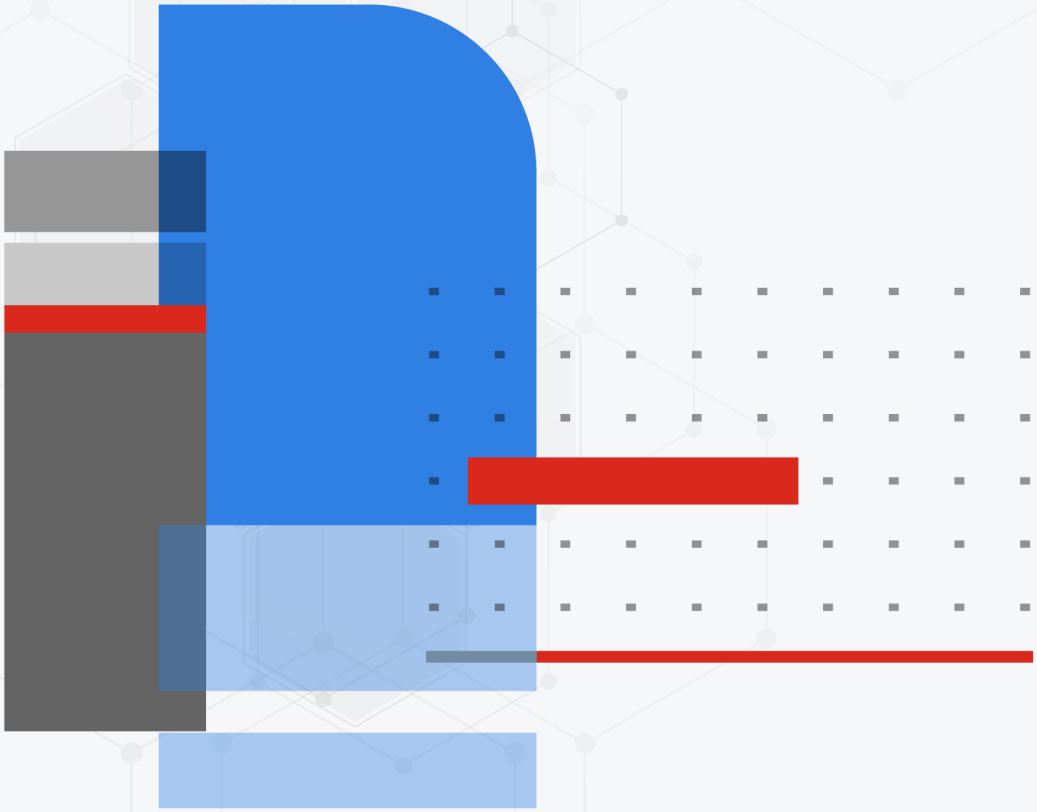
Administration Guide

FortiClient EMS 7.4.3



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



November 03, 2025
FortiClient EMS 7.4.3 Administration Guide
04-743-1010849-20251103

TABLE OF CONTENTS

Introduction **10**
FortiClient EMS components 10
Documentation 12
Getting started **13**
Getting started with managing Windows, macOS, and Linux endpoints 13
Initially deploying FortiClient software to endpoints 13
Pushing configuration information to FortiClient 14
Relationship between FortiClient EMS, FortiGate, and FortiClient 14
Getting started with managing Chromebooks 19
Configuring FortiClient EMS for Chromebooks 19
Configuring the Google Admin console 19
Deploying a profile to Chromebooks 20
How FortiClient EMS and FortiClient work with Chromebooks 20
Installation preparation **22**
System requirements 22
License types 23
FortiClient EMS 23
Component applications 27
Required services and ports 27
Telemetry data usage requirements 31
Management capacity 33
Hardware configuration when EMS and Postgres run on same machine with no FortiGate connected 33
Hardware configuration when EMS and Postgres run on different machines with no FortiGate connected 34
Hardware configuration when there are FortiGates connected to the EMS 35
FortiClient Telemetry security features 36
Server readiness checklist for installation 37
Upgrading EMS 37
Upgrading from an earlier FortiClient EMS version 37
Automatically upgrading EMS to latest patch release 39
Upgrading EMS in HA 41
Install preparation for managing Chromebooks 43
Google Workspace account 43
SSL certificates 43
Installation and licensing **45**
Downloading the installation file 45
Installing FortiClient EMS 7.4 46
Migrating EMS 7.2 to 7.4.3 46
Installation 53
Installation parameters 112
Starting FortiClient EMS and logging in 113
Configuring EMS after installation 117

Licensing FortiClient EMS 118
Licensing EMS by logging in to FortiCloud 118
Importing an EMS license via FortiFlex 122
Uploading a license file 124
License status 125
Help with licensing 125
Uninstalling FortiClient EMS 125
Installation and setup for managing Chromebooks 126
Google Admin Console setup 126
Service account credentials 133
Verifying ports and services and connection between EMS and FortiClient 143
Ports and services 143
Automating EMS DB backups using cron jobs 143
GUI 146
Banner 146
Left pane 147
Content pane 150
Dashboard 151
Viewing the Status 151
System Information widget 152
License Information widget 154
Status charts and widgets 155
Viewing the Vulnerability Scan dashboard 157
Viewing current vulnerabilities 159
Viewing the Endpoint Scan Status 161
Viewing the top 10 vulnerable endpoints with high risk vulnerabilities 164
Viewing top ten vulnerabilities on endpoints 166
Viewing the Forensics Analysis dashboard 168
Viewing the PUA dashboard 169
Viewing Chromebook Status 171
Endpoint management 172
Windows, macOS, and Linux endpoints 172
Managing groups 172
Adding endpoints 172
Viewing endpoints 176
Managing endpoints 194
All Events 208
Installing EMS with ES integration 210
Enabling ES integration after EMS install 211
EMS event-specific indexes 212
ES sizing 213
Required ES permissions 215
Index lifecycle 215
Group assignment rules 216
Group assignment rule types 216
Managing group assignment rule priority levels 217
Adding a group assignment rule 218

Enabling/disabling a group assignment rule 220
Deleting a group assignment rule 221
Google Domains 221
Adding a Google domain 221
Viewing domains 222
Editing a domain 224
Deleting a domain 224
Deployment & Installers 225
Manage Deployment 225
Creating a deployment configuration 225
Managing deployment configuration priority levels 226
Enabling/disabling a deployment configuration 227
Deleting a deployment configuration 227
Deploying FortiClient upgrades from FortiClient EMS 228
Deploying different installer IDs to endpoints using the same deployment package 228
FortiClient Installer 229
Adding a FortiClient installer 230
Adding a FortiClient hotfix installer 237
Viewing deployment packages 239
Deleting a FortiClient deployment package 239
Endpoint Policy & Components 240
Manage Policies 240
Adding an endpoint policy 240
Editing an endpoint policy 242
Deleting an endpoint policy 242
Enabling/disabling an endpoint policy 242
Managing endpoint policy priority levels 242
Editing endpoint policy view 244
FortiClient management based on Active Directory user/user groups 245
CA Certificates 246
On-fabric Detection Rules 248
Source IP address anchoring for IPsec VPN 252
Chromebook Policy 254
Endpoint Profiles 255
Editing a default profile 255
Creating a new profile 255
Adding a new Chromebook profile 256
Managing profiles 256
Editing a profile 256
Cloning a profile 257
Syncing profile changes 257
Editing sync schedules 257
Exporting a profile 258
Importing a profile 258
Deleting profiles 258
Remote Access 259

SSL VPN 262
IPsec VPN 267
Configuring a profile with application-based split tunnel 276
Configuring a profile to allow or block endpoint from VPN tunnel connection based on the applied security posture tag 280
Configuring a backup VPN connection 284
Using a browser as an external user-agent for SAML authentication in an SSL VPN connection 286
Per-machine prelogon VPN connection without user interaction 289
Autoconnect on logging in as an Entra ID user 294
Load balancing IPsec VPN gateways with a single FQDN 300
Load balancing SSL VPN gateways with one FQDN 308
Certificate path configuration for automated certificate selection 312
Autoconnect to IPsec VPN using Entra ID logon session information 314
IPsec VPN SAML-based authentication 334
IPsec VPN support for traffic going through FortiADC 365
IPsec VPN over TCP 376
Troubleshooting IPsec VPN IKEv2 with SAML authentication 394
Troubleshooting IPsec VPN IKEv1 404
ZTNA Destinations 408
Wildcard support for ZTNA FQDN rules 410
FQDN-based ZTNA TCP forwarding services 415
ZTNA automatic login using Microsoft Entra ID 417
Web Filter 422
Importing a Web profile from FortiOS or FortiManager 430
Enabling and disabling Safe Search 432
Configuring banned word check in URL 433
Syncing remote categories from imported FortiOS or FortiManager Web Filter profile 435
Video Filter 440
Vulnerability Scan 442
Malware Protection 445
AntiVirus Protection 445
Anti-Ransomware 449
Anti-Exploit 450
Cloud-Based Malware Detection 450
Removable Media Access 451
Exclusions 452
Other 454
Sandbox 455
Firewall 460
Define exceptions for Firewall Detect & Block Exploits feature 462
System Settings 465
Configuring identity compliance for endpoints 474
FortiPAM integration 475
Add FortiPAM agent to SSOMA 482
Configuring SSOMA with AD 485
Sending email events from the Microsoft Exchange server 490

XML Configuration 491
Creating a profile with XML 491
Importing a profile from an XML file 491
Configuring encrypted ZTNA rules 492
Security Posture Tags 495
Tags 495
Adding a security posture tag 496
Editing a security posture tag 498
Deleting a security posture tag 498
Importing and exporting a security posture tag 499
Security posture tagging rule types 500
Tag Monitor 507
FortiOS dynamic policies using EMS dynamic tags 508
Configuring FortiOS dynamic policies using EMS security posture tags 509
Fabric Device Monitor 513
Fabric & Connectors 514
Fabric Devices 514
Configuring EMS to share tagging information with multiple FortiGates 516
Configuring FortiGate per-VDOM connection 517
Creating connectors with OAuth 2.0 token-based authentication 519
Matched endpoints and resolved addresses 522
ZTNA Applications Catalog 527
FortiGuard Outbreak Alerts 530
Software Inventory 532
Applications 532
Hosts 556
Quarantine Management 558
Files 558
Viewing quarantined files 558
Allowlisting quarantined files 560
Configuring quarantine management 560
Allowlist 561
Viewing allowlisted files 561
Editing file descriptions 562
Deleting a file from the allowlist 562
Administration 563
Admin Users 563
Viewing users 563
Configuring user accounts 564
Activating a disabled account 565
Resetting the password for a local administrator 565
Using the PasswordRecovery tool 566
Admin roles 567
Adding an admin role 567
Cloning an admin role 568
Deleting admin roles 568

Admin role permissions reference 568
Authentication Servers 571
Adding an ADDS server 571
Adding an Entra ID server 573
Adding an API key 577
AD connector 577
Configuring Admin User Settings 581
SAML SSO 581
SAML SSO with FortiGate as IdP 581
SAML SSO with Okta as IdP 584
SAML SSO with Entra ID as IdP 585
SAML SSO with AD FS as IdP 587
SAML SSO with FortiAuthenticator as IdP 589
Licenses 592
Log Viewer 592
Generate Diagnostic Logs 592
Marking all endpoints as uninstalled 592
User Management 594
Authorized User Groups 594
Verified Users 595
Unverified Users 596
Local users 597
SAML Configuration 598
Invitations 599
Configuring user verification with an LDAP server for authentication 600
Configuring user verification with SAML authentication and an LDAP domain user account 601
Configuring user verification with Entra ID authentication 609
Configuring user verification with SAML authentication and an Entra ID server user account 613
Configuring user verification with SAML authentication and an Okta user account 619
Troubleshooting SAML user verification failure 620
Missing attribute 620
Authenticated but not authorized 622
Signature validation failed 625
System Settings 628
Configuring EMS settings 629
Generating a QR code for centrally managing FortiClient (Android) and (iOS) endpoints 636
Persistent connection 636
JWT support for ZTNA UID and tag sharing 637
Uploading custom certificate and private key for ZTNA 640
Configuring Logs settings 641
Sending EMS system log messages to FortiAnalyzer 642
Configuring FortiGuard Services settings 645

EMS Server Certificates ... 647
Adding an SSL certificate to FortiClient EMS ... 648
Alerts ... 649
Configuring EMS Alerts ... 649
Configuring Endpoint Alerts ... 650
Configuring SMTP Server settings ... 651
Viewing alerts ... 653
Custom Messages ... 653
Customizing the endpoint quarantine message ... 653
Customizing Web Filter messages ... 654
Feature Select ... 655
MDM Integration ... 658
Workspace ONE ... 658
Microsoft Intune ... 659
Jamf ... 659
ManageEngine MDM Plus ... 660
Deploying ZTNA certificates to FortiClient mobile via MDM ... 660
Multitenancy ... 661
Enabling and configuring multitenancy ... 661
Global and per-site configuration ... 662
Global configuration ... 662
Site level configuration ... 662
Left pane with multitenancy enabled ... 663
Editing a site ... 667
Adding a multitenancy administrator ... 667
Logging into EMS with multitenancy enabled ... 668
Fabric connection setup using FortiGate as a load balancer ... 670
Migrating to another EMS instance ... 673
Limitations ... 674
FortiClient EMS API ... 675
Appendix A - FortiClient EMS services ... 676
Critical severity ... 676
Medium severity ... 677
Low severity ... 677
Appendix B - CLI commands ... 679
Making configuration changes ... 679
Managing services ... 680
Accessing the database ... 680
Obtaining data from the DAS cache ... 681
Diagnosing endpoints ... 681
Integrating ES cluster ... 682
Change log ... 683

Introduction

FortiClient Endpoint Management Server (FortiClient EMS) is a security management solution that enables scalable and centralized management of multiple endpoints (computers). FortiClient EMS provides efficient and effective administration of endpoints running FortiClient. 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. FortiClient EMS also works with the FortiClient Web Filter extension to provide web filtering for Google Chromebook users.

FortiClient EMS is designed to meet the needs of small to large enterprises that deploy FortiClient on endpoints and/or provide web filtering for Google Chromebook users. Benefits of deploying FortiClient EMS include:

- Remotely deploying FortiClient software to Windows PCs
- Updating profiles for endpoint users regardless of access location
- Administering FortiClient endpoint connections, such as accepting, disconnecting, and blocking connections
- Managing and monitoring endpoints, such as status, system, and signature information
- Identifying outdated FortiClient software 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.

FortiClient EMS is part of the Fortinet Endpoint Security Management suite, which ensures comprehensive policy administration and enforcement for an enterprise network.

FortiClient EMS components

FortiClient EMS provides the infrastructure to install and manage FortiClient software on endpoints. FortiClient protects endpoints from viruses, threats, and risks.

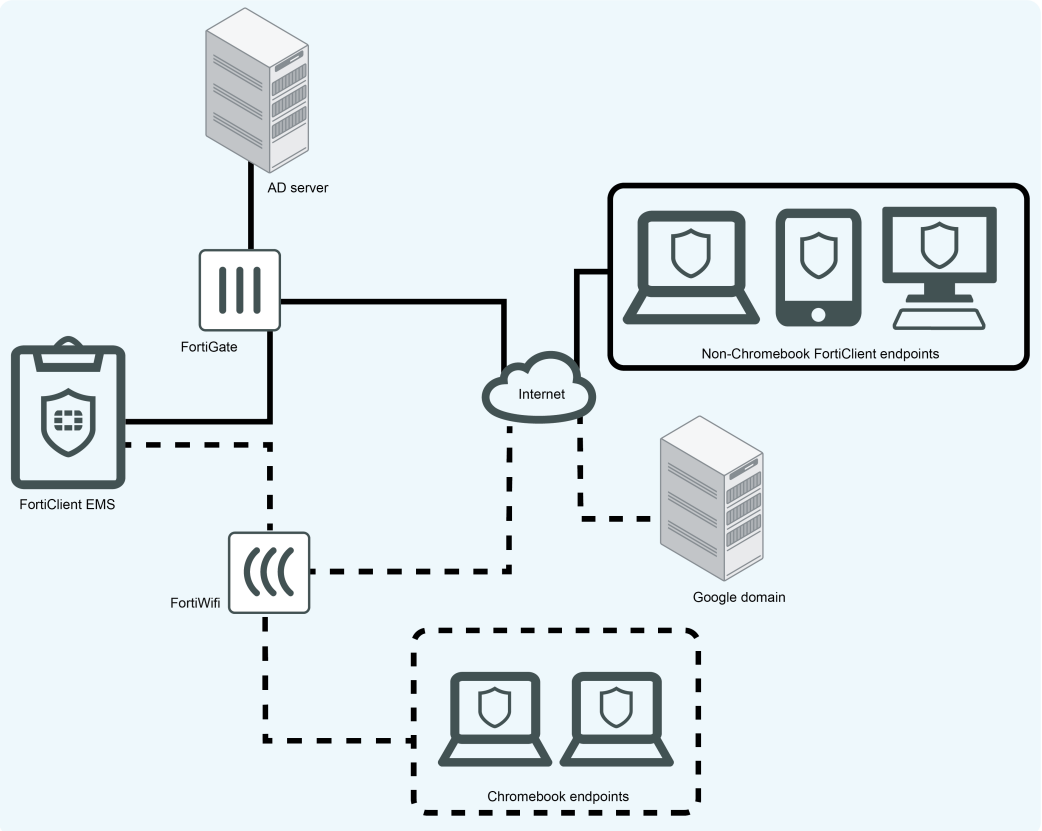
FortiClient EMS also provides the infrastructure to install and manage the FortiClient Web Filter extension on Google Chromebook endpoints. FortiClient protects endpoint users by working with FortiClient EMS to filter web content endpoint users view on Google Chromebooks.

The following table lists FortiClient EMS components:

Component	Description
FortiClient EMS	Manages FortiClient on endpoints that connect to your network.

Component	Description
	Manages the FortiClient Web Filter extension installed on Google Chromebook endpoints, which are connected to your Google domain. Includes the following software: • Console software that manages security profiles, FortiClient on endpoints, and Chromebook endpoints • Server software that provides secure communication between endpoints and the console and between Chromebook endpoints and the Google Admin console.
Database	Stores security profiles and events. Also stores user information retrieved from the Google Admin console for Chromebooks. The FortiClient EMS installation installs the PostgreSQL database.
FortiClient	Helps enforce security and protection on endpoints. It runs on servers, desktops, and portable computers you want to secure. See the FortiClient Administration Guide.
FortiClient Web Filter Extension	Communicates with FortiClient EMS and enforces web filtering on Google Chromebook endpoints.

In the diagram, the undotted lines show how different components connect to manage Windows, macOS, and Linux endpoints using FortiClient EMS. The dotted lines represent how you use components to manage Chromebook endpoints with FortiClient EMS.



FortiClient EMS allows you to:

- Establish and enforce security profiles
- Manage deployment, configuration, and updates
- Manage security profiles from an integrated management console
- Obtain a consolidated view of multiple security components across all endpoints in your network and Google domain
- Perform integrated installation of security components and set profiles
- Monitor endpoints' web browsing activity

Documentation

You can access FortiClient EMS documentation from the Fortinet Document Library.

The FortiClient EMS documentation set includes the following:

Document	Description
Administration Guide	Describes how to set up FortiClient EMS and use it to manage endpoints. It includes information on how to configure multiple endpoints, configure and manage profiles for the endpoints, and view and monitor endpoints.
New Features Guide	Describes new features and enhancements in FortiClient EMS for the release, including configuration information.
QuickStart Guide	Describes how to install and begin working with the FortiClient EMS system. It provides instructions on installation and deployment, and includes a high-level task flow for using the FortiClient EMS system.
Release Notes	Lists any known issues and limitations for the release. This document also defines supported platforms and minimum system requirements.
REST API	The FortiClient EMS API allows you to perform configuration operations on EMS. You can view the API documentation on the FortiAPI tab on FNDN.
Upgrade Paths	Provides upgrade path information for different versions of FortiClient EMS.
Compatibility Chart	Provides compatibility information for different versions of FortiClient EMS and other Fortinet products.
Jamf Deployment	Provides information about deploying FortiClient using Jamf mobile device management (MDM).
Intune Deployment	Provides information about deploying FortiClient using Intune MDM.
Workspace ONE Deployment	Provides information about deploying FortiClient using VMware Workspace ONE MDM.
HA with Multiple Databases Deployment Guide	Deployment instructions when using high availability with FortiClient EMS.

Getting started

Getting started with managing Windows, macOS, and Linux endpoints

Initially deploying FortiClient software to endpoints

Following is an overview of how to initially deploy FortiClient to endpoints and connect them to EMS. You can use one of the following methods:

Deployment method	Description
Microsoft System Center Configuration Manager (SCCM) or group policy object (GPO)	1. Create a custom deployment package (MSI file) on EMS. See Adding a FortiClient installer on page 230. 2. Deploy the FortiClient deployment package to desired endpoints using one of the following: a. SCCM: Deploy applications with Configuration Manager. b. GPO: Use Group Policy to remotely install software.
Mobile device management (MDM)	Use an MDM application to initially deploy FortiClient to the desired endpoints. FortiClient supports the following MDM applications. See the guide for each MDM application: • Intune • Workspace ONE (macOS only)
Sending installer link to end users	1. Create a custom deployment package on EMS. See Adding a FortiClient installer on page 230. 2. Create an invitation on EMS, configuring the invitation to be sent to all desired end users. See Invitations on page 599. 3. The end user receives an email or SMS notification that includes the configured invitation code and installer. They install FortiClient on their devices using the included installer and enter the invitation code to connect their FortiClient to EMS.



After FortiClient and EMS establish a Telemetry connection, you can push FortiClient updates to endpoints using EMS. The aforementioned methods are only required for initial FortiClient deployment to endpoints. See Deployment & Installers on page 225.



In 7.4.3, you cannot deploy initial FortiClient installations to Active Directory domain-joined devices. You must use one of the aforementioned methods to deploy initial FortiClient installations.



Installing FortiClient may require administrator privileges on the endpoint. See:
- Microsoft Windows
- macOS
- Linux

Pushing configuration information to FortiClient

After the endpoints' FortiClient connects Zero Trust Telemetry to FortiClient EMS, EMS manages the endpoints, and you can use FortiClient EMS to push configuration information to FortiClient software on endpoints.

To push configuration information to FortiClient:

1. Edit an existing profile or create a new profile to configure FortiClient software on endpoints. See Creating a new profile on page 255.
2. Edit an existing endpoint policy or create a new endpoint policy that is configured with desired profile. Configure the endpoint policy to apply to the desired domains and workgroups. See Adding an endpoint policy on page 240.
   After you apply the endpoint policy to endpoint groups, EMS pushes profile changes to endpoints with the next Telemetry communication.
3. Monitor the update using the *Endpoints* pane. See Viewing the Endpoints pane on page 176.

Relationship between FortiClient EMS, FortiGate, and FortiClient

You can use FortiClient EMS in standalone mode or integrated with FortiGate. The following section illustrates the topology for each configuration and the differences between the scenarios.

See FortiClient Access Control.

FortiClient in the Security Fabric

In this scenario, FortiClient Zero Trust Telemetry connects to EMS to receive a profile of configuration information as part of an endpoint policy. EMS is connected to the FortiGate to participate in the Security Fabric. EMS sends FortiClient endpoint information to the FortiGate.

The FortiGate can also receive dynamic endpoint group lists from EMS and use them to build dynamic firewall policies. EMS sends group updates to FortiOS, and FortiOS uses the updates to adjust the policies based on those groups. This feature requires FortiOS 6.2.0 or a later version.

FortiClient can also receive a device certificate from EMS that it can use to securely encrypt and tunnel TCP or HTTPS traffic through HTTPS to the FortiGate. This feature requires FortiClient 7.0.0 or a later version and FortiOS 7.0.0 or later.

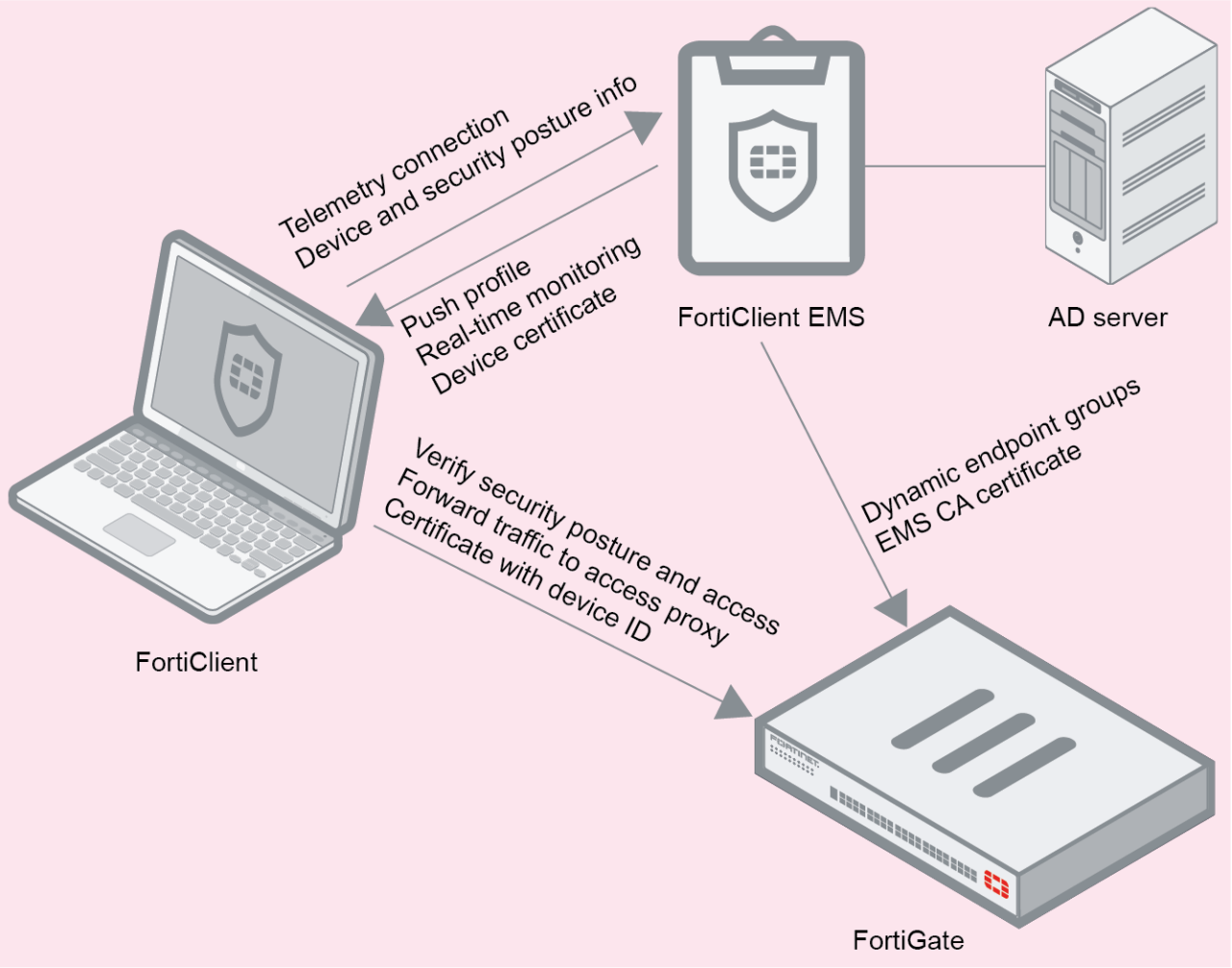


FortiGate does not provide configuration information for FortiClient and the endpoint. An administrator must configure FortiClient using an EMS endpoint policy.

Following is a summary of how the Zero Trust Telemetry connection works in this scenario. The following assumes that EMS is already connected to the FortiGate as a participant in the Security Fabric, and that FortiClient and FortiOS are also 7.0.0 or a later version:

1. EMS sends its CA certificate to the FortiGate.
2. FortiClient Telemetry attempts connection to EMS. Based on the EMS configuration, FortiClient may receive an SSL certificate from EMS to verify the connection. If the certificate is valid, FortiClient Telemetry connects to EMS. If the certificate is invalid, FortiClient may allow or deny connection to the EMS based on configured invalid certificate action.
3. FortiClient receives the following from EMS:
   - Licensing. See Windows, macOS, and Linux licenses on page 25.
   - Profile of configuration information as part of an endpoint policy. See Endpoint Profiles on page 255.
   - Device certificate that includes the FortiClient UID. FortiClient installs the received certificate to the current user certificate store for Chrome and Edge browser, and installs it to the browser certificate store for Firefox. This feature may not be available for Firefox.
4. FortiClient sends security posture information to EMS, including third-party software information, running processes, network information, and so on.
5. EMS dynamically groups the endpoint based on the information it received, using the configured security posture tagging rules. See Tags on page 495.
6. FortiOS pulls the dynamic endpoint group information from EMS. The FortiOS administrator can use this data to build dynamic firewall policies.
7. When the endpoint initiates TCP or HTTPS traffic, FortiClient works as a local proxy gateway to securely encrypt and tunnel the traffic through HTTPS to the FortiGate, using the certificate received from EMS.
8. The FortiGate retrieves the UID to identify the device and check other information using the endpoint information that EMS provided to the FortiGate. The FortiGate allows or denies the access as applicable.
9. EMS sends dynamic endpoint group updates to FortiOS. FortiOS uses the updates to adjust the policies based on those groups.

For details about dynamic endpoint groups, see FortiOS dynamic policies using EMS dynamic tags on page 508.



FortiClient follows the endpoint profile configuration that it receives from EMS. EMS locks FortiClient settings so that the endpoint user cannot manually change FortiClient configuration.

Only EMS can control the connection between FortiClient and EMS. You can only disconnect FortiClient when you are logged into EMS.

The EMS server's IP addresses are embedded in FortiClient deployment packages created in EMS. This allows the endpoint to connect FortiClient Telemetry to the specified EMS server.

EMS sends the following endpoint information to FortiOS:

- User profile:
  - Logged-in username
  - Full name
  - Email address
  - Phone number
- User avatar
- Social network account IDs
- MAC address
- OS type

- OS version
- FortiClient version
- FortiClient UUID

FortiGate also opens a websocket with EMS. EMS adds a new FcmNotify daemon to handle the websocket connection. EMS notifies the FortiGate if any of the following device information has changed. FortiOS loads the updated information:

- System information
- User avatar
- Vulnerabilities
- Security posture tags

EMS also sends the following endpoint information to FortiAnalyzer:

- Telemetry/system information
- User avatar
- Software inventory
- Processes
- Network statistics
- Classification tags

FortiClient directly sends the following information to FortiAnalyzer:

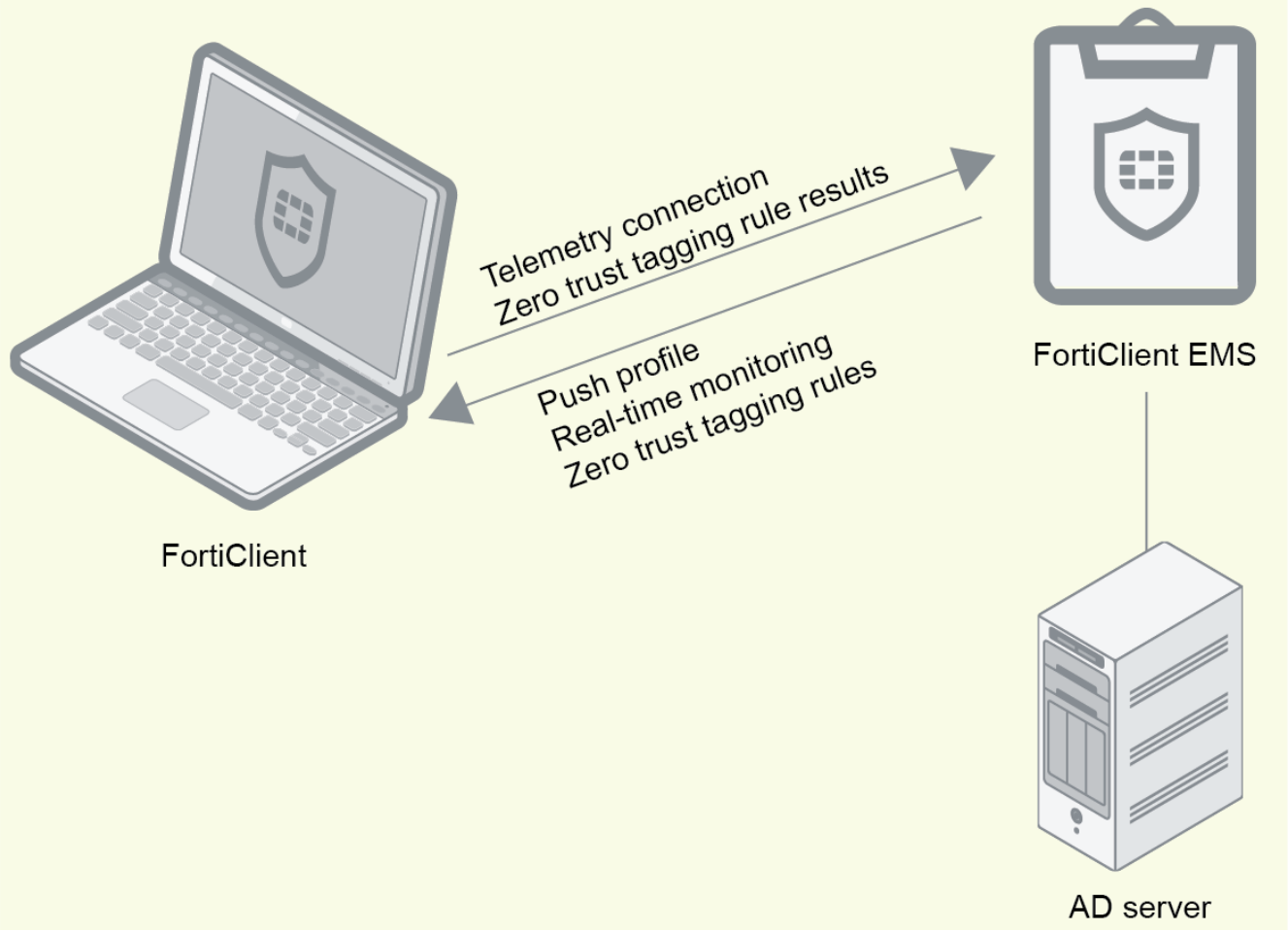
- Logs
- Windows host events

See the *FortiAnalyzer Administration Guide* for details.

FortiClient with EMS

In this scenario, EMS provides FortiClient endpoint provisioning. FortiClient EMS connects Telemetry to EMS to receive configuration information in an endpoint profile as part of an endpoint policy from EMS. EMS also sends security posture tagging rules to FortiClient, and use the results from FortiClient to dynamically group endpoints in EMS. Only EMS can control the connection between FortiClient EMS and EMS. You must make any changes to the connection from EMS, not FortiClient EMS. When FortiClient EMS is connected to EMS, EMS locks FortiClient EMS settings so that the endpoint user cannot change any configuration. To disconnect FortiClient EMS from EMS, the EMS administrator must deregister the endpoint in EMS.

In this scenario, EMS and FortiClient EMS cannot participate in the Security Fabric, since a FortiGate is not present.



Quarantining an endpoint from FortiOS using EMS

In FortiOS 6.0, an administrator can quarantine FortiClient endpoints using EMS by enabling the *Quarantine FortiClient via EMS* option. The following lists the requirements for this feature:

- The FortiClient endpoint is connected to FortiGate and managed by EMS.
- The FortiClient endpoint and FortiGate use the same FortiAnalyzer.
- The EMS managing the FortiClient endpoint is configured on the FortiGate. FortiOS allows configuration of up to three EMS servers to allow endpoint control in different locations.

Configuring *Quarantine FortiClient via EMS* requires setting the following fields in the FortiOS CLI: `automation-stitch` and `forticlient-ems`. See the *FortiOS CLI Reference*.

If *Quarantine FortiClient via EMS* is enabled, the following occurs when an indicator of compromise (IOC) is detected on an endpoint in the Security Fabric:

1. An IOC is detected on an endpoint.
2. FortiOS sends the endpoint information to EMS with instructions to quarantine the endpoint.
3. EMS identifies and quarantines the endpoint based on the request from FortiOS.

You can remove the endpoint from quarantine using EMS as Quarantining an endpoint on page 197 describes or using FortiOS:

1. The administrator identifies that EMS has quarantined an endpoint from one of the following:
   a. FortiClient on the endpoint
   b. *Quarantine Management* or *FortiClient Monitor* in FortiOS
   c. *Endpoints* pane in EMS
2. The administrator removes the endpoint from quarantine in FortiOS.
3. FortiOS sends the endpoint information to EMS with instructions to remove the endpoint from quarantine.
4. EMS identifies and removes the endpoint from quarantine based on the request from FortiOS.

Getting started with managing Chromebooks

The following tasks are specific to Chromebook management.

This section also includes a description of how FortiClient EMS and FortiClient work with Google Chromebooks after setup is complete.

Configuring FortiClient EMS for Chromebooks

To configure FortiClient EMS for Chromebooks:

1. Start and log in to FortiClient EMS. See Starting FortiClient EMS and logging in on page 113.
2. Add SSL certificates. See Adding an SSL certificate to FortiClient EMS on page 648.
3. Configure FortiClient EMS settings. See System Settings on page 628.
4. Configure user accounts and permissions. See Admin Users on page 563.

Configuring the Google Admin console

Following is an overview of how to configure the Google Admin console to prepare for adding the Google domain to FortiClient EMS. The document assumes you have created the Google domain.

To configure the Google Admin console:

1. Add the FortiClient Web Filter extension. See Adding the FortiClient Web Filter extension on page 127.
2. Configure the FortiClient Web Filter extension. See Configuring the FortiClient Web Filter extension on page 127.
3. Add root certificates. See Adding root certificates on page 129.
4. Configure unique service account credentials. See Configuring unique service account credentials on page 134.
5. Disallow incognito mode. See Disallowing incognito mode on page 131.

Deploying a profile to Chromebooks

Following is an overview of how to add a Google domain, configure profiles, and push profiles to Google Chromebooks. After you add the extension in the Google Admin console, the extension is downloaded to the Google Chromebook when the Chromebook user logs into the Chromebook.

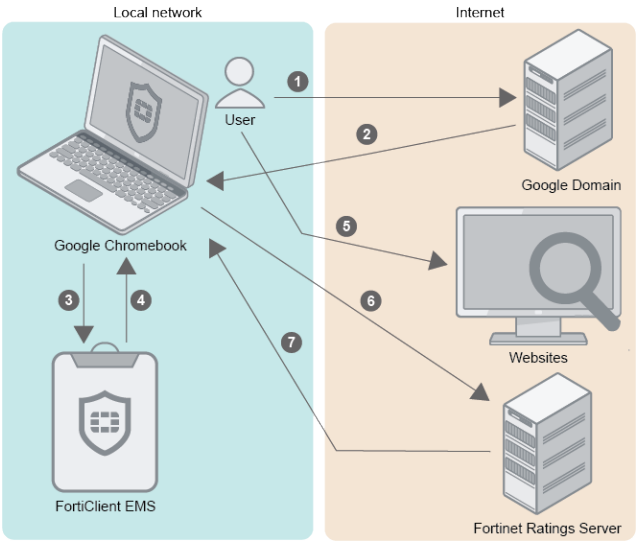
To deploy a profile to Chromebooks:

1. Add the Google domain. See Adding a Google domain on page 221.
2. Define web filtering options in one or more profiles. You can enable Safe Search in profiles. See Adding a new Chromebook profile on page 256.
3. Edit an existing endpoint policy or create a new endpoint policy that is configured with desired profile. Configure the endpoint policy to apply to domains to deploy FortiClient on Chromebooks. See Chromebook Policy on page 254.
4. Verify the FortiClient Web Filter extension. See Verifying the FortiClient Web Filter extension on page 133.
5. View Google domains and Google users. See Viewing domains on page 222.

How FortiClient EMS and FortiClient work with Chromebooks

After you install and configure FortiClient EMS, the Google Admin console, and the FortiClient Web Filter extension, the products work together to provide web filtering security for Google Chromebook users logged into the Google domain. Following is a summary of how the products work together after setup is complete:

1. A user logs into the Google Chromebook.
2. The Google Chromebook downloads the FortiClient Web Filter extension.
3. FortiClient connects to FortiClient EMS.
4. FortiClient downloads a profile to the Google Chromebook. The profile contains web filtering settings from FortiClient EMS.
5. The user browses the Internet on the Google Chromebook.
6. FortiClient sends the URL query to the Fortinet Ratings Server.
7. The Fortinet Ratings Server returns the category result to FortiClient. FortiClient compares the category result with the profile to determine whether to allow the Google Chromebook user to access the URL.


Local network
Internet
User
Google Chromebook
Google Domain
Websites
FortiClient EMS
Fortinet Ratings Server
1
2
3
4
5
6
7

Installation preparation

This section helps you prepare to install FortiClient EMS. Before installing FortiClient EMS, be aware of the following information:



Before installing FortiClient EMS, reading the *FortiClient EMS Release Notes* to become familiar with relevant software components and other important information about the product is recommended.



Because implementing or migrating to EMS 7.4.0 on the Linux platform can be complex, Fortinet highly recommends FortiClient Best Practices Service (BPS).

FortiClient Best Practices Service is an account-based annual subscription providing access to a specialized team that delivers remote guidance on deployment, upgrades, and operations. The service allows customers to share information about their deployment, user requirements, resources, and other related items. Based on the information provided, the BPS experts can provide recommended best practices, sample code, links to tools, and other materials or assistance to speed adoption and guide the customer towards best practice deployments. The team does not log into customer devices to make changes for them. This is a consulting and guidance service which may include sample configurations or playbooks. This is not an on-site professional services offer.

System requirements

The minimum system requirements for FortiClient EMS are:

- Ubuntu 22.04 or 24.04 LTS Server and Desktop
- No additional installed services
- 2.0 GHz 64-bit processor, six virtual CPUs (6 vCPU)
- 12 GB RAM
- 80 GB free hard disk
- Gigabit (10/100/1000baseT) Ethernet adapter
- Installing EMS requires an active internet connection. During installation, EMS also tries to download information about FortiClient signature updates from FortiGuard.
- For the language to install and time and currency format, select English (United States). For the keyboard or input method, select US.
- ext4 file system

Considering the ease that virtualization offers, installing EMS and PostgreSQL on virtual machines (VM) is recommended. You may save VM checkpoints or snapshots before major operating system, application, or configuration changes.



Only install FortiClient EMS and the default services for the operating system on the server. Do not install additional services on the same server as FortiClient EMS. Unnecessary services may cause port conflicts and issues during upgrades and interrupt EMS functionality.



Installing and running EMS on a domain controller is not supported.

License types

This section describes licensing options available for FortiClient EMS. It provides information for each license type to help determine which license best suits your needs.

FortiClient EMS

This section contains licensing information for FortiClient EMS:

Free trial license

After you install EMS, you can enable a free trial license. With the free trial license, you can provision and manage FortiClient on three Windows, macOS, Linux, iOS, and Android endpoints and three Chromebooks indefinitely. The trial license includes the same functionality as the zero trust network access license and does not include Sandbox Cloud support. EMS consumes one license count for each managed endpoint.

See To apply a trial license to FortiClient EMS: on page 118.

You must have an eligible FortiCloud account to activate an EMS trial license. A FortiCloud account can only have one EMS trial license.

The trial license has the following limitations:

- You should not use a trial license for production purposes.
- A trial license does not entitle you to Fortinet technical support.
- Fortinet may cancel a trial license if the terms of use are violated.
- The free trial policy terms may change at any time at Fortinet's discretion.
- You can only have one trial license per customer.
- You cannot create an installer from the FortiGuard distribution server. See Adding a FortiClient installer on page 230.



For evaluation, contacting Fortinet sales for an evaluation license is recommended. With an evaluation license, Fortinet provides support as needed during the evaluation period. See How to Buy and Product Download for FortiClient EMS.

Windows, macOS, and Linux licenses

FortiClient EMS supports per-endpoint and per-user licensing. You cannot use both license types on one FortiClient EMS instance.

The following are the latest license bundles for FortiClient EMS:

License name	Description
Endpoint protection platform (EPP)	Full license that offers all FortiClient features. Includes all features detailed for the zero trust network access (ZTNA) license, as well as antivirus (AV), antiransomware, antiexploit, cloud-based malware detection, Application Firewall, software inventory, USB device control, and advanced threat protection via FortiClient Cloud Sandbox (SaaS). Fortinet offers this license for both per-endpoint and per-user licensing.
ZTNA	Includes support for Fabric Agent for endpoint telemetry, security posture check via ZTNA tagging, remote access (IPsec and SSL VPN), Vulnerability Scan, Web Filter, and threat protection via Sandbox (appliance only). Each purchased ZTNA license allows management of one FortiClient Windows, macOS, Linux, iOS, Android, or Chromebook endpoint. You must purchase a minimum of 25 endpoint licenses, and you can have these EMS licenses for a maximum five year term. You can specify the number of endpoints and the term duration at time of purchase. If you do not apply a ZTNA license to EMS, no endpoints can register to EMS. Fortinet offers this license for both per-endpoint and per-user licensing.
FortiSASE	License that applies for deployments using FortiSASE. See FortiSASE.
FortiGuard Endpoint Forensics Analysis	The forensic service provides remote endpoint analysis to help endpoint customers respond to and recover from cyber incidents. For each engagement, forensic analysts from Fortinet's FortiGuard Labs remotely assist in the collection, examination, and presentation of digital evidence, including a final detailed report. This is an add-on license that you can apply to per-endpoint and per-user EPP, ZTNA, and FortiSASE licensing. On-premise EMS only supports this feature for Windows endpoints.

You can purchase different numbers of EPP and ZTNA licenses. For example, you can purchase 100 EPP licenses and 200 ZTNA licenses. EMS applies licenses based on the features that are enabled in the endpoint's assigned profile.

For per-user licenses, you can manually remove or exclude users from management to free up license seats. Each per-user license allows the user to register three devices. If a user registers a fourth device, they consume two licenses.

When using per-user licensing, using user verification is recommended. See User Management on page 594. If an endpoint connects to EMS by specifying the EMS IP address or using an invitation code, without using user verification, EMS considers the locally logged-in user identity as consuming a user license.

The following shows a more comprehensive comparison between the features included in the EPP and ZTNA licenses:

Feature	EPP	ZTNA
Zero Trust Security		
Zero Trust Agent	Yes	Yes
Central management via EMS	Yes	Yes
Dynamic Security Fabric connector	Yes	Yes
Vulnerability agent and remediation	Yes	Yes
SSL VPN with multifactor authentication (MFA)	Yes	Yes
IPsec VPN with MFA	Yes	Yes
Integration with FortiSandbox (on-premise/PaaS)	Yes	Yes
Next Generation Endpoint Security		
AI-powered next generation AV	Yes	
FortiClient Cloud Sandbox (SaaS)	Yes	
Automated endpoint quarantine	Yes	
Application inventory	Yes	
Application Firewall	Yes	
Software Inventory	Yes	

You must purchase a license for each registered endpoint or user.

Chromebook licenses

Each purchased Chromebook license allows management of one Google Chromebook user. You must purchase a minimum of 25 Google Chromebook user licenses and can have these EMS licenses for a maximum three year term. You can specify the number of Google Chromebook users and the term duration at time of purchase. FortiClient EMS uses one license seat per logged-in user. If the user logs out, the license seat times out (default timeout being 24 hours), and the license is released. At this point, another user can use this license seat.

If the number of Chromebooks that the EMS is managing exceeds the number of Chromebook licenses available, EMS licenses the additional Chromebooks using any available zero trust network access (ZTNA) licenses. For example, consider that your EMS instance has 50 Chromebook licenses, but 80 Chromebooks connect to the EMS instance. EMS licenses 50 Chromebooks using the Chromebook licenses, and licenses the remaining 30 Chromebooks using 30 ZTNA licenses, if available. EMS only licenses Chromebooks using ZTNA licenses if no Chromebook license is available. See Windows, macOS, and Linux licenses on page 25 for information about the ZTNA license.



EMS sends you an email when you are running out of licenses. Additionally, a log entry is entered when a client is refused connection due to unavailable licenses.

Component applications

Common services or applications do not require a license.



Installation of common services required for FortiClient EMS does not ask you for license information.

Required services and ports

You must ensure that you enable required ports and services for use by FortiClient EMS and its associated applications on your server. The required ports and services enable FortiClient EMS to communicate with endpoints and servers running associated applications. You do not need to enable ports 8013 and 10443 as the FortiClient EMS installation opens these.

Communication	Usage	Protocol	Port	Incoming or outgoing	How to customize
ACME	EMS can use certificates that are managed by Let's Encrypt and other certificate management services that use the ACME protocol. This feature also requires port 443. See Adding an SSL certificate to FortiClient EMS on page 648.	TCP	80	Incoming	N/A

Communication	Usage	Protocol	Port	Incoming or outgoing	How to customize
Active Directory (AD) server connection	Retrieving workstation and user information	TCP	389 (LDAP) or 636 (LDAPS)	Outgoing	GUI
Antivirus (AV) allowlist signature download	Downloading AV allowlist signatures	TCP	10443 (default)	Incoming	N/A
Apache/HTTPS	Web access to FortiClient EMS. Also required for the ACME feature.	TCP	443	Incoming	Installer
Communication between EMS AD connector and AD servers	Enables synchronization of AD groups and users with EMS for endpoint management, policy enforcement, and SAML-based authentication.	TCP	8871	Incoming	N/A
Communication with FortiOS	EMS is the server that opens up the port for FortiOS to connect to as a client.	TCP	8015	Incoming	N/A
FortiClient download	Downloading FortiClient deployment packages that FortiClient EMS created	TCP	10443 (default)	Incoming	Installer
FortiClient endpoint probing	FortiClient EMS uses ICMP for endpoint probing during FortiClient initial deployment.	ICMP	N/A	Outgoing	N/A
FortiClient Telemetry	FortiClient endpoint management	TCP	8013 (default)	Incoming	Installer or GUI
FortiCloud	FortiCloud services (forticlient.forticloud.com)	TCP	443	Outgoing	N/A
License synchronization	FortiCare login (support.fortinet.com) to synchronize licenses	TCP	443	Outgoing	N/A
SCEP service	Installing zero trust network access certificate	TCP	4001, 4002	Incoming	N/A

Communication	Usage	Protocol	Port	Incoming or outgoing	How to customize
SMTP server, email	Alerts for FortiClient EMS and endpoint events. When an alert is triggered, EMS sends an email notification.	TCP	25 (default)	Outgoing	GUI
Web Filter custom page download	Downloading custom Web Filter pages that the administrator created in EMS	TCP	10443 (default)	Incoming	N/A

The following ports and services only apply when using FortiClient EMS to manage Chromebooks:

Communication	Usage	Protocol	Port	Incoming or outgoing	How to customize
FortiClient on Chrome OS	Connecting to FortiClient EMS	TCP	8443 (default) You can customize this port.	Incoming	GUI
Google Workspace API/Google domain directory	Retrieving Google domain information using API calls	TCP	443	Outgoing	N/A

You should enable the following ports and services for use on Chromebooks when using FortiClient for Chromebooks:

Communication	Usage	Protocol	Port	Incoming or outgoing	How to customize
FortiClient EMS	Connecting to the profile server	TCP	8443 (default)	Outgoing	Via Google Admin console when adding the profile
FortiGuard	Rating URLs	TCP	443, 3400	Outgoing	N/A

EMS uses the following FQDN for installer creation:

Usage	Server URL	Protocol	Port	Incoming or outgoing
Create installers on Fortinet-hosted servers and download them locally to EMS for deployment to endpoints	forticlient-rs.forticloud.com	TCP	443	Incoming/outgoing

EMS connects to FortiGuard to download AV and vulnerability scan engine and signature updates and FortiClient and EMS installer downloads. EMS can connect to legacy FortiGuard or FortiGuard Anycast. The following table summarizes required services for EMS to communicate with FortiGuard:

Usage	Server URL			Protocol	Port	Incoming or outgoing	How to customize
	Global	U.S.	Europe				
AV and vulnerability signature update and FortiClient installer downloads	• forticlient.fortinet.net • myforticlient.fortinet.net	usforticlient.fortinet.net	N/A	TCP	80	Outgoing	N/A
AV and vulnerability signature updates with FortiGuard Anycast and FortiClient installer package download	fctupdate.fortinet.net	fctusupdate.fortinet.net	fcteuupdate.fortinet.net	TCP	443	Outgoing	N/A

FortiClient EMS can also connect to FortiClient Cloud Sandbox (SaaS) for integration with FortiSandbox. The following table summarizes required services for FortiClient EMS to communicate with FortiClient Cloud Sandbox (SaaS):

Usage	Server URL	Protocol	Port	Incoming or outgoing	How to customize
FortiClient EMS Cloud Sandbox (SaaS) connection	aptctrl1.fortinet.com	TCP	443 (default)	Outgoing	N/A



For the list of required services and ports for FortiClient, see the *FortiClient Administration Guide*.

Telemetry data usage requirements

Telemetry syncs between EMS and endpoints transfer data. The amount of data transferred **varies** significantly between cases and depends on many factors, such as the amount of zero trust network access (ZTNA) tags, the features enabled in the endpoint configuration, and so on.

The following table provides statistics for the average and maximum amounts of data transferred when the Telemetry sync occurs and includes certain events or configuration changes. You may find this information useful for your own sizing and deployment planning. However, this information **is not intended to provide a comprehensive overview or exact** data for your deployment.

	Data amount transferred (KB)		Notes
	Average	Maximum	
Avatar			
User uploads avatar for the first time	4.54	8.99	157 KB size image
User changes their avatar	8.85	15.39	Avatar changed from 157 KB image to 878 KB image
Endpoint registration			
Endpoint registers to EMS for the first time	14.25	58.95	
Endpoint status changes from offline to online	3.24	3.83	

	Data amount transferred (KB)		Notes
	Average	Maximum	
Endpoint maintains connection to EMS at keepalive interval	2.3	2.31	
Endpoint policy updates			
Policy includes some configuration updates. Policy does not include a VPN profile.	5.03	8.39	
Policy includes some configuration updates. Policy includes SSL VPN configuration and no IPsec VPN configuration.	5.48	8.36	
Policy includes some configuration updates. Policy includes IPsec VPN configuration and no SSL VPN configuration.	5.48	8.37	
Quarantine			
File added to allowlist	2.71	3.77	
File removed from allowlist	2.51	2.91	
ZTNA			
New ZTNA tag applied to endpoint	0.66	3.52	
Endpoint receives new ZTNA rules and displays updated tags	1.47	3.54	
Endpoint deletes non-applicable tag	2.688	3.47	
Other			
Download deployment package (Windows)	6145.18	190407.34	Example deployment package size is 185 MB. Data transfer amount measured until reboot notification appears on endpoint.
Download deployment package (macOS)	3266.82	254507.06	Example deployment package size is 276 MB. Data transfer amount measured until reboot notification appears on endpoint.

Management capacity

FortiClient EMS is intended for enterprise use and has the capacity to manage a large number of endpoints.



Having at least 200 GB of disk space available is recommended.

The following features require additional disk space:

- Multitenancy site: 1 GB per site
- Deployment package: 1.1 GB per deployment package

You can install EMS with default PostgreSQL (Postgres) shipped with EMS. When managing more than 50000 endpoints, install Postgres in a Docker container running on a different machine or install Postgres standalone on a different machine. Otherwise, you may experience database deadlocks.

The following topics include suggested host system hardware configurations for FortiClient EMS. The suggested configurations depend on the number of endpoints FortiClient EMS manages, whether Postgres and EMS are on the same or different servers, and whether there are FortiGates connected to EMS. EMS supports a maximum of 200 multitenancy sites. However, you must derive the actual number of supported sites for your configuration in conjunction with the management capacity tables. See the following for the suggested host system hardware configurations for these scenarios:

- Hardware configuration when EMS and Postgres run on same machine with no FortiGate connected on page 33
- Hardware configuration when EMS and Postgres run on different machines with no FortiGate connected on page 34
- Hardware configuration when there are FortiGates connected to the EMS on page 35

Hardware configuration when EMS and Postgres run on same machine with no FortiGate connected

The following table shows the configurations when EMS and PostgreSQL (Postgres) run on the same Linux server machine with no FortiGate connected and multitenancy disabled:

Number of managed endpoints	Number of virtual CPUs	Memory (RAM) (in GB)	Suggested keep alive (KA) interval	Deployment duration
Up to 5000	6	12	Default (60 seconds)	6 to 12 hours
5000 to 10000	10	18		12 to 24 hours
10000 to 20000	14	22	120 seconds	1 to 2 days
20000 to 50000	22	28		3 to 4 days

The following table shows the configurations when EMS and Postgres run on the same Linux server machine with no FortiGate connected and multitenancy enabled with up to 20 sites:

Number of managed endpoints	Number of virtual CPUs	Memory (RAM) (in GB)	Suggested KA interval
Up to 5000	6	16	Default (60 seconds)
5000 to 10000	10	26	
10 000 to 20 000	14	30	120 seconds
20 000 to 50 000	22	36	

Hardware configuration when EMS and Postgres run on different machines with no FortiGate connected

The following table shows the configurations when EMS and PostgreSQL (Postgres) run on different Linux server machines with no FortiGate connected and multitenancy disabled:

Number of managed endpoints	EMS server machine		Postgres server machine		Suggested keep alive (KA) interval	Deployment duration
	Number of virtual CPUs	Memory (RAM) (in GB)	Number of virtual CPUs	Memory (RAM) (in GB)		
10000 to 20000	8	6	4	16	120 seconds	1 to 2 days
20000 to 50000	16	8	6	22		3 to 4 days
50000 to 75000	20	10	10	26		4 to 5 days
75000 to 150000	26	14	16	44	180 seconds	6 to 8 days
150000 to 250000	32	20	26	56	240 seconds	10 to 14 days

The following table shows the configurations when EMS and Postgres run on different Linux server machines with no FortiGate connected and multitenancy enabled with up to 20 sites:

Number of managed endpoints	EMS server machine		Postgres server machine		Suggested KA interval
	Number of virtual CPUs	Memory (RAM) (in GB)	Number of virtual CPUs	Memory (RAM) (in GB)	
10000 to 20000	8	8	4	22	120 seconds
20000 to	16	10	8	28	

Number of managed endpoints	EMS server machine		Postgres server machine		Suggested KA interval
	Number of virtual CPUs	Memory (RAM) (in GB)	Number of virtual CPUs	Memory (RAM) (in GB)	
50000					
50000 to 75000	20	12	12	32	
75000 to 150000	26	16	18	54	180 seconds
150000 to 250000	32	22	28	66	240 seconds

The following table shows the configurations when EMS and Postgres run on different Linux server machines with no FortiGate connected and multitenancy enabled with up to 200 sites.

In addition to the recommended Postgres configuration in Installing EMS with standalone remote database without Docker on page 72, configure the following:

- `max_connections = 9999`
- `checkpoint_timeout = '2min'`

Number of sites	Number of managed endpoints	EMS server machine		Postgres server machine		Suggested keep alive interval
		Number of virtual CPUs	Memory (RAM) (in GB)	Number of virtual CPUs	Memory (RAM) (in GB)	
50	Up to 100000	24	18	26	64	180 seconds
200	Up to 20000	10	12	24	48	120 seconds

For performance issues regarding multitenancy-enabled cases, see Known issues.

Hardware configuration when there are FortiGates connected to the EMS

The following table shows the resource requirement for the following EMS setup:

- EMS and PostgreSQL (Postgres) run on the same Linux server machine
- Up to 100 FortiGates connected to the EMS
- Up to 20 security posture tags are configured

Number of managed endpoints	Number of virtual CPUs	Memory (RAM) (in GB)	Suggested keep alive (KA) interval
Up to 5000	8	14	Default (60 seconds)
5000 to 10000	12	18	
10000 to 20000	14	22	120 seconds
20000 to 50000	36	30	

The following table shows the resource requirement for the following EMS setup:

- EMS and Postgres run on different Linux server machines
- Up to 300 FortiGates connected to the EMS. FortiGates are recommended to run FortiOS 7.4.1 and later versions.
- Up to 20 security posture tags are configured

Number of managed endpoints	EMS server machine		Postgres server machine		Suggested KA interval
	Number of virtual CPUs	Memory (RAM) (in GB)	Number of virtual CPUs	Memory (RAM) (in GB)	
10000 to 20000	12	8	12	20	120 seconds
20000 to 50000	18	12	32	30	
50000 to 75000	22	14	36	36	
75000 to 150000*	26	20	48	56	180 seconds

* Supports up to 100 FortiGates only.

FortiClient Telemetry security features

FortiClient connects to EMS and FortiGate over an SSL connection. All protocol exchanges flow through this secure connection. The connection is closed after protocol exchanges between both parties are complete. The SSL connections require a valid certificate.

You can configure Telemetry connections between FortiClient and FortiGate or EMS to require a preshared password or connection key. See Configuring EMS settings on page 629.

The default Telemetry port number is 8013. You can change this in EMS and FortiClient. When a port is not provided, FortiClient always attempt to connect to the default port, which is 8013. Changing this in EMS locks out endpoints that are still using the default.

At any time, you can disconnect a rogue endpoint from EMS and prevent it from reconnecting to EMS in the future.

See Required services and ports on page 27 for a list of TCP/IP ports that EMS uses. You can block all other ports or service requests to the EMS IP address or fully qualified domain name (FQDN).

Server readiness checklist for installation

Use the following checklist to prepare your server for installation:

Checklist	Readiness factor
	Temporarily disable security applications. You must temporarily disable any antivirus software on the target server before you install FortiClient EMS. Installation may be slow or disrupted while these programs are active. A server may be vulnerable to attack when you uninstall or disable security applications.
	Consider the date and time settings you apply to your server. If managing Chromebooks, syncing the time to the Google server time is recommended.
	Confirm required services and ports are enabled and available for use by FortiClient EMS. Ensure that no conflicts exist with all ports that Required services and ports on page 27 lists as incoming.
	For air-gapped deployment, while you can operate EMS in an air-gapped environment with no access to the Internet, the initial installation still requires Internet connection and must happen in a non air-gapped environment.

Upgrading EMS

Upgrading from an earlier FortiClient EMS version



FortiClient EMS 7.4.3 only supports upgrading from 7.4.

For other versions, you must upgrade EMS to a supported 7.2 version, then migrate from the Windows Server model to the Linux model as Migrating EMS 7.2 to 7.4.3 on page 46 describes.

For instructions on upgrading EMS to 7.2, see Upgrading from an earlier FortiClient EMS version.



Before any version upgrade or other maintenance, back up the EMS database. Consider performing a full server backup or taking a VM snapshot if possible.

Legacy licenses

EMS 7.4.3 does not support legacy 158 licenses, which were in use before 2021 and have reached end-of-life. Following is a list of discontinued SKUs:

- FC1-15-EMS01-158-02-DD
- FC1-15-EMS02-158-02-DD

If you attempt an upgrade to EMS 7.4.3 with the legacy 158 licenses, the EMS installer displays an error message: *Legacy license is not supported after upgrade*. The EMS upgrade does not proceed.

EMS 7.4.3 does not support the following legacy licenses:

- FC1-15-EMS01-297-01-DD
- FC2-15-EMS01-297-01-DD
- FC3-15-EMS01-297-01-DD
- FC4-15-EMS01-297-01-DD
- FC1-15-EMS03-297-01-DD
- FC2-15-EMS03-297-01-DD
- FC1-15-EMS03-298-01-DD
- FC2-15-EMS03-298-01-DD
- FC1-15-EMS01-299-01-DD
- FC2-15-EMS01-299-01-DD
- FC3-15-EMS01-299-01-DD

You may be using the EMS migration tool to migrate your Windows Server-based EMS 7.2 to the Linux-based EMS 7.4. If you attempt to migrate EMS 7.2 using a legacy license to EMS 7.4 using the migration tool, the migration tool aborts the process and displays a `Current EMS Windows license is not supported in EMS Linux, migration is aborted` message.

```
PS C:\Users\Administrator\Downloads> .\migration.exe
------------------------------------------------------------
Current EMS Windows license is not supported in EMS Linux, migration is aborted.
------------------------------------------------------------
```

Upgrading EMS from an earlier 7.4 version

Detailed instructions on how to perform upgrades on different EMS installation modes such as standalone or high availability are available in the final section of the respective installation guides. For example, see Installing EMS in standalone mode on page 54.

To upgrade EMS from an earlier version:

1. When upgrading EMS, `/tmp` must have enough free space to hold `/opt/forticlientems`. Otherwise, the upgrade fails. Check the current size of `/opt/forticlientems`:

   ```
   du -hs /opt/forticlientems
   ```

2. Ensure that `/tmp` has enough free space to hold `/opt/forticlientems`.
3. Run `sudo -i` to log in to the shell with root privileges.

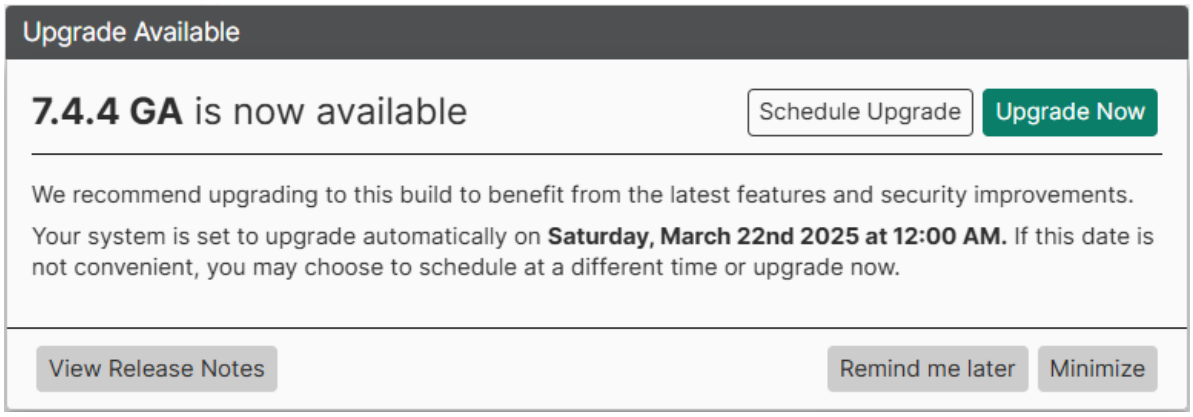
4. Change permissions and add execute permissions to the installation file:
   `chmod +x forticlientems_7.4.3.XXXX.XXX64.bin`
5. Run the following command to install EMS:
   `./forticlientems_7.4.3.XXXX.XXX64.bin -- --allowed_hosts '*' --enable_remote_https`
   Run the installer to and from any directory other than `/tmp`. Running the installer to or from `/tmp` causes issues.

Automatically upgrading EMS to latest patch release

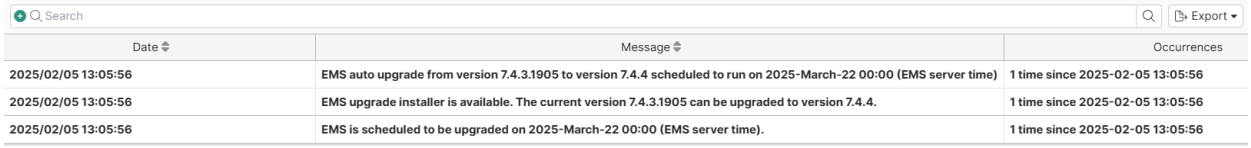
When a later patch of the current EMS version is available, by default, EMS schedules an upgrade at a date between 45 to 52 days in the future. Upgrades to the latest version are distributed over a week to ensure that Fortinet can minimize the impact of any issues and resolve them without affecting all users using that EMS version. EMS displays a prompt with the upgrade details and also offers the following options:

- Upgrade immediately
- Schedule the upgrade at a convenient time

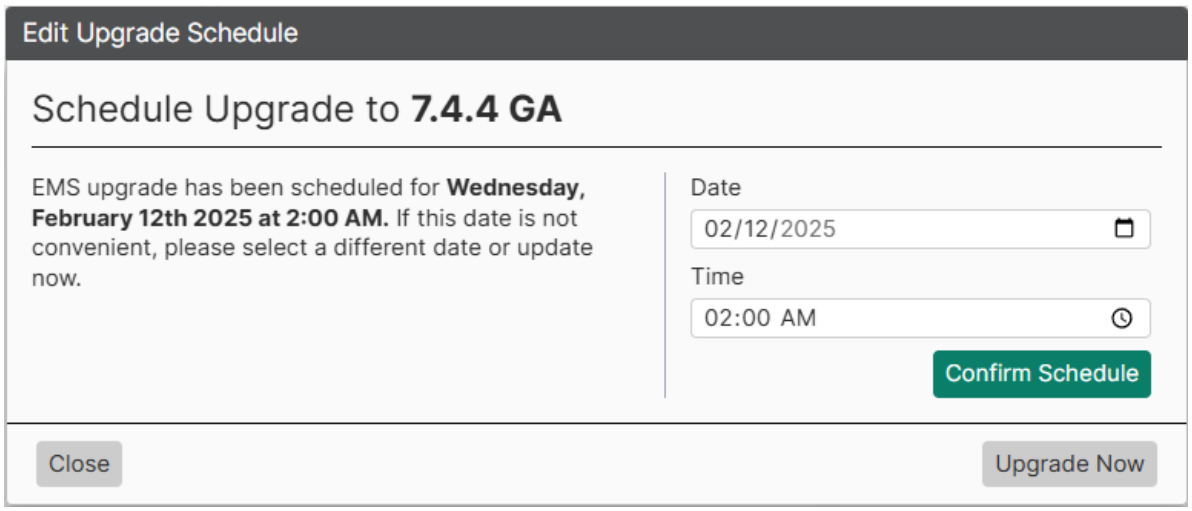
While EMS operates, it consistently pings FortiCloud to retrieve the entitlement status and latest patch release information. This encourages upgrading to the latest patch releases, which can help with vulnerability detection.



EMS also shows an alert when the upgrade is available and scheduled. If you have configured email alerts, EMS also sends email alerts regarding the upgrade.



If desired, click *Schedule Upgrade* in the notification to reschedule the upgrade within 45 days of the notification.

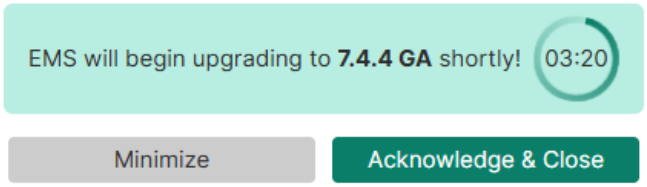


After you schedule an upgrade, you can modify it by clicking *Edit* in the upper right corner of the GUI.

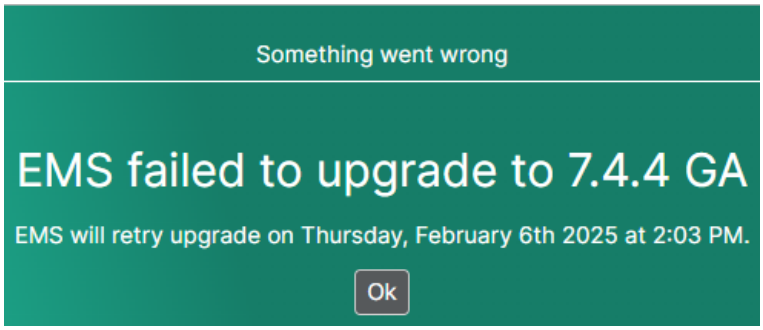


If you select *Upgrade Now*, EMS displays options to back up the EMS database (DB). After backing up the DB, you can click *Upgrade Now*. EMS starts a five-minute countdown, after which it initiates the upgrade procedure.

The prompt to back up the EMS DB only appears if you select *Upgrade Now*. Backing up the EMS DB before upgrade, including scheduled upgrades, is recommended. See To back up the DB: on page 152.



As the upgrade proceeds, EMS displays the progress. If the upgrade fails, EMS automatically reschedules the upgrade to 24 hours after the original scheduled upgrade time.

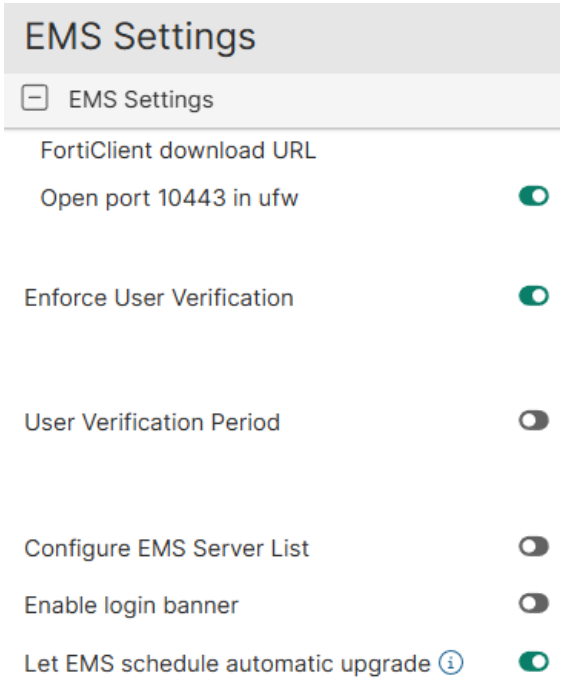


If four consecutive upgrade attempts fail, EMS deletes the upgrade schedule. After an hour, EMS pulls the version available from FortiGuard, and retries scheduling the upgrade again as if it were a fresh upgrade attempt, 45 to 52 days in the future.

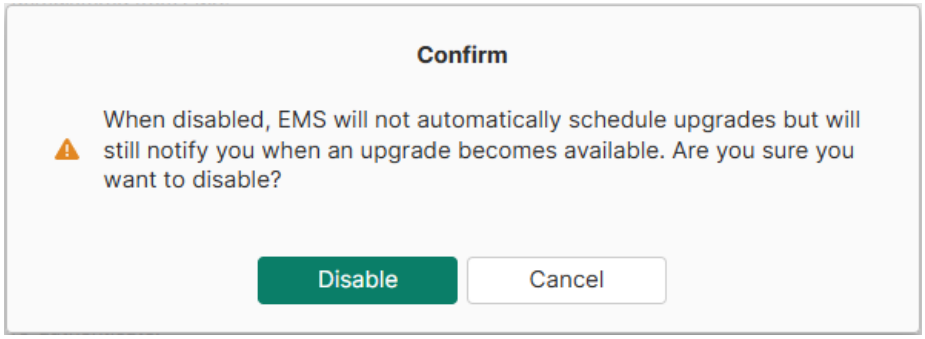
If your EMS is a member of a high availability cluster, manually upgrading the nodes is recommended instead of using auto upgrade.

Disabling automatic upgrade

In *System Settings > EMS Settings*, you can disable the *Let EMS schedule automatic upgrade* option to disable automatic upgrade behavior. EMS enables this option by default.



If you disable *Let EMS schedule automatic upgrade*, EMS removes any previously scheduled automatic upgrade.



If you disable automatic upgrade and manually schedule an upgrade, you can cancel the upgrade.

Upgrading EMS in HA

The following gives instructions on upgrading EMS nodes in a high availability (HA) cluster to 7.4.3.

To upgrade EMS in HA:

1. Stop the monitor service on secondary EMS nodes. This avoids failover while upgrading the primary EMS node:
2. On all nodes, do the following:
   a. Download the forticlientems_7.4.3.XXXX.bin file from the Fortinet Support site.
   b. Run `sudo -i` to log in to the shell with root privileges.
   c. Change permissions and add execute permissions to the installation file:
   `chmod +x forticlientems_7.4.3.XXXX.bin`
3. On the primary node, install EMS:
   a. Set `umask` to 022 on file `/etc/login.defs` if the existing `umask` setting is more restrictive.
   b. Install EMS:

```
./forticlientems_7.4.3.XXXX.bin -- --db_host "<database server 1 IP address or
FQDN>,<database 2 IP address or FQDN>" --db_user postgres --db_pass <postgres password> --
skip_db_install --allowed_hosts '*' --enable_remote_https
```

   Run the installer to and from any directory other than `/tmp`. Running the installer to or from `/tmp` causes issues.



   Configure `db_host` with your DB server IP addresses or FQDNs.
   Replace `<postgres password>` with the Postgres user password.

   c. After installation completes, check that all EMS services are running by entering the following command:

```
systemctl --all --type=service | grep -E 'fcems|apache|redis|postgres'
```

```
root@emsnode2:/home/ems/Downloads# systemctl --all --type=service | grep -E 'fcems|apache|redis|postgres'
  apache2.service                              loaded    active   running The Apache HTTP Server
  fcems_adconnector.service                    loaded    active   running adconnector service
  fcems_addaemon.service                       loaded    active   running addaemon service
  fcems_adevtsrv.service                       loaded    active   running adevtsrv service
  fcems_adtask.service                         loaded    active   running adtask service
  fcems_chromebook.service                     loaded    active   running chromebook worker service
  fcems_das.service                            loaded    active   running das service
  fcems_dbop.service                           loaded    active   running dbop worker service
  fcems_deploy.service                         loaded    active   running deploy worker service
  fcems_ecsocksrv.service                      loaded    active   running ecsocksrv service
  fcems_forensics.service                      loaded    active   running forensics worker service
  fcems_ftntdbimporter.service                 loaded    active   running FTNT DB importer worker service
  fcems_installer.service                      loaded    active   running installer worker service
  fcems_ka.service                             loaded    active   running kaworker service
  fcems_mdmproxy.service                       loaded    active   running MDM proxy service
  fcems_monitor.service                        loaded    active   running monitor worker service
  fcems_notify.service                         loaded    active   running FOS notify service
  fcems_pgbouncer.service                      loaded    active   running pgBouncer for EMS service
  fcems_probe.service                          loaded    active   running probeworker service
  fcems_reg.service                            loaded    active   running regworker service
  fcems_scep.service                           loaded    active   running SCEP service
  fcems_sip.service                            loaded    active   running software inventory processor service
  fcems_tag.service                            loaded    active   running tagworker service
  fcems_task.service                           loaded    active   running taskworker service
  fcems_update.service                         loaded    active   running update worker service
  fcems_upload.service                         loaded    active   running upload worker service
  fcems_wspgbouncer.service                    loaded    active   running pgBouncer for EMS WebServer service
  fcems_ztna.service                           loaded    active   running ztna worker service
  postgresql.service                           loaded    active   exited  PostgreSQL RDBMS
  postgresql@15-main.service                   loaded    active   running PostgreSQL Cluster 15-main
  redis-server.service                         loaded    active   running Advanced key-value store
```

The output shows that postgresql.service status displays as `exited`. This is the expected status. EMS does not create this service, which only exists to pass commands to version-specific Postgres services. It displays as part of the output as the command filters for all services that contain "postgres" in the name.

4. On the secondary node, install EMS:
   a. Set `umask` to 022 if the existing `umask` setting is more restrictive.
   b. Install EMS:

```
./forticlientems_7.4.3.XXXX.bin -- --db_host "<Postgres node 1 IP address>,<Postgres node 2 IP address>" --db_user postgres --db_pass postgres --skip_db_install --skip_db_deploy --allowed_hosts '*' --enable_remote_https
```

   Run the installer to and from any directory other than `/tmp`. Running the installer to or from `/tmp` causes issues.



   Configure `db_host` with your DB server IP addresses or FQDNs.
   Replace `<postgres password>` with the Postgres user password.

   c. After installation completes, check that EMS services are running by entering the following command. On the secondary EMS, only fcems_monitor, fcems_pgbouncer, fcems_wspgbouncer, and redis-server services should be running:

```
systemctl --all --type=service | grep -E 'fcems|apache|redis|postgres'
```

Install preparation for managing Chromebooks

Google Workspace account

You must sign up for your Google Workspace account before you can use the Google service and manage your Chromebook users.

The Google Workspace account is different from the free consumer account. The Google Workspace account is a paid account that gives access to a range of Google tools, services, and technology.

You can sign up for a Google Workspace account here.

In the signup process, you must use your email address to verify your Google domain. This also proves you have ownership of the domain.

SSL certificates

FortiClient EMS requires an SSL certificate that a Certificate Authority (CA) signed in pfx format. Use your CA to generate a certificate file in pfx format, and remember the configured password. For example, the certificate file name is *server.pfx* with password 111111.

The server where you installed FortiClient EMS should have an FQDN, such as ems.forticlient.com, and you must specify the FQDN in your SSL certificate.

If you are using a public SSL certificate, the FQDN can be included in *Common Name* or *Subject Alternative Name*. You must add the SSL certificate to FortiClient EMS. See Adding an SSL certificate to FortiClient EMS on page 648. You do not need to add the root certificate to the Google Admin console.

If you are using a self-signed certificate (non-public SSL certificate), your certificate's *Subject Alternative Name* must include `DNS:<FQDN>`, for example, `DNS:ems.forticlient.com`. You must add the SSL certificate to FortiClient EMS and the root certificate to the Google Admin console to allow the extension to trust FortiClient EMS. See Adding root certificates on page 129.

Installation and licensing

Before you install and license FortiClient EMS on a server, ensure you have:

- Reviewed License types on page 23
- Met the requirements listed in Required services and ports on page 27
- Completed the Server readiness checklist for installation on page 37
- Logged into the server as the administrator. The administrator user account provides access to all common services, FortiClient EMS, and other application tasks. You can use this account to initially log into the server and to create other user accounts for normal day-to-day use of the applications.



Installing FortiClient EMS on a dedicated server in a controlled environment is recommended. Installing other software applications can interfere with normal operation of FortiClient EMS.

Downloading the installation file

FortiClient EMS is available for download from the Fortinet Support website.

You can also receive installation files from a sales representative.

The following installation files are available for FortiClient EMS:

- forticlientems_7.4.3.xxxx.bin
- forticlientems_7.4.3.xxxx_migration_tool.zip
- forticlientems_7.4.3.xxxx_postgres-ha.tar.gz
- forticlientems_7.4.3.xxxx_postgresql15.tar.gz

For information about obtaining FortiClient EMS, contact your Fortinet reseller.

Installing FortiClient EMS 7.4

EMS 7.4 introduces a shift to a Linux-based model from the Windows Server-based model in earlier EMS versions. This change provides numerous benefits, including improved architecture and flexibility. This document provides instructions to migrate your EMS data from an existing Windows Server-based instance to the Linux-based model, as well as installation instructions for various use cases.

EMS 7.4 only supports Ubuntu 22.04 and 24.04 Server and Desktop. While EMS 7.4 supports both Ubuntu Desktop and Server, consider that Desktop uses more resources that could otherwise be available for EMS usage. You should consider proper planning for hardware resources.

Installing EMS requires an active internet connection. During installation, EMS also tries to download information about FortiClient signature updates from FortiGuard.



Because implementing or migrating to EMS 7.4.0 on the Linux platform can be complex, Fortinet highly recommends FortiClient Best Practices Service (BPS).

FortiClient Best Practices Service is an account-based annual subscription providing access to a specialized team that delivers remote guidance on deployment, upgrades, and operations. The service allows customers to share information about their deployment, user requirements, resources, and other related items. Based on the information provided, the BPS experts can provide recommended best practices, sample code, links to tools, and other materials or assistance to speed adoption and guide the customer towards best practice deployments. The team does not log into customer devices to make changes for them. This is a consulting and guidance service which may include sample configurations or playbooks. This is not an on-site professional services offer.



You can also deploy EMS using a virtual machine image. See Deploying EMS as a VM image on page 55.

Migrating EMS 7.2 to 7.4.3

The following provides instructions for migrating existing EMS 7.2 configurations to EMS 7.4.3.

Only EMS 7.2 versions that released before the target 7.4 version support the migration. For example, EMS 7.4.3 released on March 20, 2025. EMS 7.2.9 released on April 9, 2025. Since EMS 7.2.9 released after 7.4.3, you cannot migrate an EMS 7.2.9 configuration to 7.4.3. You can migrate EMS 7.2.8, which released on January 15, 2025, to EMS 7.4.3. It is highly recommended to migrate to 7.4.3 from the latest 7.2 patch that was released before 7.4.3.

To migrate earlier EMS versions to 7.4.3, first upgrade them to a 7.2 version that supports the migration as FortiClient Upgrade Path describes.



Avoid saving or deleting mobile device management (MDM) integrations while both the old and new EMS servers are running. This is necessary because both EMS servers share the same MDM service, and one server can accidentally overwrite changes made on the other.

To configure the EMS Linux machine:

1. Install EMS 7.4.3 on the Linux machine. Do not configure any settings on EMS. See Installing EMS in standalone mode on page 54.
2. The EMS migration requires a user. You can create a new user or use an existing one. Add the user to the sudo, forticlient, and www-data groups. In this example the user is "test":

```
sudo adduser test
sudo usermod -aG sudo test
sudo usermod -aG forticlientems test
sudo usermod -aG www-data test
```

3. Allow SSH access for the migration user. This is necessary if migrating to the EMS VM image. By default, the VM image restricts SSH access to the built-in "ems" user only. To allow SSH access for the new user created in step 2, follow these steps:
   a. Edit the last line of the sshd_config file:

```
sudo nano /etc/ssh/sshd_config
```

   b. Add the new user (e.g., "test") to the `AllowUsers` line (the last line):

```
AllowUsers ems test
```

   c. Restart the SSH service to apply the changes:

```
sudo systemctl restart ssh
```

   You may revert this change after the migration is complete.
4. Do one of the following:
   - Disable firewall:

```
sudo ufw disable
```

   - Enable firewall and ports 5432, 443, and 22:

```
sudo ufw enable
sudo ufw allow 5432/tcp
sudo ufw allow 22/tcp
sudo ufw allow 443/tcp
```

5. Do the following steps if your implementation does not use Docker. If using Docker, go to step 6:
   a. Update `/etc/postgresql/15/main/postgresql.conf` to allow PostgreSQL database server listening on all IP addresses of the server. The default is on TCP port 5432. Find the line that reads `#listen_addresses = 'localhost'` and paste the following in a new line after it:

```
listen_addresses = '*'

sudo nano /etc/postgresql/15/main/postgresql.conf
#listen_addresses = 'localhost'
listen_addresses = '*'
```

b. Update `/etc/postgresql/15/main/pg_hba.conf` to allow remote access to the Postgres database server. Find the line that reads `host all all 127.0.0.1/32 scram-sha-256` and comment it out by adding a # to the beginning of the line and paste the following in a new line after it:

```
host all all 0.0.0.0/0 scram-sha-256

sudo nano /etc/postgresql/15/main/pg_hba.conf
#host all all 127.0.0.1/32 scram-sha-256
host all all 0.0.0.0/0 scram-sha-256
```

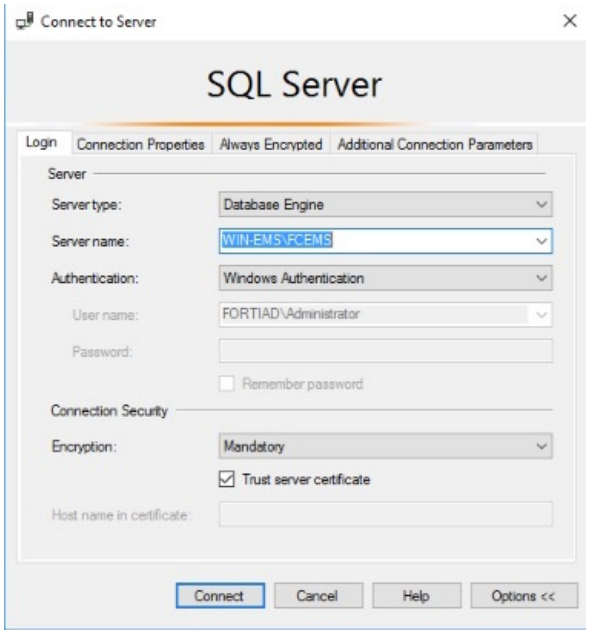
6. Restart the postgresql service:
`sudo systemctl restart postgresql`

To configure the Windows Server machine with the EMS instance to migrate:

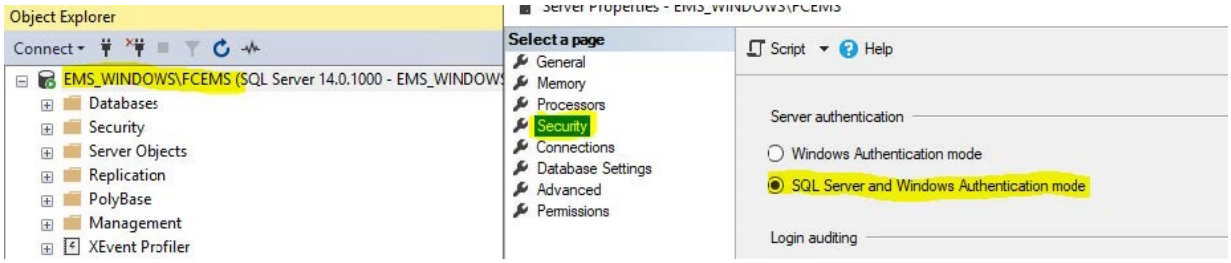
The Windows Server machine must have TLS 1.2 enabled for Client. In Registry Editor, confirm that the registry key [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client] is set to 1 or does not exist at all. Being enabled is the default behavior.

1. Create a user in SQL Server with the sysadmin role. You use this user to export the tables that contain EMS data:

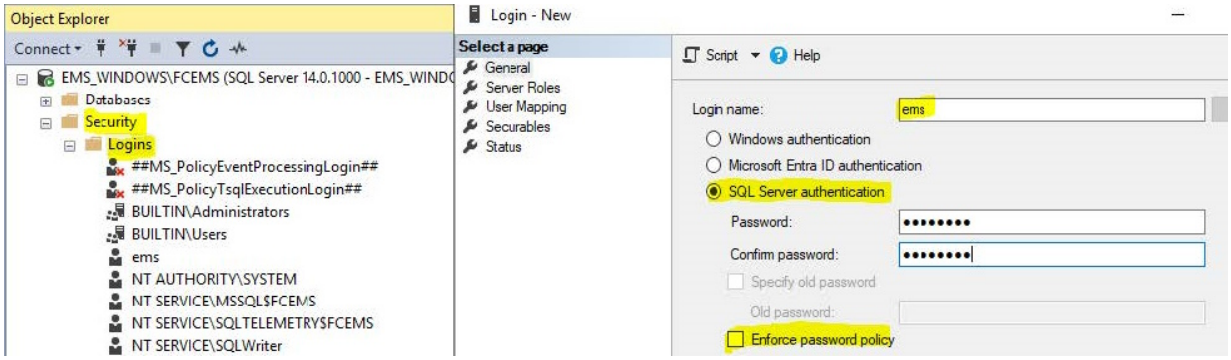
a. Log in to SQL Server Management Studio using Windows authentication. You may need to enable *Trust server certificate*.



b. In *Object Explorer*, right-click *FCEMS* and select *Properties*. Click *Security* and select *SQL Server and Windows Authentication mode*.



c. In *Object Explorer*, go to *Security* > *Logins*. Right-click and select *New login* > *General*.
d. In the *Login name* field, enter the desired login name. In this example, the login name is ems.
e. Select *SQL Server authentication*.
f. In the *Password* and *Confirm password* fields, enter the desired password.
g. Disable *Enforce password policy*. Save.



h. Go to *Server Roles*. Select *sysadmin*. Save.
i. Restart the SQL Server (FCEMS) service. The service name may differ. Check the given name during your remote SQL install.

2. If you have not enabled or installed PowerShell on the Windows Server, follow the steps in Get started with OpenSSH for Windows to install OpenSSH.
3. Generate a public key pair in PowerShell and copy it to the EMS Linux server home directory:
   a. In PowerShell, enter `ssh-keygen.exe -t rsa -b 4096`. For all subsequent prompts, press the `Enter` key. As the migration tool does not support encrypted private key files, leave the prompt empty and press `Enter` when you are prompted for a passphrase. A key pair is generated and saved to *C:\Users\Administrator\.ssh*.
   b. Enter `ssh test@172.16.1.22 mkdir -p .ssh`. In this example, 172.16.1.22 is the Linux server IP address:
   c. Enter the following command:
   ```
   cat C:\Users\Administrator\.ssh/id_rsa.pub | ssh test@172.16.1.22 'cat >> ~/.ssh/authorized_
   keys'
   ```
4. Download the migration tool from the Fortinet Support site and extract the files. The migration tool consists of an executable and a config file.
5. Open the config file in a text editor. The file consists of the following parameters:

Parameter	Value to configure
`[sqlserver]`	
`host`	SQL Server IP address. If you are using a local database (DB), enter 127.0.0.1.

Parameter	Value to configure
port	Microsoft SQL Server port.
user	User in SQL Server with sysadmin role. For an EMS with a local DB, you can leave this field blank.
password	Password for SQL user. For an EMS with a local DB, you can leave this field blank.
[postgresql]	
host	EMS Linux server IP address, as in this example the DB and EMS will be on the same Linux server.
port	Postgres port.
user	Postgres default username. For a standalone install or VM image, you can find this value by running the following command: `sudo cat /opt/forticlientems/pgbouncer/userlist.txt`
password	Postgres user password. For a standalone install or VM image, you can find this value by running the following command: `sudo cat /opt/forticlientems/pgbouncer/userlist.txt`
db_prefix	Target database prefix. This is used when the target database has any prefix. For example, if the target database includes db1001FCM and db1001FCM_Default databases, you could enter db1001 as the `db_prefix` value. You must leave this field blank for migration to VM images downloaded from the Fortinet support portal and for default standalone installations.
[linux_server]	
host	EMS Linux server IP address.
ssh_port	SSH port open in EMS Linux.
user	EMS Linux Server user (member of sudo, forticlientems, and www-data group).
password	EMS Linux Server user password.
key_file	Key file location in EMS Windows Server.



For a standalone install or VM image, you can find the values for `user` and `password` for `[postgresql]` by running the following command:

```
sudo cat /opt/forticlientems/pgbouncer/userlist.txt
```

The following shows an example:

```
[sqlserver]
host =172.16.1.3
port =1433
user =ems
password =Test123!
[postgresql]
host =172.16.1.22
port =5432
user =postgres
password =postgres
db_prefix =
[linux_server]
host =172.16.1.22
ssh_port =22
user =test
password =password#EMS Linux Servers user’s password
key_file = C:\Users\Administrator\.ssh\id_rsa#location of key file in EMS windows
[files]
# Copy a single file or a directory recursively to the remote server
# follow the pattern: file_or_folder_key = {'source' : '<file_souce>', 'target' : <file_
     target>'}
# multiple entries are allowed, file_or_folder_key is just a placeholder
# Examples:
# 1 - copying the installer directory recursively:
# installer_dir =
# {'source' : 'C:\\Program Files (x86)\\Fortinet\\FortiClientEMS\\Installers',
# 'target' : '/opt/forticlientems/data'}
# 2 - copying a specific file:
# signatures_file =
# {'source' : ''C:\\Program Files (x86)\\Fortinet
     \\FortiClientEMS\\signatures\\emsaval\\emsaval.dll',
# 'target' : '/opt/forticlientems/data/signatures/emsaval/emsaval.dll'}
```

6. Open an elevated PowerShell prompt inside the EMS Windows server and go to the directory where you extracted the migration tool. Run migration.exe:

   ```
   .\migration.exe
   ```

   If there are issues, check the migration log in the same folder as the migration tool.
7. After installation completes, check that all EMS services are running by entering the following command:

   ```
   systemctl --all --type=service | grep -E 'fcems|apache|redis|postgres'
   ```

```
root@emsnode2:/home/ems/Downloads# systemctl --all --type=service | grep -E 'fcems|apache|redis|postgres'
  apache2.service                                loaded    active   running The Apache HTTP Server
  fcems_adconnector.service                      loaded    active   running adconnector service
  fcems_addaemon.service                         loaded    active   running addaemon service
  fcems_adevtsrv.service                         loaded    active   running adevtsrv service
  fcems_adtask.service                           loaded    active   running adtask service
  fcems_chromebook.service                       loaded    active   running chromebook worker service
  fcems_das.service                              loaded    active   running das service
  fcems_dbop.service                             loaded    active   running dbop worker service
  fcems_deploy.service                           loaded    active   running deploy worker service
  fcems_ecsocksrv.service                        loaded    active   running ecsocksrv service
  fcems_forensics.service                        loaded    active   running forensics worker service
  fcems_ftntdbimporter.service                   loaded    active   running FTNT DB importer worker service
  fcems_installer.service                        loaded    active   running installer worker service
  fcems_ka.service                               loaded    active   running kaworker service
  fcems_mdmproxy.service                         loaded    active   running MDM proxy service
  fcems_monitor.service                          loaded    active   running monitor worker service
  fcems_notify.service                           loaded    active   running FOS notify service
  fcems_pgbouncer.service                        loaded    active   running pgBouncer for EMS service
  fcems_probe.service                            loaded    active   running probeworker service
  fcems_reg.service                              loaded    active   running regworker service
  fcems_scep.service                             loaded    active   running SCEP service
  fcems_sip.service                              loaded    active   running software inventory processor service
  fcems_tag.service                              loaded    active   running tagworker service
  fcems_task.service                             loaded    active   running taskworker service
  fcems_update.service                           loaded    active   running update worker service
  fcems_upload.service                           loaded    active   running upload worker service
  fcems_wspgbouncer.service                      loaded    active   running pgBouncer for EMS WebServer service
  fcems_ztna.service                             loaded    active   running ztna worker service
  postgresql.service                             loaded    active   exited  PostgreSQL RDBMS
  postgresql@15-main.service                     loaded    active   running PostgreSQL Cluster 15-main
  redis-server.service                           loaded    active   running Advanced key-value store
```

The output shows that postgresql.service status displays as `exited`. This is the expected status. EMS does not create this service, which only exists to pass commands to version-specific Postgres services. It displays as part of the output as the command filters for all services that contain "postgres" in the name.

8. Access the EMS GUI on the Linux server and verify that all configurations and data from the EMS Windows Server were migrated.

To migrate FortiClient endpoints to Linux EMS:

After EMS migration completes, do one of the following to migrate FortiClient endpoints to Linux EMS:

Method	Description
Update DNS record with Linux EMS IP address (recommended)	On the DNS server, update the DNS record for EMS with the Linux EMS IP address. FortiClient endpoints that were previously connected to Windows Server EMS resolve the new IP address to the EMS FQDN and connect to the Linux EMS. This is the recommended method to migrate FortiClient endpoints to Linux EMS. The endpoint automatically connects to Linux EMS. Even if user verification is enabled, the migration is seamless and the user does not notice any changes on the endpoint.
Switch EMS	1. On the Windows Server EMS, go to *Endpoints > All Endpoints*. 2. Select the desired endpoints. 3. Select *Action > Switch EMS > Switch by IP/Switch by Invitation*. 4. Enter the Linux EMS IP address, FQDN, or invitation. Selected endpoints connect to the Linux EMS. 5. If user verification is enabled, the user onboarding popup for the new

Method	Description
	invitation displays on the endpoint. The user must verify their identity to connect to Linux EMS.
Configure EMS server list on Windows Server EMS	This method only works if user verification is not enforced and FortiClient connects to EMS using an FQDN or IP address. 1. On the Windows Server EMS, go to *System Settings > EMS Settings*. 2. Enable *Configure EMS server list*. 3. Add the Linux EMS IP address or FQDN and port number. 4. Click *Save*. 5. After the endpoint receives the configuration changes, disconnect or shut down the EMS Windows Server. In the next keepalive interval, FortiClient connects to Linux EMS.

After migration, the license remains active on Windows Server EMS.

To complete post-migration:

When initially configuring the EMS Linux machine, if not using Docker, you updated `/etc/postgresql/15/main/postgresql.conf` to listen on all addresses and updated `/etc/postgresql/15/main/pg_hba.conf` to allow remote access to Postgres. Revert these changes to ensure optimal security settings.

Installation

The following topics provide instructions for installing EMS 7.4.3. You can install EMS in various scenarios, such as high availability (HA), with a remote database (DB), and so on. Select the appropriate installation scenario for your environment:

Install scenario	Description
Standalone install	
Installing EMS in standalone mode on page 54	Install EMS in standalone mode with a local DB on an Ubuntu machine.
Deployment as a virtual machine (VM) image	
Deploying EMS as a VM image on page 55	Deploy EMS as a VM image like many other Fortinet products. EMS supports various hypervisors, including VMware ESXi, KVM, Microsoft Hyper-V, and Oracle VirtualBox hypervisors.
Install with a PostgreSQL (Postgres) DB	
Installing EMS with Postgres in Docker on page 69	Install EMS to use a Postgres database in Docker. You can install the Postgres DB on the same machine as EMS or on a remote machine.
Installing EMS with standalone remote database without Docker on page 72	Install EMS to use a Postgres DB that is installed on a remote Ubuntu machine. This install does not use Docker for the Postgres DB.

Install scenario	Description
HA	
Installing EMS HA with standalone remote DB without Docker on page 76	Install EMS in an HA configuration with the Postgres DB installed on a remote Ubuntu machine. This install does not use Docker and uses three Ubuntu machines: two for the EMS HA nodes and one for the Postgres DB.
Installing EMS HA with Postgres HA using Bitnami Docker on page 83	Install EMS in an HA configuration with the Postgres DB also in an HA configuration using Bitnami Docker. This install uses four Ubuntu machines: two for the EMS HA nodes and two for the Postgres DB nodes.
Installing EMS HA with native Postgres HA without Docker on page 90	Install EMS in an HA configuration with the Postgres DB also in an HA configuration without using Docker. This install uses at least five servers: two for the EMS HA nodes and at least three for the Postgres DB nodes and witness node.
Installing EMS for HA georedundancy on page 108	Install EMS nodes in a geographically distant HA cluster. Each datacenter also includes PostgreSQL external DBs. The setup of a geographically distributed infrastructure allows you to ensure redundancy in case of failure on a datacenter.

Installing EMS in standalone mode

The following provides instructions for installing EMS in standalone mode with a local database (DB) and assumes that you have a machine with Ubuntu installed. You can install EMS in other scenarios, such as high availability, with a remote DB, and so on. See Installation on page 53.

To install standalone EMS:

1. Download the forticlientems_7.4.3.XXXX.arm64.bin or forticlientems_7.4.3.XXXX.amd64.bin file from the Fortinet Support site.
2. Run `sudo -i` to log in to the shell with root privileges.
3. Change permissions and add execute permissions to the installation file:
   `chmod +x forticlientems_7.4.3.XXXX.XXX64.bin`
   ```
   root@emsnode2:/home/ems/Downloads# chmod +x forticlientems_7.4.0.1745.bin
   ```
4. Set `umask` to 022 if the existing `umask` setting is more restrictive.
5. Run the following command to install EMS:
   `./forticlientems_7.4.3.XXXX.XXX64.bin -- --allowed_hosts '*' --enable_remote_https`
   Run the installer to and from any directory other than `/tmp`. Running the installer to or from `/tmp` causes issues.
6. After installation completes, check that all EMS services are running by entering the following command:

   ```
   systemctl --all --type=service | grep -E 'fcems|apache|redis|postgres'
   ```

```
root@emsnode2:/home/ems/Downloads# systemctl --all --type=service | grep -E 'fcems|apache|redis|postgres'
  apache2.service                                loaded    active   running The Apache HTTP Server
  fcems_adconnector.service                      loaded    active   running adconnector service
  fcems_addaemon.service                         loaded    active   running addaemon service
  fcems_adevtsrv.service                         loaded    active   running adevtsrv service
  fcems_adtask.service                           loaded    active   running adtask service
  fcems_chromebook.service                       loaded    active   running chromebook worker service
  fcems_das.service                              loaded    active   running das service
  fcems_dbop.service                             loaded    active   running dbop worker service
  fcems_deploy.service                           loaded    active   running deploy worker service
  fcems_ecsocksrv.service                        loaded    active   running ecsocksrv service
  fcems_forensics.service                        loaded    active   running forensics worker service
  fcems_ftntdbimporter.service                   loaded    active   running FTNT DB importer worker service
  fcems_installer.service                        loaded    active   running installer worker service
  fcems_ka.service                               loaded    active   running kaworker service
  fcems_mdmproxy.service                         loaded    active   running MDM proxy service
  fcems_monitor.service                          loaded    active   running monitor worker service
  fcems_notify.service                           loaded    active   running FOS notify service
  fcems_pgbouncer.service                        loaded    active   running pgBouncer for EMS service
  fcems_probe.service                            loaded    active   running probeworker service
  fcems_reg.service                              loaded    active   running regworker service
  fcems_scep.service                             loaded    active   running SCEP service
  fcems_sip.service                              loaded    active   running software inventory processor service
  fcems_tag.service                              loaded    active   running tagworker service
  fcems_task.service                             loaded    active   running taskworker service
  fcems_update.service                           loaded    active   running update worker service
  fcems_upload.service                           loaded    active   running upload worker service
  fcems_wspgbouncer.service                      loaded    active   running pgBouncer for EMS WebServer service
  fcems_ztna.service                             loaded    active   running ztna worker service
  postgresql.service                             loaded    active   exited  PostgreSQL RDBMS
  postgresql@15-main.service                     loaded    active   running PostgreSQL Cluster 15-main
  redis-server.service                           loaded    active   running Advanced key-value store
```

The output shows that postgresql.service status displays as `exited`. This is the expected status. EMS does not create this service, which only exists to pass commands to version-specific Postgres services. It displays as part of the output as the command filters for all services that contain "postgres" in the name.

7. Access the EMS GUI and log in.
8. If after initially installing EMS 7.4.3 you need to upgrade to a newer build, repeat the process with the new installation file.

Deploying EMS as a VM image

You can deploy EMS as a virtual machine (VM) image on VMware ESXi, KVM, Microsoft Hyper-V, and Oracle VirtualBox hypervisors. EMS provides Ubuntu-based VM images for x86_64 and ARM architectures. However, regular OS maintenance is still required.

The VM image include some OS hardening modifications as follows:

- Unneeded users are removed:
  - games
  - man
  - news
  - uucp
  - proxy
  - backup
  - list
  - irc
  - gnats
  - uuidd

    - mail
    - lp
    - nobody
    - tss
    - landscape
    - fwupd-efresh
    - usbmux
    - lxd
- The forticlientems user, which runs EMS processes, has no login.
- Only the ems user has SSH access.
- Firewall is enabled and only the following ports are enabled by default:

TCP port	Usage
22	SSH access to EMS VM or server
4001	Send zero trust network access certificates to mobile device management endpoints
8013	Telemetry
8015	Send updates to FortiOS
8443	Provision profiles to Chromebooks
8871	Connection to remote Active Directory connector
• 80 • 443 • 10443 • 9443	EMS GUI and APIs

- On first login, EMS requires changing the password for the ems user.

EMS VMs run in standalone mode.

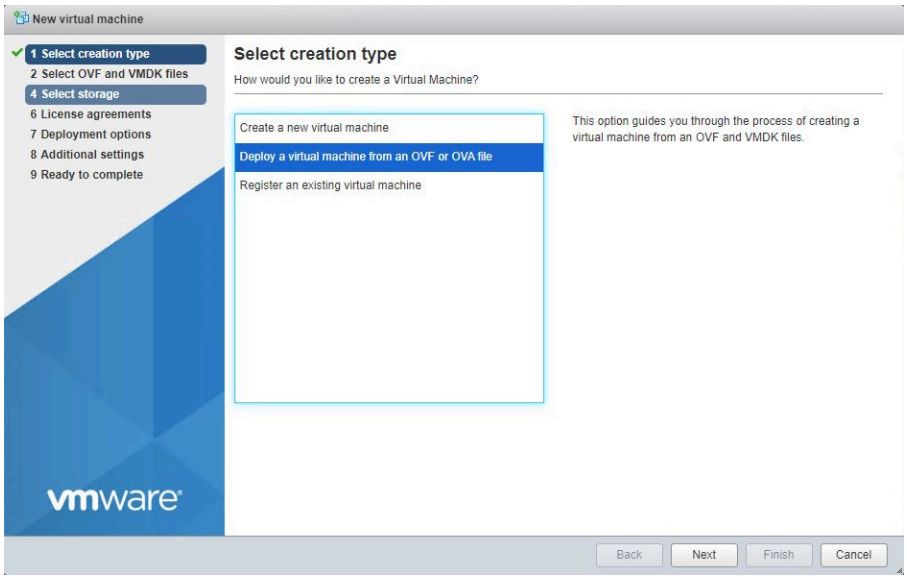
This topic contains instructions for deploying EMS as a VM as follows:

- VMware ESXi on page 56
- KVM on page 58
- Proxmox on page 59
- Hyper-V on page 64
- VirtualBox on page 65
- ARM processor on page 67
- Configuring the VM IP address by modifying Netplan configuration files on page 68

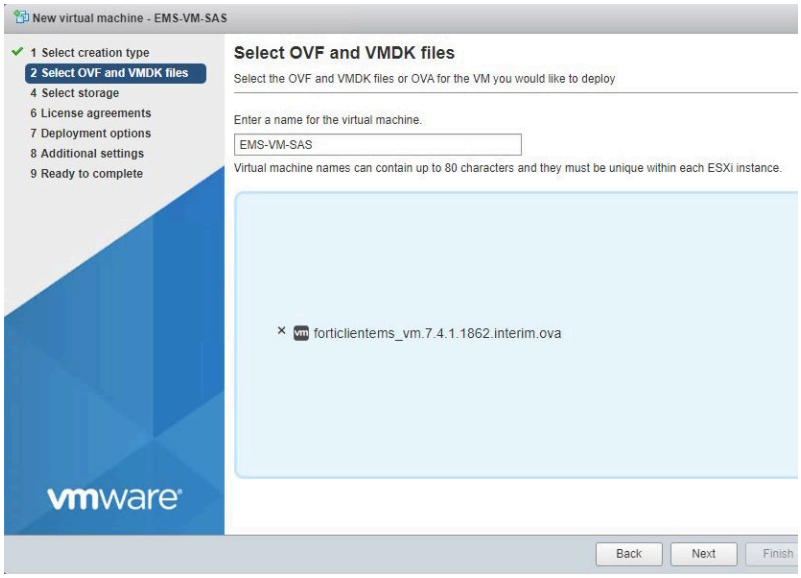
VMware ESXi

To deploy EMS on VMware ESXi:

1. Click *Create/Register VM*.
2. Select *Deploy a virtual machine from an OVF or OVA file*. Click *Next*.



3. Enter the VM name and upload the OVA file. Click *Next*.



4. Configure the VM.
5. Click *Finish*.
6. Review the configuration and start the VM. When the VM boot completes, the OS logon page displays.
7. Log in to the VM. The default credentials are:
   - Username: `ems`
   - Password: `ems`

   EMS requires you to change these credentials upon first login.
8. Change the default password when prompted.
9. Access the EMS GUI using the VM IP address or FQDN. See Starting FortiClient EMS and logging in on page 113.

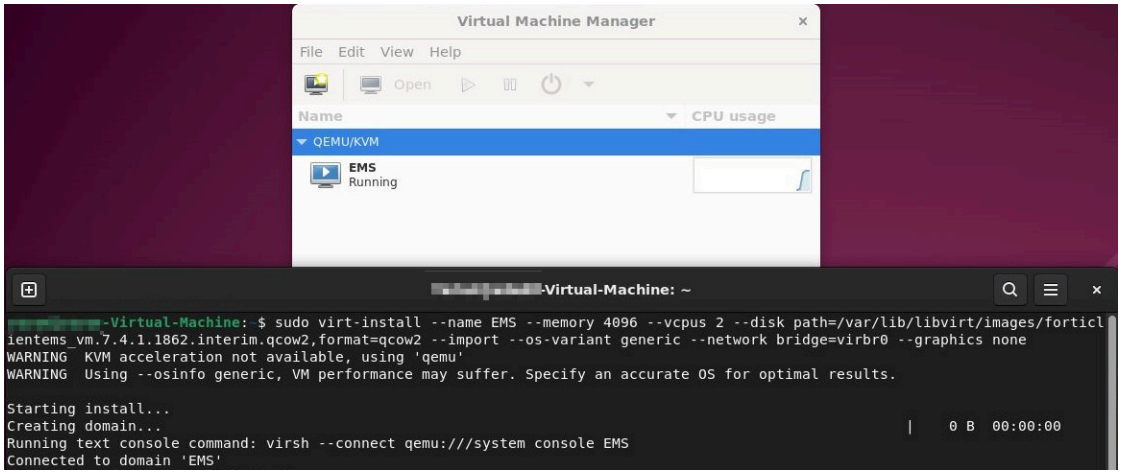
KVM

To deploy EMS on KVM:

1. Set up QEMU or KVM on a Linux host.
2. Copy the `forticlientems_vm qcow2` image under `/var/lib/libvirt/images/`.
3. Run the following command to initialize the virtual machine with the FortiClient EMS image:

```
sudo virt-install --name EMS_VM --memory 4096 --vcpus 2 --disk
path=/var/lib/libvirt/images/forticlientems_vm.7.4.3.XXXX.interim.qcow2,format=qcow2 --import
--os-variant generic --network bridge=virbr0 --graphics none
```

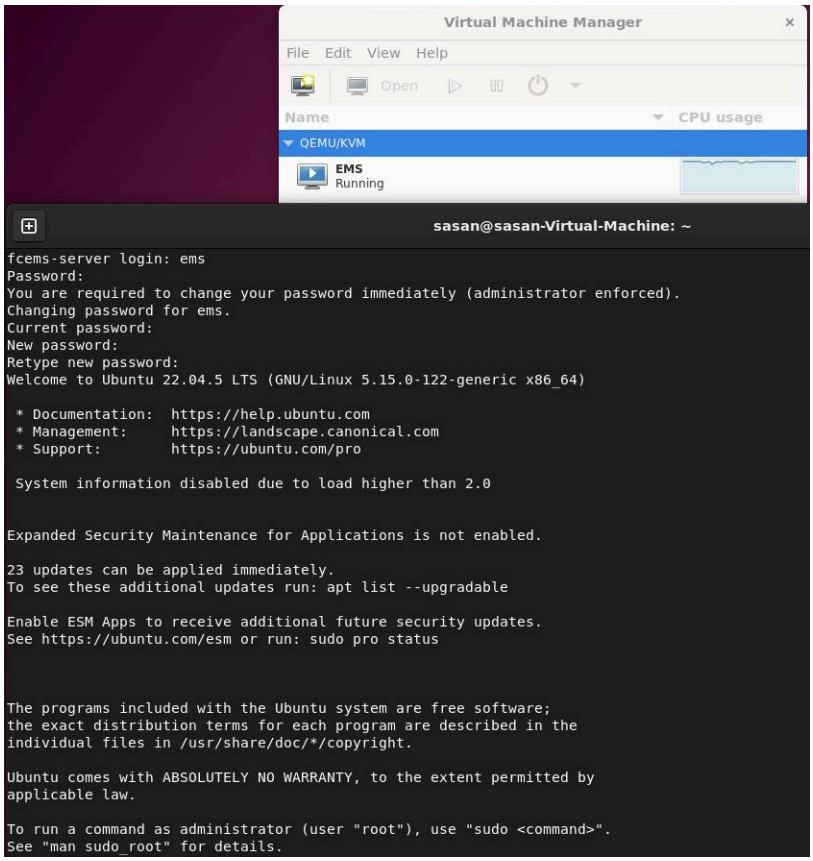
You can change the configuration in the command as needed.



4. Log in to the VM.

The default credentials are:

- Username: `ems`
- Password: `ems`



5. Access the EMS GUI using the VM IP address or FQDN. See Starting FortiClient EMS and logging in on page 113.

Proxmox

To deploy EMS on Proxmox:

1. Download the EMS KVM image files and copy them to Proxmox:
   a. Log in to the Fortinet Support Portal and select *Support > Firmware Download* from the top menu.
   b. From the *Select Product* dropdown list, select *FortiClientEMS*.
   c. On the *Download* tab, go to *v.700 > 7.4 > 7.4.3*.
   d. Download the qcow2.zip file and extract it.
   e. Copy forticlientems_vm.7.4.3.XXXX.qcow2 onto a Proxmox node. Typically, you can use the secure copy protocol (SCP). The following shows an example of using `scp forticlientems_vm.7.4.3.XXXX.qcow2 root@proxmox.test.local:/root/ forticlientems_vm.7.4.3.XXXX.qcow2` to copy the forticlientems_vm.7.4.3.XXXX.qcow2 file to the Proxmox node at proxmox.test.local. Edit the node address, which may be an IP address or FQDN, to match your Proxmox environment. The example also assumes that you are running the command as the root user and copying the file to the root user home directory at `/root`:

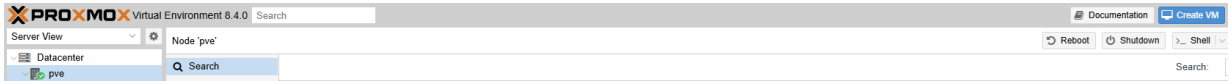
```
C:\Users\adm\Downloads\forticlientems_vm.7.4.3.XXXX.qcow2>scp forticlientems_
vm.7.4.3.XXXX.qcow2 root@proxmox.test.local:/root/forticlientems_vm.7.4.3.XXXX.qcow2
root@192.168.1.2's password:
```

```
forticlientems_vm.7.4.3.XXXX.qcow2                                    11%
1134MB  89.8MB/s   01:35 ETA
```



You can get a qcow2 image onto a Proxmox node in various ways. The example uses SCP on the command line. You can use a GUI SCP client, such as WinSCP on Windows or ForkLift on macOS. If you have file transfer protocol set up on your Proxmox node, you can use that as well. Use the method that you are comfortable with.

2. Deploy the EMS VM into Proxmox:
   a. In the Proxmox GUI, select the node you copied the EMS image to and click *Create VM*.

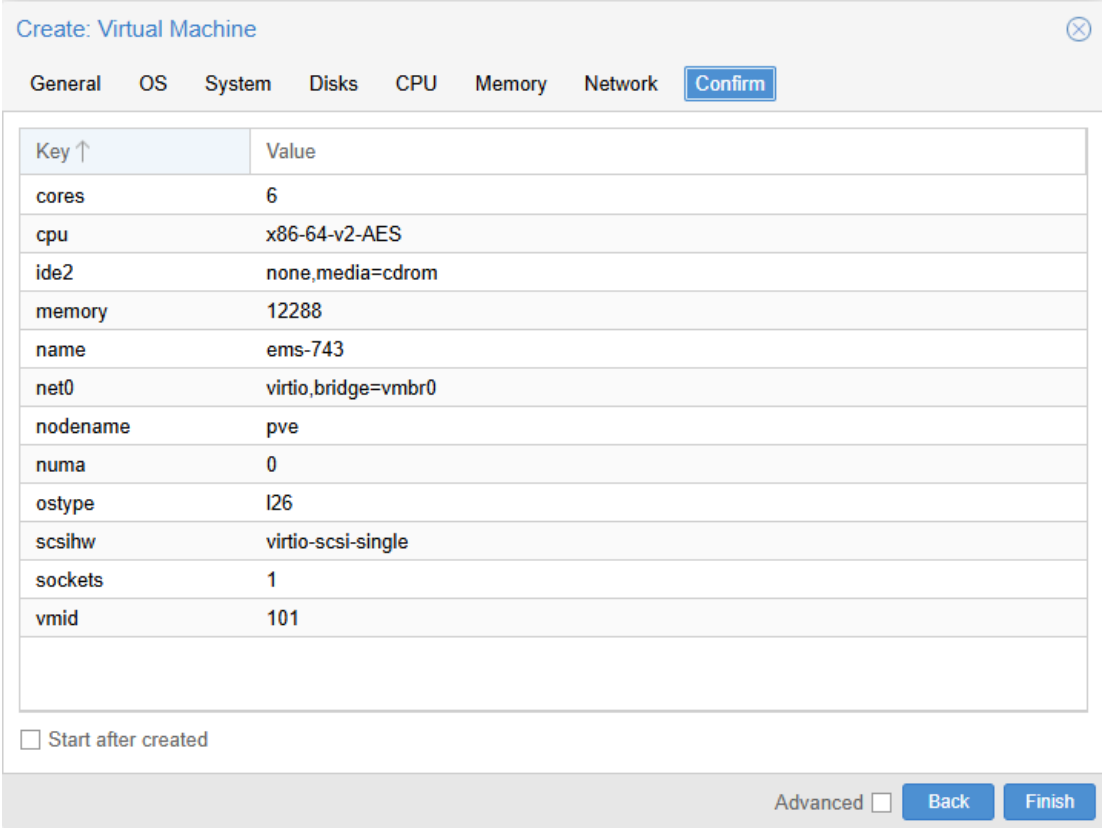


   b. In the *Create: Virtual Machine dialog*, change the *VM ID* value if desired. Note this ID value as you use it later. In the *Name* field, give the VM a useful name. Click *Next*.



You may find it useful to add the EMS version number to the end of your VM name.

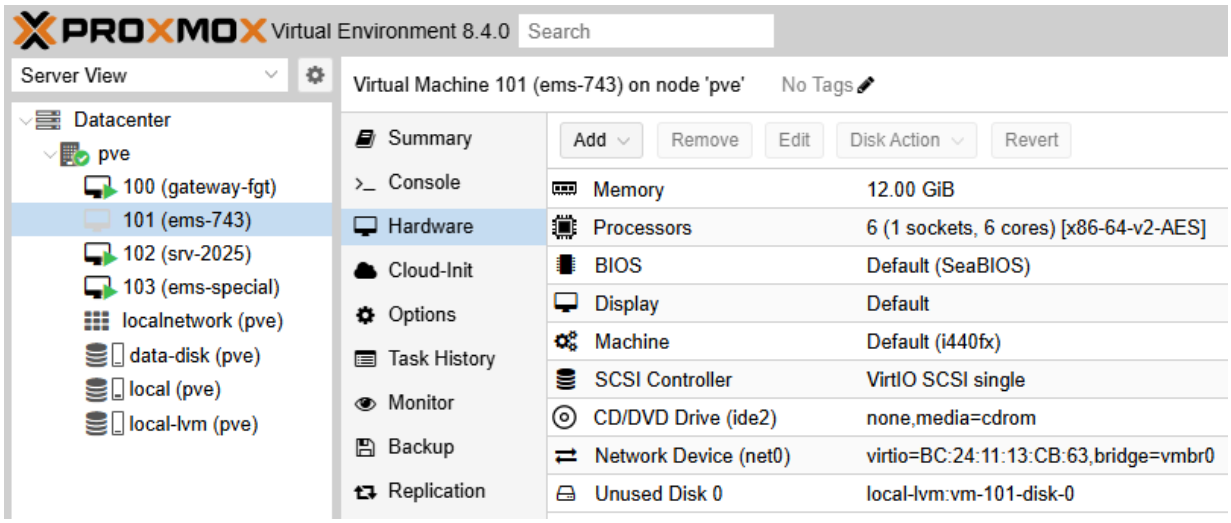
   c. In the *OS* tab, select *Do not use any media*. Leave *Type* and *Version* at their defaults of *Linux* and *6.x - 2.6 Kernel*, respectively. Click *Next*.
   d. In the *System* tab, leave the default values and click *Next*.
   e. In the *Disks* tab, by default, you see an entry for one SCSI disk named *scsi0*. Click the trashcan icon to delete this disk. You see *No Disks* displayed. Click *Next*.
   f. Set the *CPU* and *RAM* tab values per the minimum EMS system requirements. See Management capacity on page 33.
   g. In the *Network* tab, deselect *Firewall* and leave the rest of the options at their defaults. Click *Next*.
   h. In the *Confirm* tab, ensure *Start after created* is not selected. Note the *vmid* value as you use it later. Click *Finish* to build the VM.



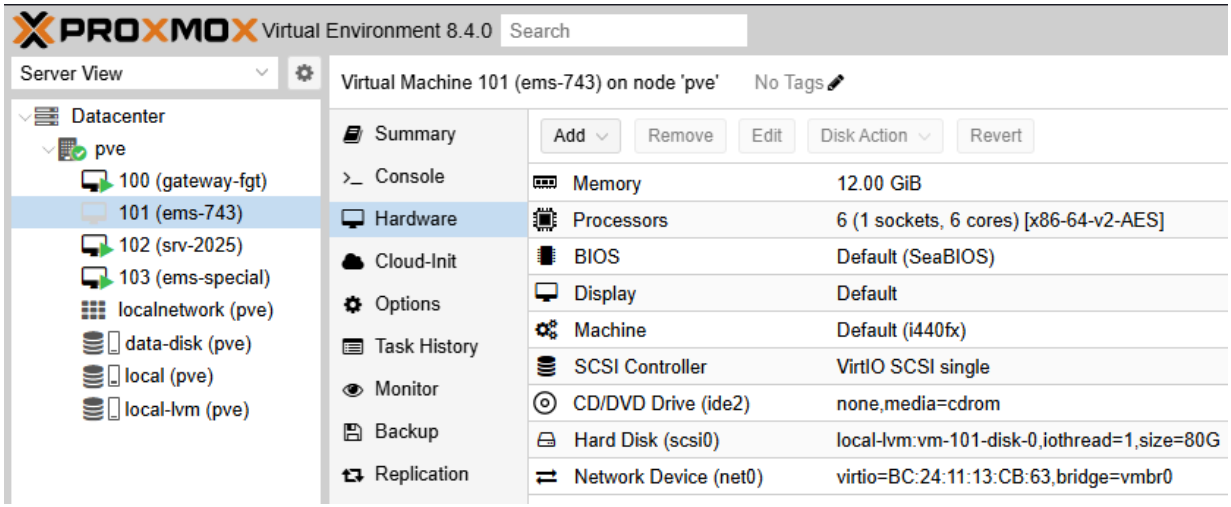
3. Import the qcow2 image into the EMS VM:
   a. After some seconds, you see the new VM in the left sidebar with the configured VM ID and name. Select the newly created VM and click *Hardware* in the middle pane. Note the presence of one network interface named *net0* and the lack of disks.
   b. Select the Proxmox node in the left sidebar and click *Shell* entry in the middle pane. After the shell appears, type `pwd` to ensure you are in the `/root` folder and then type `ls` to display the directory contents. You see the `forticlientems.qcow2` image file copied over earlier.
   c. To import the forticlientems_vm.7.4.3.XXXX.qcow2 image into your newly created VM, use the `qm disk import` command: `qm disk import <vmid> forticlientems_vm.7.4.3.XXXX.qcow2 <storage device name>`. You must adjust the command to match your configured VM ID and the storage device name of choice. By default, Proxmox creates a local and local-lvm storage device when it is installed. The example uses a VM ID of 101 and the local-lvm storage device. Note the disk name when the command finishes. In the example, the disk name is `local-lvm:vm-101-disk-0'`. See the following example:

```
root@pve:~# qm disk import 101 forticlientems_vm.7.4.3.1926.qcow2 local-lvm
importing disk 'forticlientems_vm.7.4.3.1926.qcow2' to VM 101 ...
  Logical volume "vm-101-disk-0" created.
transferred 0.0 B of 80.0 GiB (0.00%)
transferred 827.4 MiB of 80.0 GiB (1.01%)
[…]
transferred 80.0 GiB of 80.0 GiB (100.00%)
unused0: successfully imported disk 'local-lvm:vm-101-disk-0'
```

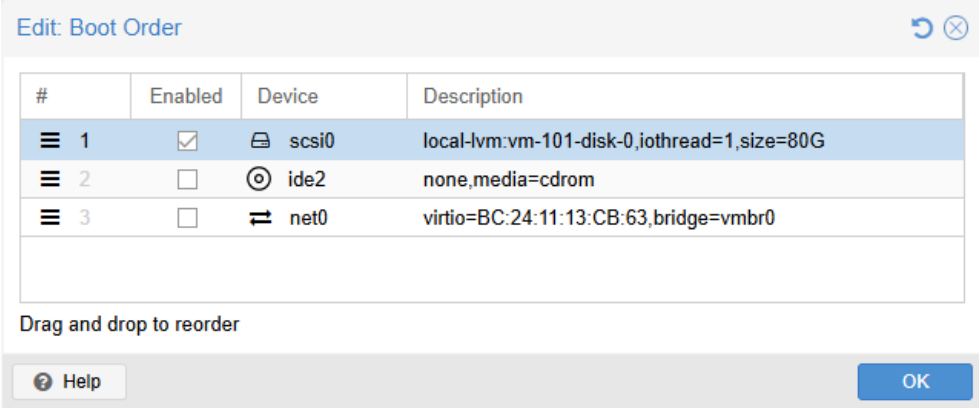
   d. Select the EMS VM in the left sidebar and click *Hardware* in the middle pane. Note the newly imported disk. At this point, it shows as *Unused Disk 0*.



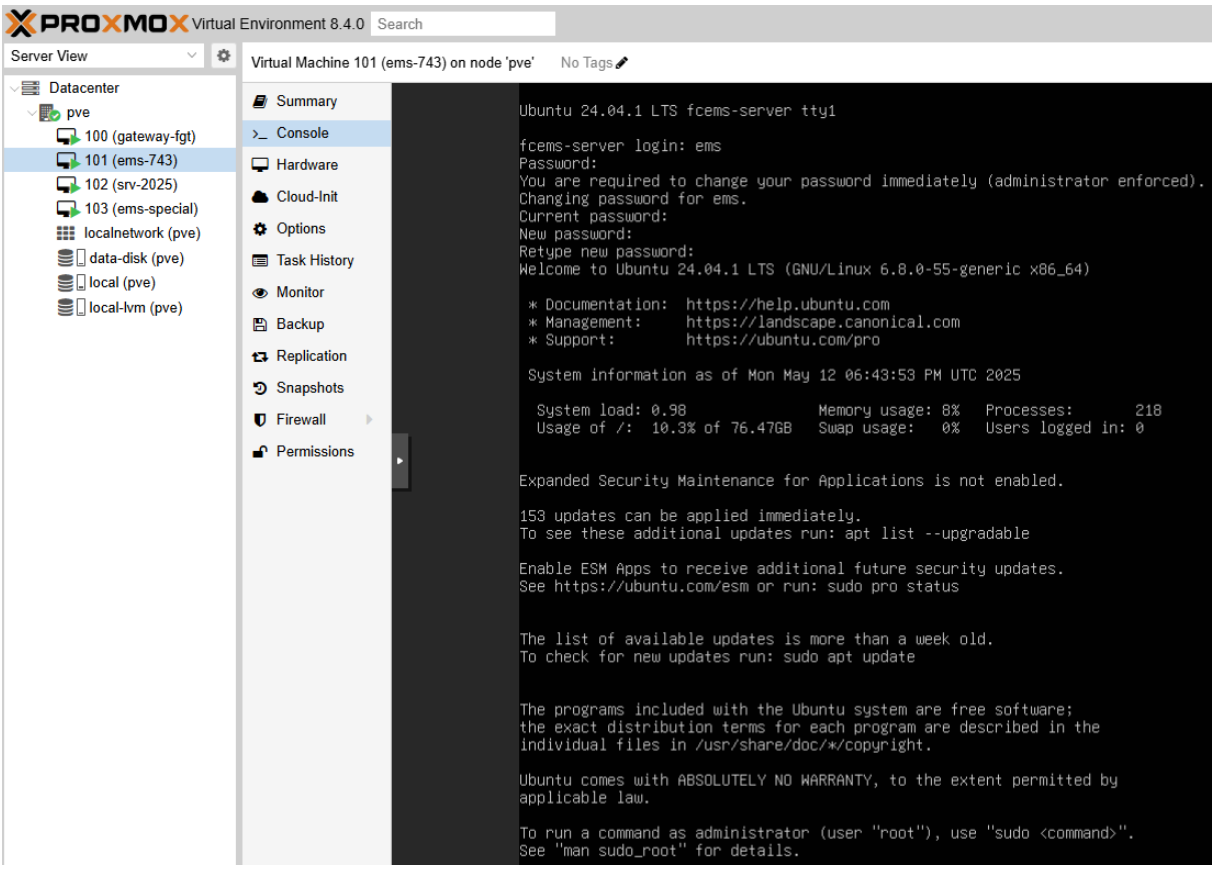
4. Add a boot disk to the EMS VM:
   a. Select *Unused Disk 0* and click *Edit*.
   b. The *Add: Unused Disk* dialog appears. Accept the defaults and click *Add*. Note the newly added *Hard Disk (scsi0)* is now mapped to the local-lvm:vm-107-disk-0 created earlier.



5. Verify the boot order:
   a. To verify the boot order, select the EMS VM in the left sidebar and click *Options* in the middle pane. Select *Boot Order* and click *Edit*. Alternately, you can double-click *Boot Order*.
   b. The *Edit: Boot Order* dialog appears. Use the selector icons to drag and drop *scsi0* to the top of the list and ensure *Enabled* for that entry is selected.



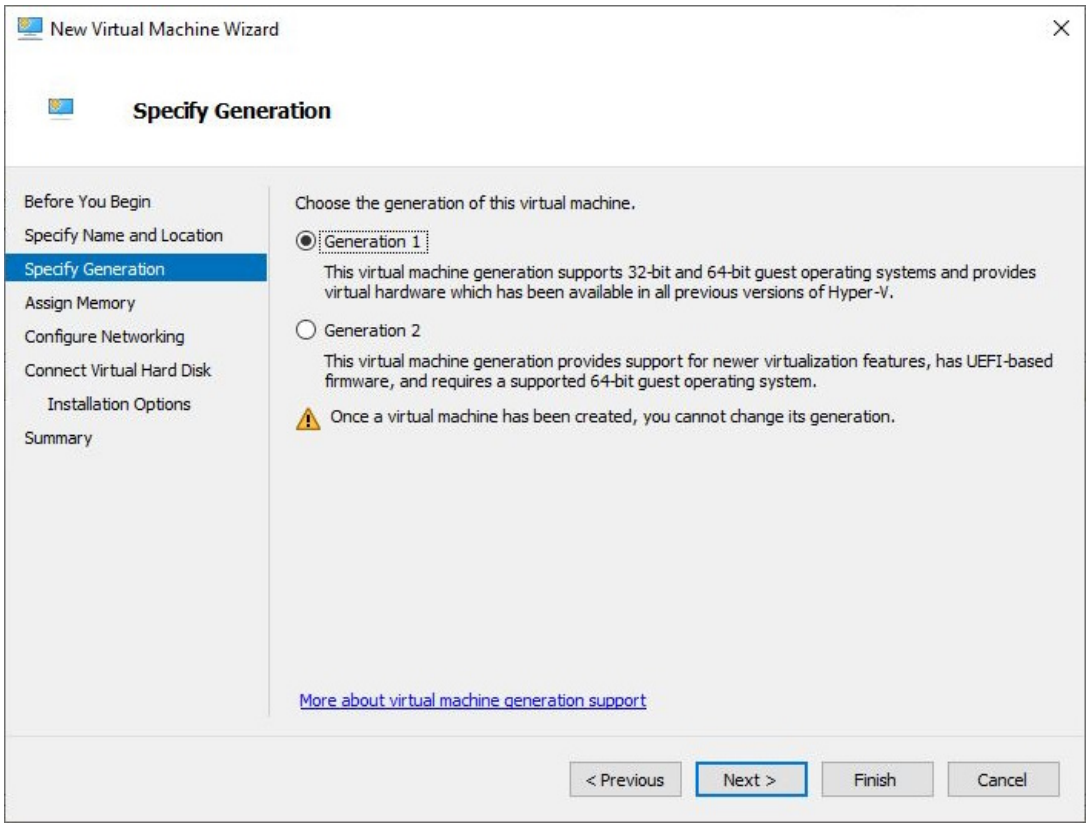
6. Select the EMS VM in the left sidebar and select *Console* in the middle pane. Click *Start* at the top or *Start Now* in the middle of the console.
7. The EMS VM starts to boot. After the reboot, the standard EMS login prompt displays. Log in with a username of ems and password ems. You are prompted to change the password and presented with the EMS shell prompt.



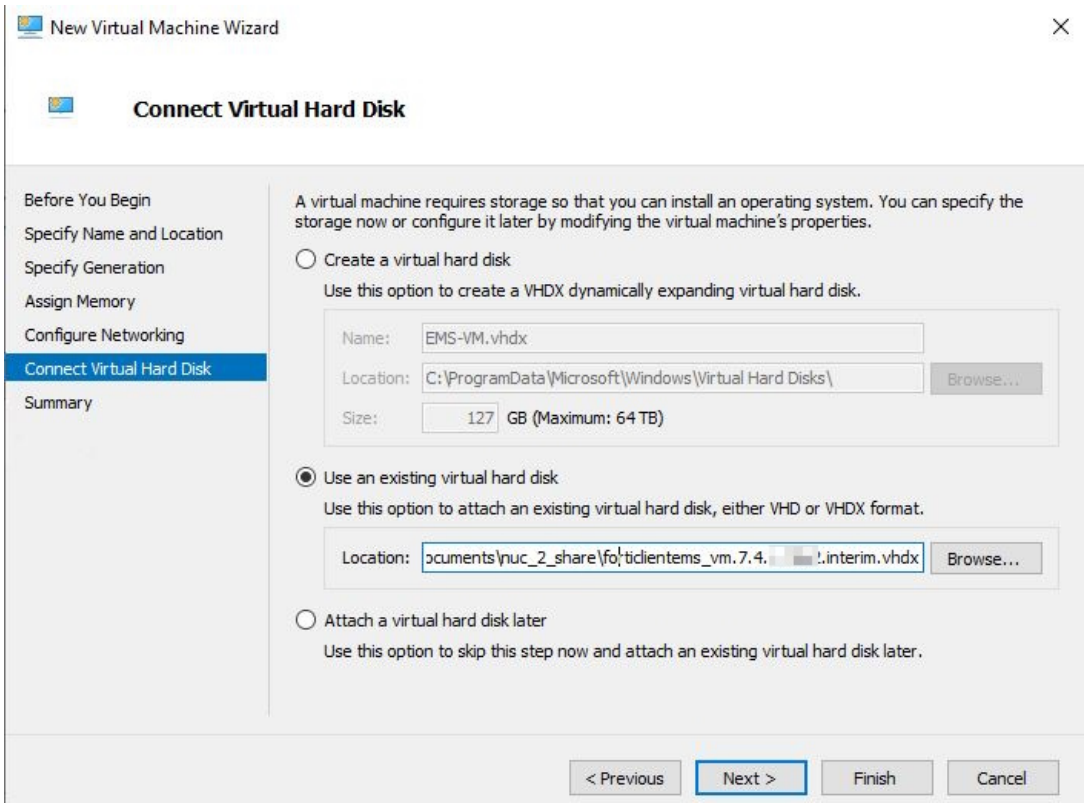
Hyper-V

To deploy EMS on Hyper-V:

1. Open the new VM wizard and define a name for the VM. Click *Next*.
2. In *Specify Generation*, select *Generation 1*. Click *Next*.



3. In *Assign Memory*, configure the required and memory settings.
4. In *Connect Virtual Hard Disk*, select *Use an existing virtual hard disk*. In *Location*, browse to and select the forticlientems_vm.7.4.3.XXXX.vhdx file. Click *Finish*. If desired, you can edit the configuration after the VM is created, such as modifying the number of virtual processors.

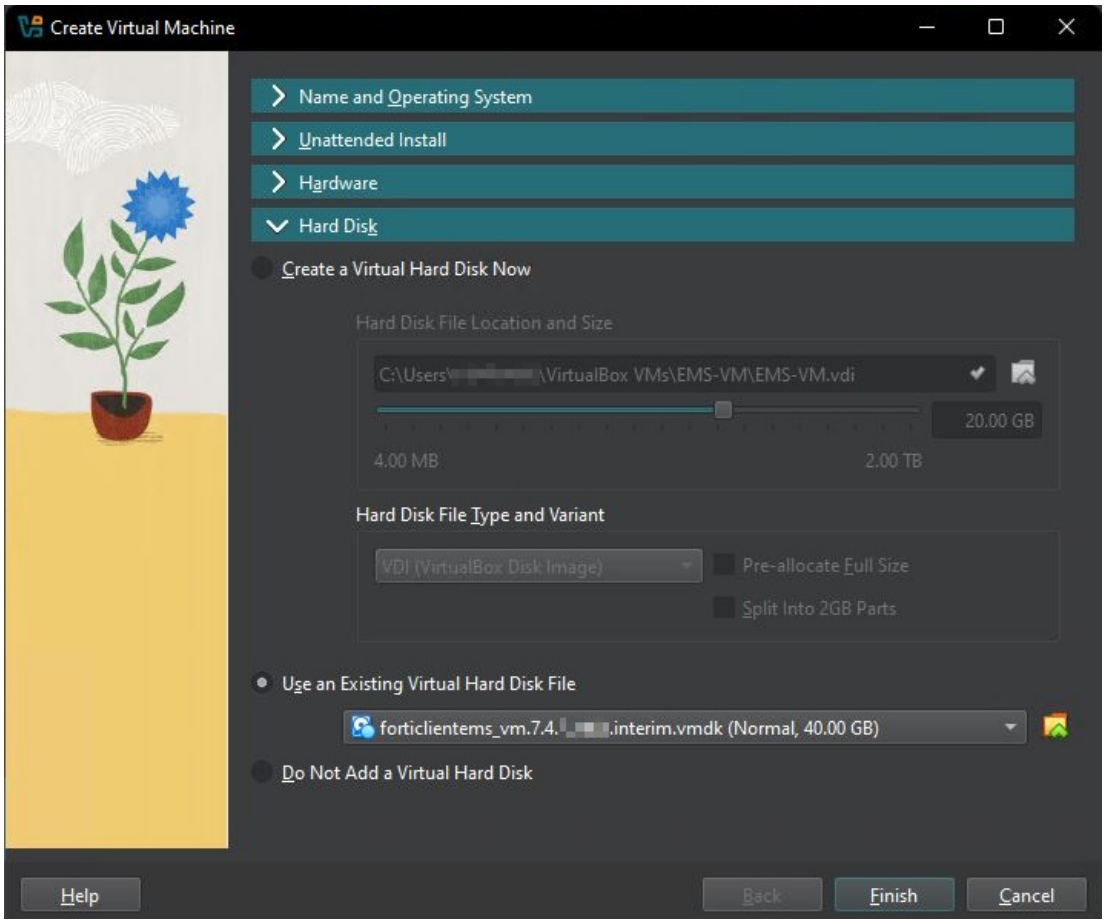


5. Start the VM.
6. After bootup, log in using the default credentials:
   - Username: ems
   - Password: ems

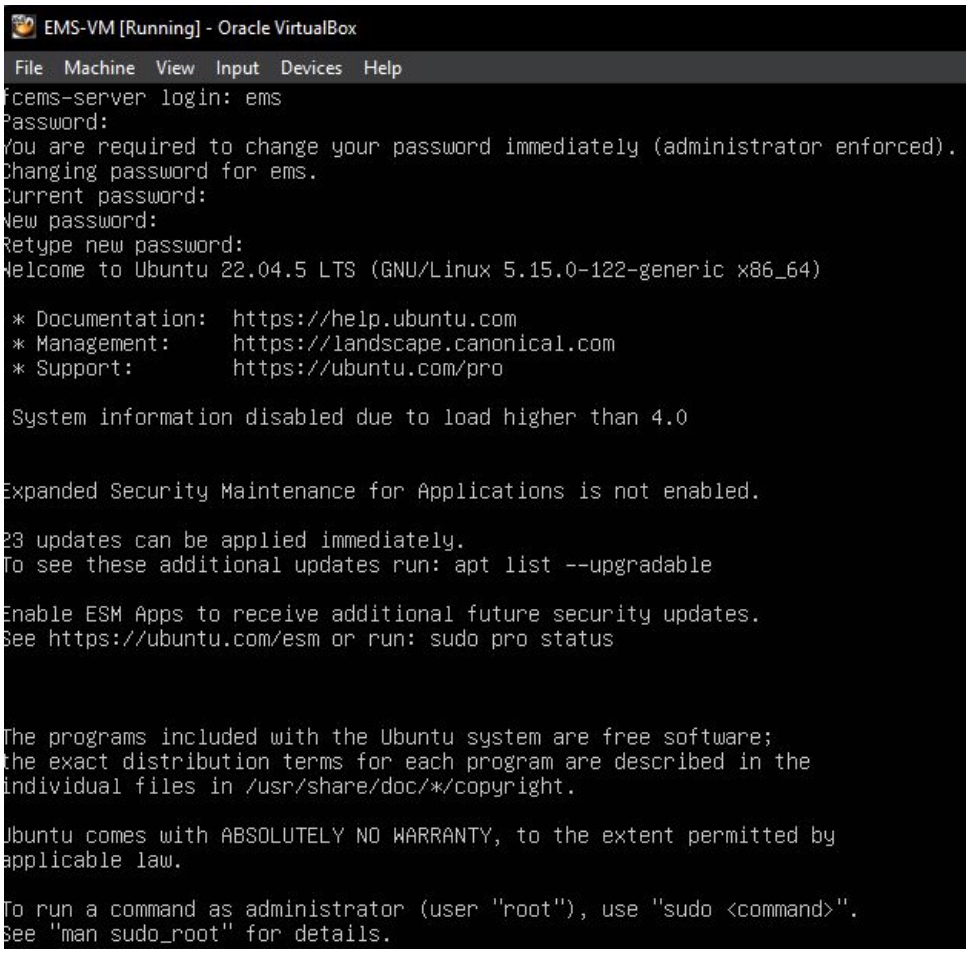
VirtualBox

To deploy EMS on VirtualBox:

1. Open the new VM wizard and define a name for the VM. Click *Next*.
2. In *Hardware*, configure the required hardware settings.
3. In *Hard Disk*, select *Use an Existing Virtual Hard Disk File*. Browse to and select the forticlientems_vm.7.4.3.XXXX.vmdk file. Click *Finish*. If desired, you can edit the configuration after the VM is created, such as modifying the number of virtual processors.



4. Start the VM.
5. After bootup, log in using the default credentials:
   - Username: ems
   - Password: ems



ARM processor

To install FortiClient EMS on ARM processor:

1. Download the ARM EMS installer from the support portal. The installer file name is in the form *forticlientems_7.4.1.1867.interim.arm64.bin*.
2. Make the installer executable:

```
sudo chmod +x ./forticlientems_7.4.1.1867.interim.arm64.bin
```

3. Run the installer:

```
sudo ./forticlientems_7.4.1.1867.interim.arm64.bin
```

4. Access the EMS GUI using the VM IP address or FQDN. See Starting FortiClient EMS and logging in on page 113.

After deploying EMS as a VM, you may want to configure the IP address on the VM. You can modify the Netplan configuration files to do so.

Configuring the VM IP address by modifying Netplan configuration files

To configure the VM IP address by modifying Netplan configuration files:

1. On the VM, locate the Netplan configuration files. Ubuntu stores Netplan configuration files in `/etc/netplan`. The files typically have a .yaml extension, such as 01-netcfg.yaml or 50-cloud-init.yaml. Run the following to list the files:

```
ls /etc/netplan/
```

2. Use a text editor such as nano or vim to open the yaml file for editing:

```
sudo nano /etc/netplan/01-netcfg.yaml
```

3. In the yaml file, find the section for your desired network interface. Do one of the following:
   - If you are using a static IP address, modify the file, setting `addresses` with your desired static IP address and subnet mask. Update the IP address under `routes: - to: default via:` with your desired gateway, and modify `nameservers` as needed. The following provides an example configuration where the static IP address is 192.168.1.100/24:

```
network:
    version: 2
    renderer: networkd
    ethernets:
        enp3s0:
            addresses:
                - 192.168.1.100/24
            nameservers:
                addresses: [8.8.8.8, 1.1.1.1]
            routes:
                - to: default
                  via: 192.168.1.1
```

   - If you are using DHCP, ensure that `dhcp4` is set to `yes`. The following provides an example configuration:

```
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      dhcp4: yes
```

4. Before applying the changes permanently, run the following to test the configuration. This command temporarily applies the configuration and gives you 120 seconds to confirm the changes. If the configuration does not work, it rolls back automatically.

```
sudo netplan try
```

5. If the test succeeds, apply the changes permanently:

```
sudo netplan apply
```

6. To verify the configuration, check that the VM IP address is updated as you configured:

```
ip addr show
```

Installing EMS with Postgres in Docker

You can install PostgreSQL (Postgres) in Docker on the same machine as EMS or on a remote machine.

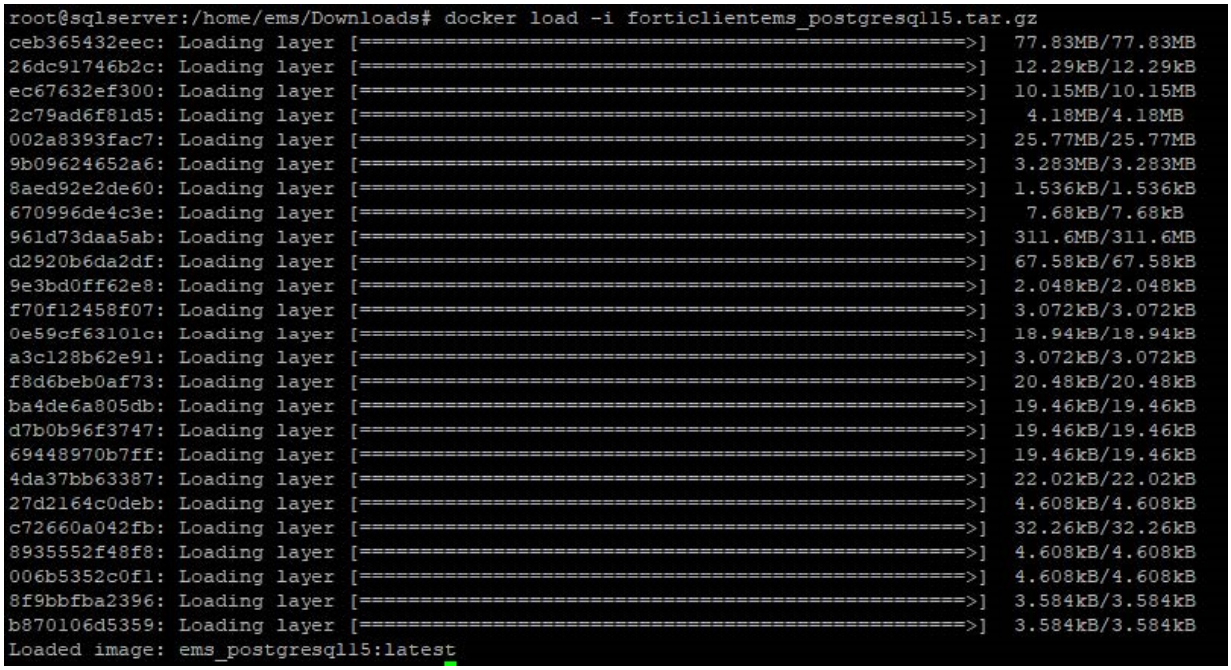
To install EMS with Postgres in Docker:

1. Prepare the desired Ubuntu machine(s). If using two machines, you install Postgres on one machine and EMS on the other machine. The following instructions designate some steps for the Postgres machine and others for the EMS machine. If you are using one machine, simply perform all configuration on that machine.
2. On the Postgres machine, do the following:
   a. Run `sudo -i` to log in to the shell with root privileges. Perform all following steps with root privileges.
   b. Install Docker:

```
apt install docker.io
```

   c. Download the Postgres Docker image forticlientems_7.4.3.XXXX_postgresql15.tar.gz file from Fortinet Support site.
   d. Load the image:

```
docker load -i forticlientems_postgresql15.tar.gz
```



e. List the images on Docker:

```
docker image ls
```

```
root@sqlserver:/home/ems/Downloads# docker image ls
REPOSITORY          TAG       IMAGE ID       CREATED       SIZE
ems_postgresql15    latest    6ce48c81f364   3 weeks ago   425MB
```

f. Run the Docker container. The following shows the command to run a container:

```
docker run --restart always --name <container name> -e POSTGRES_PASSWORD=<password> -p
<local port number>:<PostgreSQL port number:5432> -d <container instance name><default
username> -N <number>
```

The following details the options for the command:

Option	Description
-e	Set environment variables.
-p	Publish all exposed ports to random ports.
-d	Run container in the background and print container ID.
-N	Maximum number of concurrent connections allowed to the containerized Postgres database (DB).
--restart always	Ensures that if the host restarts, it starts the container automatically.

The following shows an example command with example values:

```
docker run --restart always --name ems_docker -e POSTGRES_PASSWORD=Fortinet123# -p
6434:5432 -d ems_postgresql15 postgres
```



The example command configures Fortinet123# as the password. Ensure that you configure your own unique password as to not compromise the security of your installation.



You can use any container instance name and password. In this example, the container's Postgres port, 5432, is exposed to port 6434 on the machine where Docker is running.

This allows you to have several instances of Postgres containers running and isolated from each other as long as they use different local host ports. You can use any port number as a local port for a Postgres container.

3. On the EMS machine, install EMS and connect to the DB:
   a. Download the forticlientems_7.4.3.XXXX.XXX64.bin file from the Fortinet Support site.
   b. Change permissions and add execute permissions to the installation file:
   `chmod +x forticlientems_7.4.3.XXXX.XXX64.bin`
   c. Set `umask` to 022 if the existing `umask` setting is more restrictive.
   d. Start the EMS installation and connect to the Postgres DB on the Docker container. The following shows the command to do so:

```
sudo ./<ems installation script file> -- --db_host <IP address or FQDN> --db_port <local
port> --db_user <username> --db_pass <password> --skip_db_install --allowed_hosts '*' --
enable_remote_https
```

The following shows an example command with example values:

```
./forticlientems_7.4.3.XXXX.bin -- --db_host 192.168.1.20 --db_port 6434 --db_user
postgres --db_pass Fortinet123# --skip_db_install --allowed_hosts '*' --enable_remote_
https
```



The example command configures Fortinet123# as the password. Ensure that you configure your own unique password as to not compromise the security of your installation.

Run the installer to and from any directory other than `/tmp`. Running the installer to or from `/tmp` causes issues.



`db_host` is the Postgres Docker machine IP address or FQDN.

e. After installation completes, check that all EMS services are running by entering the following command:

```
systemctl --all --type=service | grep -E 'fcems|apache|redis|postgres'
```

```
root@emsnode2:/home/ems/Downloads# systemctl --all --type=service | grep -E 'fcems|apache|redis|postgres'
  apache2.service                          loaded    active   running The Apache HTTP Server
  fcems_adconnector.service                loaded    active   running adconnector service
  fcems_addaemon.service                   loaded    active   running addaemon service
  fcems_adevtsrv.service                   loaded    active   running adevtsrv service
  fcems_adtask.service                     loaded    active   running adtask service
  fcems_chromebook.service                 loaded    active   running chromebook worker service
  fcems_das.service                        loaded    active   running das service
  fcems_dbop.service                       loaded    active   running dbop worker service
  fcems_deploy.service                     loaded    active   running deploy worker service
  fcems_ecsocksrv.service                  loaded    active   running ecsocksrv service
  fcems_forensics.service                  loaded    active   running forensics worker service
  fcems_ftntdbimporter.service             loaded    active   running FTNT DB importer worker service
  fcems_installer.service                  loaded    active   running installer worker service
  fcems_ka.service                         loaded    active   running kaworker service
  fcems_mdmproxy.service                   loaded    active   running MDM proxy service
  fcems_monitor.service                    loaded    active   running monitor worker service
  fcems_notify.service                     loaded    active   running FOS notify service
  fcems_pgbouncer.service                  loaded    active   running pgBouncer for EMS service
  fcems_probe.service                      loaded    active   running probeworker service
  fcems_reg.service                        loaded    active   running regworker service
  fcems_scep.service                       loaded    active   running SCEP service
  fcems_sip.service                        loaded    active   running software inventory processor service
  fcems_tag.service                        loaded    active   running tagworker service
  fcems_task.service                       loaded    active   running taskworker service
  fcems_update.service                     loaded    active   running update worker service
  fcems_upload.service                     loaded    active   running upload worker service
  fcems_wspgbouncer.service                loaded    active   running pgBouncer for EMS WebServer service
  fcems_ztna.service                       loaded    active   running ztna worker service
  postgresql.service                       loaded    active   exited  PostgreSQL RDBMS
  postgresql@15-main.service               loaded    active   running PostgreSQL Cluster 15-main
  redis-server.service                     loaded    active   running Advanced key-value store
```

The output shows that postgresql.service status displays as `exited`. This is the expected status. EMS does not create this service, which only exists to pass commands to version-specific Postgres

services. It displays as part of the output as the command filters for all services that contain "postgres" in the name.

f. Access the EMS GUI and log in.

g. If after initially installing EMS 7.4.3 you need to upgrade to a newer build, repeat step 3 with the new installation file.

Installing EMS with standalone remote database without Docker

The following uses PostgreSQL (Postgres) for the remote database. EMS and the Postgres database are hosted on two Ubuntu machines.

To configure the Postgres server:

1. Install Postgres 15 on the Postgres Ubuntu machine:

```
sudo apt install -y --no-install-recommends curl ca-certificates

sudo install -d /usr/share/postgresql-common/pgdg

sudo curl -o /usr/share/postgresql-common/pgdg/apt.postgresql.org.asc --fail
https://www.postgresql.org/media/keys/ACCC4CF8.asc

sudo sh -c 'echo "deb [signed-by=/usr/share/postgresql-
common/pgdg/apt.postgresql.org.asc] https://apt.postgresql.org/pub/repos/apt $(lsb_
release -cs)-pgdg main" > /etc/apt/sources.list.d/pgdg.list'

sudo apt update

sudo apt install -y postgresql-15
```

2. Install EMS custom extensions. The following commands require the ems_pg_extensions.tar.gz file, which you can download from the Fortinet Support site. Use the ems_pg_extensions.tar.gz file under the EMS 7.4.0 page to install extensions for later EMS versions:

```
sudo tar zxvf ems_pg_extensions.tar.gz -C /
sh -c 'head -c 20 /dev/urandom | md5sum | head -c 20;' |sudo tee
/var/lib/postgresql/15/symmetric_key.txt > /dev/null
sudo chown postgres:postgres /var/lib/postgresql/15/symmetric_key.txt
sudo systemctl restart postgresql
```

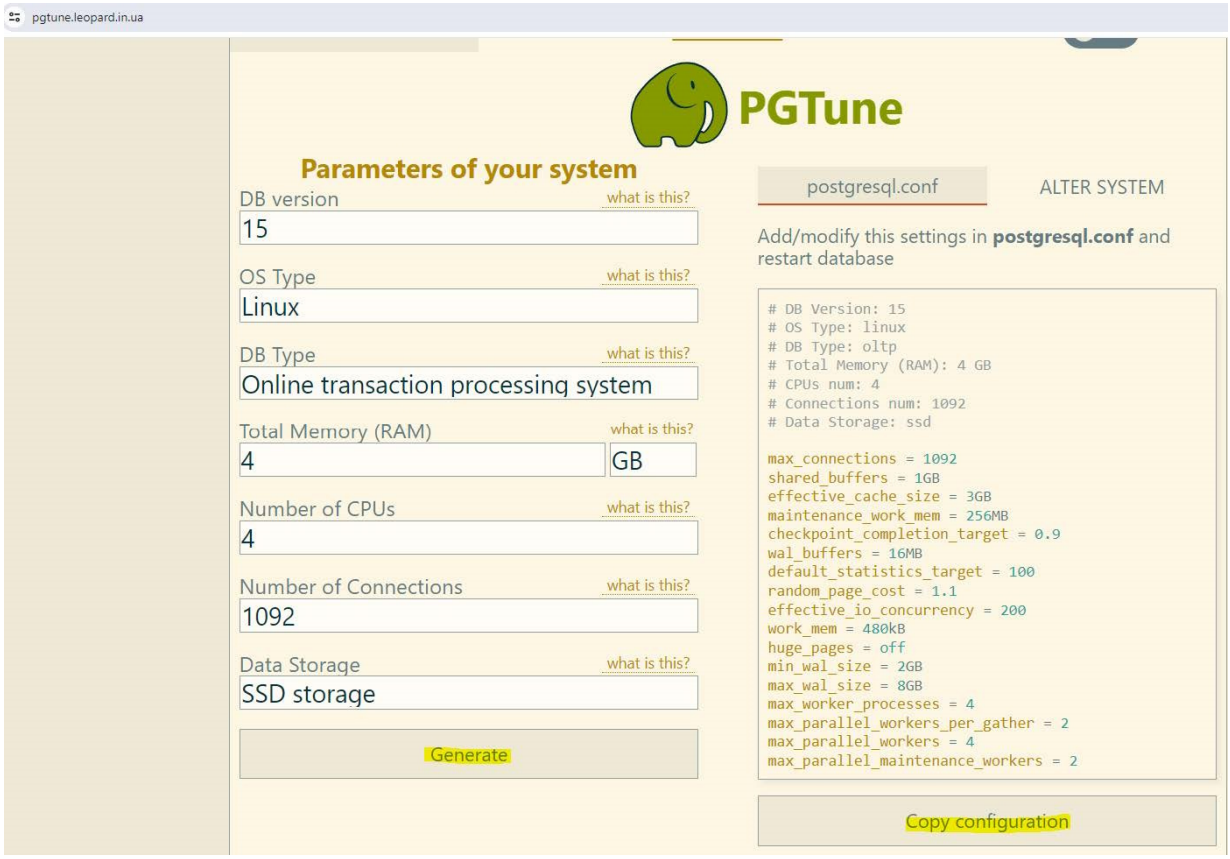
3. You can tune Postgres based on the host server specs by applying the recommended configuration. While there are various tools you can use to find the recommended configuration, these instructions use PGTune. Generate and copy the recommended configuration:

a. Go to PGTune and enter the following information:

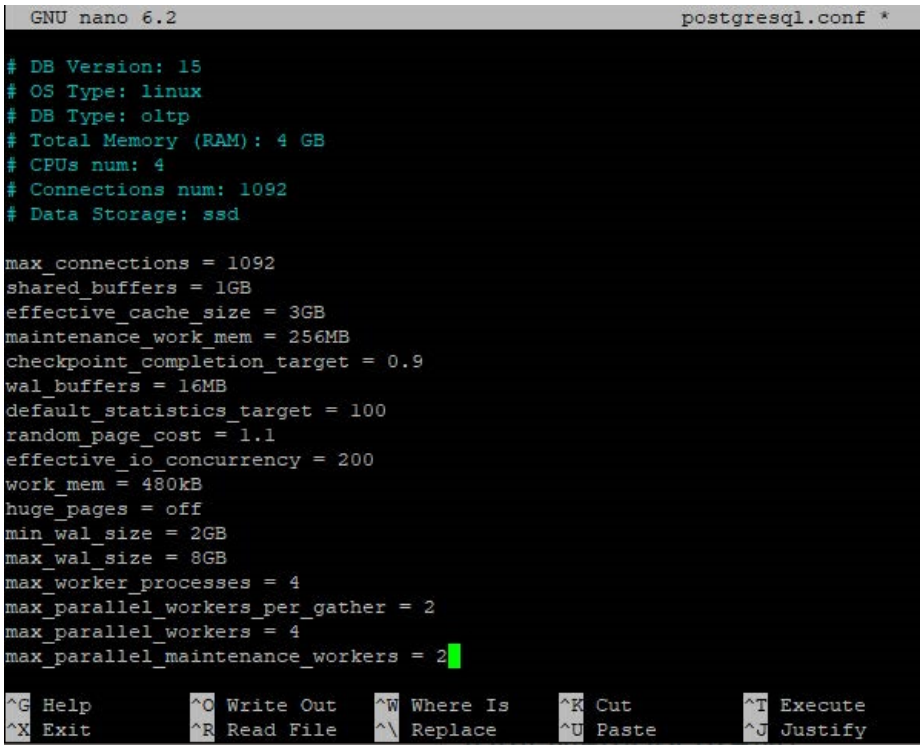
Field	Value
DB version	15
OS Type	Linux
DB Type	Online transaction processing system
Total Memory (RAM)	Enter the total memory for your Postgres server. In this example, it is 4 GB.
Number of CPUs	Enter the total number of CPUs for your Postgres server. In this example, it is 4.
Number of Connections	1092
Data Storage	Enter the data storage type as per your device. In this example, it is SSD storage.

b. Click *Generate*.

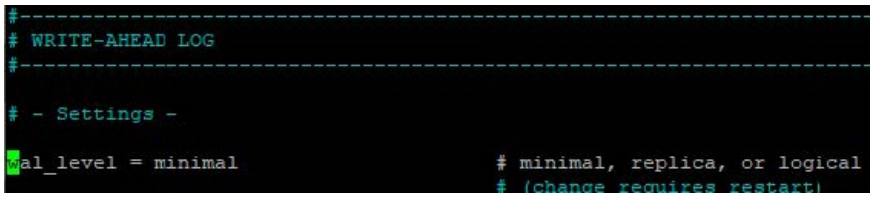
c. Click *Copy configuration*.



4. Update `/etc/postgresql/15/main/postgresql.conf`:
   a. Add or update the configuration in `/etc/postgresql/15/main/postgresql.conf` with the content that you copied in step 3.



b. Uncomment and change `wal_level` to `minimal`, e.g. `wal_level = minimal`. This removes all logging except the information required to recover from a crash or immediate shutdown.



c. Uncomment and change `max_wal_senders` to `0`, e.g. `max_wal_senders = 0`. This disables replication.

d. Uncomment and change `listen_addresses` to `'*'`, e.g. `'localhost' >> listen_addresses = '*'`.

5. Give passwordless permission to the Postgres user on the same machine by changing `/etc/postgresql/15/main/pg_hba.conf` running:

```
sed -i 's/# Database administrative login by Unix domain socket/\nhost all postgres
127.0.0.1\/32 trust\nhost all postgres ::1\/128 trust/' /etc/postgresql/15/main/pg_hba.conf
```

6. Allow connection from the remote machine by updating the following in pg_hba.conf:

```
# IPv4 local connections:
host all all 127.0.0.1/32 scram-sha-256 >> host all all 0.0.0.0/0 scram-sha-256
```

7. Restart the postgreSQL service:

```
systemctl restart postgresql
```

8. Change the postgres user password:

```
sudo -u postgres psql
ALTER USER postgres PASSWORD '<password>';
```

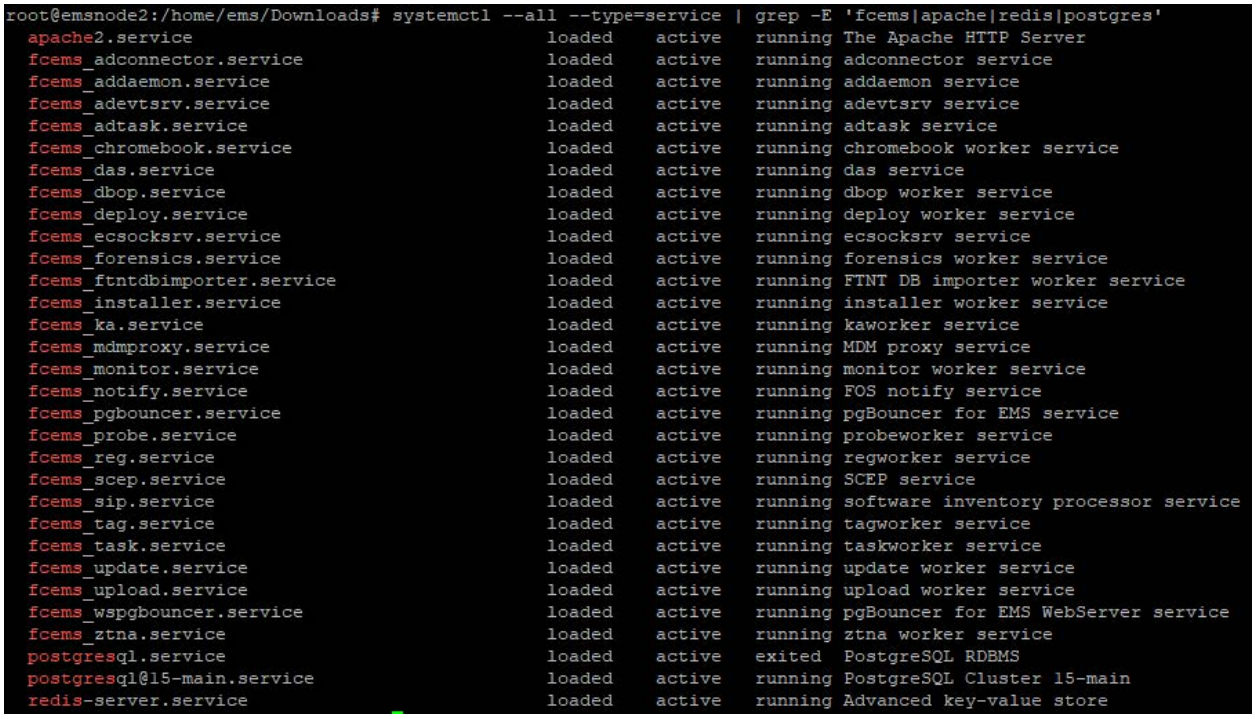
To install EMS:

1. On the second Ubuntu machine, download the forticlientems_7.4.3.XXXX.bin file from https://support.fortinet.com.
2. Set `umask` to 022 if the existing `umask` setting is more restrictive.
3. Install EMS. `db_host` is the remote Postgres server:

```
sudo chmod +x forticlientems_.XXXX.bin
sudo ./forticlientems_.XXXX.bin -- --db_host "172.16.1.26" --db_user postgres --db_pass
<password> --skip_db_install --allowed_hosts '*' --enable_remote_https
```

   Run the installer to and from any directory other than `/tmp`. Running the installer to or from `/tmp` causes issues.
4. After installation completes, check that all EMS services are running by entering the following command:

```
systemctl --all --type=service | grep -E 'fcems|apache|redis|postgres'
```



   The output shows that postgresql.service status displays as `exited`. This is the expected status. EMS does not create this service, which only exists to pass commands to version-specific Postgres services. It displays as part of the output as the command filters for all services that contain "postgres" in the name.
5. If after initially installing EMS 7.4.3 you need to upgrade to a newer build, repeat steps 1-3 with the new installation file.

Installing EMS HA with standalone remote DB without Docker

The following uses PostgreSQL (Postgres) for the remote database (DB). EMS and the Postgres DB are hosted on three Ubuntu machines.

To configure the Postgres server:

1. Install Postgres 15 on the Postgres Ubuntu machine:

```
sudo apt install -y --no-install-recommends curl ca-certificates
sudo install -d /usr/share/postgresql-common/pgdg
sudo curl -o /usr/share/postgresql-common/pgdg/apt.postgresql.org.asc --fail
https://www.postgresql.org/media/keys/ACCC4CF8.asc
sudo sh -c 'echo "deb [signed-by=/usr/share/postgresql-common/pgdg/apt.postgresql.org.asc]
https://apt.postgresql.org/pub/repos/apt $(lsb_release -cs)-pgdg main" >
/etc/apt/sources.list.d/pgdg.list'
sudo apt update
sudo apt install -y postgresql-15
```

2. Install EMS custom extensions. The following commands require the ems_pg_extensions.tar.gz file, which you can download from the Fortinet Support site. Use the ems_pg_extensions.tar.gz file under the EMS 7.4.0 page to install extensions for later EMS versions:

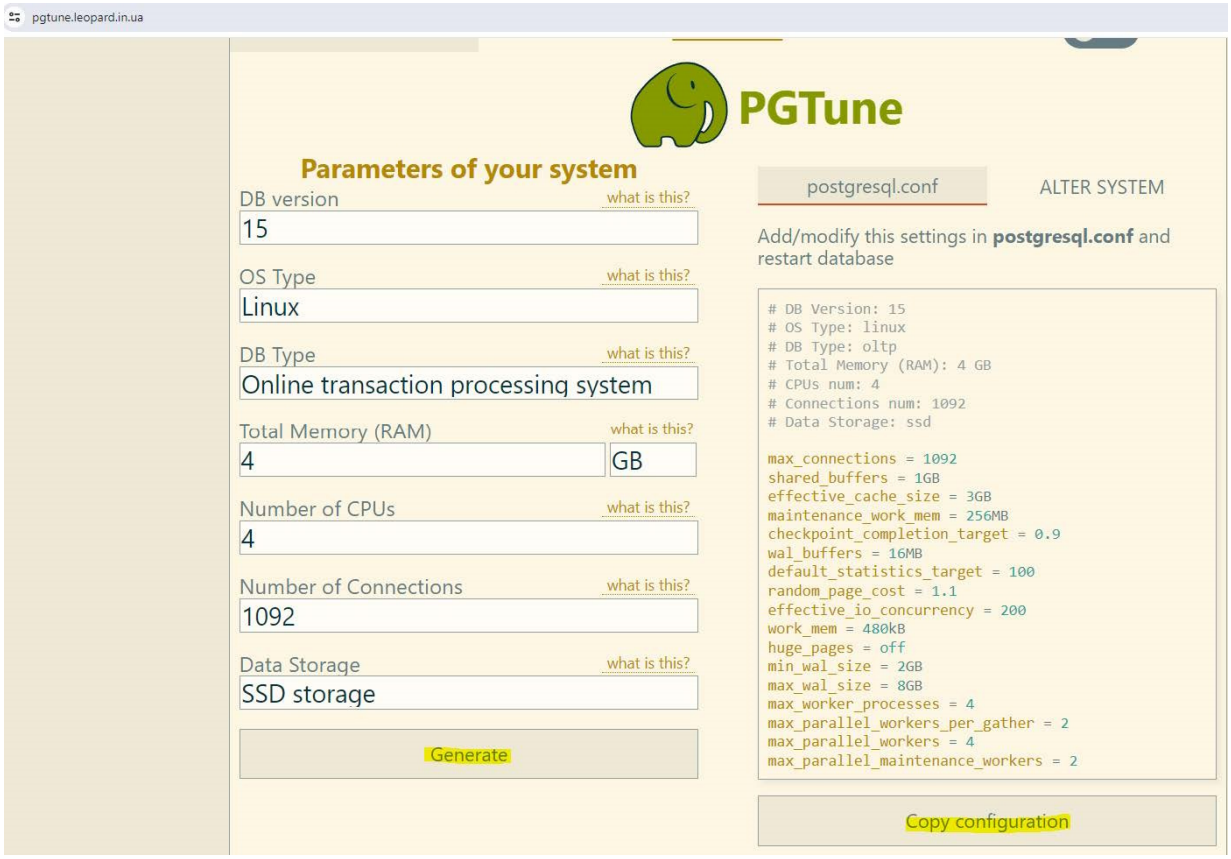
```
sudo tar zxvf ems_pg_extensions.tar.gz -C /
sh -c 'head -c 20 /dev/urandom | md5sum | head -c 20;' |sudo tee
/var/lib/postgresql/15/symmetric_key.txt > /dev/null
sudo chown postgres:postgres /var/lib/postgresql/15/symmetric_key.txt
sudo systemctl restart postgresql
```

3. You can tune Postgres based on the host server specs by applying the recommended configuration. While there are various tools you can use to find the recommended configuration, these instructions use PGTune. Generate and copy the recommended configuration:
   a. Go to PGTune and enter the following information:

Field	Value
DB version	15
OS Type	Linux
DB Type	Online transaction processing system
Total Memory (RAM)	Enter the total memory for your Postgres server. In this example, it is 4 GB.
Number of CPUs	Enter the total number of CPUs for your Postgres server. In this example, it is 4.
Number of Connections	1092
Data Storage	Enter the data storage type as per your device. In this example, it is SSD storage.

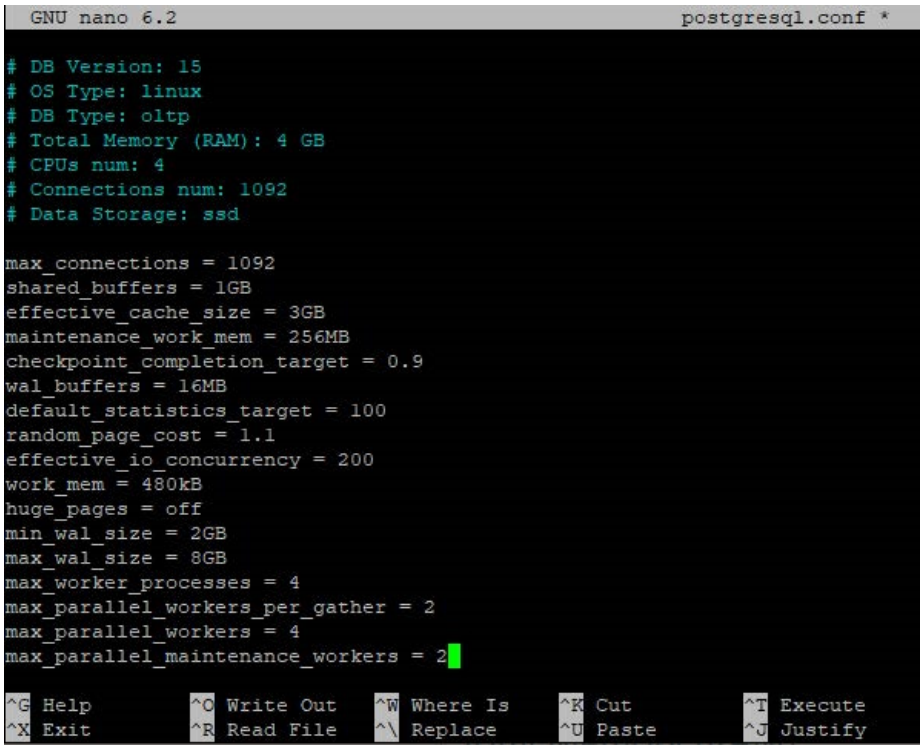
   b. Click *Generate*.

c. Click *Copy configuration*.

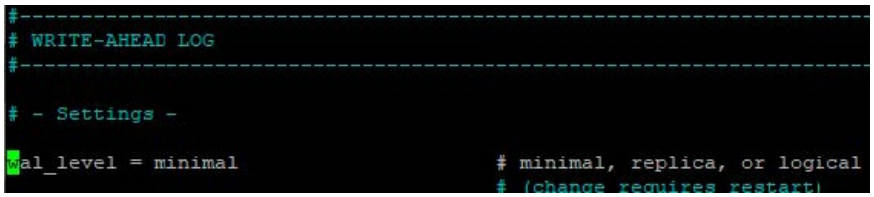


4. Update `/etc/postgresql/15/main/postgresql.conf`:

a. Add or update the configuration in `/etc/postgresql/15/main/postgresql.conf` with the content that you copied in step 3.



b. Uncomment and change `wal_level` to `minimal`, e.g. `wal_level = minimal`. This removes all logging except the information required to recover from a crash or immediate shutdown.



c. Uncomment and change `max_wal_senders` to `0`, e.g. `max_wal_senders = 0`. This disables replication.

d. Uncomment and change `listen_addresses` to `'*'`, e.g. `'localhost' >> listen_addresses = '*'`.

5. Give passwordless permission to the Postgres user on the same machine by changing `/etc/postgresql/15/main/pg_hba.conf` running:

```
sed -i 's/# Database administrative login by Unix domain socket/\nhost all postgres
127.0.0.1\/32 trust\nhost all postgres ::1\/128 trust/' /etc/postgresql/15/main/pg_hba.conf
```

6. Allow connection from the remote machine by updating the following in pg_hba.conf:

```
# IPv4 local connections:
host all all 127.0.0.1/32 scram-sha-256 >> host all all 0.0.0.0/0 scram-sha-256
```

7. Restart the postgreSQL service:

```
systemctl restart postgresql
```

8. Change the postgres user password:

```
sudo -u postgres psql
ALTER USER postgres PASSWORD '<password>';
```

To configure EMS HA:

1. On both nodes, do the following:
   a. Download the forticlientems_7.4.3.XXXX.bin file from https://support.fortinet.com.
   b. Change permissions and add execute permissions to the installation file:
   `sudo chmod +x forticlientems_7.4.3.XXXX.bin`
2. On the primary node, install EMS:
   a. Set `umask` to `022` if the existing `umask` setting is more restrictive.
   b. Install EMS:

```
sudo ./forticlientems_7.4.3.XXXX.bin -- --db_host "172.16.1.26" --db_user postgres --db_
pass <password> --skip_db_install --allowed_hosts '*' --enable_remote_https
```

   Run the installer to and from any directory other than `/tmp`. Running the installer to or from `/tmp` causes issues.



`db_host` is the remote Postgres server IP address.

   c. After installation completes, check that all EMS services are running by entering the following command:

```
systemctl --all --type=service | grep -E 'fcems|apache|redis|postgres'
```

```
root@emsnode2:/home/ems/Downloads# systemctl --all --type=service | grep -E 'fcems|apache|redis|postgres'
  apache2.service                                loaded    active   running The Apache HTTP Server
  fcems_adconnector.service                      loaded    active   running adconnector service
  fcems_addaemon.service                         loaded    active   running addaemon service
  fcems_adevtsrv.service                         loaded    active   running adevtsrv service
  fcems_adtask.service                           loaded    active   running adtask service
  fcems_chromebook.service                       loaded    active   running chromebook worker service
  fcems_das.service                              loaded    active   running das service
  fcems_dbop.service                             loaded    active   running dbop worker service
  fcems_deploy.service                           loaded    active   running deploy worker service
  fcems_ecsocksrv.service                        loaded    active   running ecsocksrv service
  fcems_forensics.service                        loaded    active   running forensics worker service
  fcems_ftntdbimporter.service                   loaded    active   running FTNT DB importer worker service
  fcems_installer.service                        loaded    active   running installer worker service
  fcems_ka.service                               loaded    active   running kaworker service
  fcems_mdmproxy.service                         loaded    active   running MDM proxy service
  fcems_monitor.service                          loaded    active   running monitor worker service
  fcems_notify.service                           loaded    active   running FOS notify service
  fcems_pgbouncer.service                        loaded    active   running pgBouncer for EMS service
  fcems_probe.service                            loaded    active   running probeworker service
  fcems_reg.service                              loaded    active   running regworker service
  fcems_scep.service                             loaded    active   running SCEP service
  fcems_sip.service                              loaded    active   running software inventory processor service
  fcems_tag.service                              loaded    active   running tagworker service
  fcems_task.service                             loaded    active   running taskworker service
  fcems_update.service                           loaded    active   running update worker service
  fcems_upload.service                           loaded    active   running upload worker service
  fcems_wspgbouncer.service                      loaded    active   running pgBouncer for EMS WebServer service
  fcems_ztna.service                             loaded    active   running ztna worker service
  postgresql.service                             loaded    active   exited  PostgreSQL RDBMS
  postgresql@15-main.service                     loaded    active   running PostgreSQL Cluster 15-main
  redis-server.service                           loaded    active   running Advanced key-value store
```

The output shows that postgresql.service status displays as `exited`. This is the expected status. EMS does not create this service, which only exists to pass commands to version-specific Postgres services. It displays as part of the output as the command filters for all services that contain "postgres" in the name.

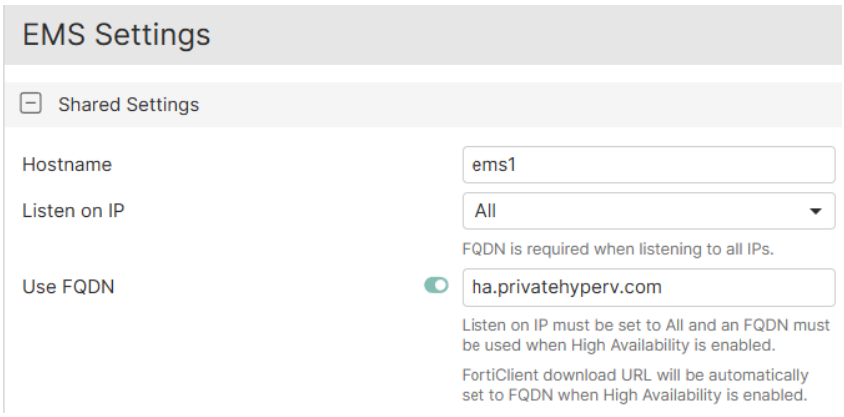
3. On the secondary node, install EMS:
   a. Set `umask` to `022` if the existing `umask` setting is more restrictive.
   b. Install EMS:

```
sudo ./forticlientems_7.4.3.XXXX.bin -- --db_host "172.16.1.26" --db_user postgres --db_
pass <password> --skip_db_install --skip_db_deploy --allowed_hosts '*' --enable_remote_
https
```

   Run the installer to and from any directory other than `/tmp`. Running the installer to or from `/tmp` causes issues.

   c. After installation completes, check that EMS services are running by entering the following command. On the secondary EMS, only fcems_monitor, fcems_pgbouncer, fcems_wspgbouncer, and redis-server services should be running:
   `systemctl --all --type=service | grep -E 'fcems|apache|redis|postgres'`
4. After installation on both nodes is complete, do the following:
   a. On the primary node, log in to EMS. License EMS as Starting FortiClient EMS and logging in on page 113describes. EMS HA requires a single license for the primary node and the secondary node(s). You only need to add the license to the primary node.
   b. Go to *System Settings* > *EMS Settings*.
   c. Under *Shared Settings*, confirm that *Listen on IP* is set to *All*.
   d. Enable *Use FQDN*.

e. Enter the desired FQDN.



f. In the *Custom hostname* field, enter a virtual IP address (VIP) that is configured in the FortiGate load balancer (LB) as the VIP for EMS. In this example, the VIP is 172.16.1.50.

g. Configure the *High Availability Keep Alive Internal* field with a value between 5 and 30 seconds.

h. Go to *Dashboard > Status*. Confirm that the *System Information* widget displays that EMS is running in HA mode. If running in HA mode, the widget also lists the HA primary and secondary nodes and their statuses.

5. Configure a FortiGate as an LB for EMS HA:

a. Create a health check:

i. Go to *Policy & Objects > Health Check*. Click *Create New*.

ii. For *Type*, select *TCP*.

iii. In the *Interval* field, enter 10.

iv. In the *Timeout* field, enter 2.

v. In the *Retry* field, enter 3.

vi. In the *Port* field, enter 8013. Click *OK*.

b. Create a virtual server:

i. Go to *Policy & Objects* and create a virtual server.

ii. Configure the fields as follows:

Field	Value
Virtual server IP	VIP that you configured in step 6. In this example, the VIP is 172.16.1.50.
Virtual server port	10443
Load Balancing method	*First Alive*
Health check	Monitor that you configured.

iii. Under *Real Servers*, select *Create New*.

iv. In the *IPv4 address* field, enter the primary EMS node IP address. In this example, it is 192.168.1.10.

v. In the *Port* field, enter 10443.

vi. In the *Max connections* field, enter 0.

vii. For *Mode*, select *Active*.

viii. Create a real server for the secondary EMS node. Click *Save*.

c. Repeat steps i-ix to create five additional virtual servers. The additional servers use ports 443, 8013, 8015, 8443, and 8871, but otherwise have identical settings to the first virtual server created. If you have enabled Chromebook management, create a virtual server for port 8443. Similarly, if you require importing an ACME certificate, create a virtual server for port 80.

d. Create a security policy that includes the LB virtual server as a destination address:

i. Go to *Policy & Objects* > *Firewall Policy*.

ii. Click *Create New*.

iii. Configure the *Incoming Interface* and *Outgoing Interface* fields. The outgoing interface connects to the primary EMS node.

iv. For *Source*, select *all*.

v. In the *Destination* field, select ports 10443, 443, 8013, 8015, 8443, and 8871.

vi. For *Service*, select *ALL*.

vii. For *Inspection Mode*, select *Proxy-based*.

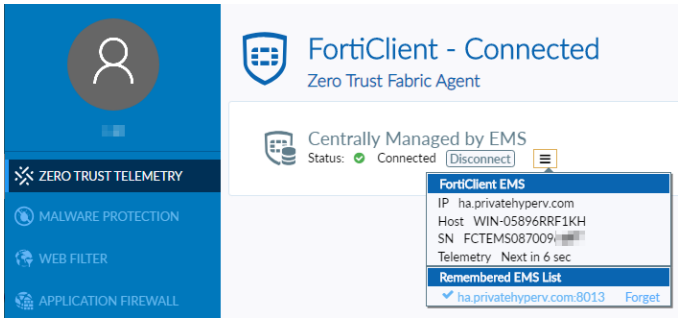
viii. Save the policy.

ix. If the EMS nodes are in different subnets, repeat these steps to configure a policy for the secondary EMS node. In this example, the nodes are in the same subnet, so you do not need to add a separate policy for the secondary EMS.

6. After the FortiGate LB configuration is complete, you can access EMS using the VIP configured in the FortiGate LB. If after initially installing EMS 7.4.3 you need to upgrade to a newer build, repeat steps 1-3 with the new installation file.

To validate the HA configuration:

1. Go to *Deployment & Installers* > *Manage Deployment*. Create a deployment package to deploy FortiClient to endpoints. See Adding a FortiClient installer on page 230.
2. On an endpoint, download the deployment package from the download link.
3. Install FortiClient on the endpoint.
4. Ensure that FortiClient can register to the EMS server successfully using the FQDN.
5. Simulate HA by stopping FortiClient Endpoint Management Server Monitor Service on the primary node. Ensure that the secondary node is now the EMS primary server.
6. Ensure that FortiClient can still register to the EMS successfully using the FQDN.



Installing EMS HA with Postgres HA using Bitnami Docker

The following provides instructions for installing EMS in a high availability (HA) configuration with the PostgreSQL (Postgres) databases (DB) also in an HA configuration using Bitnami Docker.

To configure EMS HA with Postgres HA using Bitnami Docker:

1. Prepare four Ubuntu machines. Two act as Postgres DB hosts and the other two are EMS hosts. If using cloned virtual machines for the EMS hosts, run the following commands on the cloned machine:

```
sudo rm /etc/machine-id
sudo rm /var/lib/dbus/machine-id
sudo systemd-machine-id-setup
```

2. Run `sudo -i` to log in to the shell with root privileges. Perform all following steps with root privileges.
3. Configure the Postgres HA cluster:
   a. Load the EMS Postgres Bitnami Docker image in both Postgres DB host nodes:
      i. Install Docker:

```
apt install docker.io
```

      ii. Download the Postgres Docker image forticlientems_postgres-ha.tar.gz file from the Fortinet Support site.
      iii. Load the image:

```
docker load -i forticlientems_postgres-ha.tar.gz
```

```
root@postgres1:/home/ems/Downloads# ls
ems_postgres-ha.tar.gz
root@postgres1:/home/ems/Downloads# sudo docker load -i ems_postgres-ha.tar.gz
7f19a690f50b: Loading layer [==================================================>]  280.9MB/280.9MB
259e04701d10: Loading layer [==================================================>]  19.97kB/19.97kB
34b3785e58cd: Loading layer [==================================================>]  19.46kB/19.46kB
74227982bbd0: Loading layer [==================================================>]  19.46kB/19.46kB
350f757aaff7: Loading layer [==================================================>]  19.46kB/19.46kB
30f9570f43bb: Loading layer [==================================================>]  22.02kB/22.02kB
1a1438813b9a: Loading layer [==================================================>]  4.608kB/4.608kB
a8ad2c286815: Loading layer [==================================================>]  32.26kB/32.26kB
63a09523f9fc: Loading layer [==================================================>]  4.608kB/4.608kB
9ebb0f072df7: Loading layer [==================================================>]  4.608kB/4.608kB
b7f7a4109629: Loading layer [==================================================>]  2.56kB/2.56kB
Loaded image: ems-postgres-ha:latest
root@postgres1:/home/ems/Downloads#
```

      iv. List the images on Docker to verify the image has been created or loaded:

```
docker image ls
```

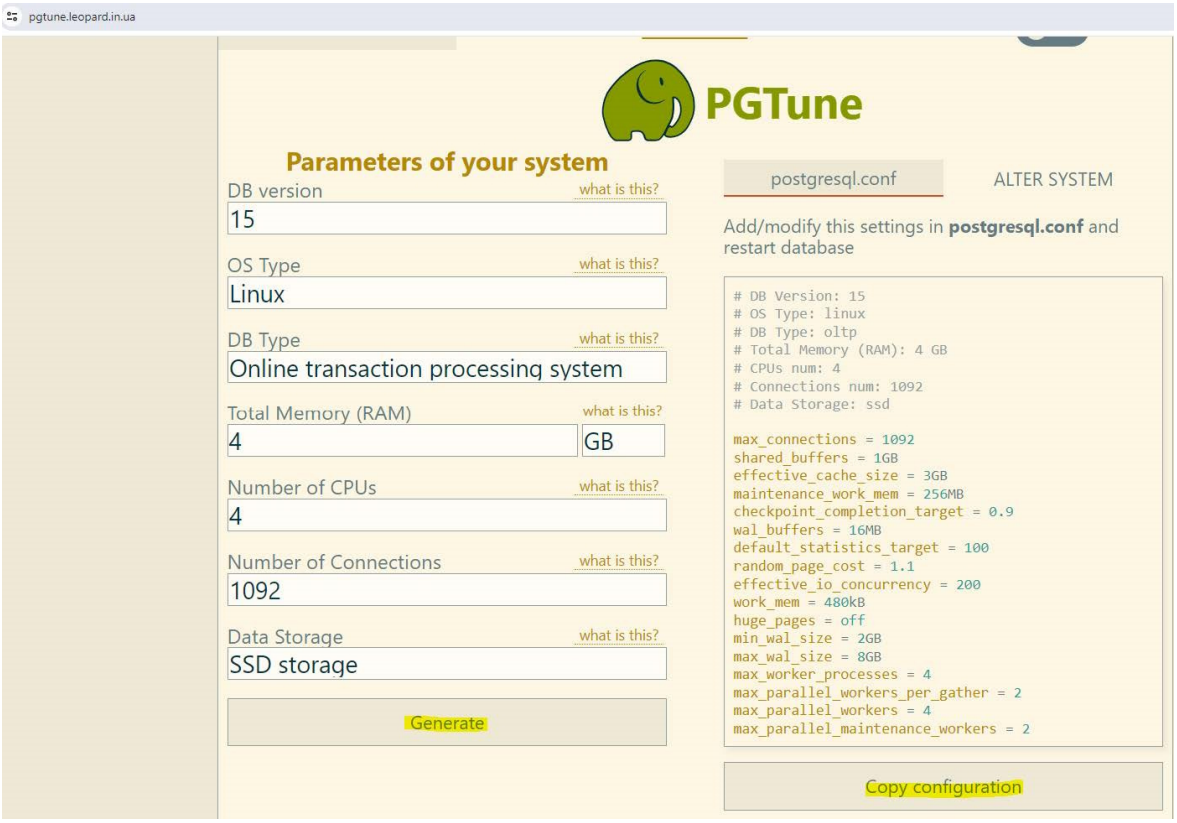
   b. You can tune Postgres based on the host server specs by applying the recommended configuration. While there are various tools you can use to find the recommended configuration, these instructions use PGTune. Generate and copy the recommended configuration:

i. Go to PGTune and enter the following information:

Field	Value
DB version	15
OS Type	Linux
DB Type	Online transaction processing system
Total Memory (RAM)	Enter the total memory for your Postgres server. In this example, it is 4 GB.
Number of CPUs	Enter the total number of CPUs for your Postgres server. In this example, it is 4.
Number of Connections	1092
Data Storage	Enter the data storage type as per your device. In this example, it is SSD storage.

ii. Click *Generate*.

iii. Click *Copy configuration*.



c. Start the primary DB:

i. Start the Postgres Bitnami container on the primary host. In this example, the primary host is pg-1:

```
docker run --restart always --detach --name pg-1 -p 5432:5432 \
--env POSTGRESQL_PASSWORD=Fortinet123# \
--env POSTGRESQL_DAEMON_USER=postgres \
--env REPMGR_PASSWORD=Fortinet123# \
--env REPMGR_PRIMARY_HOST=pg-1 \
--env REPMGR_PRIMARY_PORT=5432 \
--env REPMGR_PARTNER_NODES=pg-1,pg-2:5432 \
--env REPMGR_NODE_NAME=pg-1 \
--env REPMGR_NODE_NETWORK_NAME=pg-1 \
--env REPMGR_PORT_NUMBER=5432 \
--volume pg_1_data:/bitnami/postgresql \
--add-host pg-1:172.16.1.12 \
--add-host pg-2:172.16.1.15 \
ems-postgres-ha
```



The example command configures Fortinet123# as the password. Ensure that you configure your own unique password as to not compromise the security of your installation.

The following provides details for some of the parameters:

Parameter	Value
REPMGR_PRIMARY_HOST	Hostname or IP address of where this node is running, which other nodes can access
REPMGR_PARTNER_NODES	Comma-separated list of the hostnames or IP addresses of all nodes that form this cluster
REPMGR_NODE_NAME	Node name. This can but does not necessarily need to match the hostname. This value shows when you perform step d to verify the cluster status.
REPMGR_NODE_NETWORK_NAME	Hostname or IP address of where this node is running.

ii. Verify if the container is running:

```
docker ps -a
```

d. From the secondary DB host, start the DB:

i. Start the Postgres Bitnami container on the secondary host. In this example, the secondary host is pg-2:

```
docker run --restart always --detach --name pg-2 -p 5432:5432 \
--env POSTGRESQL_PASSWORD=Fortinet123# \
--env POSTGRESQL_DAEMON_USER=postgres \
--env REPMGR_PASSWORD=Fortinet123# \
--env REPMGR_PRIMARY_HOST=pg-1 \
--env REPMGR_PRIMARY_PORT=5432 \
--env REPMGR_PARTNER_NODES=pg-1,pg-2:5432 \
--env REPMGR_NODE_NAME=pg-2 \
--env REPMGR_NODE_NETWORK_NAME=pg-2 \
--env REPMGR_PORT_NUMBER=5432 \
```

```
--volume pg_2_data:/bitnami/postgresql \
--add-host pg-1:172.16.1.12 \
--add-host pg-2:172.16.1.15 \
ems-postgres-ha
```



The example command configures Fortinet123# as the password. Ensure that you configure your own unique password as to not compromise the security of your installation.

The following provides details for some of the parameters:

Parameter	Value
REPMGR_PRIMARY_HOST	Hostname or IP address of where the primary node is running, which other nodes can access
REPMGR_PARTNER_NODES	Comma-separated list of the hostnames or IP addresses of all nodes that form this cluster
REPMGR_NODE_NAME	Node name. This can but does not necessarily need to match the hostname.
REPMGR_NODE_NETWORK_NAME	Hostname or IP address of where this node is running

ii. Verify if the container is running:

```
docker ps -a
```

e. From the primary DB node, verify the cluster status:

```
docker exec -it pg-1 bash /opt/bitnami/scripts/postgresql-repmgr/entrypoint.sh repmgr -f
/opt/bitnami/repmgr/conf/repmgr.conf service status
```

4. After the DB cluster is up and running, configure EMS HA:
   a. On both nodes, do the following:
      i. Download the forticlientems_7.4.3.XXXX.bin file from the Fortinet Support site.
      ii. Change permissions and add execute permissions to the installation file:

```
chmod +x forticlientems_7.4.3.XXXX.bin
```

   b. On the primary node, install EMS:
      i. Set `umask` to 022 on file `/etc/login.defs` if the existing `umask` setting is more restrictive.
      ii. Install EMS:

```
./forticlientems_7.4.3.XXXX.bin -- --db_host "172.16.1.12,172.16.1.15" --db_user
postgres --db_pass Fortinet123# --skip_db_install --allowed_hosts '*' --enable_remote_
https
```

Run the installer to and from any directory other than `/tmp`. Running the installer to or from `/tmp` causes issues.

In the example, `db_host` contains IP addresses for both DB nodes. Replace the IP addresses with your DB server IP addresses or FQDNs.

iii. After installation completes, check that all EMS services are running by entering the following command:

```
systemctl --all --type=service | grep -E 'fcems|apache|redis|postgres'
```

```
root@emsnode2:/home/ems/Downloads# systemctl --all --type=service | grep -E 'fcems|apache|redis|postgres'
  apache2.service                              loaded    active   running The Apache HTTP Server
  fcems_adconnector.service                    loaded    active   running adconnector service
  fcems_addaemon.service                       loaded    active   running addaemon service
  fcems_adevtsrv.service                       loaded    active   running adevtsrv service
  fcems_adtask.service                         loaded    active   running adtask service
  fcems_chromebook.service                     loaded    active   running chromebook worker service
  fcems_das.service                            loaded    active   running das service
  fcems_dbop.service                           loaded    active   running dbop worker service
  fcems_deploy.service                         loaded    active   running deploy worker service
  fcems_ecsocksrv.service                      loaded    active   running ecsocksrv service
  fcems_forensics.service                      loaded    active   running forensics worker service
  fcems_ftntdbimporter.service                 loaded    active   running FTNT DB importer worker service
  fcems_installer.service                      loaded    active   running installer worker service
  fcems_ka.service                             loaded    active   running kaworker service
  fcems_mdmproxy.service                       loaded    active   running MDM proxy service
  fcems_monitor.service                        loaded    active   running monitor worker service
  fcems_notify.service                         loaded    active   running FOS notify service
  fcems_pgbouncer.service                      loaded    active   running pgBouncer for EMS service
  fcems_probe.service                          loaded    active   running probeworker service
  fcems_reg.service                            loaded    active   running regworker service
  fcems_scep.service                           loaded    active   running SCEP service
  fcems_sip.service                            loaded    active   running software inventory processor service
  fcems_tag.service                            loaded    active   running tagworker service
  fcems_task.service                           loaded    active   running taskworker service
  fcems_update.service                         loaded    active   running update worker service
  fcems_upload.service                         loaded    active   running upload worker service
  fcems_wspgbouncer.service                    loaded    active   running pgBouncer for EMS WebServer service
  fcems_ztna.service                           loaded    active   running ztna worker service
  postgresql.service                           loaded    active   exited  PostgreSQL RDBMS
  postgresql@15-main.service                   loaded    active   running PostgreSQL Cluster 15-main
  redis-server.service                         loaded    active   running Advanced key-value store
```

The output shows that postgresql.service status displays as `exited`. This is the expected status. EMS does not create this service, which only exists to pass commands to version-specific Postgres services. It displays as part of the output as the command filters for all services that contain "postgres" in the name.

c. On the secondary node, install EMS:

i. Set `umask` to 022 if the existing `umask` setting is more restrictive.

ii. Install EMS:

```
./forticlientems_7.4.3.XXXX.bin -- --db_host "172.16.1.12,172.16.1.15" --db_user
postgres --db_pass Fortinet123# --skip_db_install --skip_db_deploy --allowed_hosts '*'
--enable_remote_https
```

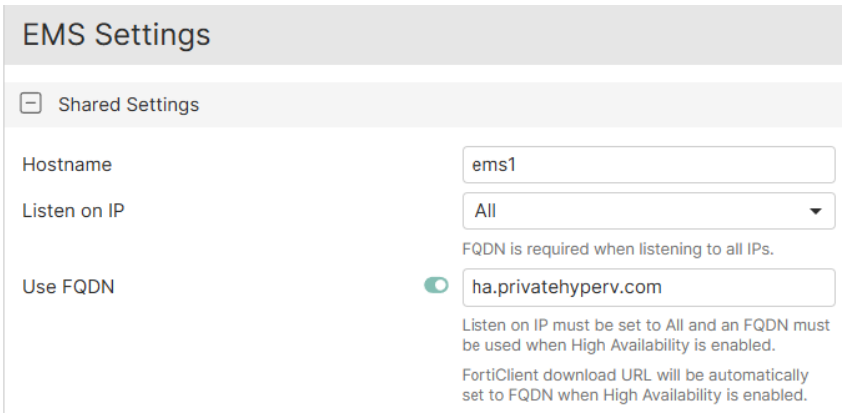
Run the installer to and from any directory other than `/tmp`. Running the installer to or from `/tmp` causes issues.

iii. After installation completes, check that EMS services are running by entering the following command. On the secondary EMS, only fcems_monitor, fcems_pgbouncer, fcems_wspgbouncer, and redis-server services should be running:

```
systemctl --all --type=service | grep -E 'fcems|apache|redis|postgres'
```

d. After installation on both nodes is complete, do the following:

i. On the primary node, log in to EMS. License EMS as Starting FortiClient EMS and logging in on page 113 describes. EMS HA requires a single license for the primary node and the secondary node(s). You only need to add the license to the primary node.
ii. Go to *System Settings > EMS Settings*.
iii. Under *Shared Settings*, confirm that *Listen on IP* is set to *All*.
iv. Enable *Use FQDN*.
v. Enter the desired FQDN.



vi. In the *Custom hostname* field, enter a virtual IP address (VIP) that is configured in the FortiGate load balancer (LB) as the VIP for EMS. In this example, the VIP is 172.16.1.50.
vii. Configure the *High Availability Keep Alive Internal* field with a value between 5 and 30 seconds.
viii. Go to *Dashboard > Status*. Confirm that the *System Information* widget displays that EMS is running in HA mode. If running in HA mode, the widget also lists the HA primary and secondary nodes and their statuses.

5. Configure a FortiGate as an LB for EMS HA:
   a. Create a health check:
      i. Go to *Policy & Objects > Health Check*. Click *Create New*.
      ii. For *Type*, select *TCP*.
      iii. In the *Interval* field, enter 10.
      iv. In the *Timeout* field, enter 2.
      v. In the *Retry* field, enter 3.
      vi. In the *Port* field, enter 8013. Click *OK*.
   b. Create a virtual server:
      i. Go to *Policy & Objects* and create a virtual server.
      ii. Configure the fields as follows:

Field	Value
Virtual server IP	VIP that you configured in step 4.f. In this example, the VIP is 172.16.1.50.
Virtual server port	10443
Load Balancing method	*First Alive*
Health check	Monitor that you configured.

Field	Value
Network Type	*TCP*

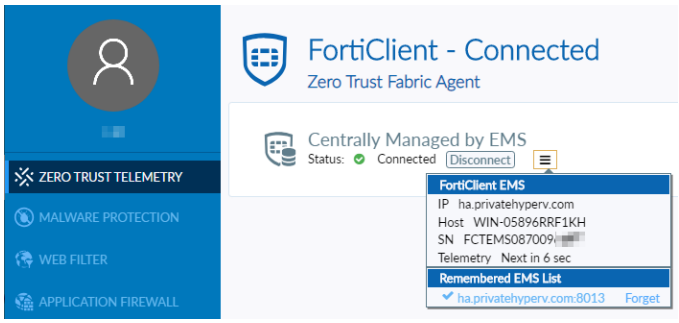
iii. Under *Real Servers*, select *Create New*.
iv. In the *IPv4 address* field, enter the primary EMS node IP address. In this example, it is 192.168.1.10.
v. In the *Port* field, enter 10443.
vi. In the *Max connections* field, enter 0.
vii. For *Mode*, select *Active*.
viii. Create a real server for the secondary EMS node. Click *Save*.

c. Repeat steps i-ix to create five additional virtual servers. The additional servers use ports 443, 8013, 8015, 8443, and 8871, but otherwise have identical settings to the first virtual server created. If you have enabled Chromebook management, create a virtual server for port 8443. Similarly, if you require importing an ACME certificate, create a virtual server for port 80.
d. Create a security policy that includes the LB virtual server as a destination address:
i. Go to *Policy & Objects > Firewall Policy*.
ii. Click *Create New*.
iii. Configure the *Incoming Interface* and *Outgoing Interface* fields. The outgoing interface connects to the primary EMS node.
iv. For *Source*, select *all*.
v. In the *Destination* field, select ports 10443, 443, 8013, 8015, 8443, and 8871.
vi. For *Service*, select *ALL*.
vii. For *Inspection Mode*, select *Proxy-based*.
viii. Save the policy.
ix. If the EMS nodes are in different subnets, repeat these steps to configure a policy for the secondary EMS node. In this example, the nodes are in the same subnet, so you do not need to add a separate policy for the secondary EMS.
e. After the FortiGate LB configuration is complete, you can access EMS using the VIP configured in the FortiGate LB. If after initially installing EMS 7.4.3 you need to upgrade to a newer build, repeat steps 4.a.-c. with the new installation file

To validate the HA configuration:

1. Go to *Deployment & Installers > Manage Deployment*. Create a deployment package to deploy FortiClient to endpoints. See Adding a FortiClient installer on page 230.
2. On an endpoint, download the deployment package from the download link.
3. Install FortiClient on the endpoint.
4. Ensure that FortiClient can register to the EMS server successfully using the FQDN.
5. Simulate HA by stopping FortiClient Endpoint Management Server Monitor Service on the primary node. Ensure that the secondary node is now the EMS primary server.

6. Ensure that FortiClient can still register to the EMS successfully using the FQDN.



Installing EMS HA with native Postgres HA without Docker

This guide gives instructions on how to set up a PostgreSQL (Postgres) high availability (HA) cluster when Postgres is natively installed (not Postgres containers) and install EMS HA.

Postgres HA requires at least three servers or virtual machines (VM):

Node	Purpose
Postgres node 1	Starts as the primary node
Postgres node 2	Starts as the standby node
Postgres witness 1	Serves as a witness to prevent split-brain scenarios where both nodes self-promote to become the primary and clash

The configuration also requires two servers or VMs for EMS nodes.

To configure Postgres node 1:

1. Install Postgres 15 and Replication Manager. Postgres recommends this replication tool:

```
sudo apt install -y --no-install-recommends curl ca-certificates apt-transport-https

sudo install -d /usr/share/postgresql-common/pgdg

sudo curl -o /usr/share/postgresql-common/pgdg/apt.postgresql.org.asc --fail
https://www.postgresql.org/media/keys/ACCC4CF8.asc

sudo sh -c 'echo "deb [signed-by=/usr/share/postgresql-common/pgdg/apt.postgresql.org.asc]
https://apt.postgresql.org/pub/repos/apt $(lsb_release -cs)-pgdg main" >
/etc/apt/sources.list.d/pgdg.list'

sudo apt update

sudo apt install -y postgresql-15 postgresql-15-repmgr
```

2. Install EMS custom extensions (`ems_pg_extensions.tar.gz`) for Postgres. You can download the extensions from the Fortinet Support site. Use the `ems_pg_extensions.tar.gz` file under the EMS 7.4.0 page to install extensions for EMS 7.4.3:

```
sudo tar zxvf ems_pg_extensions.tar.gz -C /
```

3. Create the symmetric key required that the custom extension requires. Copy the value in `symmetric_key.txt` as you must share it with the other nodes:

```
sh -c 'head -c 20 /dev/urandom | md5sum | head -c 20;' |sudo tee
/var/lib/postgresql/15/symmetric_key.txt > /dev/null
sudo chown postgres:postgres /var/lib/postgresql/15/symmetric_key.txt
cat /var/lib/postgresql/15/symmetric_key.txt
```

4. Set the password for the Postgres Linux user:

```
sudo passwd postgres
```

5. Modify `postgresql.conf` to add replication parameters. Change the following settings on `/etc/postgresql/15/main/postgresql.conf` with the indicated values:

```
listen_addresses = 'localhost,<PostgreSQL node1 server IP address>'
max_wal_senders = 10
max_replication_slots = 10
wal_level = replica
hot_standby = on
archive_mode = on
archive_command = '/bin/true'
shared_preload_libraries = 'repmgr'
```

6. Set up Postgres access to the replication user. Add the following to `/etc/postgresql/15/main/pg_hba.conf`:

```
host all all 127.0.0.1/32 trust
local replication repmgr trust
host replication repmgr 127.0.0.1/32 trust
host replication repmgr <postgres node1 ip>/32 trust
host replication repmgr <postgres node2 ip>/32 trust
host replication repmgr <witness ip>/32 trust
local repmgr repmgr trust
host repmgr repmgr 127.0.0.1/32 trust
host repmgr repmgr <postgres node1 ip>/32 trust
host repmgr repmgr <postgres node2 ip>/32 trust
host repmgr repmgr <witness ip>/32 trust
host all all 0.0.0.0/0 scram-sha-256
```



Replace `<postgres node1 ip>`, `<postgres node2 ip>`, and `<witness ip>` accordingly.

7. Create the repmgr user and database. Run the following to create the repmgr user and database on Postgres:

```
sudo -u postgres createuser -s repmgr
sudo -u postgres createdb repmgr -O repmgr
```

8. Restart the postgresql service:

```
sudo systemctl restart postgresql@15-main.service
```

9. Set Postgres user password:

```
sudo -u postgres psql
ALTER USER postgres PASSWORD '<postgres password>';
```

To configure Postgres node 2:

1. Install Postgres 15 and Replication Manager. Postgres recommends this replication tool:

```
sudo apt install -y --no-install-recommends curl ca-certificates apt-transport-https

sudo install -d /usr/share/postgresql-common/pgdg

sudo curl -o /usr/share/postgresql-common/pgdg/apt.postgresql.org.asc --fail
https://www.postgresql.org/media/keys/ACCC4CF8.asc

sudo sh -c 'echo "deb [signed-by=/usr/share/postgresql-common/pgdg/apt.postgresql.org.asc]
https://apt.postgresql.org/pub/repos/apt $(lsb_release -cs)-pgdg main" >
/etc/apt/sources.list.d/pgdg.list'

sudo apt update

sudo apt install -y postgresql-15 postgresql-15-repmgr
```

2. Install EMS custom extensions (`ems_pg_extensions.tar.gz`) for Postgres. You can download the extensions from the Fortinet Support site:

```
sudo tar zxvf ems_pg_extensions.tar.gz -C /
```

3. Create the symmetric key required that the custom extension requires. The value must be the one copied from the symmetric key from the Postgres node 1:

```
sh -c 'echo "<value copied from PostgreSQL node 1>"|head -c 20 | head -c 20;'|sudo tee
/var/lib/postgresql/15/symmetric_key.txt > /dev/null
```

4. Set the password for the Postgres Linux user:

```
sudo passwd postgres
```

5. Modify `postgresql.conf` to add replication parameters. Change the following settings on `/etc/postgresql/15/main/postgresql.conf` with the indicated values:

```
listen_addresses = 'localhost, <ip of the Postgres node2 server>'
max_wal_senders = 10
max_replication_slots = 10
wal_level = replica
hot_standby = on
archive_mode = on
```

```
archive_command = '/bin/true'
shared_preload_libraries = 'repmgr'
```

6. Set up Postgres access to the replication user. Add the following to `/etc/postgresql/15/main/pg_hba.conf`:

```
host all all 127.0.0.1/32 trust
local replication repmgr trust
host replication repmgr 127.0.0.1/32 trust
host replication repmgr <postgres node1 ip>/32 trust
host replication repmgr <postgres node2 ip>/32 trust
host replication repmgr <witness ip>/32 trust
local repmgr repmgr trust
host repmgr repmgr 127.0.0.1/32 trust
host repmgr repmgr <postgres node1 ip>/32 trust
host repmgr repmgr <postgres node2 ip>/32 trust
host repmgr repmgr <witness ip>/32 trust
host all all 0.0.0.0/0 scram-sha-256
```



Replace `<postgres node1 ip>`, `<postgres node2 ip>`, and `<witness ip>` accordingly.

7. Restart the postgresql service:

```
sudo systemctl restart postgresql@15-main.service
```

To set up SSH access between Postgres nodes 1 and 2:



When the CLI prompts you, enter the postgres password.

1. On Postgres node 1, run the following:

```
sudo -H -u postgres bash -c "ssh-keygen -t rsa -f ~/.ssh/id_rsa -N ''"
sudo -H -u postgres bash -c "ssh-copy-id -i ~/.ssh/id_rsa.pub -o StrictHostKeyChecking=no
'postgres@<postgres node2 ip>'"
```

2. On Postgres node 2, run the following:

```
sudo -H -u postgres bash -c "ssh-keygen -t rsa -f ~/.ssh/id_rsa -N ''"
sudo -H -u postgres bash -c "ssh-copy-id -i ~/.ssh/id_rsa.pub -o StrictHostKeyChecking=no
'postgres@<postgres node1 ip>'"
```

To register Postgres node1 to the cluster:

1. Create the `/etc/repmgr.conf` file on Postgres node1:

```
cluster= 'emscluster'
node_id=1
node_name=postgresqlnode1
conninfo= 'host=<postgres node1 ip> user=repmgr dbname=repmgr connect_timeout=2'
data_directory= '/var/lib/postgresql/15/main/'
pg_bindir='/usr/bin/'
log_file= '/var/log/repmgr/repmgr.log'
log_level=DEBUG
failover=automatic
promote_command= '/usr/bin/repmgr standby promote -f /etc/repmgr.conf'
follow_command= '/usr/bin/repmgr standby follow -f /etc/repmgr.conf --upstream-node-id=%n'
```



Replace `<postgres node1 ip>` accordingly.

2. Create the log directory for repmgr:

```
sudo mkdir /var/log/repmgr
sudo chown -R postgres /var/log/repmgr
```

3. Register the node as the primary:

```
sudo -u postgres /usr/bin/repmgr -f /etc/repmgr.conf primary register
```

4. Confirm registration:

```
sudo -u postgres /usr/bin/repmgr -f /etc/repmgr.conf cluster show
```

5. Create a systemd service config for repmgr by creating the file `/etc/systemd/system/repmgrd.service`:

```
[Unit]
Description=PostgreSQL Replication Manager Daemon
After=network.target postgresql.service

[Service]
Type=forking
User=postgres
ExecStart=/usr/bin/repmgrd -f /etc/repmgr.conf --daemonize
PIDFile=/tmp/repmgrd.pid
ExecStop=/bin/kill -s TERM $(cat /tmp/repmgrd.pid)
ExecReload=/bin/kill -s HUP $(cat /tmp/repmgrd.pid)
Restart=on-failure
LimitNOFILE=16384

[Install]
WantedBy=multi-user.target
```

6. Edit `/etc/default/repmgrd` to change default settings. The following provides an example:

```
# default settings for repmgrd. This file is source by /bin/sh from
# /etc/init.d/repmgrd

# disable repmgrd by default so it won't get started upon installation
# valid values: yes/no
REPMGRD_ENABLED=yes

# configuration file (required)
REPMGRD_CONF="/etc/repmgr.conf"

# additional options
#REPMGRD_OPTS=“”
# user to run repmgrd as
#REPMGRD_USER=postgres

# repmgrd binary
#REPMGRD_BIN=/usr/bin/repmgrd

# pid file
REPMGRD_PIDFILE=/tmp/repmgrd.pid
```



`REPMGR_ENABLED` changed to `yes`, `REPMGRD_CONF` was uncommented and value changed to `"/etc/repmgrd.conf"` and `REPMGRD_PIDFILE` was uncommented and value changed to `/tmp/repmgrd.pid`.

7. Kill any previous instance of repmgrd that may be running:

```
ps -ef|grep “bin/repmgrd”|grep -v grep|xargs -t -i sudo kill {}
```

8. Enable and start the repmgrd service:

```
sudo systemctl enable repmgrd.service && sudo systemctl start repmgrd
```

9. Create a monitor and reconciliation service to support automatic failover. Create the script `/var/lib/postgresql/node_monitor.sh` with ownership to the Postgres user:

```
#!/bin/bash

# Script to detect a new primary and rejoin the cluster as standby if necessary

# Configuration variables
REPMGR_CONF="/etc/repmgr.conf"
PG_SERVICE="postgresql@15-main"
CHECK_INTERVAL=10 # Check every 10 seconds
REPMGR_CMD="/usr/bin/repmgr"
PG_CTL="/usr/bin/pg_ctl"
NODE_NAME="node1"

# Function to log messages
log_message() {
```

```
    echo "$(date '+%Y-%m-%d %H:%M:%S') - $1"
}

# Main loop
while true; do
    # Ensure PostgreSQL is running before checking the cluster status
    systemctl is-active --quiet $PG_SERVICE
    PG_STATUS=$?

    if [ $PG_STATUS -eq 0 ]; then
        # Check if there is another primary in the cluster
        OTHER_PRIMARY=$(sudo -u postgres $REPMGR_CMD -f $REPMGR_CONF cluster show 2>/dev/null
| grep -v "$NODE_NAME" | grep "primary"|grep "running as primary"|sed -n 's/.*host=\([^
]*\).*/\1/p')

        # Get current node's role
        CURRENT_ROLE=$(sudo -u postgres $REPMGR_CMD -f $REPMGR_CONF node check --role
2>/dev/null | grep -oP '(?<=\().*(?=\))'|awk '{print $NF}')

        if [[ ! -z "$OTHER_PRIMARY" && "$CURRENT_ROLE" == "primary" ]]; then
            log_message "Another primary detected in the cluster. Attempting to rejoin as
standby."

            # Ensure PostgreSQL is stopped before rejoining
            systemctl stop $PG_SERVICE
            sleep 5

            # Ensure PostgreSQL is fully stopped
            systemctl is-active --quiet $PG_SERVICE
            if [ $? -eq 0 ]; then
                log_message "Failed to stop PostgreSQL service. Skipping rejoin."
            else
                # Clone the data from the current primary and rejoin as standby
                sudo -u postgres $REPMGR_CMD -h $OTHER_PRIMARY -U repmgr -d repmgr -f $REPMGR_
CONF standby clone --force 2>/dev/null && \
                sudo systemctl start $PG_SERVICE && \
                sudo -u postgres $REPMGR_CMD -f $REPMGR_CONF standby register --force
2>/dev/null

                if [ $? -eq 0 ]; then
                    log_message "Node rejoined as standby successfully."
                else
                    log_message "Failed to rejoin node as standby."
                fi
            fi
        elif [[ -z "$CLUSTER_STATUS" ]]; then
            log_message "No other primary detected, or the current node is already a standby.
Nothing to do."
        fi
    else
        log_message "PostgreSQL service is not running. Skipping checks."
    fi
```

```
    # Wait for the next check
    sleep $CHECK_INTERVAL
done
```

10. Add execute permissions to the `/var/lib/postgresql/node_monitor.sh` file:

```
sudo chmod +x node_monitor.sh
```

11. Create a monitor service by creating the file `/etc/systemd/system/pg_node_monitor.service`:

```
[Unit]
Description=Automatic Rejoin Standby Service
After=network.target postgresql.service

[Service]
Type=simple
User=root
ExecStart=/var/lib/postgresql/node_monitor.sh
Restart=on-failure
RestartSec=5s

[Install]
WantedBy=multi-user.target
```

12. Enable and start the monitor service:

```
sudo systemctl enable pg_node_monitor && sudo systemctl start pg_node_monitor
```

To register Postgres node2 to the cluster:

1. Create the `/etc/repmgr.conf` file on Postgres node2:

```
cluster='emscluster'
node_id=2
node_name=postgresqlnode2
conninfo='host=<postgres node2 ip> user=repmgr dbname=repmgr connect_timeout=2'
data_directory='/var/lib/postgresql/15/main/'
pg_bindir='/usr/bin/'

log_file='/var/log/repmgr/repmgr.log'
log_level=DEBUG

failover=automatic
promote_command='/usr/bin/repmgr standby promote -f /etc/repmgr.conf'
follow_command='/usr/bin/repmgr standby follow -f /etc/repmgr.conf --upstream-node-id=%n'
```



Replace `<postgres node2 ip>` accordingly.

2. Create the log directory for repmgr:

```
sudo mkdir /var/log/repmgr
sudo chown -R postgres /var/log/repmgr
```

3. Stop the Postgres service:

```
sudo systemctl stop postgresql
```

4. Create a clone from Postgres node1:

```
sudo -u postgres repmgr -h <postgres node1 ip> -U repmgr -d repmgr -f /etc/repmgr.conf standby
clone --force
```



Replace `<postgres node1 ip>` accordingly.

5. Restart the Postgres service:

```
sudo systemctl start postgresql
```

6. Register the node as the standby:

```
sudo -u postgres /usr/bin/repmgr -f /etc/repmgr.conf standby register
```

7. Confirm registration:

```
sudo -u postgres /usr/bin/repmgr -f /etc/repmgr.conf cluster show
```

8. Create a systemd service config for repmgr by creating file /etc/systemd/system/repmgrd.service:

```
[Unit]
Description=PostgreSQL Replication Manager Daemon
After=network.target postgresql.service

[Service]
Type=forking
User=postgres
ExecStart=/usr/bin/repmgrd -f /etc/repmgr.conf --daemonize
PIDFile=/tmp/repmgrd.pid
ExecStop=/bin/kill -s TERM $(cat /tmp/repmgrd.pid)
ExecReload=/bin/kill -s HUP $(cat /tmp/repmgrd.pid)
Restart=on-failure
LimitNOFILE=16384

[Install]
WantedBy=multi-user.target
```

9. Edit `/etc/default/repmgrd` to change default settings. The following provides an example:

```
# default settings for repmgrd. This file is source by /bin/sh from
# /etc/init.d/repmgrd
```

```
# disable repmgrd by default so it won't get started upon installation
# valid values: yes/no
REPMGRD_ENABLED=yes

# configuration file (required)
REPMGRD_CONF="/etc/repmgr.conf"

# additional options
#REPMGRD_OPTS=""

# user to run repmgrd as
#REPMGRD_USER=postgres

# repmgrd binary
#REPMGRD_BIN=/usr/bin/repmgrd

# pid file
REPMGRD_PIDFILE=/tmp/repmgrd.pid
```



`REPMGR_ENABLED` changed to `yes`, `REPMGRD_CONF` was uncommented and value changed to `"/etc/repmgrd.conf"` and `REPMGRD_PIDFILE` was uncommented and value changed to `/tmp/repmgrd.pid`.

10. Kill any previous instance of repmgrd that may be running:

```
ps -ef|grep “bin/repmgrd”|grep -v grep|xargs -t -i sudo kill {}
```

11. Enable and start the repmgrd service:

```
sudo systemctl enable repmgrd.service && sudo systemctl start repmgrd
```

12. Create a monitor and reconciliation service to support automatic failover. Create the script `/var/lib/postgresql/node_monitor.sh` with ownership to the Postgres user:

```
#!/bin/bash

# Script to detect a new primary and rejoin the cluster as standby if necessary

# Configuration variables
REPMGR_CONF="/etc/repmgr.conf"
PG_SERVICE="postgresql@15-main"
CHECK_INTERVAL=10 # Check every 10 seconds
REPMGR_CMD="/usr/bin/repmgr"
PG_CTL="/usr/bin/pg_ctl"
NODE_NAME="node2"

# Function to log messages
log_message() {
       echo "$(date '+%Y-%m-%d %H:%M:%S') - $1"
}
```

```
# Main loop
while true; do
# Ensure PostgreSQL is running before checking the cluster status
systemctl is-active --quiet $PG_SERVICE
PG_STATUS=$?

if [ $PG_STATUS -eq 0 ]; then
       # Check if there is another primary in the cluster
       OTHER_PRIMARY=$(sudo -u postgres $REPMGR_CMD -f $REPMGR_CONF cluster show 2>/dev/null | grep
-v "$NODE_NAME" | grep "primary"|grep "running as primary"|sed -n 's/.*host=\([^ ]*\).*/\1/p')

       # Get current node's role
       CURRENT_ROLE=$(sudo -u postgres $REPMGR_CMD -f $REPMGR_CONF node check --role 2>/dev/null |
grep -oP '(?<=\().*(?=\))'|awk '{print $NF}')

       if [[ ! -z "$OTHER_PRIMARY" && "$CURRENT_ROLE" == "primary" ]]; then
               log_message "Another primary detected in the cluster. Attempting to rejoin as standby."

               # Ensure PostgreSQL is stopped before rejoining
               systemctl stop $PG_SERVICE
               sleep 5

               # Ensure PostgreSQL is fully stopped
               systemctl is-active --quiet $PG_SERVICE
               if [ $? -eq 0 ]; then
                       log_message "Failed to stop PostgreSQL service. Skipping rejoin."
               else
                       # Clone the data from the current primary and rejoin as standby
                       sudo -u postgres $REPMGR_CMD -h $OTHER_PRIMARY -U repmgr -d repmgr -f $REPMGR_CONF st
clone --force 2>/dev/null && \
                       sudo systemctl start $PG_SERVICE && \
                       sudo -u postgres $REPMGR_CMD -f $REPMGR_CONF standby register --force 2>/dev/null

                       if [ $? -eq 0 ]; then
                               log_message "Node rejoined as standby successfully."
                       else
                               log_message "Failed to rejoin node as standby."
                       fi
               fi
       elif [[ -z "$CLUSTER_STATUS" ]]; then
               log_message "No other primary detected, or the current node is already a standby. Nothing to
do."
               fi
       else
               log_message "PostgreSQL service is not running. Skipping checks."
       fi
       # Wait for the next check
       sleep $CHECK_INTERVAL
done
```

13. Add execute permissions to the `/var/lib/postgresql/node_monitor.sh` file:

```
sudo chmod +x node_monitor.sh
```

14. Create a monitor service by creating the file `/etc/systemd/system/pg_node_monitor.service`:

```
[Unit]
Description=Automatic Rejoin Standby Service
After=network.target postgresql.service

[Service]
Type=simple
User=root
ExecStart=/var/lib/postgresql/node_monitor.sh
Restart=on-failure
RestartSec=5s

[Install]
WantedBy=multi-user.target
```

15. Enable and start the monitor service:

```
sudo systemctl enable pg_node_monitor && sudo systemctl start pg_node_monitor
```

To register Postgres witness server:

1. Install Postgres 15 and Replication Manager. Postgres recommends this replication tool:

```
sudo apt install -y --no-install-recommends curl ca-certificates apt-transport-https

sudo install -d /usr/share/postgresql-common/pgdg

sudo curl -o /usr/share/postgresql-common/pgdg/apt.postgresql.org.asc --fail
https://www.postgresql.org/media/keys/ACCC4CF8.asc

sudo sh -c 'echo "deb [signed-by=/usr/share/postgresql-common/pgdg/apt.postgresql.org.asc]
https://apt.postgresql.org/pub/repos/apt $(lsb_release -cs)-pgdg main" >
/etc/apt/sources.list.d/pgdg.list'

sudo apt update

sudo apt install -y postgresql-15 postgresql-15-repmgr
```

2. Modify postgresql.conf to add replication parameters. Change the following settings on `/etc/postgresql/15/main/postgresql.conf` with the indicated values:

```
listen_addresses = 'localhost,<ip of the witness server'
shared_preload_libraries = 'repmgr'
```

3. Set up Postgres access to the replication user. Add the following to `/etc/postgresql/15/main/pg_hba.conf`:

```
host all all 127.0.0.1/32 trust
local replication repmgr trust
host replication repmgr 127.0.0.1/32 trust
host replication repmgr <postgres node1 ip>/32 trust
```

```
host replication repmgr <postgres node2 ip>/32 trust
host replication repmgr <witness ip>/32 trust
local repmgr repmgr trust
host repmgr repmgr 127.0.0.1/32 trust
host repmgr repmgr <postgres node1 ip>/32 trust
host repmgr repmgr <postgres node2 ip>/32 trust
host repmgr repmgr <witness ip>/32 trust
host all all 0.0.0.0/0 scram-sha-256
```



Replace `<postgres node1 ip>`, `<postgres node2 ip>`, and `<witness ip>` accordingly.

4. Restart the postgresql service:

```
sudo systemctl restart postgresql
```

5. Create the repmgr user and database. Run the following to create the repmgr user and database on Postgres:

```
sudo -u postgres createuser -s repmgr
sudo -u postgres createdb repmgr -O repmgr
```

6. Create the log directory for repmgr:

```
sudo mkdir /var/log/repmgr
sudo chown -R postgres /var/log/repmgr
```

7. Create the `/etc/repmgr.conf` file:

```
cluster='emscluster'
node_id=3
node_name='witness1'
conninfo='host=<witness node ip> user=repmgr dbname=repmgr connect_timeout=2'
data_directory='/var/lib/postgresql/15/main' # Not used but required by repmgr
pg_bindir='/usr/bin/'
log_file='/var/log/repmgr/repmgr.log'
```



Replace `<witness node ip>` accordingly.

8. Register as witness informing the host of the primary node:

```
sudo -u postgres /usr/bin/repmgr -f /etc/repmgr.conf witness register -h <postgres node1 ip>
```



Replace `<postgres node1 ip>` accordingly.

9. Create a systemd service config for repmgr by creating file `/etc/systemd/system/repmgrd.service`:

```
[Unit]
Description=PostgreSQL Replication Manager Daemon
After=network.target postgresql.service

[Service]
Type=forking
User=postgres
ExecStart=/usr/bin/repmgrd -f /etc/repmgr.conf --daemonize
PIDFile=/tmp/repmgrd.pid
ExecStop=/bin/kill -s TERM $(cat /tmp/repmgrd.pid)
ExecReload=/bin/kill -s HUP $(cat /tmp/repmgrd.pid)
Restart=on-failure LimitNOFILE=16384

[Install]
WantedBy=multi-user.target
```

10. Edit `/etc/default/repmgrd` to change default settings. It should look like this:

```
# default settings for repmgrd. This file is source by /bin/sh from
# /etc/init.d/repmgrd
# disable repmgrd by default so it won't get started upon installation
# valid values: yes/no
REPMGRD_ENABLED=yes

# configuration file (required)
REPMGRD_CONF="/etc/repmgr.conf"

# additional options
#REPMGRD_OPTS=""

# user to run repmgrd as
#REPMGRD_USER=postgres

# repmgrd binary
#REPMGRD_BIN=/usr/bin/repmgrd

# pid file
REPMGRD_PIDFILE=/tmp/repmgrd.pid
```



`REPMGR_ENABLED` changed to `yes`, `REPMGRD_CONF` was uncommented and value changed to `"/etc/repmgrd.conf"` and `REPMGRD_PIDFILE` was uncommented and value changed to `/tmp/repmgrd.pid`.

11. Kill any previous instance of repmgrd that might be running:

```
ps -ef|grep “bin/repmgrd”|grep -v grep|xargs -t -i sudo kill {}
```

12. Enable and start the repmgrd service:

```
sudo systemctl enable repmgrd.service && sudo systemctl start repmgrd
```

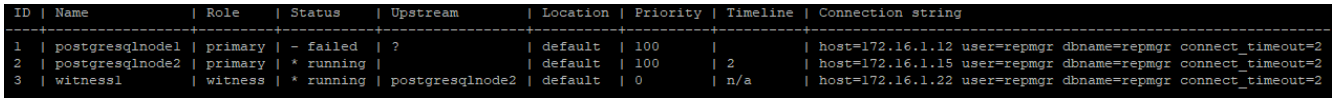
To test DB failover:

Stop the Postgres service on the primary node or shut down the primary node. By default, the health check happens every 10 seconds. Before promoting itself to the primary node, the secondary node checks if the primary is down at least six times. Therefore, failover takes 60 seconds. You can configure this value, but the default 60 seconds is an acceptable timeout or amount of downtime.

To check the failover status, run the following command on the secondary node:

```
sudo -u postgres /usr/bin/repmgr -f /etc/repmgr.conf cluster show
```

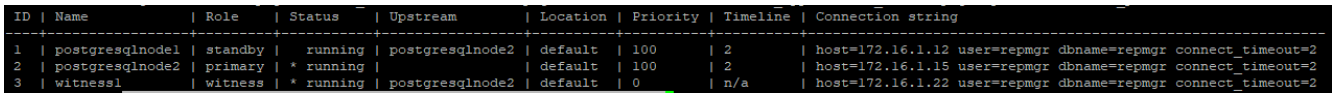
Postgressqlnode2 is promoted to the primary node:



```
ID | Name           | Role    | Status    | Upstream       | Location | Priority | Timeline | Connection string
---+----------------+---------+-----------+----------------+----------+----------+----------+-----------------------------------------------------------------
1  | postgresqlnode1 | primary | - failed  | ?              | default  | 100      |          | host=172.16.1.12 user=repmgr dbname=repmgr connect_timeout=2
2  | postgresqlnode2 | primary | * running |                | default  | 100      | 2        | host=172.16.1.15 user=repmgr dbname=repmgr connect_timeout=2
3  | witness1        | witness | * running | postgresqlnode2 | default  | 0        | n/a      | host=172.16.1.22 user=repmgr dbname=repmgr connect_timeout=2
```

Start the postgresql service on Postgressqlnode1 or turn on Postgressqlnode1. It is added as a standby. Run the following command to check the DB cluster status:

```
sudo -u postgres /usr/bin/repmgr -f /etc/repmgr.conf cluster show
```



```
ID | Name           | Role    | Status    | Upstream       | Location | Priority | Timeline | Connection string
---+----------------+---------+-----------+----------------+----------+----------+----------+-----------------------------------------------------------------
1  | postgresqlnode1 | standby |   running | postgresqlnode2 | default  | 100      | 2        | host=172.16.1.12 user=repmgr dbname=repmgr connect_timeout=2
2  | postgresqlnode2 | primary | * running |                | default  | 100      | 2        | host=172.16.1.15 user=repmgr dbname=repmgr connect_timeout=2
3  | witness1        | witness | * running | postgresqlnode2 | default  | 0        | n/a      | host=172.16.1.22 user=repmgr dbname=repmgr connect_timeout=2
```

To configure EMS HA:

1. After the database cluster is up and running, configure EMS HA:
   a. On both nodes, do the following:
      i. Download the `forticlientems_7.4.3.XXXX.bin` file from the Fortinet Support site.
      ii. Run `sudo -i` to log in to the shell with root privileges.
      iii. Change permissions and add execute permissions to the installation file:

      ```
      chmod +x forticlientems_7.4.3.XXXX.bin
      ```

   b. On the primary node, install EMS:
      i. Set `umask` to 022 on file `/etc/login.defs` if the existing `umask` setting is more restrictive.
      ii. Install EMS:

      ```
      ./forticlientems_7.4.3.XXXX.bin -- --db_host "<database server 1 IP address or
      FQDN>,<database 2 IP address or FQDN>" --db_user postgres --db_pass <postgres
      password> --skip_db_install --allowed_hosts '*' --enable_remote_https
      ```

      Run the installer to and from any directory other than `/tmp`. Running the installer to or from `/tmp` causes issues.

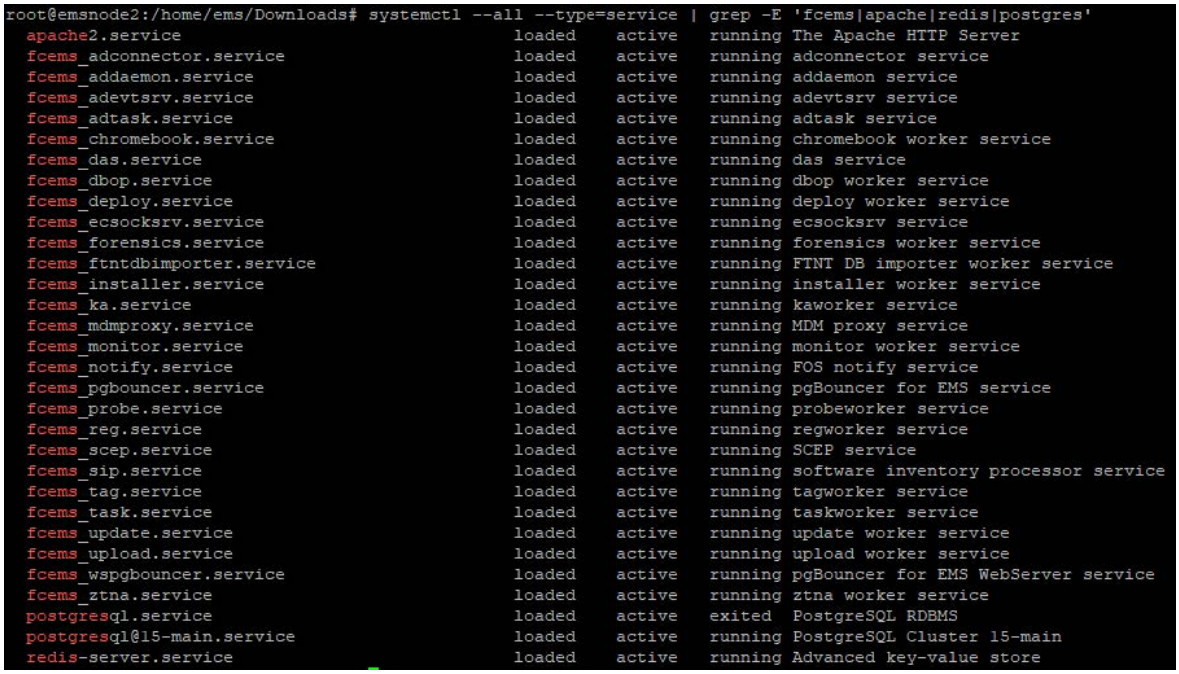
      

      In `db_host`, configure the IP addresses with your database server IP addresses or FQDNs.

      Replace `<postgres password>` with the Postgres user password that you configured in the last step of To configure Postgres node 1: on page 90.

iii. After installation completes, check that all EMS services are running by entering the following command:

```
systemctl --all --type=service | grep -E 'fcems|apache|redis|postgres'
```



The output shows that postgresql.service status displays as `exited`. This is the expected status. EMS does not create this service, which only exists to pass commands to version-specific Postgres services. It displays as part of the output as the command filters for all services that contain "postgres" in the name.

c. On the secondary node, install EMS:

i. Set `umask` to 022 if the existing `umask` setting is more restrictive.

ii. Install EMS:

```
./forticlientems_7.4.3.XXXX.bin -- --db_host "<Postgres node 1 IP address>,<Postgres node 2 IP address>" --db_user postgres --db_pass <postgres password> --skip_db_install --skip_db_deploy --allowed_hosts '*' --enable_remote_https
```

Run the installer to and from any directory other than `/tmp`. Running the installer to or from `/tmp` causes issues.



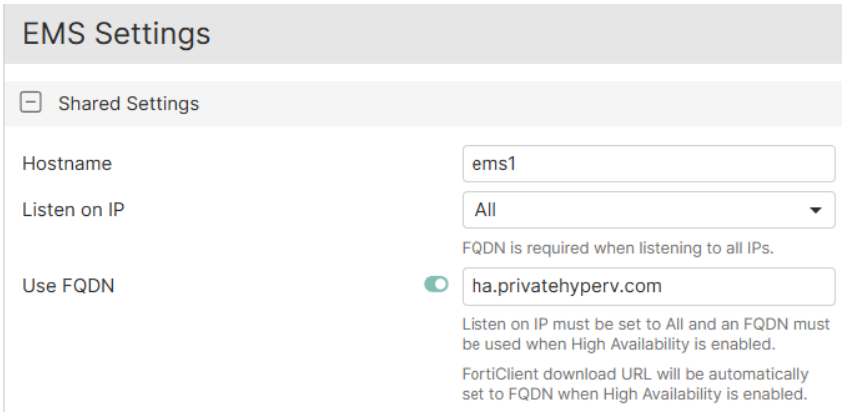
In `db_host`, configure the IP addresses with your database server IP addresses or FQDNs.

Replace `<postgres password>` with the Postgres user password that you configured in the last step of To configure Postgres node 1: on page 90.

iii. After installation completes, check that EMS services are running by entering the following command. On the secondary EMS, only `fcems_monitor`, `fcems_pgbouncer`, `fcems_wspgbouncer`, and `redis-server` services should be running:

```
systemctl --all --type=service | grep -E 'fcems|apache|redis|postgres'
```

d. After installation on both nodes is complete, do the following:
   i. On the primary node, log in to EMS. License EMS as Starting FortiClient EMS and logging in on page 113 describes. EMS HA requires a single license for the primary node and the secondary node(s). You only need to add the license to the primary node.
   ii. Go to *System Settings > EMS Settings*.
   iii. Under *Shared Settings*, confirm that *Listen on IP* is set to *All*.
   iv. Enable *Use FQDN*.
   v. Enter the desired FQDN.



   vi. In the *Custom hostname* field, enter a virtual IP address (VIP) that is configured in the FortiGate load balancer (LB) as the VIP for EMS. In this example, the VIP is 172.16.1.50.
   vii. Configure the *High Availability Keep Alive Internal* field with a value between 5 and 30 seconds.
   viii. Go to *Dashboard > Status*. Confirm that the *System Information* widget displays that EMS is running in HA mode. If running in HA mode, the widget also lists the HA primary and secondary nodes and their statuses.

2. Configure a FortiGate as an LB for EMS HA:
   a. Create a health check:
      i. Go to *Policy & Objects > Health Check*. Click *Create New*.
      ii. For *Type*, select *TCP*.
      iii. In the *Interval* field, enter 10.
      iv. In the *Timeout* field, enter 2.
      v. In the *Retry* field, enter 3.
      vi. In the *Port* field, enter 8013. Click *OK*.
   b. Create a virtual server:
      i. Go to *Policy & Objects* and create a virtual server.
      ii. Configure the fields as follows:

Field	Value
Virtual server IP	VIP that you configured in step 4.f. In this example, the VIP is 172.16.1.50.
Virtual server port	10443
Load Balancing method	*First Alive*

Field	Value
Health check	Monitor that you configured.
Network Type	*TCP*

iii. Under *Real Servers*, select *Create New*.
iv. In the *IPv4 address* field, enter the primary EMS node IP address. In this example, it is 192.168.1.10.
v. In the *Port* field, enter 10443.
vi. In the *Max connections* field, enter 0.
vii. For *Mode*, select *Active*.
viii. Create a real server for the secondary EMS node. Click *Save*.

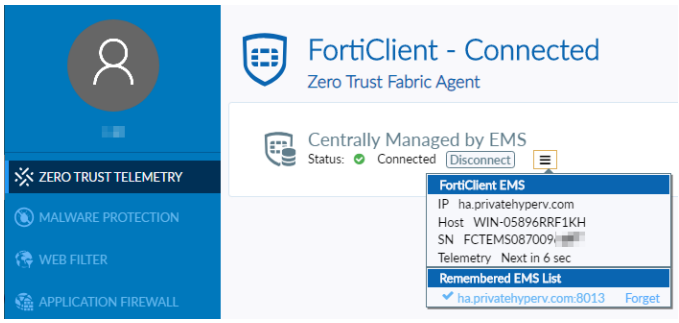
c. Repeat steps i-ix to create five additional virtual servers. The additional servers use ports 443, 8013, 8015, 8443, and 8871, but otherwise have identical settings to the first virtual server created. If you have enabled Chromebook management, create a virtual server for port 8443. Similarly, if you require importing an ACME certificate, create a virtual server for port 80.
d. Create a security policy that includes the LB virtual server as a destination address:
i. Go to *Policy & Objects > Firewall Policy*.
ii. Click *Create New*.
iii. Configure the *Incoming Interface* and *Outgoing Interface* fields. The outgoing interface connects to the primary EMS node.
iv. For *Source*, select *all*.
v. In the *Destination* field, select ports 10443, 443, 8013, 8015, 8443, and 8871.
vi. For *Service*, select *ALL*.
vii. For *Inspection Mode*, select *Proxy-based*.
viii. Save the policy.
ix. If the EMS nodes are in different subnets, repeat these steps to configure a policy for the secondary EMS node. In this example, the nodes are in the same subnet, so you do not need to add a separate policy for the secondary EMS.

3. After the FortiGate LB configuration is complete, you can access EMS using the VIP configured in the FortiGate LB. If after initially installing EMS 7.4.3 you need to upgrade to a newer build, repeat steps 4.a.-c. with the new installation file.

To validate the HA configuration:

1. Go to *Deployment & Installers > Manage Deployment*. Create a deployment package to deploy FortiClient to endpoints. See Adding a FortiClient installer on page 230.
2. On an endpoint, download the deployment package from the download link.
3. Install FortiClient on the endpoint.
4. Ensure that FortiClient can register to the EMS server successfully using the FQDN.
5. Simulate HA by stopping FortiClient Endpoint Management Server Monitor Service on the primary node. Ensure that the secondary node is now the EMS primary server.

6. Ensure that FortiClient can still register to the EMS successfully using the FQDN.



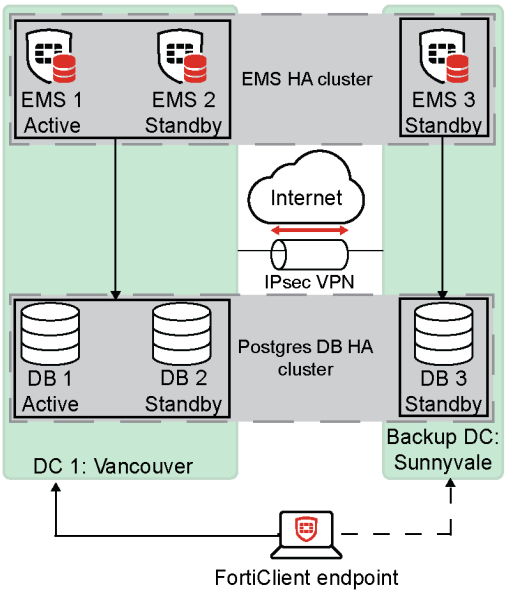
Installing EMS for HA georedundancy

EMS high availability (HA) supports georedundancy, where EMS nodes in an HA cluster are geographically distant. Each datacenter also includes PostgreSQL (Postgres) external databases (DB). The setup of a geographically distributed infrastructure allows you to ensure redundancy in case of failure on a datacenter. The following describes this EMS HA georedundant configuration:

- Failover: active-passive enabled
- EMS HA cluster can have three or four members
- PostgreSQL HA cluster can have three or four members
- Between two geographically distributed locations with passive nodes
- EMS and Postgres nodes enabled and ready to become active

This setup requires each EMS node and its associated Postgres DB to be in the same geographical location. Having the EMS and its associated Postgres DB in different geographic locations may result in performance degradation.

The following shows an example topology for this deployment:



The following describes the example topology for this deployment. EMS HA georedundancy works with configurations that do not exactly match these details. This document provides these details for reference purposes:

- Two geographically distant datacenters. In this example, DC1 is located in Vancouver, while DC2 is located in Sunnyvale. Each datacenter has the following components:
  - Three EMS nodes: two in DC1 and one in DC2. The EMS nodes are members of the same HA cluster and the configuration syncs between the nodes.
  - One Postgres DB node. The DB does not communicate with the DB in the other datacenter. Each DB receives configuration data from the EMS in its datacenter.
  - Each EMS and its Postgres DB are hosted on a VMware ESXi server.
- Site-to-site IPsec VPN connection
- 1 GB dedicated recommended site-to-site bandwidth
- FortiClient endpoints. The endpoint can access the EMS nodes in either datacenter. Typically, it accesses EMS 1. When failover occurs, it accesses EMS 2 or EMS 3.



When EMS is in a geographically distributed HA cluster and failover occurs, the failover may cause the primary EMS node and primary Postgres DB to be in different geographical locations. This may cause performance degradation. You may need to manually intervene to ensure that the primary EMS and primary Postgres nodes are in the same geographical locations.

To configure EMS georedundant HA:

1. Verify that your configuration meets all EMS, Postgres, and Docker Swarm network requirements. See Required services and ports on page 27.
2. Configure the Postgres Docker cluster and install EMS HA. See Installing EMS HA with Postgres HA using Bitnami Docker on page 83.
3. (Optional) Configure load balancing using FortiOS for EMS traffic management. See Fabric connection setup using FortiGate as a load balancer on page 670.
4. Verify the Postgres Docker cluster status:

```
:~/Downloads$ docker exec -it pg-2 bash /opt/bitnami/scripts/postgresql-repmgr/entrypoi
nt.sh repmgr -f /opt/bitnami/repmgr/conf/repmgr.conf service status
postgresql-repmgr 22:54:08.10 INFO  ==>
postgresql-repmgr 22:54:08.11 INFO  ==> Welcome to the Bitnami postgresql-repmgr container
postgresql-repmgr 22:54:08.11 INFO  ==> Subscribe to project updates by watching https://github.com/bitnami/conta
iners
postgresql-repmgr 22:54:08.11 INFO  ==> Submit issues and feature requests at https://github.com/bitnami/containe
rs/issues
postgresql-repmgr 22:54:08.11 INFO  ==> Upgrade to Tanzu Application Catalog for production environments to acces
s custom-configured and pre-packaged software components. Gain enhanced features, including Software Bill of Mate
rials (SBOM), CVE scan result reports, and VEX documents. To learn more, visit https://bitnami.com/enterprise
postgresql-repmgr 22:54:08.11 INFO  ==>

 ID | Name | Role    | Status    | Upstream | repmgrd | PID | Paused? | Upstream last seen
----+------+---------+-----------+----------+---------+-----+---------+--------------------
 1001 | pg-1 | primary | * running |          | running | 256 | no      | n/a
 1002 | pg-2 | standby |   running | pg-1     | running | 1   | no      | 1 second(s) ago
```

5. Verify that all EMS services are running by entering the following command on the primary EMS node:
   `systemctl --all --type=service | grep -E 'fcems|apache|redis|postgres'`

```
:~$ systemctl --all --type=service | grep -E 'fcems|apache|redis|postgres'
apache2.service                                  loaded    active   running The Apache HTTP Server
fcems_adconnector.service                        loaded    active   running adconnector service
fcems_addaemon.service                           loaded    active   running addaemon service
fcems_adevtsrv.service                           loaded    active   running adevtsrv service
fcems_adtask.service                             loaded    active   running adtask service
fcems_chromebook.service                         loaded    active   running chromebook worker service
fcems_das.service                                loaded    active   running das service
fcems_dbop.service                               loaded    active   running dbop worker service
fcems_deploy.service                             loaded    active   running deploy worker service
fcems_ecsocksrv.service                          loaded    active   running ecsocksrv service
fcems_forensics.service                          loaded    active   running forensics worker service
fcems_ftntdbimporter.service                     loaded    active   running FTNT DB importer worker service
fcems_installer.service                          loaded    active   running installer worker service
fcems_ka.service                                 loaded    active   running kaworker service
fcems_mdmproxy.service                           loaded    active   running MDM proxy service
fcems_monitor.service                            loaded    active   running monitor worker service
fcems_notify.service                             loaded    active   running FOS notify service
fcems_pgbouncer.service                          loaded    active   running pgBouncer for EMS service
fcems_probe.service                              loaded    active   running probeworker service
fcems_reg.service                                loaded    active   running regworker service
fcems_scep.service                               loaded    active   running SCEP service
fcems_sip.service                                loaded    active   running software inventory processor service
fcems_tag.service                                loaded    active   running tagworker service
fcems_task.service                               loaded    active   running taskworker service
fcems_update.service                             loaded    active   running update worker service
fcems_upload.service                             loaded    active   running upload worker service
fcems_wspgbouncer.service                        loaded    active   running pgBouncer for EMS WebServer service
fcems_ztna.service                               loaded    active   running ztna worker service
postgresql.service                               loaded    active   exited  PostgreSQL RDBMS
redis-server.service                             loaded    active   running Advanced key-value store
```

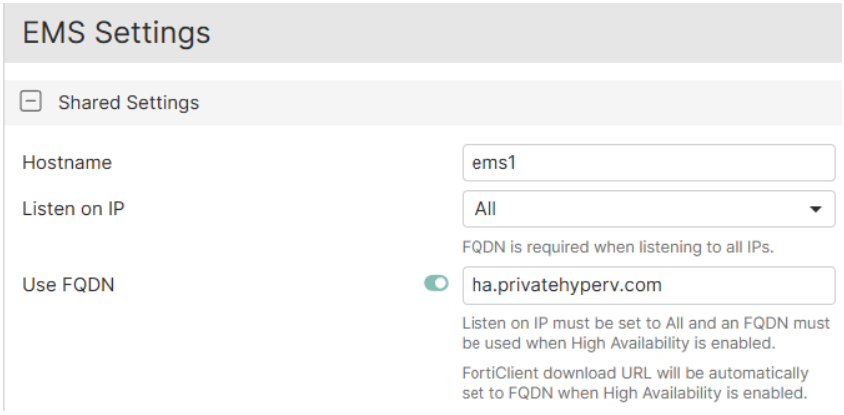
6. Verify that EMS services are running by entering the following command on the secondary EMS nodes. Only fcems_monitor, fcems_pgbouncer, and redis-server services are running on the secondary node:

```
systemctl --all --type=service | grep -E 'fcems|apache|redis|postgres'
```

```
:~/Downloads$ systemctl --all --type=service | grep -E 'fcems|apache|redis|postgres'
apache2.service                                  loaded    inactive dead    The Apache HTTP Server
fcems_adconnector.service                        loaded    inactive dead    adconnector service
fcems_addaemon.service                           loaded    inactive dead    addaemon service
fcems_adevtsrv.service                           loaded    inactive dead    adevtsrv service
fcems_adtask.service                             loaded    inactive dead    adtask service
fcems_chromebook.service                         loaded    inactive dead    chromebook worker service
fcems_das.service                                loaded    inactive dead    das service
fcems_dbop.service                               loaded    inactive dead    dbop worker service
fcems_deploy.service                             loaded    inactive dead    deploy worker service
fcems_ecsocksrv.service                          loaded    inactive dead    ecsocksrv service
fcems_forensics.service                          loaded    inactive dead    forensics worker service
fcems_ftntdbimporter.service                     loaded    inactive dead    FTNT DB importer worker service
fcems_installer.service                          loaded    inactive dead    installer worker service
fcems_ka.service                                 loaded    inactive dead    kaworker service
fcems_mdmproxy.service                           loaded    inactive dead    MDM proxy service
fcems_monitor.service                            loaded    active   running monitor worker service
fcems_notify.service                             loaded    inactive dead    FOS notify service
fcems_pgbouncer.service                          loaded    active   running pgBouncer for EMS service
fcems_probe.service                              loaded    inactive dead    probeworker service
fcems_reg.service                                loaded    inactive dead    regworker service
fcems_scep.service                               loaded    inactive dead    SCEP service
fcems_sip.service                                loaded    inactive dead    software inventory processor service
fcems_tag.service                                loaded    inactive dead    tagworker service
fcems_task.service                               loaded    inactive dead    taskworker service
fcems_update.service                             loaded    inactive dead    update worker service
fcems_upload.service                             loaded    inactive dead    upload worker service
fcems_wspgbouncer.service                        loaded    active   running pgBouncer for EMS WebServer service
fcems_ztna.service                               loaded    inactive dead    ztna worker service
postgresql.service                               loaded    active   exited  PostgreSQL RDBMS
redis-server.service                             loaded    active   running Advanced key-value store
```

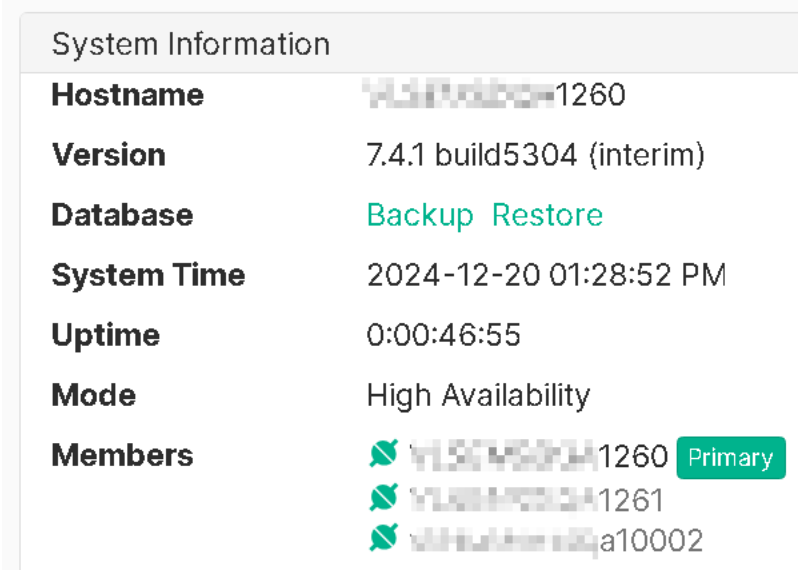
7. Log in to EMS to verify the setup is complete:
   a. On the primary node, log in to EMS. License EMS as Starting FortiClient EMS and logging in on page 113 describes. EMS HA requires a single license for the primary node and the secondary node(s). You only need to add the license to the primary node.
   b. Go to *System Settings > EMS Settings*.
   c. Under *Shared Settings*, enable *Use FQDN*.

d. Enter the desired FQDN.



e. Go to *System Settings > EMS Settings*. Configure the *High Availability Keep Alive Internal* field with a value between 5 and 30 seconds.

f. Go to *Dashboard > Status*. Confirm that the *System Information* widget displays that EMS is running in HA mode. If running in HA mode, the widget also lists the HA primary and secondary nodes and their statuses.

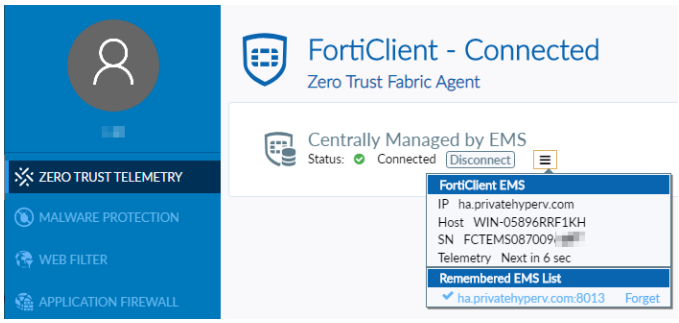


g. In *System Settings > EMS Settings*, you can configure the *High Availability Keep Alive Interval* in seconds.

To validate the HA configuration:

1. Go to *Deployment & Installers > Manage Deployment*. Create a deployment package to deploy FortiClient to endpoints. See Adding a FortiClient installer on page 230.
2. On an endpoint, download the deployment package from the download link.
3. Install FortiClient on the endpoint.
4. Ensure that FortiClient can register to the EMS server successfully using the FQDN.
5. Simulate HA by stopping FortiClient Endpoint Management Server Monitor Service on the primary node. Ensure that the secondary node is now the EMS primary server.

6. Ensure that FortiClient can still register to the EMS successfully using the FQDN.



Testing georedundancy and failover with a test endpoint is recommended before deployment to a production environment.

Installation parameters

The following provides a list of parameters that the EMS install commands support:

Parameter	Description
`allowed_hosts`	Enable remote host access.
`das_cache_engine`	Specify DAS cache engine, such as simple.
`db_host`	Remote database (DB) hostname.
`db_pass`	Remote DB password.
`db_port`	Port that remote DB uses to communicate with EMS.
`db_prefix`	Used when FortiClient Cloud uses an external DB. Prepend this value to the DBs that FortiClient Cloud uses to ensure unique DB names.
`db_user`	Remote DB username.
`elastic_api_key`	Having EMS connect to the Elasticsearch (ES) cluster using an API encoded key, rather than username and password, is considered best practice. Provide the encoded version of the key to EMS.
`elastic_ca_path`	If the ES cluster is set up to strictly check for a client certificate, you must provide the CA certificate to EMS. This must be a fully qualified path to the CA certificate file. Store the file in a location outside of `/opt/forticlientems` and be readable by the forticlientems user or group. For example, you may configure the following: `--elastic_ca_path /data/certs/es_ca.crt`

Parameter	Description
elastic_hosts	ES server IP address and port that ES uses to communicate with EMS in <ES server IP address>:<port> format. If you have multiple primary ES server nodes, provide their <IP address>:<port> in a comma-separated list with no whitespace in between. For example, you may configure the following: `elastic_hosts "node1.local:8000,node2.local:8000,node3.local:8000"`
elastic_password	Password for ES user created for EMS.
elastic_user	Username to use to connect to ES. If you provide both an API key and username and password, EMS prefers to use the API key and ignores the username and password.
enable_event_feature	Enable EMS services required for using the new DB for storing and querying events.
enable_remote_https	Enable remote HTTPS access to EMS.
fileserver_port	Customize webserver ports.
http_port	
https_port	
internal_db_port	PostgreSQL port to set for executing the DB deployment or upgrade (remote or locally).
is_paas	Only used when using EMS with a cloud DB. This parameters tells the installer that this is a special DB and needs special handling.
redis_cluster_hosts	Redis cluster hosts names.
redis_host	Redis hostname.
redis_password	Redis password.
redis_port	Port that Redis uses to communicate with EMS.
redis_username	Redis username.
scep_public_hostname	Specify the FQDN or hostname accessible by mobile endpoints to pull the ZTNA certificate from the SCEP server running on EMS.
skip_db_deploy	Skip express DB deployment.
skip_db_install	Skip express DB install.
skip_event_feature_local_install_local_install	Skip event worker local installation.

Starting FortiClient EMS and logging in

FortiClient EMS runs as a service on Linux computers.

The post-install setup wizard facilitates rapid EMS setup for users immediately following installation, prioritizing license provisioning. You must have a license to proceed and use EMS.

EMS requires you to authenticate via FortiCloud for license entitlement immediately after install. You must log in to EMS, validate your FortiCloud account, and EMS must retrieve the license for you to proceed further. Access to EMS is contingent on the validation and connection of your FortiCloud account information.

In air-gapped instances, EMS allows you to upload a license file. However, this only applies in rare cases. In the majority of deployments, you must provide FortiCloud account information and EMS retrieves the license directly from FortiCloud.

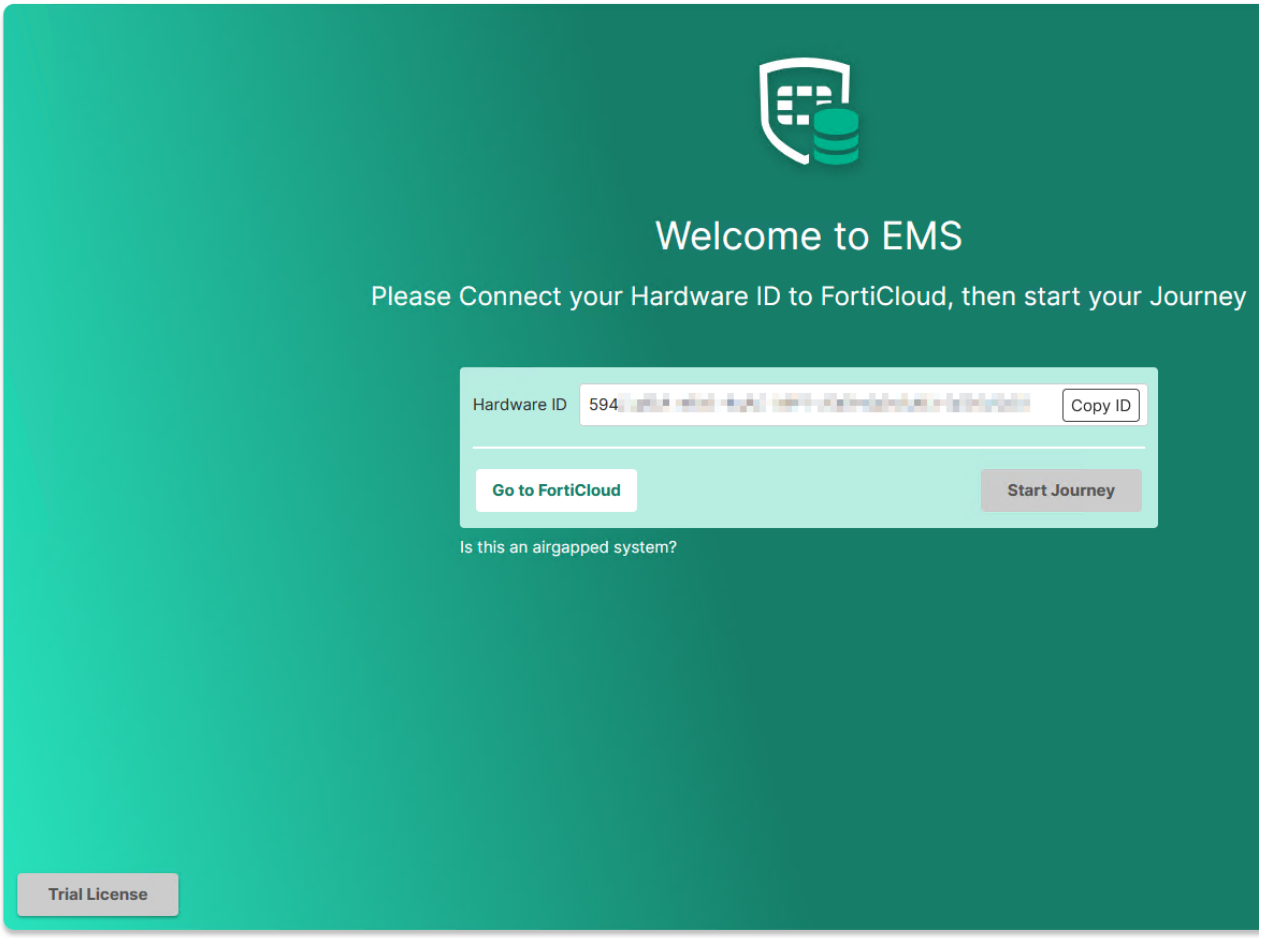
The post-install setup wizard streamlines the EMS post-install setup process.

To license EMS using the post-install setup wizard:

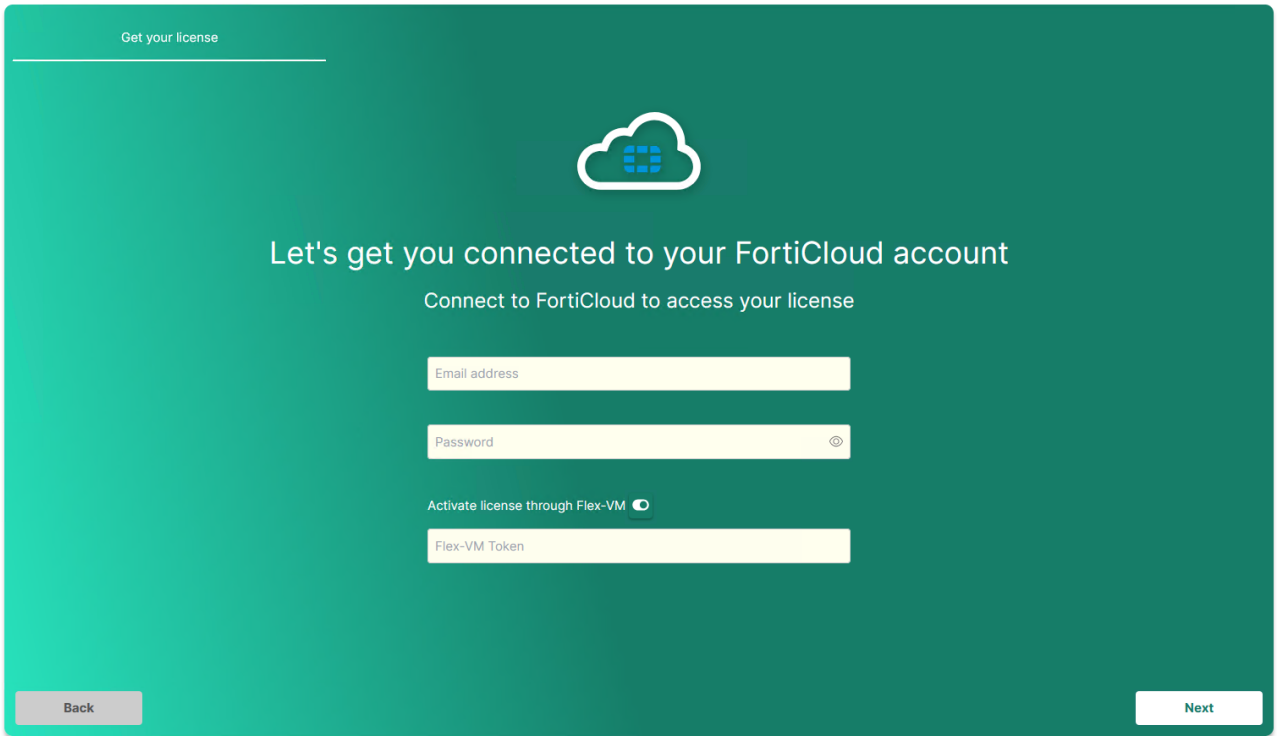
1. After installing EMS, launch it for the first time. EMS displays a *Welcome to EMS* page that displays the hardware ID of the machine that EMS is installed on. Registering and licensing EMS requires the hardware ID. Do one of the following:
   - If you have a registered license, click *Start Journey*.
   - If you do not have a registered license, click *Go to FortiCloud*. This opens the FortiCloud website, where you can register and license your EMS instance. See Licensing EMS by logging in to FortiCloud on page 118 for details on licensing EMS.
   - To try EMS on a temporary basis, click *Trial License* in the bottom left. This prompts you to enter your email address and password for trial license registration.
   - If you are using an air-gapped system or isolated network where EMS cannot access the Internet, click *Is this an airgapped system?* The wizard displays a page where you can manually upload a license file to activate EMS.



You can obtain the license file in FortiCloud by selecting *Products > My Assets*, clicking the EMS serial number, and then *License File Download*.

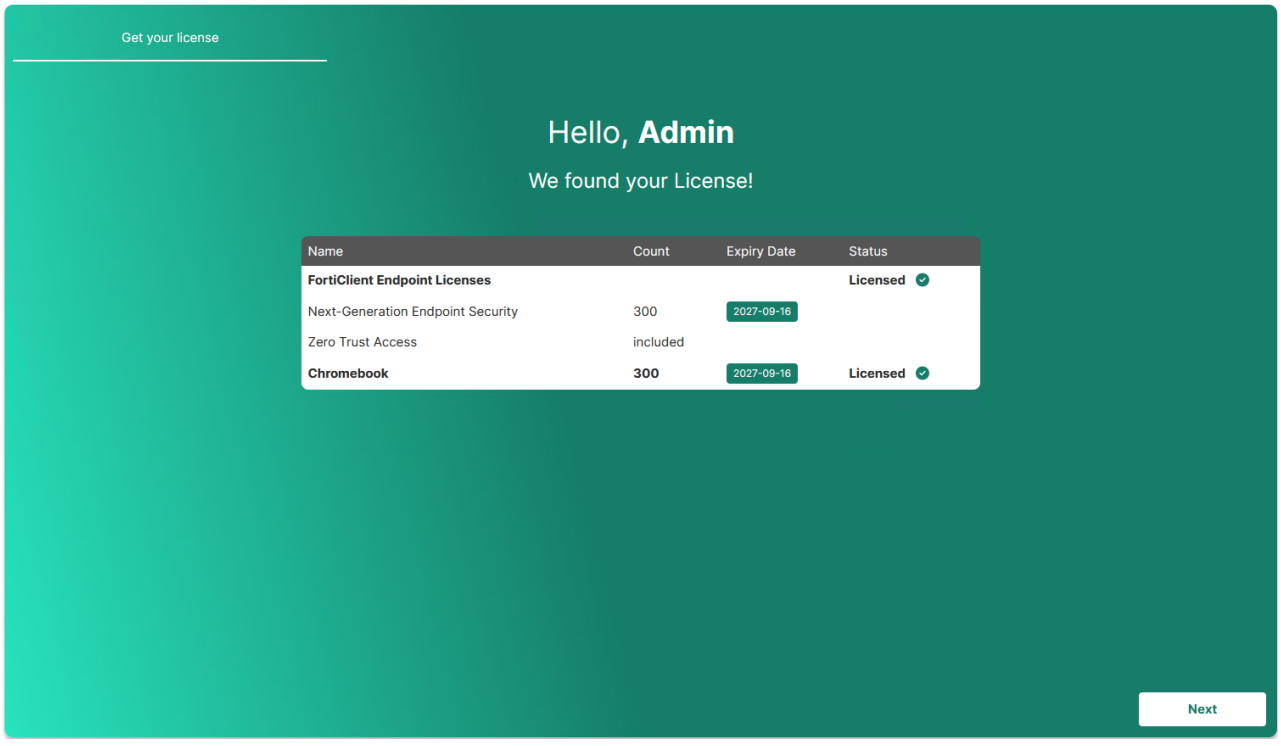


2. On the *Let's get you connected to your FortiCloud account* page, do one of the following, then click *Next*:
   - Enter your FortiCloud account credentials to retrieve your EMS license from FortiCloud.
   - Activate your EMS using FortiFlex licensing by enabling *Activate license through Flex-VM* and entering your FortiCloud account credentials and FortiFlex token.



If you enter incorrect credentials or do not have licensing registered to your account, the install wizard displays a page with *Reset password* and *Create new FortiCloud account* buttons. You can use these buttons to access FortiCloud for assistance.

3. EMS connects to FortiCloud to retrieve the license. The wizard displays the retrieved license type and entitlements and displays them. Click *Next*.



4. The wizard prompts you to enter a preferred hostname for the EMS server. If desired, configure a custom hostname, then click *Next*.
5. The wizard prompts you to enter a new admin username. Configure as desired, then click *Next*.
6. Configure a password for the new user. Click *Finish*. You can now access EMS with these credentials.

Configuring EMS after installation

You can configure a fully qualified domain name (FQDN) for EMS.

FortiClient's connection to EMS is critical to managing endpoint security. Managing this is relatively easy for internal devices. For external devices or devices that may leave the internal network, you must consider how to maintain this connection. FortiClient can connect to EMS using an IP address or FQDN. An FQDN is preferable for the following reasons:

- Easy to migrate EMS to a different IP address
- Easy to migrate to a different EMS instance
- Flexible to dynamically resolve the FQDN

The third reason is particularly valuable for environments where devices may be internal or external from day to day. When using an FQDN, you can configure your internal DNS servers to resolve the FQDN to the EMS internal IP address and register your external IP address with public DNS servers. You must then configure the device with your external IP address to forward communication received on port 8013 to your EMS internal IP address. This allows your external clients to leverage a virtual IP address on the FortiGate so that they can reach EMS, while allowing internal clients to use the same FQDN to reach EMS directly.

Alternatively, you can use a private IP address for the connection. This configuration requires external clients to establish a VPN connection to reach the EMS (VPN policies permitting). This configuration can be problematic if all endpoints need an urgent update but some are disconnected from VPN at that time.

You can also configure FortiClient EMS so that you can access it remotely using a web browser instead of the GUI.

To enable remote access to FortiClient EMS:

1. Go to *System Settings > EMS Settings*.
2. Enable *Use FQDN*. Enter the desired FQDN.
3. If desired, enable Remote HTTPS Access.
4. If desired, in the *Custom Hostname* field, enter the hostname or IP address. Otherwise, EMS uses the *Pre-defined Hostname*.
5. If desired, select *Redirect HTTP request to HTTPS*. If this option is enabled, if you attempt to remotely access EMS at *http://<server_name>*, this automatically redirects to *https://<server_name>*.
6. Click *Save*.

To remotely access FortiClient EMS:

- To access EMS from the EMS server, visit `https://localhost`
- To access the server remotely, use the server's hostname: `https://<server_name>`
  Ensure you can ping `<server_name>` remotely. You can achieve this by adding it into a DNS entry or to the Windows hosts file. You may need to modify the Windows firewall rules to allow the connection.

Licensing FortiClient EMS

There are several licensing options available with FortiClient EMS. You can use these licenses to manage Windows, macOS, Linux, iOS, Android, or Chromebook endpoints. For information on the different license types available, see License types on page 23.

There are two ways to activate, upgrade, or renew a FortiClient EMS license:

- Licensing EMS by logging in to FortiCloud on page 118: You can log in to your FortiCloud account to activate EMS using that account. Once an EMS license expires, EMS uses the FortiCloud account to obtain a new license file, if available on that account. You can use this method to apply a trial or paid license to EMS. This is the primary licensing method for EMS.
- Uploading a license file on page 124: You can upload a license file to EMS. This functions in the same way as EMS versions prior to 6.2.0. You must use this backup licensing method only if you cannot license EMS by logging into FortiCare.

You must activate an EMS license before you can manage and provision any endpoints with EMS.



Although the option to upload a license file is available in the EMS GUI, FortiCloud does not provide EMS 7.4 license files. You cannot use this option to activate, upgrade, or renew an EMS 7.4 license.



If you attempt to license EMS with a license that only later versions support, a *Future License* error appears. For example, thise error displays if you attempt to license EMS 6.4.2 or an earlier version with a zero trust network access license.

Licensing EMS by logging in to FortiCloud

You must license FortiClient EMS to use it for endpoint management and provisioning.

Applying a trial license to FortiClient EMS

To apply a trial license to FortiClient EMS:

The following steps assume that you have already acquired an EMS installation file from FortiCloud or a Fortinet sales representative for evaluation purposes and installed EMS.

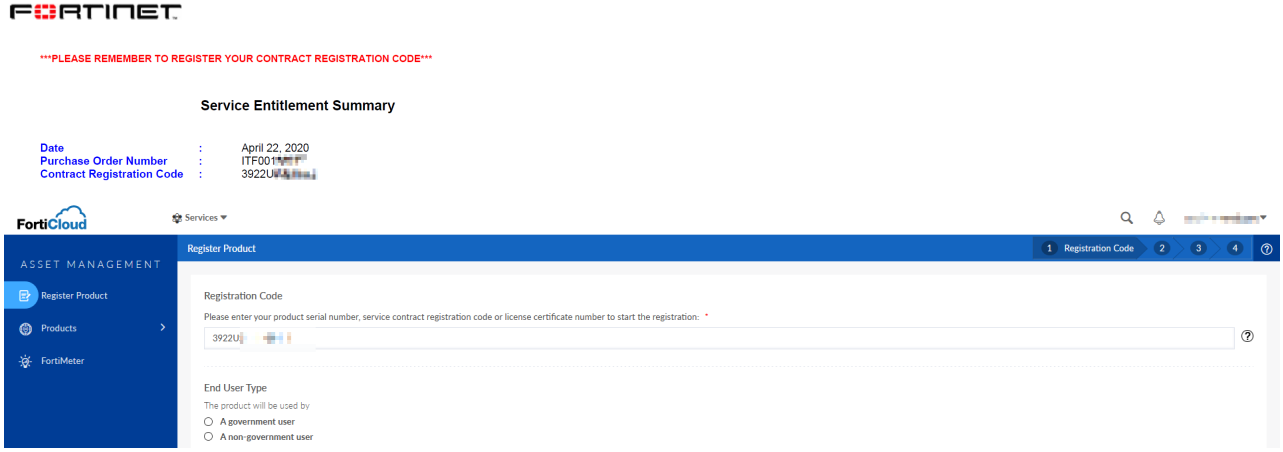
1. In EMS, in the *License Information* widget, click *Add* beside *FortiCloud Account*.
2. In the *FortiCloud Registration* dialog, enter your FortiCloud account credentials. If you do not have a FortiCloud account, create one.
3. Read and accept the license agreement terms.
4. Click *Login & Sync License Now*. If your FortiCloud account is eligible for an EMS trial license, the *License Information* widget updates with the trial license information, and you can now manage three Windows, macOS, Linux, iOS, and Android endpoints indefinitely.

Applying paid licenses to FortiClient EMS

To apply a paid license to FortiClient EMS:

The following steps assume that you have already purchased and acquired your EMS and FortiClient licenses from a Fortinet reseller.

1. Log in to your FortiCloud account on Customer Service & Support.
2. Go to *Asset Management*.
3. Click *Register More*.
4. In the *Registration Code* field, enter the *Contract Registration Code* from your service registration document. Configure other fields as required, then click *Next*.

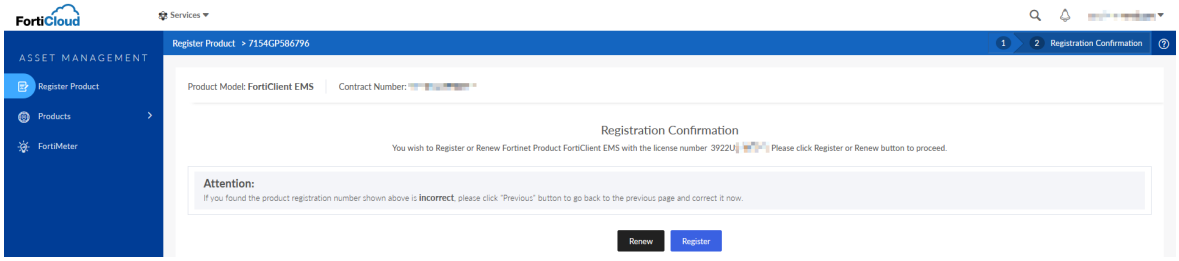


5. Do one of the following:
   - If this is the first license that you are applying to this EMS server, do the following:
     i. Click *Register*.
     ii. In the *Hardware ID* field, enter the hardware ID found in *Dashboard > Status > License Information widget > Config License* in EMS. If you register the license prior to installing EMS, you must enter the hardware ID after installation. Configure other fields as required, then click *Next*.
     iii. Complete the registration, then click *Confirm*.
     iv. In EMS, go to *Dashboard > Status > License Information* widget *> Config License*.
     v. For *License Source*, select *FortiCare*.
     vi. In the *FortiCloud Account* field, enter your FortiCloud account ID or email address.
     vii. In the *Password* field, enter your FortiCloud account password.

viii. Click *Login & Update License*. Once your account information is authenticated, EMS updates *Configure License* with the serial number and license information that it retrieved from FortiCloud.

- As describes, you can apply multiple license types to the same EMS server. For example, if you have already applied an EPP license to your EMS server, you can apply another license type, such as a ZTNA license, to the same EMS server. If desired, add another license type:
  i. On the *Registration Confirmation* page, when applying an additional license type, you must select *Renew* on the contract registration screen, regardless of the license types of the first and subsequent licenses. Selecting *Renew* combines the new license with any existing licenses for the EMS server and allows you to add the new license type to EMS while retaining previously applied license(s).

  When applying an additional license type to EMS, selecting *Register* instead of *Renew* creates an additional license file instead of combining the new license with the existing license(s). You cannot apply the new and existing licenses to the same EMS server.



ii. In the *Serial Number* field, enter the EMS serial number or select the EMS instance from the list. You can find the serial number in *Dashboard > Status > License Information widget > Configure License* in EMS. Click *Next*.

iii. Complete the registration, then click *Confirm*.

EMS reports the following information to FortiCare. FortiCloud displays this information in its dashboard and asset management pages:

- EMS software version
- Number of FortiClient endpoints currently actively licensed under and being managed by this EMS
- Endpoint license expiry statuses. You can use this information to plan license renewals.

Using a second license to extend the license expiry date does not increase the number of licensed clients. To increase the number of licensed clients, contact Fortinet Support for a co-term contract.

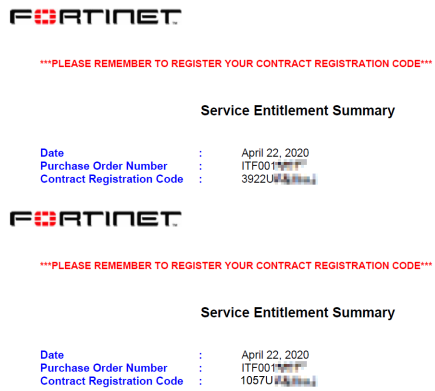
If you previously activated another license with the same EMS hardware ID, you receive a duplicated UUID error. In this case, contact Customer Support to remove the hardware ID from the old license.

To apply multiple paid licenses to FortiClient EMS:

You may want to apply multiple paid licenses of the same type to at the same time. For example, if you want EMS to manage 525 ZTNA endpoints, you can purchase two ZTNA licenses: one for 500 endpoints, and another for 25 endpoints. In this scenario, you need to register the licenses at the same time.

The following steps assume that you have already purchased and acquired your EMS and FortiClient licenses from a Fortinet reseller.

1. Log in to your FortiCloud account on Customer Service & Support.
2. Go to *Register Product*.
3. In the *Registration Code* field, enter the *Contract Registration Code*s from your service registration documents. Separate the codes with a comma. For example, to register the 3922U and 1057U codes in the following screenshots, you would enter 3922U,1057U in the *Registration Code* field. Configure other fields as required, then click *Next*.


FORTINET

PLEASE REMEMBER TO REGISTER YOUR CONTRACT REGISTRATION CODE

Service Entitlement Summary

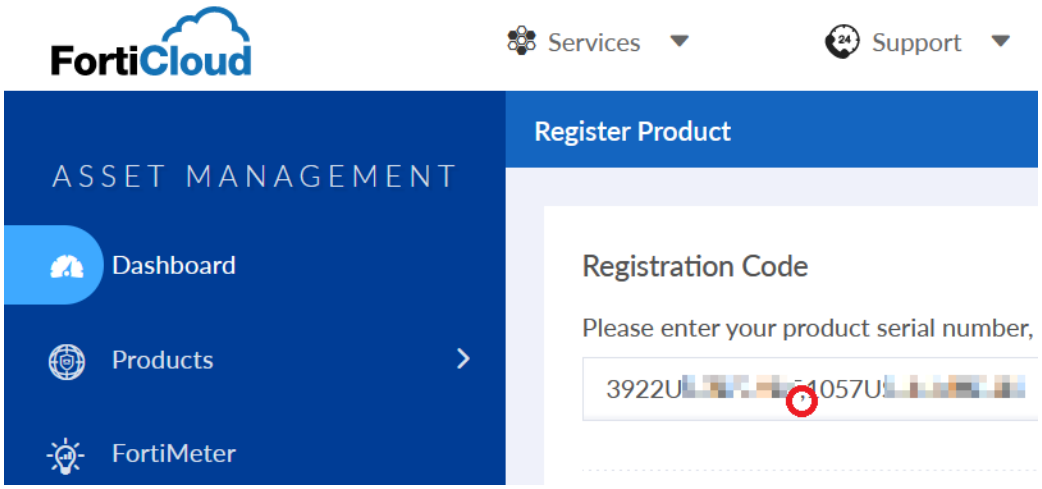
Date : April 22, 2020
Purchase Order Number : ITF001
Contract Registration Code : 3922U

FORTINET

PLEASE REMEMBER TO REGISTER YOUR CONTRACT REGISTRATION CODE

Service Entitlement Summary

Date : April 22, 2020
Purchase Order Number : ITF001
Contract Registration Code : 1057U



4. Do one of the following:
   a. If these are the first licenses that you are applying to this EMS server, do the following:
      i. Click *Register*.
      ii. In the *Hardware ID* field, enter the hardware ID found in *Dashboard > Status > License Information widget > Configure License* in EMS. If you register the licenses prior to installing EMS, you must enter the hardware ID after installation. Configure other fields as required, then click *Next*.
      iii. Complete the registration, then click *Confirm*.

iv. In EMS, go to *Dashboard > Status > License Information widget > Configure License*.
v. For *License Source*, select *FortiCare*.
vi. In the *FortiCloud Account* field, enter your FortiCloud account ID or email address.
vii. In the *Password* field, enter your FortiCloud account password.
viii. Click *Login & Update License*. Once your account information is authenticated, EMS updates the *Configure License* page with the serial number and license information that it retrieved from FortiCloud.

b. As described in , you can apply multiple license types to the same EMS server. For example, if you have already applied an EPP license to your EMS server, you can apply other license types, such as a ZTNA license, to the same EMS server. If desired, add another license type:
   i. On the *Registration Confirmation* page, when applying an additional license type, you must select *Renew* on the contract registration screen, regardless of the license types of the first and subsequent licenses. Selecting *Renew* combines the new licenses with any existing licenses for the EMS server and allows you to add the new license types to EMS while retaining previously applied license(s).



When applying an additional license types to EMS, selecting *Register* instead of *Renew* creates an additional license file instead of combining the new licenses with the existing license(s). You cannot apply the new and existing licenses to the same EMS server.

   ii. In the *Serial Number* field, enter the EMS serial number or select the EMS instance from the list. You can find the serial number in *Dashboard > Status > License Information widget > Configure License* in EMS. Click *Next*.
   iii. Complete the registration, then click *Confirm*.

EMS reports the following information to FortiCare. FortiCloud displays this information in its dashboard and asset management pages:

- EMS software version
- Number of FortiClient endpoints currently actively licensed under and being managed by this EMS
- Endpoint license expiry statuses. You can use this information to plan license renewals.



Using a second license to extend the license expiry date does not increase the number of licensed clients. To increase the number of licensed clients, contact Fortinet Support for a co-term contract.



If you previously activated another license with the same EMS hardware ID, you receive a duplicated UUID error. In this case, contact Customer Support to remove the hardware ID from the old license.

Importing an EMS license via FortiFlex

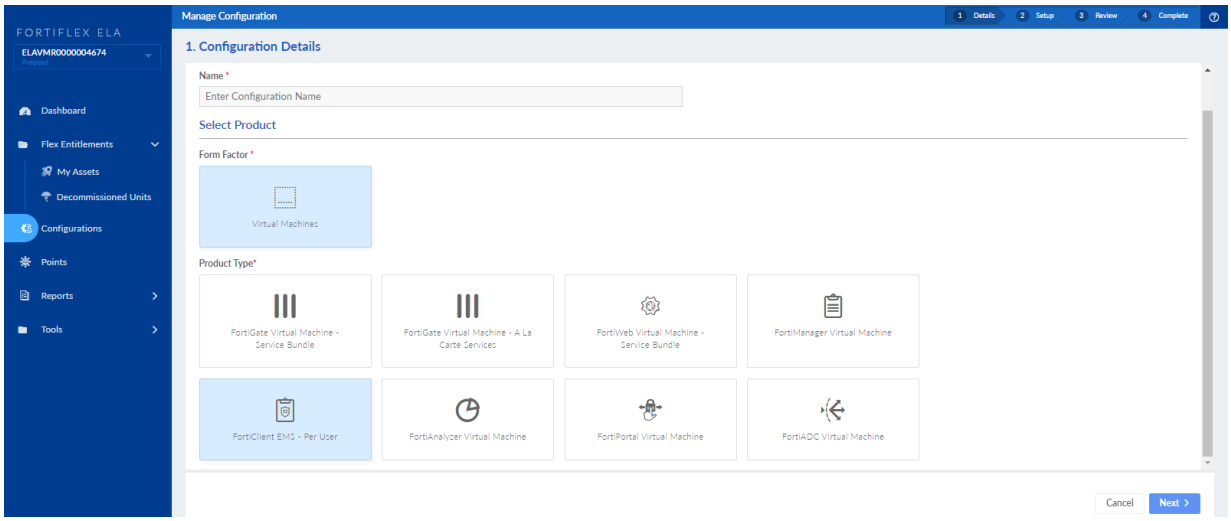
FortiFlex is a subscription service to configure and manage virtual machine (VM) usage entitlements. You can now import an EMS license via a FortiFlex VM token. You can easily manage entitlements (license seats

and expiry) from the FortiFlex portal. You can monitor point usage on the FortiFlex portal, which helps to keep track of your costs and billings.

FortiFlex only supports on-premise EMS and per-endpoint licensing.

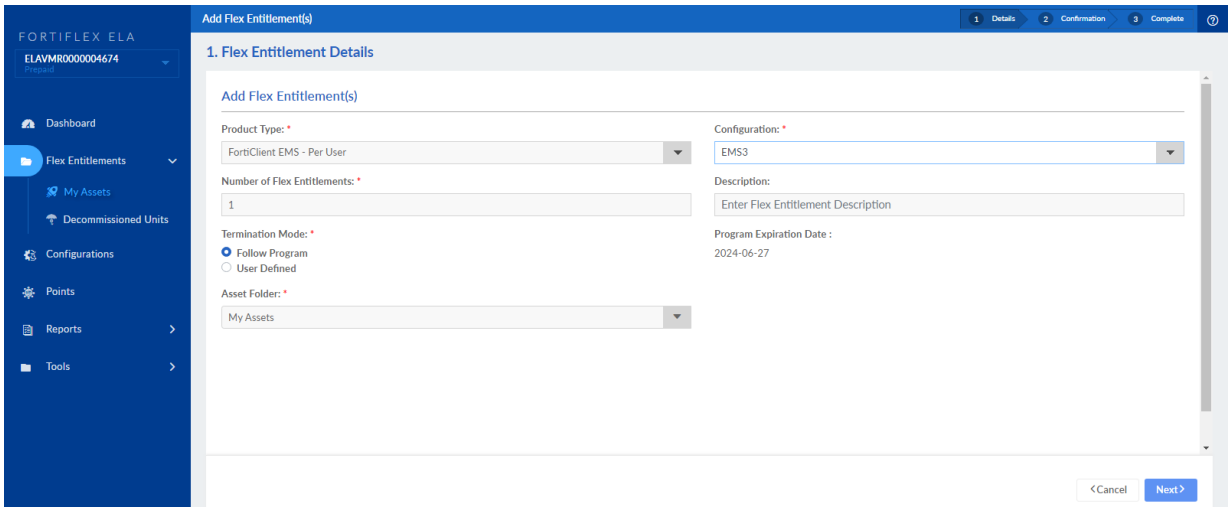
To import an EMS license via a FortiFlex VM token:

1. Register a contract for the FortiFlex program on your FortiCloud account. For FortiFlex ordering information, see the FortiFlex Program Ordering Guide.
2. Create a configuration for EMS:
   a. In the FortiFlex portal, go to *Services* > *FortiFlex* > *Configurations*.
   b. Under *Form Factor*, select *Virtual Machines*.
   c. Under *Product Type*, select *FortiClient EMS - Per Endpoint*.
   d. Configure the desired name, then click *Next*.



   e. Assign license seats as desired, then proceed to save. FortiFlex creates the configuration.
3. Create an entitlement for EMS:
   a. Go to *Flex Entitlements*.
   b. Click *New Flex Entitlement*.
   c. From the *Product Type* dropdown list, select *FortiClient EMS - Per Endpoint*.
   d. Under *Termination Mode*, select one of the following:
      i. To set the license expiry date to be the same as the FortiFlex program expiry, select *Follow Program*.
      ii. To manually set the expiry date, select *User Defined*.
   e. From the *Asset Folder* dropdown list, select the folder to create the entitlement under.
   f. From the *Configuration* dropdown list, select the configuration that you created.

g. Configure other fields as desired, then submit to create the entitlement.



4. Import the EMS license using a FortiFlex token:
   a. In the FortiFlex portal, go to *Flex Entitlements*.
   b. Select the EMS entitlement.
   c. Copy the license file token.
   d. In EMS, on the *Dashboard* > *License Information* widget, click *Add* beside *FortiCloud Account*.
   e. Enter your credentials.
   f. Enable *Activate license through Flex-VM*.
   g. In the *Flex-VM Token* field, enter the token.
   h. Click *Login & Sync License Now*. FortiCloud updates the entitlement with the EMS hardware ID. You can update the license seats and expiry in the FortiFlex portal by editing the configuration and entitlement. EMS automatically imports the new license file after syncing with FortiGuard. You can also manually sync the FortiCloud account connected to EMS.

Uploading a license file

You must use this backup licensing method only if you cannot license EMS by logging into FortiCare.

Contact Fortinet Support to activate, upgrade, or renew your FortiClient EMS license. After you have the license file, you can add it to FortiClient EMS.

To upload a license file for activation, upgrade, or renewal:

1. Go to *Dashboard* > *Status* > *License Information widget* > *Configure License*.
2. For *License Source*, select *File Upload*.
3. Click *Browse* and locate the license key file.
4. Click *Upload*.

License status

The *Dashboard > Status > License Information* widget displays your license statuses. EMS supports multiple licenses, including separate licenses for Telemetry and endpoint protection and management, for FortiClient Cloud Sandbox (SaaS) integration, and for Chromebook endpoint management. Each license's status can change. The options are:

License status	Description
Unlicensed	If you just installed FortiClient EMS, EMS is unlicensed by default. Log in to your FortiCloud account or upload a license file to update the license status.
Non-expired license	You can upgrade the license on your FortiCloud account.
Expired license	You can renew the license on your FortiCloud account. You have ten days after the license expiry date to renew the license. During this grace period, the *License Information* widget displays the expiry date, which has already passed, and FortiClient EMS functions as if the license has not expired. FortiClient EMS also displays a daily notification that the license has expired and that you are currently using FortiClient EMS as part of the ten day grace period. After ten days, FortiClient EMS reverts to unlicensed mode for that license.

After applying a trial license to EMS, you can purchase a license and register the EMS installation on your FortiCloud account as To apply a paid license to FortiClient EMS: on page 119 describes, then click *Sync License Now* in *Dashboard > Status > License Information widget > Configure License* to apply a paid license to EMS.

Help with licensing

For licensing issues with FortiClient EMS, contact the licensing team at Fortinet Technical Assistance Center (TAC):

- Phone: +1-866-648-4638
- Technical support: support.fortinet.com/

Uninstalling FortiClient EMS

To uninstall EMS:

Run the following command in the Linux terminal with sudo privileges:

```
sudo apt remove -y forticlientems
```

Installation and setup for managing Chromebooks

The following sections only apply if you plan to use FortiClient EMS to manage Chromebooks:

Google Admin Console setup

This section describes how to add and configure the FortiClient Web Filter extension on Chromebooks enrolled in the Google domain.

Following is a summary of how to set up the Google Admin console:

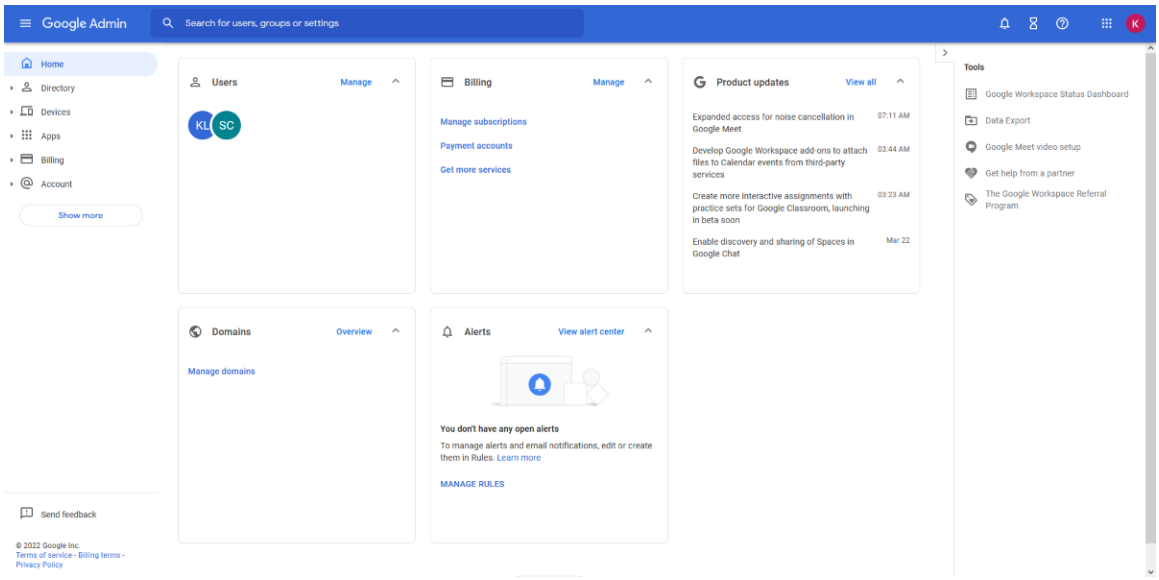
1. Log into the Google Admin console. See Logging into the Google Admin console on page 126.
2. Add the FortiClient Web Filter extension. See Adding the FortiClient Web Filter extension on page 127.
3. Configure the FortiClient Web Filter extension. See Configuring the FortiClient Web Filter extension on page 127.
4. Add the root certificate. See Adding root certificates on page 129.
5. Disable access to Chrome developer tools.
6. Disallow incognito mode.
7. Disallow guest mode.
8. Block Chrome task manager.
9. Verify the FortiClient Web Filter extension.



If you are using another Chromebook extension that uses external rendering servers, the FortiClient Web Filter settings may be bypassed. Check with the third-party extension vendor if this is the case.

Logging into the Google Admin console

Log into the Google Admin console using your Google domain admin account. The Admin console displays.

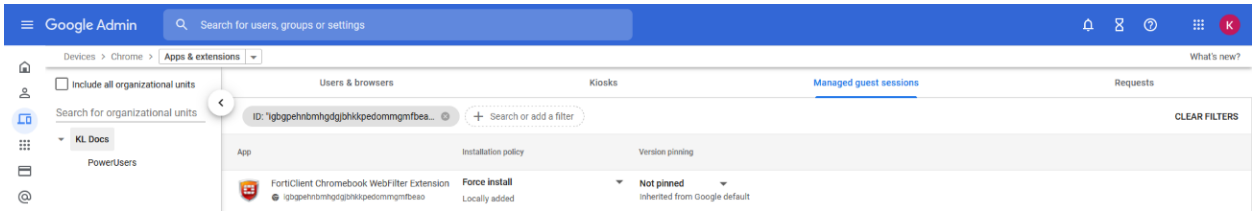


Adding the FortiClient Web Filter extension

FortiClient EMS software is unavailable for public use. You can only enable the feature using the following extension ID: igbgpehnbmhgdgjbhkkpedommgmfbeao

To add the FortiClient Web Filter extension:

1. In the Google Admin console, go to *Devices* > *Chrome* > *Settings* > *Users & browsers* > *Managed Guest Session Settings*.
2. On the left, select the organization that contains the desired users or enrolled browsers. To select all users and browsers, select the top-level organization. Otherwise, select a child.
3. From the breadcrumbs, select the dropdown list beside *Settings*, and select *Apps & extensions*.
4. In the bottom right corner, hover over the + icon, then select *Add Chrome app or extension by ID*.
5. In the *Extension ID* field, enter the following extension ID: igbgpehnbmhgdgjbhkkpedommgmfbeao.
6. Click *SAVE*. The extension displays, with the Force install installation policy.



Configuring the FortiClient Web Filter extension

You must configure the FortiClient Chromebook Web Filter extension to enable the Google Admin console to communicate with FortiClient EMS.

FortiClient EMS hosts the services that assign endpoint profiles of web filtering policies to groups in the Google domain. FortiClient EMS also handles the logs and web access statistics that the FortiClient Web Filter extensions send.

FortiClient EMS is the profile server.

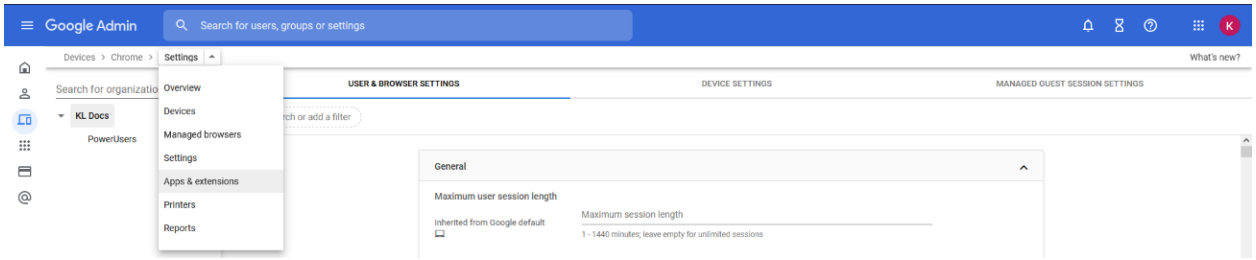
For instructions on configuring the extension for connection to FortiClient Cloud, see Managing Chromebooks with FortiClient Cloud.

To configure the FortiClient Web Filter extension:

1. In FortiClient EMS, locate the server name and port by going to *System Settings > EMS Settings*.
2. Create a text file that contains either set of the following text, depending on your deployment mode:

Deployment Mode	Text	Example
Regular	`{ "ProfileServerUrl": { "Value": "https://< ProfileServer >:< port for Profile Server >"} }`	`{ "ProfileServerUrl": { "Value": "https://ems.mydomain.com:8443"} }`
Multi-tenancy	`{ "ProfileServerUrl": { "Value": "https://< ProfileServer >:< port for Profile Server >"} }, "SiteName": { "Value": "SiteName"} }`	`{ "ProfileServerUrl": { "Value": "https://ems.mydomain.com:8443"} }, "SiteName": { "Value": "Site1"} }`

3. In the Google Admin console, go to *Devices > Chrome > Settings > Users & browsers*.
4. On the left, select the organization that contains the desired users or enrolled browsers. To select all users and browsers, select the top-level organization. Otherwise, select a child.
5. From the breadcrumbs, select the dropdown list beside *Settings*, and select *Apps & extensions*.



6. Click a domain or organizational unit (OU), then click the FortiClient Web Filter extension.
7. In the right pane, under *Policy for extensions*, paste the JSON content from step 2.

8. Click *SAVE*.
9. Go to *Devices* > *Chrome* > *Apps & extensions* to view your configured Chrome applications.

Adding root certificates

Communication with the FortiClient Chromebook Web Filter extension

The FortiClient Chromebook Web Filter extension communicates with FortiClient EMS using HTTPS connections. The HTTPS connections require an SSL certificate. You must obtain an SSL certificate and add it to FortiClient EMS to allow the extension to trust FortiClient EMS.

If you use a public SSL certificate, you only need to add the public SSL certificate to FortiClient EMS. See Adding an SSL certificate to FortiClient EMS on page 648.

However, if you prefer to use a certificate not from a common CA, you must add the SSL certificate to FortiClient EMS and push your certificate's root CA to the Google Chromebooks. Otherwise, the HTTPS connection between the FortiClient Chromebook Web Filter extension and FortiClient EMS does not work. See Uploading root certificates to the Google Admin console on page 131.

Communication with FortiAnalyzer for logging

This section applies only if you are sending logs from FortiClient to FortiAnalyzer. If you are not sending logs, skip this section.



Sending logs to FortiAnalyzer requires you enable ADOMs in FortiAnalyzer and add FortiClient EMS to FortiAnalyzer. You can add FortiClient EMS as a device to the FortiClient or Fabric ADOM in FortiAnalyzer. See the *FortiAnalyzer Administration Guide*.

FortiClient supports logging to FortiAnalyzer. If you have a FortiAnalyzer and configure FortiClient to send logs to FortiAnalyzer, a FortiAnalyzer CLI command must be enabled and an SSL certificate is required to support communication between the FortiClient Web Filter extension and FortiAnalyzer.

If you use a public SSL certificate, you only need to add the public SSL certificate to FortiAnalyzer. See Adding an SSL certificate to FortiAnalyzer.

However, if you prefer to use a certificate not from a common CA, you must add the SSL certificate to FortiAnalyzer and push your certificate's root CA to the Google Chromebooks. Otherwise, the HTTPS connection between the FortiClient Chromebook Web Filter extension and FortiAnalyzer does not work. See Uploading root certificates to the Google Admin console on page 131.



The FortiAnalyzer IP address should be specified in the SSL certificate. If you are using a public SSL certificate, the FortiAnalyzer IP address can be assigned to *Common Name* or *Alternative Name*. If you are using a self-signed (nonpublic) SSL certificate, your certificate's *Subject Alternative Name* must include `IP:<FortiAnalyzer IP>`.

You must use the FortiAnalyzer CLI to add HTTPS-logging to the allow-access list in FortiAnalyzer. This command is one step in the process that allows FortiAnalyzer to receive logs from FortiClient.

In FortiAnalyzer CLI, enter the following command:

```
config system interface
   edit "port1"
      set allowaccess https ssh https-logging
   next
end
```

Adding an SSL certificate to FortiAnalyzer

To add an SSL certificate to FortiAnalyzer:

1. In FortiAnalyzer, go to *System Settings > Certificates > Local Certificates*.
2. Click *Import*. The *Import Local Certificate* dialog appears.
3. In the *Type* list, select *Certificate* or *PKCS #12 Certificate*.
4. Beside *Certificate File*, click *Browse* to select the certificate.
5. Enter the password and certificate name.
6. Click *OK*.

Selecting a certificate for HTTPS connections

To select a certificate for HTTPS connections:

1. In FortiAnalyzer, go to *System Settings > Admin > Admin Settings*.
2. From the *HTTPS & Web Service Certificate* dropdown list, select the certificate to use for HTTPS connections, and click *Apply*.

Summary of where to add certificates

The following table summarizes where to add certificates to support communication with the FortiClient Web Filter extension and FortiAnalyzer.

Scenario	Certificate and CA	Where to add certificates
Allow the FortiClient Chromebook Web Filter extension to trust EMS	Public SSL certificate	Add SSL certificate to FortiClient EMS.
	SSL certificate not from a common CA	• Add SSL certificate to FortiClient EMS. • Add your certificate's root CA to the Google Admin console.
Allow the FortiClient Chromebook Web Filter extension to trust FortiAnalyzer for logging	Public SSL certificate	Add SSL certificate to FortiAnalyzer.
	SSL certificate not from a common CA	• Add SSL certificate to FortiAnalyzer. • Add your certificate's root CA to the Google Admin console.

Uploading root certificates to the Google Admin console

To upload root certificates to the Google Admin console:

1. In the Google Admin console, go to *Device Management > Network > Certificates (root certificate) (crt certificate)*.
2. Add the root certificate.
3. Select the *Use this certificate as an HTTPS certificate authority* checkbox.



Do not forget to select the *Use this certificate as an HTTPS certificate authority* checkbox.

Disabling access to Chrome developer tools

Disabling access to Chrome developer tools is recommended. This blocks users from disabling the FortiClient Web Filter extension.

To disable access to Chrome developer tools:

1. In the Google Admin console, go to *Devices > Chrome > Settings > Users & browsers*.
2. On the left, select the organization that contains the desired users or enrolled browsers. To select all users and browsers, select the top-level organization. Otherwise, select a child.
3. In *User & Browser Settings*, for the *Developer tools* option, select *Never allow use of built-in developer tools*.

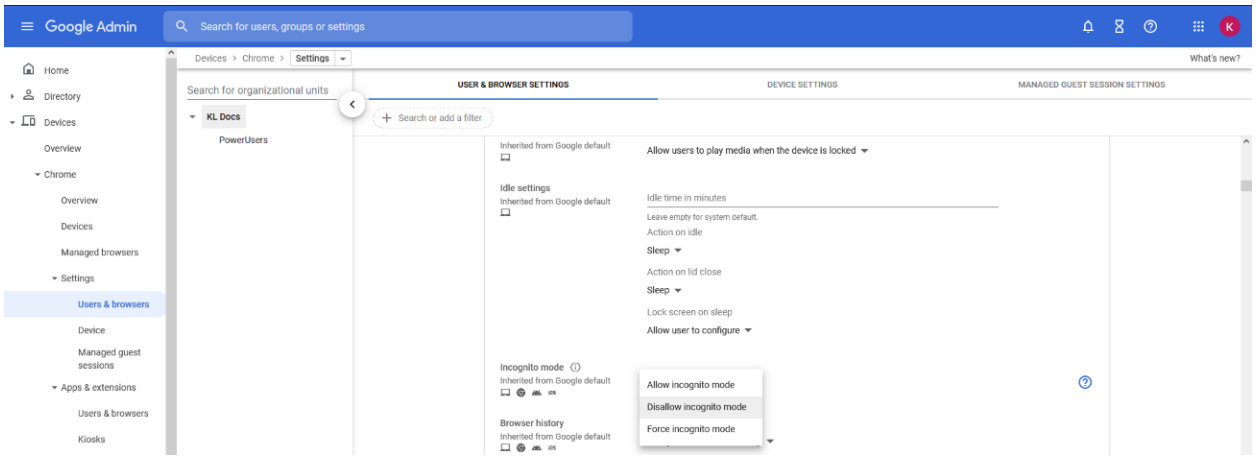
Disallowing incognito mode

When users browse in incognito mode, Chrome bypasses extensions. You should disallow incognito mode for managed Google domains.

To disallow incognito mode:

1. In the Google Admin console, go to *Devices > Chrome > Settings > Users & browsers*.
2. On the left, select the organization that contains the desired users or enrolled browsers. To select all users and browsers, select the top-level organization. Otherwise, select a child.

3. In *User & Browser Settings*, under *Security*, set *Incognito mode* to *Disallow incognito mode*.



4. Click *Save*.

Disabling guest mode

You should disallow guest mode for managed Google domains.

To disallow guest mode:

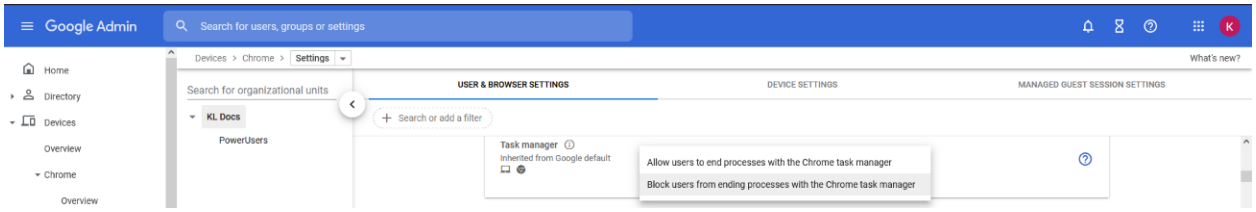
1. In the Google Admin console, go to *Devices* > *Chrome* > *Settings* > *Device*.
2. On the left, select the organization that contains the desired users or enrolled browsers. To select all users and browsers, select the top-level organization. Otherwise, select a child.
3. Under *Sign-in settings*, for *Guest mode*, select *Disable guest mode*.
4. Click *Save*.

Blocking the Chrome task manager

You should block users from ending processes with the Chrome task manager for managed Google domains.

To block the Chrome task manager:

1. In the Google Admin console, go to *Devices* > *Chrome* > *Settings* > *Users & browsers*.
2. On the left, select the organization that contains the desired users or enrolled browsers. To select all users and browsers, select the top-level organization. Otherwise, select a child.
3. In *User & Browser Settings*, under *Task manager* select *Block users from ending processes with the Chrome task manager* from the dropdown list.



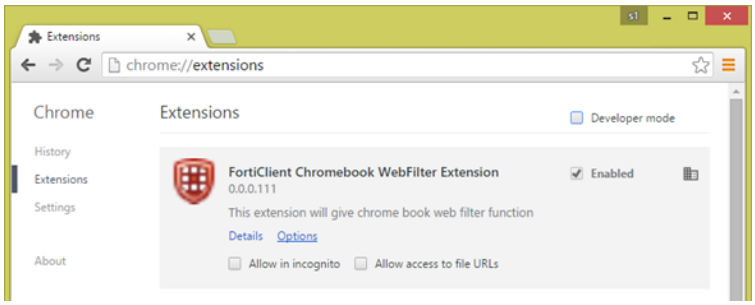
4. Click *Save*.

Verifying the FortiClient Web Filter extension

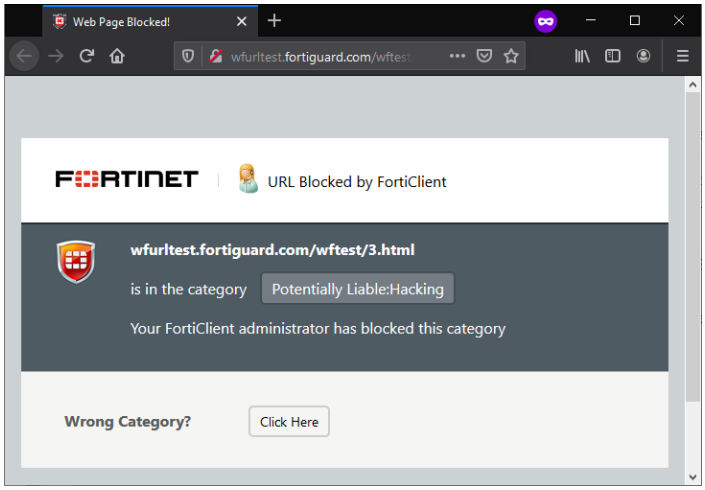
After you add the Google domain to FortiClient EMS, the Google Admin console automatically pushes the FortiClient Web Filter extension to the Chromebooks when users log into the Google domain. You can verify the feature has become available on the Chromebooks.

To verify the FortiClient Web Filter extension:

1. Open the Google Chrome browser.
2. Enter the following in the address bar: *chrome://extensions*



3. Visit any gambling site, such as https://www.777.com, and confirm the site is blocked.



Service account credentials

FortiClient EMS requires service account credentials that the Google Developer console generates. You can use the default service account credentials provided with FortiClient EMS or generate and use unique service account credentials, which is more secure.

The service account credentials must be the same in FortiClient EMS and the Google Admin console.

Configuring default service account credentials

FortiClient EMS includes the following default service account credentials that the Google Developer console generates:

Option	Default setting	Where used
Client ID	102515977741391213738	Google Admin console
Email address	account-1@forticlientwebfilter.iam.gserviceaccount.com	FortiClient EMS
Service account certificate	A certificate in `.pem` format for the service account credentials	FortiClient EMS



The service account credentials are a set. If you change one credential, you must change the other two credentials.

To configure the default service account credentials, you must add the client ID's default value to the Google Admin console. Service account credentials do not require other configuration. See Delegating domain-wide authority to the service account on page 140.

Configuring unique service account credentials

When using unique service account credentials for improved security, you must complete the following steps to add the unique service account credentials to the Google Admin console and FortiClient EMS:

1. Create unique service account credentials using the Google Developer console. See Creating unique service account credentials on page 134.
2. Add the unique service account credentials to the Google Admin console. See Delegating domain-wide authority to the service account on page 140.
3. Add the unique service account credentials to FortiClient EMS. See Adding service account credentials to EMS on page 142.

Creating unique service account credentials

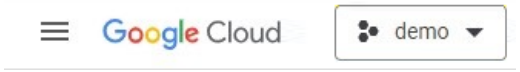
Creating a unique set of service account credentials provides more security. Unique service account credentials include the following:

- Client ID (a long number)
- Service account ID (email address)
- Service account certificate (a certificate in `.pem` format)

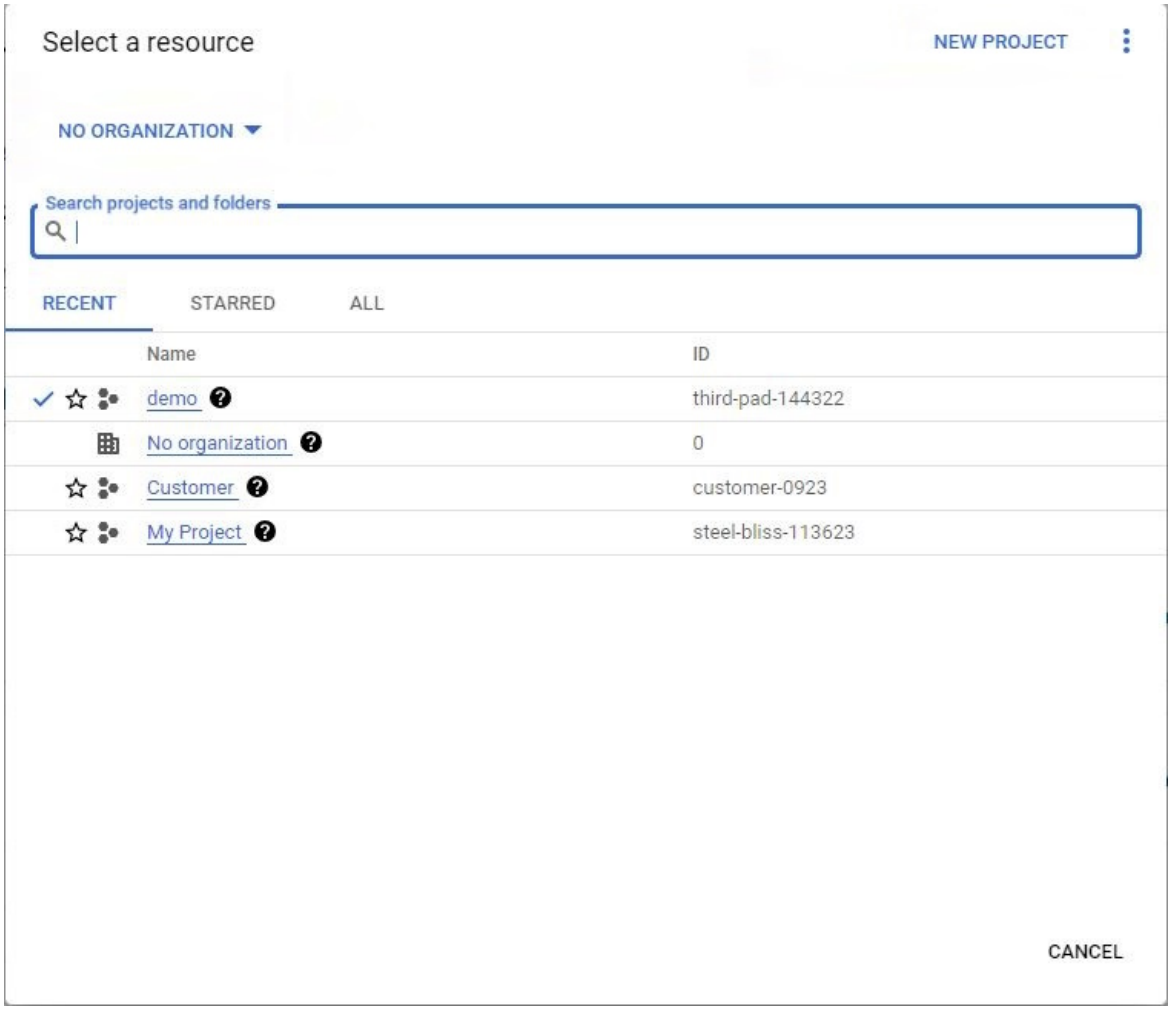
To create unique service account credentials:

1. Go to Google API Console.
2. Log in with your Google Workspace account credentials.

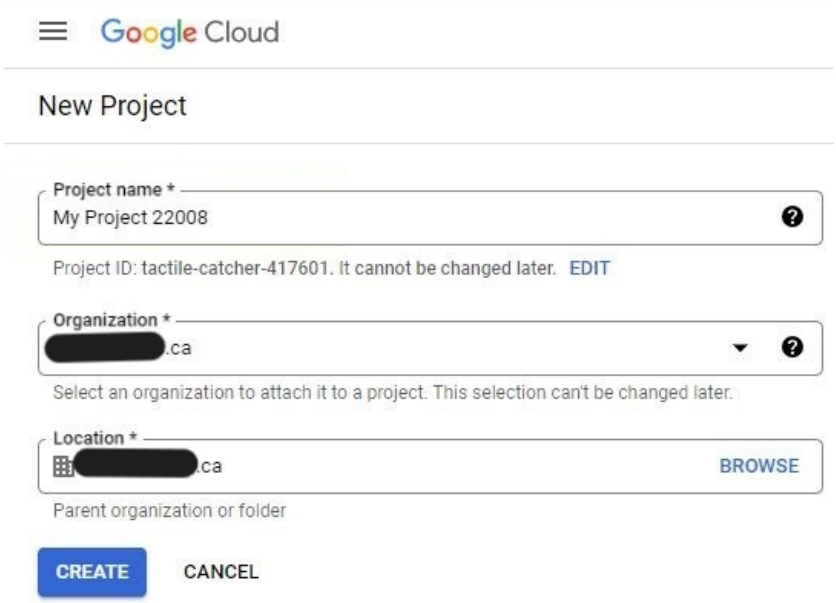
3. Create a new project:
   a. Click the toolbar list. The browser displays the following dialog.



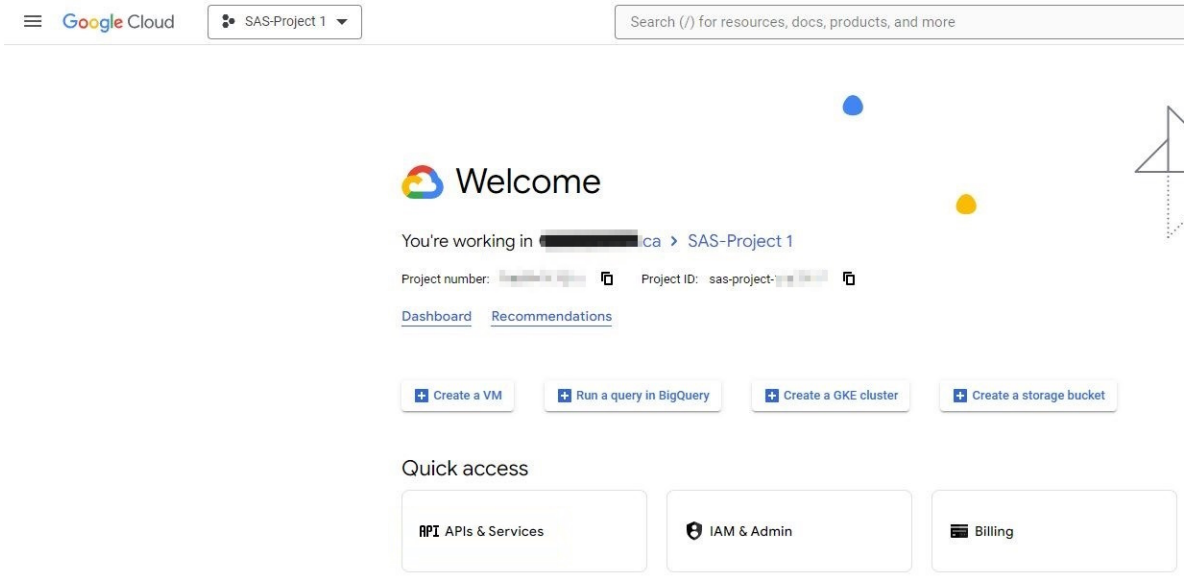
   b. Select your organization, if you see an organization dropdown list. Click *New Project*.

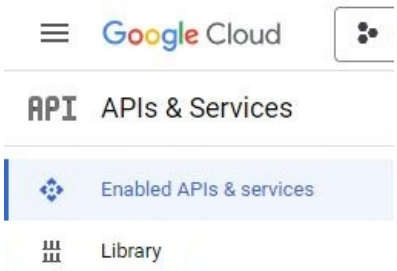


c. In the *Project name* field, enter your project name, then click *Create*.

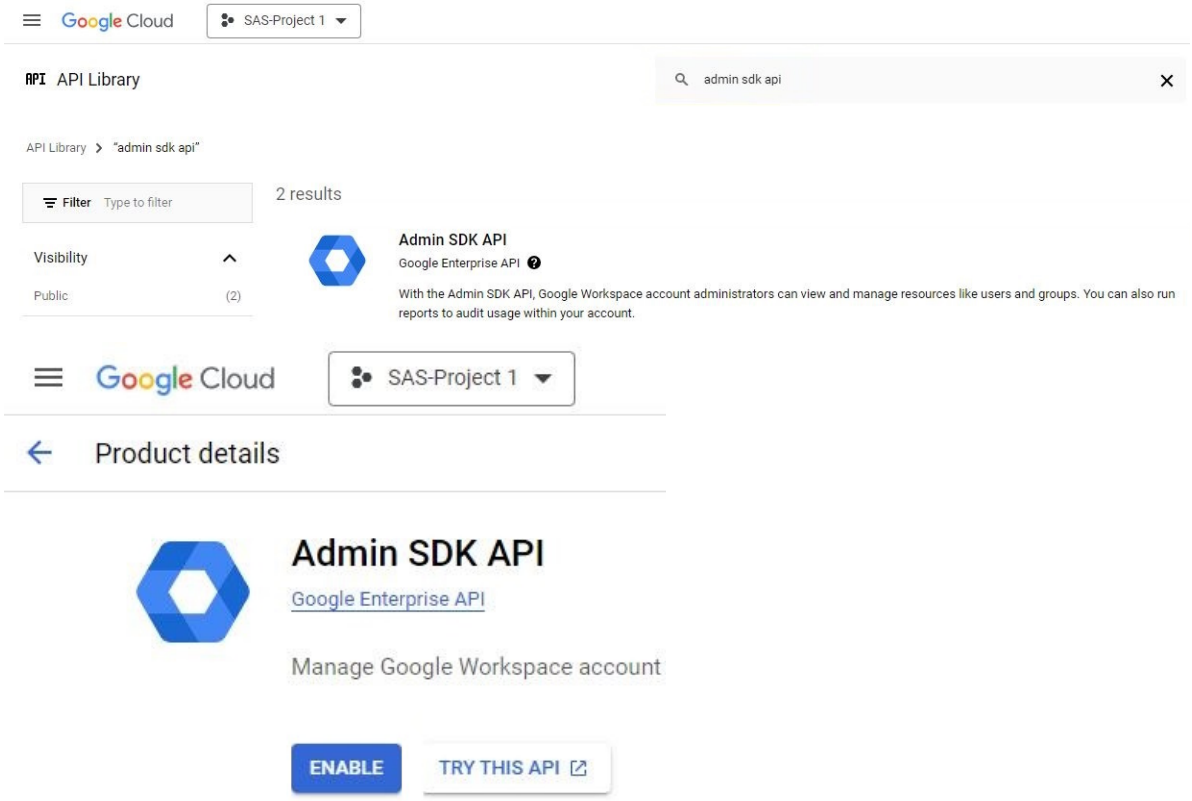


4. Enable the Admin SDK:
   a. Select your project from the toolbar list, then click *APIs & Services*.

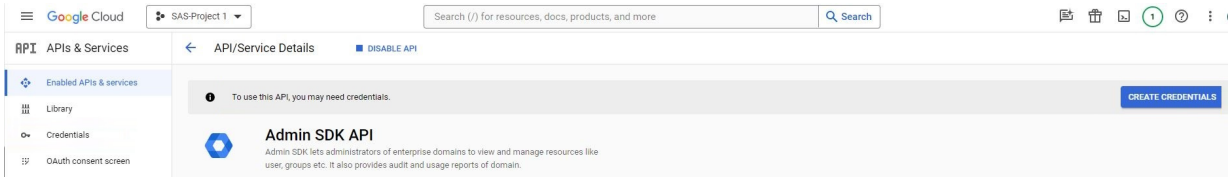




b. Under *Google Workspace APIs*, search for *Admin SDK API* and enable it.

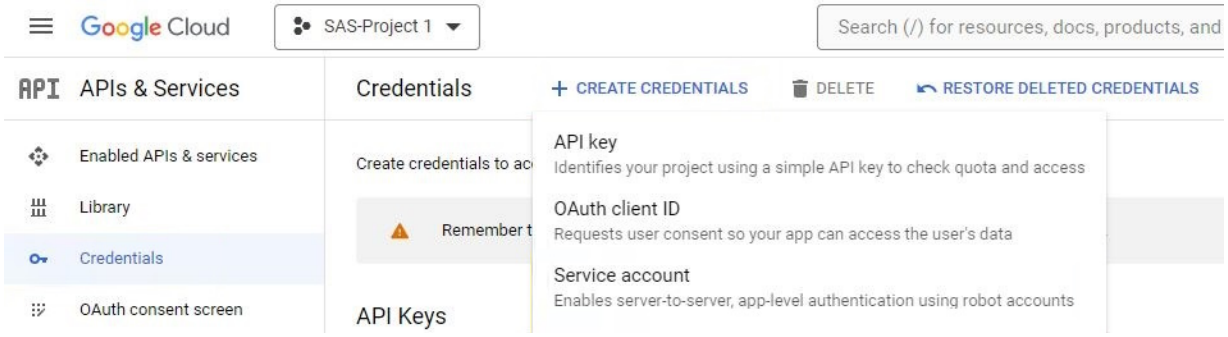


After enabling the Admin SDK API, the console displays a message indicating: *To use this API, you may need credentials*.

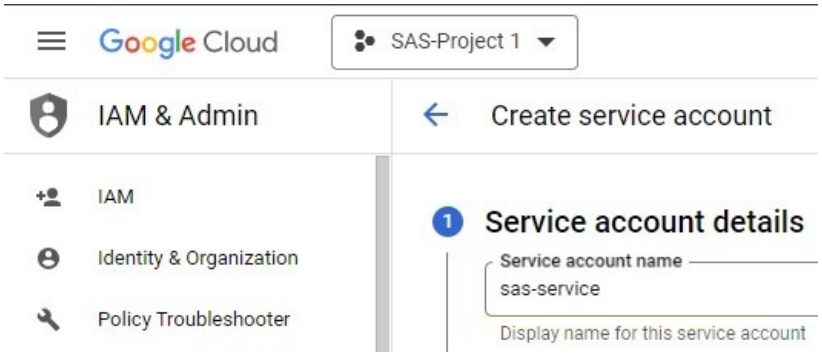


5. Create a service account:

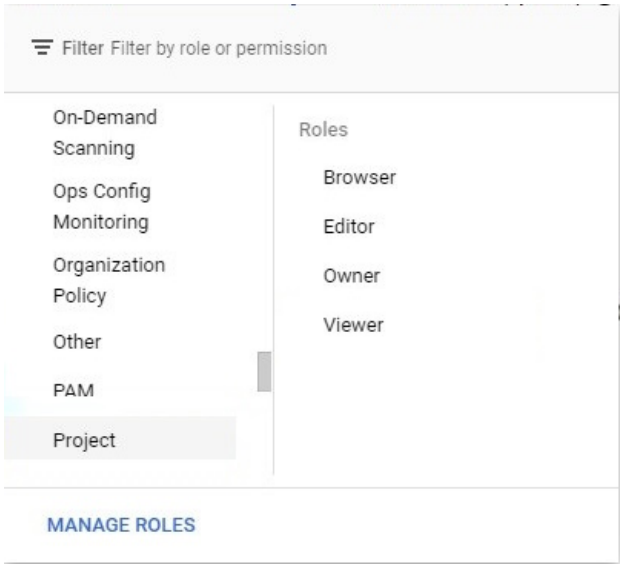
a. Go to the *Credentials* tab and select *Create Credentials* > *Service account*.



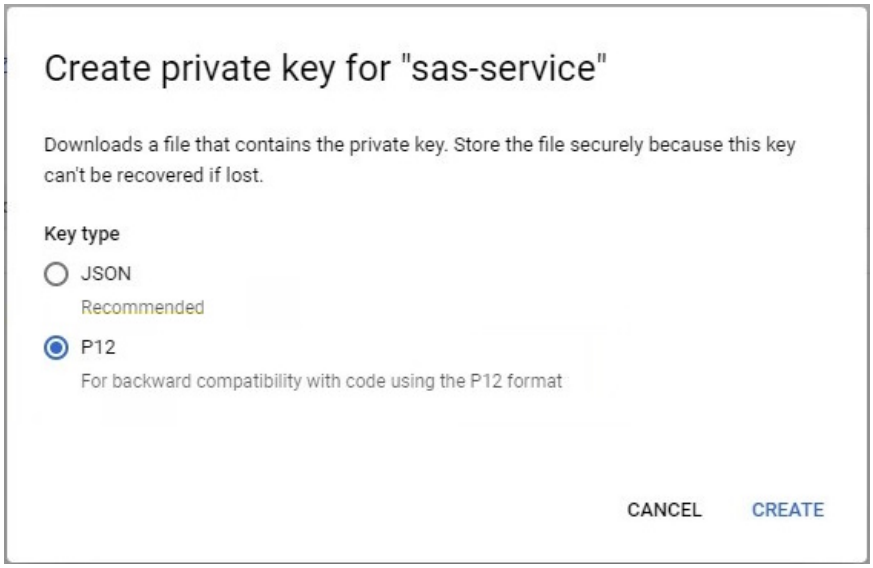
b. From the *Service account* list, select *New Service Account*. Enter a service account name.



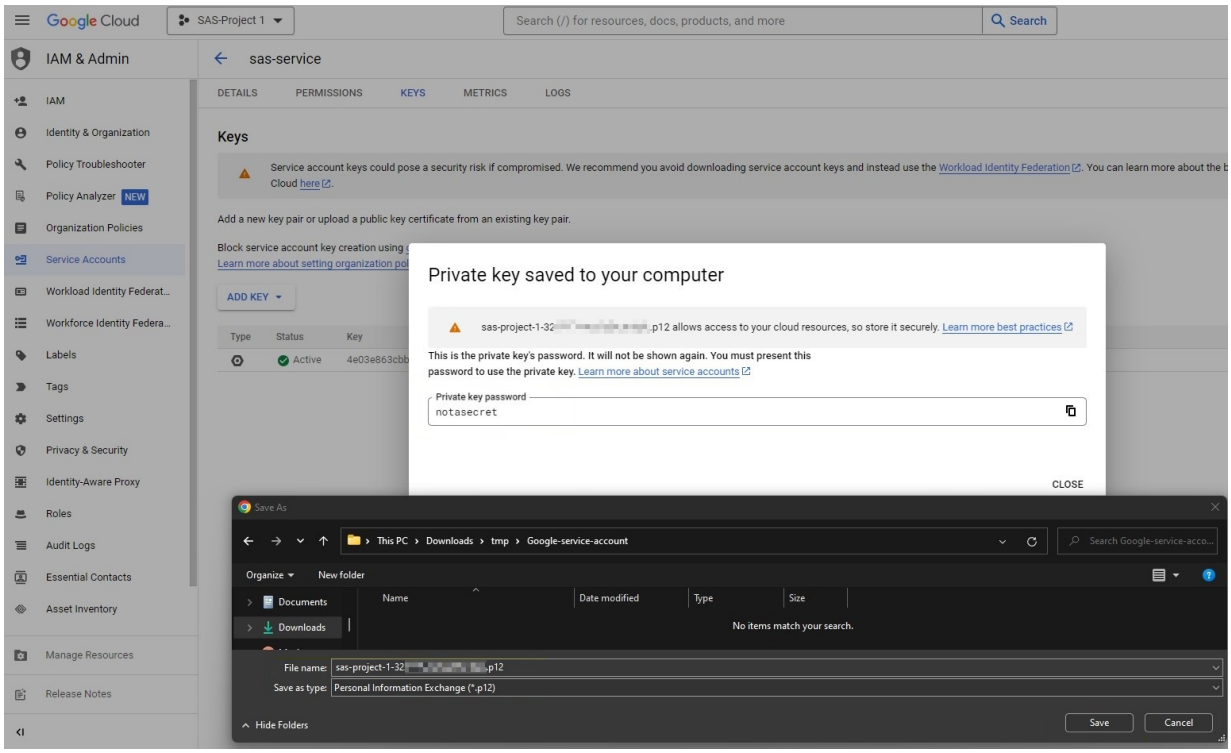
c. From the *Role* list, select *Project* > *Viewer*.



d. Edit the created service account and go to *Keys*. Click *Add Key* to create a P12 private key.

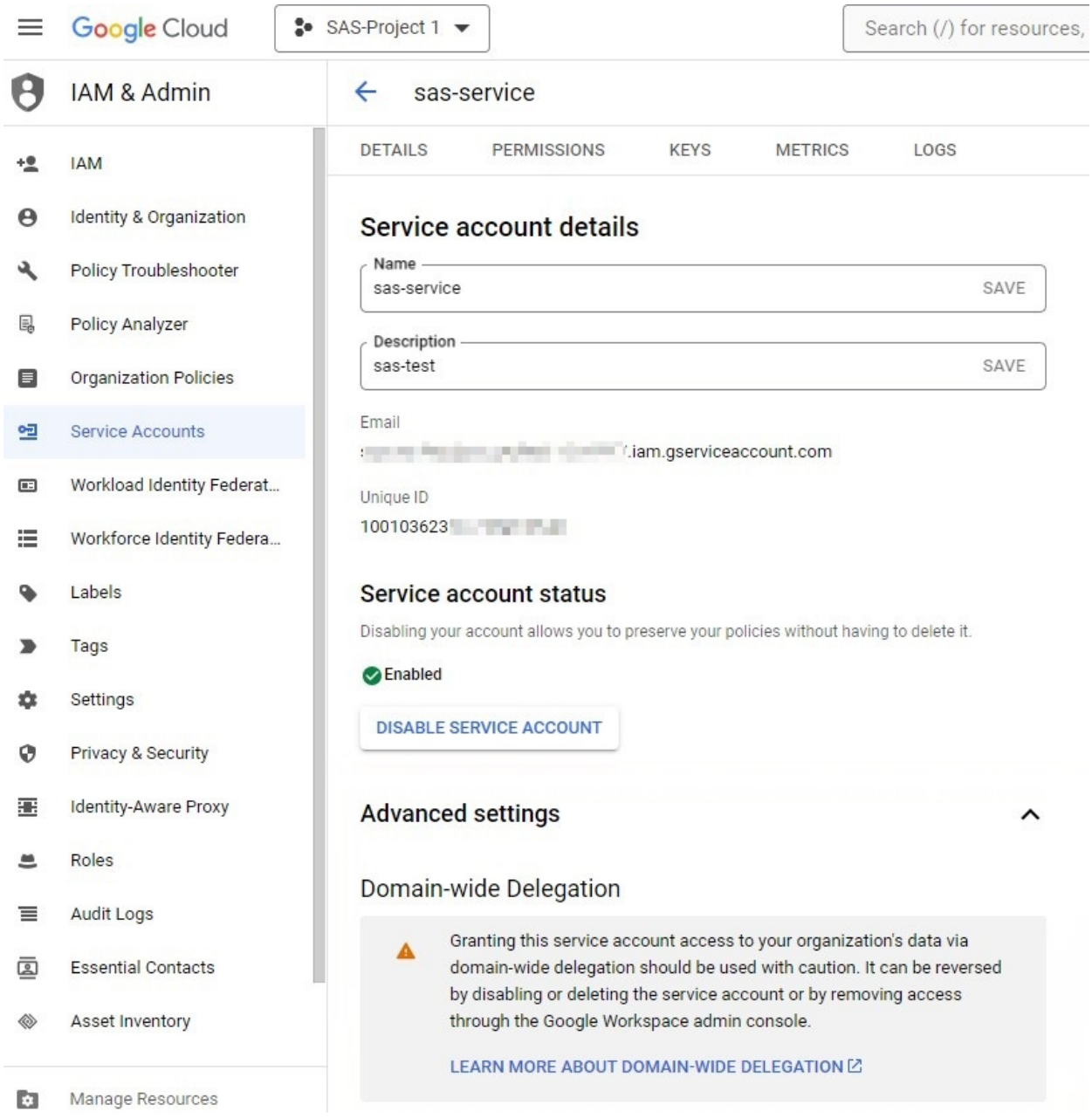


e. Save the private key and note the private key password, "notasecret".



> The private key with the P12 extension is the only copy you receive. Keep it in a safe place. You should also remember the password prompted on the screen. At this time, that password should be **notasecret**.

6. *Edit* the service account you just created and expand *Advanced settings*. There is a *Domain-wide Delegation* message and step-by-step guide.



To use the private key in EMS, you must convert it to `.pem` format. You can use the following `openssl` command to convert it. Remember to use the notasecret password.

```
C:\OpenSSL-Win64\bin>openssl pkcs12 -in demo-976b9d6e9328.p12 -out
      serviceAccount-demo.pem -nodes -nocerts
Enter Import Password:
```

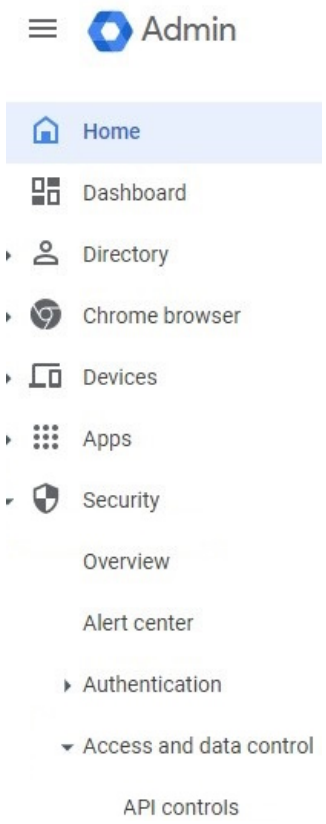
Delegating domain-wide authority to the service account

This section describes how to delegate domain-wide authority to the service account in the Google Admin console. These settings allow Google to trust FortiClient EMS, which enables FortiClient EMS to retrieve

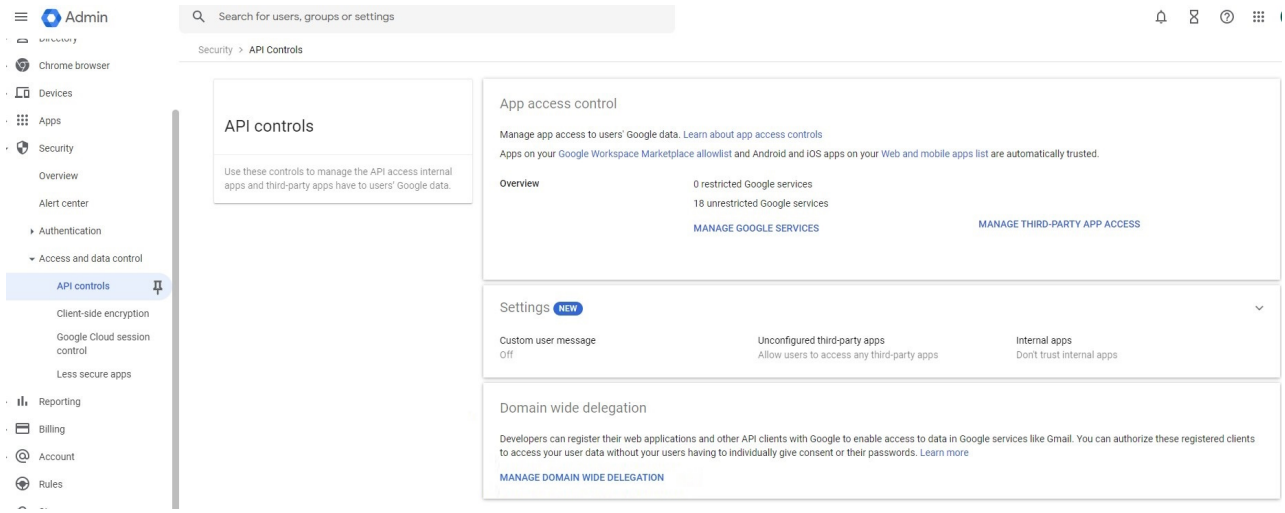
information from the Google domain.

To delegate domain-wide authority to the service account:

1. In the Google Admin console, go to *Menu > Security > Access and data control > API controls*.



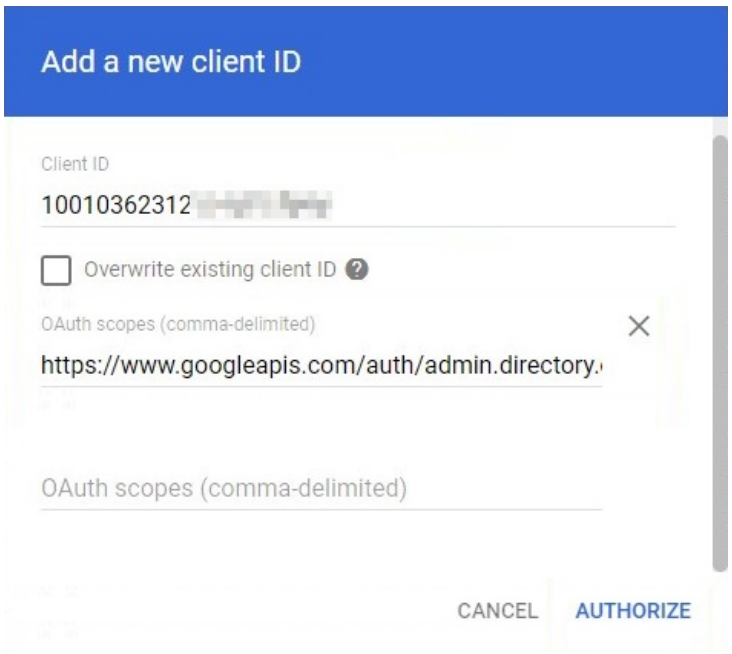
2. Click *Manage Domain Wide Delegation*, then click *Add New*.



3. Set the following options:
   a. In the *Client ID* field, add the client ID from the service account credentials.
   b. In the *OAuth Scopes* field, add the following string:
   https://www.googleapis.com/auth/admin.directory.orgunit.readonly,https://www.googleapis.com/auth/admin.directory.user.readonly

   The API scopes are case-sensitive and must be lowercase. You may need to copy the string into a text editor and remove spaces created by words wrapping to the second line in the PDF.

   c. Click *Authorize*.



Adding service account credentials to EMS

The section describes how to add the service account ID and service account certificate from the service account credentials to FortiClient EMS.

To add service account credentials to EMS:

1. In FortiClient EMS, go to *System Settings* > *EMS Settings*.
2. Enable *EMS for Chromebooks Settings*.

   The default service account credentials display. Overwrite the default settings with the unique set of service account credentials received from Fortinet.

3. The *Service account* field shows the configured email address provided for the service account credentials. Click the *Update service account* button and configure the following information:

Service Account Email	Enter a new email address for the service account credentials.
Private key	Click *Browse* and select the certificate provided with the service account credentials.

4. Click *Save*.



The service account credentials are a set. If you change one credential, you must change the other two credentials.

Verifying ports and services and connection between EMS and FortiClient

Ports and services

On the EMS server, run the following CLI command to verify the services are bound to a port:

```
sudo lsof -nP -i:8013
```

Option	Description
`-n`	Do not convert port numbers to port names.
`-p`	Do not resolve hostnames, show numerical addresses.
`-i`	Initiates the network file filter.

The following shows that EMS Linux is listening to port TCP/8013 on a particular interface: 192.168.1.22 in this case. The PID is 113194 and command is ecsocksrv.

```
ems@emsvm:~$  sudo lsof -nP -i:8013
COMMAND      PID           USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
ecsocksrv 113194 forticlientems  108u  IPv4 120770      0t0  TCP 172.16.1.22:8013 (LISTEN)
```

Automating EMS DB backups using cron jobs

The following provides instructions for creating and scheduling cron jobs for automated EMS database (DB) backups. You can also use other third-party tools to schedule EMS DB backups if desired.

To automate EMS DB backups using cron jobs:

1. Create an ems_db_backup.sh script file:

```
#!/bin/bash

backup_dir="/backup"
pg_lib_dir="/lib/postgresql/15/lib"
pg_extension_dir="/usr/share/postgresql/15/extension"
pg_data_dir="/var/lib/postgresql/15"
pg_host="localhost"
pg_user="postgres"
pg_port=5432

mkdir -p $backup_dir

databases=$(psql -h $pg_host -U $pg_user -p $pg_port -q -c "\l" | sed -n 4,/\eof/p | grep -v -
e 'template0' -e 'template1' -e 'rows' | awk -F '|' '{print $1}' | sed 's/^[[:space:]]*//;s/
[[:space:]]*$//')

dateinfo=`date '+%Y-%m-%d %H:%M:%S'`
timeslot=`date '+%Y%m%d%H%M'`

backup_dir=$backup_dir/$timeslot
mkdir $backup_dir

logfile=$backup_dir/"pgsql.log"
touch $logfile
echo "Starting backup of databases " >> $logfile

cp $pg_lib_dir/postgresextension $backup_dir/postgresextension
cp $pg_extension_dir/ems_extension--1.0.sql $backup_dir/ems_extension--1.0.sql
cp $pg_extension_dir/ems_extension.control $backup_dir/ems_extension.control
cp $pg_data_dir/symmetric_key.txt $backup_dir/symmetric_key.txt

echo "Complete backup of database extensions " >> $logfile

pg_dumpall -U $pg_user -h $pg_host -p $pg_port -c --if-exists --roles-only -f $backup_dir/ems_
roles.dump

for i in $databases; do
        #vacuumdb -z -h $pg_host -U $pg_user -p $pg_port $i >/dev/null 2>&1
        pg_dump -U $pg_user -F c -b $i -h $pg_host -p $pg_port -f $backup_dir/$i-database.dump
        echo "Backup and Vacuum complete on $dateinfo for database: $i " >> $logfile
done
echo "Done backup of databases " >> $logfile

#tail -15 $logfile | mailx youremail@domain.com
```

2. Set the permissions for ems_db_backup.sh:

```
sudo chmod +x ems_db_backup.sh
```

3. Add ems_db_backup.sh into your cron job. The following schedules the DB backup to occur every 59 minutes from Monday to Friday:

```
crontab -e
*/59 * * * 1-5 sh /home/administrator/scripts/ems_db_backup.sh
```

For cron syntax details, see Cron job format and time zone.



This example shows how to create the EMS DB backup job in a local environment where the local trust connection is already configured in pg_hba.conf. For a remote database, you must set appropriate DB permissions.

GUI

The FortiClient EMS GUI consists of the following areas:

Banner

Option		Description
Activate License to Enable Features		Displays if you have not applied a license to FortiClient EMS. 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. See Licensing FortiClient EMS on page 118.
SSL Certificate is not secure		Displays if a secure SSL certificate has not been imported to FortiClient EMS. Click the link to go to the *EMS Settings* page, where you can import a license. See Configuring EMS settings on page 629.
Download icon		Displays if a new version of FortiClient EMS is available on FDS.
Invitations		You can configure invitation codes that endpoints users can use to connect to EMS. See Invitations on page 599.
Multitenancy site		If multitenancy is enabled and you are logged into an account that can access multiple sites, you can go to another site by selecting it from a dropdown list. If you are logged in to the global site, you can also configure sites. See Multitenancy on page 661.
Help icon		
	Getting Started	Provides access to links to the FortiClient EMS *Release Notes* and other resources.
	Technical Documentation	Link to the FortiClient EMS 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 FortiClient EMS videos: • Introduction to FortiClient EMS: introductory video for FortiClient EMS, which gives an overview of features, modes, and system requirements for FortiClient EMS 1.0. • How to License FortiClient EMS: shows how to license or renew FortiClient EMS 1.0 with more endpoints. • Adding a Domain to FortiClient EMS: shows how to add an AD domain to FortiClient EMS

Option		Description
	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 FortiClient EMS.
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 FortiClient EMS.

Left pane

The left navigation pane displays content in the right pane. The following describes the left pane when multitenancy is disabled. For descriptions of the left pane with multitenancy enabled, see Left pane with multitenancy enabled on page 663.

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.
	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.

Option		Description
	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*.
	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 FortiClient EMS.
	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.

Option		Description
	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.
Administration		
	Administrators	Add and manage FortiClient EMS administrators.
	Admin Roles	Add and manage FortiClient EMS 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 FortiClient EMS license.
	Log Viewer	View log messages generated by FortiClient EMS and download raw logs.
System Settings		
	EMS Settings	Change the IP address and port and configure other EMS settings for FortiClient EMS, including enabling Chromebook management.
	Log Settings	Specify what level of log messages to capture in FortiClient EMS 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 FortiClient EMS 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 FortiClient EMS
	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.

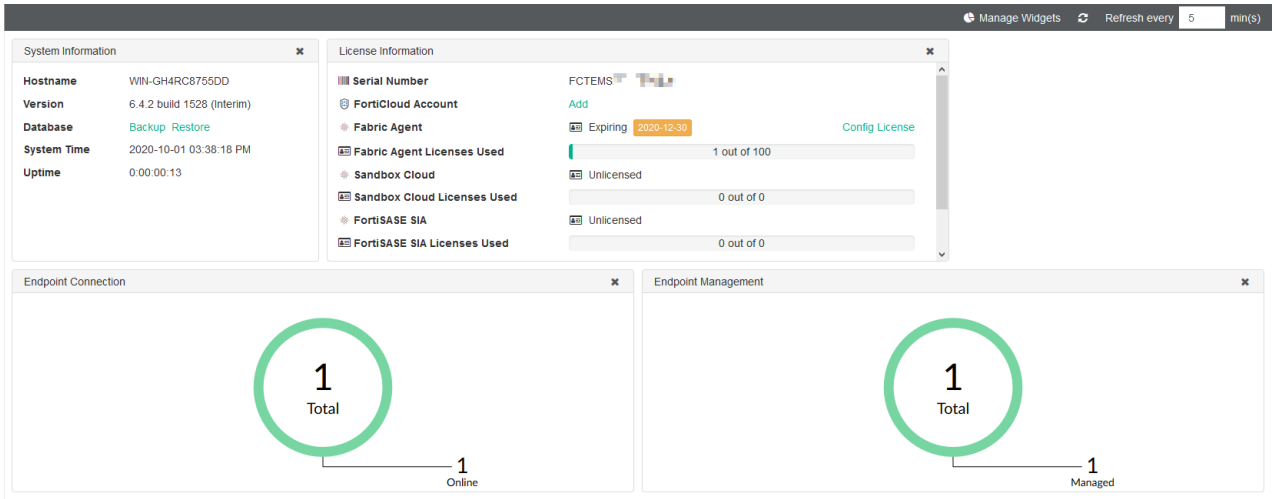
Dashboard

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 152 and Status charts and widgets on page 155.



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 176.
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 when multitenancy is disabled. If you enable multitenancy, this information displays in the global site *System Information* widget. See Global and per-site configuration on page 662.

Field	Description
Hostname	Name of the computer where you installed FortiClient EMS.
Version	Version number for FortiClient EMS. 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 152 and To restore the DB: on page 152.
System Time	Time and date that the computer where you installed FortiClient EMS uses.
Uptime	Number of days, hours, minutes, and seconds FortiClient EMS 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. 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*. FortiClient EMS backs up the DB.

To restore the DB:

1. Go to *Dashboard* > *Status*.
2. Beside *Database*, click *Restore*.
3. Click *Browse*.
4. Locate and select the DB backup file.
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.



EMS does not support restoring the DB from a standalone EMS to an EMS HA setup.

License Information widget

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

Option	Description
Serial Number	Serial number for FortiClient EMS.
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 FortiClient EMS. 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. See License status on page 125.

For details on the features included with each license type, see Windows, macOS, and Linux licenses on page 25.

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 655.

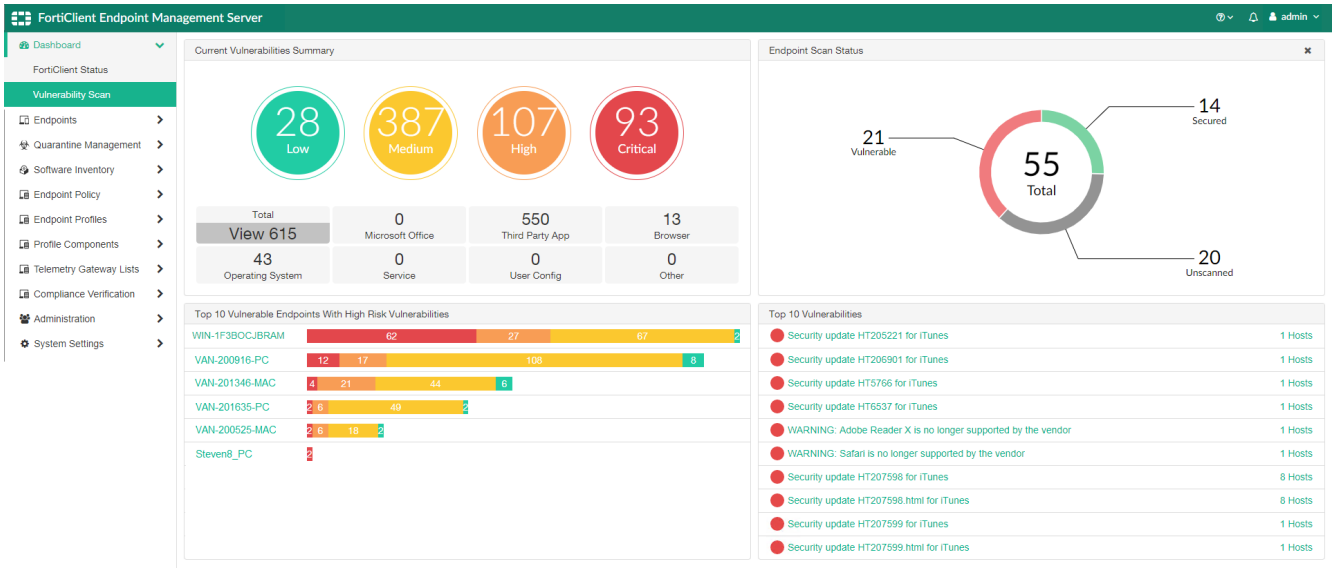
Option	Description
Endpoint Charts	
Endpoint Activity	Shows a summary of endpoint activity information. Categories are: • EMS On-fabric • EMS Off-fabric
Endpoint Alerts	Shows the number of endpoints with alerts, including pending software updates, out-of-date protection, and out-of-sync profiles.
Endpoint 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.

Option	Description
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.
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.

Option	Description
	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.
FortiGuard Outbreak Alerts Service	This chart displays endpoints that are considered suspicious or compromised according to the outbreak alert rules that FortiClient EMS has received from FortiGuard. The chart displays the number of endpoints that are vulnerable to each outbreak. See FortiGuard Outbreak Alerts on page 530. 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.

The severity levels that the charts display correspond to the risk levels in FortiGuard:

- Green (low-risk): corresponds to a two-dot risk level in FortiGuard.
- Yellow (medium-risk): corresponds to a three-dot risk level in FortiGuard.
- Orange (high-risk): corresponds to a four-dot risk level in FortiGuard.
- Red (critical risk): corresponds to a five-dot risk level in FortiGuard.

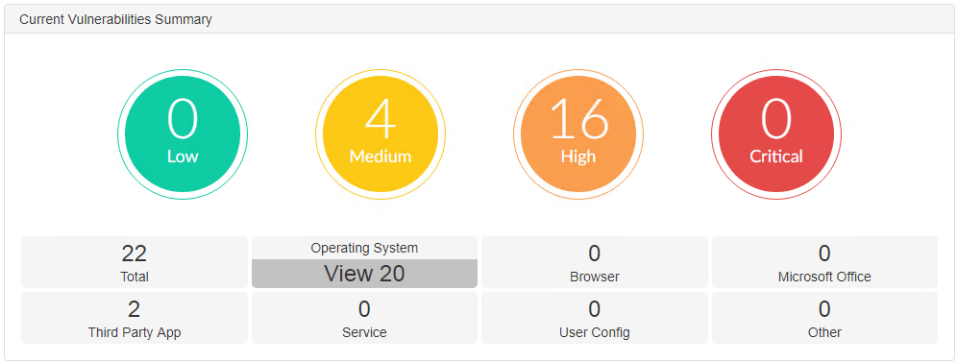
EMS does not provide information regarding vulnerabilities that are considered a one-dot risk level in FortiGuard.

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.

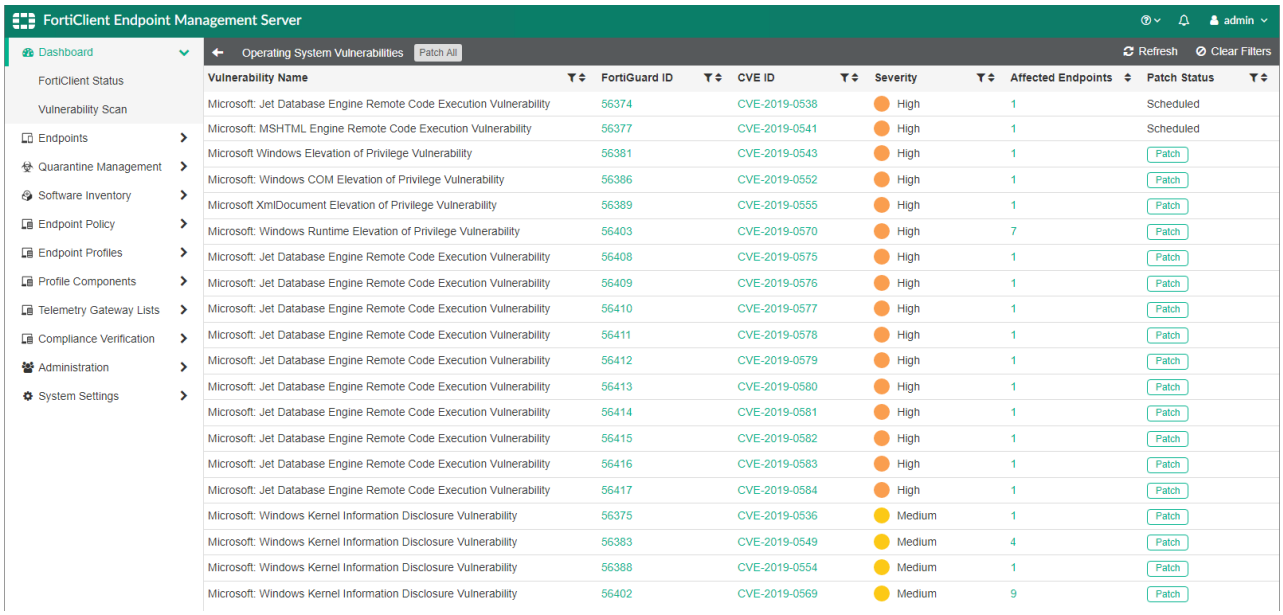
Viewing current vulnerabilities

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:

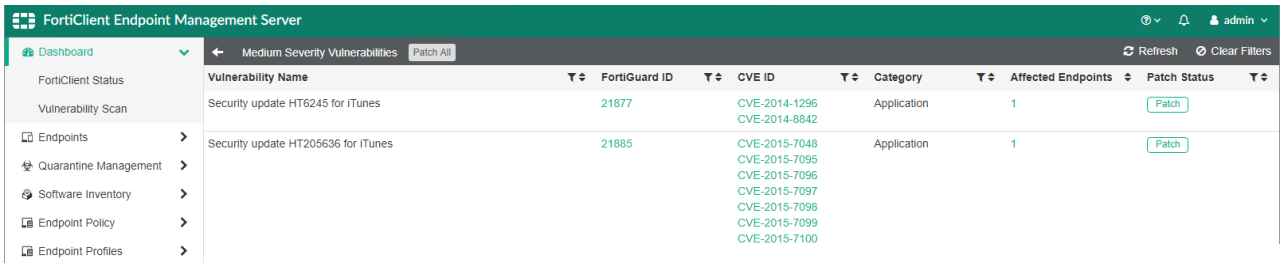


Patch All	Click this button to patch all vulnerabilities currently displayed on the content pane. The vulnerabilities are patched with the next Telemetry communication between FortiClient EMS and the endpoint.
Refresh	Click to refresh the list of vulnerabilities in the content pane.
Clear Filters	Click 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 FortiClient EMS 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.

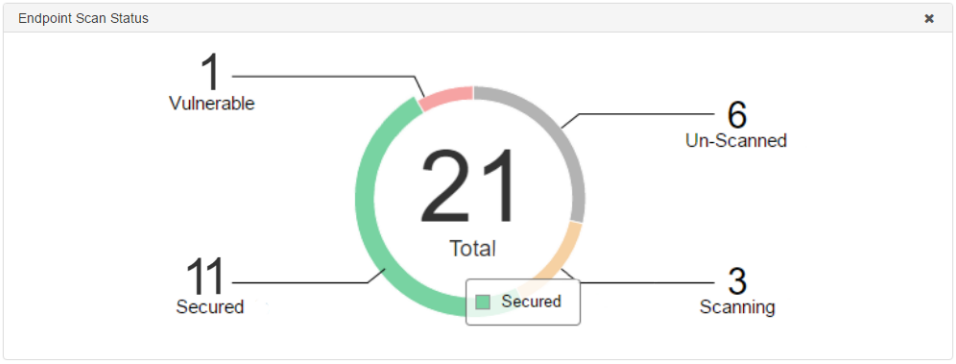
5. Return to *Dashboard > Vulnerability Scan*. You can also click a colored circle to view all vulnerabilities of the selected severity level. The following shows all medium severity third party application vulnerabilities:



Viewing the Endpoint Scan Status

To view the Endpoint Scan Status:

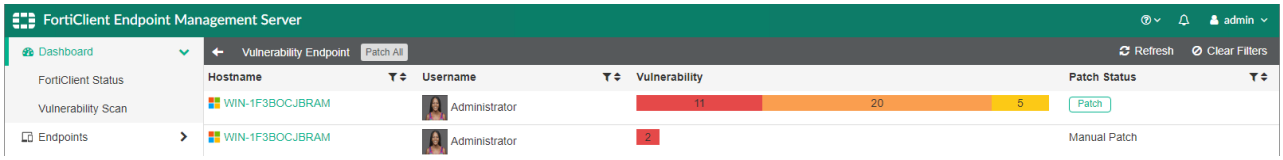
1. Go to *Dashboard* > *Vulnerability Scan*.



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:



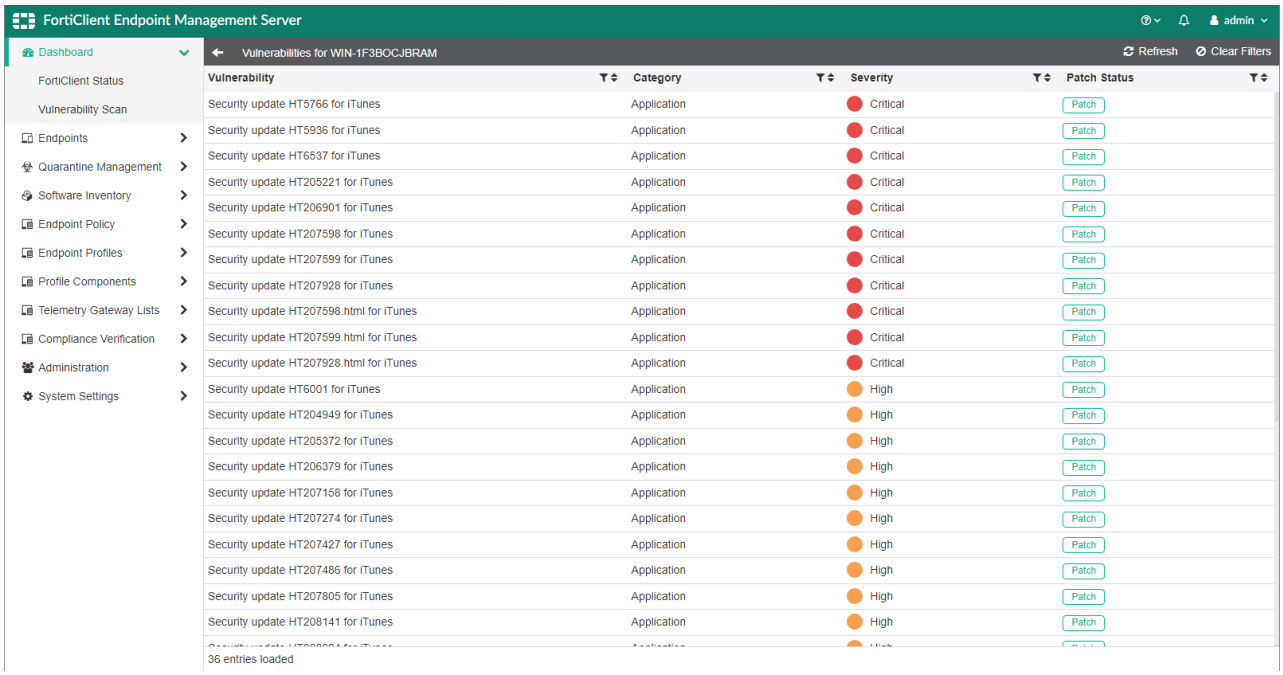
Patch All	Click this button to patch all vulnerabilities currently displayed on the content pane. The vulnerabilities are patched with the next Telemetry communication between FortiClient EMS and the endpoint.
Refresh	Click to refresh the list of vulnerabilities in the content pane.
Clear Filters	Click 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 FortiClient EMS 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*.

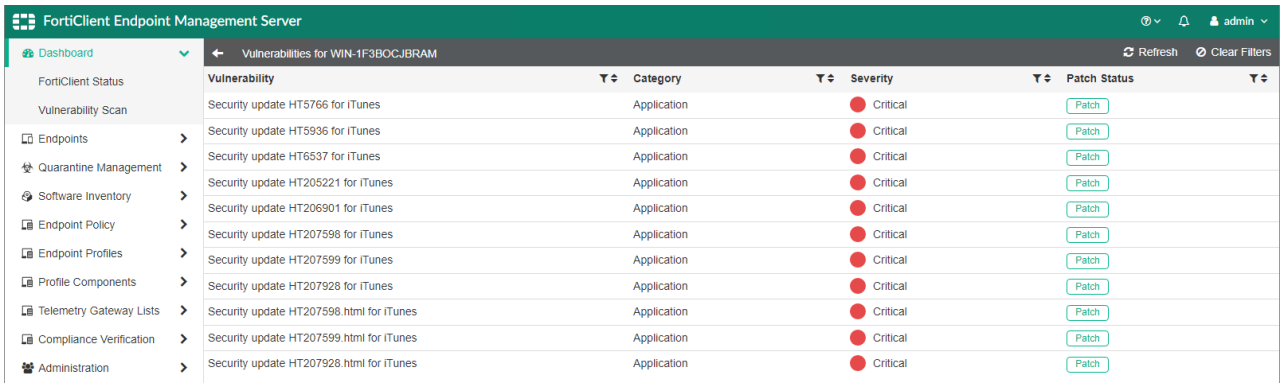
You can filter the list of vulnerable endpoints by any column by clicking the filter icon beside the desired heading. Enter the value to include in the filter. You can toggle the *All/Any/Not* button for the following options:

- *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.

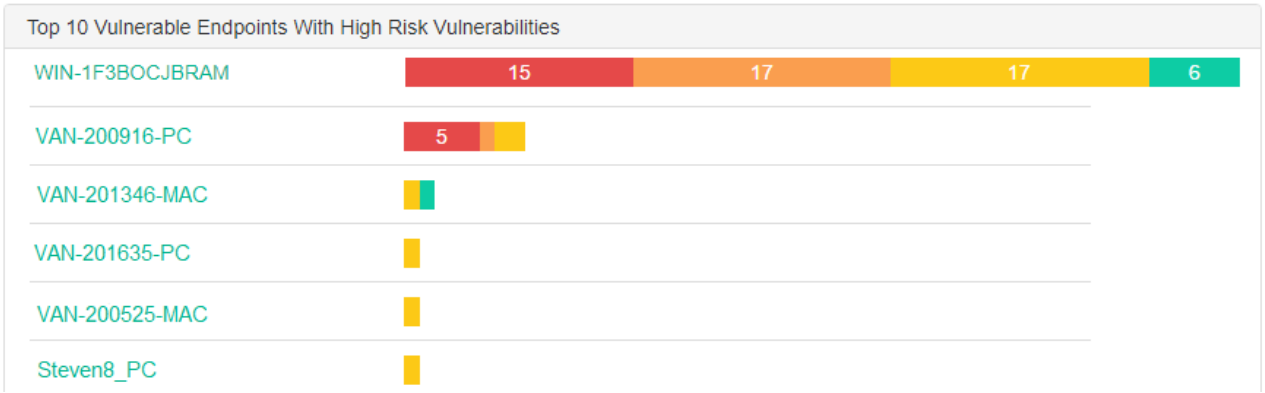


Vulnerability	Name of the vulnerability.
Category	Category of the vulnerability.
Severity	Severity level of the vulnerability.
Patch Status	You can click the *Patch* button to patch the selected vulnerability with the next Telemetry communication between FortiClient EMS and the endpoint. If a patch is 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

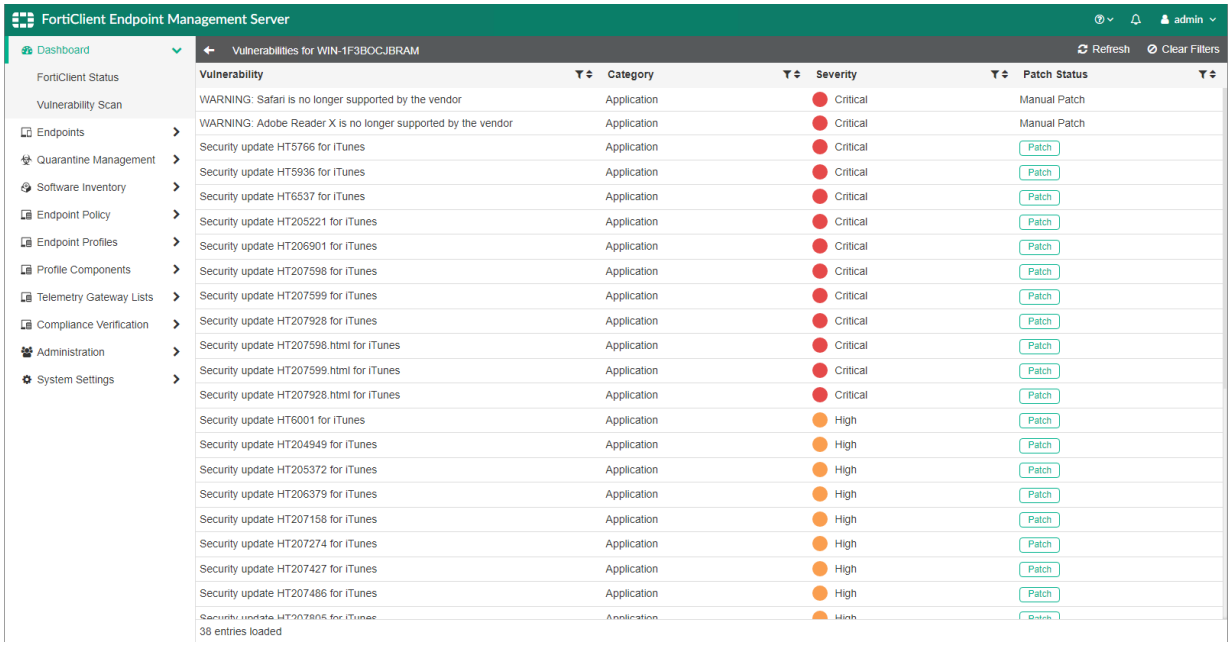
To view the top 10 vulnerable endpoints with high risk vulnerabilities:

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.

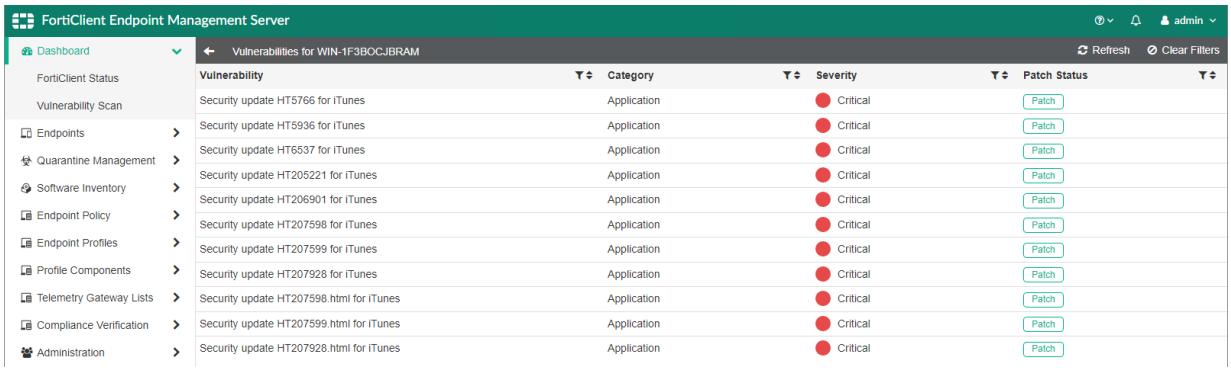


Vulnerability	Name of the vulnerability.
Category	Category of the vulnerability.
Severity	Severity level of the vulnerability.
Patch Status	You can click the *Patch* button to patch the selected vulnerability with the next Telemetry communication between FortiClient EMS and the endpoint. If a patch is 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.

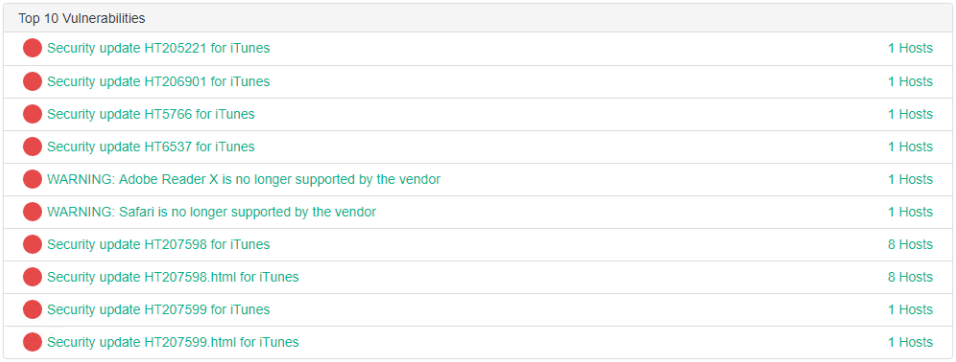
b. Click one of the sections of the vulnerability bar graph to view all vulnerabilities detected on the selected endpoint at the selected severity. The example displays all critical vulnerabilities for the selected endpoint. You can filter the list of vulnerabilities in the same way that you can filter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



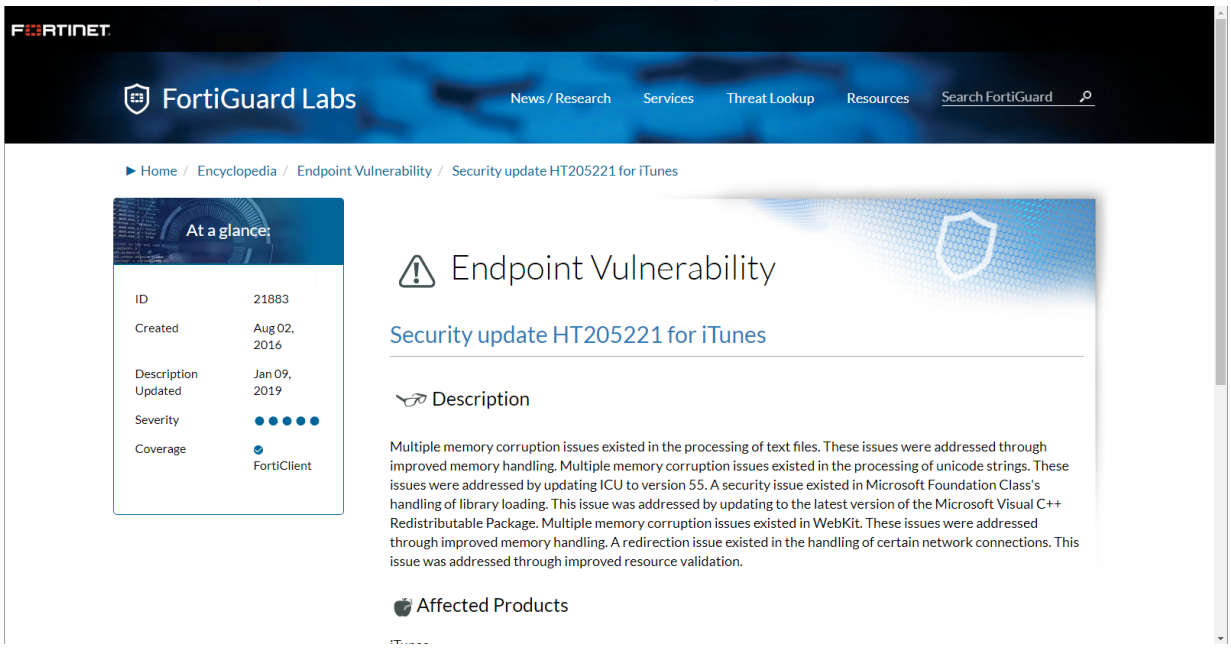
Viewing top ten vulnerabilities on endpoints

To view top ten vulnerabilities on endpoints:

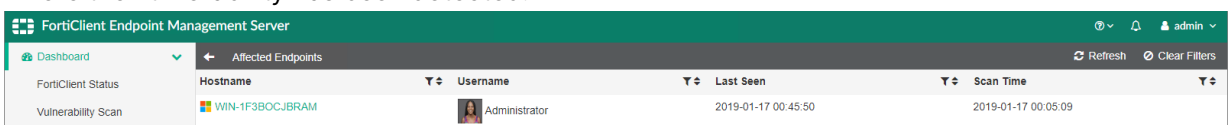
1. Go to *Dashboard* > *Vulnerability Scan*. The *Top 10 Vulnerabilities* widget displays the type of vulnerability and how many hosts the vulnerability has been detected on.



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.



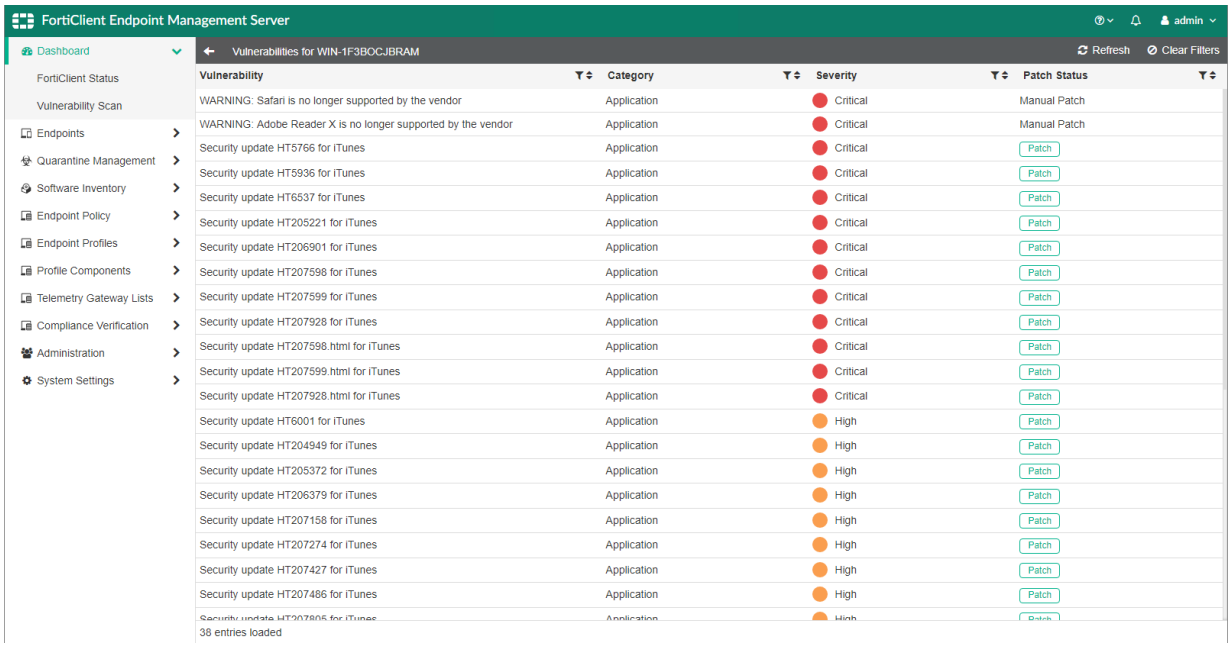
Refresh	Click to refresh the list of vulnerabilities in the content pane.
Clear Filters	Click to clear all filters applied to the list of vulnerabilities.

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 FortiClient EMS 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 FortiClient EMS 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:

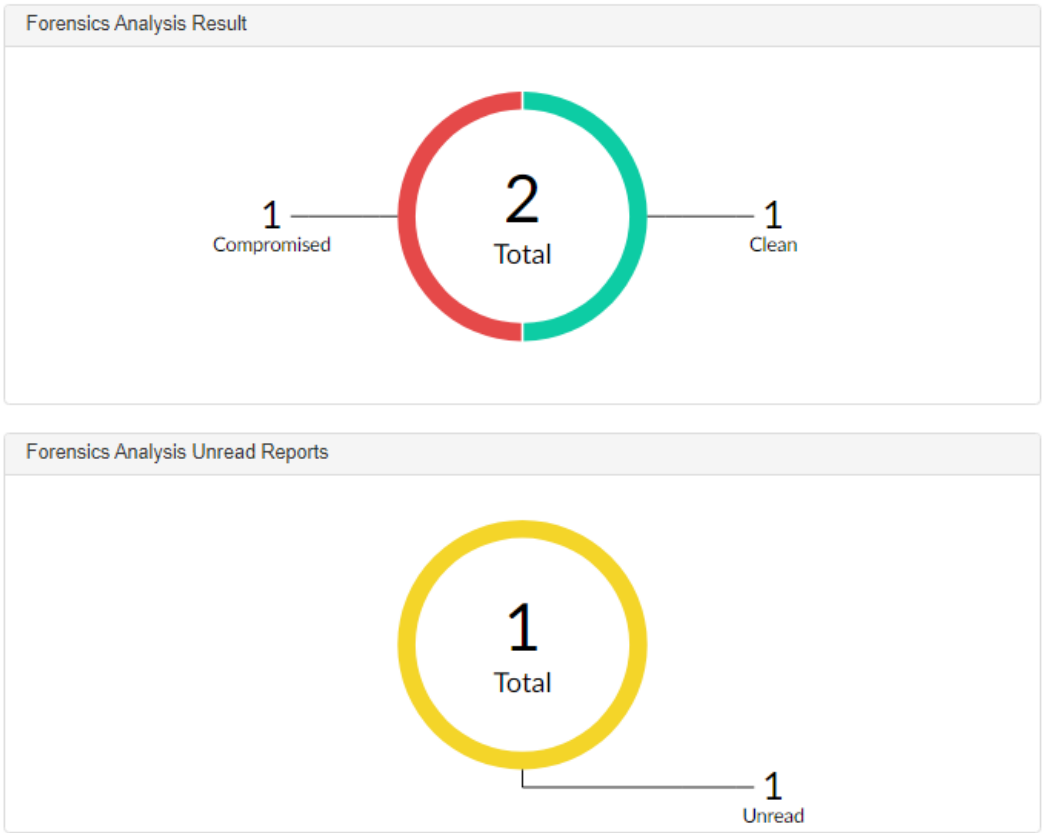
- **Third-party application vulnerabilities**: incorrect or missing installation paths
- **OS vulnerabilities**: Windows update service is disabled

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:

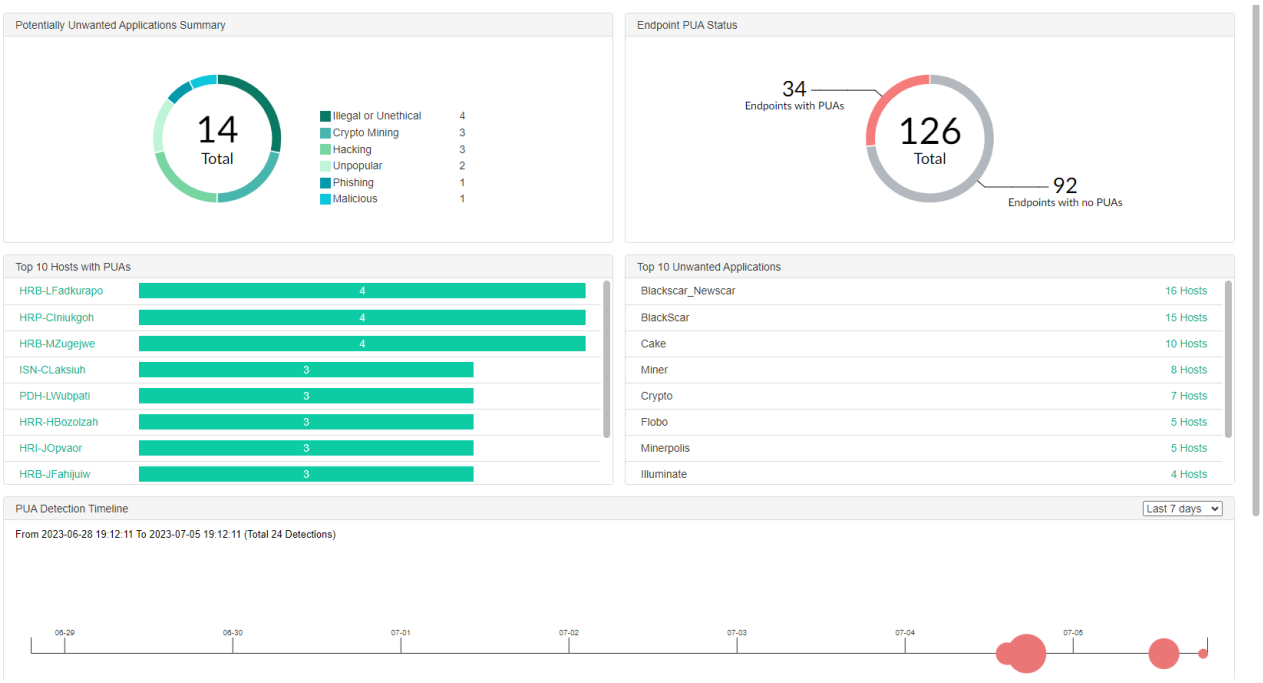
Widget	Information shown
Active Concurrent Forensics Analysis Requests	Number of active requests and available requests. You can only have five concurrent requests.
Forensics Analysis Status	Ticket status of each endpoint's forensics analysis task.
Forensics Analysis Result	Forensics verdict for analyzed 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.
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 422.
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 422.
Others	
System Information	See System Information widget on page 152.
License Information	See License Information widget on page 154.

Endpoint management

FortiClient EMS 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 571.

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 173, 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 174.
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*.

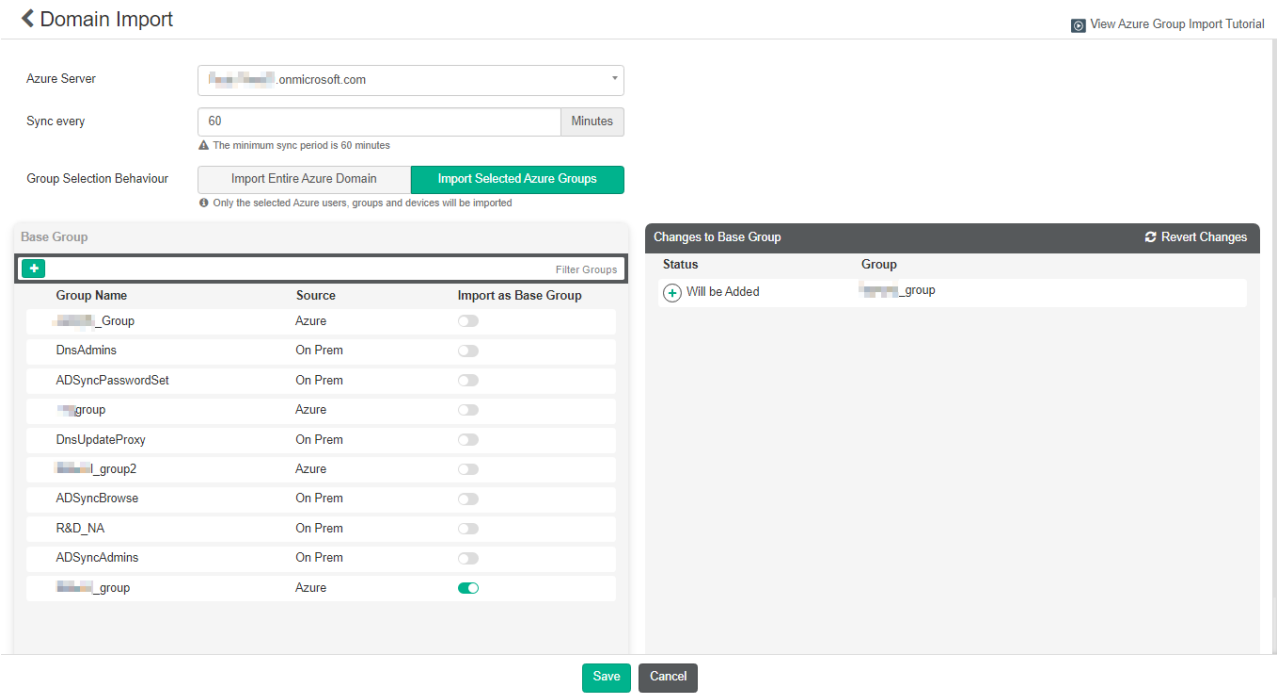
If you remove *Sub-OU: Department 2* from *OU: Premium*'s subtree, EMS does not import *Sub-OU: Department 2*. This is because you did not explicitly import *Sub-OU: Department 2*. EMS only imported it because it was in *OU: Premium*'s subtree.

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 573.

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 FortiClient EMS by specifying the IP address for FortiClient EMS in FortiClient. This process is sometimes called registering FortiClient to FortiClient EMS.

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 FortiClient EMS, 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.

Option	Description
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 FortiClient EMS. 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*.

Option	Description
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 FortiClient EMS. 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 422 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. This action is only available if the ZTNA or EPP license is applied and for endpoints running FortiClient 7.0.0 and later versions. 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. See FortiClient in the Security Fabric on page 14. • 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 184.

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 keep-alive message to EMS. This information is useful if FortiClient is offline because it indicates when the last keep-alive 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 248.
	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 495.
	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 530.
	Connection	Displays the connection status between the selected endpoint and FortiClient EMS.

	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 the *Add* button, enter the desired tag, the click the + button. When you create a tag, it is available for assignment to all endpoints in the current 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 FortiClient EMS 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 190.
	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 201.
		• **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.
	Features	Displays which features are enabled for FortiClient.
	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 AV event's 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 189.
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.
	Detected Paths	Path where FortiClient detected 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.
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

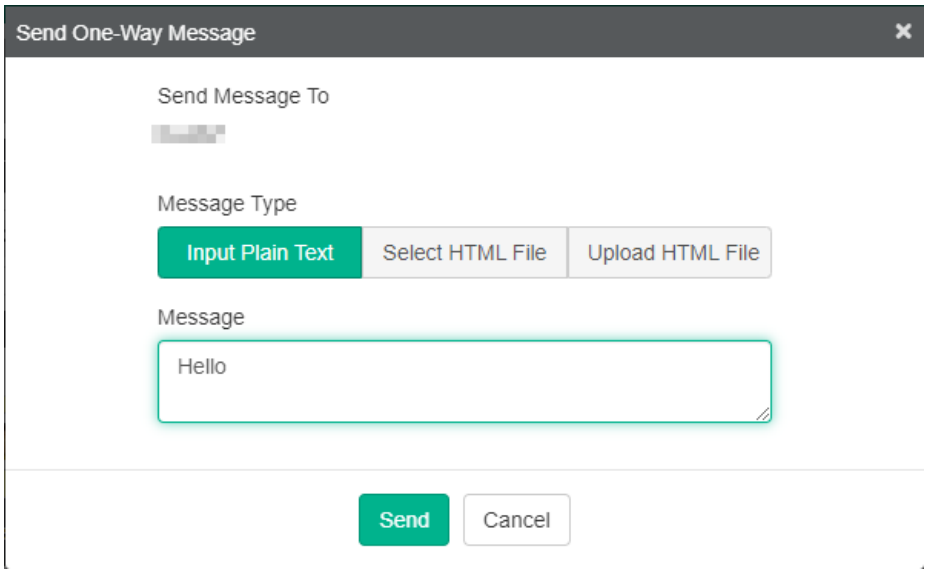
The EMS administrator can send a one-way message to endpoints in a tagged group, endpoint group, or one endpoint. For example, you may want to send a message to remind a user to upload an avatar to FortiClient. EMS sends the message at the next keepalive interval. By default, this is 60 seconds.

The message can be in plain text or HTML format.

To send an endpoint a message:

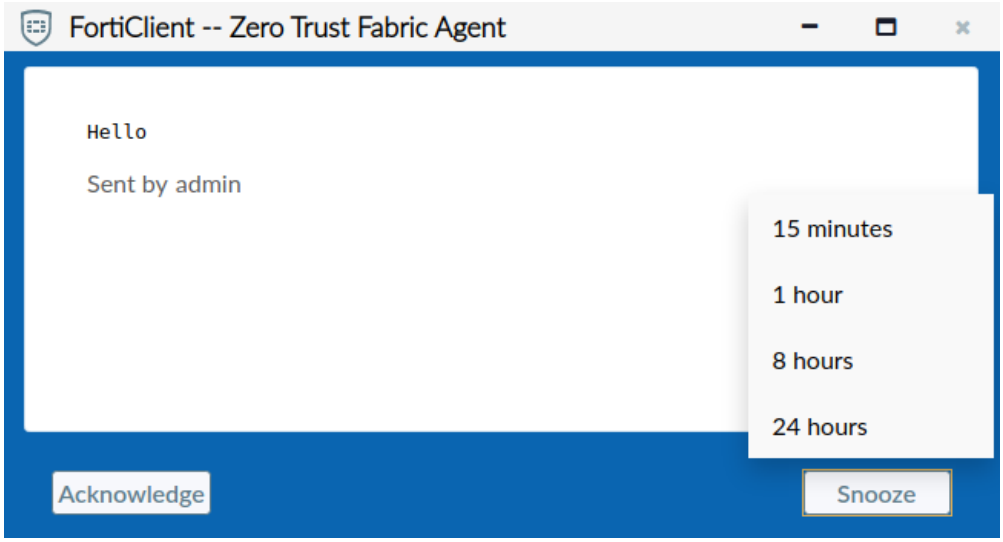
1. In EMS, go to *Endpoints* > *All Endpoints*.
2. Select the desired endpoint(s).
3. Click *Action* > *Send Message*.

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.



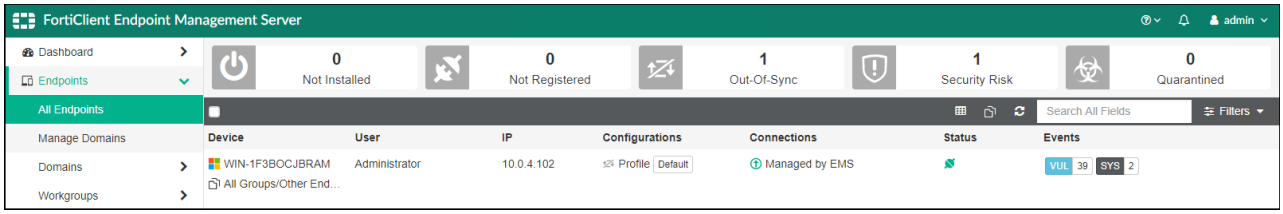
FortiClient logs a system event for when the user snoozes the message and when they acknowledge it.

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 176.

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 495 and Viewing the Endpoints pane on page 176.
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.
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:

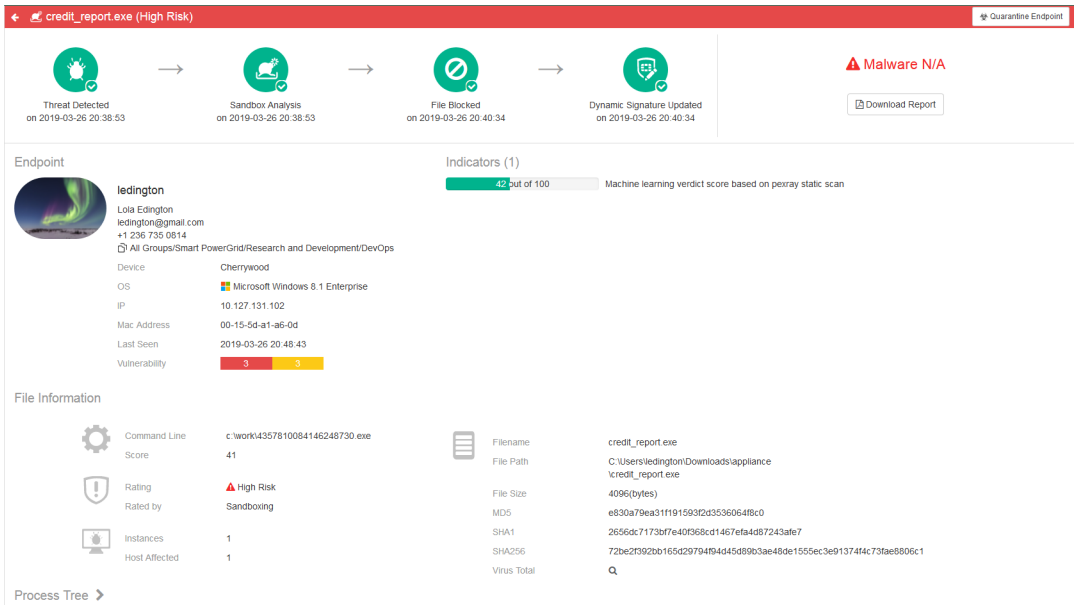
1. Go to *Endpoints*.
2. Click *All Endpoints*, a domain, or workgroup. The list of endpoints displays.
3. Click the *Filters* menu.
4. In the *Bookmarks* list, click a bookmark. The bookmark settings are used to filter the list of endpoints.

Viewing Sandbox event details

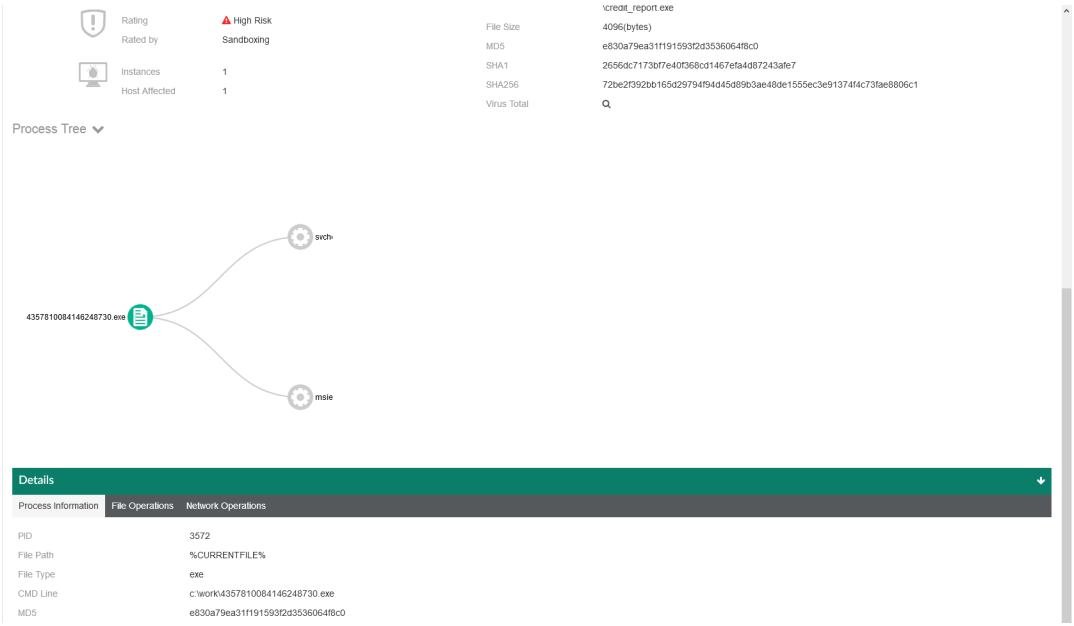
You can view a detailed report about a Sandbox event. EMS retrieves the report from FortiSandbox.

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. You can create a maximum of eight custom tags. 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.

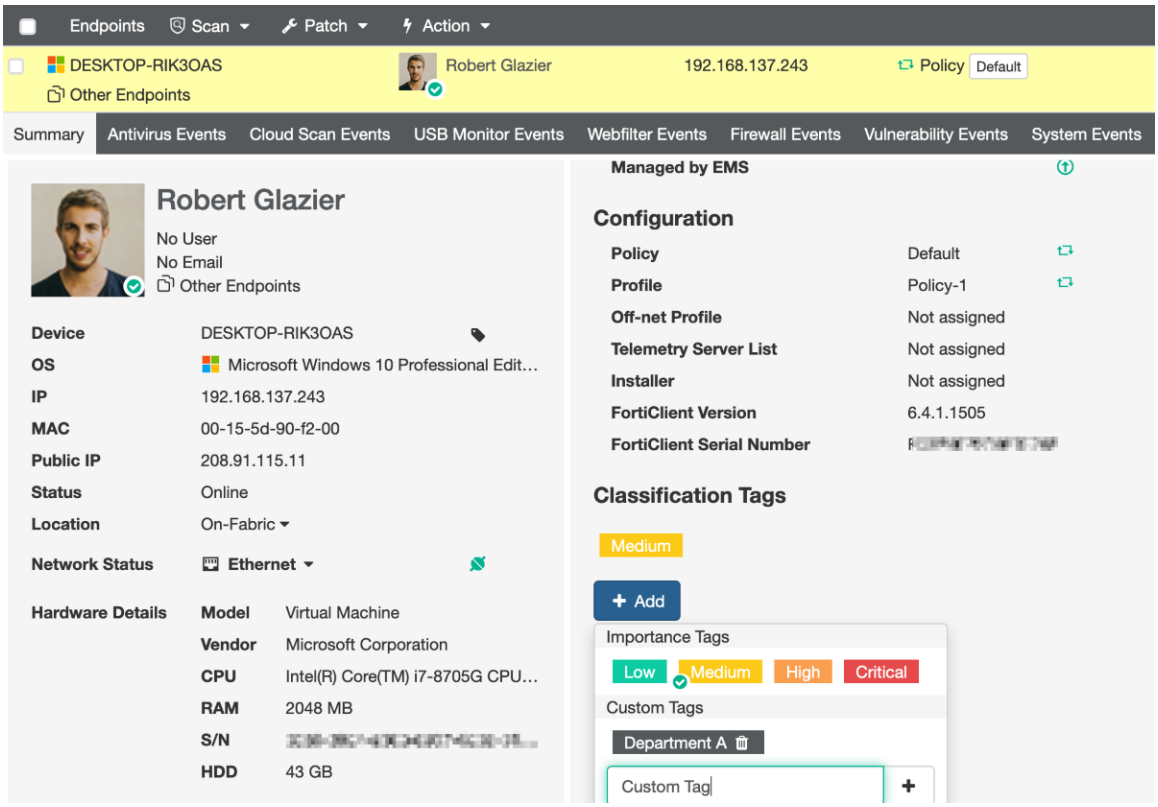
The following describes the process for configuring a classification tag and viewing the data in FortiAnalyzer:

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.

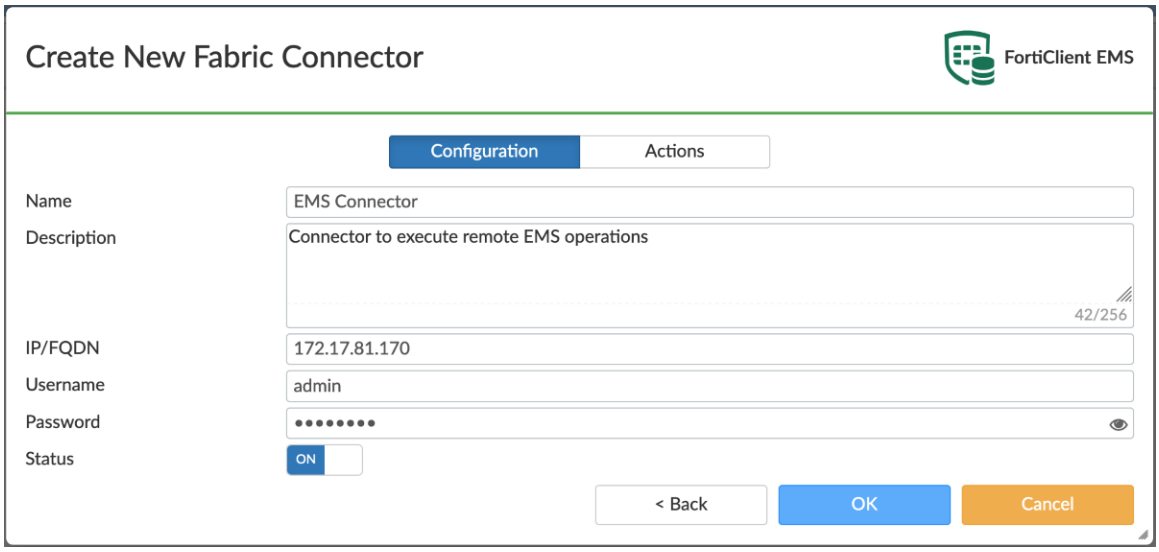
1. In EMS, go to *Endpoints*.
2. To apply tags to a single endpoint, go to the desired endpoint. Under *Classification Tags*, to create a new custom tag, click the *Add* button, enter the desired tag, the click the + button. You can also assign a new importance tag to the endpoint.



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:

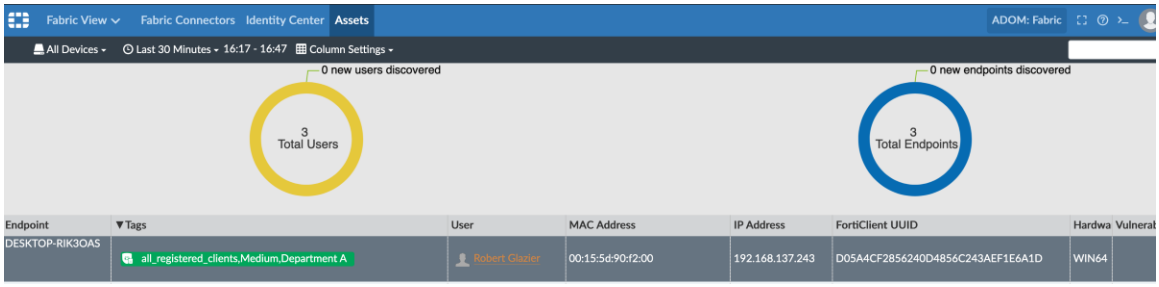
1. In FortiAnalyzer, go to *Fabric View*.
2. Click the *Fabric Connectors* tab, then click *Create New*.
3. Click the *FortiClient EMS* tile. The *Create New Fabric Connector* dialog opens.
4. In the *Configuration* tab, configure the connector settings, enter the EMS IP address and administrator credentials.



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 445.

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 FortiClient EMS. 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 FortiClient EMS 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 FortiClient EMS. The exported information is not visible in the FortiClient EMS 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 655.

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
- FortiClient EMS
- 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 255. 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 240.
- Enable *Remote HTTPS access*. See Configuring EMS settings on page 629.

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 FortiClient EMS.

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.

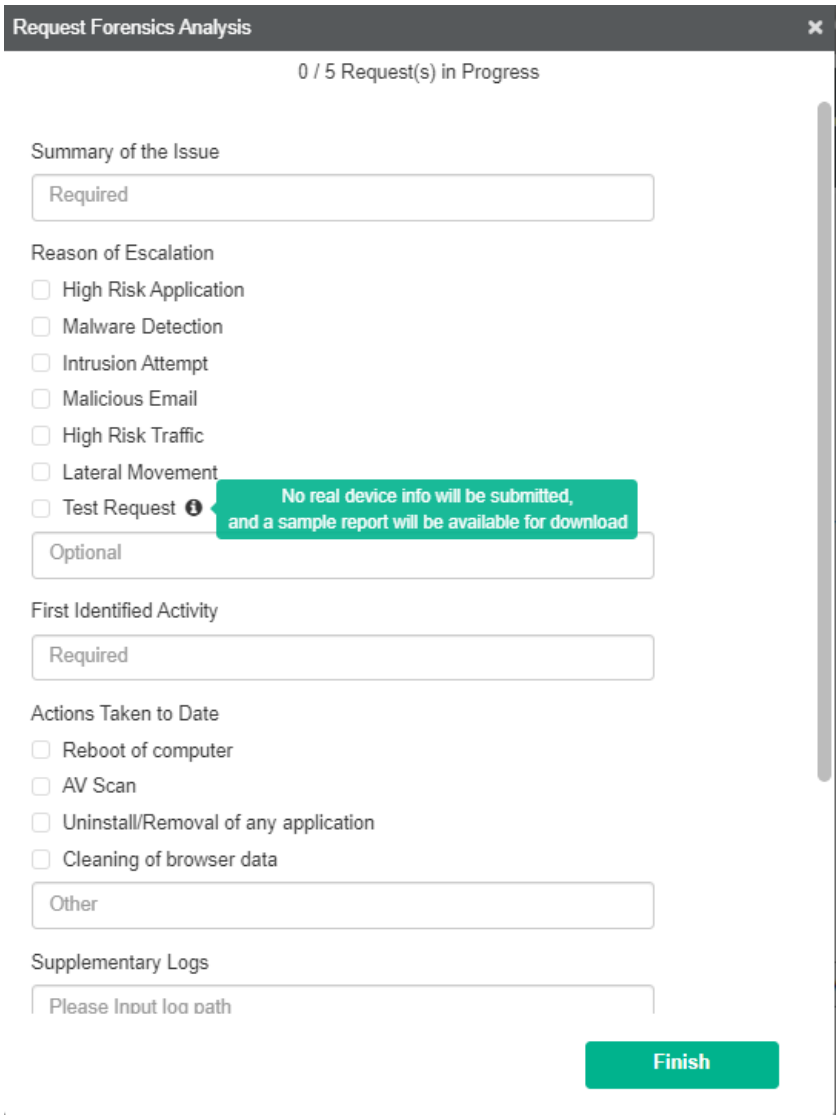
You can only request forensic analysis for Windows or macOS endpoints. FortiClient (macOS) 7.4.1 and later versions support forensic analysis.

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.

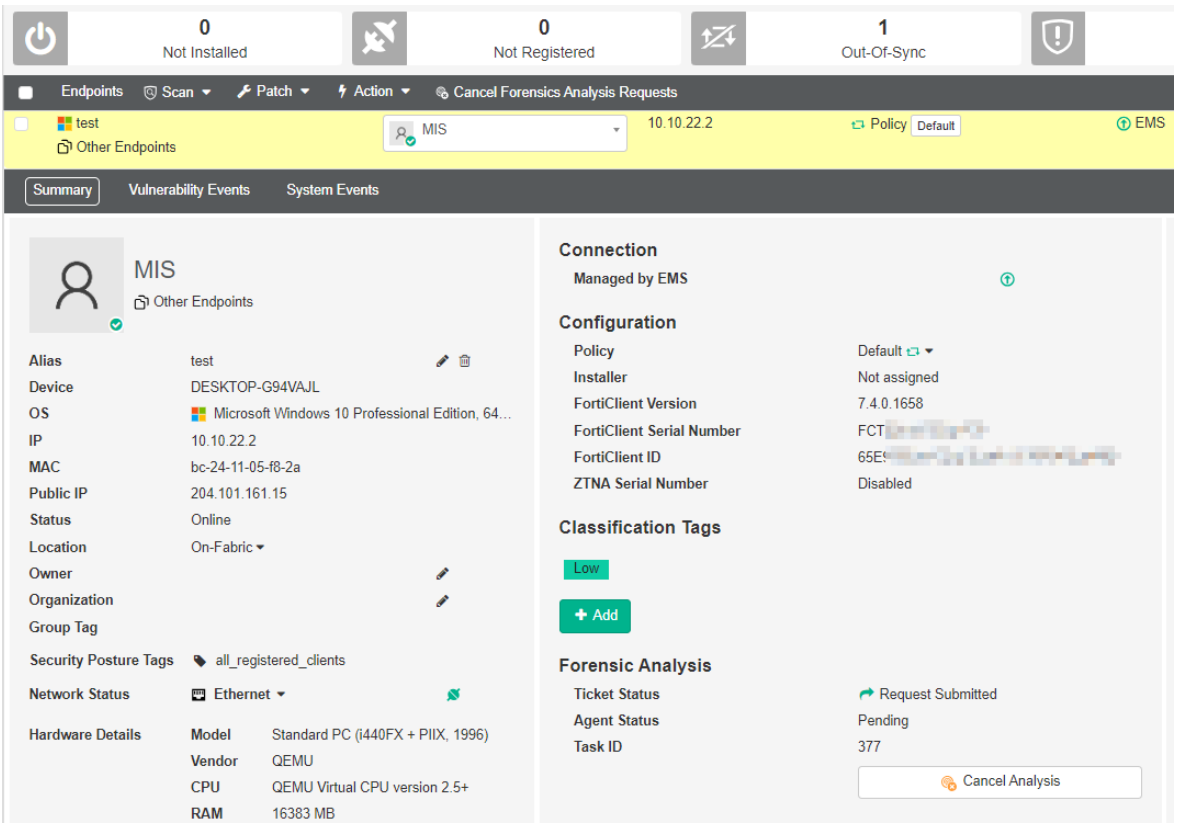
Click *Finish*. Once you submit the request, EMS notifies FortiClient and the forensics agent on the endpoint starts collecting forensics logs. FortiClient uploads the logs to the cloud and shares a link with the analyst. In EMS, you can see status of the analysis request in the endpoint summary:

Status	Description

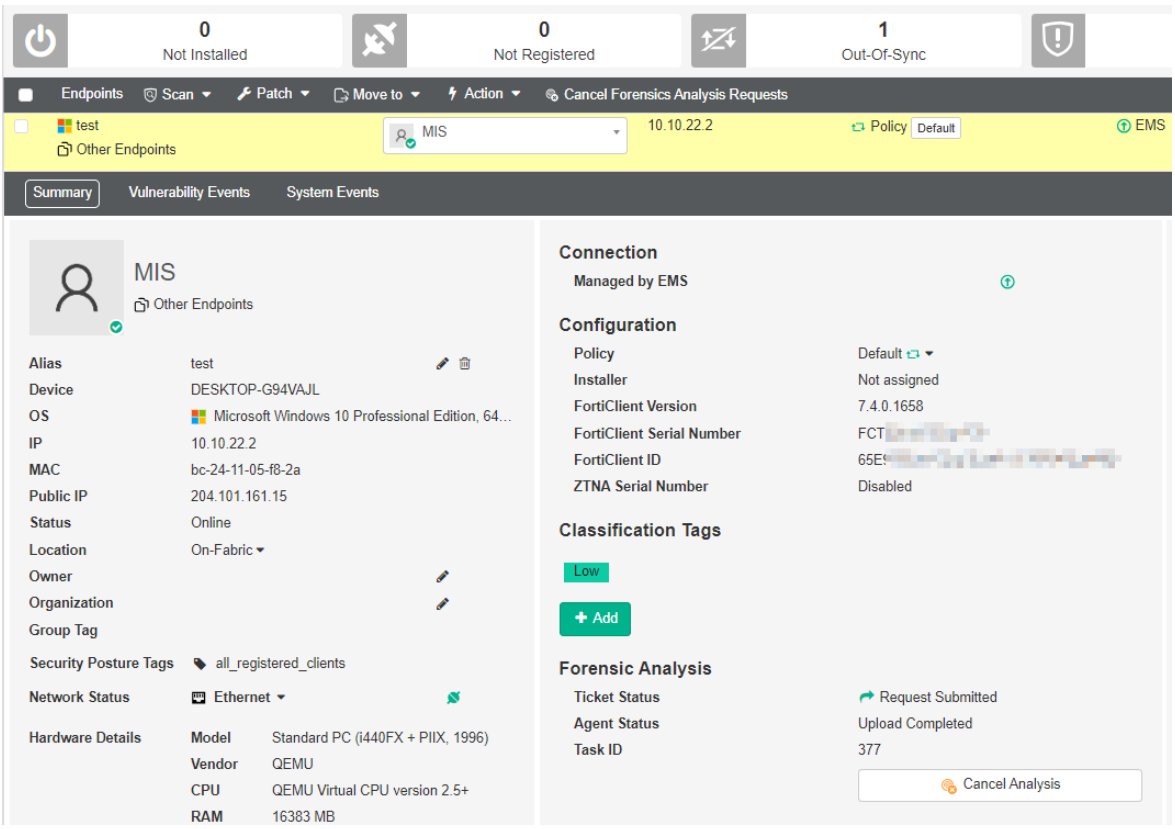
Ticket Status	Status of the ticket. Possible statuses are:
	• **Request Submitted**: EMS is creating the forensics analysis request and sending the information to the team.
	• **Pending**: Forensic analysis request has been initiated. The Forensics team has not yet assigned it to an analyst.
	• **In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

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.
Task ID	Request ID in the FortiGuard forensics system.

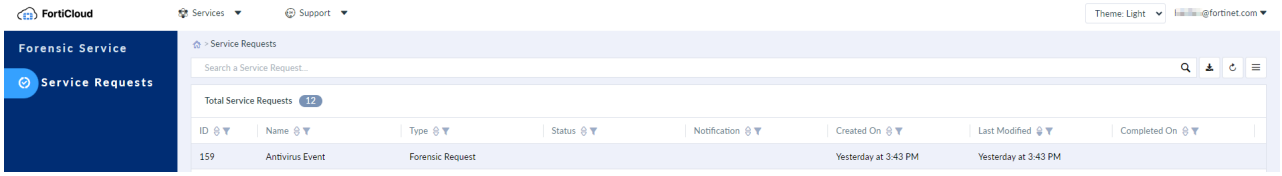
The following shows that EMS is creating the forensics analysis request and sending the information to the team. EMS has notified FortiClient that a forensic analysis request is submitted, but the forensic agent is not running yet:



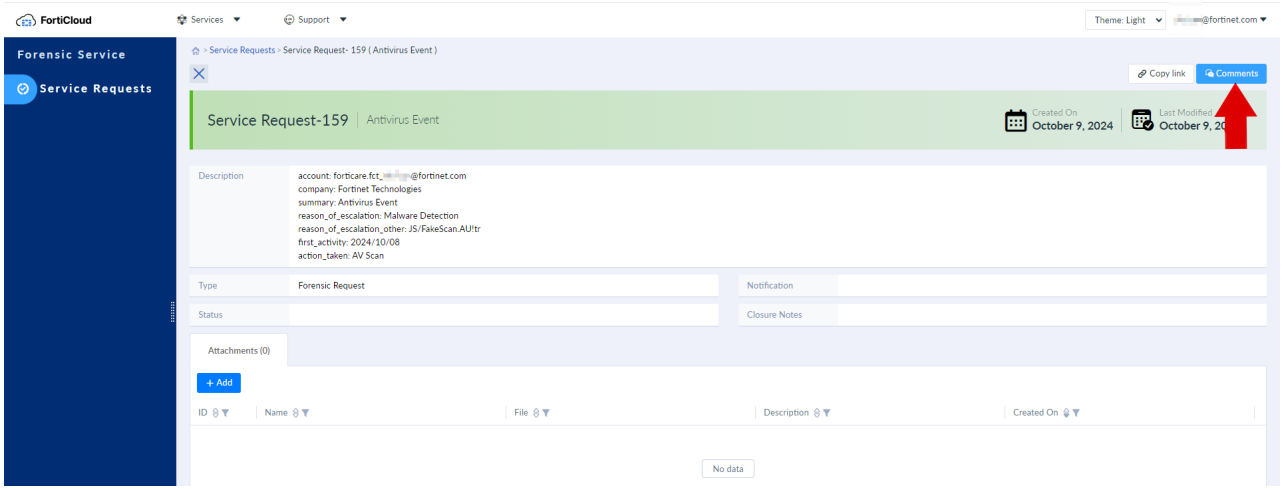
In the following screenshot, the *Agent Status* has updated to *Upload Completed*. FortiClient has completed uploading the logs to the cloud.



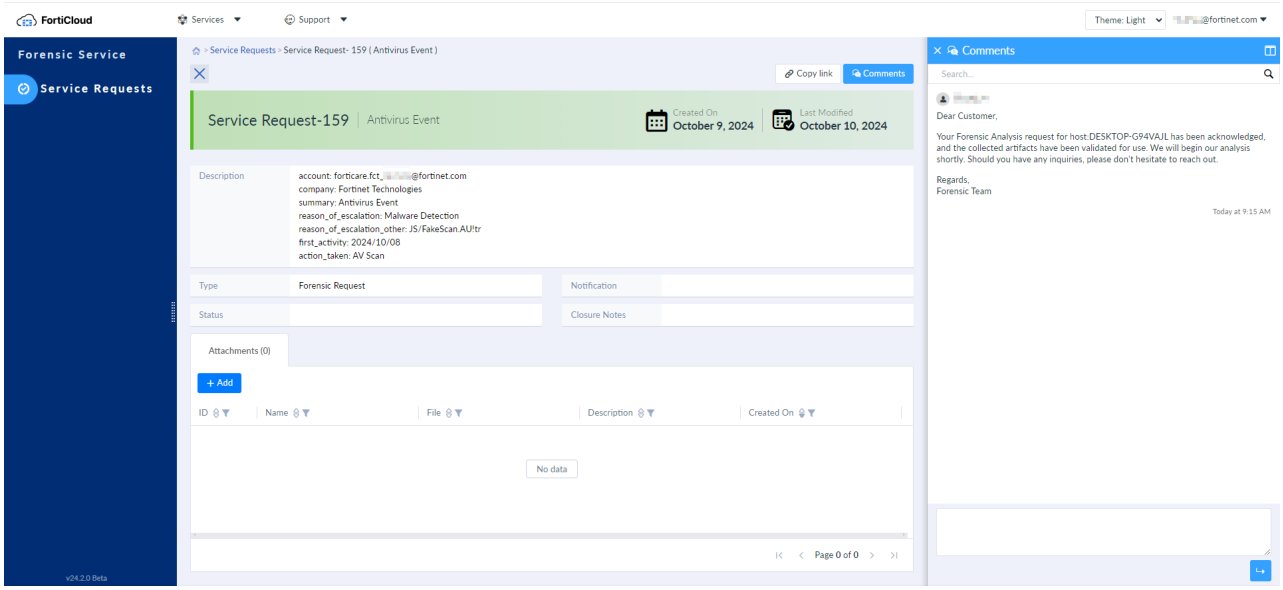
5. Do one of the following:
   - Log in to the Forensic Service portal using your FortiCloud credentials.
   - If using FortiClient Cloud, go to the *Forensics Analysis* tab on the left, then click the link to the Forensics Service portal. The link may not be available if the analyst has not created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



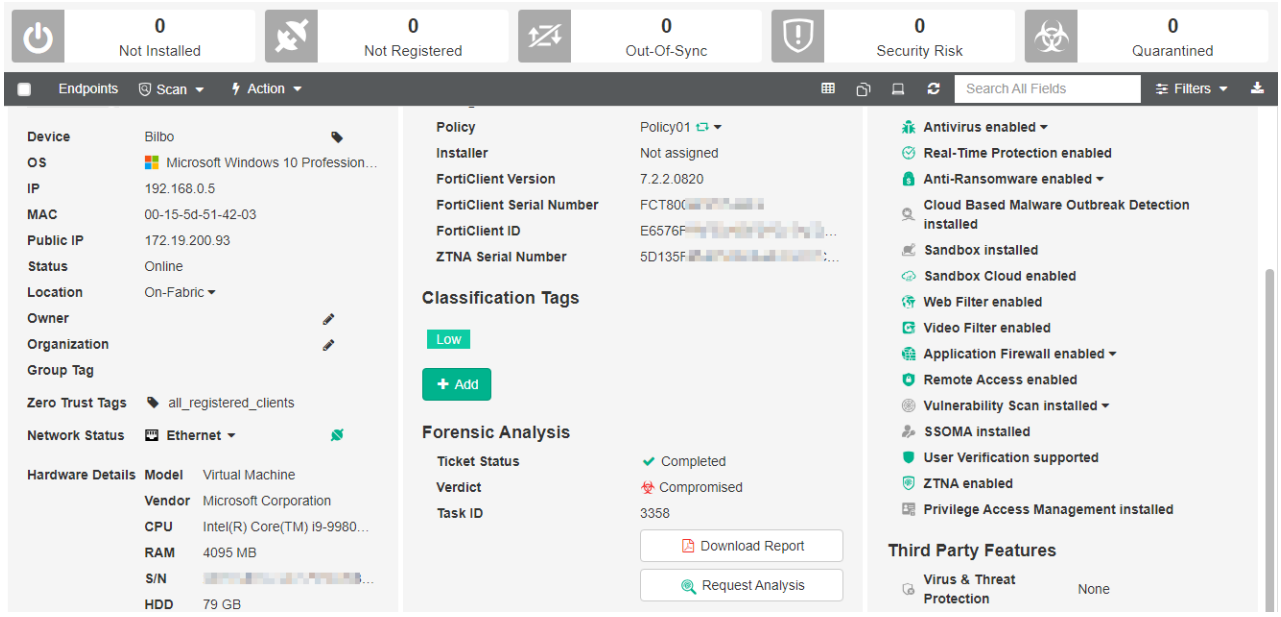
7. The service request page displays information about your request. Click *Comments* in the upper right corner.



8. 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.



9. 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
FCT80
FortiClient ID
E6576F
ZTNA Serial Number
5D135F
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

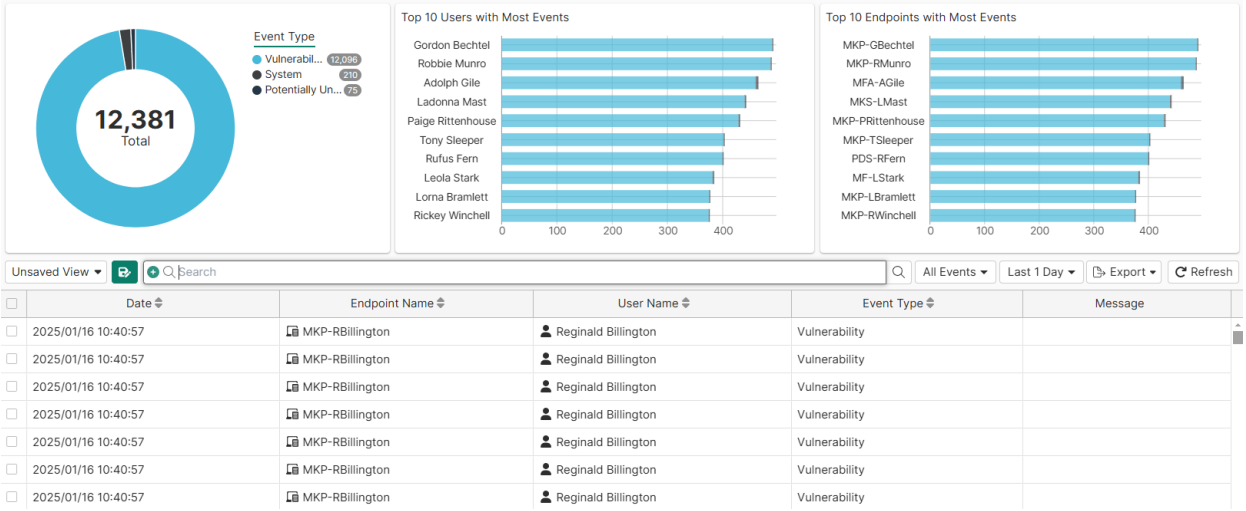
There is an *Endpoints* > *All Events* page available where you can view all events from all endpoints and take actions as necessary.

For Web Filter on page 422 events, only events of the *Block* and *Warn* categories are displayed here. Events of the *Allow* and *Monitor* categories are not displayed.

If using on-premise EMS, this feature requires integrating EMS with an Elasticsearch (ES) time-series database (DB). Otherwise, *Endpoints* > *All Events* is unavailable. If using FortiClient Cloud, this feature is available by default.

If using this feature with on-premise EMS, see:

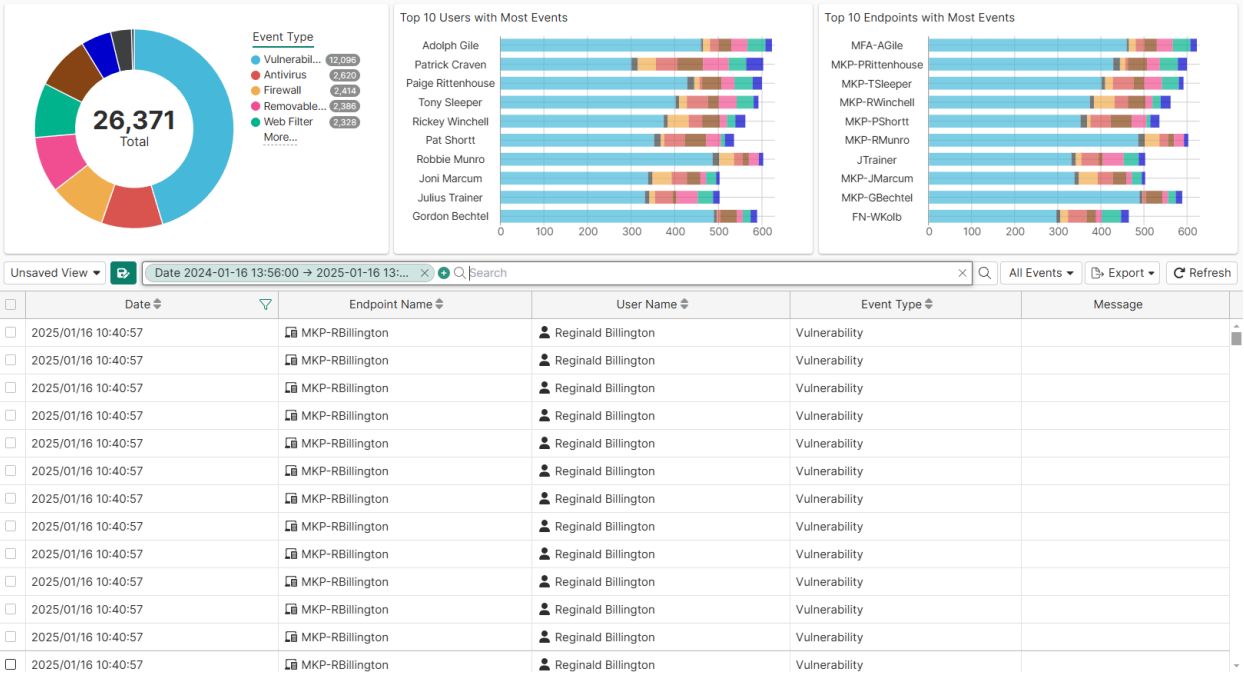
- Installing EMS with ES integration on page 210
- Enabling ES integration after EMS install on page 211
- EMS event-specific indexes on page 212
- ES sizing on page 213



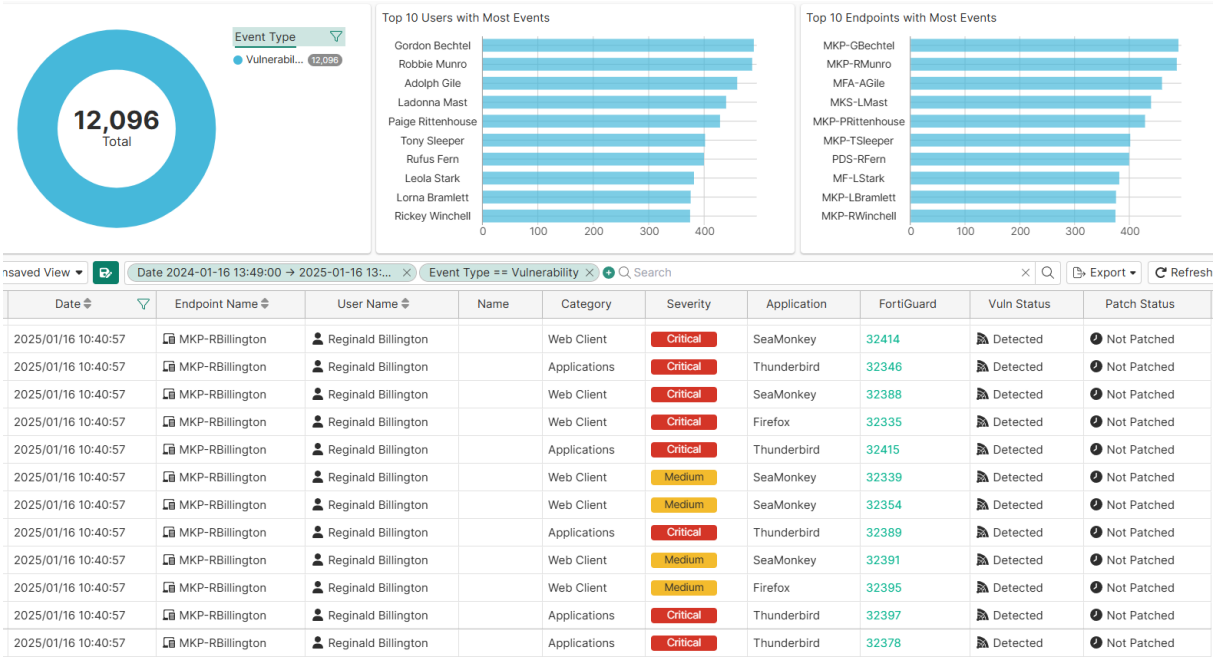
The top of the page contains the following charts:

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 176.

Installing EMS with ES integration

The following provides EMS installation instructions specific to enabling the Elasticsearch (ES) integration. For other EMS install information, see Installation on page 53.

This document does not provide extensive instructions for configuring the ES DB cluster. It assumes that you have already configured an ES DB cluster. To set up the ES cluster and nodes, see Set up Elasticsearch.



EMS can connect to existing ES clusters that are running ES 8.14.0 or later.

To install EMS with ES integration:

To install EMS with ES integration, you must use the following parameters:

Parameter	Description
`elastic_api_key`	Having EMS connect to the ES cluster using an API encoded key, rather than username/password, is considered best practice. Provide the encoded version of the key to EMS.

Parameter	Description
`elastic_ca_path`	If the ES cluster is set up to strictly check for a client certificate, you must provide the CA certificate to EMS. This must be a fully qualified path to the CA certificate file. Store the file in a location outside of `/opt/forticlientems` and be readable by the forticlientems user or group. For example, you may configure the following: `--elastic_ca_path /data/certs/es_ca.crt`
`elastic_hosts`	ES server IP address and port that ES uses to communicate with EMS in <ES server IP address:port> format. If you have multiple primary ES server nodes, provide their <IP address>:<port> in a comma-separated list with no whitespace in between. For example, you may configure the following: `elastic_hosts "node1.local:8000,node2.local:8000,node3.local:8000"`
`elastic_password`	Password for ES user created for EMS.
`elastic_user`	Username to use to connect to ES. If you provide both an API key and username and password, EMS prefers to use the API key and ignores the username and password.
`enabled_event_feature`	Enable EMS services required for using the new DB for storing and querying events.



If the elastic cluster is set up to require a certificate for SSL, you must copy the CA certificate to the EMS server in advance to a location accessible by the forticlientems user. Store this file outside of `/opt/forticlientems` as that directory is recycled during EMS upgrades.

The following provides an example install command:

```
forticlientems_7.4.3.amd64.bin -- --enabled_event_feature --elastic_hosts "10.152.78.248:8000" --
elastic_user emai --elastic_password Fortinet123# --elastic_ca_path /home/emai/Desktop/ca.crt
```



The example command configures Fortinet123# as the password. Ensure that you configure your own unique password as to not compromise the security of your installation.

Enabling ES integration after EMS install

This document does not provide extensive instructions for configuring the ES DB cluster. It assumes that you have already configured an ES DB cluster. To set up the ES cluster and nodes, see Set up Elasticsearch.



EMS can connect to existing ES clusters that are running ES 8.14.0 or later.

To enable All Events after EMS install:

Use the EMS CLI tool:

```
sudo emscli config set events --enabled=true --es.hosts="<host1:port1>,<host2:port2>" --
es.key=<api key> [--es.user=<user>|--es.password=<password>|--es.cert=<full qualified path to the
CA cert file>]
```

Parameter	Description
`es.key`	Having EMS connect to the ES cluster using an API encoded key, rather than username/password, is considered best practice. Provide the encoded version of the key to EMS.
`es.cert`	If the ES cluster is set up to strictly check for a client certificate, you must provide the CA certificate to EMS. This must be a fully qualified path to the CA certificate file. Store the file in a location outside of `/opt/forticlientems` and be readable by the forticlientems user or group. For example, you may configure the following: `--es.cert=/data/certs/es_ca.crt`
`es.hosts`	ES server IP address and port that ES uses to communicate with EMS in <ES server IP address:port> format. If you have multiple primary ES server nodes, provide their <IP address>:<port> in a comma-separated list with no whitespace in between. For example, you may configure the following: `es.hosts="node1.local:8000,node2.local:8000,node3.local:8000"`
`es.password`	Password for ES user created for EMS.
`es.user`	Username to use to connect to ES. If you provide both an API key and username and password, EMS prefers to use the API key and ignores the username and password.
`enabled=true`	Enable EMS services required for using the new DB for storing and querying events.

EMS event-specific indexes

When EMS connects to the Elasticsearch (ES) cluster, it checks whether the indexes it needs exist. If the indexes do not exist, EMS creates the necessary indexes. EMS creates and uses the following indexes to store its events:

Index	Stores...
forticlientems_vulns_v0	Endpoint events related to vulnerability detection and resolution. EMS stores one document per vulnerability detected per each endpoint and stores the vulnerability state (open or resolved).
forticlientems_alerts_v0	Endpoint-related alerts stemming from malware detection. EMS stores one document per event for each endpoint.

Index	Stores...
forticlientems_sysevs_v0	Endpoint system events, including: • Certificate signing • Receiving, acknowledging, and snoozing one-way messages • Connecting to or disconnecting from EMS • Changes in the network connections, such as connecting to or disconnecting from VPN or Wi-Fi EMS generates one document per event for each endpoint.
forticlientems_pua_v0	Stores events related to potentially unwanted applications (PUA). EMS stores one document per PUA event for each endpoint and stores the detection state (detected or resolved).

ES sizing

This guide provides recommendations for setting up an Elasticsearch (ES) cluster to store and manage event data that EMS processes. The sizing considerations in this guide are based on estimated event ingestion rates and data retention requirements.

EMS generates events for different events that endpoints report, including:

- Vulnerability detection and resolution
- Antivirus (AV), malware, or ransomware scans
- Telemetry events
- Web Filter actions

Event data overview

Each event stored in ES has the following characteristics:

- **Event size**: ~3 KB per event (in transit) / ~0.5 KB per event on disk
- **Events per day**: ~10000-15000 per 1000 endpoints
- **Minimum data retention**: 45 days
- **Growth consideration**: scales linearly with the number of endpoints.

Storage calculation

To estimate the total storage required, calculate as follows:

Daily data ingestion

Consider that for every 1000 endpoints, the daily data ingestion is expected to range as follows:

- **Minimum**: 10000 * 0.5 KB = 5 MB/day
- **Maximum**: 15000 * 0.5 KB = 7.5 MB/day

Considering that ES has minimum 45-day retention storage, the retention has the following range for storage requirements:

- **Minimum**: 5 MB * 45 = 225 MB
- **Maximum**: 7.5 MB * 45 = 337.5 MB

Thus, for every 1000 endpoints, EMS uses ~225 MB to 340 MB of raw storage.

ES has storage overhead due to indexing, replicas. The following summarizes the actual storage needs:

- **Indexing overhead**: indexes add metadata and inverted indexes, which increase storage usage by ~20-30%.
- **Replica factor** to ensure high availability, setting up at least one replica per primary shard is recommended, effectively doubling storage.
- **Total estimated storage** considering indexing overhead (~30%) and one replica, the total required storage per 1000 endpoints is calculated as follows: (225 to 337.5 MB) * 1.3 * 2 = 585 to 877.5 MB

Cluster sizing based on endpoints

Number of endpoints	Events per day	Estimated storage with overhead and replica (GB)
10000 to 20000	150000 to 300000	10 to 18
20000 to 50000	300000 to 750000	18 to 45
50000 to 75000	750000 to 1250000	45 to 65
75000 to 150000	1250000 to 2300000	65 to 130
150000 to 250000	2350000 to 3800000	130 to 220

ES node sizing recommendations

To ensure smooth operation, consider the following hardware requirements per node:

Cluster size	vCPUs per node	RAM per node (GB)	Disk type	Number of data nodes
Small (up to 40000 endpoints)	4	16	SSD (NVMe preferred)	3
Medium (40000 to 80000 endpoints)	8	32		3 to 5
Large (80000 to 250000 endpoints)	16	64		5 to 7

Additional recommendations

- **Dedicated primary nodes**: 3 nodes, 2 vCPUs, 8 GB RAM each
- **Shards and indexes**: keep shard size between 20 to 50 GB.
- **Index lifecycle management:**
  - Move older data to warm nodes with slower disks after 30 days.
  - Delete or archive data after 45 days if storage is a concern.

Conclusion

This guide provides a baseline for sizing the ES cluster based on expected event volume and retention requirements for EMS. The number of daily events can increase depending on configuration and the number of events that endpoints generate. For example, the following settings can influence the number of events that endpoints generate:

- Frequency for Vulnerability and AV scans
- Keepalive timeout
- Number of restrictive Web Filter rules

Required ES permissions

To connect to the Elasticsearch cluster, the user credentials provided to EMS require the following index privileges for the forticlientems index:

- create_index
- delete_index
- index
- view_index_metadata
- write
- create
- all
- manage

Index lifecycle

EMS does not enforce nor manage index lifecycle policies, as it is the Elasticsearch (ES) cluster administrator's responsibility to set up their own policies for the EMS-created indexes. Keeping up to 45 days of data in hot storage is recommended. However, if desired, you can keep data older than 45 days. If keeping data older than 45 days, using index lifecycle policies is recommended to move older data to warm and cold storage, based on your needs, to improve the efficiency of the memory used that the ES nodes use. As a guideline, the following is proposed:

Data age	Phase
Up to 45 days	Hot
Between 45 to 120 days	Warm
More than 120 days	Cold

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 FortiClient EMS, FortiClient EMS places them in the desired group. In this situation, the process is as follows:

1. In FortiClient EMS, 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 218.
2. Create a FortiClient deployment package. Specify the "HQ" installer ID when creating or uploading the installer. See Adding a FortiClient installer on page 230.
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 FortiClient EMS, 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 FortiClient EMS, 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 218.
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 FortiClient EMS, 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 218.
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 FortiClient EMS, 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 218.
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

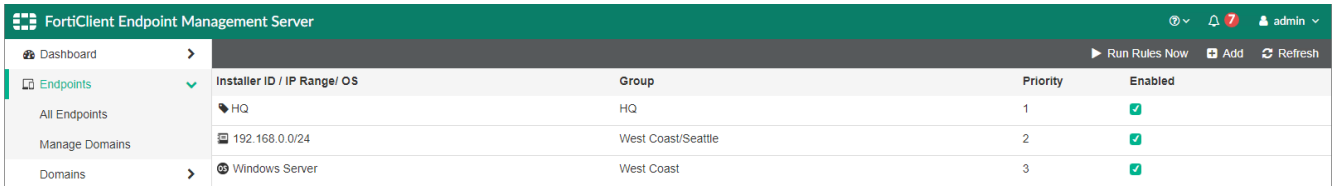
An endpoint may be eligible for multiple group assignment rules. When an endpoint is eligible for multiple endpoint group assignment rules, two factors determine which rule EMS applies to the endpoint:

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.

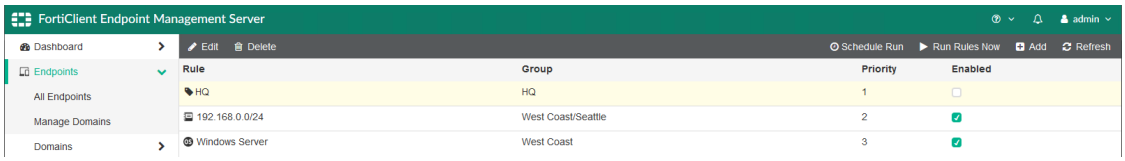
To change rule priority levels:

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

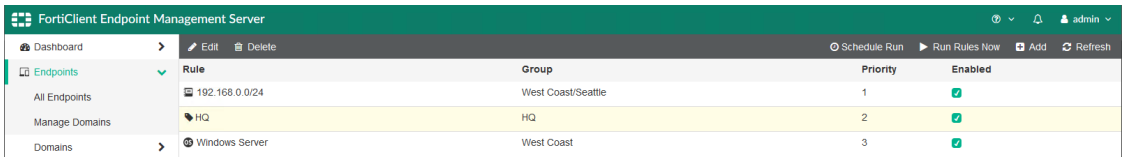
In the example, consider an endpoint where FortiClient was deployed using the "HQ" installer ID and has an IP address that belongs to the 192.168.0.0/24 subnet. The endpoint applies for two rules. In this case, the endpoint is placed in the HQ group, since the HQ rule has a higher priority level than 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. FortiClient EMS 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*. FortiClient EMS then dynamically creates any group that does not exist. For example, if both the *West Coast* and *Seattle* groups do not exist, FortiClient EMS creates both groups with the desired hierarchy. If the *West Coast* group exists, FortiClient EMS 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. FortiClient EMS 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*. FortiClient EMS then dynamically creates any group that does not exist. For example, if both the *West Coast* and *Seattle* groups do not exist, FortiClient EMS creates both groups with the desired hierarchy. If the *West Coast* group exists, FortiClient EMS 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. FortiClient EMS 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*. FortiClient EMS then dynamically creates any group that does not exist. For example, if both the *West Coast* and *Seattle* groups do not exist, FortiClient EMS creates both groups with the desired hierarchy. If the *West Coast* group exists, FortiClient EMS 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 599. 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. FortiClient EMS 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*. FortiClient EMS then dynamically creates any group that does not exist. For example, if both the *West Coast* and *Seattle* groups do not exist, FortiClient EMS creates both groups with the desired hierarchy. If the *West Coast* group exists, FortiClient EMS 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*.

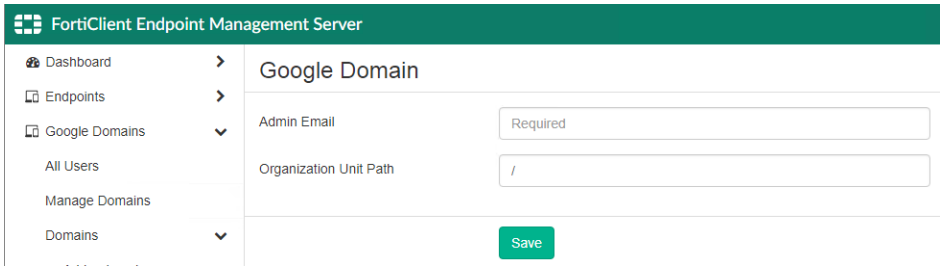
Google Domains

FortiClient EMS 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 FortiClient EMS 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

After you add domains to FortiClient EMS, 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 FortiClient EMS.

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

Google Users — Clear Filters

Name	Email	Last Login	Last Policy Retr	Domain	Organization Path
Art3 Sikes	art3.sikes@s...	8/4/2016 1:1...	Never Retrie...	schoolz...	/Young Lady's School/staff/admin
bob bob	bob.bob@ys...	8/6/2016 1:0...	Never Retrie...	schoolz...	/test
Catherine Seely	Catherine.Se...	7/25/2016 9:...	Never Retrie...	schoolz...	/Young Stars School
Dean Cagle	Dean.Cagle...	8/5/2016 10:...	Never Retrie...	schoolz...	/Young Lady's School/staff/admin
Dennis Auger	Dennis.Auger...	7/15/2016 9:...	Never Retrie...	schoolz...	/Young Lady's School/students...
Edgar Bayles	Edgar.Bayles...	8/9/2016 12:...	Never Retrie...	schoolz...	/Young Stars School/students/...
Efrain2 Tague	Efrain2.Tagu...	8/2/2016 10:...	Never Retrie...	schoolz...	/Young Stars School/students/...
Emilio Freitag	emilio.freitag...	7/25/2016 9:...	Never Retrie...	schoolz...	/Young Lady's School/students...
Garry Heinrich	Garry.Heinric...	8/3/2016 8:2...	Never Retrie...	schoolz...	/Young Lady's School/staff/admin
Gerard Rhoa...	gerard.rhoad...	7/14/2016 11...	Never Retrie...	schoolz...	/Young Lady's School/staff
jiaping xu	jpxu@school...	8/9/2016 6:4...	Never Retrie...	schoolz...	/
Joey Albrecht	joey.albrecht...	8/2/2016 10:...	Never Retrie...	schoolz...	/Young Lady's School/staff
KeriNew Coc...	Keri.Cochran...	8/4/2016 1:1...	Never Retrie...	schoolz...	/Young Lady's School/test
Leann Bast	Leann.Bast@...	8/9/2016 12:...	Never Retrie...	schoolz...	/Young Stars School/students/...

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 FortiClient EMS 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 Initially deploying FortiClient software to endpoints on page 13.

Manage Deployment

Creating a deployment configuration

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*. 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

Field	Description
	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.
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.
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 226.
Enable the Deployment	Enable or disable.

4. Click *Save*.

Managing deployment configuration priority levels

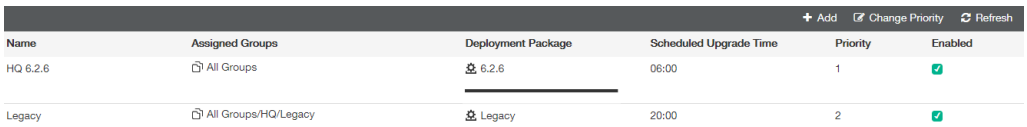
An endpoint may be eligible for multiple deployment configurations. When an endpoint is eligible for multiple endpoint deployment configurations, the following factors determine which configuration EMS applies to the endpoint:

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.

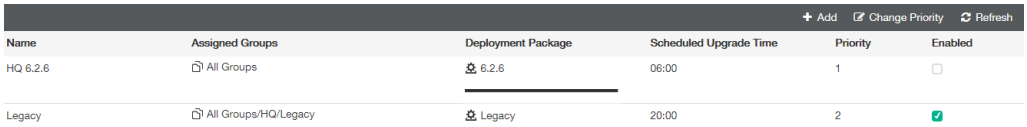
To change configuration priority levels in the GUI:

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*.

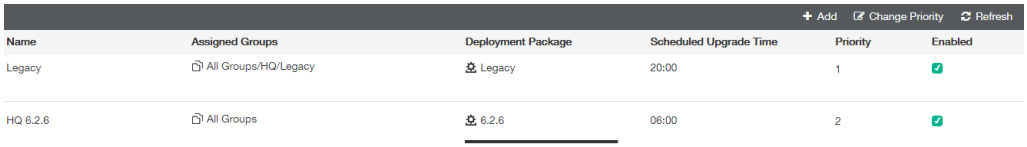
In the example, consider an endpoint that belongs to the Legacy group. The endpoint applies for two configurations. In this case, EMS applies the HQ deployment configuration to the endpoint, since the HQ configuration has a higher priority level than the Legacy configuration.



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/disabling a deployment configuration

To enable/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 FortiClient EMS

You can deploy a FortiClient software update from FortiClient EMS. 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 the 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 225. 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

Deploying different installer IDs to endpoints using the same deployment package

As Installer ID group assignment rules on page 216 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 230.
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 218.
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_7.4.3_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_7.4.3_x64.exe /v"GROUP_TAG=HR"
FortiClientSetup_7.4.3_x64.exe /v"GROUP_TAG=Marketing"
FortiClientSetup_7.4.3_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 FortiClient EMS, you cannot edit it. You can delete the deployment package from FortiClient EMS, and edit the installer outside of FortiClient EMS. You can then add the edited installer to FortiClient EMS.

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

If *Sign Software Packages* 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 629.

To create an installer or install config file:

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 the FortiClient release version to install.
Patch	Select the specific FortiClient patch version to install.
Build	Available if you select *This EMS has no internet connection*. Enter the FortiClient build number 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 237.
Auto update to the	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 237.
This EMS has no internet connection	Enable if you want to create an install config 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 655.

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 259 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.

Option	Description
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.
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. FortiClient EMS automatically groups endpoints according to installer ID group assignment rules. See Group assignment rules on page 216. 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 228.
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.

Option	Description
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 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 599.

6. Click *Next*. The *Telemetry* tab displays the hostname and IP address of the FortiClient EMS 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 FortiClient EMS 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.

Option	Description
This EMS has no internet connection	Enable.

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 655.

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 259 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.

Option	Description
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.
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. FortiClient EMS automatically groups endpoints according to installer ID group assignment rules. See Group assignment rules on page 216. 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.

Option	Description
	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 228.
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 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 599.

6. Click *Next*. The *Telemetry* tab displays the hostname and IP address of the FortiClient EMS 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 FortiClient EMS 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.

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

Installer Type	Select *Upload packaged installers*.

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

Name	Enter the FortiClient deployment package name.
Notes	(Optional) Enter notes about the FortiClient deployment package.
Repacked installers	Upload a zip file that contains 64-bit Windows, macOS, and/or Linux custom installers. You can download FortiClient installers to use with FortiClient EMS from Fortinet Customer Service & Support. This requires a support account with a valid support contract. You can also download installers from FortiClient.com. Download the Windows, macOS, or Linux installation file. The installation files on the Fortinet Customer Service & Support and FortiClient.com websites are not available in .zip format. You must package the installer as a .zip file to upload it.

5. Click *Next*. The *Telemetry* tab displays the hostname and IP address of the FortiClient EMS server, which manage FortiClient once it is installed on the endpoint.
6. Click *Finish*. The FortiClient deployment package is added to FortiClient EMS and displays on the *Deployment Installers > FortiClient Installer* pane. The deployment package may include .exe (64-bit), .msi, .dmg, .rpm, or .deb files depending on the configuration. The end user can download these files to install FortiClient on their machine with the desired configuration.

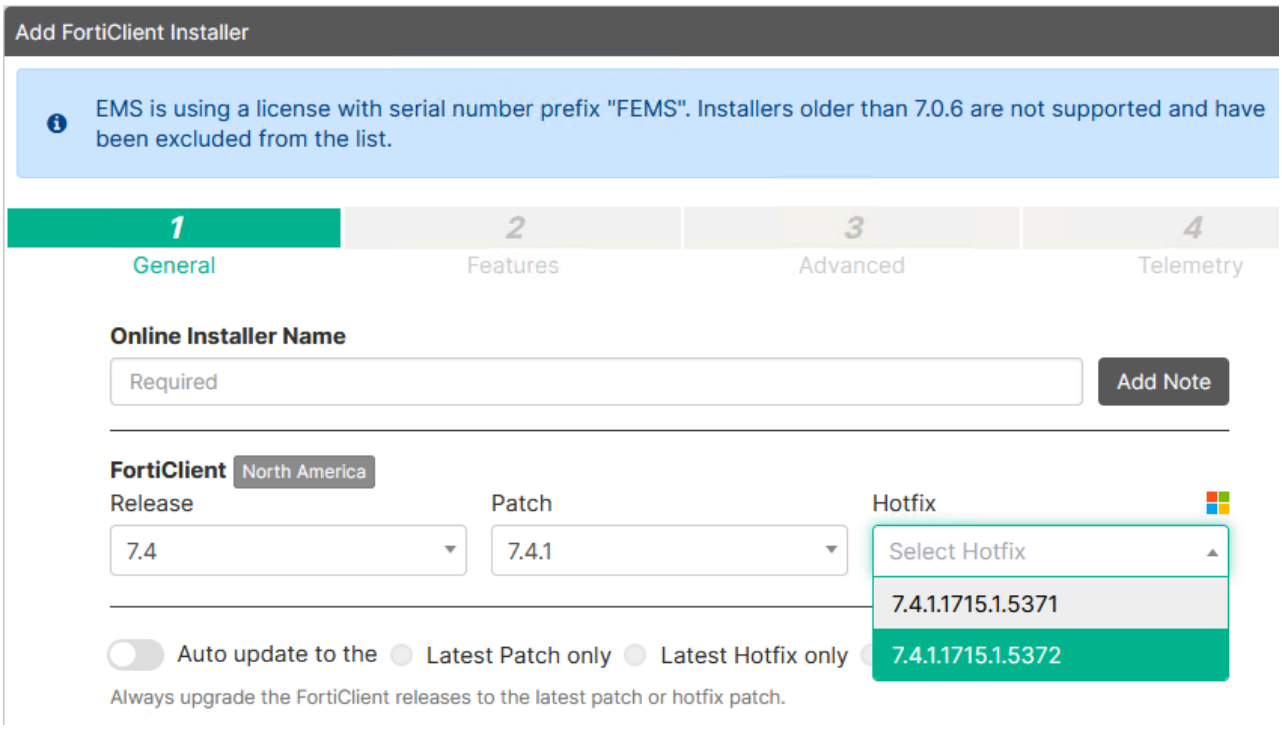
Adding a FortiClient hotfix installer

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:

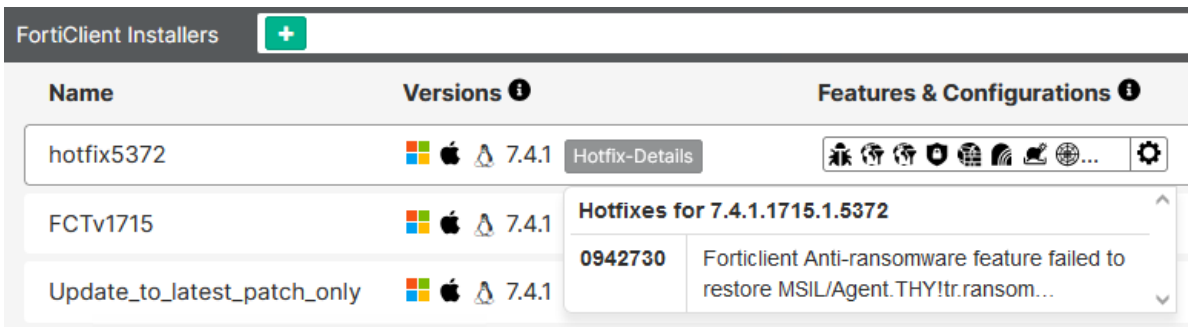
1. In EMS, go to *Deployment & Installers > FortiClient Installer*.
2. Click *Add*.
3. From the *Release* dropdown list, select the desired FortiClient version.
4. From the *Patch* release dropdown list, select the desired patch version.
5. If a hotfix is available for the selected patch, the *Hotfix*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

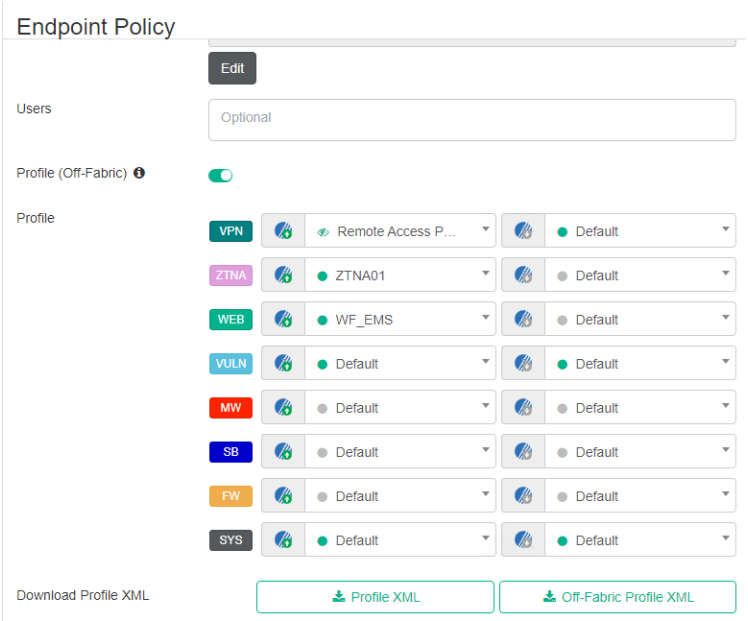
Adding an endpoint policy

To add an endpoint policy:

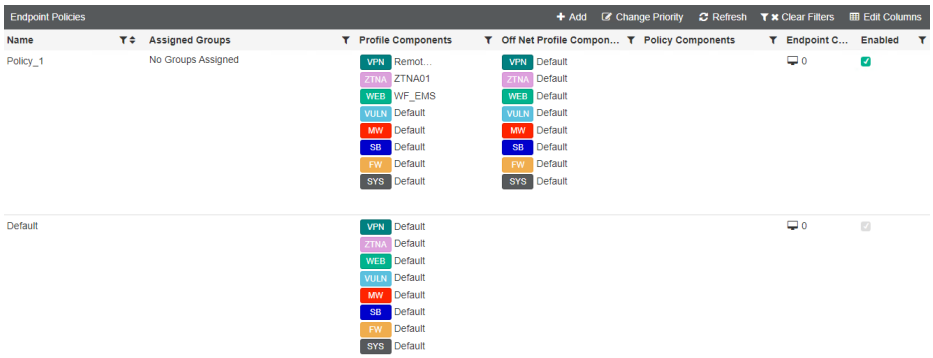
1. Go to *Endpoint Policy & Components* > *Manage Policies*.
2. Click *Add*.
3. Complete the following fields:

Field	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 EMS determines it to be 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.

Field	Description
	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.
Profile	From the dropdown lists, configure the desired endpoint profiles to apply to endpoints that EMS has applied the policy to. FortiClient EMS 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 you enable *Profile (Off-Fabric)*, 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 248.
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.

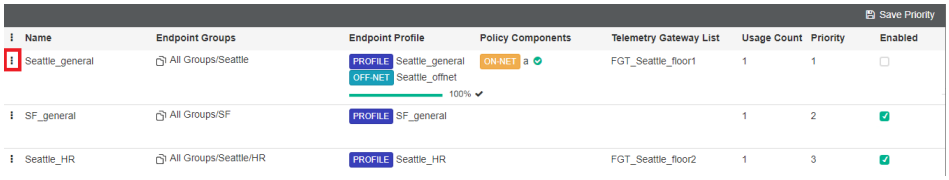
Managing endpoint policy priority levels

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.

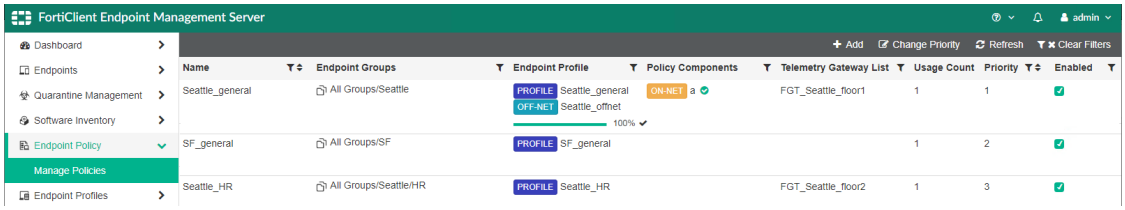


4. Click *Save Priority*.

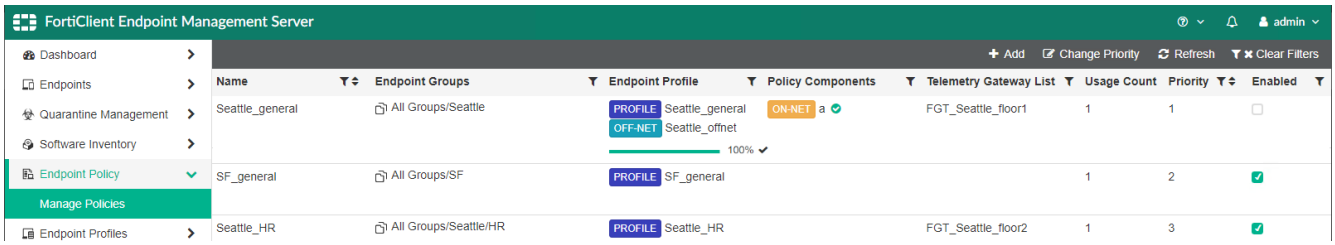
In the examples, there are three endpoint policies:

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.

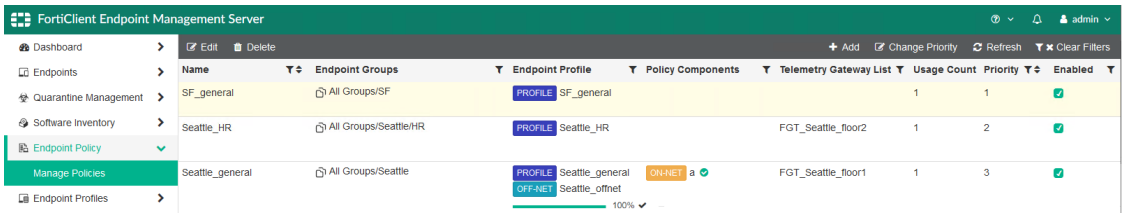


Consider that you then make the following changes:

- 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:

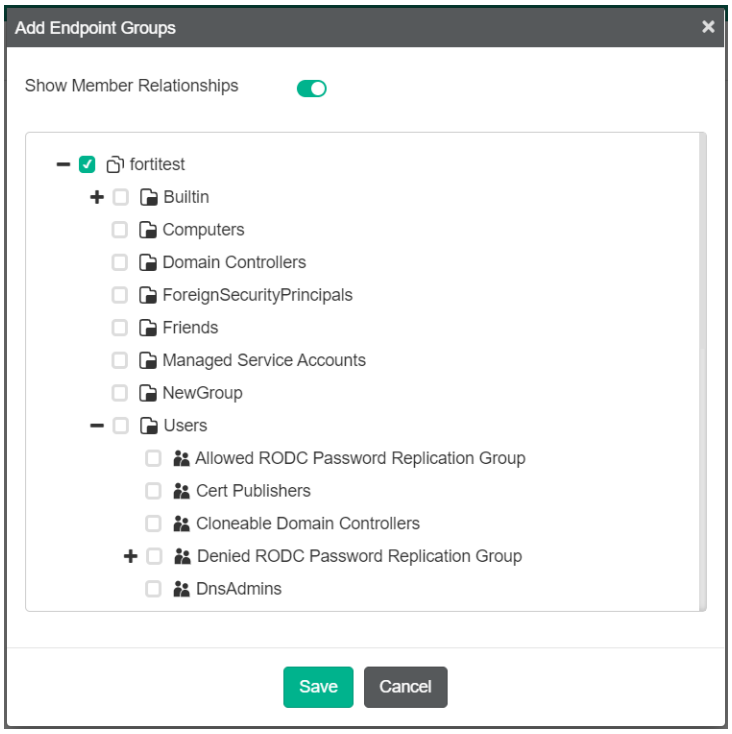
1. Go to *Endpoint Policy & Components Manage Policies*.
2. Click *Edit Columns*.
3. Enable or disable the columns as desired.
4. Click *Save*.

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*.



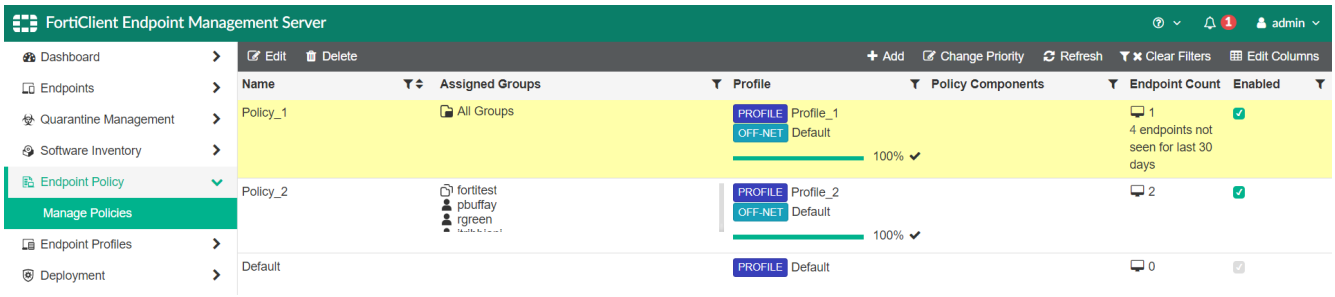
3. In the *Users* field, select the desired users.
4. Click *Save*.

When FortiClient connects to EMS, the following occurs:

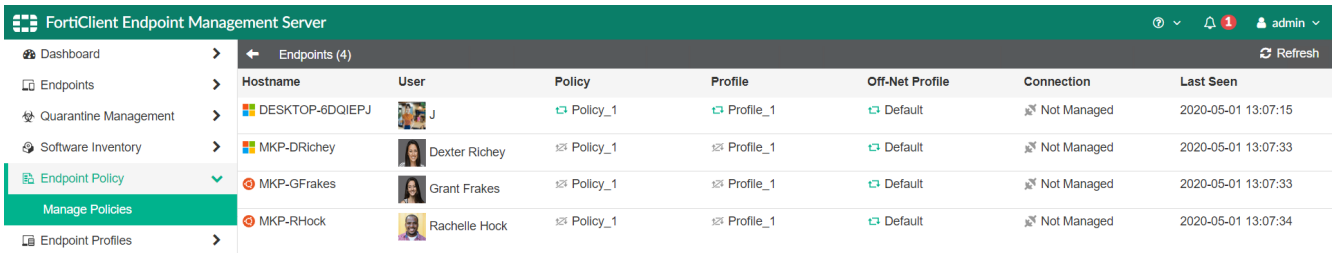
1. If a policy is assigned to the FortiClient user, EMS assigns that policy to the endpoint.
2. If there are policies for the FortiClient group container and/or user groups, EMS assigns the policy with the highest global priority.
3. If there are inherited policies for group containers and/or user groups,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

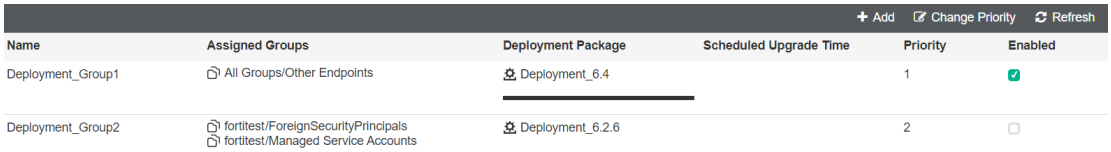


To deploy FortiClient to endpoints with user-based management:

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 225.

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 FortiClient EMS 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 465. 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 465.

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 240.

When a user switches accounts between a local non-domain account and a domain account on the same machine, 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 *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	In the *IP Address* and *MAC Address* area, configure the IP and/or MAC address for the desired DHCP server. For *DHCP Code*, configure the DHCP code for the desired DHCP server. You can configure just the *IP Address* and *MAC Address* fields, just the *DHCP Code* field, or all fields. If configuring the *IP Address* field, 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 251. 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* 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.
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.

Detection type	OS	Description
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.
Local IP/Subnet	• Windows • macOS • Linux • iOS (IP address only) • Android (IP address only)	In the *IP Range* field, enter an IP address range. In the *Default Gateway MAC Address* field, optionally enter the default gateway MAC address. EMS considers the endpoint as satisfying the rule if its Ethernet or wireless IP address is within the range specified and if its default gateway MAC address matches the one specified, if it is configured. Configuring the MAC address is optional. You can configure multiple addresses using the + button.
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 IPsec or SSL 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.

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 or 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.

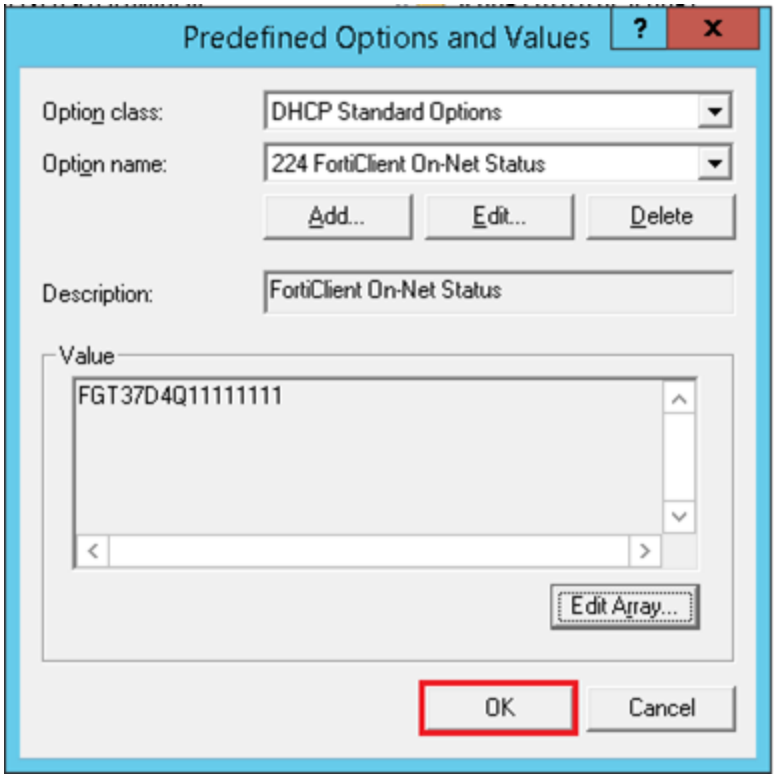
An endpoint has an offline on-fabric status when it cannot connect FortiClient Telemetry to EMS but is inside one of the on-fabric networks, or if no on-fabric rules are configured within the assigned policy.

To configure the DHCP code:

FortiClient can use a DHCP code or 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*.



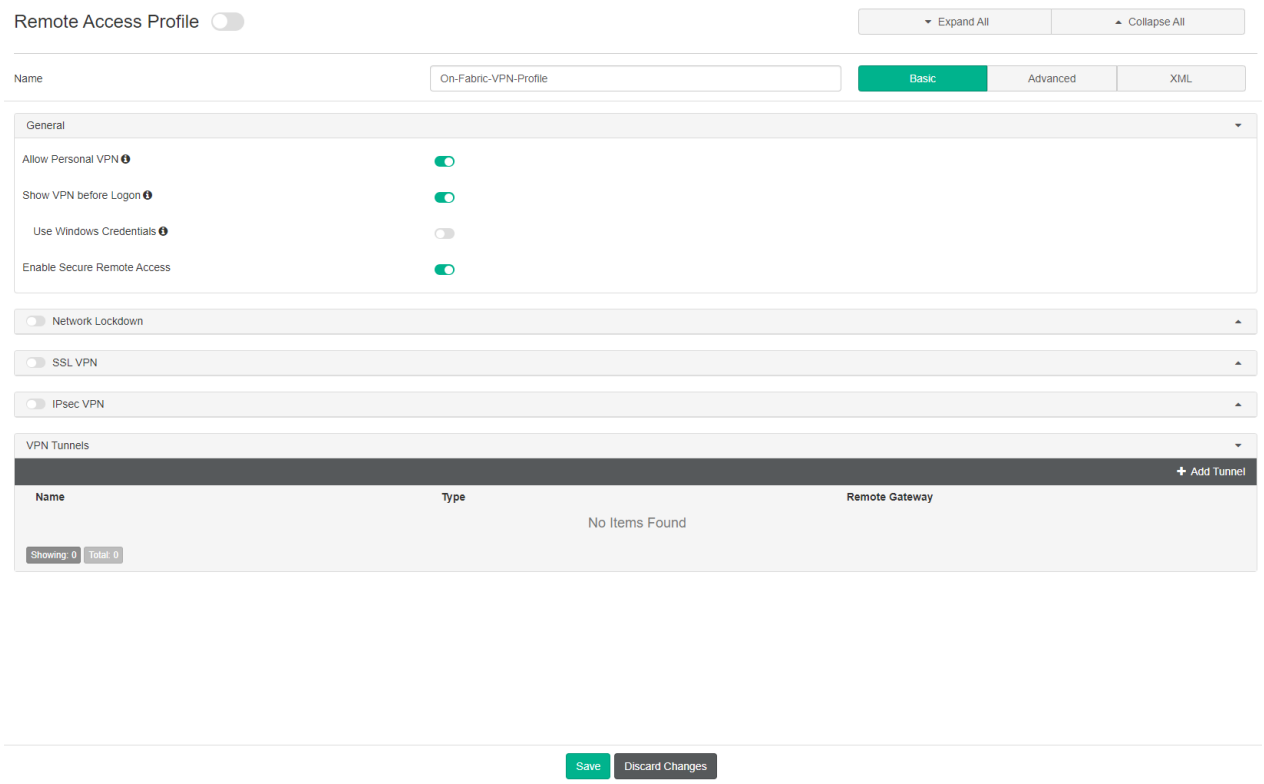
Source IP address anchoring for IPsec VPN

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 240.

Endpoint Profiles

FortiClient EMS has separate endpoint profiles for the following features:

- Remote Access on page 259
- ZTNA Destinations on page 408
- Web Filter on page 422
- Video Filter on page 440
- Vulnerability Scan on page 442
- Malware Protection on page 445
- Sandbox on page 455
- Firewall on page 460
- System Settings on page 465

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 240.

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. Configure the settings as desired.
5. 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 FortiClient EMS.

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, FortiClient EMS 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, FortiClient EMS 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 257.
   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 remote access. Enable or disable the eye icon to show or hide this feature from the end user in FortiClient.
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	Minimize FortiClient after successfully establishing a VPN connection.
Show Connection Progress	Display information on FortiClient dashboard while establishing connections.
Suppress VPN Notifications	Block FortiClient from displaying any VPN connection or error notifications.

Configuration		Description
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.
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 262 and IPsec VPN on page 267.
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 248.
	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.
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.
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.

Configuration	Description
	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).
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. Enter a value between 20 and 3600.
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 655.



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.
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
Enforce Disabling Smart Multi-Homed Name Resolution For Split DNS	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 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.

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 312.
Prompt for Username	Prompt for the username when accessing VPN.
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.
Enable SAML Login	Enable SAML SSO 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. 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 308.
Use External Browser as User-agent for SAML Login	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. See Using a browser as an external user-agent for SAML authentication in an SSL VPN connection on page 286.

Enable Azure Auto Login	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 (formerly known as Azure Active Directory) credentials. See Autoconnect on logging in as an Entra ID user on page 294.
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 495. 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 496. 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

This topic contains descriptions of IPsec VPN settings:

Configuration	Description
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 when connected to an IPv4 tunnel.
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.

Configuration	Description
	• FortiClient registers only its own tunnel interface IP address in the AD DNS server.
Do Not Accept Invalid Server Certificate	FortiClient does not complete the requested VPN connection when an invalid VPN server certificate is used.

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.
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 312.
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.
VPN Settings	
IKE	Select *Version 1* or *Version 2*.
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`

Field	Description

	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 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`

Field	Description

	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>`
	• `<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.
Authentication	Select the authentication method.

Field	Description
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. 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. 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.
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 IKE fragmentation.
Allow non-administrators to use machine certificates	Allow non-administrator users to use local machine certificates to connect IPsec VPN.
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.

Field	Description
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.
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.

Field		Description
		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.
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.

Field		Description
	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 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).

Field	Description
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.
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.
Enable SAML Login	Enable SAML SSO 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.
Use External Browser as User-agent for SAML Login	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. This option is only available for IKEv2 tunnels.
SAML Port	Enter the port number that FortiClient uses to communicate with the FortiGate, which acts as the SAML service provider.
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.

Field	Description
	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 495. 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 496. 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.

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. You can exclude high bandwidth-consuming applications. For example, you can exclude applications like the following from the VPN tunnel:

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

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

This feature does not support explicitly including traffic in the VPN tunnel.

Some applications may require you to disable IPv6 on the network for this feature to function.



FortiClient (macOS) and (Linux) do not support source application-based split tunnel.

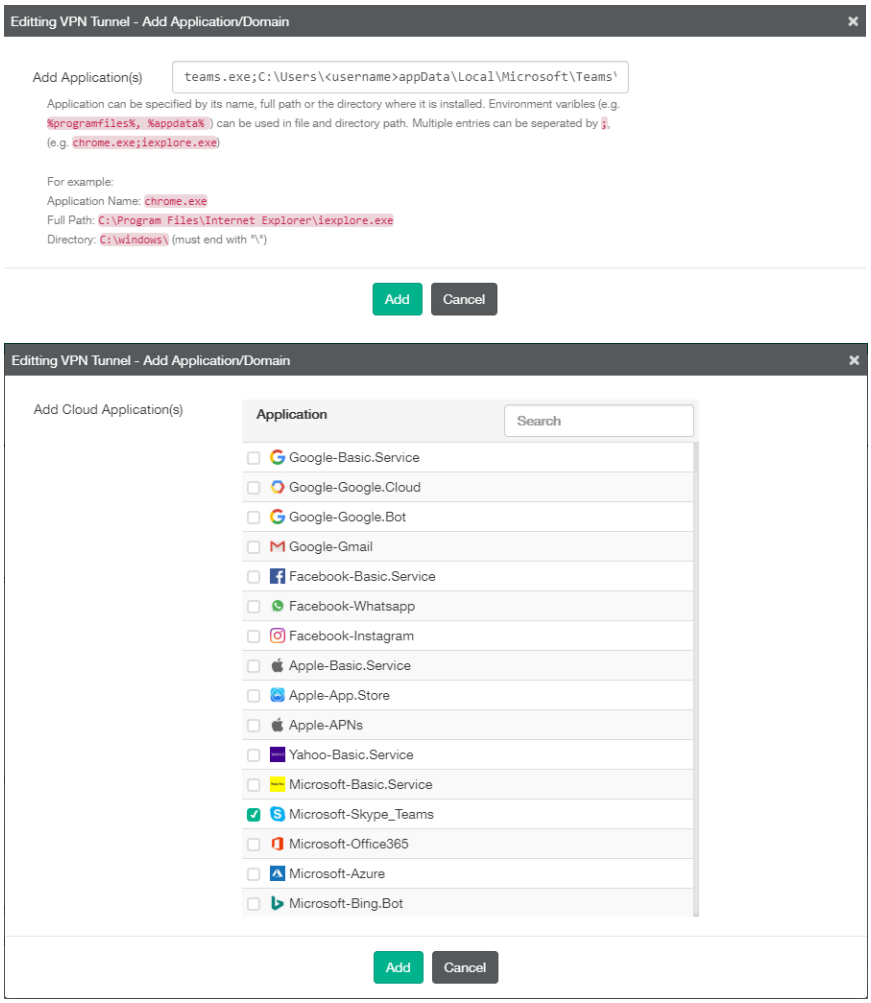
To configure application-based split tunnel using the GUI:

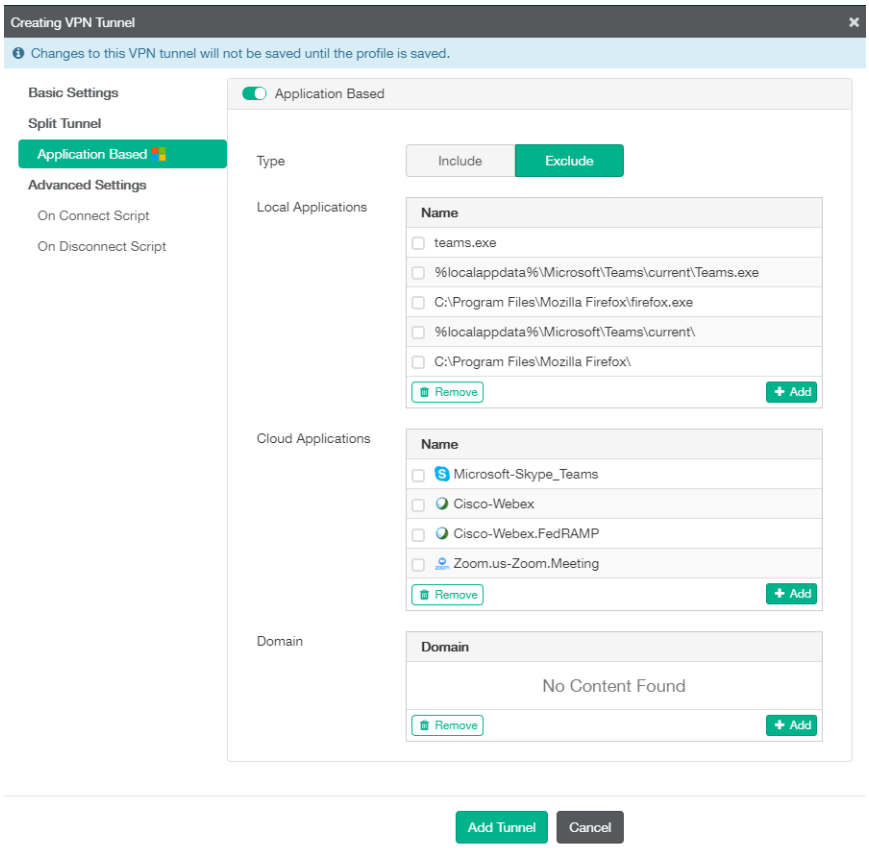
1. In EMS, go to *Endpoint Profiles*, and select the desired profile.
2. On the *VPN* tab, select an existing tunnel or create a new tunnel.
3. Under *Split Tunnel > Application Based*, configure the following fields:

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 • 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.

Configuration		Description
	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:


Editting VPN Tunnel - Add Application/Domain
Add Application(s)
teams.exe;C:\Users\<username>appData\Local\Microsoft\Teams\
Application can be specified by its name, full path or the directory where it is installed. Environment varibles (e.g. %programfiles%, %appdata%) can be used in file and directory path. Multiple entries can be seperated by ;. (e.g. chrome.exe;iexplore.exe)
For example:
Application Name: chrome.exe
Full Path: C:\Program Files\Internet Explorer\iexplore.exe
Directory: C:\windows\ (must end with "\")
Add
Cancel
Editting VPN Tunnel - Add Application/Domain
Add Cloud Application(s)
Application
Search
Google-Basic.Service
Google-Google.Cloud
Google-Google.Bot
Google-Gmail
Facebook-Basic.Service
Facebook-Whatsapp
Facebook-Instagram
Apple-Basic.Service
Apple-App.Store
Apple-APNs
Yahoo-Basic.Service
Microsoft-Basic.Service
Microsoft-Skype_Teams
Microsoft-Office365
Microsoft-Azure
Microsoft-Bing.Bot
Add
Cancel



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.

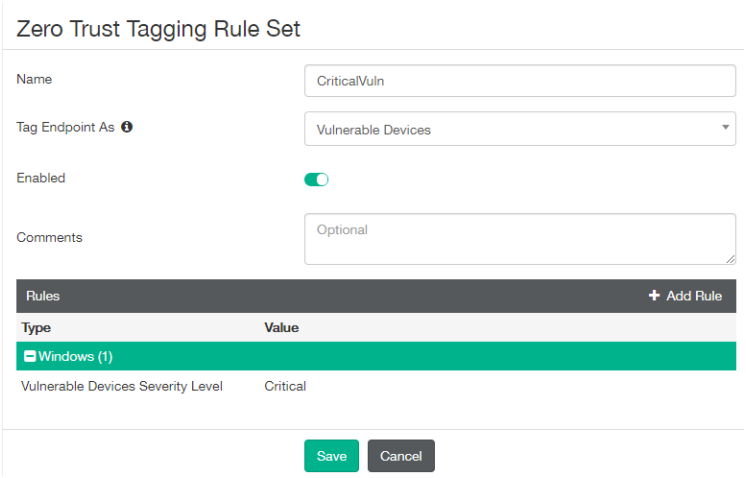
Configuring a profile to allow or block endpoint from VPN tunnel connection based on the applied security posture tag

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:

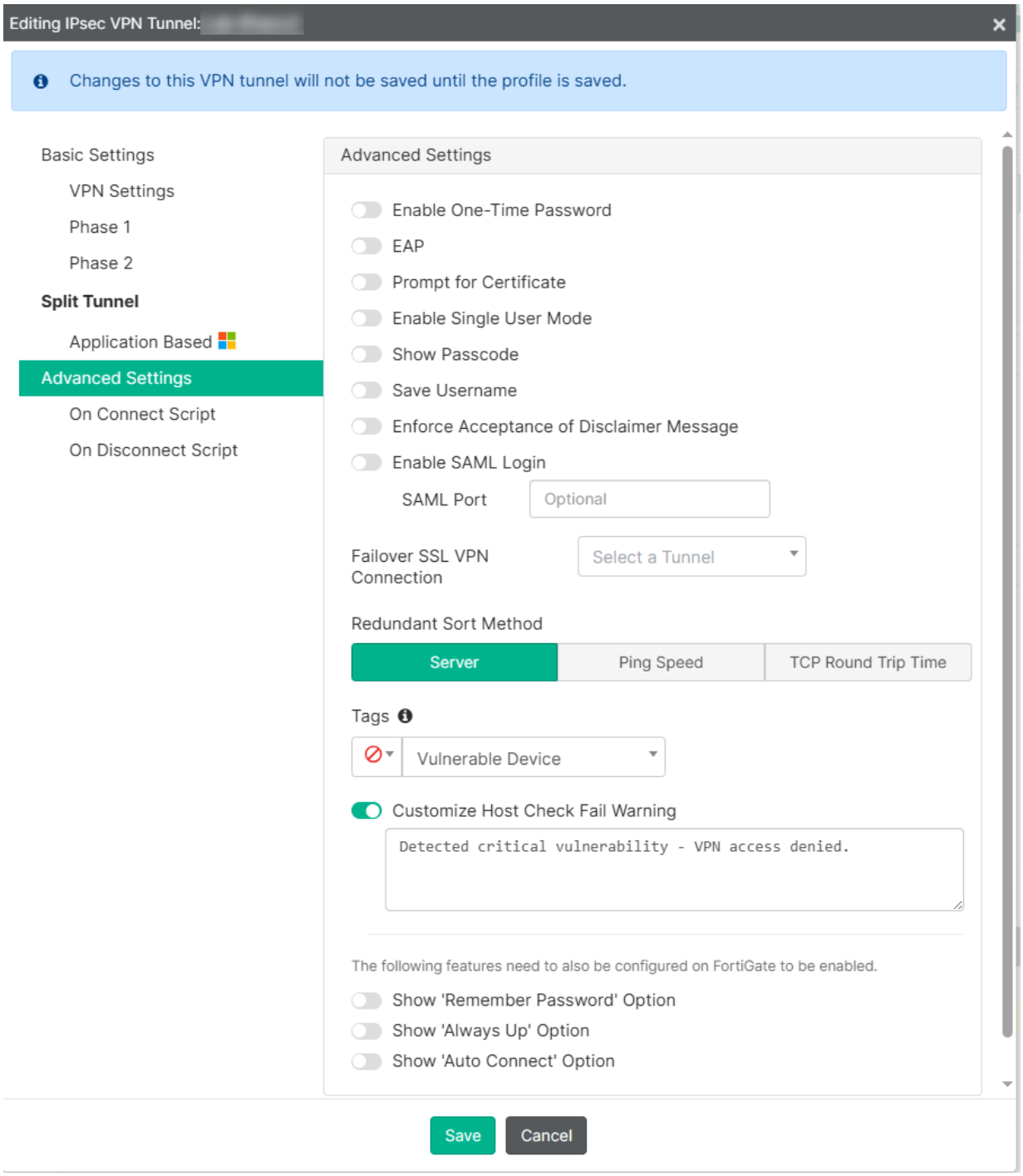
1. Create a security posture tagging rule set that tags endpoints with critical vulnerabilities with the "Vulnerable Devices" tag:
   a. Go to *Security Posture Tags* > *Security Posture Tagging Rules*.
   b. Click *Add*.
   c. In the *Tag Endpoint As* field, create a new "Vulnerable Devices" tag.
   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.

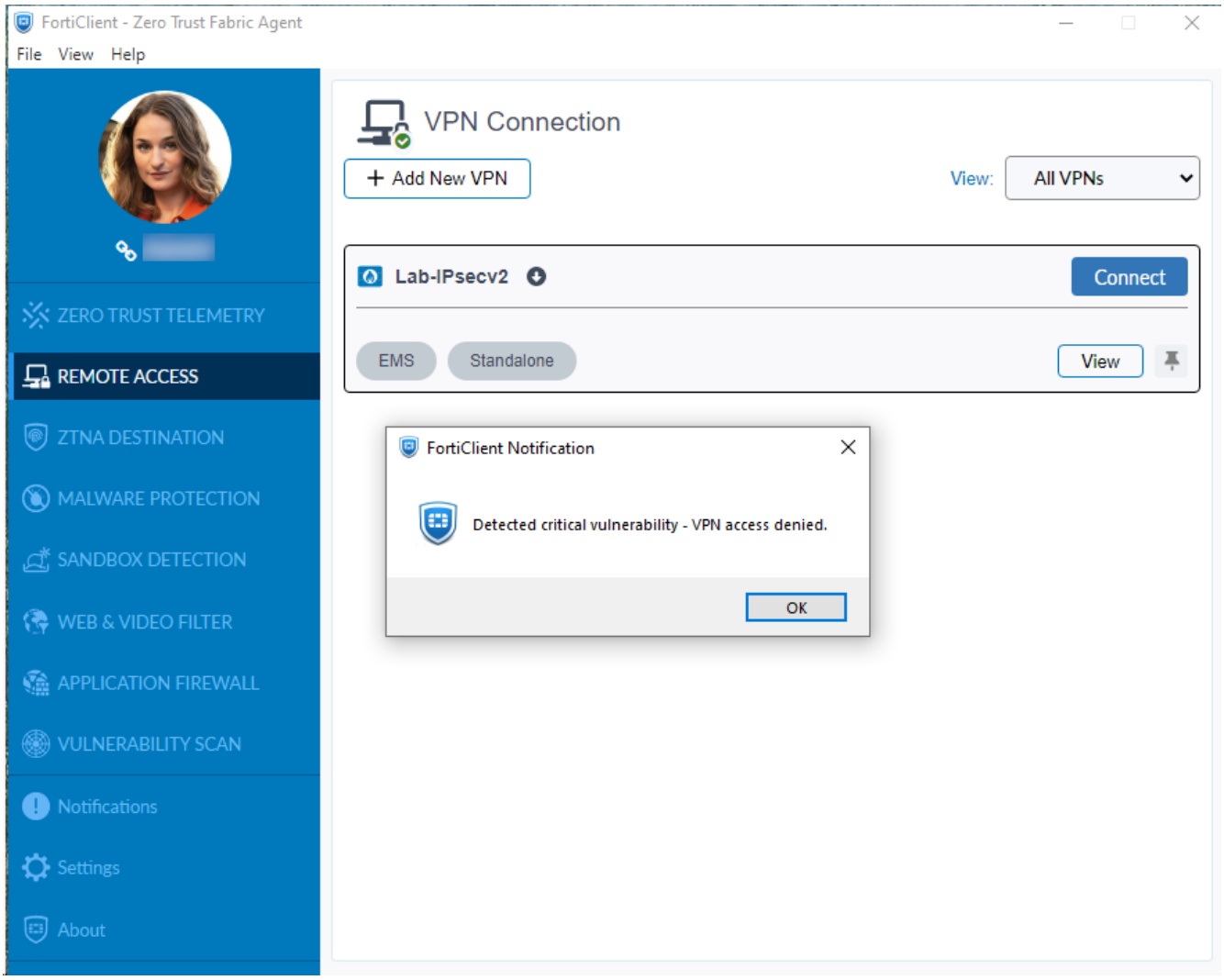


2. Configure the options on the endpoint profile:
   a. Go to *Endpoint Profiles > Remote Access*.
   b. Edit the desired profile, or create a new one.
   c. Under *General*, enable *Enable Secure Remote Access*.
   d. Select an existing VPN tunnel, or create a new one by clicking *Add Tunnel*, then *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.

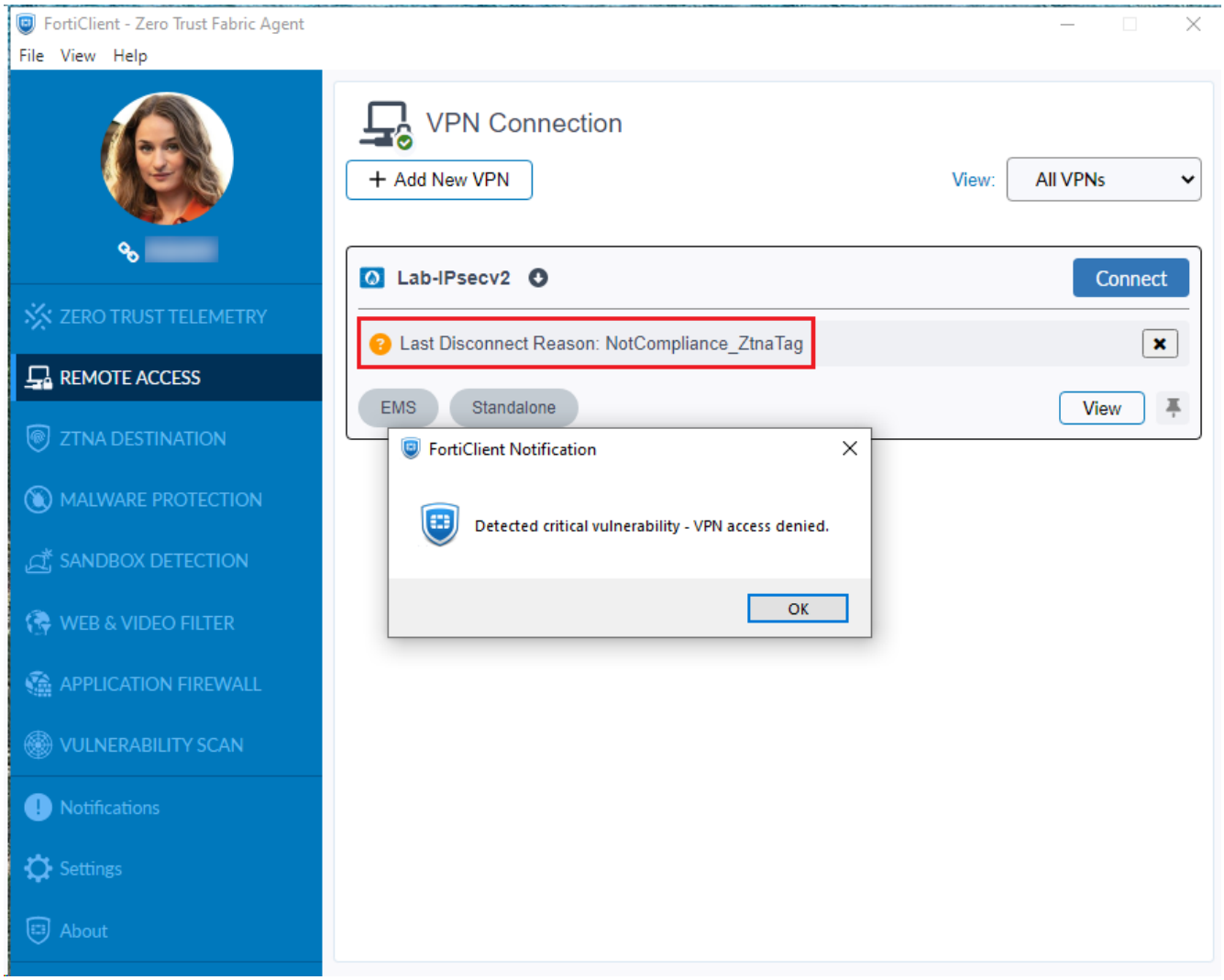
j. Save the configuration.



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.

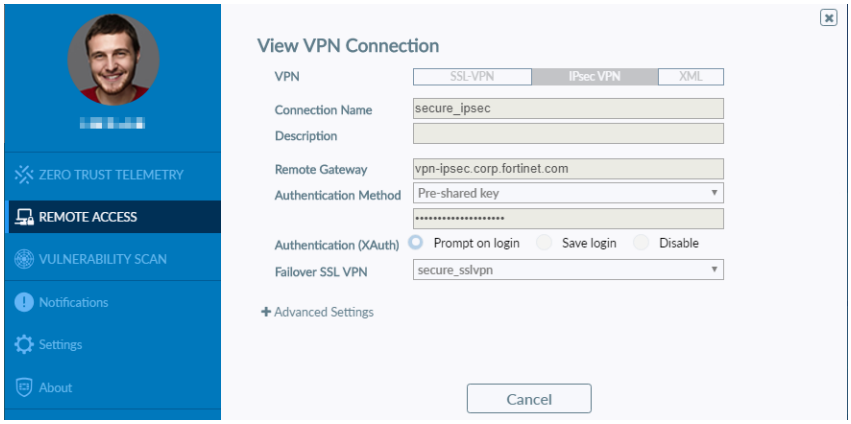
To view and configure SSL VPN settings, you must enable SSL VPN visibility in *System Settings* > *Feature Select*. See Feature Select on page 655.

To configure a backup VPN connection:

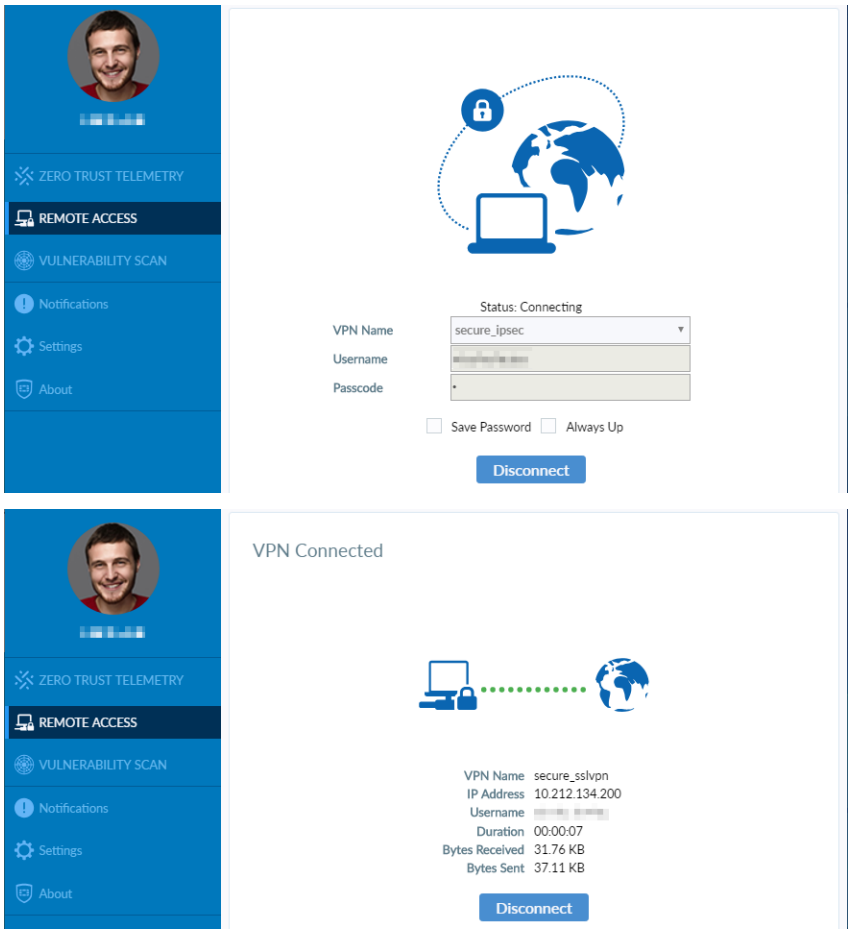
1. Go to *Endpoint Profiles* > *Manage Profiles*.
2. Edit the desired profile, then do one of the following:
   a. Configure this feature from the GUI. Do the following:
      i. Edit the desired IPsec VPN tunnel.
      ii. In *Advanced Settings*, from the *Failover SSL VPN Connection* dropdown list, 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.

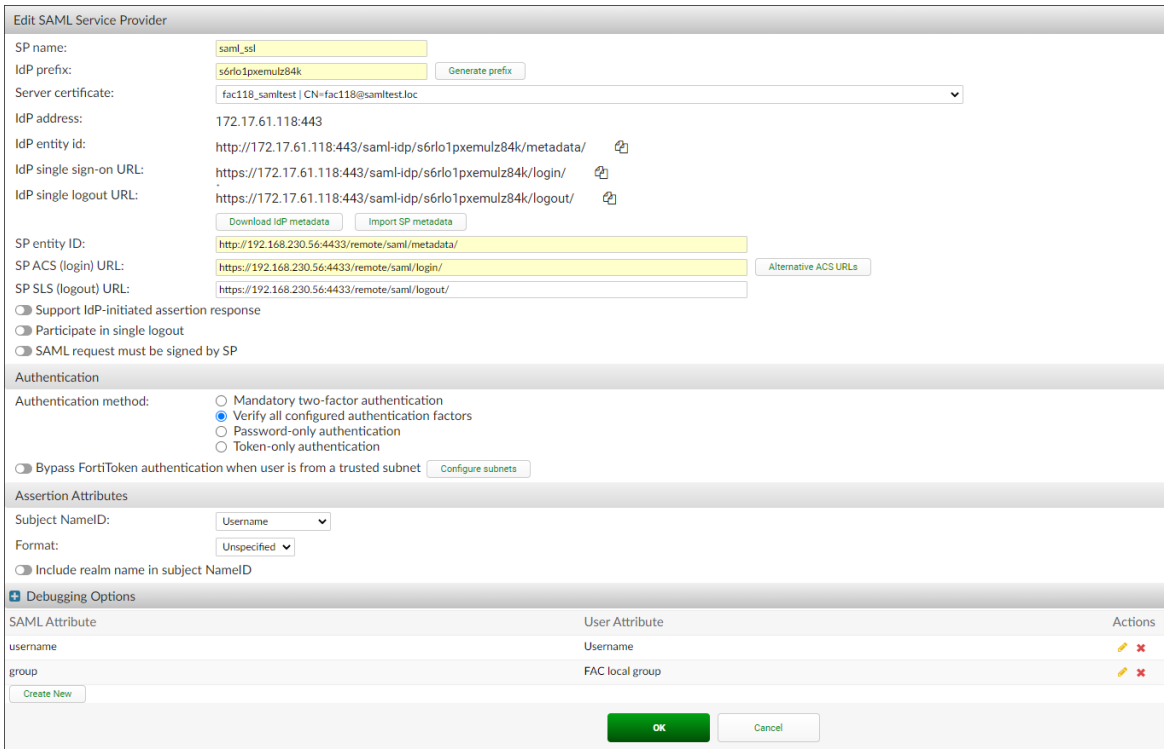
This feature is not supported when SSL VPN realms are configured. When SSL VPN realms are configured and the user provides their SAML authentication credentials in an external browser, FortiClient fails to establish the SSL VPN connection.

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:

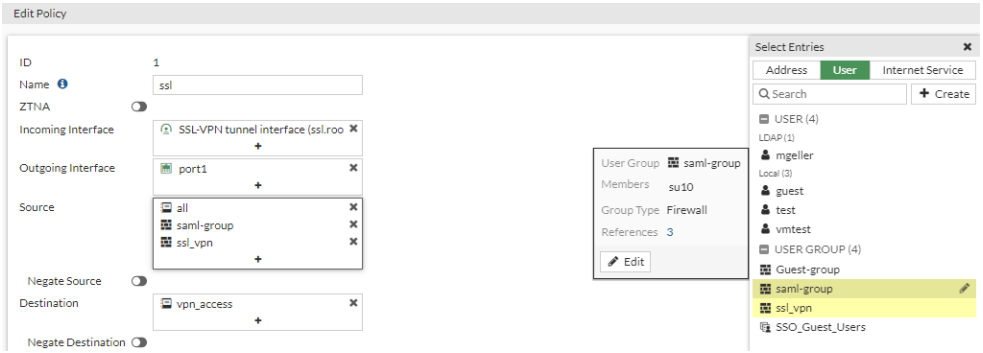
1. In the FortiOS CLI, create a SAML user. Ensure that the SP and IdP details match the details provided by FortiAuthenticator:

```
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.

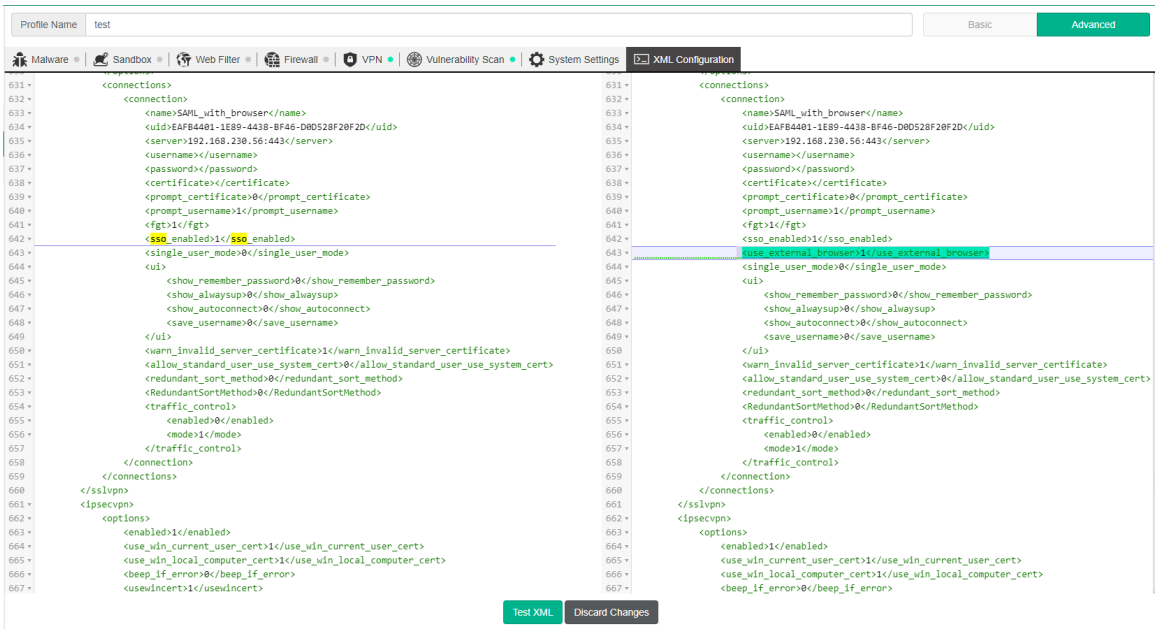


To configure external browser for authentication in EMS:



To view and configure SSL VPN settings, you must enable SSL VPN visibility in *System Settings > Feature Select*. See Feature Select on page 655.

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.	

XML tag	Description	Default value
<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 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.	1
<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.

Scenario	Behavior
	• 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. • 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 294.
- 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 295.

The following describes configuration for both methods.

The following instructions assume that you have already configured your Entra ID environment, that your FortiClient 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. See Tutorial: Azure AD SSO integration with FortiGate SSL VPN.

The following configuration requires FortiOS 7.2.1 or a later version.

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

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:

```
conf user saml
   edit "azure_saml"
      set auth-url "https://graph.microsoft.com/v1.0/me"
   next
end
```

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

To create and configure app registration in Azure:

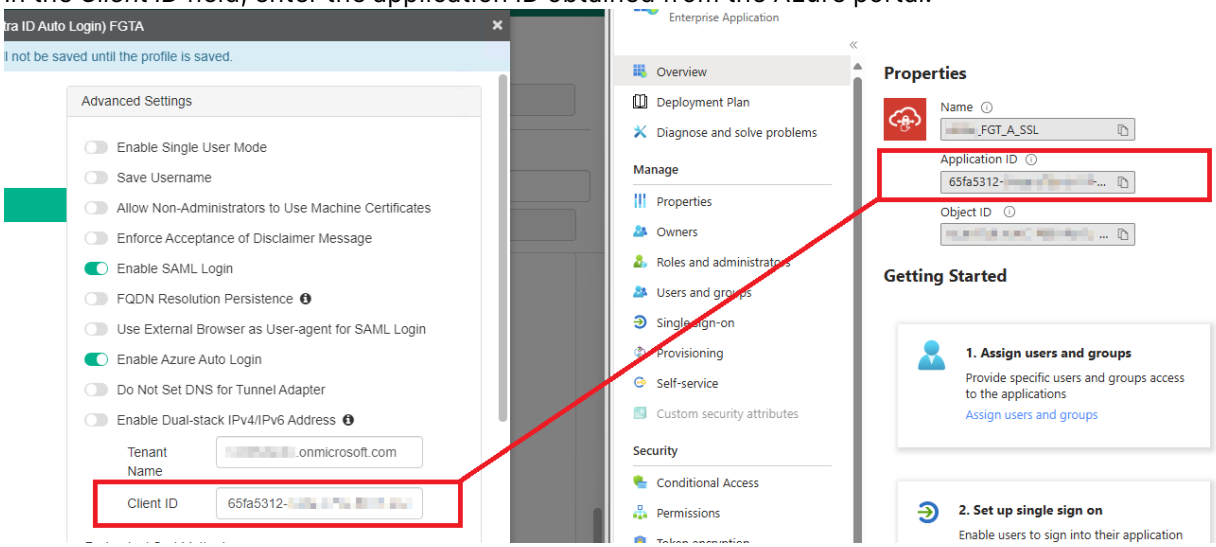
1. In the Azure portal, go to *Microsoft Entra ID > Enterprise applications*.
2. Select the FortiGate SSL VPN enterprise application.
3. Note down the application ID and Azure domain.
4. Go to *Microsoft Entra ID > App registrations > All applications*.
5. Click the application that you selected in step 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 *Enable SAML Login*.
   b. Ensure that *Use External Browser as User-agent for SAML Login* is disabled. You cannot use an eternal browser for this method.
   c. Toggle on *Enable Azure Auto Login*.
   d. In the *Tenant Name* field, enter the domain name obtained from the Azure portal.

e. 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:

```
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 "SSLVPN_SAML_Entra_ID" "msgragh"
    next
end
```

```
config user saml
   edit "azure_saml"
      set auth-url "https://graph.microsoft.com/v1.0/me"
   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>
```

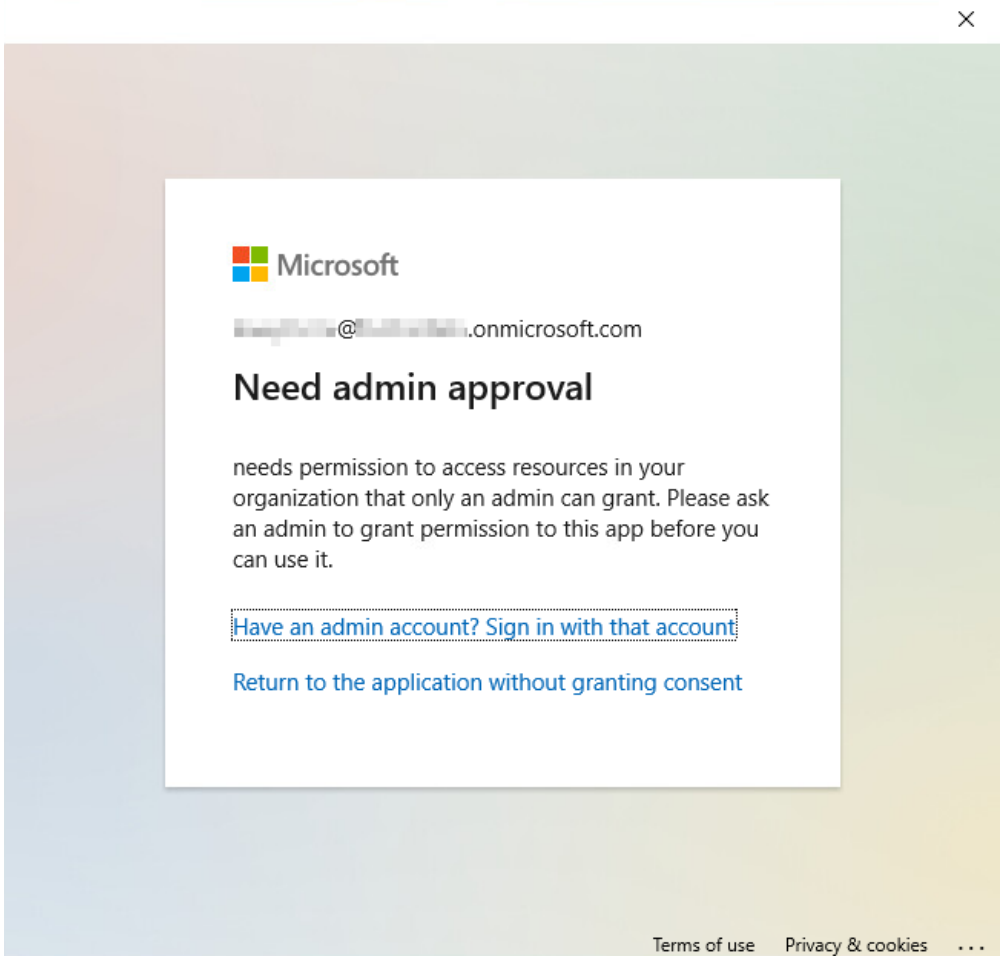
4. In general VPN settings, specify the desired tunnel as the autoconnect tunnel:

```
<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 297 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*.

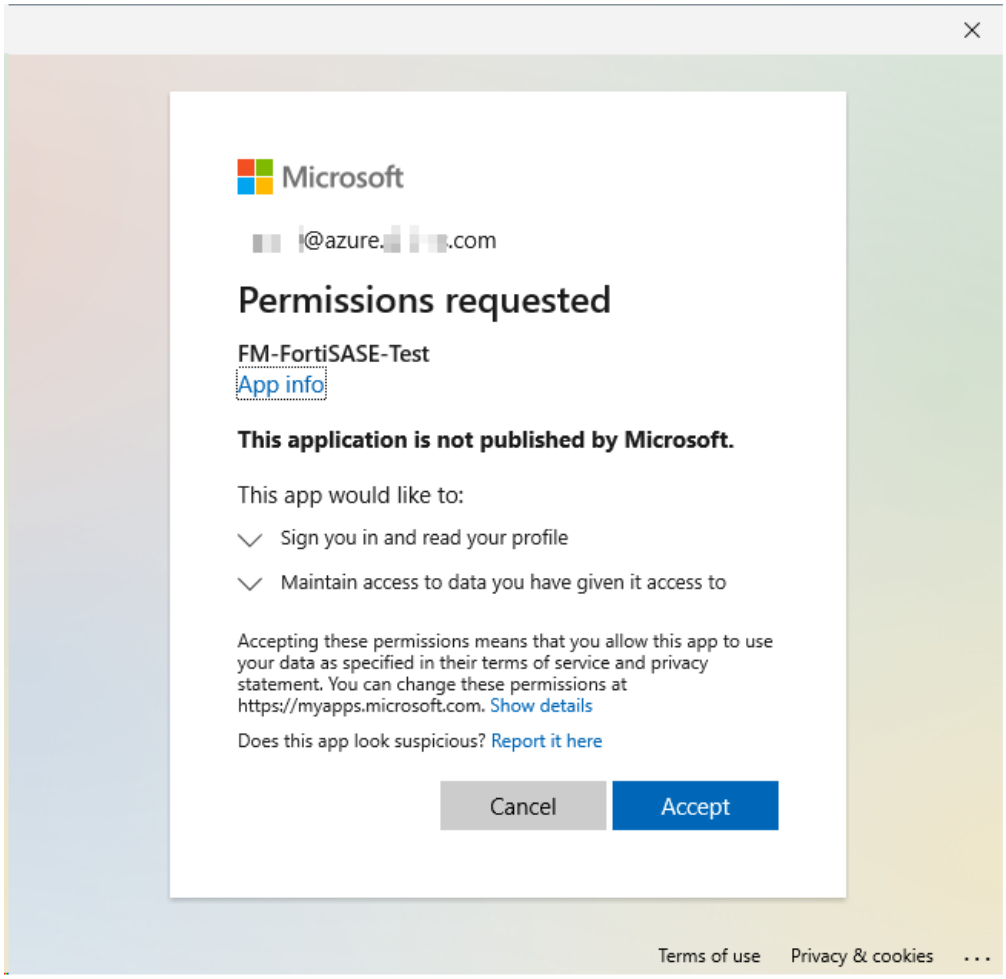
e. Go to *Home > App Registration > <Your VPN application> > (sidebar) Manage > API permissions*.
f. Right-click and remove permission.
g. If you want to disallow user consent for all applications, you can disable this by doing the following:
   i. Go to *Home > Enterprise Application > <Your VPN application> > (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:

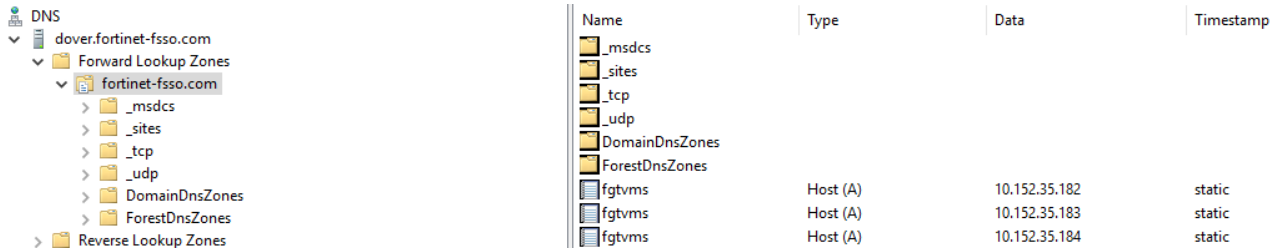
- **Three FortiGates acting as remote gateways, with the following IP addresses**:

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>
```

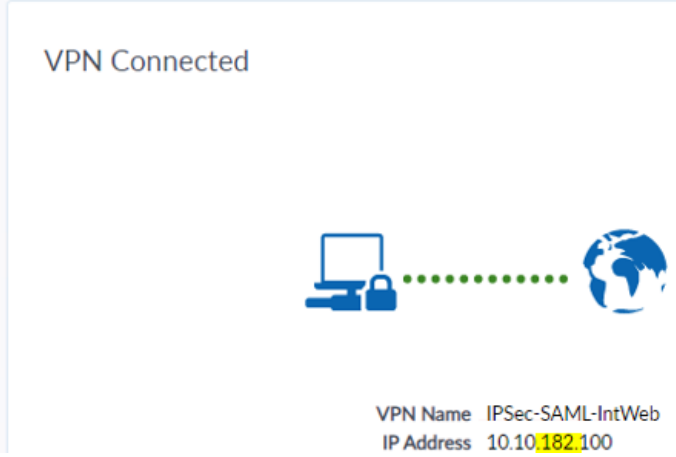
```
                        <options>
                              <use_win_current_user_cert>1</use_win_current_user_cert>
                              <enabled>1</enabled>
                              <enable_udp_checksum>0</enable_udp_checksum>
                              <usewincert>1</usewincert>
                              <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>
```

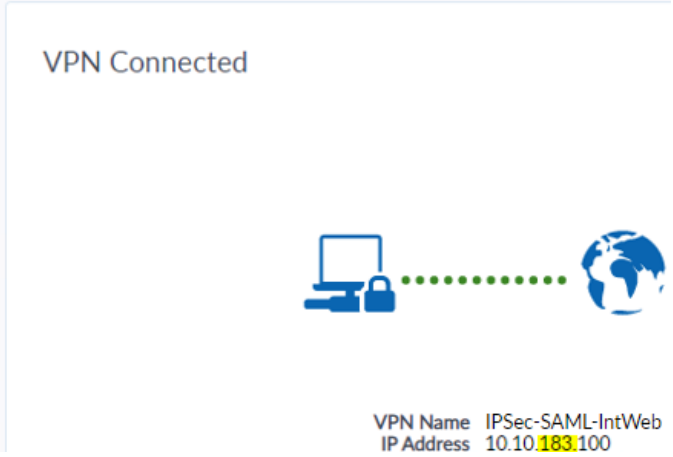
To verify the configuration using FortiClient:

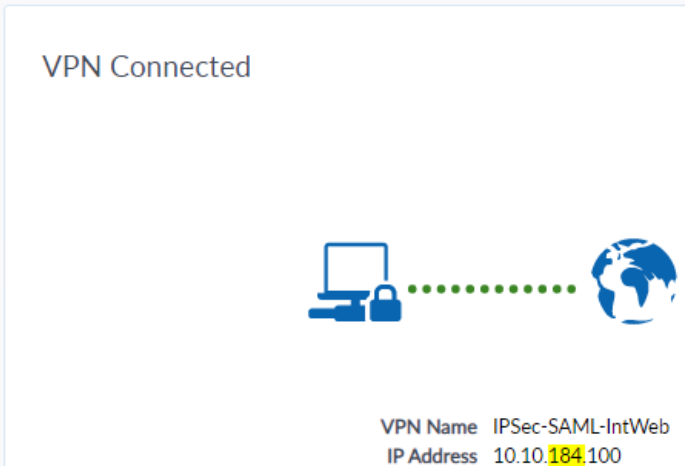
1. On three endpoints that received the profile updates, open FortiClient.
2. On the *Remote Access* tab, from the *VPN Name* dropdown list, select the configured IPsec VPN tunnel.
3. Click *Connect*.
4. FortiClient displays an authentication dialog. Enter the Entra ID credentials. If configured, you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

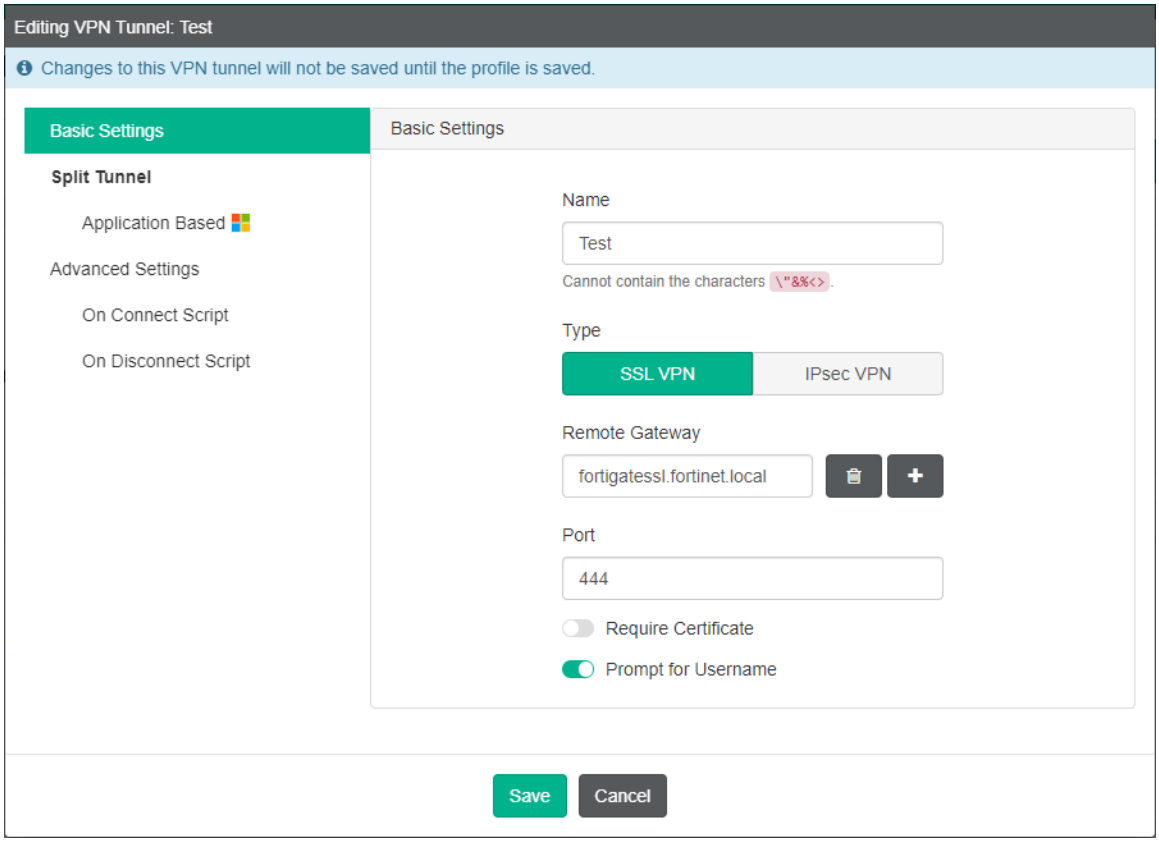
To support this feature, the DNS server must return the same IP addresss to multiple name lookup requests (sticky session).

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 655.

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. 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:

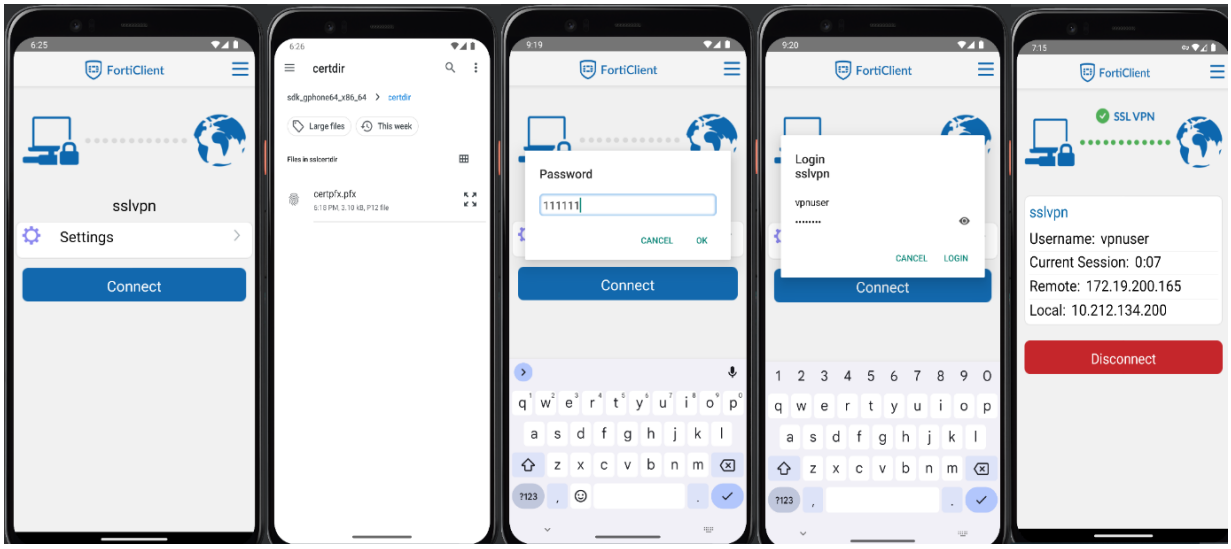
- When selecting a certificate
- When the user clicks *Connect* to connect to SSL VPN

To configure certificate path for automated certificate selection:

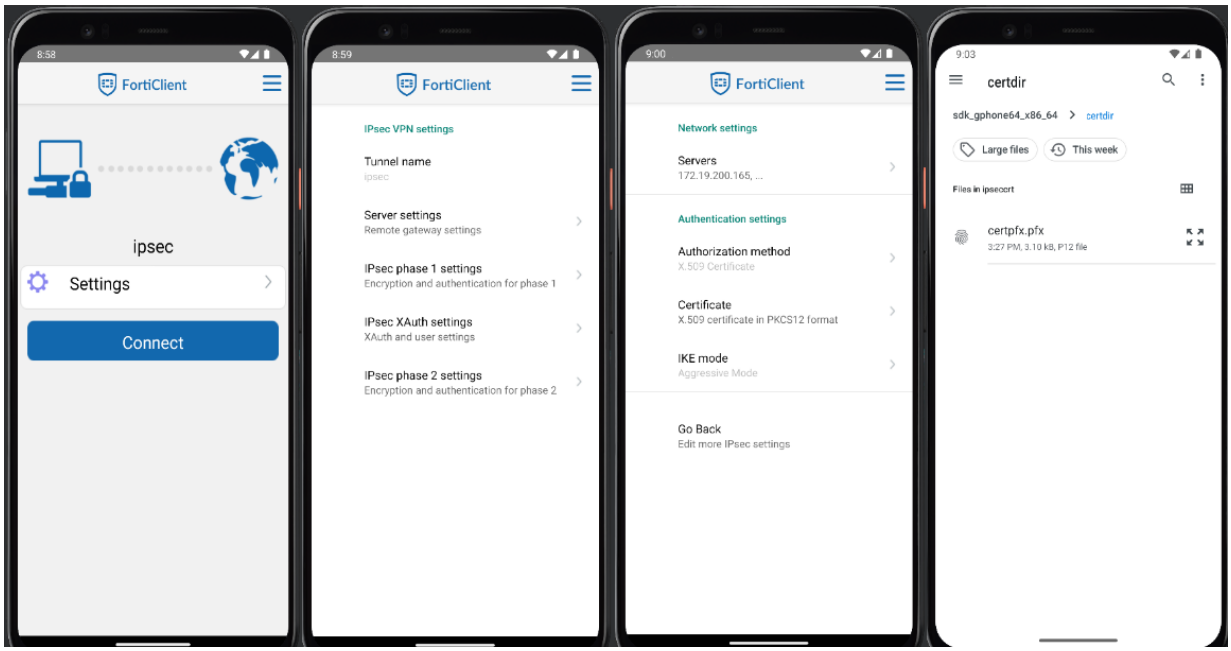
1. In EMS, go to *Endpoint Profiles* > *Remote Access*.
2. Create a new profile or edit an existing one.
3. Click *Add VPN Tunnel*.
4. Do one of the following:
   a. For an SSL VPN tunnel, enable *Require Certificate*.

   To view and configure SSL VPN settings, you must enable SSL VPN visibility in *System Settings* > *Feature Select*. See Feature Select on page 655.

   b. 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 the one of the following:
   a. For SSL VPN, connect to VPN. Clicking *Connect* automatically navigates to certdir, the configured certificate location. Clicking the certificate options in *Settings* for the VPN tunnel also goes to sslcertdir.



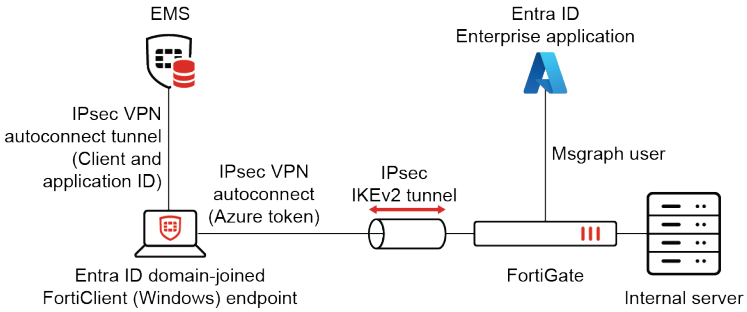
   b. For IPsec VPN, go to the tunnel, then *Settings* > *Server settings* > *Certificate*. FortiClient (Android) automatically navigates to certdir, the configured certificate location. Select the certificate, enter the password, then click *Connect*. The tunnel establishes successfully.



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>
                    <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>
                    <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>
```

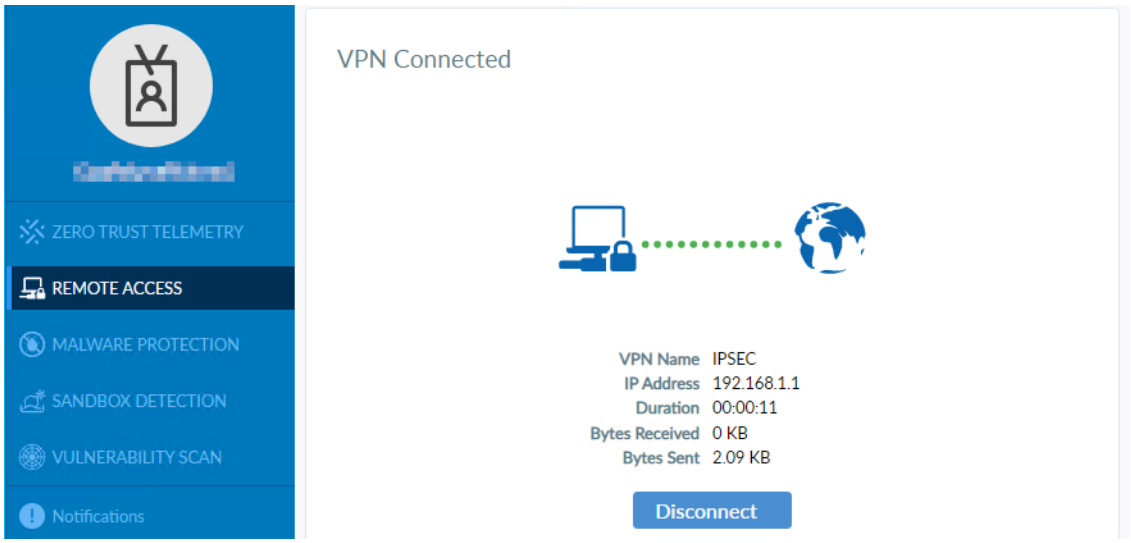
```
                        <allowed/>
                        <prohibited/>
                    </tags>
                    <host_check_fail_warning/>
                    <ike_settings>
                        <server>172.19.200.113</server>
                        <authentication_method>Preshared Key</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>
                    </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>
```

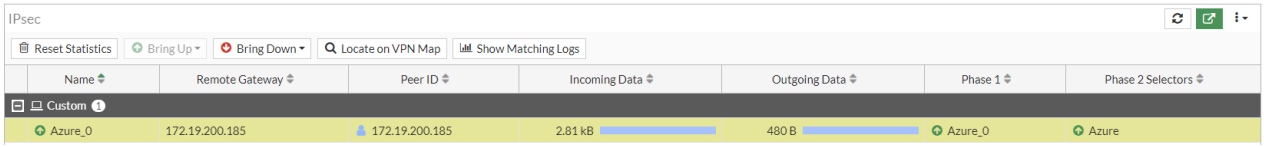
```
            <display_vpn>1</display_vpn>
        </ui>
    </endpoint_control>
</forticlient_configuration>
```

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
441774C5441774D444174597A41774D4330774D4441774D4441774D4441694C434A706

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 A70496977696
```

```
2326C6B496A6F694E4467324E4451324E6D45744F546B774F4330305A6A49324C546C6C4D7A41744F5755344D
3249344D6A49305A47526D4969776963477868644759694F69497A4969776963485670 5A434936

496A45774D444D794D4441794E445133516A45314D5463694C434A776432526664584A73496A6F69614852306
3484D364C79397762334A305957777562576C6A636D397A62325A3062323573615735 6C4C6D4E7

662533944614746755A32565159584E7A643239795A4335686333423449697769636D67694F6949774C6B4657
6130466D555756585747553462316377513078345644 6B7A6345777A5A46393354554642515546

425155464251586442515546425155464251554642515546445A45464F627934694C434A7A593341694F694A765A6D5A7
36157356C5832466A5932567A6379427663475675615751676348 4A765A6D6C735A53425663325

6794C6C4A6C595751675A573168615777694C434A7A615764756157356663335268644755694F6C7369613231
7A61534A644C434A7A645749694F694A61596D4D7964546C7955486C57636C4A4F6154464F5A31

524A65484E4352575A44566C6C4D52304A72615667795A3168324D6B354A4D325A4A4969776964475675595 73
53058334A6C5A326C76626C397A593239775A534936496B3542496977696476 4C6B496A6F694E5

751354E6A41334E3251744D6A686C5A6930304D4456694C546869597A55744D3259334E324530596D526B5A47
5A6D4969776964573570635856 6C583235686257556 94F694A6E6258567959584A7051455A7663

6E5270513278705A5735304D6A41756232357461574E7962334E765A6E5175593239744969776964584275496
A6F695A323131636D46796155424762334A3061554E736157567564444977 4C6D397562576C6A6

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 0F0E0D0C0B0A0908070605040302010F
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 89ED0540300000C0100000C800E008003000008030000020300000804000005 0
000000805000000220000 1480626D

7A23F5008349B6CC4289825B292C0000C800050000C26CB6DC83F23198EFB6B595A44AD7A2D4506D048F7E3BA
27ED14CB47FF12B2C20ED2F7C59022E698A8EEB22AC1269DE785F4E4D674261E2268E6D5219EA8

DBCD598D59CE007D831420E3654A93ED0733AA1AC51B2908611CA39D64B17ABA6E3EFC338A700480CC5CB6554
9BDA2B527FDAC9B68A4CAFBFE90ACEE70333451F31BA79FFA53B7028879E38682E2A2E74E692D6

03B41ACA394E5EAEBEDAD923ADF8DF6E5B60C19A17860A9F72079F2A9B162244DA2ED48931DA94505F8A9784C
6AE2D0000180100000007000010000 0FFFFC0A80101C0A80101000000180100000007000010000
0FFFF00000000FFFFFFFF0F0E0D0C0B0A0908070605040302010F
2023-11-28 15:52:09.561585 ike 0:Azure_0:31: out
D9AE37737FFAA01FE0E51AE3ED77F2082E2024200000000300000190210001747521BEB5752BC8166B870187B
8184577A936B1617899657B3F61B0

ACE844FACE72E945DEC6A91FC5AB1001D8120A73ED5732605FE6D0DD57CDDFD2EB624A38490841A638172E86F
AD3C27C255DF6508AE96D3C127C2FF9B479FD8007EE12B1E59227220F4A817A0BF29D9695C420F

5C0B9F5D74F910345D843AD638946098D38C7F2C5C19FD854F2BE128DD336328DBF1072308F4AAFD103AEE529
495D8D7A48233F6565104F277EFC9E8371A81A6B9EB59CA9AF66AD93332F3F767585522A750AD9

1B124CD84C903BE6A64B3D63BA3E6D212E73C744D59DED2AE2580A12EB0550AD140F7CDB7587A531291058697
2D01A39110DBF639CDF077B9B66799AA1C0F2A39C0106887F1D7E43B135B170A478A9DBF01B187

C20E21A04A953B0BDC4E71A00BCED1C0B2F95C5188F701EB0372CFF5FD0DD347BD7765540E45AB0E6419EC8EB
139099561E1A95F7C5056AB3B18E023338A23B26C32421BD7D5CB1C1308CA9EBAE191A87E50256
83811AB0C5E644
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/e0e51ae3
ed77f208:00000003
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
D9AE37737FFAA01FE0E51AE3ED77F2082E2025080000000400000050000000 34BFA2DC51F014978F5F6954626
30406B37D7311206880F4BA747BA1E786092E7F6F
34C63B6D3B48A8E6531AABAA72FE55
2023-11-28 15:52:13.240004 ike 0:Azure_0:31: dec
D9AE37737FFAA01FE0E51AE3ED77F2082E2025080000000400000020000000 04
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
D9AE37737FFAA01FE0E51AE3ED77F2082E2025200000000400000050000000 0349815B795B19825052A1CEB3BF
BDF0890035F90BFBAB8D3DC8B2D24
```

```
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 334
- Use case 2: SAML authentication with Okta as IdP on page 339
- Use case 3: SAML authentication with FortiAuthenticator as IdP on page 342

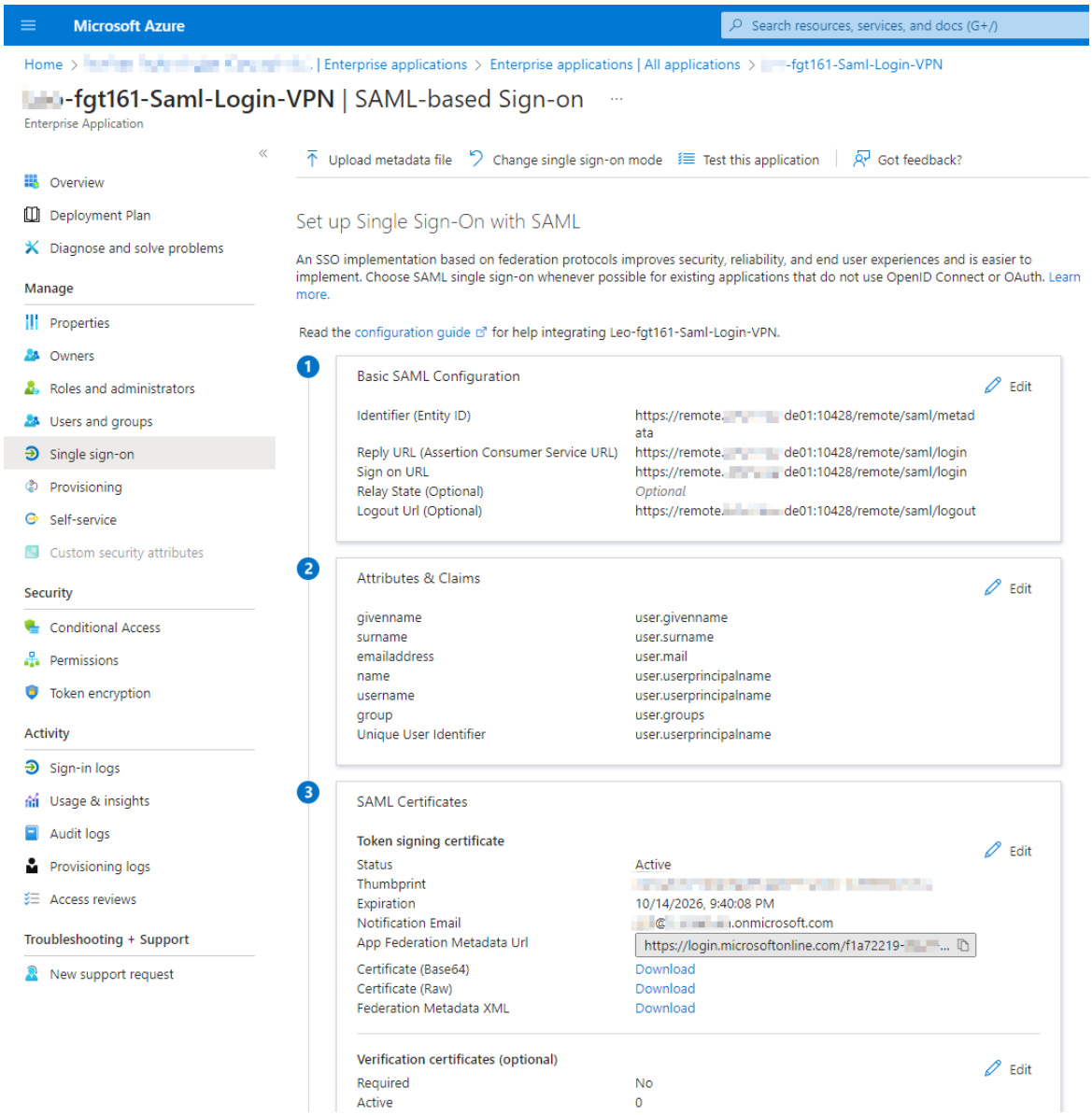
The examples use the following product versions:

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
```

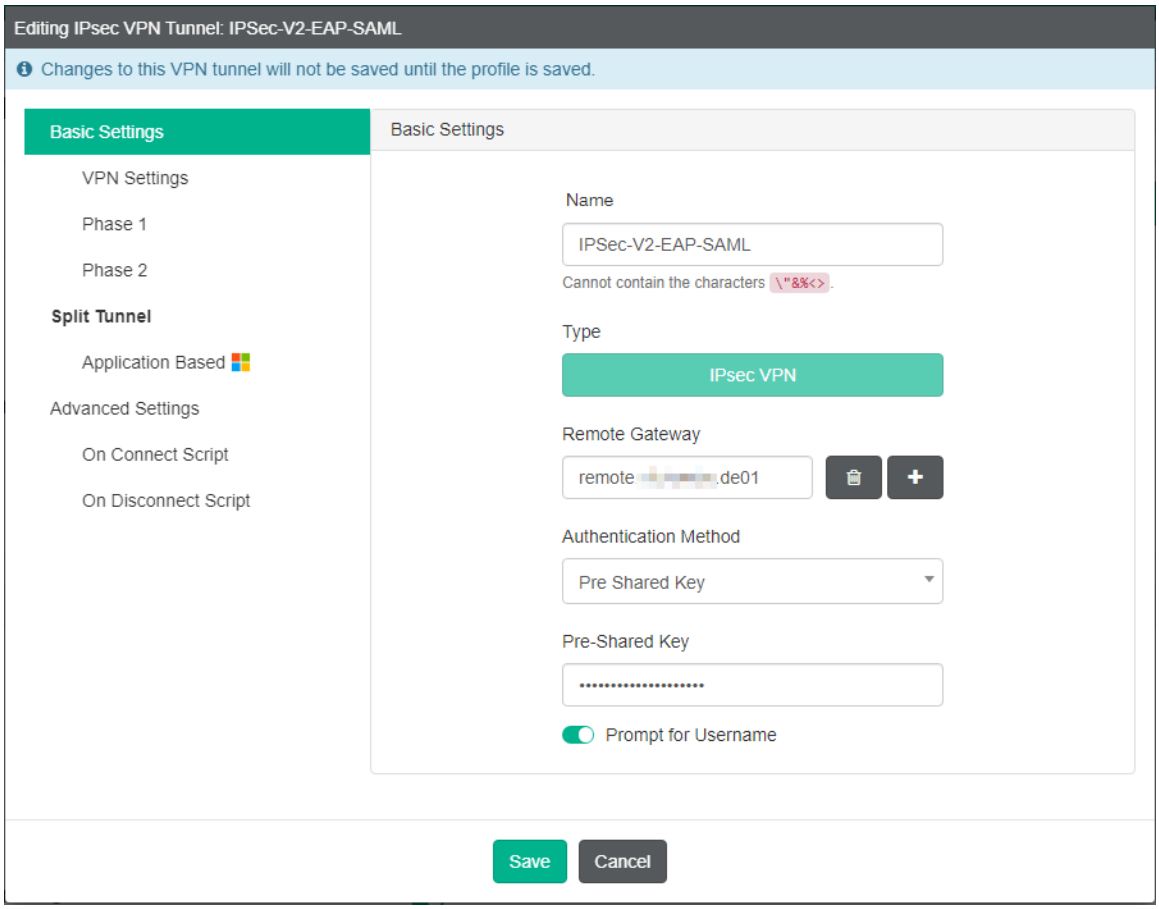
iii. Add the SAML group to the firewall policy for the VPN tunnel. In this example, ipsec-saml-group is the SAML group name, and port3 is the FortiGate LAN interface. Modify the commands to fit your environment:

```
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
```

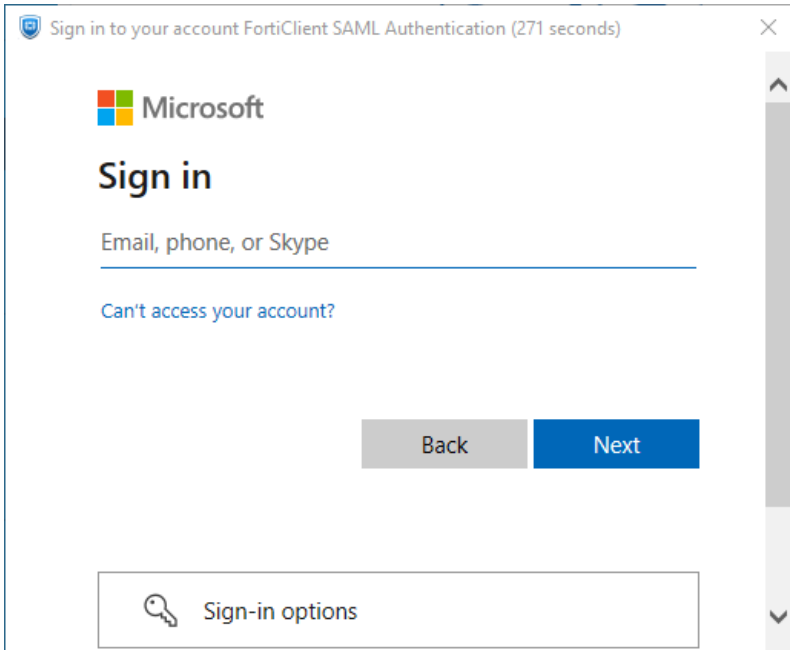
3. Configure a new IPsec VPN IKEv2 tunnel in EMS:
   a. In EMS, go to *Endpoint Profiles* > *Remote Access*.
   b. Create a new profile or edit an existing one.
   c. Under *VPN Tunnels*, click *Add Tunnel*.
   d. Select *Manual*.
   e. Configure *Basic Settings*:
      i. In the *Name* field, configure 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 342.

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 ------
```

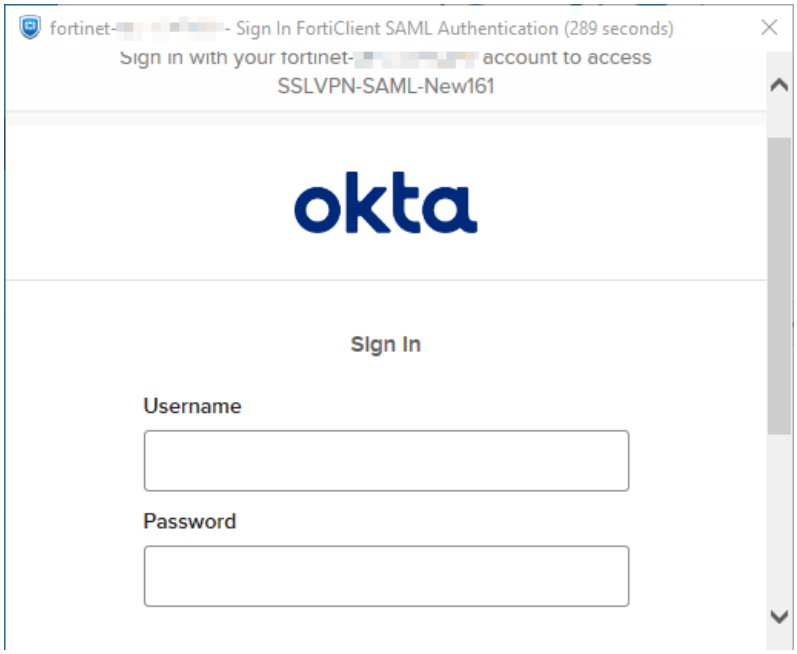
To view IKE debug log output for this access, see IKE debug log reference on page 348.

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 334. 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 334. 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 334 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
91D7E3BFD6EB8287032B6561653DE26721202220000000000000001602200003000000002C010100040300000C01000
00C800E008003000008020000020300000803000002

000000080400000528000C80005000065955E1E4681E843C5618C637FE43851C15AD4D34C8E1738B09188C6B3DA5
7CFFC88346E35095286C904E5751B1722F8FA0455F59AE7489A67180C2A36D65DAC6FA

FA4B9DADCE79F8B35851C2A22B8F452110665B6D16342709F5979D43F95CCE0617C40786355FF35D5E45864656435
6ED08A1A1CF29EA7C046246F09EFD49D3574DCC9D980EAFB1D08685642169ECB1E7081

9DB02E208F0C130FA97F071ADBD53F16E79384BA05CB0B8B18C6A0D125834119877FE45C11E7CDC77FFFA63B87290
000014473843BD329EC550DD27667C37BFDA7A2900001C00004004B752F27710DE7BFDF
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
```

```
91D7E3BFD6EB8287032B6561653DE2672E2023080000000010000026C230002508DC5174C77E069C310D8A8382293B
7125A27239C47932A34F2C27458FC9774DC6FB3E3E179F8777D69A7E54EE

CDC0F4291E3B33E953B0761FC06B39882FA1EC00FFCB4CEB559AAD7272918C485A2A125CCD4B35B34CE7244BDD04B
5183E43AFF419452A1AE12917BDF31AB2D758983B60ED97A2183EE38A98BCD8FEFA0CD

4DF478699267107DC508EFF092359589355084DAEC722EBF52DD7699B409295987A6648989CF760D2FD44F2EB83B2
F897D2653D52FB5A073BAD3687CE0913A55CD36C6D481F362F5133CEBA3D623C64F360

4F2D7187A5130A479A7029EE4291F9A9E54AC3338AC79B151F97CE9900B50FC3C986F348FABDC430B5A5357477AA0
B58F4E29C08904A43DDA6938BCE9520D0CE4193B904CED247770B70F62A0BFE41C4396

DB9386B505910AE947DFDC37E8D75C6F71E202CF163EB4B90C5E68FF5F9817D7255EA3C3AB8C8DDAE99B04D619BC1
E56CD282EAE3873316290E349578360AC5F8136C69A7C2ABD0E4F2F419AE710899F1AD

6AE8A3A50EDC29574AC4D9F3ED065D6504344E2FA553E620F7D488D19FC4232556CC35EF4A84BE3A865E31AB4C169
F0280975271DEDFCD43E53B1E60D75DFACC56801D09E0AE14B3D39161963AB92402263

65F39E975EF85E988A3BD1D2419E2CA7C0A1B354CF920DC0B453B5FCBED5CC48F5617C15869185F0501380F2687B3
0709328485EE6520AFCB174F49B2292FFAE97F11474672E1AE754A5132CCFB5A0DBEC4

AD9BCF9DEEE1EC905E464F83A8448CEA16FFE33938A96485B283A40732CA6B25AF0870A974239DA5ED7CD8362308A
4C438FC7DC4512E4
ike 0:v4-PSK-IKEv2:14: dec
91D7E3BFD6EB8287032B6561653DE2672E202308000000010000024423000004290000C010000000A9823AA29000
008000040002F0001380000F1005645523D310A4643

545645523D372E322E342E303937320A5549443D45363946374145304438343434344634411314146384446303942 4
445383539330A49503D31302E3135322E33352E3137300A4D41433D30302D31352D356

42D32332D61382D30313B0A484F53543D4445534B544F502D5550494E42524A0A555345523D453639463741453044
3834343434463441314146384446303942444538353933 0A4F535645523D4D6963726F

736F66742057696E646F777320313020456E74657270726973652045646974696F6E2C2036342D626974202862756
96C64203139303435290A5245475F5354415455533D300A454D53534E3D464354454D5

331303433353735353320A454D5349443D303030303030303030303030303030303030303030303030303030303030
3030300A00210000540100000000070010464354383030313434383131303439300001

00000002000000030000000400000000D0000001900000008000000F0000000A0000000B000070010000540A00005
40B0000700000002C000054020000280103040 3E03A386C0300000C0100000C800E008

00300000803000002000000080500000000000028020304 03E03A386C0300000C0100000C800E0100030000080300
000C000000080500000002D000018010000000700001000 00FFFF00000000FFFFFFFF00
000018010000000700001000 00FFFF00000000FFFFFFFF
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
005010E0D0C0B0A09080706050403020 10E
ike 0:v4-PSK-IKEv2:14: out
91D7E3BFD6EB8287032B6561653DE2672E2023200000000010000007C240000601997569 6D3E610D0A55FCE2141CE0
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
91D7E3BFD6EB8287032B6561653DE2672E202308000000020000004930000004000000029028C00250145363946374
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
91D7E3BFD6EB8287032B6561653DE2672E2023080000000030000007F300000040000005F028D005B1A028D005631C
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
0000003C018E00381A038D0033533D433037373736363541423444333736423632393936343636424544383530363
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
```

```
91D7E3BFD6EB8287032B6561653DE2672E2023080000000040000002A300000040000000A028E00061A03
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
91D7E3BFD6EB8287032B6561653DE2672E202320000000040000004C300000309A60CF863B708309D8C1418333CF2
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
91D7E3BFD6EB8287032B6561653DE2672E2023080000000050000005C270000409F291281AD48EC4CD1DFEF5961D33
BE185A04F1810661E66FBC1F5846796CD0A535C063D19A0E930A51130F3D
9413512EF92EC71E582D10991B7FE42
ike 0:v4-PSK-IKEv2:14: dec
91D7E3BFD6EB8287032B6561653DE2672E2023080000000050000003C270000040000001C0200000063A2A164BD0FE
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
758626B20300000C0100000C800E008003000008030000020000000805000000 2D0000
```

```
1801000000070000100000FFFFC0A80164C0A80164000000180100000007000010000FFFF00000000FFFFFFFF0C0
B0A09080706050403020 10C
ike 0:v4-PSK-IKEv2_0:14: out
91D7E3BFD6EB8287032B6561653DE2672E2023200000000050000015C24000140F73C9BCD7A9F971B02F6A48AE9B37
644762FCA3FB4E3D0E2136A72A1BBC4113F7A87F3

9A611CBE1B0E5036D73020A46B6455BEE66FFC5F95E237337C4CFF0A4CCA52BB18DC3A17F497E12FDDE5D8A6953B4
295109F0BEDBA72459E3750D6924159BE555D8011EF5B9C0EA1EA91BFA6F0E850A7296

B813DE95FF47F40545584CCC00264377258E6C3769A64834AE9161B286DD9067B689E53EC59C6C3E28BE798401730
A6E01CC23756A75142244140C1EA6FE3D771F24E768D2E092888F08E3BFC3CE5486819

1B5BFB6CE6E97764CF75B6AE068B5C7398EF72C0E963FC15EDAD00A166AFECCFE35EB6314C7FD27C2C5F718777FE7
3ADBB8472255BB4FDDD9CE39E39743258 5200246F891A68A86CEE05748502CC58770BB
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
91D7E3BFD6EB8287032B6561653DE2672E202508000000060000004C000000308313D182BDFE6429ACF9CD754A0CA
A19E6997AD0F915E69445D9C1256C6CBF7694582330F8AED0C6F892FD1D
ike 0:v4-PSK-IKEv2_0:14: dec 91D7E3BFD6EB8287032B6561653DE2672E202508000000060000002000000004
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
91D7E3BFD6EB8287032B6561653DE2672E202520000000060000004C00000030E74A78C1B6607A4209955C934EBD0
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
91D7E3BFD6EB8287032B6561653DE2672E202508000000070000004C00000030B7731C94B7CD08C9325F550EC0EAB
E733FC5DA5E50A1440AE3FE358726D1DE7EFE61CC3D02674FE0155CE28F
ike 0:v4-PSK-IKEv2_0:14: dec 91D7E3BFD6EB8287032B6561653DE2672E202508000000070000002000000004
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
91D7E3BFD6EB8287032B6561653DE2672E202520000000070000004C0000003042E9544F9024C5ED6F72E90A613C9
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
```

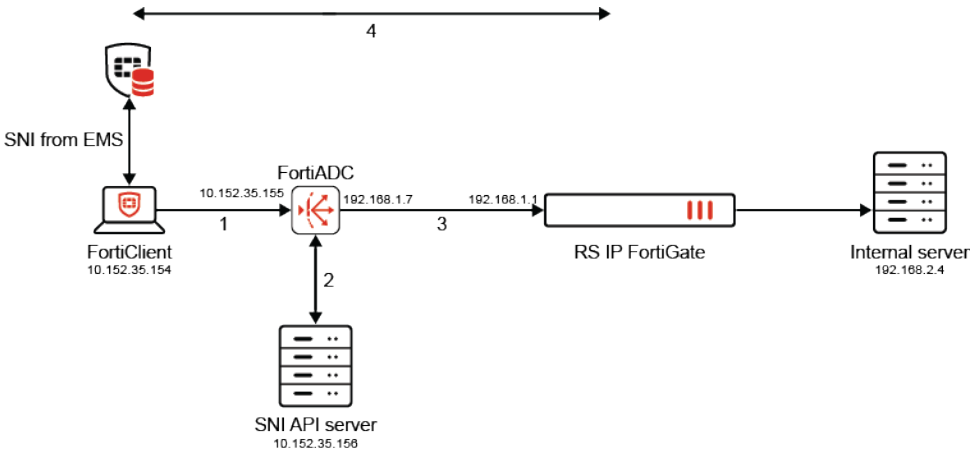
IPsec VPN support for traffic going through FortiADC

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:

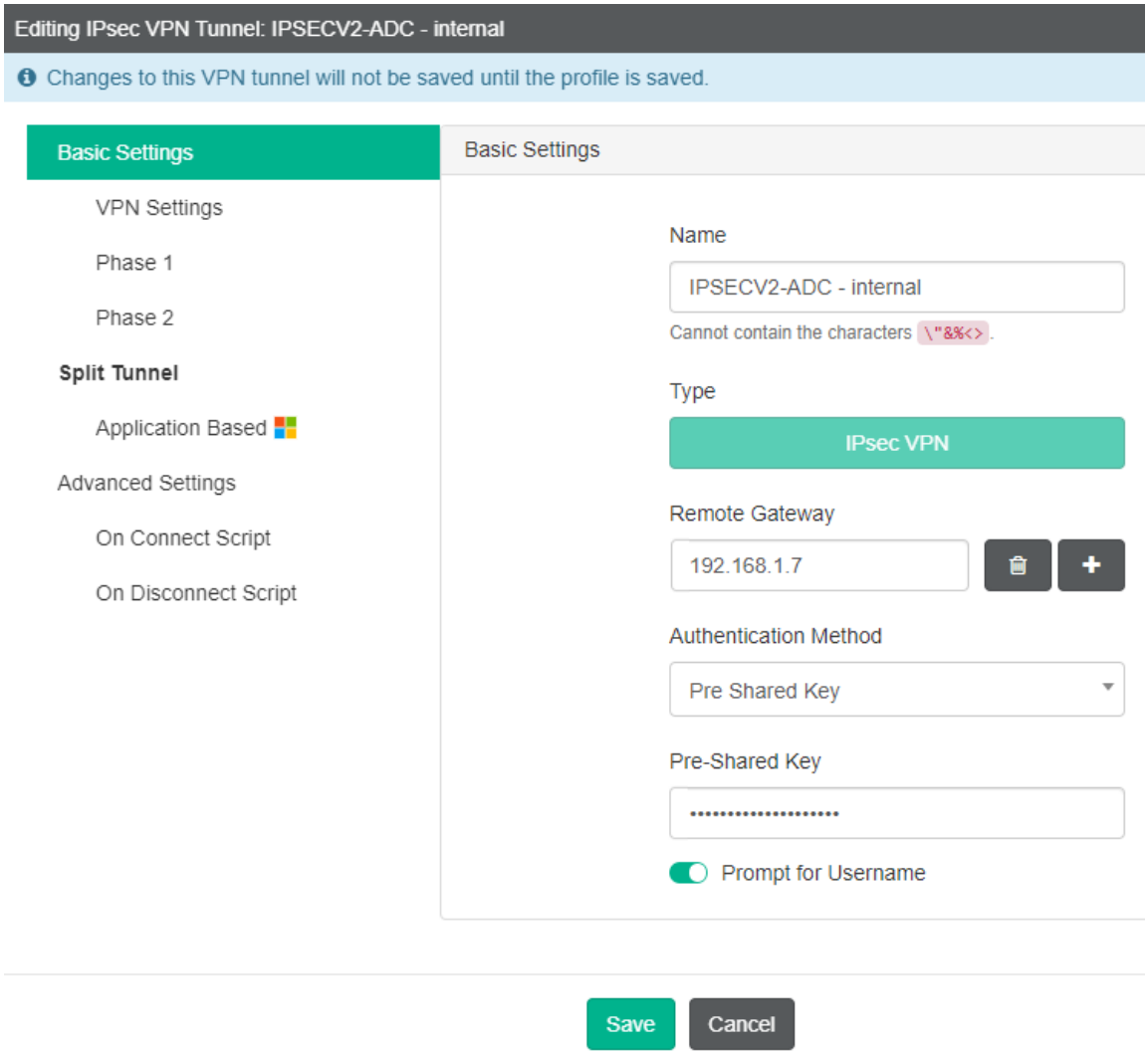
```
config load-balance virtual-server
  edit "INTERNALIPSEC"
    set interface port1
    set ip 192.168.1.7
    set port 4500
    set load-balance-profile IKERESOURCE
    set load-balance-method LB_METHOD_SNIPROXY
    set load-balance-pool FGT-POOL
    set traffic-log enable
    set traffic-group default
    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
FD23616068EA787B0000000000000000212022080000000000000001F82200005C0200002C0101000403000000C010000
0C800E008003000008020000020300000803000002000000080400000500000002C020100040300000C0100000C800E
008003000008020000050300000803000000C000000080400000052800000C80005000002985CB0E49090C90FF1B01C95
C5CBE283C13C57C98C796D1AB5301AB30E5D5BD3C3B438A41F95CFDD8C2FC1086DCD18F6B3A6EAAF8AF9E54022F8FA
0B4FC16BAAF42AA3F4DDB5CC2846F09CD0CDA74B513851EAB6F9A8EAB128B0DB8D5B4F819EA4C775B037A77BD35813
230C0708077C34EB02BD3F8A71613B84365F5FCE93528C2C54FF72ADA276E7C4B37DF6C6A9AAAE2CA0370957B43853
45ED403118D6A0D68A49834069CC7543F0597AD83FA75FE90967A40A31F3F8CE28ABFBDE25822B000014BDDC4BD20A
F71BA16FFE6AA24508B0162B0000144C53427B6D465D1B337BB755A37A7FEF2B000014B4F01CA951E9DA8D0BAFBBD3
4AD3044E29000014C1DC4350476B98A429B91781914CA43E290000180100F103464354454D53383832343039303331
3529000018010 0F103464354454D5338383234303930333135290000 1C0000400408C1FCB91852BE008BC80B00D5AD
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
FD23616068EA787B8A56F0004EEC7C3D21202220000000000000016022000030000000 2C020100040300000C010000
0C800E0080030000080200000503000008030000 0C0000008040000052800 00C80005000000AE7B893BC5E3A52AA6
63A0334F31B4E900C9F5635E5CE2817A0FD7734EA390EEDF0898E22540B9AE00E8C4E1DECB51DA24B0A7C326FF6286
ADF943020E4027FF73A6E4752FEA8B133EBAB7553723BDC61E43FBC99C2D95FA88BC5BF8E322B7598FAB4F5C55A13B
2226D71DF952B088256A57D88E16C671881DDD028AC24D9E4ACA40DC26017C87C0553EDDE75D031FCFC0DBB74B4F26
E9EE0AC662A66FAD4E48A3D2232E0BDB7552E3855535D340BF34B28873D28C8FABB2FCAC5194A5373E29000014DE64
99159A9592FF9CF6A3386978107829000 01C0000400412CB23AF2CCA5494532E14CE0775D4D1CFA05EA40000001C00
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
FD23616068EA787B8A56F0004EEC7C3D2E2023080000000100000023A2300000 42900000C01000000C0A8010B290000
08000040002F00012E0000F1005645523D310A4643545645523D372E322E342E303937320A5549443D393546303735
303343423732344245303833323038463937454542394346383 20A49503D3139322E3136382E312E31310A4D41433D
30302D31352D35642D32332D61382D34613B30302D31352D35642D32332D61382D35613B0A484F53543D4445534B54
4F502D493134495656430A555345523D69707365630A4F535645523D4D6963726F736F66742057696E646F77732031
3020456E7465727072697365204564697469 6F6E2C2036342D6269742028627569 6C6420139303435290A5245475F
5354415455533D300A454D53534E3D464354454D533838323430393033331350A454D5349443D303030303030303030
303030303030303030303030303030303030303030303030300A00210000540100000000070010464354383030313637
383932393934000100000002000000030000000400000 0D00000019000000080000000F0000000A0000000B000070
010000540A0000540B0000700000002C00005402000028010304038DE23FFD0300000C0100000C800E008003000008
030000020000000805000000000000028020304038DE23FFD0300000C0100000C800E008003000008300000C000000
08050000002D000018010000000700001000 00FFFF00000000FFFFFFFF000000180100000007000010000 0FFFF0000
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.
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 IKEv2 with SAML authentication

This document focuses on multiple scenarios of IPsec VPN IKEv2 with SAML authentication failures. This document provides details regarding FortiGate diagnostics and FortiClient log highlights.

When troubleshooting IPsec VPN IKEv2 SAML authentication failures, use the following logs for troubleshooting:

- FortiClient diagnostics
- FortiGate CLI diagnostics

- FortiGate system events (VPN events)

The following provides the FortiOS commands to enable debugging to view the aforementioned logs for troubleshooting:

```
diagnose debug reset
diagnose debug console timestamp enable
diagnose debug app ike -1
diagnose debug app fnbamd -1
diagnose debug enable
```

You can also complete the diagnostics with the following commands, depending on your use case:

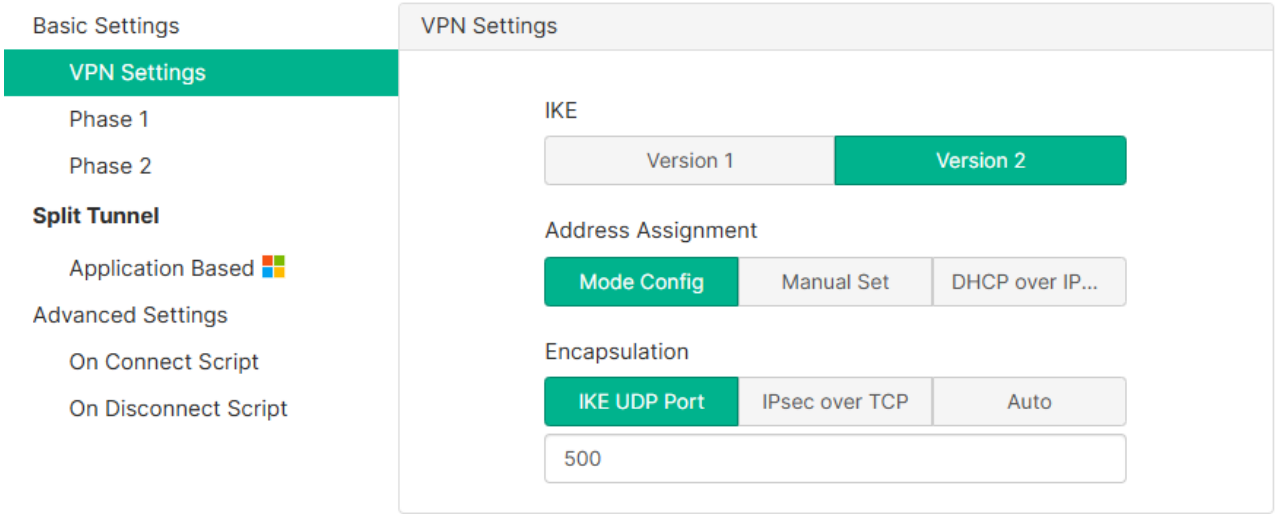
```
diagnose debug app eap_proxy -1
diagnose debug app authd -1
diagnose debug app samld -1
```

Verifying SAML configuration

Verify that SAML is configured correctly on EMS and FortiOS.

To verify the SAML configuration on EMS:

1. In EMS, go to *Endpoint Profiles* > *Remote Access*.
2. Edit the desired profile.
3. Under *VPN Tunnels*, edit the desired IPsec VPN tunnel.
4. In *Basic Settings* > *VPN Settings*, confirm that *Version 2* is selected under *IKE*.



5. Go to *Advanced Settings*.
6. Confirm that *EAP* is enabled.
7. Confirm that *Enable SAML Login* is toggled on and that you defined a custom port in *SAML Port*.

To verify the SAML configuration in FortiOS:

1. Confirm that `auth-ike-saml-port` is configured under `config system global` and matched to SAML port defined on EMS.
2. Ensure that the SAML user group is referenced in the firewall IPsec VPN policy or under `config vpn ipsec phase1-interface` as the `authusrgrp` parameter.
3. Confirm that the SAML server is mapped to an external port serving VPN connections, such as the WAN interface:

```
config system interface
       edit "port1"
               set ike-saml-server "<SAML server>"
       next
end
```

4. Verify that EAP is enabled:

```
config vpn ipsec phase1-interface
       set eap enable
       set eap-identity send-request
end
```

For a complete configuration guide, see IPsec VPN SAML-based authentication on page 334.

IPsec VPN SAML connection sequence

Understanding the sequence of the IPsec SAML connection process is crucial before beginning troubleshooting. See SAML-based authentication for FortiClient remote access dialup IPsec VPN clients.

Troubleshooting use cases

The majority of failures are results of misconfiguration. Therefore, it is critical to verify your SAML configuration prior to troubleshooting. See Verifying SAML configuration on page 395.

PSK mismatch

Peer authentication via a preshared key (PSK) occurs during the IKE_AUTH phase (`exchange=AUTH` in FortiGate IKE diagnostics).

If there is a PSK mismatch, the authentication process between FortiClient and FortiGate does not proceed beyond AUTH exchange.

In this case, the FortiGate IKE debug logs ends at `AUTH_RESPONSE`:

```
ike V=root:0:FSTP_SAML:33: received FCT-UID : 2665C39D4EE1467383FB49594AF45B38
ike V=root:0:FSTP_SAML:33: received EMS SN : FCTEMS8825002288
ike V=root:0:FSTP_SAML:33: received EMS tenant ID : 00000000000000000000000000000000
ike V=root:0:FSTP_SAML:33: re-validate gw ID
ike V=root:0:FSTP_SAML:33: gw validation OK
ike V=root:0:FSTP_SAML:33: responder preparing EAP identity request
```

```
ike 0:FSTP_SAML:33: enc
2700000C010000000A80CCE03000002802000000FCAFD5785CFDFC91EC4C6C4F3DE8F191DB3097928025144317E1A3F51F
1F23740000000901960005010201 02
ike 0:FSTP_SAML:33: out F6F0BE78E3ECDF1D55FC35815C84...
ike V=root:0:FSTP_SAML:33: sent IKE msg (AUTH_RESPONSE): 10.128.204.224:500->10.10.11.2:500,
len=128, vrf=0, id=f6f0be78e3ecdf1d/55fc35815c843162:00000001, oif=5
diag debug disable
```

This is because the FortiClient does not follow up in the authentication process due to authentication failure:

```
[FortiIKE  4553   debug] 0:FSTP IPsec (SAML):0: initiator received AUTH msg
[FortiIKE  1224   debug] 0:FSTP IPsec (SAML):0: peer identifier IPV4_ADDR 10.128.204.224
[FortiIKE  1494   debug] ikev2_verified: iph1 0x0000022290B63A80 auth verify done
[FortiIKE  4738   debug] 0:FSTP IPsec (SAML):0: initiator AUTH continuation
[FortiIKE  4765   debug] 0:FSTP IPsec (SAML):0: authentication failed
[FortiIKE  481   debug] 0:FSTP IPsec (SAML):0: schedule delete of IKE SA
f6f0be78e3ecdf1d:55fc35815c843162 iph1 0x0x0000022290B63A80
[FortiIKE  481   debug] 0:FSTP IPsec (SAML):0: schedule delete of IKE SA
f6f0be78e3ecdf1d:55fc35815c843162 iph1 0x0x0000022290B63A80
```

To resolve this issue:

Ensure that the PSK is identical between the FortiGate and FortiClient.



On newer FortiOS versions, you can download a FortiClient-compatible XML file for each IPsec VPN tunnel using the *Download tunnel XML* button. You can then insert this XML into EMS to ensure that the PSK value is the same between your FortiGate and FortiClient.

EAP response is empty

You may observe the following error due to user group misconfiguration.

```
ike V=root:0:FSTP_SAML:53: initiating EAP authentication
ike V=root:0:FSTP_SAML: EAP user "2665C39D4EE1467383FB49594AF45B38"
ike V=root:0:FSTP_SAML: EAP failed for user "2665C39D4EE1467383FB49594AF45B38"
ike V=root:0:FSTP_SAML: EAP response is empty
ike V=root:0:FSTP_SAML: connection expiring due to EAP failure
```

To resolve this issue:

Do one of the following in FortiOS:

- In the applicable IPsec VPN firewall policy, reference the applicable user group.
- In the CLI, configure the applicable user group under `config vpn ipsec phase1-interface` as follows:

```
config vpn ipsec phase1-interface
       edit <name>
               set authusrgrp "<SAML user group>"
```

```
        next
end
```

Do not apply both of the listed configurations.

gw validation failed

There can be multiple reasons for this error and most of them are configuration-related. Therefore, once observed, it is critical to verify your SAML configuration prior to troubleshooting. See Verifying SAML configuration on page 395.

```
ike V=root:0:FSTP_SAML:41: gw validation failed
ike V=root:FSTP_SAML Negotiate SA Error: gateway validation failed
```

Local or peer ID misconfiguration

Ensure that the local ID defined on EMS matches `peerid` on the FortiGate.

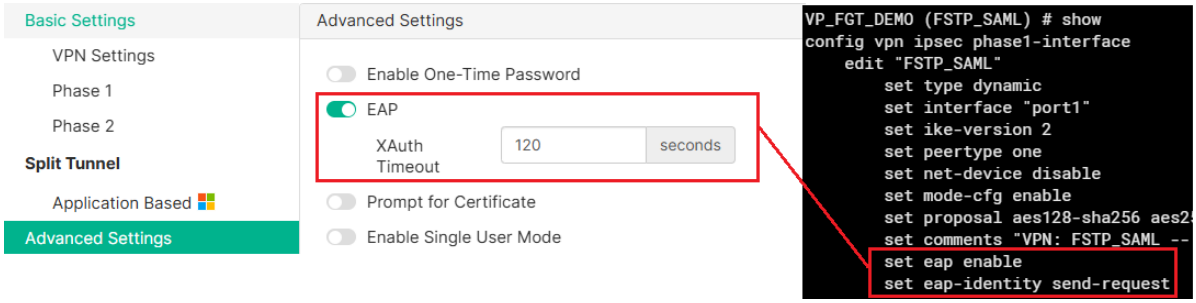
To verify the local and peer ID configuration:

1. In EMS, go to *Endpoint Profiles* > *Remote Access*.
2. Edit the desired profile.
3. Under *VPN Tunnels*, edit the desired IPsec VPN tunnel.
4. In *Phase 1*, observe the value under *Local ID*.
5. In FortiOS, run the following commands. Confirm that the value in `set peerid` matches the local ID configured on EMS:

```
config vpn ipsec phase1-interface
        edit <name>
        show
```

EAP misconfiguration

When EAP is disabled in EMS or the FortiGate, FortiGate IKE diagnostics may present `gw validation failed` error. Ensure that EAP is enabled for both EMS and FortiOS. See Verifying SAML configuration on page 395.



No SAML method found

When FortiClient does not open a browser for SAML authentication and simply reverts to login, include `diagnose debug app authd -1` in the FortiGate diagnostics.

An error like this may appear:

```
[authd_local_saml_auth:5844]: SAML login with UID '2665C39D4EE1467383FB49594AF45B38'.
[authd_local_saml_auth:5857]: No SAML method found.
```

To resolve this issue:

Ensure that the FortiGate interface that acts as a first point of contact for incoming traffic from the FortiClient dialup connections has `set ike-saml-server` configured. This interface may or may not be the WAN interface.

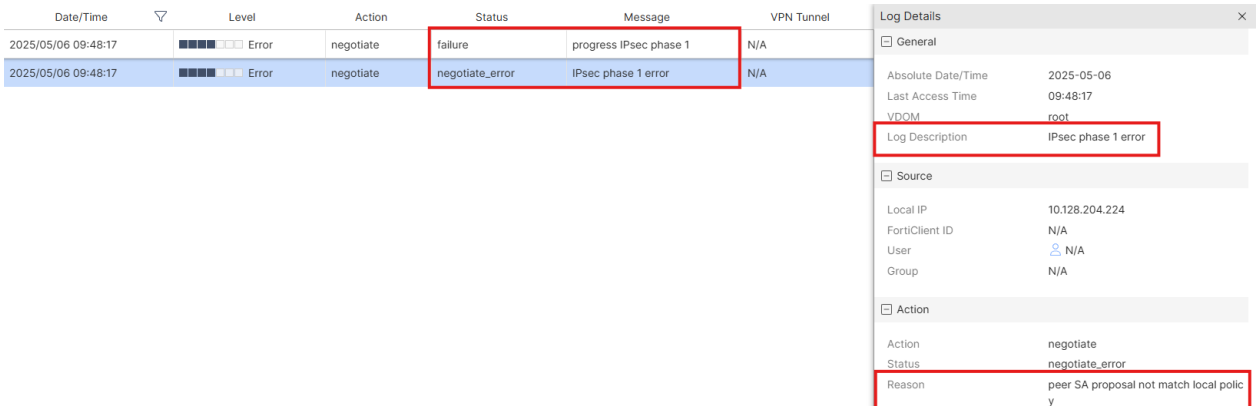
No proposal chosen

This error may appear during two phases of IKEv2 connection - IKE_SA_INIT (phase 1 configuration on FortiClient) and IKE_AUTH (phase 2 configuration on FortiClient).

The following shows an example of the FortiOS CLI output for this issue:

```
ike V=root:0:d8196d424283cd4e/0000000000000000:36: no proposal chosen
ike V=root:d8196d424283cd4e/0000000000000000 Negotiate SA Error: peer SA proposal not match local
policy
ike V=root:0:d8196d424283cd4e/0000000000000000:36: no proposal chosen, send error response
```

The following shows an example of a VPN *System Event* log view showing IPsec VPN phase 1 (IKE_SA_INIT) negotiation failure. A similar message shows for phase 2.



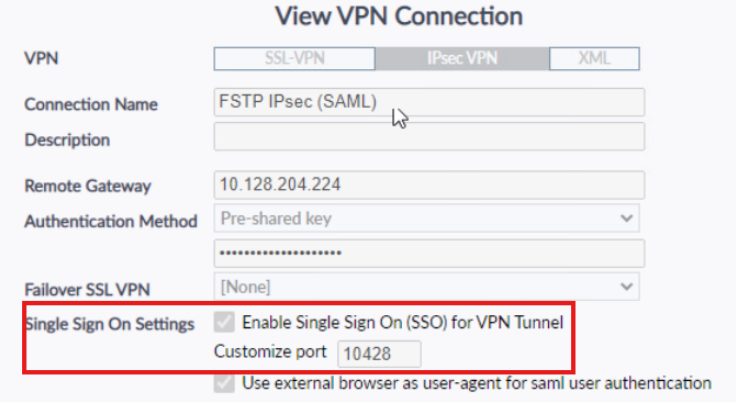
To resolve this issue:

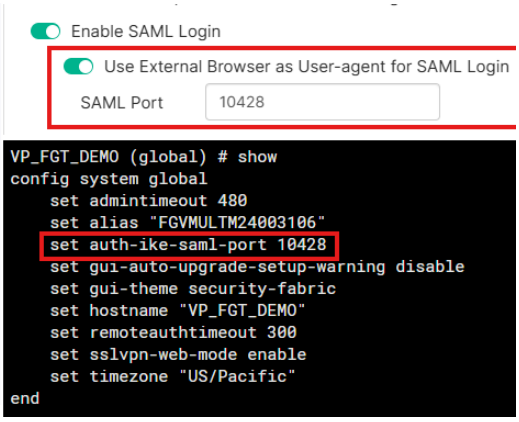
1. Validate that the IPsec VPN tunnels have IKEv2 enabled on EMS and FortiOS.
2. Ensure that the incoming SA (FortiClient IKE proposal) is accurately matched to the phase 1 configuration under `config vpn ipsec phase1-interphase` on FortiGate.
3. Verify the security parameters of phase 1 SAs match on FortiClient and FortiGate.
4. Verify the security parameters of phase 2 SAs match on FortiClient and FortiGate.

Browser issues

When user clicks *Connect*, FortiClient sends a request to the FortiGate port defined by `auth-ike-saml-port` as SAML-based authentication for FortiClient remote access dialup IPsec VPN clients describes.

When the browser does not open, FortiClient gets stuck, or no authentication window displays, it can mean `auth-ike-saml-port` is misconfigured or, more generally, FortiClient fails to reach the FortiGate over that port.





The web framework used for SAML authentication affects the logs. See Technical Tip: FortiClient SAML Authentication Configuration Demystified. Depending on the framework used, verify the following logs:

External browser

FortiTray

```
[580:12804] [fortitray  220   debug] SamlAuth::QueryIpsecSamlDataExtBrowser() called.
[580:12804] [fortitray  4713   error] CFortiTrayDlg::RequestMissingVPNCredentials() could not get
saml data.
[580:12804] [fortitray  4753   debug] CFortiTrayDlg::RequestMissingVPNCredentials() ends. res=3
[580:7416] [fortitray  192   debug] cbPIPEMSG_VPN_CONNECTION_ERROR 2053
```

FortiTray.exe_FortiAuth.log

```
[580:12804] [FortiAuth  101   error] GetHttpResponse() WinHttpSendRequest failed.
[580:12804] [FortiAuth  458   error] QueryIpsecExtBrowserSamlStartUrl() could not extract the
start url in response.()
[580:12804] [FortiAuth  528   error] GetIpsecSamlDataExternalBrowser() Failed to get ipsec saml
external browser start url.
```

WebView2

FortiTray

```
[2025-05-07 11:25:05.7873592 UTC-07:00] [7804:11976] [fortitray  251   debug]
SamlAuth::PickSamlAuthProvider() saml auth provided: 0
[2025-05-07 11:25:13.6196951 UTC-07:00] [7804:8008] [fortitray  311    info]
SamlAuth::QuerySamlData::<lambda_2737bdf304228843c31873ebb86af054>::operator ()() Response
returned.
[2025-05-07 11:25:13.6197081 UTC-07:00] [7804:8008] [fortitray  350   debug]
SamlGetResponse=0xa7000006
[2025-05-07 11:25:13.6197098 UTC-07:00] [7804:8008] [fortitray  359   error]
SamlAuth::QuerySamlData() Get Saml Response ERROR ret=0xa7000006
[2025-05-07 11:25:13.6199290 UTC-07:00] [7804:8008] [fortitray  4591   debug]
CFortiTrayDlg::StartIPSecSAML() lRet=0xa7000006
[2025-05-07 11:25:13.6199343 UTC-07:00] [7804:8008] [fortitray  4593   error] QuerySamlData()
failed. lRet=0xa7000006
```

FortiTray.exe_FortiAuth.log

```
[7804:11692] [FortiAuth  228   debug] RunFortiAuthInSession() CMD to start auth module:  --
provider-name=WebView2 --receiver=2844  --object="saml:ipsecvpn:2665C39D4EE1467383FB49594AF45B38"
--object-name="FSTP IPsec (SAML)" --url="https://10.128.204.224:10429/saml_login?" --
description="FortiClient SAML Authentication" --ignore-certificate=1 --timeout=300 --delete-
cookies
[7804:11692] [FortiAuth  245    info] CreateProcessW() returned 1
[7804:11692] [FortiAuth  248   debug] Process Id: 3584
[7804:11692] [FortiAuth  292    info] Caller deliberately terminates auth process.
[7804:11692] [FortiAuth  224   error] RunFortiAuthInSession=0xa7000007
[7804:11692] [FortiAuth  261    info] SamlGetResponseUsingExternalAuthProvider exit with
HRESULT=0x0xa7000007
```

Electron

FortiTray.exe_FortiAuth.log

```
[7804:7224] [FortiAuth  228   debug] RunFortiAuthInSession() CMD to start auth module:  --
provider-name=Electron --receiver=2936  --
object="saml:ipsecvpn:2665C39D4EE1467383FB49594AF45B38" --object-name="FSTP IPsec (SAML)" --
url="https://10.128.204.224:10429/saml_login?" --description="FortiClient SAML
Authentication" --ignore-certificate=1 --timeout=300 --delete-cookies
[7804:7224] [FortiAuth  245    info] CreateProcessW() returned 1
[7804:7224] [FortiAuth  248   debug] Process Id: 6316
[7804:7224] [FortiAuth  276   debug] Daemon exit code: 0xa7000006
[7804:7224] [FortiAuth  234   debug] decode base64 to cipher binary, cipher len=304
[7804:7224] [FortiAuth  224   error] RunFortiAuthInSession=0xa7000006
[7804:7224] [FortiAuth  261    info] SamlGetResponseUsingExternalAuthProvider exit with
HRESULT=0x0xa7000006
```

FortiTray

```
[7804:8008] [fortitray  4573   debug] CFortiTrayDlg::StartIPSecSAML() connection_name=FSTP
IPsec (SAML) remote_gateway=10.128.204.224 dwSSOPort=10429
[7804:8008] [fortitray  231   debug] szRetUrl=https://10.128.204.224:10429/saml_login?
[7804:8008] [fortitray  301   debug] Reset cancel event.
[7804:7224] [fortitray  36   debug] ThreadGetResponse() called.
[7804:7224] [fortitray  251   debug] SamlAuth::PickSamlAuthProvider() saml auth provided: 1
[7804:8008] [fortitray  311    info] SamlAuth::QuerySamlData::<lambda_
2737bdf304228843c31873ebb86af054>::operator ()() Response returned.
[7804:8008] [fortitray  350   debug] SamlGetResponse=0xa7000006
[7804:8008] [fortitray  359   error] SamlAuth::QuerySamlData() Get Saml Response ERROR
ret=0xa7000006
[7804:8008] [fortitray  4591   debug] CFortiTrayDlg::StartIPSecSAML() lRet=0xa7000006
[7804:8008] [fortitray  4593   error] QuerySamlData() failed. lRet=0xa7000006
```

samlauth.log

```
[info]  doSAMLConnect - saml_auth_request={"saml_auth_
url":"https://10.128.204.224:10429/saml_login?","saml_auth_
object":"saml:ipsecvpn:2665C39D4EE1467383FB49594AF45B38","saml_auth_object_name":"FSTP IPsec
(SAML)","saml_auth_ignore_certificate":1,"saml_auth_timeout":"300","saml_auth_
description":"FortiClient SAML Authentication","saml_auth_delete_cookies":true,"saml_auth_
receiver":"2936"}
[info]  deleteSAMLTunnelCookies tunnel_name=FSTP IPsec (SAML) tunnel_type=ipsecvpn
[info]  deleteSAMLTunnelCookies tunnel_cookies=
[info]  doSAMLConnect saml_auth_request={"saml_auth_url":"https://10.128.204.224:10429/saml_
login?","saml_auth_object":"saml:ipsecvpn:2665C39D4EE1467383FB49594AF45B38","saml_auth_
object_name":"FSTP IPsec (SAML)","saml_auth_ignore_certificate":1,"saml_auth_
timeout":"300","saml_auth_description":"FortiClient SAML Authentication","saml_auth_delete_
cookies":true,"saml_auth_receiver":"2936"}
[info]  SAMLAUTH - openURL url=https://10.128.204.224:10429/saml_login?
type=saml:ipsecvpn:2665C39D4EE1467383FB49594AF45B38
[info]  SAMLAUTH - loadUrlWithType Obj=saml:ipse url=https://10.128.204.224:10429/saml_login?
[info]  load ipsec saml uid=2665C39D4EE1467383FB49594AF45B38
[info]  SAMLAUTH - did-fail-load errorCode=-118 errorDescription=ERR_CONNECTION_TIMED_OUT
validatedURL=https://10.128.204.224:10429/saml_login?
[info]  saveSAMLResponse saml_auth_receiver=2936 saml_response.length=282
[info]  SAMLAUTH - exit with code=-1493172218
```

Web browser

FortiTray

```
[fortitray  251   debug] SamlAuth::PickSamlAuthProvider() saml auth provided: 2
[fortitray  311    info] SamlAuth::QuerySamlData::<lambda_
2737bdf304228843c31873ebb86af054>::operator ()() Response returned.
```

```
[fortitray  350   debug] SamlGetResponse=0xa7000000
[fortitray  353   error] FCT_AUTH_UNKNOWN, tries=0
[fortitray  359   error] SamlAuth::QuerySamlData() Get Saml Response ERROR ret=0xa7000000
```

FortiAuth.log

```
[FortiAuthExe] [Info] [4594s] [4594:1] Auth start
[FortiAuthExe] [Info] --provider-name=WebBrowser
[FortiAuthExe] [Info] --receiver=2796
[FortiAuthExe] [Info] --object=saml:ipsecvpn:2665C39D4EE1467383FB49594AF45B38
[FortiAuthExe] [Info] --object-name=FSTP IPsec (SAML)
[FortiAuthExe] [Info] --url=https://10.128.204.224:10429/saml_login?
[FortiAuthExe] [Info] --description=FortiClient SAML Authentication
[FortiAuthExe] [Info] --ignore-certificate=1
[FortiAuthExe] [Info] --timeout=300
[FortiAuthExe] [Info] --delete-cookies
[FormSamlAuth] [Info] WebBrowserMajorVersion=11
[FormSamlAuth] [Info] ShowForm=False
[FormSamlAuth] [Error] Program.FCT_AUTH_UNKNOWN->The operation has timed out
```

FortiTray.exe_FortiAuth.log

```
[FortiAuth  228   debug] RunFortiAuthInSession() CMD to start auth module:  --provider-
name=WebBrowser --receiver=2796  --object="saml:ipsecvpn:2665C39D4EE1467383FB49594AF45B38" --
object-name="FSTP IPsec (SAML)" --url="https://10.128.204.224:10429/saml_login?" --
description="FortiClient SAML Authentication" --ignore-certificate=1 --timeout=300 --delete-
cookies
[FortiAuth  245    info] CreateProcessW() returned 1
[FortiAuth  248   debug] Process Id: 1304
[FortiAuth  276   debug] Daemon exit code: 0xa7000000
[FortiAuth  234   debug] decode base64 to cipher binary, cipher len=0
[FortiAuth  285   error] Could not decrypt saml data. nRet=-10
[FortiAuth  224   error] RunFortiAuthInSession=0xa7000000
```

SAML authentication issues

Most authentication issues, if not on the identity provider (Microsoft Entra ID, Okta, FortiAuthenticator, and so on) side are group-related, such as a group mismatch, unless EAP is misconfigured, as in EAP response is empty.

When troubleshooting SAML authentication issues, ensure to include the following FortiGate CLI commands on top of `ike` diagnostics:

```
diagnose debug app fnbamd -1
diagnose debug app samld -1
```

Troubleshooting IPsec VPN IKEv1

This document focuses on troubleshooting multiple scenarios of IPsec VPN IKEv1 connection failures.

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.

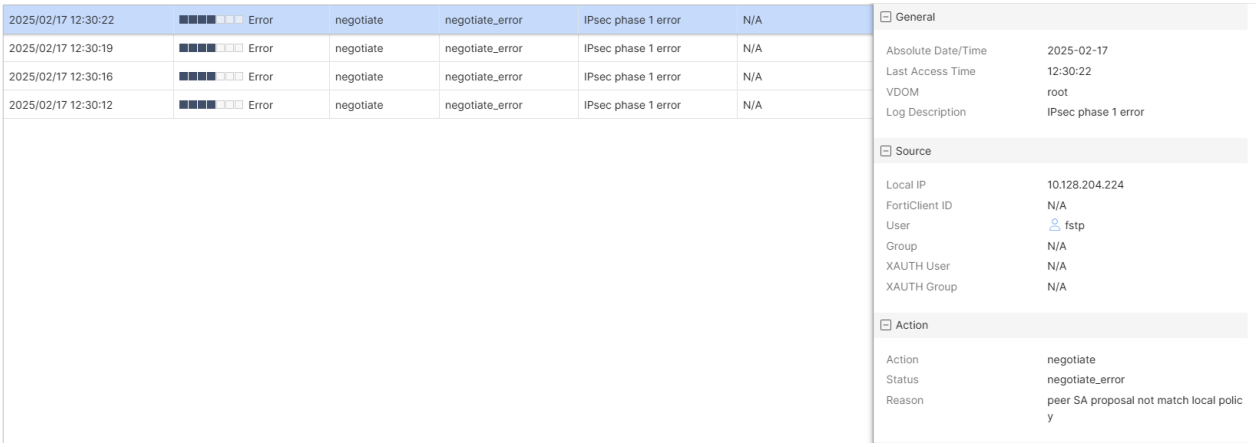
Since FortiClient is in a loop, FortiOS IKE diagnostics will reflect multiple repeated incoming SA proposals. The result of each proposal is the same when there is a proposal mismatch. In this situation, you may run the following FortiOS IKE diagnostic commands for troubleshooting:

```
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.

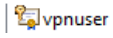
FortiClient cannot obtain certificate

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 267.

   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 267.
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:

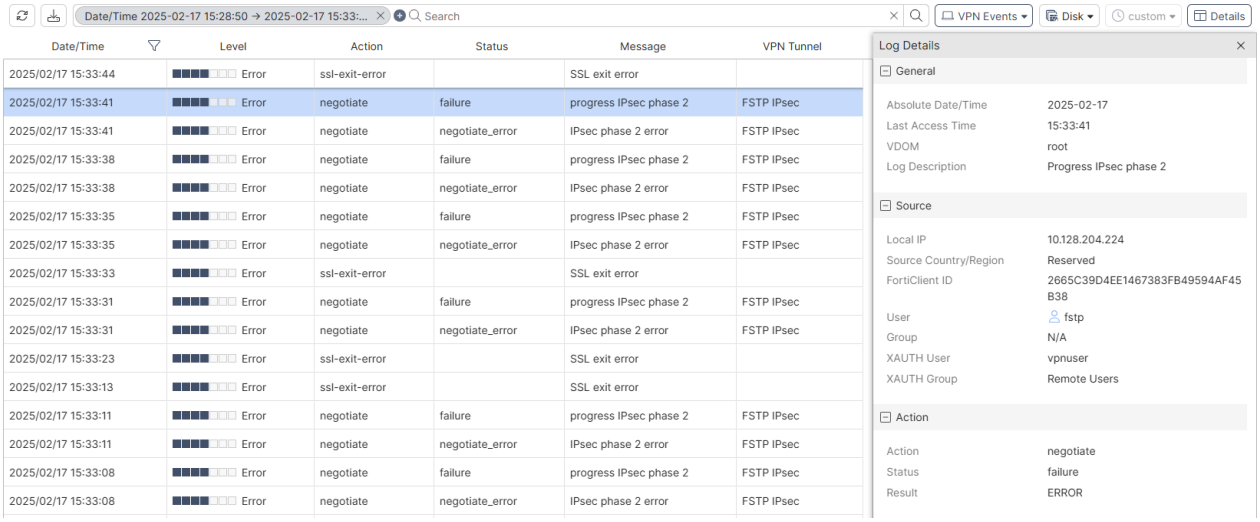
1. Include `fnbamd` diagnostics.
2. Verify firewall group settings in the IPsec VPN firewall policy and/or `config vpn ipsec phase1-interface` > `authgrp`. Typically, either one of them should be used.
3. Ensure that the credentials are correct.

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 267 and Phase 1 configuration.
2. Ensure that the PFS settings match on the FortiClient and FortiGate as well as the DH group.

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.

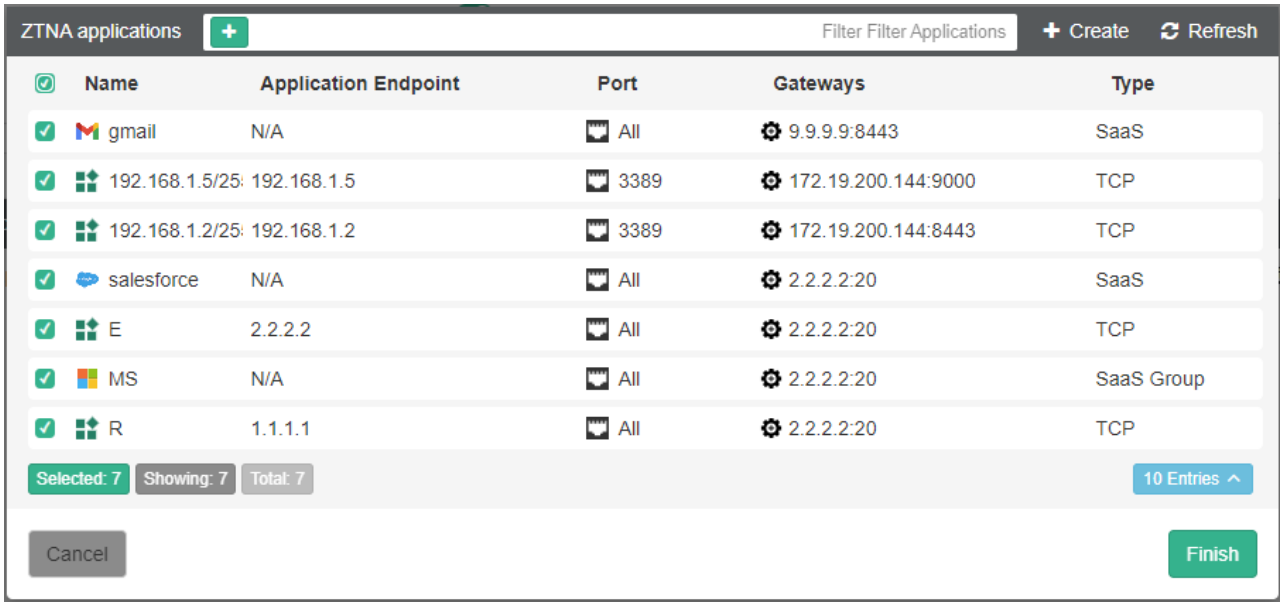
See ZTNA Applications Catalog on page 527 to view the ZTNA applications available for selection.

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.

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.

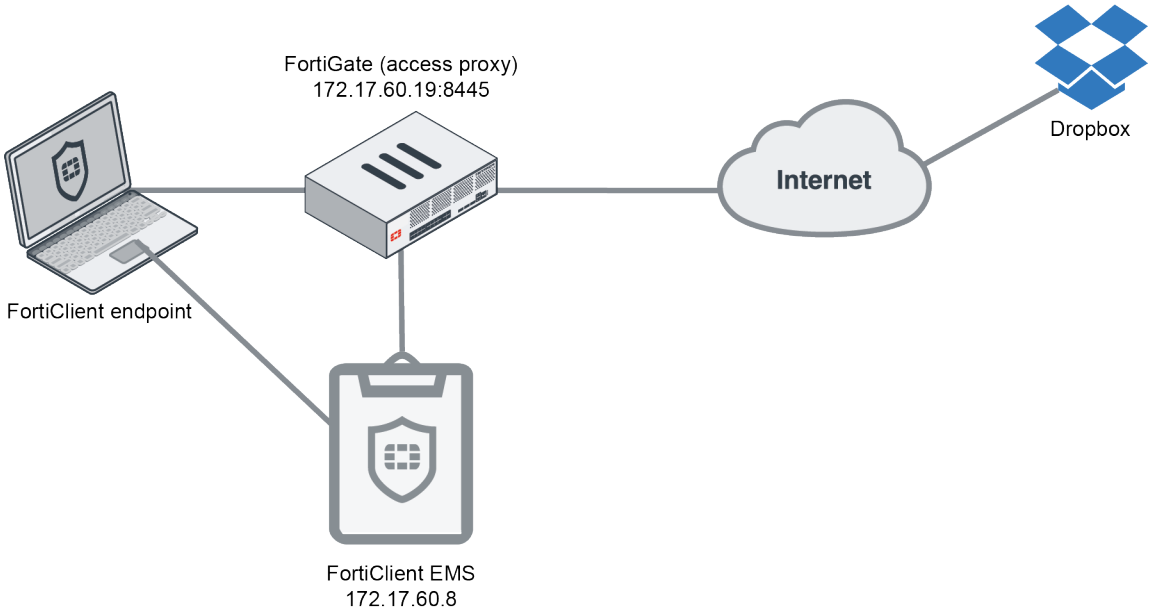
8. On an endpoint that received the profile changes, go to *ZTNA Destination*. You can see the ZTNA applications from the list that EMS received from FortiOS.

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



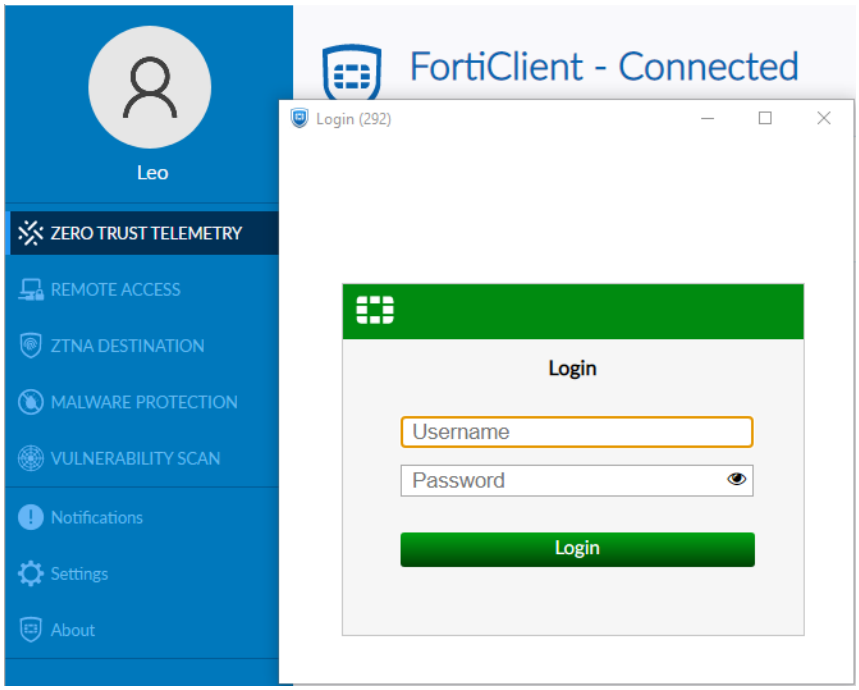
In the example topology, the EMS IP address is 172.17.60.8. The FortiGate acts as an access proxy, with virtual IP address 172.17.60.19 and port 8445. You can use one of the following methods to configure a ZTNA rule that supports wildcard FQDNs:

- Configuring a ZTNA rule in EMS
- Configuring FortiClient to pull SaaS application information from FortiOS

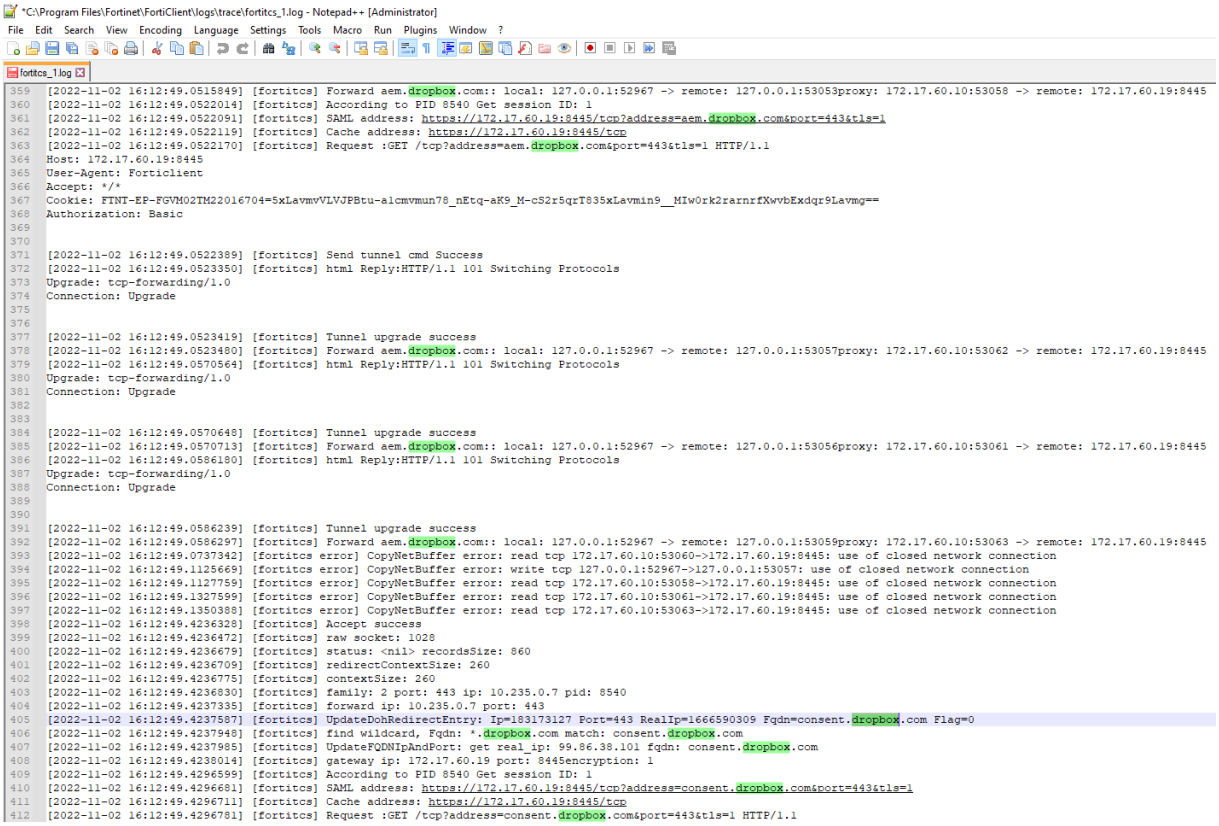
To configure a ZTNA rule for an FQDN in wildcard format using method 1:

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
```

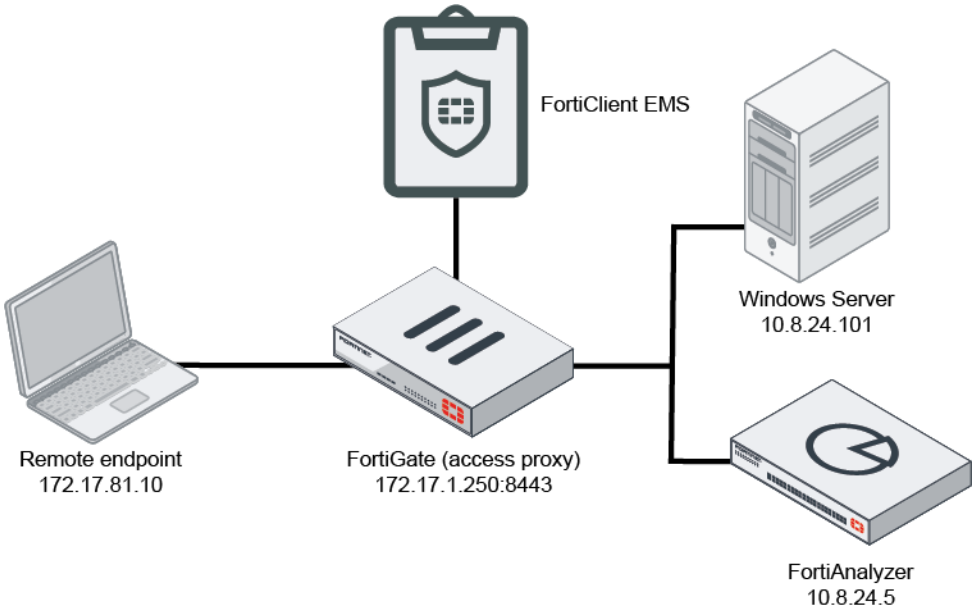
Normal text file

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.

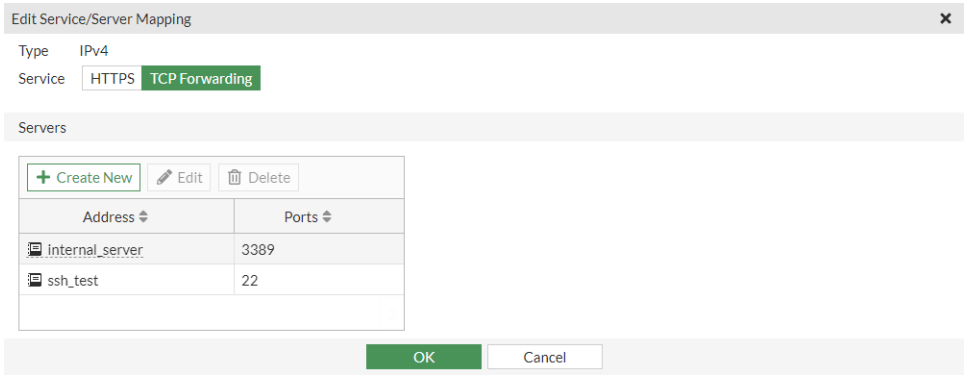
The following shows the topology for this example. This example uses two FQDNs, rdp.win.test and ssh.win.test, in place of the Windows server IP address, 10.8.24.100. This hides the internal IP address, 10.8.24.100, from end users.



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.

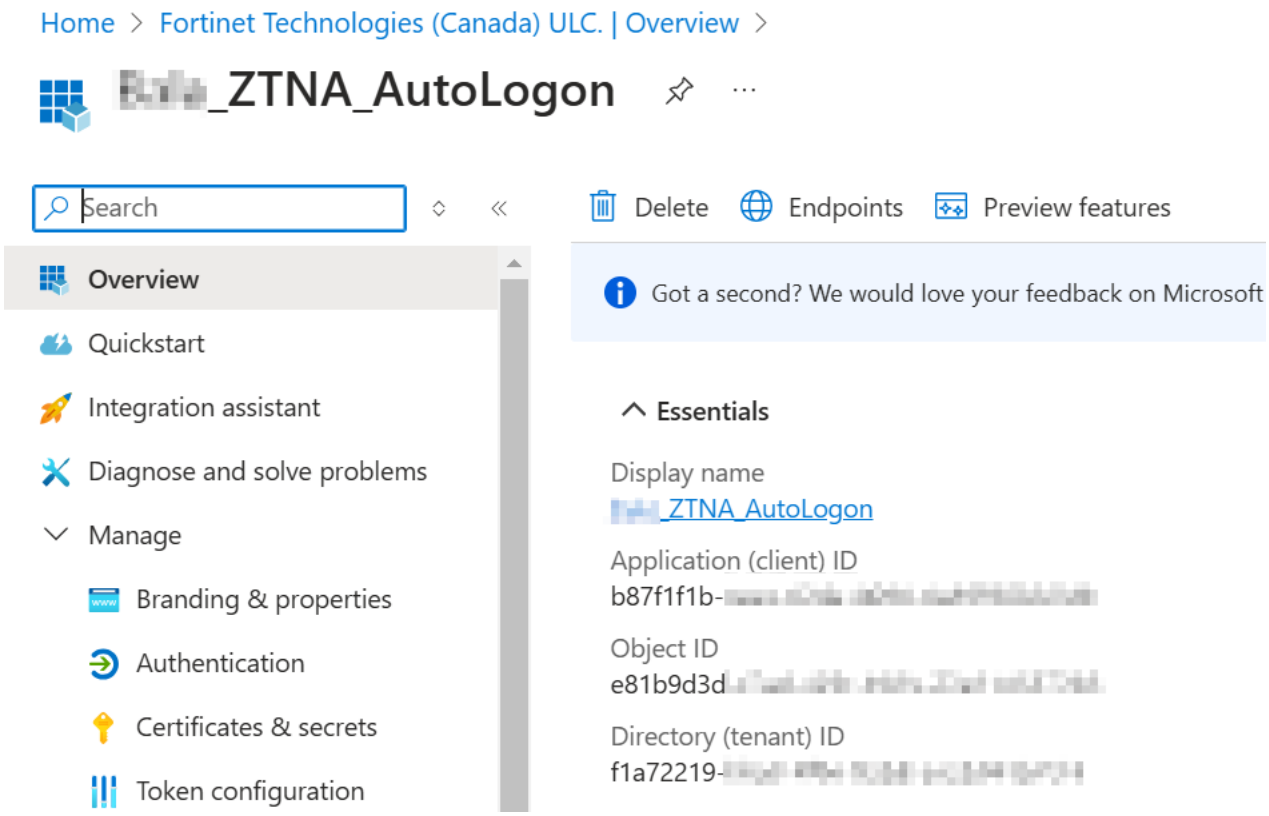
1. Go to *Fabric & Connectors > ZTNA Applications Catalog*.
2. Create the RDP ZTNA application:
   a. Click *Add*.
   b. Select *FQDN*, then enter rdp.win.test. This field does not support entering a hostname.
   c. Select *Port*, then enter the desired port number.
   d. Click *Add Gateway*.
   e. In 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
```

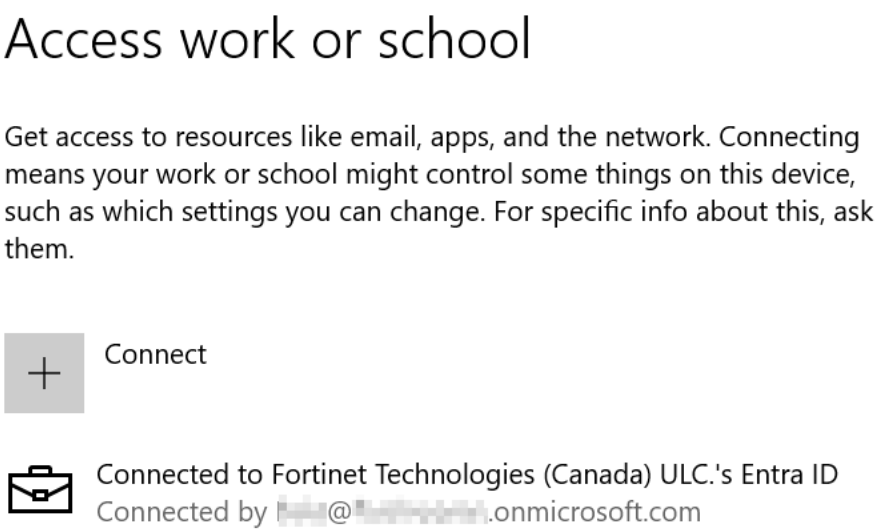
```
config authentication scheme
    edit "Autologon"
        set method entra-sso
        set external-idp "eip1"
    next
end
config authentication rule
    edit "Auth"
        set srcintf "port1"
        set srcaddr "all"
        set ip-based disable
        set sso-auth-method "Autologon"
        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. Click *XML*, then click *Edit*.
   d. Configure the profile as follows. Configure `<client_id>` and `<tenant_name>` with the *Application (client) ID* and *Directory (tenant)* ID values for the enterprise application in the Entra ID portal. Lines bolded in the XML sample highlight key fields to support this feature:

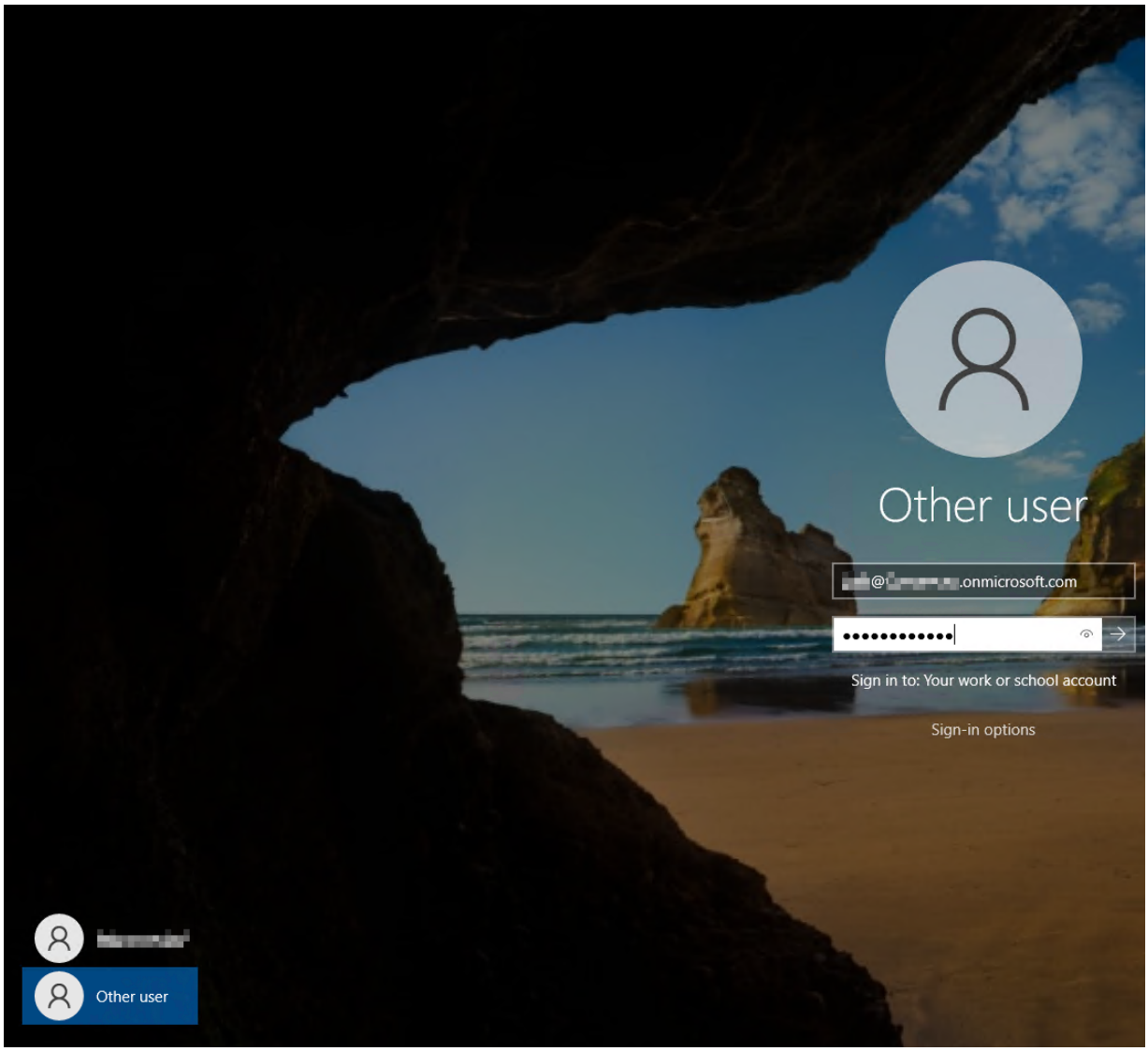
```
<forticlient_configuration>
    <ztna>
        <enabled>1</enabled>
        <notify_on_error>1</notify_on_error>
        <portals_enabled>1</portals_enabled>
        <web_proxy_rules>
            <web_proxy_rule>
                <gateway>10.152.35.188:8445</gateway>
                <gateway_ip>10.152.35.188:8445</gateway_ip>
            </web_proxy_rule>
        </web_proxy_rules>
        <azure_auto_login>
            <enabled>1</enabled>
            <azure_app>
                <client_id>b87f1f1b...</client_id>
                <tenant_name>f1a72219...</tenant_name>
            </azure_app>
        </azure_auto_login>
        <gateways_enabled>1</gateways_enabled>
        <allow_personal_rules>1</allow_personal_rules>
        <disallow_invalid_server_certificate>0</disallow_invalid_server_certificate>
        <rules>
            <rule uid="3BDCA7D2-75EE-404F-8322-1FECFAF85109">
                <name>ssh.example.com:22</name>
                <enable_udp>0</enable_udp>
```

```
                <type>private</type>
                <app_uid>6ea31259-617a-59b5-16e5-74a61f8cd31a</app_uid>
                <allow_all_gateways>1</allow_all_gateways>
                <mask/>
                <encryption>0</encryption>
                <mode>transparent</mode>
                <destination>ssh.example.com:22</destination>
                <gateway>fgt2.example.com:8445</gateway>
                <redirect>0</redirect>
                <gateway_ip>10.152.35.188</gateway_ip>
            </rule>
        </rules>
        <disabled_rules/>
    </ztna>
<forticlient_configuration>
```

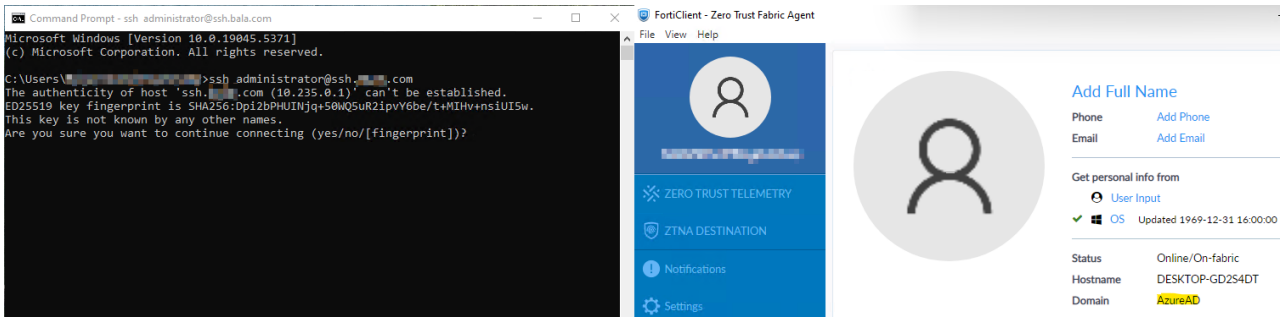
3. Connect the endpoint to the Entra ID domain:
   a. Go to *Settings > Access work or school > Join this device to Microsoft Entra ID*.
   b. Log in with your Entra ID credentials.
   c. Confirm that the endpoint connected successfully.



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

Configuration		Description
		that you have configured to be allowed in the blocklist.
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 248.
Log All URLs		Log all URLs. When this setting is disabled, 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 this option is enabled, 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	When this option is enabled, 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.
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.

Configuration	Description
	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.
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 208 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.

Configuration	Description
Adult/Mature Content	• Abortion • Advocacy Organizations • Alcohol • Alternative Beliefs • Dating • Gambling • Lingerie and Swimsuit • Marijuana • Nudity and Risque • 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 435.
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 208 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 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 FortiClient EMS, then synchronize the Web Filter profile settings to an endpoint profile in FortiClient EMS.

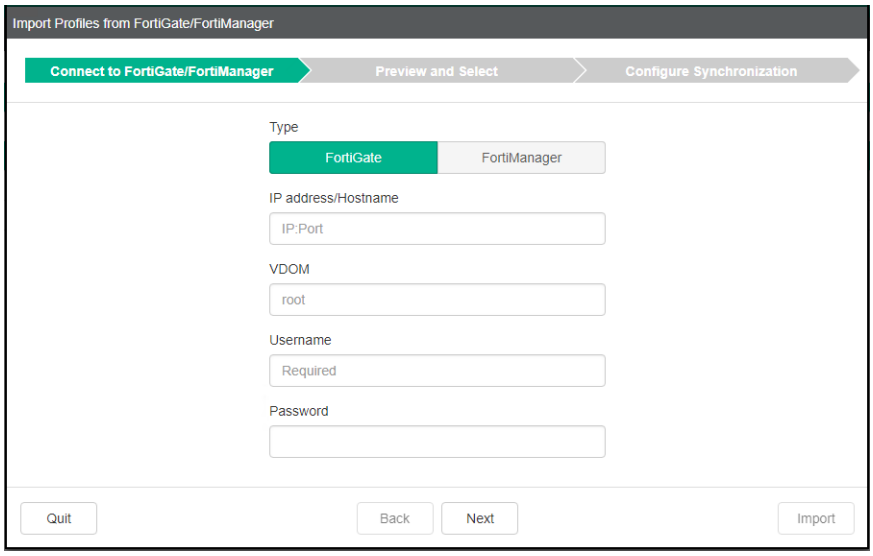
This feature is only available if Web Filter is enabled in *Feature Select*. See Feature Select on page 655.

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
```

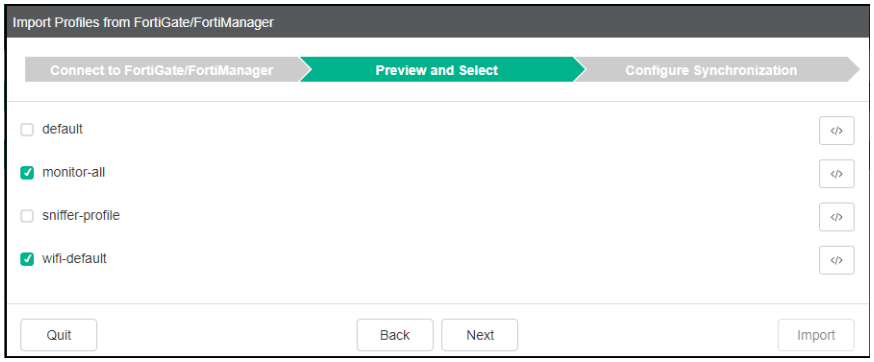
2. Go to *Endpoint Profiles* > *Import from FortiGate / FortiManager*. Click *Import from FortiGate / FortiManager*.



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.

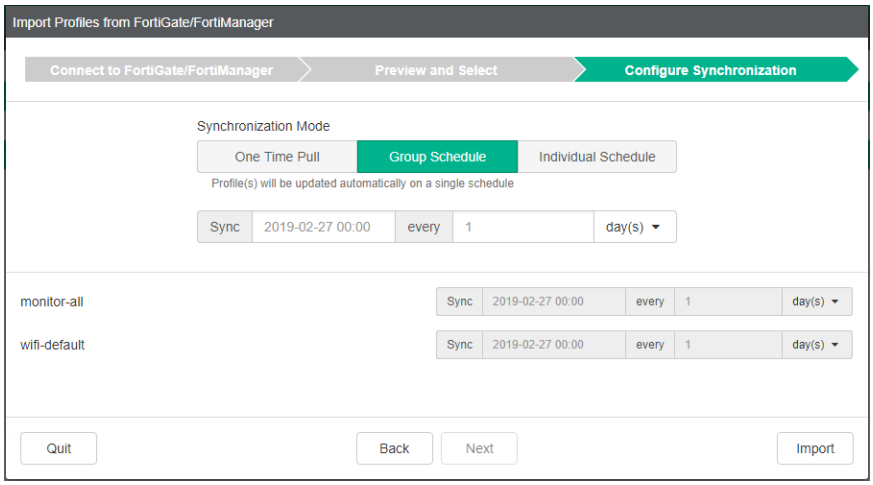
The list of Web Filter profiles configured on the FortiGate or FortiManager displays.



You can click the </> icon beside each profile to preview the settings in XML format.

5. Select the profiles to import into FortiClient EMS and click *Next*.

6. Under *Synchronization Mode*, select one of the following options.



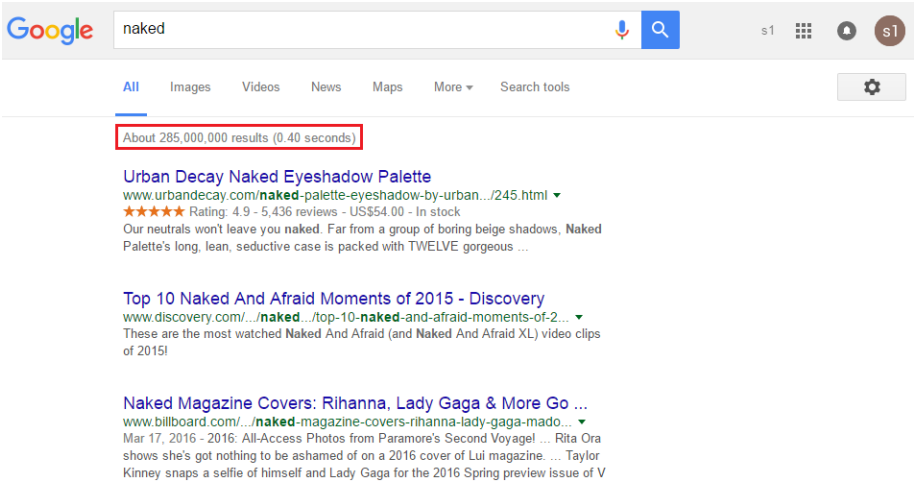
   a. *One Time Pull*: FortiClient EMS does not automatically sync profile changes from the FortiGate or FortiManager. You can manually sync profile changes after importing the profile. See Syncing profile changes on page 257.
   b. *Group Schedule*: Configure a group synchronization schedule for all selected 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 422.
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

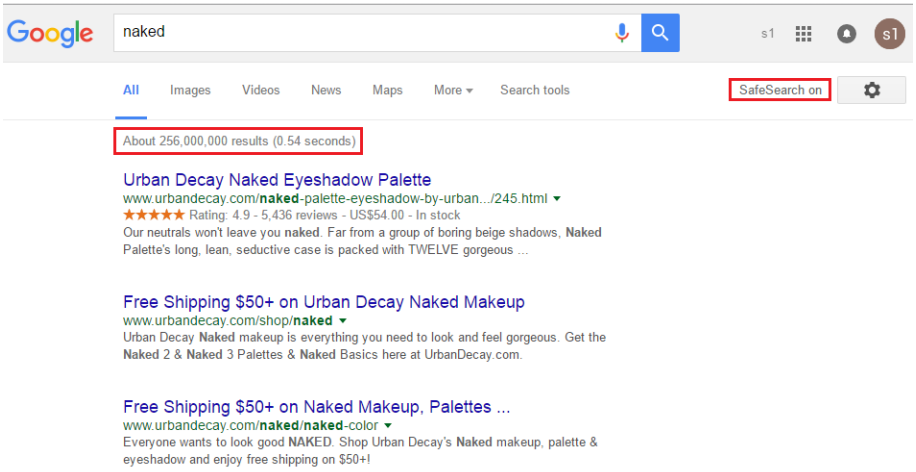
The search engine provides a Safe Search feature that blocks inappropriate or explicit images from search results. The Safe Search feature helps avoid most adult content. FortiClient EMS supports Safe Search for most common search engines, such as Google, Yahoo, and Bing.

The profile in FortiClient EMS 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 FortiClient EMS, 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

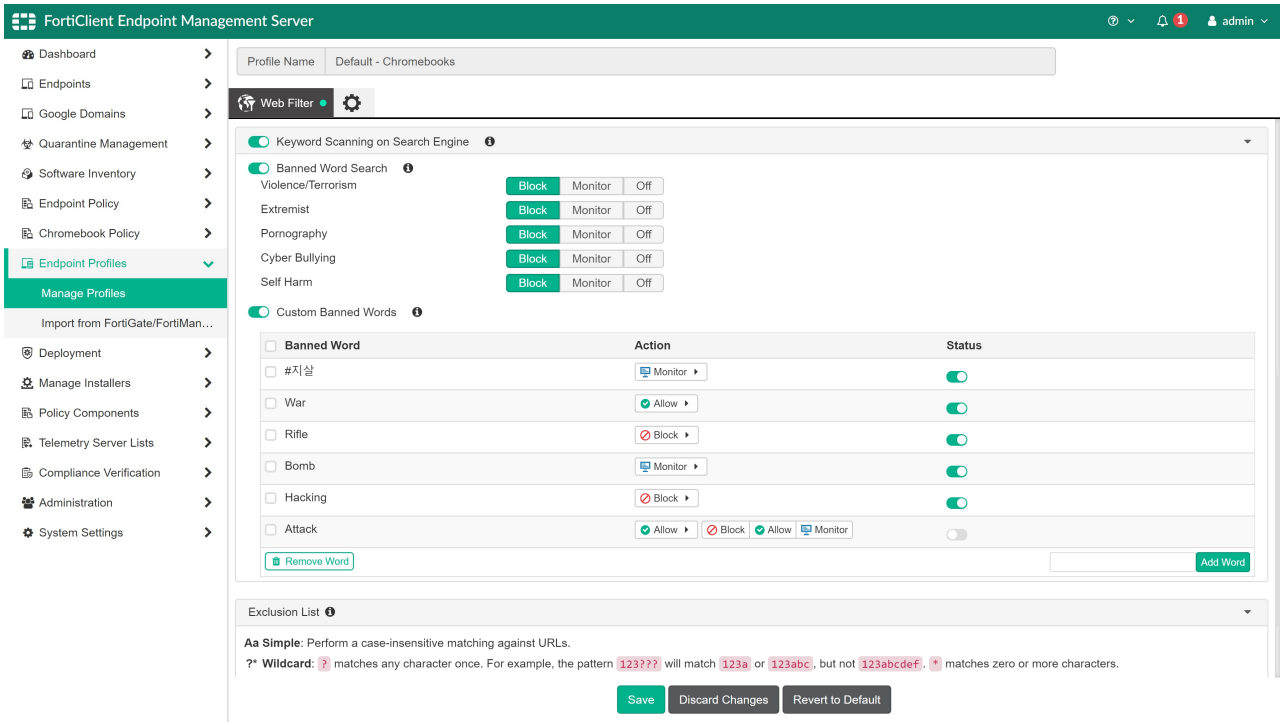
Configuring banned word check in URL

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.

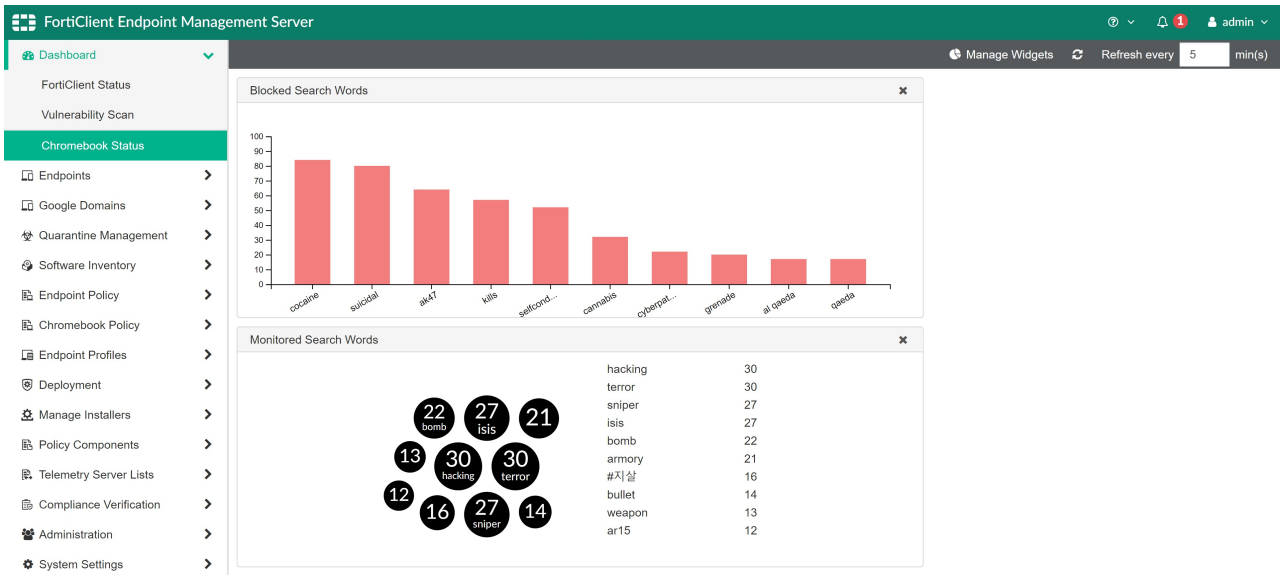
To enable keyword scanning on search engines:

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:

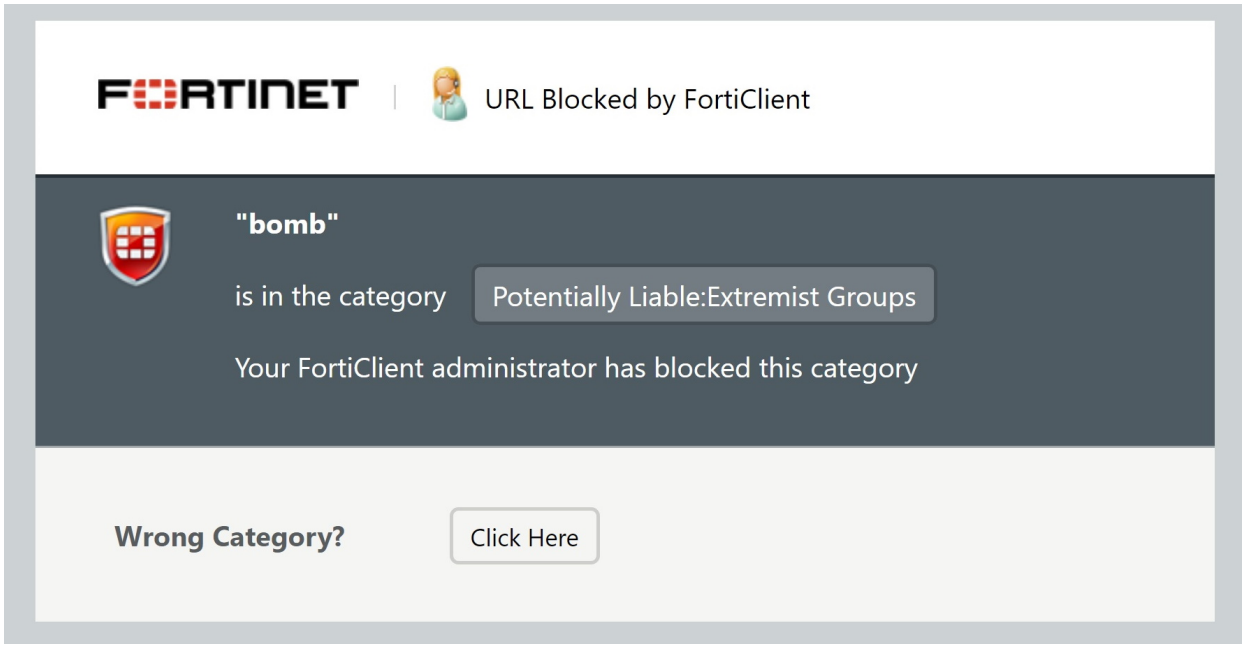
Banned Word Search	Enable to configure actions (block or monitor) to take when the user searches for terms that belong to the following categories: • Violence/Terrorism • Extremist • Pornography • Cyber Bullying • Self Harm
Custom Banned Words	Configure actions for individual terms. Enable *Custom Banned 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.



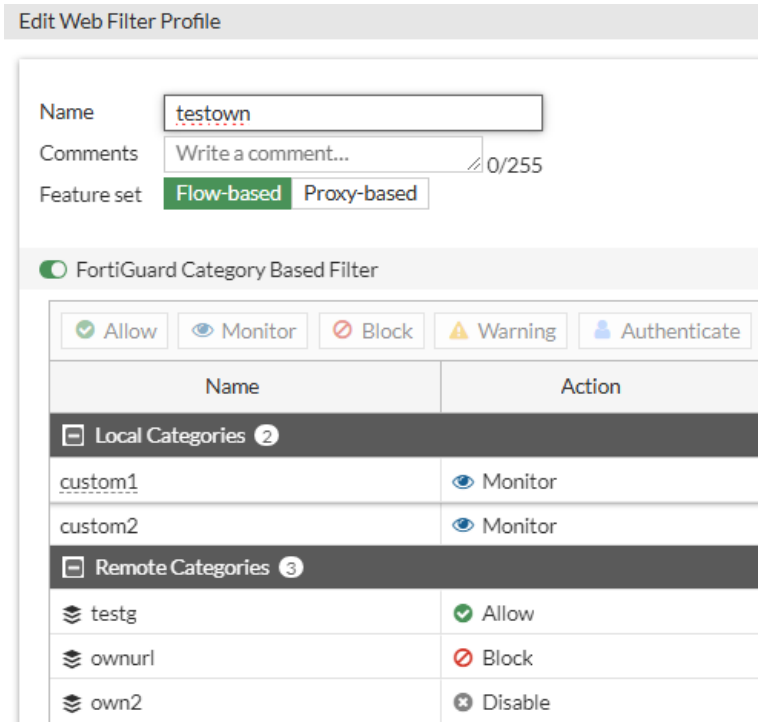
Syncing remote categories from imported FortiOS or FortiManager Web Filter profile

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

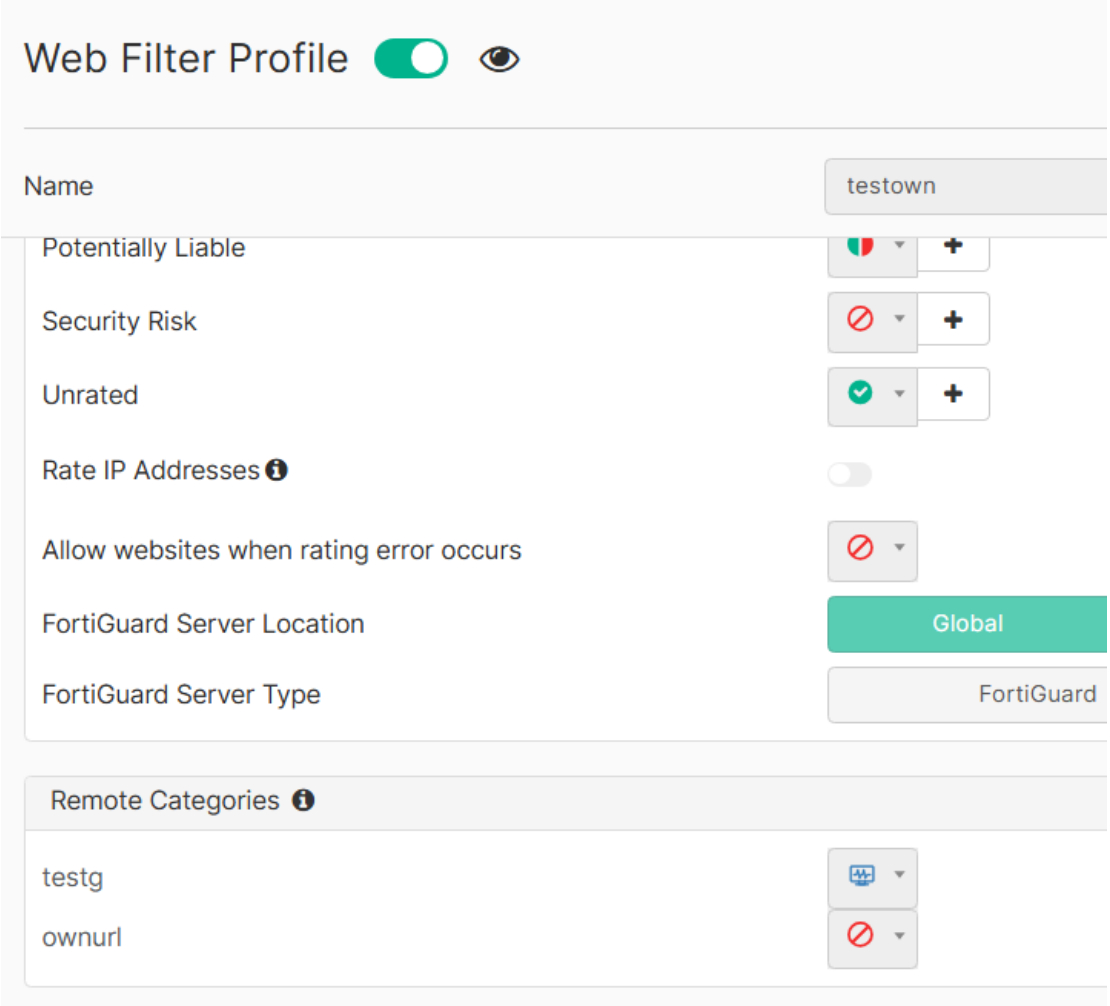
the profile name, URL list, and the configured action for this URL list: allow, monitor, or block. Prior to this enhancement, customers manually updated the FortiOS static URL filter list, which was time-consuming, error-prone, and inconvenient.

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.

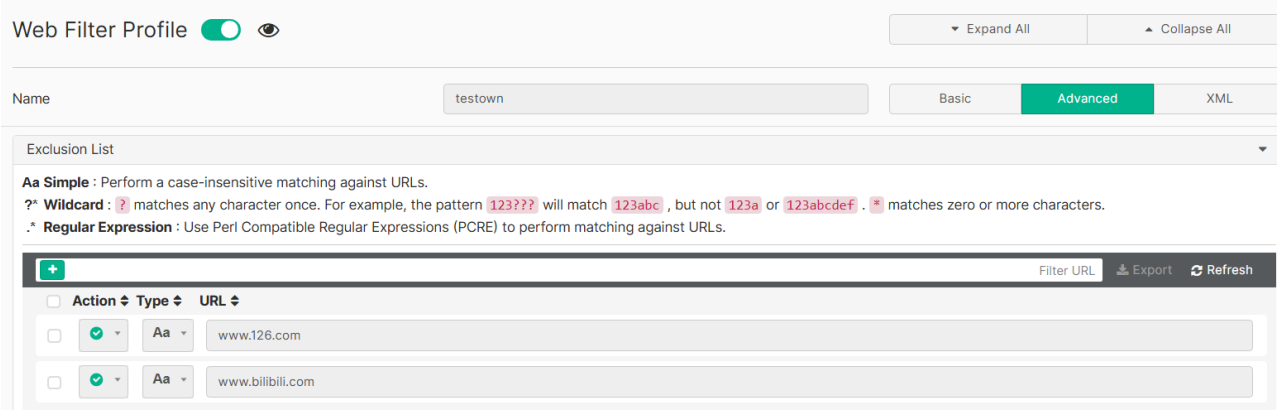


2. Import the profile to EMS and deploy it to endpoints:
   a. In EMS, go to *Endpoint Profiles* > *Web Filter*.
   b. Click *Import* > *Import from FortiGate / FortiManager*.
   c. Configure the FortiGate fields as required, then click *Next*.
   d. Select the desired profile to import. Click *Next*.
   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.

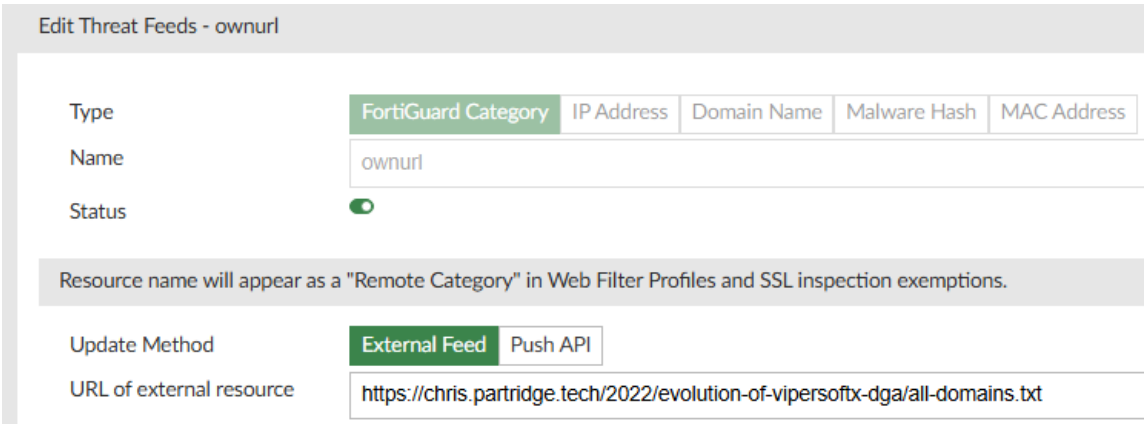
3. On an endpoint that received the updated profile, confirm that FortiClient applies the configured action to a URL in the remote category list. The block page displays the category name.
4. On EMS, in *Endpoints > All Endpoints*, select the endpoint.
5. On the *Web Filter Events* tab, you can view 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.



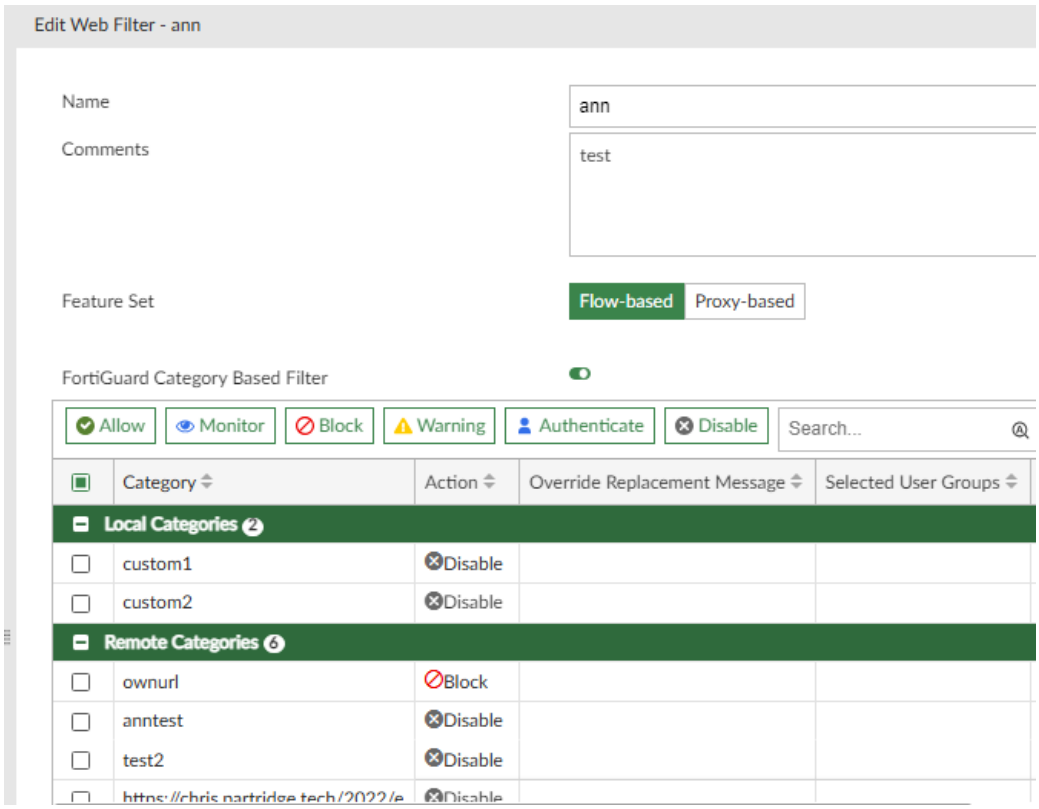
To import a Web Filter profile with remote categories from FortiManager to EMS:

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.

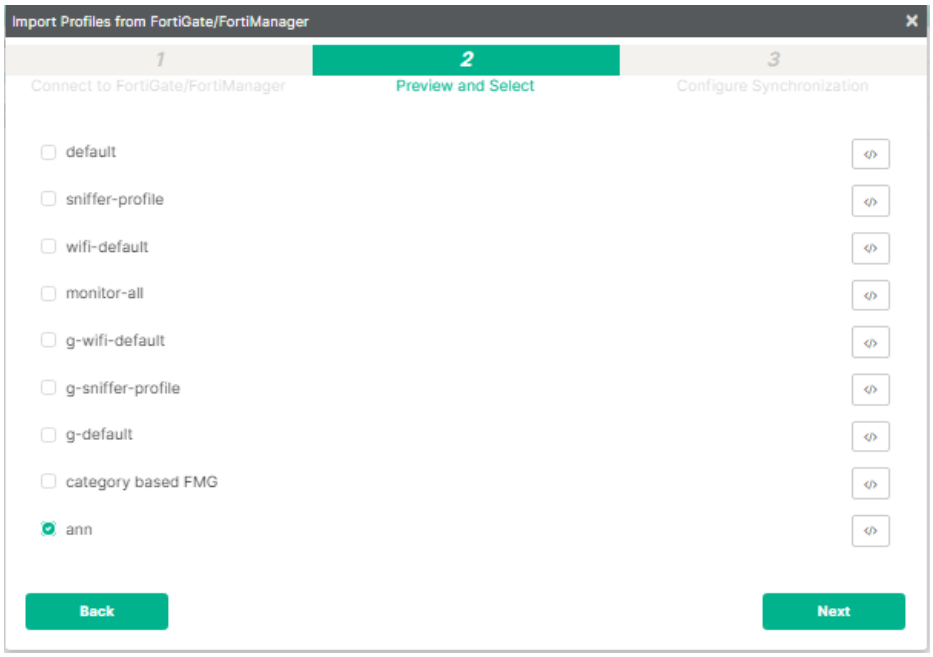
1. In FortiManager, configure the following:
   a. Configure a threat feed as Creating threat feed connectors describes. Use the following values:
      i. For *Type*, select *FortiGuard Category*.
      ii. For *Update Method*, select *External Feed*.
      iii. In the *URL of external resource* field, 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.

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

Configuration	Description
	• 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.
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

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	Run system updates for the underlying operating system (OS): • For an endpoint with Microsoft Windows installed, this option scans for and applies Windows OS patches for security updates. • For an endpoint with macOS installed, this option runs the OS software updates. FortiClient notifies the OS to do these 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.

Configuration	Description
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*.
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.

Configuration		Description
	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 FortiClient EMS is licensed for are available for configuration. See Windows, macOS, and Linux licenses on page 25 for details on which features each license type includes.

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 Windows 10 endpoints. 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.
On Demand Scanning	

Options	Description
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. FortiClient automatically updates antiransomware signatures and engines as available from FortiGuard Distribution Servers.



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 560. • *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*.

Options	Description
	• If the user selects *No*, FortiClient resumes the processes unless the 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 FortiClient EMS 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. FortiClient EMS 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 FortiClient EMS 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. See Windows, macOS, and Linux licenses on page 25 for details on which features each license type includes.

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.

Options	Description
	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. 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 189.
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 189.
Region	FortiClient Cloud Sandbox (SaaS) region. See Configuring FortiGuard Services settings on page 645.
Time Offset	FortiClient Cloud Sandbox (SaaS) time offset. See Configuring FortiGuard Services settings on page 645.
License Status	Displays the Sandbox Cloud license status. Using FortiClient Cloud Sandbox (SaaS) requires an additional license. See FortiClient EMS on page 23.

Options	Description

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*: FortiClient inspects all supported file extensions and sends to FortiSandbox as appropriate. This option is only available for a FortiSandbox appliance.

Options	Description
Excluded File Extensions	Select a file extension to exclude from FortiSandbox scanning. You can select multiple file extensions.
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 • Fortinet

Options	Description
	• 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. FortiClient EMS 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.

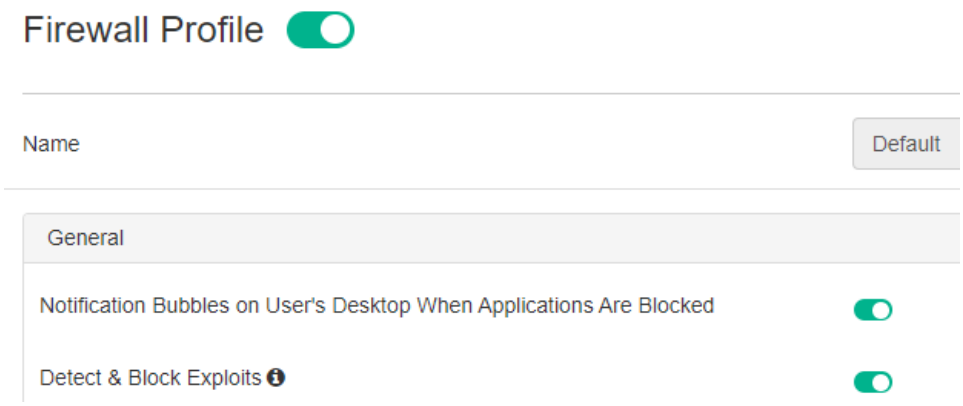
Define exceptions for Firewall Detect & Block Exploits feature

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:

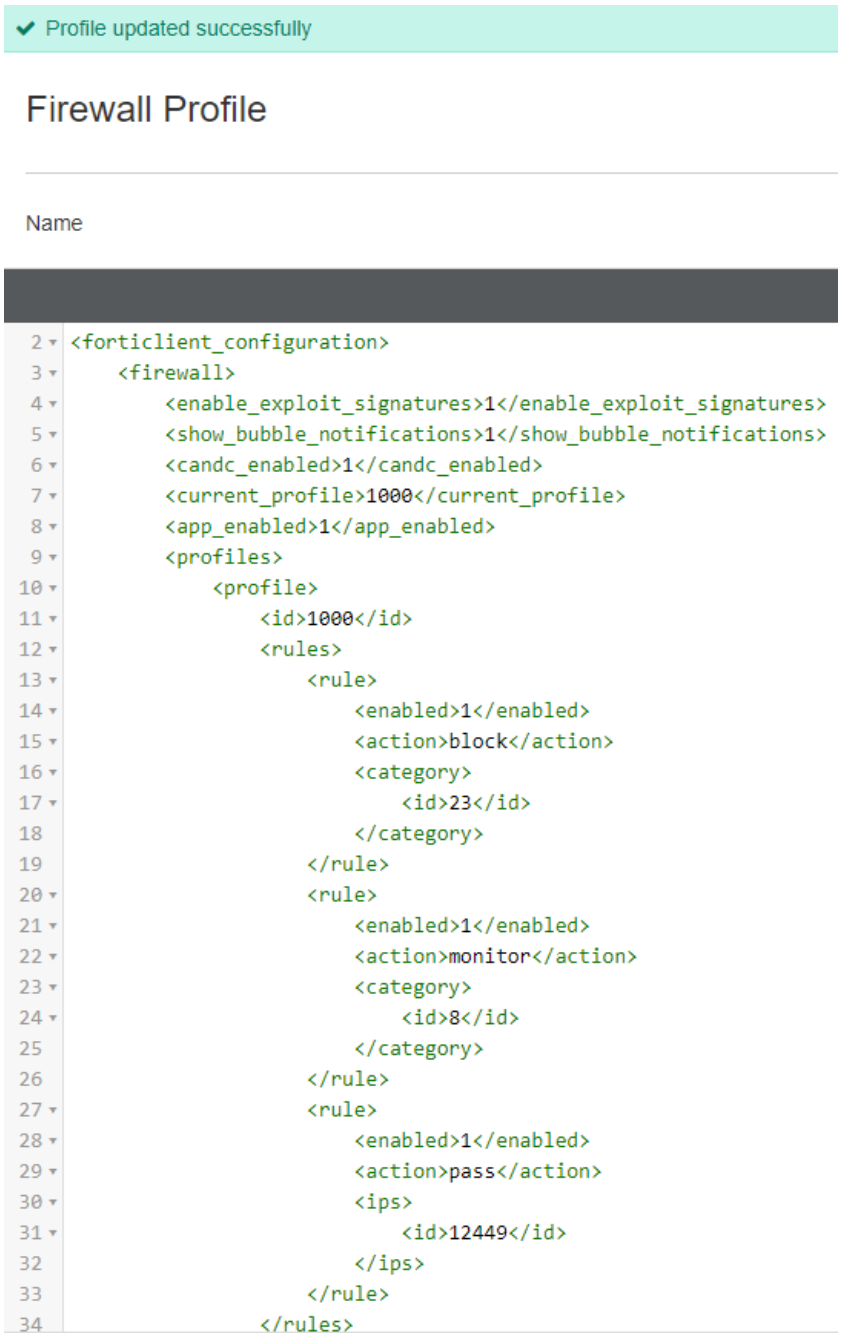
1. In EMS, go to *Endpoint Profiles* > *Firewall*.
2. Under *General*, enable *Detect & Block Exploits*.



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>
```




```
<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>
```

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.

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 FortiClient EMS.
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.
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 495.

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: • AntiVirus • Application Firewall • Telemetry • FSSOMA • Proxy • IPsec VPN • AntiExploit • SSL VPN • Update • Vulnerability • Web Filter • Sandbox
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 248.
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.

Configuration		Description
		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.
	Upload UTM Logs	Upload unified threat management (traffic) 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.
	Upload Vulnerability Logs	Upload vulnerability logs to FortiAnalyzer or FortiManager.
	Upload Event Logs	Upload event logs to FortiAnalyzer or FortiManager.
	Send Software Inventory	EMS sends FortiClient software inventory to FortiAnalyzer or FortiManager. This feature requires the EPP license. See FortiClient EMS on page 23.
	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.
	IP Address/Hostname	Enter the FortiAnalyzer IP address or hostname/FQDN. With Chromebook profiles, use the format *https://FAZ-IP:port/logging*. If using a port other than the default, use <address>:<port>.

Configuration		Description
		For FortiAnalyzer Cloud, you must enter an FQDN. You cannot enter an IP address. For FortiAnalyzer Cloud, the FQDN is the URL that you use to access the FortiAnalyzer Cloud instance. For example, the FQDN may be 1208151.ca-west-1.fortianalyzer.forticloud.com. You may also need to configure the server name indication. See Log settings.
	SSL Enabled	Enable SSL.
	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.
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.

Configuration		Description
Use FortiManager for Client Signature Update		Enable FortiClient EMS 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.
		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 FortiClient EMS.
On-Fabric Subnets		Turn on to enable on-fabric subnets.

Configuration		Description
		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 248.
	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 FortiClient EMS. 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 532. This feature requires the EPP license. See FortiClient EMS on page 23.
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. • **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 201.
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:

Configuration	Description

	• 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. You can add certificates by going to *Endpoint Policy & Components > CA Certificates*. See CA Certificates on page 246. 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.

Configuration		Description
	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.
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:

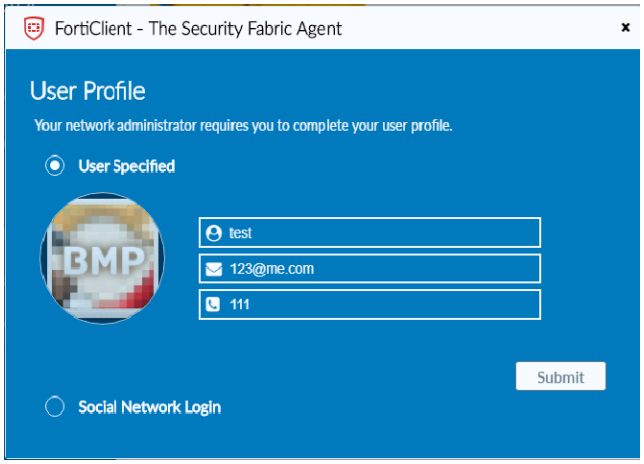
- User input
- OS
- LinkedIn
- Google
- Salesforce

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.

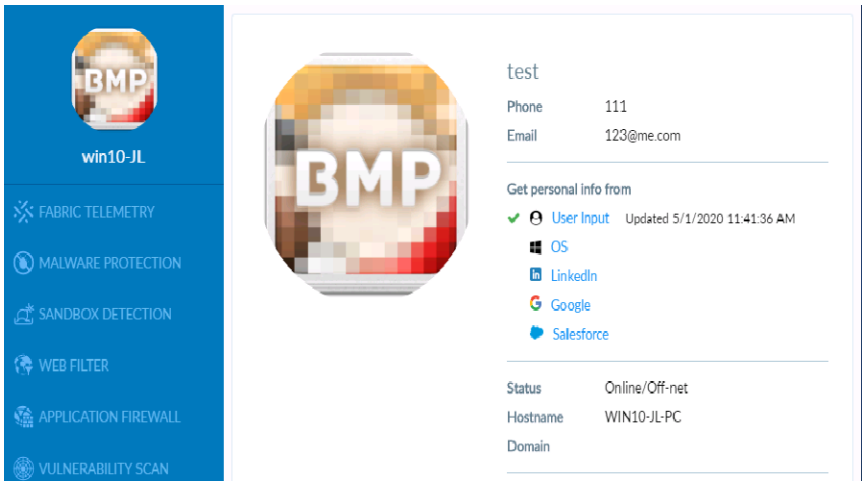
To configure identity compliance:

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*.

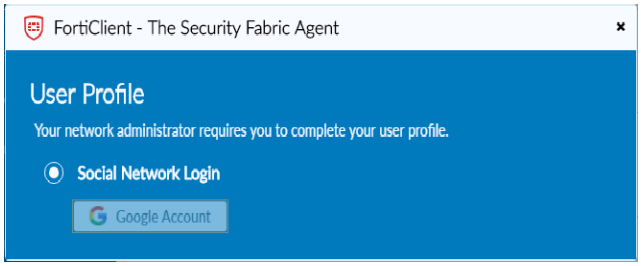
When *Notify Users to Submit User Identity Information* is enabled, the user sees the following notification on the endpoint. If *Manually Enter User Details* is enabled, the user can enter their information manually.



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 476.
- 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 478.
- 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 479.

This document also describes the following use cases:

- To configure a secret for SSH to a FortiGate: on page 479
- To use a secret to log in to a website: on page 481

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
```

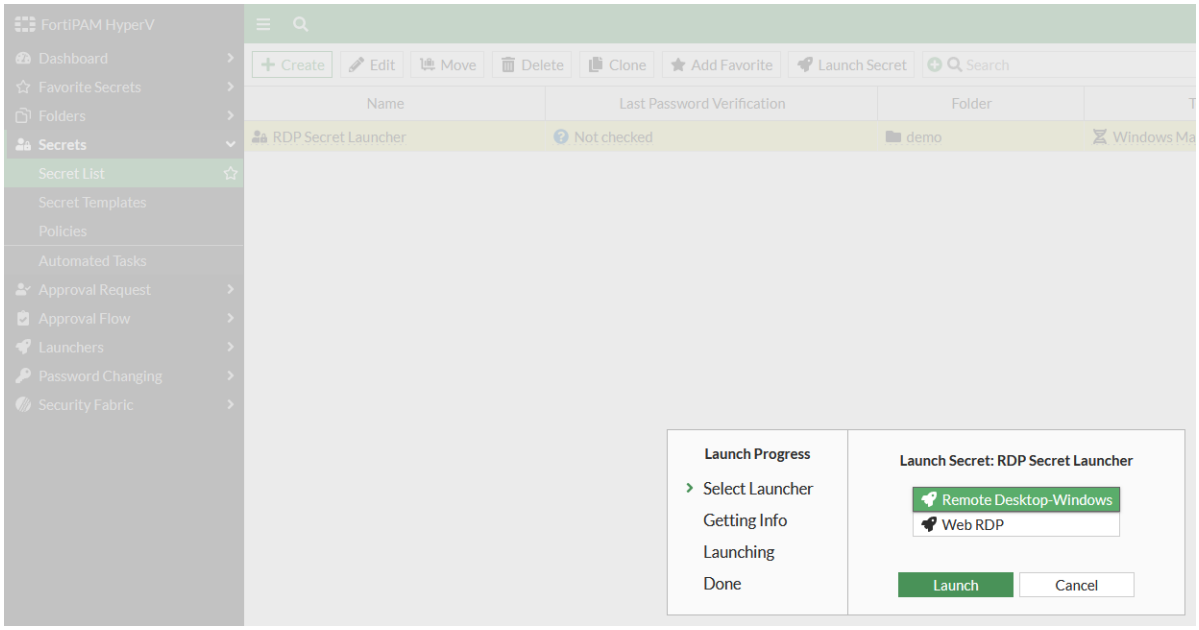
To enable the FortiPAM feature in EMS:

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:

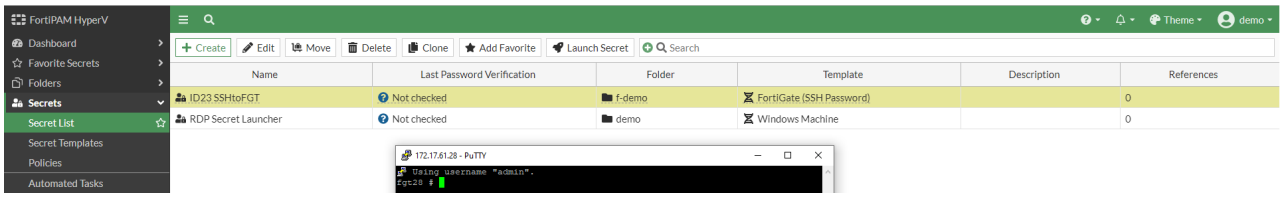
1. Install PuTTY on the client machine.
2. Install FortiClient on the endpoint. The FortiPAM feature must be enabled.
3. Register FortiClient to EMS. Ensure that the profile assigned to the endpoint has the FortiPAM feature enabled.
4. Log in to FortiPAM as the administrator. Add the SSH secret:
   a. 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 481, 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:

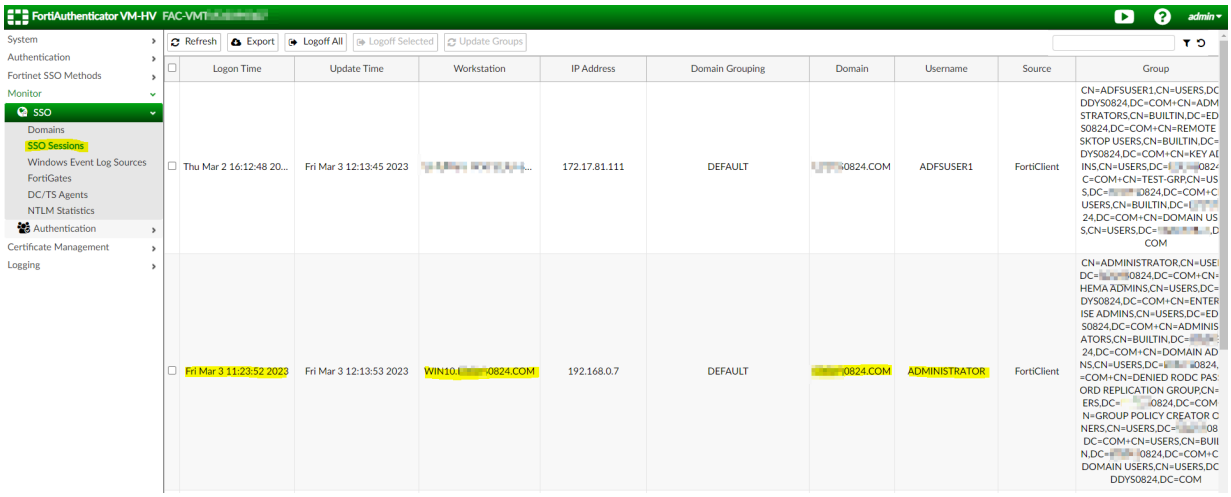
- **Method 1:** Install FortiPAM, export and edit the configuration file to include the SSOMA configuration, and reimport the configuration file.
- **Method 2:** Install and run the SSO configuration tool file to create new installer files, and run the installers to install or upgrade the FortiClient PAM agent.

To use Method 1:

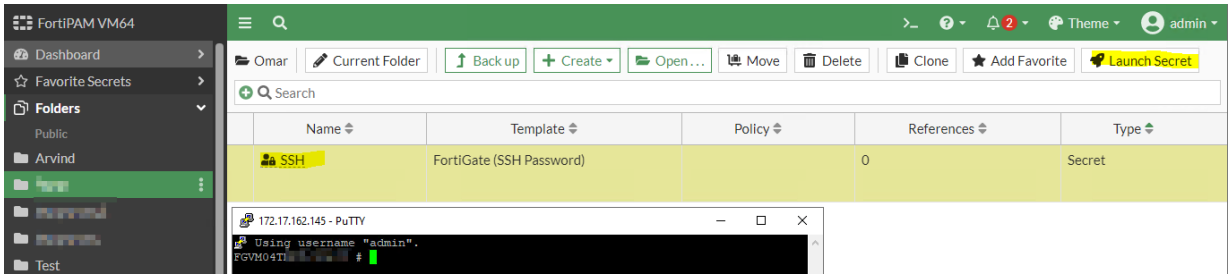
1. Install FortiPAM using an installer.
2. In Command Prompt, go to the FortiClient directory.
3. Export the configuration file using the following command: `FCConfig.exe -o export -f C:\config.conf -p 11111111`
4. Edit the configuration file and add the SSOMA configuration. Confirm that the FortiPAM 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.

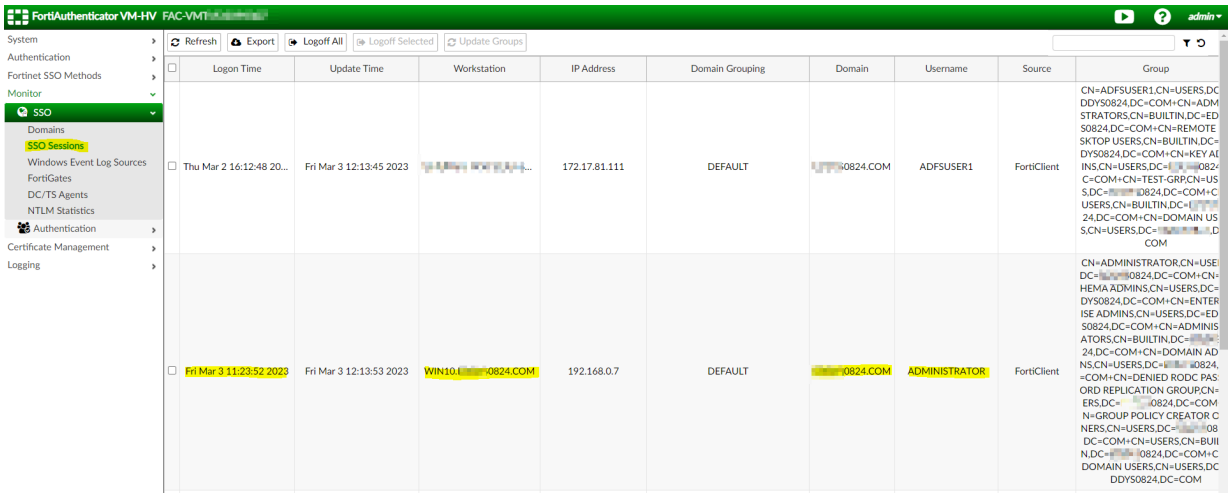


c. In FortiPAM, confirm that you can access a secret created in FortiPAM.

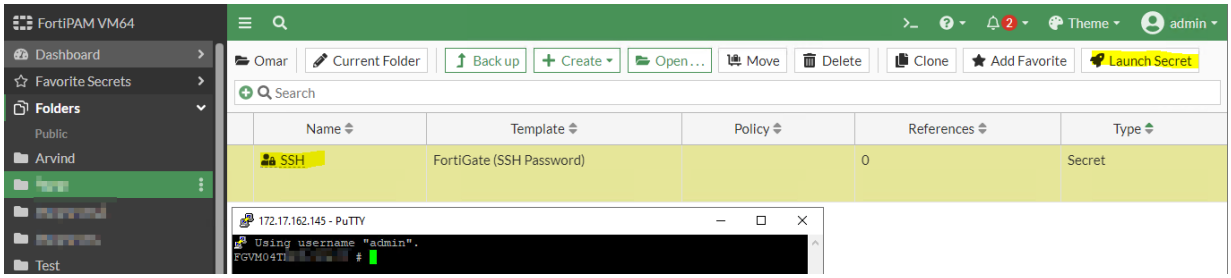


To use Method 2:

1. Acquire and unzip the FortiClientSSOConfigurationTool_7.2.1.XXXX.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:

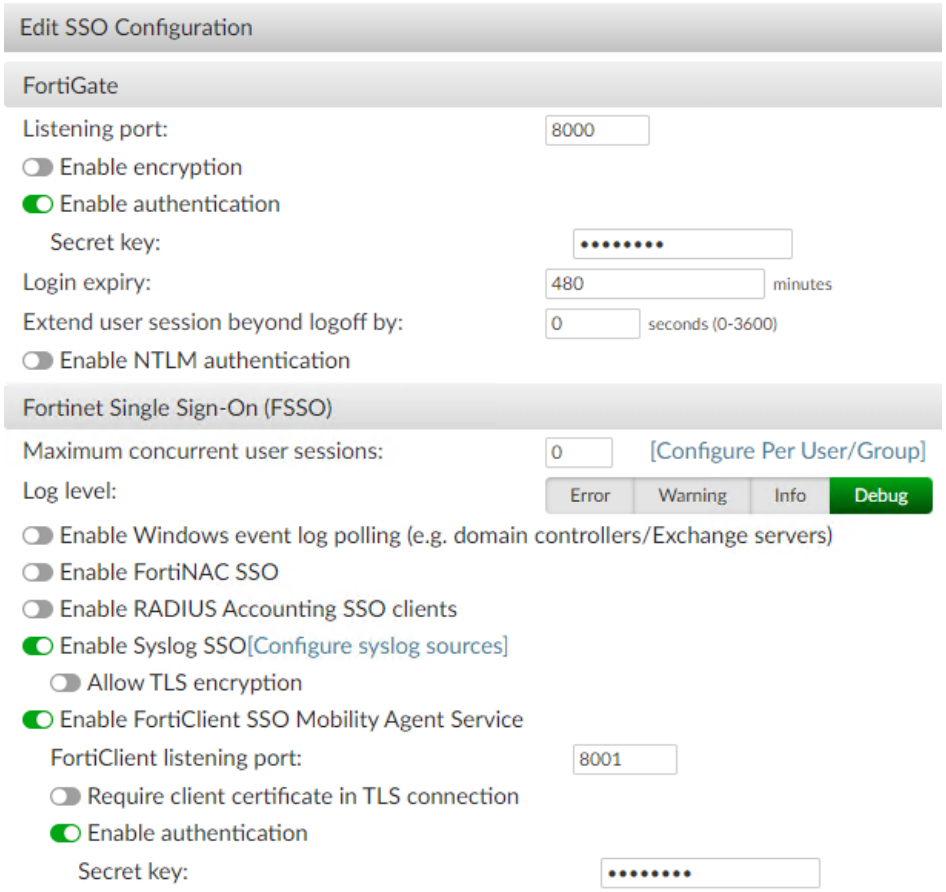
- Support for pure Microsoft Entra ID (formerly known as Azure Active Directory (AD)) mode. SSOMA sends the Entra ID domain and tenant ID to FortiAuthenticator in pure/native Entra ID mode.
- Sends FortiClient UUID and EMS serial number/tenant ID to FortiAuthenticator.
- Sets the SNI field when communicating 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.

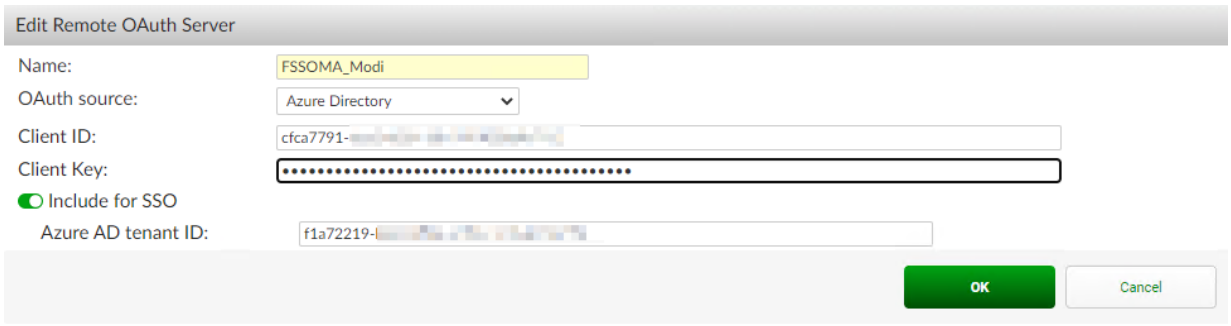
d. Set the newly created enterprise application as a directory reader:
   i. Go to *Home > Manage Azure Active Directory > View button > Manage > Roles and Administrators*.
   ii. In the *Administrative Roles* list, search for and select *Directory Readers*.
   iii. Add *Assignments* > Search for the 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 FortiClient EMS 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*.

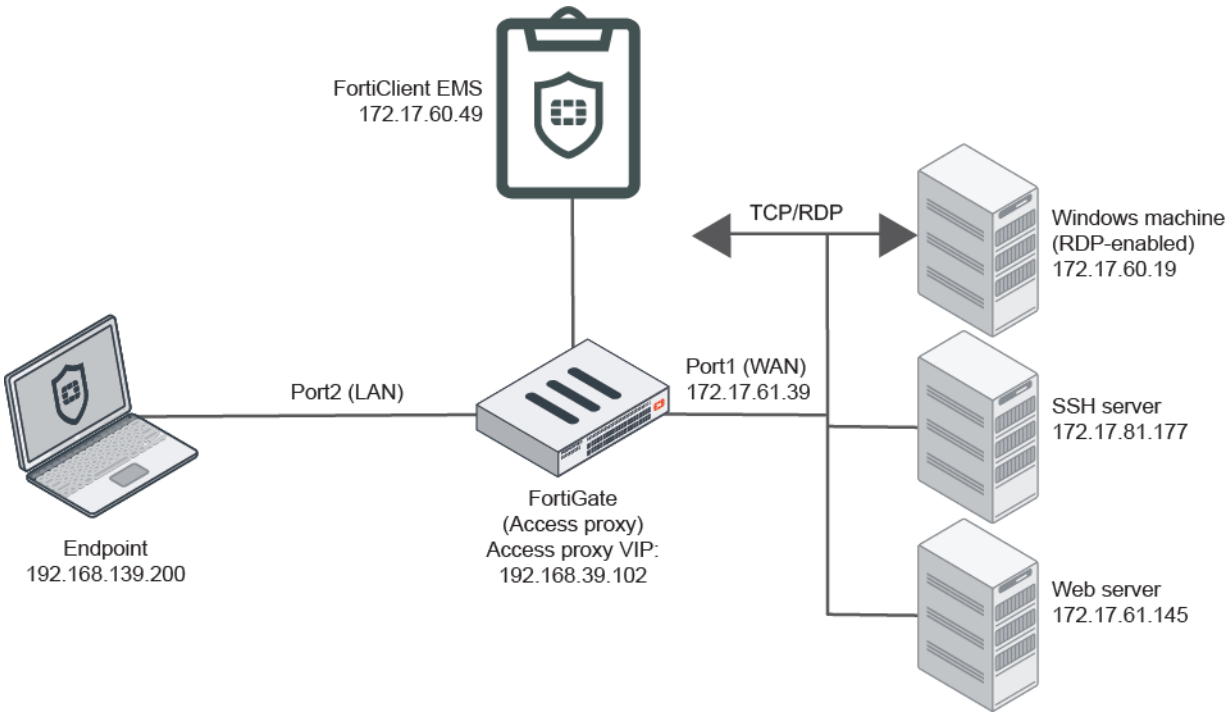
If the profile has a feature enabled that is disabled in Feature Select, EMS displays a warning that the feature is disabled on endpoints that the profile is deployed to. To enable this feature on the endpoint, you must enable the feature in Feature Select. See Feature Select on page 655.

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:

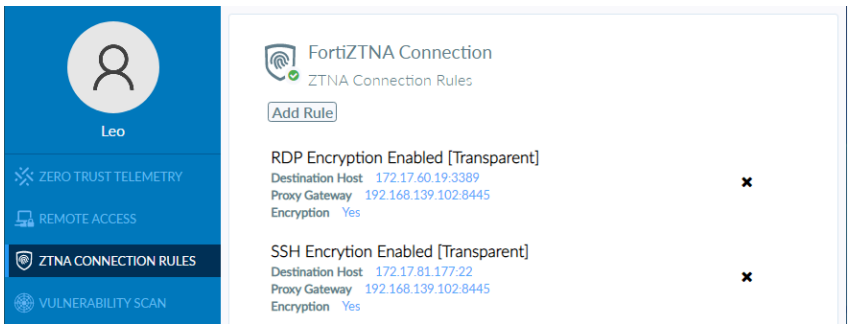
```
<ztna>
   <enabled>1</enabled>
   <rules>
      <rule>
         <name>RDP Forwarding</name>
         <destination>172.17.60.19:3389</destination>
         <gateway>192.168.139.102:8445</gateway>
         <encryption>1</encryption>
         <mode>transparent</mode>
```

```
        </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:

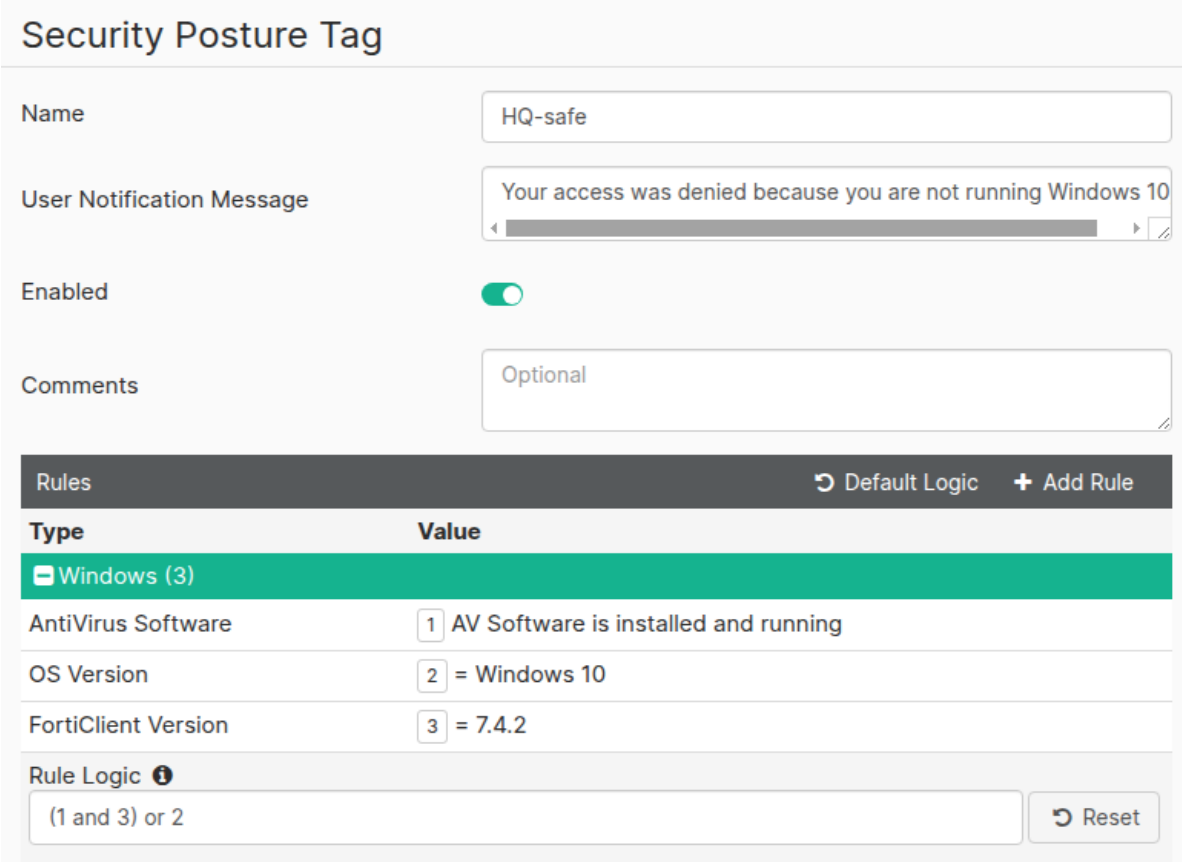
1. EMS sends security posture tags and rules to endpoints via Telemetry communication.
2. FortiClient checks endpoints using the provided rules and sends the results to EMS. When endpoint network changes or user logon and logoff events occur, FortiClient triggers an X-FFCK-TAG message to EMS, even if 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 629.
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 507.

Adding a security posture tag

To add a security posture tag:

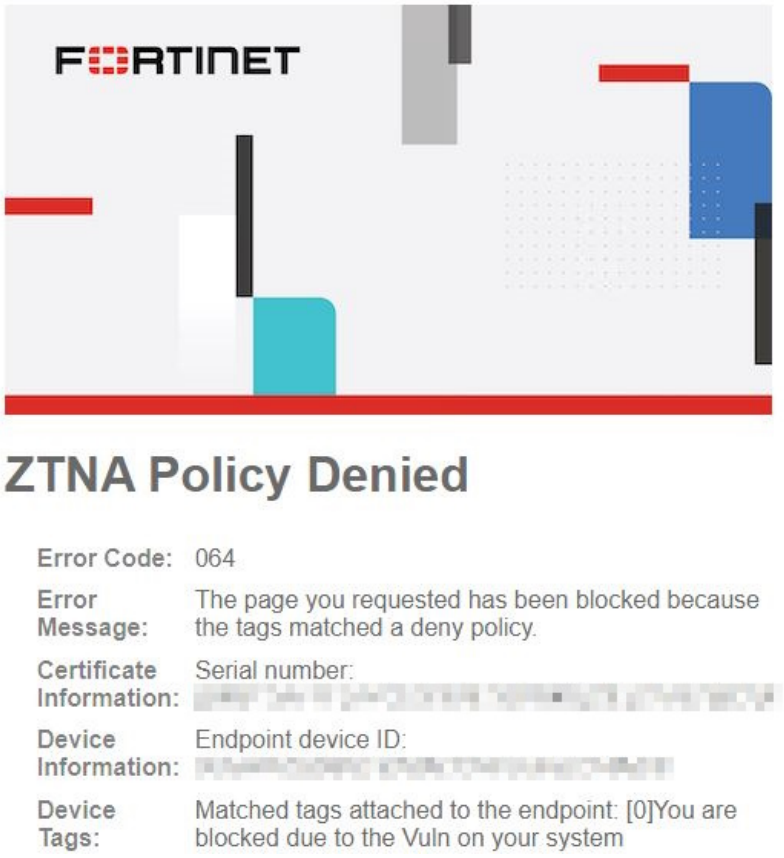
1. Go to *Security Posture Tags* > *Tags*, and click *Create*.
2. In the *Name* field, enter the desired tag name.
3. In the *User Notification Message* field, enter a message that explains to the end user why FortiOS denied their access. In FortiOS in *Policy & Objects* > *ZTNA* > *Security Posture 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 500 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 77.4.3. 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:

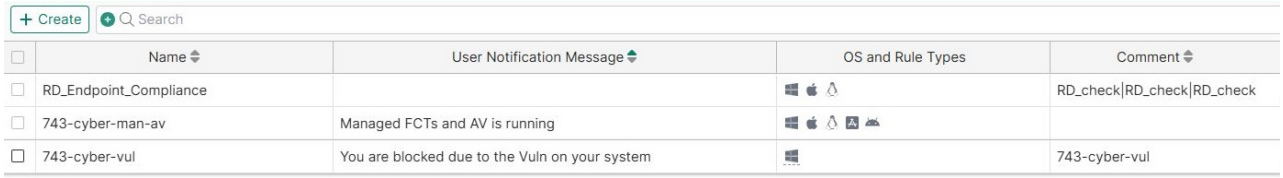
1. If importing a tag set from an older EMS version, in the older EMS version, go to *Security Posture Tags* > *Security Posture Tagging Rules*.
2. Click *Export*.



3. In EMS 7.4.3, 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

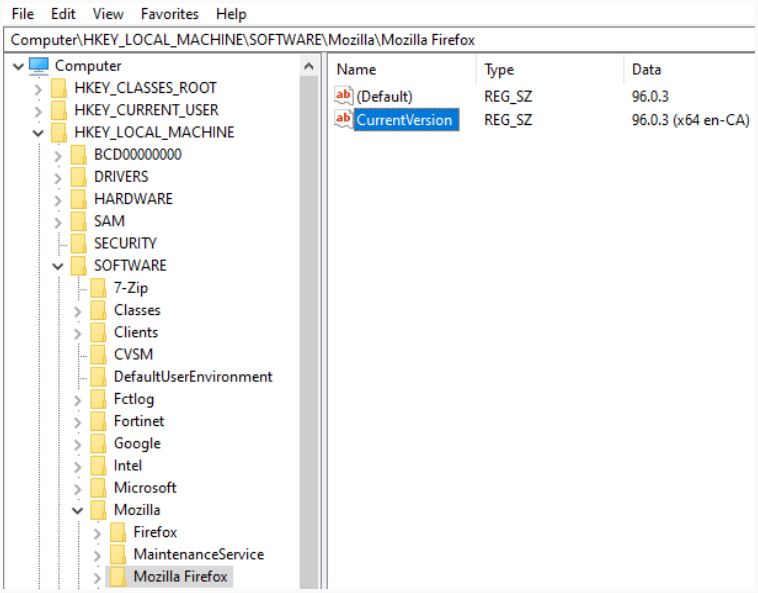
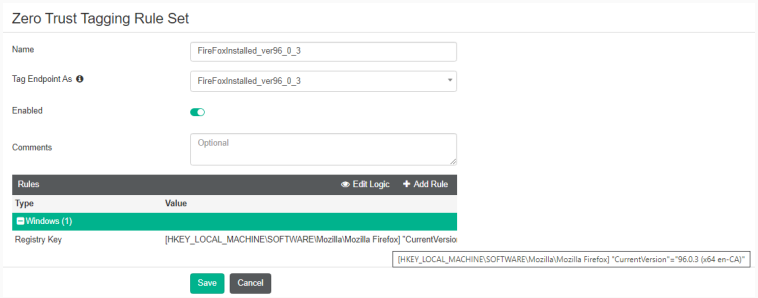
The following table describes security posture tagging rule types and the operating systems (OS) that they are available for. For all rule types, you can configure multiple conditions using *+*.

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.

Rule type	OS	Description
		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. 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. 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.

Rule type	OS	Description
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.
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. If the rule is configured for multiple domains, EMS considers the endpoint as satisfying the rule if it 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.

Rule type	OS	Description
		• *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.
Registry Key	• Windows	In the *Key* field, enter the registry path or value name enclosed in square brackets [ ]. End the path with \ to indicate a registry path, or without \ to indicate a registry value name. In the *Key Name* field, enter the registry key name, enclosed in double quotation marks "". From the dropdown list, select the desired comparator. In the *Value* field, enter the desired key value. For a dword key value, enter the value as dword:<value>. For example, if the dword key value is 1, enter dword:1 in the *Value* field. For a non-dword key value, enter the value enclosed in double quotation marks "". You can also use the NOT option to indicate that the rule requires that a certain registry path or value name is not as configured in the rule. For example, the following shows a system where Firefox is installed. In this example, the registry path is `HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox`. The value name is `CurrentVersion`, and the value data is `96.0.3 (x64 en-CA)`. You can configure a registry key rule to match `HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox` as the path, `CurrentVersion` as the registry value name, or the value data as `96.0.3 (x64 en-CA)`. The example shown configures a rule to match the value data as `96.0.3 (x64 en-CA)`. Note the configured rule includes square brackets around the registry path, and double quotation marks around the key name and value.

Rule type	OS	Description
		  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.
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.
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.

Rule type	OS	Description
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 594.
		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. By default, EMS performs AD group lookup, which is considered more efficient and prevents the issue where an endpoint loses all AD-related tags when it goes offline. You can also configure FortiClient to perform AD group lookup instead by enabling *Evaluate on FortiClient*. 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. You can 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 173. 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 inappropriately decommissioned computers. BitLocker enhances file and system protections and helps render data inaccessible when

Rule type	OS	Description
		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 495.
FortiGuard outbreak alert tags	See FortiGuard Outbreak Alerts on page 530.
Classification tags	See Viewing the Endpoints pane on page 176.
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 465.

Tag	Description
	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 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 176. 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 FortiClient EMS 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 514 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 *FortiClient EMS 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 509
2. Configuring the EMS connector on page 510:
   a. Uploading certificates to EMS and FortiOS on page 510
   b. Creating the EMS connector in FortiOS on page 510
   c. Authorizing the FortiOS EMS connector in EMS on page 511
   d. Verifying the FortiOS-EMS connection in FortiOS on page 512
3. Creating an address group for the security posture tags on page 512
4. Creating a dynamic firewall policy using security posture tags from EMS on page 513



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 496.
- After FortiClient connects Telemetry to EMS, confirm that EMS dynamically tags endpoints based on the security posture tagging rules. See Tag Monitor on page 507.
- 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.

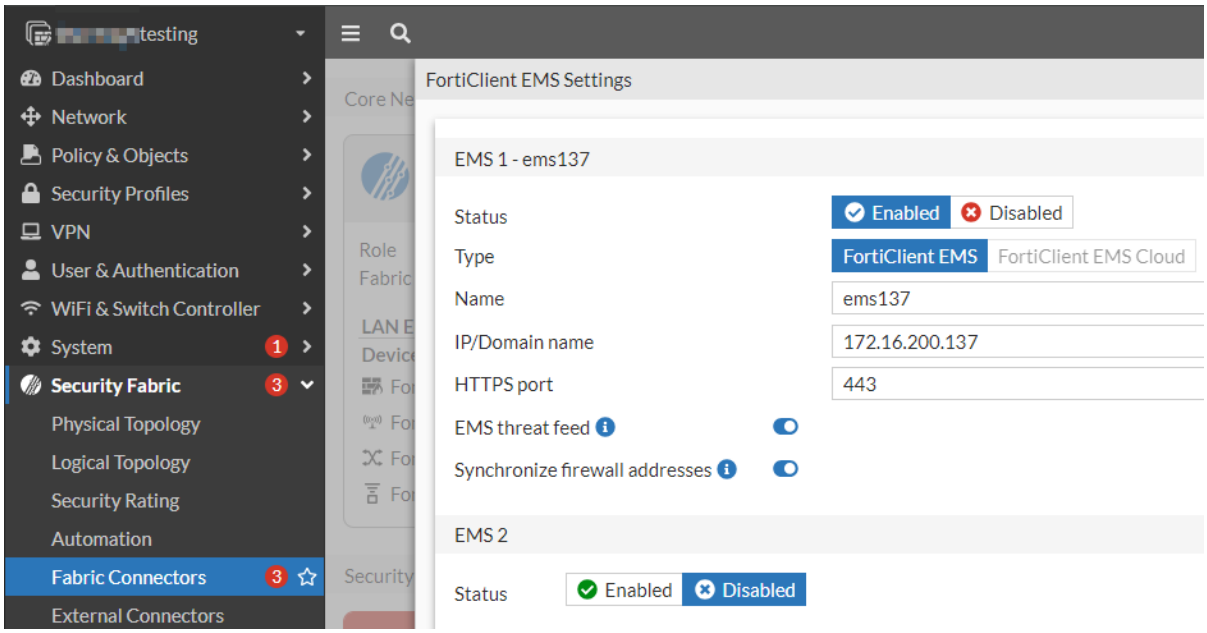
1. Configure the server certificate in EMS:
   a. Go to *System Settings > EMS Server Certificates*.
   b. Click *Add*.
   c. Configure the certificate as desired.
   d. Go to *System Settings > EMS Settings*.
   e. Under *Shared Settings*, from the *Webserver certificate* dropdown list, select the configured 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 *FortiClient EMS*.
5. In the *Name* field, enter the desired name.
6. In the *IP/Domain name* field, enter the EMS IP address or domain name. If EMS multitenancy is enabled, you must enter the FQDN instead of the IP address. You must enter the FQDN in the format site.fqdn to integrate the FortiGate to the specific EMS multitenancy site. For example, if the site name is sitea, enter sitea.ems.example.com. See Multitenancy on page 661.
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:

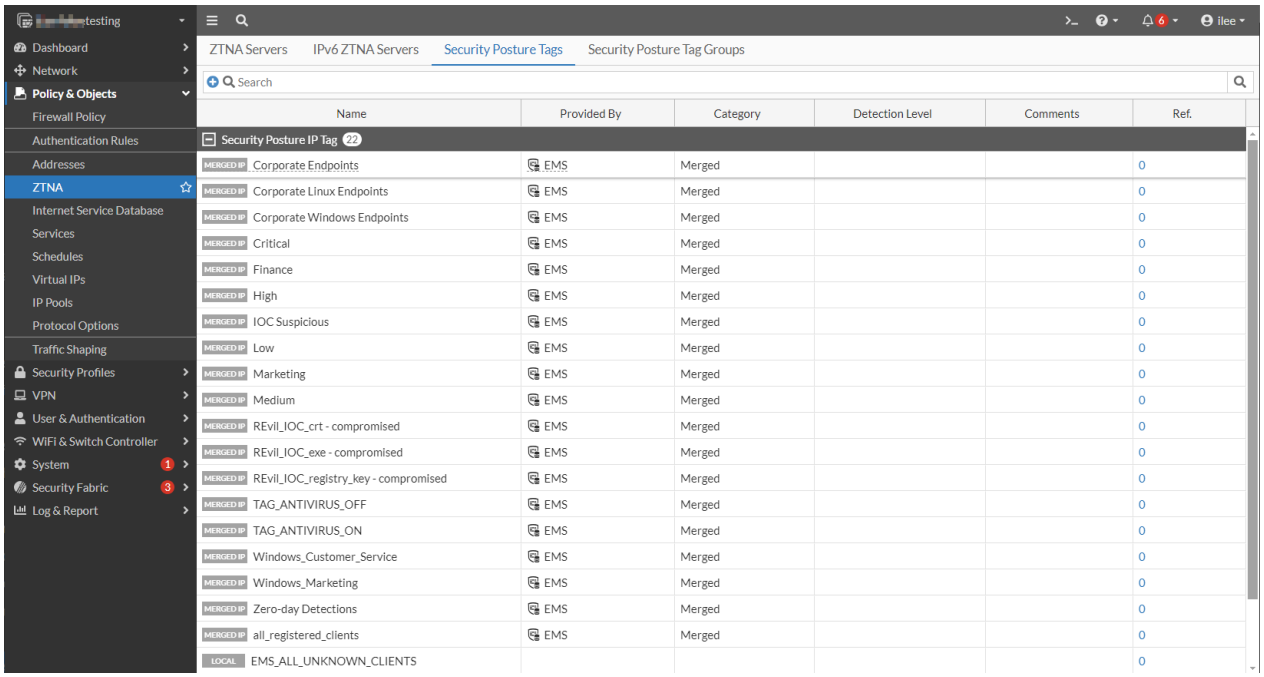
- Log in to EMS. A prompt displays to authorize the FortiGate. Click *Authorize*.
- Go to *Fabric & Connectors* > *Fabric Devices*. Select the desired FortiGate, then click *Authorize*.

You can view all FortiGates that the EMS authorized in *Fabric & Connectors* > *Fabric Devices*. See Fabric Devices on page 514.

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 508.

For each connected FortiGate, you can view the following information:

- Serial number
- IP address
- FortiOS version installed
- Last sync time between FortiClient EMS and the FortiGate
- Dynamic endpoint groups shared with the FortiGate and the number of endpoints in each group

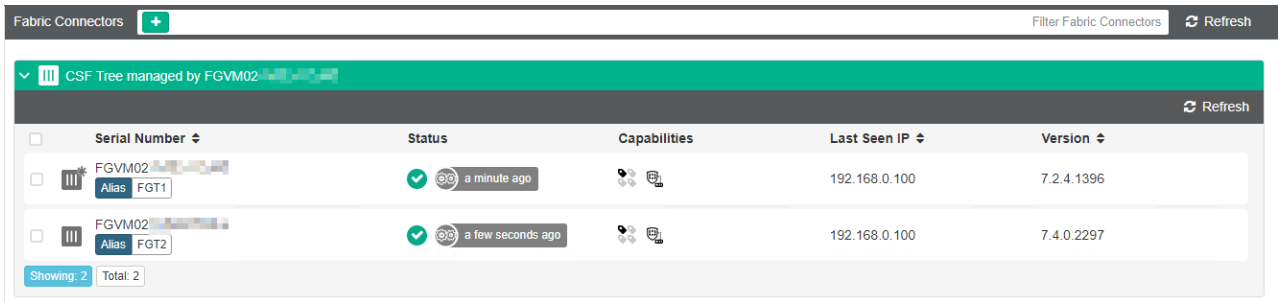
Fabric & Connectors

In *Fabric & Connectors*, you can access *Fabric Devices* to view all FortiGates that the EMS has authorized. You can also go to *ZTNA Applications Catalog* to add a zero trust network access (ZTNA) application or view a ZTNA application that EMS retrieved from FortiOS 7.4.4 and later versions.

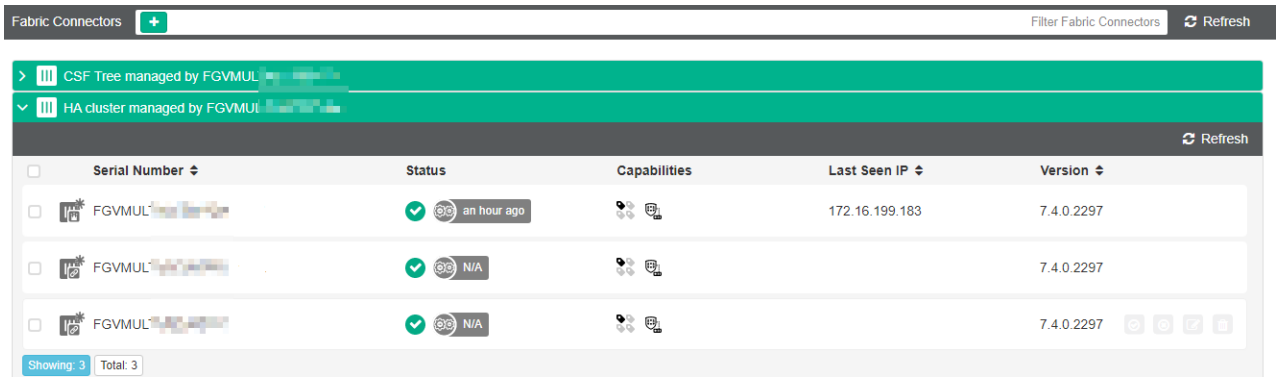
Fabric Devices

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 495.
FortiGuard outbreak alert tags	See FortiGuard Outbreak Alerts on page 530.
Classification tags	See Viewing the Endpoints pane on page 176.
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 465. 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 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 176. 7. If FortiGate is configured to receive all tags for this specific endpoint, EMS sends the tag to FortiGate.

Tag	Description
	See EMS API support for FortiAnalyzer to notify and tag suspicious endpoints.

5. Click *Save*.

To change the FortiGate authorization status:

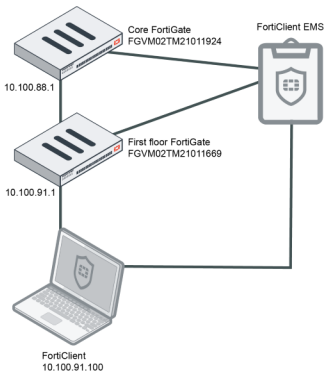
1. Go to *Fabric & Connectors* > *Fabric Devices*.
2. Select the desired FortiGate.
3. Click *Deny* or *Authorize*. The FortiGate status in the *Authorized* column changes.

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:

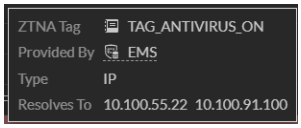
- Both FortiGates are connected to EMS as part of a Security Fabric.
- FortiClient is registered to EMS.
- The FortiClient gateway points to the first floor FortiGate.
- The FortiClient endpoint has the TAG_ANTIVIRUS_ON security posture tag applied.
- The host tag of the FortiClient endpoint with TAG_ANTIVIRUS_ON 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

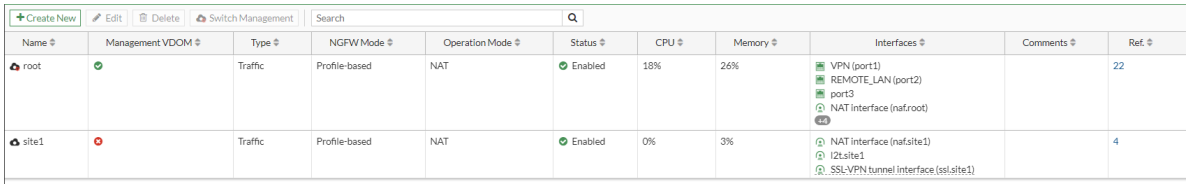
Each FortiOS virtual domain (VDOM) can connect to a separate EMS or EMS multitenancy site. This provides EMS with the ability to only send FortiClient and tagging information to a single FortiOS VDOM.

This feature requires FortiOS 7.4.

To configure EMS support for FortiGate per-VDOM connection:

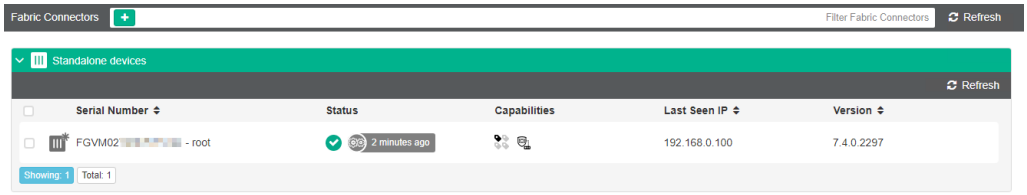
1. In FortiOS, enable the VDOM feature by doing one of the following:
   a. Go to *System* > *VDOM* and create a new site.
   b. Run the following commands:

```
config system global
   set vdom-mode multi-vdom
end
```



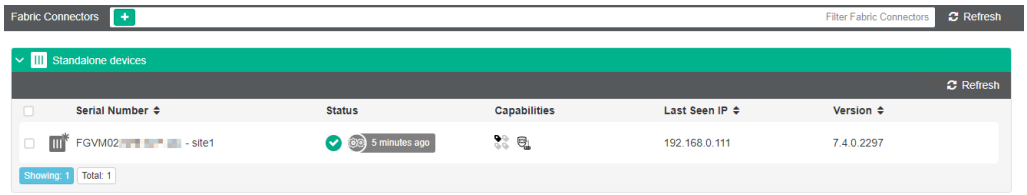
2. In EMS, enable multitenancy. Create a new multitenancy site.
3. Configure a Fortinet Security Fabric connection from the FortiGate root VDOM to the EMS default site. Once connected, the EMS default site shows the FortiGate root VDOM in *Fabric & Connectors > Fabric Devices* in <FortiGate serial number> - <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
```

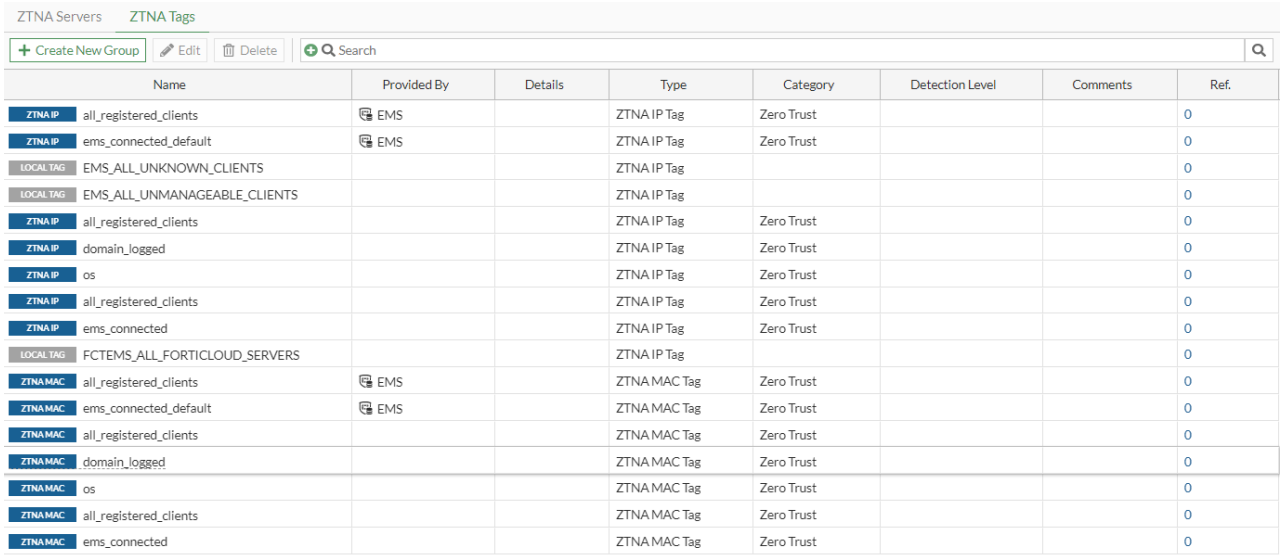


4. Configure a Fabric connection from the FortiGate non-root VDOM to the EMS non-default site. Once connected, the EMS non-default site shows the FortiGate non-root VDOM in *Fabric & Connectors > Fabric Devices* in <FortiGate serial number> - <VDOM name> format:

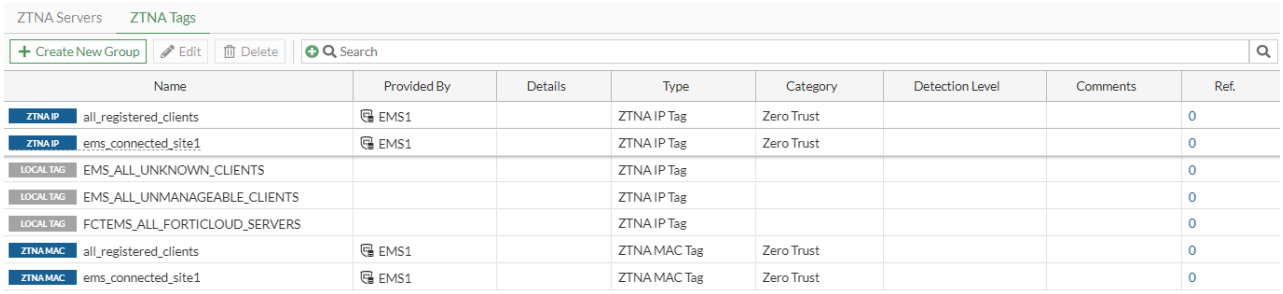
```
config vdom
edit site1
config endpoint-control settings
    set override enable
end
config endpoint-control fctems-override
    edit 1
        set status enable
        set name "ems_site1"
        set server "site1.ems1.fortitest.ca"
    next
end
```



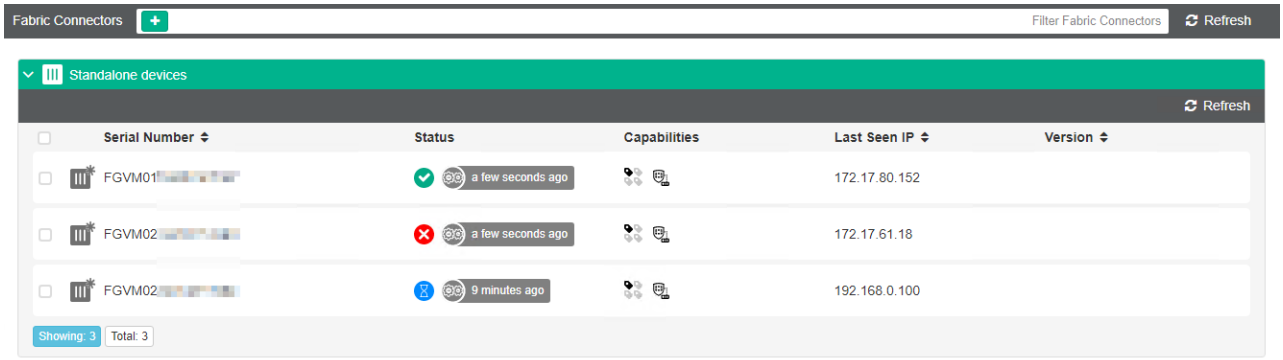
5. Tagging information from an EMS site is only shared with the FortiGate VDOM that the EMS site has established a Fabric connection with. In this example, the ems_connected_default site is a tag configured on the EMS default site.



ems_connected_site1 is a tag configured on the EMS non-default site.



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

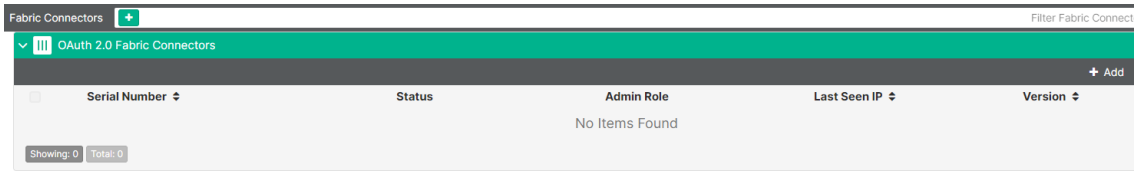
EMS supports a connector type that uses OAuth 2.0 token-based authentication. When you create an OAuth 2.0 connector, EMS generates a client ID and secret to for the Fortinet product on the other side of

the connector to use. You can integrate EMS with the following Fortinet products:

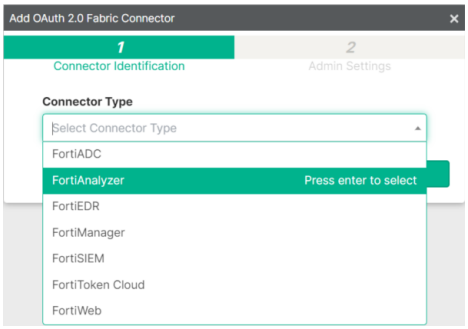
- FortiADC
- FortiAnalyzer
- FortiEDR
- FortiManager
- FortiSIEM
- FortiToken Cloud
- FortiWeb

To create a connector with OAuth 2.0 token-based authentication:

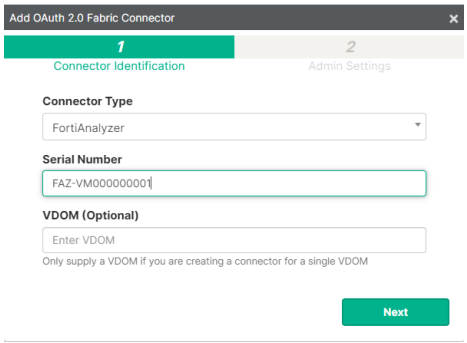
1. Go to *Fabric & Connectors* > *Fabric Devices*.



2. Click *Add*. The *Add OAuth 2.0 Fabric Connector* dialog displays.
3. Configure the connector:
   a. From the *Connector Type* dropdown list, select the desired Fortinet product to configure the integration for.

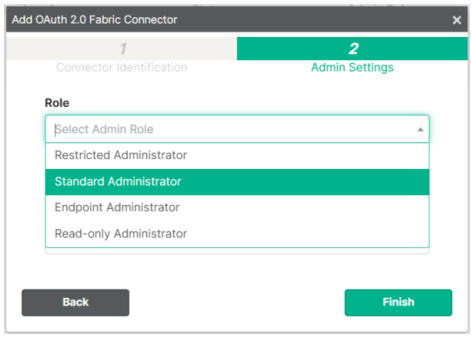


   b. Enter the device *Serial Number*.

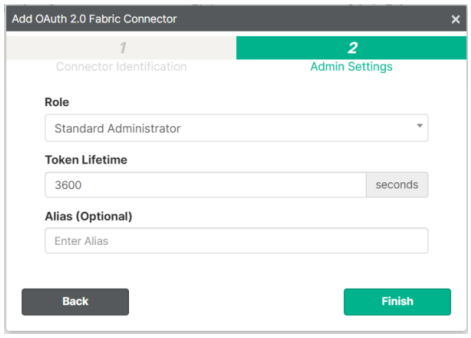


   c. Enter the *VDOM* name if desired. Click *Next*.
   d. Select the *Role*. The EMS admin role selected defines which EMS APIs (and therefore, features) that the Fabric device connector can access. For example, a Fabric connector that is configured with the standard administrator role can access EMS APIs for endpoint and policy permissions and has

read-only permissions to settings permissions. See Admin roles on page 567.

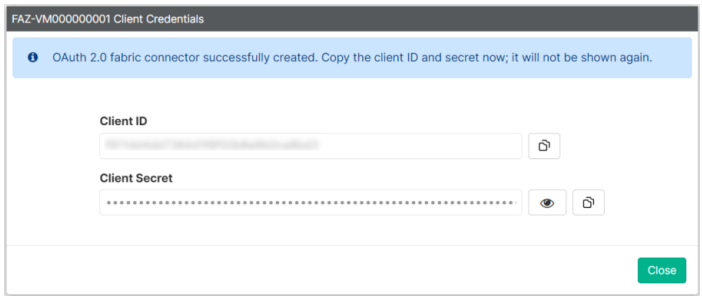


e. Enter the desired *Token Lifetime* value in seconds. After the configured amount of time passes, the token cannot be authorized. The default value is 3600 seconds and the minimum value is 60 seconds.

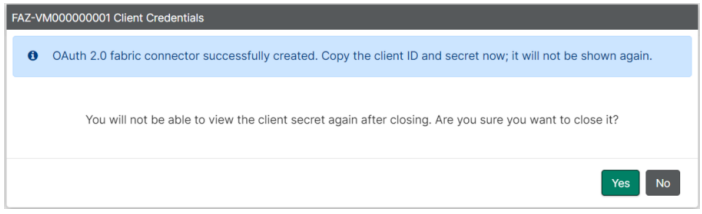


f. Enter the *Alias*, if desired.

g. Click *Finish*. EMS generates the *Client ID* and *Client Secret*.



h. Copy the *Client ID* and *Client Secret*. Click *Close*. A confirmation dialog displays.



i. Click *Yes*. Other Fortinet devices that support OAuth 2.0 Fabric connector features can use the *Client ID* and *Client Secret* to call EMS APIs.

Matched endpoints and resolved addresses

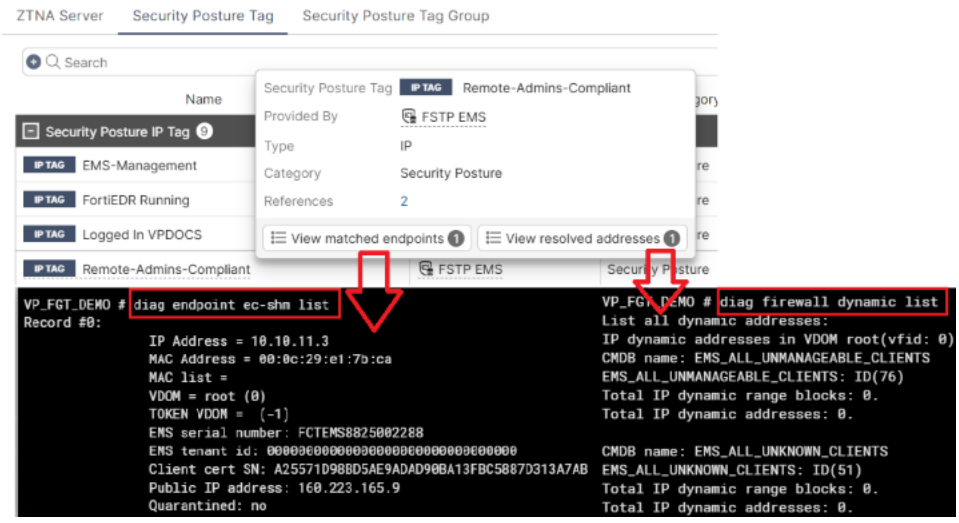
This document clarifies what matched endpoints and resolved addresses are and how they are populated.

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 shown under *Resolved addresses* in the FortiOS GUI are 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. Refer to 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, the *Resolved addresses* table is not populated with the endpoint's IP or MAC address.

Resolved addresses only applies to IP/MAC access control on page 523 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

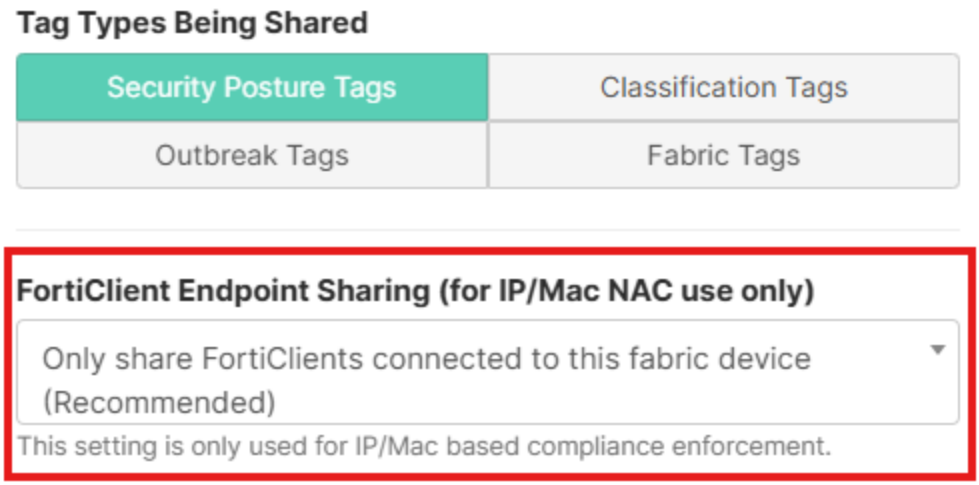
When an endpoint's gateway address points to the FortiGate or FortiClient performs direct VPN connection to it, the FortClient's address shows in the *Resolved addresses*. For a directly connected client, the endpoint's MAC and IP addresses are populated. For a VPN-connected client, only the IP address is populated.

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.

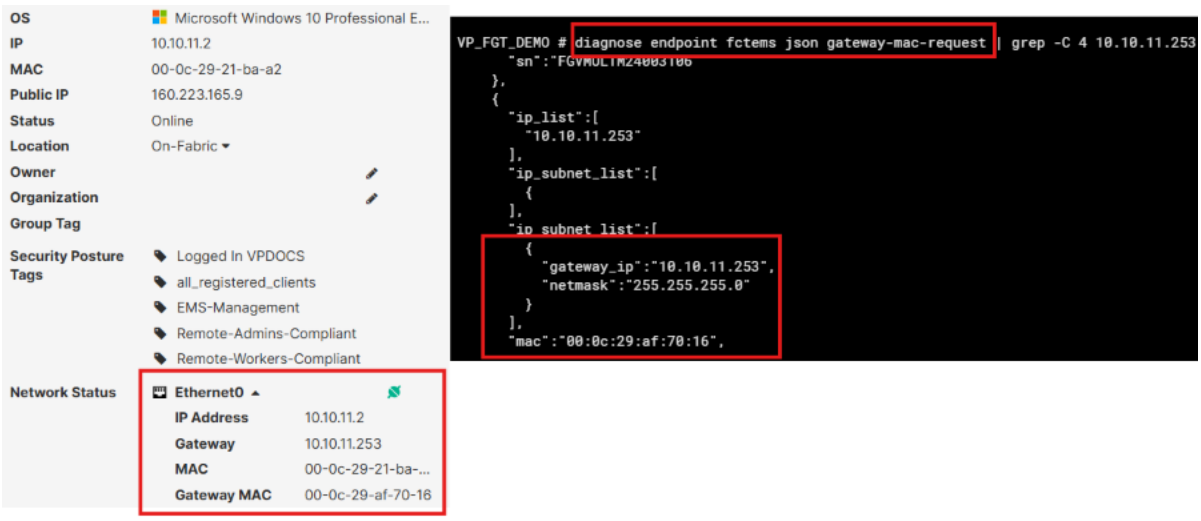
Only share FortiClients connected to this fabric device

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*.

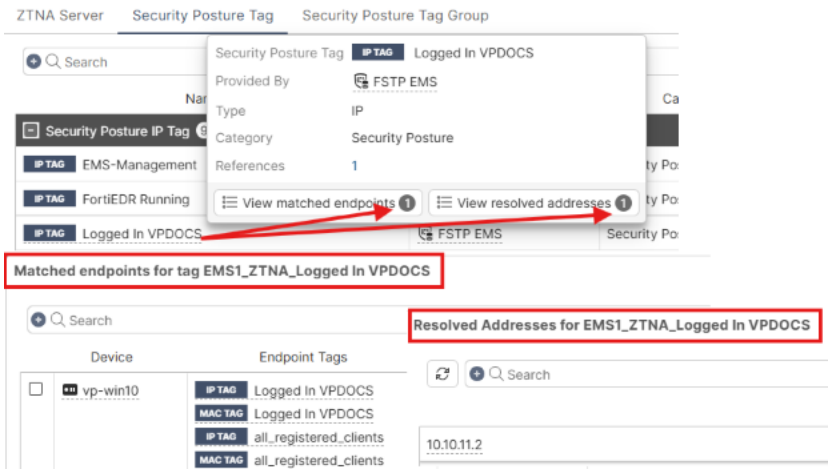


FortiGate as default gateway

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.

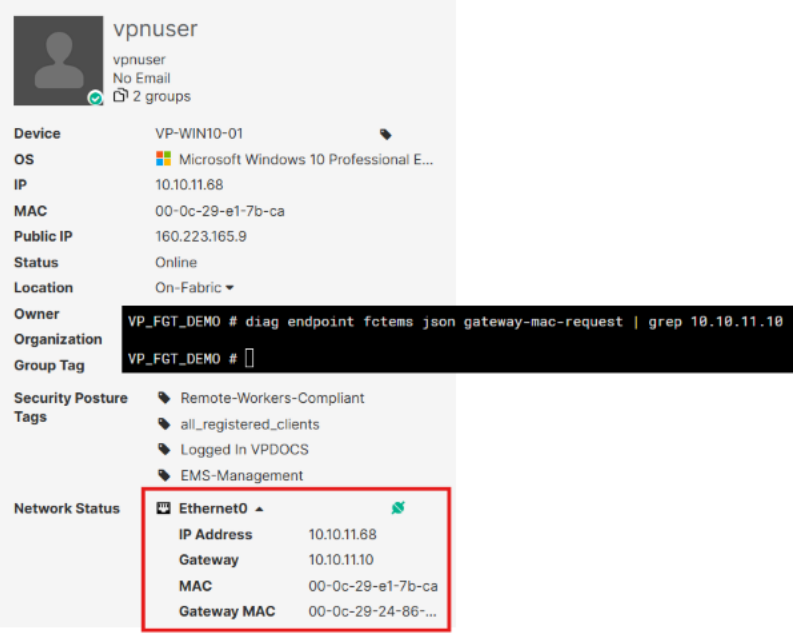


As a result, the endpoint shows under *Matched endpoints* and *Resolved addresses*.

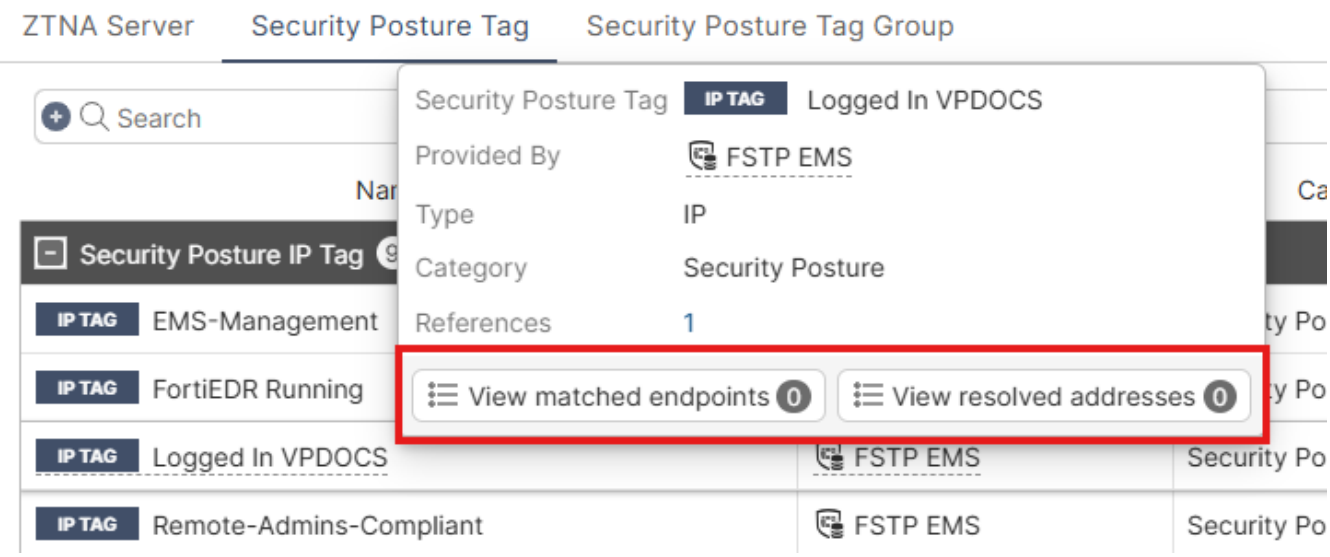


FortiGate not as default gateway

In the following, the FortiClient gateway address does not point to the FortiGate in question.



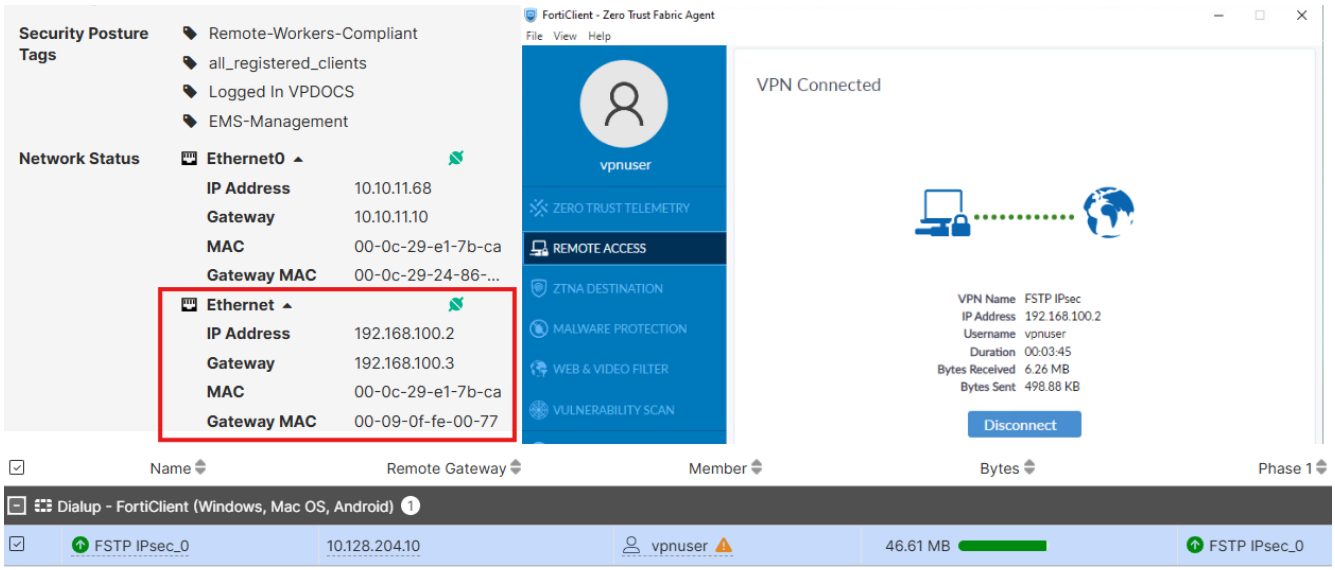
As a result, the endpoint does not show *Matched endpoints* or *Resolved addresses*.



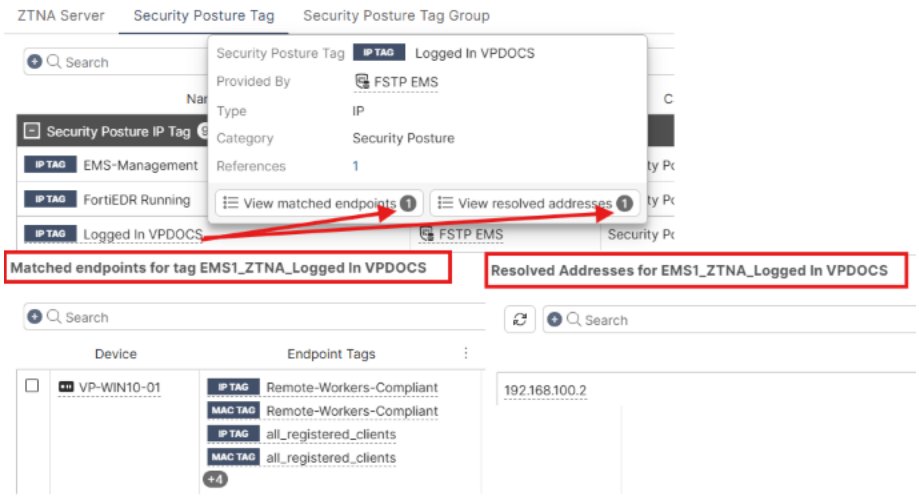
FortiGate as VPN server

This example uses the same endpoint as in FortiGate not as default gateway on page 524.

FortiClient is connected to FortiGate VPN.



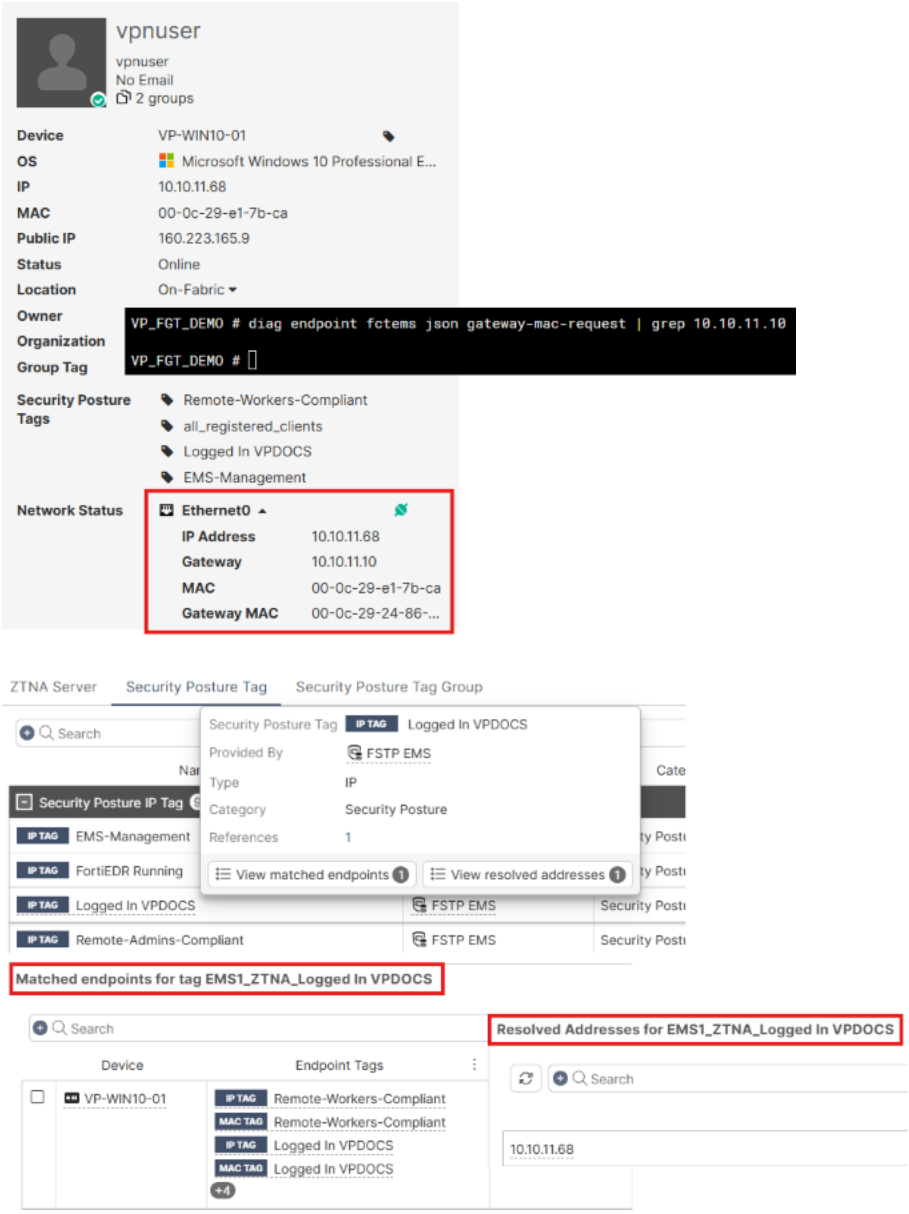
This results in the endpoint showing under both *Matched endpoints* and *Resolved addresses*.



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 516.

Enabling *Share all FortiClients* results in both *Resolved addresses* and *Matched endpoints* being populated for remote FortiClients.



ZTNA Applications Catalog

ZTNA Applications Catalog displays configured zero trust network access (ZTNA) applications.

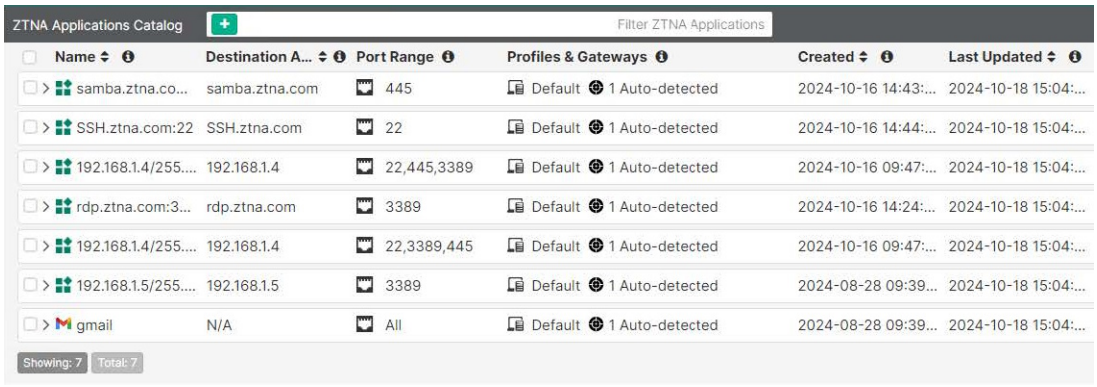
If you have configured a Fortinet Security Fabric connection between FortiOS 7.4.4 or later and EMS and a ZTNA server is configured in FortiOS, EMS can retrieve non-web (TCP forwarding) ZTNA applications from FortiOS. See Configuring FortiClient EMS. You can view the ZTNA applications catalog in *Fabric & 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

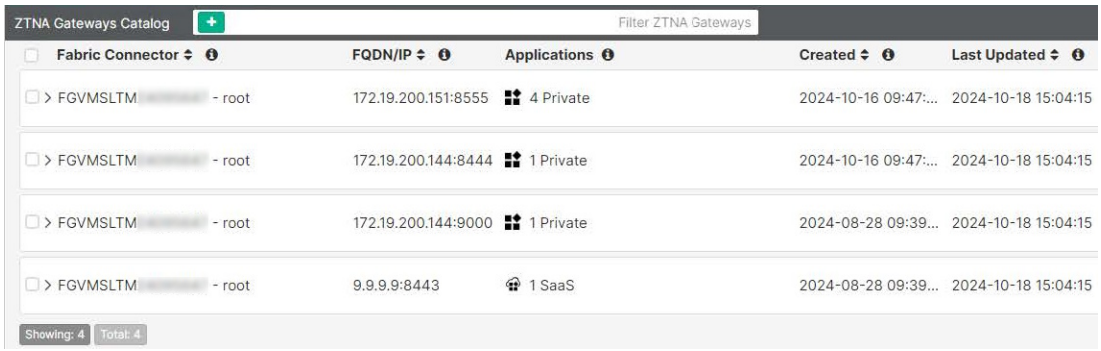
autodetected ZTNA gateways or applications on EMS. Autodetected gateways are not available for gateway selection for a ZTNA application manually defined on EMS.

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:

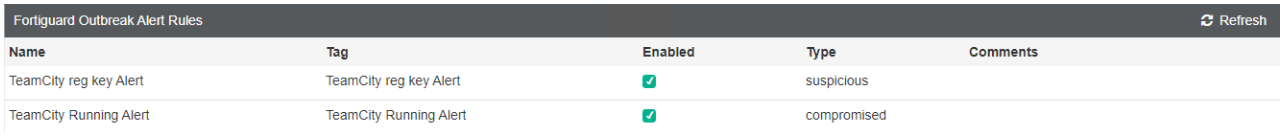
1. Go to *Fabric & Connectors > ZTNA Applications Catalog*.
2. Click *Add*.
3. For *Application Type*, select *SaaS*.
4. Configure SaaS applications by searching for and selecting the desired application in the dropdown list.
5. From the *Select Gateways* dropdown list, selected the desired gateway. 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

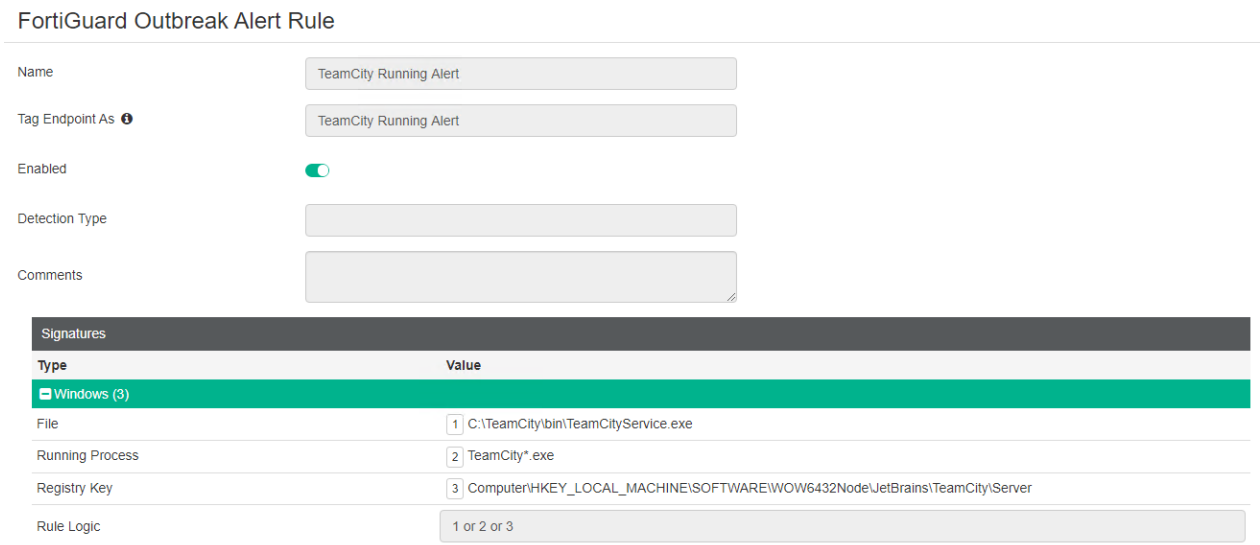
FortiClient EMS receives predefined outbreak alert rules from FortiGuard to help protect your network from vulnerabilities. For example, consider that FortiGuard Labs discovers a zero-day vulnerability in a popular application. The Fortinet team then creates a new FortiGuard outbreak alert rule, which 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 508.

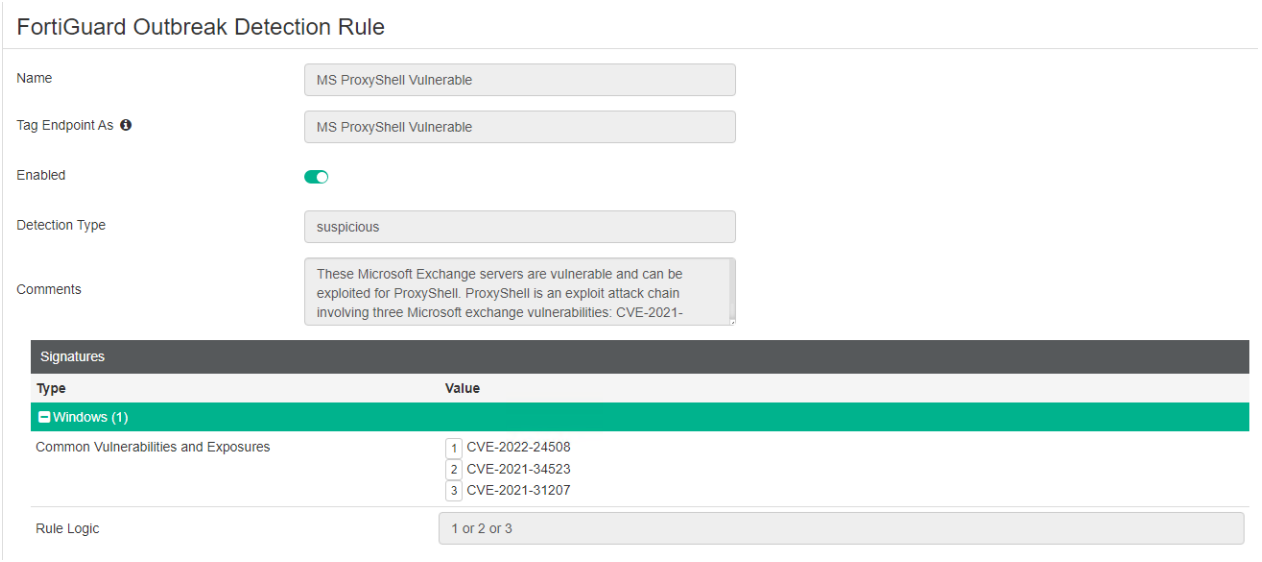
Unlike security posture tagging rules, you cannot modify or delete FortiGuard outbreak alert rules. You can only enable or disable them from the *FortiGuard Outbreak Alert Rules* pane.



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 FortiClient EMS.

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 465.

This feature requires the EPP license. See FortiClient EMS on page 23.

Applications

The FortiClient EMS 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.
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"""
```

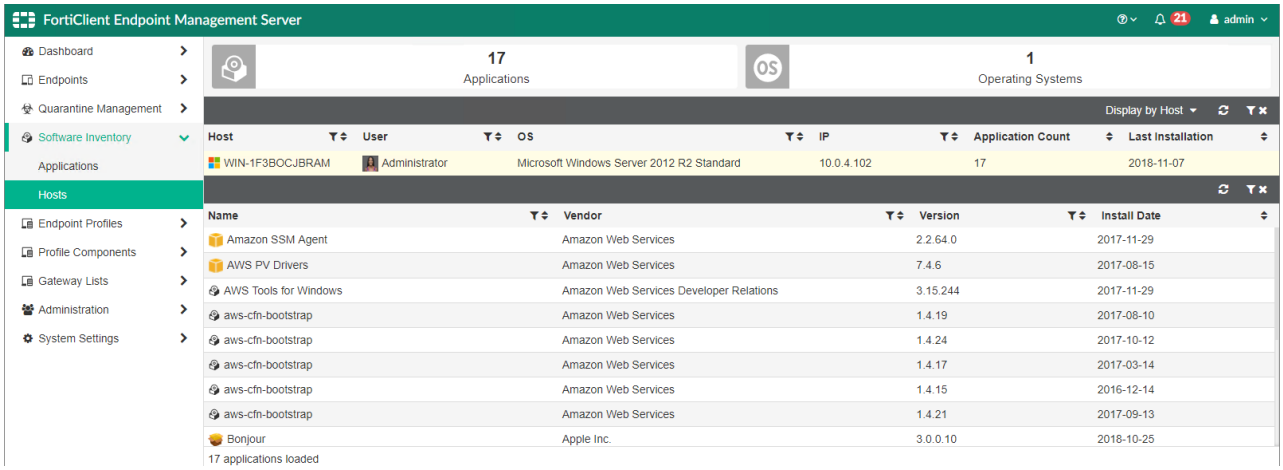
Hosts

The FortiClient EMS 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 532.
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 533 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 FortiClient EMS. You can view quarantined file information for all managed endpoints in *Files* pane and allowlist files from FortiClient EMS if needed.

Viewing quarantined files

After FortiClient quarantines files on endpoints and sends the quarantined file information to FortiClient EMS, 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.

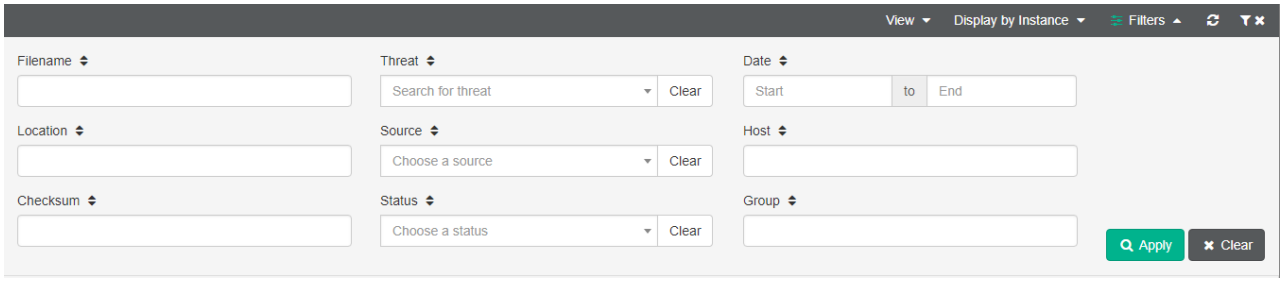
Quarantined Files	Number of files that FortiClient has quarantined on endpoints. Click to display the list of quarantined files.
Restored Files	Number of files that have been restored on endpoints. Click to display the list of restored files.
Affected Hosts	Number of hosts where FortiClient has quarantined 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 FortiClient EMS 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

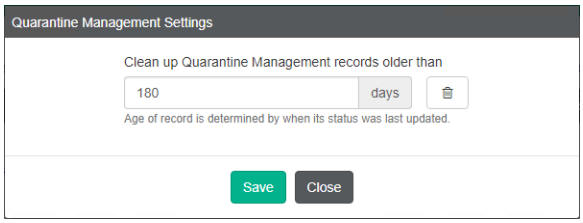
You can configure EMS to delete quarantine records after a configured number of days.

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

This section describes how to configure Windows and LDAP users, create new user accounts, and activate disabled user accounts:

Viewing users

You can view the default *admin* user and all users added to FortiClient EMS.

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 FortiClient EMS 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 FortiClient EMS.
Role	Admin role assigned to the user. See Admin roles on page 567.
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 Activating a disabled account on page 565.
Comments	Comments added when creating/configuring the user.

Configuring user accounts

You can configure Windows and LDAP users to have no access or administrator access to FortiClient EMS. You can also create a new user account in EMS.

EMS derives the Windows users from the host server that it is installed on. To add more Windows users, you must add them to the host server. EMS derives the list of LDAP users from those in the Active Directory (AD) domain imported into FortiClient EMS. If you want to add more LDAP users, they must already exist in the AD domain configured as the user server.

To configure Windows and LDAP user accounts:

1. Go to *Administration > Admin Users*.
2. Click *Add*.
3. Under *User source*, select *Choose from Windows users* or *Choose from LDAP*.
4. If you selected *Choose from LDAP*, select the desired server from the *Authentication Server* dropdown list. You must have already configured an authentication server. See Adding an ADDS server on page 571.
5. Click *Next*.
6. Configure the user:

Option	Description
Username	(New user account only) enter the desired username.
User	(Windows/LDAP only) Select the user to configure permissions for.
Role	Select the desired admin role for this user. See Admin roles on page 567.
Domain Access	Select or add access to a domain for the user. If desired, enable *Allow all domains* to allow this user access to all domains connected to EMS.
Restrict Login to Trusted Hosts	When this option is enabled, users can only log into this account from a trusted host machine. In the *Trusted Hosts* field, enter a trusted host machine's IP address. Use the + button to add multiple trusted host machines.
Comment	Enter optional comments/information for the Windows/LDAP user.

7. Click *Save*.



When an admin user from an AD domain logs into EMS, they must provide the domain name as part of their username to log in successfully. For example, if the domain name is "example-domain" and the username is "admin", the user must enter "example-domain/admin" when logging into EMS.

Activating a disabled account

FortiClient EMS disables user accounts that have been inactive for the period configured in *Admin User Settings > Allowed inactive days*. See Configuring Admin User Settings on page 581.

When EMS disables an account, the user cannot log into FortiClient EMS and sees an error message that reads "Your account has been disabled due to inactivity. Please contact an EMS admin for assistance."

An FortiClient EMS super administrator can activate the disabled account. After the super administrator activates the account, the user can log in as usual.



The built-in *admin* user account is always active. The *Allowed inactive days* setting does not affect the *admin* account.

To activate a disabled account:

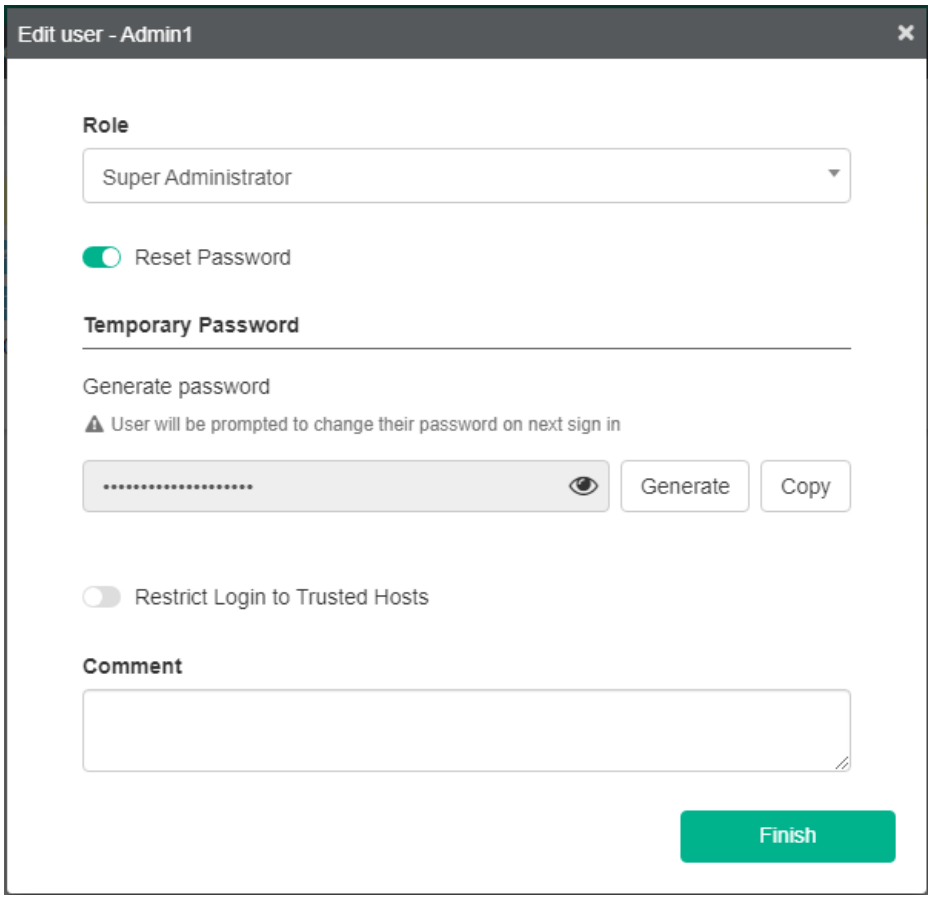
1. Go to *Administration > Admin Users*. EMS shows the deactivated user with a lock icon beside their name. *Last login or activation* shows that EMS has disabled the account.
2. Click *Activate*. The user's status updates and they can log in as usual.

Resetting the password for a local administrator

A global super administrator can reset the password for EMS local administrators from the EMS GUI. When multitenancy is enabled, this option is only available in the global site.

To reset the password for EMS local administrators:

1. Log in to EMS as a super administrator.
2. Go to *Administration > Admin Users*.
3. Edit the desired local administrator.
4. Enable *Reset Password*.
5. EMS automatically generates a temporary password. If desired, click *Generate* to generate a new random password. Click *Copy*, then click *Finish*.



6. Log out of EMS.
7. Log in to EMS as the local administrator. In the *Password* field, paste in the temporary password.
8. EMS prompts you to update your password. Enter a new password, then click *Submit*.

Using the PasswordRecovery tool

If the EMS built-in administrator password is forgotten, a super administrator cannot access EMS. In this case, you can use the PasswordRecovery tool.

To use the PasswordRecovery tool:

1. On the EMS machine, run `sudo -i` to log in to the shell with root privileges.
2. Go to `/opt/forticlientems/bin`.
3. Run `./PasswordRecovery`.
4. Enter `yes` to proceed. This resets the password for the built-in admin user and generates a temporary password.
5. Log in to EMS as admin and enter the temporary password.
6. EMS prompts you to create a new user. Create a new user and password, then click *Submit*.



You must have execute permissions to run PasswordRecovery to create a temporary password.

Admin roles

You can use admin roles to define the permissions each administrator account has in FortiClient EMS. You can use a default admin role in FortiClient EMS 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 FortiClient EMS. You cannot edit or delete these admin roles:

Name	Description
Super administrator	Most privileged admin role. Complete access to all FortiClient EMS 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 568.
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. See Configuring user accounts on page 564.
Manage Google domains*	Manage connections to Google domains to decide which Chromebooks to manage. See Google Domains on page 221.
Manage custom groups	Create, rename, and edit endpoint groups. See Managing groups on page 172.
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 194.

Permission	Link to description
Block/Unblock/Quarantine/Unquarantine/Reregister endpoints	Manage endpoint access to the network through blocking, quarantine, and registration. See Managing endpoints on page 194.
Manage and assign endpoint policies	See Endpoint Policy & Components on page 240.
View group assignment rules	View group assignment rules. See Group assignment rules on page 216.
Manage group assignment rules	Create, delete, and edit group assignment rules. See Group assignment rules on page 216.
View endpoint filter bookmarks	View endpoint filter bookmarks. See Using bookmarks to filter the list of endpoints on page 188.
Manage endpoint filter bookmarks	Create, delete, and edit endpoint filter bookmarks. See Using bookmarks to filter the list of endpoints on page 188.
View quarantine management	View lists of quarantined and allowlisted files. See Quarantine Management on page 558.
Manage quarantine management	Allowlist and restore quarantined files and remove files from the allowlist. See Quarantine Management on page 558.
View software inventory	See Software Inventory on page 532.
Manage software inventory	See Software Inventory on page 532.

Policy permissions

Permission	Link to description
View endpoint policies*	View endpoint policies. See Endpoint Policy & Components on page 240.
View endpoint profiles*	View endpoint profiles. See Endpoint Profiles on page 255.
Manage endpoint profiles*	Create, delete, and edit endpoint profiles. See Endpoint Profiles on page 255.
View Security Posture tagging rules	View security posture tagging rules. See Tags on page 495.
Manage Security Posture tagging rules	Create, delete, and edit security posture tagging rules. See Tags on page 495.

Permission	Link to description
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 229.
Manage installers	Create, delete, and edit installers. See FortiClient Installer on page 229.
View CA certificates	View CA certificates. See CA Certificates on page 246.
Manage CA certificates	Upload, import, and delete CA certificates. See CA Certificates on page 246.
View on-fabric detection rules	View on-fabric detection rules. See On-fabric Detection Rules on page 248.
Manage on-fabric detection rules	Create, delete, and edit on-fabric detection rules. See On-fabric Detection Rules on page 248.

Setting permissions

Permission	Link to description
View server settings*	View *Server* settings. See Configuring EMS settings on page 629
Manage server settings*	Modify *Server* settings. See Configuring EMS settings on page 629.
View Fortinet services settings	View *FortiGuard Services* settings. See Configuring FortiGuard Services settings on page 645.
Manage Fortinet services settings	Modify *FortiGuard Services* settings. See Configuring FortiGuard Services settings on page 645.
View endpoint settings	View *Endpoints* settings. See Configuring EMS settings on page 629.

Permission	Link to description
Manage endpoint settings	Modify *Endpoints* settings. See Configuring EMS settings on page 629.
View login banner settings*	View login banner settings. See Configuring EMS settings on page 629.
Manage login banner settings*	Modify login banner settings. See Configuring EMS settings on page 629.
View alert settings*	View *Alerts* settings. See Alerts on page 649.
Manage alert settings*	Modify *Alerts* settings. See Alerts on page 649.
View custom message settings	View endpoint quarantine message settings. See Customizing the endpoint quarantine message on page 653.
Manage custom message settings	Modify endpoint quarantine message settings. See Customizing the endpoint quarantine message on page 653.
View feature select settings	View feature select settings. See Feature Select on page 655.
Manage feature select settings	Modify feature select settings. See Feature Select on page 655.

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.

Option	Description
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 577.
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 172.

Adding an Entra ID server

FortiClient (macOS) and (Linux) do not support Entra ID integration with EMS.

To create an enterprise application for FortiClient:

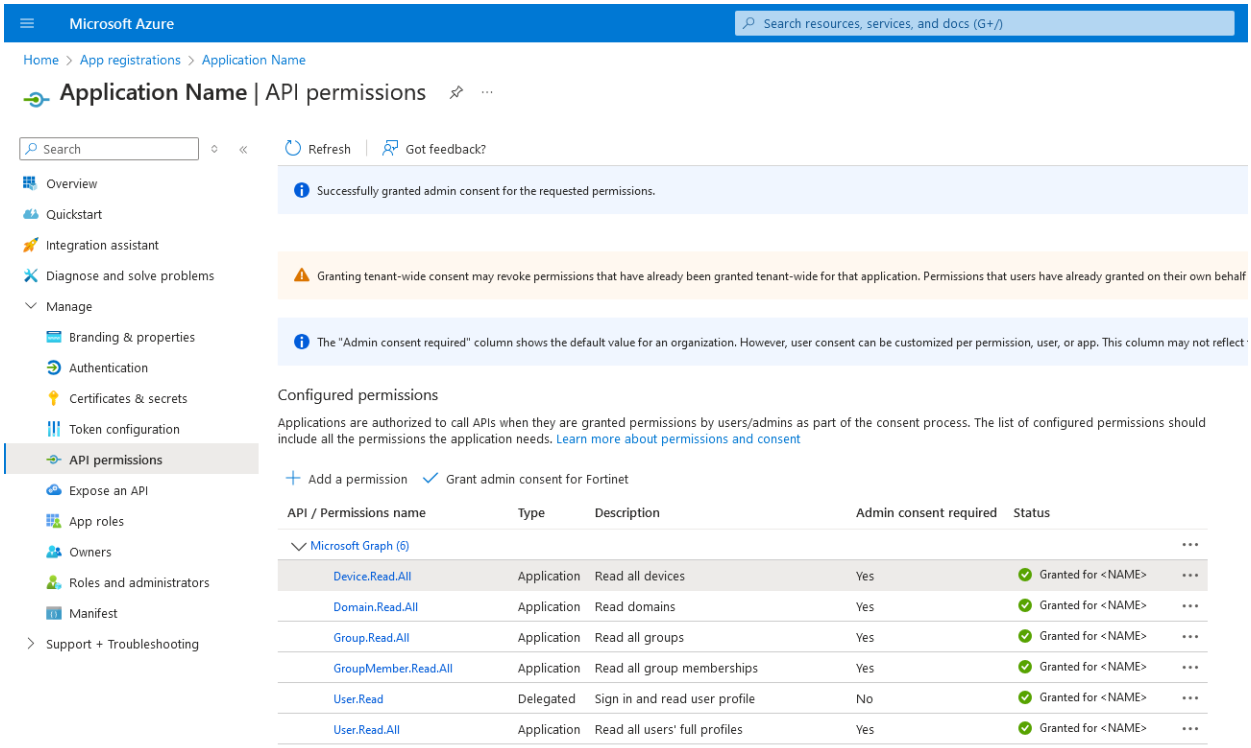
1. In the Azure portal, go to *Microsoft Entra ID > Enterprise applications > New application*.
2. Click *Create your own application*.
3. In the *What's the name of your app?* field, enter the desired name.
4. Under *What are you looking to do with your application?*, select *Register an application 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.

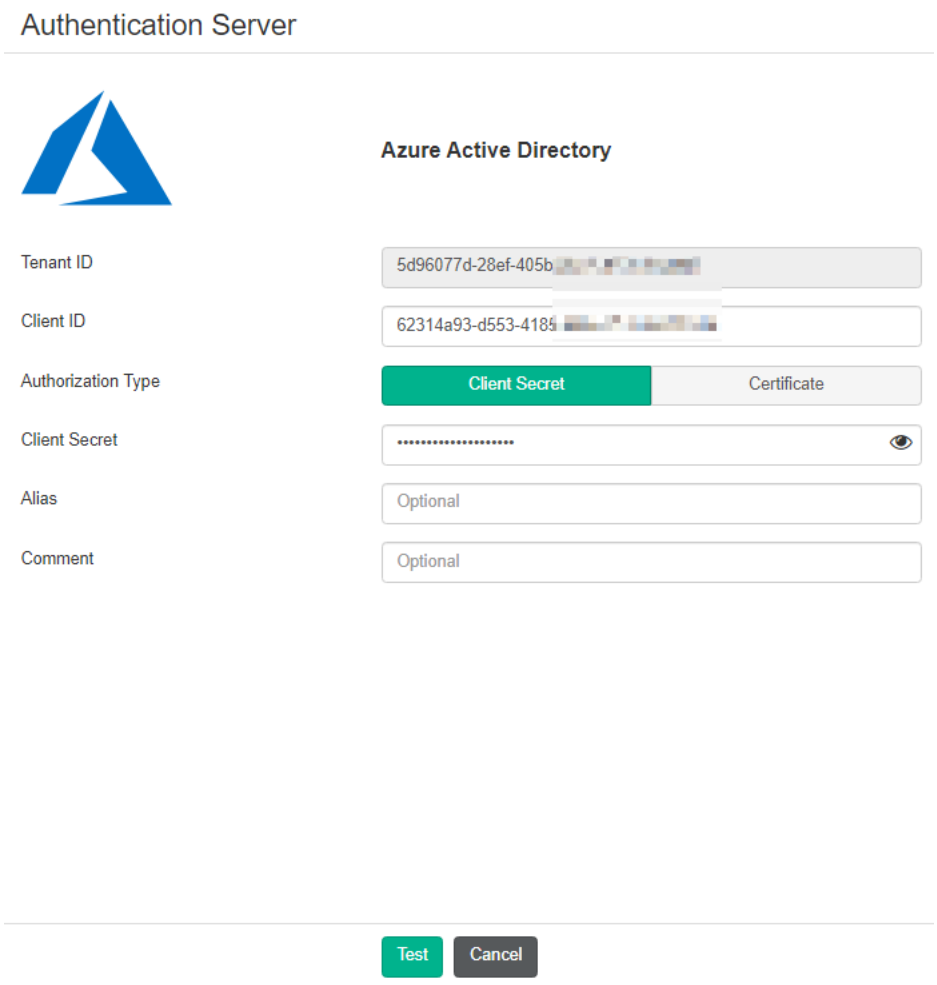
To upload the CA root certificate to Azure:

This only applies if you use certificate authentication. The following assumes that you have a certificate authority (CA) root 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 root certificate.

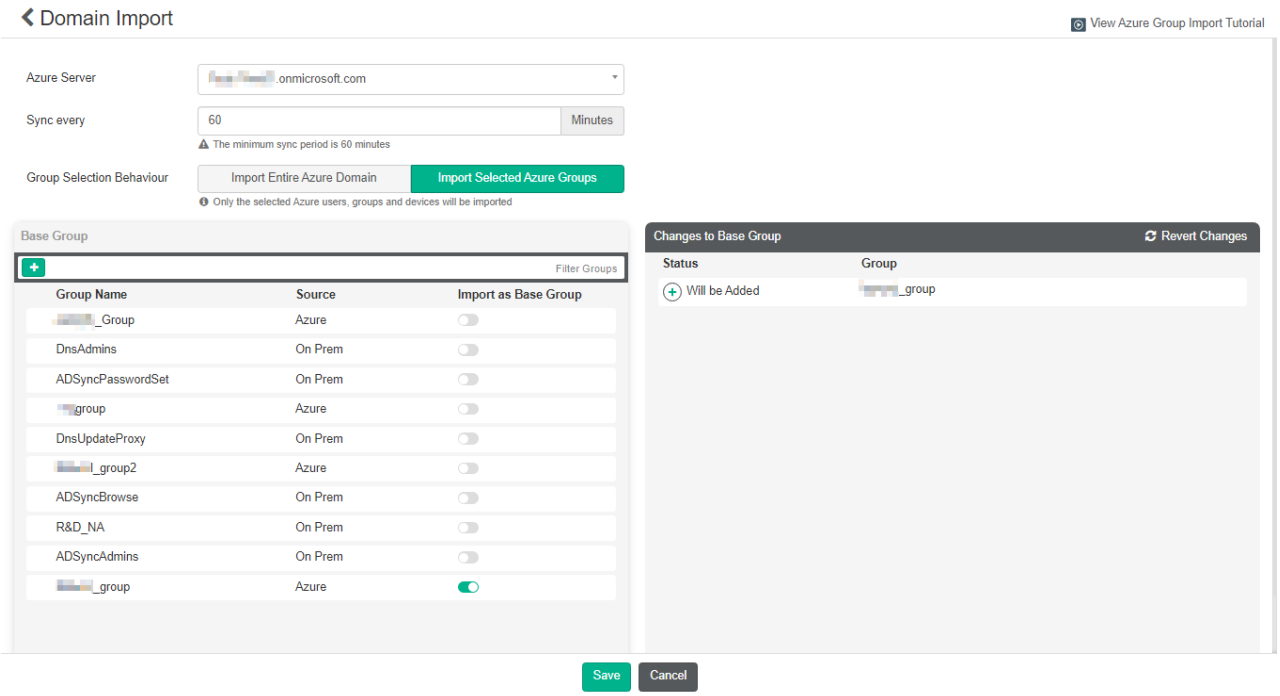
To configure an Entra ID server in EMS:

1. Configure the Entra ID server as an authentication server in EMS:
   a. Go to *Administration > Authentication Servers*.
   b. Click *Add > Azure*.
   c. Do one of the following:
      - To use client secret authentication, in the Azure management console, collect your tenant ID, client ID, and client secret. In the *Tenant ID* and *Client ID* fields, enter the IDs that you collected from the Azure management console. For *Authorization Type*, select *Client Secret*. In the *Client Secret* field, enter the client secret that you collected from the Azure management console.
      - To use certificate authentication, for *Authorization Type*, select *Certificate*. Browse to and select the desired CA-signed client certificate. If this client certificate matches the root certificate that you uploaded to Azure in To upload the CA root certificate to Azure: on page 574, Azure allows the integration.
   d. Configure other fields as desired.
   e. Click *Test*.



   f. After the test succeeds, click *Save*.
2. Go to *Endpoints > Manage Domains*.
3. Click *Add*, then *Azure*.

4. From the *Azure Server* dropdown list, select the desired server.
5. In the *Sync every* field, enter the number of minutes after which EMS syncs with the Azure server.
6. For *Group Selection Behaviour*, select *Import Entire Azure Domain* or *Import Selected Azure Groups*.
7. 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 AD server.

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 577.

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.

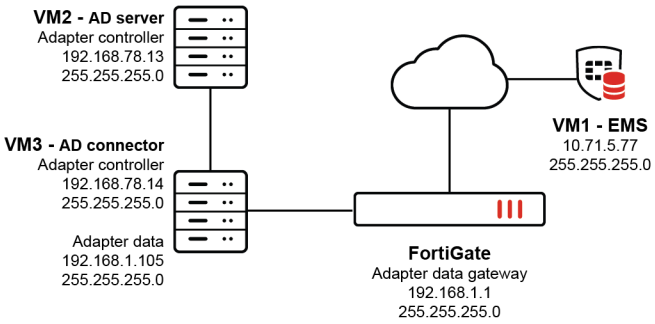


AD connector

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.

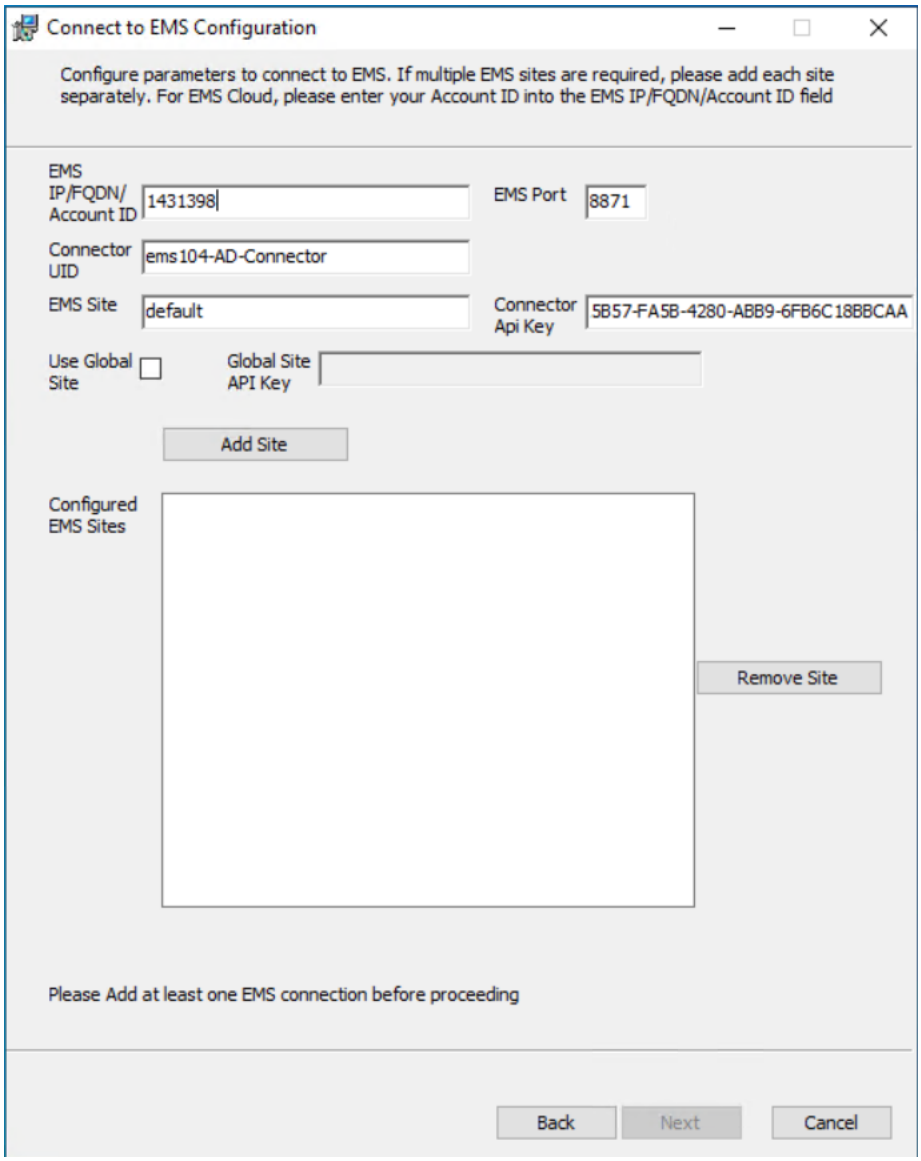
The AD connector and EMS versions must match for this feature to function. The SSL certificate that the AD server sends to establish a TLS handshake can have a maximum RSA key size of 8192 bits.

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.

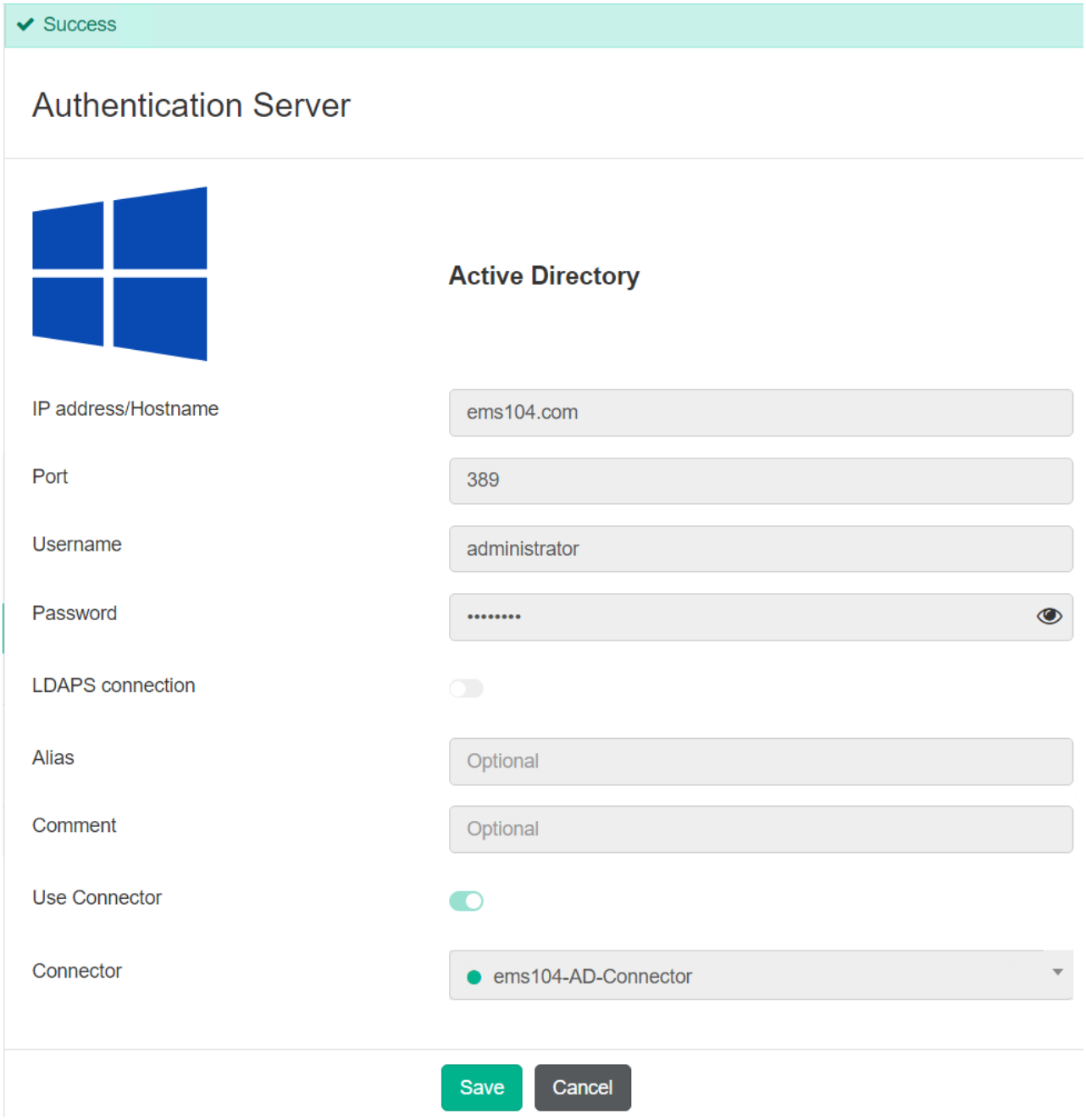


2. Create the AD connector:
   a. You can install the AD connector in a host that EMS and the AD server can reach. On the host machine, from the EMS installation package, run FortiClientEndpointManagementServerADConnector_7.4.3.XXXX_x64.msi.
   b. In the *Connect to EMS Configuration* dialog, enter the 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.



Configuring Admin User Settings

To configure Admin User Settings:

1. Go to *Administration > Admin User Settings*.
2. Set the following options:

Option	Description
Expire login session after x minutes	Specify how long to keep inactive users logged into FortiClient EMS. When the time expires, EMS automatically logs the user out. Enter 0 to keep inactive users logged into FortiClient EMS indefinitely.
Disable administrators' accounts when inactive for x days	Specify the number of days of inactivity after which to disable a user account. For example, if you specify this field to 10 and a user does not log into FortiClient EMS for ten days, EMS disables their account so that they cannot log into FortiClient EMS. A super administrator can reactivate their account. See Activating a disabled account on page 565.
Change password after x days	Specify the number of days after which to force the user to change their password. Enter 0 to disable this setting. This setting only applies to built-in users such as the admin user and local administrators created in EMS.

3. Click *Save*.

SAML SSO

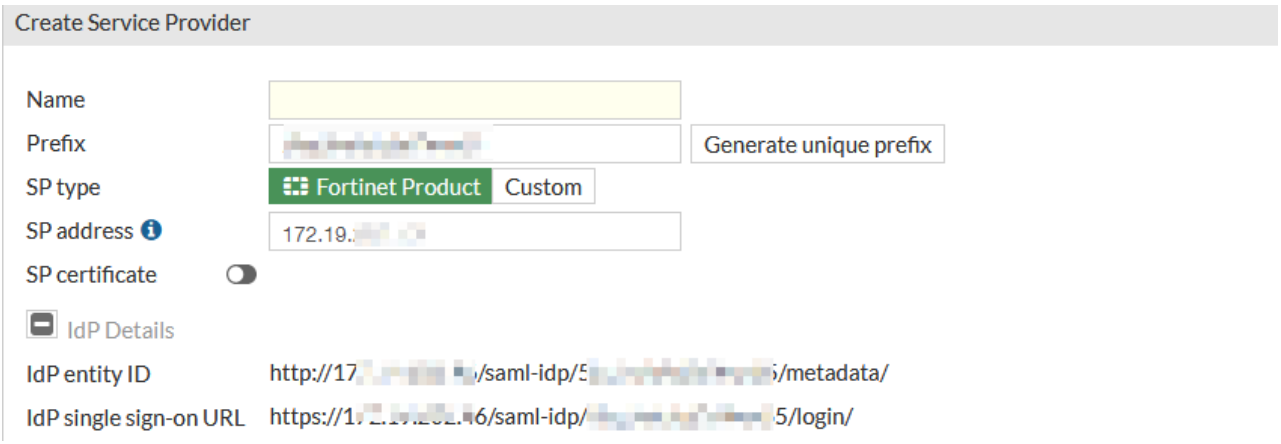
You can enable SAML single sign on (SSO) to allow users to log in to EMS using an identity provider (IdP), such as FortiAuthenticator (on-premise and Cloud), FortiOS, and third party IdPs such as Azure, Okta, and Active Directory Federation Services. The following topics provide information on configuring SSO with different IdPs:

SAML SSO with FortiGate as IdP

You can enable SAML SSO to allow users to log in to EMS using a FortiGate as an identity provider (IdP).

To configure SAML SSO:

1. Configure SAML SSO in FortiOS with EMS as the service provider (SP). See Configuring single-sign-on in the Security Fabric. Ensure that you download the IdP certificate and copy the IdP entity ID and IdP single sign-on URL values to use when configuring SAML SSO on EMS.



2. In EMS, configure SAML SSO:
   a. Go to *Administration > SAML SSO*.
   b. Click *Add*.
   c. Configure general options:
      i. In the *Name* field, enter the desired name.
      ii. If desired, enable *Match Any Other Domains*. If you enable this setting, when an admin attempt login to EMS, EMS matches their credentials against this IdP configuration if they do not match another SAML SSO configuration on this site. You can only enable this setting on one SAML SSO configuration per site.
      iii. In *Domain Names*, enter the desired domain names for the IdP.
   d. Configure *Assertion Attributes*:
      i. EMS prepopulates the *Assertion Attributes > Username Claim* field with *username* as the value. This is the same default value as in FortiOS. If you change this value, ensure that you also change the value in FortiOS by going to *Security Fabric > Fabric Connectors > Security Fabric Settings > SAML Single Sign-On Advanced Options*. Edit the EMS SP and confirm that the value for *SAML Attribute > Name* for *Value type Username* is the same as the value in EMS in *Assertion Attributes > Username Claim*.
      ii. To configure a role-based access control (RBAC) rule to assign an EMS admin role to a user that belongs to a specific FortiOS user group, enter group in the *Group name* field. This is the default value in FortiOS. If you change this value, ensure that you also change the value in FortiOS by going to *Security Fabric > Fabric Connectors > Security Fabric Settings > SAML Single Sign-On Advanced Options*. Edit the EMS SP and confirm that the value in *SAML Attribute > Name* for *Value type Profile Name* is the same as the value in EMS in *Assertion Attributes > Username Claim*.
   e. Configure *Service Provider Settings*:

Setting	Description
SP Address	Enter the EMS IP address. You can also click the *Use Current Browser Address* button to autopopulate the field. Your browser must be able to access this IP address.

Setting	Description
SP Entity ID	This field is prepopulated. You do not need to provide this value to FortiOS when configuring SAML SSO for EMS using FortiGate as an IdP.
SP ACS (login URL)	
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 FortiOS in step 1.

f. Configure *Identity Provider Settings*. In this configuration, the FortiGate is the IdP:

Setting	Description
IdP Entity ID	Enter the IdP entity ID value that you copied from FortiOS.
IdP single sign-on URL	Enter the IdP single sign-on URL value that you copied from FortiOS.
IdP Certificate	Click *Upload new certificate* to upload the IdP certificate. Upload the same certificate that you configured for the IdP (the FortiGate) in FortiOS in step 1.

g. Under *Access Control*, you can configure rules for RBAC. You can create authorization rules to assign EMS administrator roles to specific users or user groups from the IdP. To add a role, do the following:

i. Click *Add*, then select *User Based* or *Group Based*.

ii. In the *Authorization Rule* field, do the following:

- If you are configuring a rule to assign a role to a specific user, enter the user name, ID, or email address.
- If you are configuring a rule to assign a role to a user group, enter the group name.

iii. From the *Role* dropdown list, select the desired role. See Admin roles on page 567.

iv. (Optional) Click *Advanced Settings*.

v. (Optional) Select access to a domain for the user. If desired, enable *Allow all domains* to allow this user access to all domains connected to EMS.

vi. (Optional) Enable *Restrict Login to Trusted Hosts*. When this option is enabled, users can only log into this account from a trusted host machine. In the *Trusted Hosts* field, enter a trusted host machine's IP address. Use the + button to add multiple trusted host machines.

vii. Click *Finish*.

viii. Enable the rule.

ix. Configure multiple rules as desired. If desired, click *Change Priority* and click and drag the rules to edit the priority levels of the rules. If a user is applicable for multiple rules, EMS applies the rule with the highest priority level to the user. Only SSO users from the IdP with usernames that match the configured authorization rules can access EMS as an admin user. Deleting an authorization rule does not remove its associated users as admin users from EMS. You must delete them from *Administration > Admin Users*.

h. Click *Save*.

3. In FortiOS, create a new system administrator. These users can log in to EMS using SAML SSO.



For a user to log in using SAML SSO, you must enable remote HTTPS access on EMS. See Configuring EMS settings on page 629.

To log in to EMS using SSO:

1. Double-click the *FortiClient Endpoint Management Server* icon.
2. Click *Sign in with SSO*.
3. EMS displays the SSO login page. Enter a username and password configured in FortiOS, then click *Login*.



When an administrator logs in to EMS with SSO for the first time, they have restricted permissions. An EMS super administrator can adjust permissions for the new administrator.

SAML SSO with Okta as IdP

You can configure a single sign on (SSO) connection with Okta via SAML, where Okta is the identity provider (IdP) and FortiClient EMS is the service provider (SP). This feature allows administrators to log in to EMS by logging in with their Okta credentials.

To configure FortiClient EMS with Okta SSO:

1. In EMS, start creating the SAML configuration:
   a. Go to *Administration > SAML SSO*.
   b. Click *Add*.
   c. In the *Name* field, enter the desired name.
   d. If desired, enable *Match Any Other Domains*. If you enable this setting, when an admin attempt login to EMS, EMS matches their credentials against this IdP configuration if they do not match another SAML SSO configuration on this site. You can only enable this setting on one SAML SSO configuration per site.
   e. In *Domain Names*, enter the desired domain names for the IdP.
   f. Under *Assertion Attributes*, to configure a role-based access control (RBAC) rule to assign an EMS admin role to a specific Okta user, enter email in the *Username* field.
   g. To configure a RBAC rule to assign an EMS admin role to a user that belongs to a specific Okta user group, enter groupnames in the *Group name* field.
   h. *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 an SP in Okta. Copy these values.
2. Create and configure your FortiClient EMS environment in Okta:
   a. Add the FortiClient EMS application to Okta:
      i. On the Okta administration page, go to *Applications*.
      ii. Click *Add Application*.
      iii. In the searchbox, search for and select FortiClient EMS.

iv. Click *Add*.
v. Under *General Settings*, click *Done*.

b. On the *Assignment* tab, from the *Assign* dropdown list, select *Assign to People*.
c. In the dialog, assign the desired users to the FortiClient EMS Okta application.

3. Obtain the IdP information from Okta:
   a. On the *Sign On* tab in Okta, click *View Setup Instructions*.
   b. Scroll to step 5. This step lists the IdP information that you must provide to FortiClient EMS. Copy the values in the *IdP Entity ID* and *IdP Single Sign-On URL* fields.
   c. Download the IdP certificate from the provided link. Save the certificate to your device.
4. Configure the IdP information in FortiClient EMS:
   a. In FortiClient EMS, 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. (Optional) If desired, configure the *Assertion Attributes > Username Claim* field. Only configure this option if you want to use a value other than `username`.
   c. From the *IdP Certificate* dropdown list, select *Create*, then upload the certificate that you downloaded. Click *Next*.
5. Under *Access Control*, you can configure rules for RBAC. You can create authorization rules to assign EMS administrator roles to specific users or user groups from the IdP. To add a role, do the following:
   a. Click *Add*, then select *User Based* or *Group Based*.
   b. In the *Authorization Rule* field, do the following:
      - If you are configuring a rule to assign a role to a specific user, enter the user name, ID, or email address.
      - If you are configuring a rule to assign a role to a user group, enter the group name.
   c. From the *Role* dropdown list, select the desired role. See Admin roles on page 567.
   d. (Optional) Click *Advanced Settings*.
   e. (Optional) Select access to a domain for the user. If desired, enable *Allow all domains* to allow this user access to all domains connected to EMS.
   f. (Optional) Enable *Restrict Login to Trusted Hosts*. When this option is enabled, users can only log into this account from a trusted host machine. In the *Trusted Hosts* field, enter a trusted host machine's IP address. Use the + button to add multiple trusted host machines.
   g. Click *Finish*.
   h. Enable the rule.
   i. Configure multiple rules as desired. If desired, click *Change Priority* and click and drag the rules to edit the priority levels of the rules. If a user is applicable for multiple rules, EMS applies the rule with the highest priority level to the user. Only SSO users from the IdP with usernames that match the configured authorization rules can access EMS as an admin user. Deleting an authorization rule does not remove its associated users as admin users from EMS. You must delete them from *Administration > Admin Users*.
6. Review the SAML configuration, then click *Save*.

SAML SSO with Entra ID as IdP

You can configure a single sign on (SSO) connection with Microsoft Entra ID (formerly known as Azure Active Directory (AD)) via SAML, where Entra ID is the identity provider (IdP) and FortiClient EMS is the

service provider (SP). This feature allows users to log in to EMS by logging in with their Entra ID credentials.

To configure FortiClient EMS with Entra ID SSO:

1. In FortiClient EMS, start configuring SAML:
   a. Go to *Administration > SAML SSO*.
   b. Click *Add*.
   c. In the *Name* field, enter the desired name.
   d. If desired, enable *Match Any Other Domains*. If you enable this setting, when an admin attempt login to EMS, EMS matches their credentials against this IdP configuration if they do not match another SAML SSO configuration on this site. You can only enable this setting on one SAML SSO configuration per site.
   e. In *Domain Names*, enter the desired domain names for the IdP.
   f. *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 an SP in Azure. Copy these values.
2. Create and configure your FortiClient EMS environment in Azure:
   a. In the Azure portal, go to *Microsoft Entra ID > Enterprise applications > New application*.
   b. Click *Create your own application* and provide a name, for instance, FortiClient EMS.
   c. Click *Create*.
   d. Assign Entra ID users and groups to FortiClient EMS.
   e. Go to *Set up single sign on*.
   f. For the SSO method, select *SAML*.
   g. In *Basic Configuration*, enter the values that you copied in step 1. The following summarizes the mapping between EMS fields and Azure fields:

EMS Service Provider Settings field	Entra ID Basic SAML configuration field
SP Entity ID	Identifier (Entity ID)
SP ACS (login) URL	Reply URL (Assertion Consumer Service URL)
SP Address	Sign on URL

3. Obtain the *Assertion Attributes* information from Azure:
   a. Go to *Attributes & Claims*.
   b. Copy the claim names for *user.mail* and *user.groups [All]*.
   c. Paste the claim name for user.mail in the *Username* field in EMS.
   d. Paste the claim name for user.groups [All] in the *Group name* field in EMS. You must do this to configure a role-based access control (RBAC) rule to assign an EMS admin role to a user that belongs to a specific Entra ID user group.
4. Obtain the IdP information from Azure:
   a. The *SAML Signing Certificate* box contains links to download the SAML certificate. Download the certificate.
   b. The *Set up <FortiClient EMS instance name>* box lists the IdP information that you must provide to FortiClient EMS. Copy the values in the *Login URL* and *Entra ID Identifier* fields.
5. Configure the IdP information in FortiClient EMS:
   a. In EMS, under *Identity Provider Settings*, In the *IdP Entity ID* and *IdP single sign-on URL* fields, paste the values that you copied from the *Entra ID Identifier* and *Login URL* fields, respectively.

   b. From the *IdP Certificate* dropdown list, select *Create*, then upload the certificate that you downloaded. Click *Next*.
6. Under *Access Control*, you can configure rules for RBAC. You can create authorization rules to assign EMS administrator roles to specific users or user groups from the IdP. To add a role, do the following:
   a. Click *Add*, then select *User Based* or *Group Based*.
   b. In the *Authorization Rule* field, do the following:
      - If you are configuring a rule to assign a role to a specific user, enter the user email address.
      - If you are configuring a rule to assign a role to a user group, enter the group object ID. You can find the object ID in Azure on the user group overview page.
   c. From the *Role* dropdown list, select the desired role. See Admin roles on page 567.
   d. (Optional) Click *Advanced Settings*.
   e. (Optional) Select access to a domain for the user. If desired, enable *Allow all domains* to allow this user access to all domains connected to EMS.
   f. (Optional) Enable *Restrict Login to Trusted Hosts*. When this option is enabled, users can only log into this account from a trusted host machine. In the *Trusted Hosts* field, enter a trusted host machine's IP address. Use the *+* button to add multiple trusted host machines.
   g. Click *Finish*.
   h. Enable the rule.
   i. Configure multiple rules as desired. If desired, click *Change Priority* and click and drag the rules to edit the priority levels of the rules. If a user is applicable for multiple rules, EMS applies the rule with the highest priority level to the user. Only SSO users from the IdP with usernames that match the configured authorization rules can access EMS as an admin user. Deleting an authorization rule does not remove its associated users as admin users from EMS. You must delete them from *Administration > Admin Users*.
7. Review the SAML configuration, then click *Save*.

SAML SSO with AD FS as IdP

You can configure a single sign on (SSO) connection with Active Directory Federation Services (AD FS), where AD FS is the identity provider (IdP) and FortiClient EMS is the service provider (SP). This feature allows users to log in to EMS by logging in with their AD FS credentials.

The following instructions assume that you have already installed and configured AD FS.

To configure SAML SSO with AD FS as IdP:

1. In EMS, start creating the SAML configuration:
   a. Go to *Administration > SAML SSO*.
   b. Click *Add*.
   c. In the *Name* field, enter the desired name.
   d. If desired, enable *Match Any Other Domains*. If you enable this setting, when an admin attempts login to EMS, EMS matches their credentials against this IdP configuration if they do not match another SAML SSO configuration on this site. You can only enable this setting on one SAML SSO configuration per site.
   e. In *Domain Names*, enter the desired domain names for the IdP.

   f. Under *Assertion Attributes*, to configure a role-based access control (RBAC) rule to assign an EMS admin role to a user that belongs to a specific AD FS user group, enter groupName in the *Group name* field.
   g. *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 an SP in AD FS. Copy these values.
2. Create and configure your FortiClient EMS environment in AD FS:
   a. Open AD FS Management and right-click *Relying Party Trusts* and select *Add Relying Party Trust*. This launches the *Add Relying Party Trust Wizard*. Select *Claims Aware* and click *Next*.
   b. In *Select Data Source*, select *Enter data about the relying party manually* and click *Next*.
   c. Enter a *Display name* and click *Next*.
   d. In *Configure Certificate*, leave the certificate settings at their default values. Click *Next*.
   e. In *Configure URL*, select *Enable Support for the SAML 2.0 WebSSO protocol*, then enter the SAML SSO URL obtained from EMS (*SP ACS (login) URL*).
   f. In *Configure Identifiers*, enter the *Relying party trust identifier* URL obtained from EMS (*SP Entity ID*), then click *Add* and *Next*.
   g. In *Choose Access Control Policy*, leave the default value (*Permit everyone*) and click *Next*.
   h. In *Ready to Add Trust*, review your settings, click *Next*.
   i. In *Finish*, select *Configure claims issuance policy for this application*, then click *Close*.
3. Create claim rules:
   a. In the *Issuance Transform Rules* tab of the *Claim Rules* editor, click *Add Rule*.
   b. In *Choose Rule Type*, select *Send LDAP Attributes as Claims* from the dropdown list, then click *Next*.
   c. In *Configure Claim Rule*, enter a *Claim Rule Name*, select *Active Directory* as the *Attribute Store*, then add the following mapping: from the *LDAP Attribute* column, select *SAM-Account-Name*. In the *Outgoing Claim Type* column, enter *Name ID*, then click *Finish* to add the rule. Click *OK*.
4. Export the IdP certificate, which you must later upload to EMS to finish SAML configuration:
   a. Open the AD FS management snap-in, select *AD FS > Service > Certificates*, then double-click the certificate under *Token-signing*. You can also right-click the field, then select *View Certificate* in the context menu.
   b. In *Certificate*, open the *Details* tab, then select *Copy to File* and click *OK*.
   c. In *Certificate Export Wizard*, click *Next*.
   d. Select *Base-64 encoded X.509 (.CER)*, then click *Next*.
   e. In *Certificate Export Wizard*, select *Browse* to specify the location to export the IdP certificate to, then specify the file name and click *Next*.
   f. In *Completing the Certificate Export Wizard*, click *Finish*, then click *OK* to confirm the export succeeded.
5. Configure the IdP information in FortiClient EMS:
   a. Export the metadata from AD FS by appending *FederationMetadata/2007-06/FederationMetadata.xml* to the AD FS server root URL. See the following example: https://adfs.domain.com/federationmetadata/2007-06/FederationMetadata.xml. The following shows an example on a local AD FS server: https://localhost/FederationMetadata/2007-06/FederationMetadata.xml.
   b. Obtain the IdP single sign-on URL and entity ID from the metadata. The following shows example values: IdP entity ID: http:/adfs.domain.com/adfs/services/trust IdP single sign-on URL: https:/adfs.domain.com/adfs/ls/

   c. In EMS, under *Identity Provider Settings*, paste the values obtained from the metadata in the *IdP Entity ID* and *IdP single sign-on URL* fields.
   d. Provide the certificate extracted in previous steps.
6. Under *Access Control*, you can configure rules for RBAC. You can create authorization rules to assign EMS administrator roles to specific users or user groups from the IdP. To add a role, do the following:
   a. Click *Add*, then select *User Based* or *Group Based*.
   b. In the *Authorization Rule* field, do the following:
      - If you are configuring a rule to assign a role to a specific user, enter the user name, ID, or email address.
      - If you are configuring a rule to assign a role to a user group, enter the group name.
   c. From the *Role* dropdown list, select the desired role. See Admin roles on page 567.
   d. (Optional) Click *Advanced Settings*.
   e. (Optional) Select access to a domain for the user. If desired, enable *Allow all domains* to allow this user access to all domains connected to EMS.
   f. (Optional) Enable *Restrict Login to Trusted Hosts*. When this option is enabled, users can only log into this account from a trusted host machine. In the *Trusted Hosts* field, enter a trusted host machine's IP address. Use the + button to add multiple trusted host machines.
   g. Click *Finish*.
   h. Enable the rule.
   i. Configure multiple rules as desired. If desired, click *Change Priority* and click and drag the rules to edit the priority levels of the rules. If a user is applicable for multiple rules, EMS applies the rule with the highest priority level to the user. Only SSO users from the IdP with usernames that match the configured authorization rules can access EMS as an admin user. Deleting an authorization rule does not remove its associated users as admin users from EMS. You must delete them from *Administration > Admin Users*.
7. Review the SAML configuration, then click *Save*.

SAML SSO with FortiAuthenticator as IdP

You can configure a single sign on (SSO) connection with FortiAuthenticator via SAML, where FortiAuthenticator is the identity provider (IdP) and FortiClient EMS is the service provider (SP). This feature allows users to log in to EMS by logging in with their FortiAuthenticator credentials.

The following instructions assume that you have already configured users and user groups in FortiAuthenticator.

To configure FortiClient EMS with FortiAuthenticator SSO:

1. In FortiClient EMS, start configuring SAML:
   a. Go to *Administration > SAML SSO*.
   b. Click *Add*.
   c. In the *Name* field, enter the desired name.
   d. If desired, enable *Match Any Other Domains*. If you enable this setting, when an admin attempt login to EMS, EMS matches their credentials against this IdP configuration if they do not match another SAML SSO configuration on this site. You can only enable this setting on one SAML SSO configuration per site.

e. In *Domain Names*, enter the desired domain names for the IdP.
f. *Service Provider Settings* displays the *SP Entity ID* and *SP ACS (login) URL* fields. You use these values to configure FortiClient EMS as an SP in FortiAuthenticator. Copy these values.

2. Create and configure your FortiClient EMS environment in FortiAuthenticator:
   a. In FortiAuthenticator, go to *SAML IdP > Service Providers*.
   b. Create a new SP.
   c. In the *SP entity ID* and *SP ACS (login) URL* fields, enter the values that you copied in step 1.
3. Obtain the IdP information from FortiAuthenticator:
   a. From the same page in *SAML IdP > Service Providers*, copy the values in the *IdP entity id* and *IdP single sign-on URL* fields.
   b. Go to *Certificate Management > Certificate Authorities > Local CAs*.
   c. Select *FortiAuthenticator*.
   d. Click *Export Certificate*.
4. Configure the IdP information in FortiClient EMS:
   a. In EMS, under *Identity Provider Settings*, In the *IdP Entity ID* and *IdP single sign-on URL* fields, paste the values that you copied from FortiAuthenticator.
   b. From the *IdP Certificate* dropdown list, select *Create*, then upload the certificate that you expprted. Click *Next*.
5. Configure *Assertion Attributes*:
   a. EMS prepopulates the *Assertion Attributes > Username Claim* field with *username* as the value. This is the same default value as in FortiAuthenticator. If you change this value, ensure that you also change the value in FortiAuthenticator by going to *SAML IdP > Service Providers*. Edit the EMS SP and confirm that a value for *Assertion Attributes > SAML attribute* for *User attribute Username* is the same as the value in EMS in *Assertion Attributes > Username Claim*.
   b. To configure a role-based access control (RBAC) rule to assign an EMS admin role to a user that belongs to a specific FortiOS user group, enter group in the *Group name* field. This is the default value in FortiAuthenticator. If you change this value, ensure that you also change the value in FortiAuthenticator by going to *SAML IdP > Service Providers*. Edit the EMS SP and confirm that a value for *Assertion Attributes > SAML attribute* for *User attribute Username* is the same as the value in EMS in *Assertion Attributes > Username Claim*.
6. Under *Access Control*, you can configure rules for RBAC. You can create authorization rules to assign EMS administrator roles to specific users or user groups from the IdP. To add a role, do the following:
   a. Click *Add*, then select *User Based* or *Group Based*.
   b. In the *Authorization Rule* field, do the following:
      - If you are configuring a rule to assign a role to a specific user, enter the username.
      - If you are configuring a rule to assign a role to a user group, enter the user group name.
   c. From the *Role* dropdown list, select the desired role. See Admin roles on page 567.
   d. (Optional) Click *Advanced Settings*.
   e. (Optional) Select access to a domain for the user. If desired, enable *Allow all domains* to allow this user access to all domains connected to EMS.
   f. (Optional) Enable *Restrict Login to Trusted Hosts*. When this option is enabled, users can only log into this account from a trusted host machine. In the *Trusted Hosts* field, enter a trusted host machine's IP address. Use the *+* button to add multiple trusted host machines.
   g. Click *Finish*.
   h. Enable the rule.

   i. Configure multiple rules as desired. If desired, click *Change Priority* and click and drag the rules to edit the priority levels of the rules. If a user is applicable for multiple rules, EMS applies the rule with the highest priority level to the user. Only SSO users from the IdP with usernames that match the configured authorization rules can access EMS as an admin user. Deleting an authorization rule does not remove its associated users as admin users from EMS. You must delete them from *Administration > Admin Users*.

7. Review the SAML configuration, then click *Save*.

Licenses

See Licensing FortiClient EMS on page 118.

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 FortiClient EMS generates.

1. Go to *Administration > Logs*.
2. Click *Download*. A zip of the raw logs is downloaded to your computer.

Generate Diagnostic Logs

You can create a diagnostic logs package that includes a snapshot of EMS CPU and memory usage, PostgreSQL logs, performance data, and so on. You can send this package to the Fortinet technical support team for troubleshooting.

To create a diagnostic logs package:

1. Go to *Administration > Generate Diagnostic Logs*.
2. If desired, select *Include Database Backup*. If enabled, the package includes a partial database backup. This backup is not intended to replace the regular backup. See To back up the DB: on page 152.
3. If you select to include a database backup, EMS displays fields to enter a password. In the *Password* and *Confirm Password* fields, enter the password.
4. Click *Create*.

Marking all endpoints as uninstalled

You can mark all endpoints as uninstalled, which erases their historical event data.

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 mark all endpoints as uninstalled, 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 mark all endpoints as uninstalled:

1. Go to *Administration > Mark All Endpoints As Uninstalled*.
2. In the dialog, click *Yes*.

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 597.
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 173.
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 598.

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 594.
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 599.
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 FortiClient EMS.

This feature requires per-user licensing. See Windows, macOS, and Linux licenses on page 25.

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	Can be *Authorized* or *Excluded*. If a group is authorized, its users can onboard to EMS. If a group is excluded, its users cannot onboard to EMS.

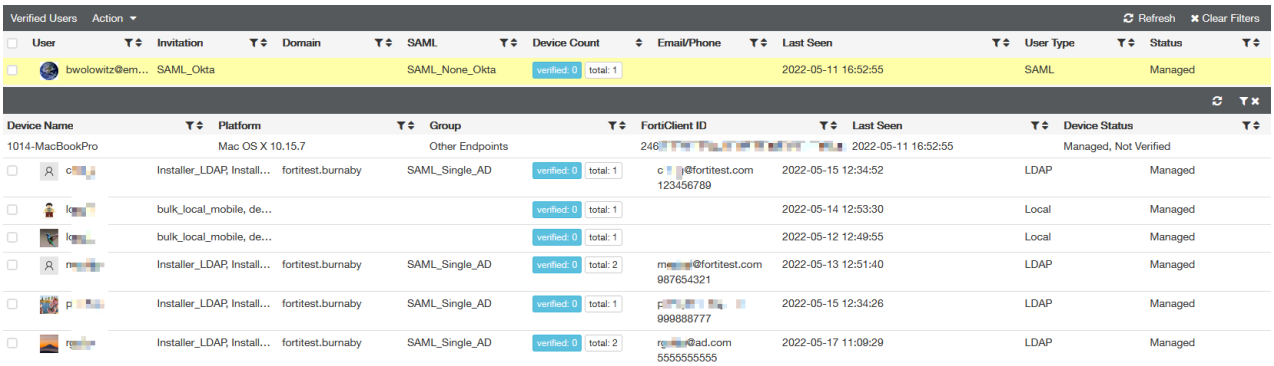
You can filter the list of groups by authorized or excluded, OUs or groups.

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 FortiClient EMS 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 FortiClient EMS. 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. This allows end users to connect to FortiClient EMS 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*, select one of the following:
   - *LDAP* to associate a domain with this SAML configuration. From the *Domain* dropdown list, select the desired domain.
   - *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 Active Directory 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 599.

Invitations

You can configure invitation codes to email to end users. After installing FortiClient, end users can enter the invitation codes to connect FortiClient to EMS.

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. Enable *Send Email Notifications*. You can only enable this option if you have configured SMTP settings. See Configuring SMTP Server settings on page 651.
   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 230.
   e. In the *Email recipients* field, enter the email addresses of the desired end users.
   f. 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:

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 597.
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 173.

Verification type	Description
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 598.

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*.

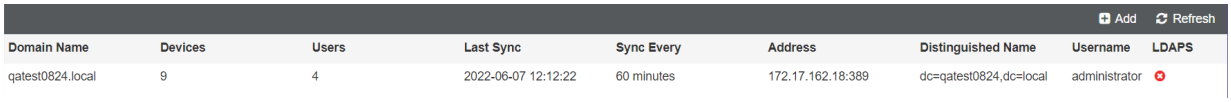
To install FortiClient on the user device:

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 FortiClient EMS.

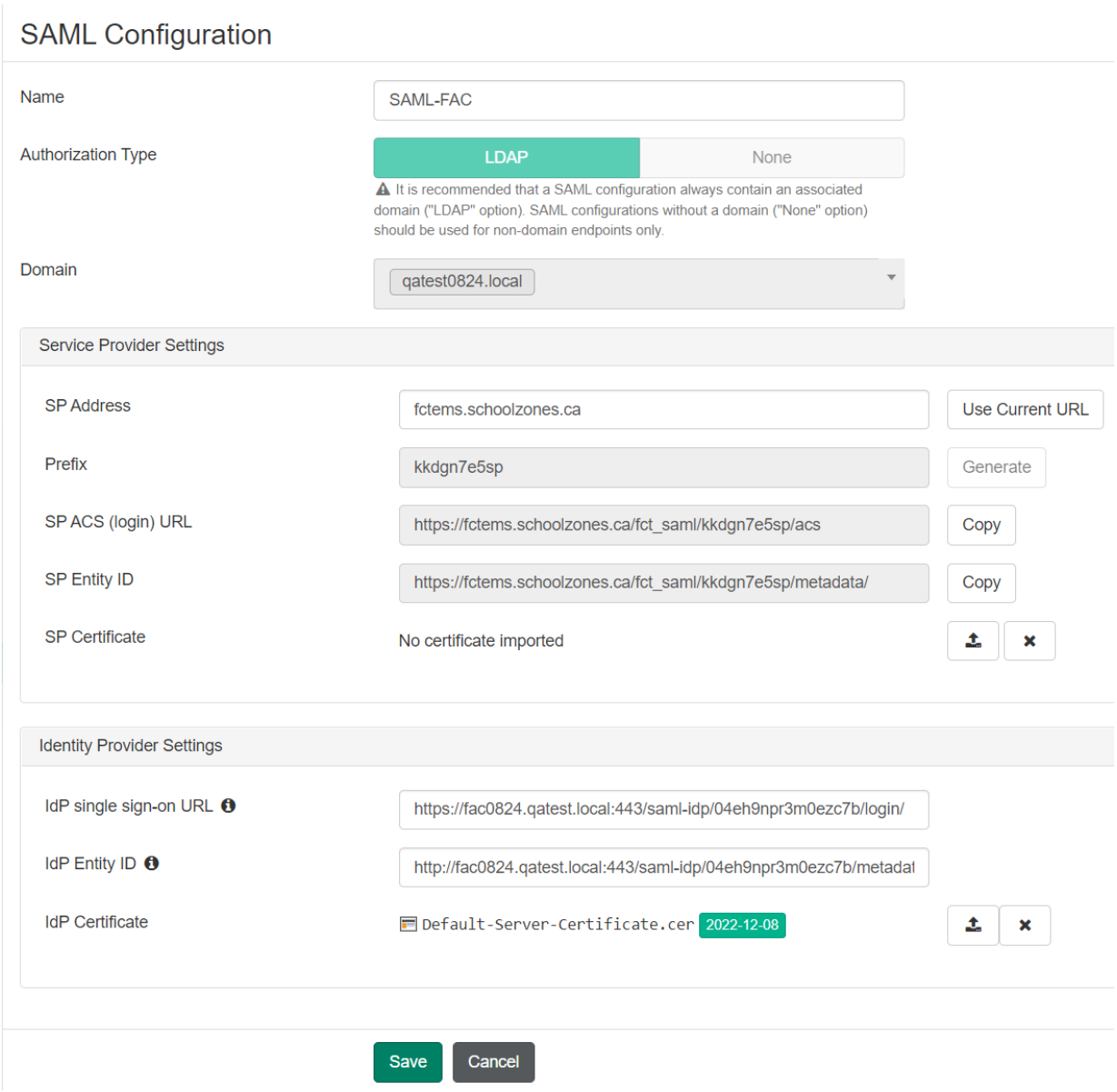
Configuring user verification with SAML authentication and an LDAP domain user account

To configure individual onboarding with SAML authentication using an LDAP domain user account:

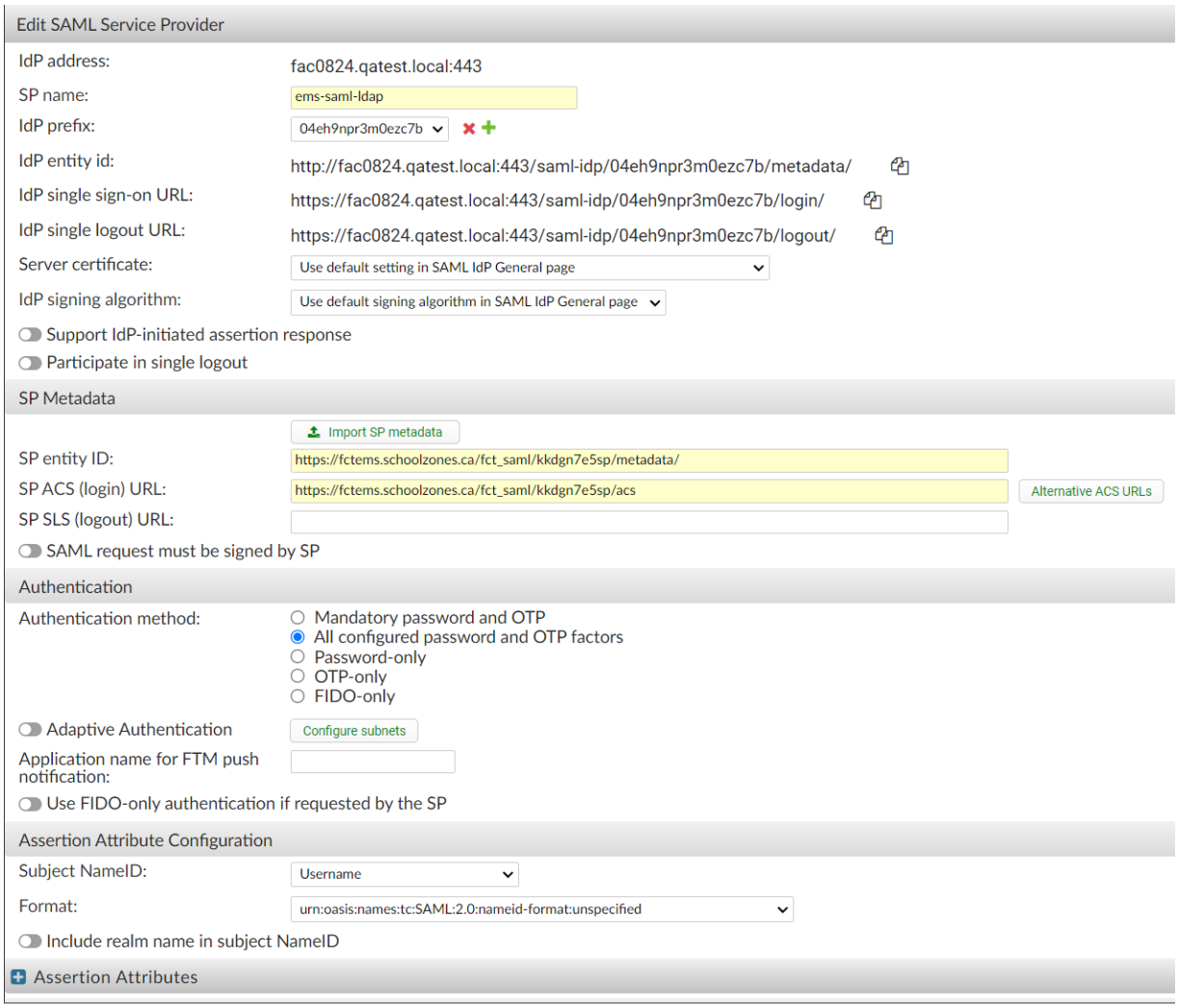
1. Configure EMS:
   a. In EMS, go to *Endpoints* > *Manage Domains*.
   b. Import the desired Active Directory domain. During the onboarding process, EMS authenticates user identities based on this domain. In this example, the domain is qatest0824.local.

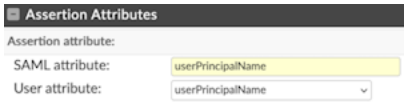


   c. Go to *User Management* > *SAML Configuration*.
   d. Add a SAML configuration with the imported domain. For *Authorization Type*, select *LDAP*. From the *Domain* dropdown list, select the newly imported domain. In this configuration, EMS is the service provider (SP), and FortiAuthenticator is the identity provider (IdP). Under *Identity Provider Settings*, enter your FortiAuthenticator details. Click *Save*.

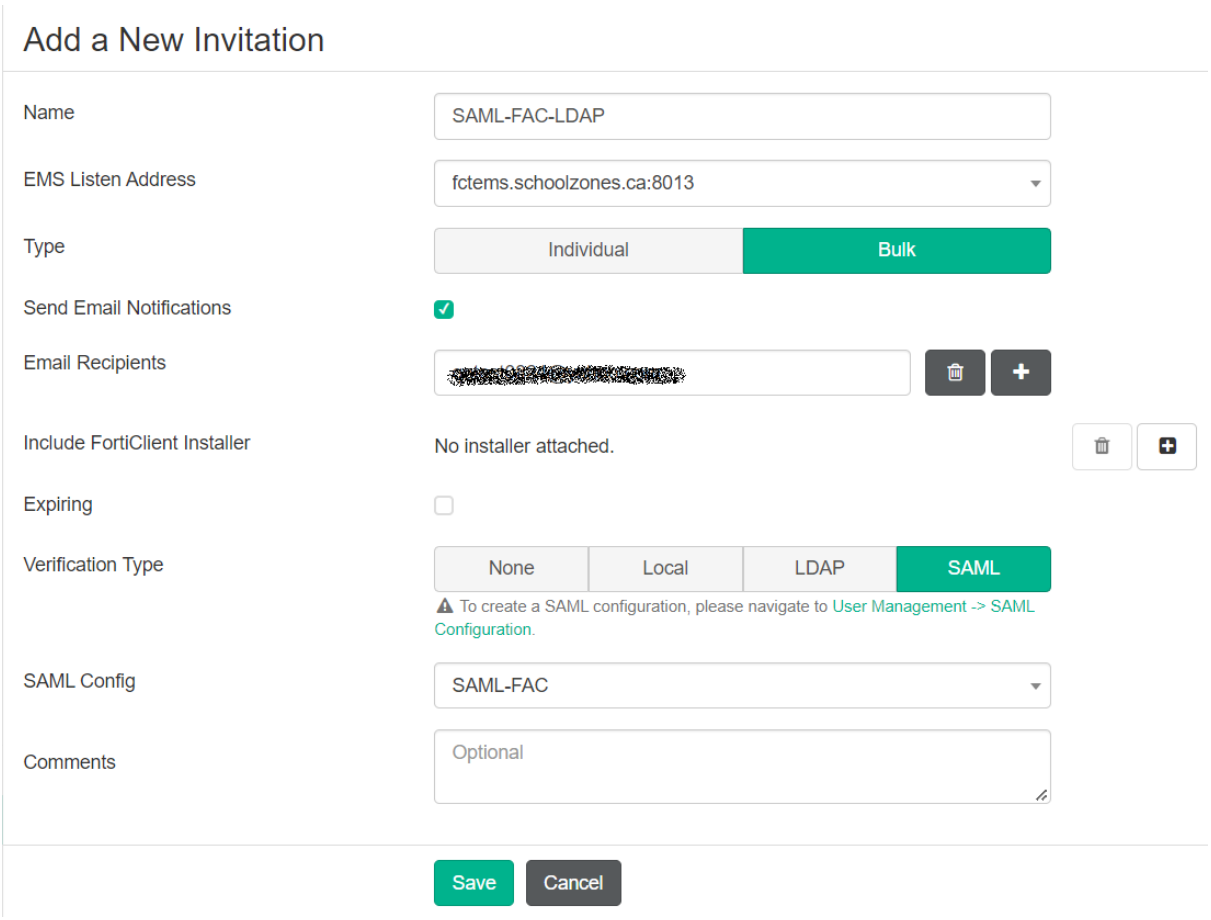

SAML Configuration
Name
SAML-FAC
Authorization Type
LDAP
None
It is recommended that a SAML configuration always contain an associated domain ("LDAP" option). SAML configurations without a domain ("None" option) should be used for non-domain endpoints only.
Domain
qatest0824.local
Service Provider Settings
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.

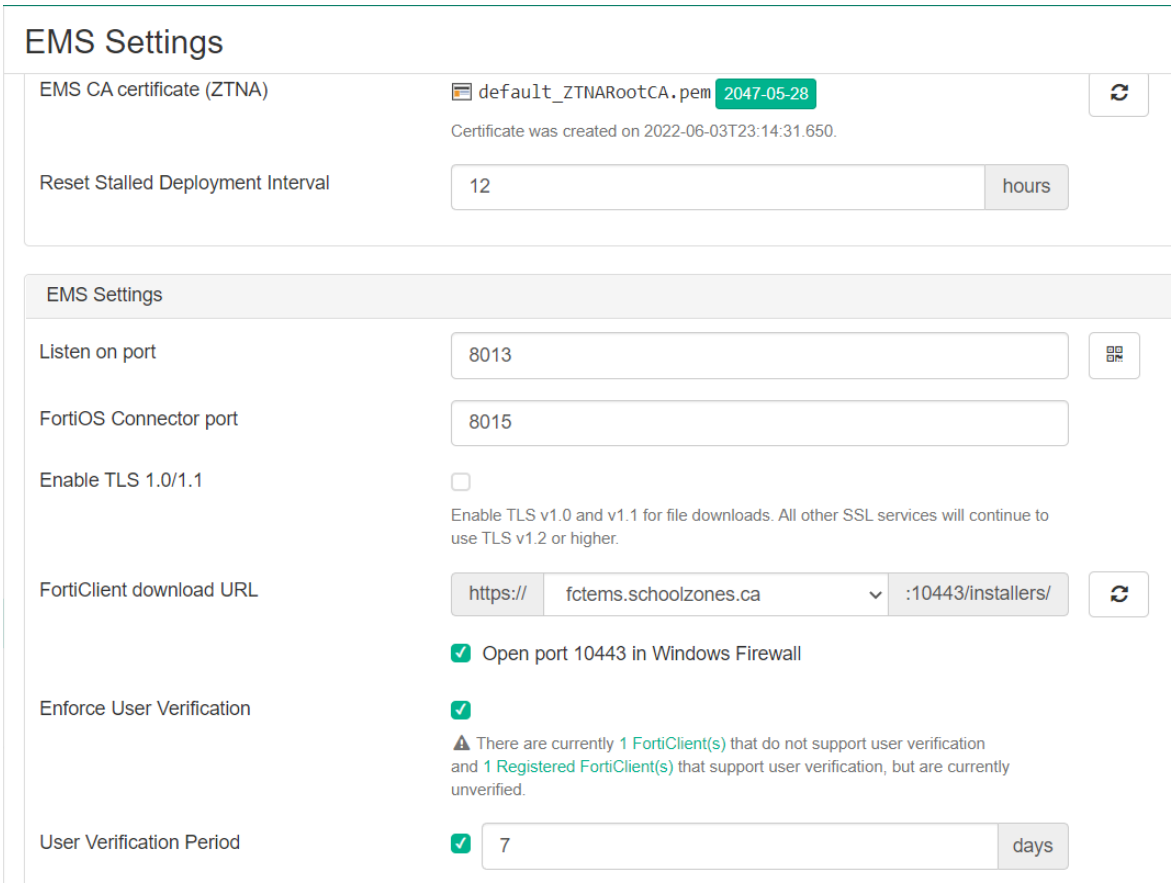




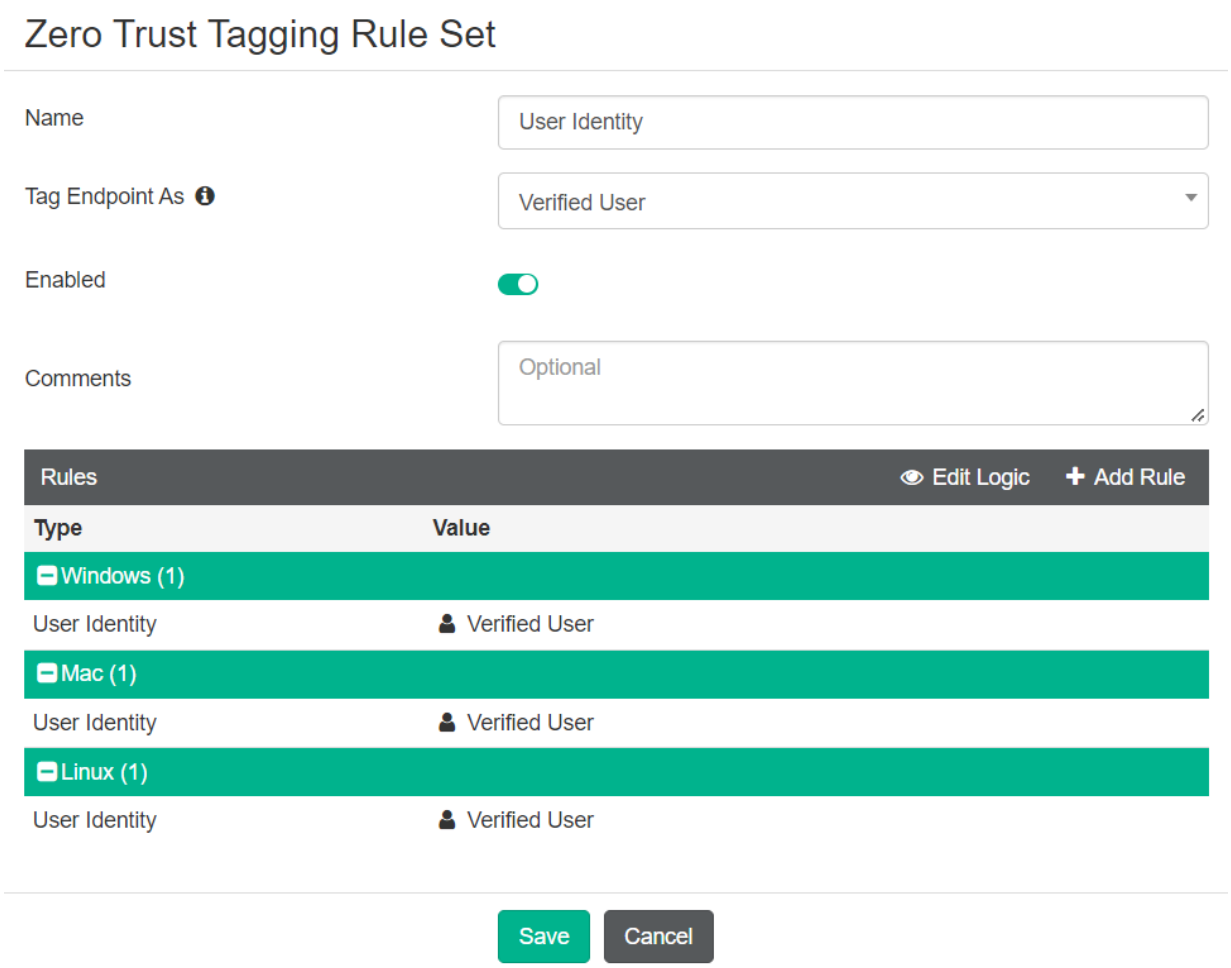
f. In EMS, go to *User Management* > *Invitations*. Click *Add*. Configure the desired recipients to receive their invitation codes over email. For *Verification Type*, select *SAML*. From the *SAML Config* dropdown list, select the SAML configuration that you created. Click *Save*.



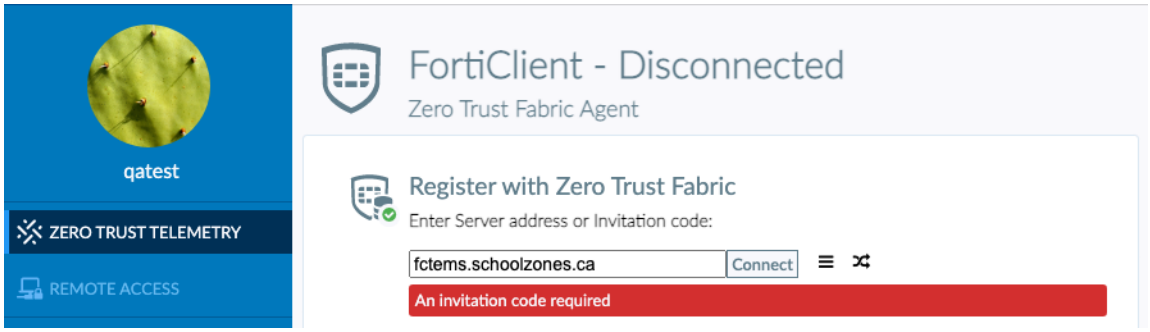
g. Go to *System Settings > EMS Settings*. Enable *Enforce User Verification*. This forces FortiClient to register to EMS using user onboarding.



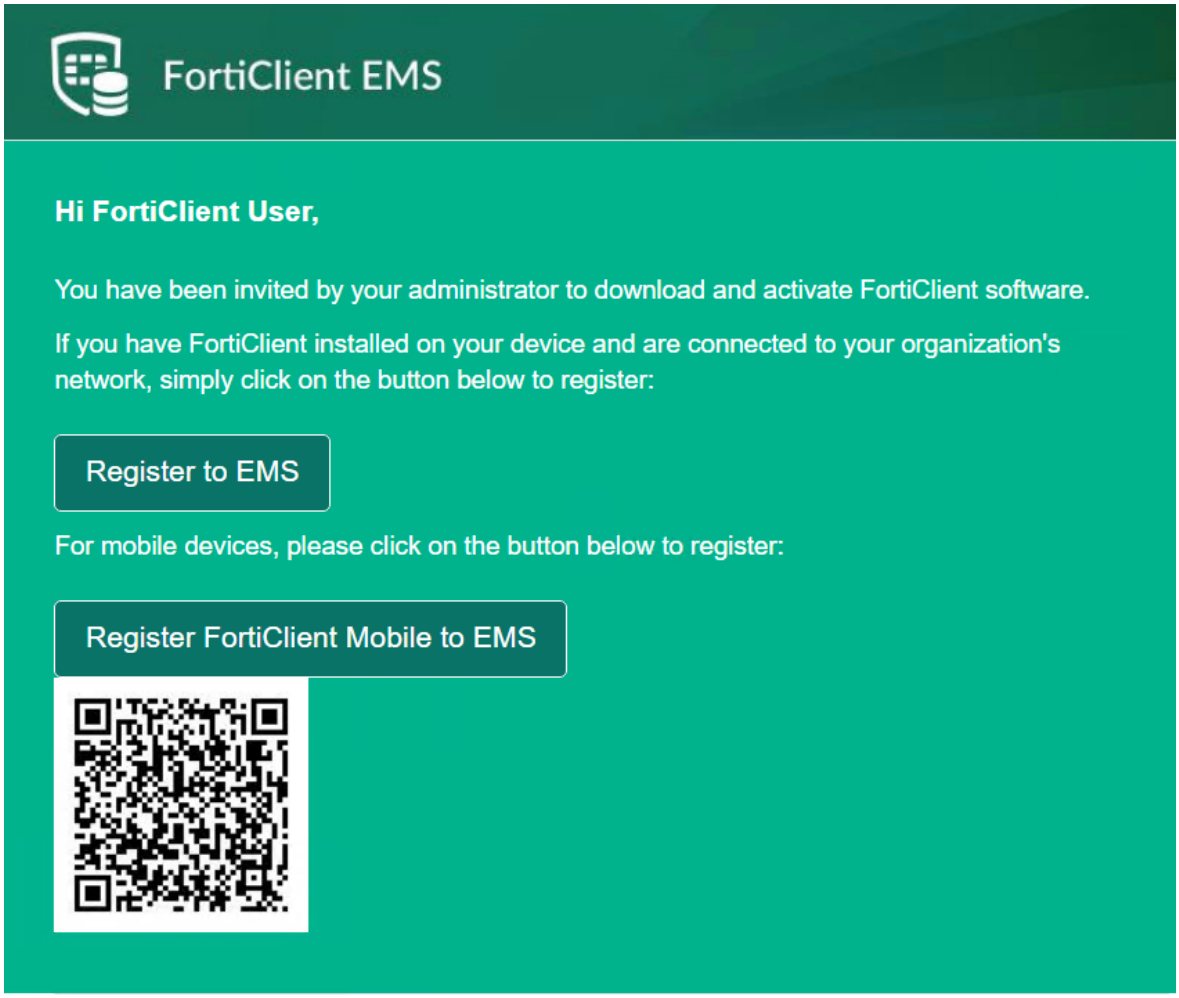
h. Go to *Security Posture Tags > Security Posture Tagging Rules*. Add a security posture tagging rule to tag registered endpoints with verified users.



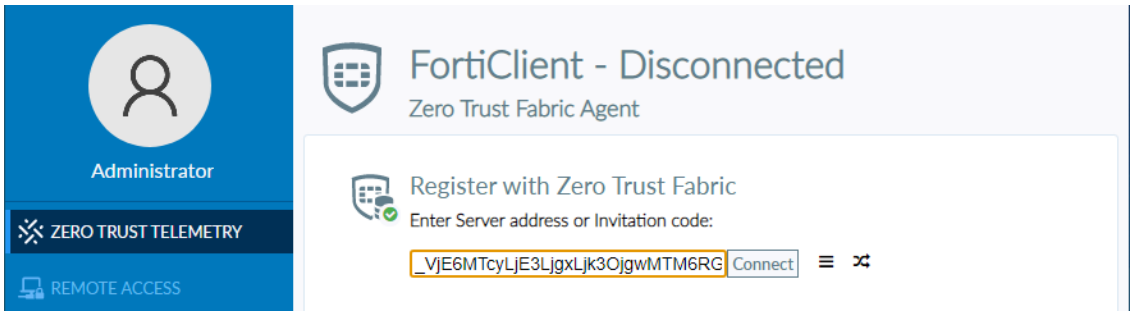
2. In FortiClient on an unregistered endpoint, attempt to register to EMS using the EMS fully qualified domain name. EMS rejects the connection attempt. FortiClient displays an error that EMS require an invitation code.



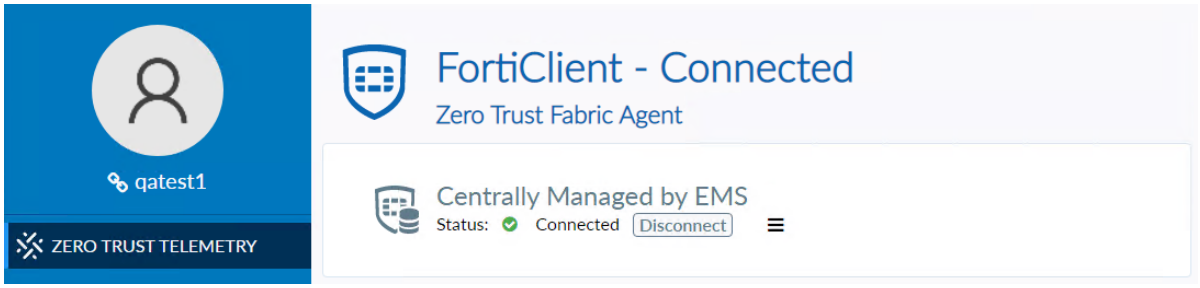
3. Register FortiClient to EMS:
   a. Do one of the following to start the process of registering FortiClient to EMS:
      i. Open the invitation email. and click *Register to EMS*. Follow the instructions to register to EMS.



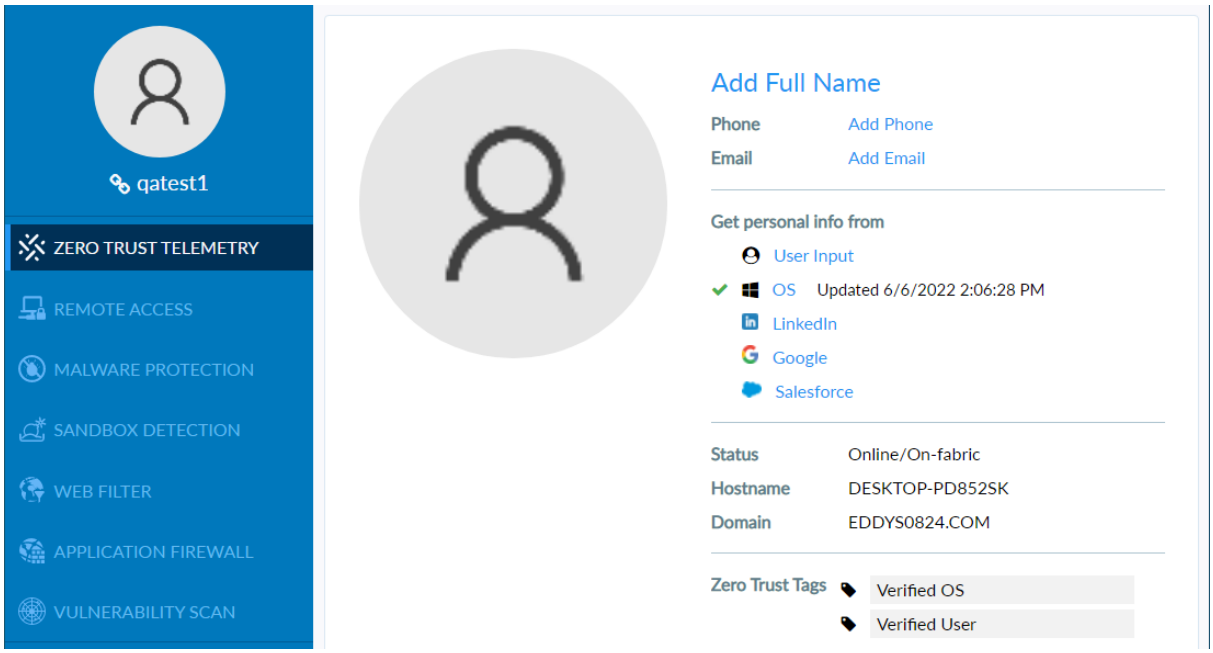
      ii. Open the invitation email, and copy the invitation code. Enter the invitation code on the *Zero Trust Telemetry* tab, and click *Connect*.



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.

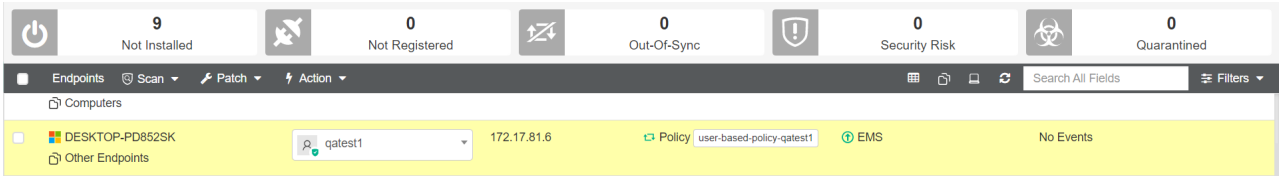


4. Go to the About page to confirm that the Verified User tag displays.

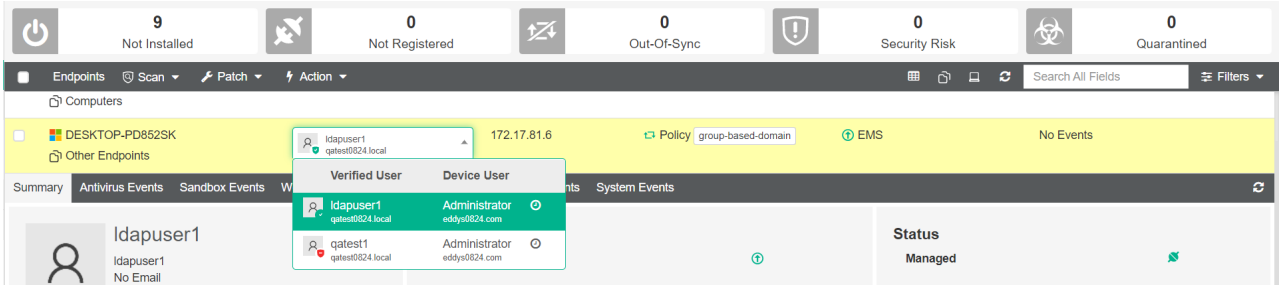


5. In EMS, go to *Endpoint Policy & Components* > *Managed Policies*. Create a policy to apply to the selected user. In the *Users* field, select the desired user. This policy takes priority over group-based policies that the endpoint may also be eligible for.

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

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):

This is necessary for registering an Entra ID endpoint to EMS using an invitation code. This only applies for Entra ID-joined endpoints. This feature is supported just on Microsoft Windows endpoints with `AzureAdJoined : YES` in the output from `dsregcmd /status`.

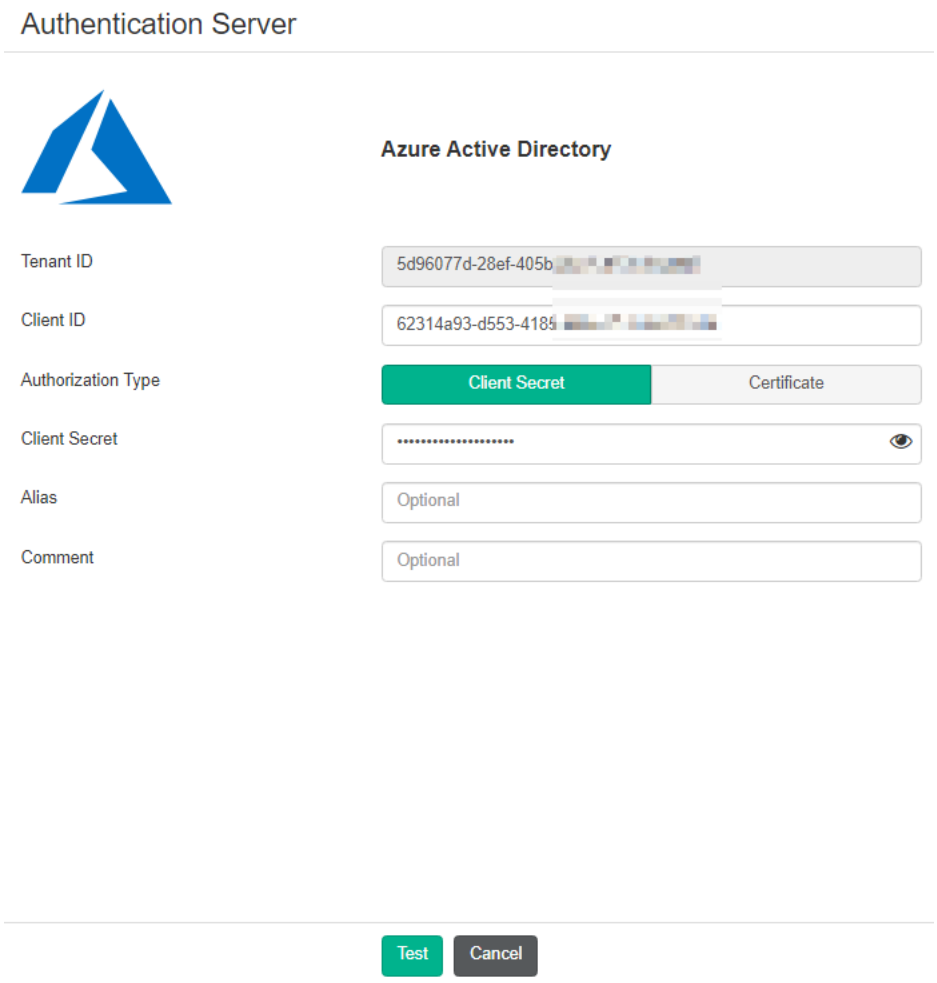
1. Configure the redirect URL:
   a. In the Azure portal, go to *App registration*. Copy the application/client ID of the application used to connect with EMS.
   b. Click the application, then click the *Redirect URIs* link.
   c. Click *Add a Platform* > *Select Mobile and Desktop applications*.
   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.

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*.

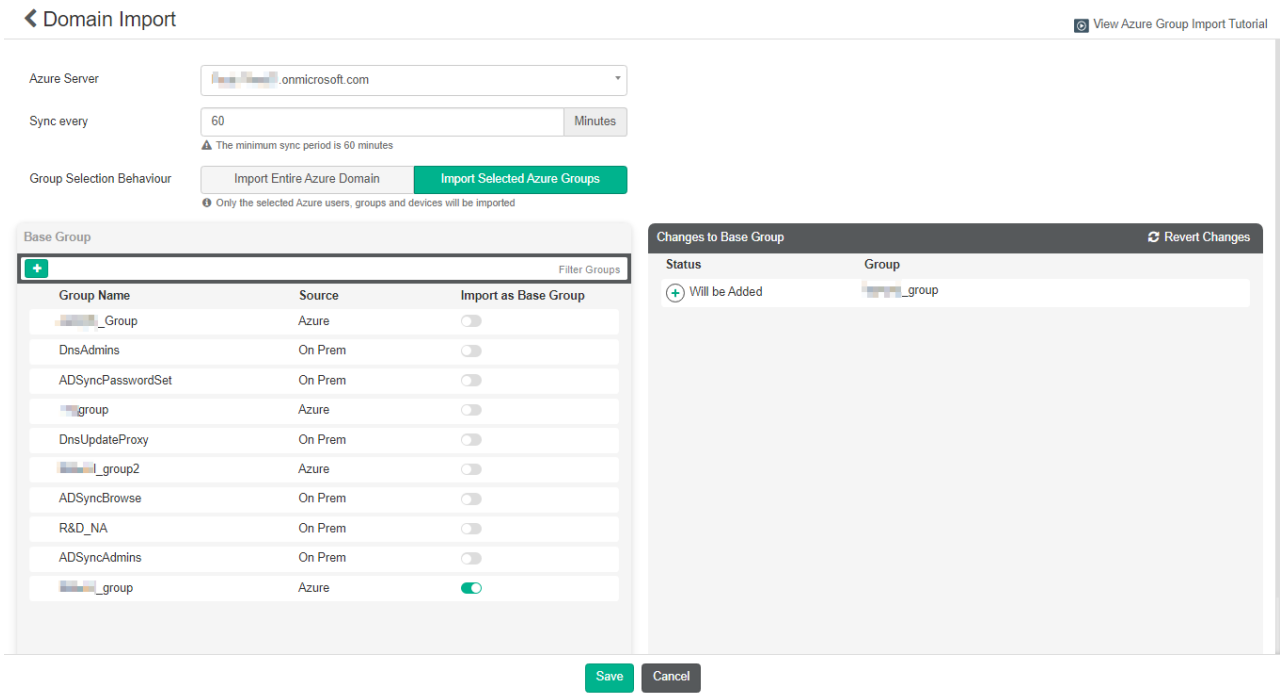


i. After the test succeeds, click *Save*.

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 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 other settings as desired, then click *Save*.
2. On the endpoint, go to *Settings* > *Accounts*.
3. Click *Join this device to Azure Active Directory*.
4. Under *Access work or school*, click *Connect*.
5. Log in as an Entra ID user.
6. 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

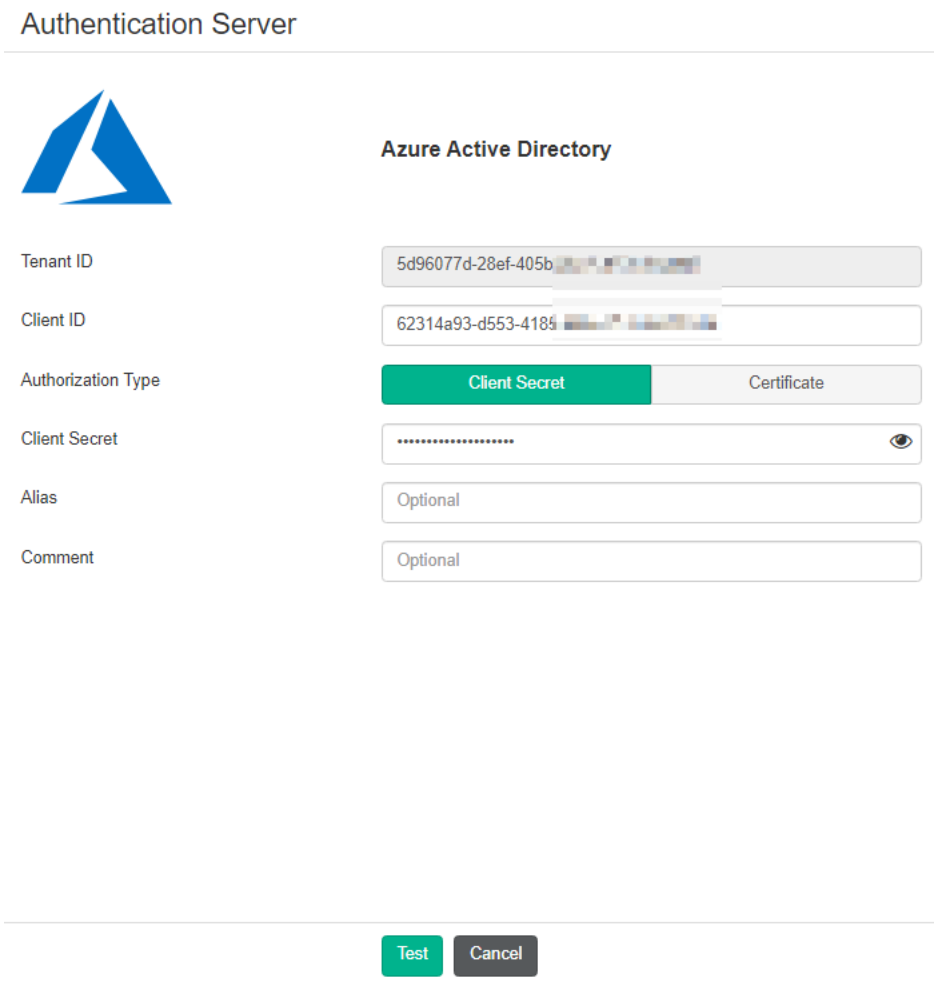
The following provides an example of configuring user verification, using a Microsoft Entra ID (formerly known as Azure Active Directory (AD)) server for authentication. This configuration consists of the following steps:

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*.

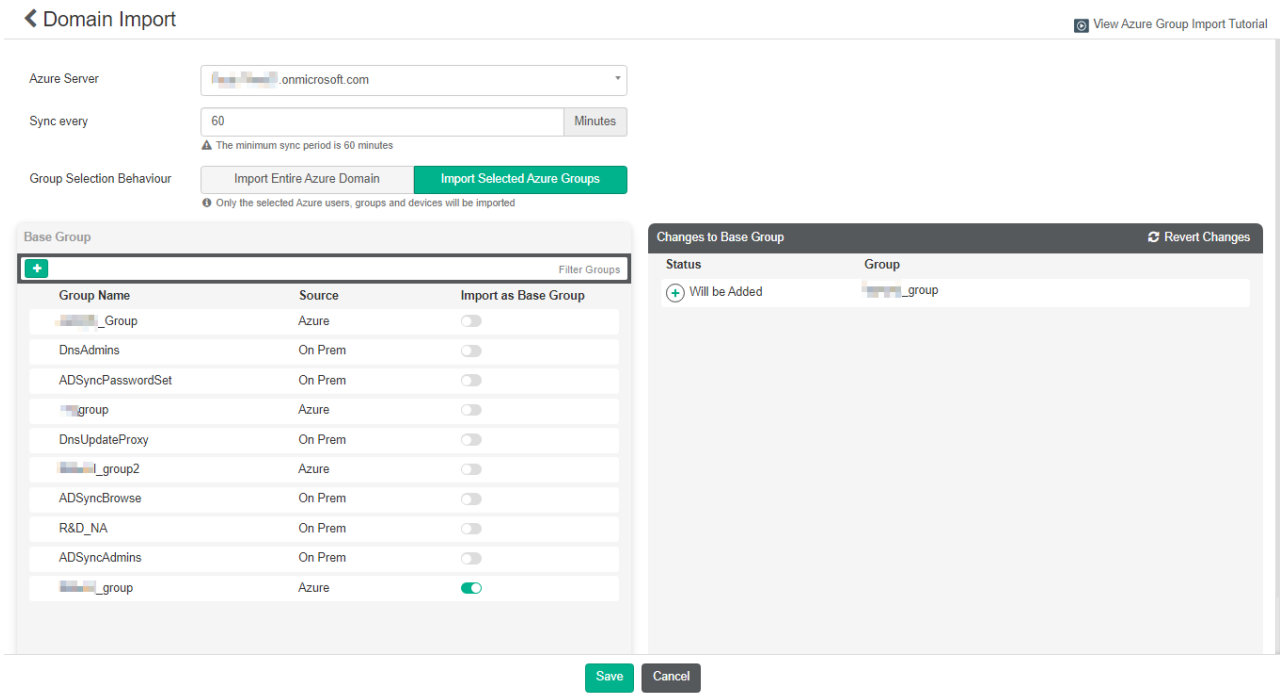


i. After the test succeeds, click *Save*.

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*.

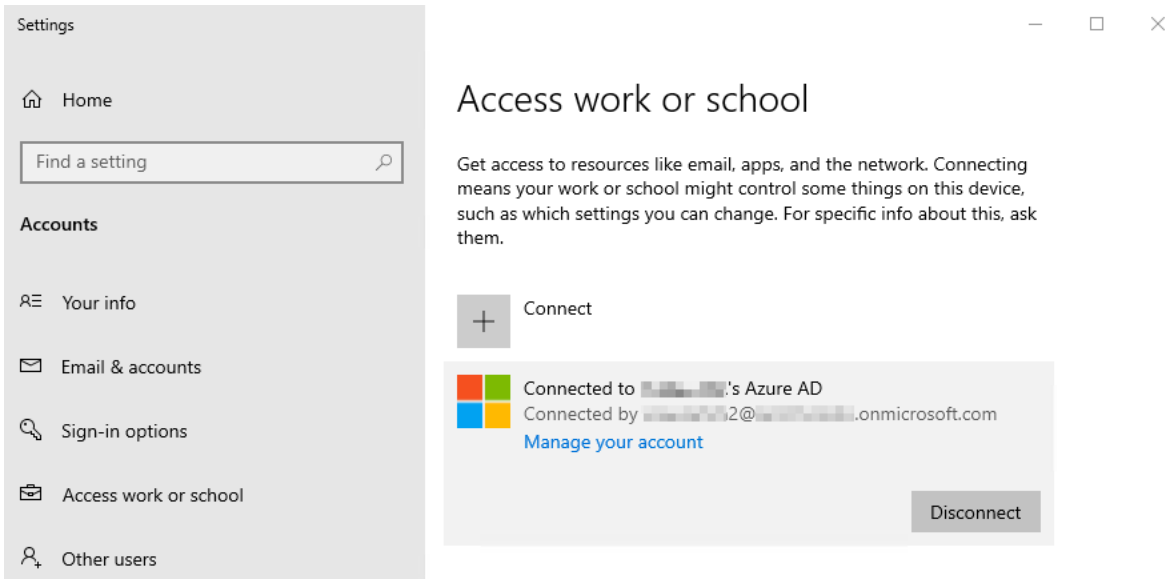


Endpoints > *Domains* lists the Entra ID server domain groups and subgroups. It lists subgroups as a flat list and does not preserve the hierarchy from the Entra ID server.

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:

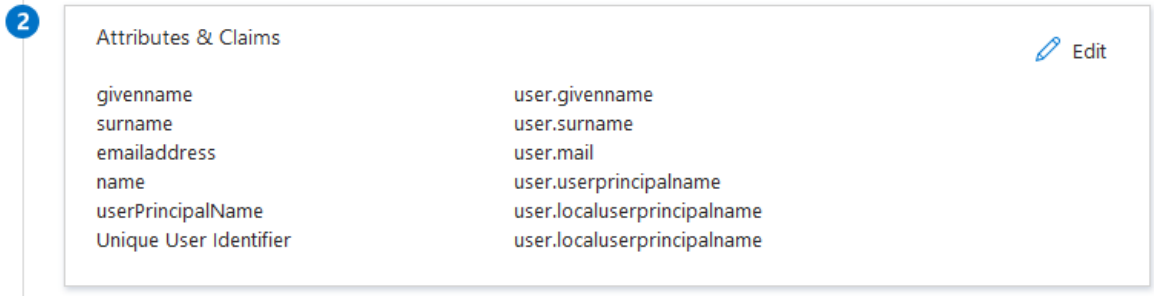
You must copy some values from the Azure portal to EMS and other values from EMS to the Azure portal to complete the configuration.

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*.

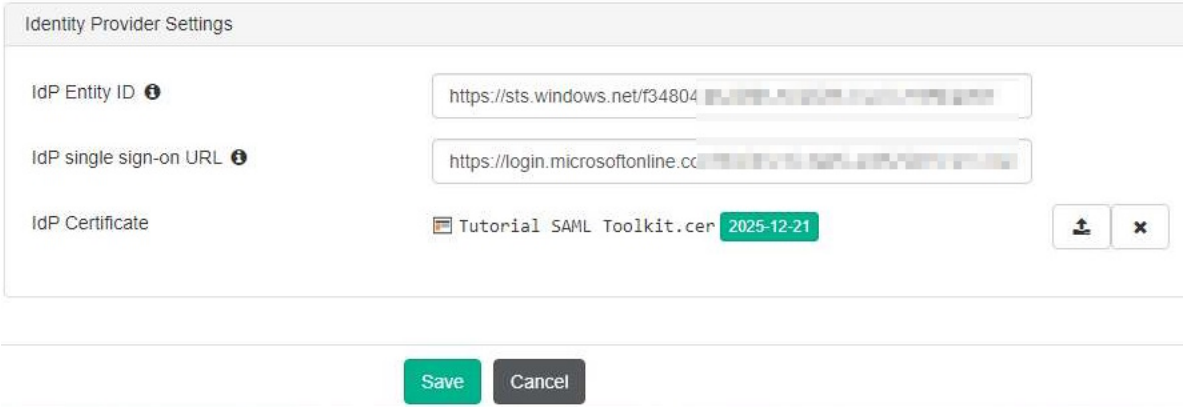
EMS SAML field	Entra ID Basic SAML Configuration field
SP Entity ID	Identifier (Entity ID)

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*.

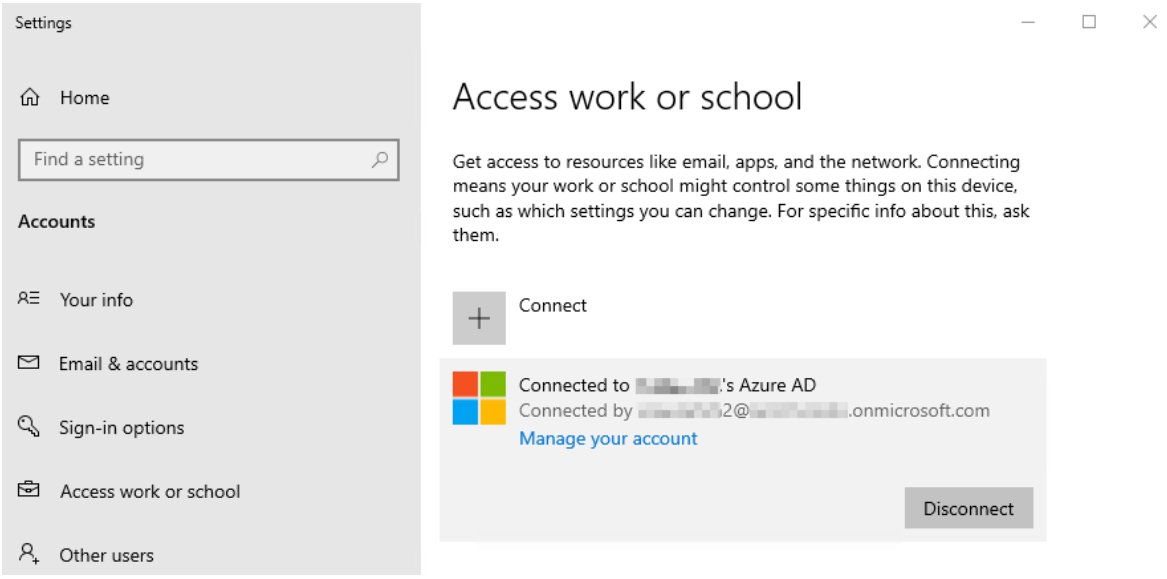


3. In Azure, add a new claim:
   a. Click *Add new claim*.
   b. In the *Name* field, enter the domain identification value from EMS. You can find this value on EMS in *User Management* > *SAML Configuration* > *Assertion Attributes* > *Domain Identification*. This field is only visible when *LDAP* is 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.



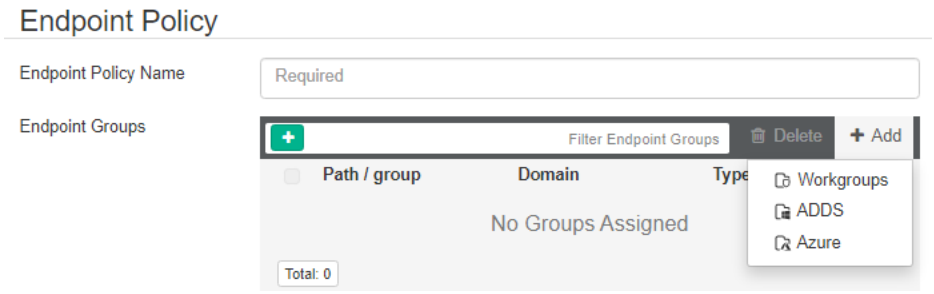
5. In Azure, go to *Users and groups*. Add users to the list as desired. Azure authorizes any user added to this list to connect to EMS.

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 FortiClient EMS:
   a. In FortiClient EMS, 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:

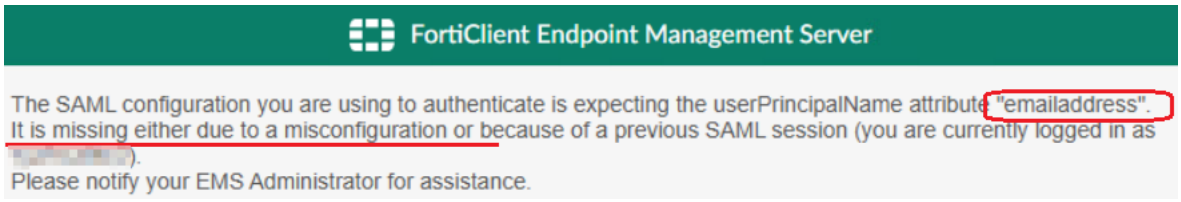
1. In the top banner, click *Invitations*.
2. Click *Add*.
3. For *Verification Type*, select *SAML*.
4. From the *SAML Config* dropdown list, select the Okta SAML configuration.
5. Configure other settings as desired, then click *Save*.
6. In FortiClient, on the *Zero Trust Telemetry* tab, enter the 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).

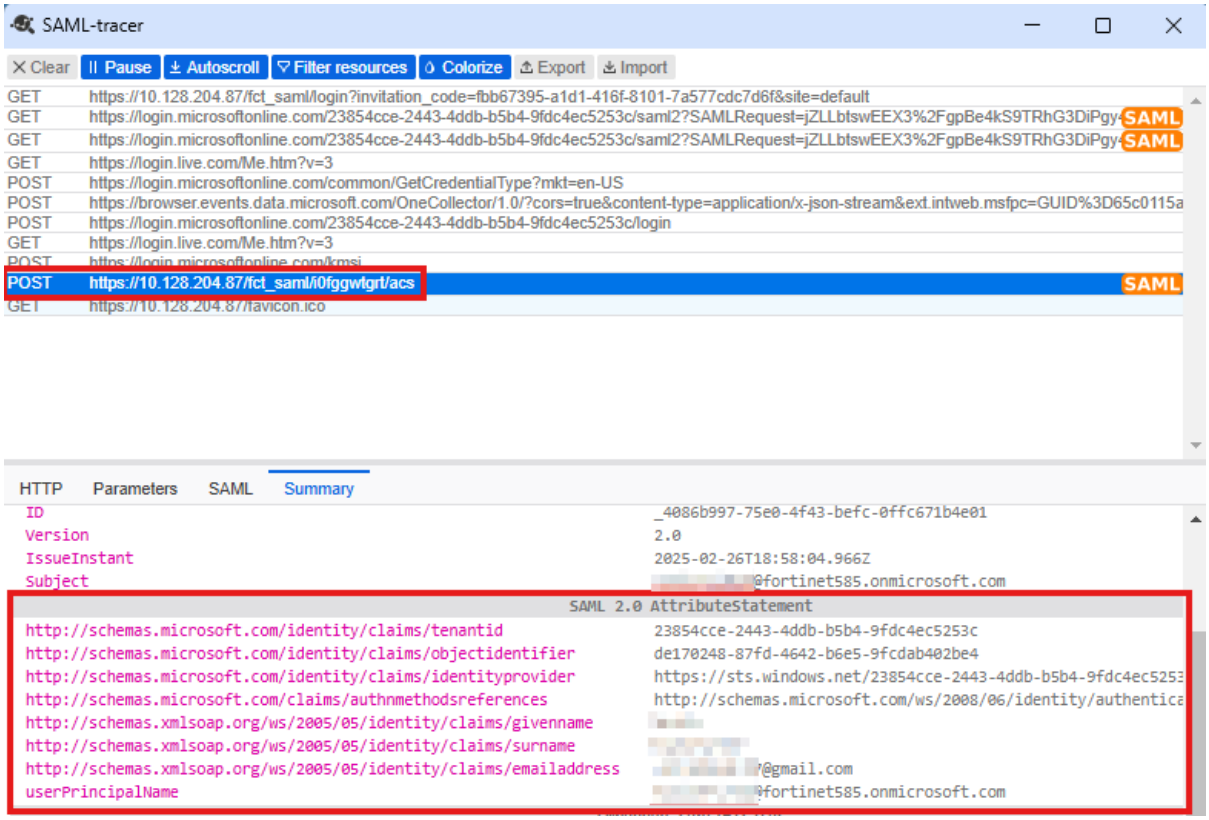
Go to *User Management* > *SAML Configuration* and confirm what is configured in the *Domain Identification* field.



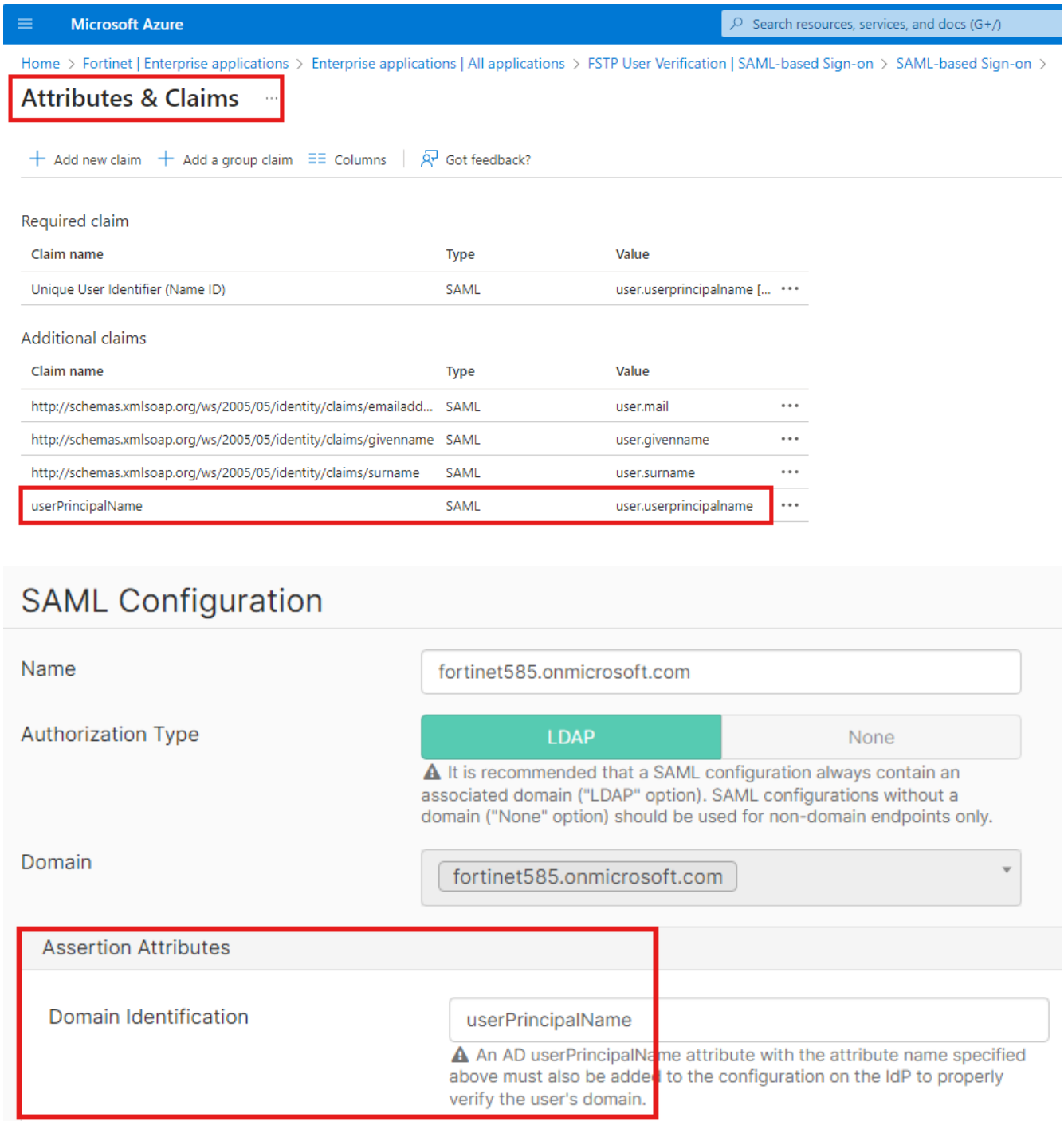
Based on the screenshot, EMS expects the "emailaddress" attribute in the SAML authentication response. This attribute holds the username in userPrincipalName format. EMS matches the domain name from the username value to the configured *Domain*. In this example, EMS matches the domain name against fortinet585.onmicrosoft.com, 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.

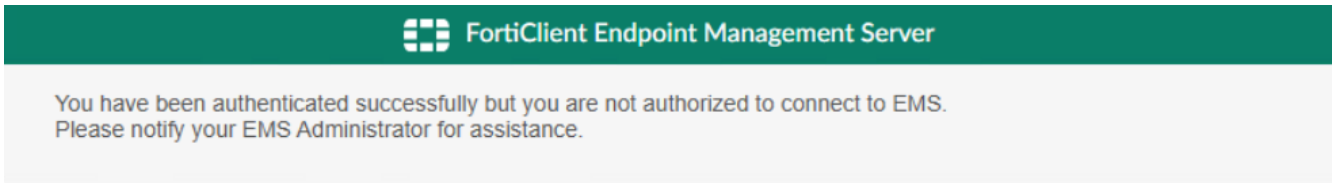


A correct configuration is one where the domain identification attribute configured in EMS matches one on the IdP. The following provides an example of a correct configuration in Entra ID. You can see that the *userPrincipalName* claim exists in the Entra ID portal under *Attributes & Claims* and that this is also configured in the *Domain Identification* field in EMS.

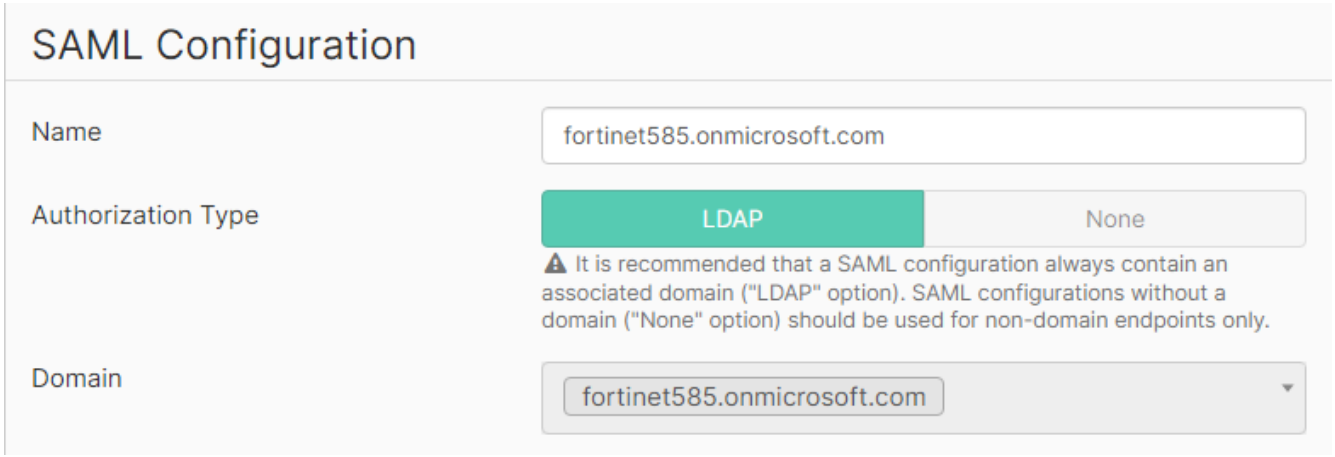


Authenticated but not authorized

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

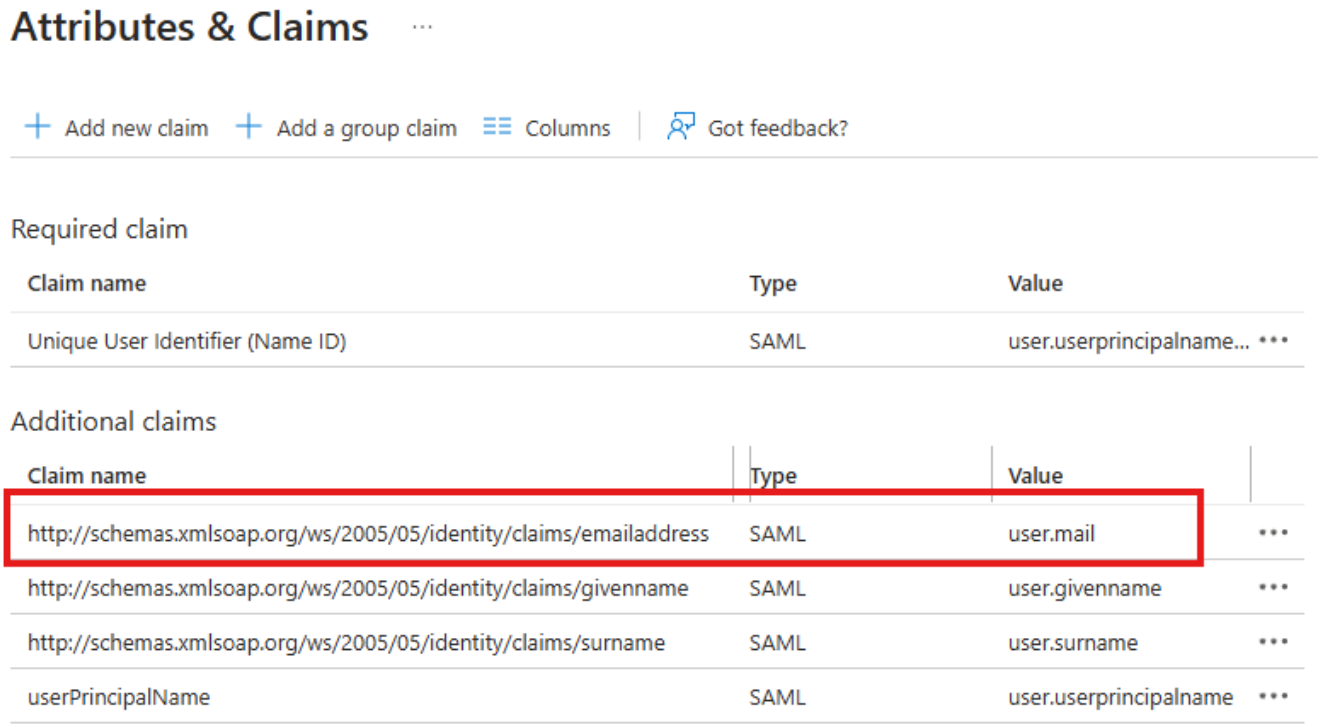
The SAML assertion attribute is misconfigured.

This is similar to Missing attribute on page 620, 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.

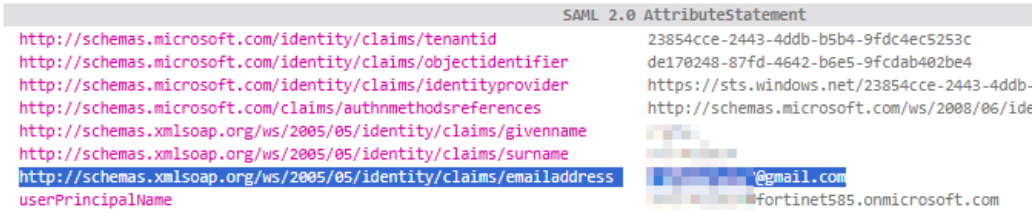
The following screenshots provide an example of this case. In EMS, *Domain Identification* is configured as https://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress.



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.

Domain mismatch

This issue occurs when the domain configured on the IdP does not match the one imported to EMS.

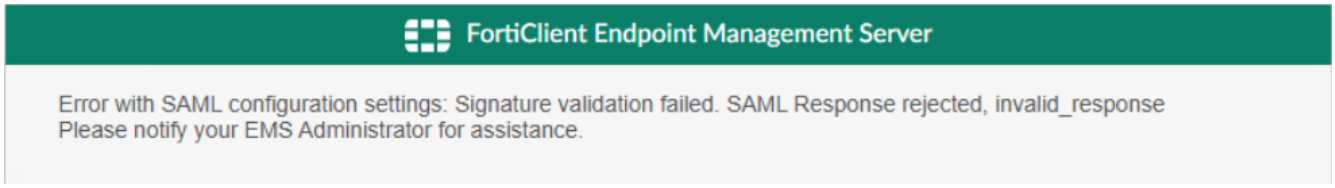
Hybrid environments are common, so you may use SAML for authentication using Entra ID and authorize against an Active Directory Domain Services domain. In this case, the domains' names may differ.

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*.

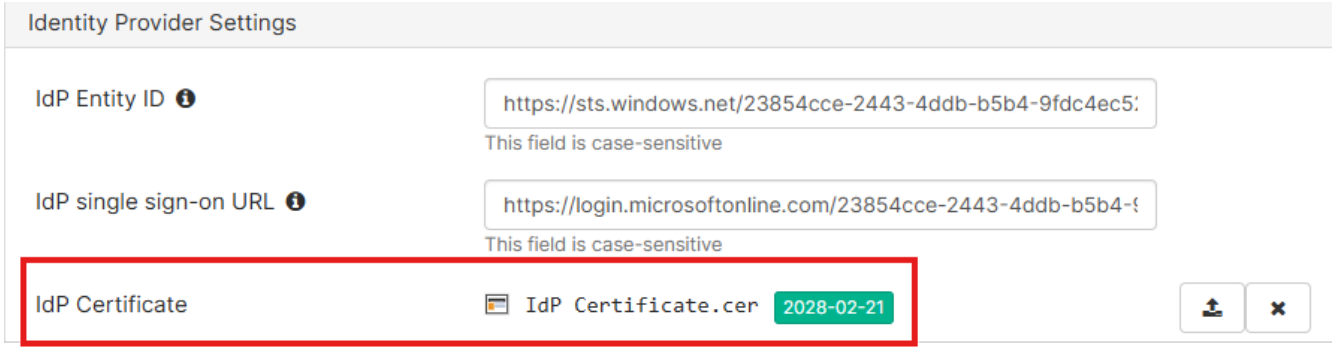
Signature validation failed

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.

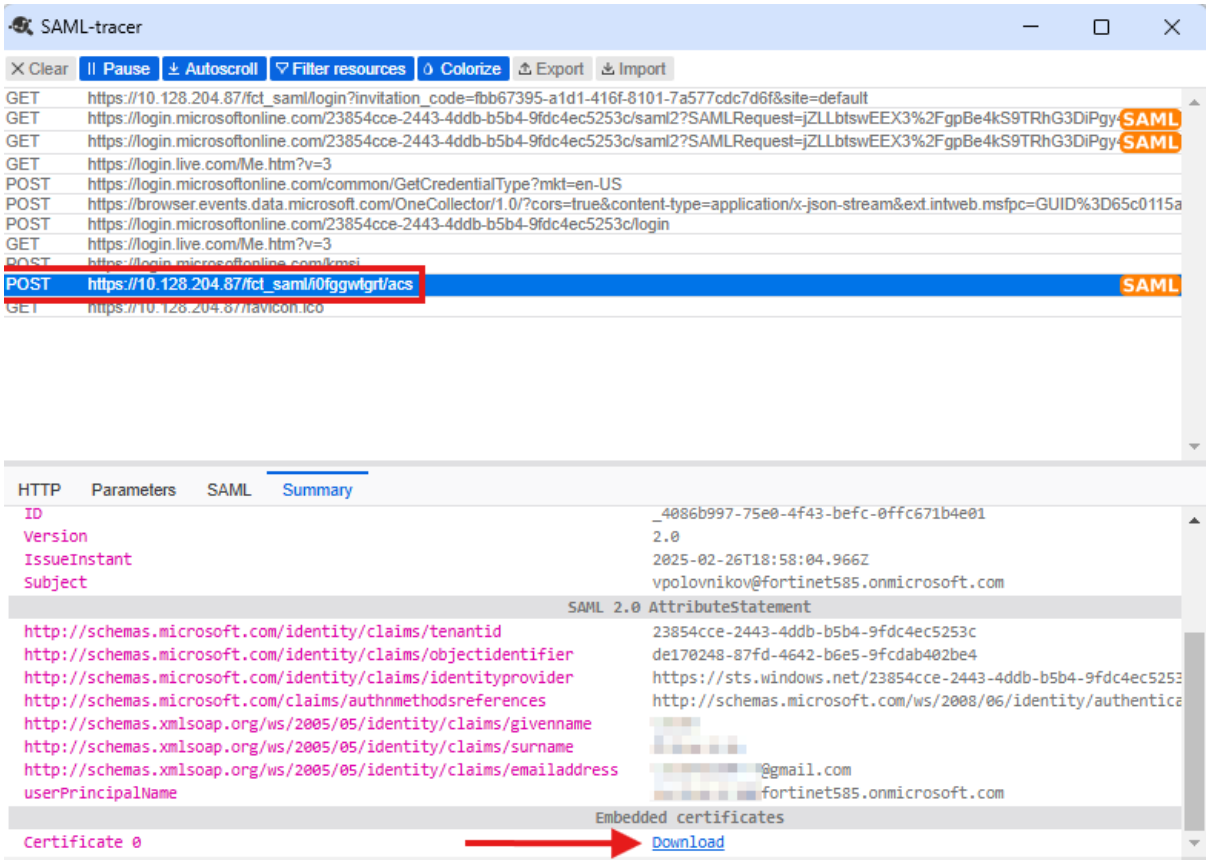
To fix this error, ensure that the certificate coming from the IdP is the same as the one configured on EMS under *IdP Certificate* .



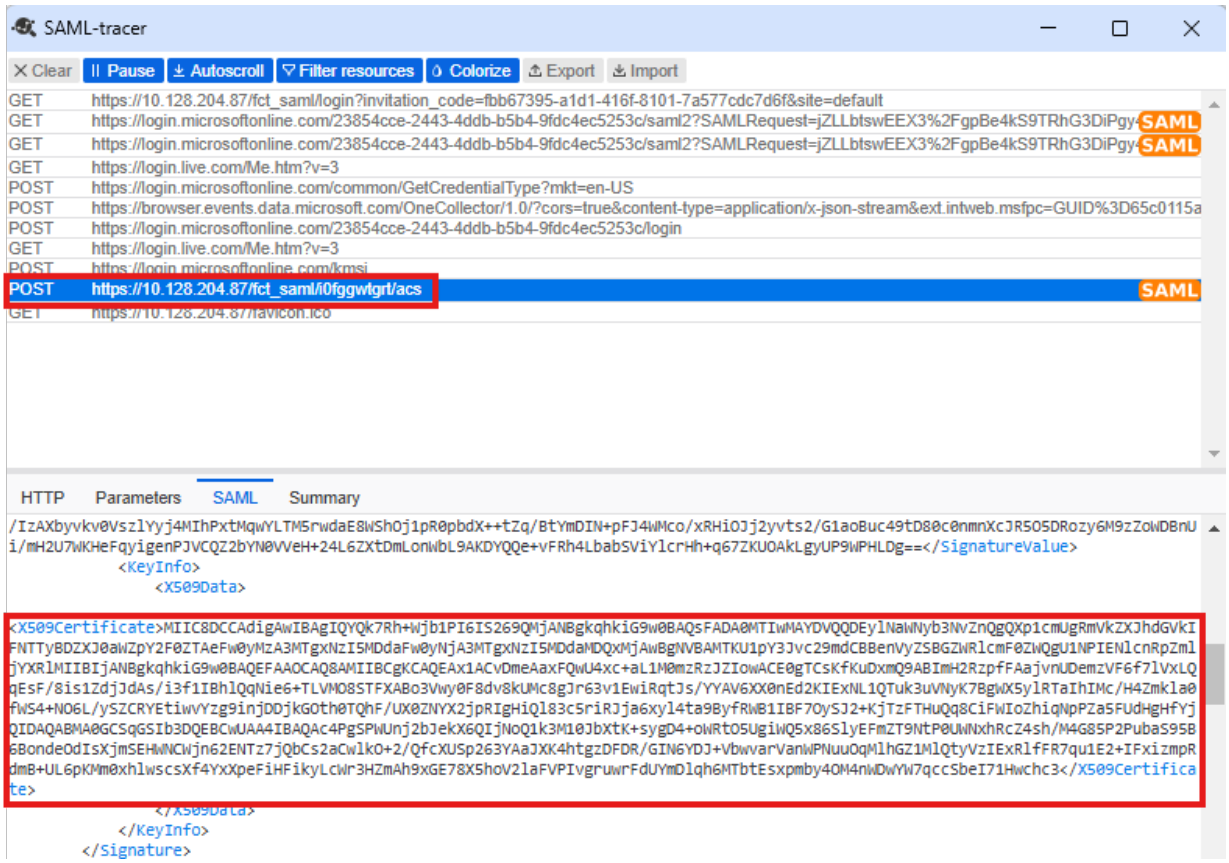
If desired, you can extract the IdP certificate via SAML-tracer.

To extract the IdP certificate via SAML-tracer:

1. Repeat the steps in To debug this error: on page 621.
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

FortiClient EMS installs with a default IP address and port configured. You can change the IP address and port and configure other server settings for FortiClient EMS.

When you enable multitenancy, you must configure some EMS settings at the global level, and other settings at the site level. See Global and per-site configuration on page 662.

To configure EMS settings:

1. Go to *System Settings > EMS Settings*.
2. Configure the following options under *Shared Settings*. EMS uses these settings for FortiClient EMS managing Windows, macOS, and Linux endpoints, and FortiClient EMS managing Chromebook endpoints:

Option	Description
Hostname	Displays the FortiClient EMS server hostname.
Listen on IP	Displays the IP addresses for the FortiClient EMS server. FortiClient connects to FortiClient EMS on the specified IP address. You can generate a QR code for the specified IP address. See Generating a QR code for centrally managing FortiClient (Android) and (iOS) endpoints on page 636.
Use FQDN	Specify a fully qualified domain name (FQDN) for the FortiClient EMS server. FortiClient can connect using the specified IP address in the *Listen on IP Addresses* option or the specified FQDN. FortiClient's connection to EMS is critical to managing endpoint security. Managing this is relatively easy for internal devices. For external devices or devices that may leave the internal network, you must consider how to maintain this connection. FortiClient can connect to EMS using an IP address or FQDN. An FQDN is preferable for the following reasons: • Easy to migrate EMS to a different IP address • Easy to migrate to a different EMS instance • Flexible to dynamically resolve the FQDN

Option		Description
		The third reason is particularly valuable for environments where devices may be internal or external from day to day. When using an FQDN, you can configure your internal DNS servers to resolve the FQDN to the EMS internal IP address and register your external IP address with public DNS servers. You must then configure the device with your external IP address to forward communication received on port 8013 to your EMS internal IP address. This allows your external clients to leverage a virtual IP address on the FortiGate so that they can reach EMS, while allowing internal clients to use the same FQDN to reach EMS directly. Alternatively, you can use a private IP address for the connection. This configuration requires external clients to establish a VPN connection to reach the EMS (VPN policies permitting). This configuration can be problematic if all endpoints need an urgent update but some are disconnected from VPN at that time.
Remote HTTPS access		Specify settings for remote administration access to FortiClient EMS. Enable or disable remote HTTPS access to FortiClient EMS. When enabled, enter a hostname in *Custom Hostname* to let administrators use a browser and HTTPS to log into FortiClient EMS. When disabled, administrators can only log into FortiClient EMS on the server.
	HTTPS Port	Available when you enable *Remote HTTPS Access*. Displays the predefined HTTPS port. You cannot change the port.
	Pre-defined Hostname	Available when you enable *Remote HTTPS Access*. Displays the predefined hostname. You cannot change the name.
	Custom Hostname	Available when you enable *Remote HTTPS Access*. Displays the predefined hostname of the server on which FortiClient EMS is installed. You can customize the hostname. When you change the hostname, the web server restarts.
	Management IP	Available when you enable *Remote HTTPS Access*. If the EMS has an IP address that is usually not publicly reachable but the FortiGate could reach, specify this IP address. In most cases, this is an internal IP address. The FortiOS administrator can use this IP address to connect the FortiGate to the EMS using a Fortinet Security Fabric connector.
	Management Port	Available when you enable *Remote HTTPS Access*. Specify the management port for a FortiGate to use to reach EMS.
	Redirect HTTP Request to HTTPS	Available when you enable *Remote HTTPS Access*. If you enable this option and attempt to remotely access FortiClient EMS at *http://<server_name>*, this automatically redirects to *https://<server_name>*.

Option	Description
Webserver Certificate	Displays the SSL certificate used for the Apache service and the Notify (websockets) daemon. If desired, you can select another certificate from the dropdown list. See EMS Server Certificates on page 647.
Use Webserver certificate for Endpoint Control	Enable to use the certificate uploaded in the *Webserver certificate* field for endpoint control.
Endpoint Control certificate	Displays the SSL certificate currently used on port 8013 for the Endpoint Control daemon. If desired, you can select another certificate from the dropdown list. See EMS Server Certificates on page 647. When this option is enabled and FortiClient tries to connect to EMS using the endpoint control protocol, EMS sends the SSL certificate so that FortiClient can use the certificate to verify the connection. If the SSL certificate is from a publicly signed certificate authority, only endpoints with the following FortiClient versions can connect to EMS: • 6.4.7 and later • 7.0.2 and later
EMS CA certificate (ZTNA)	This feature requires the ZTNA or EPP license and only applies for endpoints running FortiClient 7.0.0 and later versions. See Windows, macOS, and Linux licenses on page 25. Displays the EMS CA certificate expiry. EMS sends this certificate to FortiOS. See FortiClient in the Security Fabric on page 14. 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 640.
Enable ZTNA token	Enable the ZTNA JSON web token (JWT). See JWT support for ZTNA UID and tag sharing on page 637.
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.
Admin Lockout Attempt	Configure the number of unsuccessful login attempts after which EMS locks out the admin. The default is 3 times. The maximum is 10 times.

Option	Description
Admin Lockout Period	Configure the number of seconds that EMS locks out an admin for after they have reached the number of unsuccessful login attempts configured in *Admin Lockout Attempt*. During the admin lockout period, any login attempt does not succeed, even if the admin provides correct credentials. Each login attempt during the lockout period causes the admin lockout period to reset and begin again. After the configured admin lockout period passes, the lockout resets and the admin can again attempt to log in multiple times per the number of attempts configured in *Admin Lockout Attempt*. If they again reach the maximum number of attempts, the admin lockout period begins again.

3. Configure the following options under *EMS Settings*. FortiClient EMS uses these settings when managing Windows, macOS, and Linux endpoints:

Option	Description
Listen on port	Displays the FortiClient EMS server default port. You can change the port by typing a new port number. FortiClient connects using the specified port number.
Use persistent connections	Allow FortiClient to create a persistent connection with EMS. This feature allows it to not tear down and renegotiate the TLS connection at every keepalive (KA) interval.
FortiOS Connector port	Displays the default port that FortiClient EMS uses to connect to FortiOS, where FortiClient EMS is the server and FortiOS is a client. You can change the port by typing a new port number. FortiOS connects using the specified port number.
FortiClient download URL	FortiClient deployment packages created in FortiClient EMS are available for download at this URL.
Open port 10443 in Windows Firewall	Open port 10443 or close port 10443. Port 10443 is used to download FortiClient.
High Availability Keep Alive Interval	Configure the keepalive (KA) interval between the EMS high availability (HA) nodes in seconds. If EMS cannot detect the primary node after 2 keepalive intervals and 60 seconds, HA failover is triggered. The default KA interval value is 10 seconds. For example, if you retain the default value of 10 seconds, HA failover is triggered after 80 seconds (10* 2 + 60 = 80).
Enforce User Verification	Enforce user verification for endpoints. Users must log in to verified user accounts to register to EMS. See Invitations on page 599.

Option	Description
Enforce invitation-only registration for	Enforce invitation-only registration for some or all users. When you select all, FortiClient can only register to EMS using an invitation. See Invitations on page 599.
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.
Sign software packages	Enable this option to have Windows FortiClient software installers created by or uploaded to FortiClient EMS digitally signed with a code signing certificate.
Timestamp server	Enter the server address to timestamp software installers with.
Certificate	Upload the desired code signing certificate. This must be a .pfx file. After a certificate has been uploaded, its expiry date is also displayed.
Password	Enter the certificate password. This is required for FortiClient EMS to sign the software installers with the certificate.
Configure EMS server list	Select an option from the dropdown list. Users can configure this IP address in *Shared Settings > Listen on IP*.
Connect to local subnets only	Only allow connection to local subnets.
Enable login banner	When you enable the login banner, a message appears prior to a user logging into FortiClient EMS. In the *Message* field, type your message. The *Preview* section displays a preview of the message.
Let EMS schedule automatic upgrade	Enable or disable automatic upgrade behavior. EMS enables this option by default. See Automatically upgrading EMS to latest patch release on page 39.

4. If managing Chromebooks, enable *EMS for Chromebooks Settings*. You may need to restart FortiClient EMS after enabling this option.
5. Configure the following options under *EMS for Chromebooks Settings*. These settings are used by FortiClient EMS managing Chromebook endpoints:

Listen on port	Displays the default port for the FortiClient EMS server for Chromebooks. You can change the port by typing a new port number. The FortiClient Web Filter extension on Chromebooks connects to FortiClient EMS 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).
Chromebook certificate	Displays the SSL certificate currently used for the Chromebook daemon. If desired, you can select another certificate from the dropdown list. See EMS Server Certificates on page 647.
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.
ID	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*:

Field	Description
FortiClient telemetry connection key	Add the FortiClient Telemetry connection key for FortiClient EMS. 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 636.
Keep alive 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.

Field	Description
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.
EMS license timeout	Configure the number of days after the endpoint has not contacted EMS that EMS removes that endpoint's registration record from EMS.
FortiClient license timeout	Configure the number of days after the endpoint has not contacted EMS that EMS removes the license from FortiClient. This setting only applies for endpoints running FortiClient 6.4.
Delete 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 594 . 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 FortiClient EMS 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. Enable *Manage Multiple Customer Sites*. This enables multitenancy for EMS.
8. Configure the following options under *EMS FSSO Settings*. These settings add SSL encryption to the Fortinet single sign on protocol between EMS and FortiOS.

SSL certificate	Displays the SSL certificate currently imported. If you have already uploaded an SSL certificate, a *Replace* button displays.
Certificate	Browse and upload a new SSL certificate file.
Password	Configure a new SSL password.

9. Click *Save*.

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 FortiClient EMS.

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 *View QR Code*.
   - To generate the QR code with a connection key, ensure that *FortiClient Telemetry Connection Key* is populated, then click *View QR Code* beside it.
3. Click *Download*.
4. 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.

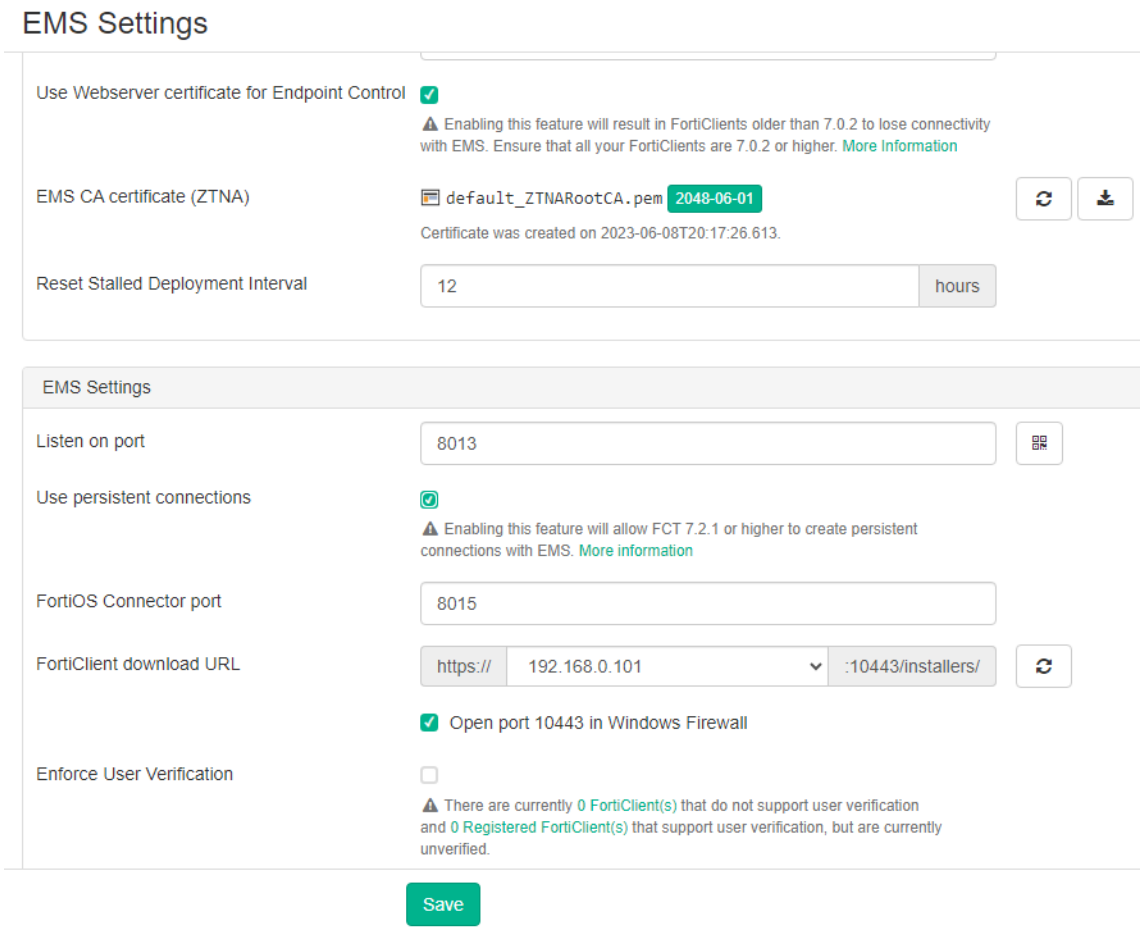
Persistent connection

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.

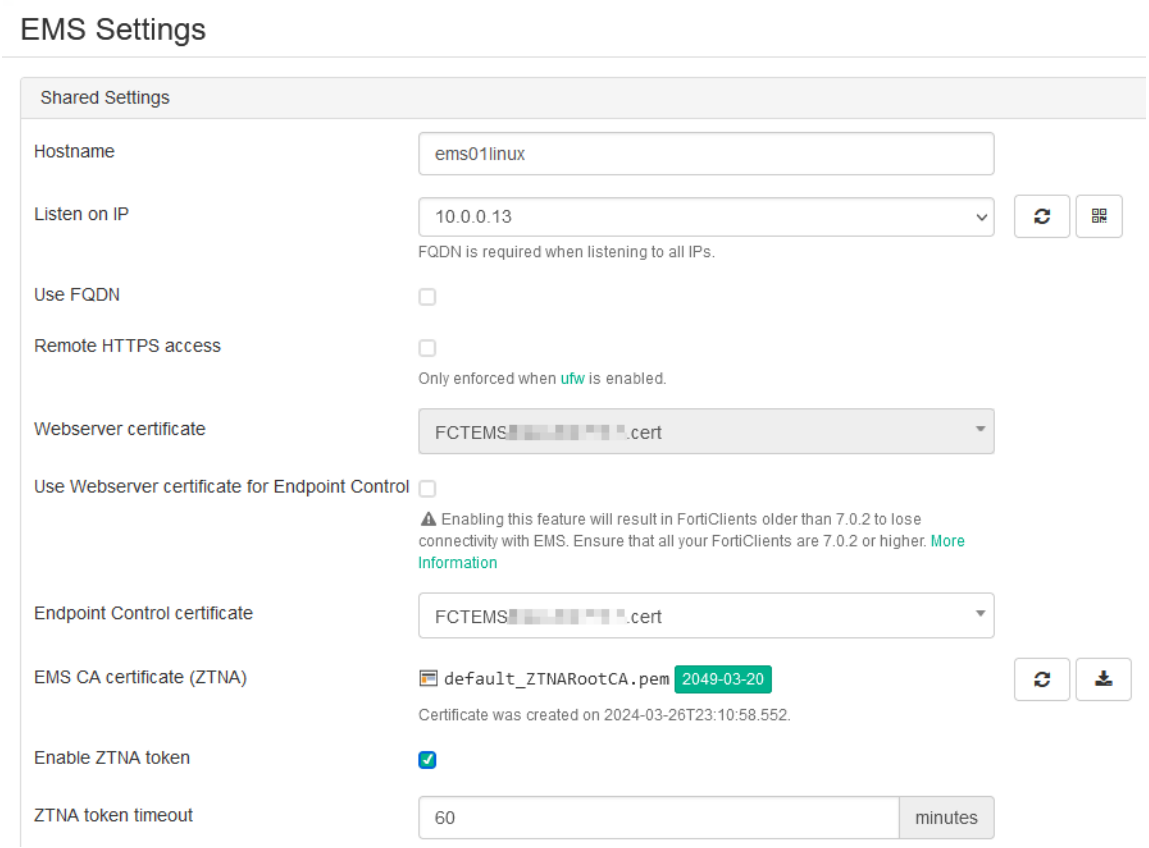
Prior to the addition of JWT support, in the event of connection loss between FortiClient and EMS or a Fabric connection issue between EMS and FortiOS, legitimate endpoints could not access remote resources via a ZTNA server.

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:

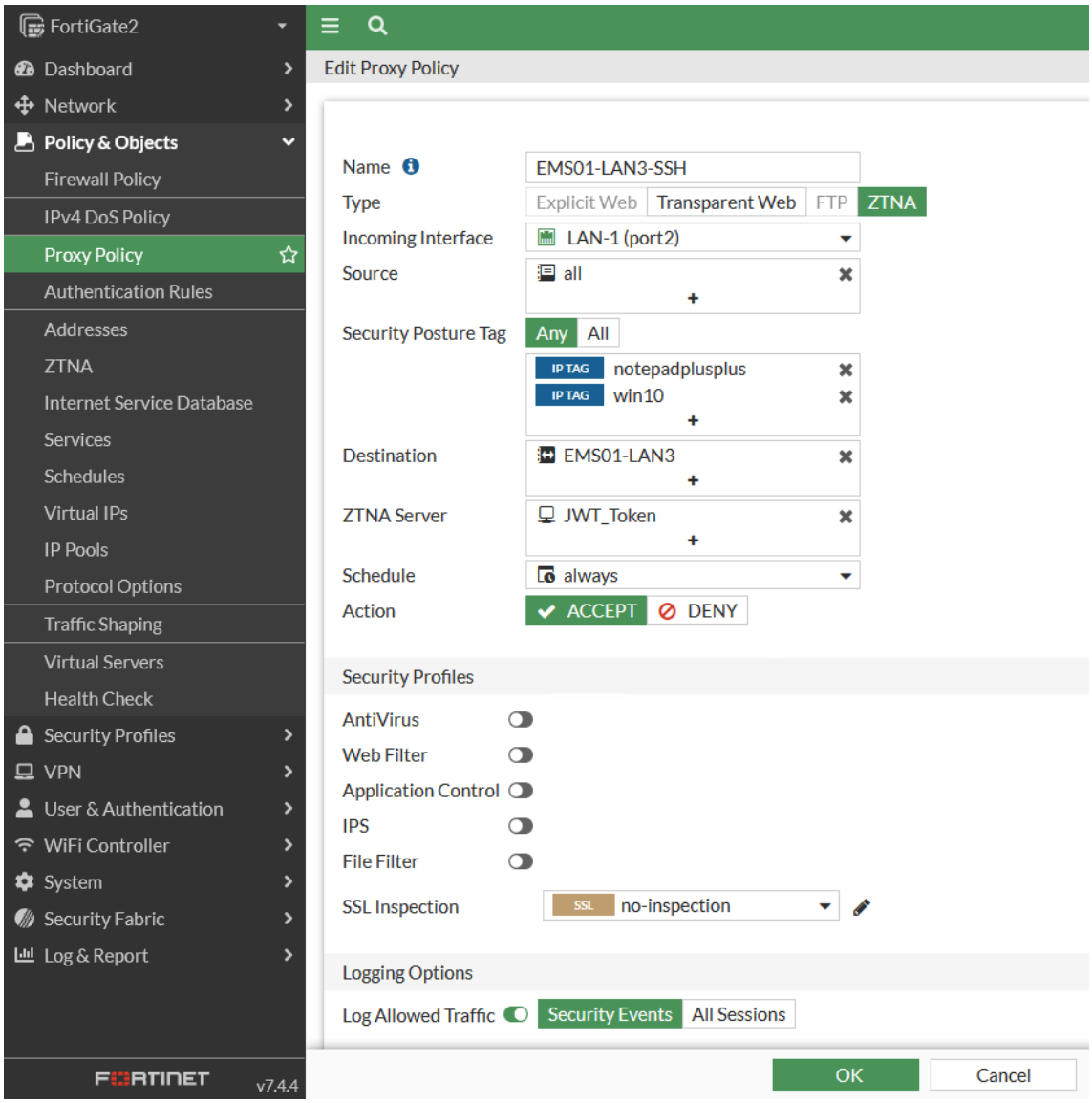
1. Configure the feature in EMS:
   a. Configure *EMS Settings*:
      i. Go to *System Settings > EMS Settings*.
      ii. Click *Enable ZTNA token*.
      iii. In the *ZTNA token timeout* field, enter the JWT expiry time in minutes. The minimum and default value is 60 minutes. When the expiry time 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:

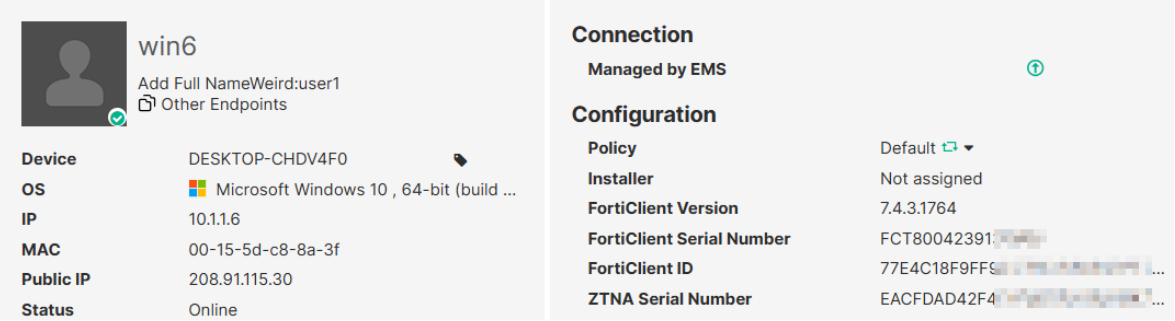
- 1.3.6.1.4.1.12356.101.15.1.102 (EMS serial number (SN))
- 1.3.6.1.4.1.12356.101.15.1.101 (tenant ID)

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

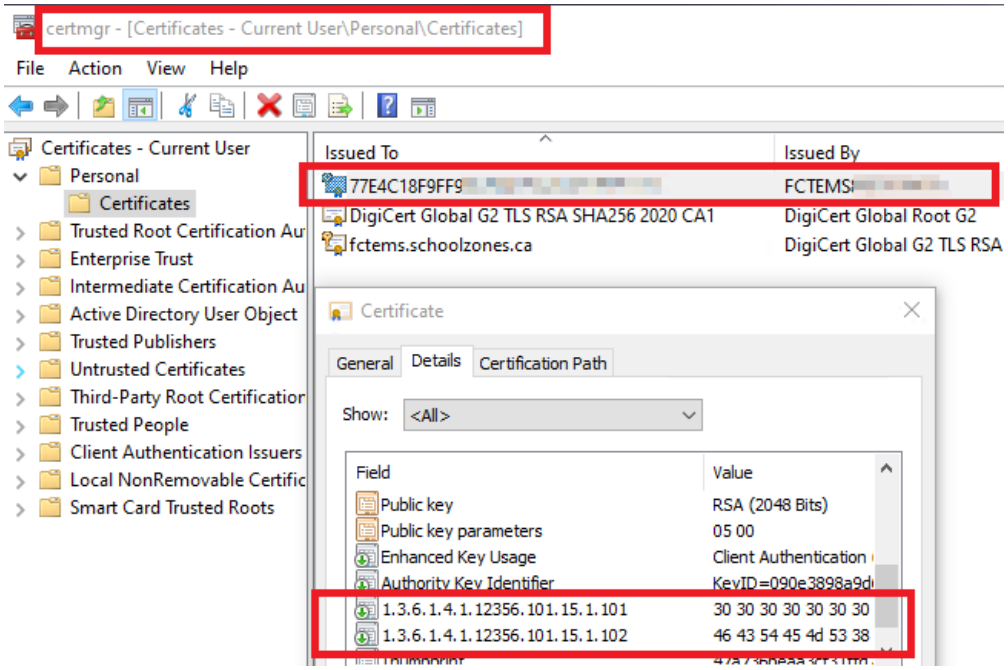
To upload a custom CA certificate:

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)



Configuring Logs settings

You can specify what level of log messages to capture in the logs for FortiClient EMS. 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 FortiClient EMS logs. For example, if you select *Info*, all log messages from *Info* to *Emergency* are added to the FortiClient EMS 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 FortiClient EMS logs or alerts.
Send system log messages externally	Select one of the following: • *Disabled*: FortiClient EMS does not send system log messages to an external server. • *FortiAnalyzer*: configure a FortiAnalyzer for FortiClient EMS 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 642. • *SysLog*: configure a syslog server for FortiClient EMS 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

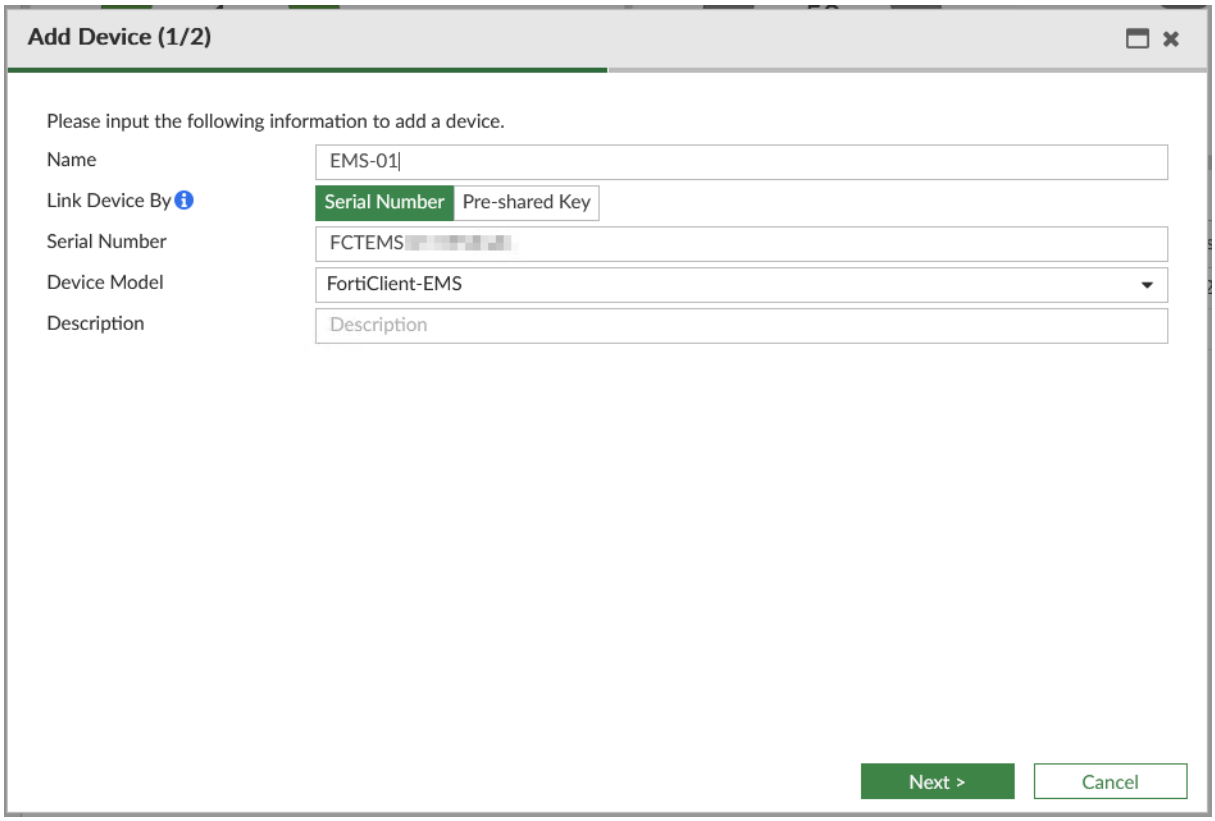
EMS can send server logs to FortiAnalyzer for reporting and investigation. For audit purposes, you should log all admin activity.

To configure sending EMS system log messages to FortiAnalyzer:

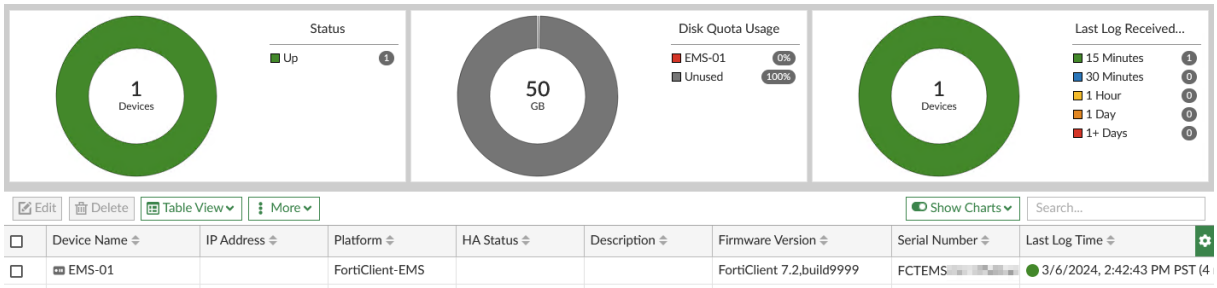
1. Authorize the EMS in FortiAnalyzer to allow FortiAnalyzer to receive logs from the EMS instance:
   a. In FortiAnalyzer, go to *Device Manager*.
   b. Click *Add Device*.

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*.

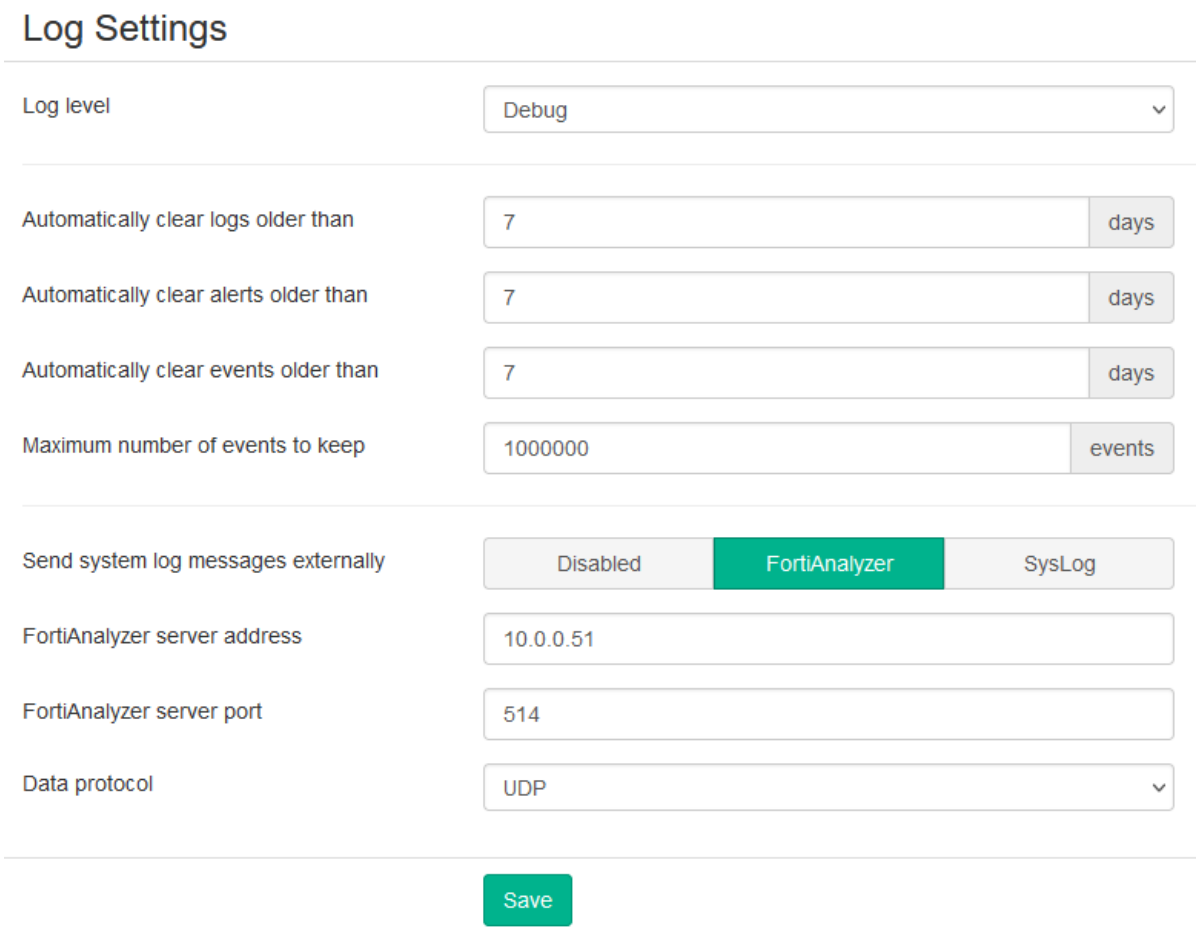


EMS is added as an authorized device and FortiAnalyzer is ready to receive its logs.

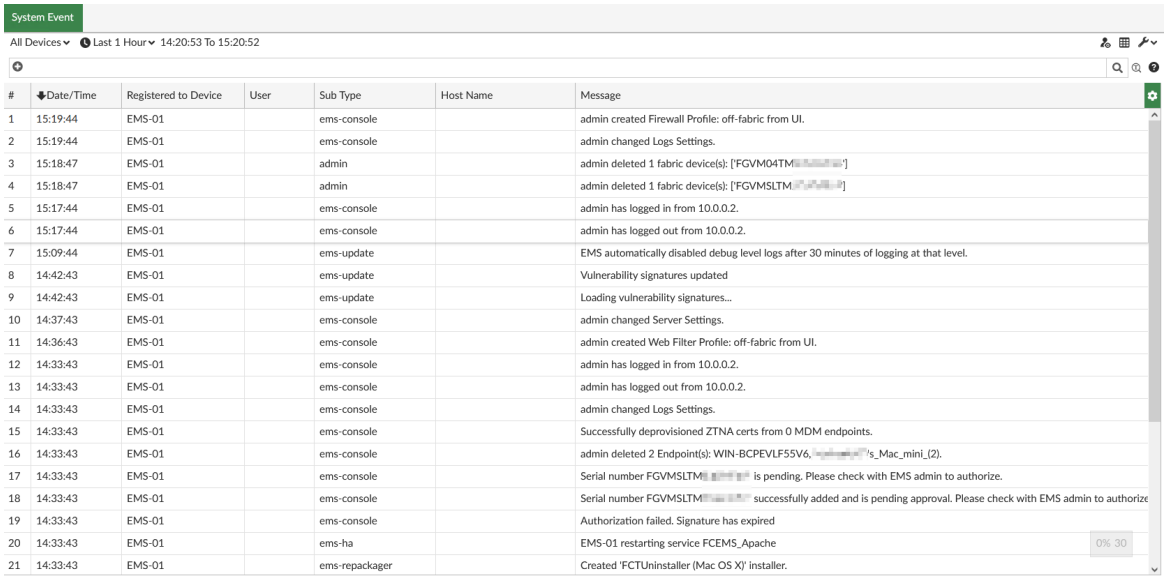


2. In EMS, go to *System Settings > Log Settings*.
3. For *Send system logs externally*, select *FortiAnalyzer*.
4. In the *FortiAnalyzer server address* field, enter the FortiAnalyzer server IP address.
5. In the *FortiAnalyzer server port* field, configure the desired port. This example keeps the default 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.



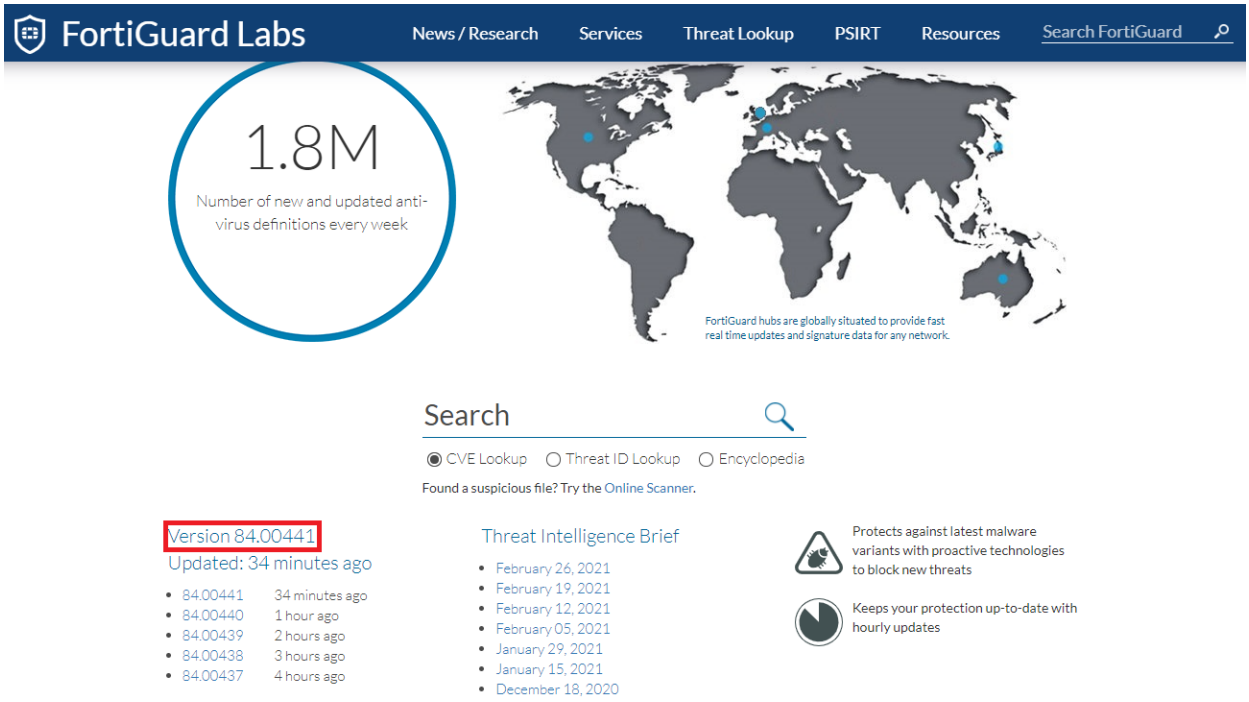
Configuring FortiGuard Services settings

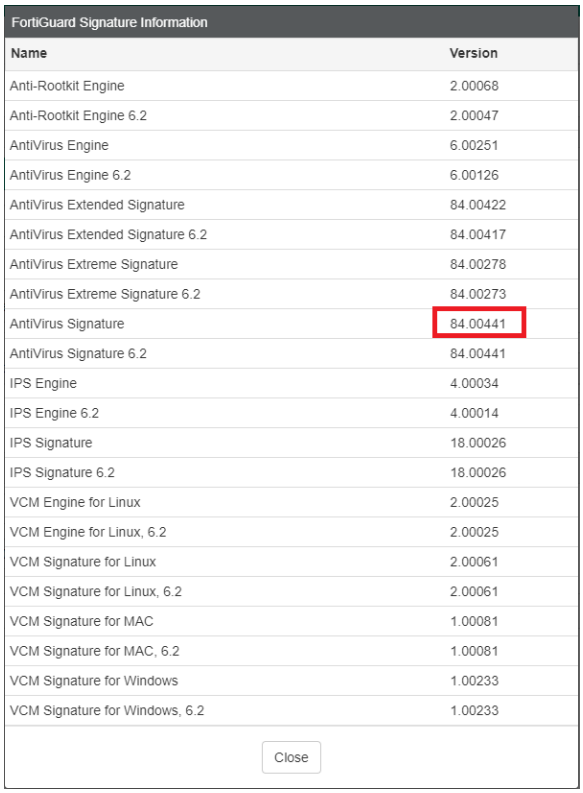
FortiClient relies on several signature databases to identify and stop malware. Keeping these database up-to-date to remain protected from new threats as they are identified is imperative.

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 650.

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.





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*.

EMS Server Certificates

You can view and manage certificates from *EMS Server Certificates*.

EMS supports the following certificate types:

Type	Description
Default	EMS uses this certificate when there are no other available certificates. You cannot delete this certificate. Using the other certificate types is recommended. When other certificates are present, you cannot select the default certificate for use.
Uploaded	User-uploaded certificates. You can upload certificates in PEM, DER, or PKCS12 format. See Adding an SSL certificate to FortiClient EMS on page 648.
ACME	The public Let's Encrypt certificate authority uses the Automated Certificate Management Environment (ACME), as defined in RFC 8555, to provide free SSL server certificates. You can configure FortiClient EMS to use certificates managed by Let's Encrypt and other certificate management services that use the ACME protocol. See Adding an SSL certificate to FortiClient EMS on page 648.
FortiCare	When you apply or renew a license on EMS, EMS retrieves FortiCare-generated certificates with the license information. These certificates are named FCTEMS<serial number>.1.cert and FCTEMS<serial number>.2.cert. While browsers normally do not trust these certificates, they are preferred over the default certificate. In the case that only these certificates and the default certificate are available, EMS uses these certificates, with a preference for .1.cert over .2. cert. You cannot delete these certificates.

EMS uses certificates for the following services. If EMS uses a certificate for a certain service, *EMS Server Certificates* displays this information in the *Assigned To* column:

Service	Description	Ports used
Webserver	Apache service and the Notify (websockets) daemon. Any browser connecting to EMS must trust this certificate. Otherwise, a warning displays. You can configure the certificate for this service in *System Settings > EMS Settings > Shared Settings*. See Configuring EMS settings on page 629.	Apache service: • 443 (GUI) • 10443 (installers) Notify (websockets) daemon: 8015
Endpoint control	Endpoint Control daemon. You can configure the certificate for this service in *System Settings > EMS Settings > Shared Settings*. See Configuring EMS settings on page 629.	8013
Chromebook	Chromebook daemon. You can configure the certificate for this service in *System Settings > EMS Settings > EMS for Chromebooks Settings*. See Configuring EMS settings on page 629.	8443

You can delete certificates from *EMS Server Certificates*. If an ACME certificate is eligible for renewal (within 30 days of expiry), you can also select the certificate to renew it.

Adding an SSL certificate to FortiClient EMS

The following procedures describe how to configure an ACME certificate or manually upload a certificate to EMS. The other certificate types do not require user upload or configuration.

To configure an automated SSL certificate in FortiClient EMS:

1. Go to *System Settings > EMS Settings*.
2. Ensure that *Remote HTTPS Access* and *Redirect HTTP Request to HTTPS* are enabled. Externally accessing EMS via ports 80 and 443 using the configured fully qualified domain name (FQDN) is possible.
3. Add an automated certificate:
   a. Go to *System Settings > EMS Server Certificates*.
   b. Click *Add*.
   c. For *Type*, select *Automated*.
   d. In the *Domain* field, enter the EMS FQDN. For the Let's Encrypt server to issue the certificate, the public DNS server must resolve the EMS FQDN to the EMS public IP address.
   e. In the *Email* field, enter a valid email address.
   f. If desired, enable *Auto Renew*. When you enable *Auto Renew*, FortiClient EMS automatically renews the certificate before expiry.
   g. If desired, expand *Advanced* to configure a certificate authority (CA) server address and HTTP challenge port to communicate with an alternative public CA.

h. Select the checkbox to agree to Let's Encrypt's terms of service.
i. Click *Import*.

To manually upload an SSL certificate in FortiClient EMS:

1. Go to *System Settings > EMS Server Certificates*.
2. Click *Add*.
3. For *Type*, select *Upload PKCS12* or *Upload PEM*.
4. In the *Certificate* field, browse to and select the desired certificate.
5. In the *Certificate Password* field or *Private Key* field, configure the desired password or private key for the certificate.
6. Click *Upload*.

Alerts

Configuring EMS Alerts

You can set up an SMTP server to enable alerts for FortiClient EMS 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 FortiClient EMS version is available.
	Remind me everyday for 2 weeks	Remind you when a new FortiClient EMS 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 FortiClient EMS license.
EMS fails to sync with LDAP domains		FortiClient EMS 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 FortiClient EMS 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 651.

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.
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 Windows cannot verify the certificate.

Viewing alerts

You can view alerts that FortiClient EMS 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 FortiClient EMS 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 version of FortiClient. 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*.

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:

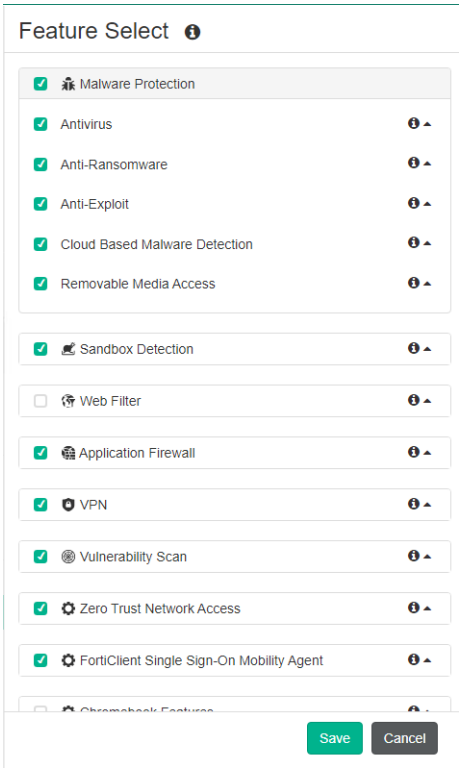
Feature to enable in Feature Select	FortiClient functionalities
Firewall	• C&C blocking • Endpoint quarantine
Web and Video Filtering	• Category-based malicious site blocking • Keyword blocking (also requires web browser plugin)

Only features that FortiClient EMS is licensed for are available for enablement in Feature Select. For example, if you have only applied the zero trust network access license, you cannot enable Firewall. See Windows, macOS, and Linux licenses on page 25 for details on which features each license type includes.

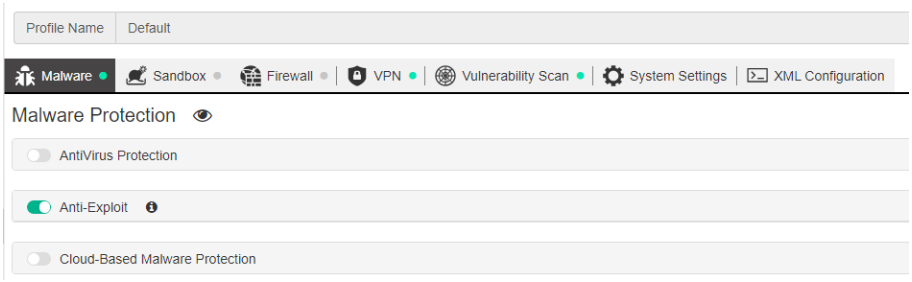
You cannot disable Web Filter if you have enabled the Chromebook feature in Feature Select.

To enable/disable a feature in Feature Select:

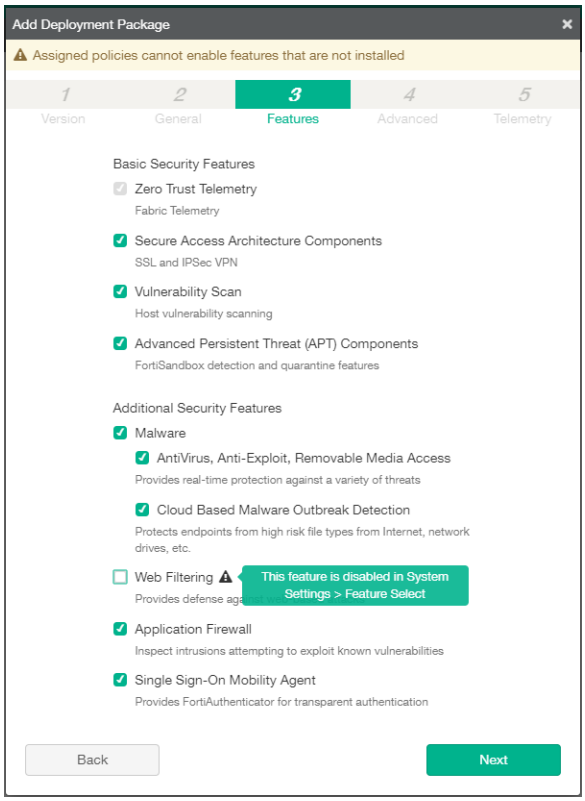
1. Go to *System Settings* > *Feature Select*.
2. Enable or disable features as desired. This example disables Web Filter.



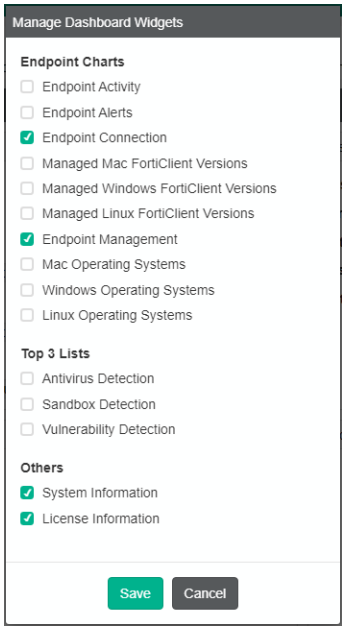
3. Click *Save*. The *Web Filter* tab is not available for configuration in an endpoint profile. The *Import from FortiGate/FortiManager* option under *Endpoint Profiles* in the left pane is also not available.



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

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. You can use the following mobile device management (MDM) platforms to deploy ZTNA certificates to FortiClient (Android) and (iOS):

MDM platform	Supported FortiClient mobile platforms
Intune	• Android • iOS
Workspace ONE	iOS
Jamf	

FortiClient (Android) and (iOS) do not support ZTNA for TCP forwarding.

See the following:

- Mobile
- Provisioning ZTNA certificates to FortiClient (iOS) using Jamf
- Provisioning ZTNA certificates to FortiClient (iOS) using Workspace ONE

Multitenancy

With EMS multitenancy, you can create multiple sites to provide granular access to different sites for different administrators and separate endpoint data and configuration into different sites. The sites are completely separate from each other and cannot share data between them. For example, if an administrator only has access to Site A, they cannot view data from any other site. See Management capacity on page 33 for information on the number of sites supported.

The following sections detail how to enable multitenancy and multitenancy-specific settings.

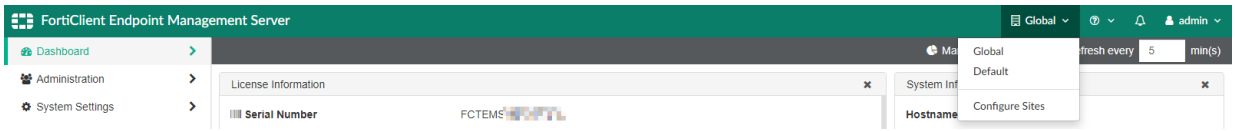
When you enable multitenancy, Fortinet Security Fabric connectors must use an FQDN to connect to EMS, where the FQDN hostname matches a site name in EMS (including "Default"). The following are examples of FQDNs to provide when configuring the connector to connect to the default site and to a site named SiteA, respectively: default.ems.yourcompany.com, sitea.ems.yourcompany.com.

Enabling and configuring multitenancy

By default, multitenancy is disabled in EMS.

To configure multitenancy:

1. Go to *System Settings* > *EMS Settings*.
2. Enable *Manage Multiple Customer Sites*, then click *Save*. EMS forces the GUI to restart for the changes to take effect. After you enable multitenancy, all previously created administrators except the default admin user become administrators for the default site.
3. After restarting, the GUI displays the global dashboard. When you initially enable multitenancy, there are two sites: global, where you can set and view global settings; and default, which contains your original EMS instance's endpoints. Your original EMS instance's settings are retained. To switch between sites, select the site name in the upper right corner, then select the desired site from the dropdown list.



4. Select *Configure Sites* from the site selection list. You can also go to *Administration* > *Configure Sites*. This page displays all sites and their license usage.
5. Click *Add*.
6. In the *Add FortiClient EMS Site* dialog, enter the desired site name. You must use only ASCII characters in site names.
7. Select the checkboxes to assign the desired number of licenses to this site. The dialog displays how many licenses are available for assignment. Click *Save*. The newly created site appears in the FortiClient Sites list. You can go to the site using the site selection list in the upper right corner.

Global and per-site configuration

When you enable multitenancy, you can configure some settings only from the global level, and other settings only from the site level. You cannot view site-level settings from the global site. For setting descriptions, see the relevant section in this document.

Global configuration

The following lists settings you must configure from the global site:

- System Settings > EMS Settings:
  - Shared Settings:
    - Hostname
    - Listen on IP
    - Use FQDN
    - Remote HTTPS access
    - SSL certificate
    - Show FortiGate Server List
  - EMS Settings:
    - Listen on port
    - Enable TLS 1.0/1.1
    - FortiClient download URL
    - Enable login banner. This login banner only shows when you sign in to the global site.
  - EMS for Chromebooks Settings:
    - Listen on port
    - SSL certificate
    - Service account
- Administrators with multisite access. See Adding a multitenancy administrator on page 667.
- Database backup and restoration
- (On-premise EMS-only) License management: You must license EMS from the global site. You can then assign the licenses to other sites. For example, consider that you have three other sites: Sites A, B, and C. If you then activate 500 ZTNA licenses on the global site, you could assign 200 ZTNA licenses to Site A, 150 to Site B, and 150 Site C. See Editing a site on page 667.
- EMS Alerts
- SMTP Server

On the global site Dashboard, you can only view the System and License Information widgets. The other widgets, which display endpoint information, are available at the site level.

Site level configuration

The following lists settings you must configure separately for each site:

- System Settings > EMS Settings:
  - Shared Settings > Reset Stalled Deployment Interval
  - EMS Settings:
    - Sign software packages
    - Enable Managed by EMS
    - Enable login banner. This login banner only shows when you sign in to the current specified site.
  - EMS for Chromebooks Settings:
    - User inactivity timeout
    - Profile update interval
  - Endpoints Settings
  - EMS FSSO Settings
- System Settings > FortiGuard Services
- System Settings > Custom Messages
- System Settings > Feature Select
- Dashboard widgets and charts. The License Information widget for each site displays the information for the licenses that are assigned to that site. When using an on-premise EMS, you cannot update any licensing information from the site-level Dashboard.
- (FortiClient Cloud-only) License management: You must license EMS at the site level. You cannot later assign these licenses to other sites.
- Site-level administrator permissions
- Endpoint management
- Endpoint policies
- Endpoint profiles
- Deployment packages. When an endpoint installs FortiClient using a deployment package configured from a particular site, it registers to that site automatically.
- Endpoint profile components
- Security posture tagging rules
- Software Inventory
- Email endpoint alerts

Left pane with multitenancy enabled

The left navigation pane displays content in the right pane. The following describes the left pane for the global site when multitenancy is enabled:

Option	Description
Dashboard	
Status	Displays a dashboard of information about all managed endpoints.

Option		Description
Administration		
	Administrators	Add and manage FortiClient EMS administrators.
	User Settings	Configure the inactivity timeout and other user settings.
	Configure License	Upgrade or renew the FortiClient EMS license.
	Configure Sites	Configure multitenancy sites.
	Log Viewer	View log messages generated by FortiClient EMS and download raw logs.
System Settings		
	EMS Settings	Change the IP address and port and configure other EMS settings for FortiClient EMS, including enabling Chromebook management.
	Log Settings	Specify what level of log messages to capture in FortiClient EMS 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 FortiClient EMS events.
	SMTP Server	Set up an SMTP server to enable email alerts.

The following describes the left pane at the site level when multitenancy is enabled. For all options at the site-level, you can only view and manage endpoints and settings for the current selected site:

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.
	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.

Option		Description
	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*.
	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 FortiClient EMS.
	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.

Option		Description
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.
Administration		
	Administrators	Add and manage FortiClient EMS administrators.
	Admin Roles	Add and manage FortiClient EMS admin roles and permissions.
	Fabric Devices	View Fabric devices connected to EMS.
	SAML SSO	Configure SAML SSO authentication.
	Log Viewer	View log messages generated by FortiClient EMS and download raw logs.
System Settings		
	EMS Settings	Change the IP address and port and configure other EMS settings for FortiClient EMS, including enabling Chromebook management.
	Log Settings	Specify what level of log messages to capture in FortiClient EMS 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 FortiClient EMS 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 FortiClient EMS
	Feature Select	Choose which features to show and hide in EMS.

Editing a site

To edit a site:

1. From the global site, go to *Administration* > *Configure Sites*.
2. Select the desired site.
3. Click *Edit*.
4. Edit the site as desired. You can edit its name and the number and type of licenses assigned.
5. Click *Save*.

Adding a multitenancy administrator

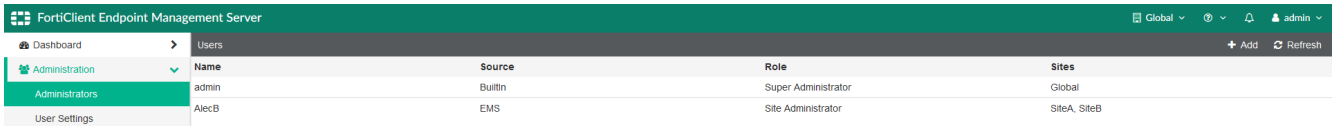
To add a multitenancy administrator:

1. From the global site, go to *Administration* > *Administrators*.
2. Click *Add*.
3. Configure the administrator as Configuring user accounts on page 564 describes. When adding a new administrator from the global site, you can create a local administrator or configure a Windows or LDAP user. When adding a new administrator from the site level, you can only configure an LDAP user. Administrator names from the same source (EMS, LDAP, or Windows) must be unique across all sites. Administrators can have the same name if they are from different sources. When configuring the administrator role, select from one of the following. The following administrator roles are specific to global administrator mangement when multitenancy is enabled:

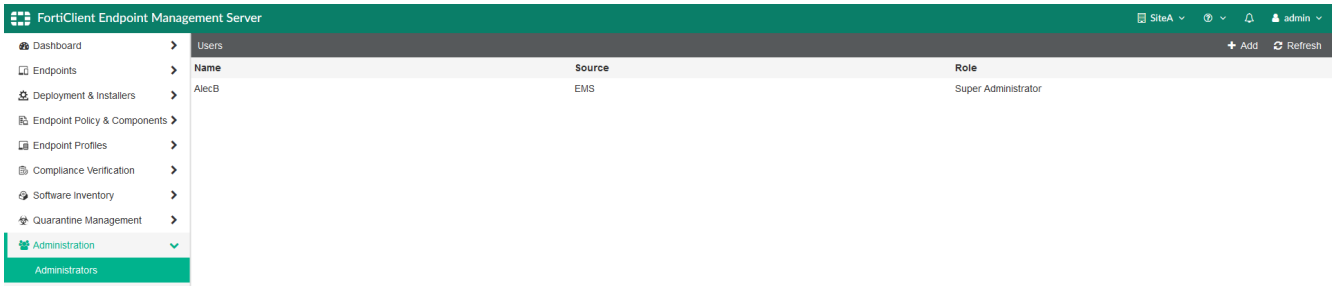
Administrator role	Description
Super administrator	Full access to the global site and all other sites. Can access all configuration options on all sites, including the global site. The built-in admin account is a super administrator and cannot be configured as another administrator role.
Settings administrator	Access to the global site only. Can access all configuration options on the global site, except for administrator configuration.
Site administrator	Access to specified sites only, with no access to the global site. A site administrator can have access to multiple sites. By default, a site administrator is a super administrator for all sites that they have access to. A site administrator can configure the site license and system settings, including server, FortiGuard, login banner, alerts, and SMTP server settings. You can modify the site administrator's available configuration options for a site by assigning them a different admin role for that site after you log in to the site. See Admin roles on page 567.

4. Click *Finish*. The new administrator appears on the *Administrators* page.

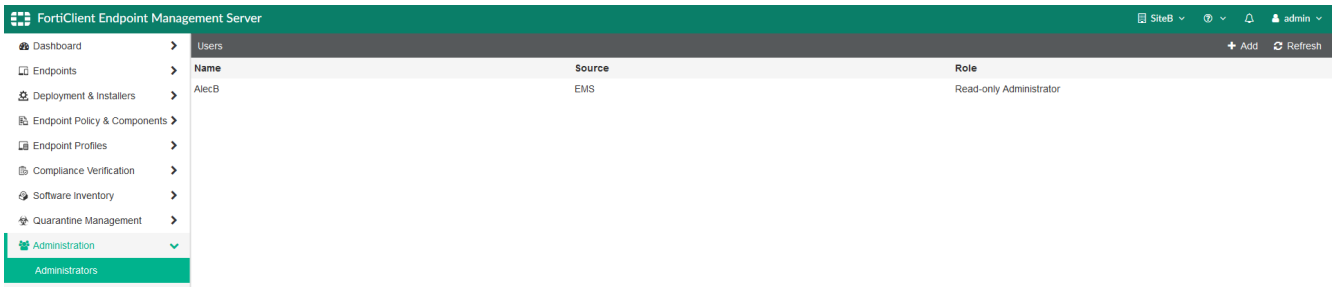
The following example shows a site administrator, AlecB. The *Global Administration > Administrators* page shows that AlecB has access to two sites, SiteA and SiteB.



The SiteA *Administration > Administrators* page shows that AlecB is a super administrator for this site. This means that AlecB has complete access to all EMS permissions within SiteA, as described in Admin roles on page 567.



The SiteB *Administration > Administrators* page shows that AlecB is a read-only administrator for this site. This means that AlecB has only read-only access to endpoint, policy, and settings permissions within SiteB, as described in Admin roles on page 567.



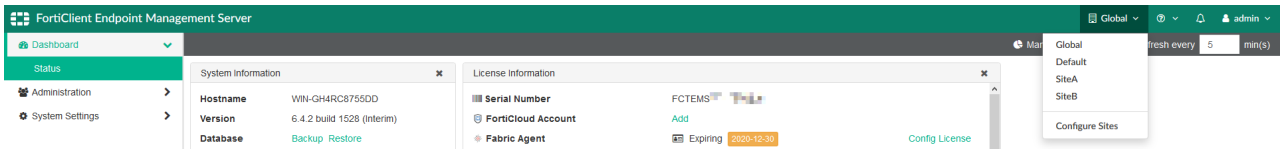
If you had configured a SAML SSO administrator prior to enabling multitenancy, enabling multitenancy causes this administrator to become a global superadministrator. You can configure a different role for this administrator. You can only have one SAML SSO administrator for the entire EMS server.

Logging into EMS with multitenancy enabled

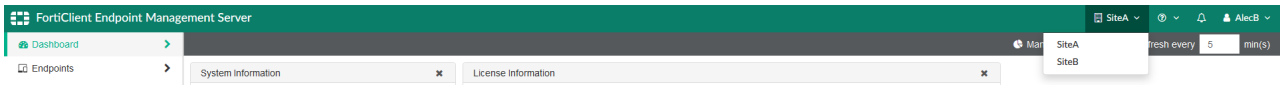
To log into EMS with multitenancy enabled:

1. Double-click the *FortiClient Endpoint Management Server* icon.
2. Enter the username and password for an administrator with the desired site access. If you are logging in as an LDAP user, add the domain prefix for the user.

3. Click *Sign in*. If you logged in as a global administrator, the EMS GUI displays the Global dashboard. You can then switch sites using the site selection list in the upper right corner.



If you logged in as a site administrator, the EMS GUI displays the dashboard for the first site that you have access to in the dropdown list. The site selection list displays sites that you have access to in alphabetical order.

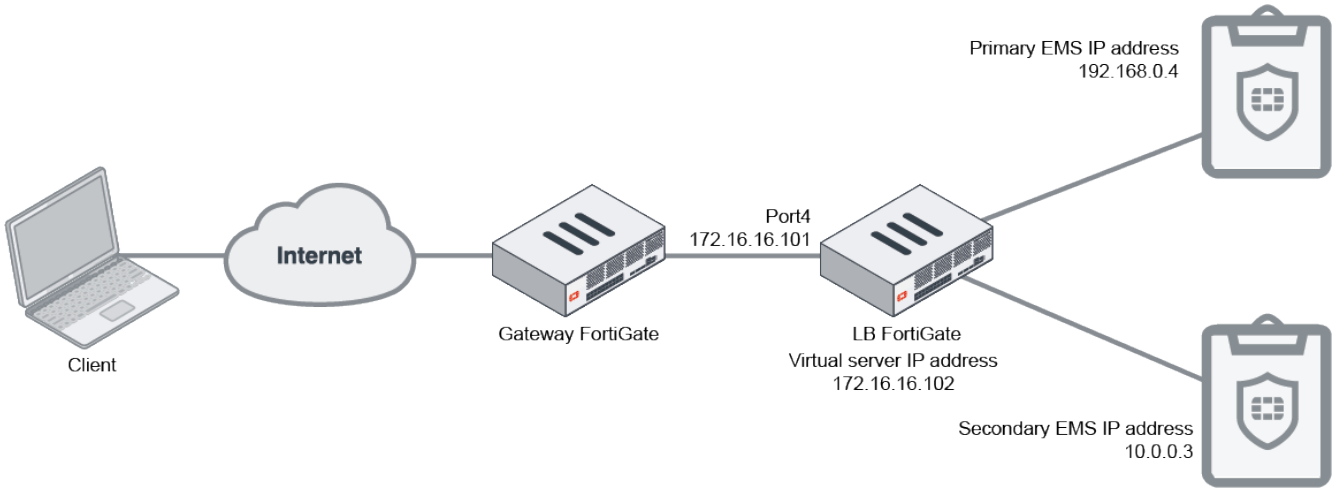


Fabric connection setup using FortiGate as a load balancer

The FortiGate to EMS Fortinet Security Fabric connection in a high availability (HA) environment has the following limitations:

- If round robin is enabled on the DNS server, FortiOS may reach a secondary EMS node during Fabric connection, resulting in Fabric connection failing.
- If there is a Fabric connection that is already configured, after EMS failover, the connector disconnects, since DNS still resolves to the primary EMS node.

For EMS HA failover to function correctly with FortiOS Fabric connectors, you can use a FortiGate as a load balancer (LB). This effectively brokers the data routing to the correct EMS based on availability.



To demonstrate this configuration, the example EMS HA environment uses the following components:

- Two EMS nodes configured in an HA environment
- FortiGate acting as the LB
- FortiGate acting as the gateway
- Endpoint running FortiClient

To configure a FortiGate as the LB:

1. On the FortiGate acting as the LB, configure the secondary IP address for port4. FortiOS uses this secondary IP address as a virtual IP address to connect with EMS. In this case, the virtual server IP address is 172.16.16.102.
2. Go to *Policy & Objects* > *Health Check*.
3. Click *Create New*.
4. For *Type*, select *TCP*.
5. In the *Port* field, enter 8013.
6. Configure other fields as desired.

7. Create virtual servers:
   a. Go to *Policy & Objects*.
   b. Create a virtual server.
   c. In the *Virtual Server IP* field, enter the secondary IP address that you configured in step 1. In this example, it is 172.16.16.102.
   d. In the *Virtual Server Port* field, enter 8013.
   e. For *Load Balancing* method, select *First Alive*.
   f. For *Health check*, select monitor that you configured.
   g. Configure real servers:
      i. On the *Real Servers* tab, select Create New.
      ii. In the *IPv4 address* field, enter the primary EMS node IP address. In this example, it is 192.168.0.4.
      iii. In the *Port* field, enter 8013.
      iv. In the *Max connections* field, enter 0.
      v. For *Mode*, select *Active*.
      vi. Repeat these steps for the secondary EMS node. Click *Save*.
   h. Repeat steps a-g to create three additional virtual servers. The additional servers use ports 443, 8015, and 10443, but otherwise have identical settings to the first virtual server created. If you have enabled Chromebook management, create a virtual server for port 8443. Similarly, if you require importing an ACME certificate, create a virtual server for port 80.



8. Create a security policy that includes the LB virtual server as a destination address:
   a. Go to *Policy & Objects > Firewall Policy*.
   b. Click *Create New*.
   c. Configure the *Incoming Interface* and *Outgoing Interface* fields. The outgoing interface connects to the primary EMS node.
   d. For *Source*, select *all*.
   e. In the *Destination* field, select ports 10443, 443, 8013, and 8015.
   f. For *Service*, select *ALL*.
   g. For *Inspection Mode*, select *Proxy-based*.
   h. Save the policy.
   i. If the EMS nodes are in different subnets, repeat these steps to configure a policy for the secondary EMS node. In this example, the nodes are in the same subnet, so you do not need to add a separate policy for the secondary EMS.

The FortiGate LB monitors the EMS nodes' statuses and forwards traffic to the active EMS node for ports 8013, 8015, 443, and 10443.

To configure the Fabric connection between FortiOS and EMS:

1. In FortiOS, go to *Security Fabric > Fabric Connectors*.
2. Double-click the *FortiClient EMS* card.

3. Under *FortiClient EMS Settings*, in the *IP/Domain name* field, enter the EMS fully qualified domain name (FQDN). The FQDN resolves to the virtual server IP address, which in this case is 172.16.16.102. Similarly, the end user uses the FQDN to connect FortiClient to EMS.

Migrating to another EMS instance

You can simply and efficiently move configurations, data, and endpoint connections between EMS instances without disrupting FortiClient endpoint functionality. This document describes migrating one EMS on-premise environment to another. This migration requires the following:

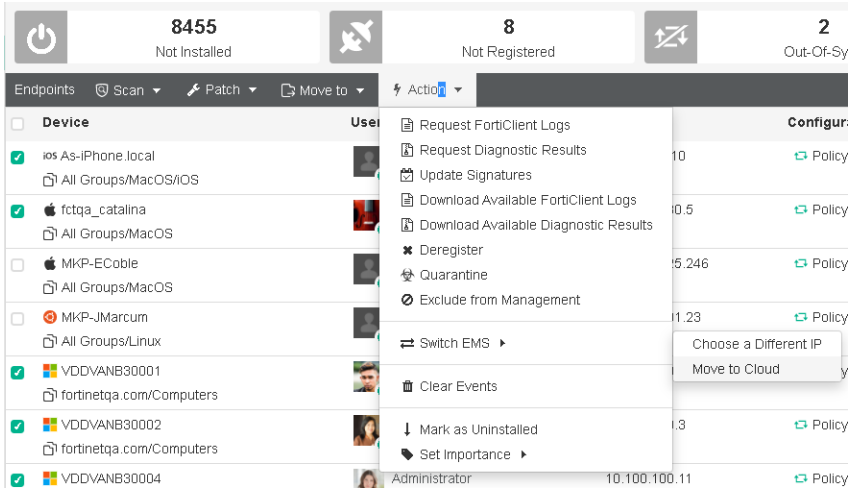
- The EMS version in both environments is 6.4.3 GA or newer.
- FortiClient for all supported endpoint platforms (Windows, macOS, Linux, Android, and iOS) are connected before, during, and after migration.
- You have fully configured EMS and generated data such as logs and events before starting the migration.
- Licensing on the two EMS instances is similar, if not the same, in terms of the number of seats, entitlement, license types, and duration.

This guide only provides instructions for migrating one EMS on-premise environment to another. Migrating an on-premise EMS environment to FortiClient Cloud requires a Best Practice Service (BPS) license. Contact the BPS team for details.

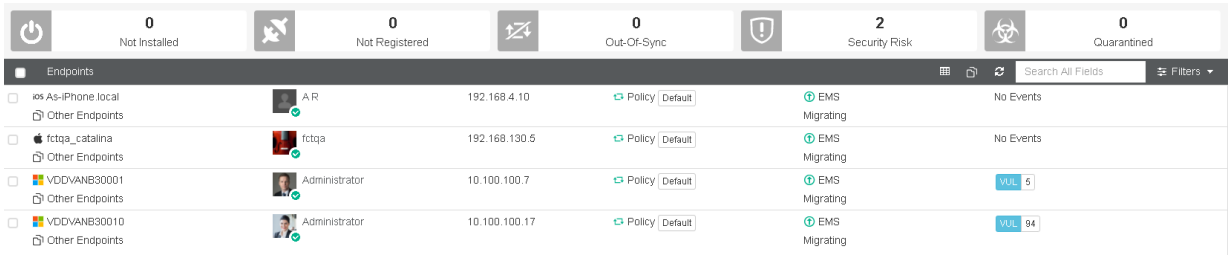
This guide refers to the EMS instance that you are migrating from as "EMS A". It refers to the EMS instance that you are migrating to as "EMS B".

To migrate from EMS A to EMS B:

1. Install and license EMS B as Installation and licensing on page 45 describes.
2. Back up the EMS A database as To back up the DB: on page 152 describes.
3. Restore the database on EMS B as To restore the DB: on page 152 describes.
4. Migrate the FortiClient endpoints. This migration process supports all FortiClient endpoint platforms, except Chromebook:
   a. On EMS A, go to *Endpoints*.
   b. Select the desired endpoints to migrate.
   c. Select *Action > Switch EMS > Choose a Different IP*.



d. In the dialog, enter the EMS B FQDN or IP address. Once the migration begins, the *Connections* column on the *Endpoints* pane in EMS B for the selected endpoints displays as *Migrating*. Events may not display immediately on the *Endpoints* pane in EMS B, but are present in the database. Endpoints that are offline when you apply the *Choose a Different IP* action migrate when they reconnect to EMS A.



e. Shut down EMS A.

f. For any remaining endpoints that have not been migrated, manually connect them to EMS B by entering the EMS B IP address on the Zero Trust Telemetry tab. See Connecting FortiClient Telemetry after installation.

g. Monitor EMS B services and system performance to ensure stability.

Limitations

- **Chromebook**: The migration does not support migration for Chromebook endpoints.

FortiClient EMS API

The FortiClient EMS API allows you to perform configuration operations on EMS. You can view the API documentation on the *FortiAPI* tab on FNDN.

Appendix A - FortiClient EMS services

The following lists FortiClient EMS services:

Critical severity

Service	Description
apache2	Serves the EMS administration console and the APIs that FortiOS uses to get endpoint and posture information.
fcems_chromebook	Processes requests and serves profiles to Chromebook endpoints.
fcems_das	Allows most processes to access and cache endpoint-related data. When this service is down, processing requests from endpoints results in error.
fcems_ecsocksrv	Receives connections from endpoints and routes their requests to other processes within EMS. If this process is down, endpoints cannot communicate with EMS.
fcems_ka	Processes heartbeat requests from endpoints and pushes profile changes and commands to be executed on the endpoints (vuln scan, AV scan, etc.)
fcems_monitor	Ensures EMS services are running and restarts ones that are down. It also can restart running services when it detects settings that affect those services have changed to ensure they use the latest settings.
fcems_notify	Notifies FortiOS when there are important changes in the endpoints.
fcems_pgbouncer	Database connection pooler. This is where all EMS processes except apache2 connect to to connect to the database.
fcems_probe	Handles probe requests, which are tests that endpoints perform to ensure they are talking to a supported EMS. When this service is down, new endpoints cannot connect to EMS and existing endpoints cannot reconnect.
fcems_reg	Handles registration requests from endpoints.
fcems_tag	Processes network change requests from endpoints. When down, network changes that affect the endpoint's posture may take longer for EMS to realized and inform FortiOS of.
fcems_wspgbouncer	Exclusive database connection pooler for the webserver (apache2).
fcems_ztna	Provides some APIs that FortiOS consumes to get information on endpoints and posture.

Medium severity

Service	Description
fcems_adconnector	Connects and pulls data from Active Directory (AD) or Microsoft Entra ID to add to EMS.
fcems_addaemon	Parses AD information and links it to existing endpoints or adds new devices, groups, and users pulled from those directories to EMS.
fcems_adtask	Performs periodical syncs to get updates from AD added to EMS.
fcems_deploy	Schedules deployment of FortiClient upgrades to eligible endpoints.
fcems_sip	Processes software inventory lists that endpoints uploads and checks for potentially unwanted applications.
fcems_task	Performs schedule tasks for license maintenance, such as removing seats from endpoints that have not connected to EMS in a long time, and other functions, such as revoking expired zero trust network access (ZTNA) certificates.
fcems_update	Downloads updates from FortiGuard distribution servers (FDS) and other Fortinet systems. This includes FortiClient installer lists and vulnerability and signature information.

fcems_upload	Processes data uploads from endpoints. Uploads can be any of the following:
	• Endpoint logs
	• Endpoint diagnostics
	• Software inventory
	• Alerts:
	  • Web Filter
	  • Antivirus
	  • Firewall
	• Vulnerability Scan results

redis	Used by most other services for caching and inter-process communication.

Low severity

Service	Description
fcems_adevtsrv	If syncing AD to EMS using a remote connector, this process parses the connector's requests.

Service	Description
fcems_dbop	Performs database-related tasks, such as site database creation, deletion, update, backup, and restore.
fcems_forensics	Integrates with the Forensics platform to pull updates from Forensics tickets associated with any of the endpoints under management.
fcems_ftntdbimporter	Decodes and imports signature and vulnerability databases downloaded from FDS.
fcems_installer	Interfaces with the FortiCloud repackaging services to generate installers with the EMS configuration.
fcems_mdmproxy	Integrates with mobile device management (MDM) platforms to exchange information about mobile endpoints.
fcems_scep	Serves ZTNA certificates for mobile endpoints that MDM platforms manage.

Appendix B - CLI commands

An EMS CLI tool, `/opt/forticlientems/bin/emscli`, is available. The following summarizes the CLI commands available for EMS:

Making configuration changes

You can make EMS configuration changes, such as enabling and disabling remote HTTPS access to EMS, through `emscli`. You can access usage information by using the following commands:

```
/opt/forticlientems/bin/emscli config set console -h
Sets auto upgrade specific configuration

Usage:
  emscli config set console [flags]

Flags:
      --allowed.hosts string    Comma separated list, with not spaces of allowed hosts to refer to
the console with
      --disable.remote.access   Disables remote https access to the EMS console
      --enable.remote.access    Enables remote https access to the EMS console
      --fileserver.port int     New fileserver port for the EMS console. By default it uses port
10443
  -h, --help                    help for console
      --http.port int           New http port for the EMS console. By default it uses port 80
      --https.port int          New https port for the EMS console. By default it uses port 443
```

You can also make configuration changes to the EMS database. You can access usage information by using the following commands:

```
/opt/forticlientems/bin/emscli config set db -h
Sets the DB config from the specified flags

Usage:
  emscli config set db [flags]

Flags:
      --db.host string       new DB host to set the application config to
      --db.password string   new DB password to set the application config to
      --db.port string       new DB port to set the application config to
      --db.user string       new DB user to set the application config to
  -h, --help                 help for db
```

Managing services

You can check, start, and restart EMS services. You can also enable and disable debugging for specific services and follow logs. You may find these options helpful for troubleshooting. You can access usage information by using the following commands:

```
/opt/forticlientems/bin/emscli service -h
service operations (get|start|stop|restart)

Usage:
  emscli service [command]

Available Commands:
  disable-debug disables debug logging for service or services
  enable-debug  enables debug logging for service or services
  get           returns information about a service or services
  log           prints and follows the latest log for a service or services
  restart       restarts a service or services
  start         starts a service or services
  stop          stops a service or services
```

To stop a specific service (fcems_monitor in this example), you can enter `/opt/forticlientems/bin/emscli service stop fcems_monitor`.

Accessing the database

You can access the EMS database(s). You can access usage information by using the following commands:

```
/opt/forticlientems/bin/emscli db -h
Command used to access the EMS DB using psql and be able to run queries. If a query is provided in
the command line, that query will be executed and psql will exit.

Usage:
  emscli db [flags]

Flags:
      --db string      The database to connect to (default "fcm_default")
  -h, --help           help for db
      --query string   The query to execute on the database
```

For example, to access an EMS database named DB1, enter `/opt/forticlientems/bin/emscli db --db DB1`.

Obtaining data from the DAS cache

You can obtain data from the DAS cache. You can access usage information by using the following commands:

```
/opt/forticlientems/bin/emscli cache -h
returns data from the DAS cache

Usage:
  emscli cache [command]

Available Commands:
  get         returns data from the DAS cache. Flags are mandatory
```

```
/opt/forticlientems/bin/emscli cache get -h
returns data from the DAS cache. Flags are mandatory

Usage:
  emscli cache get [flags]

Flags:
      --db string      The DB name. It must be prefixed with fcm_ for vdom dbs.
      --format         Prints the response json in pretty format.
  -h, --help           help for get
      --id string      The ID of the object to retrieve from the DAS cache
      --model string   The name of the das model to query. Options are: generic, fct, users,
devices
```

Diagnosing endpoints

You can diagnose endpoints to obtain endpoint data. You can access usage information by using the following commands:

```
/opt/forticlientems/bin/emscli diag -h
Command used to diagnose

Usage:
  emscli diag [command]

Available Commands:
  endpoint    Shows details for an endpoint to help with troubleshooting
```

```
/opt/forticlientems/bin/emscli diag endpoint -h
Shows details for an endpoint to help with troubleshooting

Usage:
```

```
  emscli diag endpoint [flags]

Flags:
      --dev-only      Return only device data
      --fct-only      Return only fct & fct user data
      --full          Return all device, FCT and FCT user data
  -h, --help          help for endpoint
      --id string     The id for the endpoint. Can be a host name or the endpoint UUID
      --logs          Includes the latest log entries for the endpoint/device
      --site string   If using multitenancy, the name of the site. (default "default")
```

For example, to retrieve all device, FortiClient, and FortiClient user data for an endpoint with ID EXAMPLEID, enter `/opt/forticlientems/bin/emscli diag endpoint --id EXAMPLEID --full`.

Integrating ES cluster

You can configure an Elasticsearch (ES) cluster to enable the *All Events* page in EMS. See All Events on page 208.

```
Usage:
   emscli config set events [flags]

Flags:
   --enabled string Enable the endpoint events feature. Values true|false
   --es.cert string The path to the Elasticsearch CA certificate
   --es.hosts string The Elasticsearch host
   --es.key string The Elasticsearch API key
   --es.password string The Elasticsearch account password
   --es.user string The Elasticsearch user
-h, --help Help for events
```

Change log

Date	Change description
2025-03-20	Initial release.
2025-03-24	Updated: • System requirements on page 22 • Migrating EMS 7.2 to 7.4.3 on page 46 • Deploying EMS as a VM image on page 55 • Installing EMS for HA georedundancy on page 108
2025-03-25	Updated Web Filter on page 422.
2025-03-28	Added Troubleshooting SAML user verification failure on page 620.
2025-03-31	Updated Upgrading from an earlier FortiClient EMS version on page 37.
2025-04-02	Updated Remote Access on page 259.
2025-04-07	Updated Migrating EMS 7.2 to 7.4.3 on page 46.
2025-04-09	Updated Firewall on page 460.
2025-04-21	Added Integrating ES cluster on page 682. Updated: • Upgrading EMS from an earlier 7.4 version on page 38 • Migrating EMS 7.2 to 7.4.3 on page 46
2025-04-22	Updated: • Upgrading EMS from an earlier 7.4 version on page 38 • Migrating EMS 7.2 to 7.4.3 on page 46 • To configure the VM IP address by modifying Netplan configuration files: on page 68 • Viewing endpoints on page 176 • Remote Access on page 259 • Configuring a profile with application-based split tunnel on page 276
2025-04-24	Updated Installing EMS HA with Postgres HA using Bitnami Docker on page 83.
2025-04-28	Updated: • SSL VPN on page 262 • Sandbox on page 455
2025-05-05	Updated To configure auto transport mode: on page 389.
2025-05-12	Added Proxmox on page 59.
2025-05-13	Updated: • Adding an Entra ID server on page 573 • AD connector on page 577

Date	Change description
2025-05-14	Updated Proxmox on page 59.
2025-05-15	Updated Viewing the Vulnerability Scan dashboard on page 157.
2025-05-28	Updated Installation on page 53 and subtopics.
2025-06-02	Added Troubleshooting IPsec VPN IKEv2 with SAML authentication on page 394. Updated Installing EMS HA with native Postgres HA without Docker on page 90.
2025-06-03	Added Matched endpoints and resolved addresses on page 522. Updated ZTNA Applications Catalog on page 527.
2025-06-04	Updated: • Creating a deployment configuration on page 225 • Using the PasswordRecovery tool on page 566
2025-06-05	Updated: • Viewing the Endpoints pane on page 176 • Adding an ADDS server on page 571 • Configuring EMS settings on page 629
2025-06-06	Updated Configuring EMS settings on page 629.
2025-06-10	Updated Quarantining an endpoint from FortiOS using EMS on page 197.
2025-06-12	Added Upgrading EMS in HA on page 41. Updated: • Installing EMS HA with standalone remote DB without Docker on page 76 • Installing EMS HA with Postgres HA using Bitnami Docker on page 83 • Installing EMS HA with native Postgres HA without Docker on page 90 • Installing EMS for HA georedundancy on page 108
2025-06-13	Updated IPsec VPN SAML-based authentication on page 334.
2025-06-19	Updated: • Required services and ports on page 27 • SSL VPN on page 262 • IPsec VPN on page 267 • Creating connectors with OAuth 2.0 token-based authentication on page 519
2025-06-24	Updated: • On-fabric Detection Rules on page 248 • IPsec VPN on page 267
2025-06-27	Updated Web Filter on page 422.
2025-06-30	Updated Viewing the Endpoints pane on page 176.
2025-07-02	Updated: • Management capacity on page 33 • Multitenancy on page 661
2025-07-09	Updated:

Date	Change description
	• Management capacity on page 33 • FortiClient management based on Active Directory user/user groups on page 245 • Remote Access on page 259 • Configuring a profile to allow or block endpoint from VPN tunnel connection based on the applied security posture tag on page 280 • Configuring user verification with Entra ID authentication on page 609 • Multitenancy on page 661
2025-07-10	Updated Malware Protection on page 445.
2025-07-11	Updated Remote Access on page 259.
2025-07-17	Updated: • Installing EMS with Postgres in Docker on page 69 • Installing EMS with standalone remote database without Docker on page 72 • Installing EMS HA with Postgres HA using Bitnami Docker on page 83 • Installing EMS HA with standalone remote DB without Docker on page 76 • Installing EMS with ES integration on page 210
2025-07-18	Updated Adding an endpoint policy on page 240.
2025-07-23	Updated System Settings on page 465.
2025-07-24	Updated Vulnerability Scan on page 442.
2025-07-28	Updated: • Adding an Entra ID server on page 573 • Configuring user verification with Entra ID authentication on page 609
2025-07-29	Added Troubleshooting IPsec VPN IKEv1 on page 404.
2025-07-30	Updated Adding an ADDS server on page 571.
2025-08-08	Updated: • Configuring the FortiClient Web Filter extension on page 127 • Installing EMS HA with native Postgres HA without Docker on page 90
2025-08-14	Updated Deploying EMS as a VM image on page 55.
2025-08-20	Updated: • Server readiness checklist for installation on page 37 • Starting FortiClient EMS and logging in on page 113
2025-08-22	Updated Configuring a profile to allow or block endpoint from VPN tunnel connection based on the applied security posture tag on page 280.
2025-08-25	Updated Installing EMS HA with Postgres HA using Bitnami Docker on page 83.
2025-08-27	Updated: • Viewing the Endpoints pane on page 176 • All Events on page 208 • Web Filter on page 422

Date	Change description
2025-09-08	Updated Installation parameters on page 112.
2025-10-24	Updated the following: • Using a browser as an external user-agent for SAML authentication in an SSL VPN connection on page 286 • Autoconnect on logging in as an Entra ID user on page 294 • SSL VPN on page 262
2025-11-03	Updated Installing EMS HA with native Postgres HA without Docker on page 90.



www.fortinet.com

Copyright© 2025 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.