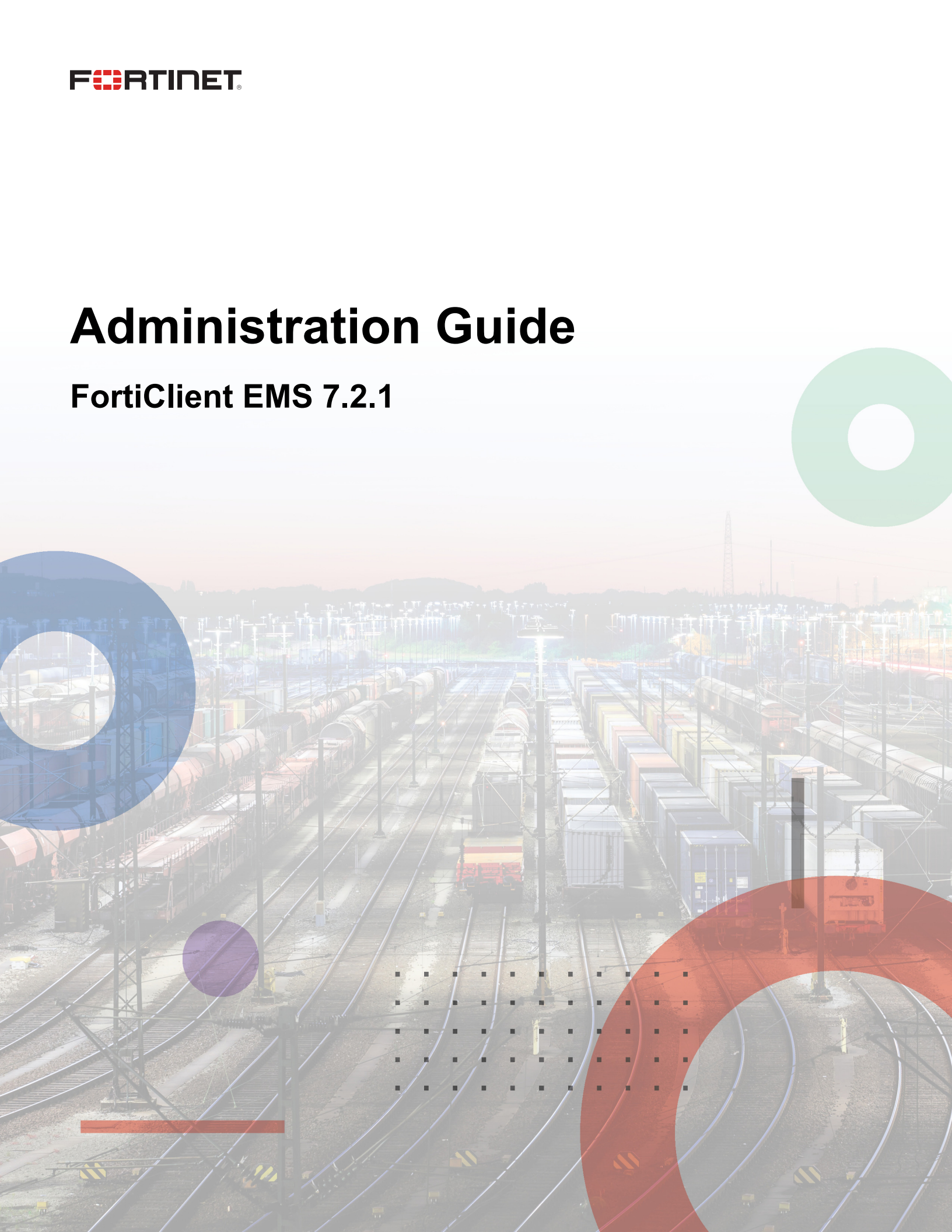


Administration Guide

FortiClient EMS 7.2.1



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



June 12, 2023

FortiClient EMS 7.2.1 Administration Guide

04-721-877345-20230612

TABLE OF CONTENTS

Introduction	9
FortiClient EMS components	9
Documentation	11
Getting started	12
Getting started with managing Windows, macOS, and Linux endpoints	12
Initially deploying FortiClient software to endpoints	12
Pushing configuration information to FortiClient	13
Relationship between FortiClient EMS, FortiGate, and FortiClient	13
Getting started with managing Chromebooks	18
Configuring FortiClient EMS for Chromebooks	18
Configuring the Google Admin console	18
Deploying a profile to Chromebooks	18
How FortiClient EMS and FortiClient work with Chromebooks	19
Installation preparation	20
System requirements	20
License types	21
FortiClient EMS	21
Component applications	24
Required services and ports	24
Management capacity	27
Hardware configuration when EMS and SQL Server run on same machine with no FortiGate connected	28
Hardware configuration when EMS and SQL Server run on different machines with no FortiGate connected	29
Hardware configuration when there are FortiGates connected to the EMS	29
FortiClient Telemetry security features	30
Server readiness checklist for installation	31
Upgrading from an earlier FortiClient EMS version	31
Legacy licenses	31
Upgrading EMS and FortiClient	32
Upgrading EMS from an earlier version	32
Install preparation for managing Chromebooks	33
Google Workspace account	33
SSL certificates	33
Installation and licensing	34
Downloading the installation file	34
Installing FortiClient EMS	34
Installing FortiClient EMS to specify SQL Server Enterprise or Standard instance	36
Installing FortiClient EMS using the CLI	38
Allowing remote access to FortiClient EMS and using custom port numbers	41
Customizing the SQL Server Express install directory	41
Starting FortiClient EMS and logging in	42
Configuring EMS after installation	42

Licensing FortiClient EMS	43
Licensing EMS by logging in to FortiCloud	44
Uploading a license file	48
Licensing EMS in an air-gapped network	48
License status	49
Help with licensing	50
Specifying different ports	50
Upgrading Microsoft SQL Server Express to Microsoft SQL Server Standard or Enterprise	50
Uninstalling FortiClient EMS	51
Installation and setup for managing Chromebooks	53
Google Admin Console setup	53
Service account credentials	59
Verifying ports and services and connection between EMS and FortiClient	65
Ports and services	65
Connectivity between EMS and FortiClient	65
GUI	67
Banner	67
Left pane	68
Content pane	70
Dashboard	71
Viewing the Status	71
System Information widget	71
License Information widget	73
Status charts and widgets	74
Viewing the Vulnerability Scan dashboard	76
Viewing current vulnerabilities	77
Viewing the Endpoint Scan Status	80
Viewing the top 10 vulnerable endpoints with high risk vulnerabilities	82
Viewing top ten vulnerabilities on endpoints	84
Viewing Chromebook Status	86
Endpoint management	88
Windows, macOS, and Linux endpoints	88
Managing groups	88
Adding endpoints	88
Viewing endpoints	91
Managing endpoints	104
Group assignment rules	111
Group assignment rule types	111
Managing group assignment rule priority levels	112
Adding a group assignment rule	113
Enabling/disabling a group assignment rule	115
Deleting a group assignment rule	115
Google Domains	115
Adding a Google domain	115
Viewing domains	116
Editing a domain	118

Deleting a domain	118
Deployment & Installers	119
Manage Deployment	119
Creating a deployment configuration	119
Managing deployment configuration priority levels	120
Enabling/disabling a deployment configuration	121
Deleting a deployment configuration	121
Deploying FortiClient upgrades from FortiClient EMS	121
Deploying different installer IDs to endpoints using the same deployment package	122
FortiClient Installer	122
Adding a FortiClient deployment package	123
Viewing deployment packages	126
Deleting a FortiClient deployment package	126
Endpoint Policy & Components	127
Manage Policies	127
Adding an endpoint policy	127
Editing an endpoint policy	129
Deleting an endpoint policy	129
Enabling/disabling an endpoint policy	129
Managing endpoint policy priority levels	129
Editing endpoint policy view	131
FortiClient management based on Active Directory user/user groups	131
CA Certificates	133
On-fabric Detection Rules	135
Chromebook Policy	139
Endpoint Profiles	140
Editing a default profile	140
Creating a new profile	140
Adding a new Chromebook profile	141
Managing profiles	141
Editing a profile	141
Cloning a profile	142
Syncing profile changes	142
Editing sync schedules	142
Exporting a profile	142
Importing a profile	143
Deleting profiles	143
Remote Access	143
SSL VPN	145
IPsec VPN	148
Configuring a profile with application-based split tunnel	153
Configuring a profile to allow or block endpoint from VPN tunnel connection based on the applied Zero Trust tag	157
Configuring a backup VPN connection	159
Using a browser as an external user-agent for SAML authentication in an SSL VPN connection	161
Per-machine prelogon VPN connection without user interaction	163

Autoconnect on logging in as an Azure AD user	167
Load balancing SSL VPN gateways with one FQDN	169
ZTNA Destinations	174
Wildcard support for ZTNA FQDN rules	176
FortiGate ZTNA service portal support	182
Inline CASB solution for SaaS applications	188
Web Filter	193
Importing a Web profile from FortiOS or FortiManager	201
Enabling and disabling Safe Search	202
Support banned word check in URL	203
Video Filter	206
Vulnerability Scan	208
Malware Protection	210
AntiVirus Protection	210
Anti-Ransomware	213
Anti-Exploit	214
Cloud-Based Malware Detection	214
Removable Media Access	215
Exclusions	216
Other	217
Sandbox	219
Firewall	222
System Settings	223
Configuring identity compliance for endpoints	232
FortiPAM integration	233
Add FortiPAM agent to SSOMA	240
XML Configuration	242
Creating a profile with XML	242
Importing a profile from an XML file	243
Configuring encrypted ZTNA rules	243
Zero Trust Tags	246
Zero Trust Tagging Rules	246
Adding a Zero Trust tagging rule set	246
Editing a Zero Trust tagging rule set	247
Deleting a Zero Trust tagging rule	248
Importing and exporting a Zero Trust tagging rule set	248
Uploading signatures for FortiGuard Outbreak Alerts service	248
Managing tags	249
Zero Trust tagging rule types	249
Zero Trust Tag Monitor	255
FortiOS dynamic policies using EMS dynamic endpoint groups	256
Configuring FortiOS dynamic policies using EMS dynamic endpoint groups	256
Restricting VPN access to rogue/non-compliant devices with Security Fabric	259
Fabric Device Monitor	266
FortiGuard Outbreak Alerts	267
Software Inventory	269
Applications	269

Hosts	270
Quarantine Management	272
Files	272
Viewing quarantined files	272
Allowlisting quarantined files	274
Configuring quarantine management	274
Allowlist	275
Viewing allowlisted files	275
Editing file descriptions	276
Deleting a file from the allowlist	276
Administration	277
Administrators	277
Viewing users	277
Configuring user accounts	278
Activating a disabled account	278
Admin roles	279
Adding an admin role	280
Cloning an admin role	280
Deleting admin roles	280
Admin role permissions reference	280
Authentication Servers	283
Adding an ADDS server	283
Adding an Azure AD server	284
Adding an API key	290
AD connector	291
Configuring Admin User Settings	296
Fabric Devices	296
Configuring EMS to share tagging information with multiple FortiGates	298
Configuring FortiGate per-VDOM connection	299
SAML SSO	302
Licenses	304
Log Viewer	304
Generate Diagnostic Logs	304
Marking all endpoints as uninstalled	304
User Management	306
Authorized User Groups	306
Verified Users	307
Unverified Users	308
Local users	309
SAML Configuration	309
Invitations	310
Configuring user verification with an LDAP server for authentication	312
Configuring user verification with SAML authentication and an LDAP domain user account	313
Configuring user verification with Azure AD authentication	321
Configuring user verification with SAML authentication and an Azure AD server user	324

account	
System Settings	328
Configuring EMS settings	329
Generating a QR code for centrally managing FortiClient (Android) and (iOS)	
endpoints	334
Persistent connection	334
Configuring Logs settings	335
Configuring FortiGuard Services settings	336
Server Certificates	338
Adding an SSL certificate to FortiClient EMS	340
Alerts	340
Configuring EMS Alerts	340
Configuring Endpoint Alerts	341
Configuring SMTP Server settings	342
Viewing alerts	344
Custom Messages	344
Customizing the endpoint quarantine message	344
Customizing Web Filter messages	345
Feature Select	346
Multitenancy	349
Enabling and configuring multitenancy	349
Global and per-site configuration	350
Global configuration	350
Site level configuration	350
Left pane with multitenancy enabled	351
Editing a site	354
Adding a multitenancy administrator	355
Logging into EMS with multitenancy enabled	356
Redundancy	357
Fabric connection setup using traffic manager	362
Fabric connection setup using FortiGate as a load balancer	365
Azure SQL managed instance	367
Configuring EMS HA using AWS RDS Microsoft SQL Server	371
Creating a support package	378
Migrating to another EMS instance	379
Limitations	380
FortiClient EMS API	381
Change log	382

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.

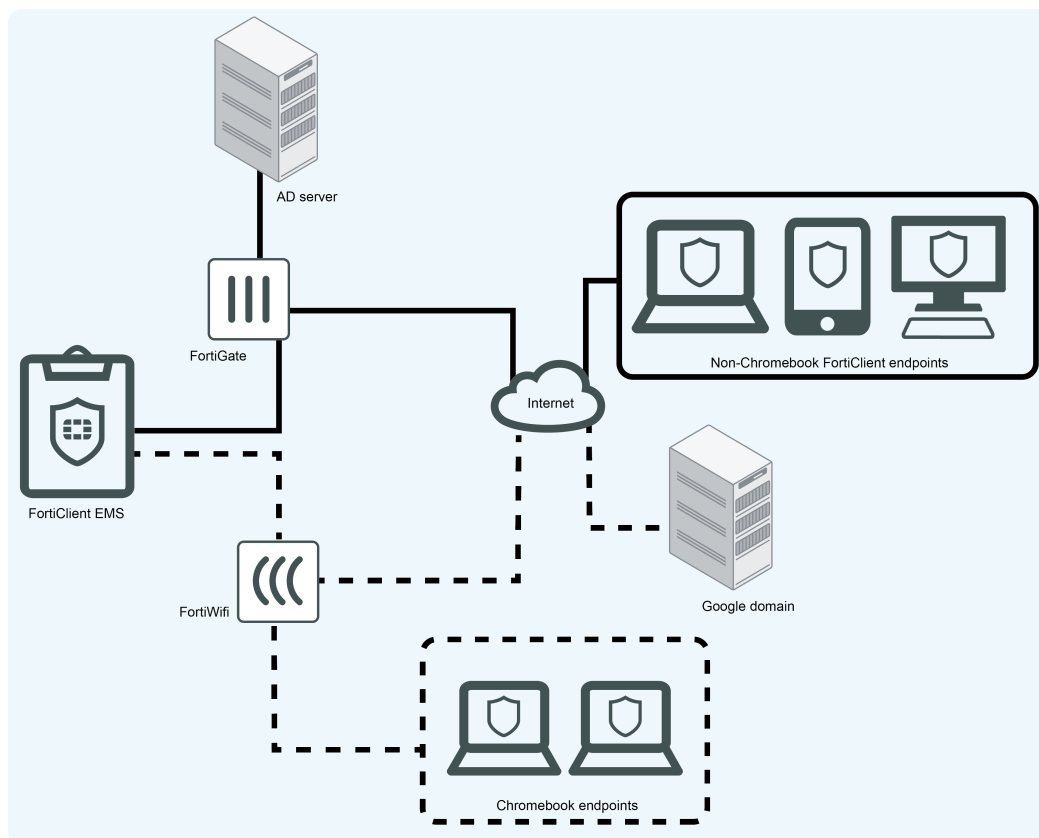
FortiClient EMS also provides the infrastructure to install and manage the FortiClient Web Filter extension on Google Chromebook endpoints. FortiClient protects endpoint users by working with FortiClient EMS to filter web content endpoint users view on Google Chromebooks.

The following table lists FortiClient EMS components:

Component	Description
FortiClient EMS	Manages FortiClient on endpoints that connect to your network. Manages the FortiClient Web Filter extension installed on Google Chromebook endpoints, which are connected to your Google domain.

Component	Description
	Includes the following software: <ul style="list-style-type: none"> • 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 SQL 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 for information.
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)	<ol style="list-style-type: none">1. Create a custom deployment package (MSI file) on EMS. See Adding a FortiClient deployment package on page 123.2. Deploy the FortiClient deployment package to desired endpoints using one of the following:<ol style="list-style-type: none">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: <ul style="list-style-type: none">• Intune• Workspace ONE (macOS only)
Sending installer link to end users	<ol style="list-style-type: none">1. Create a custom deployment package on EMS. See Adding a FortiClient deployment package on page 123.2. Create an invitation on EMS, configuring the invitation to be sent to all desired end users. See Invitations on page 310.3. 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 119](#).



In 7.2.1, 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.

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 140](#).
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 127](#). 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 91](#).

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.

For details, see the [FortiClient 7.2 Compliance Guide](#).

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.



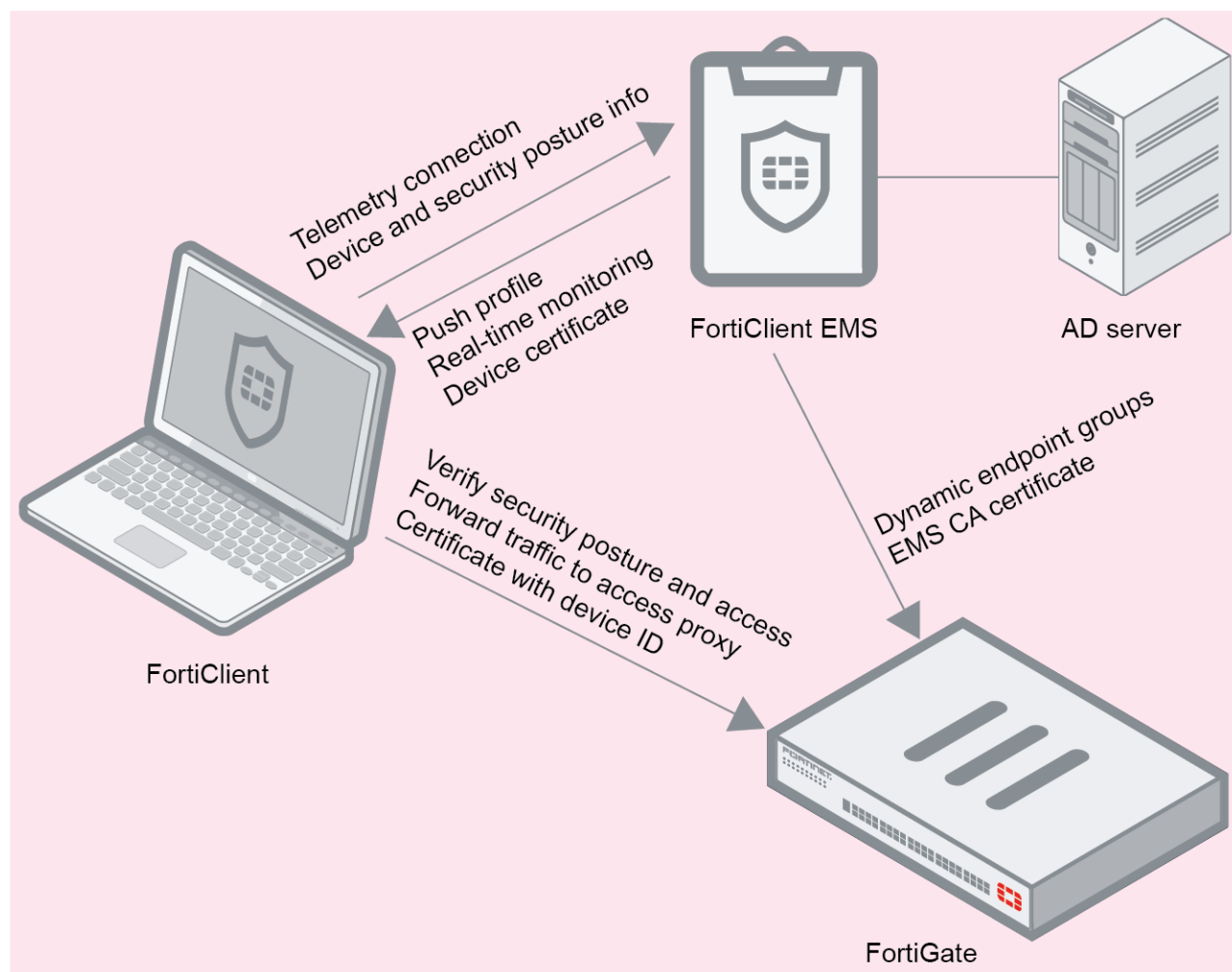
FortiGate does not provide configuration information for FortiClient and the endpoint. An administrator must configure FortiClient using an EMS endpoint policy.

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 22](#).
 - Profile of configuration information as part of an endpoint policy. See [Endpoint Profiles on page 140](#).
 - 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 Zero Trust tagging rules. See [Zero Trust Tagging Rules on page 246](#).
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 endpoint groups on page 256](#).



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
- Zero Trust 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:

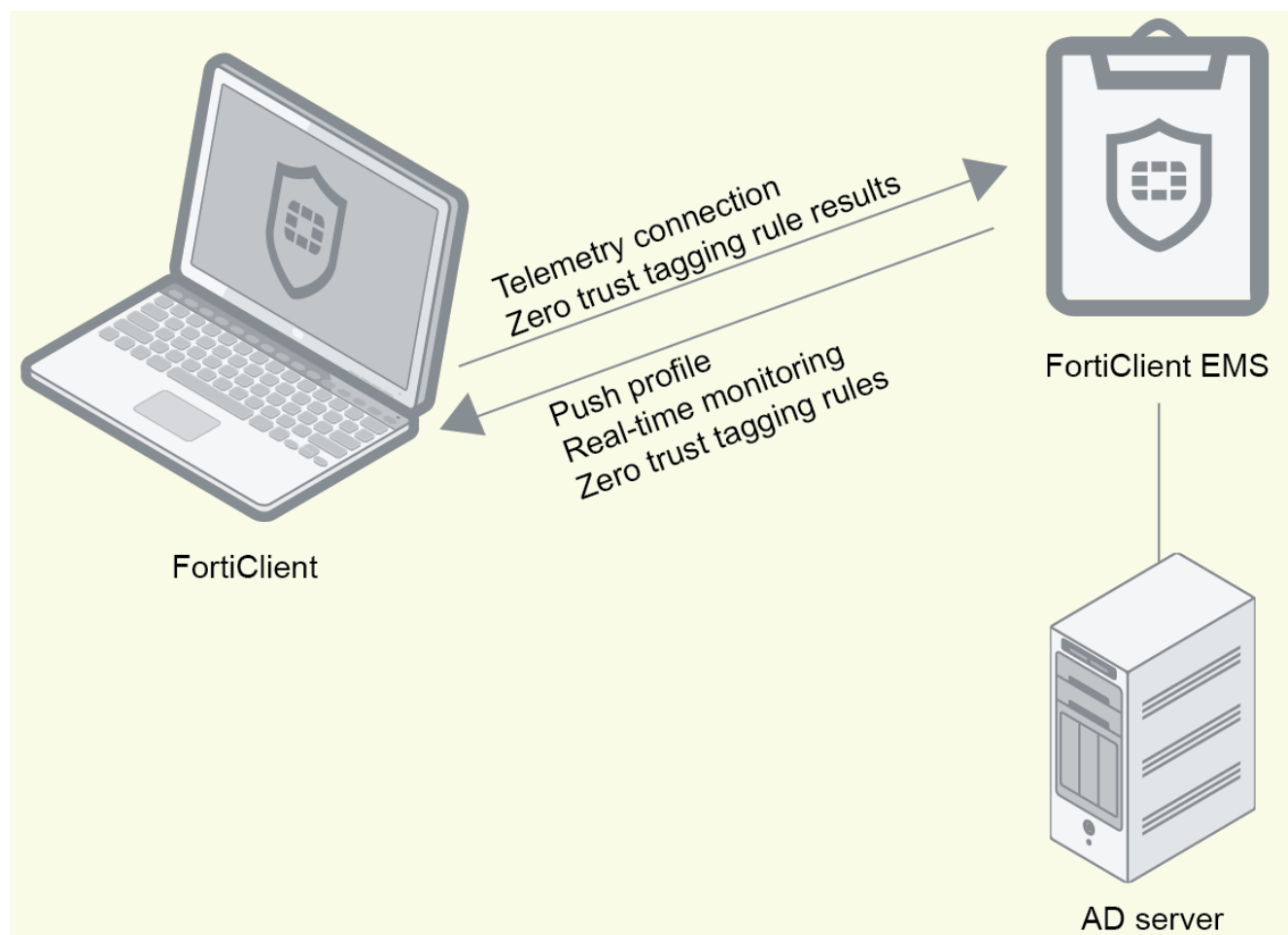
- Logs
- Windows host events

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 Zero Trust 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 107](#) 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 42](#).
2. Add SSL certificates. See [Adding an SSL certificate to FortiClient EMS on page 340](#).
3. Configure FortiClient EMS settings. See [System Settings on page 328](#).
4. Configure user accounts and permissions. See [Administrators on page 277](#). See [Administration](#).

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 54](#).
2. Configure the FortiClient Web Filter extension. See [Configuring the FortiClient Web Filter extension on page 54](#).
3. Add root certificates. See [Adding root certificates on page 55](#).
4. Configure unique service account credentials. See [Configuring unique service account credentials on page 60](#).
5. Disallow incognito mode. See [Disallowing incognito mode on page 57](#).

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.

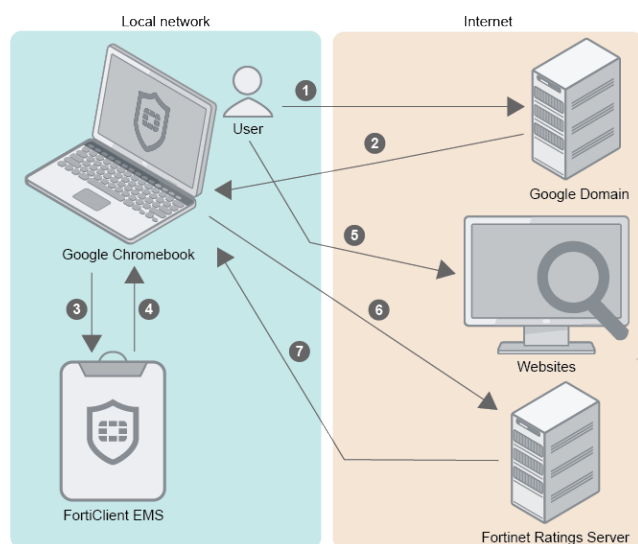
To deploy a profile to Chromebooks:

1. Add the Google domain. See [Adding a Google domain on page 115](#).
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 141](#).
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 139](#).
4. Verify the FortiClient Web Filter extension. See [Verifying the FortiClient Web Filter extension on page 59](#).
5. View Google domains and Google users. See [Viewing domains on page 116](#).

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.



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.

System requirements

The minimum system requirements for FortiClient EMS are:

- Microsoft Windows Server 2022, 2019, 2016, or 2012 R2
- No additional installed services
- 2.0 GHz 64-bit processor, six virtual CPUs (6 vCPU)
- 8 GB RAM (10 GB RAM or more is recommended)
- 40 GB free hard disk
- Gigabit (10/100/1000baseT) Ethernet adapter
- Internet access is recommended, but optional, during installation. SQL Server may require some dependencies to be downloaded over the Internet. 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.



You should only install FortiClient EMS and the default services for the operating system on the server. You should 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 44](#).

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

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.



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](#).

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 (PaaS). 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 (SSL and IPsec 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 EPP, ZTNA, and FortiSASE licensing.

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 306](#). 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
Sandbox appliance	Yes	Yes
Next Generation Endpoint Security		
AI-powered next generation AV	Yes	
FortiClient Cloud Sandbox (PaaS)	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 22](#) 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/Outgoing	How to customize
FortiClient Telemetry	FortiClient endpoint management	TCP	8013 (default)	Incoming	Installer/GUI
Samba (SMB) service	FortiClient EMS uses the SMB service during FortiClient initial deployment.	TCP	445	Outgoing	N/A
Distributed Computing Environment/Remote Procedure Calls (DCE/RPC)	FortiClient EMS connects to endpoints using RPC for FortiClient initial deployment.	TCP	135 1024-5000* 49152-65535*	Outgoing	You can configure ranges noted with *. See How to configure RPC dynamic port allocation to work with firewalls.
Active Directory server connection	Retrieving workstation and user information	TCP	389 (LDAP) or 636 (LDAPS)	Outgoing	GUI

Communication	Usage	Protocol	Port	Incoming/Outgoing	How to customize
FortiClient download	Downloading FortiClient deployment packages created by FortiClient EMS	TCP	10443 (default)	Incoming	Installer
Web Filter custom page download	Downloading custom Web Filter pages that the administrator created in EMS.	TCP	10443 (default)	Incoming	N/A
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
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
FortiClient endpoint probing	FortiClient EMS uses ICMP for endpoint probing during FortiClient initial deployment.	ICMP	N/A	Outgoing	N/A
FSSO	Connection to FortiOS.	TCP	8000	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

Communication	Usage	Protocol	Port	Incoming/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 340.	TCP	80	Incoming	N/A

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

Communication	Usage	Protocol	Port	Incoming/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/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

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

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



For the list of required services and ports for FortiClient, see the [FortiClient Administration Guide](#).

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.

You can use FortiClient EMS with SQL Server Express, Enterprise, or Standard. When managing more than 5000 endpoints, install SQL Server Enterprise or Standard instead of SQL Server Express, which the EMS installation installs by default. Otherwise, you may experience database deadlocks. See [Installing FortiClient EMS to specify SQL Server Enterprise or Standard instance on page 36](#). The following table summarizes which SQL Server edition to use for different numbers of managed endpoints.

Number of managed endpoints	Required SQL Server edition	Other configuration notes
Up to 5000	Express. Optionally, you can use SQL Server Enterprise or Standard.	You can install EMS and SQL Server on the same Windows Server machine, or two different Windows Server machines.
5000 to 50000	Enterprise or Standard	You can install EMS and SQL Server on the same Windows Server machine, or two different Windows Server machines.
More than 50000	Enterprise or Standard	You must install EMS and SQL Server on two different Windows Server machines.

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 SQL Server and EMS are on the same or different servers, and whether there are FortiGates connected to EMS. The configurations in the following topics apply when a maximum of 20 multitenancy sites are configured. See the following for the suggested host system hardware configurations for these scenarios:

- [Hardware configuration when EMS and SQL Server run on same machine with no FortiGate connected on page 28](#)
- [Hardware configuration when EMS and SQL Server run on different machines with no FortiGate connected on page 29](#)
- [Hardware configuration when there are FortiGates connected to the EMS on page 29](#)



The requirements listed for managing 50000 to 75000 endpoints are considered best practice, even when managing a smaller number of endpoints.

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

The following table shows the configurations when EMS and SQL Server are running on the same Windows Server machine with no FortiGate connected:

Number of managed endpoints	Number of virtual CPUs	Memory (RAM) (in GB)	Suggested keep alive interval
Up to 5000	6	8	Default (60 seconds)
5000 to 10000	8	12	Default (60 seconds)
10000 to 20000	12	14	120 seconds
20000 to 30000	16	18	120 seconds
30000 to 40000	18	20	120 seconds
40000 to 50000	20	22	120 seconds

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

The following table shows the configurations when EMS and SQL Server are running on different Windows Server machines with no FortiGate connected:

Number of managed endpoints	EMS server machine		SQL server machine		Suggested keep alive interval
	Number of virtual CPUs	Memory (RAM) (in GB)	Number of virtual CPUs	Memory (RAM) (in GB)	
10000 to 20000	6	4	6	12	120 seconds
20000 to 30000	8	6	8	16	120 seconds
30000 to 40000	10	8	10	20	120 seconds
40000 to 50000	12	10	10	24	120 seconds
50000 to 75000	16	12	14	28	120 seconds
75000 to 150000	20	14	20	36	180 seconds

Hardware configuration when there are FortiGates connected to the EMS

The following table shows the configurations with the following host hardware configuration:

- EMS and SQL Server are running on the same Windows Server machine
- Up to 100 FortiGates connected to the EMS
- Up to 20 Zero Trust tags are configured

Number of managed endpoints	Number of virtual CPUs	Memory (RAM) (in GB)	Suggested keep alive interval
Up to 5000	6	8	Default (60 seconds)
5000 to 10000	8	10	Default (60 seconds)
10000 to 20000	12	16	120 seconds
20000 to 30000	16	20	120 seconds
30000 to 40000	22	24	120 seconds
40000 to 50000	30	28	120 seconds

The following table shows the configurations with the following host hardware configuration:

- EMS and SQL Server are running on different Windows Server machines
- Up to 100 FortiGates connected to the EMS
- Up to 20 Zero Trust tags are configured

Number of managed endpoints	EMS server machine		SQL server machine		Suggested keep alive interval
	Number of virtual CPUs	Memory (RAM) (in GB)	Number of virtual CPUs	Memory (RAM) (in GB)	
10000 to 20000	4	4	10	12	120 seconds
20000 to 30000	6	4	14	16	120 seconds
30000 to 40000	6	6	18	24	120 seconds
40000 to 50000	8	6	26	26	120 seconds
50000 to 75000	10	8	30	34	120 seconds
75000 to 150000	14	12	48	56	180 seconds

The following table shows the configurations with the following host hardware configuration:

- EMS and SQL Server are running on the same Windows Server machine
- Up to 300 FortiGates connected to the EMS
- Up to 20 Zero Trust tags are configured

Number of managed endpoints	Number of virtual CPUs	Memory (RAM) (in GB)	Suggested keep alive interval
10000 to 20000	20	22	120 seconds

The following table shows the configurations with the following host hardware configuration:

- EMS and SQL Server are running on different Windows Server machines
- Up to 300 FortiGates connected to the EMS
- Up to 20 Zero Trust tags are configured

Number of managed endpoints	EMS server machine		SQL server machine		Suggested keep alive interval
	Number of virtual CPUs	Memory (RAM) (in GB)	Number of virtual CPUs	Memory (RAM) (in GB)	
10000 to 20000	10	10	12	14	120 seconds

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 329](#).

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 24](#) 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 (AV) 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 no conflict exists with port 443 for the Apache service to function properly.
	Ensure no conflict exists with ports 8013 and 8443 for the EMS service to function properly.

Upgrading from an earlier FortiClient EMS version

FortiClient EMS 7.2.1 supports upgrading from previous EMS versions as [FortiClient and FortiClient EMS Upgrade Paths](#) outlines.



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 7.2.1 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 7.2.1 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 7.2.1 supports the Fabric Agent license. You do not need to convert a Fabric Agent to upgrade to EMS 7.2.1.

Upgrading EMS and FortiClient

When EMS is managing FortiClient endpoints, you must consider the version compatibilities between EMS and FortiClient before upgrading EMS. Ensure that you follow these instructions when upgrading EMS and FortiClient:

See the [EMS Compatibility Chart](#) for EMS and FortiClient compatibility information.

To upgrade EMS and FortiClient:

1. If EMS is already upgraded to the latest version, do the following:
 - a. For endpoints where the FortiClient version is compatible with the EMS version, deploy the latest FortiClient version as an upgrade from EMS. EMS can only upgrade FortiClient versions that it is compatible with. See [Deploying FortiClient upgrades from FortiClient EMS on page 121](#).
 - b. For endpoints where the FortiClient version is incompatible with the EMS version, manually uninstall FortiClient from the endpoint. Then, install the latest FortiClient version on the endpoint. See [Uninstalling FortiClient](#) and [Installing FortiClient on computers](#).
2. If EMS is not yet upgraded to the latest version, do one of the following:
 - a. Incrementally upgrade EMS and FortiClient to ensure that they remain compatible with each other at every step of the installation process. For example, if you want to upgrade EMS and FortiClient from 6.2 to 7.0, do the following:
 - i. Upgrade EMS from 6.2 to 6.4 as [To upgrade EMS from an earlier version: on page 32](#) describes.
 - ii. Deploy FortiClient upgrade from 6.2 to 6.4 from EMS as [Deploying FortiClient upgrades from FortiClient EMS on page 121](#) describes.
 - iii. Upgrade EMS from 6.4 to 7.0 as [To upgrade EMS from an earlier version: on page 32](#) describes..
 - iv. Deploy FortiClient upgrade from 6.4 to 7.0 from EMS as [Deploying FortiClient upgrades from FortiClient EMS on page 121](#) describes.
 - b. Uninstall FortiClient, then deploy the latest version from EMS:
 - i. Uninstall FortiClient by creating an Uninstall deployment configuration to deploy to endpoints. See [Creating a deployment configuration on page 119](#).
 - ii. Upgrade EMS to the latest version as [To upgrade EMS from an earlier version: on page 32](#) describes.
 - iii. Deploy the latest FortiClient version to endpoints as [Manage Deployment on page 119](#) describes.

Upgrading EMS from an earlier version

To upgrade EMS from an earlier version:

1. Close FortiClient EMS.
2. Install FortiClient EMS 7.2.1 using the downloaded installer. You may complete the upgrade using one of the following methods. You can download the installer files from [Customer Service & Support](#).
 - a. Fortinet can enable push notifications on FDS for a new EMS GA build. If Fortinet has enabled this, a notification appears on the FortiClient EMS GUI. Click the notification, then review and accept the upgrade message.
 - b. Run the full FortiClient EMS installer as an administrator.

- c. Run the light FortiClient EMS installer as an administrator. This installer connects to the FDS to check for, download, and run the latest full FortiClient EMS installer.
 - d. Run the full FortiClient EMS installer as an administrator using the CLI. This is necessary for FortiClient EMS installations using a remote SQL database.
3. Monitor FortiClient EMS performance for at least two days, including testing use cases.

Install preparation for managing Chromebooks

Google Workspace account

You must sign up for your Google Workspace (formerly G Suite) 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 signed by a Certificate Authority (CA) 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 340](#). 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 55](#).

Installation and licensing

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

- Reviewed [License types on page 21](#)
- Met the requirements listed in [Required services and ports on page 24](#)
- Completed the [Server readiness checklist for installation on page 31](#)
- Logged into the server as the administrator. The administrator user account is equivalent to a Windows administrator account and 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.



When installing SQL Server for use with EMS, ensure that Database Engine Services is selected. This is the minimum required feature set for SQL Server when used with EMS.

Downloading the installation file

FortiClient EMS is available for download from the [Fortinet Support website](#).

You can also receive the installation file from a sales representative.

The following installation file is available for FortiClient EMS:

`FortiClientEndpointManagement_7.2.1.<build>_x64.exe`

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

Installing FortiClient EMS

The FortiClient EMS installation package includes:

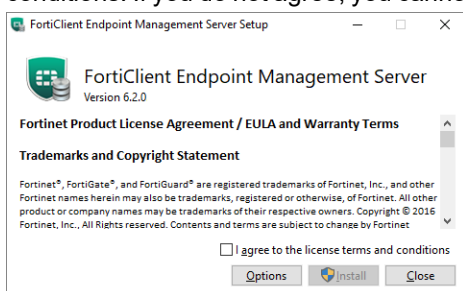
- FortiClient EMS
- Microsoft SQL Server 2017 Express Edition
- Apache HTTP server



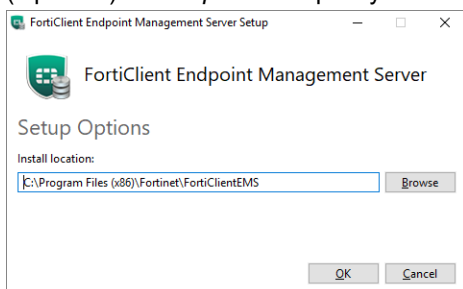
Installing FortiClient EMS requires local administrator rights. Internet access is recommended, but optional, during installation. SQL Server may require some dependencies to be downloaded over the Internet. EMS also tries to download information about FortiClient signature updates from FortiGuard.

To install EMS:

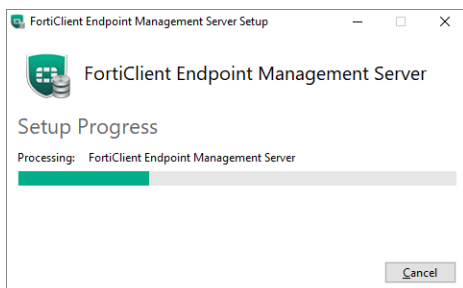
1. Do one of the following:
 - a. If you are logged into the system as an administrator, double-click the downloaded installation file.
 - b. If you are not logged in as an administrator, right-click the installation file, and select *Run as administrator*.
2. If applicable, select **Yes** in the *User Account Control* window to allow the program to make changes to your system.
3. In the installation window, select *I agree to the license terms and conditions* if you agree with the license terms and conditions. If you do not agree, you cannot install the software.



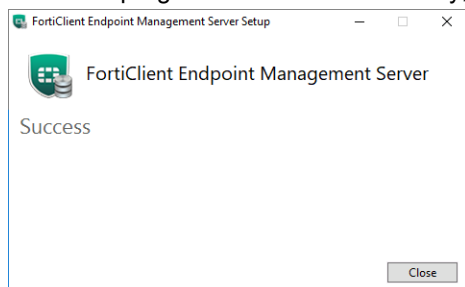
4. (Optional) Click *Options* to specify a custom directory for the FortiClient EMS installation.



- a. Click *Browse* to locate and select the custom directory.
 - b. Click *OK* to return to the installation wizard.
5. Click *Install*.
The installation may take 30 minutes or longer. It may appear to stop at times, but this is only because certain steps in the installation process take longer than others.



6. When the program has installed correctly, the *Success* window displays. Click *Close*.



A *FortiClient Endpoint Management Server* icon is added to the desktop.

Installing FortiClient EMS to specify SQL Server Enterprise or Standard instance

If you are using SQL Server Enterprise or Standard with FortiClient EMS, you must install FortiClient EMS using the CLI to specify the correct SQL Server instance. Ensure you have already installed and configured SQL Server Enterprise or Standard.

For FortiClient EMS installation CLI option descriptions, see [Installing FortiClient EMS using the CLI on page 38](#).

The following SQL permissions are required when using a local or remote database:

- CONTROL SERVER permission on the server. See [BACKUP SERVICE MASTER KEY \(Transact-SQL\)](#).
- Membership in the sysadmin fixed server role or the db_owner fixed database role. See [DBCC SHRINKFILE \(Transact-SQL\)](#).
- BACKUP DATABASE and BACKUP LOG permissions, which default to members of the sysadmin fixed server role and the db_owner and db_backupoperator fixed database roles. See [BACKUP \(Transact-SQL\)](#).

Local existing database

This section lists the CLI commands for when FortiClient EMS and SQL Server Enterprise or Standard are installed on the same machine.

Database type	Command
Local default instance using SQL authentication	<pre>FortiClientEndpointManagement_7.2.1.XXXX_x64.exe SQLUser=<username> SQLUserPassword=<password> InstallSQL=0 ScriptDB=1 SQLServerInstance= SQLService=<instance_name> SQLCmdlineOptions="/INSTANCENAME=" DBInitialSize=31MB DBInitialLogSize=4MB DBGrowth=11MB DBLogGrowth=11% DBLoginTimeout=31 DBQueryTimeout=61</pre>
Local default instance using local Windows authentication	<pre>FortiClientEndpointManagement_7.2.1.XXXX_x64.exe SQLServerInstance= SQLService=<instance_name> SQLCmdlineOptions="/INSTANCENAME=" InstallSQL=0 ScriptDB=1</pre>
Local named instance using SQL authentication	<pre>FortiClientEndpointManagement_7.2.1.XXXX_x64.exe SQLUser=<username> SQLUserPassword=<password> InstallSQL=0 ScriptDB=1 SQLServerInstance=<instance_name> SQLService=mssql\$<instance_name> SQLCmdlineOptions="/INSTANCENAME=<instance_name>"</pre>

Database type	Command
Local named instance using local Windows authentication	<pre>FortiClientEndpointManagement_7.2.1.XXXX_x64.exe SQLServerInstance=<instance_name> SQLService=mssql\$<instance_name> SQLCmdlineOptions="/INSTANCENAME=<instance_name>" InstallSQL=0 ScriptDB=1</pre>

For example, consider installing FortiClient EMS and pointing to a local instance with the following attributes:

- Named "database000"
- Using SQL authentication
- SQL username "janedoe"
- SQL password "password123"
- Database initial size of 31 MB
- Database initial log size of 4 MB
- Database growth rate of 11 MB
- Database log growth rate of 11%
- Database login timeout of 31 seconds
- Database SQL query timeout of 61 seconds

The installation command for this example is as follows:

```
FortiClientEndpointManagement_7.2.1.XXXX_x64.exe SQLUser=janedoe SQLUserPassword=password123
InstallSQL=0 ScriptDB=1 SQLServerInstance=database000 SQLService=mssql$database000
SQLCmdlineOptions="/INSTANCENAME=database000" DBInitialSize=31MB DBInitialLogSize=4MB
DBGrowth=11MB DBLogGrowth=11% DBLoginTimeout=31 DBQueryTimeout=61
```

Remote existing database

To create a backup directory:

Prior to installing FortiClient EMS, create a backup directory on the EMS server. The SQL Server service that is running on the EMS server and the Apache service that is running on the databaser server must both be able to access the backup directory. You must configure the backup directory as a subdirectory of a shared directory. The backup directory should be on the EMS server, not the SQL server.

1. On the EMS server, create a shared directory.
2. Create a backup directory inside the shared directory that you created.
3. Right-click the shared directory and select *Properties*.
4. On the *Security* tab, ensure all users have full control of the directory.
5. On the *Sharing* tab, go to *Advanced Sharing > Permissions*.
6. Ensure the following permissions are configured:
 - Services on the SQL server host have Change permissions.
 - Windows user that the services are running under has Change permissions.

Installation commands for remote existing databases

For remote instances using Windows authentication (domain user), do the following:

1. Join the EMS and database servers to the same domain.
2. Create a database user that maps to the domain user.

3. In Command Prompt on the EMS server, run `gpedit` to open the Local Group Policy Editor.
4. In Local Group Policy Editor, go to *Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment*.
5. Double-click the Log on as a service. In the dialog, add the desired username from the Active Directory domain.

Database type	Command
Remote default or named instance using SQL authentication	<pre>FortiClientEndpointManagementServer_7.2.1.XXXX_x64.exe SQLServer=<SQL_Server_name> SQLUser=<username> SQLUserPassword=<SQL password> InstallSQL=0 ScriptDB=1 BackupDir=\\WIN-0888\Backup DB InitialSize=31MB DBInitialLogSize=4MB DBGrowth=11MB DBLogGrowth=11% DBLoginTimeout=31 DBQueryTimeout=61</pre>
Remote default or named instance using Windows authentication (domain user)	<pre>FortiClientEndpointManagement_7.2.1.XXXX_x64.exe SQLServer=<SQL_Server_name> WindowsUser=<domain name>\<username> WindowsUserPassword=<password> InstallSQL=0 ScriptDB=1 BackupDir=<backupdirectorypath> DBInitialSize=31MB DBInitialLogSize=4MB DBGrowth=11MB DBLogGrowth=11% DBLoginTimeout=31 DBQueryTimeout=61</pre>

For example, consider installing FortiClient EMS and pointing to a remote named instance with the following attributes:

- On a computer with DNS name WIN-088
- Using Windows authentication
- Domain name "forticlient.ca"
- Database initial size of 31 MB
- Database initial log size of 4 MB
- Database growth rate of 11 MB
- Database log growth rate of 11%
- Database login timeout of 31 seconds
- Database SQL query timeout of 61 seconds
- Backup directory of \\WIN-0888\Backup

The installation command for this example is as follows. This example also includes the optional `SQLEncryptConnection` option:

```
FortiClientEndpointManagement_7.2.1.XXXX_x64.exe SQLServer=WIN-0888
  WindowsUser=forticlient.ca\janedoe WindowsUserPassword=password123 InstallSQL=0
  ScriptDB=1 BackupDir=\\WIN-0888\Backup SQLEncryptConnection=no DBInitialSize=31MB
  DBInitialLogSize=4MB DBGrowth=11MB DBLogGrowth=11% DBLoginTimeout=31 DBQueryTimeout=61
```

Installing FortiClient EMS using the CLI

Installing FortiClient EMS using the CLI allows you to enable certain options during installation, such as customizing the EMS installation directory, using custom port numbers, and so on.

You may need to wrap certain CLI option values in double quotation marks. For example, if the backup directory path includes a space, you must wrap the path in double quotation marks, such as: `BackupDir="\\WIN-0888 AHAMILTON\Backup"`. Do not use single quotation marks.

The following table provides a description of all options available when installing FortiClient EMS using the CLI. These options are case-sensitive:

Option	Description
AllowedWebHostnames	The default value is <code>localhost, 127.0.0.1</code> . To clear this value, first enter <code>AllowedWebHostnames=*</code> , then enter the desired <code>AllowedWebHostnames</code> value. Otherwise, the value that you enter is appended to <code>[localhost, 127.0.0.1]</code> , so that <code>AllowedWebHostNames=localhost, 127.0.0.1, <new_value></code> .
ApacheServerAdminEmail	Enter the Apache Server administrator's email address. By default, this is <code>admin@yourcompany.com</code> .
BackupDir	Enter the desired backup directory UNC path for SQL Server.
ClientDownloadPort	Enter the HTTP port number. The default is 80.
RemoteManagementPort	Enter the HTTPS port number. The default is 443.
InstallFolder	Specify the directory to install EMS to.
InstallsSQL	Controls whether the installer installs SQL Server Express on the same server as FortiClient EMS. Enter 1 to install SQL Server Express. Otherwise, enter 0. By default, the EMS installation also installs SQL Server Express.
ScriptDB	Controls where the installer attempts to create the database from db scripts. Enter 1 to create the database from db scripts. You should only enter 0 if you have already set up databases on the server and you are only installing EMS components locally.
ServerHostname	Enter the preferred hostname (the remote hostname). The default is the local host.
SQLAuthType	Enter <code>sql</code> .
SQLCmdlineOptions="/INSTANCEDIR"	Enter the desired directory to install SQL Server Express to.
SQLCmdlineOptions="/INSTANCENAME"	Enter the SQL Server instance name.
SQLEncryptConnection	(Optional) Enter <code>yes</code> to encrypt the connection to SQL Server. Otherwise, enter <code>no</code> . The default is <code>yes</code> .
SQLPort	Enter the port number the remote SQL Server instance listens on. You should configure SQL Server to use a static port number.
SQLServer	If using an instance with a custom name, enter the DSN name of the computer where SQL Server is already installed.
SQLServerInstance	Enter the SQL Server instance name.
SQLService	If using a default database instance, enter the instance name. If using a named database instance, enter <code>mssql\$<instance_name></code> . For example, if your instance is named "database000", enter <code>mssql\$database000</code> .

Option	Description
SQLTrustServerCertificate	(Optional) Enter <code>yes</code> to trust the SQL Server certificate on the machine where FortiClient EMS is installed. If entering <code>no</code> , you must install the issuing CA certificate of SQL Server's certificate onto the machine you are connecting FortiClient EMS from.
SQLUser	Enter the SQL username used to connect to the database instance. You must preconfigure this user in SQL Server.
SQLUserPassword	Enter the SQL password used to connect to the database instance.
WindowsUser	Enter the Windows username that EMS services, once installed, uses to connect to the database instance. You must preconfigure this user in SQL Server.
WindowsUserPassword	Enter the Windows password that EMS services, once installed, uses to connect to the database instance.
DBInitialSize	Enter the database initial size. The default value is 30 MB. This option is used exclusively during installation and can be used to override SQL Server model database settings.
DBInitialLogSize	Enter the database initial log size. The default value is 3 MB. This option is used exclusively during installation and can be used to override SQL Server model database settings.
DBGrowth	Enter the database growth value. The default value is 10 MB. This option is used exclusively during installation and can be used to override SQL Server model database settings.
DBLogGrowth	Enter the database log growth rate. The default value is 10%. This option is used exclusively during installation and can be used to override SQL Server model database settings.
DBLoginTimeout	Enter the database login timeout value in seconds. This option is only useful for remote databases. You must increase <code>DBLoginTimeout</code> if there is ephemerally higher than expected latency between the EMS server and the remote SQL server. However, if this latency is always high, then it is likely that EMS underperforms. In that case, fix the latency. The default value for this option is 30. The installer only uses this option when creating/scripting the EMS databases. This option is unused once EMS is installed.
DBQueryTimeout	Enter the database query timeout value in seconds. The installation uses a SQL query to instruct SQL Server to create a database. The default value for this option is 60. It can take a long time to create the actual database file system due to a slow hard drive.

Option	Description
	The installer only uses this option when creating/scripting the EMS databases. This option is unused once EMS is installed.
EPCPort	Enter the default listening port that endpoints connect to. The default value for this option is 8013.
StartServices	The default value of this option is 1. Setting this option to 0 results in the installer not starting EMS services when installation is complete.
SQLServerCheck	The default value of this option is 1. Setting this option to 0 results in the installer skipping its initial SQL server accessibility test. Skipping this test may result in installation or upgrade rollbacks, if the SQL server cannot be reached during installation.

Allowing remote access to FortiClient EMS and using custom port numbers

To allow remote access to FortiClient EMS from a web browser, install FortiClient EMS by entering the following command in the CLI. You can also specify custom HTTP and HTTPS port numbers:

```
FortiClientEndpointManagement_7.2.1.XXXX_x64.exe ServerHostname=<preferred_host_name>
ClientDownloadPort=<HTTP_port_number> RemoteManagementPort=<HTTPS_port_number>
AllowedWebHostnames=<allowed_web_host_names> ApacheServerAdminEmail=<Apache_Server_
admin_email_address>
```

The example specifies the server hostname as emshost.ems.com, appends emshost.ems.com to the allowed web hostnames, and specifies example@example.com as the Apache server administrator email. This example changes the HTTP and HTTPS ports to 1080 and 22443, respectively.

```
FortiClientEndpointManagement_7.2.1.XXXX_x64.exe ServerHostname=emshost.ems.com
ClientDownloadPort=1080 RemoteManagementPort=22443 AllowedWebHostnames=emshost.ems.com
ApacheServerAdminEmail=example@example.com
```

Customizing the SQL Server Express install directory

By default, the FortiClient EMS installation also installs SQL Server Express. Using the CLI to install FortiClient EMS allows you to customize the SQL Server Express install directory.

These instructions do not apply for SQL Server Enterprise or Standard, which you must install separately from FortiClient EMS. For information on SQL Server Enterprise or Standard and FortiClient EMS, see [Installing FortiClient EMS to specify SQL Server Enterprise or Standard instance on page 36](#).

Customizing the SQL Server Express install to a local directory

Use the following command to customize the SQL Server Express install to a local directory:

```
FortiClientEndpointManagement_7.2.1.XXXX_x64 SQLCmdlineOptions="/INSTANCENAME=FCEMS
/INSTANCEDIR=<desired_directory>"
```

The example installs FortiClient EMS, installing SQL Server to the C:\sqlserver directory:

```
FortiClientEndpointManagement_7.2.1.XXXX_x64 SQLCmdlineOptions="/INSTANCENAME=FCEMS  
/INSTANCEDIR=c:\sqlserver"
```

Customizing the SQL Server Express install to a remote directory

Use the following command to customize the SQL Server Express install to a remote directory:

```
FortiClientEndpointManagement_7.2.1.XXXX_x64 InstallFolder=<desired_directory>  
SQLServer=<SQL_Server_name> SQLServerInstance= SQLService=MSSQLSERVER
```

The example installs FortiClient EMS, installing SQL Server to the C:\sqlserver directory on a computer with DNS name WIN-088:

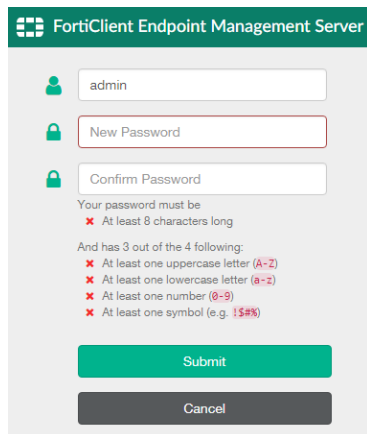
```
FortiClientEndpointManagement_7.2.1.XXXX_x64 InstallFolder=c:/sqlserver SQLServer=WIN-0888  
SQLServerInstance= SQLService=MSSQLSERVER
```

Starting FortiClient EMS and logging in

FortiClient EMS runs as a service on Windows computers.

To start FortiClient EMS and log in:

1. Double-click the *FortiClient Endpoint Management Server* icon.
2. By default, the *admin* user account has no password. Sign in with the username *admin* and no password.
3. You must now EMS add a password for increased security. Change the password following the rules shown. Click *Submit*.



4. EMS displays a popup after login in the following scenarios:
 - If you did not import a secure SSL certificate. See [Server Certificates on page 338](#).
 - If you imported a secure SSL certificate to EMS, but configure it in *Endpoint Control certificate*. See [Configuring EMS settings on page 329](#).

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*. In the *FQDN* field, enter the desired FQDN.
3. If desired, in the *Custom hostname* field, enter the hostname or IP address. Otherwise, EMS uses the *Pre-defined hostname*.
4. If desired, select the *Redirect HTTP request to HTTPS* checkbox. If this option is enabled, if you attempt to remotely access EMS at *http://<server_name>*, this automatically redirects to *https://<server_name>*.
5. 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 21](#).

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

- [Licensing EMS by logging in to FortiCloud on page 44](#): 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 48](#): 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.

You can license an EMS instance that is in an isolated environment and completely isolated from the Internet using an Air-Gap license. To obtain an Air-Gap license, contact [Fortinet Customer Service & Support](#).



Although the option to upload a license file is available in the EMS GUI, FortiCloud does not provide EMS 7.2 license files. You cannot use this option to activate, upgrade, or renew an EMS 7.2 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*.



PLEASE REMEMBER TO REGISTER YOUR CONTRACT REGISTRATION CODE

Service Entitlement Summary

Date : April 22, 2020
Purchase Order Number : ITP001
Contract Registration Code : 3922U

5. Do one of the following:

- a. 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 the *Configure License* page with the serial number and license information that it retrieved from FortiCloud.
- b. As [Windows, macOS, and Linux licenses on page 22](#) 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 Codes* 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

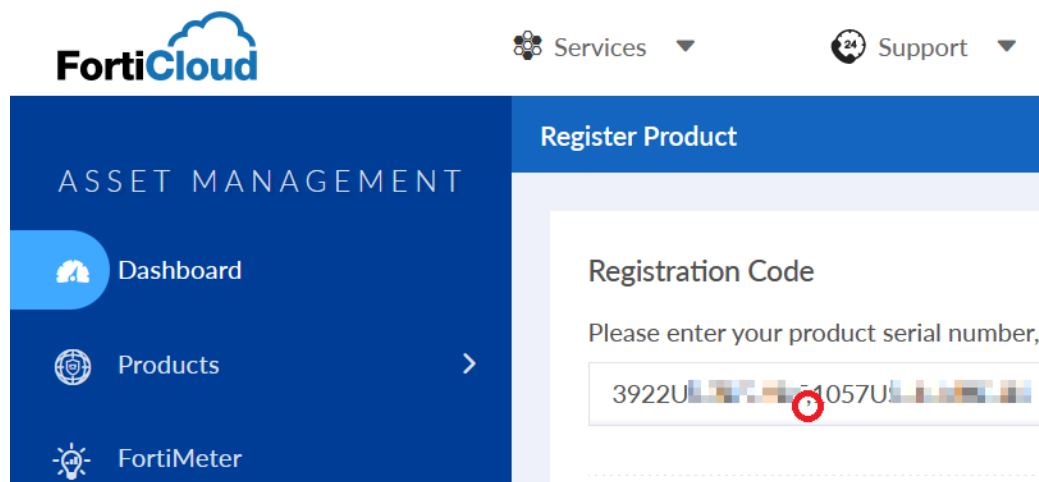
Date : April 22, 2020
Purchase Order Number : ITF001
Contract Registration Code : 3922U

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 [Windows, macOS, and Linux licenses on page 22](#), 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.

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*.

Licensing EMS in an air-gapped network

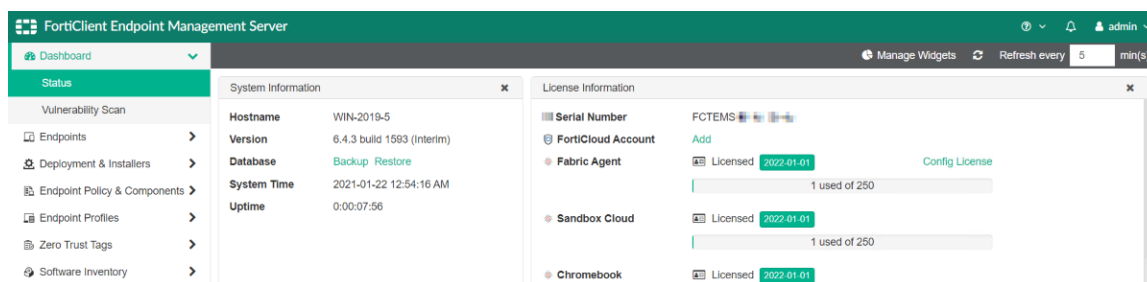
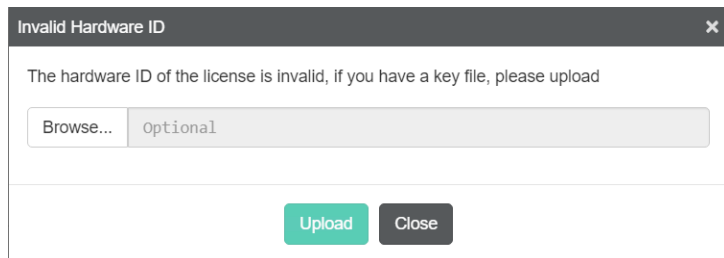
If you are deploying EMS in an air-gapped or isolated network where EMS cannot access the Internet, you can configure EMS to receive updates from FortiManager to deploy to FortiClient. In offline mode, FortiManager allows export and import of FortiGuard packages from FortiManager for provisioning as a FortiGuard distribution server. You can export FortiGuard packages from an online FortiManager to import to an offline FortiManager that provides signature, engine, and FortiClient installer updates to EMS. EMS receives AntiVirus, Web Filter, Application Firewall, Vulnerability Scan, and Sandbox signatures and engines updates and FortiClient installers from FortiManager and deploys updates to FortiClient while in an air-gapped or isolated network.

This feature is also useful if you have experienced hardware failure and need to install EMS on another server. Fortinet customer support can provide a key file to allow you to apply your original license to EMS on the new server.

To configure EMS for an air-gapped network:

1. Contact [Fortinet Customer Service & Support](#). Provide them with your original EMS license file and the IP address of the new machine where you install EMS. They provide you with a key file.
2. Install EMS. See [Installing FortiClient EMS](#).
3. Go to *System Settings > EMS settings*. Ensure that the value in the *Listen on IP* field matches the IP address that you gave to Customer Service & Support in step 1. Otherwise, EMS cannot validate the key file.
4. In EMS, on the *License Information* widget, select *Config License*.

5. For *License Source*, select *File Upload*.
6. In *License File*, browse to and upload your original license file.
7. EMS detects that the hardware ID associated with the license has changed and prompts you to upload the key file. Browse to and upload the key file that Customer Service & Support provided to you. If the key file matches the license file, the EMS license is activated.



8. Enable EMS to use FortiManager for signature updates:
 - a. Go to *System Settings > FortiGuard Services*.
 - b. Enable *Use FortiManager for client software/signature updates*.
 - c. Configure the fields for the desired FortiManager.
 - d. Click *Save*.
9. Enable endpoint profiles to use FortiManager for signature updates:
 - a. Go to *Endpoint Profiles > Manage Profiles*.
 - b. Select the desired profile.
 - c. On the *System Settings* tab, under *Update*, enable *Use FortiManager for Client Signature Update*.
 - d. Configure the fields for the same FortiManager as you configured in step 8.
 - e. Configure the update schedule as desired.
 - f. Click *Save*.

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 (PaaS) 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.

License status	Description
Expired license	<p>You can renew the license on your FortiCloud account.</p> <p>You have ten days after the license expiry date to renew the license. During this grace period, the <i>License Information</i> widget displays the expiry date, which has already passed, and FortiClient EMS functions as if the license has not expired.</p> <p>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.</p> <p>After ten days, FortiClient EMS reverts to unlicensed mode for that license.</p>

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 44](#) 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/

Specifying different ports

In cases where there are pre-existing services running on default FortiClient EMS ports, you can specify another port using the CLI to run the installer. You can use the following commands:

Command	Port usage
<code>ClientDownloadPort</code>	Download FortiClient from FortiClient EMS
<code>RemoteManagementPort</code>	EMS administration

Upgrading Microsoft SQL Server Express to Microsoft SQL Server Standard or Enterprise

The FortiClient EMS installation also installs Microsoft SQL Server Express, which has a file size limit of 10 GB per database. Log entries recorded in the database are rotated on a schedule of seven days (one week) by default. If the FortiClient deployment is large, the database size may reach the 10 GB limit over time. The FortiClient EMS administrator may upgrade the default SQL Server installation from Express to Standard or Enterprise edition. The database file size limit for these editions is in the PB range, which is unlimited for most practical usage. When managing more than 5000 endpoints, installing SQL Server Standard or Enterprise instead of SQL Server Express is recommended.



Microsoft SQL Server Express is free. All other editions require a license from Microsoft.

See the following Microsoft documentation on upgrading between editions called [Upgrade to a Different Edition of SQL Server \(Setup\)](#).

The EMS database is saved in the `C:\Program Files\Microsoft SQL Server\MSSQL12.FCEMS\MSSQL\DATA\FCM_root.mdf` file in the EMS host server. This file's size should remain below the 10 GB limit for Microsoft SQL Server Express.



Upgrading a database edition outside normal production hours is recommended.

The minimum SQL Server version that FortiClient EMS supports is 2017.

To upgrade SQL Server Express to Standard or Enterprise:

1. Attach the SQL Server 2017 installation media to the FortiClient EMS server.
The installation media is a DVD or ISO file. If using the DVD, insert the DVD into the EMS host computer (host server). If your host server is a virtual machine, use the ISO file.
2. Run the SQL Server setup application wizard.
3. In the *SQL Server Installation Center* wizard, go to *Installation > Upgrade from a previous version of SQL Server*.
4. Enter the product key.
5. Accept the license terms, then click *Next*.
6. Under *Select Instance*, in the *Specify the instance of SQL Server* dropdown list, select *FCEMS*. Then, click *Next*.
7. Under *Ready to upgrade edition*, click *Upgrade*.
8. After the upgrade is complete, click *Finish*.

To test the SQL server upgrade:

Running a short test on FortiClient EMS after the upgrade to verify proper operations is recommended. A simple test may be to:

1. Connect FortiClient on one or two test endpoints to FortiClient EMS.
2. Create a new custom group in FortiClient EMS and add the test endpoints to it.
3. Create new endpoint profiles.
4. Create a new endpoint policy that is configured with the newly created profiles. Assign the policy to the new custom group.
5. Check that FortiClient on the test endpoints received the new profile.

Monitor the system closely over the first few days for any unusual behavior.

Uninstalling FortiClient EMS

Use the *Programs and Features* pane of the Microsoft Windows Control Panel to uninstall FortiClient EMS.

FortiClient EMS installs the following dependencies. If other applications on the same computer are not using them, you can uninstall them manually after removing FortiClient EMS.

- Browser for SQL Server 2017
- Microsoft ODBC Driver 13 for SQL Server
- Microsoft SQL Server 2012 Native Client
- Microsoft SQL Server 2017 (64-bit)
- Microsoft SQL Server 2017 Setup (English)
- Microsoft SQL Server 2017 T-SQL Language Service
- Microsoft Visual C++ 2017 Redistributable (x64) - 14.11.25325.0
- Microsoft Visual C++ 2017 Redistributable (x86) - 14.11.25325.0
- Microsoft VSS Writer for SQL Server 2017

To uninstall EMS:

1. Select *Start > Control Panel > Programs > Uninstall a program*.
2. Select *FortiClient Endpoint Management Server*, and click *Uninstall*.
3. Follow the uninstallation wizard prompts.

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:

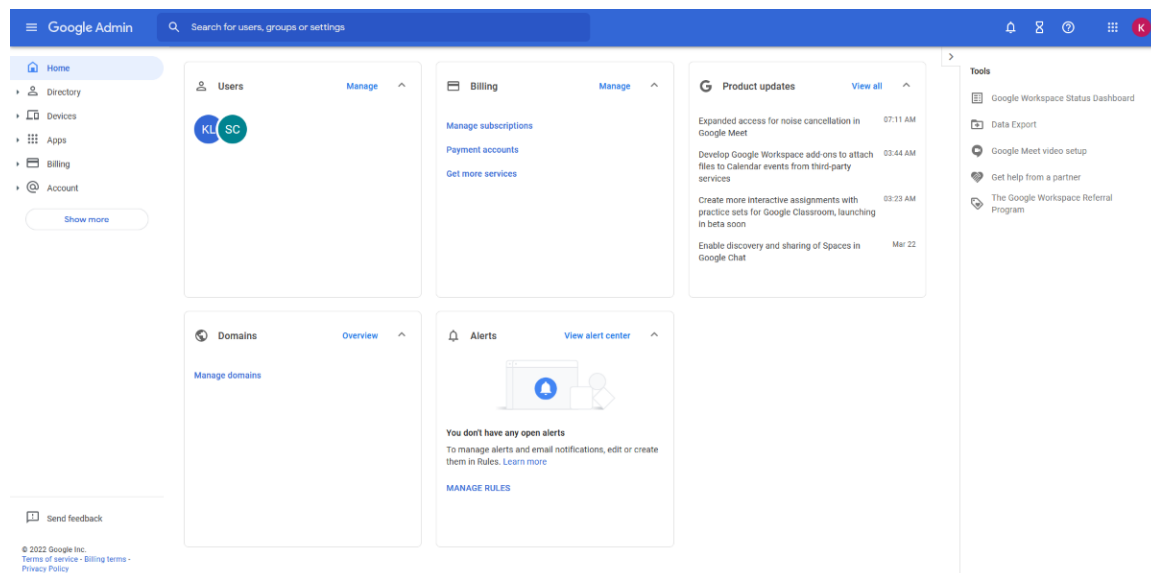
1. Log into the Google Admin console. See [Logging into the Google Admin console on page 53](#).
2. Add the FortiClient Web Filter extension. See [Adding the FortiClient Web Filter extension on page 54](#).
3. Configure the FortiClient Web Filter extension. See [Configuring the FortiClient Web Filter extension on page 54](#).
4. Add the root certificate. See [Adding root certificates on page 55](#).



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.



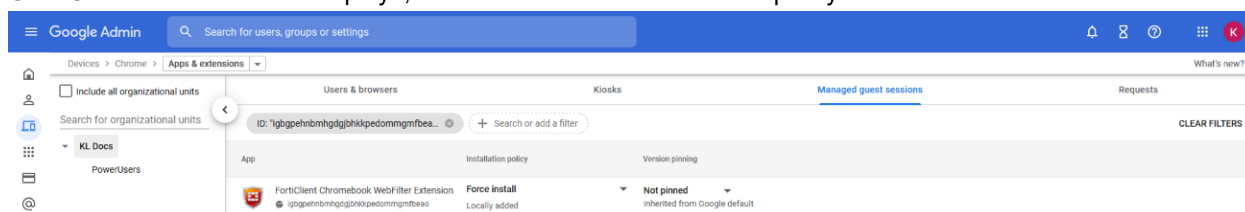
Adding the FortiClient Web Filter extension



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

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: igbgpehnbmhdgjbhkkpedommgmfbear.
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 the following text:

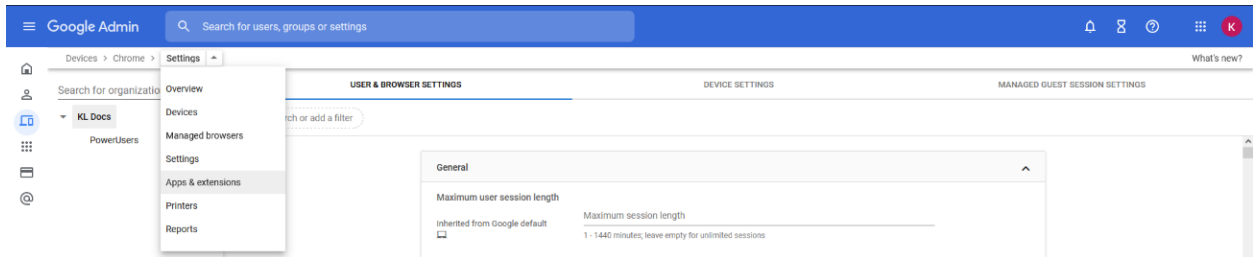
```
{
  "ProfileServerUrl": { "Value": "https://< ProfileServer >:< port for Profile Server >" }
```

```
}
```

For example:

```
{  
  "ProfileServerUrl": { "Value": "https://ems.mydomain.com:8443"}  
}
```

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 340](#).

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 57](#).

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. FortiClient EMS is added as a device to the FortiClient 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 57](#).



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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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*.

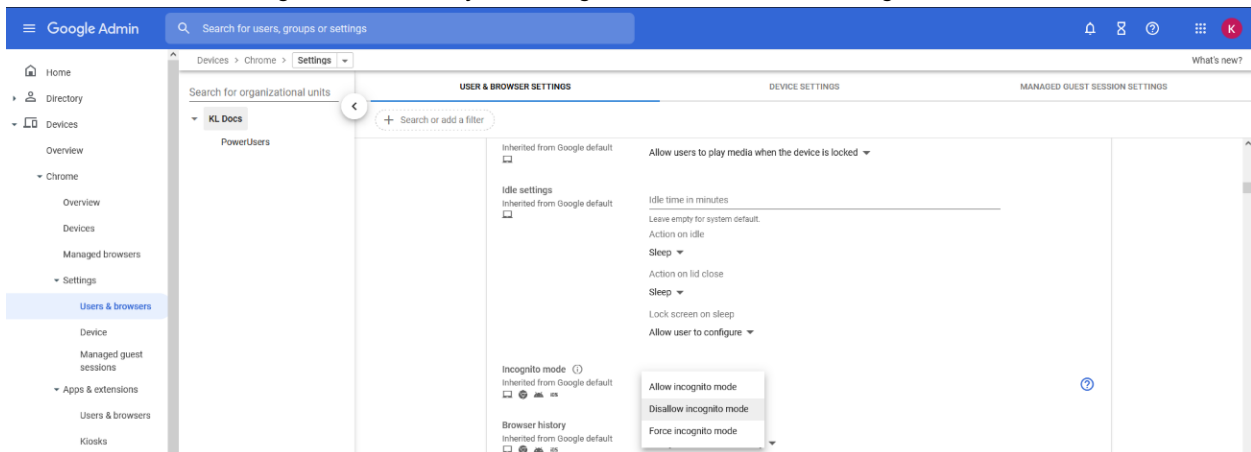
Disallowing incognito mode

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:

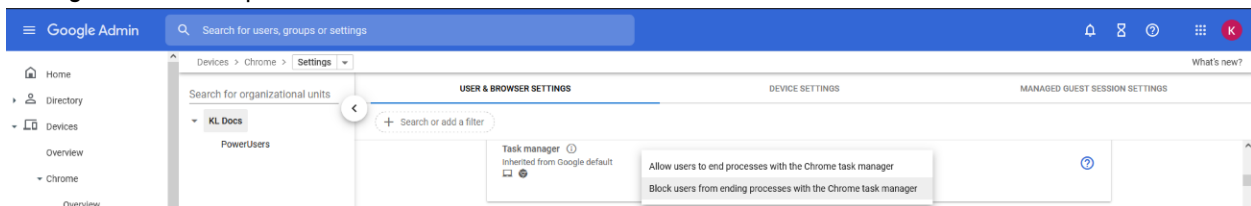
1. In the Google Admin console, go to *Devices > Chrome > Settings > Device*.
2. On the left, select the organization that contains the desired users or enrolled browsers. To select all users and browsers, select the top-level organization. Otherwise, select a child.
3. Under *Sign-in settings*, for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



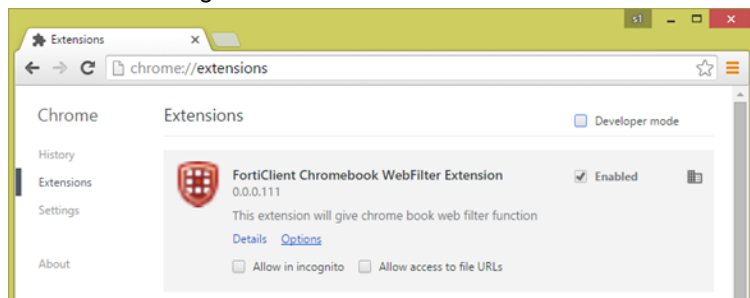
4. Click **Save**.

Verifying the FortiClient Web Filter extension

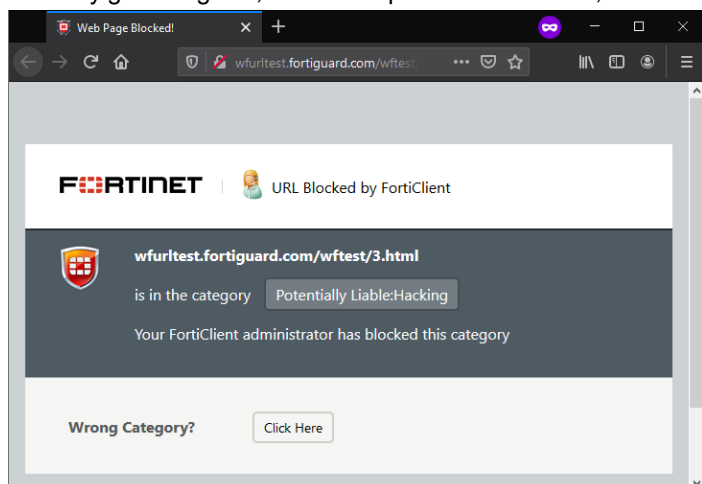
After you add the Google domain to FortiClient EMS, the Google Admin console automatically pushes the FortiClient Web Filter extension to the Chromebooks when users log into the Google domain. You can verify the feature has become available on the Chromebooks.

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 [Adding service account credentials to the Google Admin console on page 64](#).

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 60](#).
2. Add the unique service account credentials to the Google Admin console. See [Adding service account credentials to the Google Admin console on page 64](#).
3. Add the unique service account credentials to FortiClient EMS. See [Adding service account credentials to EMS on page 64](#).

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)
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.

Select

No organization ▾ Search projects and folders 🔍 +

Recent All

Name	ID
✓ My Project	steel-bliss-113623
No organization	0
Customer	customer-0923
demo	third-pad-144322

CANCEL OPEN

- b. Select your organization, if you see an organization dropdown list.
- c. Click the + button.
- d. 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 go to the *Library* tab.
- b. Under *Google Workspace APIs*, click *Admin SDK*.

Google APIs My Project ▾ 🔍

API API Manager

Dashboard

Library


Credentials


Library


Google APIs


Search all 100+ APIs


Popular APIs


**Google Cloud APIs**
Compute Engine API
BigQuery API
Cloud Storage Service
Cloud Datastore API
Cloud Deployment Manager API
Cloud DNS API
More

**Google Cloud Machine Learning**
Vision API
Natural Language API
Speech API
Translation API
Machine Learning Engine API

**Google Maps APIs**
Google Maps Android API
Google Maps SDK for iOS
Google Maps JavaScript API
Google Places API for Android
Google Places API for iOS
Google Maps Roads API
More

**G Suite APIs**
Drive API
Calendar API
Gmail API
Sheets API
Google Apps Marketplace SDK
Admin SDK
More

**Mobile APIs**
Google Cloud Messaging
Google Play Game Services
Google Play Developer API
Google Places API for Android

**Social APIs**
Google+ API
Blogger API
Google+ Pages API
Google+ Domains API

c. Click **ENABLE**.

The screenshot shows the Google API Manager interface. On the left, there's a sidebar with 'API Manager' selected. The main area shows the 'Admin SDK' API page. The 'ENABLE' button is highlighted with a red box. Below the header, there's a section 'About this API' with a description and links to 'Documentation' and 'Try this API in APIs Explorer'. There are also two diagrams: 'Using credentials with this API' showing a flow from 'Your app' to 'User consent' to 'User data', and 'Server-to-server interaction' showing a flow from 'Your service' to 'Authorization' to 'Google service'.

5. Create a service account:

- Go to the *Credentials* tab and select *Create Credentials > Service account key*.
- From the *Service account* list, select *New Service Account*. Enter a service account name.
- From the *Role* list, select *Project > Viewer*.
- Select *P12* as the *Key type* and click *Create*.

The screenshot shows the 'Create service account key' form in the Google API Manager. The 'Service account' dropdown is set to 'New service account'. The 'Service account name' is 'test' and the 'Role' is 'Viewer'. The 'Service account ID' is 'test-410@voltaic-facet-170220.iam.gserviceaccount.com'. Under 'Key type', 'P12' is selected, with a note 'For backward compatibility with code using the P12 format'. The 'Create' button is highlighted.

After you create the service account, a private key with the P12 extension is saved on your computer.



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 **not a secret**.

Service account and key created

New service account **test** has been created.

The account's private key **My Project 2-ac6fe25ed1ac.p12** has been saved on your computer. This is the only copy of the key, so store it securely.

This is the private key's password. It will not be shown again. You must present this password to use the private key. [Learn more](#)

notasecret

[CLOSE](#)

6. Go to the *Credentials* page > *Manage service accounts*.
7. *Edit* the service account you just created and select the *Enable Google Apps Domain-Wide Delegation* checkbox. Enter a *Product name for the consent screen* if this field appears.

Edit service account

Service account name ?

test

☒ Enable G Suite Domain-wide Delegation

Allows this service account to be authorized to access all users' data on a G Suite domain without manual authorization on their part. [Learn more](#)

i To change settings for G Suite domain, product name for the OAuth consent screen must be configured. Assign the product name below or configure the OAuth consent screen.

Product name for the consent screen

Product name

[CANCEL](#) [SAVE](#) [CONFIGURE CONSENT SCREEN](#)

8. Click *Save*.
9. Click *View Client ID* to see your service account information. Record the client ID, service account, and the associated private key (downloaded in step 5d).

Google APIs

My Project

Search

API Manager

Dashboard

Library

Credentials

Client ID for Service account client

DOWNLOAD JSON

DELETE

Service account clients are created when domain-wide delegation is enabled on a service account.

Manage service accounts

Client ID

115703365324425320868

Service account

test

test-410@voltaic-facet-170220.iam.gserviceaccount.com

Creation date

Jun 12, 2017, 1:58:28 PM

Name

Client for test-410

Save

Cancel



To use the private key in EMS, it needs to be converted 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:

Adding service account credentials to the Google Admin console

This section describes how to add the client ID from the service account credentials to the Google Admin console. These settings allow Google to trust FortiClient EMS, which enables FortiClient EMS to retrieve information from the Google domain.

To add service account credentials to the Google Admin console:

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.

4. 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.

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 <i>Browse</i> and select the certificate provided with the service account credentials.

4. Click *Save*.
5. Update the client ID in the Google Admin console.



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:

```
netstat -ano | find "<port number>"
```

a: displays all connections and listening ports

n: displays addresses and port numbers in numerical form

o: displays process ID (PID) associated with each connection

The following shows that Windows is listening to port TCP/8013 on a particular interface: 192.168.1.200 in this case. The PID is 2732.

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>netstat -ano | find "8013"
TCP    192.168.1.200:8013    0.0.0.0:0             LISTENING       2732
```

You can confirm the process by finding that PID on the Task Manager Details tab:

Name	PID	Status	User name	CPU	Memory (p...)	Description
FcmDaemon.exe	2732	Running	SYSTEM	00	9,008 K	FortiClient Endpoint Management Daemon

Connectivity between EMS and FortiClient

In addition to the services running correctly, there must be connectivity between EMS and the endpoint. This section defines connectivity as a route and traffic on a given port. You can use Command Prompt and the built-in Telnet application to verify this. Ensure that Telnet is enabled on your device by going to *Control Panel > Turn Windows features on or off*, and ensuring that the *Telnet Client* checkbox is selected. In this example, 192.168.1.200 is the endpoint IP address, and 445 is the port that is being checked:

```
telnet 192.168.1.200 445
```

If the command is successful, Command Prompt returns `_`. Since the service on 445 is not Telnet, this is the expected result.

If the command is unsuccessful, Command Prompt returns a warning that the connection could not be opened.

C:\WINDOWS\system32\cmd.exe

C:\Users>telnet 192.168.1.200 9999

Connecting To 192.168.1.200...Could not open connection to the host, on port 9999: Connect failed

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 the <i>Configure License</i> page, where you can apply a license by logging in to your FortiCloud account or uploading a license file. See Licensing FortiClient EMS on page 43 .
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 <i>EMS Settings</i> page, where you can import a license. See Configuring EMS settings on page 329 .
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 310 .
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 349 .
Help icon		
	Getting Started	Provides access to links to the FortiClient EMS <i>Release Notes</i> 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: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none"> 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 351](#).

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 <i>EMS for Chromebooks Settings</i> option is enabled in <i>System Settings > EMS Settings</i> .
Endpoints	
All Endpoints	Manage all endpoints.
Manage Domains	Add and manage AD domains.
Domains	Manage endpoints from AD domains. You can also add an AD domain if none exist.
Workgroups	Manage endpoints from workgroups.
Group Assignment Rules	Configure rules to automatically place endpoints into custom groups based on their installer ID, IP address, or OS.

Option	Description
Google Domains	Only available if the <i>EMS for Chromebooks Settings</i> option is enabled in <i>System Settings > EMS Settings</i> .
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 <i>EMS for Chromebooks Settings</i> option is enabled in <i>System Settings > EMS Settings</i> .
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.
Zero Trust Tags	
Zero Trust Tagging Rules	Define Zero Trust tagging rules.
Zero Trust Tag Monitor	View tagged endpoints.
Fabric Device Monitor	View all FortiGates connected to EMS for Zero Trust tagging and the list of tags that are shared with each FortiGate.
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	

Option	Description
Files	View and allowlist files on endpoints that Sandbox or AV has quarantined.
Allowlist	View and delete allowlisted files from the <i>Allowlist</i> 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

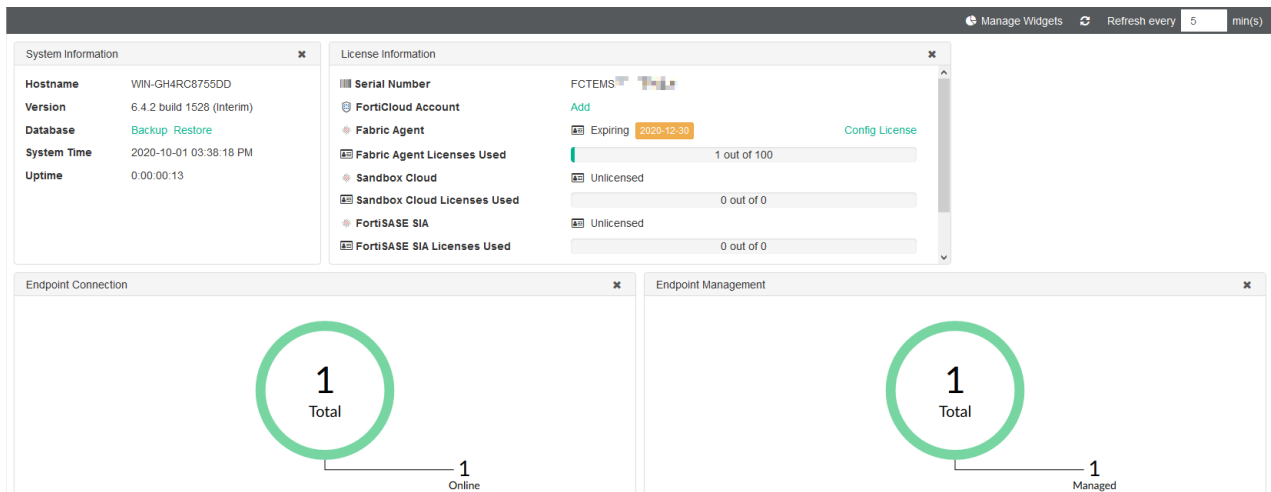
You can use the Dashboard to view summary information about the system and endpoints. You can view summary information about vulnerability scans on endpoints.

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 71](#) and [Status charts and widgets on page 74](#).



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 91](#).
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.

Endpoint Event Summary						Refresh
Endpoint	User	Connection	Lastseen	Current AV Signature Version	New AV Signature Version	
DESKTOP-R04VSP2	user	Online	2020-06-11 12:53:41	1.00000	78.00089	

System Information widget

The following information displays in the *System Information* widget when multitenancy is disabled. If multitenancy is enabled, this information displays in the global site *System Information* widget. See [Global and per-site configuration on](#)

[page 350](#).

Option	Description
Hostname	Name of the computer where you installed FortiClient EMS.
Version	Version number for FortiClient EMS. Also displays the build number. If the current build is an interim build, also displays (<i>Interim</i>) beside the build number.
Database	Options to back up and restore the database. See To back up the database: on page 72 and To restore the database: on page 72 .
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.

To back up the database:

1. Go to *Dashboard > Status*.
2. Beside *Database*, click *Backup*.
3. Set the following options:

Password	Enter a password for backing up and restoring the database.
Confirm password	Reenter the password to confirm it.

4. Click *Back up*. FortiClient EMS backs up the database.

To restore the database:

1. Go to *Dashboard > Status*.
2. Beside *Database*, click *Restore*.
3. Click *Browse*.
4. Locate the database backup file, and click *Open*.
5. In the *Password* field, enter the password used to back up the database.
6. Click *Restore*. When the database is restored, a message appears. The message instructs you to wait for the restored database to reload.
7. Wait for the restored database to be reloaded.

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 49](#).

For details on the features included with each license type, see [Windows, macOS, and Linux licenses on page 22](#).

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 346](#).

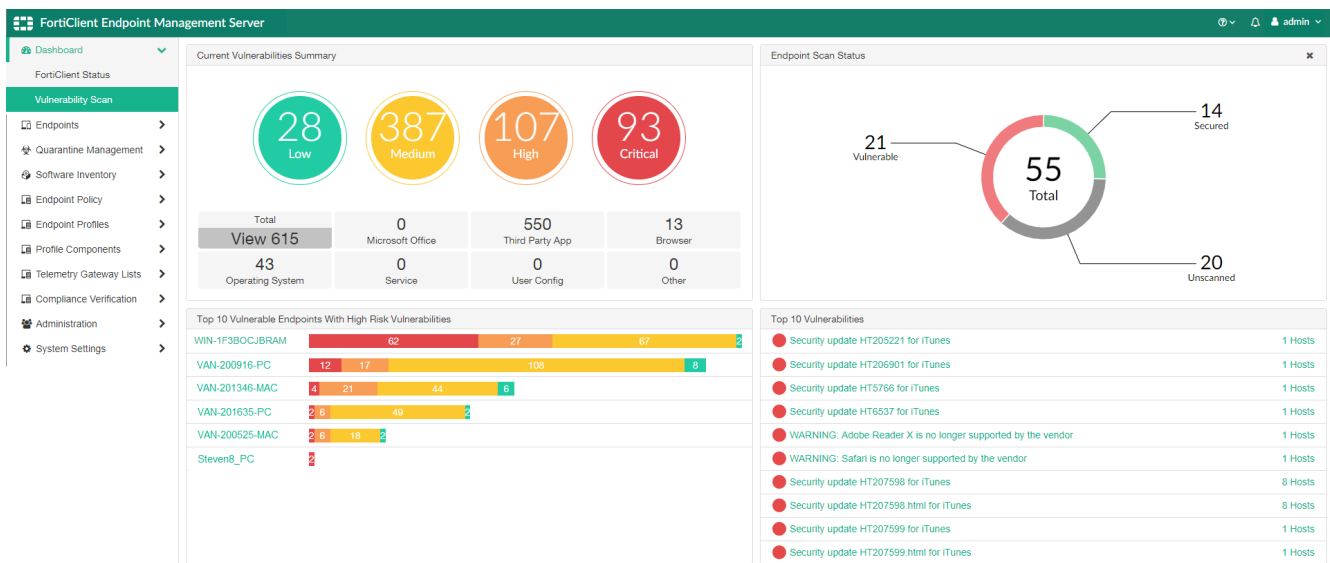
Option	Description
Endpoint Charts	
Endpoint Activity	Shows a summary of endpoint activity information. Categories are: <ul style="list-style-type: none"> EMS On-fabric EMS Off-fabric
Endpoint Alerts	Shows the number of endpoints with alerts, including pending software updates, out-of-date protection, and out-of-sync profiles.
Endpoint Connection	Shows the number of endpoints that are: <ul style="list-style-type: none"> Online Offline for less than one hour Offline Offline for 30 days or more
Managed Mac FortiClient Versions	<p>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.</p> <p>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.</p>
Managed Windows FortiClient Versions	<p>This chart indicates the percentage of Windows endpoints with each version of FortiClient installed. You can sort the data by version or count.</p> <p>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.</p> <p>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.</p>
Managed Linux FortiClient Versions	<p>This chart indicates the percentage of Linux endpoints with each version of FortiClient installed. You can sort the data by version or count.</p>

Option	Description
Endpoint Management	This chart indicates how many endpoints are disconnected and connected.
Mac Operating Systems	<p>This chart indicates the number of endpoints running each version of the macOS operating system. You can sort the data by version or count.</p> <p>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.</p> <p>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.</p>
Windows Operating Systems	<p>This chart indicates the number of endpoints running each version of the Windows operating system. You can sort the data by version or count.</p> <p>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.</p> <p>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.</p>
Linux Operating Systems	<p>This chart indicates the number of endpoints running each version of the Linux operating system. You can sort the data by version or count.</p> <p>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.</p> <p>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.</p>
iPhone Operating Systems	<p>This chart indicates the number of endpoints running each version of the iOS operating system. You can sort the data by version or count.</p> <p>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.</p> <p>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.</p>
Android Operating Systems	<p>This chart indicates the number of endpoints running each version of the Android operating system. You can sort the data by version or count.</p> <p>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.</p> <p>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.</p>

Option	Description
FortiGuard Outbreak Alerts Service	<p>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 267.</p> <p>You can drill down by clicking the outbreak bar. From here, you can quarantine the endpoint if desired.</p>
Top 3 Lists	
Antivirus Detection	This chart indicates the top three endpoints with AV alerts, including the number of AV alerts for each endpoint.
Sandbox Detection	This chart indicates the top three endpoints with FortiSandbox alerts, including the number of FortiSandbox alerts for each endpoint.
Vulnerability Detection	This chart indicates the top three endpoints with vulnerability alerts, including the number of vulnerabilities detected for each endpoint.
Web Filter Detection	This chart indicates the top three endpoints with web filter alerts, including the number of web filter alerts for each endpoint.

Viewing the Vulnerability Scan dashboard

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



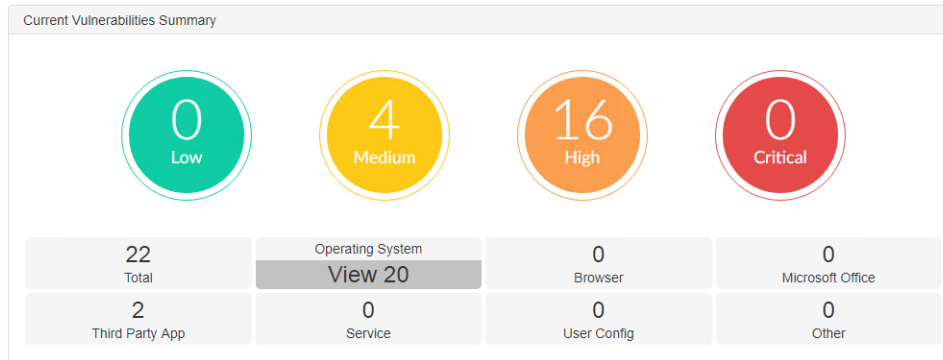
The *Vulnerability Scan* dashboard displays a number of charts. Each chart provides a summary of endpoint information. The sections in each chart are links. You can click sections of the charts or any row in the table to display more details.

Chart	Description
Current Vulnerabilities Summary	<p>Displays the following summaries of current vulnerabilities:</p> <ul style="list-style-type: none"> • 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) <p>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.</p>
Endpoint Scan Status	<p>Displays the following summaries about endpoints:</p> <ul style="list-style-type: none"> • 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:

FortiClient Endpoint Management Server									
<div> <div>Dashboard</div> <div>FortiClient Status</div> <div>Vulnerability Scan</div> <div>Endpoints</div> <div>Quarantine Management</div> <div>Software Inventory</div> <div>Endpoint Policy</div> <div>Endpoint Profiles</div> <div>Profile Components</div> <div>Telemetry Gateway Lists</div> <div>Compliance Verification</div> <div>Administration</div> <div>System Settings</div> </div>									
<div> <div>Operating System Vulnerabilities</div> <div>Patch All</div> <div>Refresh</div> <div>Clear Filters</div> </div>									
Vulnerability Name	FortiGuard ID	CVE ID	Severity	Affected Endpoints	Patch Status				
Microsoft: Jet Database Engine Remote Code Execution Vulnerability	56374	CVE-2019-0538	High	1	Scheduled				
Microsoft: MSHTML Engine Remote Code Execution Vulnerability	56377	CVE-2019-0541	High	1	Scheduled				
Microsoft: Windows Elevation of Privilege Vulnerability	56381	CVE-2019-0543	High	1	Patch				
Microsoft: Windows COM Elevation of Privilege Vulnerability	56386	CVE-2019-0552	High	1	Patch				
Microsoft: XmlDocument Elevation of Privilege Vulnerability	56389	CVE-2019-0555	High	1	Patch				
Microsoft: Windows Runtime Elevation of Privilege Vulnerability	56403	CVE-2019-0570	High	7	Patch				
Microsoft: Jet Database Engine Remote Code Execution Vulnerability	56408	CVE-2019-0575	High	1	Patch				
Microsoft: Jet Database Engine Remote Code Execution Vulnerability	56409	CVE-2019-0576	High	1	Patch				
Microsoft: Jet Database Engine Remote Code Execution Vulnerability	56410	CVE-2019-0577	High	1	Patch				
Microsoft: Jet Database Engine Remote Code Execution Vulnerability	56411	CVE-2019-0578	High	1	Patch				
Microsoft: Jet Database Engine Remote Code Execution Vulnerability	56412	CVE-2019-0579	High	1	Patch				
Microsoft: Jet Database Engine Remote Code Execution Vulnerability	56413	CVE-2019-0580	High	1	Patch				
Microsoft: Jet Database Engine Remote Code Execution Vulnerability	56414	CVE-2019-0581	High	1	Patch				
Microsoft: Jet Database Engine Remote Code Execution Vulnerability	56415	CVE-2019-0582	High	1	Patch				
Microsoft: Jet Database Engine Remote Code Execution Vulnerability	56416	CVE-2019-0583	High	1	Patch				
Microsoft: Jet Database Engine Remote Code Execution Vulnerability	56417	CVE-2019-0584	High	1	Patch				
Microsoft: Windows Kernel Information Disclosure Vulnerability	56375	CVE-2019-0536	Medium	1	Patch				
Microsoft: Windows Kernel Information Disclosure Vulnerability	56383	CVE-2019-0549	Medium	4	Patch				
Microsoft: Windows Kernel Information Disclosure Vulnerability	56388	CVE-2019-0554	Medium	1	Patch				
Microsoft: Windows Kernel Information Disclosure Vulnerability	56402	CVE-2019-0569	Medium	9	Patch				

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	<p>You can click the <i>Patch</i> button to patch the selected vulnerability with the next Telemetry communication between FortiClient EMS and the endpoint.</p> <p>If a patch is already scheduled for the vulnerability, this column displays <i>Scheduled</i>.</p> <p>If the vulnerability must be patched manually, this column displays <i>Manual Patch</i>.</p> <p>FortiClient may be unable to automatically patch the vulnerability due to one of the following reasons:</p> <ul style="list-style-type: none"> • Third-party application vulnerabilities: incorrect or missing installation paths • OS vulnerabilities: Windows update service is disabled <p>In these cases, EMS may incorrectly display the status of these vulnerabilities that were selected to be automatically patched as <i>Scheduled</i> instead of <i>Failed</i>.</p>

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:

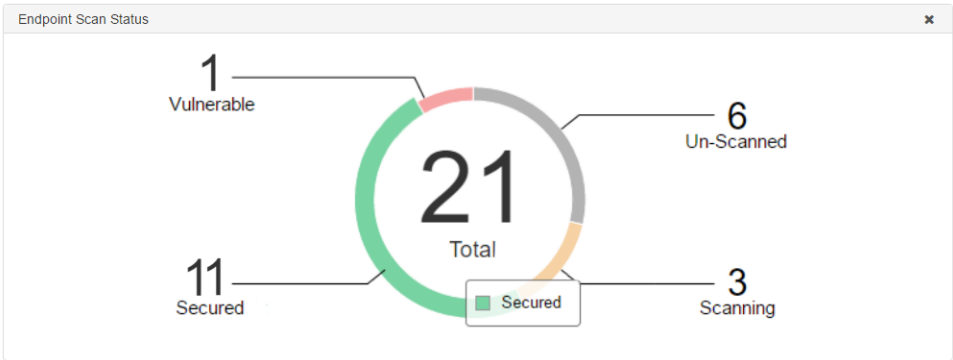
The screenshot shows the FortiClient Endpoint Management Server interface. The left sidebar contains navigation links: Dashboard, FortiClient Status, Vulnerability Scan, Endpoints, Quarantine Management, Software Inventory, Endpoint Policy, and Endpoint Profiles. The main content area is titled 'Medium Severity Vulnerabilities' and includes a 'Patch All' button. It displays a table with columns: Vulnerability Name, FortiGuard ID, CVE ID, Category, Affected Endpoints, and Patch Status. Two vulnerabilities are listed: 'Security update HT6245 for iTunes' and 'Security update HT205636 for iTunes'. Each entry has a 'Patch' button next to it.

Vulnerability Name	FortiGuard ID	CVE ID	Category	Affected Endpoints	Patch Status
Security update HT6245 for iTunes	21877	CVE-2014-1296 CVE-2014-8842	Application	1	Patch
Security update HT205636 for iTunes	21885	CVE-2015-7048 CVE-2015-7095 CVE-2015-7096 CVE-2015-7097 CVE-2015-7098 CVE-2015-7099 CVE-2015-7100	Application	1	Patch

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:

FortiClient Endpoint Management Server				
Dashboard Vulnerability Endpoint Patch All Refresh Clear Filters				
Hostname	Username	Vulnerability		Patch Status
WIN-1F3BOCJBRAM	Administrator	11	20	5 Patch
WIN-1F3BOCJBRAM	Administrator	2		Manual Patch

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	<p>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.</p> <p>The same endpoint also has 2 critical vulnerabilities that must be manually patched.</p>
Patch Status	You can click the <i>Patch</i> 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.

Vulnerability	Category	Severity	Patch Status
Security update HT5766 for iTunes	Application	Critical	Patch
Security update HT5936 for iTunes	Application	Critical	Patch
Security update HT6537 for iTunes	Application	Critical	Patch
Security update HT205221 for iTunes	Application	Critical	Patch
Security update HT206901 for iTunes	Application	Critical	Patch
Security update HT207598 for iTunes	Application	Critical	Patch
Security update HT207599 for iTunes	Application	Critical	Patch
Security update HT207928 for iTunes	Application	Critical	Patch
Security update HT207598.html for iTunes	Application	Critical	Patch
Security update HT207599.html for iTunes	Application	Critical	Patch
Security update HT207928.html for iTunes	Application	Critical	Patch
Security update HT6001 for iTunes	Application	High	Patch
Security update HT204949 for iTunes	Application	High	Patch
Security update HT205372 for iTunes	Application	High	Patch
Security update HT206379 for iTunes	Application	High	Patch
Security update HT207158 for iTunes	Application	High	Patch
Security update HT207274 for iTunes	Application	High	Patch
Security update HT207427 for iTunes	Application	High	Patch
Security update HT207486 for iTunes	Application	High	Patch
Security update HT207805 for iTunes	Application	High	Patch
Security update HT208141 for iTunes	Application	High	Patch

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.

FortiClient Endpoint Management Server

Dashboard

FortiClient Status

Vulnerability Scan

Endpoints

Quarantine Management

Software Inventory

Endpoint Policy

Endpoint Profiles

Profile Components

Telemetry Gateway Lists

Compliance Verification

Administration

Vulnerabilities for WIN-1F3BOCJBRAM

Refresh

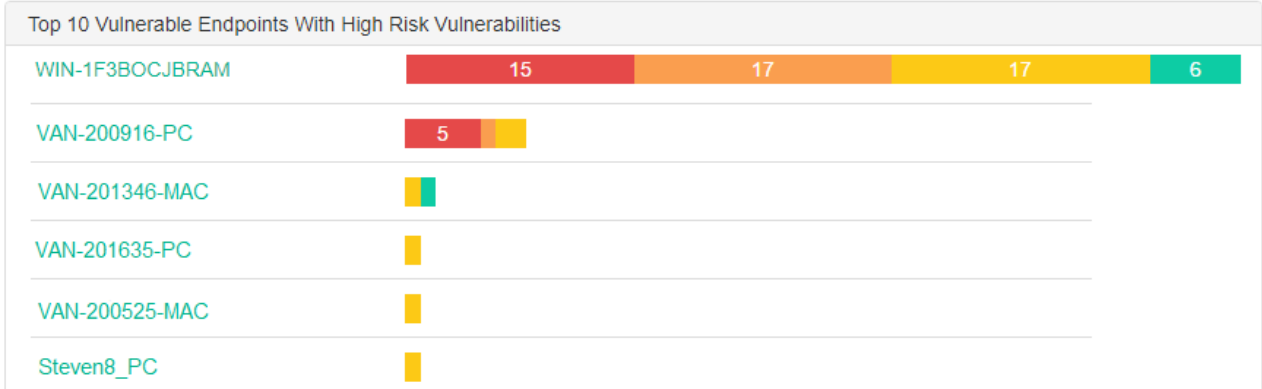
Clear Filters

Vulnerability	Category	Severity	Patch Status
Security update HT5766 for iTunes	Application	Critical	Patch
Security update HT5936 for iTunes	Application	Critical	Patch
Security update HT6537 for iTunes	Application	Critical	Patch
Security update HT205221 for iTunes	Application	Critical	Patch
Security update HT206901 for iTunes	Application	Critical	Patch
Security update HT207598 for iTunes	Application	Critical	Patch
Security update HT207599 for iTunes	Application	Critical	Patch
Security update HT207928 for iTunes	Application	Critical	Patch
Security update HT207598.html for iTunes	Application	Critical	Patch
Security update HT207599.html for iTunes	Application	Critical	Patch
Security update HT207928.html for iTunes	Application	Critical	Patch

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

Viewing the top 10 vulnerable endpoints with high risk vulnerabilities

- To view the top 10 vulnerable endpoints with high risk vulnerabilities:
- 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	Category	Severity	Patch Status
WARNING: Safari is no longer supported by the vendor	Application	Critical	Manual Patch
WARNING: Adobe Reader X is no longer supported by the vendor	Application	Critical	Manual Patch
Security update HT5766 for iTunes	Application	Critical	Patch
Security update HT5936 for iTunes	Application	Critical	Patch
Security update HT6537 for iTunes	Application	Critical	Patch
Security update HT205221 for iTunes	Application	Critical	Patch
Security update HT206901 for iTunes	Application	Critical	Patch
Security update HT207598 for iTunes	Application	Critical	Patch
Security update HT207599 for iTunes	Application	Critical	Patch
Security update HT207928 for iTunes	Application	Critical	Patch
Security update HT207598.html for iTunes	Application	Critical	Patch
Security update HT207599.html for iTunes	Application	Critical	Patch
Security update HT207928.html for iTunes	Application	Critical	Patch
Security update HT6001 for iTunes	Application	High	Patch
Security update HT204949 for iTunes	Application	High	Patch
Security update HT205372 for iTunes	Application	High	Patch
Security update HT206379 for iTunes	Application	High	Patch
Security update HT207158 for iTunes	Application	High	Patch
Security update HT207274 for iTunes	Application	High	Patch
Security update HT207427 for iTunes	Application	High	Patch
Security update HT207486 for iTunes	Application	High	Patch
Security update HT207805 for iTunes	Application	High	Patch

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.

FortiClient Endpoint Management Server						
Dashboard	Vulnerabilities for WIN-1F3BOCJBRAM					
FortiClient Status	Vulnerability	Category	Severity	Patch Status		
Vulnerability Scan	Security update HT5766 for iTunes	Application	Critical	Patch		
Endpoints	Security update HT5936 for iTunes	Application	Critical	Patch		
Quarantine Management	Security update HT6537 for iTunes	Application	Critical	Patch		
Software Inventory	Security update HT205221 for iTunes	Application	Critical	Patch		
Endpoint Policy	Security update HT206901 for iTunes	Application	Critical	Patch		
Endpoint Profiles	Security update HT207598 for iTunes	Application	Critical	Patch		
Profile Components	Security update HT207599 for iTunes	Application	Critical	Patch		
Telemetry Gateway Lists	Security update HT207928 for iTunes	Application	Critical	Patch		
Compliance Verification	Security update HT207598.html for iTunes	Application	Critical	Patch		
Administration	Security update HT207599.html for iTunes	Application	Critical	Patch		

Viewing top ten vulnerabilities on endpoints

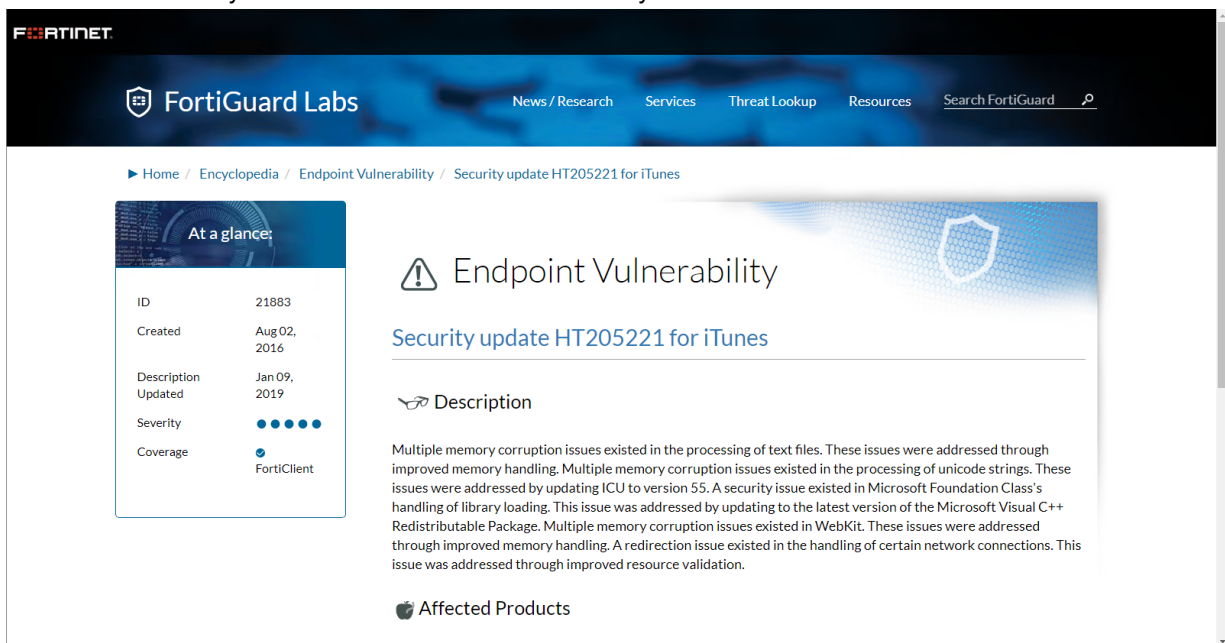
To view top ten vulnerabilities on endpoints:

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.

Top 10 Vulnerabilities	
Security update HT205221 for iTunes	1 Hosts
Security update HT206901 for iTunes	1 Hosts
Security update HT5766 for iTunes	1 Hosts
Security update HT6537 for iTunes	1 Hosts
WARNING: Adobe Reader X is no longer supported by the vendor	1 Hosts
WARNING: Safari is no longer supported by the vendor	1 Hosts
Security update HT207598 for iTunes	8 Hosts
Security update HT207598.html for iTunes	8 Hosts
Security update HT207599 for iTunes	1 Hosts
Security update HT207599.html for iTunes	1 Hosts

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.

FortiClient Endpoint Management Server				
Dashboard	Affected Endpoints			
FortiClient Status				
Vulnerability Scan				
Hostname	Username	Last Seen	Scan Time	
WIN-1F3B0CJB8AM	Administrator	2019-01-17 00:45:50	2019-01-17 00:05:09	

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.

FortiClient Endpoint Management Server					
Dashboard	Vulnerabilities for WIN-1F3BOCJBRAM				
FortiClient Status	Vulnerability	Category	Severity	Patch Status	
Vulnerability Scan	WARNING: Safari is no longer supported by the vendor	Application	Critical	Manual Patch	
	WARNING: Adobe Reader X is no longer supported by the vendor	Application	Critical	Manual Patch	
Endpoints	Security update HT5766 for iTunes	Application	Critical	Patch	
Quarantine Management	Security update HT5936 for iTunes	Application	Critical	Patch	
Software Inventory	Security update HT6537 for iTunes	Application	Critical	Patch	
Endpoint Policy	Security update HT205221 for iTunes	Application	Critical	Patch	
Endpoint Profiles	Security update HT206901 for iTunes	Application	Critical	Patch	
Profile Components	Security update HT207598 for iTunes	Application	Critical	Patch	
Telemetry Gateway Lists	Security update HT207599 for iTunes	Application	Critical	Patch	
Compliance Verification	Security update HT207928 for iTunes	Application	Critical	Patch	
Administration	Security update HT207598.html for iTunes	Application	Critical	Patch	
System Settings	Security update HT207599.html for iTunes	Application	Critical	Patch	
	Security update HT207928.html for iTunes	Application	Critical	Patch	
	Security update HT6001 for iTunes	Application	High	Patch	
	Security update HT204949 for iTunes	Application	High	Patch	
	Security update HT205372 for iTunes	Application	High	Patch	
	Security update HT206379 for iTunes	Application	High	Patch	
	Security update HT207158 for iTunes	Application	High	Patch	
	Security update HT207274 for iTunes	Application	High	Patch	
	Security update HT207427 for iTunes	Application	High	Patch	
	Security update HT207486 for iTunes	Application	High	Patch	
	Security update HT207806 for iTunes	Application	High	Patch	
	38 entries loaded				

Vulnerability	Name of the vulnerability.
Category	Category of the vulnerability.
Severity	Severity level of the vulnerability.
Patch Status	<p>You can click the <i>Patch</i> 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 <i>Scheduled</i>.</p> <p>If the vulnerability must be patched manually, this column displays <i>Manual Patch</i>.</p> <p>FortiClient may be unable to automatically patch the vulnerability due to one of the following reasons:</p> <ul style="list-style-type: none"> Third-party application vulnerabilities: incorrect or missing installation paths OS vulnerabilities: Windows update service is disabled <p>In these cases, EMS may incorrectly display the status of these vulnerabilities that were selected to be automatically patched as <i>Scheduled</i> instead of <i>Failed</i>.</p>

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 <i>System Settings > Logs</i> .
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 <i>System Settings > Logs</i> .
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 193 .
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 193 .
Others	
System Information	See System Information widget on page 71 .
License Information	See License Information widget on page 73 .

Endpoint management

FortiClient EMS needs to determine which devices to manage. For Windows, macOS, and Linux endpoints, device information can come from an AD 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 283](#).

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 OUs, containers, and groups from the AD server to EMS. The *Changes to Selected Base DN* pane summarizes the changes to your selected base DNs.
5. Click *Save*.

Adding endpoints using an Azure AD server

To add endpoints using an Active Directory (AD) domain server, you must configure add an Azure AD server to EMS in *Administration > Authentication Servers*. See [Adding an Azure AD server on page 284](#).

To add endpoints using an Azure AD 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**.

Domain Import View Azure Group Import Tutorial

Azure Server:

Sync every: Minutes
⚠ The minimum sync period is 60 minutes

Group Selection Behaviour:
ⓘ Only the selected Azure users, groups and devices will be imported

Base Group

Group Name	Source	Import as Base Group
_Group	Azure	<input type="checkbox"/>
DnsAdmins	On Prem	<input type="checkbox"/>
ADSyncPasswordSet	On Prem	<input type="checkbox"/>
_group	Azure	<input type="checkbox"/>
DnsUpdateProxy	On Prem	<input type="checkbox"/>
_group2	Azure	<input type="checkbox"/>
ADSyncBrowse	On Prem	<input type="checkbox"/>
R&D_NA	On Prem	<input type="checkbox"/>
ADSyncAdmins	On Prem	<input type="checkbox"/>
_group	Azure	<input checked="" type="checkbox"/>

Changes to Base Group

Status	Group
<input checked="" type="checkbox"/> Will be Added	_group

Endpoints > Domains lists the Azure AD server domain groups and subgroups. It lists subgroups as a flat list and does not preserve the hierarchy from the AD 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 on the *Endpoints* pane.

To view the *Endpoints* pane:

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

Not Installed	Number of endpoints that do not have FortiClient installed. Click to display the list of endpoints without FortiClient installed.
Not Registered	Number of endpoints that are not connected to 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: <i>Device</i> , <i>User</i> , <i>IP</i> , <i>Configurations</i> , <i>Connections</i> , and <i>Alerts and Events</i> .
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 <i>Enter</i> 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: <ul style="list-style-type: none"> • 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.

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: <ul style="list-style-type: none">• 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 13](#).
- Clear Events
- Mark as Uninstalled
- Set Importance
- Set Custom Tags. This option is only available if you have already created a custom tag.
- Delete Device
- Send Message. See [Sending endpoints one-way message on page 97](#).

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 135 .
Network Status	Displays the following information for the networks that the endpoint is connected to: <ul style="list-style-type: none"> • 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.
Zero Trust Tags	Displays which tags have been applied to the endpoint based on the Zero Trust tagging rules. See Zero Trust Tags on page 246 .
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 267 .
Connection	Displays the connection status between the selected endpoint and FortiClient EMS.
Configuration	Displays the following information for the selected endpoint: <ul style="list-style-type: none"> • 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 currently 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 <i>Add</i> 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.

	<p>You can assign a classification tag to multiple endpoints by selecting the endpoints, then selecting <i>Action > Set Importance</i> or <i>Set Custom Tags</i>. Tags that FortiClient EMS receives from FortiAnalyzer also display under <i>Classification Tags</i>.</p> <p>See Sending endpoint classification tags to FortiAnalyzer on page 102.</p>
Classification Tags - Fabric	<p>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 <i>Classification Tags - Fabric</i>. You can also unassign a tag from the endpoint. The following lists the predefined tags for FortiEDR use:</p> <ul style="list-style-type: none"> • 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. <p>See Identity Management integration.</p>
Status	<p>Displays one of the following statuses:</p> <ul style="list-style-type: none"> • 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 101 .
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, <i>Security update available for Adobe Reader</i> .
	Category	Displays the vulnerability's category. For example, <i>Third Party App</i> .
	Application	Displays the name of the application with the vulnerability.
	Severity	Displays the vulnerability's severity.
	Patch Type	Displays the patch type for this vulnerability: <i>Auto</i> or <i>Manual</i> .
	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.
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.

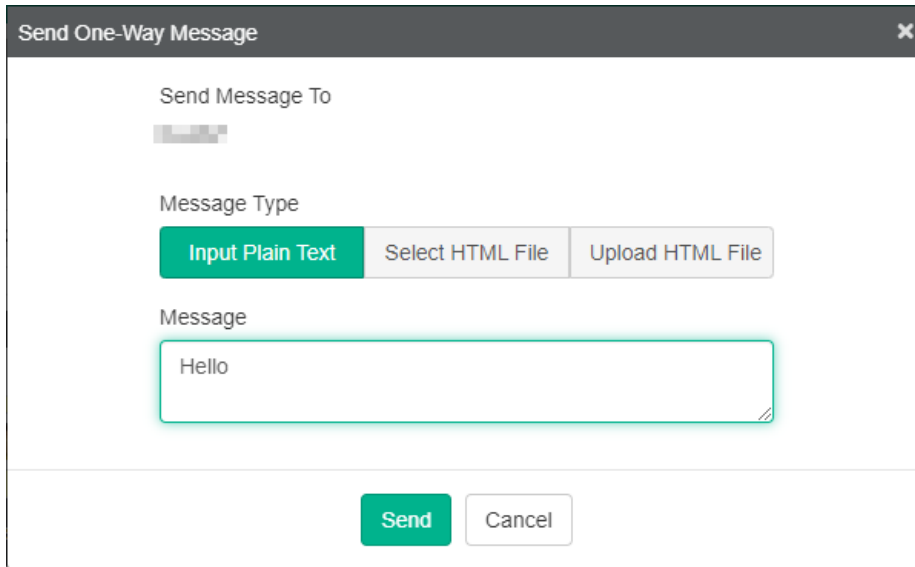
The message can be in plain text or HTML format.

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:

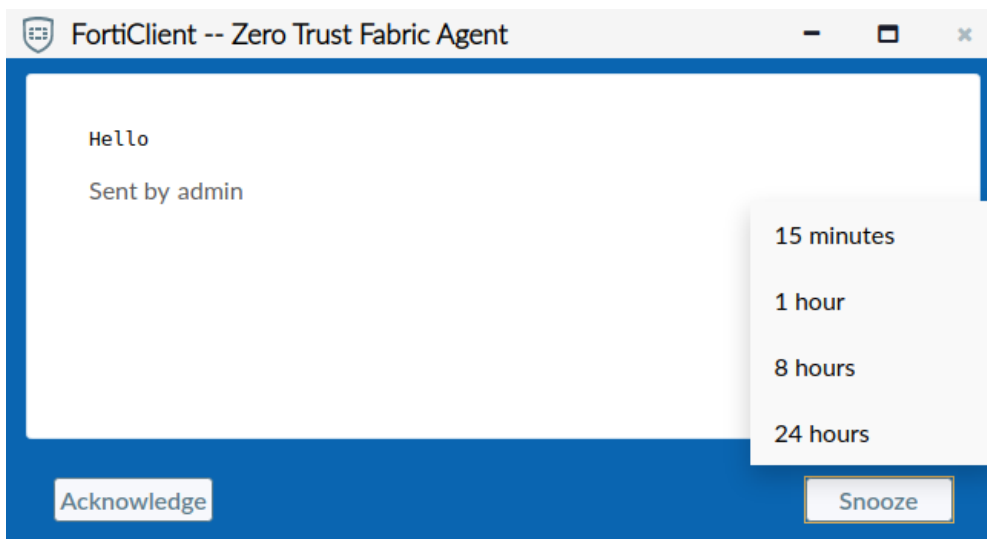
- a.** To send a plain text message, select *Input Plain Text*. In the *Message* field, enter the desired text. Click *Send*.



The image shows a 'Send One-Way Message' dialog box. It has a title bar with a close button. Inside, there's a 'Send Message To' field with a blurred placeholder. Below that is the 'Message Type' section with three buttons: 'Input Plain Text' (highlighted in green), 'Select HTML File', and 'Upload HTML File'. Underneath is a 'Message' text area containing the word 'Hello'. At the bottom are 'Send' and 'Cancel' buttons.

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

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



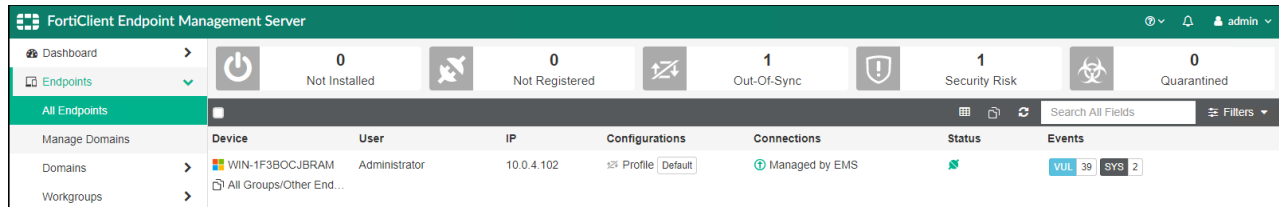
FortiClient logs a system event for when the user snoozes the message and when they acknowledge it.

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 91](#).

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 Zero Trust tagging and classification tags. See Zero Trust Tags on page 246 and Viewing the Endpoints pane on page 91 .
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 <i>Synced</i> and <i>Out-Of-Sync</i> . 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.
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 <i>Bookmark</i> 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 <i>Search</i> button to apply the filter setting.
Reset	Click the <i>Reset</i> button to clear the filter settings.
Bookmark	Click the <i>Bookmark</i> 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.

credit_report.exe (High Risk) [Quarantine Endpoint]

Timeline: Threat Detected (2019-03-26 20:38:53) → Sandbox Analysis (2019-03-26 20:38:53) → File Blocked (2019-03-26 20:40:34) → Dynamic Signature Updated (2019-03-26 20:40:34)

Endpoint: ledington
 Lola Edington
 ledington@gmail.com
 +1 236 735 0814
 All Groups/Smart PowerGrid/Research and Development/DevOps
 Device: Cherrywood
 OS: Microsoft Windows 8.1 Enterprise
 IP: 10.127.131.102
 Mac Address: 00-15-5d-a1-a6-0d
 Last Seen: 2019-03-26 20:48:43
 Vulnerability: 3

Indicators (1)
 42 out of 100 Machine learning verdict score based on peysay static scan

File Information

Command Line	c:\work\4357810084146248730.exe	Filename	credit_report.exe
Score	41	File Path	C:\Users\ledington\Downloads\appliance\credit_report.exe
Rating	High Risk	File Size	4096(bytes)
Rated by	Sandboxing	MD5	e830a79ea31f1191593d335360648c0
Instances	1	SHA1	2656dc7173b7fe40f368cd1467efa4d87243afe7
Host Affected	1	SHA256	72be2f392bb165d29794f9445d89b3ae48de1555ec3e91374f4c73tae8806c1
		Virus Total	Q

Process Tree

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

Rating: High Risk
Rated by: Sandboxing

Instances: 1
Host Affected: 1

File Size: 4096(bytes)
MD5: e830a79ea31f1191593d335360648c0
SHA1: 2656dc7173b7fe40f368cd1467efa4d87243afe7
SHA256: 72be2f392bb165d29794f9445d89b3ae48de1555ec3e91374f4c73tae8806c1
Virus Total: Q

Process Tree

Details

Process Information	File Operations	Network Operations
PID	3572	
File Path	%CURRENTFILE%	
File Type	exe	
CMD Line	c:\work\4357810084146248730.exe	
MD5	e830a79ea31f1191593d335360648c0	

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, then 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.

Create New Fabric Connector

FortiClient EMS

Configuration | Actions

Name: EMS Connector

Description: Connector to execute remote EMS operations

IP/FQDN: 172.17.81.170

Username: admin

Password: ••••••••

Status: ☒ ON

< Back OK Cancel

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.

Endpoint	Tags	User	MAC Address	IP Address	FortiClient UUID	Hardware	Vulnerability
DESKTOP-RIK3OAS	all_registered_clients, Medium, Department A	Robert Clasper	00:15:5d:90:f2:00	192.168.137.243	D05A4CF2856240D4856C243AEF1E6A1D	WIN64	

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 210](#).

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 346](#).

To quarantine an endpoint:

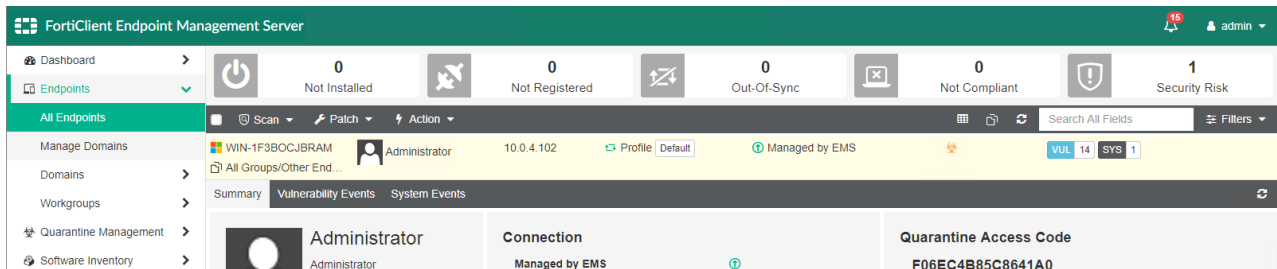
1. Go to *Endpoints*.
2. Click *All Endpoints*, a domain, or workgroup. A list of endpoints displays.

- 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 Security Fabric offers visibility of endpoints 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

You must connect FortiClient to both the EMS and FortiGate. The FortiGate and FortiClient must both be sending logs to the FortiAnalyzer. You must configure the EMS IP address on the FortiGate, as well as administrator login credentials.

This configuration 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 the login credentials for 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

1. You must create a profile for the endpoint. See [Creating a new profile on page 140](#).
2. 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 127](#).
3. Enable *Remote HTTPS access*. See [Configuring EMS settings on page 329](#).

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 firewall address object](#). This is only required if using a FortiOS version earlier than 6.2.0.
5. [Configure EMS endpoint control](#).

To create an automation trigger, enter the following commands in the CLI:

```
config system automation-trigger
  edit "trigger01"
    set trigger-type event-based
    set event-type ioc
    set ioc-level high
  next
end
```

To create an automation action, enter the following commands in the CLI:

```
config system automation-action
  edit "action01"
    set action-type quarantine-forticlient
    set minimum-interval 0
  next
end
```

To create an automation stitch, enter the following commands in the CLI:

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

To create an EMS firewall address object, enter the following commands in the CLI:

This step is only necessary when using a version of FortiOS prior to 6.2.0.

```
config firewall address
  edit "EMS01"
    set type ipmask
    set subnet <EMS_IP_address> 255.255.255.255
  next
end
```

To configure EMS endpoint control:

There are separate instructions when using FortiOS 6.2.0 or a later version, and a version of FortiOS earlier than 6.2.0.

If using FortiOS 6.2.0 or a later version, do the following:

1. Go to *Security Fabric > Settings*.
2. Enable *FortiClient Endpoint Management System (EMS)*.
3. In the *Name* field, enter the desired EMS name.
4. In the *IP/Domain Name* field, enter the EMS IP address or FQDN.
5. In the *Serial Number* field, enter the EMS serial number. You can find this in the *System Information* widget on the EMS dashboard.
6. In the *Admin User* field, enter the EMS admin username.
7. In the *Password* field, enter the admin user's password.
8. Click *Apply*.

If using a FortiOS version earlier than 6.2.0, enter the following commands in the CLI. In the following commands, <EMS_SERIAL_NUMBER> is the EMS serial number, <EMS_ADMIN> is the EMS administrator name, and <PASSWORD> is the EMS administrator's password:

```
config endpoint-control forticlient-ems
  edit "e01"
    set address "EMS01"
    set serial-number <EMS_SERIAL_NUMBER>
    set rest-api-auth userpass
    set https-port 443
    set admin-username <EMS_ADMIN>
    set admin-password <PASSWORD>
    set admin-type Windows
  next
end
```

Executing automation

Once prerequisites are met, you can trigger the automation process. The following procedure triggers the quarantine action on the endpoint at <endpoint_ip_address>:

```
diag endpoint forticlient-ems-rest-api queue-quarantine-ipv4 <endpoint_ip_address>
```

After this action, EMS and FortiOS both display that the endpoint is quarantined.

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.

Group assignment rules

You can use group assignment rules to automatically place endpoints into custom groups based on their installer ID, IP address, or OS.

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 their installer ID, IP address, or OS.

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 113](#).
2. Create a FortiClient deployment package. Specify the "HQ" installer ID when creating or uploading the installer. See [Adding a FortiClient deployment package on page 123](#).
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 113](#).
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 113](#).
2. With the next FortiClient Telemetry communication, endpoints with the specified OS installed 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.

FortiClient Endpoint Management Server				
Dashboard	Run Rules Now Add Refresh			
Endpoints	Installer ID / IP Range/ OS	Group	Priority	Enabled
All Endpoints	HQ	HQ	1	<input checked="" type="checkbox"/>
Manage Domains	192.168.0.0/24	West Coast/Seattle	2	<input checked="" type="checkbox"/>
Domains	Windows Server	West Coast	3	<input checked="" type="checkbox"/>

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.

FortiClient Endpoint Management Server				
Dashboard	Edit Delete	Schedule Run Run Rules Now Add Refresh		
Endpoints	Rule	Group	Priority	Enabled
All Endpoints	HQ	HQ	1	<input type="checkbox"/>
Manage Domains	192.168.0.0/24	West Coast/Seattle	2	<input checked="" type="checkbox"/>
Domains	Windows Server	West Coast	3	<input checked="" type="checkbox"/>

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

FortiClient Endpoint Management Server				
Dashboard	Edit Delete	Schedule Run Run Rules Now Add Refresh		
Endpoints	Rule	Group	Priority	Enabled
All Endpoints	192.168.0.0/24	West Coast/Seattle	1	<input checked="" type="checkbox"/>
Manage Domains	HQ	HQ	2	<input checked="" type="checkbox"/>
Domains	Windows Server	West Coast	3	<input checked="" type="checkbox"/>

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 *Add*.
3. Under *Type*, select *Installer ID*.
4. In the *Installer ID* field, enter the desired installer ID.
5. In the *Group* field, do one of the following:
 - a. To place the endpoints into an existing group, select the desired group from the dropdown list.
 - b. To place the endpoints into a new group, click *Create a new group* and 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 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:
 - a. To place the endpoints into an existing group, select the desired group from the dropdown list.
 - b. To place the endpoints into a new group, click *Create a new group* and 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 2008" to only place endpoints that have Windows Server 2008 installed into the specified endpoint group.
5. In the *Group* field, do one of the following:
 - a. To place the endpoints into an existing group, select the desired group from the dropdown list.
 - b. To place the endpoints into a new group, click *Create a new group* and 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*.

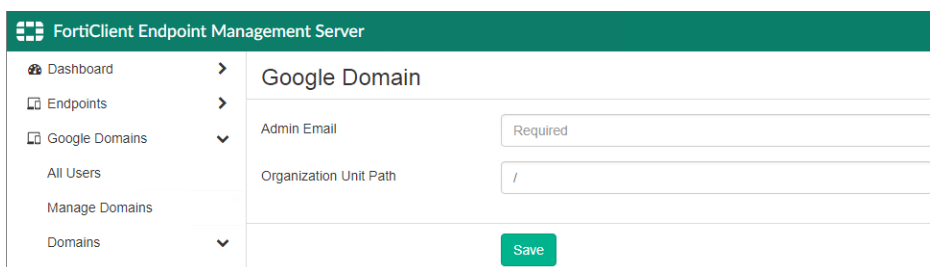
Google Domains

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 <i>System Settings > Logs</i> .
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 <i>System Settings > Logs</i> .

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 12](#).

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.
Action	Select <i>Install</i> or <i>Uninstall</i> .
Deployment Package	Select the desired deployment package from the dropdown list.
Start at a Scheduled Time	Specify what time to start installing FortiClient on endpoints. If this feature is disabled, the FortiClient installation starts immediately without user interaction.
Unattended Installation	When enabled, the end user cannot modify the installation schedule. If needed, the device reboots without warning logged-in users.
Reboot When Needed	Reboot the endpoint to install FortiClient when needed.
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.
Enable the Deployment	Enable or disable.

4. Click *Save*.

Managing deployment configuration priority levels

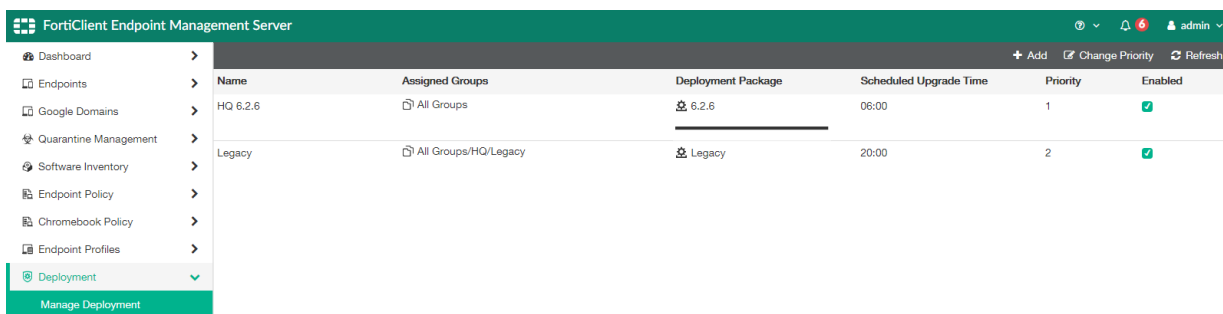
An endpoint may be eligible for multiple deployment configurations. When an endpoint is eligible for multiple endpoint deployment configurations, the following factors determine which configuration EMS applies to the endpoint:

1. EMS applies deployment configurations to endpoints only if the configurations are enabled on the *Deployment > 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:

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*.

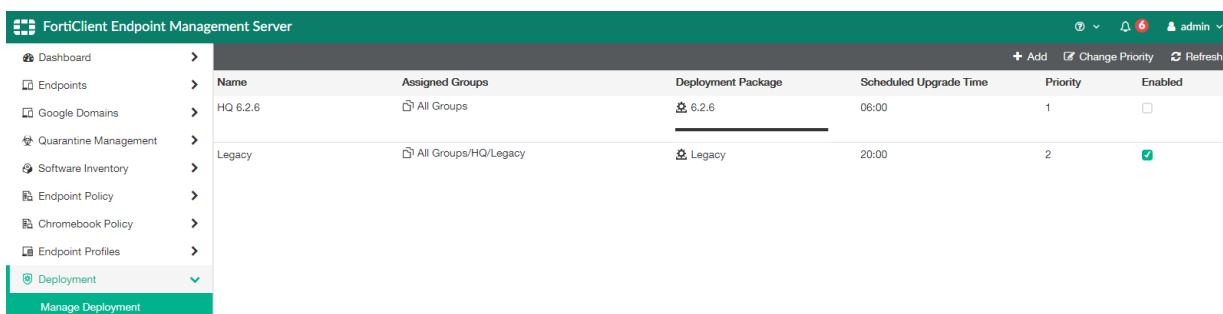
In the example, consider an endpoint that belongs to the Legacy group. The endpoint applies for two configurations. In this case, EMS applies the HQ deployment configuration to the endpoint, since the HQ configuration has a higher priority level than the Legacy configuration.



The screenshot shows the FortiClient Endpoint Management Server interface. On the left is a navigation menu with options: Dashboard, Endpoints, Google Domains, Quarantine Management, Software Inventory, Endpoint Policy, Chromebook Policy, Endpoint Profiles, and Deployment (selected). Below the menu is a 'Manage Deployment' button. The main area displays a table with columns: Name, Assigned Groups, Deployment Package, Scheduled Upgrade Time, Priority, and Enabled. There are two rows: 'HQ 6.2.6' with priority 1 and 'Legacy' with priority 2. Both are enabled (checked).

Name	Assigned Groups	Deployment Package	Scheduled Upgrade Time	Priority	Enabled
HQ 6.2.6	All Groups	6.2.6	06:00	1	<input checked="" type="checkbox"/>
Legacy	All Groups/HQ/Legacy	Legacy	20:00	2	<input checked="" type="checkbox"/>

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



This screenshot is similar to the previous one, but the 'HQ 6.2.6' configuration is now disabled (unchecked). The 'Legacy' configuration remains enabled (checked) and is at priority 2.

Name	Assigned Groups	Deployment Package	Scheduled Upgrade Time	Priority	Enabled
HQ 6.2.6	All Groups	6.2.6	06:00	1	<input type="checkbox"/>
Legacy	All Groups/HQ/Legacy	Legacy	20:00	2	<input checked="" type="checkbox"/>

You can reenabling 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.

FortiClient Endpoint Management Server						
	Name	Assigned Groups	Deployment Package	Scheduled Upgrade Time	Priority	Enabled
	Legacy	All Groups/HQ/Legacy	Legacy	20:00	1	<input checked="" type="checkbox"/>
	HQ 6.2.6	All Groups	6.2.6	06:00	2	<input checked="" type="checkbox"/>

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:

Prompt option	Description
<i>Install Now</i>	FortiClient performs the upgrade and automatically restarts your computer.
<i>Install Later</i>	Indicate the time to start the upgrade. The default is 8:00 PM. Your computer automatically restarts after the upgrade finishes.
<i>No Option</i>	<p>If you do not select an option, the upgrade occurs by default at 8:00 PM. After FortiClient EMS uninstalls the previous version, it asks if the user wants to reboot. The prompt requests the user to do one of the following:</p> <ul style="list-style-type: none"> • <i>Reboot</i>: have the reboot occur immediately. • <i>Reboot later</i>: reboot the computer later. You cannot select a specific reboot time. Use this option at your discretion.

Deploying different installer IDs to endpoints using the same deployment package

As [Installer ID group assignment rules on page 111](#) 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 deployment package on page 123](#).
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 113](#).
3. Install FortiClient on endpoints using the following CLI commands:

Installer	CLI command
.msi	<pre>msiexec /i forticlient.msi GROUP_TAG="<installer_ID>"</pre> <p>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:</p> <pre>msiexec /i "FortiClient Setup.msi" GROUP_TAG="<installer_ID>"</pre>
.exe	<pre>FortiClientSetup_7.2.1_x64.exe /v"GROUP_TAG=<installer_ID>"</pre>

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_7.2.1_x64.exe /v"GROUP_TAG=HR"
FortiClientSetup_7.2.1_x64.exe /v"GROUP_TAG=Marketing"
FortiClientSetup_7.2.1_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 deployment package



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

To add a deployment package:

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

Installer Type	Use an official or custom FortiClient installer. When using a custom FortiClient installer, you can select from a list of previously uploaded installers, or upload a new custom installer. You can also remove previously created installers. To upload a new custom FortiClient installer, enter the desired name, then upload Windows (64-bit and 32-bit) and/or macOS 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 or macOS installation file. The installation files on the Fortinet Customer Service & Support and FortiClient.com websites are not available in .msi or .zip format. You must package the installer as an .msi or .zip file to upload it.
Release	Select the FortiClient release version to install.
Patch	Select the specific FortiClient patch version to install.
Keep updated to the latest patch	Enable EMS to repackage EMS-created FortiClient deployment package to the latest patch release.

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.

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



Available options may differ depending on the features you have enabled or disabled in *Feature Select*. See [Feature Select on page 346](#).

Zero Trust Telemetry	Enabled by default and cannot be disabled. Installs FortiClient with Telemetry enabled.
Secure Access Architecture Components	<p>Install FortiClient with SSL and IPsec VPN enabled. Disable to omit SSL and IPsec VPN support from the FortiClient deployment package.</p> <p>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.</p> <p>See Remote Access on page 143 for details on configuring a VPN tunnel.</p>
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.
Additional Security Features	<p>Enable any of the following features:</p> <ul style="list-style-type: none"> • Malware <ul style="list-style-type: none"> • AntiVirus, Anti-Exploit, Removable Media Access • Anti-Ransomware • Cloud Based Malware Outbreak Detection • Web Filtering • Application Firewall • Single Sign-On mobility agent • Zero Trust Network Access. Note that the zero trust network access feature is always installed on a macOS endpoint, regardless of whether this option is enabled or disabled. • Privilege Access Management <p>Disable to exclude features from the FortiClient deployment package.</p>

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.

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

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.

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 111](#). 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 122](#).

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.

7. 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.
8. 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 (32-bit and 64-bit), .msi, and .dmg files depending on the configuration. The following shows an example of a deployment package that includes .exe, .msi, and .dmg files. The end user can download these files to install FortiClient on their machine with the desired configuration.

Name	Last modified	Size
 Parent Directory		-
 msi/	2019-04-29 15:00	-
 FortiClient_6.2.0.DMG	2019-04-29 15:21	76M
 FortiClientSetup_6.2.0_x64.exe	2019-04-29 15:22	108M
 FortiClientSetup_6.2.0_x86.exe	2019-04-29 15:21	90M



If the *Sign software packages* option is enabled in *System Settings > EMS Settings*, Windows deployment packages display as being from the publisher specified in the certificate file. See [Configuring EMS settings on page 329](#).

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:

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	<p>Search for and select desired domain users to apply the policy to.</p> <p>If an endpoint is applicable for both a user-based and a group-based policy, the user-based policy takes precedence and is applied to the endpoint.</p>
Profile (Off-Fabric)	<p>Configure the desired endpoint profiles to apply to the endpoint when it is off-fabric according to the on-fabric detection rules configured in this policy. For example, you may want to apply more restrictive profiles to the endpoint when it is determined to be off-fabric. From the dropdown list, select the desired endpoint profiles.</p> <p>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.</p> <p>When you enable this toggle, the <i>Profile</i> 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.</p>
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 <i>Profile XML</i> button. This downloads one XML file that contains the XML configuration for all selected endpoint profiles.

If *Profile (Off-Fabric)* is enabled, you can use the *Off-Fabric Profile XML* button to download an XML file that contains the XML configuration for all selected endpoint profiles for off-fabric endpoints.

On-Fabric Detection Rules

Select the on-fabric detection rules to include in the policy. You can select multiple rules.

You must have already created on-fabric detection rules to include them in an endpoint policy. See [On-fabric Detection Rules on page 135](#).

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*.

Endpoint Policy

Edit

Users

Optional

Profile (Off-Fabric)

☒

Profile

VPN

Remote Access P...

Default

ZTNA

ZTNA01

Default

WEB

WF_EMS

Default

VULN

Default

Default

MW

Default

Default

SB

Default

Default

FW

Default

Default

SYS

Default

Default

Download Profile XML

Profile XML

Off-Fabric Profile XML

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

Endpoint Policies						
+ Add Change Priority Refresh Clear Filters Edit Columns						
Name	Assigned Groups	Profile Components		Off Net Profile Compon...	Policy Components	Endpoint C...
Policy_1	No Groups Assigned	<div>VPN</div>	Remot...	<div>VPN</div>	Default	0
		<div>ZTNA</div>	ZTNA01	<div>ZTNA</div>	Default	
		<div>WEB</div>	WF_EMS	<div>WEB</div>	Default	
		<div>VULN</div>	Default	<div>VULN</div>	Default	
		<div>MW</div>	Default	<div>MW</div>	Default	
		<div>SB</div>	Default	<div>SB</div>	Default	
		<div>FW</div>	Default	<div>FW</div>	Default	
		<div>SYS</div>	Default	<div>SYS</div>	Default	
Default		<div>VPN</div>	Default	<div>VPN</div>	Default	0
		<div>ZTNA</div>	Default	<div>ZTNA</div>	Default	
		<div>WEB</div>	Default	<div>WEB</div>	Default	
		<div>VULN</div>	Default	<div>VULN</div>	Default	
		<div>MW</div>	Default	<div>MW</div>	Default	
		<div>SB</div>	Default	<div>SB</div>	Default	
		<div>FW</div>	Default	<div>FW</div>	Default	
		<div>SYS</div>	Default	<div>SYS</div>	Default	

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 determines which policy to apply using the following order:
 - a. If there is a policy directly assigned to the user (configured in the *Users* field for the endpoint policy), EMS assigns that policy to the endpoint.
 - b. If there are policies assigned to the group container and/or user group, EMS assigns the policy with the highest priority level to the endpoint.
 - c. If there are inherited policies for group container and/or user group (policies assigned to a parent container or group), EMS assigns the policy with the highest priority level 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.

Name	Endpoint Groups	Endpoint Profile	Policy Components	Telemetry Gateway List	Usage Count	Priority	Enabled
Seattle_general	All Groups/Seattle	PROFILE Seattle_general OFF-NET Seattle_offnet	ON-NET a	FGT_Seattle_floor1	1	1	<input type="checkbox"/>
SF_general	All Groups/SF	PROFILE SF_general			1	2	<input checked="" type="checkbox"/>
Seattle_HR	All Groups/Seattle/HR	PROFILE Seattle_HR		FGT_Seattle_floor2	1	3	<input checked="" type="checkbox"/>

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.

Name	Endpoint Groups	Endpoint Profile	Policy Components	Telemetry Gateway List	Usage Count	Priority	Enabled
Seattle_general	All Groups/Seattle	PROFILE Seattle_general OFF-NET Seattle_offnet	ON-NET a	FGT_Seattle_floor1	1	1	<input checked="" type="checkbox"/>
SF_general	All Groups/SF	PROFILE SF_general			1	2	<input checked="" type="checkbox"/>
Seattle_HR	All Groups/Seattle/HR	PROFILE Seattle_HR		FGT_Seattle_floor2	1	3	<input checked="" type="checkbox"/>

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.

Name	Endpoint Groups	Endpoint Profile	Policy Components	Telemetry Gateway List	Usage Count	Priority	Enabled
Seattle_general	All Groups/Seattle	PROFILE Seattle_general OFF-NET Seattle_offnet	ON-NET a	FGT_Seattle_floor1	1	1	<input type="checkbox"/>
SF_general	All Groups/SF	PROFILE SF_general			1	2	<input checked="" type="checkbox"/>
Seattle_HR	All Groups/Seattle/HR	PROFILE Seattle_HR		FGT_Seattle_floor2	1	3	<input checked="" type="checkbox"/>

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.

Name	Endpoint Groups	Endpoint Profile	Policy Components	Telemetry Gateway List	Usage Count	Priority	Enabled
SF_general	All Groups/SF	PROFILE SF_general			1	1	<input checked="" type="checkbox"/>
Seattle_HR	All Groups/Seattle/HR	PROFILE Seattle_HR		FGT_Seattle_floor2	1	2	<input checked="" type="checkbox"/>
Seattle_general	All Groups/Seattle	PROFILE Seattle_general OFF-NET Seattle_offnet	ON-NET a	FGT_Seattle_floor1	1	3	<input checked="" type="checkbox"/>

Editing endpoint policy view

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

To edit endpoint policy view:

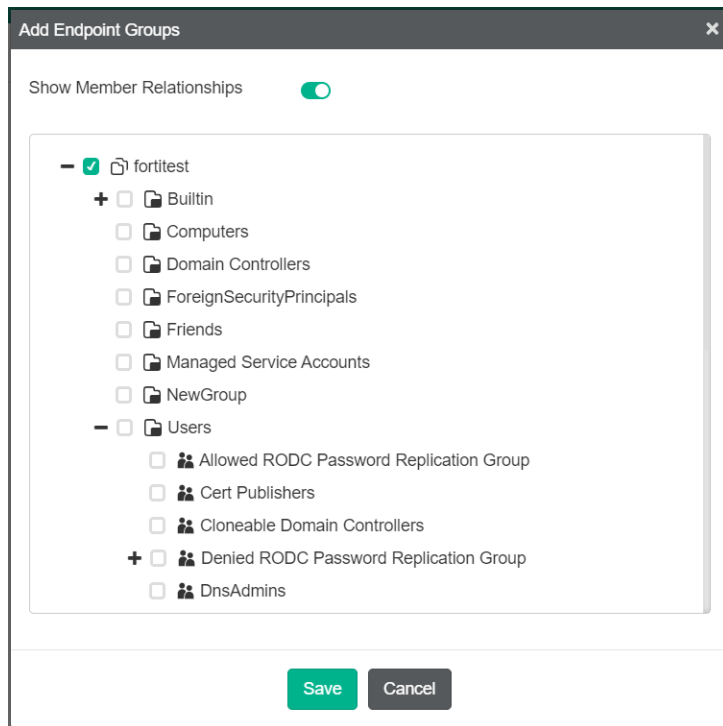
1. Go to *Endpoint Policy & Components Manage Policies*.
2. Click *Edit Columns*.
3. Enable or disable the columns as desired.
4. Click *Save*.

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.

FortiClient Endpoint Management Server						
<div> <div>Dashboard</div> <div>Endpoints</div> <div>Quarantine Management</div> <div>Software Inventory</div> <div>Endpoint Policy</div> <div>Manage Policies</div> <div>Endpoint Profiles</div> <div>Deployment</div> </div> <div> <div>Edit</div> <div>Delete</div> <div>Add</div> <div>Change Priority</div> <div>Refresh</div> <div>Clear Filters</div> <div>Edit Columns</div> </div>						
Name	Assigned Groups	Profile	Policy Components	Endpoint Count	Enabled	
Policy_1	All Groups	<div>PROFILE Profile_1</div> <div>OFF-NET Default</div> <div>100% ✓</div>		<div>1</div> <div>4 endpoints not seen for last 30 days</div>	✓	
Policy_2	<div>fortitest</div> <div>pbuffay</div> <div>rgreen</div>	<div>PROFILE Profile_2</div> <div>OFF-NET Default</div> <div>100% ✓</div>		<div>2</div>	✓	
Default		<div>PROFILE Default</div>		<div>0</div>	✓	

Click the endpoint count to see the endpoint list.

FortiClient Endpoint Management Server							
Endpoints (4)							
Hostname	User	Policy	Profile	Off-Net Profile	Connection	Last Seen	
DESKTOP-6DQIEPJ	J	Policy_1	Profile_1	Default	Not Managed	2020-05-01 13:07:15	
MKP-DRichey	Dexter Richey	Policy_1	Profile_1	Default	Not Managed	2020-05-01 13:07:33	
MKP-GFrakes	Grant Frakes	Policy_1	Profile_1	Default	Not Managed	2020-05-01 13:07:33	
MKP-RIHock	Rachelle Hock	Policy_1	Profile_1	Default	Not Managed	2020-05-01 13:07:34	

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 the [FortiClient EMS Administration Guide](#).

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

FortiClient Endpoint Management Server						
<div> <div>Dashboard</div> <div>Endpoints</div> <div>Quarantine Management</div> <div>Software Inventory</div> <div>Endpoint Policy</div> <div>Manage Policies</div> <div>Endpoint Profiles</div> <div>Deployment</div> <div>Manage Deployment</div> </div>						
Name	Assigned Groups	Deployment Package	Scheduled Upgrade Time	Priority	Enabled	
Deployment_Group1	All Groups/Other Endpoints	Deployment_6.4		1	<input checked="" type="checkbox"/>	
Deployment_Group2	fortitest/ForeignSecurityPrincipals fortitest/Managed Service Accounts	Deployment_6.2.6		2	<input type="checkbox"/>	

CA Certificates

If FortiOS is connected to EMS using the EMS API, deep inspection is enabled, and the Fabric connection between FortiOS and FortiClient EMS has already been 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 223](#). 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 223](#).

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 127](#).

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

To add an on-fabric detection rule set:

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

Detection type	Description
DHCP Server	<p>On the <i>IP/MAC Address</i> tab, configure the IP and/or MAC address for the desired DHCP server. On the <i>DHCP Code</i> tab, configure the DHCP code for the desired DHCP server. You can configure just the <i>IP/MAC Address</i> tab, just the <i>DHCP Code</i> tab, or both tabs. If configuring the <i>IP/Mac Address</i> tab, the MAC Address field is optional.</p> <p>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 137.</p> <p>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.</p>
DNS Server	<p>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.</p>
EMS Connection	<p>The only available option for this detection type is that EMS considers the endpoint as satisfying the rule if it is online with EMS.</p>

Detection type	Description
Local IP/Subnet	<p>In the <i>IP Range</i> field, enter a range of IP addresses. In the <i>Default Gateway MAC Address</i> 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.</p> <p>This is the only detection type that applies to endpoints running FortiClient 6.4.0 and earlier versions. Other detection types do not apply to these endpoints.</p>
Default Gateway	<p>In the <i>IP Address</i> field, enter the default gateway IP address. In the <i>MAC Address</i> 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.</p>
Ping Server	<p>In the <i>IP Address</i> 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.</p>
Public IP	<p>In the <i>IP Address</i> 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.</p>
Connection Media	<p>From the <i>Ethernet</i> and/or <i>Wi-Fi</i> dropdown lists, select <i>Connected</i> or <i>Not Connected</i>. EMS considers the endpoint as satisfying the rule if its network settings match all configured fields.</p>
VPN Tunnel	<p>In the <i>Name</i> field, enter an SSL or IPsec VPN tunnel name. EMS considers the endpoint as satisfying the rule if it is connected to a VPN tunnel with a matching name. You can configure tunnels using the + button.</p>

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

To edit an on-fabric detection rule set:

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

To delete an on-fabric detection rule set:

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

3. Click *Delete*.
4. In the confirmation dialog, click *Yes*.

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

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

To enable/disable an on-fabric detection rule:

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

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

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

To configure the DHCP code:

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

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

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

The screenshot shows a dialog box titled "Predefined Options and Values". It has a blue header bar with a question mark icon and a close button (X). The dialog contains the following fields and controls:

- Option class:** A dropdown menu showing "DHCP Standard Options".
- Option name:** A dropdown menu showing "224 FortiClient On-Net Status".
- Buttons:** "Add...", "Edit...", and "Delete" buttons are located below the "Option name" dropdown.
- Description:** A text field containing "FortiClient On-Net Status".
- Value:** A large text area containing "FGT37D4Q11111111". To the right of the text area are up and down arrow buttons. Below the text area are left and right arrow buttons and an "Edit Array..." button.
- Footer:** "OK" and "Cancel" buttons. The "OK" button is highlighted with a red rectangle.

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 127](#).

Endpoint Profiles

FortiClient EMS has separate endpoint profiles for the following features:

- [Remote Access on page 143](#)
- [ZTNA Destinations on page 174](#)
- [Web Filter on page 193](#)
- [Video Filter on page 206](#)
- [Vulnerability Scan on page 208](#)
- [Malware Protection on page 210](#)
- [Sandbox on page 219](#)
- [Firewall on page 222](#)
- [System Settings on page 223](#)

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 127](#).

You can also import profiles to EMS.

Editing a default profile

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

To edit a default profile:

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

Creating a new profile

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

To create a profile to configure FortiClient:

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

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

Adding a new Chromebook profile

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

You can add new Chromebook profiles to deploy different settings to Chromebook 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 142](#).
 - 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 descriptions of general remote access settings.

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 <i>Connect/Disconnect</i> button when using <i>Auto Connect</i> with VPN.

Configuration	Description
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.
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.
Use Vendor ID	Use vendor ID. Enter the vendor ID in the <i>Vendor ID</i> field.
Enable Secure Remote Access	FortiClient denies or allows the endpoint to connect to a VPN tunnel based on the tunnel's <i>Host Tag</i> configuration. See the <i>Host Tag</i> field description in SSL VPN on page 145 and IPsec VPN on page 148 .
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.
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 135 .
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	<p>Configure network lockdown for off-fabric endpoints when they are not connected to SSL VPN.</p> <p>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 SSL 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, as well as 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.</p>

Configuration	Description
Grace Period	Configure a grace period in seconds during which an off-fabric endpoint that is not connected to SSL VPN can continue to access LAN and the Internet without restrictions.
Maximum Connection Attempts	Configure the maximum number of attempts for the end user of an off-fabric endpoint to enter valid SSL VPN credentials.
Excluded Applications	Enter the path to applications that an off-Fabric endpoint that is not connected to SSL VPN can still access.
Excluded IPs	Enter IP addresses that an off-Fabric endpoint that is not connected to SSL VPN can still access.

SSL VPN

This topic contains descriptions of SSL VPN settings.

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 <i>Prefer SSL VPN DNS</i> 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 SSL 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.

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 <i>SSL VPN</i> .
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.
Require Certificate	Require a certificate.
Prompt for Username	Prompt for the username when accessing VPN.
Split Tunnel	
Application Based	<p>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:</p> <ul style="list-style-type: none"> • Microsoft Office 365 • Microsoft Teams • Skype • GoToMeeting • Zoom • WebEx • YouTube <p>Once the VPN tunnel is up, FortiClient binds the specified excluded applications to the physical interface.</p>
Type	Select <i>Include</i> or <i>Exclude</i> to configure whether to include or exclude certain application traffic from the VPN tunnel.
Local Applications	<p>You can only exclude local applications from the VPN tunnel. Click <i>Add</i>. In the <i>Add Application(s)</i> 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.</p> <p>For example, to exclude Microsoft Teams and Firefox from the VPN tunnel, you can enter any of the following combinations:</p> <ul style="list-style-type: none"> • 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\ <p>To find a running application's full path, on the <i>Details</i> tab in Task Manager, add the <i>Image path name</i> column.</p> <p>Select the application checkbox, then click <i>Remove</i> to remove it from the list.</p>
Cloud Applications	<p>You can exclude or include cloud applications. Click <i>Add</i>. In the list, select the desired applications, then click <i>Add</i>.</p> <p>Select the application checkbox, then click <i>Remove</i> to remove it from the list.</p>

Domain	<p>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 <i>Add</i>. In the <i>Add Domain(s)</i> field, enter the desired domains, using ; to configure multiple entries.</p> <p>For example, if you configure the VPN tunnel to exclude youtube.com, youtube.com and *.youtube.com are excluded from the tunnel.</p> <p>Select the application checkbox, then click <i>Remove</i> to remove it from the list.</p>
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. See SAML SSO on page 302 .
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 169 .
Use External Browser as User-agent for SAML Login	Display the SAML authentication prompt in an external browser instead of in the FortiClient GUI. See Using a browser as an external user-agent for SAML authentication in an SSL VPN connection on page 161 .
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 Azure Active Directory credentials. See Autoconnect on logging in as an Azure AD user on page 167 .
Redundant Sort Method	<p>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.</p> <p>When <i>Server</i> is selected, FortiClient tries the order explicitly defined in the server settings.</p> <p>When <i>Ping Speed</i> is selected, FortiClient determines the order by the ping response speed.</p> <p>When <i>TCP Round Trip Time</i> is selected, FortiClient determines the order by the TCP round trip time.</p>
Tag	Select <i>Allow</i> or <i>Prohibit</i> , then select the desired Zero Trust tag from the <i>Select a Tag</i> dropdown list. Tags only display in the list if they are already configured. See Zero Trust Tags on page 246 .

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 Zero Trust tagging rule that tags all endpoints without up-to-date AV signatures. See [Adding a Zero Trust tagging rule set on page 246](#).
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.

FortiClient (macOS) and (Linux) do not support this feature.

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 Zero Trust tag. For the example configuration described in the <i>Host Tag</i> 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 login.
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	PC 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.

Configuration	Description
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.

When you click the *Add Tunnel* button in the *VPN Tunnels* section, 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:

Basic Settings	
Name	Enter a VPN name. Use only standard alphanumeric characters. Do not use symbols or accented characters.
Type	Select <i>IPsec VPN</i> .
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.
Authentication Method	Select the authentication method for the VPN.
Pre-Shared Key	Enter the preshared key required. Available if you selected <i>Pre-Shared Key</i> for <i>Authentication Method</i> .
Prompt for Username	Prompt for the username when accessing VPN.
Split Tunnel	
Application Based	<p>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:</p> <ul style="list-style-type: none"> • Microsoft Office 365 • Microsoft Teams • Skype • GoToMeeting • Zoom

	<ul style="list-style-type: none"> • WebEx • YouTube <p>Once the VPN tunnel is up, FortiClient binds the specified excluded applications to the physical interface.</p>
Type	Select <i>Include</i> or <i>Exclude</i> to configure whether to include or exclude certain application traffic from the VPN tunnel.
Local Applications	<p>You can only exclude local applications from the VPN tunnel. Click <i>Add</i>. In the <i>Add Application(s)</i> 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.</p> <p>For example, to exclude Microsoft Teams and Firefox from the VPN tunnel, you can enter any of the following combinations:</p> <ul style="list-style-type: none"> • 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\ <p>To find a running application's full path, on the <i>Details</i> tab in Task Manager, add the <i>Image path name</i> column.</p> <p>Select the application checkbox, then click <i>Remove</i> to remove it from the list.</p>
Cloud Applications	<p>You can exclude or include cloud applications. Click <i>Add</i>. In the list, select the desired applications, then click <i>Add</i>.</p> <p>Select the application checkbox, then click <i>Remove</i> to remove it from the list.</p>
Domain	<p>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 <i>Add</i>. In the <i>Add Domain(s)</i> field, enter the desired domains, using ; to configure multiple entries.</p> <p>For example, if you configure the VPN tunnel to exclude youtube.com, youtube.com and *.youtube.com are excluded from the tunnel.</p> <p>Select the application checkbox, then click <i>Remove</i> to remove it from the list.</p>
VPN Settings	
IKE	Select <i>Version 1</i> or <i>Version 2</i> .
Mode	Select <i>Main</i> or <i>Aggressive</i> .
Options	Select <i>Mode Config</i> , <i>Manual Set</i> , or <i>DHCP over IPsec</i> .
Specify DNS Server (IPv4)	Specify the DNS server for the VPN tunnel. Available if you selected <i>Manual Set</i> .

Assign IP Address (IPv4)	Enter the IP address to assign for the VPN tunnel. Available if you selected <i>Manual Set</i> .
Split Table	Enter the IP address and subnet mask for the VPN tunnel. Available if you selected <i>Manual Set</i> or <i>DHCP over IPsec</i> .
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.
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.
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.
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.
Advanced Settings	
Enable One-Time Password	Enable one-time password.
Enable XAuth	When IKEv1 is selected, enable IKE Extended Authentication (xAuth). When IKEv2 is selected, enable Extensible Authentication Protocol (EAP).
XAuth Timeout	Only available if <i>Enable XAuth</i> 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 <i>VPN</i> 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.
Failover SSL VPN Connection	If the IPsec VPN connection fails, FortiClient attempts to connect to the specified SSL VPN tunnel.
Enable SAML Login	Enable SAML SSO login for this VPN tunnel. See SAML SSO on page 302 .
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 <i>Server</i> is selected, FortiClient tries the order explicitly defined in the server settings. When <i>Ping Speed</i> is selected, FortiClient determines the order by the ping response speed. When <i>TCP Round Trip Time</i> is selected, FortiClient determines the order by the TCP round trip time.
Host Tag	Select <i>Allow</i> or <i>Prohibit</i> , then select the desired Zero Trust tag from the <i>Select a Tag</i> dropdown list. Tags only display in the list if they are already configured. See Zero Trust Tags on page 246 .

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 Zero Trust tagging rule that tags all endpoints without up-to-date AV signatures. See [Adding a Zero Trust tagging rule set on page 246](#).
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 Zero Trust 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 SSL or IPsec VPN server in FortiOS. See the [FortiOS documentation](#).

This feature does not support explicitly including traffic in the VPN tunnel.



Currently FortiClient (macOS) and FortiClient (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	<p>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:</p> <ul style="list-style-type: none"> • Microsoft Office 365 • Microsoft Teams • Skype • GoToMeeting • Zoom • WebEx • YouTube <p>Once the VPN tunnel is up, FortiClient binds the specified excluded applications to the physical interface.</p>
Type	Select <i>Exclude</i> to configure whether to exclude certain application traffic from the VPN tunnel.
Local Applications	<p>You can only exclude local applications from the VPN tunnel. Click <i>Add</i>. In the <i>Add Application(s)</i> 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.</p> <p>For example, to exclude Microsoft Teams and Firefox from the VPN tunnel, you can enter any of the following combinations:</p> <ul style="list-style-type: none"> • 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

Configuration	Description
	<p>Files\Mozilla Firefox\</p> <p>To find a running application's full path, on the <i>Details</i> tab in Task Manager, add the <i>Image path name</i> column.</p> <p>Select the application checkbox, then click <i>Remove</i> to remove it from the list.</p>
Cloud Applications	<p>You can exclude cloud applications. Click <i>Add</i>. In the list, select the desired applications, then click <i>Add</i>.</p> <p>Select the application checkbox, then click <i>Remove</i> to remove it from the list.</p>
Domain	<p>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 <i>Add</i>. In the <i>Add Domain(s)</i> field, enter the desired domains, using ; to configure multiple entries.</p> <p>For example, if you configure the VPN tunnel to exclude youtube.com, youtube.com and *.youtube.com are excluded from the tunnel.</p> <p>Select the application checkbox, then click <i>Remove</i> to remove it from the list.</p>

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:

Editing VPN Tunnel - Add Application/Domain ✕

Add Application(s)

Application can be specified by its name, full path or the directory where it is installed. Environment variables (e.g. %programfiles%, %appdata%) can be used in file and directory path. Multiple entries can be separated by ; (e.g. chrome.exe;explore.exe)

For example:
 Application Name: chrome.exe
 Full Path: C:\Program Files\Internet Explorer\explore.exe
 Directory: C:\windows\ (must end with "\")

Add
Cancel

Editing 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

Creating VPN Tunnel

Changes to this VPN tunnel will not be saved until the profile is saved.

Basic Settings

Split Tunnel

Application Based

Advanced Settings

On Connect Script

On Disconnect Script

Application Based

Type

Include

Exclude

Local Applications

Name

☐ teams.exe

☐ %localappdata%\Microsoft\Teams\current\Teams.exe

☐ C:\Program Files\Mozilla Firefox\firefox.exe

☐ %localappdata%\Microsoft\Teams\current\

☐ C:\Program Files\Mozilla Firefox\

Remove

+ Add

Cloud Applications

Name

☒ Microsoft-Skype_Teams

☐ Cisco-Webex

☐ Cisco-Webex.FedRAMP

☐ Zoom.us-Zoom.Meeting

Remove

+ Add

Domain

Domain

No Content Found

Remove

+ Add

Add Tunnel

Cancel

- 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 Zero Trust tag


You can configure a profile to allow or block an endpoint from connecting to a VPN tunnel based on its applied Zero Trust tag. This feature is only available for Windows endpoints. 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 Zero Trust tagging rule set that tags endpoints with critical vulnerabilities with the "Vulnerable Devices" tag:
 - a. Go to *Zero Trust Tags > Zero Trust 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.

Zero Trust Tagging Rule Set

Name

Tag Endpoint As 

Enabled ☒

Comments

Rules + Add Rule	
Type	Value
Windows (1)	
Vulnerable Devices Severity Level	Critical

2. Configure the options on the endpoint profile:
 - a. Go to *Endpoint Profiles > Manage Profiles*.
 - b. Edit the desired profile, or create a new one.
 - c. On the *VPN* tab, enable *Enable Secure Remote Access*.
 - d. Select an existing VPN tunnel, or create a new one by clicking *Add Tunnel*.
 - e. In *Advanced Settings*, for *Host Tag*, select *Prohibit*.
 - f. From the *Select a Tag* dropdown list, select *Vulnerable Devices*.
 - 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.

Editing VPN Tunnel: New EMS Manual SSL

Changes to this VPN tunnel will not be saved until the profile is saved.

Basic Settings

Split Tunnel

Application Based

Advanced Settings

On Connect Script

On Disconnect Script

Advanced Settings

☒ Enable Single User Mode

☒ Save Username

☒ Allow Non-Administrators to Use Machine Certificates

☒ Enforce Acceptance of Disclaimer Message

SSL VPN Enforced disclaimer

☐ Enable SAML Login

Redundant Sort Method

Server Ping Speed TCP Round Trip Time

Host Tag

Allow Prohibit Vulnerable Devices

☒ Customize Host Check Fail Warning

Host tag checking failed for Vulnerable Devices

The following features need to also be configured on FortiGate to be enabled.

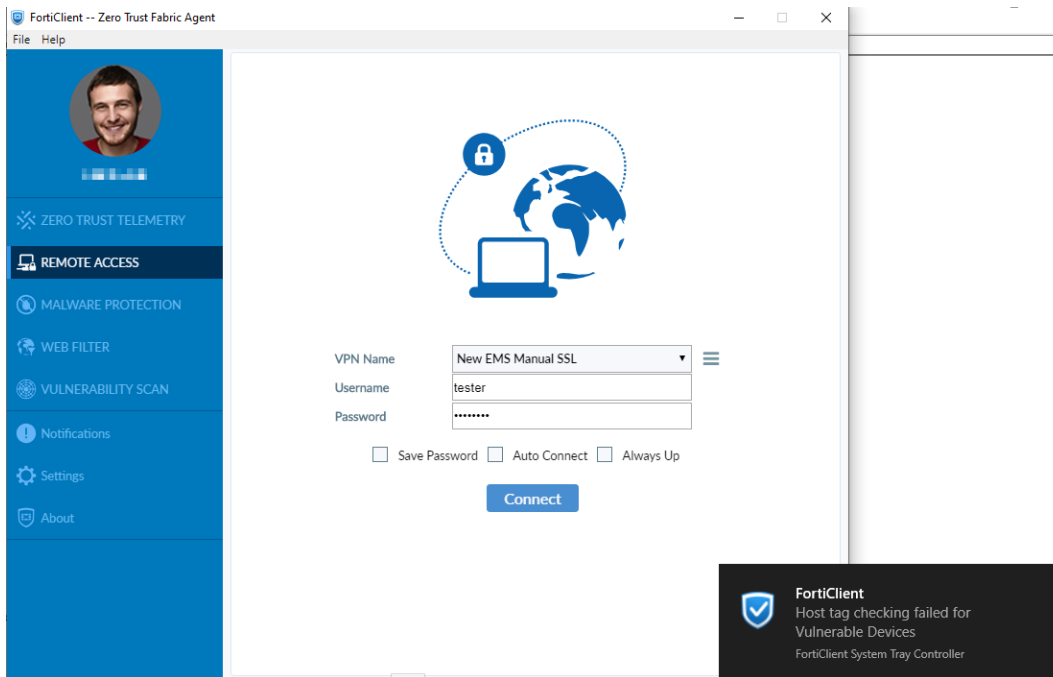
☒ Show "Remember Password" Option

☒ Show "Always Up" Option

☒ Show "Auto Connect" Option

Save Tunnel Cancel

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, FortiClient allows them to establish the VPN connection.



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 performing 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.

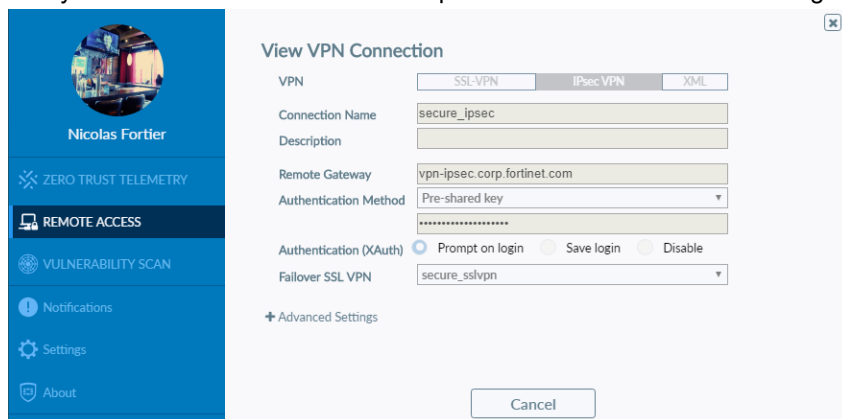
To configure a backup VPN connection:

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:

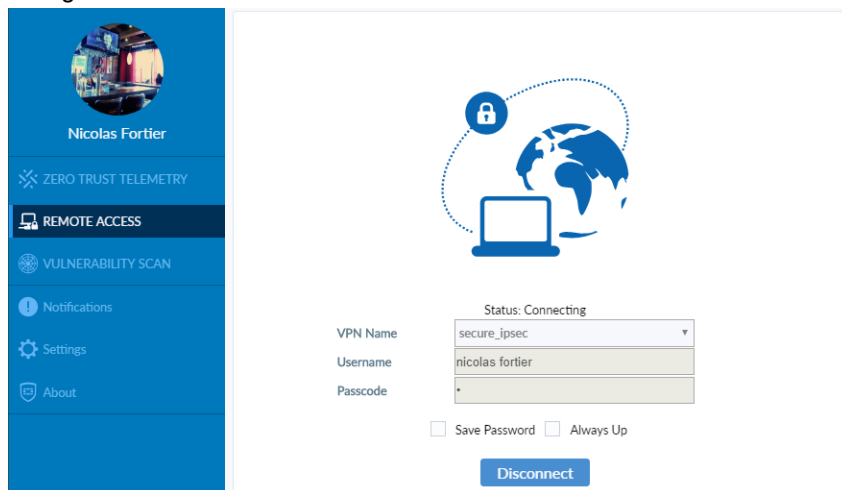

```
<forticlient_configuration>
  <vpn>
    <ipsecvpn>
      <connections>
        <connection>
          <ike_settings>
            <failover_sslvpn_connection>SSLVPN HQ</failover_sslvpn_connection>
          <ike_settings>
        <connection>
      <connections>
    </ipsecvpn>
  </vpn>
</forticlient_configuration>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

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.

FortiClient (Windows) and (macOS) 7.0.1 and EMS 7.0.1 support this feature. FortiClient (Linux) 7.0.1 does not support this feature.

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.

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.

Edit SAML Service Provider

SP name:

IdP prefix: [Generate prefix](#)

Server certificate:

IdP address:

IdP entity id: [🔗](#)

IdP single sign-on URL: [🔗](#)

IdP single logout URL: [🔗](#)

[Download IdP metadata](#) [Import SP metadata](#)

SP entity ID:

SP ACS (login) URL: [Alternative ACS URLs](#)

SP SLS (logout) URL:

☐ Support IdP-initiated assertion response

☐ Participate in single logout

☐ SAML request must be signed by SP

Authentication

Authentication method:

- ☐ Mandatory two-factor authentication
- ☒ Verify all configured authentication factors
- ☐ Password-only authentication
- ☐ Token-only authentication

☐ Bypass FortiToken authentication when user is from a trusted subnet [Configure subnets](#)

Assertion Attributes

Subject NameID:

Format:

☐ Include realm name in subject NameID

Debugging Options

SAML Attribute	User Attribute	Actions
username	Username	✎ ✖
group	FAC local group	✎ ✖

[Create New](#) [OK](#) [Cancel](#)

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

```

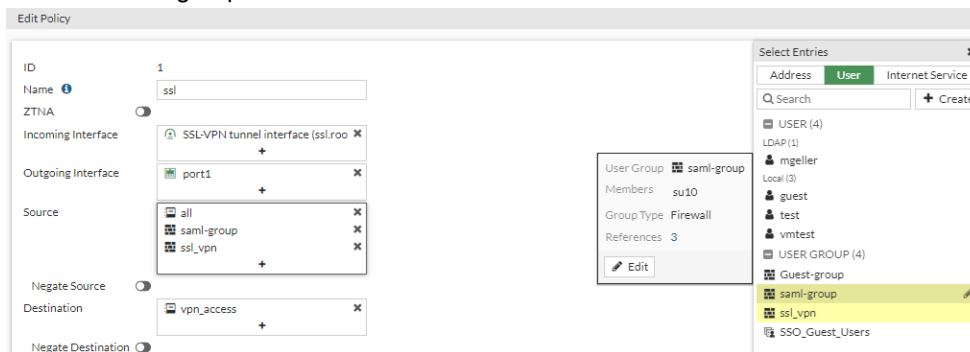
2. Ensure that the SAML redirect port is set to 8020. SAML external browser authentication uses port 8020 by default. If another service or application is occupying this port, FortiClient displays a message showing that the SAML redirect port is unavailable.:

```

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

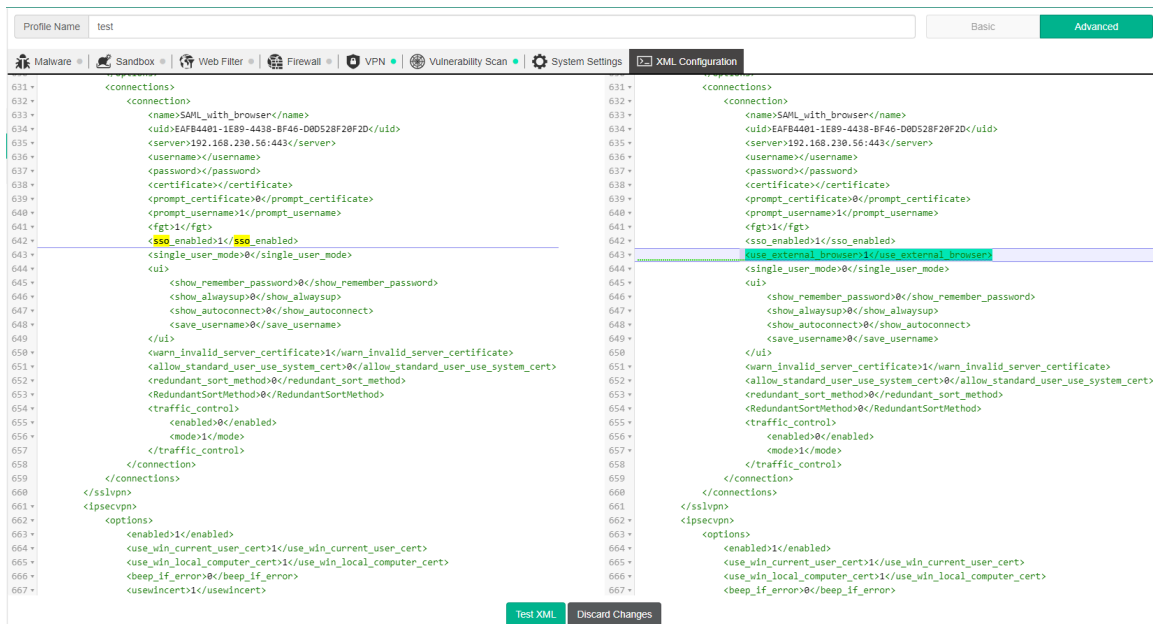
```

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:

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 prelogin 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
<code><show_vpn_before_logon></code>	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
<code><on_os_start_connect></code>	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 <code><machine></code> tag.	
<code><on_os_start_connect_has_priority></code>	When per-user and per-machine autoconnect configurations both exist, the following occurs: <ul style="list-style-type: none"> If this tag is set to 1, the per-machine autoconnect 	1

XML tag	Description	Default value
	configuration remains connected. <ul style="list-style-type: none"> If this tag is set to 0, after logging into Windows, the per-machine autoconnect configuration drops, and the per-user autoconnect configuration connects. 	
<machine>	Enabling this tag indicates that FortiClient should use this tunnel for per-machine autoconnect. This tag must be enabled for per-machine autoconnect to start to connect. Boolean: [1 0]	0
<username>	Enter the remote gateway authentication username if xAuth is enabled. If using public key infrastructure (PKI) authentication, do not configure this tag.	
<password>	Enter the password for the remote gateway authentication username if xAuth is enabled. If using PKI authentication, do not configure this tag.	
<keep_running>	When this tag is enabled and the network status changes from up to down to up again, the tunnel autoconnects when the network status is up again. This tag applies whether before or after logging in to Windows. Boolean: [1 0]	0

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

SSL VPN example

```

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

```

```

<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 <code><keep_running></code> disabled is configured.	<ul style="list-style-type: none"> 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 <code><keep_running></code> enabled is configured.	<ul style="list-style-type: none"> The per-user tunnel only connects after the user logs in to the device. The per-user tunnel does not disconnect. When the device disconnects from the network, the per-user tunnel disconnects. When the device reconnects to the network, the per-user tunnel reconnects. When the user manually disconnects the per-user tunnel, the tunnel does not automatically reconnect.
Only a per-machine autoconnect tunnel with <code><keep_running></code> disabled is configured.	<ul style="list-style-type: none"> 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.

Scenario	Behavior
Only a per-machine autoconnect tunnel with <code><keep_running></code> enabled is configured.	<ul style="list-style-type: none"> 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.
<p>The following tunnels are configured:</p> <ul style="list-style-type: none"> A per-machine autoconnect tunnel with <code><keep_running></code> disabled A per-user autoconnect tunnel with: <ul style="list-style-type: none"> <code><keep_running></code> disabled <code><show_remember_password></code> enabled <code><show_autoconnect></code> enabled 	<ul style="list-style-type: none"> 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.
<p>The following tunnels are configured:</p> <ul style="list-style-type: none"> A per-machine autoconnect tunnel with <code><keep_running></code> enabled A per-user autoconnect tunnel with <code><keep_running></code> enabled 	<ul style="list-style-type: none"> 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 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 Azure AD user

You can configure FortiClient to automatically connect to a specified VPN tunnel immediately after it installs and receives its configuration from EMS. In this example, FortiClient authenticates the connection using Azure Active Directory (AD) credentials. When the user logs in to Windows using their Azure AD credentials, FortiClient silently and automatically connects to the specified VPN tunnel, without the user needing to reenter their credentials or open the FortiClient console.

The following instructions assume that you have already configured your Azure AD 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.

To create and configure app registration in Azure:

1. In the Azure portal, go to *Azure Active Directory > Enterprise applications*.
2. Select the FortiGate SSL VPN enterprise application.
3. Note down the application ID and Azure domain.
4. Go to *Azure Active Directory > 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 FortiOS:

```
conf 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:

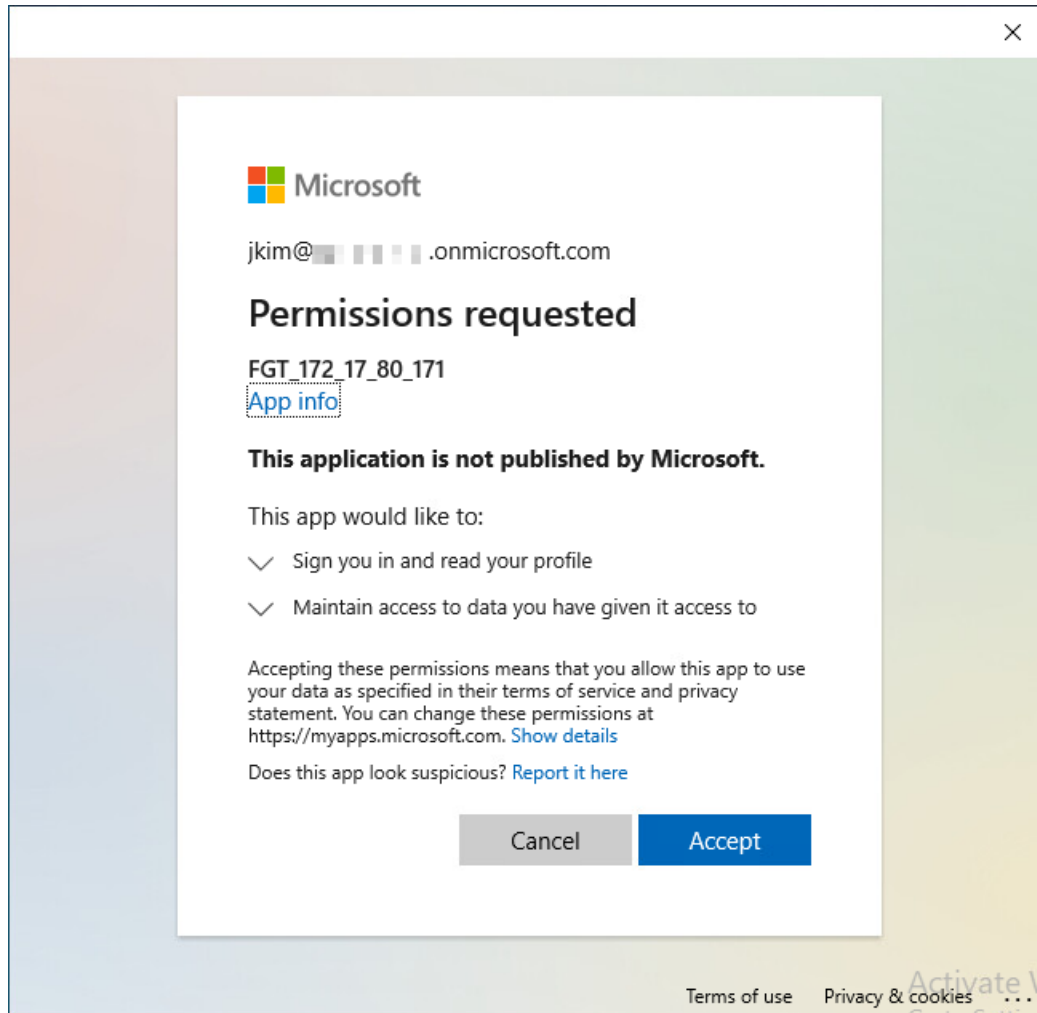
```
<vpn>
  <sslvpn>
    <connections>
      <connection>
        <name>SSL VPN HQ</name>
        <sso_enabled>1</sso_enabled>
        <azure_auto_login>
          <enabled>1</enabled>
          <azure_app>
            <tenant_name>Domain name obtained from the Azure portal</tenant_name>
            <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 grant permissions requests as an end user:

1. As an end user, log in to an endpoint that has the profile configured in [To configure EMS: on page 168](#) 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 Azure AD account. Select the desired account.
3. Windows displays a prompt for the end user to grant permissions to the Azure enterprise application configured for FortiGate SAML single sign on. Click *Accept*. This prompt does not display the next time that FortiClient attempts to connect to this VPN tunnel.



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 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 configure load balancing SSL VPN gateways with one FQDN:

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.

Editing VPN Tunnel: Test

Changes to this VPN tunnel will not be saved until the profile is saved.

Basic Settings

Split Tunnel

Application Based

Advanced Settings

On Connect Script

On Disconnect Script

Name

Test

Cannot contain the characters \ " & % < > .

Type

SSL VPN IPsec VPN

Remote Gateway

fortigatessl.fortinet.local

Port

444

☐ Require Certificate

☒ Prompt for Username

Save Cancel

- d. In *Advanced Settings*, enable *Enable SAML Login*, *FQDN Resolution Persistence*, and *Use External Browser as User-agent for SAML Login*.
- 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>
      <use_external_browser>1</use_external_browser>
      <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/>
    </connection>
  </connections>
</sslvpn>

```

```

        <server>fortigatessl.fortinet.local:444</server>
        <on_connect>
            <script>
                <os>windows</os>
            </script>
        </on_connect>
        <on_disconnect>
            <script>
                <os>windows</os>
            </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.

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 can configure these destinations in a ZTNA Destinations profile in EMS to deploy to endpoints as part of an endpoint policy. You can also configure FortiGate service portals for FortiClient to learn ZTNA destination rules from.

To configure a ZTNA destination:

1. Go to *Endpoint Profiles > ZTNA Destinations*.
2. Select a profile or create a new one.
3. Click *Advanced*.
4. In the *Name* field, enter the desired name.
5. If desired, enable *Allow Personal Destinations*. This feature allows end users to configure personal ZTNA destinations.
6. If desired, enable *Do Not Accept Invalid Server Certificate*. This feature blocks end users from accessing ZTNA destinations if they have an invalid server certificate.
7. If desired, enable *Notify user on error*. If enabled, FortiClient displays an error message to users when a TCP forwarding error occurs.
8. Enable *Destinations*.
9. Add a destination:
 - a. Click *Add*.
 - b. Add a proxy gateway:
 - i. In the *Enter gateway proxy address* field, enter the FortiGate access IP address and port in the format <IP address or FQDN>:<port>.
 - ii. Under *Select browser user-agent for SAML login*, select *Use external browser* or *Use FortiClient embedded browser*. FortiClient presents a SAML authentication request to the end user in a web browser or FortiClient embedded browser for traffic that is eligible for this rule.
 - iii. In the *Alias* field, enter an alias for this destination.

iv. Click *Next*.

Add New Gateway

1 Proxy Gateway 2 Private Applications 3 SaaS Applications

Enter gateway proxy address

172.17.80.207:8443

Select browser user-agent for SAML login

Use external browser Use FortiClient embedded browser

Alias

SaaS

Next

- c. Configure private applications. You can add a private application by searching for it, importing it from your device, or by manually adding it. Click *Next*.
- d. Configure SaaS applications by searching for the desired application in the *SaaS Applications/Groups* field. Selected applications appear as *Will be Added* under *Changes to Apps/Groups*.

Add New Gateway

1 Proxy Gateway 2 Private Applications 3 SaaS Applications

Select Apps/Groups

Search SaaS Applications/Groups

- ☐ MS
- ☒ Google
- ☐ salesforce
- ☐ egnyte
- ☐ webex
- ☐ zoom
- ☐ google-office
- ☐ ms-excel
- ☐ ms-onedrive
- ☐ ms-outlook
- ☐ ms-powerpoint
- ☐ ms-teams
- ☐ gmail

Back

Changes to Apps/Groups Revert Changes

Status	App/Group
+ Will be Added	Google
+ Will be Added	dropbox

Finish

e. Click *Finish*.

To configure a ZTNA portal in EMS:

1. Go to *Endpoint Profiles > ZTNA Destinations*.
2. Create a new profile or select the desired profile.
3. Enable *Portals*.
4. Click *Add*.
5. In the *Add New Portal* dialog, in the *Gateway* field, enter the gateway FortiGate IP address and port in <IP address>:<port> format.
6. Under *Select browser user-agent for SAML login*, select *Use external browser* or *Use FortiClient embedded browser*. FortiClient presents a SAML authentication request to the end user in a web browser or FortiClient embedded browser for traffic that is eligible for this rule.
7. In the *Interval (minutes)* field, enter the number of minutes after which FortiClient attempts syncing with the FortiGate ZTNA portal configuration.

The screenshot shows the 'Add New Portal' dialog box. The 'Alias' field contains 'SaaS'. The 'Gateway' field contains '172.17.80.207:8443'. Under 'Select browser user-agent for SAML login', the 'Use FortiClient embedded browser' option is selected. The 'Interval (minutes)' field contains '15'. The 'Save' button is highlighted in green.

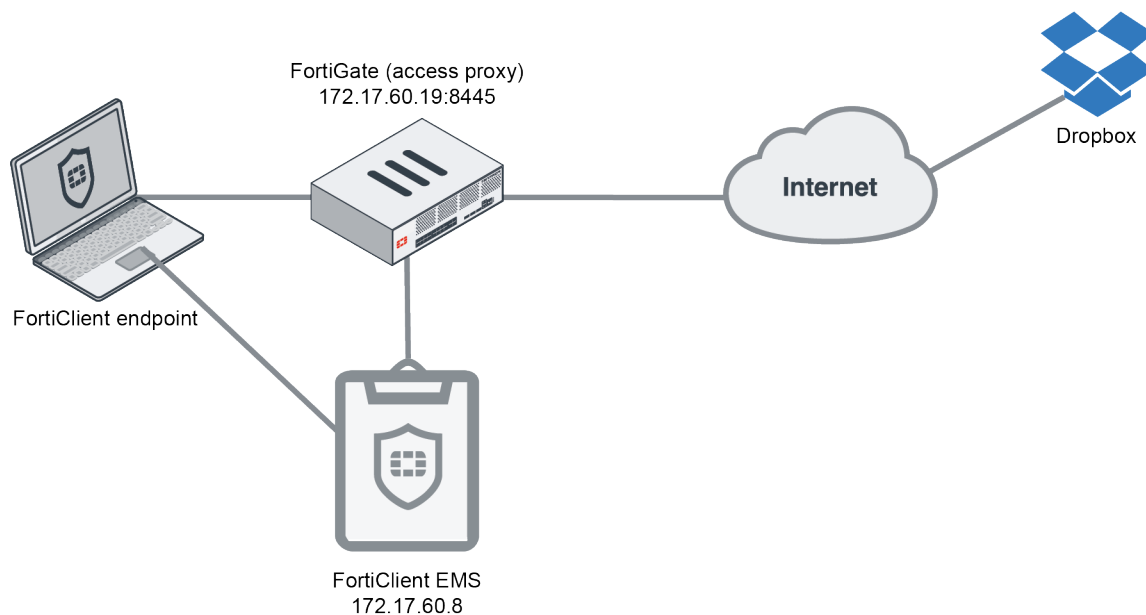
8. Click *Save*.

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 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 *Endpoint Profiles > ZTNA Destinations*.
2. Click *Add Destination*. Configure the following:
 - a. In the *Destination Host* field, enter *.dropbox.com:443.
 - b. In the *Proxy Gateway* field, enter the FortiGate IP address and port. In this example, the value is 172.17.60.19:8445.
 - c. Configure other fields as desired.
 - d. Click *Save*.
3. Click *XML*.

4. Confirm that the `<ztna><portals>` element is empty.

ZTNA Destinations Profile

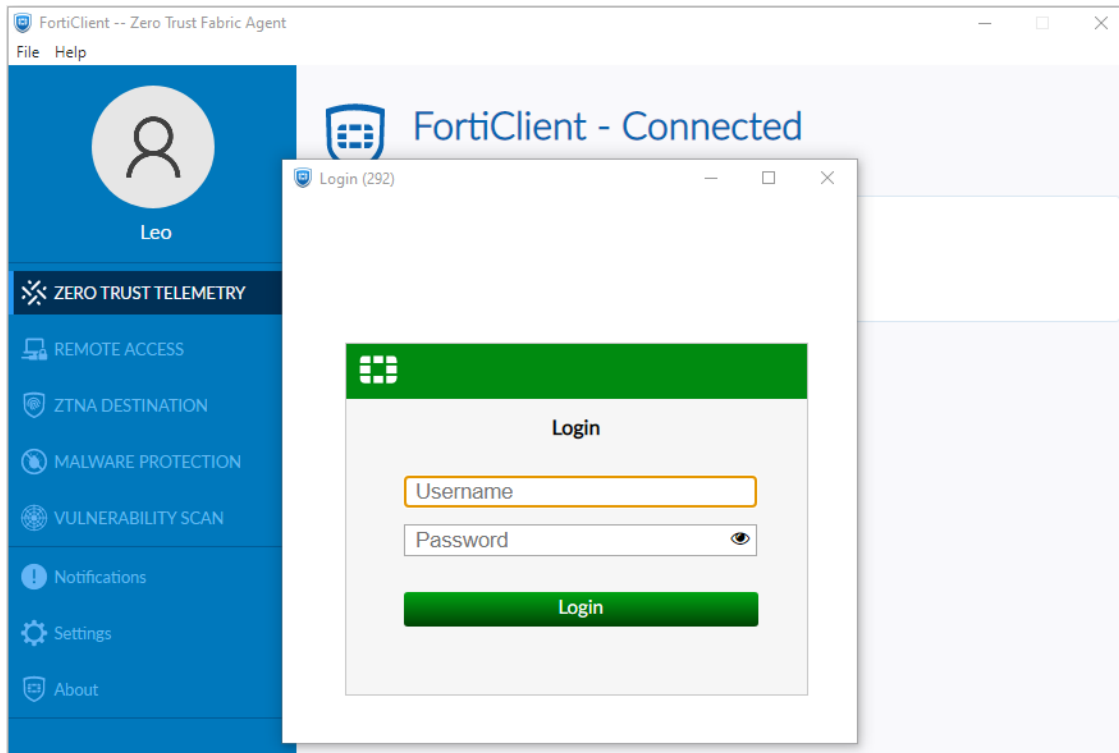
Name

```

36 <type>private</type>
37 </rule>
38 <rule uid="796EA176-24DD-4FB9-872D-51DACD49A2E0">
39   <name>Info fortinet com</name>
40   <destination>info.fortinet.com:443</destination>
41   <gateway>172.17.60.19:8445</gateway>
42   <mode>transparent</mode>
43   <local_port>7788</local_port>
44   <encryption>1</encryption>
45   <redirect>0</redirect>
46   <type>private</type>
47 </rule>
48 <rule uid="56475319-A2C1-4D71-A74D-97850C11C27B">
49   <name>RDP ztna local</name>
50   <destination>rdp.ztna.local:3389</destination>
51   <gateway>172.17.60.19:8445</gateway>
52   <mode>transparent</mode>
53   <local_port>7788</local_port>
54   <encryption>1</encryption>
55   <redirect>0</redirect>
56   <type>private</type>
57 </rule>
58 <rule uid="72912BC7-5772-4EE7-B113-7BB92EBD8772">
59   <name>ssh ztna local</name>
60   <destination>ssh.ztna.local:22</destination>
61   <gateway>172.17.60.19:8445</gateway>
62   <mode>transparent</mode>
63   <local_port>7788</local_port>
64   <encryption>1</encryption>
65   <redirect>0</redirect>
66   <type>private</type>
67 </rule>
68 </rules>
69 <portals/>
70 </ztna>

```

5. 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.



6. 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.

```

C:\Program Files\Fortinet\FortiClient\logs\trace\fortitcs_1.log - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

fortitcs_1.log
359 [2022-11-02 16:12:49.0515849] [fortitcs] Forward aem.dropbox.com: local: 127.0.0.1:52967 -> remote: 127.0.0.1:53053proxy: 172.17.60.10:53058 -> remote: 172.17.60.19:8445
360 [2022-11-02 16:12:49.0522014] [fortitcs] According to PID 8540 Get session ID: 1
361 [2022-11-02 16:12:49.0522091] [fortitcs] SAML address: https://172.17.60.19:8445/tcp?address=aem.dropbox.com&port=443&tls=1
362 [2022-11-02 16:12:49.0522119] [fortitcs] Cache address: https://172.17.60.19:8445/tcp
363 [2022-11-02 16:12:49.0522170] [fortitcs] Request :GET /tcp?address=aem.dropbox.com&port=443&tls=1 HTTP/1.1
364 Host: 172.17.60.19:8445
365 User-Agent: FortiClient
366 Accept: */*
367 Cookie: FTNT-EP-FGVM02TM22016704=5xLamvMVLVJFBUu-alcvmun78_nEtq-aK9_M-cS2r5qrT835xLavin9_MiW0rk2rarnrfXwvbExdqr9Lamv==
368 Authorization: Basic
369
370
371 [2022-11-02 16:12:49.0523389] [fortitcs] Send tunnel cmd Success
372 [2022-11-02 16:12:49.0523350] [fortitcs] html Reply:HTTP/1.1 101 Switching Protocols
373 Upgrade: tcp-forwarding/1.0
374 Connection: Upgrade
375
376
377 [2022-11-02 16:12:49.0523419] [fortitcs] Tunnel upgrade success
378 [2022-11-02 16:12:49.0523480] [fortitcs] Forward aem.dropbox.com: local: 127.0.0.1:52967 -> remote: 127.0.0.1:53057proxy: 172.17.60.10:53062 -> remote: 172.17.60.19:8445
379 [2022-11-02 16:12:49.0570564] [fortitcs] html Reply:HTTP/1.1 101 Switching Protocols
380 Upgrade: tcp-forwarding/1.0
381 Connection: Upgrade
382
383
384 [2022-11-02 16:12:49.0570648] [fortitcs] Tunnel upgrade success
385 [2022-11-02 16:12:49.0570713] [fortitcs] Forward aem.dropbox.com: local: 127.0.0.1:52967 -> remote: 127.0.0.1:53056proxy: 172.17.60.10:53061 -> remote: 172.17.60.19:8445
386 [2022-11-02 16:12:49.0586180] [fortitcs] html Reply:HTTP/1.1 101 Switching Protocols
387 Upgrade: tcp-forwarding/1.0
388 Connection: Upgrade
389
390
391 [2022-11-02 16:12:49.0586239] [fortitcs] Tunnel upgrade success
392 [2022-11-02 16:12:49.0586297] [fortitcs] Forward aem.dropbox.com: local: 127.0.0.1:52967 -> remote: 127.0.0.1:53059proxy: 172.17.60.10:53063 -> remote: 172.17.60.19:8445
393 [2022-11-02 16:12:49.0737342] [fortitcs error] CopyNetBuffer error: read tcp 172.17.60.10:53060->172.17.60.19:8445: use of closed network connection
394 [2022-11-02 16:12:49.1125669] [fortitcs error] CopyNetBuffer error: write tcp 127.0.0.1:52967->127.0.0.1:53057: use of closed network connection
395 [2022-11-02 16:12:49.1127759] [fortitcs error] CopyNetBuffer error: read tcp 172.17.60.10:53058->172.17.60.19:8445: use of closed network connection
396 [2022-11-02 16:12:49.1327599] [fortitcs error] CopyNetBuffer error: read tcp 172.17.60.10:53061->172.17.60.19:8445: use of closed network connection
397 [2022-11-02 16:12:49.1350388] [fortitcs error] CopyNetBuffer error: read tcp 172.17.60.10:53063->172.17.60.19:8445: use of closed network connection
398 [2022-11-02 16:12:49.4236328] [fortitcs] Accept success
399 [2022-11-02 16:12:49.4236472] [fortitcs] raw socket: 1028
400 [2022-11-02 16:12:49.4236679] [fortitcs] status: <nul> recordsSize: 860
401 [2022-11-02 16:12:49.4236709] [fortitcs] redirectContextSize: 260
402 [2022-11-02 16:12:49.4236775] [fortitcs] contextSize: 260
403 [2022-11-02 16:12:49.4236830] [fortitcs] family: 2 port: 443 ip: 10.235.0.7 pid: 8540
404 [2022-11-02 16:12:49.4237335] [fortitcs] forward ip: 10.235.0.7 port: 443
405 [2022-11-02 16:12:49.4237587] [fortitcs] UpdateDohRedirectEntry: Ip=183173127 Port=443 RealIp=1666590309 Fqdn=consent.dropbox.com Flag=0
406 [2022-11-02 16:12:49.4237948] [fortitcs] find wildcard, Fqdn: *.dropbox.com match: consent.dropbox.com
407 [2022-11-02 16:12:49.4237985] [fortitcs] UpdateFQDNIPandPort: get real_ip: 99.86.38.101 fqdn: consent.dropbox.com
408 [2022-11-02 16:12:49.4238014] [fortitcs] gateway ip: 172.17.60.19 port: 8445 encryption: 1
409 [2022-11-02 16:12:49.4236599] [fortitcs] According to PID 8540 Get session ID: 1
410 [2022-11-02 16:12:49.4236681] [fortitcs] SAML address: https://172.17.60.19:8445/tcp?address=consent.dropbox.com&port=443&tls=1
411 [2022-11-02 16:12:49.4236711] [fortitcs] Cache address: https://172.17.60.19:8445/tcp
412 [2022-11-02 16:12:49.4236781] [fortitcs] Request :GET /tcp?address=consent.dropbox.com&port=443&tls=1 HTTP/1.1

```

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.

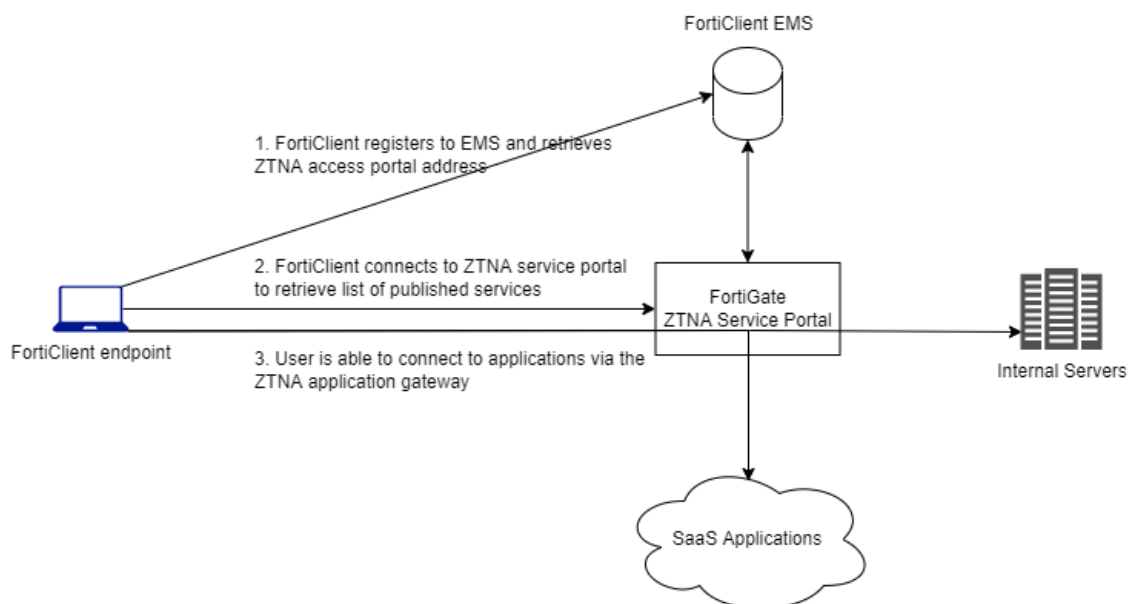
fortitcs_1_111.log				
3962	[2022-11-02 17:23:01.6680483]	[fortitcs]	gateway: 172.17.60.19:8445	
3963	[2022-11-02 17:23:01.6680502]	[fortitcs]	encryption: 1	
3964	[2022-11-02 17:23:01.6680520]	[fortitcs]	FQDN: *dl.dropboxusercontent.com	
3965	[2022-11-02 17:23:01.6680537]	[fortitcs]	FQDN_flag: 1	
3966	[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.

FortiGate ZTNA service portal support

In [FortiOS 7.2.1](#), the ZTNA service portal was added to allow the FortiGate to publish ZTNA services directly to FortiClients. This allows the FortiClient to retrieve the list of ZTNA services directly through the service portal without them being pushed from the FortiClient EMS.

The following demonstrates how EMS can provision a ZTNA service portal gateway list to FortiClient, which consists of the address to the FortiGate access portal(s). Once the FortiClient connects to the service portal gateway, it can retrieve the ZTNA service list containing a list of applications being published by the FortiGate.



To configure the ZTNA service portal in FortiOS:

```
config firewall vip
    edit "ztna_proxy"
        set type access-proxy
        set extip 192.168.3.101
        set extintf "port2"
        set server-type https
        set extport 4443
        set ssl-certificate "Fortinet_SSL"
    next
end
config firewall access-proxy
    edit "Ztna_SaaS"
        set vip "ztna_proxy"
        set log-blocked-traffic enable
        config api-gateway
            edit 1
```

```
        set url-map "/tcp"
        set service tcp-forwarding
        config realservers
            edit 1
                set address "smb_rdp_servers_range"
                set mappedport 445 3389-3390
            next
            edit 2
                set address "ssh server"
                set mappedport 22
            next
        end
    next
    edit 2
        set url-map "saas"
        set service saas
        set application "dropbox" "zoom" "Google"
    next
end
next
end
config firewall proxy-policy
    edit 2
        set uuid b680d4a6-4fdc-51ed-8fd7-c6f19c3b39c5
        set name "deny"
        set proxy access-proxy
        set access-proxy "Ztna_SaaS"
        set srcintf "port2"
        set srcaddr "all"
        set dstaddr "all"
        set ztna-ems-tag "EMS1_ZTNA_subnet1"
        set schedule "always"
        set logtraffic disable
    next
    edit 1
        set uuid 7aa5d142-45b0-51ed-1c02-b2c78813cd31
        set name "ZTNA_Rule_SaaS"
        set proxy access-proxy
        set access-proxy "Ztna_SaaS"
        set srcintf "port2"
        set srcaddr "all"
        set dstaddr "all"
        set ztna-ems-tag "EMS1_ZTNA_subnet2"
        set action accept
        set schedule "always"
        set logtraffic all
    next
end
```

The FortiGate ZTNA access portal is reachable on 192.168.3.101:4443, and it publishes a set of TCP forwarding services to SMB, RDP and SSH servers as well as SaaS applications in the Cloud. The ZTNA policies block endpoints with ZTNA tag belonging to subnet1, while allow endpoints with ZTNA tag belonging to subnet2 to access the services and applications.

To configure EMS to push the ZTNA access portal gateway to managed endpoints:

1. In EMS, go to *Endpoint Profiles > ZTNA Destinations*.
2. Select an existing profile and click *Edit* or add a new profile.
3. Switch the view from *Basic* to *XML*. Click *Edit* to edit the XML content.
4. Configure the ZTNA access portal gateway settings as follows. This example adds a second portal for demonstration purposes.

```
<?xml version="1.0" ?>
<forticlient_configuration>
  <ztna>
    <enabled>1</enabled>
    <allow_personal_rules>1</allow_personal_rules>
    <rules/>
    <portals>
      <portal>
        <addr>192.168.3.101:4443</addr>
        <query_interval_m>3</query_interval_m>
      </portal>
      <portal>
        <addr>172.17.80.3:8443</addr>
        <query_interval_m>3</query_interval_m>
      </portal>
    </portals>
  </ztna>
  <endpoint_control>
    <ui>
      <display_ztna>0</display_ztna>
    </ui>
  </endpoint_control>
</forticlient_configuration>
```

ZTNA Destinations Profile

▼ Expand All

▲ Collapse All

Name

ztna profile

Basic

Advanced

XML

```

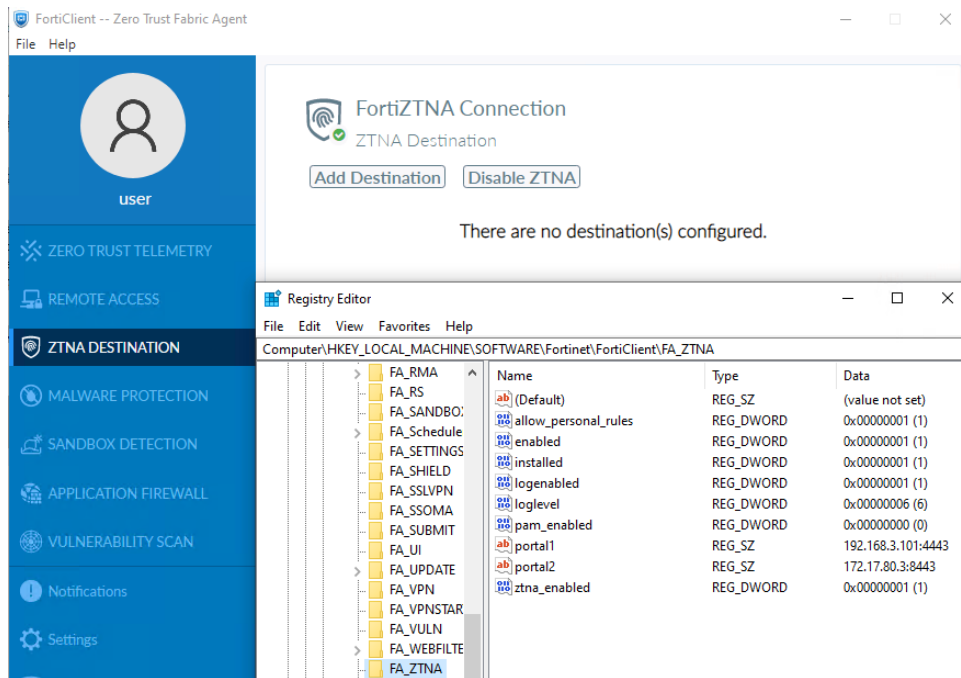
1 <?xml version="1.0" ?>
2 <forticlient_configuration>
3   <ztna>
4     <enabled>1</enabled>
5     <allow_personal_rules>1</allow_personal_rules>
6     <disallow_invalid_server_certificate>1</disallow_invalid_server_certificate>
7     <rules/>
8     <portals>
9       <portal>
10        <addr>192.168.3.101:4443</addr>
11        <query_interval_m>3</query_interval_m>
12      </portal>
13      <portal>
14        <addr>172.17.80.3:8443</addr>
15        <query_interval_m>3</query_interval_m>
16      </portal>
17    </portals>
18  </ztna>
19 </endpoint_control>
20   <ui>
21     <display_ztna>0</display_ztna>
22   </ui>
23 </endpoint_control>
24 </forticlient_configuration>

```

5. Save the profile. EMS automatically pushes the service portal addresses to managed FortiClient endpoints.

To verify FortiClient received the service portal and retrieved a list of ZTNA services:

1. On the PC, open FortiClient. On the *ZTNA Destination* tab, confirm that there is no destination added for the service portal or ZTNA services and applications.
2. Open the computer's registry, and go to Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Fortinet\FortiClient\FA_ZTNA. The ZTNA access portal addresses are added as portal1 and portal2. When multiple portals are configured, FortiClient selects the portal with lower latency to learn the ZTNA services.



3. Using FortiClient's Fortitcs logs, further verify that FortiClient retrieved the list of ZTNA services from the FortiGate service portal. This set of ZTNA rules are stored in memory and refreshes each time FortiClient queries the service portal:

```
"vips": [
  {
    "gateways": [
      {
        "path": "/tcp",
        "path-pattern": "sub-string",
        "servers": [
          {
            "address": {
              "type": "ip-range",
              "value": [
                {
                  "end": "172.16.1.10",
                  "start": "172.16.1.1"
                }
              ]
            },
            "mappedport": [
              {
                "end": "445",
                "start": "445"
              },
              {
                "end": "3390",
                "start": "3389"
              }
            ]
          }
        ]
      }
    ]
  }
]
```

```

        }
    ]
},
{
    "address": {
        "type": "ip",
        "value": [
            {
                "ip": "172.16.1.3",
                "mask": "255.255.255.255"
            }
        ]
    },
    "mappedport": [
        {
            "end": "22",
            "start": "22"
        }
    ]
}
],
"type": "tcp-fwd",
"virtual-host": ""
},
{
    "applications": [
        {
            "app": "dropbox"
        },
        {
            "app": "zoom"
        },
        {
            "grp": "Google"
        }
    ],
    "path": "saas",
    "path-pattern": "sub-string",
    "type": "saas",
    "virtual-host": ""
}
],
"vip": "192.168.3.101:4443"
}
]
}

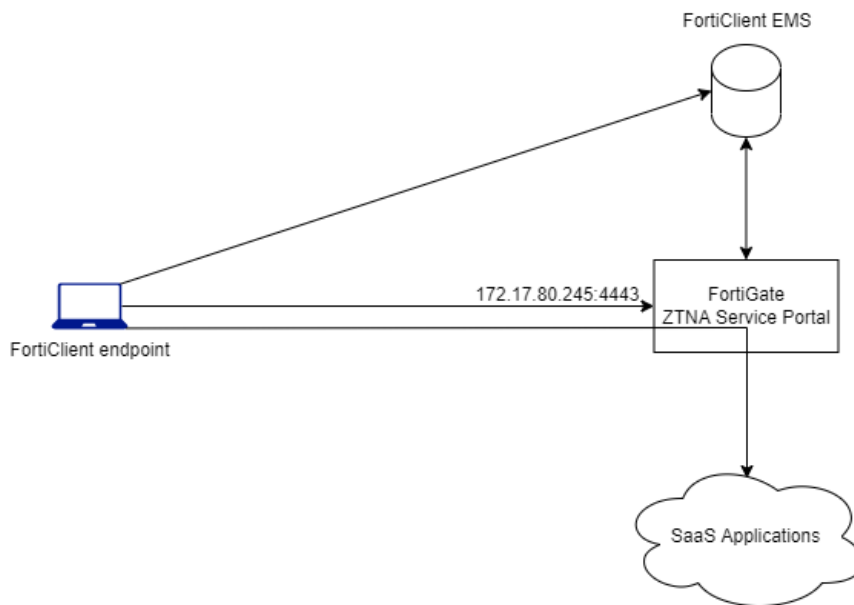
```

Users can now access the ZTNA destination services and applications.

Inline CASB solution for SaaS applications

When protecting SaaS applications, one difficulty is to dynamically identify the addresses and locations of various SaaS services. With the FortiGuard Inline CASB Database (ICDB) introduced in [FortiOS 7.2.1](#), both FortiGate and FortiClient can access this database to determine popular SaaS application addresses.

In this example, FortiGate publishes the SaaS applications Dropbox, Zoom and the Microsoft application group to its ZTNA service portal. EMS pushes the address of the FortiGate service portal to FortiClient. FortiClient then learns the SaaS applications that are published and builds local ZTNA rules for the SaaS application addresses in memory. When an end user tries to access Dropbox while FortiClient is registered to EMS, the traffic is forwarded to the FortiGate ZTNA application gateway where a ZTNA policy allows the access. When an end user is not registered or does not have the proper ZTNA tag required by FortiGate's ZTNA policy, the traffic is blocked.



To configure the ZTNA service portal in FortiOS:

```

config firewall vip
  edit "ztna_proxy"
    set type access-proxy
    set extip 172.17.80.245
    set extintf "port1"
    set server-type https
    set extport 4443
    set ssl-certificate "Fortinet_SSL"
  next
end
config firewall access-proxy
  edit "Ztna_SaaS"
    set vip "ztna_proxy"
    set auth-portal enable
    set log-blocked-traffic enable
    config api-gateway
      edit 1
        set url-map "saas"
        set service saas
    end
  end
end
  
```

```
        set application "dropbox" "zoom" "MS"
    next
end
config firewall proxy-policy
edit 3
    set name "ZTNA Saas"
    set proxy access-proxy
    set access-proxy "Ztna_SaaS"
    set srcintf "port1"
    set srcaddr "all"
    set dstaddr "all"
    set ztna-ems-tag "EMS1_ZTNA_ZTNA SAAS"
    set action accept
    set schedule "always"
next
end
```

To configure EMS to push ZTNA access portal gateway settings to managed endpoints:

1. In EMS, go to *Endpoint Profiles* > *ZTNA Destinations*.
2. Select an existing profile and click *Edit* or add a new profile.
3. Switch the view from *Basic* to *XML*. Click *Edit* to edit the XML content.
4. Configure the ZTNA access portal gateway settings as follows. This example adds a second portal for demonstration purposes.

```
<?xml version="1.0" ?>
<forticlient_configuration>
    <ztna>
        <enabled>1</enabled>
        <allow_personal_rules>1</allow_personal_rules>
        <rules/>
        <portals>
            <portal>
                <addr>172.17.80.245:4443</addr>
                <query_interval_m>5</query_interval_m>
            </portal>
        </portals>
    </ztna>
    <endpoint_control>
        <ui>
            <display_ztna>0</display_ztna>
        </ui>
    </endpoint_control>
</forticlient_configuration>
```

ZTNA Destinations Profile

Expand All
Collapse All

Name

Basic
Advanced
XML

```

1 <?xml version="1.0" ?>
2 <forticlient_configuration>
3   <ztna>
4     <enabled>1</enabled>
5     <allow_personal_rules>1</allow_personal_rules>
6     <disallow_invalid_server_certificate>0</disallow_invalid_server_certificate>
7     <rules/>
8     <portals>
9       <portal>
10        <addr>172.17.80.245:4443</addr>
11        <query_interval_m>5</query_interval_m>
12      </portal>
13    </portals>
14  </ztna>
15  <endpoint_control>
16    <ui>
17      <display_ztna>1</display_ztna>
18    </ui>
19  </endpoint_control>
20 </forticlient_configuration>

```

5. Save the profile. EMS automatically pushes the service portal addresses to managed FortiClient endpoints.

To verify a registered FortiClient endpoint can access Dropbox:

1. On a remote PC that has FortiClient installed, ensure that it is registered to FortiClient EMS. Also ensure that it has the ZTNA tag needed for access, in this case the ZTNA SaaS tag.
2. Use the steps in [To verify FortiClient received the service portal and retrieved a list of ZTNA services: on page 185](#) to verify the service portal address is added to registry and FortiClient learned the SaaS application services from the FortiGate.
3. In a browser, go to dropbox.com. Access is granted.
4. From the FortiClient ZTNA log (/Application Support/Fortinet/FortiClient/Logs/ztna.log), note the connections to the FortiGate application gateway address of 172.17.80.245:4443.

```

testqa - tail -f ~/Library/Application Support/Fortinet/FortiClient/Logs/ztna.log -- 225x49
~ - tail -f ~/Library/Application Support/Fortinet/FortiClient/Logs/ztna.log

C:\Windows
~ - tail -f ~/Library/Application Support/Fortinet/FortiClient/Logs/ztna.log
Fortinet/FortiClient/Logs/ztna.log
Last login: Fri Dec 2 09:44:47 on console
Restored session: Fri 2 Dec 2022 09:44:00 PST
testqa@ ~ % tail -f ~/Library/Application Support/Fortinet/FortiClient/Logs/ztnafw.log
tail: /Users/testqa/Library/Application Support/Fortinet/FortiClient/Logs/ztnafw.log: No such file or directory
testqa@ ~ % tail -f ~/Library/Application Support/Fortinet/FortiClient/Logs/ztna.log
2022-12-02T18:22:43.109Z info ztna exit #Tunnel -> conn &({0x14000486008 0x14000587ec0})->&({0x14000663380}) err:<nil>
2022-12-02T18:22:43.109Z info ztna conn -> Tunnel &({0x14000663380})->&({0x14000486008 0x14000587ec0}) err:<nil>
2022-12-02T18:22:43.109Z info ztna tunnel closed &({0x14000486008 0x14000587ec0},err:<nil>)
2022-12-02T18:22:52.146Z info ztna modified file:/tmp/4DFD10201FBF4C8C8AB391FCC701F420
2022-12-02T18:22:55.196Z info ztna mergeCfg:&{1 [] [(172.17.80.245:4443)]}
2022-12-02T18:22:55.196Z info ztna config is the same after merged preConfig&{1 [] [(172.17.80.245:4443)]}
2022-12-02T18:22:55.229Z info ztna modified file:/tmp/4DFD10201FBF4C8C8AB391FCC701F420
2022-12-02T18:22:58.284Z info ztna mergeCfg:&{1 [] [(172.17.80.245:4443)]}
2022-12-02T18:22:58.284Z info ztna config is the same after merged preConfig&{1 [] [(172.17.80.245:4443)]}
2022-12-02T18:23:03.956Z info ztna conn -> Tunnel &({0x140000b0900})->&({0x14000130a30 0x14000262a80}) err:<nil>
2022-12-02T18:23:08.945Z info ztna exit #Tunnel -> conn &({0x14000130a30 0x14000262a80})->&({0x140000b0900}) err:<nil>
2022-12-02T18:23:08.945Z info ztna tunnel closed &({0x14000130a30 0x14000262a80},err:<nil>)
2022-12-02T18:23:14.992Z info ztna conn -> Tunnel &({0x14000290780})->&({0x14000130a30 0x14000270060}) err:<nil>
2022-12-02T18:23:19.387Z info ztna conn -> Tunnel &({0x14000290780})->&({0x14000130a30 0x14000270060}) err:<nil>
2022-12-02T18:23:19.387Z info ztna tunnel closed &({0x14000130a30 0x14000270060},err:<nil>)
2022-12-02T18:23:19.387Z info ztna tunnel closed &({0x14000130a30 0x14000262540},err:<nil>)
2022-12-02T18:23:19.387Z info ztna conn(127.0.0.1:49162)->Tunnel(o:8({0x14000212520 0x14000095f20})-> conn(127.0.0.1:49162)
2022-12-02T18:23:21.147Z info ztna Dail fgtgateway url:https://172.17.80.245:4443/saas?address=dropbox.com&port=443&tls=0
2022-12-02T18:23:21.232Z info ztna redirect 127.0.0.1:49162 -> 198.18.3.98:443
2022-12-02T18:23:21.232Z info ztna Dail fgtgateway url:https://172.17.80.245:4443/saas?address=marketing.dropbox.com&port=443&tls=0
2022-12-02T18:23:21.232Z info ztna resp.StatusCode=101
2022-12-02T18:23:21.232Z info ztna 101,fgtgateway(https://172.17.80.245:4443/saas?address=dropbox.com&port=443&tls=0) connected ,redirect to auth
2022-12-02T18:23:21.232Z info ztna fgtTunnel((0)172.17.80.245:4443/saas,o:8({0x14000212520 0x14000095f20})-> conn(127.0.0.1:49162)
2022-12-02T18:23:21.232Z info ztna conn(127.0.0.1:49162)->Tunnel(o:8({0x14000212520 0x14000095f20})-> conn(127.0.0.1:49162)
2022-12-02T18:23:21.339Z info ztna redirect 127.0.0.1:49162 -> 198.18.3.92:443
2022-12-02T18:23:21.339Z info ztna Dail fgtgateway url:https://172.17.80.245:4443/saas?address=www.google.com&port=443&tls=0
2022-12-02T18:23:26.413Z info ztna resp.StatusCode=101
2022-12-02T18:23:26.413Z info ztna 101,fgtgateway(https://172.17.80.245:4443/saas?address=www.google.com&port=443&tls=0) connected ,redirect to auth
2022-12-02T18:23:26.413Z info ztna fgtTunnel((0)172.17.80.245:4443/saas,o:8({0x14000212520 0x14000095f20})-> conn(127.0.0.1:49162)
2022-12-02T18:23:26.413Z info ztna conn(127.0.0.1:49162)->Tunnel(o:8({0x14000212520 0x14000095f20})-> conn(127.0.0.1:49162)
2022-12-02T18:23:26.413Z info ztna modified file:/tmp/4DFD10201FBF4C8C8AB391FCC701F420
2022-12-02T18:23:26.413Z info ztna redirect 127.0.0.1:49162 -> 198.18.3.40:443
2022-12-02T18:23:26.413Z info ztna Dail fgtgateway url:https://172.17.80.245:4443/saas?address=l.evidon.com&port=443&tls=0
2022-12-02T18:23:26.413Z info ztna redirect 127.0.0.1:49162 -> 198.18.3.40:443
2022-12-02T18:23:26.413Z info ztna Dail fgtgateway url:https://172.17.80.245:4443/saas?address=l.evidon.com&port=443&tls=0
2022-12-02T18:23:26.413Z info ztna mergeCfg:&{1 [] [(172.17.80.245:4443)]}
2022-12-02T18:23:26.413Z info ztna config is the same after merged preConfig&{1 [] [(172.17.80.245:4443)]}
2022-12-02T18:23:26.413Z info ztna modified file:/tmp/4DFD10201FBF4C8C8AB391FCC701F420

```

5. From the FortiGate, view the access logs from **Log & Report > ZTNA Traffic**.

<

6. Alternatively, use the following commands to display ZTNA logs:

```

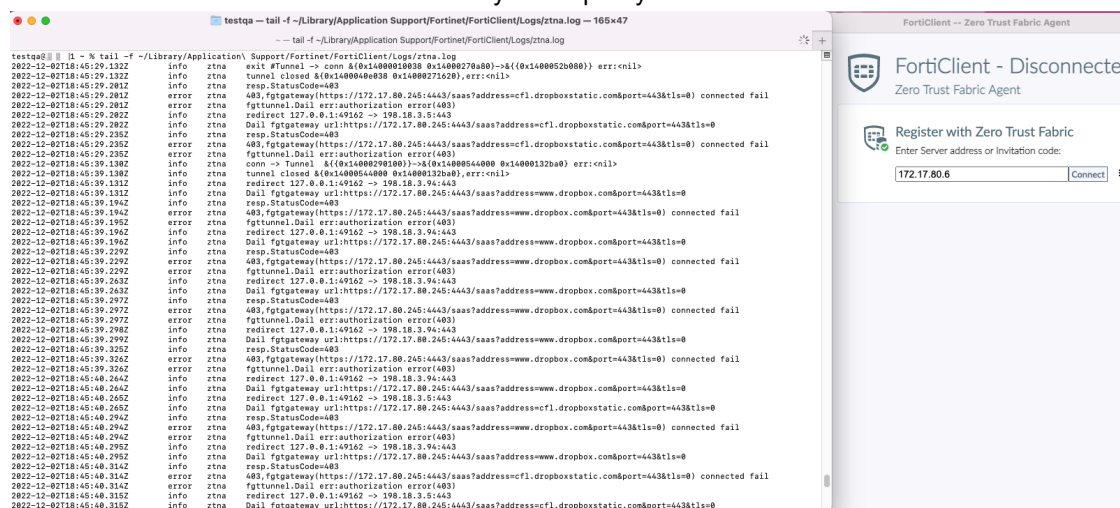
Fortigate# exec log filter category 0
Fortigate# exec log filter field subtype ztna
Fortigate# exec log display
1: date=2022-12-02 time=11:53:21 eventtime=1670010801641703801 tz="-0800"
logid="0005000024" type="traffic" subtype="ztna" level="notice" vd="root"

```

```
srcip=172.17.80.70 srcport=50677 srcintf="port1" srcintfrole="lan"
dstcountry="Canada" srccountry="Reserved" dstip=23.11.240.246 dstport=443
dstintf="port1" dstintfrole="lan" sessionid=210454 service="HTTPS" proto=6
action="accept" policyid=3 policytype="proxy-policy" poluuid="5c072b96-70da-51ed-
d2d9-2c1aaf2417bc" policyname="ZTNA SaaS" duration=125 gatewayid=1 vip="ztna_proxy"
accessproxy="Ztna_SaaS" clientdeviceid="4553FF07359B5B6AADD4DD75421E9C5A"
saasname="dropbox" clientdevicetags="on-line/MAC_EMS1_CLASS_Low/EMS1_CLASS_Low/MAC_
EMS1_ZTNA_all_registered_clients/EMS1_ZTNA_all_registered_clients" wanin=425
rcvdbyte=425 wanout=1209 lanin=3980 sentbyte=3980 lanout=2607
fctuid="4553FF07359B5B6AADD4DD75421E9C5A" appcat="unsccanned"
```

To verify an unregistered FortiClient endpoint cannot access Dropbox:

1. On the same PC, open FortiClient. On the *Zero Trust Telemetry* tab, disconnect from EMS.
2. In a new browser window, go to dropbox.com. The browser cannot load the page.
3. From the FortiClient ZTNA log (/Application Support/Fortinet/FortiClient/Logs/ztna.log), notice that connection fails when FortiClient tries to connect to the FortiGate application gateway. FortiGate automatically closes the connection when the traffic fails to match any ZTNA policy.



4. From the FortiGate, view the access logs from *Log & Report > ZTNA Traffic*.

Dashboard	Source 172.17.80.70, Result == deny	Memory	Details
Network			
Policy & Objects			
Security Profiles			
VPN			
User & Authentication			
WiFi Controller			
System			
Security Fabric			
Log & Report			
Forward Traffic			
Local Traffic			
Multicast Traffic			
Sniffer Traffic			
ZTNA Traffic			
System Events			
Security Events			
Log Settings			
Threat Weight			

Date/Time	Source	ZTNA Server	Destination	Service	Result	Policy ID	Group	SaaS name
2022/12/02 11:35:41	172.17.80.70	Ztna_SaaS	172.17.80.245	tcp/4443	Deny	Implicit Deny		dropbox
2022/12/02 11:35:41	172.17.80.70	Ztna_SaaS	172.17.80.245	tcp/4443	Deny	Implicit Deny		zoom
2022/12/02 11:35:41	172.17.80.70	Ztna_SaaS	172.17.80.245	tcp/4443	Deny	Implicit Deny		zoom
2022/12/02 11:35:41	172.17.80.70	Ztna_SaaS	172.17.80.245	tcp/4443	Deny	Implicit Deny		zoom
2022/12/02 11:35:41	172.17.80.70	Ztna_SaaS	172.17.80.245	tcp/4443	Deny	Implicit Deny		zoom
2022/12/02 11:35:41	172.17.80.70	Ztna_SaaS	172.17.80.245	tcp/4443	Deny	Implicit Deny		dropbox
2022/12/02 11:35:41	172.17.80.70	Ztna_SaaS	172.17.80.245	tcp/4443	Deny	Implicit Deny		dropbox
2022/12/02 11:35:41	172.17.80.70	Ztna_SaaS	172.17.80.245	tcp/4443	Deny	Implicit Deny		dropbox
2022/12/02 11:35:41	172.17.80.70	Ztna_SaaS	172.17.80.245	tcp/4443	Deny	Implicit Deny		dropbox
2022/12/02 11:35:41	172.17.80.70	Ztna_SaaS	172.17.80.245	tcp/4443	Deny	Implicit Deny		dropbox
2022/12/02 11:35:41	172.17.80.70	Ztna_SaaS	172.17.80.245	tcp/4443	Deny	Implicit Deny		dropbox
2022/12/02 11:35:41	172.17.80.70	Ztna_SaaS	172.17.80.245	tcp/4443	Deny	Implicit Deny		zoom
2022/12/02 11:35:41	172.17.80.70	Ztna_SaaS	172.17.80.245	tcp/4443	Deny	Implicit Deny		dropbox
2022/12/02 11:35:41	172.17.80.70	Ztna_SaaS	172.17.80.245	tcp/4443	Deny	Implicit Deny		dropbox
2022/12/02 11:35:41	172.17.80.70	Ztna_SaaS	172.17.80.245	tcp/4443	Deny	Implicit Deny		zoom
2022/12/02 11:35:41	172.17.80.70	Ztna_SaaS	172.17.80.245	tcp/4443	Deny	Implicit Deny		zoom
2022/12/02 11:34:45	172.17.80.70	Ztna_SaaS	172.17.80.245	tcp/4443	Deny	Implicit Deny		zoom

5. Alternatively, use the following commands to display ZTNA logs:

```
Fortigate# exec log filter category 0
Fortigate# exec log filter field subtype ztna
Fortigate# exec log display
1. date=2022-12-02 time=12:11:04 eventtime=1670011864162361201 tz="-0800"
logid="0005000024" type="traffic" subtype="ztna" level="notice" vd="root"
srcip=172.17.80.70 srcport=51283 srcintf="port1" srcintfrole="lan"
dstcountry="Reserved" srccountry="Reserved" dstip=172.17.80.245 dstport=4443
dstintf="root" dstintfrole="undefined" sessionid=4119 service="tcp/4443" proto=6
action="deny" policyid=0 policytype="proxy-policy" duration=0 vip="ztna_proxy"
accessproxy="Ztna_SaaS" clientdeviceid="4553FF07359B5B6AADD4DD75421E9C5A"
saasname="dropbox" clientdevicetags="offline/MAC_EMS1_CLASS_Low/EMS1_CLASS_Low"
msg="Denied: failed to match a proxy-policy" wanin=0 rcvdbyte=0 wanout=0 lanin=2761
sentbyte=2761 lanout=2050 fctuid="4553FF07359B5B6AADD4DD75421E9C5A"
appcat="unscanned" crscore=30 craction=131072 crlevel="high"
```

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.



FortiClient can block webpages outside of web filtering. This includes:

- Application Firewall: If the webpage matches a given signature where the action is set to block or if *Block Access to Malicious Websites* is enabled. See [Firewall on page 222](#).

Webpage blocks generate an entry in the local FortiClient logs. If a website block cause is unclear, review the logs.

If *Block Access to Malicious Websites* is enabled on the Application Firewall profile and another action is configured for malicious websites on the Web Filter profile, *Block Access to Malicious Websites* takes precedence and FortiClient blocks access to malicious websites.

Configuration	Description
Web Filter	<p>Enable web filtering.</p> <p>Enable or disable the eye icon to show or hide this feature from the end user in FortiClient.</p>
General	
Enable WebFiltering on FortiClient	<p>Select <i>Always On</i> to enable client web filtering when on-fabric.</p> <p>Select <i>Only When Endpoint is Off-Fabric</i> to enable Web Filter on endpoints only when the endpoint is considered off-Fabric. See On-fabric Detection Rules on page 135.</p> <p>This setting affects the <i>Block Access to Malicious Websites</i> setting in Malware Protection on page 210.</p>
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	<ul style="list-style-type: none"> • 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. After 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.
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, the plugin checks all URL requests.

Configuration	Description
Enable Safe Search	<p>For Windows endpoints and Chromebooks, when enabling Safe Search, you can configure the Restriction Level to Strict or Moderate. This setting affects the content that endpoint users can access via YouTube and search engine, including Google and Bing. For Chromebooks, to set YouTube access to Unrestricted, you can disable Safe Search and configure Google Search and YouTube access with the Google Admin Console instead of FortiClient EMS. For macOS endpoints, enabling Safe Search sets the endpoint's Google search to Restricted mode and YouTube access to Strict Restricted access.</p> <p>Enabling Safe Search adds records, including Yandex.ru, to the client device's hosts file in order to redirect search engine requests.</p> <p>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.</p>
Site Categories	<p>Enable site categories from FortiGuard. When you disable site categories, the exclusion list protects FortiClient.</p> <p>See the FortiGuard website for descriptions of the available categories and subcategories.</p> <p>For all categories, you can configure an action for the entire site category by selecting one of the following:</p> <ul style="list-style-type: none"> • Block • Warn • Allow • Monitor <p>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.</p>
Adult/Mature Content	<ul style="list-style-type: none"> • 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)

Configuration	Description
Bandwidth Consuming	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Dynamic DNS • Malicious Websites • Newly Observed Domain • Newly Registered Domain • Phishing • Spam URLs
Unrated	<p>Sites that FortiGuard categorizes as unrated.</p> <p>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 <i>Unrated</i> category for cloud applications, and click <i>Add</i> to configure an action for selected cloud applications using ISDB. In the <i>Add Cloud Application</i> dialog, select the desired cloud application, configure the desired action, then click <i>Add</i>.</p>
Rate IP Addresses	<p>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.</p> <p>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 action is determined by the classification based on the domain name and other times it is determined by the classification that is based on the IP address.</p> <p>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.</p>

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: <ul style="list-style-type: none"> 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 <i>FortiGuard Anycast</i> is selected for the <i>Server</i> field, you can select from global, U.S., or Europe. If <i>FortiGuard</i> is selected for the <i>Server</i> field, you can select from global or U.S. When <i>Global</i> 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: <ul style="list-style-type: none"> FortiGuard: <ul style="list-style-type: none"> Global: fgd1.fortigate.com U.S.: usfgd1.fortigate.com FortiGuard Anycast: <ul style="list-style-type: none"> Global: fctguard.fortinet.net U.S.: fctusguard.fortinet.net Europe: fcteuguard.fortinet.net
Server	Configure the FortiGuard server to <i>FortiGuard</i> or <i>FortiGuard Anycast</i> .
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: <ul style="list-style-type: none"> Violence/Terrorism Extremist

Configuration	Description
	<ul style="list-style-type: none"> • Pornography • Cyber Bullying • Self Harm
Custom Banned Words	<p>Configure actions for individual terms. Enable <i>Custom Banned Words</i>, type the desired term in the <i>Add Word</i> field, then click <i>Add Word</i>. Configure the action for the term (<i>Block</i>, <i>Monitor</i>, or <i>Allow</i>), then toggle the <i>Status</i> to <i>On</i>.</p> <p>You can remove a term from the <i>Custom Banned Word</i> list by selecting the checkbox beside the term, then clicking the <i>Remove Word</i> button.</p> <p>The custom term may belong to a category under <i>Banned Word Search</i>. If the action configured for the category under <i>Banned Word Search</i> and the action configured for the term under <i>Custom Banned Words</i> differ, EMS applies the action configured under <i>Custom Banned Words</i>.</p>
Exclusion List	Adding more than 1000 exclusions is not recommended and can cause EMS instability.
Action	<p>Select one of the following actions:</p> <ul style="list-style-type: none"> • Allow • Block • Monitor
URL	Enter specific URLs to allow, block, or monitor. You can provide the full URL or only the domain name.
Referrer/Host	<p>Enter a specific referrer or host to allow, block, or monitor. You can provide the full URL or only the domain name.</p> <p>If the end user visits the URL through the referrer provided, EMS considers the rule a match and applies the specified action.</p> <p>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.</p>
Type	<p>Select one of the following types:</p> <ul style="list-style-type: none"> • Simple • Wildcard • Regular Expression <p>You can use wildcard characters and Perl Compatible Regular Expressions (PCRE).</p> <p>This field only applies to the value in the <i>URL</i> field and does not apply to the value in the <i>Referrer/Host</i> field.</p>
Move this rule up/Move this rule down	Move the exclusion rule up/down in the list. If multiple exclusion rules are applicable, EMS applies the first applicable exclusion rule.

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 346](#).

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-write*.
 - 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: <code><ip address>:<port></code> .
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.

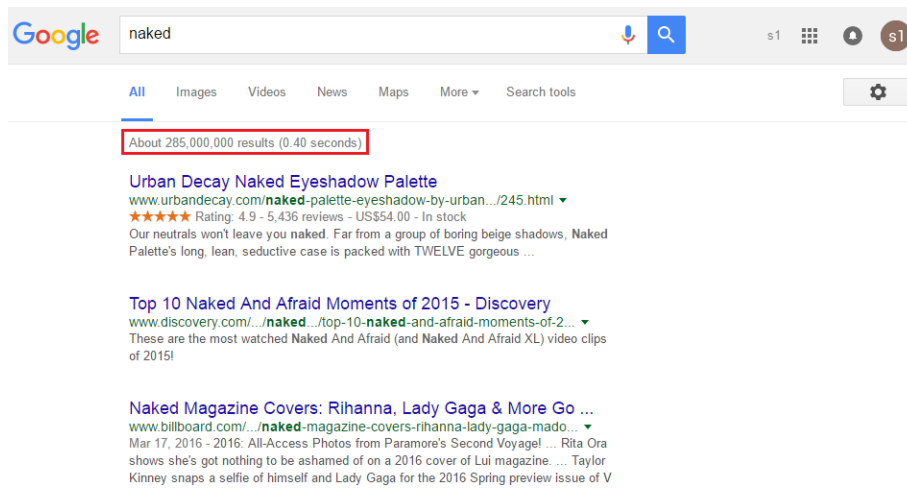
- a. **One Time Pull:** FortiClient EMS does not automatically sync profile changes from the FortiGate or FortiManager. You can manually sync profile changes after importing the profile. See [Syncing profile changes on page 142](#).
 - b. **Group Schedule:** Configure a group synchronization schedule 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 193](#).
 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

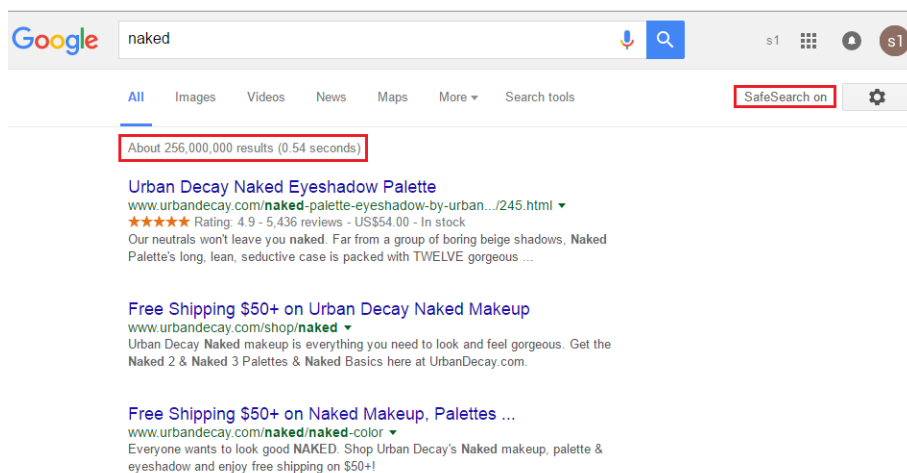
The search engine provides a Safe Search feature that blocks inappropriate or explicit images from search results. The Safe Search feature helps avoid most adult content. FortiClient EMS supports Safe Search for most common search engines, such as Google, Yahoo, and Bing.

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

Support 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. The *Keyword Scanning on Search*

Engine feature 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*.

FortiClient Endpoint Management Server

Profile Name: Default - Chromebooks

Web Filter

☒ Keyword Scanning on Search Engine

☒ Banned Word Search

Category	Block	Monitor	Off
Violence/Terrorism	Block	Monitor	Off
Extremist	Block	Monitor	Off
Pornography	Block	Monitor	Off
Cyber Bullying	Block	Monitor	Off
Self Harm	Block	Monitor	Off

☒ Custom Banned Words

Banned Word	Action	Status
#지살	Monitor	<input checked="" type="checkbox"/>
War	Allow	<input checked="" type="checkbox"/>
Rifle	Block	<input checked="" type="checkbox"/>
Bomb	Monitor	<input checked="" type="checkbox"/>
Hacking	Block	<input checked="" type="checkbox"/>
Attack	Allow, Block, Allow, Monitor	<input type="checkbox"/>

Exclusion List

Simple: Perform a case-insensitive matching against URLs.

Wildcard: ? matches any character once. For example, the pattern 123??? will match 123a or 123abc, but not 123abcdef. * matches zero or more characters.

Save Discard Changes Revert to Default

You can view user statistics on the *Blocked Search Words* and *Monitored Search Words* widgets in *Dashboard > Chromebook Status*.

FortiClient Endpoint Management Server

Dashboard

FortiClient Status

Vulnerability Scan

Chromebook Status

Endpoints

Google Domains

Quarantine Management

Software Inventory

Endpoint Policy

Chromebook Policy

Endpoint Profiles

Deployment

Manage Installers

Policy Components

Telemetry Server Lists

Compliance Verification

Administration

System Settings

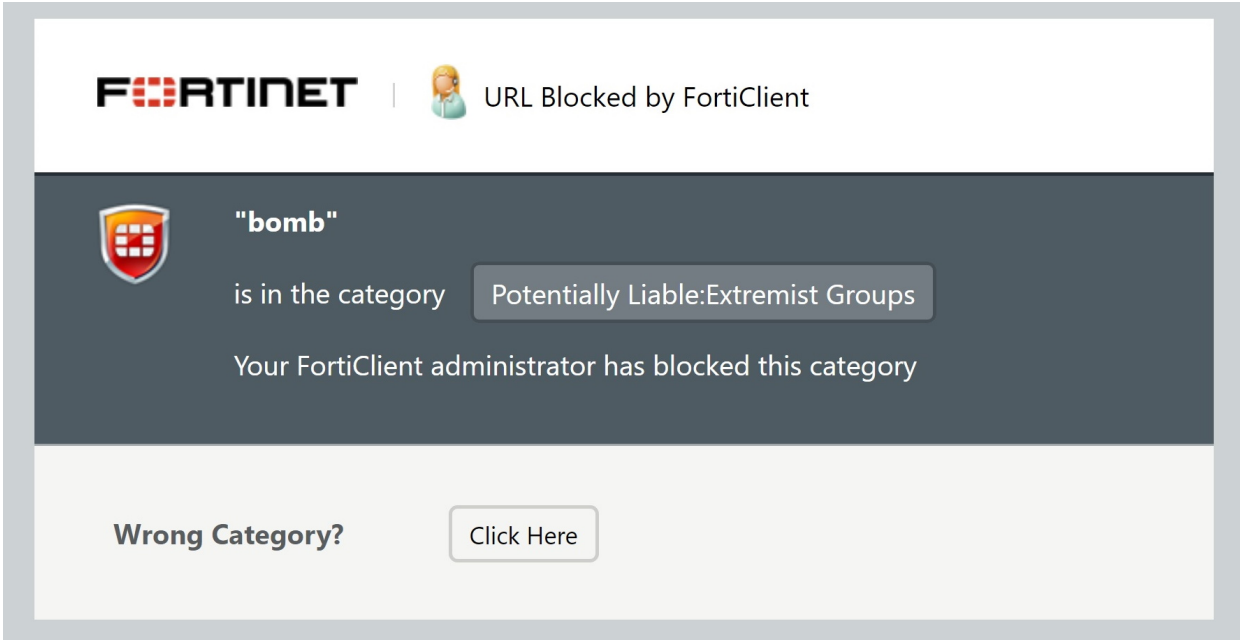
Blocked Search Words

Word	Frequency
cocaine	85
suicide	80
ak47	65
kills	55
selfcomb...	50
cannabis	35
cyberpat...	25
grenade	20
at quada	15
qanda	15

Monitored Search Words

Word	Frequency
hacking	30
terror	30
sniper	27
isis	27
bomb	22
armory	21
#지살	16
bullet	14
weapon	13
ar15	12

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.



Video Filter

This feature requires the Web Filter profile and *Enable Web Browser Plugin for Web Filtering* to be enabled. This feature is only available for FortiClient (Windows) endpoints.

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: <ul style="list-style-type: none">BlockWarnAllowMonitor The following lists the available categories: <ul style="list-style-type: none">Not RatedKnowledgePeopleBusinessLifestyleSociety

Configuration	Description
	<ul style="list-style-type: none"> • 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	<p>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.</p> <p>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.</p>
Channel Override List	<p>Configure access for a specific YouTube channel. In the <i>Channel ID</i> field, enter the YouTube channel ID. You can also import a list of channels using a CSV file.</p> <p>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.</p>
Video Override List	Configure access for a specific YouTube video. In the <i>Video URL</i> 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	<p>Select an action for FortiClient to take for YouTube videos when it cannot reach the FortiGuard server. Select one of the following:</p> <ul style="list-style-type: none"> • Block • Warn • Allow • Monitor
FortiGuard Server Location	<p>Configure the FortiGuard server location. FortiClient connects to FortiGuard to query for URL ratings.</p> <p>The URLs connected to for each server location are as follows:</p> <ul style="list-style-type: none"> • Global: fctguard.fortinet.net • U.S.: fctusguard.fortinet.net
FortiGuard Server Type	Only FortiGuard Anycast is available.

Vulnerability Scan



If you enable both *Automatic Maintenance* and *Scheduled Scan*, FortiClient EMS only uses the *Automatic Maintenance* settings.

Configuration	Description
Vulnerability Scan	<p>Enable or disable Vulnerability Scan.</p> <p>Enable or disable the eye icon to show or hide this feature from the end user in FortiClient.</p>
Scanning	
Scan on Registration	Scan endpoints upon connecting to a FortiGate.
Scan on Vulnerability Signature Update	Scan endpoints upon updating a vulnerability signature.
Scan for OS Updates	<p>Run system updates for the underlying operating system (OS):</p> <ul style="list-style-type: none"> 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. <p>FortiClient notifies the OS to do these updates.</p>
Enable Proxy	Enable using proxy settings configured in when downloading updates for vulnerability patches.
Automatic Maintenance	<p>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.</p>
Period	Specify how often Vulnerability Scan needs to be started during automatic maintenance. Enter the desired number of days.
Deadline	<p>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.</p> <p>This value must be greater than the <i>Period</i> value.</p>
Scheduled Scan	Configure settings for scheduled scanning.
Schedule Type	Select <i>Daily</i> , <i>Weekly</i> , <i>Monthly</i> .

Configuration	Description
Scan On	Configure the day the scan will run. This only applies if the schedule type is configured to <i>Weekly</i> or <i>Monthly</i> . 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	<p>Patches are installed automatically when vulnerabilities are detected. Select one of the following:</p> <ul style="list-style-type: none"> • 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. <p>Automatic patching may require the endpoint to reboot.</p>
Exclusions	
Exempt Application Vulnerabilities Requiring Manual Update from Vulnerability Compliance Check	<p>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.</p>
Exclude Selected Applications from Vulnerability Compliance Check	<p>In the <i><number> Applications</i> list, click the applications to exclude from vulnerability compliance check, and they are automatically moved to the <i><number> Excluded Applications</i> list.</p> <p>In the <i><number> Excluded Applications</i> list, click the applications to remove from the exclusion list.</p> <p>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.</p>
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 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 22](#) 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.
Real-Time Protection	Enable real-time protection (RTP).
Action On Virus Discovery	<ul style="list-style-type: none"> 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 <i>Virus Alert</i> 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.
Identify Malware and Exploits Using Signatures Received from FortiSandbox	Uses signatures from FortiSandbox to identify malware and exploits. This option is available only if the <i>Sandbox Detection</i> tab is enabled. Enter the number of minutes after which to update signatures.
Scan Compressed Files	Scan archive files, including zip, rar, and tar files, for threats. RTP exclusions list default file extensions.
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.

Options	Description
Scan Files Accessed by User Process	<p>Configure when RTP should scan files that a user-initiated process accesses. Select one of the following:</p> <ul style="list-style-type: none"> • 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	<p>Enable system process scanning. Select one of the following:</p> <ul style="list-style-type: none"> • 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	<p>Enable Microsoft Anti-Malware Interface Scan (AMSI). This feature is only available for Windows 10 endpoints. AMSI scans memory for the following malicious behavior:</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <p>From the <i>Action On Virus Discovery With Machine Learning Analysis</i> dropdown list, select one of the following:</p> <ul style="list-style-type: none"> • <i>Log detection and warn the User</i>: detect the sample, display a warning message, and log the activity. • <i>Quarantine Infected Files</i>: 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	
Action On Virus Discovery	<p>Select one of the following from the dropdown list:</p> <ul style="list-style-type: none"> • 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

Options		Description
Integrate FortiClient into Windows Explorer's Context Menu		Adds a <i>Scan with FortiClient AntiVirus</i> 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.
Max Scan Speed on Computers With		<p>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:</p> <ul style="list-style-type: none"> • 4 GB • 6 GB • 8 GB • 12 GB • 16 GB
Enable Machine Learning Analysis		<p>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.</p> <p>From the <i>Action On Virus Discovery With Machine Learning Analysis</i> dropdown list, select one of the following:</p> <ul style="list-style-type: none"> • <i>Log detection and warn the User</i>: detect the sample, display a warning message, and log the activity.

Options	Description
	<ul style="list-style-type: none"> • 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 <i>Daily</i> , <i>Weekly</i> , or <i>Monthly</i> .
Scan On	If <i>Weekly</i> is selected, select the day of the week to perform the scan. If <i>Monthly</i> 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: <ul style="list-style-type: none"> • 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 <i>Scan Folder</i> field, enter the full path of the folder on your local hard disk drive to scan.
Scan Priority	Set to <i>Low</i> , <i>Normal</i> , or <i>High</i> . 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 anti-ransomware 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.

Options	Description
Protected Folders	Select the desired folders from the list, or click <i>Add Folder</i> to add a custom directory. FortiClient anti-ransomware protects all content in the selected folders against unauthorized changes. To remove a folder, select it then click the <i>Remove Folder</i> button. This field supports path variables.

Options	Description
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, you would enter <code>txt</code> , as opposed to <code>.txt</code> .
Action	<p>When anti-ransomware detects suspicious activity, it displays a popup asking the user if they want to terminate the process:</p> <ul style="list-style-type: none"> • If the user selects <i>Yes</i>, FortiClient terminates the suspicious process. • If the user selects <i>No</i>, FortiClient allows the process to continue. • If the user does not select an option, FortiClient waits for the configured action timeout, then does one of the following, as configured: <ul style="list-style-type: none"> • Block access and warn user if suspicious activity is detected: FortiClient terminates the suspicious process. • Warn user and resume after the timeout: FortiClient allows the process to continue.
Action Timeout	Enter the desired timeout value.
Bypass Valid Signer	Enable FortiClient to exclude a process from the selected anti-ransomware action if it has a valid signer.
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 the Anti-Exploit feature to function.

Cloud-Based Malware Detection

Enable cloud-based malware outbreak detection. The cloud-based malware protection feature 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 submitted 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 signed by trusted sources from cloud-based malware protection submission.
Remediation Actions	
Action	Choose <i>Quarantine</i> or <i>Alert & Notify</i> for malicious files. The user can access the file depending on <i>Wait for Cloudscan Results before Allowing File Access</i> and <i>Deny Access to File When There Is No Cloudscan Result</i> 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.
- [USBDeviceview](#)

Options	Description
Show bubble notifications	Display a bubble notification when FortiClient takes action with a removable media device.

Options	Description
Action	<p>Configure the action to take with removable media devices connected to the endpoint that match this rule. Available options are:</p> <ul style="list-style-type: none"> • <i>Allow</i>: Allow access to removable media devices connected to the endpoint that match this rule. • <i>Block</i>: Block access to removable media devices connected to the endpoint that match this rule. • <i>Monitor</i>: Log removable media device connections to the endpoint that match this rule.
Description	Enter the desired rule description.
Type	<p>Select <i>Simple</i> or <i>Regular Expression</i> for the rule type.</p> <p>When <i>Simple</i> is selected, FortiClient performs case-insensitive matching against classes, manufacturers, vendor IDs, product IDs, and revisions.</p> <p>When <i>Regular Expression</i> is selected, FortiClient uses Perl Compatible Regular Expressions (PCRE) to perform matching against classes, manufacturers, vendor IDs, product IDs, and revisions.</p>
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	<p>Configure the action to take with removable media devices that do not match any configured rules. Available options are:</p> <ul style="list-style-type: none"> • <i>Allow</i>: Allow access to removable media devices connected to the endpoint that do not match any configured rules. • <i>Block</i>: Block access to removable media devices connected to the endpoint that do not match any configured rules. • <i>Monitor</i>: 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 not 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 used by malware to protect themselves 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.

Options	Description
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, presents 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 (CDs, DVDs, Blu-ray disks, USB keys, etc.) on insertion.
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: <ul style="list-style-type: none">• 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 ZTNA license, the FortiClient Cloud Sandbox (PaaS) options are unavailable. See [Windows, macOS, and Linux licenses on page 22](#) 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 (PaaS). If multiple files are submitted around the same time, FortiClient sends one file to FortiClient Cloud Sandbox (PaaS), waits until it receives the verdict for that file, then sends the next file to FortiClient Cloud Sandbox (PaaS).



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	<p>Enable Sandbox Detection.</p> <p>Enable or disable the eye icon to show or hide this feature from the end user in FortiClient.</p>
Server	
FortiSandbox	<p>To configure connection to an on-premise FortiSandbox appliance or FortiSandbox Cloud, select <i>Appliance</i>. Select <i>Cloud</i> to configure connection to FortiClient Cloud Sandbox (PaaS). FortiClient Cloud Sandbox (PaaS) 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 (PaaS) does not offer the full range of features that a FortiSandbox appliance offers. FortiClient Cloud Sandbox (PaaS) is a service that uploads and analyzes files that FortiClient antivirus (AV) marks as suspicious.</p> <p>If FortiClient Cloud Sandbox (PaaS) 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 (PaaS) detection to ten hours if FortiGuard Labs is involved.</p> <p>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.</p> <p>FortiClient Cloud Sandbox (PaaS) is only available with the Endpoint Protection Platform license.</p>

Options	Description
IP address/Hostname	<p>For a FortiSandbox appliance, enter the FortiSandbox's IP address, FQDN, or hostname.</p> <p>Although the <i>IP address/Hostname</i> field is only available when <i>Appliance</i> is selected, you can also configure this option for FortiSandbox Cloud. Enter the FortiSandbox Cloud FQDN and account ID in the <i>Account ID</i> field.</p> <p>Click <i>Test Connection</i> to ensure that EMS can communicate with FortiSandbox. This option is only available when <i>Appliance</i> is selected.</p>
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 <i>Sandbox Events</i> tab. See Viewing Sandbox event details on page 101 .
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 <i>Sandbox Events</i> tab. See Viewing Sandbox event details on page 101 .
Region	FortiClient Cloud Sandbox (PaaS) region. See Configuring FortiGuard Services settings on page 336 .
Time Offset	FortiClient Cloud Sandbox (PaaS) time offset. See Configuring FortiGuard Services settings on page 336 .
License Status	Displays the Sandbox Cloud license status. Using FortiClient Cloud Sandbox (PaaS) requires an additional license. See FortiClient EMS on page 21 .
Inspection Mode	<p>Select one of the following:</p> <ul style="list-style-type: none"> <i>None</i>: FortiClient does not send any files to FortiSandbox for inspection. <i>High-Risk Files</i>: FortiClient inspects all supported high-risk files and sends to FortiSandbox as appropriate. The following are considered high-risk file types: exe, bat, vbs, js, htm, htm, gz, rar, tar, lzh, upx, zip, cab, bz2, 7z, pdf, xz, swf, rtf, dll, doc, xls, ppt, docx, xlsx, pptx, thmx, apk, exe, lnk, kgb, z, ace, jar, msi, mime, mac, dmg, mac, iso, elf, arj <i>All Supported Extensions</i>: FortiClient inspects all supported file extensions and sends to FortiSandbox as appropriate. This option is only available for a FortiSandbox appliance.
Excluded File Extensions	Select a file extension to exclude from FortiSandbox scanning. You can select multiple file extensions.
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.

Options	Description
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.
Remediation Actions	
Action	Choose <i>Quarantine</i> or <i>Alert & Notify</i> for infected files. The user can access the file depending on <i>Wait for FortiSandbox Results before Allowing File Access</i> and <i>Deny Access to File When There Is No Sandbox Result</i> configuration. Whether FortiClient quarantines the file depends on if FortiSandbox reports the file as malicious and the <i>FortiSandbox Detection Verdict Level</i> setting.
FortiSandbox Detection Verdict Level	Select the desired detection verdict level. For FortiClient to apply the action selected in the <i>Action</i> field to an infected file, FortiSandbox must detect the file as this level or higher. For example, if <i>Action</i> is configured as <i>Quarantine</i> and <i>FortiSandbox Detection Verdict Level</i> is configured as <i>Medium</i> , 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: <ul style="list-style-type: none"> • Microsoft • Fortinet • Mozilla • Windows • Google • Skype • Apple • Yahoo! • Intel
Exclude Specified Folders/Files	Exclude specified folders/files from FortiSandbox submission. You must also create the exclusion list.
Inclusions	
Include Specified Folders/Files	Include specified folders/files in FortiSandbox submission. You must also create the inclusion list.
Other	

Options	Description
Hide Sandbox Scan from Windows Explorer's Context Menu	Hide Sandbox scan option from Windows Explorer's right-click context menu.
Notification Type	<p>Select the desired notification type to display to end users when FortiClient Cloud Sandbox (PaaS) detects an infected file:</p> <ul style="list-style-type: none"> • 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	<p>Enable application control.</p> <p>Enable or disable the eye icon to show or hide this feature from the end user in FortiClient.</p>
General	
Notification Bubbles on User's Desktop When Applications Are Blocked	Enable notification bubbles when applications are blocked.
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 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: <ul style="list-style-type: none"> • Botnet • Business • 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	Enable FortiClient firewall to allow, block, or monitor applications based on their signature. Adding more than 1000 application overrides is not recommended and can cause EMS instability.
Delete	Delete an application.
Add Signatures	Add a signature to an application.

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.

Configuration	Description
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 <i>System Setting > UI > Require Password to Disconnect from EMS</i> and provides a password. This allows the FortiClient endpoint administrator to uninstall FortiClient using the msixexec 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).
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 Zero Trust Tags on page 246 .

Configuration	Description
Language	<p>Configure the language that FortiClient uses. By default, FortiClient uses the system operating language. Select one of the following:</p> <ul style="list-style-type: none">• 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	<p>From the dropdown list, select the tab for FortiClient to display by default when the user opens the console.</p>
Log	<p>Specify FortiClient log settings.</p>

Configuration	Description
Level	<p>This option is available for Chromebook profiles. Generates logs equal to and more critical than the selected level. Select one of the following:</p> <ul style="list-style-type: none"> • 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	<p>Select features to generate logs for:</p> <ul style="list-style-type: none"> • AntiVirus • Application Firewall • Telemetry • FSSOMA • Proxy • IPsec VPN • AntiExploit • SSL VPN • Update • Vulnerability • Web Filter • Sandbox
Client-Based Logging When On-Fabric	<p>Include local log messages when FortiClient is on-fabric. FortiClient hides the <i>Export log</i> and <i>Clear log</i> 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 135.</p>
Upload Logs to FortiAnalyzer/FortiManager	<p>This option and all nested options are available for Chromebook profiles. Configure endpoints to send logs to the FortiAnalyzer or FortiManager at the specified address or hostname.</p> <p>The <i>Upload UTM Logs</i>, <i>Upload System Event</i>, and <i>Upload Security Event</i> fields only apply to FortiClient 6.4.3 and later versions.</p> <p>The <i>Upload Vulnerability Logs</i> and <i>Upload Event Log</i> fields only apply to FortiClient 6.4.2 and earlier versions.</p>

Configuration	Description
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 21 .
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 <code>/var/log/system.log</code> . 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 <code>https://FAZ-IP:port/logging</code> . If using a port other than the default, use <code><address>:<port></code> . 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 <code>1208151.ca-west-1.fortianalyzer.forticloud.com</code> . 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.

Configuration	Description
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.
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: <ul style="list-style-type: none"> • 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 <i>Show Password</i> to show the password in plain text.
Update	Specify whether to use FortiManager to update FortiClient on endpoints.
Use FortiManager for Client Signature Update	Enable FortiClient EMS to obtain 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.

Configuration	Description
FortiGuard Server Location	<p>Configure the FortiGuard server location. If <i>FortiGuard Anycast</i> is selected for the <i>Server</i> field, you can select from global, U.S., or Europe. If <i>FortiGuard</i> is selected for the <i>Server</i> field, you can select from global or U.S. When <i>Global</i> is selected, FortiClient uses the closest FortiGuard server.</p> <p>FortiClient connects to FortiGuard to query for AV and vulnerability scan engine and signature updates.</p> <p>The URLs connected to for each server location are as follows:</p> <ul style="list-style-type: none"> FortiGuard: <ul style="list-style-type: none"> Global: forticlient.fortinet.net U.S.: usforticlient.fortinet.net FortiGuard Anycast: <ul style="list-style-type: none"> Global: fctupdate.fortinet.net U.S.: fctusupdate.fortinet.net Europe: fcteuupdate.fortinet.net
Server	Configure the FortiGuard server to <i>FortiGuard</i> or <i>FortiGuard Anycast</i> .
FortiProxy	Enable FortiProxy (disable only when troubleshooting). You must enable FortiProxy to use Web Filter and some AV options.
HTTPS Proxy	Enable HTTPS proxy. If disabled, FortiProxy no longer inspects HTTPS traffic.
HTTP Timeout	Enter the HTTP connection timeout interval in seconds. FortiProxy determines if the remote server is available based on this timeout value. Lower this timeout value if your client requires a faster fail response.
POP3 Client Comforting	Enable POP3 client comforting. Client comforting helps to prevent POP3 clients from complaining that the server has not responded in time.
POP3 Server Comforting	Enable POP3 server comforting. Server comforting helps to prevent POP3 servers from complaining that the client has not responded in time. You may use this in a situation where FortiClient is installed on a mail server.
SMTP Client Comforting	Enable SMTP client comforting. SMTP comforting helps to prevent SMTP clients from complaining that the server has not responded in time.

Configuration	Description
Self Test	<p>FortiProxy can detect if other software is disrupting internal traffic between FortiProxy's internal modules. It does this by sending packets periodically to 1.1.1.1, which are intercepted by FortiClient and dropped (they never leave the computer). If the packets are not detected, then it is deemed highly likely that third party software is intercepting the packets, signaling that FortiProxy cannot perform regular traffic filtering.</p> <p>Enable self tests. FortiProxy periodically checks its own connectivity to determine if it is able to proxy other applications' traffic.</p>
Notify	Display a bubble notification when self-testing detects that a third party program has blocked HTTP/HTTPS filtering and SMTP/POP3 AV scanning.
Last Port	<p>Enter the last port number used. This is the highest port number you want to allow FortiProxy to listen on. Use to prevent FortiProxy from binding to another port that another service normally uses.</p> <p>The available port range is 65535 to 10000.</p>
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	<p>Turn on to enable on-fabric subnets.</p> <p>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 135.</p>
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	<p>Send installed application information to FortiClient EMS. If the <i>Upload Logs to FortiAnalyzer/FortiManager</i> option is enabled, the endpoint also sends the software inventory information to FortiAnalyzer. See Software Inventory on page 269.</p> <p>This feature requires the EPP license. See FortiClient EMS on page 21.</p>
Invalid Certificate Action	<p>Select the action to take when FortiClient attempts to connect to EMS with an invalid certificate:</p> <ul style="list-style-type: none"> • Allow: allows FortiClient to connect to EMS with an invalid

Configuration	Description
	<p>certificate.</p> <ul style="list-style-type: none"> • 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.
User Identity Settings	
Allow Users to Specify Identity Using	<p>Enable users to specify their identity in FortiClient using the following methods:</p> <ul style="list-style-type: none"> • Manually entering their details in FortiClient • Logging in to their account for the following social media services: <ul style="list-style-type: none"> • LinkedIn • Google • Salesforce <p>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.</p> <p>If this option is disabled, EMS obtains and displays user details from the endpoint OS.</p>
Notify Users to Submit User Identity Information	<p>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.</p>
Other	
Install CA Certificate on Client	<p>Turn on to select and install a CA certificate on the FortiClient endpoint.</p> <p>You can add certificates by going to <i>Endpoint Policy & Components > CA Certificates</i>.</p>
FortiClient Single Sign-On Mobility Agent	<p>Enable Single Sign-On Mobility Agent for FortiAuthenticator. To use this feature you need to apply a FortiClient SSO mobility agent license to your FortiAuthenticator.</p>
IP Address/Hostname	Enter the FortiAuthenticator IP address or hostname.
Port	Enter the port number.

Configuration	Description
Pre-Shared Key	Enter the preshared key. The preshared key should match the key configured on your FortiAuthenticator.
iOS	
Distribute Configuration Profile	Enable and browse for your <code>.mobileconfig</code> file to distribute the configuration profile.
Privacy	
Send Usage Statistics to Fortinet	Submit virus information to FDS. Fortinet uses this information to improve product quality and user experience.
Privilege Access Management	Enable privilege 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.

Configuring identity compliance for endpoints

You can assign different user identification options to different endpoints. These options, visible in FortiClient, include:

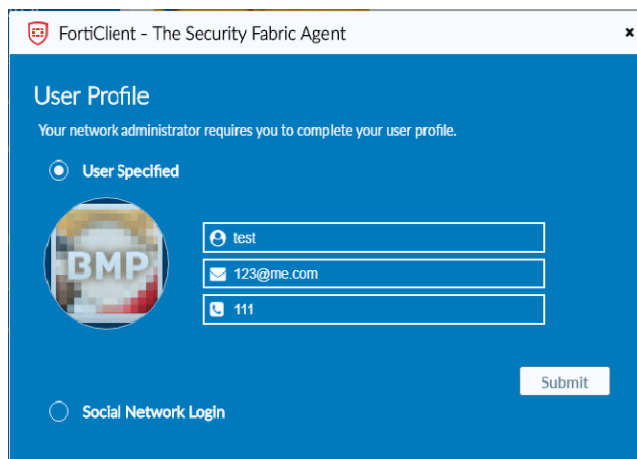
- User Input
- OS
- LinkedIn
- Google
- Salesforce

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 - The Security Fabric Agent

User Profile

Your network administrator requires you to complete your user profile.

☒ User Specified

☐ Social Network Login

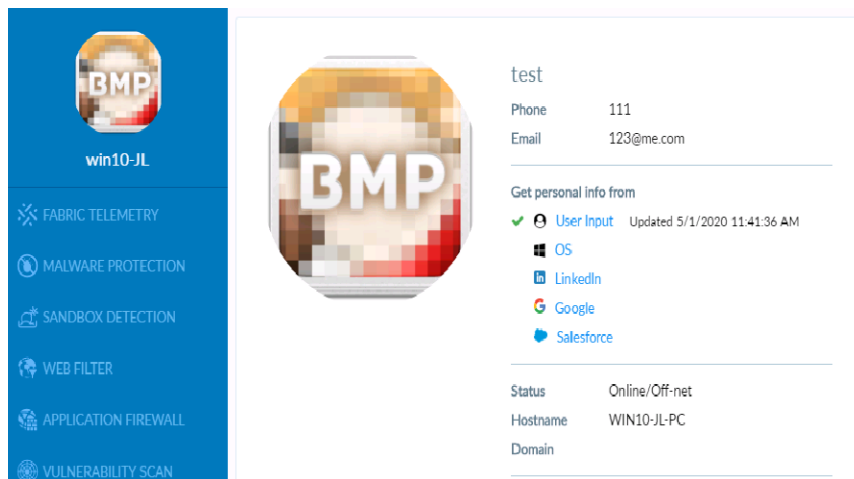
test

123@me.com

111

Submit

FortiClient displays the entered login information.



win10-JL

FABRIC TELEMETRY

MALWARE PROTECTION

SANDBOX DETECTION

WEB FILTER

APPLICATION FIREWALL

VULNERABILITY SCAN

test

Phone 111

Email 123@me.com

Get personal info from

✓ User Input Updated 5/1/2020 11:41:36 AM

OS

LinkedIn

Google

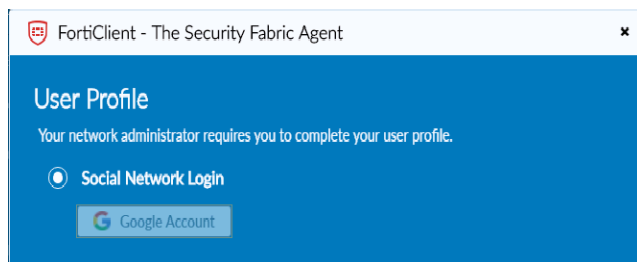
Salesforce

Status Online/Off-net

Hostname WIN10-JL-PC

Domain

If Google is enabled, the user can log in to their Google account.



FortiClient - The Security Fabric Agent

User Profile

Your network administrator requires you to complete your user profile.

☐ User Specified

☒ Social Network Login

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 234](#).

- 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 236](#).
- 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 237](#).

This document also describes the following use cases:

- [To configure a secret for SSH to a FortiGate: on page 237](#)
- [To use a secret to log in to a website: on page 238](#)

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 https ssh http telnet
        set type physical
        set monitor-bandwidth enable
        set snmp-index 1
    next
end
```

3. Clear the browser cache.
4. Log into FortiPAM via its interface IP address using HTTP. For example, if the interface IP address is 172.17.61.167, go to <http://172.17.61.167>. Do not use HTTPS. FortiPAM does not support HTTPS before license validation.
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-4ele-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:

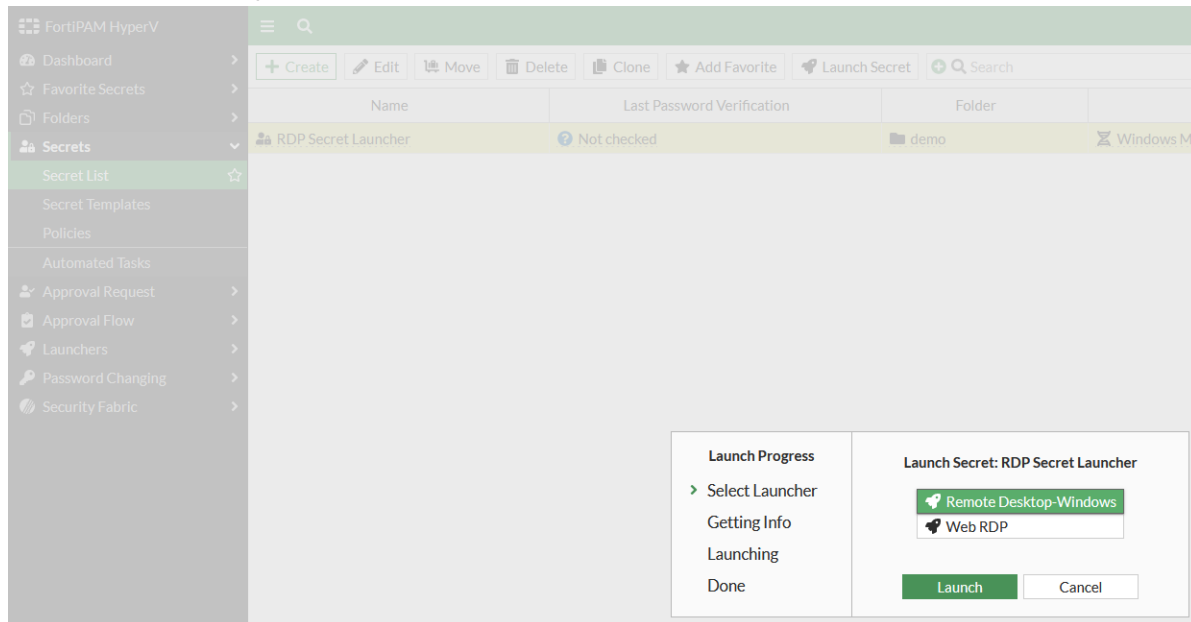
```
config secret database
  edit 22
    set name "RDP Secret Launcher"
    set folder 5
    set template "Windows Machine"
    set recording enable
    set proxy enable
    set block-rdp-clipboard disable
    set rdp-service-status up
    set samba-service-status up
    config credentials-history
    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 1LUCAA722LevoHAohj7+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 *Privilege Access Management*.
4. In the *Port* field, enter 9191.
5. 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:

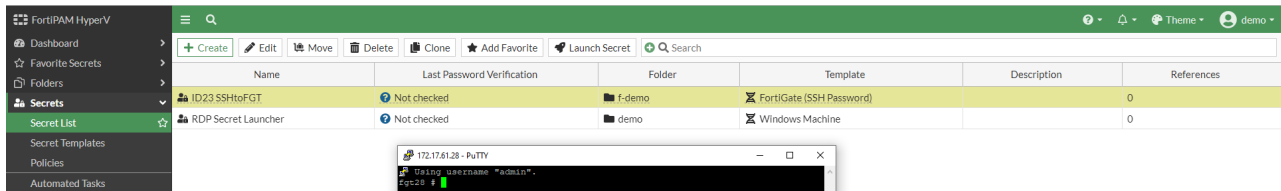
```
config secret database
  edit 23
    set name "ID23 SSHtoFGT"
```

```

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 kseKVIs1SftEmwBy8OqUPyYryoA="
  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
end

```

```

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.




Root user sign in ⓘ

Email: @gmail.com

Password

[Forgot password?](#)

Use FortiPAM session credentials 

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 238](#), 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:

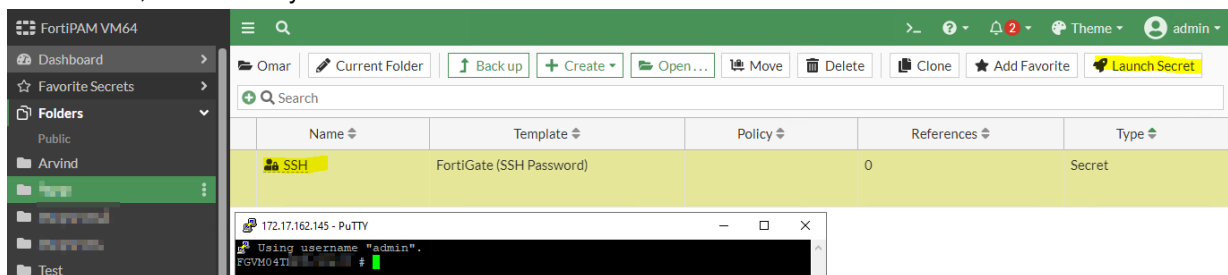
```
<forticlient_configuration>
  <fssoma>
    <enabled>1</enabled>
    <serveraddress>fac0824.test.local:8001</serveraddress>
    <presaredkey>
      <![CDATA[Fortinet123!]]>
    </presaredkey>
    <address_category>0</address_category>
  </fssoma>
  <pam>
    <enabled>1</enabled>
    <default_port>9191</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.

Logon Time	Update Time	Workstation	IP Address	Domain Grouping	Domain	Username	Source	Group
Thu Mar 2 16:12:48 2023	Fri Mar 3 12:13:45 2023		172.17.81.111	DEFAULT	10824.COM	ADFSUSER1	FortiClient	CN=ADFSUSER1,CN=USERS.DC=DDYS0824.DC=COM+CN=ADMINISTRATORS,CN=BUILTIN.DC=EDS0824.DC=COM+CN=REMOTE SKTOPUSERS,CN=BUILTIN.DC=EDS0824.DC=COM+CN=KEYALINS,CN=USERS.DC=10824.COM+CN=TEST-GRPCN=USERS.CN=BUILTIN.DC=EDS0824.DC=COM+CN=DOMAINUSERS,CN=USERS.DC=10824.COM
Fri Mar 3 11:23:52 2023	Fri Mar 3 12:13:53 2023	WIN10-10824.COM	192.168.0.7	DEFAULT	10824.COM	ADMINISTRATOR	FortiClient	CN=ADMINISTRATOR,CN=USERS.DC=10824.DC=COM+CN=HEMA-ADMINS,CN=USERS.DC=EDS0824.DC=COM+CN=ENTERISE-ADMINS,CN=USERS.DC=EDS0824.DC=COM+CN=ADMINISTRATORS,CN=BUILTIN.DC=EDS0824.DC=COM+CN=DOMAINADNS,CN=USERS.DC=10824.COM+CN=DENIED RODC PASORD REPLICATION GROUP,CN=USERS.DC=10824.DC=COM+CN=GROUP POLICY CREATOR,CN=USERS.DC=10824.DC=COM+CN=USERS,CN=BUILTIN.DC=EDS0824.DC=COM+CN=DOMAINUSERS,CN=USERS.DC=DDYS0824.DC=COM

- 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.

Logon Time	Update Time	Workstation	IP Address	Domain Grouping	Domain	Username	Source	Group
Thu Mar 2 16:12:48 20...	Fri Mar 3 12:13:45 2023	WIN10-10824.COM	172.17.81.111	DEFAULT	10824.COM	ADFSUSER1	FortiClient	CN=ADFSUSER1,CN=USERS,DC=DDYS0824.DC=COM+CN=ADMINISTRATORS,CN=BUILTIN,DC=EDS0824.DC=COM+CN=REMOTE SKTOP,USERS,CN=BUILTIN,DC=DYS0824.DC=COM+CN=KEY AI INS,CN=USERS,DC=10824.DC=COM+CN=TEST-GRP,CN=USERS,DC=10824.DC=COM+CN=USERS,CN=BUILTIN,DC=10824.DC=COM+CN=DOMAIN US S,CN=USERS,DC=10824.DC=COM
Fri Mar 3 11:23:52 2023	Fri Mar 3 12:13:53 2023	WIN10-10824.COM	192.168.0.7	DEFAULT	10824.COM	ADMINISTRATOR	FortiClient	CN=ADMINISTRATOR,CN=USERS,DC=10824.DC=COM+CN=HEMA ADMIN,CN=USERS,DC=DYS0824.DC=COM+CN=ENTERISE ADMIN,CN=USERS,DC=EDS0824.DC=COM+CN=ADMINISTRATORS,CN=BUILTIN,DC=10824.DC=COM+CN=DOMAIN ADMIN,CN=USERS,DC=10824.DC=COM+CN=CN=DENIED RODC PAS ORD REPLICATION GROUP,CN=ERS,DC=10824.DC=COM+CN=GROUP POLICY CREATOR C NERS,CN=USERS,DC=10824.DC=COM+CN=USERS,CN=BUI N,DC=10824.DC=COM+CN=DOMAIN USERS,CN=USERS,DC=DDYS0824.DC=COM

c. In FortiPAM, confirm that you can access a secret created in FortiPAM.

Name	Template	Policy	References	Type
SSH	FortiGate (SSH Password)		0	Secret

Below the table, a terminal window shows a successful login for the 'admin' user on 172.17.162.145.

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*.

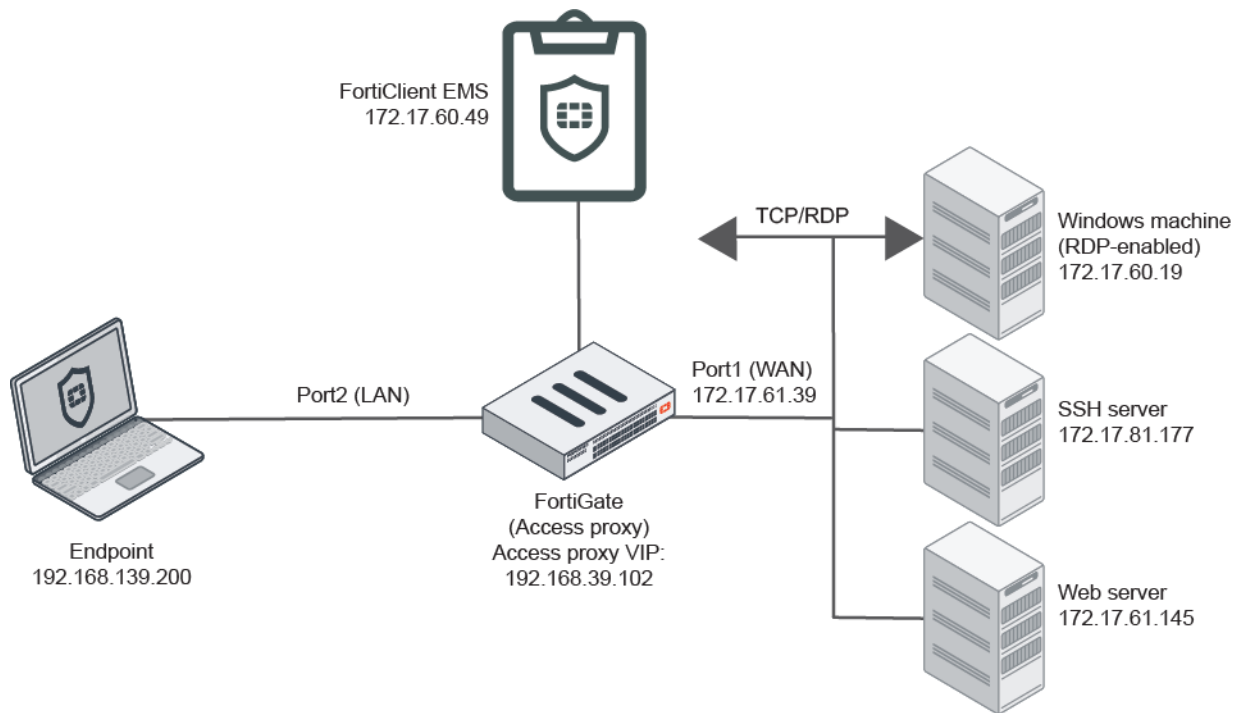
If the profile has a feature enabled that is disabled in Feature Select, EMS displays a warning that the feature is disabled on endpoints that the profile is deployed to. To enable this feature on the endpoint, you must enable the feature in Feature Select. See [Feature Select on page 346](#).

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:

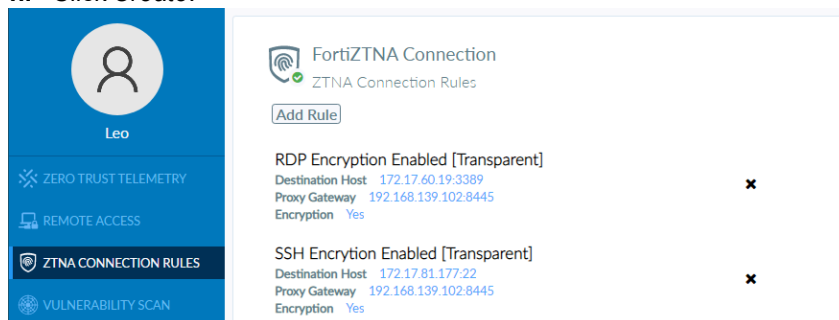
1. In EMS, go to *Endpoint Profiles > Manage Profiles*.
2. Edit the desired profile.
3. On the *XML Configuration* tab, add the following configuration:

```
<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 HTTP/1.1`. When encryption is disabled, the debug logs contain the line `GET tcpaddress=172.17.81.177&port=22&tls=0 HTTP/1.1`.

Zero Trust Tags

Zero trust network access (ZTNA) is an access control method that uses client device identification, authentication, and Zero Trust 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 device verification, authenticating the user's identity, authorizing the user, and then performing context based posture checks using Zero Trust 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. User experience is also affected when multiple VPNs are needed to get to various resources. ZTNA can improve this experience.

You can create Zero Trust tagging rules for endpoints based on their operating system versions, logged in domains, running processes, and other criteria. EMS uses the rules to dynamically group endpoints. FortiOS can use the dynamic endpoint groups to build dynamic policy rules.

See the [Zero Trust Application Gateway Admin Guide](#) for more information about ZTNA.

Zero Trust Tagging Rules

You can create, edit, and delete Zero Trust tagging rules for endpoints. You can also view and manage the tags used to dynamically group endpoints.

The following occurs when using Zero Trust tagging rules with EMS and FortiClient:

1. EMS sends Zero Trust tagging 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 log-on/log-off 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 329](#).
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 *Zero Trust Tags > Zero Trust Tag Monitor*. See [Zero Trust Tag Monitor on page 255](#).

Adding a Zero Trust tagging rule set

To add a Zero Trust tagging rule set:

1. Go to *Zero Trust Tags > Zero Trust Tagging Rules*, and click *Add*.
2. In the *Name* field, enter the desired rule name.
3. In the *Tag Endpoint As* dropdown list, select an existing tag or enter a new tag. EMS uses this tag to dynamically group together endpoints that satisfy the rule, as well as any other rules that are configured to use this 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 [Zero Trust tagging rule types on page 249](#) 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 rule set. 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 Windows 7 and antivirus (AV) software is installed and running

With the default rule set logic, an endpoint would be eligible for the rule set if it is running Windows 7 or 10 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 Windows 7 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*.

Zero Trust Tagging Rule Set

Name

Tag Endpoint As

Enabled ☒

Comments

Rules		Default Logic	+ Add Rule
Type	Value		
Windows (2)			
AntiVirus Software	1 AV Software is installed and running		
OS Version	2 Windows 7		
	3 Windows 10		
Rule Logic	<input type="text" value="(1 and 3) or 2"/>		<input type="button" value="Reset"/>

9. Click *Save*.

Editing a Zero Trust tagging rule set

To edit a Zero Trust tagging rule:

1. Go to *Zero Trust Tags > Zero Trust Tagging Rules*.
2. Select the Zero Trust tagging rule.

3. Click *Edit*.
4. Edit as desired.
5. Click *Save*.

Deleting a Zero Trust tagging rule

To delete a Zero Trust tagging rule:

1. Go to *Zero Trust Tags > Zero Trust Tagging Rules*.
2. Click the desired Zero Trust tagging rule.
3. Click *Delete*.
4. In the confirmation dialog, click *Yes*.

Importing and exporting a Zero Trust tagging rule set

You can import and export Zero Trust tagging rule set as a JSON file.

To import a Zero Trust tagging rule set:

1. Go to *Zero Trust Tags > Zero Trust Tagging Rules*.
2. Click *Import*.
3. In the *Import Rule Sets* dialog, browse to and select the desired rule set JSON file.
4. Click *Import*.

To export a Zero Trust tagging rule set:

1. Go to *Zero Trust Tags > Zero Trust Tagging Rules*.
2. Select the desired rule set.
3. Click *Export*.
4. Save the JSON file to the desired directory.

Uploading signatures for FortiGuard Outbreak Alerts service

You can use a Zero Trust tagging rule as a predefined rule for FortiGuard outbreak alerts by uploading rule signatures.

To configure a Zero Trust tagging rule as a predefined rule for outbreak alerts by uploading rule signatures:

1. In EMS, go to *Zero Trust Tags > Zero Trust Tagging Rules*.
2. Click *Import Signatures*.

The screenshot shows the FortiClient Endpoint Management Server interface. On the left is a navigation menu with options: Dashboard, Endpoints, Deployment & Installers, Endpoint Policy & Components, Endpoint Profiles, Zero Trust Tags (selected), Zero Trust Tagging Rules, Zero Trust Tag Monitor, and Fabric Device Monitor. The main area displays a table titled 'Zero Trust Tagging Rule Sets'. The table has columns: Name, Tag, Enabled, and Comments. The 'Name' column is sorted by 'Tag'. The table contains 10 rows of predefined rules, all of which are enabled (indicated by a green checkmark in the 'Enabled' column).

Name	Tag	Enabled	Comments
Chrome Running File_Linux	Chrome Running File_Linux	✓	
Managed by EMS	EMS_Managed_Endpoint_Windows	✓	
Firefox Running Process_Linux	Firefox Running Process_Linux	✓	
Firefox Running Process_Mac	Firefox Running Process_Mac	✓	
Skype Running File_Mac	Skype Running File_Mac	✓	
Skype Running File_Windows	Skype Running File_Windows	✓	
Skype Running Process_Windows	Skype Running Process_Windows	✓	
Skype Running Registry_Windows	Skype Running Registry_Windows	✓	

3. In the *Import FortiGuard Outbreak Alert Signatures* dialog, upload a JSON file. The JSON file should contain an array of alert objects, each with a tag name and array of signatures. Each signature should have the following properties: `os` (windows, mac, linux, ios, android), `type` (file, registry, process), and `content`. If the import succeeds, EMS displays a *FortiGuard outbreak alert signatures imported successfully* message. If the file is formatted incorrectly, EMS shows an *Invalid JSON* error.
4. View tagged endpoints in *Zero Trust Tags > Zero Trust Tag Monitor*.

Managing tags

The *Manage Tags* window displays all configured tags.

To manage tags:

1. Go to *Zero Trust Tags > Zero Trust Tagging Rules*.
2. Click *Manage Tags*. You can see the list of tags and the associated rules.
3. You can configure a user notification message. The user notification message displays to the user when zero trust network access control rules on the FortiGate block FortiClient because of the applied tag. Click *Edit Description*, then enter the desired message in the text box. You can also delete an existing description using the *Delete Description* button.
4. Click *Save*.

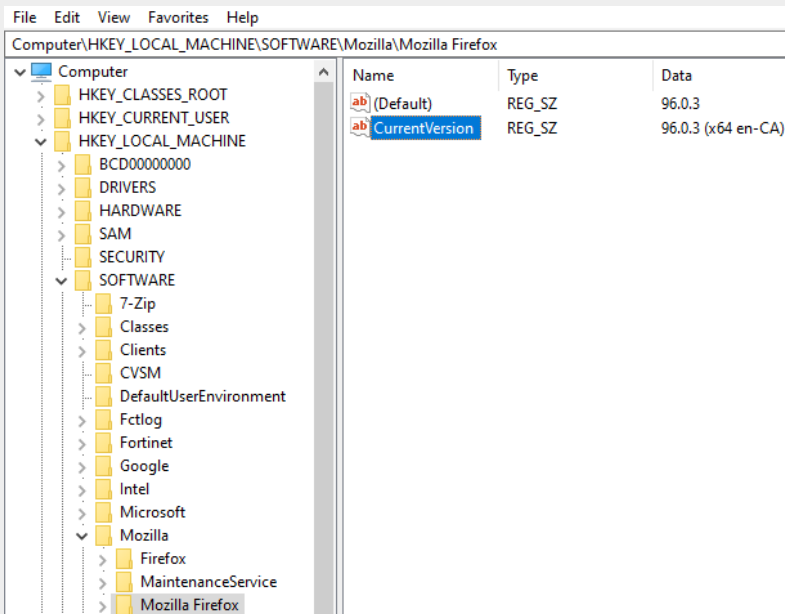
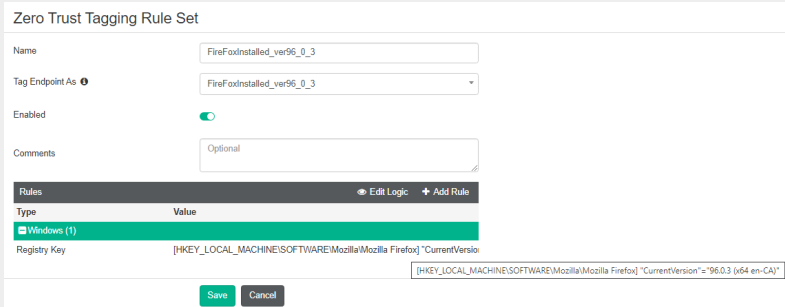
Zero Trust tagging rule types

The following table describes Zero Trust tagging rule types and the operating systems (OS) that they are available for. For all rule types, you can configure multiple conditions using the + button.

Rule type	OS	Description
User in AD Group	<ul style="list-style-type: none"> Windows macOS 	From the <i>AD Group</i> 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.

Rule type	OS	Description
		<p>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 <i>Evaluate on FortiClient</i>.</p> <p>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.</p> <p>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.</p> <p>To use this option, you must configure your domain under <i>Endpoints</i>. See Adding endpoints using an AD domain server on page 89.</p>
AntiVirus Software	<ul style="list-style-type: none"> Windows macOS Linux 	<p>From the <i>AV Software</i> dropdown list, select the desired conditions. You can require that an endpoint have 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.</p> <p>For Windows, this feature supports third party AV applications. For macOS and Linux, this feature can only check if FortiClient AV protection is enabled and does not recognize third party AV applications.</p> <p>The endpoint must satisfy all configured conditions to satisfy this rule.</p>
Certificate	<ul style="list-style-type: none"> Windows macOS Linux 	<p>In the <i>Subject CN</i> and <i>Issuer CN</i> 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.</p> <p>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.</p> <p>For Linux, FortiClient checks root CA certificates installed on the system. For Ubuntu, FortiClient checks <code>/etc/ssl/certs/ca-certificates.crt</code>. For CentOS and Red Hat, FortiClient checks <code>/etc/pki/tls/certs/ca-bundle.crt</code>. For Linux, FortiClient does not check user certificates.</p> <p>The <i>Subject CN</i> and <i>Issuer CN</i> fields do not support wildcards.</p>

Rule type	OS	Description
		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.
EMS Management	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Windows macOS Linux 	<p>In the <i>File</i> 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.</p> <p>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.</p>
Logged in Domain	<ul style="list-style-type: none"> Windows macOS 	In the <i>Domain</i> 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.
OS Version	<ul style="list-style-type: none"> Windows macOS Linux iOS Android 	<p>From the <i>OS Version</i> field, select the OS version. If the rule is configured for multiple OS versions, EMS considers the endpoint as satisfying the rule if it has one of the configured OS versions installed.</p> <p>The following options are available for Windows:</p> <ul style="list-style-type: none"> <i>Enable latest update check</i>: FortiClient checks if Windows OS updates were recently installed. <i>Latest update within</i>: 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.
On-Fabric Status	<ul style="list-style-type: none"> 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.
Registry Key	<ul style="list-style-type: none"> Windows 	In the <i>Key</i> 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 <i>Key Name</i> field, enter the registry key name, enclosed in double quotation marks "". From the dropdown list, select the desired comparator. In the <i>Value</i> 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 <i>Value</i> field. For a non-dword key value, enter the value enclosed in double quotation marks "".

Rule type	OS	Description
		<p>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.</p> <p>For example, the following shows a system where Firefox is installed. In this example, the registry path is <code>HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox</code>. The value name is <code>CurrentVersion</code>, and the value data is <code>96.0.3 (x64 en-CA)</code>. You can configure a registry key rule to match <code>HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox</code> as the path, <code>CurrentVersion</code> as the registry value name, or the value data as <code>96.0.3 (x64 en-CA)</code>. The example shown configures a rule to match the value data as <code>96.0.3 (x64 en-CA)</code>. Note the configured rule includes square brackets around the registry path, and double quotation marks around the key name and value.</p>   <p>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.</p>

Rule type	OS	Description
Running Process	<ul style="list-style-type: none"> Windows macOS Linux 	<p>In the <i>Running Process</i> 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.</p> <p>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.</p>
Sandbox Detection	<ul style="list-style-type: none"> Windows macOS 	<p>From the <i>Sandbox Detection</i> 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.</p>
User Identity	<ul style="list-style-type: none"> Windows macOS Linux iOS Android 	<p>Under <i>User Identity</i>, select the following:</p> <ul style="list-style-type: none"> <i>User Specified</i>: endpoint user manually entered their personal information in FortiClient. <i>Social Network Login</i>: 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: <ul style="list-style-type: none"> <i>All Accounts</i>: all endpoints where the user logged in to the specified social network account type. <i>Specified</i>: 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. <i>Verified User</i>: 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 306. <p>EMS considers the endpoint as satisfying the rule if it satisfies one of the conditions.</p> <p>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.</p> <p>FortiClient iOS does not support social network login with LinkedIn or Salesforce. FortiClient Android does not support social network login with Salesforce.</p>
Vulnerable Devices	<ul style="list-style-type: none"> Windows macOS Linux 	<p>From the <i>Severity Level</i> dropdown list, select the desired vulnerability severity level. If the rule 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.</p>
Security	<ul style="list-style-type: none"> macOS 	<p>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.</p>

Rule type	OS	Description
Windows Security	<ul style="list-style-type: none"> Windows 	<p>From the <i>Windows Security</i> dropdown list, select the desired conditions. You can require that an endpoint have one or more of the following applications enabled:</p> <ul style="list-style-type: none"> 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 computers are decommissioned or recycled. See BitLocker. 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. <p>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.</p>
Common Vulnerabilities and Exposures	<ul style="list-style-type: none"> Windows macOS Linux iOS Android 	<p>In the <i>CVEs</i> 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.</p> <p>EMS considers the endpoint as satisfying the rule if it satisfies one of the conditions.</p>
Firewall Threat	<ul style="list-style-type: none"> Windows macOS Linux iOS Android 	<p>In the <i>Firewall Threat ID</i> field, enter the firewall threat ID. You can find this ID in FortiGuard or on the <i>Firewall Events</i> 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.</p> <p>EMS considers the endpoint as satisfying the rule if it satisfies one of the conditions.</p>
FortiEDR	<ul style="list-style-type: none"> Windows macOS Linux 	<p>From the <i>FortiEDR</i> dropdown list, select <i>FortiEDR is installed and running</i>. EMS considers the endpoint as satisfying the rule if the endpoint has FortiEDR installed and running.</p>

Zero Trust Tag Monitor

You can view all dynamic endpoint groups in *Zero Trust Tags > Zero Trust Tag Monitor*. EMS creates dynamic endpoint groups based on the tag configured for each rule. This page shows endpoints tagged using the following tag types:

Tag	Description
Zero Trust tags	See Zero Trust Tags on page 246 .
FortiGuard outbreak alert tags	See FortiGuard Outbreak Alerts on page 267 .
Classification tags	See Viewing the Endpoints pane on page 91 .
Fabric tags	<p>Fabric tags require connection to FortiAnalyzer. See the following process:</p> <ol style="list-style-type: none"> 1. EMS administrator configures FortiAnalyzer in a System Settings profile. See System Settings on page 223. 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 <i>Zero Trust Tag Monitor</i>. This tag displays as a Fortinet Security Fabric tag in <i>Zero Trust Tag Monitor</i>, but the tag displays under <i>Classification Tags</i> in endpoint details. See Viewing the Endpoints pane on page 91. 7. If FortiGate is configured to receive all tags for this specific endpoint, EMS sends the tag to FortiGate. <p>See EMS API support for FortiAnalyzer to notify and tag suspicious endpoints.</p>

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	<p>Type of tag that the endpoint was tagged with. This can be one of the following:</p> <ul style="list-style-type: none"> • 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 endpoint groups

After defining Zero Trust 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.



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 dynamic endpoint groups

FortiOS uses an EMS connector to retrieve dynamic endpoint groups from EMS. Configuring this feature requires the following steps:

1. [Checking prerequisites on page 256](#)
2. [Configuring the EMS connector on page 257](#):
 - a. [Uploading certificates to EMS and FortiOS on page 257](#)
 - b. [Creating the EMS connector in FortiOS on page 257](#)
 - c. [Authorizing the FortiOS EMS connector in EMS on page 258](#)
 - d. [Verifying the FortiOS-EMS connection in FortiOS on page 258](#)
3. [Creating a dynamic firewall policy using dynamic endpoint groups from EMS on page 259](#)



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 Zero Trust 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 Zero Trust tagging rules. See [Adding a Zero Trust tagging rule set on page 246](#).
- After FortiClient connects Telemetry to EMS, confirm that EMS dynamically groups endpoints based on the Zero Trust tagging rules. See [Zero Trust Tag Monitor on page 255](#).

- 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:

Certificates are required to set up a secure connection between EMS and FortiOS. Uploading the CA-signed certificate to FortiOS allows FortiOS to trust the certificate that you upload to EMS.

1. Upload the server certificate to EMS:
 - a. Go to *System Settings > EMS Settings*.
 - b. Under *Shared Settings*, click the *Upload new SSL certificate* button.
 - c. Upload the server certificate and private key. Click *Test*.
 - d. Click *Save*.
2. Upload the certificate to FortiOS:
 - a. Go to *System > Certificates*.
 - b. From the *Import* dropdown list, select *CA Certificates*.
 - 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. Double-click the *FortiClient EMS* card.
3. In the *Name* field, enter the desired name.
4. 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 349](#).
5. Ensure that *Synchronize firewall addresses* is enabled. This allows FortiOS to automatically create and synchronize firewall addresses for dynamic endpoint groups received from EMS.
6. Click *OK*.

To create the EMS connector in the FortiOS CLI:

```
config endpoint-control fctems
  edit "ems137"
    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 5000
next
end

```

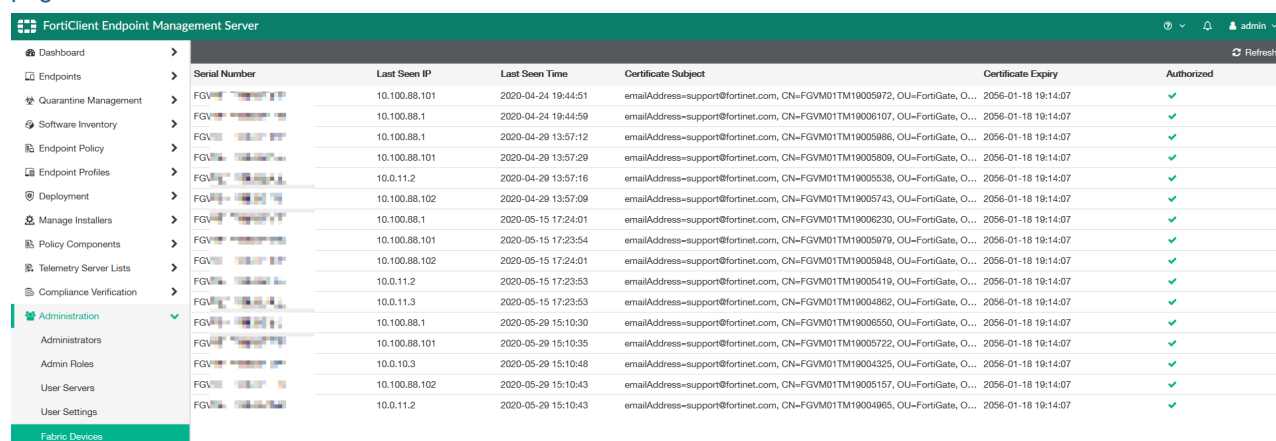
Authorizing the FortiOS EMS connector in EMS

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 *Administration > Fabric Devices*. Select the desired FortiGate, then click *Authorize*.

You can view all FortiGates that the EMS has authorized in *Administration > Fabric Devices*. See [Fabric Devices on page 296](#).



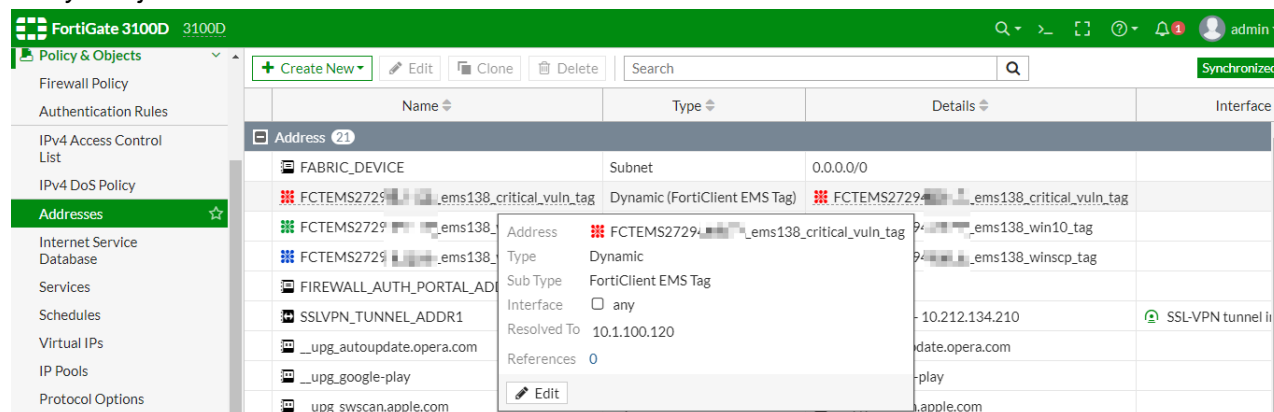
Serial Number	Last Seen IP	Last Seen Time	Certificate Subject	Certificate Expiry	Authorized
FGV...	10.100.88.101	2020-04-24 19:44:51	emailAddress=support@fortinet.com, CN=FGVM01TM19005972, OU=FortiGate, O...	2056-01-18 19:14:07	✓
FGV...	10.100.88.1	2020-04-24 19:44:59	emailAddress=support@fortinet.com, CN=FGVM01TM19006107, OU=FortiGate, O...	2056-01-18 19:14:07	✓
FGV...	10.100.88.1	2020-04-29 13:57:12	emailAddress=support@fortinet.com, CN=FGVM01TM19005886, OU=FortiGate, O...	2056-01-18 19:14:07	✓
FGV...	10.100.88.101	2020-04-29 13:57:29	emailAddress=support@fortinet.com, CN=FGVM01TM19005809, OU=FortiGate, O...	2056-01-18 19:14:07	✓
FGV...	10.0.11.2	2020-04-29 13:57:16	emailAddress=support@fortinet.com, CN=FGVM01TM19005538, OU=FortiGate, O...	2056-01-18 19:14:07	✓
FGV...	10.100.88.102	2020-04-29 13:57:09	emailAddress=support@fortinet.com, CN=FGVM01TM19005743, OU=FortiGate, O...	2056-01-18 19:14:07	✓
FGV...	10.100.88.1	2020-05-15 17:24:01	emailAddress=support@fortinet.com, CN=FGVM01TM19006230, OU=FortiGate, O...	2056-01-18 19:14:07	✓
FGV...	10.100.88.101	2020-05-15 17:23:54	emailAddress=support@fortinet.com, CN=FGVM01TM19005979, OU=FortiGate, O...	2056-01-18 19:14:07	✓
FGV...	10.100.88.102	2020-05-15 17:24:01	emailAddress=support@fortinet.com, CN=FGVM01TM19005948, OU=FortiGate, O...	2056-01-18 19:14:07	✓
FGV...	10.0.11.2	2020-05-15 17:23:53	emailAddress=support@fortinet.com, CN=FGVM01TM19005419, OU=FortiGate, O...	2056-01-18 19:14:07	✓
FGV...	10.0.11.3	2020-05-15 17:23:53	emailAddress=support@fortinet.com, CN=FGVM01TM19004862, OU=FortiGate, O...	2056-01-18 19:14:07	✓
FGV...	10.100.88.1	2020-05-29 15:10:30	emailAddress=support@fortinet.com, CN=FGVM01TM19006550, OU=FortiGate, O...	2056-01-18 19:14:07	✓
FGV...	10.100.88.101	2020-05-29 15:10:35	emailAddress=support@fortinet.com, CN=FGVM01TM19005722, OU=FortiGate, O...	2056-01-18 19:14:07	✓
FGV...	10.0.10.3	2020-05-29 15:10:48	emailAddress=support@fortinet.com, CN=FGVM01TM19004325, OU=FortiGate, O...	2056-01-18 19:14:07	✓
FGV...	10.100.88.102	2020-05-29 15:10:43	emailAddress=support@fortinet.com, CN=FGVM01TM19005157, OU=FortiGate, O...	2056-01-18 19:14:07	✓
FGV...	10.0.11.2	2020-05-29 15:10:43	emailAddress=support@fortinet.com, CN=FGVM01TM19004965, OU=FortiGate, O...	2056-01-18 19:14:07	✓

Verifying the FortiOS-EMS connection in FortiOS

To verify the FortiOS-EMS connection in FortiOS:

- Authorize the connection by doing one of the following:
 - In the right pane, under *FortiClient EMS Status*, click *Authorize*.
 - After EMS authorizes the FortiGate, authorize the connection in the FortiOS CLI by running the `execute fctems verify <fctems>` command.
- FortiOS should now automatically pull the dynamic endpoint groups from EMS as dynamic firewall addresses. Go to

Policy & Objects > Addresses to view the addresses.



Creating a dynamic firewall policy using dynamic endpoint groups from EMS

To create a dynamic firewall policy using dynamic endpoint groups from EMS:

1. In FortiOS, go to *Policy & Objects > Firewall Policy*. Click *Create New*.
2. In the *Source* field, click *+*. The *Select Entries* pane appears. On the *Address* tab, select the address based on the desired dynamic endpoint group 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.

Restricting VPN access to rogue/non-compliant devices with Security Fabric

The following guide provides instructions on configuring the Security Fabric to restrict VPN access to rogue/non-compliant devices using EMS and FortiOS. You can configure this feature with IPsec and SSL VPN. Configuring this feature consists of the following steps:

1. Create two Zero Trust tagging rules in EMS: one rule for compliant endpoints and one rule for non-compliant endpoints. In this example, one rule tags endpoints as "AV-Running" if they have antivirus software installed and running. The second rule tags endpoints as "RED-Alert" if they have the risk.txt file present. You must also configure the EMS connector in FortiOS. See [Configuring FortiOS dynamic policies using EMS dynamic endpoint groups on page 256](#)
2. Configuring VPN settings:
 - a. [IPsec VPN](#)
 - b. [SSL VPN](#)
3. Verify the configuration in FortiClient:
 - a. [IPsec VPN](#)
 - b. [SSL VPN](#)

Configuring VPN settings

To configure FortiOS IPsec VPN settings:

1. In FortiOS, go to *VPN > IPsec Tunnels*.
2. Click *Create New > IPsec Tunnel*.
3. On the *VPN Setup* tab, for *Template type*, select *Remote Access*.
4. For *Remote device type*, select *Client-based*, then *FortiClient*. Click *Next*.
5. On the *Authentication* tab, for *Authentication method*, select *Pre-shared Key*. Configure the desired preshared key (PSK).
6. Configure other fields as desired, then create the tunnel.
7. Configure policies:
 - a. Go to *Policy & Objects > Firewall Policy*.
 - b. Select the VPN IPS policy. Right-click, then select *Copy*.
 - c. Right-click, then select *Paste > Above*. Repeat to paste two copies of the policy.
 - d. Edit the top pasted policy to allow endpoint and EMS connection:
 - i. For *Destination*, select the EMS destination.
 - ii. For *Service*, set to EMS port 8013.
 - iii. Set the *Action* to *ACCEPT*.
 - iv. Enable, then save the policy.

New Policy	
Name	EMSConnection
Incoming Interface	TeleWork
Outgoing Interface	Fabric (lan4)
Source	TeleWork_range
IP/MAC Based Access Control	
Destination	EMS-ADSRV
Schedule	always
Service	EMSTCP8013
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY
Inspection Mode	Flow-based Proxy-based

- e. Edit the second pasted policy to restrict access to high-risk managed endpoints:
 - i. In the *Source* field, select the tag that you configured to apply to non-compliant endpoints.
 - ii. Set the *Action* to *DENY*.

iii. Enable, then save the policy.

f. Configure the third policy to permit only compliant endpoints to access resources:

- i. In *Source*, select the tag that you configured to apply to compliant endpoints.
- ii. Set the *Action* to *ALLOW*.
- iii. Enable, then save the policy.

8. Ensure that the policies are in the correct sequence and enabled.

14	EMSConnection	TeleWork	Fabric (lan4)	TeleWork_range	EMS-ADSRV	always	EMSTCP8013	✓ ACCEPT	✓ Enabled
15	Deny-HostRisk	TeleWork	Fabric (lan4)	TeleWork_range RED-ALERT	all	always	ALL	✗ DENY	
12	vpn_TeleWork_remote	TeleWork	Fabric (lan4)	TeleWork_range AV-RUNNING	all	always	ALL	✓ ACCEPT	✓ Enabled

To configure FortiOS SSL VPN settings:

1. In FortiOS, go to *VPN > SSL-VPN Settings*.
2. Configure the *Listen on Port* and *HTTPS port* fields as desired.
3. Under *Authentication/Portal Mapping*, select *All Other Users/Groups*, then select the portal from the *Portal* dropdown list.
4. Click the *Apply* button.
5. Configure policies:
 - a. FortiOS displays a message that no SSL VPN policies exist. Select to create a new SSL VPN policy using the newly configured settings:
 - i. From the *Outgoing Interface* dropdown list, select *Internal*.
 - ii. For *Source*, select the desired users.

- iii. For *Destination*, select the EMS server.
- iv. Under *Service*, create a custom service with destination port 8013.
- v. Enable, then save the policy.

The screenshot shows two windows from the FortiClient EMS interface. The 'New Policy' window on the left has the following configuration:

- Name: VPNCorp-EMSAccess
- Incoming Interface: SSL-VPN tunnel interface (ssl.roo)
- Outgoing Interface: Internal
- Source: all, VPNCorp
- Destination: EMSCorp
- Schedule: always
- Service: EMSTCP8013
- Action: ACCEPT (checked), DENY
- Inspection Mode: Flow-based (selected), Proxy-based
- Firewall / Network Options: NAT is disabled, Protocol Options is default.

The 'Edit Service' window on the right has the following configuration:

- Name: EMSTCP8013
- Comments: Write a comment... (0/255)
- Color: Change
- Show in Service List: checked
- Category: Uncategorized
- Protocol Options: Protocol Type is TCP/UDP/SCTP, Address is IP Range 0.0.0.0, Destination Port is TCP 8013 - 8013.
- Specify Source Ports: disabled

- b. Select the SSL VPN policy. Right-click, then select *Copy*.
- c. Right-click, then select *Paste > Below*. Repeat to paste two copies of the policy.
- d. Configure the policies:
 - i. Edit the top pasted policy:
 - i. For *Source*, select the tag that you configured to apply to non-compliant endpoints.
 - ii. For *Destination*, select *all*.
 - iii. For *Service*, select *ALL*.
 - iv. Set the *Action* to *DENY*.
 - v. Enable, then save the policy.

The screenshot shows the 'Edit Policy' window and the 'Select Entries' dialog. The 'Edit Policy' window has the following configuration:

- Name: SSL-DenyHostRisk
- Incoming Interface: SSL-VPN tunnel interface (ssl.roo)
- Outgoing Interface: Internal
- Source: all, RED-ALERT
- Destination: all
- Schedule: always
- Service: ALL
- Action: ACCEPT (checked), DENY (checked)
- Log Violation Traffic: disabled
- Comments: (Copy of VPNCorp-EMSAccess) 28/10/23
- Enable this policy: checked

The 'Select Entries' dialog on the right shows a list of entries with 'RED-ALERT' selected. The list includes:

- USER (1)
- Local (1)
- guest
- USER GROUP (3)
- Guest-group
- SSO_Guest_Users
- VPNCorp
- FSSO GROUP (3)
- CorpEMS (3)
- ADFERANSIWIN
- AV-RUNNING
- RED-ALERT (selected)

- ii. Edit the second pasted policy:
 - i. In the *Source* field, select the tag that you configured to apply to compliant endpoints.
 - ii. For *Destination*, select *all*.
 - iii. For *Service*, select *ALL*.
 - iv. Set the *Action* to *ACCEPT*.
 - v. Enable, then save the policy.

6. Ensure that the policies are sequenced and enabled.

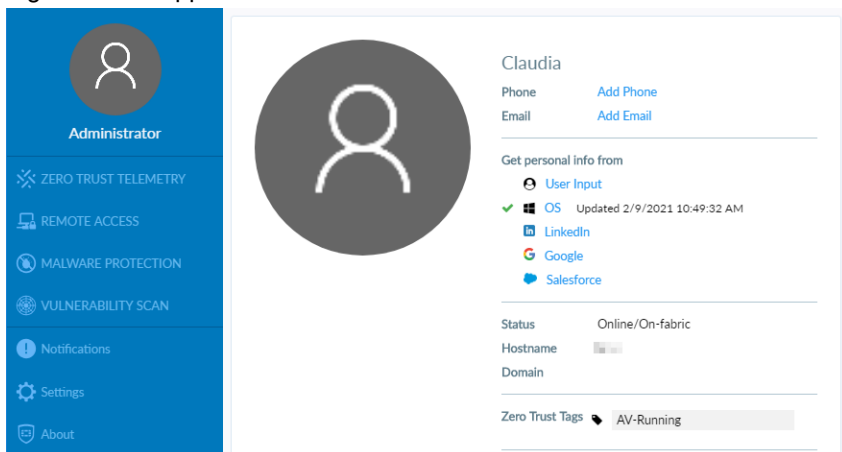
ID	Name	Source	Destination	Schedule	Service	Action	NAT
GuestWiFi (guestwifi) → wan							
2		all	all	always	ALL	✓ ACCEPT	✓ Enabled
Internal → wan							
1		all	all	always	ALL	✓ ACCEPT	✓ Enabled
Internal → wwan							
3		all	all	always	ALL	✓ ACCEPT	✓ Enabled
SSL-VPN tunnel interface (ssl.root) → Internal							
4	VPNCorp-EMSAccess	all VPNCorp	EMSCorp	always	EMSTCP8013	✓ ACCEPT	✗ Disabled
5	SSL-DenyHostRisk	all RED-ALERT	all	always	ALL	✗ DENY	
6	SSL-TeleWorkVPNCorp	all AV-RUNNING	all	always	ALL	✓ ACCEPT	✗ Disabled

Verifying the configuration in FortiClient

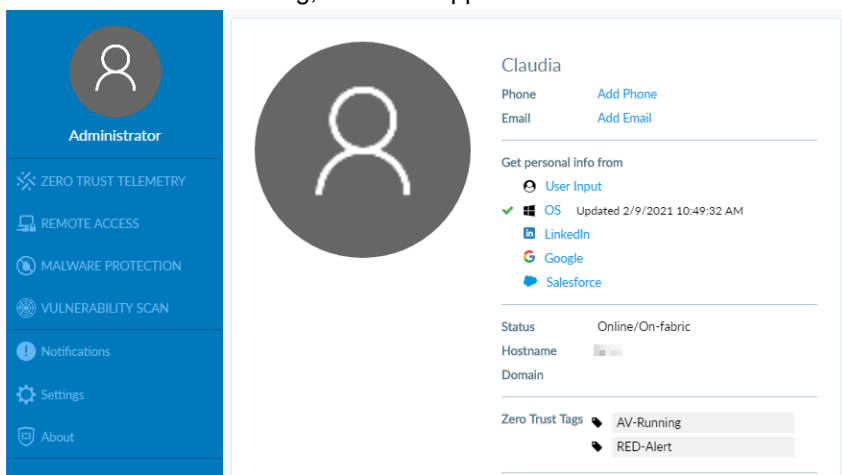
To verify the configuration for IPsec VPN on FortiClient:

1. Install FortiClient on an endpoint and ensure that it is connected to EMS.
2. Configure and connect to an IPsec VPN tunnel.

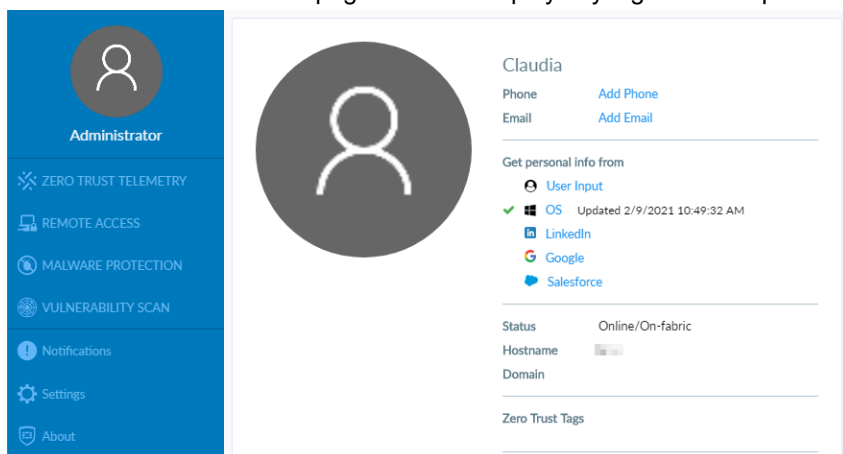
3. Ensure that EMS and FortiOS apply the correct tags and policies for a compliant endpoint:
 - a. On the user details page, ensure that EMS has applied the appropriate tag. In this example, the AV-Running tag should be applied.



- b. Ping a device on the network to ensure that it can be reached.
4. Ensure that EMS and FortiOS apply the correct tags and policies for a non-compliant endpoint:
 - a. Change the endpoint condition so that it becomes non-compliant. In this example, that would be creating the risk.txt file on the endpoint. After a few minutes, the ping becomes denied.
 - b. Go to the user details page to ensure that the appropriate tag has been applied. Both tags, in this example RED-Alert and AV-Running, should be applied.

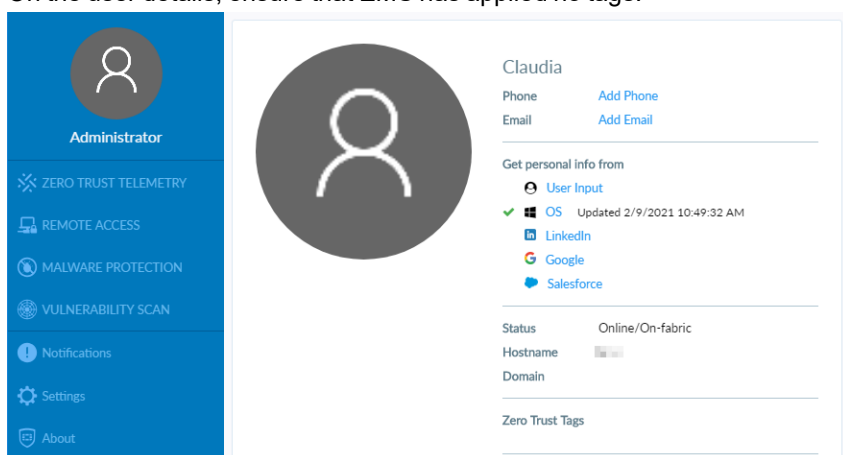


5. Ensure that EMS and FortiOS apply the correct tags and policies for a rogue endpoint:
 - a. Delete the risk.txt file, and stop AV services.
 - b. Ensure that the user details page does not display any tags. The endpoint should lose network access.



To verify the configuration for SSL VPN on FortiClient:

1. Install FortiClient on an endpoint.
2. Configure and connect to an SSL VPN tunnel.
3. Ensure that EMS and FortiOS apply the correct tags and policies for a rogue endpoint:
 - a. Ensure that AV services are not running.
 - b. On the user details, ensure that EMS has applied no tags.










- c. Ping the EMS server. The endpoint should be unable to access internal resources.
 - d. In FortiOS, go to *Monitor > Firewall User Monitor*. Ensure that there is no tag attribute for the user/device.

Refresh

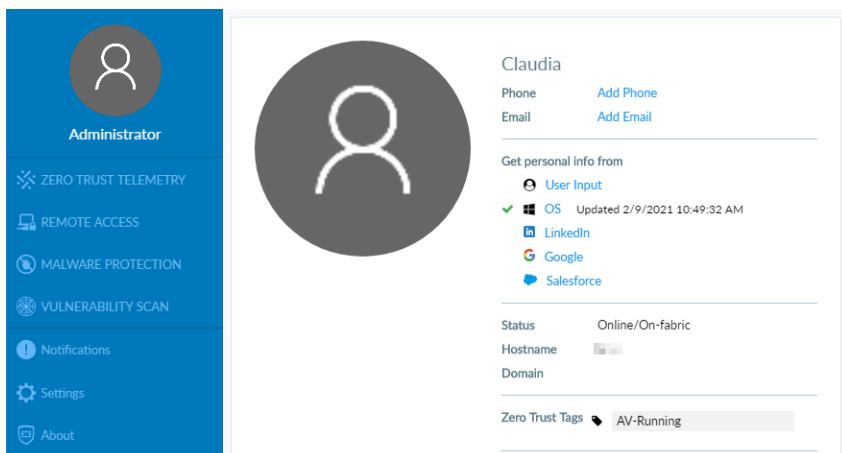
Deauthenticate

Show all FSSO Logons

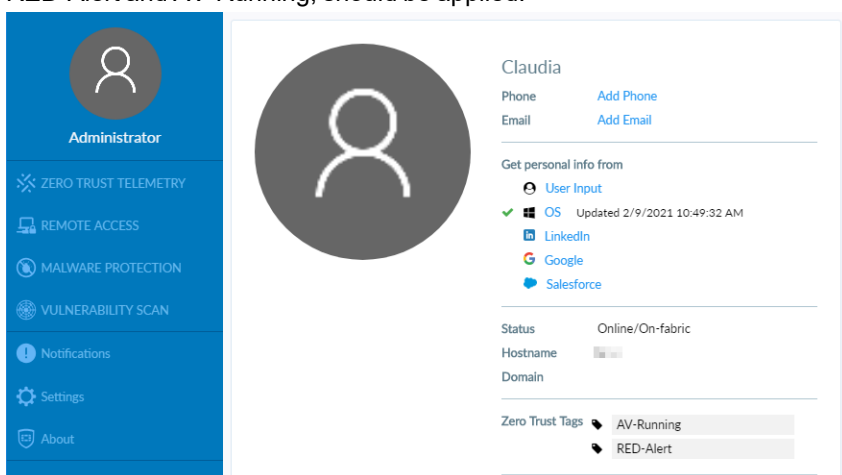
Search

User Name	User Group	Duration	IP Address	Traffic Volume	Method
 CLAUDIA	 AV-RUNNING	1 minute(s) and 21 second(s)	10.6.1.10	0 B	 Fortinet Single Sign-On
 administrator	 VPNCorp	13 minute(s) and 57 second(s)	10.212.134.200	706.87 kB <div><div></div></div>	 Fortinet Single Sign-On  Firewall

4. Ensure that EMS and FortiOS apply the correct tags and policies for a compliant endpoint:
 - a. Ensure that AV services are running.
 - b. Go to the user details page to ensure that the appropriate tag has been applied. In this example, only AV-Running should be applied.



- c. Ping the EMS server again. The endpoint should be able to access internal resources.
5. Ensure that EMS and FortiOS apply the correct tags and policies for a non-compliant endpoint:
 - a. Change the endpoint condition so that it becomes non-compliant. In this example, that would be creating the risk.txt file on the endpoint. After a few minutes, the ping becomes denied.
 - b. Go to the user details page to ensure that the appropriate tag has been applied. Both tags, in this example RED-Alert and AV-Running, should be applied.



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 endpoint groups on page 256](#).

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

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 Zero Trust 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 endpoint groups on page 256](#).

Unlike Zero Trust 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.

FortiGuard Outbreak Alert Rules					Refresh
Name	Tag	Enabled	Type	Comments	
TeamCity reg key Alert	TeamCity reg key Alert	<input checked="" type="checkbox"/>	suspicious		
TeamCity Running Alert	TeamCity Running Alert	<input checked="" type="checkbox"/>	compromised		

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.

FortiGuard Outbreak Alert Rule

Name	TeamCity Running Alert
Tag Endpoint As ⓘ	TeamCity Running Alert
Enabled	<input checked="" type="checkbox"/>
Detection Type	
Comments	

Signatures	
Type	Value
Windows (3)	
File	1 C:\TeamCity\bin\TeamCityService.exe
Running Process	2 TeamCity*.exe
Registry Key	3 Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\JetBrains\TeamCity\Server
Rule Logic	1 or 2 or 3

EMS also receives FortiGuard outbreak alert rules that detect common vulnerabilities and exposures on endpoints. These rules include a description of the vulnerabilities:

FortiGuard Outbreak Detection Rule

Name	MS ProxyShell Vulnerable
Tag Endpoint As ⓘ	MS ProxyShell Vulnerable
Enabled	<input checked="" type="checkbox"/>
Detection Type	suspicious
Comments	These Microsoft Exchange servers are vulnerable and can be exploited for ProxyShell. ProxyShell is an exploit attack chain involving three Microsoft exchange vulnerabilities: CVE-2021-
Signatures	
Type	Value
Windows (1)	
Common Vulnerabilities and Exposures	<div><div>1</div>CVE-2022-24508</div> <div><div>2</div>CVE-2021-34523</div> <div><div>3</div>CVE-2021-31207</div>
Rule Logic	1 or 2 or 3

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 223](#).

This feature requires the EPP license. See [FortiClient EMS on page 21](#).

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.

Name	Vendor	Version	First Detected	Last Installed	Install Count
Amazon SSM Agent	Amazon Web Services	2.2.64.0	2018-11-15	2017-11-29	1
AWS PV Drivers	Amazon Web Services	7.4.6	2018-11-15	2017-08-15	1
AWS Tools for Windows	Amazon Web Services Developer Relations	3.15.244	2018-11-15	2017-11-29	1
aws-cfn-bootstrap	Amazon Web Services	1.4.19	2018-11-15	2017-08-10	1
aws-cfn-bootstrap	Amazon Web Services	1.4.24	2018-11-15	2017-10-12	1
aws-cfn-bootstrap	Amazon Web Services	1.4.17	2018-11-15	2017-03-14	1
aws-cfn-bootstrap	Amazon Web Services	1.4.15	2018-11-15	2016-12-14	1
aws-cfn-bootstrap	Amazon Web Services	1.4.21	2018-11-15	2017-09-13	1
Bonjour	Apple Inc.	3.0.0.10	2018-11-15	2018-10-25	1
EC2ConfigService	Amazon Web Services	4.9.2218.0	2018-11-15	2017-11-29	1
FortiClient	Fortinet Technologies Inc.	6.2.0.0705	2018-11-15	2018-11-07	1

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.
Display by	Select to toggle between the following options: <ul style="list-style-type: none"> • 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.

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.

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.

Host	User	OS	IP	Application Count	Last Installation
WIN-1F3BOCJBRAM	Administrator	Microsoft Windows Server 2012 R2 Standard	10.0.4.102	17	2018-11-07

Name	Vendor	Version	Install Date
Amazon SSM Agent	Amazon Web Services	2.2.64.0	2017-11-29
AWS PV Drivers	Amazon Web Services	7.4.6	2017-08-15
AWS Tools for Windows	Amazon Web Services Developer Relations	3.15.244	2017-11-29
aws-cfn-bootstrap	Amazon Web Services	1.4.19	2017-08-10
aws-cfn-bootstrap	Amazon Web Services	1.4.24	2017-10-12
aws-cfn-bootstrap	Amazon Web Services	1.4.17	2017-03-14
aws-cfn-bootstrap	Amazon Web Services	1.4.15	2016-12-14
aws-cfn-bootstrap	Amazon Web Services	1.4.21	2017-09-13
Bonjour	Apple Inc.	3.0.0.10	2018-10-25

17 applications loaded

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 269 .
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 270](#) 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. The FortiClient EMS administrator can view quarantined file information for all managed endpoints on the *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: <ul style="list-style-type: none">• 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 <i>Enter</i> 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: <ul style="list-style-type: none"> • Scheduled Scan • Email Scan • Startup Scan • Manual Scan • Realtime Scan • Rootkit Manual Scan • Sandbox Scan
Status	Status of the file: <i>Quarantined</i> , <i>Quarantined & Allowlisted</i> , <i>Restored</i> , or <i>Deleted</i> . 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 status(es) 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

Administrators

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 > Administrators*. The following information displays:

Add	Add a new user.
Refresh	Refresh the list of users.
Name	The username.
Source	Type of user: <ul style="list-style-type: none">• 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 279 .
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 278 .
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. If you want 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 > Administrators*.
2. Click the *Add* button.
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 283](#).
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 279 .
Domain Access	Select or add access to a domain for the user. If desired, enable <i>Allow all domains</i> 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 <i>Trusted Hosts</i> 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 296](#).

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 > Administrators*. EMS shows the deactivated user with a lock icon beside their name. The *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.

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 <i>Administration</i> 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 280](#).
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 278 .
Manage Google domains*	Manage connections to Google domains to decide which Chromebooks to manage. See Google Domains on page 115 .
Manage custom groups	Create, rename, and edit groups to manage endpoints. See Managing groups on page 88 .

Permission	Link to description
Run commands on endpoints	Perform actions to endpoints on the <i>Endpoints</i> pane, including uploading FortiClient logs, requesting diagnostic results, and so on. See Managing endpoints on page 104 .
Block/Unblock/Quarantine/Unquarantine/Reregister endpoints	Manage endpoint access to the network through blocking, quarantine, and registration. See Managing endpoints on page 104 .
Manage and assign endpoint policies	See Endpoint Policy & Components on page 127 .
View group assignment rules	View group assignment rules. See Group assignment rules on page 111 .
Manage group assignment rules	Create, delete, and edit group assignment rules. See Group assignment rules on page 111 .
View endpoint filter bookmarks	View endpoint filter bookmarks. See Using bookmarks to filter the list of endpoints on page 101 .
Manage endpoint filter bookmarks	Create, delete, and edit endpoint filter bookmarks. See Using bookmarks to filter the list of endpoints on page 101 .
View quarantine management	View lists of quarantined and allowlisted files. See Quarantine Management on page 272 .
Manage quarantine management	Allowlist and restore quarantined files and remove files from the allowlist. See Quarantine Management on page 272 .
View software inventory	See Software Inventory on page 269 .
Manage software inventory	See Software Inventory on page 269 .

Policy permissions

Permission	Link to description
View endpoint policies*	View endpoint policies. See Endpoint Policy & Components on page 127 .
View endpoint profiles*	View endpoint profiles. See Endpoint Profiles on page 140 .
Manage endpoint profiles*	Create, delete, and edit endpoint profiles. See Endpoint Profiles on page 140 .
View Zero Trust tagging rules	View Zero Trust tagging rules. See Zero Trust Tagging Rules on page 246 .
Manage Zero Trust tagging rules	Create, delete, and edit Zero Trust tagging rules. See Zero Trust Tagging Rules on page 246 .

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 122.
Manage installers	Create, delete, and edit installers. See FortiClient Installer on page 122.
View CA certificates	View CA certificates. See CA Certificates on page 133.
Manage CA certificates	Upload, import, and delete CA certificates. See CA Certificates on page 133.
View on-fabric detection rules	View on-fabric detection rules. See On-fabric Detection Rules on page 135.
Manage on-fabric detection rules	Create, delete, and edit on-fabric detection rules. See On-fabric Detection Rules on page 135.

Setting permissions

Permission	Link to description
View server settings*	View <i>Server</i> settings. See Configuring EMS settings on page 329
Manage server settings*	Modify <i>Server</i> settings. See Configuring EMS settings on page 329.
View Fortinet services settings	View <i>FortiGuard Services</i> settings. See Configuring FortiGuard Services settings on page 336.
Manage Fortinet services settings	Modify <i>FortiGuard Services</i> settings. See Configuring FortiGuard Services settings on page 336.
View endpoint settings	View <i>Endpoints</i> settings. See Configuring EMS settings on page 329.
Manage endpoint settings	Modify <i>Endpoints</i> settings. See Configuring EMS settings on page 329.

Permission	Link to description
View login banner settings*	View login banner settings. See Configuring EMS settings on page 329 .
Manage login banner settings*	Modify login banner settings. See Configuring EMS settings on page 329 .
View alert settings*	View <i>Alerts</i> settings. See Alerts on page 340 .
Manage alert settings*	Modify <i>Alerts</i> settings. See Alerts on page 340 .
View custom message settings	View endpoint quarantine message settings. See Customizing the endpoint quarantine message on page 344 .
Manage custom message settings	Modify endpoint quarantine message settings. See Customizing the endpoint quarantine message on page 344 .
View feature select settings	View feature select settings. See Feature Select on page 346 .
Manage feature select settings	Modify feature select settings. See Feature Select on page 346 .

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.

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 > ADDS*.
3. Configure the following options:

IP address/Hostname	Enter the domain server IP address or hostname.
Port	Enter the port number.
Username	Available when <i>Bind type</i> is set to <i>Regular</i> . Enter the username.
Password	Available when <i>Bind type</i> is set to <i>Regular</i> . Enter the user password.
Show Password	Available when <i>Bind type</i> is set to <i>Regular</i> . Turn on and off to show or hide the password.
LDAPS connection	Enable a secure connection protocol when <i>Bind Type</i> is set to <i>Regular</i> .
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 <i>LDAPS connection</i> is enabled.
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 291 .
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 88](#).

Adding an Azure AD server

You can integrate Azure Active Directory (AD) with on-premise EMS and FortiClient Cloud.

To create an enterprise application for FortiClient:

1. In the Azure portal, go to *Azure Active Directory > 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:
 - Application Access API
 - Application.ReadWrite.OwnedBy
 - Directory.ReadWrite.All
 - Domain.ReadWrite.All
 - Group.ReadWrite.All
 - User.ReadWrite.All
 - Delegate Access API
 - Directory.ReadWrite.All
 - User.ReadWrite.All
 - User.Read
 - Directory.AccessAsUser.All
 - Other API Permission
 - Application
 - AdministrativeUnit.ReadWrite.All
 - DelegatedPermissionGrant.ReadWrite.All
 - Device.ReadWrite.All
 - User.ManageIdentities.All
 - Delegate
 - User.ReadBasic.All
7. Click *Add permissions*.
8. In the *API permissions* page, 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:

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 configure an Azure AD server in EMS:


1. Configure the Azure AD server as an authentication server in EMS:
 - a. In the Azure management console, collect your AD 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*.

Authentication Server




Azure Active Directory

Tenant ID

5d96077d-28ef-405b-

Client ID


62314a93-d553-4185-

Authorization Type

Client Secret

Certificate

Client Secret

.....

Alias

Optional

Comment

Optional

Test

Cancel

- i. 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**.

Domain Import View Azure Group Import Tutorial

Azure Server: onmicrosoft.com

Sync every: 60 Minutes
⚠ The minimum sync period is 60 minutes

Group Selection Behaviour: Import Entire Azure Domain Import Selected Azure Groups
ⓘ Only the selected Azure users, groups and devices will be imported

Group Name	Source	Import as Base Group
_Group	Azure	<input type="checkbox"/>
DnsAdmins	On Prem	<input type="checkbox"/>
ADSyncPasswordSet	On Prem	<input type="checkbox"/>
group	Azure	<input checked="" type="checkbox"/>
DnsUpdateProxy	On Prem	<input type="checkbox"/>
group2	Azure	<input type="checkbox"/>
ADSyncBrowse	On Prem	<input type="checkbox"/>
R&D_NA	On Prem	<input type="checkbox"/>
ADSyncAdmins	On Prem	<input type="checkbox"/>
group	Azure	<input checked="" type="checkbox"/>

Changes to Base Group Revert Changes

Status	Group
+ Will be Added	group

Save **Cancel**

Endpoints > Domains lists the Azure AD 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, Azure AD users can register their FortiClient to EMS using an invitation code or with SAML.

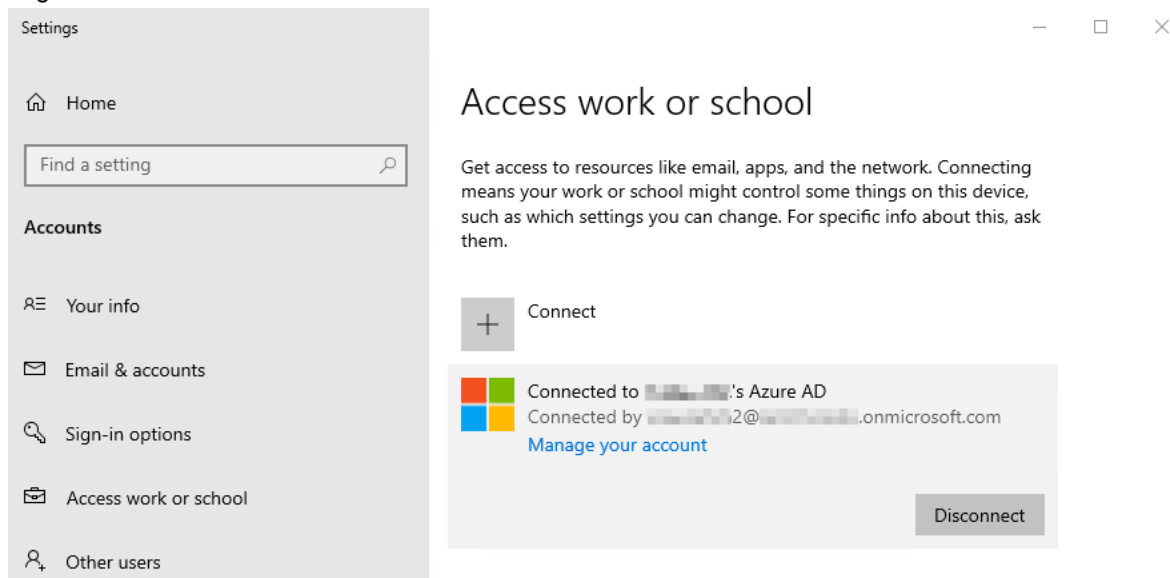
To configure the Azure tenant app for initiating passthrough (domain):

This is necessary for registering an Azure AD endpoint to EMS using an invitation code. This only applies for Azure AD-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 Azure AD:
 - 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 register an Azure AD 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 Azure AD 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 Azure AD user.



9. In FortiClient, on the *Zero Trust Telemetry* tab, enter the invitation code to register to EMS. FortiClient registers to EMS as the logged in Azure AD user without additional prompts.

To register an Azure AD 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 Azure AD server.
 - e. In this configuration, EMS acts as the service provider, while the Azure AD 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 Azure AD SAML Toolkit:
 - a. Go to *Enterprise applications*, then click *New application*.
 - b. Search for and select *Azure AD 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 Azure AD. Configure as the table summarizes, then click *Save*.

EMS SAML field	Azure AD 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

- 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.localprincipalname*. 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 *Azure AD 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.

Identity Provider Settings

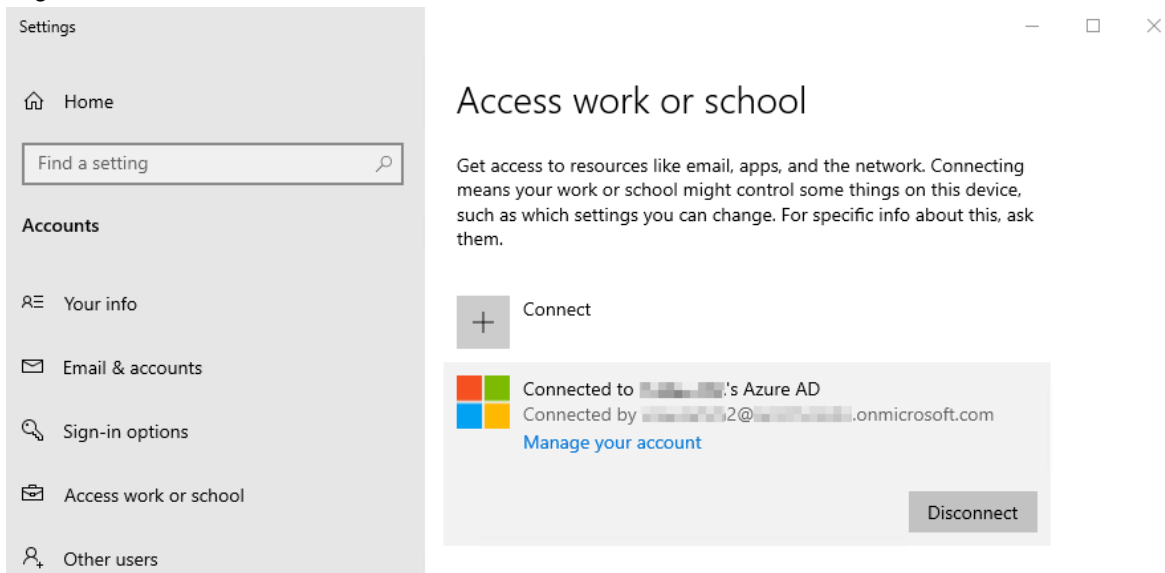
IdP Entity ID ⓘ

IdP single sign-on URL ⓘ

IdP Certificate 2025-12-21

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*.

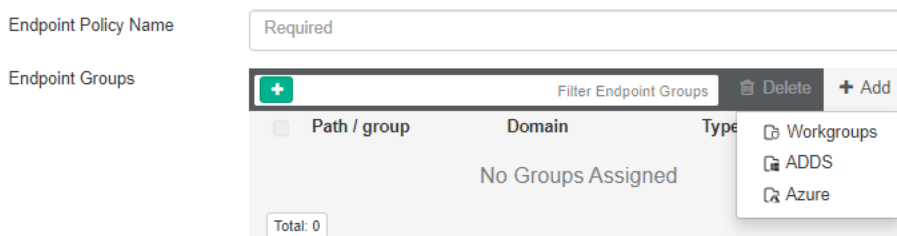
- d. From the *SAML Config* dropdown list, select the SAML configuration.
- e. Configure other settings as desired, then click **Save**.
- 7. You can authenticate the endpoint using Azure AD by doing one of the following:
 - a. To join the device to the Azure AD server, do the following:
 - i. On the endpoint, go to *Settings > Accounts*.
 - ii. Under *Access work or school*, click **Connect**.
 - iii. Log in as an Azure AD user.



- iv. In FortiClient, on the *Zero Trust Telemetry* tab, enter the invitation code to register to EMS. FortiClient registers to EMS as the logged in Azure AD 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 Azure AD user credentials to authenticate and connect FortiClient to EMS.

The EMS administrator can configure endpoint policies and deployment configurations for specific endpoint groups from an Azure AD server.

Endpoint Policy




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 291](#).

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*.

Connector API Keys			+ Add	Refresh
Alias	Key	Create Date		
AD_Connector_API-Key	 DC423532-797C-4649-ABDD-7542687764F8	2022-12-09 12:26:42		

Showing: 1

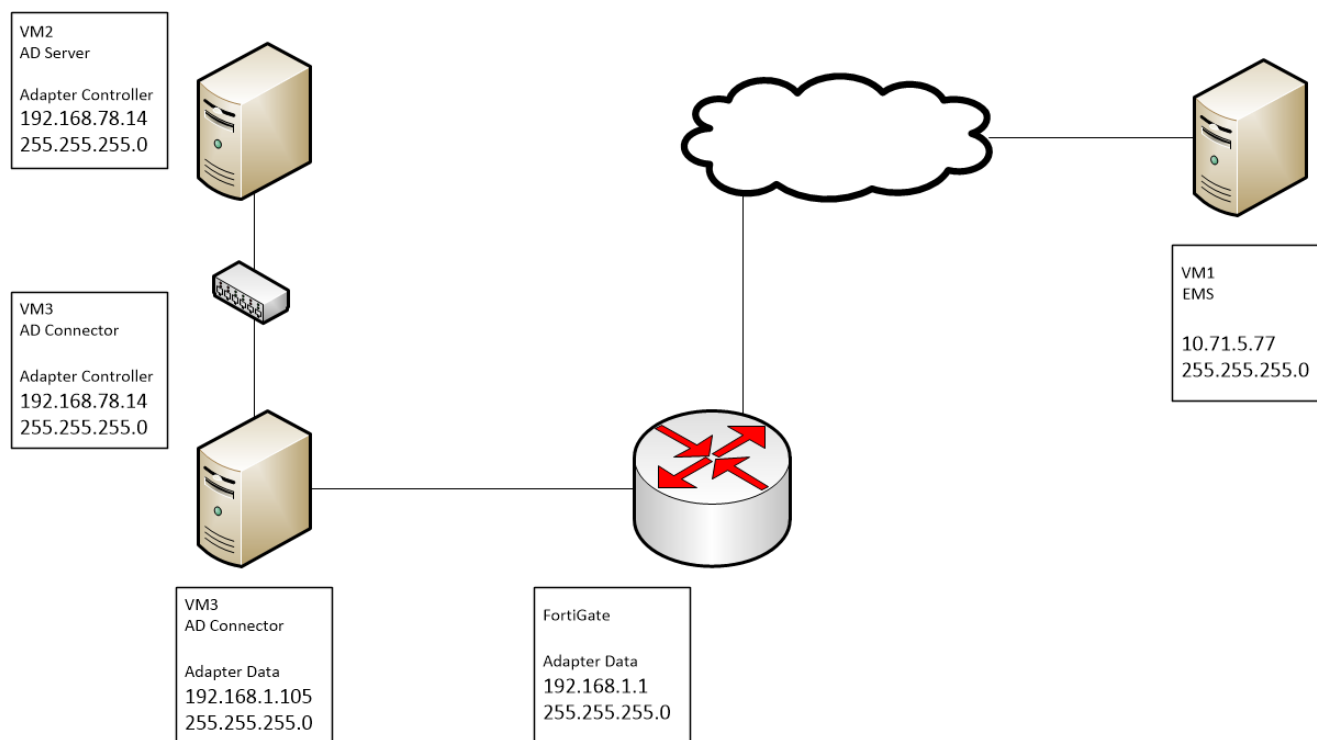
Close

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 192.168.178.14/24. 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 controller	192.168.78.14
Adapter data	192.168.1.1/24

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.

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.

Connector API Keys			+ Add	Refresh
Alias	Key	Create Date		
AD_Connector_API-Key	 DC423532-797C-4649-ABDD-7542687764F8	2022-12-09 12:26:42		

Showing: 1

Close

2. Create the AD connector:
- 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_7.2.0.XXXX_x64.msi`.
 - 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.
 - In the *EMS Port* field, enter the port number.
 - In the *Connector UID* field, enter the AD connector UID.
 - In the *Connector Api Key* field, enter the API key value.
 - Click *Add Site*, and enter the EMS site information. Ensure that a *Connection established* message displays,

then click *Next*.

Connect to EMS Configuration

Configure parameters to connect to EMS. If multiple EMS sites are required, please add each site separately. For EMS Cloud, please enter your Account ID into the EMS IP/FQDN/Account ID field

EMS IP/FQDN/Account ID: 1431398 EMS Port: 8871

Connector UID: ems104-AD-Connector

EMS Site: default Connector Api Key: 5B57-FA5B-4280-ABB9-6FB6C18BBCAA

Use Global Site: ☐ Global Site API Key:

Add Site

Configured EMS Sites

Remove Site

Please Add at least one EMS connection before proceeding

Back Next Cancel

3. Go to *Administration > Authentication Servers > Connectors* to confirm that you successfully created an AD connector.
4. Go to *Administration > Authentication Servers*.
5. Enable *Use Connector*.
6. From the *Connector* dropdown list, select the AD connector.

7. Save the configuration. EMS successfully adds the AD server as an authentication server.

✓ Success

Authentication Server



Active Directory

IP address/Hostname

ems104.com

Port

389

Username

administrator

Password

.....



LDAPS connection



Alias

Optional

Comment

Optional

Use Connector



Connector

● ems104-AD-Connector ▼

Save

Cancel

Configuring Admin User Settings

To configure Admin User Settings:

1. Go to *Administration > Admin User Settings*.
2. Set the following options:

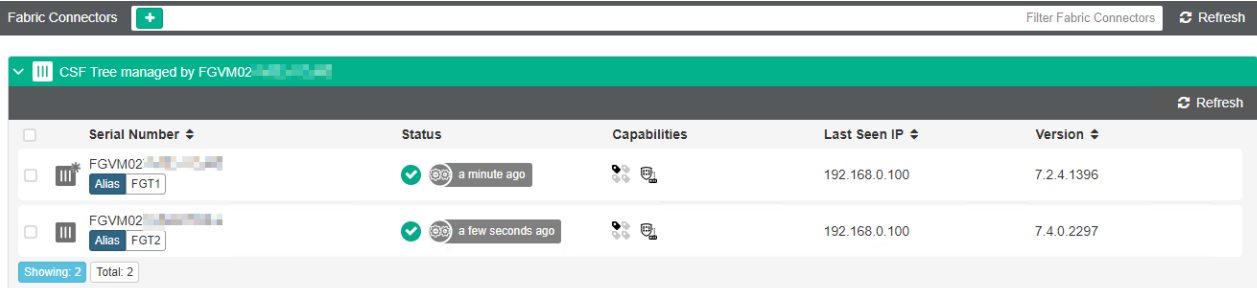
Inactivity timeout	Specify how long to keep inactive users logged into FortiClient EMS. When the time expires, EMS automatically logs the user out. Enter 0 to keep inactive users logged into FortiClient EMS indefinitely.
Allowed inactive days	Specify the number of days of inactivity after which to disable 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 278 .
Maximum password age	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 EMS users.

3. Click **Save**.

Fabric Devices

You can view all FortiGates that the EMS has authorized in *Administration > 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 the *Fabric Devices* page showing two FortiGates that are part of a CSF tree:



Serial Number	Status	Capabilities	Last Seen IP	Version
FGVM02 Alias: FGT1	Online a minute ago	...	192.168.0.100	7.2.4.1396
FGVM02 Alias: FGT2	Online a few seconds ago	...	192.168.0.100	7.4.0.2297

Showing: 2 Total: 2

The following shows the *Fabric Devices* page showing two FortiGates that are part of an HA cluster:

Fabric Connectors +				
Filter Fabric Connectors Refresh				
<div> <div>CSF Tree managed by FGVMUL</div> <div>HA cluster managed by FGVMUL</div> </div>				
Refresh				
<input type="checkbox"/> Serial Number	Status	Capabilities	Last Seen IP	Version
<input type="checkbox"/> FGVMUL	✓ an hour ago		172.16.199.183	7.4.0.2297
<input type="checkbox"/> FGVMUL	✓ N/A			7.4.0.2297
<input type="checkbox"/> FGVMUL	✓ N/A			7.4.0.2297
Showing: 3 Total: 3				

FortiOS versions 7.0.2 to 7.0.6 only support zero trust 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 *Administration > 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	The 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)	This is the default setting. The 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: <ul style="list-style-type: none"> • 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. *Zero Trust Tags* is selected by default and cannot be deselected. EMS only shares the selected tag types with the configured Fabric devices.

Tag	Description
Zero Trust tags	See Zero Trust Tags on page 246 .
FortiGuard outbreak alert tags	See FortiGuard Outbreak Alerts on page 267 .
Classification tags	See Viewing the Endpoints pane on page 91 .
Fabric tags	Fabric tags require connection to FortiAnalyzer. See the following process: <ol style="list-style-type: none"> 1. EMS administrator configures FortiAnalyzer in a System Settings profile. See System Settings on page 223. 2. FortiClient connects to EMS and receives FortiAnalyzer connection

Tag	Description
	<p>information from the profile.</p> <ol style="list-style-type: none"> 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 <i>Zero Trust Tag Monitor</i>. This tag displays as a Fortinet Security Fabric tag in <i>Zero Trust Tag Monitor</i>, but the tag displays under <i>Classification Tags</i> in endpoint details. See Viewing the Endpoints pane on page 91. 7. If FortiGate is configured to receive all tags for this specific endpoint, EMS sends the tag to FortiGate. <p>See EMS API support for FortiAnalyzer to notify and tag suspicious endpoints.</p>

5. Click **Save**.

To change the FortiGate authorization status:

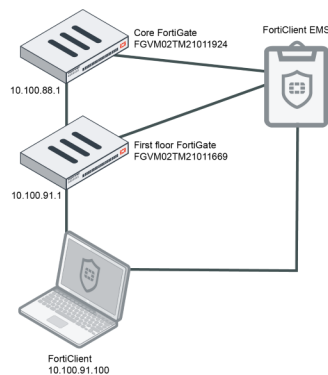
1. Go to *Administration > Fabric Devices*.
2. Select the desired FortiGate.
3. Click *Deny* or *Authorize*. The FortiGate status in the *Authorized* column changes.

Configuring EMS to share tagging information with multiple FortiGates

When an endpoint has a Zero Trust 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:

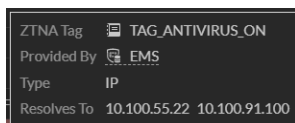
- Both FortiGates are connected to EMS as part of a Security Fabric.
- FortiClient is registered to EMS.
- The FortiClient gateway points to the first floor FortiGate.
- The FortiClient endpoint has the TAG_ANTIVIRUS_ON Zero Trust tag applied.
- The host tag of the FortiClient endpoint with TAG_ANTIVIRUS_ON 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 *Administration > 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
```

+ Create New Edit Delete Switch Management <input type="text"/> <input type="button" value="Q"/>										
Name	Management VDOM	Type	NGFW Mode	Operation Mode	Status	CPU	Memory	Interfaces	Comments	Ref.
root		Traffic	Profile-based	NAT	Enabled	18%	26%	VPN (port1) REMOTE_LAN (port2) port3 NAT interface (naf.root)		22
site1		Traffic	Profile-based	NAT	Enabled	0%	3%	NAT interface (naf.site1) l2site1 SSL-VPN tunnel interface (ssl.site1)		4

- In EMS, enable multitenancy. Create a new multitenancy site.
- 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 *Administration > 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
```

Fabric Connectors +					Filter Fabric Connectors	Refresh
Standalone devices Refresh						
<input type="checkbox"/>	Serial Number	Status	Capabilities	Last Seen IP	Version	
<input type="checkbox"/>	FGV02 - root	2 minutes ago		192.168.0.100	7.4.0.2297	
Showing: 1 Total: 1						

- 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 *Administration > 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
```

Fabric Connectors +					Filter Fabric Connectors	Refresh
Standalone devices Refresh						
<input type="checkbox"/>	Serial Number	Status	Capabilities	Last Seen IP	Version	
<input type="checkbox"/>	FGV02 - site1	5 minutes ago		192.168.0.111	7.4.0.2297	
Showing: 1 Total: 1						

5. Tagging information from an EMS site is only shared with the FortiGate VDOM that the EMS site has established a Fabric connection with. In this example, the `ems_connected_default` site is a tag configured on the EMS default site.

ZTNA ServersZTNA Tags

+ Create New Group

Edit

Delete

Search

`ems_connected_site1` is a tag configured on the EMS non-default site.

ZTNA ServersZTNA Tags

+ Create New Group

Edit

Delete

Search

	Name	Provided By	Details	Type	Category	Detection Level	Comments	Ref.
ZTNA IP	all_registered_clients	EMS1		ZTNA IP Tag	Zero Trust			0
ZTNA IP	ems_connected_site1	EMS1		ZTNA IP Tag	Zero Trust			0
LOCAL TAG	EMS_ALL_UNKNOWN_CLIENTS			ZTNA IP Tag				0
LOCAL TAG	EMS_ALL_UNMANAGEABLE_CLIENTS			ZTNA IP Tag				0
LOCAL TAG	FCTEMS_ALL_FORTICLOUD_SERVERS			ZTNA IP Tag				0
ZTNA MAC	all_registered_clients	EMS1		ZTNA MAC Tag	Zero Trust			0
ZTNA MAC	ems_connected_site1	EMS1		ZTNA MAC Tag	Zero Trust			0

You can hover over the FortiGate in EMS and select *Edit* to update tag and FortiClient endpoint sharing information. You can also configure an alias for easier FortiGate identification. EMS shows one of the following authorization states for the Fabric connection: authorized, deauthorized, or pending.

Fabric Connectors

+

Filter Fabric Connectors

Refresh

Standalone devices

Refresh

<input type="checkbox"/>	Serial Number	Status	Capabilities	Last Seen IP	Version
<input type="checkbox"/>	<div><div></div><div>FGVM01</div></div>	<div><div>✓</div><div>a few seconds ago</div></div>	<div><div></div><div></div></div>	172.17.80.152	
<input type="checkbox"/>	<div><div></div><div>FGVM02</div></div>	<div><div>✗</div><div>a few seconds ago</div></div>	<div><div></div><div></div></div>	172.17.61.18	
<input type="checkbox"/>	<div><div></div><div>FGVM02</div></div>	<div><div>⚙</div><div>9 minutes ago</div></div>	<div><div></div><div></div></div>	192.168.0.100	

Showing 3

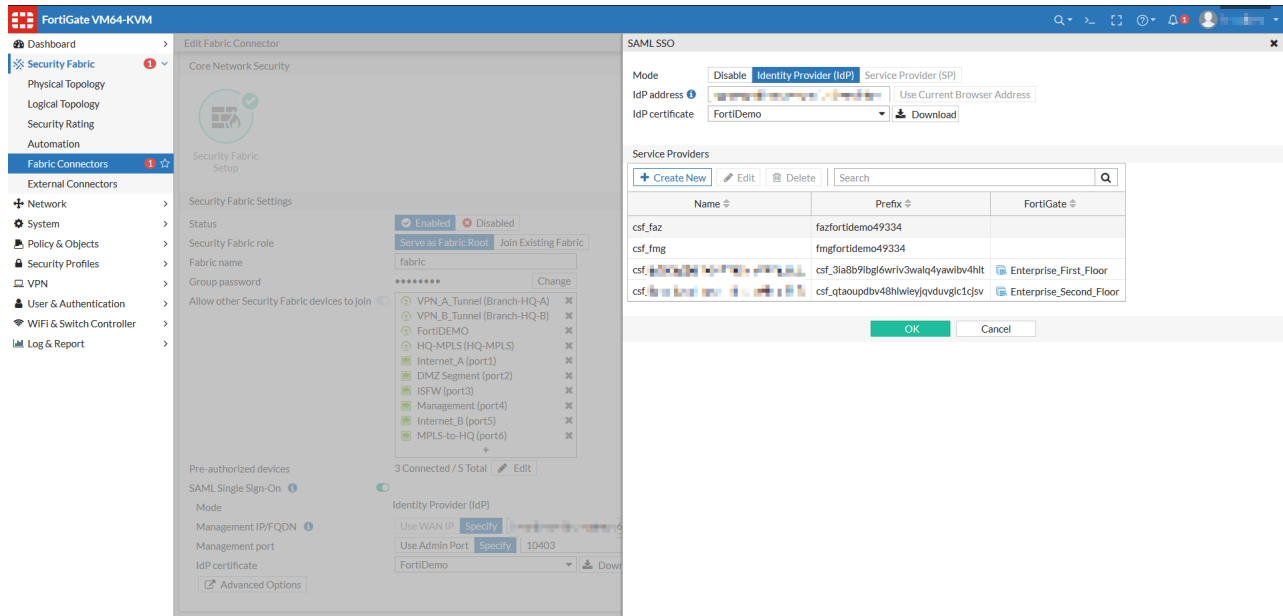
Total: 3

SAML SSO

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. See [Configuring single-sign-on in the Security Fabric](#). Ensure that you download the IdP certificate and copy the SP prefix to use when configuring SAML SSO on EMS.



2. In EMS, go to *System Settings > SAML SSO*.
3. Click *Enable SAML SSO*.
4. Configure *Service Provider Settings*. In this configuration, EMS is the Service Provider (SP):

Setting	Description
SP Address	Enter the EMS IP address. You can also click the <i>Use Current Browser Address</i> button to autopopulate the field. Your browser must be able to access this IP address.
SP Certificate	Click <i>Upload new certificate</i> 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.

5. Configure *Identity Provider Settings*. In this configuration, the FortiGate is the IdP:

Setting	Description
IdP Address	Enter the FortiGate IP address. Your browser must be able to access this IP address.
Prefix	Enter the prefix generated in FortiOS for the SP.
IdP Certificate	Click <i>Upload new certificate</i> to upload the IdP certificate.

Setting	Description
	Upload the same certificate that you configured for the IdP (the FortiGate) in FortiOS in step 1.

The screenshot shows the 'SAML SSO' configuration page in the FortiClient Endpoint Management Server. The left sidebar contains a navigation menu with options like Dashboard, Endpoints, Quarantine Management, Software Inventory, Endpoint Policy, Endpoint Profiles, Manage Installers, Policy Components, Telemetry Gateway Lists, Compliance Verification, Administration, System Settings (selected), Server, Logs, Fortinet Services, and Endpoints. The main content area is titled 'SAML SSO' and includes a toggle for 'Enable SAML SSO' which is checked. Below this, there are two sections: 'Service Provider Settings' and 'Identity Provider Settings'. The Service Provider settings include 'SP Address' (10.0.4.103) and 'SP Certificate' (No certificate imported). The Identity Provider settings include 'IDP Address' (10.0.4.104), 'Prefix' (csf_3la8b9tbg16wriv3walq4yawibv4hit), and 'IDP Certificate' (Fortinet_CA_SSL.cer, 2029-05-21). A 'Save' button is located at the bottom of the configuration area.

6. Click **Save**.
7. 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 329](#).

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.

Licenses

See [Licensing FortiClient EMS on page 43](#).

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, SQL Server 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 database: on page 72](#).
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 <i>User Management > Local Users</i> to connect to EMS. You must create a local user to configure this option. See Local users on page 309 .
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 89 .
SAML	End user must provide their credentials for an SAML identity provider, such as Azure Active Directory (AD), to connect to EMS. You must configure SAML settings to configure this option. See SAML Configuration on page 309 .

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 306](#).
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 310](#).
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 22](#).

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 <i>Authorized</i> or <i>Excluded</i> . 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.

Verified Users										Refresh	Clear Filters
<input type="checkbox"/>	User	Invitation	Domain	SAML	Device Count	Email/Phone	Last Seen	User Type	Status		
<input type="checkbox"/>	 bwolowitz@em...	SAML_Okta		SAML_None_Okta	<div>verified: 0</div> total: 1		2022-05-11 16:52:55	SAML	Managed		
<div>⌂ ⌕</div>											

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 Azure Active Directory (AD). This allows end users to connect to FortiClient EMS and authenticate using their relevant credentials, such as to Azure AD.

To add a SAML configuration:

1. In EMS, go to *User Management > SAML Configuration*.
2. In the *Name* field, enter the desired name for this configuration.
3. For *Authorization Type*, do one of the following:
 - a. Select *LDAP* to associate a domain with this SAML configuration. From the *Domain* dropdown list, select the desired domain.
 - b. Select *None* to not associate a domain with this SAML configuration. This is only recommended for non-domain endpoints.
4. Configure *Service Provider Settings*. EMS is the service provider (SP):

Setting	Description
SP Address	Enter the EMS IP address. You can also click the <i>Use Current URL</i> 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 <i>Generate</i> button.
SP ACS (login) URL	Enter the SP login URL.
SP Entity ID	Enter the SP entity ID.
SP Certificate	Click <i>Upload new certificate</i> 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.

5. 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 <i>Upload new certificate</i> to upload the IdP certificate. Upload the same certificate that you configured in the IdP.

6. Click *Save*.

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:
 - a. To create a new invitation code, click *Add*.
 - b. To edit an existing invitation code, select the desired invitation code. Click *Edit*.
3. Configure the invitation:
 - a. From the *EMS Listen Address*, 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 342](#).
 - 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 deployment package on page 123](#).
 - 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 <i>User Management > Local Users</i> to connect to EMS. You must create a local user to configure this option. See Local users on page 309 .
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 89 .
SAML	End user must provide their credentials for an SAML identity provider, such as Azure Active Directory, to connect to EMS. You must configure SAML settings to configure this option. See SAML Configuration on page 309 .

- 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.

Add Refresh								
Domain Name	Devices	Users	Last Sync	Sync Every	Address	Distinguished Name	Username	LDAPS
qatest0824.local	9	4	2022-06-07 12:12:22	60 minutes	172.17.162.18:389	dc=qatest0824,dc=local	administrator	🔴

- 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	<input type="text" value="SAML-FAC"/>		
Authorization Type	<div><div>LDAP</div><div>None</div></div> <p><small>⚠ 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.</small></p>		
Domain	<div><input type="text" value="qatest0824.local"/></div>		
Service Provider Settings			
SP Address	<input type="text" value="fctems.schoolzones.ca"/>	<div>Use Current URL</div>	
Prefix	<input type="text" value="kkdgn7e5sp"/>	<div>Generate</div>	
SP ACS (login) URL	<input type="text" value="https://fctems.schoolzones.ca/fct_saml/kkdgn7e5sp/acs"/>	<div>Copy</div>	
SP Entity ID	<input type="text" value="https://fctems.schoolzones.ca/fct_saml/kkdgn7e5sp/metadata/"/>	<div>Copy</div>	
SP Certificate	No certificate imported		<div><div>📄</div><div>✕</div></div>
Identity Provider Settings			
IdP single sign-on URL ⓘ	<input type="text" value="https://fac0824.qatest.local:443/saml-idp/04eh9npr3m0ezc7b/login/"/>		
IdP Entity ID ⓘ	<input type="text" value="http://fac0824.qatest.local:443/saml-idp/04eh9npr3m0ezc7b/metadata/"/>		
IdP Certificate	<div><div>📄</div> Default-Server-Certificate.cer <div>2022-12-08</div></div>		<div><div>📄</div><div>✕</div></div>
<div><div>Save</div><div>Cancel</div></div>			

- e. In FortiAuthenticator, configure EMS as an SP.

Edit SAML Service Provider

IdP address: fac0824.qatest.local:443
SP name:
IdP prefix:  
IdP entity id: 
IdP single sign-on URL: 
IdP single logout URL: 
Server certificate: 
IdP signing algorithm: 
☐ Support IdP-initiated assertion response
☐ Participate in single logout



SP Metadata

SP entity ID:
SP ACS (login) URL:
SP SLS (logout) URL:
☐ SAML request must be signed by SP

Authentication

Authentication method: ☐ Mandatory password and OTP
☒ All configured password and OTP factors
☐ Password-only
☐ OTP-only
☐ FIDO-only
☐ Adaptive Authentication
Application name for FTM push notification:
☐ Use FIDO-only authentication if requested by the SP






Assertion Attribute Configuration

Subject NameID: 
Format: 
☐ Include realm name in subject NameID

+ Assertion Attributes

- f. In EMS, go to *User Management > Invitations*. 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*.

Add a New Invitation



Name	<input type="text" value="SAML-FAC-LDAP"/>		
EMS Listen Address	<input type="text" value="fctems.schoolzones.ca:8013"/>		
Type	<div><div>Individual</div><div>Bulk</div></div>		
Send Email Notifications	<input checked="" type="checkbox"/>		
Email Recipients	<div><input type="text" value="redacted_email@schoolzones.ca"/>  </div>		
Include FortiClient Installer	<div>No installer attached.  </div>		
Expiring	<input type="checkbox"/>		
Verification Type	<div><div>None</div><div>Local</div><div>LDAP</div><div>SAML</div></div> <p><small>⚠ To create a SAML configuration, please navigate to User Management -> SAML Configuration.</small></p>		
SAML Config	<input type="text" value="SAML-FAC"/>		
Comments	<div><input type="text" value="Optional"/> </div>		

Save




Cancel

- g. Go to *System Settings > EMS Settings*. Enable *Enforce User Verification*. This forces FortiClient to register to EMS using user onboarding.

EMS Settings


EMS CA certificate (ZTNA)	 default_ZTNARootCA.pem 2047-05-28	
Certificate was created on 2022-06-03T23:14:31.650.		
Reset Stalled Deployment Interval	<input type="text" value="12"/>	hours









EMS Settings

Listen on port	<input type="text" value="8013"/>	
FortiOS Connector port	<input type="text" value="8015"/>	
Enable TLS 1.0/1.1	<input type="checkbox"/>	
Enable TLS v1.0 and v1.1 for file downloads. All other SSL services will continue to use TLS v1.2 or higher.		
FortiClient download URL	<input type="text" value="https://"/> <input type="text" value="fctems.schoolzones.ca"/> <input type="text" value=":10443/installers/"/>	
	<input checked="" type="checkbox"/> Open port 10443 in Windows Firewall	
Enforce User Verification	<input checked="" type="checkbox"/>  There are currently 1 FortiClient(s) that do not support user verification and 1 Registered FortiClient(s) that support user verification, but are currently unverified.	
User Verification Period	<input checked="" type="checkbox"/> <input type="text" value="7"/>	days

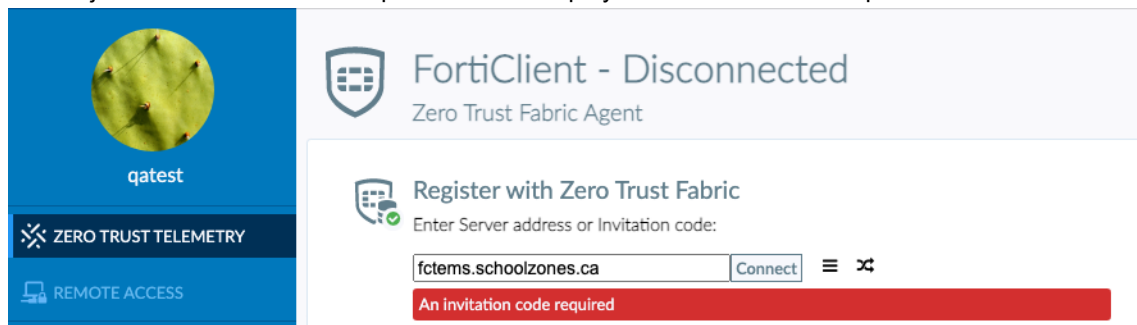
- h. Go to *Zero Trust Tags > Zero Trust Tagging Rules*. Add a Zero Trust tagging rule to tag registered endpoints with verified users.

Zero Trust Tagging Rule Set

Name	<input type="text" value="User Identity"/>
Tag Endpoint As 	<input type="text" value="Verified User"/>
Enabled	<input checked="" type="checkbox"/>
Comments	<input type="text" value="Optional"/>

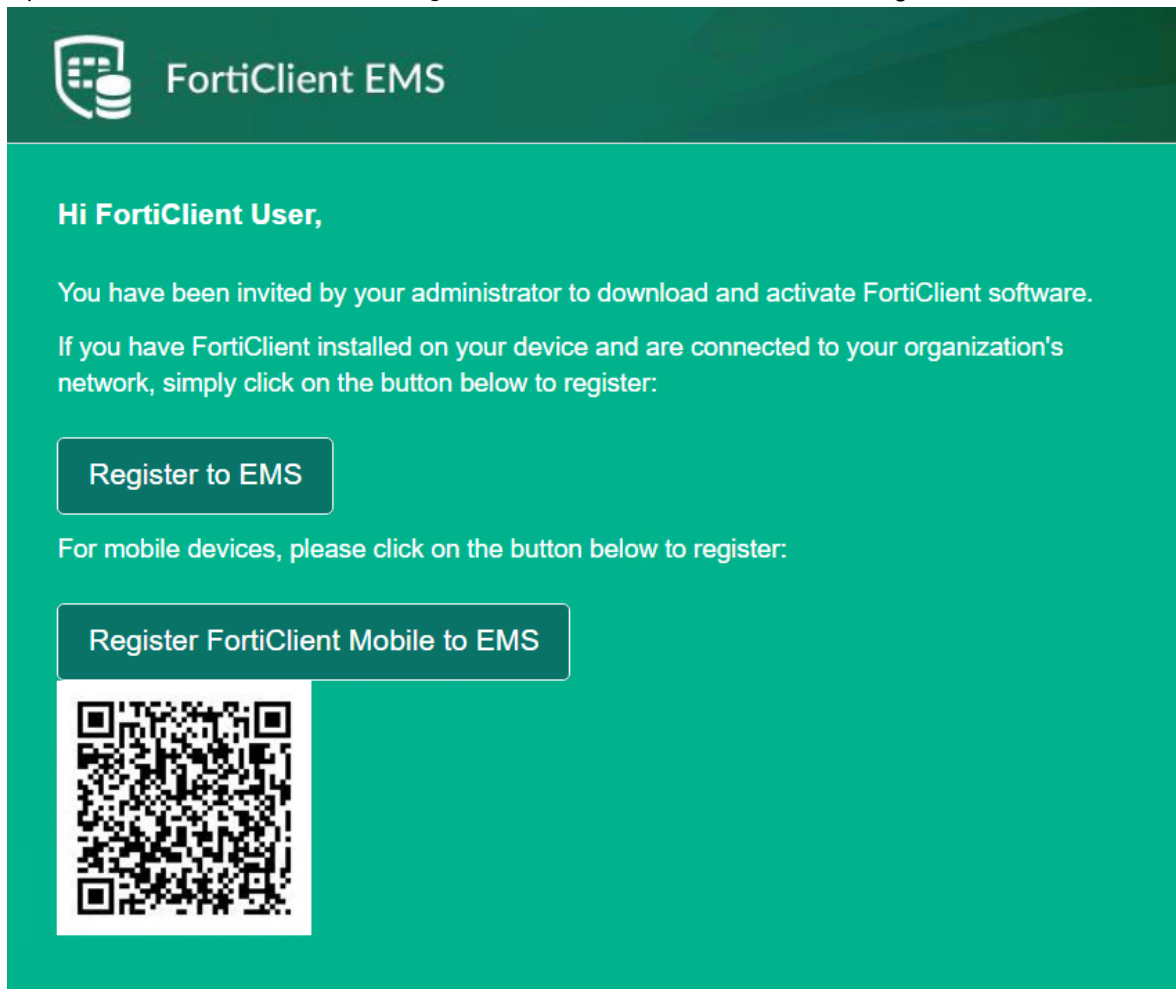
Rules		 Edit Logic	 Add Rule
Type	Value		
 Windows (1)			
User Identity	 Verified User		
 Mac (1)			
User Identity	 Verified User		
 Linux (1)			
User Identity	 Verified User		

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.



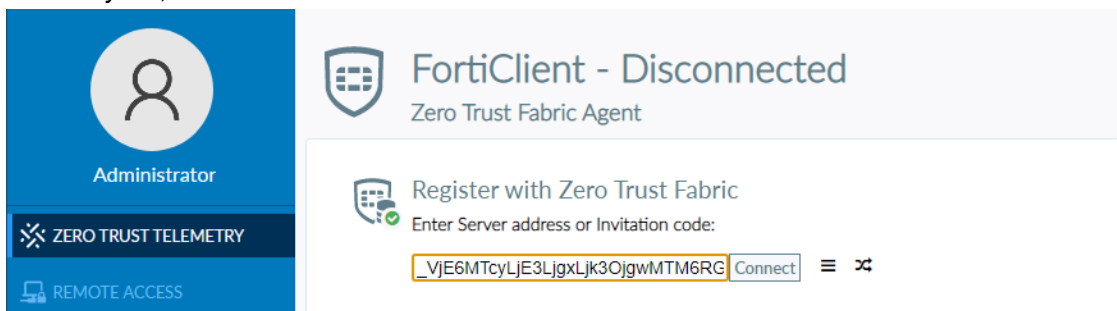
Register to EMS Manually

Alternatively, you can follow the steps below to register your FortiClient using this invitation code:

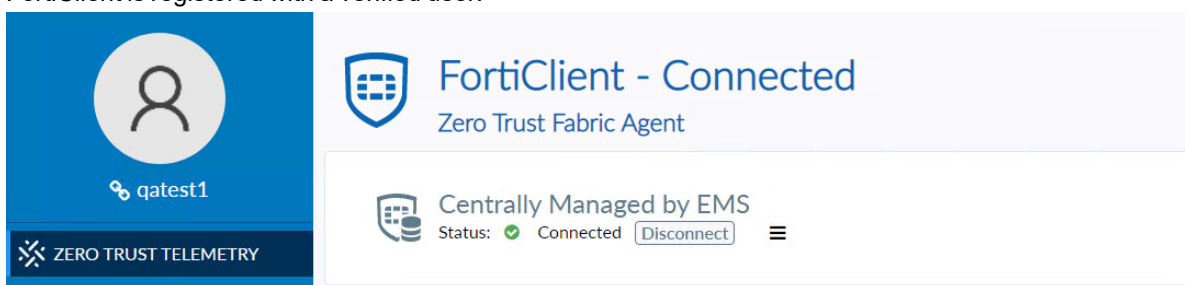
`_VjE6ZmN0ZW1zLnNjaG9vbHpvbmVzLmNhOjgwMTM6RGVmYXVsdDpENzY5NTY4Ny00RjkwLTlTRCMUitQjVlYXQ1FNUQxOTYyNTczNUU=`

- ii. Open the invitation email, and copy the invitation code. Enter the invitation code on the *Zero Trust*

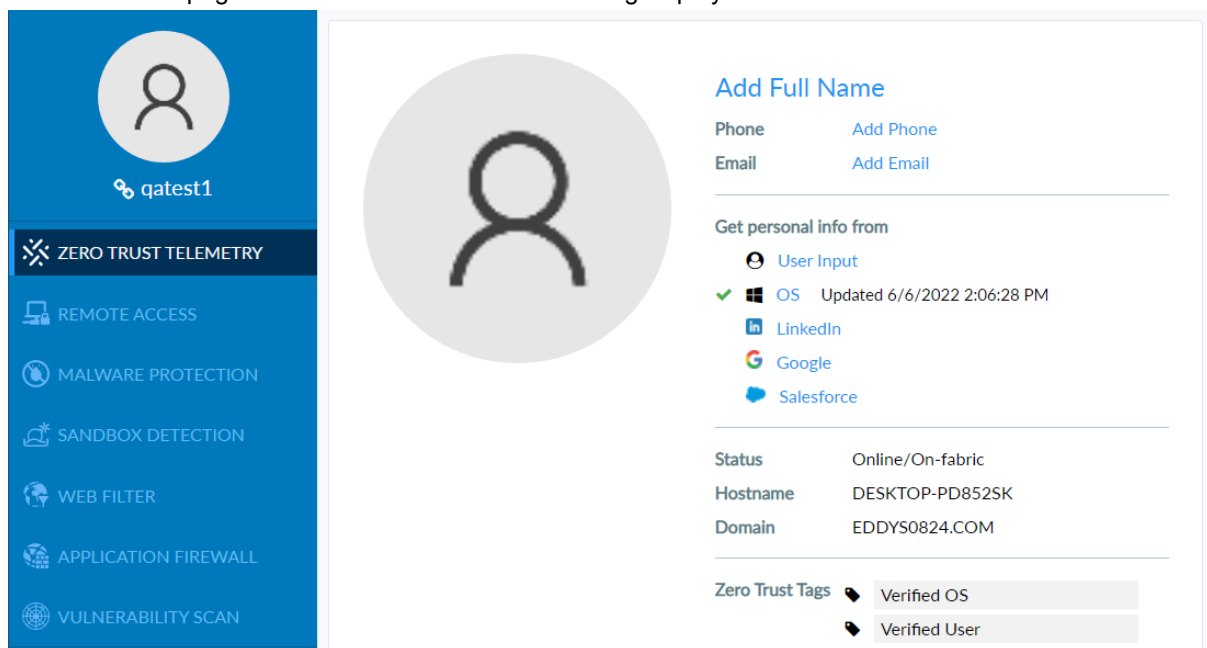
Telemetry tab, and click **Connect**.



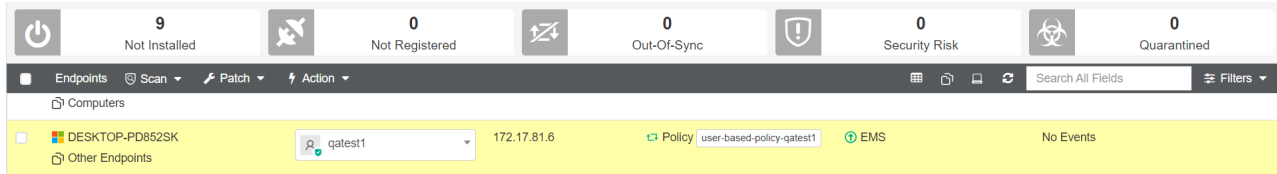
- b. In the popup, provide your LDAP user credentials, then click **Login**. FortiClient proceeds with the registration process after authentication succeeds. After FortiClient successfully registers to EMS, the username in FortiClient changes to the verified user account, and a chain icon appears beside the username to indicate that FortiClient is registered with a verified user.



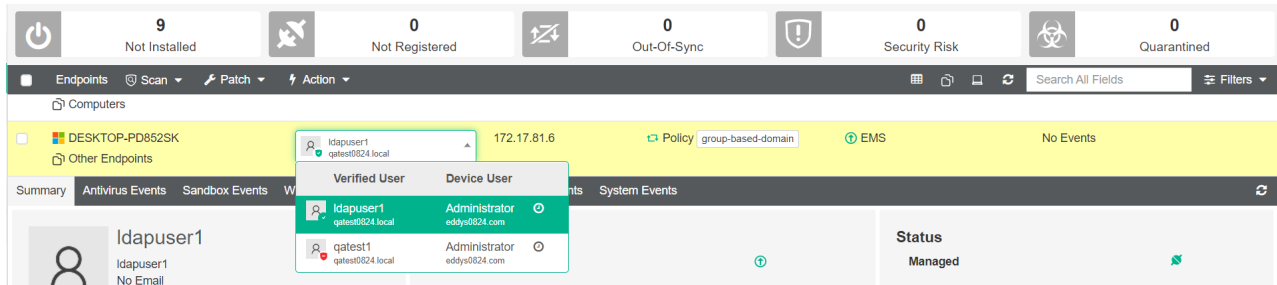
4. Go to the About page to confirm that the Verified User tag displays.



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 Azure AD authentication

The following provides an example of configuring user verification, using an Azure Active Directory (AD) server for authentication. This configuration consists of the following steps:


1. The EMS administrator adds the Azure AD 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 Azure AD credentials.

To configure an Azure AD server in EMS:

1. Configure the Azure AD server as an authentication server in EMS:
 - a. In the Azure management console, collect your AD 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*.

Authentication Server



Azure Active Directory

Tenant ID

5d96077d-28ef-405b

Client ID

62314a93-d553-4185

Authorization Type

Client Secret

Certificate

Client Secret

.....

👁

Alias

Optional

Comment

Optional

Test

Cancel

i. After the test succeeds, click *Save*.

To add endpoints using an Azure AD 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**.

Domain Import View Azure Group Import Tutorial

Azure Server:

Sync every: Minutes
⚠ The minimum sync period is 60 minutes

Group Selection Behaviour:
ⓘ Only the selected Azure users, groups and devices will be imported

Group Name	Source	Import as Base Group
Group	Azure	<input type="checkbox"/>
DnsAdmins	On Prem	<input type="checkbox"/>
ADSyncPasswordSet	On Prem	<input type="checkbox"/>
group	Azure	<input type="checkbox"/>
DnsUpdateProxy	On Prem	<input type="checkbox"/>
group2	Azure	<input type="checkbox"/>
ADSyncBrowse	On Prem	<input type="checkbox"/>
R&D_NA	On Prem	<input type="checkbox"/>
ADSyncAdmins	On Prem	<input type="checkbox"/>
group	Azure	<input checked="" type="checkbox"/>

Changes to Base Group Revert Changes

Status	Group
+ Will be Added	group

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

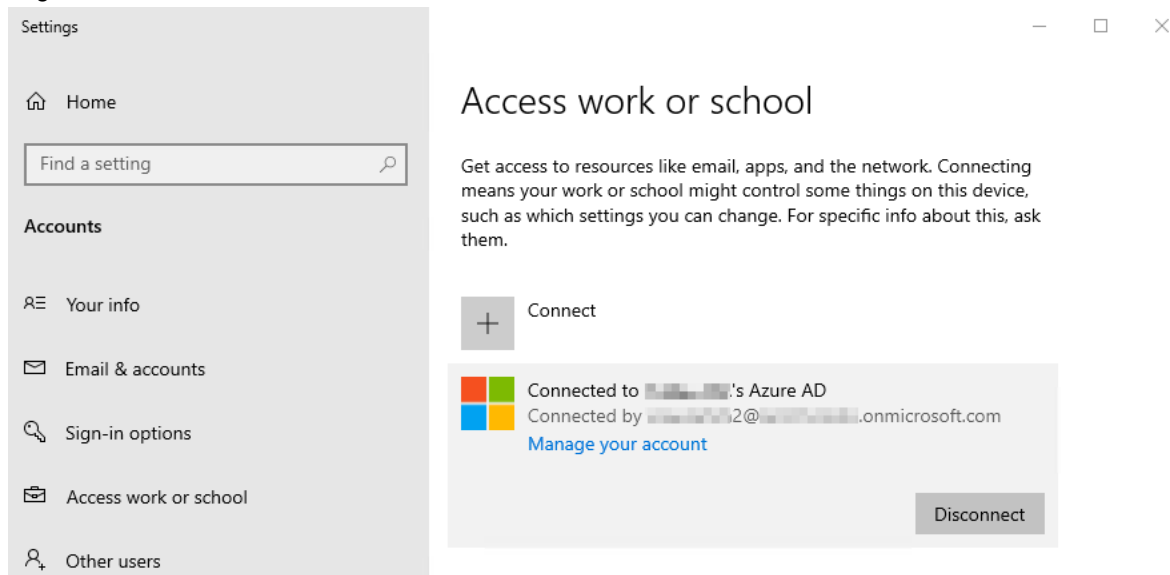
To create an invitation code:

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 Azure AD 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 Azure AD 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 Azure AD user.



9. In FortiClient, on the *Zero Trust Telemetry* tab, enter the invitation code to register to EMS. FortiClient registers to EMS as the logged-in Azure AD user without additional prompts.

Configuring user verification with SAML authentication and an Azure AD server user account

The following provides an example of configuring user verification, using an Azure Active Directory (AD) server for authentication. This configuration consists of the following steps:


1. The EMS administrator adds the Azure AD server to EMS.
2. The EMS administrator creates a SAML configuration in EMS, with EMS as the service provider (SP) and the Azure AD server as the identity provider (IdP).
3. The EMS administrator configures an invitation code, and sends 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 Azure AD credentials.

To configure an Azure AD server in EMS:


1. Configure the Azure AD server as an authentication server in EMS:
 - a. In the Azure management console, collect your AD 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*.

Authentication Server



Azure Active Directory

Tenant ID	<input type="text" value="5d96077d-28ef-405b-"/>
Client ID	<input type="text" value="62314a93-d553-4185-"/>
Authorization Type	<div><div>Client Secret</div><div>Certificate</div></div>
Client Secret	<input type="password" value="....."/> 
Alias	<input type="text" value="Optional"/>
Comment	<input type="text" value="Optional"/>

Test

Cancel

- i. After the test succeeds, click *Save*.

To add endpoints using an Azure AD 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**.

Domain Import View Azure Group Import Tutorial

Azure Server:

Sync every: Minutes
⚠ The minimum sync period is 60 minutes

Group Selection Behaviour:
ⓘ Only the selected Azure users, groups and devices will be imported

Base Group

Group Name	Source	Import as Base Group
Group	Azure	<input type="checkbox"/>
DnsAdmins	On Prem	<input type="checkbox"/>
ADSyncPasswordSet	On Prem	<input type="checkbox"/>
group	Azure	<input checked="" type="checkbox"/>
DnsUpdateProxy	On Prem	<input type="checkbox"/>
group2	Azure	<input type="checkbox"/>
ADSyncBrowse	On Prem	<input type="checkbox"/>
R&D_NA	On Prem	<input type="checkbox"/>
ADSyncAdmins	On Prem	<input type="checkbox"/>
group	Azure	<input checked="" type="checkbox"/>

Changes to Base Group

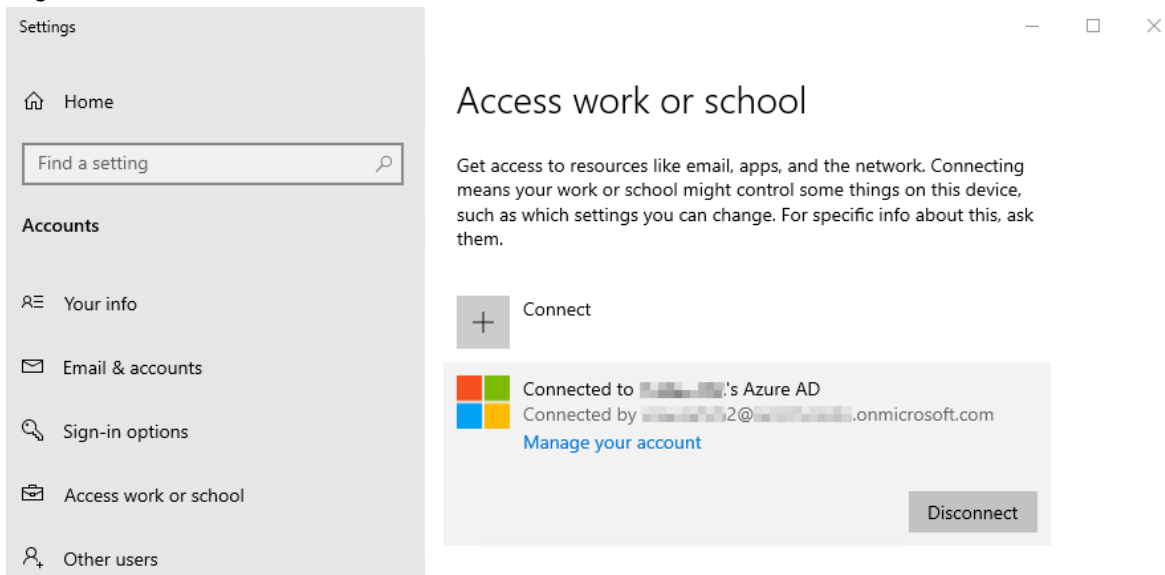
Status	Group
<input checked="" type="checkbox"/> Will be Added	group

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

To register an Azure AD user's endpoint to EMS using SAML:

- Create a SAML configuration:
 - In EMS, go to *User Management > SAML Configuration*.
 - Click **Add**.
 - For *Authorization Type*, select **LDAP**.
 - From the *Domain* dropdown list, select the Azure AD server.
 - 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.
 - Under *Identity Provider Settings*, enter the Azure AD entity ID and single sign on URLs. Click **Save**.
- In the top banner, click *Invitations*.
- Click **Add**.
- For *Verification Type*, select **SAML**.
- From the *SAML Config* dropdown list, select the SAML configuration.
- Configure other settings as desired, then click **Save**.
- You can authenticate the endpoint using Azure AD by doing one of the following:
 - To join the device to the Azure AD server, do the following:
 - On the endpoint, go to *Settings > Accounts*.
 - Under *Access work or school*, click **Connect**.

iii. Log in as an Azure AD user.



- iv. In FortiClient, on the *Zero Trust Telemetry* tab, enter the invitation code to register to EMS. FortiClient registers to EMS as the logged in Azure AD 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 Azure AD user credentials to authenticate and connect FortiClient to EMS.

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 350](#).

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:

Hostname	Displays the FortiClient EMS server's hostname.
Listen on IP	<p>Displays the IP addresses for the FortiClient EMS server. FortiClient connects to FortiClient EMS on the specified IP address.</p> <p>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 334.</p>
Use FQDN	<p>Specify a fully qualified domain name (FQDN) for the FortiClient EMS server. 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:</p> <ul style="list-style-type: none">• Easy to migrate EMS to a different IP address• Easy to migrate to a different EMS instance• Flexible to dynamically resolve the FQDN <p>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.</p> <p>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.</p>

FQDN	Enter the FortiClient EMS server FQDN. FortiClient can connect using the specified IP address in the <i>Listen on IP Addresses</i> option or the specified FQDN.
Remote HTTPS access	Specify settings for remote administration access to FortiClient EMS. Turn remote HTTPS access to FortiClient EMS on and off. When enabled, enter a hostname in the <i>Custom hostname</i> field 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 <i>Remote HTTPS Access</i> is enabled. Displays the predefined HTTPS port. You cannot change the port.
Pre-defined hostname	Available when <i>Remote HTTPS Access</i> is enabled. Displays the predefined hostname. You cannot change the name.
Custom hostname	Available when <i>Remote HTTPS Access</i> is turned on. 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 and Port	Available when <i>Remote HTTPS Access</i> is turned on. 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 Fabric connector.
Redirect HTTP request to HTTPS	Available when <i>Remote HTTPS Access</i> is turned on. If this option is enabled, if you attempt to remotely access FortiClient EMS at <i>http://<server_name></i> , this automatically redirects to <i>https://<server_name></i> .
Webserver certificate	Displays the SSL certificate currently used for the Apache service and the Notify (websockets) daemon. If desired, you can select another certificate from the dropdown list. See Server Certificates on page 338 .
Use Webserver certificate for Endpoint Control	Enable to use the certificate uploaded in the <i>Webserver certificate</i> 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 Server Certificates on page 338 . 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: <ul style="list-style-type: none"> • 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 22 .

Displays the EMS CA certificate expiry. EMS sends this certificate to FortiOS. See [FortiClient in the Security Fabric on page 13](#).

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.

Reset Stalled Deployment Interval

Enter number of hours after which to reset stalled deployments.

3. Configure the following options under *EMS Settings*. FortiClient EMS uses these settings when managing Windows, macOS, and Linux endpoints:

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 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.

Enable TLS 1.0/1.1

Enable TLS 1.0 and 1.1 for file downloads.
You must enable this option when upgrading FortiClient on a Windows 7 device via FortiClient EMS.

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.

Enforce User Verification

Enforce user verification for endpoints. Users must log in to verified user accounts to register to EMS. See [Invitations on page 310](#).

User Verification Period

Enter the desired number of days for the user verification period. Five days before the reauthentication timeout, a notification displays on FortiClient to reauthenticate to keep FortiClient features active.

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.
Enable Managed by EMS	Select an option from the dropdown list. Users can configure this IP address in <i>Shared Settings > Listen on IP</i> .
Connect to local subnets only	Only allow connection to local subnets.
Use connection key	Enable the connection key endpoints can use to connect to FortiGates. Enter and reenter the connection key.
Enable login banner	When you enable the login banner, a message appears prior to a user logging into FortiClient EMS. In the <i>Message</i> field, type your message. The <i>Preview</i> section displays a preview of the message.

- If managing Chromebooks, enable *EMS for Chromebooks Settings*. You may need to restart FortiClient EMS after enabling this option.
- 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 Server Certificates on page 338 .
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 <i>Reset</i> button. This restores the default service account. You must <i>Save</i> the settings for the change to take effect.
ID	Available if the <i>Update service account</i> button is clicked. Enter a new service account ID.
Private key	Available if the <i>Update service account</i> button is clicked. Upload a new service account private key.

6. Configure the following options under *Endpoints Settings*:

FortiClient telemetry connection key	Add the FortiClient Telemetry connection key for FortiClient EMS. FortiClient must provide this key during connection. 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 334 .
Keep alive interval	Each connected FortiClient endpoint sends a short keep-alive (KA) message to FortiClient EMS at the specified interval.
Offline timeout	Configure the number of KA intervals after which EMS considers the endpoint to be offline.
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 <i>Delete now</i> to delete the records immediately.
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.

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 <i>Replace</i> 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 server.

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:
 - a. To generate the QR code without a connection key, beside the *Listen on IP* field, click the *View QR Code* button.
 - b. To generate the QR code with a connection key, ensure that the *FortiClient telemetry connection key* field is populated, then click the *View QR Code* button beside it.
3. In the dialog, select or deselect *Show FortiClient telemetry connection key* as desired.
4. Click *Continue*.
5. Click *Download*.
6. Save the QR code image to your machine.
7. Email the QR code to FortiClient (Android) and FortiClient (iOS) users.

For instructions on scanning the QR code from an Android or iOS device, see [Launching FortiClient \(Android\) for the first time](#) or [Running FortiClient iOS](#).

Persistent connection

When *Use persistent connections* is enabled, FortiClient creates a persistent connection with EMS. It does not tear down and renegotiate the TLS connection at every keepalive interval.

To enable persistent connections:

1. In EMS, go to *System Settings > EMS Settings*.
2. Under *EMS Settings*, enable *Use persistent connections*.

3. Click **Save**.

EMS Settings

Use Webserver certificate for Endpoint Control ☒

⚠ Enabling this feature will result in FortiClients older than 7.0.2 to lose connectivity with EMS. Ensure that all your FortiClients are 7.0.2 or higher. [More Information](#)

EMS CA certificate (ZTNA)

default_ZTNARootCA.pem

2048-06-01

↺

↻

Certificate was created on 2023-06-08T20:17:26.613.

Reset Stalled Deployment Interval

12

hours

EMS Settings

Listen on port

8013

⚙

Use persistent connections

☒

⚠ Enabling this feature will allow FCT 7.2.1 or higher to create persistent connections with EMS. [More information](#)

FortiOS Connector port

8015

FortiClient download URL

https://

192.168.0.101

⌵

:10443/installers/

↺

☒ Open port 10443 in Windows Firewall

Enforce User Verification

☐

⚠ There are currently 0 FortiClient(s) that do not support user verification and 0 Registered FortiClient(s) that support user verification, but are currently unverified.

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.

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 <i>Info</i> , all log messages from <i>Info</i> to <i>Emergency</i> 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	<p>Select one of the following:</p> <ul style="list-style-type: none"> • <i>Disabled</i>: FortiClient EMS does not send system log messages to an external server. • <i>FortiAnalyzer</i>: 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. • <i>SysLog</i>: configure a syslog server for FortiClient EMS to send system log messages to by entering the desired syslog server address, port, and data protocol. <p>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:</p> <ul style="list-style-type: none"> • When FortiClient status changes to online • When EMS considers the FortiClient status as offline • When FortiClient reports a change in its IP address <p>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.</p>

3. Click **Save**.

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 341](#).

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.

The screenshot shows the FortiGuard Labs website. At the top, there's a navigation bar with links: News / Research, Services, Threat Lookup, PSIRT, Resources, and a search bar. Below the navigation bar, a large circular graphic displays '1.8M' with the text 'Number of new and updated anti-virus definitions every week'. To the right is a world map with blue dots indicating FortiGuard hubs. Below the map, a search bar is present with a magnifying glass icon. Under the search bar, there are radio buttons for 'CVE Lookup' (selected), 'Threat ID Lookup', and 'Encyclopedia'. Below these, it says 'Found a suspicious file? Try the Online Scanner.'.

On the left side, there's a section titled 'Version 84.00441' with a red box around the version number. Below it, it says 'Updated: 34 minutes ago'. A list of versions follows:

- 84.00441 34 minutes ago
- 84.00440 1 hour ago
- 84.00439 2 hours ago
- 84.00438 3 hours ago
- 84.00437 4 hours ago

To the right of this list is a 'Threat Intelligence Brief' section with a list of dates:

- February 26, 2021
- February 19, 2021
- February 12, 2021
- February 05, 2021
- January 29, 2021
- January 15, 2021
- December 18, 2020

On the far right, there are two icons with text: a shield icon with 'Protects against latest malware variants with proactive technologies to block new threats' and a circular arrow icon with 'Keeps your protection up-to-date with hourly updates'.

At the bottom, there's a 'FortiGuard Signature Information' table with two columns: 'Name' and 'Version'. The table lists various engines and their versions. The 'AntiVirus Signature' row has the version '84.00441' highlighted with a red box.

Name	Version
Anti-Rootkit Engine	2.00068
Anti-Rootkit Engine 6.2	2.00047
AntiVirus Engine	6.00251
AntiVirus Engine 6.2	6.00126
AntiVirus Extended Signature	84.00422
AntiVirus Extended Signature 6.2	84.00417
AntiVirus Extreme Signature	84.00278
AntiVirus Extreme Signature 6.2	84.00273
AntiVirus Signature	84.00441
AntiVirus Signature 6.2	84.00441
IPS Engine	4.00034
IPS Engine 6.2	4.00014
IPS Signature	18.00026
IPS Signature 6.2	18.00026
VCM Engine for Linux	2.00025
VCM Engine for Linux, 6.2	2.00025
VCM Signature for Linux	2.00061
VCM Signature for Linux, 6.2	2.00061
VCM Signature for MAC	1.00081
VCM Signature for MAC, 6.2	1.00081
VCM Signature for Windows	1.00233
VCM Signature for Windows, 6.2	1.00233

At the bottom of the table, there is a 'Close' button.

To configure FortiGuard Services settings:

1. Go to *System Settings > FortiGuard Services*.
2. Configure the *Software and Signature Update Services* options:

FortiGuard	
Server Location	Configure FortiGuard server location to <i>Global</i> , <i>US</i> , or <i>Europe</i> . Europe is only available if you have selected the <i>Enable SSL</i> 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.

3. 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.

4. Click **Save**.

Server Certificates

You can view and manage certificates from the *Server Certificates* page.

Server Certificates						+ Add	Refresh
<input type="checkbox"/>	Name	Type	Expiry Date	Assigned To			
<input type="checkbox"/>	default_server.crt	Default	Valid 2035-11-19 08:36:53 AM				
<input type="checkbox"/>	haems.fortitest.burnaby.crt	Uploaded	Valid 2031-11-27 01:25:56 PM	Chromebook			
<input type="checkbox"/>	fortitest.ca.p12	Uploaded	Valid 2024-06-29 05:05:47 PM	Webserver			
<input type="checkbox"/>	certems.fortitest.burnaby.crt Renew Required	ACME	Expiring Soon 2022-10-22 08:13:27 AM	Endpoint Control			
<input type="checkbox"/>	FCTEMS-2.crt	FortiCare	Valid 2056-01-18 07:14:07 PM				
<input type="checkbox"/>	FCTEMS-1.crt	FortiCare	Valid 2056-01-18 07:14:07 PM				

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 340 .
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 that Let's Encrypt manages and other certificate management services that use the ACME protocol. See Adding an SSL certificate to FortiClient EMS on page 340 .
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 is currently using a certificate for a certain service, *Server Certificates* displays this information in the *Assigned To* column:

Service	Description	Ports used
Web server	Apache service and the Notify (websockets) daemon. This certificate must be trusted by any browser connecting to EMS or a warning is shown. You can configure the certificate for this service in <i>System Settings > EMS Settings > Shared Settings</i> . See Configuring EMS settings on page 329 .	Apache service: <ul style="list-style-type: none"> • 443 (GUI) • 10443 (installers) Notify (websockets) daemon: 8015
Endpoint control	Endpoint Control daemon. You can configure the certificate for this service in <i>System Settings > EMS Settings > Shared Settings</i> . See Configuring EMS settings on page 329 .	8013
Chromebook	Chromebook daemon. You can configure the certificate for this service in <i>System Settings > EMS Settings > EMS for Chromebooks Settings</i> . See Configuring EMS settings on page 329 .	8443

You can delete certificates from *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 > Server Certificates*.
 - b. Click *Add*.
 - c. For *Type*, select *Automated*.
 - d. In the *Domain* field, enter the EMS fully qualified domain name (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 *Auto Renew* is enabled, FortiClient EMS automatically renews the certificate before expiry.
 - g. If desired, expand the *Advanced* section 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 > 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.

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 342](#).

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:

Server	Enter the SMTP server name.
Port	Enter the port number.
Security	Select <i>None</i> , <i>STARTTLS</i> , or <i>SMTPS</i> for the security type, or select the <i>Auto Detect</i> button to automatically select the security type. If <i>STARTTLS</i> or <i>SMTPS</i> is selected, the <i>Username</i> and <i>Password</i> fields become available.
Username	Enter the username.
Password	Enter the password.
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 <i>Enter</i> 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 AD 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.

1. Click the *Alert* icon (a bell) in the toolbar.
2. Click the *Filter* icon in each column heading to apply filters.
3. Click *Clear Filters* to remove the filters.

Custom Messages

You can customize messages that display on endpoints in certain situations, such as if EMS has 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.

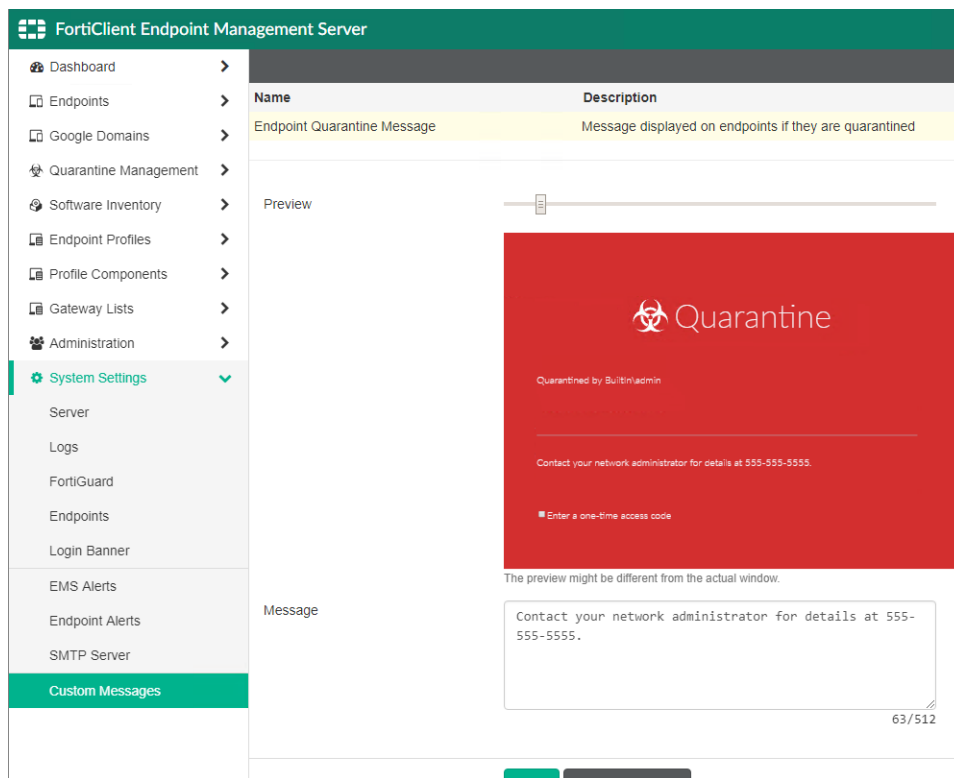
Customizing the endpoint quarantine message

You can customize the message that displays on an endpoint when FortiClient EMS has quarantined 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 Filter in Feature Select results in the following:

- Endpoint profiles:
 - The Web Filter tab is not available for configuration.
 - The option to enable Web Filter logs on the System Settings tab is not available.
- 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 not available on the Status dashboard.
- Importing a profile from FortiGate/FortiManager is not available.

Only an EMS superadministrator can enable and disable features in Feature Select. Other EMS users can view which features are enabled and disabled on the Feature Select page, 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
Application Firewall	<ul style="list-style-type: none">• C&C blocking• Endpoint quarantine
Web Filter	<ul style="list-style-type: none">• 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 ZTNA license, you cannot enable Application Firewall. See [Windows, macOS, and Linux licenses on page 22](#) 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.

Feature Select ⓘ

- ☒ Malware Protection ⓘ
- ☒ Antivirus ⓘ
- ☒ Anti-Ransomware ⓘ
- ☒ Anti-Exploit ⓘ
- ☒ Cloud Based Malware Detection ⓘ
- ☒ Removable Media Access ⓘ
- ☒ Sandbox Detection ⓘ
- ☐ Web Filter ⓘ
- ☒ Application Firewall ⓘ
- ☒ VPN ⓘ
- ☒ Vulnerability Scan ⓘ
- ☒ Zero Trust Network Access ⓘ
- ☒ FortiClient Single Sign-On Mobility Agent ⓘ
- ☐ Chromebook Features ⓘ

Save Cancel

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.

Profile Name Default

Malware Protection ⓘ

- ☐ AntiVirus Protection
- ☒ Anti-Exploit ⓘ
- ☐ Cloud-Based Malware Protection

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*.

Add Deployment Package

Assigned policies cannot enable features that are not installed

12345
VersionGeneralFeaturesAdvancedTelemetry

Basic Security Features

☒ Zero Trust Telemetry
Fabric Telemetry

☒ Secure Access Architecture Components
SSL and IPSec VPN

☒ Vulnerability Scan
Host vulnerability scanning

☒ Advanced Persistent Threat (APT) Components
FortiSandbox detection and quarantine features

Additional Security Features

☒ Malware

☒ AntiVirus, Anti-Exploit, Removable Media Access
Provides real-time protection against a variety of threats

☒ Cloud Based Malware Outbreak Detection
Protects endpoints from high risk file types from Internet, network drives, etc.

☐ Web Filtering ⚠ This feature is disabled in System Settings > Feature Select
Provides defense ag

☒ Application Firewall
Inspect intrusions attempting to exploit known vulnerabilities

☒ Single Sign-On Mobility Agent
Provides FortiAuthenticator for transparent authentication

BackNext

In **Dashboard > Status**, when you click **Manage Widgets**, the Web Filter Detection widget is not available under Top 3 Lists.

Manage Dashboard Widgets

Endpoint Charts

☐ Endpoint Activity

☐ Endpoint Alerts

☒ Endpoint Connection

☐ Managed Mac FortiClient Versions

☐ Managed Windows FortiClient Versions

☐ Managed Linux FortiClient Versions

☒ Endpoint Management

☐ Mac Operating Systems

☐ Windows Operating Systems

☐ Linux Operating Systems

Top 3 Lists

☐ Antivirus Detection

☐ Sandbox Detection

☐ Vulnerability Detection

Others

☒ System Information

☒ License Information

SaveCancel

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. EMS supports up to 20 multitenancy sites.

The following sections detail how to enable multitenancy and multitenancy-specific settings.

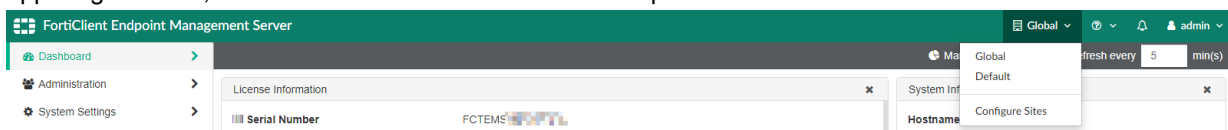
When multitenancy is enabled, Fortinet Security Fabric connectors must use an FQDN to connect to EMS, where the FQDN hostname matches a site name in EMS (including "Default"). The following are examples of FQDNs to provide when configuring the connector to connect to the default site and to a site named 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 multitenancy is enabled, 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 355](#).
- 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 354](#).
- 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
- Zero Trust 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.
Administration	
Administrators	Add and manage FortiClient EMS administrators.

Option	Description
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 <i>EMS for Chromebooks Settings</i> option is enabled in <i>System Settings > EMS Settings</i> .
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.

Option	Description
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 <i>EMS for Chromebooks Settings</i> option is enabled in <i>System Settings > EMS Settings</i> .
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 <i>EMS for Chromebooks Settings</i> option is enabled in <i>System Settings > EMS Settings</i> .
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.
Zero Trust Tags	
Zero Trust Tagging Rules	Define Zero Trust tagging rules.
Zero Trust Tag Monitor	View tagged endpoints.
Fabric Device Monitor	View all FortiGates connected to EMS for Zero Trust tagging and the list of tags that are shared with each FortiGate.
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 <i>Allowlist</i> 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 278](#) 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 management 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 279 .

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.

FortiClient Endpoint Management Server				
Administration		Users		
	Name	Source	Role	Sites
	admin	Builtin	Super Administrator	Global
	AlecB	EMS	Site Administrator	SiteA, 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 279](#).

Name	Source	Role
AlecB	EMS	Super Administrator

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 279](#).

Name	Source	Role
AlecB	EMS	Read-only Administrator

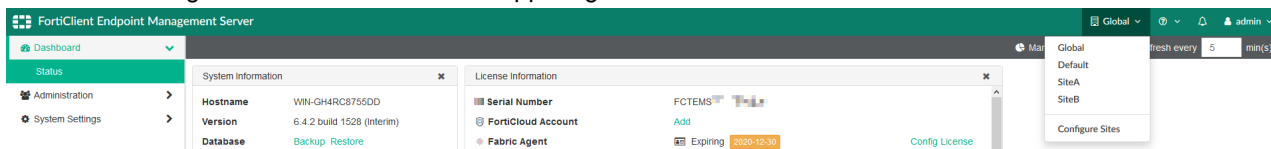


If you had configured a SAML SSO administrator prior to enabling multitenancy, enabling multitenancy causes this administrator to become a global superadministrator. You can configure a different role for this administrator. You can only have one SAML SSO administrator for the entire EMS server.

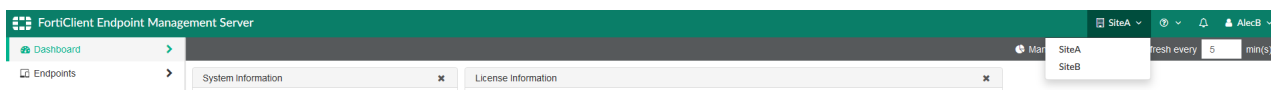
Logging into EMS with multitenancy enabled

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.



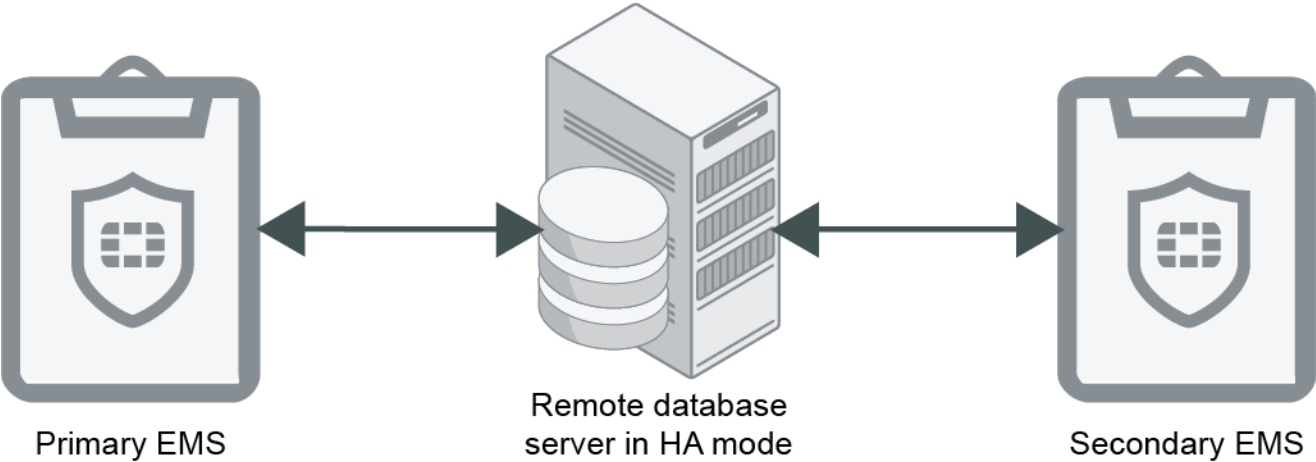
Redundancy

The following describes redundancy or high availability (HA) options for EMS where endpoint information is synced between multiple EMS nodes running in active-passive HA mode. Consider a scenario where two EMS nodes, EMS A and EMS B, run in HA mode with EMS A as the primary node and EMS B as the secondary node. Both EMS nodes are connected to the same remote database server. Endpoints are connected to EMS A. If EMS A fails, EMS B is promoted to become the primary node, and endpoints automatically register to EMS B.

EMS HA mode supports configuring multiple EMS servers with one SQL Server. SQL Server should be running on a remote, separate Windows server. If you want to add database HA support, you can configure a SQL Server failover cluster. For EMS HA with SQL Server failover setup, see [HA with Multiple Databases Deployment Guide](#). For EMS HA with always on SQL setup, see [Always on HA in multisubnet environment](#).

This guide focuses on configuring HA for EMS services. It assumes that you have completed SQL Server failover cluster setup.

The example setup has two EMS nodes and one database server.



Note the following:

- Sharing files between EMS nodes relies on network shares that different EMS nodes can access.
- There are multiple ways to implement DNS and load balancing to handle EMS failover:

Method	Description
DNS round robin or failover	EMS running in HA mode must always configure a fully qualified domain name (FQDN), and FortiClient endpoints must point to a DNS server that has enabled DNS round robin or supports DNS failover, so that endpoints can always connect to the correct primary EMS server. Endpoint users must ensure that endpoints do not cache the DNS result for more than 30 seconds so that FortiClient can resolve the FQDN to the new primary EMS server with a new IP address in case EMS failover happens quickly.

Method	Description
Load balancer	DNS round robin configuration may cause Fortinet Security Fabric connector to send data to the failover node, which by design has all but the monitor FCEMS services off. This results in Fabric connection failure. To overcome this limitation, set up the Fabric connection using traffic manager or FortiGates as a load balancer. See Fabric connection setup using traffic manager on page 362 and Fabric connection setup using FortiGate as a load balancer on page 365 .

- If logged in to an EMS server as a domain user, add the domain user to the local logon as a service. Otherwise, EMS services may not start up properly.

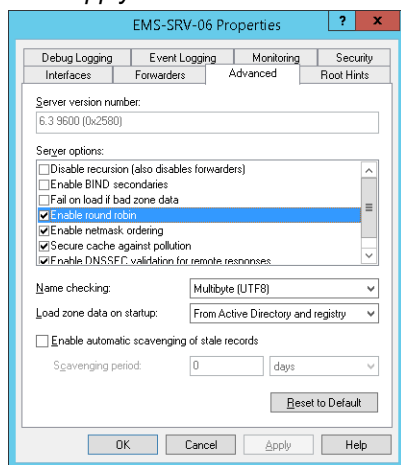


This configuration uses DNS round robin, which may cause Fabric connector connections to send data to the failover node, which by design has all but the monitor FCEMS services off. This causes the Fabric connection to drop.

To configure DNS round robin on the DNS server:

By configuring DNS round robin, you can configure load balancing by pointing the same hostname to multiple servers with different IP addresses in DNS.

1. Open DNS Manager.
2. Right-click the server name, then select *Properties*.
3. On the *Advanced* tab, under *Server options*, click *Enable round robin*.
4. Click *Apply*.



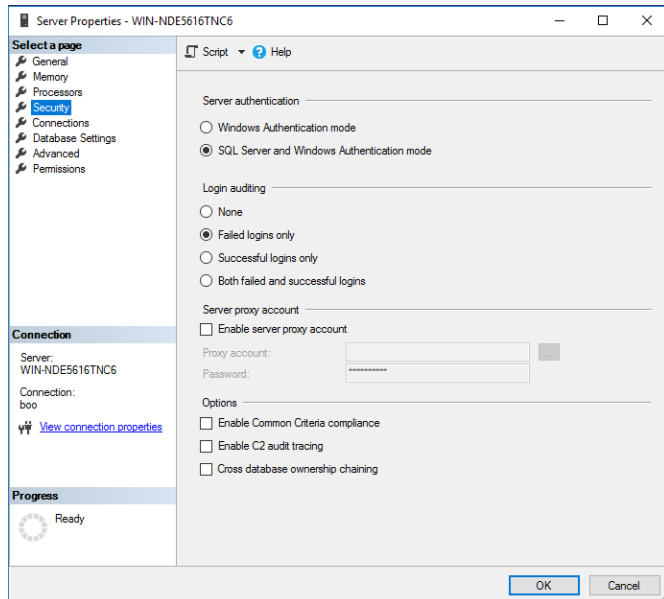
To configure SQL Server options on the remote database server:

The example uses SQL Server security login to connect to the remote database server to create the EMS database during EMS installation. You must enable certain SQL Server options before installing EMS.

If the SQL Server has multiple databases configured, ensure that each database is listening on a different port.

1. Open Microsoft SQL Server Management Studio as an administrator.
2. In the *Object Explorer* pane, select *Connect > Database Engine*.
3. In the *Connect to Server* dialog, enter your credentials and connect to the database server.

4. In the *Object Explorer* pane, right-click the server, then select *Properties*.
5. In the *Server Properties* dialog, go to *Security*.
6. Under *Server authentication*, select *SQL Server and Windows Authentication mode*.



7. Create a SQL login user:
 - a. Right-click *Security*, then select *New > Login*.
 - b. In the *Login name* field, enter the desired username. In this example, the username is "cbreaux".
 - c. Select *SQL Server authentication*.
 - d. In the *Password* and *Confirm password* fields, enter the desired password. In this example, the password is "MyPassword".
 - e. Disable *Enforce password policy*.
 - f. Go to *Server Roles*.
 - g. Select *sysadmin*, then click *OK*.
8. On the EMS node, open SQL Server Management Studio and attempt to connect to the remote database with the SQL user that you created to ensure that the node can connect to the database server using the credentials.

To install EMS:

Joining EMS nodes to a domain is unnecessary, as you use a SQL user account to connect to the database instance on the remote SQL Server database server.

EMS 7.2 does not rely on FILESTREAM for file synchronization between EMS nodes. Instead, it uses network share. Install EMS:

1. Create and share a folder on the network. This file share is used to share files between EMS nodes. All EMS nodes should be able to access the file share. During EMS installation, the installer mounts the file share as the W:\ drive. Ensure that the W:\ drive is free on all EMS nodes.
2. On EMS-1, open Command Prompt as an administrator.
3. Run the following command:


```
FortiClientEndpointManagementServer_7.2.0.0686_x64.exe
SQLServer= WIN-NDE5616TNC6 SQLUser= cbreaux SQLUserPassword=MyPassword InstallSQL=0
ScriptDB=1 FileStorageNic=\\Server\fileshare FileStorageNicUser=LAB\administrator
FileStorageNicPass=Admin123! BackupDir=\\EMS-1\backup DBInitialSize=31MB
DBInitialLogSize=4MB DBGrowth=11MB DBLogGrowth=11% DBLoginTimeout=31
```

DBQueryTimeout=61

Parameter	Description
ScriptDB=1	Specifies that this is the primary active server.
BackupDir	Configured to \\EMS-1\backup, which is a locally shared folder on EMS-1. EMS and the SQL service user must have read/write/modify permissions to this folder.
FileStorageNic	Fileshare path.
FileStorageNicUser	Username for account with read/write/modify permissions to the shared folder.
FileStorageNicPass	Password for account with read/write/modify permissions to the shared folder.

The following is an example of the command when using a named SQL instance. In this example, the SQL instance is EMSNAMED: FortiClientEndpointManagementServer_7.2.0.0686_x64.exe SQLServer= WIN-NDE5616TNC6 \EMSNAMED SQLUser=cbreaux SQLUserPassword=MyPassword InstallSQL=0 ScriptDB=1 FileStorageNic=\\Server\fileshare FileStorageNicUser=LAB\administrator FileStorageNicPass=Admin123! BackupDir=\\EMS-1\backup DBInitialSize=31MB DBInitialLogSize=4MB DBGrowth=11MB DBLogGrowth=11% DBLoginTimeout=31 DBQueryTimeout=61

4. On EMS-2, open Command Prompt as an administrator. Run the following command:

```
FortiClientEndpointManagementServer_7.2.0.0686_x64.exe SQLServer= WIN-NDE5616TNC6
\EMSNAMED SQLUser=cbreaux SQLUserPassword=MyPassword InstallSQL=0 ScriptDB=1
FileStorageNic=\\Server\fileshare FileStorageNicUser=LAB\administrator
FileStorageNicPass=Admin123! BackupDir=\\EMS-1\backup DBInitialSize=31MB
DBInitialLogSize=4MB DBGrowth=11MB DBLogGrowth=11% DBLoginTimeout=31
DBQueryTimeout=61
```

Parameter	Description
ScriptDB=0	Indicates the upgrade does not execute scripts to upgrade the database because you upgraded the database in step 3.
BackupDir	Configured to \\EMS-2\backup, which is a locally shared folder on EMS-2. EMS and the SQL service user must have read/write/modify permissions to this folder.
FileStorageNic	Fileshare path.
FileStorageNicUser	Username for account with read/write/modify permissions to the shared folder.
FileStorageNicPass	Password for account with read/write/modify permissions to the shared folder.

The following is an example of the command when using a named SQL instance. In this example, the SQL instance is EMSNAMED: FortiClientEndpointManagementServer_7.2.0.0686_x64.exe SQLServer=WIN-NDE5616TNC6\EMSNAMED SQLUser=cbreaux SQLUserPassword=MyPassword InstallSQL=0 ScriptDB=0 FileStorageNic=\\Server\fileshare FileStorageNicUser=LAB\administrator FileStorageNicPass=Admin123! BackupDir=\\EMS-2\backup DBInitialSize=31MB

```
DBInitialLogSize=4MB DBGrowth=11MB DBLogGrowth=11% DBLoginTimeout=31
DBQueryTimeout=61
```

To configure EMS:

1. On the primary node, log in to EMS.
2. Go to *System Settings > Server*.
3. Enable *Use FQDN*.
4. In the *FQDN* field, enter the desired FQDN.

Server

Shared Settings

Hostname: WIN-05896RRF1KH

Listen on IP: All FQDN is required when listening to all IPs.

Use FQDN: ☒

FQDN: ha.privatehyperv.com

5. Go to *System Settings > EMS Settings*. Configure the *High Availability Keep Alive Internal* field with a value between 5 and 30 seconds.
6. 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.
7. Update the EMS licensing:
 - a. Go to *License Information widget > Configure License*.
 - b. For *License Source*, select *FortiCare*.
 - c. In the *FortiCloud Account* field, enter your FortiCloud account ID or email address.
 - d. In the *Password* field, enter your FortiCloud account password.
 - e. 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.

Configure License

Serial number: FCTEMS0000099

Hardware ID: C4A7D922-CC9B-490A-BFA2-1DD86D4317FA-5291E64E

Fabric Agent with Endpoint Protection: Licensed 2020-05-21

Sandbox Cloud: Licensed 2020-05-21

FortiClient Licenses Used: 2 out of 50

Chromebook: Licensed 2020-05-21

Chromebook Licenses Used: 0 out of 50

License Source: FortiCare (selected) | File Upload

FortinetOne Account: @fortinet.com

Buttons: Sync License Now, Edit Account, Delete Account

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.

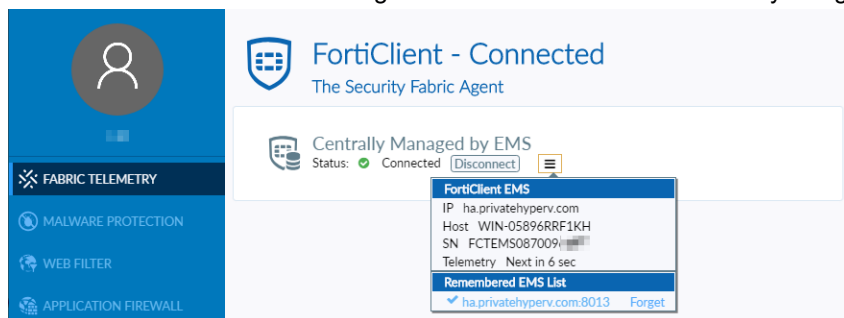


As this HA deployment uses DNS round robin, when you attempt to log in to EMS, you may be directed to the passive EMS. If this occurs, the browser displays `ERR_CONNECTION_CLOSED`. The login succeeds if DNS resolves the FQDN to the active EMS.

To avoid this, you can log in to EMS using the EMS IP address instead of the FQDN if you can confirm which EMS is currently the primary node and no failover has occurred.

To validate the HA configuration:

1. Go to *Manage Installers > Deployment Packages*. Create a deployment package to deploy FortiClient to endpoints. See [Adding a FortiClient deployment package](#).
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 server successfully using the FQDN.



To upgrade EMS in HA mode:

1. Stop all services in all secondary EMS servers to avoid failover while the primary EMS server is upgrading.
2. Upgrade the primary server while it is running.
3. After successfully upgrading the primary server, upgrade the secondary EMS servers. If you have multiple secondary EMS servers, you can upgrade them one by one, or simultaneously.

Fabric connection setup using traffic manager

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 traffic manager in your topology. This effectively brokers the data routing to the correct EMS based on availability.

To demonstrate this configuration, the example EMS HA environment is configured in Azure Cloud. This deployment uses the following components in Azure:

- Two EMS nodes
- SQL Server
- Traffic manager

You should use FortiOS 7.2.1 or 7.0.7 and later versions for this setup.

To configure traffic manager:

1. Log in to the Azure portal.
2. Select the desired resource group.
3. Search for traffic manager, and create the profile. The traffic manager profile overview displays the DNS name, which you use to set up the Fabric connection and register FortiClient endpoints.
4. You must add traffic manager profile endpoints. In this example, the endpoints are EMS nodes. On the *Endpoints* tab, select *Add*.
5. For *Target Resource type*, select *Public IP Address*. emsnode1 and emsnode2 are added as endpoints in traffic manager. Due to the configuration, the nodes are monitored. emsnode1 is the primary node and emsnode2 is the secondary.

The screenshot shows the Azure portal interface for a Traffic Manager profile named 'emsharelease'. The left sidebar contains navigation options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Configuration, Real user measurements, Traffic view, and Endpoints. The main content area displays the 'Essentials' tab for the profile. It shows the Resource group as 'ECTMS_Release', Status as 'Enabled', Subscription as 'Software Development/Engineering', and Subscription ID as '3f4a74b-5e8a-408f-8b5b-c8bfed336d28'. The DNS name is 'http://emsharelease.trafficmanager.net', Monitor status is 'Degraded', and Routing method is 'Performance'. Below this, there are tags for Name, Username, ExpectedUseThrough, VMState, ShutdownAtNight, and CostCenter. At the bottom, the 'Endpoints' tab is active, showing a table with two endpoints: emsnode1 (Enabled, Online, Azure endpoint, West US 2) and emsnode2 (Enabled, Degraded, Azure endpoint, North Central US).

Name	Status	Monitor status	Type	Location
emsnode1	Enabled	Online	Azure endpoint	West US 2
emsnode2	Enabled	Degraded	Azure endpoint	North Central US

6. Go to **Settings > Configuration**. Confirm that traffic manager is set to monitor TCP port 8013.

The screenshot shows the 'emsharelease | Configuration' page for a 'Traffic Manager profile'. The left sidebar contains navigation links: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (with sub-links for Configuration, Real user measurements, Traffic view, Endpoints, Properties, Locks), Monitoring (with sub-links for Alerts, Metrics, Diagnostic settings, Logs), and a search bar. The main content area shows configuration settings for the 'Performance' routing method. The 'DNS time to live (TTL)' is set to 20 seconds. The 'Endpoint monitor settings' show 'Protocol' as TCP, 'Port' as 8013, and 'Path' as empty. The 'Fast endpoint failover settings' show 'Probing interval' as 10 and 'Tolerated number of failures' as 2. The 'Probe timeout' is set to 5 seconds.

After failover when the EMS secondary node becomes responsive, meaning that all FCEMS services are on, the traffic manager status changes from degraded to online.

The screenshot shows the 'emsharelease Essentials' page. It displays the 'Resource group' as 'FCEMS_Release', 'Status' as 'Enabled', 'Subscription' as 'Software Development/Engineering', and 'Subscription ID' as '3f4a7f4a-5e6a-408f-8b5b-c8bfeb636628'. The 'DNS name' is 'http://emshareleasetrafficmanager.net', 'Monitor status' is 'Degraded', and 'Routing method' is 'Performance'. Below this, a table lists the endpoints:

Name	Status	Monitor status	Type	Location
emsnodet1	Enabled	Degraded	Azure endpoint	West US 2
emsnodet2	Enabled	Online	Azure endpoint	North Central US

To configure the Fabric connection between FortiOS and EMS:

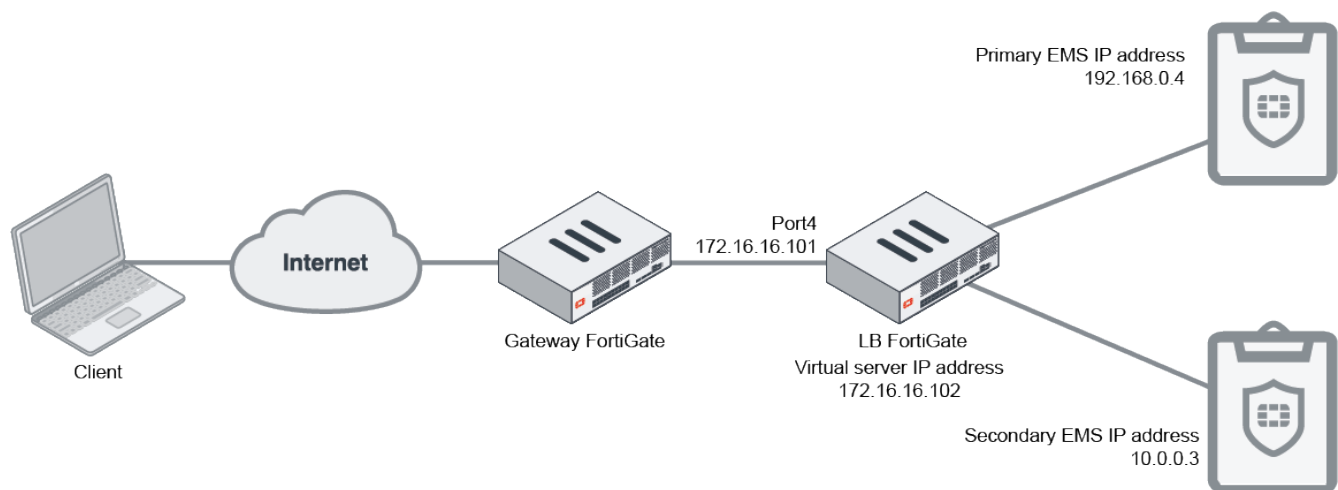
1. In FortiOS, go to **Security Fabric > Fabric Connectors**.
2. Double-click the **FortiClient EMS** card.
3. Under **FortiClient EMS Settings**, in the **IP/Domain name** field, enter the traffic manager fully qualified domain name (FQDN). The FQDN resolves to the active EMS node's IP address. After EMS failover, the secondary EMS node status in traffic manager changes from degraded to online. The new EMS active node IP address is returned, and FortiOS continues to be connected and authorized. For earlier FortiOS versions, the FQDN is resolved only once, and the Fabric connector uses the same IP address failover, causing the WebSocket connection to disconnect. FortiOS 7.2.1 or 7.0.7 and later versions periodically checks if the FQDN has a new IP address and switches to it after EMS failover.

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.

IPv4 Virtual Server									
PORT_10443	TCP	172.16.16.102:10443	First Alive	Monitor_8013	192.168.0.4 10.0.0.3	REMOTE_LAN (port4)	0		
PORT_443	TCP	172.16.16.102:443	First Alive	Monitor_8013	192.168.0.4 10.0.0.3	REMOTE_LAN (port4)	1,360	<div></div>	6 seconds ago
PORT_8013	TCP	172.16.16.102:8013	First Alive	Monitor_8013	192.168.0.4 10.0.0.3	REMOTE_LAN (port4)	210	<div></div>	15 seconds ago
PORT_8015	TCP	172.16.16.102:8015	First Alive	Monitor_8013	192.168.0.4 10.0.0.3	REMOTE_LAN (port4)	7	<div></div>	16 minutes ago

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.

Azure SQL managed instance

You can deploy EMS using an Azure SQL managed instance. Azure provides two SQL-based offerings: Azure SQL managed instances and Azure SQL databases, which are mutually incompatible. EMS only supports Azure SQL managed instances. Azure SQL databases do not provide all features that EMS requires.

The following example deploys Azure virtual machines (VM) for EMS nodes. However, the deployment also supports on-premise EMS instances. You can set up on-premise EMS nodes outside of the Azure environment.

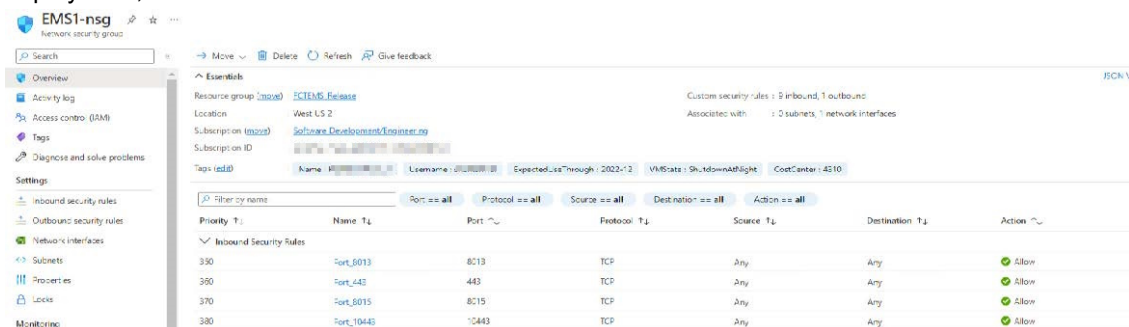
The deployment consists of the following steps:

1. Deploy VMs in Azure. See [To deploy VMs in Azure: on page 367](#).
2. Install an Azure SQL managed instance. See [To install an Azure SQL managed instance: on page 368](#).
3. Configure file sharing. See [To configure file sharing: on page 368](#).
4. Install EMS. See [To install EMS: on page 369](#).

The document also provides information on backing up and restoring a database on EMS when using this deployment. See [To restore a database: on page 371](#).

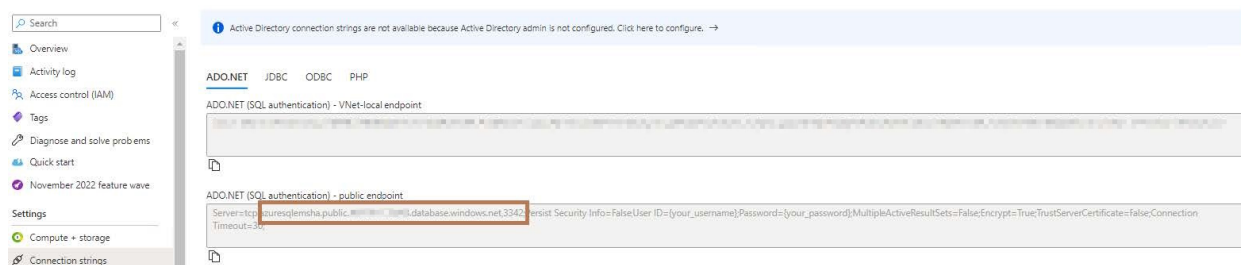
To deploy VMs in Azure:

1. In the Azure marketplace, select the desired VM listing.
2. Click *Create*, then *Create a virtual machine hosted by Azure*.
3. Configure the basic configuration fields as follows:
 - a. If you require VM redundancy, select the desired availability option. Otherwise, select *No infrastructure redundancy required*.
 - b. Select the desired VM image. See [Management capacity on page 27](#).
 - c. Configure other fields as desired. Click *Next*.
4. For OS disk type, select *Premium SSD*. Click *Next*.
5. Configure network settings:
 - a. Create a virtual network (VNet) if it is not already configured.
 - b. Create a public IP address if you require outside communication.
6. Configure other settings as desired, then create the VM. This example uses default settings.
7. For both EMS nodes, configure security group inbound ports and allow access to ports 8013, 443, 8015, 10443, and 8443 for endpoint connection, EMS web access, FortiGate Fortinet Security Fabric connection, FortiClient package deployment, and Chromebook access.



To install an Azure SQL managed instance:

1. In the Azure marketplace, search for SQL managed instance.
2. Click *Create*.
3. When configuring the number of vCores and the storage size, consider the sizing guidelines in [Management capacity on page 27](#). Configure other fields as desired, then click *Next*.
4. Configure network settings:
 - a. From the *Virtual network / subnet* dropdown list, select the EMS servers' VNet.
 - b. For the *Connection type (VNet-local endpoint)* dropdown list, leave the default value, *Proxy (Default)*.
 - c. If the EMS server may need to access this SQL instance over the Internet, enable *Public endpoint (data)*. Otherwise, disable this option.
5. Configure other settings as desired, then create the instance.
6. After deployment finishes, go to *Settings > Connection strings*. Note the SQL database FQDN and listen port. The EMS installation requires these values.



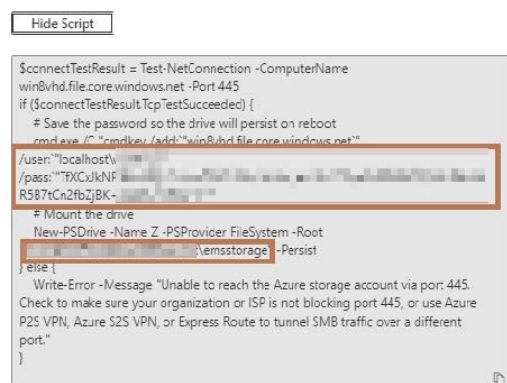
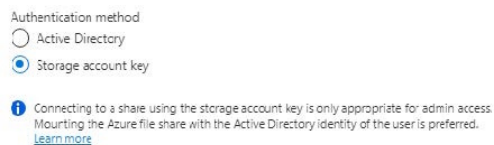
7. If you plan to have the EMS server access the SQL database publicly, go to the SQL managed instance network security group and add an inbound rule to allow access for port 3342.

To configure file sharing:

Sharing files between EMS nodes relies on network shares that only the EMS nodes can access. If you deploy on-premise EMS nodes, you can use a shared folder. For this deployment, where you deploy the EMS nodes on Azure, file sharing uses Azure blob file share.

1. Create a storage account:
 - a. In the Azure marketplace, search for storage account.
 - b. Click *Create*.
 - c. For *Performance*, select *Premium*.
 - d. From the *Premium account type* dropdown list, select *Block blobs*. Configure other fields as desired, then click *Next*.
 - e. On the *Advanced* tab, leave the default settings. Click *Next*.
 - f. Under *Public network access*, select *Enabled from selected virtual networks and IP addresses*.
 - g. Under *Virtual networks*, select the EMS server VNet.
 - h. Set *Routing Preference* to *Microsoft network routing*.
 - i. Leave the default settings for data protection and encryption. Proceed to create the account.
2. Once Azure creates the storage account, verify the following settings under *Configuration*:
 - a. *Secure Transfer required* is disabled.
 - b. *Blob public access* is enabled.
 - c. *Storage account key access* is enabled.
 - d. *Version 1.2* is configured for minimum TLS version.
3. Go to *Security + networking > Networking*.

4. Under *Firewall*, add IP addresses to allow access from the Internet.
5. Enable *Allow Azure services on the trusted services list to access this storage account*.
6. Go to *Data storage > File shares*.
7. Create a file share.
8. From the context menu, click *Connect*, then select *Show Script*.
9. Note the path, username, and password values to use during EMS installation.



To install EMS:

Do one of the following:

1. If installing EMS on nodes in Azure, do the following:
 - a. During EMS installation, the installer mounts file shares as the W:\ drive. Ensure that the W:\ drive is free on all EMS nodes.
 - b. Start the EMS installation on the primary node using the following command:


```

FortiClientEndpointManagementServer_7.2.X._x64.exe SQLServer=<Azure SQL FQDN>
SQLPort=<Azure SQL port> PaaS=azure SQLUser=<SQL user> SQLUserPassword=<SQL
password> InstallSQL=0 ScriptDB=1 FileStorageNic= FileStorageNicUser=
FileStorageNicPass=
          
```

Parameter	Description
PaaS=azure	Informs EMS that it will connect to an Azure SQL managed instance.
FileStorageNic	Fileshare path.
FileStorageNicUser	Fileshare username.
FileStorageNicPass	Fileshare password.
ScriptDB=1	Specifies that this is the primary node.

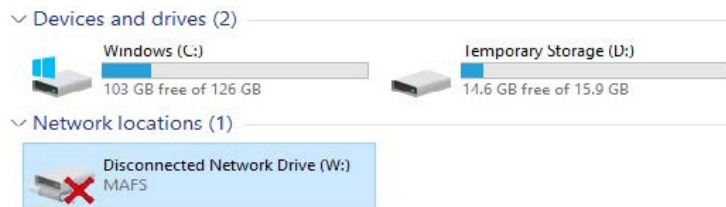
The following provides an example command:

```

SQLServer=azuresqlemsha.public.123456789.database.windows.net SQLPort=3342
PaaS=azure SQLUser=emsadmin SQLUserPassword=Password123# InstallSQL=0 ScriptDB=1
  
```

```
FileStorageNic= \\fileshare.file.core.windows.net\storage
FileStorageNicUser=localhost\fileshare FileStorageNicPass=
TfXCxJkNP4kbzR78GhOYYxcZS22hGQ+lMcke
```

After installation completes, a mapped drive for the fileshare is created.



- c. Start the EMS installation on the secondary node using the following command:

```
FortiClientEndpointManagementServer_7.2.X._x64.exe
SQLServer=azuresqlemsha.public.123456789.database.windows.net SQLPort=3342
PaaS=azure SQLUser=emsadmin SQLUserPassword=Password123# InstallSQL=0 ScriptDB=0
FileStorageNic= \\fileshare.file.core.windows.net\storage
FileStorageNicUser=localhost\fileshare FileStorageNicPass=
TfXCxJkNP4kbzR78GhOYYxcZS22hGQ+lMcke
```

ScriptDB=0 indicates that this is the secondary node.

For Azure traffic manager setup in an Azure environment, see [Fabric connection setup using traffic manager](#).

2. If installing on-premise EMS, do the following:

- a. Create and share a folder on the network. This share folder is mounted as a drive during EMS installation.

- b. Install EMS on the primary node with the following

```
command: FortiClientEndpointManagementServer_7.2.X._x64.exe SQLServer=<Azure_SQL_
FQDN> SQLPort=<Azure_SQL_Port> PaaS=azure SQLUser=<SQL User>
SQLUserPassword=<SQL_Password> InstallSQL=0 ScriptDB=1 FileStorageNic=
FileStorageNicUser= FileStorageNicPass=.
```

The following provides an example command: FortiClientEndpointManagementServer_7.2.X._x64.exe SQLServer=azuresqlemsha.public.123456789.database.windows.net SQLPort=3342 PaaS=azure SQLUser=emsadmin SQLUserPassword=AzureSql123!@# InstallSQL=0 ScriptDB=1 FileStorageNic= \\Server\emsshare FileStorageNicUser=LAB\administrator FileStorageNicPass= Admin123!

Parameter	Description
FileStorageNic	Fileshare path.
FileStorageNicUser	Username for account with read/write/modify permissions to the shared folder.
FileStorageNicPass	Password for account with read/write/modify permissions to the shared folder.

- c. Install EMS on the secondary node with the following command:

```
FortiClientEndpointManagementServer_7.2.X._x64.exe
SQLServer=azuresqlemsha.public.123456789.database.windows.net SQLPort=3342
PaaS=azure SQLUser=emsadmin SQLUserPassword=AzureSql123!@# InstallSQL=0
ScriptDB=0 FileStorageNic= \\Server\emsshare
FileStorageNicUser=LAB\administrator FileStorageNicPass= Admin123!
```

To restore a database:

When using an Azure SQL managed instance database, EMS cannot manage database backups or restore backups generated from another EMS instance. Azure provides a comprehensive dashboard to set up and managed automatic database backups. This is the recommended method of database restore and backup for this deployment. Restoring a regular SQL server backup and upgrading EMS from an existing SQL server installation to an EMS with Azure SQL managed instance database is not supported.

1. In the Azure portal, go to *Databases*.
2. Select the FCM database.
3. Click *Restore*.
4. Enter a unique name.
5. Repeat the process for all EMS databases.
6. Log in to SQL Server Management Studio and confirm that it lists the backup databases.
7. To restore a database, delete the original database from the Azure portal.
8. Rename the backup database to the original name using the following command. For example, to restore the FCM_backup database, rename it to FCM as follows: `ALTER DATABASE [FCM_backup] MODIFY NAME = [FCM]`.

Configuring EMS HA using AWS RDS Microsoft SQL Server

This document provides information about deploying FortiClient EMS using AWS Relational Database Service (RDS) Microsoft SQL Server. It aims to provide a step-by-step guide on EMS high availability (HA) with some basic coverage of AWS services. There may be some inaccuracies as regards to AWS services. Do not use this guide for AWS architectural design.

The example deployment that this document describes uses the following components:

- Two EC2 instances for EMS primary and secondary nodes
- Amazon FSx file system for network file share
- RDS Microsoft SQL Server

Before deploying virtual machine (VM) instances in AWS, review the following:

- [Virtual private clouds \(VPC\)](#)
- [Control traffic to resources using security groups](#)

This deployment consists of the following steps:

1. Deploy VMs in AWS. See [To deploy VMs in AWS: on page 372](#).
2. Launch RDS Microsoft SQL Server. See [To launch RDS Microsoft SQL Server: on page 372](#).
3. Set up an FSx file system. See [To set up an FSx file system: on page 372](#).
4. Install EMS. See [To install EMS: on page 374](#).
5. Set up health check and Route53 DNS for failover. See [To set up health check and Route 53 DNS for failover: on page 375](#).
6. Restore a database (DB). See [To restore a DB: on page 376](#).

This example configures EMS nodes in the same zone. You can also deploy the EMS nodes in different zones.

To deploy VMs in AWS:

1. In the AWS console, search for EC2.
2. Select *Launch Instance*.
3. Configure the basic configuration fields as follows:
 - a. For *Application and OS Images*, select *Windows server* and *Machine Image*.
 - b. Select the desired instance type. See [Management capacity on page 27](#).
 - c. Create a key pair if you need to be able to access the machine via RDP. See [Create a key pair using Amazon EC2](#).
4. Configure *Network Settings* as follows:
 - a. Assign the desired VPC and subnet.
 - b. Enable *Auto-assign public IP*.
 - c. Select the desired security group.
5. Configure other settings as desired, then launch the instance. This example uses default settings.
6. Repeat steps 2-5 to launch the secondary EMS instance.
7. For both EMS instances, configure security group inbound ports and allow access to the following ports:

Port	Usage
8013	Endpoint connection
443	EMS web access
8015	FortiGate Fortinet Security Fabric connection
10443	FortiClient package deployment
8443	Chromebook connection

To launch RDS Microsoft SQL Server:

1. In the AWS console, search for RDS.
2. Select *Create Database*. This example uses *Standard create*.
3. For *Engine options*, select *Microsoft SQL Server*. This example uses SQL Server Standard Edition.
4. Configure settings as follows:
 - a. Set the DB instance identifier.
 - b. Set the desired master username and password.
 - c. For SQL instance compute configuration, see [Management capacity on page 27](#). This example uses *Standard classes*.
5. Configure *Storage settings* and *Availability & Durability* as required.
6. Configure *Connectivity Settings* as follows:
 - a. Select *Don't connect to an EC2 compute resource*.
 - b. Assign a VPC and subnet to the instance. This example enables public access.
 - c. Assign a security group with inbound access enabled for the SQL port. In this example, the port is 1433.
7. Configure other settings as desired, and create the DB.

To set up an FSx file system:

Sharing files between EMS nodes relies on network fileshares. AWS FSx uses Active Directory (AD) for setup. This example uses a self-managed Microsoft AD and an EC2 AD instance set up on AWS which also acts as a DNS server.

Both EMS nodes can reach AD and resolve FQDN. Ensure that the AD domain controller and DNS server are reachable from FSx. Before setup, see [Prerequisites for using a self-managed Microsoft AD](#).

Both EMS nodes should be able to reach the FSx fileshare. In this example, FSx and the EMS nodes are in the same VPC and subnet. If they are in different VPCs, establish VPC peering for reachability. See [Create a VPC peering connection](#).

1. In the AWS console, search for FSx.
2. Create a new file system:
 - a. Select *Amazon FSx for Windows File Server*.
 - b. Configure a desired name for the file system. This example uses Single-AZ 2.
 - c. For *Storage type*, select *SSD*.
 - d. Enter the desired storage capacity.
 - e. Configure *Network & Security* as follows:
 - i. Assign a VPC and subnet to the file system.
 - ii. Select the desired security group. Ensure that the inbound ports are opened as [Prerequisites for using a self-managed Microsoft AD](#) describes.
 - f. Configure Windows authentication as follows:
 - i. For user authentication, select *Self-managed Microsoft Active Directory*.
 - ii. In the *Active Directory domain name* field, enter the AD domain name.
 - iii. In the *DNS server IP addresses* field, enter the DNS server IP address.
 - iv. In the *Service account username* and *Service account password* fields, enter credentials for the desired account with delegated permissions. See [Prerequisites for using a self-managed Microsoft AD](#) for service account permissions.

Active Directory domain name

This is the fully qualified domain name of your self-managed directory

aws-emsha.com

DNS server IP addresses

The IPv4 DNS server IP addresses for your domain. At least one IP address is required.

172.31.16.111

10.0.0.2 - optional

Service account username

The username of the service account your resource will use to join your Active Directory. Do not include a domain prefix or suffix. For example, for 'EXAMPLE/ADMIN', exclude the domain prefix 'EXAMPLE'.

administrator

Service account password

Provide the password for the service account you are using to join this resource to your Active Directory.

Maximum of 128 characters.

Confirm password

Organizational Unit (OU) within which you want to join your file system - optional [Info](#)

Provide the distinguished path name of the OU here

OU=org,DC=example,DC=com

Ensure that the service account provided has permissions delegated to the above OU or to the default OU if none is provided.

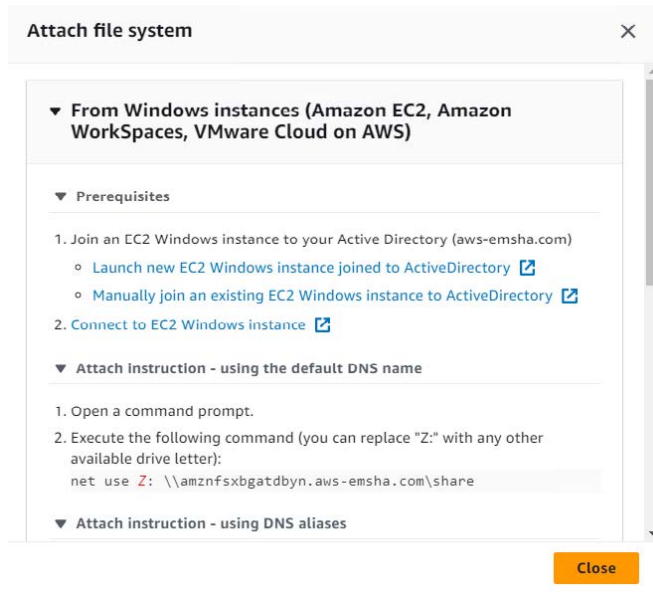
Delegated file system administrators group - optional [Info](#)

Name of the group in your Active Directory that can administer your file system. By default, this is 'Domain Admins'.

Domain Admins

- g. Configure other settings as desired, then create the file system.

3. To obtain the fileshare URL, highlight the FSx and select *Attach*. In this example, the URL is `file:///amznfsxbgatdbyn.aws-emsha.com/share`. You use this URL during EMS installation.



To install EMS:

During EMS installation, the installer mounts fileshares as the W:\ drive. Ensure that the W:\ drive is free on all EMS nodes.

- Start the EMS installation on the primary node using the following command:
`FortiClientEndpointManagementServer_7.2.1._x64.exe SQLServer=<AWS_RDS_FQDN>
SQLPort=<AWS_SQL_port> PaaS=aws SQLUser=<SQL_user> SQLUserPassword=<SQL_password>
InstallSQL=0 ScriptDB=1 FileStorageNic= FileStorageNicUser= FileStorageNicPass=`
The following table describes the command parameters:

Parameter	Description
PaaS=aws	Informs EMS that it will connect to an AWS RDS.
ScriptDB=1	Specifies that this is the primary node.
FileStorageNic	Fileshare path.
FileStorageNicUser	Fileshare username.
FileStorageNicPass	Fileshare password.



The `FileStorageNicUser` format is `domain\username`. The user should have read/write permissions to the share.

The following provides an example command: `SQLServer=mssqldb.awsmysql12345.us-east-1.rds.amazonaws.com SQLPort=1433 PaaS=aws SQLUser=awssql
SQLUserPassword=Passowrd123! InstallSQL=0 ScriptDB=1 FileStorageNic=
\\amznfsxbgatdbyn.aws-emsha.com\share FileStorageNicUser=aws-
emsha.com\Administrator FileStorageNicPass=)J(Sz2W5RKAoA4.Hgq87GH=q`

When installation completes, a mapped drive for the fileshare is created.



2. Start the EMS installation on the secondary node using the following command:

```
FortiClientEndpointManagementServer_7.2.1._x64.exe SQLServer=
mssqldb.awsmsql12345.us-east-1.rds.amazonaws.com SQLPort=1433 PaaS=aws SQLUser=
awssql SQLUserPassword=Password123! InstallSQL=0 ScriptDB=0 FileStorageNic=
\\amznfsxbgatdbyn.aws-emsha.com\share FileStorageNicUser=aws-
emsha.com\Administrator FileStorageNicPass=)J(Sz2W5RKAoA4.Hgq87GH=q
ScriptDB=0 indicates that this is the secondary node.
```

To set up health check and Route 53 DNS for failover:

1. In AWS, search for and select Route 53.
2. From the navigation pane, select *Health Checks*.
3. Click *Create health check*.
4. Configure the following:
 - a. For *What to monitor*, select *Endpoint*.
 - b. For *Specify endpoint by*, select either option.
 - c. Enter the EMS primary node domain name or IP address.
 - d. From the *Protocol* dropdown list, select *TCP*.
 - e. In the *Port* field, enter 8013.

Configure health check ?

Route 53 health checks let you track the health status of your resources, such as web servers or mail servers, and take action when an outage occurs.

Name ?

What to monitor ☒ Endpoint ?
☐ Status of other health checks (calculated health check)
☐ State of CloudWatch alarm

Monitor an endpoint

Multiple Route 53 health checkers will try to establish a TCP connection with the following resource to determine whether it's healthy.
[Learn more](#)

Specify endpoint by ☐ IP address ☒ Domain name

Protocol ?

Domain name * ?

Port * ?

Advanced configuration

URL ?

- f. Create the health check.
5. Repeat steps 3-4 for the EMS secondary node.
 6. Check the status on the health check page. The primary node status is healthy and the secondary node status is unhealthy.

7. You must configure the FQDN to use for EMS HA in a Route 53-hosted zone to effectively send traffic to the correct EMS based on availability. In this example, the FQDN is `fctemsha.aws-emsha.com`. You can configure this on EMS in System Settings > EMS Settings. For this example, configuration is as follows:
 - a. Select to create a hosted zone, and enter the domain name.
 - b. For *Type*, select *Public hosted zone*. Create the zone. You should register the domain before adding it to a hosted zone. You can use AWS domain registration services to register a domain if not already registered.
 - c. After AWS creates the hosted zone, select the zone and create a record.
 - d. Configure the record:
 - i. From the *Record type* dropdown list, select *CNAME*.
 - ii. In the *Value* field, enter the primary EMS node domain name.
 - iii. From the *Routing policy* dropdown list, select *Failover*.
 - iv. From the *Failover record type* dropdown list, select *Primary*.
 - v. In the *Health check ID* field, enter the EMS primary node health check ID.
 - vi. In the *Record ID* field, enter a unique record ID.
 - e. Repeat steps c-i to create a record for the secondary EMS node. For *Failover record type*, select *Secondary*. In the *Health check ID* field, enter the EMS secondary node health check ID.

Records (4) [info](#)

Automatic mode is the current search behavior optimized for best filter results. [To change modes go to settings.](#)

Filter records by property or value

Type ▼ Routing pol... ▼ Alias ▼

<input type="checkbox"/>	Record name	Type	Routin...	Differ...	Alias	Value/Route traffic to	TTL (s...)	Health ...	Evalua...	f
<input type="checkbox"/>	aws-emsha.com	NS	Simple	-	No	ns-245.awsdns-30.com. ns-1133.awsdns-13.org. ns-594.awsdns-10.net. ns-1927.awsdns-48.co.uk.	172800	-	-	-
<input type="checkbox"/>	aws-emsha.com	SOA	Simple	-	No	ns-245.awsdns-30.com. a...	900	-	-	-
<input type="checkbox"/>	fctemsha.aws-emsha.com	CNAME	Failover	Primary	No	ec2-50-18-76-220.us-wes...	300	0deec825...	-	f
<input type="checkbox"/>	fctemsha.aws-emsha.com	CNAME	Failover	Secondary	No	ec2-54-176-164-51.us-we...	300	c6acc91f-...	-	f

To restore a DB:

When using an AWS RDS, EMS cannot manage database backups or restore backups generated from another EMS instance. Therefore, these functionalities are disabled during EMS installation. Taking a database snapshot from the AWS console and restoring the snapshot is the preferred backup and restore method. This deployment does not support restoring EMS using a regular SQL Server backup or upgrading EMS from an existing SQL server installation to an EMS with AWS RDS.

1. In the AWS console, go to the RDS DB.
2. From the navigation pane, select *Snapshots > Take snapshot*.
3. Select the desired DB instance.
4. Enter the desired snapshot name.
5. Select *Actions > Restore snapshot*.
6. Restoring a snapshot requires a new RDS DB instance creation. Follow the steps in [To launch RDS Microsoft SQL Server: on page 372](#).
7. Update EMS to point to the new RDS instance:
 - a. On the primary EMS node, go to `C:\Program Files (x86)\Fortinet\FortiClientEMS`.
 - b. Open `das.conf` in a text editor.
 - c. Update the *Server* field to the new RDS instance.
 - d. Save.
 - e. Open `db.conf` in a text editor.

- f. Update the *Server* field to the new RDS instance.

```
[config]
version=2
[Global]
IsPaaSDB=1
ProviderString=Provider=MSOLEDBSQL
IntegratedCredentials=Trusted_Connection=yes
SQLCredentials=Uid=[[User]];Pwd=[[Password]]
SQLCredentialsGOLANG=user id=[[User]];password=[[Password]]
Server=mssqldb.cfasrfkdnfurh.us-east-2.rds.amazonaws.com
```

- g. Save.
- h. Repeat steps a-g on the EMS secondary node.

Creating a support package

You can create a support package to provide to the [Fortinet technical support team](#) for troubleshooting. Creating a support package backs up your database but clears all sensitive username and password fields.

To create a support package:

1. Go to *Help > Create Support Package*.
2. In the *Password* field, enter a password that conforms to the displayed rules. The Fortinet technical support team needs this password to access the support package.
3. In the *Confirm Password* field, enter the password again.
4. Click *Create*.

Migrating to another EMS instance

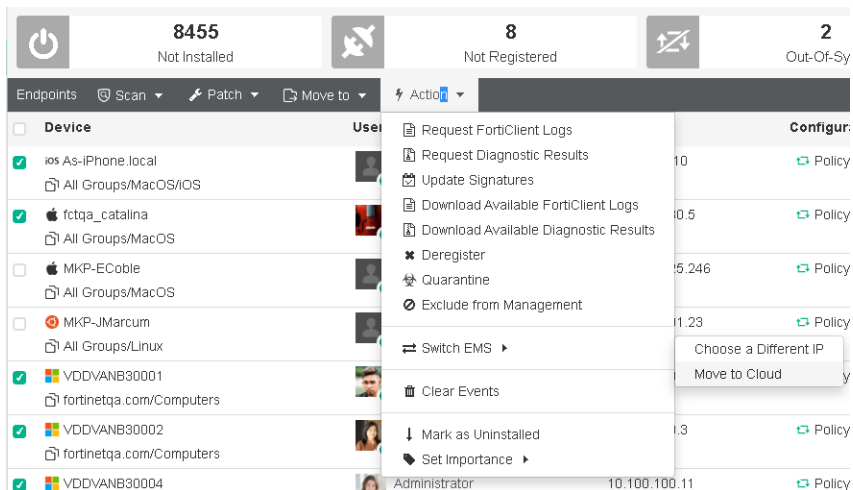
You can simply and efficiently move configurations, data, and endpoint connections between EMS instances without disrupting FortiClient endpoint functionality. This document describes migrating one EMS on-premise environment to another. This migration requires the following:

- 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 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 34](#) describes.
2. Back up the EMS A database as [To back up the database: on page 72](#) describes.
3. Restore the database on EMS B as [To restore the database: on page 72](#) 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.

 <div>0 Not Installed</div>		 <div>0 Not Registered</div>		 <div>0 Out-Of-Sync</div>		 <div>2 Security Risk</div>		 <div>0 Quarantined</div>	
<div>Endpoints</div>									
<input type="checkbox"/>	<div><div>As-iPhone local</div><div>Other Endpoints</div></div>	<div>A.R</div>	192.168.4.10	<div>Policy</div> <div>Default</div>	<div>EMS</div> <div>Migrating</div>	No Events			
<input type="checkbox"/>	<div><div>ftcqa_catalina</div><div>Other Endpoints</div></div>	<div>ftcqa</div>	192.168.130.5	<div>Policy</div> <div>Default</div>	<div>EMS</div> <div>Migrating</div>	No Events			
<input type="checkbox"/>	<div><div>VDDVNB30001</div><div>Other Endpoints</div></div>	<div>Administrator</div>	10.100.100.7	<div>Policy</div> <div>Default</div>	<div>EMS</div> <div>Migrating</div>	<div>VUL 5</div>			
<input type="checkbox"/>	<div><div>VDDVNB30010</div><div>Other Endpoints</div></div>	<div>Administrator</div>	10.100.100.17	<div>Policy</div> <div>Default</div>	<div>EMS</div> <div>Migrating</div>	<div>VUL 94</div>			

- Shut down EMS A.
- 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](#).
- 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](#).

Change log

Date	Change Description
2023-06-12	Initial release.



www.fortinet.com

Copyright© 2023 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 General Counsel, 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.