RelayState=magic%3D060806859681f2ed&SigAlg=ht
tp%3A%2F%2Fwww.w3.org%2F2000%2F09%2Fxmldsig%23rsa-sha1&Signature=RkHly

fm3PThl8ei43dJ%2BERS%2B42ngKeo%2FQGxdcbl7pfcuipF%2B0tt%2FctYzOQYMXmai3zBrmOWL%2FT6UHdySEPB3xy
1puf%2BxwPfBYh%2BWnR6S6OQKwkYpsBwUsXWbgrENrQxRFv1RRxm9TFiORyyWJCSCf94T

HDC0Uu%2BNmG2lyfoDXnmWUfy3hpBdMAKAQL3DJs2l2cKotLmSpPRvK9%2BG%2BYxDcUwDDXyfTzIW7pvo57qmO3L9DRD
F1woftJ4Psn4p44LTxvV7bcW4WdhSfji7Z%2F%2FyXzcg7TGnFC1pAw%2FsSXfzp%2FdHS
ym3TT%2FMIWtpa8JuKrmRWhBMzCP5IIUVxNQr5WiaIA%3D%3D
samld_send_common_reply [119]: Sent resp: 3517, pid=2293, job_id=563454.
samld_process_request [145]: len=10189, cmd=2, pid=2293, job_id=563454
samld_process_request [162]: Received 10189, 0x1272e30
__samld_sp_login_resp [815]:
SP Login Response Msg Body (7536)
<samlp:Response ID="_d41828f1-07df-448b-af4d-d59b291280eb" Version="2.0" IssueInstant="2024-
03-06T03:57:28.827Z" Destination="https://remote...de01:10428
/remote/saml/login" InResponseTo="_14B8833DC689A095A1B3AFAD0EB510B4"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"><Issuer
xmlns="urn:oasis:names:tc:SAML:2.0:
assertion">https://sts.windows.net/f1a72219-.../</Issuer><samlp:Status><samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Success"
/></samlp:Status><Assertion ID="_af843ea7-5620-4f6b-bf20-4fb6db7f1100" IssueInstant="2024-03-
06T03:57:28.824Z" Version="2.0" xmlns="urn:oasis:names:tc:SAML:2.0:ass
ertion"><Issuer>https://sts.windows.net/f1a72219-.../</Issuer><Signature
xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo><Canonicali
zationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/><SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/><Reference URI="#
_af843ea7-5620-4f6b-bf20-4fb6db7f1100"><Transforms><Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/><Transform
Algorithm="http://www.w
3.org/2001/10/xml-exc-c14n#"/></Transforms><DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/><DigestValue>SxoMOgM7+7Chj+VhUVBdW5moKwv
+PwCErZyb49+g
```

```
CSY=</DigestValue></Reference></SignedInfo><SignatureValue>fgdYi3m3yz3ns7pdC3GFNg6Lu4OwvXiw1q
h4AR5zXlcq0uQiXMgqQzRKFb1fWuI8zGtOfb451kOlACyD7gLjmdVTcNe4mQJHAKxOWWRi

VpUw10r2NMXOvxF1hlCxpYdAYljAUt/Omu94QYShzZHQI49JrF9wA49cEPptiH83kYR+xU3u11jCpwovz1y4CRX/g6/pn
g6cqstX2nDvwvYPbnsAsMSYovUAvG/pqGjtwzO771TdYSDDCEPVTvGZMzYgJdLfZB2qVzc

0pU419vIYgoFitgJZG9sP1WOecOBJO2ozaU69QxpRIZsNBntnOm2nzPqEAwpXUmmF6xiDV5R/SQ==</SignatureValue
><KeyInfo><X509Data><X509Certificate>MIIC8DCCAdigAwIBAgIQReSC88H5bbBLd

kflSF49uzANBgkqhkiG9w0BAQsFADA0MTIwMAYDVQQDEylNaWNyb3NvZnQgQXp1cmUgRmVkZXJhdGVkIFNTTyBDZXJ0aW
ZpY2F0ZTAeFw0yMzEwMTUwNDQwMDhaFw0yNjEwMTUwNDQwMDhaMDQxMjAwBgNVBAMTKU1p

Y3Jvc29mdCBBenVyZSBGZWRlcmF0ZWQgU1NPIENlcnRpZmljYXRlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCA
QEAtwvk0AblPyElViGWIIup8qDUBeFoBV469YOUY87DFmQNGyTPbujE6iheWrLtBPwAnIZ

1A75FBaUNXY980vj/Oc6E+kbOy7nCm9GWueI0NvGLnS7HUKi2TrM+EcHhAR+ftV0egq/3MrdBKFKITYYYwO6P0W0JtBjy
CMY+XwGoxzREkajSXJnpsscNPwj/XdUBio7I6hnLCRzrTNy9l84nxXIFLZk+O/jzfdaYur

blfJJVa8895sMu/Ka5PBow5KJHGnFpjbOJegPBc5kdXjNGisAgpLoZEMNjA8kFSGhlOD6BBs4XGMx7SvM7w/+BPGGbjVy
Rn94YCoII9KWd7ZHpmQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQAs1OVASBqPuz09n0Xqt

koSnCgmQufBObUF5FpY990LBEPs/0Uv8LfPUuOukiJJOzbqewgBeIAJLtxfs8ckq40kiL+PjZWvRRVolJGUOiuUO+l+Wq
dI6O2D3euadlguERdOK3yjs7tFTPhgqtEcQ60QuAWjwEdpjZL0UT2NTdlJz67LRXAjCjB+

bXHQ7SndSQfbMtI+DhGo6n+J5XDWQRvhrKI4f1XqzvhkwlPvxUH1f3xo+KnhCYNPY8Ge0yRHHKzS+pHKv4O16GeG34SmJ
X0Rv17xr8xXuSY2fDQOK9JnHiLWHYRVuB+Mp5lyY+5EpGd7zErPjU7jycmSJcbWMgNH</X
509Certificate></X509Data></KeyInfo></Signature><Subject><NameID
Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress">user@example.onmicrosoft.com</
NameID><SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"><SubjectConfirmationData InResponseTo="_
14B8833DC689A095A1B3AFAD0EB510B4" NotOnOrAfter="
2024-03-06T04:57:28.694Z"
Recipient="https://remote...de01:10428/remote/saml/login"/></SubjectConfirmation></Subject><C
onditions NotBefore="2024-03-06T03
:52:28.694Z" NotOnOrAfter="2024-03-
06T04:57:28.694Z"><AudienceRestriction><Audience>https://remote...de01:10428/remote/saml/meta
data</Audience></Audience
Restriction></Conditions><AttributeStatement><Attribute
Name="http://schemas.microsoft.com/identity/claims/tenantid"><AttributeValue>f1a72219-...</At
tributeValue></Attribute><Attribute
Name="http://schemas.microsoft.com/identity/claims/objectidentifier"><AttributeValue>a6de82a
6-05c4-4093-8288-65af3624
2d67</AttributeValue></Attribute><Attribute
Name="http://schemas.microsoft.com/identity/claims/displayname"><AttributeValue>Yuyue
Li</AttributeValue></Attribute><A
ttribute
```

```
Name="http://schemas.microsoft.com/identity/claims/identityprovider"><AttributeValue>https://
sts.windows.net/f1a72219-.../</Attrib
uteValue></Attribute><Attribute
Name="http://schemas.microsoft.com/claims/authnmethodsreferences"><AttributeValue>http://sche
mas.microsoft.com/ws/2008/06/identity/
authenticationmethod/password</AttributeValue></Attribute><Attribute
Name="http://schemas.microsoft.com/ws/2008/06/identity/claims/wids"><AttributeValue>88d8e3e3-
8
f55-4a1e-953a-9b9898b8876b</AttributeValue><AttributeValue>62e90394-69f5-4237-9190-
012177145e10</AttributeValue><AttributeValue>b79fbf4d-3ef9-4689-8143-76b194e8550
9</AttributeValue></Attribute><Attribute
Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname"><AttributeValue>Yuyue<
/AttributeValue></Attribute><
Attribute
Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname"><AttributeValue>Li</Attr
ibuteValue></Attribute><Attribute Name="http://schemas.xmlso

ap.org/ws/2005/05/identity/claims/name"><AttributeValue>user@example.onmicrosoft.com</Attribu
teValue></Attribute><Attribute Name="username"><AttributeValue>yyl
i@fortinetvan.onmicrosoft.com</AttributeValue></Attribute><Attribute
Name="group"><AttributeValue>e6bbee59-c1d8-49e6-916b-
2fe6339a3d1e</AttributeValue><AttributeVa
lue>1cd4e267-054c-4e6c-b1ed-fc0f62dde5e6</AttributeValue><AttributeValue>3ccdd7c1-b59c-41c3-
a985-229ab4ded5a2</AttributeValue></Attribute></AttributeStatement><Aut
hnStatement AuthnInstant="2024-03-06T03:51:23.739Z" SessionIndex="_af843ea7-5620-4f6b-bf20-
4fb6db7f1100"><AuthnContext><AuthnContextClassRef>urn:oasis:names:tc:SAM

L:2.0:ac:classes:Password</AuthnContextClassRef></AuthnContext></AuthnStatement></Assertion><
/samlp:Response>
__samld_sp_login_resp [836]:
**** Assertion Dump ****
<Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID="_af843ea7-5620-4f6b-bf20-4fb6db7f1100"
IssueInstant
="2024-03-06T03:57:28.824Z"
Version="2.0"><Issuer>https://sts.windows.net/f1a72219-.../</Issuer><Signature
xmlns="http://www.w3.org/2000/09
/xmldsig#"><SignedInfo><CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/><SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-m
ore#rsa-sha256"/><Reference URI="#_af843ea7-5620-4f6b-bf20-
4fb6db7f1100"><Transforms><Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
<Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/></Transforms><DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/><DigestValue>SxoMOg

M7+7Chj+VhUVBdW5moKwv+PwCErZyb49+gCSY=</DigestValue></Reference></SignedInfo><SignatureValue>
fgdYi3m3yz3ns7pdC3GFNg6Lu4OwvXiw1qh4AR5zXlcq0uQiXMgqQzRKFb1fWuI8zGtOfb
```

```
451kOlACyD7gLjmdVTcNe4mQJHAKxOWWRiVpUw10r2NMXOvxF1hlCxpYdAYljAUt/Omu94QYShzZHQI49JrF9wA49cEPp
tiH83kYR+xU3u11jCpwovz1y4CRX/g6/png6cqstX2nDvwvYPbnsAsMSYovUAvG/pqGjtw

zO771TdYSDDCEPVTvGZMzYgJdLfZB2qVzc0pU419vIYgoFitgJZG9sP1WOecOBJO2ozaU69QxpRIZsNBntnOm2nzPqEAw
pXUmmF6xiDV5R/SQ==</SignatureValue><KeyInfo><X509Data><X509Certificate

>MIIC8DCCAdigAwIBAgIQReSC88H5bbBLdkflSF49uzANBgkqhkiG9w0BAQsFADA0MTIwMAYDVQQDEylNaWNyb3NvZnQg
QXp1cmUgRmVkZXJhdGVkIFNTTyBDZXJ0aWZpY2F0ZTAeFw0yMzEwMTUwNDQwMDhaFw0yNj

EwMTUwNDQwMDhaMDQxMjAwBgNVBAMTKU1pY3Jvc29mdCBBenVyZSBGZWRlcmF0ZWQgU1NPIENlcnRpZmljYXRlMIIBIjA
NBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtwvk0AblPyElViGWIIup8qDUBeFoBV469

YOUY87DFmQNGyTPbujE6iheWrLtBPwAnIZ1A75FBaUNXY980vj/Oc6E+kbOy7nCm9GWueI0NvGLnS7HUKi2TrM+EcHhAR
+ftV0egq/3MrdBKFKITYYYwO6P0W0JtBjyCMY+XwGoxzREkajSXJnpsscNPwj/XdUBio7I

6hnLCRzrTNy9l84nxXIFLZk+O/jzfdaYurblfJJVa8895sMu/Ka5PBow5KJHGnFpjbOJegPBc5kdXjNGisAgpLoZEMNjA
8kFSGhlOD6BBs4XGMx7SvM7w/+BPGGbjVyRn94YCoII9KWd7ZHpmQIDAQABMA0GCSqGSIb

3DQEBCwUAA4IBAQAs1OVASBqPuz09n0XqtkoSnCgmQufBObUF5FpY990LBEPs/0Uv8LfPUuOukiJJOzbqewgBeIAJLtxf
s8ckq40kiL+PjZWvRRVolJGUOiuUO+l+WqdI6O2D3euadlguERdOK3yjs7tFTPhgqtEcQ6

0QuAWjwEdpjZL0UT2NTdlJz67LRXAjCjB+bXHQ7SndSQfbMtI+DhGo6n+J5XDWQRvhrKI4f1XqzvhkwlPvxUH1f3xo+Kn
hCYNPY8Ge0yRHHKzS+pHKv4O16GeG34SmJX0Rv17xr8xXuSY2fDQOK9JnHiLWHYRVuB+Mp

5lyY+5EpGd7zErPjU7jycmSJcbWMgNH</X509Certificate></X509Data></KeyInfo></Signature><Subject><N
ameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">
user@example.onmicrosoft.com</NameID><SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"><SubjectConfirmationData InResponseTo="_
14B8833DC689A0
95A1B3AFAD0EB510B4" NotOnOrAfter="2024-03-06T04:57:28.694Z"
Recipient="https://remote...de01:10428/remote/saml/login"/></SubjectConfirmation></Subject><C
onditions NotBefore="2024-03-06T03:52:28.694Zike :shrank heap by 172032 bytes
ike V=root:0: comes 10.152.35.170:500->10.152.35.161:500,ifindex=3,vrf=0,len=456....
ike V=root:0: IKEv2 exchange=SA_INIT id=91d7e3bfd6eb8287/0000000000000000 len=456
ike 0: in
91D7E3BFD6EB828700000000000000000212022080000000000001C82200005C0200002C0101000403000000C01000
00C800E00800300000802000002030000080300000200000008040000050

000002C020100040300000C0100000C800E0100030000080200000503000008030000C0000000804000005280000
C800050000A5F0F0154C1F23D09D2C498ABD86C9875EFFC0E746A12E55AE182E3FBAFA

D9BA91FCAA52E25EB1E78AD3C6BD6A389E119BDBB8D07480F81680DACAF5D162042DF7FDAD3A091A9E0C2A026388A
39B658D8913B2376AF01B2F02E2AC22E6FC9309393388CF76676F136DB18B5BCE96EE1

87E06C3F481C0214A4392641C4F0163F2DA7A8B4F2C7168FE09C7F485C17A02360BA1A3358DEC4992DA2784338ACD
23A03ADABB04146732E3D51C4A4F1530F66E5951E668DAD51BB9FA1EF9D9C45F302B2B
```

```
000014FC1604191670582A2C223ECA5E6FD1862B0000144C53427B6D465D1B337BB755A37A7FEF2B000014B4F01CA
951E9DA8D0BAFBBD34AD3044E29000014C1DC4350476B98A429B91781914CA43E29000

01C000040049CFF24AC5C389CA04560B76DE2EA4DAD3980D4E90000001C00004005C736780986F56FDCFB69E529BD
4EFEB9405FBB47
ike V=root:0:91d7e3bfd6eb8287/0000000000000000:14: responder received SA_INIT msg
ike V=root:0:91d7e3bfd6eb8287/0000000000000000:14: VID forticlient connect license
4C53427B6D465D1B337BB755A37A7FEF
ike V=root:0:91d7e3bfd6eb8287/0000000000000000:14: VID Fortinet Endpoint Control
B4F01CA951E9DA8D0BAFBBD34AD3044E
ike V=root:0:91d7e3bfd6eb8287/0000000000000000:14: VID unknown (16):
C1DC4350476B98A429B91781914CA43E
ike V=root:0:91d7e3bfd6eb8287/0000000000000000:14: received notify type NAT_DETECTION_SOURCE_
IP
ike V=root:0:91d7e3bfd6eb8287/0000000000000000:14: received notify type NAT_DETECTION_
DESTINATION_IP
ike V=root:0:91d7e3bfd6eb8287/0000000000000000:14: incoming proposal:
ike V=root:0:91d7e3bfd6eb8287/0000000000000000:14: proposal id = 1:
ike V=root:0:91d7e3bfd6eb8287/0000000000000000:14: protocol = IKEv2:
ike V=root:0:91d7e3bfd6eb8287/0000000000000000:14: encapsulation = IKEv2/none
ike V=root:0:91d7e3bfd6eb8287/0000000000000000:14: type=ENCR, val=AES_CBC (key_len = 128)
ike V=root:0:91d7e3bfd6eb8287/0000000000000000:14: type=INTEGR, val=AUTH_HMAC_SHA_96
ike V=root:0:91d7e3bfd6eb8287/0000000000000000:14: type=PRF, val=PRF_HMAC_SHA
ike V=root:0:91d7e3bfd6eb8287/0000000000000000:14: type=DH_GROUP, val=MODP1536.
ike V=root:0:91d7e3bfd6eb8287/0000000000000000:14: proposal id = 2:
ike V=root:0:91d7e3bfd6eb8287/0000000000000000:14: protocol = IKEv2:
ike V=root:0:91d7e3bfd6eb8287/0000000000000000:14: encapsulation = IKEv2/none
ike V=root:0:91d7e3bfd6eb8287/0000000000000000:14: type=ENCR, val=AES_CBC (key_len = 256)
ike V=root:0:91d7e3bfd6eb8287/0000000000000000:14: type=INTEGR, val=AUTH_HMAC_SHA2_256_128
ike V=root:0:91d7e3bfd6eb8287/0000000000000000:14: type=PRF, val=PRF_HMAC_SHA2_256
ike V=root:0:91d7e3bfd6eb8287/0000000000000000:14: type=DH_GROUP, val=MODP1536.
ike V=root:0: cache rebuild start
ike V=root:0:V4-PSK: cached as dynamic
ike V=root:0:v4-Cert: cached as dynamic
ike V=root:0:v4-PSK-IKEv2: cached as dynamic
ike V=root:0: cache rebuild done
ike V=root:0:91d7e3bfd6eb8287/0000000000000000:14: matched proposal id 1
ike V=root:0:91d7e3bfd6eb8287/0000000000000000:14: proposal id = 1:
ike V=root:0:91d7e3bfd6eb8287/0000000000000000:14: protocol = IKEv2:
ike V=root:0:91d7e3bfd6eb8287/0000000000000000:14: encapsulation = IKEv2/none
ike V=root:0:91d7e3bfd6eb8287/0000000000000000:14: type=ENCR, val=AES_CBC (key_len = 128)
ike V=root:0:91d7e3bfd6eb8287/0000000000000000:14: type=INTEGR, val=AUTH_HMAC_SHA_96
ike V=root:0:91d7e3bfd6eb8287/0000000000000000:14: type=PRF, val=PRF_HMAC_SHA
ike V=root:0:91d7e3bfd6eb8287/0000000000000000:14: type=DH_GROUP, val=MODP1536.
ike V=root:0:91d7e3bfd6eb8287/0000000000000000:14: lifetime=86400
ike V=root:0:91d7e3bfd6eb8287/0000000000000000:14: SA proposal chosen, matched gateway v4-
PSK-IKEv2
ike V=root:0:v4-PSK-IKEv2: created connection: 0xe9bf900 3 10.152.35.161->10.152.35.170:500.
```

```
ike V=root:0:v4-PSK-IKEv2:14: processing notify type NAT_DETECTION_SOURCE_IP
ike V=root:0:v4-PSK-IKEv2:14: processing NAT-D payload
ike V=root:0:v4-PSK-IKEv2:14: NAT not detected
ike V=root:0:v4-PSK-IKEv2:14: process NAT-D
ike V=root:0:v4-PSK-IKEv2:14: processing notify type NAT_DETECTION_DESTINATION_IP
ike V=root:0:v4-PSK-IKEv2:14: processing NAT-D payload
ike V=root:0:v4-PSK-IKEv2:14: NAT not detected
ike V=root:0:v4-PSK-IKEv2:14: process NAT-D
ike V=root:0:v4-PSK-IKEv2:14: FEC vendor ID received FEC but IP not set
ike V=root:0:v4-PSK-IKEv2:14: responder preparing SA_INIT msg
ike V=root:0:v4-PSK-IKEv2:14: generate DH public value request queued
ike V=root:0:v4-PSK-IKEv2:14: responder preparing SA_INIT msg
ike V=root:0:v4-PSK-IKEv2:14: compute DH shared secret request queued
ike V=root:0:v4-PSK-IKEv2:14: responder preparing SA_INIT msg
ike V=root:0:v4-PSK-IKEv2:14: create NAT-D hash local 10.152.35.161/500 remote
10.152.35.170/500
ike 0:v4-PSK-IKEv2:14: out
91D7E3BFD6EB8287032B6561653DE26721202220000000000000016022000030000000 2C010100040300000C01000
00C800E008003000008020000020300000803000002

000000080400000052800 00C80005000065955E1E4681E843C5618C637FE43851C15AD4D34C8E1738B09188C6B3DA5
7CFFC88346E35095286C904E5751B1722F8FA0455F59AE7489A67180C2A36D65DAC6FA

FA4B9DADCE79F8B35851C2A22B8F452110665B6D16342709F5979D43F95CCE0617C40786355FF35D5E45864656435
6ED08A1A1CF29EA7C046246F09EFD49D3574DCC9D980EAFB1D08685642169ECB1E7081

9DB02E208F0C130FA97F071ADBD53F16E79384BA05CB0B8B18C6A0D125834119877FE45C11E7CDC77FFFA63B87290
00014473843BD329EC550DD27667C37BFDA7A2900001C00004004B752F27710DE7BFDF
FDDC48461DDFE77FE24B70F0000001C000040054F2308001BB502EDADE2CF75B498CCFD47FCEE4A
ike V=root:0:v4-PSK-IKEv2:14: sent IKE msg (SA_INIT_RESPONSE): 10.152.35.161:500-
>10.152.35.170:500, len=352, vrf=0, id=91d7e3bfd6eb8287/032b6561653de267, oif=3
ike 0:v4-PSK-IKEv2:14: IKE SA 91d7e3bfd6eb8287/032b6561653de267 SK_ei
16:8B1FC416E2A711C0A33BF3074485A78F
ike 0:v4-PSK-IKEv2:14: IKE SA 91d7e3bfd6eb8287/032b6561653de267 SK_er
16:A4BB868B7D8FBB81EDE5C9FD1555365E
ike 0:v4-PSK-IKEv2:14: IKE SA 91d7e3bfd6eb8287/032b6561653de267 SK_ai
20:2CB9528C9AE4B625B6F4A931ED07641416A51DCA
ike 0:v4-PSK-IKEv2:14: IKE SA 91d7e3bfd6eb8287/032b6561653de267 SK_ar
20:7F182EEB73D4DE03695AF202E620B2C741CF503A
ike V=root:0: comes 10.152.35.170:500->10.152.35.161:500,ifindex=3,vrf=0,len=620....
ike V=root:0: IKEv2 exchange=AUTH id=91d7e3bfd6eb8287/032b6561653de267:00000001 len=620
ike 0: in
91D7E3BFD6EB8287032B6561653DE2672E2023080000000 10000026C230002508DC5174C77E069C310D8A8382293B
7125A27239C47932A34F2C27458FC9774DC6FB3E3E179F8777D69A7E54EE

CDC0F4291E3B33E953B0761FC06B39882FA1EC00FFCB4CEB559AAD7272918C485A2A125CCD4B35B34CE7244BDD04B
5183E43AFF419452A1AE12917BDF31AB2D758983B60ED97A2183EE38A98BCD8FEFA0CD
```

```
4DF478699267107DC508EFF092359589355084DAEC722EBF52DD7699B409295987A6648989CF760D2FD44F2EB83B2
F897D2653D52FB5A073BAD3687CE0913A55CD36C6D481F362F5133CEBA3D623C64F360

4F2D7187A5130A479A7029EE4291F9A9E54AC3338AC79B151F97CE9900B50FC3C986F348FABDC430B5A5357477AA0
B58F4E29C08904A43DDA6938BCE9520D0CE4193B904CED247770B70F62A0BFE41C4396

DB9386B505910AE947DFDC37E8D75C6F71E202CF163EB4B90C5E68FF5F9817D7255EA3C3AB8C8DDAE99B04D619BC1
E56CD282EAE3873316290E349578360AC5F8136C69A7C2ABD0E4F2F419AE710899F1AD

6AE8A3A50EDC29574AC4D9F3ED065D6504344E2FA553E620F7D488D19FC4232556CC35EF4A84BE3A865E31AB4C169
F0280975271DEDFCD43E53B1E60D75DFACC56801D09E0AE14B3D39161963AB92402263

65F39E975EF85E988A3BD1D2419E2CA7C0A1B354CF920DC0B453B5FCBED5CC48F5617C15869185F0501380F2687B3
0709328485EE6520AFCB174F49B2292FFAE97F11474672E1AE754A5132CCFB5A0DBEC4

AD9BCF9DEEE1EC905E464F83A8448CEA16FFE33938A96485B283A40732CA6B25AF0870A974239DA5ED7CD8362308A
4C438FC7DC4512E4
ike 0:v4-PSK-IKEv2:14: dec
91D7E3BFD6EB8287032B6561653DE2672E2023080000000100000244230000042900000C010000000A9823AA29000
008000040002F0001380000F1005645523D310A4643

545645523D372E322E342E303937320A5549443D45363946374145304438343434344634413141463844463039424
445383539330A49503D31302E3135322E33352E3137300A4D41433D30302D31352D356

42D32332D61382D30313B0A484F53543D4445534B544F502D5550494E42524A0A555345523D453639463741453044
38343434344634413141463844463039424445383539330A4F535645523D4D6963726F

736F66742057696E646F777320313020456E74657270726973652045646974696F6E2C2036342D626974202862756
96C64203139303435290A5245475F5354415455533D300A454D53534E3D464354454D5

331303433353735353320A454D5349443D303030303030303030303030303030303030303030303030303030303030
3030300A00210000540100000000070010464354383030313434383131303439300001

000000020000000300000004000000D0000001900000008000000F0000000A0000000B000070010000540A00005
40B0000700000002C000054020000280103040 3E03A386C0300000C0100000C800E008

003000008030000020000000805000000000000280203040 3E03A386C0300000C0100000C800E0100030000080300
000C000000080500000002D000018010000000700001000 00FFFF00000000FFFFFFFF00
00001801000000070000100000FFFF00000000FFFFFFFF
ike V=root:0:v4-PSK-IKEv2:14: responder received AUTH msg
ike V=root:0:v4-PSK-IKEv2:14: processing notify type INITIAL_CONTACT
ike V=root:0:v4-PSK-IKEv2:14: processing notify type FORTICLIENT_CONNECT
ike V=root:0:v4-PSK-IKEv2:14: received FCT data len = 304, data = 'VER=1
FCTVER=7.2.4.0972
UID=E69F7AE0D84444F4A1AF8DF09BDE8593
IP=10.152.35.170
MAC=00-15-5d-23-a8-01;
HOST=DESKTOP-UPINBRJ
```

```
USER=E69F7AE0D84444F4A1AF8DF09BDE8593
OSVER=Microsoft Windows 10 Enterprise Edition, 64-bit (build 19045)
REG_STATUS=0
EMSSN=FCTEMS1043575532
EMSID=00000000000000000000000000000000
'
ike V=root:0:v4-PSK-IKEv2:14: received FCT-UID : E69F7AE0D84444F4A1AF8DF09BDE8593
ike V=root:0:v4-PSK-IKEv2:14: peer identifier IPV4_ADDR 10.152.35.170
ike V=root:0:v4-PSK-IKEv2:14: re-validate gw ID
ike V=root:0:v4-PSK-IKEv2:14: gw validation OK
ike V=root:0:v4-PSK-IKEv2:14: responder preparing EAP identity request
ike 0:v4-PSK-IKEv2:14: enc
2700000C010000000A9823A13000001C0200000066323F7A3C4C726A3D4D29D163A1D2EE26A29F1600000009018C0
005010E0D0C0B0A0908070605040302010E
ike 0:v4-PSK-IKEv2:14: out
91D7E3BFD6EB8287032B6561653DE2672E2023200000000010000007C2400006019975696D3E610D0A55FCE2141CE0
7B6CADD98E08E17E48B28D411CC7807751490126226

6AC460CEB8EF355E8DF5E1990674923144292715C8A7FFBE5186369083671645EB6300E98FAEE17C0613A79BBE393
4314FCE2BABD0835112
ike V=root:0:v4-PSK-IKEv2:14: sent IKE msg (AUTH_RESPONSE): 10.152.35.161:500-
>10.152.35.170:500, len=124, vrf=0, id=91d7e3bfd6eb8287/032b6561653de267:00000001, oi
f=3
ike V=root:0: comes 10.152.35.170:500->10.152.35.161:500,ifindex=3,vrf=0,len=108....
ike V=root:0: IKEv2 exchange=AUTH id=91d7e3bfd6eb8287/032b6561653de267:00000002 len=108
ike 0: in
91D7E3BFD6EB8287032B6561653DE2672E2023080000000020000006C30000050D355C65E627AB11AA4880DB9B65E4
660D5CE9F3414AD9C4ED0F64CCF1A4A250265D56EE573F5AF208A1E4EA6F
BC2CEED73E7EE8AB356C80FEC7B02D78C7CC1E7328CEF9F039CA8F6D3D9175B
ike 0:v4-PSK-IKEv2:14: dec
91D7E3BFD6EB8287032B6561653DE2672E2023080000000200000049300000040000002902 8C00250145363946374
145304438343434344634413141463844463039424 4
4538353933
ike V=root:0:v4-PSK-IKEv2:14: responder received EAP msg
ike V=root:0:v4-PSK-IKEv2:14: send EAP message to FNBAM
ike V=root:0:v4-PSK-IKEv2:14: initiating EAP authentication
ike V=root:0:v4-PSK-IKEv2: EAP user "E69F7AE0D84444F4A1AF8DF09BDE8593"
ike V=root:0:v4-PSK-IKEv2: auth candidate group 'ipsec-saml-group' 6
ike V=root:0:v4-PSK-IKEv2: EAP 300162803 pending
ike V=root:0:v4-PSK-IKEv2:14 EAP 300162803 result FNBAM_CHALLENGED
ike V=root:0:v4-PSK-IKEv2: EAP challenged for user "E69F7AE0D84444F4A1AF8DF09BDE8593"
ike V=root:0:v4-PSK-IKEv2:14: responder preparing EAP pass through message
ike 0:v4-PSK-IKEv2:14: enc
00000025018D00211A018D001C10127D990A0E60029A5973F7E9DB3C302D686F73746170640A09080706050403020
10A
ike 0:v4-PSK-IKEv2:14: out
91D7E3BFD6EB8287032B6561653DE2672E2023200000000020000006C3000005023BDD3F892B81FF71C36F5A1F8818
AAC1B5E266CA932E002099308830C1AD89103AE2A6C
```

```
BF22418D54EF94C27A081D1BDF9AFC403110DF51F2ACDC00FDCF48A3CB4FAC40AAEC2DA278FD1019
ike V=root:0:v4-PSK-IKEv2:14: sent IKE msg (AUTH_RESPONSE): 10.152.35.161:500-
>10.152.35.170:500, len=108, vrf=0, id=91d7e3bfd6eb8287/032b6561653de267:00000002, oi
f=3
ike V=root:0: comes 10.152.35.170:500->10.152.35.161:500,ifindex=3,vrf=0,len=156....
ike V=root:0: IKEv2 exchange=AUTH id=91d7e3bfd6eb8287/032b6561653de267:00000003 len=156
ike 0: in
91D7E3BFD6EB8287032B6561653DE2672E2023080000000030000009C30000080C3287818C3211DB53758AFFEA523D
CFCA3299F4AFBEBBBE50EC3DB44EA5D914B612529B169CD10D41F0220488

8F1AEEB193BA3640B87DA27AF7772921FC74494B837E26EEA63393ABF21AC2CD3532B128AF2BFBE362DE8A10A4DD9
7775353B65175262B421E4483DBA79842E0CA09D2C3F52DD7149658445582DC8C1
ike 0:v4-PSK-IKEv2:14: dec
91D7E3BFD6EB8287032B6561653DE2672E2023080000000030000007F30000040000005F028D005B1A028D005631C
828BD1F5DC09E2EAE44A295D803BD5E000000000000

00000D807F3A068A31FDCDBEA9D6273968C91D3F1F5EB1CFFB7E0045363946374145304438343434346344131414
6384446303942444538353933
ike V=root:0:v4-PSK-IKEv2:14: responder received EAP msg
ike V=root:0:v4-PSK-IKEv2:14: send EAP message to FNBAM
ike V=root:0:v4-PSK-IKEv2: EAP 300162803 pending
ike V=root:0:v4-PSK-IKEv2:14 EAP 300162803 result FNBAM_CHALLENGED
ike V=root:0:v4-PSK-IKEv2: EAP challenged for user "E69F7AE0D84444F4A1AF8DF09BDE8593"
ike V=root:0:v4-PSK-IKEv2:14: responder preparing EAP pass through message
ike 0:v4-PSK-IKEv2:14: enc
0000003C018E00381A038D0033533D43303737373636354142344433373642363239393634363642454438353036363
5424641374243333820 4D3D4F4B03020103
ike 0:v4-PSK-IKEv2:14: out
91D7E3BFD6EB8287032B6561653DE2672E2023200000000030000007C3000006062B69000FB6AEE38971A70EACE989
7104893B4B65D8E8CB390C129332713613C9F1EE27F

B09FDDBCA849ACA0E9852F3BA62AF9472271F3A29BFF603E74E5BF2B45A818A679B93D29F4C24B1A33761B950B654
B4EF14D417BF1E40510
ike V=root:0:v4-PSK-IKEv2:14: sent IKE msg (AUTH_RESPONSE): 10.152.35.161:500-
>10.152.35.170:500, len=124, vrf=0, id=91d7e3bfd6eb8287/032b6561653de267:00000003, oi
f=3
ike V=root:0: comes 10.152.35.170:500->10.152.35.161:500,ifindex=3,vrf=0,len=76....
ike V=root:0: IKEv2 exchange=AUTH id=91d7e3bfd6eb8287/032b6561653de267:00000004 len=76
ike 0: in
91D7E3BFD6EB8287032B6561653DE2672E2023080000000040000004C30000030BC217F9ADF27626EC3E13C22D8659
8BEC75E9887C9407B868045ED29084660F870974CD011CFAFDEF02D58C5
ike 0:v4-PSK-IKEv2:14: dec
91D7E3BFD6EB8287032B6561653DE2672E2023080000000040000002A30000040000000A028E00061A03
ike V=root:0:v4-PSK-IKEv2:14: responder received EAP msg
ike V=root:0:v4-PSK-IKEv2:14: send EAP message to FNBAM
ike V=root:0:v4-PSK-IKEv2: EAP 300162803 pending
ike V=root:0:v4-PSK-IKEv2:14 EAP 300162803 result FNBAM_SUCCESS
ike V=root:0:v4-PSK-IKEv2: user 'user@example.onmicrosoft.com' authenticated group 'ipsec-
```

```
saml-group' 6
ike V=root:0:v4-PSK-IKEv2:14: responder preparing EAP pass through message
ike 0:v4-PSK-IKEv2:14: enc 00000008038E00040706050403020107
ike 0:v4-PSK-IKEv2:14: out
91D7E3BFD6EB8287032B6561653DE2672E20232000000040000004C300000309A60CF863B708309D8C1418333CF2
1EC2A32E00615FDDF53EF5072DE9422A4D280605F88
257E11FED22FF0D5
ike V=root:0:v4-PSK-IKEv2:14: sent IKE msg (AUTH_RESPONSE): 10.152.35.161:500-
>10.152.35.170:500, len=76, vrf=0, id=91d7e3bfd6eb8287/032b6561653de267:00000004, oif
=3
ike V=root:0: comes 10.152.35.170:500->10.152.35.161:500,ifindex=3,vrf=0,len=92....
ike V=root:0: IKEv2 exchange=AUTH id=91d7e3bfd6eb8287/032b6561653de267:00000005 len=92
ike 0: in
91D7E3BFD6EB8287032B6561653DE2672E20230800000005000000 5C270000409F291281AD48EC4CD1DFEF5961D33
BE185A04F1810661E66FBC1F5846796CD0A535C063D19A0E930A51130F3D
9413512EF92EC71E582D10991B7FE42
ike 0:v4-PSK-IKEv2:14: dec
91D7E3BFD6EB8287032B6561653DE2672E2023080000000500000003C270000040000001C0200000063A2A164BD0FE
9F4D29DDA752517ACD373B1567E
ike V=root:0:v4-PSK-IKEv2:14: responder received AUTH msg
ike V=root:0:v4-PSK-IKEv2:14: auth verify done
ike V=root:0:v4-PSK-IKEv2:14: responder AUTH continuation
ike V=root:0:v4-PSK-IKEv2:14: authentication succeeded
ike V=root:0:v4-PSK-IKEv2:14: responder creating new child
ike V=root:0:v4-PSK-IKEv2:14: mode-cfg type 7 request 16:'46435438303031343438313130343930'
ike V=root:0:v4-PSK-IKEv2:14: mode-cfg received APPLICATION_VERSION 'FCT8001448110490'
ike V=root:0:v4-PSK-IKEv2:14: mode-cfg type 1 request 0:''
ike V=root:0:v4-PSK-IKEv2: mode-cfg allocate 192.168.1.100/0.0.0.0
ike V=root:0:v4-PSK-IKEv2:14: mode-cfg using allocated IPv4 192.168.1.100
ike V=root:0:v4-PSK-IKEv2:14: mode-cfg type 2 request 0:''
ike V=root:0:v4-PSK-IKEv2:14: mode-cfg type 3 request 0:''
ike V=root:0:v4-PSK-IKEv2:14: mode-cfg type 4 request 0:''
ike V=root:0:v4-PSK-IKEv2:14: mode-cfg WINS ignored, no WINS servers configured
ike V=root:0:v4-PSK-IKEv2:14: mode-cfg type 13 request 0:''
ike V=root:0:v4-PSK-IKEv2:14: mode-cfg type 25 request 0:''
ike V=root:0:v4-PSK-IKEv2:14: mode-cfg type 8 request 0:''
ike V=root:0:v4-PSK-IKEv2: IPv6 pool is not configured
ike V=root:0:v4-PSK-IKEv2:14: mode-cfg could not allocate IPv6 address
ike V=root:0:v4-PSK-IKEv2:14: mode-cfg type 15 request 0:''
ike V=root:0:v4-PSK-IKEv2:14: mode-cfg type 10 request 0:''
ike V=root:0:v4-PSK-IKEv2:14: mode-cfg type 11 request 0:''
ike V=root:0:v4-PSK-IKEv2:14: mode-cfg type 11 not supported, ignoring
ike V=root:0:v4-PSK-IKEv2:14: mode-cfg type 28673 request 0:''
ike V=root:0:v4-PSK-IKEv2:14: mode-cfg UNITY type 28673 requested
ike V=root:0:v4-PSK-IKEv2:14: mode-cfg type 21514 request 0:''
ike V=root:0:v4-PSK-IKEv2:14: mode-cfg type 21514 requested
ike V=root:0:v4-PSK-IKEv2:14: mode-cfg type 21515 request 0:''
ike V=root:0:v4-PSK-IKEv2:14: mode-cfg type 21515 requested
```

```
ike V=root:0:v4-PSK-IKEv2:14: mode-cfg type 28672 request 0:''
ike V=root:0:v4-PSK-IKEv2:14: mode-cfg UNITY type 28672 requested
ike V=root:0:v4-PSK-IKEv2:14: mode-cfg no banner configured, ignoring
ike V=root:0:v4-PSK-IKEv2:14:10: peer proposal:
ike V=root:0:v4-PSK-IKEv2:14:10: TSi_0 0:0.0.0.0-255.255.255.255:0
ike V=root:0:v4-PSK-IKEv2:14:10: TSr_0 0:0.0.0.0-255.255.255.255:0
ike V=root:0:v4-PSK-IKEv2:14:v4-PSK-IKEv2:10: comparing selectors
ike V=root:0:v4-PSK-IKEv2:14:v4-PSK-IKEv2:10: matched by rfc-rule-2
ike V=root:0:v4-PSK-IKEv2:14:v4-PSK-IKEv2:10: phase2 matched by subset
ike V=root:0:v4-PSK-IKEv2:14:v4-PSK-IKEv2:10: using mode-cfg override 0:192.168.1.100-
192.168.1.100:0
ike V=root:0:v4-PSK-IKEv2:14:v4-PSK-IKEv2:10: accepted proposal:
ike V=root:0:v4-PSK-IKEv2:14:v4-PSK-IKEv2:10: TSi_0 0:192.168.1.100-192.168.1.100:0
ike V=root:0:v4-PSK-IKEv2:14:v4-PSK-IKEv2:10: TSr_0 0:0.0.0.0-255.255.255.255:0
ike V=root:0:v4-PSK-IKEv2:14:v4-PSK-IKEv2:10: dialup
ike V=root:0:v4-PSK-IKEv2:14:v4-PSK-IKEv2:10: incoming child SA proposal:
ike V=root:0:v4-PSK-IKEv2:14:v4-PSK-IKEv2:10: proposal id = 1:
ike V=root:0:v4-PSK-IKEv2:14:v4-PSK-IKEv2:10: protocol = ESP:
ike V=root:0:v4-PSK-IKEv2:14:v4-PSK-IKEv2:10: encapsulation = TUNNEL
ike V=root:0:v4-PSK-IKEv2:14:v4-PSK-IKEv2:10: type=ENCR, val=AES_CBC (key_len = 128)
ike V=root:0:v4-PSK-IKEv2:14:v4-PSK-IKEv2:10: type=INTEGR, val=SHA
ike V=root:0:v4-PSK-IKEv2:14:v4-PSK-IKEv2:10: type=ESN, val=NO
ike V=root:0:v4-PSK-IKEv2:14:v4-PSK-IKEv2:10: PFS is disabled
ike V=root:0:v4-PSK-IKEv2:14:v4-PSK-IKEv2:10: matched proposal id 1
ike V=root:0:v4-PSK-IKEv2:14:v4-PSK-IKEv2:10: proposal id = 1:
ike V=root:0:v4-PSK-IKEv2:14:v4-PSK-IKEv2:10: protocol = ESP:
ike V=root:0:v4-PSK-IKEv2:14:v4-PSK-IKEv2:10: encapsulation = TUNNEL
ike V=root:0:v4-PSK-IKEv2:14:v4-PSK-IKEv2:10: type=ENCR, val=AES_CBC (key_len = 128)
ike V=root:0:v4-PSK-IKEv2:14:v4-PSK-IKEv2:10: type=INTEGR, val=SHA
ike V=root:0:v4-PSK-IKEv2:14:v4-PSK-IKEv2:10: type=ESN, val=NO
ike V=root:0:v4-PSK-IKEv2:14:v4-PSK-IKEv2:10: PFS is disabled
ike V=root:0:v4-PSK-IKEv2:14:v4-PSK-IKEv2:10: lifetime=43200
ike V=root:0:v4-PSK-IKEv2:14: responder preparing AUTH msg
ike V=root:0:v4-PSK-IKEv2: IPv6 pool is not configured
ike V=root:0:v4-PSK-IKEv2: adding new dynamic tunnel for 10.152.35.170:500
ike V=root:0:v4-PSK-IKEv2_0: tunnel created tun_id 192.168.1.100/::10.0.0.11 remote_location
0.0.0.0
ike V=root:0:v4-PSK-IKEv2_0: added new dynamic tunnel for 10.152.35.170:500
ike V=root:0:v4-PSK-IKEv2_0:14: established IKE SA 91d7e3bfd6eb8287/032b6561653de267
ike V=root:0:v4-PSK-IKEv2_0:14: check peer route: if_addr4_rcvd=0, if_addr6_rcvd=0, mode_
cfg=1
ike V=root:0:v4-PSK-IKEv2_0:14: processing INITIAL-CONTACT
ike V=root:0:v4-PSK-IKEv2_0: flushing
ike V=root:0:v4-PSK-IKEv2_0: flushed
ike V=root:0:v4-PSK-IKEv2_0:14: processed INITIAL-CONTACT
ike V=root:0:v4-PSK-IKEv2_0:14: mode-cfg assigned (1) IPv4 address 192.168.1.100
ike V=root:0:v4-PSK-IKEv2_0:14: mode-cfg assigned (2) IPv4 netmask 255.255.255.255
ike V=root:0:v4-PSK-IKEv2_0:14: mode-cfg send (13) 0:192.168.235.0/255.255.255.0:0
```

```
ike V=root:0:v4-PSK-IKEv2_0:14: mode-cfg send (3) IPv4 DNS(1) 172.17.60.6
ike V=root:0:v4-PSK-IKEv2_0:14: mode-cfg send (3) IPv4 DNS(2) 8.8.8.8
ike V=root:0:v4-PSK-IKEv2_0:14: mode-cfg send INTERNAL_IP6_SUBNET
ike V=root:0:v4-PSK-IKEv2_0:14: mode-cfg IPv6 DNS ignored, no IPv6 DNS servers found
ike V=root:0:v4-PSK-IKEv2_0:14: mode-cfg send APPLICATION_VERSION 'FortiGate-VM64-HV
v7.4.3,build2573,240201 (GA.F)'
ike V=root:0:v4-PSK-IKEv2_0:14: mode-cfg send (28673) UNITY_SAVE_PASSWD
ike V=root:0:v4-PSK-IKEv2_0:14: mode-cfg send (21514) FNT_AUTO_NEGOTIATE
ike V=root:0:v4-PSK-IKEv2_0:14: mode-cfg send (21515) FNT_KEEP_ALIVE
ike V=root:0:v4-PSK-IKEv2_0:14:v4-PSK-IKEv2:10: replay protection enabled
ike V=root:0:v4-PSK-IKEv2_0:14:v4-PSK-IKEv2:10: set sa life soft seconds=43189.
ike V=root:0:v4-PSK-IKEv2_0:14:v4-PSK-IKEv2:10: set sa life hard seconds=43200.
ike V=root:0:v4-PSK-IKEv2_0:14:v4-PSK-IKEv2:10: IPsec SA selectors #src=1 #dst=1
ike V=root:0:v4-PSK-IKEv2_0:14:v4-PSK-IKEv2:10: src 0 7 0:0.0.0.0-255.255.255.255:0
ike V=root:0:v4-PSK-IKEv2_0:14:v4-PSK-IKEv2:10: dst 0 7 0:192.168.1.100-192.168.1.100:0
ike V=root:0:v4-PSK-IKEv2_0:14:v4-PSK-IKEv2:10: add dynamic IPsec SA selectors 682
ike V=root:0:v4-PSK-IKEv2_0:14:v4-PSK-IKEv2:10: added dynamic IPsec SA proxyids new 1 682
ike V=root:0:v4-PSK-IKEv2:10: add route 192.168.1.100/255.255.255.255 gw 192.168.1.100 oif
v4-PSK-IKEv2(14) metric 15 priority 1
ike V=root:0:v4-PSK-IKEv2_0:14:v4-PSK-IKEv2:10: tunnel 1 of VDOM limit 0/0
ike V=root:0:v4-PSK-IKEv2_0:14:v4-PSK-IKEv2:10: add IPsec SA: SPIs=758626b2/e03a386c
ike 0:v4-PSK-IKEv2_0:14:v4-PSK-IKEv2:10: IPsec SA dec spi 758626b2 key
16:5F6D51E51801CDD3C5DDFFCD55CEBF18 auth 20:4284FFE8D12D3E617DDEEADE9E71ECBEBE07918E
ike 0:v4-PSK-IKEv2_0:14:v4-PSK-IKEv2:10: IPsec SA enc spi e03a386c key
16:CF5000829B184D71E97B4839BB221801 auth 20:1C9497F99E0EEFD7091A20EECA7CC95E6672FDFB
ike V=root:0:v4-PSK-IKEv2_0:14:v4-PSK-IKEv2:10: added IPsec SA: SPIs=758626b2/e03a386c
ike V=root:0:v4-PSK-IKEv2_0:14:v4-PSK-IKEv2:10: sending SNMP tunnel UP trap
ike V=root:0:v4-PSK-IKEv2_0: tunnel up event assigned address 192.168.1.100
ike V=root:0:v4-PSK-IKEv2_0: sent tunnel-up message to EMS: (fct-
uid=E69F7AE0D84444F4A1AF8DF09BDE8593, intf=v4-PSK-IKEv2_0, addr=192.168.1.100, vdom=root)
ike V=root:0:v4-PSK-IKEv2_0: user 'user@example.onmicrosoft.com' 192.168.1.100 groups 1
ike 0:v4-PSK-IKEv2_0:14: enc
2700000C010000000A9823A12F00001C02000000DE195F007E8D93462142A62E9452006F4D98B2682100008F02000
00000010004C0A8016400020004FFFFFFFF000D00

08C0A8EB00FFFFFF0000030004AC113C0600030004080808000F00110000000000000000000000000000000000000
0070030466F727469476174652D564D36342D48562076372E342E332C6275696C64323

537332C32343032303120284741 2E4629700100020001540A00020001540B000200012C00002C0000002801030403
758626B20300000C0100000C800E00800300000803000002000000080500000002D0000

1801000000070000100000FFFFC0A80164C0A80164000000180100000007000010000 0FFFF00000000FFFFFFFF0C0
B0A0908070605040302010C
ike 0:v4-PSK-IKEv2_0:14: out
91D7E3BFD6EB8287032B6561653DE2672E202320000000050000015C24000140F73C9BCD7A9F971B02F6A48AE9B37
644762FCA3FB4E3D0E2136A72A1BBC4113F7A87F3
```

```
9A611CBE1B0E5036D73020A46B6455BEE66FFC5F95E237337C4CFF0A4CCA52BB18DC3A17F497E12FDDE5D8A6953B4
295109F0BEDBA72459E3750D6924159BE555D8011EF5B9C0EA1EA91BFA6F0E850A7296

B813DE95FF47F40545584CCC00264377258E6C3769A64834AE9161B286DD9067B689E53EC59C6C3E28BE798401730
A6E01CC23756A75142244140C1EA6FE3D771F24E768D2E092888F08E3BFC3CE5486819

1B5BFB6CE6E97764CF75B6AE068B5C7398EF72C0E963FC15EDAD00A166AFECCFE35EB6314C7FD27C2C5F718777FE7
3ADBB8472255BB4FDDD9CE39E39743258520024 6F891A68A86CEE05748502CC58770BB
128F31D2FFAF62526C987A9CEFBFD15644DEB317102BB51DDD54D7C206DF42F010FC7ACCE
ike V=root:0:v4-PSK-IKEv2_0:14: sent IKE msg (AUTH_RESPONSE): 10.152.35.161:500-
>10.152.35.170:500, len=348, vrf=0, id=91d7e3bfd6eb8287/032b6561653de267:00000005,
oif=3
ike V=root:0:v4-PSK-IKEv2_0: link is idle 3 10.152.35.161->10.152.35.170:0 dpd=1 seqno=1 rr=0
ike V=root:0: comes 10.152.35.170:500->10.152.35.161:500,ifindex=3,vrf=0,len=76....
ike V=root:0: IKEv2 exchange=INFORMATIONAL id=91d7e3bfd6eb8287/032b6561653de267:00000006
len=76
ike 0: in
91D7E3BFD6EB8287032B6561653DE2672E2025080000000600000004C000000308313D182BDFE6429ACF9CD754A0CA
A19E6997AD0F915E69445D9C1256C6CBF7694582330F8AED0C6F892FD1D
ike 0:v4-PSK-IKEv2_0:14: dec 91D7E3BFD6EB8287032B6561653DE2672E2025080000000600000002000000004
ike V=root:0:v4-PSK-IKEv2_0:14: received informational request
ike 0:v4-PSK-IKEv2_0:14: enc 0F0E0D0C0B0A09080706050403020 10F
ike 0:v4-PSK-IKEv2_0:14: out
91D7E3BFD6EB8287032B6561653DE2672E2025200000000600000004C00000030E74A78C1B6607A4209955C934EBD0
486354D124282E51DAEF58CBFB26AAABE8E4E905A
2ED459F3DD076CFD23
ike V=root:0:v4-PSK-IKEv2_0:14: sent IKE msg (INFORMATIONAL_RESPONSE): 10.152.35.161:500-
>10.152.35.170:500, len=76, vrf=0, id=91d7e3bfd6eb8287/032b6561653de267:00
000006, oif=3
ike :shrank heap by 331776 bytes
ike V=root:0: comes 10.152.35.170:500->10.152.35.161:500,ifindex=3,vrf=0,len=76....
ike V=root:0: IKEv2 exchange=INFORMATIONAL id=91d7e3bfd6eb8287/032b6561653de267:00000007
len=76
ike 0: in
91D7E3BFD6EB8287032B6561653DE2672E2025080000000700000004C00000030B7731C94B7CD08C9325F550EC0EAB
E733FC5DA5E50A1440AE3FE358726D1DE7EFE61CC3D02674FE0155CE28F
ike 0:v4-PSK-IKEv2_0:14: dec 91D7E3BFD6EB8287032B6561653DE2672E2025080000000700000002000000004
ike V=root:0:v4-PSK-IKEv2_0:14: received informational request
ike 0:v4-PSK-IKEv2_0:14: enc 0F0E0D0C0B0A09080706050403020 10F
ike 0:v4-PSK-IKEv2_0:14: out
91D7E3BFD6EB8287032B6561653DE2672E2025200000000700000004C0000003042E9544F9024C5ED6F72E90A613C9
9A7EA7AFE3534D71E8FEC8CA3B65DB1708473F80D
5395ABBD30500A38DA
ike V=root:0:v4-PSK-IKEv2_0:14: sent IKE msg (INFORMATIONAL_RESPONSE): 10.152.35.161:500-
>10.152.35.170:500, len=76, vrf=0, id=91d7e3bfd6eb8287/032b6561653de267:00
000007, oif=3
ike V=root:0: comes 10.152.35.170:500->10.152.35.161:500,ifindex=3,vrf=0,len=76....
ike V=root:0: IKEv2 exchange=INFORMATIONAL id=91d7e3bfd6eb8287/032b6561653de267:00000008
```

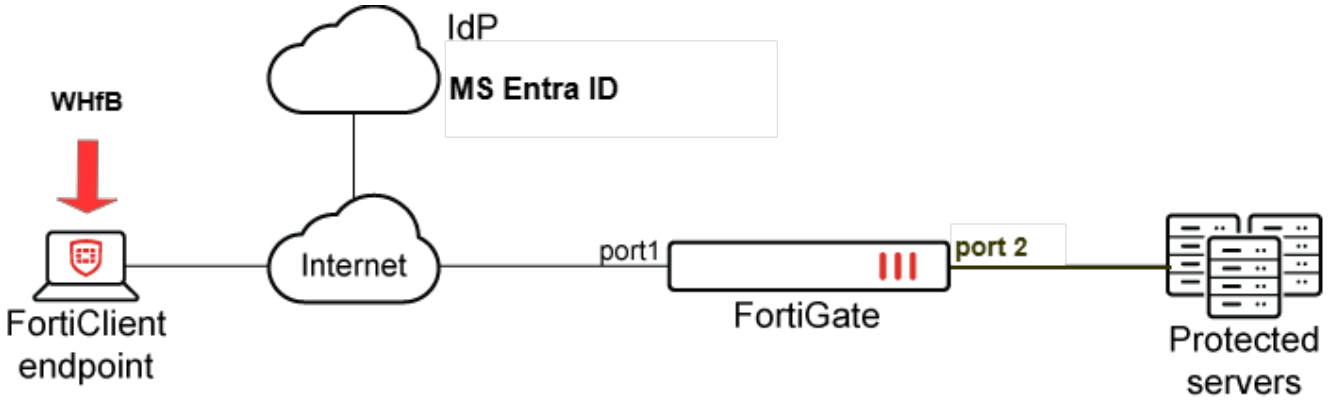
```
len=76
ike 0: in
91D7E3BFD6EB8287032B6561653DE2672E2025080000000800000004C00000030D72FA651DD9192B8390213F8D30CF
93C1F47EAC9934E09391EBB7F7E55C8DF0574AAFA1CCCBFD5C34F93AFD8
ike 0:v4-PSK-IKEv2_0:14: dec 91D7E3BFD6EB8287032B6561653DE2672E2025080000000800000002000000004
ike V=root:0:v4-PSK-IKEv2_0:14: received informational request
ike 0:v4-PSK-IKEv2_0:14: enc 0F0E0D0C0B0A09080706050403020 10F
ike 0:v4-PSK-IKEv2_0:14: out
91D7E3BFD6EB8287032B6561653DE2672E2025200000000800000004C00000030494190DE9E0047C7B17F642218C27
C46615E9AA717E1BDEFA2B56938BD8990C9B54783
49D4AD0420063AE9B4
ike V=root:0:v4-PSK-IKEv2_0:14: sent IKE msg (INFORMATIONAL_RESPONSE): 10.152.35.161:500-
>10.152.35.170:500, len=76, vrf=0, id=91d7e3bfd6eb8287/032b6561653de267:00
000008, oif=3
```

Windows Hello Business support for FortiGate SAML-based IPsec VPN

For FortiGate SAML-based auto-connect IPsec VPN tunnels using Microsoft Entra ID, Windows Hello for Business (key-based or certificate-based) authentication users automatically connect to the tunnel after Windows login (using MFA with PIN or biometrics, such as fingerprint or facial recognition) without the need to re-authenticate for the VPN connection using the Entra ID username and password.

The following is an example of a FortiGate SAML-based IPsec VPN auto-connecting seamlessly using PIN or biometric Windows login via Windows Hello for Business.

Topology



FortiGate configuration

To configure a FortiGate SAML-based auto-connect IPsec VPN tunnel using Microsoft Entra ID:

```
config system global
    set auth-ike-saml-port 1234
```

```
end
config user saml
    edit "saml_azure"
        set entity-id "https://fgtvms.fortinet-fsso.com:1234/remote/saml/metadata"
        set single-sign-on-url "https://fgtvms.fortinet-fsso.com:1234/remote/saml/login"
        set single-logout-url "https://fgtvms.fortinet-fsso.com:1234/remote/saml/logout"
        set idp-entity-id "https://sts.windows.net/f1a72219-bba3-4f6e-93b8-ce3b341b7cf4/"
        set idp-single-sign-on-url "https://login.microsoftonline.com/f1a72219-bba3-4f6e-93b8-
ce3b341b7cf4/saml2"
        set idp-single-logout-url "https://login.microsoftonline.com/f1a72219-bba3-4f6e-93b8-
ce3b341b7cf4/saml2"
        set idp-cert "REMOTE_Cert_1"
        set user-name "http://schemas.microsoft.com/identity/claims/displayname"
        set group-name "user.groups"
        set digest-method sha1
    next
end
config user group
    edit "VPN_Group"
        set member "saml_azure"
    next
end
config system interface
    edit "port1"
        set ike-saml-server "saml_azure"
    next
end
config firewall address
    edit "IPsec_Tunnel_Add"
        set uuid eb1ef2de-6f22-51f0-cb1c-29661de3254e
        set type iprange
        set start-ip 192.168.183.100
        set end-ip 192.168.183.200
    next
end
config vpn ipsec phase1-interface
    edit "IKEV2-SAML-AZ"
        set type dynamic
        set interface "port1"
        set ike-version 2
        set peertype any
        set net-device disable
        set mode-cfg enable
        set proposal aes128-sha256 aes256-sha256
        set dpd on-idle
        set comments "VPN: IKEV2_SAML_AZ (Created by VPN wizard)"
        set dhgrp 5 15
        set eap enable
        set eap-identity send-request
        set wizard-type dialup-forticlient
        set reauth enable
        set authusrgrp "VPN_Group"
```

```
        set client-resume enable
        set client-resume-interval 120
        set network-overlay enable
        set network-id 20
        set transport udp
        set assign-ip-from name
        set dns-mode auto
        set ipv4-name "IPsec_Tunnel_Add"
        set save-password enable
        set client-auto-negotiate enable
        set client-keep-alive enable
        set psksecret ENC
zJrtRzDllMxyinqk+NaPcXu2gSVqqqQidEssBnIFrlEDjPa2tR5JRElNQ4pmJlAno1Vogwdt2S39fqyBgjbCSpp50YNFE//+g9
ycAR6fukJ/93VdgYvNo48cRtK0li6gWyNn+ryF0yul88U2gMQ3+1HavwkD8Q2G73m7uj6ehKf/SRuz+j1Sddr/o8dH01TllxrJ
pVlmMjY3dkVA
    next
end
config vpn ipsec phase2-interface
    edit "IKEV2_SAML_AZ"
        set phase1name "IKEV2-SAML-AZ"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm
chacha20poly1305
        set dhgrp 15
        set comments "VPN: IKEV2_SAML_AZ (Created by VPN wizard)"
    next
end
```

FortiClient EMS configuration

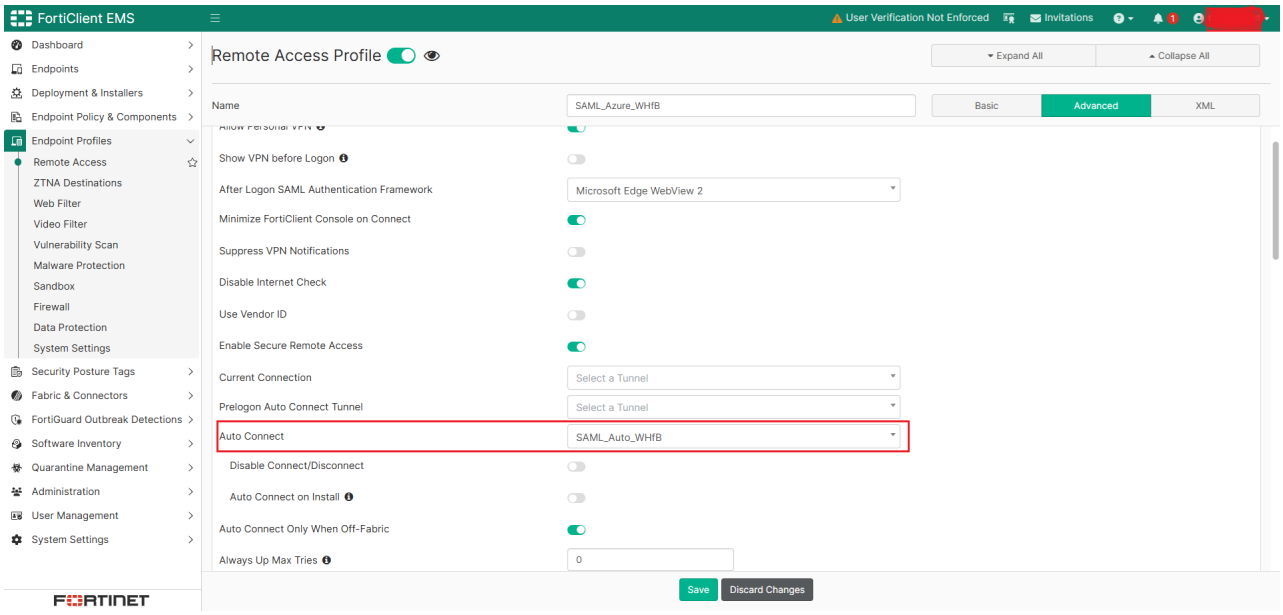
You must configure the FortiGate SAML-based IPsec VPN tunnel with *Auto Connect* enabled in the EMS XML or GUI:

- **XML:**

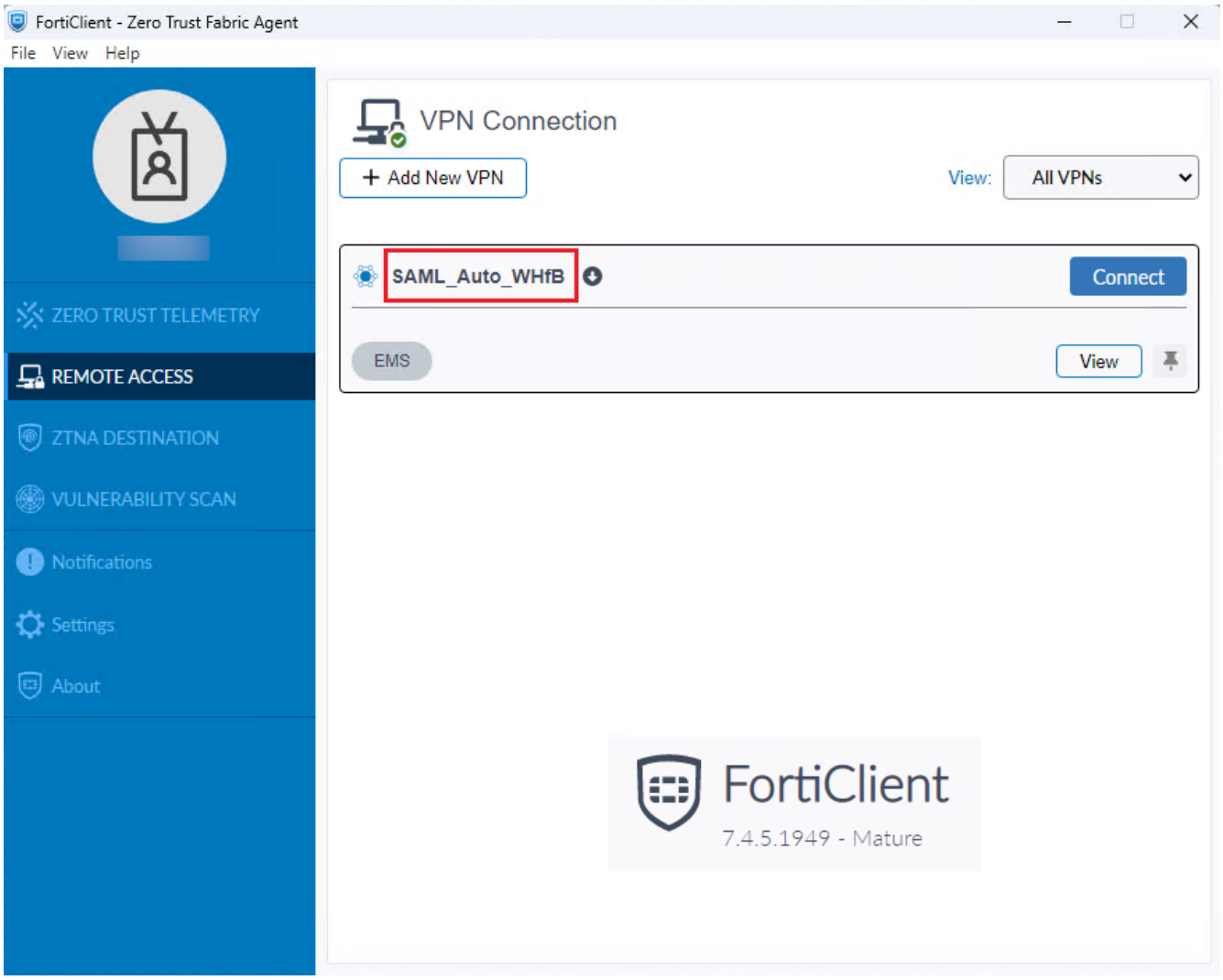
```
<forticlient_configuration>
    <vpn>
        <ipsecvpn>
            <connections>
                <connection>
                    <name>SAML_Auto_WHfB</name>
                    <ike_settings>
                        <version>2</version>
                        <authentication_method>Preshared Key</authentication_method>
                        <server>fgtvms.fortinet-fsso.com</server>
                         <ike_saml_port>1234</ike_saml_port>
                    </ike_settings>
                    <sso_enabled>1</sso_enabled>
                </connection>
            </connections>
        </ipsecvpn>
        <options>
            <autoconnect_tunnel>SAML_Auto_WHfB</autoconnect_tunnel>
```

```
        </options>
    </vpn>
</forticlient_configuration>
```

- **GUI:**



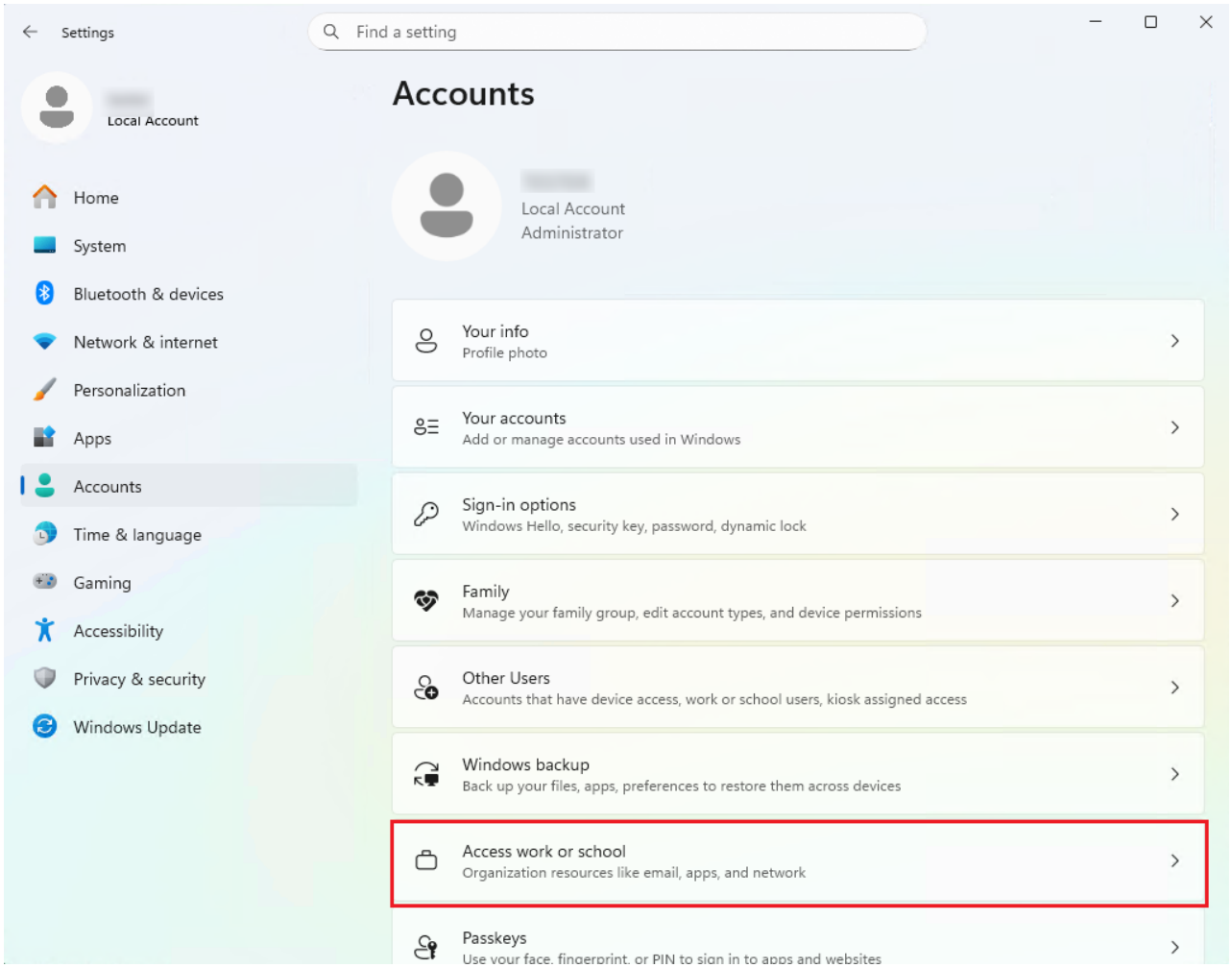
After the EMS configuration, verify that the FortiGate SAML-based IPsec VPN tunnel has been pushed to FortiClient via EMS:


FortiClient - Zero Trust Fabric Agent
File View Help
ZERO TRUST TELEMETRY
REMOTE ACCESS
ZTNA DESTINATION
VULNERABILITY SCAN
Notifications
Settings
About
VPN Connection
+ Add New VPN
View:
All VPNs
SAML_Auto_WHfB
Connect
EMS
View
FortiClient
7.4.5.1949 - Mature

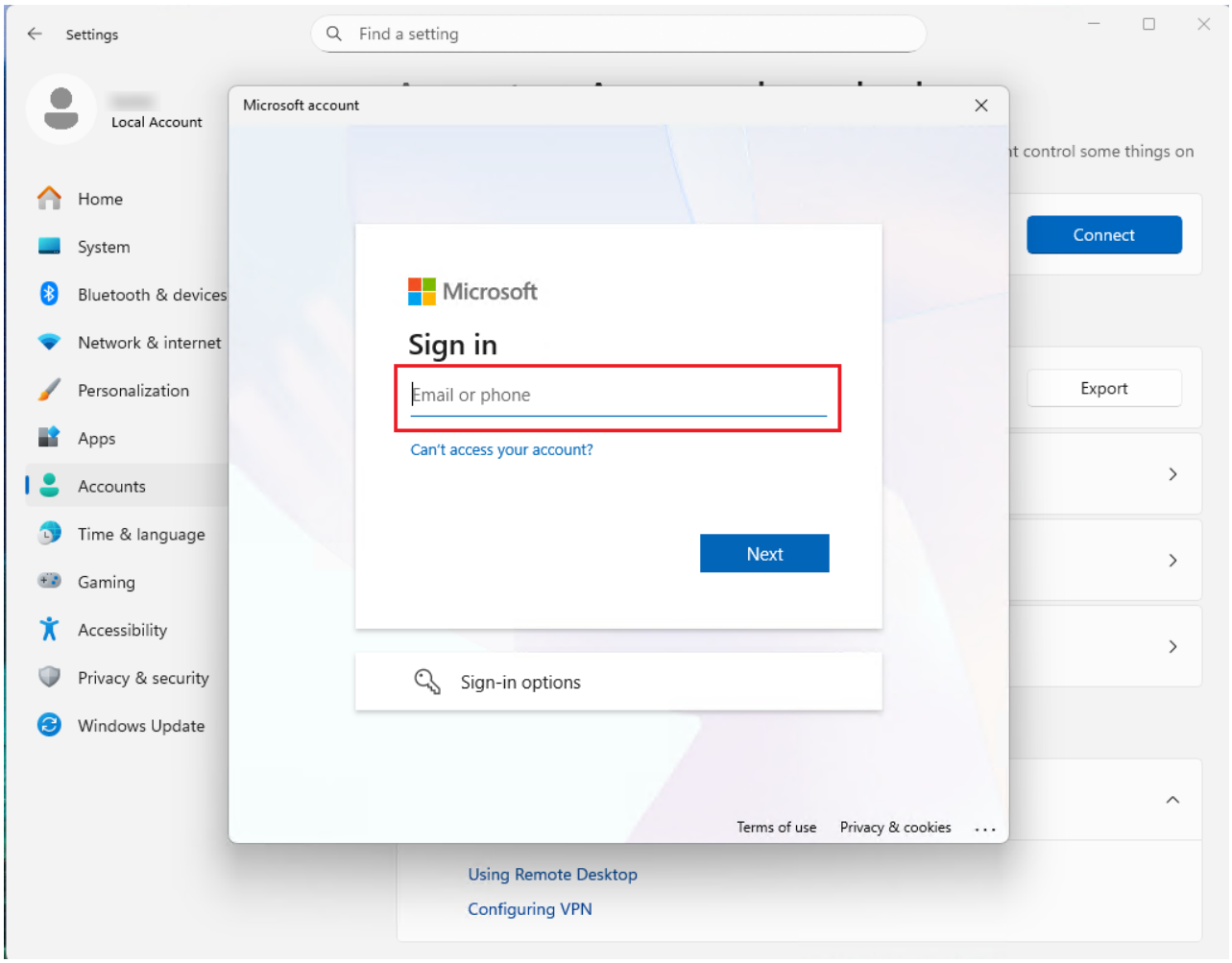
Windows Hello for Business configuration

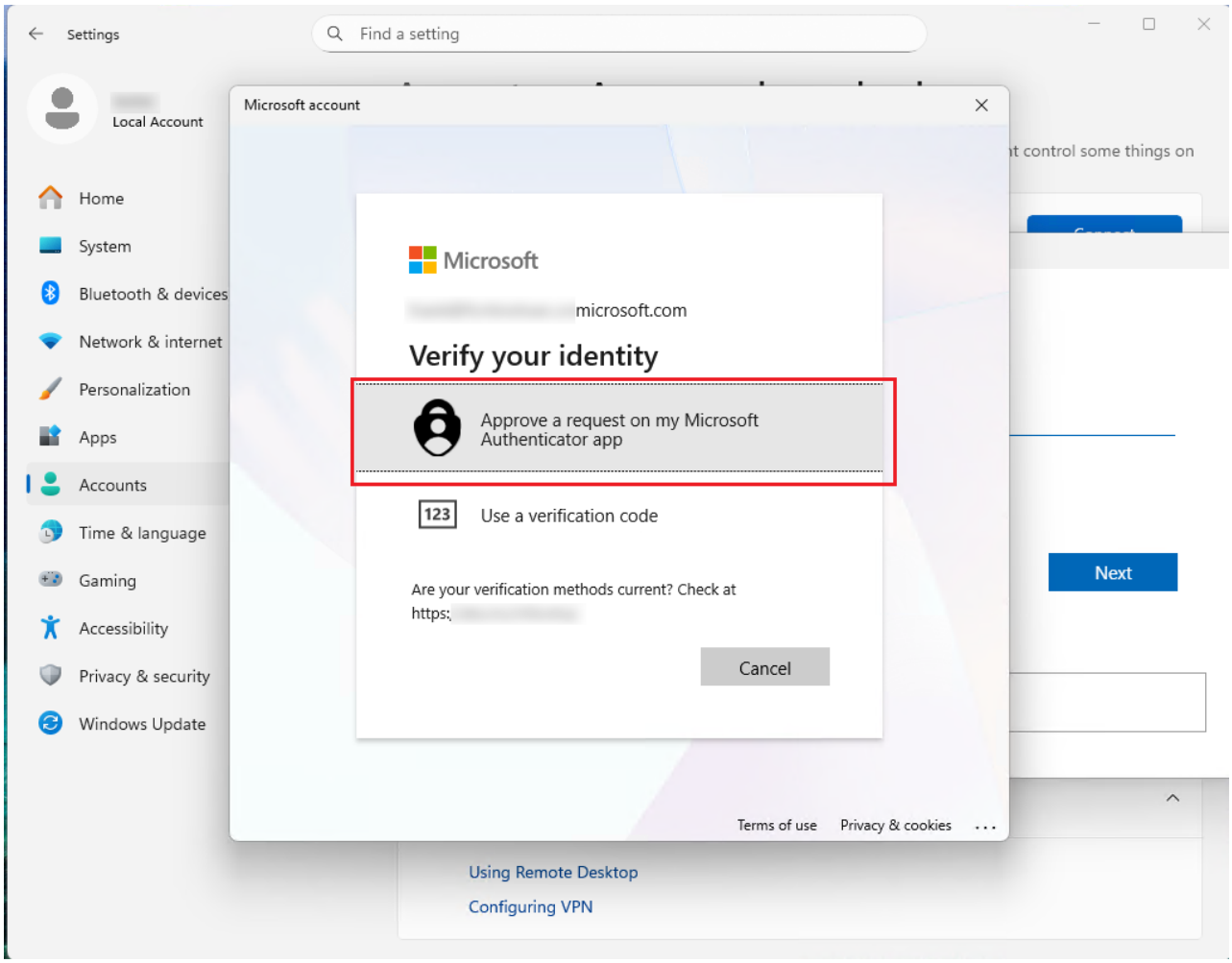
To configure Windows Hello for Business on Entra-joined devices to satisfy MFA claims for SAML SSO VPN authentication:

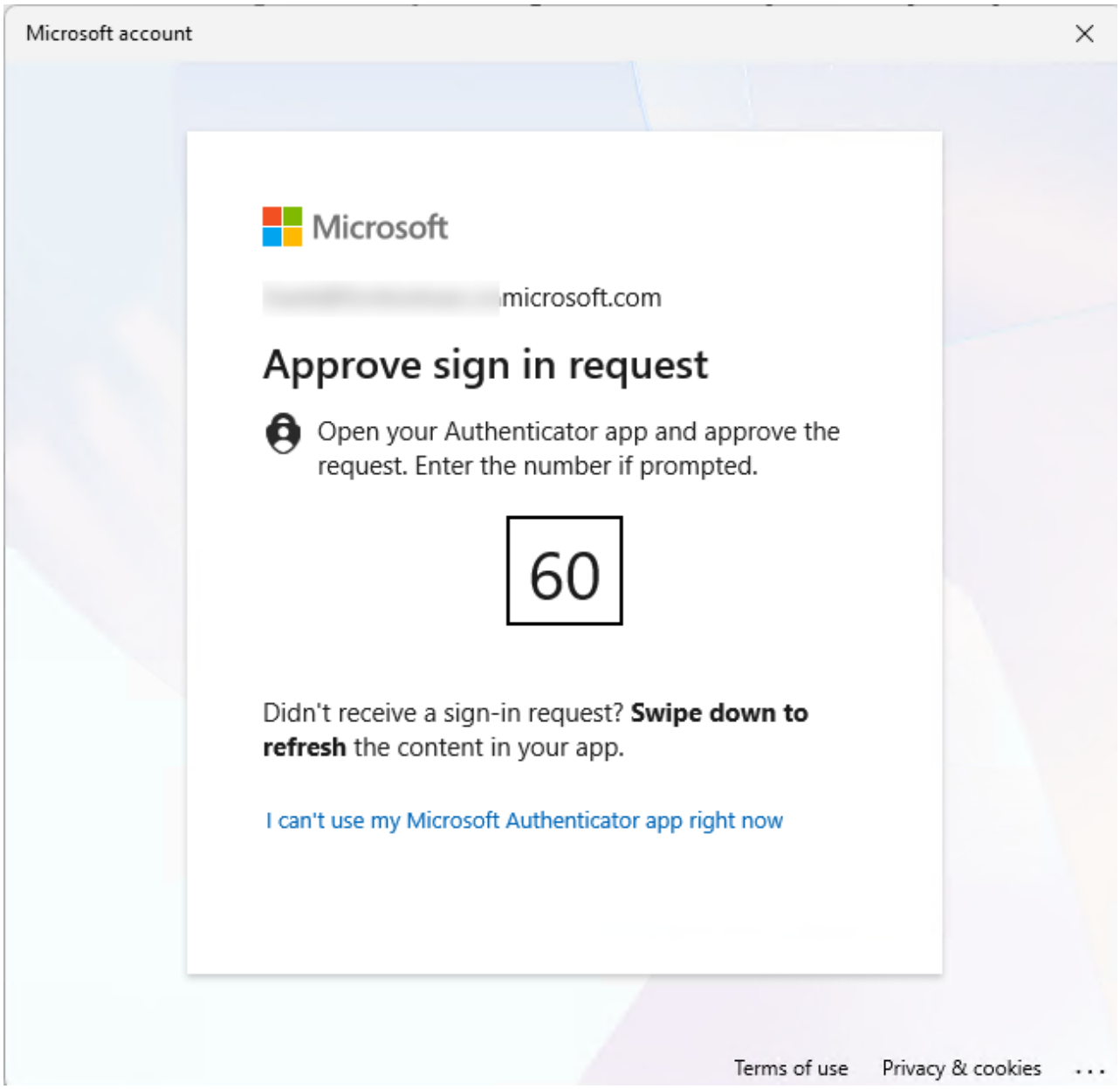
1. Add the device to Entra ID by setting up *Access work or school*:

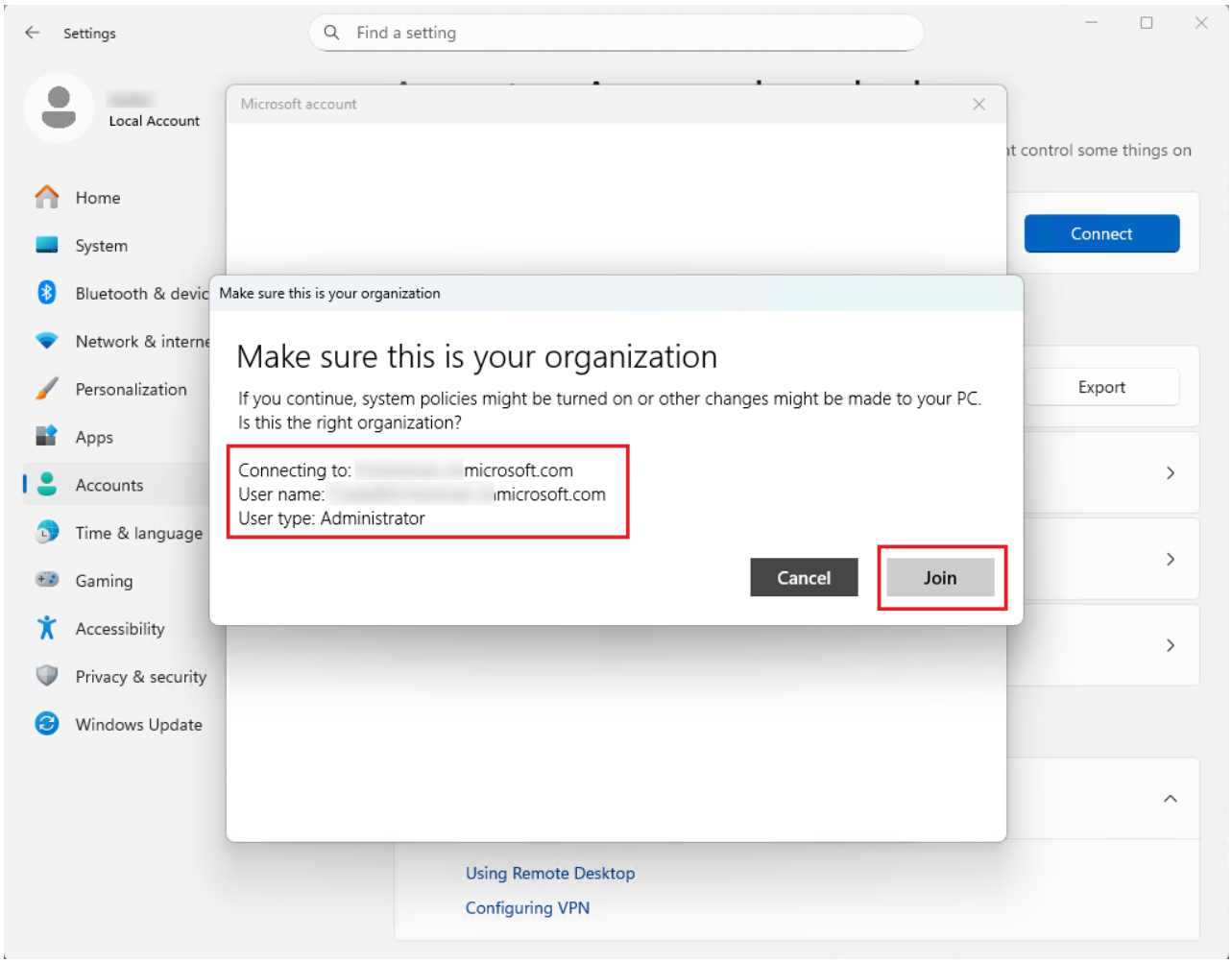


2. Follow the instruction to enter the Entra ID credential and respond the MFA verification by approving Microsoft Authenticator app, which can be installed on the smartphone.

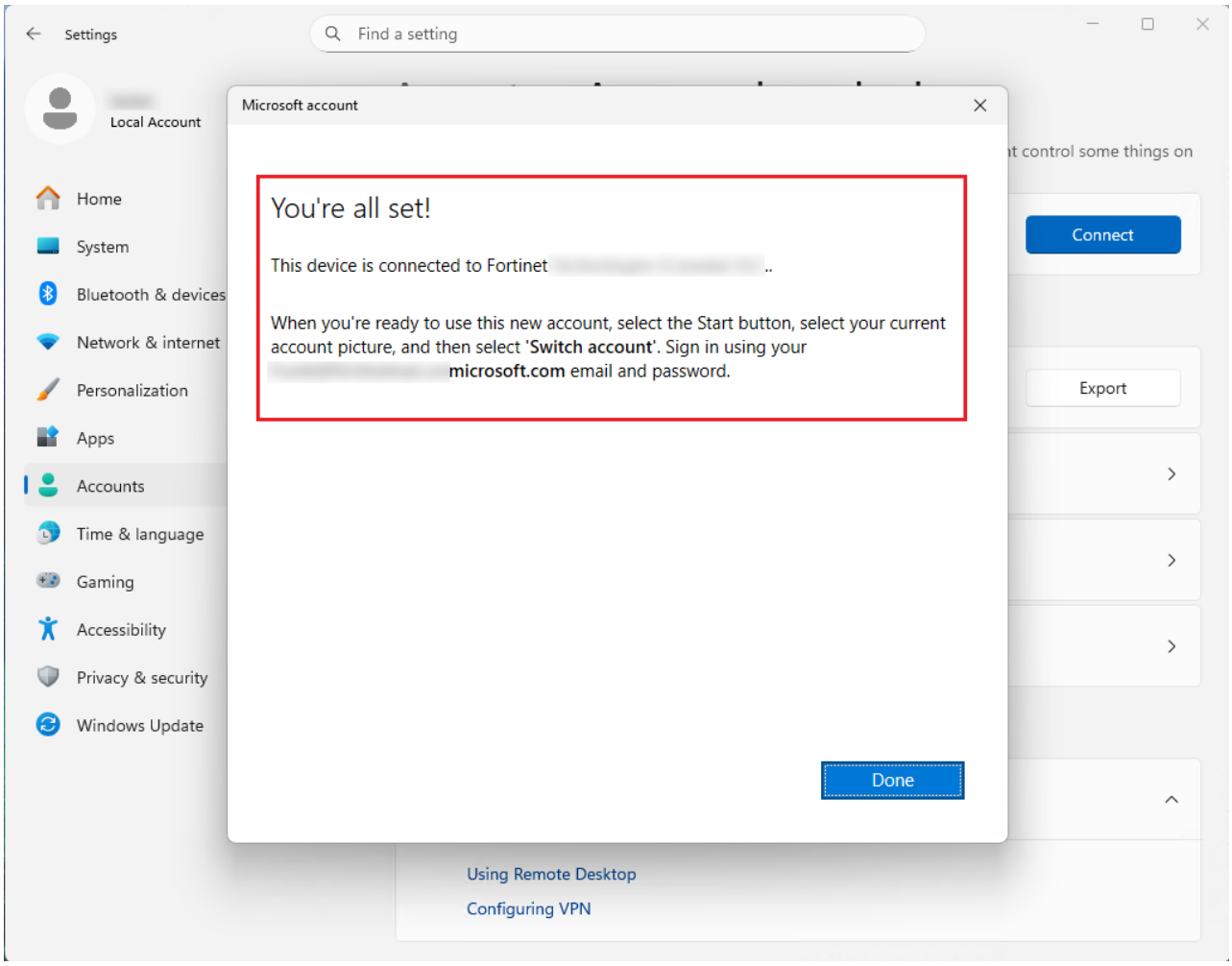

Settings
Find a setting
Local Account
Home
System
Bluetooth & devices
Network & internet
Personalization
Apps
Accounts
Time & language
Gaming
Accessibility
Privacy & security
Windows Update
Microsoft account
Microsoft
Sign in
Email or phone
Can't access your account?
Next
Sign-in options
Terms of use
Privacy & cookies
Connect
Export
Using Remote Desktop
Configuring VPN


Settings
Find a setting
Local Account
Home
System
Bluetooth & devices
Network & internet
Personalization
Apps
Accounts
Time & language
Gaming
Accessibility
Privacy & security
Windows Update
Microsoft account
Microsoft
microsoft.com
Verify your identity
Approve a request on my Microsoft Authenticator app
Use a verification code
Are your verification methods current? Check at https:
Cancel
Terms of use
Privacy & cookies
Next
Using Remote Desktop
Configuring VPN

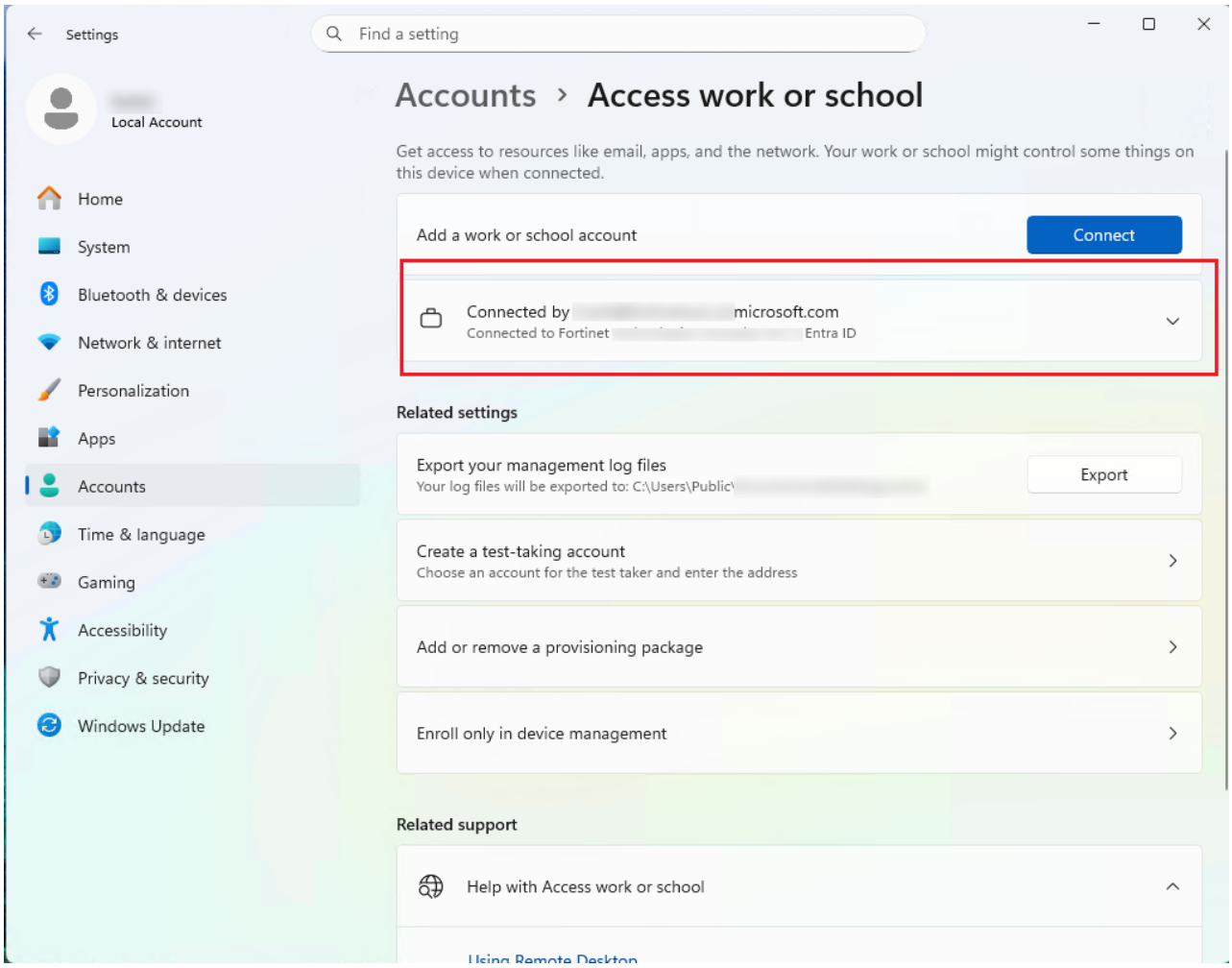

Microsoft account
Microsoft
microsoft.com
Approve sign in request
Open your Authenticator app and approve the request. Enter the number if prompted.
60
Didn't receive a sign-in request? Swipe down to refresh the content in your app.
I can't use my Microsoft Authenticator app right now
Terms of use
Privacy & cookies
...

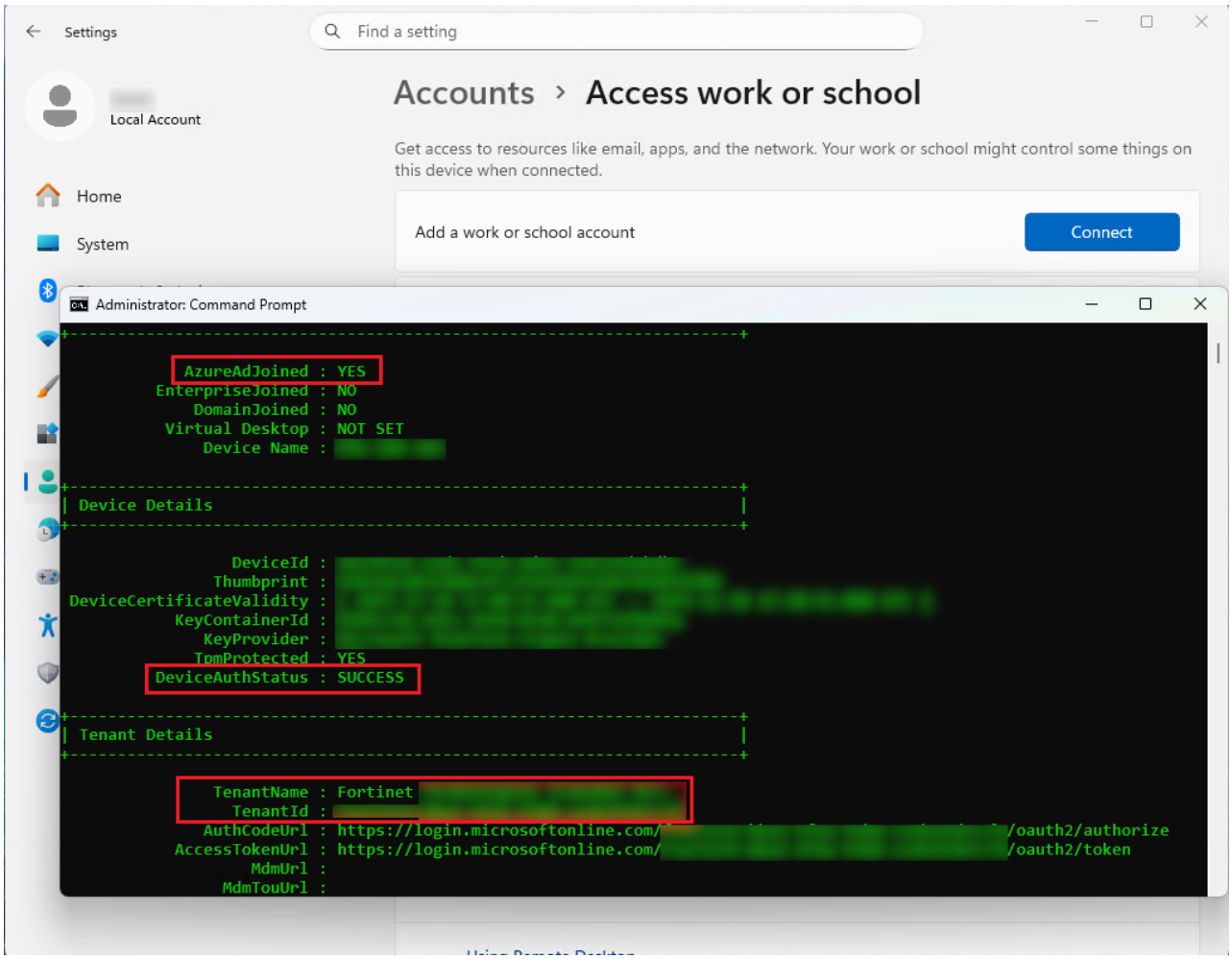


3. Click *Done* in the window that confirms the device is connected to the Entra ID.

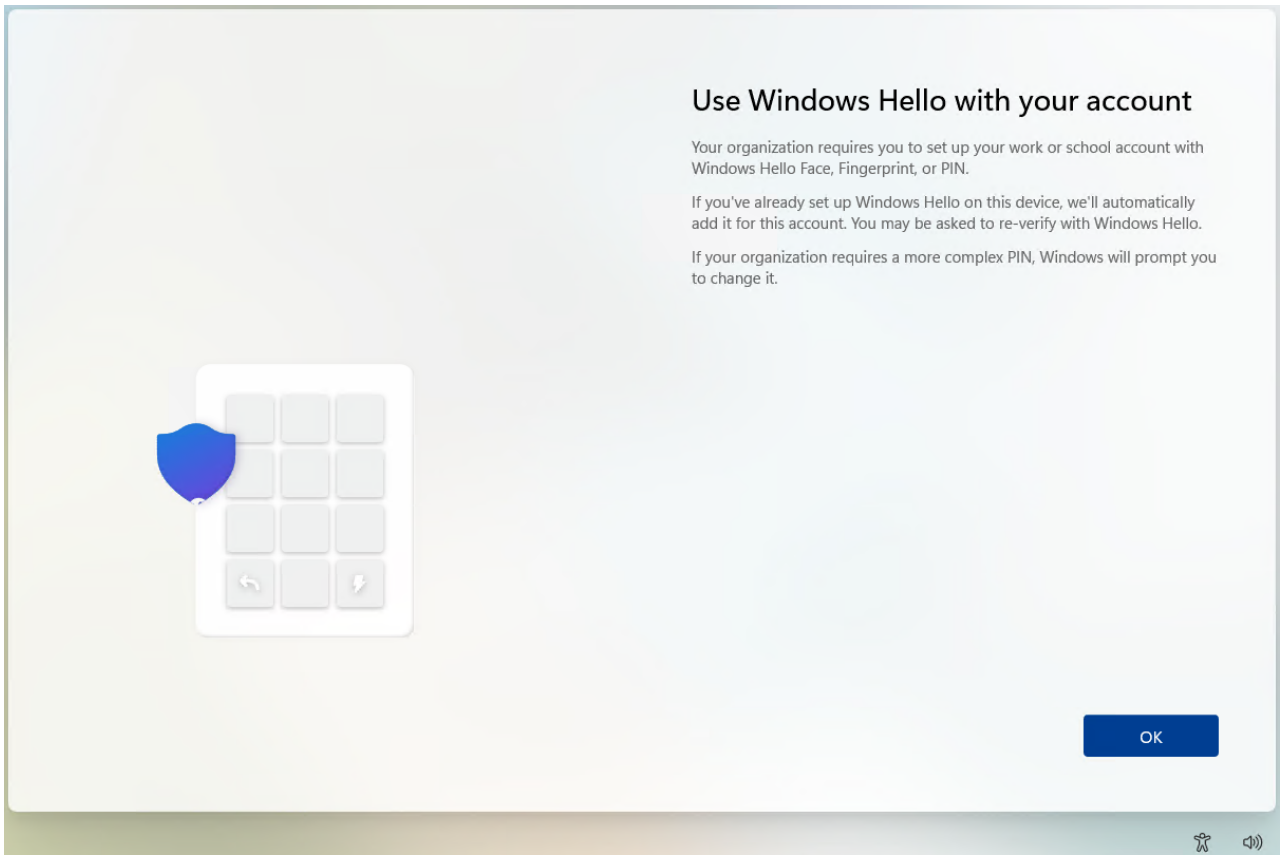


4. Verify that the device has joined the Entra ID.

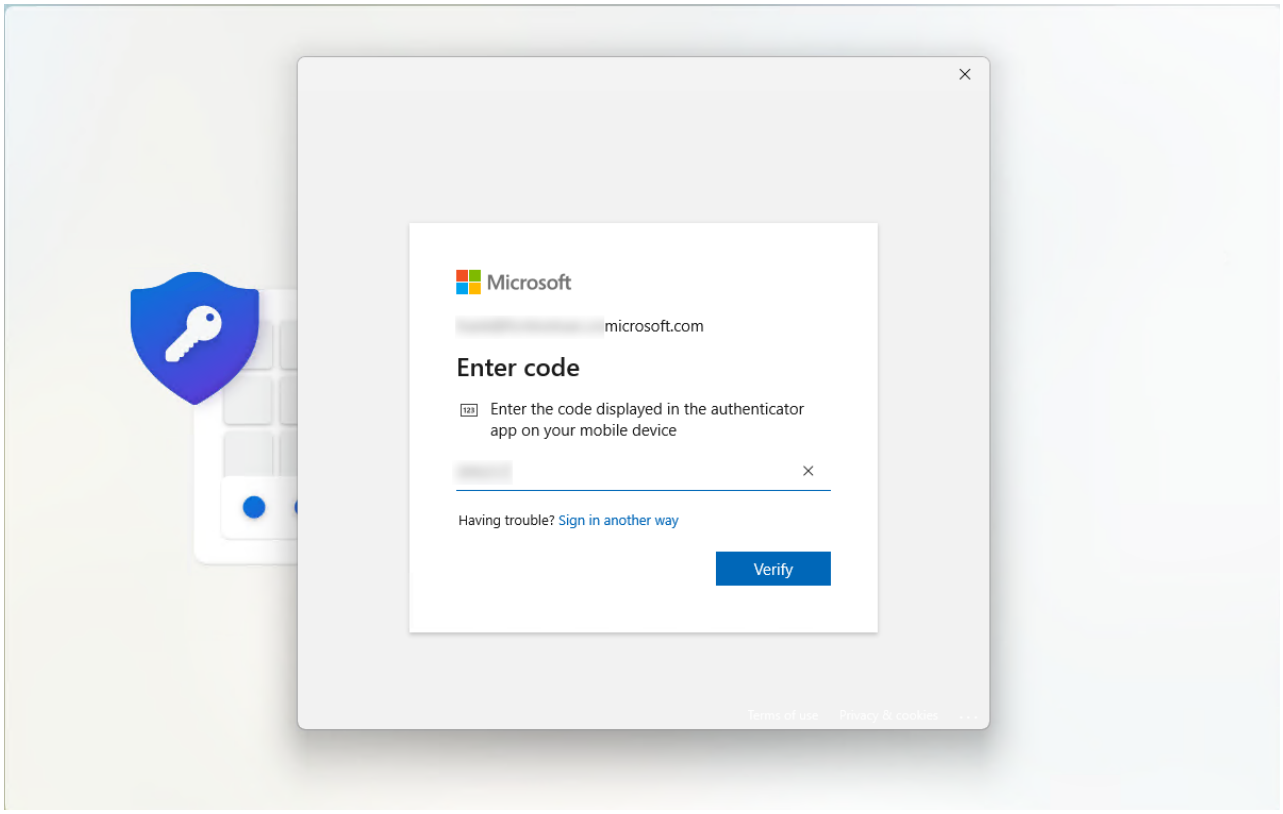

Settings
Find a setting
Local Account
Home
System
Bluetooth & devices
Network & internet
Personalization
Apps
Accounts
Time & language
Gaming
Accessibility
Privacy & security
Windows Update
Accounts › Access work or school
Get access to resources like email, apps, and the network. Your work or school might control some things on this device when connected.
Add a work or school account
Connect
Connected by microsoft.com
Connected to Fortinet Entra ID
Related settings
Export your management log files
Your log files will be exported to: C:\Users\Public
Export
Create a test-taking account
Choose an account for the test taker and enter the address
Add or remove a provisioning package
Enroll only in device management
Related support
Help with Access work or school



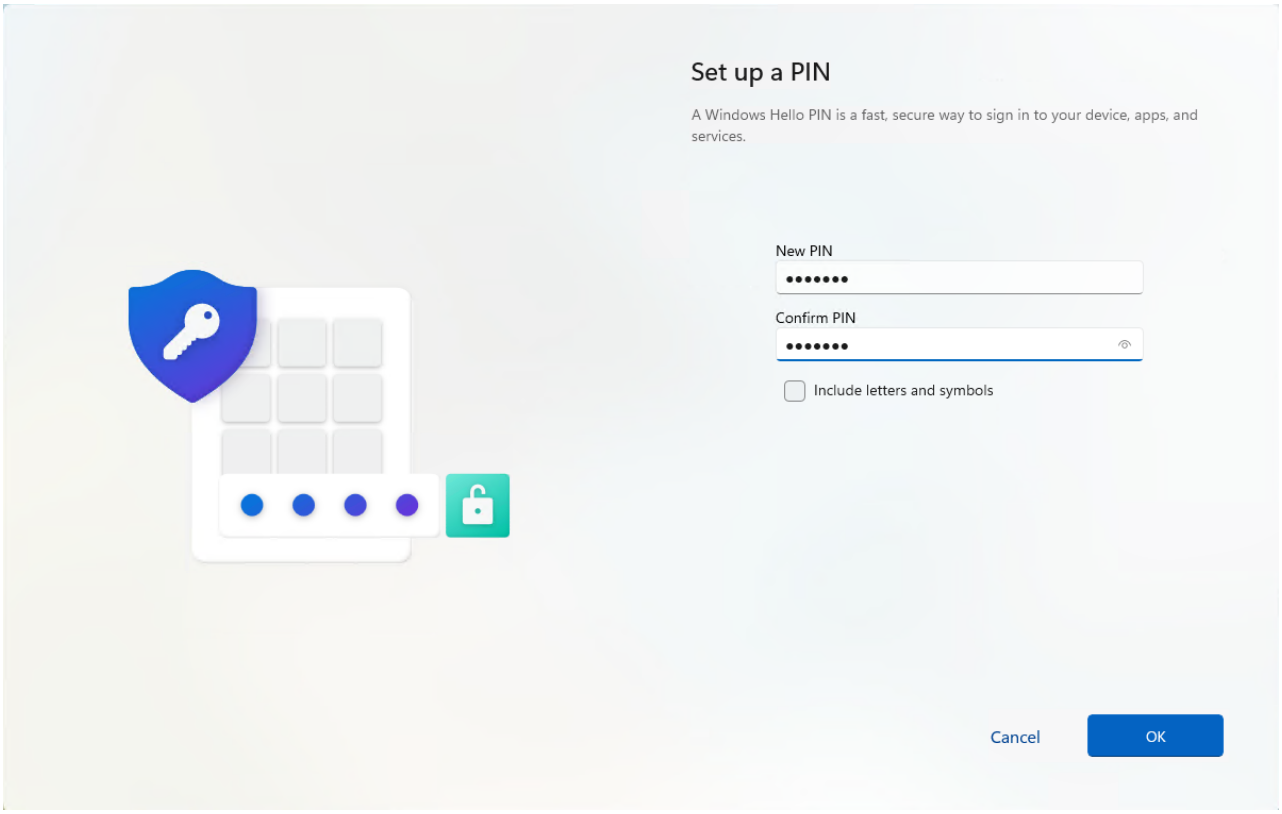
5. Sign in with the Entra ID account on the machine. Windows will automatically prompt to set up WHfB. Click *OK*.

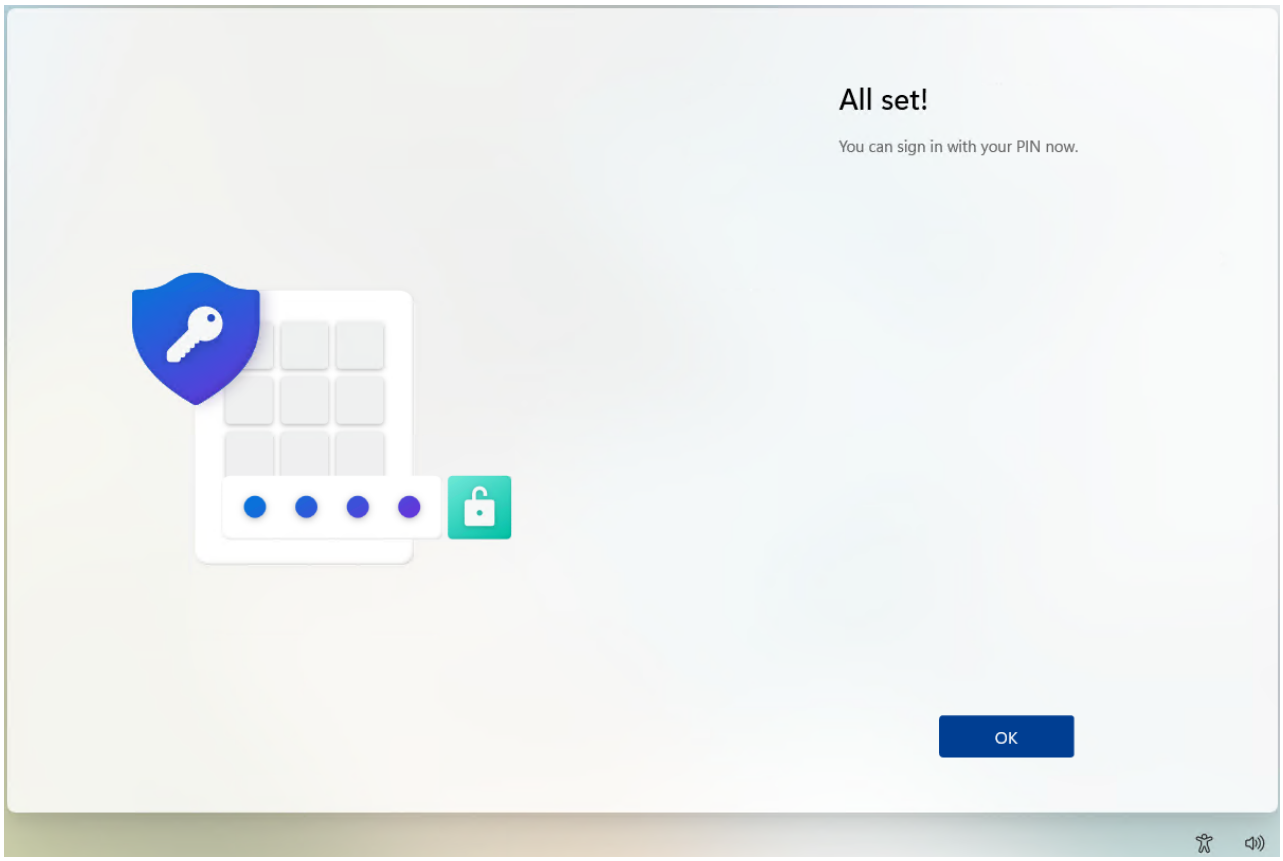


6. Go through the Microsoft Entra MFA setup as required to verify identity.

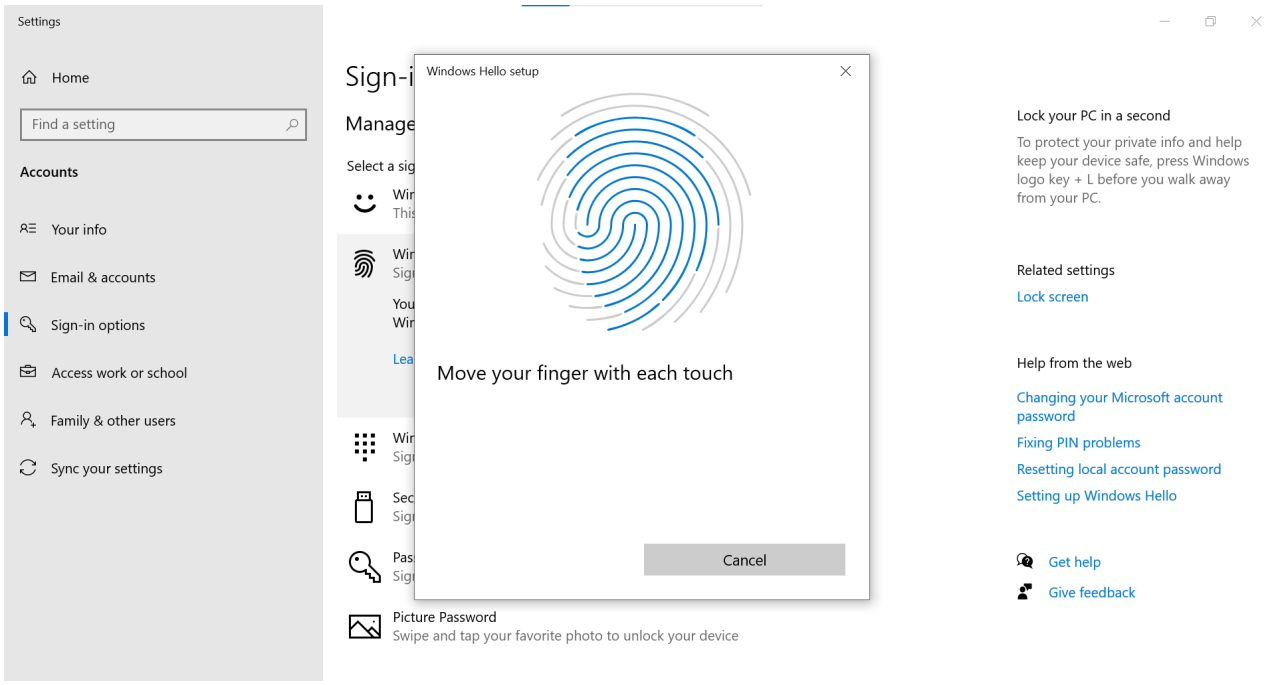


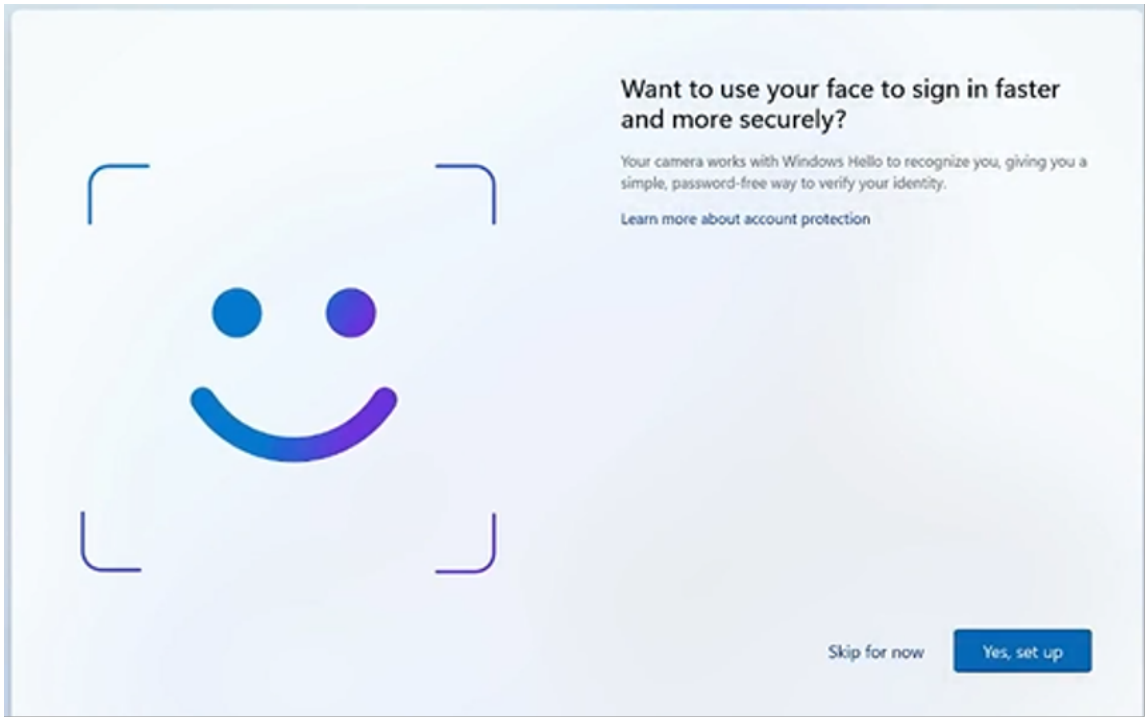
7. Create a PIN as required.





8. Enable biometric sign-in (fingerprint and facial recognition) for Windows Hello for Business.

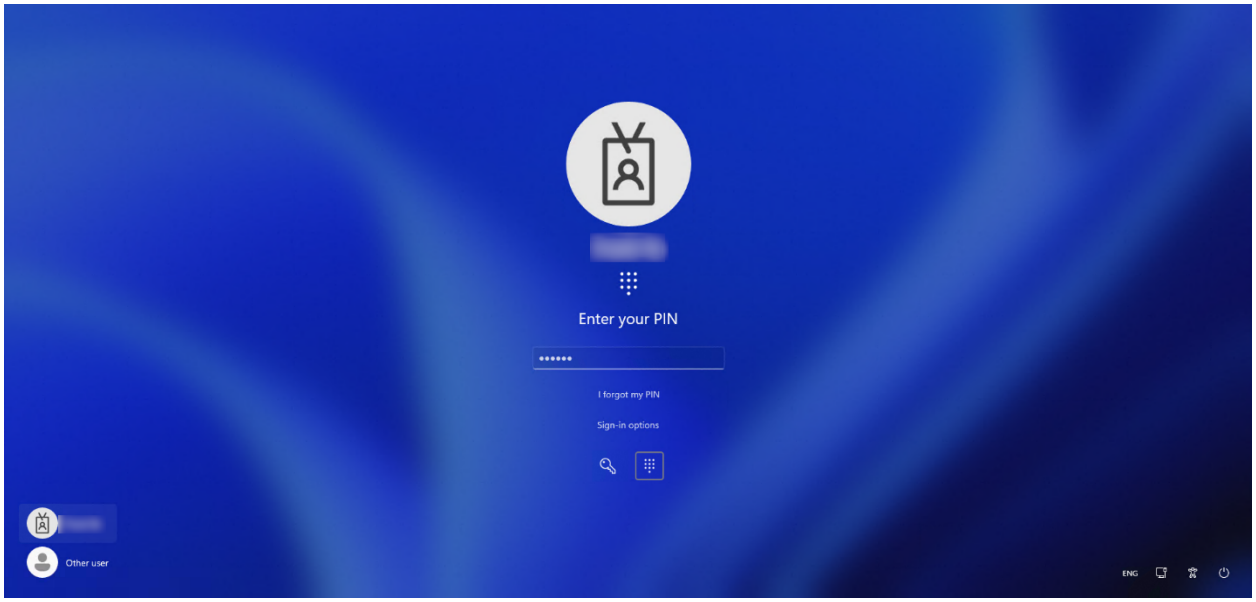


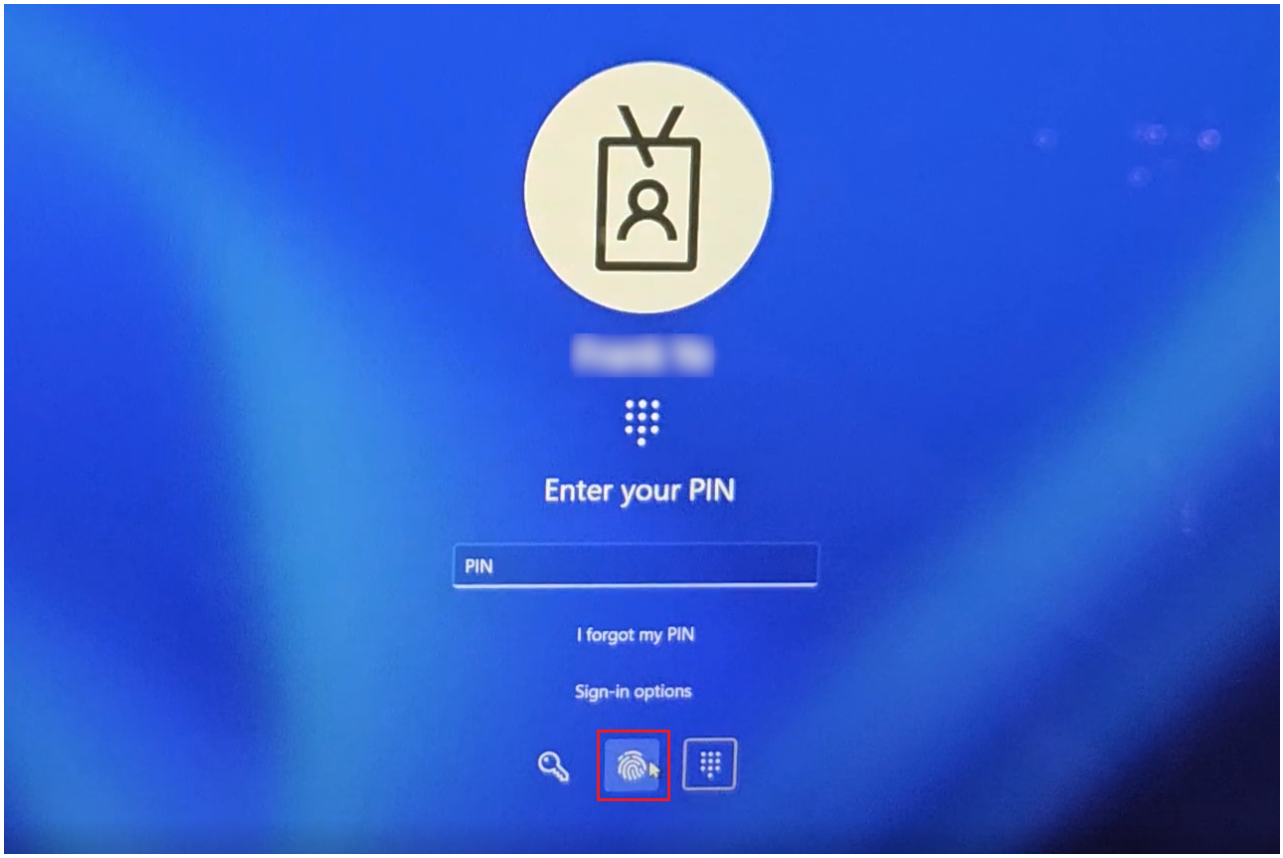


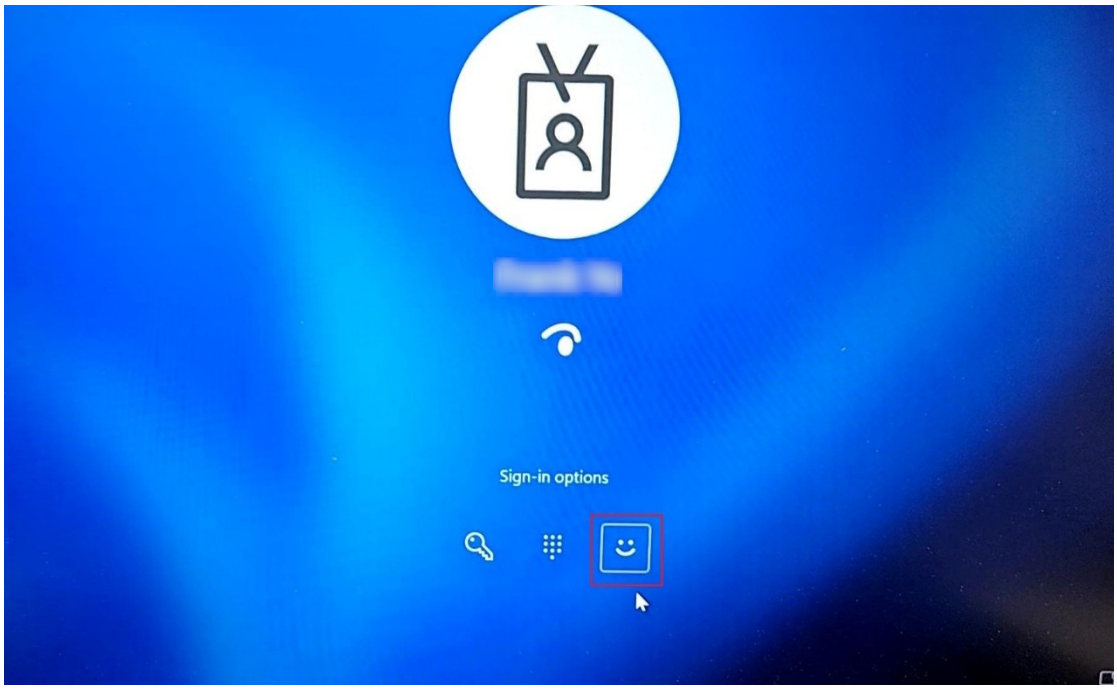
Verification

After Windows Hello for Business (WHfB) is provisioned, verify that the FortiGate SAML-based IPsec VPN auto-connects seamlessly after Windows login via Windows Hello for Business using PIN or biometrics:

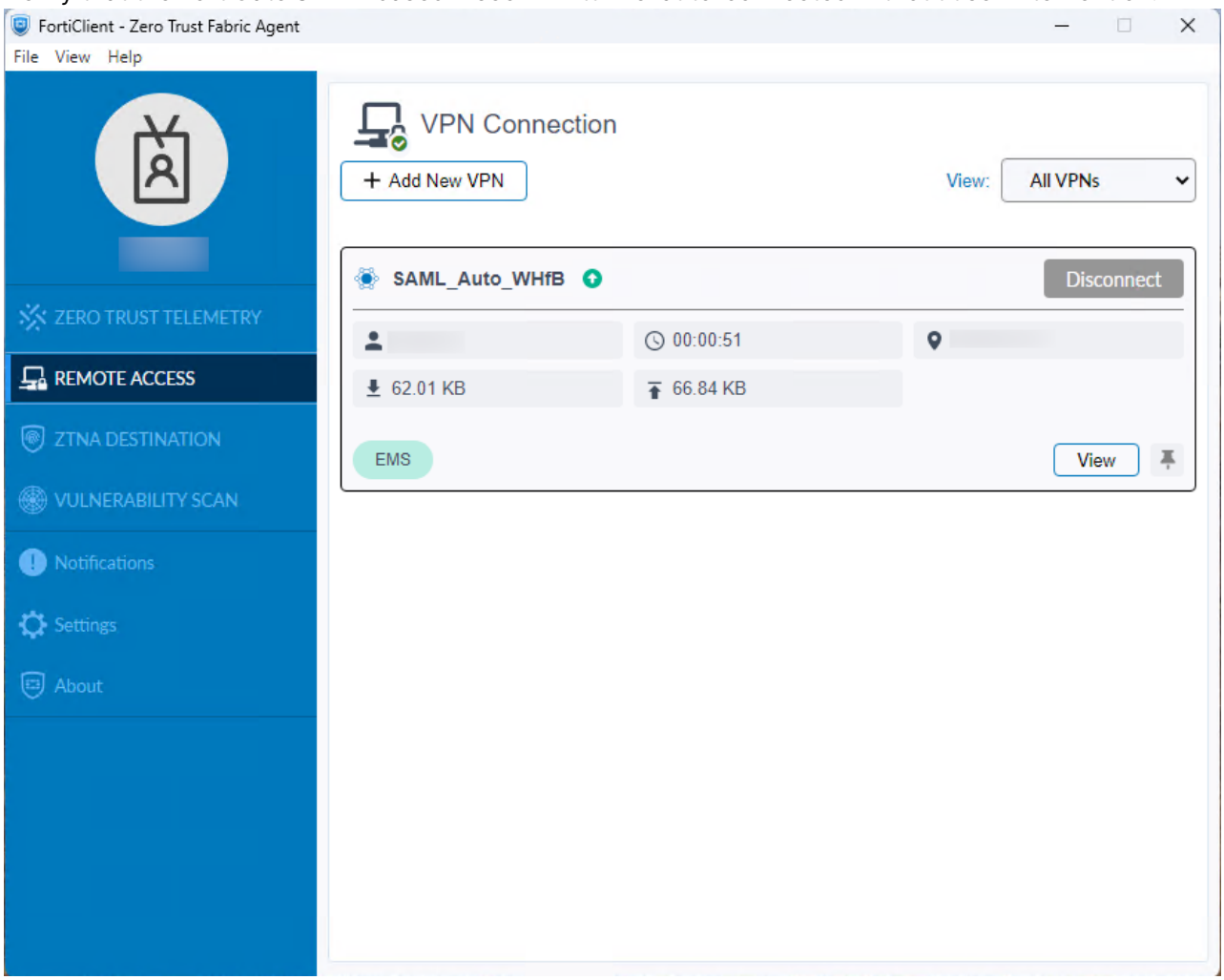
1. Sign-in with PIN or biometrics (fingerprint or facial recognition):






Sign-in options

2. Verify that the FortiGate SAML-based IPsec VPN tunnel auto-connected without user intervention.



IPsec VPN support for traffic going through FortiADC

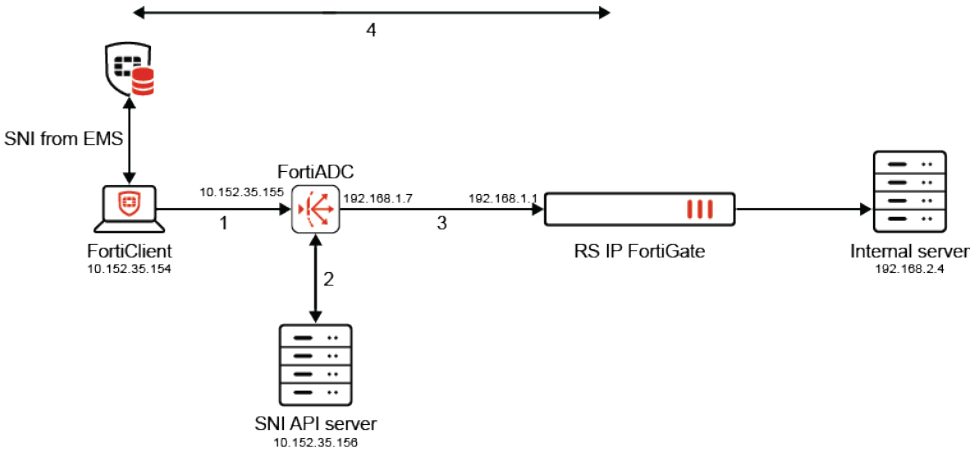
IPsec VPN can support traffic that first goes through FortiADC. Only IKEv2 tunnels support this feature.

The example uses the following product versions:

Product	Version
FortiClient	7.2.4
FortiClient EMS	
FortiGate	7.4.3
FortiADC	6.1.3

In this example use case, an organization has implemented a comprehensive security strategy that includes the use of IPsec (Internet Protocol Security) for securing communications between its network resources. By combining the secure communication that IPsec provides with the traffic optimization capabilities of

FortiADC, the company can achieve a robust, secure, and high-performance network infrastructure for interconnecting branch offices with the central data center. Also, this setup enables efficient data exchange while maintaining the confidentiality and integrity of the transmitted information.



The following illustrates the flow in the diagram:

1. FortiClient sends a request to IKE port 4500 with the SNI information from EMS.
2. FortiADC sends the SNI to the API server and receives the real server (RS) IP address.
3. FortiADC sends a packet to the RS IP address:port and response.
4. VPN is setup and an IKE UDP 4500 packet is sent automatically.

The following assumes that you already have an SNI API server configured with Go service running on port 3001.

To configure FortiADC:

1. Configure a load balance profile for IKE traffic:

```
config load-balance profile
  edit "IKERESOURCE"
    set type udp
    set inner-protocol ike
  next
end
```

2. Configure the SNI API server. In this example, 10.152.35.156 is the SNI API server IP address, and 3001 is the port used:

```
config load-balance sniproxy-domain
  set url http://10.152.35.156:3001/api/v1/system/sni-resolvers?region=region1
  set url-udp http://10.152.35.156:3001/api/v1/system/sni-resolvers?region=region1
end
```

3. Configure the RS pool and add members (the FortiOS firewall IP address) to the pool:

```
config load-balance pool
  edit "FGT-POOL"
    set health-check-list LB_HLTHCK_ICMP LB_HLTHCK_HTTPS LB_HLTHCK_TCP_ECHO LB_HLTHCK_HTTP
```

```
    set real-server-ssl-profile NONE
    config  pool_member
      edit 1
        set pool_member_service_port 0
        set pool_member_cookie rs1
        set real-server FGT2
      next
    end
  next
end
```

4. Configure a virtual server. FortiClient will initiate an IPsec connection to 192.168.1.7, the remote gateway and FortiADC interface IP address, on port 4500:

```
config load-balance virtual-server
  edit "INTERNALIPSEC"
    set interface port1
    set ip 192.168.1.7
    set port 4500
    set load-balance-profile IKERESOURCE
    set load-balance-method LB_METHOD_SNIPROXY
    set load-balance-pool FGT-POOL
    set traffic-log enable
    set traffic-group default
    set fortiview enable
  next
end
```

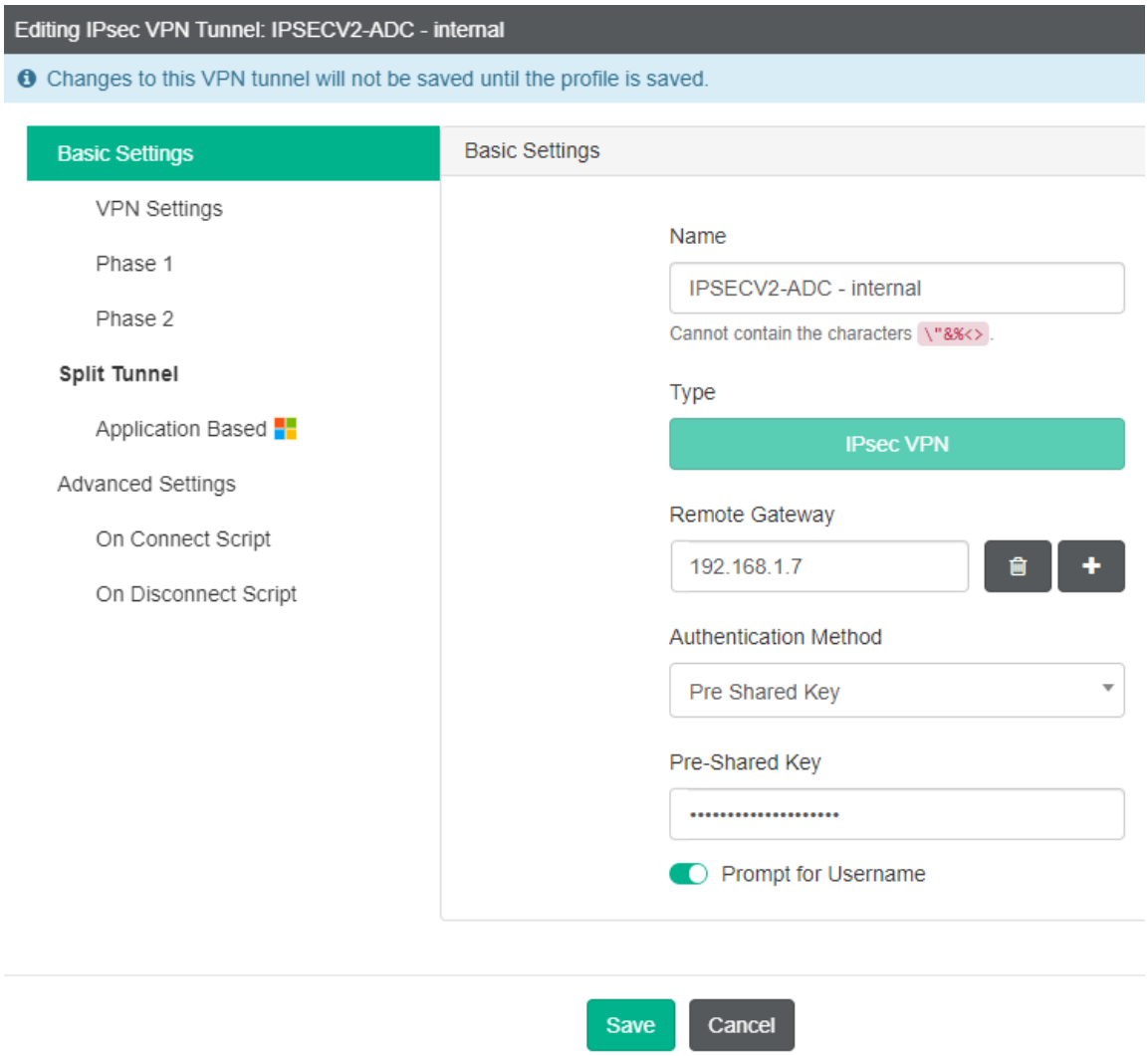
To create an IPsec VPN IKEv2 tunnel in FortiOS:

```
config vpn ipsec phase1-interface
    edit "ADC Tunnel"
        set type dynamic
        set interface "port2"
        set ike-version 2
        set peertype any
        set net-device disable
        set mode-cfg enable
        set proposal aes128-sha256 aes256-sha256 aes128gcm-prfsha256 aes256gcm-prfsha384
chacha20poly1305-prfsha256
        set comments "VPN: ADC Tunnel (Created by VPN wizard)"
        set eap enable
        set eap-identity send-request
        set authusrgrp "IPSEC"
        set ipv4-start-ip 20.21.21.1
        set ipv4-end-ip 20.21.21.250
        set dns-mode auto
        set save-password enable
        set client-auto-negotiate enable
        set client-keep-alive enable
        set psksecret ENC
```

```
FzFV1gODmlxtAzxGdBQgxyAs7EvbfThS6hbrqFrBWgAQ3LAaxZ8i7V2XsjFSOJ0D5xp/cWODWxPyUBxL/j5ItiT/DG9Hl6l28u
A7gMeAzagGs+avmaauE4vu3/TX+wTQ2cAD19zpiBu7I33l0EMM8hnmKTgwG3stznB/A4oKfEG72nQvrxk4TyXMRmjKdoQIvOz2
SA==
    next
end
```

To configure EMS:

1. In EMS, go to *Endpoint Profiles* > *Remote Access*.
2. Create a new profile or edit an existing one.
3. Under *VPN Tunnels*, click *Add Tunnel*.
4. Select *Manual*.
5. Configure *Basic Settings*:
   a. In the *Name* field, configure the desired tunnel name.
   b. For *Type*, select *IPsec VPN*.
   c. In the *Remote Gateway* field, enter the remote gateway, which is the same as the FortiADC IP address. In this example it is 192.168.1.7
   d. From the *Authentication Method* dropdown list, select *Pre Shared Key*.
   e. In the *Pre-Shared Key* field, enter the same key that you configured in FortiOS.



6. Configure other fields as desired, and save.
7. Click *XML*, then *Edit*.
8. Under `<ike_settings>`, set `<sase_mode>` to 1. This sets the IPsec port to 4500. The following shows the XML configuration:

```
<forticlient_configuration>
    <vpn>
        <enabled>1</enabled>
        <sslvpn>
            <connections/>
            <options>
                <disallow_invalid_server_certificate>0</disallow_invalid_server_certificate>
                <use_gui_saml_auth>0</use_gui_saml_auth>
                <no_dns_registration>0</no_dns_registration>
                <preferred_dtls_tunnel>0</preferred_dtls_tunnel>
                <negative_split_tunnel_metric/>
                <warn_invalid_server_certificate>1</warn_invalid_server_certificate>
                <dnscache_service_control>0</dnscache_service_control>
```

```
            <prefer_sslvpn_dns>1</prefer_sslvpn_dns>
            <enabled>1</enabled>
        </options>
    </sslvpn>
    <ipsecvpn>
        <connections>
            <connection>
                <name>IPSECV2-ADC - internal</name>
                <uid>650F4D40-6942-4E25-B927-7EE6C5D99878</uid>
                <machine>0</machine>
                <keep_running>0</keep_running>
                <disclaimer_msg/>
                <sso_enabled>0</sso_enabled>
                <single_user_mode>0</single_user_mode>
                <type>manual</type>
                <ui>
                    <show_remember_password>1</show_remember_password>
                    <show_alwaysup>1</show_alwaysup>
                    <show_autoconnect>1</show_autoconnect>
                    <show_passcode>0</show_passcode>
                    <save_username>0</save_username>
                </ui>
                <redundant_sort_method>0</redundant_sort_method>
                <tags>
                    <allowed/>
                    <prohibited/>
                </tags>
                <host_check_fail_warning/>
                <ike_settings>
                    <server>192.168.1.7</server>
                    <authentication_method>Preshared Key</authentication_method>
                    <fgt>1</fgt>
                    <prompt_certificate>1</prompt_certificate>
                    <xauth>
                        <use_otp>0</use_otp>
                        <enabled>1</enabled>
                        <prompt_username>1</prompt_username>
                    </xauth>
                    <version>2</version>
                    <mode>aggressive</mode>
                    <key_life>86400</key_life>
                    <localid/>
                    <implied_SPDO>0</implied_SPDO>
                    <implied_SPDO_timeout>0</implied_SPDO_timeout>
                    <nat_traversal>1</nat_traversal>
                    <sase_mode>1</sase_mode>
                    <nat_alive_freq>5</nat_alive_freq>
                    <enable_local_lan>1</enable_local_lan>
                    <enable_ike_fragmentation>0</enable_ike_fragmentation>
                    <mode_config>1</mode_config>
                    <dpd>1</dpd>
```

```
                        <run_fcauth_system>0</run_fcauth_system>
                        <sso_enabled>0</sso_enabled>
                        <ike_saml_port>443</ike_saml_port>
                        <dpd_retry_count>3</dpd_retry_count>
                        <dpd_retry_interval>5</dpd_retry_interval>
                        <xauth_timeout>120</xauth_timeout>
                        <auth_data>
                            <preshared_key>Enc
7de9d08db7716deba8e66e5526eac5d952c1afb46e2edd5d51646228a1a2</preshared_key>
                        </auth_data>
                        <dhgroup>5</dhgroup>
                        <proposals>
                            <proposal>AES128|SHA1</proposal>
                            <proposal>AES256|SHA256</proposal>
                        </proposals>
                    </ike_settings>
                    <ipsec_settings>
                        <remote_networks>
                            <network>
                                <addr>0.0.0.0</addr>
                                <mask>0.0.0.0</mask>
                            </network>
                            <network>
                                <addr>::/0</addr>
                                <mask>::/0</mask>
                            </network>
                        </remote_networks>
                        <dhgroup>5</dhgroup>
                        <key_life_type>seconds</key_life_type>
                        <key_life_seconds>43200</key_life_seconds>
                        <key_life_Kbytes>5200</key_life_Kbytes>
                        <replay_detection>1</replay_detection>
                        <pfs>1</pfs>
                        <use_vip>1</use_vip>
                        <virtualip>
                            <type>modeconfig</type>
                            <ip>0.0.0.0</ip>
                            <mask>0.0.0.0</mask>
                            <dnsserver>0.0.0.0</dnsserver>
                            <winserver>0.0.0.0</winserver>
                        </virtualip>
                        <proposals>
                            <proposal>AES128|SHA1</proposal>
                            <proposal>AES256|SHA256</proposal>
                        </proposals>
                    </ipsec_settings>
                    <android_cert_path/>
                    <warn_invalid_server_certificate>1</warn_invalid_server_certificate>
                    <on_connect>
                        <script>
                            <os>windows</os>
```

```
                        <script/>
                    </script>
                    <script>
                        <os>MacOSX</os>
                        <script/>
                    </script>
                    <script>
                        <os>linux</os>
                        <script/>
                    </script>
                </on_connect>
                <on_disconnect>
                    <script>
                        <os>windows</os>
                        <script/>
                    </script>
                    <script>
                        <os>MacOSX</os>
                        <script/>
                    </script>
                    <script>
                        <os>linux</os>
                        <script/>
                    </script>
                </on_disconnect>
                <traffic_control>
                    <enabled>0</enabled>
                    <mode>1</mode>
                </traffic_control>
            </connection>
        </connections>
        <options>
            <usewincert>1</usewincert>
            <disallow_invalid_server_certificate>0</disallow_invalid_server_certificate>
            <uselocalcert>0</uselocalcert>
            <beep_if_error>0</beep_if_error>
            <check_for_cert_private_key>0</check_for_cert_private_key>
            <no_dns_registration>0</no_dns_registration>
            <enhanced_key_usage_mandatory>0</enhanced_key_usage_mandatory>
            <disable_default_route>0</disable_default_route>
            <use_win_current_user_cert>1</use_win_current_user_cert>
            <enable_udp_checksum>0</enable_udp_checksum>
            <show_auth_cert_only>0</show_auth_cert_only>
            <usesmcardcert>1</usesmcardcert>
            <block_ipv6>1</block_ipv6>
            <use_win_local_computer_cert>1</use_win_local_computer_cert>
            <enabled>1</enabled>
        </options>
    </ipsecvpn>
    <lockdown>
        <grace_period>120</grace_period>
```

```
            <max_attempts>3</max_attempts>
            <exceptions>
                <apps/>
                <ips/>
            </exceptions>
            <enabled>0</enabled>
        </lockdown>
        <options>
            <suppress_vpn_notification>0</suppress_vpn_notification>
            <secure_remote_access>0</secure_remote_access>
            <keep_running_max_tries>0</keep_running_max_tries>
            <use_windows_credentials>0</use_windows_credentials>
            <allow_personal_vpns>1</allow_personal_vpns>
            <show_vpn_before_logon>0</show_vpn_before_logon>
            <use_legacy_vpn_before_logon>0</use_legacy_vpn_before_logon>
            <on_os_start_connect/>
            <disable_connect_disconnect>0</disable_connect_disconnect>
            <show_negotiation_wnd>0</show_negotiation_wnd>
            <on_os_start_connect_has_priority>0</on_os_start_connect_has_priority>
            <autoconnect_on_install>0</autoconnect_on_install>
            <autoconnect_only_when_offnet>0</autoconnect_only_when_offnet>
            <minimize_window_on_connect>1</minimize_window_on_connect>
        </options>
    </vpn>
    <endpoint_control>
        <ui>
            <display_vpn>1</display_vpn>
        </ui>
    </endpoint_control>
</forticlient_configuration>
```

9. Save. After FortiClient receives the profile changes from EMS, it can connect to an IPsec VPN tunnel pushed from FortiADC.

To verify this configuration:

1. In FortiOS, go to *Dashboard* > *Network*.
2. Expand the IPsec widget.
3. Verify that the IPsec VPN tunnel is up.
4. If desired, you can enable and view FortiOS:

```
FGVMULTM12345 # diagnose debug enable

FGVMULTM212345 # diagnose debug application ike -1
Debug messages will be on for 30 minutes.

FGVMULTM12345 # ike V=root:0: comes 192.168.1.11:4500-
>192.168.1.1:4500,ifindex=5,vrf=0,len=508....
ike V=root:0: IKEv2 exchange=SA_INIT id=fd23616068ea787b/0000000000000000 len=504
ike 0: in
```

```
FD23616068EA787B0000000000000000021202208000000000000001F82200005C0200002C0101000403000000C010000
0C800E00800300000802000002030000080300000200000008040000050000002C020100040300000C0100000C800E
00800300000802000005030000080300000C000000080400000528000C80005000002985CB0E49090C90FF1B01C95
C5CBE283C13C57C98C796D1AB5301AB30E5D5BD3C3B438A41F95CFDD8C2FC1086DCD18F6B3A6EAAF8AF9E54022F8FA
0B4FC16BAAF42AA3F4DDB5CC2846F09CD0CDA74B513851EAB6F9A8EAB128B0DB8D5B4F819EA4C775B037A77BD35813
230C0708077C34EB02BD3F8A71613B84365F5FCE93528C2C54FF72ADA276E7C4B37DF6C6A9AAAE2CA0370957B43853
45ED403118D6A0D68A49834069CC7543F0597AD83FA75FE90967A40A31F3F8CE28ABFBDE25822B000014BDDC4BD20A
F71BA16FFE6AA24508B0162B0000144C53427B6D465D1B337BB755A37A7FEF2B000014B4F01CA951E9DA8D0BAFBBD3
4AD3044E29000014C1DC4350476B98A429B91781914CA43E290000180100F103464354454D53383832343039303331
35290000180100F103464354454D533838323430393033313529000001C0000400408C1FCB91852BE008BC80B00D5AD
2667C42A04940000001C000040053DDAE5A62679ABFBD748AFCB830BBB25F2195192
Ike V=root:0:fd23616068ea787b/0000000000000000:897: responder received SA_INIT msg
ike V=root:0:fd23616068ea787b/0000000000000000:897: VID forticlient connect license
4C53427B6D465D1B337BB755A37A7FEF
ike V=root:0:fd23616068ea787b/0000000000000000:897: VID Fortinet Endpoint Control
B4F01CA951E9DA8D0BAFBBD34AD3044E
ike V=root:0:fd23616068ea787b/0000000000000000:897: VID unknown (16):
C1DC4350476B98A429B91781914CA43E
ike V=root:0:fd23616068ea787b/0000000000000000:897: received notify type 61699
ike V=root:0:fd23616068ea787b/0000000000000000:897: ignoring unauthenticated notify payload
(61699)
ike V=root:0:fd23616068ea787b/0000000000000000:897: received notify type 61699
ike V=root:0:fd23616068ea787b/0000000000000000:897: ignoring unauthenticated notify payload
(61699)
ike V=root:0:fd23616068ea787b/0000000000000000:897: received notify type NAT_DETECTION_SOURCE_
IP
ike V=root:0:fd23616068ea787b/0000000000000000:897: received notify type NAT_DETECTION_
DESTINATION_IP
ike V=root:0:fd23616068ea787b/0000000000000000:897: incoming proposal:
ike V=root:0:fd23616068ea787b/0000000000000000:897: proposal id = 1:
ike V=root:0:fd23616068ea787b/0000000000000000:897:   protocol = IKEv2:
ike V=root:0:fd23616068ea787b/0000000000000000:897:      encapsulation = IKEv2/none
ike V=root:0:fd23616068ea787b/0000000000000000:897:         type=ENCR, val=AES_CBC (key_len =
128)
ike V=root:0:fd23616068ea787b/0000000000000000:897:         type=INTEGR, val=AUTH_HMAC_SHA_96
ike V=root:0:fd23616068ea787b/0000000000000000:897:         type=PRF, val=PRF_HMAC_SHA
ike V=root:0:fd23616068ea787b/0000000000000000:897:         type=DH_GROUP, val=MODP1536.
ike V=root:0:fd23616068ea787b/0000000000000000:897: proposal id = 2:
ike V=root:0:fd23616068ea787b/0000000000000000:897:   protocol = IKEv2:
ike V=root:0:fd23616068ea787b/0000000000000000:897:      encapsulation = IKEv2/none
ike V=root:0:fd23616068ea787b/0000000000000000:897:         type=ENCR, val=AES_CBC (key_len =
128)
ike V=root:0:fd23616068ea787b/0000000000000000:897:         type=INTEGR, val=AUTH_HMAC_SHA2_
256_128
ike V=root:0:fd23616068ea787b/0000000000000000:897:         type=PRF, val=PRF_HMAC_SHA2_256
ike V=root:0:fd23616068ea787b/0000000000000000:897:         type=DH_GROUP, val=MODP1536.
ike V=root:0:fd23616068ea787b/0000000000000000:897: matched proposal id 2
ike V=root:0:fd23616068ea787b/0000000000000000:897: proposal id = 2:
ike V=root:0:fd23616068ea787b/0000000000000000:897:   protocol = IKEv2:
ike V=root:0:fd23616068ea787b/0000000000000000:897:      encapsulation = IKEv2/none
ike V=root:0:fd23616068ea787b/0000000000000000:897:         type=ENCR, val=AES_CBC (key_len =
```

```
128)
ike V=root:0:fd23616068ea787b/0000000000000000:897:         type=INTEGR, val=AUTH_HMAC_SHA2_
256_128
ike V=root:0:fd23616068ea787b/0000000000000000:897:         type=PRF, val=PRF_HMAC_SHA2_256
ike V=root:0:fd23616068ea787b/0000000000000000:897:         type=DH_GROUP, val=MODP1536.
ike V=root:0:fd23616068ea787b/0000000000000000:897: lifetime=86400
ike V=root:0:fd23616068ea787b/0000000000000000:897: SA proposal chosen, matched gateway ADC
Tunnel
ike V=root:0:ADC Tunnel: created connection: 0xf9e2ff0 5 192.168.1.1->192.168.1.11:4500.
ike V=root:0:ADC Tunnel:897: processing notify type NAT_DETECTION_SOURCE_IP
ike V=root:0:ADC Tunnel:897: processing NAT-D payload
ike V=root:0:ADC Tunnel:897: NAT detected: PEER
ike V=root:0:ADC Tunnel:897: process NAT-D
ike V=root:0:ADC Tunnel:897: processing notify type NAT_DETECTION_DESTINATION_IP
ike V=root:0:ADC Tunnel:897: processing NAT-D payload
ike V=root:0:ADC Tunnel:897: NAT detected: ME PEER
ike V=root:0:ADC Tunnel:897: process NAT-D
ike V=root:0:ADC Tunnel:897: enable FortiClient endpoint compliance check, use 169.254.7.1
ike V=root:0:ADC Tunnel:897: responder preparing SA_INIT msg
ike V=root:0:ADC Tunnel:897: generate DH public value request queued
ike V=root:0:ADC Tunnel:897: responder preparing SA_INIT msg
ike V=root:0:ADC Tunnel:897: compute DH shared secret request queued
ike V=root:0:ADC Tunnel:897: responder preparing SA_INIT msg
ike V=root:0:ADC Tunnel:897: create NAT-D hash local 192.168.1.1/4500 remote 192.168.1.11/4500
ike 0:ADC Tunnel:897: out
FD23616068EA787B8A56F0004EEC7C3D212022200000000000000160220000300000002C020100040300000C010000
0C800E008003000008020000050300000803000000C000000080400000528000C80005000000AE7B893BC5E3A52AA6
63A0334F31B4E900C9F5635E5CE2817A0FD7734EA390EEDF0898E22540B9AE00E8C4E1DECB51DA24B0A7C326FF6286
ADF943020E4027FF73A6E4752FEA8B133EBAB7553723BDC61E43FBC99C2D95FA88BC5BF8E322B7598FAB4F5C55A13B
2226D71DF952B088256A57D88E16C671881DDD028AC24D9E4ACA40DC26017C87C0553EDDE75D031FCFC0DBB74B4F26
E9EE0AC662A66FAD4E48A3D2232E0BDB7552E3855535D340BF34B28873D28C8FABB2FCAC5194A5373E29000014DE64
99159A9592FF9CF6A338697810782900001C0000400412CB23AF2CCA5494532E14CE0775D4D1CFA05EA40000001C00
00400514E0C02BB1C1041736812AF33F10C047BDEB6A36
ike V=root:0:ADC Tunnel:897: sent IKE msg (SA_INIT_RESPONSE): 192.168.1.1:4500-
>192.168.1.11:4500, len=352, vrf=0, id=fd23616068ea787b/8a56f0004eec7c3d, oif=5
ike 0:ADC Tunnel:897: IKE SA fd23616068ea787b/8a56f0004eec7c3d SK_ei
16:5204278EAA78717A3D501DB8ED8FD673
ike 0:ADC Tunnel:897: IKE SA fd23616068ea787b/8a56f0004eec7c3d SK_er
16:7B38711FE8D81E238370F4D9D75B4954
ike 0:ADC Tunnel:897: IKE SA fd23616068ea787b/8a56f0004eec7c3d SK_ai
32:68CF5D7F413B68413D0E6411181CD5F0EE4AA630D72274B56E6790A7EE7568F8
ike 0:ADC Tunnel:897: IKE SA fd23616068ea787b/8a56f0004eec7c3d SK_ar
32:6033D1AFE65E3A3B65B1D6B58B0B7CC7083D077684039D03897CF68F23C96DAE
ike V=root:0: comes 192.168.1.11:4500->192.168.1.1:4500,ifindex=5,vrf=0,len=612....
ike V=root:0: IKEv2 exchange=AUTH id=fd23616068ea787b/8a56f0004eec7c3d:00000001 len=608
ike 0: in
FD23616068EA787B8A56F0004EEC7C3D2E2023080000000100000260230002 44B257D3A5A3F8787BF85F7EAA6C6842
1A1613119EB8BB13C7FF639E41A46A81372B058C22714F93996558DCAEC8062BD8B1D1E9521B52D41E32A0CAF350D9
865ECEB0E65118D7E6E4B6531A0F459D852390B9A560FEFFF4191C52FFB9A123C58A18EA5F9D7DF7B39823A92FBB5F
EDFA291A7936B14D3EC484252C3D199A4260FC7AC9AFD89377376397B7A043B9969ED189E6590A9F68A5832A56E8D1
```

```
14E75C8736806DF7B85DA894EA7B7582894051CBE24AD640DC00BADF578DFC5BCA6F2895F71FDB1F3D4BE11DFD6C2D
63F3735C3931BCE9109BDD47110112FEC282A94EB7C855F401F2BD53403E6F302506914CA81888C8AE0AD9E1E90F25
2F8C1AD288BC1C5295FE046A176F107F79E6397E4428C30160FFEEACEA0B2BCCA9BC34DA2E35EE233745B0A05665E8
A95747D760282784B987DAB28DDCF50348B2550B414BE20297647BD15500EC8D4E6E5113BC403772153A671DA85879
20F7C7E1C9E3A9341F3C5094DC01DC4E3539B19E178DB92A6D282D891FDAC63CB9F95F1821DBE530FD9C42106E0AE2
DB13C8722039335FAE1A840E1BA2BC125AA48279530799BB48D91DF3DC5F000917B21DAD85BB55E2A14EC068DA364F
A8941F0DFA25C267349C21F7125E7836B19ACC6E42FB581061D7D4F81D2D581B42C96BFE4E710B14148D4E1EEA2D8C
6C361566F8BABFDB5A66A1A59E07F25BAC6CA8AD8698C8E0B2D0F73D7E06697504110A83ACC586E4C3227AEF2CE616
041F18C464A0CC31374E1A18993FD8B92ABF2C4A1C900A7EF444684BD683E8013A237D8E7E6780831EF13D24
ike 0:ADC Tunnel:897: dec
FD23616068EA787B8A56F0004EEC7C3D2E2023080000000010000023A2300000042900000C01000000C0A8010B290000
08000040002F00012E0000F1005645523D310A4643545645523D372E322E342E303937320A5549443D393546303735
303343423732344245303833323038463937454542394346382 0A49503D3139322E3136382E312E31310A4D41433D
30302D31352D35642D32332D61382D34613B30302D31352D35642D32332D61382D35613B0A484F53543D4445534B54
4F502D493134495656430A555345523D69707365630A4F535645523D4D6963726F736F66742057696E646F77732031
3020456E7465727072697365204564697469 6F6E2C2036342D62697420286275696C642031393034352 90A5245475F
5354415455533D300A454D53534E3D464354454D533838323430393033331350A454D5349443D303030303030303030
3030303030303030303030303030303030303030303030303030300A00210000540100000000070010464354383030313634373
38393239393400010000000200000003000000040000000D0000001900000008000000 0F0000000A0000000B000070
010000540A0000540B0000700000002C000054020000280103040 38DE23FFD0300000C0100000C800E008003000008
030000020000000805000000000000280203040 38DE23FFD0300000C0100000C800E00800300000803000 00C000000
08050000002D000018010000000700001000 00FFFF00000000FFFFFFFF0000001801000000070000100000FFFF0000
0000FFFFFFFF
ike V=root:0:ADC Tunnel:897: responder received AUTH msg
ike V=root:0:ADC Tunnel:897: processing notify type INITIAL_CONTACT
ike V=root:0:ADC Tunnel:897: processing notify type FORTICLIENT_CONNECT
ike V=root:0:ADC Tunnel:897: received FCT data len = 294, data = 'VER=1
FCTVER=7.2.4.0972
UID=95F07503CB724BE083208F97EEB9CF82
IP=192.168.1.11
MAC=00-15-5d-23-a8-4a;00-15-5d-23-a8-5a;
HOST=DESKTOP-I14IVVC
USER=ipsec
OSVER=Microsoft Windows 10 Enterprise Edition, 64-bit (build 19045)
REG_STATUS=0
EMSSN=FCTEMS12345
EMSID=00000000000000000000000000000000
'
ike V=root:0:ADC Tunnel:897: received FCT-UID : 123456
ike V=root:0:ADC Tunnel:897: peer identifier IPV4_ADDR 192.168.1.11
ike V=root:0:ADC Tunnel:897: re-validate gw ID
ike V=root:0:ADC Tunnel:897: gw validation OK
ike V=root:0:ADC Tunnel:897: responder preparing EAP identity request
ike 0:ADC Tunnel:897: enc
2700000C01000000C0A80101300000280200000002CC85F24CD85A4D9BBD5130FD954CDE9631E41538971618AC5CA89
FFDA271E450000000901B8000501020102
ike 0:ADC Tunnel:897: out
FD23616068EA787B8A56F0004EEC7C3D2E2023200000000100000080240000642D7B15B7617F0AAB77FB620A310E31
571D63B20BDE4BF92244B54828CCEA823498115B71F5CF9E3A6CE97DDB9C2256805BA9204032A89FF3D43D7772BFF5
1C427158D5E20A7CCE25EEF29F6B9AFEFCB4ED31E7DFDB6171994083D5F59A0DDF25
ike V=root:0:ADC Tunnel:897: sent IKE msg (AUTH_RESPONSE): 192.168.1.1:4500-
```

```
>192.168.1.11:4500, len=128, vrf=0, id=fd23616068ea787b/8a56f0004eec7c3d:00000001, oif=5
ike V=root:0: comes 192.168.1.11:4500->192.168.1.1:4500,ifindex=5,vrf=0,len=84....
ike V=root:0: IKEv2 exchange=AUTH id=fd23616068ea787b/8a56f0004eec7c3d:00000002 len=80
```

5. After the VPN connection succeeds, ping internal servers located behind the FortiGate from the endpoint to verify that it can access them. Ping should succeed:

```
ping 192.168.2.4
Pinging 192.168.2.4 with 32 bytes of data:
Reply from 192.168.2.4: bytes=32 time=1ms TTL=127
Reply from 192.168.2.4: bytes=32 time<1ms TTL=127
Reply from 192.168.2.4: bytes=32 time=1ms TTL=127
Reply from 192.168.2.4: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.2.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

IPsec VPN over TCP

IPsec VPN, dependent on UDP, can now run over TCP. IPsec over TCP can help VPN traffic pass through restrictive firewalls, especially when only TCP-based traffic is allowed. An IPsec VPN can be configured to use UDP or TCP exclusively or automatically switch to TCP mode if UDP mode is blocked. In high latency or congested networks, UDP-based VPN connections may experience packet loss or degradation in performance. TCP's built-in mechanisms for error correction and retransmission can improve the reliability and stability of the VPN connection in these conditions. IPsec over TCP is especially useful in mobile or dynamic environments (e.g., public Wi-Fi, hotel networks, or cellular data) where the network conditions or restrictions can vary significantly. It allows for more seamless and stable VPN connectivity in a wider range of scenarios.

To configure this feature:

1. FortiOS 7.4.5 and 7.6 use IKE port 500 and 4500 for UDP and TCP, respectively, for NAT traversal. You can configure custom ports as follows:

```
config system settings
    set ike-port 5000
    set ike-tcp-port 5500
end
```

2. In EMS, you can configure this feature using `<transport_mode>`. The following summarizes the available values for this element:

Value	Description
`0`	UDP transport mode. This is the default and used for most VPN connections.

Value	Description
1	TCP transport mode. This is recommended for use in restrictive networks.
2	Auto mode. FortiOS dynamically selects the transport mode.

You can also configure custom ports using the <tcp_port> and <udp_port> elements. The following provides an example of the <transport_mode> and <udp_port> elements. This example does not include all elements required for a functioning VPN connection:

```
<forticlient_configuration>
    <vpn>
        <ipsecvpn>
            <connections>
                <connection>
                        <transport_mode>1</transport_mode>
                         <tcp_port>5500</tcp_port>
                </connection>
            </connections>
    </vpn>
</forticlient_configuration>
```

The following describes configuring IPsec VPN for UDP, TCP, or auto mode.

Example: Configuring UDP transport mode

UDP is the standard IPsec VPN transport mode that encapsulates IPsec VPN traffic within UDP packets.

To configure UDP transport mode:

1. In FortiOS, configure an IPsec VPN IKEv2 tunnel:

```
config vpn ipsec phase1-interface
    edit "v2_psk-120"
        set type dynamic
        set interface "port1"
        set ike-version 2
        set peertype any
        set net-device disable
        set mode-cfg enable
        set ipv4-dns-server1 8.8.8.8
        set proposal aes128-sha256 aes256-sha256 aes128gcm-prfsha256 aes256gcm-prfsha384
chacha20poly1305-prfsha256
        set localid "120"
        set comments "VPN: v2_psk-120 (Created by VPN wizard)"
        set eap enable
        set eap-identity send-request
        set authusrgrp "IPSEC"
        set transport udp
        set ipv4-start-ip 9.5.6.7
        set ipv4-end-ip 9.5.6.70
```

```
        set save-password enable
        set client-auto-negotiate enable
        set client-keep-alive enable
        set psksecret ENC
STwYpf2ddbBq+9YPcCGIFoBBk4N7lbCV1CtQ43ABjxb3RalrZrmrUv0lyYCaqrpy9ReJb4pj98coVdNtSd9PrWWzhwk3TA
6AhbQqdDpierIe+WgNYOlPCrVkTMJXOMC+EGo0/Bk5q/othaLhIQNWeyaZcjFiwNYv4Eq8kjsPxIWguopaaGd4yhaSxO+c
WxxdDwehLVlmMjY3dkVA
    next
end
```

2. In EMS, go to *Endpoint Profiles > Remote Access*.
3. Select an existing profile or create a new one.
4. Click *XML*, then *Edit*. The following provides an example XML configuration for the feature:

```
<?xml version="1.0" ?>
<forticlient_configuration>
    <vpn>
        <enabled>1</enabled>
        <sslvpn>
            <connections/>
            <options>
                <dnscache_service_control>0</dnscache_service_control>
                <warn_invalid_server_certificate>1</warn_invalid_server_certificate>
                <disallow_invalid_server_certificate>0</disallow_invalid_server_certificate>
                <negative_split_tunnel_metric/>
                <enabled>1</enabled>
                <prefer_sslvpn_dns>1</prefer_sslvpn_dns>
                <no_dns_registration>0</no_dns_registration>
                <preferred_dtls_tunnel>0</preferred_dtls_tunnel>
                <block_ipv6>1</block_ipv6>
                <show_auth_cert_only>0</show_auth_cert_only>
                <use_gui_saml_auth>0</use_gui_saml_auth>
            </options>
        </sslvpn>
        <ipsecvpn>
            <connections>
                <connection>
                    <name>v2_psk_120</name>
                    <uid>FE3DDC0A-C4D4-48CB-8FF6-3B88EED55A03</uid>
                    <machine>0</machine>
                    <keep_running>0</keep_running>
                    <disclaimer_msg/>
                    <single_user_mode>0</single_user_mode>
                    <type>manual</type>
                    <ui>
                        <show_remember_password>1</show_remember_password>
                        <show_alwaysup>1</show_alwaysup>
                        <show_autoconnect>1</show_autoconnect>
                        <show_passcode>1</show_passcode>
                        <save_username>1</save_username>
                    </ui>
```

```
                    <redundant_sort_method>0</redundant_sort_method>
                    <tags>
                        <allowed/>
                        <prohibited/>
                    </tags>
                    <host_check_fail_warning/>
                    <ike_settings>
                        <server>10.152.35.150</server>
                        <authentication_method>Preshared Key</authentication_method>
                        <transport_mode>0</transport_mode>
                         <udp_port>5000</udp_port>
                        <fgt>1</fgt>
                        <prompt_certificate>0</prompt_certificate>
                        <xauth>
                            <use_otp>0</use_otp>
                            <enabled>1</enabled>
                            <prompt_username>1</prompt_username>
                        </xauth>
                        <version>2</version>
                        <mode>aggressive</mode>
                        <key_life>86400</key_life>
                        <localid>120</localid>
                        <implied_SPDO>0</implied_SPDO>
                        <implied_SPDO_timeout>0</implied_SPDO_timeout>
                        <nat_traversal>1</nat_traversal>
                        <nat_alive_freq>5</nat_alive_freq>
                        <enable_local_lan>1</enable_local_lan>
                        <enable_ike_fragmentation>1</enable_ike_fragmentation>
                        <mode_config>1</mode_config>
                        <dpd>1</dpd>
                        <dpd_retry_count>3</dpd_retry_count>
                        <dpd_retry_interval>5</dpd_retry_interval>
                        <run_fcauth_system>1</run_fcauth_system>
                        <sso_enabled>0</sso_enabled>
                        <auth_data>
                            <preshared_key>Enc
56ab85d0afa80ae6acb61fdfc19dc33b917298bf68f004a3e49a2e0684c4</preshared_key>
                        </auth_data>
                        <xauth_timeout>120</xauth_timeout>
                        <dhgroup>5</dhgroup>
                        <proposals>
                            <proposal>AES128|SHA1</proposal>
                            <proposal>AES256|SHA256</proposal>
                        </proposals>
                    </ike_settings>
                    <ipsec_settings>
                        <remote_networks>
                            <network>
                                <addr>0.0.0.0</addr>
                                <mask>0.0.0.0</mask>
                            </network>
```

```
            <network>
                <addr>::/0</addr>
                <mask>::/0</mask>
            </network>
        </remote_networks>
        <dhgroup>5</dhgroup>
        <key_life_type>seconds</key_life_type>
        <key_life_seconds>43200</key_life_seconds>
        <key_life_Kbytes>5200</key_life_Kbytes>
        <replay_detection>1</replay_detection>
        <pfs>1</pfs>
        <use_vip>1</use_vip>
        <virtualip>
            <type>modeconfig</type>
            <ip>0.0.0.0</ip>
            <mask>0.0.0.0</mask>
            <dnsserver>0.0.0.0</dnsserver>
            <winserver>0.0.0.0</winserver>
        </virtualip>
        <proposals>
            <proposal>AES128|SHA1</proposal>
            <proposal>AES256|SHA256</proposal>
        </proposals>
    </ipsec_settings>
    <android_cert_path/>
    <warn_invalid_server_certificate>1</warn_invalid_server_certificate>
    <on_connect>
        <script>
            <os>windows</os>
            <script/>
        </script>
        <script>
            <os>MacOSX</os>
            <script/>
        </script>
        <script>
            <os>linux</os>
            <script/>
        </script>
    </on_connect>
    <on_disconnect>
        <script>
            <os>windows</os>
            <script/>
        </script>
        <script>
            <os>MacOSX</os>
            <script/>
        </script>
        <script>
            <os>linux</os>
```

```
                        <script/>
                    </script>
                </on_disconnect>
                <traffic_control>
                    <enabled>0</enabled>
                    <mode>1</mode>
                </traffic_control>
            </connection>
        </connections>
        <options>
            <uselocalcert>0</uselocalcert>
            <use_win_local_computer_cert>1</use_win_local_computer_cert>
            <check_for_cert_private_key>0</check_for_cert_private_key>
            <disable_default_route>0</disable_default_route>
            <disallow_invalid_server_certificate>0</disallow_invalid_server_certificate>
            <usewincert>1</usewincert>
            <enhanced_key_usage_mandatory>0</enhanced_key_usage_mandatory>
            <enabled>1</enabled>
            <beep_if_error>0</beep_if_error>
            <use_win_current_user_cert>1</use_win_current_user_cert>
            <no_dns_registration>0</no_dns_registration>
            <block_ipv6>1</block_ipv6>
            <usesmcardcert>1</usesmcardcert>
            <enable_udp_checksum>0</enable_udp_checksum>
            <show_auth_cert_only>0</show_auth_cert_only>
        </options>
    </ipsecvpn>
    <lockdown>
        <exceptions>
            <ips/>
            <icdb_domains/>
            <domains/>
            <apps/>
        </exceptions>
        <grace_period>120</grace_period>
        <max_attempts>3</max_attempts>
        <enabled>0</enabled>
    </lockdown>
    <options>
        <show_vpn_before_logon>0</show_vpn_before_logon>
        <use_windows_credentials>0</use_windows_credentials>
        <certs_require_keyspec>0</certs_require_keyspec>
        <on_os_start_connect_has_priority>0</on_os_start_connect_has_priority>
        <use_legacy_vpn_before_logon>0</use_legacy_vpn_before_logon>
        <autoconnect_only_when_offnet>0</autoconnect_only_when_offnet>
        <secure_remote_access>0</secure_remote_access>
        <on_os_start_connect/>
        <allow_personal_vpns>1</allow_personal_vpns>
        <show_negotiation_wnd>0</show_negotiation_wnd>
        <suppress_vpn_notification>0</suppress_vpn_notification>
        <autoconnect_on_install>0</autoconnect_on_install>
```

```
            <keep_running_max_tries>0</keep_running_max_tries>
            <disable_connect_disconnect>0</disable_connect_disconnect>
            <after_logon_saml_auth>0</after_logon_saml_auth>
            <minimize_window_on_connect>1</minimize_window_on_connect>
        </options>
    </vpn>
    <endpoint_control>
        <ui>
            <display_vpn>1</display_vpn>
        </ui>
    </endpoint_control>
</forticlient_configuration>
```

5. In FortiClient, connect to the tunnel.
6. In FortiOS, run `diagnose vpn ike gateway list` to verify the IPsec VPN tunnel status. Note `addr` shows the UDP custom port value and transport shows `UDP`:

```
vd: root/0
name: v2_psk-120_0
version: 2
interface: port1 3
addr: 10.152.35.150:5000 -> 10.152.35.193:5000
tun_id: 9.5.6.7/::10.0.0.22
remote_location: 0.0.0.0
network-id: 0
transport: UDP
virtual-interface-addr: 169.254.1.1 -> 169.254.1.1
created: 633s ago
eap-user: ipsec
2FA: no
peer-id: 120
peer-id-auth: no
FortiClient UID: B70BAD123010487E86DB102969115E99
assigned IPv4 address: 9.5.6.7/255.255.255.255
nat: peer
pending-queue: 0
PPK: no
IKE SA: created 1/1  established 1/1  time 20/20/20 ms
IPsec SA: created 1/1  established 1/1  time 0/0/0 ms

  id/spi: 22 e14bbad06bc282a3/fd72048d5f1911d7
  direction: responder
  status: established 633-633s ago = 20ms
  proposal: aes256-sha256
  child: no
  SK_ei: 7cf79efa1dd1964a-98692d8f641b6624-be5dd5c659abccc9-b79d6391beb1af0e
  SK_er: 73cf8cf9ec463dee-a7d2cf4acfa23cf9-2428429fbfd88dd9-faf6261916aa13c5
  SK_ai: 81037c42a5f9e571-0eafd0157a02a501-948abb44f1f23603-3b9b5553a08aa135
  SK_ar: 7ddb59bdbffab109-76bc5dfb810f7707-54fb81094e46345a-0b9b4ad5dc49c8d3
  PPK: no
  message-id sent/recv: 0/132
  QKD: no
```

```
  lifetime/rekey: 86400/85496
  DPD sent/recv: 00000000/00000000
  peer-id: 120
```

Example: Configuring TCP transport mode

TCP mode ensures VPN traffic can pass through restrictive firewalls that block UDP traffic but allow TCP, such as port 443 (HTTPS). You can specify a custom port to avoid conflict with the management port on the FortiGate.

To configure TCP transport mode:

1. In FortiOS, configure an IPsec VPN IKEv2 tunnel:

```
config vpn ipsec phase1-interface
    edit "v2_psk-120"
        set type dynamic
        set interface "port1"
        set ike-version 2
        set peertype any
        set net-device disable
        set mode-cfg enable
        set ipv4-dns-server1 8.8.8.8
        set proposal aes128-sha256 aes256-sha256 aes128gcm-prfsha256 aes256gcm-prfsha384
chacha20poly1305-prfsha256
        set localid "120"
        set comments "VPN: v2_psk-120 (Created by VPN wizard)"
        set eap enable
        set eap-identity send-request
        set authusrgrp "IPSEC"
        set transport tcp
        set ipv4-start-ip 9.5.6.7
        set ipv4-end-ip 9.5.6.70
        set save-password enable
        set client-auto-negotiate enable
        set client-keep-alive enable
        set psksecret ENC
STwYpf2ddbBq+9YPcCGIFoBBk4N7lbCV1CtQ43ABjxb3RalrZrmrUv0lyYCaqrpy9ReJb4pj98coVdNtSd9PrWWzhwk3TA
6AhbQqdDpierIe+WgNYOlPCrVkTMJXOMC+EGo0/Bk5q/othaLhIQNWeyaZcjFiwNYv4Eq8kjsPxIWguopaaGd4yhaSxO+c
WxxdDwehLVlmMjY3dkVA
    next
end
```

2. In EMS, go to *Endpoint Profiles* > *Remote Access*.
3. Select an existing profile or create a new one.
4. Click *XML*, then *Edit*. The following provides an example XML configuration for the feature:

```
<?xml version="1.0" ?>
<forticlient_configuration>
    <vpn>
        <enabled>1</enabled>
```

```
        <sslvpn>
            <connections/>
            <options>
                <dnscache_service_control>0</dnscache_service_control>
                <warn_invalid_server_certificate>1</warn_invalid_server_certificate>
                <disallow_invalid_server_certificate>0</disallow_invalid_server_certificate>
                <negative_split_tunnel_metric/>
                <enabled>1</enabled>
                <prefer_sslvpn_dns>1</prefer_sslvpn_dns>
                <no_dns_registration>0</no_dns_registration>
                <preferred_dtls_tunnel>0</preferred_dtls_tunnel>
                <block_ipv6>1</block_ipv6>
                <show_auth_cert_only>0</show_auth_cert_only>
                <use_gui_saml_auth>0</use_gui_saml_auth>
            </options>
        </sslvpn>
        <ipsecvpn>
            <connections>
                <connection>
                    <name>v2_psk_120</name>
                    <uid>FE3DDC0A-C4D4-48CB-8FF6-3B88EED55A03</uid>
                    <machine>0</machine>
                    <keep_running>0</keep_running>
                    <disclaimer_msg/>
                    <single_user_mode>0</single_user_mode>
                    <type>manual</type>
                    <ui>
                        <show_remember_password>1</show_remember_password>
                        <show_alwaysup>1</show_alwaysup>
                        <show_autoconnect>1</show_autoconnect>
                        <show_passcode>1</show_passcode>
                        <save_username>1</save_username>
                    </ui>
                    <redundant_sort_method>0</redundant_sort_method>
                    <tags>
                        <allowed/>
                        <prohibited/>
                    </tags>
                    <host_check_fail_warning/>
                    <ike_settings>
                        <server>10.152.35.150</server>
                        <authentication_method>Preshared Key</authentication_method>
                        <transport_mode>1</transport_mode>
                         <tcp_port>5500</tcp_port>
                        <fgt>1</fgt>
                        <prompt_certificate>0</prompt_certificate>
                        <xauth>
                            <use_otp>0</use_otp>
                            <enabled>1</enabled>
                            <prompt_username>1</prompt_username>
                        </xauth>
```

```
                        <version>2</version>
                        <mode>aggressive</mode>
                        <key_life>86400</key_life>
                        <localid>120</localid>
                        <implied_SPDO>0</implied_SPDO>
                        <implied_SPDO_timeout>0</implied_SPDO_timeout>
                        <nat_traversal>1</nat_traversal>
                        <nat_alive_freq>5</nat_alive_freq>
                        <enable_local_lan>1</enable_local_lan>
                        <enable_ike_fragmentation>1</enable_ike_fragmentation>
                        <mode_config>1</mode_config>
                        <dpd>1</dpd>
                        <dpd_retry_count>3</dpd_retry_count>
                        <dpd_retry_interval>5</dpd_retry_interval>
                        <run_fcauth_system>1</run_fcauth_system>
                        <sso_enabled>0</sso_enabled>
                        <auth_data>
                            <preshared_key>Enc
56ab85d0afa80ae6acb61fdfc19dc33b917298bf68f004a3e49a2e0684c4</preshared_key>
                        </auth_data>
                        <xauth_timeout>120</xauth_timeout>
                        <dhgroup>5</dhgroup>
                        <proposals>
                            <proposal>AES128|SHA1</proposal>
                            <proposal>AES256|SHA256</proposal>
                        </proposals>
                    </ike_settings>
                    <ipsec_settings>
                        <remote_networks>
                            <network>
                                <addr>0.0.0.0</addr>
                                <mask>0.0.0.0</mask>
                            </network>
                            <network>
                                <addr>::/0</addr>
                                <mask>::/0</mask>
                            </network>
                        </remote_networks>
                        <dhgroup>5</dhgroup>
                        <key_life_type>seconds</key_life_type>
                        <key_life_seconds>43200</key_life_seconds>
                        <key_life_Kbytes>5200</key_life_Kbytes>
                        <replay_detection>1</replay_detection>
                        <pfs>1</pfs>
                        <use_vip>1</use_vip>
                        <virtualip>
                            <type>modeconfig</type>
                            <ip>0.0.0.0</ip>
                            <mask>0.0.0.0</mask>
                            <dnsserver>0.0.0.0</dnsserver>
                            <winserver>0.0.0.0</winserver>
```

```
                    </virtualip>
                    <proposals>
                        <proposal>AES128|SHA1</proposal>
                        <proposal>AES256|SHA256</proposal>
                    </proposals>
                </ipsec_settings>
                <android_cert_path/>
                <warn_invalid_server_certificate>1</warn_invalid_server_certificate>
                <on_connect>
                    <script>
                        <os>windows</os>
                        <script/>
                    </script>
                    <script>
                        <os>MacOSX</os>
                        <script/>
                    </script>
                    <script>
                        <os>linux</os>
                        <script/>
                    </script>
                </on_connect>
                <on_disconnect>
                    <script>
                        <os>windows</os>
                        <script/>
                    </script>
                    <script>
                        <os>MacOSX</os>
                        <script/>
                    </script>
                    <script>
                        <os>linux</os>
                        <script/>
                    </script>
                </on_disconnect>
                <traffic_control>
                    <enabled>0</enabled>
                    <mode>1</mode>
                </traffic_control>
            </connection>
        </connections>
        <options>
            <uselocalcert>0</uselocalcert>
            <use_win_local_computer_cert>1</use_win_local_computer_cert>
            <check_for_cert_private_key>0</check_for_cert_private_key>
            <disable_default_route>0</disable_default_route>
            <disallow_invalid_server_certificate>0</disallow_invalid_server_certificate>
            <usewincert>1</usewincert>
            <enhanced_key_usage_mandatory>0</enhanced_key_usage_mandatory>
            <enabled>1</enabled>
```

```
                <beep_if_error>0</beep_if_error>
                <use_win_current_user_cert>1</use_win_current_user_cert>
                <no_dns_registration>0</no_dns_registration>
                <block_ipv6>1</block_ipv6>
                <usesmcardcert>1</usesmcardcert>
                <enable_udp_checksum>0</enable_udp_checksum>
                <show_auth_cert_only>0</show_auth_cert_only>
            </options>
        </ipsecvpn>
        <lockdown>
            <exceptions>
                <ips/>
                <icdb_domains/>
                <domains/>
                <apps/>
            </exceptions>
            <grace_period>120</grace_period>
            <max_attempts>3</max_attempts>
            <enabled>0</enabled>
        </lockdown>
        <options>
            <show_vpn_before_logon>0</show_vpn_before_logon>
            <use_windows_credentials>0</use_windows_credentials>
            <certs_require_keyspec>0</certs_require_keyspec>
            <on_os_start_connect_has_priority>0</on_os_start_connect_has_priority>
            <use_legacy_vpn_before_logon>0</use_legacy_vpn_before_logon>
            <autoconnect_only_when_offnet>0</autoconnect_only_when_offnet>
            <secure_remote_access>0</secure_remote_access>
            <on_os_start_connect/>
            <allow_personal_vpns>1</allow_personal_vpns>
            <show_negotiation_wnd>0</show_negotiation_wnd>
            <suppress_vpn_notification>0</suppress_vpn_notification>
            <autoconnect_on_install>0</autoconnect_on_install>
            <keep_running_max_tries>0</keep_running_max_tries>
            <disable_connect_disconnect>0</disable_connect_disconnect>
            <after_logon_saml_auth>0</after_logon_saml_auth>
            <minimize_window_on_connect>1</minimize_window_on_connect>
        </options>
    </vpn>
    <endpoint_control>
        <ui>
            <display_vpn>1</display_vpn>

         </ui>
    </endpoint_control>
</forticlient_configuration>
```

5. In FortiClient, connect to the tunnel.
6. In FortiOS, run `diagnose vpn ike gateway list` to verify the IPsec VPN tunnel status. Note `addr` shows the TCP custom port value and transport shows `TCP`:

```
vd: root/0
name: v2_psk-120_0
version: 2
interface: port1 3
addr: 10.152.35.150:5500 -> 10.152.35.193:54854
tun_id: 9.5.6.7/::10.0.0.23
remote_location: 0.0.0.0
network-id: 0
transport: TCP
virtual-interface-addr: 169.254.1.1 -> 169.254.1.1
created: 592s ago
eap-user: ipsec
2FA: no
peer-id: 120
peer-id-auth: no
FortiClient UID: B70BAD123010487E86DB102969115E99
assigned IPv4 address: 9.5.6.7/255.255.255.255
nat: me peer
pending-queue: 0
PPK: no
IKE SA: created 1/1  established 1/1  time 80/80/80 ms
IPsec SA: created 1/1  established 1/1  time 0/0/0 ms

  id/spi: 23 93b6803bff7cff00/f89d6f9965fbf3a7
  direction: responder
  status: established 592-592s ago = 80ms
  proposal: aes256-sha256
  child: no
  SK_ei: f93108f3f8d9a94e-3e0a78289defb329-4d1ae67365f2cb56-e0d471a57ccb4f8d
  SK_er: 58b37cf4d2e96cb3-cb7e334a48905459-ac8e4ff743c86e5c-630454f2e35b97e6
  SK_ai: fc83b139808121a2-1dd68396d804e28d-bd619c0c4778dbda-9a1eb9e6fdf13808
  SK_ar: edad89ee56bf9ecc-81443426c00c78f5-0574d6b71163a43b-d9ebf04c3ae4b87f
  PPK: no
  message-id sent/recv: 0/124
  QKD: no
  lifetime/rekey: 86400/85537
  DPD sent/recv: 00000000/00000000
  peer-id: 120
```

Example: Configuring auto transport mode

In auto mode, the FortiGate dynamically selects the best mode based on the network conditions. If UDP traffic is blocked, it will switch to TCP transport mode automatically.

This provides flexibility to the VPN connection, ensuring the best possible transport method is used for stable and reliable connectivity.

To configure auto transport mode:

1. In FortiOS, configure an IPsec VPN IKEv2 tunnel. The following gives instructions for FortiOS 7.6. For FortiOS 7.4.4 and later versions, configure `set transport udp-fallback-tcp` instead of `set transport auto`:

```
config vpn ipsec phase1-interface
    edit "v2_psk-120"
        set type dynamic
        set interface "port1"
        set ike-version 2
        set peertype any
        set net-device disable
        set mode-cfg enable
        set ipv4-dns-server1 8.8.8.8
        set proposal aes128-sha256 aes256-sha256 aes128gcm-prfsha256 aes256gcm-prfsha384
chacha20poly1305-prfsha256
        set localid "120"
        set comments "VPN: v2_psk-120 (Created by VPN wizard)"
        set eap enable
        set eap-identity send-request
        set authusrgrp "IPSEC"
        set transport auto
        set ipv4-start-ip 9.5.6.7
        set ipv4-end-ip 9.5.6.70
        set save-password enable
        set client-auto-negotiate enable
        set client-keep-alive enable
        set psksecret ENC
STwYpf2ddbBq+9YPcCGIFoBBk4N7lbCV1CtQ43ABjxb3RalrZrmrUv0lyYCaqrpy9ReJb4pj98coVdNtSd9PrWWzhwk3TA
6AhbQqdDpierIe+WgNYOlPCrVkTMJXOMC+EGo0/Bk5q/othaLhIQNWeyaZcjFiwNYv4Eq8kjsPxIWguopaaGd4yhaSxO+c
WxxdDwehLVlmMjY3dkVA
    next
end
```

2. In EMS, go to *Endpoint Profiles > Remote Access*.
3. Select an existing profile or create a new one.
4. Click *XML*, then *Edit*. The following provides an example XML configuration for the feature:

```
<?xml version="1.0" ?>
<forticlient_configuration>
    <vpn>
        <enabled>1</enabled>
        <sslvpn>
            <connections/>
            <options>
                <dnscache_service_control>0</dnscache_service_control>
                <warn_invalid_server_certificate>1</warn_invalid_server_certificate>
                <disallow_invalid_server_certificate>0</disallow_invalid_server_certificate>
                <negative_split_tunnel_metric/>
                <enabled>1</enabled>
                <prefer_sslvpn_dns>1</prefer_sslvpn_dns>
                <no_dns_registration>0</no_dns_registration>
                <preferred_dtls_tunnel>0</preferred_dtls_tunnel>
                <block_ipv6>1</block_ipv6>
                <show_auth_cert_only>0</show_auth_cert_only>
                <use_gui_saml_auth>0</use_gui_saml_auth>
```

```
            </options>
        </sslvpn>
        <ipsecvpn>
            <connections>
                <connection>
                    <name>v2_psk_120</name>
                    <uid>FE3DDC0A-C4D4-48CB-8FF6-3B88EED55A03</uid>
                    <machine>0</machine>
                    <keep_running>0</keep_running>
                    <disclaimer_msg/>
                    <single_user_mode>0</single_user_mode>
                    <type>manual</type>
                    <ui>
                        <show_remember_password>1</show_remember_password>
                        <show_alwaysup>1</show_alwaysup>
                        <show_autoconnect>1</show_autoconnect>
                        <show_passcode>1</show_passcode>
                        <save_username>1</save_username>
                    </ui>
                    <redundant_sort_method>0</redundant_sort_method>
                    <tags>
                        <allowed/>
                        <prohibited/>
                    </tags>
                    <host_check_fail_warning/>
                    <ike_settings>
                        <server>10.152.35.150</server>
                        <authentication_method>Preshared Key</authentication_method>
                       <transport_mode>2</transport_mode>
                        <tcp_port>5500</tcp_port>
                        <udp_port>5000</udp_port>
                        <fgt>1</fgt>
                        <prompt_certificate>0</prompt_certificate>
                        <xauth>
                            <use_otp>0</use_otp>
                            <enabled>1</enabled>
                            <prompt_username>1</prompt_username>
                        </xauth>
                        <version>2</version>
                        <mode>aggressive</mode>
                        <key_life>86400</key_life>
                        <localid>120</localid>
                        <implied_SPDO>0</implied_SPDO>
                        <implied_SPDO_timeout>0</implied_SPDO_timeout>
                        <nat_traversal>1</nat_traversal>
                        <nat_alive_freq>5</nat_alive_freq>
                        <enable_local_lan>1</enable_local_lan>
                        <enable_ike_fragmentation>1</enable_ike_fragmentation>
                        <mode_config>1</mode_config>
                        <dpd>1</dpd>
                        <dpd_retry_count>3</dpd_retry_count>
```

```
                        <dpd_retry_interval>5</dpd_retry_interval>
                        <run_fcauth_system>1</run_fcauth_system>
                        <sso_enabled>0</sso_enabled>
                        <xauth_timeout>120</xauth_timeout>
                        <auth_data>
                            <preshared_key>Enc
56ab85d0afa80ae6acb61fdfc19dc33b917298bf68f004a3e49a2e0684c4</preshared_key>
                        </auth_data>
                        <dhgroup>5</dhgroup>
                        <proposals>
                            <proposal>AES128|SHA1</proposal>
                            <proposal>AES256|SHA256</proposal>
                        </proposals>
                    </ike_settings>
                    <ipsec_settings>
                        <remote_networks>
                            <network>
                                <addr>0.0.0.0</addr>
                                <mask>0.0.0.0</mask>
                            </network>
                            <network>
                                <addr>::/0</addr>
                                <mask>::/0</mask>
                            </network>
                        </remote_networks>
                        <dhgroup>5</dhgroup>
                        <key_life_type>seconds</key_life_type>
                        <key_life_seconds>43200</key_life_seconds>
                        <key_life_Kbytes>5200</key_life_Kbytes>
                        <replay_detection>1</replay_detection>
                        <pfs>1</pfs>
                        <use_vip>1</use_vip>
                        <virtualip>
                            <type>modeconfig</type>
                            <ip>0.0.0.0</ip>
                            <mask>0.0.0.0</mask>
                            <dnsserver>0.0.0.0</dnsserver>
                            <winserver>0.0.0.0</winserver>
                        </virtualip>
                        <proposals>
                            <proposal>AES128|SHA1</proposal>
                            <proposal>AES256|SHA256</proposal>
                        </proposals>
                    </ipsec_settings>
                    <android_cert_path/>
                    <warn_invalid_server_certificate>1</warn_invalid_server_certificate>
                    <on_connect>
                        <script>
                            <os>windows</os>
                            <script/>
                        </script>
```

```
                    <script>
                        <os>MacOSX</os>
                        <script/>
                    </script>
                    <script>
                        <os>linux</os>
                        <script/>
                    </script>
                </on_connect>
                <on_disconnect>
                    <script>
                        <os>windows</os>
                        <script/>
                    </script>
                    <script>
                        <os>MacOSX</os>
                        <script/>
                    </script>
                    <script>
                        <os>linux</os>
                        <script/>
                    </script>
                </on_disconnect>
                <traffic_control>
                    <enabled>0</enabled>
                    <mode>1</mode>
                </traffic_control>
            </connection>
        </connections>
        <options>
            <uselocalcert>0</uselocalcert>
            <use_win_local_computer_cert>1</use_win_local_computer_cert>
            <check_for_cert_private_key>0</check_for_cert_private_key>
            <disable_default_route>0</disable_default_route>
            <disallow_invalid_server_certificate>0</disallow_invalid_server_certificate>
            <usewincert>1</usewincert>
            <enhanced_key_usage_mandatory>0</enhanced_key_usage_mandatory>
            <enabled>1</enabled>
            <beep_if_error>0</beep_if_error>
            <use_win_current_user_cert>1</use_win_current_user_cert>
            <no_dns_registration>0</no_dns_registration>
            <block_ipv6>1</block_ipv6>
            <usesmcardcert>1</usesmcardcert>
            <enable_udp_checksum>0</enable_udp_checksum>
            <show_auth_cert_only>0</show_auth_cert_only>
        </options>
    </ipsecvpn>
    <lockdown>
        <exceptions>
            <ips/>
            <icdb_domains/>
```

```
                <domains/>
                <apps/>
            </exceptions>
            <grace_period>120</grace_period>
            <max_attempts>3</max_attempts>
            <enabled>0</enabled>
        </lockdown>
        <options>
            <show_vpn_before_logon>0</show_vpn_before_logon>
            <use_windows_credentials>0</use_windows_credentials>
            <certs_require_keyspec>0</certs_require_keyspec>
            <on_os_start_connect_has_priority>0</on_os_start_connect_has_priority>
            <use_legacy_vpn_before_logon>0</use_legacy_vpn_before_logon>
            <autoconnect_only_when_offnet>0</autoconnect_only_when_offnet>
            <secure_remote_access>0</secure_remote_access>
            <on_os_start_connect/>
            <allow_personal_vpns>1</allow_personal_vpns>
            <show_negotiation_wnd>0</show_negotiation_wnd>
            <suppress_vpn_notification>0</suppress_vpn_notification>
            <autoconnect_on_install>0</autoconnect_on_install>
            <keep_running_max_tries>0</keep_running_max_tries>
            <disable_connect_disconnect>0</disable_connect_disconnect>
            <after_logon_saml_auth>0</after_logon_saml_auth>
            <minimize_window_on_connect>1</minimize_window_on_connect>
        </options>
    </vpn>
    <endpoint_control>
        <ui>
            <display_vpn>1</display_vpn>
        </ui>
    </endpoint_control>
</forticlient_configuration>
```

5. In FortiClient, connect to the tunnel. If the network blocks UDP, the connection switches to TCP transport mode automatically.
6. In FortiOS, run `diagnose vpn ike gateway list` to verify the IPsec VPN tunnel status. `addr` shows the TCP custom port value and transport shows `TCP` if the network blocks UDP:

```
vd: root/0
name: v2_psk-120_0
version: 2
interface: port1 3
addr: 10.152.35.150:5500 -> 10.152.35.193:54854
tun_id: 9.5.6.7/::10.0.0.23
remote_location: 0.0.0.0
network-id: 0
transport: TCP
virtual-interface-addr: 169.254.1.1 -> 169.254.1.1
created: 592s ago
eap-user: ipsec
2FA: no
peer-id: 120
```

```
peer-id-auth: no
FortiClient UID: B70BAD123010487E86DB102969115E99
assigned IPv4 address: 9.5.6.7/255.255.255.255
nat: me peer
pending-queue: 0
PPK: no
IKE SA: created 1/1  established 1/1  time 80/80/80 ms
IPsec SA: created 1/1  established 1/1  time 0/0/0 ms

  id/spi: 23 93b6803bff7cff00/f89d6f9965fbf3a7
  direction: responder
  status: established 592-592s ago = 80ms
  proposal: aes256-sha256
  child: no
  SK_ei: f93108f3f8d9a94e-3e0a78289defb329-4d1ae67365f2cb56-e0d471a57ccb4f8d
  SK_er: 58b37cf4d2e96cb3-cb7e334a48905459-ac8e4ff743c86e5c-630454f2e35b97e6
  SK_ai: fc83b139808121a2-1dd68396d804e28d-bd619c0c4778dbda-9a1eb9e6fdf13808
  SK_ar: edad89ee56bf9ecc-81443426c00c78f5-0574d6b71163a43b-d9ebf04c3ae4b87f
  PPK: no
  message-id sent/recv: 0/124
  QKD: no
  lifetime/rekey: 86400/85537
  DPD sent/recv: 00000000/00000000
  peer-id: 120
```

Troubleshooting IPsec VPN IKEv1

This document focuses on troubleshooting multiple scenarios of IPsec VPN IKEv1 connection failures.



FortiClient 7.4.4 and later versions do not support IPsec VPN IKEv1. Configure IPsec VPN IKEv2 if using FortiClient 7.4.4 and later versions.

When troubleshooting various IKEv1 connection failure scenarios, you may need to use various FortiClient and FortiOS logs and diagnostics. The following provides guidance on where to find these resources:

- FortiClient:
  - *Settings > Export logs*
  - For IKE logs, see *C:\Program Files\Fortinet\trace\logs\FortiIKE.log* or use the FortiClient diagnostic tool. See Diagnostic Tool.
- FortiOS
  - To view VPN events on FortiOS, go to *Log & Report > System Events*.
  - To gather diagnostic information related to IKEv1, run the following commands in the CLI:

```
diagnose debug app ike -1
diagnose debug app fnbamd -1
diagnose debug enable
```

Phase 1 negotiation failure

Usually, if phase 1 negotiation fails, FortiClient reports that the peer failed to complete phase 1 negotiation due to timeout. The following provides example logs for this scenario. The following is an example of logs exported from FortiClient in *Settings* > *Export Logs* in this scenario:

```
No response from the peer, phase1 retransmit reaches maximum count.
```

Another way to verify phase 1 negotiation failure is checking FortiClient IKE logs located under `C:\Program Files\Fortinet\trace\logs\FortiIKE.log`. In this scenario, FortiClient likely loops in the `resend phase1` packet state.

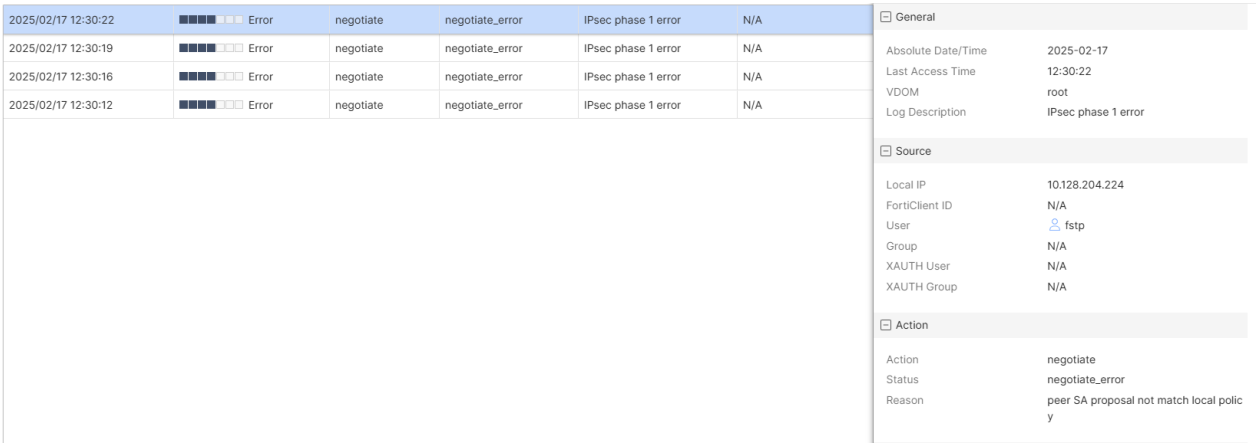
Since FortiClient is in a loop, FortiOS IKE diagnostics will reflect multiple repeated incoming SA proposals. The result of each proposal is the same when there is a proposal mismatch. In this situation, you may run the following FortiOS IKE diagnostic commands for troubleshooting:

```
diagnose debug application ike -1
diagnose debug enable
```

The following shows sample logs for these commands:

```
2025-02-17 12:30:16.076630 ike V=root:0:910fd95fd1c9ea25/0000000000000000:12: negotiation failure
2025-02-17 12:30:16.076651 ike V=root:Negotiate ISAKMP SA Error:
2025-02-17 12:30:16.076656 ike V=root:0:910fd95fd1c9ea25/0000000000000000:12: no SA proposal
chosen
```

The following shows an example of VPN events with an IPsec VPN phase 1 negotiation failure as shown in the FortiOS GUI:



When troubleshooting phase 1 negotiation failure, ensure that the FortiGate settings under the respective IKE SA (`config vpn ipsec phase1-interface`) match the FortiClient phase 1 configuration.

PSK authentication failure

In the case that there is a preshared key (PSK) mismatch between FortiOS and FortiClient, FortiOS CLI diagnostics and VPN events do not reveal apparent issues when PSK authentication fails.

The FortiOS CLI diagnostics show multiple phase 1 retransmissions without any clear errors:

```
2025-02-17 12:58:40.549909 ike V=root:0:FSTP IPsec:17: sent IKE msg (retransmit):
10.128.204.224:500->10.10.11.2:500, len=600, vrf=0, id=ae4505eb62a5e5e1/0c3bed05b632a5ef
```

In this situation, FortiClient logs, exported in *Settings* > *Export Logs*, can provide more information, showing logs similar to the following:

```
2/17/2025 12:59:23 PM   info    ipsecvpn ... msg="IKE phase1 authentication fail as peer's certificate
is not
verified"
2/17/2025 12:59:23 PM  error   ipsecvpn ... status=negotiate_error init=local mode=xauth_clinet
stage=1
dir=inbound status=failureInitiator: parsed 10.128.204.224 aggressive mode message #1 (ERROR)"
```

FortiClient IKE diagnostics reveal a HASH mismatch:

```
[2025-02-17 12:53:29.3101064 UTC-07:00] [1600:9808] [FortiIKE  1325   debug] HASH received:
[2025-02-17 12:53:29.3101114 UTC-07:00] [1600:9808] [FortiIKE  123    info]  768a6795 07217a94
d15025fb 3f291e9d d9387369 493e8e02 414b2d8f 4dd70fac
...
[2025-02-17 12:53:29.3102000 UTC-07:00] [1600:9808] [FortiIKE  1030   debug] HASH computed:
[2025-02-17 12:53:29.3102052 UTC-07:00] [1600:9808] [FortiIKE  123    info]  3d16d1c4 58cdbcbf
6f11e20d 57258c39 7d1d04e3 6fac054b 66ee3c8e dfcd87d4
[2025-02-17 12:53:29.3102065 UTC-07:00] [1600:9808] [FortiIKE  1352   error] HASH mismatched
```

When troubleshooting PSK mismatch, ensure that the PSK matches on the FortiClient and FortiGate.

Signature authentication failure

Signature authentication failures can be divided into two broad categories:

- FortiClient fails to retrieve local certificate.
- FortiGate fails to authenticate FortiClient based on the certificate provided.

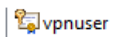
FortiClient cannot obtain certificate

A common issue is that FortiClient cannot retrieve a certificate for signature authentication. Following is an example of the FortiClient debug IKE log in this scenario:

```
[2025-02-18 11:28:14.8061460 UTC-07:00] [7364:9836] [FortiIKE  225   debug] Could not obtain
certificate. Quit now.
[2025-02-18 11:28:14.8062425 UTC-07:00] [7364:9836] [FortiIKE  764   debug] addspspec pki_get_
mycert() failed
```

To troubleshoot scenario where FortiClient cannot obtain the certificate:

1. Ensure that the FortiClient certificate has *Client Authentication* extended key usage.
2. Verify that the FortiClient certificate has been imported with a private key.



You can configure FortiClient to check for a certificate private key by enabling *Check for Certificate Private Key* under *IPsec VPN* in a Remote Access profile. See IPsec VPN on page 145.

If this verification is disabled and FortiClient is missing a certificate private key, a similar log is generated in the %localappdata%\FortiClient\logs\trace\certificates_1.txt log file:

```
Certificates_GetCertificate CryptGetUserKey failed. LastError=000000b7
```

3. Verify *Prompt for Certificate* is enabled under *Advanced Settings* in the Remote Access profile in EMS. See IPsec VPN on page 145.
4. Ensure that the certificate type is as configured in the Remote Access profile as local, SmartCard, or system store.

FortiGate server certificate validation failure

When FortiClient cannot validate the FortiGate IPsec VPN server certificate, the FortiClient FortiIKE.log displays the following error:

```
[2025-02-18 12:07:02.5029633 UTC-07:00] [7812:7816] [FortiIKE  1529   debug] root ca CERT failed
[2025-02-18 12:07:02.5030032 UTC-07:00] [7812:7816] [FortiIKE  1549   error] the peer's
certificate is not verified.
```

To troubleshoot scenario where FortiClient cannot validate the FortiGate IPsec VPN server certificate:

1. Ensure that the FortiGate certificate is trusted by the endpoint, namely that the root CA and subordinate CAs are in the endpoint certificate store.
2. Ensure that the FortiGate certificate has *Server Authentication* as an extended key usage. You can validate what server certificate is in use by running `config vpn ipsec phase1-interface`. You can confirm the extended key usage by going to *System > Certificates > Local Certificate*.
3. Ensure that the FortiGate IP address or FQDN is in the *CN/SAN* field. You can disable this check by disabling *Do Not Accept Invalid Server Certificate* in the Remote Access endpoint profile.

FortiGate Xauth misconfiguration

When using signatures as the authentication method, disable XAuth under `config vpn ipsec phase1-interface set xauthtype disable` as well as on FortiClient. Otherwise, FortiGate sends XAuth request after successful phase 1 negotiation, which may result in VPN connection failure.

The following shows a FortiClient IKE error that may displayed when XAuth is configured on FortiGate with signature authentication. The error may differ depending on the versions used:

```
[2025-02-18 12:19:06.1940780 UTC-07:00] [560:7580] [FortiIKE  229   error] failed to get ID.
[2025-02-18 12:19:06.1944175 UTC-07:00] [560:7580] [FortiIKE  1110   error] failed to begin ipsec
sa negotiation.
```

If seen, verify if XAuth is disabled on the FortiGate IKE SA configuration.

FortiGate PKI group mismatch

Whenever a PKI user is not a member of the PKI group, phase 1 negotiation fails. Following is an example of FortiGate IKE diagnostics in this scenario:

```
ike V=root:0:3f7ef718adc35ab3/0000000000000000:50: negotiation failure
ike V=root:Negotiate ISAKMP SA Error:
ike V=root:0:3f7ef718adc35ab3/0000000000000000:50: no SA proposal chosen
```

When troubleshooting a PKI group mismatch, verify whether a PKI user (`config user peer`) is a member of the PKI group (`config user peergrp`) referenced under `config vpn ipsec phase1-interface` configuration (`set peergrp`) .

XAuth failure

When user authentication is likely to be an issue, ensure to include `fnbamd` in the FortiGate CLI diagnostics. The following shows an example FortiOS CLI `fnbamd` output in this scenario:

```
2025-02-17 14:44:40.426768 ike V=root:0:FSTP IPsec_0:20: XAUTH 11652250210315 result FNBAM_DENIED
2025-02-17 14:44:40.426800 ike V=root:0:FSTP IPsec_0: XAUTH failed for user "vpnuser", retry(2).
```

The `fnbamd` process handles authentication. If it denies the authentication request, it means that the credentials are incorrect or that group mismatch has occurred.

To trouble XAuth failure:

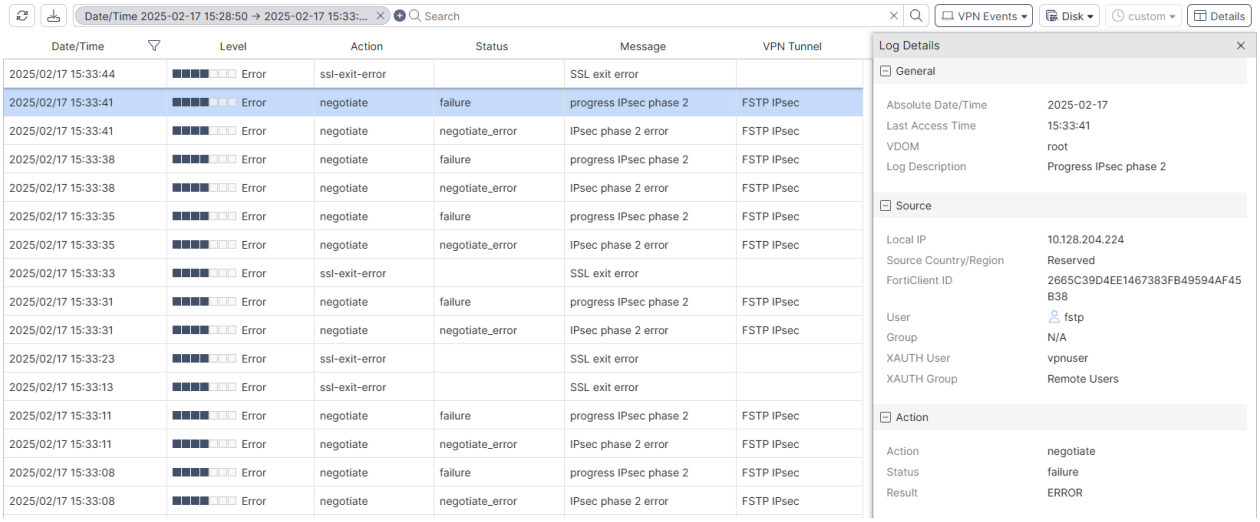
1. Include `fnbamd` diagnostics.
2. Verify firewall group settings in the IPsec VPN firewall policy and/or `config vpn ipsec phase1-interface` > `authgrp`. Typically, either one of them should be used.
3. Ensure that the credentials are correct.

Phase 2 negotiation failure

Same as with phase 1, if IPsec VPN proposals are misaligned, then FortiGate outputs the following in the `diagnose debug app ike -1` CLI diagnostics:

```
2025-02-17 15:32:39.313221 ike V=root:0:FSTP IPsec_0:25:FSTP IPsec:18816: negotiation failure
2025-02-17 15:32:39.313242 ike V=root:Negotiate IPsec SA Error:
2025-02-17 15:32:39.313247 ike V=root:0:FSTP IPsec_0:25:18816: no SA proposal chosen
```

The following shows an example of VPN events with an IPsec VPN phase 2 error as shown in the FortiOS GUI:



To troubleshoot phase 2 negotiation failure:

1. Ensure that the FortiGate settings under the desired IPsec VPN SA (`config vpn ipsec phase2-interface`) match the FortiClient phase 2 configuration. See IPsec VPN on page 145 and Phase 1 configuration.
2. Ensure that the PFS settings match on the FortiClient and FortiGate as well as the DH group.

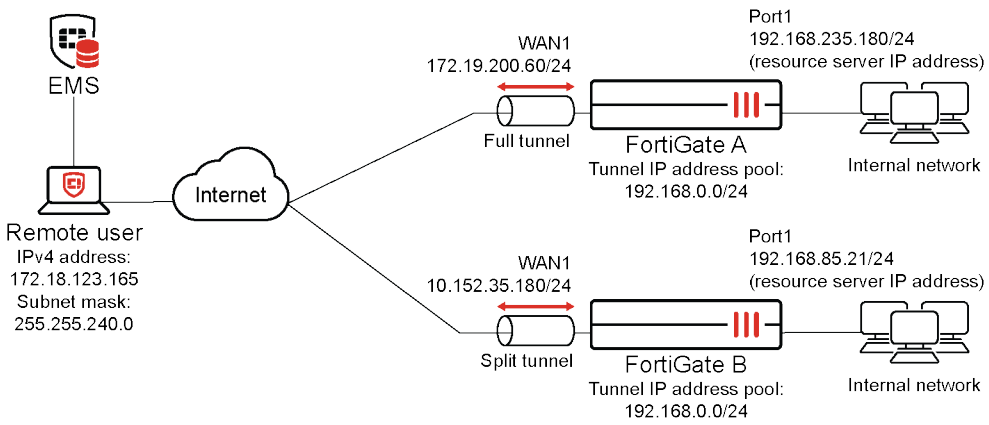
Dual IPsec VPN tunnel support

FortiClient 7.4.4 and later versions support dual IPsec VPN IKEv2 connections for EMS-managed IPsec VPN tunnels. You can route internet traffic through multiple VPN gateways for enhanced security.

The example configures two VPN tunnels, which FortiClient can be connected to at the same time in a parallel configuration. The two tunnels are as follows:

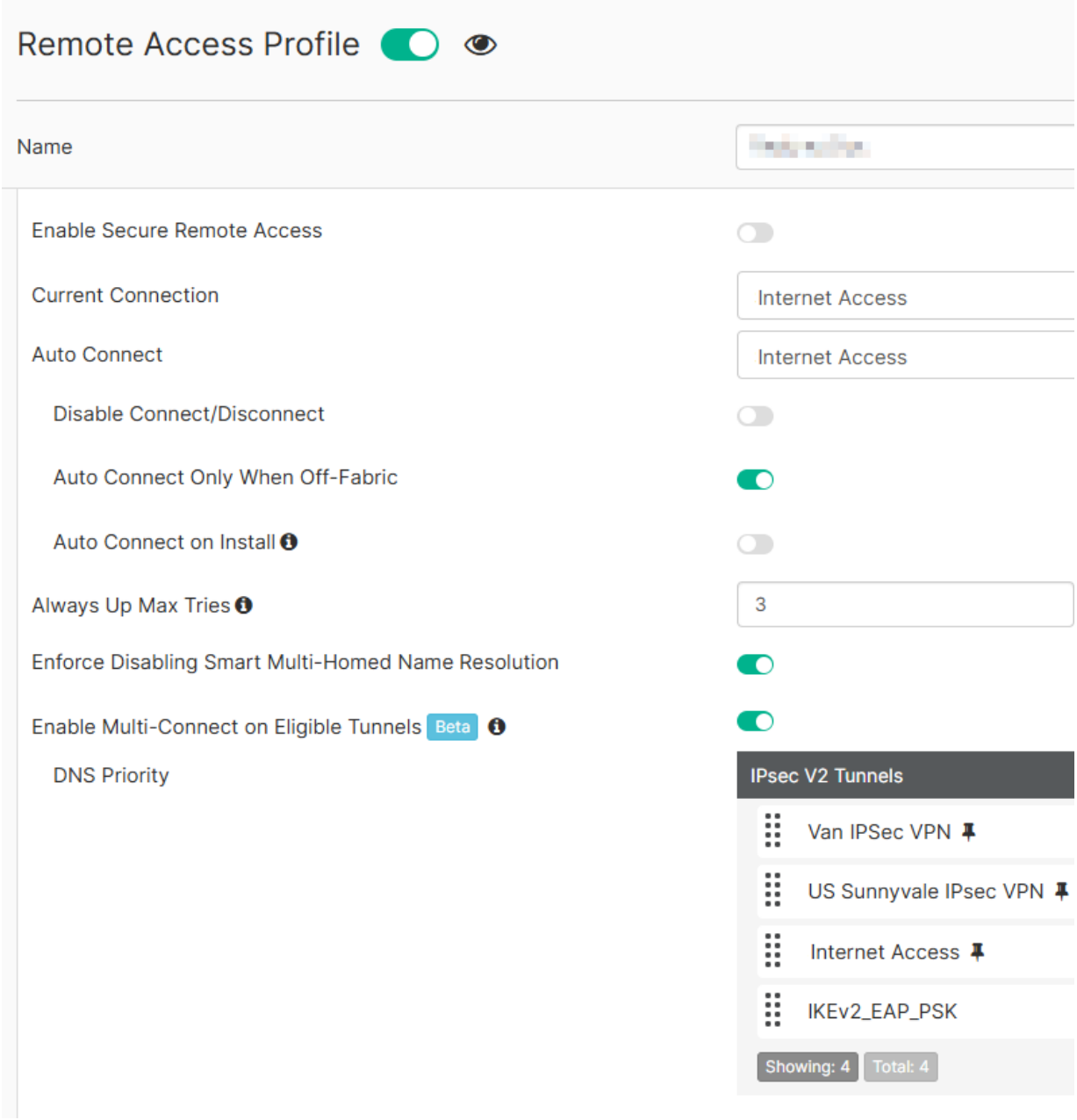
- Internet Access, a full tunnel
- Van IPSec VPN, a split tunnel

After FortiClient connects to both tunnels successfully, the end user can access file servers behind each FortiGate via the respective VPN tunnel.



To configure dual VPN tunnel support on EMS:

1. Go to *Endpoint Profiles > Remote Access*.
2. Create a new profile or edit an existing one.
3. Under *General*, toggle on *Enable Multi-Connect on Eligible Tunnels*.
4. Eligible tunnels appear below the toggle. There can be a maximum of 50 such tunnels per profile. Drag and drop tunnels to define the DNS query priority. The priority list determines which tunnel interface has higher priority for DNS queries on Windows. When performing a DNS query, Windows queries the DNS server from the tunnel with the highest priority. If the query fails, then Windows queries the DNS server from the tunnel with the next highest priority, and so on. The DNS priority is the same as the VPN tunnel interface metric.



5. If desired, you can pin tunnels, which increases their visibility in FortiClient. Create or edit an existing VPN tunnel as desired.
6. In *Basic Settings*, enable *Pinned Tunnel*.
7. Click *Save*, then click *Save* again.

You can also configure these features using XML elements. See XML configuration on page 306.

To connect to dual VPN tunnels from FortiClient:

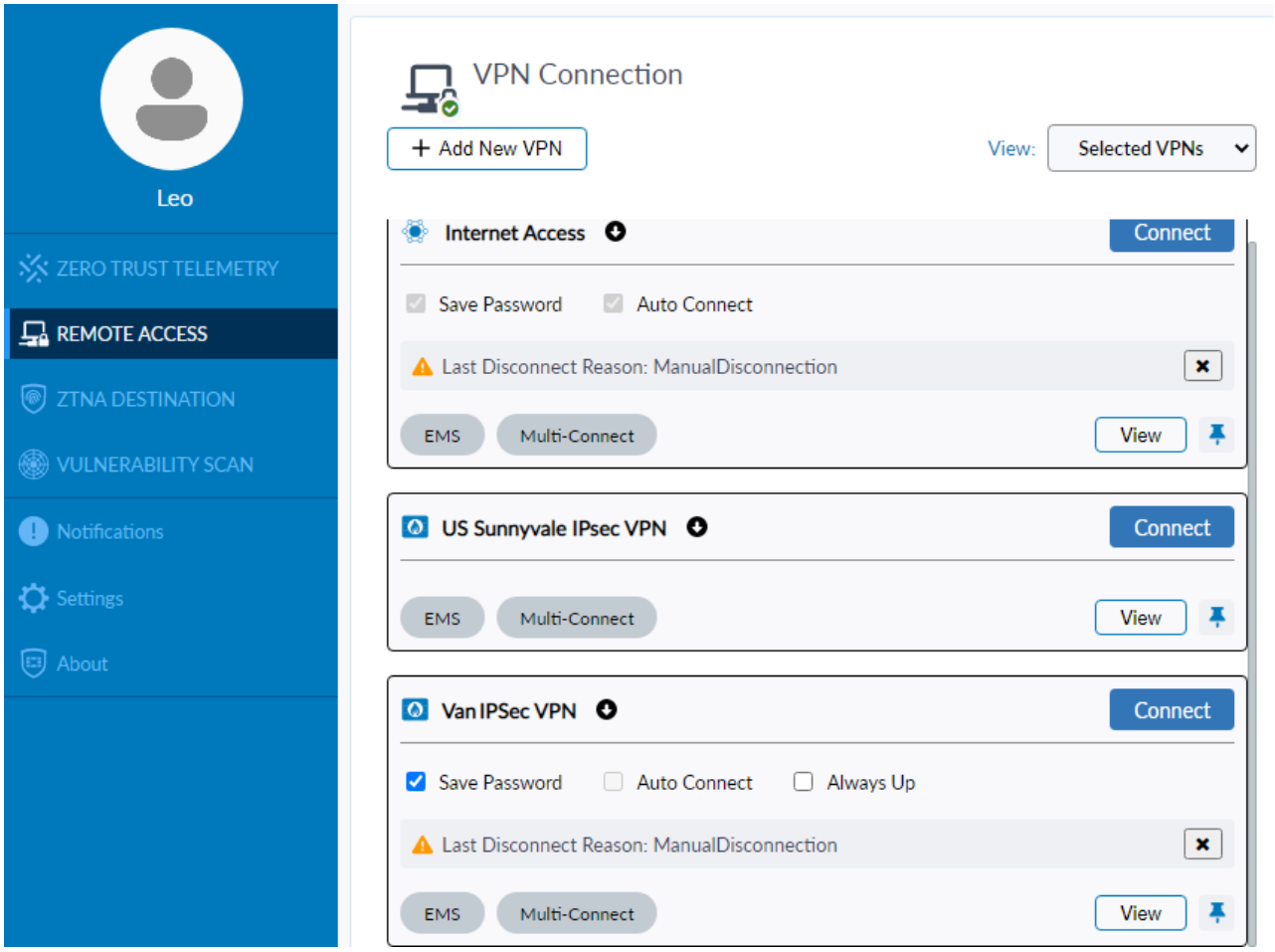
1. On the endpoint, to verify the configuration before connecting to any VPN tunnel, run `ipconfig` in Command Prompt. The following shows an example output:

```
Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : mshome.net
   Link-local IPv6 Address . . . . . : fe80::bf3a:ec09:aac8:8d0f%12
   IPv4 Address. . . . . . . . . . . : 172.18.123.165
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 172.18.112.1
```

2. After FortiClient receives the profile updates from EMS, go to *Remote Access*.
3. From the *View* dropdown list, select *Selected VPNs*. Only pinned tunnels display in FortiClient and FortiTray. If *Enable View Selected VPNs* is not enabled in EMS, FortiClient remembers the *Selected VPNs* setting and only shows pinned tunnels for that user when they open the FortiClient console in the future. FortiClient respects the local setting over the EMS setting in this case.
4. Click *Connect* for the first desired tunnel. In this example, this tunnel is Internet Access.



5. Run `ipconfig` again. The output differs now that FortiClient is connected to the Internet Access tunnel:

```
Windows IP Configuration
Unknown adapter Internet Access:
```

```
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::549c:eb47:9f4a:b437%20
   Default Gateway . . . . . . . . . : 192.168.0.12

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : mshome.net
   Link-local IPv6 Address . . . . . : fe80::bf3a:ec09:aac8:8d0f%12
   IPv4 Address. . . . . . . . . . . : 172.18.123.165
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 172.18.112.1
```

6. Run `route print` to view the routing table information. At this point, all traffic goes through the tunnel interface with an IP address of 192.168.0.11:

```
===========================================================================
Interface List
 20...........................Fortinet VPN-V Network Adapter
 12...00 15 5d a1 9f 1b ......Microsoft Hyper-V Network Adapter #2
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     172.18.112.1   172.18.123.165     15
          0.0.0.0          0.0.0.0     192.168.0.12     192.168.0.11      4
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
     172.18.112.0    255.255.240.0         On-link    172.18.123.165    271
   172.18.123.165  255.255.255.255         On-link    172.18.123.165    271
   172.18.127.255  255.255.255.255         On-link    172.18.123.165    271
    172.19.200.60  255.255.255.255     172.18.112.1   172.18.123.165     16
      192.168.0.0    255.255.255.0         On-link      192.168.0.11    259
     192.168.0.11  255.255.255.255         On-link      192.168.0.11    259
    192.168.0.255  255.255.255.255         On-link      192.168.0.11    259
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link    172.18.123.165    271
        224.0.0.0        240.0.0.0         On-link      192.168.0.11    259
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link    172.18.123.165    271
  255.255.255.255  255.255.255.255         On-link      192.168.0.11    259
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
```

```
 If Metric Network Destination      Gateway
  1    331 ::1/128                  On-link
 12    271 fe80::/64                On-link
 20    261 fe80::/64                On-link
 20    261 fe80::549c:eb47:9f4a:b437/128
                                    On-link
 12    271 fe80::bf3a:ec09:aac8:8d0f/128
                                    On-link
  1    331 ff00::/8                 On-link
 12    271 ff00::/8                 On-link
 20    261 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

7. Click *Connect* for the second desired tunnel. In this example, this tunnel is Van IPSec VPN.
8. Run commands in Command Prompt to verify the endpoint network configuration with the dual VPN connections:
   a. Run `ipconfig` again. The output differs now that FortiClient is connected to two tunnels:

```
Unknown adapter Van IPSec VPN:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::549c:eb47:9f4a:b437%22
   IPv4 Address. . . . . . . . . . . : 192.168.180.21
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.180.22

Unknown adapter Internet Access:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::549c:eb47:9f4a:b437%20
   IPv4 Address. . . . . . . . . . . : 192.168.0.11
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.12

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : mshome.net
   Link-local IPv6 Address . . . . . : fe80::bf3a:ec09:aac8:8d0f%12
   IPv4 Address. . . . . . . . . . . : 172.18.123.165
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 172.18.112.1
```

   b. Run `netsh interface ipv4 show interface` to verify the VPN tunnel interface metrics. You can see that Van IPSec VPN has the lowest metric (the value in the `Met` column):

```
Idx     Met         MTU          State                Name
---  ----------  ----------  ------------  ---------------------------
  1          75  4294967295  connected     Loopback Pseudo-Interface 1
 20           3        1280  connected     Internet Access
```

```
22           1        1280  connected     Van IPSec VPN
12          15        1500  connected     Ethernet 2
```

c. Run `route print` to view the routing table information. As the Van IPSec VPN tunnel has the lowest metric, traffic destined for split tunnels goes through the Van IPSec VPN tunnel:

```
===========================================================================
Interface List
 22...........................Fortinet VPN-V Network Adapter #2
 20...........................Fortinet VPN-V Network Adapter
 12...00 15 5d a1 9f 1b ......Microsoft Hyper-V Network Adapter #2
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     172.18.112.1   172.18.123.165     15
          0.0.0.0          0.0.0.0   192.168.180.22   192.168.180.21   9001
          0.0.0.0          0.0.0.0     192.168.0.12     192.168.0.11      4
         10.0.0.0        255.0.0.0   192.168.180.22   192.168.180.21      2
    10.152.35.180  255.255.255.255     172.18.112.1   172.18.123.165     16
    24.206.65.136  255.255.255.255   192.168.180.22   192.168.180.21      2
    24.206.65.139  255.255.255.255   192.168.180.22   192.168.180.21      2
    24.206.65.140  255.255.255.255   192.168.180.22   192.168.180.21      2
     34.54.83.208  255.255.255.255   192.168.180.22   192.168.180.21      2
    35.227.253.95  255.255.255.255   192.168.180.22   192.168.180.21      2
      38.21.198.0    255.255.255.0   192.168.180.22   192.168.180.21      2
       66.35.16.0    255.255.240.0   192.168.180.22   192.168.180.21      2
       96.45.38.0    255.255.255.0   192.168.180.22   192.168.180.21      2
       96.45.39.0    255.255.255.0   192.168.180.22   192.168.180.21      2
       96.45.40.0    255.255.255.0   192.168.180.22   192.168.180.21      2
       96.45.41.0    255.255.255.0   192.168.180.22   192.168.180.21      2
       96.45.42.0    255.255.255.0   192.168.180.22   192.168.180.21      2
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      149.5.234.0    255.255.255.0   192.168.180.22   192.168.180.21      2
       154.52.0.0    255.255.240.0   192.168.180.22   192.168.180.21      2
       172.16.0.0      255.240.0.0   192.168.180.22   192.168.180.21      2
     172.18.112.0    255.255.240.0         On-link    172.18.123.165    271
   172.18.123.165  255.255.255.255         On-link    172.18.123.165    271
   172.18.127.255  255.255.255.255         On-link    172.18.123.165    271
    172.19.200.60  255.255.255.255     172.18.112.1   172.18.123.165     16
      192.168.0.0    255.255.255.0         On-link      192.168.0.11    259
     192.168.0.11  255.255.255.255         On-link      192.168.0.11    259
    192.168.0.255  255.255.255.255         On-link      192.168.0.11    259
    192.168.180.0    255.255.255.0         On-link    192.168.180.21    257
   192.168.180.21  255.255.255.255         On-link    192.168.180.21    257
  192.168.180.255  255.255.255.255         On-link    192.168.180.21    257
    192.168.235.0    255.255.255.0   192.168.180.22   192.168.180.21      2
```

```
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link    172.18.123.165    271
        224.0.0.0        240.0.0.0         On-link      192.168.0.11    259
        224.0.0.0        240.0.0.0         On-link    192.168.180.21    257
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link    172.18.123.165    271
  255.255.255.255  255.255.255.255         On-link      192.168.0.11    259
  255.255.255.255  255.255.255.255         On-link    192.168.180.21    257
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    331 ::1/128                  On-link
 12    271 fe80::/64                On-link
 20    261 fe80::/64                On-link
 22    261 fe80::/64                On-link
 20    261 fe80::549c:eb47:9f4a:b437/128
                                    On-link
 22    261 fe80::549c:eb47:9f4a:b437/128
                                    On-link
 12    271 fe80::bf3a:ec09:aac8:8d0f/128
                                    On-link
  1    331 ff00::/8                 On-link
 12    271 ff00::/8                 On-link
 20    261 ff00::/8                 On-link
 22    261 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

d. Confirm access to protected networks by pinging resources behind the FortiGates.

i. Ping a resource behind the first FortiGate. This example pings 192.168.235.180, the IP address of a file server behind FortiGate A:

```
ping 192.168.235.180 -t

Pinging 192.168.235.180 with 32 bytes of data:
Reply from 192.168.235.180: bytes=32 time=1ms TTL=127
Reply from 192.168.235.180: bytes=32 time=1ms TTL=127
Reply from 192.168.235.180: bytes=32 time=2ms TTL=127

Ping statistics for 192.168.235.180:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

ii. Ping a resource behind the second FortiGate. This example pings 192.168.85.1, the IP address of the LAN behind FortiGate B:

```
ping 192.168.85.1

Pinging 192.168.85.1 with 32 bytes of data:
Reply from 192.168.85.1: bytes=32 time<1ms TTL=255
Reply from 192.168.85.1: bytes=32 time=1ms TTL=255
Reply from 192.168.85.1: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.85.1:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

XML configuration

This feature introduces the following new XML tags:

Tag	Description
<enable_multi_vpn>	Allows FortiClient to connect to multiple VPN tunnels concurrently.
<allow_concurrent>	Per-tunnel configuration. Allow user to connect to this tunnel via the FortiClient console or FortiTray as one of multiple concurrent VPN tunnels.
<pinned>	Per-tunnel configuration. A pinned tunnel displays in the FortiTray menu and in the FortiClient GUI when *View > Selected VPNs* is selected.
<enable_view_selected_vpns>	Enable for FortiClient to display pinned tunnels by default. If disabled, the FortiClient GUI displays all configured VPN tunnels. The user can select *View > Selected VPNs* to only display pinned tunnels. FortiClient remembers this setting and only shows pinned tunnels for that user when they open the FortiClient console in the future. FortiClient respects the local setting over the EMS setting in this case.
<dns_priority>	Per-tunnel configuration. A lower value means that the tunnel has higher priority for DNS queries on Windows when the endpoint is connected to multiple tunnels. The priority list determines which tunnel interface has higher priority for DNS queries on Windows. When performing a DNS query, Windows queries the DNS server from the tunnel with the highest priority. If the query fails, then Windows queries the DNS server from the tunnel with the next highest priority, and so on.

The following provides the example XML configuration. The XML sample is an incomplete configuration that does not provide all necessary tags:

```
<forticlient_configuration>
    <vpn>
        <ipsecvpn>
            <connections>
                <connection>
                    <name>Van IPSec VPN</name>
                    <dns_priority>1</dns_priority>
```

```
                    <pinned>1</pinned>
                    <allow_concurrent>1</allow_concurrent>
                </connection>
            </connections>
        </ipsecvpn>
        <options>
            <autoconnect_tunnel>Internet Access</autoconnect_tunnel>
            <enable_multi_vpn>1</enable_multi_vpn>
            <enable_view_selected_vpns>0</enable_view_selected_vpns>
        </options>
    </vpn>
</forticlient_configuration>
```

ZTNA Destinations

You can use FortiClient to create a secure encrypted connection to protected applications without using VPN. Acting as a local proxy gateway, FortiClient works with the FortiGate application proxy feature to create a secure connection via HTTPS using a certificate received from EMS that includes the FortiClient UID. The FortiGate retrieves the UID to identify the device and check other endpoint information that EMS provides to the FortiGate, which can include other identity and posture information. The FortiGate allows or denies the access as applicable. See the *FortiOS Administration Guide* for FortiOS configuration requirements. For TCP forwarding to non-web-based applications, you must define ZTNA destinations as follows.

You an configure these destinations in a ZTNA Destinations profile in EMS to deploy to endpoints as part of an endpoint policy.

See ZTNA Applications Catalog on page 446 to view the ZTNA applications available for selection.

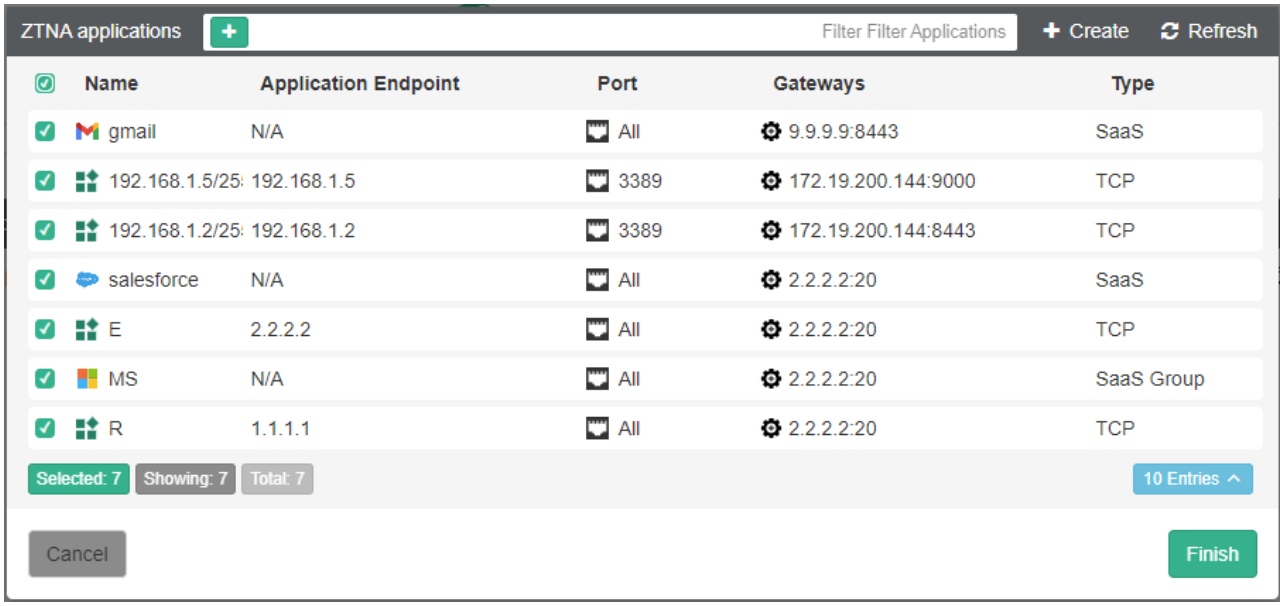
To configure a ZTNA destination profile:

1. Go to *Endpoint Profiles > ZTNA Destinations*. Select the desired profile or create a new one.
2. In the *Name* field, enter the desired name.
3. If desired, enable the following options:

Option	Description
Allow Personal Destinations 1.	Allows end users to configure personal ZTNA destinations.
Enforce Valid Server Certificate 1.	Blocks end users from accessing ZTNA destinations if they have an invalid server certificate.
Notify user on error	FortiClient displays an error message to users when a TCP forwarding error occurs.
Enable Azure Auto Login	Enables ZTNA automatic login using Microsoft Entra ID. You must specify the tenant name and client ID of the application used to connect with EMS that you collected from the Azure management console.

Option	Description
	When this option is enabled and configured, users logged in to an Entra ID domain on an endpoint are automatically authenticated with the FortiGate (7.6.1 or later) using Entra ID credentials when they attempt to access zero trust network access (ZTNA) TCP-forwarding traffic. See ZTNA automatic login using Microsoft Entra ID on page 316 for more details about FortiOS configuration.
Proxy Mode	Configure one of the following for ZTNA on FortiClient (macOS) to use for network traffic interception and redirection: • **4**: use the FortiClient (macOS) proxy extension. Otherwise, ZTNA uses macOS packet filter (pf). This is the solution that Apple officially recommends. • **0** (default): use the macOS pf.
Excluded DNS	Define exceptions for wildcard domains in ZTNA destinations. Separate multiple domains with a semicolon. For example, `www.example.com;www.test.com`.

4. Under *Rules*, click *Add*.
5. In the dialog, select the required applications. Click *Finish*.



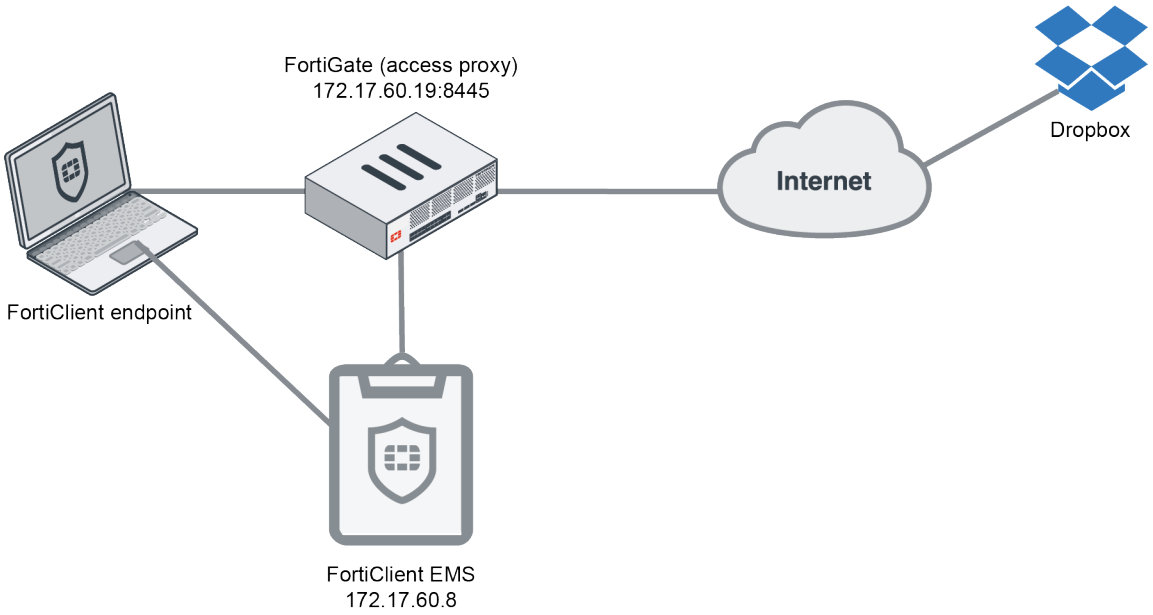
6. For each destination, if desired, you can enable *Redirect* to use the default external browser for ZTNA SAML authentication. If disabled, FortiClient uses the FortiClient embedded browser for ZTNA SAML authentication.
7. Save the profile.
8. On an endpoint that received the profile changes, go to *ZTNA Destination*. You can see the ZTNA applications from the list that EMS received from FortiOS.

Wildcard support for ZTNA FQDN rules

This feature requires FortiOS 7.2.2 or a later version.

This example uses external browser-based SAML authentication for the zero trust network access (ZTNA) policy. This configuration requires the following:

- A Fortinet Security Fabric connector is established between FortiOS and EMS.
- FortiOS ZTNA settings are configured.
- FortiClient is registered to EMS



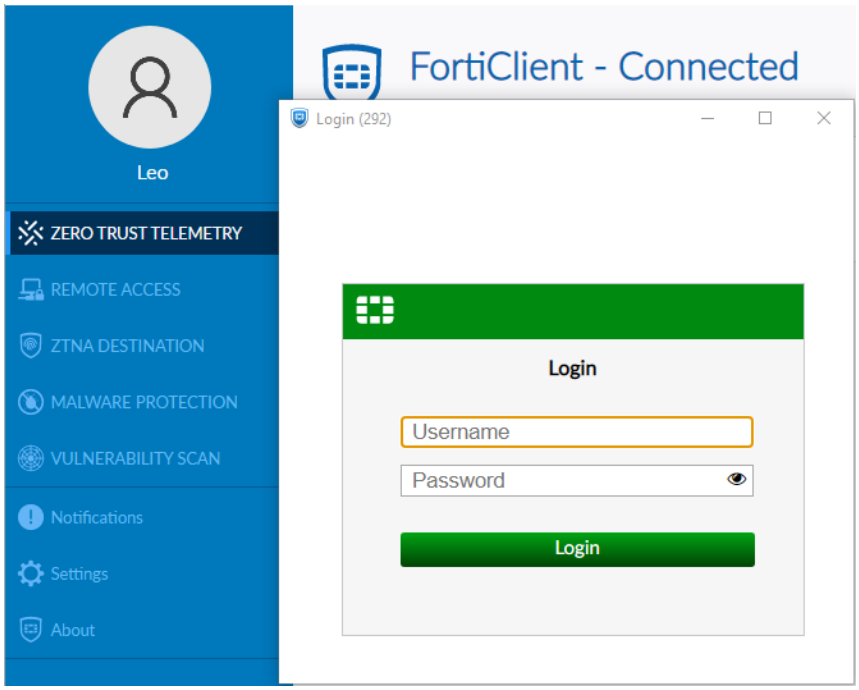
In the example topology, the EMS IP address is 172.17.60.8. The FortiGate acts as an access proxy, with virtual IP address 172.17.60.19 and port 8445. You can use one of the following methods to configure a ZTNA rule that supports wildcard FQDNs:

- Configuring a ZTNA rule in EMS
- Configuring FortiClient to pull SaaS application information from FortiOS

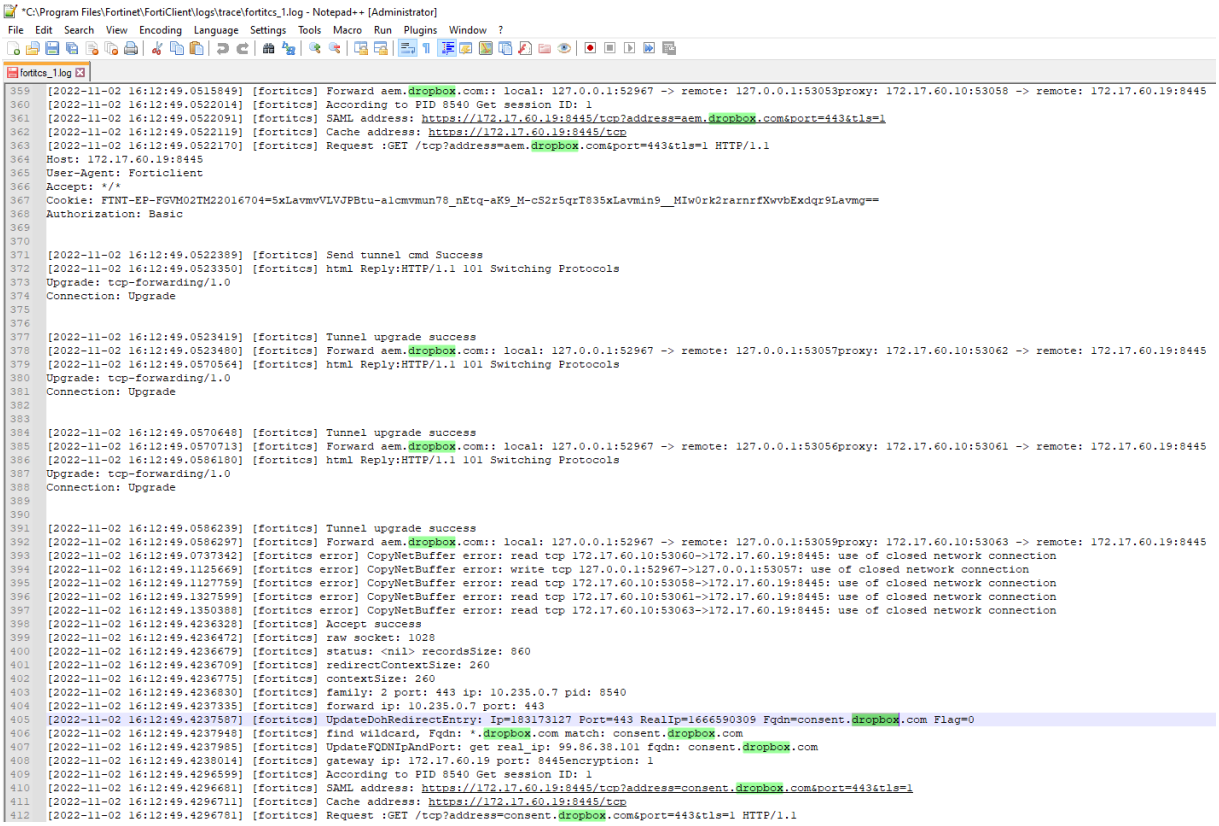
To configure a ZTNA rule for an FQDN in wildcard format using method 1:

1. In EMS, go to *Fabric & Connectors > ZTNA Applications Catalog*.
2. Click *Add*. Configure the following:
   a. Select *Wildcard FQDN*.
   b. Enter *.dropbox.com.
   c. Select *Port*, then enter 443.
   d. Beside the *Select Gateways* dropdown list, click *Add Gateway*.
   e. In the *Address* and *Port* fields, enter the FortiGate IP address and port. In this example, the value is 172.17.60.19:8445.
   f. Configure other fields as desired.
   g. Click *Finish*.
3. Go to *Endpoint Profiles > ZTNA Destinations*.
4. Select an existing profile or create a new one.
5. Under *Rules*, click *Add*.
6. Click *Create*.

7. Select the destination that you configured. Click *Finish*.
8. On an endpoint with the profile applied, attempt to access Dropbox in a browser. The browser displays a SAML authentication prompt. Provide the appropriate credentials to proceed to access Dropbox.



9. To troubleshoot this configuration, you can view the ZTNA debug log file (fortitcs_1.log) to confirm that all traffic requests to *.dropbox.com, such as to aem.dropbox.com or consent.dropbox.com, go through the ZTNA tunnel. You can also use the log to verify that FortiClient handles the request to *.dropbox.com.



Consider that it may be difficult to configure all URLs embedded in a website, such as *.dropbox.com.

To configure a ZTNA rule for an FQDN in wildcard format using method 2:

For this method, you do not need to configure a ZTNA rule as in the previous method. This method assumes that SSH and RDP TCP forwarding are configured on the FortiGate and continue to work. FortiClient pulls SSH and RDP rules from the FortiGate based on the EMS portal settings mapped to the FortiGate virtual access proxy server.

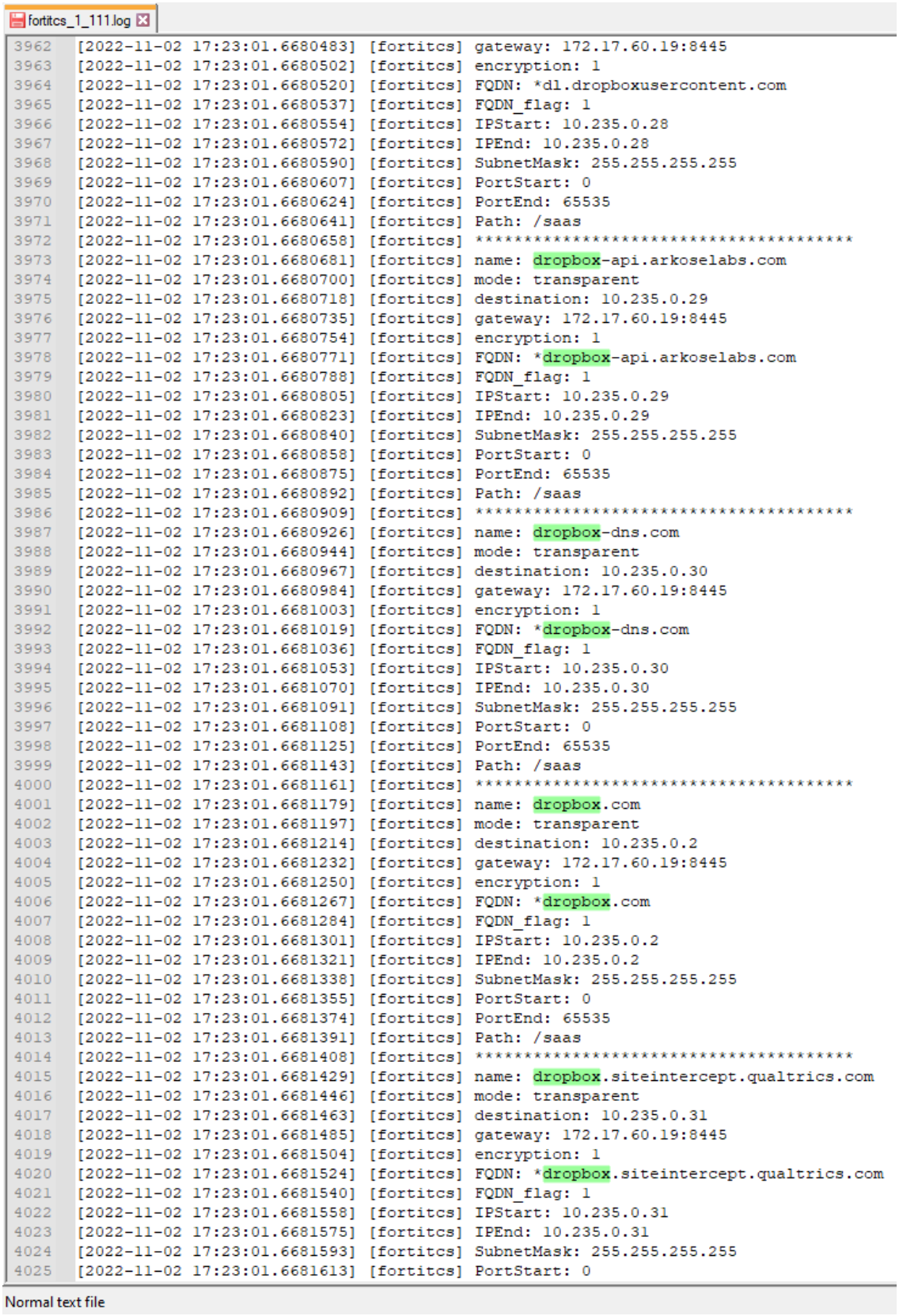
FortiClient actively queries FortiGate for ZTNA setting changes every 30 seconds and pulls changes as needed.

Configure the following in the FortiOS CLI:

```
config firewall access-proxy
   edit "ZTNA-tcp-server"
      set vip "ZTNA-tcp-server"
      set auth-portal enable
      config api-gateway
         edit 5
            set url-map "/saas"
            set service saas
            set application "dropbox"
         next
      end
   next
end
```

On the endpoint, clear the browser cache and FortiClient SAML cookies, then attempt to access Dropbox. The browser displays a SAML authentication prompt. Provide the appropriate credentials to proceed to access Dropbox.

To troubleshoot this configuration, you can view the ZTNA debug log file (fortitcs_1_111.log). FortiClient prints all related FQDNs for a defined application, in this case dropbox.com, and all related URLs contained in the website based on the ICDB signature to the ZTNA debug log. The ICDB signature file is in the FortiClient installation directory *vir_sig\icdb* in JSON format. FortiClient reads the related parts from the ICDB signature file-based SaaS/application settings in FortiOS and updates them if there are updates on the FortiOS side.

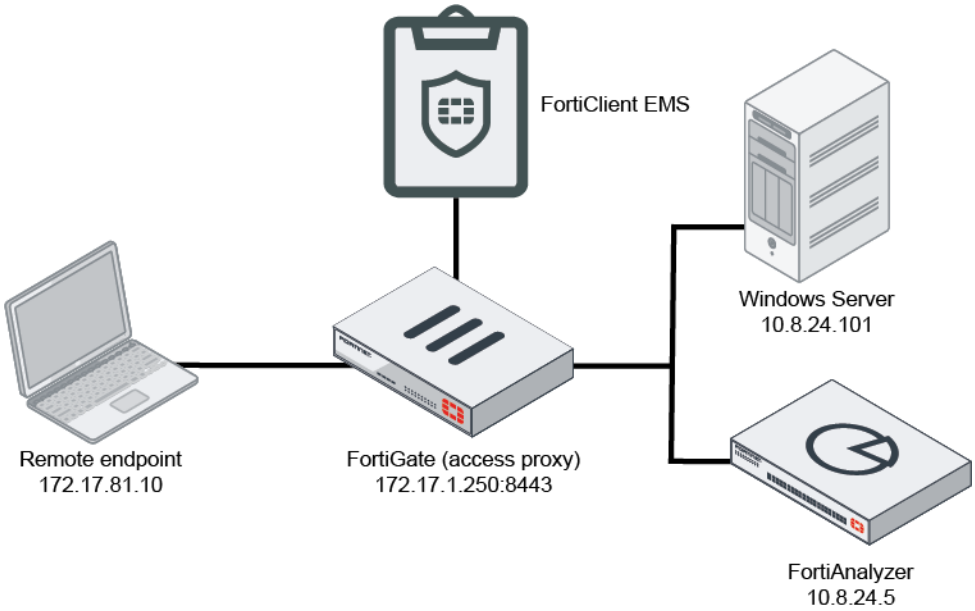

fortitcs_1_111.log
3962 [2022-11-02 17:23:01.6680483] [fortitcs] gateway: 172.17.60.19:8445
3963 [2022-11-02 17:23:01.6680502] [fortitcs] encryption: 1
3964 [2022-11-02 17:23:01.6680520] [fortitcs] FQDN: *dl.dropboxusercontent.com
3965 [2022-11-02 17:23:01.6680537] [fortitcs] FQDN_flag: 1
3966 [2022-11-02 17:23:01.6680554] [fortitcs] IPStart: 10.235.0.28
3967 [2022-11-02 17:23:01.6680572] [fortitcs] IPEnd: 10.235.0.28
3968 [2022-11-02 17:23:01.6680590] [fortitcs] SubnetMask: 255.255.255.255
3969 [2022-11-02 17:23:01.6680607] [fortitcs] PortStart: 0
3970 [2022-11-02 17:23:01.6680624] [fortitcs] PortEnd: 65535
3971 [2022-11-02 17:23:01.6680641] [fortitcs] Path: /saas
3972 [2022-11-02 17:23:01.6680658] [fortitcs] **
3973 [2022-11-02 17:23:01.6680681] [fortitcs] name: dropbox-api.arkoselabs.com
3974 [2022-11-02 17:23:01.6680700] [fortitcs] mode: transparent
3975 [2022-11-02 17:23:01.6680718] [fortitcs] destination: 10.235.0.29
3976 [2022-11-02 17:23:01.6680735] [fortitcs] gateway: 172.17.60.19:8445
3977 [2022-11-02 17:23:01.6680754] [fortitcs] encryption: 1
3978 [2022-11-02 17:23:01.6680771] [fortitcs] FQDN: *dropbox-api.arkoselabs.com
3979 [2022-11-02 17:23:01.6680788] [fortitcs] FQDN_flag: 1
3980 [2022-11-02 17:23:01.6680805] [fortitcs] IPStart: 10.235.0.29
3981 [2022-11-02 17:23:01.6680823] [fortitcs] IPEnd: 10.235.0.29
3982 [2022-11-02 17:23:01.6680840] [fortitcs] SubnetMask: 255.255.255.255
3983 [2022-11-02 17:23:01.6680858] [fortitcs] PortStart: 0
3984 [2022-11-02 17:23:01.6680875] [fortitcs] PortEnd: 65535
3985 [2022-11-02 17:23:01.6680892] [fortitcs] Path: /saas
3986 [2022-11-02 17:23:01.6680909] [fortitcs] **
3987 [2022-11-02 17:23:01.6680926] [fortitcs] name: dropbox-dns.com
3988 [2022-11-02 17:23:01.6680944] [fortitcs] mode: transparent
3989 [2022-11-02 17:23:01.6680967] [fortitcs] destination: 10.235.0.30
3990 [2022-11-02 17:23:01.6680984] [fortitcs] gateway: 172.17.60.19:8445
3991 [2022-11-02 17:23:01.6681003] [fortitcs] encryption: 1
3992 [2022-11-02 17:23:01.6681019] [fortitcs] FQDN: *dropbox-dns.com
3993 [2022-11-02 17:23:01.6681036] [fortitcs] FQDN_flag: 1
3994 [2022-11-02 17:23:01.6681053] [fortitcs] IPStart: 10.235.0.30
3995 [2022-11-02 17:23:01.6681070] [fortitcs] IPEnd: 10.235.0.30
3996 [2022-11-02 17:23:01.6681091] [fortitcs] SubnetMask: 255.255.255.255
3997 [2022-11-02 17:23:01.6681108] [fortitcs] PortStart: 0
3998 [2022-11-02 17:23:01.6681125] [fortitcs] PortEnd: 65535
3999 [2022-11-02 17:23:01.6681143] [fortitcs] Path: /saas
4000 [2022-11-02 17:23:01.6681161] [fortitcs] **
4001 [2022-11-02 17:23:01.6681179] [fortitcs] name: dropbox.com
4002 [2022-11-02 17:23:01.6681197] [fortitcs] mode: transparent
4003 [2022-11-02 17:23:01.6681214] [fortitcs] destination: 10.235.0.2
4004 [2022-11-02 17:23:01.6681232] [fortitcs] gateway: 172.17.60.19:8445
4005 [2022-11-02 17:23:01.6681250] [fortitcs] encryption: 1
4006 [2022-11-02 17:23:01.6681267] [fortitcs] FQDN: *dropbox.com
4007 [2022-11-02 17:23:01.6681284] [fortitcs] FQDN_flag: 1
4008 [2022-11-02 17:23:01.6681301] [fortitcs] IPStart: 10.235.0.2
4009 [2022-11-02 17:23:01.6681321] [fortitcs] IPEnd: 10.235.0.2
4010 [2022-11-02 17:23:01.6681338] [fortitcs] SubnetMask: 255.255.255.255
4011 [2022-11-02 17:23:01.6681355] [fortitcs] PortStart: 0
4012 [2022-11-02 17:23:01.6681374] [fortitcs] PortEnd: 65535
4013 [2022-11-02 17:23:01.6681391] [fortitcs] Path: /saas
4014 [2022-11-02 17:23:01.6681408] [fortitcs] **
4015 [2022-11-02 17:23:01.6681429] [fortitcs] name: dropbox.siteintercept.qualtrics.com
4016 [2022-11-02 17:23:01.6681446] [fortitcs] mode: transparent
4017 [2022-11-02 17:23:01.6681463] [fortitcs] destination: 10.235.0.31
4018 [2022-11-02 17:23:01.6681485] [fortitcs] gateway: 172.17.60.19:8445
4019 [2022-11-02 17:23:01.6681504] [fortitcs] encryption: 1
4020 [2022-11-02 17:23:01.6681524] [fortitcs] FQDN: *dropbox.siteintercept.qualtrics.com
4021 [2022-11-02 17:23:01.6681540] [fortitcs] FQDN_flag: 1
4022 [2022-11-02 17:23:01.6681558] [fortitcs] IPStart: 10.235.0.31
4023 [2022-11-02 17:23:01.6681575] [fortitcs] IPEnd: 10.235.0.31
4024 [2022-11-02 17:23:01.6681593] [fortitcs] SubnetMask: 255.255.255.255
4025 [2022-11-02 17:23:01.6681613] [fortitcs] PortStart: 0
Normal text file

In this configuration, FortiClient depends on ICDB signatures being updated properly. In the case, FortiClient automatically and dynamically updates and refreshes the FQDNs if there are any changes in the SaaS applications as defined in FortiOS. FortiClient also pulls SSH/RDP/SMBA settings and specific FQDNs including rules using wildcard formats from FortiOS, if available.

FQDN-based ZTNA TCP forwarding services

FortiClient supports using fully qualified domain names (FQDN) as destination hosts in zero trust network access (ZTNA) TCP forwarding destinations. This allows you to avoid exposing private/internal IP addresses to end users by using FQDNs instead.

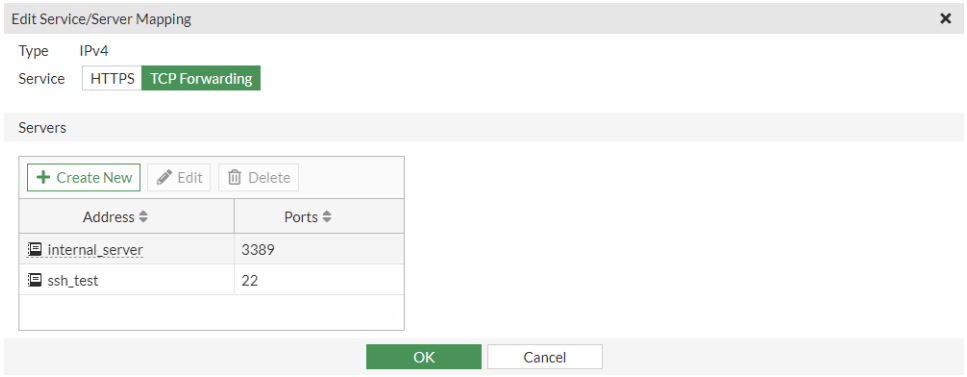
The following shows the topology for this example. This example uses two FQDNs, rdp.win.test and ssh.win.test, in place of the Windows server IP address, 10.8.24.100. This hides the internal IP address, 10.8.24.100, from end users.



To configure FortiOS:

1. In FortiOS, go to *Policy & Objects* > *ZTNA* > *ZTNA Servers*.
2. Click *Create New*.
3. For *Type*, select *IPv4*.
4. For *Service*, select *TCP Forwarding*.

5. Under *Servers*, configure RDP and SSH services.



6. Click *OK*.
7. In the CLI, add the rdp.win.test FQDN to RDP and SSH services as the domain:

```
config firewall access-proxy
    edit "ZTNA-test"
        set vip "ZTNA-test"
        set client-cert enable
        config api-gateway
            edit 2
                set url-map "/tcp"
                set service tcp-forwarding
                config realservers
                    edit 1
                        set address "internal_server"
                        set domain "rdp.win.test"
                        set mappedport 3389
                    next
                    edit 2
                        set address "ssh_test"
                        set domain "ssh.win.test"
                        set mappedport 22
                    next
                end
            next
        end
    next
end
```

8. Ensure that you have configured the ZTNA policy rule and firewall policy as desired.

To configure ZTNA destinations:

You can configure ZTNA destinations from EMS or FortiClient. Using EMS is the recommended method. If using FortiClient, connect to the EMS that is connected to the FortiGate acting as the TCP forwarding server.

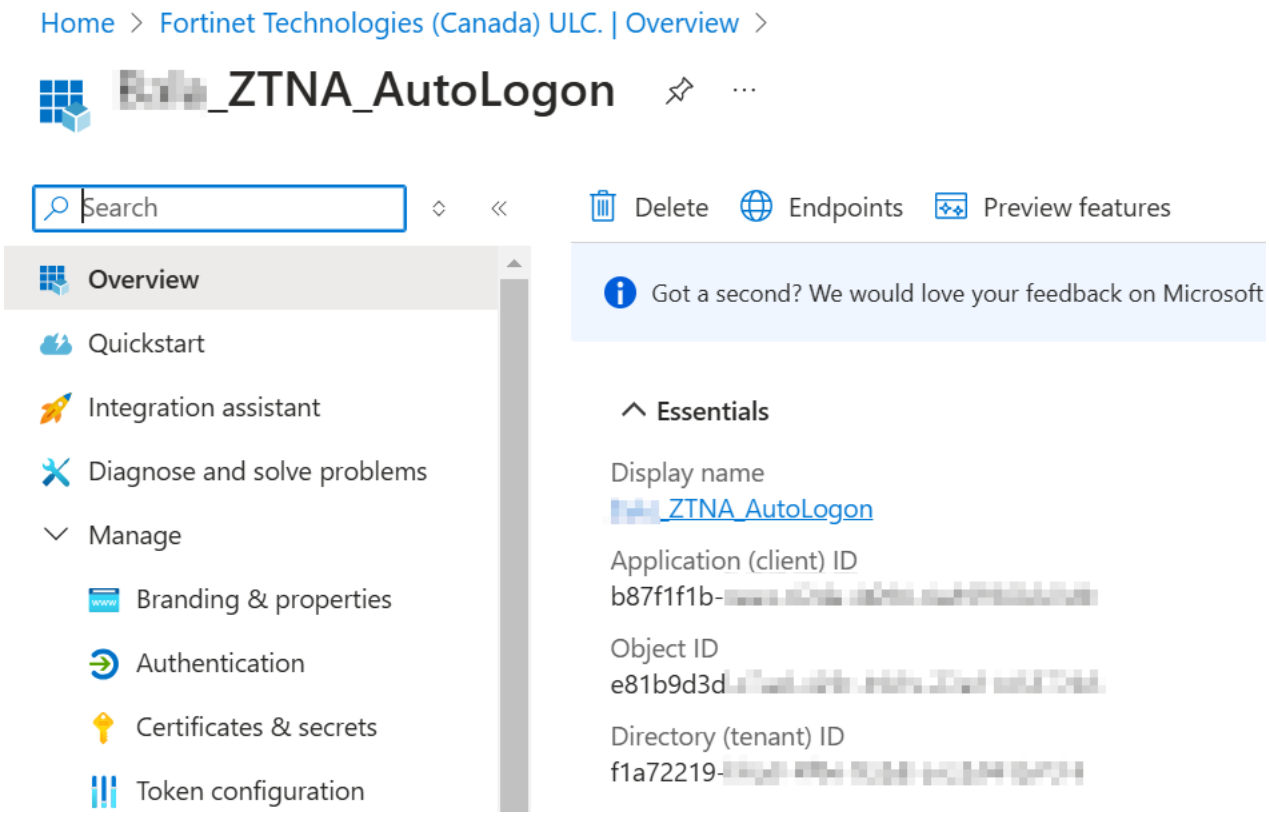
1. Go to *Fabric & Connectors > ZTNA Applications Catalog*.
2. Create the RDP ZTNA application:
   a. Click *Add*.
   b. Select *FQDN*, then enter rdp.win.test. This field does not support entering a hostname.
   c. Select *Port*, then enter the desired port number.
   d. Click *Add Gateway*.
   e. In the *Address* and *Port* fields, enter the FortiGate IP address and port number. In this example, it is 172.17.81.250:8443.
   f. Click *Create*.
   g. Configure other fields as desired, then click *Finish*.
3. Create the SSH server rule:
   a. Click *Add*.
   b. Select *FQDN*, then enter ssh.win.test. This field does not support entering a hostname.
   c. Select *Port*, then enter the desired port number.
   d. Click *Add Gateway*.
   e. In the *Address* and *Port* fields, enter the FortiGate IP address and port number. In this example, it is 172.17.81.250:8443.
   f. Click *Create*.
   g. Configure other fields as desired, then click *Finish*.
4. Go to *Endpoint Profiles > ZTNA Destinations*.
5. Create a new profile or edit an existing one.
6. Under *Rules*, click *Add*.
7. Select the applications that you configured. Click *Finish*.
8. Configure the profile as desired, and click *Save*.

ZTNA automatic login using Microsoft Entra ID

When a user is logged in to an Entra ID domain on an endpoint then attempts to access zero trust network access (ZTNA) TCP-forwarding traffic, FortiClient automatically authenticates with the FortiGate using the Entra ID credentials. This simplifies the user experience by eliminating the need for manual authenticate.

This feature requires FortiOS 7.6.1 or a later version.

The following instructions assume that you have configured a FortiClient enterprise application in the Entra ID portal.



In this example, the application has the following values which you configure in the FortiClient ZTNA Destinations profile:

Entra ID portal field	Corresponding FortiClient XML profile element	Value
Application (client) ID	`<client_id>`	`b87f1f1b...`
Directory (tenant) ID	`<tenant_name>`	`f1a72219...`

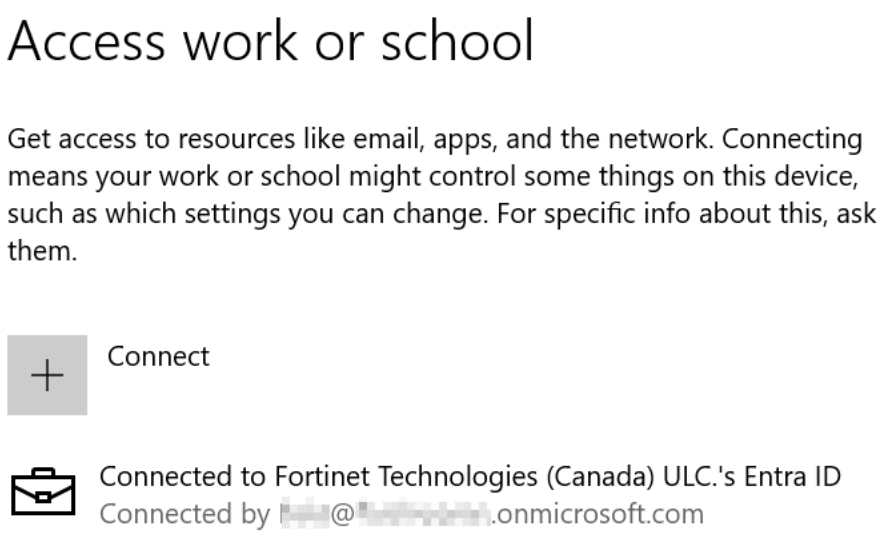
To configure ZTNA automatic login using Entra ID:

1. In FortiOS, run the following commands to configure support for this feature. Lines bolded in the CLI sample highlight key commands to support this feature:

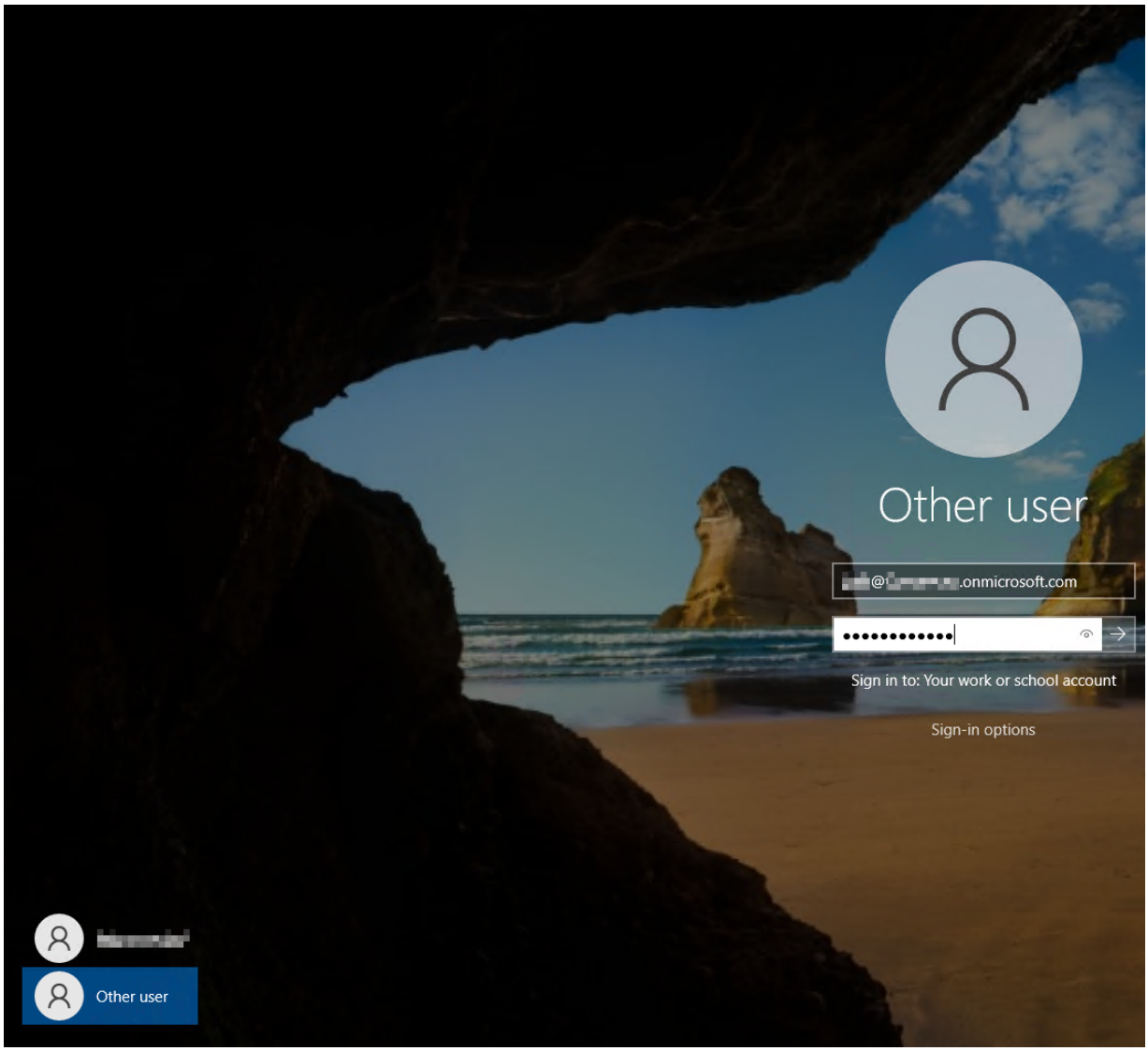
```
config user external-identity-provider
    edit "eip1"
        set type ms-graph
        set version v1.0
    next
end
config user group
    edit "Autologon"
        set member "eip1"
    next
end
```

```
config authentication scheme
    edit "Autologon"
        set method entra-sso
        set external-idp "eip1"
    next
end
config authentication rule
    edit "Auth"
        set srcintf "port1"
        set srcaddr "all"
        set ip-based disable
        set sso-auth-method "Autologon"
        set web-auth-cookie enable
    next
end
```

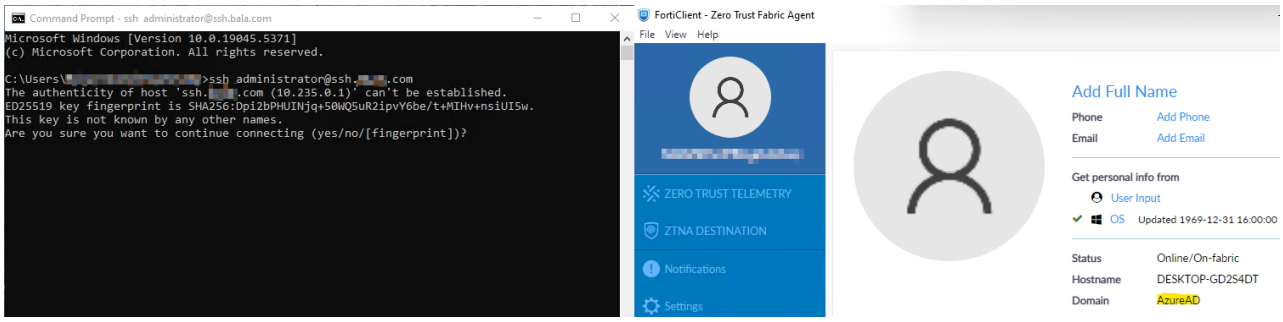
2. In EMS, configure support for this feature:
   a. Go to *Endpoint Profiles > ZTNA Destinations*.
   b. Create a new profile or edit an existing one.
   c. Enable *Enable Azure Auto Login* and specify the tenant name and client ID of the application used to connect with EMS that you collected from the Azure management console.
   d. Configure other options as needed. See ZTNA Destinations on page 307 for more details.
3. Connect the endpoint to the Entra ID domain:
   a. Go to *Settings > Access work or school > Join this device to Microsoft Entra ID*.
   b. Log in with your Entra ID credentials.
   c. Confirm that the endpoint connected successfully.



4. Log out, then log in to Windows using the Entra ID credentials.



5. Connect FortiClient to EMS.
6. Click the avatar. In the *Domain* field, confirm that the endpoint is joined to Entra ID (previously known as Azure Active Directory).
7. Go to the *ZTNA Destination* tab to confirm that FortiClient received the desired ZTNA Destinations profile from EMS.
8. Attempt to access a ZTNA destination. In this example, the user attempts to access an SSH TCP forwarding destination. The user can access the protected resource without authentication since FortiClient automatically authenticated with the FortiGate using the provided Entra ID credentials.



Web Filter

For Windows, macOS, and Linux profiles, you must enable *FortiProxy (Disable Only When Troubleshooting)* on the *System Settings* tab to use the *Web Filter* options.

Configuration	Description
Web Filter	Enable web filtering. Enable or disable the eye icon to show or hide this feature from the end user in FortiClient.
Scheduling	Enable to have Web Filter settings only take effect during the configured schedule. This feature functions based on the system time in EMS. Time changes on the endpoint do not affect this feature.
Days of Week	From the dropdown list, select the days of the week for the schedule.
All Day	If desired, enable *All Day* to schedule Web Filter settings to take effect all day long on the selected days of the week.
Start At	Select the desired time for the Web Filter settings to start on the selected days of the week. This option is not available if you select *All Day*.
End At	Select the desired time for the Web Filter settings to end on the selected days of the week. This option is not available if you select *All Day*.
Fallback Action	Select the desired action for Web Filter to take for web traffic outside of the scheduled times. • When you configure *Fallback Action* as *Allow*, FortiClient allows all web access on the endpoint, including categories that Web Filter is set to block during the schedule timeframe. • When you configure *Fallback Action* as *Block*, FortiClient blocks all web access on the endpoint, excluding URLs that you have configured to be allowed in the blocklist.

Configuration		Description
General		
Request Timeout		Configure the desired timeout value in seconds for a Web Filter site rating request to FortiGuard times out. You can configure a value between 1 to 30 seconds.
Enable WebFiltering on FortiClient		Select *Always On* to enable client web filtering when on-fabric. Select *Only When Endpoint is Off-Fabric* to enable Web Filter on endpoints only when the endpoint is considered off-Fabric. See On-fabric Detection Rules on page 124.
Keep Extension When Endpoint is Off-Fabric		If disabled, the FortiClient Web Filter extension is uninstalled when the endpoint goes from being on- to off-net. For Firefox, the Web Filter extension is not automatically uninstalled, due to the Firefox default behavior. Instead, you can manually remove the extension. This is a Firefox limitation.
Log All URLs		When you disable this setting, FortiClient only logs URLs as specified by per-category or per-URL settings. FortiClient only logs these logs locally or sends them to FortiAnalyzer if configured.
Log User Initiated Traffic		Log only user-initiated traffic.
Action On HTTPS Site Blocking		• *Display In-Browser Message* • *Fail Connection & Show Bubble Notification* • *Fail Connection*
Enable Web Browser Plugin for HTTPS Web Filtering		Enable a web browser plugin for HTTPS web filtering. This improves detection and enforcement of Web Filter rules on HTTPS sites. When you enable this option, the user must open the browser to approve installing the new plugin. EMS only installs the web browser plugin for the Google Chrome, Mozilla Firefox, and Microsoft Edge browsers on Windows platforms. If HTTP/3 is enabled on the browser or device, you must enable this option to ensure Web Filter is applied.
	Sync Mode	The web browser waits for a response from an HTTPS request before sending another HTTPS request.
	Check User Initiated Traffic Only	Use the web browser plugin for only user-initiated traffic. This allows for faster processing. When this option is disabled, FortiClient checks all URL requests.
	Enforce WF plugin permission in private browsing	Configure whether to force run the FortiClient Web Filter extension in incognito or private mode:

Configuration	Description
	 As Chrome and Edge explicitly prevent extensions from silently enabling extension access in Incognito for user privacy and security, when this option is enabled, Chrome and Edge users must manually enable an option in the browser to allow running the FortiClient Web Filter extension for Incognito (private browsing). FortiClient cannot force enable the FortiClient Web Filter extension for Incognito in Chrome and Edge.
	Enabled • **(Firefox)** The FortiClient Web Filter extension will be active in incognito or private mode. • **(Chrome or Edge)** Users will be prompted to enable the option in the browser to allow running the FortiClient Web Filter extension for Incognito. If the user does not enable the option in the browser as requested, Internet access will be disabled completely for both regular and private browsing.
	Disabled The FortiClient Web Filter extension will not run in Incognito. Web Filter will not apply to websites accessed in Incognito.
Enable Safe Search	For Windows endpoints and Chromebooks, when enabling Safe Search, you can configure the Restriction Level to Strict or Moderate. This setting affects the content that endpoint users can access via YouTube and search engine, including Google and Bing. For Chromebooks, to set YouTube access to Unrestricted, you can disable Safe Search and configure Google Search and YouTube access with the Google Admin Console instead of FortiClient EMS. For macOS endpoints, enabling Safe Search sets the endpoint's Google search to Restricted mode and YouTube access to Strict Restricted access. Enabling Safe Search adds records, including Yandex.ru, to the client device's hosts file in order to redirect search engine requests. You can enable Safe Search on the Video Filter and Web Filter profiles. When Safe Search is enabled on both profiles, the more restrictive settings are applied to YouTube.

Configuration	Description
Wildcard Match Root Domain	FortiClient applies wildcard matching to the sites in the exclusion list, even if they are not configured with wildcard characters. For example, if you configured office365.com in the exclusion list and enable *Wildcard Match Root Domain*, FortiClient excludes (.*\.)?office365\.com. Enabling *Wildcard Match Root Domain* causes the exclusion list to include subdomains such as outlook.office365.com.
Bypass Private IP	Enable bypassing private IP addresses. This feature is enabled by default.
Enable HTTPS Deep Inspection	Toggle to enable or disable HTTPS deep inspection on FortiClient (macOS) and (Linux) endpoints. When you enable HTTPS deep inspection, FortiClient can proxy HTTPS requests and rate whole HTTPS URL requests. Otherwise, FortiClient can only rate domain URLs for HTTPS requests.
Site Categories	Enable site categories from FortiGuard. When you disable site categories, the exclusion list protects FortiClient. See the FortiGuard website for descriptions of the available categories and subcategories. For all categories, you can configure an action for the entire site category by selecting one of the following: • Block • Warn • Allow • Monitor  Only events of the *Block* and *Warn* categories are displayed in the All Events on page 89 page and Endpoints pane. You can also click the + button beside the site category to view all subcategories and configure individual actions (Block, Warn, Allow, Monitor) for each subcategory. The following lists each site category's subcategories.
Adult/Mature Content	• Abortion • Advocacy Organizations • Alcohol • Alternative Beliefs • Dating • Gambling • Lingerie and Swimsuit • Marijuana • Nudity and Risque

Configuration	Description
	• Other Adult Materials • Pornography • Sex Education • Sports Hunting and War Games • Tobacco • Weapons (Sales)
Bandwidth Consuming	• File Sharing and Storage • Freeware and Software Downloads • Internet Radio and TV • Internet Telephony • Peer-to-peer File Sharing • Streaming Media and Download
General Interest-Business	• Armed Forces • Business • Charitable Organizations • Finance and Banking • General Organizations • Government and Legal Organizations • Information Technology • Information and Computer Security • Online Meeting • Remote Access • Search Engines and Portals • Secure Websites • Web Analytics • Web Hosting • Web-based Applications

Configuration	Description
General Interest-Personal	• Advertising • Arts and Culture • Auction • Brokerage and Trading • Child Education • Content Servers • Digital Postcards • Domain Parking • Dynamic Content • Education • Entertainment • Folklore • Games • Global Religion • Health and Wellness • Instant Messaging • Job Search • Meaningless Content • Medicine • News and Media • Newsgroups and Message Boards • Personal Privacy • Personal Vehicles • Personal Websites and Blogs • Political Organizations • Real Estate • Reference • Restaurant and Dining • Shopping • Social Networking • Society and Lifestyles • Sports • Travel • Web Chat • Web-based Email

Configuration	Description
Potentially Liable	• Child Sexual Abuse • Crypto Mining • Discrimination • Drug Abuse • Explicit Violence • Extremist Groups • Hacking • Illegal or Unethical • Plagiarism • Potentially Unwanted Program • Proxy Avoidance • Terrorism
Security Risk	• Dynamic DNS • Malicious Websites • Newly Observed Domain • Newly Registered Domain • Phishing • Spam URLs
Unrated	Sites that FortiGuard categorizes as unrated. If FortiClient receives an unrated IP address for specific cloud applications that FortiGuard categorizes as unrated, it may use the Internet Service Database (ISDB) as a backup. You can expand the *Unrated* category for cloud applications, and click *Add* to configure an action for selected cloud applications using ISDB. In the *Add Cloud Application* dialog, select the desired cloud application, configure the desired action, then click *Add*.
Rate IP Addresses	Have FortiClient request the rating of the site by URL and IP address separately, providing additional security against attempts to bypass the FortiGuard Web Filter. If the rating determined by the domain name and the rating determined by the IP address differ, a weighting assigned to the different categories determines the action that FortiClient enforces. The higher weighted category takes precedence in determining the action. This has the side effect that sometimes the classification based on the domain name determines the action and other times the classification that is based on the IP address determines the action. FortiGuard Web Filter ratings for IP addresses are not updated as quickly as ratings for URLs. This can sometimes cause FortiClient to allow access to sites that should be blocked, or to block sites that should be allowed.

Configuration	Description
	An example of how this works is if a URL's rating based on the domain name indicates that it belongs in the category Lingerie and Swimsuit, which is allowed but the category assigned to the IP address was Pornography which has an action of Block, because the Pornography category has a higher weight, the effective action is Block.
Use HTTPS Rating Server	By default, Web Filter sends URL rating requests to the FortiGuard rating server via UDP protocol. You can instead enable Web Filter to send the requests via TCP protocol.
Allow websites when rating error occurs	Configure the action to take with all websites when FortiGuard is temporarily unavailable. This may occur when an endpoint is forced to access a network via a captive portal. FortiClient takes the configured action until contact is reestablished with FortiGuard. Available options are: • Block: Deny access to any websites. This may prevent endpoints from accessing captive portals. • Warn: Display in-browser warning to user, with an option to proceed to the website • Allow: Allow full, unfiltered access to all websites • Monitor: Log the site access

FortiGuard Server Location	Configure the FortiGuard server location. If *FortiGuard Anycast* is selected for the *Server* field, you can select from global, U.S., or Europe. If *FortiGuard* is selected for the *Server* field, you can select from global or U.S. When *Global* is selected, FortiClient uses the closest FortiGuard server.
	FortiClient connects to FortiGuard to query for URL ratings.
	The URLs connected to for each server location are as follows:
	• FortiGuard:
	  • Global: fgd1.fortigate.com
	  • U.S.: usfgd1.fortigate.com
	• FortiGuard Anycast:
	  • Global: fctguard.fortinet.net
	  • U.S.: fctusguard.fortinet.net
	  • Europe: fcteuguard.fortinet.net

FortiGuard Server Type	Configure the FortiGuard server to *FortiGuard* or *FortiGuard Anycast*.
Keyword Scanning on Search Engine	Use rating categories from FortiGuard to allow, block, or monitor searches for certain terms. This feature is only available for Chromebooks.
Banned Word Search	Enable to configure actions (block or monitor) to take when the user searches for terms that belong to the following categories:

Configuration	Description
	• Violence/Terrorism • Extremist • Pornography • Cyber Bullying • Self Harm
Custom Banned Words	Configure actions for individual terms. Enable *Custom Banned Words*, type the desired term in the *Add Word* field, then click *Add Word*. Configure the action for the term (*Block*, *Monitor*, or *Allow*), then toggle the *Status* to *On*. You can remove a term from the *Custom Banned Word* list by selecting the checkbox beside the term, then clicking the *Remove Word* button. The custom term may belong to a category under *Banned Word Search*. If the action configured for the category under *Banned Word Search* and the action configured for the term under *Custom Banned Words* differ, EMS applies the action configured under *Custom Banned Words*.
Remote Categories	Displays remote categories imported from a FortiGate or FortiManager Web Filter profile. You can configure an action for a category and view the URLs associated with each category. See Syncing remote categories from imported FortiOS or FortiManager Web Filter profile on page 334.
Exclusion List	Adding more than 1000 exclusions is not recommended and can cause EMS instability.
Action	Select one of the following actions: • *Allow* • *Block* • *Monitor* • *Warn*  Only events of the *Block* and *Warn* actions are displayed in the All Events on page 89 page and Endpoints pane.
URL	Enter specific URLs to allow, block, monitor, or warn. You can provide the full URL or only the domain name.
Referrer/Host	Enter a specific referrer or host to allow, block, or monitor. You can provide the full URL or only the domain name. If the end user visits the URL through the referrer provided, EMS considers the rule a match and applies the specified action.

Configuration	Description
	If the end user visits the URL directly or through a different referrer, EMS does not consider the rule a match and does not apply the specified action. This option is only available for FortiClient Windows, macOS, Linux, and Chromebooks.
Type	Select one of the following types: • *Simple* • *Wildcard* • *Regular Expression* You can use wildcard characters and Perl Compatible Regular Expressions. This field only applies to the value in the *URL* field and does not apply to the value in the *Referrer/Host* field.
Move this rule up/Move this rule down	Move the exclusion rule up or down in the list. If multiple exclusion rules are applicable, EMS applies the first applicable exclusion rule.



You cannot configure Web Filter to block the Chrome web store URL, as it is a critical resource to download the FortiClient Web Filter extension. FortiClient can access the Chrome web store URL regardless of the Web Filter configuration.

Importing a Web profile from FortiOS or FortiManager

You can import a Web Filter profile from FortiOS or FortiManager into FortiEndpoint, then synchronize the Web Filter profile settings to an endpoint profile in FortiEndpoint.

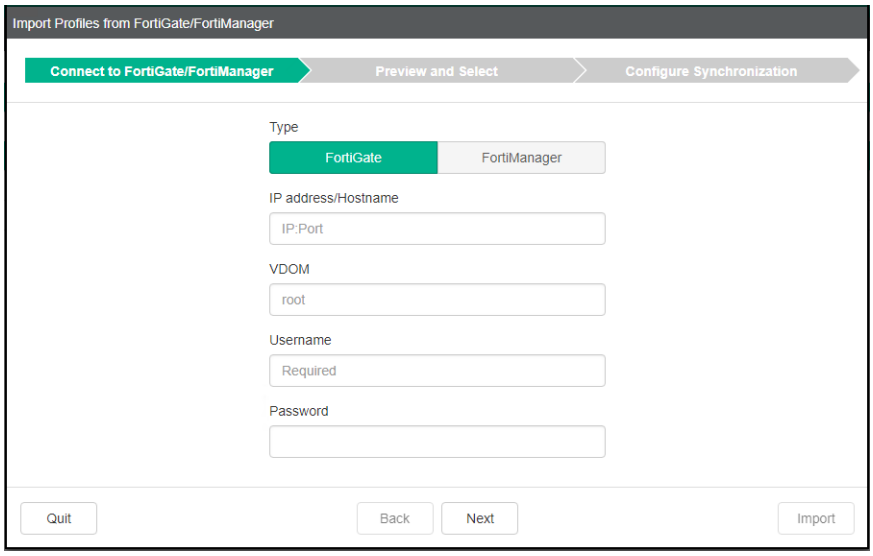
This feature is only available if Web Filter is enabled in *Feature Select*. See Feature Select on page 555.

To import a Web Filter profile:

1. Configure FortiOS or FortiManager to allow EMS profile importation:
   a. If using FortiOS, go to *Network* > *Interfaces*, select the desired port, and under *Administrative Access*, enable the *HTTPS* checkbox.
   b. If using FortiManager, do the following:
      i. Go to *System Settings* > *Network* and enable the *HTTPS* checkbox under *Administrative Access*.
      ii. You must set Remote Procedure Call to `read`. Run the `get system admin user admin` command. Ensure that `rpc-permit` is set to `read`.
      iii. If `rpc-permit` is not set to `read`, run the following commands:

```
config system admin user
   edit "admin"
      set rpc-permit read
end
```

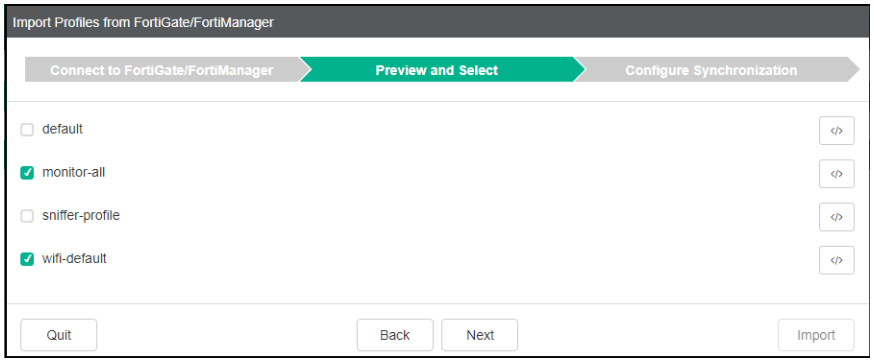
2. Go to *Endpoint Profiles* > *Import from FortiGate / FortiManager*. Click *Import from FortiGate / FortiManager*.



3. Under *Type*, select *FortiGate* or *FortiManager*.
4. Complete the following options, and click *Next*.

IP address/Hostname	Enter the IP address and port of the FortiGate or FortiManager from which you are importing the profile, in the format: `<ip address>:<port>`.
VDOM	Enter a VDOM name from the FortiGate or FortiManager if applicable.
Username	Enter a username for the FortiGate or FortiManager.
Password	Enter the password for the user account entered above.

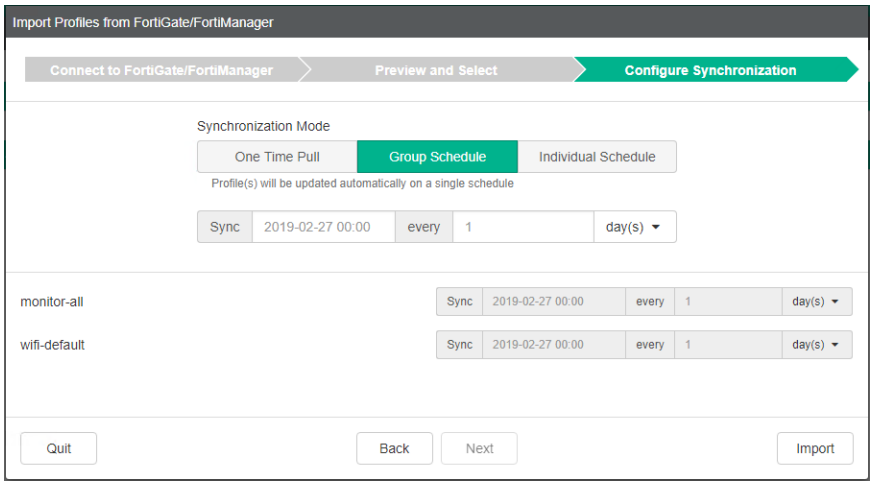
The list of Web Filter profiles configured on the FortiGate or FortiManager displays.



You can click the </> icon beside each profile to preview the settings in XML format.

5. Select the profiles to import into FortiEndpoint and click *Next*.

6. Under *Synchronization Mode*, select one of the following options.



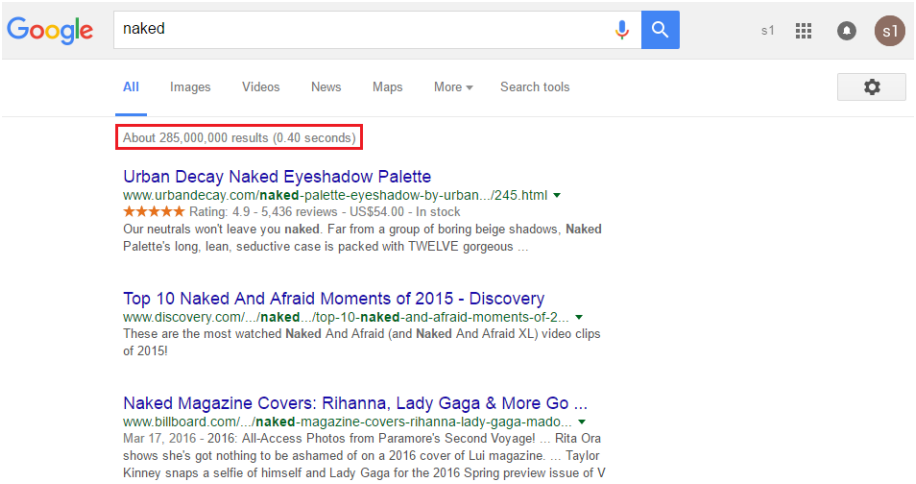
   a. *One Time Pull*: FortiEndpoint does not automatically sync profile changes from the FortiGate or FortiManager. You can manually sync profile changes after importing the profile. See Syncing profile changes on page 133.
   b. *Group Schedule*: Configure a group synchronization schedule for all selected profiles. Select the next date and time to automatically update the profiles, and the profile update interval in days, hours, or minutes.
   c. *Individual Schedule*: Configure an individual synchronization schedule for each selected profile. Select the next date and time to automatically update each profile, and the profile update interval in days, hours, or minutes.
7. Click *Import*. EMS imports the selected profiles and displays them in *Endpoint Profiles > Import from FortiGate/FortiManager* in a group named after the FortiGate or FortiManager that you imported them from. You can now configure an EMS endpoint profile to synchronize Web Filter settings from the imported FortiGate or FortiManager Web Filter profile. See Web Filter on page 320.
8. After importing the profile, you can synchronize the profile from the FortiGate or FortiManager on-demand by selecting the profile, then clicking *Sync Now*.

Enabling and disabling Safe Search

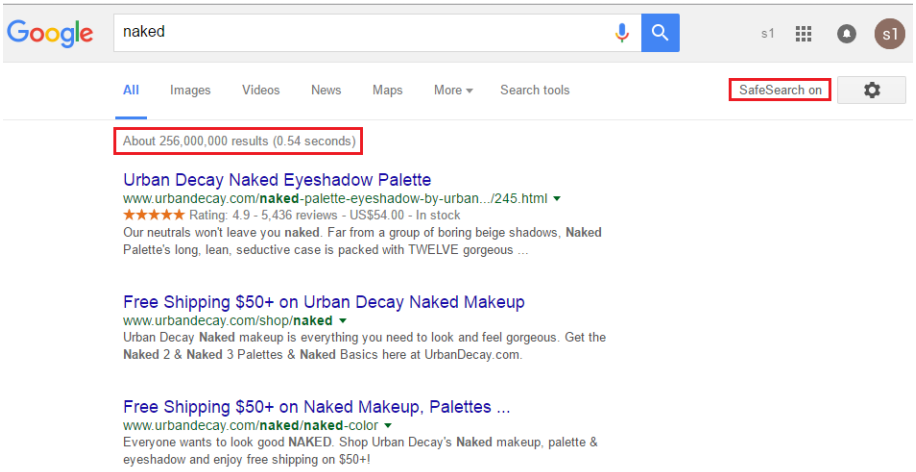
The search engine provides a Safe Search feature that blocks inappropriate or explicit images from search results. The Safe Search feature helps avoid most adult content. FortiEndpoint supports Safe Search for most common search engines, such as Google, Yahoo, and Bing.

The profile in FortiEndpoint controls the Safe Search feature.

Following are examples of search results with the Safe Search feature disabled and enabled. Notice the difference between the number of results. Here are the search results when the Safe Search feature is disabled, which has about 285000000 results:



Here are the search results when the Safe Search feature is enabled, which has about 256000000 results.



To enable or disable Safe Search:

1. In FortiEndpoint, in the *Endpoint Profiles > Manage Profiles* area, click the *Default - Chromebooks* profile or another profile.
2. On the *Web Filter* tab, enable or disable *Enable Safe Search*.

You can enable Safe Search on the Video Filter and Web Filter profiles. When Safe Search is enabled on both profiles, the more restrictive settings are applied to YouTube

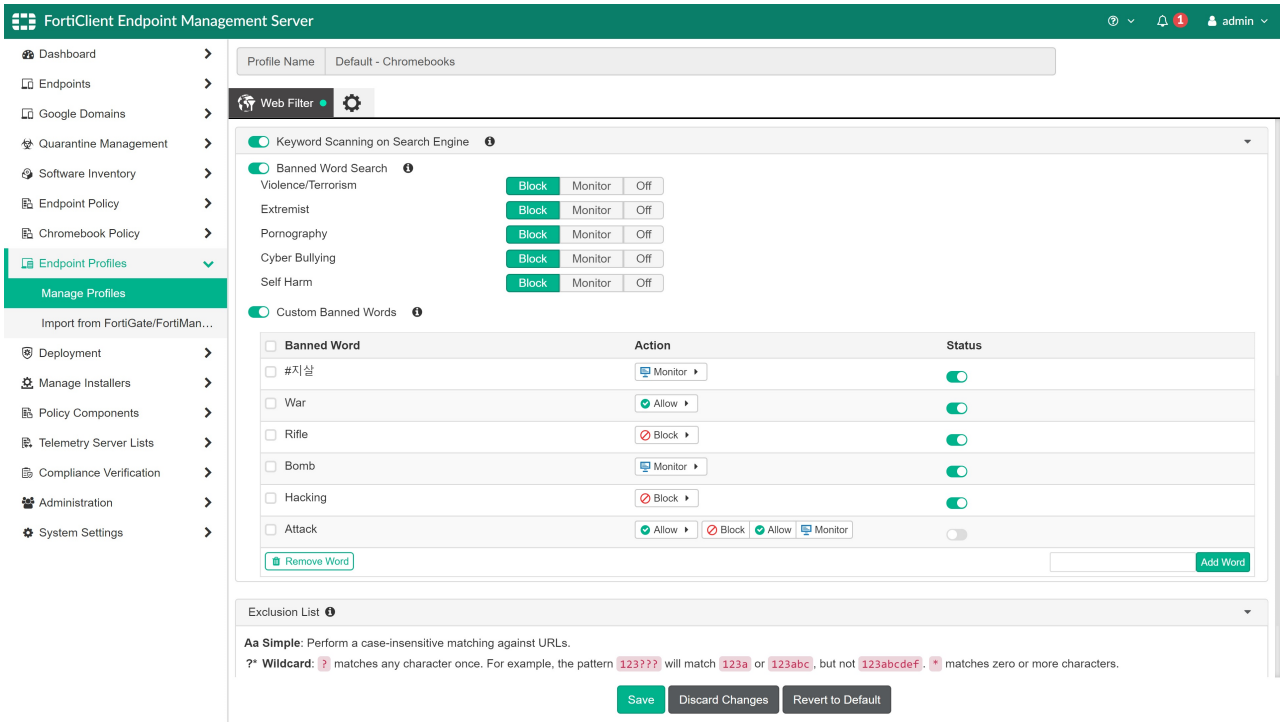
Configuring banned word check in URL

You can configure keyword scanning on search engines for Chromebook endpoints. EMS has a content safeguard service-provided file with a list of words in various languages for different categories. *Keyword Scanning on Search Engine* supports monitoring and blocking searches for banned words that users perform in popular search engines. You can use this feature to protect students from inappropriate and malicious content.

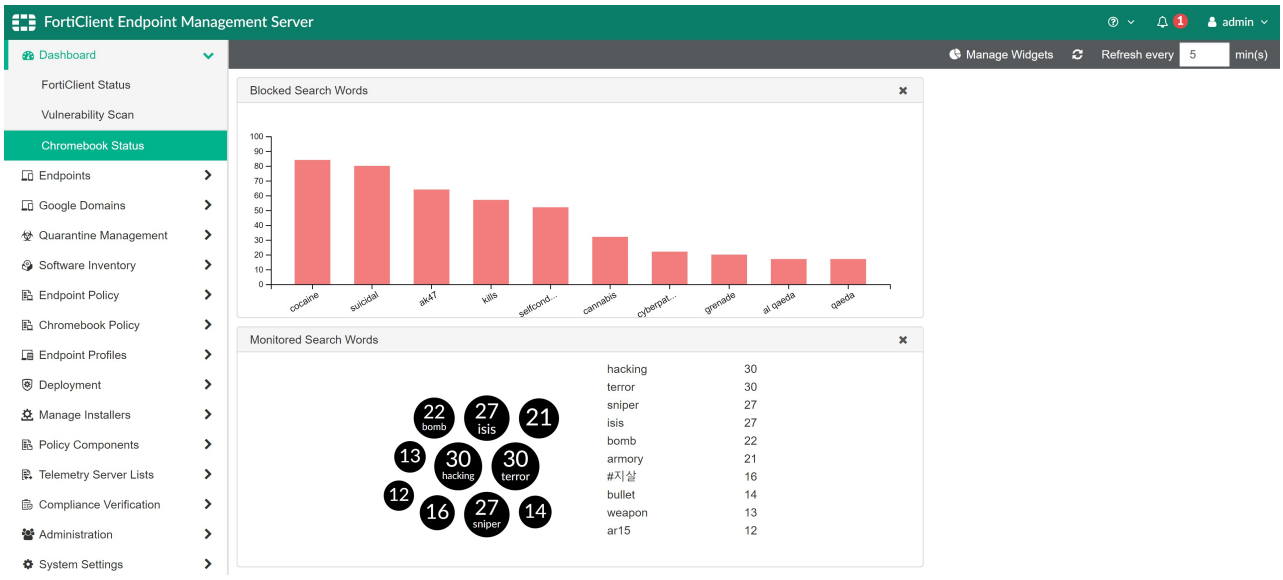
To enable keyword scanning on search engines:

1. In EMS, go to *Endpoint Profiles*. Select the desired Chromebook profile, or create a new one.
2. Enable *Keyword Scanning on Search Engine*.
3. Configure the following features:

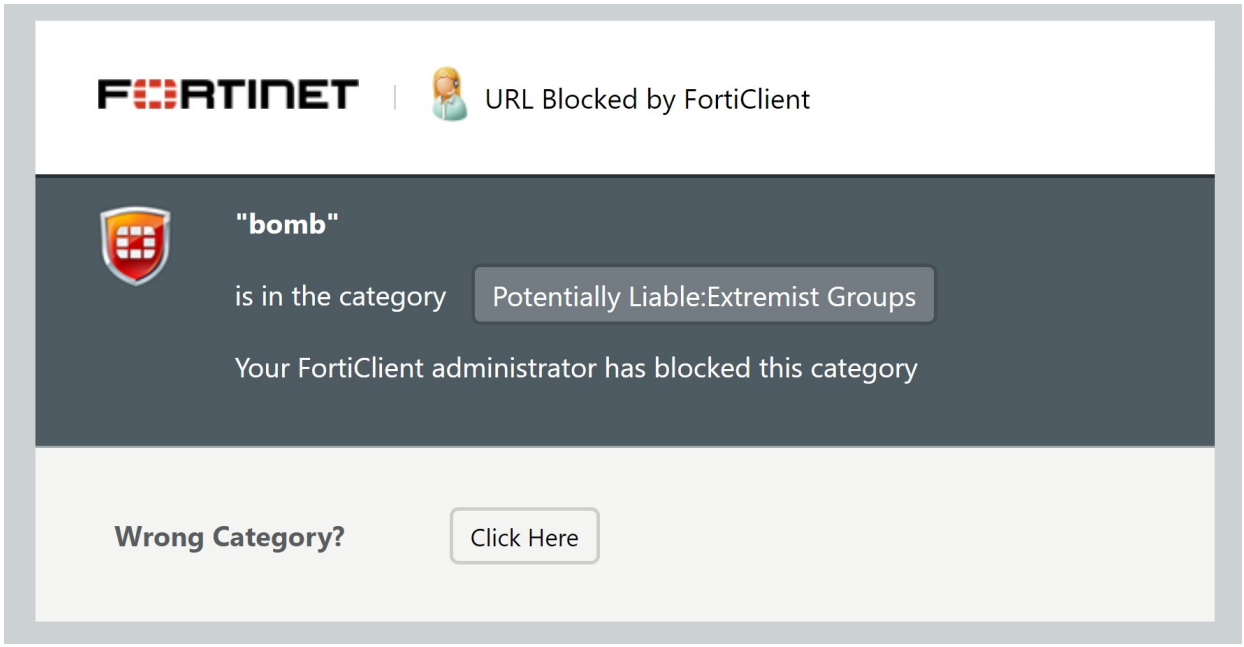
Banned Word Search	Enable to configure actions (block or monitor) to take when the user searches for terms that belong to the following categories: • Violence/Terrorism • Extremist • Pornography • Cyber Bullying • Self Harm
Custom Banned Words	Configure actions for individual terms. Enable *Custom Banned Words*, type the desired term in the *Add Word* field, then click *Add Word*. Configure the action for the term (*Block*, *Monitor*, or *Allow*), then toggle the *Status* to *On*. You can remove a term from the *Custom Banned Word* list by selecting the checkbox beside the term, then clicking the *Remove Word* button. The custom term may belong to a category under *Banned Word Search*. If the action configured for the category under *Banned Word Search* and the action configured for the term under *Custom Banned Words* differ, EMS applies the action configured under *Custom Banned Words*.



You can view user statistics on the *Blocked Search Words* and *Monitored Search Words* widgets in *Dashboard > Chromebook Status*.



When the user searches for a banned word, they see the following. In the example, the user searched for "bomb", which belongs to the Extremist category.



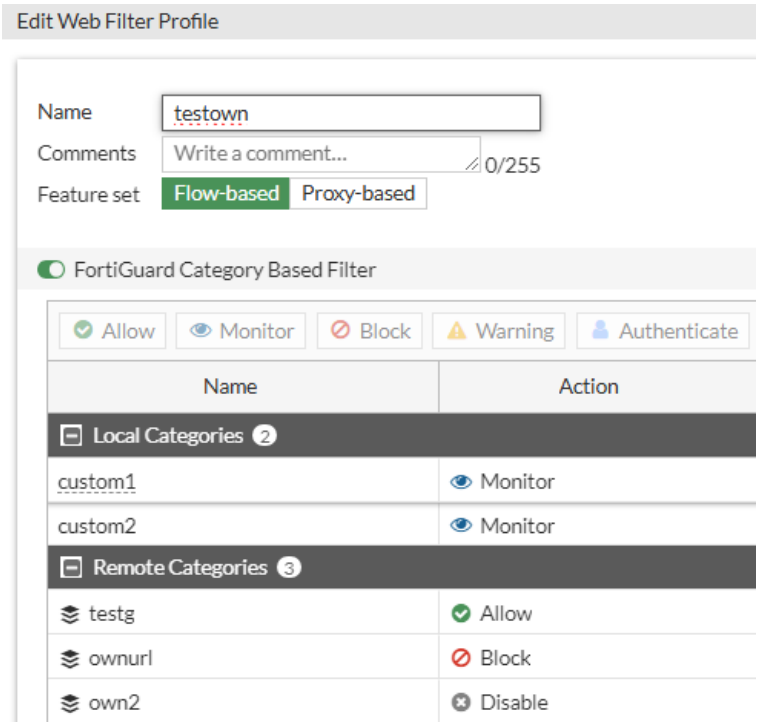
Syncing remote categories from imported FortiOS or FortiManager Web Filter profile

Web Filter profiles imported from FortiOS or FortiManager to EMS now include *FortiGuard Category Based Filter > Remote Categories*. Endpoints that are assigned this profile can follow this URL filter list to block outbound connections to known malicious URLs and domains. In EMS, remote the remote categories display the profile name, URL list, and the configured action for this URL list: allow, monitor, or block. Prior to this

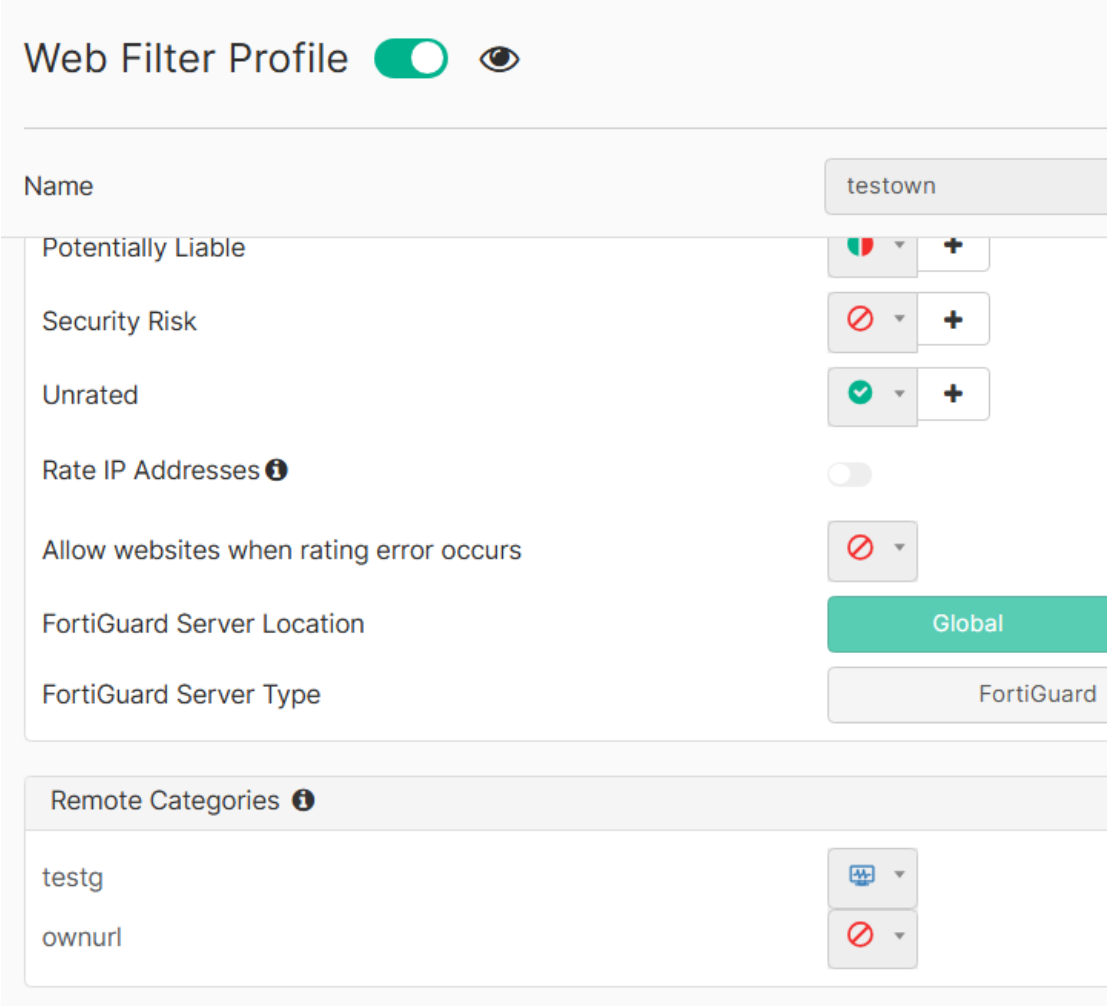
enhancement, customers manually updated the FortiOS static URL filter list, which was time-consuming, error-prone, and inconvenient.

To import a Web Filter profile with remote categories from FortiOS to EMS:

1. Configure the Web Filter profile in FortiOS:
   a. Configure a FortiGuard category threat feed to populate the FortiGuard remote categories for the desired Web Filter profile. See FortiGuard category threat feed.
   b. Go to *Security Profiles* > *Web Filter*.
   c. Create a new profile or edit an existing one.
   d. Under *FortiGuard Category Based Filter* > *Remote Categories*, configure the desired actions for the categories from the threat feed. If you set a category action to *Disable*, EMS does not import it. Save.



2. Import the profile to EMS and deploy it to endpoints:
   a. In EMS, go to *Endpoint Profiles* > *Web Filter*.
   b. Click *Import* > *Import from FortiGate / FortiManager*.
   c. Configure the FortiGate fields as required, then click *Next*.
   d. Select the desired profile to import. Click *Next*.
   e. Select the desired synchronization mode for the profile. Click *Import*.
   f. Edit the imported Web Filter profile. Confirm that *Remote Categories* displays with the same categories and actions as seen in FortiOS. In this example, EMS did not import the own2 category as its action is set to *Disable* in FortiOS. You can click the category name to view the associated URLs.



g. Go to *Endpoint Policy & Components*.
h. Create a new policy or edit an existing one.
i. From the *Profile > WF* dropdown list, select the imported profile. Save.

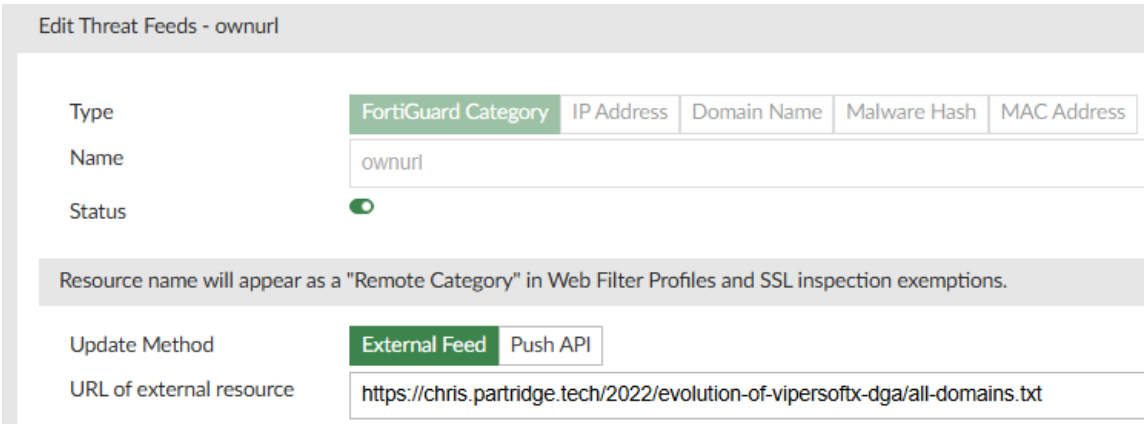
3. On an endpoint that received the updated profile, confirm that FortiClient applies the configured action to a URL in the remote category list. The block page displays the category name.
4. On EMS, in *Endpoints > All Endpoints*, select the endpoint.
5. On the *Web Filter Events* tab, you can view the blocked URL events for that category.
6. If desired, in FortiOS, you can configure exempt URLs in a Web Filter profile under *Static URL Filter*.
7. After this profile is imported to EMS, you can view the exclusion list. You cannot modify it as it can only be modified from FortiOS.



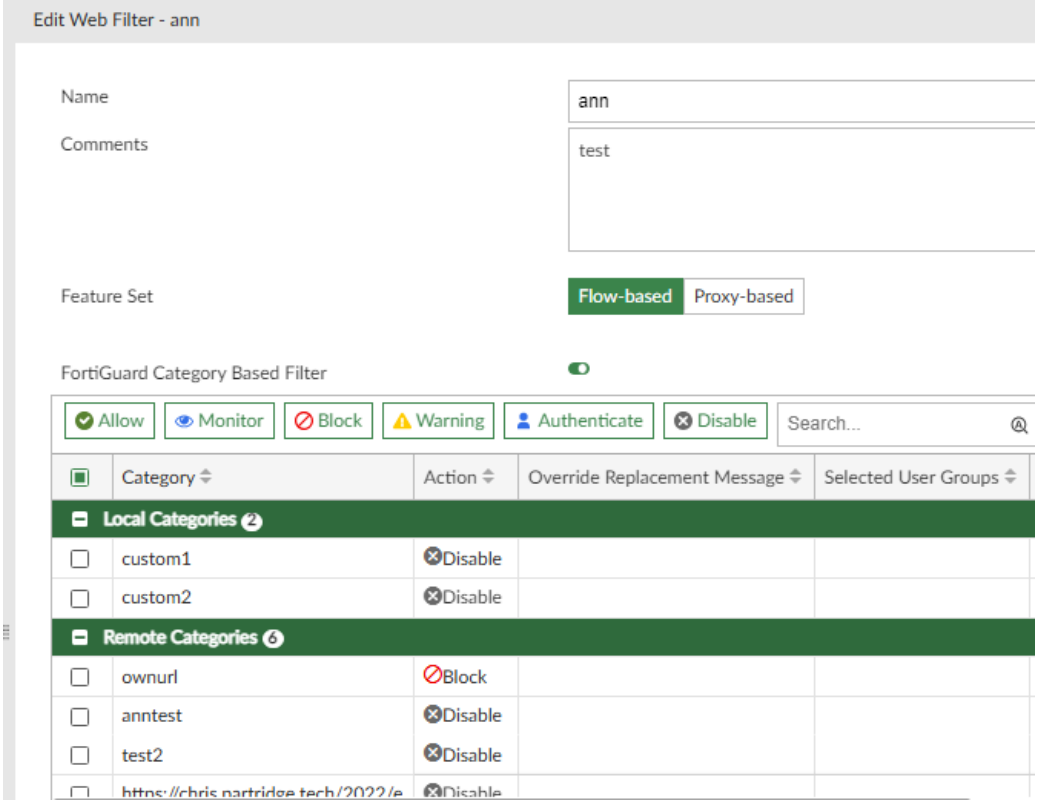
To import a Web Filter profile with remote categories from FortiManager to EMS:

The procedure for importing a Web Filter profile with remote categories from FortiManager to EMS is almost identical to importing such a profile from FortiOS.

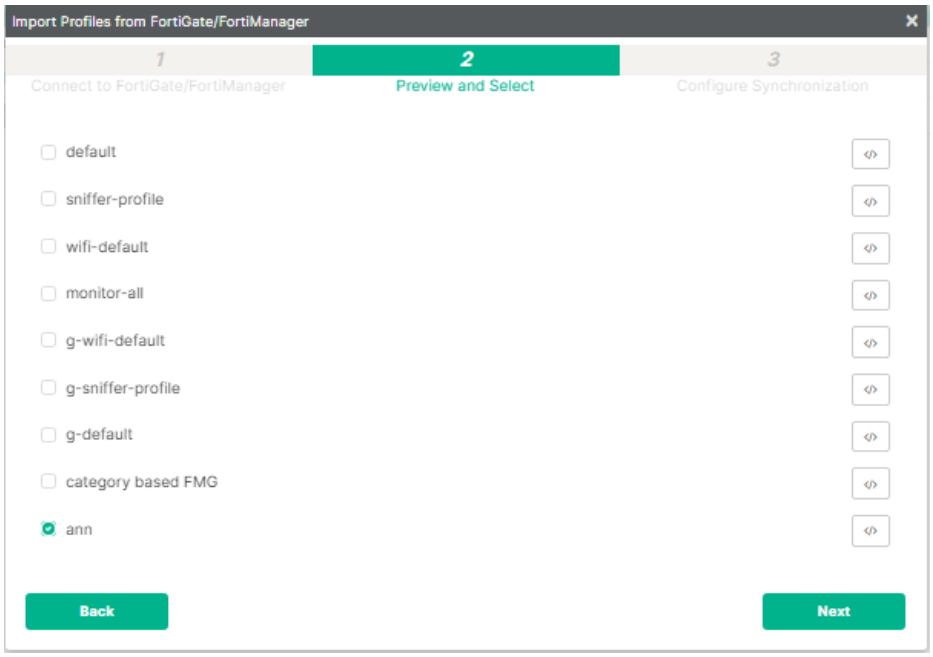
1. In FortiManager, configure the following:
   a. Configure a threat feed as Creating threat feed connectors describes. Use the following values:
      i. For *Type*, select *FortiGuard Category*.
      ii. For *Update Method*, select *External Feed*.
      iii. In the *URL of external resource* field, enter a URL that points to a text file with the relevant URLs listed.



   b. Go to *Policy & Objects* > *Security Profiles*.
   c. Create a Web Filter profile or edit an existing one.
   d. Under *FortiGuard Category Based Filter* > *Remote Categories*, configure the desired actions for the categories from the threat feed. If you set a category action to *Disable*, EMS does not import it. Save.



2. Import the profile to EMS and deploy it to endpoints:
   a. In EMS, go to *Endpoint Profiles* > *Web Filter*.
   b. Click *Import* > *Import from FortiGate / FortiManager*.
   c. Configure the FortiManager fields as required, then click *Next*.
   d. Select the desired profile to import. Click *Next*.



   e. Select the desired synchronization mode for the profile. Click *Import*.

f. Edit the imported Web Filter profile. Confirm that *Remote Categories* displays with the same categories and actions as seen in FortiManager. You can click the category name to view the associated URLs.
g. Go to *Endpoint Policy & Components*.
h. Create a new policy or edit an existing one.
i. From the *Profile > WF* dropdown list, select the imported profile. Save.

3. On an endpoint that received the updated profile, confirm that FortiClient applies the configured action to a URL in the remote category list. The block page displays the category name.
4. On EMS, in *Endpoints > All Endpoints*, select the endpoint.
5. On the *Web Filter Events* tab, you can view the blocked URL events for that category.
6. If desired, in FortiManager, you can configure exempt URLs in a Web Filter profile under *Static URL Filter*.
7. After this profile is imported to EMS, you can view the exclusion list. You cannot modify it as it can only be modified from FortiManager.

Using Referrer Host on Windows, macOS, Linux, and Chromebooks

You can define exclusions based on the referrer host (source) URL on FortiClient Windows, macOS, Linux, and Chromebooks using the *Referrer Host* option in EMS (see Web Filter on page 320) or the `<referrer>` XML option.

```
<urls>
       <url>
               <action>allow</action>
               <type>simple</type>
               <address>youtube.com</address>
               <referrer>google.com</referrer>
        </url>
</urls>
```

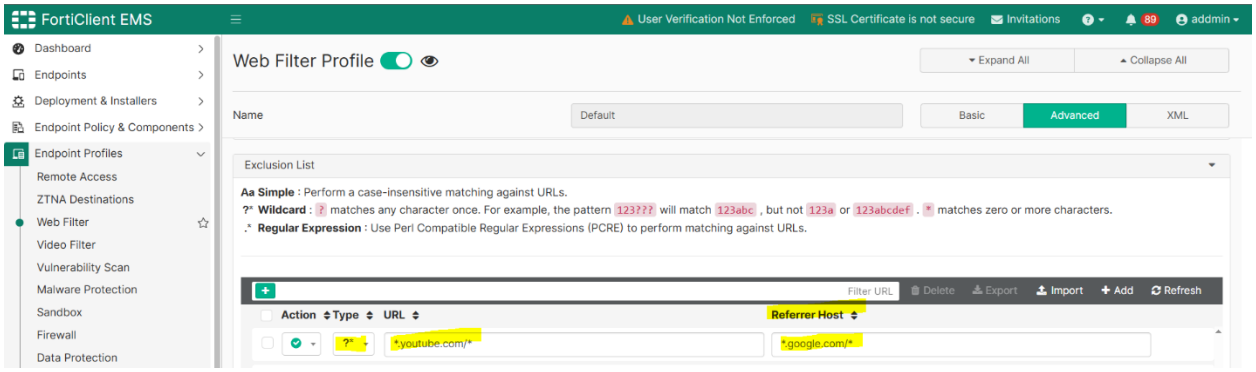
As opposed to allowing a site regardless of how the user reaches it (using the destination URL pattern), admins can block direct access attempts while ensuring that legitimate searches via allowed referrers are permitted. For example, admins can allow YouTube videos when accessed through Google search results while blocking direct access to YouTube. This provides more precise control, reduces the risk of unwanted content access, and helps maintain a better security posture while keeping user access flexible.

Example

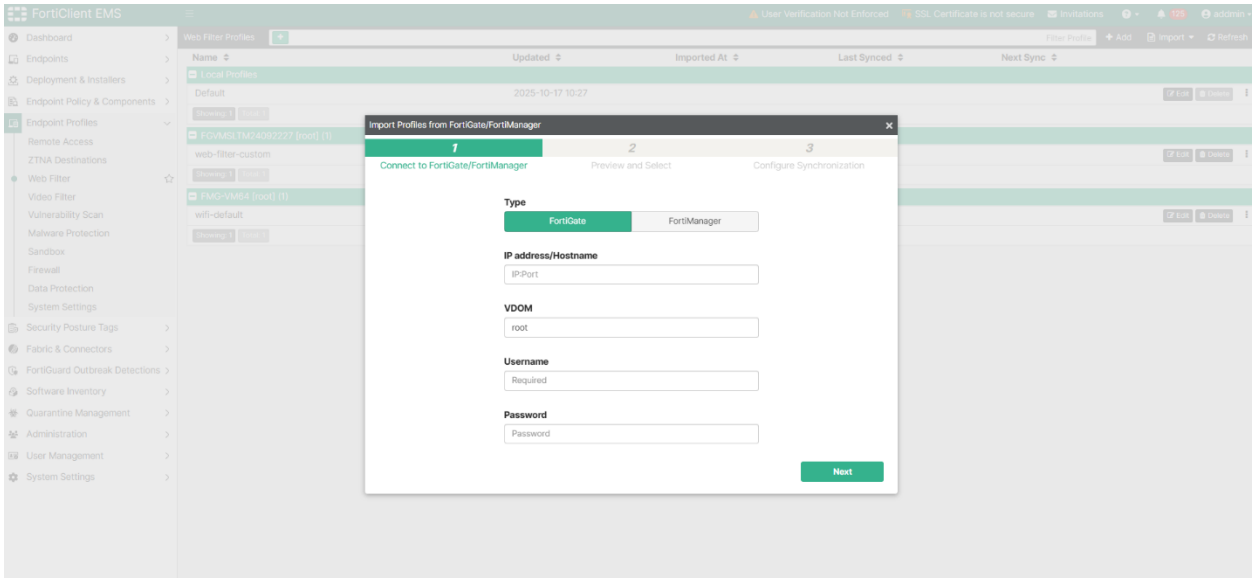
An organization wants to allow access to YouTube videos only when users open them through Google search results but not when they visit YouTube directly.

1. Navigate to *Endpoint Profiles > Web Filter*.
2. Create a new profile or edit an existing one.
3. Block category *Bandwidth Consuming* and make sure *Web Browser Plugin for Web Filtering* is enabled.
4. Scroll down to *Exclusion List* and add a *Web Filter* exclusion on EMS with *Referrer Host* defined:
   - URL: *.youtube.com/*
   - Referrer Host: *.google.com/*

- Type: Wildcard
- Action: Allow



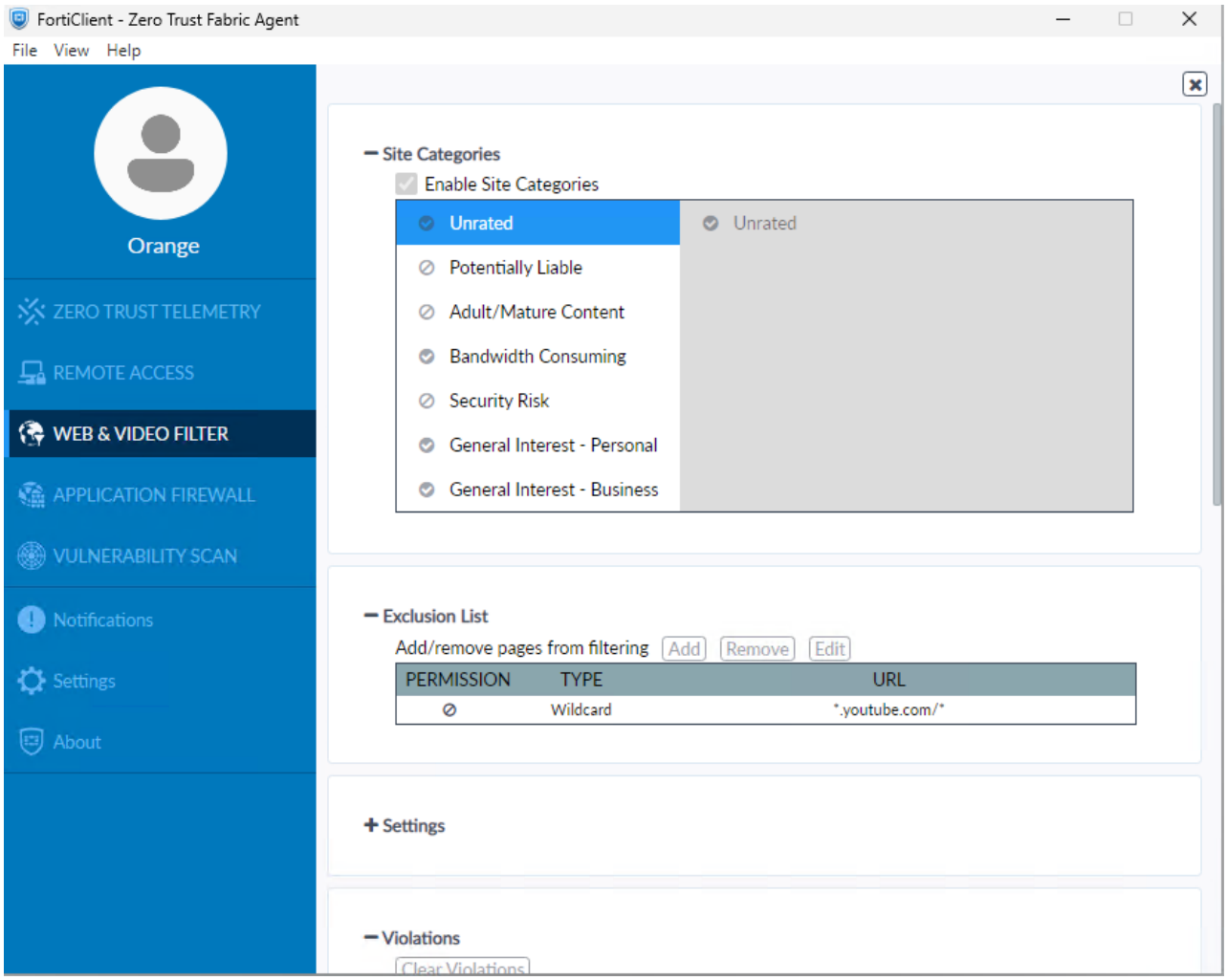
Alternatively, you can click Import to import an existing exclusion list from FortiManager or FortiGate with the referrer already defined.



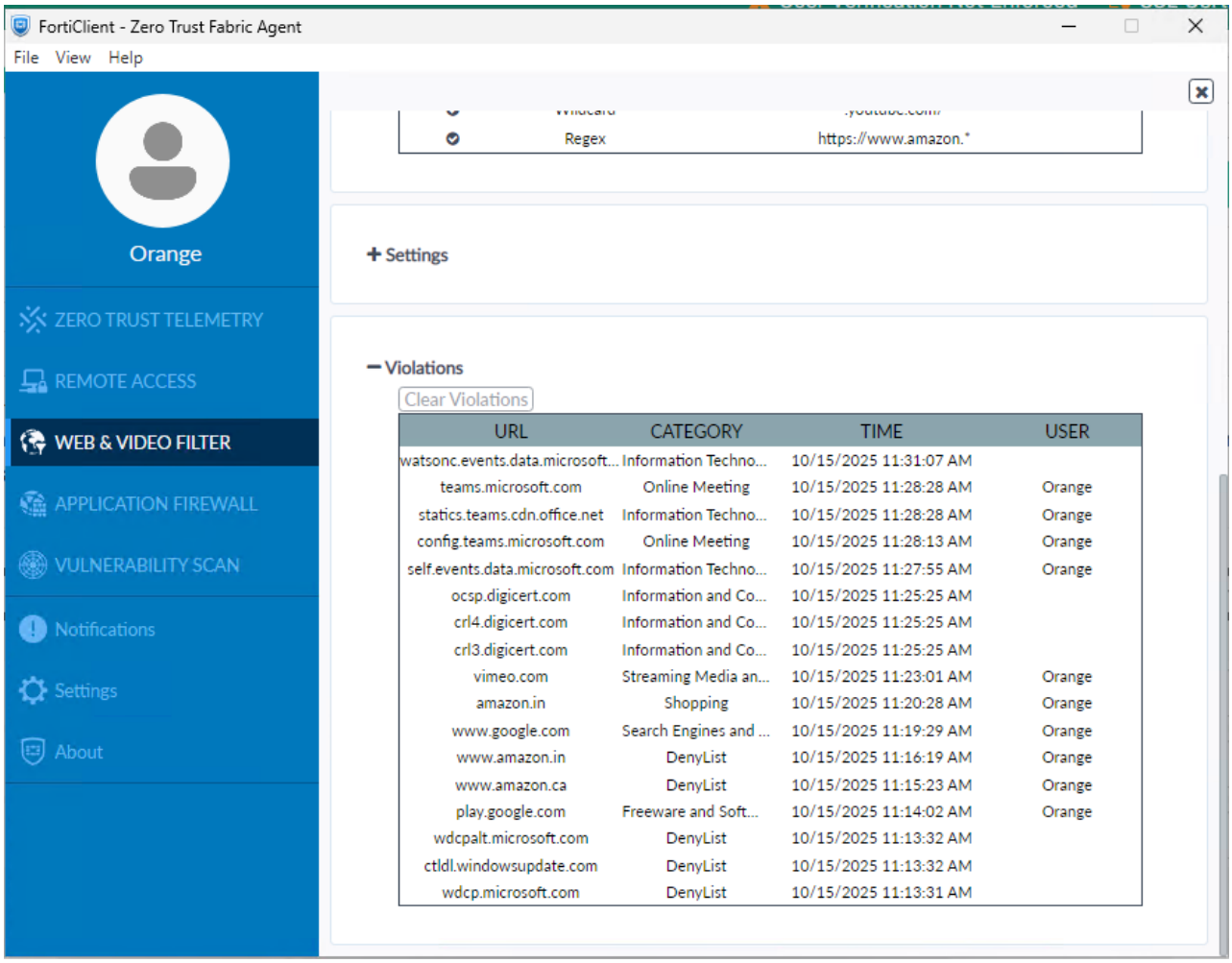


Referrer-based exclusions imported from FortiGate or FortiManager work exactly as configured on FortiGate or FortiManager. The entries cannot be modified from EMS GUI or XML for integrity.

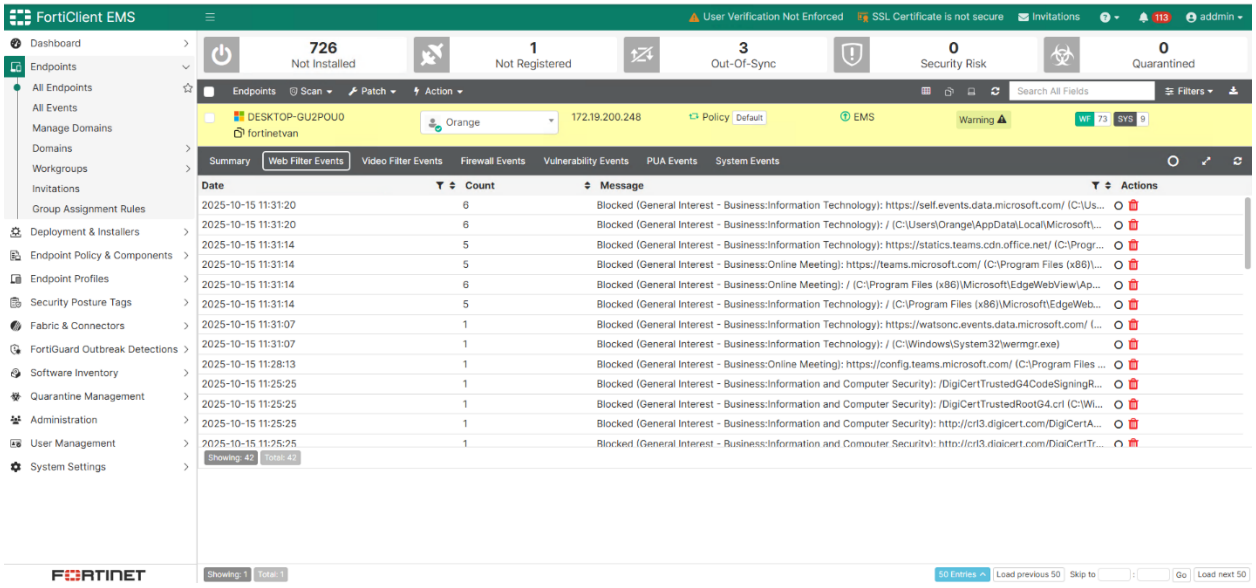
5. Save the profile and deploy it to relevant endpoints.
6. On an endpoint, open FortiClient and verify that the configured exclusion list is visible under the *Web & Video Filter* tab after syncing from the EMS.
7. Open any browser on the endpoint and verify that *web filter extension* is imported.



8. Try accessing `youtube.com` directly and it should be blocked.
9. Try searching for something on Google (e.g., “how to fix Wi-Fi”) and play the video directly from the Google search results. It should play successfully.
10. Go to the *Violations* section in the FortiClient GUI and verify that the attempt to access a blocked site directly (or via an untrusted referrer) is logged.



11. Go to EMS and verify that violations are also logged for that specific endpoint:



Video Filter

This feature requires the Web Filter profile and *Enable Web Browser Plugin for Web Filtering* to be enabled. For FortiClient (macOS) and (Linux) endpoints, you must also enable *Enable HTTPS Deep Inspection*. The endpoint must be able to reach globalvideoquery.fortinet.net or usvideoquery.fortinet.net for Video Filter to work.

Configuration	Description
Video Filter Profile	Enable video filtering. Enable or disable the eye icon to show or hide this feature from the end user in FortiClient.
Name	Enter a name for the profile.
Categories	Enable categories. When you disable categories, the channel and video override lists protect FortiClient. For all categories, you can configure an action for the entire category by selecting one of the following: • Block • Warn • Allow • Monitor The following lists the available categories: • Not Rated • Knowledge • People • Business • Lifestyle • Society • Entertainment • Music • Sports • Games • News
Youtube Advanced Settings	Enable advanced settings for YouTube filtering.
Hide Video Comments	Hide YouTube comments from end users.
Enable Safe Search	When enabling Safe Search, you can configure the Restriction Level to Strict or Moderate. This setting affects the content that endpoint users can access via YouTube. You can enable Safe Search on the Video Filter and Web Filter profiles. When Safe Search is enabled on both profiles, the more restrictive settings are applied to YouTube.

Configuration	Description
Channel Override List	Configure access for a specific YouTube channel. In the *Channel ID* field, enter the YouTube channel ID. You can also import a list of channels using a CSV file. If you block access to a channel and allow access to a specific video that belongs to the blocked channel, FortiClient blocks access to the video. The action configured for the channel overrides the action configured for the specific video.
Video Override List	Configure access for a specific YouTube video. In the *Video URL* field, enter the video URL in the format: youtube.com/watch?v=<video ID>. You can also import a list of videos using a CSV file.
Other FortiGuard Settings	
Traffic Action When FortiGuard Server is Unreachable for Rating	Select an action for FortiClient to take for YouTube videos when it cannot reach the FortiGuard server. Select one of the following: • Block • Warn • Allow • Monitor
FortiGuard Server Location	Configure the FortiGuard server location. FortiClient connects to FortiGuard to query for URL ratings. The URLs connected to for each server location are as follows: • Global: fctguard.fortinet.net • U.S.: fctusguard.fortinet.net
FortiGuard Server Type	Only FortiGuard Anycast is available.

Vulnerability Scan



FortiClient does not report OS or Microsoft office (that updates via KB ID) vulnerabilities when the Windows operating system is out of support or Windows Update is not active.

Configuration	Description
Vulnerability Scan	Enable or disable Vulnerability Scan. Enable or disable the eye icon to show or hide this feature from the end user in FortiClient.
Scanning	
Scan on Registration	Scan endpoints upon connecting to EMS.
Scan on Vulnerability Signature Update	Scan endpoints upon updating a vulnerability signature.
Scan OS Vulnerabilities	Scan endpoints for system updates for the underlying operating system (OS) and notify the OS to do these updates.

Configuration		Description
		• For Windows endpoints, this option scans for and applies Windows OS patches for security updates.  This option does not apply to endpoints running an operating system that is out of support or if Windows Update is not active. • For macOS endpoints, this option runs the OS software updates.
	Force Enable Windows Update	If you disable this option, FortiClient sends a message to EMS to specify the endpoint paused Windows Update. If you enable this option and Windows Update is in a paused state, FortiClient deletes the Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsUpdate\UX\Settings registry key and Windows Update resumes so that FortiClient VCM can detect OS vulnerabilities again.
Enable Proxy		Enable using proxy settings configured in when downloading updates for vulnerability patches.
Show Vulnerabilities Popup		Configure FortiClient to display a *FortiClient Vulnerabilities Scan Summary* popup to the user. when it completes a vulnerability scan on the endpoint. The user can click *View All Vulnerabilities* in the popup to view the scan results.
Automatic Maintenance		Configure settings for automatic maintenance. This configures Vulnerability Scan to run as part of Windows automatic maintenance. Adding FortiClient Vulnerability Scans to the Windows automatic maintenance queue allows the system to choose an appropriate time for the scan that minimally impacts the user, PC performance, and energy efficiency. See Automatic maintenance.
Period		Specify how often Vulnerability Scan needs to be started during automatic maintenance. Enter the desired number of days.
Deadline		Specify when Windows must start Vulnerability Scan during emergency automatic maintenance, if Vulnerability Scan did not complete during regular automatic maintenance. Enter the desired number of days. This value must be greater than the *Period* value.
Scheduled Scan		Configure settings for scheduled scanning.
Schedule Type		Select *Daily*, *Weekly*, *Monthly*.

Configuration	Description
Scan On	Configure the day the scan will run. This only applies if the schedule type is configured to *Weekly* or *Monthly*. Select a day of the week (Sunday through Monday) or a day of the month (1st through the 31st).
Start At	Configure the time the scan starts.
Automatic Patching	
Patch Level	Patches are installed automatically when vulnerabilities are detected. Select one of the following: • Critical: Patch critical vulnerabilities only • High: Patch high severity and above vulnerabilities • Medium: Patch medium severity and above vulnerabilities • Low: Patch low severity and above vulnerabilities • All: Patch all vulnerabilities. Automatic patching may require the endpoint to reboot.
Exclusions	
Exempt Application Vulnerabilities Requiring Manual Update from Vulnerability Compliance Check	All applications that require the endpoint user to manually patch vulnerabilities are excluded from vulnerability compliance check. This option does not exclude applications from vulnerability scanning.
Exclude Selected Applications from Vulnerability Compliance Check	In the *<number> Applications* list, click the applications to exclude from vulnerability compliance check, and they are automatically moved to the *<number> Excluded Applications* list. In the *<number> Excluded Applications* list, click the applications to remove from the exclusion list. Applications on the exclusion list are exempt from needing to install software patches within the time frame specified in FortiGate compliance rules to maintain compliant status and network access. Applications on the list are not excluded from vulnerability scanning.
Disable Automatic Patching for These Applications	Disable automatic patching for the applications excluded from vulnerability compliance check.

Malware Protection

The *Malware Protection* tab contains options for configuring antivirus (AV), anti-ransomware, anti-exploit, cloud-based malware detection, removable media access, exclusions list, and other options. Some options only display if you enable *Advanced* view.

Only features that FortiEndpoint is licensed for are available for configuration.

Enable or disable the eye icon to show or hide this feature from the end user in FortiClient.

AntiVirus Protection

Enable AV protection. FortiClient's AV component supports twelve levels of nested compressed files for scanning.

Options	Description
General	These settings apply to all AV protection.
Delete Malware Files After	Enter the number of days after which to delete malware files from the client.
Identify Malware and Exploits Using Signatures Received From FortiSandbox	Enable to allow FortiClient to use signatures from FortiSandbox to identify malware and exploits for real-time protection (RTP) and on-demand scanning. This option is available only if the *Sandbox Detection* tab is enabled.
Update Sandbox Signatures Every	Enter the number of minutes after which to update signatures.
Real-Time Protection	Enable real-time protection (RTP).
Action On Virus Discovery	• Quarantine Infected Files. You can use FortiClient to view the quarantined file, virus name, and logs, as well as submit the file to FortiGuard. • Deny Access to Infected Files • Ignore Infected Files
Alert When Viruses Are Detected	Displays the *Virus Alert* dialog when RTP detects a virus while attempting to download a file via a web browser. The dialog allows you to view recently detected viruses, their locations, and statuses.
Scan Compressed Files	Scan archive files, including zip, rar, and tar files, for threats. RTP exclusions list default file extensions.

Options	Description
Max Size	Only scan files under the specified size. To allow scanning compressed files of any size, enter 0. For compressed files, FortiClient supports a maximum file size of 1 GB for antivirus scanning. For a compressed file with a size larger than 1 GB, FortiClient scans it after decompression.
Scan Files Accessed by User Process	Configure when RTP should scan files that a user-initiated process accesses. Select one of the following: • Scan Files When Processes Read or Write Them • Scan Files When Processes Read Them • Scan Files When Processes Write Them
Scan Network Files	Scan network files for threats when a user-initiated process accesses them.
System Process Scanning	Enable system process scanning. Select one of the following: • Scan Files When System Processes Read or Write Them • Scan Files When System Processes Read Them • Scan Files When System Processes Write Them • Do Not Scan Files When System Processes Read or Write Them
Enable Windows Antimalware Scan Interface	Enable Microsoft Anti-Malware Interface Scan (AMSI). This feature is only available for endpoints running FortiClient Windows. AMSI scans memory for the following malicious behavior: • User Account Control (elevation of EXE, COM, MSI, or ActiveX installation) • PowerShell (scripts, interactive use, and dynamic code evaluation) • Windows Script Host (wscript.exe and script.exe) • JavaScript and VBScript • Office VBA macros
Enable Machine Learning Analysis	Enable or disable machine learning (ML). This feature uses the new FortiClient AV engine, which incorporates smarter signature-less ML-based advanced threat detection. The antimalware solution includes ML models static and dynamic analysis of threats. From the *Action On Virus Discovery With Machine Learning Analysis* dropdown list, select one of the following: • *Log detection and warn the User*: detect the sample, display a warning message, and log the activity. • *Quarantine Infected Files*: quarantine infected files. You can view, restore, or delete the quarantined file, as well as view the virus name, submit the file to FortiGuard, and view logs.

Options	Description
On Demand Scanning	
Action On Virus Discovery	Select one of the following from the dropdown list: • Warn the User If a Process Attempts to Access Infected Files • Quarantine Infected Files. You can use FortiClient to view the quarantined file, virus name, and logs, as well as submit the file to FortiGuard. • Ignore Infected Files
Integrate FortiClient into Windows Explorer's Context Menu	Adds a *Scan with FortiClient AntiVirus* option to the Windows Explorer right-click menu.
Hide AV Scan from Windows Explorer's Context Menu	Hide AV scan option from Windows Explorer's context menu.
Hide AV Analyse from Windows Explorer's Context Menu	Hide option to submit file for AV analysis from Windows Explorer's context menu.
Pause Scanning When Running on Battery Power	Pause scanning when the computer is running on battery power.
Allow Admin Users to Terminate Scheduled and On-Demand Scans from FortiClient Console	Control whether the local administrator can stop a scheduled or on-demand AV scan initiated by the EMS administrator. A user who is not a local administrator cannot stop a scheduled or on-demand AV scan regardless of this setting.
Automatically Submit Suspicious Files to FortiGuard for Analysis.	Automatically submit suspicious files to FortiGuard for analysis. You do not receive feedback for files submitted for analysis. The FortiGuard team can create signatures for any files that are submitted for analysis and determined to be malicious.
Scan Compressed Files	Scan archive files, including zip, rar, and tar files, for threats.
Max Size	Only scan files under the specified size (in MB). To allow scanning compressed files of any size, enter 0. For compressed files, FortiClient supports a maximum file size of 1 GB for antivirus scanning. For a compressed file with a size larger than 1 GB, FortiClient scans it after decompression.

Options	Description
Max Scan Speed on Computers With	Select the minimum amount of memory that must be installed on a computer to maximize scan speed. AV maximizes scan speed by loading signatures on computers with a minimum amount of memory: • 4 GB • 6 GB • 8 GB • 12 GB • 16 GB
Enable Machine Learning Analysis	Enable or disable machine learning (ML). This feature uses the new FortiClient AV engine, which incorporates smarter signature-less ML-based advanced threat detection. The antimalware solution includes ML models static and dynamic analysis of threats. From the *Action On Virus Discovery With Machine Learning Analysis* dropdown list, select one of the following: • *Log detection and warn the User*: detect the sample, display a warning message, and log the activity. • *Quarantine Infected Files*: quarantine infected files. You can view, restore, or delete the quarantined file, as well as view the virus name, submit the file to FortiGuard, and view logs.
Scheduled Scan	Enable scheduled scans.
Schedule Type	Select *Daily*, *Weekly*, or *Monthly*.
Scan On	If *Weekly* is selected, select the day of the week to perform the scan. If *Monthly* is selected, select the day of the month to perform the scan. If you configure monthly scans to occur on the 31st of each month, the scan occurs on the first day of the month for months with fewer than 31 days.
Start At	Configure the start time for the scheduled scan.
Scan Type	Select one of the following: • *Quick*: Runs the rootkit detection engine to detect and remove rootkits. The quick scan only scans executable files, DLLs, and drivers that are currently running for threats. • *Full*: Runs the rootkit detection engine to detect and remove rootkits, then performs a full system scan of all files, executable files, DLLs, and drivers. • *Custom*: Runs the rootkit detection engine to detect and remove rootkits. In the *Scan Folder* field, enter the full path of the folder on your local hard disk drive to scan.

Options	Description
Scan Priority	Set to *Low*, *Normal*, or *High*. This refers to the amount of processing power that the scan uses and its impact on other processes.
Scan Removable Media	Scan connected removable media, such as USB drives, for threats, if present.
Scan Network Drives	Scan attached or mounted network drives for threats.
Enable Scheduled Scans Even When a Third-Party AV Product Is Present	Enable scheduled scans even when a third party AV product is present.

Anti-Ransomware

Enable antiransomware to protect specific files, folders, or file types on your endpoints from unauthorized changes. After detecting ransomware behavior on the endpoint, FortiClient restores files that were encrypted by the detected ransomware.



The antiransomware feature is not supported on FortiClient macOS.

Options	Description
Protected Folders	Select the desired folders from the list or click *Add Folder* to add a custom directory. Antiransomware protects all content in the selected folders against unauthorized changes. To remove a folder, select it then click *Remove Folder*. This field supports path variables.
Protected File Types	Enter the desired file types to protect from suspicious activity, separating each file type with a comma. Do not include the leading dot when entering a file type. For example, to include text files, enter `txt` as opposed to `.txt`.

Action	Select the desired action for when antiransomware detects suspicious activity:
	• *Terminate ransomware behavior with Anti-Ransomware detection*: FortiClient terminates the suspicious processes, which can include child processes, depending on the ransomware, and quarantines the files that the detected ransomware modified. If you enable *Enable File Backup*, FortiClient backs up files from the protected locations and recovers the files from the backup folder to the protected locations. If you disable *Enable File Backup*, FortiClient cannot recover the files. You can allowlist the quarantined files if you must access them. See Allowlisting quarantined files on page 477.
	• *Wait for user response with Anti-Ransomware detection*: suspend the processes and display a popup asking the user if they want to terminate the process:
	  • If the user selects *Yes*, FortiClient terminates the process as described for *Terminate ransomware behavior with Anti-Ransomware detection*.
	  • If the user selects *No*, FortiClient resumes the processes unless the

Options	Description
	process is already exited by the time of detection. • If the user does not select an option, FortiClient waits for the configured *Action Timeout*, then terminates the process as described for *Terminate ransomware behavior with Anti-Ransomware detection*. • *Monitor only with Anti-Ransomware detection*: log when antiransomware detects suspicious activity.
Action Timeout	Enter the desired timeout value.
Bypass Valid Signer	Enable FortiClient to exclude a process from the selected antiransomware action if it has a valid signer. FortiClient considers the file as having a valid signer if it is digitally signed with a valid certificate that a trusted certificate authority (CA) issued. Enabling this feature may reduce false positives and speed up file analyses.
Enable File Backup	Enable FortiClient to restore files that the detected ransomware encrypted after detecting ransomware behavior on the endpoint.
Backup Interval	Enter the desired backup interval value in hours. FortiClient backs up files in protected folders that were last modified at a time that is longer ago than the backup interval value. The backup only occurs when the files are modified.
Backup File Size Limit	Enter the desired size limit in MB for ransomware-encrypted files for FortiClient to back up. The size limit refers to the original file size, not the size limit after encryption.
Free Disk Quota	Enter the desired backup disk quota value as a percentage of free disk space.

Anti-Exploit

Enable anti-exploit engine to detect suspicious processes (payload) running from legitimate applications. You must enable *Real-Time Protection* for anti-exploit to function.

Cloud-Based Malware Detection

Enable cloud-based malware outbreak detection. Cloud-based malware protection helps protect endpoints from high-risk file types from external sources such as the internet or network drives by querying FortiGuard to determine whether files are malicious. The following describes the process for cloud-based malware protection:

1. A high risk file is downloaded or executed on the endpoint.
2. FortiClient generates a SHA1 checksum for the file.
3. FortiClient sends the checksum to FortiGuard to determine if it is malicious against the FortiGuard checksum library.
4. If the checksum is found in the library, FortiGuard communicates to FortiClient that the file is deemed malware. By default, FortiClient quarantines the file.

This feature only submits high-risk file types such as .exe, .doc, .pdf, and .dll to FortiGuard. The list of high-risk file types is the same as the list of file types that FortiClient submits to Sandbox by default.

Options	Description
Server	
Wait for Cloudscan Results before Allowing File Access	Have the endpoint user wait for cloud scanning results before being allowed access to files. Set the timeout in seconds.
Deny Access to File When There is No Cloudscan Result	Deny access to downloaded files if there is no cloud scan result. This may happen if FortiEndpoint cannot reach FortiGuard.
File Submission Options	
All Files Executed from Removable Media	Submit all files executed on removable media, such as USB drives, to FortiSandbox for analysis.
All Files Executed from Mapped Network Drives	Submit all files executed from mapped network drives.
All Web Downloads	Submit all web downloads.
All Email Downloads	Submit all email downloads.
Exclude Files from Trusted Sources	Exclude files that trusted sources signed from cloud-based malware protection submission. FortiClient considers the file as from a trusted source if it is digitally signed with a valid certificate that a trusted CA issued. Enabling this feature may reduce false positives and speed up file analyses.
Remediation Actions	
Action	Choose *Quarantine* or *Alert & Notify* for malicious files. The user can access the file depending on *Wait for Cloudscan Results before Allowing File Access* and *Deny Access to File When There Is No Cloudscan Result* configuration. Whether FortiClient quarantines the file depends on if FortiGuard reports the file as malicious.

Removable Media Access

Control access to removable media devices, such as USB drives. You can configure rules to allow or block specific removable devices.

FortiClient (macOS) and (Linux) only support the action configured for *Default removable media access*. FortiClient (macOS) and (Linux) do not support other removable media access rules received from EMS.

For the class, manufacturer, vendor ID, product ID, and revision, you can find the desired values for the device in one of the following ways:

- Microsoft Windows Device Manager: select the device and view its properties.
- USBDeview

Options	Description
Show bubble notifications	Display a bubble notification when FortiClient takes action with a removable media device.
Action	Configure the action to take with removable media devices connected to the endpoint that match this rule. Available options are: • *Allow*: Allow access to removable media devices connected to the endpoint that match this rule. • *Block*: Block access to removable media devices connected to the endpoint that match this rule. • *Monitor*: Log removable media device connections to the endpoint that match this rule.
Description	Enter the desired rule description.
Type	Select *Simple* or *Regular Expression* for the rule type. When *Simple* is selected, FortiClient performs case-insensitive matching against classes, manufacturers, vendor IDs, product IDs, and revisions. When *Regular Expression* is selected, FortiClient uses Perl Compatible Regular Expressions (PCRE) to perform matching against classes, manufacturers, vendor IDs, product IDs, and revisions.
Class	Enter the device class.
Manufacturer	Enter the device manufacturer.
Vendor ID	Enter the device vendor ID.
Product ID	Enter the device product ID.
Revision	Enter the device revision number.
Remove this rule	Remove this rule from the profile.
Add a new rule	Add a new removable media access rule.
Move this rule up/down	Move this rule up or down. If a connected device is eligible for multiple rules, FortiClient applies the highest rule to the device.
Default removable media access	Configure the action to take with removable media devices that do not match any configured rules. Available options are: • *Allow*: allow access to removable media devices connected to the endpoint that do not match any configured rules. • *Block*: block access to removable media devices connected to the endpoint that do not match any configured rules. • *Monitor*: log removable media device connections to the endpoint that do not match any configured rules.

Exclusions

Enable exclusions from AV scanning. FortiEndpoint supports using wildcards and path variables to specify files and folders to exclude from scanning. EMS supports the following wildcards and variables:

- Using wildcards to exclude a range of file names with a specified extension, such as Edb*.jrs
- Using wildcards to exclude all files with a specified extension, such as *.jrs
- Path variable %allusersprofile%
- Path variable %appdata%
- Path variable %localappdata%
- Path variable %systemroot%
- Path variable %systemdrive%
- Path variable %userprofile%
- Path variable %windir%

Combinations of wildcards and variables are supported.

Having a longer exclusion list affects AV performance. It is advised to keep the exclusion list as short as possible.



Exclusion lists are case-sensitive.



When excluding a network share, you may enter the path using drive letters (Z:\folder\) or the UNC path (\\172.17.60.193\fileserver\folder).

Options	Description
Paths to Excluded Folders	Enter fully qualified excluded folder paths in the provided text box to exclude these folders from RTP and on-demand scanning.
Paths to Excluded Files	Enter fully qualified excluded files in the provided text box to exclude these files from RTP and on-demand scanning.
File Extensions Excluded from Real-Time Protection	RTP skips scanning files with the specified extensions.
File Extensions Excluded from On Demand Scanning	On-demand AV protection skips scanning files with the specified extensions.

Other

Options	Description
Scan for Rootkits	Scan for files implementing advanced OS hooks that malware uses to protect itself from being shutdown, killed, or deleted. A rootkit is a collection of programs that enable administrator-level access to a computer or computer network. Typically a rootkit is installed on a computer after first obtaining user-level access by exploiting a known vulnerability or cracking a password.
Scan for Adware	Scan for adware. Adware is a form of software that downloads or displays unwanted ads when a user is online.
Scan for Riskware	Scan for riskware. Riskware refers to legitimate programs which, when installed and executed, present a possible but not definite risk to the computer.
Enable Advanced Heuristics	Enable AV scan with heuristics signature. Advanced heuristics is a sequence of heuristics to detect complex malware.
Scan Removable Media on Insertion	Scan removable media on insertion. FortiClient scans the following media types on insertion: • Floppy drives • Thumb drives • Flash card reader • USB devices (BusTypeUsb) • External hard drives (BusType1394) This feature does not scan the following on insertion: • Remote (network) drive • CD-ROM drive • RAM disk
Scan Email	Scan emails for threats with SMTP and POP3 protocols.
Scan MIME Files (Inbox Files)	Scan inbox email content with Multipurpose Internet Mail Extensions (MIME) file types. MIME is an Internet standard that extends the format of the email to support the following: • Text in character sets other than ASCII • Non text attachments (audio, video, images, applications) • Message bodies with multiple parts
Enable FortiGuard Analytics	Automatically sends suspicious files to FortiGuard for analysis.
Notify Logged in Users if Their AV Signatures Expired	Notify logged in users if their AV signatures expired.

Sandbox

Enable Sandbox Detection. Some options only display if you enable *Advanced* view.

Some options on this tab are only available for configuration if your FortiEndpoint license includes the Sandbox Cloud feature. For example, if you have only applied the zero trust network access license, the FortiClient Cloud Sandbox (SaaS) options are unavailable.

For each endpoint, FortiClient can send a maximum of 300 files daily to FortiClient Cloud Sandbox (SaaS). If multiple files are submitted around the same time, FortiClient sends one file to FortiClient Cloud Sandbox (SaaS), waits until it receives the verdict for that file, then sends the next file to FortiClient Cloud Sandbox (SaaS).



This feature does not rely on FortiClient real-time protection and can be used alongside other real-time antimalware applications such as Windows Defender. Files that these applications have quarantined cannot be sent to FortiSandbox.

Configure the following options:

Options	Description
Sandbox Detection	Enable Sandbox Detection. Enable or disable the eye icon to show or hide this feature from the end user in FortiClient.
Server	
FortiSandbox	To configure connection to an on-premise FortiSandbox appliance or FortiSandbox Cloud, select *Appliance*. Select *Cloud* to configure connection to FortiClient Cloud Sandbox (SaaS). FortiClient Cloud Sandbox (SaaS) offers a more affordable alternative to a FortiSandbox appliance, since it is a cloud service that you do not need to host on-site. However, FortiClient Cloud Sandbox (SaaS) does not offer the full range of features that a FortiSandbox appliance offers. FortiClient Cloud Sandbox (SaaS) is a service that uploads and analyzes files that FortiClient antivirus (AV) marks as suspicious. If FortiClient Cloud Sandbox (SaaS) is enabled and configured on the assigned profile, FortiClient uploads suspicious files to FortiGuard for analysis. Once uploaded, the file is executed and the resulting behavior analyzed for risk. If the file exhibits risky behavior or is found to contain a virus, a new virus signature is created and added to the FortiGuard AV signature database. The next time the FortiClient updates its AV database it has the new signature. The turnaround time on Cloud Sandboxing and AV submission ranges from ten minutes for automated FortiClient Cloud Sandbox (SaaS) detection to ten hours if FortiGuard Labs is involved. FortiGuard Labs considers a file suspicious if it exhibits some unusual behavior, yet does not contain a known virus. The behaviors that it considers suspicious change depending on the current threat climate and other factors.

Options	Description
	FortiClient Cloud Sandbox (SaaS) is only available with the Endpoint Protection Platform license.
IP address/Hostname	For a FortiSandbox appliance, enter the FortiSandbox's IP address, FQDN, or hostname. Although the *IP address/Hostname* field is only available when *Appliance* is selected, you can also configure this option for FortiSandbox Cloud. Enter the FortiSandbox Cloud FQDN and account ID in the *Account ID* field. Click *Test Connection* to ensure that EMS can communicate with FortiSandbox. This option is only available when *Appliance* is selected.
Account ID	Optional. Enter the FortiSandbox Cloud account ID. You should only use this option when configuring a FortiSandbox Cloud using the FQDN.
Username	Optional. Enter the FortiSandbox username. This option is only available for a FortiSandbox appliance. When using a FortiSandbox appliance, the username is necessary to view detailed FortiSandbox reports on the *Sandbox Events* tab. See Viewing Sandbox event details on page 70.
Password	Optional. Enter the FortiSandbox password. This option is only available for a FortiSandbox appliance. When using a FortiSandbox appliance, the password is necessary to view detailed FortiSandbox reports on the *Sandbox Events* tab. See Viewing Sandbox event details on page 70.
Region	FortiClient Cloud Sandbox (SaaS) region. See Configuring FortiGuard Services settings on page 546.
Time Offset	FortiClient Cloud Sandbox (SaaS) time offset. See Configuring FortiGuard Services settings on page 546.
License Status	Displays the Sandbox Cloud license status. Using FortiClient Cloud Sandbox (SaaS) requires an additional license.
Inspection Mode	Select one of the following: • *None*: FortiClient does not send any files to FortiSandbox for inspection. • *High-Risk Files*: FortiClient inspects all supported high-risk files and sends to FortiSandbox as appropriate. The following are considered high-risk file types: 7z, ace, apk, arj, bat, bz2, cab, dll, dmg, doc, docx, elf, exe, gz, htm, iso, jar, js, kgb, lnk, lzh, mac, mime, msi, pdf, ppt, pptx, rar, rtf, swf, tar, thmx, upx, vbs, xls, xlsx, xz, z, zip • *All Supported Extensions*: when you select *All Supported Extensions*, a yellow caution banner appears to inform you that you must enter a valid Sandbox configuration and click *Test Connection* for EMS to receive the full list of extensions that your FortiSandbox appliance supports. FortiClient inspects all of the supported file extensions and sends to FortiSandbox as appropriate. This option is only available for a FortiSandbox appliance.
Excluded File Extensions	Select a file extension to exclude from FortiSandbox scanning. You can select multiple file extensions.

Options	Description
	When *All Supported Extensions* is configured for *Inspection Mode*, the list of file extensions available to select as *Excluded File Extensions* updates to the extensions that the configured FortiSandbox appliance supports.
Wait for FortiSandbox Results before Allowing File Access	Have the endpoint user wait for FortiSandbox scanning results before being allowed access to files. Set the timeout in seconds.
Deny Access to File When There Is No Sandbox Result	Deny access to downloaded files if there is no FortiSandbox result. This may happen if FortiSandbox is offline.
File Submission Options	
File Size Limit	The default value is 200 MB. For a FortiSandbox appliance, you can configure a file size limit up to 500 MB. For FortiClient Cloud Sandbox (SaaS), you can configure a file size limit up to 100 MB.
All Files Executed from Removable Media	Submit all files executed on removable media, such as USB drives, to FortiSandbox for analysis.
All Files Executed from Mapped Network Drives	Submit all files executed from mapped network drives.
All Web Downloads	Submit all web downloads.
All Email Downloads	Submit all email downloads.
Remediation Actions	
Action	Choose *Quarantine* or *Alert & Notify* for infected files. The user can access the file depending on *Wait for FortiSandbox Results before Allowing File Access* and *Deny Access to File When There Is No Sandbox Result* configuration. Whether FortiClient quarantines the file depends on if FortiSandbox reports the file as malicious and the *FortiSandbox Detection Verdict Level* setting.
FortiSandbox Detection Verdict Level	Select the desired detection verdict level. For FortiClient to apply the action selected in the *Action* field to an infected file, FortiSandbox must detect the file as this level or higher. For example, if *Action* is configured as *Quarantine* and *FortiSandbox Detection Verdict Level* is configured as *Medium*, FortiClient quarantines all infected files that FortiSandbox detects as Medium or a higher level (High or Malicious). FortiClient does not quarantine files for which FortiSandbox returns a verdict below this level (Low Risk or Clean).
Exceptions	
Exclude Files from Trusted Sources	Exclude files signed by trusted sources from FortiSandbox submission. Following is a list of sources trusted by FortiSandbox: • Microsoft

Options	Description
	• Fortinet • Mozilla • Windows • Google • Skype • Apple • Yahoo! • Intel
Exclude Specified Folders/Files	Exclude specified folders/files from FortiSandbox submission. You must also create the exclusion list. FortiEndpoint supports using wildcards and path variables to specify files and folders to exclude from scanning. EMS supports the following wildcards and variables: • Using wildcards to exclude a range of file names with a specified extension, such as Edb*.jrs • Using wildcards to exclude all files with a specified extension, such as *.jrs • Path variable %allusersprofile% • Path variable %appdata% • Path variable %localappdata% • Path variable %systemroot% • Path variable %systemdrive% • Path variable %userprofile% • Path variable %windir% Combinations of wildcards and variables are supported.
Inclusions	
Include Specified Folders/Files	Include specified folders/files in FortiSandbox submission. You must also create the inclusion list.
Other	
Hide Sandbox Scan from Windows Explorer's Context Menu	Hide Sandbox scan option from Windows Explorer's right-click context menu.
Notification Type	Select the desired notification type to display to end users when FortiClient Cloud Sandbox (SaaS) detects an infected file: • **Lite**: Displays notification balloon when FortiSandbox detects malware in a submission. • **Full**: Displays a popup for all FortiSandbox file submissions. • **None**: Does not display any notification for FortiSandbox file submissions, malware detection, or quarantine.



In addition to the configuration above, you must also configure the connection to EMS on the FortiSandbox. In FortiSandbox, go to *Scan Input* > *Devices*, and search for and authorize EMS using its serial number. You can find the EMS serial number on the *System Information* widget on the Dashboard.

Firewall

FortiClient does not include SSL deep inspection. As FortiClient cannot apply signatures marked as *Deep Inspection*, do not use these signatures in a profile.

Configuration	Description
Application Firewall	Enable application control. Enable or disable the eye icon to show or hide this feature from the end user in FortiClient.
General	
Notification Bubbles on User's Desktop When Applications Are Blocked	Enable notification bubbles when FortiClient blocks applications.
Detect & Block Exploits	Inspect network traffic for intrusions attempting to exploit known vulnerabilities.
Block Known Communication Channels Used by Attackers	Enable Command and Control (C&C) detection using IP address reputation database signatures. Check network traffic against known C&C IP address plus port number combinations.
Categories	Enable FortiClient firewall to allow, block, or monitor applications based on their signature.

Configuration	Description
	Block, allow or monitor the following categories: • Botnet • Business • Cloud.Applications • Cloud.IT • Collaboration • Email • Game • General.Interest • Industrial • Mobile • Network.Service • P2P • Proxy • Remote.Access • Social.Media • Storage.Backup • Update • Video/Audio • VoIP • Web.Client • All Other Unknown Applications
Application Overrides	Configure FortiClient firewall to allow, block, or monitor specific applications based on their signature. Adding more than 1000 application overrides is not recommended and can cause EMS instability.
Add	1. Click *Add* to configure a custom application override. 2. In the *Firewall Application Signatures* dialog, select the desired application signature(s) for which to configure an override. For each application signature, the dialog displays its name, application category, whether the signature requires deep inspection, and other fields. As FortiClient cannot apply signatures marked as *Deep Inspection*, do not use these signatures in a profile. 3. At the bottom of the dialog, select the desired action for this signature: *Allow*, *Block*, or *Monitor*. 4. Click *Add*. You can filter the list of application overrides by the signature, category, action, and so on.
Delete	Delete an application signature override.
Custom Application Overrides	FortiClient does not support this feature. Do not configure it.

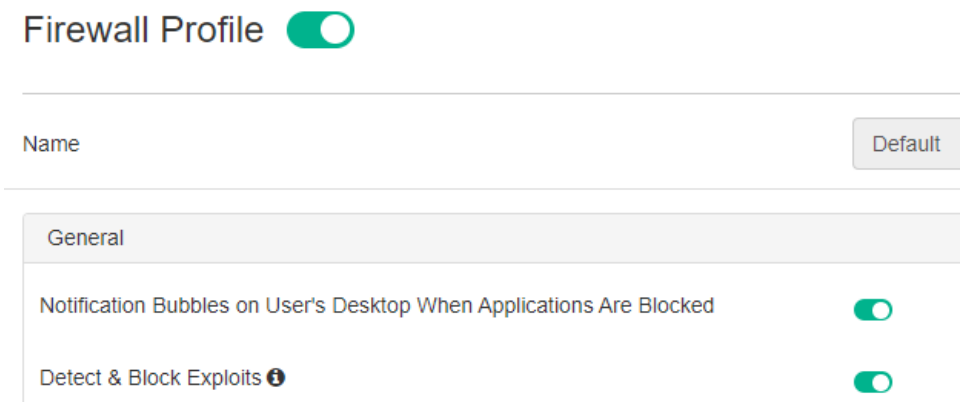
Define exceptions for Firewall Detect & Block Exploits feature

When you enable *Detect & Block Exploits* in an Application Firewall profile in EMS, FortiClient inspects network traffic for intrusions attempting to exploit known vulnerabilities and blocks application traffic based on the intrusion prevention system (IPS) signature IDs. You can define exceptions to allow any application traffic based on the IPS signature ID. You can obtain the signature IDs from FortiGuard Labs. Application Firewall allows access to application traffic that matches signature IDs configured in the pass action list. You can configure multiple signature IDs on the same rule.

This feature is helpful for when you want to allow network access for an application that *Detect & Block Exploits* blocks. In the example, Veeam Data Platform, a data backup and restore application, backs up data to a remote server through Remote.CMD.Shell. The example configures an exception for Remote.CMD.Shell IPS signature ID to allow network access to the Veeam application. If you do not configure an exception, Application Firewall detects Remote.CMD.Shell as an exploit and blocks Veeam application traffic.

To define exceptions for Application Firewall Detect & Block Exploits:

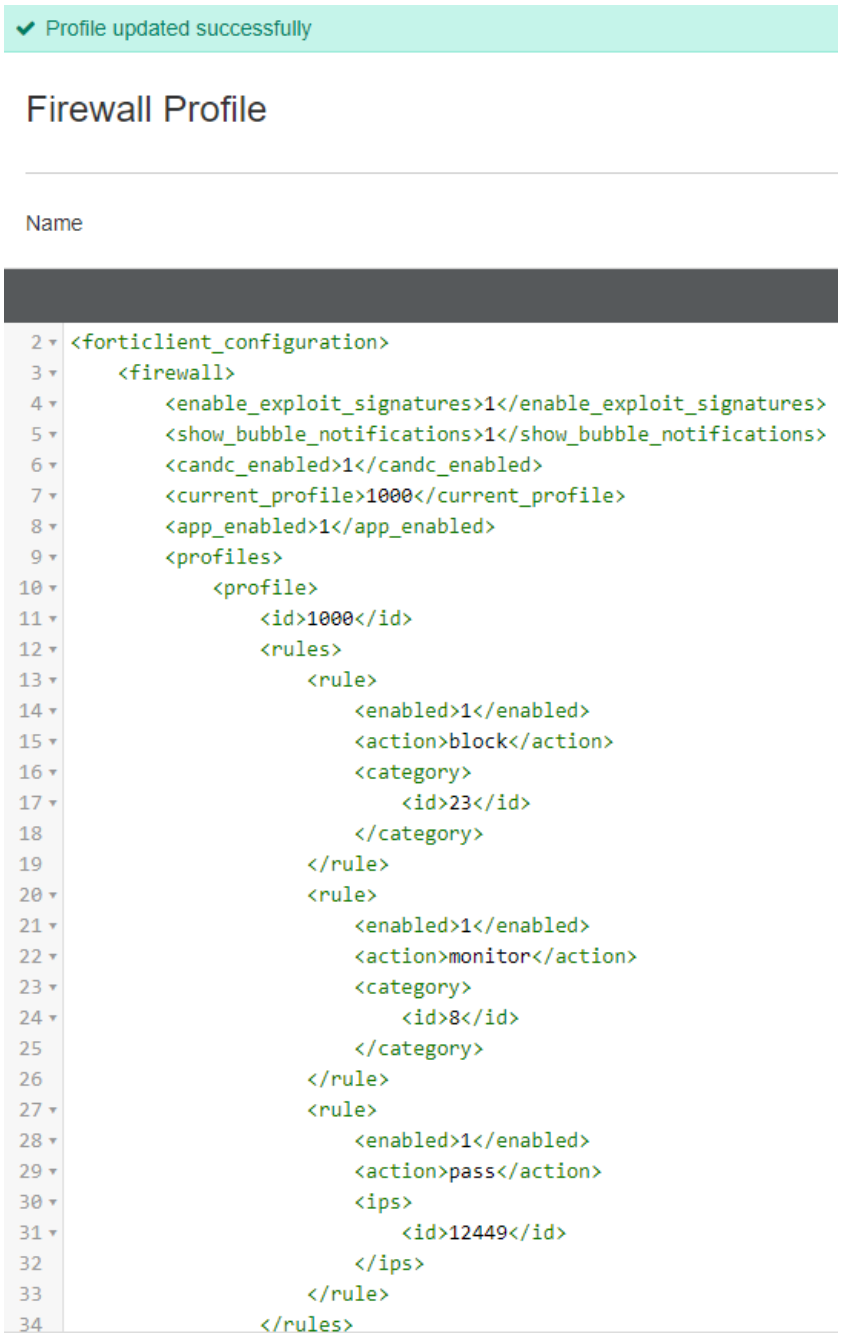
1. In EMS, go to *Endpoint Profiles* > *Firewall*.
2. Under *General*, enable *Detect & Block Exploits*.



3. Click *XML*, then *Edit*.
4. Add the following pass rule for IPS detection, using the `<ips>` element, entering the IPS signature ID of the desired application. The example enters 12449, the IPS signature ID for Remote.CMD.Shell:

```
<forticlient_configuration>
    <firewall>
        <enable_exploit_signatures>1</enable_exploit_signatures>
        <show_bubble_notifications>1</show_bubble_notifications>
        <candc_enabled>1</candc_enabled>
        <current_profile>1000</current_profile>
        <app_enabled>1</app_enabled>
        <profiles>
            <profile>
                <id>1000</id>
                <rules>
                    <rule>
                        <enabled>1</enabled>
                        <action>block</action>
```

```
                        <category>
                            <id>23</id>
                        </category>
                    </rule>
                    <rule>
                        <enabled>1</enabled>
                        <action>monitor</action>
                        <category>
                            <id>8</id>
                        </category>
                    </rule>
                    <rule>
                        <enabled>1</enabled>
                        <action>pass</action>
                        <ips>
                            <id>12449</id>
                        </ips>
                    </rule>
                </rules>
            </profile>
        </profiles>
    </firewall>
    <endpoint_control>
        <ui>
            <display_firewall>1</display_firewall>
        </ui>
    </endpoint_control>
</forticlient_configuration>
```



After an endpoint (Endpoint A) receives the configuration update, you can access Endpoint A's Command Prompt from another endpoint (Endpoint B) if Endpoint B has an application installed for launching a remote command shell. You can pass Windows commands to execute on Endpoint A from Endpoint B. FortiClient on Endpoint A does not block the execution of these commands because of the configuration of Remote.CMD.Shell IPS signature ID (12449) as an exception.

Data Protection

You can configure an integration between FortiClient, EMS, and FortiData. FortiData is a document classification and labeling service. It contains a database (DB) of your file hashes, along with file metadata, including a data category (optional) and a label. The file data labels work in the same way as Microsoft's Purview Information Protection labels, although the labels are not included in the file content but are associated with the file hash in the FortiData DB. A label taxonomy is defined to represent the various classification levels required for an organization. FortiClient can integrate with FortiData to retrieve file data labels and use them to control file access.

The following describes how the integration functions once configured:

1. The EMS administrator configures a FortiData Fortinet Security Fabric Connector to establish trust. EMS and FortiData communicate in the following ways:
   - EMS pulls a data label list from FortiData to use in Data Protection profiles.
   - EMS send its certificate to FortiData to verify tokens that managed endpoints send for lookup.
   - FortiData must provide a connector API key for Fabric connection with EMS.
   - Any other information exchanges between EMS and FortiData are done via this connector.
   - FortiData only accepts requests from endpoints that this EMS manages. FortiData verifies this using the EMS serial number.
   - EMS sends FortiData a zero trust network access (ZTNA) certificate that FortiData to verify FortiClient requests. FortiData must provide the API key to receive the ZTNA certificate.
2. The EMS administrator defines a Data Protection profile to monitor access to a file based on its data label.
3. The EMS administrator defines which file types to send to FortiData for classification lookup. FortiClient only sends the selected file types for lookup. FortiData supports file uploads for OCR, such as JPEG and GIF.
4. When a user downloads or opens a file that matches the configuration, FortiClient performs a hash lookup and retrieves the data label from FortiData for that file.
5. FortiClient sends its token with the request to authenticate with FortiData to authorize the endpoint.
6. FortiClient enforces file access based on classification rules that EMS defined. All file monitor activity is logged.

FortiClient and EMS support integration with FortiData 7.6.1 and later versions. This feature requires the Endpoint Protection Platform license.

See Configuring FortiData integration on page 367.

Options	Description
Server	Select the desired FortiData server. You must configure a FortiData Fabric connector for a FortiData server to be available for selection. See Creating connectors with OAuth 2.0 token-based authentication on page 433.
Data Labels	For each data label, configure the desired action. FortiClient supports the Monitor action.
Enable On	Enable any of the following as desired: • Browser: FortiClient applies the configured action to a file that matches data label and is uploaded to a website.

Options	Description
	• Messaging Clients: FortiClient applies the configured action to a file that matches data label and is uploaded to a messaging client. This feature supports Microsoft Teams and Telegram. • Clipboard: FortiClient applies the configured action to a file that is copied to the clipboard. For example, if you open the file and take a screenshot, it is copied to the clipboard.
File Extensions	Select the desired extensions to apply the data protection settings on.
Exclude Specified Folders/Files	Exclude specified folders or files from FortiData submission. You must also create the exclusion list.
Paths to Excluded Folders	Configure specific folders to exclude from FortiData submission.
Paths to Excluded Files	Configure specific files to exclude from FortiData submission.

Configuring FortiData integration

You can configure an integration between FortiClient, EMS, and FortiData. FortiData is a document classification and labeling service. It contains a database (DB) of your file hashes, along with file metadata, including a data category (optional) and a label. The file data labels work in the same way as Microsoft's Purview Information Protection labels, although the labels are not included in the file content but are associated with the file hash in the FortiData DB. A label taxonomy is defined to represent the various classification levels required for an organization. FortiClient can integrate with FortiData to retrieve file data labels and use them to control file access.

The following describes how the integration functions once configured:

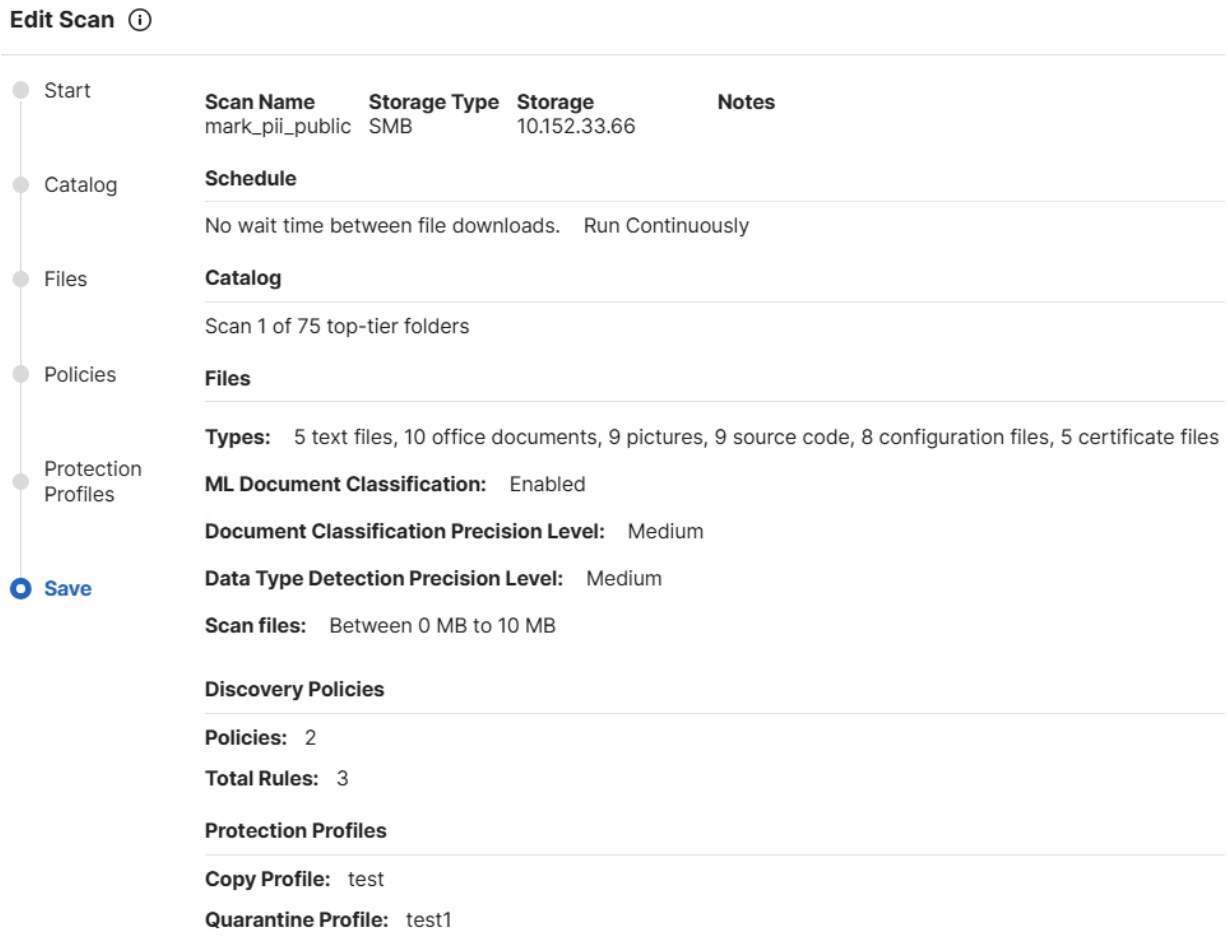
1. The EMS administrator configures a FortiData Fortinet Security Fabric Connector to establish trust. EMS and FortiData communicate in the following ways:
   - EMS pulls a data label list from FortiData to use in Data Protection profiles.
   - EMS send its certificate to FortiData to verify tokens that managed endpoints send for lookup.
   - FortiData must provide a connector API key for Fabric connection with EMS.
   - Any other information exchanges between EMS and FortiData are done via this connector.
   - FortiData only accepts requests from endpoints that this EMS manages. FortiData verifies this using the EMS serial number.
   - EMS sends FortiData a zero trust network access (ZTNA) certificate that FortiData to verify FortiClient requests. FortiData must provide the API key to receive the ZTNA certificate.
2. The EMS administrator defines a Data Protection profile to monitor access to a file based on its data label.
3. The EMS administrator defines which file types to send to FortiData for classification lookup. FortiClient only sends the selected file types for lookup. FortiData supports file uploads for OCR, such as JPEG and GIF.

4. When a user downloads or opens a file that matches the configuration, FortiClient performs a hash lookup and retrieves the data label from FortiData for that file.
5. FortiClient sends its token with the request to authenticate with FortiData to authorize the endpoint.
6. FortiClient enforces file access based on classification rules that EMS defined. All file monitor activity is logged.

FortiClient and EMS support integration with FortiData 7.6.1 and later versions. This feature requires the Endpoint Protection Platform license.

To configure FortiData for the integration:

1. Install FortiData-VM 7.6.1.
2. Configure FortiData discovery policies for file scanning on the endpoint:
   a. Go to *Discovery* > *Policies*.
   b. Create and configure a policy as desired.
3. Configure scan policies to scan for those files. FortiData scans files and assigns labels to files that match the policy after the scan completes:
   a. Go to *Discovery* > *Scans*.
   b. Configure the scan policy as desired.



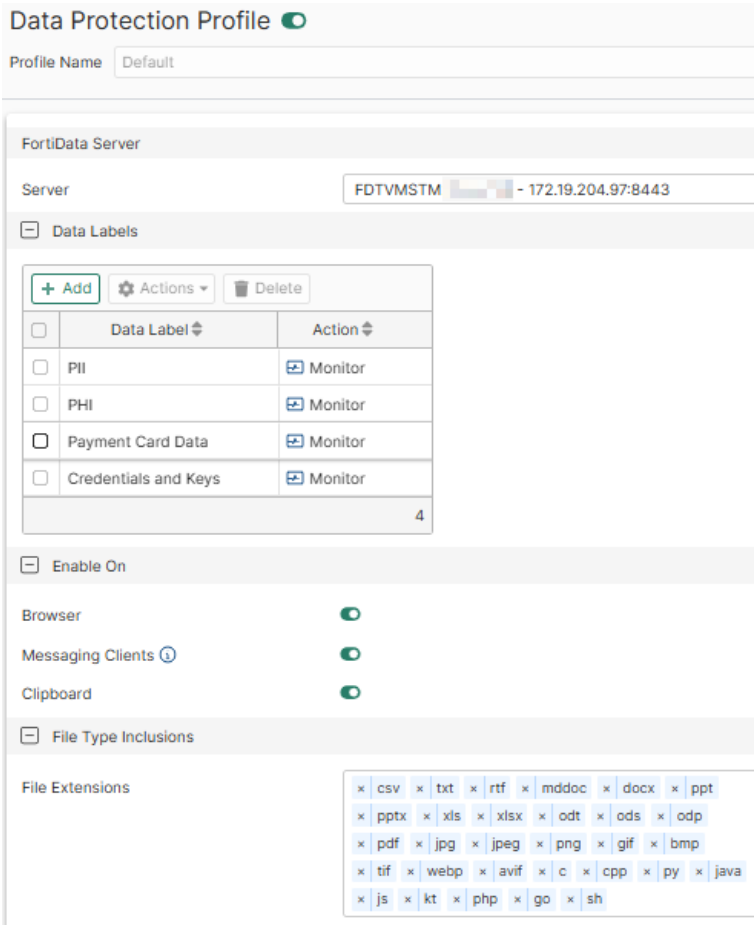
4. For FortiData and EMS to establish Fabric connection, you must upload a publicly signed certificate to FortiData. Upload the certificate:

   a. Go to *System > Certificates*.
   b. Click *Import Certificate > Add a new certificate*.
   c. Upload the certificate and key files.
5. Go to *Fabric > HTTP2 Service > API Keys. Click New API Key*. You will use this API key to establish Fabric connection between EMS and FortiData.
6. Create a Fabric connector for EMS in FortiData:
   a. Go to *Fabric > HTTP2 Service*.
   b. Under *Settings*, configure a new device.
   c. From the *Device Type* dropdown list, select *FortiClient EMS*.
   d. In the *IPv4 Address / Ranges* field, enter 0.0.0.0/0.
   e. Click *Enable API Key Authentication*.
   f. From the *Associated Scan Policies* dropdown list, select the scan policy that you created.
   g. From the *Associated Discovery Policies* dropdown list, select the discovery policy that you created.
   h. Click *Save*.
7. Create a Fabric connector for FortiClient in FortiData:
   a. Go to *Fabric > HTTP2 Service*.
   b. Under *Settings*, configure a new device.
   c. From the *Device Type* dropdown list, select *FortiClient*.
   d. Click *Enable Client Certificate Validation Using EMS CA*.
   e. Click *Save*.

To configure the integration in EMS:

1. Create a FortiData connector:
   a. In EMS, go to *Fabric & Connectors* . *Fabric Devices*.
   b. Click *Add*.
   c. From the *Connector Type* dropdown list, select *FortiData*.
   d. In the *FortiData Hostname / IP address* field, enter the FortiData IP address.
   e. In the *FortiData Port* field, enter 8443.
   f. In the *FortiData REST API Key* field, paste the key that you created in FortiData.
   g. Click *Next* and complete creating the FortiData connector. Once EMS establishes the connection with FortiData, it queries tags and file types from FortiData.
2. Create a data protection profile:
   a. Go to *Endpoint Profiles > Data Protection*.
   b. Create a new profile.
   c. From the *Server* dropdown list, select the FortiData server.
   d. Under *Enable On*, enable *Browser*, *Messaging Clients*, or *Clipboard* to enable the data protection feature on.

e. Under *File Extensions*, select the desired extensions.



3. Configure the certificate that you created in FortiData in EMS:
   a. Go to *Endpoint Policy & Components* > *CA Certificates*.
   b. Click *Upload*.
   c. Click *Upload File*.
   d. Browse to and select the certificate that you created in FortiData. Click *OK*.
   e. Go to *Endpoint Profiles* > *System Settings*.
   f. Create a new profile or edit an existing one.
   g. Under *Other*, enable *Install CA Certificate on Client*.
   h. Ensure that the desired certificate is selected. FortiClient uses certificate chain validation to verify the FortiData server identity. If you generated your own self-signed certificate for FortiData, you only need to install a root certificate authority (CA) certificate on the endpoint. Using an SSL certificate from a trusted CA is recommended.
   i. Click *Save*.

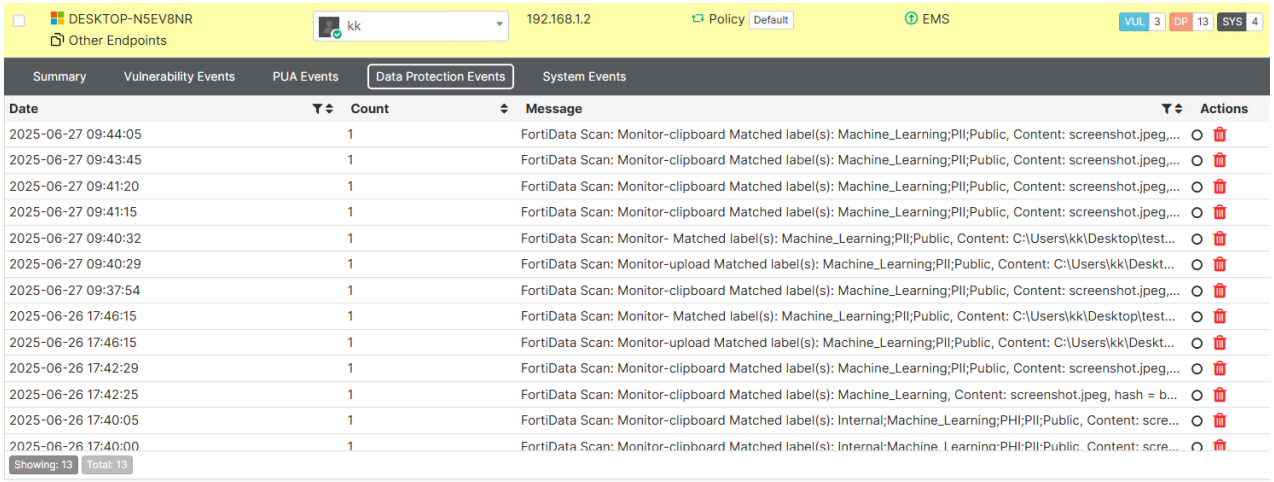
To install FortiClient with FortiData support:

1. Run the FortiClient installer on the endpoint. In *Additional Security Features*, select *Data Protection*. Configure other installation options as desired.
2. After FortiClient connects to EMS, in Registry Editor, confirm that `Computer\HKEY_LOCAL\SOFTWARE\Fortinet\FortiClient\FA_FTDATA` exists and includes the configurations from EMS.

To verify the FortiData integration:

1. Do one of the following from the endpoint, using a file that matches the conditions configured in FortiData:
   - Upload a file to a website.
   - Upload a file on a messaging client, such as Microsoft Teams.
   - Open a file and take a screenshot. This copies the file to the clipboard.

   FortiClient calculates the hash of the file, sends it to FortiData, and checks if the hash matches any labels. If there is a label match, FortiClient monitors access to the file and sends event details to EMS.
2. In EMS, go to *Endpoints* > *All Endpoints*.
3. Select the desired endpoint.
4. Go to the *Data Protection Events* tab. This tab lists the following information about data protection events:



   - Date/time of event
   - User name
   - Hostname
   - Action type, i.e. monitor or block.
   - Mode: either simulation or protection mode.
   - File hash
   - Data Label
   - Filename/path
5. After uploading the file check fcaptmontrace_1 logs in the trace folder, you can see the matched label and file name and uploaded platform. The following shows example logs for different scenarios:

Scenario	Log example
Browser upload	[2025-06-27 09:59:25.2311041 UTC-07:00] [4244:4656] [fcaptmontrace 431 info] sending ems alert,C:\Users\kk\Desktop\testpkg\testpkg\phi_internal\phi_1_patient_admission_notes--patient_name-dob-diagnosis.png,Monitor- Matched label(s): Internal;Machine_Learning;PHI;PII, Content: C:\Users\kk\Desktop\testpkg\testpkg\phi_internal\phi_1_patient_admission_notes--patient_name-dob-diagnosis.png, hash = 9fc7c807621dadcf29e459db8569884ddce8e718,,Monitor,9fc7c807621dadcf29e459db8569884ddce8e718,Internal;Machine_Learning;PHI;PII,chrome.exe
Screenshotted (clipboard)	[2025-06-26 17:40:04.2583481 UTC-07:00] [5780:10548] [fcaptmontrace 431 info] sending ems alert,screenshot.jpeg,Monitor-clipboard Matched label(s): Internal;Machine_Learning;PHI;PII;Public, Content: screenshot.jpeg, hash = fedbfa3746a420fbd86342077eb04dbd7d821947,clipboard,Monitor,fedbfa3746a420fbd86342077eb04dbd7d821947,Internal;Machine_Learning;PHI;PII;Public,clipboard
Sent via Microsoft Teams	[2025-06-26 17:46:15.0600390 UTC-07:00] [5780:12240] [fcaptmontrace 431 info] sending ems alert,C:\Users\kk\Desktop\testpkg\testpkg\pii_public\pii--50_names.txt,Monitor- Matched label(s): Machine_Learning;PII;Public, Content: C:\Users\kk\Desktop\testpkg\testpkg\pii_public\pii--50_names.txt, hash = 42f2c523834b26ae6934d73de2238a656eafba22,,Monitor,42f2c523834b26ae6934d73de2238a656eafba22,Machine_Learning;PII;Public,msedgewebview2.exe
Sent via Telegram	[2025-06-27 09:40:28.7196748 UTC-07:00] [4244:5768] [fcaptmontrace 431 info] sending ems alert,C:\Users\kk\Desktop\testpkg\testpkg\pii_public\pii--50_names-50_ssns-50_us_drivers_licenses.xlsx,Monitor- Matched label(s): Machine_Learning;PII;Public, Content: C:\Users\kk\Desktop\testpkg\testpkg\pii_public\pii--50_names-50_ssns-50_us_drivers_licenses.xlsx, hash = 3a0b43d3e2e5998e40c45adbaae260bf7900d9be,,Monitor,3a0b43d3e2e5998e40c45adbaae260bf7900d9be,Machine_Learning;PII;Public,Telegram.exe

6. To check the logs in FortiData, run the following commands:

```
diagnose logs http2 50
diagnose logs analyzer 50
```

The following shows example output from these commands:

```
[DEBUG]  2025/06/26 03:10:28.160563 tag_info_service.go:58  Updated tag cache: map
[APPI:Compliance APPs:Compliance ASIA:Data Residency AUSTRALIA:Data Residency BRAZIL:Data
Residency CCPA:Compliance CSL:Compliance Clinical Records:Data Classification Clinical
Studies:Data Classification Compliance and Risk Management:Data Classification
Confidential:Sensitivity Configuration Files:Data Classification Contracts and Agreements:Data
Classification Credentials and Keys:Data Classification Credit and Risk Management:Data
Classification DPA:Compliance Development Documentation:Data Classification EU:Data Residency
Education:Data Classification FERPA:Compliance FISMA:Compliance Finance:Data Classification
Financial Report:Data Classification Financial Strategy and Research:Data Classification
GDPR:Compliance GLBA:Compliance HIPAA:Compliance HR Documentation:Data Classification
Healthcare:Data Classification Highly Confidential:Sensitivity Information Technology:Data
Classification Insurance and Settlement:Data Classification Internal:Sensitivity JAPAN:Data
Residency LGPD:Compliance Legal:Data Classification License Agreement:Data Classification
Manufacture:Data Classification Medication Management:Data Classification NDA Form:Data
Classification NIST 800-53 and NIST 800-171:Compliance Operational Documentation:Data
Classification PCI_DSS:Compliance PHI:Data Classification PII:Data Classification
PIPEDA:Compliance Patent:Data Classification Payment Card Data:Data Classification Performance
```

```
Review:Data Classification Public:Sensitivity Restricted:Sensitivity SOX:Compliance Source
Code:Data Classification Test Documentation:Data Classification Timesheet:Data Classification
Training Materials:Data Classification Transaction Record:Data Classification UK:Data
Residency US:Data Residency User Documentation:Data Classification]
[DEBUG]  2025/06/26 03:15:28.160441 tag_info_service.go:58  Updated tag cache: map
[APPI:Compliance APPs:Compliance ASIA:Data Residency AUSTRALIA:Data Residency BRAZIL:Data
Residency CCPA:Compliance CSL:Compliance Clinical Records:Data Classification Clinical
Studies:Data Classification Compliance and Risk Management:Data Classification
Confidential:Sensitivity Configuration Files:Data Classification Contracts and Agreements:Data
Classification Credentials and Keys:Data Classification Credit and Risk Management:Data
Classification DPA:Compliance Development Documentation:Data Classification EU:Data Residency
Education:Data Classification FERPA:Compliance FISMA:Compliance Finance:Data Classification
Financial Report:Data Classification Financial Strategy and Research:Data Classification
GDPR:Compliance GLBA:Compliance HIPAA:Compliance HR Documentation:Data Classification
Healthcare:Data Classification Highly Confidential:Sensitivity Information Technology:Data
Classification Insurance and Settlement:Data Classification Internal:Sensitivity JAPAN:Data
Residency LGPD:Compliance Legal:Data Classification License Agreement:Data Classification
Manufacture:Data Classification Medication Management:Data Classification NDA Form:Data
Classification NIST 800-53 and NIST 800-171:Compliance Operational Documentation:Data
Classification PCI_DSS:Compliance PHI:Data Classification PII:Data Classification
PIPEDA:Compliance Patent:Data Classification Payment Card Data:Data Classification Performance
Review:Data Classification Public:Sensitivity Restricted:Sensitivity SOX:Compliance Source
Code:Data Classification Test Documentation:Data Classification Timesheet:Data Classification
Training Materials:Data Classification Transaction Record:Data Classification UK:Data
Residency US:Data Residency User Documentation:Data Classification]
[DEBUG]  2025/06/26 03:20:28.159709 tag_info_service.go:58  Updated tag cache: map
[APPI:Compliance APPs:Compliance ASIA:Data Residency AUSTRALIA:Data Residency BRAZIL:Data
Residency CCPA:Compliance CSL:Compliance Clinical Records:Data Classification Clinical
Studies:Data Classification Compliance and Risk Management:Data Classification
Confidential:Sensitivity Configuration Files:Data Classification Contracts and Agreements:Data
Classification Credentials and Keys:Data Classification Credit and Risk Management:Data
Classification DPA:Compliance Development Documentation:Data Classification EU:Data Residency
Education:Data Classification FERPA:Compliance FISMA:Compliance Finance:Data Classification
Financial Report:Data Classification Financial Strategy and Research:Data Classification
GDPR:Compliance GLBA:Compliance HIPAA:Compliance HR Documentation:Data Classification
Healthcare:Data Classification Highly Confidential:Sensitivity Information Technology:Data
Classification Insurance and Settlement:Data Classification Internal:Sensitivity JAPAN:Data
Residency LGPD:Compliance Legal:Data Classification License Agreement:Data Classification
Manufacture:Data Classification Medication Management:Data Classification NDA Form:Data
Classification NIST 800-53 and NIST 800-171:Compliance Operational Documentation:Data
Classification PCI_DSS:Compliance PHI:Data Classification PII:Data Classification
PIPEDA:Compliance Patent:Data Classification Payment Card Data:Data Classification Performance
Review:Data Classification Public:Sensitivity Restricted:Sensitivity SOX:Compliance Source
Code:Data Classification Test Documentation:Data Classification Timesheet:Data Classification
Training Materials:Data Classification Transaction Record:Data Classification UK:Data
Residency US:Data Residency User Documentation:Data Classification]
[DEBUG]  2025/06/26 03:25:28.159904 tag_info_service.go:58  Updated tag cache: map
[APPI:Compliance APPs:Compliance ASIA:Data Residency AUSTRALIA:Data Residency BRAZIL:Data
Residency CCPA:Compliance CSL:Compliance Clinical Records:Data Classification Clinical
Studies:Data Classification Compliance and Risk Management:Data Classification
Confidential:Sensitivity Configuration Files:Data Classification Contracts and Agreements:Data
```

```
Classification Credentials and Keys:Data Classification Credit and Risk Management:Data
Classification DPA:Compliance Development Documentation:Data Classification EU:Data Residency
Education:Data Classification FERPA:Compliance FISMA:Compliance Finance:Data Classification
Financial Report:Data Classification Financial Strategy and Research:Data Classification
GDPR:Compliance GLBA:Compliance HIPAA:Compliance HR Documentation:Data Classification
Healthcare:Data Classification Highly Confidential:Sensitivity Information Technology:Data
Classification Insurance and Settlement:Data Classification Internal:Sensitivity JAPAN:Data
Residency LGPD:Compliance Legal:Data Classification License Agreement:Data Classification
Manufacture:Data Classification Medication Management:Data Classification NDA Form:Data
Classification NIST 800-53 and NIST 800-171:Compliance Operational Documentation:Data
Classification PCI_DSS:Compliance PHI:Data Classification PII:Data Classification
PIPEDA:Compliance Patent:Data Classification Payment Card Data:Data Classification Performance
Review:Data Classification Public:Sensitivity Restricted:Sensitivity SOX:Compliance Source
Code:Data Classification Test Documentation:Data Classification Timesheet:Data Classification
Training Materials:Data Classification Transaction Record:Data Classification UK:Data
Residency US:Data Residency User Documentation:Data Classification]
```

FortiDeceptor Campaign

FortiDeceptor can connect to EMS, leveraging EMS capabilities to push deception tokens to FortiClient endpoints more efficiently without requiring mobile device management or group policy objects. The following summarizes the workflow for this integration:

1. Configure a Fortinet Security Fabric connector for FortiDeceptor in EMS. This leverages the same Fabric connection that FortiGate uses. See Configuring a Fabric connector for FortiDeceptor in EMS: on page 374.
2. Import a campaign profile from FortiDeceptor to EMS. See Importing a FortiDeceptor campaign profile to EMS on page 375.
3. Apply the profile to the desired endpoint policy. See Applying the profile to the desired endpoint policy on page 376.
4. After FortiClient receives the profile update, it downloads and installs the FortiDeception token. The token deploys lure services across various locations on the endpoint to attract potential attackers. If an attacker triggers the lure, FortiClient generates an incident report and sends it to the FortiDeceptor. If you enabled quarantine integration, the endpoint is automatically quarantined. You can remove the endpoint from quarantine using EMS or FortiDeceptor. See FortiDeceptor integration on FortiClient and EMS on page 376.

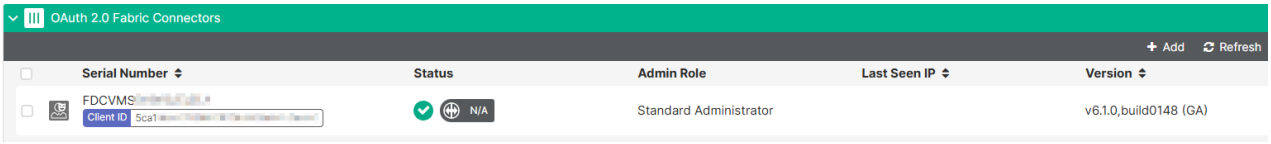
This feature supports FortiClient (Windows) and (Linux).

Configuring a Fabric connector for FortiDeceptor in EMS:

To configure a Fabric connector for FortiDeceptor in EMS:

1. Enable the FortiDeceptor integration feature in EMS:
   a. Go to *System Settings* > *Feature Select*.
   b. Enable *FortiDeceptor (Beta)*.
   c. Click *Save*.
2. Go to *Fabric & Connectors* > *Fabric Devices*.

3. Under *OAuth 2.0 Fabric Connectors*, click *Add*.
4. From the *Connector Type* dropdown list, select *FortiDeceptor*.
5. Configure the fields as applicable for your FortiDeceptor. You can generate the REST API key on FortiDeceptor in *Account* > *REST API* > *Generate*. Click *Test*.
6. After verifying the connection, on the *Admin Settings* tab, configure the fields as desired. For *Role*, the EMS admin role selected defines which EMS APIs (and therefore, features) that the Fabric device connector can access. For example, a Fabric connector that is configured with the Standard administrator role can access EMS APIs for endpoint and policy permissions and has read-only permissions to settings permissions. Click *Finish*.
7. The *Client Credentials* dialog displays the client ID and secret, which are required to configure quarantine integration. Copy these values and save them in a secure location. The client secret is not visible once you close this dialog. Click *Close*.
8. Click *Yes* to confirm closing the dialog. The Fabric connection successfully establishes and displays in the OAuth 2.0 Fabric Connectors list. *Status* updates when quarantine integration is enabled on FortiDeceptor. Otherwise, it displays as *N/A*.



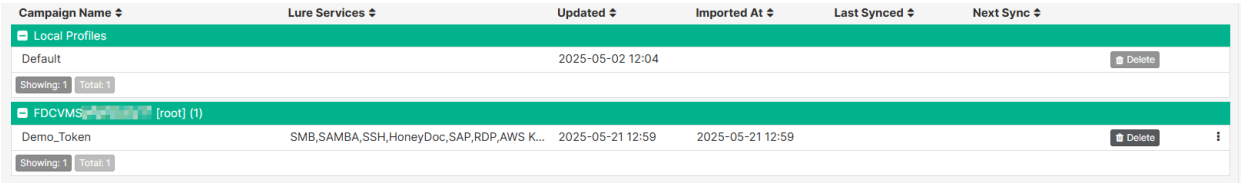
Importing a FortiDeceptor campaign profile to EMS

To import a FortiDeceptor campaign profile to EMS:

1. Go to *Endpoint Profiles* > *FortiDeceptor Campaign*.
2. Click *Import Profile from FortiDeceptor*.
3. From the dropdown list, select the desired FortiDeceptor. Click *Next*.
4. Select the desired FortiDeception token. Click *Next*.
5. Configure the synchronization mode as desired:

Option	Description
One Time Pull	FortiClient EMS does not automatically sync profile changes from the FortiGate or FortiManager. You can manually sync profile changes after importing the profile.
Group Schedule	Configure a group synchronization schedule for all selected profiles. Select the next date and time to automatically update the profiles, and the profile update interval in days, hours, or seconds.
Individual Schedule	Configure an individual synchronization schedule for each selected profile. Select the next date and time to automatically update each profile, and the profile update interval in days, hours, or seconds.

6. Click *Import*. The FortiDeceptor campaign profile displays in the campaign list.



You cannot import a FortiDeceptor campaign profile in EMS. You can edit it in FortiDeceptor and sync it to EMS as per the configured synchronization mode.

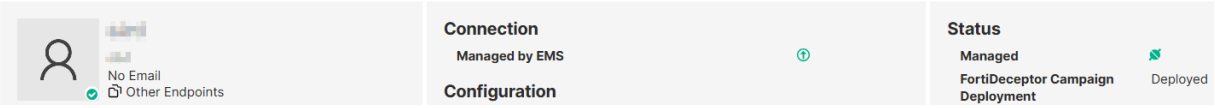
Applying the profile to the desired endpoint policy

To apply the profile to the desired endpoint policy:

1. Go to *Endpoint Policy & Components* > *Manage Policies*.
2. Edit the desired existing policy or create a new one.
3. In the *Profile* > *FDC* dropdown list, select the imported profile.
4. Configure other fields as desired, then click *Save*.

FortiDeceptor integration on FortiClient and EMS

After FortiClient receives the policy change from EMS, FortiClient retrieves the FortiDeception token from EMS and installs it on the endpoint. When viewing the endpoint in EMS, the *Status* > *FortiDeceptor Campaign Deployment* field displays the current status of the token, which progresses from *Pending* to *Notified* to *Deployed*.



In *Endpoints*, you can filter endpoints by their FortiDeceptor campaign deployment status.

After FortiClient installs the token, it strategically distributes lures across various locations on the endpoint. For example, an RDP lure is placed in the Documents folder. Linux supports a limited set of lure types. Possible locations may include the following:

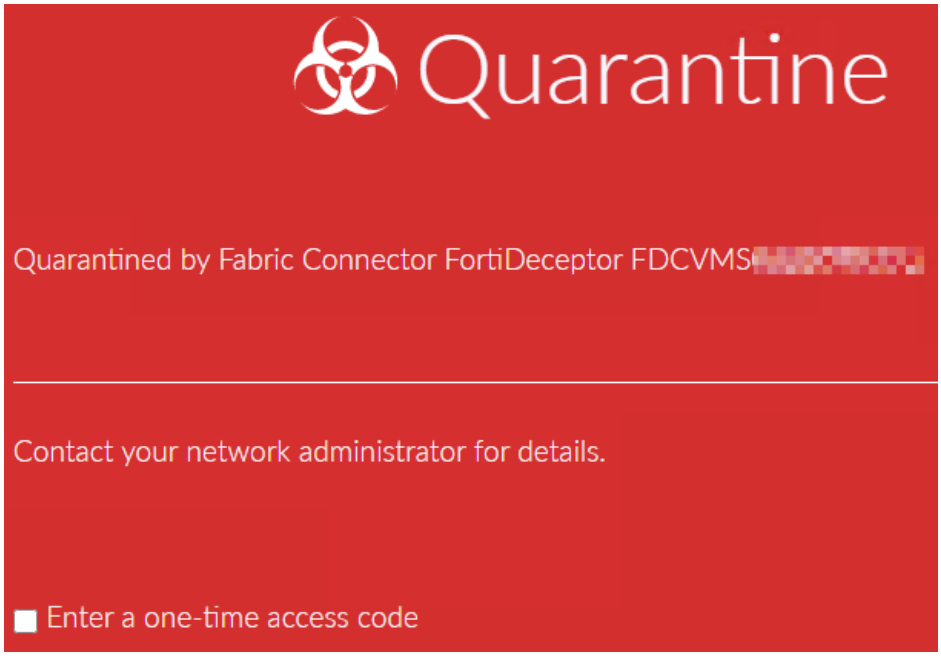
Lure type	OS support	Description
AWS	• Windows	Specify where to create the lure file, aws_access_test2222222222222222_key.JSON, in FortiDeceptor.
Azure	• Windows	Specify where to create the lure file, azure_access.JSON, in FortiDeceptor.
Cached credentials	• Windows	Multiple cmd.exe and conhost.exe processes are created and visible in Task Manager.
HoneyDoc	• Windows	Specify where to create the lure file in FortiDeceptor.

Lure type	OS support	Description
ODBC	• Windows	Added to the User Data sources list and can be viewed using the ODBC Data Source Administrator (32-bit) application.
RDP	• Windows • Linux	RDP config file located in: • Windows: Documents directory • Linux: ~/Documents
SAP	• Windows	sap_logon.ini file created at C:\Users\Username\AppData\Roaming\SAP\Common
SMB/Samba	• Windows • Linux	SMB lure service file installed at: • Windows: Documents directory. Run `net use` command in Command Prompt to display all active SMB connections, including the lure. • Linux: ~/Documents
SSH	• Windows • Linux	SSH config file located at: • Windows: C:\Usersfct2\.ssh\config • Linux: ~/.ssh/config

When a lure service is triggered on the endpoint, FortiClient detects the event and reports the incident to FortiDeceptor. For example, if an RDP file is executed, it initiates a connection to the remote decoy machine, and the incident is logged in FortiDeceptor in *Incident > Analysis*.

Quarantine integration

If FortiDeceptor is configured with quarantine integration, it can automatically quarantine an endpoint when a lure service is triggered.



You can remove an endpoint from quarantine using FortiDeceptor or EMS.

To remove an endpoint from quarantine:

Do one of the following:

- To remove an endpoint from quarantine using FortiDeceptor, go to *Fabric > Quarantine Status*, select the endpoint, and click *Unblock*.
- To remove an endpoint from quarantine using EMS, see Quarantining an endpoint on page 79.

FortiClient sends FortiDeceptor quarantine events to EMS. You can view them on the endpoint *System Events* tab.

Removing the FortiDeceptor token from an endpoint

You can disable the FortiDeceptor profile from an endpoint. For example, you can reconfigure the assigned endpoint policy to use the default FortiDeceptor profile, which is not configured with tokens. When FortiClient receives the profile change, it uninstalls the token and removes all lures from the endpoint. In *Endpoints*, the *FortiDeceptor Campaign Deployment* status progresses from *Pending to uninstall* to *Notified to uninstall* to *Clean*. The *FortiDeceptor Campaign Deployment* field will eventually no longer be visible for the endpoint.

System Settings

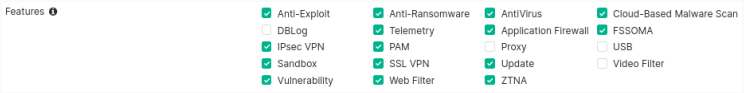
The majority of these configuration options are only available for Windows, macOS, and Linux profiles. The table indicates which options are available for Chromebook profiles, such as *Upload Logs to FortiAnalyzer/FortiManager*.

Some options are only available when *Advanced* view is enabled.

Configuration		Description
UI		Specify how the FortiClient user interface appears when installed on endpoints.
Require Password to Disconnect from EMS		Turn on password lock for FortiClient.
	Password	Enter a password. The endpoint user must enter this password to disconnect FortiClient from FortiEndpoint.
	Allow endpoint admin to disconnect without a password	This setting is only available if you enable *System Setting > UI > Require Password to Disconnect from EMS* and provide a password. This allows the FortiClient endpoint administrator to uninstall FortiClient using the msiexec command line without needing to use the configured EMS disconnection password. This feature is especially useful if you are using a mobile device management solution to deploy FortiClient. Because FortiClient endpoint users have no administrative privileges, so there is no risk that an endpoint user could intentionally or accidentally uninstall FortiClient.

Configuration	Description
Do Not Allow User to Back Up Configuration	Disallow users from backing up the FortiClient configuration.
Allow User to Shutdown When Registered to EMS	Allows user to shut down FortiClient while registered to EMS. This feature is only available for FortiClient (Windows). The user must have admin privileges to shut down FortiClient.
Hide User Information	Hide the User Details panel where the user can provide user details (avatar, name, phone number, email address), and link to a social media (LinkedIn, Google, Salesforce) account.
Hide System Tray Icon	Hide the FortiClient system tray icon.
Show Host Tag on FortiClient GUI	Show the applied host tag on the FortiClient GUI. See Security Posture Tags on page 408.

Configuration	Description
Language	Configure the language that FortiClient uses. By default, FortiClient uses the system operating language. Select one of the following: • os-default (System operating language, selected by default) • zh-tw (Taiwanese Mandarin) • cs-cz (Czech) • de-de (German) • en-us (United States English) • fr-fr (French) • hu-hu (Hungarian) • ru-ru (Russian) • ja-jp (Japanese) • ko-kr (Korean) • pt-br (Brazilian Portuguese) • sk-sk (Slovak) • es-es (Spanish) • zh-cn (Chinese (Simplified)) • et-ee (Estonian) • lv-lv (Latvian) • lt-lt (Lithuanian) • fi-fi (Finnish) • sv-se (Swedish) • da-dk (Danish) • pl-pl (Portuguese (Portugal)) • nb-no (Norwegian) • fr-ca (Canadian French)
Default Tab	From the dropdown list, select the tab for FortiClient to display by default when the user opens the console.
Log	Specify FortiClient log settings.

Configuration	Description
Level	This option is available for Chromebook profiles. Generates logs equal to and more critical than the selected level. Select one of the following: • Emergency: The system becomes unstable. • Alert: Immediate action is required. • Critical: Functionality is affected. • Error: An error condition exists and may affect functionality. • Warning: Functionality could be affected. • Notice: Information about normal events. • Info: General information about system operations. • Debug: Debug FortiClient. Detailed debug logs for the selected features are generated on the endpoint. You can request the creation and download of the diagnostic tool output, which includes these logs.
Features	Select features to generate logs for: 
Client-Based Logging When On-Fabric	Include local log messages when FortiClient is on-fabric. FortiClient hides the *Export log* and *Clear log* options from the GUI when the endpoint is off-fabric. FortiClient still sends logs to FortiAnalyzer, if one is configured. If the FortiAnalyzer is unreachable because endpoint is off-fabric, FortiClient retains the logs until it can reach FortiAnalyzer and forward the logs. See On-fabric Detection Rules on page 124.
Upload Logs to FortiAnalyzer/FortiManager	This option and all nested options are available for Chromebook profiles. Configure endpoints to sends logs to the FortiAnalyzer or FortiManager at the specified address or hostname. The *Upload Vulnerability Logs* and *Upload Event Log* fields only apply to FortiClient 6.4.2 and earlier versions. This field does not allow configuration to send endpoint logs to a syslog server. For endpoints to send logs to a syslog server, you must configure `<log_protocol>` and `<netlog_server>`. See Log settings.
IP Address/Hostname	Enter the FortiAnalyzer or FortiManager IP address or hostname/FQDN. If using a port other than the default, use `<address>:<port>`. With Chromebook profiles, use the format `https://FAZ-IP:port/logging`.

Configuration		Description
		For FortiAnalyzer Cloud, enter the FQDN that you use to access the FortiAnalyzer Cloud instance (such as `1208151.ca-west-1.fortianalyzer.forticloud.com`). You must also configure the SNI for FortiAnalyzer Cloud by switching to the XML view and adding the `<log_uploadserver_sni>` tag (see Log settings).
	SSL Enabled	Enable SSL.
	Upload UTM Logs	Upload unified threat management (traffic) logs to FortiAnalyzer or FortiManager.
	Upload Vulnerability Logs	Upload vulnerability logs to FortiAnalyzer or FortiManager.
	Upload Event Logs	Upload event logs to FortiAnalyzer or FortiManager.
	Upload System Event	Upload system events to FortiAnalyzer or FortiManager. This includes logs for endpoint control, update, and FortiClient events.
	Upload Security Event	Upload security events to FortiAnalyzer or FortiManager. This includes logs for Malware Protection, Web Filter, Vulnerability Scan, and Application Firewall events.
	Send Software Inventory	EMS sends FortiClient software inventory to FortiAnalyzer or FortiManager.
	Send OS Events	EMS sends endpoint host events to FortiAnalyzer or FortiManager. EMS supports this feature for Windows and macOS endpoints. For Windows endpoints, FortiClient sends all events found in the Windows Events Viewer under the System, Security, and Applications categories, including user login and logout. For macOS endpoints, OS event logs are stored at `/var/log/system.log`. For details on what events are sent to FortiAnalyzer or FortiManager, see FortiAnalyzer documentation, such as Windows Events logs or Threat Hunting.
	Event telemetry interval	Enter the interval in seconds for FortiClient to upload OS events to FortiAnalyzer or FortiManager.
	Upload Schedule	Configure the interval in minutes for FortiClient to upload logs to FortiAnalyzer or FortiManager. If there are no logs, no upload takes place.
	Log Generation Timeout	Configure the maximum time in seconds for FortiClient to gather logs before sending them to FortiAnalyzer or FortiManager.
	Log Retention	Configure the amount of time in days that logs are kept locally on the endpoint before starting to rewrite them.

Configuration		Description
Proxy		
Use Proxy for Updates		Access FortiGuard using the configured proxy. FortiClient (macOS) does not support signature update via proxy.
	Connect to FDN Directly If Proxy Is Offline	Connect to FDN directly if proxy is offline.
Use Proxy for Virus Submission		Use the configured proxy to submit viruses to FortiGuard.
	Type	Configure the type. Options include: • http • socks4 • socks5
	IP Address/Hostname	Enter the proxy server's IP address/hostname.
	Port	Enter the proxy server's port number. The port range is from 1 to 65535.
	Username	If the proxy requires authentication, enter the username. Enter the encrypted or non-encrypted username.
	Password	If the proxy requires authentication, enter the password. Enter the encrypted or non-encrypted username. Enable *Show Password* to show the password in plain text.
Update		Specify whether to use FortiManager to update FortiClient on endpoints.
Use FortiManager for Client Signature Update		Enable FortiEndpoint to obtain antivirus (AV) signatures from the FortiManager at the specified IP address or hostname.
	IP Address/Hostname	Enter the FortiManager IP address/hostname.
	Port	Enter the port number.
	Failover Port	Enter the failover port.
	Timeout	Enter the timeout interval.
	Failover to FDN When FortiManager Is Not Available	Fail over to FDN when FortiManager is not available.
FortiGuard Server Location		Configure the FortiGuard server location. If *FortiGuard Anycast* is selected for the *Server* field, you can select from global, U.S., or Europe. If *FortiGuard* is selected for the *Server* field, you can select from global or U.S. When *Global* is selected, FortiClient uses the closest FortiGuard server.

Configuration		Description

		FortiClient connects to FortiGuard to query for AV and vulnerability scan engine and signature updates.
		The URLs connected to for each server location are as follows:
		• FortiGuard:
		  • Global: forticlient.fortinet.net
		  • U.S.: usforticlient.fortinet.net
		• FortiGuard Anycast:
		  • Global: fctupdate.fortinet.net
		  • U.S.: fctusupdate.fortinet.net
		  • Europe: fcteuupdate.fortinet.net

Server		Configure the FortiGuard server to *FortiGuard* or *FortiGuard Anycast*.
Endpoint Control		
Show Bubble Notifications		Show bubble notifications when FortiClient installs new policies on endpoints.
Log off When User Logs Out of Windows		Log off FortiClient when the endpoint user logs out of Windows. Turn off to remain logged in.
Disable Disconnect		Forbid users from disconnecting FortiClient from FortiEndpoint.
On-Fabric Subnets		Turn on to enable on-fabric subnets. This option only applies for endpoints running FortiClient 6.2.1 and earlier versions. For endpoints running FortiClient 6.2.2 and later versions, see On-fabric Detection Rules on page 124.
	IP Addresses/Subnet Masks	Enter IP addresses/subnet mask to connect to on-fabric subnets.
	Gateway MAC Address	Enable gateway MAC address.
	MAC Addresses	Enter MAC addresses.
Send Software Inventory		Send installed application information to FortiEndpoint. If the *Upload Logs to FortiAnalyzer/FortiManager* option is enabled, the endpoint also sends the software inventory information to FortiAnalyzer. See Software Inventory on page 450.
Invalid Certificate Action		Select the action to take when FortiClient attempts to connect to EMS with an invalid certificate: • **Allow**: allows FortiClient to connect to EMS with an invalid certificate.

Configuration	Description
	• **Warn**: warn the user about the invalid server certificate. Ask the user whether to proceed with connecting to EMS, or terminate the connection attempt. FortiClient remembers the user's decision for this EMS, but displays the warning prompt if FortiClient attempts to connect to another EMS (using a different EMS FQDN/IP address and certificate) with an invalid certificate. • **Deny**: block FortiClient from connecting to EMS with an invalid certificate.
Enable Forensics Feature	Enable the forensic analysis feature. You can request forensic analysis on a suspected device from on-premise EMS. The Fortinet forensics team investigates the logs and provides a detailed report with their verdict. You can download the report from EMS. See Requesting forensic analysis on an endpoint on page 83.
Enable DNS Cache	When enabled, FortiClient uses the previously resolved EMS IP address only when the DNS server fails to respond to the endpoint DNS query. FortiClient keeps the cached EMS IP address in memory.
User Identity Settings	

Allow Users to Specify Identity Using	Enable users to specify their identity in FortiClient using the following methods:
	• Manually entering their details in FortiClient
	• Logging in to their account for the following social media services:
	  • LinkedIn
	  • Google
	  • Salesforce
	By default, EMS obtains user details from the endpoint OS. If the user provides their details using one of the methods above, EMS obtains the user-specified details instead.
	If this option is disabled, EMS obtains and displays user details from the endpoint OS.

Notify Users to Submit User Identity Information	Displays a notification on the endpoint for the user to specify their identity. If the user closes the notification without specifying their identity, the notification displays every ten minutes until the user submits their identity information.
Other	
Install CA Certificate on Client	Turn on to select and install a CA certificate on the FortiClient endpoint.

Configuration		Description
		You can add certificates by going to *Endpoint Policy & Components > CA Certificates*. See CA Certificates on page 122. For FortiClient (iOS) and (Android), the certificate is not installed on the endpoint. The user must manually download and install the certificate. The Telemetry page displays a message instructing the user to do so after saving a certificate in the download folder (Android) or *Files* (iOS) that EMS sent.
FortiClient Single Sign-On Mobility Agent		Enable Single Sign-On Mobility Agent (SSOMA) for FortiAuthenticator. To use this feature you need to apply a FortiClient SSO mobility agent license to your FortiAuthenticator. When SSOMA is enabled and a Windows user locks their screen, disconnects from RDP, or the device sleeps from inactivity, FortiClient SSOMA is not logged out and stays in the FortiAuthenticator logging session. If a different user signs in, FortiClient sends a logout message to FortiAuthenticator for the original user, then a logon message with the new user. If the original user logs in, the user session is not interrupted. The `<prefer_azure>` element affects this feature. See SSOMA.
	IP Address/Hostname	Enter the FortiAuthenticator IP address or hostname.
	Port	Enter the port number.
	Pre-Shared Key	Enter the preshared key. The preshared key should match the key configured on your FortiAuthenticator.
iOS		
Distribute Configuration Profile		EMS no longer supports this option. See one of the following for instructions on pushing configuration to FortiClient (iOS): • Creating a Mobileconfig profile • Intune Deployment Guide • Workspace ONE Deployment Guide • Jamf Deployment Guide
Privacy		
Send Usage Statistics to Fortinet		Submit virus information to FDS. Fortinet uses this information to improve product quality and user experience.

Configuration	Description
Privileged Access Agent	Enable privileged access management (PAM). This enables FortiClient to communicate with FortiPAM.
Port	Enter the port for FortiClient to use to communicate with FortiPAM. The default port for this communication is 9191. If you change this value, ensure that you also change it in FortiPAM.

The System Setting profile has several settings available to configure for client signature updates. The following summarizes which setting takes effect in various scenarios:

Use FortiManager for Client Signature Update	*Failover to FDN When FortiManager Is Not Available*	Result
Disabled	Disabled	FortiClient uses *FortiGuard Server Location* and *FortiGuard Server Type* settings for client signature updates.
Enabled	Enabled or disabled	FortiClient prioritizes updating signatures using the configured FortiManager settings. This configuration supports port failover. FortiClient uses the same protocol as configured for FortiGuard (dependent on whether legacy or Anycast FortiGuard is selected) to connect to FortiManager.
Enabled without FortiManager settings configured	Enabled	FortiClient fails over to FortiGuard based on the FortiGuard server settings.

Configuring identity compliance for endpoints

You can assign different user identification options to different endpoints. These options, visible in FortiClient, include:

- User input
- OS
- LinkedIn
- Google
- Salesforce

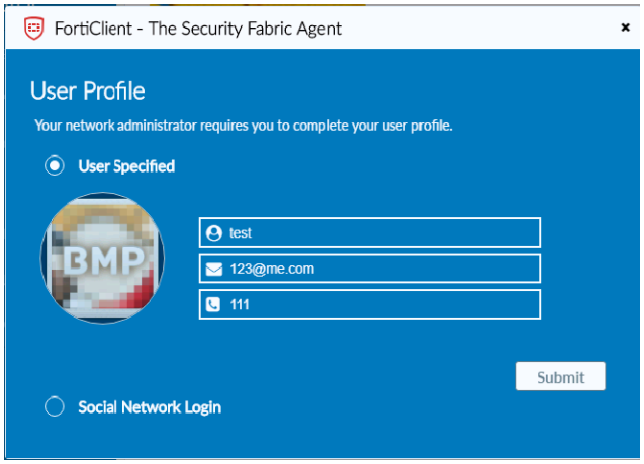
EMS sends a notification to the endpoint where the user must enter their login information. If the user closes the notification without entering any information, the notification appears again within ten minutes.

To configure identity compliance:

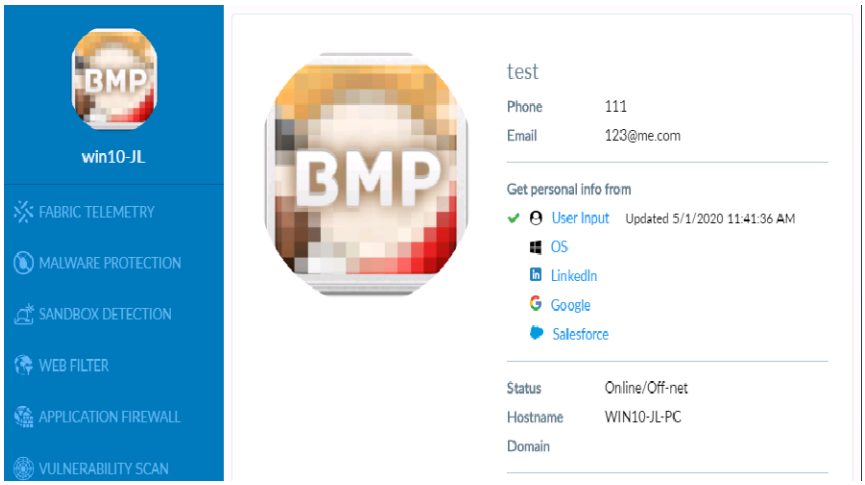
1. In EMS, go to *Endpoint Profiles*. Select the desired *System Settings* profile or create a new one.
2. Under *User Identity Settings*, enable the desired user identification method.

3. If desired, enable *Notify Users to Submit User Identity Information*.
4. Click *Save*.

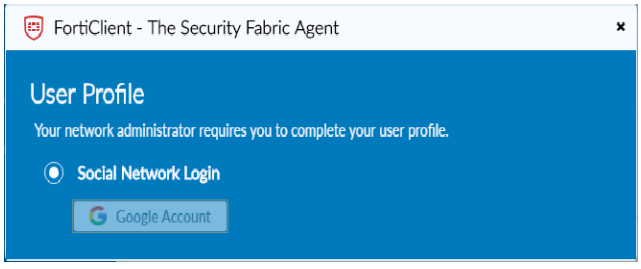
When *Notify Users to Submit User Identity Information* is enabled, the user sees the following notification on the endpoint. If *Manually Enter User Details* is enabled, the user can enter their information manually.



FortiClient displays the entered login information.



If *Google* is enabled, the user can log in to their Google account.



FortiClient displays the Google login information.

FortiPAM integration

To configure the FortiPAM integration for FortiClient, you must configure the following:

- FortiPAM. The following instructions assume that you have a licensed FortiPAM ready for configuration. See To configure FortiPAM: on page 389.
- Enable the FortiPAM feature in EMS. If using a standalone FortiPAM agent, there is no EMS involved. See To enable the FortiPAM feature in EMS: on page 392.
- Install FortiClient with the FortiPAM feature enabled, then register FortiClient to EMS. Ensure that the FortiPAM password filler extension is installed in the browser. See To install FortiClient with the FortiPAM feature enabled and verify the configuration: on page 392.

This document also describes the following use cases:

- To configure a secret for SSH to a FortiGate: on page 393
- To use a secret to log in to a website: on page 394

To configure FortiPAM:

1. Log in to FortiPAM via the console.
2. Configure the management IP address, default gateway, and DNS settings:

```
config system dns
    set primary 208.91.112.53
    set secondary 96.45.46.46
end
config router static
    edit 1
        set gateway 172.17.162.3
        set device "port1"
    next
end
config system interface
    edit "port1"
        set ip 172.17.162.167 255.255.254.0
        set allowaccess ping ssh telnet
        set type physical
        set monitor-bandwidth enable
        set snmp-index 1
    next
end
```

3. Clear the browser cache.
4. Upload a license to FortiPAM as To upload the license via the FortiPAM-VM GUI: describes.
5. Configure zero trust network access (ZTNA) rules and server in FortiPAM. This example sets the ZTNA server external IP address to 172.17.162.166. Users log in to FortiPAM with this IP address to launch a secret.

```
config firewall vip
    edit "fortipam_vip"
        set uuid 188232bc-3534-51ed-897e-7d522767d173
```

```
        set type access-proxy
        set extip 172.17.162.166
        set extintf "any"
        set server-type https
        set extport 443
        set ssl-certificate "Fortinet_SSL"
    next
end
config firewall access-proxy
    edit "fortipam_access_proxy"
        set vip "fortipam_vip"
        config api-gateway
            edit 1
                set url-map "/pam"
                set service pam-service
            next
            edit 2
                set url-map "/tcp"
                set service tcp-forwarding
                config realservers
                    edit 1
                        set address "all"
                    next
                end
            next
            edit 3
                set service gui
                config realservers
                    edit 1
                        set ip 127.0.0.1
                        set port 80
                    next
                end
            next
        end
    next
end
config firewall policy
    edit 1
        set type access-proxy
        set uuid 075cff8c-4e1e-51ed-4d83-41cb5da1944e
        set srcintf "any"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set access-proxy "fortipam_access_proxy"
        set groups "SSO_Guest_Users"
        set ssl-ssh-profile "deep-inspection"
    next
end
```

6. Log in to FortiPAM as the admin user account. Add a "demo" user that will be used to log in to FortiPAM to launch predefined secrets for the user, or allow the user to create their own secret:

```
config system admin
    edit "demo"
        set accprofile "Power User"
        set password "1"
    next
end
```

7. Create a secret folder. This example folder is called "f-demo". In FortiPAM, each secret must belong to a secret folder. The FortiPAM administrator can assign appropriate permissions for a user to the folder, such as owner or view-only permissions. Give owner permissions to the demo and admin users for the f-demo folder:

```
config secret folder
    edit 5
        set name "f-demo"
        set inherit-policy disable
        set inherit-permission disable
        config user-permission
            edit 1
                set user-name "demo" "admin"
                set folder-permission owner
                set secret-permission owner
            next
        end
    next
end
```

8. Add the "RDP Secret Launcher" secret and make it display in the f-demo folder. This example folder ID is 5:

```
config secret database
    edit 22
        set name "RDP Secret Launcher"
        set folder 5
        set template "Windows Machine"
        set recording enable
        set proxy enable
        set block-rdp-clipboard disable
        set rdp-service-status up
        set samba-service-status up
        config credentials-history
        end
        config field
            edit 1
                set name "Host"
                set value "172.17.60.8"
            next
            edit 2
                set name "Username"
                set value "qa"
```

```
            next
            edit 3
                set name "Password"
                set value "ENC lLUCAA722LevoHAohj7+Jnsyp0A="
            next
        end
    next
end
```

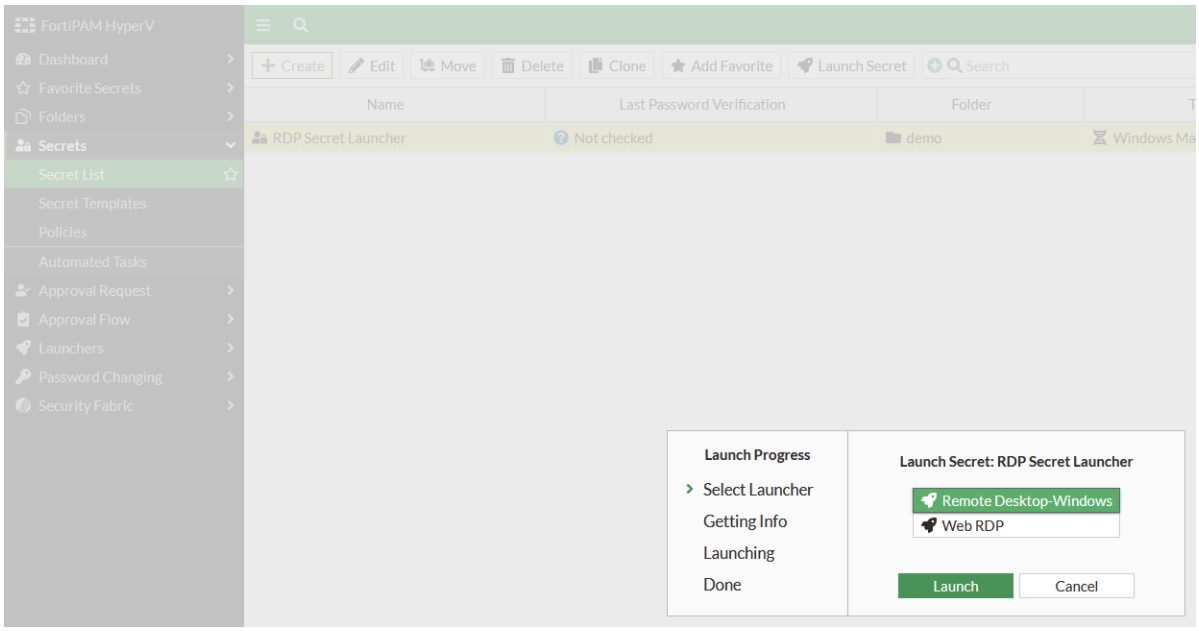
To enable the FortiPAM feature in EMS:

1. The default port for communication between FortiPAM and EMS is 9191. This must match the port configured in FortiPAM in *System > Settings > Client Port*. To use a custom port, modify the port in both EMS and FortiPAM. In EMS, go to *Endpoint Profiles > System Settings*.
2. Edit the desired profile or create a new one.
3. Enable *Privileged Access Agent*.
4. In the *Port* field, enter 9191.
5. Click *Save*.
6. Go to *System Settings > ZTNA Destinations*.
7. Enable *Allow Personal Destinations*. You must enable *Allow Personal Destinations* for FortiPAM to proxy RDP and SSH connections.
8. Click *Save*.

To install FortiClient with the FortiPAM feature enabled and verify the configuration:

1. On an endpoint with the FortiPAM feature enabled, open Task Manager. Confirm that the Fortvrs.exe and Fortitcs.exe daemons are running.
2. On the desired browser, ensure that the FortiPAM password filler extension is installed.
3. In FortiPAM, go to *Secrets > Secret List*.
4. Select *RDP Secret Launcher*, then click *Launch Secret*.

5. Select *Remote Desktop-Windows*, then click *Launch*.



6. In the prompt, select *Yes*. You should successfully log in to the remote Windows machine without needing to enter credentials.

To configure a secret for SSH to a FortiGate:

1. Install PuTTY on the client machine.
2. Install FortiClient on the endpoint. The FortiPAM feature must be enabled.
3. Register FortiClient to EMS. Ensure that the profile assigned to the endpoint has the FortiPAM feature enabled.
4. Log in to FortiPAM as the administrator. Add the SSH secret:
   a. Obtain the ID for the secret folder that you will use for this secret by running `show secret folder`. The example desired directory is f-demo, which has an ID of 5.
   b. Obtain the list of secret IDs being used by running `show secret database`. In this example, the ID 22 is already being used. The example uses 23 as the ID for the new SSH secret:

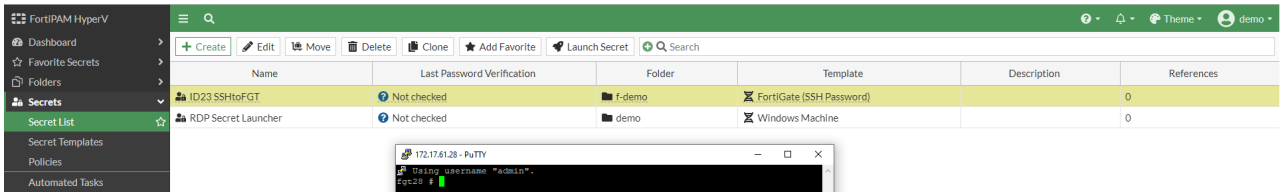
```
show secret database
id    Secret ID.
22  RDP Secret Launcher
```

   c. Add a secret for SSH to FortiGate, using secret ID 23. The following commands enable proxy and session recording. Replace the demo, host, username, password, and URL values for your own configuration before running the commands:

```
config secret database
    edit 23
        set name "ID23 SSHtoFGT"
        set folder 5
        set template "FortiGate (SSH Password)"
        set recording enable
        set proxy enable
```

```
        set ssh-filter enable
        set ssh-filter-profile "DEMO"
        set ssh-service-status up
        config credentials-history
        end
        config field
            edit 1
                set name "Host"
                set value "172.17.61.28"
            next
            edit 2
                set name "Username"
                set value "admin"
            next
            edit 3
                set name "Password"
                set value "ENC kseKVIslSftEmwBy8OqUPyYryoA="
            next
            edit 4
                set name "URL"
                set value "https://172.17.61.28"
            next
        end
    next
end
```

5. In Microsoft Edge, log in to FortiPAM as the demo user to launch the secret and ensure that it works properly by going to *Secrets* > *Secret List*, selecting the newly created, secret, and clicking *Launch Secret*. Edge is preferred over Chrome and Firefox for testing this configuration. You should be able to log in to FortiOS successfully without needing to provide for credentials. A PuTTY dialog opens. After the end of the session, go to *Log & Reports* > *Secrets* > *Secret Video* to ensure that a video was recorded as configured.



To use a secret to log in to a website:

The following provides instructions on how to use a secret to log in to a website. The example website is AWS.

1. Log in to FortiPAM and create a secret to log in to AWS:

```
config secret database
    edit 25
        set name "Login AWS"
        set folder 5
        set template "AWS Web Account"
        set recording enable
```

```
        set proxy enable
        config credentials-history
        end
        config field
            edit 1
                set name "URL"
                set value "https://aws.amazon.com/"
            next
            edit 2
                set name "Username"
                set value "yours@gmail.com"
            next
            edit 3
                set name "Password"
                set value "ENC yNhlyigiX2TX0nJNuetRYI3EJI4="
            next
            edit 4
                set name "AccountID"
            next
        end
    next
end
```

2. Click *Launch Secret*.
3. Click *Sign in*.
4. Click the root user email address.
5. Select *Use FortiPAM session credentials* to autofill the user account, then click *Next*.
6. Select *Use FortiPAM session credentials* to autofill in the password, then click *Sign in*. FortiClient starts the session recording and sending the video to FortiPAM until the session finishes.



To debug the integration:

By default, FortiClient-side FortiPAM daemon (fortivrs.exe) debug logs are enabled. File names are as follows. You can find the files in the trace folder:

- fortivrs_session_0_1.log
- fortivrs_session_1_1.log

The C:\Users\Public\FortiClient\ztna\config.json directory contains zero trust network access (ZTNA) rules. In the example from To use a secret to log in to a website: on page 394, the file contains one ZTNA rule entry as follows: `{"rules": [{"name":"InternalPamRuleItem1","mode":"transparent","destination":"aws.amazon.com:443","gateway":"172.17.162.166:443","encryption":0}]}`.

To debug on the FortiPAM side, you can do the following:

- Go to *Network* > *Packet Capture*.
- Use the following commands to troubleshoot:

```
diagnose debug enable
diagnose wad debug enable level verbose
diagnose wad debug enable category secret
diagnose wad debug enable category ssh
diagnose debug console timestamp enable
```

Add FortiPAM agent to SSOMA

You must separately purchase FortiClient single sign on mobility agent (SSOMA) licenses for use of SSO features with FortiAuthenticator. Most key private access management (PAM) features require the FortiClient PAM agent. FortiClient supports installing SSOMA and FortiPAM agent on the same device.

You can use the following methods to install FortiPAM and SSOMA on the same device. You can also use these same methods to upgrade an existing SSOMA-only or FortiPAM-only endpoint to include both features:

- **Method 1:** Install FortiPAM, export and edit the configuration file to include the SSOMA configuration, and reimport the configuration file.
- **Method 2:** Install and run the SSO configuration tool file to create new installer files, and run the installers to install or upgrade the FortiClient PAM agent.

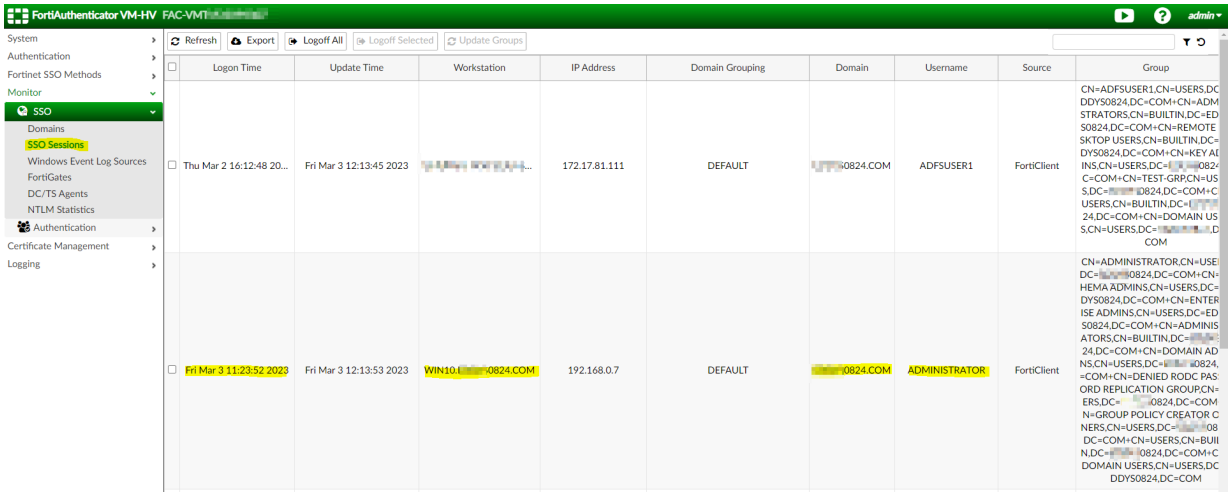
To use Method 1:

1. Install FortiPAM using an installer.
2. In Command Prompt, go to the FortiClient directory.
3. Export the configuration file using the following command: `FCConfig.exe -o export -f C:\config.conf -p 11111111`
4. Edit the configuration file and add the SSOMA configuration. Confirm that the FortiPAM default port is configured as 9191. The following provides an example:

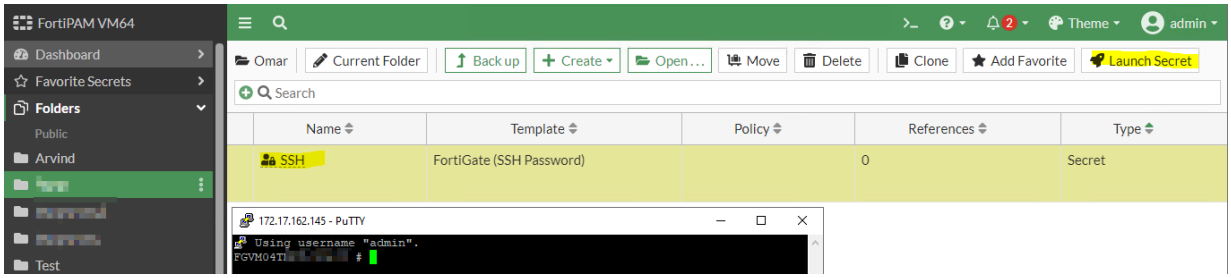
```
<forticlient_configuration>
     <fssoma>
              <enabled>1</enabled>
              <serveraddress>fac0824.test.local:8001</serveraddress>
              <presharedkey>
             <![CDATA[Fortinet123!]]>
             </presharedkey>
             <address_category>0</address_category>
      </fssoma>
```

```
        <pam>
            <enabled>1</enabled>
            <default_port>9191</default_port>
        </pam>
</forticlient_configuration>
```

5. Save the configuration file.
6. In Command Prompt, go to the FortiClient directory.
7. Import the configuration file using the following command: `FCConfig.exe -o import -f C:\config.conf -p 11111111`
8. Verify the configuration:
   a. Log in to the endpoint as a domain user.
   b. In FortiAuthenticator, go to *Monitor* > *SSO* > *SSO Sessions* to confirm whether the SSOMA session is functioning.



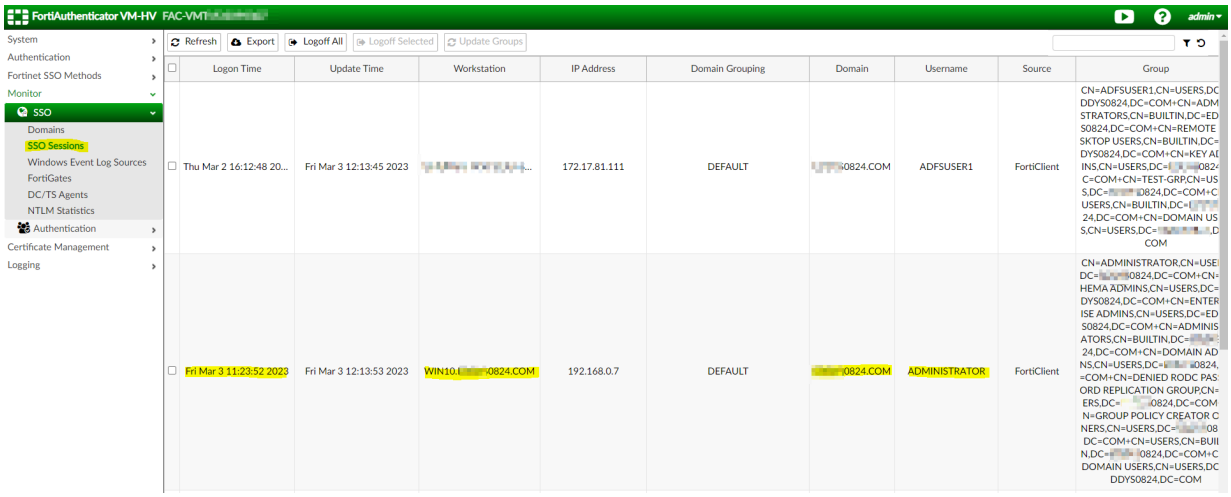
   c. In FortiPAM, confirm that you can access a secret created in FortiPAM.



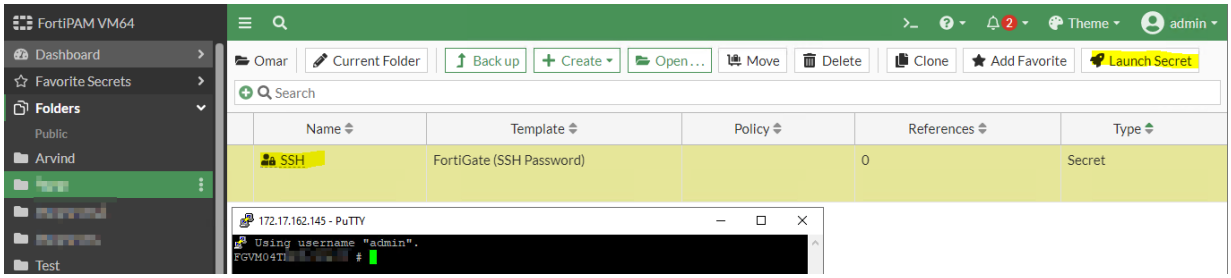
To use Method 2:

1. Acquire and unzip the FortiClientSSOConfigurationTool_26.1.b.[[[Undefined variable FortinetVariables.Build]]].zip file.
2. Run the FortiClientSSOConfigurator.
3. In the Single Sign-On Mobility Agent Settings dialog, configure SSOMA as per your deployment.
4. Enable *Include PAM*.
5. In the *PAM Port* field, enter 9191. Click *Next*. This creates a new folder, which includes x64 and x86 bit installer files.

6. Open Command Prompt as an administrator, and run the following command to run the installer:
   `msiexec /i FortiClientSSO.msi TRANSFORMS=FortiClientSSO.mst\`
7. Verify the configuration:
   a. Log in to the endpoint as a domain user.
   b. In FortiAuthenticator, go to *Monitor* > *SSO* > *SSO Sessions* to confirm whether the SSOMA session is functioning.



   c. In FortiPAM, confirm that you can access a secret created in FortiPAM.



Configuring SSOMA with AD

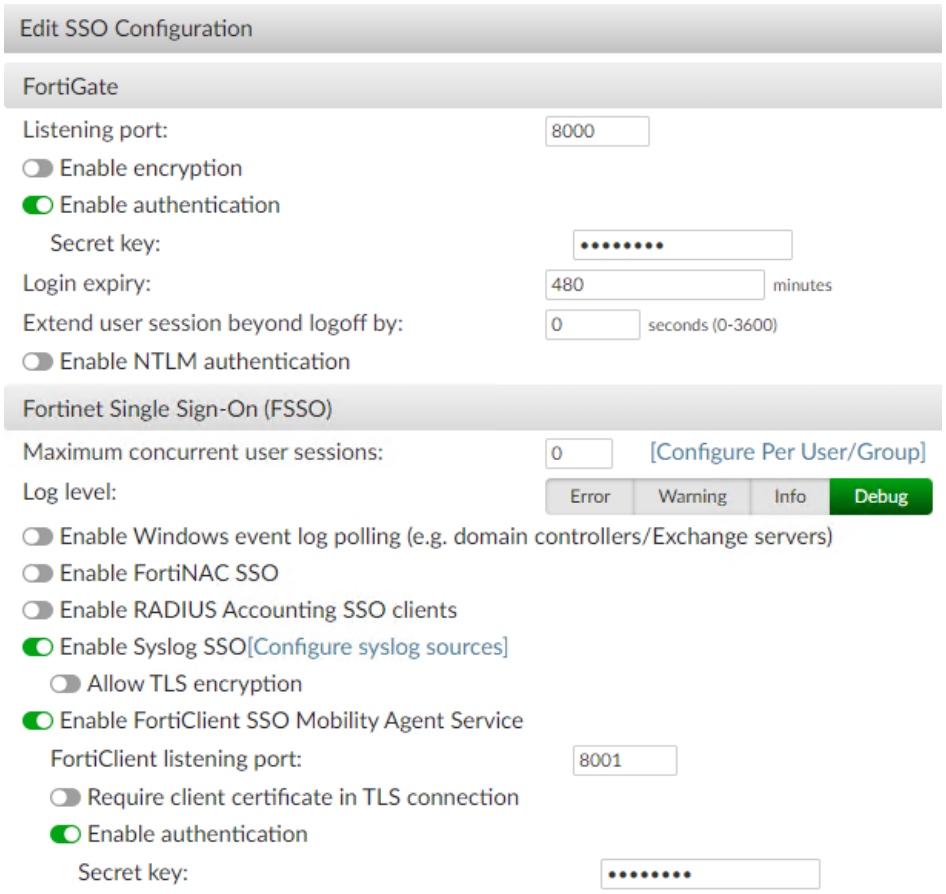
The FortiClient single sign on mobility agent (SSOMA) supports the following features:

- Support for pure Microsoft Entra ID (formerly known as Azure Active Directory (AD)) mode. SSOMA sends the Entra ID domain and tenant ID to FortiAuthenticator in pure/native Entra ID mode. On FortiClient macOS, the Entra ID JAMF Connector is required.
- Sends FortiClient UUID and EMS serial number/tenant ID to FortiAuthenticator.
- Sets the SNI field when communicating with FortiAuthenticator.

The following document uses two use cases to illustrate these features. Use case A illustrates a scenario using a local AD. Use Case B illustrates a scenario using a pure/native Entra ID or a hybrid Entra ID.

Use case A: local AD

1. Configure FortiAuthenticator:
   a. In FortiAuthenticator, go to *Fortinet SSO Methods > SSO > General*.
   b. Toggle on *Enable FortiClient SSO Mobility Agent Service*.
   c. In the *FortiClient listening port* field, enter 8001.
   d. Toggle on *Enable authentication*.
   e. In the *Secret key* field, enter the desired preshared key. In this example, it is Fortinet123!



   f. Go to *Authentication > Remote Auth. Servers > LDAP*.
   g. Add the remote authentication server. In this case, it is the local AD server.
2. In EMS, edit the desired endpoint profile's XML configuration to match the IP address, port, and PSK configured on the FortiAuthenticator:

```
<fssoma>
        <enabled>1</enabled>
        <serveraddress>fac0824.local:8001</serveraddress>
        <presharedkey>Fortinet123!</presharedkey>
</fssoma>
```

3. After FortiClient connects to EMS and receives the profile changes, go to *Settings*. Under *Advanced*, confirm that SSOMA is enabled and the configuration is updated.

4. Under *Logging*, click *Export logs*. Confirm that SSOMA sends the FortiClient UUID and EMS serial number/tenant ID to FortiAuthenticator:

```
6/13/2023 11:38:04 AM    debug    fsso    UUID:2ECE708...

6/13/2023 11:38:04 AM    debug    fsso    strUsername:administrator,
strAZDomain:MYFOREST.LOCAL

6/13/2023 11:38:26 AM    debug    fsso    GetAZureSessionUserInfo(), Calling of
RunExternalProgram is successful
6/13/2023 11:38:26 AM    debug    fsso    GetAZureSessionUserInfo(), Calling of
ParseConsoleOutput is failed, error:-1
6/13/2023 11:38:26 AM    debug    fsso    session ID:2 has added to session table
6/13/2023 11:38:26 AM    debug    fsso    Succeede to add session 2
6/13/2023 11:38:26 AM    debug    fsso    Found current user, session ID: 2
6/13/2023 11:38:26 AM    debug    fsso    CSessionManager::AddSession has been called,
dwSession:65536
6/13/2023 11:38:26 AM    debug    fsso    Failed to call WTSQueryUserToken for session
ID:65536,error:2
6/13/2023 11:38:26 AM    debug    fsso    Failed to get token for session
ID:65536,error:2
6/13/2023 11:38:26 AM    debug    fsso    failed to add session 65536
6/13/2023 11:38:26 AM    debug    fsso    current active session 2
6/13/2023 11:38:26 AM    debug    fsso    Found current logon session 2 in session list
6/13/2023 11:38:26 AM    debug    fsso    CSessionManager::GetAllIPAddress is called
6/13/2023 11:38:26 AM    debug    fsso    CSessionManager::GetAllIPAddress:1293 IPv4
address:192.168.90.2
6/13/2023 11:38:26 AM    debug    fsso    EMS SN:FCTEMS8821090628
6/13/2023 11:38:26 AM    debug    fsso    Start to resolve address for
FortiAuthenticator:fac0824.local, TICC:5894281, TID:9072
6/13/2023 11:38:26 AM    debug    fsso    Succeeded to resolve address for
FortiAuthenticator:fac0824.local, FAC IP:172.19.200.110, TICC:5894281, TID:9072
6/13/2023 11:38:26 AM    debug    fsso    SendAndReceive(), Local IP:192.168.90.2, FAC
IP:172.19.200.110, FAC Port:8001, TICC:5894281, TID:9072
6/13/2023 11:38:26 AM    debug    fsso    SendAndReceive(), succeeded to send event to
authenticator, TID:9072
6/13/2023 11:38:26 AM    debug    fsso    FortiAuthenticator config:fac0824.local:8001
6/13/2023 11:38:26 AM    debug    fsso    Address Category:0
6/13/2023 11:38:26 AM    info    fsso    date=2023-06-13 time=11:38:25 logver=1 id=96980
type=securityevent subtype=fsso eventtype=status level=info uid=2ECE708...
devid=FCT8000... hostname=DESKTOP-JSOHIL9 pcdomain=myforest.local deviceip=192.168.90.2
devicemac=00-15-5d-23-03-0e site=default fctver=7.2.0.0690 fgtserial=N/A
emsserial=FCTEMS88... usingpolicy=Default os="Microsoft Windows 10 Professional Edition,
64-bit (build 19045)" user=administrator msg="Single Sign-On event" action=logon
domain="MYFOREST.LOCAL,Workstation Name:DESKTOP-
JSOHIL9,IP:192.168.90.2,FAC:172.19.200.110,succeeded to send session info, TICC:5894375,
TID:9072"
```

Use case B: pure/native or hybrid Entra ID

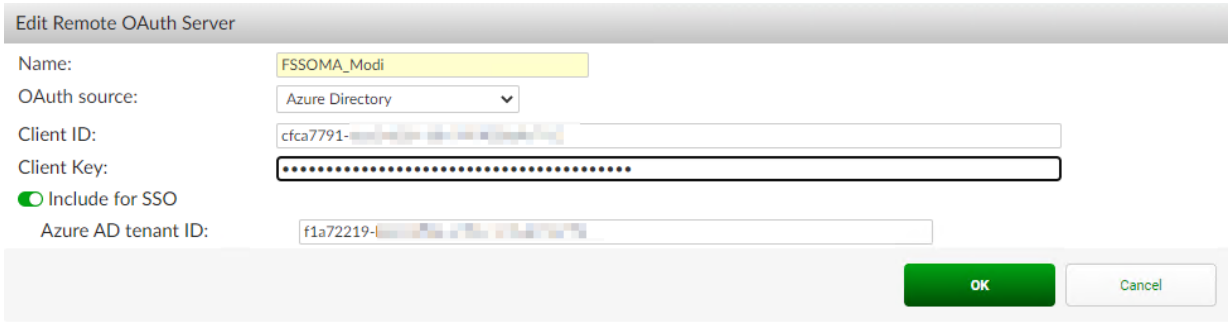
1. Configure Entra ID and add an enterprise application for FSSO:
   a. Sign in to the Entra ID portal as an administrator. Some configurations require a global administrator privilege.
   b. Create a user and ensure that users may join devices:
      i. Go to *Home > Manage Azure Active Directory > View button > Manage > Users > New User*. Configure a new user as desired.
      ii. Go to *Home > Manage Azure Active Directory > View button > Manage > Devices > Device Settings*. Enable *Users may join devices to Entra ID*.
   c. Create an enterprise application:
      i. Go to *Home > Manage Azure Active Directory > View button > Manage > Enterprise Applications > New Application > Create Your Own Application*.
      ii. Select *Integrate any other application you don't find in the gallery (Non-gallery)*. Configure other settings as desired.
   d. Set the newly created enterprise application as a directory reader:
      i. Go to *Home > Manage Azure Active Directory > View button > Manage > Roles and Administrators*.
      ii. In the *Administrative Roles* list, search for and select *Directory Readers*.
      iii. Add *Assignments* > Search for the name of the newly created enterprise application > *Add* button.
   e. Register the enterprise application with the Microsoft Identity Platform and generate an authentication key:
      i. Go to *Home > Manage Azure Active Directory > View button > Manage > App Registrations > All Applications*.
      ii. Search for and select the newly created enterprise application.
      iii. Click *Manage > Certificates & Secrets > New Client Secret*.
      iv. In the *Add a Client* dialog, set a description and expiry date, then click *Add*.
      v. Note down the string in the *Value* column. This value is only visible immediately after creation and will be hidden after you leave this page. You will use this value later.
2. In EMS, edit the desired endpoint profile's XML configuration to match the IP address, port, and PSK configured on the FortiAuthenticator, and to have FortiClient detect Azure user information and send it to FortiAuthenticator:

```
<fssoma>
        <enabled>1</enabled>
        <serveraddress>fac0824.local:8001</serveraddress>
        <presharedkey>Fortinet123!</presharedkey>
        <prefer_azure>1</prefer_azure>
</fssoma>
```

3. In FortiAuthenticator, configure OAuth:
   a. Go to *Authentication > Remote Auth. Servers > OAUTH > Create New*.
   b. From the *OAuth source* dropdown list, select *Azure Directory*.
   c. In the *Client ID* field, enter the application ID of the enterprise application that you created. You can find the client ID in Azure by going to *Home > Manage Azure Active Directory > View button > (in sidebar) Manage > Enterprise Applications > Search for Application Name*.
   d. In the *Client Key* field, enter the value from the Value column in step 1.e.v.

e. Enable *Include for SSO*.

f. In the *Azure AD tenant ID* field, enter the tenant ID. You can find this value in Azure by going to *Home > Manage Azure Active Directory > View button > Overview > Tenant ID*. Click *OK*.



4. Connect the endpoint with Entra ID. On the endpoint, go to *Settings > Accounts*. Beside *Add a work or school account*, click *Connect*.
5. Install FortiClient on the endpoint. Go to *Settings* and verify that FortiClient has received the SSOMA configuration from EMS.
6. In FortiAuthenticator, go to *Monitor > SSO > SSO Sessions*. Confirm that there is an entry for the endpoint.
7. In FortiClient, go to *Settings > Logging* and click *Export logs*. Confirm that SSOMA sends the FortiClient UUID and EMS serial number/tenant ID to FortiAuthenticator:

```
6/13/2023 11:29:30 AM    debug    fsso    GetAZureSessionUserInfo(), Calling of
RunExternalProgram is successful
6/13/2023 11:29:30 AM    debug    fsso    GetAZureSessionUserInfo(), username:jkim,
domain:fortinetvan.onmicrosoft.com, tenantID:f1a72219-...
6/13/2023 11:29:30 AM    debug    fsso    strAZUsername:jkim,
strAZDomain:fortinet.onmicrosoft.com, strAZTenantID:f1a72219-...
6/13/2023 11:29:30 AM    debug    fsso    session ID:2 has added to session table
6/13/2023 11:29:30 AM    debug    fsso    Succeede to add session 2
6/13/2023 11:29:30 AM    debug    fsso    Found current user, session ID: 2
6/13/2023 11:29:30 AM    debug    fsso    CSessionManager::AddSession has been called,
dwSession:65536
6/13/2023 11:29:30 AM    debug    fsso    Failed to call WTSQueryUserToken for session
ID:65536,error:2
6/13/2023 11:29:30 AM    debug    fsso    Failed to get token for session
ID:65536,error:2
6/13/2023 11:29:30 AM    debug    fsso    failed to add session 65536
6/13/2023 11:29:30 AM    debug    fsso    CSessionManager::AddSession has been called,
dwSession:65537
6/13/2023 11:29:30 AM    debug    fsso    Failed to call WTSQueryUserToken for session
ID:65537,error:2
6/13/2023 11:29:30 AM    debug    fsso    Failed to get token for session
ID:65537,error:2
6/13/2023 11:29:30 AM    debug    fsso    failed to add session 65537
6/13/2023 11:29:30 AM    debug    fsso    current active session 2
6/13/2023 11:29:30 AM    debug    fsso    Found current logon session 2 in session list
6/13/2023 11:29:30 AM    debug    fsso    CSessionManager::GetAllIPAddress is called
```

```
6/13/2023 11:29:30 AM    debug    fsso    CSessionManager::GetAllIPAddress:1325 IPv4
address:192.168.90.5
6/13/2023 11:29:30 AM    debug    fsso    EMS SN:FCTEMS882...
6/13/2023 11:29:30 AM    debug    fsso    Start to resolve address for
FortiAuthenticator:fac0824.local, TICC:-1981885328, TID:9452
6/13/2023 11:29:30 AM    debug    fsso    Succeeded to resolve address for
FortiAuthenticator:fac0824.local, FAC IP:172.19.200.110, TICC:-1981885328, TID:9452
6/13/2023 11:29:30 AM    debug    fsso    SendAndReceive(), Local IP:192.168.90.5, FAC
IP:172.19.200.110, FAC Port:8001, TICC:-1981885312, TID:9452
6/13/2023 11:29:30 AM    info    fsso    date=2023-06-13 time=11:29:29 logver=1 id=96980
type=securityevent subtype=fsso eventtype=status level=info uid=FDE6A554A2...
devid=FCT800... hostname=Arjuna pcdomain=N/A deviceip=192.168.90.5 devicemac=00-15-5d-23-
03-3f site=default fctver=7.2.1.0759 fgtserial=N/A emsserial=FCTEMS882...
usingpolicy=Default os="Microsoft Windows 11 Professional Edition, 64-bit (build 22621)"
user=jkim msg="Single Sign-On event" action=logon
domain="fortinet.onmicrosoft.com,Workstation
Name:Arjuna,IP:192.168.90.5,FAC:172.19.200.110,succeeded to send session info, TICC:-
1981885234, TID:9452"
6/13/2023 11:29:30 AM    debug    fsso    SendAndReceive(), succeeded to send event to
authenticator, TID:9452
6/13/2023 11:29:30 AM    debug    fsso    FortiAuthenticator config:fac0824.local:8001
6/13/2023 11:29:30 AM    debug    fsso    Address Category:0
```

Sending email events from the Microsoft Exchange server

You can configure FortiClient to send email events from Microsoft Exchange server. These events can contain metadata such as the email sender and recipient, date and time, subject, size, IP address, and so on. A SOAR or SIEM can use this metadata to correlate with security events.

To send email events from the Microsoft Exchange server to FortiAnalyzer:

1. Go to *Endpoint Profiles > System Settings*.
2. Edit the XML settings to enable `send_ms_exch_events` and define the interval:

```
<forticlient_configuration>
   <system>
      <log_setting>
         <remote_logging>
            <send_ms_exch_events>
               <enabled>1</enabled>
               <interval>120</interval>
            </send_ms_exch_events>
         </remote_logging>
      </log_setting>
   </system>
</forticlient_configuration>
```

3. Set the following registry to true:

Path	Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Fortinet\FortiClient\FA_DBLOG

Value name	`send_exch_events`
Value	`TRUE`

4. Configure the exchange server.
5. In FortiAnalyzer, verify that the Exchange server event was transmitted from FortiClient in *Log View* > *Fabric* using the filter *Host OS Family=MS Exchange*.

XML Configuration

Configuration	Description
XML editor	Configure the endpoint profile using the XML editor. See the *FortiClient XML Reference Guide*.

Creating a profile with XML

You can configure FortiClient profile settings in FortiEndpoint by using XML or a custom XML configuration file. The custom XML file must include all settings required by the endpoint at the time of deployment. For information about how to configure a profile with XML, see the *FortiClient XML Reference*.

To create a profile with XML:

1. Go to *Endpoint Profiles* > *Manage Profiles*, and click the *Add* button.
2. In the *Profile Name* field, enter a name for the profile.
3. Click the *Advanced* button. The *XML Configuration* tab displays, and the profile configuration displays in XML.
4. Click the *XML Configuration* tab, and click the *Edit* button.
5. Edit the XML.
6. Click *Test XML*.
7. Click *Save* to save the profile.

Importing a profile from an XML file

To import a profile from an XML file:

1. Go to *Endpoint Profiles* > *Manage Profiles*.
2. Click *Import From File*.
3. In the *Name* field, enter the desired name.
4. Under *XML*, browse to and select the desired XML profile configuration file.
5. Click *Upload*.

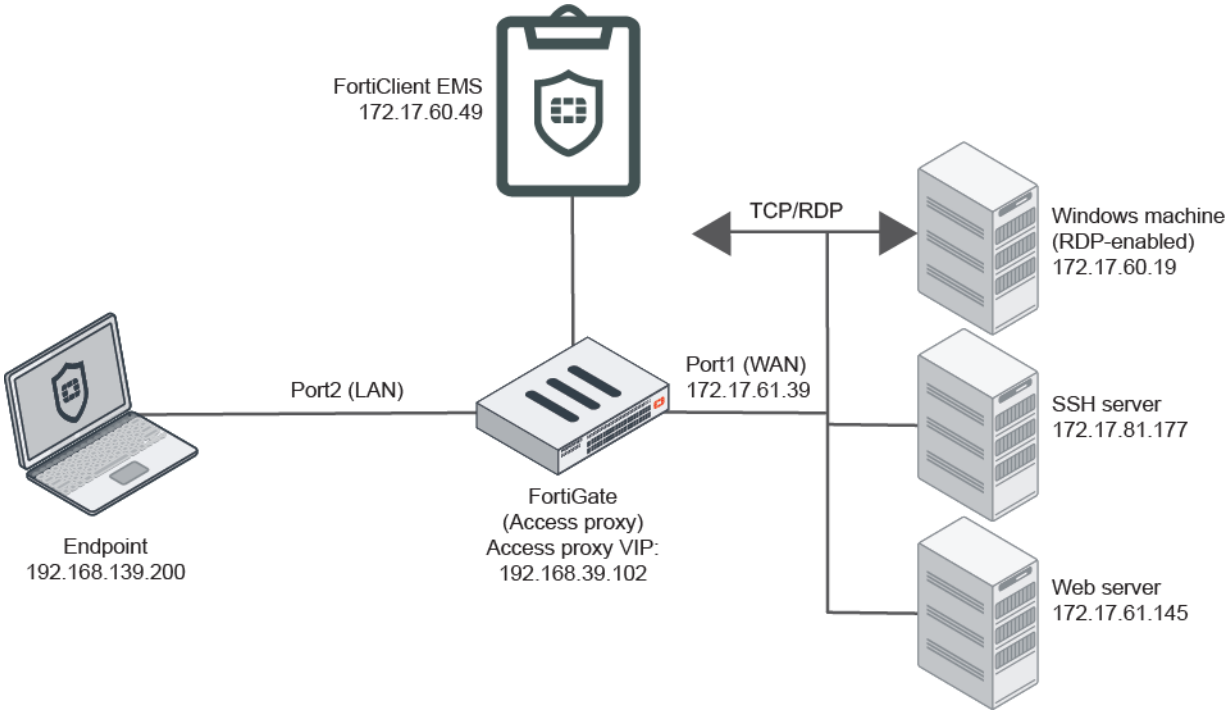
If the profile has a feature enabled that is disabled in Feature Select, EMS displays a warning that the feature is disabled on endpoints that the profile is deployed to. To enable this feature on the endpoint, you must enable the feature in Feature Select. See Feature Select on page 555.

Configuring encrypted ZTNA rules

FortiClient supports encryption and non-encryption modes for Zero Trust Network Access (ZTNA) via a toggle switch. You can manually add ZTNA rules in the FortiClient GUI or receive rules from EMS. This feature requires the prerequisites:

- A Security Fabric connector between FortiOS and EMS must be configured.
- FortiOS ZTNA-related settings must be configured properly. See ZTNA TCP forwarding access proxy example.
- FortiClient must be registered to EMS.
- You must add ZTNA rules in EMS or FortiClient.

The following shows the topology for the example configuration. In this topology, RDP access is configured to one server, and SSH access to another.



To configure ZTNA rules in EMS:

1. In EMS, go to *Endpoint Profiles* > *Manage Profiles*.
2. Edit the desired profile.
3. On the *XML Configuration* tab, add the following configuration:

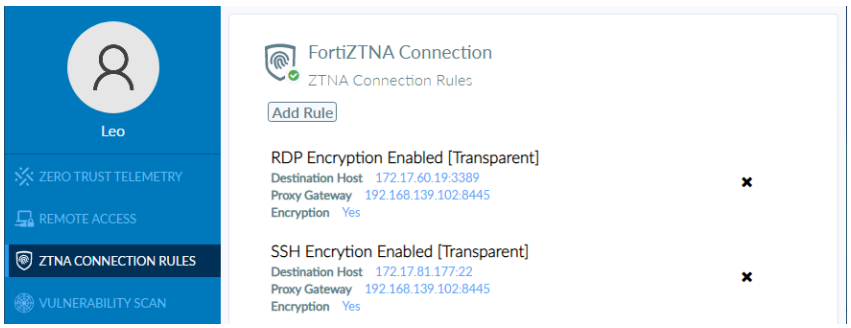
```
<ztna>
   <enabled>1</enabled>
   <rules>
      <rule>
         <name>RDP Forwarding</name>
         <destination>172.17.60.19:3389</destination>
         <gateway>192.168.139.102:8445</gateway>
         <encryption>1</encryption>
         <mode>transparent</mode>
```

```
        </rule>
        <rule>
           <name>SSH Forwarding</name>
           <destination>172.17.81.177:22</destination>
           <gateway>192.168.139.102:8445</gateway>
           <encryption>1</encryption>
           <mode>transparent</mode>
        </rule>
     </rules>
</ztna>
```

4. Save the configuration.

To configure ZTNA rules in FortiClient:

1. In FortiClient, go to the *ZTNA Connection Rules* tab.
2. Create the RDP forwarding rule:
   a. Click *Add Rule*.
   b. In the *Rule Name* field, enter RDP Encryption Enabled.
   c. In the *Destination Host* field, enter 172.17.60.19:3389.
   d. In the *Proxy Gateway* field, enter 192.168.139.102:8445.
   e. For *Mode*, select *Transparent*.
   f. Select the *Encryption* checkbox.
3. Create the SSH forwarding rule:
   a. Click *Create*.
   b. Click *Add Rule*.
   c. In the *Rule Name* field, enter SSH Encryption Enabled.
   d. In the *Destination Host* field, enter 172.17.81.177:22.
   e. In the *Proxy Gateway* field, enter 192.168.139.102:8445.
   f. For *Mode*, select *Transparent*.
   g. Select the *Encryption* Checkbox.
   h. Click *Create*.



To verify the configuration:

1. Start an SSH connection to 172.17.81.177 via ZTNA.
2. Run debug commands in FortiOS:

```
diagnose wad debug enable category all
diagnose wad debug enable level verbose
diagnose debug enable
```

3. Check the debug logs to verify whether encryption is enabled. When encryption is enabled, the debug logs contain the line `GET tcpaddress=172.17.81.177&port=22&tls=1 HTTP1.1`. When encryption is disabled, the debug logs contain the line `GET tcpaddress=172.17.81.177&port=22&tls=0 HTTP1.1`.

Security Posture Tags

Zero trust network access (ZTNA) is an access control method that uses client device identification, authentication, and security posture tags to provide role-based application access. It gives administrators the flexibility to manage network access for on-net local users and off-net remote users. Access to applications is granted only after verifying the device, authenticating the user's identity, authorizing the user, and then performing context-based posture checks using security posture tags.

Traditionally, a user and a device have different sets of rules for on-net access and off-net VPN access to company resources. With a distributed workforce and access that spans company networks, data centers, and cloud, managing the rules can become complex. This also affects user experience when multiple VPNs are needed to get to various resources. ZTNA can improve this experience.

You can create security posture tagging rules for endpoints based on their operating system versions, logged in domains, running processes, and other criteria. EMS uses the rules to dynamically tag endpoints. FortiOS can use the dynamic endpoint tags to build dynamic policy rules.

When using ZTNA, configuring dynamic DNS (DDNS) updates as *Secure only* is not supported.

See the Zero Trust Application Gateway Admin Guide for more information about ZTNA.

Tags

You can create, edit, and delete security posture tags for endpoints. You can also view and manage the rules used to dynamically tag endpoints.

The following occurs when using security posture tags with EMS and FortiClient:

1. EMS sends security posture tags and rules to endpoints via Telemetry communication.
2. FortiClient checks endpoints using the provided rules and sends the results to EMS. When endpoint network changes or user logon and logoff events occur, FortiClient triggers an X-FFCK-TAG message to EMS, even if there are no tag changes. Once EMS receives the tags, it processes them immediately, and FortiOS tags are updated within five seconds from the REST API response. For other tag changes, FortiClient sends the information to EMS regularly as per the configured keepalive intervals. See Configuring EMS settings on page 533.
3. EMS receives the results from FortiClient.
4. EMS dynamically groups endpoints together using the tag configured for each rule. You can view the dynamic endpoint groups in *Security Posture Tags > Tag Monitor*. See Tag Monitor on page 420.

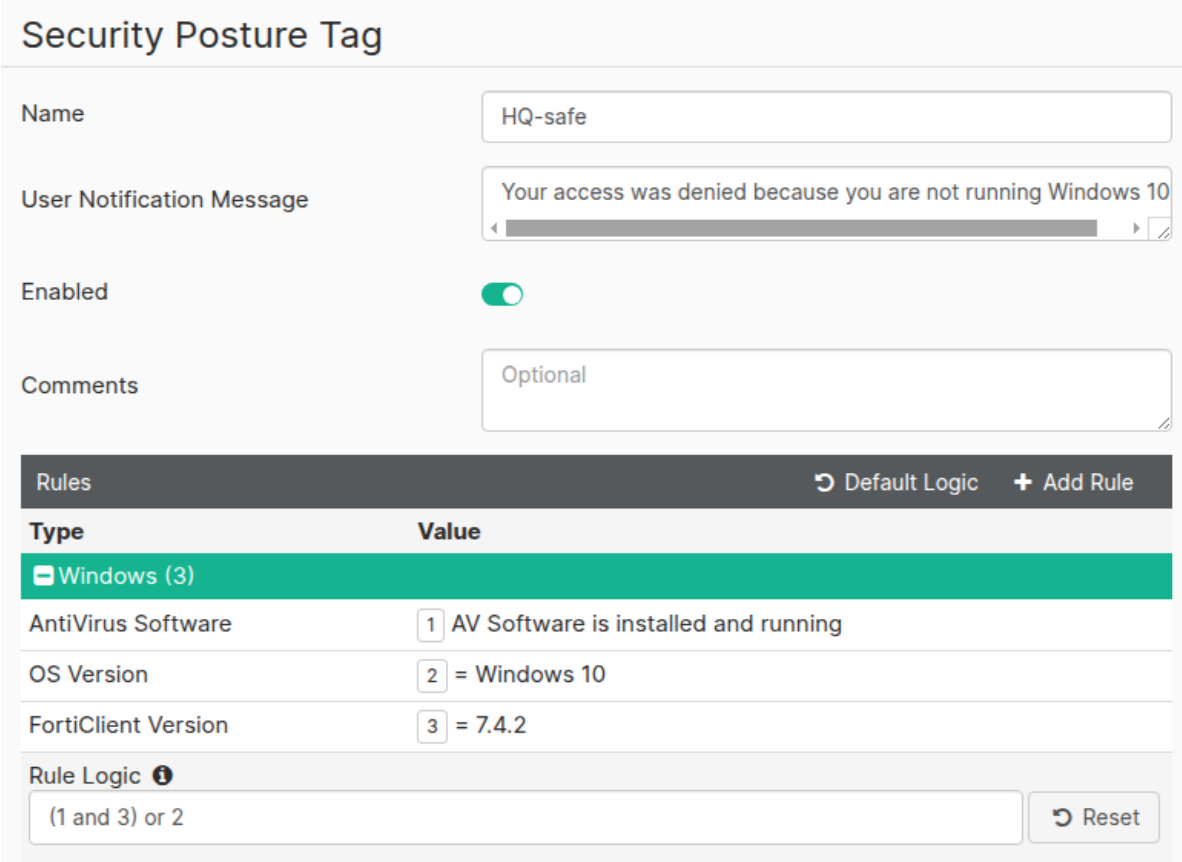
Adding a security posture tag

To add a security posture tag:

1. Go to *Security Posture Tags > Tags*, and click *Create*.
2. In the *Name* field, enter the desired tag name.

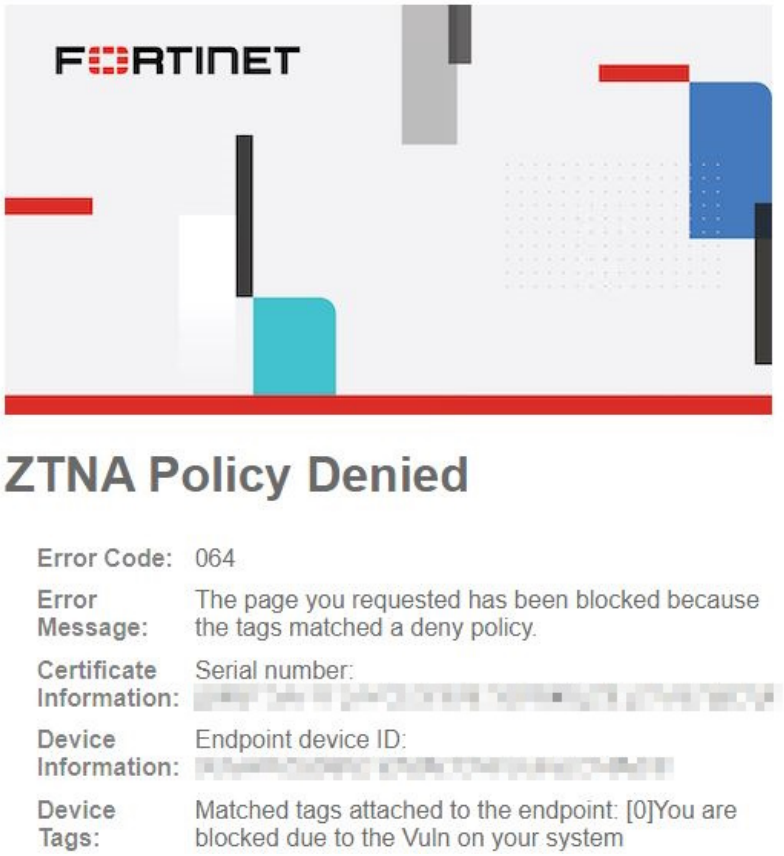
3. In the *User Notification Message* field, enter a message that explains to the end user why FortiOS denied their access. In FortiOS in *Policy & Objects > ZTNA > Security Posture Tags*, the *Comments* column displays the configured user notification message for a tag.
4. Toggle *Enabled* on or off to enable or disable the rule.
5. (Optional) In the *Comments* field, enter any desired comments.
6. Click *Add Rule*.
7. Configure the rules:
   a. For *OS*, select the desired OS. This affects what rule types are available.
   b. From the *Rule Type* dropdown list, select the rule type and configure the related options. Ensure that you click the + button after entering each criterion. See Security posture tagging rule types on page 413 for descriptions of the rule types.
   c. Click *Save*.
   d. Configure additional rules as desired.
8. By default, an endpoint must satisfy all configured rules to be eligible for the tag. You may want to apply the tag to endpoints that satisfy some, but not all, of the configured rules. In this case, you can modify the rule set logic. For example, consider that you want to apply the same tag to endpoints that fulfill one of the following criteria:
   - Running Windows 10
   - Running FortiClient 7.4.2 and antivirus (AV) software is installed and running

   With the default logic, an endpoint would be eligible for the rule set if it is running Windows 10 and FortiClient 7.4.2 and has AV software installed and running. To modify the rule set logic, do the following:
   a. Click *Edit Logic*.
   b. Clicking *Edit Logic* assigns numerical values to each configured rule. In the *Rule Logic* field, enter the desired logic for the rule set using the numerical values. You can use `and` and `or` to define the rule logic. You cannot use `not` when defining the rule logic. You can also use parentheses to group rules. For this example, you would enter `(1 and 3) or 2`, to indicate that endpoints that satisfy both the AV and FortiClient 7.4.2 rules (rules 1 and 3) or only the Windows 10 rule (rule 2) satisfy the rule set. To restore the default logic, you can click *Default Logic*.



9. Click *Save*.

The following shows a *ZTNA Policy Denied* page. It shows the user notification message in the *Device Tags* field.



Editing a security posture tag

To edit a security posture tagging rule:

1. Go to *Security Posture Tags* > *Tags*.
2. Select the security posture tag.
3. Click *Edit*.
4. Edit as desired.
5. Click *Save*.

Deleting a security posture tag

To delete a security posture tag:

1. Go to *Security Posture Tags* > *Tags*.
2. Click the desired security posture tag.
3. Click *Delete*.
4. In the confirmation dialog, click *Yes*.

Importing and exporting a security posture tag

You can import and export security posture tag set as a JSON file.

You can import tagging rule sets from an older EMS version to EMS 726.1.b. If multiple tagging rule sets apply the same tag to an endpoint, after import, EMS combines the entries into one in *Tags*.

To import a tag set:

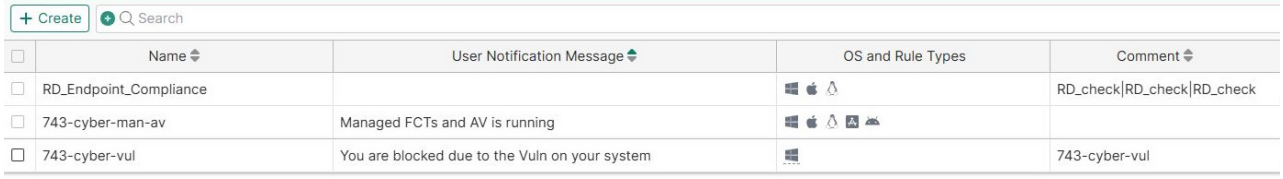
1. If importing a tag set from an older EMS version, in the older EMS version, go to *Security Posture Tags* > *Security Posture Tagging Rules*.
2. Click *Export*.



3. In EMS 26.1.b, go to *Security Posture Tags* > *Tags*.
4. Click *More* > *Import tag configuration*.
5. In the *File* field, upload the desired JSON file.
6. For *On tag name conflict*, select one of the following actions to take if the imported tag has the same name as an existing security posture tag in EMS:

Option	Description
Rename	Rename the imported tag. This option adds a -1 to the imported tag. For example, if the existing and imported tags share the name *AV-Not-Installed*, this option renames the imported tag to *AV-Not-Installed-1*. If *AV-Not-Installed-1* already exists as well, EMS renames the imported tag *AV-Not-Installed-2*, and so on.
Overwrite	Overwrite the existing tag with the imported tag. The overwritten tag only contains the rules for the imported tag. Rules for the existing tag are not retained.
Do not import	Stop importing the new tag.

7. Click *OK*. In the example, after import, the rule sets that all applied RD_Endpoint_Compliance are combined into a single entry for the RD_Endpoint_Compliance tag, with the multiple OSes displayed under the *OS and Rule Types* column.



To export a security posture tagging rule set:

1. Go to *Security Posture Tags* > *Tags*.
2. Click *More* > *Export tag configuration*.

Security posture tagging rule types

The following table describes security posture tagging rule types and the operating systems (OS) that they are available for. For all rule types, you can configure multiple conditions using *+*.

Rule type	OS	Description
AntiVirus Software	• Windows • macOS • Linux	From the *AV Software* dropdown list, select the desired conditions. You can require that an endpoint have antivirus (AV) software installed and running and that the AV signature is up-to-date. You can also use the NOT option for the rule to require that the endpoint does not have AV software installed or running or that the AV signature is not up-to-date. This rule applies for FortiClient AV and third-party AV software that registers to the Windows Security Center. The third-party software notifies the Windows Security Center of the status of its signatures. FortiClient queries the Windows Security Center to determine what third party AV software is installed and if the software reports signatures as up-to-date. • For Windows, this feature supports third party AV applications. • For Windows Server, macOS, and Linux, this feature can only check if FortiClient AV protection is enabled and does not recognize third party AV applications. The following options are available. The following options are limited to FortiClient AV and cannot be used for third-party AV applications: • *Enable latest update check*: FortiClient checks if FortiClient AV software or signatures were recently updated. • *Latest update within*: Configure the amount of time after the last FortiClient AV software or signatures update was received that FortiClient considers the AV protection outdated. For example, if you configure this option to be 60 days, FortiClient considers the AV protection outdated 61 days after the most recent update. The endpoint must satisfy all configured conditions to satisfy this rule.
Certificate	• Windows • macOS • Linux	In the *Subject CN* and *Issuer CN* fields, enter the certificate subject and issuer. You can also use the NOT option to indicate that the rule requires that a certain certificate is not present for the endpoint. For Windows and macOS, FortiClient checks certificates in the current user personal store and local computer personal store. It does not check in trusted root or other stores. For Linux, FortiClient checks root CA certificates installed on the system. For Ubuntu, FortiClient checks `/etc/ssl/certs/ca-certificates.crt`. For CentOS and Red Hat, FortiClient checks `/etc/pki/tls/certs/ca-bundle.crt`. For Linux, FortiClient does not check user certificates. The *Subject CN* field supports wildcards, regular expressions, and case-insensitivity. You can also leave the *Subject CN* field blank.

Rule type	OS	Description
		The *Issuer CN* field does not support wildcards or regular expressions. The endpoint must satisfy all conditions to satisfy this rule. For example, if the rule is configured to require certificate A, certificate B, and NOT certificate C, then the endpoint must have both certificates A and B and not certificate C.
Common Vulnerabilities and Exposures	• Windows • macOS • Linux	In the *CVEs* field, enter the common vulnerabilities and exposures (CVE) ID in the format CVE-xxxx-xxxxx. For example, you could enter CVE-2020-26950. You can also use the *NOT* option to indicate that the rule requires that a CVE is not present on the endpoint. EMS considers the endpoint as satisfying the rule if it satisfies one of the conditions.
CrowdStrike ZTA Score	Windows	In the *CrowdStrike ZTA Score* field, enter a zero trust assessment (ZTA) score value between 1 and 100. You can use comparators to configure the rule to apply to endpoints with a range of ZTA scores. You can also use the *NOT* option to indicate that the rule requires that the endpoint does not have a ZTA score within a certain range. EMS considers the endpoint as satisfying the rule if it satisfies one of the conditions.
EMS Management	• Windows • macOS • Linux • iOS • Android	EMS considers the endpoint as satisfying the rule if the endpoint has FortiClient installed and Telemetry connected to EMS.
File	• Windows • macOS • Linux	In the *File* field, enter the file path. You can also use the NOT option to indicate that the rule requires that a certain file is not present on the endpoint. Optionally, in the *SHA256 Hash* field, enter the file hash. This can ensure the integrity of the file being checked, enhancing security. FortiClient 7.4.4 and later versions support this feature. The endpoint must satisfy all configured conditions to satisfy this rule. For example, if the rule is configured to require file A, file B, and NOT file C, then the endpoint must have both files A and B and not file C. Also, if configured, the file hash must also match.
Firewall Threat	• Windows • macOS	In the *Firewall Threat ID* field, enter the firewall threat ID. You can find this ID in FortiGuard or on the *Firewall Events* tab of the endpoint details page. You can also use the NOT option to indicate that the rule requires that a firewall threat is not present on the endpoint. EMS considers the endpoint as satisfying the rule if it satisfies one of the conditions.

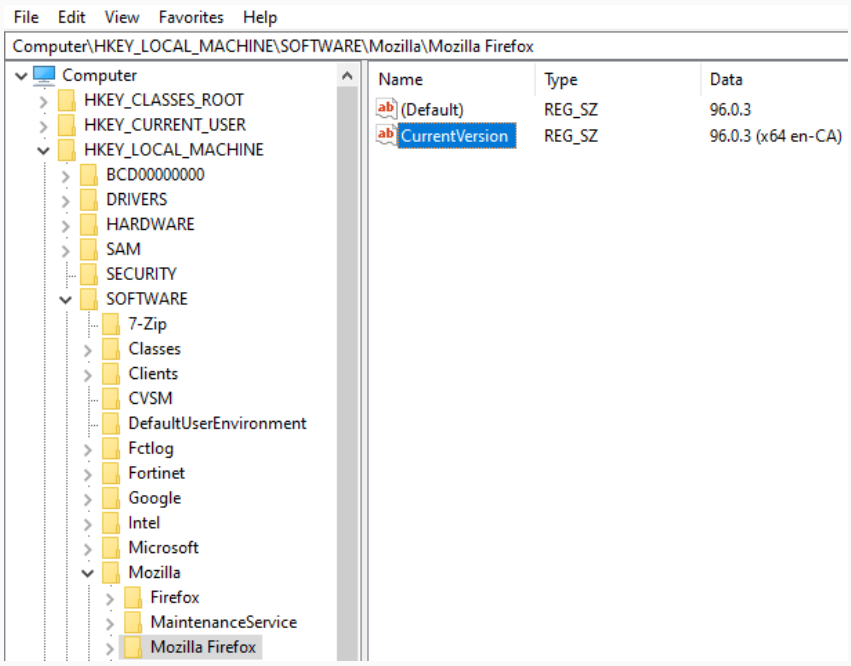
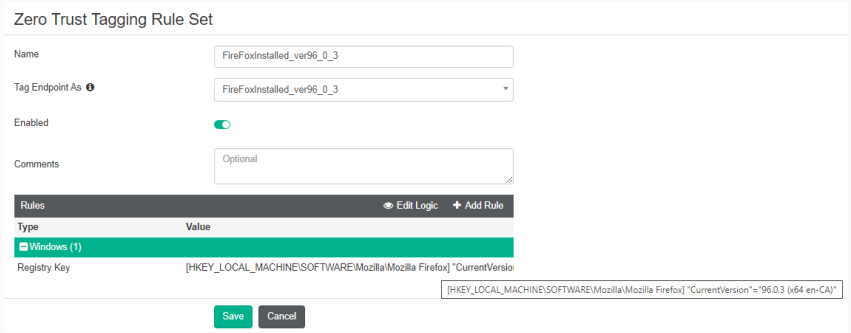
Rule type	OS	Description
FortiClient Version	• Windows • macOS • Linux • iOS • Android	In the *FortiClient Version* field, enter the desired FortiClient version. You can use comparators to configure the rule to apply to endpoints with a range of FortiClient versions. You can also use the NOT option for the rule to require that the endpoint not have a certain version of FortiClient installed.
FortiEDR	• Windows • macOS • Linux	From the *FortiEDR* dropdown list, select *FortiEDR is installed and running*. EMS considers the endpoint as satisfying the rule if the endpoint has FortiEDR installed and running.
IP Range	• Windows • macOS • Linux • iOS • Android	In the *IP Range* field, enter the IP address range. If the rule is configured for multiple ranges, EMS considers the endpoint as satisfying the rule if it belongs to one of the configured ranges.
Logged in Domain	• Windows • macOS • Linux	In the *Domain* field, enter the domain name. You can specify multiple domains. This rule checks for logged-in domain user or machine. FortiEndpoint EMS considers the endpoint as satisfying the rule if the device is in one of the configured domains or if the logged-in user belongs to one of the configured domains.
On-Fabric Status	• Windows • macOS • Linux • iOS • Android	By default, the rule requires that the endpoint is on-Fabric. You can also use the NOT option to indicate that the rule requires that the endpoint is off-Fabric.
OS Version	• Windows • macOS • Linux • iOS • Android	From the *OS Version* dropdown list, select the OS version. You can use comparators to configure the rule to apply to endpoints with a range of OS versions. Only FortiClient 7.2.2 and later versions support comparators. FortiClient 7.2.1 and earlier versions do not support comparators and will apply rules with comparators as if they are using =. If the rule set is configured for multiple OS versions, EMS considers the endpoint as satisfying the rule if it has one of the configured OS versions installed. The following options are available for Windows: • *Enable latest update check*: FortiClient checks if Windows OS updates were recently installed. • *Latest update within*: Configure the amount of time after the last system update was received that FortiClient considers the OS outdated. For example, if you configure this option to be 60 days, FortiClient considers the OS outdated 61 days after the most recent system update.

<table>
<tr><th>Rule type</th><th>OS</th><th>Description</th></tr>
<tr><td>Registry Key</td><td>• Windows</td><td>Configure a registry key rule using the registry path or name, key name, and key value data.

<table><tr><th>Option</th><th>Description</th></tr><tr><td>NOT</td><td>Enable to indicate that the rule requires that a certain registry path or value name is not as configured in the rule.</td></tr><tr><td>Key</td><td>Enter the registry path or name enclosed in square brackets [ ]. End the path with \ to indicate a registry path, or without \ to indicate a registry name.</td></tr><tr><td>Key Name</td><td>Enter the registry key name, enclosed in double quotation marks "".</td></tr><tr><td>comparator</td><td>Select the desired comparator from the dropdown list.</td></tr><tr><td>Value</td><td>Enter the desired key value data. Only the REG_DWORD (32-bit binary number) and REG_SZ (standard null-terminated string) types are supported:
• For a DWORD key value, enter the value data as <code>dword:<value></code>. For example, if the DWORD key value data is 1, enter <code>dword:1</code>.
• For a SZ key value, enter the value data enclosed in double quotation marks "".</td></tr></table>
The endpoint must satisfy all configured conditions to satisfy this rule. For example, if the rule is configured to require certain values for registry key A, registry key B, and NOT the configured value for registry key C, then the endpoint must have both the required values registry keys A and B and not the configured value for registry key C.

Example:

The following shows a system where Firefox is installed. The registry path is <code>HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox</code>. The key name is <code>CurrentVersion</code>, and the key value data is <code>96.0.3 (x64 en-CA)</code>.</td></tr>
</table>

Rule type	OS	Description
		 You can configure a registry key rule to match `HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox` as the path, `CurrentVersion` as the key name, and `96.0.3 (x64 en-CA)` as the key value, as shown below. Note that the registry path is enclosed in square brackets and the key name and value are enclosed in double quotation marks. 
Running Process	• Windows • macOS • Linux	In the *Running Process* field, enter the process name. You can also use the NOT option to indicate that the rule requires that a certain process is not running on the endpoint. The endpoint must satisfy all configured conditions to satisfy this rule. For example, if the rule is configured to require process A, process B, and NOT process C, then the endpoint must have both processes A and B running and process C not running.

Rule type	OS	Description
Sandbox Detection	• Windows • macOS	From the *Sandbox Detection* dropdown list, select the desired condition. You can require that Sandbox detected malware on the endpoint in the last seven days. You can also use the NOT option for the rule to require that Sandbox did not detect malware on the endpoint in the last seven days.
Security	• macOS	Select the checkbox to require that File Vault is enabled on the endpoint. You can also use the NOT option to indicate that the rule requires that File Vault is disabled on the endpoint.
Security Status	• iOS • Android	Select one of the following: • **Jail-broken**: device where software restrictions that the manufacturer or operating system provider imposes on devices have been removed. • **Passcode-Enabled**: device with screen lock enabled. • **Biometrics Protected**: device with touch or face ID enabled. You can also use the NOT option for the rule to require that the endpoint not have a certain security status.

User Identity	• Windows
	• macOS
	• Linux
	• iOS
	• Android
		Under *User Identity*, select the following:
		• *User Specified*: endpoint user manually entered their personal information in FortiClient.
		• *Social Network Login*: endpoint user provided their personal information by logging in to their Google, LinkedIn, or Salesforce account in FortiClient. You can further select one of the following:
		  • *All Accounts*: all endpoints where the user logged in to the specified social network account type.
		  • *Specified*: enter a specific Google, LinkedIn, or Salesforce account. For example, you can enter joanexample@gmail.com to configure the rule to apply specifically to only that Google account. You can specify multiple social network accounts.
		• *Verified User*: endpoint user must be a verified user that has authenticated their connection to EMS as a member of an authorized user group. See User Management on page 498.
		EMS considers the endpoint as satisfying the rule if it satisfies one of the conditions.
		You can also use the NOT option for the rule to require that the endpoint user has not manually entered user details or logged in to a social network account to allow FortiClient to obtain user details.
		FortiClient iOS does not support social network login with LinkedIn or Salesforce. FortiClient Android does not support social network login with Salesforce.

Rule type	OS	Description
User in AD Group	• Windows • macOS • Linux	From the *AD Group* dropdown list, select the desired Active Directory (AD) group. EMS considers the endpoint as satisfying the rule if the logged in user belongs to the selected AD group. The rule considers the logged-in user's group membership, not the computer's attributes. The *Evaluate on FortiClient* option is a legacy option that was originally implemented when AD group tagging was first introduced: **Disable** (default) — EMS performs AD group lookup. This is recommended as EMS evaluation is more efficient and prevents the issue where an endpoint loses all AD-related tags when it goes offline. **Enable** — FortiClient performs AD group lookup with the following limitations: • FortiClient evaluation is not real-time, leading to inconsistent or delayed posture tag updates . • No support for Entra ID integration. In cases where the user/endpoint is a member only of a subgroup or of top and sublevel groups, EMS can apply tags for both levels. Use the NOT option to indicate that the rule requires that the logged in user does not belong to certain AD groups. You cannot use the NOT option to indicate that the rule requires that the logged in user does not belong to any AD group. EMS does not support a rule to dynamically group all endpoints that do not belong to a domain. To use this option, you must configure your domain under *Endpoints*. See Adding endpoints using an AD domain server on page 54. When using a *User in AD Group* rule, disabling the Windows switch users option is recommended to ensure EMS applies the AD tag correctly.
Vulnerable Devices	• Windows • macOS • Linux	From the *Severity Level* dropdown list, select the desired range of vulnerability severity levels. If the rule set is configured for multiple severity levels, EMS considers the endpoint as satisfying the rule if it has a vulnerability of one of the configured severity levels or higher. You can also use the NOT option to indicate that the rule requires that the endpoint does not have vulnerabilities of a certain severity level present.
Windows Security	• Windows	From the *Windows Security* dropdown list, select the desired conditions. You can require that an endpoint have one or more of the following applications or configurations enabled: • **Windows Defender**: antimalware component of Windows. Scans files to detect and remediate threats. • **Bitlocker Disk Encryption**: data protection feature that integrates with the operating system (OS) and addresses the threats of data theft or exposure from lost, stolen, or

Rule type	OS	Description
		inappropriately decommissioned computers. BitLocker enhances file and system protections and helps render data inaccessible when computers are decommissioned or recycled. See BitLocker overview. • **Exploit Guard**: automatically applies exploit mitigation techniques to OS processes and applications. When Exploit Guard finds a mitigation, Windows displays a notification from the Action Center. See Protect devices from exploits. • **Application Guard**: helps to prevent old and newly emerging attacks by isolating enterprise-defined untrusted sites. For example, Application Guard helps prevent untrusted Microsoft Word, PowerPoint, and Excel files from accessing trusted resources by opening untrusted files in an isolated Microsoft Hyper-V-enabled container. See Microsoft Defender Application Guard overview. • **Windows Firewall**: firewall component of Windows. Helps prevent hackers and malicious software from gaining access to the device through the Internet or a network. • **Automatic Updates**: downloads and installs security and other important updates to your computer automatically. You can also use the NOT option for the rule to require that the endpoint have one or more of the listed applications disabled. The endpoint must satisfy all configured conditions to satisfy this rule.

Tag Monitor

You can view all dynamic endpoint tag information in *Security Posture Tags* > *Tag Monitor*. EMS applies endpoint tags dynamically based on the rules configured for each tag. This page shows endpoints tagged using the following tag types:

Tag	Description
Security posture tags	See Security Posture Tags on page 408.
FortiGuard outbreak alert tags	See FortiGuard Outbreak Alerts on page 448.
Classification tags	See Viewing the Endpoints pane on page 57.
Fabric tags	Fabric tags require connection to FortiAnalyzer. See the following process: 1. EMS administrator configures FortiAnalyzer in a System Settings profile. See System Settings on page 378. 2. FortiClient connects to EMS and receives FortiAnalyzer connection information from the profile. 3. FortiClient sends logs to FortiAnalyzer. 4. FortiAnalyzer administrator configures rule to tag endpoints which

Tag	Description
	have indicators of compromise (IOC). 5. If a log entry received from FortiClient on the FortiAnalyzer matches an IOC, FortiAnalyzer adds a tag to that endpoint. 6. EMS adds this tag to the endpoint. You can view the tag in the endpoint details, as well as in *Security Posture Tag Monitor*. This tag displays as a Fortinet Security Fabric tag in *Security Posture Tag Monitor*, but the tag displays under *Classification Tags* in endpoint details. See Viewing the Endpoints pane on page 57. 7. If FortiGate is configured to receive all tags for this specific endpoint, EMS sends the tag to FortiGate. See EMS API support for FortiAnalyzer to notify and tag suspicious endpoints.

The panes at the top show how many tags belong to each tag type. You can click each pane to display only tags that belong to that tag type.

Refresh	Click to refresh the list of tagged endpoints in the content pane.
Endpoint	Endpoint's hostname.
User	Name of the user logged into the endpoint.
OS	OS currently installed on the endpoint.
IP	Endpoint's IP address.
Category	Type of tag that the endpoint was tagged with. This can be one of the following: • Zero Trust • FortiGuard outbreak alert • Classification • Fabric
Tagged on	Date and time that EMS added the endpoint to the dynamic endpoint group.

FortiOS dynamic policies using EMS dynamic tags

After defining security posture tagging rules in EMS, you can configure FortiOS to receive the dynamic endpoint groups from EMS using the FortiEndpoint Fabric connector which supports SSL and imports trusted certificates. When a change to the dynamic endpoint groups occurs, such as an endpoint being added to or removed from a group, EMS sends the update to FortiOS, and FortiOS updates its dynamic policies accordingly, providing dynamic access control based on endpoint status.



FortiOS only receives endpoint information and enforces compliance for directly connected endpoints. Directly connected endpoints are the ones that have FortiGate as the default gateway. See Fabric Devices on page 427 for information on configuring Fabric device tag sharing settings.

This feature works for endpoints that are connected to a VPN tunnel as long as they can access EMS and the FortiOS version is compatible with EMS. See the *FortiEndpoint Compatibility Chart*.

Configuring FortiOS dynamic policies using EMS security posture tags

FortiOS uses an EMS connector to retrieve security posture tags from EMS. Configuring this feature requires the following steps:

1. Checking prerequisites on page 422
2. Configuring the EMS connector on page 422:
   a. Uploading certificates to EMS and FortiOS on page 422
   b. Creating the EMS connector in FortiOS on page 423
   c. Authorizing the FortiOS EMS connector in EMS on page 424
   d. Verifying the FortiOS-EMS connection in FortiOS on page 424
3. Creating an address group for the security posture tags on page 425
4. Creating a dynamic firewall policy using security posture tags from EMS on page 425

If you configure a connection between EMS and a FortiGate that is part of a Security Fabric with multiple FortiGates, the root FortiGate can also obtain security posture tags from EMS. However, the root FortiGate does not have any IP addresses to associate with the received tags.

Checking prerequisites

You must ensure that the following prerequisites are met before configuring this feature:

- Create security posture tagging rules. See Adding a security posture tag on page 408.
- After FortiClient connects Telemetry to EMS, confirm that EMS dynamically tags endpoints based on the security posture tagging rules. See Tag Monitor on page 420.
- Export a certificate authority (CA)-signed certificate to upload to FortiOS and web server certificate to upload to EMS. For details on configuring a server certificate using the Microsoft Certification Authority Management Console, see Configure the Server Certificate Template. You can use another CA as desired.

Configuring the EMS connector

Uploading certificates to EMS and FortiOS

To upload certificates to EMS and FortiOS:

Setting up a secure connection between EMS and FortiOS requires a certificate. Uploading the CA-signed certificate to FortiOS allows FortiOS to trust the certificate that you configure in EMS.

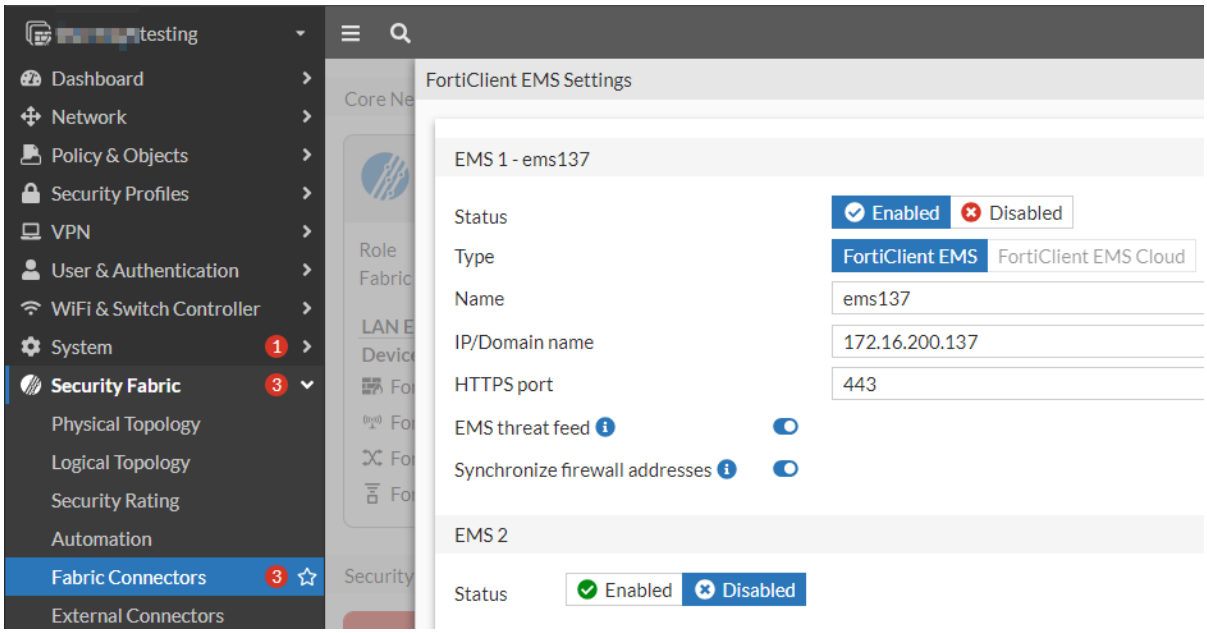
1. Configure the server certificate in EMS:
   a. Go to *System Settings* > *EMS Server Certificates*.
   b. Click *Add*.
   c. Configure the certificate as desired.
   d. Go to *System Settings* > *EMS Settings*.
   e. Under *Shared Settings*, from the *Webserver certificate* dropdown list, select the configured certificate.
   f. Click *Save*.
2. Upload the certificate to FortiOS:
   a. Go to *System* > *Certificates*.
   b. From the *Create/Import* dropdown list, select *CA Certificate*.
   c. Upload the CA-signed certificate.

Creating the EMS connector in FortiOS

You can create the EMS connector in the FortiOS GUI or CLI.

To create the EMS connector in the FortiOS GUI:

1. Go to *Security Fabric* > *Fabric Connectors*.
2. Right-click *FortiClient EMS*, then select *Edit*.
3. For *Status*, select *Enabled*.
4. For *Type*, select *FortiEndpoint*.
5. In the *Name* field, enter the desired name.
6. In the *IP/Domain name* field, enter the EMS IP address or domain name.
7. Ensure to enable *Synchronize firewall addresses*. This allows FortiOS to automatically create and synchronize firewall addresses for security posture tags received from EMS.



8. Click *OK*.

To create the EMS connector in the FortiOS CLI:

```
config endpoint-control fctems
   edit 1
      set fortinetone-cloud-authentication disable
      set server "172.16.200.137"
      set https-port 443
      set source-ip 0.0.0.0
      set pull-sysinfo enable
      set pull-vulnerabilities enable
      set pull-avatars enable
      set pull-tags enable
      set call-timeout 180
   next
end
```

Authorizing the FortiOS EMS connector in EMS

To authorize the FortiOS EMS connector in EMS:

EMS must authorize the Fabric connector created in FortiOS. Do one of the following:

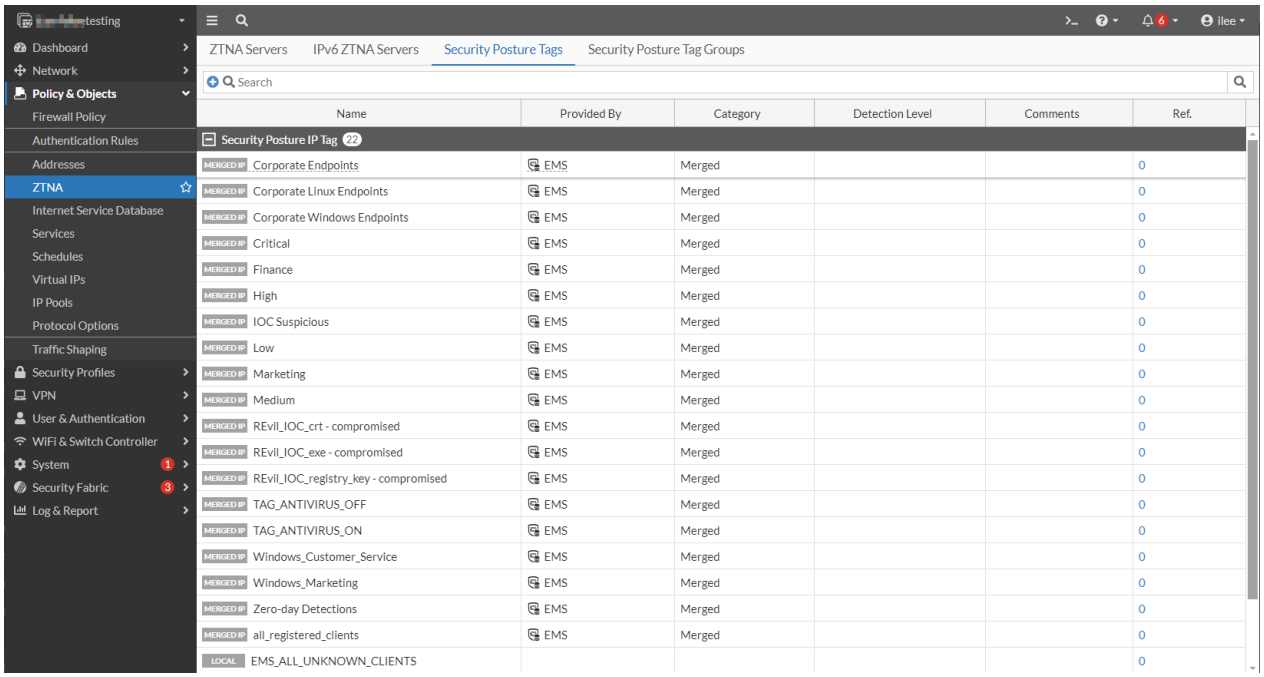
- Log in to EMS. A prompt displays to authorize the FortiGate. Click *Authorize*.
- Go to *Fabric & Connectors* > *Fabric Devices*. Select the desired FortiGate, then click *Authorize*.

You can view all FortiGates that the EMS authorized in *Fabric & Connectors* > *Fabric Devices*. See Fabric Devices on page 427.

Verifying the FortiOS-EMS connection in FortiOS

To verify the FortiOS-EMS connection in FortiOS:

1. Authorize the connection by doing one of the following:
   a. In *Security Fabric* > *Fabric Connectors*, click the desired EMS connector. Click *Authorize*.
   b. After EMS authorizes the FortiGate, authorize the connection in the FortiOS CLI by running the `execute fctems verify <EMS ID>` command.
2. FortiOS should now automatically pull security posture tags from EMS. Go to *Policy & Objects* > *ZTNA* > *Security Posture Tags* to view the tags.



Creating an address group for the security posture tags

To create an address group for the ZTNA tags in the FortiOS CLI:

```
config firewall addrgrp
   edit SPgroup
      set category ztna-ems-tag
   next
end
```

Creating a dynamic firewall policy using security posture tags from EMS

To create a dynamic firewall policy using ZTNA tags from EMS:

1. In FortiOS, go to *Policy & Objects* > *Firewall Policy*. Click *Create new*.
2. In the *Security posture tag* field, click +. The *Select Entries* pane appears. Under *Security Posture Tag*, select the desired tag from EMS.
3. Configure other options as desired. Click *OK*.
4. Go to *Policy & Objects* > *Firewall Policy* to ensure the policy was created. FortiOS updates this policy when it receives updates from EMS.

Fabric Device Monitor

On the *Fabric Device Monitor* page, you can view all FortiGates that are connected to EMS. For information on connecting a FortiGate to EMS, see FortiOS dynamic policies using EMS dynamic tags on page 421.

For each connected FortiGate, you can view the following information:

- Serial number
- IP address
- FortiOS version installed
- Last sync time between FortiEndpoint and the FortiGate
- Dynamic endpoint groups shared with the FortiGate and the number of endpoints in each group

Fabric & Connectors

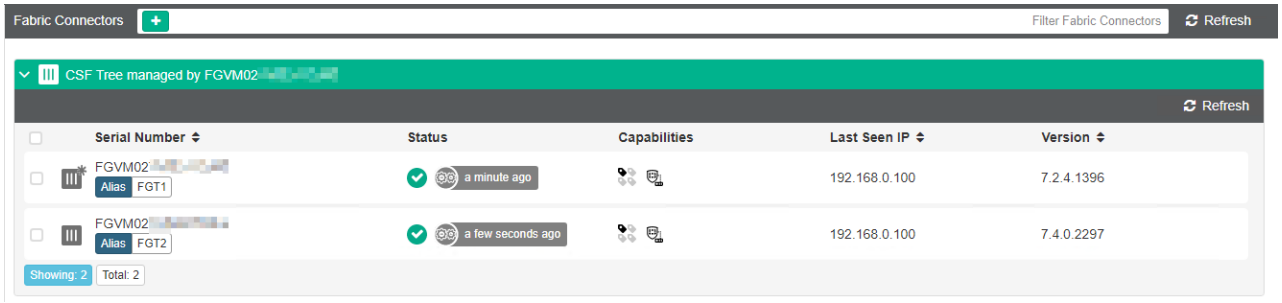
In *Fabric & Connectors*, you can access the following pages:

- Fabric Devices on page 427—View all FortiGates that the EMS has authorized.
- Troubleshooting on page 441—Troubleshoot ZTNA and VPN integration issues between FortiGate and EMS using time-correlated VPN (both SSL and IPsec) and ZTNA-related logs.
- ZTNA Applications Catalog on page 446—Add a zero trust network access (ZTNA) application or view a ZTNA application that EMS retrieved from FortiOS 7.4.4 and later versions.

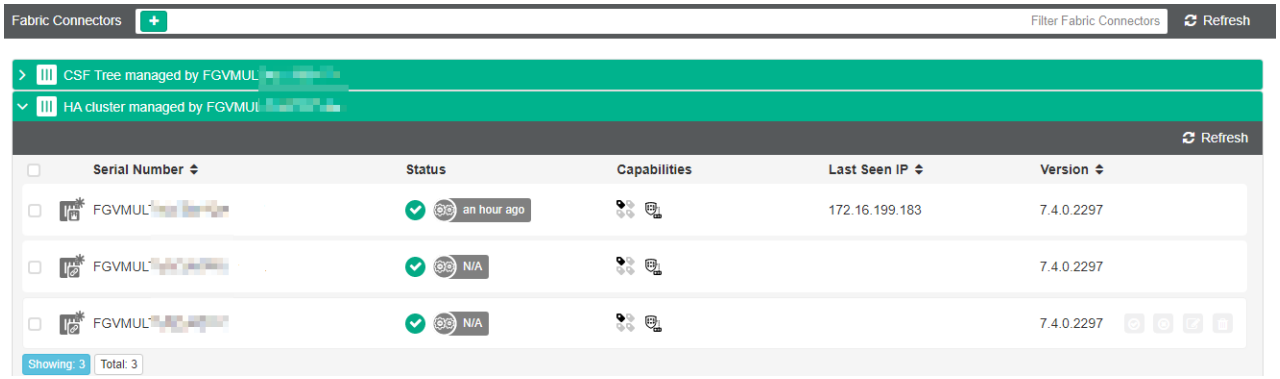
Fabric Devices

You can view all FortiGates that the EMS has authorized in *Fabric & Connectors > Fabric Devices*. You can also deny or authorize a FortiGate. These FortiGates receive endpoint data from EMS. FortiClient does not directly connect to FortiGates listed on this page.

The *Fabric Devices* page displays the relationships between FortiGates if they are part of a cooperative Security Fabric (CSF) or high availability (HA) cluster. The following shows *Fabric Devices* showing two FortiGates that are part of a CSF tree:



The following shows *Fabric Devices* showing two FortiGates that are part of an HA cluster:



FortiOS versions 7.0.2 to 7.0.6 only support security posture tags and does not support other tag types when used with EMS. FortiClient endpoints connected via zero trust network access do not provide IP addresses to FortiOS.

For connection to FortiAnalyzer, see Incoming ports.

To edit the Fabric device tag sharing settings:

1. Go to *Fabric & Connectors* > *Fabric Devices*.
2. Select the desired device, then select *Edit*.
3. From the *FortiClient Endpoint Sharing* dropdown list, select one of the following:

Option	Description
Share all FortiClients	Selected FortiGate receives all endpoints' resolved IP or MAC addresses (hereafter referred to as "host tag"), regardless of whether the gateways point to the selected FortiGate.
Only share FortiClients connected to this fabric device (Recommended)	Default setting. Selected FortiGate only receives the host tags for endpoints whose gateways point to the selected FortiGate.
Share FortiClients connected to selected fabric devices	The selected FortiGate receives host tags for the following: • Endpoints whose gateways point to the selected FortiGate • Endpoints whose gateways point to the configured additional FortiGates. You can configure up to four additional FortiGates.

4. In *Tag Types Being Shared*, select at least one of the tag types to share. *Security Posture Tags* is selected by default and you cannot deselect it. EMS only shares the selected tag types with the configured Fortinet Security Fabric devices.

Tag	Description
Security posture tags	See Security Posture Tags on page 408.
FortiGuard outbreak alert tags	See FortiGuard Outbreak Alerts on page 448.
Classification tags	See Viewing the Endpoints pane on page 57.
Fabric tags	Fabric tags require connection to FortiAnalyzer. See the following process: 1. EMS administrator configures FortiAnalyzer in a System Settings profile. See System Settings on page 378. 2. FortiClient connects to EMS and receives FortiAnalyzer connection information from the profile. 3. FortiClient sends logs to FortiAnalyzer. 4. FortiAnalyzer administrator configures rule to tag endpoints which have indicators of compromise (IOC). 5. If a log entry received from FortiClient on the FortiAnalyzer matches an IOC, FortiAnalyzer adds a tag to that endpoint. 6. EMS adds this tag to the endpoint. You can view the tag in the

Tag	Description
	endpoint details, as well as in *Security Posture Tag Monitor*. This tag displays as a Fortinet Security Fabric tag in *Security Posture Tag Monitor*, but the tag displays under *Classification Tags* in endpoint details. See Viewing the Endpoints pane on page 57. 7. If FortiGate is configured to receive all tags for this specific endpoint, EMS sends the tag to FortiGate. See EMS API support for FortiAnalyzer to notify and tag suspicious endpoints.

5. Click *Save*.

To change the FortiGate authorization status:

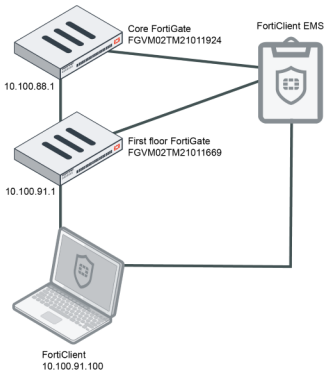
1. Go to *Fabric & Connectors* > *Fabric Devices*.
2. Select the desired FortiGate.
3. Click *Deny* or *Authorize*. The FortiGate status in the *Authorized* column changes.

Configuring EMS to share tagging information with multiple FortiGates

When an endpoint has a security posture tag applied and EMS is operating as part of a Fortinet Security Fabric, the FortiGate that the endpoint's FortiClient gateway points to receives the endpoint's resolved IP or MAC address (hereafter referred to as "host tag") from EMS.

If your EMS is operating as part of a Security Fabric with multiple FortiGates, you may want to configure EMS to send the host tag to other FortiGates in the Fabric, in addition to the FortiGate that the endpoint's FortiClient gateway points to. You can configure this as follows.

The following illustrates the topology in this example:



The following is true for this scenario:

- Both FortiGates are connected to EMS as part of a Security Fabric.
- FortiClient is registered to EMS.
- The FortiClient gateway points to the first floor FortiGate.
- The FortiClient endpoint has the TAG_ANTIVIRUS_ON security posture tag applied.

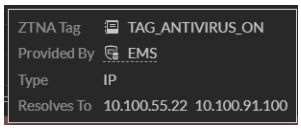
- The host tag of the FortiClient endpoint with TAG_ANTIVIRUS_ON applied is 10.100.91.100.

By default in this example, the core FortiGate does not retrieve the host-tag information for TAG_ANTIVIRUS_ON. This is because the FortiClient device gateway is 10.100.91.1, which does not match the core FortiGate.

You can configure the core FortiGate to retrieve the host tag for TAG_ANTIVIRUS_ON by allowing the host tag to sync from FortiClient endpoints connected to the first floor FortiGate to the core FortiGate.

To configure EMS to share the host tag to additional FortiGates:

1. Go to *Fabric & Connectors* > *Fabric Devices*.
2. Select the serial number associated with the core FortiGate. In this example, it is FGVM02TM21011924.
3. Click *Edit*.
4. From the *FortiClient Endpoint Sharing* dropdown list, select *Share FortiClients connected to selected fabric devices*.
5. From the *Filter Tag IPs From Specific FortiGates* dropdown list, select the serial number of the FortiGate on the first floor. In this example, it is FGVM02TM21011669. This change triggers EMS to resynchronize tag information to the first floor FortiGate.
6. Click *Save*.
7. Reselect the core FortiGate. It now displays that it receives host tag information from the first floor FortiGate.
8. Verify that the core FortiGate is receiving the tag information:
   a. In FortiOS on the core FortiGate, go to *Policy & Objects* > *ZTNA* > *ZTNA Tags*.
   b. Hover over the ZTNA tag *TAG_ANTIVIRUS_ON*. Confirm that the *Resolves To* IP address displays the FortiClient IP address.



Configuring FortiGate per-VDOM connection

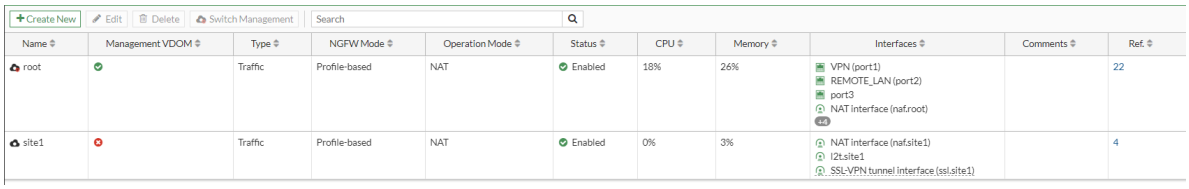
Each FortiOS virtual domain (VDOM) can connect to a separate EMS or EMS multitenancy site. This provides EMS with the ability to only send FortiClient and tagging information to a single FortiOS VDOM.

This feature requires FortiOS 7.4.

To configure EMS support for FortiGate per-VDOM connection:

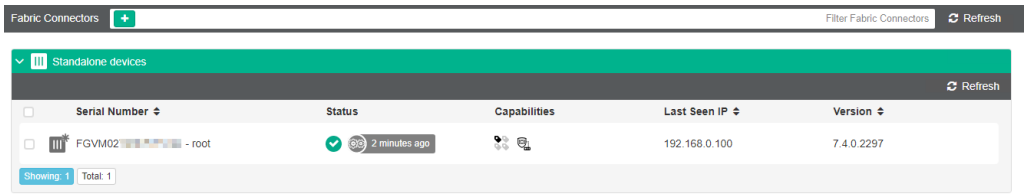
1. In FortiOS, enable the VDOM feature by doing one of the following:
   a. Go to *System* > *VDOM* and create a new site.
   b. Run the following commands:

```
config system global
   set vdom-mode multi-vdom
end
```



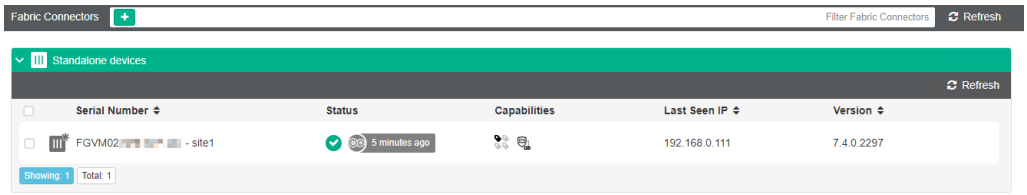
2. In EMS, enable multitenancy. Create a new multitenancy site.
3. Configure a Fortinet Security Fabric connection from the FortiGate root VDOM to the EMS default site. Once connected, the EMS default site shows the FortiGate root VDOM in *Fabric & Connectors > Fabric Devices* in <FortiGate serial number> - <VDOM name> format:

```
config vdom
edit root
config endpoint-control settings
    set override enable
end
config endpoint-control fctems-override
    edit 1
        set status enable
        set name "ems_default"
        set server "default.ems1.fortitest.ca"
    next
end
```



4. Configure a Fabric connection from the FortiGate non-root VDOM to the EMS non-default site. Once connected, the EMS non-default site shows the FortiGate non-root VDOM in *Fabric & Connectors > Fabric Devices* in <FortiGate serial number> - <VDOM name> format:

```
config vdom
edit site1
config endpoint-control settings
    set override enable
end
config endpoint-control fctems-override
    edit 1
        set status enable
        set name "ems_site1"
        set server "site1.ems1.fortitest.ca"
    next
end
```



5. Tagging information from an EMS site is only shared with the FortiGate VDOM that the EMS site has established a Fabric connection with. In this example, the ems_connected_default site is a tag configured on the EMS default site.

ZTNA Servers ZTNA Tags

Create New Group | Edit | Delete | Search

Name	Provided By	Details	Type	Category	Detection Level	Comments	Ref.
ZTNA IP all_registered_clients	EMS		ZTNA IP Tag	Zero Trust			0
ZTNA IP ems_connected_default	EMS		ZTNA IP Tag	Zero Trust			0
LOCAL TAG EMS_ALL_UNKNOWN_CLIENTS			ZTNA IP Tag				0
LOCAL TAG EMS_ALL_UNMANAGEABLE_CLIENTS			ZTNA IP Tag				0
ZTNA IP all_registered_clients			ZTNA IP Tag	Zero Trust			0
ZTNA IP domain_logged			ZTNA IP Tag	Zero Trust			0
ZTNA IP os			ZTNA IP Tag	Zero Trust			0
ZTNA IP all_registered_clients			ZTNA IP Tag	Zero Trust			0
ZTNA IP ems_connected			ZTNA IP Tag	Zero Trust			0
LOCAL TAG FCTEMS_ALL_FORTICLOUD_SERVERS			ZTNA IP Tag				0
ZTNA MAC all_registered_clients	EMS		ZTNA MAC Tag	Zero Trust			0
ZTNA MAC ems_connected_default	EMS		ZTNA MAC Tag	Zero Trust			0
ZTNA MAC all_registered_clients			ZTNA MAC Tag	Zero Trust			0
ZTNA MAC domain_logged			ZTNA MAC Tag	Zero Trust			0
ZTNA MAC os			ZTNA MAC Tag	Zero Trust			0
ZTNA MAC all_registered_clients			ZTNA MAC Tag	Zero Trust			0
ZTNA MAC ems_connected			ZTNA MAC Tag	Zero Trust			0

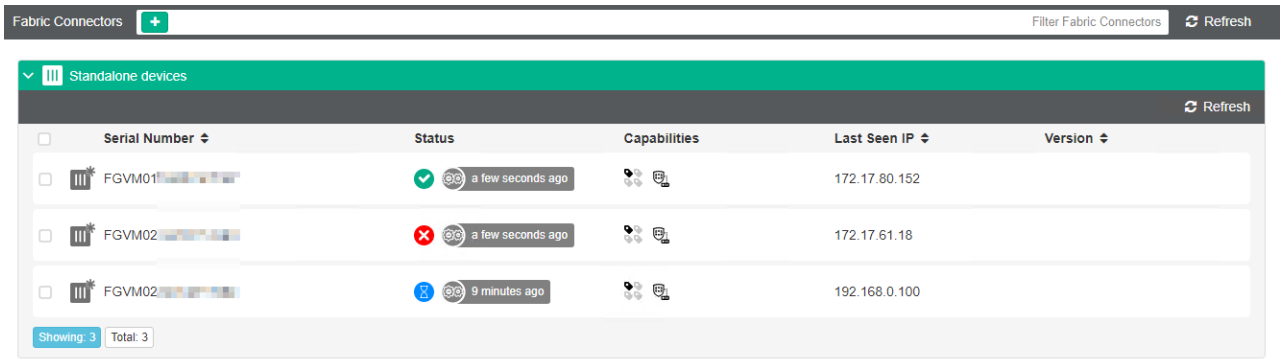
ems_connected_site1 is a tag configured on the EMS non-default site.

ZTNA Servers ZTNA Tags

Create New Group | Edit | Delete | Search

Name	Provided By	Details	Type	Category	Detection Level	Comments	Ref.
ZTNA IP all_registered_clients	EMS1		ZTNA IP Tag	Zero Trust			0
ZTNA IP ems_connected_site1	EMS1		ZTNA IP Tag	Zero Trust			0
LOCAL TAG EMS_ALL_UNKNOWN_CLIENTS			ZTNA IP Tag				0
LOCAL TAG EMS_ALL_UNMANAGEABLE_CLIENTS			ZTNA IP Tag				0
LOCAL TAG FCTEMS_ALL_FORTICLOUD_SERVERS			ZTNA IP Tag				0
ZTNA MAC all_registered_clients	EMS1		ZTNA MAC Tag	Zero Trust			0
ZTNA MAC ems_connected_site1	EMS1		ZTNA MAC Tag	Zero Trust			0

You can hover over the FortiGate in EMS and select *Edit* to update tag and FortiClient endpoint sharing information. You can also configure an alias for easier FortiGate identification. EMS shows one of the following authorization states for the Fabric connection: authorized, deauthorized, or pending.



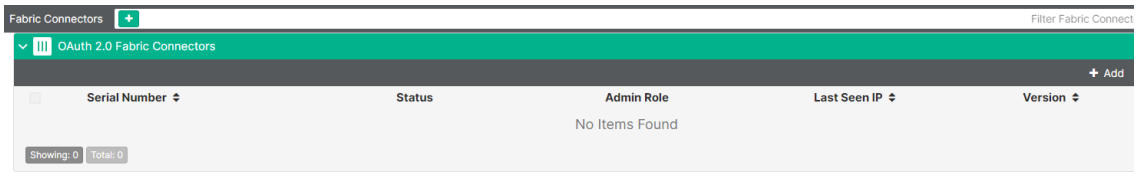
Creating connectors with OAuth 2.0 token-based authentication

EMS supports a connector type that uses OAuth 2.0 token-based authentication. When you create an OAuth 2.0 connector, EMS generates a client ID and secret for use by the Fortinet product on the other side of the connector. You can integrate EMS with the following Fortinet products:

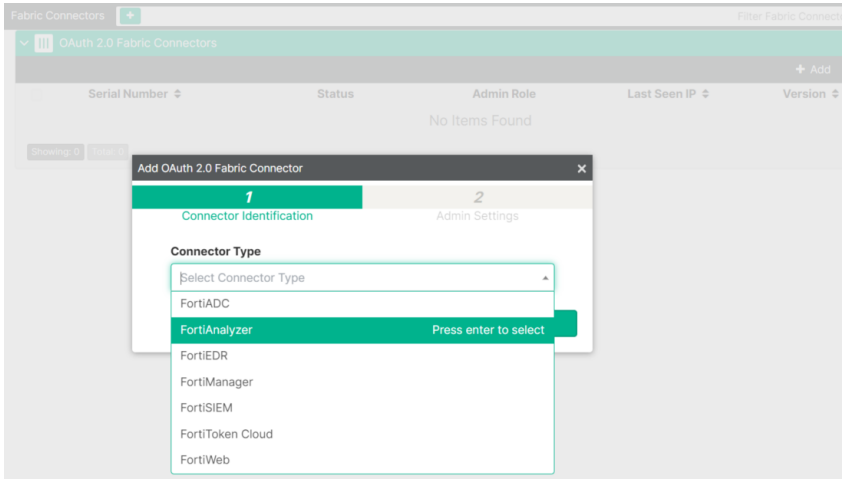
- FortiADC
- FortiAnalyzer
- FortiData
- FortiDeceptor
- FortiEDR
- FortiManager
- FortiSIEM
- FortiToken Cloud
- FortiWeb

To create a connector with OAuth 2.0 token-based authentication:

1. Go to *Fabric & Connectors* > *Fabric Devices*.



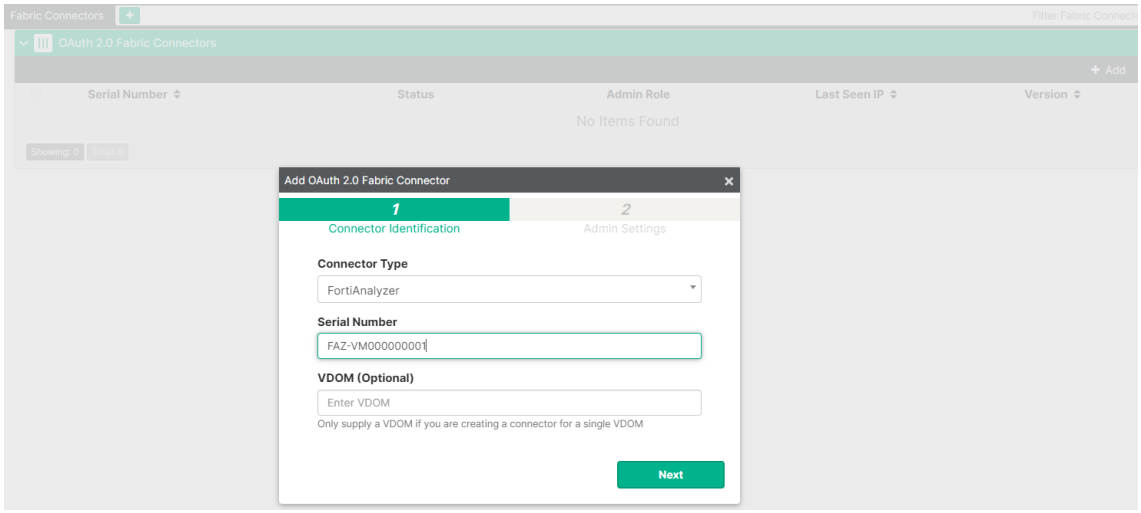
2. Click *Add*. The *Add OAuth 2.0 Fabric Connector* dialog displays.
3. From the *Connector Type* dropdown list, select the desired Fortinet product to integrate with EMS.



4. Do one of the following:
   a. If you are configuring a connector for FortiData, configure the following:
      i. In the *FortiData Hostname / IP address* field, enter the FortiData IP address.
      ii. In the *FortiData Port* field, enter 8443.
      iii. In the *FortiData REST API Key* field, paste the key that you created in FortiData.

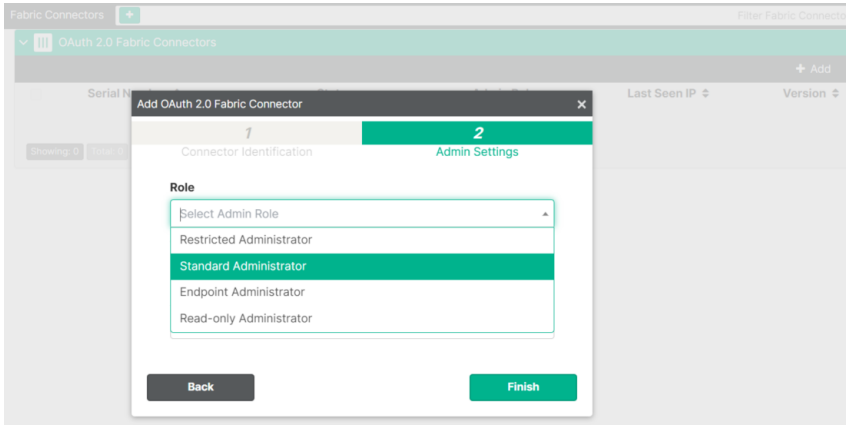
b. Otherwise, configure the following:

i. Enter the *Serial Number*.

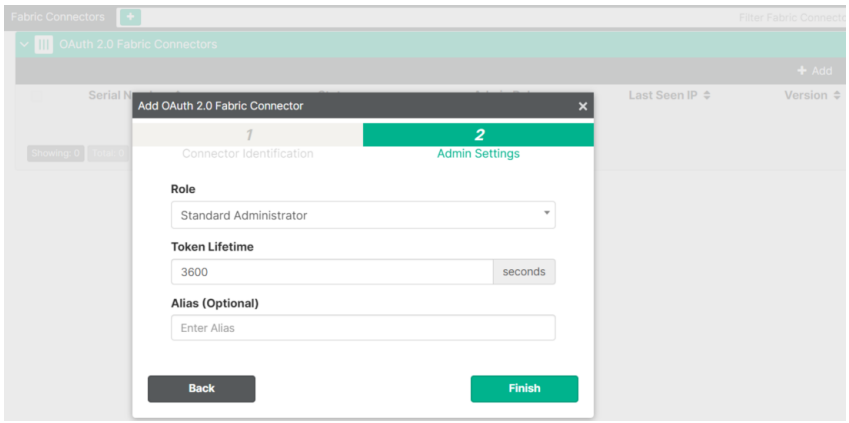


ii. Enter the *VDOM*, if desired.

5. Click *Next*.
6. Select the *Role*. The EMS admin role selected defines which EMS APIs (and therefore, features) that the Fabric device connector can access. For example, a Fabric connector that is configured with the Standard administrator role can access EMS APIs for endpoint and policy permissions and has read-only permissions to settings permissions. See Admin roles on page 480. Click *Finish*.

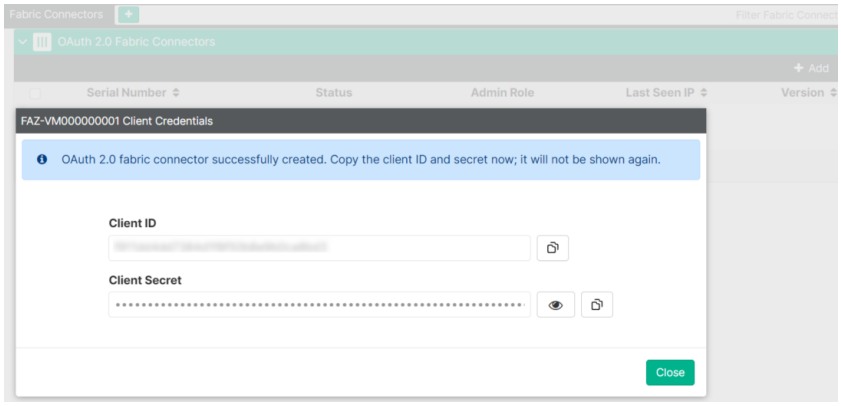


7. Enter the *Token Lifetime*.

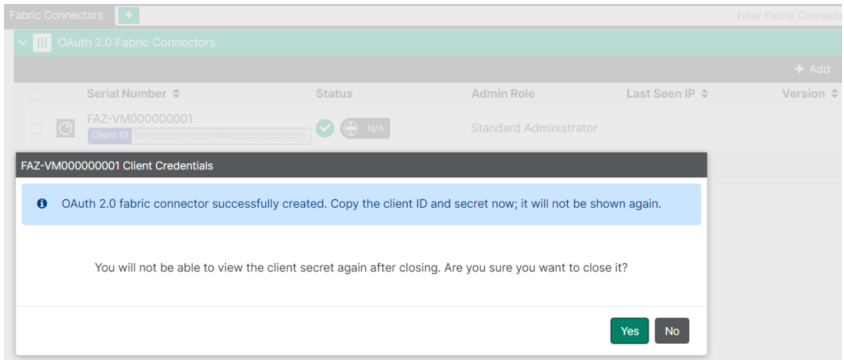


After the *Token Lifetime* is expired, the token is can no longer be authorized. The default value is 3600 seconds and the minimum value is 60 seconds.

8. Enter the *Alias*, if desired.
9. Click *Finish*. The *Client ID* and *Client Secret* are generated.



10. Copy the *Client ID* and *Client Secret*.
11. Click *Close*. A confirmation dialog is displayed.



12. Click *Yes*.

    The *Client ID* and *Client Secret* can be used by other Fortinet devices that support OAuth 2.0 Fabric connector features to call FortiClient EMS APIs.

Matched endpoints and resolved addresses

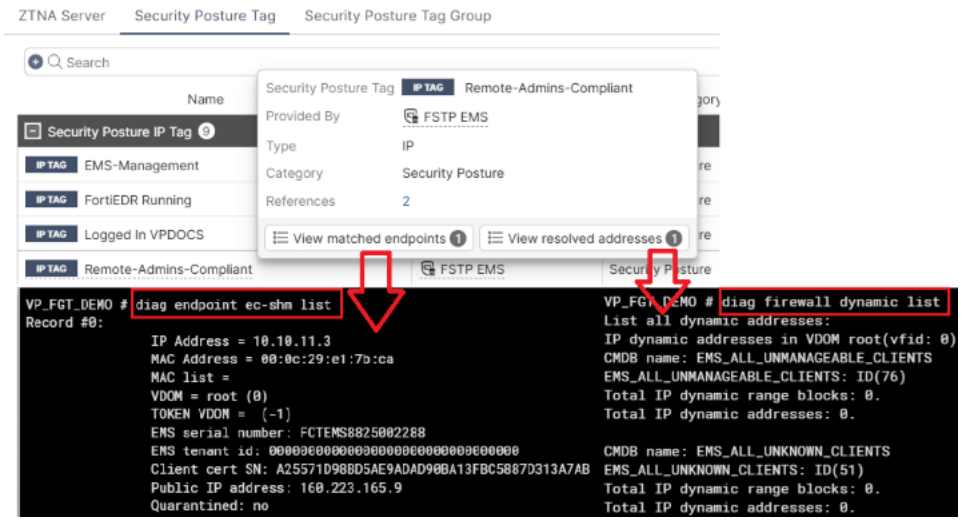
This document clarifies what matched endpoints and resolved addresses are and how they are populated.

Field	Description	How it is populated
Resolved addresses	Dynamic addresses that a FortiGate receives from EMS for tagged endpoints. The endpoints must be connected to a FortiGate directly or via a VPN tunnel. A FortiGate may receive dynamic addresses for endpoints that are not connected to it directly or via VPN if the EMS administrator enables *Share all FortiClients*. *Resolved addresses* only applies to IP/MAC access control (zero trust network access (ZTNA) NAC) and does not apply to pure ZTNA.	Endpoint MAC and/or IP addresses shows under *Resolved addresses* in the FortiOS GUI as a result of `/tags` API calls that the FortiGate makes towards EMS.
Matched endpoints	List of endpoint information that EMS supplies to FortiOS. Depending on the EMS version, *FortiClient Endpoint Sharing* configuration, and endpoint location, results can differ. See the different scenarios that this document presents to find out whether to expect *matched endpoints* to be populated.	*Matched endpoints* gets populated with EMS's responses to FortiGate's `/sysinfo` API call.

To retrieve resolved addresses and matched endpoints, run the following commands on the FortiGate CLI, respectively:

```
diagnose firewall dynamic list
```

```
diagnose endpoint ec-shm list
```



ZTNA vs IP/MAC access control

Using ZTNA or IP/MAC access control influences resolved addresses and matched endpoints.

ZTNA

When FortiClient performs ZTNA connection, *Resolved addresses* is not populated with the endpoint's IP or MAC address.

Resolved addresses only applies to IP/MAC access control on page 437 as the FortiGate relies on a source address, IP or MAC, to process incoming traffic via firewall policy with security posture tags enforced.

Matched endpoints is populated with the endpoint's information when FortiClient performs ZTNA connection.

IP/MAC access control

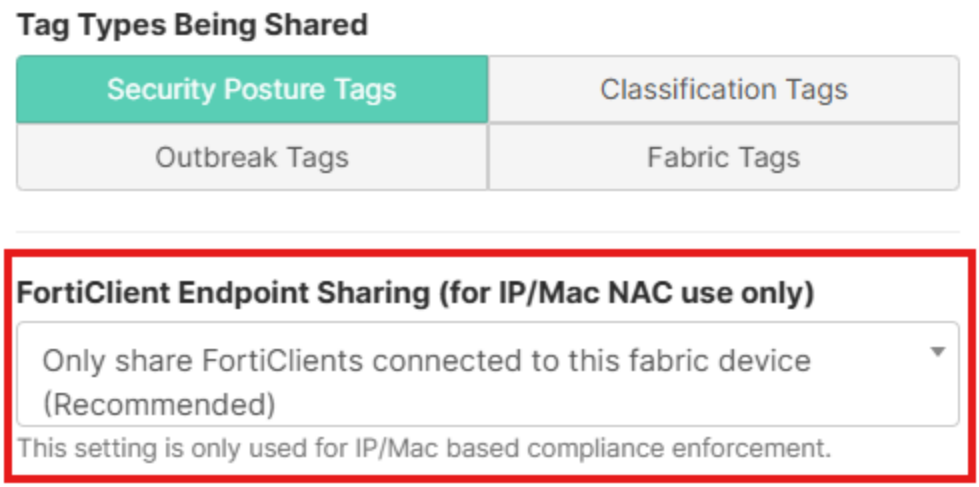
When an endpoint's gateway address points to the FortiGate or FortiClient performs direct VPN connection to it, the FortiClient address shows in *Resolved addresses*. For a directly connected client, the endpoint MAC and IP addresses populate. For a VPN-connected client, only the IP address populates.

FortiGate uses this address to filter incoming traffic and associate it with a tag applied to the firewall policy.

Matched endpoints also populates with directly or VPN-connected FortiClients.

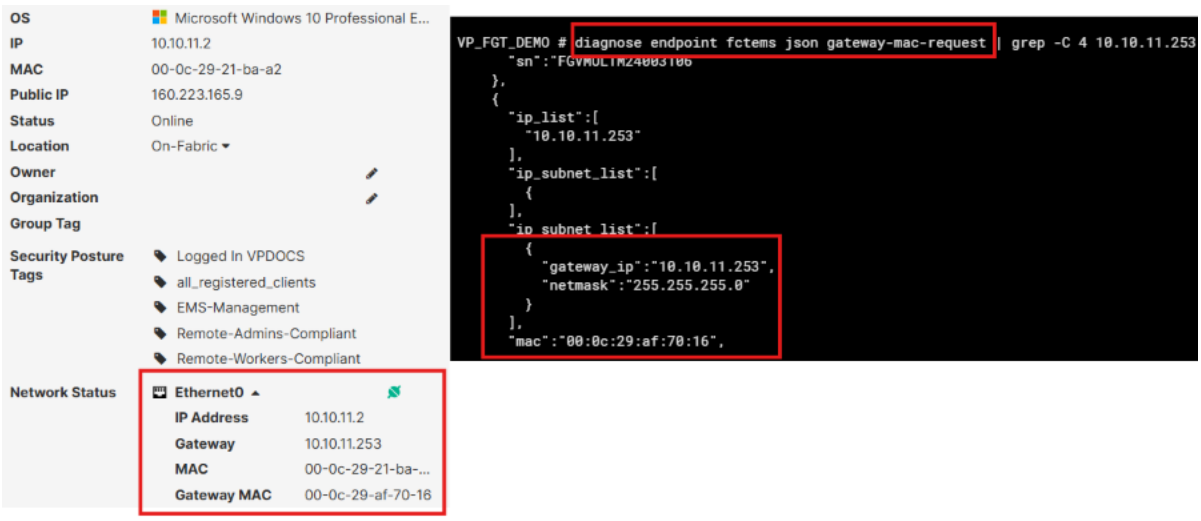
Only share FortiClients connected to this fabric device

The following sections cover common topological scenarios and how they affect *Matched endpoints* and *Resolved addresses* with *Only share FortiClients connected to this fabric device* selected for *FortiClient Endpoint Sharing*.

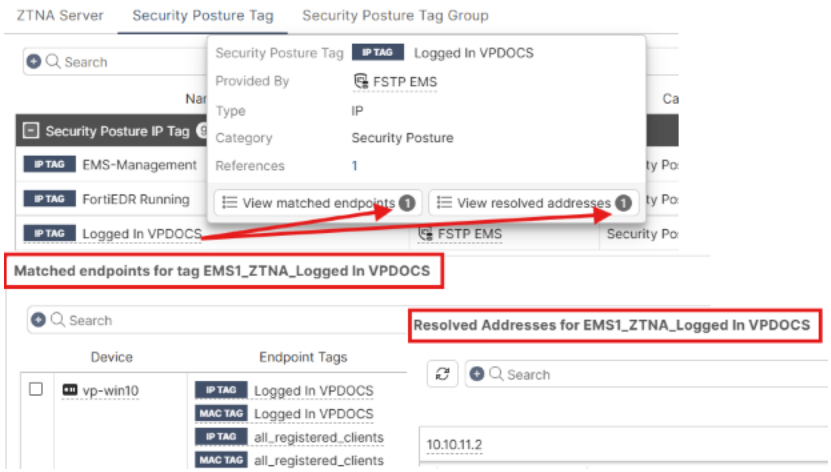


FortiGate as default gateway

A following contains an endpoint's networking details, including its gateway IP and MAC addresses, which match one of the FortiGate's interfaces as shown in the output of the `diagnose endpoint fctems json gateway-mac-request` command.

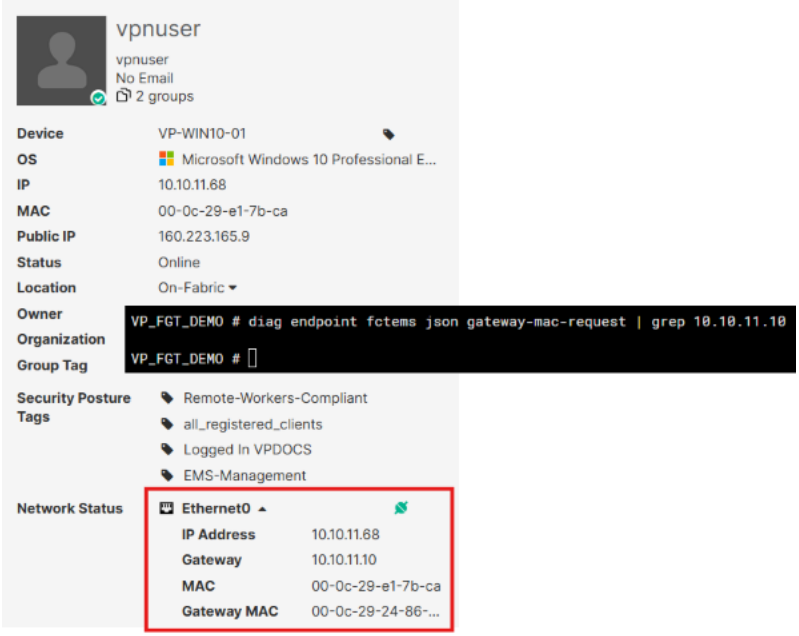


As a result, the endpoint shows under *Matched endpoints* and *Resolved addresses*.

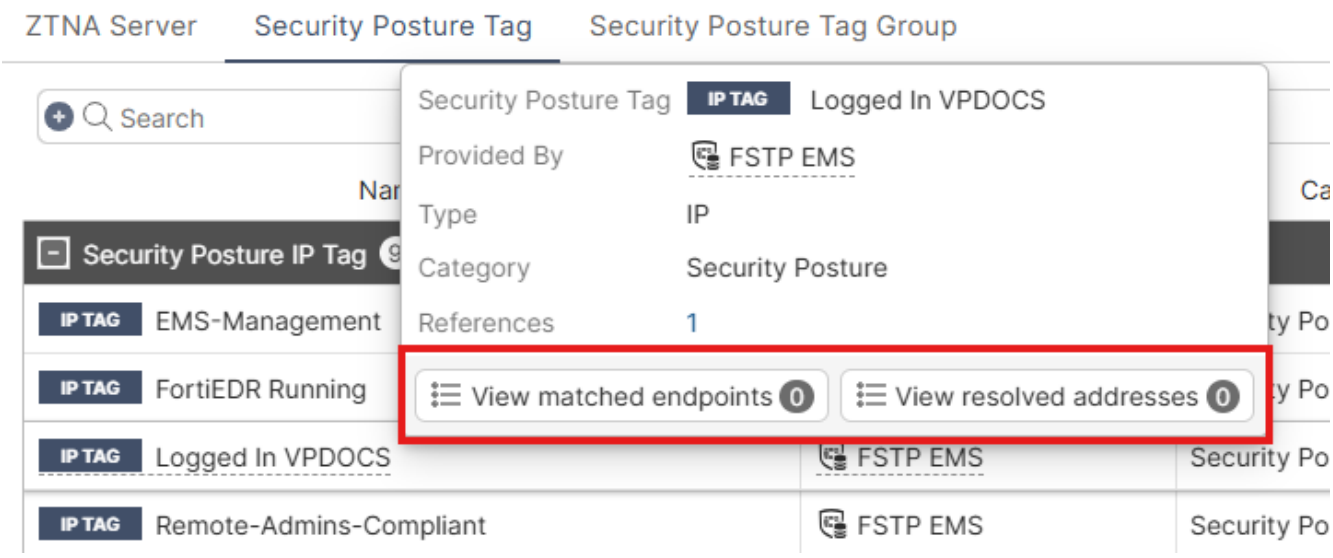


FortiGate not as default gateway

In the following, the FortiClient gateway address does not point to the FortiGate in question.



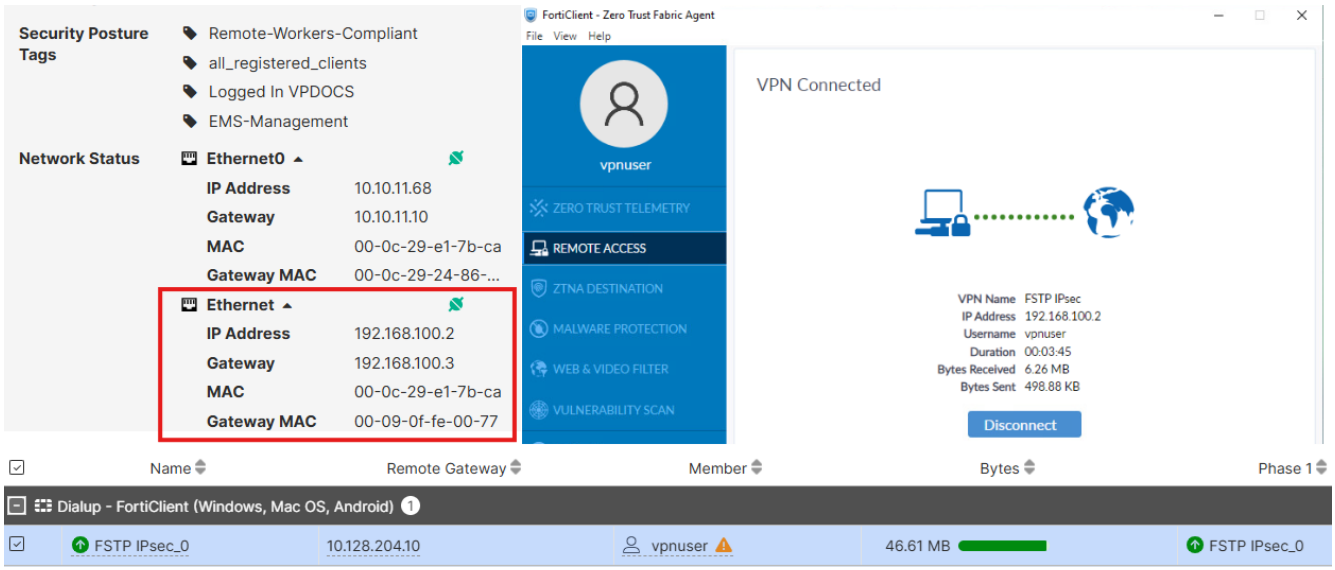
As a result, the endpoint does not show *Matched endpoints* or *Resolved addresses*.



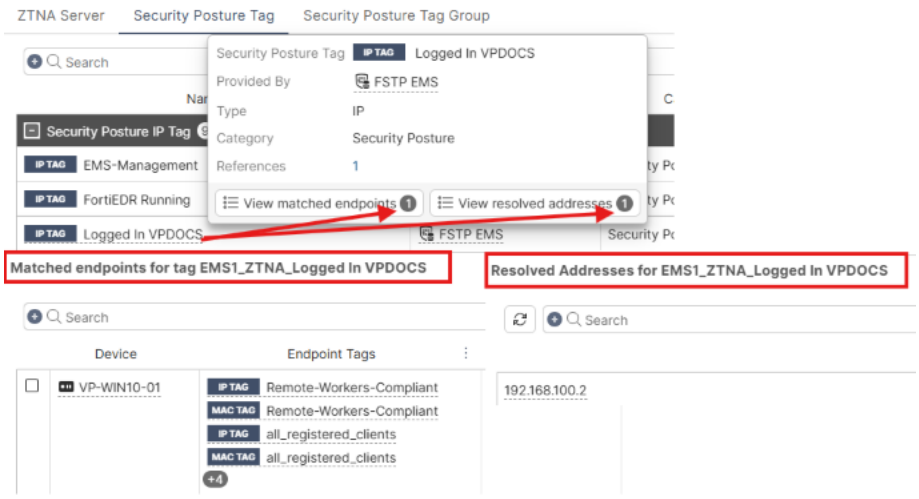
FortiGate as VPN server

This example uses the same endpoint as in FortiGate not as default gateway on page 438.

FortiClient is connected to FortiGate VPN.



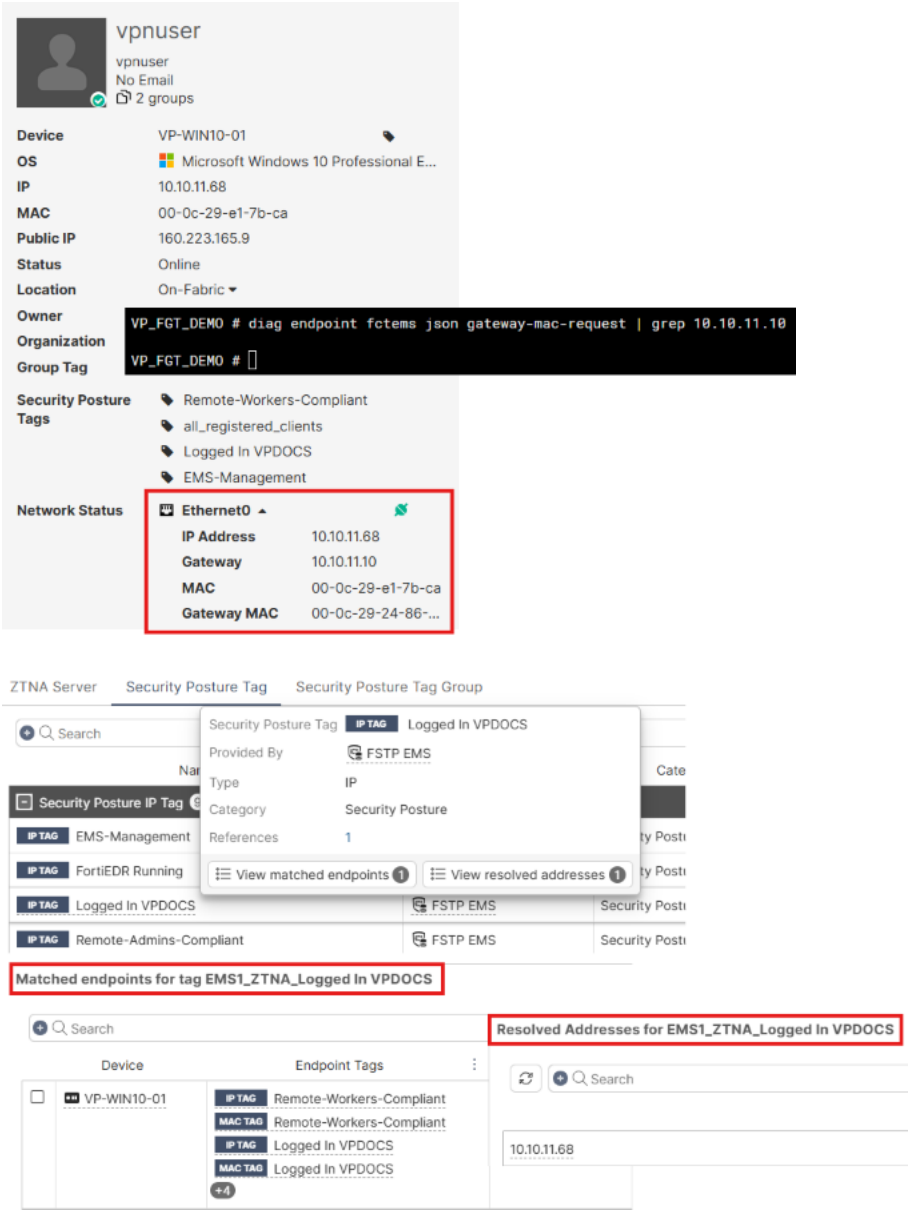
This results in the endpoint showing under both *Matched endpoints* and *Resolved addresses*.



Share all FortiClients

You can use *Share all FortiClients* when the endpoint has no direct connection to FortiGate, neither by having its interface's gateway address pointing to the FortiGate nor having direct VPN connection to it. See Configuring EMS to share tagging information with multiple FortiGates on page 429.

Enabling *Share all FortiClients* results in both *Resolved addresses* and *Matched endpoints* being populated for remote FortiClients.



Troubleshooting

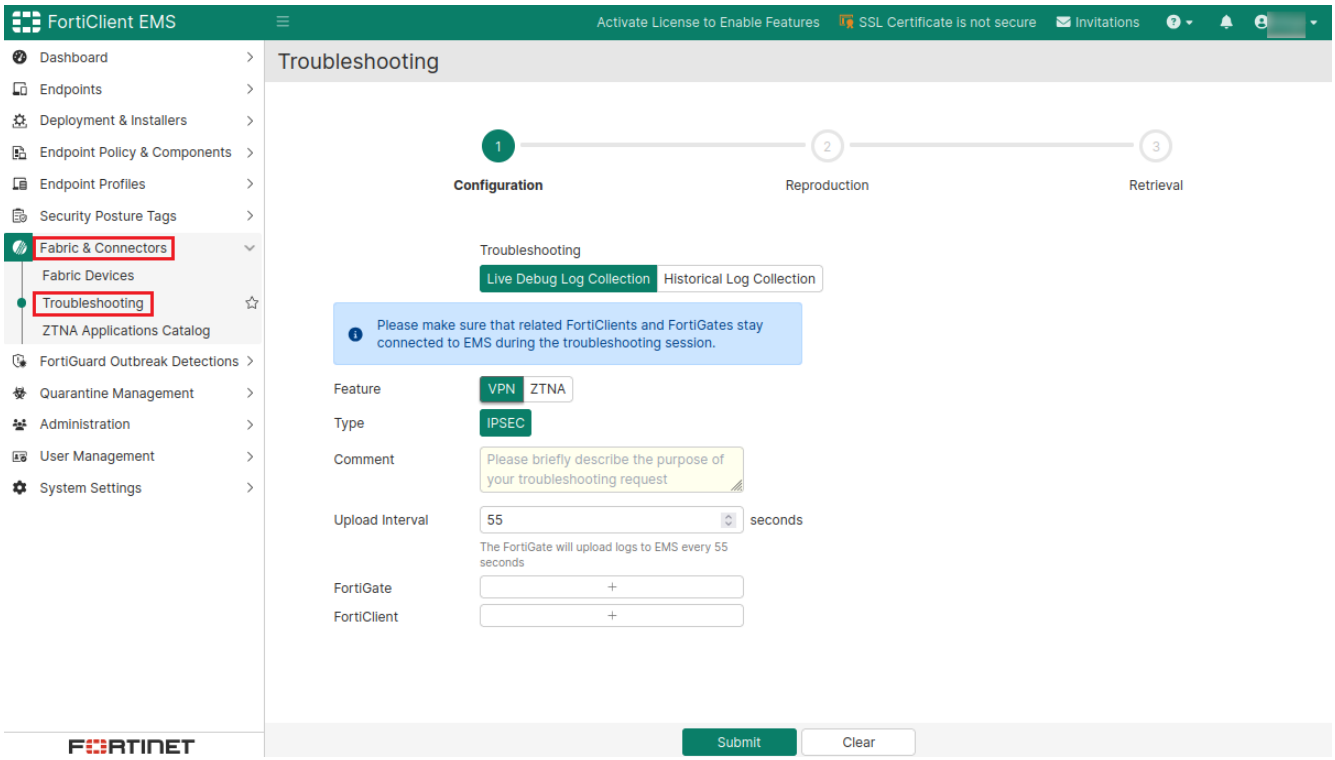
EMS collects time-correlated IPsec VPN and ZTNA-related logs from FortiGate and FortiClient to help troubleshoot ZTNA and IPsec VPN integration issues between FortiGate and EMS.

The *Fabric & Connectors >Troubleshooting* page includes the following troubleshooting options:

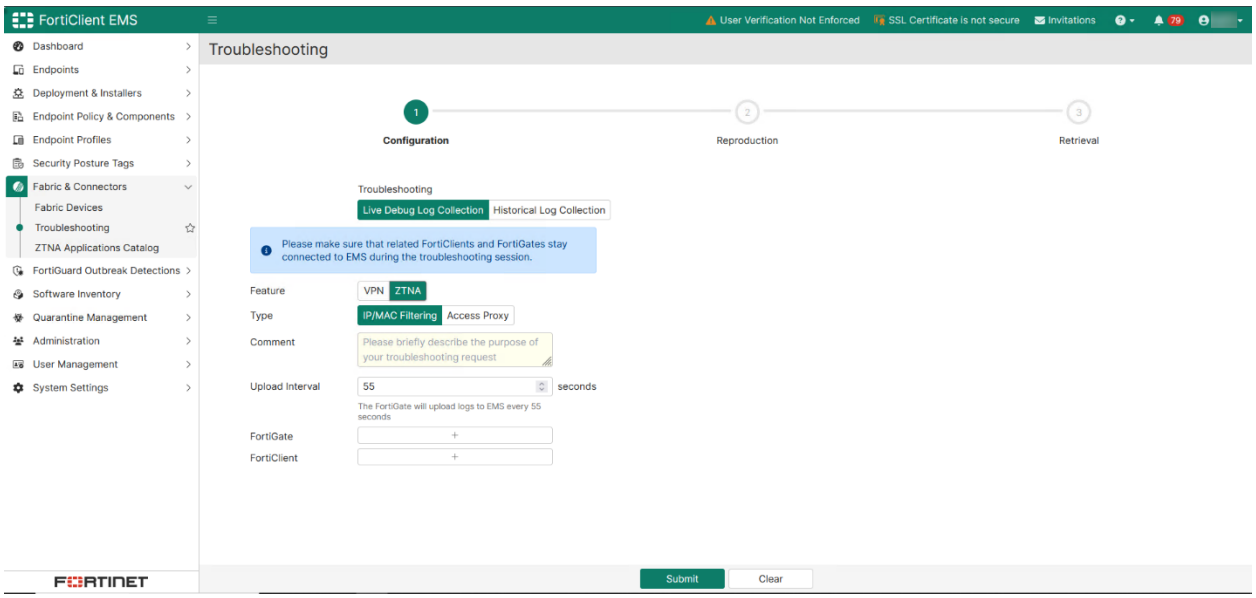
- *Live Debug Log Collection*—Collect real-time IPsec VPN or ZTNA log.
- *Historical Log Collection*—Collect IPsec VPN or ZTNA log within a specific historical period.

Live Debug Log Collection

You can configure the feature (VPN or ZTNA) and log type to be collected. The following is an example of *Live Debug Log Collection* for IPsec VPN.

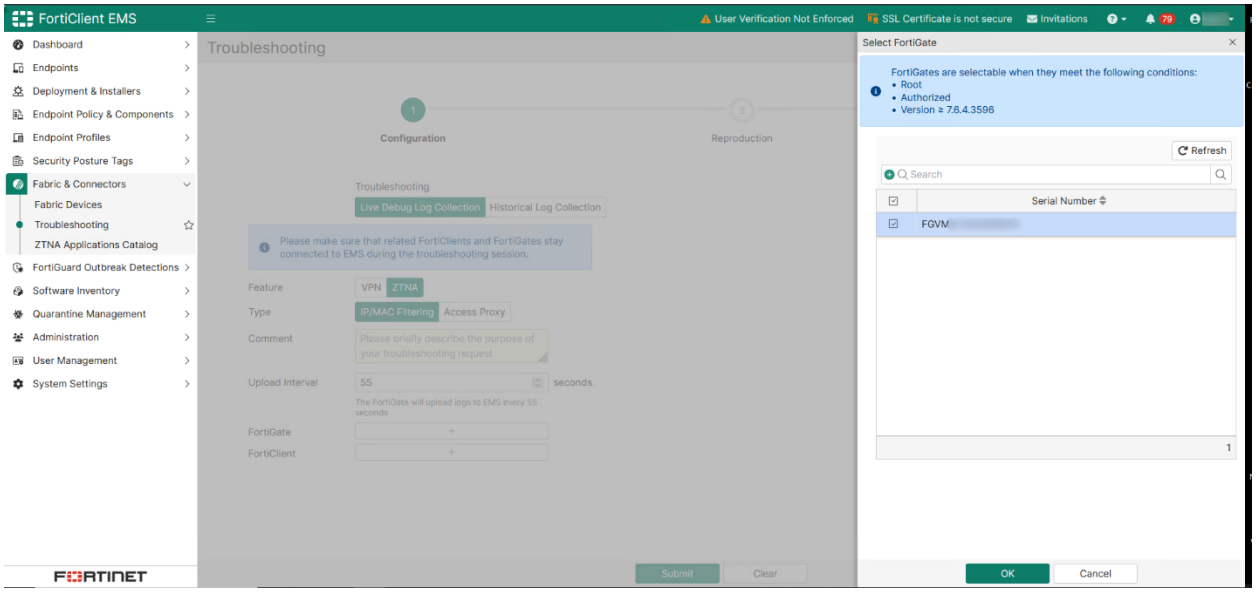


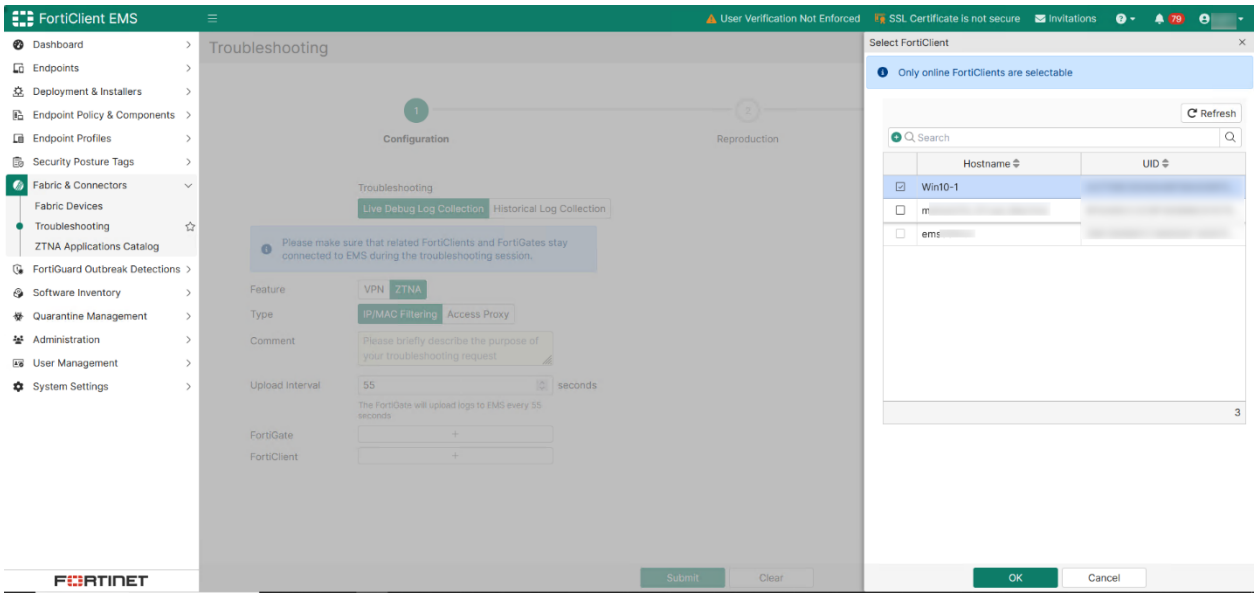
You can also select *Live Debug Log Collection* for ZTNA, which provides two types: *IP/MAC Filtering* and *Access Proxy*, depending on your log collection requirement.



Specify the upload interval within a range (between 20 to 86,400 seconds) at which the FortiGate device uploads logs to EMS.

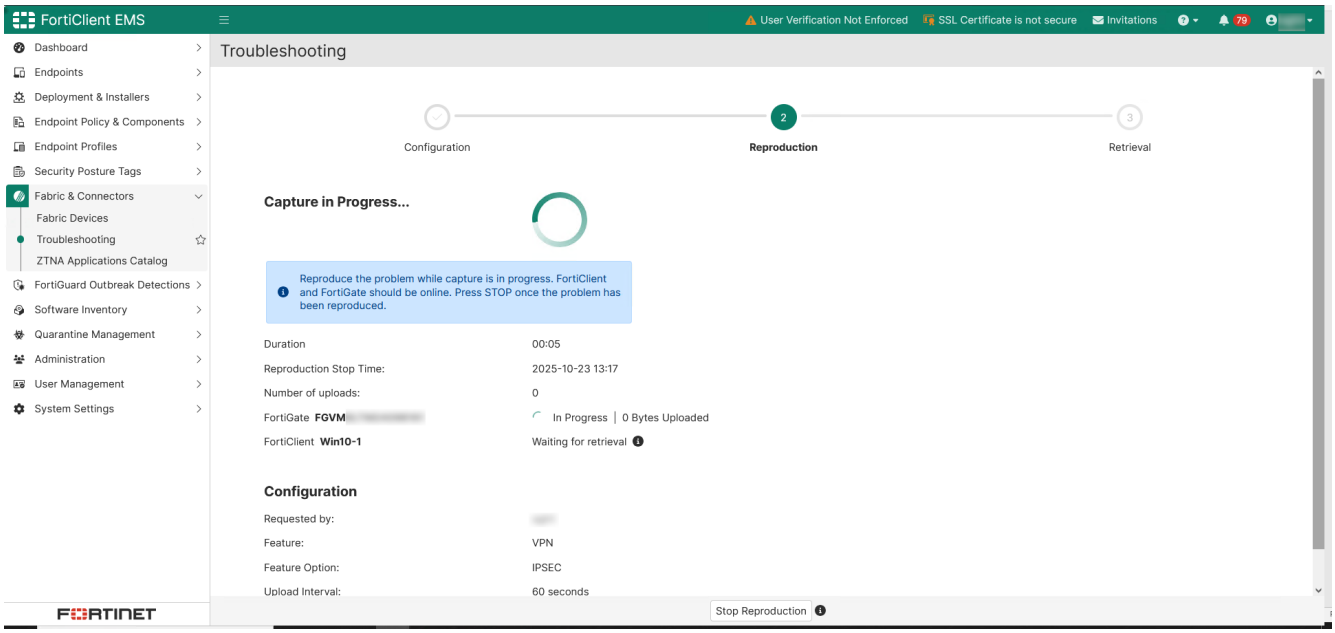
Use the *FortiGate (+)* and *FortiClient (+)* options to add FortiGate and FortiClient devices to collect logs from. Filter or search for specific FortiGate or FortiClient devices within the slide-out panel to refine the selection.





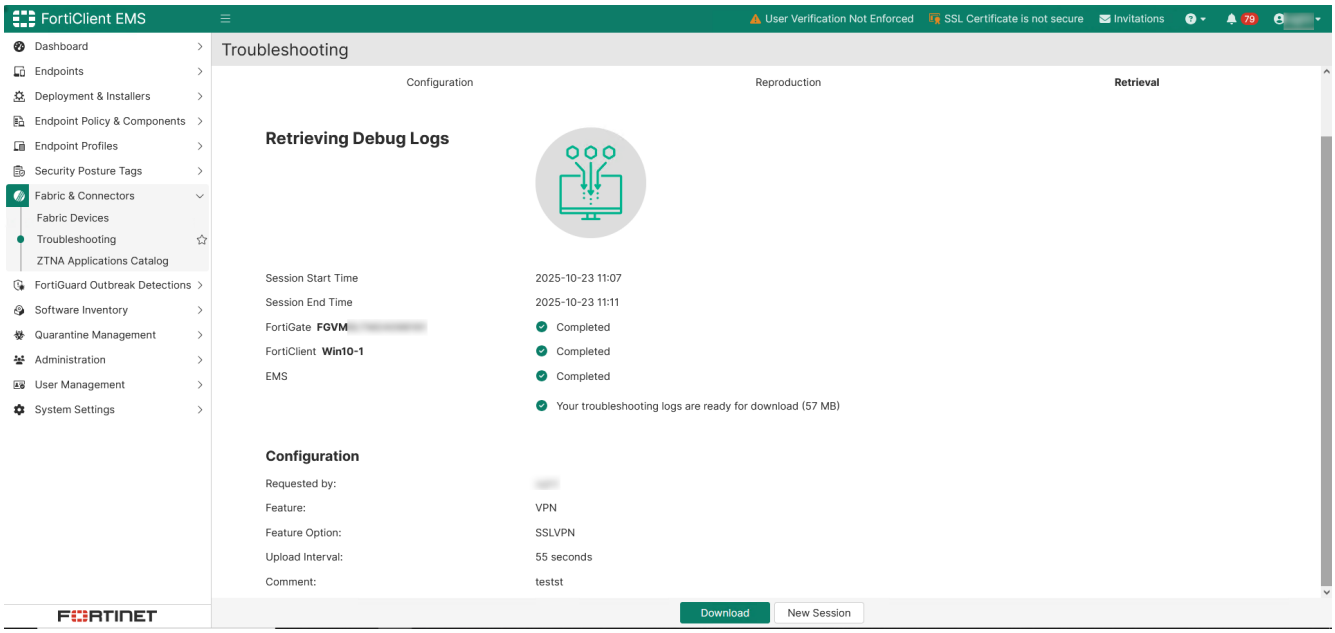
Click *Submit* and EMS will initiate the log collection request from the selected FortiGate and FortiClient devices on the*Reproduction* page.

Related FortiGate and FortiClient devices must stay connected to EMS during the troubleshooting session to ensure that logs are captured during the active occurrence of the issue for accurate troubleshooting.



After the logs have been captured or when you click *Stop Reproduction*, EMS proceeds to the *Retrieval* page where you can download the captured logs as a `.zip` file for troubleshooting or further analysis.

To start a new troubleshooting session, click *New Session*.

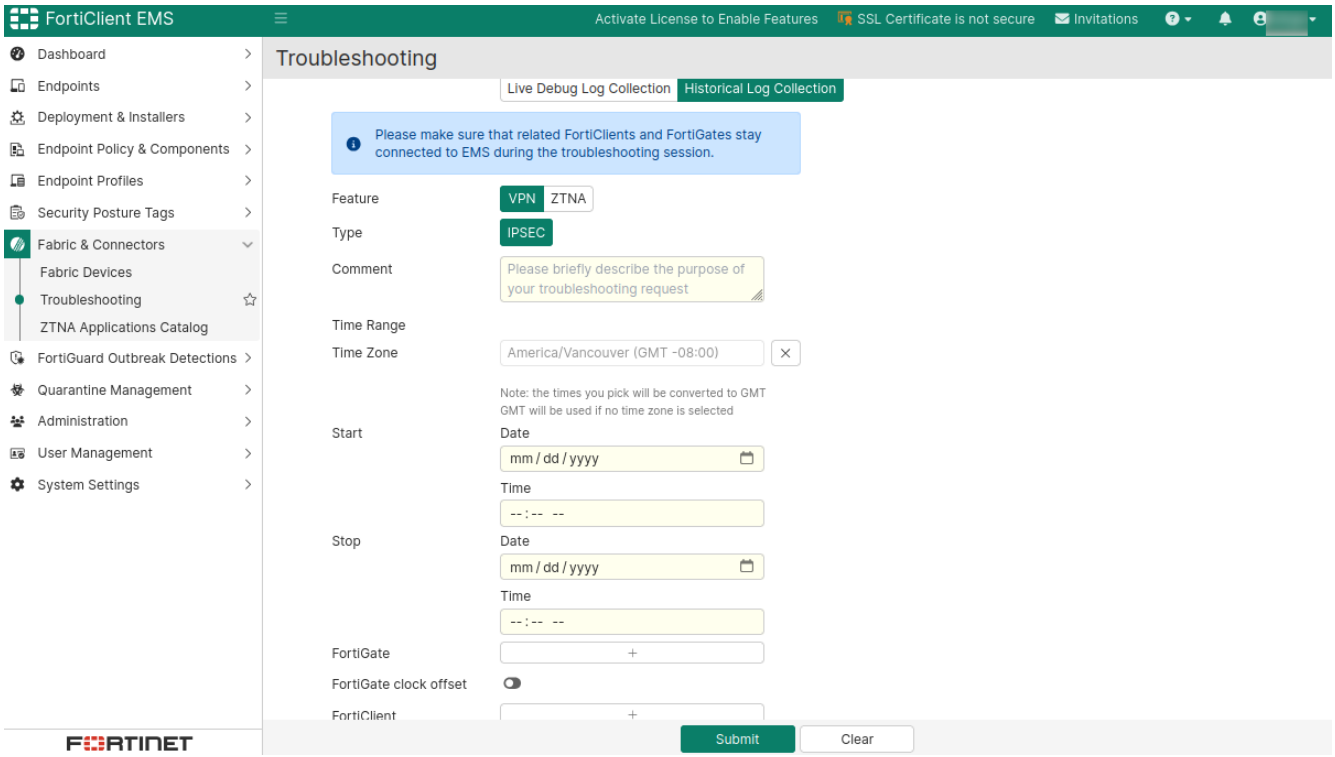


The following is a debug log snippet indicating that an endpoint attempts to establish a connection to the IPsec VPN on this FortiGate device. The log shows the negotiation steps involved in the process, which were collected by EMS during troubleshooting.

```
2025-10-24 17:32:39.825976 ike V-root:0: IKEv2 exchange=AUTH id=e09780e6e87dd25f/8e83be145ab38f67:00000001 len=576
2025-10-24 17:32:39.830054 ike 0: in E09780E6E87DD25F8E83BE145AB38F672E2023080000000100000240230002248236A1A3E275C3778EA41F83F92582E9D938F00033B6847A100AE2D72D654F26783718C6E3EEBD58B3B695558114 2E164C91E4A3018DC0FFCB9B176B38F9A01432AF6B6CDB8FACBCF11E1D08E289DE67038F33A29E4A24247B44188ZDFBA9B1545DEBDD6C66EB9C3401CD03C492B31D696FD1BDB00FF22F594648799C5D3FFFB08E72E9D056283CAED4251D8D5A73AD6131FEAE23AF95
2025-10-24 17:32:39.866127 ike V-root:0: invalid IKE request SPI e09780e6e87dd25f/8e83be145ab38f67:00000001
2025-10-24 17:33:00.105975 ike V-root:0: comes 10.0.0.10:51626->10.0.0.11:4500,ifindex=5,vrf=0,len=466....
2025-10-24 17:33:00.112182 ike V-root:0: IKEv2 exchange=SA_INIT id=a580d8f0c4cf182d/0000000000000000 len=462
2025-10-24 17:33:00.120298 ike 0: in A580D8F0C4CF182D0000000000000000212022080000000000001CE2200008C020000440101000703000008030000020300000C0100000C800E0080030000080400001403000008020000050300000802000006030000080200000700000000802000002
2025-10-24 17:33:00.150356 ike V-root:0:a580d8f0c4cf182d/0000000000000000:1: responder received SA_INIT msg
2025-10-24 17:33:00.153268 ike V-root:0:a580d8f0c4cf182d/0000000000000000:1: VID forticlient connect license 4C53427B6D465D1B337BB755A37A7FEF5824944DF77F0000
2025-10-24 17:33:00.157333 ike V-root:0:a580d8f0c4cf182d/0000000000000000:1: VID Fortinet Endpoint Control B4F01CA951E9DA8D0BAFBBD34AD3044E7824944DF77F0000
2025-10-24 17:33:00.161435 ike V-root:0:a580d8f0c4cf182d/0000000000000000:1: VID Forticlient EAP Extension C1DC4350476B98A429B91781914CA43E58F00F0ABB000000
2025-10-24 17:33:00.169453 ike V-root:0:a580d8f0c4cf182d/0000000000000000:1: received notify type NAT_DETECTION_SOURCE_IP
2025-10-24 17:33:00.175391 ike V-root:0:a580d8f0c4cf182d/0000000000000000:1: received notify type NAT_DETECTION_DESTINATION_IP
2025-10-24 17:33:00.178760 ike V-root:0:a580d8f0c4cf182d/0000000000000000:1: received notify type SIGNATURE_HASH_ALGORITHMS
2025-10-24 17:33:00.183036 ike V-root:0:a580d8f0c4cf182d/0000000000000000:1: incoming proposal:
2025-10-24 17:33:00.186837 ike V-root:0:a580d8f0c4cf182d/0000000000000000:1: proposal id = 1:
2025-10-24 17:33:00.190293 ike V-root:0:a580d8f0c4cf182d/0000000000000000:1:   protocol = IKEv2:
2025-10-24 17:33:00.193822 ike V-root:0:a580d8f0c4cf182d/0000000000000000:1:     encapsulation = IKEv2/none
2025-10-24 17:33:00.197839 ike V-root:0:a580d8f0c4cf182d/0000000000000000:1:         type=ENCR, val=AES_CBC (key_len = 128)
2025-10-24 17:33:00.202193 ike V-root:0:a580d8f0c4cf182d/0000000000000000:1:         type=INTEGR, val=AUTH_HMAC_SHA_96
2025-10-24 17:33:00.207288 ike V-root:0:a580d8f0c4cf182d/0000000000000000:1:         type=PRF, val=PRF_HMAC_SHA
2025-10-24 17:33:00.211729 ike V-root:0:a580d8f0c4cf182d/0000000000000000:1:         type=PRF, val=PRF_HMAC_SHA2_512
2025-10-24 17:33:00.216134 ike V-root:0:a580d8f0c4cf182d/0000000000000000:1:         type=PRF, val=PRF_HMAC_SHA2_384
2025-10-24 17:33:00.220500 ike V-root:0:a580d8f0c4cf182d/0000000000000000:1:         type=PRF, val=PRF_HMAC_SHA2_256
2025-10-24 17:33:00.220655 ike V-root:0:a580d8f0c4cf182d/0000000000000000:1:         type=DH_GROUP, val=ECP384.
2025-10-24 17:33:00.220678 ike V-root:0:a580d8f0c4cf182d/0000000000000000:1: proposal id = 2:
2025-10-24 17:33:00.220685 ike V-root:0:a580d8f0c4cf182d/0000000000000000:1:   protocol = IKEv2:
2025-10-24 17:33:00.220690 ike V-root:0:a580d8f0c4cf182d/0000000000000000:1:     encapsulation = IKEv2/none
2025-10-24 17:33:00.220696 ike V-root:0:a580d8f0c4cf182d/0000000000000000:1:         type=ENCR, val=AES_CBC (key_len = 256)
2025-10-24 17:33:00.220702 ike V-root:0:a580d8f0c4cf182d/0000000000000000:1:         type=INTEGR, val=AUTH_HMAC_SHA2_256_128
2025-10-24 17:33:00.220709 ike V-root:0:a580d8f0c4cf182d/0000000000000000:1:         type=PRF, val=PRF_HMAC_SHA
2025-10-24 17:33:00.220715 ike V-root:0:a580d8f0c4cf182d/0000000000000000:1:         type=PRF, val=PRF_HMAC_SHA2_512
2025-10-24 17:33:00.220720 ike V-root:0:a580d8f0c4cf182d/0000000000000000:1:         type=PRF, val=PRF_HMAC_SHA2_384
2025-10-24 17:33:00.220725 ike V-root:0:a580d8f0c4cf182d/0000000000000000:1:         type=PRF, val=PRF_HMAC_SHA2_256
2025-10-24 17:33:00.220730 ike V-root:0:a580d8f0c4cf182d/0000000000000000:1:         type=DH_GROUP, val=ECP384.
2025-10-24 17:33:00.220750 ike V-root:0:a580d8f0c4cf182d/0000000000000000:1: matched proposal id 2
2025-10-24 17:33:00.220757 ike V-root:0:a580d8f0c4cf182d/0000000000000000:1: proposal id = 2:
2025-10-24 17:33:00.220763 ike V-root:0:a580d8f0c4cf182d/0000000000000000:1:   protocol = IKEv2:
2025-10-24 17:33:00.220768 ike V-root:0:a580d8f0c4cf182d/0000000000000000:1:     encapsulation = IKEv2/none
2025-10-24 17:33:00.220773 ike V-root:0:a580d8f0c4cf182d/0000000000000000:1:         type=ENCR, val=AES_CBC (key_len = 256)
2025-10-24 17:33:00.220778 ike V-root:0:a580d8f0c4cf182d/0000000000000000:1:         type=INTEGR, val=AUTH_HMAC_SHA2_256_128
2025-10-24 17:33:00.220783 ike V-root:0:a580d8f0c4cf182d/0000000000000000:1:         type=PRF, val=PRF_HMAC_SHA2_256
2025-10-24 17:33:00.220788 ike V-root:0:a580d8f0c4cf182d/0000000000000000:1:         type=DH_GROUP, val=ECP384.
2025-10-24 17:33:00.220793 ike V-root:0:a580d8f0c4cf182d/0000000000000000:1: lifetime=86400
2025-10-24 17:33:00.220800 ike V-root:0:a580d8f0c4cf182d/0000000000000000:1: SA proposal chosen, matched gateway ipsec
2025-10-24 17:33:00.220824 ike V-root:0:ipsec:ipsec: created connection: 0x557cf5cb3160 5 10.0.0.11->10.0.0.10:51626.
2025-10-24 17:33:00.220845 ike V-root:0:ipsec:1: processing notify type NAT_DETECTION_SOURCE_IP
2025-10-24 17:33:00.220878 ike V-root:0:ipsec:1: ignoring unauthenticated notify payload (NAT_DETECTION_SOURCE_IP)
2025-10-24 17:33:00.220884 ike V-root:0:ipsec:1: processing notify type NAT_DETECTION_DESTINATION_IP
2025-10-24 17:33:00.220894 ike V-root:0:ipsec:1: ignoring unauthenticated notify payload (NAT_DETECTION_DESTINATION_IP)
2025-10-24 17:33:00.220900 ike V-root:0:ipsec:1: processing notify type SIGNATURE_HASH_ALGORITHMS
2025-10-24 17:33:00.220910 ike V-root:0:ipsec:1: FEC vendor ID received FEC but IP not set
2025-10-24 17:33:00.220916 ike 0:ipsec:1: FCT EAP 2FA extension vendor ID received
```

Historical Log Collection

In *Historical Log Collection* mode, users must specify a start and stop time, which can be set to a period in the past. Additionally, the *Time Zone* can be selected to ensure the log collection aligns with the desired temporal context.



ZTNA Applications Catalog

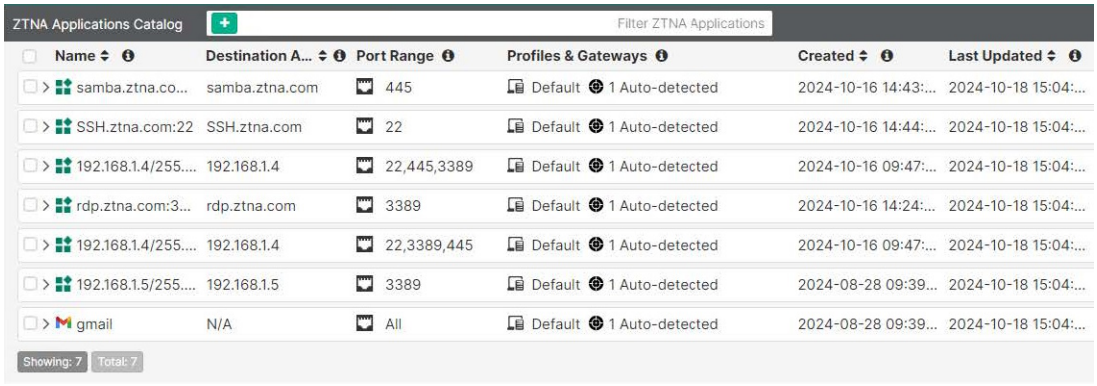
ZTNA Applications Catalog displays configured zero trust network access (ZTNA) applications.

If you have configured a Fortinet Security Fabric connection between FortiOS 7.4.4 or later and EMS and a ZTNA server is configured in FortiOS, EMS can retrieve non-web (TCP forwarding) ZTNA applications from FortiOS. See Configuring FortiClient EMS. You can view the ZTNA applications catalog in *Fabric & Connectors > ZTNA Applications Catalog*.

When a ZTNA application is defined on a FortiGate that connects to EMS via the Security Fabric wizard, EMS defines that ZTNA gateway (the FortiGate) and the ZTNA application as autodetected. You cannot modify autodetected ZTNA gateways or applications on EMS. Autodetected gateways are not available for gateway selection for a ZTNA application manually defined on EMS.

A ZTNA gateway that is defined manually on EMS is available for gateway selection when adding a ZTNA application manually in EMS.

You can switch between *Applications View* and *Gateway View*. *Applications View* displays automatically detected and manually added ZTNA applications.



Gateway View displays ZTNA applications by ZTNA proxy gateway.



You can also manually add ZTNA applications.

To add a private ZTNA application:

1. Go to *Fabric & Connectors > ZTNA Applications Catalog*.
2. Click *Add*.
3. For *Application Type*, select *Private*.

4. Select *IP*, *IP Range*, *FQDN*, *Wildcard FQDN*, or *CIDR* to define the destination. Enter the desired value in the field.
5. In the *Subnet Mask* field, enter the desired subnet mask.
6. If desired, select a port option and configure the desired port.
7. From the *Select Gateways* dropdown list, selected the desired gateway. If desired, click *Add Gateway* to create a new gateway and define the IP address or FQDN, port, and alias.
8. In the *Name* field, enter the desired name.
9. If desired, select *Enable UDP* to enable UDP forwarding.
10. Click *Finish*.

To add a SaaS ZTNA application:

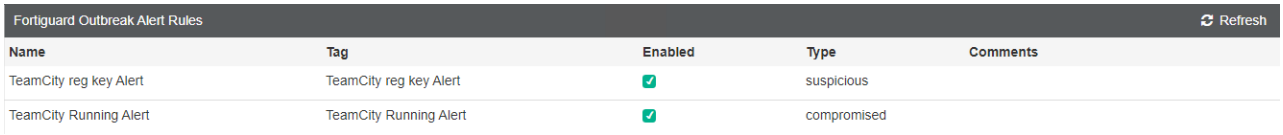
1. Go to *Fabric & Connectors > ZTNA Applications Catalog*.
2. Click *Add*.
3. For *Application Type*, select *SaaS*.
4. Configure SaaS applications by searching for and selecting the desired application in the dropdown list.
5. From the *Select Gateways* dropdown list, selected the desired gateway. If desired, click *Add Gateway* to create a new gateway and define the IP address or FQDN, port, and alias.
6. If desired, select *Enable UDP* to enable UDP forwarding.
7. Click *Finish*.

FortiGuard Outbreak Alerts

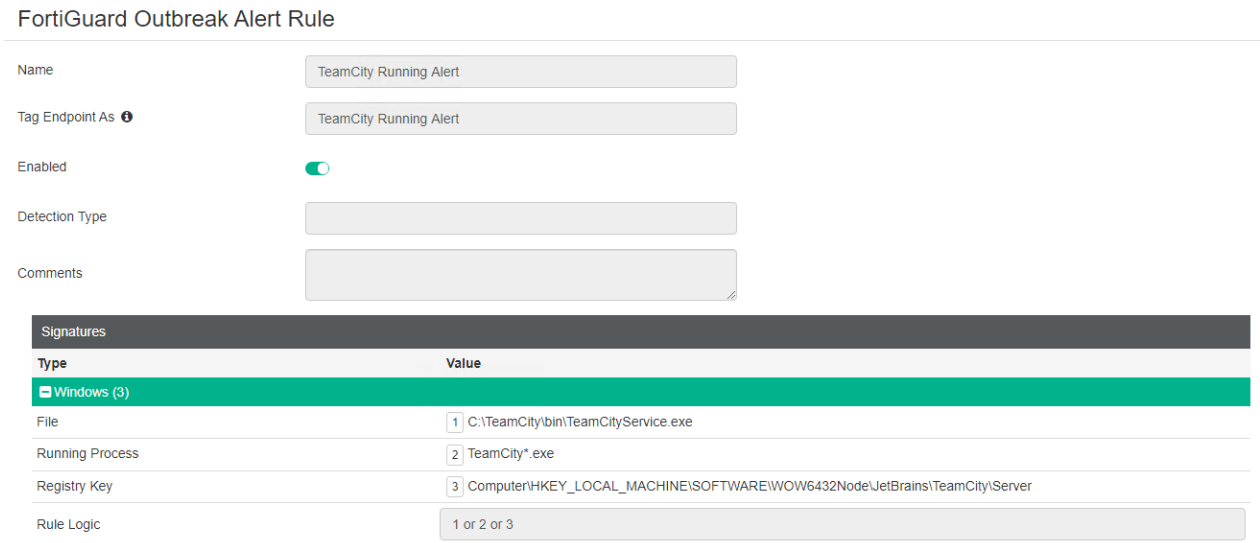
FortiEndpoint receives predefined outbreak alert rules from FortiGuard to help protect your network from vulnerabilities. For example, consider that FortiGuard Labs discovers a zero-day vulnerability in a popular application. The Fortinet team then creates a new FortiGuard outbreak alert rule, which tags endpoints with that application installed as vulnerable. After EMS receives this new rule from FortiGuard, you can easily see which endpoints are vulnerable to the new outbreak.

FortiGuard outbreak alert rules are similar to security posture tagging rules in that you can use the tags to dynamically group endpoints, and the FortiOS administrator can also use the dynamic endpoint groups to build dynamic policy rules. See FortiOS dynamic policies using EMS dynamic tags on page 421.

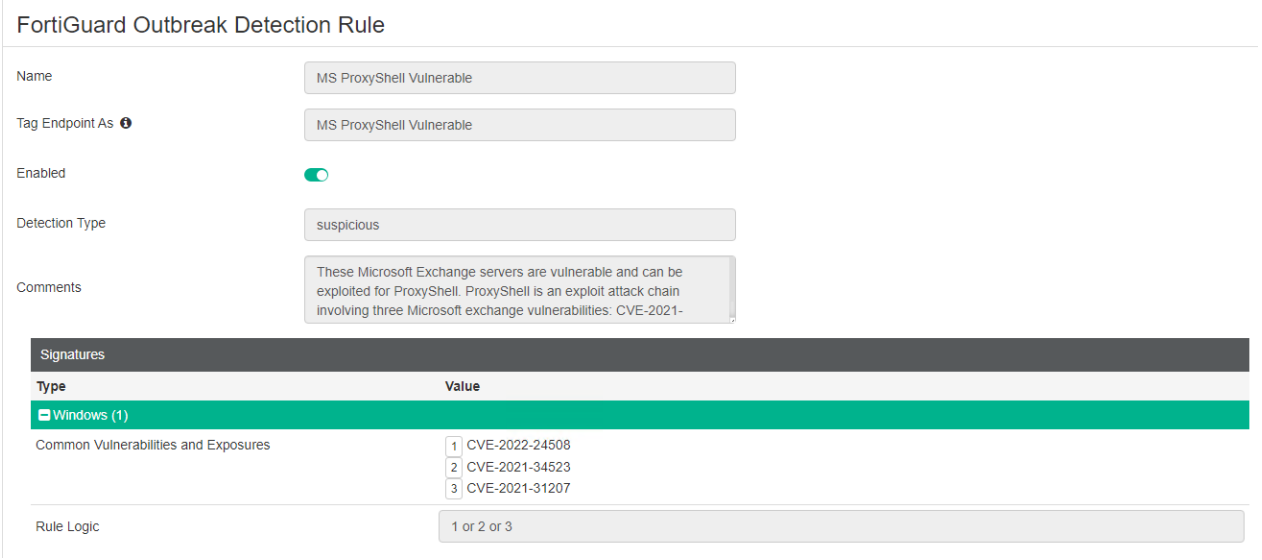
Unlike security posture tagging rules, you cannot modify or delete FortiGuard outbreak alert rules. You can only enable or disable them from the *FortiGuard Outbreak Alert Rules* pane.



You can also view a rule to see its details. In this example, the endpoint only needs to satisfy one of the three criteria to be eligible for the rule. If EMS does not display the *Rule Logic* field, the default rule logic is an "or" relationship.



EMS also receives FortiGuard outbreak alert rules that detect common vulnerabilities and exposures on endpoints. These rules include a description of the vulnerabilities:



You can enable a maximum of ten rule sets.

Software Inventory

You can centrally view a list of software installed on all endpoints. The list includes details for each application such as vendor and version information. You can view this information by application or vendor on the *Applications* pane or by host on the *Hosts* pane. FortiClient sends installed application information to FortiEndpoint.

EMS sends software inventory logs to FortiAnalyzer for real-time and historic logging and reporting. FortiClient sends the software inventory information to EMS when it first registers to EMS. If software changes occur on the endpoint, such as installing new software, updating existing software, or removing existing software, FortiClient sends an updated inventory to EMS and EMS sends the changes to FortiAnalyzer. See System Settings on page 378.

Applications

The FortiEndpoint administrator can view installed application information for all managed endpoints on the *Applications* pane.

To view the Applications content pane:

You can view information about installed applications on the *Applications* content pane.

1. Go to *Software Inventory* > *Applications*. The list of applications, a quick status bar, and a toolbar display in the content pane.

Total Applications	Number of applications that have been installed on all managed endpoints. Click to display the list of installed applications.
Total Vendors	Number of vendors whose applications have been installed on managed endpoints. Click to display the list of installed applications sorted by vendor.
New Detections	Number of applications that have been detected as newly installed since the last Telemetry communication. Click to display newly detected applications sorted by date detected.
PUAs	Number of applications that EMS detects as potentially unwanted applications (PUA) based on the PUA signatures that it receives from FortiGuard. Click to display PUAs.
Display by	Select to toggle between the following options: • Display applications alphabetically by application name. • Sort applications by vendor name.
Refresh	Click to refresh the list of applications in the content pane.
Clear Filters	Click to clear all filters applied to the list of files.
Name	Name of the installed application.

Vendor	Name of the installed application's vendor.
Version	Version number of the installed application.
First Detected	Date the application was first detected as installed on the endpoint.
Last Installed	Date the application was last installed on an endpoint.
Install Count	Number of endpoints the application is installed on.
PUA Category	If EMS detects the application as a PUA, this column displays the PUA category that the application belongs to. Otherwise, this column dislays N/A. PUA categories are as follows: • Illegal or unethical • Cryptomining • Hacking • Unpopular • Phishing • Malicious

To filter applications:

You can filter the list of applications displayed on the *Applications* content pane.

1. Go to *Software Inventory* > *Applications*. The list of applications displays.
2. You can apply filters by application name, vendor name, and version number. Click the filter icon beside the desired heading. Enter the value to include in the filter. You can toggle the *All/Any/Not* button for the following options:
   - *All:* Display all files that match the set filter.
   - *Any:* Display any file that matches the set filter.
   - *Not:* Display only files that do not match the set filter.
3. To remove a filter, click the *X* icon beside the filter. To remove all filters, click the *Clear Filters* icon on the toolbar.

You can export software inventory information from EMS as a CSV file. You can use this data for compliance, software auditing, and so on.

To export software inventory information:

1. In EMS, go to *Software Inventory* > *Applications*.
2. In the top right corner, click *Export CSV*.
3. For *Export mode*, select one of the following:

Mode	Description
Processed	Exports a CSV file for each selected operating system. All CSV files are compressed into a single ZIP file. The CSV files include `name`, `vendor`, `pua_category_name`, and `install_count` information for applications.

Mode	Description
Raw	Exports one CSV file for all operating systems. The CSV file includes `host`, `os_type`, `username`, `name`, `vendor`, `version`, `install_date`, and `install_dir` application information for each host.

4. If you selected *Processed* for *Export mode*, select the desired operating systems for which to export software inventory information.
5. Click *Export*. This downloads a file to the device which contains endpoint information in .csv format. The following shows an example of a processed file:

```
name,vendor,pua_category_name,install_count

"""Microsoft Edge""","""Microsoft Corporation""","""""","""4"""

"""ms-resource:AppxManifest_DisplayName""","""Microsoft Corporation""","""""","""4"""

"""Windows Shell Experience""","""Microsoft Corporation""","""""","""4"""

"""Microsoft Visual C++ 2015 UWP Runtime Package""","""Microsoft Platform
Extensions""","""""","""4"""

"""WindowsAppRuntime.1.3""","""Microsoft Corporation""","""""","""3"""

"""Microsoft Edge Update""","""""","""""","""2"""

"""Work or school account""","""Assigned by your organization""","""""","""2"""

"""Your account""","""Email, phone, or Skype""","""""","""2"""

"""FortiClient""","""Fortinet Technologies Inc""","""""","""2"""

"""Google Chrome""","""Google LLC""","""""","""2"""

"""Narrator""","""Microsoft""","""""","""2"""

"""NcsiUwpApp""","""Microsoft""","""""","""2"""

"""Add Folder Suggestions dialog""","""Microsoft Corporation""","""""","""2"""

"""App Installer""","""Microsoft Corporation""","""""","""2"""

"""Assigned Access Lock app""","""Microsoft Corporation""","""""","""2"""

"""AsyncTextService""","""Microsoft Corporation""","""""","""2"""

"""Captive Portal Flow""","""Microsoft Corporation""","""""","""2"""

"""CapturePicker""","""Microsoft Corporation""","""""","""2"""
```

```
"""Cortana""","""Microsoft Corporation""","""""","""2"""

"""Credential Dialog""","""Microsoft Corporation""","""""","""2"""

"""Email and accounts""","""Microsoft Corporation""","""""","""2"""

"""Eye Control""","""Microsoft Corporation""","""""","""2"""

"""Feedback Hub""","""Microsoft Corporation""","""""","""2"""

"""Get Help""","""Microsoft Corporation""","""""","""2"""

"""HEIF Image Extensions""","""Microsoft Corporation""","""""","""2"""

"""Microsoft .Net Native Framework Package 1.7""","""Microsoft
Corporation""","""""","""2"""

"""Microsoft .Net Native Framework Package 2.2""","""Microsoft
Corporation""","""""","""2"""

"""Microsoft .Net Native Runtime Package 1.7""","""Microsoft
Corporation""","""""","""2"""

"""Microsoft .Net Native Runtime Package 2.2""","""Microsoft
Corporation""","""""","""2"""

"""Microsoft 365 (Office)""","""Microsoft Corporation""","""""","""2"""

"""Microsoft Content""","""Microsoft Corporation""","""""","""2"""

"""Microsoft Edge DevTools Client""","""Microsoft Corporation""","""""","""2"""

"""Microsoft Edge WebView2 Runtime""","""Microsoft Corporation""","""""","""2"""

"""Microsoft family features""","""Microsoft Corporation""","""""","""2"""

"""Microsoft Pay""","""Microsoft Corporation""","""""","""2"""

"""Microsoft People""","""Microsoft Corporation""","""""","""2"""

"""Microsoft Photos""","""Microsoft Corporation""","""""","""2"""

"""Microsoft Sticky Notes""","""Microsoft Corporation""","""""","""2"""

"""Microsoft Store""","""Microsoft Corporation""","""""","""2"""

"""Microsoft Tips""","""Microsoft Corporation""","""""","""2"""
```

```
"""Microsoft Update Health Tools""","""Microsoft Corporation""","""""","""2"""

"""Movies & TV""","""Microsoft Corporation""","""""","""2"""

"""MSN Weather""","""Microsoft Corporation""","""""","""2"""

"""ms-resource://microsoft.windowscommunicationsapps/hxoutlookintl/AppManifest_
OutlookDesktop_DisplayName""","""Microsoft Corporation""","""""","""2"""

"""ms-resource:Common.View.UWP/Resources/StoreAppName""","""Microsoft
Corporation""","""""","""2"""

"""ms-resource:LensSDK/Resources/AppStoreName""","""Microsoft
Corporation""","""""","""2"""

"""ms-resource:XboxApp.Resource/Resources/App_Title""","""Microsoft
Corporation""","""""","""2"""

"""Network Connection Flow""","""Microsoft Corporation""","""""","""2"""

"""OneNote for Windows 10""","""Microsoft Corporation""","""""","""2"""

"""Paint 3D""","""Microsoft Corporation""","""""","""2"""

"""Phone Link""","""Microsoft Corporation""","""""","""2"""

"""PinningConfirmationDialog""","""Microsoft Corporation""","""""","""2"""

"""Snip & Sketch""","""Microsoft Corporation""","""""","""2"""

"""Store Experience Host""","""Microsoft Corporation""","""""","""2"""

"""Take a Test""","""Microsoft Corporation""","""""","""2"""

"""UDK Package""","""Microsoft Corporation""","""""","""2"""

"""VP9 Video Extensions""","""Microsoft Corporation""","""""","""2"""

"""Web Media Extensions""","""Microsoft Corporation""","""""","""2"""

"""Webp Image Extensions""","""Microsoft Corporation""","""""","""2"""

"""Windows Barcode Preview""","""Microsoft Corporation""","""""","""2"""

"""Windows Calculator""","""Microsoft Corporation""","""""","""2"""

"""Windows Clock""","""Microsoft Corporation""","""""","""2"""
```

```
"""Windows Default Lock Screen""","""Microsoft Corporation""","""""","""2"""

"""Windows Defender SmartScreen""","""Microsoft Corporation""","""""","""2"""

"""Windows Hello Setup""","""Microsoft Corporation""","""""","""2"""

"""Windows Maps""","""Microsoft Corporation""","""""","""2"""

"""Windows Media Player""","""Microsoft Corporation""","""""","""2"""

"""Windows Print""","""Microsoft Corporation""","""""","""2"""

"""Windows Search""","""Microsoft Corporation""","""""","""2"""

"""Windows Security""","""Microsoft Corporation""","""""","""2"""

"""Windows Voice Recorder""","""Microsoft Corporation""","""""","""2"""

"""WindowsAppRuntime.1.2""","""Microsoft Corporation""","""""","""2"""

"""Xbox Game Bar""","""Microsoft Corporation""","""""","""2"""

"""Xbox Game Bar Plugin""","""Microsoft Corporation""","""""","""2"""

"""Xbox Game Speech Window""","""Microsoft Corporation""","""""","""2"""

"""Xbox Game UI""","""Microsoft Corporation""","""""","""2"""

"""Xbox Identity Provider""","""Microsoft Corporation""","""""","""2"""

"""Xbox TCUI""","""Microsoft Corporation""","""""","""2"""

"""Microsoft Visual C++ 2015 UWP Desktop Runtime Package""","""Microsoft Platform
Extensions""","""""","""2"""

"""Microsoft.UI.Xaml.2.0""","""Microsoft Platform Extensions""","""""","""2"""

"""Microsoft.UI.Xaml.2.1""","""Microsoft Platform Extensions""","""""","""2"""

"""Microsoft.UI.Xaml.2.3""","""Microsoft Platform Extensions""","""""","""2"""

"""Microsoft.UI.Xaml.2.4""","""Microsoft Platform Extensions""","""""","""2"""

"""Microsoft.UI.Xaml.2.7""","""Microsoft Platform Extensions""","""""","""2"""

"""Microsoft.UI.Xaml.2.8""","""Microsoft Platform Extensions""","""""","""2"""
```

```
"""Solitaire & Casual Games""","""Microsoft Studios""","""""","""2"""

"""Windows Feature Experience Pack""","""Microsoft Windows""","""""","""2"""

"""ms-resource:AppDisplayName""","""ms-resource:PublisherDisplayName""","""""","""2"""

"""ms-resource:DisplayName""","""ms-resource:PublisherDisplayName""","""""","""2"""

"""ms-resource:StartMenuExperienceHost/PkgDisplayName""","""ms-
resource:StartMenuExperienceHost/PublisherDisplayName""","""""","""2"""

"""Skype""","""Skype""","""""","""2"""

"""FortiClient EMS AD Connector""","""Fortinet Technologies Inc""","""""","""1"""

"""Kits Configuration Installer""","""Microsoft""","""""","""1"""

"""Mixed Reality Portal""","""Microsoft Corporation""","""""","""1"""

"""SDK Debuggers""","""Microsoft Corporation""","""""","""1"""

"""Update for Windows 10 (KB5001716)""","""Microsoft Corporation""","""""","""1"""

"""Update for Windows 10 for x64-based Systems (KB5001716)""","""Microsoft
Corporation""","""""","""1"""

"""Windows Software Development Kit - Windows 10.0.19041.685""","""Microsoft
Corporation""","""""","""1"""

"""Windows SDK EULA""","""Microsoft Corporations""","""""","""1"""

"""Spotify Music""","""Spotify AB""","""""","""1"""
```

The following shows an example of a raw file:

```
host,os_type,username,name,vendor,version,install_date,install_dir

"""Bilbo""","""WIN64""","""test""","""Add Folder Suggestions dialog""","""Microsoft
Corporation""","""10.0.19041.1023""","""2021-08-
06""","""C:\Windows\SystemApps\Microsoft.Windows.AddSuggestedFoldersToLibraryDialog_
cw5n1h2txyewy"""

"""Bilbo""","""WIN64""","""test""","""App Installer""","""Microsoft
Corporation""","""1.19.11071.0""","""2023-06-12""","""C:\Program
Files\WindowsApps\Microsoft.DesktopAppInstaller_1.19.11071.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Assigned Access Lock app""","""Microsoft
Corporation""","""1000.19041.1023.0""","""2021-08-
```

```
06""","""C:\Windows\SystemApps\Microsoft.Windows.AssignedAccessLockApp_cw5n1h2txyewy"""

"""Bilbo""","""WIN64""","""test""","""AsyncTextService""","""Microsoft
Corporation""","""10.0.19041.1023""","""2021-08-
06""","""C:\Windows\SystemApps\Microsoft.AsyncTextService_8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Captive Portal Flow""","""Microsoft
Corporation""","""10.0.19041.1023""","""2021-08-
06""","""C:\Windows\SystemApps\Microsoft.Windows.OOBENetworkCaptivePortal_
cw5n1h2txyewy"""

"""Bilbo""","""WIN64""","""test""","""CapturePicker""","""Microsoft
Corporation""","""10.0.19041.1023""","""2021-08-
06""","""C:\Windows\SystemApps\Microsoft.Windows.CapturePicker_cw5n1h2txyewy"""

"""Bilbo""","""WIN64""","""test""","""Cortana""","""Microsoft
Corporation""","""4.2204.13303.0""","""2023-06-12""","""C:\Program
Files\WindowsApps\Microsoft.549981C3F5F10_4.2204.13303.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Credential Dialog""","""Microsoft
Corporation""","""10.0.19041.1023""","""2021-08-
06""","""C:\Windows\SystemApps\microsoft.creddialoghost_cw5n1h2txyewy"""

"""Bilbo""","""WIN64""","""test""","""Email and accounts""","""Microsoft
Corporation""","""10.0.19041.1023""","""2021-08-
06""","""C:\Windows\SystemApps\Microsoft.AccountsControl_cw5n1h2txyewy"""

"""Bilbo""","""WIN64""","""test""","""Eye Control""","""Microsoft
Corporation""","""10.0.19041.1023""","""2021-08-
06""","""C:\Windows\SystemApps\Microsoft.ECApp_8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Feedback Hub""","""Microsoft
Corporation""","""1.2304.1243.0""","""2023-06-12""","""C:\Program
Files\WindowsApps\Microsoft.WindowsFeedbackHub_1.2304.1243.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""FortiClient EMS AD Connector""","""Fortinet
Technologies Inc""","""7.33.793.0""","""2023-06-12""","""C:\Program
Files\Fortinet\FortiClientEMSADConnector\"""

"""Bilbo""","""WIN64""","""test""","""FortiClient""","""Fortinet Technologies
Inc""","""7.2.1.0779""","""2023-06-12""","""C:\Program Files\Fortinet\FortiClient\"""

"""Bilbo""","""WIN64""","""test""","""Get Help""","""Microsoft
Corporation""","""10.2303.10961.0""","""2023-06-12""","""C:\Program
Files\WindowsApps\Microsoft.GetHelp_10.2303.10961.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Google Chrome""","""Google
LLC""","""114.0.5735.198""","""2023-06-26""","""C:\Program
```

```
Files\Google\Chrome\Application"""

"""Bilbo""","""WIN64""","""test""","""HEIF Image Extensions""","""Microsoft
Corporation""","""1.0.61171.0""","""2023-06-12""","""C:\Program
Files\WindowsApps\Microsoft.HEIFImageExtension_1.0.61171.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Kits Configuration
Installer""","""Microsoft""","""10.1.19041.685""","""2021-08-06""","""""""

"""Bilbo""","""WIN64""","""test""","""MSN Weather""","""Microsoft
Corporation""","""4.53.51461.0""","""2023-06-12""","""C:\Program
Files\WindowsApps\Microsoft.BingWeather_4.53.51461.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Microsoft .Net Native Framework Package
1.7""","""Microsoft Corporation""","""1.7.27413.0""","""2021-08-06""","""C:\Program
Files\WindowsApps\Microsoft.NET.Native.Framework.1.7_1.7.27413.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Microsoft .Net Native Framework Package
2.2""","""Microsoft Corporation""","""2.2.29512.0""","""2021-06-04""","""C:\Program
Files\WindowsApps\Microsoft.NET.Native.Framework.2.2_2.2.29512.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Microsoft .Net Native Runtime Package
1.7""","""Microsoft Corporation""","""1.7.27422.0""","""2021-08-06""","""C:\Program
Files\WindowsApps\Microsoft.NET.Native.Runtime.1.7_1.7.27422.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Microsoft .Net Native Runtime Package
2.2""","""Microsoft Corporation""","""2.2.28604.0""","""2021-06-04""","""C:\Program
Files\WindowsApps\Microsoft.NET.Native.Runtime.2.2_2.2.28604.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Microsoft 365 (Office)""","""Microsoft
Corporation""","""18.2305.1222.0""","""2023-06-12""","""C:\Program
Files\WindowsApps\Microsoft.MicrosoftOfficeHub_18.2305.1222.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Microsoft Content""","""Microsoft
Corporation""","""10.0.19041.1023""","""2021-08-
06""","""C:\Windows\SystemApps\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy"""

"""Bilbo""","""WIN64""","""test""","""Microsoft Edge DevTools Client""","""Microsoft
Corporation""","""1000.19041.1023.0""","""2021-08-
06""","""C:\Windows\SystemApps\Microsoft.MicrosoftEdgeDevToolsClient_8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Microsoft Edge
Update""","""""""","""1.3.175.29""",NULL,"""""""

"""Bilbo""","""WIN64""","""test""","""Microsoft Edge WebView2 Runtime""","""Microsoft
Corporation""","""114.0.1823.58""","""2023-06-26""","""C:\Program Files
(x86)\Microsoft\EdgeWebView\Application"""
```

```
"""Bilbo""","""WIN64""","""test""","""Microsoft Edge""","""Microsoft
Corporation""","""114.0.1823.58""","""2023-06-26""","""C:\Program
Files\WindowsApps\Microsoft.MicrosoftEdge.Stable_114.0.1823.58_neutral__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Microsoft Edge""","""Microsoft
Corporation""","""44.19041.1266.0""","""2022-03-
02""","""C:\Windows\SystemApps\Microsoft.MicrosoftEdge_8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Microsoft Pay""","""Microsoft
Corporation""","""2.4.18324.0""","""2019-12-07""","""C:\Program
Files\WindowsApps\Microsoft.Wallet_2.4.18324.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Microsoft People""","""Microsoft
Corporation""","""10.2202.31.0""","""2023-06-12""","""C:\Program
Files\WindowsApps\Microsoft.People_10.2202.31.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Microsoft Photos""","""Microsoft
Corporation""","""2023.10030.27002.0""","""2023-06-12""","""C:\Program
Files\WindowsApps\Microsoft.Windows.Photos_2023.10030.27002.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Microsoft Sticky Notes""","""Microsoft
Corporation""","""4.6.0.0""","""2023-06-12""","""C:\Program
Files\WindowsApps\Microsoft.MicrosoftStickyNotes_4.6.0.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Microsoft Store""","""Microsoft
Corporation""","""22305.1401.1.0""","""2023-06-23""","""C:\Program
Files\WindowsApps\Microsoft.WindowsStore_22305.1401.1.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Microsoft Tips""","""Microsoft
Corporation""","""10.2303.3.0""","""2023-06-12""","""C:\Program
Files\WindowsApps\Microsoft.Getstarted_10.2303.3.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Microsoft Update Health Tools""","""Microsoft
Corporation""","""3.72.0.0""","""2023-06-13""","""""""

"""Bilbo""","""WIN64""","""test""","""Microsoft Visual C++ 2015 UWP Desktop Runtime
Package""","""Microsoft Platform Extensions""","""14.0.32530.0""","""2023-06-
12""","""C:\Program Files\WindowsApps\Microsoft.VCLibs.140.00.UWPDesktop_14.0.32530.0_
x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Microsoft Visual C++ 2015 UWP Runtime
Package""","""Microsoft Platform Extensions""","""14.0.30035.0""","""2021-08-
06""","""C:\Program Files\WindowsApps\Microsoft.VCLibs.140.00_14.0.30035.0_x64__
8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Microsoft Visual C++ 2015 UWP Runtime
Package""","""Microsoft Platform Extensions""","""14.0.30704.0""","""2022-03-
02""","""C:\Program Files\WindowsApps\Microsoft.VCLibs.140.00_14.0.30704.0_x64__
```

```
8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Microsoft Visual C++ 2015 UWP Runtime
Package""","""Microsoft Platform Extensions""","""14.0.32530.0""","""2023-06-
12""","""C:\Program Files\WindowsApps\Microsoft.VCLibs.140.00_14.0.32530.0_x64__
8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Microsoft family features""","""Microsoft
Corporation""","""1000.19041.1023.0""","""2021-08-
06""","""C:\Windows\SystemApps\ParentalControls_cw5n1h2txyewy"""

"""Bilbo""","""WIN64""","""test""","""Microsoft.UI.Xaml.2.0""","""Microsoft Platform
Extensions""","""2.1810.18004.0""","""2019-12-07""","""C:\Program
Files\WindowsApps\Microsoft.UI.Xaml.2.0_2.1810.18004.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Microsoft.UI.Xaml.2.1""","""Microsoft Platform
Extensions""","""2.11906.6001.0""","""2021-08-06""","""C:\Program
Files\WindowsApps\Microsoft.UI.Xaml.2.1_2.11906.6001.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Microsoft.UI.Xaml.2.3""","""Microsoft Platform
Extensions""","""2.32002.13001.0""","""2021-08-06""","""C:\Program
Files\WindowsApps\Microsoft.UI.Xaml.2.3_2.32002.13001.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Microsoft.UI.Xaml.2.4""","""Microsoft Platform
Extensions""","""2.42007.9001.0""","""2021-07-08""","""C:\Program
Files\WindowsApps\Microsoft.UI.Xaml.2.4_2.42007.9001.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Microsoft.UI.Xaml.2.7""","""Microsoft Platform
Extensions""","""7.2208.15002.0""","""2023-04-27""","""C:\Program
Files\WindowsApps\Microsoft.UI.Xaml.2.7_7.2208.15002.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Microsoft.UI.Xaml.2.8""","""Microsoft Platform
Extensions""","""8.2305.5001.0""","""2023-06-12""","""C:\Program
Files\WindowsApps\Microsoft.UI.Xaml.2.8_8.2305.5001.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Mixed Reality Portal""","""Microsoft
Corporation""","""2000.21051.1282.0""","""2021-08-06""","""C:\Program
Files\WindowsApps\Microsoft.MixedReality.Portal_2000.21051.1282.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Movies & TV""","""Microsoft
Corporation""","""10.22091.10041.0""","""2023-06-12""","""C:\Program
Files\WindowsApps\Microsoft.ZuneVideo_10.22091.10041.0_x64__8wekyb3d8bbwe"""


"""Bilbo""","""WIN64""","""test""","""Narrator""","""Microsoft""","""10.0.19041.1023""","
""2021-08-06""","""C:\Windows\SystemApps\microsoft.windows.narratorquickstart_
8wekyb3d8bbwe"""
```

```
"""Bilbo""","""WIN64""","""test""","""NcsiUwpApp""","""Microsoft""","""1000.19041.1023.0"
"","""2021-08-06""","""C:\Windows\SystemApps\NcsiUwpApp_8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Network Connection Flow""","""Microsoft
Corporation""","""10.0.19041.1023""","""2021-08-
06""","""C:\Windows\SystemApps\Microsoft.Windows.OOBENetworkConnectionFlow_
cw5n1h2txyewy"""

"""Bilbo""","""WIN64""","""test""","""OneNote for Windows 10""","""Microsoft
Corporation""","""16001.14326.21452.0""","""2023-06-21""","""C:\Program
Files\WindowsApps\Microsoft.Office.OneNote_16001.14326.21452.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Paint 3D""","""Microsoft
Corporation""","""6.2203.1037.0""","""2022-04-27""","""C:\Program
Files\WindowsApps\Microsoft.MSPaint_6.2203.1037.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Phone Link""","""Microsoft
Corporation""","""1.23052.121.0""","""2023-06-27""","""C:\Program
Files\WindowsApps\Microsoft.YourPhone_1.23052.121.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""PinningConfirmationDialog""","""Microsoft
Corporation""","""1000.19041.1023.0""","""2021-08-
06""","""C:\Windows\SystemApps\Microsoft.Windows.PinningConfirmationDialog_
cw5n1h2txyewy"""

"""Bilbo""","""WIN64""","""test""","""SDK Debuggers""","""Microsoft
Corporation""","""10.1.19041.685""","""2021-08-06""","""""""

"""Bilbo""","""WIN64""","""test""","""Skype""","""Skype""","""15.99.3202.0""","""2023-06-
23""","""C:\Program Files\WindowsApps\Microsoft.SkypeApp_15.99.3202.0_x64__
kzf8qxf38zg5c"""

"""Bilbo""","""WIN64""","""test""","""Snip & Sketch""","""Microsoft
Corporation""","""10.2008.3001.0""","""2023-06-12""","""C:\Program
Files\WindowsApps\Microsoft.ScreenSketch_10.2008.3001.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Solitaire & Casual Games""","""Microsoft
Studios""","""4.16.3140.0""","""2023-06-12""","""C:\Program
Files\WindowsApps\Microsoft.MicrosoftSolitaireCollection_4.16.3140.0_x64__
8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Spotify Music""","""Spotify
AB""","""1.214.1149.0""","""2023-06-23""","""C:\Program
Files\WindowsApps\SpotifyAB.SpotifyMusic_1.214.1149.0_x86__zpdnekdrzrea0"""

"""Bilbo""","""WIN64""","""test""","""Store Experience Host""","""Microsoft
Corporation""","""22305.1401.2.0""","""2023-06-27""","""C:\Program
```

```
Files\WindowsApps\Microsoft.StorePurchaseApp_22305.1401.2.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Take a Test""","""Microsoft
Corporation""","""10.0.19041.2311""","""2023-04-
12""","""C:\Windows\SystemApps\Microsoft.Windows.SecureAssessmentBrowser_cw5n1h2txyewy"""

"""Bilbo""","""WIN64""","""test""","""UDK Package""","""Microsoft
Corporation""","""10.0.19041.1023""","""2021-08-
06""","""C:\Windows\SystemApps\MicrosoftWindows.UndockedDevKit_cw5n1h2txyewy"""

"""Bilbo""","""WIN64""","""test""","""Update for Windows 10 for x64-based Systems
(KB5001716)""","""Microsoft Corporation""","""8.91.0.0""","""2023-04-12""","""""""

"""Bilbo""","""WIN64""","""test""","""VP9 Video Extensions""","""Microsoft
Corporation""","""1.0.52781.0""","""2023-04-27""","""C:\Program
Files\WindowsApps\Microsoft.VP9VideoExtensions_1.0.52781.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Web Media Extensions""","""Microsoft
Corporation""","""1.0.61591.0""","""2023-06-26""","""C:\Program
Files\WindowsApps\Microsoft.WebMediaExtensions_1.0.61591.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Webp Image Extensions""","""Microsoft
Corporation""","""1.0.52351.0""","""2023-04-27""","""C:\Program
Files\WindowsApps\Microsoft.WebpImageExtension_1.0.52351.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Windows Barcode Preview""","""Microsoft
Corporation""","""10.0.19041.1023""","""2021-08-
06""","""C:\Windows\SystemApps\Windows.CBSPreview_cw5n1h2txyewy"""

"""Bilbo""","""WIN64""","""test""","""Windows Calculator""","""Microsoft
Corporation""","""11.2210.0.0""","""2023-04-27""","""C:\Program
Files\WindowsApps\Microsoft.WindowsCalculator_11.2210.0.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Windows Clock""","""Microsoft
Corporation""","""11.2304.0.0""","""2023-06-21""","""C:\Program
Files\WindowsApps\Microsoft.WindowsAlarms_11.2304.0.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Windows Default Lock Screen""","""Microsoft
Corporation""","""10.0.19041.1023""","""2021-08-
06""","""C:\Windows\SystemApps\Microsoft.LockApp_cw5n1h2txyewy"""

"""Bilbo""","""WIN64""","""test""","""Windows Defender SmartScreen""","""Microsoft
Corporation""","""1000.19041.1023.0""","""2021-08-
06""","""C:\Windows\SystemApps\Microsoft.Windows.AppRep.ChxApp_cw5n1h2txyewy"""

"""Bilbo""","""WIN64""","""test""","""Windows Feature Experience Pack""","""Microsoft
Windows""","""1000.19041.1000.0""","""2023-04-
27""","""C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy"""
```

```
"""Bilbo""","""WIN64""","""test""","""Windows Hello Setup""","""Microsoft
Corporation""","""10.0.19041.1023""","""2021-08-
06""","""C:\Windows\SystemApps\Microsoft.BioEnrollment_cw5n1h2txyewy"""

"""Bilbo""","""WIN64""","""test""","""Windows Maps""","""Microsoft
Corporation""","""11.2303.5.0""","""2023-06-12""","""C:\Program
Files\WindowsApps\Microsoft.WindowsMaps_11.2303.5.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Windows Media Player""","""Microsoft
Corporation""","""11.2304.2.0""","""2023-06-12""","""C:\Program
Files\WindowsApps\Microsoft.ZuneMusic_11.2304.2.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Windows Print""","""Microsoft
Corporation""","""6.2.1.0""","""2021-08-06""","""C:\Windows\PrintDialog"""

"""Bilbo""","""WIN64""","""test""","""Windows SDK EULA""","""Microsoft
Corporations""","""10.1.19041.685""","""2021-08-06""","""""""

"""Bilbo""","""WIN64""","""test""","""Windows Search""","""Microsoft
Corporation""","""1.14.10.19041""","""2023-06-
13""","""C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy"""

"""Bilbo""","""WIN64""","""test""","""Windows Security""","""Microsoft
Corporation""","""10.0.19041.1865""","""2023-04-
12""","""C:\Windows\SystemApps\Microsoft.Windows.SecHealthUI_cw5n1h2txyewy"""

"""Bilbo""","""WIN64""","""test""","""Windows Shell Experience""","""Microsoft
Corporation""","""10.0.19041.1023""","""2021-08-
06""","""C:\Windows\SystemApps\Microsoft.Windows.PeopleExperienceHost_cw5n1h2txyewy"""

"""Bilbo""","""WIN64""","""test""","""Windows Shell Experience""","""Microsoft
Corporation""","""10.0.19041.1949""","""2023-04-
12""","""C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy"""

"""Bilbo""","""WIN64""","""test""","""Windows Software Development Kit - Windows
10.0.19041.685""","""Microsoft Corporation""","""10.1.19041.685""","""2021-08-
06""","""""""

"""Bilbo""","""WIN64""","""test""","""Windows Voice Recorder""","""Microsoft
Corporation""","""10.2103.28.0""","""2021-08-06""","""C:\Program
Files\WindowsApps\Microsoft.WindowsSoundRecorder_10.2103.28.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""WindowsAppRuntime.1.2""","""Microsoft
Corporation""","""2000.802.31.0""","""2023-06-12""","""C:\Program
Files\WindowsApps\Microsoft.WindowsAppRuntime.1.2_2000.802.31.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""WindowsAppRuntime.1.3""","""Microsoft
```

```
Corporation""","""3000.851.1712.0""","""2023-06-12""","""C:\Program
Files\WindowsApps\Microsoft.WindowsAppRuntime.1.3_3000.851.1712.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""WindowsAppRuntime.1.3""","""Microsoft
Corporation""","""3000.882.2207.0""","""2023-06-16""","""C:\Program
Files\WindowsApps\Microsoft.WindowsAppRuntime.1.3_3000.882.2207.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Work or school account""","""Assigned by your
organization""","""1000.19041.1023.0""","""2021-08-
06""","""C:\Windows\SystemApps\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy"""

"""Bilbo""","""WIN64""","""test""","""Xbox Game Bar Plugin""","""Microsoft
Corporation""","""1.54.4001.0""","""2021-06-04""","""C:\Program
Files\WindowsApps\Microsoft.XboxGameOverlay_1.54.4001.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Xbox Game Bar""","""Microsoft
Corporation""","""5.823.3261.0""","""2023-06-12""","""C:\Program
Files\WindowsApps\Microsoft.XboxGamingOverlay_5.823.3261.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Xbox Game Speech Window""","""Microsoft
Corporation""","""1.21.13002.0""","""2021-06-04""","""C:\Program
Files\WindowsApps\Microsoft.XboxSpeechToTextOverlay_1.21.13002.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Xbox Game UI""","""Microsoft
Corporation""","""1000.19041.1023.0""","""2021-08-
06""","""C:\Windows\SystemApps\Microsoft.XboxGameCallableUI_cw5n1h2txyewy"""

"""Bilbo""","""WIN64""","""test""","""Xbox Identity Provider""","""Microsoft
Corporation""","""12.95.3001.0""","""2023-04-27""","""C:\Program
Files\WindowsApps\Microsoft.XboxIdentityProvider_12.95.3001.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Xbox TCUI""","""Microsoft
Corporation""","""1.24.10001.0""","""2021-06-04""","""C:\Program
Files\WindowsApps\Microsoft.Xbox.TCUI_1.24.10001.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""Your account""","""Email, phone, or
Skype""","""10.0.19041.1266""","""2022-03-
02""","""C:\Windows\SystemApps\Microsoft.Windows.CloudExperienceHost_cw5n1h2txyewy"""

"""Bilbo""","""WIN64""","""test""","""ms-
resource://microsoft.windowscommunicationsapps/hxoutlookintl/AppManifest_OutlookDesktop_
DisplayName""","""Microsoft Corporation""","""16005.14326.21490.0""","""2023-06-
27""","""C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_
16005.14326.21490.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""ms-resource:AppDisplayName""","""ms-
resource:PublisherDisplayName""","""1000.19041.1023.0""","""2021-08-
06""","""C:\Windows\SystemApps\Microsoft.Windows.CallingShellApp_cw5n1h2txyewy"""
```

```
"""Bilbo""","""WIN64""","""test""","""ms-resource:AppxManifest_
DisplayName""","""Microsoft Corporation""","""10.0.19041.1023""","""2021-08-
06""","""C:\Windows\SystemApps\Microsoft.Windows.FilePicker_cw5n1h2txyewy"""

"""Bilbo""","""WIN64""","""test""","""ms-resource:AppxManifest_
DisplayName""","""Microsoft Corporation""","""10.0.19041.1949""","""2023-04-
12""","""C:\Windows\SystemApps\Microsoft.Windows.FileExplorer_cw5n1h2txyewy"""

"""Bilbo""","""WIN64""","""test""","""ms-
resource:Common.View.UWP/Resources/StoreAppName""","""Microsoft
Corporation""","""7.2211.24012.0""","""2023-04-27""","""C:\Program
Files\WindowsApps\Microsoft.Microsoft3DViewer_7.2211.24012.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""ms-resource:DisplayName""","""ms-
resource:PublisherDisplayName""","""10.0.19041.1023""","""2021-08-
06""","""C:\Windows\SystemApps\Microsoft.Win32WebViewHost_cw5n1h2txyewy"""

"""Bilbo""","""WIN64""","""test""","""ms-
resource:LensSDK/Resources/AppStoreName""","""Microsoft
Corporation""","""2023.2304.11.0""","""2023-06-12""","""C:\Program
Files\WindowsApps\Microsoft.WindowsCamera_2023.2304.11.0_x64__8wekyb3d8bbwe"""

"""Bilbo""","""WIN64""","""test""","""ms-
resource:StartMenuExperienceHost/PkgDisplayName""","""ms-
resource:StartMenuExperienceHost/PublisherDisplayName""","""10.0.19041.1023""","""2021-
08-06""","""C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_
cw5n1h2txyewy"""

"""Bilbo""","""WIN64""","""test""","""ms-resource:XboxApp.Resource/Resources/App_
Title""","""Microsoft Corporation""","""48.89.25001.0""","""2023-06-12""","""C:\Program
Files\WindowsApps\Microsoft.XboxApp_48.89.25001.0_x64__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Add Folder Suggestions dialog""","""Microsoft
Corporation""","""10.0.19041.1023""","""2021-11-
26""","""C:\Windows\SystemApps\Microsoft.Windows.AddSuggestedFoldersToLibraryDialog_
cw5n1h2txyewy"""

"""Boromir""","""WIN32""","""brando""","""App Installer""","""Microsoft
Corporation""","""1.19.11071.0""","""2023-06-15""","""C:\Program
Files\WindowsApps\Microsoft.DesktopAppInstaller_1.19.11071.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Assigned Access Lock app""","""Microsoft
Corporation""","""1000.19041.1023.0""","""2021-11-
26""","""C:\Windows\SystemApps\Microsoft.Windows.AssignedAccessLockApp_cw5n1h2txyewy"""

"""Boromir""","""WIN32""","""brando""","""AsyncTextService""","""Microsoft
Corporation""","""10.0.19041.1023""","""2021-11-
```

```
26""","""C:\Windows\SystemApps\Microsoft.AsyncTextService_8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Captive Portal Flow""","""Microsoft
Corporation""","""10.0.19041.1023""","""2021-11-
26""","""C:\Windows\SystemApps\Microsoft.Windows.OOBENetworkCaptivePortal_
cw5n1h2txyewy"""

"""Boromir""","""WIN32""","""brando""","""CapturePicker""","""Microsoft
Corporation""","""10.0.19041.1023""","""2021-11-
26""","""C:\Windows\SystemApps\Microsoft.Windows.CapturePicker_cw5n1h2txyewy"""

"""Boromir""","""WIN32""","""brando""","""Cortana""","""Microsoft
Corporation""","""4.2204.13303.0""","""2023-05-09""","""C:\Program
Files\WindowsApps\Microsoft.549981C3F5F10_4.2204.13303.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Credential Dialog""","""Microsoft
Corporation""","""10.0.19041.1023""","""2021-11-
26""","""C:\Windows\SystemApps\microsoft.creddialoghost_cw5n1h2txyewy"""

"""Boromir""","""WIN32""","""brando""","""Email and accounts""","""Microsoft
Corporation""","""10.0.19041.1023""","""2021-11-
26""","""C:\Windows\SystemApps\Microsoft.AccountsControl_cw5n1h2txyewy"""

"""Boromir""","""WIN32""","""brando""","""Eye Control""","""Microsoft
Corporation""","""10.0.19041.1023""","""2021-11-
26""","""C:\Windows\SystemApps\Microsoft.ECApp_8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Feedback Hub""","""Microsoft
Corporation""","""1.2304.1243.0""","""2023-05-09""","""C:\Program
Files\WindowsApps\Microsoft.WindowsFeedbackHub_1.2304.1243.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""FortiClient""","""Fortinet Technologies
Inc""","""7.2.0.0690""","""2023-06-12""","""C:\Program Files\Fortinet\FortiClient\"""

"""Boromir""","""WIN32""","""brando""","""Get Help""","""Microsoft
Corporation""","""10.2303.10961.0""","""2023-05-09""","""C:\Program
Files\WindowsApps\Microsoft.GetHelp_10.2303.10961.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Google Chrome""","""Google
LLC""","""114.0.5735.135""","""2023-06-26""","""C:\Program
Files\Google\Chrome\Application"""

"""Boromir""","""WIN32""","""brando""","""HEIF Image Extensions""","""Microsoft
Corporation""","""1.0.61171.0""","""2023-05-12""","""C:\Program
Files\WindowsApps\Microsoft.HEIFImageExtension_1.0.61171.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""MSN Weather""","""Microsoft
Corporation""","""4.53.51461.0""","""2023-06-15""","""C:\Program
```

```
Files\WindowsApps\Microsoft.BingWeather_4.53.51461.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Microsoft .Net Native Framework Package
1.7""","""Microsoft Corporation""","""1.7.27413.0""","""2021-06-04""","""C:\Program
Files\WindowsApps\Microsoft.NET.Native.Framework.1.7_1.7.27413.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Microsoft .Net Native Framework Package
2.2""","""Microsoft Corporation""","""2.2.29512.0""","""2021-06-04""","""C:\Program
Files\WindowsApps\Microsoft.NET.Native.Framework.2.2_2.2.29512.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Microsoft .Net Native Runtime Package
1.7""","""Microsoft Corporation""","""1.7.27422.0""","""2021-06-04""","""C:\Program
Files\WindowsApps\Microsoft.NET.Native.Runtime.1.7_1.7.27422.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Microsoft .Net Native Runtime Package
2.2""","""Microsoft Corporation""","""2.2.28604.0""","""2021-06-04""","""C:\Program
Files\WindowsApps\Microsoft.NET.Native.Runtime.2.2_2.2.28604.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Microsoft 365 (Office)""","""Microsoft
Corporation""","""18.2305.1222.0""","""2023-06-15""","""C:\Program
Files\WindowsApps\Microsoft.MicrosoftOfficeHub_18.2305.1222.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Microsoft Content""","""Microsoft
Corporation""","""10.0.19041.1023""","""2021-11-
26""","""C:\Windows\SystemApps\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy"""

"""Boromir""","""WIN32""","""brando""","""Microsoft Edge DevTools Client""","""Microsoft
Corporation""","""1000.19041.1023.0""","""2021-11-
26""","""C:\Windows\SystemApps\Microsoft.MicrosoftEdgeDevToolsClient_8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Microsoft Edge
Update""","""""","""1.3.175.29""",NULL,"""""

"""Boromir""","""WIN32""","""brando""","""Microsoft Edge WebView2 Runtime""","""Microsoft
Corporation""","""114.0.1823.58""","""2023-06-26""","""C:\Program
Files\Microsoft\EdgeWebView\Application"""

"""Boromir""","""WIN32""","""brando""","""Microsoft Edge""","""Microsoft
Corporation""","""114.0.1823.58""","""2023-06-26""","""C:\Program
Files\WindowsApps\Microsoft.MicrosoftEdge.Stable_114.0.1823.58_neutral__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Microsoft Edge""","""Microsoft
Corporation""","""44.19041.1266.0""","""2022-03-
02""","""C:\Windows\SystemApps\Microsoft.MicrosoftEdge_8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Microsoft Pay""","""Microsoft
Corporation""","""2.4.18324.0""","""2019-12-07""","""C:\Program
Files\WindowsApps\Microsoft.Wallet_2.4.18324.0_x86__8wekyb3d8bbwe"""
```

```
"""Boromir""","""WIN32""","""brando""","""Microsoft People""","""Microsoft
Corporation""","""10.2202.31.0""","""2023-06-15""","""C:\Program
Files\WindowsApps\Microsoft.People_10.2202.31.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Microsoft Photos""","""Microsoft
Corporation""","""2023.10030.27002.0""","""2023-05-09""","""C:\Program
Files\WindowsApps\Microsoft.Windows.Photos_2023.10030.27002.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Microsoft Sticky Notes""","""Microsoft
Corporation""","""4.6.0.0""","""2023-05-09""","""C:\Program
Files\WindowsApps\Microsoft.MicrosoftStickyNotes_4.6.0.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Microsoft Store""","""Microsoft
Corporation""","""22305.1401.1.0""","""2023-06-23""","""C:\Program
Files\WindowsApps\Microsoft.WindowsStore_22305.1401.1.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Microsoft Tips""","""Microsoft
Corporation""","""10.2303.3.0""","""2023-05-09""","""C:\Program
Files\WindowsApps\Microsoft.Getstarted_10.2303.3.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Microsoft Update Health Tools""","""Microsoft
Corporation""","""3.72.0.0""","""2023-05-10""","""""""

"""Boromir""","""WIN32""","""brando""","""Microsoft Visual C++ 2015 UWP Desktop Runtime
Package""","""Microsoft Platform Extensions""","""14.0.32530.0""","""2023-06-
15""","""C:\Program Files\WindowsApps\Microsoft.VCLibs.140.00.UWPDesktop_14.0.32530.0_
x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Microsoft Visual C++ 2015 UWP Runtime
Package""","""Microsoft Platform Extensions""","""14.0.32530.0""","""2023-06-
15""","""C:\Program Files\WindowsApps\Microsoft.VCLibs.140.00_14.0.32530.0_x86__
8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Microsoft family features""","""Microsoft
Corporation""","""1000.19041.1023.0""","""2021-11-
26""","""C:\Windows\SystemApps\ParentalControls_cw5n1h2txyewy"""

"""Boromir""","""WIN32""","""brando""","""Microsoft.UI.Xaml.2.0""","""Microsoft Platform
Extensions""","""2.1810.18004.0""","""2019-12-07""","""C:\Program
Files\WindowsApps\Microsoft.UI.Xaml.2.0_2.1810.18004.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Microsoft.UI.Xaml.2.1""","""Microsoft Platform
Extensions""","""2.11906.6001.0""","""2021-06-04""","""C:\Program
Files\WindowsApps\Microsoft.UI.Xaml.2.1_2.11906.6001.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Microsoft.UI.Xaml.2.3""","""Microsoft Platform
Extensions""","""2.32002.13001.0""","""2021-09-23""","""C:\Program
```

```
Files\WindowsApps\Microsoft.UI.Xaml.2.3_2.32002.13001.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Microsoft.UI.Xaml.2.4""","""Microsoft Platform
Extensions""","""2.42007.9001.0""","""2021-06-04""","""C:\Program
Files\WindowsApps\Microsoft.UI.Xaml.2.4_2.42007.9001.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Microsoft.UI.Xaml.2.7""","""Microsoft Platform
Extensions""","""7.2208.15002.0""","""2023-05-09""","""C:\Program
Files\WindowsApps\Microsoft.UI.Xaml.2.7_7.2208.15002.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Microsoft.UI.Xaml.2.8""","""Microsoft Platform
Extensions""","""8.2305.5001.0""","""2023-05-09""","""C:\Program
Files\WindowsApps\Microsoft.UI.Xaml.2.8_8.2305.5001.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Movies & TV""","""Microsoft
Corporation""","""10.22091.10041.0""","""2023-05-09""","""C:\Program
Files\WindowsApps\Microsoft.ZuneVideo_10.22091.10041.0_x86__8wekyb3d8bbwe"""


"""Boromir""","""WIN32""","""brando""","""Narrator""","""Microsoft""","""10.0.19041.1023"
"","""2021-11-26""","""C:\Windows\SystemApps\microsoft.windows.narratorquickstart_
8wekyb3d8bbwe"""


"""Boromir""","""WIN32""","""brando""","""NcsiUwpApp""","""Microsoft""","""1000.19041.102
3.0""","""2021-11-26""","""C:\Windows\SystemApps\NcsiUwpApp_8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Network Connection Flow""","""Microsoft
Corporation""","""10.0.19041.1023""","""2021-11-
26""","""C:\Windows\SystemApps\Microsoft.Windows.OOBENetworkConnectionFlow_
cw5n1h2txyewy"""

"""Boromir""","""WIN32""","""brando""","""OneNote for Windows 10""","""Microsoft
Corporation""","""16001.14326.21452.0""","""2023-06-21""","""C:\Program
Files\WindowsApps\Microsoft.Office.OneNote_16001.14326.21452.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Paint 3D""","""Microsoft
Corporation""","""6.2305.16087.0""","""2023-06-23""","""C:\Program
Files\WindowsApps\Microsoft.MSPaint_6.2305.16087.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Phone Link""","""Microsoft
Corporation""","""1.23052.121.0""","""2023-06-27""","""C:\Program
Files\WindowsApps\Microsoft.YourPhone_1.23052.121.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""PinningConfirmationDialog""","""Microsoft
Corporation""","""1000.19041.1023.0""","""2021-11-
26""","""C:\Windows\SystemApps\Microsoft.Windows.PinningConfirmationDialog_
cw5n1h2txyewy"""
```

```
"""Boromir""","""WIN32""","""brando""","""Skype""","""Skype""","""15.99.3202.0""","""202
3-06-26""","""C:\Program Files\WindowsApps\Microsoft.SkypeApp_15.99.3202.0_x86__
kzf8qxf38zg5c"""

"""Boromir""","""WIN32""","""brando""","""Snip & Sketch""","""Microsoft
Corporation""","""10.2008.3001.0""","""2023-05-09""","""C:\Program
Files\WindowsApps\Microsoft.ScreenSketch_10.2008.3001.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Solitaire & Casual Games""","""Microsoft
Studios""","""4.16.3140.0""","""2023-05-09""","""C:\Program
Files\WindowsApps\Microsoft.MicrosoftSolitaireCollection_4.16.3140.0_x86__
8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Store Experience Host""","""Microsoft
Corporation""","""12303.1401.1.0""","""2023-06-19""","""C:\Program
Files\WindowsApps\Microsoft.StorePurchaseApp_12303.1401.1.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Take a Test""","""Microsoft
Corporation""","""10.0.19041.2311""","""2023-05-
10""","""C:\Windows\SystemApps\Microsoft.Windows.SecureAssessmentBrowser_cw5n1h2txyewy"""

"""Boromir""","""WIN32""","""brando""","""UDK Package""","""Microsoft
Corporation""","""10.0.19041.1023""","""2021-11-
26""","""C:\Windows\SystemApps\MicrosoftWindows.UndockedDevKit_cw5n1h2txyewy"""

"""Boromir""","""WIN32""","""brando""","""Update for Windows 10
(KB5001716)""","""Microsoft Corporation""","""8.92.0.0""","""2023-05-24""","""""""

"""Boromir""","""WIN32""","""brando""","""VP9 Video Extensions""","""Microsoft
Corporation""","""1.0.52781.0""","""2023-05-09""","""C:\Program
Files\WindowsApps\Microsoft.VP9VideoExtensions_1.0.52781.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Web Media Extensions""","""Microsoft
Corporation""","""1.0.61591.0""","""2023-06-26""","""C:\Program
Files\WindowsApps\Microsoft.WebMediaExtensions_1.0.61591.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Webp Image Extensions""","""Microsoft
Corporation""","""1.0.52351.0""","""2023-05-09""","""C:\Program
Files\WindowsApps\Microsoft.WebpImageExtension_1.0.52351.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Windows Barcode Preview""","""Microsoft
Corporation""","""10.0.19041.1023""","""2021-11-
26""","""C:\Windows\SystemApps\Windows.CBSPreview_cw5n1h2txyewy"""

"""Boromir""","""WIN32""","""brando""","""Windows Calculator""","""Microsoft
Corporation""","""11.2210.0.0""","""2023-05-09""","""C:\Program
```

```
Files\WindowsApps\Microsoft.WindowsCalculator_11.2210.0.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Windows Clock""","""Microsoft
Corporation""","""11.2304.0.0""","""2023-06-21""","""C:\Program
Files\WindowsApps\Microsoft.WindowsAlarms_11.2304.0.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Windows Default Lock Screen""","""Microsoft
Corporation""","""10.0.19041.1023""","""2021-11-
26""","""C:\Windows\SystemApps\Microsoft.LockApp_cw5n1h2txyewy"""

"""Boromir""","""WIN32""","""brando""","""Windows Defender SmartScreen""","""Microsoft
Corporation""","""1000.19041.1023.0""","""2021-11-
26""","""C:\Windows\SystemApps\Microsoft.Windows.AppRep.ChxApp_cw5n1h2txyewy"""

"""Boromir""","""WIN32""","""brando""","""Windows Feature Experience Pack""","""Microsoft
Windows""","""1000.19041.1000.0""","""2023-05-
12""","""C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy"""

"""Boromir""","""WIN32""","""brando""","""Windows Hello Setup""","""Microsoft
Corporation""","""10.0.19041.1023""","""2021-11-
26""","""C:\Windows\SystemApps\Microsoft.BioEnrollment_cw5n1h2txyewy"""

"""Boromir""","""WIN32""","""brando""","""Windows Maps""","""Microsoft
Corporation""","""11.2303.5.0""","""2023-05-09""","""C:\Program
Files\WindowsApps\Microsoft.WindowsMaps_11.2303.5.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Windows Media Player""","""Microsoft
Corporation""","""11.2304.2.0""","""2023-06-15""","""C:\Program
Files\WindowsApps\Microsoft.ZuneMusic_11.2304.2.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Windows Print""","""Microsoft
Corporation""","""6.2.1.0""","""2021-11-26""","""C:\Windows\PrintDialog"""

"""Boromir""","""WIN32""","""brando""","""Windows Search""","""Microsoft
Corporation""","""1.14.10.19041""","""2023-06-
15""","""C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy"""

"""Boromir""","""WIN32""","""brando""","""Windows Security""","""Microsoft
Corporation""","""10.0.19041.1865""","""2022-09-
06""","""C:\Windows\SystemApps\Microsoft.Windows.SecHealthUI_cw5n1h2txyewy"""

"""Boromir""","""WIN32""","""brando""","""Windows Shell Experience""","""Microsoft
Corporation""","""10.0.19041.1023""","""2021-11-
26""","""C:\Windows\SystemApps\Microsoft.Windows.PeopleExperienceHost_cw5n1h2txyewy"""

"""Boromir""","""WIN32""","""brando""","""Windows Shell Experience""","""Microsoft
Corporation""","""10.0.19041.1949""","""2023-05-
10""","""C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy"""
```

```
"""Boromir""","""WIN32""","""brando""","""Windows Voice Recorder""","""Microsoft
Corporation""","""10.2103.28.0""","""2021-09-23""","""C:\Program
Files\WindowsApps\Microsoft.WindowsSoundRecorder_10.2103.28.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""WindowsAppRuntime.1.2""","""Microsoft
Corporation""","""2000.802.31.0""","""2023-05-09""","""C:\Program
Files\WindowsApps\Microsoft.WindowsAppRuntime.1.2_2000.802.31.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""WindowsAppRuntime.1.3""","""Microsoft
Corporation""","""3000.882.2207.0""","""2023-06-19""","""C:\Program
Files\WindowsApps\Microsoft.WindowsAppRuntime.1.3_3000.882.2207.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Work or school account""","""Assigned by your
organization""","""1000.19041.1023.0""","""2021-11-
26""","""C:\Windows\SystemApps\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy"""

"""Boromir""","""WIN32""","""brando""","""Xbox Game Bar Plugin""","""Microsoft
Corporation""","""1.54.4001.0""","""2021-06-04""","""C:\Program
Files\WindowsApps\Microsoft.XboxGameOverlay_1.54.4001.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Xbox Game Bar""","""Microsoft
Corporation""","""5.823.3261.0""","""2023-05-09""","""C:\Program
Files\WindowsApps\Microsoft.XboxGamingOverlay_5.823.3261.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Xbox Game Speech Window""","""Microsoft
Corporation""","""1.21.13002.0""","""2021-06-04""","""C:\Program
Files\WindowsApps\Microsoft.XboxSpeechToTextOverlay_1.21.13002.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Xbox Game UI""","""Microsoft
Corporation""","""1000.19041.1023.0""","""2021-11-
26""","""C:\Windows\SystemApps\Microsoft.XboxGameCallableUI_cw5n1h2txyewy"""

"""Boromir""","""WIN32""","""brando""","""Xbox Identity Provider""","""Microsoft
Corporation""","""12.95.3001.0""","""2023-05-09""","""C:\Program
Files\WindowsApps\Microsoft.XboxIdentityProvider_12.95.3001.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Xbox TCUI""","""Microsoft
Corporation""","""1.24.10001.0""","""2021-06-04""","""C:\Program
Files\WindowsApps\Microsoft.Xbox.TCUI_1.24.10001.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""Your account""","""Email, phone, or
Skype""","""10.0.19041.1266""","""2022-03-
02""","""C:\Windows\SystemApps\Microsoft.Windows.CloudExperienceHost_cw5n1h2txyewy"""

"""Boromir""","""WIN32""","""brando""","""ms-
resource://microsoft.windowscommunicationsapps/hxoutlookintl/AppManifest_OutlookDesktop_
DisplayName""","""Microsoft Corporation""","""16005.14326.21490.0""","""2023-06-
```

```
27""","""C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_
16005.14326.21490.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""ms-resource:AppDisplayName""","""ms-
resource:PublisherDisplayName""","""1000.19041.1023.0""","""2021-11-
26""","""C:\Windows\SystemApps\Microsoft.Windows.CallingShellApp_cw5n1h2txyewy"""

"""Boromir""","""WIN32""","""brando""","""ms-resource:AppxManifest_
DisplayName""","""Microsoft Corporation""","""10.0.19041.1023""","""2021-11-
26""","""C:\Windows\SystemApps\Microsoft.Windows.FilePicker_cw5n1h2txyewy"""

"""Boromir""","""WIN32""","""brando""","""ms-resource:AppxManifest_
DisplayName""","""Microsoft Corporation""","""10.0.19041.1949""","""2023-05-
10""","""C:\Windows\SystemApps\Microsoft.Windows.FileExplorer_cw5n1h2txyewy"""

"""Boromir""","""WIN32""","""brando""","""ms-
resource:Common.View.UWP/Resources/StoreAppName""","""Microsoft
Corporation""","""7.2211.24012.0""","""2023-05-09""","""C:\Program
Files\WindowsApps\Microsoft.Microsoft3DViewer_7.2211.24012.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""ms-resource:DisplayName""","""ms-
resource:PublisherDisplayName""","""10.0.19041.1023""","""2021-11-
26""","""C:\Windows\SystemApps\Microsoft.Win32WebViewHost_cw5n1h2txyewy"""

"""Boromir""","""WIN32""","""brando""","""ms-
resource:LensSDK/Resources/AppStoreName""","""Microsoft
Corporation""","""2023.2304.11.0""","""2023-06-15""","""C:\Program
Files\WindowsApps\Microsoft.WindowsCamera_2023.2304.11.0_x86__8wekyb3d8bbwe"""

"""Boromir""","""WIN32""","""brando""","""ms-
resource:StartMenuExperienceHost/PkgDisplayName""","""ms-
resource:StartMenuExperienceHost/PublisherDisplayName""","""10.0.19041.1023""","""2021-
11-26""","""C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_
cw5n1h2txyewy"""

"""Boromir""","""WIN32""","""brando""","""ms-resource:XboxApp.Resource/Resources/App_
Title""","""Microsoft Corporation""","""48.89.25001.0""","""2022-07-05""","""C:\Program
Files\WindowsApps\Microsoft.XboxApp_48.89.25001.0_x86__8wekyb3d8bbwe"""
```

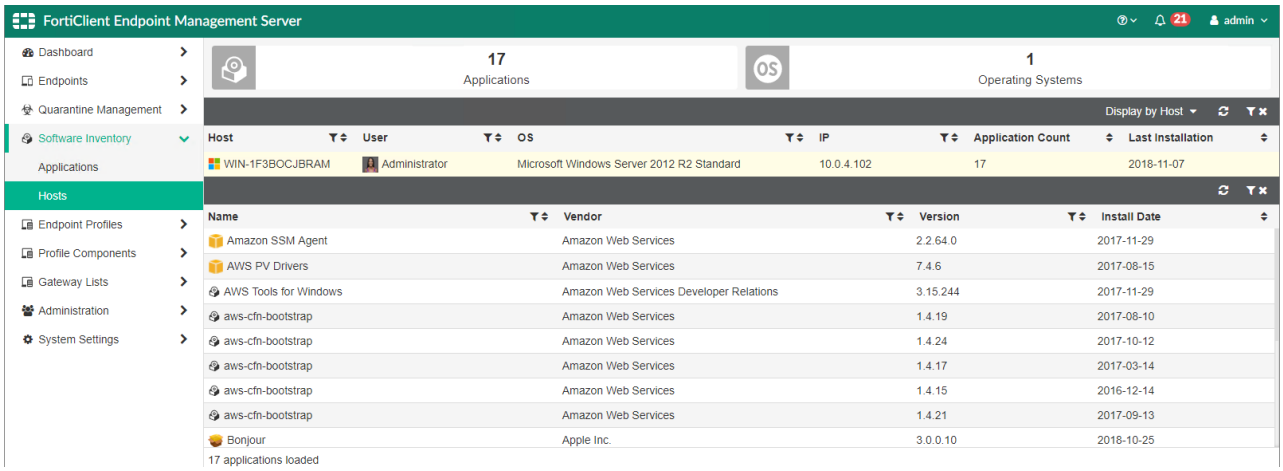
Hosts

The FortiEndpoint administrator can view installed application information for all managed endpoints by host on the *Hosts* pane.

To view the Hosts content pane:

You can view information about installed applications by host on the *Hosts* content pane.

1. Go to *Software Inventory* > *Hosts*. The list of hosts, a quick status bar, and a toolbar display in the content pane.



Applications	Number of applications that have been installed on all managed endpoints.
Operating Systems	Number of different operating systems on managed endpoints.
View Details	Displays list of software installed on the selected endpoint. For details on the application list headings, see To view the Applications content pane: on page 450.
Refresh	Click to refresh the list of applications in the content pane.
Clear Filters	Click to clear all filters applied to the list of files.
Host	Hostname.
User	Name of the endpoint user.
OS	Operating system installed on the endpoint.
IP	IP address of the endpoint.
Application Count	Number of applications installed on the endpoint.
Last Installation	Date of the most recent application installation on the endpoint.

To filter hosts:

You can filter the list of hosts displayed on the *Hosts* content pane.

1. Go to *Software Inventory* > *Hosts*. The list of hosts displays.
2. You can apply filters by hostname, user name, OS name, and IP address. Click the filter icon beside the desired heading. Enter the value to include in the filter. You can toggle the *All/Any/Not* button for the following options:
   - *All:* Display all files that match the set filter.
   - *Any:* Display any file that matches the set filter.
   - *Not:* Display only files that do not match the set filter.
3. To remove a filter, click the *X* icon beside the filter. To remove all filters, click the *Clear Filters* icon on the toolbar.

To filter the list of applications installed on an endpoint, select the endpoint and click *View Details*. See To filter applications: on page 451 for details on filtering the list of applications.

Quarantine Management

You can view and allowlist files that FortiSandbox or AV has quarantined from a central management *Files* pane. You can also view and delete allowlisted files from the *Allowlist* pane.

This feature is only supported for Windows endpoints.

Files

FortiClient sends quarantined file information to FortiEndpoint. You can view quarantined file information for all managed endpoints in *Files* pane and allowlist files from FortiEndpoint if needed.

Viewing quarantined files

After FortiClient quarantines files on endpoints and sends the quarantined file information to FortiEndpoint, you can view the list of quarantined files on the *Files* pane. You can also view details about each quarantined file and use filters to access quarantined files with specific qualities.

To view the Files content pane:

You can view information about quarantined files on the *Files* content pane.

1. Go to *Quarantine Management* > *Files*. The list of quarantined files, a quick status bar, and a toolbar display in the content pane.

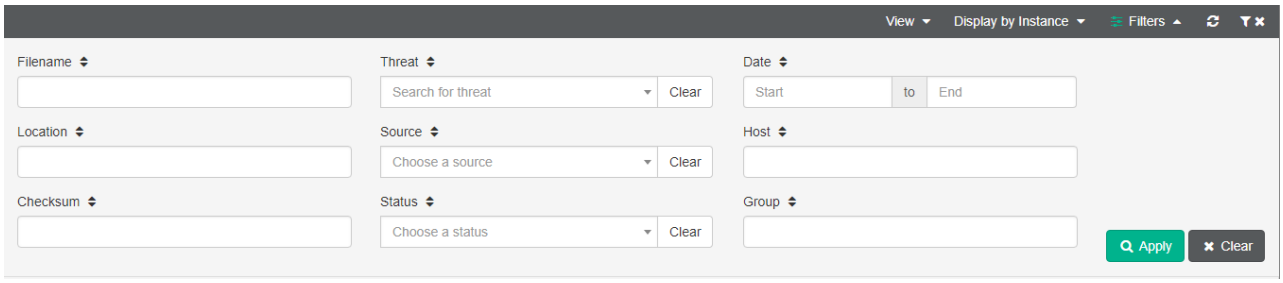
Quarantined Files	Number of files that FortiClient has quarantined on endpoints. Click to display the list of quarantined files.
Restored Files	Number of files that have been restored on endpoints. Click to display the list of restored files.
Affected Hosts	Number of hosts where FortiClient has quarantined files. Click to display the list of quarantined files sorted by hostname.
New Detections	Number of new detections. Click to display the list of newly detected threats sorted by date detected.

View	Toggle between the following options: • View all files or view only quarantined files • Show or hide full path names for files
Display by	Select to display the list of files by instance, host, threat, or date.
Search All Fields	Enter a value and press *Enter* to search for the value in the list of files.
Filters	Click to display and hide filters you can use to filter the list of files.
Refresh	Click to refresh the list of files in the content pane.
Clear Filters	Click to clear all filters applied to the list of files.
Checkbox	Click to select all files displayed in the content pane.
Host	Hostname of the endpoint. Also shows the group the endpoint belongs to.
File	Name of the file.
Size	Size of the file in bytes.
Threat	Name of threat.
Source	Displays how FortiClient detected the threat: • Scheduled Scan • Email Scan • Startup Scan • Manual Scan • Realtime Scan • Rootkit Manual Scan • Sandbox Scan
Status	Status of the file: *Quarantined*, *Quarantined & Allowlisted*, *Restored*, or *Deleted*. Also shows the time that FortiClient quarantined the file.
Summary	Displays the number of threat instances and number of affected hosts.

To filter the file list:

You can filter the list of files displayed on the *Files* content pane.

1. Go to *Quarantine Management* > *Files*. The list of files displays.
2. Click the *Filters* menu, and set filters.
   The filter options display.
   For text values, you can use a comma (,) to separate values and an exclamation mark (!) to exclude a value.



Filename	Enter the file name(s) to include in the filter.
Location	Enter the file location(s) to include in the filter.
Checksum	Enter the checksum(s) to include in the filter.
Threat	Enter the threat(s) to include in the filter. You can also select the desired threat(s) from the dropdown list.
Source	Enter the source(s) to include in the filter. You can also select the desired source(s) from the dropdown list.
Status	Enter the status(es) to include in the filter. You can also select the desired statuse(s) from the dropdown list.
Date	Enter the range of dates to include in the filter.
Host	Enter the host(s) to include in the filter. You can also select the desired host(s) from the dropdown list.
Group	Enter the endpoint group(s) to include in the filter. You can also select the desired group(s) from the dropdown list.

3. Click *Apply*. The filtered list of files displays.
4. Click *Clear Filters* to clear the filter settings.

Allowlisting quarantined files

You can allowlist and restore quarantined files. This releases the files from quarantine and makes them accessible on the endpoint with the next Telemetry communication between FortiEndpoint and FortiClient.

To allowlist quarantined files:

1. Go to *Quarantine Management* > *Files*.
2. Select the desired files.
3. Click *Allowlist & Restore*.
4. In the confirmation dialog, click *Yes*, then *Okay*. The file status changes to *Quarantined & Allowlisted*.

Configuring quarantine management

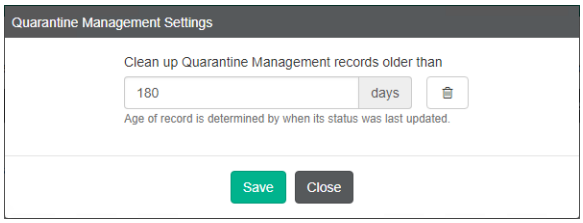
You can configure EMS to delete quarantine records after a configured number of days.

You cannot use EMS to delete quarantined files from endpoints. To configure EMS to delete quarantined files from an endpoint after a specified duration, configure the `<cullage>` XML option.

To configure quarantine management:

1. Go to *Quarantine Management* > *Files*.
2. Click the *Quarantine Management Settings* icon on the toolbar.
3. Enter the number of days after which to delete quarantine records from EMS. EMS determines the age of the quarantined file as when its status was last updated. For example, if you configure the duration

as 180 days, EMS deletes the quarantine record 180 days after the file was last updated.



Allowlist

Viewing allowlisted files

You can view the list of allowlisted files in the *Allowlist* pane. You can also view details about each allowlisted file and use filters to access allowlisted files with specific qualities:

Go to *Quarantine Management* > *Allowlist*. The list of allowlisted files and a toolbar display in the content pane.

Refresh	Click to refresh the list of files in the content pane.
Clear Filters	Click to clear all filters applied to the list of files.
Advanced Information	Click to view the FortiSandbox and AV signature and engine versions.
Date	Date and time the file was allowlisted.
File	Name of the file.
Checksum	File's checksum.
Threat	Name of threat.
Description	The file's description. Blank by default.

To filter allowlisted files:

1. Go to *Quarantine Management* > *Allowlist*. The list of files displays.
2. You can apply filters by date, file name, checksum, threat, and description. Do the following:
   a. To filter files by date, click the filter icon beside the *Date* heading. Select the desired date range in the *Start* and *End* fields. You can also enter a start time and end time on the selected dates. The default time is 12:00 PM.
   b. To filter by file name, checksum, threat, or description, click the filter icon beside the desired heading. Enter the value to include in the filter. You can toggle the *All/Any/Not* button for the following options:
      - *All:* Display all files that match the set filter.
      - *Any:* Display any file that matches the set filter.
      - *Not:* Display only files that do not match the set filter.

   The filtered list of files displays.

3. To remove a filter, click the *X* icon beside the filter. To remove all filters, click the *Clear Filters* icon on the toolbar.

Editing file descriptions

You can edit an allowlisted file's description. By default, the file description is blank.

To edit an allowlisted file's description:

1. Go to *Quarantine Management > Allowlist*.
2. Select the desired file.
3. Click *Edit Description*.
4. In the *Required* field, enter the desired description.
5. Click *Confirm*. The description appears under the *Description* heading.

Deleting a file from the allowlist

You can delete files from the allowlist. This reverts the file's status to quarantined on the endpoint with the next Telemetry communication.

To delete a file from the allowlist:

1. Go to *Quarantine Management > Allowlist*.
2. Select the desired file.
3. Click *Delete*.
4. In the confirmation dialog, click *Yes*. EMS deletes the file from the allowlist. FortiClient quarantines the file on the endpoint with the next Telemetry communication. You can view the file on the *Files* pane.

Administration

Admin Users

You can view the default *admin* user and all users added to FortiEndpoint.

Go to *Administration* > *Admin Users*. The following information displays:

Add	Add a new user.
Refresh	Refresh the list of users.
Name	The username.
Source	Type of user: • BuiltIn: User accounts built into FortiEndpoint by default, such as the admin user. • Windows: User accounts derived from Windows user accounts on the host server. • LDAP: User accounts derived from users belonging to a configured AD domain. • EMS: User accounts created in FortiEndpoint.
Role	Admin role assigned to the user. See Admin roles on page 480.
Trusted hosts	Trusted hosts configured for this user.
Last login or activation	Date and time of the user's last login or activation. Also shows if the account has been disabled due to inactivity. See .
Comments	Comments added when creating/configuring the user.

Admin roles

You can use admin roles to define the permissions each administrator account has in FortiEndpoint. You can use a default admin role in FortiEndpoint or create a new admin role to assign to an administrator account. Each admin role can include permissions from the following categories: endpoint, policy, and settings.

The following describes the default admin roles in FortiEndpoint. You cannot edit or delete these admin roles:

Name	Description
Super administrator	Most privileged admin role. Complete access to all FortiEndpoint permissions, including modification, user permissions, approval, discovery, and deployment. Only built-in role that has access to the *Administration* section of the GUI. Has access to all configured Windows and LDAP servers and users and authority to configure user privileges and permissions. The default admin account is a super administrator. You cannot assign another admin role to the admin account.
Standard administrator	Includes all endpoint and policy permissions and read-only permissions to settings permissions.
Endpoint administrator	Includes all endpoint permissions and read-only permissions to policy and settings permissions.
Read-only administrator	Includes read-only permissions to endpoint, policy, and settings permissions.
Restricted administrator	No permissions enabled.

For admin roles that are not authorized for certain tasks or devices, EMS hides or disables the related menu items, items in content pages, and buttons.

Adding an admin role

To add an admin role:

1. Go to *Administration* > *Admin Roles*.
2. Click *Add*.
3. In the *Name* field, enter the admin role name.
4. (Optional) In the *Description* field, enter the description.
5. Configure the permissions as desired. See Admin role permissions reference on page 482.
6. Click *Save*.

Cloning an admin role

1. Go to *Administration* > *Admin Roles*.
2. Select the desired admin role.
3. Click *Clone*.
4. Configure settings for the cloned admin role, then click *Save*.

Deleting admin roles

1. Go to *Administration* > *Admin Roles*.
2. Select the desired admin role.

3. Click *Delete*.
4. In the confirmation dialog, click *Yes*.

Admin role permissions reference

The following tables list the permissions available when configuring an admin role. The tables also include a description of what the permission allows the user to do and a link to the relevant section in this guide.

Permissions that apply to Chromebook management are denoted with an asterisk (*).

Endpoint permissions

Permission	Link to description
Manage LDAPs	Manage connections to LDAP servers to import users from.
Manage Google domains*	Manage connections to Google domains to decide which Chromebooks to manage. See Google Domains on page 96.
Manage custom groups	Create, rename, and edit endpoint groups. See Managing groups on page 53.
Run commands on endpoints	Perform actions to endpoints on the *Endpoints* pane, including uploading FortiClient logs, requesting diagnostic results, and so on. See Managing endpoints on page 76.
Block/Unblock/Quarantine/Unquarantine/Reregister endpoints	Manage endpoint access to the network through blocking, quarantine, and registration. See Managing endpoints on page 76.
Manage and assign endpoint policies	See Endpoint Policy & Components on page 116.
View group assignment rules	View group assignment rules. See Group assignment rules on page 92.
Manage group assignment rules	Create, delete, and edit group assignment rules. See Group assignment rules on page 92.
View endpoint filter bookmarks	View endpoint filter bookmarks. See Using bookmarks to filter the list of endpoints on page 70.
Manage endpoint filter bookmarks	Create, delete, and edit endpoint filter bookmarks. See Using bookmarks to filter the list of endpoints on page 70.
View quarantine management	View lists of quarantined and allowlisted files. See Quarantine Management on page 475.

Permission	Link to description
Manage quarantine management	Allowlist and restore quarantined files and remove files from the allowlist. See Quarantine Management on page 475.
View software inventory	See Software Inventory on page 450.
Manage software inventory	See Software Inventory on page 450.

Policy permissions

Permission	Link to description
View endpoint policies*	View endpoint policies. See Endpoint Policy & Components on page 116.
View endpoint profiles*	View endpoint profiles. See Endpoint Profiles on page 131.
Manage endpoint profiles*	Create, delete, and edit endpoint profiles. See Endpoint Profiles on page 131.
View Security Posture tagging rules	View security posture tagging rules. See Tags on page 408.
Manage Security Posture tagging rules	Create, delete, and edit security posture tagging rules. See Tags on page 408.
View Zero Trust telemetry server lists	View Telemetry server lists.
Manage Zero Trust telemetry server lists	Create, delete, and edit Telemetry server lists.
View installers	View installers. FortiClient Installer on page 106.
Manage installers	Create, delete, and edit installers. See FortiClient Installer on page 106.
View CA certificates	View CA certificates. See CA Certificates on page 122.
Manage CA certificates	Upload, import, and delete CA certificates. See CA Certificates on page 122.
View on-fabric detection rules	View on-fabric detection rules. See On-fabric Detection Rules on page 124.

Permission	Link to description
Manage on-fabric detection rules	Create, delete, and edit on-fabric detection rules. See On-fabric Detection Rules on page 124.

Setting permissions

Permission	Link to description
View server settings*	View *Server* settings. See Configuring EMS settings on page 533
Manage server settings*	Modify *Server* settings. See Configuring EMS settings on page 533.
View Fortinet services settings	View *FortiGuard Services* settings. See Configuring FortiGuard Services settings on page 546.
Manage Fortinet services settings	Modify *FortiGuard Services* settings. See Configuring FortiGuard Services settings on page 546.
View endpoint settings	View *Endpoints* settings. See Configuring EMS settings on page 533.
Manage endpoint settings	Modify *Endpoints* settings. See Configuring EMS settings on page 533.
View login banner settings*	View login banner settings. See Configuring EMS settings on page 533.
Manage login banner settings*	Modify login banner settings. See Configuring EMS settings on page 533.
View alert settings*	View *Alerts* settings. See Alerts on page 548.
Manage alert settings*	Modify *Alerts* settings. See Alerts on page 548.
View custom message settings	View endpoint quarantine message settings. See Customizing the endpoint quarantine message on page 552.

Permission	Link to description
Manage custom message settings	Modify endpoint quarantine message settings. See Customizing the endpoint quarantine message on page 552.
View feature select settings	View feature select settings. See Feature Select on page 555.
Manage feature select settings	Modify feature select settings. See Feature Select on page 555.

Authentication Servers

Adding an ADDS server

You can manually import endpoints from an Active Directory Domain Services (ADDS) server. You can import and synchronize information about computer accounts with an LDAP or LDAPS service. You can add endpoints by identifying endpoints that are part of an AD domain server. EMS supports Kerberos or NTLM authentication for LDAP(S).

The LDAP connection is read-only.



A video on how to add a domain is available in the Fortinet Video Library.



You can add the entire domain or an organization unit (OU) from the domain.



EMS does not support importing subdomains if you have already imported the parent domain in to EMS.

To add endpoints using an AD domain server:

1. Go to *Administration* > *Authentication Servers*.
2. Click *Add* > *Active Directory*.

3. Configure the following options:

Option	Description
IP address/Hostname	If using NTLM authentication, enter the LDAP server IP address or FQDN. If using Kerberos authentication, enter the domain FQDN. The Windows Active Directory DNS server should be reachable for EMS to resolve the FQDN and communicate with the resolved server to obtain the Kerberos ticket over TCP port 88.
Port	Enter the port number.
Username	Enter the username. If using Kerberos authentication, the username is case-sensitive. Enter the username in one of the following formats: • <domain>\<username> • <username>@<domain>.com
Password	Enter the user password.
Show Password	Turn on and off to show or hide the password.
LDAPS connection	Enable a secure connection protocol.
Certificate	Browse to and upload a certificate authority or server certificate in PEM or DER format to secure the LDAPS connection. This option is only available if you enable *LDAPS connection*.
Certificate hostname check	When enabled, EMS checks if the provided certificate's common name (CN) matches the CN of the certificate that the LDAPS connection provides.
Alias	Enter the alias (optional).
Comment	If desired, enter a comment about the server (optional).
Use Connector	If desired, enable this option to configure an AD connector to act as a proxy between EMS and the AD server. See AD connector on page 492.
Connector	From the dropdown list, select the desired AD connector.

4. Click *Test* to test the domain settings connection.
5. If the test succeeds, click *Save* to save the new domain. If not, correct the information as required, then test the settings again.



After importing endpoints from an AD server, you can move them to custom created groups. These groups are not seen in AD and EMS does not have the ability to modify the AD server in any way. See Managing groups on page 53.

Adding an Entra ID server



Entra ID integration with EMS has the following limitations:

- FortiClient (Linux) does not support Entra ID integration with EMS.
- FortiClient (macOS) does not support native Entra ID integration with EMS. For the integration to work, macOS endpoints must be managed by Intune or JAMF and enrolled to company portal using Entra ID.
- Azure Government (e.g. GCC, GCC High, GCC DoD) is not supported. Only commercial subscription is supported.

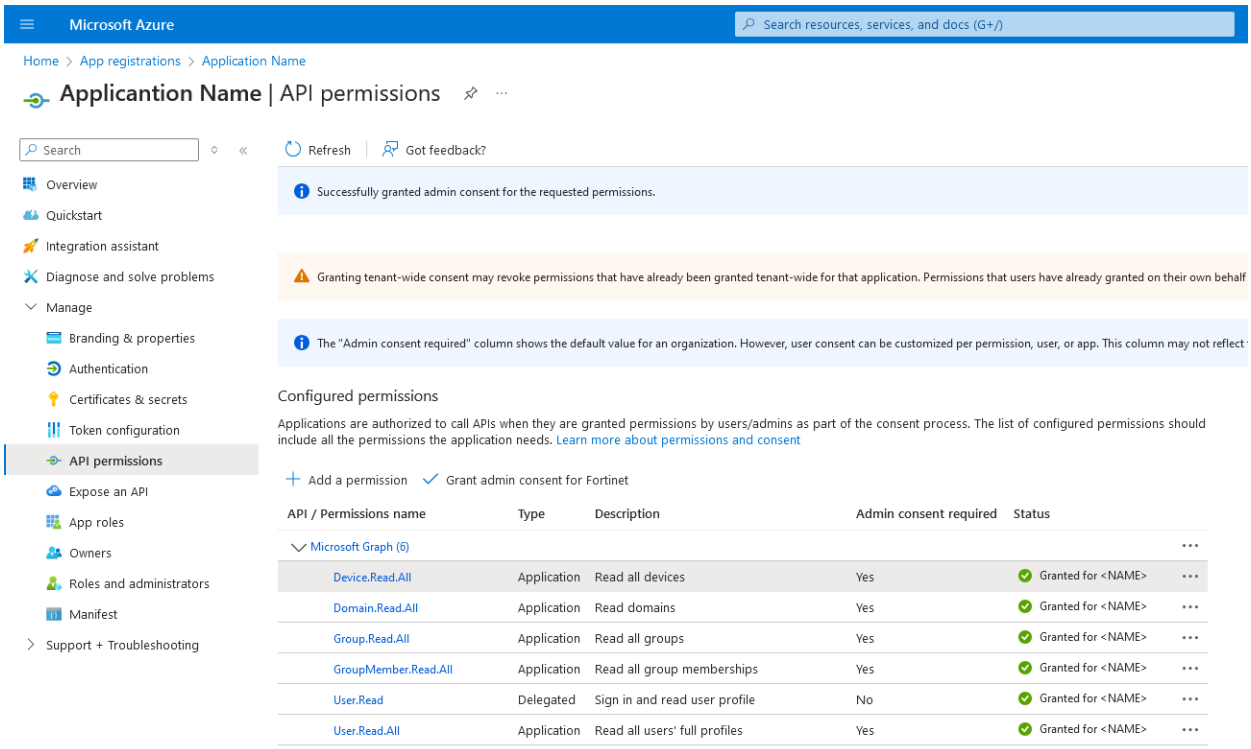
To create an enterprise application for FortiClient:

1. In the Azure portal, go to *Microsoft Entra ID > Enterprise applications > New application*.
2. Click *Create your own application*.
3. In the *What's the name of your app?* field, enter the desired name.
4. Under *What are you looking to do with your application?*, select *Register an application to integrate with Azure AD (App you're developing)*.
5. Click *Create*.

To add Microsoft Graph API application permissions required for searching user groups:

1. In the left menu, click *App registrations*, then click the *All applications* tab.
2. Click your FortiClient enterprise application.
3. In the left menu, click *API permissions*, and click *Add a permission*.
4. In the *Request API permissions* slide-in, click *Microsoft Graph*.
5. Select *Application permissions*.
6. In the *Select permissions* section, search for and select the following permissions:
   - *Device.Read.All*
   - *Domain.Read.All*
   - *Group.Read.All*
   - *GroupMember.Read.All*
   - *User.Read*
   - *User.Read.All*

7. Click *Add permissions*.



8. In *API permissions*, click *Grant admin consent for Default Directory*. If this option is grayed out, you must log into an Azure admin account to perform this step.

To add a client secret string and determine its value:

This only applies if you use client secret authentication.

1. In the left menu, click *App registrations*, then click the *All applications* tab.
2. Click your FortiClient enterprise application.
3. In the left menu, click *Certificates & secrets*, and click *New client secret*.
4. In the *Add a Client Secret* slide-in, add a *Description* and select the desired *Expires* option. Click *Add*.
5. Observe that a new client secret has been created. Immediately after creation, copy the *Value* of the client secret string, which EMS uses as the *Azure Client Secret*. This value is not visible after this initial creation step and moving to another page.

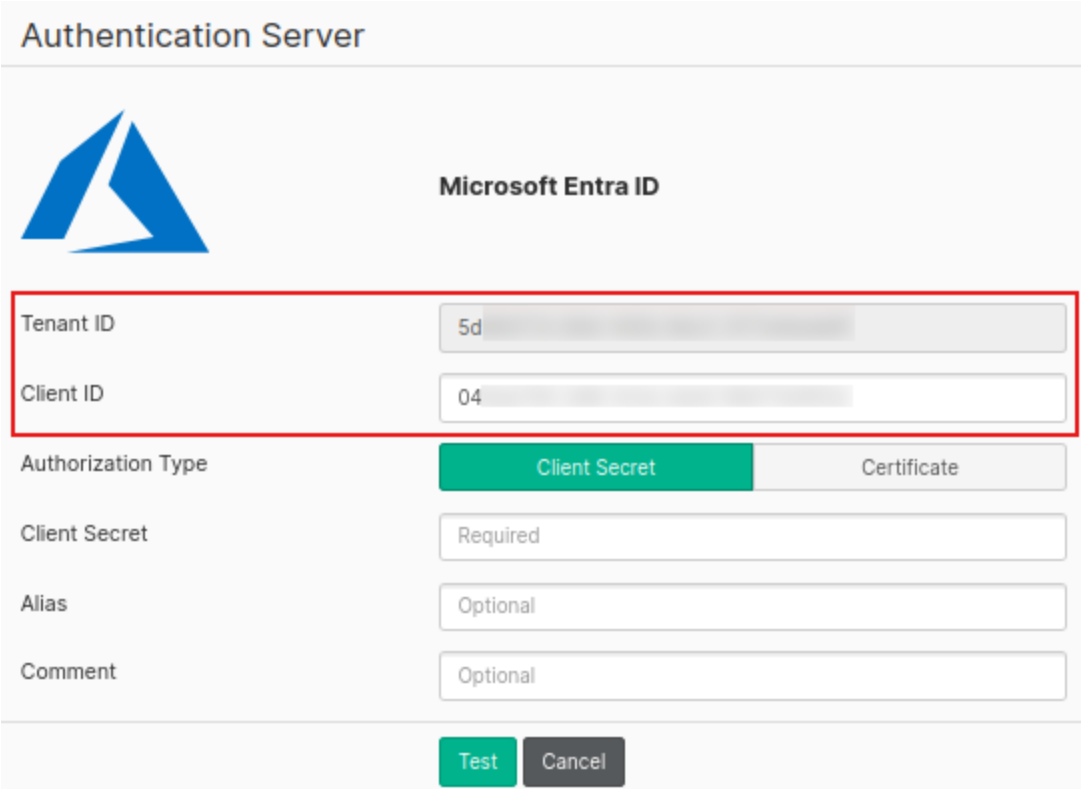
To upload a CA-signed certificate to Azure:

This only applies if you use certificate authentication. The following assumes that you have a certificate authority (CA)-signed certificate.

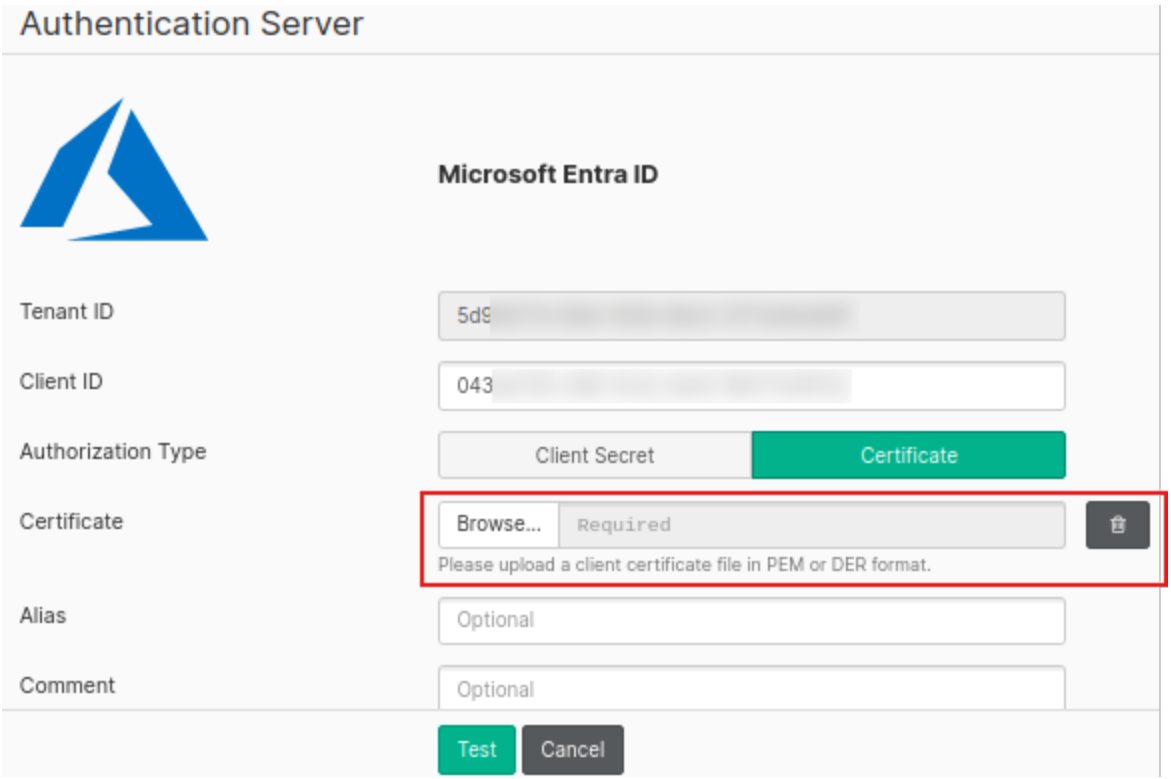
1. In the left menu, click *App registrations*, then click the *All applications* tab.
2. Click your FortiClient enterprise application.
3. In the left menu, click *Certificates & secrets*, and click *Certificates*.
4. Click *Upload certificate*, and select the desired certificate.

To configure an Entra ID server in EMS:

1. Configure the Entra ID server as an authentication server in EMS:
   a. Go to *Administration > Authentication Servers*.
   b. Click *Add > Microsoft Entra*.
   c. In the *Tenant ID* and *Client ID* fields, enter the tenant ID and client ID that you collected from the Azure management console.

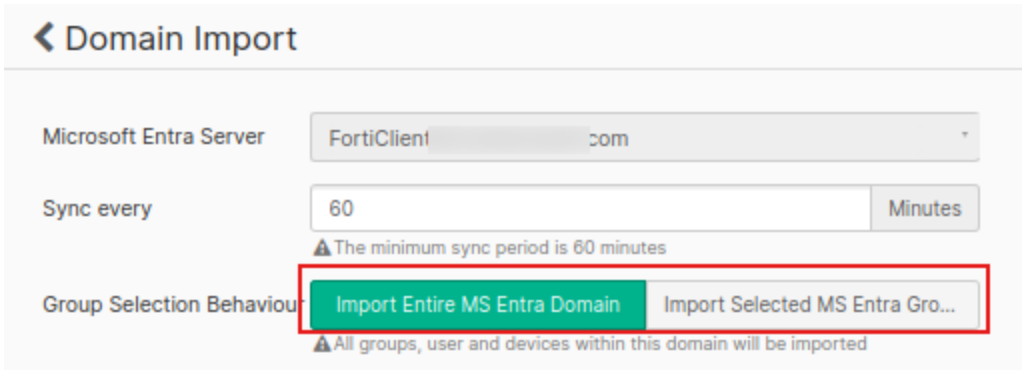


   d. In *Authorization Type*, select *Client Secret* or *Certificate* as needed:
      - To use client secret authentication, select *Client Secret* and enter the client secret that you collected from the Azure management console in the *Client Secret* field.
      - To use certificate authentication, select *Certificate* and browse to select the CA-signed certificate that you uploaded to Azure in To upload a CA-signed certificate to Azure: on page 488.



e. Configure other fields as desired.
f. Click *Test*.
g. After the test succeeds, click *Save*.

2. Go to *Endpoints* > *Manage Domains*.
3. Click *Add*, then *Microsoft Entra*.
4. From the *Microsoft Entra Server* dropdown list, select the desired server.
5. In the *Sync every* field, enter the number of minutes after which EMS syncs with the Microsoft Entra server.
6. For *Group Selection Behaviour*, select *Import Entire MS Entra Domain* or *Import Selected MS Entra Groups*.

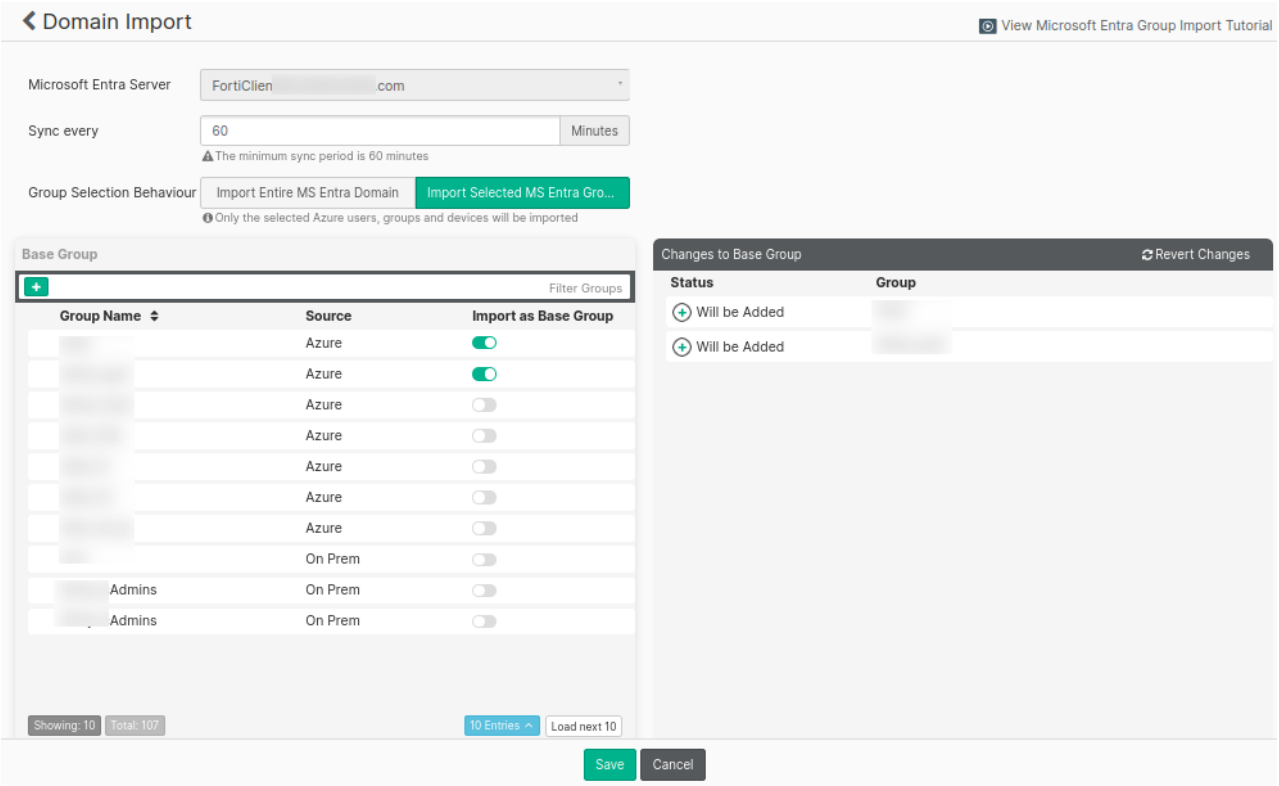


Option	Description
Import Entire MS Entra Domain	All enabled devices, users, and groups from the Microsoft Entra server will be imported.

Option	Description
Import Selected MS Entra Groups	Only the enabled devices, users, and groups from the selected Microsoft Entra groups will be imported.

7. When *Import Selected MS Entra Groups* is selected, enable *Import as Base Group* for the desired groups as needed.

   Note that subgroups are listed flat without preserving the hierarchy from the Microsoft Entra server.



8. Click *Save*. EMS then syncs all enabled devices, users, and groups from all or selected Microsoft Entra groups in the Microsoft Entra server. Disabled devices, users, and groups are excluded.

When using user management, Entra ID users can register their FortiClient to EMS using an invitation code or with SAML.

To configure the Azure tenant app for initiating passthrough (domain):

This is necessary for registering an Entra ID endpoint to EMS using an invitation code. This only applies for Entra ID-joined endpoints.

1. Configure the redirect URL:
   a. In the Azure portal, go to *App registration*. Copy the application/client ID of the application used to connect with EMS.
   b. Click the application, then click the *Redirect URIs* link.
   c. Click *Add a Platform* > *Select Mobile and Desktop applications*.
   d. Add the following URL: `ms-appx-web://microsoft.aad.brokerplugin/<application client ID>`.
   e. Under *Allow public client flows*, toggle to *Yes* for *Enable the following mobile and desktop flows*.

f. Save the configuration.

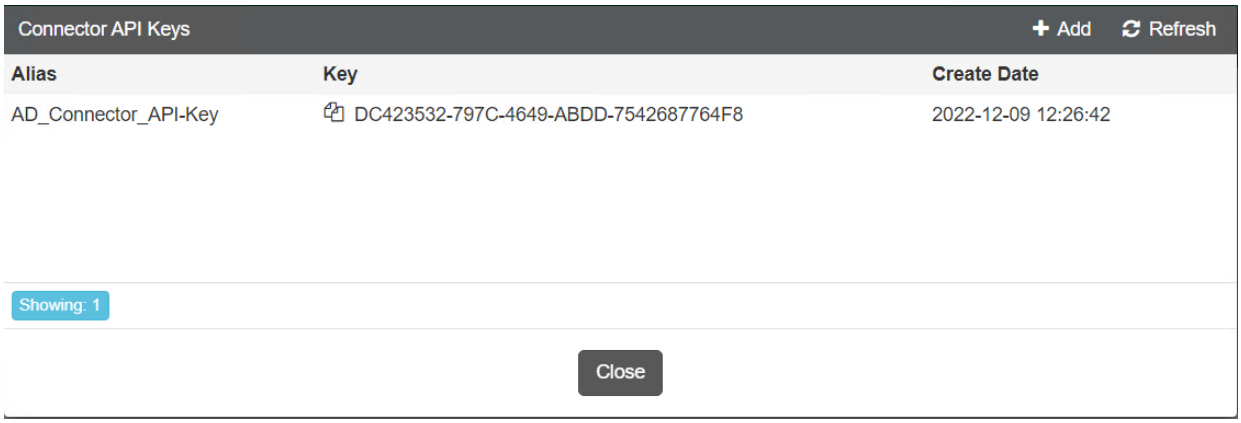
2. Go to *Roles and administrators*.
3. Search for and select *Directory Readers*.
4. Click *Add assignments*.
5. Select the application used to connect with EMS.
6. Add desired users to the application in Entra ID:
   a. Go to *Enterprise applications*, and select the application used to connect with EMS.
   b. Go to *Users and groups*.
   c. Click *Add user/group*, and select the users that you will invite to EMS using an invitation code.

Adding an API key

You can add an API key and use it to configure an Active Directory (AD) connector to act as a proxy between EMS and the AD server. See AD connector on page 492.

To add an API key:

1. Go to *Administration > Authentication Servers*.
2. Click *Connectors*.
3. Click *API Keys*, then *Add*.
4. In the *Alias* field, enter the desired alias, then click Add.

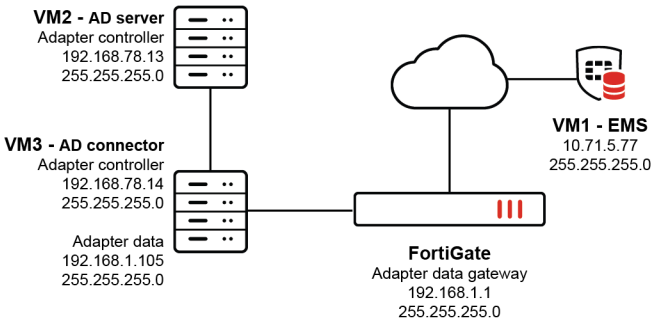


AD connector

You can configure an Active Directory (AD) connector that acts as a proxy between the AD server and EMS.

The following shows an example environment, which consists of the following virtual machines (VM):

- VM1: EMS
- VM2: AD server (ems104.com)
- VM3: AD connector



In this example, VM2 is connected to a local network with an IP address of 192.168.178.13/24. EMS is connected to a public network with an IP address of 10.71.5.77/24. In this scenario, when you attempt to add the AD server as an authentication server in *Administration > Authentication Servers* in EMS, it cannot reach the AD server. The AD connector solves this problem. The AD connector has the following network adapters:

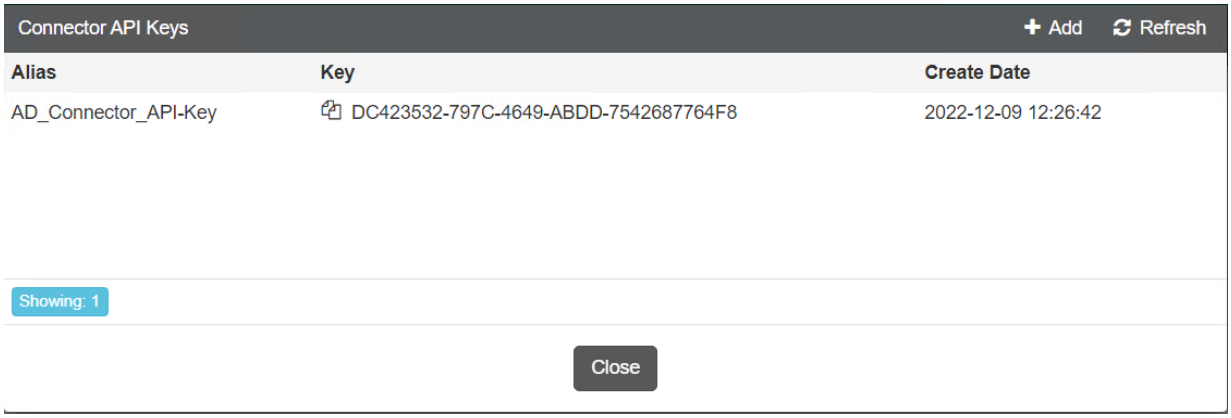
Adapter	IP address
Adapter connector	192.168.78.14
Adapter data	192.168.1.105
Default gateway	192.168.1.1

The gateway for adapter data is 192.168.1.1, which is a FortiGate that is connected to the internet. The AD server cannot directly connect to EMS. EMS cannot access the AD server. The connector serves as a proxy to add the AD server to EMS.

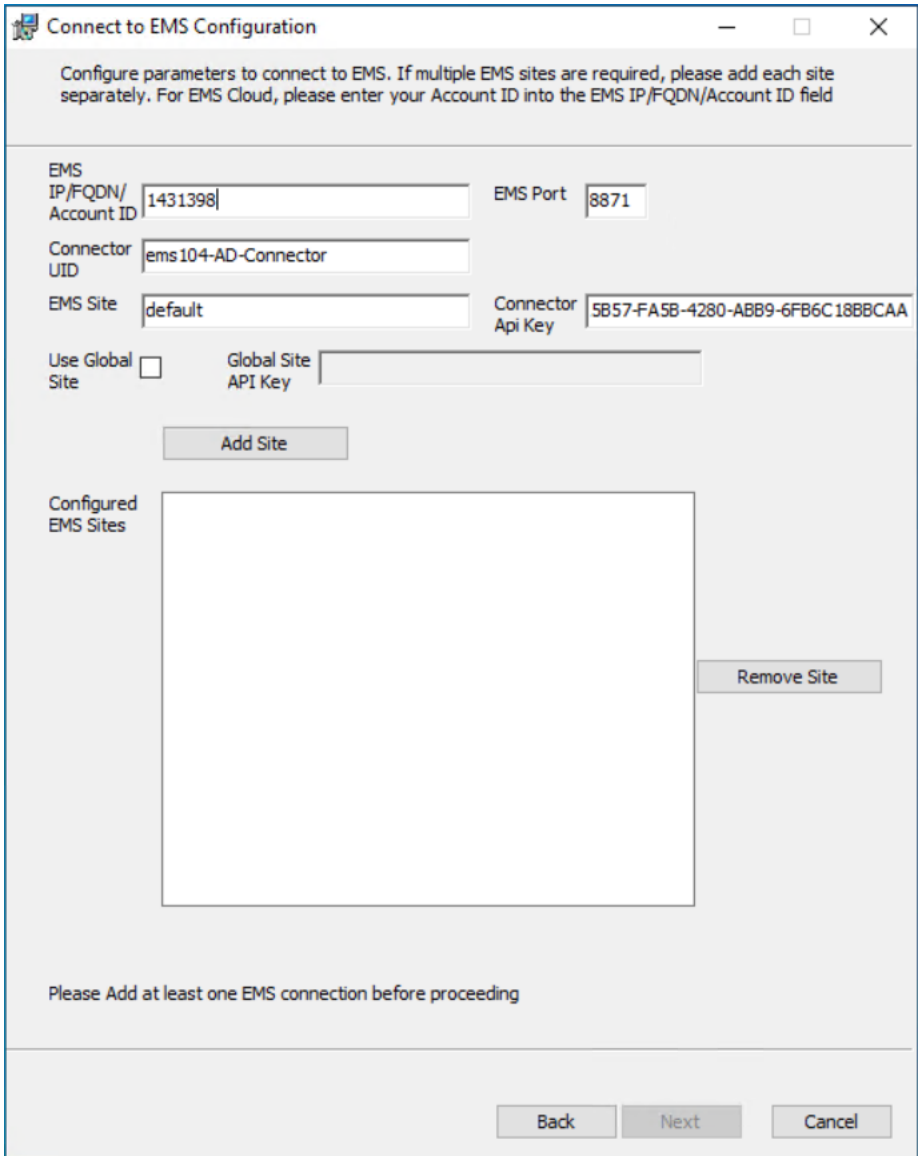
The AD connector and EMS versions must match for this feature to function. The SSL certificate that the AD server sends to establish a TLS handshake can have a maximum RSA key size of 8192 bits.

To configure the AD connector:

1. Add an API key:
   a. In EMS, go to *Administration > Authentication Servers*.
   b. Click *Connectors*.
   c. Click *API Keys*, then *Add*. Add a new API key.

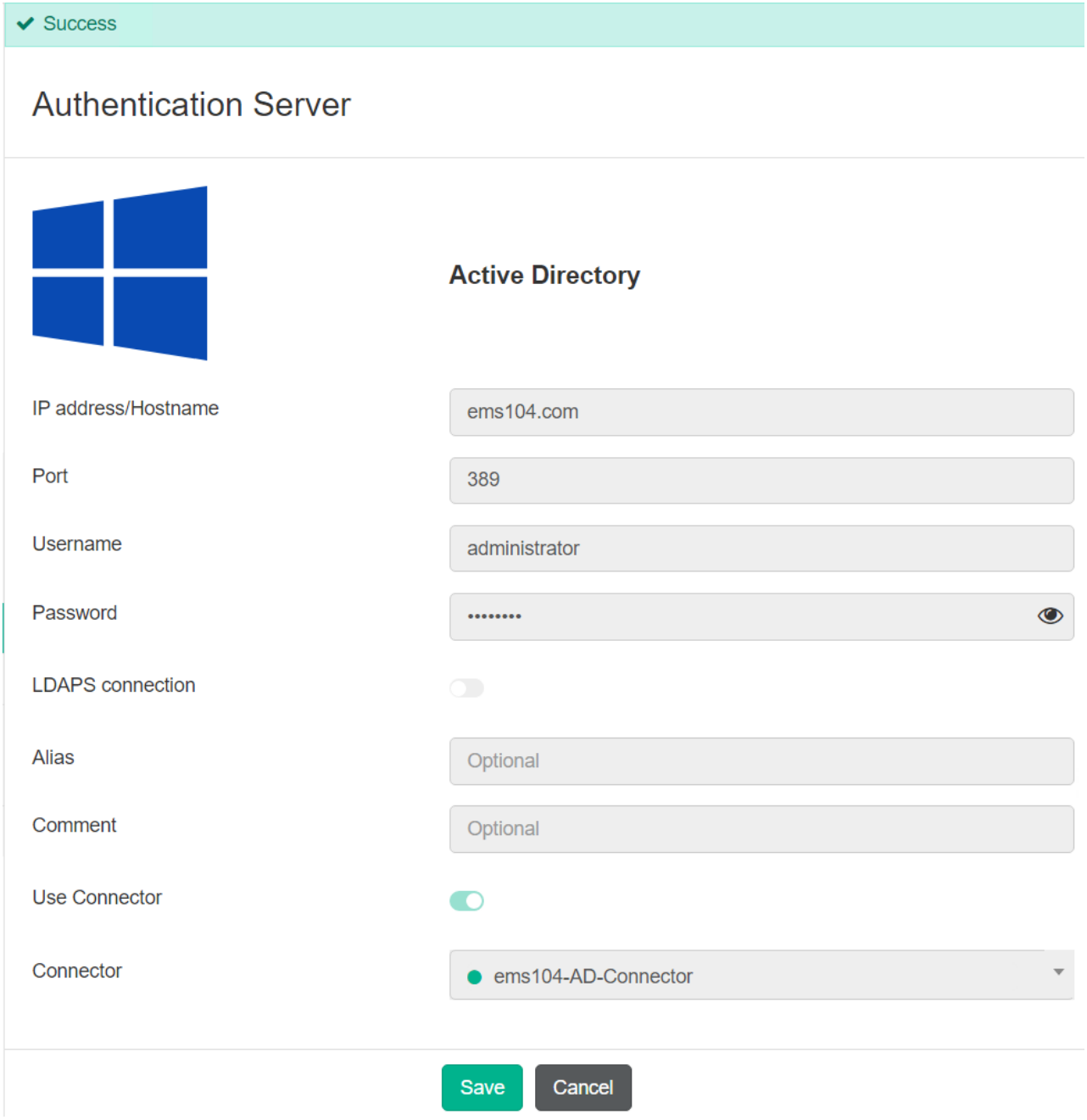


2. Create the AD connector:
   a. You can install the AD connector in a host that EMS and the AD server can reach. On the host machine, from the EMS installation package, run FortiClientEndpointManagementServerADConnector_26.1.b.[[[Undefined variable FortinetVariables.Build]]]_x64.msi.
   b. In the *Connect to EMS Configuration* dialog, enter the EMS IP address, fully qualified domain name, or account ID in the *EMS IP/FQDN/Account ID* field.
   c. In the *EMS Port* field, enter the port number.
   d. In the *Connector UID* field, enter the desired AD connector UID. Entering a meaningful string to help identify the AD connector is recommended. Do not leave this field blank.
   e. In the *Connector Api Key* field, enter the API key value.
   f. Click *Add Site*, and enter the EMS site information. Ensure that a *Connection established* message displays, then click *Next*.



3. If desired, configure the directories configuration. You can also click *Next* to configure it later:
   a. In the *Directory Host* field, enter the hostname of the desired AD server.
   b. In the *Directory Port* field, enter the port number that the AD server uses to communicate with EMS.
   c. In the *Username* and *Password* fields, enter the credentials used to log in to the AD server.
   d. If desired, enable *Use LDAPS*.
   e. If you enabled *LDAPS*, in the *CA Certificate Path* field, enter the path to the desired CA certificate to use for the LDAPS connection.
   f. If you enabled LDAPS, if desired, enable *Check Cert Hostname*.
   g. Under *Non-Selected Sites for Directory* and *Selected Sites for Directory*, click *Include Sites* and *Exclude Sites* to include and exclude sites as desired.
   h. Click *Add Directory* and *Remove Directory* to populate the *Configured Directories List* as desired. Click *Next*.
4. In EMS, go to *Administration > Authentication Servers > Connectors* to confirm that you successfully created an AD connector.
5. Go to *Administration > Authentication Servers*.
6. Enable *Use Connector*.
7. From the *Connector* dropdown list, select the AD connector.

8. Save the configuration. EMS successfully adds the AD server as an authentication server.



Log Viewer

To view logs:

1. Go to *Administration > Log Viewer*.
2. Click the *Filter* icon in each column heading to apply filters.
3. Click *Clear Filters* to remove the filters.

To download logs:

You can download the logs that FortiEndpoint generates.

1. Go to *Administration > Logs*.
2. Click *Download*. A zip of the raw logs is downloaded to your computer.

User Management

In *User Management*, you can configure options for user verification. EMS supports the following user verification methods:

Verification type	Description
None	End user does not need to provide any credentials to connect to EMS.
Local	End user must provide credentials that match a local user configured in *User Management* > *Local Users* to connect to EMS. You must create a local user to configure this option. See Local users on page 501.
LDAP	End user must provide their domain credentials to connect to EMS. You must configure an LDAP domain to configure this option. See Adding endpoints using an AD domain server on page 54.
SAML	End user must provide their credentials for an SAML identity provider, such as Microsoft Entra ID (formerly kown as Azure Active Directory (AD)), to connect to EMS. You must configure SAML settings to configure this option. See SAML Configuration on page 502.

The process is as follows:

1. The EMS administrator configures the desired verification method. For example, the EMS administrator can configure an AD server for EMS to connect to. EMS imports user groups from the configured AD server. See Authorized User Groups on page 498.
2. The EMS administrator creates an invitation, which includes a FortiClient installer and verification method. In this example, the EMS administrator would create an invitation that only applies to users that belong to the desired AD domain. See Invitations on page 503.
3. The EMS administrator sends the invitation to end users by email or SMS.
4. The end user downloads the FortiClient installer using the link included in the email.
5. The end user installs FortiClient on their endpoint.
6. FortiClient automatically launches and prompts for the user to enter their credentials. The end user enters their AD credentials. EMS verifies that the credentials match a known user in the AD domain that was configured in the invitation code and allows the user to connect to FortiEndpoint.

Authorized User Groups

Authorized User Groups displays OUs and user groups from all imported LDAP servers.

This page displays the following columns of information:

Column	Description
Domain Name	Group name.
Server IP	LDAP server IP address.
Last Synced	Time that EMS and the LDAP server last synchronized configurations.
Invitation Status	Whether an invitation was created for this user group.

Selecting a domain in the list displays the following columns of information:

Column	Description
Group Name	Group name.
Users	Number of users that belong to the group.
Group Status	• *Authorized* (default)—If a group is authorized, its users can onboard to EMS as long as the user does not belong to any excluded groups. • *Excluded*—If a group is excluded, its users are blocked from connecting and cannot onboard to EMS, even if the user also belongs to other authorized groups. **Example:** Assuming that we have two LDAP groups: Group A and Group B, both authorized with a shared user Adam. Adam can be verified and join the ForitClient EMS because he belongs to an authorized group but not any excluded groups. If you change the status of Group B to *Excluded*, Adam will not be able to be verified or join the FortiClient EMS any more even if Adam also belongs to Group A which is authorized.

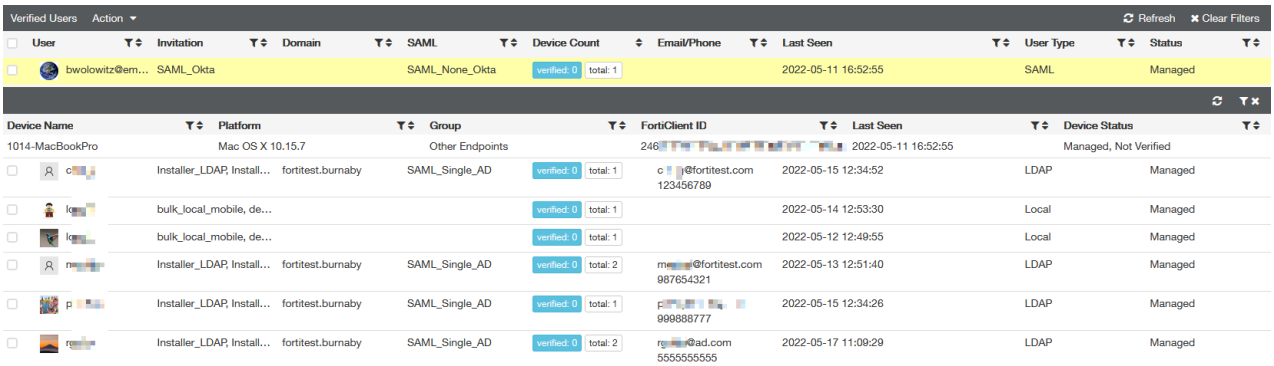
You can filter the list of groups by authorized or excluded, OUs or groups.

To authorize or exclude a group:

1. Go to *User Management* > *Authorized User Groups*.
2. Select the desired domain.
3. Select the desired group(s).
4. Click *Authorize* or *Exclude*.

Verified Users

Verified Users shows a list of users who have successfully connected to FortiEndpoint by using an invitation and authenticating using a specified verification method.



This page displays the following columns of user information:

Column	Description
User	Username of the connected user.
Invitation	Names of the invitation(s) that the user received.
Domain	Domain that the user used to authenticate and connect to EMS, if applicable.
SAML	SAML server that the user used to authenticate and connect to EMS, if applicable.
Device Count	Number of devices that the user has connected to EMS.
Email/Phone	User's email address and phone number.
Last Seen	Time that the user was last active.
User Type	Displays the type of authentication the user used to connect to EMS.
Status	Displays whether the user is currently managed by EMS.

You can click the user to view the devices that they have currently connected to EMS. The following information displays for devices:

Column	Description
Device Name	Name of the connected device.
Platform	Operating system installed on the device.
Group	Endpoint group that the device belongs to.
FortiClient ID	ID of the FortiClient instance installed on the device.
Last Seen	Time that the device was last active.
Device Status	Displays whether the device is currently managed by EMS and whether the device is licensed.

You can exclude users from management. This frees up the license seat that the user was consuming.

To exclude users from management:

1. Go to *User Management* > *Verified Users*.
2. Select the desired users.
3. From the *Action* dropdown list, select *Exclude from Management*.

Unverified Users

Unverified Users shows a list of users who have not verified their identity using one of the specified authentication methods. This page displays the following columns of user information:

Column	Description
User Name	Username of the user.
Domain	Domain that the user used to authenticate and connect to EMS, if applicable.
Device Count	Number of devices that the user has connected to EMS.
Email/Phone	User's email address and phone number.
Last Seen	Time that the user was last active.

You can click the user to view the devices that they have currently connected to EMS. The following information displays for devices:

Column	Description
Device Name	Name of the connected device.
Platform	Operating system installed on the device.
Group	Endpoint group that the device belongs to.
FortiClient ID	ID of the FortiClient instance installed on the device.
Last Seen	Time that the device was last active.
Device Status	Displays whether the device is currently managed by EMS and whether the device is licensed.

Local users

You can configure local users. Users can provide credentials that match a configured local user to connect their FortiClient to FortiEndpoint. This is mainly useful for environments that do not use Active Directory or SAML.

To add a local user:

1. Go to *User Management* > *Local Users*.
2. Click *Add*.
3. In the *Username* field, enter the desired username.
4. In the *Password* and *Confirm Password* fields, enter a password that conforms to the displayed password rules.
5. (Optional) In the *Comments* field, enter any desired notes.
6. Click *Save*.

SAML Configuration

In *SAML Configuration*, you can configure connections to SAML identity providers (IdP), such as Microsoft Entra ID (formerly known as Azure Active Directory (AD)). This allows end users to connect to FortiEndpoint and authenticate using their relevant credentials, such as to Entra ID.

To add a SAML configuration:

1. In EMS, go to *User Management* > *SAML Configuration*.
2. In the *Name* field, enter the desired name for this configuration.
3. For *Authorization Type*, do one of the following:
   a. Select *LDAP* to associate a domain with this SAML configuration. From the *Domain* dropdown list, select the desired domain.
   b. Select *None* to not associate a domain with this SAML configuration. This is only recommended for non-domain endpoints.
4. In the *Domain Identification* field, enter an AD userPrincipalName attribute name for EMS to use to verify the user's domain. You must add the same attribute to the IdP for verification to succeed.
5. Configure *Service Provider Settings*. EMS is the service provider (SP):

Setting	Description
SP Address	Enter the EMS IP address. You can also click the *Use Current URL* button to autopopulate the field. Your browser must be able to access this IP address.
Prefix	Enter the prefix generated in EMS for the IdP. You can generate a new prefix by clicking the *Generate* button.
SP ACS (login) URL	Enter the SP login URL.
SP Entity ID	Enter the SP entity ID.
SP Certificate	Click *Upload new certificate* to upload the SP certificate. Only upload an SP certificate if you uploaded the same certificate for this SP (in this case, EMS) in the IdP server.

6. Configure *Identity Provider Settings*:

Setting	Description
IdP single sign-on URL	Enter the IdP single sign-on URL, including the http or https prefix as applicable.
IdP entity ID	Enter the IdP entity ID, including the http or https prefix as applicable.
IdP Certificate	Click *Upload new certificate* to upload the IdP certificate. Upload the same certificate that you configured in the IdP.

7. Click *Save*.



To use SAML to verify user identity when users connect FortiClient to EMS using an invitation code, you must select *SAML* for the *Verification Type* when configuring an invitation. See Invitations on page 503.

Invitations

After installing FortiClient, end users must enter the invitation codes to connect FortiClient to EMS. You can generate invitation codes for all authentication types (local, LDAP, or SAML-based), including scenarios where no authentication is required, which can be used for headless onboarding. The invitation codes can be shared with end users via email.

To add an invitation code:

1. Go to *Invitations* in the upper right corner, in *Endpoints* > *Invitations*, or in *User Management* > *Invitations*.
2. Do one of the following:
   - To create a new invitation code, click *Add*.
   - To edit an existing invitation code, select the desired invitation code. Click *Edit*.
3. Configure the invitation:
   a. From the *EMS Listen Address* dropdown list, select the desired address.
   b. To send the code to a single recipient, select *Individual*. Otherwise, select *Bulk*.
   c. If desired, configure sending email notifications:
      i. Enable *Send Email Notifications*. You can only enable this option if you have configured SMTP settings. See Configuring SMTP Server settings on page 550.
      ii. In the *Email Recipients* field, enter the desired recipient's email address. Click *+* and repeat with all desired recipients.
      iii. From the *Invitation Email Template* dropdown list, select the desired email template. See Invitation Email Template on page 553.
   d. In the *Include FortiClient Installer* field, click *Create a new installer* to add a deployment package to the invitation. The invitation email includes a link that the user can download the configured deployment package from. For deployment package option details, see Adding a FortiClient installer on page 106.
   e. In the *Email recipients* field, enter the email addresses of the desired end users.
   f. **(FortiClient Cloud only)** If desired, enable *Send SMS notifications*.

g. If desired, enable *Expiring*.
h. In the *Expiry date* field, set the expiry date.
i. For *Verification Type*, select one of the following user verification methods, which will be used when *Enforce User Verification* is enabled in *System Settings* > *EMS Settings*:

Verification type	Description
None	End user does not need to provide any credentials to connect to EMS. However, users cannot register with the EMS directly using IP address or FQDN. Endpoints with no user are registered automatically without any user interaction.
Local	End user must provide credentials that match a local user configured in *User Management* > *Local Users* to connect to EMS. You must create a local user to configure this option. See Local users on page 501.
Domain	End user must provide their domain credentials to connect to EMS. You must configure an LDAP domain to configure this option. See Adding endpoints using an AD domain server on page 54.
SAML	End user must provide their credentials for an SAML identity provider, such as Microsoft Entra ID (formerly known as Azure Active Directory), to connect to EMS. You must configure SAML settings to configure this option. See SAML Configuration on page 502.

j. In the *Comments* field, enter any comments if desired. Click *Save*.

End users receive an email or SMS notification as configured that includes the configured invitation code and installer. They can install FortiClient on their devices using the included installer, and enter the invitation code in the *Register with Zero Trust Fabric* field on the *FortiClient Zero Trust Telemetry* tab to connect to EMS if their FortiClient did not connect automatically to EMS after installation. Based on the verification type configured in the invitation code, the user may also need to enter their credentials to connect to EMS.

Configuring user verification with an LDAP server for authentication

The following provides an example of configuring user verification, using an LDAP server for authentication. This example sends the invitation code to a single user. This configuration consists of the following steps:

1. The EMS administrator adds the LDAP server to EMS.
2. The EMS administrator configures an invitation code, and send the invitation code to the desired user.
3. The end user receives the invitation email, and uses it to download FortiClient.
4. The end user connects to EMS using their Active Directory (AD) credentials.

To add the LDAP server to EMS:

1. Go to *Administration > Authentication Servers*.
2. Click *Add*.
3. In the *IP address/Hostname* field, enter the server IP address.
4. In the *Username* and *Password* fields, provide the credentials required to access the LDAP server.
5. Enable *LDAPS connection* and upload a certificate authority certificate or server certificate file in PEM or DER format.
6. If needed, configure other fields.
7. Click *Test*.
8. After the test succeeds, click *Save*. After a few minutes, EMS imports devices from the LDAP server.

To create an invitation code:

1. Go to *User Management > Invitations*.
2. Click *Add*.
3. Configure the invitation:
   a. In the *Name* field, enter the desired invitation name.
   b. For *Type*, select *Individual*.
   c. Enable *Send Email Notifications*.
   d. In the *Email Recipients* field, enter the desired user email address.
   e. In the *Include FortiClient Installer* field, add a FortiClient deployment package. The email that the user receives includes a link to download this deployment package.
   f. If desired, use the *Expiring* and *Expiry Date* fields to set an expiry date for this invitation.
   g. For *Verification Type*, select *LDAP*.
   h. From the *LDAP Domain User* dropdown list, select the desired domain user. This option is available when configuring an invitation to send to an individual. When configuring a bulk invitation, you select an LDAP domain instead of a domain user.
4. Click *Save*.

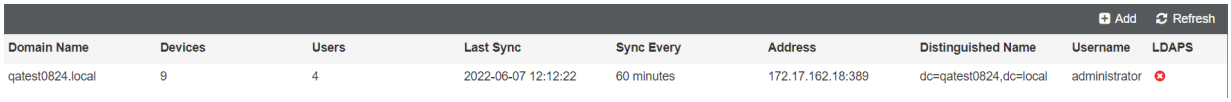
To install FortiClient on the user device:

1. The endpoint user receives the invitation email. They click the download link the email to download the FortiClient deployment package.
2. The user uses the deployment package to install FortiClient on their endpoint.
3. Once the install completes, FortiClient launches and prompts for the user to enter their AD credentials. EMS verifies that the credentials match a known user in the AD domain that was configured in the invitation code and allows the user to connect to FortiEndpoint.

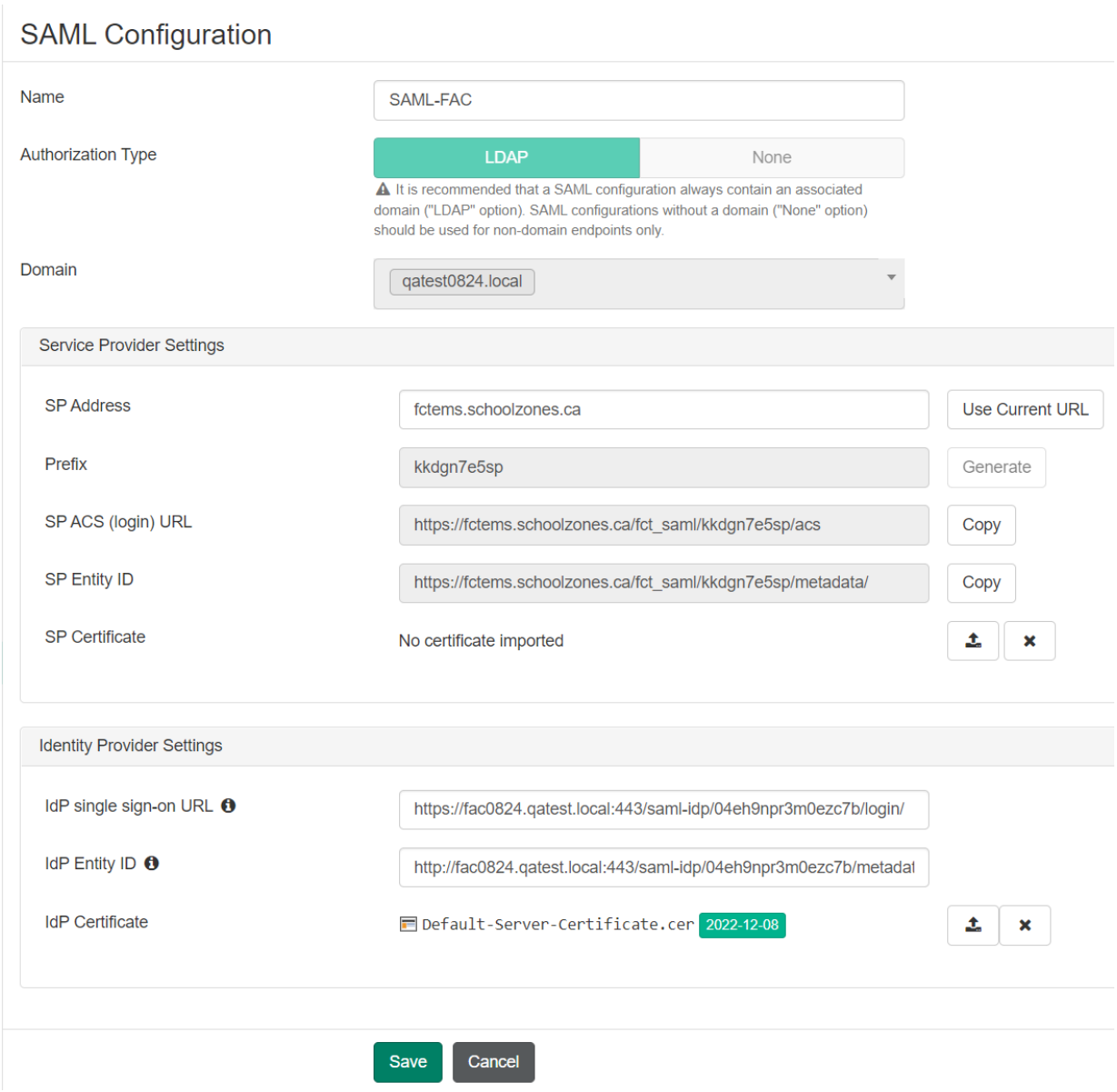
Configuring user verification with SAML authentication and an LDAP domain user account

To configure individual onboarding with SAML authentication using an LDAP domain user account:

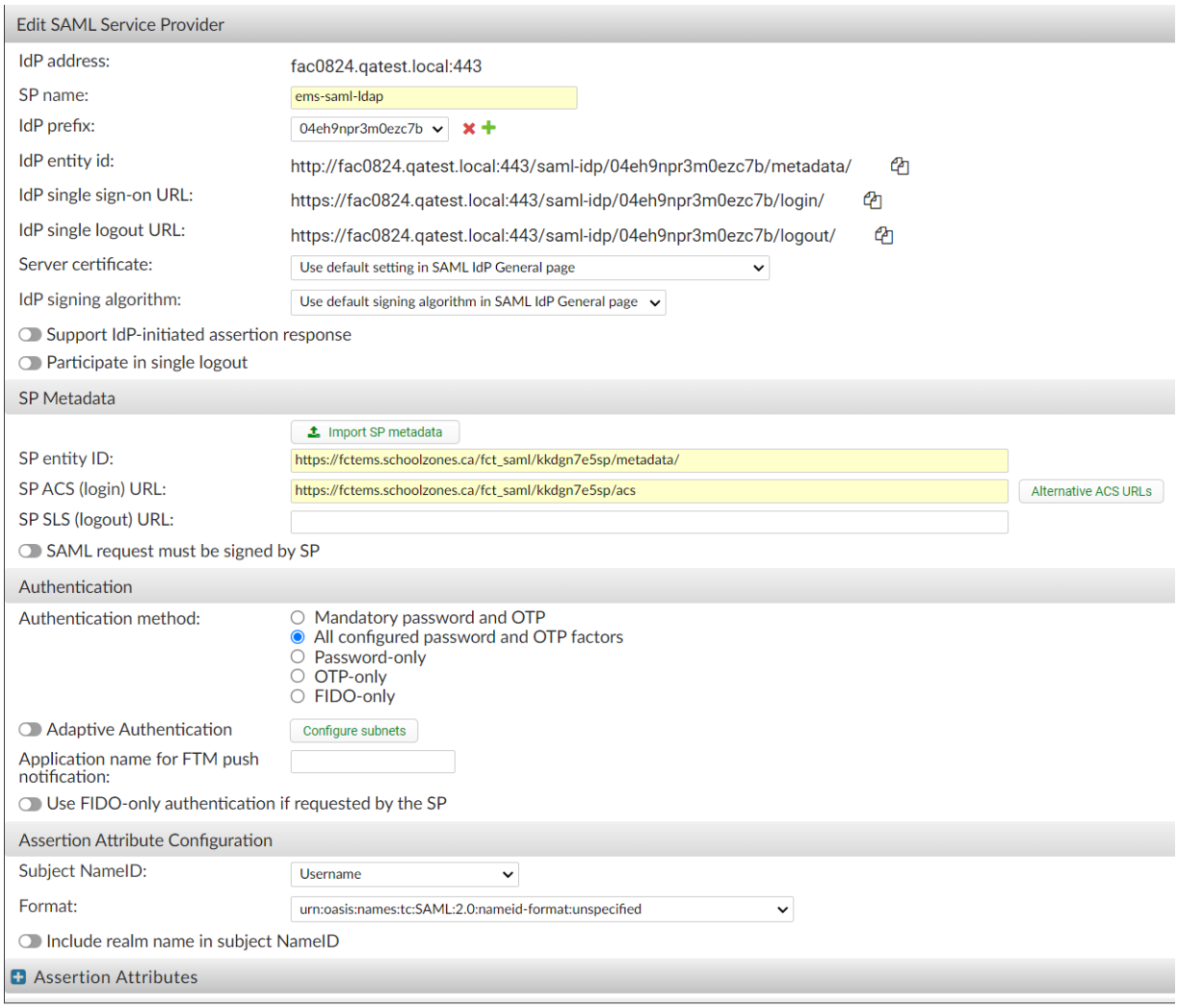
1. Configure EMS:
   a. In EMS, go to *Endpoints* > *Manage Domains*.
   b. Import the desired Active Directory domain. During the onboarding process, EMS authenticates user identities based on this domain. In this example, the domain is qatest0824.local.

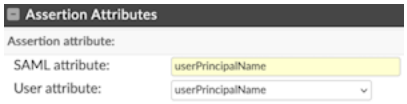


   c. Go to *User Management* > *SAML Configuration*.
   d. Add a SAML configuration with the imported domain. For *Authorization Type*, select *LDAP*. From the *Domain* dropdown list, select the newly imported domain. In this configuration, EMS is the service provider (SP), and FortiAuthenticator is the identity provider (IdP). Under *Identity Provider Settings*, enter your FortiAuthenticator details. Click *Save*.

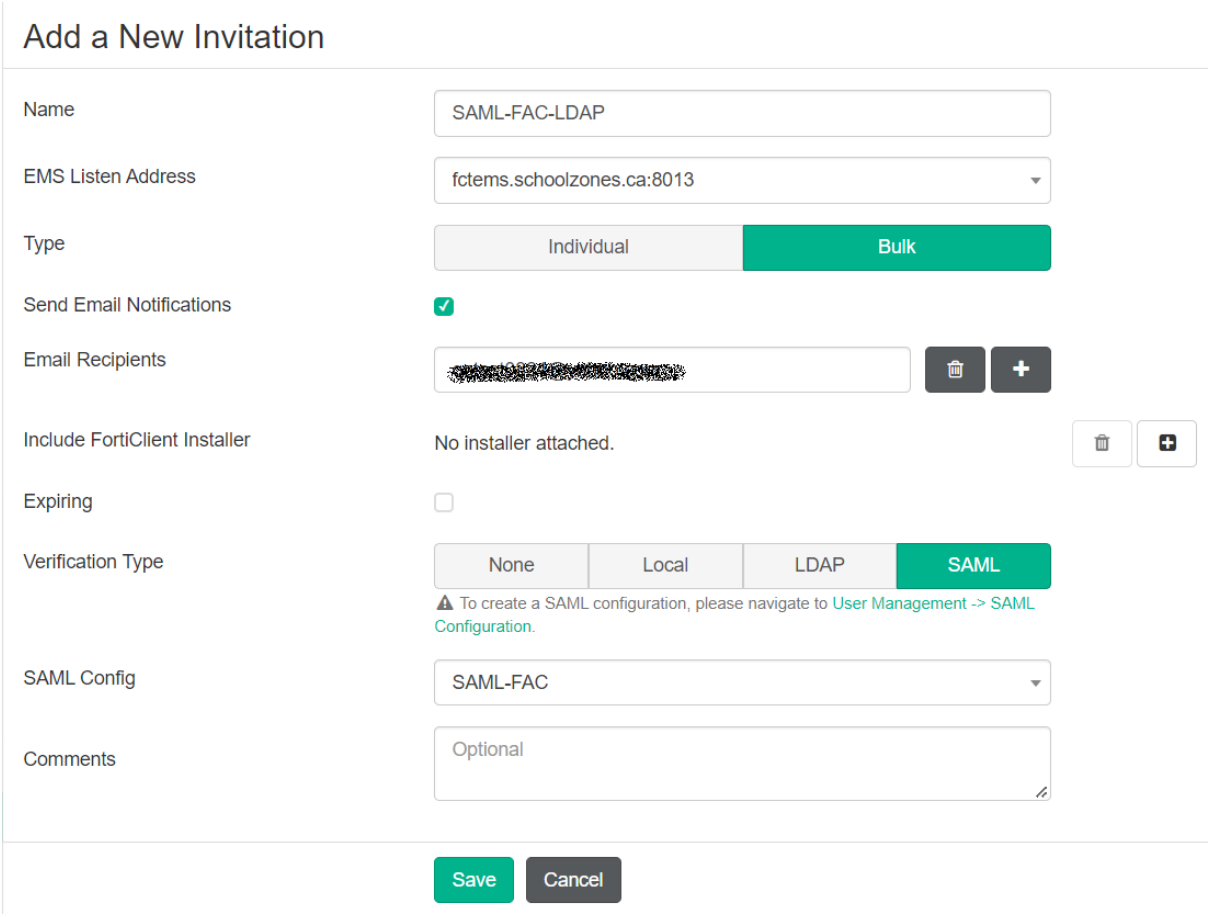

SAML Configuration
Name
SAML-FAC
Authorization Type
LDAP
None
It is recommended that a SAML configuration always contain an associated domain ("LDAP" option). SAML configurations without a domain ("None" option) should be used for non-domain endpoints only.
Domain
qatest0824.local
Service Provider Settings
SP Address
fctems.schoolzones.ca
Use Current URL
Prefix
kkdgn7e5sp
Generate
SP ACS (login) URL
https://fctems.schoolzones.ca/fct_saml/kkdgn7e5sp/acs
Copy
SP Entity ID
https://fctems.schoolzones.ca/fct_saml/kkdgn7e5sp/metadata/
Copy
SP Certificate
No certificate imported
Identity Provider Settings
IdP single sign-on URL
https://fac0824.qatest.local:443/saml-idp/04eh9npr3m0ezc7b/login/
IdP Entity ID
http://fac0824.qatest.local:443/saml-idp/04eh9npr3m0ezc7b/metadat
IdP Certificate
Default-Server-Certificate.cer
2022-12-08
Save
Cancel

e. In FortiAuthenticator, configure EMS as an SP.

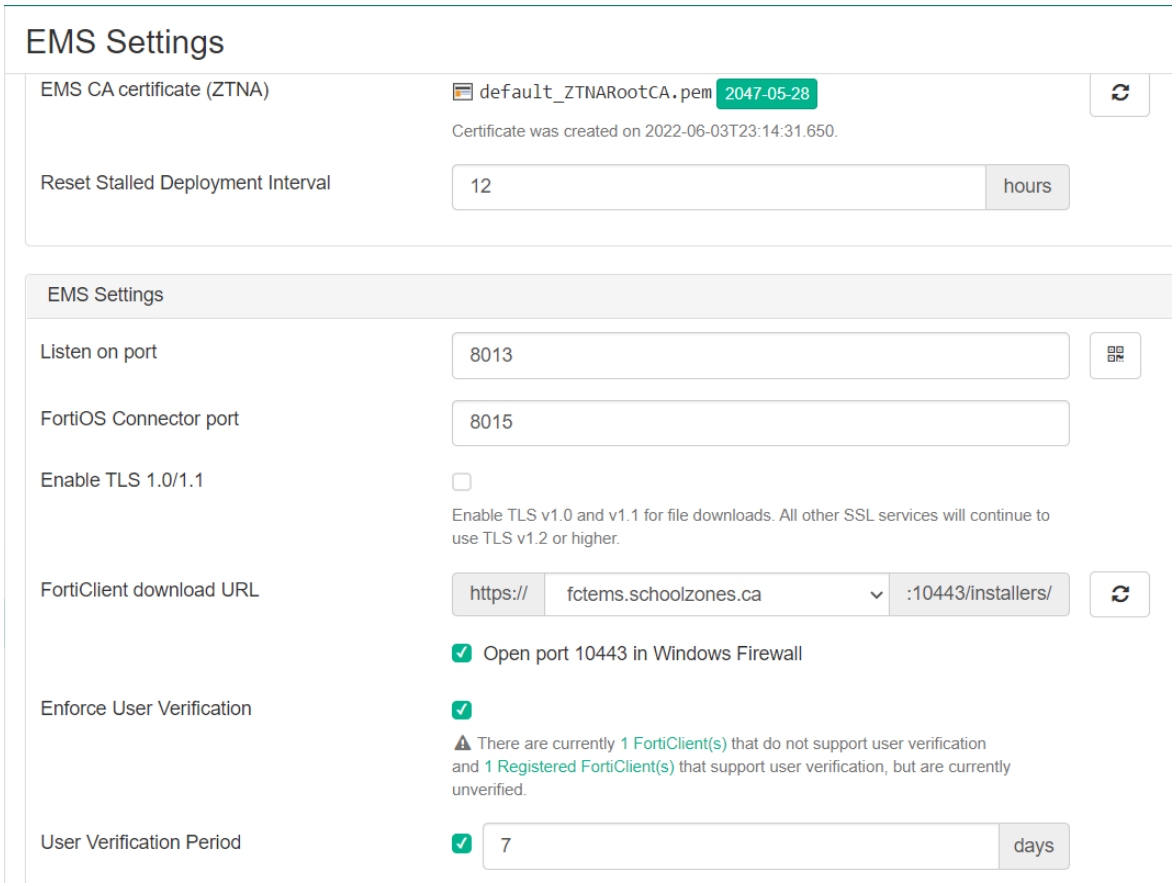




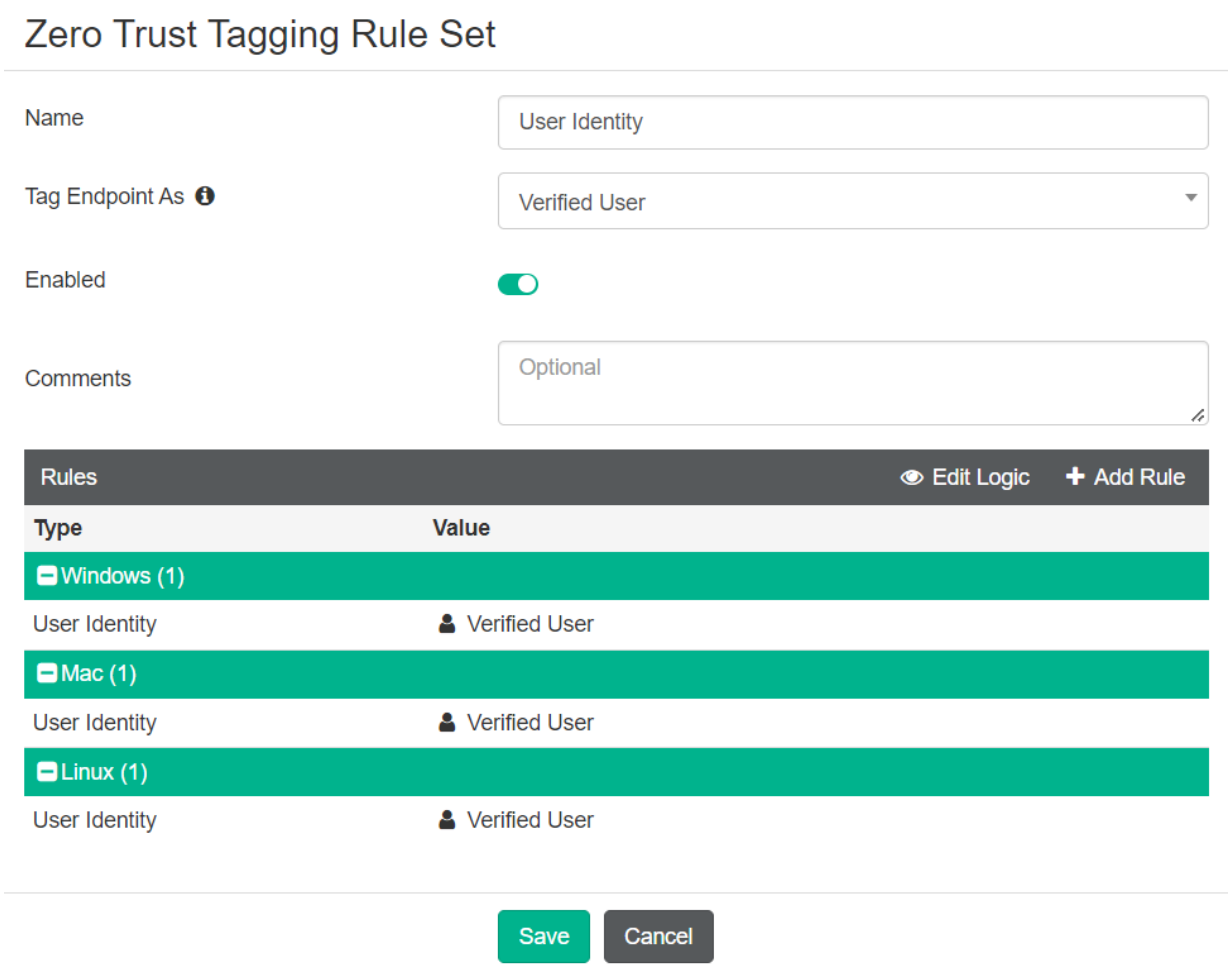
f. In EMS, go to *User Management* > *Invitations*. Click *Add*. Configure the desired recipients to receive their invitation codes over email. For *Verification Type*, select *SAML*. From the *SAML Config* dropdown list, select the SAML configuration that you created. Click *Save*.



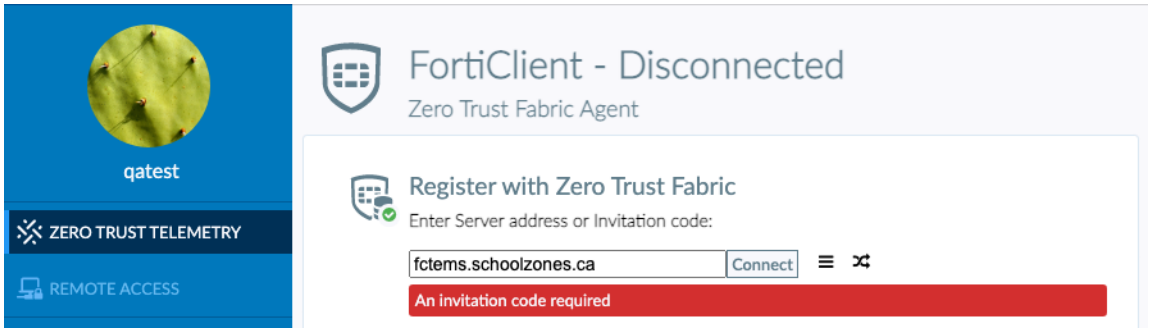
g. Go to *System Settings > EMS Settings*. Enable *Enforce User Verification*. This forces FortiClient to register to EMS using user onboarding.



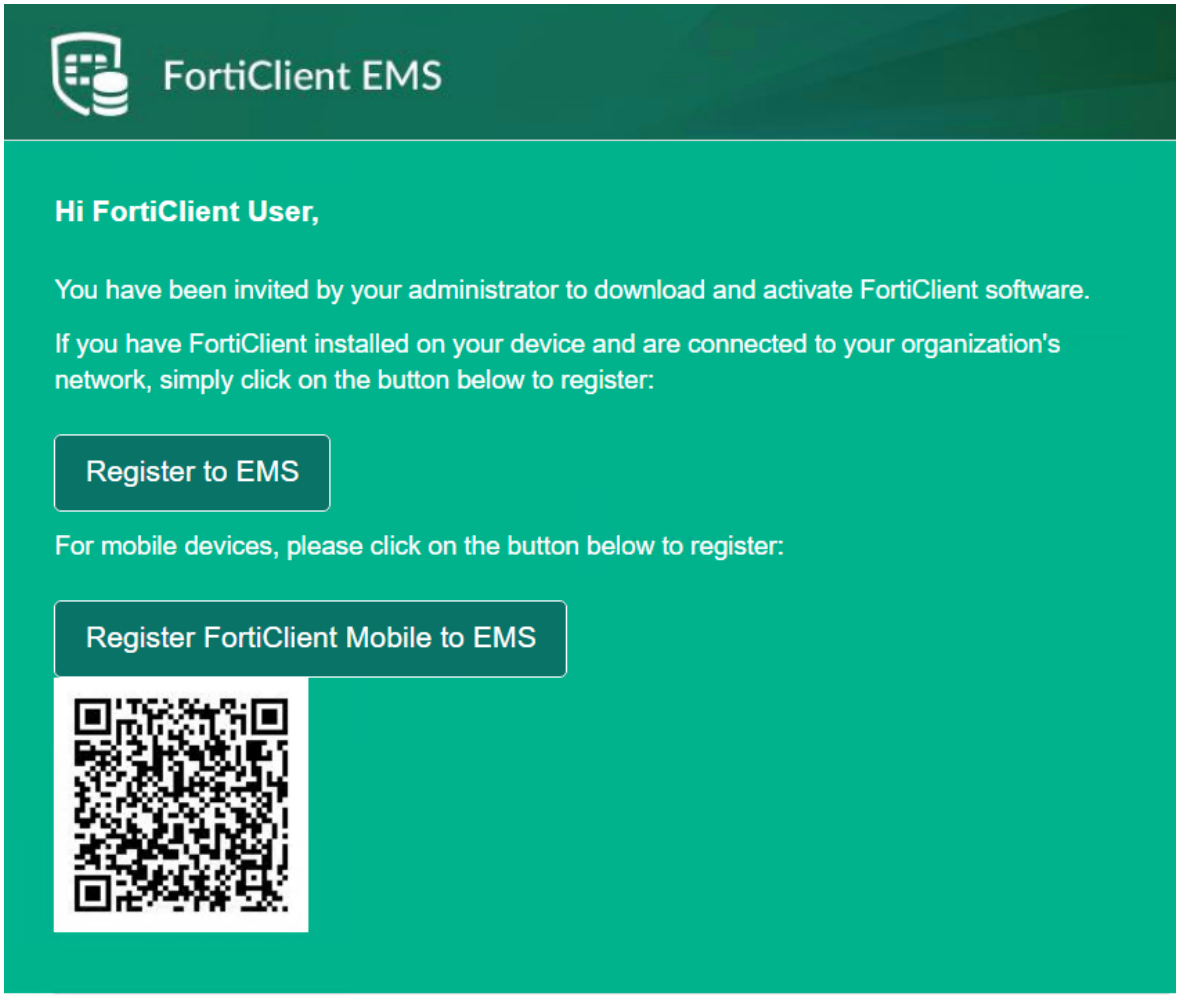
h. Go to *Security Posture Tags > Security Posture Tagging Rules*. Add a security posture tagging rule to tag registered endpoints with verified users.



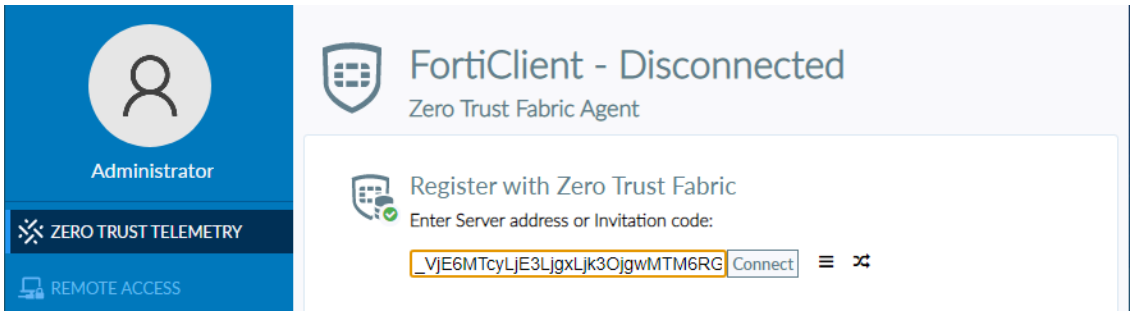
2. In FortiClient on an unregistered endpoint, attempt to register to EMS using the EMS fully qualified domain name. EMS rejects the connection attempt. FortiClient displays an error that EMS require an invitation code.



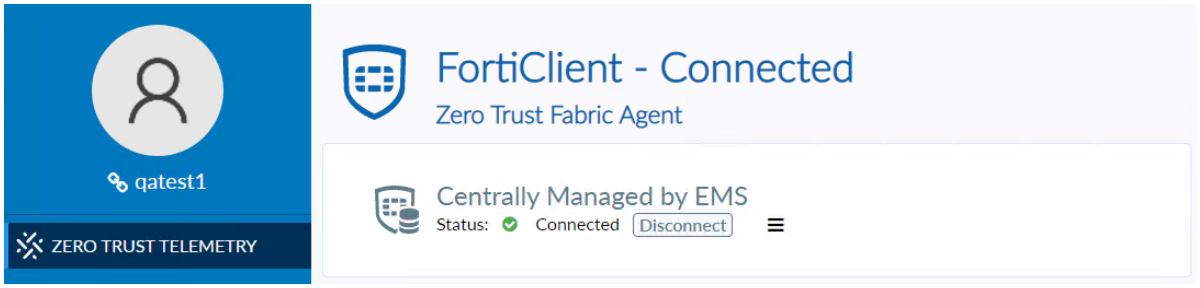
3. Register FortiClient to EMS:
   a. Do one of the following to start the process of registering FortiClient to EMS:
      i. Open the invitation email. and click *Register to EMS*. Follow the instructions to register to EMS.



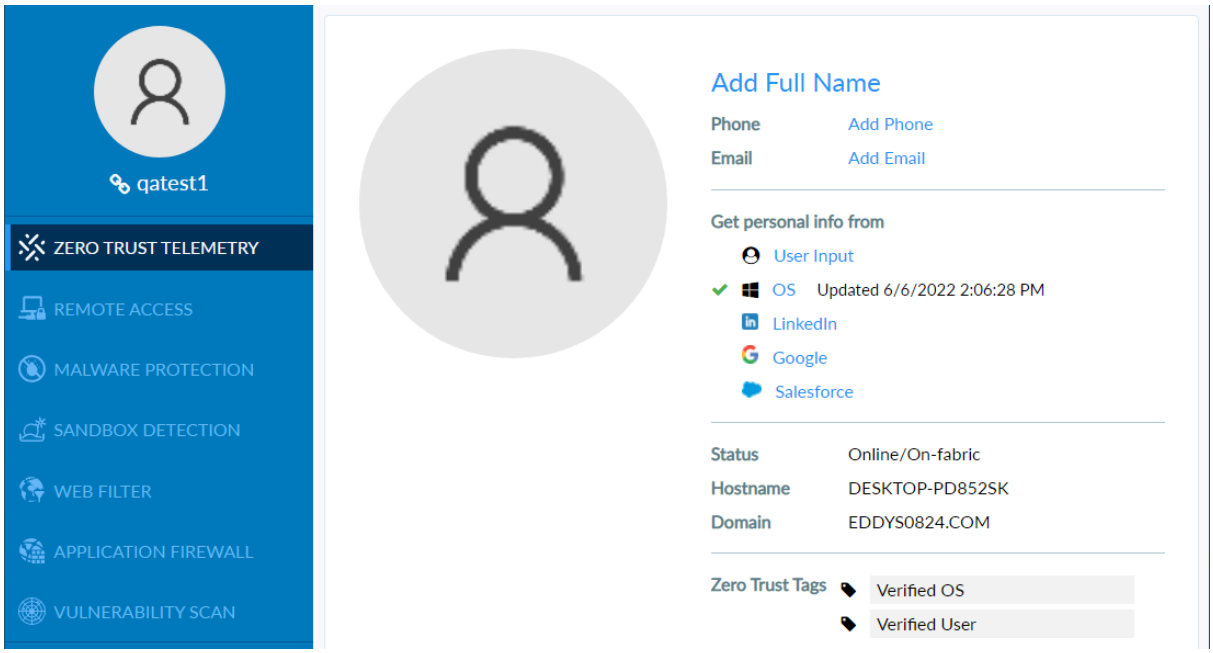
      ii. Open the invitation email, and copy the invitation code. Enter the invitation code on the *Zero Trust Telemetry* tab, and click *Connect*.



b. In the popup, provide your LDAP user credentials, then click *Login*. FortiClient proceeds with the registration process after authentication succeeds. After FortiClient successfully registers to EMS, the username in FortiClient changes to the verified user account, and a chain icon appears beside the username to indicate that FortiClient is registered with a verified user.

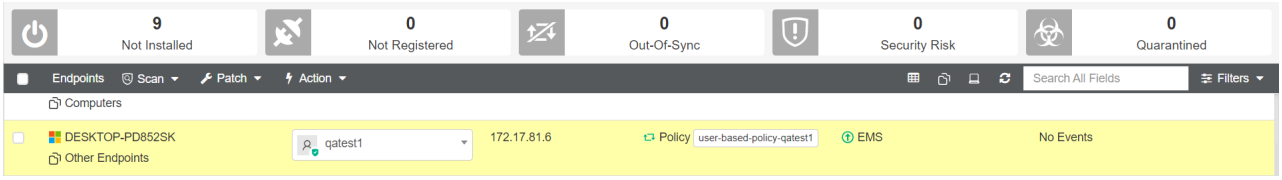


4. Go to the About page to confirm that the Verified User tag displays.

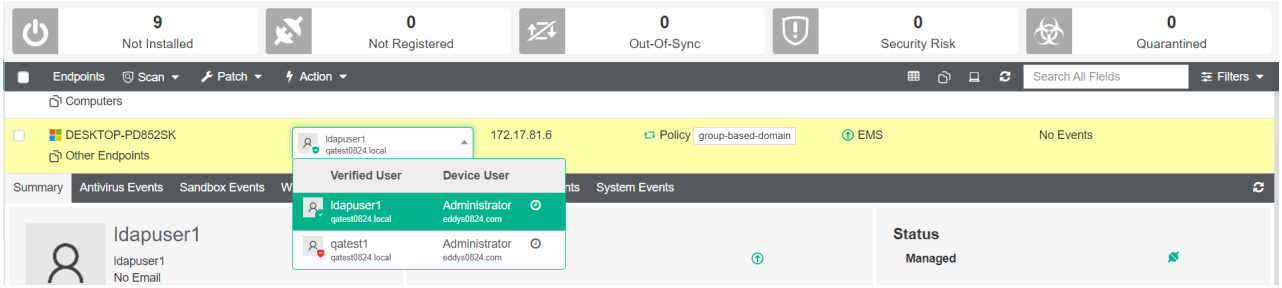


5. In EMS, go to *Endpoint Policy & Components* > *Managed Policies*. Create a policy to apply to the selected user. In the *Users* field, select the desired user. This policy takes priority over group-based policies that the endpoint may also be eligible for.

6. Go to *Endpoints* > *All Endpoints*. Select the endpoint. Confirm that EMS applied the user-specific policy that you created to the endpoint.



7. On the same endpoint, register FortiClient with a new user. the endpoint summary displays a new active user. As the endpoint is no longer eligible for the user-specific policy, EMS applies a group-based policy to the endpoint instead. You can view all registered users for that endpoint.



Configuring user verification with Entra ID authentication

This feature only applies to Entra ID-joined Windows endpoints, which has `AzureAdJoined : YES` in the output if you run `dsregcmd /status`.

The following provides an example of configuring user verification, using an Microsoft Entra ID server for authentication. This configuration consists of the following steps:

1. The EMS administrator adds the Entra ID server to EMS.
2. The EMS administrator configures an invitation code, and send the invitation code to the desired user.
3. The end user receives the invitation email, and uses it to download FortiClient.
4. The end user connects to EMS using their Entra ID credentials.

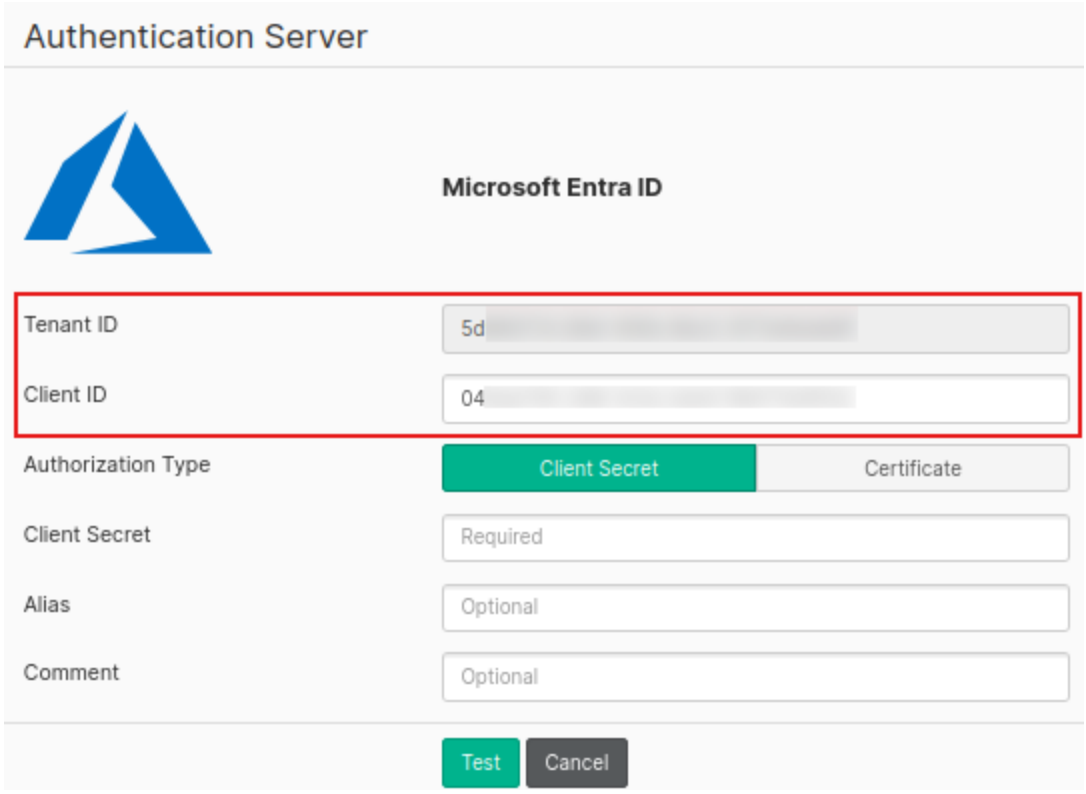
To configure the Azure tenant app for initiating passthrough (domain):

1. Configure the redirect URL:
   a. In the Azure portal, go to *App registration*. Copy the application or client ID of the application used to connect with EMS.
   b. Click the application, then click the *Redirect URIs* link.
   c. Click *Add a Platform* > *Select Mobile and Desktop applications*.
   d. Add the following URL: `ms-appx-web://microsoft.aad.brokerplugin/<application client ID>`.
   e. Under *Allow public client flows*, toggle to *Yes* for *Enable the following mobile and desktop flows*.
   f. Save the configuration.
2. Go to *Roles and administrators*.
3. Search for and select *Directory Readers*.
4. Click *Add assignments*.

5. Select the application used to connect with EMS.
6. Add desired users to the application in Entra ID:
   a. Go to *Enterprise applications*, and select the application used to connect with EMS.
   b. Go to *Users and groups*.
   c. Click *Add user/group*, and select the users that you will invite to EMS using an invitation code.
7. If an MFA-based Conditional Access policy is configured in Entra ID, temporarily disable it as Entra ID verification does not support MFA during EMS onboarding.

To configure an Entra ID server in EMS:

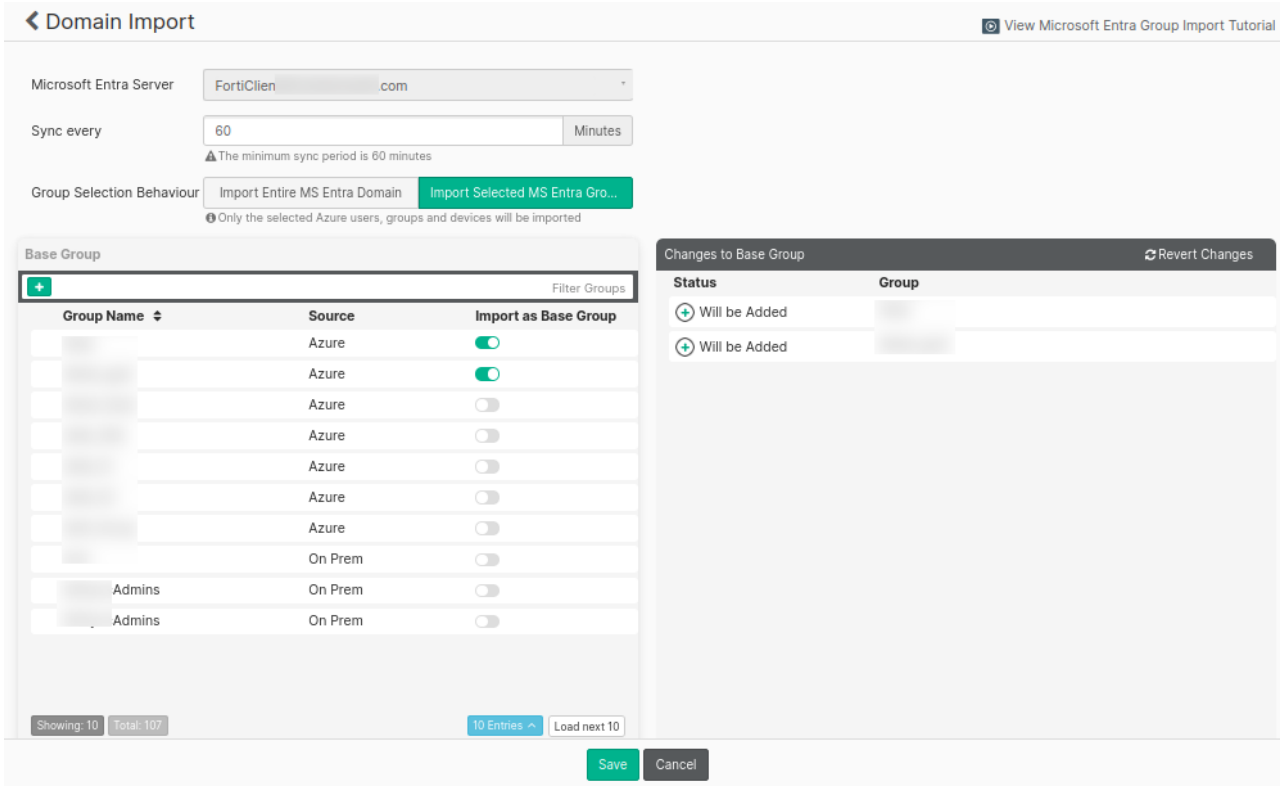
1. Configure the Entra ID server as an authentication server in EMS:
   a. In the Azure management console, collect your tenant ID, client ID, and client secret.
   b. In EMS, go to *Administration* > *Authentication Servers*.
   c. Click *Add* > *Microsoft Entra*.
   d. In the *Tenant ID* and *Client ID* fields, enter the IDs that you collected from the Azure management console.
   e. For *Authorization Type*, select *Client Secret*.
   f. In the *Client Secret* field, enter the client secret that you collected from the Azure management console.
   g. Configure other fields as desired.
   h. Click *Test*.



   i. After the test succeeds, click *Save*.

To add endpoints using an Entra ID server:

1. Go to *Endpoints* > *Manage Domains*.
2. Click *Add*, then *Azure*.
3. From the *Azure Server* dropdown list, select the desired server.
4. In the *Sync every* field, enter the number of minutes after which EMS syncs with the Azure server.
5. For *Group Selection Behaviour*, select *Import Entire Azure Domain* or *Import Selected Azure Groups*.
6. Enable *Import as Base Group* for the desired groups, then click *Save*.



Endpoints > *Domains* lists the Entra ID server domain groups and subgroups. It lists subgroups as a flat list and does not preserve the hierarchy from the Entra ID server.

To create an invitation code:

1. Go to *User Management* > *Invitations*.
2. Click *Add*.
3. Configure the invitation:
   a. In the *Name* field, enter the desired invitation name.
   b. For *Type*, select *Individual*.
   c. Enable *Send Email Notifications*.
   d. In the *Email Recipients* field, enter the desired user email address.
   e. In the *Include FortiClient Installer* field, add a FortiClient deployment package. The email that the user receives includes a link to download this deployment package.
   f. If desired, use the *Expiring* and *Expiry Date* fields to set an expiry date for this invitation.

g. For *Verification Type*, select *LDAP*.
h. From the *LDAP Domain User* dropdown list, select the desired domain user. This option is available when configuring an invitation to send to an individual. When configuring a bulk invitation, you select an LDAP domain instead of a domain user.

4. Click *Save*.

To register an Entra ID user's endpoint to EMS using an invitation code:

1. Add an invitation:
   a. In the EMS top banner, click *Invitations*.
   b. Click *Add*.
   c. For *Verification Type*, select *Domain*.
   d. From the *LDAP Domain* dropdown list, select the Entra ID server.
   e. Configure settings as desired, then click *Save*.
2. On the endpoint, go to *Settings > Accounts > Access work or school*.
3. Click *Connect*.
4. Log in as an Entra ID user.
5. In FortiClient, on the *Zero Trust Telemetry* tab, enter the invitation code to register to EMS. FortiClient register to EMS as the logged in Entra ID user without additional prompts.

Configuring user verification with SAML authentication and an Entra ID server user account

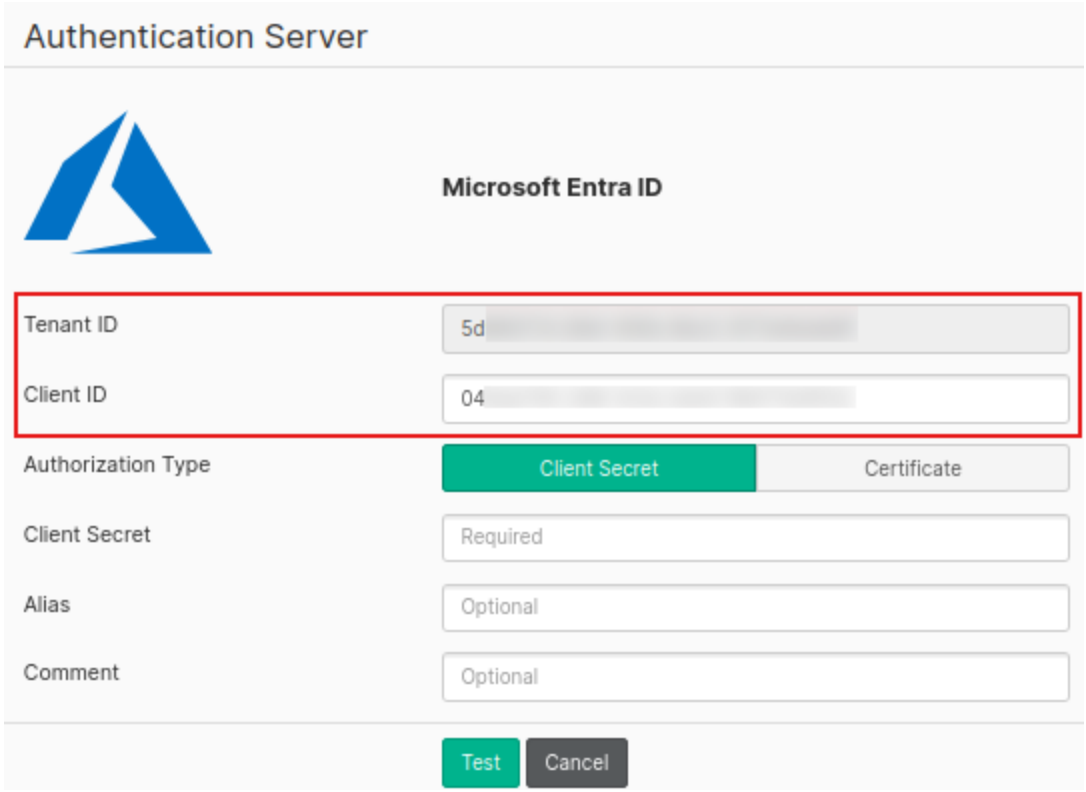
The following provides an example of configuring user verification, using a Microsoft Entra ID (formerly known as Azure Active Directory (AD)) server for authentication. This configuration consists of the following steps:

1. The EMS administrator adds the Entra ID server to EMS.
2. The EMS administrator creates a SAML configuration in EMS, with EMS as the service provider (SP) and the Entra ID server as the identity provider (IdP).
3. The EMS administrator configures an invitation code, and send the invitation code to the desired user.
4. The end user receives the invitation email, and uses it to download FortiClient.
5. The end user connects to EMS using their Entra ID credentials.

To configure an Entra ID server in EMS:

1. Configure the Entra ID server as an authentication server in EMS:
   a. In the Azure management console, collect your tenant ID, client ID, and client secret.
   b. Go to *Administration > Authentication Servers*.
   c. Click *Add > Azure*.
   d. In the *Tenant ID* and *Client ID* fields, enter the IDs that you collected from the Azure management console.
   e. For *Authorization Type*, select *Client Secret*.

f. In the *Client Secret* field, enter the client secret that you collected from the Azure management console.
g. Configure other fields as desired.
h. Click *Test*.

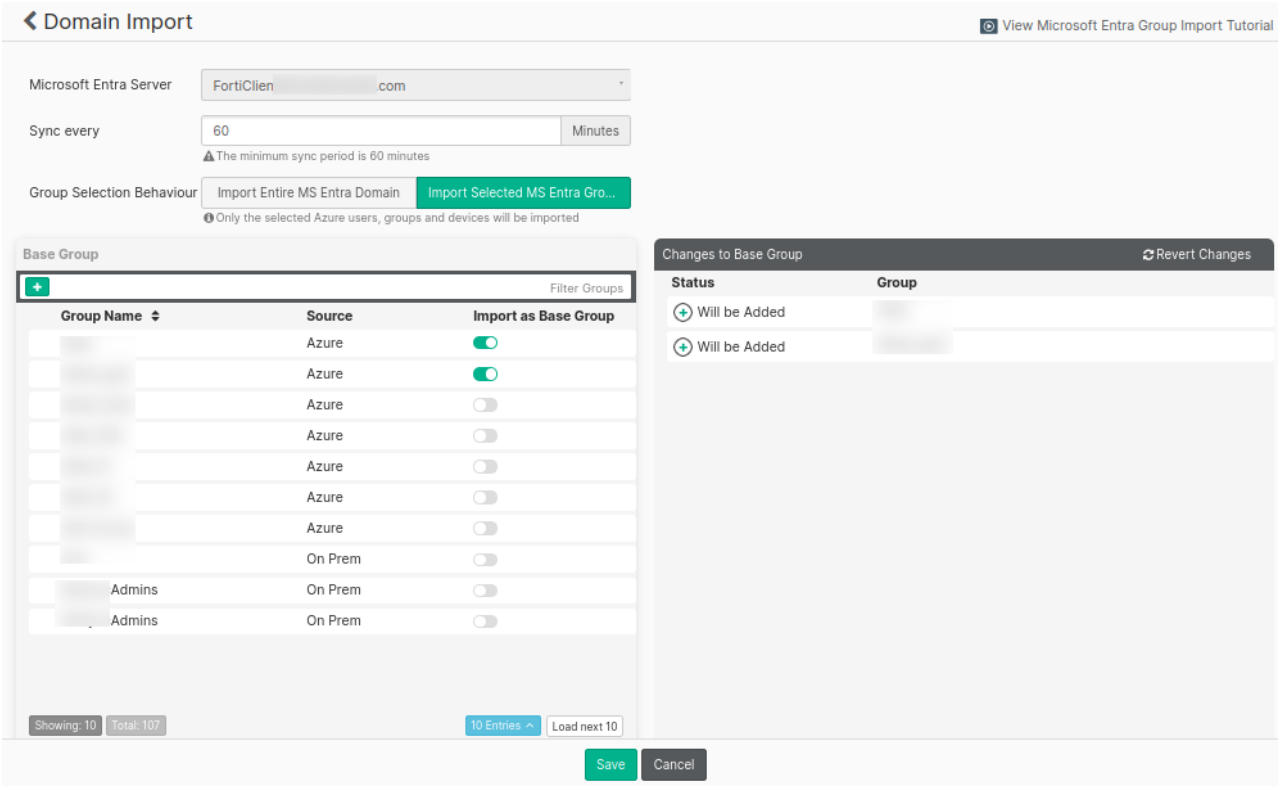


i. After the test succeeds, click *Save*.

To add endpoints using an Entra ID server:

1. Go to *Endpoints* > *Manage Domains*.
2. Click *Add*, then *Azure*.
3. From the *Azure Server* dropdown list, select the desired server.
4. In the *Sync every* field, enter the number of minutes after which EMS syncs with the Azure server.
5. For *Group Selection Behaviour*, select *Import Entire Azure Domain* or *Import Selected Azure Groups*.

6. Enable *Import as Base Group* for the desired groups, then click *Save*.

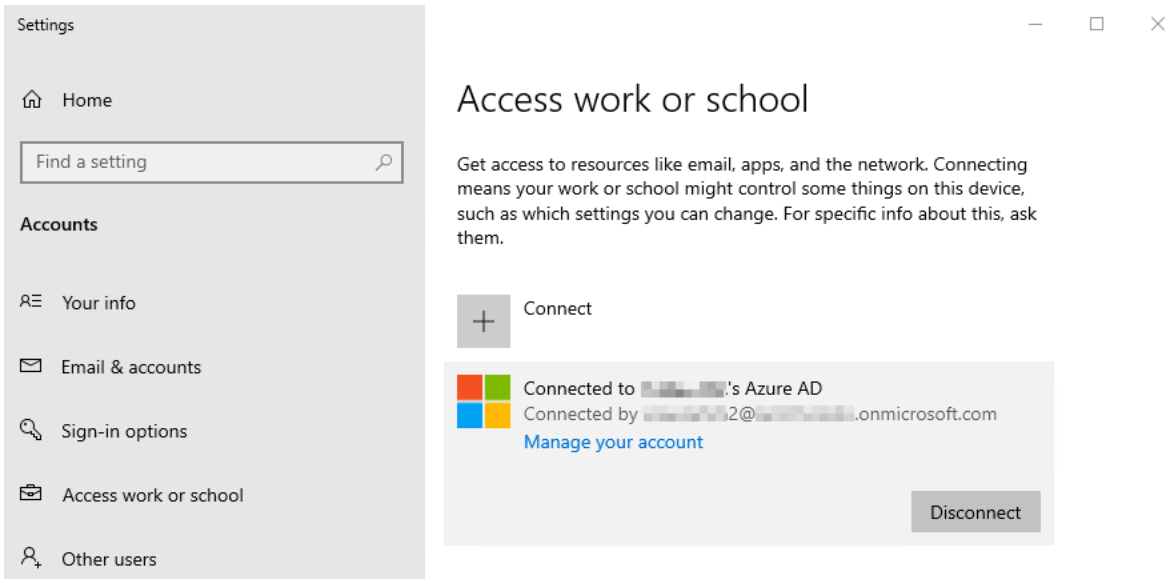


Endpoints > *Domains* lists the Entra ID server domain groups and subgroups. It lists subgroups as a flat list and does not preserve the hierarchy from the Entra ID server.

To register an Entra ID user's endpoint to EMS using an invitation code:

1. In the EMS top banner, click *Invitations*.
2. Click *Add*.
3. For *Verification Type*, select *Domain*.
4. From the *LDAP Domain* dropdown list, select the Entra ID server.
5. Configure other settings as desired, then click *Save*.
6. On the endpoint, go to *Settings* > *Accounts*.
7. Under *Access work or school*, click *Connect*.

8. Log in as an Entra ID user.



9. In FortiClient, on the *Zero Trust Telemetry* tab, enter the invitation code to register to EMS. FortiClient register to EMS as the logged in Entra ID user without additional prompts.

To register an Entra ID user's endpoint to EMS using SAML:

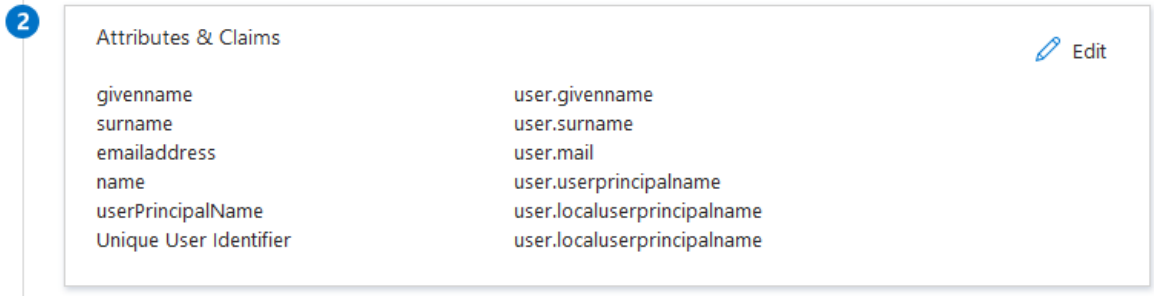
You must copy some values from the Azure portal to EMS and other values from EMS to the Azure portal to complete the configuration.

1. In EMS, create a SAML configuration:
   a. In EMS, go to *User Management* > *SAML Configuration*.
   b. Click *Add*.
   c. For *Authorization Type*, select *LDAP*.
   d. From the *Domain* dropdown list, select the Entra ID server.
   e. In this configuration, EMS acts as the service provider, while the Entra ID server is the identity provider. In the *SP Address* field, enter the EMS IP address or FQDN. You can also use the *Use Current URL* button to populate the field.
2. In Azure, add and configure the Entra ID SAML Toolkit:
   a. Go to *Enterprise applications*, then click *New application*.
   b. Search for and select *Microsoft Entra SAML Toolkit*.
   c. Configure a name for the toolkit as desired, then click *Create*.
   a. Click into the toolkit, select *Single sign-on*, then *SAML*.
   b. Under *Basic SAML Configuration*, click *Edit*.
   c. Copy the values from EMS in *User Management* > *SAML Configuration* > *Service Provider Settings* to the Azure portal. This table maps the EMS SAML fields that you must copy from EMS and configure in Entra ID. Configure as the table summarizes, then click *Save*.

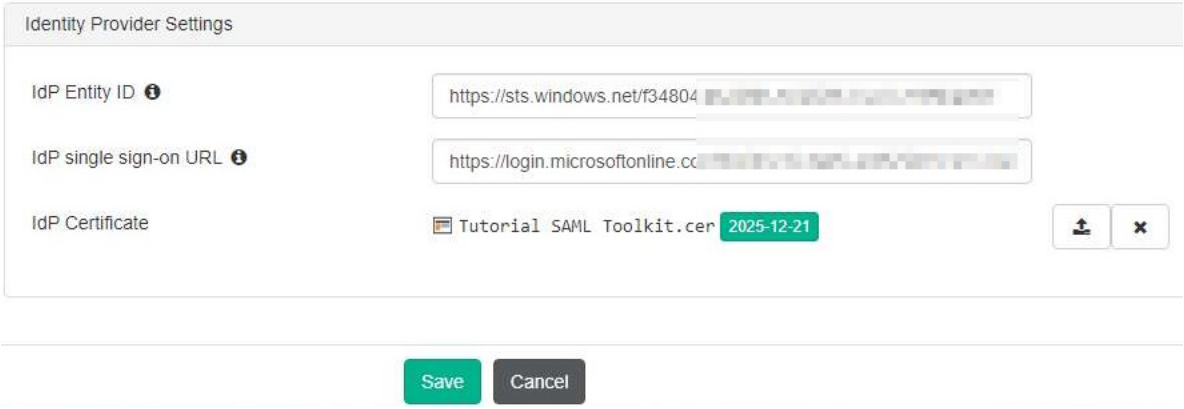
EMS SAML field	Entra ID Basic SAML Configuration field
SP Entity ID	Identifier (Entity ID)

EMS SAML field	Entra ID Basic SAML Configuration field
SP ACS (login) URL	Reply URL (Assertion Consumer Service URL)
SP Address	Sign on URL

d. Under *Attributes & Claims*, click *Edit*.
e. Click *Unique User Identifier*.
f. From the *Source attribute* dropdown list, select *user.localuserprincipalname*. Click *Save*.

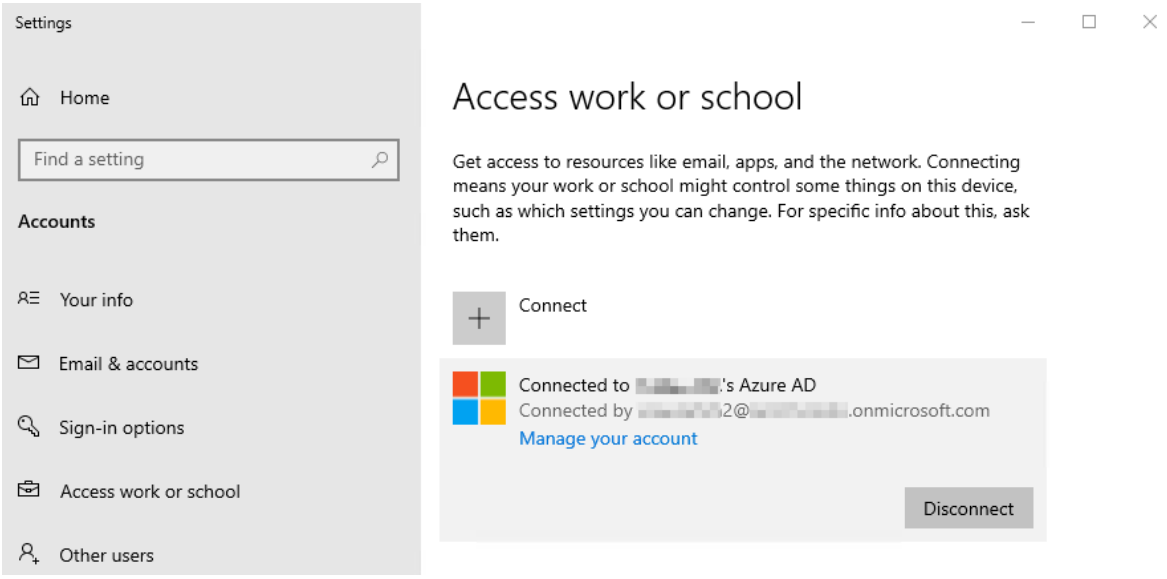


3. In Azure, add a new claim:
   a. Click *Add new claim*.
   b. In the *Name* field, enter the domain identification value from EMS. You can find this value on EMS in *User Management* > *SAML Configuration* > *Assertion Attributes* > *Domain Identification*. This field is only visible when *LDAP* is selected as the *Authorization Type* and the *Domain* field is populated in *SAML Configuration*.
   c. Ensure that *Namespace* is empty.
   d. From the *Source attribute* field, select *user.localuserprincipalname*. Click *Save*.
   e. Under *SAML Certificates*, download the *Certificate (Base64)* file.
4. Copy the URLs under *Set up Tutorial SAML Toolkit* to EMS:
   a. Copy the *Entra ID Identifier* value to the *IdP Entity ID* field in EMS.
   b. Copy the *Login URL* value to the *IdP single sign-on URL* field in EMS.
   c. In the IdP certificate field, upload the certificate that you downloaded in step 3. Save the SAML configuration in EMS.



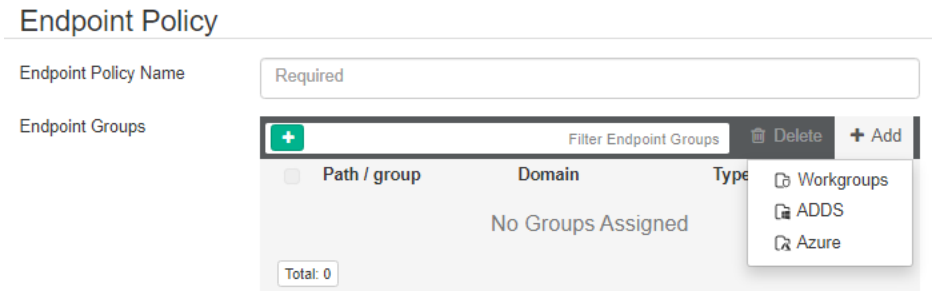
5. In Azure, go to *Users and groups*. Add users to the list as desired. Azure authorizes any user added to this list to connect to EMS.

6. Configure the invitation in EMS:
   a. In the top banner, click *Invitations*.
   b. Click *Add*.
   c. For *Verification Type*, select *SAML*.
   d. From the *SAML Config* dropdown list, select the SAML configuration.
   e. Configure other settings as desired, then click *Save*.
7. You can authenticate the endpoint using Entra ID by doing one of the following:
   a. To join the device to the Entra ID server, do the following:
      i. On the endpoint, go to *Settings* > *Accounts*.
      ii. Under *Access work or school*, click *Connect*.
      iii. Log in as an Entra ID user.



      iv. In FortiClient, on the *Zero Trust Telemetry* tab, enter the invitation code to register to EMS. FortiClient register to EMS as the logged in Entra ID user without additional prompts.
   b. For a workgroup endpoint or an endpoint joined to an on-premise domain, in FortiClient, on the *Zero Trust Telemetry* tab, enter the invitation code to register to EMS. A Microsoft single sign on prompt displays. Enter the Entra ID user credentials to authenticate and connect FortiClient to EMS.

You can configure endpoint policies and deployment configurations for specific endpoint groups from an Entra ID server.



Configuring user verification with SAML authentication and an Okta user account

The following provides an example of configuring user verification, using an Okta server for authentication.

To configure user verification with SAML authentication and an Okta user account:

1. In EMS, start the SAML configuration:
   a. Go to *User Management > SAML Configuration*.
   b. Click *Add*.
   c. In the *Name* field, enter the desired name.
   d. For *Authorization Type*, select *None*.
   e. *Service Provider Settings* displays the *SP Address*, *SP Entity ID*, and *SP ACS (login) URL* fields. You use these values to configure FortiClient EMS as a service provider (SP) in Okta. Copy these values.
2. Create and configure your FortiClient EMS environment in Okta:
   a. In the Okta portal, go to *Applications* and click *Create App Integration*.
   b. Select *SAML 2.0* and click *Next*.
   c. Define an *App name* and click *Next*.
   d. On the *Configure SAML* page, provide the *Single sign-on URL* and *SP Entity ID* that you collected from EMS. Complete the wizard.
   e. Click *View SAML setup instructions*. Copy the *Identity Provider Single Sign-On URL* and *Identity Provider Issuer* values and download the certificate.
3. Configure the IdP information in FortiEndpoint:
   a. In FortiEndpoint, in the *IdP Entity ID* and *IdP single sign-on URL* fields, paste the values that you copied from the *IdP Entity ID* and *IdP Single Sign-On URL* fields, respectively.
   b. From the *IdP Certificate* dropdown list, select *Create*, then upload the certificate that you downloaded. Click *Next*.
4. Save the SAML configuration.

To register an Okta user's endpoint to EMS using SAML:

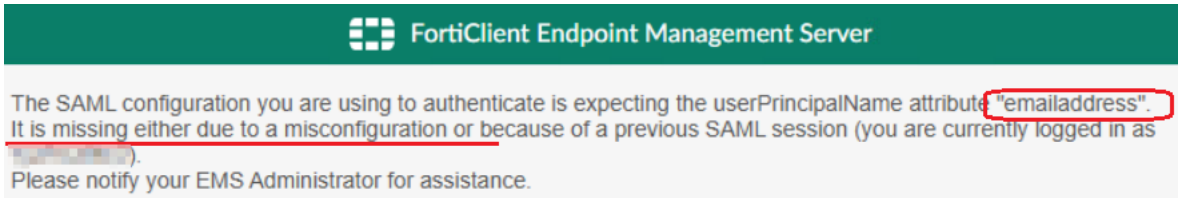
1. In the top banner, click *Invitations*.
2. Click *Add*.
3. For *Verification Type*, select *SAML*.
4. From the *SAML Config* dropdown list, select the Okta SAML configuration.
5. Configure other settings as desired, then click *Save*.
6. In FortiClient, on the *Zero Trust Telemetry* tab, enter the invitation code to register to EMS. A Okta single sign on prompt displays. Enter the Okta user credentials to authenticate and connect FortiClient to EMS.

Troubleshooting SAML user verification failure

This document covers multiple scenarios of SAML user verification failures as well as approaches to address them.

Missing attribute

The following error is an example of a user verification issue that is a result of misconfiguring the identity provider (IdP) (Microsoft Entra ID, Okta, and so on) or *Assertion Attributes* in EMS.



The error means that the "emailaddress" attribute configured on EMS is missing from the authentication response (SAML assertion).

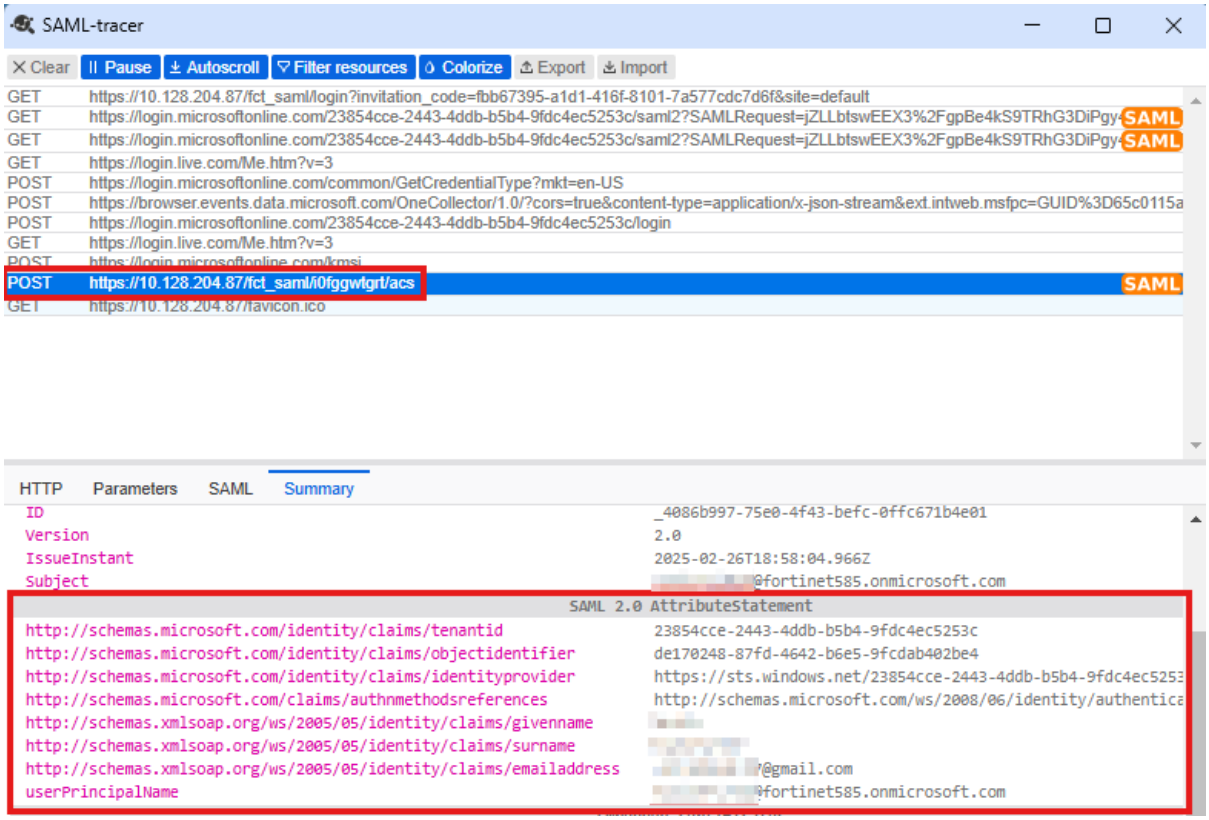
Go to *User Management* > *SAML Configuration* and confirm what is configured in the *Domain Identification* field.



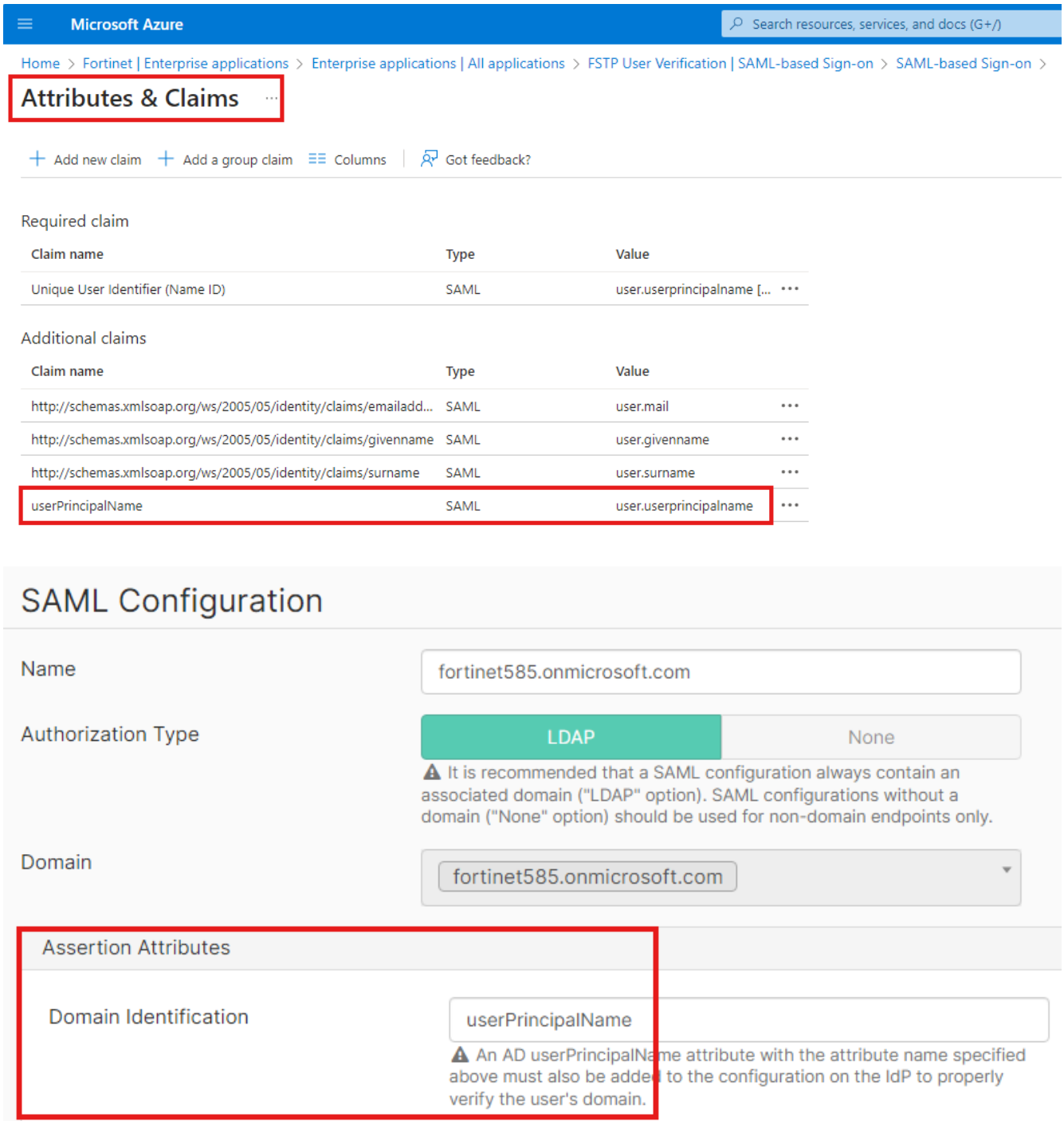
Based on the screenshot, EMS expects the "emailaddress" attribute in the SAML authentication response. This attribute holds the username in userPrincipalName format. EMS matches the domain name from the username value to the configured *Domain*. In this example, EMS matches the domain name against fortinet585.onmicrosoft.com, which is configured in the *Domain* field.

To debug this error:

1. Install a SAML tracer browser extension your default browser. See Test SAML app implementation with SAML-tracer. If using Microsoft Edge, use SAML, WS-Federation and OAuth 2.0 tracer.
2. Start the trace, close the browser, and attempt to connect to EMS.
3. A browser opens. Once authentication fails, pause the trace and click the URL ending with */acs*. This is marked with an orange SAML badge.
4. In the tracer, go to the *Summary* tab and view the attributes under *AttributeStatement*. In this example, the emailaddress attribute does not exist as configured in the *Domain Identification* attribute in EMS. If there are no attributes that exactly match the *Domain Identification* attribute configured on EMS, it results in the attribute missing error. In this example, you can rectify the error by configuring http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress in the *Domain Identification* attribute in EMS.

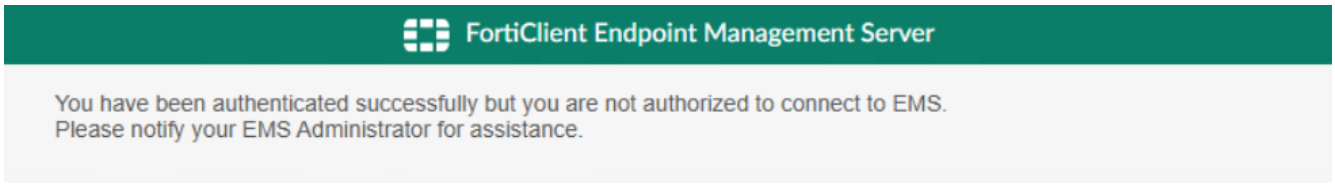


A correct configuration is one where the domain identification attribute configured in EMS matches one on the IdP. The following provides an example of a correct configuration in Entra ID. You can see that the *userPrincipalName* claim exists in the Entra ID portal under *Attributes & Claims* and that this is also configured in the *Domain Identification* field in EMS.

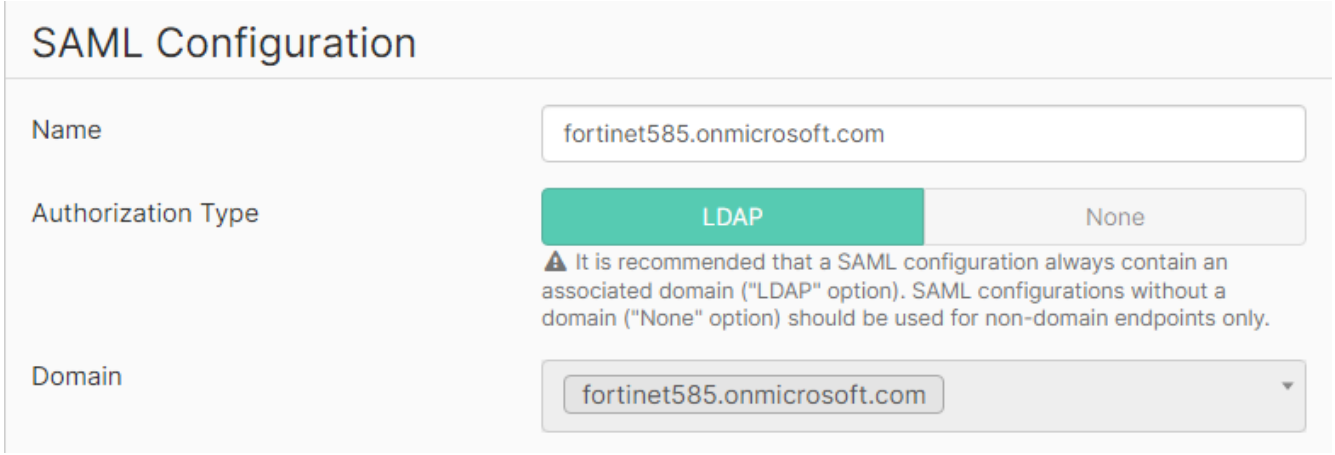


Authenticated but not authorized

The following shows an error that occurs when the IdP successfully authenticates a user but does not authorize them.



This error occurs when the username domain suffix does not match a domain configured for LDAP authorization.



The following are reasons why this may occur:

Misconfigured attributes

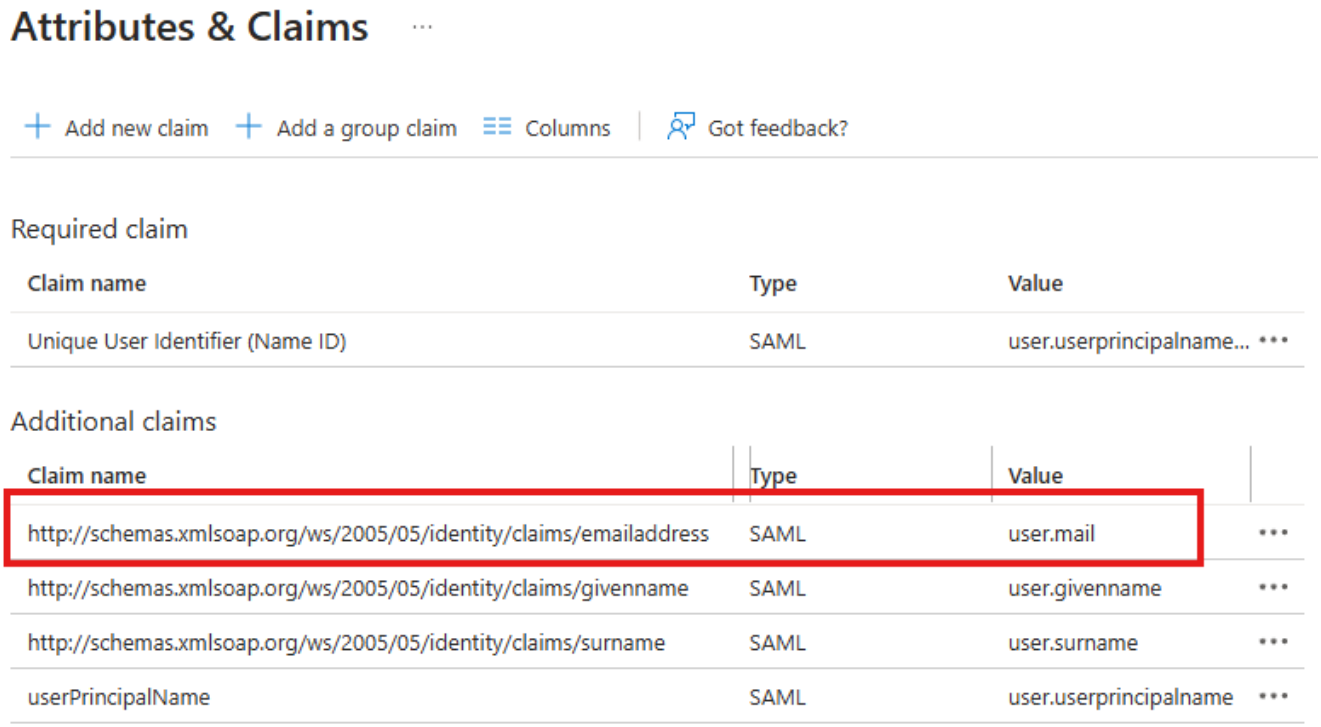
The SAML assertion attribute is misconfigured.

This is similar to Missing attribute on page 524, but in this case, the configured attribute matches between EMS and the IdP but the value carried within the attribute in the SAML assertion does not match a domain in the authentication server that you specified in the *Domain* setting in EMS.

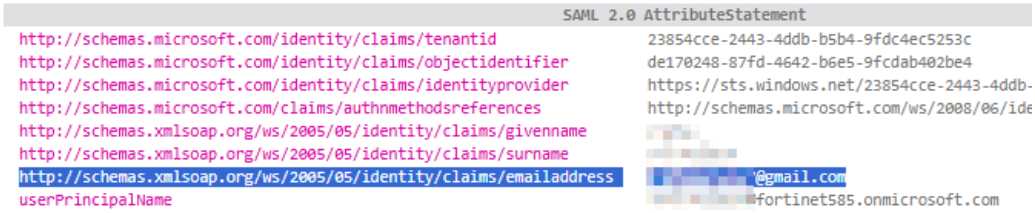
The following screenshots provide an example of this case. In EMS, *Domain Identification* is configured as https://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress.



In Entra ID, https://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress exists and has a value of user.mail.



The SAML tracer capture of the authentication response shows that the value for https://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress does not match the domain suffix that EMS expects, which is fortinet585.onmicrosoft.com. Instead, the value domain suffix is gmail.com. Therefore, authorization fails.



To correct this issue, ensure the following:

- Attributes match on the IdP and EMS.
- The attribute value (username) contains a domain suffix that matches the authentication server domain configured under *Domain* in EMS.
- The attribute value (username) contains a domain suffix that matches the authentication server domain configured under *Domain* in EMS.

Domain mismatch

This issue occurs when the domain configured on the IdP does not match the one imported to EMS.

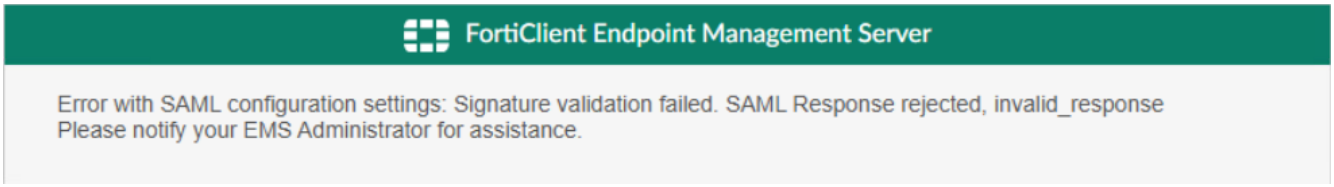
Hybrid environments are common, so you may use SAML for authentication using Entra ID and authorize against an Active Directory Domain Services domain. In this case, the domains' names may differ.

In this case, if you properly configured the attributes, the IdP authenticates users but cannot authorize them, since their username's domain suffix does not match a domain set for authorization. In this example, there is a mismatch between the *Domain* configured on EMS, which is *fortinet585.com*, and the domain suffix for the username that authenticates via SAML, which is *fortinet585.onmicrosoft.com*.

The solution is to ensure that the SAML and EMS imported domains match. If this is not possible, you can disable authorization by setting it to *None*.

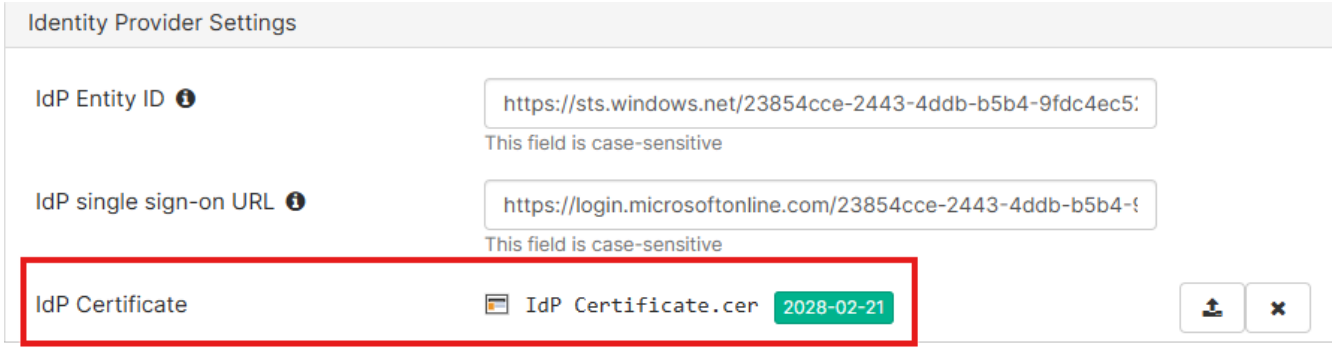
Signature validation failed

This error may display when signature verification fails:



This error occurs because an incorrect *IdP Certificate* is configured on EMS, which results in SAML authentication response validation failure.

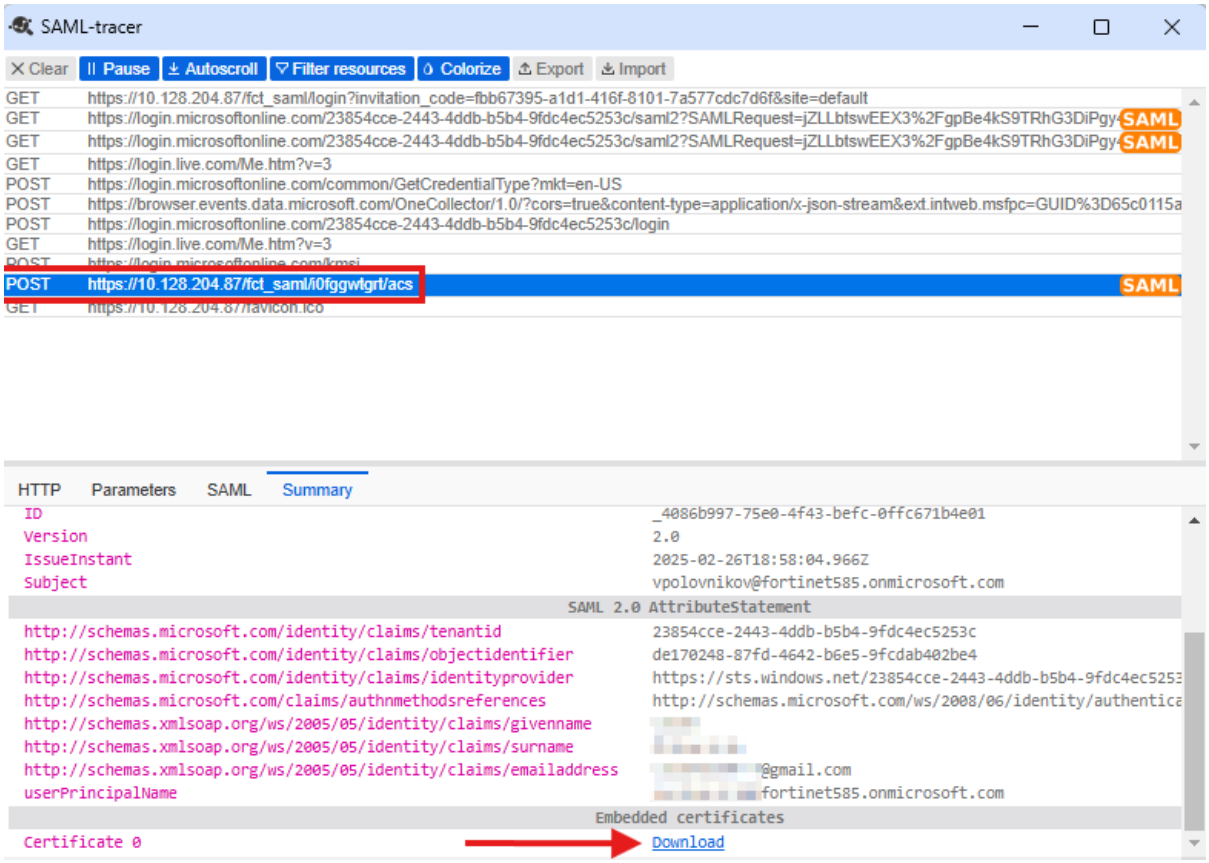
To fix this error, ensure that the certificate coming from the IdP is the same as the one configured on EMS under *IdP Certificate* .



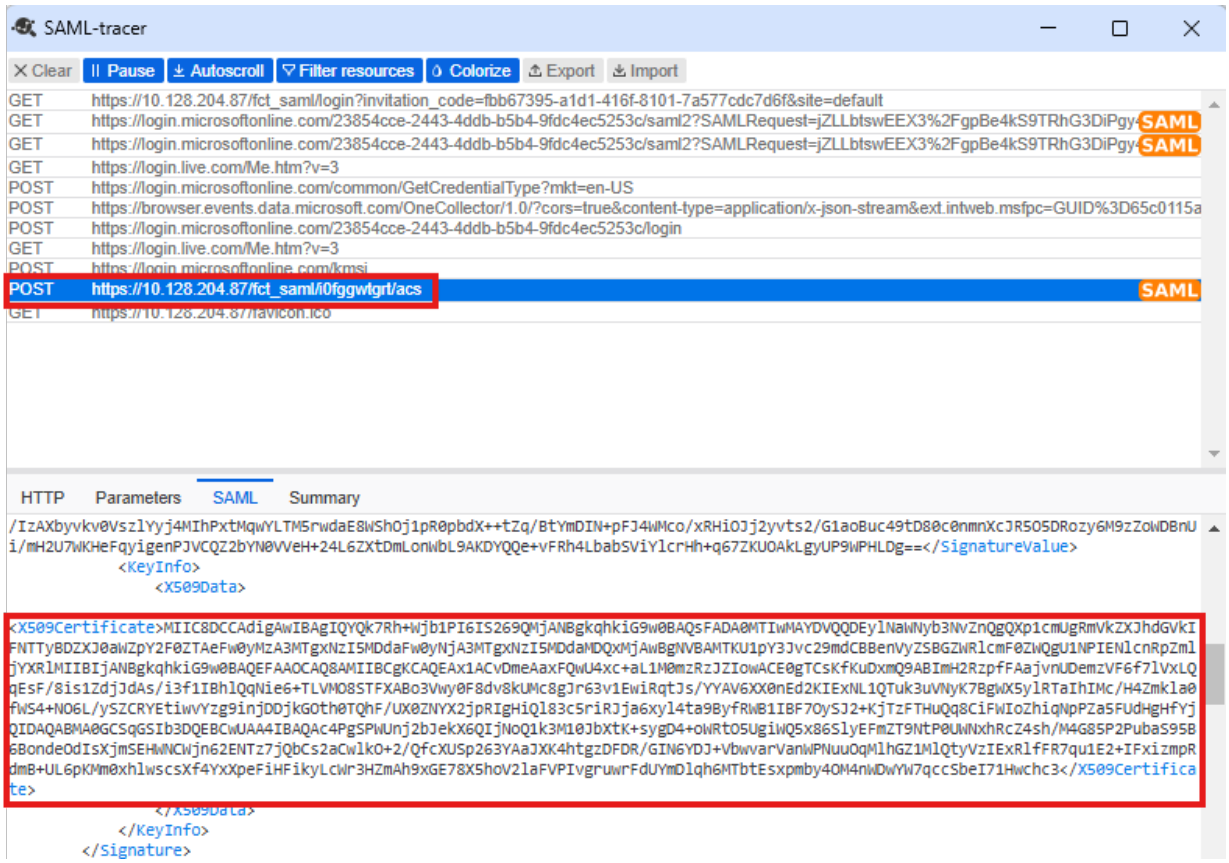
If desired, you can extract the IdP certificate via SAML-tracer.

To extract the IdP certificate via SAML-tracer:

1. Repeat the steps in To debug this error: on page 525.
2. Do one of the following:
   - On the *Summary* tab, under *Certificate*, click *Download*.



   - On the *SAML* tab, copy the value enclosed in the `<X509Certificate>` tag. Format the certificate via a certificate formatting tool, paste it into a text file, and save as a .cer file.



3. In EMS, upload the certificate in the *IdP Certificate* field.

System Settings

Configuring EMS settings

FortiEndpoint installs with a default IP address and port configured. You can change the IP address and port and configure other server settings for FortiEndpoint.

To configure EMS settings:

1. Go to *System Settings > EMS Settings*.
2. Configure the following options under *Shared Settings*. EMS uses these settings for FortiEndpoint managing Windows, macOS, and Linux endpoints, and FortiEndpoint managing Chromebook endpoints:

Option	Description
EMS CA certificate (ZTNA)	Displays the EMS CA certificate expiry. EMS sends this certificate to FortiOS. Click the *Revoke and Update* button to revoke and update the certificate. You may want to revoke a certificate if it is compromised and can no longer be trusted. When a certificate is revoked, EMS prompts FortiOS and FortiClient with a new certificate signing request. This may affect existing connections. You can also configure a custom certificate. See Uploading custom certificate and private key for ZTNA on page 540.
Enable ZTNA token	Enable the ZTNA JSON web token (JWT). See JWT support for ZTNA UID and tag sharing on page 537.
ZTNA token timeout	If you enabled the ZTNA JWT, enter the JWT expiry time in minutes. The minimum and default value is 60 minutes. When the expiry time is reached, EMS generates a new JWT and sends it to endpoints.
Reset Stalled Deployment Interval	Enter number of hours after which to reset stalled deployments.

3. Configure the following options under *EMS Settings*. FortiEndpoint uses these settings when managing Windows, macOS, and Linux endpoints:

Option	Description
Enforce User Verification	Enforce user verification for endpoints so that only verified users can register their endpoints with EMS. **Enable** — To register to EMS, users must log into verified user accounts using the verification type configured in Invitations on page 503. If you enable this option on an existing deployment, current FortiClient users will be disconnected until user verification.

Option	Description
	Disable Users do not need to log into verified user accounts to register to EMS. A warning message "*User Verification Not Enforced*" appears at the top of the EMS GUI.
User Verification Period	Enter the desired number of days for the user verification period. The minimum number of days is seven. When enable enforcing user verification, EMS deauthenticates all authenticated users that were authenticated earlier than the configured verification period. For example, if you configure the period as 30 days and then enable it, EMS immediately deauthenticates users that were authenticated more than 30 days ago. The timeout takes effect immediately.
Cloud Region to Repackage Installers	Select the cloud region for repackage installers.
Enforce Password Change Check for Domain Users	Enable to require FortiClient users to re-authenticate if the domain user password (LDAP or Azure) is changed.
Sign Software Packages	Enable this option to have Windows FortiClient software installers created by or uploaded to FortiEndpoint digitally signed with a code signing certificate.

4. If managing Chromebooks, enable *EMS for Chromebooks Settings*.
5. Configure the following options under *EMS for Chromebooks Settings*. These settings are used by FortiEndpoint managing Chromebook endpoints:

Listen on port	Displays the default port for the FortiEndpoint server for Chromebooks. You can change the port by typing a new port number. The FortiClient Web Filter extension on Chromebooks connects to FortiEndpoint using the specified port number.
User inactivity timeout	Enter the number of hours of inactivity after which to timeout the user.
Profile update interval	Specify the profile update interval (in seconds).
Service account	Displays the service account ID currently in use.
Update service account	Update the service account with new credentials.
Reset service account	In the event your service account is broken, you can revert back to the default service account by clicking the *Reset* button. This restores the default service account. You must *Save* the settings for the change to take effect.

Email	Available if the *Update service account* button is clicked. Enter a new service account ID.
Private key	Available if the *Update service account* button is clicked. Upload a new service account private key.

6. Configure the following options under *Endpoints Settings*:

FortiClient Telemetry Connection Key	Add the FortiClient Telemetry connection key for FortiEndpoint. FortiClient must provide this key during connection. The key cannot contain a semicolon ;. You can generate a QR code for the specified key. See Generating a QR code for centrally managing FortiClient (Android) and (iOS) endpoints on page 536.
Keepalive Interval	Each connected FortiClient endpoint sends a short KA message to FortiClient EMS, reports client-side changes, and checks for configuration changes on EMS at the specified interval. A large number of endpoints frequently connecting to the EMS server can affect server and network performance. In this case, increasing the KA interval is recommended.
Offline Timeout	Configure the number of KA intervals after which EMS considers the endpoint to be offline.
Tag Timeout	Configure the number of minutes after EMS considers an endpoint to be offline (as configured in the *Offline timeout* field), that EMS then removes tags from the endpoint.
License Timeout	Configure the number of days after the endpoint has not contacted EMS that EMS removes that endpoint's registration record from EMS.
Delete Device Timeout	Configure the number of days after which EMS deletes a deregistered endpoint. For example, if you configure this value to be 45 days, EMS deletes the endpoint 45 days after its deregistration.
Deauthorized User Inactivity Timeout	Enable and configure the number of days after which EMS deletes FortiClient user records for unauthorized users.
Stale Verified User Cleanup Timeout	Enable and configure the number of days after which EMS deletes FortiClient user records associated with a single device user for unauthorized users. You can click *Delete now* to delete the records immediately.
Onboarding Lockout Attempt	Configure the maximum number of unsuccessful attempts to allow an end user to attempt verification to EMS. After the user reaches the maximum number of attempts, EMS locks out the user. This only applies if user verification is enabled. See User Management on page 498 . The default value is 3 times. The maximum is 10 times.
Onboarding Lockout Period	Configure the number of seconds that EMS locks out an end user for after they have reached the number of unsuccessful verification attempts configured in *Onboarding Lockout Attempt*.

	During the onboarding lockout period, any verification attempt does not succeed, even if the user provides correct credentials. Each verification attempt during the lockout period causes the onboarding lockout period to reset and begin again. After the configured onboarding lockout period passes, the lockout resets and the user can again attempt to verification multiple times per the number of attempts configured in *Onboarding Lockout Attempt*. If they again reach the maximum number of attempts, the onboarding lockout period begins again.
Automatically Upload Avatars	FortiClient uploads user avatars to all FortiGates, FortiAnalyzers, and FortiEndpoint servers it is connected to.
Enable Endpoint Snapshot Reports	Enable endpoint snapshot reports and enter the interval at which to take reports in seconds. The interval must be between 300 and 86400 seconds. The snapshot contains process and network information of the endpoint's current state.

7. Click *Apply*.

Generating a QR code for centrally managing FortiClient (Android) and (iOS) endpoints

You can create a QR code to distribute to FortiClient (Android) and (iOS) users. FortiClient (Android) and (iOS) users can scan the QR code from their device to automatically enable FortiTelemetry and attempt connection to the specified FortiEndpoint.

QR codes can contain the FortiClient telemetry connection key if desired.

To generate the QR code:

1. Go to *System Settings > EMS Settings*.
2. Do one of the following:
   - To generate the QR code without a connection key, beside the *Listen on IP* field, click the *View QR Code* button.
   - To generate the QR code with a connection key, ensure that the *FortiClient telemetry connection key* field is populated, then click the *View QR Code* button beside it.
3. In the dialog, select or deselect *Show FortiClient telemetry connection key* as desired.
4. Click *Continue*.
5. Click *Download*.
6. Save the QR code image to your machine.
7. Email the QR code to FortiClient (Android) and FortiClient (iOS) users.

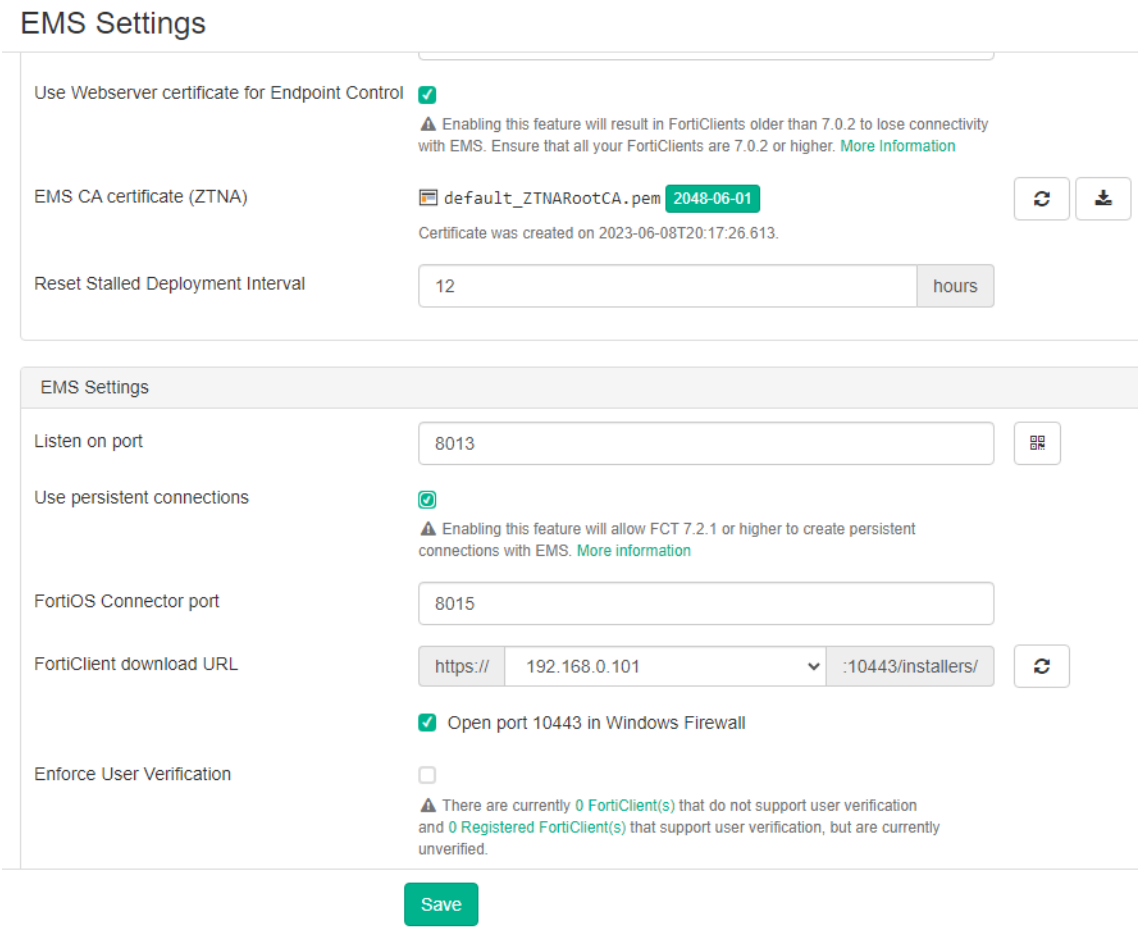
For instructions on scanning the QR code from an Android or iOS device, see Launching FortiClient (Android) for the first time or Running FortiClient iOS.

Persistent connection

When *Use persistent connections* is enabled, FortiClient creates a persistent connection with EMS. It does not tear down and renegotiate the TLS connection at every keepalive interval.

To enable persistent connections:

1. In EMS, go to *System Settings* > *EMS Settings*.
2. Under *EMS Settings*, enable *Use persistent connections*.
3. Click *Save*.



This feature requires FortiClient 7.2.1 and EMS 7.2.1. If either FortiClient or EMS is on a version older than 7.2.1, FortiClient and EMS establish a non-persistent connection.

JWT support for ZTNA UID and tag sharing

As an enhancement to security posture tag sharing in the Fortinet Security Fabric connection between EMS and FortiOS, EMS now also sends security posture tags to FortiClient in JSON web token (JWT) format. You can install JWTs on endpoints. A browser on an endpoint can use JWTs to share endpoint identity and tags with FortiOS directly. This feature makes security posture tag sharing more resilient, resulting in a

more fault-tolerant zero trust network access (ZTNA) connection between the endpoint and ZTNA server. This feature makes it possible for endpoints to access remote resources via the ZTNA server in the event of EMS, FortiClient, and FortiOS network loss or connection interruption.

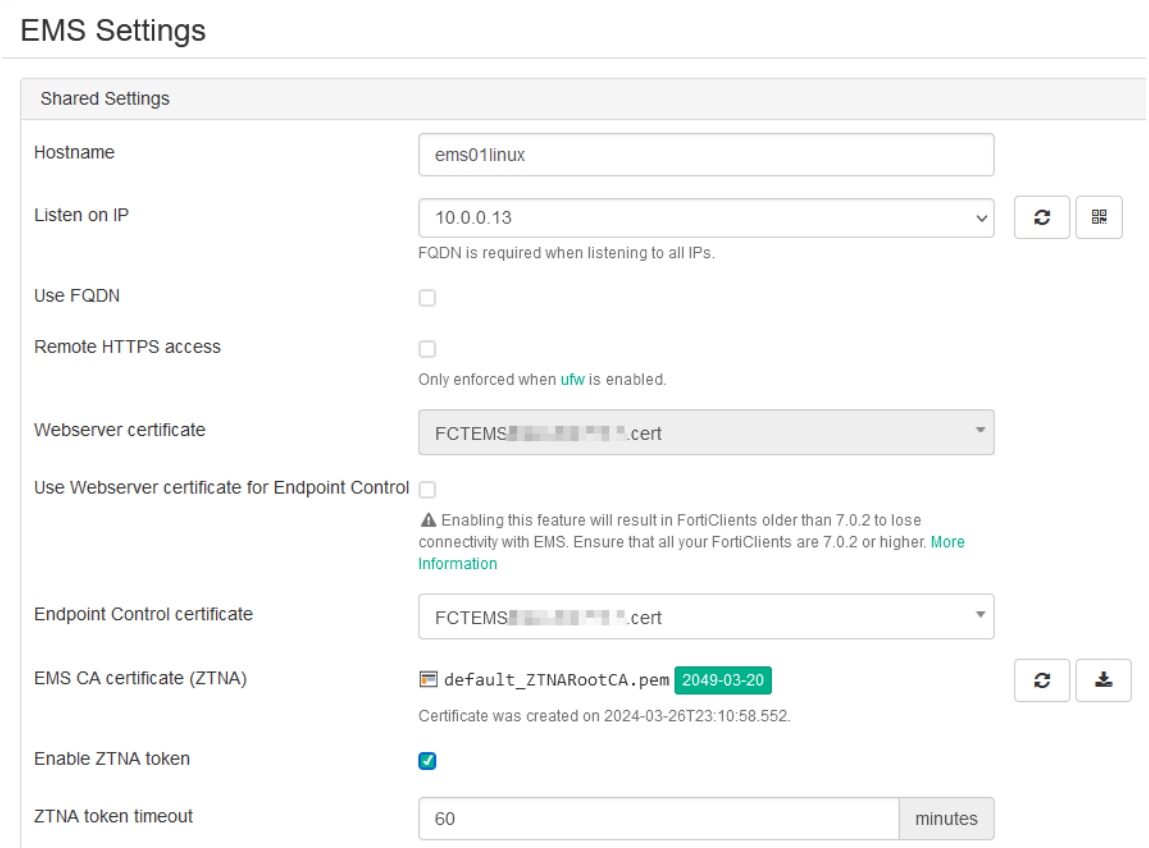
Prior to the addition of JWT support, in the event of connection loss between FortiClient and EMS or a Fabric connection issue between EMS and FortiOS, legitimate endpoints could not access remote resources via a ZTNA server.

This feature has the following limitations:

- Endpoint default gateway must be the ZTNA server.
- The FortiGate only receives tokens on physical interfaces.
- ZTNA server configuration only uses TCP forwarding.

To configure JWT support for ZTNA UID and tag sharing:

1. Configure the feature in EMS:
   a. Configure *EMS Settings*:
      i. Go to *System Settings > EMS Settings*.
      ii. Click *Enable ZTNA token*.
      iii. In the *ZTNA token timeout* field, enter the JWT expiry time in minutes. The default is 1440 minutes (24 hours). The minimum is 60 minutes. When the expiry time is reached, EMS generates a new JWT and sends it to endpoints. Configure other fields as desired, then save.

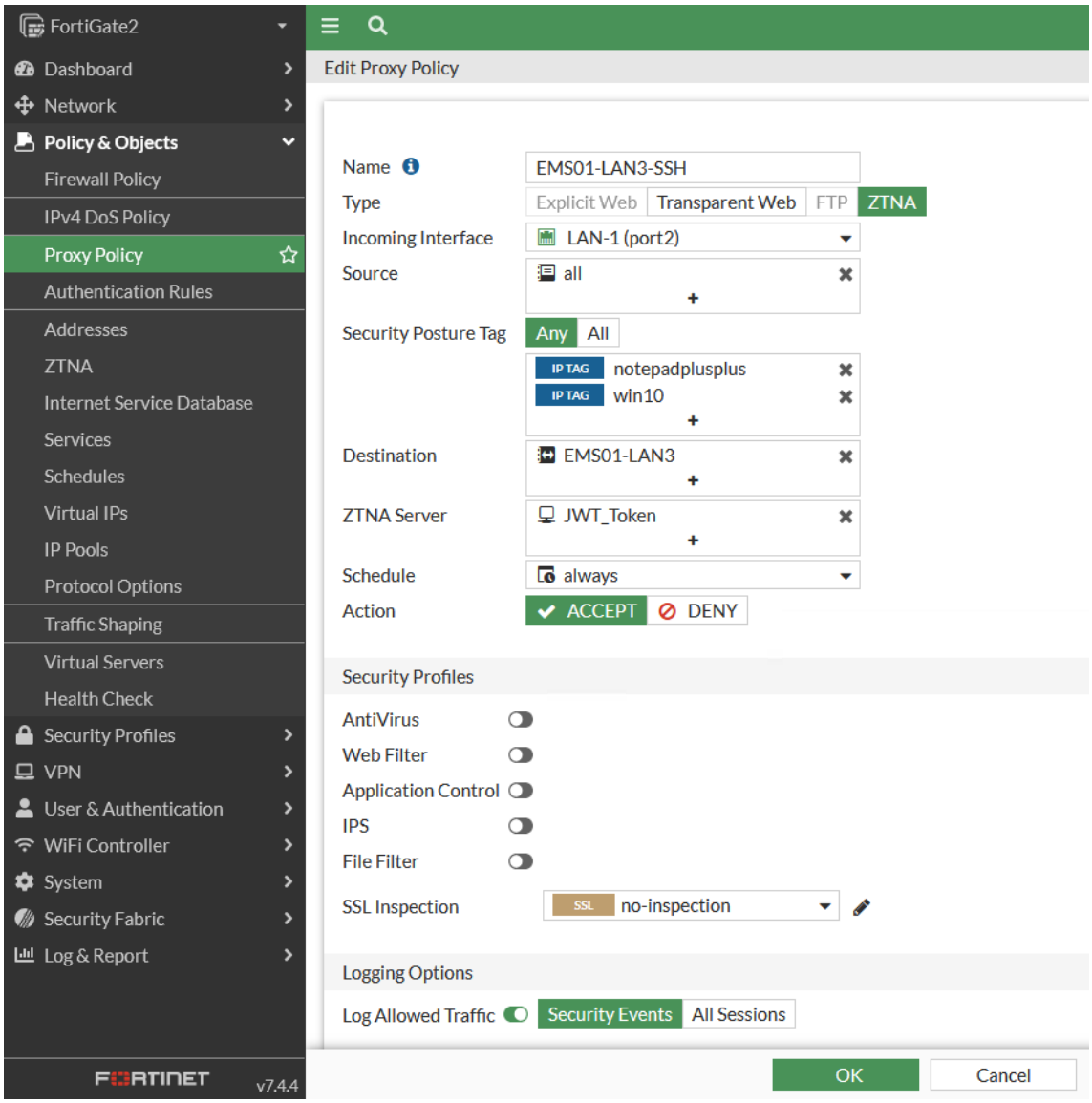


   b. Go to *Endpoint Profiles > ZTNA Destinations*.

c. Create a new profile or edit an existing one.
d. Enable *Destinations*.
e. Add a remote resource and ZTNA server address to the profile. Configure other fields as desired, then save.
f. Go to *Fabric & Connectors > Fabric Devices*.
g. Confirm that EMS has authorized the FortiGate which acts as the ZTNA server. This FortiGate must also be the default gateway for endpoints that use the JWT.
h. Go to *Security Posture Tags > Security Posture Tagging Rules*.
i. Configure tags and tagging rules as desired. The JWT and FortiGate ZTNA server use these tags to allow traffic to remote resources if the ZTNA policy matches with the tags. For example, you could create a security posture tagging rule that tags endpoints as win10 if they have Windows 10 installed.

2. In FortiOS, go to *Policy & Objects > Proxy Policy*.
3. Create a new policy or edit an existing one.
4. For *Type*, select *ZTNA*.
5. Under *Security Posture Tag*, select the tags that you configured in EMS.

6. Configure other fields as desired, then click *OK*.



7. After FortiClient receives the profile changes from EMS, in FortiClient, go to the *ZTNA Destination* tab to view the ZTNA destination received from EMS.
8. To ensure EMS successfully pushed the generated JWT to FortiClient, in Registry Editor, view `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Fortinet\FortiClient\FA_ESNAC\ztna_token`.
9. To verify that FortiClient maintains ZTNA connection with the ZTNA server to access remote resources in the event of EMS network connection loss or Fabric connection interruption, disable EMS interfaces to simulate the network connection loss. Confirm that FortiClient can still access a remote resource via the ZTNA server, for example an SSH server that runs in a different subnet.

Uploading custom certificate and private key for ZTNA

You can upload a custom intermediate root certificate and private keys to EMS to use for signing zero trust network access (ZTNA) endpoint certificates instead of relying on the default EMS certificate, default_

ZTNARootCA.pem. This provides flexibility for organizations that need custom certificate chains for compliance or security reasons. It can also streamline the end user experience by helping to avoid certificate trust issues.

When you upload a custom signing certificate to EMS, FortiOS retrieves it from EMS after the Fortinet Security Fabric connection establishes. EMS uses this certificate to sign FortiClient client certificates. In the FortiClient certificate's subject field, the common name (CN) is set to <fct_uid>, and two custom X.509 extensions are included:

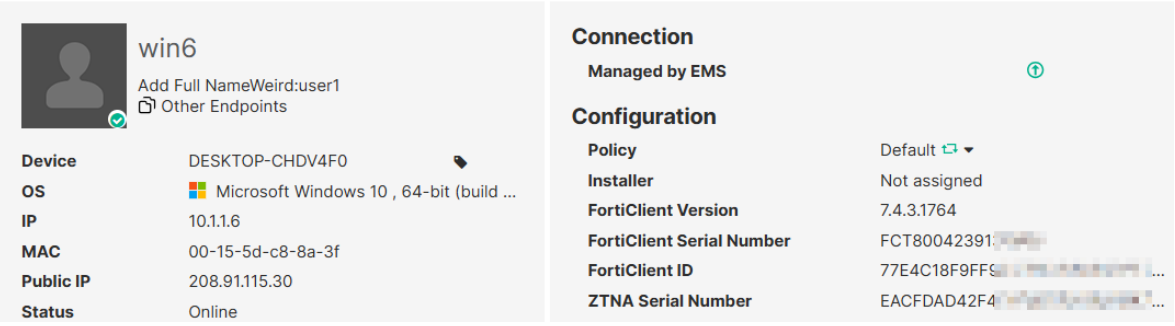
- 1.3.6.1.4.1.12356.101.15.1.102 (EMS serial number (SN))
- 1.3.6.1.4.1.12356.101.15.1.101 (tenant ID)

FortiOS uses the downloaded signing certificate to validate the FortiClient certificate and extracts the following details:

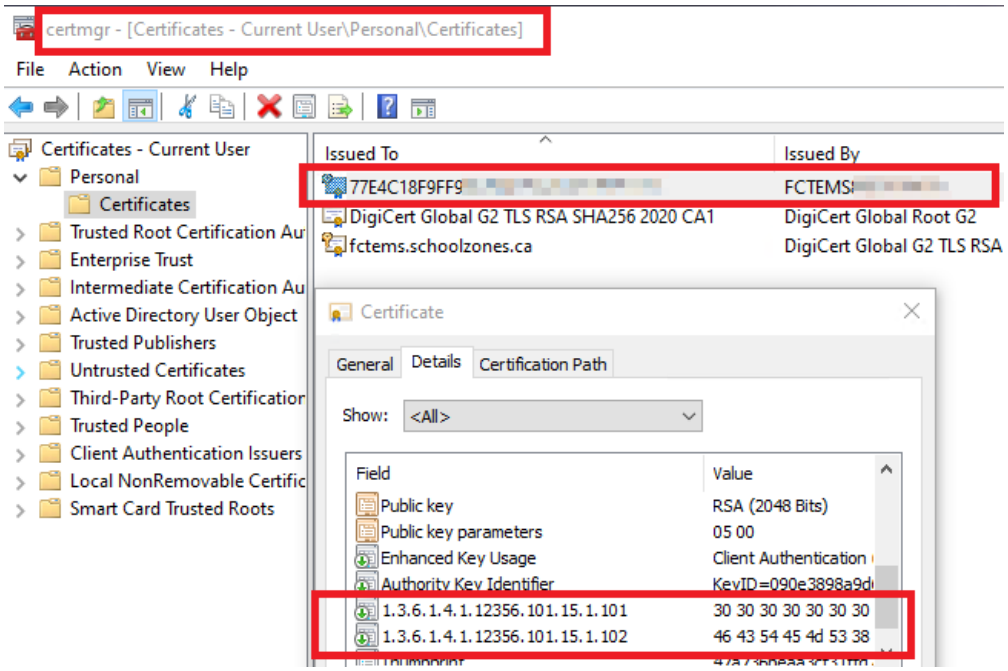
- FCT UID from the subject CN
- EMS SN from the X.509v3 extension 1.3.6.1.4.1.12356.101.15.1.102
- Tenant ID from the X.509v3 extension 1.3.6.1.4.1.12356.101.15.1.101

To upload a custom CA certificate:

1. In EMS, go to *System Settings* > *EMS Settings*.
2. Beside *EMS CA Certificate (ZTNA)*, click *Upload Custom CA Certificate*.
3. Click *Update*.
4. You can upload a PEM or PKCS12 certificate. Upload the desired certificate, then click *OK*.
5. Click *Apply*.
6. You can verify the certificate change on an endpoint using the FortiClient ID:
   a. Go *Endpoints* > *All Endpoints*.
   b. Select the desired endpoint.
   c. Note the FortiClient ID.



   d. On the endpoint device, open *Manage user certificates*.
   e. Go to *Certificates - Current User\Personal\Certificates*.
   f. Open the certificate that shows the FortiClient ID that you noted.
   g. On the *Details* tab, confirm that the two X.509 extensions display:
      - *1.3.6.1.4.1.12356.101.15.1.102* (EMS serial number (SN))
      - *1.3.6.1.4.1.12356.101.15.1.101* (tenant ID)



Uninstalling all endpoints

Super administrators can remove all endpoints from EMS, which erases all associated data, such as telemetry and historical logs.

This option is mainly useful for customers using virtual desktop infrastructure environments, where temporary desktop instances are used for a short duration, then terminated. After you use this option to remove all endpoints, only active instances reconnect to EMS. This conveniently frees up the licenses that the terminated instances were using, and you can provision these licenses to active unlicensed endpoints.

To remove all endpoints from EMS as a super administrator:

1. Go to *System Settings > Uninstall All Endpoints*.
2. Read the warning message and details about the consequences and click *Confirm All Endpoint Uninstall*.
3. Enter the generated code to confirm the operation.

Configuring Logs settings

You can specify what level of log messages to capture in the logs for FortiEndpoint. You can also specify when to automatically delete logs and alerts.

To configure Logs settings:

1. Go to *System Settings* > *Logs*.
2. Configure the following options:

Log level	Select the level of messages to include in FortiEndpoint logs. For example, if you select *Info*, all log messages from *Info* to *Emergency* are added to the FortiEndpoint logs.
Automatically clear logs older than	Enter the number of days that you want to store logs. For example, if you enter 30, EMS stores logs for 30 days. EMS automatically deletes any logs older than 30 days.
Automatically clear alerts older than	Enter the number of days that you want to keep alerts. For example, if you enter 30, EMS keeps alerts for 30 days. EMS automatically deletes any alerts older than 30 days.
Automatically clear events older than	Enter the number of days that you want to keep events. For example, if you enter 30, EMS keeps events for 30 days. EMS automatically deletes any events older than 30 days.
Automatically clear Chromebook events older than	Enter the number of days that you want to keep Chromebook events. For example, if you enter 30, EMS keeps Chromebook events for 30 days. EMS automatically deletes any Chromebook events older than 30 days.
Clear all now	Click to immediately delete all FortiEndpoint logs or alerts.
Send system log messages externally	Select one of the following: • *Disabled*: FortiEndpoint does not send system log messages to an external server. • *FortiAnalyzer*: configure a FortiAnalyzer for FortiEndpoint to send system log messages to by entering the desired FortiAnalyzer address, port, and data protocol. See Incoming ports and Sending EMS system log messages to FortiAnalyzer on page 544. • *SysLog*: configure a syslog server for FortiEndpoint to send system log messages to by entering the desired syslog server address, port, and data protocol. When you have configured a FortiAnalyzer or syslog server for this option, EMS sends system log messages for the following events. This list is not exhaustive: • When FortiClient status changes to online • When EMS considers the FortiClient status as offline • When FortiClient reports a change in its IP address System log messages include information regarding date, time, hostname, device IP and MAC addresses, event time, operational system, message (online/offline/IP-changed, and so on), policy name, EMS name, and EMS serial number.

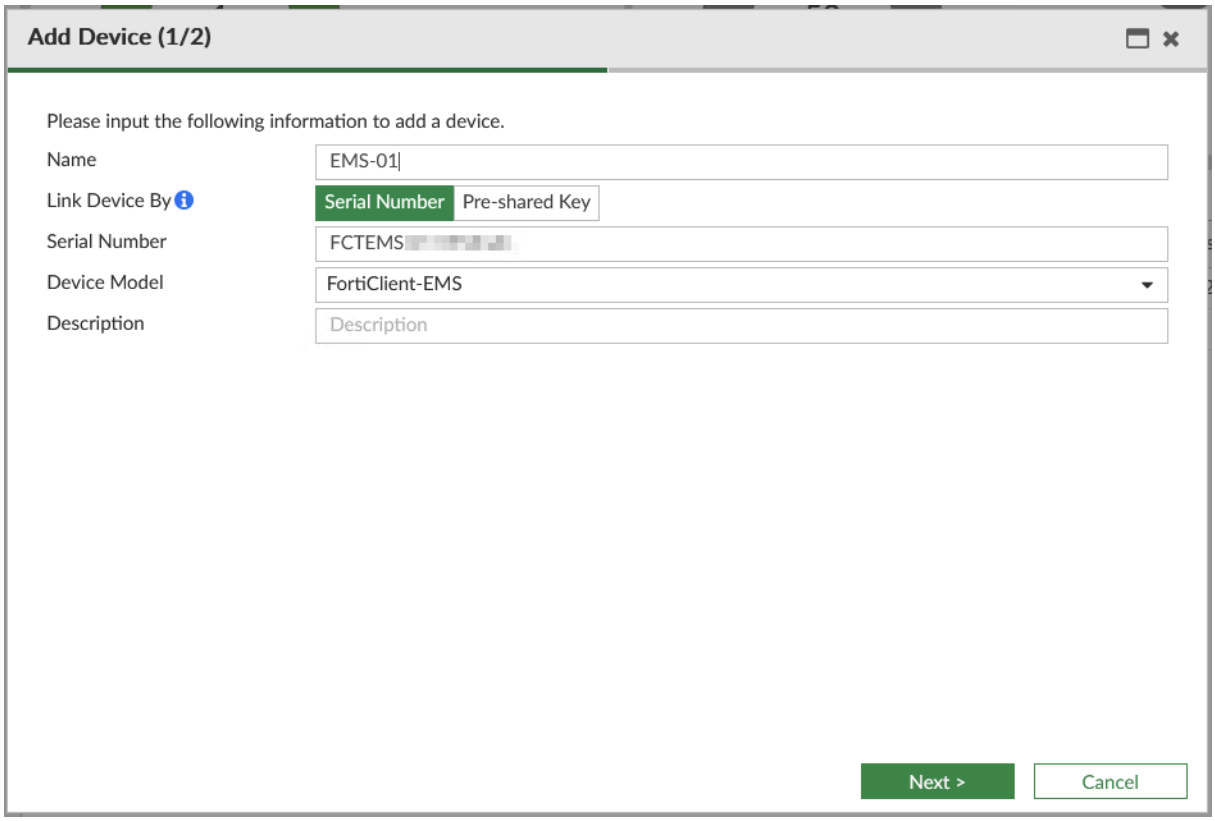
3. Click *Save*.

Sending EMS system log messages to FortiAnalyzer

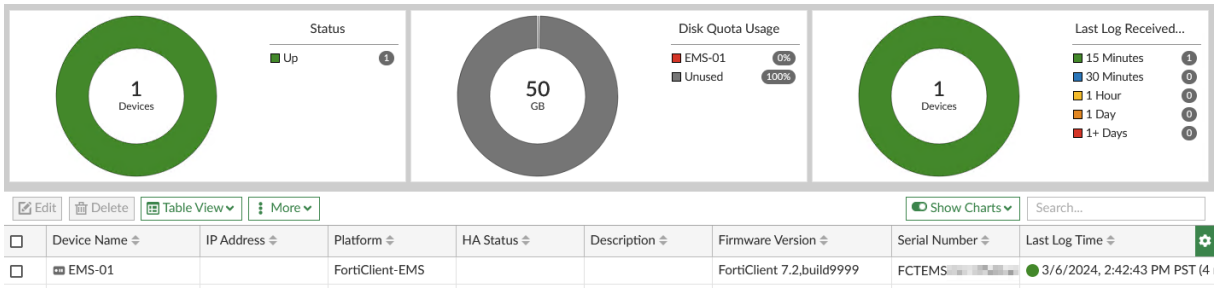
EMS can send server logs to FortiAnalyzer for reporting and investigation. For audit purposes, you should log all admin activity.

To configure sending EMS system log messages to FortiAnalyzer:

1. Authorize the EMS in FortiAnalyzer to allow FortiAnalyzer to receive logs from the EMS instance:
   a. In FortiAnalyzer, go to *Device Manager*.
   b. Click *Add Device*.
   c. In the *Add Device* dialog, in the *Serial Number* field, enter the EMS serial number. FortiAnalyzer automatically recognizes that the device is an EMS instance from the serial number.
   d. Configure other fields as desired, then click *Next*.

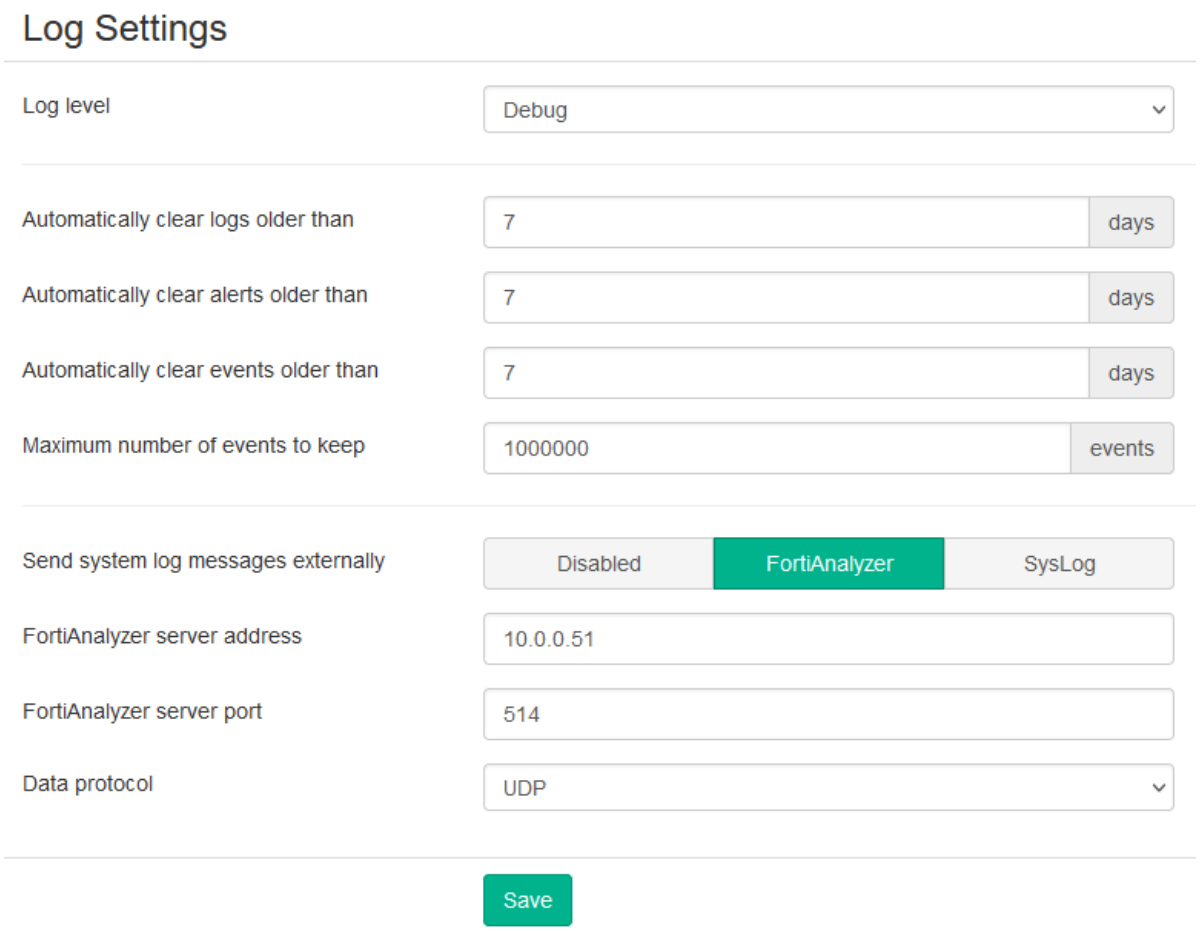


EMS is added as an authorized device and FortiAnalyzer is ready to receive its logs.

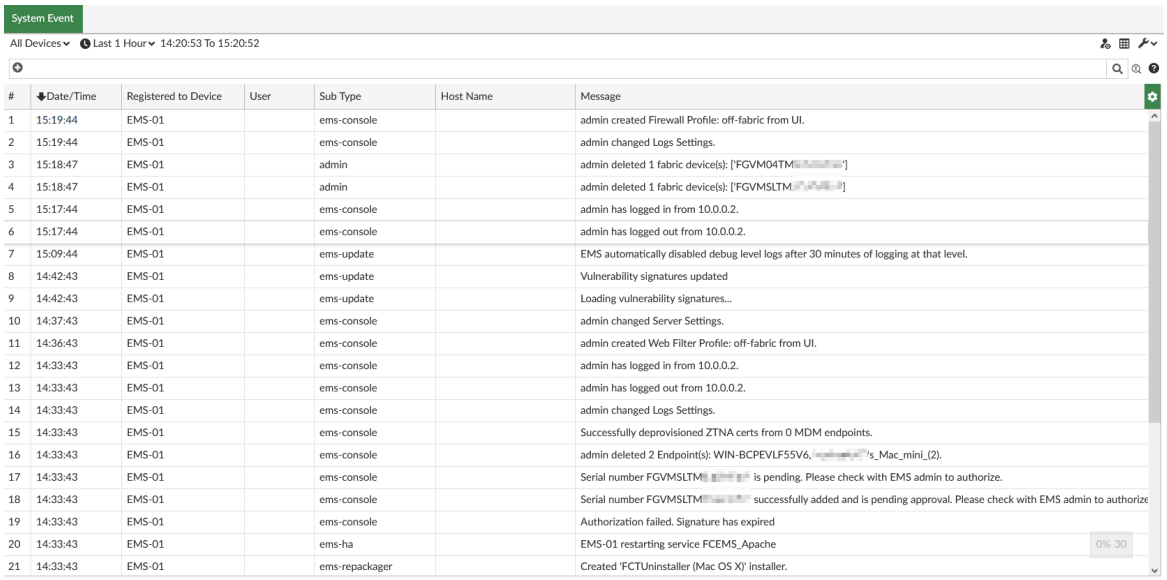


2. In EMS, go to *System Settings* > *Log Settings*.

3. For *Send system logs externally*, select *FortiAnalyzer*.
4. In the *FortiAnalyzer server address* field, enter the FortiAnalyzer server IP address.
5. In the *FortiAnalyzer server port* field, configure the desired port. This example keeps the default value, 514.
6. From the *Data protocol* dropdown list, select the desired data protocol. This example selects UDP.
7. Click *Save*.



8. In FortiAnalyzer, go to *Log View* > *FortiClient* to view EMS logs.



#	Date/Time	Registered to Device	User	Sub Type	Host Name	Message
1	15:19:44	EMS-01		ems-console		admin created Firewall Profile: off-fabric from UI.
2	15:19:44	EMS-01		ems-console		admin changed Logs Settings.
3	15:18:47	EMS-01		admin		admin deleted 1 fabric device(s): ['FGVM04TM
4	15:18:47	EMS-01		admin		admin deleted 1 fabric device(s): ['FGVMSLTM
5	15:17:44	EMS-01		ems-console		admin has logged in from 10.0.0.2.
6	15:17:44	EMS-01		ems-console		admin has logged out from 10.0.0.2.
7	15:09:44	EMS-01		ems-update		EMS automatically disabled debug level logs after 30 minutes of logging at that level.
8	14:42:43	EMS-01		ems-update		Vulnerability signatures updated
9	14:42:43	EMS-01		ems-update		Loading vulnerability signatures...
10	14:37:43	EMS-01		ems-console		admin changed Server Settings.
11	14:36:43	EMS-01		ems-console		admin created Web Filter Profile: off-fabric from UI.
12	14:33:43	EMS-01		ems-console		admin has logged in from 10.0.0.2.
13	14:33:43	EMS-01		ems-console		admin has logged out from 10.0.0.2.
14	14:33:43	EMS-01		ems-console		admin changed Logs Settings.
15	14:33:43	EMS-01		ems-console		Successfully deprovisioned ZTNA certs from 0 MDM endpoints.
16	14:33:43	EMS-01		ems-console		admin deleted 2 Endpoint(s): WIN-BCPEVLF55V6, 's_Mac_mini_(2).
17	14:33:43	EMS-01		ems-console		Serial number FGVMSLTM is pending. Please check with EMS admin to authorize.
18	14:33:43	EMS-01		ems-console		Serial number FGVMSLTM successfully added and is pending approval. Please check with EMS admin to authorize
19	14:33:43	EMS-01		ems-console		Authorization failed. Signature has expired
20	14:33:43	EMS-01		ems-ha		EMS-01 restarting service FCEMS_Apache
21	14:33:43	EMS-01		ems-repackager		Created 'FCTUninstaller (Mac OS X)' installer.

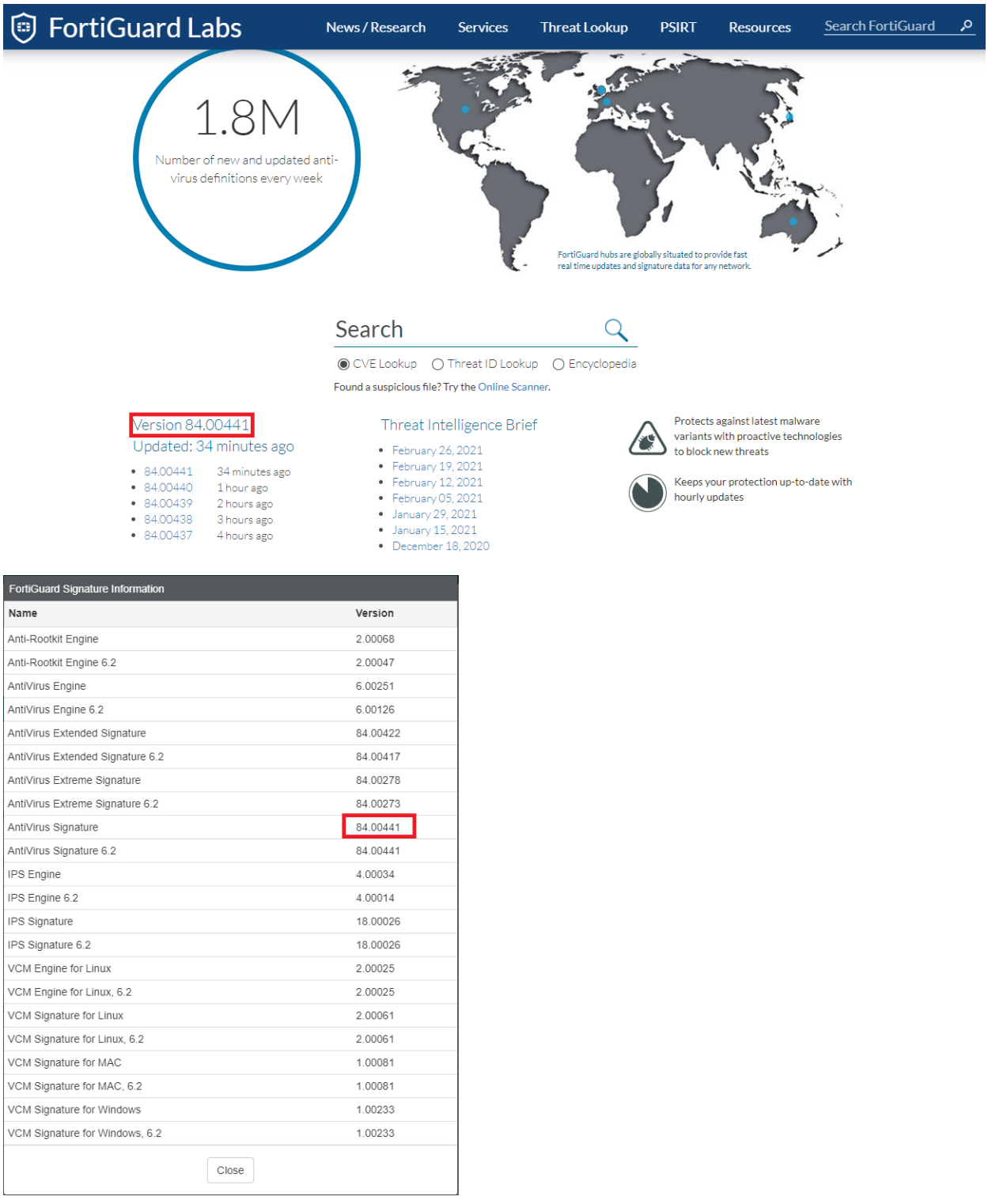
Configuring FortiGuard Services settings

FortiClient relies on several signature databases to identify and stop malware. Keeping these database up-to-date to remain protected from new threats as they are identified is imperative.

In some situations, FortiClient may fail to update these signatures. In these situations, you must be able to readily identify these endpoints so corrective action can be taken.

EMS can detect when an endpoint is out-of-date by downloading a list of the current versions for signatures and engines and comparing that to the versions reported from FortiClient status updates. EMS can also send an email when this happens. See Configuring Endpoint Alerts on page 550.

You can verify if EMS has up-to-date signatures by going to *System Settings* > *FortiGuard Services* > *View Signature List*, and comparing that to *FortiGuard.com* > *Services* > *Service of interest*, such as AV.


FortiGuard Labs
News / Research
Services
Threat Lookup
PSIRT
Resources
Search FortiGuard
1.8M
Number of new and updated anti-virus definitions every week
FortiGuard hubs are globally situated to provide fast real time updates and signature data for any network.
Search
CVE Lookup
Threat ID Lookup
Encyclopedia
Found a suspicious file? Try the Online Scanner.
Version 84.00441
Updated: 34 minutes ago
84.00441 34 minutes ago
84.00440 1 hour ago
84.00439 2 hours ago
84.00438 3 hours ago
84.00437 4 hours ago
Threat Intelligence Brief
February 26, 2021
February 19, 2021
February 12, 2021
February 05, 2021
January 29, 2021
January 15, 2021
December 18, 2020
Protects against latest malware variants with proactive technologies to block new threats
Keeps your protection up-to-date with hourly updates
FortiGuard Signature Information
Name
Version
Anti-Rootkit Engine 2.00068
Anti-Rootkit Engine 6.2 2.00047
AntiVirus Engine 6.00251
AntiVirus Engine 6.2 6.00126
AntiVirus Extended Signature 84.00422
AntiVirus Extended Signature 6.2 84.00417
AntiVirus Extreme Signature 84.00278
AntiVirus Extreme Signature 6.2 84.00273
AntiVirus Signature 84.00441
AntiVirus Signature 6.2 84.00441
IPS Engine 4.00034
IPS Engine 6.2 4.00014
IPS Signature 18.00026
IPS Signature 6.2 18.00026
VCM Engine for Linux 2.00025
VCM Engine for Linux, 6.2 2.00025
VCM Signature for Linux 2.00061
VCM Signature for Linux, 6.2 2.00061
VCM Signature for MAC 1.00081
VCM Signature for MAC, 6.2 1.00081
VCM Signature for Windows 1.00233
VCM Signature for Windows, 6.2 1.00233
Close

To configure FortiGuard Services settings:

1. Go to *System Settings* > *FortiGuard Services*.
2. Under *Forensics Services*, select the desired upload server location for FortiGuard forensic analysis logs.
3. Configure the *Software and Signature Update Services* options:

FortiGuard	
Server Location	Configure FortiGuard server location to *Global*, *US*, or *Europe*. Europe is only available if you have selected the *Enable SSL* checkbox.
Port	Enter the desired port number to communicate to the FortiGuard server.
Enable SSL	Enable SSL to connect to FortiGuard using HTTPS, or disable SSL to connect using HTTP. HTTPS must be enabled to use the FortiGuard Europe server.
View Signature List	View a list of latest signature versions.
Use FortiManager for client software/signature updates	Turn on to use FortiManager for updating FortiClient software or signatures. You must specify the IP address or hostname for FortiManager as well as the port number.
IP address/Hostname	Enter the IP address/hostname.
Port	Configure the port number.
Failover port	Configure the failover port.
Timeout	Configure the timeout interval (in seconds).
Failover	Enable failover to FDN when FortiManager is unavailable.

4. Configure the *Cloud Services* options:

FortiCloud	
Region	Select the FortiCloud region from the dropdown list.
Time Offset	Select the FortiCloud time offset from the dropdown list.

5. Click *Save*.

Alerts

Configuring EMS Alerts

You can set up an SMTP server to enable alerts for FortiEndpoint or endpoint events. When an alert is triggered, EMS sends an email notification.

To configure EMS Alerts:

1. Go to *System Settings > EMS Alerts*.
2. Set the following options to send an email when the following events happen:

Version Alerts		
New EMS version is available for deployment		New FortiEndpoint version is available.
	Remind me everyday for 2 weeks	Remind you when a new FortiEndpoint version is available everyday for two weeks.
New FortiClient version is available for deployment		New FortiClient version is available for deployment.
	Remind me everyday for 2 weeks	Remind you when a new FortiClient version is available for deployment everyday for two weeks.
FortiClient Alerts		
EMS license is expired or about to expire		Expiring or expired FortiEndpoint license.
EMS fails to sync with LDAP domains		FortiEndpoint does not sync with LDAP domains.
Less than 10% of client licenses are left		Be notified when there are less than 10% of client licenses left.
Client licenses have run out		Be notified when you run out of client licenses.
New software is detected		Be notified when new FortiClient software is detected.
Forensics Analysis is updated		Be notified when a forensic analysis task is updated.
AD Connector is offline		Be notified when the Active Directory connector is offline.
Server certificate expiring		Be notified when the server certificate is close to expiry.
FortiClient for Chromebook Alerts		
EMS license for Chromebooks is expired or about to expire		Expiring or expired FortiEndpoint license for Chromebooks.
Less than 10% of the client licenses for Chromebooks are left		Be notified when there are less than 10% of client licenses left for Chromebooks.
Client licenses for Chromebooks have run out		Be notified when you run out of client licenses for Chromebooks.

3. Click *Save*. If you have not already set up an SMTP server, the GUI automatically prompts you to configure SMTP server settings. See Configuring SMTP Server settings on page 550.

Configuring Endpoint Alerts

To configure endpoint alerts:

1. Go to *System Settings* > *Endpoint Alerts*.
2. From the *Send an email every...* dropdown list, select the frequency to send emails.
3. Select the events to send emails for:
   a. Malware is detected
   b. Repeated malware is detected (same malware is detected on the same machine within the last 24 hours)
   c. Multiple malwares are detected (different malwares are detected on the same machine within the last 24 hours)
   d. Malware outbreak is detected (same malware is detected on different endpoints within the last 24 hours)
   e. Zero-day malware is detected by FortiSandbox
   f. C&C attack communication channel is detected
   g. Critical vulnerability is detected
   h. Endpoint FortiClient Telemetry is manually disconnected by user
   i. Endpoint signature database is out-of-date
   j. Endpoint software is out-of-date
   k. Ransomware is detected

Configuring SMTP Server settings

You can set up an SMTP server to enable alerts for EMS and endpoint events. When an alert is triggered, EMS sends an email notification to the configured email address(es).

To configure SMTP server settings:

1. Go to *System Settings* > *SMTP Server*.
2. Set the following options:

Option		Description
Server		Enter the SMTP IP address or fully qualified domain name.
Port		Enter the port number.
Security		Select *None*, *STARTTLS*, or *SMTPS* for the security type, or select *Auto Detect* to automatically select the security type. If you select *STARTTLS* or *SMTPS*, the *Username* and *Password* fields become available.
	Username	Enter the username.
	Password	Enter the password.

Option	Description
Default Email Size	EMS detects the maximum email size from the configured SMTP server and sets it as the default value. Otherwise, EMS sets the default value to 10 MB.
Custom Email Size	You can optionally configure a custom email size in MB. If you configure a size larger than the maximum and default value, EMS displays a warning as such.
From	Enter the email address to send the alerts from.
Reply to	Enter the email address to send the replies to.
Subject	The sent e-mail alert's subject.
Recipients	Enter email address(es) to send alerts to. Press *Enter* to add more email addresses.
Test Subject	Test email's subject.
Test Message	Test email's message.
Test Recipient	Email address to send the test email to.
Send Test Email	Click the button to test the configured email settings.

3. Click *Save*.

To confirm that the EMS server can verify the SMTP server certificate:

When using STARTTLS or SMTPS, the SMTP server presents a certificate to prove its identity. If the server hosting EMS does not have the corresponding CA in its certificate store, EMS cannot trust the SMTP server certificate and the connection fails to establish.

You can verify this using tools on the server hosting EMS to establish a secure connection to the SMTP server. Using openssl as an example, you can run the following from the Windows command line:

```
openssl s_client -starttls smtp -crlf -connect <smtp_url:port>
```

The following is an example of an SMTP URL and port: smtp.office365.com:587

The command output displays the certificate that the mail server offers in the first few lines, accompanied by `unable to get local issuer certificate`. This indicates that the certificate presented by the SMTP server cannot be verified.

Viewing alerts

You can view alerts that FortiEndpoint generates. Examples of events that generate an alert include:

- A new version of FortiClient is available.
- FortiClient deployment failed.
- Failed to check for signature updates
- Error encountered when downloading Active Directory server entries
- Error encountered when scanning for local computers

A red label is associated with the *Alert* icon when new notifications are available or received. EMS clears the label when you view the alert.

To view alerts:

1. Click the *Alert* icon (a bell) in the toolbar.
2. Click the *Filter* icon in each column heading to apply filters.
3. Remove filters as desired.

Custom Messages

You can customize messages that display on endpoints in certain situations, such as if EMS quarantined the endpoint. For example, you can customize the message to include your organization's help desk phone number so that users can contact the network administration about their machine.

Customizing the endpoint quarantine message

You can customize the message that displays on an endpoint when FortiEndpoint quarantines it.

To customize the endpoint quarantine message:

1. Go to *System Settings > Custom Messages*.
2. Select *Endpoint Quarantine Message*.
3. In the *Message* field, enter the desired message. You can enter up to 512 characters. The *Preview* section displays the custom message as it would appear on the latest FortiClient version. You can also use the *Preview* slider to zoom in and out on the message preview.
4. Click *Save*.

Customizing Web Filter messages

You can customize the messages that display on an endpoint in in-browser Web Filter result pages.

To customize Web Filter messages:

1. Go to *System Settings > Custom Messages*.
2. Select *WebFilter Custom Messages*. The left panel displays the customization fields, while the right panel previews the custom messages as they appear in a web browser when using the latest version of FortiClient. There are different types of Web Filter messages:
   - Blocklisted page
   - Blocked page
   - Blocked FortiGuard inaccessible page
   - Warning page
   - Warning FortiGuard inaccessible page

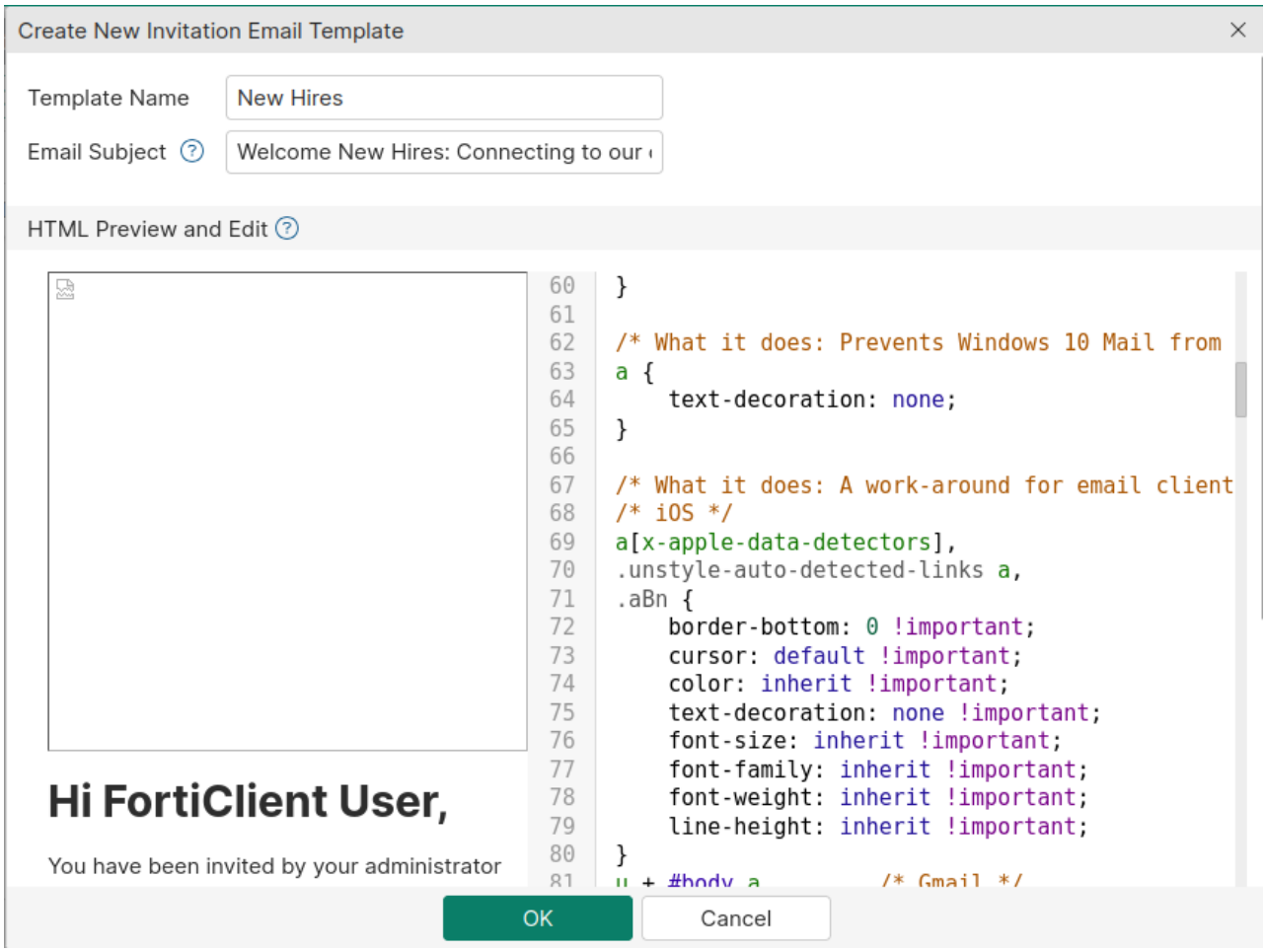
   Some customization fields apply to all messages, while others apply to only specific messages. This is indicated beside the field name.
3. In the left pane, enable/disable the fields and enter the desired messages. You can also upload images for logo and icon fields. The right pane displays previews of the messages.
4. Click *Save*.

Invitation Email Template

You can customize the invitation email that end users receive from EMS.

To customize an invitation email template:

1. Go to *System Settings > Invitation Email Template*. This page displays available invitation email templates. For each template, it displays the name, email subject line, template type (default or custom) and status (used or unused). EMS includes a default email template.
2. To create a custom template, click *Create new*.
3. In the *Template Name* field, enter the desired template name.
4. In the *Email Subject* field, enter the email subject line that displays to end users. If you do not enter a value in this field, EMS uses the default invitation email subject line.
5. Edit email content on the right pane and preview your changes on the left pane. Ensure that your email content contains `{{invitation_code}}` since it is used to render the invitation code in the email. If desired, you can modify the install package download URLs. If you use custom links for the package download URLs, you must ensure that the links are correct. The CSS is rendered when you send the invitation to users.
6. Click *OK* to save the invitation email template. You must select this template in an invitation to send users an email that uses this template. See Invitations on page 503.


Create New Invitation Email Template
Template Name
New Hires
Email Subject
Welcome New Hires: Connecting to our
HTML Preview and Edit
Hi FortiClient User,
You have been invited by your administrator
}
/* What it does: Prevents Windows 10 Mail from
a {
text-decoration: none;
}
/* What it does: A work-around for email client
/* iOS */
a[x-apple-data-detectors],
.unstyle-auto-detected-links a,
.aBn {
border-bottom: 0 !important;
cursor: default !important;
color: inherit !important;
text-decoration: none !important;
font-size: inherit !important;
font-family: inherit !important;
font-weight: inherit !important;
line-height: inherit !important;
}
OK
Cancel

Feature Select

In *Feature Select*, you can choose which features to show and hide in EMS. Only features that are enabled in *Feature Select* are available for configuration in other areas of EMS. For example, disabling Web and Video Filtering in *Feature Select* results in the following:

- Endpoint profiles:
  - The Web and Video Filter profiles are unavailable for configuration.
  - The options to enable Web and Video Filter logs on System Settings profiles are unavailable.
- If you enable Web Filter in a deployment package, the deployment package installs Web Filter on the endpoint. However, the Web Filter feature is disabled on the endpoint and does not appear in the FortiClient GUI.
- The Web Filter Detection widget is unavailable on the Status dashboard.
- Importing a profile from FortiGate/FortiManager is unavailable.

Only an EMS superadministrator can enable and disable features in Feature Select. Other EMS users can view which features are enabled and disabled in Feature Select, but cannot modify the configuration.

If an endpoint previously had a feature enabled, but you later disable the feature in Feature Select, EMS then disables the feature on the endpoint.

The following table provides details on features that you must enable for certain functionalities to be available in FortiClient. You must enable the feature in *Feature Select*, then configure on the applicable endpoint profile for the functionality to be available in FortiClient. This table is not exhaustive:

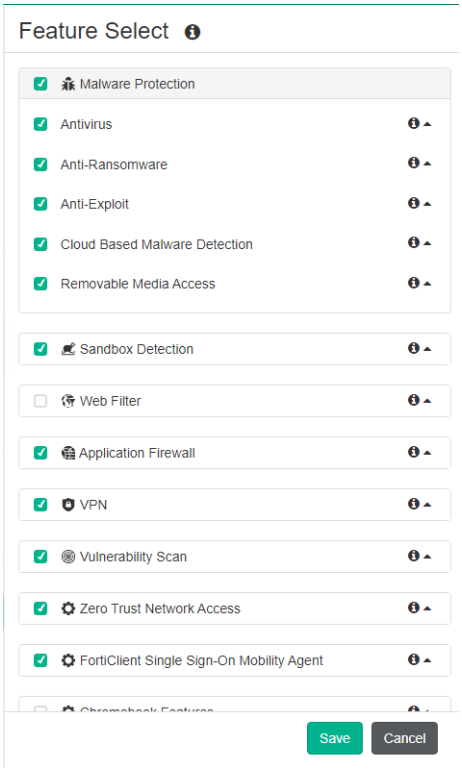
Feature to enable in Feature Select	FortiClient functionalities
Firewall	• C&C blocking • Endpoint quarantine
Web and Video Filtering	• Category-based malicious site blocking • Keyword blocking (also requires web browser plugin)

Only features that FortiEndpoint is licensed for are available for enablement in Feature Select.

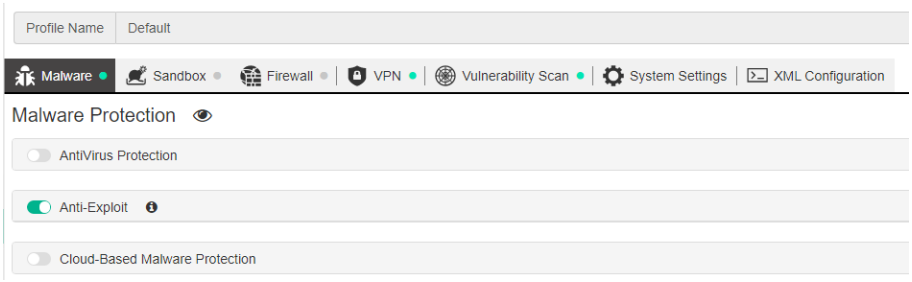
You cannot disable Web Filter if you have enabled the Chromebook feature in Feature Select.

To enable/disable a feature in Feature Select:

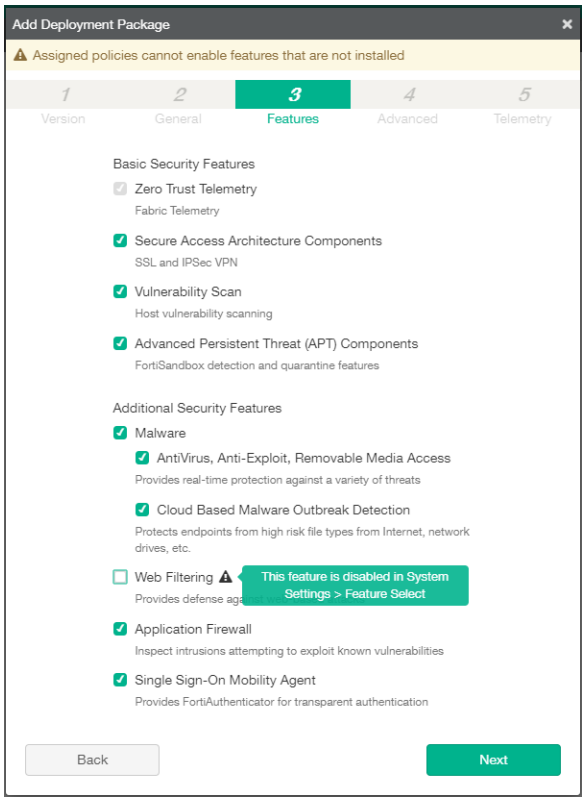
1. Go to *System Settings* > *Feature Select*.
2. Enable or disable features as desired. This example disables Web Filter.



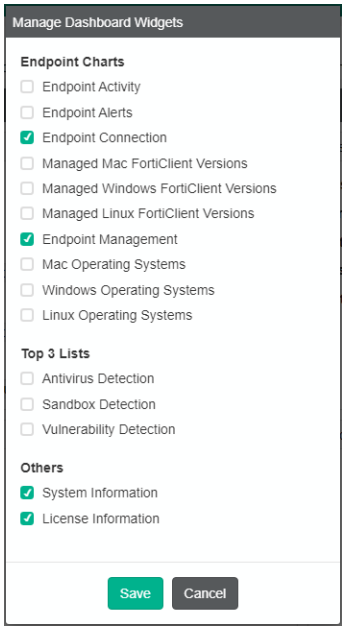
3. Click *Save*. The *Web Filter* tab is not available for configuration in an endpoint profile. The *Import from FortiGate/FortiManager* option under *Endpoint Profiles* in the left pane is also not available.



When creating a deployment package, a warning displays beside Web Filtering that the feature is disabled. You cannot create a deployment package that installs the Web Filter feature on endpoints while Web Filter is disabled in *Feature Select*.



In *Dashboard > Status*, when you click *Manage Widgets*, the Web Filter Detection widget is not available under Top 3 Lists.



MDM Integration

You can configure integration with a mobile device management (MDM) platform, such as VMware Workspace ONE. The following table provides descriptions for options that are common to all supported MDM platforms:

Option	Description
Enable MDM Integration	Enable MDM integration configuration.
Vendor	Select the desired MDM platform. This feature supports the following: • VMware Workspace ONE • Microsoft Intune • Jamf
Test Connection	After configuring other fields as the following tables describe, verify that EMS can communicate with the MDM platform.

For details on deployments using MDM, see:

- Workspace ONE Deployment Guide
- Intune Deployment Guide
- Jamf Deployment Guide
- ManageEngine Deployment Guide

The following provides descriptions for options that are specific to each MDM platform:

Workspace ONE

Option	Description
Site URL	Enter your site URL. Workspace ONE is a software-as-a-service deployment and each enterprise has a unique URL. The URL format is https://<unique identifier>.awmdm.com/api.
Smart Group Name	Enter the name of the Workspace ONE assignment group that contains the mobile devices to issue zero trust network access certificates to.
Authorization Type	Select *Basic Auth*, *Certificate*, or *OAuth 2.0* for the authorization between EMS and Workspace ONE. The on-premise version of Workspace ONE does not support OAuth. When using OAuth, ensure that you are using the SaaS version of Workspace ONE.
API Key	Available if you selected *Basic Auth* or *Certificate* for the authorization type. Enter the API key value from Workspace ONE.

Option	Description
Username	Available if you selected *Basic Auth* for the authorization type. Enter the Workspace ONE username.
Certificate	Available if you selected *Certificate* for the authorization type. Upload the certificate that you exported from Workspace ONE. You must create an admin user with certificate authentication and the *Console Administrator* role in Workspace ONE, and then export hthe certificate.
Password	Available if you selected *Basic Auth* or *Certificate* for the authorization type. Enter the Workspace ONE password.
Region	Available if you selected *OAuth 2.0* for the authorization type. Select your assigned geographic region. For redundancy, VMware has set up multiple servers to generate OAuth tokens
Client ID	Available if you selected *OAuth 2.0* for the authorization type. Enter the client ID from the Workspace ONE portal.
Client Secret	Available if you selected *OAuth 2.0* for the authorization type. Enter the client secret from the Workspace ONE portal.

Microsoft Intune

Option	Description
Tenant ID	Enter the tenant ID from Intune.
Authorization Type	Select *Client Secret* or *Certificate* for the authorization between EMS and Intune.
Client ID	Enter the client ID from Intune.
Client Secret	Enter the client secret from Intune.
Certificate	Available if you selected *Certificate* for the authorization type. Upload the certificate from Intune.

Jamf

Option	Description
Site URL	Enter your site URL.
Username	Enter the Jamf username.
Password	Enter the Jamf password.
Site Name	This field is optional. Enter the Jamf site name.

ManageEngine MDM Plus

Option	Description
Deployment	Select *On-Premise* or *Cloud* depending on your ManageEngine Mobile Device Manager (MDM) Plus deployment.
Site URL	Available for on-premise ManageEngine MDM. Enter your site URL. ManageEngine MDM Plus is a software-as-a-service deployment and each enterprise has a unique URL.
API Key	Available for on-premise ManageEngine MDM. Enter the API key value from ManageEngine MDM.
Region	Available for cloud ManageEngine MDM. Select your assigned geographic region. For redundancy, ManageEngine MDM has set up multiple servers.
Client ID	Enter the client ID from ManageEngine MDM.
Client Secret	Enter the client secret from ManageEngine MDM.

Deploying ZTNA certificates to FortiClient mobile via MDM

FortiClient (Android) and (iOS) 7.2.2 and later versions support zero trust network access (ZTNA) to create a secure connection via HTTPS. Use the following mobile device management (MDM) platforms to deploy ZTNA certificates to FortiClient (Android) and (iOS):

FortiClient mobile platform	Supported MDM platforms
Android	• Intune • ManageEngine
iOS	• Intune • ManageEngine • Workspace ONE • Jamf



ZTNA for TCP forwarding is unsupported.

Endpoint detection and response (EDR)

The FortiEndpoint EDR page (accessible from the FortiEndpoint menu) provides multi-layered, post- and pre-infection protection that stops advanced malware in real time. EDR 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. FortiEndpoint EDR's unique virtual patching technique, which only blocks malicious outbound communications, enables employees to continue working as usual even when their devices are infected.

Concepts and workflow

This section introduces general EDR concepts and provides an overview of the FortiEndpoint architecture and workflow:

- EDR terminology on page 561
- FortiEndpoint EDR components on page 564
- How does FortiEndpoint EDR work? on page 567
- Using FortiEndpoint EDR - workflow on page 567

EDR terminology

The following provides basic explanation of common EDR terms.

Execution prevention

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

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

Data exfiltration

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

EDR is a realtime targeted-attack exfiltration prevention platform.

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

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

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

EDR 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.

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

EDR 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.

EDR prevents, in real time, an attacker's attempt to encrypt or modify data. EDR 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.

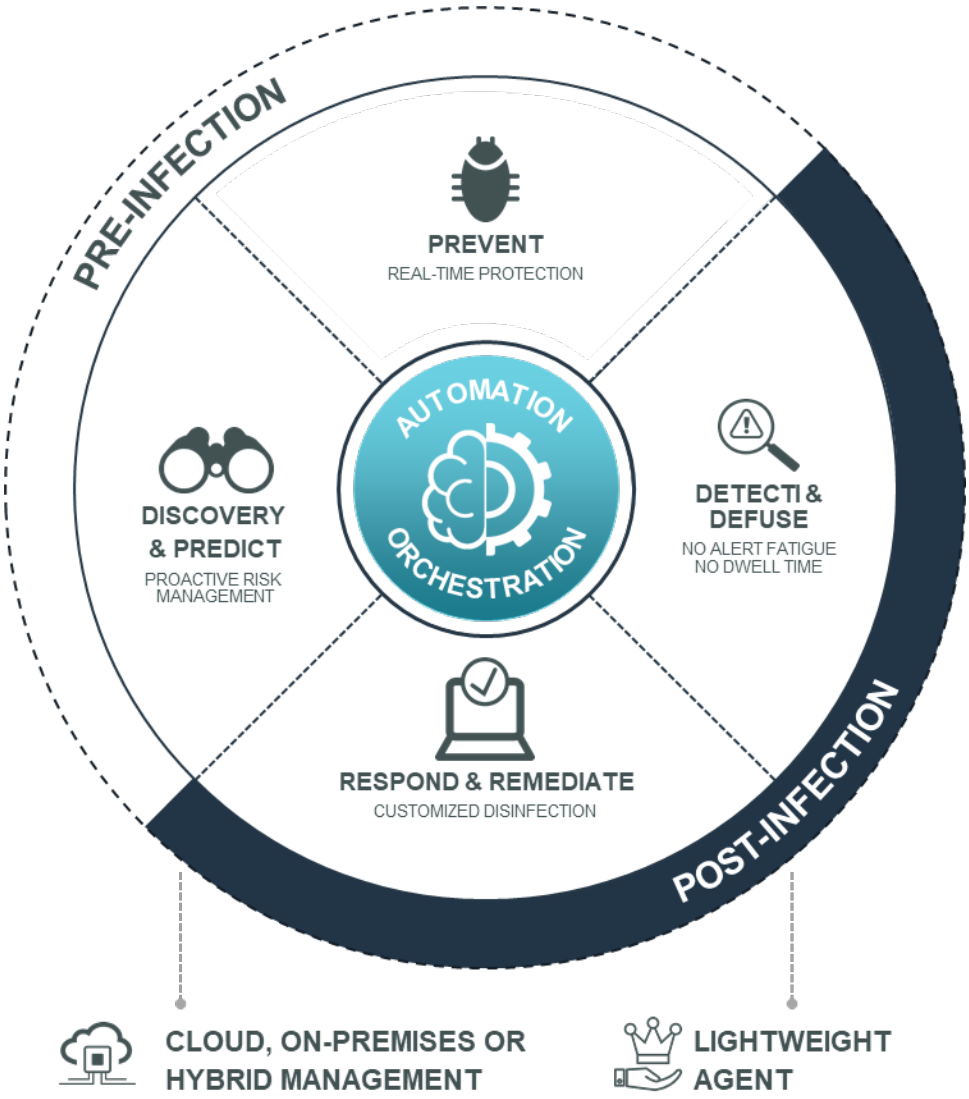
Threat hunting

EDR'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.

EDR 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.

EDR 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.

EDR 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.

EDR'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.

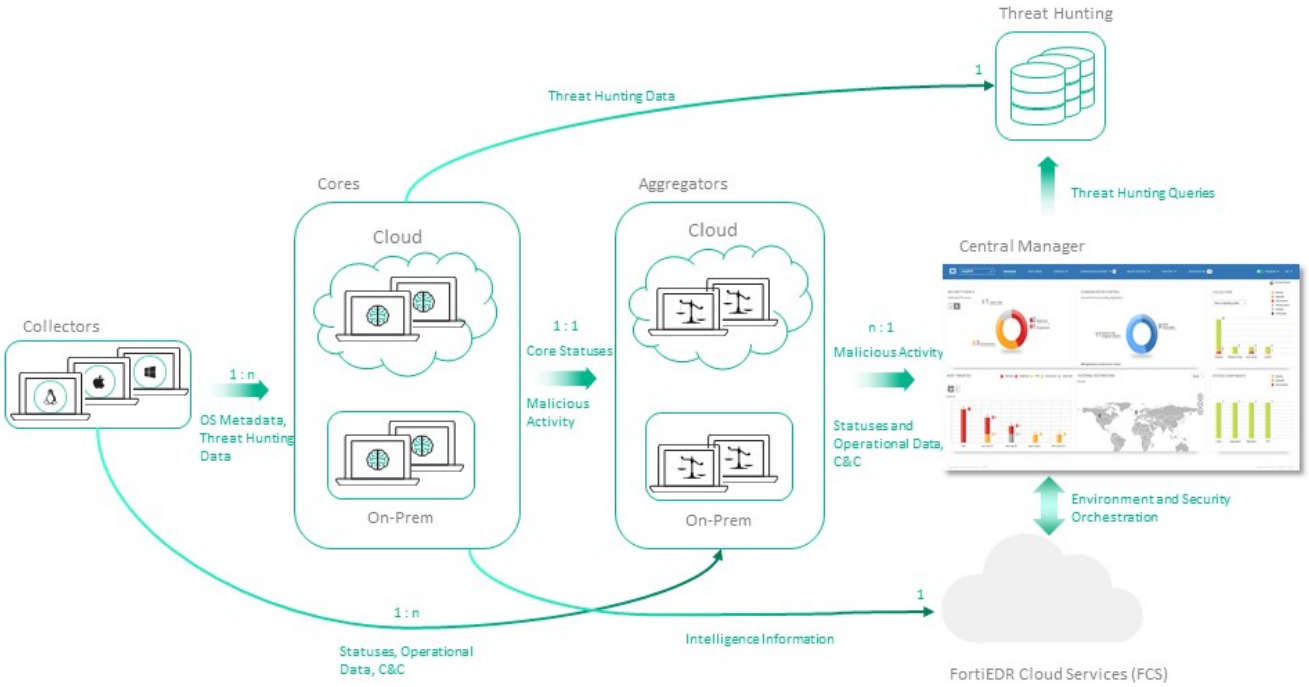
Our research revealed that all legitimate outgoing communications must pass through the operating system. Thus, by monitoring the operating system internals it is possible to verify that a connection was established in a valid manner. EDR gathers OS stack data, thread and process related data and conducts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

EDR'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.

FortiEndpoint EDR components

FortiEndpoint EDR collects the connection establishment flow of your organization's communicating devices directly from each device's operating system internals. EDR 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 FortiEndpoint EDR is comprised of the following components:



EDR Collector

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

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

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

An EDR Collector should be installed on each communicating device in your organization. The following are the connections established between the EDR Collector and other EDR components:

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



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

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

Negligible footprint

The EDR 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. EDR's traffic consumption requirements are low because the EDR Collector sends to the Core its activity events, the size of which depends on the amount of activity, and sends to the Aggregator security events which are small in size. Additionally, EDR uses message compression in order to further reduce the traffic sent to the network. You may refer to Collector System Requirements for the exact specifications of the system requirements.

The Windows *Incidents* view records whenever an EDR Collector blocks communication from a device, as described in Incidents on page 569.

EDR Central Manager console

The EDR Central Manager console (accessible from the FortiEndpoint menu) is a software-only central web user interface and backend server for viewing and analyzing events and configuring the system. Chapters from Profiles on page 673 to Threat Hunting on page 608 describe the user interface of the EDR Central Manager. The EDR Central Manager is the only component that has a user interface. It enables you to:

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

- Monitor system status and health

EDR Core

The EDR 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.

EDR 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 an EDR Core, thus enabling it to block each outgoing connection establishment request that is malicious.
- When the EDR Core receives a connection establishment request, it comes enriched with metadata collected by the EDR Collector that describes the operating system activities that preceded it.
- The EDR 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 EDR to determine where the foul occurred.



The EDR Core only reviews EDR Collector metadata without seeing the outgoing traffic.

The following are the connections established between the EDR Core and other EDR components:

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

EDR Aggregator

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

EDR Cloud Service

The EDR Cloud Service (FCS) enriches and enhances system security by performing deep, thorough analysis and investigation about the classification of a security event. The FCS is a cloud-based, GDPR-

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

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

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

- Tuning: Automated security event exception (allowlisting). After a triggered security event is reclassified as Safe, an automated cross-environment exception can be pushed downstream and expire the event, preventing it from triggering again. For more details, see Exception Manager on page 683
- Playbook Actions: All Playbook policy remediation actions are based on the final determination of the FCS. For more details see Remediation on page 790.

How does FortiEndpoint EDR work?

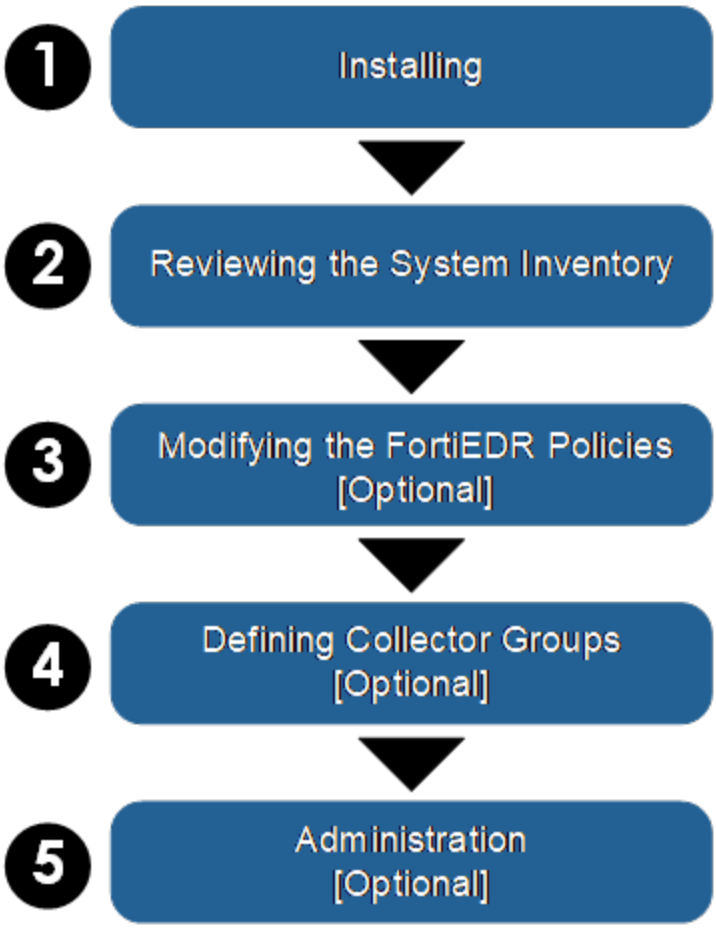
1. **The EDR Collector collects OS metadata**: An EDR Collector runs on each communicating device in the organization and transparently collects OS metadata on the computing device.
2. **Communicating device makes a connection establishment request**: When any connection establishment request is made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

Using FortiEndpoint EDR - workflow

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

Setup workflow overview

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



1. **Installing**: Install all EDR components, as described in Deploying FortiEndpoint, Adding a FortiClient deployment package, and Installing FortiEndpoint on an endpoint and registering to FortiEndpoint EMS on page 16.
2. **Reviewing the Inventory**: Review the health status and details of all the EDR components in the FortiEndpoint EMS dashboard. EDR Collectors are automatically assigned EDR's default policies.
3. **[Optional] Modifying the EDR Policies**: By default, the EDR policies are ready to log out-of-the-box. If needed, use the Profiles on page 673 to modify the default policies for blocking and/or to create additional policies.
4. **[Optional] Defining Collector Groups**: By default, the EDR default policies are assigned to a default Collector Group that contains all EDR Collectors. Policies in EDR are assigned per Collector Group. You can assign the required policy to each Collector Group (see Assigning a security policy to a Collector Group on page 681)
5. **[Optional] Administration**: The EDR system installs with a single administrator user. This user can:
   - Create additional users of the EDR Central Manager.
   - Define the recipients to receive email notifications of EDR events.
   - Configure a SIEM to receive notifications of EDR events via Syslog.

Ongoing workflow overview

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



- **Monitoring**: Monitor and analyze the events triggered by EDR in the following locations:
  - FortiEndpoint EMS Dashboard on page 34
  - Incidents on page 569
  - Syslog on page 793
- **[Optional] Creating Event Exceptions**: EDR precisely pinpoints interesting system events. However, if needed, you can create exceptions in order to stop certain events from being triggered for certain IP addresses, applications, protocols and so on. See Playbooks on page 784.
- **[Optional] Investigating Events**: Deep investigation into a security event, including meta data. You can also audit all operating system activities with Threat Hunting on page 608.
- **[Optional] Handling Events**: Mark security events that you have handled and optionally describe how they were handled. See Marking a security event as handled/unhandled on page 597.

Incidents

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

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

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

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

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

Event Aggregation

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

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

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

- You can drill down on a device/process to display the security events for that device/process. Each security event row is marked with a flag indicator.
  In the Process view, the Destinations column indicates the number of destinations to which the process attempted to connect. If only one destination was accessed, its IP address is shown. If more than one destination was accessed, the number of destination IPs is shown in the Destinations column.
  In the Process view, the Device column indicates the number of devices the malware attempted to attack. If only one device was attacked, its device name is shown. If more than one device was attacked, the number of devices is shown in the Device column.
- You can drill down further in a security event row to view the variants for that event by clicking on the icon. Variants display the relevant information collected by EDR from the device. For example, if a specific process was connecting to 500 destinations, then 500 variant rows display for that security event. For example, in the figure below, the security event comprises 2 variants, coming from different devices and going to different destinations. You can click the < Back icon to return to the aggregated security event view.

The following actions can be performed in the Incidents view:

- Marking a security event as handled/unhandled on page 597
- Manually changing the classification of a security event on page 598
- Viewing Application Control security events on page 600
- Viewing Device Control security events on page 601
- Other options in the Incidents viewer on page 602

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

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

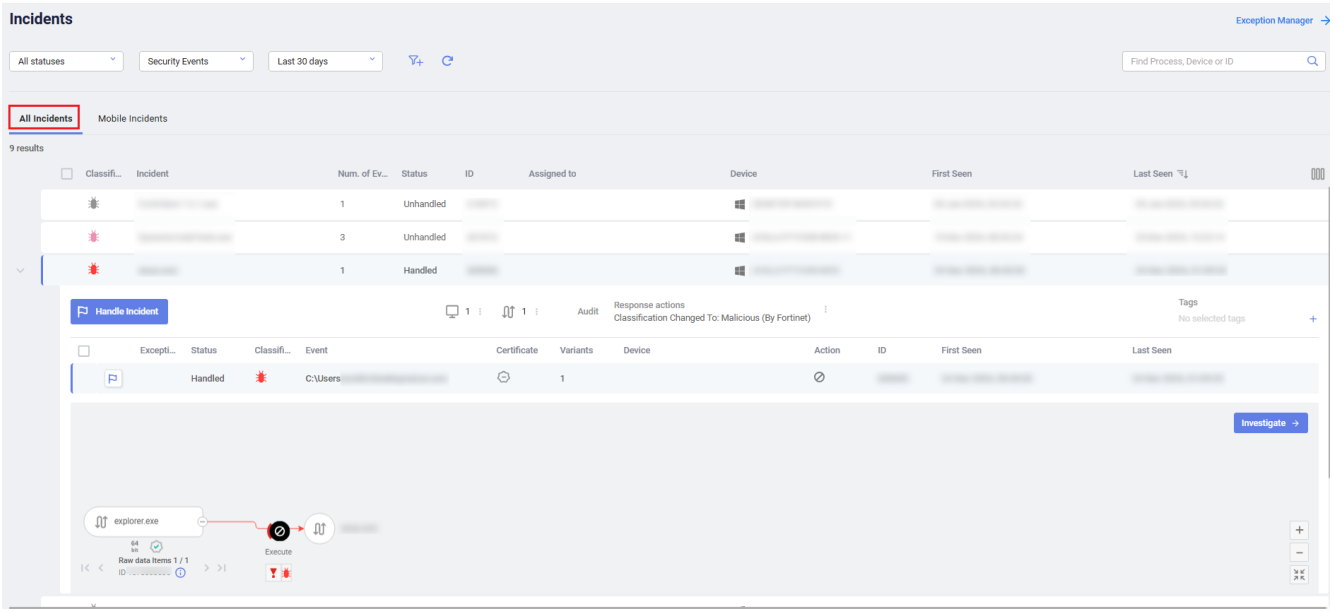
In some cases, *Updated* displays next to the number of new unread security events indicator. Updated means that EDR originally classified one of the unread events, but that classification was later changed by

the user. After more data for this security event was received, EDR overrode the manual classification of the event by the user and changed the classification for the event again, based on the newly received data.

Incidents pane

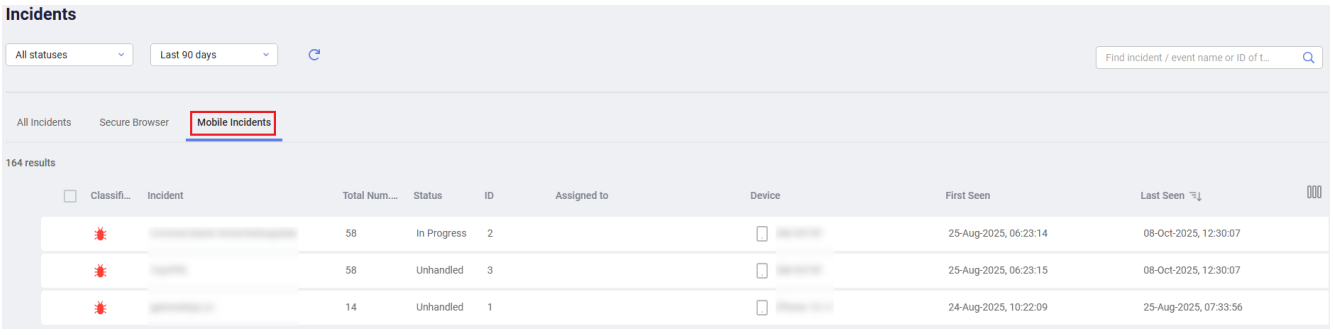
Clicking a security event expands it to show more details and enables the buttons at the top of the window. The following information is provided for each security event:

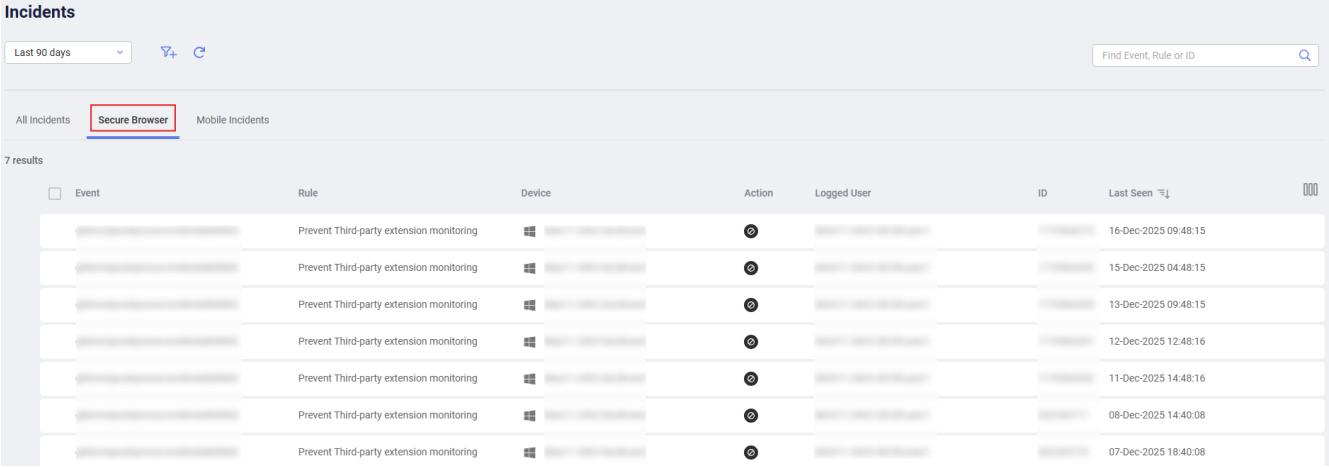
Desktop incidents:



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

Mobile Incidents and **Secure Browser**:





The mobile incidents view displays incidents specific to Mobile and secure browser view displays incidents specific to Secure Browser on page 710. The details for each mobile or secure browser incident are similar to those in the desktop incidents view except that the *Investigate* button is unavailable.

Information Field	Description
View Indicator	Indicates the view context for the security event aggregation. displays for a device and displays for a process.
Handled/Not Handled	Specifies whether any EDR Central Manager user handled this security event, as described on Marking a security event as handled/unhandled on page 597
ID	Specifies an automatically assigned unique identifier for each security event generated by EDR. 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 the Core but can be changed either automatically as the result of additional post-processing, deep, thorough analysis and investigation by the EDR Cloud Service (FCS) or manually. See Overview on page 575 for more detailed information about the classification of the event, such as the classification history. Classifications are as follows:

<table>
<tr><th>Information Field</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Icon</th><th>Classification</th><th>Definition</th><th>Recommended Action</th></tr>
<tr><td>  </td><td>Malicious</td><td>Events with the following characteristics:
Verified to have malicious capability
Intended to harm the infected device
Have no commercially viable use</td><td>Remediate</td></tr>
<tr><td>  </td><td>Suspicious</td><td>Events that behave in ways that strongly indicate malware, but are not verified malware.</td><td>Review and remediate</td></tr>
<tr><td>  </td><td>Inconclusive</td><td>Further investigation needed to determine if the event is malicious.</td><td>Administrator review</td></tr>
<tr><td>  </td><td>PUP (Potentially Unwanted Program)</td><td>Events triggered by programs that are bundled with legitimate software or commercial software that may be used for malicious purposes, for example, torrents.</td><td>Administrator to review whether the program should be removed (recommended) or allowed</td></tr>
<tr><td>  </td><td>Likely Safe</td><td>Events that probably carry no risk, and are most likely legitimate.</td><td>Administrator review</td></tr>
<tr><td>  </td><td>Safe (Confirmed Safe Software)</td><td>Events triggered by legitimate software that was intended for use by the customer, for example, security software.</td><td>No action necessary</td></tr>
</table>
</td></tr>
<tr><td>Received</td><td>Specifies the first time that this security event was triggered. For aggregations, the earliest received time is displayed.</td></tr>
</table>

Information Field	Description
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. EDR 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. • **Post Detection**: The exfiltration attempt was detected after the FCS verdict, which means the event is already running on the Collector. We recommend isolating the Collector for security. • **Simulated Post Detection**: The policy that protected this device was set to *Simulation* mode. Therefore, the exfiltration attempt was detected after the FCS verdict but the event is not running on the Collector. If the policy had been set to *Prevention* mode, the event would have been running on the Collector and you would have to follow the recommenation of isolating the Collector for security.

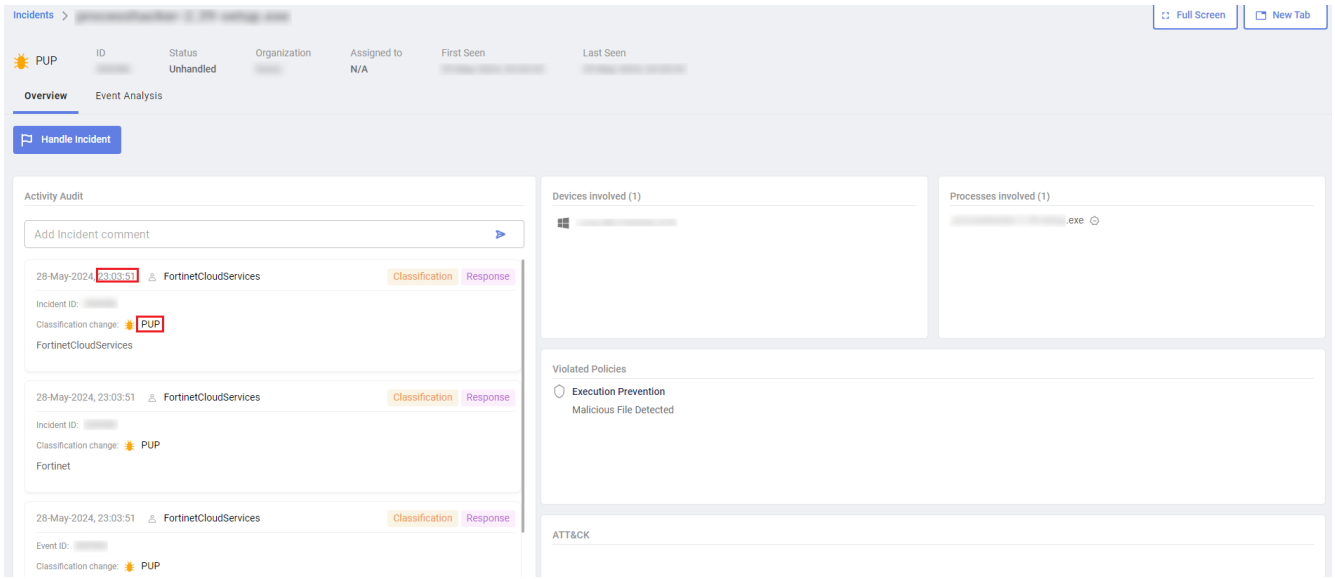
For variants, the following information is available:

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

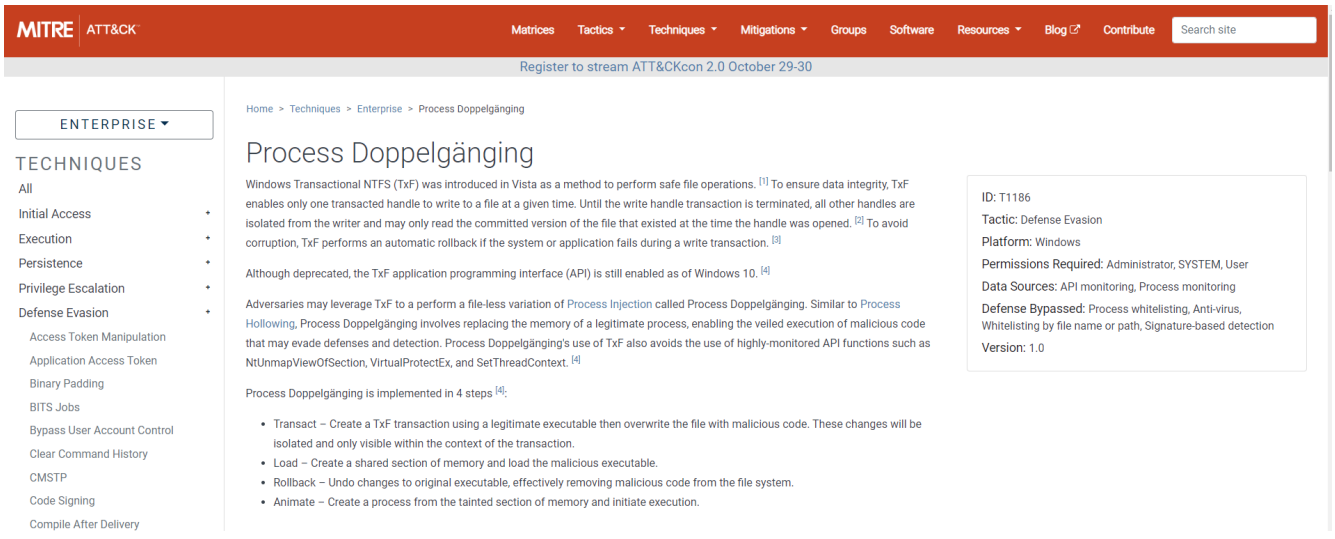
Overview

After you select an incident in the Incidents pane on page 571 and click *Investigate*, the *Overview* pane displays detailed information about the audit history, violated policies, and rules assigned to the EDR Collector that triggered this security event.

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



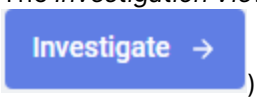
The ATT&CK section lists techniques that were used in this incident based on the MITRE ATT&CK common techniques scheme. Clicking the technique opens the MITRE web page, providing additional details, as shown below.



In the *Violated Policies* pane, only policies that were violated are displayed. The rule's configured action is displayed for each rule, as defined in *POLICIES*. The Action that was actually executed is displayed in the

action column of the *Incidents* pane of this window. The action taken is determined by the rule with the highest priority.

Investigation View

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

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

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

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

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

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

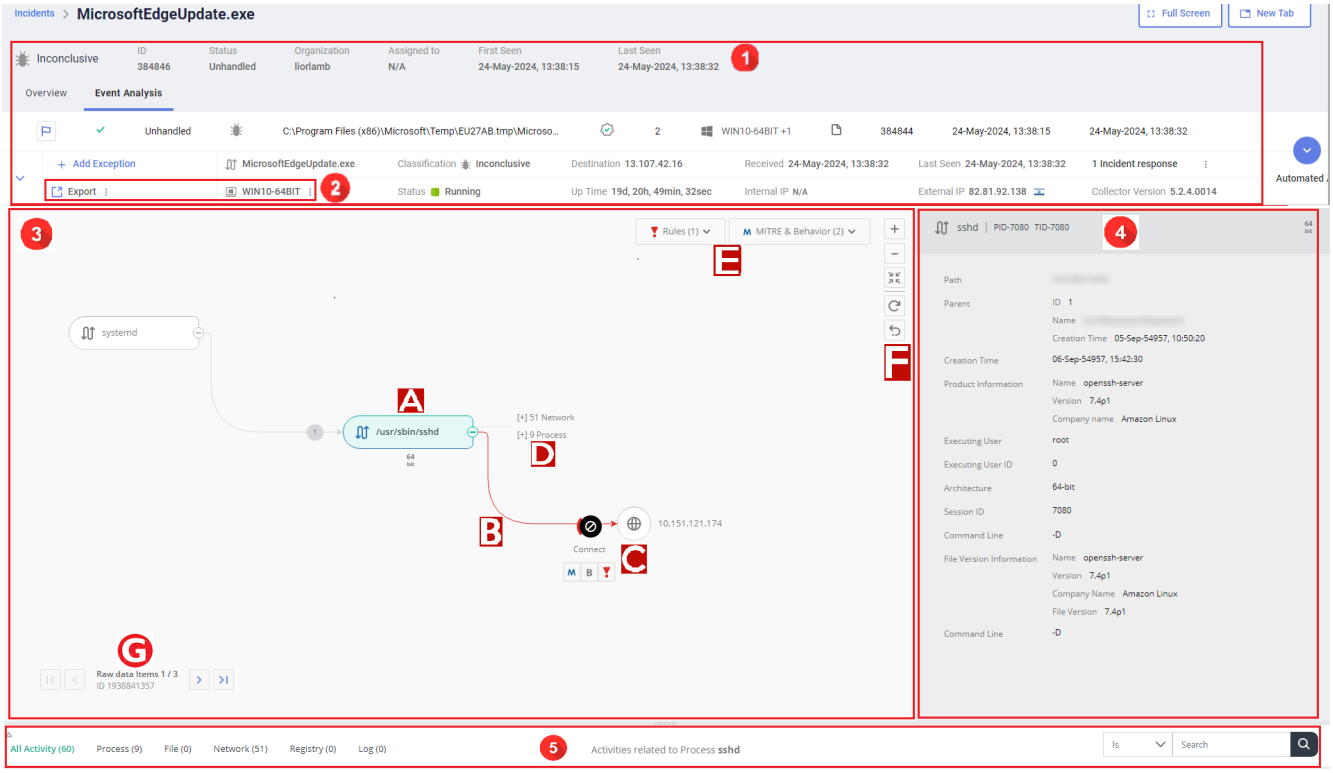
You can also perform certain actions, such as:

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



The view adds visualization and interaction of existing data that is already available in other non-graphical and non-interactive forms without creating or generating any additional data.

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

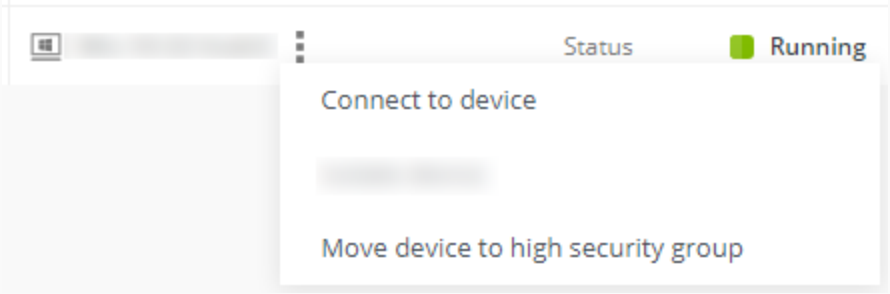
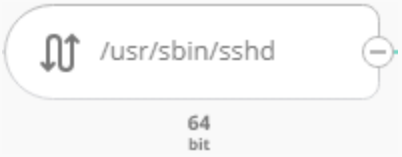


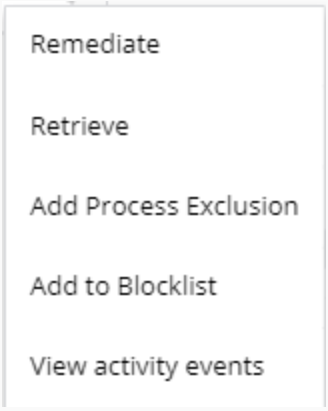
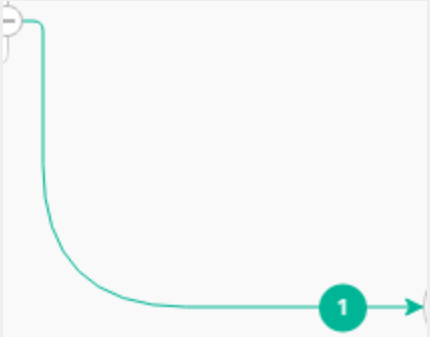
Compared with the investigation view window launched from the Details Pane under *Threat Hunting*, this view includes the following additional functionality:

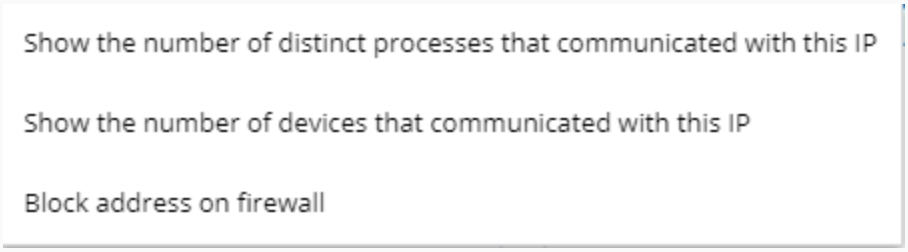
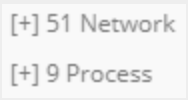
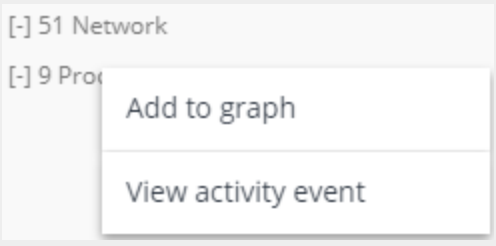
- Advanced threat hunting and investigation capabilities, such as exporting the graph as JSON, variants navigation graph, and Stacks view on page 583.
- General event details in the first row, such as classification and incident response.

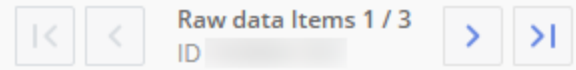
Component	Description
1	General details about the event, such as event ID, process name, classification, IP address, and incident responses.

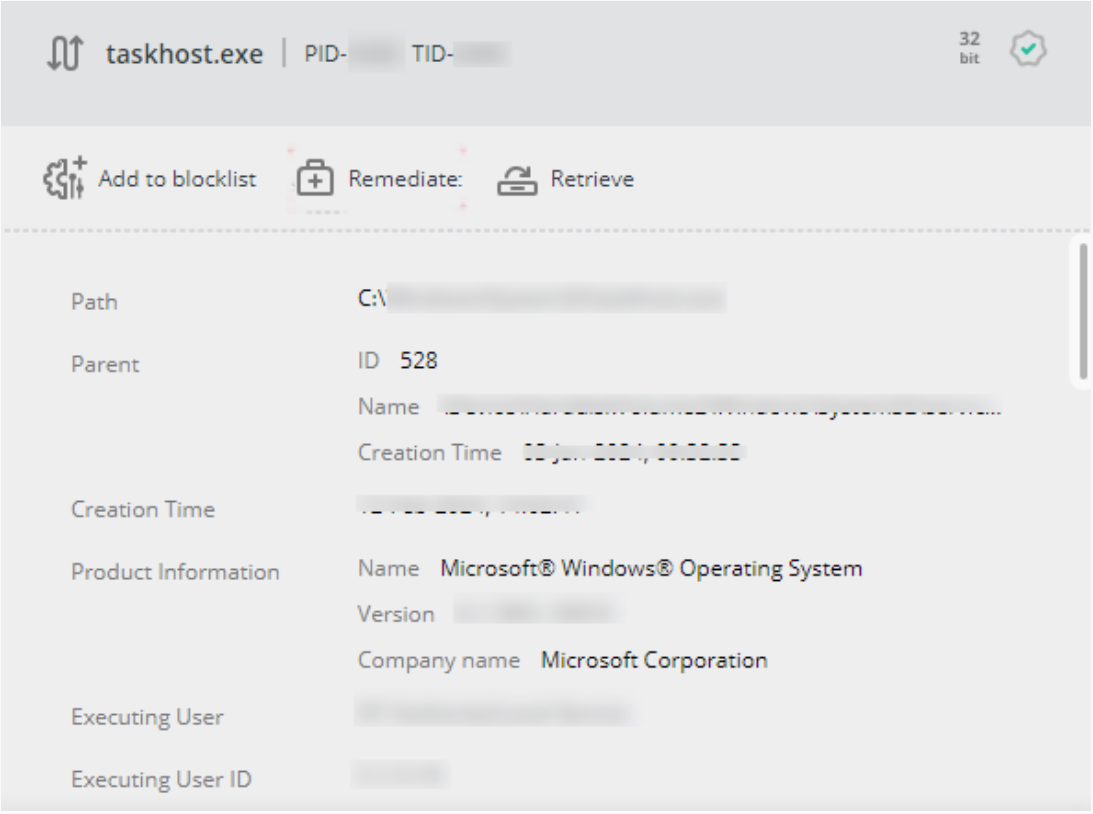
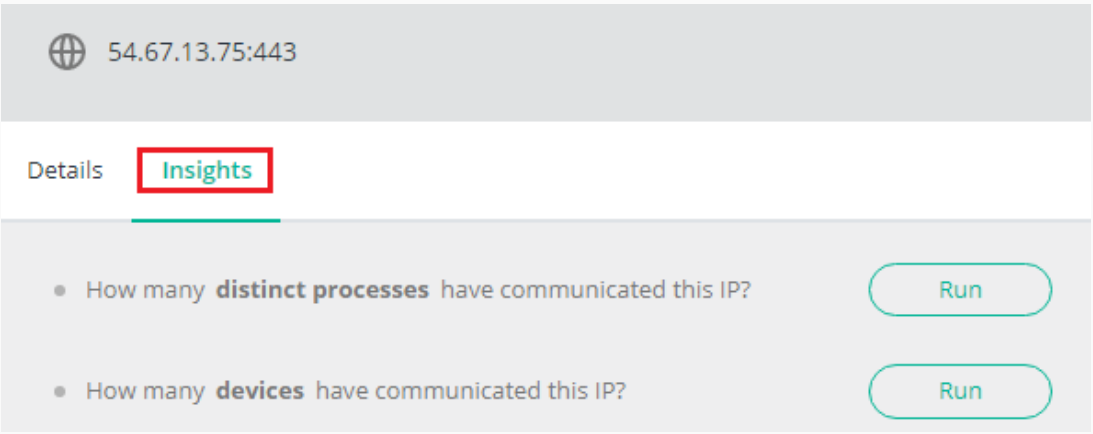
2	• Use the *Export* button (Export) to save files for sharing or record reasons:
	  • *JSON*—Export the event data as a JSON file.
	  • *SVG*—Export the investigation view graph as an SVG file. This is the only option to save a graph that includes dynamic changes based on the default graph view, such as adding processes.
	 
	
	• Use the following buttons, accessible by clicking the eclipses on the right of the

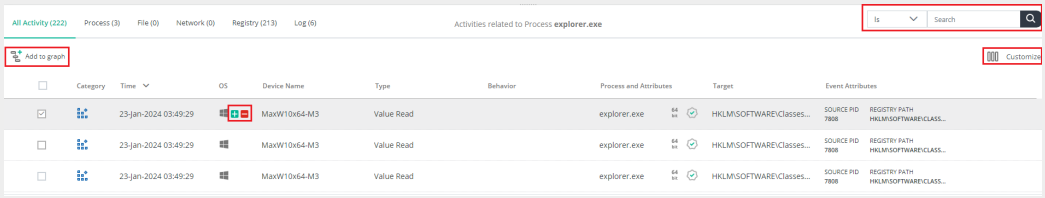
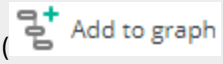
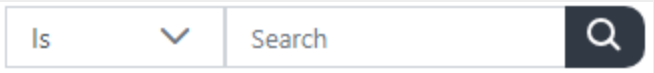
Component	Description
	device name, to connect to a device or move the device to high security group. 
3	Graphical flow diagram with a process tree that you can build according to your investigation needs, from left to right and top to bottom. The tree is also interactive, which means you can click on a specific component to drill down for more details or contextual actions.
A	**Node**—Source of an activity or event, which can be a process, an endpoint, a thread or service, or another security product. Nodes are represented by boxes with icons for the activity type, some with descriptions under the boxes.  • Click on a node to display the Details pane on page 628 on the right and the Activity events tables on page 624 on the bottom with contextual information about that specific node. • Click the *Collapse* ( ) or *Expand* ( ) icon in the right of a node icon to show or hide all the downstream nodes, edges, and leaves. • Right-click a node to perform actions allowed on the node, including any custom actions you defined. These action buttons also appear in the *Details Pane*, which is available on the right after you click the node. The list of available options varies by node type. The following is an example list of actions for a process node.

Component	Description
	
B	**Edge**—Activity event type or action represented by a curved line with an arrow. An edge can be one activity event/action or an aggregation of several. The numbered arrows indicate the sequence of actions and specify the action that was performed, such as *Process Creation*, *Socket Close*, *Block* and so on. Multiple operations performed between two processes are represented by multiple arrows between them. Edges that triggered the event are indicated in red.  Click on an edge to display the Details pane on page 628 on the right and the Stacks view on page 583 on the bottom with contextual information about that specific edge. Edges may also have icons below them indicating classification or violation of certain rules and MITRE & Behavior models. Click on an icon for more detailed information. 

Component	Description
C	**Leaf**—Target of activity event of type File, Registry Key, Registry Value, Network components (IP/DNS/URL). A leaf can also be a group of artifacts. For example, all the files created or modified by a process. Leaves have a round shape (). • Click on a leaf to display the Details pane on page 628 on the right and the Activity events tables on page 624 on the bottom with contextual information about that specific leaf. • Right-click a leaf to perform actions allowed on the leaf, including any custom actions you defined. These action buttons are also available in the *Details Pane*, which appear on the right after you click the leaf. The list of available options varies by leaf type. The following is an example list of actions for a network leaf: 
D	**Hint**—Categorized groups of activities related to a node that are not part of the main chain of activity events and thus not represented in the graphical diagram. Click a node to show the number of relevant activities. The hints no longer display after you move the selection to another node or edge.  • Click the *Expand* ([+]) or *Collapse* ([-]) icon near a leaf hint to show or hide the node or leaf list of that type. • Right-click the type name of a hint and select *Add to graph* to add the relevant leaves to the graph or select *View activity event* to pull out the Activity events tables on page 624 for this specific file type. The *Add to graph* option is unavailable when the number of hints exceeds 500, in which case you can only choose to view the activity event. 

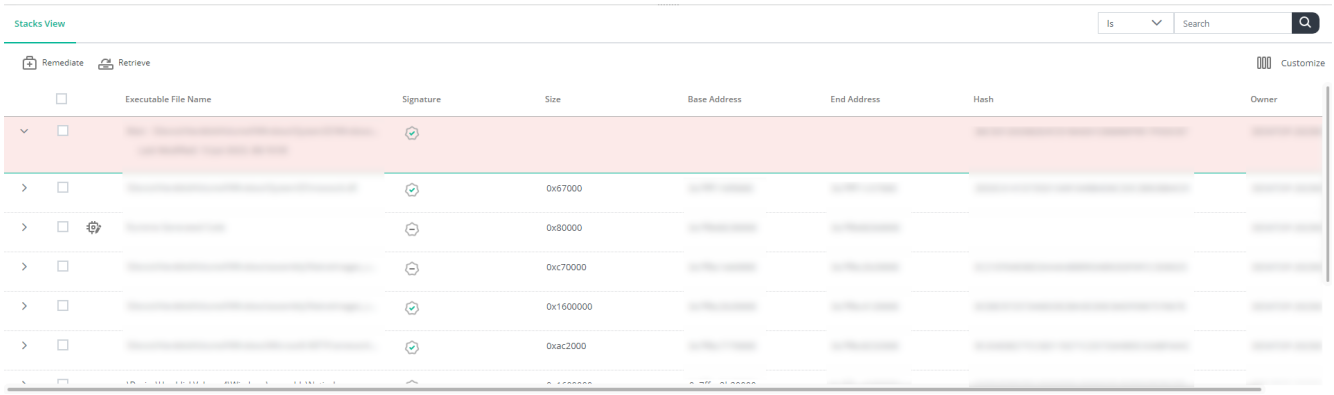
Component	Description	
	E	Use the *Rules* or *MITRE & Behavior* legends to highlight the corresponding icons below relevant edges in the diagram. 
	F	• Use the *Zoom In* ( ), *Zoom Out* ( ), and *Zoom To Fit* ( ) buttons to adjust the graph window size. • Use the *Reset* ( ) button to restore the graph to the default view. • Use the *Undo* ( ) button to cancel an operation.
	G	Navigate between the graphs of the various variants for a security event using the right and left arrows. 
4	Details pane on page 628 for the selected node, edge, or leaf where you can view details of the activity, action, or target, and perform common actions on a node or leaf, such as retrieving a file, remediating devices upon malware detection, or adding an application to the Application Control policy blocklist. The actions can also be performed by right-clicking a node or leaf and selecting the option from the menu.	

Component	Description
	 For specific leaf types, this pane also includes an *Insights* tab which allows you to run queries to retrieve analytics data, such as the number of communicating processes or devices of a certain IP. The *Insights* options are also available from the right-click menu of those leaf types. 
5	• When a node or leaf is selected, the contextual Activity events tables on page 624 appears at the bottom, which is organized by tabs of activity types. Drag the top edge of the table up for a fuller view of the table. Activities with a number at the front of the row are already in the graph and the number matches the one in the graph.

Component	Description
	 • To add activities to the graph, select the corresponding rows and click *Add to graph* (). • To customize the columns to display in the table, click *Customize* (). • To search for a specific activity or event, enter keywords in the search bar on the top right corner (). • To filter the results in the Activity Events table to include or exclude a specific value, use the green plus () and red minus () icons that appear when you hover over the value. Multiple filters are supported. To delete a filter, click the cancel icon that appear when you hover over the filter on the top-left of the table. • When an edge is selected, the Stacks view on page 583 appears at the bottom instead.

Stacks view

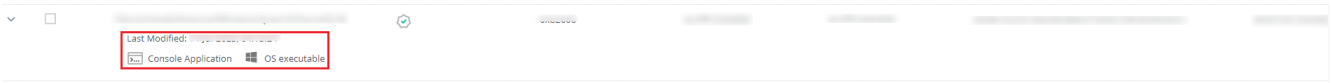
The stacks view displays the stacks that were collected during the action performed between two process nodes in the Investigation View on page 576 when an edge is selected. The stack entries include the executables and DLLs involved in the process stack. The stack entries due to which the event was triggered are highlighted with a red background. The main stack entry, which means the first one, is marked with a separator.



For each executable, you can see the following information:

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

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



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

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

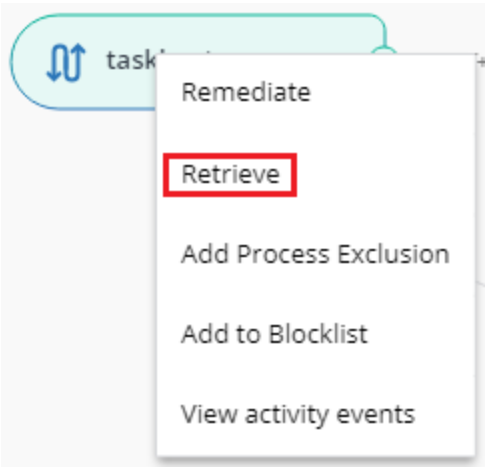
Retrieving memory

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

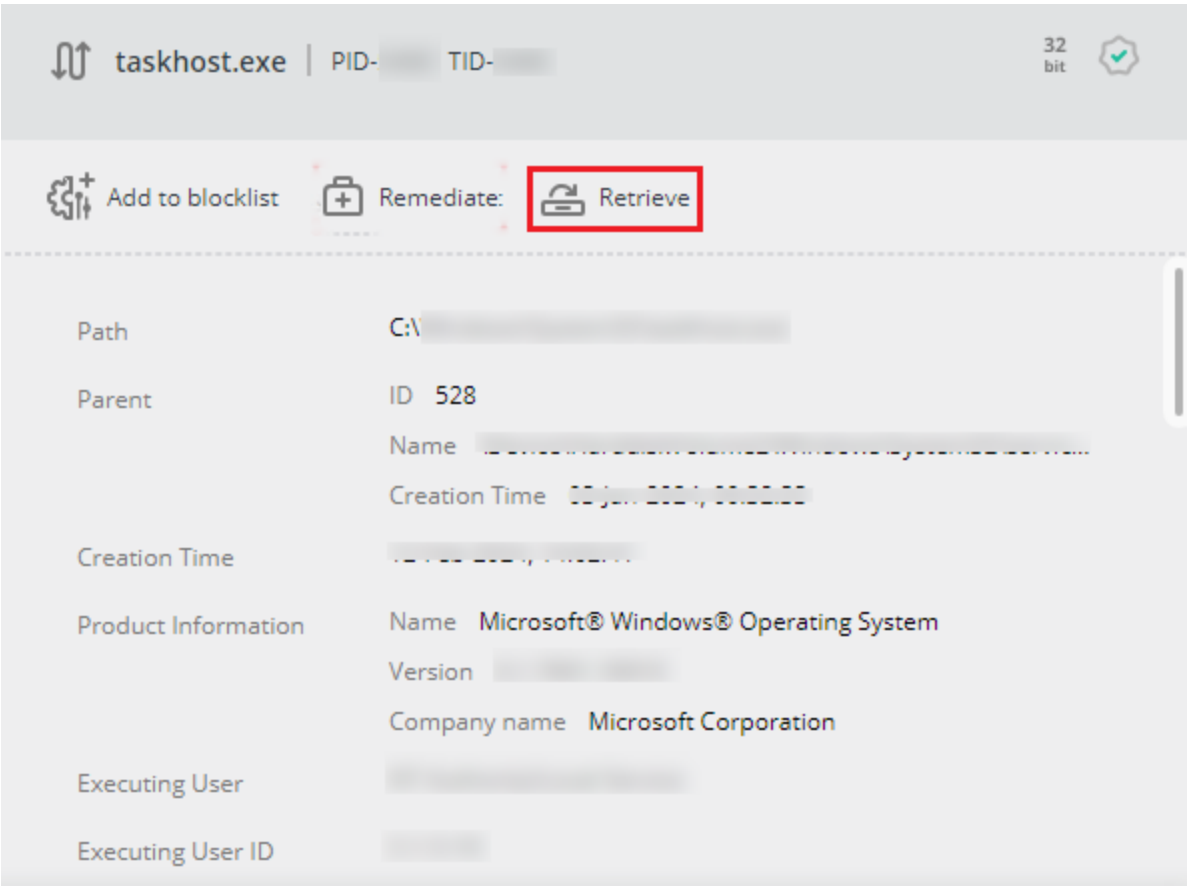
This function is accessible from the Investigation View on page 576 (detailed in the procedure below) or by connecting to the device directly using the EDR Connect on page 592 functionality.

To retrieve memory for a Collector from the investigation view:

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

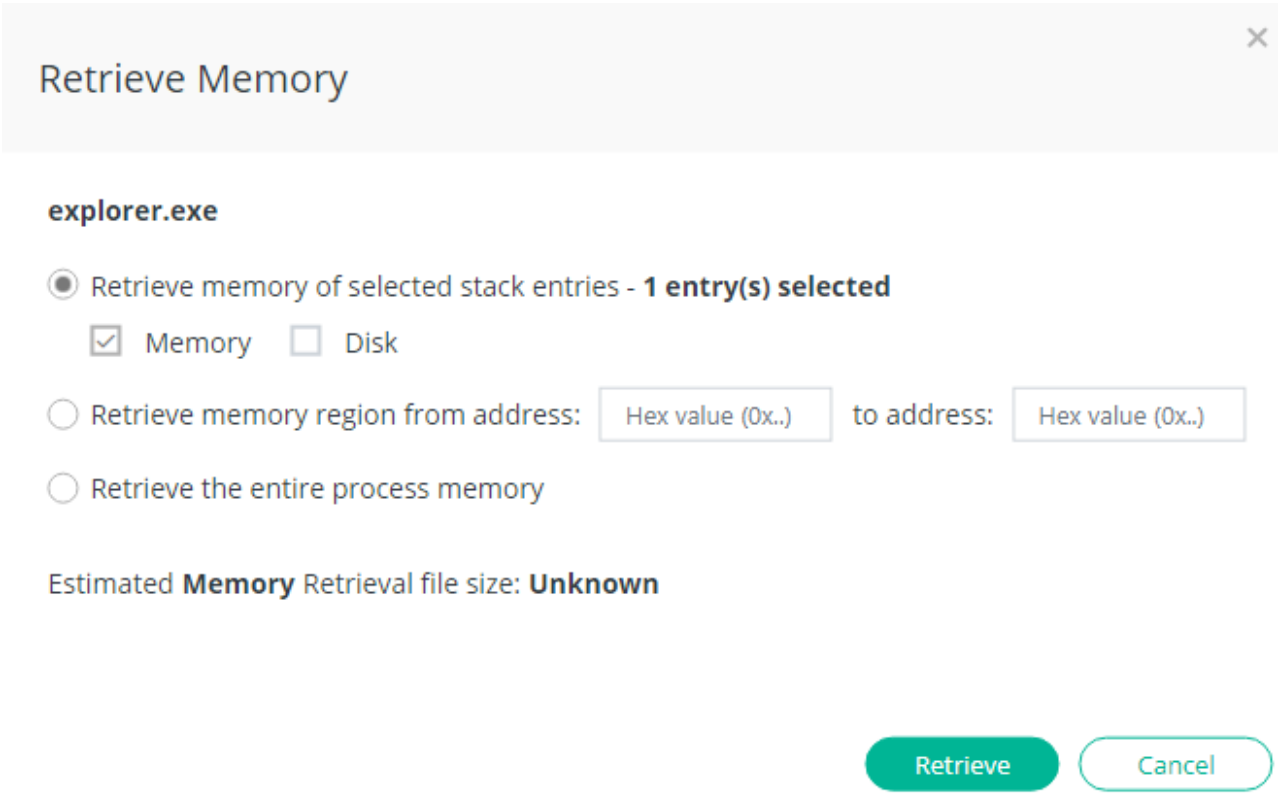


Alternatively, select the node of the relevant activity event and click the *Retrieve* button in the *Details Pane* that appears on the right.



The *Retrieve* button is also available from the Stacks view on page 583, which is available when an edge is selected.

2. The following window displays:



3. Select one of the following options:
   a. *Retrieve memory of selected stack entries*: Select this radio button to retrieve memory for one or more specific stack entries. Then, select the stack entries you want to analyze by checking their checkboxes.
   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.
   b. *Retrieve memory region from address*: Select this option to retrieve memory from a specific memory region. Specify the *To* and *From* addresses for the region in the adjacent fields.
   c. *Retrieve the entire process memory*: Select this option to retrieve memory for an entire process. This option retrieves all the stack entries comprising the process.
4. Click *Retrieve*.

Remediating a device upon malware detection

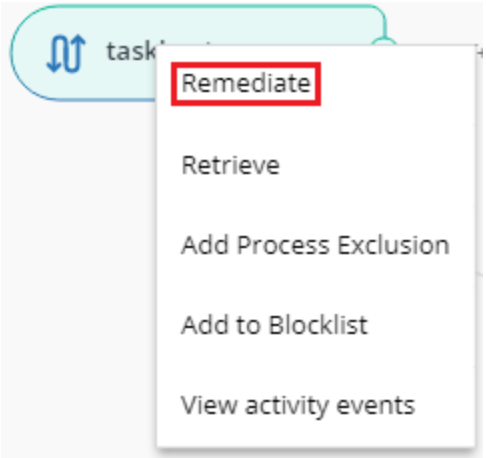
After malware is detected on a device, you can remediate the device from the Investigation View on page 576 (detailed in the procedure below) or by connecting to the device directly using the EDR Connect on page 592 functionality.

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

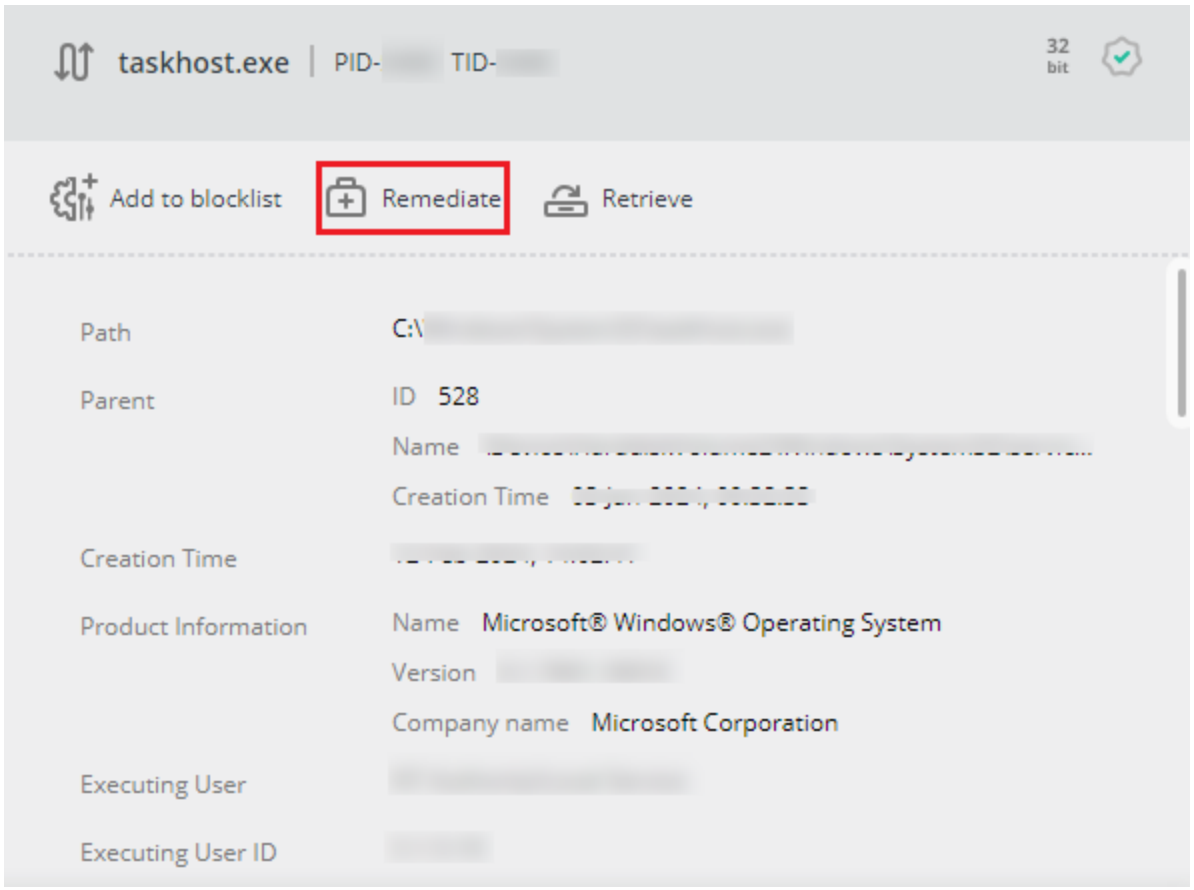
Method	Description
Terminate the Process	This method does not guarantee that the affected process will not attempt to execute again.
Delete the Affected File from the Computer	This method ensures that the file does not attempt to exfiltrate data again, as the file is permanently removed from the device.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

To remediate a device from the Investigation View on page 576:

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

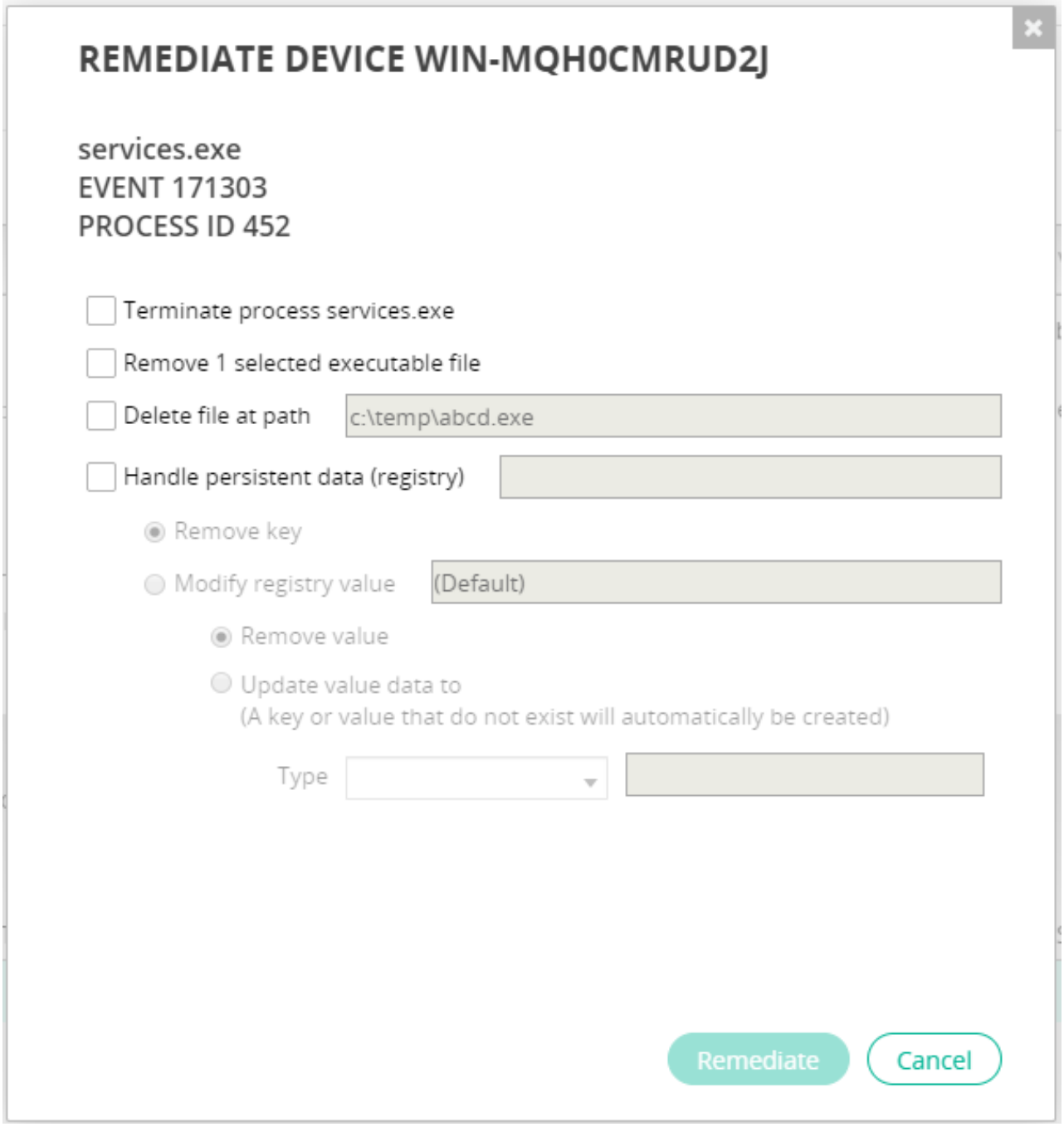


Alternatively, select the node of the relevant activity event and click the *Remediate* button in the *Details Pane* that appears on the right.

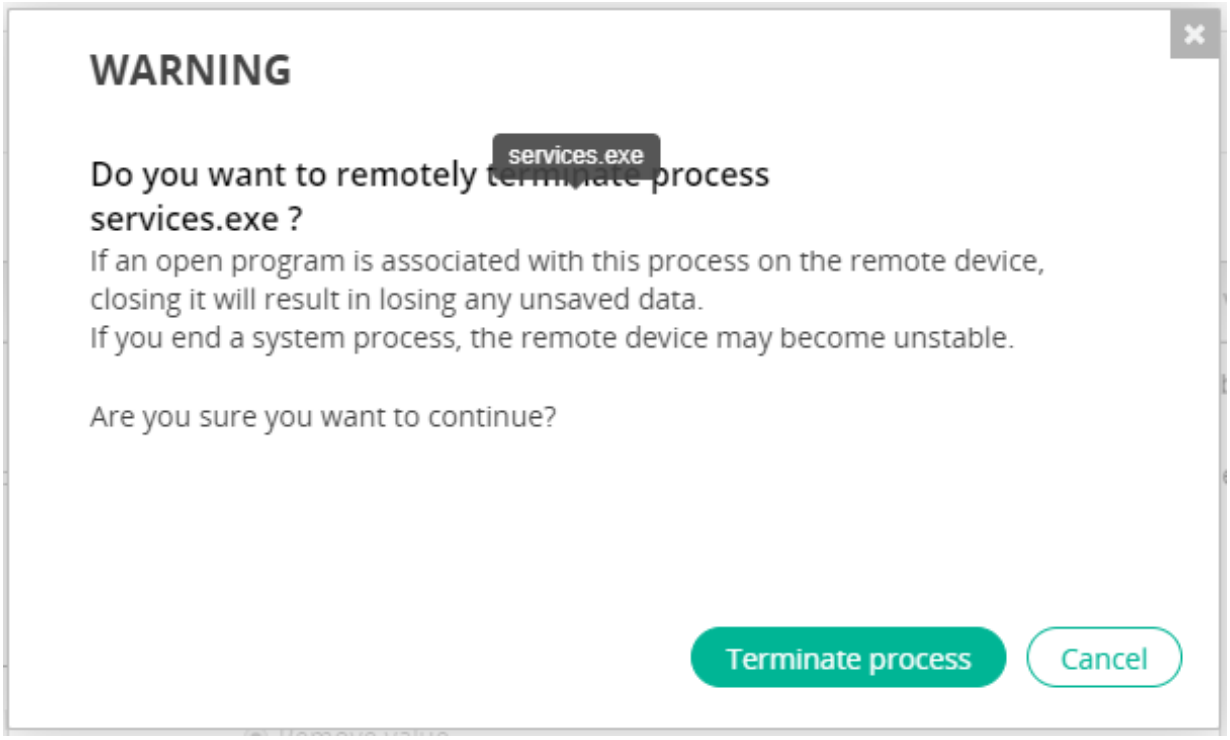


The *Remediate* button is also available from the Stacks view on page 583, which is available when an edge is selected.

2. The following window displays:

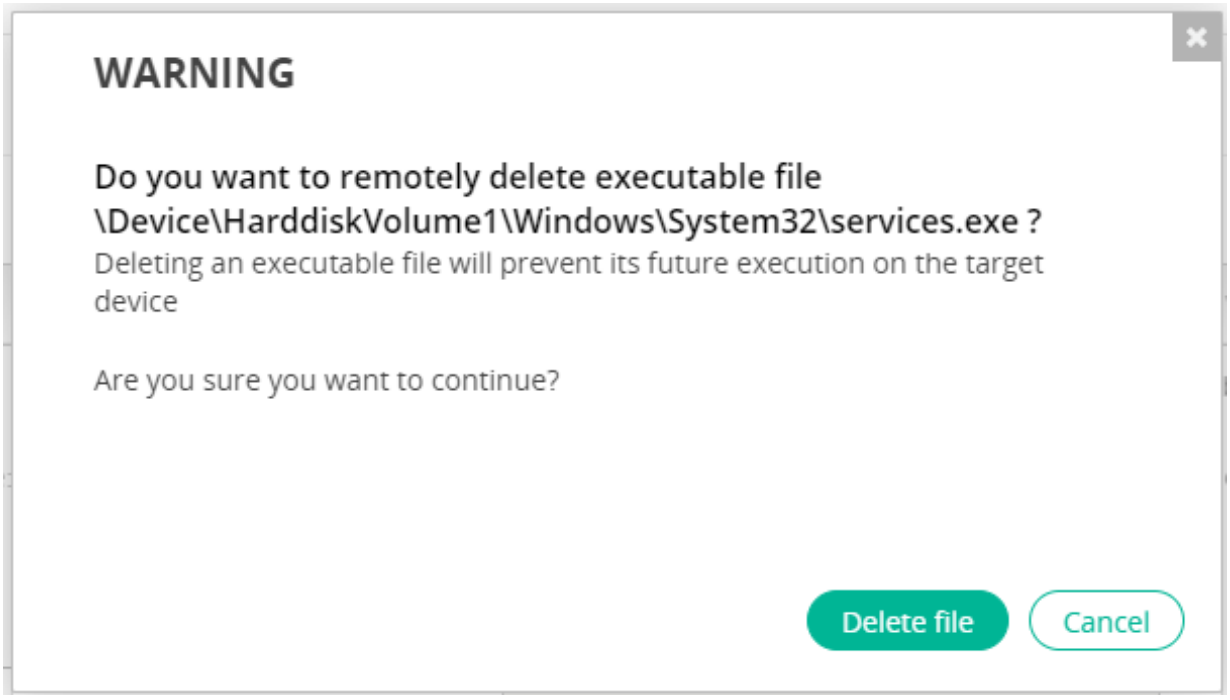


3. Do one of the following:
   a. Check the *Terminate process* checkbox to terminate the selected process. A warning message displays.



Click *Terminate process* to terminate the selected process.

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

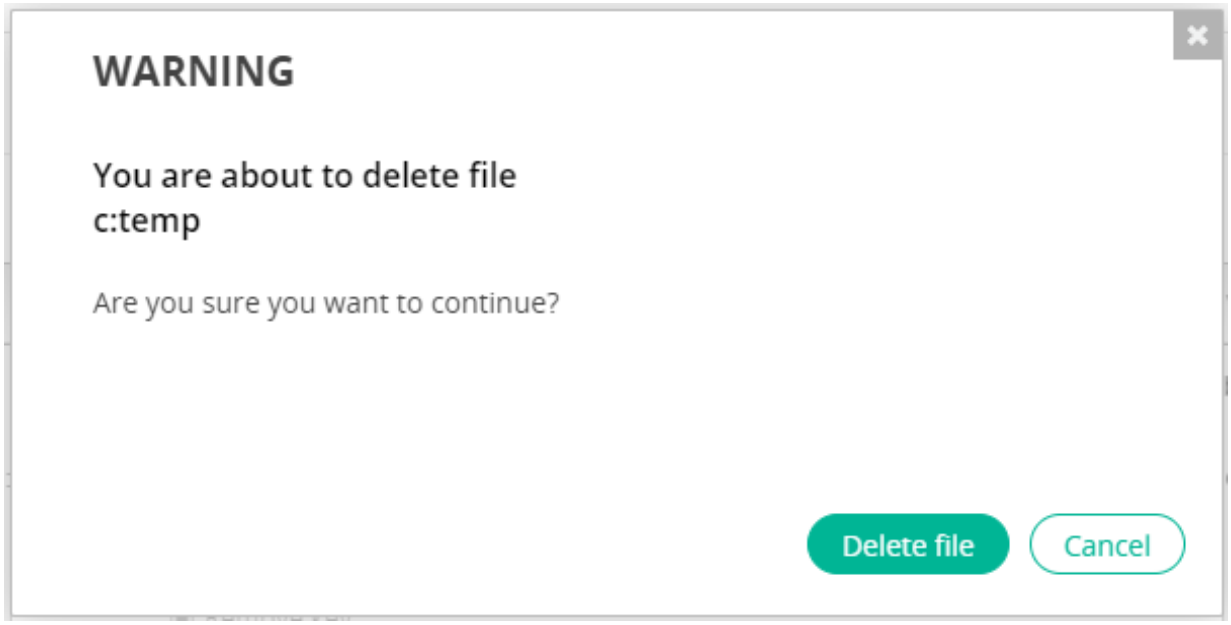


Click *Delete file* to remove the selected file.

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

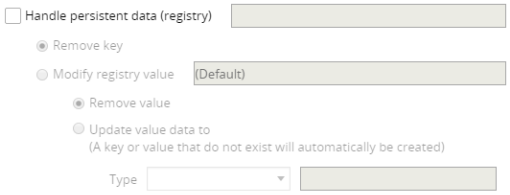


A warning message displays.



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

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



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

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

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

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

4. Click *Remediate*.

EDR Connect

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

An EDR Connect console can be accessed from various EDR pages that list devices, such as the *Threat Hunting on page 608* tab and the Investigation View on page 576.

- A *Connect to Device* button appears at the top of these pages, which enables you to connect to the device that is selected in the list.
- You can only connect to a single device in each EDR Connect session. See Connecting to an EDR-protected device on page 592.
- A device can only be connected to a single session at a time.
- Each EDR user can have up to ten EDR Connect sessions open and connected at the same time – each to a different device.
- Multiple users in your organization can open up EDR Connect sessions (on the EDR Manager), but no more than 30 sessions can be opened at the same time.

Connecting to an EDR-protected device

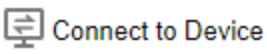
The following describes how to open an EDR Connect console session that connects you directly to an EDR-protected device.

To directly access an EDR-protected device:

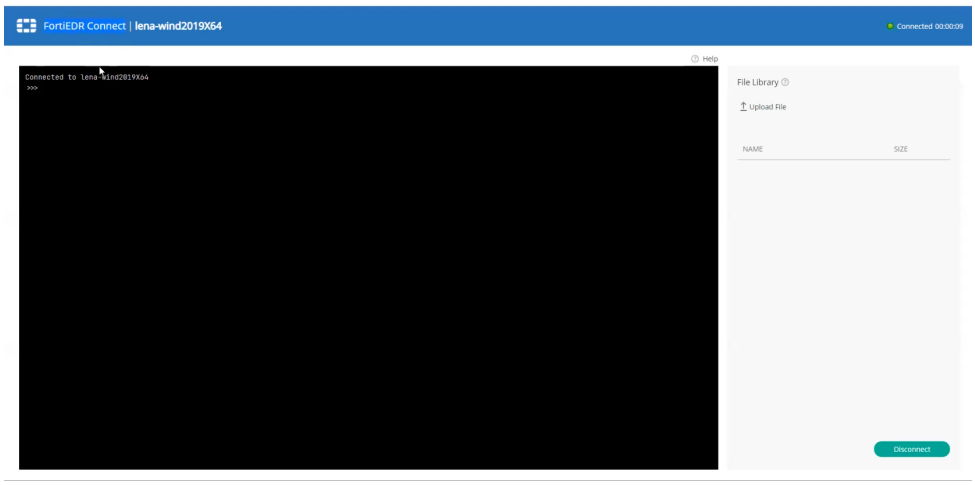
1. An EDR Connect console can be accessed from various EDR pages that list devices, such as the *Threat Hunting on page 608* tab and the Investigation View on page 576. The operation of the EDR Connect console is the same regardless of where it was accessed from.
2. Select the relevant device from the list.
   You can only connect to a single device at a time, and therefore, if you select more than one device, the *Connect to Device* button is deactivated.
   You can only connect to accessible devices. For example, the *Connect to Device* button is deactivated, when you select a disconnected device.

   If the list only displays a single device, then the *Connect to Device* button automatically applies to that device without you needing to select it.
3. Click the *Connect to Device* button at the top of the list. For example, as shown below –

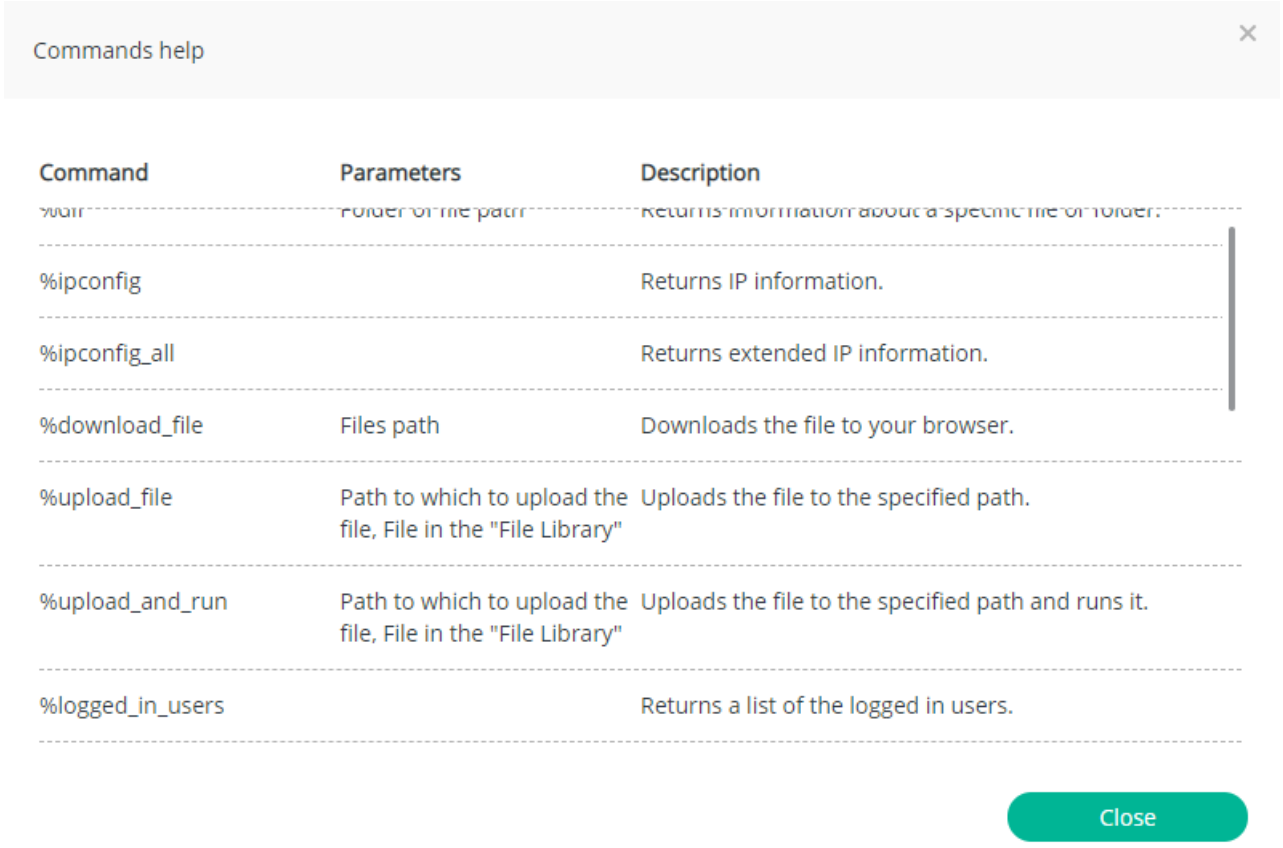
   A Shell window opens in a new browser tab. You may be requested to wait while the connection is established.
   The following displays after the connection has been established:



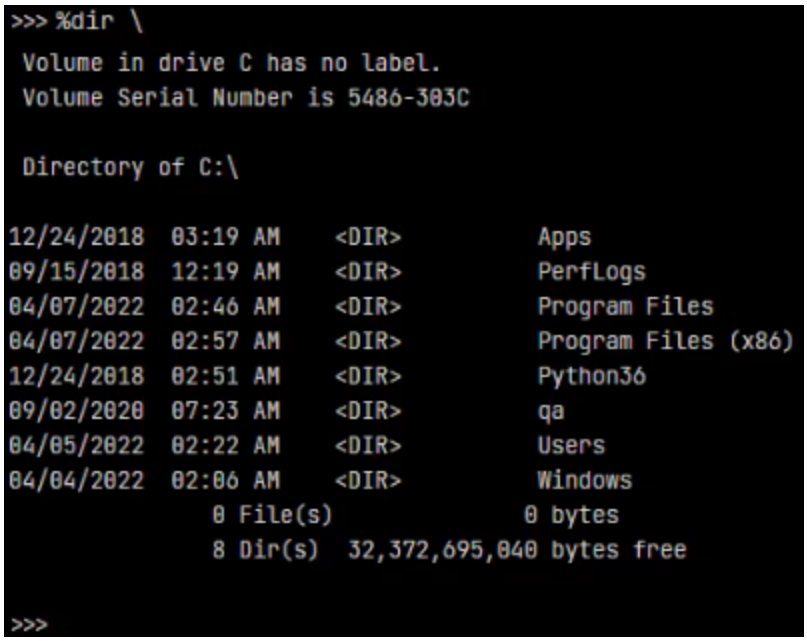
The name of the device is displayed in the top left corner of the page.

The connection status and a timer is displayed in the top right corner of the page.

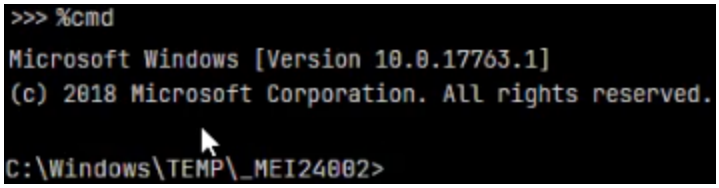
4. The main part of this page shows a terminal screen (black) with a prompt (>>>) at the top left where you can type commands.
   Clicking the *Help* button at the top right of the terminal screen displays a list of the commands (and their parameters) that you can run. To run a command, simply type it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



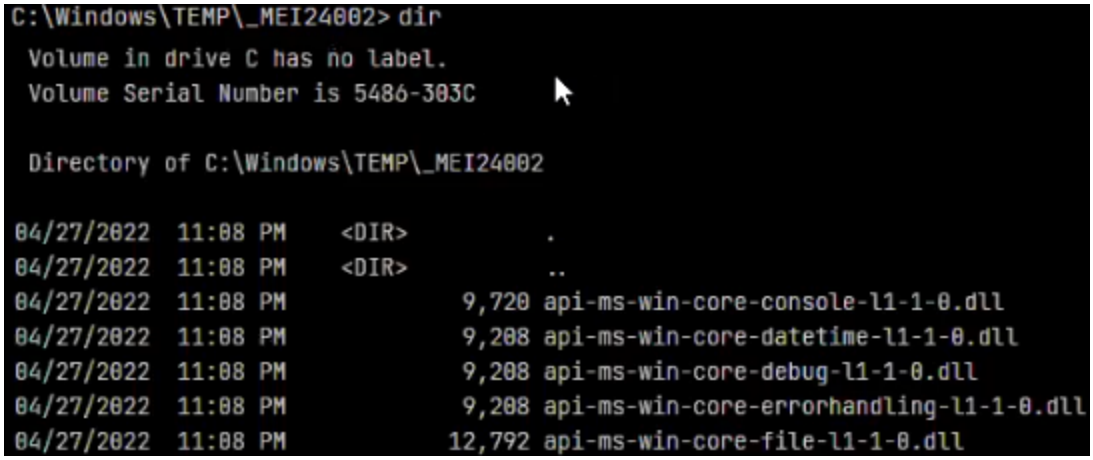
Most of these are EDR-specific commands. For example, typing `%dir \` displays the following:



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



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



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

File Library pane

The File Library pane on the right enables you to upload, download and reuse files during EDR Connect sessions from/to EDR-protected device. No other users can see these files or upload/download from/to

your EDR Connect session. These files are deleted everywhere when you close the EDR Connect Console, as described in Disconnecting EDR Connect session on page 597. An EDR Connect session enables you to:

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

Uploading a file to the EDR file library

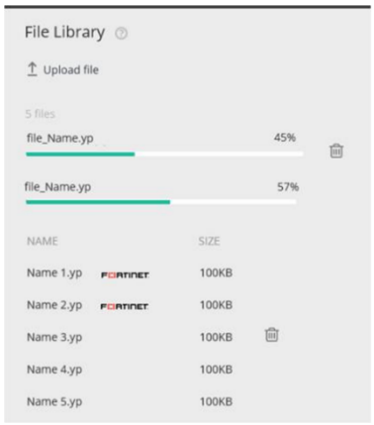
The *File Library* page lists the files that you have uploaded to the EDR file library on the EDR Manager during the current EDR Connect sessions, and that are available to be uploaded on the devices.

To upload a file to the EDR file library:

1. Open a EDR Connect session with an EDR-protected device.
2. Click the *Upload File* button in the *File Library* pane. A standard file selection window is displayed.
3. Select a file and click the *Open* button.

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

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



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

Uploading a file from the EDR file library to an EDR-protected device

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

To upload a file to an EDR-protected device:

1. Open a EDR Connect session with an EDR-protected device, as Connecting to an EDR-protected device on page 592.
2. In case the file doesn't appear at the file library, upload a file to the EDR file library on the EDR Manager, as described on File Library pane on page 594. The File Library page lists the files that you have uploaded to the EDR file library.
3. At the prompt in the EDR console, enter the `%upload_file` or `%upload_and_run` command and specify the path to which it should be uploaded, including the name it should have at the uploaded location, and file name to be uploaded. For example:

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

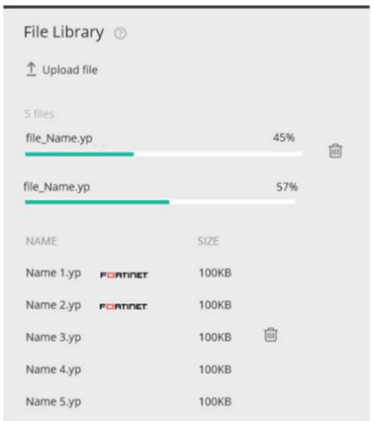
Download a file from an EDR-protected device

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

To download a file from an EDR-protected device:

Open a EDR Connect session with an EDR-protected device, as described on Connecting to an EDR-protected device on page 592. At the prompt in the EDR console, enter the `%download_file` command and specify the full path and file name to be downloaded. For example, `%download_file c:\SuspiciousDir\abcfilename`

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



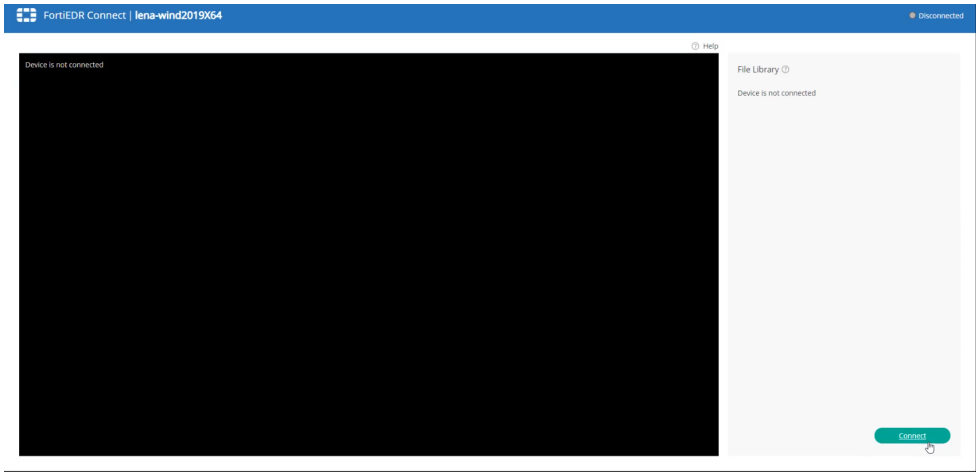
Disconnecting EDR Connect session

Disconnect an EDR Connect session in one of the following ways:

- Clicking the *Disconnect* button at the bottom right of the *File Library* pane.
- Closing the browser tab by clicking the *Close* button.
- Logging out of the EDR Console.
- Rebooting/shutting down the EDR-protected device. For example, using `reboot/sh`.
- Timing out. If you are not working with the EDR console session, then at some point the session will timeout and disconnect it.

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

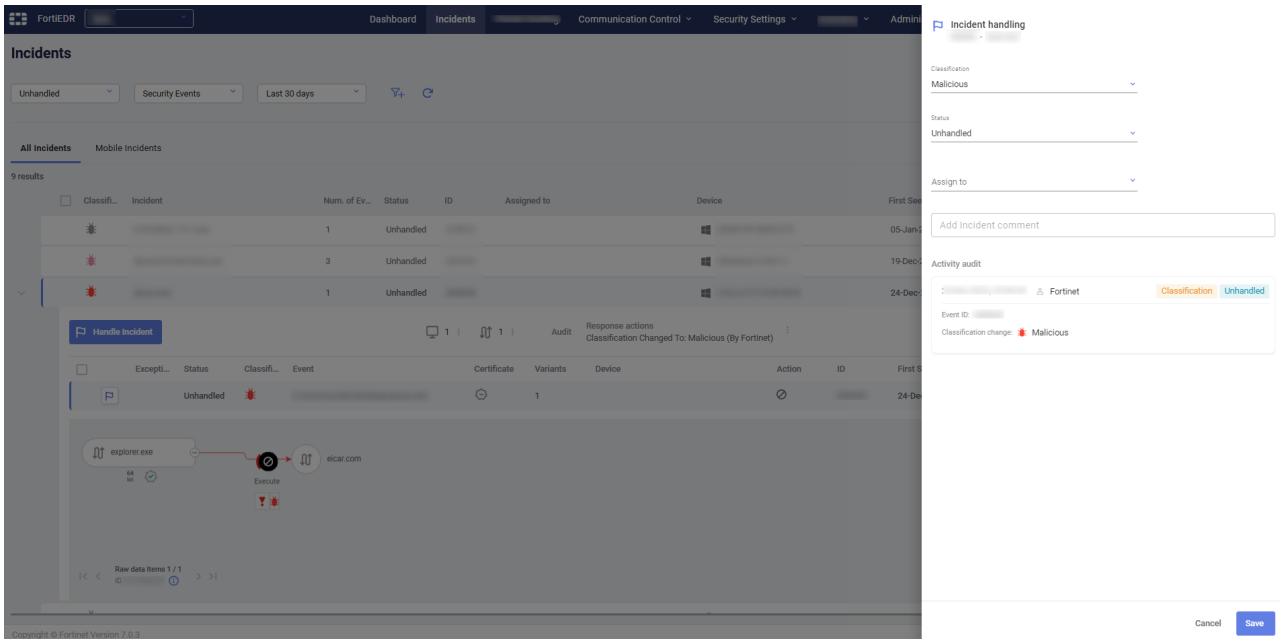
A connected button is then displayed which you can click to reconnect to the same session, as shown below:



Marking a security event as handled/unhandled

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

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



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

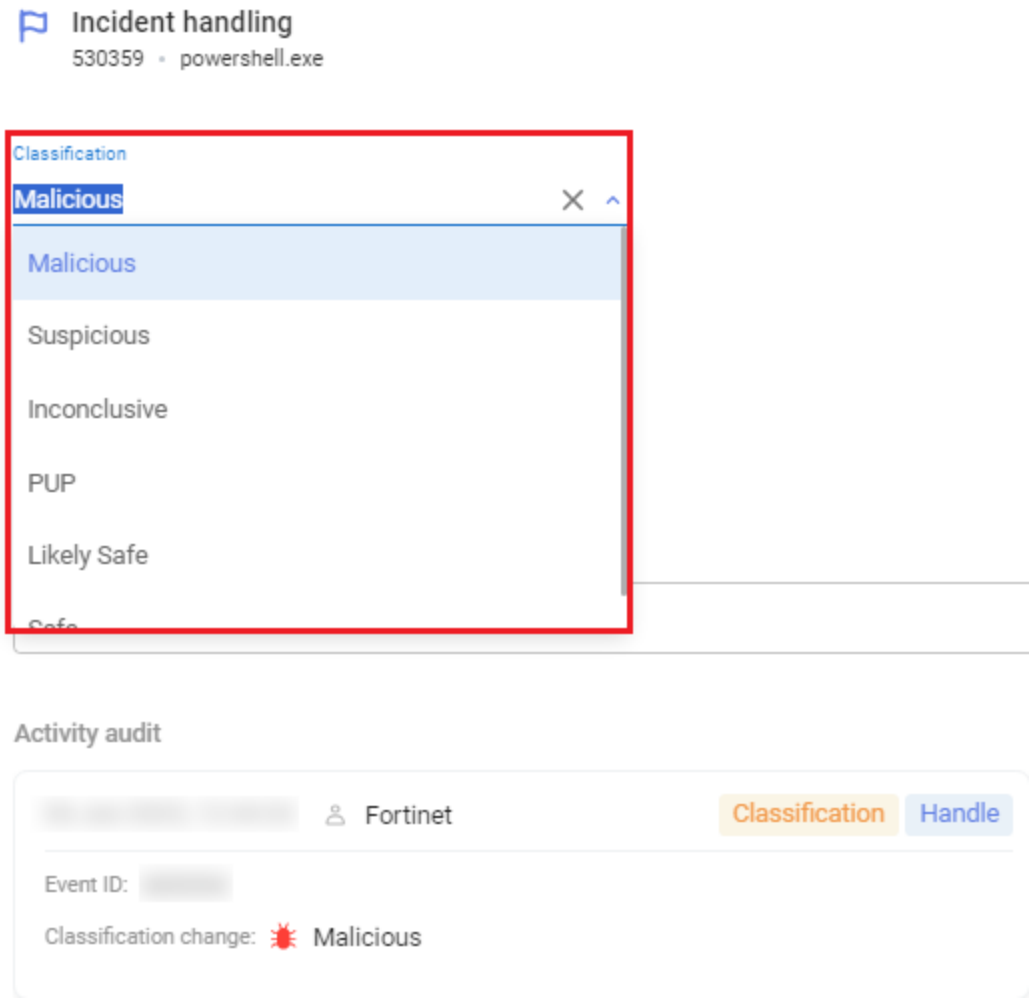
2. In the *Classification* dropdown list, change the classification for the security event, if needed. For more details, see Manually changing the classification of a security event on page 598.
3. In the comments box, use free text to describe how you handled the security event.
4. Click the *Save* button.

Manually changing the classification of a security event

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

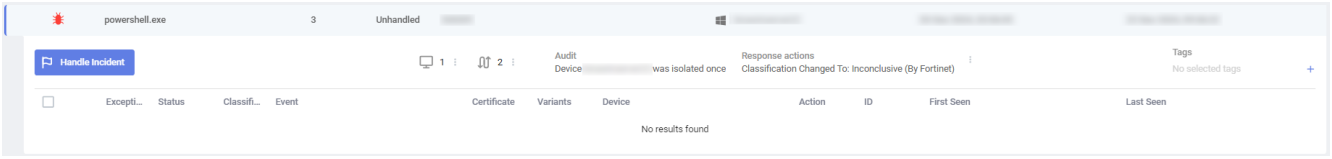
1. Select the rule's checkbox and then click the *Handle Incident* button or just click the flag icon of the security event row. The *Incident handling* window displays.

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



3. Click *Save*.

After changing the classification of a security event, the Overview on page 575 pane displays the history of any actions (Playbook policy-related actions and others) that were made automatically by EDR. 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 Playbooks on page 784.



When the Fortinet logo appears next to an entry in the Overview on page 575 pane, it indicates that the security event was automatically classified by EDR. Security events that are manually classified do not display the Fortinet logo.

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

Defining security event exceptions

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

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

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

Details describing how to edit an existing exception are described in Editing Security Event Exceptions. You can access the Exception Manager by clicking the *Exception Manager* button at the top of the *Incidents* pane or by selecting *SECURITY SETTINGS* > *Exception Manager*. Additional options for managing exceptions are provided in the *SECURITY SETTINGS* tab, as described in Exception Manager on page 683.

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 Playbooks on page 784



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).

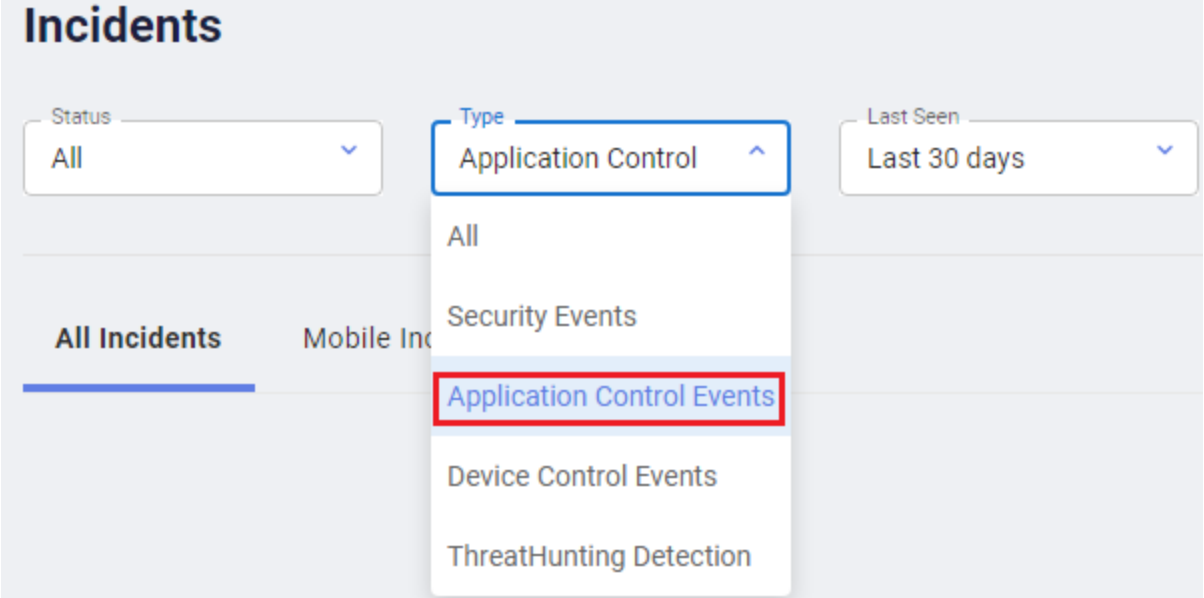
In cases where an exception was defined for the security event but it does not fully cover all the existing occurrences or variants of this event, a slightly different icon is displayed, as described and shown below.



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

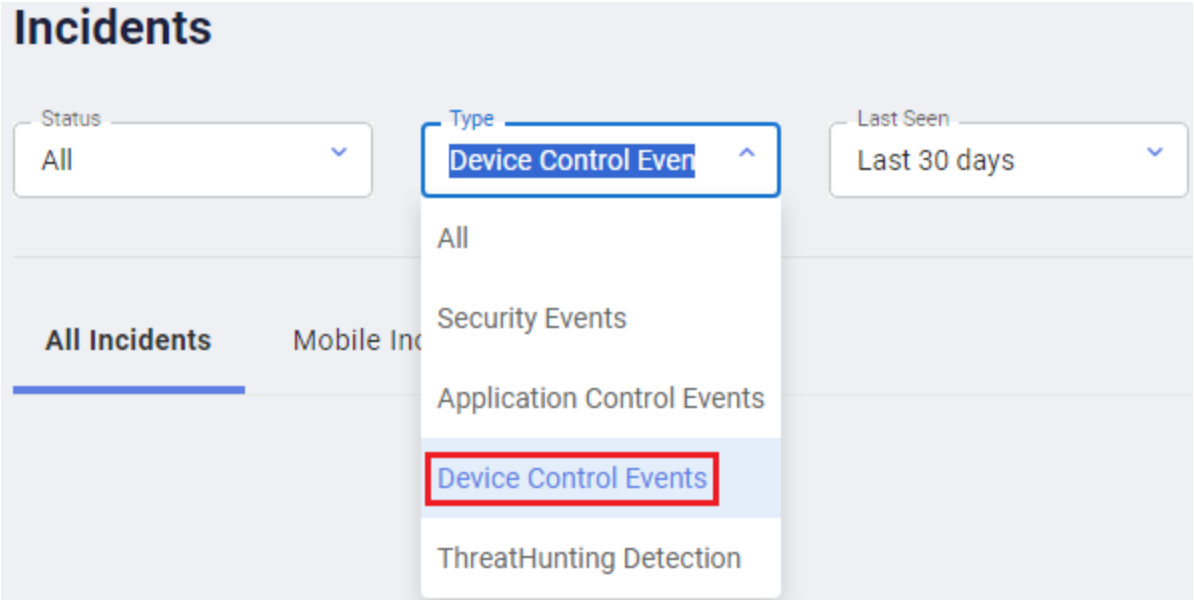
Viewing Application Control security events

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



Viewing Device Control security events

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



Other options in the Incidents viewer

Option	Description
Sorting incidentss	Click any column name to sort security events. For example, you may want to sort by process and collector in order to see the history of everything that happened to that process on that device.
Free text search	Enter text in the search field to search by process, device, or ID.
Time Filter	Click the down arrow in the Time Filter to display a list of time period options. The default is *Last 30 days*.
Deleting incidents	Select an event and click the *Delete* button ( ) to completely delete a security event from the EDR system. A deleted incident cannot be restored or retrieved. Unless you are having storage capacity issues, we highly recommend just hiding incidents and not deleting them.
Exception Manager	Click the *Exception Manager* button (Exception Manager) at the top right corner to access the Exception Manager on page 683.
Forensics	The EDR Forensics add-on enables you to perform deep analysis of security events, as described in Forensics on page 602.
Investigating incidents	Click the *Investigate* (Investigate) button for a graphical and interactive view to further drill down the chain of activities involved in the event. See Investigation View on page 576.

Forensics

The Forensics functionality is unavailable for mobile incidents.

Use the *Forensics* menu to delve deeply into the actual internals of the communicating devices' operating system that led up to the security event.

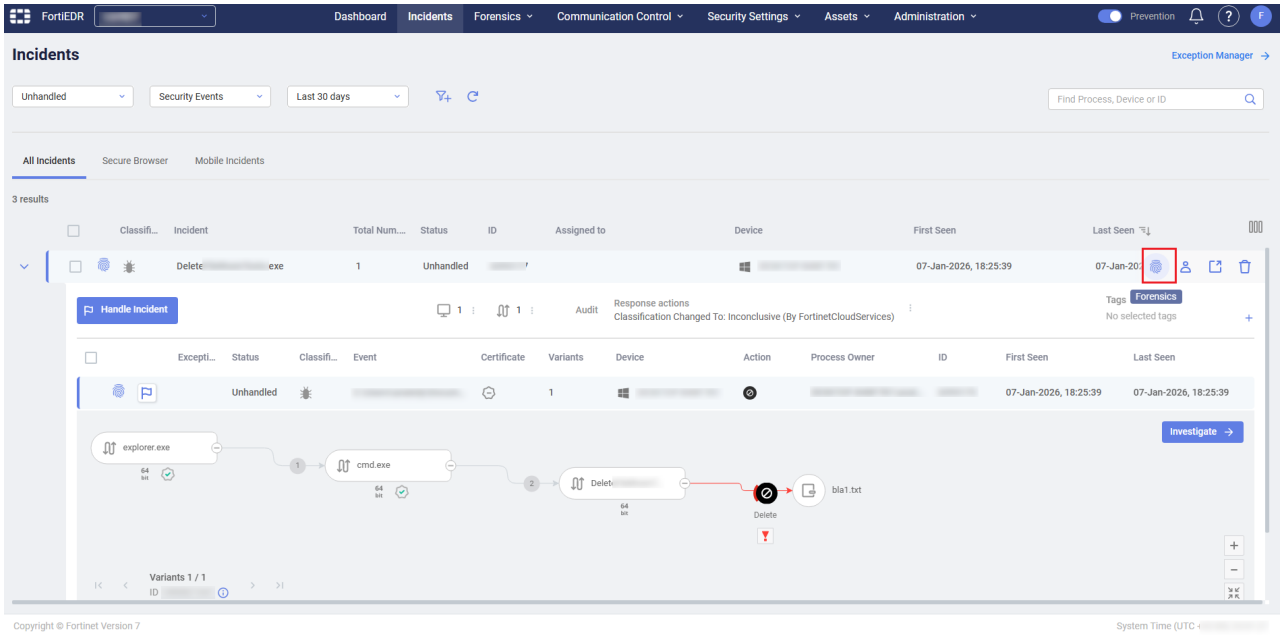
The *Forensic Viewer* provides an abundance of deep analysis and drill-down options that reveal the process flows, memory stacks and a variety of operating system parameters in a graphic view, such as:

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

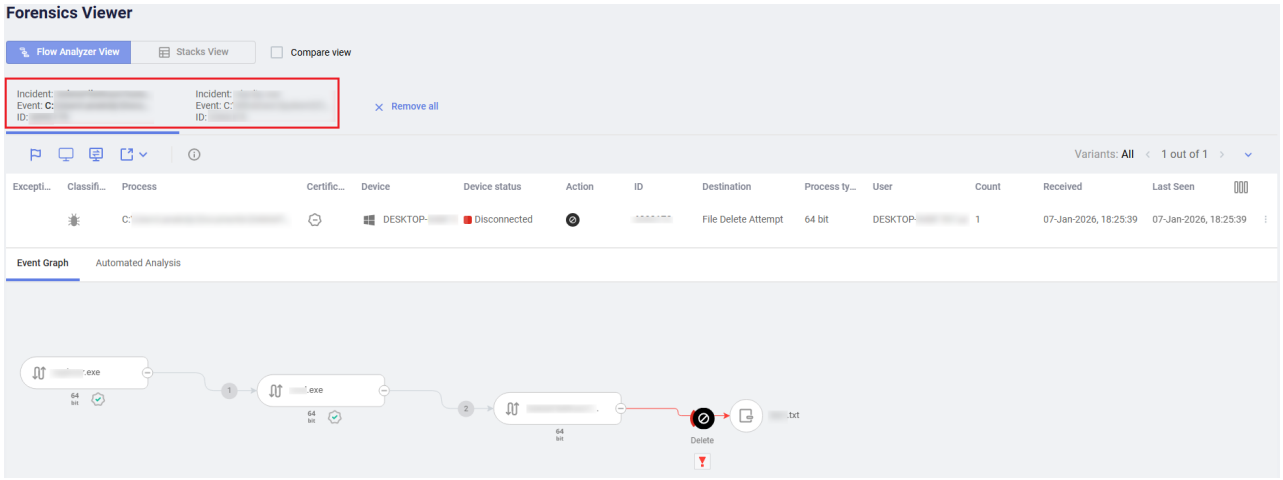
- Side-by-side security event comparisons.

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

- In the *Incidents* view, 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.



In this case, the Forensics viewer shows a separate tab for each security event associated with the security event aggregation. For example, the figure below shows 4 tabs for a security event aggregation containing two events.

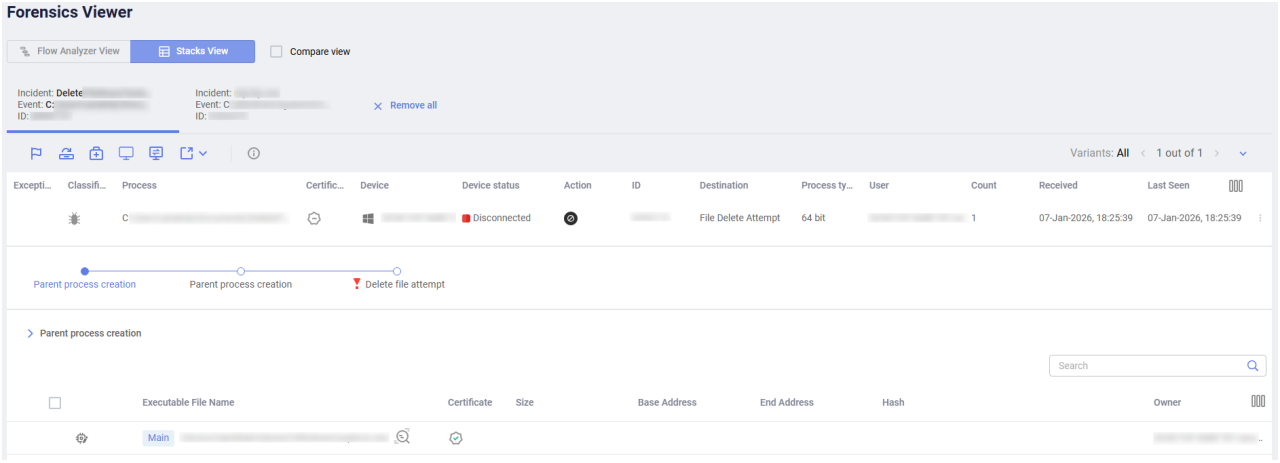


- Select an individual security event in the Event Viewer and then click the *Forensics* button ( ). In this case, the Forensics viewer shows a single tab for the selected security event, with all of its related variants.

- Select a variant when in drill down, and then click the *Forensics* button ( ). In this case, the Forensics Viewer shows a single tab for the selected security event with a single variant.

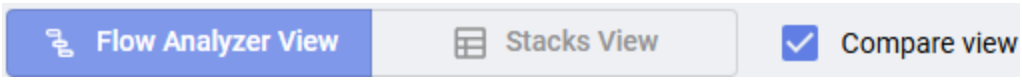
To perform deep Forensic analysis:

1. Select the security events to analyze using one of the methods described in Incidents on page 569. Selected security events that are currently loaded to the *Forensics Viewer* are marked in the *Incidents* with a fingerprint icon.
2. Each selected security event is then displayed in the *Incidents* as a separate tab:

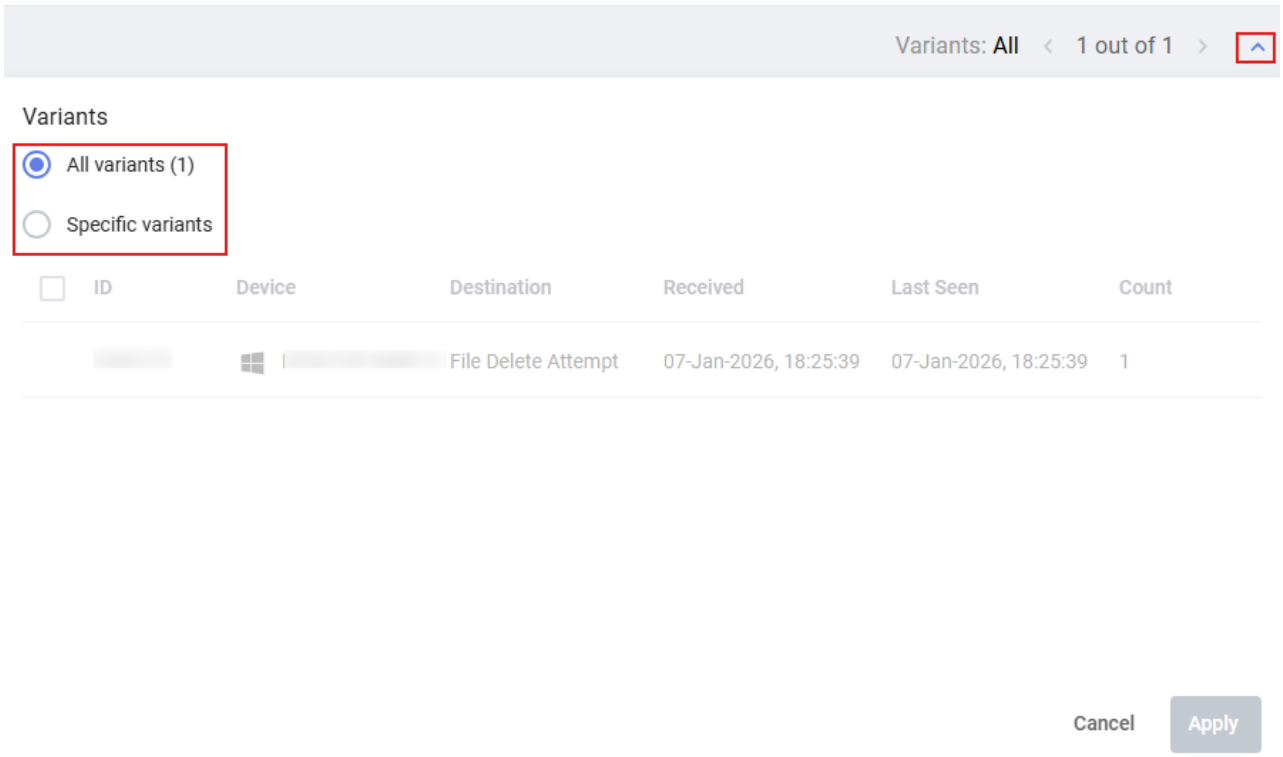


Each tab shows the same information as in the Incidents on page 569, with additional information as described below.

The following options for viewing more information are provided:



In the *Variants* area, expand and select all or specific variants to display for a security event.



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

The *Connect to Device* button opens a console that provides direct access to EDR-protected devices.

Flow Analyzer view

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

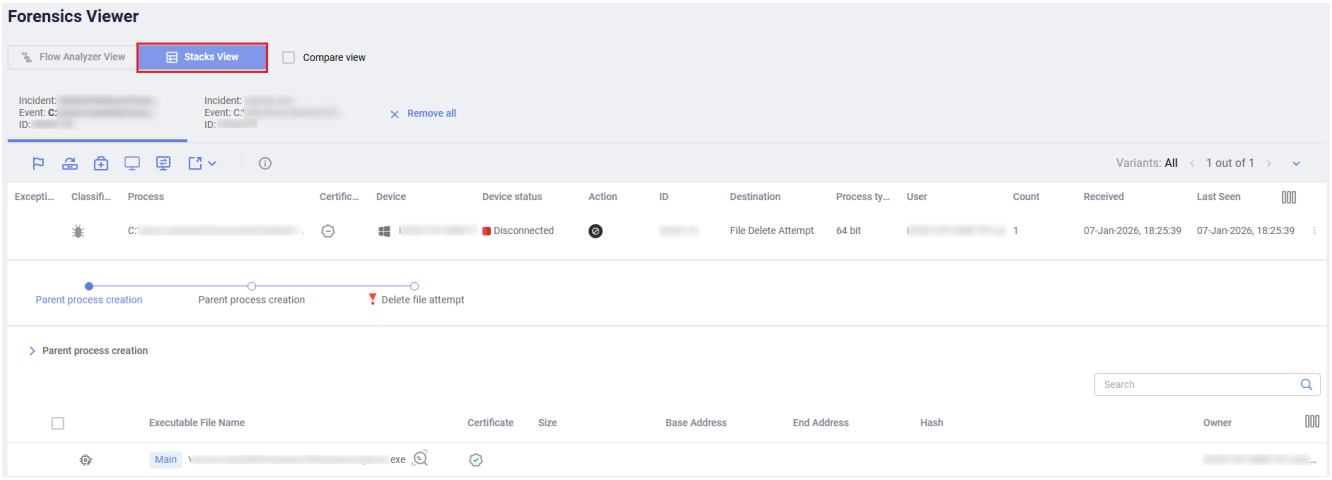
The arrows indicate the sequence of processes and specify the operation that was performed, such as *Create*, *Inject*, *Open* and so on. If multiple operations were performed between two processes, then multiple arrows are shown between them.

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

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

The flow chart is interactive. Clicking on a specific node or arrow drills down to perform further investigation. See Investigation View on page 576 for more details.

Stack view



The Stack view displays the following sections of information:

Field	Description
Incident	Shows the same information as in the Incidents on page 569.
Stacks	A control toolbar that depicts the stacks that were collected in each step prior to the connection establishment requester file access. A red exclamation mark ! 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. Click the *Process Hash* link to display a dropdown menu with the following options:  • *VirusTotal*: Checks whether this hash was seen elsewhere. This involves searching another external website (VirusTotal). Clicking the link runs the query in VirusTotal. Alternatively, you can go to www.virustotal.com, click the *Search* tab, paste the hash from EDR and then click *Search It*. • *Threat Hunting*: Checks the activity events that are relevant to this

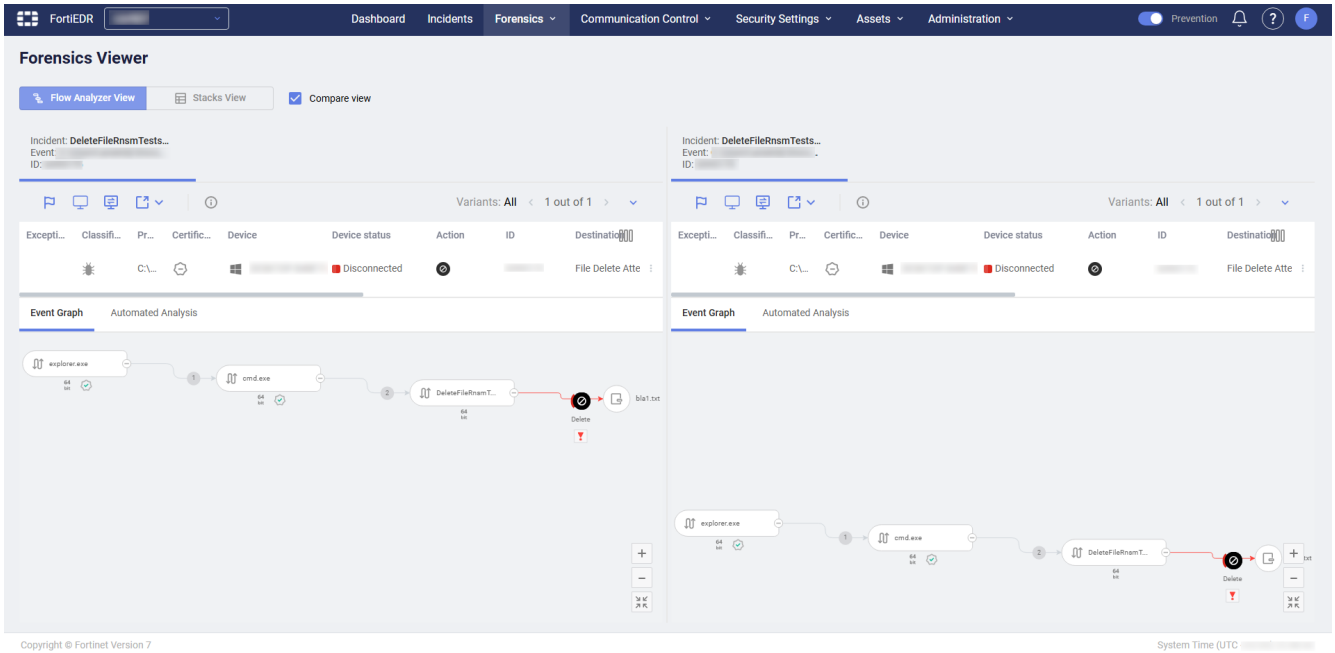
Field	Description
	hash. Clicking this option takes you to the *Threat Hunting* page. • *Add to Blocklist*: Adds this hash to the Application Control block list, as described in Application Control on page 701. Clicking this option opens up the *Add Application* Window with this hash specified.

For each executable, you can see the following information:

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

The row of the executable that triggered the EDR security event is highlighted with a red exclamation mark ❗. This indicates the row that you may want to investigate further. You can expand an executable row to display an even deeper level of information describing that process.

Compare view



The Compare view enables you to display two views side-by-side. They can both be either Flow Analyzer view on page 605 or Stack view on page 606.

Threat Hunting

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

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

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

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

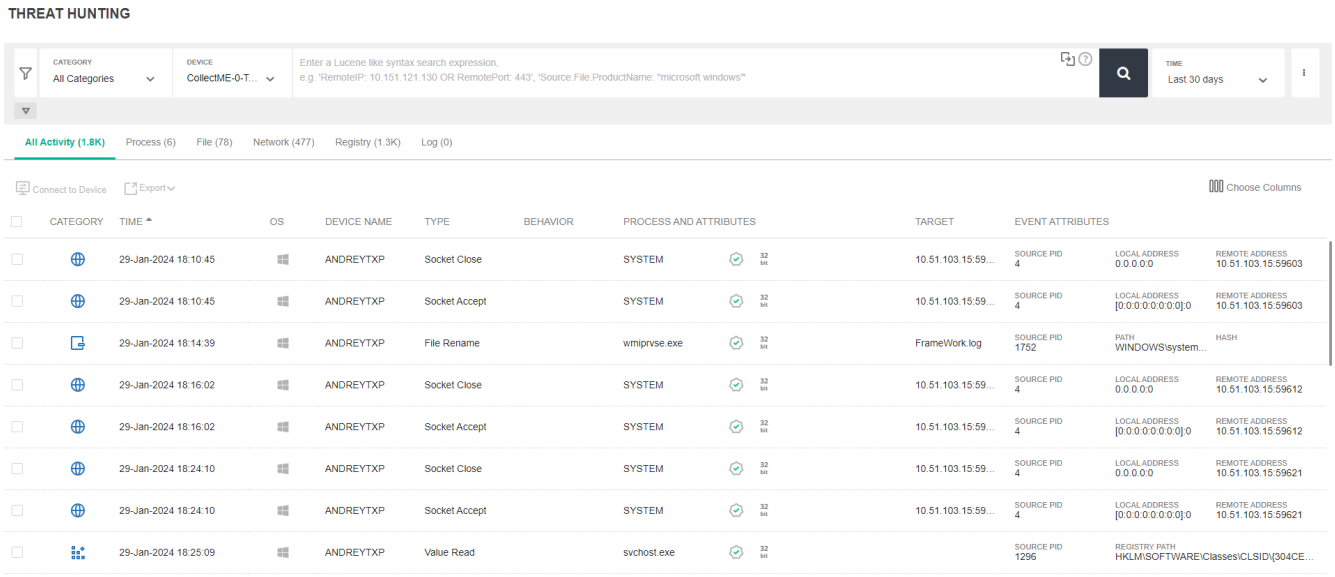


Activity events are not the same as the security events identified in the *Incidents* tab. Unlike *Incidents* tab security events, which are only reported in the *Incidents* tab as they occur and are detected, activity events are continuously collected based on a wealth of data, activity and actions occurring in your system and the chosen Threat Hunting Profile. See Collection profiles on page 723 and Collection Exclusions on page 717 for more information.

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

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

The *Threat Hunting* page contains the following areas:



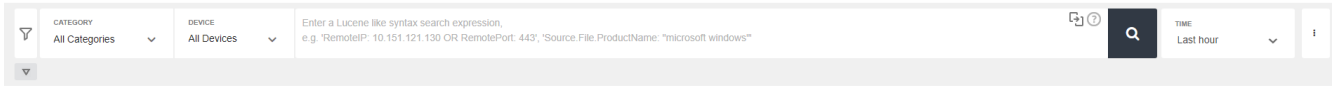
- Filters on page 609
- Facets on page 621
- Activity events tables on page 624
- Details pane on page 628
- Investigation View on page 636

To set up Threat Hunting in EDR, configure the following:

- Collection profiles on page 723
- Collection Exclusions on page 717

Filters

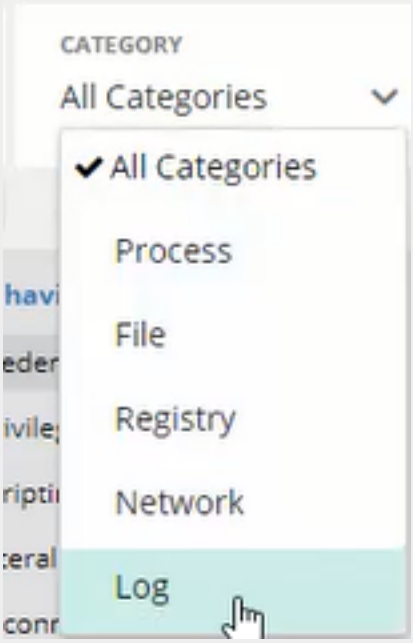
The Filters area enables you to define a query that filters the activity events to display in the result tables. It comprises the following filters:

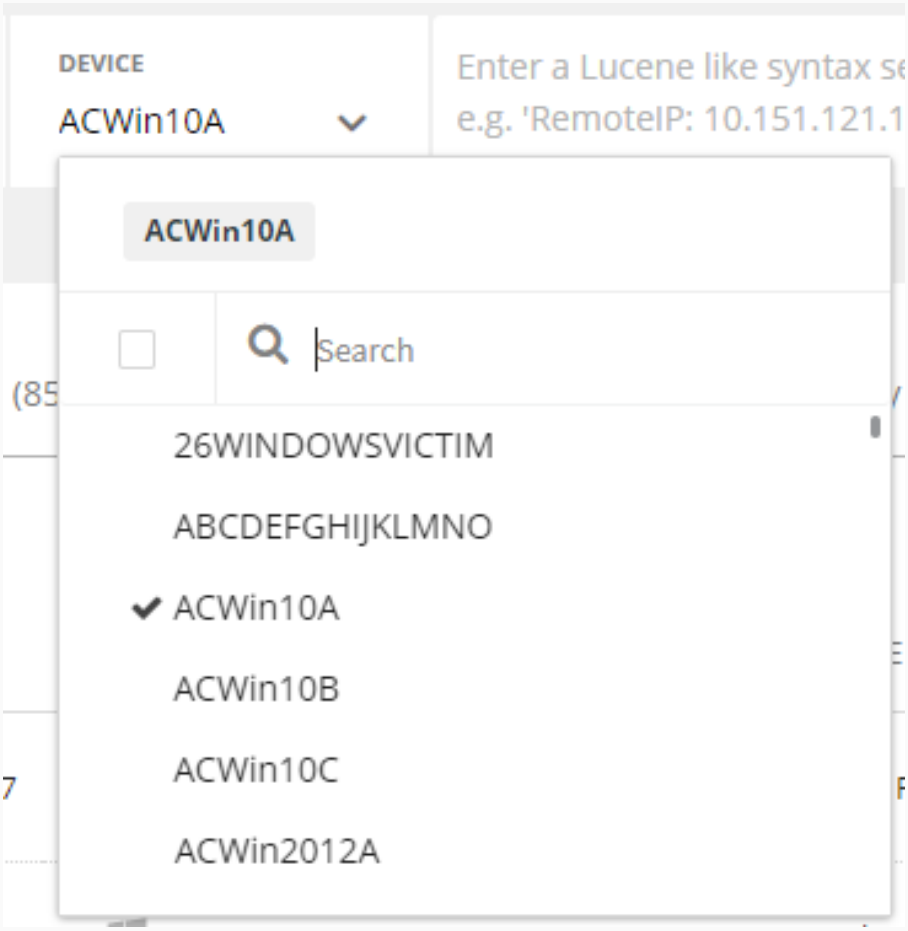
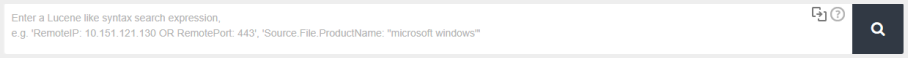


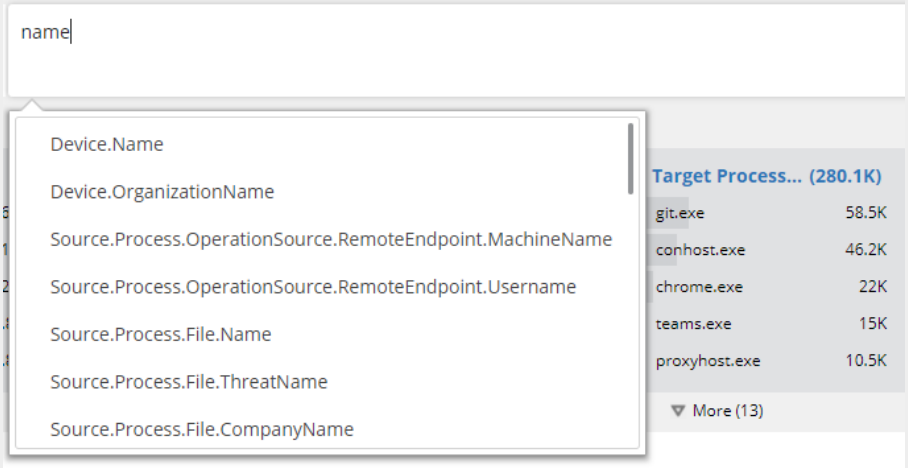


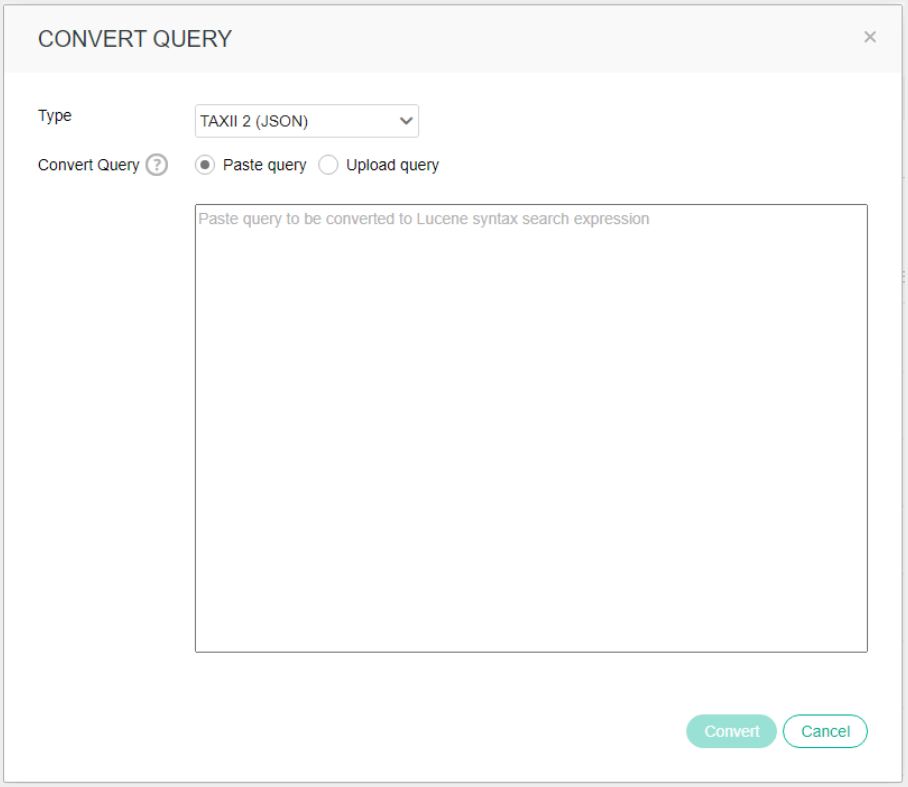
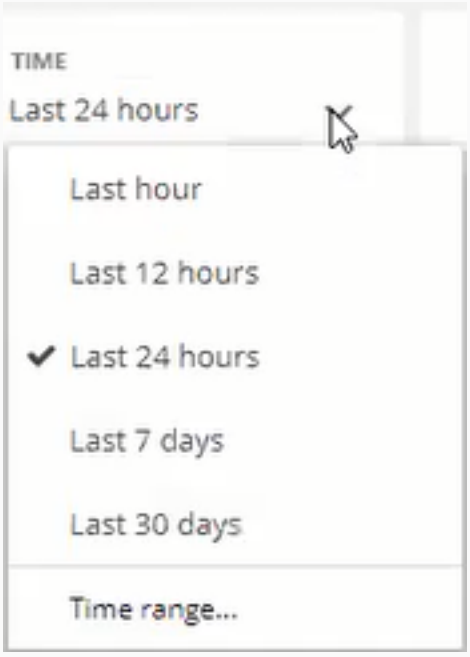
This area also enables you to save queries and to redisplay saved queries, as described in Saving queries and saved queries on page 614.

Filter	Description
Category	The *Category* filter enables you to filter the activity events by their category.

Filter	Description
	
Device	The *Device* filter enables you to filter by a specific device[s].

Filter	Description
	
Free-text Query	This filter enables you to specify a free-text Lucene-syntax query to filter the results. You can also convert STIX JSON and STIX XML syntax queries into Lucene syntax using the *Convert Query* button.  For Lucene-syntax queries, to simplify definition, the free-text query filter has an auto-complete helper dropdown list that contains all the available activity event fields, as well as available syntax operators. Simply start typing to see a dropdown menu of options. The automatic-complete helper guides you through the process of creating a query by displaying appropriate options in the dropdown menus, such as fields and operators when appropriate.

Filter	Description
	 For JSON and XML syntax queries, use the *Convert Query* button to convert the query into Lucene syntax.  You can then select the file type and paste the query or upload a JSON or XML file in the *CONVERT QUERY* window. The following indicators are supported and will be translated into Lucene syntax: hashes, file names, files size, paths, IPs, usernames, registry keys, URLs and domain names.

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

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

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

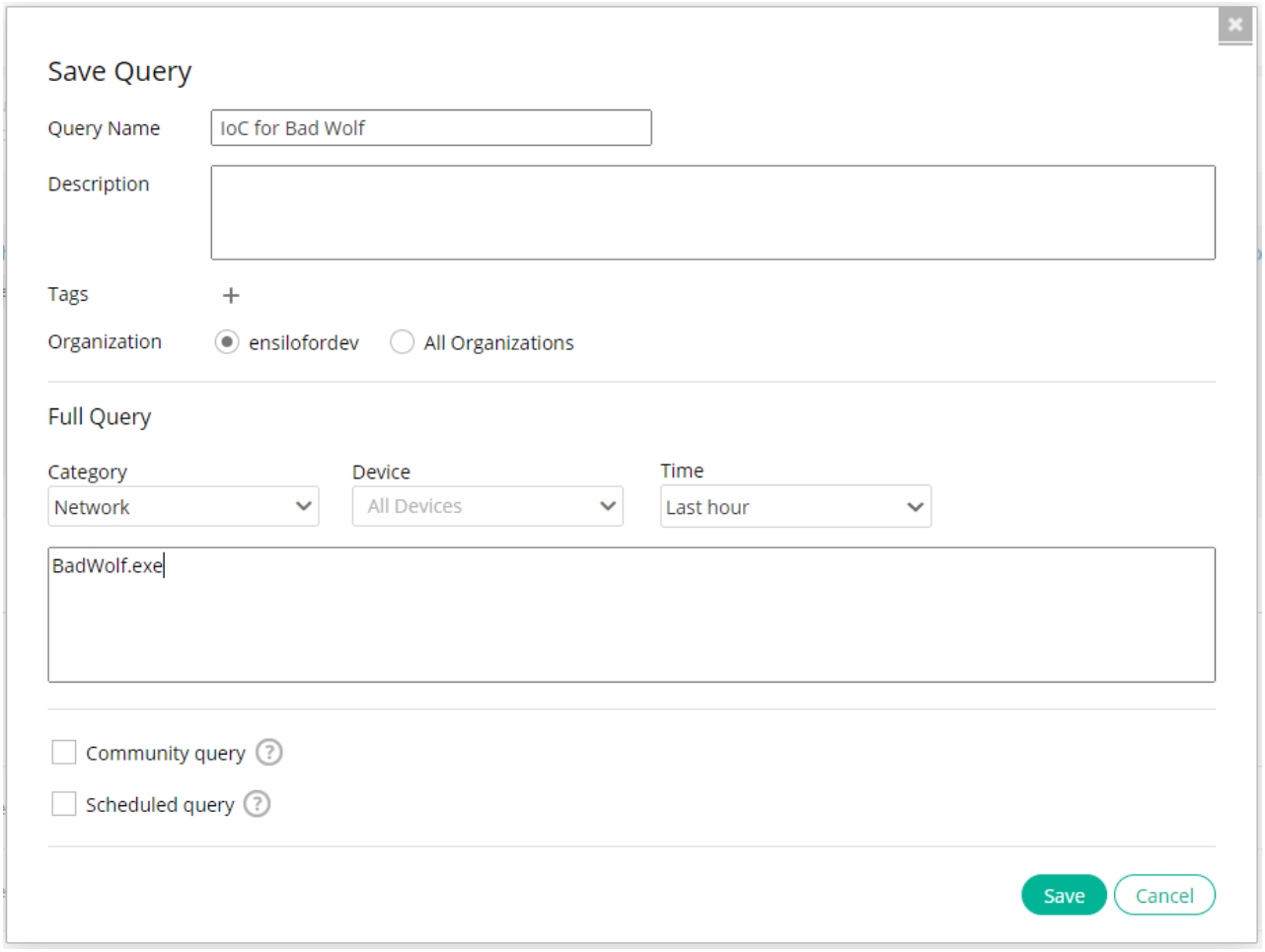
Saving queries and saved queries

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

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

To save a query:

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



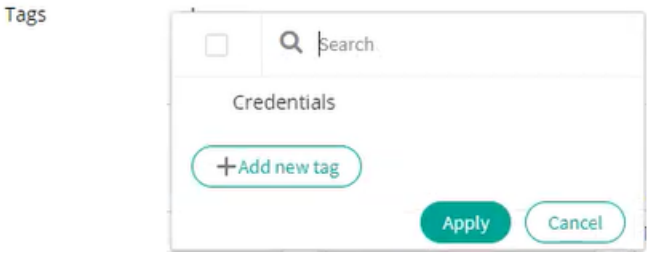
3. Fill in or modify the definitions of this saved query, as follows:
   - *Query Name*: Enter any free text name describing this query.
   - *Description*: Enter any free text description of this query.
   - *Tags*: Enables you to assign one or more metadata tags to this query. You can assign a previously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

   These tags only relate to saved queries.

   Tags +

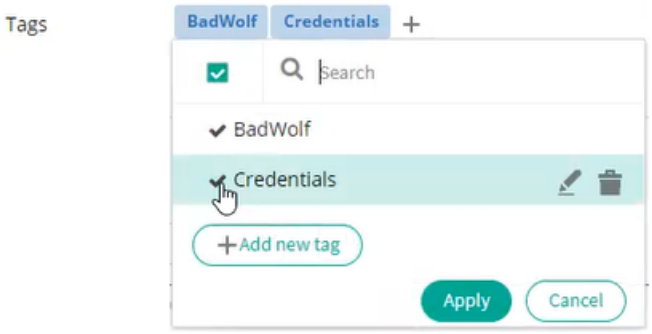
   Click the *Add* button to assign tag(s) to this query. The following displays:



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

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

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



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



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

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

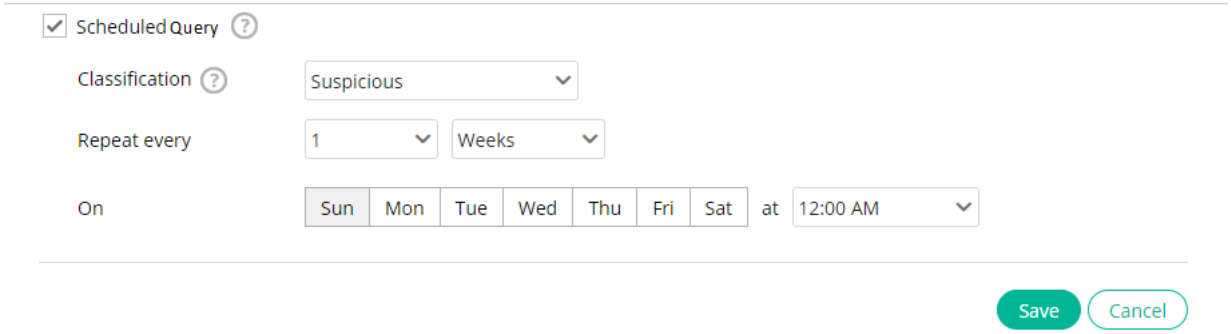
Click the *Apply* button to assign all the selected tags (with checkmarks) to this query.

- *Organization*: Specifies the name of the organization in a multi-organization EDR environment when the logged in user has a Hoster role. In a single-organization EDR 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 EDR community including other organizations.



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

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



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

  Define the scheduled query, as follows:

Field	Definition
Classification	Select the classification of the Security Event to be issued when the scheduled query has run and found matches. The Classification specifies how malicious the security event is, if at all. Classifications are initially determined by EDR automatically or manually and are shown in the *Incidents* tab, as described in Overview on page 575. They can be: • Malicious • Suspicious • Inconclusive • Likely Safe • PUP (Potentially Unwanted Program) • Safe
Repeat Every/On	These options enable you to define the frequency and schedule when this query will be run. For example, to repeat the query every week on Sunday, make the selections shown in the screen above.
Trigger Playbook Actions	Specifies whether to allow EDR to trigger the corresponding Playbook action of the triggered security event from the scheduled query. Enabling this checkbox allows EDR to automatically apply the action of the Playbook that is assigned to the Collector Group the triggering device belongs to. Configure the following options:

Field	Definition

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

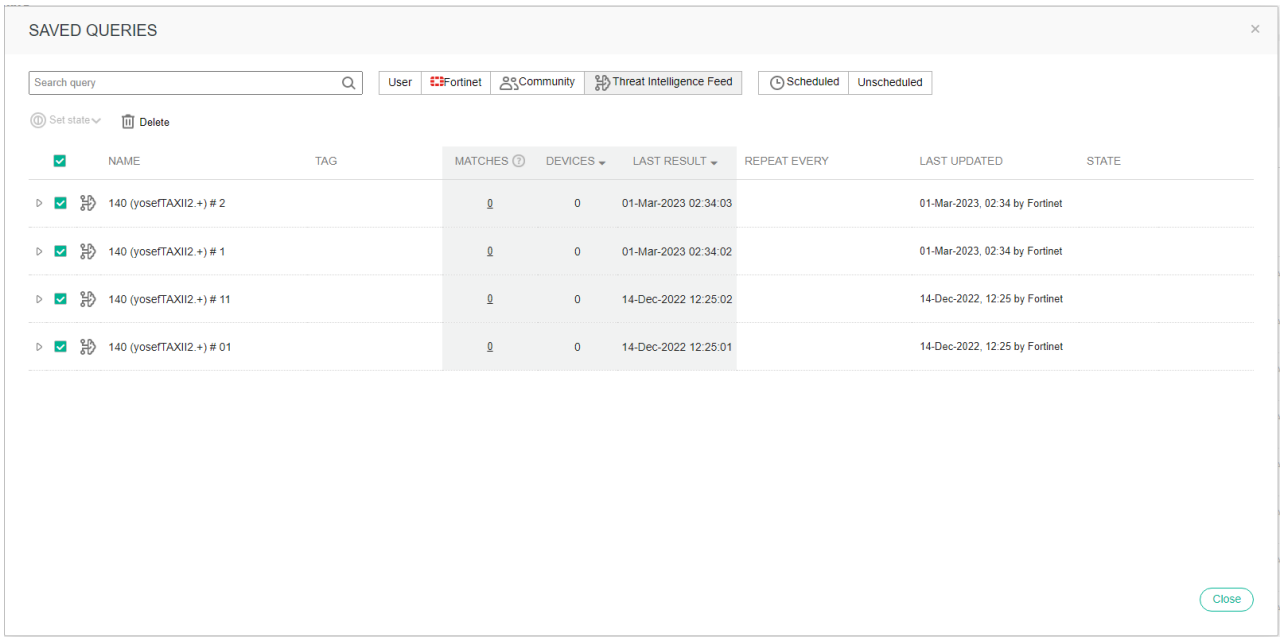
4. Click *Save* to save this query so that it is available to be redisplayed, as described below. The system runs the query immediately in order to verify that it is functional.



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

To display a saved query:

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



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

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:

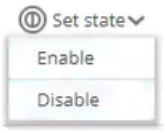


3. You can filter this list of saved queries by typing into the *Search* field and/or selecting one of the following options:
   a. /*User*: To select defined queries. Selecting *User* filters by saved queries that were created by a user.
   b. *Community/User*: To specify that Community Queries are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



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

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

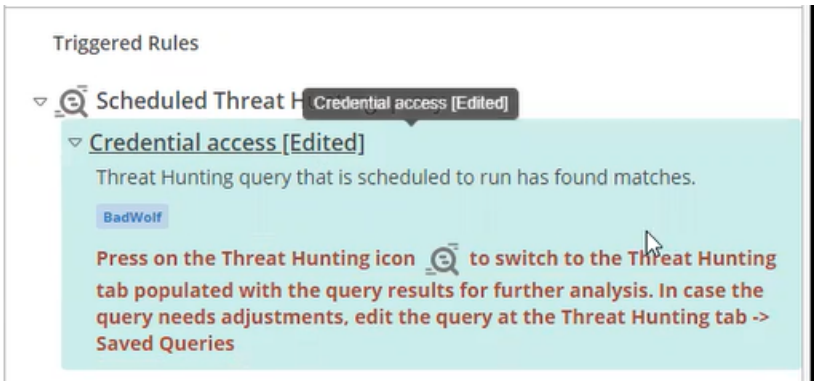


Scheduled queries

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

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

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



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

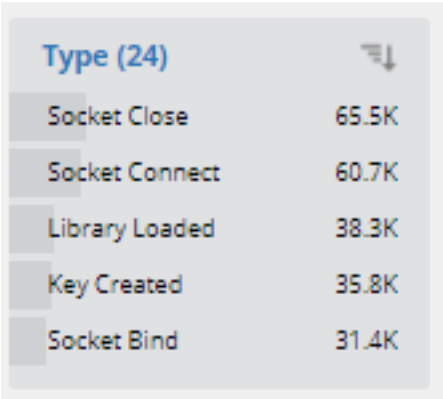
Facets

As expected, the continuous, realtime collection of Threat Hunting data produces numerous activity events. The sheer volume of activity data makes working directly with these activity events almost unmanageable. Therefore, EDR uses facets to summarize the data displayed in the results tables. Facets are predefined in EDR 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.



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

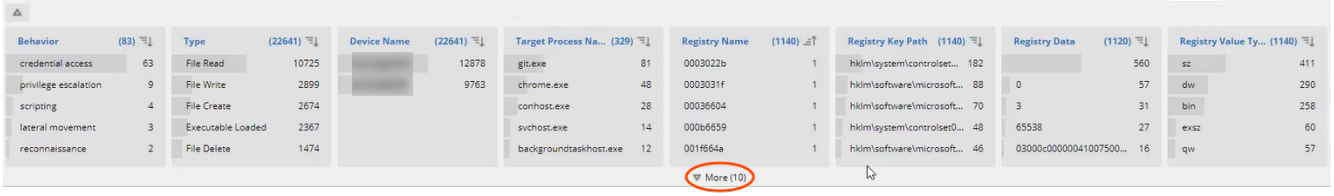
Facet can show the bottom five instead of the top five. In order to switch from the top five to the bottom five for this specific facet, click on the arrow on the right side of the number  .



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.

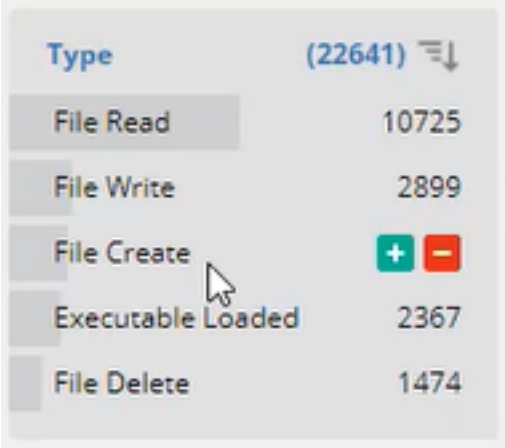
You can click the *More* link to display additional facets.



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.



Then, click the *Apply* button.

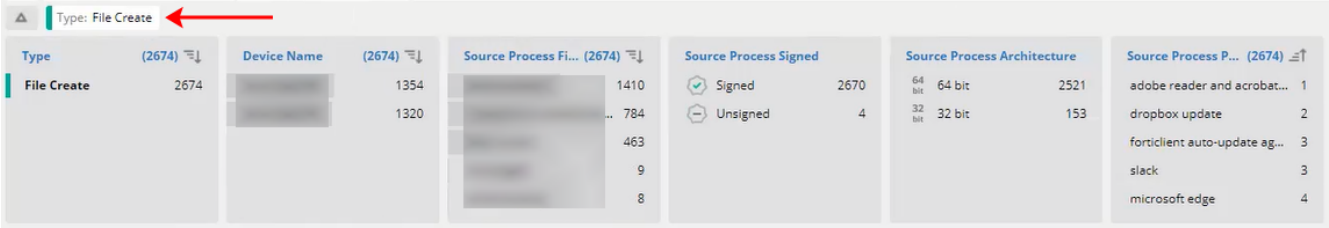


An item highlighted in green 

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 

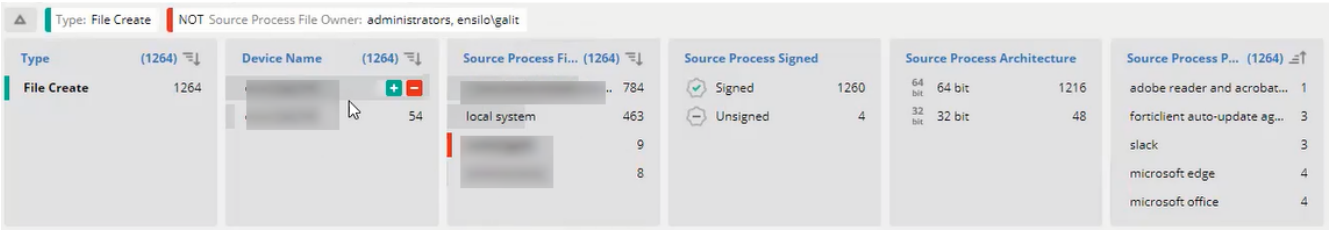
indicates that it has been marked as an exclusion filter, but has not yet been applied by clicking *Apply*.

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



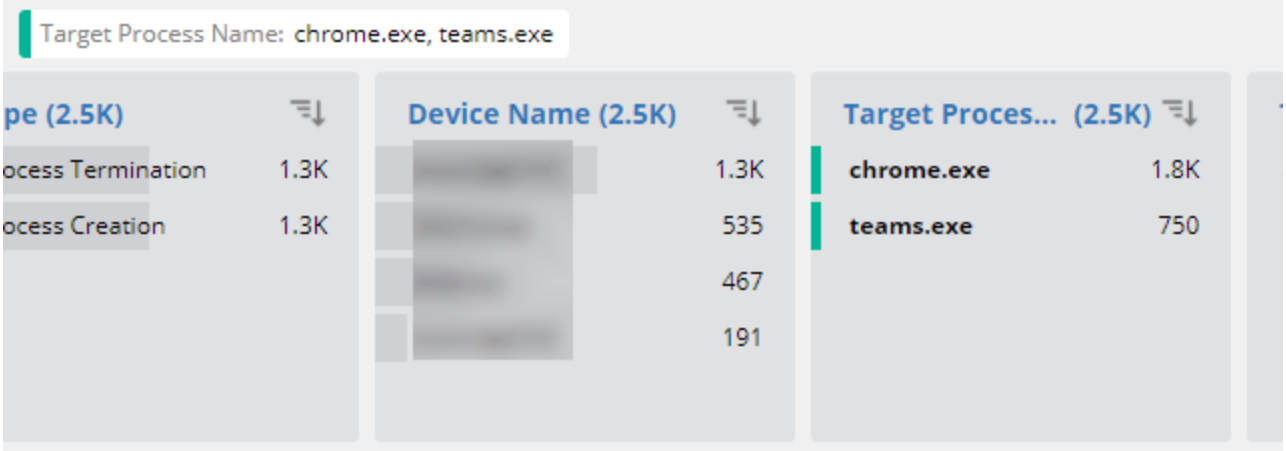
Each chip has either a green or red border on its left side to indicate whether it was defined to include (green) or exclude (red) that item in the filter.

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

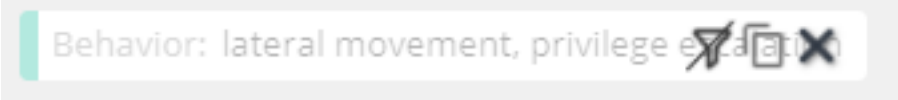


You can define an unlimited number of chip filters, with an AND relationship between multiple filters. Each facet can create up to two chips, one for the inclusion of values and one for the exclusion of values.

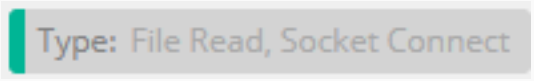
If two values have been added to the query from the same *Facet* pane, the relationship between the values in the chip is OR. The following example shows that the query includes activity events in which their *Target Process Name* is either `chrome.exe` or `teams.exe`, which is shown below in both the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



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



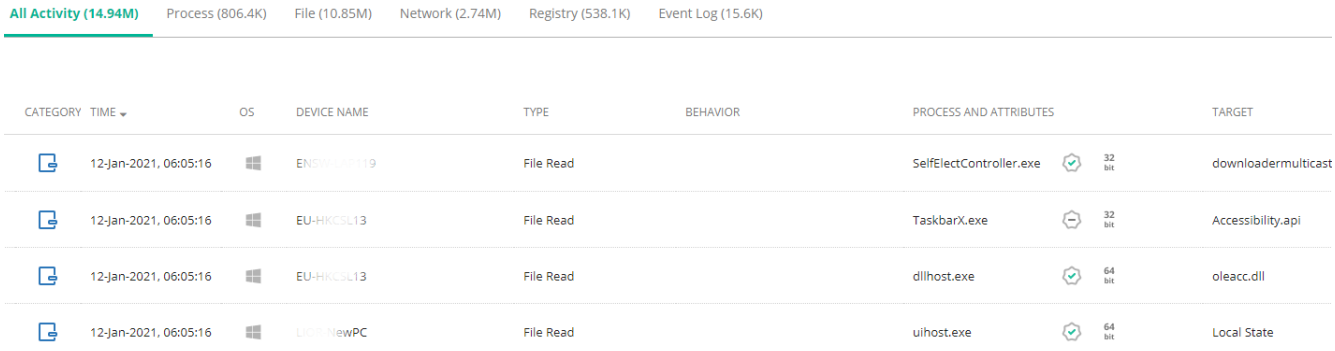
Tool	Definition
Remove	The chip is removed and the Facets and Result tables are updated accordingly.

Tool	Definition
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: 
Copy	The chip content is copied to memory and can be pasted into the query for further editing.

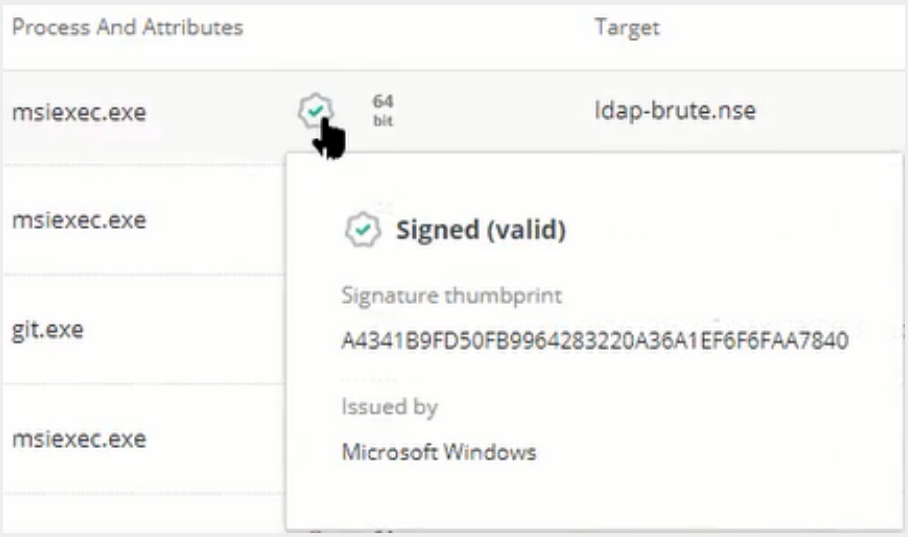
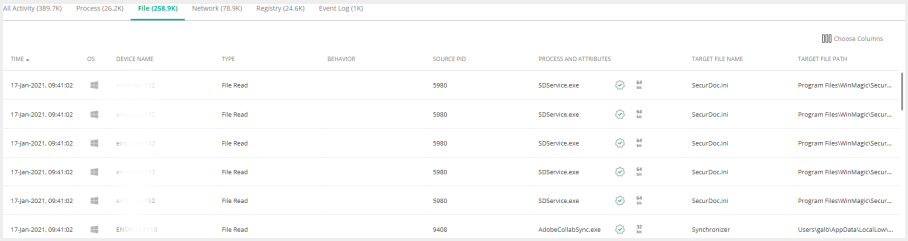
In order to enable a disabled chip and update the results according to its criteria, click the *Enable* icon.

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:

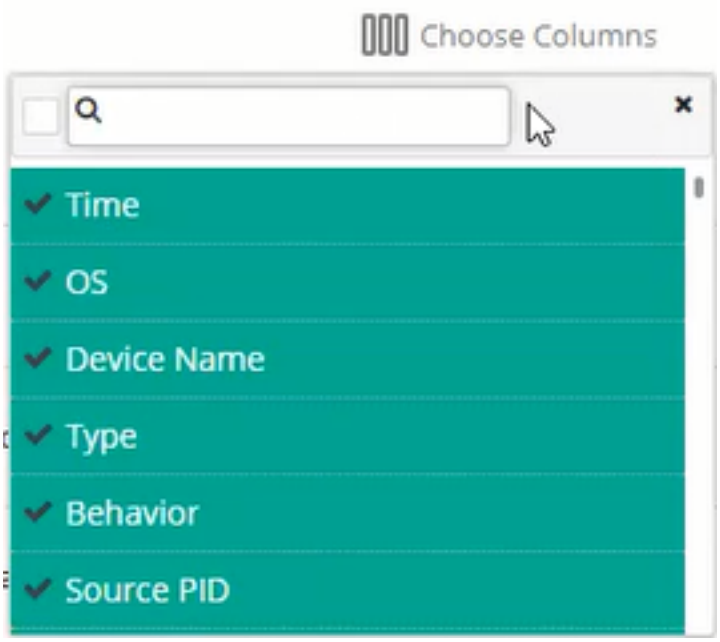


Category	Definition
All Activity	This tab lists all activity events, based on the filters defined for the Threat Hunting query. The number in parentheses () specifies the total number of activity events, based on your query criteria. This total equals the sum of the activity events in the other five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

Category	Definition
	 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. 
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.

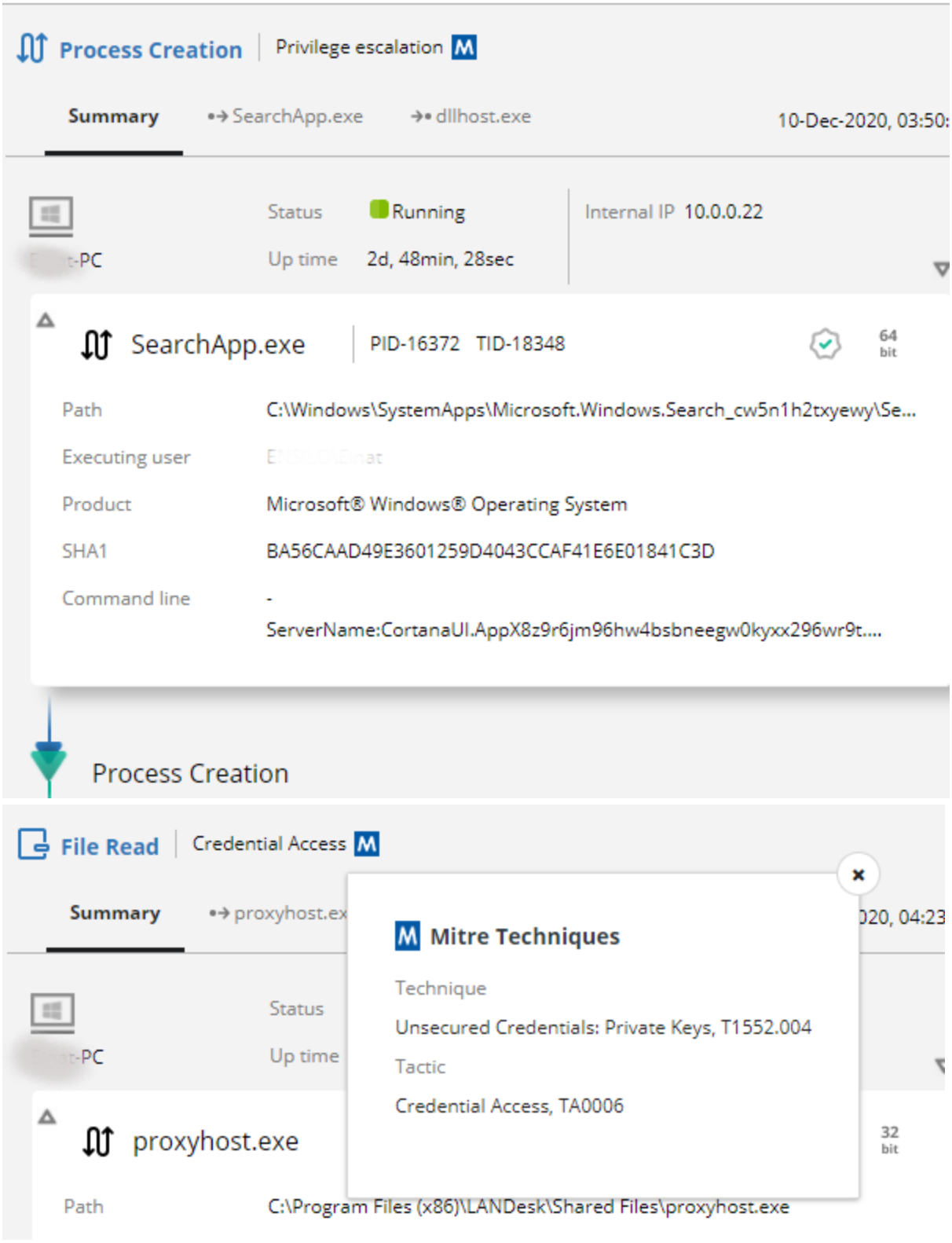


Each activity event may also be a part of a *behavior* and/or a MITRE Technique. A behavior indicates that this activity event is part of a specific behavior as determined by EDR. A MITRE type (Technique or Tactic) indicates that the activity event is part of specification of a technique and tactic as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

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

When an activity event has a related MITRE indication, it is indicated in the Details pane on page 628 (see below). You can hover over the associated icon to display more details.



Filtering using activity events tables

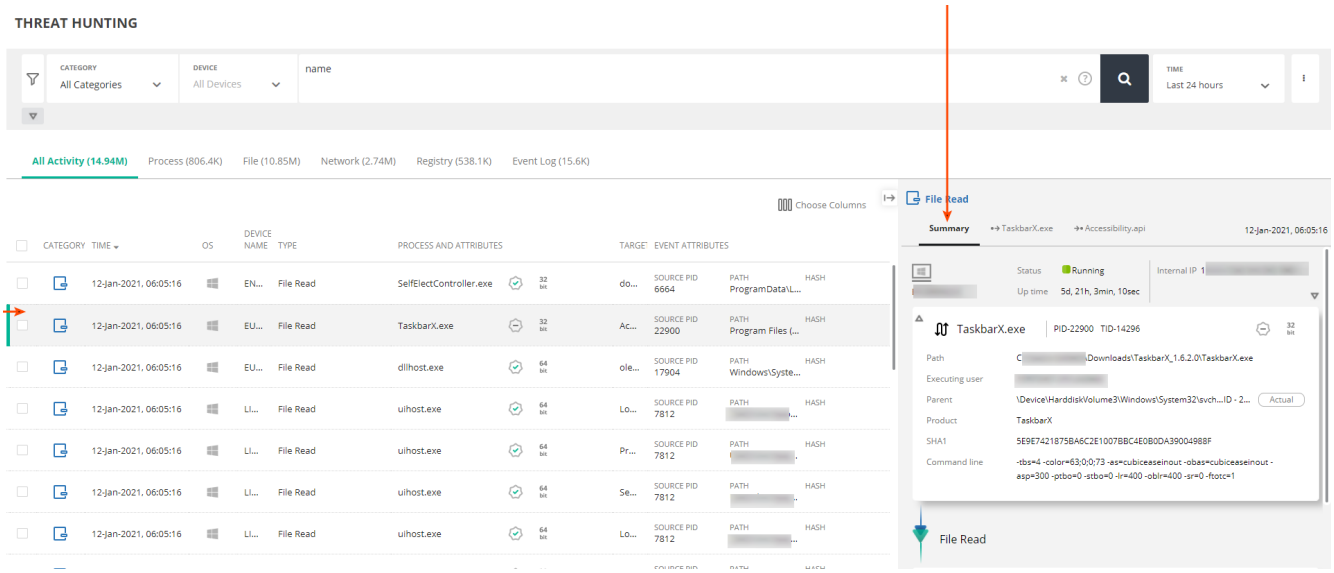
The activity events tables area can be used to add filters to the query in a similar manner as facets.

When you hover over an item in the table, a green and red button appear to its right. Click the green plus button ( )to include that item as a filter or click the red minus button ( ) to exclude that item as a filter. For more details, see Filtering using facets on page 622.

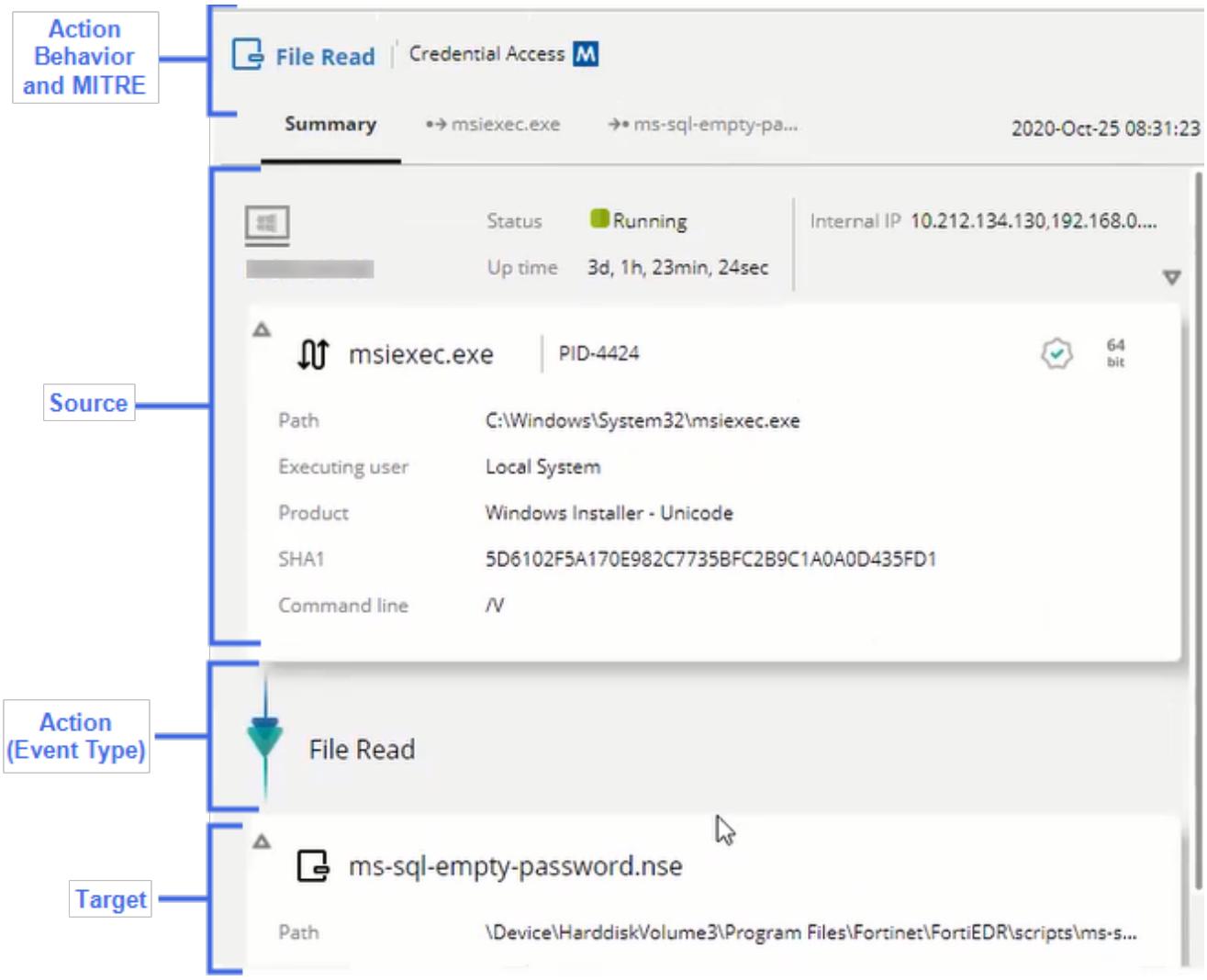


Details pane

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

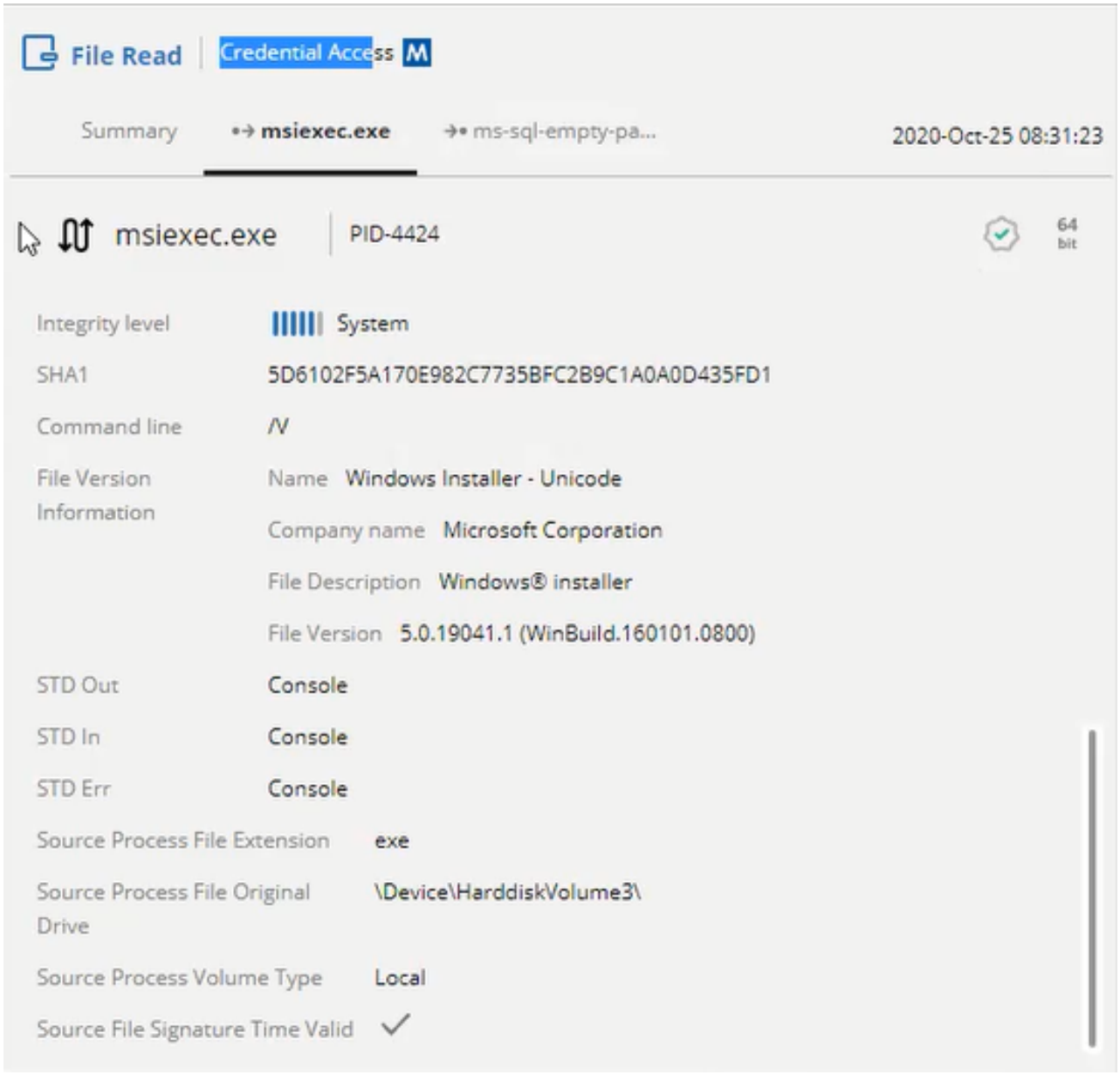


The Details pane for an activity event contains a *Summary* tab, one or two other tabs, and the *Investigation View* (Investigate →) button, as follows:

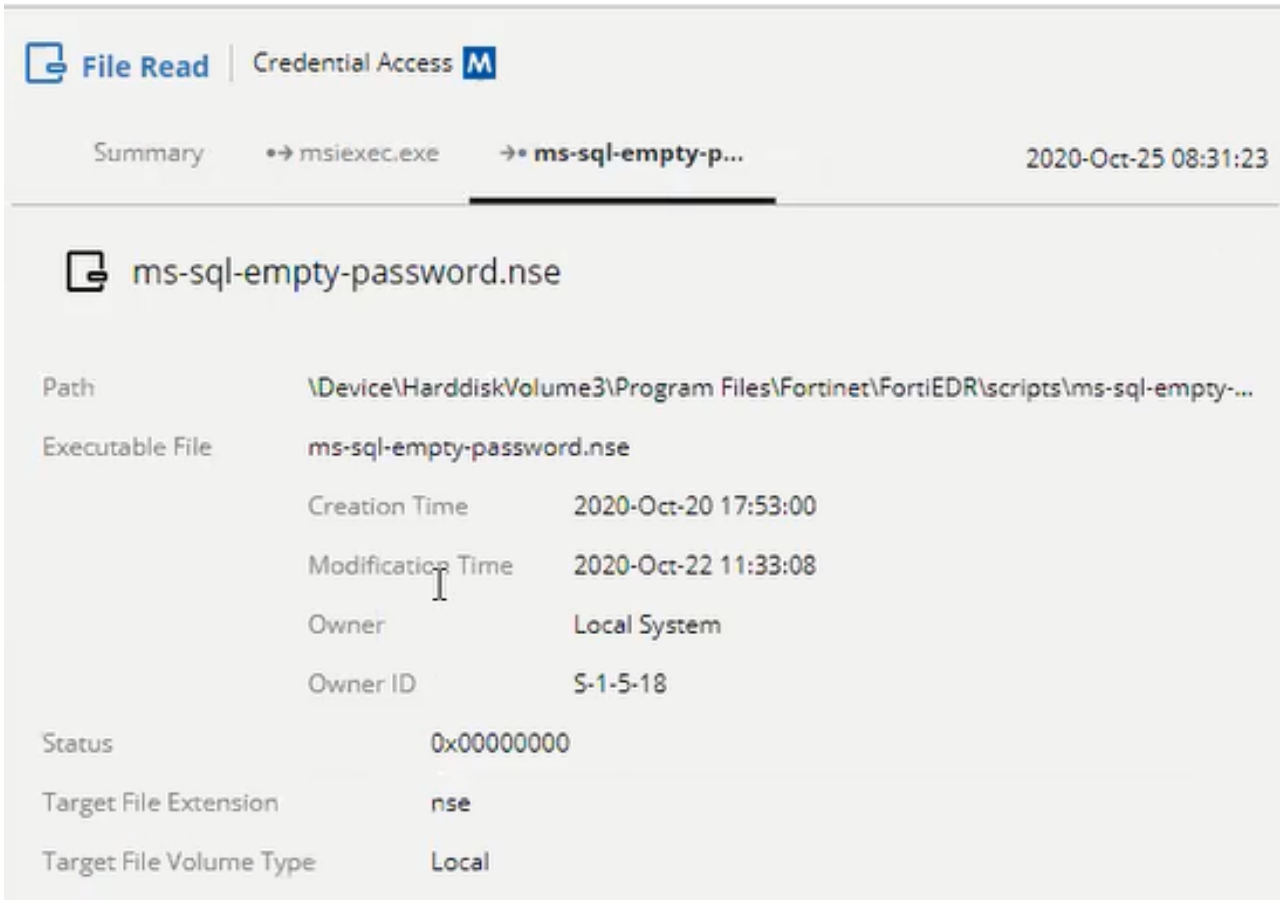


- *Summary* tab: This tab specifies a summary of the activity event. At the top of the tab, it shows details about the endpoint, including the endpoint and its IP, path, operating system, and so on. The area below the endpoint section shows the source process and its detail. The area below the source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

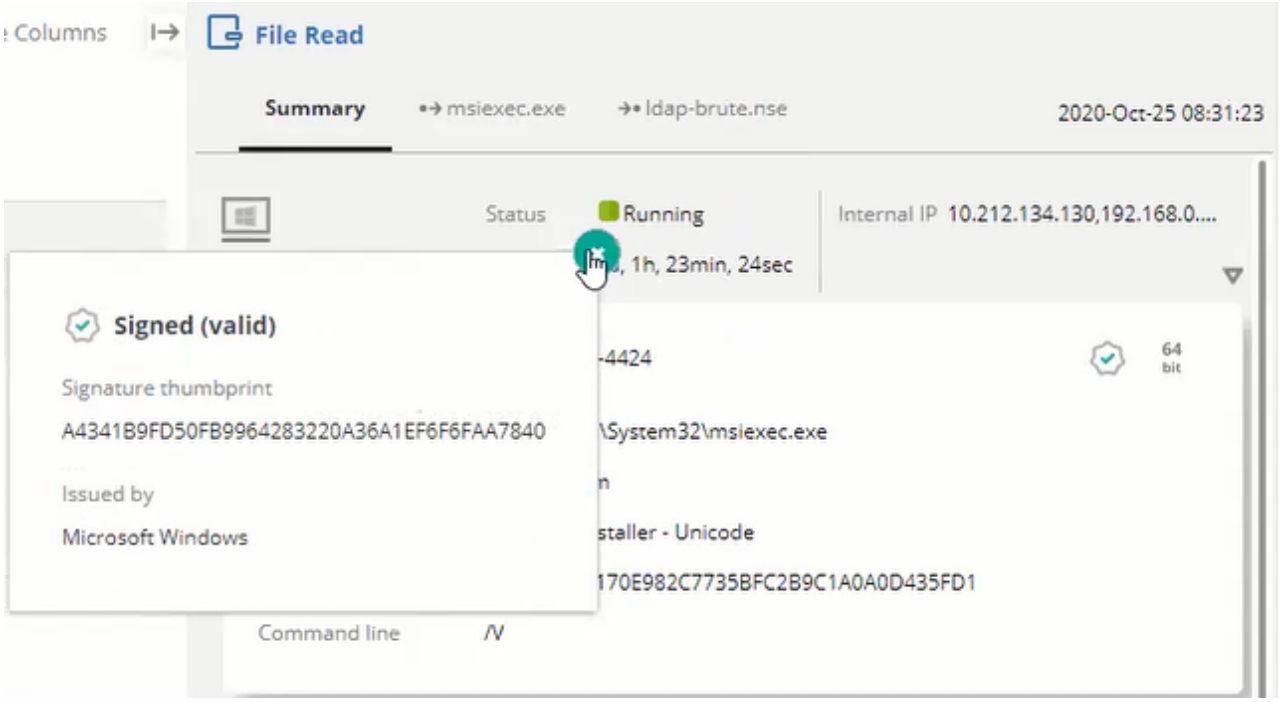
- *Process* tab: This tab shows additional details about the source process.



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



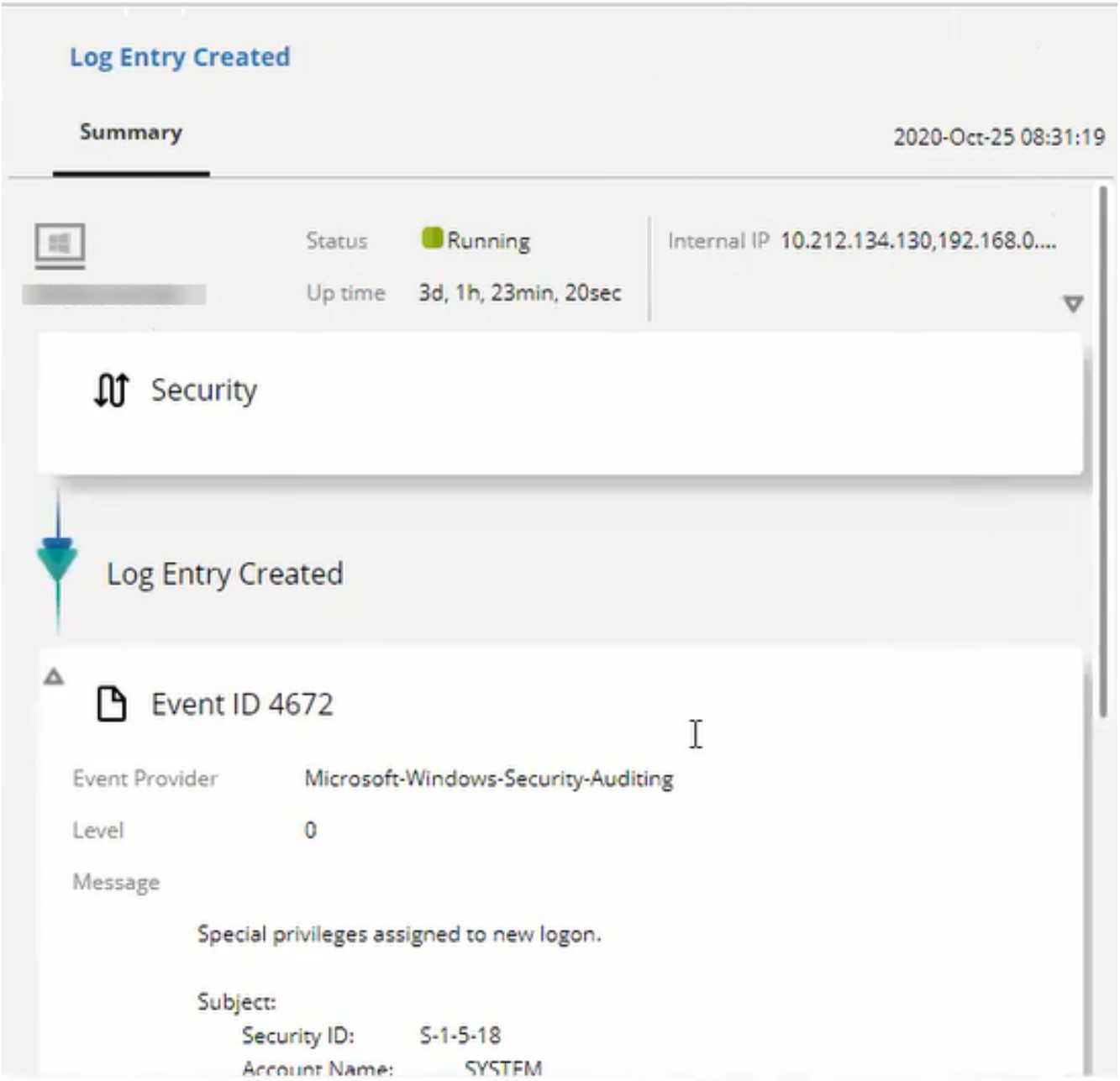
You can click an icon in the Details pane to display additional details, as shown below:



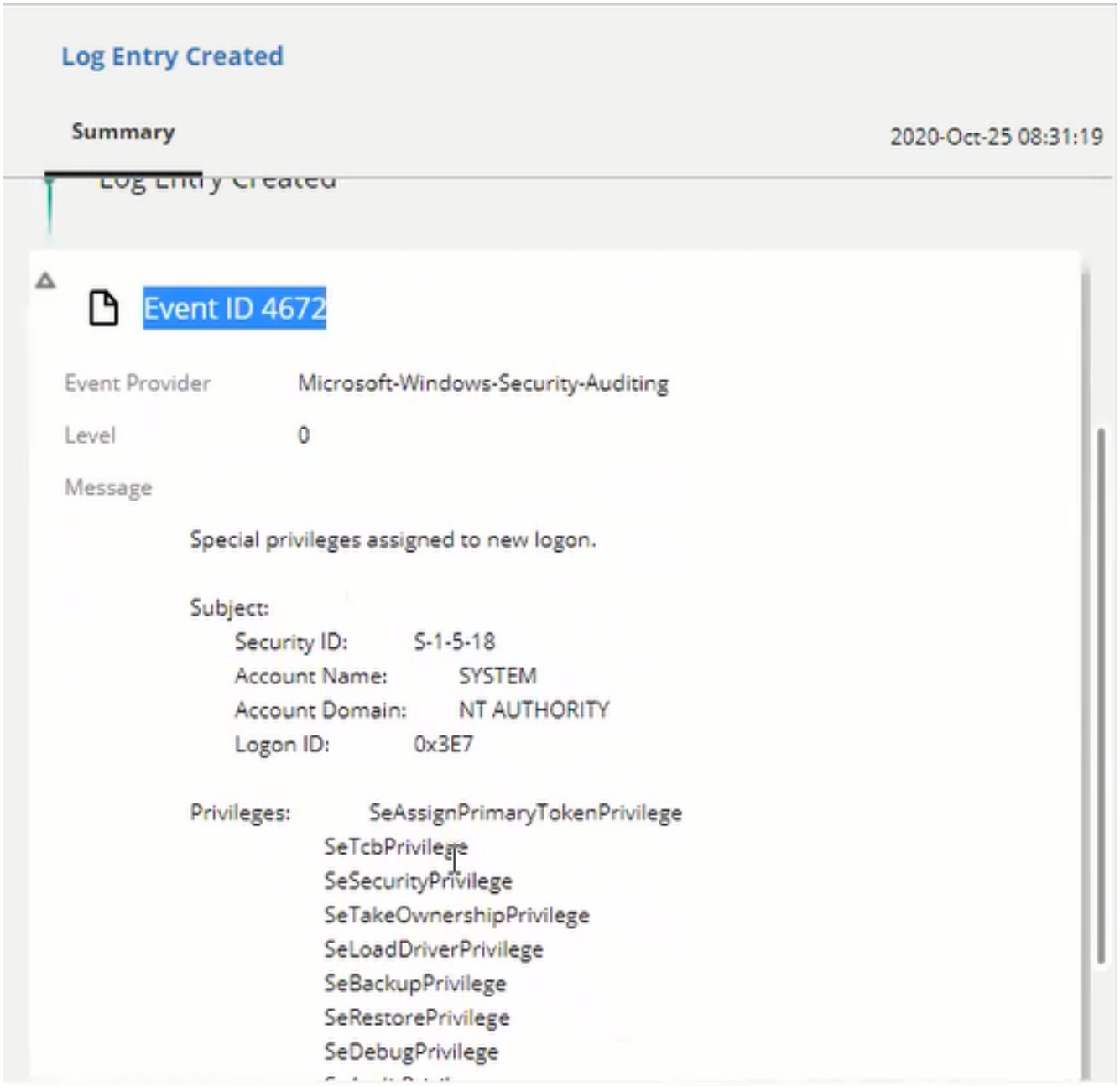
- *Investigation View* (Investigate →) button: This button opens a graphical Investigation View on page 636 of the activity events details: source, action and target. The graphical view provides the ability to add more activity events to the graph and show the relationship and timeline of the occurrence of those activities for better understanding of the flow of activity events.

Event Log Details pane

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



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

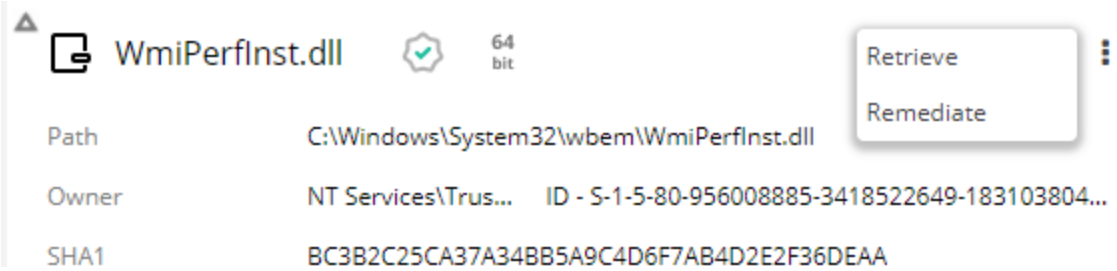


Retrieving a file / Remediating devices upon malware detection

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

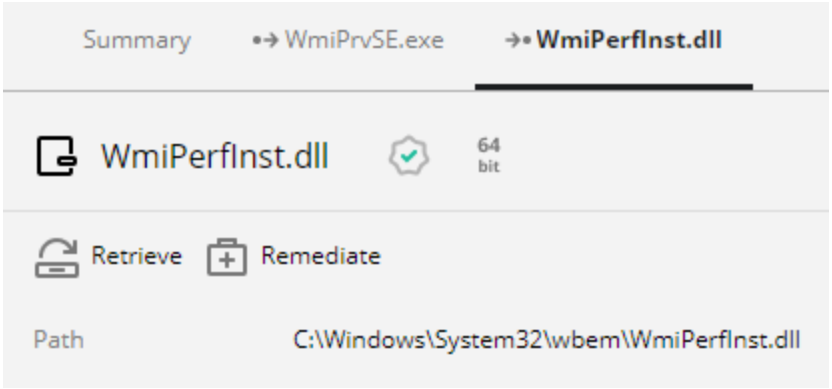
To retrieve a file or remediate the process:

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



   – OR –

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

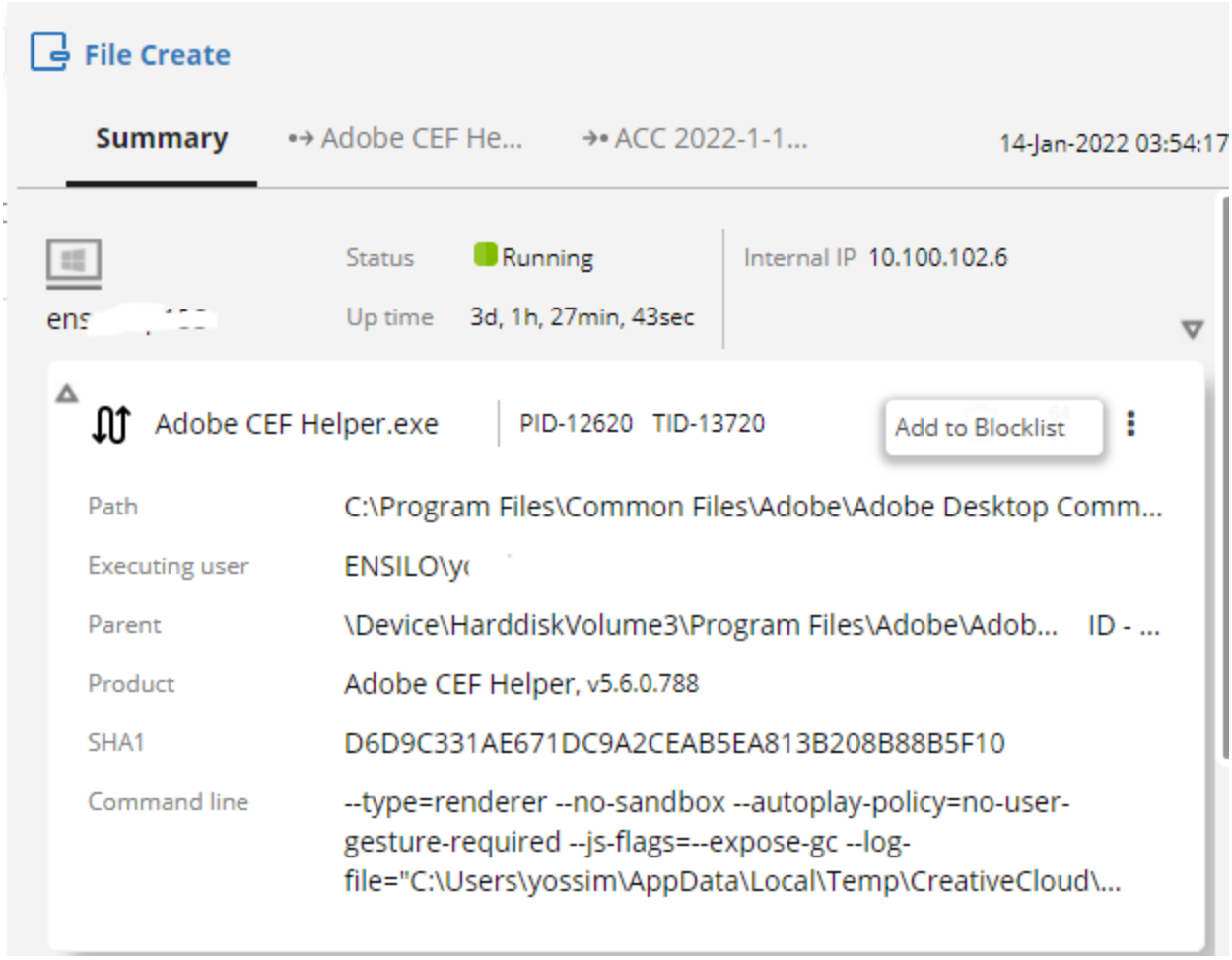


Adding an application to the Application Control policy blocklist

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

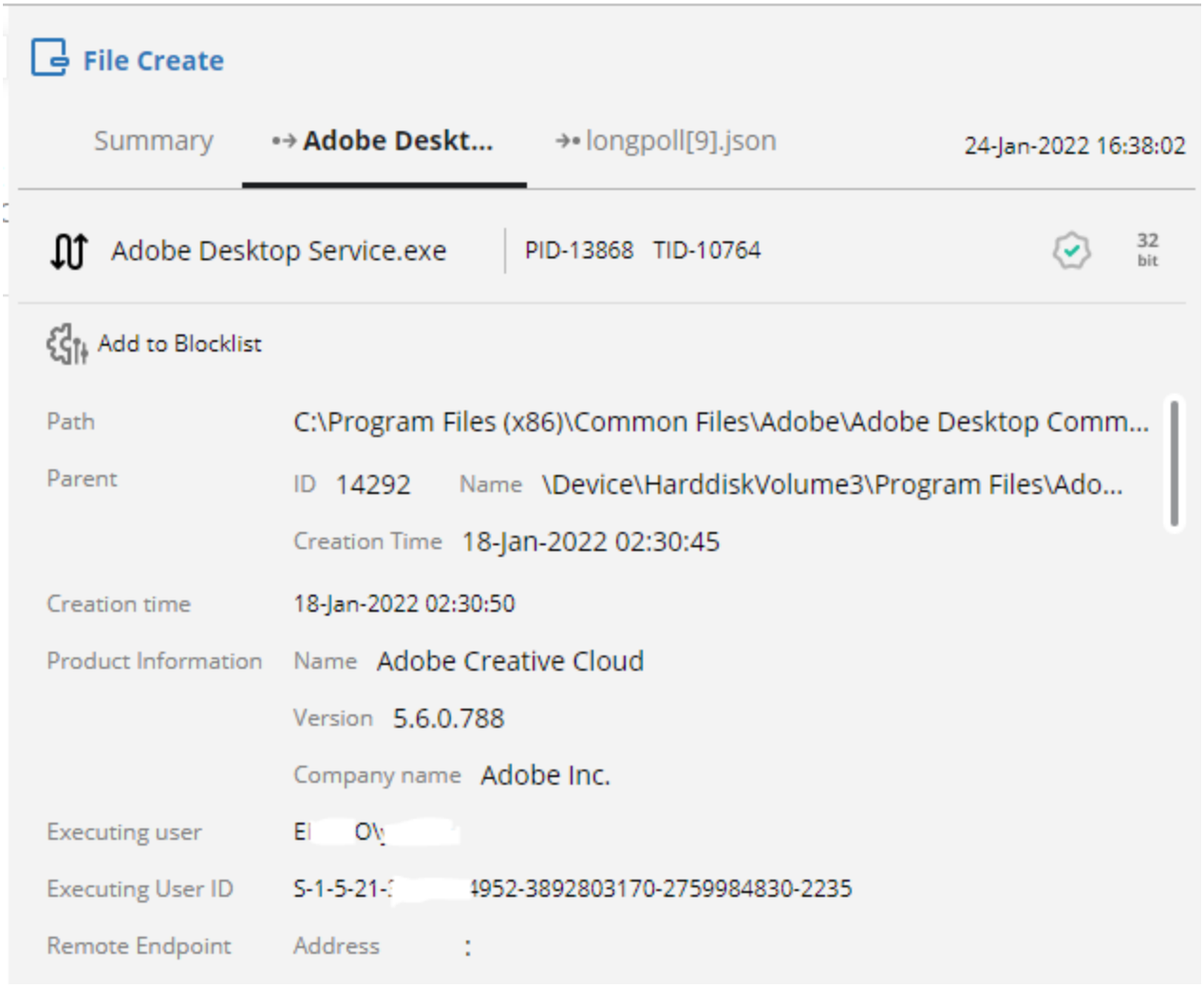
To add a process to an Application Control policy:

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



OR

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



Investigation View

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

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

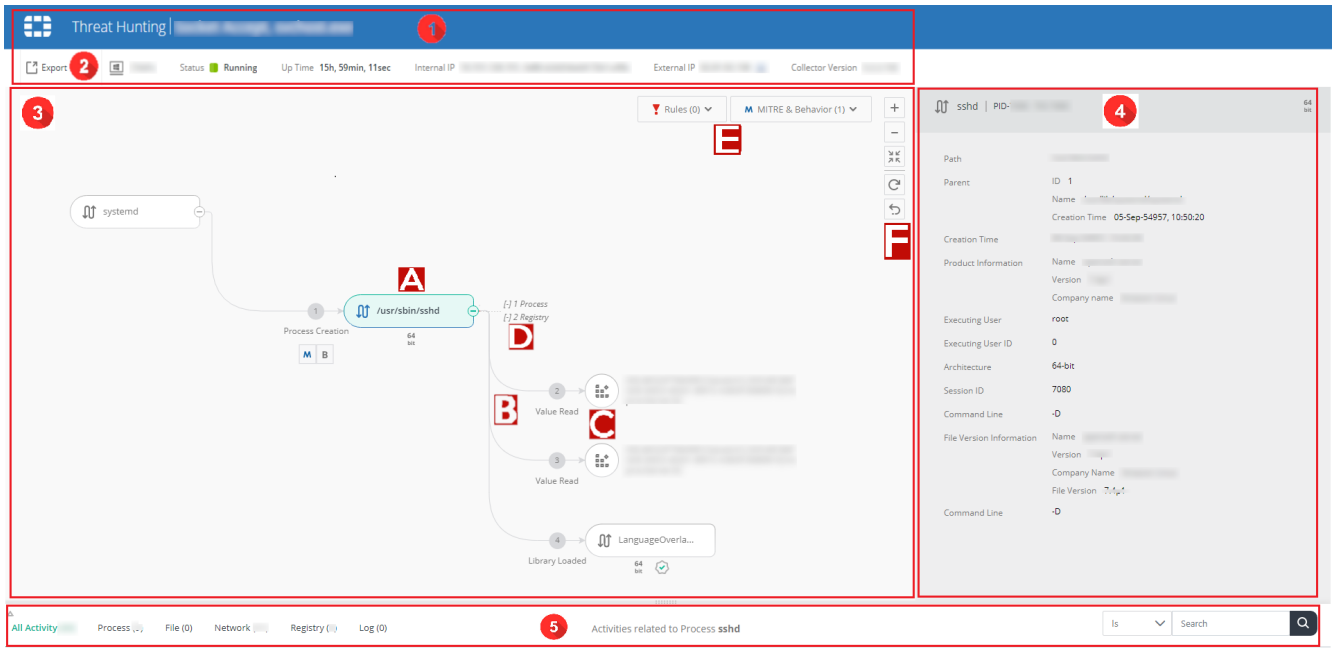
- All actions performed by a given process
- All files the process has created or updated
- All IPs the process has initiated communication with

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

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

The view adds visualization and interaction of existing data that is already available in other non-graphical and non-interactive forms without creating or generating any additional data.

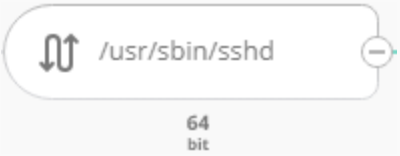
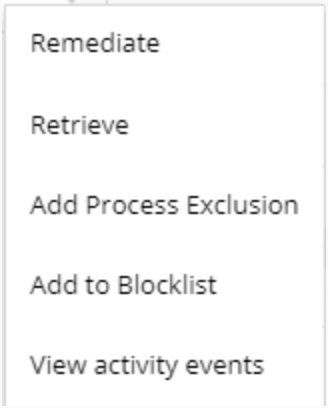
The following figure illustrates the various components of an *Investigation View* window launched from the Details Pane under *Threat Hunting*, which has the window title "*Threat Hunting* + `activity name`.

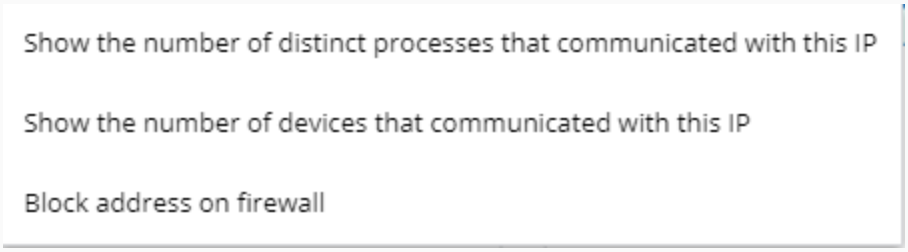


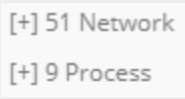
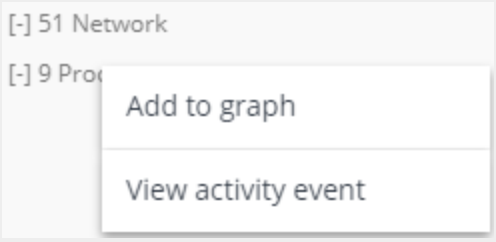
Compared with the Investigation View on page 576 window launched from the *Incidents* view, this view has the following limitations:

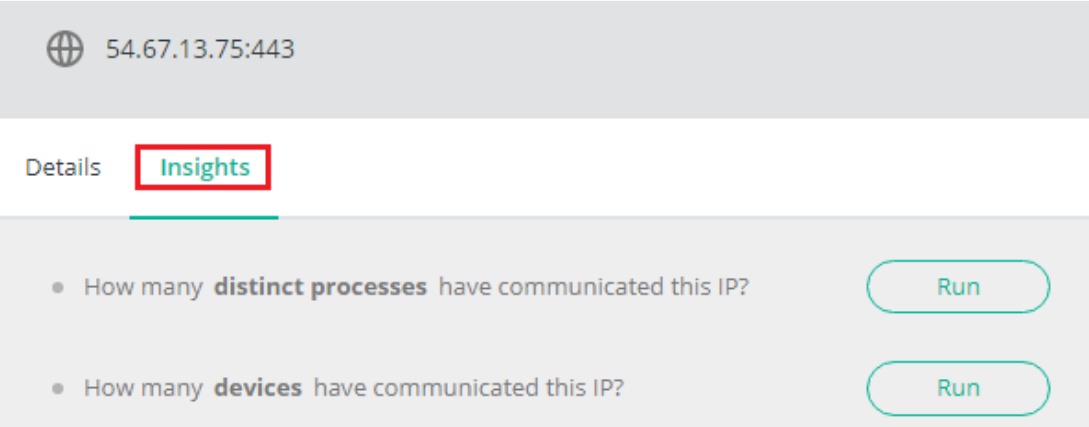
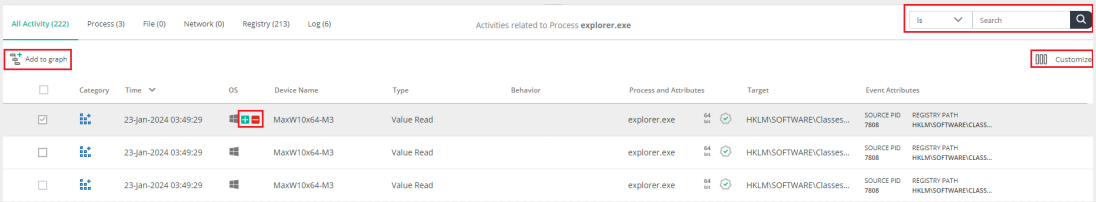
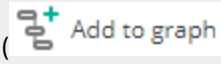
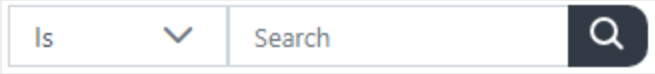
- Some threat hunting and investigation capabilities are unavailable, such as exporting the graph as JSON, variants navigation graph, and Stacks view on page 583.
- Some general event details are missing in the first row, such as classification and incident response.

Component	Description
1	General details about the device that generated the event, such as Collector status, process name, and IP address.
2	Use the *Export* button (Export) to export the *Investigation View* window as an SVG file to share with others or for record reasons. This is the only option to save a graph that includes dynamic changes based on the default graph view, such as adding processes.

Component	Description
3	Graphical flow diagram with a process tree that you can build according to your investigation needs, from left to right and top to bottom. The tree is also interactive, which means you can click on a specific component to drill down for more details or contextual actions.
A	**Node**—Source of an activity or event, which can be a process, an endpoint, a thread or service, or another security product. Nodes are represented by boxes with icons for the activity type, some with descriptions under the boxes.  • Click on a node to display the Details pane on page 628 on the right and the Activity events tables on page 624 on the bottom with contextual information about that specific node. • Click the *Collapse* ( ) or *Expand* ( ) icon in the right of a node icon to show or hide all the downstream nodes, edges, and leaves. • Right-click a node to perform actions allowed on the node, including any custom actions you defined. These action buttons also appear in the *Details Pane*, which is available on the right after you click the node. The list of available options varies by node type. The following is an example list of actions for a process node. 
B	**Edge**—Activity event type or action represented by a curved line with an arrow. An edge can be one activity event/action or an aggregation of several. The numbered arrows indicate the sequence of actions and specify the action that was performed, such as *Process Creation*, *Socket Close*, *Block* and so on. Multiple operations performed between two processes are represented by multiple arrows between them. Edges that triggered the event are indicated in red.

Component	Description
	 Click on an edge to display the Details pane on page 628 on the right with contextual information about that specific edge. Edges may also have icons below them indicating classification or MITRE & Behavior models. Click on an icon for more detailed information. 
C	**Leaf**—Target of activity event of type File, Registry Key, Registry Value, Network components (IP/DNS/URL). A leaf can also be a group of artifacts. For example, all the files created or modified by a process. Leaves have a round shape (). • Click on a leaf to display the Details pane on page 628 on the right and the Activity events tables on page 624 on the bottom with contextual information about that specific leaf. • Right-click a leaf to perform actions allowed on the leaf, including any custom actions you defined. These action buttons are also available in the *Details Pane*, which appear on the right after you click the leaf. The list of available options varies by leaf type. The following is an example list of actions for a network leaf: 

Component	Description	
	D	**Hint**—Categorized groups of activities related to a node that are not part of the main chain of activity events and thus not represented in the graphical diagram. Click a node to show the number of relevant activities. The hints no longer display after you move the selection to another node or edge.  • Click the *Expand* ([+]) or *Collapse* ([-]) icon near a leaf hint to show or hide the node or leaf list of that type. • Right-click the type name of a hint and select *Add to graph* to add the relevant leaves to the graph or select *View activity event* to pull out the Activity events tables on page 624 for this specific file type. The *Add to graph* option is unavailable when the number of hints exceeds 500, in which case you can only choose to view the activity event. 
	E	Use the *MITRE & Behavior* legend to highlight the corresponding icons below relevant edges in the diagram. 
	F	• Use the *Zoom In* (), *Zoom Out* (), and *Zoom To Fit* () buttons to adjust the graph window size. • Use the *Reset* () button to restore the graph to the default view. • Use the *Undo* () button to cancel an operation.
4	Details pane on page 628 for the selected node, edge, or leaf where you can view details of the activity, action, or target, and perform common actions on a node or leaf, such as retrieving a file, remediating devices upon malware detection, or adding an application to the Application Control policy blocklist. The actions can also be performed by right-clicking a node or leaf and selecting the option from the menu. For specific leaf types, this pane also includes an *Insights* tab which allows you to run queries to retrieve analytics data, such as the number of communicating processes or devices of a certain IP. The *Insights* options are also available from the right-click menu of those leaf types.	

Component	Description
	
5	Contextual Activity events tables on page 624 for the selected node or leaf organized by tabs of activity types. Drag the top edge of the table up for a fuller view of the table. Activities with a number at the front of the row are already in the graph and the number matches the one in the graph.  • To add activities to the graph, select the corresponding rows and click *Add to graph* (). • To customize the columns to display in the table, click *Customize* (). • To search for a specific activity or event, enter keywords in the search bar on the top right corner (). • To filter the results in the Activity Events table to include or exclude a specific value, use the green plus () and red minus () icons that appear when you hover over the value. Multiple filters are supported. To delete a filter, click the cancel icon that appear when you hover over the filter on the top-left of the table.

Remediating a device upon malware detection

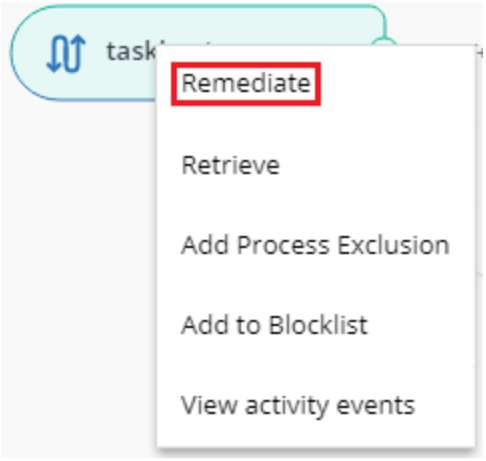
After malware is detected on a device, you can remediate the device from the Investigation View on page 576 (detailed in the procedure below) or by connecting to the device directly using the EDR Connect on page 592 functionality.

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

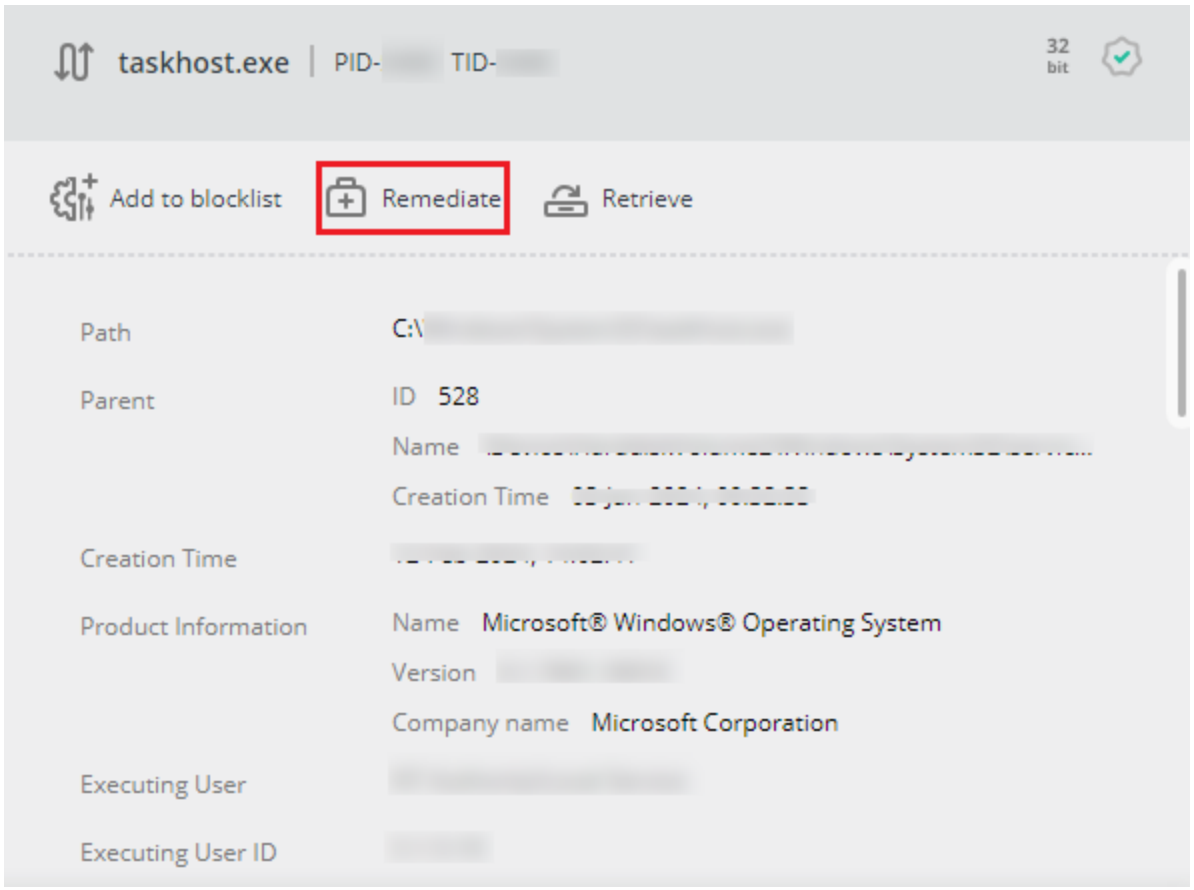
Method	Description
Terminate the Process	This method does not guarantee that the affected process will not attempt to execute again.
Delete the Affected File from the Computer	This method ensures that the file does not attempt to exfiltrate data again, as the file is permanently removed from the device.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

To remediate a device from the Investigation View on page 576:

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

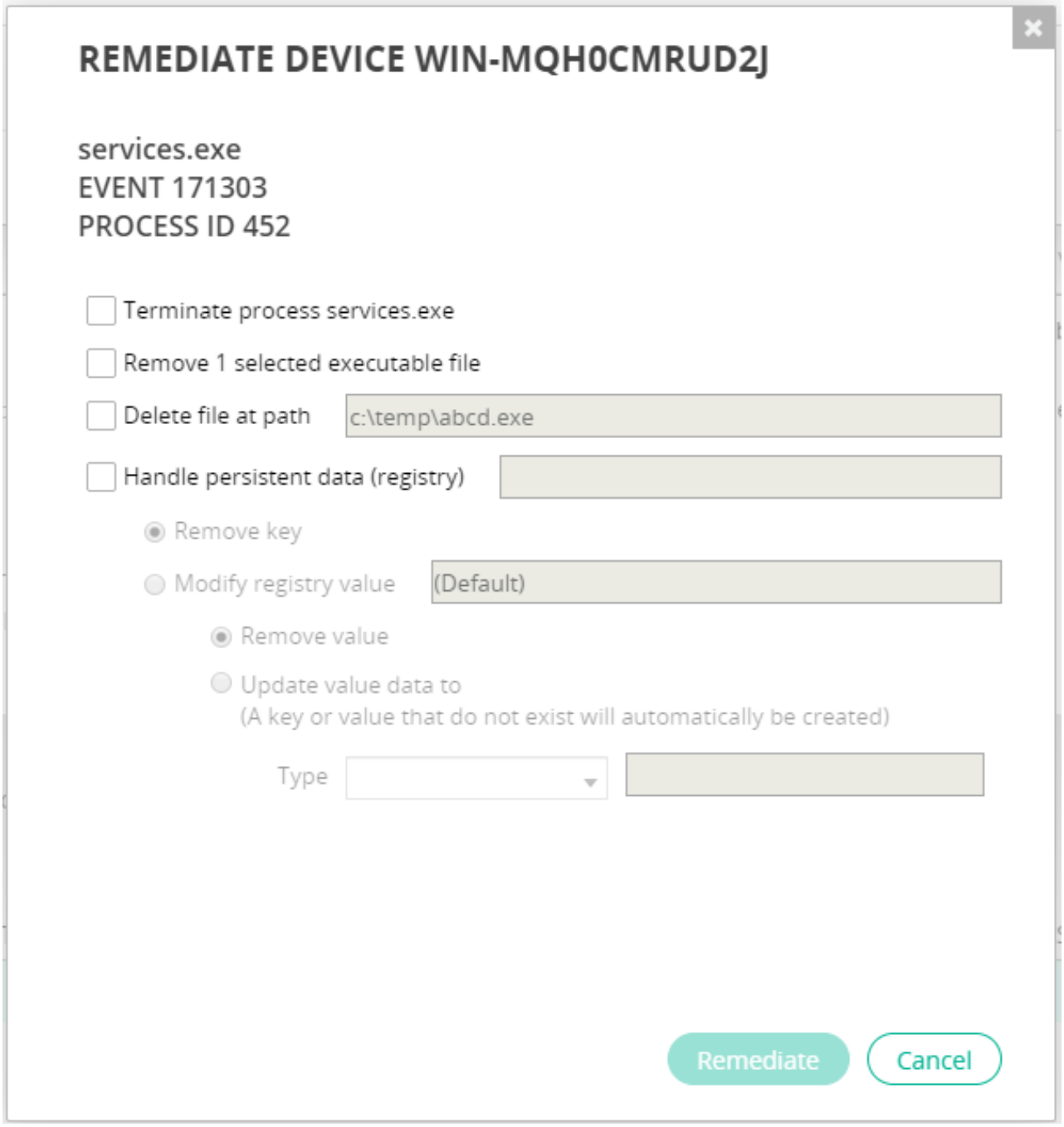


Alternatively, select the node of the relevant activity event and click the *Remediate* button in the *Details Pane* that appears on the right.

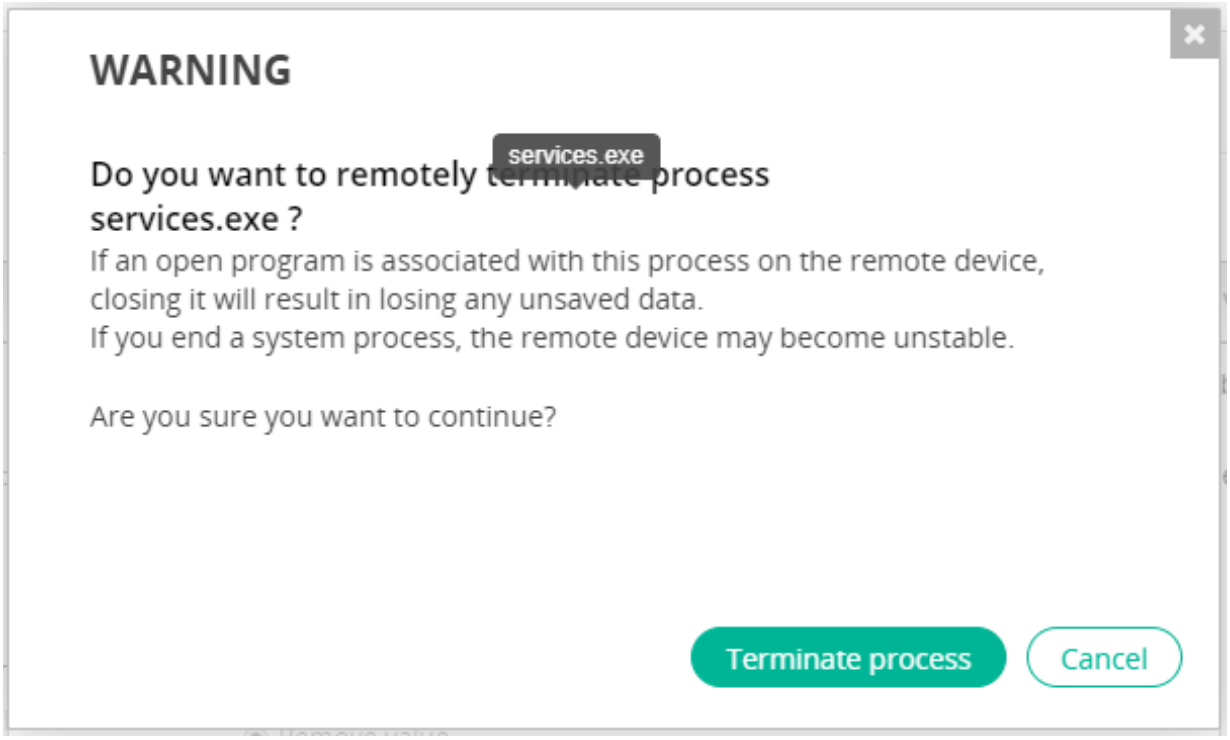


The *Remediate* button is also available from the Stacks view on page 583, which is available when an edge is selected.

2. The following window displays:

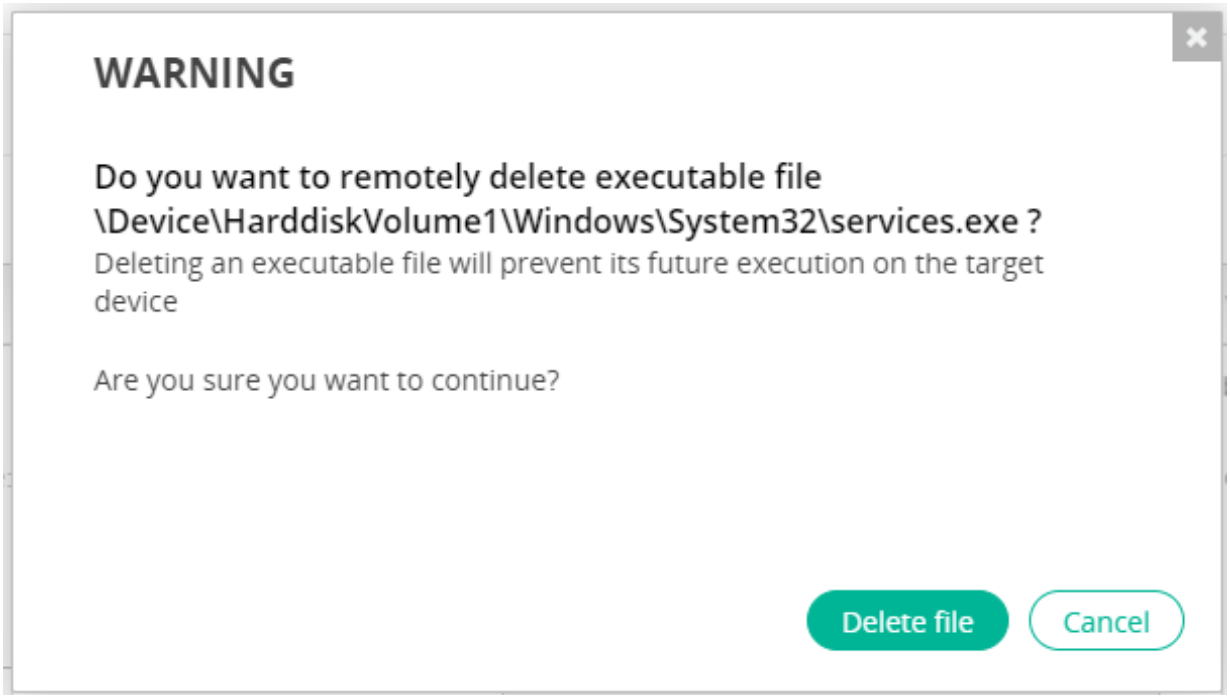


3. Do one of the following:
   a. Check the *Terminate process* checkbox to terminate the selected process. A warning message displays.



Click *Terminate process* to terminate the selected process.

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

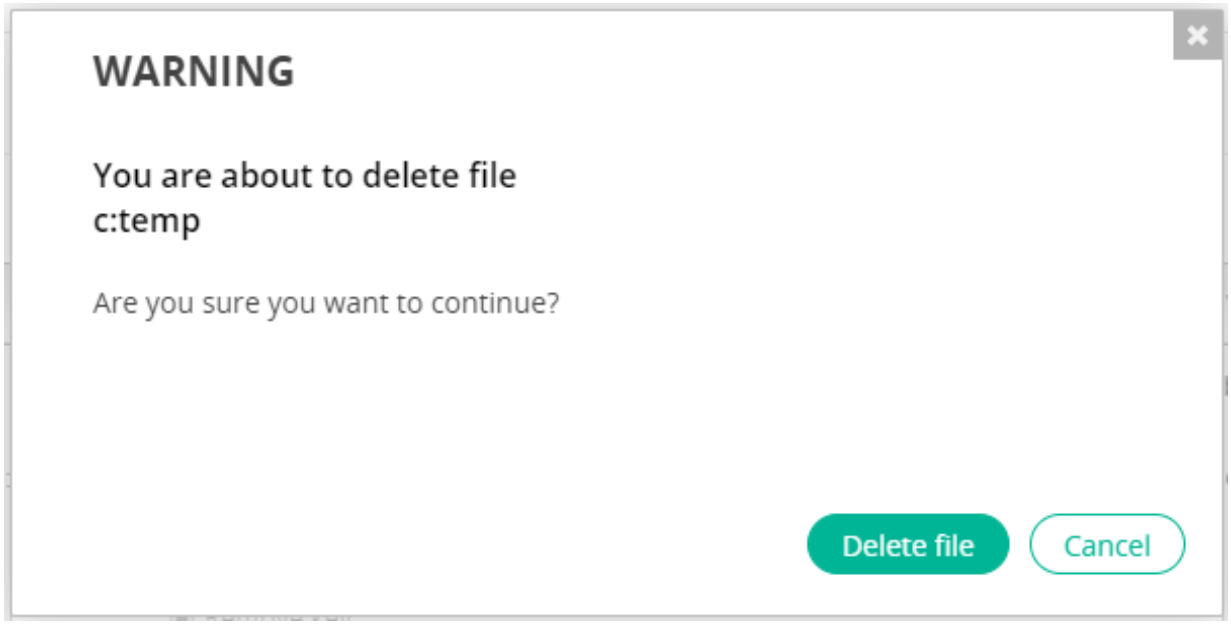


Click *Delete file* to remove the selected file.

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

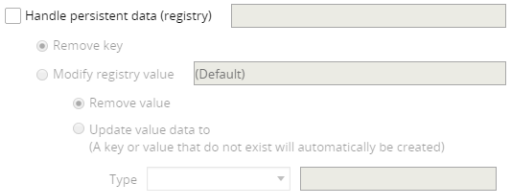


A warning message displays.



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

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



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

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

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

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

4. Click *Remediate*.

Communication control

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

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

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

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

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

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

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

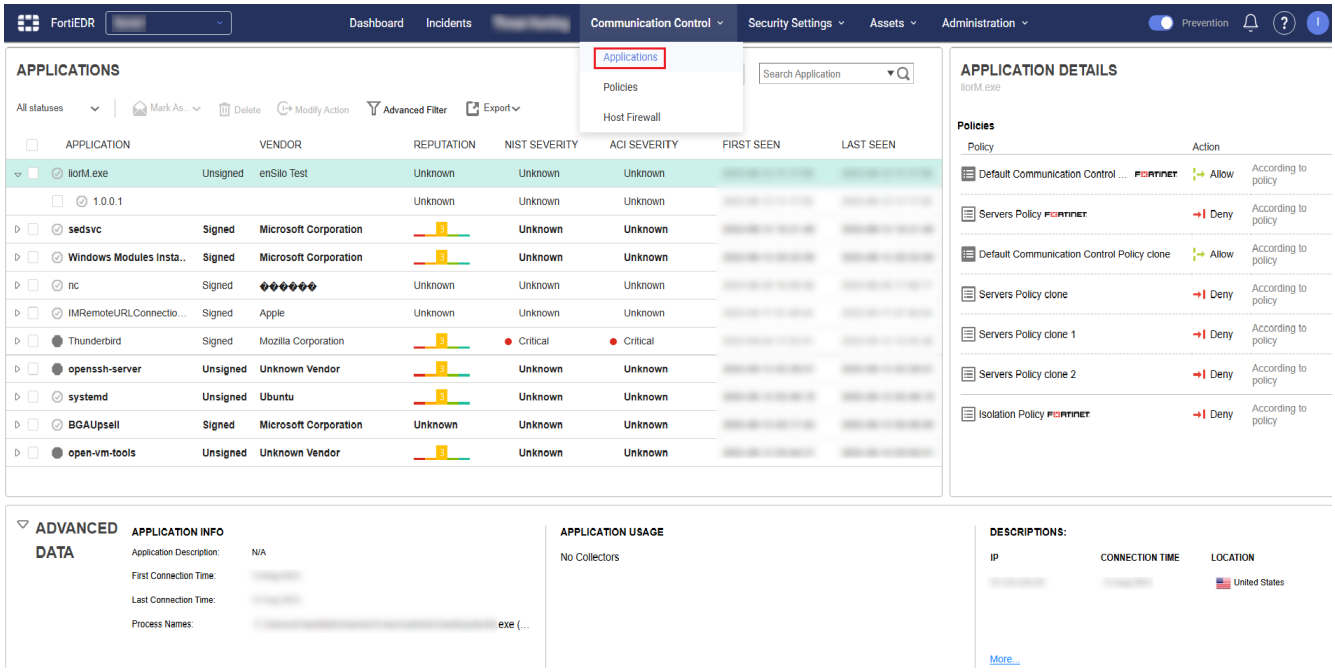
The *COMMUNICATION CONTROL* tab contains the following pages:

- Applications on page 647
- Policies on page 662
- Host Firewall on page 672

Applications

The *APPLICATIONS* page lists all communicating applications detected in your organization that have ever attempted to communicate. By default, applications are sorted according to their first-seen indicator,

placing new applications at the top. To access this page, click the down arrow next to *COMMUNICATION CONTROL* and then select *Applications*.



Information is organized hierarchically in a two-level tree. The first (top) level specifies the name of the application. The second level specifies the application version.

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

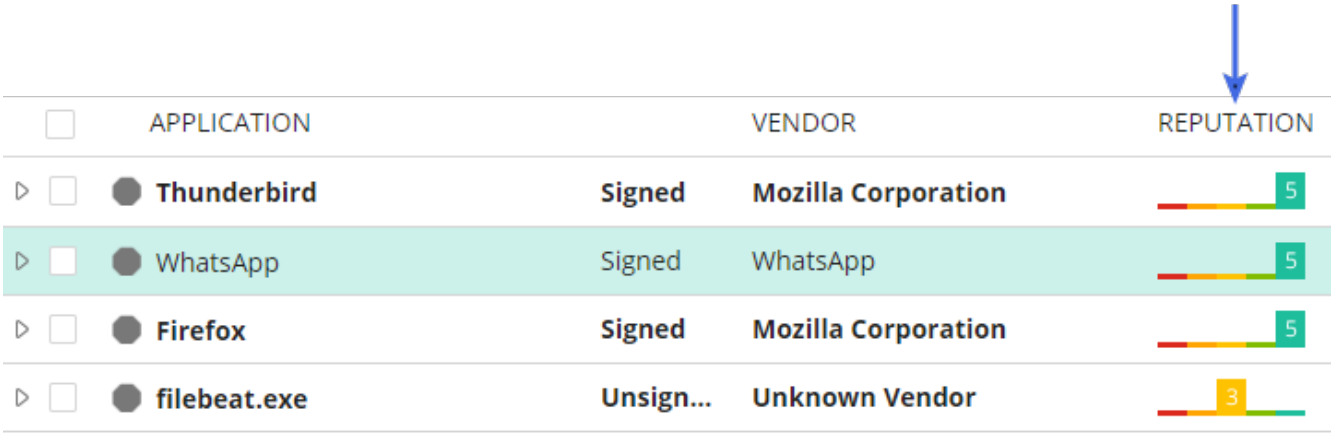
- Selection checkbox
- Resolving status icon
- Signed/Unsigned indication
- *APPLICATION/VERSION*: The name of the application/version.
- *VENDOR*: The application's vendor and certificate details.
- *REPUTATION*: The reputation score of the application. For more details, Reputation score on page 648
- *VULNERABILITY*: The highest CVE vulnerability score for the application. For more details, see Severity on page 649
- *FIRST SEEN*: The date and time when the application was first seen in the organization.
- *LAST SEEN*: The date and time of the last connection of this application.

The *APPLICATION DETAILS* area of the window on the right displays policy-related details for the entity (application or version) selected in the application list. This area displays the policy action (Allow or Deny) for each communication control policy.

The *Advanced Data* area at the bottom of the window presents statistics about the selected application/version in the application list. For more details, see Advanced Data on page 656.

Reputation score

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



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

Reputation Score	Reputation Description
1	Known as bad
2	Assumed as bad
3	Unclear, indication a contradiction or inability to determine the reputation
4	Assumed as good
5	Known as good

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

Severity

EDR's severity scoring system provides a useful tool for vulnerability assessment and enables you to review the weaknesses detected in your environment that could be exploited by attackers before they actually occur. You can then use virtual patching to block applications with known critical vulnerabilities so that they cannot connect until the system is patched for the CVEs listed.

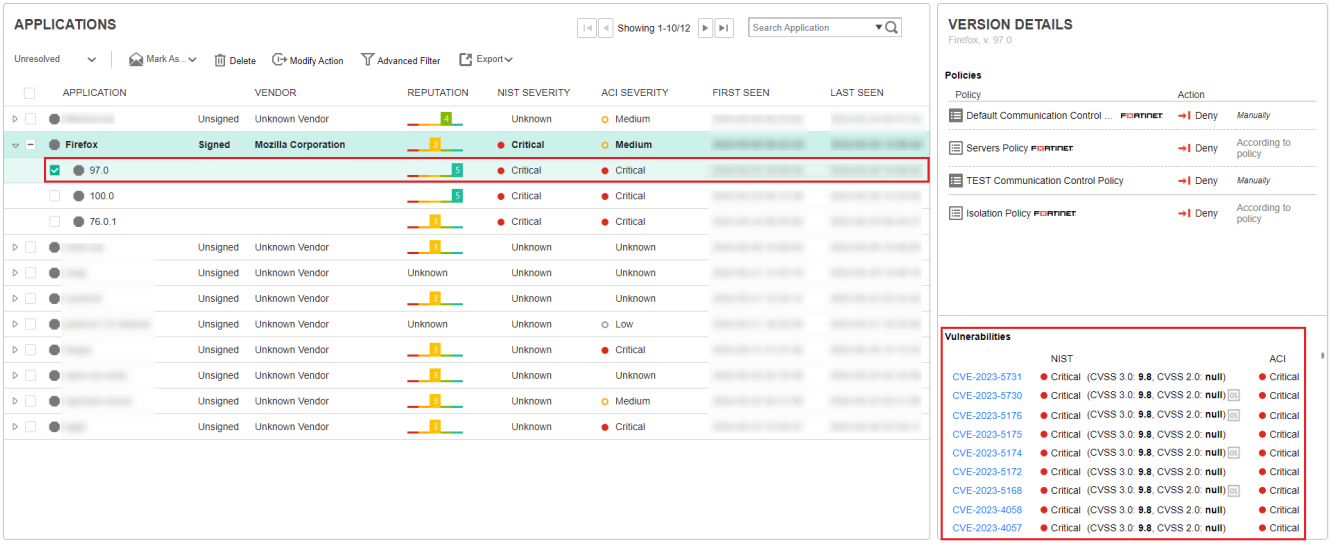
It also provides comprehensive visibility into the organization's external attack surface so that analysts can prioritize security alerts and incidents based on risk factors such as severity of vulnerabilities, relevance of threat intelligence feeds, and severity of affected endpoints, ensuring that efforts are focused on addressing the most significant risks to the organization.

Each application and version in the application list shows two severity ratings:

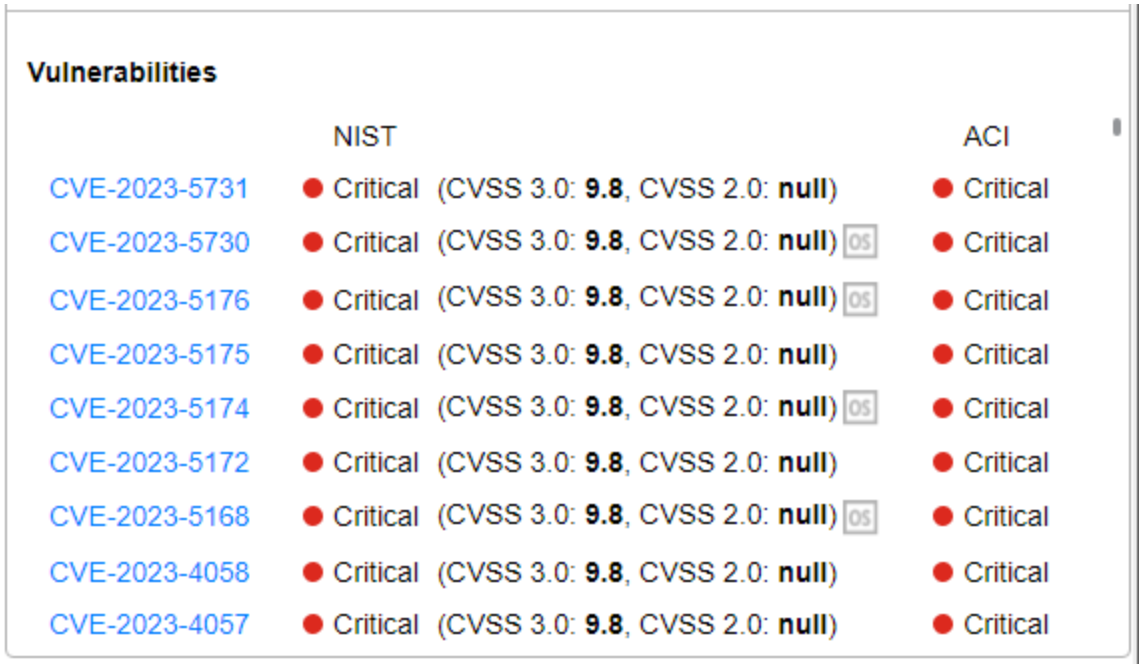
- NIST Severity—Rating provided by EDR's vulnerability scoring system leveraging the NIST Cybersecurity Framework.
- ACI Severity—Adversary Centric Intelligence (ACI) rating provided by FortiRecon leveraging FortiGuard Threat Analysts to provide comprehensive coverage of dark web, open source, and technical threat intelligence, including threat actor insights. This information enables administrators to proactively assess risks, respond faster to incidents, better understand their attackers, and protect assets.

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

- Unknown
- Low
- Medium
- High
- Critical

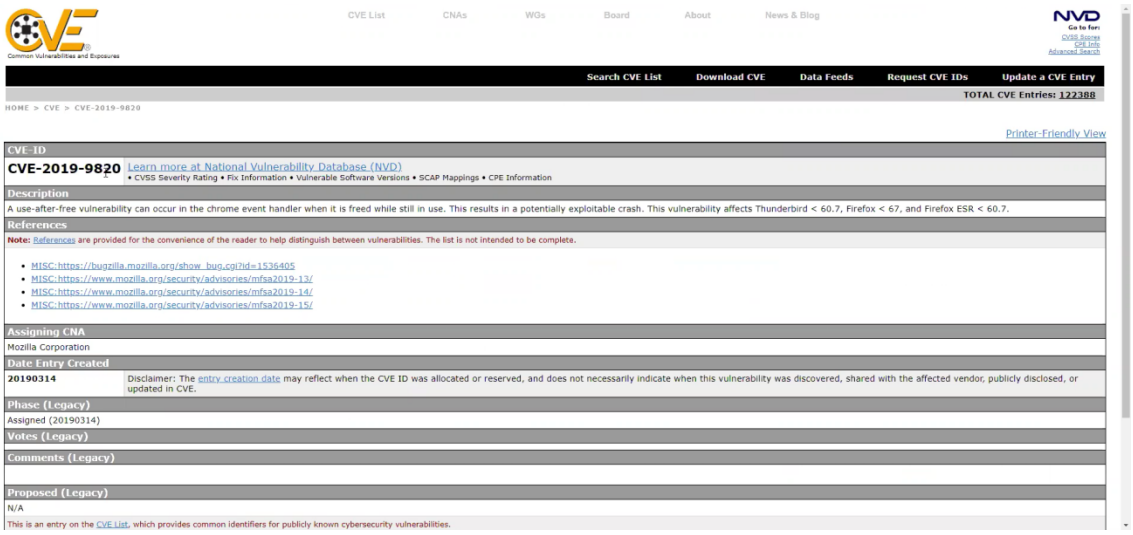


The Vulnerabilities area at the bottom right of the window lists the CVE-identified vulnerabilities for the selected application and version. Each CVE row includes the CVE identifier, the NIST and ACI severity category and the Common Vulnerability Scoring System (CVSS) vulnerability score .



CVSS scoring utilizes two systems: CVSS 3.0, the most recent, and CVSS 2.0, its predecessor. EDR vulnerability information presents both CVSS 3.0 and CVSS 2.0 scores.s

You can click a CVE identifier link to view more details about that vulnerability in your browser, including the type of vulnerability, the application(s) it affects, the version(s) it affects and so on.



After a vulnerability is detected in your system, you can decide the type of the action needed to address it. Typically, it is recommended to upgrade to a newer version of the application, meaning one that does not have the identified vulnerability. Alternatively, virtual patching can be applied with vulnerability-based policy that is configured to block communication of any application with known critical vulnerability. For more details, see Policies on page 662. The information presented in the *Advanced Data* area of the window also provides useful information to help protect against vulnerabilities. For more details, see Advanced Data on page 656.

Resolved vs. unresolved applications

By default, all new applications have an Unresolved status. Unresolved means that either EDR 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.

EDR 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 EDR. Applications with the Resolved status are indicated by the ⊘ icon in the application list. You can also change applications to the Resolved status manually.

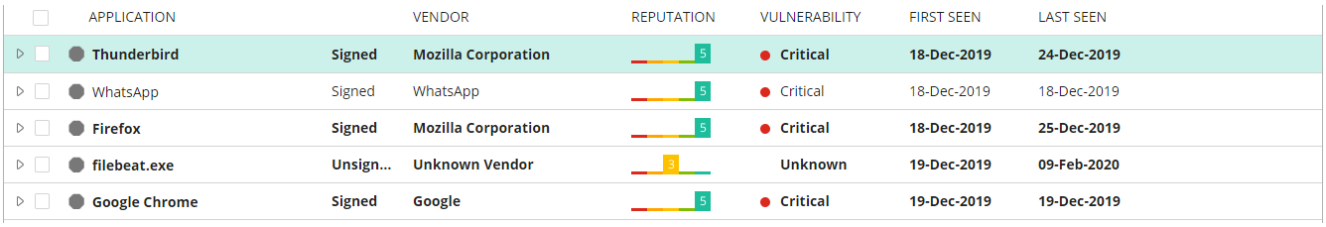
Sorting the Application List

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

Marking an Entry as Read/Unread

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

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

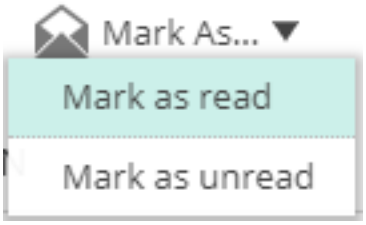


APPLICATION		VENDOR	REPUTATION	VULNERABILITY	FIRST SEEN	LAST SEEN
Thunderbird	**Signed**	**Mozilla Corporation**	5	**Critical**	**18-Dec-2019**	**24-Dec-2019**
WhatsApp	Signed	WhatsApp	5	Critical	18-Dec-2019	18-Dec-2019
Firefox	**Signed**	**Mozilla Corporation**	5	**Critical**	**18-Dec-2019**	**25-Dec-2019**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

To mark an entity as read:

Select the entity's (application or version) checkbox and then click the down arrow on the 

button and select **Mark as read**. The text no longer displays in bold.

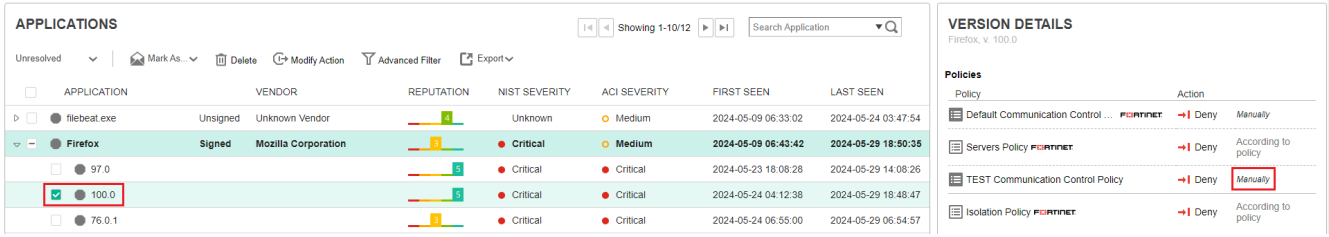


Note – If you mark an application version as read, all lower levels in the version hierarchy for that application are also marked as read.

Modifying a Policy Action

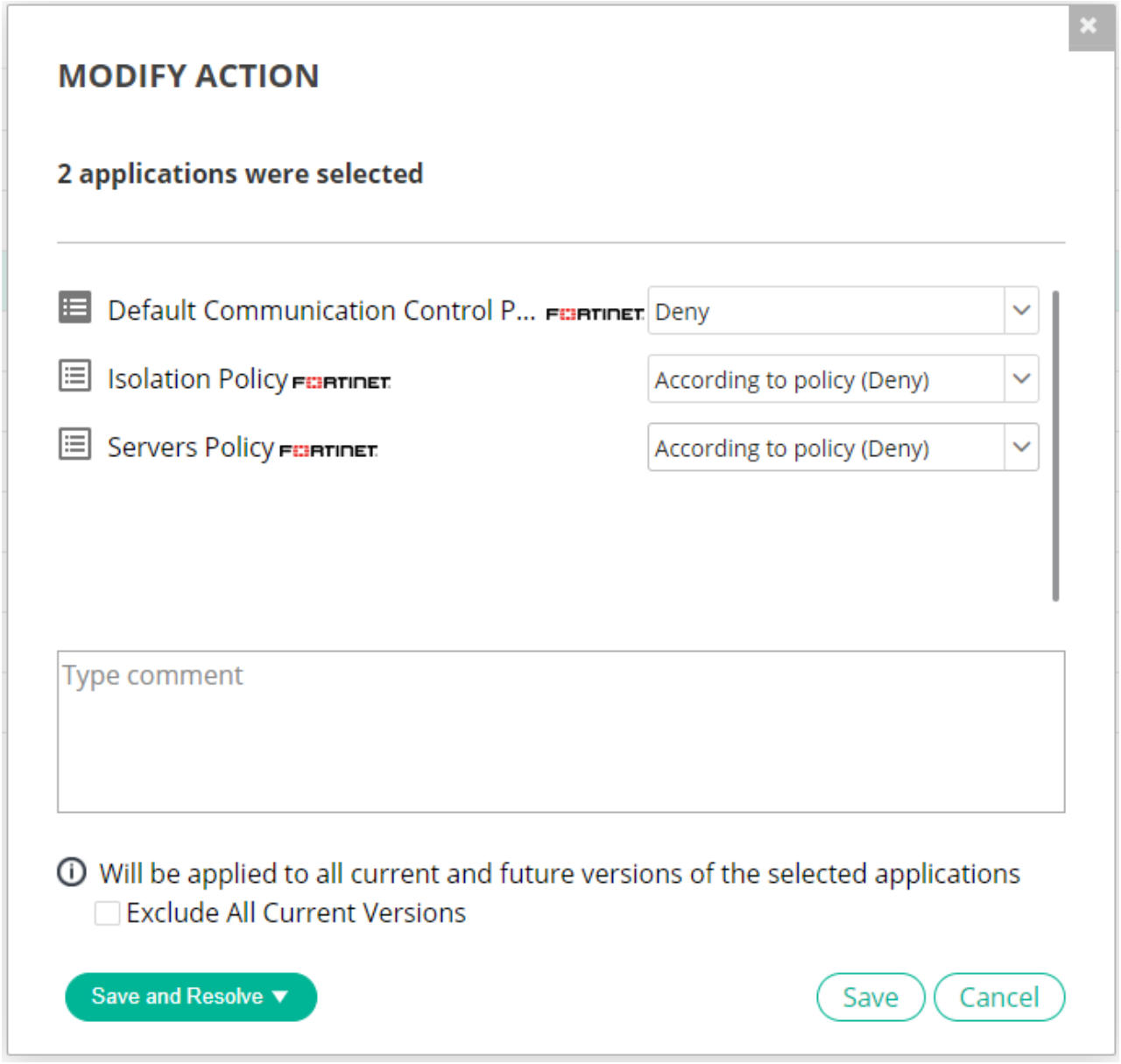
The following describes how to apply a different action to an application/version other than that specified in the current policy for that application/version. In this case, the application/version is excluded from the current action defined in the policy (Allow or Deny).

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



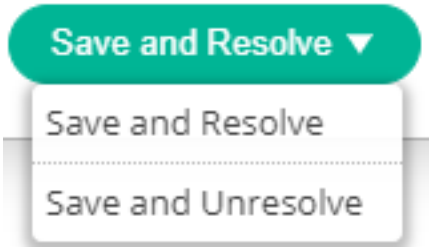
To modify a policy action:

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



2. In the dropdown list on the right of the policy row whose action you want to change, click the down arrow and then select the action to apply to the selected entity. You can change the action for one or more policies.
3. [Optional] In the Comment field, enter a free-text comment describing the action change. By default, the date and time when the policy action was changed automatically displays.



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

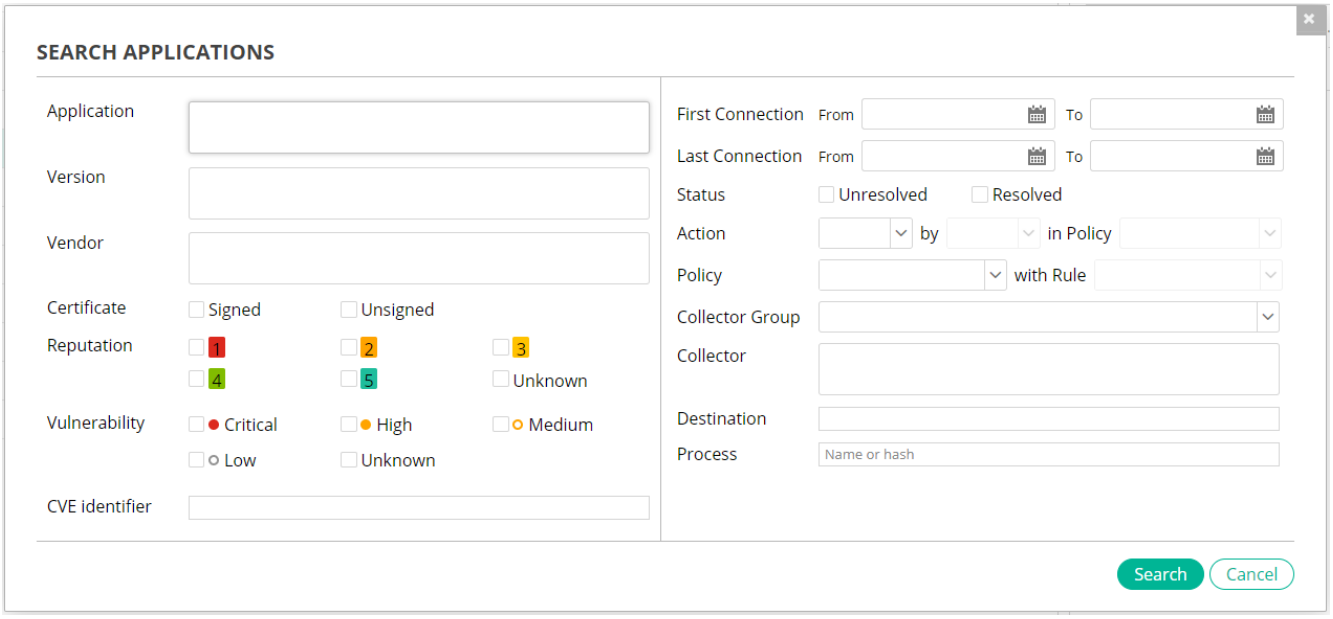
button to save the new communication control decision for the selected application(s).

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

Searching the Application List

You can use the 

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



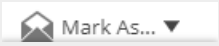
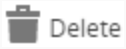
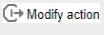
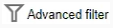
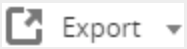
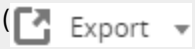
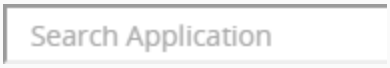
You can filter the application list by the following criteria:

Filter	Criteria
Application	Filters by application name

Filter	Criteria
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.
Vulnerability	Filters by vulnerability score.
CVE Identifier	Filters by exact match of the vulnerability identifier, using the following format – CVE-YYYY-nnnn.
First Connection / Last Connection	Filters by the specified date range when the first/last connection of the application was detected in the system.
Status	Filters by status (Resolved, Unresolved,).
Action	Filters by action.
In Policy	Filters by policy. If you specify a specific action in the Action field, then you can only select from policies with that specific action.
Policy	Filters by a specific policy.
With Rule	Filters by a specific policy predefined rule.
Collector Group	Filters by the Collector Group used to communicate. This means that a device(s) in the specified Collector Group was used to communicate.
Collector	Filters by the Collector (device) used to communicate.
Destination	Filters by the Collector destination (IP address).
Process (Name/Hash)	Filters by the process name or hash value.

Other options in the Application pane

Option	Function
	Click the down arrow in the button and then select an option in the dropdown list to filter the application list accordingly. You can filter the list by:
All	Lists all applications for the organization.
Unresolved	Lists applications that have not been resolved by either the user or EDR. 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 EDR. Applications with this status are indicated by the ⊘ icon in the application list.

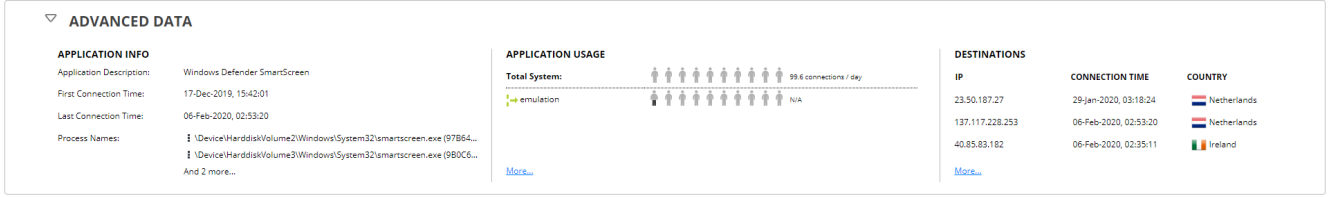
Option	Function
Unknown Vendors	Lists applications whose for which the vendor is not known in the system.
Low Reputation	Lists applications with a low reputation score.
Critical CVE	Lists applications with a Critical CVE score.
Unread	Lists applications that have not yet been viewed in the application list.
	Click the down arrow on the  button and then select *Mark as read* or *Mark as unread*. For more details, you may refer to the Marking an Entry as Read/Unread on page 652.
	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.
	Click the button to change the current policy action to be applied for the selected entity, as described in Modifying a Policy Action on page 652
	Click the advanced filter to review applications by suspicious characteristics, such as existing vulnerabilities or reputation score. This filter can be used to set up policy rules. See Policy rules on page 666. 
	Click the down arrow in the *Export* button ( and select the format for exporting data. You can select *Excel* or *JSON*.
	Use the *Search Application* field to perform an advanced search, as described in Searching the Application List on page 654.

Advanced Data

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

Application Advanced Data

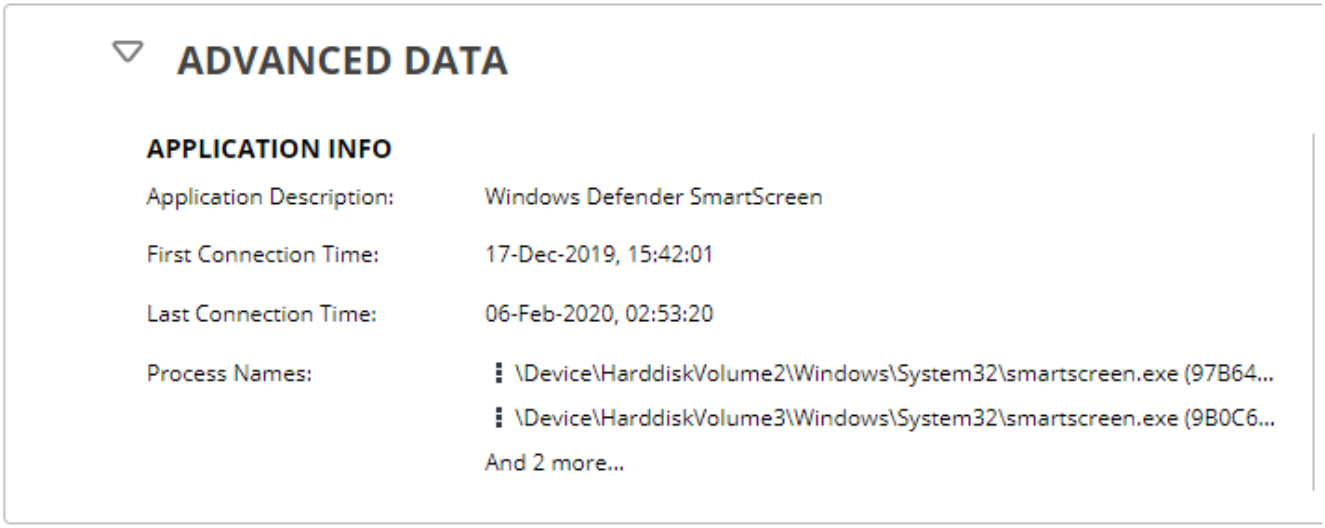
When an application is selected in the application list, the *ADVANCED DATA* area displays the following information for it:



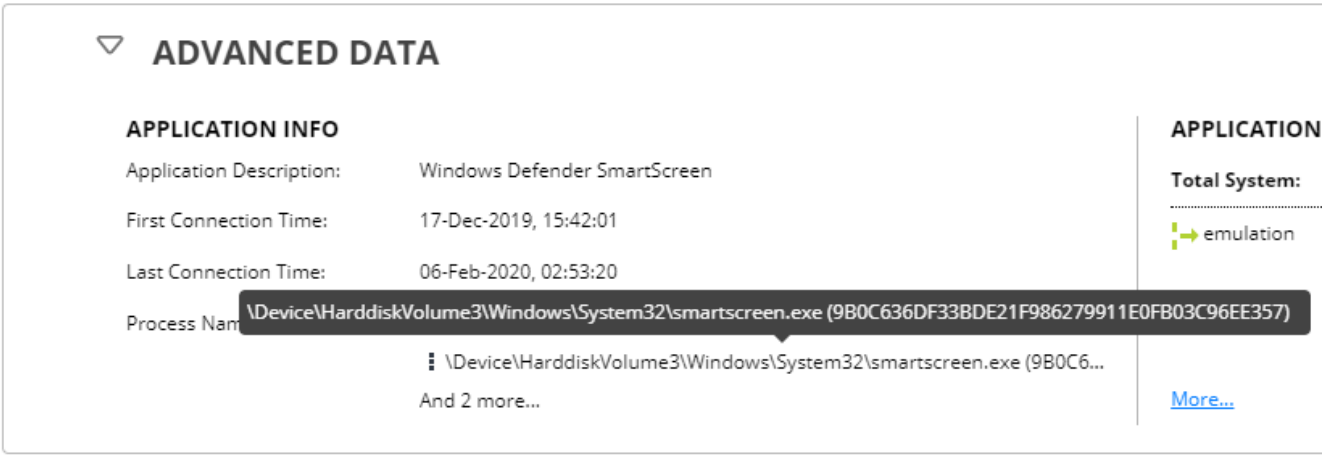
- Application information on page 657
- Application Usage on page 658
- Destinations on page 659

Application information

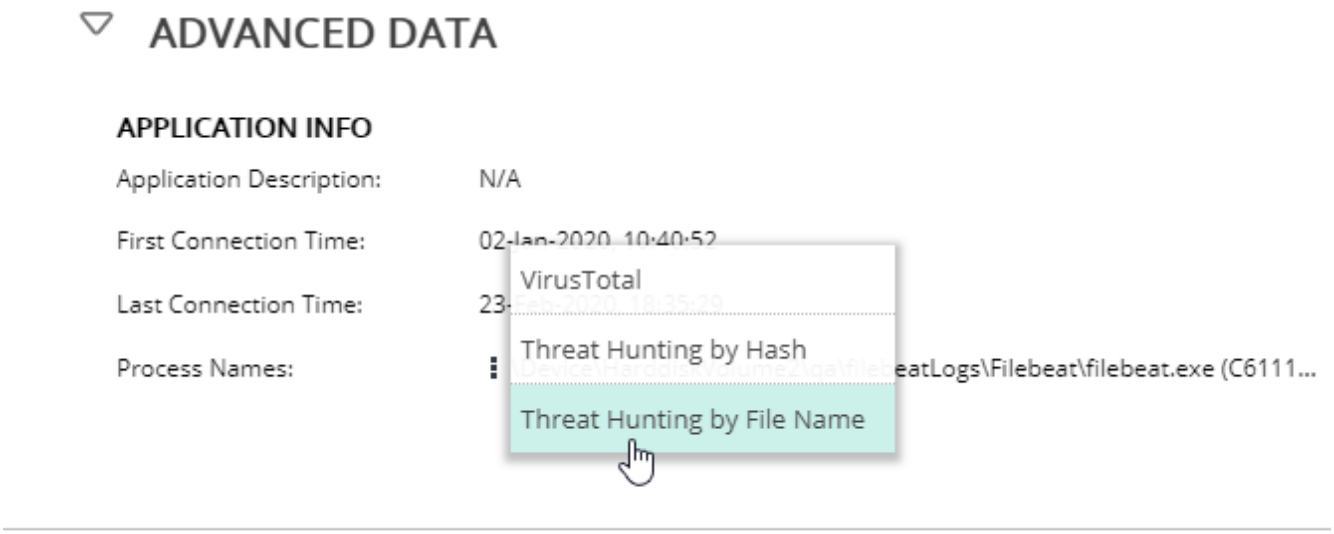
The *APPLICATION INFO* area displays summary information about the selected application.



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

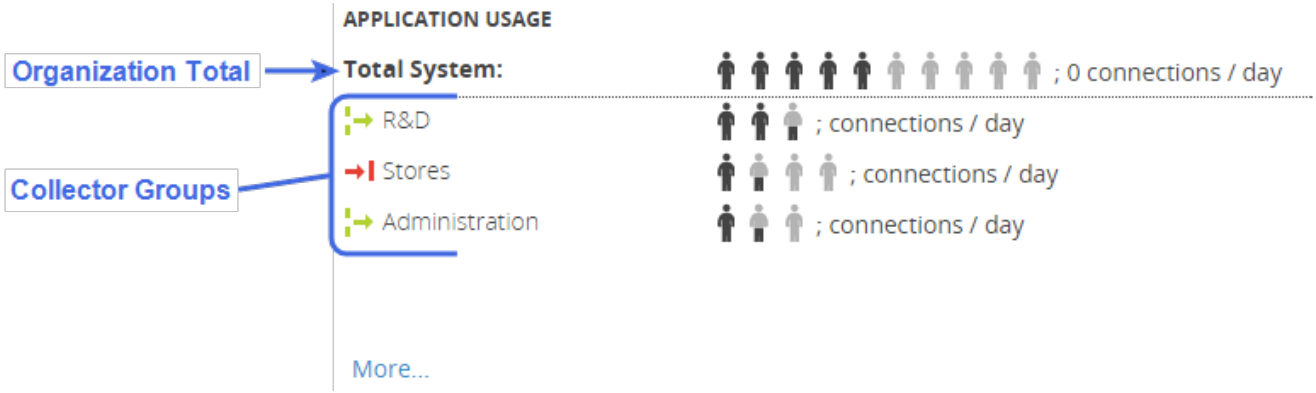


You can click the three dots next to the *Process names* field to navigate to the Threat Hunting window for that process name or hash, or to explore the hash in VirusTotal, as shown below:



Application Usage

The *APPLICATION USAGE* area displays details about usage of the selected application.

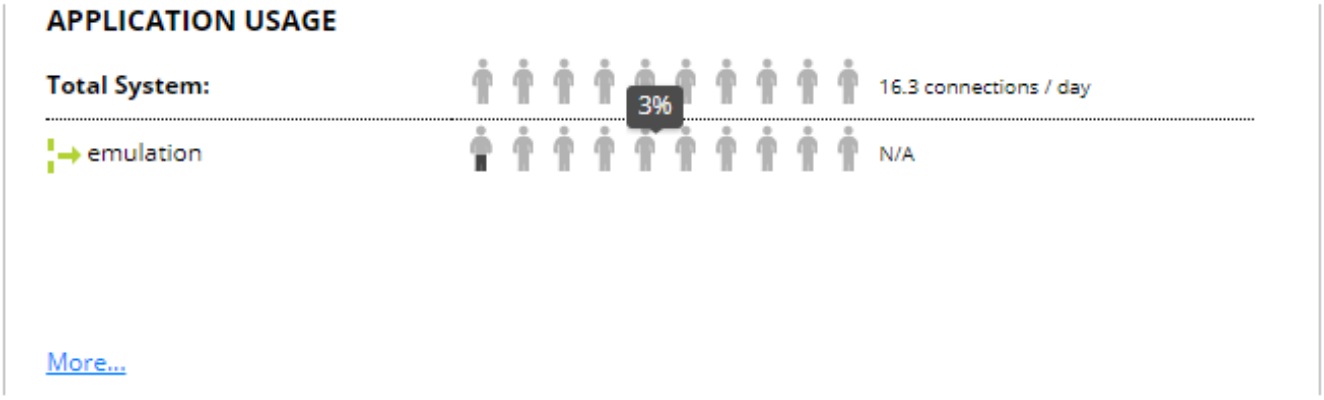


This area shows the number of connections (communication sessions) per day. The top line shows the total number of devices within the organization on which the selected application is installed.

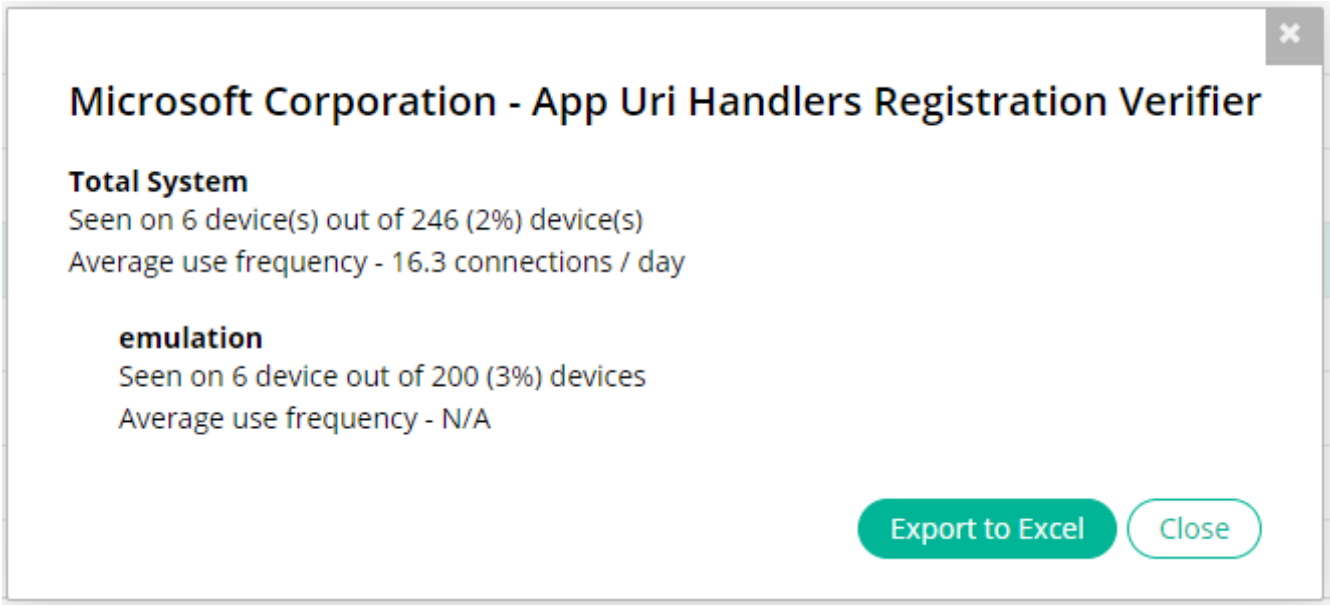
Each row below the underline represents a different Collector Group, and shows the number of devices in the organization in that Collector Group.

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

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



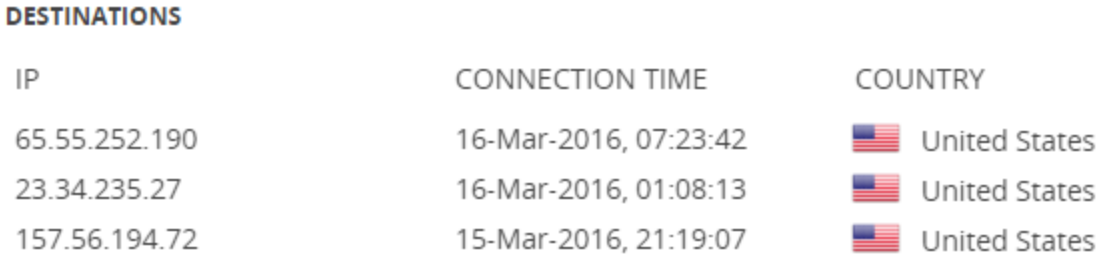
Click the *More* link to open the following window, in which you can view additional details about the selected application.



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

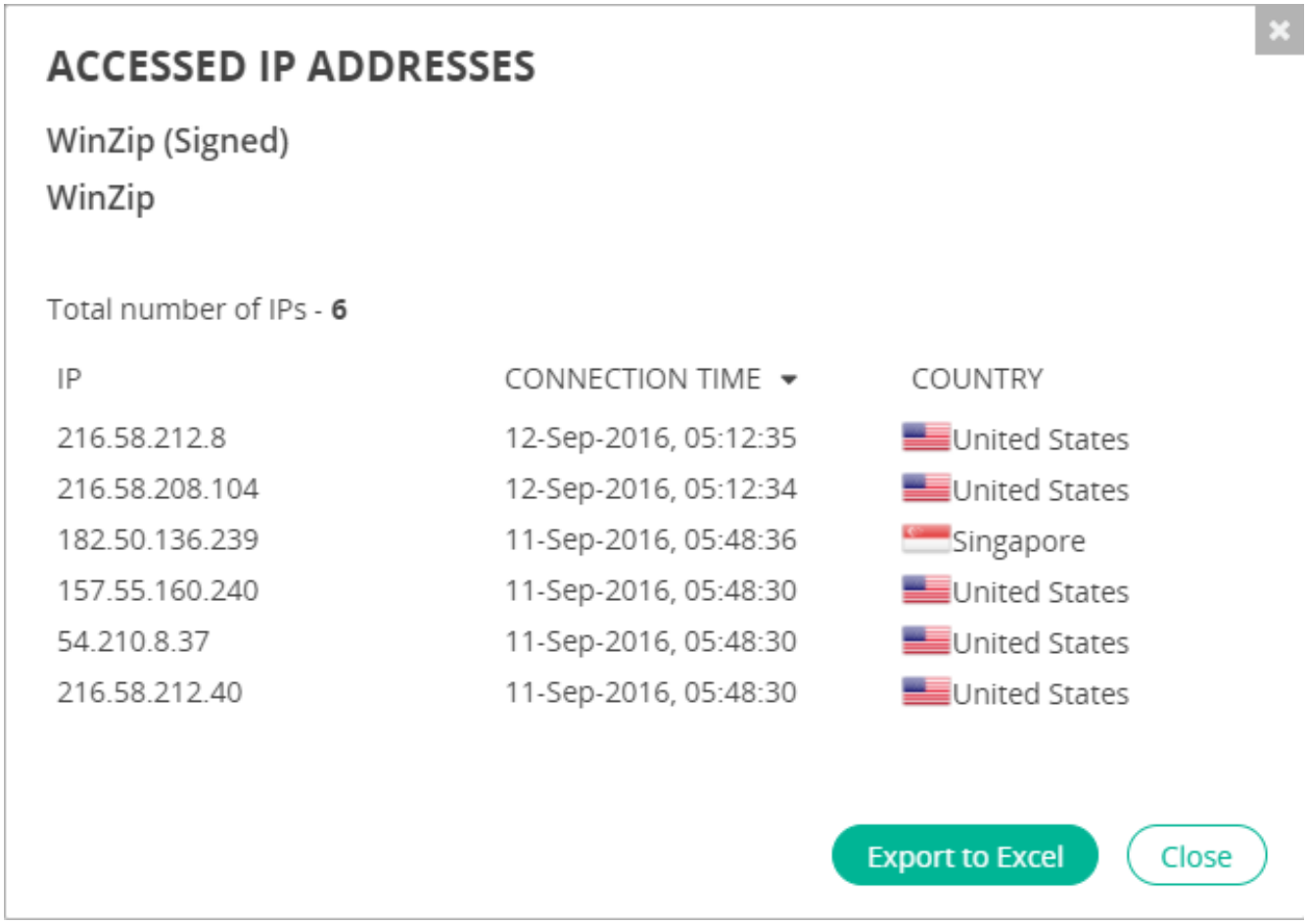
Destinations

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



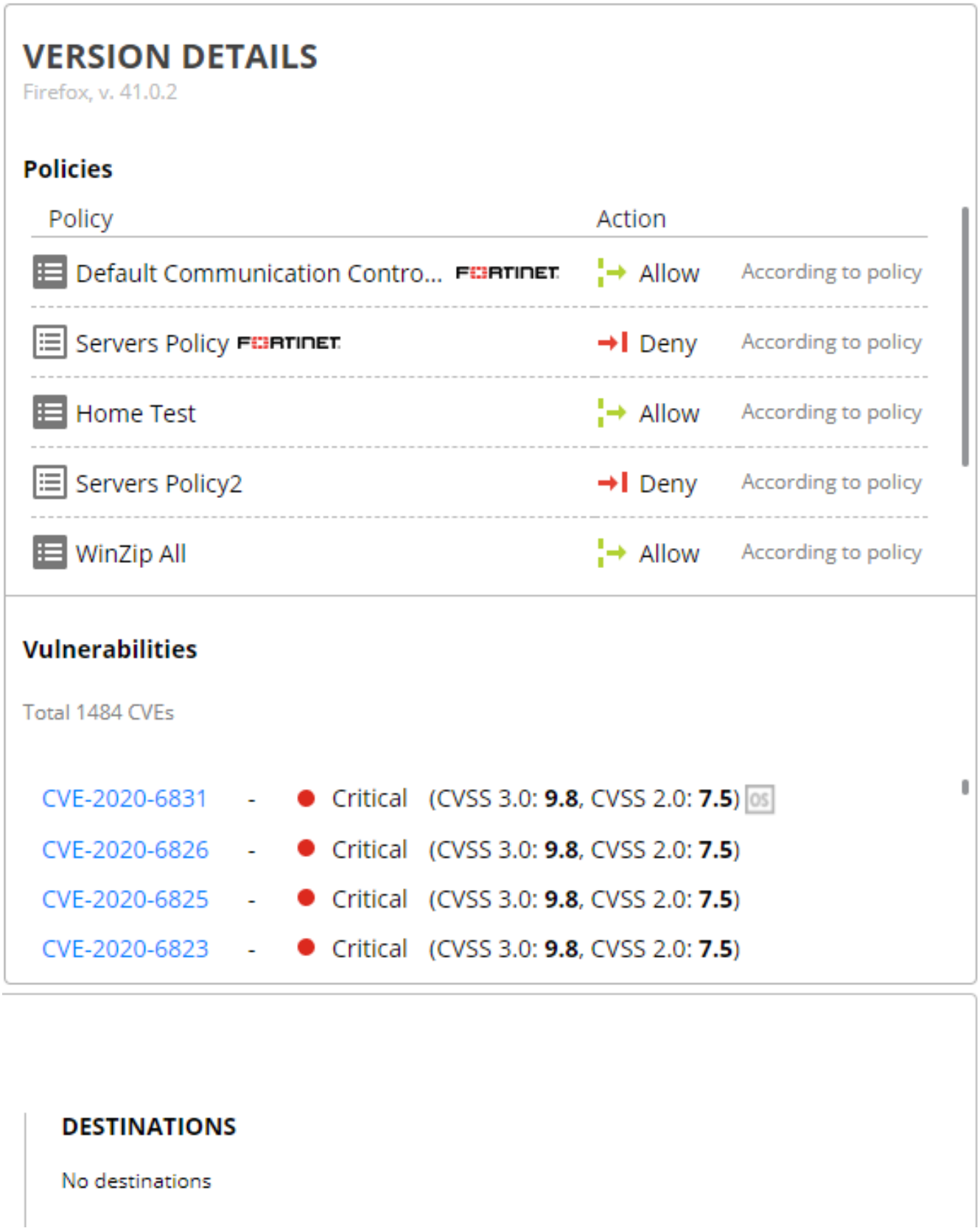
Each row shows the IP address, connection time and country of the destination.

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



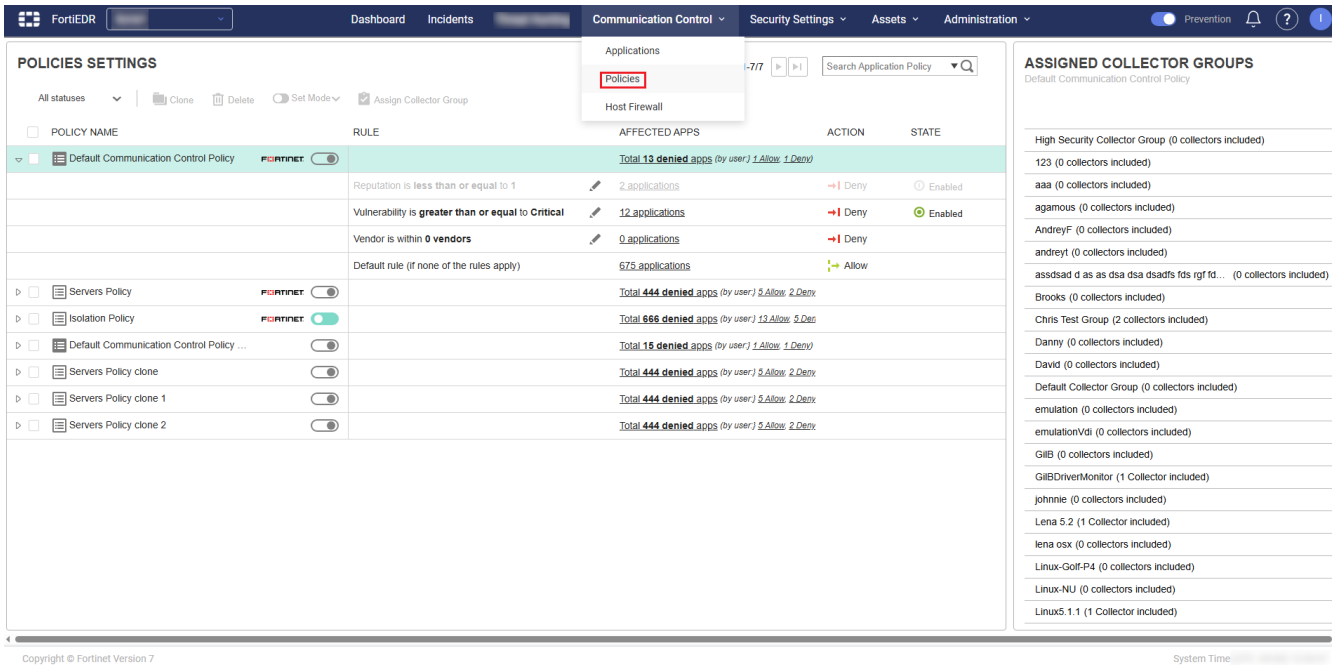
Version Details

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


VERSION DETAILS
Firefox, v. 41.0.2
Policies
Policy
Action
Default Communication Contro...
Allow
According to policy
Servers Policy
Deny
According to policy
Home Test
Allow
According to policy
Servers Policy2
Deny
According to policy
WinZip All
Allow
According to policy
Vulnerabilities
Total 1484 CVEs
CVE-2020-6831 - Critical (CVSS 3.0: 9.8, CVSS 2.0: 7.5)
CVE-2020-6826 - Critical (CVSS 3.0: 9.8, CVSS 2.0: 7.5)
CVE-2020-6825 - Critical (CVSS 3.0: 9.8, CVSS 2.0: 7.5)
CVE-2020-6823 - Critical (CVSS 3.0: 9.8, CVSS 2.0: 7.5)
DESTINATIONS
No destinations

Policies

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

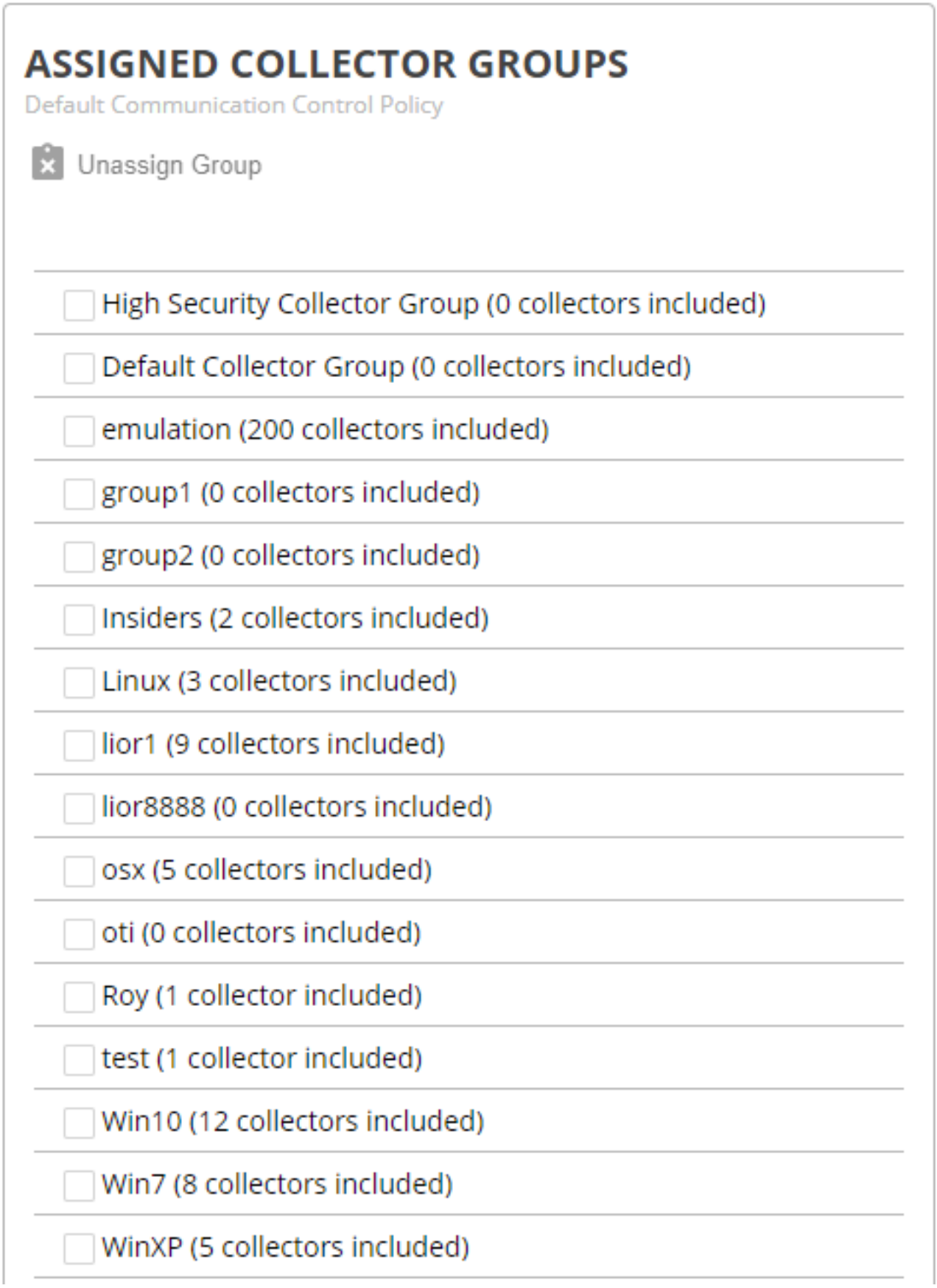


Communication Control policies define the actions to be taken for a given application or application version. Each policy applies to a different Collector Group(s), and all the devices that belong to that Collector Group (s). A Collector Group can only be assigned to one policy.

The following information is defined for each communication policy:

Information Field	Description
Policy Name	The policy name appears in the leftmost column. The policy name is defined when the policy is created.
Rule	The rule as it applies to the policy. The default action for the policy is displayed under the default rule of the policy. For more details, see the Policy rules on page 666.
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

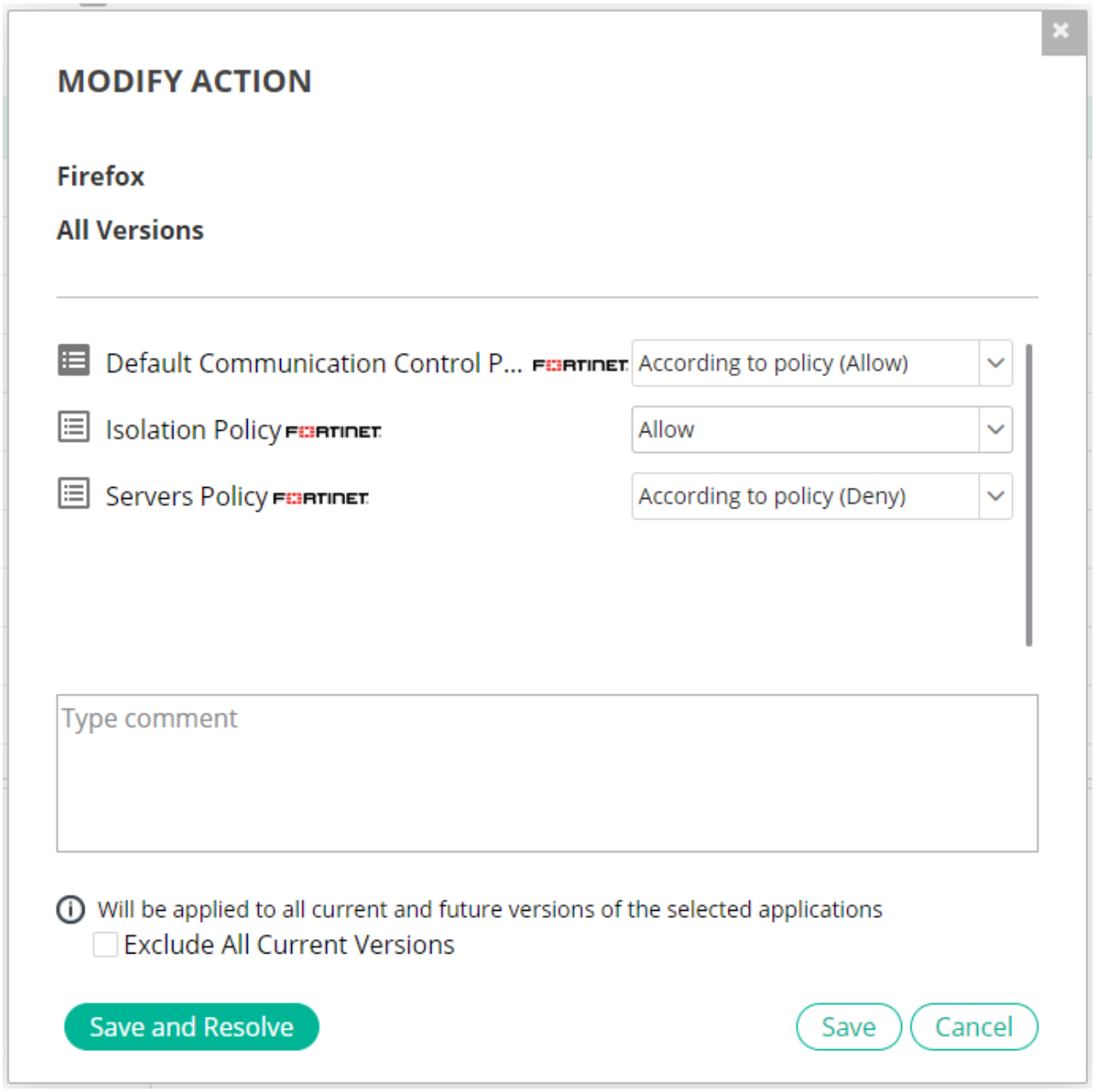
EDR is provided out-of-the-box with several predefined policies, ready for you to get started. These policies are marked with the FORTINET logo.

- The Default Communication Control policy is one such policy, and is always listed first in the list of policies. The Default Communication Control policy is a blocklisting policy that is automatically applied to any Collector Group that is not assigned to any of the other Communication Control policies.
- The *Servers* predefined policy is an allowlist policy that assigns a Deny action to all applications by default, except for a list of known, recognized and legitimate applications, which are allowed. This policy gives your organization a jump-start, as some of the leg work to identify legitimate applications in your organization has already been done for you.
- The Isolation predefined policy isolates (blocks) communication to/from a device. This policy cannot be deleted and only applies in Prevention mode. When this policy is in force and communication for a given device has been blocked, you can manually permit communication to/from the device for a specific application using the procedure below.

To permit communication to/from the device for a specific application:

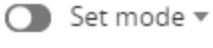
1. Select the *APPLICATIONS* page.
2. Select the application/version to which you want to permit communication.

3. Click the *Modify Action* button. The following displays:



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

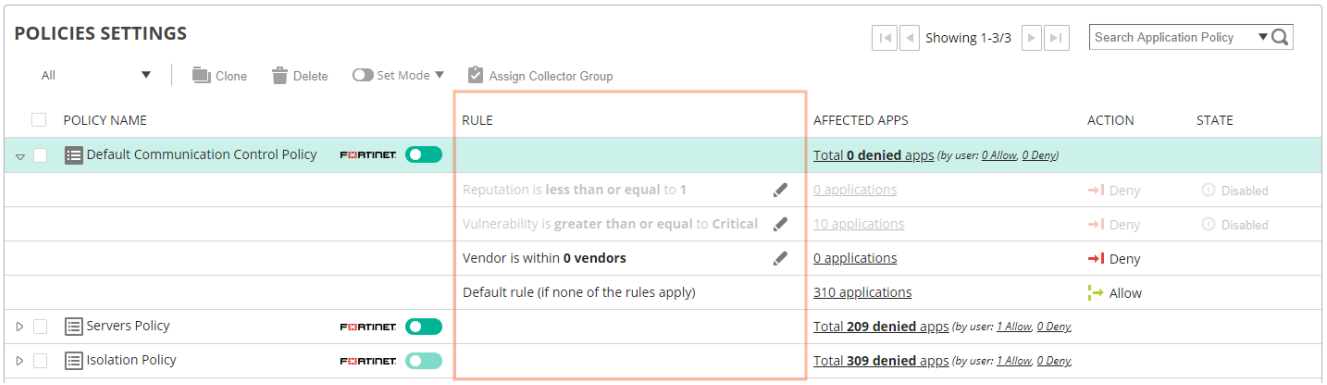
Policy mode

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 Protection or Simulation mode on page 675.

Policy rules

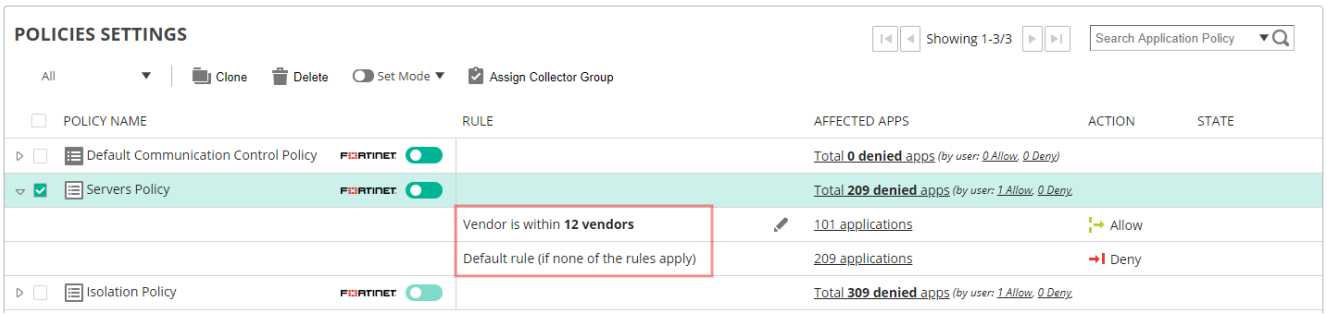
For each communication policy, EDR provides four rules out of the box. These rules can be modified to specify the connections to be blocked/unblocked according to several parameters. EDR provides the following communication policy rules:



Policy Rule	Description
Default rule	This rule applies when none of the other three rules apply.
Reputation is less than or equal to X	This rule enables EDR to block/unblock by reputation score.
Vendor is within X vendors	This rule enables EDR 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 EDR to block/unblock by vulnerability. In the rules, X represents a user-defined value.

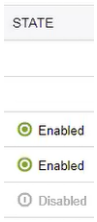
In the rules, **X** represents a user-defined value.

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



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

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

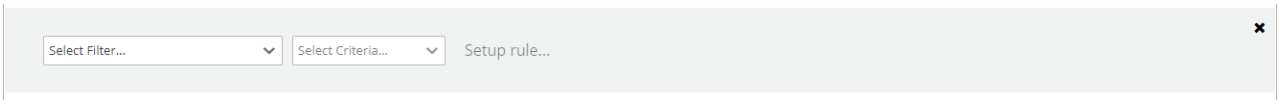


Editing a policy rule

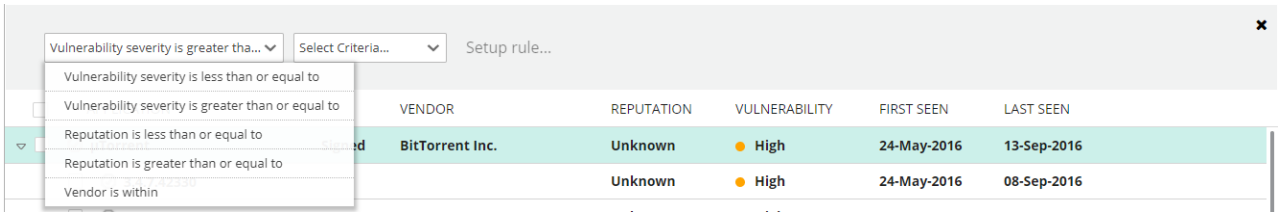
The four rules for a policy can be modified, as needed.

To edit a rule:

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



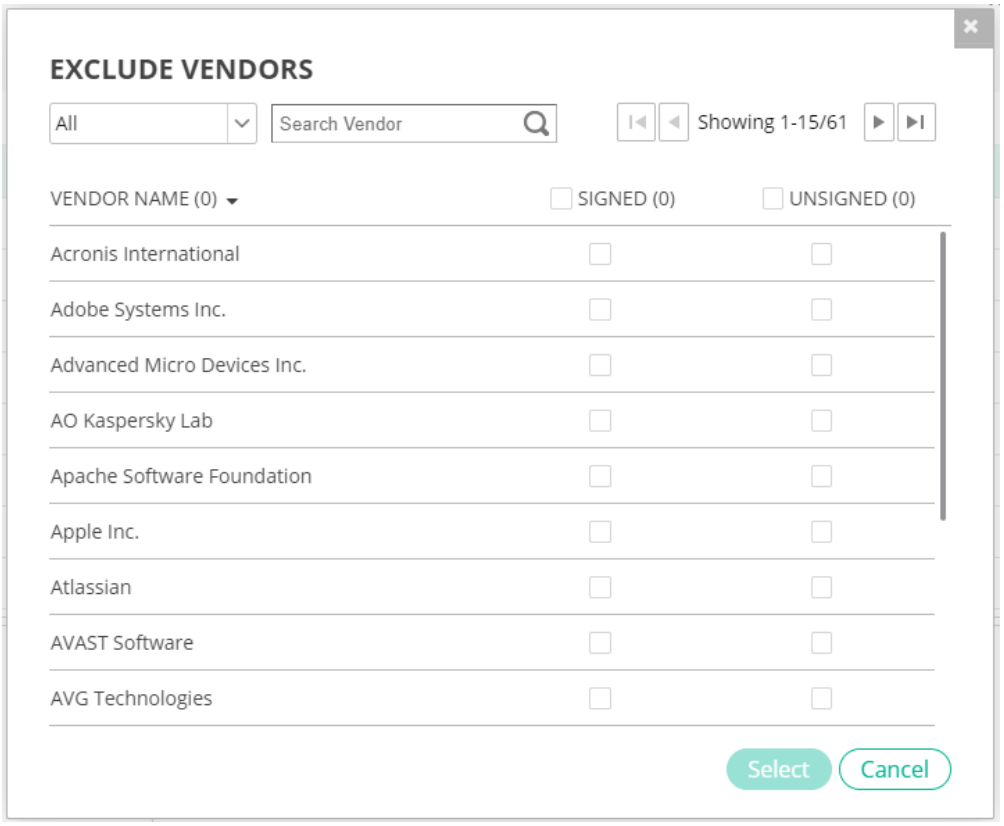
2. In the *Select Filter* dropdown list, select the parameter whose value you want to set in the rule. This dropdown list lists the parameters available to configure for the rule.



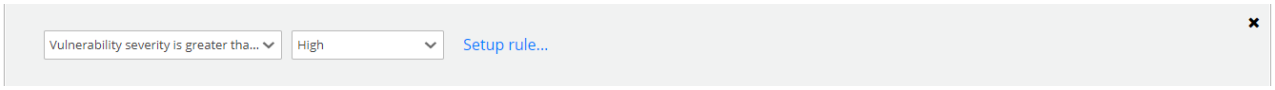
3. In the rightmost *Select Criteria* dropdown list, select the value for the parameter. This dropdown list lists the values available to configure for the parameter specified in step 2.



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



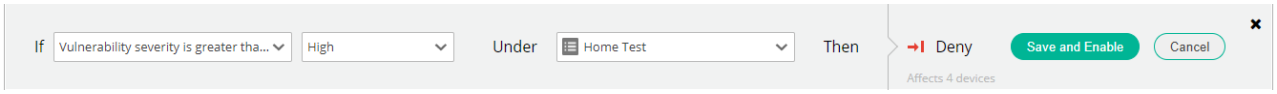
4. Click the *Setup rule* link.



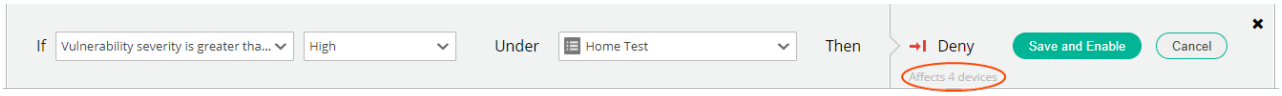
5. In the *Under* dropdown list, select the policy to which this rule applies.



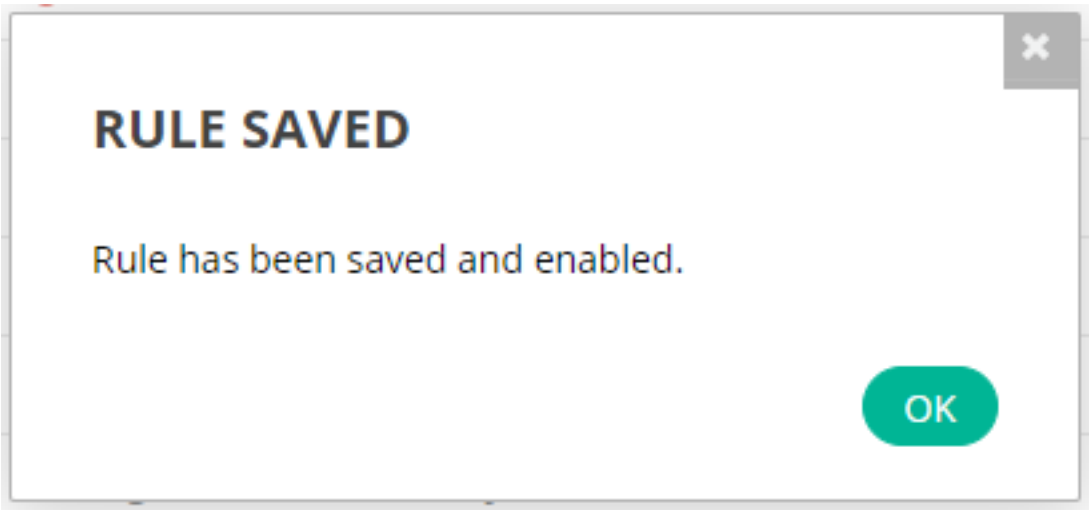
6. In the *Then* field, specify whether to Allow or Deny the application based on this rule.



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



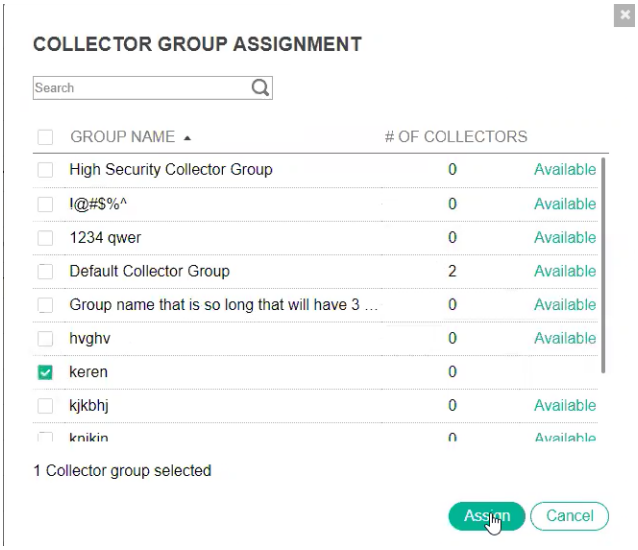
7. Click the *Save and Enable* button to save and enable the changes to the rule. A confirmation window displays, confirming the rule change.



8. Click *OK*.

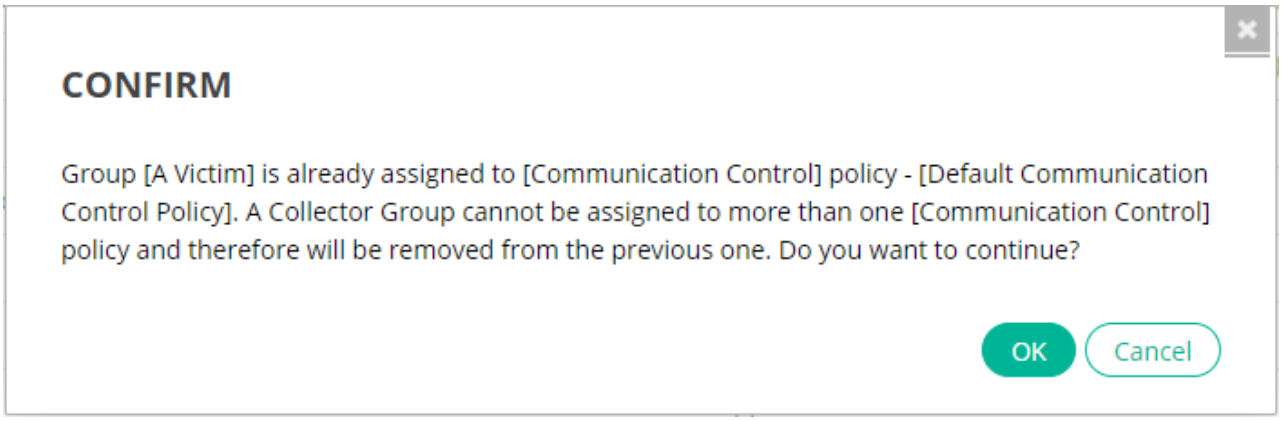
Assigning a policy to a Collector Group

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

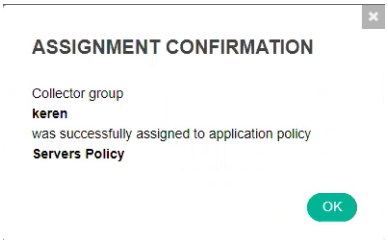


2. Check the checkbox of the Collector Group you want to assign to the policy.

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



4. Click *OK*. The following displays:



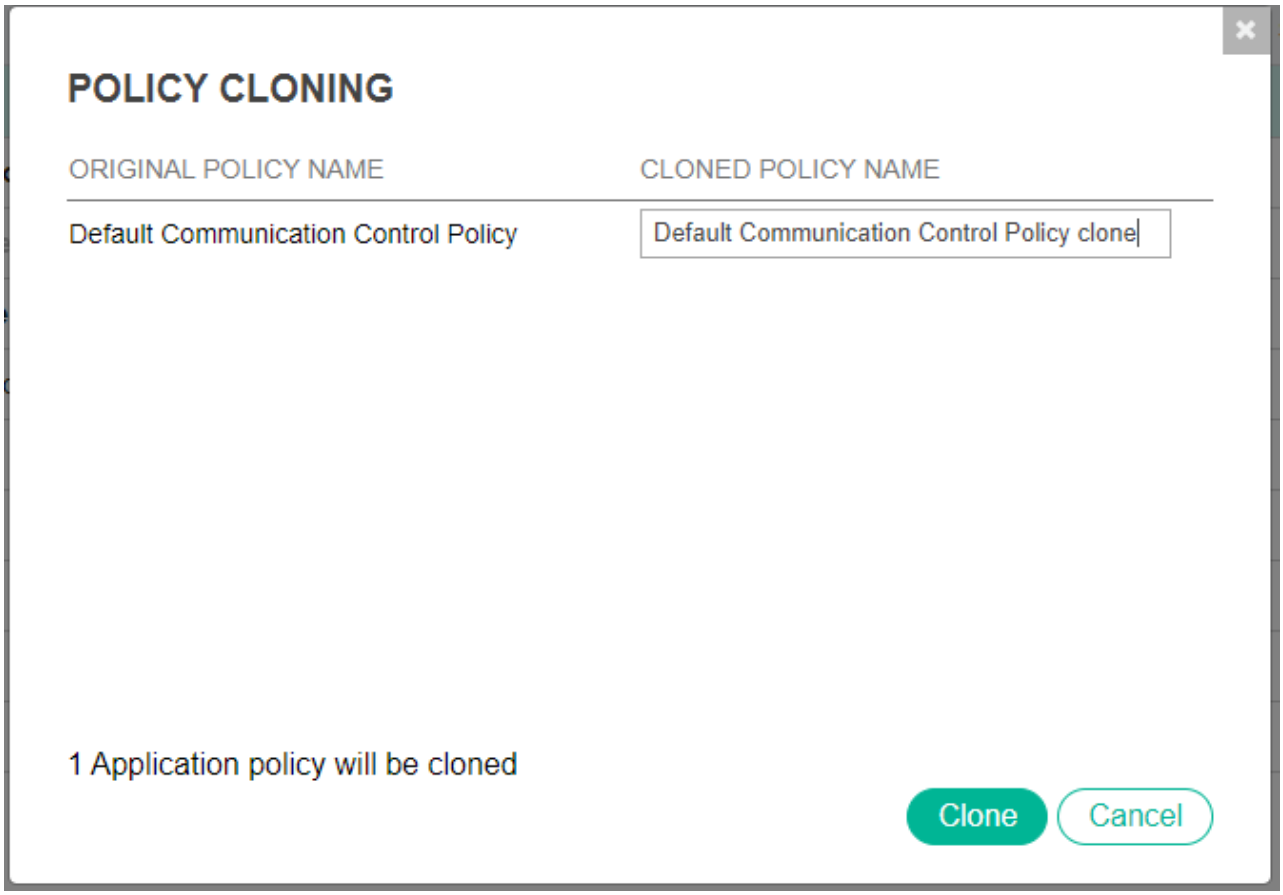
5. Click *OK*.

Creating a new Communication Control policy

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

1. In the policy list, check the policy that you want to clone. There are two types of Communication Control policies: blocklisting policies ( ), such as the Default communication control policy, which allows any connection by default, and allowlisting policies ( ), such as the Servers policy, which denies any connection by default.

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



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

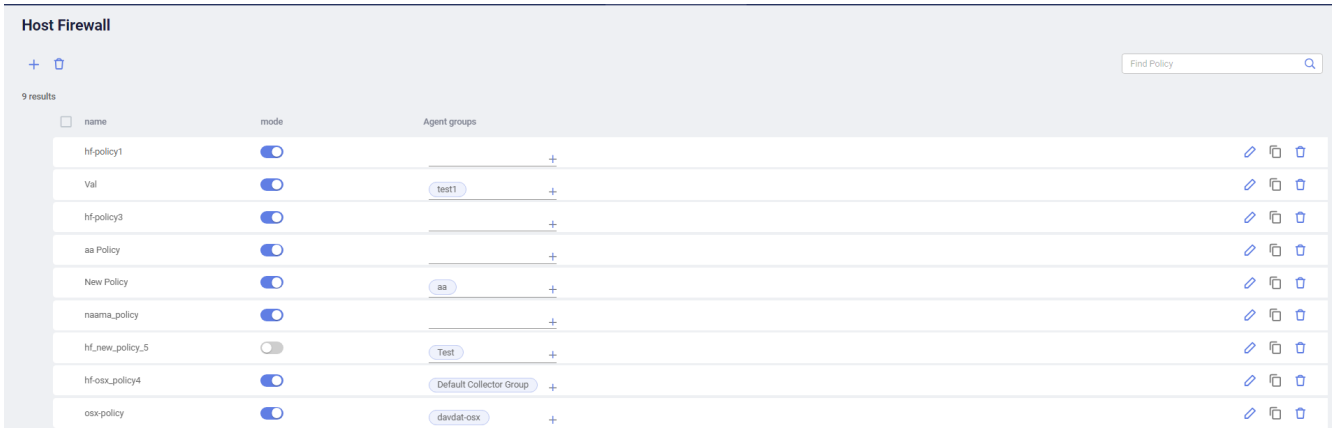
Other options in the Policies pane

Option	Description
All	Click the down arrow in the All button and then select an option in the dropdown list to filter the policy list accordingly.
Clone	Click this button to clone a policy.
Delete	Click this button to delete a policy. Before deletion, a confirmation message displays, prompting you to confirm the deletion of the policy.
Set mode	Click the down arrow in the Set mode button and then select the mode for the policy, as described in Policy mode on page 665

Host Firewall

Use the *Communications Control > Host Firewall* page to configure host firewall policies to control incoming and outgoing network traffic to protect endpoints against unwanted connections based on remote addresses, protocols, or applications in use to reflect the organization's network policies. Host firewall policies reduce the attack surface by protecting the host while working outside the enterprise network (public Internet, home, or other networks).

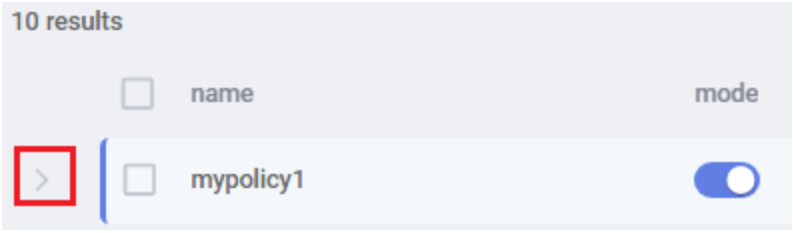




To configure a host firewall policy:

1. In the *Communications Control > Host Firewall* page, click the *Add* button at the top left corner.
2. Specify a name for the host firewall policy.
3. Select the Collector groups that the host firewall policy applies to.
4. Click *Save* to save the host firewall policy.
   The host firewall policy appears in the list.
5. **(Optional)** Add or remove Collector groups for the host firewall policy in the *Collector group* column.
6. Define rules to associate with the host firewall policy:

a. Expand the row of the host firewall policy in the table.



b. Click the *Add* button under the host firewall policy.
c. Enable the rule if you want to enforce the rule immediately after creation. You can also choose to enable it later.
d. Specify a name for the rule.
e. Specify the application name or IP address and port combination that the rule applies to.
   The IP address and port can be single or a range, including wildcard. For example, 192.168.0.1 or 192.168.0.1-192.168.0.100.
f. Select the protocol, which can be TCP, UDP, or any.
g. In the *Process* field, specify an application name to apply the rule to one specific application or use the default *Any*, which means the rule applies to all applications.
h. In the *Action* dropdown, select whether to allow or deny matching connections.
   The action applies to both incoming and outgoing traffic.
i. **(Optional)** Add a description for the rule.
j. Click *Save* to save the rule.
   The rule appears under the host firewall policy in the table.
k. Add more rules by repeating the steps above as needed.
l. When more than one rule exists, drag and drop the rules in the order of priority. When the criteria of multiple groups are met, the first matching rule will be used.

7. Enable or disable the host firewall policy or a specific rule using the mode button.
8. To log connections blocked by a Collector, check the *Firewall Block* action in the Collector's assigned Threat Hunting Collection profiles on page 723.



Host firewall policies work side by side with existing Communication Control policies. In case of contradictions, EDR applies the more restrictive out of the two. For example, if a group is assigned to a host firewall policy that allows any connection to a specific remote address but the Communication Control policy assigned to the group restricts connections to low reputation applications, connections to the remote address will be blocked if the connection goes to low reputation applications.

Profiles

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

Security policies

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

To access the EDR *Security Policies* page, click the down arrow next to *Profiles* > *Security* > *Policies*.

Out-of-the-box policies

EDR provides the following out-of-the-box policies. Each policy comes with multiple highly intelligent rules that enforce it.

- *Application Control*: This policy enables EDR to block user-defined applications from running, so that they do not launch. Blocklist management is done on the Application Control on page 701 page.

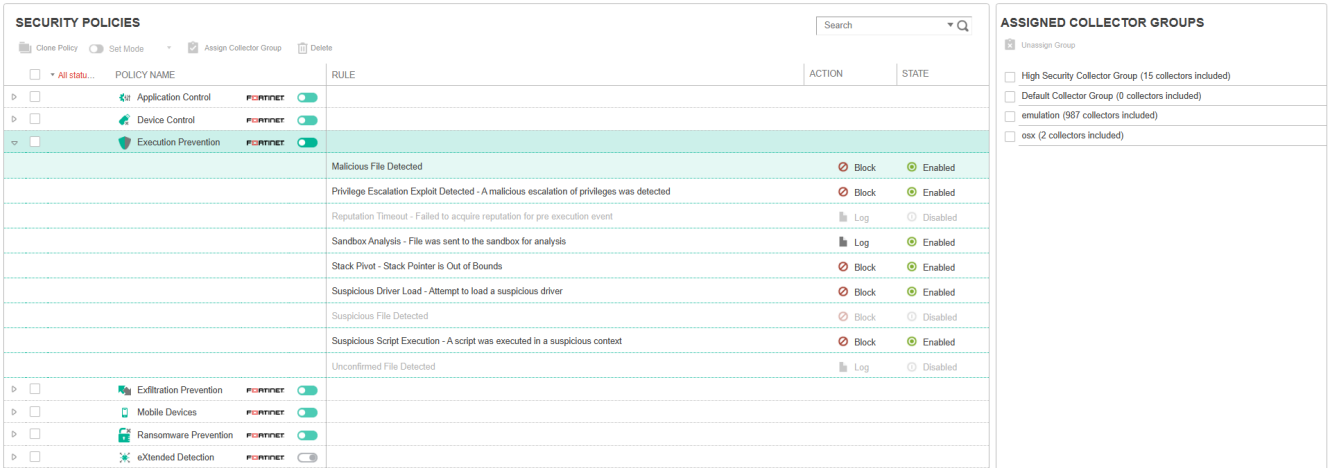
  

  Application Control security events are displayed under dedicated *Application Control* filter in the *Incidents* page and are not listed as part of the *All* filter.

- *Device Control*: This policy enables EDR to detect and block the usage of USB devices, such as USB mass storage devices. In this policy, detection is based on the device type.
- *Execution Prevention*: This policy blocks the execution of files that are identified as malicious or suspected to be malicious. For this policy, each file is analyzed to find evidence for malicious activity. One of the following rules is triggered, based on the analysis result:
  - *Most Likely a Malicious File*: A Malicious File Execution rule is triggered with a critical severity. By default, the file is blocked.
  - *Probably a Malicious File*: A Suspicious File Execution rule is triggered with a high severity. By default, the file is blocked.
  - *Show Evidence of Malicious File*: An Unresolved file rule is triggered with a medium severity. By default, the file is logged, but is not blocked.
- *Exfiltration Prevention*: This policy enables EDR to distinguish which connection establishment requests are malicious ones.
- *Mobile Devices*: This policy enables EDR to detect and prevent access to malicious URL and IP addresses from the mobile devices.
- *Ransomware Prevention*: This policy enables EDR to detect and block malware that prevents or limits users from accessing their own system.
- *eXtended Detection Policy*: This policy provides visibility into data across multiple security systems and identifies abnormal or malicious activity by applying analytics and correlating data from various systems. Events are logged and displayed in the *Incidents* tab. No blocking options are provided. The exceptions options are not available in the *Incidents* tab for security events triggered by this policy.

  This policy requires that you configure an XDR source connector in the *Profiles* > *Integrations* > *Connectors* section.



All security policies can run simultaneously. However, these security policies detect rule violations at different places and points in time in the operating system. When multiple security policies are triggered, EDR uses the following guidelines to avoid generating duplicate security events:

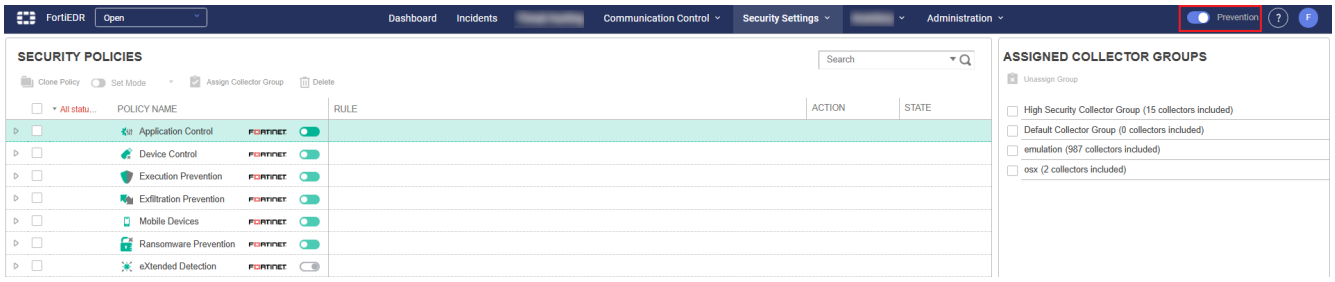
- For connection establishment attempts, the Exfiltration Prevention rule violation is detected.
- For attempts to lock files or access their data (for example, by encrypting the data), the Ransomware rule violation is detected.
- When a malicious file is being executed by the user or by the operation system, the Execution Prevention rule violation is detected.
- For attempts to use a USB device, such as a mass storage device, the Device Control rule violation is detected. It is supported on Windows devices only.
- For execution attempts of an application that is included in the blocklist, the Application Control rule violation is detected.
- When malicious activity is identified across network, endpoints, and cloud, an Extended Detection rule violation is detected.

Protection or Simulation mode

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

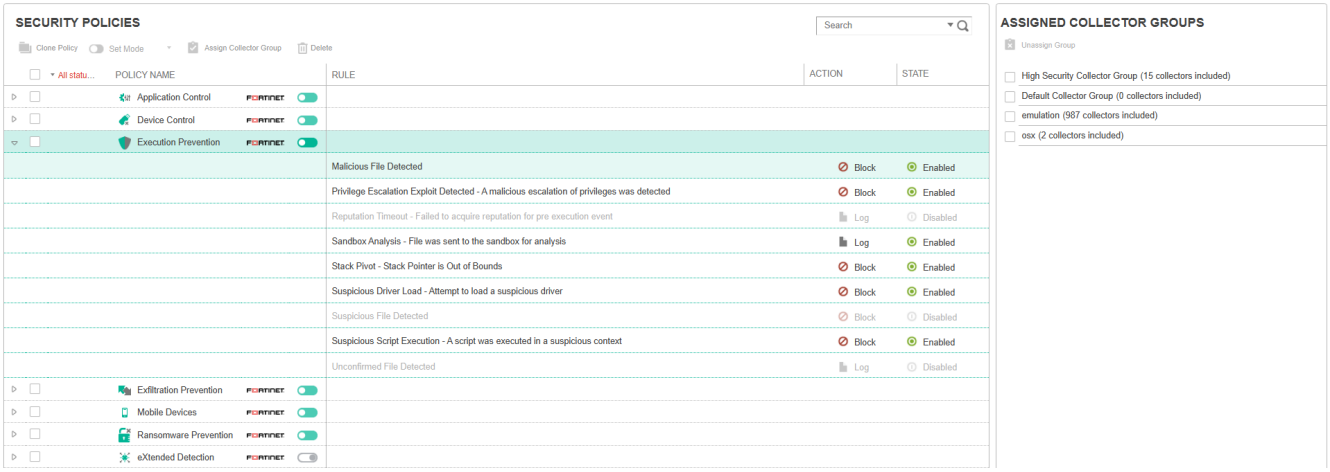
- *Protection:* EDR enforces its active exfiltration prevention policy that blocks all connections that violate the relevant EDR security policy rules.
- *Simulation (Notification Only):* EDR *only* issues an alert (described below) for all connections that violate any rule in the EDR security policy. In this mode, EDR does not block exfiltration. EDR comes out-of-the-box set to this mode.

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



Security Policies page

The *Profiles* > *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.



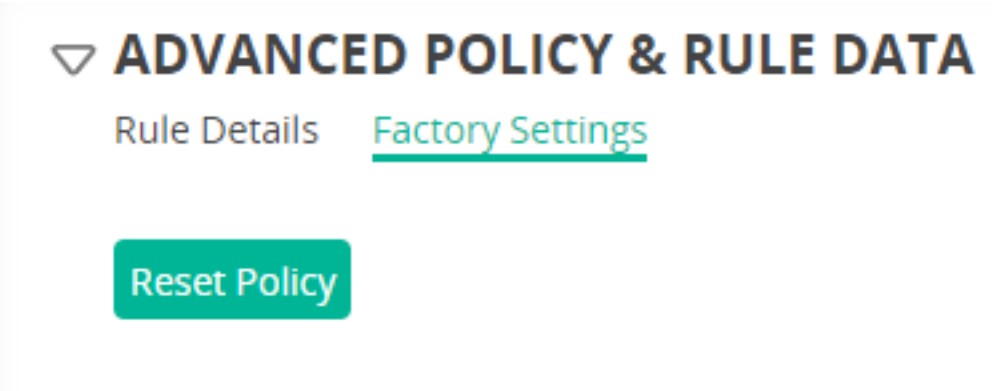
EDR is provided out-of-the-box with several predefined security policies, ready for you to get started. By default, all policies are set to Simulation mode (meaning that they only log and do not block) and show the FORTINET logo. This page also enables you to define additional policies. See Out-of-the-box policies on page 674 for more details.

Security Policy	Icon
Application Control Policies	
Device Control Policies	
Execution Prevention	
Exfiltration Prevention	
Mobile Devices	
Ransomware Prevention	
Extended Detection	

The following information is defined per security policy:

Information Field	Description
Policy Name	The policy name appears in the left most column. The policy name is defined when the policy is created. The name of the *Default Policy* cannot be changed.
Rule Name	EDR's proprietary rules come predefined and are the primary component of EDR's proprietary security solution. This column displays a short description for the purpose of this rule. You can expand the *ADVANCED POLICY & RULES DATA* area at the bottom left of the window to display a more detailed description of what the rule does and how it works.
Action	Specifies the action that is enforced when this rule is violated. You can change this field, as follows: • *Block* Block: When this policy is set to *Prevention* mode (Setting a security policy's Prevention or Simulation mode on page 678), 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 EDR ***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. EDR's rules have been created as a result of extensive expertise and experience. Therefore, we do not recommend disabling any of them.

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



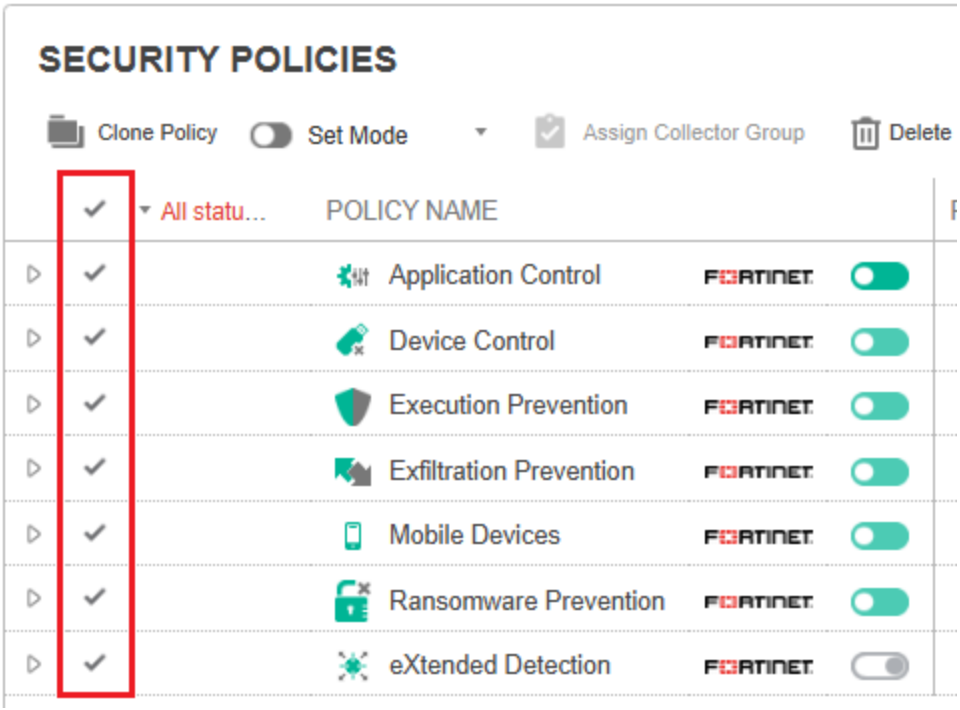
Setting a security policy's Prevention or Simulation mode

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

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

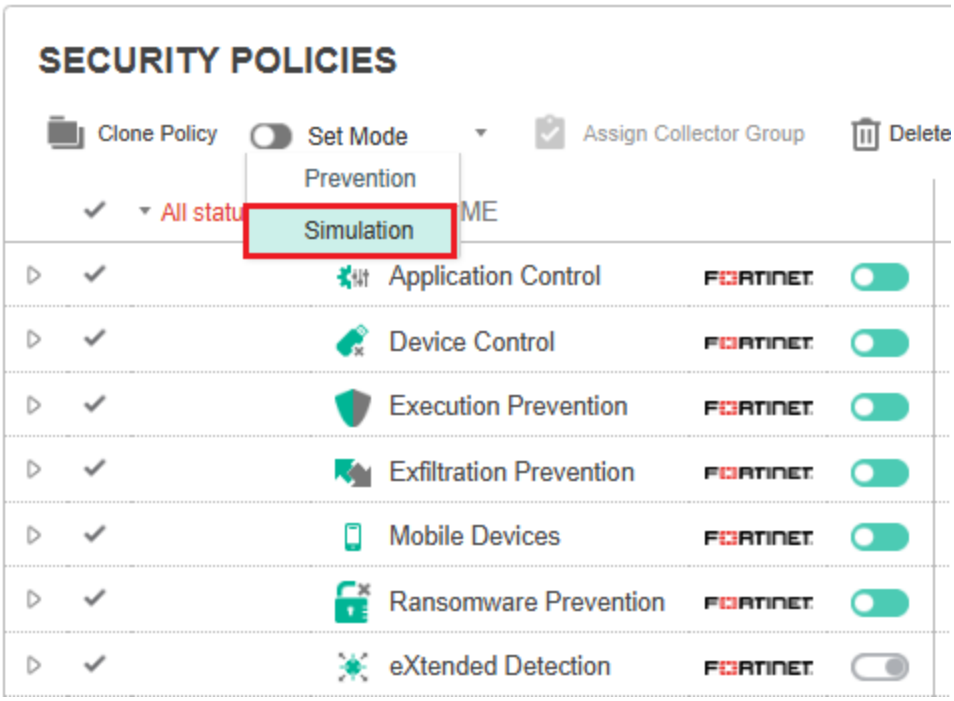
To set a security policy to Prevention or Simulation mode:

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



2. You can now either:
   a. Set mode : Click *Set Mode* and select either *Prevention* or *Simulation*, as shown above.
   b. : Move the slider to the left for Prevention or to the right for Simulation.

You can also set all EDR policies to Simulation mode at once by moving the slider at the top-left corner to Simulation, as shown below:

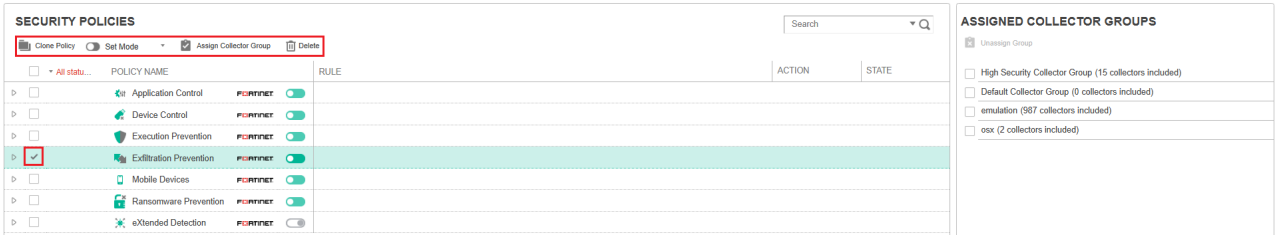


Creating a new security policy

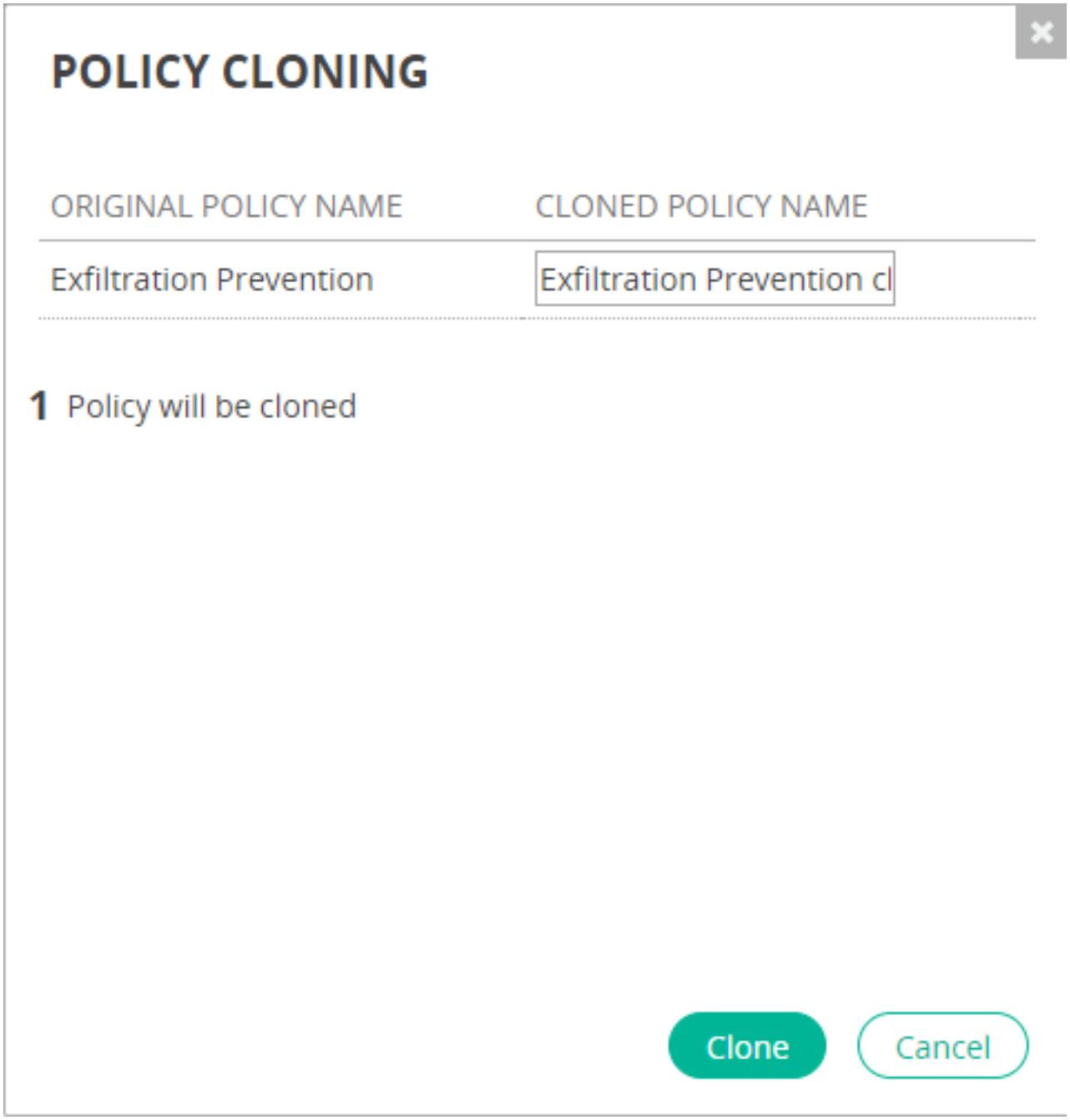
A new security policy can be created by cloning an existing policy, as described below. New security policies are only needed if you are going to assign different policies to different Collector Groups. Otherwise, you can simply modify one of the default policies that are provided out-of-the-box and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

To create a new security policy:

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



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



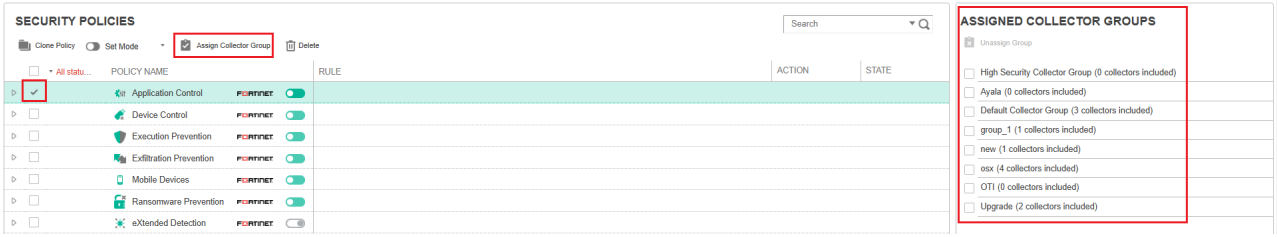
3. Specify the name of the new security policy and click the *Clone* button.
4. If needed, assign the security policy to the required Collector Group so that it protects all the EDR Collectors in that group, as described in Assigning a security policy to a Collector Group on page 681.

Assigning a security policy to a Collector Group

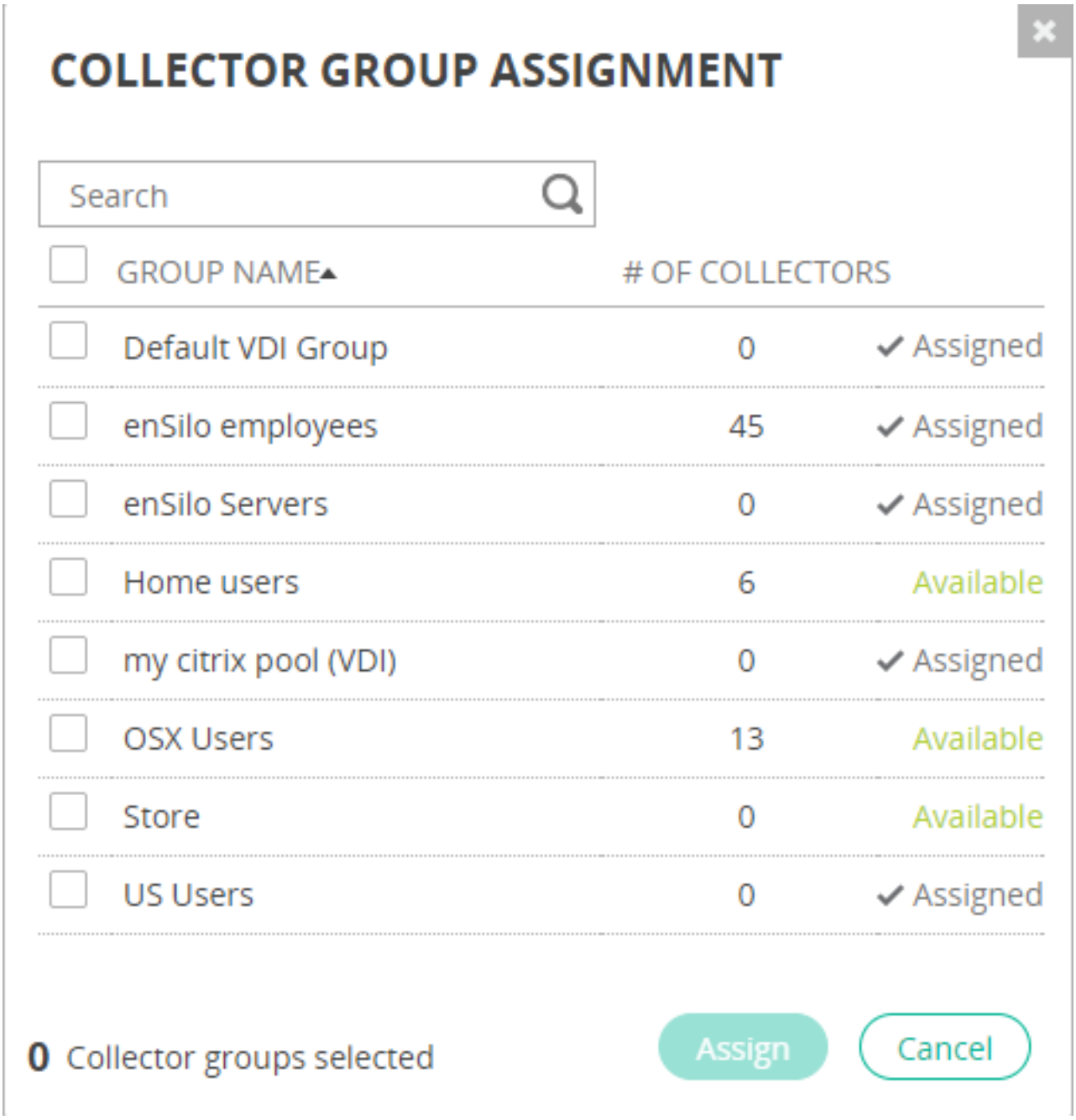
By default, a security policy protects the EDR Collectors that belong to that Collector Group. A security policy can be assigned to more than one Collector Group. Multiple security policies can be assigned to each Collector Group.

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.

1. In the *SECURITY POLICIES* page, select the name of the security policy to be assigned by clicking its checkbox. The right side of the window displays the Collector Groups to which this policy is assigned.



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



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

Deleting a security policy

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

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

Exception Manager

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

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

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

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

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

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

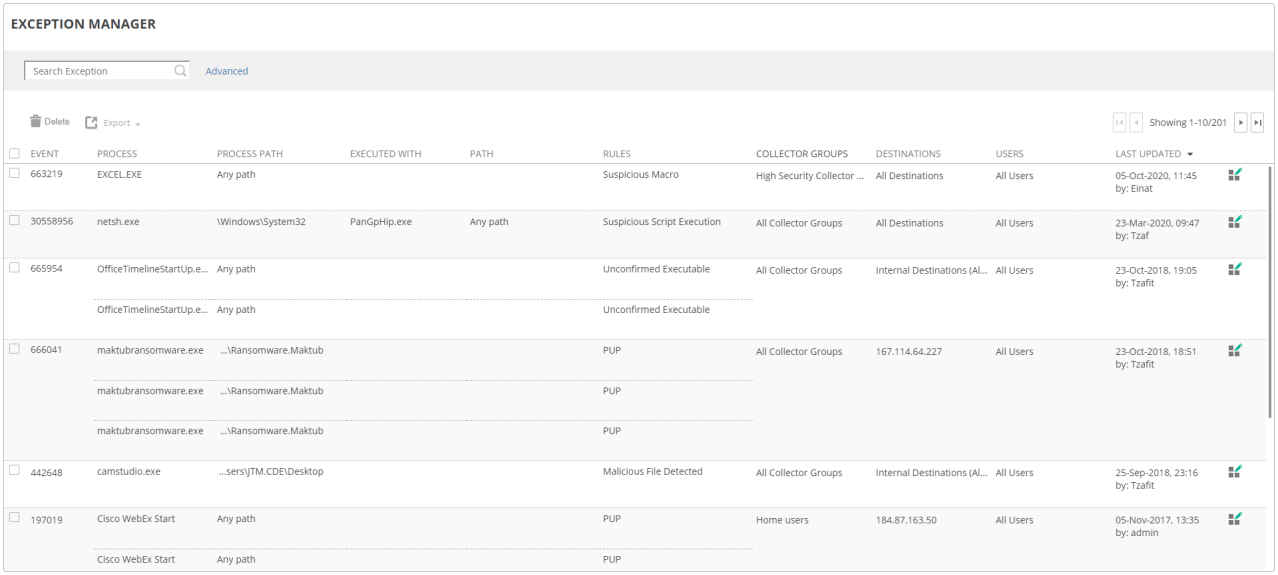
Any exception that you define applies to all policies.

Exceptions are created in the *Incidents* tab, as described onDefining security event exceptions on page 600

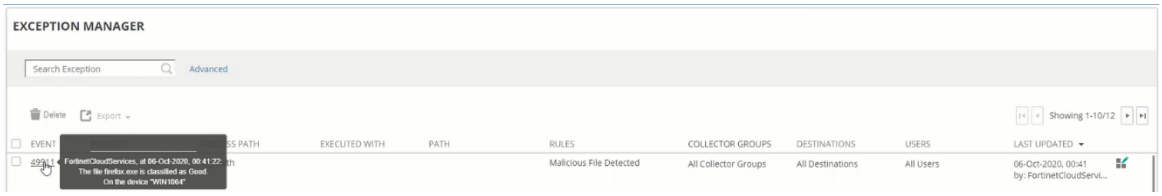
Fortinet Cloud Services (FCS) may push an automated exception in cases where extended analysis and investigation of a security event leads to its reclassification as Safe. This prevents the security event from triggering again. In such cases, the security event is moved under handled events and the exception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

To manage exceptions:

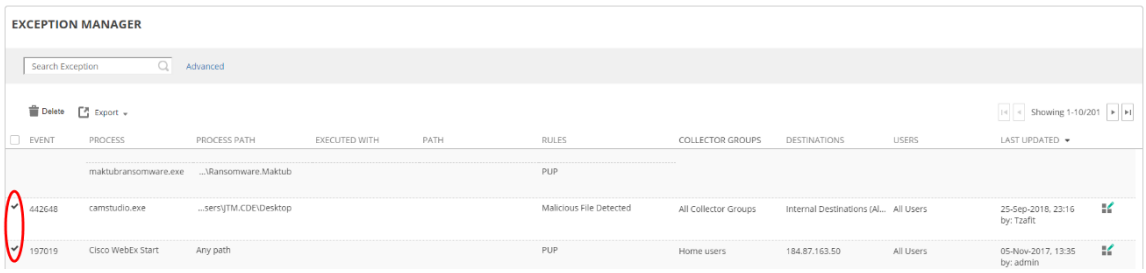
1. Select *SECURITY SETTINGS* > *Security Events* > *Exception Manager*. Alternatively, in the *Incidents* tab, click the *Exception Manager* button. The following window displays, showing the list of previously created exceptions:



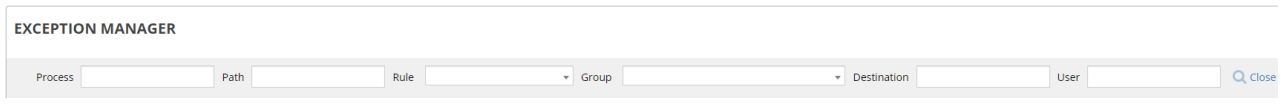
If the exception includes a free-text comment, you can hover over the Event ID in the Exception Manager to display it.



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



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

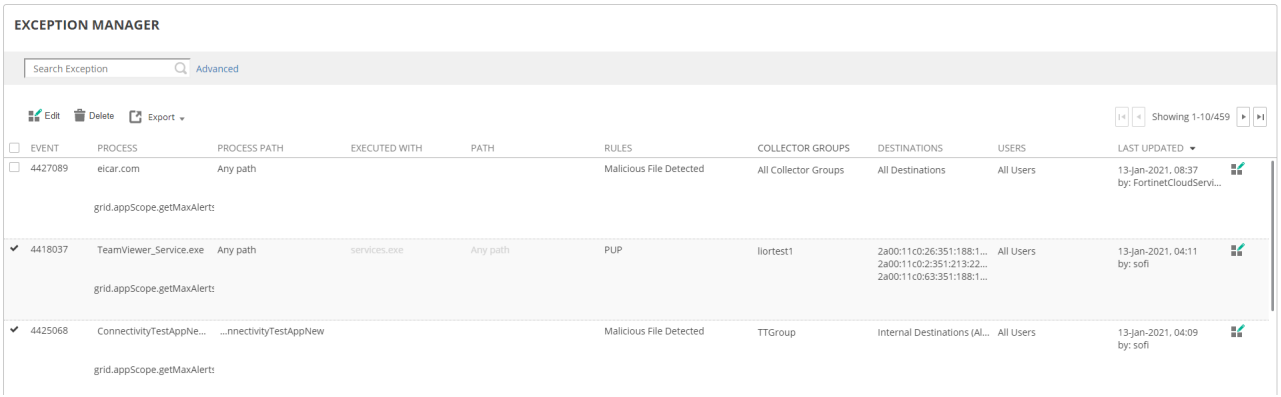


Click the *Basic search* button to access the standard search options.

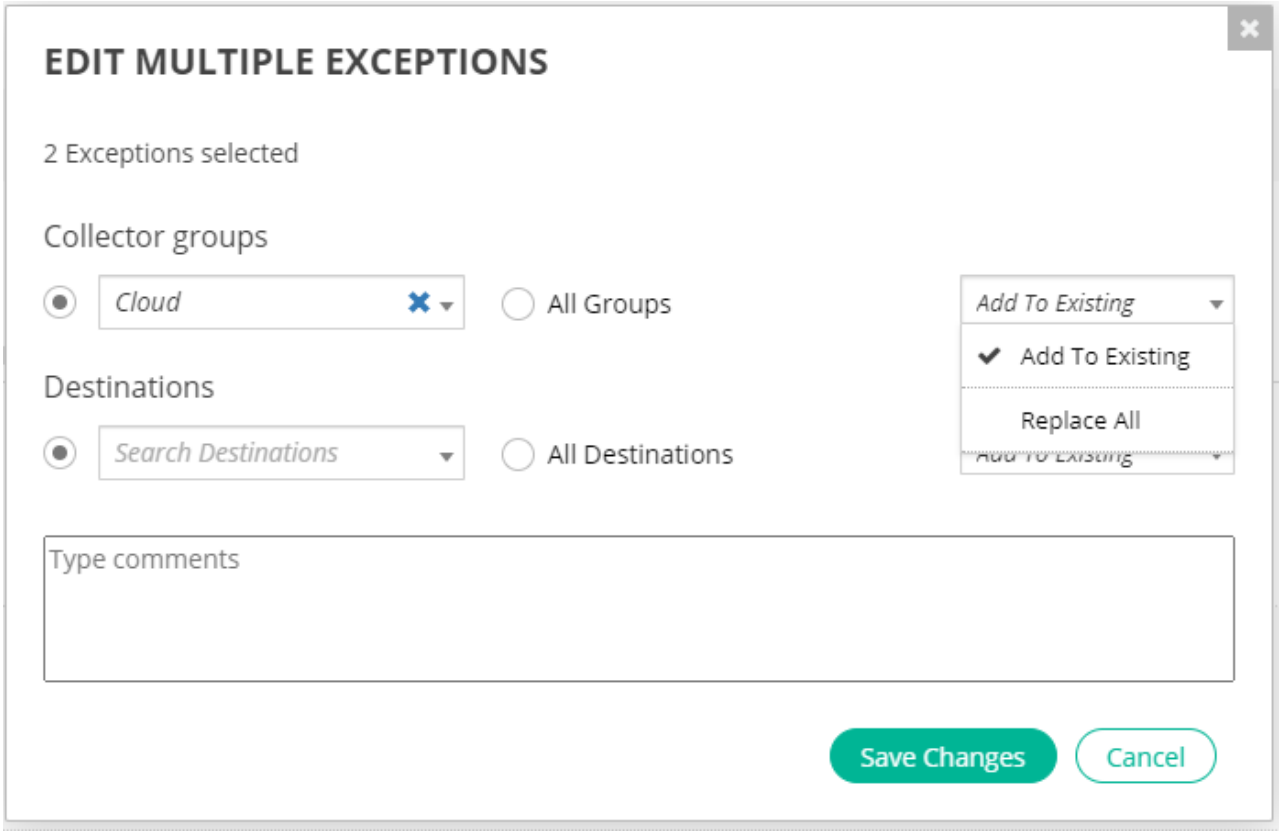
Click the *Edit Exception* button in an exception row to edit that exception. For more details, see Editing Security Event Exceptions on Editing Security Event Exceptions.

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:



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:



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

Exclusion Manager

The Exclusion Manager enables you to define which processes, files, or domains are excluded from Security Policies monitoring. Three types of exclusions can be defined in the Exclusion Manager:

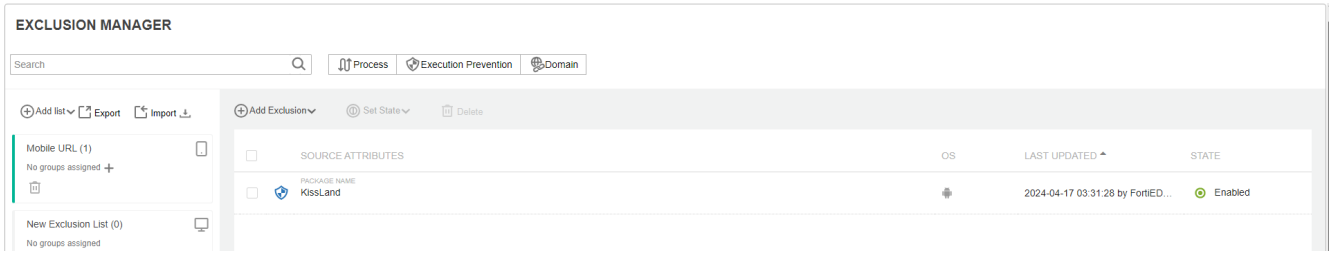
- **(PC only) Process Exclusions**: This type of exclusion specifies that EDR does not inspect the actions that are performed by specific processes, so that these processes do not trigger security events. The processes that are excluded are identified by the attributes of the processes, according to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

  There may be various reasons for excluding a process in this manner. For example, when a process's performance/functionality is affected by EDR's inspection, but the customer knows that this process is good/safe (this example is relevant, even when the process does not trigger security events). Therefore, in this case, the exclusion will specify that EDR no longer inspects the specified processes.

  Please note that adding this type of exclusion excludes this process from being monitored by all EDR features and all activities of this process are ignored.
- **Execution Prevention Exclusions**: The Execution Prevention policy inspects/scans files and then blocks their execution if they are identified as malicious or suspected to be malicious. Execution Prevention Exclusions specify that EDR does not apply the Execution Prevention policy inspection, which analyzes files in order to find evidence of malicious activity, as described in Profiles on page 673. The files that are excluded are identified by the attributes of the files that are the target of the Execution Prevention actions, according to your definitions.
- **(Mobile only) Domain Exclusions**: The Malicious URL/IP Detected policy inspects/scans URLs/domains and blocks connections to them if they are identified as malicious or suspected to be malicious. Domain Exclusions specify that EDR does not apply the Malicious URL/IP Detected policy inspection. The domains that are excluded are identified according to your definitions.

To manage exclusions:

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



The list of exclusions in the *Exclusion Manager* page contains the following columns:

Column	Description
Checkbox	Enables you to select multiple rows.
Icon	Represents the type of exclusion •  - Process •  - Execution Prevention

Column	Description
	•  - Domain
SOURCE ATTRIBUTES	Specifies the attributes that were defined in order to identify the Process/File/Domain, as described in Defining exclusions on page 689
OS	Specifies the operating system to which the exclusion applies.
LAST UPDATED	Specifies when this exclusion was last updated and by whom.
STATE	Specifies whether this exclusion is enabled or disabled.
	Edit and delete excursion tools.

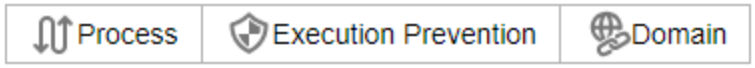
The following actions can be performed in the *Exclusion Manager* page:

- Filtering on page 687
- Defining Exclusion ListsAn Exclusion List contains a list of exclusions. You can assign Collector Groups to an Exclusion List in order to specify that the exclusions in the Exclusion List apply to the Collectors in the Collector Groups assigned to it. Exclusion Lists enable you to logically organize, categorize and group exclusions based on the type of activity data they are to exclude. For example, let's say that you want to collect network activity data for your system, but a specific application generates quite a bit of uninteresting logistical network activity that you do not want to collect. In this case, you can define an Exclusion List named after that application that contains one or more exclusions that relate specifically to the network activity generated by that application. Exclusion Lists can be organized anyway you see fit. For example, you can create an Exclusion List for security products, a different one for PDF documents, a different one for HR-related software and so on. EDR provides two types of exclusion lists: PC and mobile, which can be applied to PC Collector groups and mobile Collector groups, respectively. The type is indicated by the PC or mobile icon at the top right corner of the exclusion list card.Adding an Exclusion ListTo define an Exclusion List:Click the + Add List option, select the type (PC or Mobile), and provide a name to create a new Exclusion List. 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.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 ListYou can perform the following operations on an Exclusion List:OperationDescriptionAssign 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 ListClick the Delete button. Note that all Exclusions in this list will be removed and will no longer be applied to the assigned Collector groups. on page 1
- Defining exclusions on page 689
- Exporting and importing exclusion lists on page 697

Filtering

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

To filter the list of exclusions by type, click one of the following options:

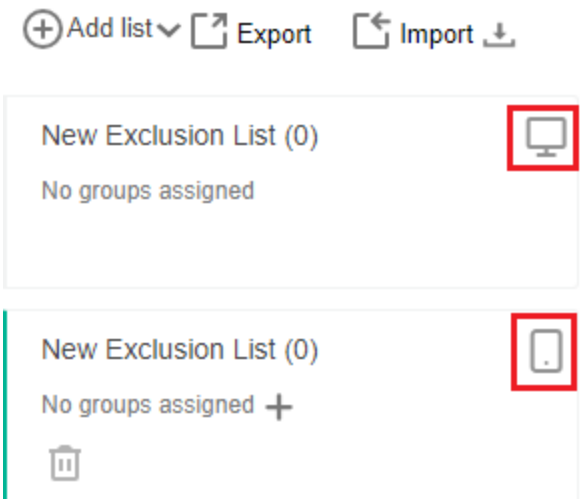


Defining Exclusion Lists

An Exclusion List contains a list of exclusions. You can assign Collector Groups to an Exclusion List in order to specify that the exclusions in the Exclusion List apply to the Collectors in the Collector Groups assigned to it. Exclusion Lists enable you to logically organize, categorize and group exclusions based on the type of activity data they are to exclude.

For example, let's say that you want to collect network activity data for your system, but a specific application generates quite a bit of uninteresting logistical network activity that you do not want to collect. In this case, you can define an Exclusion List named after that application that contains one or more exclusions that relate specifically to the network activity generated by that application. Exclusion Lists can be organized anyway you see fit. For example, you can create an Exclusion List for security products, a different one for PDF documents, a different one for HR-related software and so on.

EDR provides two types of exclusion lists: PC and mobile, which can be applied to PC Collector groups and mobile Collector groups, respectively. The type is indicated by the PC or mobile icon at the top right corner of the exclusion list card.

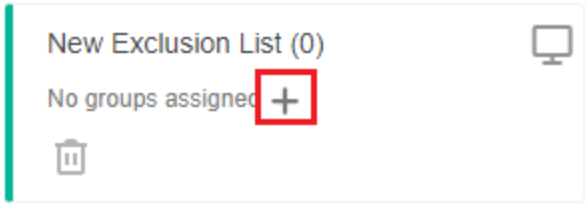


Adding an Exclusion List

To define an Exclusion List:

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

Assigning a Collector Group to an Exclusion List



You can perform the following operations on an Exclusion List:

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

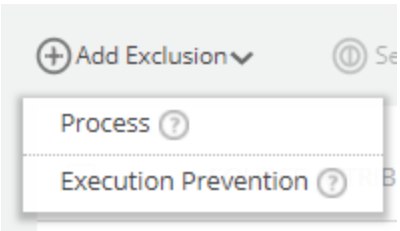
Defining exclusions

All exclusions must belong to an exclusion list. Select an exclusion list on the left to display the exclusions that are defined in it.

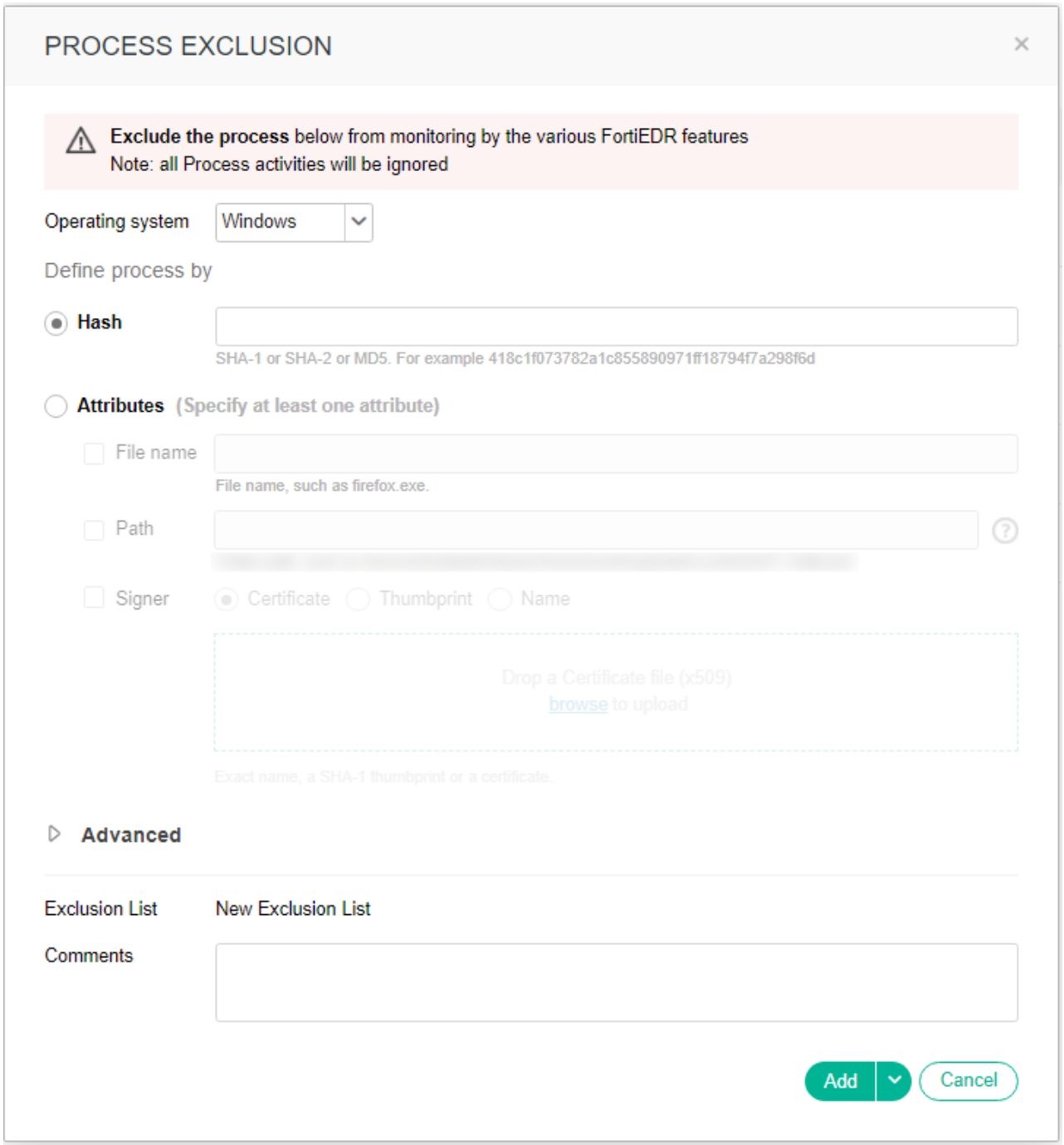
The following describes how to define a Process Exclusion (PC only), Execution Prevention Exclusion, and Domain Exclusion (mobile only).

Adding a Process Exclusion

1. In the left pane, click the PC Exclusion List to which to add the process exclusion.
2. In the right pane, click the *+ Add Exclusion* button. The following displays providing a choice of the two types of exclusions that you can define.

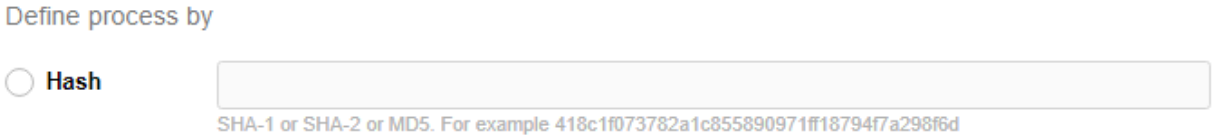


3. Select *Process*. The following displays:

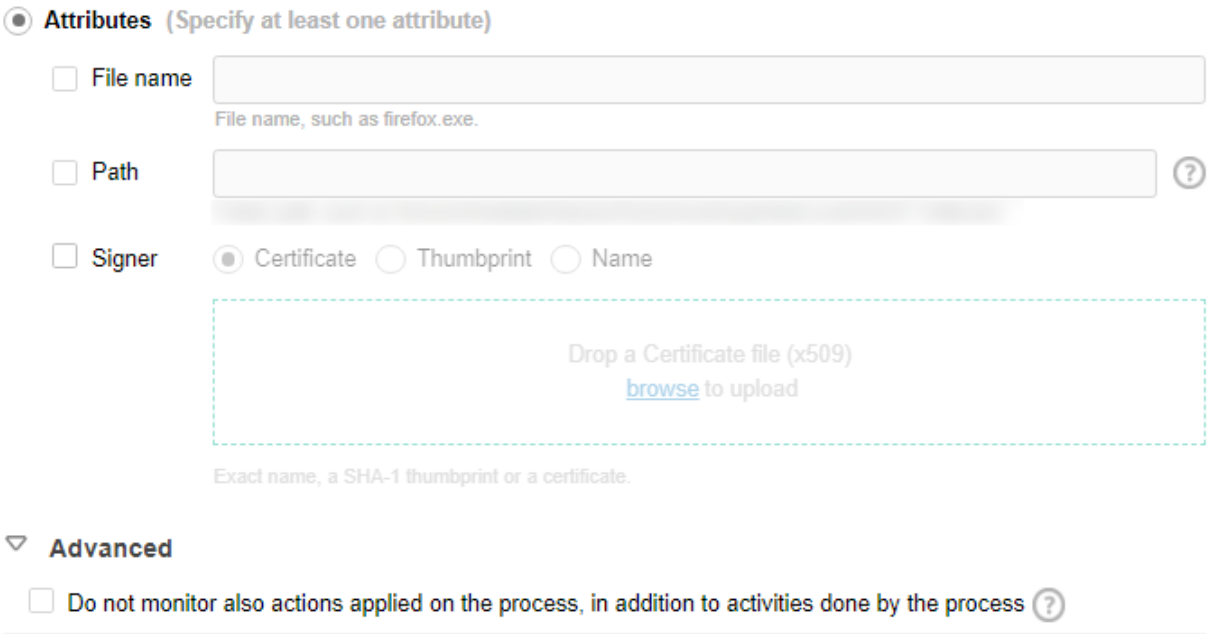


4. The *Operating system* dropdown menu specifies *Windows*, which is currently the only operating system supported for exclusions.
5. Define the processes to be excluded using one of the following options: **Hash** or any combination of **File Name / Path / Signer**, as follows:

- **Hash**: Mark the Hash radio button and specify the Hash that uniquely identifies this process.



- **File Name / Path / Signer**: Mark the *Attributes* radio button and check at least one of the *File Name* / *Path* / *Signer* fields checkboxes and fill the relevant values, as follows:



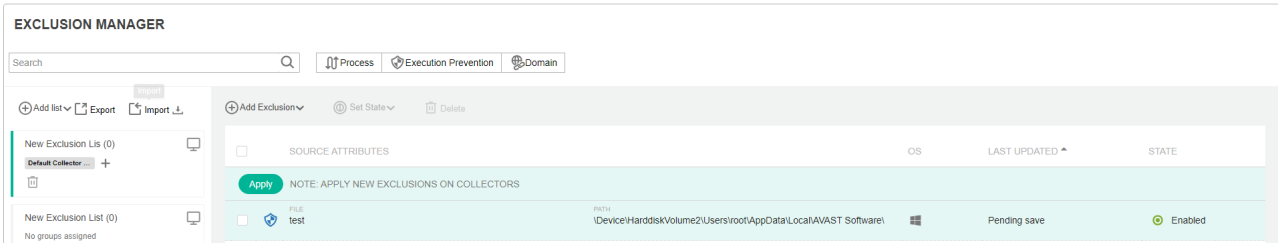
  - Specify the file and/or directory to be excluded by filling in the *File name* field, the *Path* field or both. If you fill in both fields, then that file is only excluded in that path. If you only fill in the *File name* field, then that file is excluded wherever it appears. Refer to the Defining an exclusion path on page 696 section for more details about defining an exclusion path.
  - If you want to specify a signer, select *Signer*, then either upload the Signer's Certificate, provide its thumbprint or provide the Signer's name.
  - When a process is identified by file name and/or path only (which means *Signer* is not selected), you can disable monitoring of the process completely, including actions applied on the process, by selecting *Do not monitor also actions applied on the process, in addition to activities done by the process* under *Advanced*.



This option significantly reduces EDR protection on the process and lowers the security level of the process. Use this option only for issues that regular exclusions cannot solve, such as VDI freezes or other application malfunctions due to basic monitoring of the process by the EDR Collector.

6. The *Exclusion List* field specifies the Exclusion List that was selected, when the *Add Exclusion* option was selected. This field is not editable.

7. Click the *Add* button. This new exclusion is then listed in the *Exclusion Manager* page, as shown below:

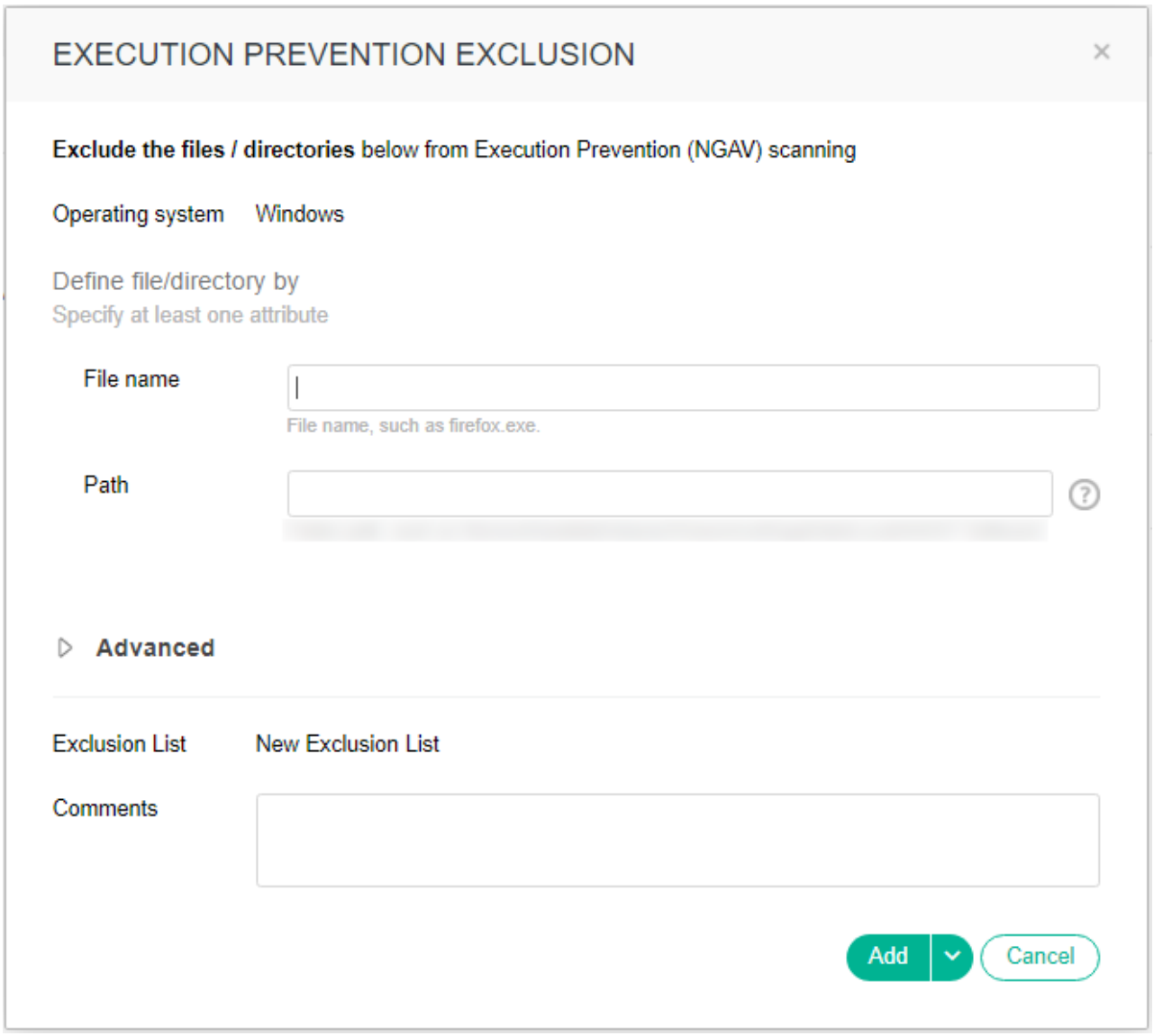


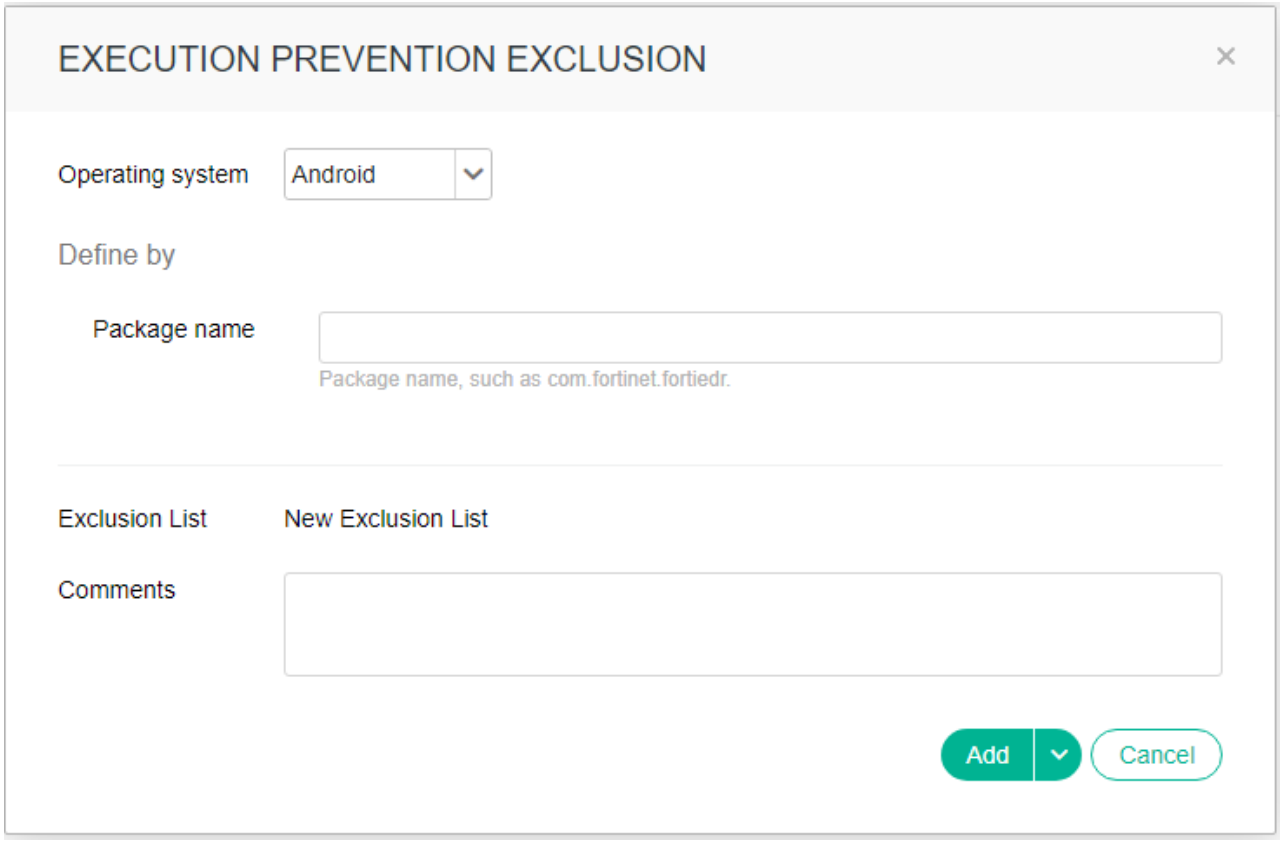
8. The newly defined exclusions appear with a green background and the words *Pending save* appear in their *LAST UPDATED* column. To define that these exclusions take effect, you must click the *Apply* button and then click the *Save* button in the window that pops up. Their *LAST UPDATED* column then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

Adding an Execution Prevention Exclusion

1. In the left pane, click the Exclusion List to which to add the exclusion.
2. In the right pane, click the *+ Add Exclusion* button and select *Execution Prevention*. Depending on the exclusion list type (PC or mobile), one of the following windows displays:

3.

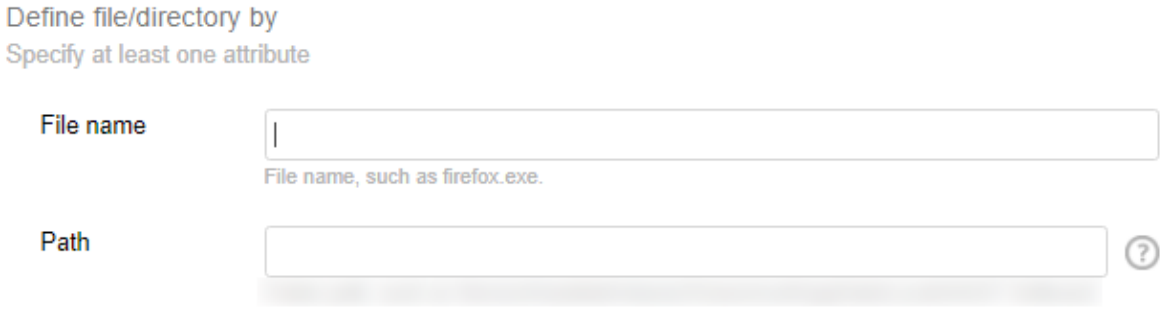

EXECUTION PREVENTION EXCLUSION
Exclude the files / directories below from Execution Prevention (NGAV) scanning
Operating system
Windows
Define file/directory by
Specify at least one attribute
File name
File name, such as firefox.exe.
Path
Advanced
Exclusion List
New Exclusion List
Comments
Add
Cancel



4. Specify the values to define the exclusion:
   - For PC, follow the steps below:

     The *Operating system* dropdown menu specifies *Windows*, which is currently the only operating system supported for exclusions.

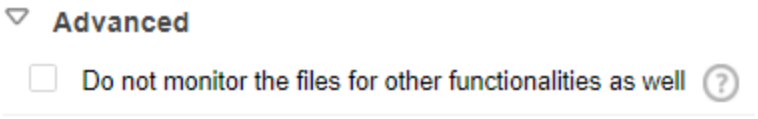
     i. Specify the file and/or directory to be excluded by filling in the *File name* field, the *Path* field or both. If you fill in both fields, then that file is only excluded in that path. If you only fill in the *File name* field, then that file is excluded wherever it appears. Refer to the Defining an exclusion path on page 696 section for more details about defining an exclusion path.

     ii. Under *Advanced*, you can select *Do not monitor the files for other functionalities as well* to disable monitoring of the file/directory completely, including backup of the files for Ransomware protection.



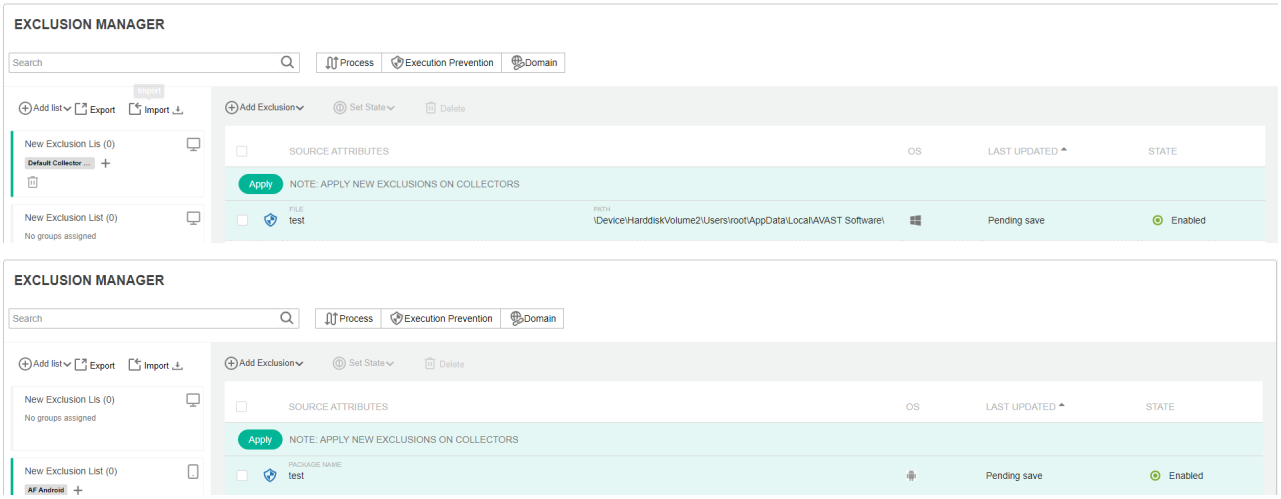
This option significantly reduces EDR protection on the files and lowers the security level of the files. Use this option only for issues that regular exclusions cannot solve, such as VDI freezes or other application malfunctions due to basic monitoring of the files by the EDR Collector.



iii. The *Exclusion List* field specifies the Exclusion List that was selected, when the *Add Exclusion* option was selected. This field is not editable.

- For mobile, select *Android* for *Operating system* and specify the package name. Note that EDR does not support execution prevention on iOS.

5. Click the *Add* button. This new exclusion is then listed in the *Exclusion Manager* page, as shown below:

6. 

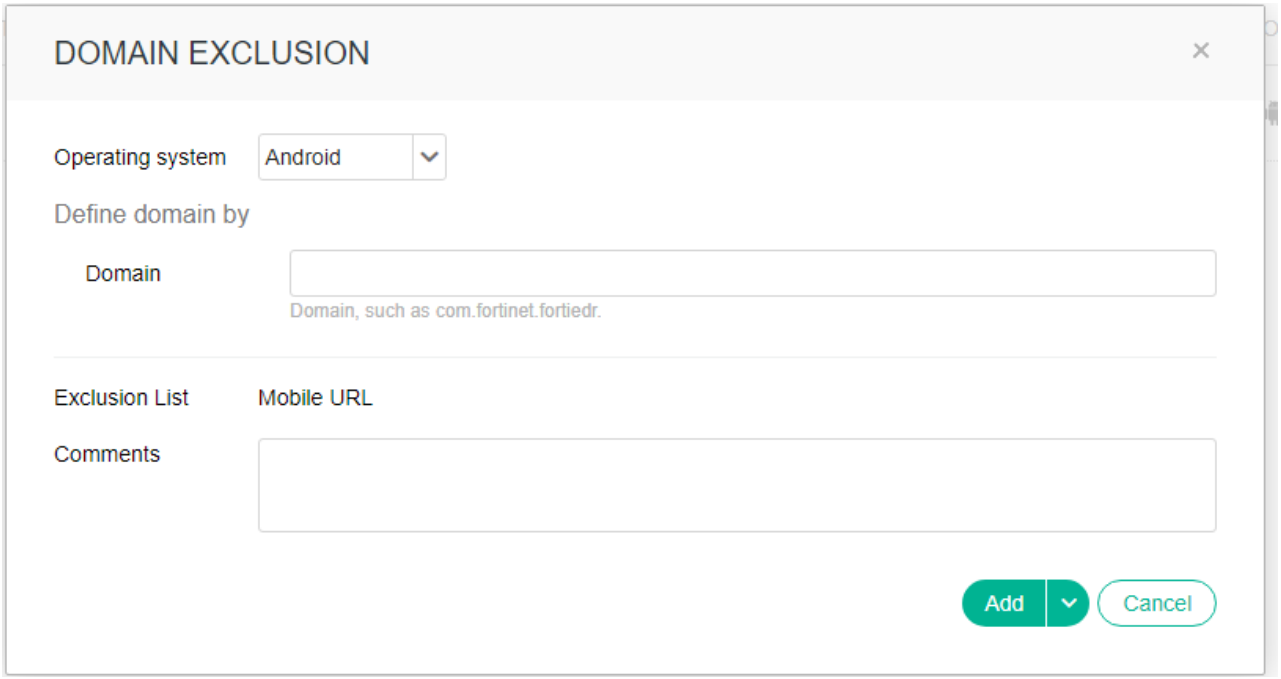
7. The newly defined exclusion appears with a green background and the words *Pending save* appear in its *LAST UPDATED* column. To define that these exclusions take effect, you must click the *Apply* button and then click the *Save* button in the window that pops up. Their *LAST UPDATED* column then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

(Mobile only) Adding a Domain Exclusion

1. In the left pane, click the mobile Exclusion List to which to add the domain exclusion.
2. In the right pane, click the *+ Add Exclusion* button. The following displays providing a choice of the two types of exclusions that you can define.



3. Select *Domain*. The following displays:



4. In the *Operating system* dropdown menu, select *Android* or *iOS*.
5. Specify the domain to exclude.
6. Click the *Add* button. This new exclusion is then listed in the *Exclusion Manager* page., as shown below:
7. The newly defined exclusions appear with a green background and the words *Pending save* appear in their *LAST UPDATED* column. To define that these exclusions take effect, you must click the *Apply* button and then click the *Save* button in the window that pops up. Their *LAST UPDATED* column then shows the timestamp when they were saved.

Defining an exclusion path

The table below provides examples of exclusion paths with explanations of which folders apply or do not apply:

Exclusion path	Folders that apply	Folders that do not apply
`\Documents\Personal\`	`\Documents\Personal`	• `\Documents` • `\Documents\Personal\temp`
`\Documents\Personal\*`	• `\Documents\Personal\subfolder\` • `\Documents\Personal\subfolder\subfolder\etc\`	• `\Documents` • `\Documents\Personal`
`\Documents\Personal*\`	• `\Documents\Personal` • `\Documents\Personal2` • `\Documents\Personal\subfolder\`	`\Documents`

Exclusion path	Folders that apply	Folders that do not apply
*\Documents\Personal\	• \Documents\Personal • \Windows\Documents\Personal	• \Documents • \Documents\Personal\temp
\Documents\Personal	• \Documents\Personal\subfolder\ • \Parent\Documents\Personal\subfolder	• \Documents • \Documents\Personal



- Including a wildcard in a path excludes only the parent folders and/or sub-folders and files within those parent and/or sub-folders but not the folder itself. To exclude a directory and also the parent or sub-directories, you must define an exclusion path for each case. For example, to exclude \Documents\Personal and all the sub-folders, define the following exclusion paths:
  - \Documents\Personal
  - \Documents\Personal*
- Physical prefix (e.g. \Device) and logical prefix or drive (e.g., C:\) are not required in the exclusion path.

Setting the state of an exclusion

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

For changing the state of multiple Exclusions, check the checkboxes of all relevant exclusions and then select the state from the *Set State* dropdown under the toolbar.

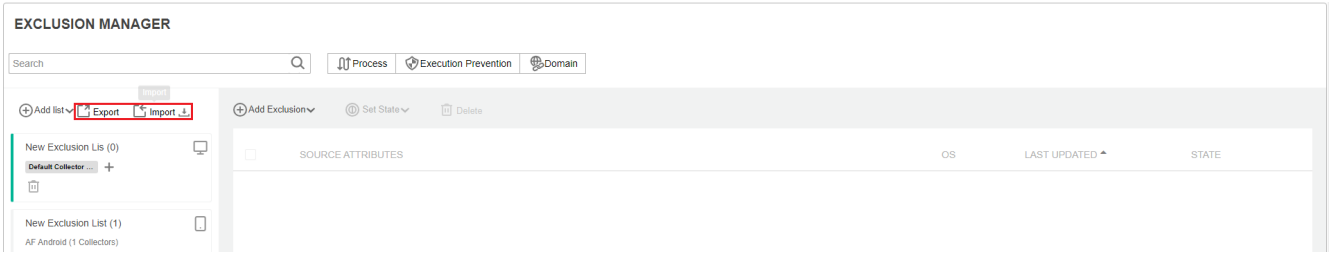
Deleting an exclusion

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

To delete multiple Exclusions, check the checkboxes of all relevant exclusions and then select the *Delete* option in the toolbar.

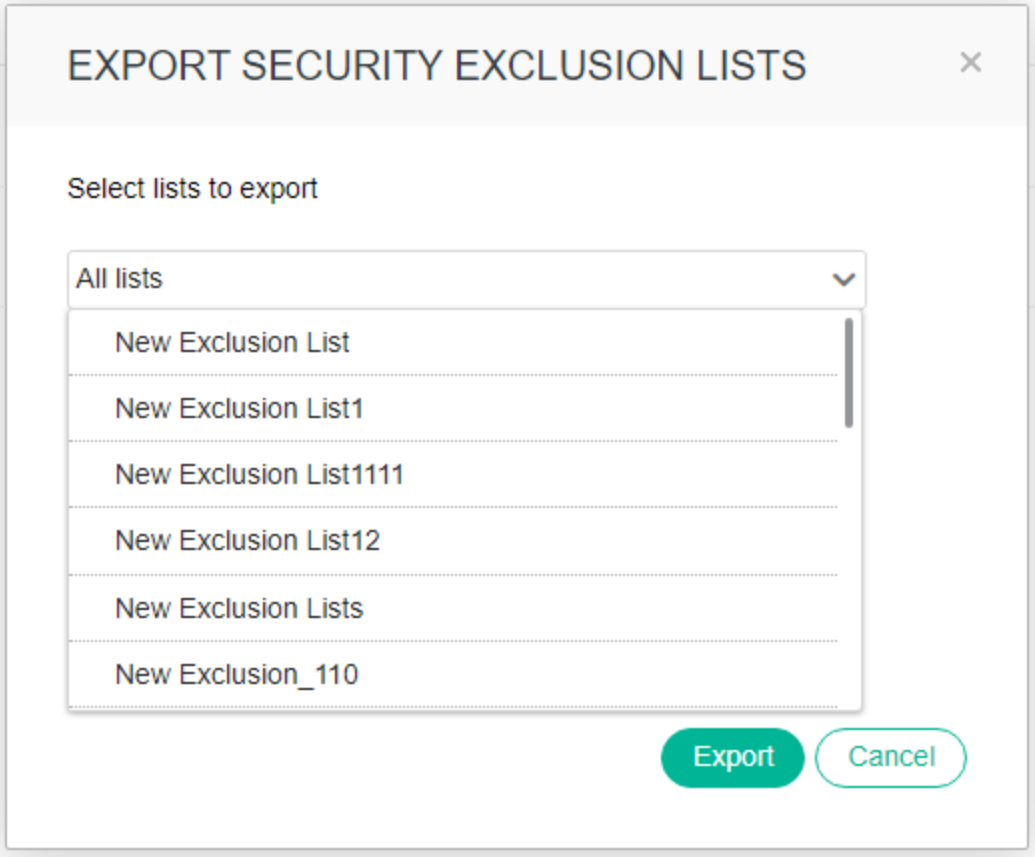
Exporting and importing exclusion lists

You can export or import exclusion lists for Process Exclusions and Execution Prevention Exclusions using the *Export* and *Import* buttons at the top-left of the Exclusion Manager page. This function is handy in a muiti-tenant environment where you can easily duplicate the exclusion lists for some or all organizations without the need to re-define exclusions for each organization separately.



To export one or multiple exclusion lists:

1. In the Exclusion Manager page, click *Export* at the top-left corner.
2. In the window that appears, select the list(s) to export. To export all lists, select *All lists*.

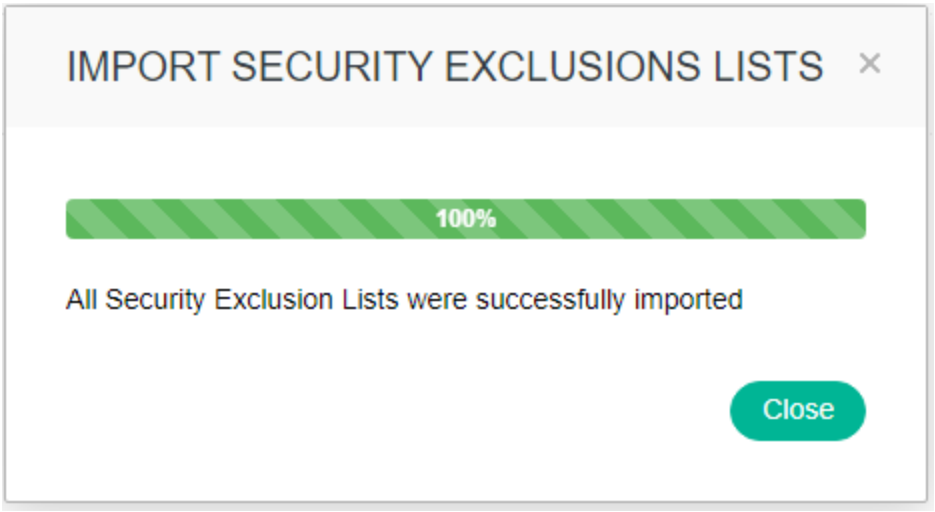


3. Click *Export*.
4. After the export is complete, click *Download* to save the file and then click *Close*.
   The file includes all exported exclusions and the exclusion lists that each exclusion belongs to.

To import one or multiple exclusion lists:

1. In the Exclusion Manager page, click *Import* at the top-left corner.
2. Select the list(s) to import (that you have saved or exported) and click *Open*.

3. Wait for the import to complete and click *Close*.

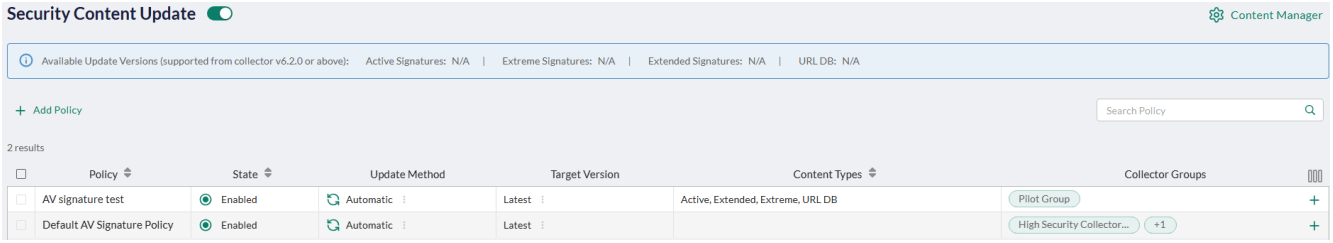


If a list name in the imported list already exists in the system, EDR adds a suffix to the name of the newly imported list without touching the existing list.

For example, if the list name "AV" already exists, EDR renames the imported list as "AV_1" that will appear in addition to the existing "AV" list. If such a list name ("AV") gets imported again, EDR increments the number in the suffix of the list name for each subsequent import, which would be "AV_2", "AV_3", etc.

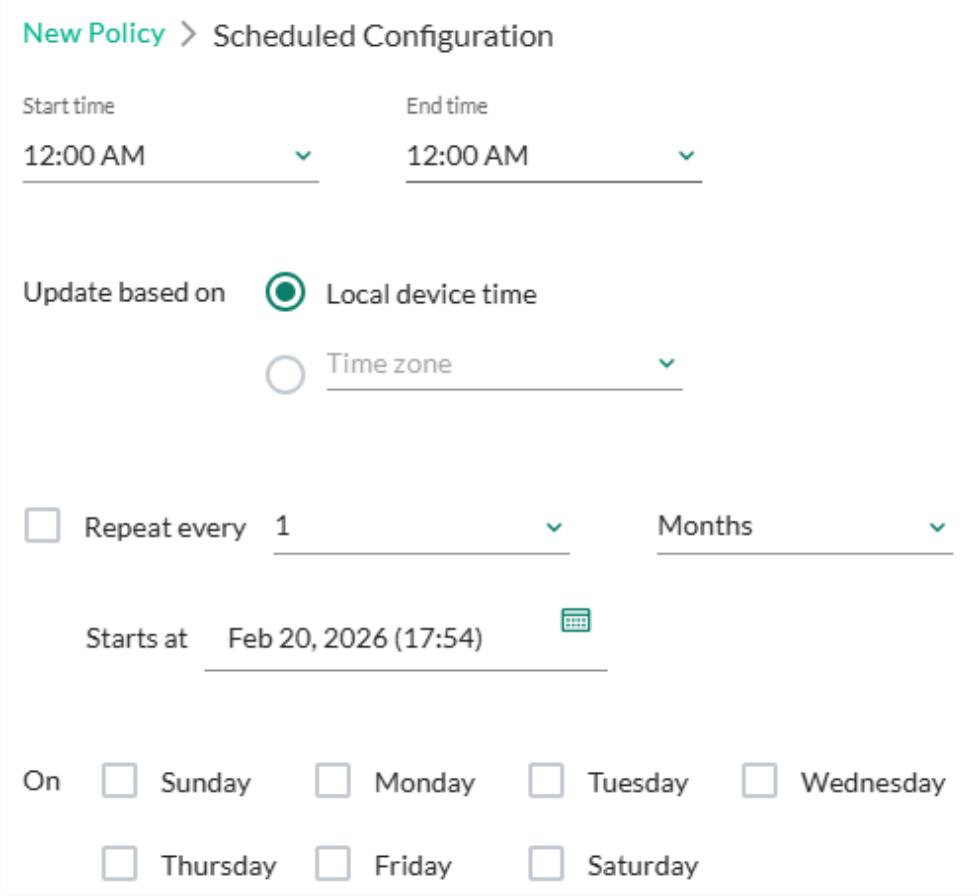
Security Content Update

Use the *Profiles* > *Security* > *Security Content Update* page to configure AV signature policies to define when and how Collector groups download AV signatures for each type (Active, Extended, Extreme, and URL DB) based on time-based rules and time zones.



To configure an AV signature policy:

1. In the *Profiles* > *Security* > *Security Content Update* page, click the *Add Policy* button at the top left corner.
2. Specify a name for the AV signature policy.
3. Select the Collector groups that the AV signature policy applies to.
4. Select the update method, which can be the following:

Automatic	FortiEndpoint automatically updates AV signatures to the latest or a specific version when it becomes available.
Scheduled	FortiEndpoint updates AV signatures to the latest or a specific version based on the configured schedule. Click *Add Config* to set up an update schedule. You can add multiple schedules. 

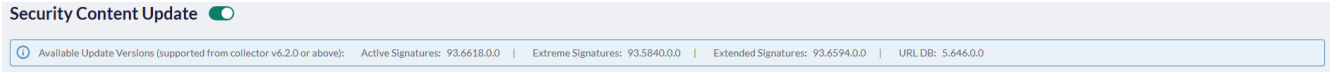
5. Select the content types to update, which can be the following:
   - Active
   - Extended
   - Extreme
   - URL DB

   See the FortiOS documentation for details about the content types.
6. Select the target version of AV signatures to update to, which can be the latest (default) or a specific version (you can specify the version for each type).
7. Click *Save* to save the AV signature policy.

   The AV signature policy appears in the list.
8. **(Optional)** Add or remove Collector groups for the AV signature policy in the *Collector Groups* column.
9. Enable or disable the AV signature policy by clicking the *Enabled/Disabled* button in the *State* column.

   Once the configuration update with the new AV Signature updates, the Collectors will retrieve and download the signature updates according to the policy.

The AV signature versions are displayed at the top of the page.



Application Control

The Application Control policy enables EDR to block pre-defined applications from running, so that it does not launch. It enables limiting the usage of non-desired applications on specific collector groups.

This differs from Applications on page 647 under *Communication Control*, which enables you to control which applications can communicate outside of the organization, but does not stop them from launching.

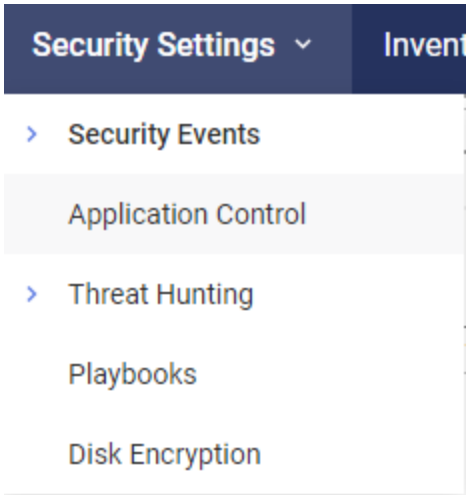
This section describes how to define the applications to be blocked by adding them in the Application Control. In addition, applications can be added to the list of applications to be blocked by adding them from the Investigation View on page 576. These applications are then listed in the Application Control Manager.

In general, in order to block applications so that they are not launched

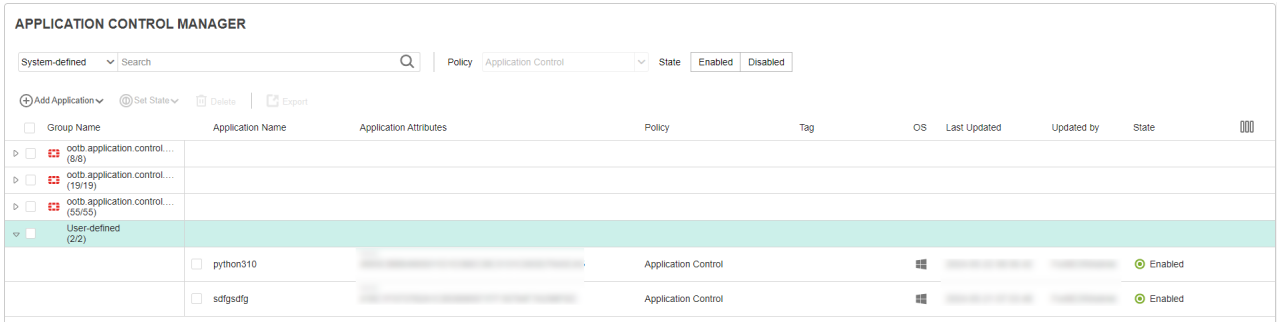
- The applications must be added to the Application Control Manager under the user-defined group
- Collector groups must be assigned to this policy
- The blocklist rule must be enabled on the Application Control Policy.

To add applications to the blocklist:

1. Select *Profiles* > *Security* > *Application Control* .



The following window displays, showing a list of different groups of applications that have been defined to be blocked by the Application Control policies.



Predefined application groups (indicated by the Fortinet logo by the group name) are always at the top of the application list and are assigned to the *Application Control* policy by default. You cannot add or delete applications from predefined application groups but you can disable specific applications or change the policy settings.

Applications added by the user are automatically categorized under the *User-defined* group with a default state of disabled, which means they are not blocked by default.

2. You can then perform any of the following actions:
   - Adding application(s) to be blocked on page 702
   - Exporting the list of applications to be blocked on page 707
   - Enabling/disabling application blocking on page 708
   - Changing the policy under which the application is blocked on page 708
   - Searching and filtering applications on page 709
   - Editing an Application by selecting the *Edit* button on the right side of that Application's row.
   - Deleting an Application by selecting the *Delete Application* option at the top of the window or selecting the *Delete* button on the right side of that Application's row.

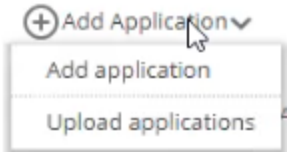


You cannot delete a group, change or search any group names.

Adding application(s) to be blocked

To add an application(s) to be blocked:

1. Click the *+ Add Application* option. The following displays:



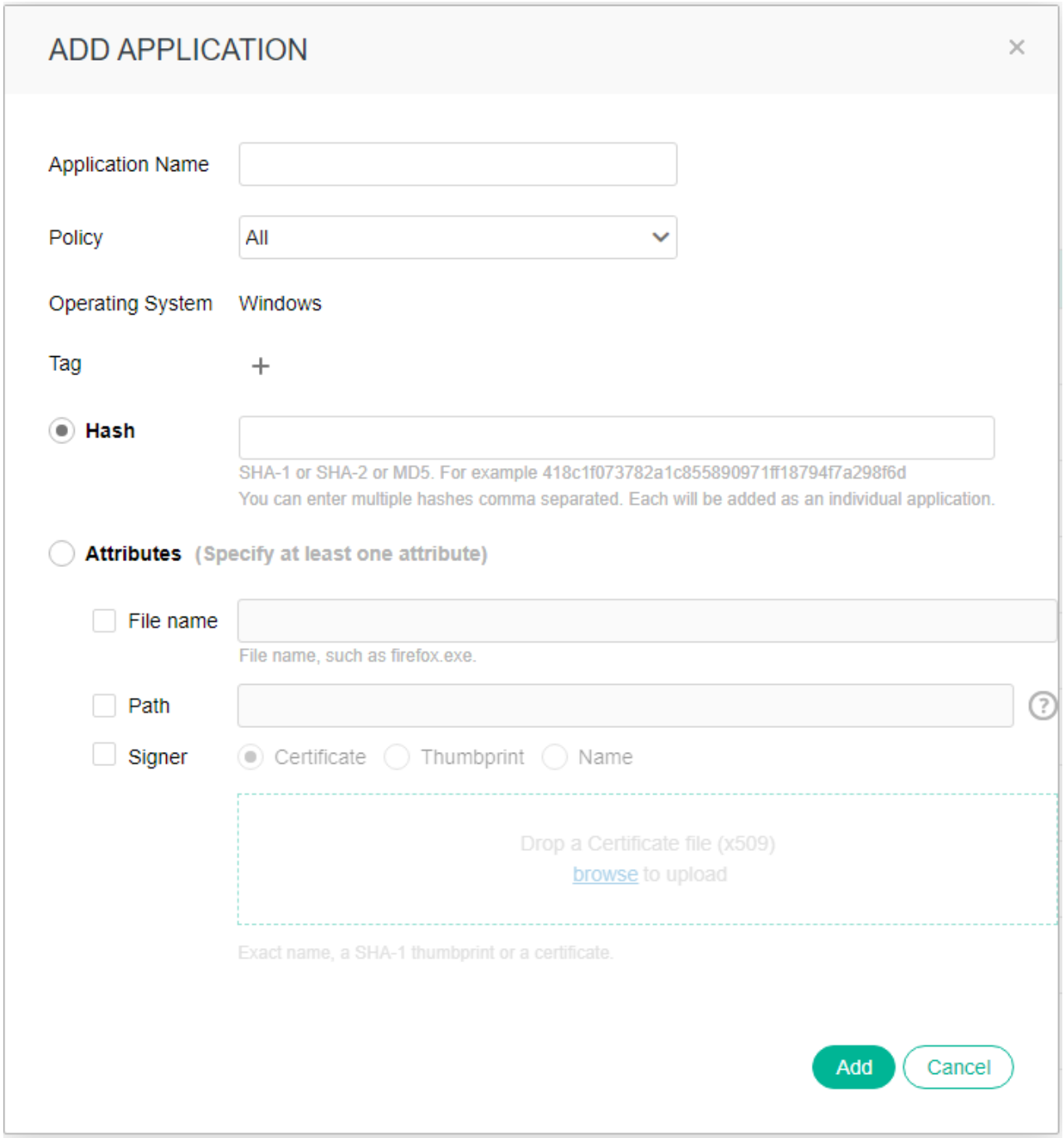
This dropdown menu provides two options for adding applications to be blocked:

- Manually adding an application to be blocked on page 703
- Uploading application(s) to be blocked on page 706

Manually adding an application to be blocked

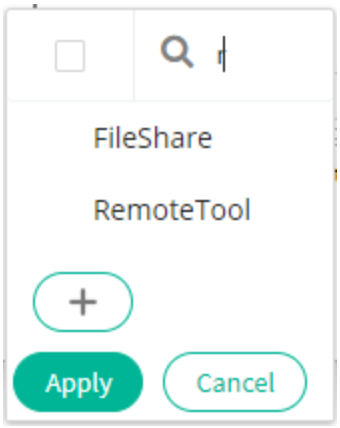
To manually add an application to be blocked:

1. Select *Add application*. The following displays:



2. In the *Application Name* field, specify a name to identify the application. The application name must be unique within the *User-defined* group.

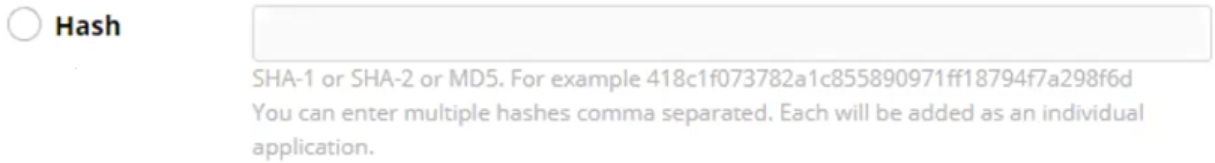
3. From the *Policy* dropdown menu, select one or more of the *Application Control* policies in which to block this application or select the *All* option to specify that this application is to be blocked by all Application Control type policies. EDR is provided out-of-the-box with a single Application Control type policy and you can clone it in order to create additional Application Control type policies as needed.
4. You can optionally use the *Tag* field in order to classify this application. Tags can be helpful for classifying and filtering long lists of applications. In the *Tag* field, click the *Add* button + to specify the tag to be added to the application. You can assign a previously defined tag or define a new tag.



5. Define the application(s) to be blocked (so that they are not executed) using one of the following options: **Hash** or any combination of **File Name / Path / Signer**, as follows:

EDR blocks only executables and DLLs that meet the defined criteria. When determining whether a file is an executable, DLL, or another type, EDR adheres to the file nature rather than the file name (such as the `.exe` extension).

- Hash: Mark the Hash radio button and specify one or more Hashes. Each hash is the unique identifier of an individual application. If you enter multiple hashes, then they must be comma separated. Supported hash formats are specified under the field.



OR

- **File Name / Path / Signer**: Mark the *Attributes* radio button, check at least one of the *File Name / Path / Signer* fields checkboxes and fill the relevant values, as follows:
  - Specify the executable file of the application to be blocked by filling in the *File name* field.
  - Specify the path to the executable file of the application to be blocked by filling in the Path field.

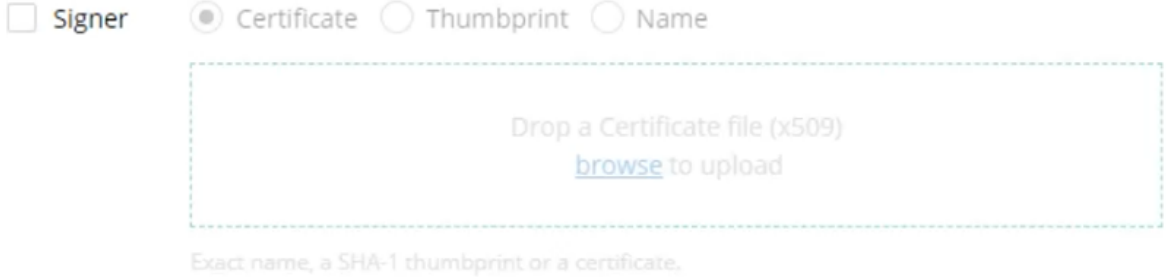
    If you fill in both the *File name* field (described above) and the *Path* field, then that application is only blocked if its executable is in that path. If you only fill in the *File name* field, then that application is blocked no matter where its executable file appears.

    Wildcards can be used in a folder name by placing a single wildcard (*) at the beginning, end and middle of the path.

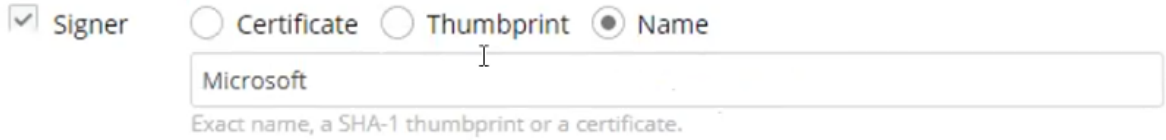
    For example: `*\folder0\folder1*\folder2*`



- If you select *Signer*, then either upload the Signer's Certificate (as shown below), provide its thumbprint or type in the Signer's name. Uploading a certificate or specifying thumbprint is more secured that specifying signer name and hence recommended.



For example, selecting the *Name* radio button, then entering the word `Microsoft`, blocks the execution of any application that was signed by Microsoft. You must enter the exact name of the Signer.

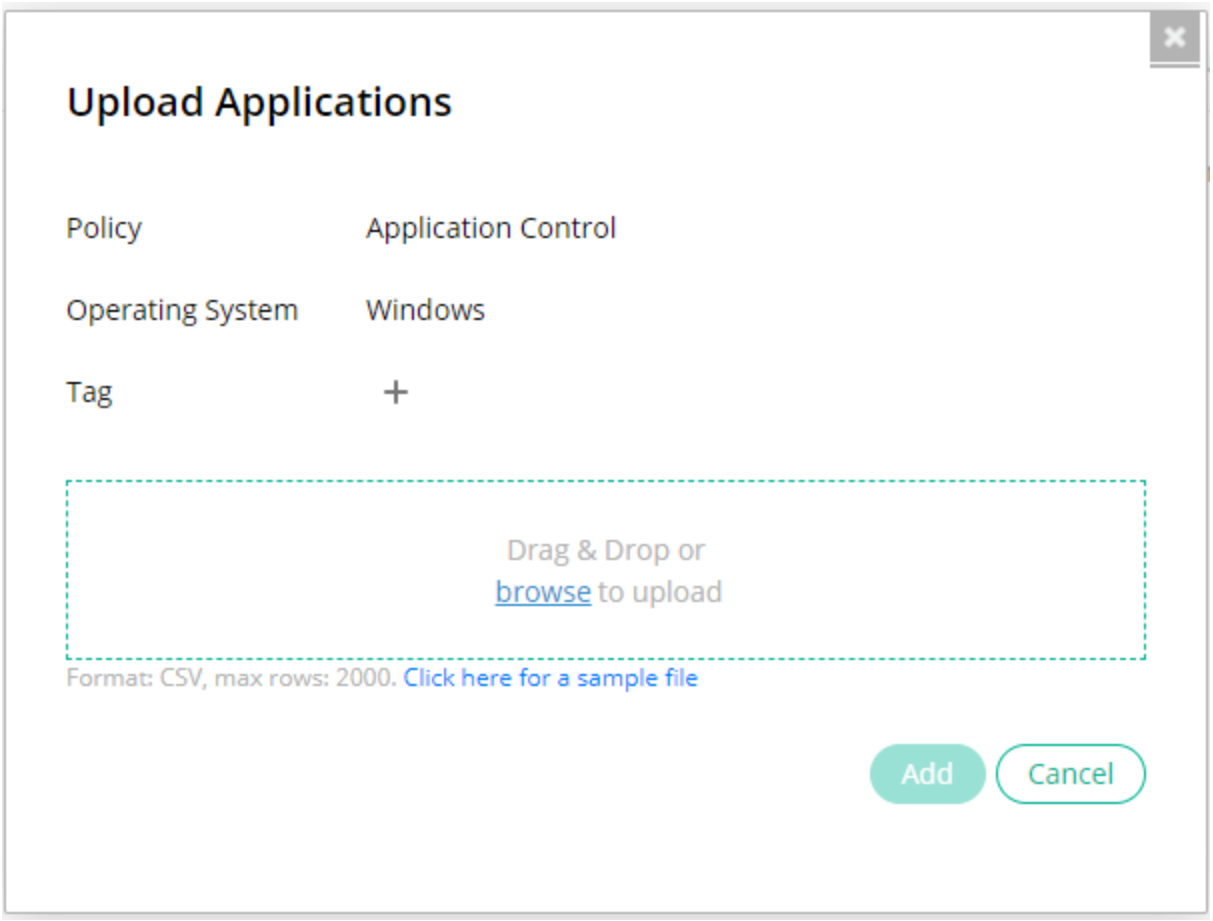


6. Click the *Add* button. The application is then listed under the *User-defined* group.
When a Collector Group is assigned to the application control policy (specify above), then all these applications are blocked and cannot be launched.

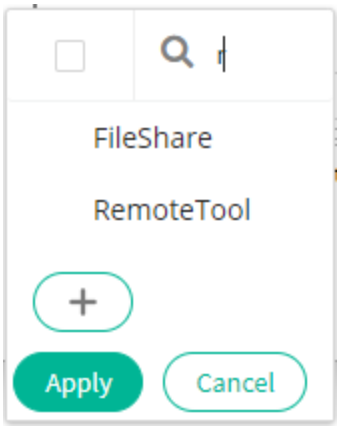
Uploading application(s) to be blocked

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

1. Select *Add Application* > *Upload Applications*. The following displays:



2. From the *Policy* dropdown menu, select one or more of the *Application Control* policies in which to block the applications specified in the file to be uploaded.
3. You can optionally use the *Tag* field in order to classify this application. Tags can be helpful for classifying and filtering long lists of applications. In the *Tag* field, click to specify the tag to be added to the application. You can assign a previously defined tag or define a new tag.



4. In the bottommost field of this window, select the CSV file that contains the list of applications to be blocked. This file should be a CSV file in which the five leftmost columns (shown below) identify the application to be blocked. A sample file can be downloaded from this window. Alternatively, you can use the same file as can be exported, as described in Exporting the list of applications to be blocked on page 707.

FORTINET [redacted] Report created by user [redacted] Confic

APPLICATIONS CONTROL

GROUP NAME	APPLICATION NAME	HASH	SIGNER THUMBPRINT	SIGNER NAME	PATH	FILE NAME	POLICY	TAG	OS	LAST UP
User-defined	aaaaaaa								Windows	2024-02-0
User-defined	aaaaaaa								Windows	2024-02-0
User-defined	aaaaaaa								Windows	2024-02-0
User-defined	uuuuu2								Windows	2024-02-0
User-defined	uuuuu2								Windows	2024-02-0
User-defined	Application_-1749470844								Windows	2024-02-0
User-defined	uuuu								Windows	2024-02-0
User-defined	test								Windows	2024-02-0
User-defined	sewefsefsfse								Windows	2024-01-2
User-defined	hash13								Windows	2024-01-2

5. Click the *Add* button. The Application Control Manager then lists a row for each application in the uploaded file under the *User-defined* group.
   When a Collector Group is assigned to the Application Control policy (specify above), then all the applications that are added will be blocked and will not be launched.

Exporting the list of applications to be blocked

To export the list of EDR applications to be blocked:

1. Select the group(s) that you want to export.
2. Click *Export* to export the applications list as an Excel file.

Enabling/disabling application blocking

If you wish to disable the blocking of all the applications that are under a specific policy, we recommend simply disabling the blocklist rule of that policy. Alternatively, in order to temporarily block only specific applications, then we recommend enabling/disabling each application separately. If an application no longer needs to be on the blocklist, then we recommend deleting it using the *Delete* button in the right-most column or in the toolbar.

To enable/disable the blocking of specific applications:

1. Select *Profiles* > *Security* > *Application Control* to display the Application Control Manager. Each row represents an application to be blocked.
2. Select the application(s) to block. To block all applications in a specific group, select the group instead.
3. In the *STATUS* column on the right, toggle the value between *Enabled* and *Disabled*. Alternatively, you can check the checkboxes of the desired application rows, and then select the *Enabled* or the *Disabled* option from the *Set State* dropdown.



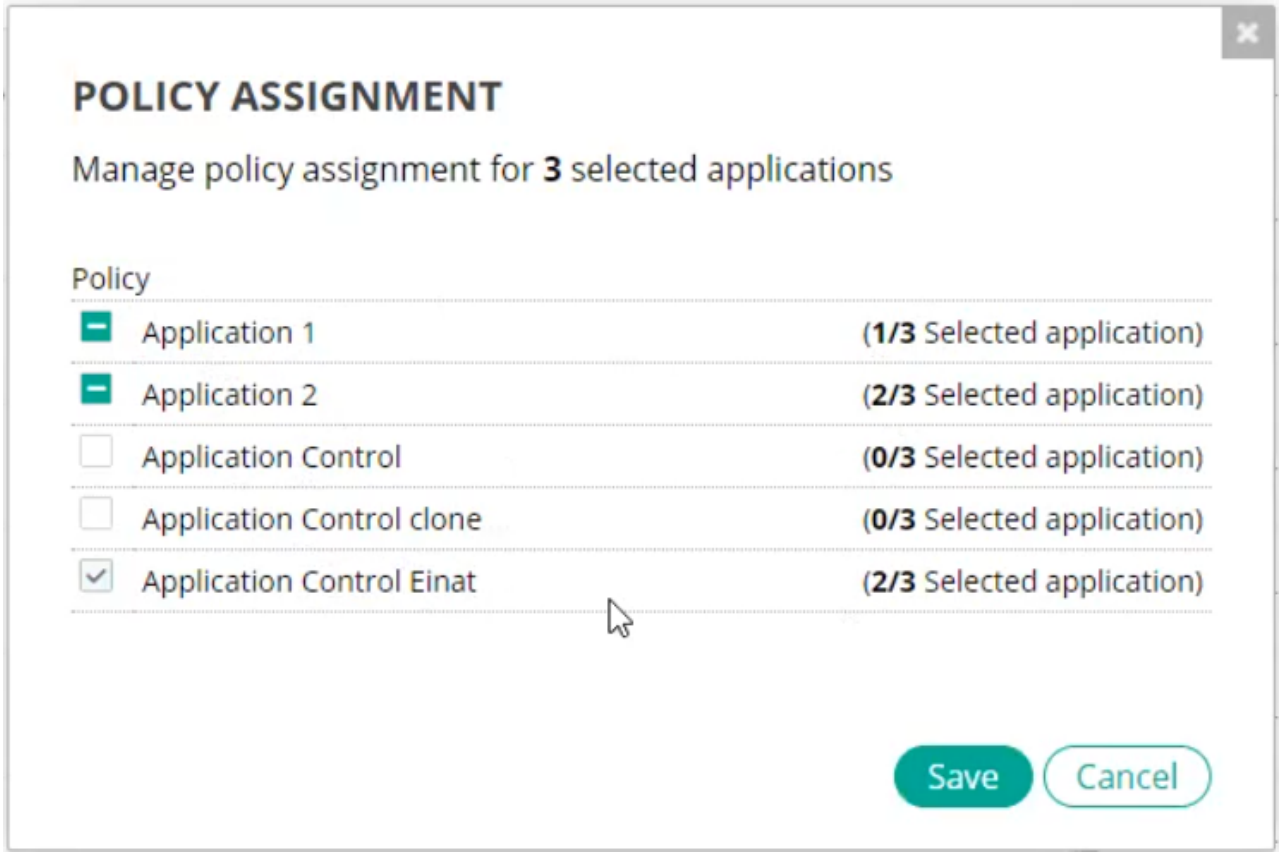
Newly added applications are set to be disabled by default, which means they are not blocked

Changing the policy under which the application is blocked

To change the policy that blocks an application:

1. Select *Profiles* > *Security* > *Application Control* to display the Application Control Manager. Each row represents an application to be blocked.
2. In the Application Control Manager window, select the application(s) to change policy. To change policy of all applications in a specific group, select the group instead.

3. Click the *Policy Assignment* option. The following displays.



The policies that have a checkbox to their left have already been assigned all the selected applications. The policies that have a green minus sign to their left have already been assigned some of the applications. The right side of the window indicates how many of the applications that you selected in the Application Control Manager window have been assigned to that policy. The policies that have an empty box to their left were not assigned any of the selected applications.

4. In the *Policy Assignment* window, check (or uncheck) the checkboxes of the policies that should block the currently selected applications.
5. Click the *Save* button.

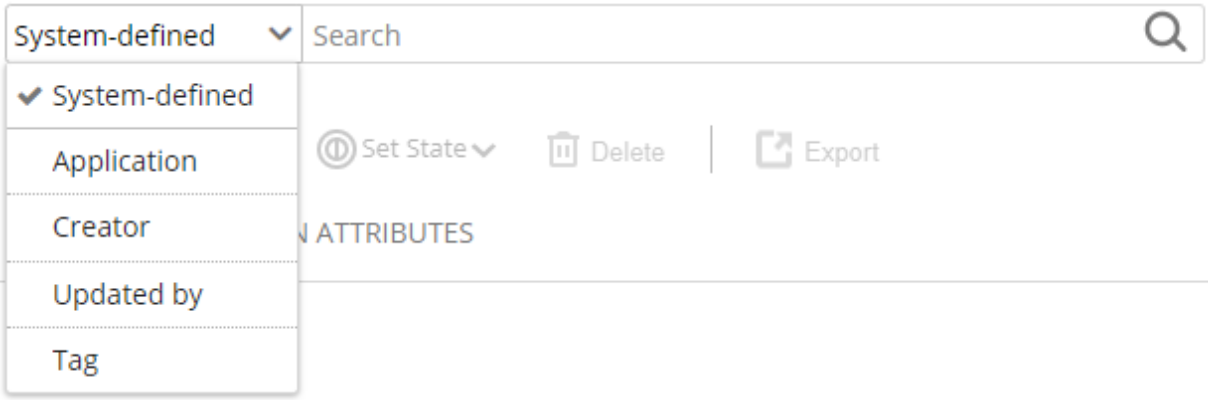
Alternatively, in order to modify the policy to which a specific application is assigned, select the *Edit* button in the Application Control Manager window in the right side of that application's row.

Searching and filtering applications

To filter the list of applications defined in the Application Control Manager, use the fields at the top of the window, as follows:

1. Enter text in the *Search* field. This search field uses exact word matching.
   - By default, the *System-defined* option is selected, which specifies that the search is performed on the most relevant fields and then the list is filtered accordingly. Alternatively, from this dropdown

menu, you can select the column that is searched, as follows:



2. Select the relevant policy from the *Policy* field.
3. In the *State* field, select *Enabled* or *Disabled*.

Secure Browser

The secure browser feature is disabled by default and will be gradually rolled out. To be considered as an early adopter, please contact Fortinet Support. The feature supports the following OSes only:

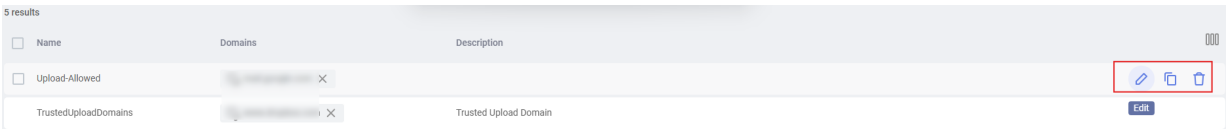
- Windows 11 - 21H2/22H2/23H2/24H2/25H2 (64-bit)
- Windows 10 22H2 (64-bit)
- Windows server 2019 or later

Use the *Profiles* > *Security* > *Secure Browser* pages to secure browsing in Google Chrome on the endpoint:

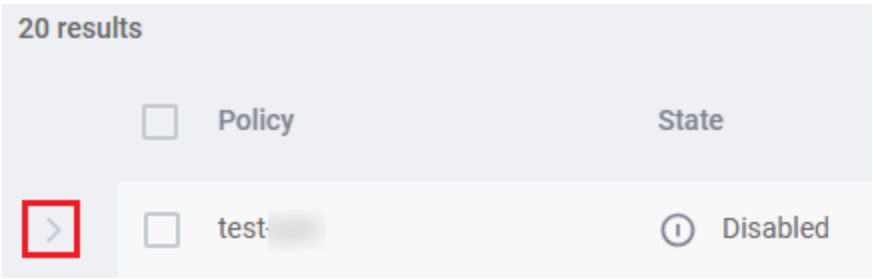
- Approve or protect for file upload/download for specific domains.
- Protect data in specific domains by preventing pasting content from those domains.
- Block traffic to specific website categories.
- Block specific third-party extensions.

To configure secure browsing:

1. Create a list of domains and URLs to allow file upload/download or data transfer as needed:
   a. Go to the *Profiles* > *Security* > *Secure Browser* > *Domain Groups* page and click *Add Group*.
   b. Specify a name for the domain group. For example, *Allow file upload*. The domain group name is case-sensitive.
   c. Optionally, provide a description.
   d. Click *Add Domain* and specify the exact URL of the website to approve or protect. For example, `www.abc.com`. Wildcard is unsupported.
   Repeat this step to add more URLs to the group as needed.
   e. Click *Save*.
   f. Repeat the procedure to add more domain group as needed.
   You can also edit, clone, or delete a domain group using the following options:



2. Create a secure browser policy and connect the domain groups to it:
   a. Go to the *Profiles* > *Security* > *Secure Browser* > *Policies* page and click *Add Policy*.
   b. Specify a name for the policy. The policy name is case-sensitive.
   c. Select the Collector groups that the policy applies to.
   d. Click *Save* to save the policy.
      The policy appears in the list.
   e. **(Optional)** Add or remove Collector groups for the policy in the *Collector group* column.
      A Collector group can only be added to one secure browser policy.
   f. Expand the row of the policy in the table and configure the rules to associate with the policy.

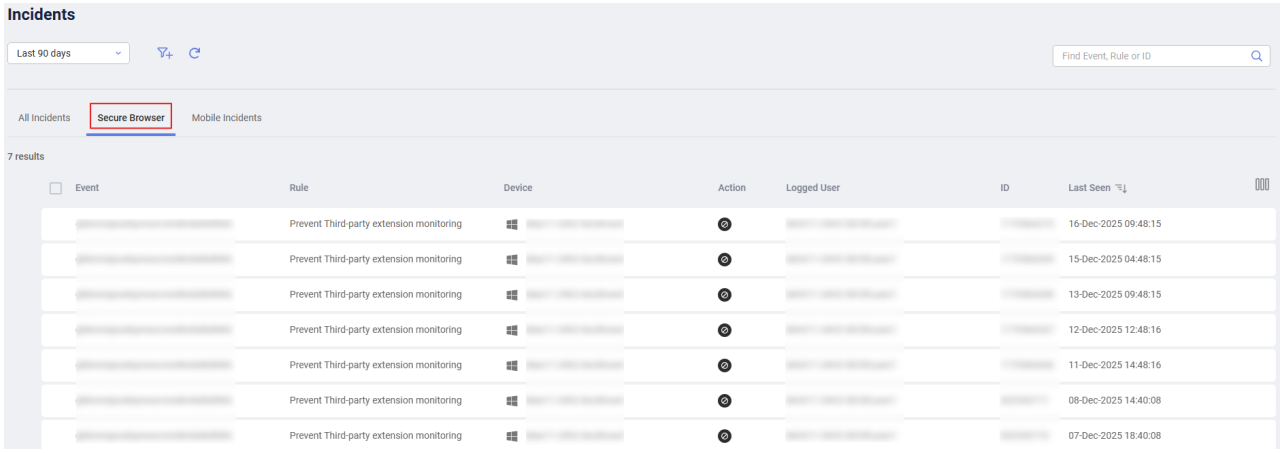


FortiEndpoint EDR provides the following built-in rules, which are all enabled by default. Click the *Enable* button to disable it. To edit a rule, click the *Edit* button to the right of the rule.

Rule	Description
Prevent upload	By default, all file uploads are blocked in the policy. To allow upload from specific websites, edit the rule and click *Add Domain Group* to select the relevant domain groups, such as *Allow file upload*.
Prevent download	By default, all file downloads are blocked in the policy. To allow download from specific websites, edit the rule and click *Add Domain Group* to select the relevant domain groups, such as *Allow file download*.
Prevent data transfer	By default, all data transfers are allowed in the policy, which means you can copy content from any website and paste it to another website. To prevent pasting content copied from specific websites, edit the rule and click *Add Domain Group* to select the relevant domain groups to the protected domain groups list. Content copied from the protected domains will then only be allowed to be pasted into the same domain or another protected domain.
URL reputation	By default, all website categories are allowed in the policy. To block or log traffic to specific website categories, edit the rule and click *Add category* to select the relevant categories and configure the block or log action. **Block** Prevent user access to the website category.

Rule	Description	
	Log	Allow user access to the website category but a notification will be sent about the activity.
Prevent Third-party extension monitoring	By default, all third-party extensions are allowed by the policy. **To block or log specific third-party extensions:** 1. Edit the rule by clicking the *Edit* button to the right of the rule. 2. Configure the block or log action, which applies to all third-party extensions in the block list. **Block** — Disable the block list of third-party extensions. **Log** — Allow user access to the block list of third-party extensions but a notification will be sent about the activity. 3. Click *Add Extension* to define a list of third-party extensions to block using the extension ID. You can retrieve the extension ID by turning on *Developer mode* in `chrome://extensions/`.	

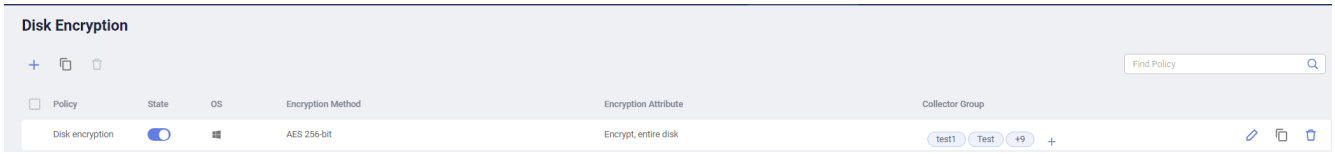
3. Check incidents for secure browser in the *Secure Browser* tab of the *Incidents* view.



Disk Encryption

Use the *Profiles* > *Disk Encryption* page to configure disk encryption policies to enforce disk encryption on Windows 7 or later (using BitLocker, TPM required) and macOS (using FileVault) endpoints to ensure consistent security configurations and compliance with regulatory requirements. You can also configure disk decryption policies to allow users to decrypt an encrypted disk.





To configure a disk encryption policy to enforce disk encryption on specific Collector groups:

1. In the *Profiles* > *Disk Encryption* page, click the *Add* button at the top left corner.
2. Specify a name for the policy.
3. Enable the policy if you want to enforce the policy immediately after creation. You can also choose to enable it later.
4. Select the OS and configure the relevant options:

Windows	macOS
1. Under *Action*, select *Encrypt all disks* or *Encrypt only used disk*. 2. Under *Method*, select an encryption method for Windows 10 or later.	1. Under *Action*, select *Encrypt*. 2. Under *Method*, select the number of allowed user logins with an unencrypted disk. For example, if *3* is selected, the user will not be able to log in on the third attempt without confirming the disk encryption. 3. Upload the FileVaultMaster certificate.

5. Click *Save*.
   The policy appears in the disk encryption policies table.
6. Enable or disable the policy by toggling the button in the *State* column.
7. Add or remove Collector groups for the policy in the *Collector Group* column.
8. **(macOS)** To verify the disk encryption status, run `sudo fdesetup status` on the endpoint. You can run the command multiple times to see the progress. When the encryption is complete, the status will show that FileVault is on. Encryption speed depends on HD size and Mac model.

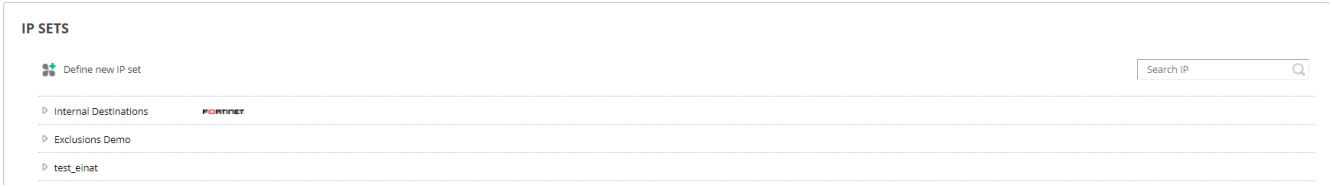
To configure a disk decryption policy to allow users of specific Collector groups to decrypt an encrypted disk:

1. In the *Profiles* > *Disk Encryption* page, click the *Add* button at the top left corner.
2. Specify a name for the policy.
3. Enable the policy if you want to enforce the policy immediately after creation. You can also choose to enable it later.
4. Select the OS and select *Decrypt* under *Action*.
5. Click *Save*.
   The policy appears in the disk encryption policies table.
6. Enable or disable the policy by toggling the button in the *State* column.
7. Add or remove Collector groups for the policy in the *Collector Group* column.
   (macOS) Users from those Collector groups can then manually disable FileVault (user credentials required) from *Setting* > *FileVault* > *Disable FileVault*. If the Collector is not assigned to the decrypt policy, the disk will be automatically encrypted again even after the user manually disables FileVault.
8. **(macOS)** To verify the disk decryption status, run `sudo fdesetup status` on the endpoint. You can run the command multiple times to see the progress. When the decryption is complete, the status will show that FileVault is off. Decryption speed depends on HD size and Mac model.

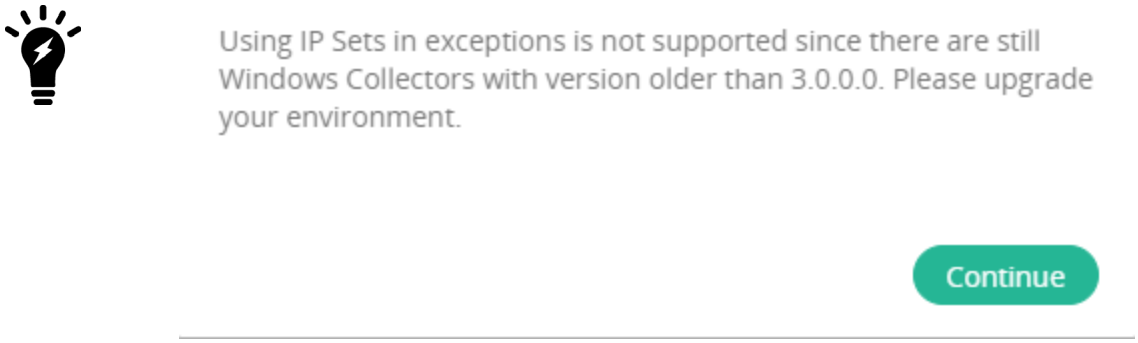
IP sets

IP Sets enable you to define a set(s) of IPs to include or exclude for some security events. This feature is used when defining exceptions.

This page is only available to users with Admin, IT, or Senior Analyst permissions.



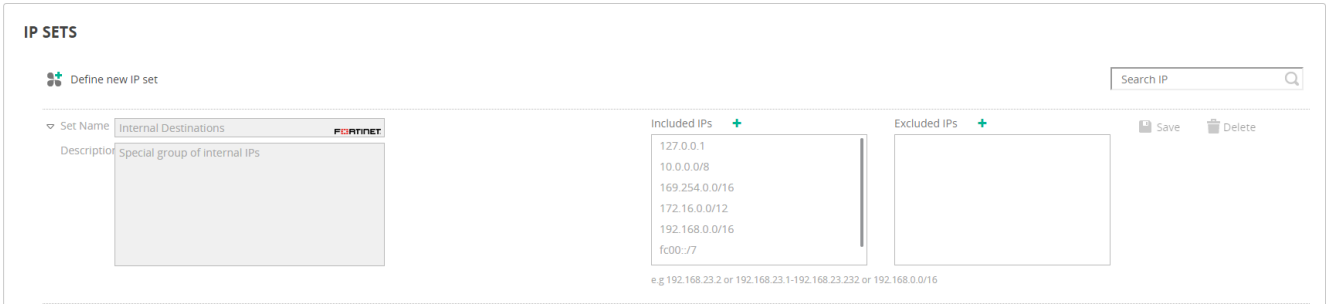
IP Sets can only be defined if all Collectors are V3.0.0.0 and up. If you attempt to define an exception and all Collectors are not V3.0.0.0 or above, the following error message displays:



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 EDR logo), which defines the default IPs that are included in and excluded from the EDR system. All organizations in a multi-organization system are provided with this default IP set. In a single-organization system, the main organization is provided with it. The Internal Destinations IP set cannot be deleted. However, an Administrator can add Included IPs or Excluded IPs to it.

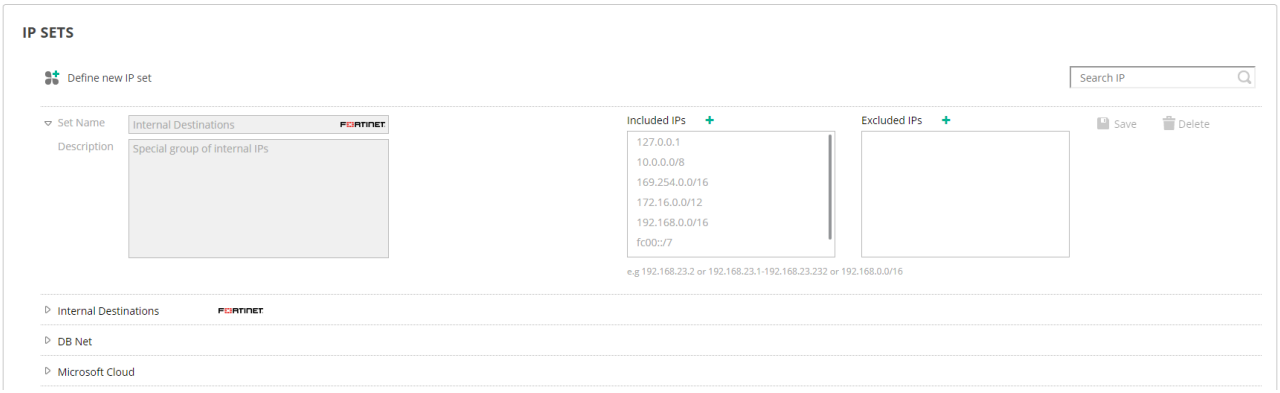
The *IP Sets* page lists all the IP sets. Users can only edit an IP set that was specifically created for his/her organization. For example, if the administrator is assigned to only organization A, he/she can edit an IP set create for organization A but not an IP set that applies to all organizations.

Click the FORTINET logo in the Internal Destinations row to view its definition, as shown below:



To define an IP set:

1. Click the *Define new IP set* button (Define new IP set) button. The following window displays:



2. In the *Set Name* field, enter a name for the IP set.
3. In the *Organization* dropdown list, select the organization to which the IP set applies or select All organizations for the IP set to apply to all organizations in the EDR system.
4. In the *Description* field, enter a description for the IP set.
5. In the *Included IPs* area, click the *Add* button (+) to add an IP, IP range, or IP mask to be included in the IP set's definition. Each click of the *Add* button (+) adds a new line to the list. Each entry appears in its own line. For example, you could add 192.168.23.2, 192.168.23.1-192.168.232 or 192.168.0.0/16. Similarly, in the *Excluded IPs* area, click the *Add* button (+) to add an IP, IP range, or IP mask that is to be excluded.
6. Click the *Save* button.

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

To use an IP set:

Select an IP set in the *Destinations* area when defining an exception.

EDR

Use the *Profiles* > *EDR* tab to configure profiles and exclusions for EDR threat hunting, which features a set of software tools and information sources focused on detecting, investigating, containing, and mitigating suspicious activities on end-user devices.

To set up Threat Hunting in EDR, configure the following:

- Collection profiles on page 723
- Collection Exclusions on page 717
- Threat Hunting data retention on page 725

Collection Exclusions

Exclusions are needed for reducing the amount of Threat Hunting data that is collected and by doing so prolonging the data retention. The less data that is collected, the longer it will be stored in the databases.

Exclusions enable you to define certain types of activity events to be excluded from being collected by Threat Hunting data (even though should be collected according to the Threat Hunting Collection Profile assigned to a Collector group, which was described in Collection profiles on page 723). For example, if you know that a certain process is legitimate, but it creates many activity events that are not relevant to your Threat Hunting investigation, you can use the Collection Exclusions to define that these activities are not collected.

The Collection Exclusions enables you to define and manage exclusion lists and the exclusions that they contain.

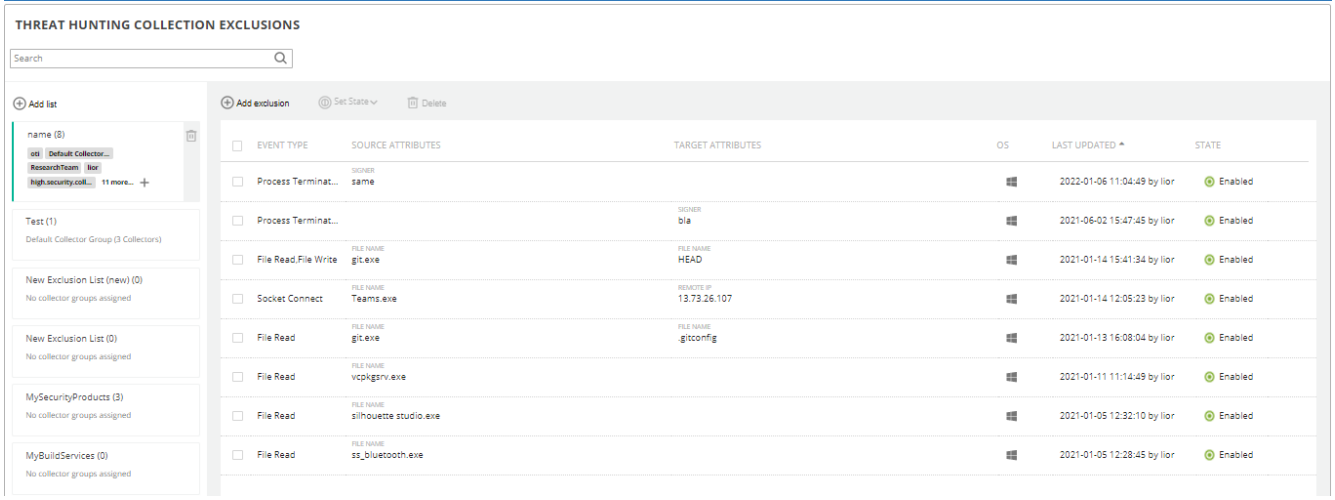


Exclusions are different than security event exceptions, as follows:

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

To access the Collection Exclusions, select *SECURITY SETTINGS* > *Threat Hunting* > *Collection Exclusions*.

The Collection Exclusions page contains the following areas:



Filters

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

Defining Collection Exclusion Lists

A Collection Exclusion List contains a list of exclusions. You can assign Collector Groups to an Exclusion List in order to specify that the exclusions in the Exclusion List apply to the Collectors in the Collector

Groups assigned to it. Exclusion Lists enable you to logically organize, categorize and group exclusions based on the type of activity data they are to exclude.

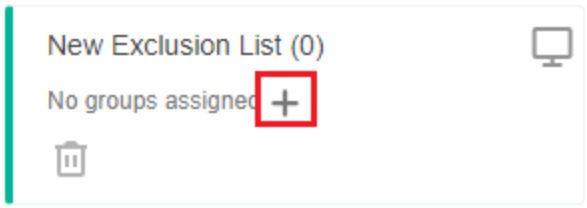
For example, let's say that you want to collect network activity data for your system, but a specific application generates quite a bit of uninteresting logistical network activity that you do not want to collect. In this case, you can define an Exclusion List named after that application that contains one or more exclusions that relate specifically to the network activity generated by that application. Exclusion Lists can be organized anyway you see fit. For example, you can create an Exclusion List for security products, a different one for PDF documents, a different one for HR-related software and so on.

Adding an Exclusion List

To define an Exclusion List:

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

Assigning a Collector Group to an Exclusion List



You can perform the following operations on an Exclusion List:

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

Defining Collection Exclusions

All exclusions must belong to an Exclusion List. Select an Exclusion List on the left to display the exclusions that are defined in it.

Exclusions can be defined for a

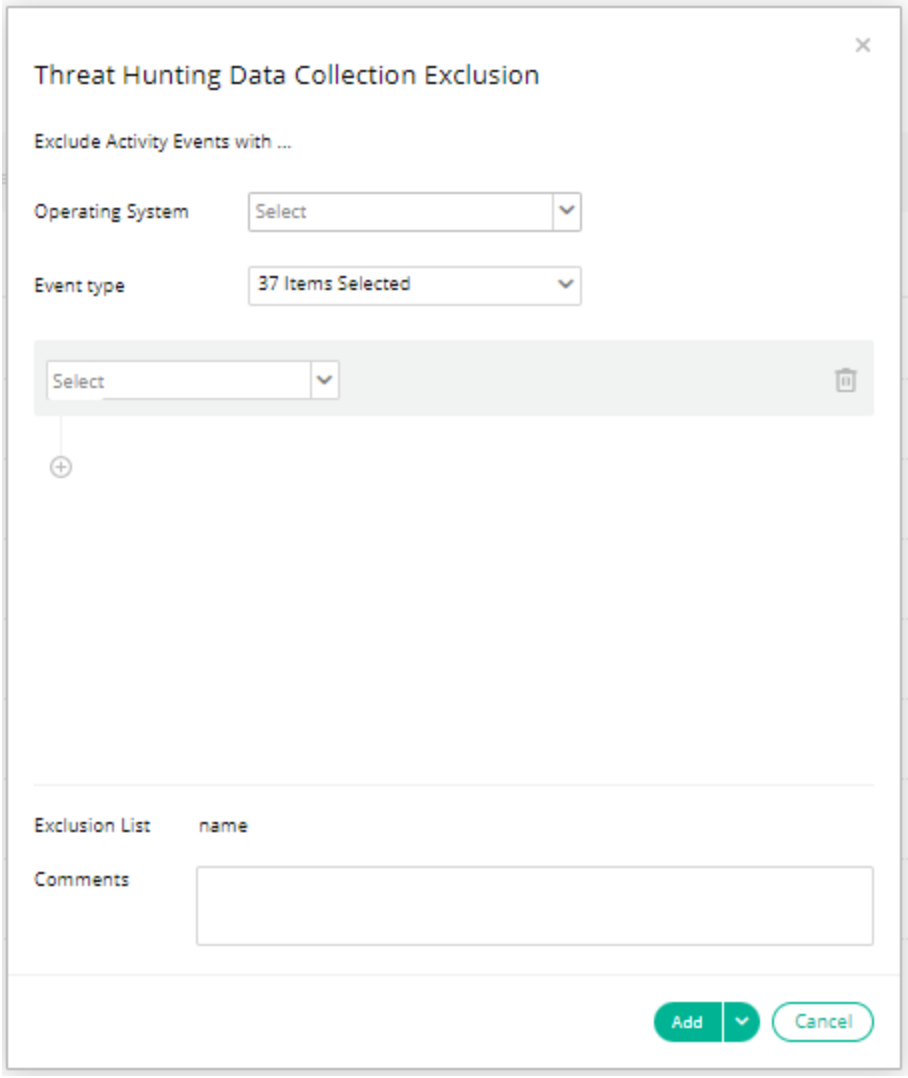
- **Source (process)** – Which is identified by a source attribute, such as a Signer.
- **Type/Action** – Activity event types, as described in Threat Hunting on page 608.
- **Target** – Which is identified by a target attribute, such as IP & Port.

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

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

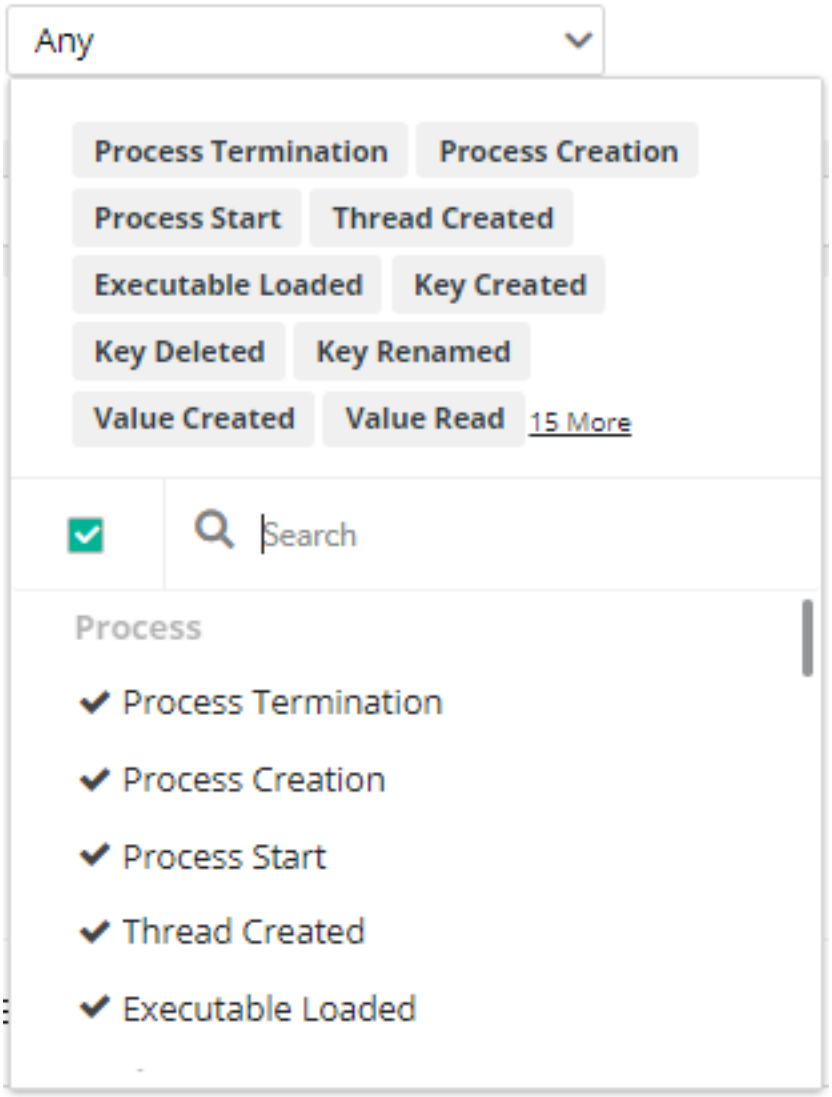
Adding an Exclusion

1. In the left pane, click the Exclusion List to which to add the exclusion.
2. In the right pane, click the *+ Add Exclusion* button. The following displays:

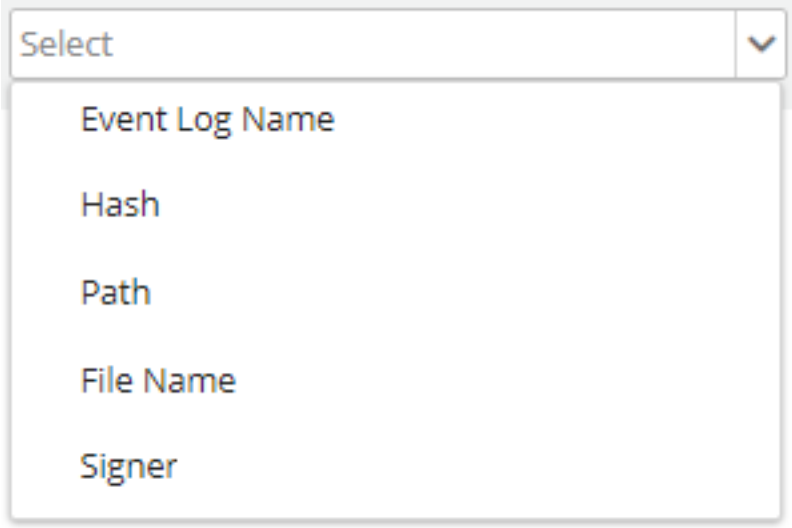


3. From the *Operating system* dropdown menu, select the OS, such as *Windows*.
4. To define that an exclusion includes a specific Activity Event Type, select the type of action(s) to exclude from the displayed dropdown list. Alternatively, select the Any option (the default option),

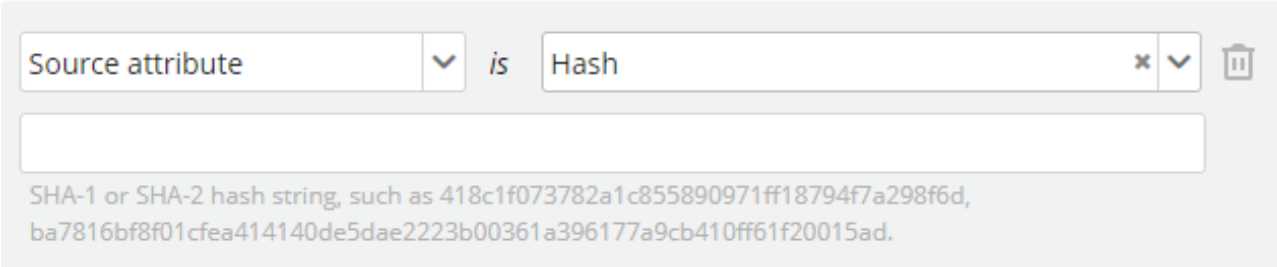
which means that you are not specifying a specific action type.
All action types to be collected are listed according to Category. You can select one or more actions from a single Category. Actions cannot be selected from different categories. For example, you can select the *Process Termination* and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



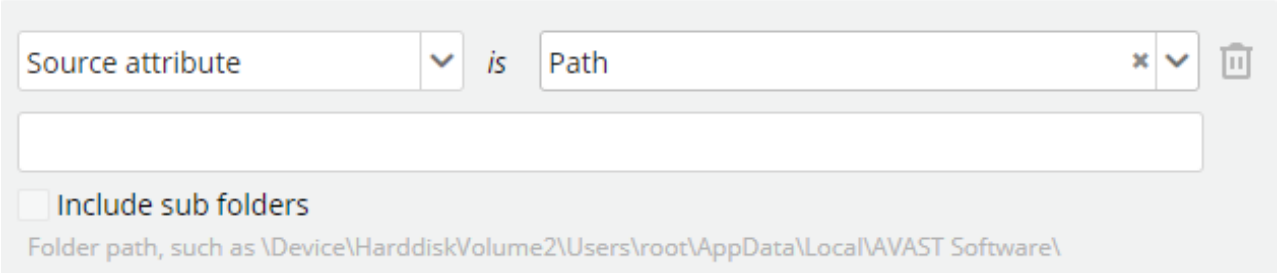
5. To define that an exclusion includes a *Source* attribute condition, from the *Select* box, select *Source attribute*, which can be identified by file name, path, hash and signer for Source Process or Event Log Name for event log related activity events, as shown below:



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

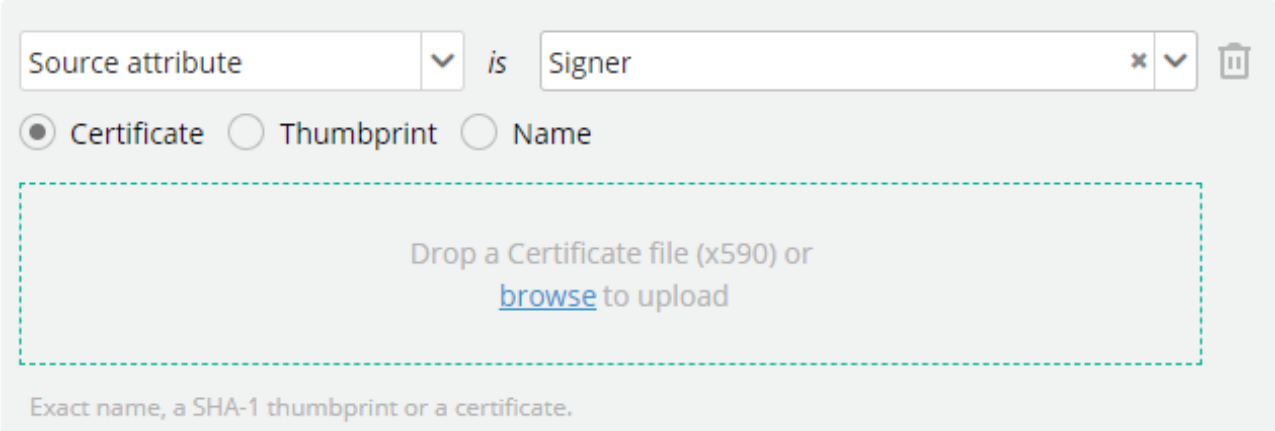


If you select *Path*, then specify the *Path*, as shown below. A path can include wild cards. If you wish to include sub-folders as well, check the *Select sub folders* checkbox.



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

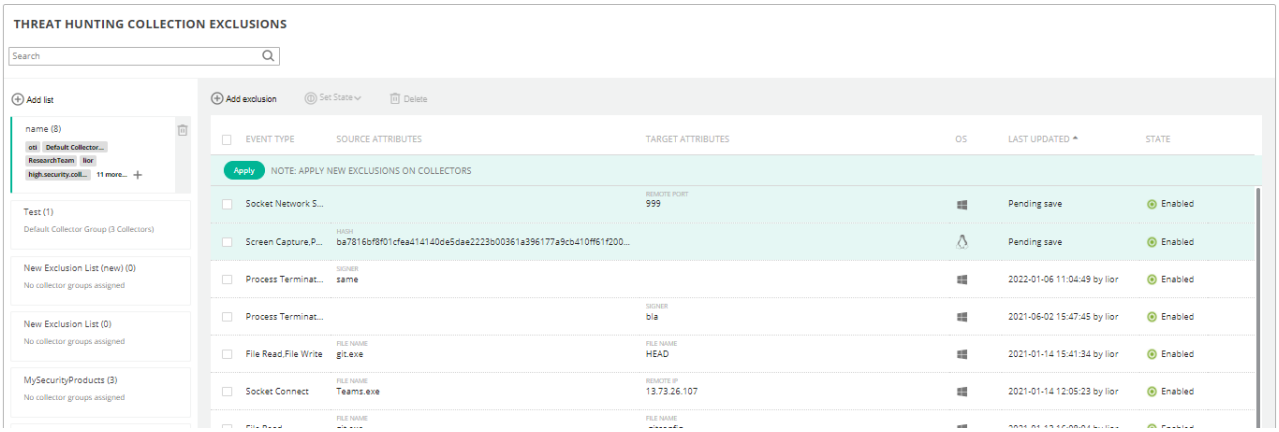
If you select Signer, then either upload the Signer's Certificate, provide its thumbprint or provide the Signer's name.



6. To define that an exclusion includes a *Target* attribute condition, click the *+* button. From the *Select* box, select the *Target Attribute* and then define the target criteria, as described below:
   Targets can be identified by various criteria, depending on the selected Activity Event Category.
   - A process Category event is identified by hash, path, file name or Signer.
   - A network Category event is identified by network-related properties, such as a remote IP and port.
   - A registry Category event is identified by a registry key path, value name, value type or value size.
   - An Event log Category event is identified by the Event Log ID.

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

   Note: If an OR relationship is needed between the conditions that you define, simply create another exclusion.
7. Click the *Add* button. This new exclusion is then listed in the Collection Exclusions page, as shown below:



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

Setting the state of an Exclusion

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

Deleting an Exclusion

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

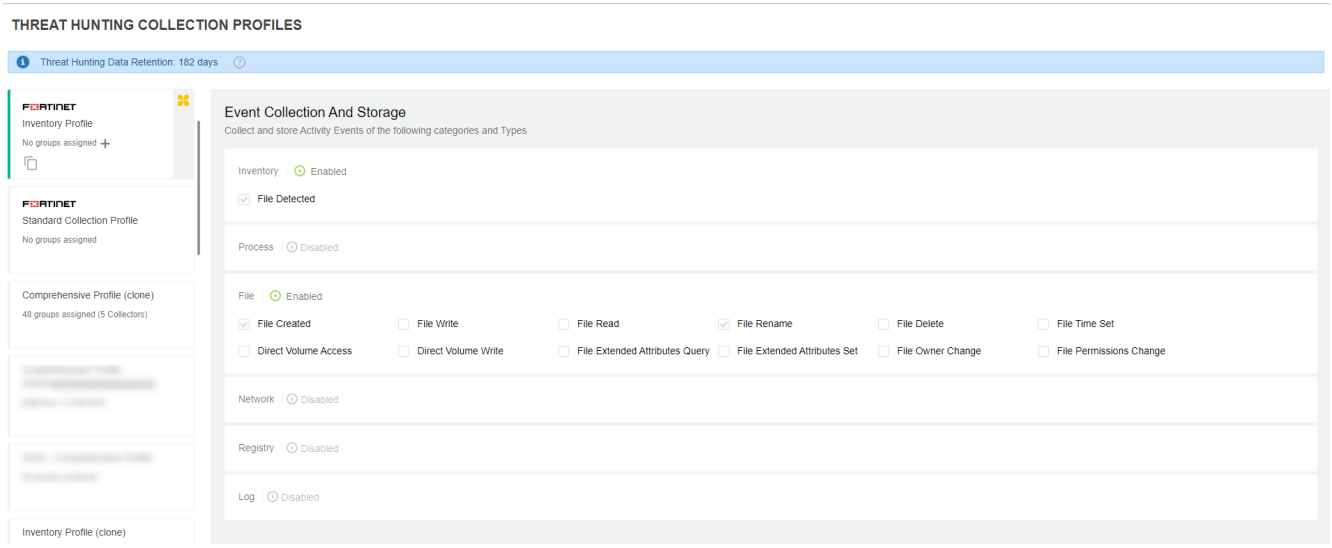
To delete multiple exclusions, check the requested exclusions checkboxes and click *Delete* in the toolbar.

Collection profiles

Threat Hunting Collection Profiles control the type of activity data that is collected for the Threat Hunting feature (which is described in Threat Hunting on page 608). Activity data that is collected is stored on the Repository server.

To access Threat Hunting settings, select *Profiles* > *EDR* > *Collection profiles on page 723*.

The following page displays:



The left side of the page shows a list of profiles. A profile defines the activity event categories and actions to be collected. EDR comes with several predefined profiles, which cannot be modified. In addition to the pre-defined profiles, you can define your own custom profiles by cloning an existing profile.

The default collection profile for Collector groups is *Inventory Profile*, which is indicated by the *Default Collection Profile* ( ) icon). To change the default profile, hover over to the top-right corner of the target profile card and click the *Set profile as the default profile* ( ) icon.

You can also assign a collection profile to one or more Collector groups. See Assigning a Collector group to a profile on page 723.

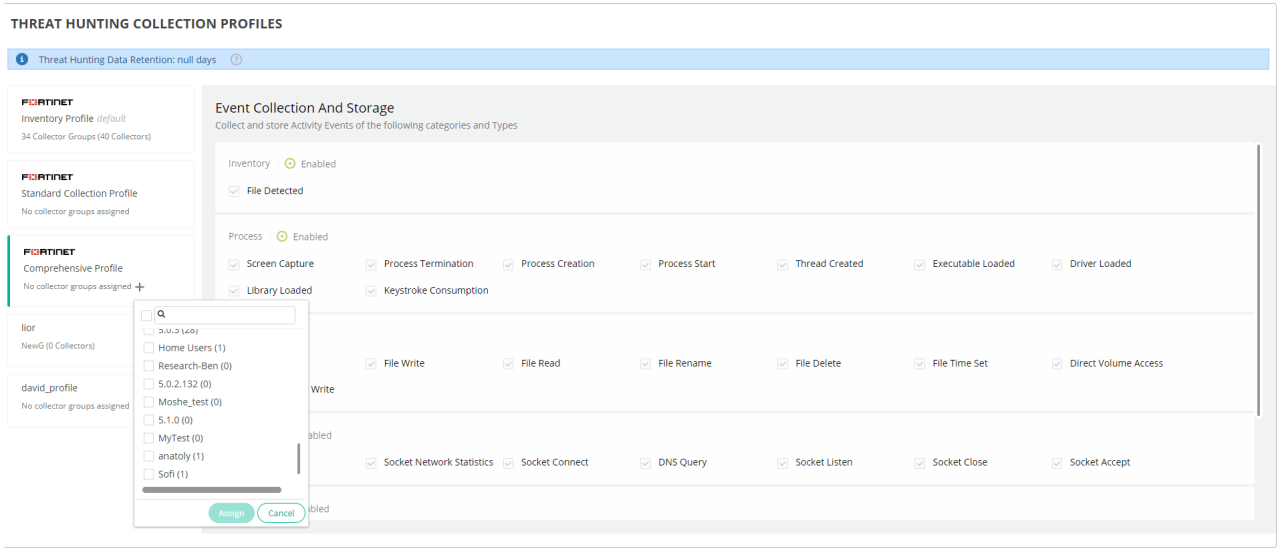
The pane on the right side of the page lists all activity event categories and their associated actions. These categories are the same as those described on Threat Hunting on page 608. Selecting a profile on the left displays the categories and actions defined for that profile in the right pane. Check the checkboxes of the actions for which EDR will collect activity data.

Assigning a Collector group to a profile

Profiles are assigned to Collector groups. Only a single profile can be assigned to each Collector group.

To assign a Collector group to a profile:

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

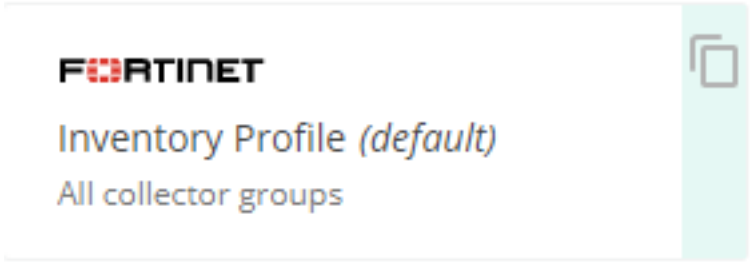


2. Select the checkbox(s) of the Collector group(s) to assign to the profile.
3. Click *Assign*.
4. When prompted with a message that the selected groups are currently assigned to another profile and will be reassigned, click *Assign* to confirm.

Creating/cloning a profile

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

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



2. Enter the name of the new profile.
3. On the right side, enable the activity events to be collected and disable the activity events that should not be collected.
4. Click *Save*.
5. Assign the Collector group(s) on which to apply the newly created profile.

Threat Hunting data retention

Because the size of the Threat Hunting Repository database is limited, the data that is written to it is overwritten in a cyclical manner when it gets full.

Therefore, the amount of time that the data is retained is dependent upon –

- The size of the repository database.
  – AND –
- The amount of data that is collected.

The amount of data that is collected is dependent upon –

- The Threat Hunting Data Collection Profiles, which is defined in *Profiles > EDR > Collection Profiles*
  – AND –
- The Threat Hunting Data Collection Exclusions, which is defined in *Profiles > EDR > Collection Exclusions*

In order to extend the data retention period, you can –

Reduce the amount of data that is collected, by either defining the Collection Profiles (so that they collect less data) or defining more Collection Exclusions (so that they exclude more data), as described above.

Regarding Threat Hunting Collection Profiles, switching from the Inventory Scan Profile typically reduces data retention by at least 50% and switching to the Comprehensive Profile typically reduces data retention by an additional 50%.

To see an estimate of the Threat Hunting data retention:

Select *Profiles > EDR > Collection Profiles*. The data retention period is displayed in the top left corner.

Integrations

Connectors enable you to configure connectors to external systems, which enables you to trigger predefined types of actions. EDR provides various connectors out-of-the-box, such as Firewalls and NAC systems. The out-of-the-box EDR connectors utilize Fortinet products' APIs to automatically perform the required actions in order to extend its automatic Playbook actions.

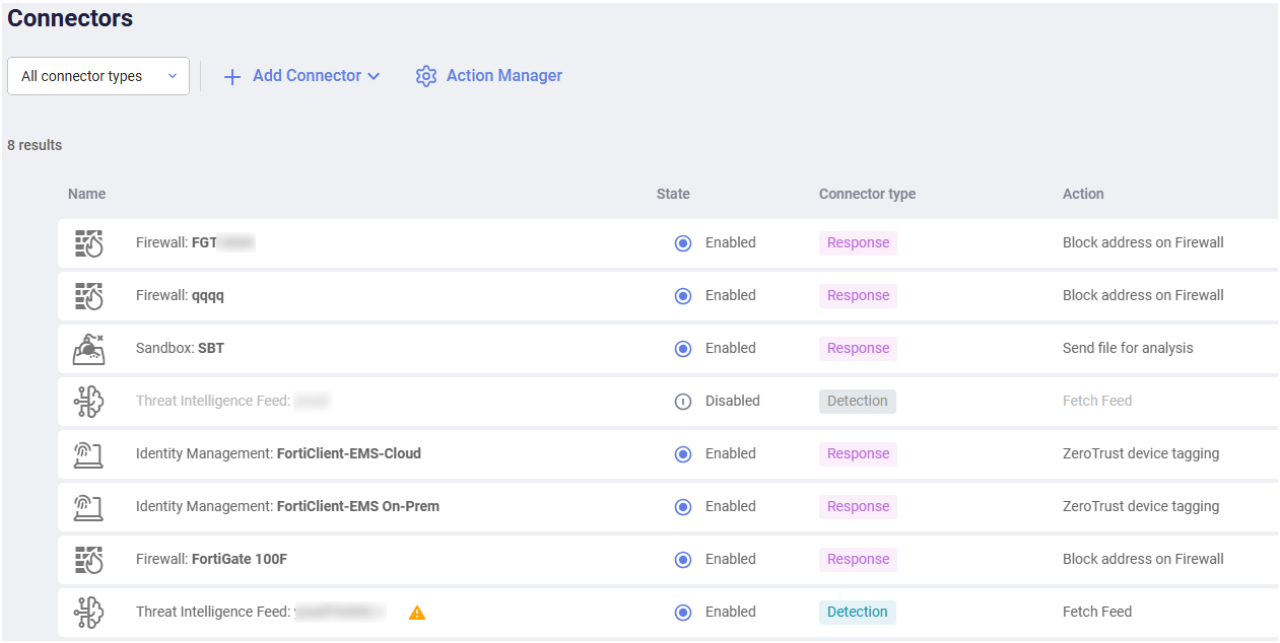
You can set up an unlimited number of connectors for each type and use them by associating Playbook policies or Security policies to the actions defined for these integration connectors, as described below.



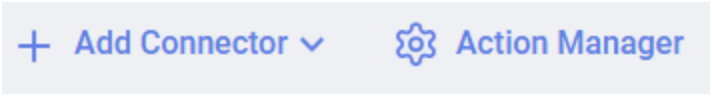
The *Connectors* menu is only available when the environment is connected to Fortinet Cloud Services (FCS).

To display the *Connectors* page:

1. Select *Profiles* > *Integrations* > *Connectors*.



The top left of this page provides two buttons, as shown below:



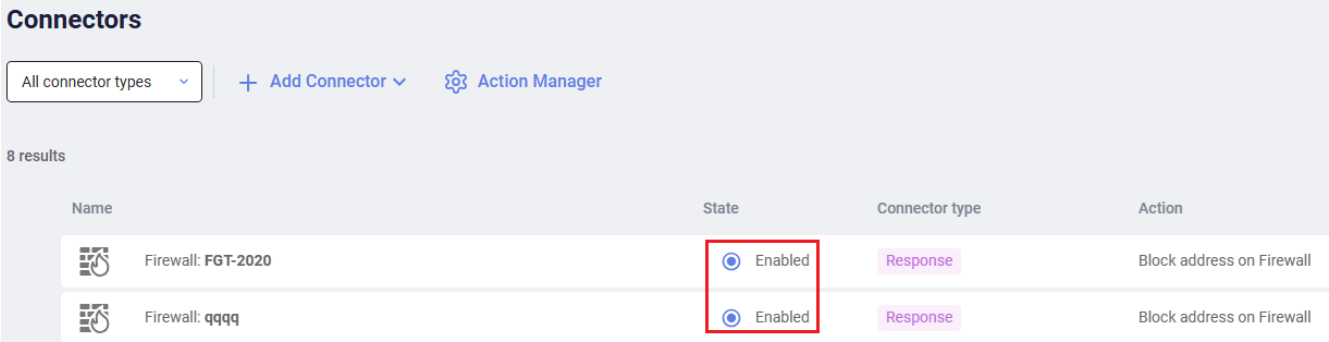
- Adding connectors on page 726 enables you to add and configure connectors for integration with EDR.
- Action Manager on page 777 enables you to upload and manage (add, modify and delete) actions (Python scripts that call third-party system APIs) to be automatically triggered by EDR as incident responses. Python 2.7 or later is supported.

Adding connectors

The following types of integration connectors are provided to be configured:

- Firewall integration on page 727
- Network Access Control (NAC) integration on page 735
- Sandbox integration on page 755
- eXtended detection source integration on page 757
- Custom integration on page 770
- Identity Management integration on page 741
- User Access integration on page 748
- Threat Intelligence Feed integration on page 775

You can enable or disable a connector by clicking the *Enabled/Disabled* button next to the connector name. This button toggles between *Enabled/Disabled*.



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, verify the following:

- You have installed an EDR Core and configured the Core as a Jumpbox with connectivity to the firewall. To request the EDR Core ISO, contact Fortinet Support.
- You have a valid API user with access to the external firewall. See Configuring FortiGate or Configuring FortiManager for detailed instructions about configuring FortiGate or FortiManager for the integration.

Follow the steps below to automatically deny access on the firewall to malicious destination addresses detected by EDR.

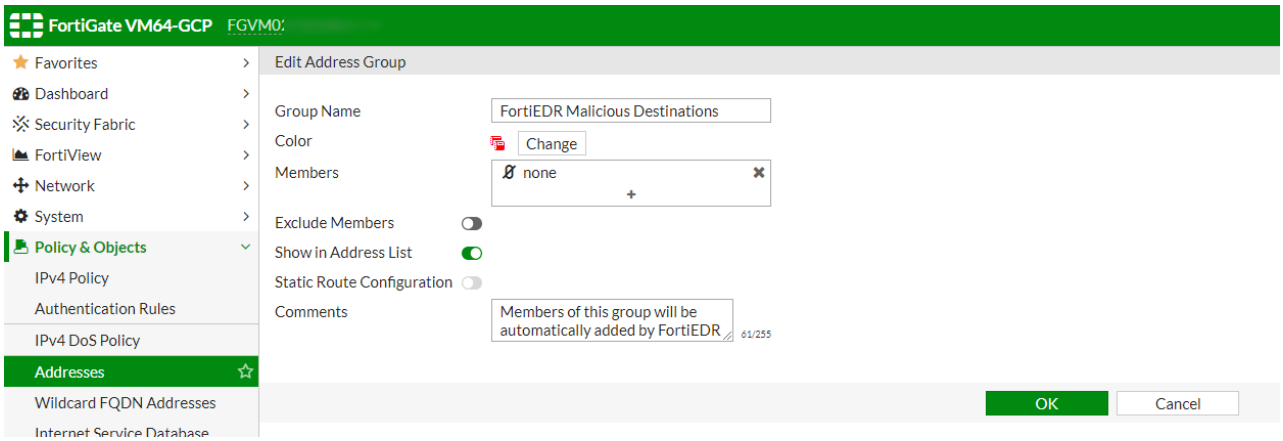
The example below describes how to define an address group on FortiGate and associate it with a FortiGate policy rule, such that it blocks connections to the addresses in the group. The address group is then used when configuring the EDR connector so that it is automatically populated with malicious destinations upon detection by EDR.

The same address group can obviously be used for multiple firewall policies in order to cover any VLAN-to-WAN interface in the network.

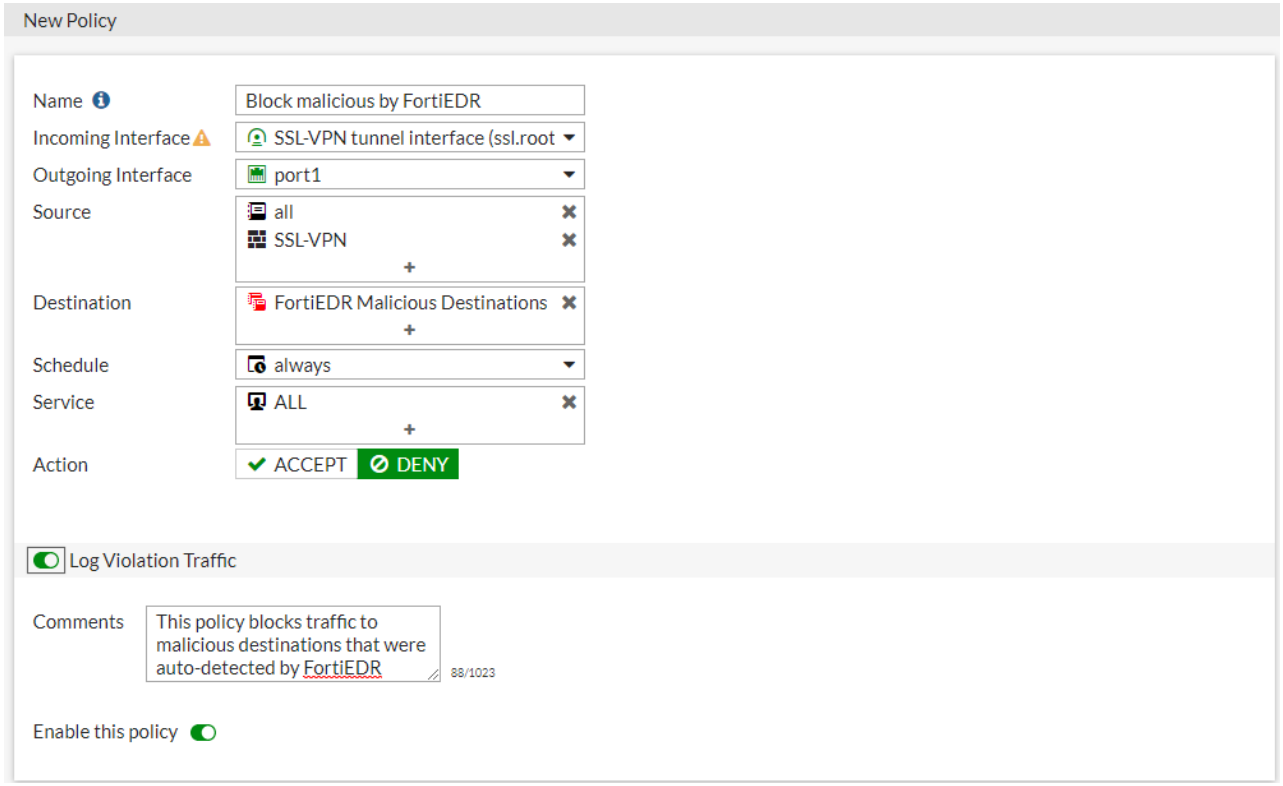
FortiGate configuration

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 EDR. The new address group now appears in the FortiGate Addresses table.



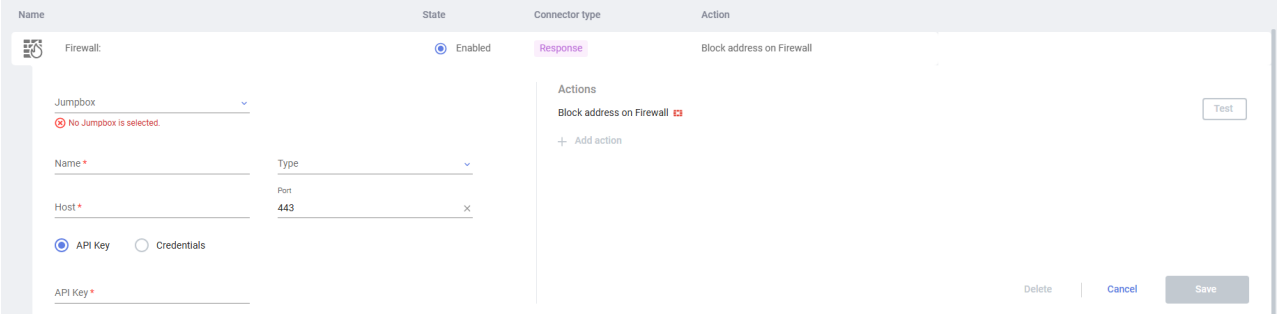
3. Go to *Policy & Objects* > *IPv4 Policy*.
4. Create a new policy to deny traffic to any address in the address group that was created as part of step 2. The new policy now appears in the FortiGate Policies table.



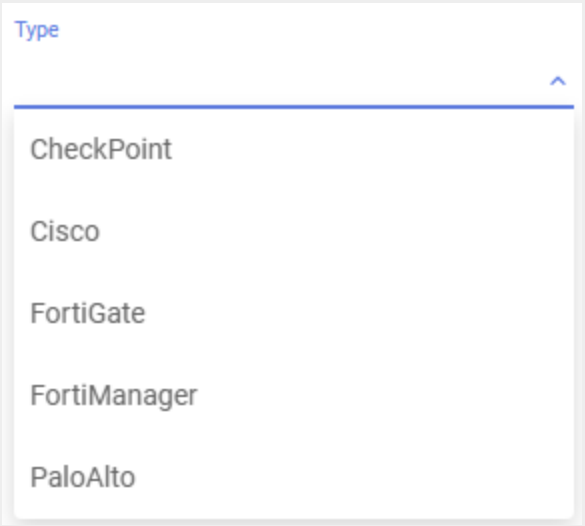
EDR firewall connector configuration

To set up a Firewall connector with EDR:

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

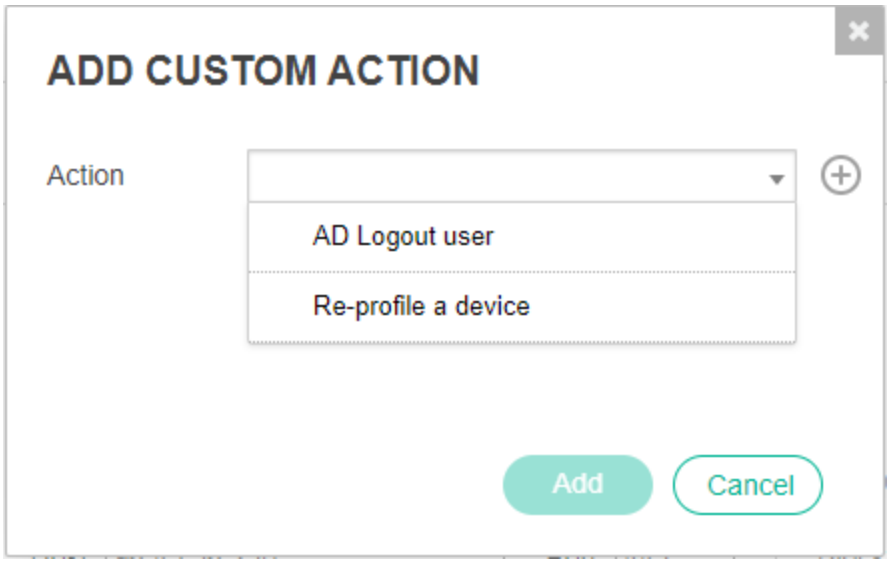


2. Fill in the following fields:

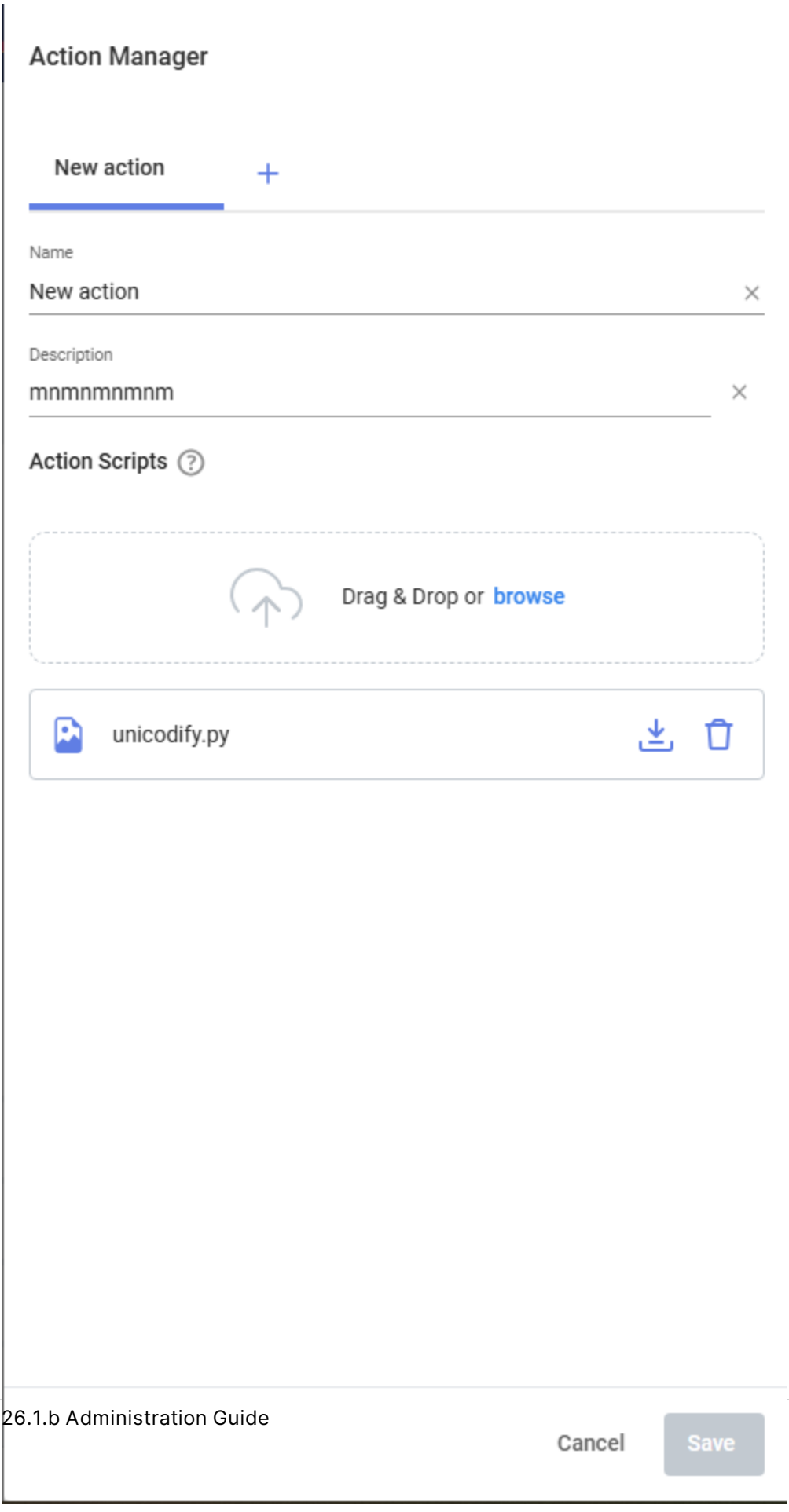
Field	Definition
Jumpbox	Select the EDR Jumpbox to communicate with the firewall.
Name	Specify a name of your choice to be used to identify this firewall.
Type	Select the type of firewall to be used in the dropdown list. 
Host	Specify the IP or DNS address of your firewall.
Port	Specify the port that 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.

3. In the *Actions* area on the right, define an action to be taken by this connector.
   You have the option to either use an action provided out-of-the-box with EDR (for example, *Block address on Firewall*) or to create and use your own custom actions.
   a. To block an address on the Firewall, in the *Address Group* field, specify the name of a previously defined address group on the firewall. For FortiManager and FortiGate integrations, you can optionally specify the name of the VDOM domain in the *VDOM* field. EDR uses the default root VDOM if the *VDOM* field is empty.
      - OR -

b. To trigger a custom action on the Firewall, click the *Add Action* button to display the following popup window:



- In the *Action* dropdown menu, select one of the previously defined custom integration actions (which were defined in EDR as described in Custom integration on page 770).
  – OR –
- Click the *Create New Action* button in this popup window to define a new action on the Firewall to be triggered according to the definitions in the Playbook, as described below. The following displays:

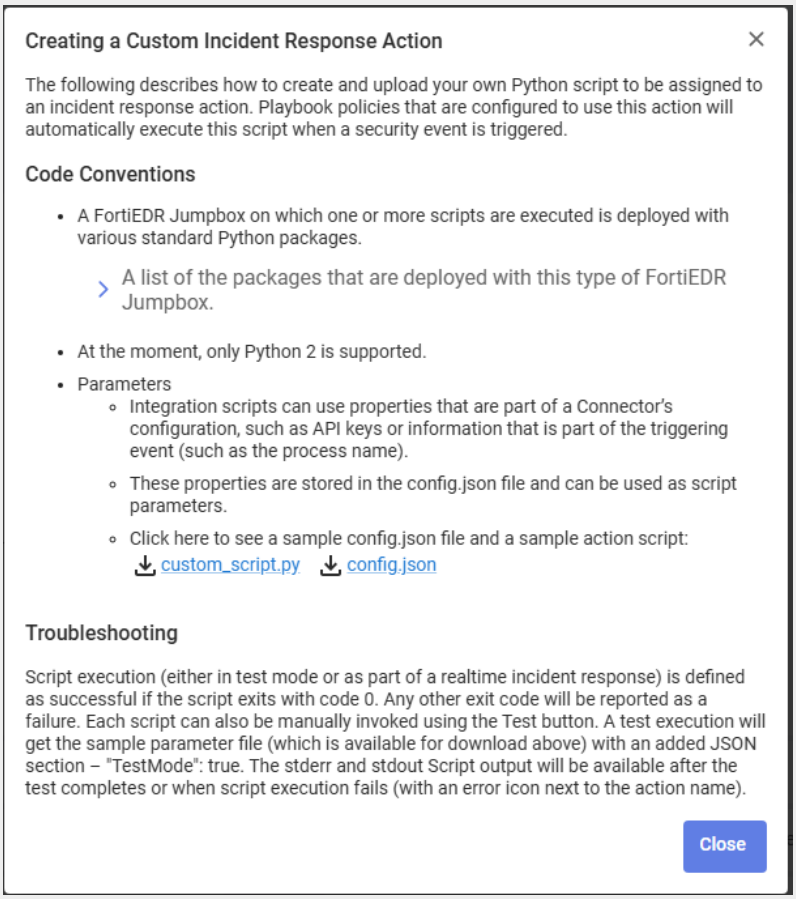

Action Manager
New action
Name
New action
Description
mnmnmnmnm
Action Scripts
Drag & Drop or browse
unicodify.py
Cancel
Save

Fill out the fields of this window as follows in order to define a new action to be triggered in response to an incident.



In order to trigger this action, a Playbook policy must be defined that triggers this action to execute the script when a security event is triggered. The definition of this new action here automatically adds this action as an option in a Playbook policy. This action however, is not selected by default in the Playbook policy. Therefore, you must go to the Playbook policy and select it in order for it to be triggered when a security event is triggered.

Field	Definition
Name	Enter any name for this action.
Description	Enter a description of this action.
Upload	Upload a Python script that calls an API in the third-party system in order to perform the relevant action. Python 2.7 or later is supported. This Python script must be created according to the coding conventions that can be displayed by clicking the icon next to the *Action Scripts* field. The following displays providing an explanation of these coding conventions and provides various links that you can click to see more detail and or/to download sample files.

Field	Definition
	

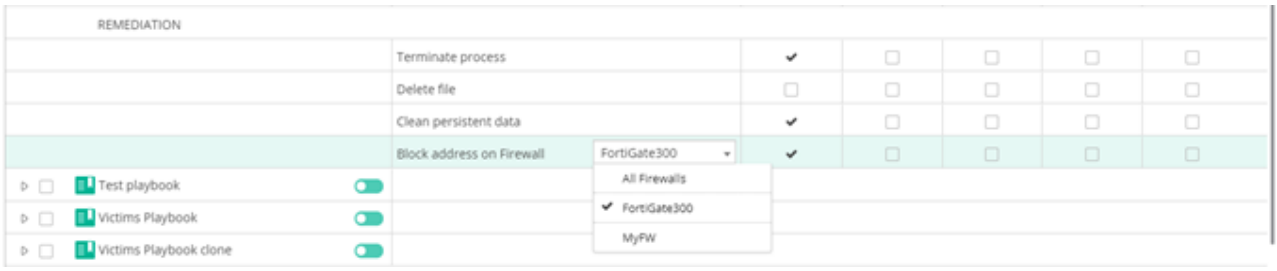
4. Click *Save*. The new action is then listed in the *Actions* area.
5. You can click the *Test* button next to an action to execute that action.

If you are working with a FortiManager in order to manage firewalls, use the same instructions to integrate with the firewall, but select *FortiManager* as the integrated device Type when configuring the EDR Connector in the *Profiles* > *Integrations* > *Connectors* page.

Playbooks configuration

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

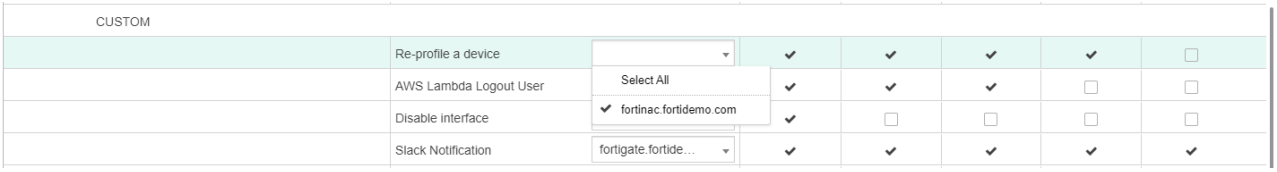
1. Navigate to the *Profiles* > *Playbooks* page.
2. Open the Playbook policy that is applied on devices for which you want the block IP incident response to apply and place a checkmark in the relevant *Classification* column next to the *Block address on Firewall* row that is under the *REMEDIATION* 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:



EDR 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 EDR security events.

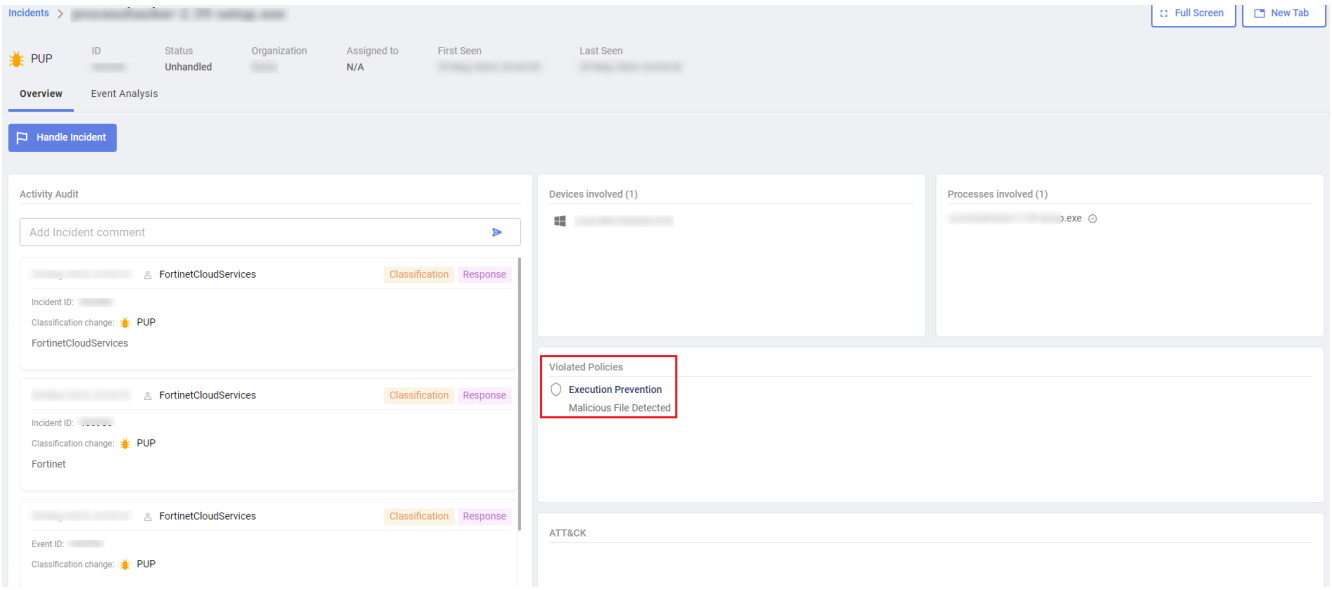
To configure an automated incident response that uses a firewall connector to perform a custom action upon the triggering of a security event:

1. Navigate to the *Profiles* > *Playbooks* page.
2. Open the Playbook policy that is applied on devices for which you want the custom action (defined above) to apply.
3. In the *CUSTOM* section, place a checkmark in the relevant *Classification* columns next to the row of the relevant custom action.
4. In the dropdown menu next to the relevant custom action, select the relevant firewall connector with which to perform the action, as shown below:



EDR is now configured to trigger this action in the third-party system upon the triggering of a security event.

Automatic incident response actions are listed in the *Overview* tab when you select the incident and click *Investigate* in the *Incidents* pane, as shown below:



Network Access Control (NAC) integration

When a Network Access Control connector such as FortiNAC is set and Playbook policies are configured, automatic incident response actions can include isolating a device by a NAC system upon security event triggering.

Before you start NAC configuration, verify the following:

- You have installed an EDR Core and configured the Core as a Jumpbox with connectivity to the NAC server. To request the EDR Core ISO, contact Fortinet Support.
- You have a valid API user with access to FortiNAC or equivalent network access control system. See Configuring FortiNAC for detailed instructions about creating a FortiNAC admin user.

Follow the steps below in order to automatically isolate a device by NAC upon the detection of an EDR security event. The example below describes how to define an API user on FortiNAC in order to enable EDR to perform automatic device isolation after an EDR security event.

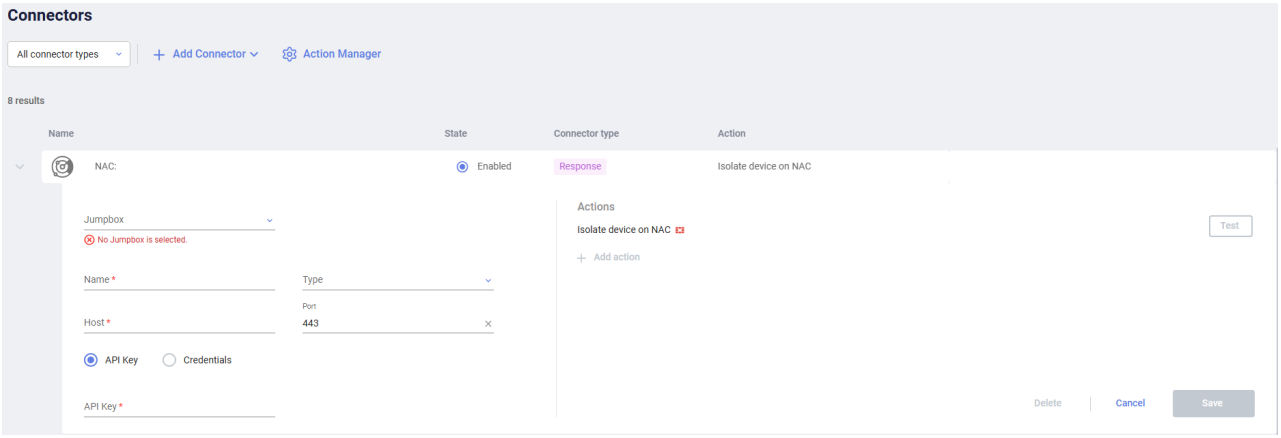


Make sure to add EDR domains and/or IP addresses to the exclusion list on the VLAN that is being used for isolation on the FortiNAC system such that the EDR Collector would still be able to communicate with its servers when the device is being isolated.

EDR Connector configuration

To configure NAC integration:

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



2. Fill in the following fields:

Field	Definition
Jumpbox	Select the EDR 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:

Field	Definition
	FortiNAC.
Host	Specify the IP or DNS address of the external NAC system.
Port	Specify the port that is used for communication with the external NAC system.
API Key	Specify authentication details of the external NAC system. To use an API token, click the API Key radio button and copy the token value into the text box. To use API credentials, click the *Credentials* radio button and fill in the external NAC system API username and password.

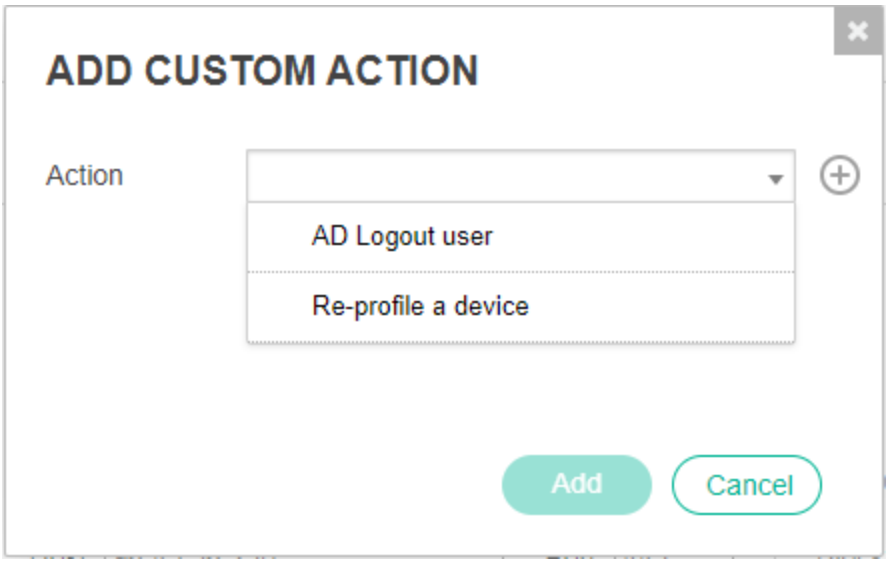
3. 3 In the *Actions* area on the right, define the action to be taken by this connector.

You have the option to either use an action provided out-of-the-box with EDR (for example, *Isolate Device on NAC*)

– OR –

To create or select one of the Custom Integration actions (if one or more have already been defined in EDR, as described in Custom integration on page 770.

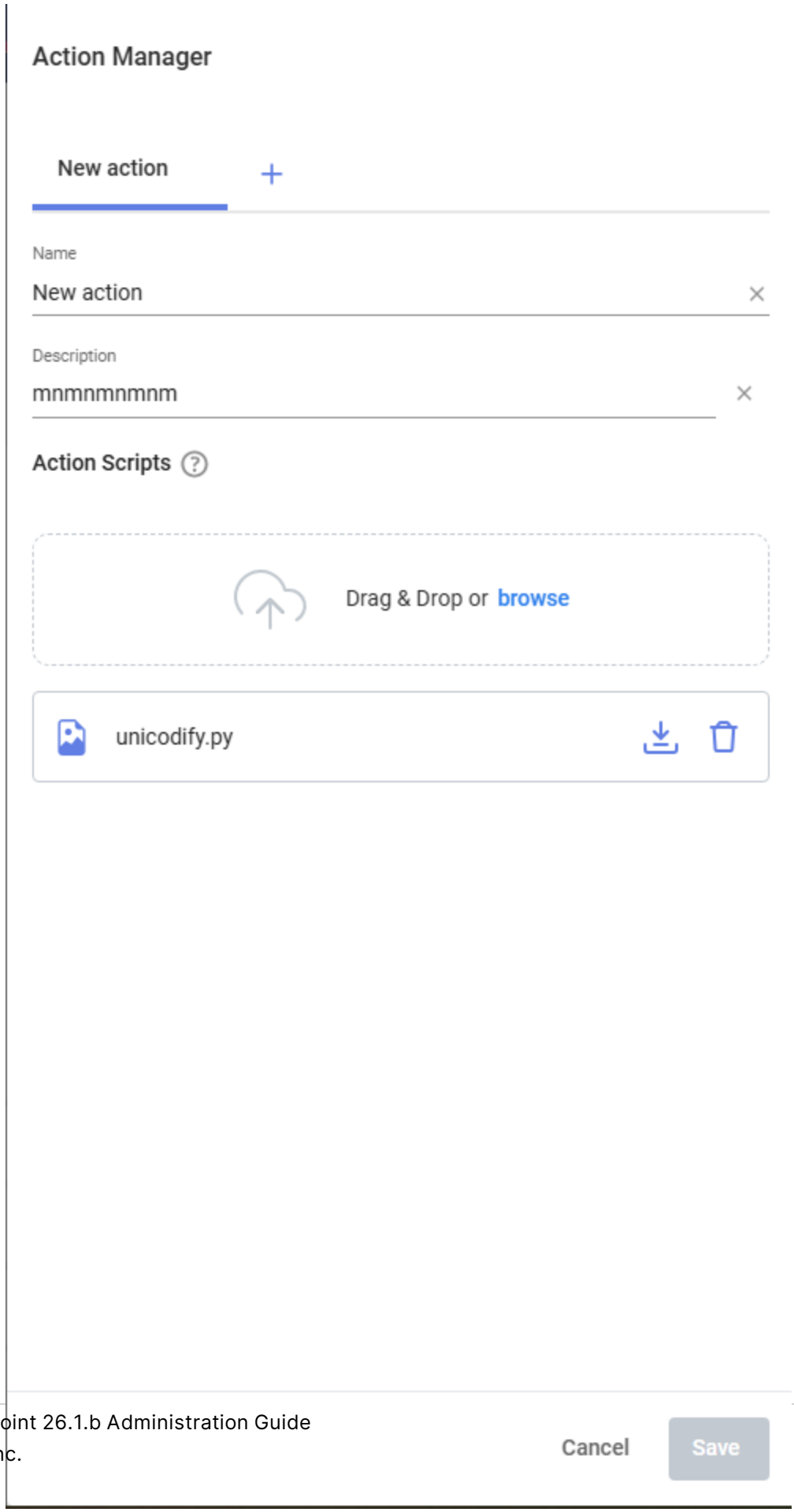
- To trigger an action on a custom connected third-party system, click the *+ Add Action* button to display the following popup window:



a. In the *Action* dropdown menu, select one of the previously defined actions (which were defined in EDR as described in Custom integration on page 770).

- OR -

b. Click the *Create New Action* ⊕ button in this popup window to define a new action that can be triggered according to the definitions in the Playbook, as described below. The following displays:

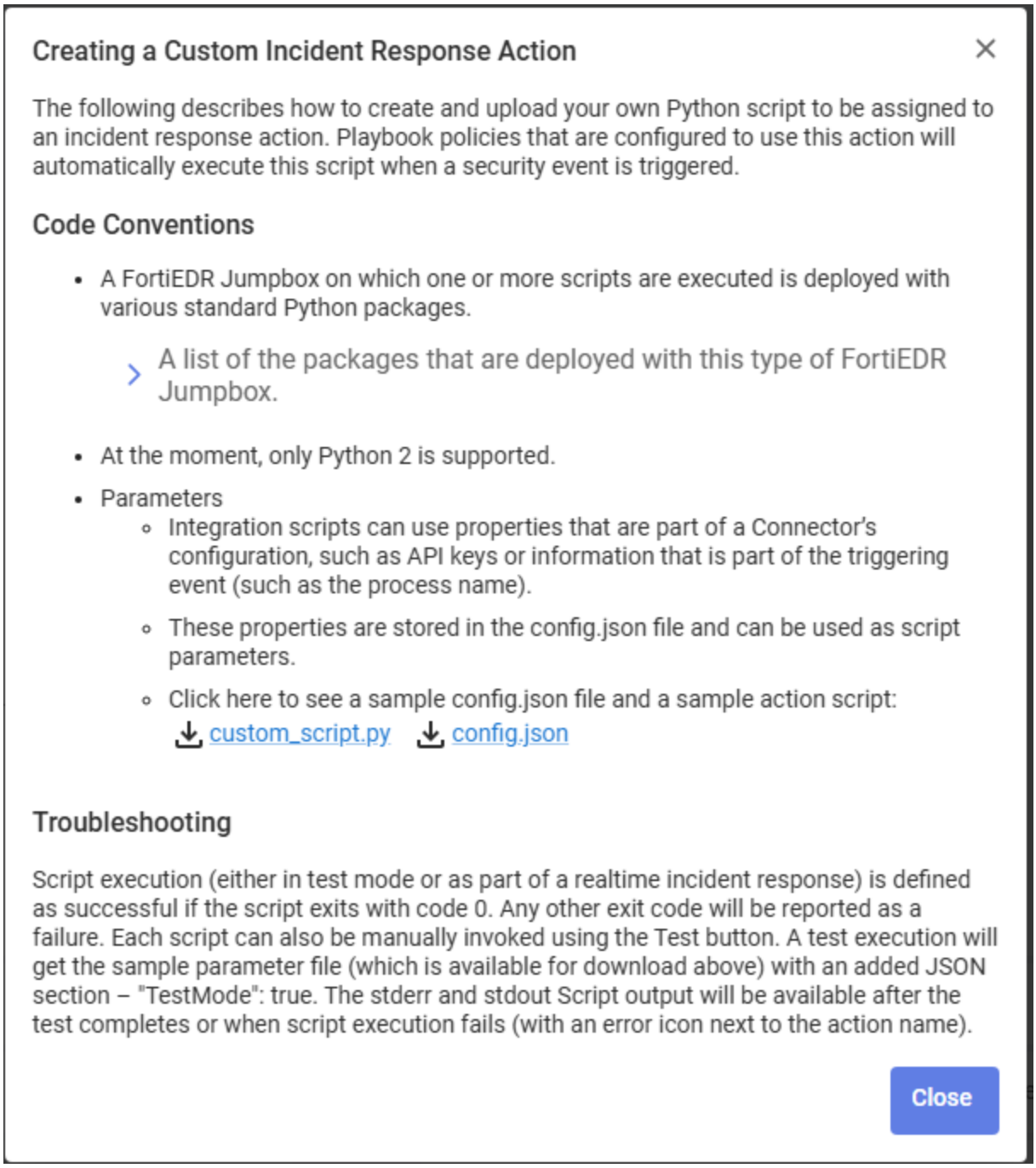

Action Manager
New action
Name
New action
Description
mnmnmnmnm
Action Scripts
Drag & Drop or browse
unicodify.py
Cancel
Save

Fill out the fields of this window as follows in order to define a new action to be triggered in response to an incident.



In order to trigger this action, a Playbook policy must be defined that triggers this action to execute the script when a security event is triggered. The definition of this new action here automatically adds this action as an option in a Playbook policy. This action however, is not selected by default in the Playbook policy. Therefore, you must go to the Playbook policy and select it in order for it to be triggered when a security event is triggered.

Field	Definition
Name	Enter any name for this action
Description	Enter a description of this action
Upload	Upload a Python script that calls an API from the third-party system in order to perform the relevant action. Python 2.7 or later is supported. This Python script must be created according to the coding conventions that can be displayed by clicking the icon next to the *Action Scripts* field. The following displays providing an explanation of these coding conventions and provides various links that you can click to see more detail and/or to download sample files.

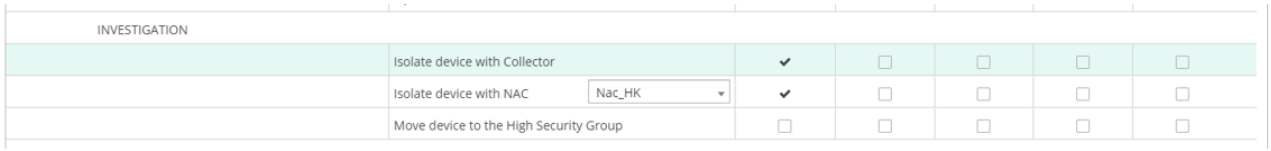


4. Click *Save*. The new action is then listed in the Actions area.
5. You can click the *Test* button next to an action to execute that action.

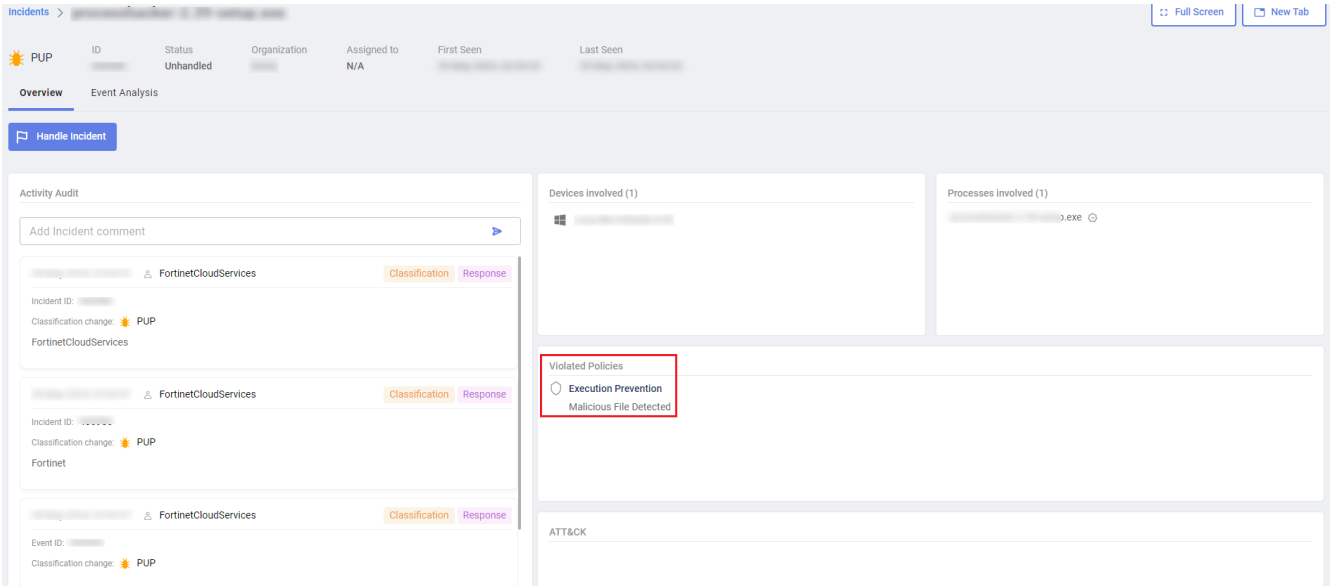
Playbooks configuration

To configure an automated incident response that uses a NAC connector to isolate a device upon security event triggering:

1. Navigate to the *Profiles* > *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.



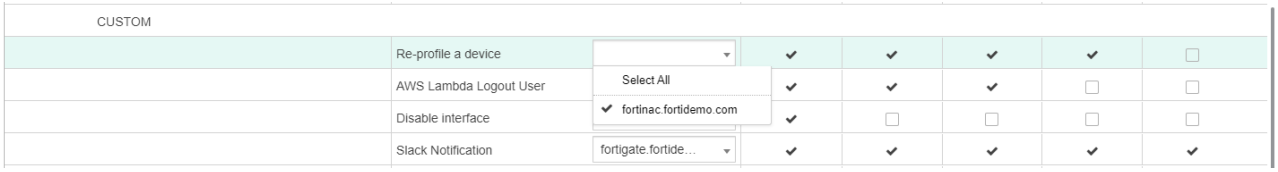
EDR is now configured to automatically isolate the device upon triggering of a security event. Automatic incident response actions are listed in the *Overview* tab when you select the incident and click *Investigate* in the *Incidents* pane, as shown below:



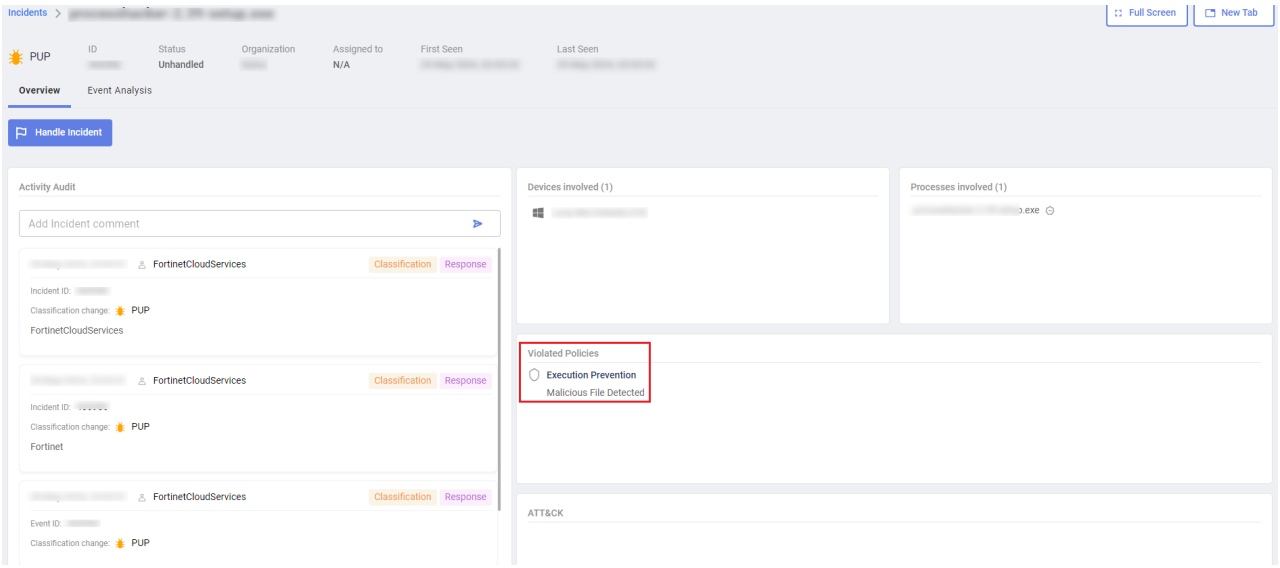
Note that isolation by NAC will only be done for devices that are managed on the specified NAC.

To configure an automated incident response that uses a NAC connector to perform a custom action upon the triggering of a security event:

1. Navigate to the *Profiles* > *Playbooks* page.
2. Open the Playbook policy that is applied on devices for which you want the custom action (defined above) to apply.
3. In the *CUSTOM* section, place a checkmark in the relevant *Classification* columns next to the row of the relevant custom action.
4. In the dropdown menu next to the relevant custom action, select the relevant NAC connector with which to perform the action, as shown below:



EDR is now configured to trigger this action in the third-party system upon the triggering of a security event. This automatic incident response action appears in the*Overview* tab when you select the incident and click *Investigate*.



Identity Management integration

When an Identity Management connector, such as FortiClient Endpoint Management Server (EMS), is set and Playbook policies are configured, automatic incident response actions can include ZeroTrust device tagging on FortiClient EMS upon security event triggering.

Prerequisites

Before you start Identity Management configuration, verify the following:

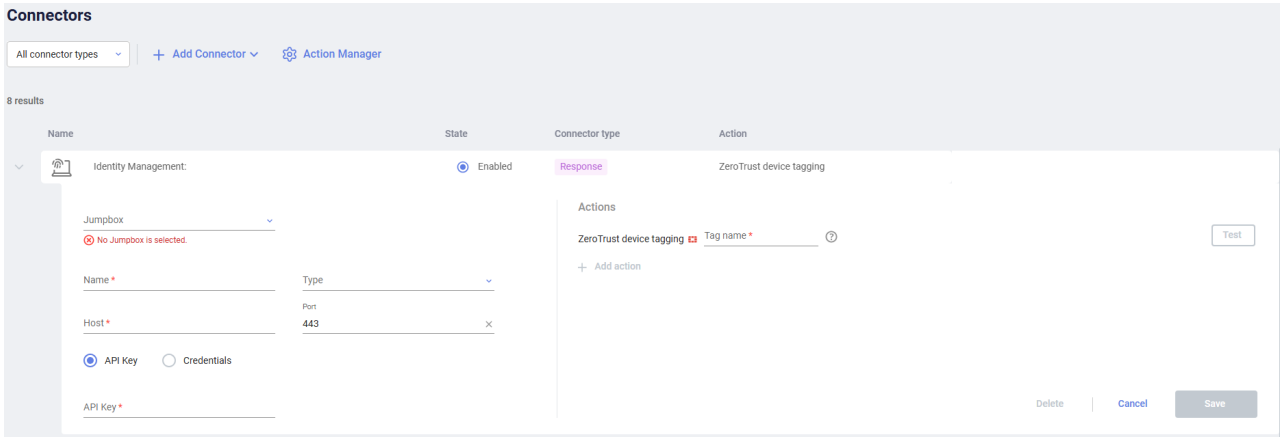
- You have installed an EDR Core and configured the Core as a Jumpbox with connectivity to the identity management server. To request the EDR Core ISO, contact Fortinet Support.
- You have a valid user with access to the identity management system. For FortiClient EMS, the following type of user is required depending on the deployment type:
  - **FortiClient EMS On-Premise**—A valid API user. See Configuring FortiClient EMS on-premise for detailed instructions.
  - **FortiClient EMS Cloud**— FortiCloud master user (e.g. email address) with read/write access to the FortiClient EMS Cloud portal. Sub user accounts cannot be used. See the FortiCloud IAM documentation for detailed instructions about creating a permission profile and an API user.

Follow the steps below to tag a device as non-trusted automatically upon the detection of an EDR security event.

Configuring an EDR Connector

To configure Identity Management integration:

1. Click the *Add Connector* button and select *Identity Management* from the dropdown list. The following displays:

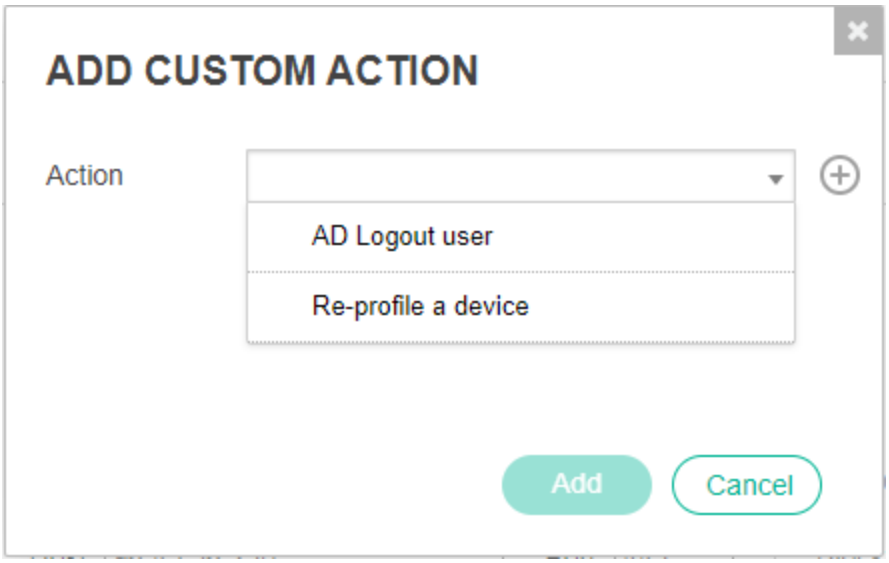


2. Fill in the following fields:

Field	Description
Jumpbox	Select the EDR Jumpbox that will communicate with this Identity Management system.
Name	Specify a name of your choice to be used to identify this Identity Management system.
Type	Select the type of Identity Management to be used in the dropdown list. For example, *FortiClient EMS*.
Host	Specify the IP or DNS address of the external Identity Management system.
Port	Specify the port that is used for communication with the external Identity Management system.
API Key/Credentials	Specify authentication details of the external Identity Management system. Fill in the external Identity Management system API username/Account and password/key. For FortiClient EMS, specify the following depending on your deployment type: • **(FortiClient EMS on-premise)** Specify the username and password of the FortiClient EMS Admin User. • **(FortiClient EMS cloud)** Specify the account (e.g. email address) and password of the FortiCloud master user with read/write access to the FortiClient EMS Cloud portal. Sub user accounts cannot be used.

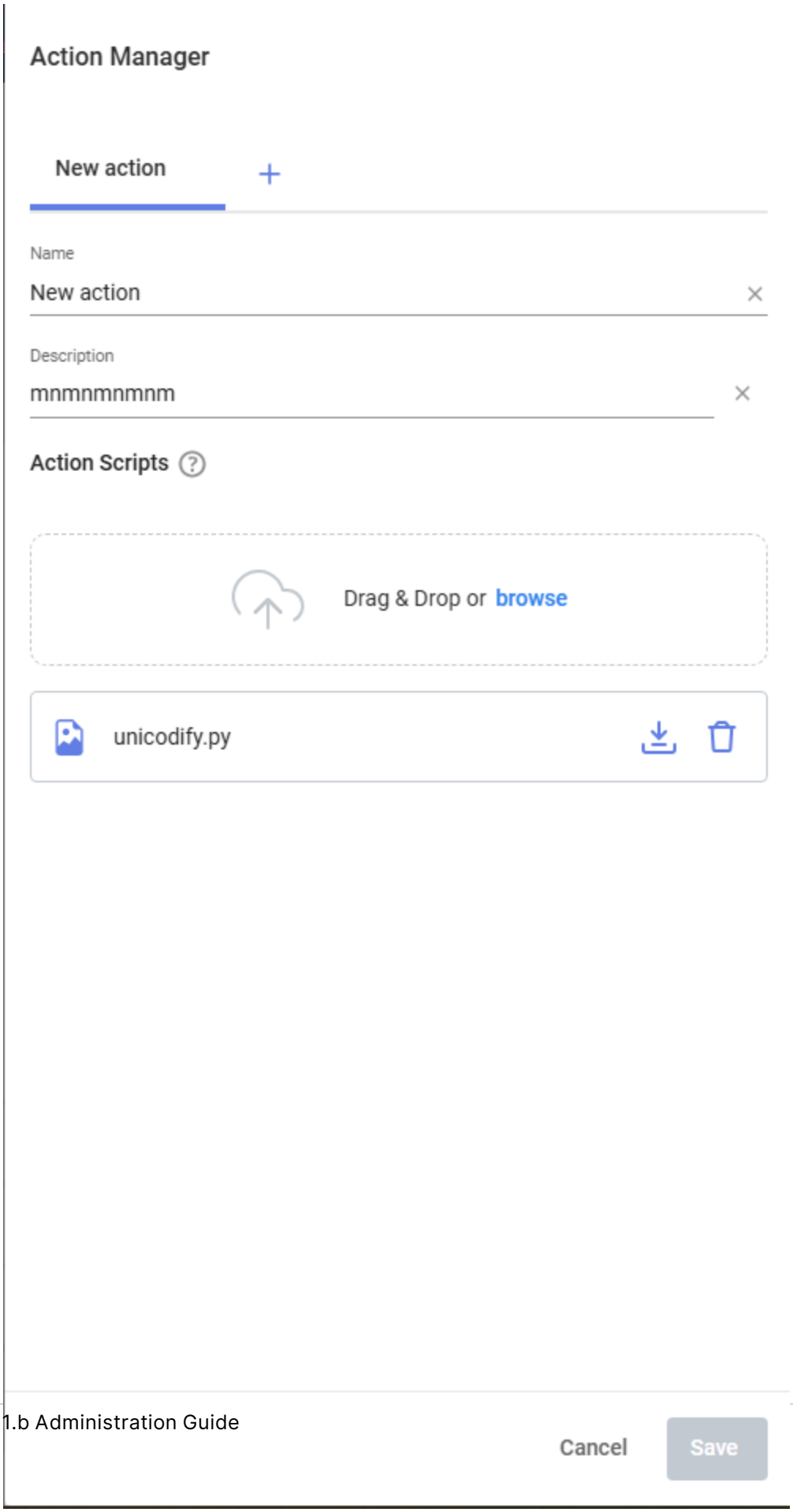
3. In the *Actions* area on the right, define the action to be taken by this connector:
   - To use an action provided out-of-the-box with EDR (for example, Zero Trust device tagging on FortiClient EMS), tag the device as non-trusted the Identity management system and specify the classification tag to apply on the device in the *Tag name* field.
     This step is optional for FortiClient EMS 7.2 or later as it has the following fabric tags predefined for EDR. Both the predefined fabric tags and classification tags, if any, will be used by FortiClient EMS 7.2 or later to tag the device.
     - **FortiEDR_Malicious**: EDR has classified this endpoint as malicious.
     - **FortiEDR_PUP**: EDR has detected a potentially unwanted program on this endpoint.
     - **FortiEDR_Suspicious**: EDR has detected suspicious activity on this endpoint.
     - **FortiEDR_Likely_Safe**: EDR has detected this endpoint as likely to be safe.
     - **FortiEDR_Probably_Good**: EDR has determined that this endpoint is not a safety risk.

     See the FortiClient EMS Administration Guide for more information about endpoint tagging in FortiClient EMS.
   - To use a custom integration action:
     i. Click the *+ Add Action* button. The following popup window displays:



     ii. In the *Action* dropdown menu, select one of the previously defined actions (which were defined in EDR as described in Custom integration on page 770), or define a new action that can be triggered according to the definitions in the Playbook:

i. Click the *Create New Action* button. The following displays:

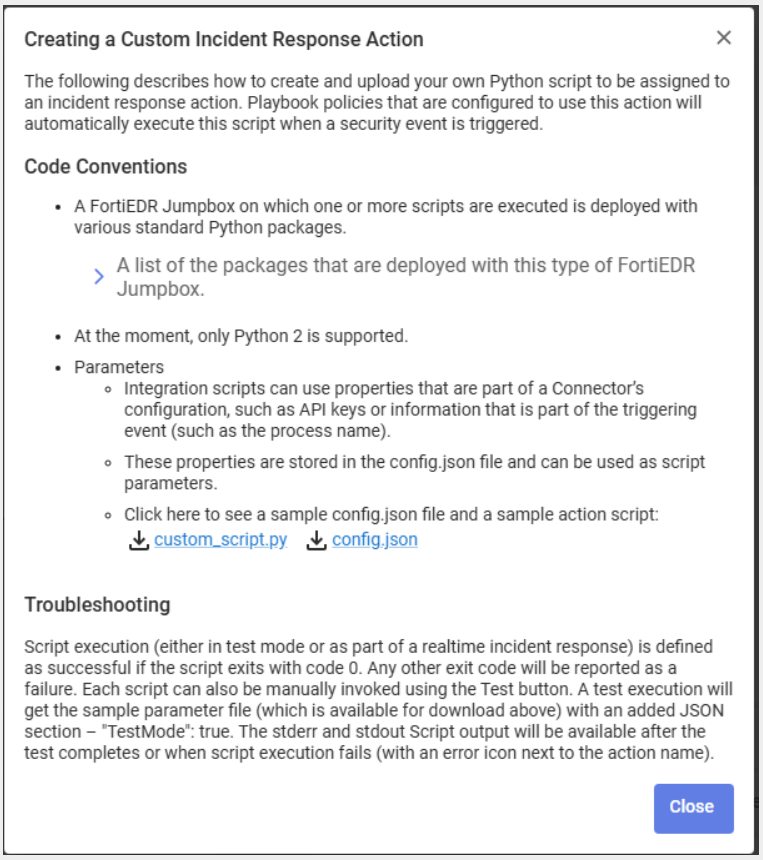

Action Manager
New action
Name
New action
Description
mnmnmnmnm
Action Scripts
Drag & Drop or browse
unicodify.py
Cancel
Save

ii. Fill out the fields of this window as follows in order to define a new action to be triggered in response to an incident.



In order to trigger this action, a Playbook policy must be defined that triggers this action to execute the script when a security event is triggered. The definition of this new action here automatically adds this action as an option in a Playbook policy. However, this action is not selected by default in the Playbook policy. Therefore, you must go to the Playbook policy and select it in order for it to be triggered when a security event is triggered.

Field	Definition
Name	Enter any name for this action.
Description	Enter a description of this action.
Upload	Upload a Python script that calls an API from the third-party system in order to perform the relevant action. Python 2.7 or later is supported. The Python script must be created according to the coding conventions that can be displayed by clicking the icon next to the *Action Scripts* field. The following displays providing an explanation of the coding conventions and provides various links that you can click to see more detail and/or to download sample files.

Field	Definition
	

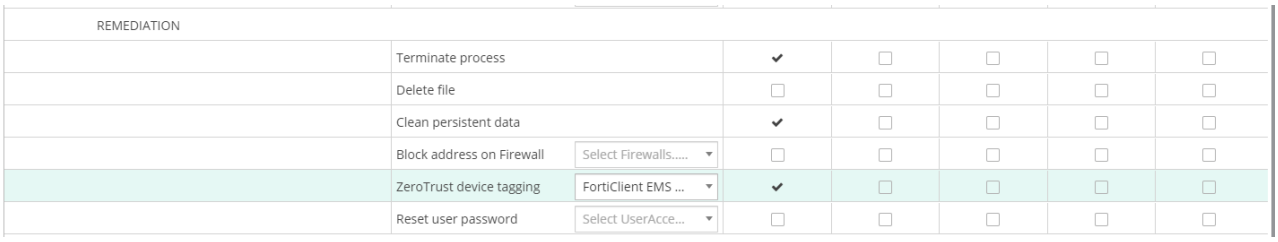
iii. Click *Save*. The new action is then listed in the *Actions* area.

4. You can click the *Test* button next to an action to execute that action.
5. Click *Save* to save the connector configuration.

Configuring Playbooks

To configure an automated incident response that uses an Identity Management connector to tag a device upon security event triggering:

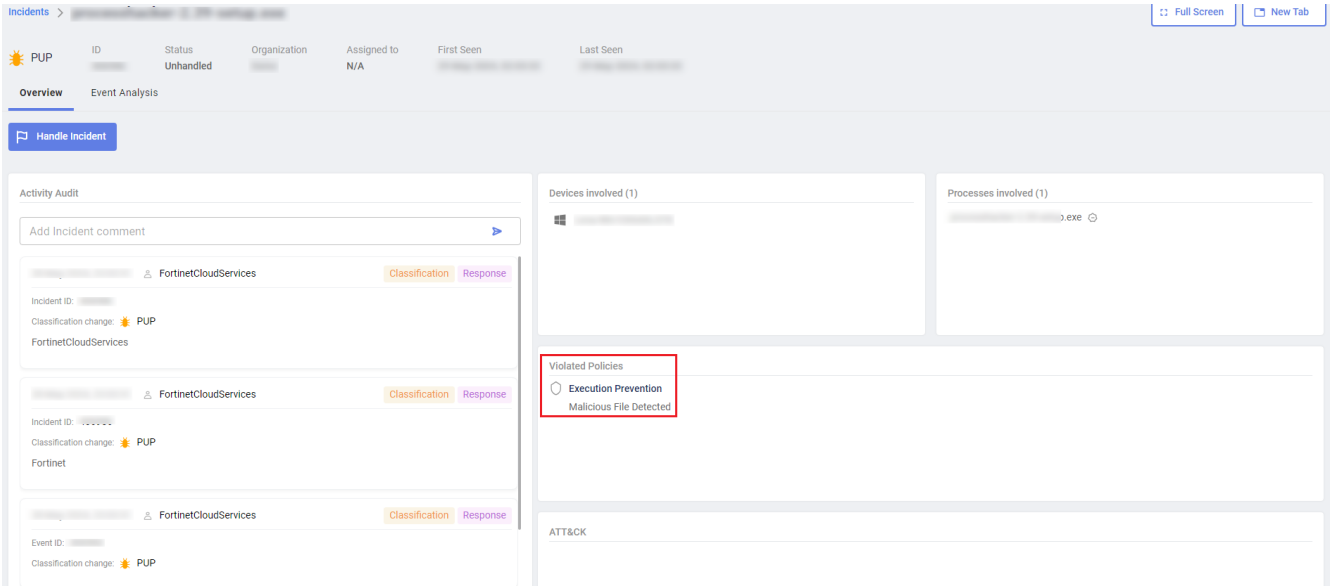
1. Navigate to the *Profiles* > *Playbooks* page.
2. Open the Playbook policy that is applied on devices for which you want the identity management response to apply.
3. Place a checkmark in the relevant *Classification* column next to the *Zero Trust device tagging* row under the *REMEDIATION* section.
   EDR is now configured to automatically tag a device as non-trusted upon triggering of a security event.



To configure an automated incident response that uses an Identity Management connector to perform a custom action upon the triggering of a security event:

1. Navigate to the *Profiles* > *Playbooks* page.
2. Open the Playbook policy that is applied on devices for which you want the custom action (defined above) to apply.
3. In the *CUSTOM* section, place a checkmark in the relevant *Classification* columns next to the row of the relevant custom action.
4. In the dropdown menu next to the relevant custom action, select the relevant Identity Management connector with which to perform the action.
   EDR is now configured to trigger this action in the third-party system upon the triggering of a security event.

Automatic incident response actions are listed in the *Overview* tab when you select the incident and click *Investigate* in the *Incidents* pane, as shown below:



User Access integration

When a user access connector, such as Active Directory, is set and Playbook policies are configured, automatic incident response actions can include resetting user's password or disabling user account on domain controller upon security event triggering.

Prerequisites

Before you start User Access configuration, verify the following:

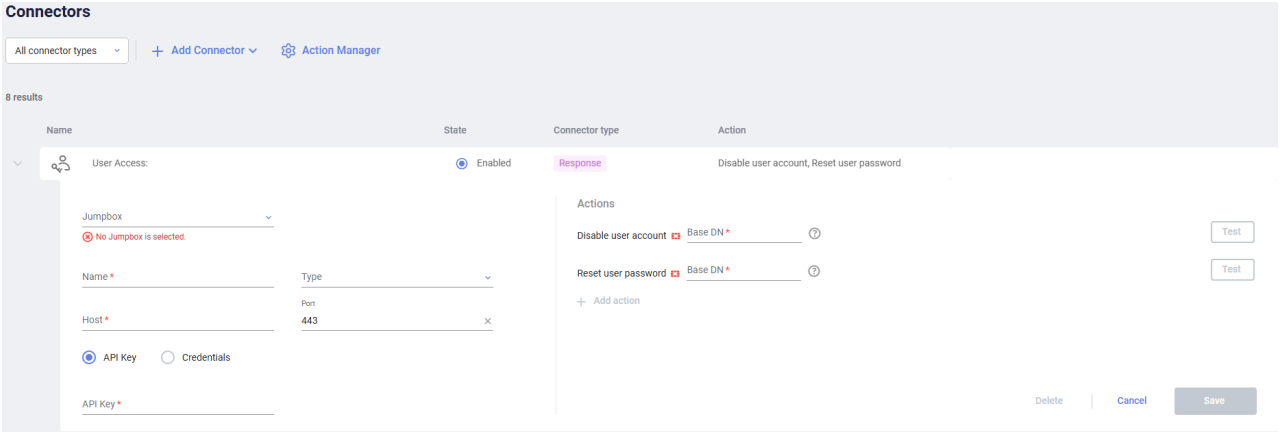
- You have installed an EDR Core and configured the Core as a Jumpbox with connectivity to the domain controller server. To request the EDR Core ISO, contact Fortinet Support.
- You have a valid API user with access to Active Directory or equivalent domain control system. See Configuring Active Directory for detailed instructions about creating an Active Directory admin user.

Follow the steps below to perform user access actions automatically upon the detection of an EDR security event.

Configuring an EDR Connector

To configure User Access integration:

1. Click the *Add Connector* button and select *User Access* from the dropdown list.
   The following displays:

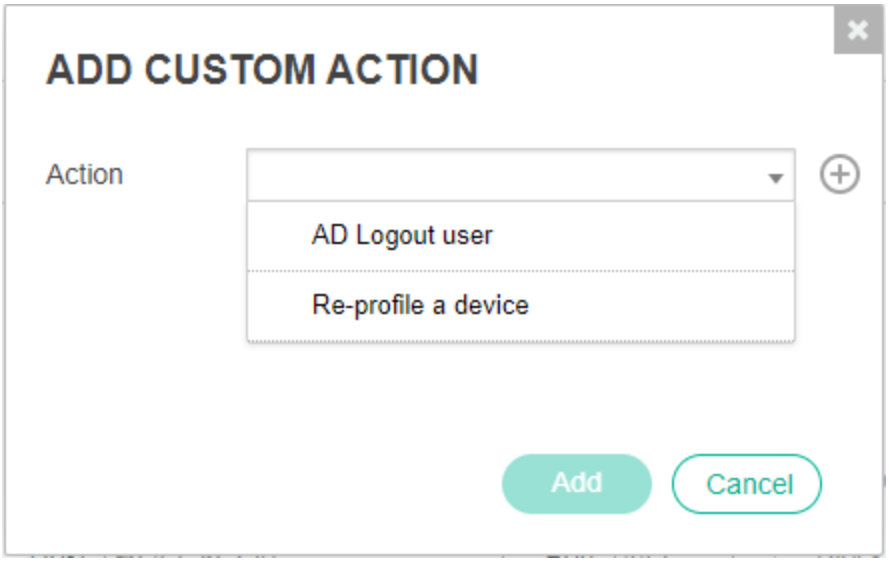


2. Fill in the following fields:

Field	Description
Jumpbox	Select the EDR Jumpbox that will communicate with this User Access system.
Name	Specify a name of your choice to be used to identify this User Access system.
Type	Select the type of user access to be used in the dropdown list. For example, *Active Directory*.
Host	Specify the IP or DNS address of the external User Access system.
Port	Specify the port that is used for communication with the external User Access system.
API Key/Credentials	Specify authentication details of the external user access system: • To use an API token , click the *API Key* radio button and copy the token value into the text box.

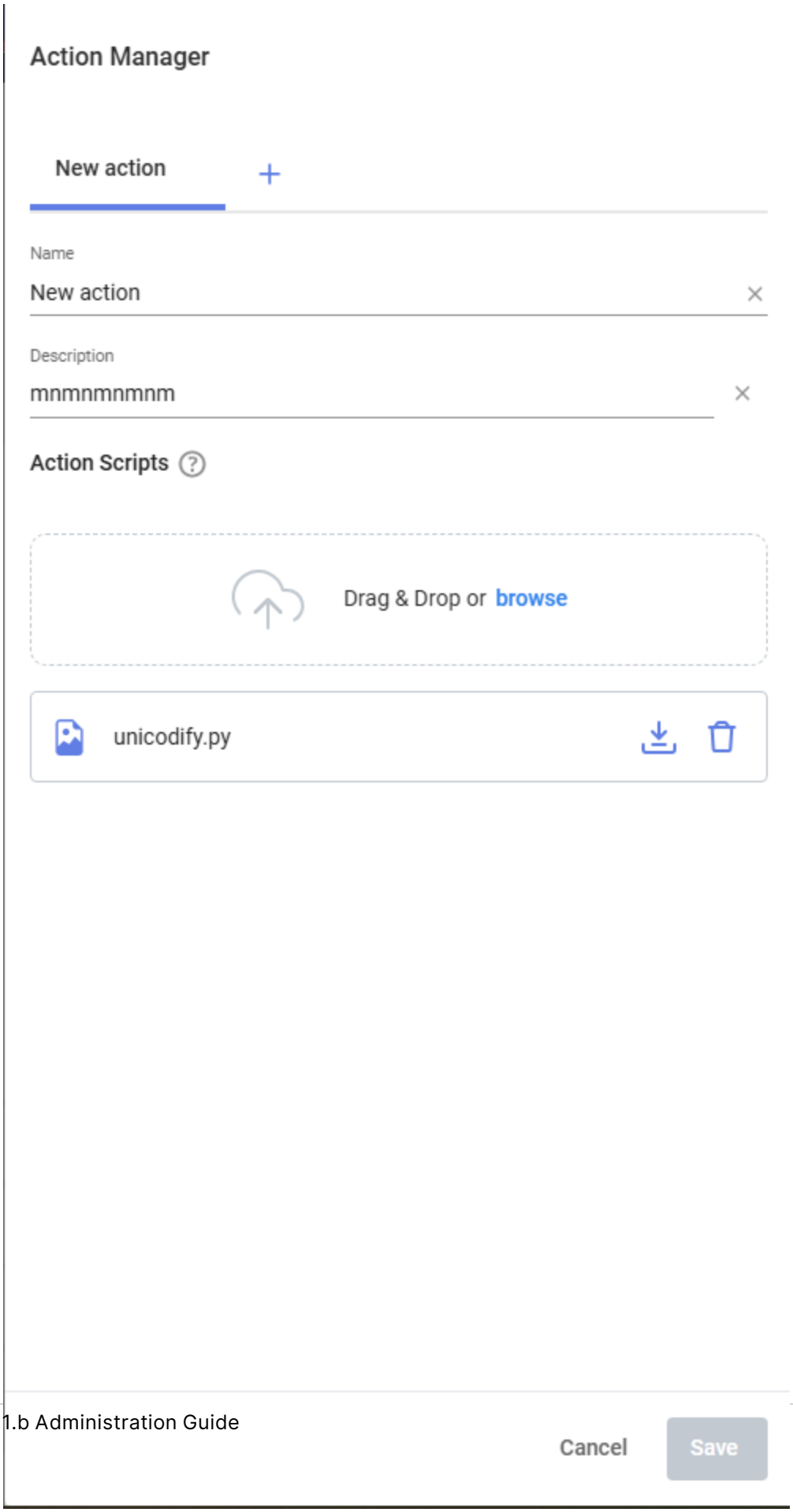
Field	Description
	• To use API credentials, click the *Credentials* radio button and fill in the external User Access system API username (or Bind User DN) and password.

3. In the *Actions* area on the right, define the action to be taken by this connector:
   - To use an action provided out-of-the-box with EDR (for example, Disable user account on Active Directory), in the *baseDN* field of *Disable user account* or *Reset user password*, specify where EDR starts searching for the user upon which actions are performed.
   - To use a custom integration action:
     i. Click the *+ Add Action* button. The following popup window displays:



     ii. In the *Action* dropdown menu, select one of the previously defined actions (which were defined in EDR as described in Custom integration on page 770), or define a new action that can be triggered according to the definitions in the Playbook:

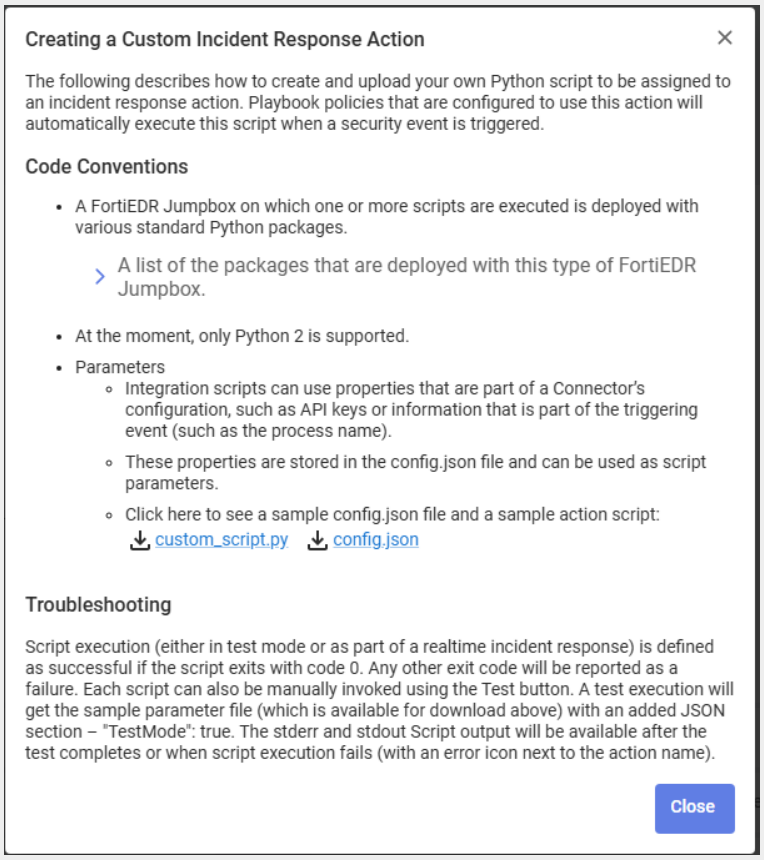
i. Click the *Create New Action* button. The following displays:


Action Manager
New action
Name
New action
Description
mnmnmnmnm
Action Scripts
Drag & Drop or browse
unicodify.py
Cancel
Save

ii. Fill out the fields of this window as follows in order to define a new action to be triggered in response to an incident.

	In order to trigger this action, a Playbook policy must be defined that triggers this action to execute the script when a security event is triggered. The definition of this new action here automatically adds this action as an option in a Playbook policy. However, this action is not selected by default in the Playbook policy. Therefore, you must go to the Playbook policy and select it in order for it to be triggered when a security event is triggered.

Field	Definition
Name	Enter any name for this action.
Description	Enter a description of this action.
Upload	Upload a Python script that calls an API from the third-party system in order to perform the relevant action. Python 2.7 or later is supported. The Python script must be created according to the coding conventions that can be displayed by clicking the  icon next to the *Action Scripts* field. The following displays providing an explanation of the coding conventions and provides various links that you can click to see more detail and/or to download sample files.

Field	Definition
	

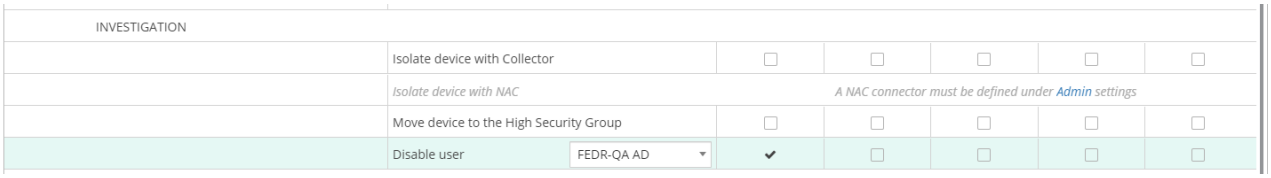
iii. Click *Save*. The new action is then listed in the *Actions* area.

4. You can click the *Test* button next to an action to execute that action.
5. Click *Save* to save the connector configuration.

Configuring Playbooks

To configure an automated incident response that uses a user access connector to reset user password or disable a user upon security event triggering:

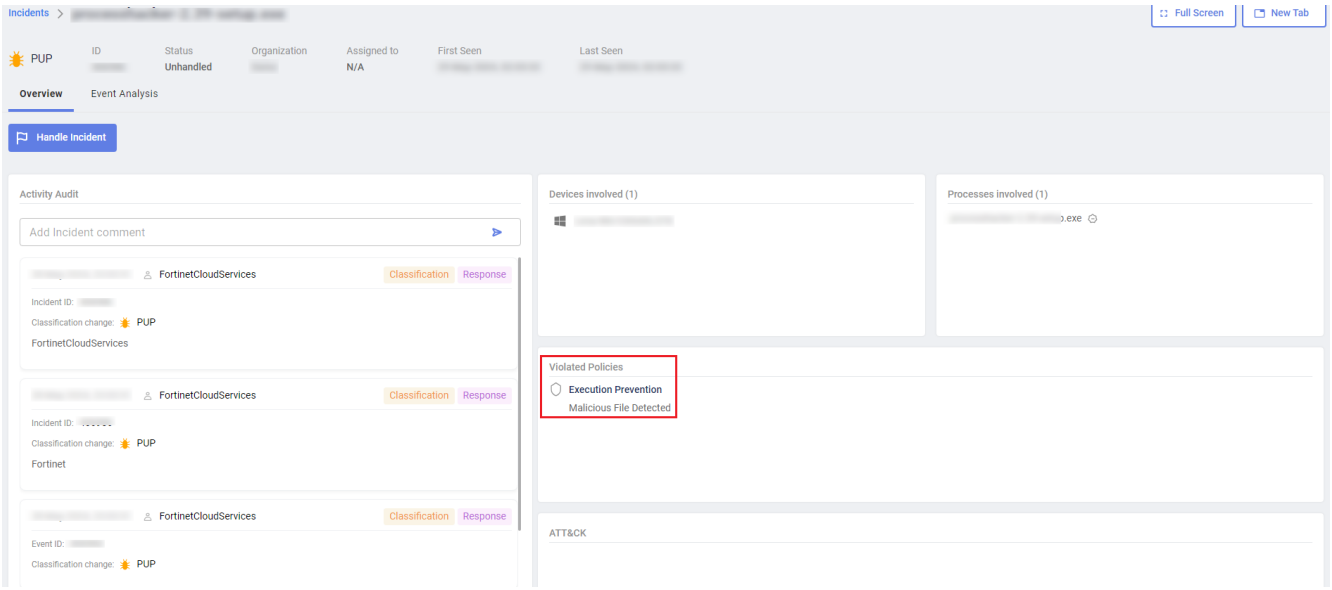
1. Navigate to the *Profiles* > *Playbooks* page.
2. Open the Playbook policy that is applied on devices for which you want the user access response to apply.
3. Place a checkmark in the relevant *Classification* column next to the *Disable user* row under the *INVESTIGATION* section or the *Reset user password* row under the *REMEDIATION* section.
   EDR is now configured to automatically perform user access actions upon triggering of a security event.



To configure an automated incident response that uses a User Access connector to perform a custom action upon the triggering of a security event:

1. Navigate to the *Profiles* > *Playbooks* page.
2. Open the Playbook policy that is applied on devices for which you want the custom action (defined above) to apply.
3. In the *CUSTOM* section, place a checkmark in the relevant *Classification* columns next to the row of the relevant custom action.
4. In the dropdown menu next to the relevant custom action, select the relevant User Access connector with which to perform the action.
   EDR is now configured to trigger this action in the third-party system upon the triggering of a security event.

Automatic incident response actions are listed in the*Overview* tab when you select the incident and click *Investigate* in the *Incidents* pane, as shown below:



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 EDR and are sent to the sandbox. The conditions are a combination of several items, such as the file was downloaded from the Internet and was not signed by a known vendor. If the file is found to be clean, the event is automatically classified as safe and marked as handled. If the file is determined by the sandbox to be suspicious or malicious, then the event is classified as non-safe and any future execution attempt of the file in the environment is blocked by one of the Pre-execution (NGAV) Policy rules. Note that in all cases the first file execution is not delayed or blocked.

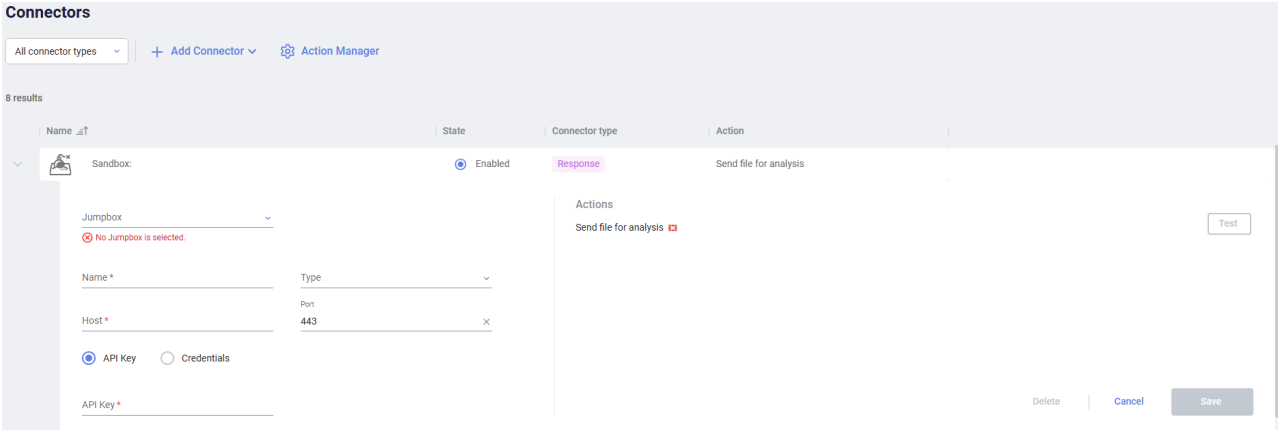
Before you start sandbox connector configuration, verify the following:

- You have installed an EDR Core and configured the Core as a Jumpbox with connectivity to the sandbox. To request the EDR Core ISO, contact Fortinet Support.

- **(FortiSandbox)** A FortiSandbox administrator account with JSON API access enabled. Refer to Configuring FortiSandbox on-premise for detailed instructions.
- **(FortiSandbox Cloud)** A valid FortiCloud API user under a permission profile with read/write access to the FortiSandbox Cloud portal. See the FortiCloud IAM documentation for detailed instructions about creating a permission profile and an API user.

To set up a sandbox connector with EDR:

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



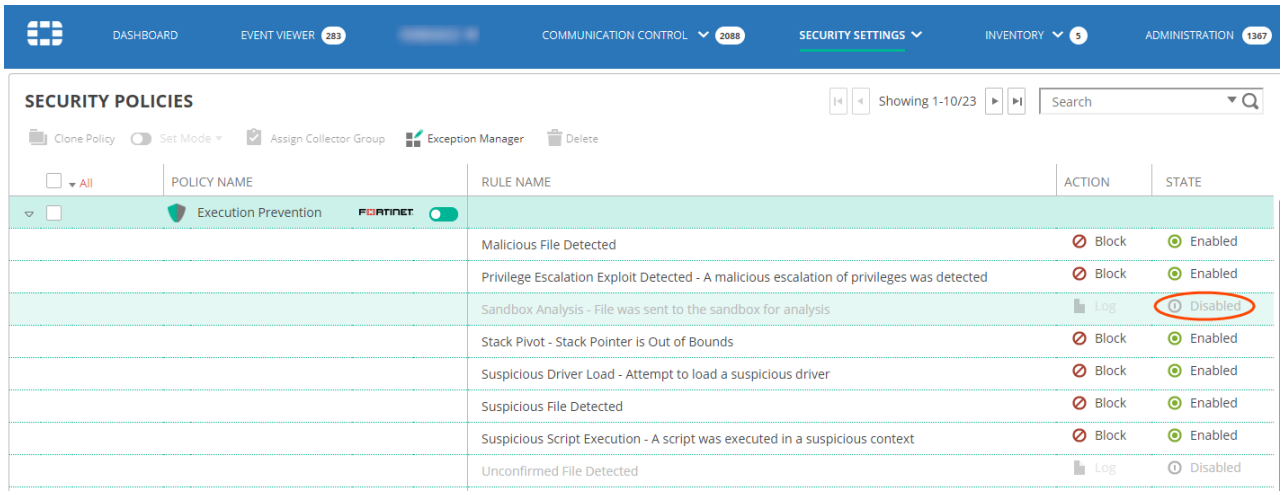
2. Fill in the following fields:

Field	Definition
Jumpbox	Select the EDR Jumpbox that will communicate with this sandbox.
Name	Specify a name of your choice which will be used to identify this sandbox.
Type	Select the type of sandbox to be used in the dropdown list, for example: *FortiSandbox*.
Host	Specify the IP or DNS address of you sandbox.
Port	Specify the port that is used for API communication with your sandbox.
API Key / Credentials	Specify authentication details of the FortiSandbox or FortiSandbox Cloud. • **(FortiSandbox)** To use an API token, select *API Key* and copy the token value into the text box. To use credentials, select *Credentials* and fill in the FortiSandbox username and password. • **(FortiSandbox Cloud)** Select *API Key* and copy the token value into the text box.

3. Click *Save*.
In order to complete sandbox integration, the Sandbox Scan rule must be enabled with the EDR 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:



EDR is now configured to send unknown files to the sandbox.

You can check file analysis on your sandbox console.

In addition, you can see sandbox analysis events in the*Overview* tab when you select the incident and click *Investigate* in the *Incidents* pane. Events of files that were found to be clean appear under the *Handled* filter and events of files that were found to be risky are displayed under the *All statuses* filter. A sandbox analysis digest is added to the security event's handling comment.

eXtended detection source integration

You can connect to external systems to collect activity log by adding a new connector for extended detection. The aggregated data is then being sent to Fortinet Cloud Services (FCS) where it is correlated and analyzed to detect malicious indications that will result in security events of eXtended Detection policy rule violations.

EDR supports extended detection with the following external systems:

- FortiAnalyzer or FortiAnalyzer Cloud on page 757
- Google Cloud Security Command Center (SCC) on page 760
- AWS GuardDuty on page 763
- Custom on page 767

FortiAnalyzer or FortiAnalyzer Cloud

You can integrate EDR with FortiAnalyzer or FortiAnalyzer Cloud to correlate data between EDR and the Fortinet Security Fabric and issue eXtended detection alerts. To complete the integration, you must configure an eXtended detection source connector for FortiAnalyzer or FortiAnalyzer Cloud and enable the eXtended detection rules and EDR Threat Hunting events collection.

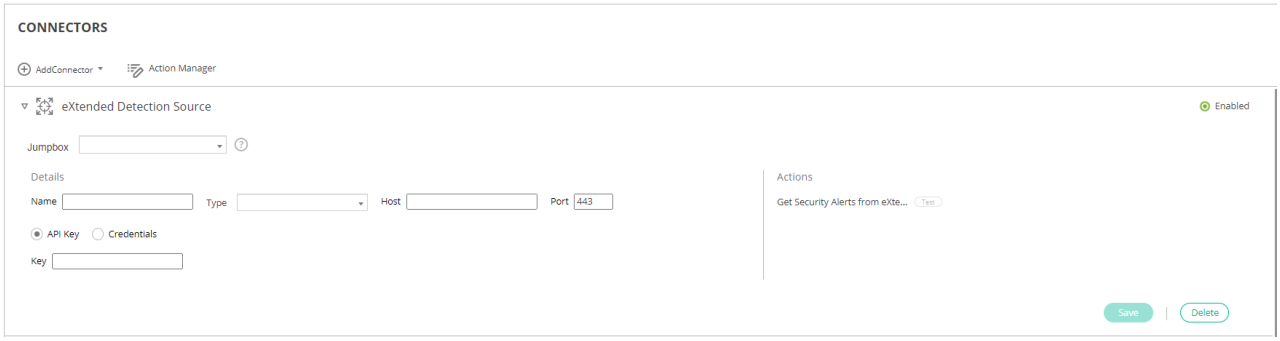
Prerequisites

Before you start integrating EDR with FortiAnalyzer or FortiAnalyzer Cloud, verify the following:

- You have installed an EDR Core and configured the Core as a Jumpbox with connectivity to FortiAnalyzer. To request the EDR Core ISO, contact Fortinet Support.
- **(FortiAnalyzer)** A FortiAnalyzer administrator account with JSON API access enabled. Refer to the FortiAnalyzer Administration Guide for more information.
- **(FortiAnalyzer Cloud)** A valid FortiCloud API user under a permission profile with read/write access to the FortiAnalyzer Cloud portal. See the FortiCloud IAM documentation for detailed instructions about creating a permission profile and an API user.

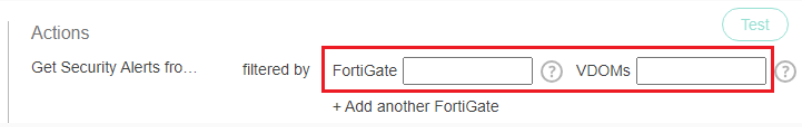
Setting up a connector for FortiAnalyzer or FortiAnalyzer Cloud

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



2. Fill in the following fields:

Field	Definition
Enabled	Check this checkbox to enable blocking of malicious IP addresses by the FortiAnalyzer or FortiAnalyzer Cloud.
Jumpbox	Select the EDR Jumpbox that will communicate with the FortiAnalyzer or FortiAnalyzer Cloud.
Name	Specify a name of your choice to identify the connector.
Type	Select *FortiAnalyzer*.
Host	Specify the IP or DNS address of the FortiAnalyzer or FortiAnalyzer Cloud.
Port	Specify the port that is used for API communication with the FortiAnalyzer or FortiAnalyzer Cloud.
API Key/Credentials/Authentication	Specify authentication details of the FortiAnalyzer or FortiAnalyzer Cloud. • **(FortiAnalyzer)** Select *Credentials* and fill in the FortiAnalyzer username and password. • **(FortiAnalyzer Cloud)** Specify the username and password of the FortiCloud API user with read/write access to the

Field	Definition
	FortiAnalyzer Cloud portal.
Actions	Configure the FortiGate and VDOM logs to be correlated with EDR data by specifying the FortiGate or VDOM name in the following fields. If both fields are empty, EDR uses the default value, which is *All*. 

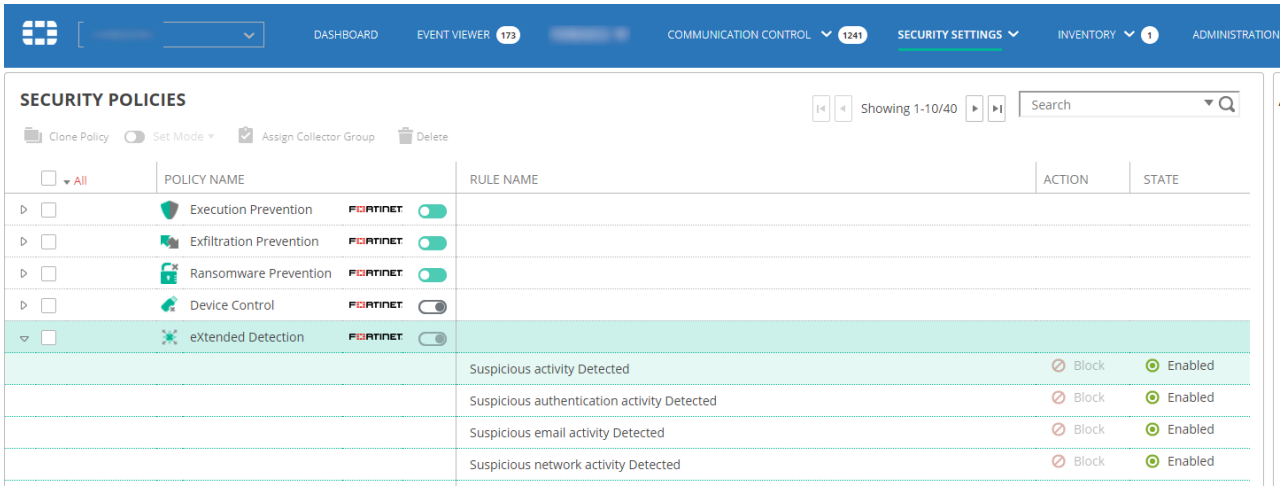
3. Click *Save*.

Setting up EDR Central Manager

In order to complete the integration with FortiAnalyzer or FortiAnalyzer Cloud, the eXtended detection rules and EDR Threat Hunting events collection must be enabled with the EDR Central Manager, as follows.

To enable eXtended detection rules:

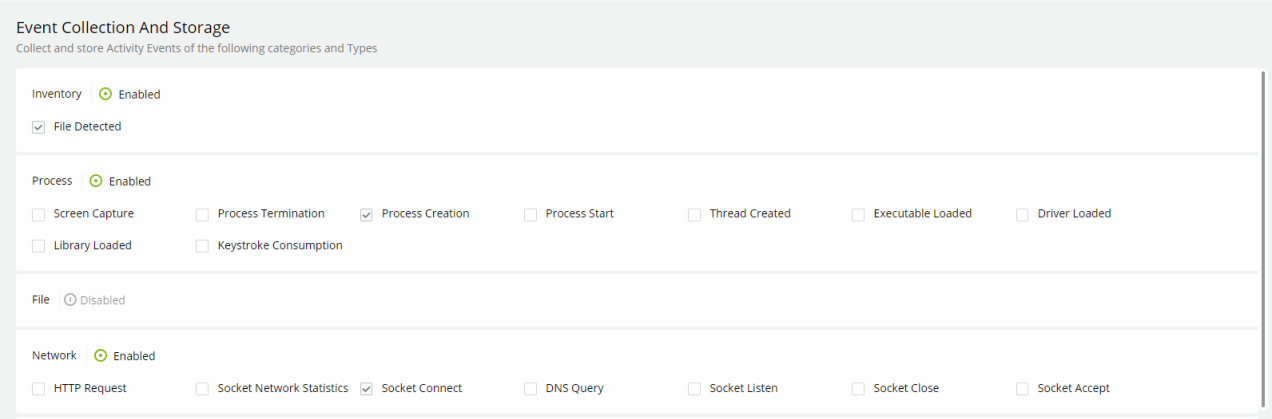
1. Navigate to the *SECURITY SETTINGS* > *Security Policies* page.
2. Open the eXtended detection policy that is applied on devices on which you want the eXtended detection policy to apply and click the *Disabled* button next to each of the underlying rules to enable it, as shown below:



To enable EDR Threat Hunting events collection:

1. Navigate to the *SECURITY SETTINGS* > *Threat Hunting* > *Collection Profiles* page.
2. Open the Threat Hunting collection profile that is applied on devices on which you want the eXtended detection policy to apply.
3. Select the following event types on that profile:
   - Socket Connect
   - Process Creation

- File Create
- File Detected



EDR is now configured to issue eXtended detection alerts from FortiAnalyzer or FortiAnalyzer Cloud.

Google Cloud Security Command Center (SCC)

To integrate EDR with Google Cloud Security Command Center (SCC) to collect activity log and issue eXtended detection alerts, you must configure Google SCC for threat logging and API access, configure an eXtended detection source connector with Google Cloud SCC in EDR, and enable the eXtended detection rules and EDR Threat Hunting events collection in EDR.

Prerequisites

Before you start integrating EDR with Google SCC, verify the following:

- You have installed an EDR Core and configured the Core as a Jumpbox with connectivity to Google SCC. To request the EDR Core ISO, contact Fortinet Support.
- You have the Google Cloud licensing of Security Command Center Premium tier that has Event Threat Detection feature.

Configuring Google SCC

Perform the following steps to configure Google SCC:

1. Enable threat logging in Google SCC:
   a. Enable Event Threat Detection per monitored project in the organization. The following Event Threat Detection rules are required:
      - Malware: bad IP
      - Malware: bad domain

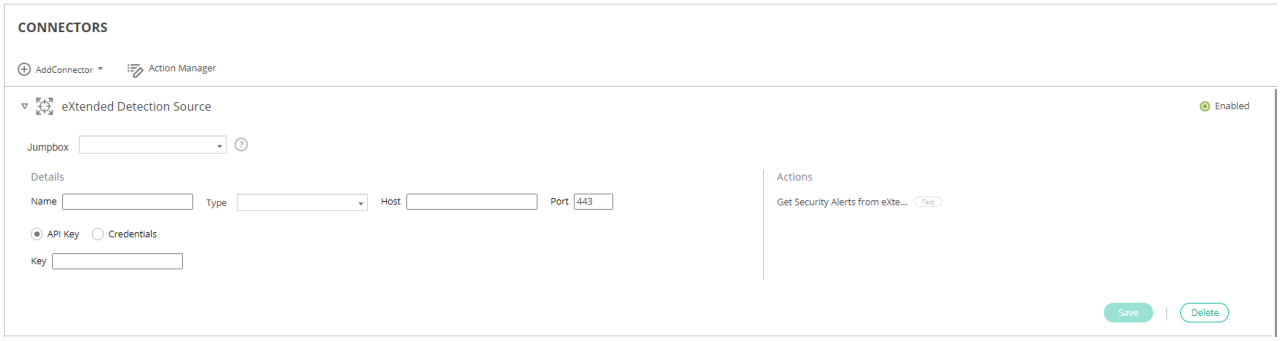
      Make sure to enable all log source types that are needed for these rules detectors to work, such as Cloud DNS logs and Admin Activity log. For more details about Event Threat Detection rules and the required log sources, see Google Documentation.
   b. Verify that raw log items now show on Google's Logs Explorer and Event Threat Detection findings show on Security Command Center as described in Google Documentation.

2. Enable API access to Google for fetching threat logs:
   a. Set up a service account on Google, as described in Google Documentation.
   b. Download the json key file for this service account. This file should be uploaded vian EDR console as part of setting up the extended detection source connector (see section below).
   c. Grant the following permission to the service account to allow API access:
      - Organization Admin (resourcemanager.organizationAdmin)
      - Security Command Center Admin (securityCenter.admin)

      See Google Documentation for more details about permissions.

Setting up a connector for Google SCC

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



2. Fill in the following fields:

Field	Definition
Enabled	Check this checkbox to enable blocking of malicious IP addresses by Google SCC.
Jumpbox	Select the EDR Jumpbox that will communicate with Google SCC.
Name	Specify a name of your choice to identify the connector.
Type	Select *Google SCC*.
Authentication	Upload the JSON file that was created for your Google Service account.
Actions	Specify the unique organization resource identifier in Google cloud or ID of Google cloud project to use for fetching alerts. 

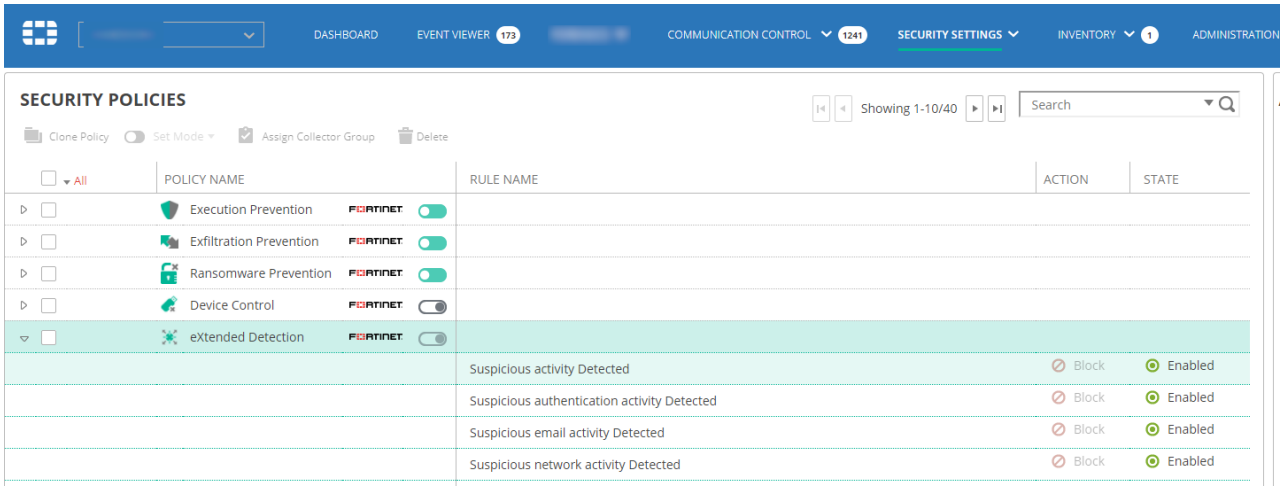
3. Click *Save*.

Setting up EDR Central Manager

In order to complete the integration with Google SCC, the eXtended detection rules and EDR Threat Hunting events collection must be enabled with the EDR Central Manager, as follows.

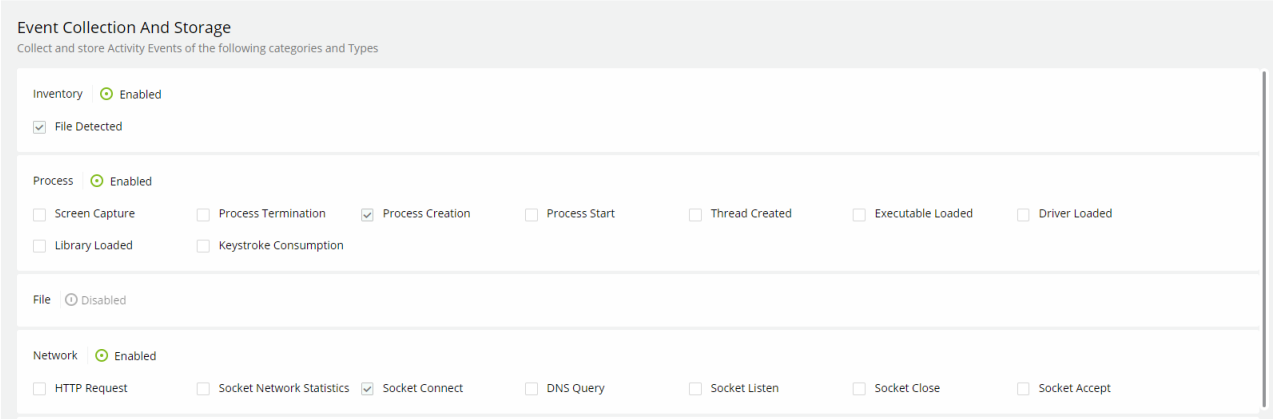
To enable eXtended detection rules:

1. Navigate to the *SECURITY SETTINGS > Security Policies* page.
2. Open the eXtended detection policy that is applied on devices on which you want the eXtended detection policy to apply and click the *Disabled* button next to each of the underlying rules to enable it, as shown below:



To enable EDR Threat Hunting events collection:

1. Navigate to the *SECURITY SETTINGS > Threat Hunting > Collection Profiles* page.
2. Open the Threat Hunting collection profile that is applied on devices on which you want the eXtended detection policy to apply.
3. Select the following event types on that profile:
   - Socket Connect
   - Process Creation
   - File Create
   - File Detected



EDR is now configured to issue eXtended detection alerts from Google SCC.

AWS GuardDuty

To integrate EDR with AWS GuardDuty to collect activity log and issue eXtended detection alerts, you must configure AWS GuardDuty, configure an eXtended detection source connector with AWS GuardDuty in EDR, and enable the eXtended detection rules and EDR Threat Hunting events collection.

Prerequisites

Before you start integrating EDR with AWS GuardDuty, verify that you have installed an EDR Core and configured the Core as a Jumpbox with connectivity to AWS GuardDuty. To request the EDR Core ISO, contact Fortinet Support.

Configuring AWS GuardDuty

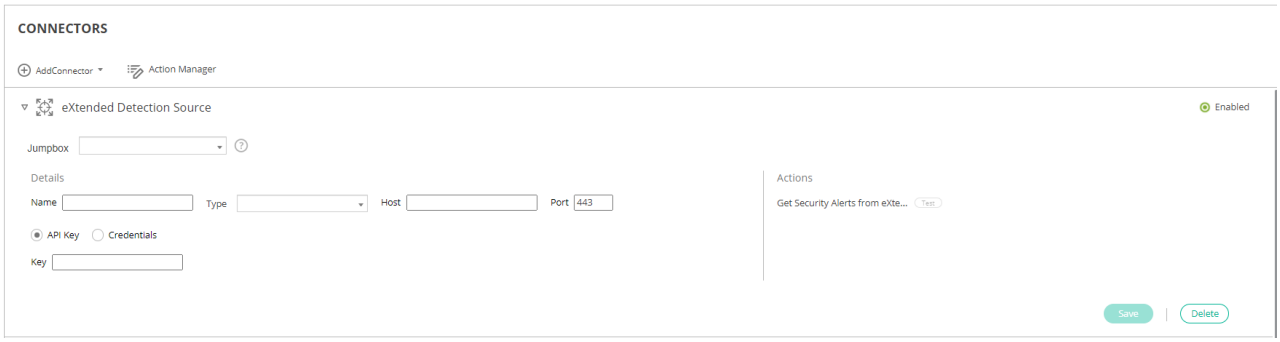
Perform the following steps to configure AWS GuardDuty:

1. Enable Amazon GuardDuty in your account as described in AWS Documentation.
   The following GuardDuty finding types are correlated with the EDR events:
   - Backdoor:EC2/C&CActivity.B!DNS
   - Discovery:Kubernetes/MaliciousIPCaller

   You are encouraged to test that GuardDuty generates these findings as described on AWS documentation.
2. Create IAM user on AWS console as described here:
   a. Set Programmatic Access for this user to allow API calls.
   b. Set full permissions to access GuardDuty service.
   c. Show and copy access key ID and secret access key of this user, which will be used on EDR console when you set up the extended detection source connector in the following section.

Setting up a connector for AWS GuardDuty

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



2. Fill in the following fields:

Field	Definition
Enabled	Check this checkbox to enable blocking of malicious IP addresses by

Field	Definition
	AWS GuardDuty.
Jumpbox	Select the EDR Jumpbox that will communicate with AWS GuardDuty.
Name	Specify a name of your choice to identify the connector.
Type	Select *AWS GuardDuty*.
Authentication	Specify the access key ID and secret access key.
Actions	Specify the AWS region for API calls. 

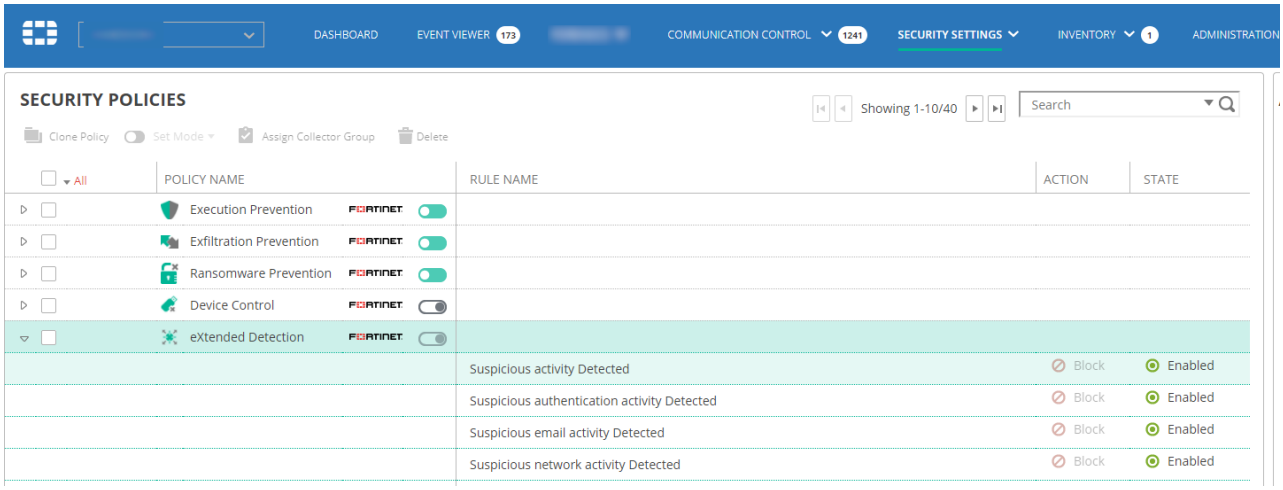
3. Click *Save*.

Setting up EDR Central Manager

In order to complete the integration with AWS GuardDuty, the eXtended detection rules and EDR Threat Hunting events collection must be enabled with the EDR Central Manager, as follows.

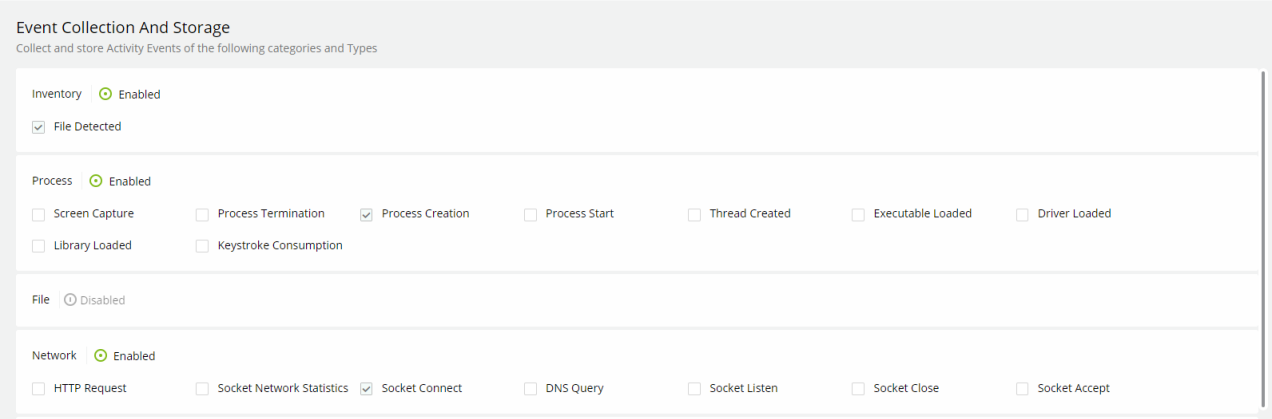
To enable eXtended detection rules:

1. Navigate to the *SECURITY SETTINGS* > *Security Policies* page.
2. Open the eXtended detection policy that is applied on devices on which you want the eXtended detection policy to apply and click the *Disabled* button next to each of the underlying rules to enable it, as shown below:



To enable EDR Threat Hunting events collection:

1. Navigate to the *SECURITY SETTINGS > Threat Hunting > Collection Profiles* page.
2. Open the Threat Hunting collection profile that is applied on devices on which you want the eXtended detection policy to apply.
3. Select the following event types on that profile:
   - Socket Connect
   - Process Creation
   - File Create
   - File Detected



EDR is now configured to issue eXtended detection alerts from AWS GuardDuty.

FortiSIEM or FortiSIEM Cloud

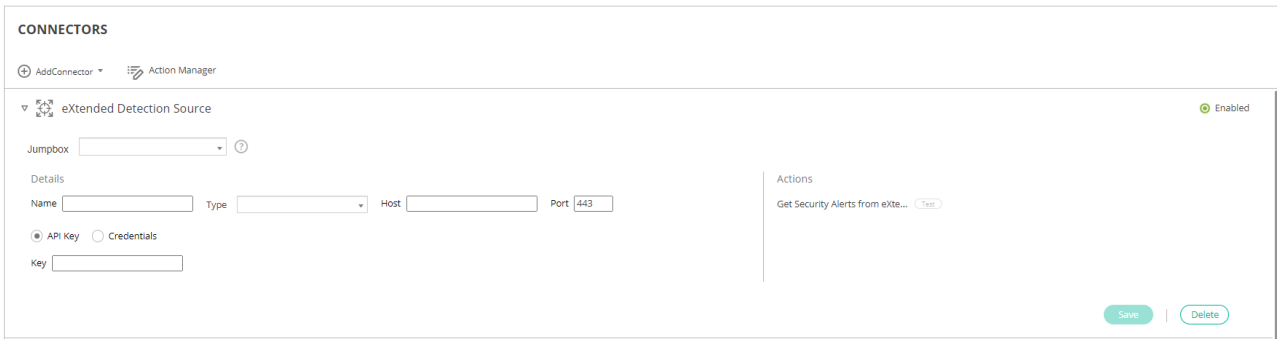
To integrate EDR with FortiSIEM or FortiSIEM Cloud to collect activity log and issue eXtended detection alerts, you must configure an eXtended detection source connector with FortiSIEM or FortiSIEM Cloud and enable the eXtended detection rules and EDR Threat Hunting events collection.

Setting up a connector for FortiSIEM or FortiSIEM Cloud

requirements for using FortiSIEM as an XDR data source: required data sources in fortisiem? what rules need to be enabled (if any)?

- You need to create the user in the super org (read only to whichever organizations)
- 4 different searches are executed, replicating what XDR does with FAZ for FGT and FML datasets.
  - FortiGate webfilter allow/denies where the category = Malicious Websites
  - FortiMail antispam filter triggered by malicious file attachment
  - FortiMail antispam filter triggered by malicious URL
  - Permitted/denied UDP traffic to port 53 (DNS) that is from an private network source, to a destination that is not an internal DNS server, an internal Application, FortiSIEM, or well-known public DNS

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



2. Fill in the following fields:

Field	Definition
Enabled	Check this checkbox to enable blocking of malicious IP addresses by FortiSIEM or FortiSIEM Cloud.
Jumpbox	Select the EDR Jumpbox that will communicate with FortiSIEM or FortiSIEM Cloud.
Name	Specify a name of your choice to identify the connector.
Type	Select *FortiSIEM*.
Host	Specify the IP or DNS address of FortiSIEM or FortiSIEM Cloud.
Port	Specify the port that is used for API communication with FortiSIEM or FortiSIEM Cloud.
API Key/Credentials	Specify authentication details of FortiSIEM or FortiSIEM Cloud. To use an API token, click the *API Key* radio button and copy the token value into the text box. To use API credentials, click the *Credentials* radio button and fill in the external system API username/password or Access key ID/Secret access key.
Actions Parameters	

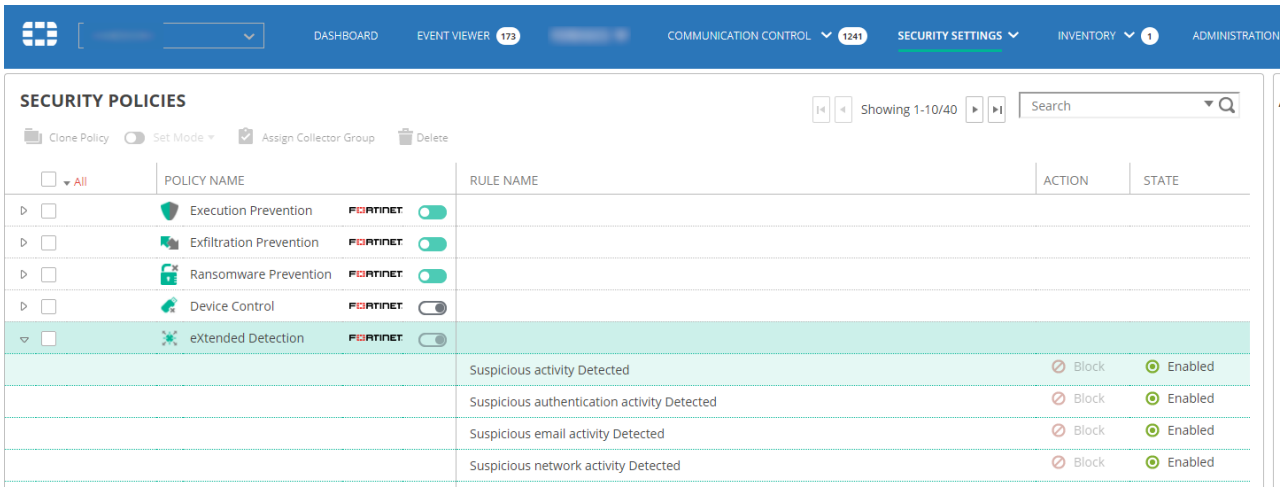
3. Click *Save*.

Setting up EDR Central Manager

In order to complete the integration with FortiSIEM or FortiSIEM Cloud, the eXtended detection rules and EDR Threat Hunting events collection must be enabled with the EDR Central Manager, as follows.

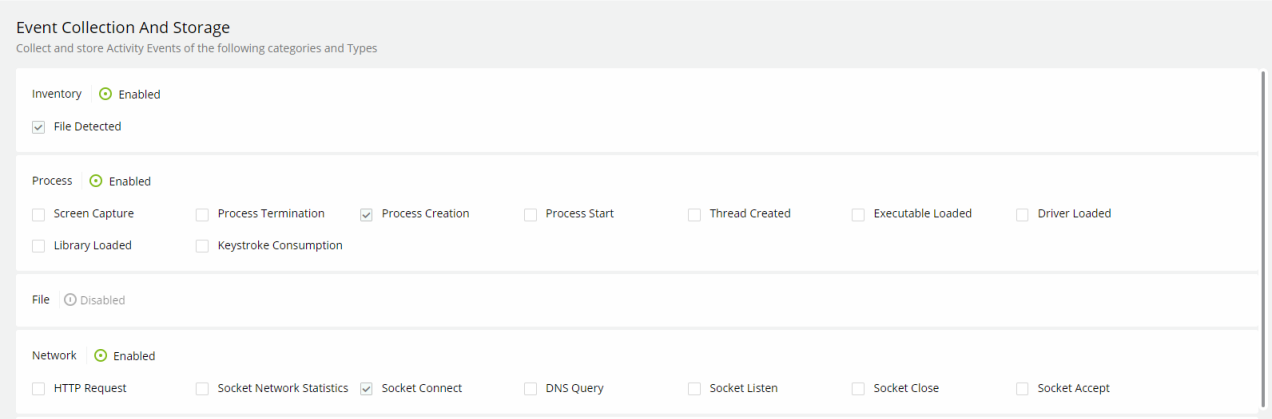
To enable eXtended detection rules:

1. Navigate to the *SECURITY SETTINGS > Security Policies* page.
2. Open the eXtended detection policy that is applied on devices on which you want the eXtended detection policy to apply and click the *Disabled* button next to each of the underlying rules to enable it, as shown below:



To enable EDR Threat Hunting events collection:

1. Navigate to the *SECURITY SETTINGS > Threat Hunting > Collection Profiles* page.
2. Open the Threat Hunting collection profile that is applied on devices on which you want the eXtended detection policy to apply.
3. Select the following event types on that profile:
   - Socket Connect
   - Process Creation
   - File Create
   - File Detected



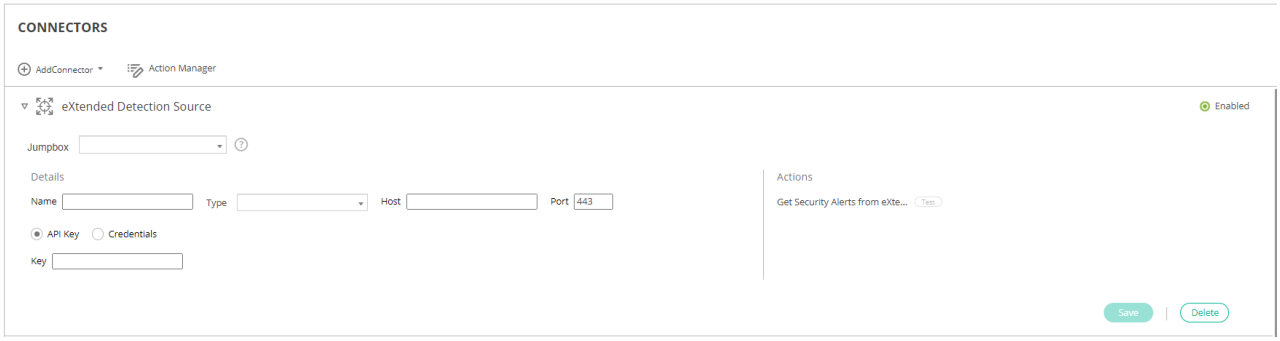
EDR is now configured to issue eXtended detection alerts from FortiSIEM or FortiSIEM Cloud.

Custom

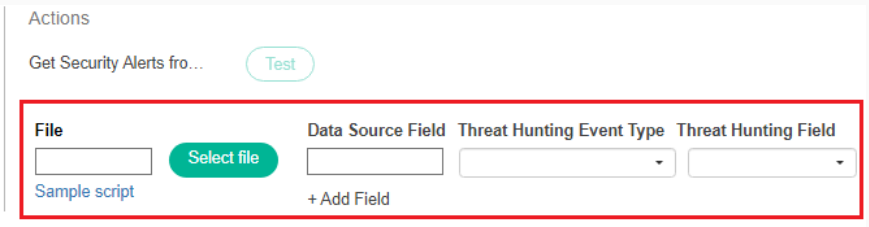
To integrate EDR with a custom system to collect activity log and issue eXtended detection alerts, you must configure an eXtended detection source connector with the custom system and enable the eXtended detection rules and EDR Threat Hunting events collection.

Setting up a connector for the custom system

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



2. Fill in the following fields:

Field	Definition
Enabled	Check this checkbox to enable blocking of malicious IP addresses by the custom system.
Jumpbox	Select the EDR Jumpbox that will communicate with the custom system.
Name	Specify a name of your choice to identify the custom system.
Type	Select *Custom*.
Host	Specify the IP or DNS address of the custom system.
Port	Specify the port that is used for API communication with the custom system.
API Key/Credentials	Specify authentication details of the custom system.
Actions Parameters	1. Upload a script file that contains all the authentication details for the external system and the query for EDR to pull data from the system. Use the sample script as a starting point to build your own script by replacing all the values with those for your system. 2. Specify the name of the data source field in the external system for EDR to correlate with. You can add fields as needed. 3. For each data source field, select the corresponding *Threat Hunting Event Type* and *Threat Hunting Field* for EDR to correlate data with. 

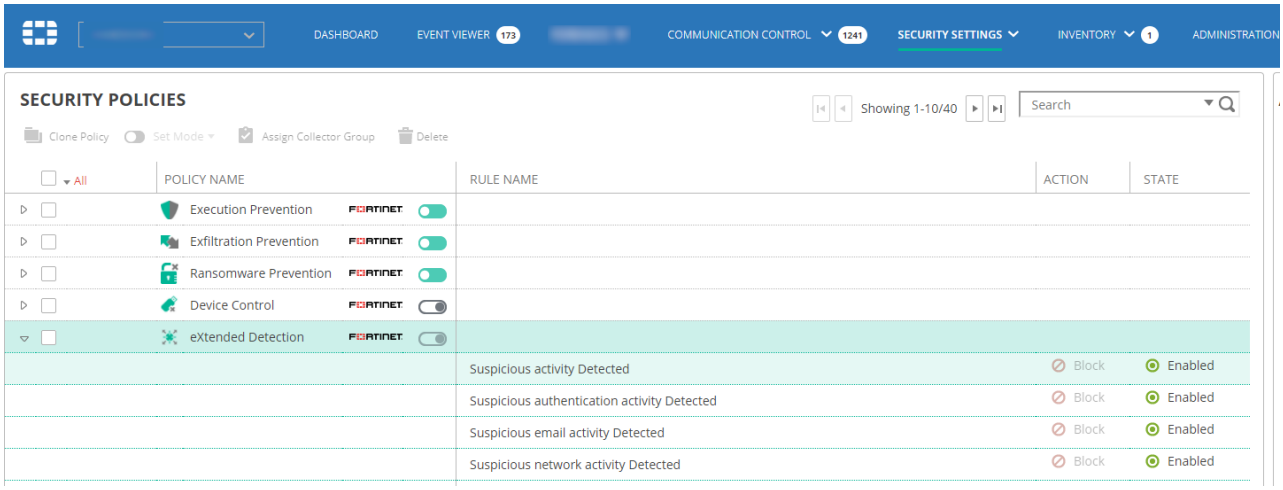
3. Click *Save*.

Setting up EDR Central Manager

In order to complete the integration with the custom system, the eXtended detection rules and EDR Threat Hunting events collection must be enabled with the EDR Central Manager, as follows.

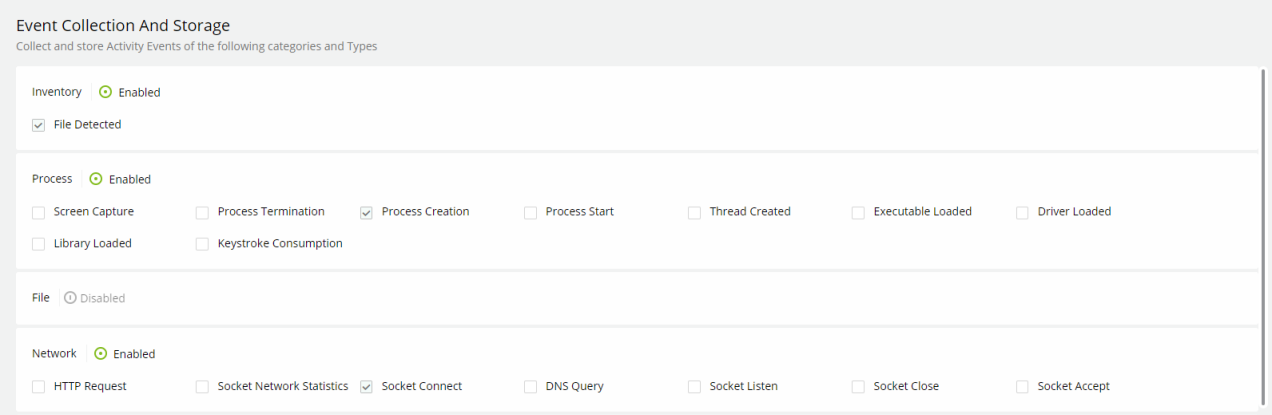
To enable eXtended detection rules:

1. Navigate to the *SECURITY SETTINGS > Security Policies* page.
2. Open the eXtended detection policy that is applied on devices on which you want the eXtended detection policy to apply and click the *Disabled* button next to each of the underlying rules to enable it, as shown below:



To enable EDR Threat Hunting events collection:

1. Navigate to the *SECURITY SETTINGS > Threat Hunting > Collection Profiles* page.
2. Open the Threat Hunting collection profile that is applied on devices on which you want the eXtended detection policy to apply.
3. Select the following event types on that profile:
   - Socket Connect
   - Process Creation
   - File Create
   - File Detected



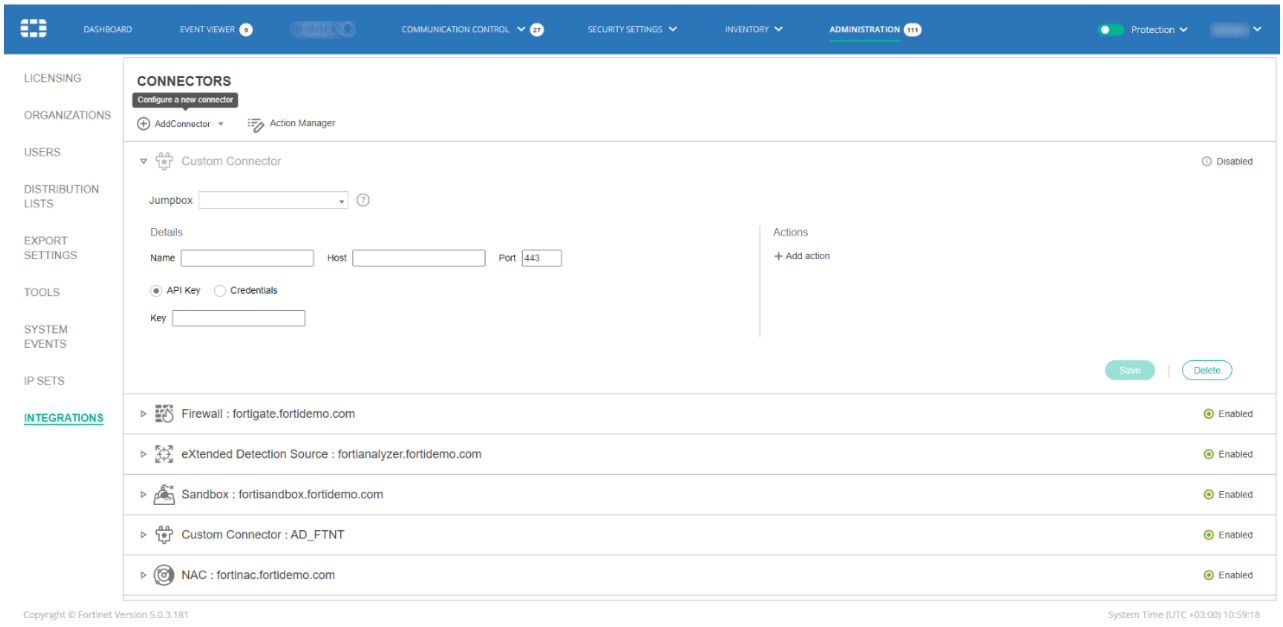
EDR is now configured to issue eXtended detection alerts from the custom system.

Custom integration

The *CUSTOM* section enables you to connect to any third-party system in order to automatically trigger an incident response in that third-party system as the result of a security event detected by EDR. After you define a Custom Integration connector (and its actions) and configure a relevant Playbook policy, an automatic incident response action will be triggered in the third-party system upon the triggering of a security event.

To set up a custom integration connector in EDR:

1. Click the *Add Connector* button and select *Custom Connector* from the dropdown list. The following displays:

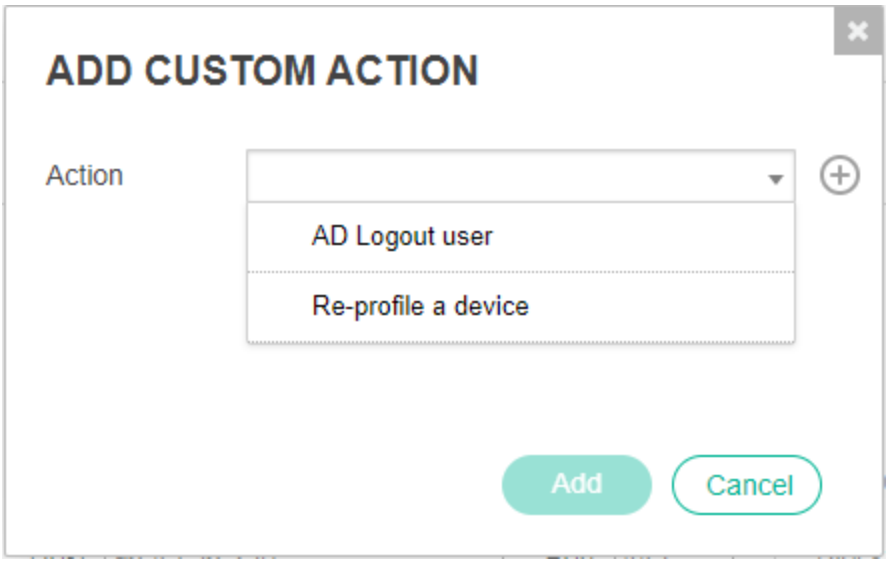


2. Fill in the following fields:

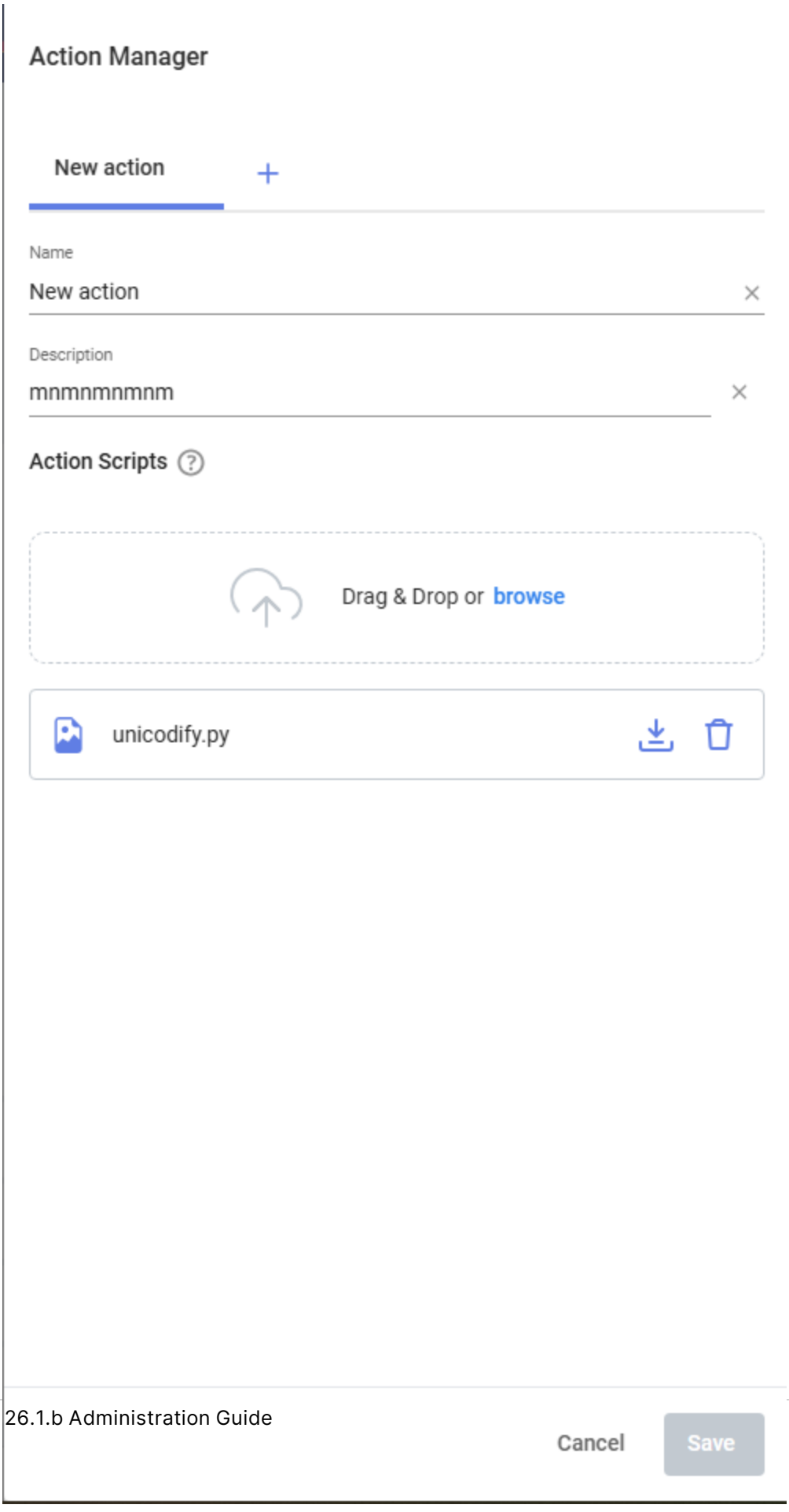
Field	Description
Jumpbox	Select the EDR Jumpbox that will communicate with the third-party system. An EDR deployment must include a Jumpbox that has connectivity to the external system of this custom integration connector. This Jumpbox must be exclusive to this organization and cannot function as a Core.
Name	Specify a name of your choice to be used to identify this custom connector.
Host	Specify the IP or DNS address of the relevant third-party application.
Port	Specify the port that is used for API communication with the relevant third-party application.

Field	Description
API Key/Credentials	Specify authentication details of the relevant third-party application. To use an API token, click the *API Key* radio button and copy the token value into the text box. To use API credentials, click the *Credentials* radio button and enter the relevant third-party application's API username and password.

3. In the *Actions* area on the right, define the action to be taken by this custom connector, as follows:
   - To trigger an action on a custom connected third-party system, click the **+ Add Action** button to display the following popup window:



   1. In the *Action* dropdown menu, select one of the previously defined actions (which were defined in EDR as described Custom integration on page 770).
      -OR-
   2. Click the *Create New Action* button in this popup window to define a new action that can be triggered according to the definitions in the Playbook, as described in the next section below. The following displays:

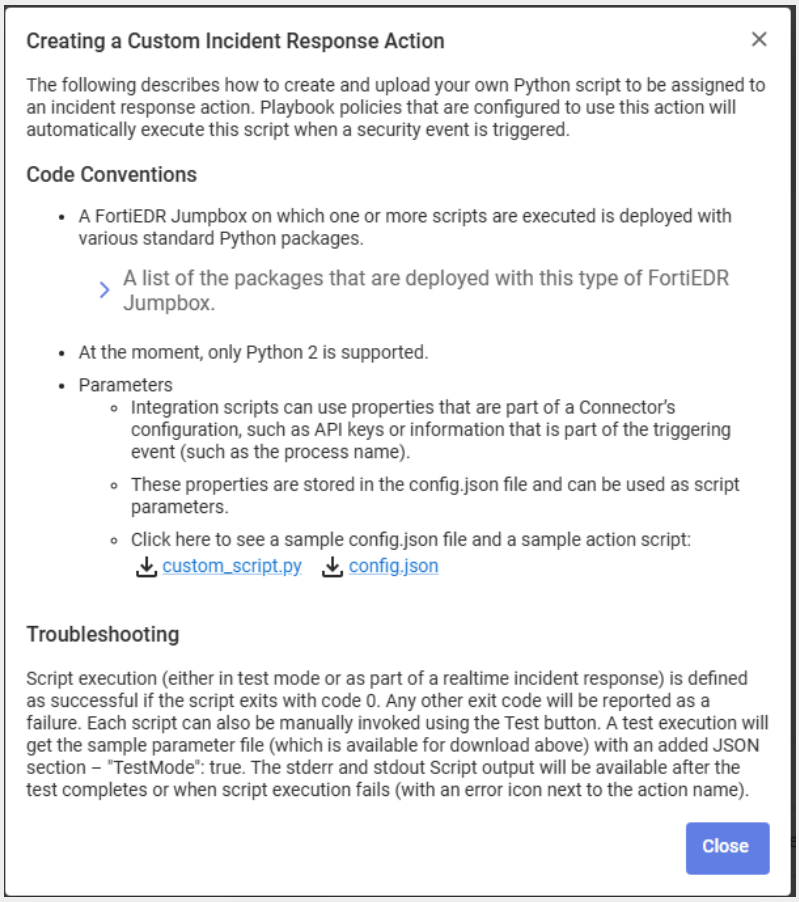

Action Manager
New action
Name
New action
Description
mnmnmnmnm
Action Scripts
Drag & Drop or browse
unicodify.py
Cancel
Save

Fill out the fields of this window as follows in order to define a new action to be triggered in response to an incident.



In order to trigger this action, a Playbook policy must be defined that triggers this action to execute the script when a security event is triggered. The definition of this new action here automatically adds this action as an option in a Playbook policy. This action however, is not selected by default in the Playbook policy. Therefore, you must go to the Playbook policy and select it in order for it to be triggered when a security event is triggered.

Field	Definition
Name	Enter any name for this action.
Description	Enter a description of this action.
Upload	Upload a Python script that calls an API from the third-party system in order to perform the relevant action. Python 2.7 or later is supported. The Python script must be created according to the coding conventions that can be displayed by clicking the icon next to the *Action Scripts* field. The following displays providing an explanation of the coding conventions and provides various links that you can click to see more detail and/or to download sample files.

Field	Definition
	

3. Click *Save*. The new action is then listed in the Actions area.

4. Select this action to associate it with the custom connector.
5. You can click the *Test* button next to it to execute this action.
   A new row is added to the *CUSTOM* section of the *Automated Incident Response – Playbooks* page. In order for this custom integration connector to trigger an action, you must define it in the Playbook, as described below.

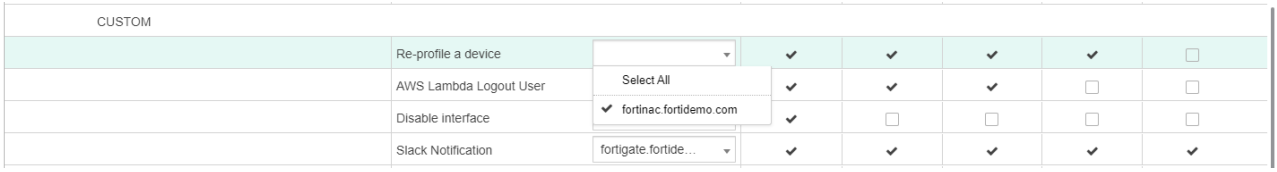


The actions that you define here can also be selected as an action for a Firewall integration on page 727 connector or Network Access Control (NAC) integration on page 735 connector. These integration connectors might use the same API. Alternatively, you may need to upload a different script that will be used to perform the same action on different third-party products. You can associate several scripts with the same action and select the appropriate one per connector. For example, an IM notification action could have two scripts – one for notifications via Slack and the other for notifications via Teams.

Playbooks configuration

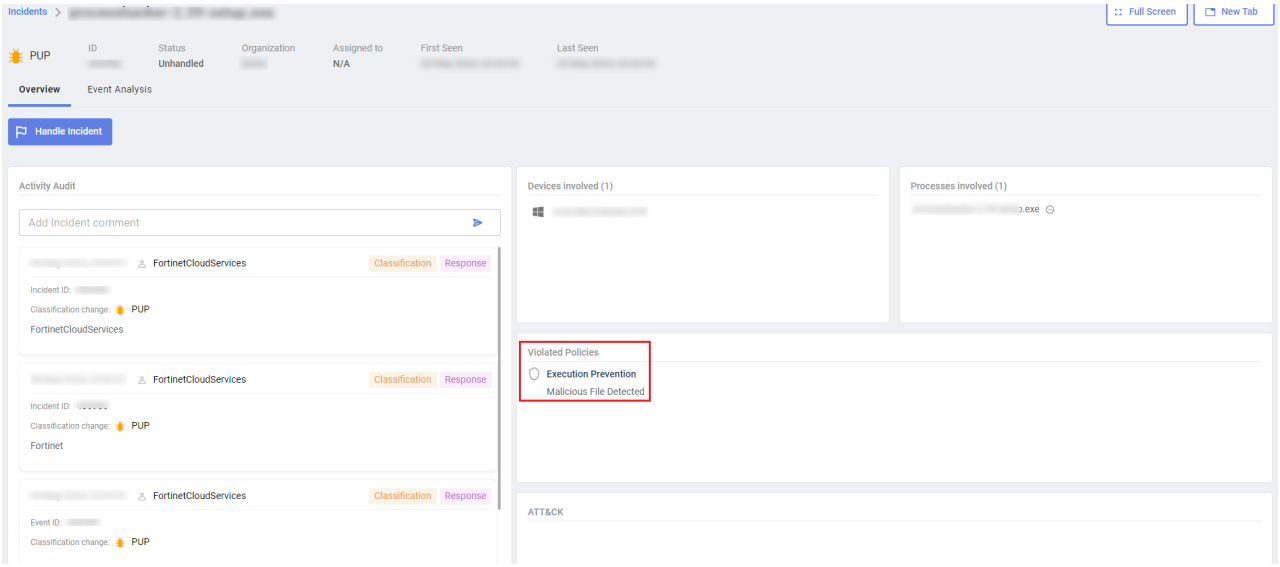
To configure an automated incident response that triggers an action using this custom integration connector upon the triggering of a security event:

1. Navigate to the *Profiles* > *Playbooks* page.
2. Open the Playbook policy that is applied on devices for which you want the custom action (defined above) to apply.
3. In the *CUSTOM* section, place a checkmark in the relevant Classification columns next to the row of that action.
4. In the dropdown menu next to the action, select the connector with which to perform the action or click *Select All*, as shown below:



The example above showed how to configure two custom connectors by using the same action named IM notification in the Playbook – one for notifications via Teams and the other for notifications via Slack.

EDR is now configured to trigger this action in the third-party system upon the triggering of a security event. This automatic incident response action appears in the *Overview* tab when you select the incident and click *Investigate* in the *Incidents* pane.



Threat Intelligence Feed integration

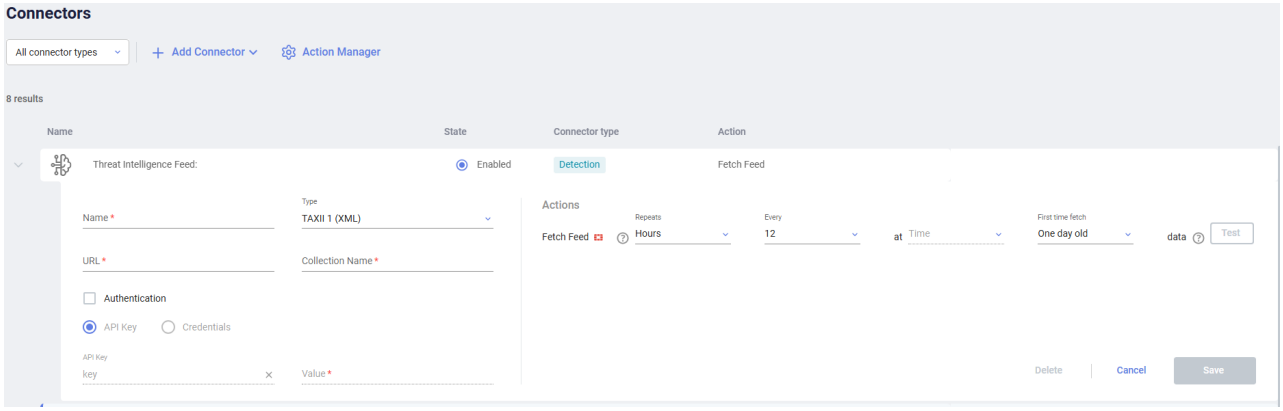
When a Threat Intelligence Feed connector is configured, EDR creates a Threat Hunting query based on the data fetched from STIX/TAXII feed. The related query is updated upon each scheduled retrieval of collection data which covers the following indicators: hashes, file names, files size, paths, IPs, usernames, registry keys, URLs, and domain names. You can find the relevant queries under *Threat Hunting > Saved Queries*.



As one Threat Hunting query can include only 150 to 1000 conditions, depending on the indicator type, EDR may create multiple query entries for the same collection.

To set up a Threat Intelligence Feed connector with EDR:

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



2. In the *Details* section, fill in the following fields:

Field	Definition
Name	Specify a name of your choice which will be used to identify this Threat Intelligence Feed Collection.
Type	Select the syntax type of the original query, for example: *TAXII (JSON)* or *TAXII 1 (XML)*.
URL	Specify the IP or DNS address of the Threat Intelligence server.
Collection ID	Specify the collection name of the XML query or collection ID of the JSON query.
Authentication	Select this option to specify authentication details of your Threat Intelligence Feed. To use an API token, click the *API Key* radio button and copy the token value into the text box. To use API credentials, click the *Credentials* radio button and fill in the external system API username and password.
Enabled	Use this option to enable or disable EDR integration with this Threat Intelligence Feed.

3. In the *Actions* section, specify the schedule for EDR to retrieve the provided collection data, which covers the following indicators: hashes, file names, files size, paths, IPs, usernames, registry keys, URLs, and domain names.
4. Specify the age of collection data for the initial retrieval. For example, *One day old* means that only indicators that were added to the Collection during the last day will be retrieved for the initial retrieval.
5. Click the *Test* button to execute the action.
6. Click *Save*.
   The Threat Intelligence Feed connector is set up and relevant queries will be created in Saved Queries under Threat Hunting on page 608.

Action Manager

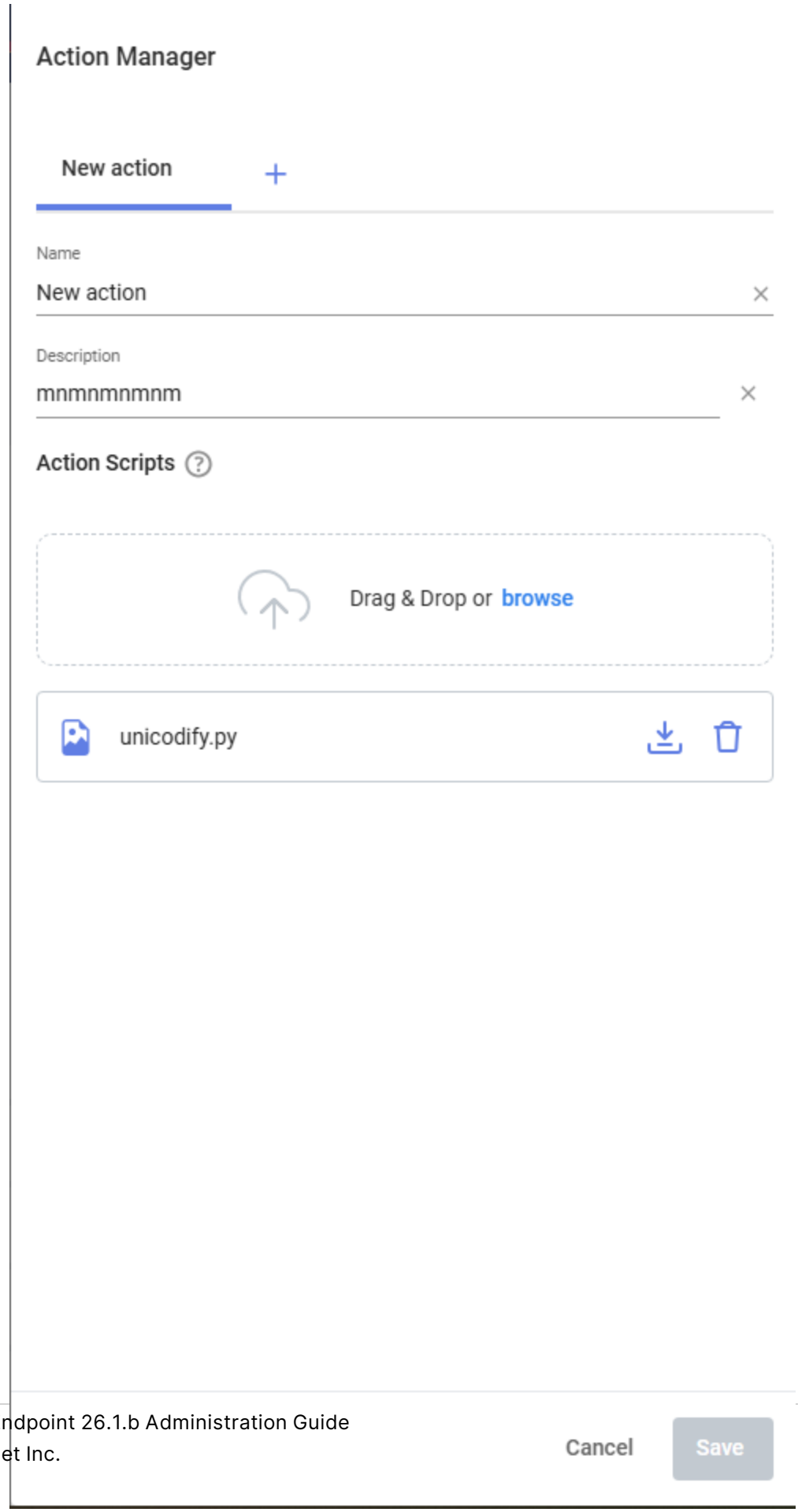
EDR enables you to define connectors to external systems, so that EDR will automatically trigger predefined actions when a security event is triggered in EDR. You can define your own actions while defining a Custom integration connector, Firewall integration connector or NAC integration connector (as described above). Each action is comprised of a Python script (one or several ones) that calls an API from the third-party system in order to perform the relevant action.

The Action Manager enables you to upload and manage (add, modify and delete) these actions and the Python scripts that call third-party systems' APIs. Python 2.7 or later is supported.

To display the Action Manager:

1. Go to *Profiles* > *Integrations* > *Connectors*.

2. Click the *Action Manager* button. The following displays:


Action Manager
New action
Name
New action
Description
mnmnmnmnm
Action Scripts
Drag & Drop or browse
unicodify.py
Cancel
Save

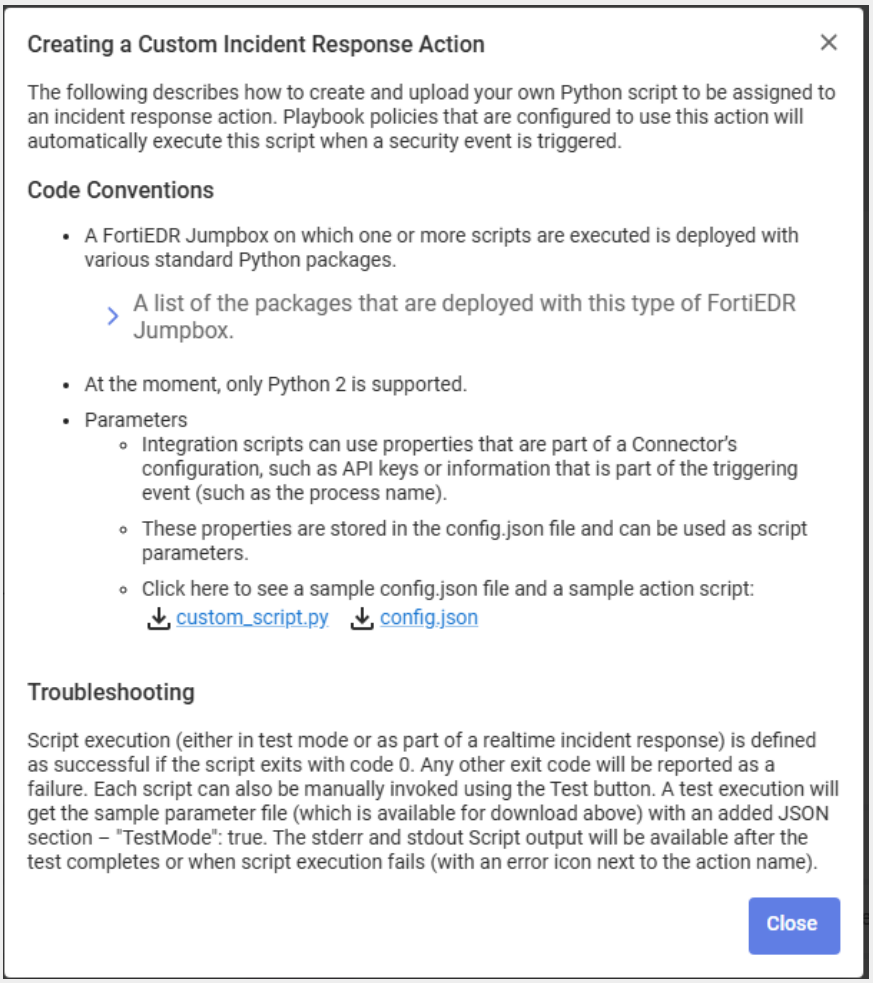
To define a new action:

1. Click the *+ Add action* button.
2. Fill out the fields of this window as follows in order to define a new action to be triggered in response to an incident.



In order to trigger this action, a Playbook policy must be defined that triggers this action to execute the script when a security event is triggered. The definition of this new action here automatically adds this action as an option in a Playbook policy. This action however, is not selected by default in the Playbook policy. Therefore, you must go to the Playbook policy and select it in order for it to be triggered when a security event is triggered.

Field	Definition
Name	Enter any name for this action.
Description	Enter a description of this action.
Upload	Upload a Python script that calls an API from the third-party system in order to perform the relevant action. Python 2.7 or later is supported. This Python script must be created according to the coding conventions that can be displayed by clicking the icon next to the *Action Scripts* field. The following displays providing an explanation of these coding conventions and provides various links that you can click to see more detail and/or to download sample files.

Field	Definition
	

3. Click *Save*.

To modify the script of an action:

1. Go to *Profiles* > *Integrations* > *Connectors*.
2. Click the *Action Manager* button.
3. Select the action of the script to be modified.
4. In the *Action Scripts* area, hover over the name of the script in order to display various tools, as follows:

Tool	Description
	To download the action's current script. For example, so that you can edit it.
	To delete the action's selected script.

Tool	Description
	To upload a new Python script that calls an API from the third-party system in order to perform the relevant action. Python 2.7 or later is supported.

5. Click *Save*.

Playbooks

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

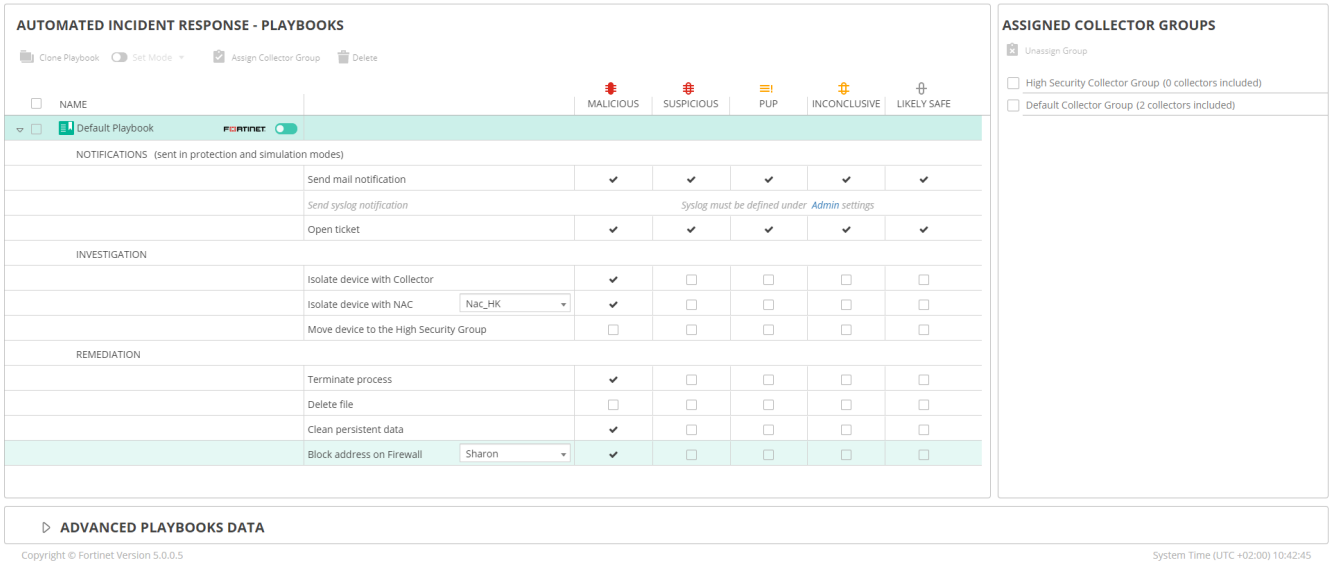
EDR provides the following Playbook policy out of the box:

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

Automated Incident Response - Playbooks Page

The *AUTOMATED INCIDENT RESPONSE – PLAYBOOKS* page displays a row for each Playbook policy. To access this page, select *Profiles* > *Playbooks*.

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



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

- There are more options and actions than those shown above that can be added to a Playbook policy, such as the blocking of a malicious IP address. You may consult Fortinet Support about how to add them.
- Automatic Incident Response Playbook features can also be triggered by extended detection events when follow-up actions are configured for the Collector Group of a device on which the event triggered. This enables the system to follow up upon the detection of such an event and execute a sequence of actions, such as to block an address on a firewall or to isolate the device in which part of the event occurred.

Assigned Collector Groups

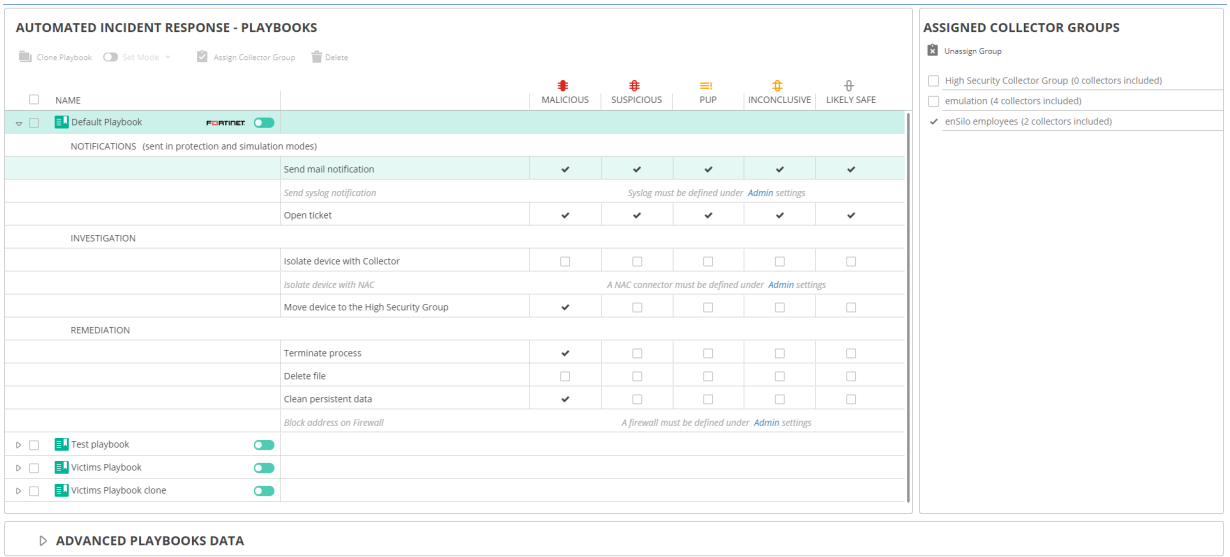
The Assigned Collector Groups pane on the right lists the various Collector Groups in the system. By default, all Collector Groups are assigned to the Default Playbook policy. You can reassign one or more Collector Groups to different Playbook policies, if preferred.

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

Cloning a Playbook Policy

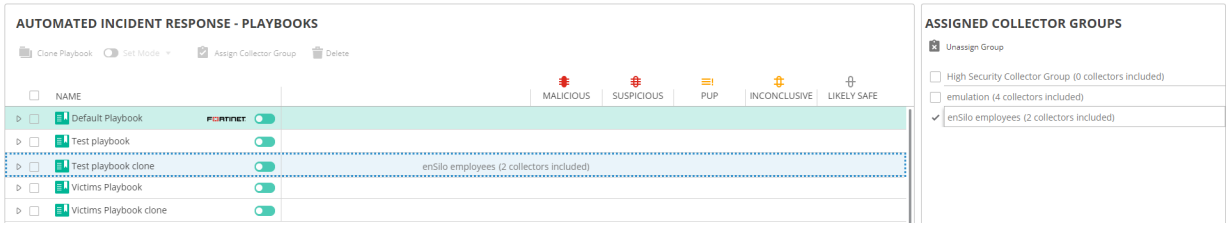
Cloning a Playbook policy unassigns the policy from one Collector Group and then reassigns it to a different Collector Group. A Collector Group can only be assigned to one Playbook policy.

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

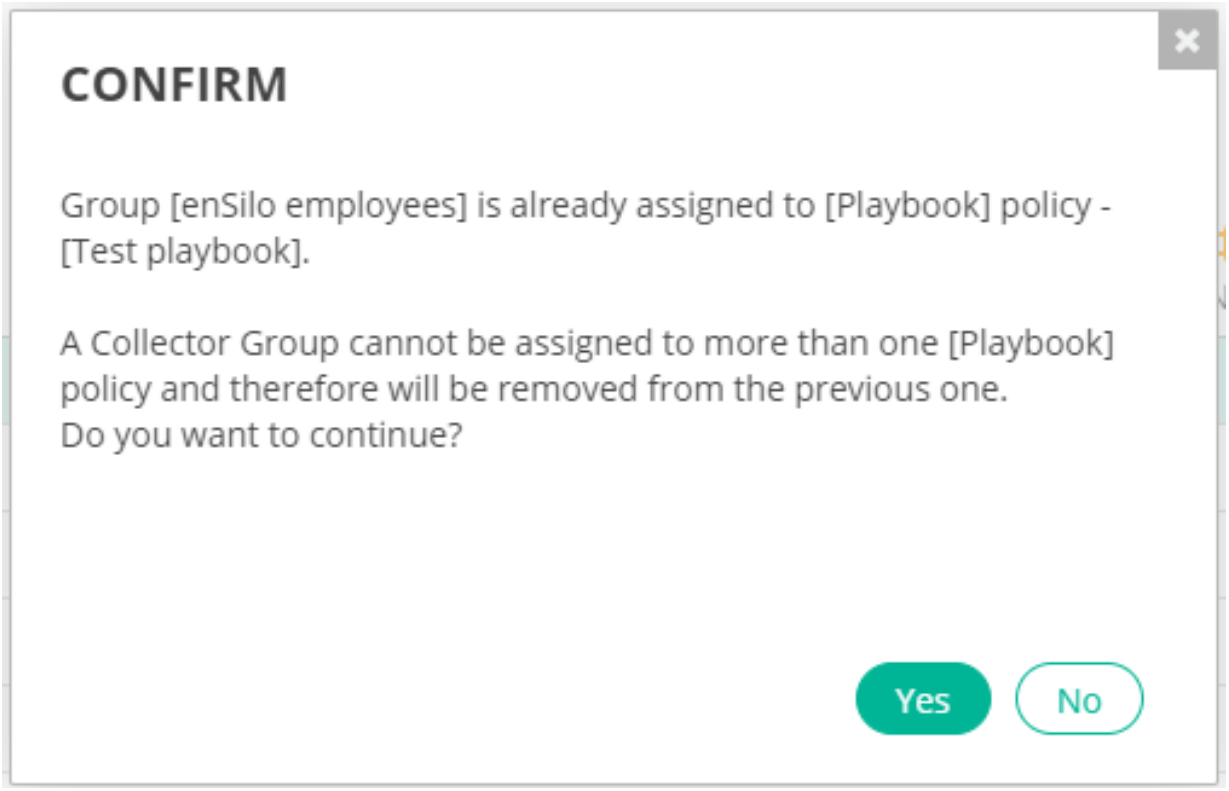


   b. Click *Collector Group* in the *Assigned Collector Groups* pane that you want to assign to the cloned Playbook policy. Then, drag the Collector Group onto the cloned Playbook policy in the *Playbook*

Policies list, as shown below:



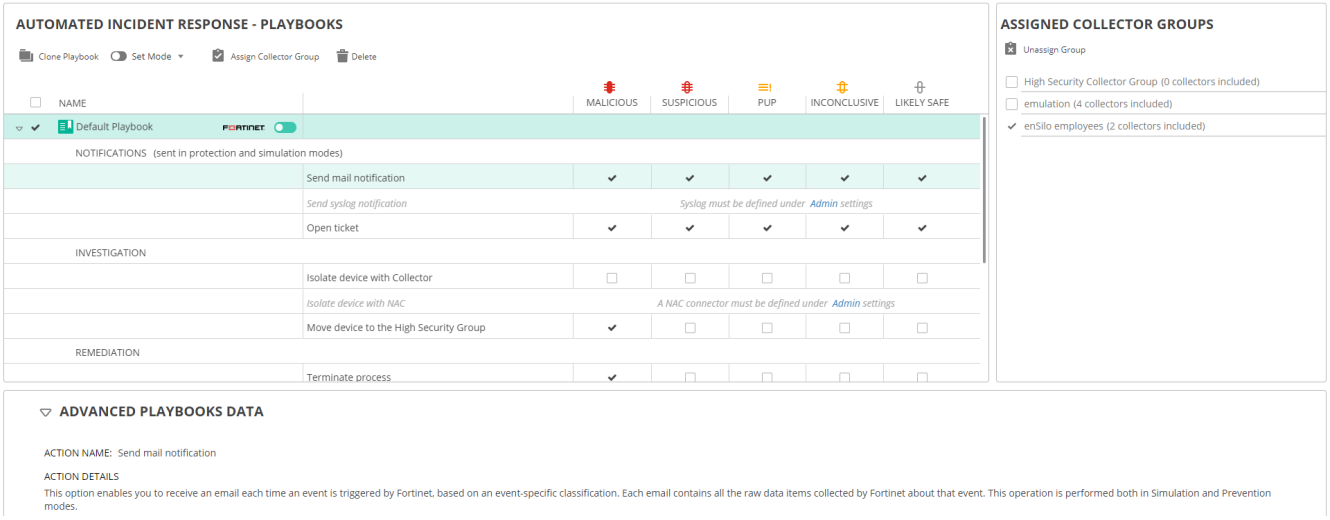
The following message displays.



Click *Yes*.

Advanced Playbooks Data

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



Playbook policy actions

Playbook policy actions are divided into the following types:

- Notifications on page 787
- Investigation on page 789
- Remediation on page 790
- Custom on page 791

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 EDR modes (Simulation and Prevention).

Notifications can be one of the following types:

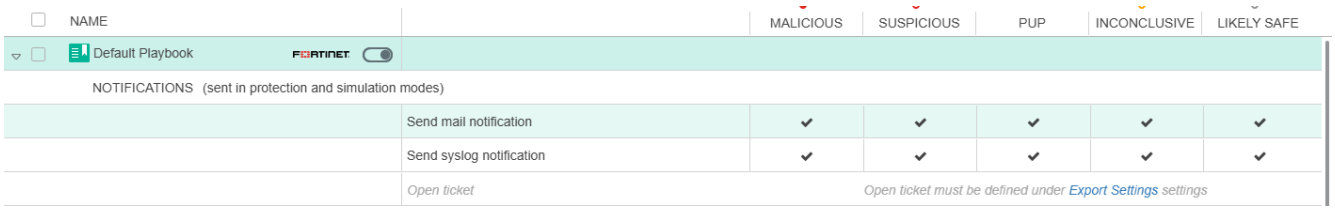
- Emails
- Syslog
- Open Ticket

Notification actions must be enabled in order to be implemented by a Playbook policy. If notifications are disabled, they are not implemented by the Playbook policy, even if that policy is configured to send notifications. For more details see .

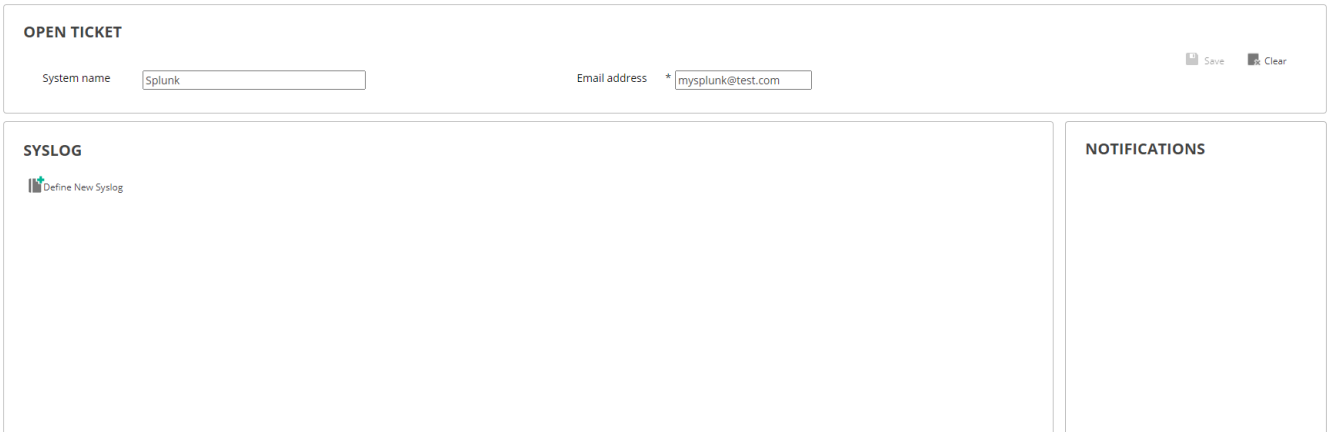
Each row under *Notifications* corresponds to a single type of notification (mail [email] notification, Syslog notification or Open Ticket notification). In the *Notifications* area, you configure each notification type to indicate whether or not it is to automatically send the relevant notification, once triggered by a security event.

The *Malicious*, *Suspicious*, *PUP*, *Inconclusive*, and *Likely Safe* columns correspond to the possible classifications (see Overview on page 575 and Incidents pane on page 571) for a security event. When a checkmark ✔ appears in one of these columns, it means that a notification of the specified type is sent when an event is triggered with that classification.

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



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, with a link to the following configuration page when clicked:



Notifications are sent based on the Core or EDR Cloud Service (FCS) classification of the event, depending on whether the FCS classification happens within the timeout period and whether the FCS classification result differs from the one from the Core:

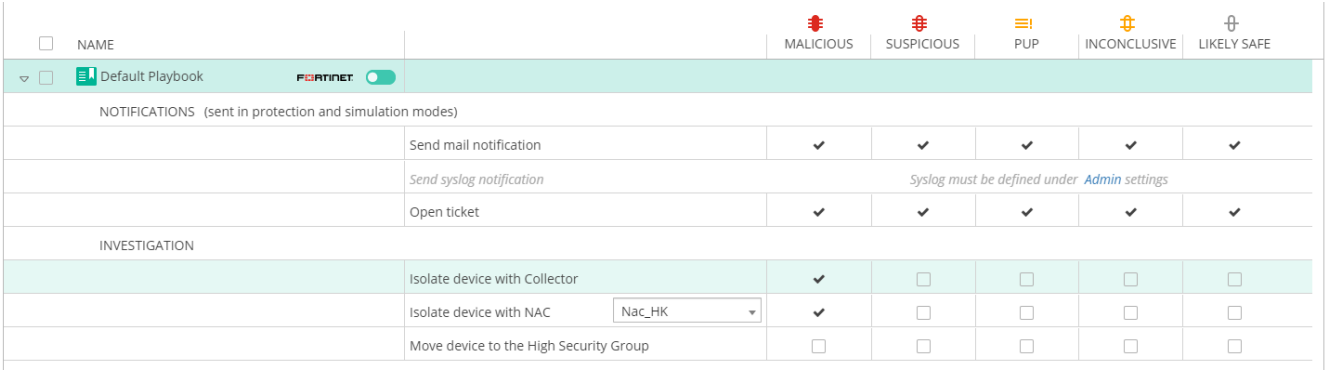


The default timeout period for FCS classification is 3 minutes. To change the default FCS timeout value for your dedicated environment, contact Fortinet Support.

- If the FCS classification is received within the timeout period, the notification is sent based on the FCS classification.
- If the FCS classification result is not received within the timeout period, a notification is sent by the end of the timeout based on the initial Core classification.
- If the FCS classification comes in after the timeout with a different result from the Core classification, an updated notification is sent based on the final classification by the FCS.

Investigation

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



Investigation actions can be one of the following types:

- Isolate device with NAC on page 789
- Move device to High Security Group on page 789

All investigation actions are performed based on EDR Cloud Service (FCS) classification. If FCS is not running, EDR performs investigation actions based on Core classification instead.

Isolate device with NAC

This action blocks the communication to/from the affected device by disabling this host on an external Network Access Control system. A NAC connector must already be configured in order to perform this action. For details about how to configure NAC connectors, see Network Access Control (NAC) integration on page 735.

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

Devices that were isolated using an external system such as a NAC are not indicated as such on the EDR Console and un-isolation is only possible on the external NAC system.

Move device to High Security Group

EDR 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.

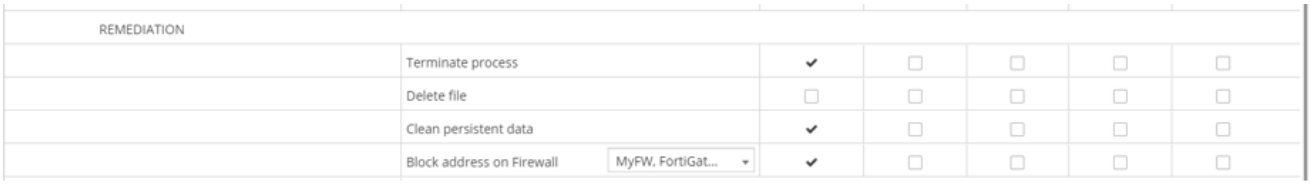
A checkmark ✔ in a classification column here means that the device is automatically moved (assigned) to the High Security Collector Group when a security event is triggered that has that classification. This feature is useful when you want to mark Collectors that triggered malicious events.

Move device to High security group	✔	✔	✔	✔	☐

Remediation

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

All EDR remediation actions are based on the final classification of a security event by the EDR Cloud Service (FCS), which is a cloud-based, software only service that determines the exact classification of security events with a high degree of accuracy.



Remediation actions can be one of the following types:

- Terminate process on page 790
- Delete file on page 790
- Clean persistent data on page 790
- Block address on Firewall on page 790

Terminate process

This action terminates the affected process. It does not guarantee that the affected process will not attempt to execute again. This action can also be performed manually using the Forensics add-on, as described on Remediating a device upon malware detection on page 641

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

Delete file

This action ensures that the file does not attempt to exfiltrate data again, as the file is permanently removed from the device. This action can also be performed manually using the Forensics add-on, as described on Remediating a device upon malware detection on page 641

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

Clean persistent data

This action cleans the registry keys in Windows. This action can also be performed manually using the Forensics add-on, as described on Remediating a device upon malware detection on page 641.

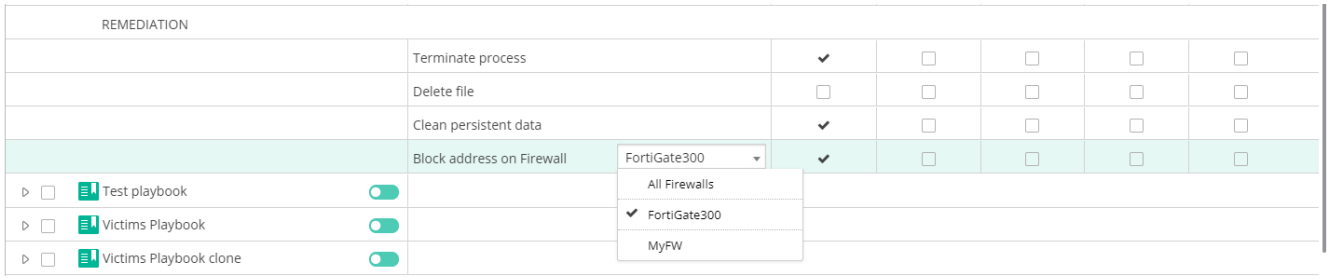
A checkmark ✔ in a classification column here means that the affected registry key is automatically cleaned on the device when a security event is triggered that has that classification.

Block address on Firewall

This action ensures that connections to remote malicious addresses that are associated with the security event are blocked. A Firewall Connector must already be configured in order to perform this action. For

details about how to configure firewall connectors, see Firewall Integration on Firewall integration on page 727.

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:



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.

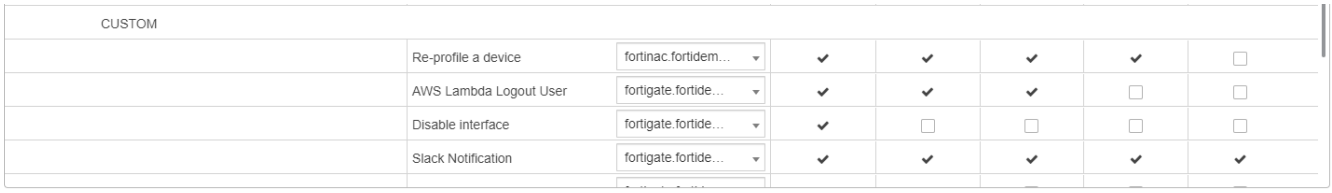
The firewall must already be configured in order to add malicious destinations to blocked addresses. If its settings are not already configured, the relevant row in the Remediation list displays a message indicating that you must first configure it, with a link to the relevant place in the user interface to configure it.



Clicking

Custom

Custom actions enable you to automatically trigger an incident response in a third-party system as the result of a security event detected by EDR, according to the Custom Integration connector (and its actions) that you define.



The *CUSTOM* section of the *Playbook* page lists the actions that have been defined for Custom Integration Connectors, as described on Custom integration on page 770.

This list appears empty if no custom integration connector has been defined.

A checkmark ✔ in a classification column here means that the defined action is triggered in the third-party system when a security event is triggered that has that classification.

Other options in the Playbooks tab

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

- *Clone Playbook*: Clones a Playbook policy, as described on Playbooks on page 784.
- *Set Mode*: Changes the mode of the Playbook policy. This process is similar to that for setting the mode for a standard security policy, which is described on Setting a security policy's Prevention or Simulation mode on page 678
- *Assign Collector Group*: Assigns a Playbook policy to a Collector Group. This process is similar to that for assigning a standard security policy to a Collector Group, which is described on Assigning a security policy to a Collector Group on page 681.
- *Delete*: Deletes a cloned Playbook policy. Default Playbook policies cannot be deleted.



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

Export settings

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

- Open Ticket on page 792
- Syslog on page 793

Open Ticket

The *Open Ticket* option enables you to send events to an event-management tool such as Jira or ServiceNow. Open Ticket automatically opens a ticket and attaches the relevant event to a ticket.

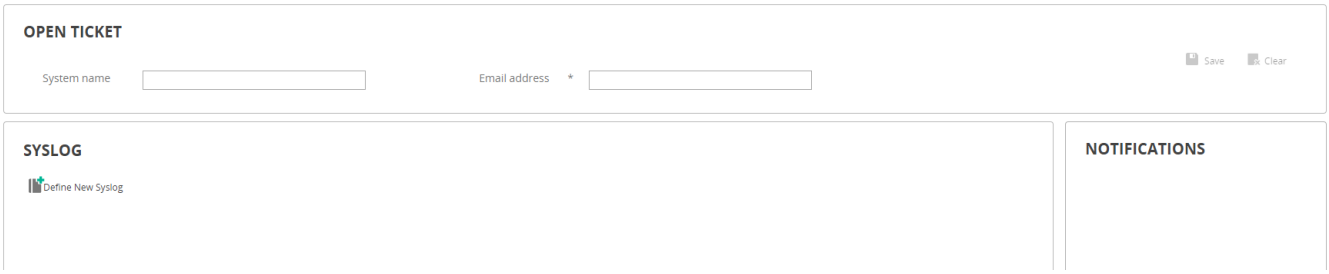
In order for the Open Ticket feature to work properly, you must set up an email feed in the event-management tool to be used.



Most event-management tools are supported. EDR 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 799.



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.

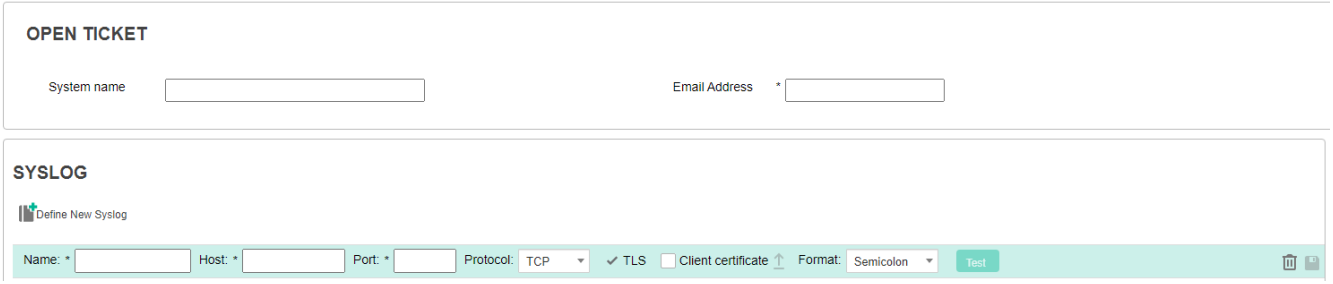


To configure Open Ticket settings:

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 EDR. All tickets from all organizations are sent to this email.
3. Click *Save*.

Syslog

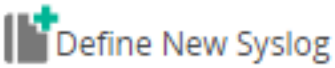
The *SYSLOG* option enables you to configure EDR to automatically send EDR events to one or more standard Security Information and Event Management (SIEM) solutions (such as FortiAnalyzer) via Syslog.



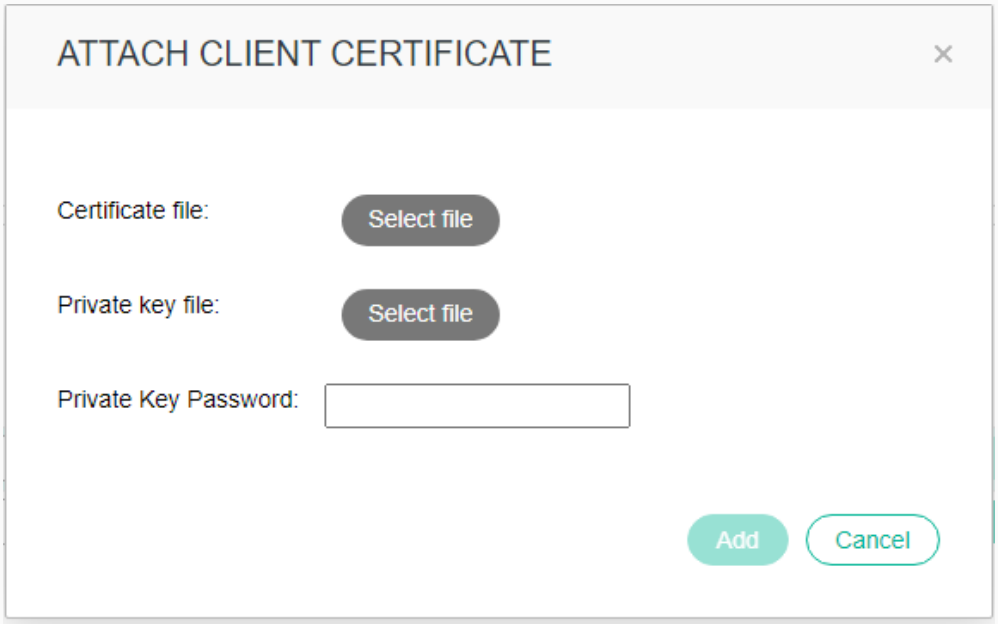
All Syslog messages in EDR originate from the Central Manager. The source IP address for syslog messages is the IP of the Central Manager. The EDR Central Manager server sends the raw data for security event aggregations. Each entry contains a raw data ID and an event ID. Variants belonging to the same 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 EDR system.

Syslog messages are only sent for security events that occur on devices that are part of Collector Groups that are assigned to a Playbook policy in which the *Send Syslog Notification* option is checked.

To define a new Syslog destination:

1. Click the 

button.
2. Specify the following attributes:

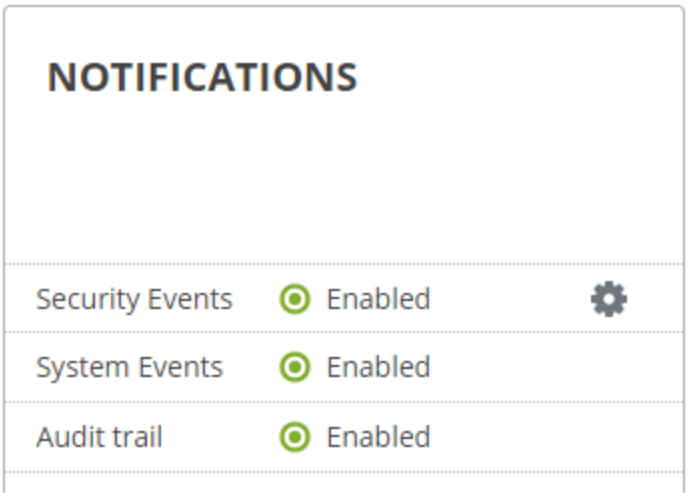
Attribute	Description
Syslog Name	Free-text field that identifies this destination in the EDR.
Host	Host name of the Syslog server.
Port	Port of the Syslog server.
Protocol	Protocol of the Syslog server. You can select *TCP* or *UDP*.
TLS	When *TCP* is selected in *Protocol*, use this option to specify whether to enable TLS. If the Syslog server requires a client-side certificate, you must enable *TLS* before you can upload the certificate.
Client Certificate	If the Syslog server requires a client-side certificate, enable *TLS* and use this option to upload a certificate. For example, if your FortiAnalyzer server requires a client-side certificate, contact Fortinet Support to obtain appropriate client certificate files and upload them here. 
Format	Select the type of the syslog server: • *Semicolon*—Select this option if the syslog server is not one the following three. EDR then uses the default CSV syslog format. • *FAZ*—The syslog server is FortiAnalyzer. FortiAnalyzer Cloud is not supported. • *CEF*—The syslog server uses the CEF syslog format. • *LEEF*—The syslog server uses the LEEF syslog format.

Attribute	Description
	Refer to EDR Syslog Message Reference for more details about syslog message fields for different formats.

3. Click the *Test* button to test the connection to the Syslog destination server.
4. Click the button to save the Syslog destination.

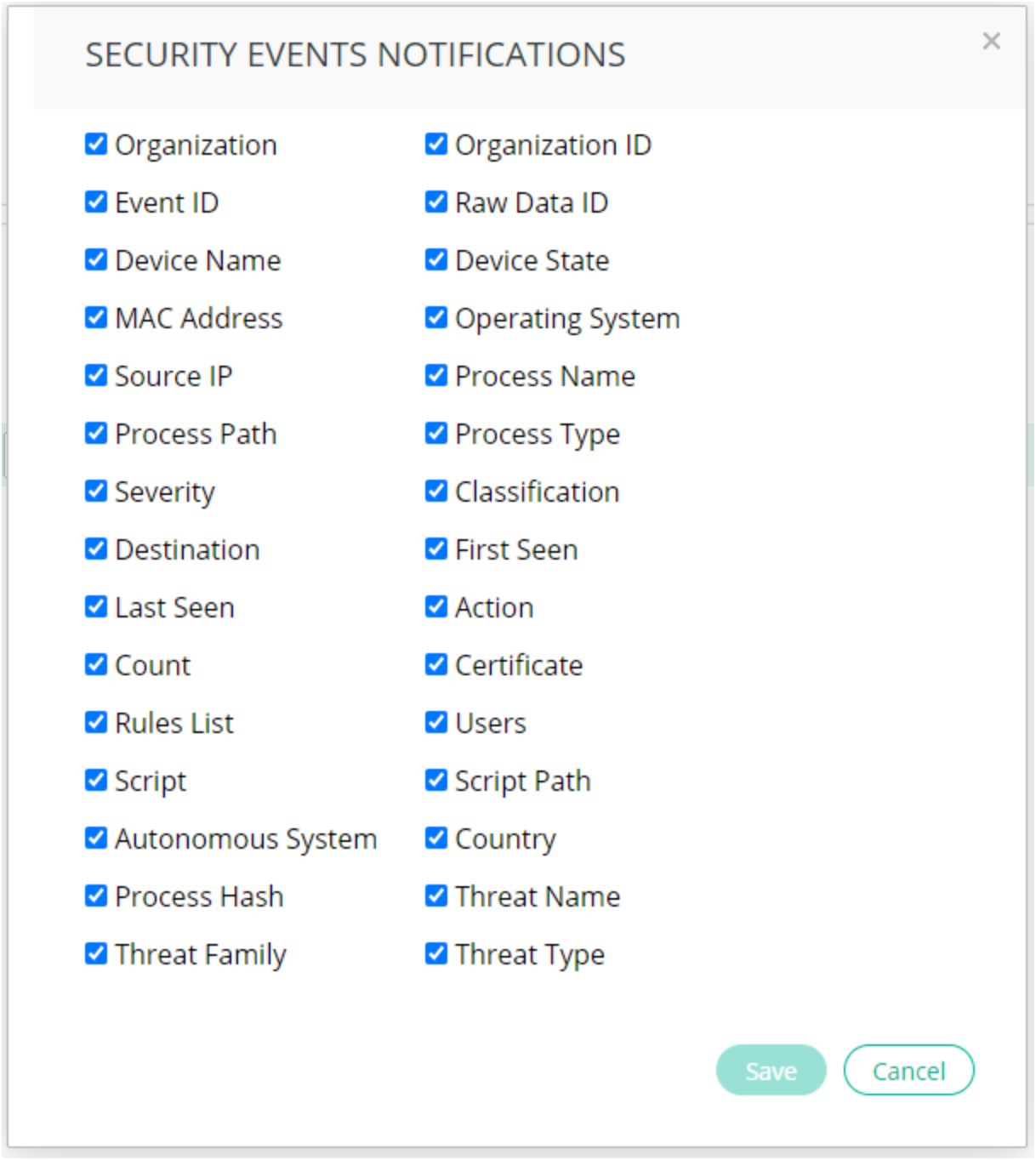
To select which syslog messages to send:

1. Select a syslog destination row.
2. Use the sliders in the *NOTIFICATIONS* pane on the right to enable or disable the destination per event type (system events, security events or audit trail) as shown below:



To select which fields will be included in the syslog messages:

Click the button on the right of the event type and check the checkbox of the fields that you want to be sent to your Syslog.



You can also define a Syslog destination via REST API, including the upload of a certificate using Rest API during the process. By default, all available syslog fields and all notifications options, including security, system, and audit events, are enabled. For more details, refer to the EDR RESTful API Guide. You must log in to the Fortinet Developer Network to access the guide.

Warning: If syslog is configured for both Hoster view and an organization, two syslog events will be sent.

For more information on syslog messages, such as message types and fields, see EDR Syslog Message Reference.

Troubleshooting

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



For debugging and troubleshooting, Fortinet Support may request that you provide the logs for the EDR devices deployed in your organization.



If your system includes the Forensics add-on, you can use the Retrieve Memory function to retrieve memory related to a specific stack on a specific Collector. For more details, you may refer to Retrieving memory on page 584.

An EDR Collector does not display in the EMS *Endpoints > All Endpoints* tab

After an EDR Collector is first launched, it registers with the EDR Central Manager console and is displayed in the *Endpoints > All Endpoints* tab in EMS. If it does not appear to have registered, then perform the following:

1. Check that the device on which the EDR Collector is installed is powered on and has an Internet connection.
2. Validate that ports 8081 and 555 are available and that no other third-party product is blocking these ports.

No events on the EDR Central Manager console

If no events are displayed in the EDR 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 EDR Collector and connecting to the EDR Core IP via port 555.
- Running Telnet on the EDR Core and attempting to connect to the EDR Aggregator IP on port 8081.

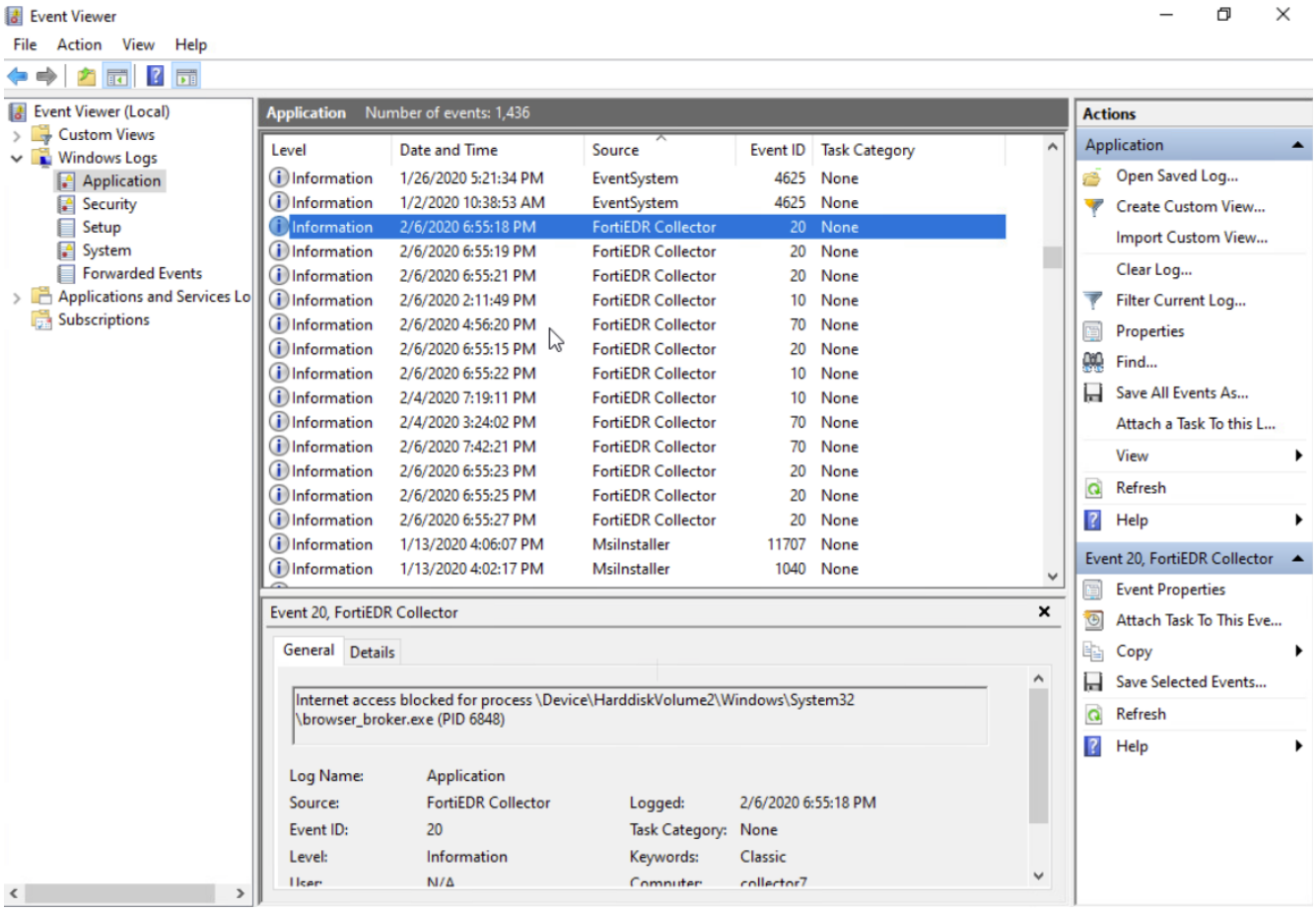


Make sure that Telnet is enabled on Windows.

User cannot communicate externally or files modification activity is blocked

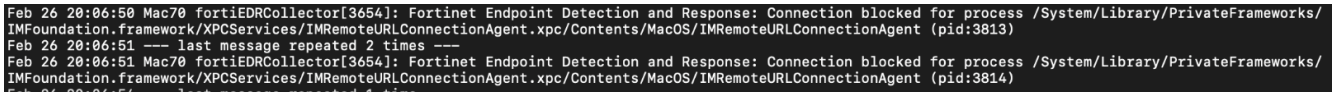
Microsoft Windows-based devices

The Windows Event Viewer records whenever an EDR Collector blocks communication from a device or file modification related to ransomware activity. This information is recorded in the Windows Event Viewer log located in the following location: *Event Viewer > Windows Logs > Application*.



macOS-based devices

The mconsole records whenever an EDR 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:



Threat Hunting tab does not show expected activity events

If the Threat Hunting tab does not show expected activity events after installation, perform the following troubleshooting steps:

1. Check which Collectors group the triggering device belongs to.
2. Check the Threat Hunting Collection profile assigned to this group and make sure the profile includes the activity events you are searching for in the Threat Hunting tab.
3. If the profile includes the activity events but the Threat Hunting tab still does not show them, check the installation status of the Threat Hunting repository by running the `kubectl get pods -n edr2-onprem` command in the Threat Hunting repository console.
4. Verify the status is *Running* for all entries. See example below. Otherwise, reinstall the Threat Hunting repository.

```
master1 [~]# kubectl get pods -n edr2-onprem
NAME                                          READY   STATUS    RESTARTS   AGE
edr2-onprem-edr-streamer-c4d4dc9f4-25scq      1/1     Running   0          54m
edr2-onprem-edr-streamer-c4d4dc9f4-vmw2r      1/1     Running   4          56m
edr2-onprem-edr-streamer-sink-5d79bd87c4-2r56m   1/1     Running   0          54m
edr2-onprem-edr-streamer-sink-5d79bd87c4-66plb   1/1     Running   0          54m
edr2-onprem-entity-operator-56855b7b8d-qrm2m  3/3     Running   18         6d14h
edr2-onprem-kafka-0                           2/2     Running   9          6d14h
edr2-onprem-kafka-exporter-bc648bcb5-v6vt9    1/1     Running   12         6d14h
edr2-onprem-middleware-5df46877b6-wglx6       1/1     Running   0          57m
edr2-onprem-od-kibana-8567c97c88-m9glx        1/1     Running   3          6d14h
edr2-onprem-od-master-0                       1/1     Running   3          6d14h
edr2-onprem-od-opendistrowarm-data-0          1/1     Running   3          6d14h
edr2-onprem-zookeeper-0                       1/1     Running   5          6d14h
svclb-edr2-onprem-middleware-xtf5m            1/1     Running   3          6d14h
```

Collector is slow or hangs

If an endpoint is slow or hangs, check the Collector logs. It might be caused by collision with another AV product that EDR is running in parallel with. You can fix the collision by excluding AV exceptions in both EDR and the other AV product.

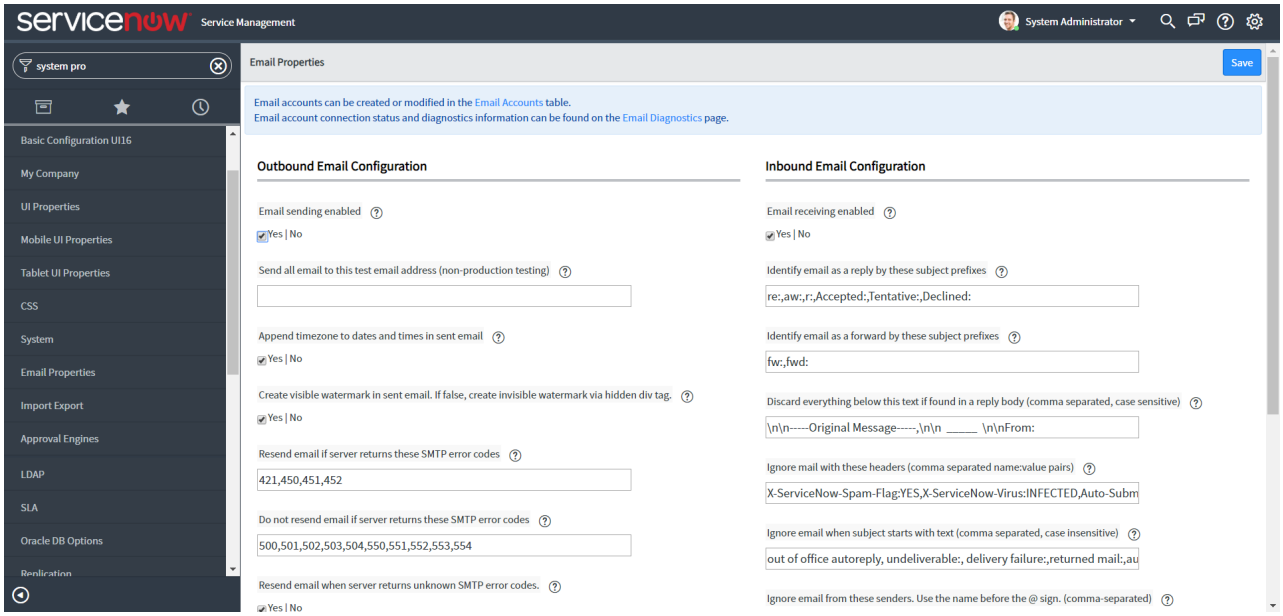
Appendix A – Setting up an email feed for open ticket

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

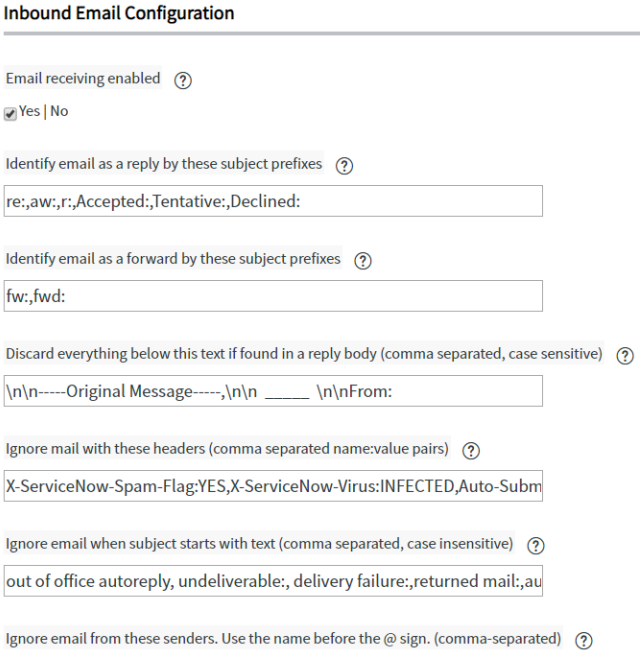
In order for the Open Ticket feature to work properly, you must set up a receiving email feed in the event-management tool to be used. This appendix provides an example that describes how to set up the required email feed in ServiceNow.

To set up an email feed in ServiceNow:

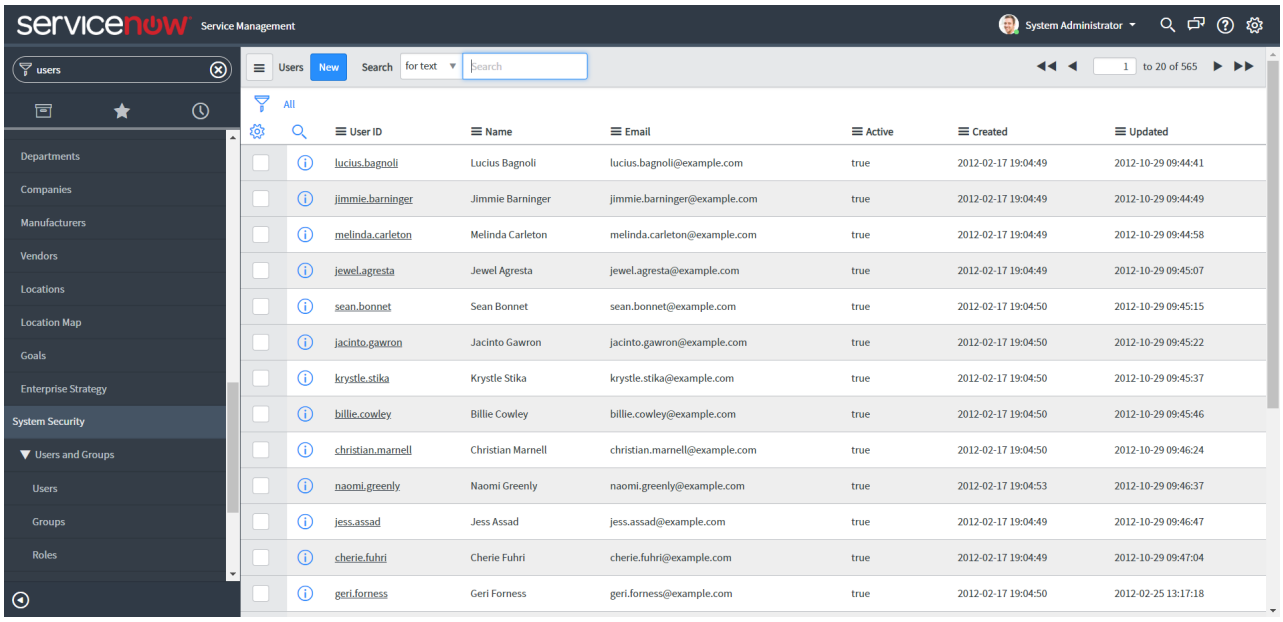
1. Launch ServiceNow.
2. In the window that opens, select *System Properties* > *Email Properties*. The following window displays:



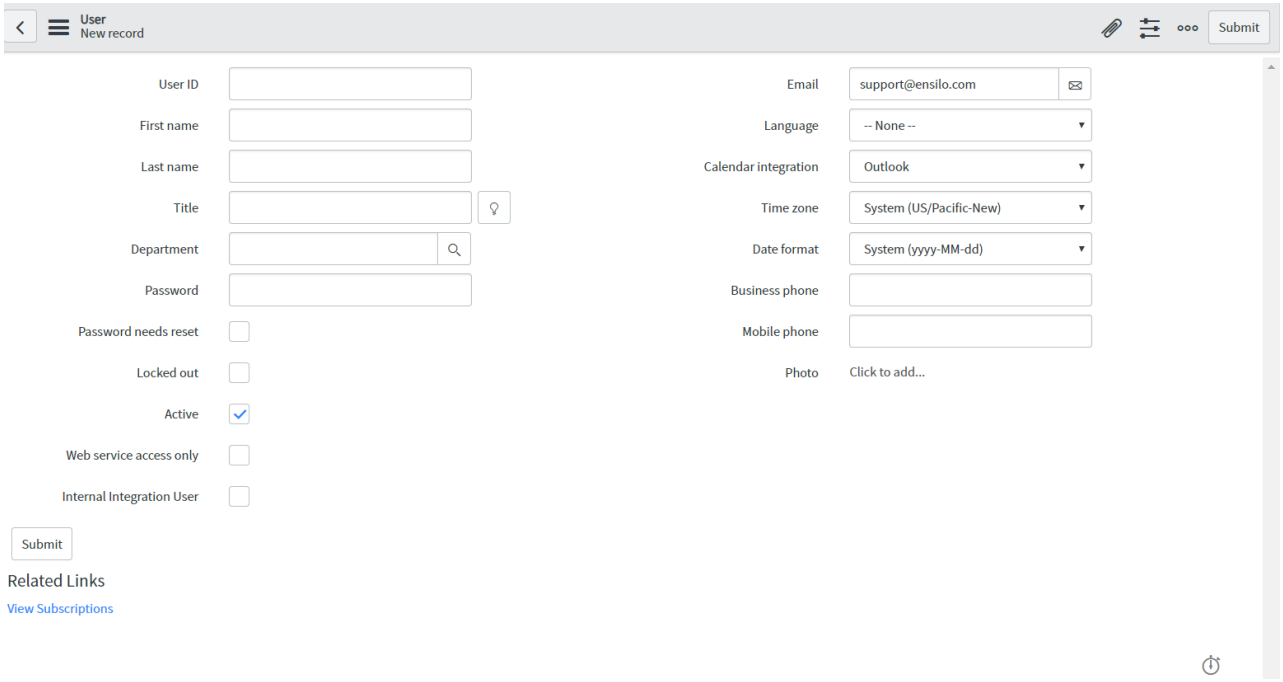
3. In the *Inbound Email Configuration* area, check the *Email receiving enabled* checkbox.



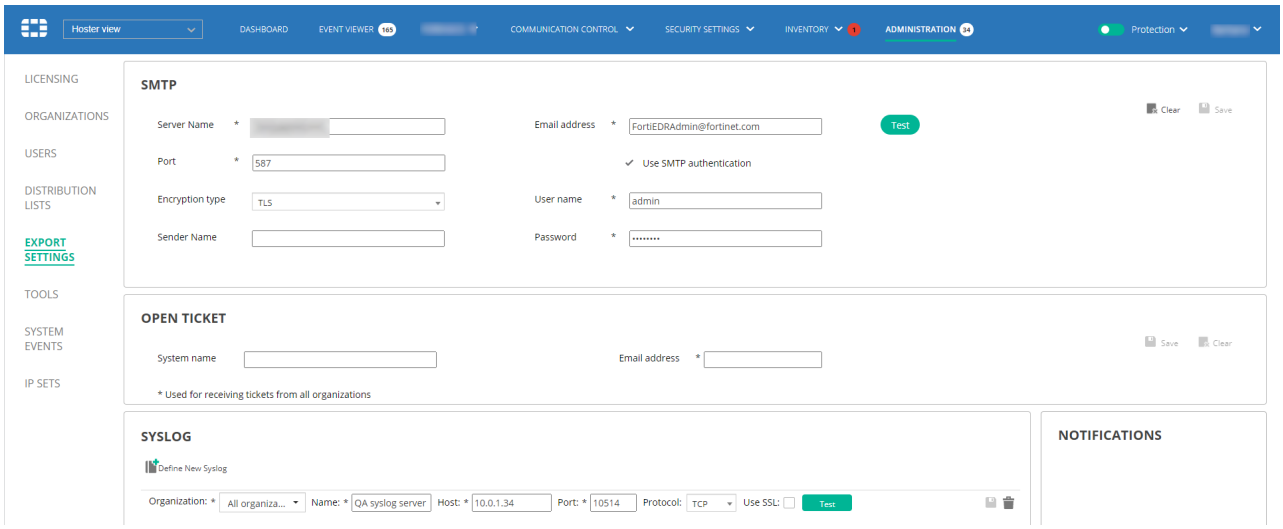
4. In the left pane, select *System Security* > *Users and Groups* > *Users*. The following window displays:



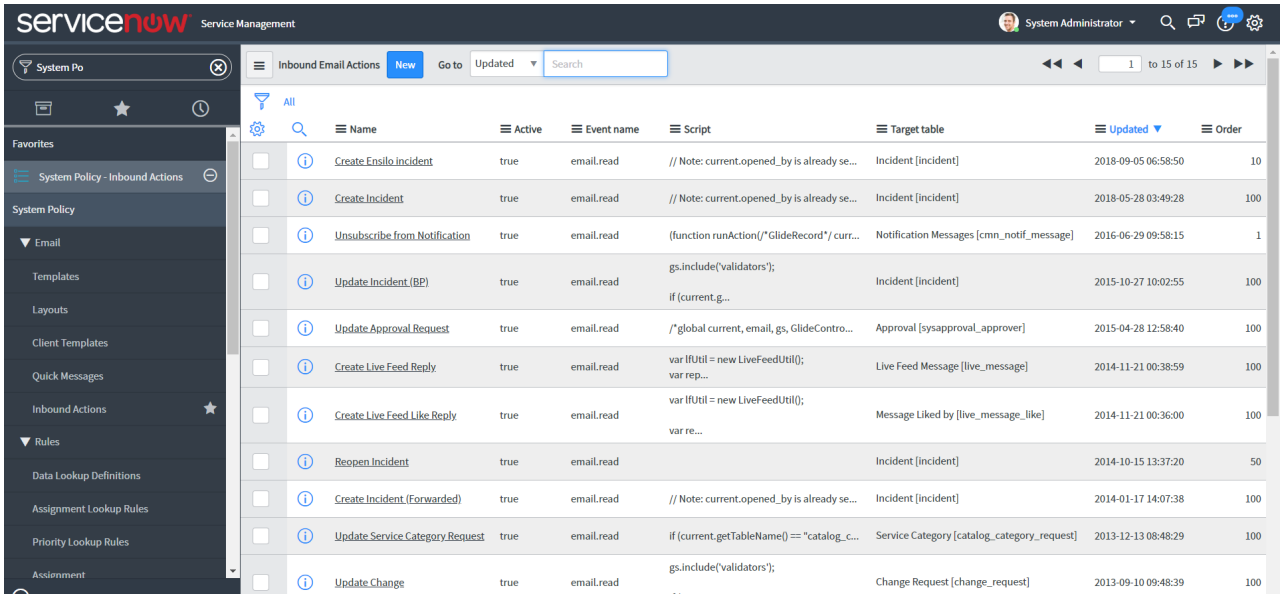
5. Click the *New* button to create a new user. The following window displays:



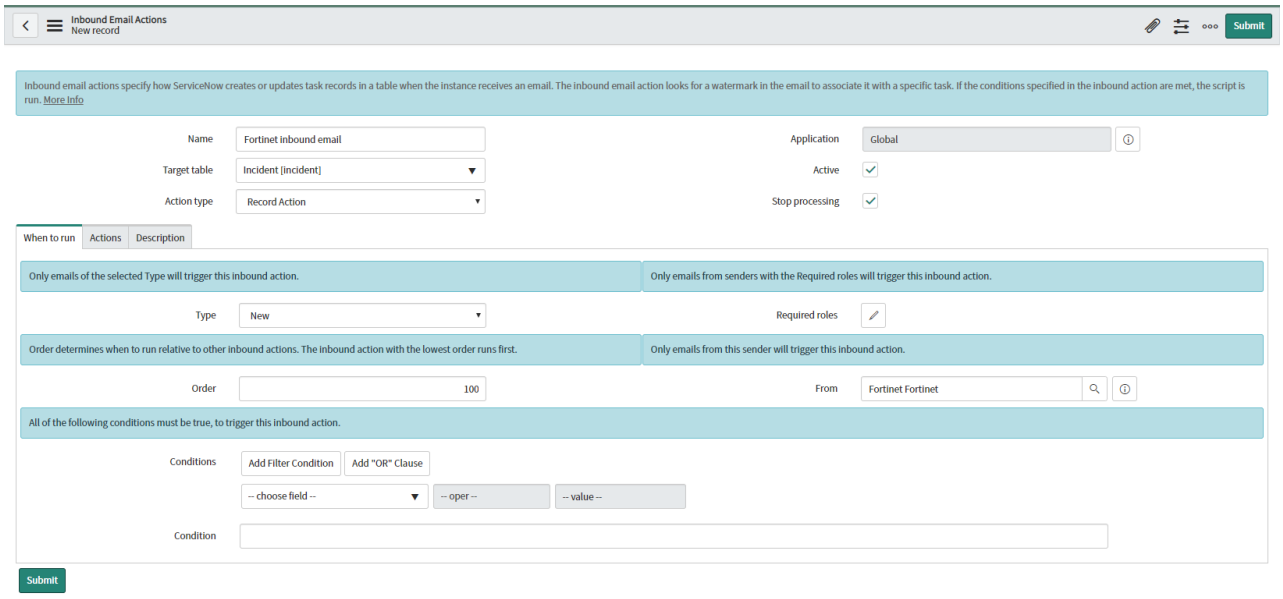
6. In the *Email* field, enter the email address of the EDR messaging system. This email address is specified in the *Email Address* field of the EDR Open Ticket settings, which can be accessed by selecting *Profiles* > *Export Settings* in the EDR user interface, as shown below:



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



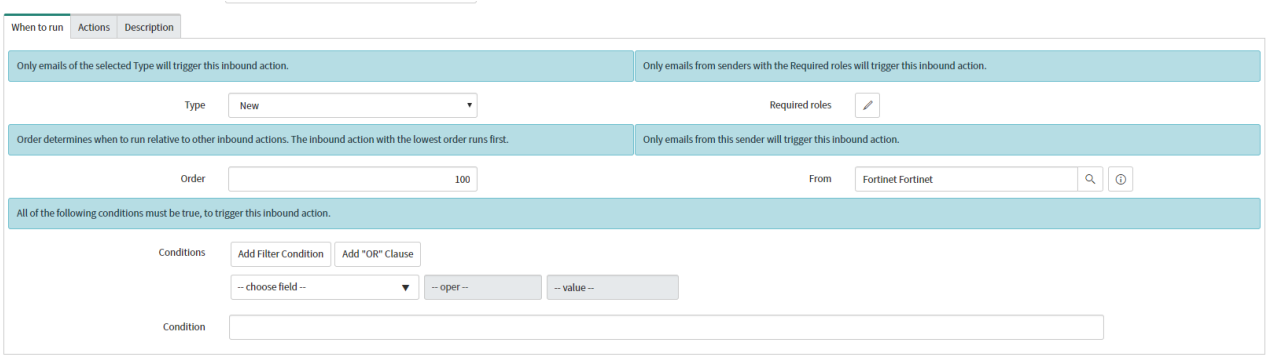
8. Click the *New* blue button to create new inbound email actions. The following window displays:



9. Fill in the following fields in this window:

Field	Definition
Name	Enter a free-text name for the inbound email feed. For example, `Fortinet inbound email`.
Target table	Select *Incident [incident]* in the dropdown list.
Action type	Select *Record Action* in the dropdown list.
Active	Check this checkbox to select it.
Stop Processing	Check this checkbox to select it.

10. In this window, select the *When to run* tab and then in the *From* field, select the EDR user created in step 6.



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

```
//  Note: current.opened_by is already set to the first UserID that matches the From: email
address
current.caller_id = gs.getUserID();
current.comments = “received from: “ + email.origemail + “\n\n” + email.body_text;
current.short_description = email.subject;
current.category = “request”;
current.incident_state = 1;
current.notify = 2;
current.contact_type = “email”;

//set highest priority for emails from EDR notification
if (email.origemail == "doNotReply@fortinet.com") {
    current.impact=1;

    current.urgency=1;
}

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

if (email.importance != undefined) {
    if (email.importance.toLowerCase() == "high")
        current.priority = 1;
}

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

```
var classificationStart = email.body_text.indexOf('Classification:') + 15;

var destinitionStart = email.body_text.indexOf('Destinations:');


var severity = email.body_text.slice(severityStart, classificationStart -15 );

var classification = email.body_text.slice(classificationStart, destinitionStart);

 current.insert();
```

12. When pasting in the JavaScript, make sure that:
    - The emails address on line 11(see above) is the same as that specified in Email Address field of the EDR Open Ticket settings (see step 6).
    - You set the *current.impact* and *current.urgency* fields on lines 12 and 14 to specify the impact and urgency values for ServiceNow.
      Various types of information can be extracted from the email sent by EDR. For example, the text on line 33 in the JavaScript (see above) is an example of how to extract the classification value of this event from the email.
13. Click the *Submit* button in the ServiceNow window. This completes the email feed setup.
    When EDR 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);

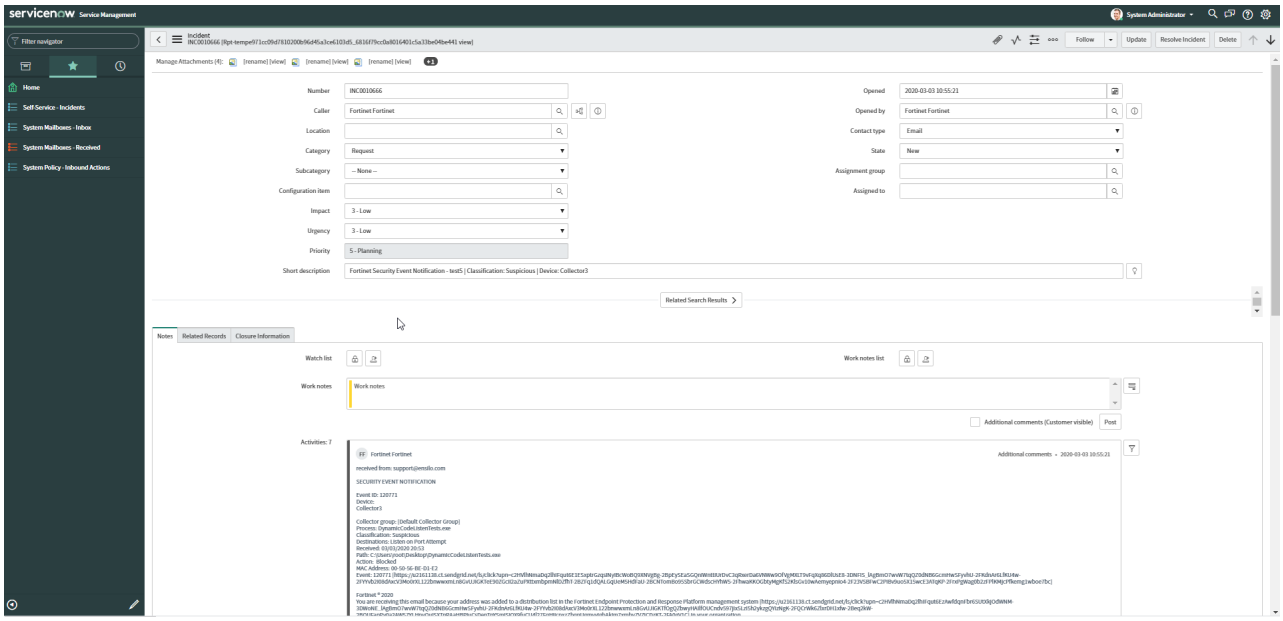
            current.comments =("EventId from JSON: " + parsed.EventId);

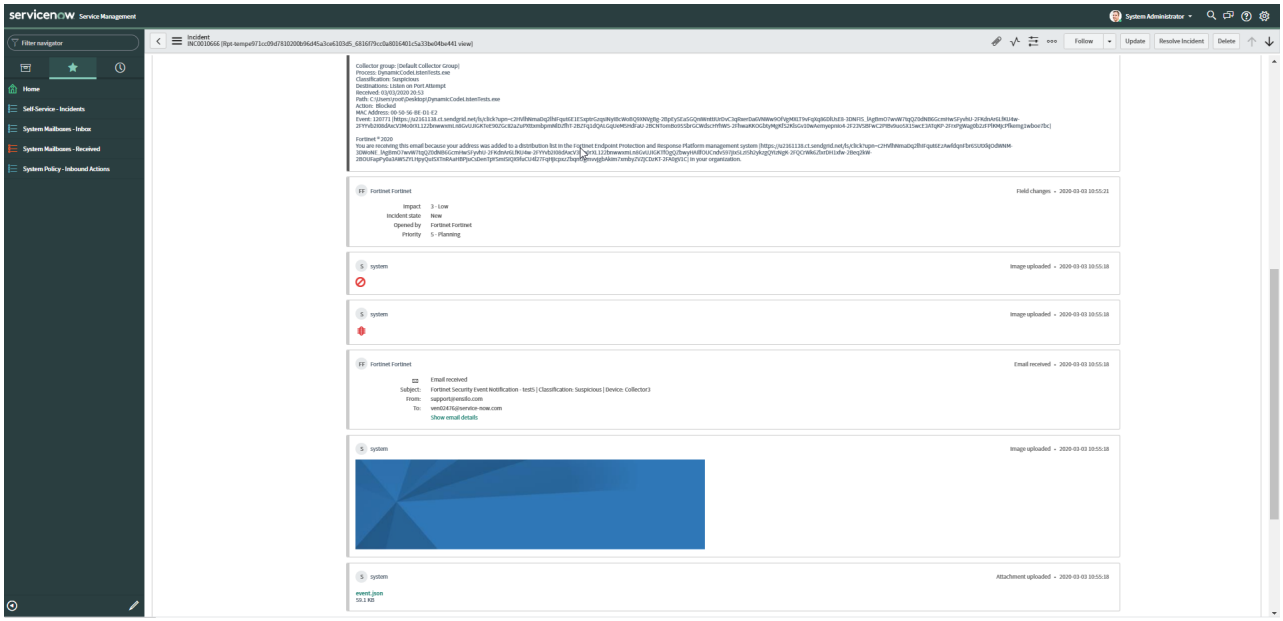
            }

    }

}
```

The following shows how an event appears when received in ServiceNow, after being sent from EDR:





Appendix B - Lucene syntax

The EDR Threat Hunting free-text query is based on Lucene syntax. This syntax consists of terms and operators, as described below. For more details about the use of this query, see Threat Hunting on page 608.



You can convert JSON and XML syntax queries into Lucene syntax using the built-in *Convert Query* button in the *Free-text Query* filter.

Terms

A *free-text term* is a single word (for example NetworkService or CryptSvc) or a phrase surrounded by double quotes (for example, ”NetworkService -p -s CryptSvc”) that searches for all the words in a phrase (in the same order) regardless of the field in which the words appear.

A *Field: Value* term is a combination of a field and a value.

A list of available fields is provided in the query box, which is an automatically-complete dropdown list.

Examples

Where the Source command line contains the value NetworkService:

```
Source.CommandLine: NetworkService
```

Where the value of the remote IP is 10.151.121.130:

```
RemoteIP: 10.151.121.130
```

Operators

Operators enable you to customize the search and/or to create more complex queries.

Operators are case insensitive.

Operators	Definition
OR , ||	The query should match either one of the terms/values.
AND, &&	The query should match both of the terms/values.
NOT, !	The query should not match the term/value.
exists	The query should match when the field value is not null.
+ –	The term following this operator must be present.
•	The term following this operator must not be present.

Example

Where the Event includes either the RemoteIP field that contains 10.151.121.130 or the Remote Port field that contains 443

```
RemoteIP: 10.151.121.130 OR RemotePort: 443
```

Where the ProductName field contains both Microsoft and Windows

```
Source.Process.File.ProductName: (microsoft AND windows){}
```

Where the ProductName field contains Microsoft and does not include Windows

```
Source.File.ProductName: (microsoft -windows)
```

Where the Product Name field contains the exact phrase “Microsoft Windows”

```
Source.Process.File.ProductName: microsoft\ windows
```

Where the field Behavior has any non-null value

```
_exists_: Behavior
```

Where the field PID does not include the value 5292

```
Source.PID: (NOT 5292)
```

Where the Event does not include the value 5292 in any of the Event fields

```
NOT 5292
```

Wildcards

Wildcard searches can be run on individual terms using a **?** (question mark) to replace a single character, and an ***** (asterisk) to replace zero or more characters. For example: `Progr?m Fil*`.

If the value contains a space, escape it with a backslash. For example:

- `Source.Process.File.Path: Program\ Files*`
- `Source.Process.CompanyName: Microsoft\ Corporation`

Do not enclose wildcard search values with double quotes.



Wildcard queries may consume huge amounts of memory and perform poorly.

Ranges

Ranges can be specified for date, numeric or string fields. The inclusive ranges are specified with square brackets

[min TO max] and exclusive ranges with curly brackets {min TO max}.

Numbers 1..5

```
count:[1 TO 5]
```

Numbers from 10 upwards

```
count:[10 TO *]
```

Dates before 2012

```
date:{* TO 2012-01-01}
```

Ranges of IPs

```
RemoteIP: "140.100.100.0/24"
```

Reserved characters

Should you need to use any of the characters that function as operators in the query itself (and not as operators), then you should escape them with a leading backslash (\). For instance, to search for *c:\Windows*, write the query as *c\:\\Windows*.

Reserved characters are +,-, =, &&, ||, >, <, !, ( ), { }, [ ], ^, ", ~, *, ?, :, \ and /.

Platform administration

The following sections provide instructions about managing the FortiEndpoint platform:

- Accounts on page 811
- API access keys on page 813
- Upgrading FortiEndpoint on page 815
- Allowlisting the FortiEndpoint IP addresses
- Notifications on page 819
- Using the Fortinet email server for sending alerts on page 823

Accounts

The following provides account-related information:

- Adding a secondary admin account on page 811
- IAM users on page 812

You cannot control the admin role for the following user types from FortiEndpoint EMS:

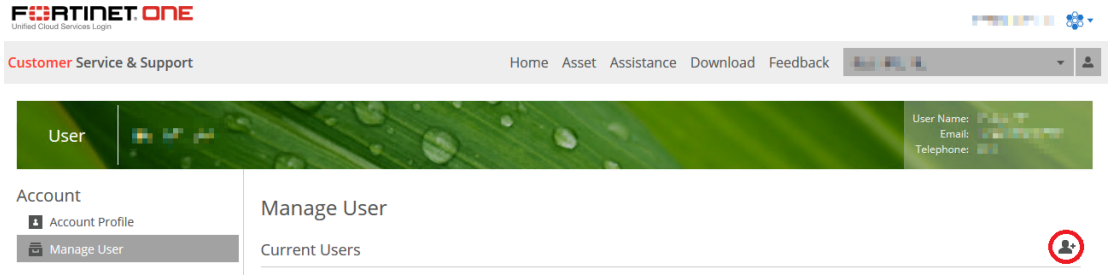
- When a user is configured as Admin or Viewer in FortiCloud. In FortiEndpoint EMS, these users become super administrators and restricted administrators, respectively.
- Secondary user who has full access permission in FortiCloud

Adding a secondary admin account

The FortiEndpoint primary administrator (the user who created the FortiEndpoint instance) can add secondary administrators from their FortiCloud account.

To create a secondary admin account:

1. Log in to Fortinet Service & Support with your FortiCloud account.
2. Click your account name in the top right corner, then select *My Account*.
3. Select *Manage User*.
4. Click the *Add User* icon.



5. Enter the user information as required. If the new user does not have a FortiCloud account, they must create one. Click *Save*. A user added on this page becomes visible on the FortiEndpoint GUI in *Administrators* and can log in to FortiEndpoint with their FortiCloud account. These users have limited permissions. For details on configuring permissions for these administrators, see Admin roles on page 480.

FortiEndpoint supports resource-based access control using FortiCloud permission profiles. See Creating a permission profile.

IAM users

FortiCloud Identity & Access Management (IAM) supports creating IAM users with access to FortiEndpoint using the admin role. See Adding IAM users for details on configuring IAM users.



The IAM user should not have organization units (OUs) enabled as FortiEndpoint does not support enabling OUs or registering it under existing OUs.

To log in to FortiEndpoint as an IAM user (without OUs enabled):

1. In the FortiEndpoint landing page, click *Login*.
2. Select *IAM Login*.
3. Enter your account ID/alias, username, and password, then click *Log In*.

API access keys

FortiEndpoint supports an option for the administrator to define an access code to identify an instance. A Fabric device can establish connection to a FortiEndpoint instance by providing one of the following in the SNI:

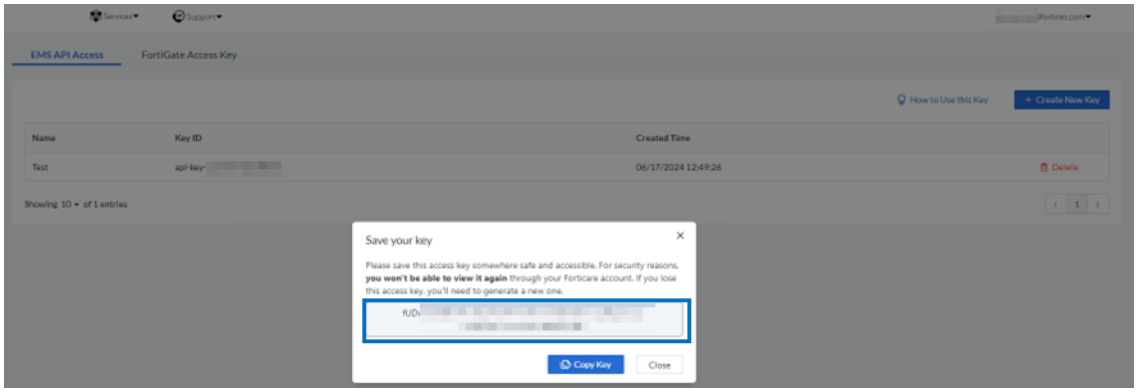
- FortiCloud account ID. The connection succeeds if the FortiCloud account has only one FortiEndpoint instance and there is no organizational unit structure.
- FortiCloud account ID and FortiEndpoint access key

This feature supports the following key types:

- EMS API access key. Only a primary account can create EMS API access keys. These keys do not expire.
- FortiGate access key. This feature requires FortiOS 7.4.4 or later.

To create an EMS API access key:

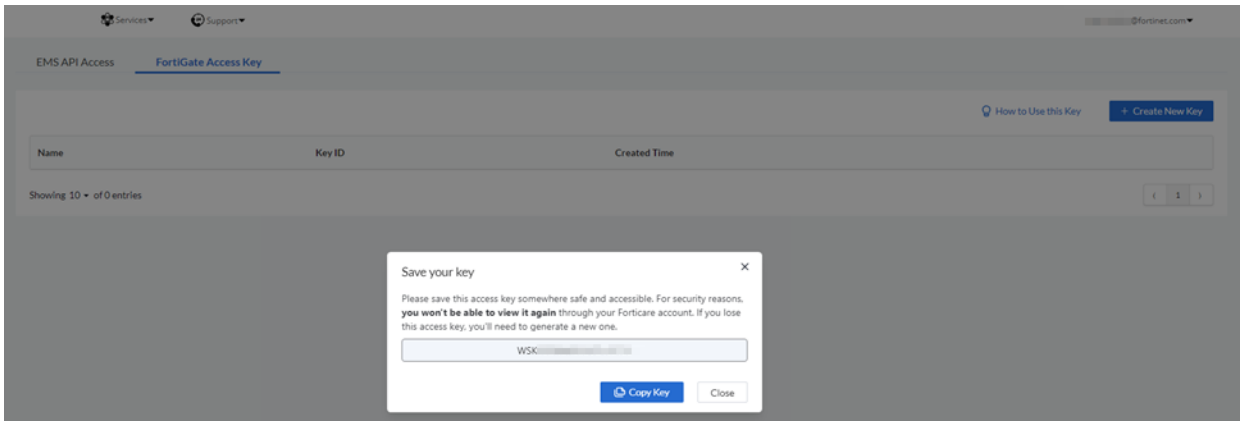
1. In FortiEndpoint, go to *Access Key* > *EMS API Access*.
2. Click *Create New Key*.
3. In the *Name* field, enter a unique name, then click *OK*.
4. Once the key is created, copy it to a safe location, as it does not display again after you close the dialog. Click *Close*.



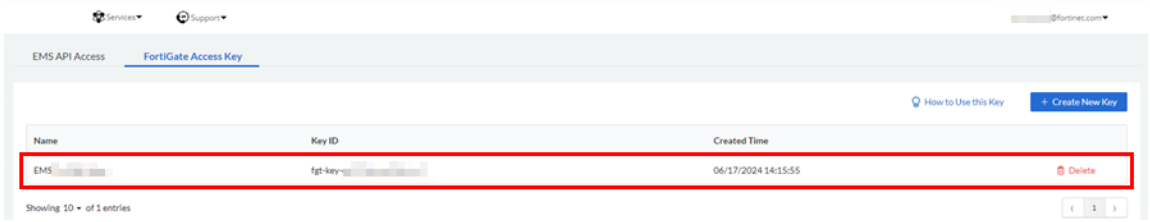
5. The EMS API keys display in the *EMS API Access* table. Note that the key ID is not the same as the generated API key that you copied in step 4. To view information about the keys, click *How to Use this Key*.

To create a FortiGate access key:

1. In FortiEndpoint, go to *Access Key* > *FortiGate Access Key*.
2. Click *Create New Key*.
3. In the *Name* field, enter a unique name, then click *OK*.
4. Once the key is created, copy it to a safe location, as it does not display again after you close the dialog. Click *Close*.



5. The FortiGate keys display in the *FortiGate Access Key* table. Note that the key ID is not the same as the generated API key that you copied in step 4. To view information about the keys, click *How to Use this Key*.



6. On the FortiGate, configure the key on the EMS Fabric connector:

```
config endpoint-control fctems
                                        edit 1
                                        set status enable
                                        set name "ems-cloud"
                                        set fortinetone-cloud-authentication enable
                                        set cloud-authentication-access-key "<FortiGate key>"
                                        next
                    end
```

7. In EMS, authorize the FortiGate to complete the connection. Standalone FortiGates or separate virtual domains from the same FortiGate can establish Fabric connection with FortiEndpoint.

Upgrading FortiEndpoint

FortiEndpoint is a SaaS service where Fortinet continuously updates the version for all customers. You can expect a FortiEndpoint upgrade to be available two to four weeks after a stable minor GA version release announcement.

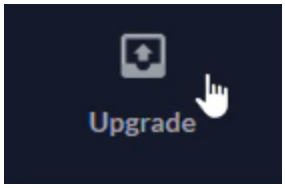
A FortiEndpoint upgrade can occur in one of the following ways:

- You can schedule the upgrade yourself from the FortiEndpoint portal.
- You can send an upgrade request to Fortinet Support.
- Fortinet forces an upgrade. This generally occurs to avoid compatibility issues. Fortinet sends an email notification seven to ten business days prior to the upgrade. The email includes the upgrade time and version information. You can also view the upgrade schedule on the FortiEndpoint portal.

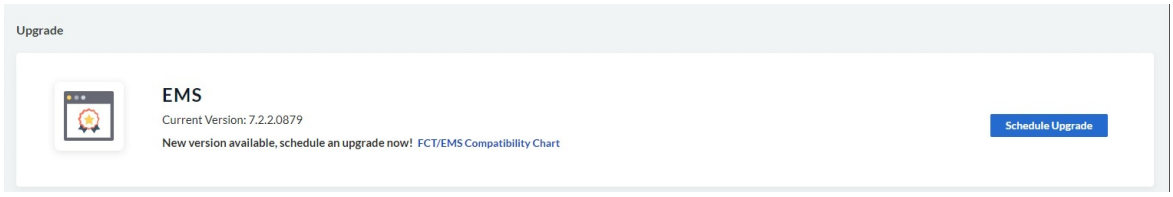
To schedule an upgrade:

If your FortiEndpoint is not at the latest version, you can schedule to upgrade to the latest version.

1. In the FortiEndpoint portal, click the menu icon (●) at the bottom right corner and then select *Upgrade*.



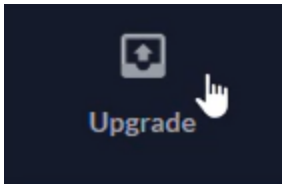
2. Click *Schedule Upgrade*.



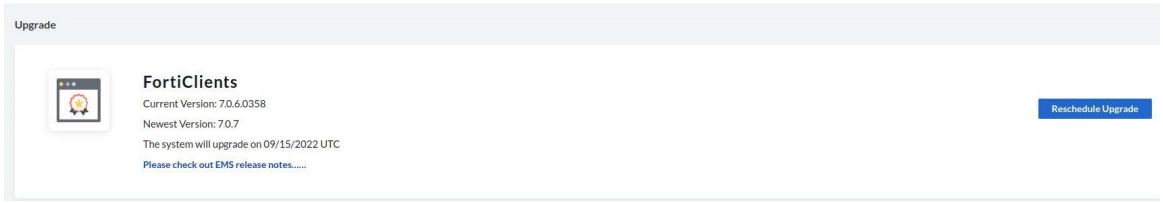
3. From the *Upgrade Version* dropdown list, select the desired version to upgrade to.
4. In the *Scheduled Upgrade Time* field, select the desired date. You must select a date before the displayed last day to upgrade. If you need to upgrade on a day after the displayed last day to upgrade, or you have a specific critical issue, contact Fortinet Support to discuss if the upgrade can be delayed to a future date.
5. Click *OK*.

To reschedule an upgrade:

1. In the FortiEndpoint portal, click the menu icon ( ) at the bottom right corner and then select *Upgrade*.

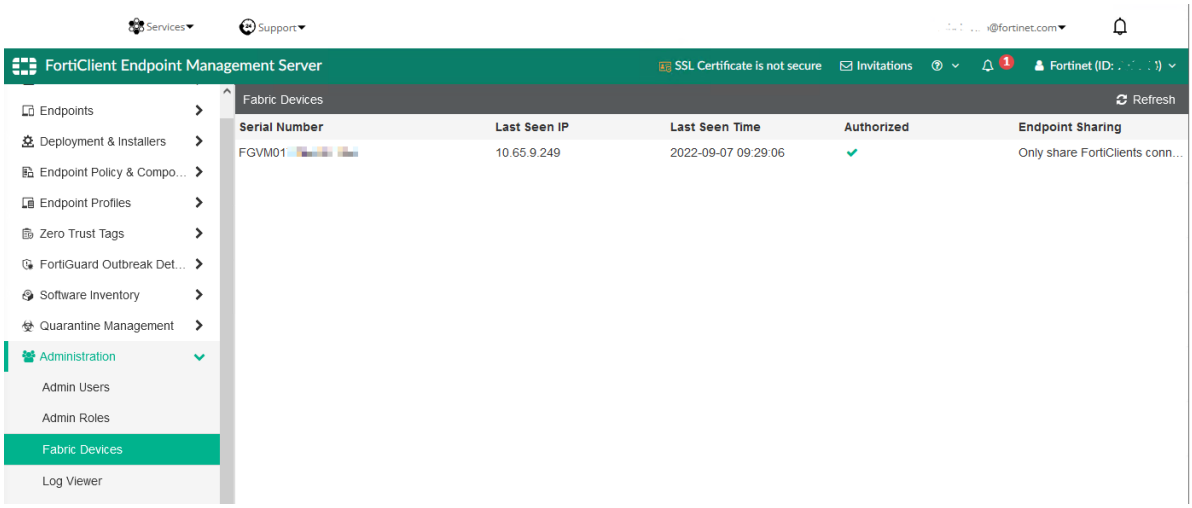


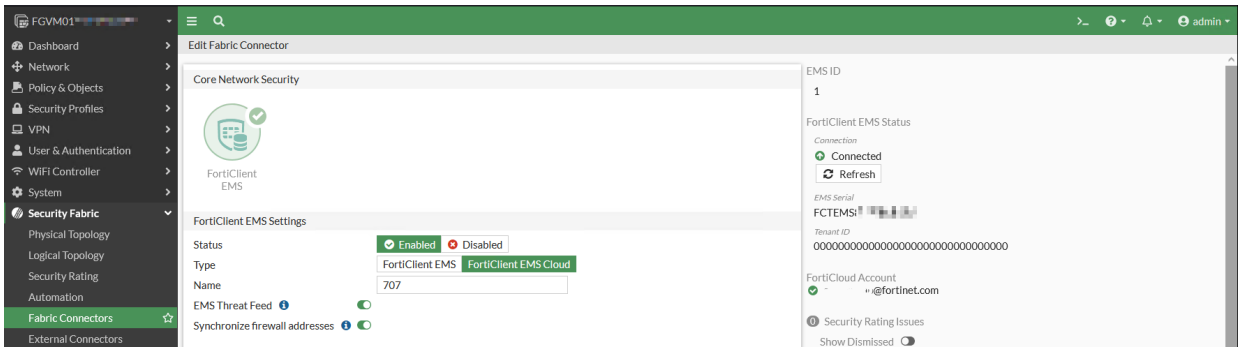
2. Click *Reschedule Upgrade*.



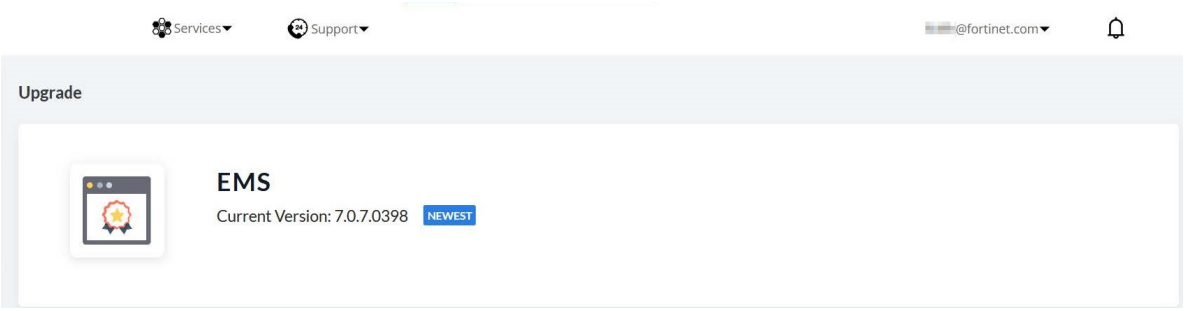
3. In the *System Upgrade Time* field, select the desired date. You must select a date before the displayed last day to upgrade. If you need to upgrade on a day after the displayed last day to upgrade, or you want to cancel the upgrade, contact Fortinet Support.
4. Click *OK*.

After the upgrade, view your FortiOS connectors to ensure that they are functioning correctly and that the desired FortiGates are authorized on FortiEndpoint and vice-versa.





The following shows the *Upgrade* page when EMS is at the latest version. In this case, there is no need to upgrade.



Allowlisting the FortiEndpoint IP addresses

Communication from endpoints to FortiEndpoint

The following public domains and ports are involved in the communication from endpoints to FortiEndpoint:

- `forticlient.forticloud.com` (browser, FortiEndpoint)
- `*.ems.forticlient.forticloud.com` (browser)
- `forticlient-emsproxy.forticloud.com` (FortiEndpoint, FortiGate, Active Directory (AD) connector)
- Port 559/555 (used by EDR Core with/without SSL)
- Port 8081 (used by EDR Aggregator)
- Port 443 (browser connection to the EDR Central Manager console)



Make sure the IP addresses of these public domains and these ports are not blocked by your firewall product (if one is deployed). As a security best practice, set up a narrow opening for these ports in the firewall rules. For example:

- Open the TCP outbound port 555 only to the Core IP address.
- Open the TCP outbound port 8081 only to the Aggregator IP address.

Additional connectivity requirements for endpoints:

- 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.
- Connectivity to the EDR Core and the FortiEDR Aggregator. You can check this by browsing to the Core's IP address and the Aggregator's IP address. For problems connecting, see Troubleshooting on page 797.
- Up to 5 Mbps of additional network workload for each 1,000 endpoints.

Communication from FortiEndpoint to endpoints

You must allowlist the FortiEndpoint external IP address to allow communication from FortiEndpoint to endpoints for the following features:

- AD integration
- Importing a profile from FortiGate or FortiManager
- SMTP server configuration

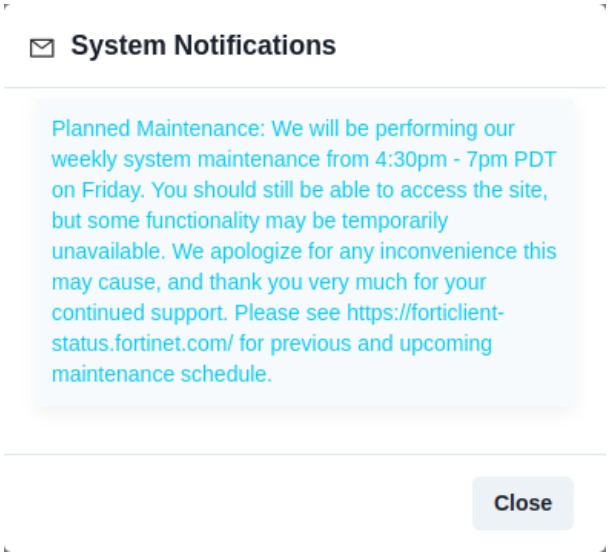
In the FortiEndpoint portal, go to *About*. The IP address row displays the IP address that you must allowlist for the listed features.

Notifications

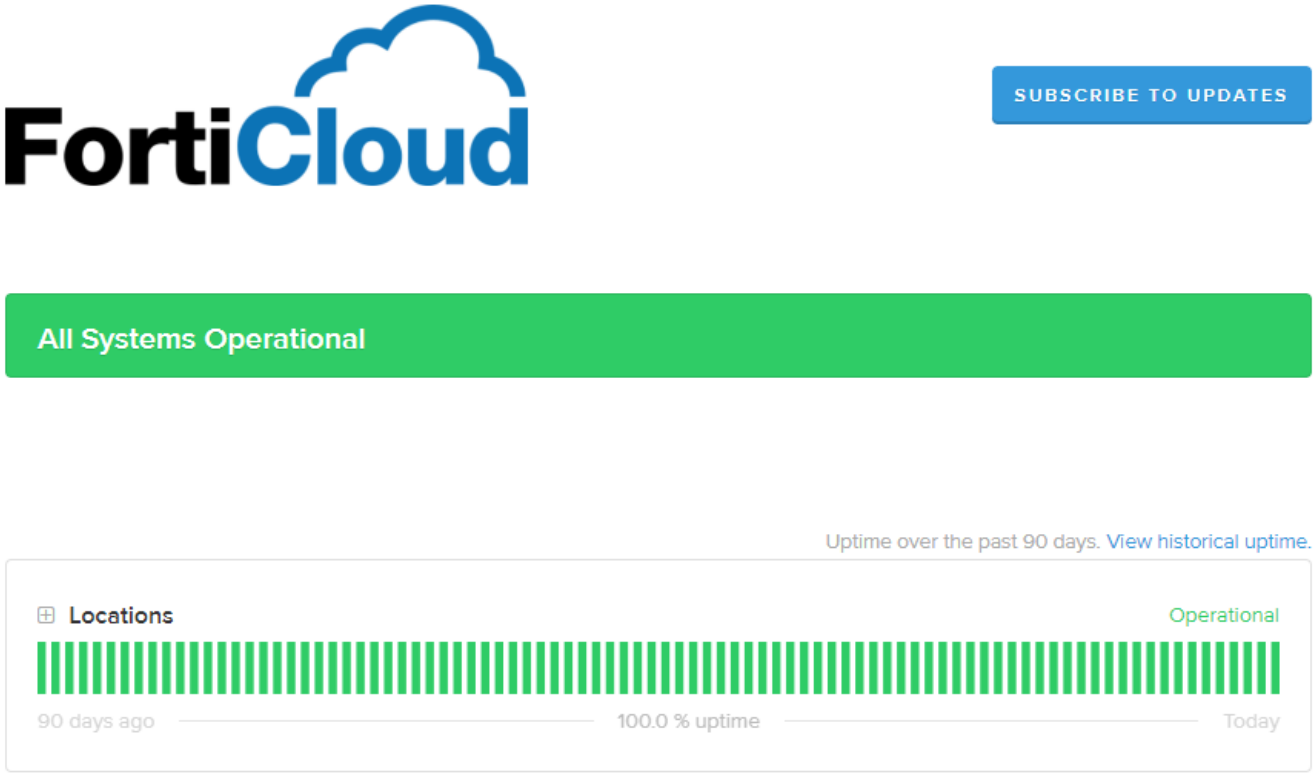
The following summarizes types of notifications that you may observe on FortiEndpoint:

System maintenance

These notifications alert you to system maintenance that is planned for all users in that datacenter due to a release, backend environment issue, or maintenance need. There is no action required for customers. You can view this notification from the GUI:

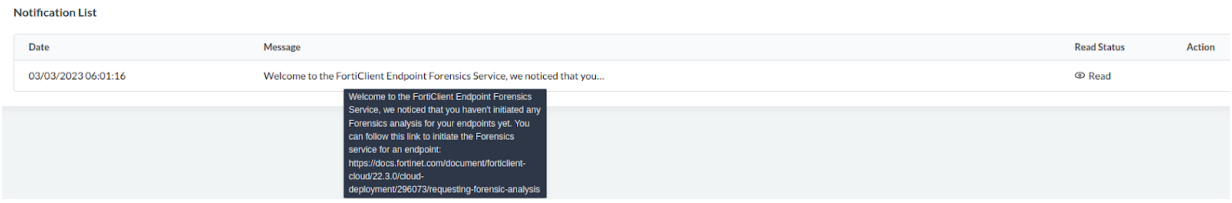


You can also view this notification from FortiEndpoint Status.

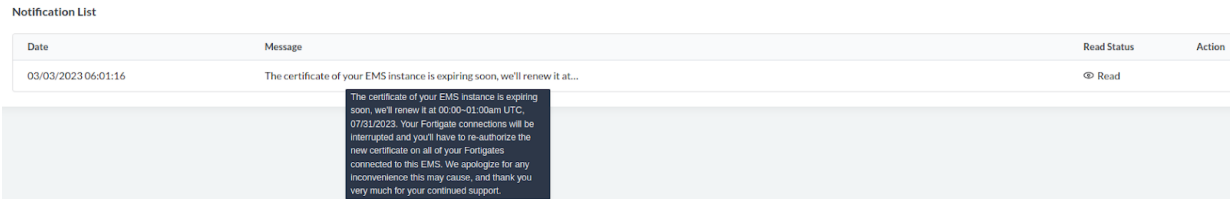


Targeted notifications

These notifications target specific customers and may require an action from the user. You can find them in the *Notifications* tab on the left panel. The following shows an example of a targeted notification for a new Forensics service user:



The following shows an example of a targeted notification for EMS certificate renewal:



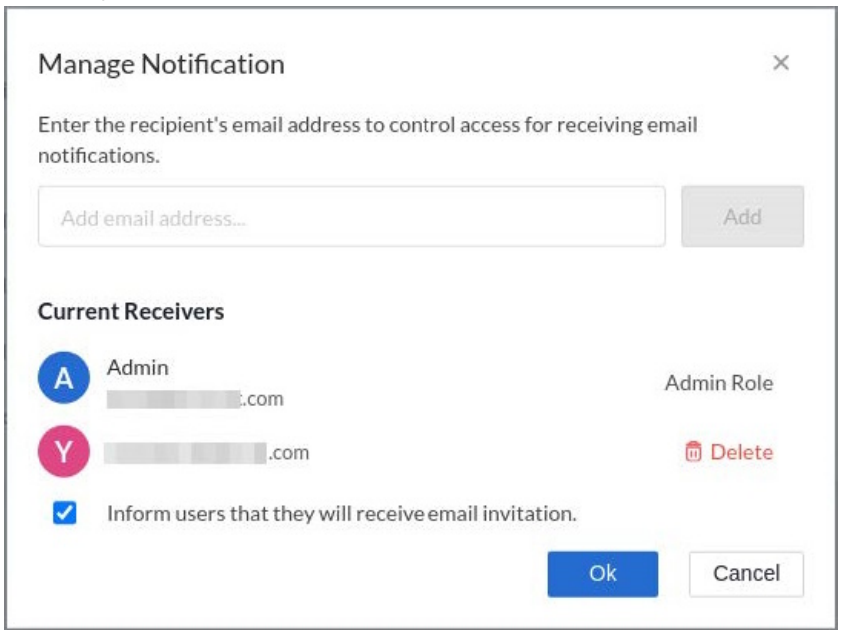
Managing notifications in the FortiEndpoint portal

To configure notification recipients:

1. Log in to the FortiEndpoint portal using your primary account credentials.

   If you log in as a non-primary user (subuser or Identity & Access Management user), you have read-only permissions and cannot edit the recipient list.

2. Go to *Notifications*.
3. Click *Manage Notification*.
4. The *Manage Notification* dialog displays the list of notification recipients. Add new recipients by entering their email address in the *Add email address* field or remove recipients by clicking *Delete*. If adding a new recipient, you can select *Inform users that they will receive email invitation*. to notify them that they will receive notifications.



If desired, the recipient can unsubscribe by using a link in the subscription notice email.



Dear Customer,

We are pleased to inform you that your administrator '[redacted].com' has added you as a designated recipient for FortiClient Cloud notifications. This means you will now receive essential updates, alerts, and information related to FortiClient Cloud directly in your email inbox.

If, at any point, you wish to stop receiving these notifications, you can easily unsubscribe by clicking the "Unsubscribe" link provided below.

Should you have any questions or if you believe this addition was made in error, please don't hesitate to reach out to your administrator or our support team.

Thank you for your cooperation.

Regards,
FortiClient Cloud Team

click to unsubscribe from all communications

Using the Fortinet email server for sending alerts

By default, FortiEndpoint uses the Fortinet built-in email server to send email alerts. This eliminates the need to specify your own SMTP or mail server before sending alert emails. You only need to configure the recipient email addresses.

If desired, you can still manually specify your own SMTP server.

To configure email settings:

1. In FortiEndpoint, go to *System Settings* > *SMTP Server*.
2. By default, *Fortinet* is selected as *Mail Server*. Configure recipients and test recipient settings as desired. Save.

The following shows an example alert email. The sender email address is no-reply@notification.fortinet.net.





www.fortinet.com

Copyright© 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.