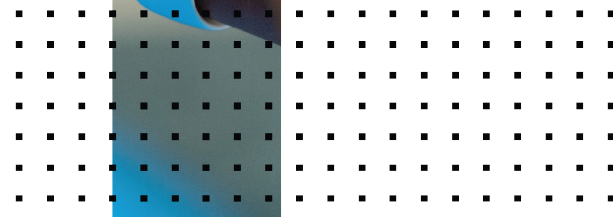


Administration Guide

FortiClient EMS 7.0.7



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

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

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



February 20, 2024

FortiClient EMS 7.0.7 Administration Guide

04-707-706783-20240220

TABLE OF CONTENTS

Introduction	9
FortiClient EMS components	9
Documentation	11
Getting started	12
Getting started with managing Windows, macOS, and Linux endpoints	12
Deploying FortiClient software to endpoints	12
Pushing configuration information to FortiClient	13
Relationship between FortiClient EMS, FortiGate, and FortiClient	14
Getting started with managing Chromebooks	18
Configuring FortiClient EMS for Chromebooks	18
Configuring the Google Admin console	18
Deploying a profile to Chromebooks	19
How FortiClient EMS and FortiClient work with Chromebooks	19
Installation preparation	20
System requirements	20
License types	20
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 FortiGates are connected to EMS	29
FortiClient Telemetry security features	31
Server readiness checklist for installation	31
Upgrading from an earlier FortiClient EMS version	32
Upgrading EMS and FortiClient	32
Upgrading EMS from an earlier version	33
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	43
Licensing FortiClient EMS	44

Licensing EMS by logging in to FortiCloud	44
Uploading a license file	48
Licensing EMS in an air-gapped network	48
License status	50
Help with licensing	50
Specifying different ports	50
Upgrading Microsoft SQL Server Express to Microsoft SQL Server Standard or Enterprise	51
Uninstalling FortiClient EMS	52
Installation and setup for managing Chromebooks	53
Google Admin Console setup	53
Service account credentials	60
Verifying ports and services and connection between EMS and FortiClient	66
Ports and services	66
Connectivity between EMS and FortiClient	66
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	90
Managing endpoints	102
Group assignment rules	109
Group assignment rule types	109
Managing group assignment rule priority levels	110
Adding a group assignment rule	111
Enabling/disabling a group assignment rule	112
Deleting a group assignment rule	112
Google Domains	112
Adding a Google domain	113
Viewing domains	113
Editing a domain	116
Deleting a domain	116

Deployment & Installers	117
Manage Deployment	117
Preparing the AD server for deployment	117
Preparing Windows endpoints for FortiClient deployment	119
Creating a deployment configuration	119
Managing deployment configuration priority levels	120
Enabling/disabling a deployment configuration	121
Deleting a deployment configuration	122
Deploying initial installations of FortiClient (macOS)	122
Deploying FortiClient upgrades from FortiClient EMS	122
Deploying different installer IDs to endpoints using the same deployment package	122
FortiClient Installer	123
Adding a FortiClient deployment package	123
Viewing deployment packages	127
Deleting a FortiClient deployment package	127
Endpoint Policy & Components	128
Manage Policies	128
Adding an endpoint policy	128
Editing an endpoint policy	130
Deleting an endpoint policy	130
Enabling/disabling an endpoint policy	130
Managing endpoint policy priority levels	130
Editing endpoint policy view	132
Managing FortiClient based on AD user/user groups	132
CA Certificates	134
On-fabric Detection Rules	136
Chromebook Policy	140
Endpoint Profiles	141
Editing a default profile	141
Creating a new profile	141
Adding a new Chromebook profile	142
Managing profiles	142
Editing a profile	142
Cloning a profile	143
Syncing profile changes	143
Editing sync schedules	143
Exporting a profile	143
Importing a profile	144
Deleting a profile	144
Remote Access	144
SSL VPN	145
IPsec VPN	149
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	160
Using a browser as an external user agent for SAML authentication in an SSL VPN	162

connection	
Per-machine prelogon VPN connection without user interaction	164
Autoconnect on logging in as an Entra ID user	168
ZTNA Destinations	173
Web Filter	174
Importing a Web profile from FortiOS or FortiManager	180
Enabling and disabling Safe Search	182
Support banned word check in URL	183
Vulnerability Scan	185
Malware Protection	188
AntiVirus Protection	188
Anti-Ransomware	191
Antiexploit	192
Cloud-Based Malware Detection	192
Removable Media Access	193
Exclusions	194
Other	195
Sandbox	197
Firewall	200
System Settings	201
Configuring identity compliance for endpoints	208
XML Configuration	210
Creating a profile with XML	210
Importing a profile from an XML file	211
Configuring encrypted ZTNA rules	211
Zero Trust Tags	214
Zero Trust Tagging Rules	214
Adding a Zero Trust tagging rule set	214
Editing a Zero Trust tagging rule set	215
Deleting a Zero Trust tagging rule	216
Importing and exporting a Zero Trust tagging rule set	216
Uploading signatures for FortiGuard Outbreak Alerts service	216
Managing tags	217
Zero Trust tagging rule types	217
Zero Trust Tag Monitor	222
FortiOS dynamic policies using EMS dynamic endpoint groups	224
Configuring FortiOS dynamic policies using EMS dynamic endpoint groups	224
Restricting VPN access to rogue/non-compliant devices with Security Fabric	228
Fabric Device Monitor	234
FortiGuard Outbreak Alerts	235
Software Inventory	237
Applications	237
Hosts	238
Quarantine Management	240
Files	240
Viewing quarantined files	240

Allowlisting quarantined files	242
Configuring quarantine management	242
Allowlist	243
Viewing allowlisted files	243
Editing file descriptions	244
Deleting a file from the allowlist	244
Administration	245
Administrators	245
Viewing users	245
Configuring user accounts	246
Activating a disabled account	247
Admin roles	248
Adding an admin role	248
Cloning an admin role	248
Deleting admin roles	249
Admin role permissions reference	249
Configuring User Settings	252
Fabric Devices	252
Configuring EMS to share tagging information with multiple FortiGates	254
SAML SSO	255
Licenses	258
Log Viewer	258
Generate Diagnostic Logs	258
Marking all endpoints as uninstalled	258
User Management	260
Authorized User Groups	260
Verified Users	261
Unverified Users	263
Local users	263
SAML Configuration	264
Invitations	265
Configuring user verification with an LDAP server for authentication	266
Configuring user verification with SAML authentication and an LDAP domain user account	267
System Settings	276
Configuring EMS settings	277
Adding an SSL certificate to FortiClient EMS	281
Adding an SSL certificate to FortiClient EMS for Chromebook endpoints	282
Generating a QR code for centrally managing FortiClient (Android) and (iOS) endpoints	283
Configuring Logs settings	284
Configuring FortiGuard Services settings	285
Alerts	287
Configuring EMS Alerts	287
Configuring Endpoint Alerts	288
Configuring SMTP Server settings	288

Viewing alerts	290
Custom Messages	290
Customizing the endpoint quarantine message	290
Customizing Web Filter messages	291
Feature Select	292
Multitenancy	295
Enabling and configuring multitenancy	295
Global and per-site configuration	296
Global configuration	296
Site level configuration	297
Left pane with multitenancy enabled	298
Editing a site	301
Adding a multitenancy administrator	301
Logging into EMS with multitenancy enabled	303
Redundancy	304
Fabric connection setup using traffic manager	310
Fabric connection setup using FortiGate as a load balancer	312
Creating a support package	315
Migrating to another EMS instance	316
Limitations	317
FortiClient EMS API	318
Change log	319

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.

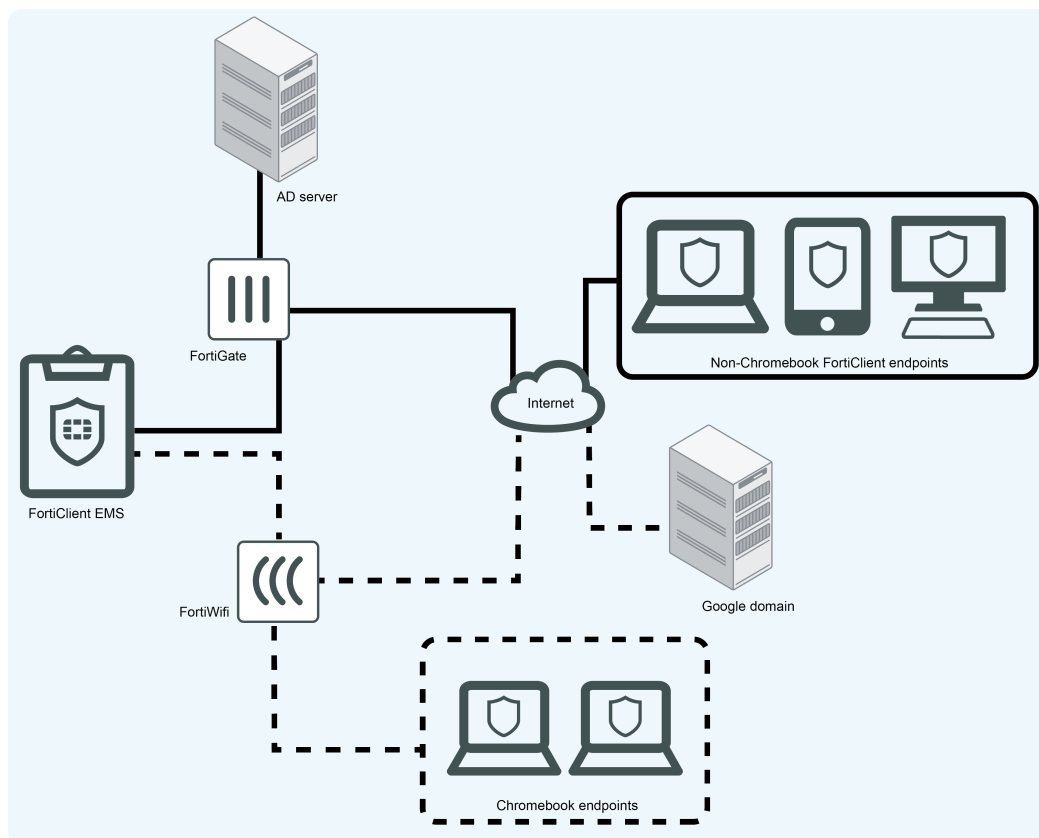
FortiClient EMS also provides the infrastructure to install and manage the FortiClient Web Filter extension on Google Chromebook endpoints. FortiClient protects endpoint users by working with FortiClient EMS to filter web content endpoint users view on Google Chromebooks.

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



An informative video introducing you to FortiClient EMS is available in the [Fortinet Video Library](#).

Documentation

You can access FortiClient EMS documentation from the [Fortinet Document Library](#).

The FortiClient EMS documentation set includes the following:

Document	Description
<i>Administration Guide</i>	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.
<i>New Features Guide</i>	Describes new features and enhancements in FortiClient EMS for the release, including configuration information.
<i>QuickStart Guide</i>	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.
<i>Release Notes</i>	Lists any known issues and limitations for the release. This document also defines supported platforms and minimum system requirements.
<i>REST API</i>	The FortiClient EMS API allows you to perform configuration operations on EMS. You can view the API documentation on the <i>FortiAPI</i> tab on FNDN.
<i>Upgrade Paths</i>	Provides upgrade path information for different versions of FortiClient EMS.
<i>Compatibility Chart</i>	Provides compatibility information for different versions of FortiClient EMS and other Fortinet products.

Getting started

Getting started with managing Windows, macOS, and Linux endpoints

Deploying FortiClient software to endpoints

Following is an overview of how to add endpoints to FortiClient EMS and configure FortiClient EMS to deploy FortiClient to endpoints.

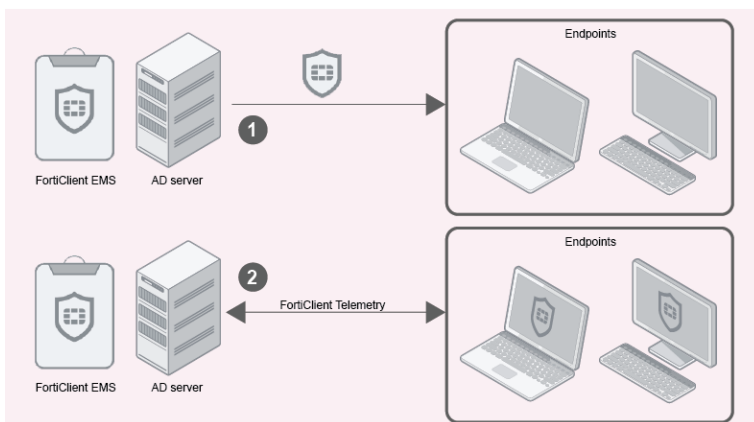
You can deploy FortiClient to endpoints using Active Directory (AD) servers and workgroups. There are differences between using AD servers and workgroups.

When using an AD server, you can deploy an initial installation of FortiClient (Windows) to endpoints, but you cannot deploy an initial installation of FortiClient (macOS). After FortiClient for Windows or macOS installs on endpoints and endpoints are connected to FortiClient EMS, you can deploy upgrades, uninstallations, and replacements of both FortiClient for Windows and macOS using AD servers.

When using workgroups, you cannot deploy an initial installation of FortiClient to endpoints. However, after FortiClient installs on endpoints and endpoints are connected to FortiClient EMS, you can use workgroups to uninstall and update FortiClient on endpoints.

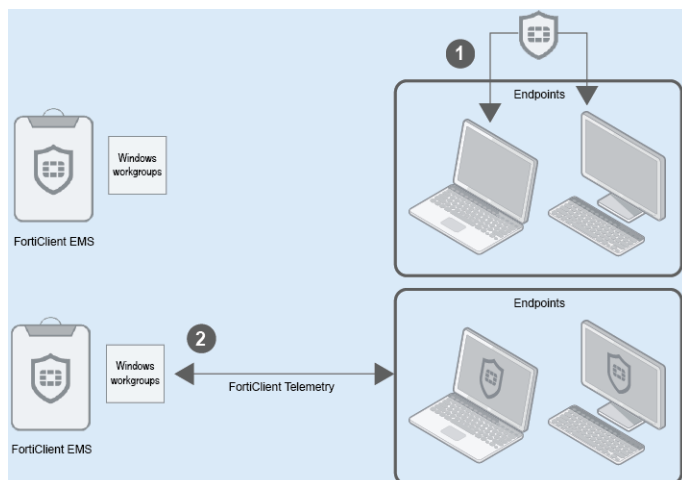
The following shows a deployment of FortiClient using FortiClient EMS with an AD server:

1. Deploy FortiClient from FortiClient EMS using an AD server to the desired endpoints.
2. The endpoints now have FortiClient installed and FortiClient Telemetry is connected to FortiClient EMS.



The following shows a deployment of FortiClient (Windows) using FortiClient EMS with Windows workgroups:

1. You cannot use workgroups with FortiClient EMS to initially install FortiClient on endpoints. You must install FortiClient directly on endpoints. You can configure deployment packages that endpoint users can download to install FortiClient on endpoints. See [Viewing deployment packages on page 127](#).
2. The endpoints now have FortiClient installed and FortiClient Telemetry is connected to FortiClient EMS.



To deploy FortiClient software to endpoints:

1. Add endpoints with an AD server or Windows workgroups. See [Adding endpoints on page 88](#).
Endpoints added using an AD service display in *Endpoints > Domains*, and endpoints added using Windows workgroups display in *Endpoints > Workgroups*. You can install FortiClient on endpoints using an AD server without connecting FortiClient to FortiClient EMS as long as the username and password are correct for the applied deployment configuration in *Deployment* in FortiClient EMS. You can only use workgroups to upgrade or uninstall FortiClient if it is already installed on the endpoints and connected to FortiClient EMS. You cannot use workgroups for initial installations of FortiClient. When using workgroups, the deployment configuration credentials in *Deployment* in FortiClient EMS are not taken into account.
2. Create a FortiClient deployment package in FortiClient EMS. See [Adding a FortiClient deployment package on page 123](#).
3. Create a profile that includes the desired configuration information for FortiClient software on endpoints. See [Creating a new profile on page 141](#).
4. Prepare domains and workgroups for deployment. See [Preparing the AD server for deployment on page 117](#).
5. Create a deployment configuration with the desired deployment package. Configure the deployment configuration for the desired workgroup, domain, endpoint group, or organizational group. See [Creating a deployment configuration on page 119](#).
Depending on the selected profile's configuration, FortiClient installs on the endpoints to which the profile is applied. After FortiClient installation, the endpoint connects FortiClient Telemetry to FortiClient EMS to receive the profile configuration and complete endpoint management setup.
6. Monitor the installation process using the *Endpoints* pane. See [Viewing the Endpoints pane on page 90](#).

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 141](#).

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 128](#). 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 90](#).

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 7.0 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.



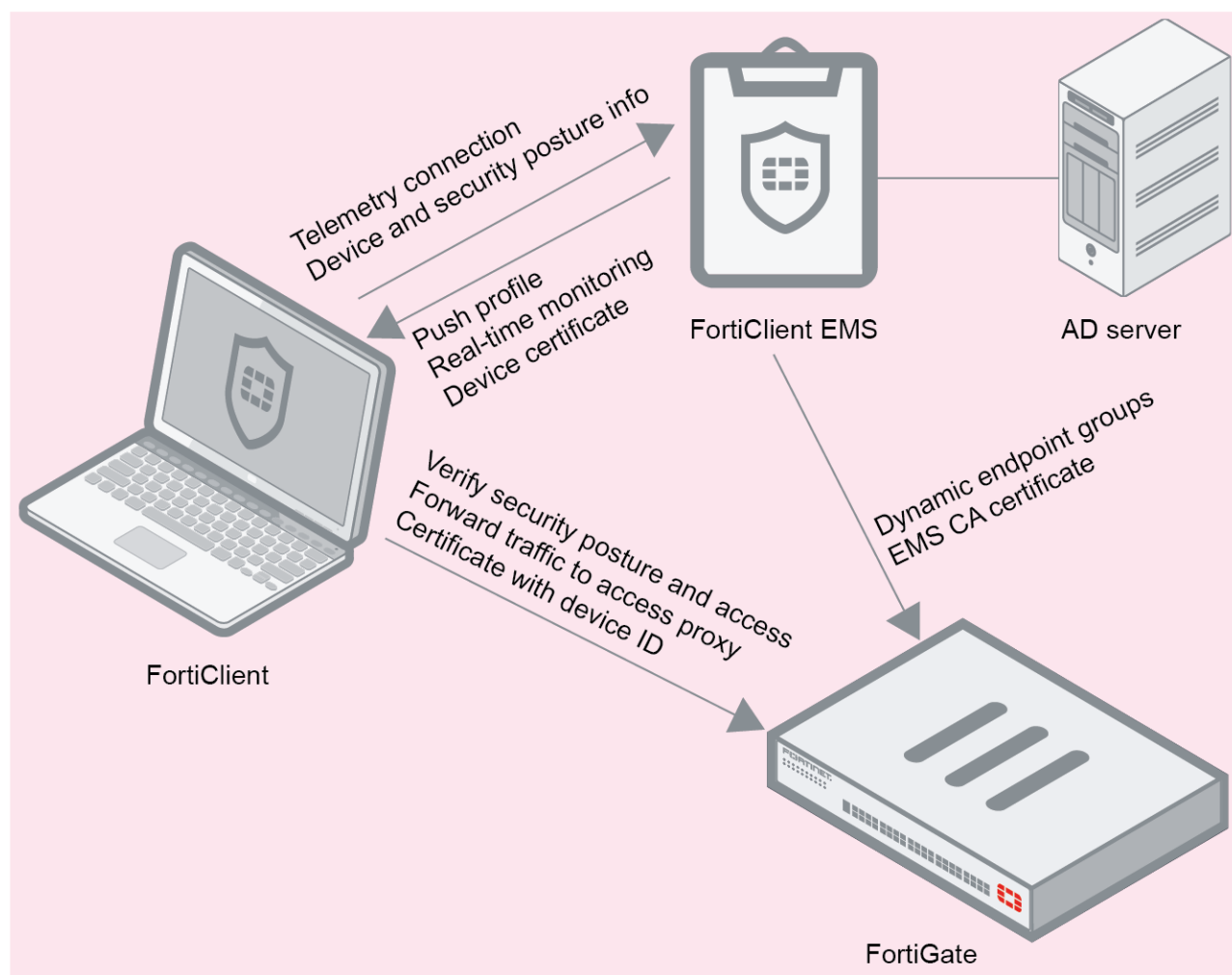
FortiGate does not provide configuration information for FortiClient and the endpoint. An administrator must configure FortiClient using an EMS endpoint policy.

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 141](#).
 - 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 214](#).
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 224](#).



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:

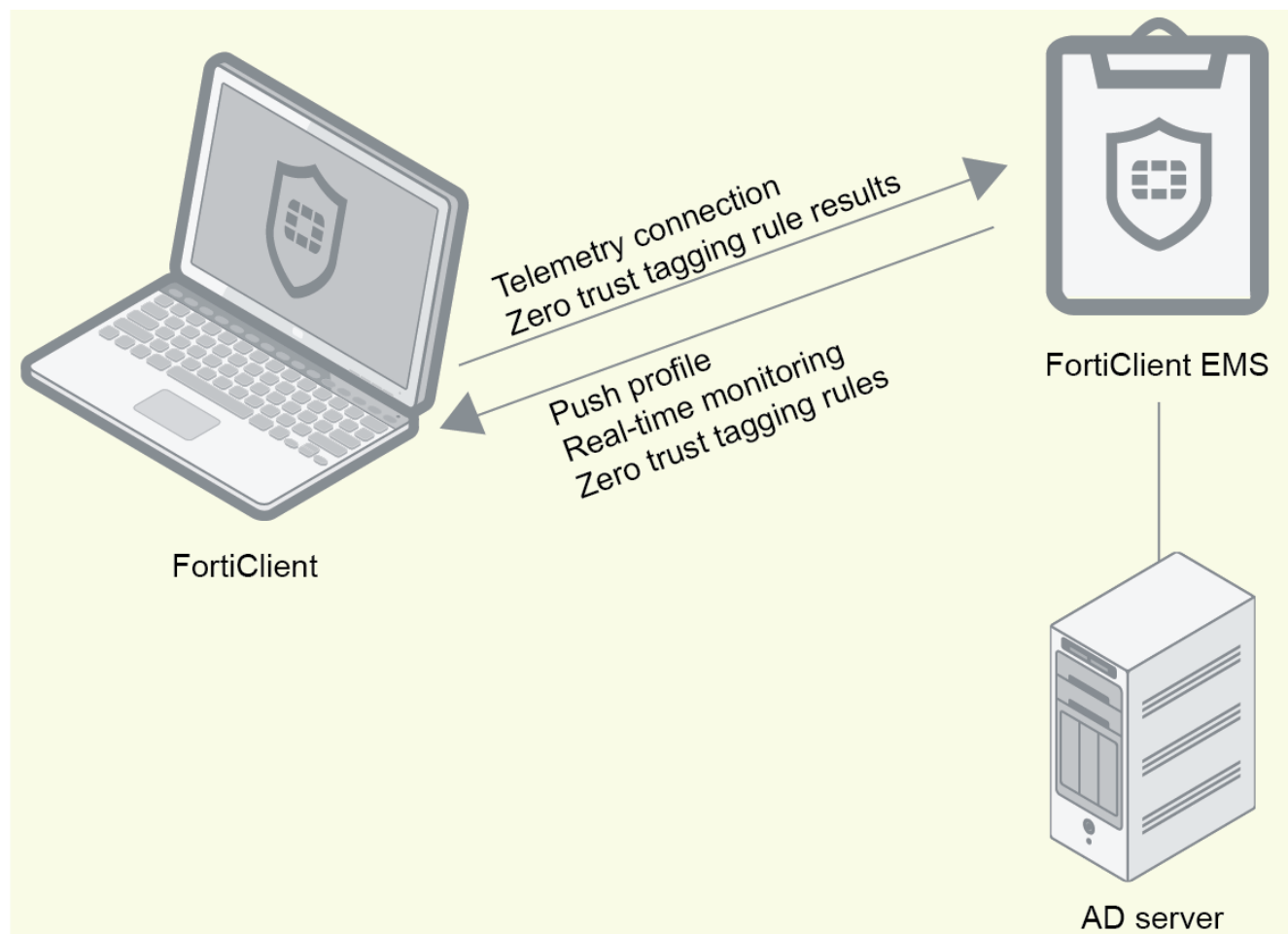
- Logs
- Windows host events

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 105](#) 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 for Chromebook endpoints on page 282](#).
3. Configure FortiClient EMS settings. See [System Settings on page 276](#).
4. Configure user accounts and permissions. See [Administrators on page 245](#). 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 61](#).
5. Disallow incognito mode. See [Disallowing incognito mode on page 58](#).

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.

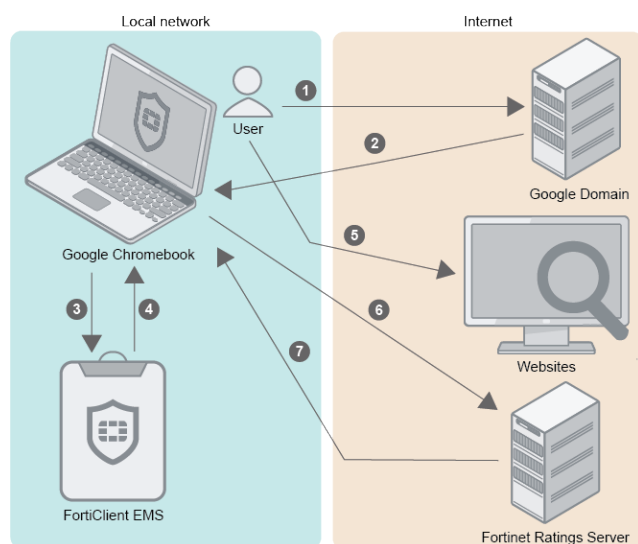
To deploy a profile to Chromebooks:

1. Add the Google domain. See [Adding a Google domain on page 113](#).
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 142](#).
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 140](#).
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 113](#).

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.



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 indefinitely. The trial license does not include management of Chromebook endpoints. The trial license includes the same functionality as the zero trust network access license and does not include FortiClient Cloud Sandbox (SaaS) 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. 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 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 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 260](#). 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	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.

Communication	Usage	Protocol	Port	Incoming/Outgoing	How to customize
Active Directory server connection	Retrieving workstation and user information	TCP	389 (LDAP) or 636 (LDAPS)	Outgoing	GUI
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	Usage	Protocol	Port	Incoming/Outgoing	How to customize
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
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 281 .	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.	EMS and SQL Server can be installed on the same Windows Server machine, or two different Windows Server machines.
5000 to 50000	Enterprise or Standard	EMS and SQL Server can be installed on the same Windows Server machine, or two different Windows Server machines.
More than 50000	Enterprise or Standard	EMS and SQL Server must be installed 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 is managing, 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 FortiGates are connected to 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

Number of managed endpoints	Number of virtual CPUs	Memory (RAM) (in GB)	Suggested keep alive interval
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 run 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
150000 to 250000	32	26	34	60	240 seconds

Hardware configuration when FortiGates are connected to EMS

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

- EMS and SQL Server run on the same Windows Server machine
- Up to 100 FortiGates connected to the EMS
- Up to 20 Zero Trust tags 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)

Number of managed endpoints	Number of virtual CPUs	Memory (RAM) (in GB)	Suggested keep alive interval
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 run on different Windows Server machines
- Up to 100 FortiGates connected to the EMS
- Up to 20 Zero Trust tags 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 run on the same Windows Server machine
- Up to 300 FortiGates connected to the EMS
- Up to 20 Zero Trust tags 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 run on different Windows Server machines
- Up to 300 FortiGates connected to the EMS
- Up to 20 Zero Trust tags 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 closes after protocol exchanges between parties 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 277](#).

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 7.0.7 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.

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 122](#).
 - 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 33](#) describes.
 - ii. Deploy FortiClient upgrade from 6.2 to 6.4 from EMS as [Deploying FortiClient upgrades from FortiClient EMS on page 122](#) describes.
 - iii. Upgrade EMS from 6.4 to 7.0 as [To upgrade EMS from an earlier version: on page 33](#) describes..
 - iv. Deploy FortiClient upgrade from 6.4 to 7.0 from EMS as [Deploying FortiClient upgrades from FortiClient EMS on page 122](#) 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 33](#) describes.
 - iii. Deploy the latest FortiClient version to endpoints as [Manage Deployment on page 117](#) describes.

Upgrading EMS from an earlier version

To upgrade EMS from an earlier version:

1. Close FortiClient EMS.
2. Install FortiClient EMS 7.0.7 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 for Chromebook endpoints on page 282](#). 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 20](#)
- 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.



EMS does not currently support high availability. For increased data reliability, consider Microsoft SQL Server redundancy. See [Microsoft's documentation](#) for details.



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_7.0.7.<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

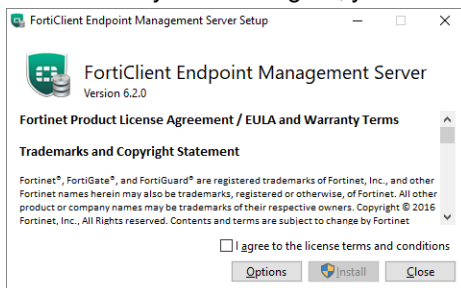
- Apache HTTP server



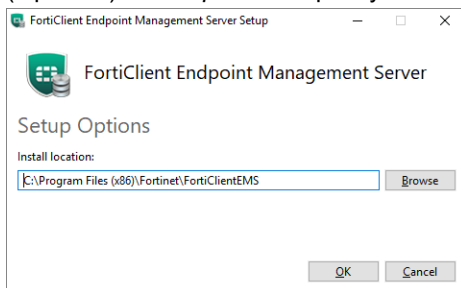
Installing FortiClient EMS requires local administrator rights. Internet access is recommended, but optional, during installation. SQL Server may require some dependencies to be downloaded over the internet. EMS also tries to download information about FortiClient signature updates from FortiGuard.

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.

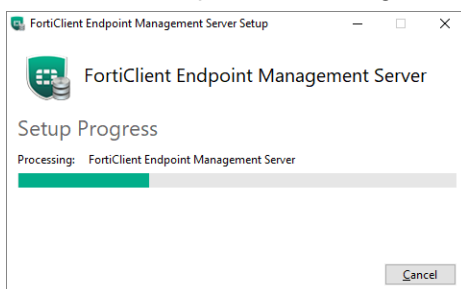


4. (Optional) Click *Options* to specify a custom directory for the FortiClient EMS installation.

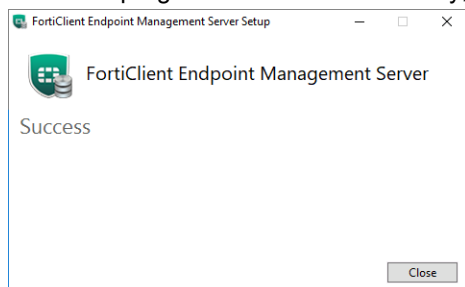


- a. Click *Browse* to locate and select the custom directory.
 - b. Click *OK* to return to the installation wizard.
5. Click *Install*.

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 use 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_7.0.7.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_7.0.7.XXXX_x64.exe SQLServerInstance= SQLService=<instance_name> SQLCmdlineOptions="/INSTANCENAME=" InstallSQL=0 ScriptDB=1</pre>
Local named instance using SQL authentication	<pre>FortiClientEndpointManagement_7.0.7.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_7.0.7.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_7.0.7.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

If you are using a separately set up remote SQL server, you must set the recovery mode to simple instead of full.

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_7.0.7.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_7.0.7.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_7.0.7.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 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, 127.0.01, <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.
InstallSQL	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 is listening 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.

Option	Description
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> .
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 DBLoginTimeout 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 will not perform well. In that case, you should 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.

Option	Description
DBQueryTimeout	Enter the database query timeout value in seconds. During installation, a SQL query is used 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. 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 completes.
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_7.0.7.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_7.0.7.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_7.0.7.XXXX_x64 SQLCmdlineOptions="/INSTANCENAME=FCEMS
/INSTANCEDIR=<desired_directory>"
```

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

```
FortiClientEndpointManagement_7.0.7.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_7.0.7.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:

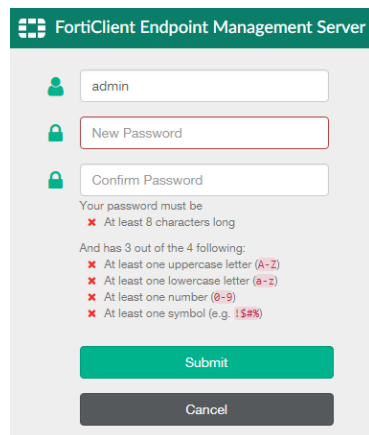
```
FortiClientEndpointManagement_7.0.7.XXXX_x64 InstallFolder=c:/sqlserver SQLServer=WIN-0888
SQLServerInstance= SQLService=MSSQLSERVER
```

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 to EMS.
 - If you imported a secure SSL certificate to EMS, but the *Use SSL Certificate for Endpoint Control* option is disabled.Configure certificate-related and other options by going to *System Settings*.

Configuring EMS after installation

You can configure an 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 fully qualified domain name (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 would require 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 not connected to 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 20](#).

You can activate, upgrade, or renew a FortiClient EMS license in the following ways:

Method	Description
Licensing EMS by logging in to FortiCloud on page 44	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	Upload a license file to EMS. You must use this backup licensing method only if you cannot license EMS by logging into FortiCloud.

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 7.0 license files. You cannot use this option to activate, upgrade, or renew an EMS 7.0 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 & Start Trial*. 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 : ITF0017
 Contract Registration Code : 3922UJ

FortiCloud Services

ASSET MANAGEMENT Register Product

Registration Code

Please enter your product serial number, service contract registration code or license certificate number to start the registration: *

3922UJ

End User Type

The product will be used by

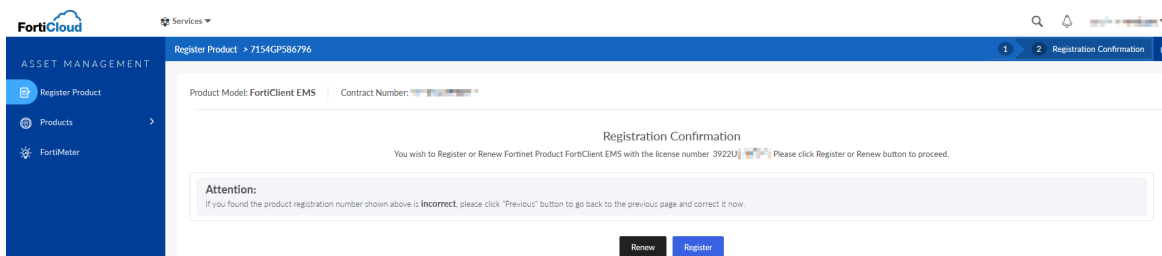
☒ A government user

☐ A non-government user

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. For example, if you have already applied an Endpoint Protection Platform (EPP) license to your EMS, you can apply another license type, such as a zero trust network access (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 will not be able to 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 FortiCloud. 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 must 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*.



PLEASE REMEMBER TO REGISTER YOUR CONTRACT REGISTRATION CODE

Service Entitlement Summary

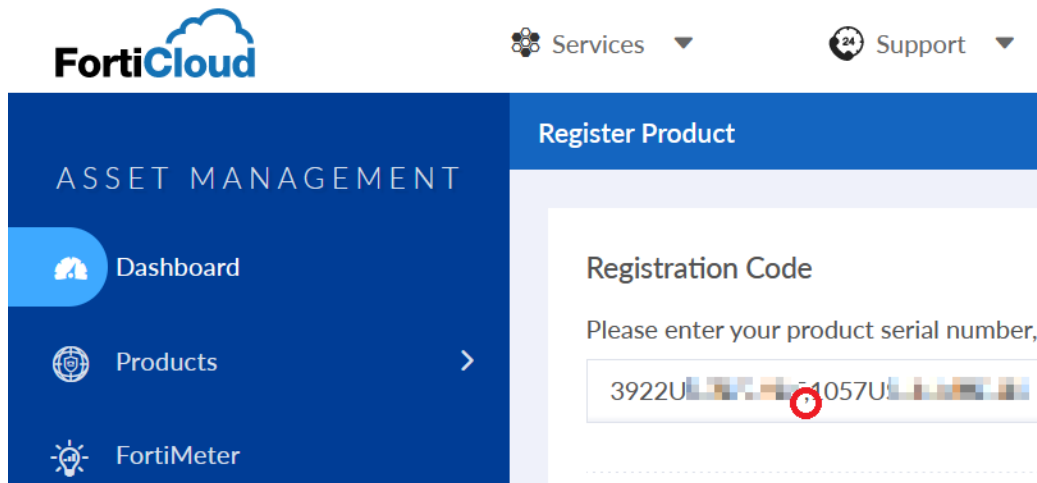
Date : April 22, 2020
Purchase Order Number : ITF001
Contract Registration Code : 3922U



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 [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 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 will not be able to 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 FortiCloud. 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 FortiCloud.

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

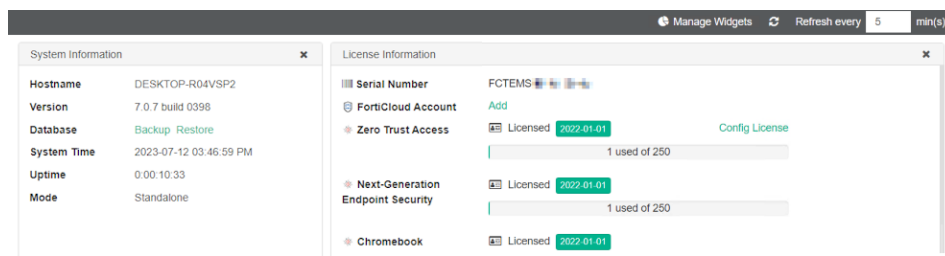
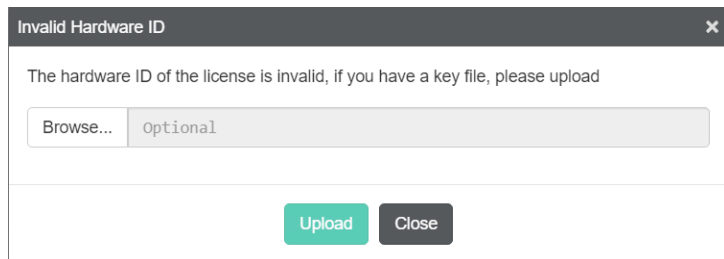
If you are deploying EMS in an air-gapped or isolated network where EMS cannot access the Internet, you can configure EMS to receive updates from FortiManager to deploy to FortiClient. In offline mode, FortiManager allows export and import of FortiGuard packages from FortiManager for provisioning as a FortiGuard distribution server. You can export FortiGuard packages from an online FortiManager to import to an offline FortiManager that will provide 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 must 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 will install EMS. They provide you with a key file.
2. Install EMS. See [Installing FortiClient EMS on page 34](#).
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 *Dashboard > 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 (SaaS) integration, and for Chromebook endpoint management. Each license's status can change. The options are:

License status	Description
Unlicensed	If you just installed FortiClient EMS, EMS is unlicensed by default. Log in to your FortiCloud account or upload a license file to update the license status.
Non-expired license	You can upgrade the license on your FortiCloud account.
Expired license	<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 45](#) 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
ClientDownloadPort	Download FortiClient from FortiClient EMS
RemoteManagementPort	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. You 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 completes, 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:

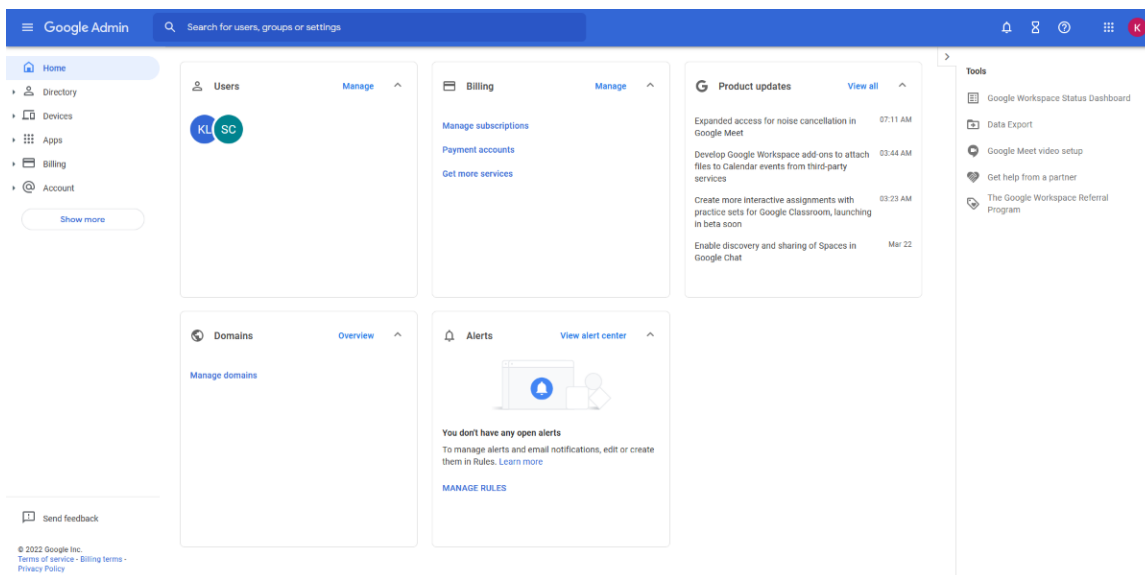
1. Log into the Google Admin console. See [Logging into the Google Admin console on page 53](#).
2. Add the FortiClient Web Filter extension. See [Adding the FortiClient Web Filter extension on page 54](#).
3. Configure the FortiClient Web Filter extension. See [Configuring the FortiClient Web Filter extension on page 54](#).
4. Add the root certificate. See [Adding root certificates on page 55](#).
5. Disable access to Chrome developer tools. See [Disabling access to Chrome developer tools on page 57](#).
6. Disallow incognito mode. See [Disallowing incognito mode on page 58](#).
7. Disable guest mode. See [Disabling guest mode on page 58](#).
8. Block the Chrome task manager. See [Blocking the Chrome task manager on page 59](#).
9. Verify the FortiClient Web Filter extension. See [Verifying the FortiClient Web Filter extension on page 59](#).



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.



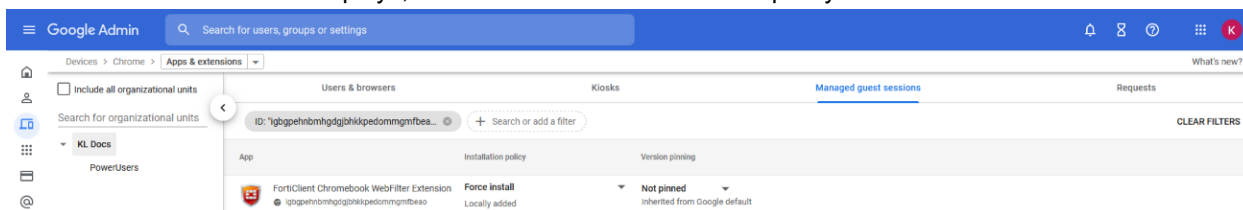
Adding the FortiClient Web Filter extension



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](#).

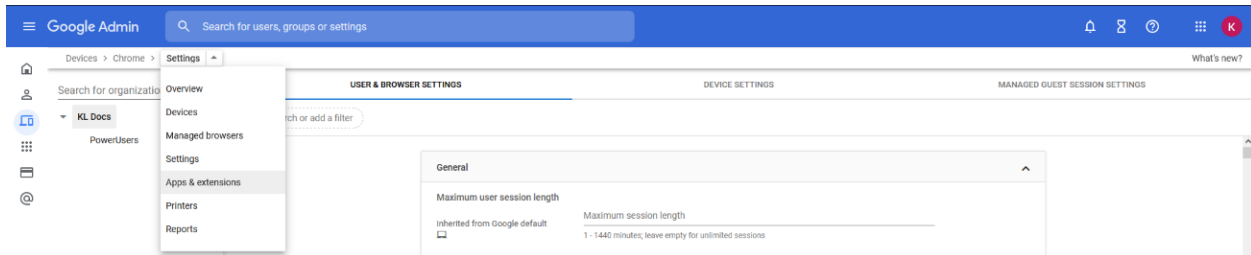
To configure the FortiClient Web Filter extension:

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 apps.

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 for Chromebook endpoints on page 282](#).

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:

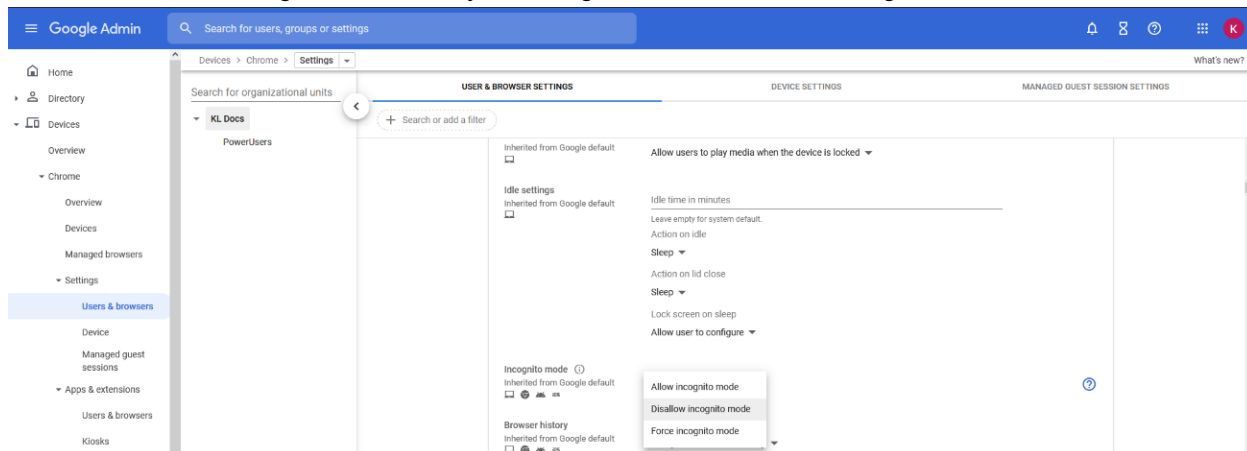
1. In the Google Admin console, go to *Devices > Chrome > Settings > Users & browsers*.
2. On the left, select the organization that contains the desired users or enrolled browsers. To select all users and browsers, select the top-level organization. Otherwise, select a child.
3. In *User & Browser Settings*,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

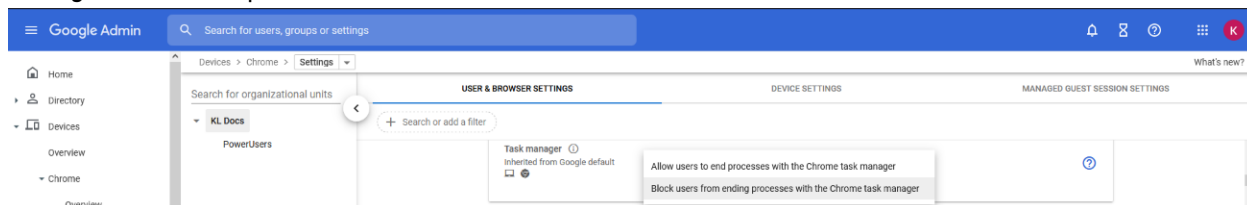
1. In the Google Admin console, go to *Devices > Chrome > Settings > Device*.
2. On the left, select the organization that contains the desired users or enrolled browsers. To select all users and browsers, select the top-level organization. Otherwise, select a child.
3. Under *Sign-in settings*, for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



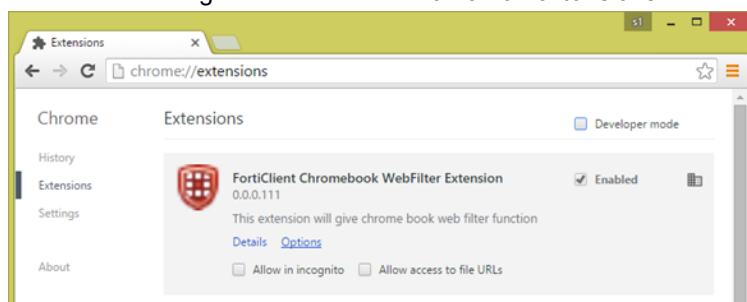
4. Click Save.

Verifying the FortiClient Web Filter extension

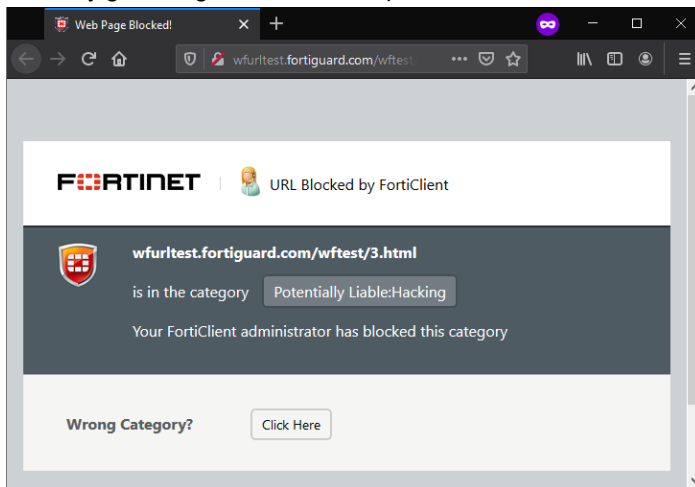
After you add the Google domain to FortiClient EMS, the Google Admin console automatically pushes the FortiClient Web Filter extension to the Chromebooks when users log into the Google domain. You can verify the feature has become available on the Chromebooks.

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 that the extension blocks the site.



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

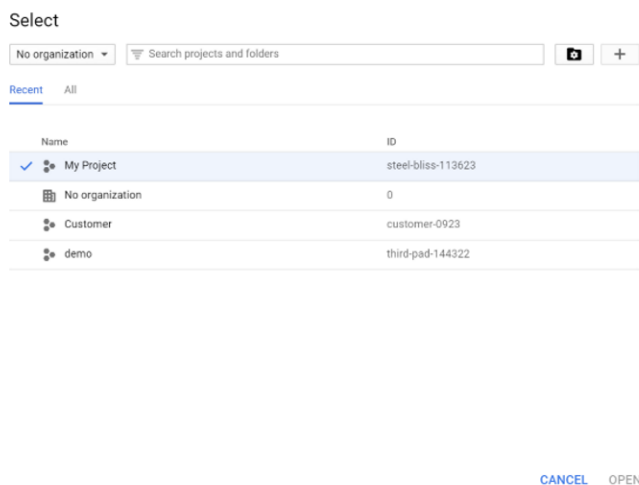
When using unique service account credentials for improved security, you must complete the following steps to add the unique service account credentials to the Google Admin console and FortiClient EMS:

1. Create unique service account credentials using the Google Developer console. See [Creating unique service account credentials on page 61](#).
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 65](#).

Creating unique service account credentials

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

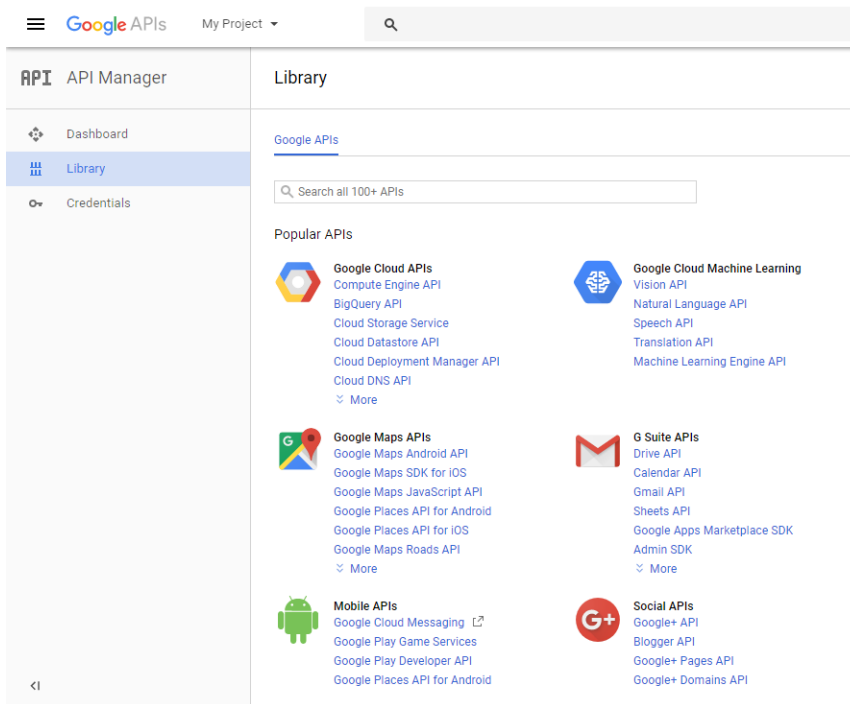
- Client ID (a long number)
 - Service account ID (email address)
 - Service account certificate (a certificate in .pem format)
1. Go to [Google API Console](#).
 2. Log in with your Google Workspace account credentials.
 3. Create a new project:
 - a. Click the toolbar list. The browser displays the following dialog.



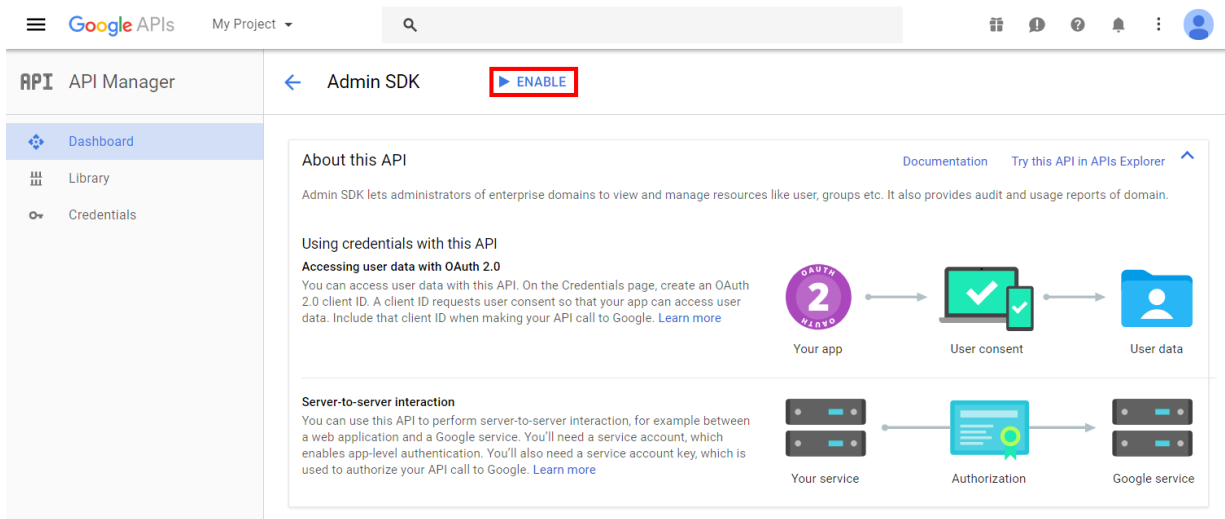
- b. Select your organization, if you see an organization dropdown list.
- c. Click the + button.
- d. In the *Project name* field, enter your project name, then click *Create*.

4. Enable the Admin SDK:

- Select your project from the toolbar list, then go to the *Library* tab.
- Under *Google Workspace APIs*, click *Admin SDK*.



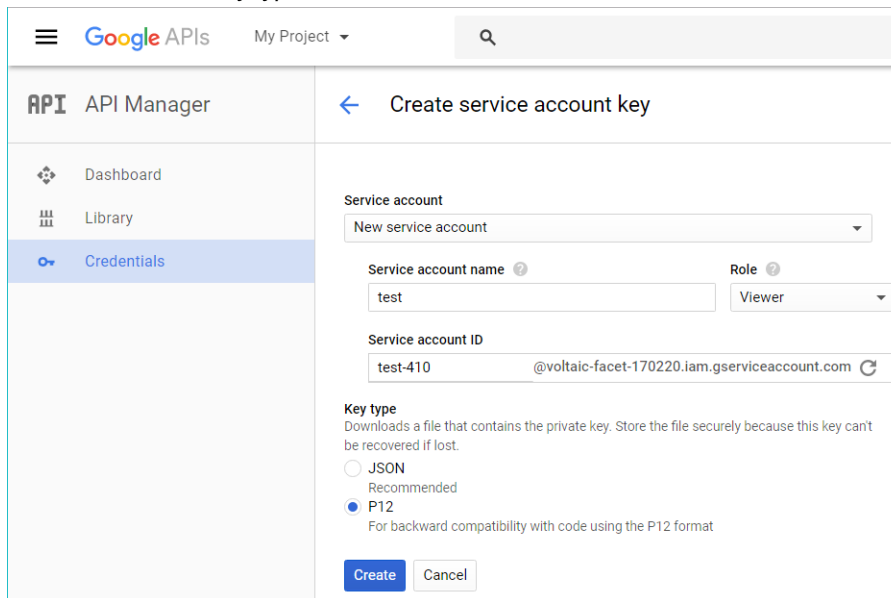
c. Click **ENABLE**.



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*.

- d. Select *P12* as the *Key type* and click *Create*.



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 **notasecret**.

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

API

API Manager

Dashboard

Library

Credentials

←

Client ID for Service account client

DOWNLOAD JSON

DELETE

i

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.

To add service account credentials to EMS:

1. In FortiClient EMS, go to *System Settings > EMS Settings*.
2. Enable *EMS for Chromebooks Settings*.



The default service account credentials display. Overwrite the default settings with the unique set of service account credentials received from Fortinet.

3. The *Service account* field shows the configured email address provided for the service account credentials. Click the *Update service account* button and configure the following information:

Service Account Email	Enter a new email address for the service account credentials.
Private key	Click <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

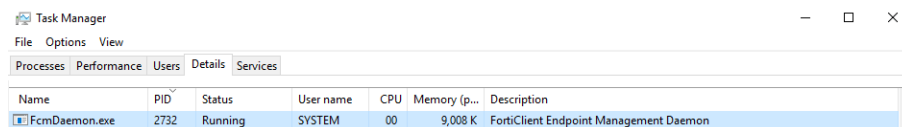
o: displays process ID (PID) associated with each connection

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:



If you want to deploy FortiClient to your domain-joined endpoints and have followed the [Preparing the AD server for deployment on page 117](#) instructions, you can use the same steps to verify the ports for SMB and RPC. See the [FortiClient Administration Guide](#).

Connectivity between EMS and FortiClient

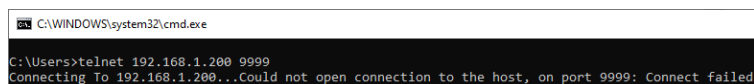
In addition to the services running correctly, there must be connectivity between EMS and the endpoint. This section defines connectivity as a route and traffic on a given port. You can use Command Prompt and the built-in Telnet application to verify this. Ensure that Telnet is enabled on your device 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.



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 44 .
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 277 .
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 265 .
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 295 .
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 298](#).

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.

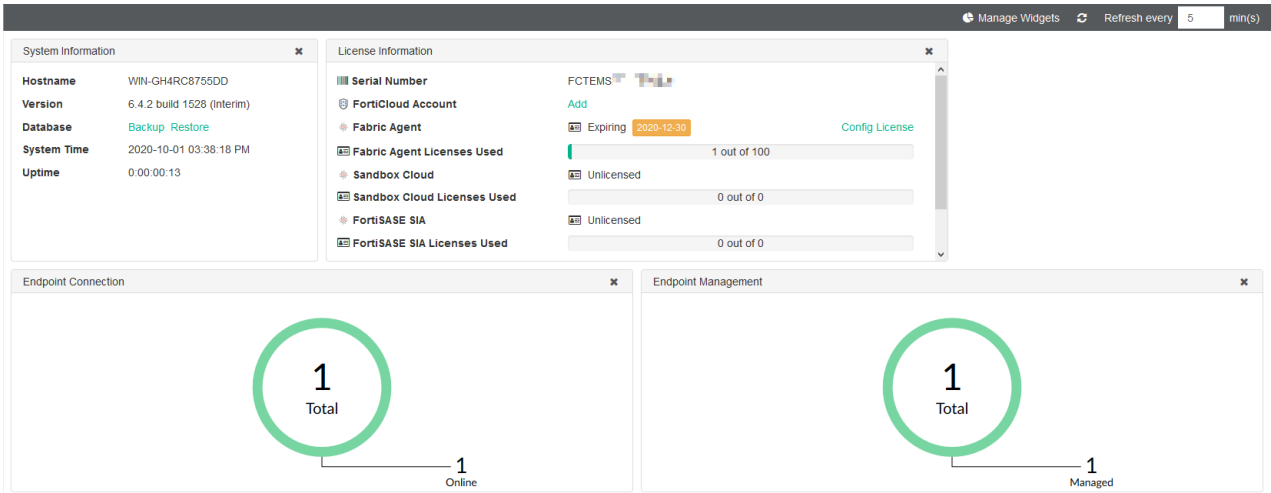
Dashboard

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 90](#).
- 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 296](#).

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 50](#).

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 292](#).

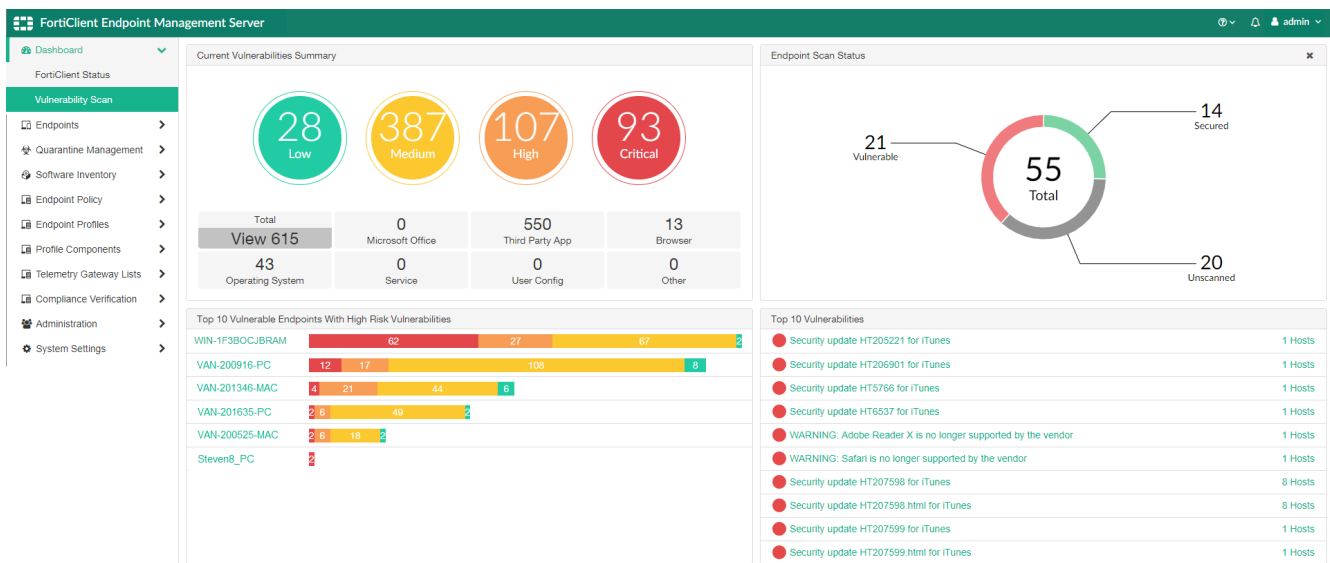
Option	Description
Endpoint Charts	
Endpoint Activity	Shows a summary of endpoint activity information. Categories are: <ul style="list-style-type: none"> EMS On-fabric EMS Off-fabric
Endpoint Alerts	Shows the number of endpoints with alerts, including pending software updates, out-of-date protection, 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 235.</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.



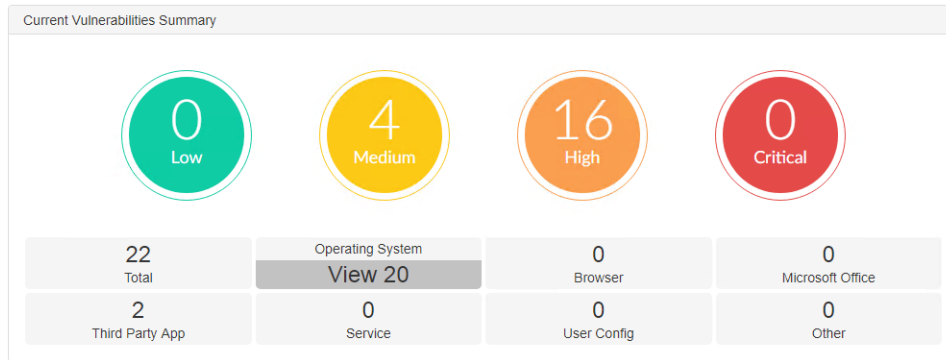
The *Vulnerability Scan* dashboard displays a number of charts. Each chart provides a summary of endpoint information. The sections in each chart are links. You can click sections of the charts or any row in the table to display more details.

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.

- 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:

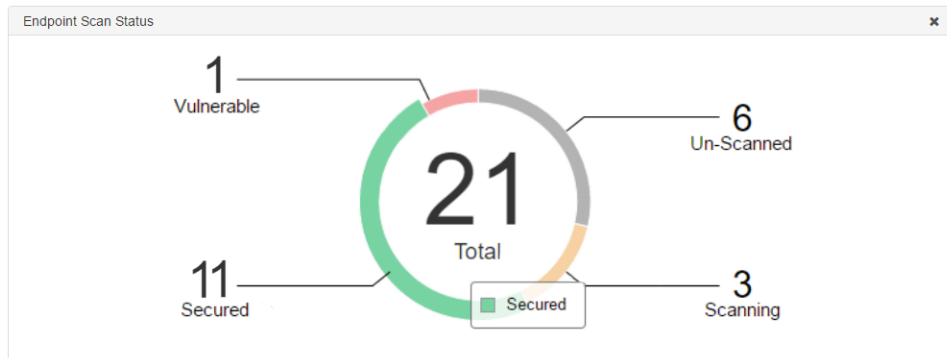
The screenshot shows the FortiClient Endpoint Management Server interface. On the left is a sidebar with navigation options: Dashboard, FortiClient Status, Vulnerability Scan, Endpoints, Quarantine Management, Software Inventory, Endpoint Policy, and Endpoint Profiles. The main area displays a table titled 'Medium Severity Vulnerabilities' with a 'Patch All' button. The table has columns for 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'. Both have a FortiGuard ID of 21877 and 21885 respectively, and are categorized as 'Application'. The CVE IDs are listed as CVE-2014-1296, CVE-2014-8842, CVE-2015-7048, CVE-2015-7095, CVE-2015-7096, CVE-2015-7097, CVE-2015-7098, CVE-2015-7099, and CVE-2015-7100. Both vulnerabilities have 1 affected endpoint and a 'Patch' button in the Patch Status column.

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				
<div> <div>Dashboard</div> <div>Vulnerability Endpoint</div> <div>Patch All</div> </div> <div> <div>FortiClient Status</div> <div>Vulnerability Scan</div> <div>Endpoints</div> </div>				
Hostname	Username	Vulnerability	Patch Status	
WIN-1F3BOCJBRAM	Administrator	11	20	5
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

Displays the number of vulnerabilities detected on the endpoint at each severity level. In this example, the endpoint has 11 critical vulnerabilities, 20 high risk vulnerabilities, and 5 medium risk vulnerabilities that can be patched using FortiClient.

The same endpoint also has 2 critical vulnerabilities that must be manually patched.

Patch Status

You can click the *Patch* button to patch the selected vulnerability with the next Telemetry communication between FortiClient EMS and the endpoint.

If a patch is already scheduled for the vulnerability, this column displays *Scheduled*.

If the vulnerability must be patched manually, this column displays *Manual Patch*.

FortiClient may be unable to automatically patch the vulnerability due to one of the following reasons:

- **Third-party application vulnerabilities:** incorrect or missing installation paths
- **OS vulnerabilities:** Windows update service is disabled

In these cases, EMS may incorrectly display the status of these vulnerabilities that were selected to be automatically patched as *Scheduled* instead of *Failed*.

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

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

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

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

36 entries loaded

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	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.

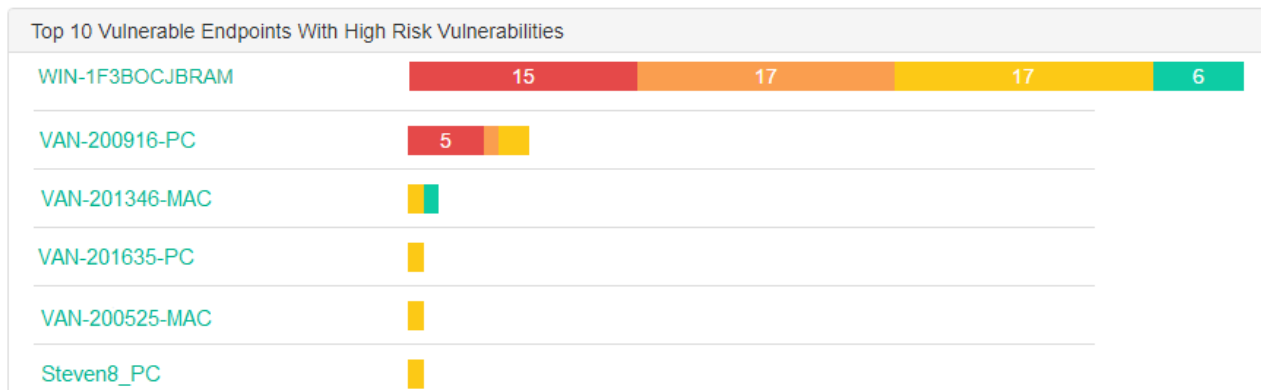
Severity Severity level of the vulnerability.

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

Viewing the top 10 vulnerable endpoints with high risk vulnerabilities

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

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



WIN-1F3BOCJBRAM has the following:

- 15 *Critical Vulnerabilities* (red bar)
- 17 *High Risk Vulnerabilities* (orange bar)
- 17 *Medium Risk Vulnerabilities* (yellow bar)
- 6 *Low Risk Vulnerabilities* (green bar)

2. Do one of the following:

- a. Click the endpoint hostname. You can view a list of all vulnerabilities detected on that endpoint.

Vulnerability	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	<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>

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 HT207598.html for iTunes	Application	Critical	Patch		
Compliance Verification	Security update HT207599.html for iTunes	Application	Critical	Patch		
Administration	Security update HT207928.html for iTunes	Application	Critical	Patch		

Viewing top ten vulnerabilities on endpoints

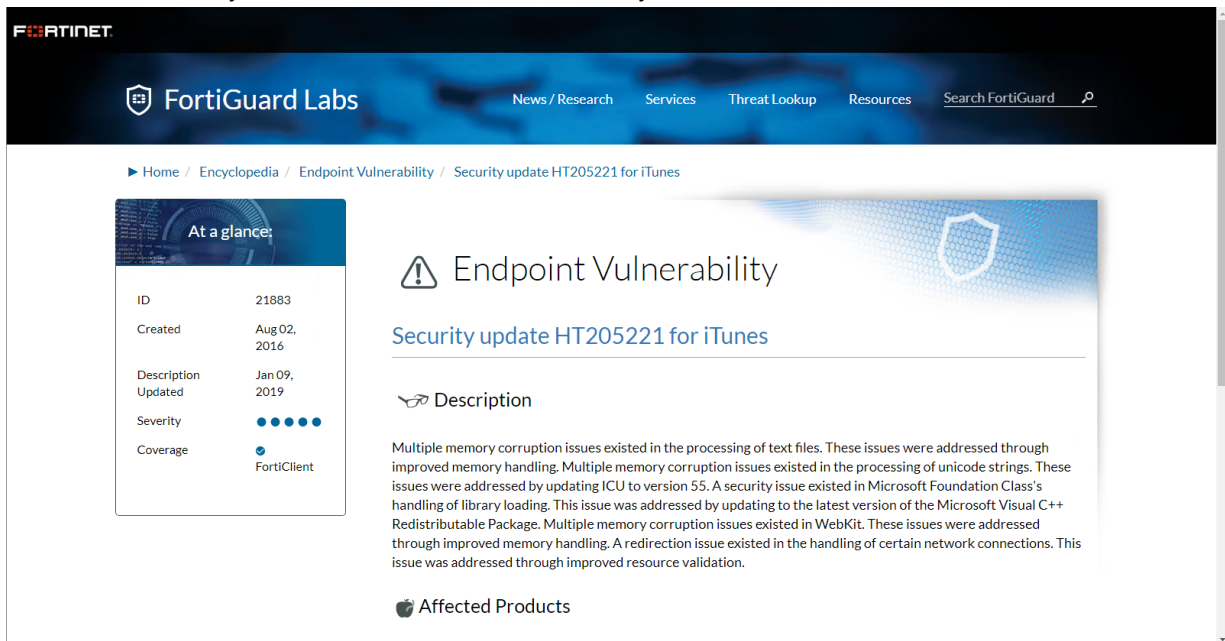
To view top ten vulnerabilities on endpoints:

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.

The screenshot shows the FortiClient Endpoint Management Server interface. The left sidebar has 'Dashboard' selected. The main area is titled 'Affected Endpoints' and contains a table with the following data:

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 174 .
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 174 .
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

You can manually import endpoints from an Active Directory (AD) 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. Do one of the following:
 - a. Go to *Endpoints > Manage Domains > Add*.
 - b. Go to *User Management > Authorized User Groups > Add*.
2. Configure the following options:

IP address/Hostname	Enter the domain server IP address or hostname.
Port	Enter the port number.
Distinguished name	Enter the distinguished name (DN) (optional). You must use only capital letters when configuring the DN. You cannot import domains and OUs that have a DN with more than 256 characters.
Alias	Enter the alias (optional).
Bind type	Select the bind type: <i>Simple</i> , <i>Anonymous</i> , or <i>Regular</i> . When you select <i>Regular</i> , you must enter the <i>Username</i> and <i>Password</i> .
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.
Sync every	Enter the sync schedule between FortiClient EMS and the domain in minutes. The default and minimum is sixty minutes.

- Click *Test* to test the domain settings connection.
- 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](#).

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:

- In FortiClient on the endpoint, go to the *Fabric Telemetry* tab.
- 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	<p>Visible when headings are displayed. Displays the name and icon of the user logged into the endpoint. Also displays the status of the endpoint:</p> <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. <p>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.</p>
IP	Visible when headings are displayed. Displays the endpoint's 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: <ul style="list-style-type: none"> • Request FortiClient Logs • Request Diagnostic Results • Update Signatures • Download Available FortiClient Logs • Download Available Diagnostic Results • Deregister • Quarantine • Un-quarantine • Exclude from Management • Revoke Client Certificate. This action is only available if the ZTNA or EPP license is applied and for endpoints running FortiClient 7.0.0 and later versions. Revoke the certificate that FortiClient is using to securely encrypt and tunnel TCP traffic through HTTPS to the FortiGate. You may want to revoke a certificate if it becomes compromised and can no longer be trusted. When a certificate is revoked, EMS prompts FortiOS and FortiClient with a new certificate signing request. See FortiClient in the Security Fabric on page 14. • Clear Events • Mark as Uninstalled • Set Importance • Set Custom Tags. This option is only available if you have already created a custom tag. • Delete Device

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 136 .
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 214 .
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 235 .
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 • Profile: Profiles assigned to the selected endpoint • Off-fabric Profile: Off-fabric profiles 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.

Classification Tags	<p>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, then click the + button. When you create a tag, it is available for assignment to all endpoints in the current site.</p> <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 100.</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.
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 99 .	
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.	
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> .	

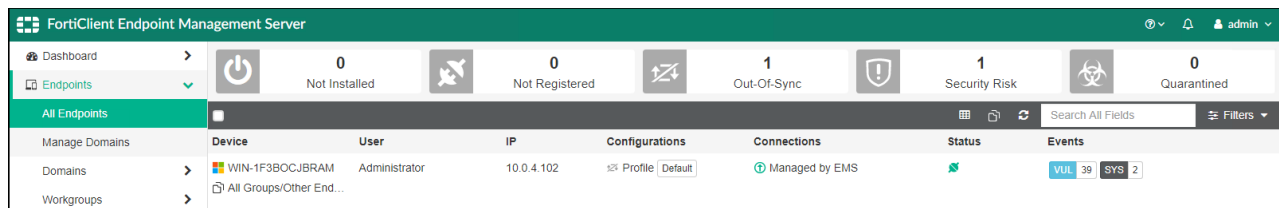
Application	Displays the name of the application with the vulnerability.
Severity	Displays the vulnerability's severity.
Patch Type	Displays the patch type for this vulnerability: <i>Auto</i> or <i>Manual</i> .
FortiGuard	Displays the FortiGuard ID number. If you click the FortiGuard ID number, it redirects 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.

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 90](#).

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 214 and Viewing the Endpoints pane on page 90 .
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.

- Click *Search*. The filtered list of endpoints displays.
- 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:

- Go to *Endpoints*.
- Click *All Endpoints*, a domain, or workgroup. The list of endpoints displays.
- Click the *Filters* menu, and set filters.
- Click the *Bookmark* button.
- 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:

- Go to *Endpoints*.
- Click *All Endpoints*, a domain, or workgroup. The list of endpoints displays.
- Click the *Filters* menu.
- 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.

The screenshot displays the FortiClient EMS interface for a detailed report on a Sandbox event. The top section shows a timeline of events: Threat Detected (on 2019-03-26 20:38:53), Sandbox Analysis (on 2019-03-26 20:38:53), File Blocked (on 2019-03-26 20:40:34), and Dynamic Signature Updated (on 2019-03-26 20:40:34). A red banner at the top indicates 'credit_report.exe (High Risk)' and a 'Quarantine Endpoint' button is visible.

The main content area is divided into two sections: Endpoint and Indicators (1). The Endpoint section shows details for 'ledington' (Lola Edington, ledington@gmail.com, +1 236 735 0814, All Groups/Smart PowerGrid/Research and Development/DevOps). The Indicators section shows a 'Machine learning verdict score based on peay static scan' of 42 out of 100.

The File Information section provides details for 'credit_report.exe':

Property	Value
Command Line	c:\work\4357810084146248730.exe
Score	41
Rating	High Risk
Rated by	Sandboxing
Instances	1
Host Affected	1
Filename	credit_report.exe
File Path	C:\Users\ledington\Downloads\appliance\credit_report.exe
File Size	4096(bytes)
MD5	e830a79ea311f91593f2d3536064f8c0
SHA1	2656dc7173b7e40f568cd1467efa4d87243afe7
SHA256	72be2f392bb165d297949445d89b3ae48de1555ec3e91374f4c73fae8806c1
Virus Total	Q

The Process Tree section is partially visible at the bottom.

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

created on FortiSandbox.

Details		
Process Information	File Operations	Network Operations
PID	3572	
File Path	%CURRENTFILE%	
File Type	exe	
CMD Line	c:\work\4357810084146248730.exe	
MD5	e830a79ea311f1915932d35360648c0	

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:

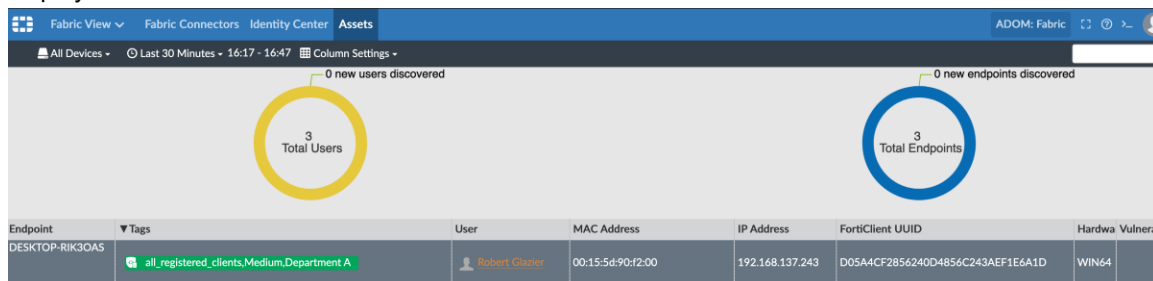
1. In FortiAnalyzer, go to *Fabric View*.
2. Click the *Fabric Connectors* tab, then click *Create New*.
3. Click the *FortiClient EMS* tile. The *Create New Fabric Connector* dialog opens.
4. In the *Configuration* tab, configure the connector settings, enter the EMS IP address and administrator credentials.

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.



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 188](#).

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.

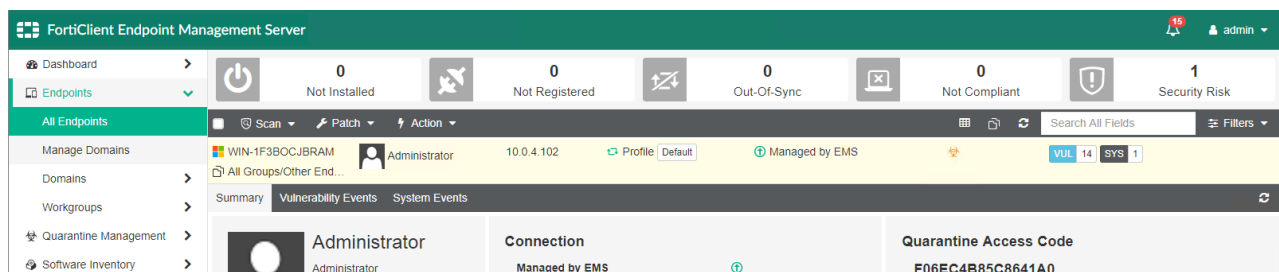
You must enable Application Firewall for this feature to function. See [Feature Select on page 292](#).

To quarantine an endpoint:

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

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

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



Quarantining an endpoint from FortiOS using EMS

The 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 141](#).
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 128](#).
3. Enable *Remote HTTPS access*. See [Configuring EMS settings on page 277](#).

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 operating system.

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 operating system (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 111](#).
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 111](#).
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 111](#).
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

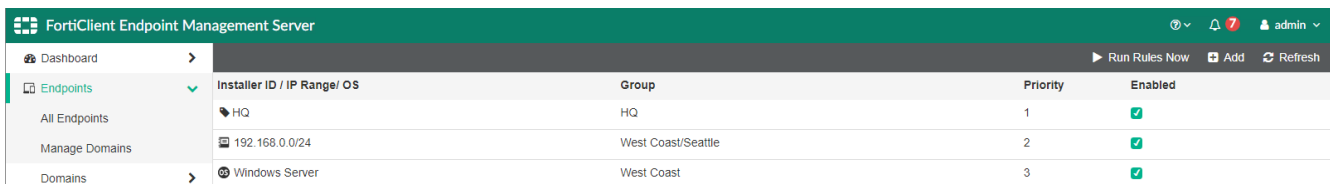
An endpoint may be eligible for multiple group assignment rules. When an endpoint is eligible for multiple endpoint group assignment rules, two factors determine which rule EMS applies to the endpoint:

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:

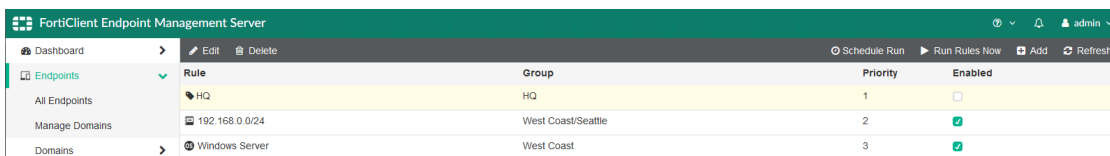
1. Go to *Endpoints > Group Assignment Rules*.
2. Click and hold the rule, then drag to the desired position.

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.



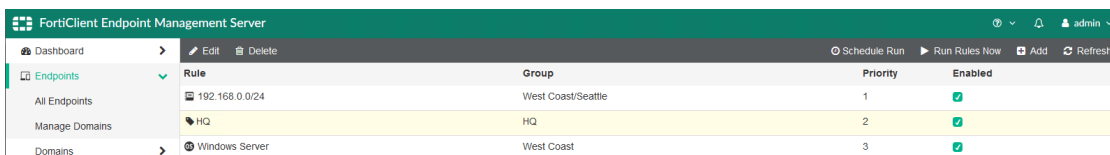
Installer ID / IP Range/ OS	Group	Priority	Enabled
HQ	HQ	1	<input checked="" type="checkbox"/>
192.168.0.0/24	West Coast/Seattle	2	<input checked="" type="checkbox"/>
Windows Server	West Coast	3	<input checked="" type="checkbox"/>

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.



Rule	Group	Priority	Enabled
HQ	HQ	1	<input type="checkbox"/>
192.168.0.0/24	West Coast/Seattle	2	<input checked="" type="checkbox"/>
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.



Rule	Group	Priority	Enabled
192.168.0.0/24	West Coast/Seattle	1	<input checked="" type="checkbox"/>
HQ	HQ	2	<input checked="" type="checkbox"/>
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

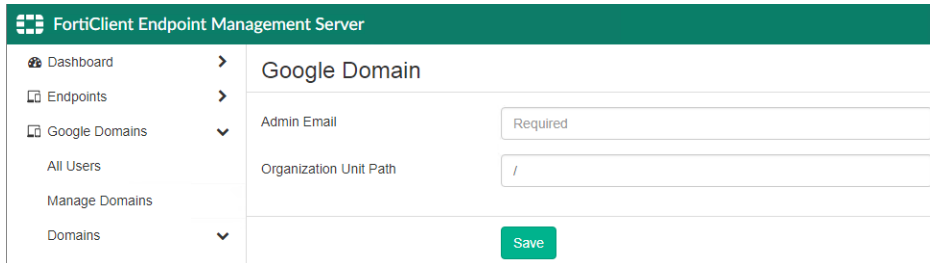
FortiClient EMS must determine which Chromebooks to manage. Device information comes from the Google Admin console. *Google Domains* is only available if you enabled *System Settings > EMS Settings > EMS for Chromebooks*

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 domain root.

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

Viewing domains

After you add domains to FortiClient EMS, you can view the domain list 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 Google users list 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 Retri...	schoolz...	/Young Lady's School/staff/admin
bob bob	bob.bob@ys...	8/6/2016 1:0...	Never Retri...	schoolz...	/test
Catherine Seely	Catherine.Se...	7/25/2016 9:...	Never Retri...	schoolz...	/Young Stars School
Dean Cagle	Dean.Cagle...	8/5/2016 10:...	Never Retri...	schoolz...	/Young Lady's School/staff/admin
Dennis Auger	Dennis.Auger...	7/15/2016 9:...	Never Retri...	schoolz...	/Young Lady's School/students...
Edgar Bayles	Edgar.Bayles...	8/9/2016 12:...	Never Retri...	schoolz...	/Young Stars School/students/...
Efrain2 Tague	Efrain2.Tagu...	8/2/2016 10:...	Never Retri...	schoolz...	/Young Stars School/students/...
Emilio Freitag	emilio.freitag...	7/25/2016 9:...	Never Retri...	schoolz...	/Young Lady's School/students...
Garry Heinrich	Garry.Heinric...	8/3/2016 8:2...	Never Retri...	schoolz...	/Young Lady's School/staff/admin
Gerard Rhoa...	gerard.rhoad...	7/14/2016 11:...	Never Retri...	schoolz...	/Young Lady's School/staff
jiaping xu	jpxu@school...	8/9/2016 6:4...	Never Retri...	schoolz...	/
Joey Albrecht	joey.albrecht...	8/2/2016 10:...	Never Retri...	schoolz...	/Young Lady's School/staff
KeriNew Coc...	Keri.Cochran...	8/4/2016 1:1...	Never Retri...	schoolz...	/Young Lady's School/test
Leann Bast	Leann.Bast@...	8/9/2016 12:...	Never Retri...	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 name.
Email	Chromebook user 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 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 domain list displays.
2. Click a domain. The Google users list 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 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 on endpoints. Deploying FortiClient from FortiClient EMS requires the following steps:

1. Prepare the AD server. See [Preparing the AD server for deployment on page 117](#).
2. Prepare Windows endpoints for FortiClient. See [Preparing Windows endpoints for FortiClient deployment on page 119](#).
3. Add the AD server to FortiClient EMS. See [Adding endpoints using an AD domain server on page 89](#).
4. Add a profile and configure FortiClient features in the profile. See [Creating a new profile on page 141](#).
5. Create a deployment package with the profile in step 4 configured. See [Adding a FortiClient deployment package on page 123](#).
6. Create a deployment configuration. See [Creating a deployment configuration on page 119](#).

After you deploy FortiClient on endpoints and endpoints connect to FortiClient EMS, you can update endpoints by editing the associated profiles.

You can also use FortiClient EMS to uninstall and upgrade FortiClient on endpoints.



You cannot use workgroups to deploy an initial installation of FortiClient to endpoints. However, after FortiClient installs on endpoints and endpoints connect to FortiClient EMS, you can use workgroups to uninstall and update FortiClient on endpoints.



You cannot use FortiClient EMS to deploy an initial installation of FortiClient (macOS) to endpoints. However, after FortiClient (macOS) is installed on endpoints and endpoints connect to FortiClient EMS, you can use FortiClient EMS to uninstall and update FortiClient (macOS) on endpoints.

Manage Deployment

Preparing the AD server for deployment

Before you can successfully deploy a FortiClient installation, ensure you install and prepare the Active Directory server as follows:

1. [Configuring a group policy on the AD server on page 118](#)
2. [Configuring required Windows services on page 118](#)
3. [Creating deployment rules for Windows firewall on page 118](#)
4. [Configuring Windows firewall domain profile settings on page 118](#)

Configuring a group policy on the AD server

To configure a group policy on the AD server:

1. On the Active Directory (AD) server, open *Group Policy Management*.
2. Right-click the *Default Domain Policy* setting. The Group Policy Management Editor opens. A new policy is applied to the entire AD domain. Alternatively, you can create a new group policy object, and link it to one or more organization units in the AD server that contain the endpoint computers that you will deploy FortiClient to.

Configuring required Windows services

To configure required Windows services:

1. In the Group Policy Management Editor, in the left panel, go to *Computer Configuration > Policies > Windows Settings > Security Settings > System Services*.
2. In the right panel, select the following:
 - a. Task Scheduler: Automatic
 - b. Windows Installer: Manual
 - c. Remote Registry: Automatic

Creating deployment rules for Windows firewall

To create deployment rules for Windows firewall:

1. In the Group Policy Management Editor, in the left panel, go to *Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Inbound Rules*.
2. Right-click *Inbound Rules* and select *New Rule*.
3. Select *Predefined* from the dropdown list and select *File and Printer Sharing*. Click *Next*.
4. Ensure that *File and Printer Sharing (SMB-In)* is selected and click *Next*.
5. Select *Allow the connection* and click *Finish*.
6. Repeat steps 1 to 2.
7. Select *Predefined* from the dropdown list and select *Remote Scheduled Tasks Management* and click *Next*.
8. Ensure that the *Remote Scheduled Tasks Management (RPC)* box is checked and click *Next*.
9. Select *Allow the connection* and click *Finish*.

Configuring Windows firewall domain profile settings

To configure Windows firewall domain profile settings:

1. In the Group Policy Management Editor, in the left panel, go to *Computer Configuration > Policies > Administrative Templates > Network > Network Connections > Windows Firewall > Domain Profile*.
2. Select *Allow inbound file and printer sharing exception*:
 - a. Right-click and select *Edit*.
 - b. Enable the radio button.
 - c. Provide the FortiClient EMS server IP address in the text box.
 - d. Allow unsolicited incoming messages from these IP addresses.
 - e. Click OK.

3. Select *Allow inbound remote administration* exception. Repeat step 2 to create an exception.
4. Select *Allow ICMP Exceptions*:
 - a. Right-click and select *Edit*.
 - b. Enable the radio button.
 - c. Select the *Allow inbound echo request* checkbox.
 - d. Click *OK*.



To deploy the group policy manually, execute `gpupdate /force` on the Active Directory (AD) server to update the group profile on all endpoints.

Execute `gpresult.exe /H gpresult.html` on any AD client to view the group policy deployed on the endpoints.

Preparing Windows endpoints for FortiClient deployment

You must enable and configure the following services on each Windows endpoint before deploying FortiClient:

- Task Scheduler: Automatic
- Windows Installer: Manual
- Remote Registry: Automatic



You must configure Windows Firewall to allow the following inbound connections:

- File and Printer Sharing (SMB-In)
 - Remote Scheduled Tasks Management (RPC)
-

Active Directory (AD) group deployments require an AD administrator account. For non-AD deployments, you can share the deployment package URL with users, who can then download and install FortiClient manually. You can locate the deployment package URL in *Deployment & Installers > FortiClient Installer*.



When adding endpoints using an AD domain server, FortiClient EMS automatically resolves endpoint IP addresses during initial FortiClient deployment. FortiClient EMS can deploy FortiClient (Windows) to AD endpoints that do not have FortiClient installed, as well as upgrade existing FortiClient installations if the endpoints are already connected to FortiClient EMS.

Creating a deployment configuration

To create a deployment configuration:

1. Go to *Deployment > 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.
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.
Username	Enter the username to perform deployment on AD. You must enter the admin credentials for the AD. The credentials allow FortiClient EMS to install FortiClient on endpoints using AD. If the credentials are wrong, the installation fails, and an error displays in FortiClient EMS.
Password	Enter the password to perform deployment on AD.
Enable the Deployment	Enable or disable.

4. Click **Save**.

Managing deployment configuration priority levels

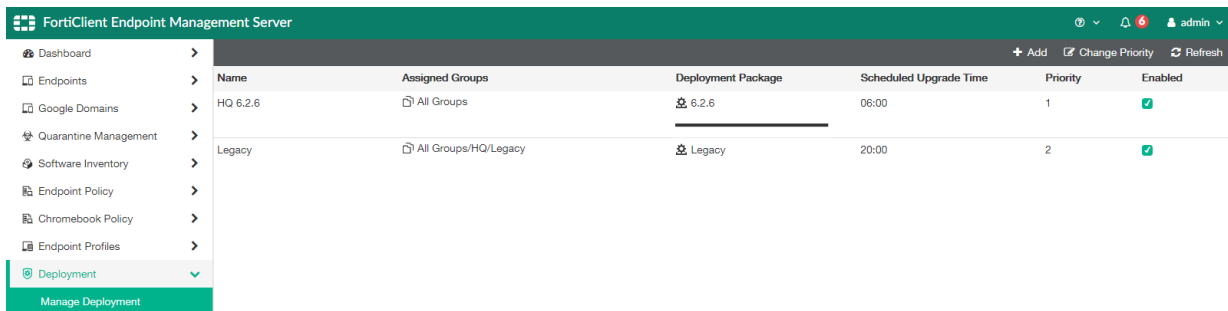
An endpoint may be eligible for multiple deployment configurations. When an endpoint is eligible for multiple endpoint deployment configurations, two factors determine which configuration EMS applies to the endpoint:

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 > Manage Deployment*.
2. Click *Change Priority*.
3. Click and hold the configuration, then drag to the desired position.

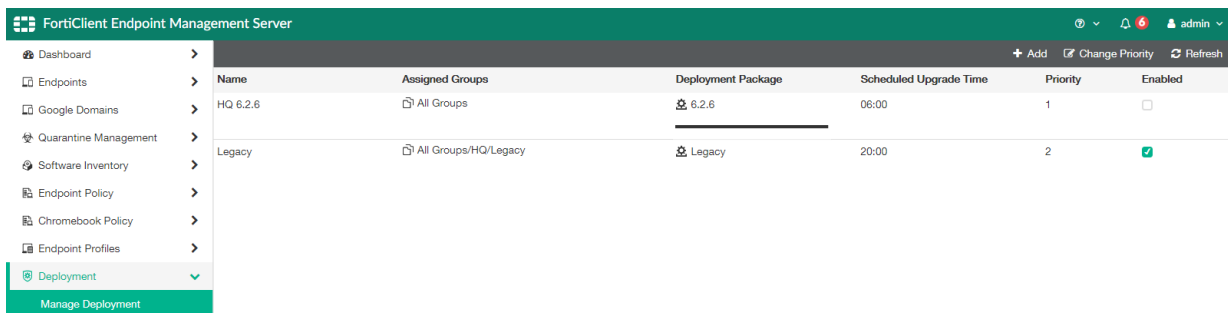
In the example, consider an endpoint that belongs to the Legacy group. The endpoint applies for two configurations. In this case, EMS applies the HQ 6.2.6 deployment configuration to the endpoint, since the HQ 6.2.6 configuration has a higher priority level than the Legacy configuration.



The screenshot shows the FortiClient Endpoint Management Server interface. The left sidebar has a menu with options: Dashboard, Endpoints, Google Domains, Quarantine Management, Software Inventory, Endpoint Policy, Chromebook Policy, Endpoint Profiles, and Deployment (selected). The main table displays deployment configurations:

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"/>

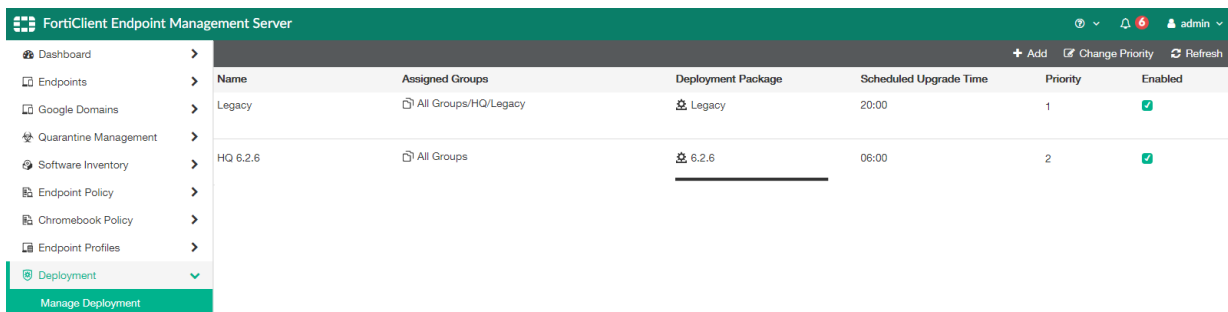
However, if you disable the HQ 6.2.6 configuration, EMS applies the Legacy deployment configuration to the endpoint in the Legacy group.



The screenshot shows the FortiClient Endpoint Management Server interface. The left sidebar has a menu with options: Dashboard, Endpoints, Google Domains, Quarantine Management, Software Inventory, Endpoint Policy, Chromebook Policy, Endpoint Profiles, and Deployment (selected). The main table displays deployment configurations:

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 reenable the HQ 6.2.6 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.



The screenshot shows the FortiClient Endpoint Management Server interface. The left sidebar has a menu with options: Dashboard, Endpoints, Google Domains, Quarantine Management, Software Inventory, Endpoint Policy, Chromebook Policy, Endpoint Profiles, and Deployment (selected). The main table displays deployment configurations:

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 > Manage Deployment*.
2. Select or deselect the *Enabled* checkbox for the desired deployment configuration.

Deleting a deployment configuration

To delete a deployment configuration:

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

Deploying initial installations of FortiClient (macOS)

You cannot use FortiClient EMS to deploy initial installations of FortiClient (macOS). You can deploy an initial installation of FortiClient (macOS) by doing one of the following:

- Create a custom FortiClient (macOS) deployment package on FortiClient EMS with the FortiClient EMS IP address embedded. Send the deployment package download link to users so they can install FortiClient manually on the endpoint. Once installed, FortiClient (macOS) automatically connects to FortiClient EMS and supports future deployments from FortiClient EMS directly.
- Use a third party application to perform initial deployment of FortiClient (macOS) to endpoints.

After FortiClient (macOS) is installed on endpoints and has connected FortiClient Telemetry to FortiClient EMS, you can use FortiClient EMS to replace, upgrade, and uninstall FortiClient (macOS).

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:

- *Install Now*: If you select this option, FortiClient performs the upgrade and automatically restarts your computer.
- *Install Later*: If you select this option, you can indicate the time to start the upgrade. The default is 8:00 PM. Your computer automatically restarts after the upgrade has finished.
- *No Option*: 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:
 - a. *Reboot*: Select this option to have the reboot occur immediately.
 - b. *Reboot later*: Select this option to 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 109](#) 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 111](#).
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_7.0.7_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_7.0.7_x64.exe /v"GROUP_TAG=HR"
FortiClientSetup_7.0.7_x64.exe /v"GROUP_TAG=Marketing"
FortiClientSetup_7.0.7_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	<p>Use an official or custom FortiClient installer.</p> <p>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.</p> <p>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 unavailable in .msi or .zip format. You must package the installer as an .msi or .zip file to upload it.</p>
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 292](#).

Zero Trust Telemetry	Enabled by default and cannot be disabled. Installs FortiClient with Telemetry enabled.
Secure Access Architecture Components	Install FortiClient with SSL and IPsec VPN enabled. Disable to omit SSL and IPsec VPN support from the FortiClient deployment package.

If you enable this feature for a deployment package and include a preconfigured VPN tunnel in the included endpoint profile, users who use this deployment package to install FortiClient can connect to this preconfigured VPN tunnel for three days after their initial FortiClient installation. This is useful for remote users, as it allows them to connect to the corporate network to activate their FortiClient license. If the user does not activate their FortiClient license within the three days, all FortiClient features, including VPN, stop working on their device.

See [Remote Access on page 144](#) for details on configuring a VPN tunnel.

Vulnerability Scan

Enabled by default and cannot be disabled. Installs FortiClient with Vulnerability Scan enabled.

Advanced Persistent Threat (APT) Components

Install FortiClient with APT components enabled. Disable to omit APT components from the FortiClient deployment package. Includes FortiSandbox detection and quarantine features.

Additional Security Features

Enable any of the following features:

- Malware
 - 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 for FortiClient (macOS) 7.0.1 and later versions, the zero trust network access feature is always installed, regardless of whether this option is enabled or disabled.

Disable to exclude features from the FortiClient deployment package.

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 109](#).

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 manages FortiClient once it is installed on the endpoint.
8. Click *Finish*. EMS adds the FortiClient deployment package to *Deployment Installers > FortiClient Installer*. 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 277](#).

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 136](#).

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	VPN	Remot...	VPN	Default	0
		ZTNA	ZTNA01	ZTNA	Default	
		WEB	WF_EMS	WEB	Default	
		VULN	Default	VULN	Default	
		MW	Default	MW	Default	
		SB	Default	SB	Default	
		FW	Default	FW	Default	
		SYS	Default	SYS	Default	
Default		VPN	Default	VPN	Default	0
		ZTNA	Default	ZTNA	Default	
		WEB	Default	WEB	Default	
		VULN	Default	VULN	Default	
		MW	Default	MW	Default	
		SB	Default	SB	Default	
		FW	Default	FW	Default	
		SYS	Default	SYS	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

To delete 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

To enable or disable 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:

- EMS only applies endpoint policies to endpoints if they are enabled on the *Endpoint Policy & Components > Manage Policies* page.
- 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	<div> <div>PROFILE</div> <div>OFF-NET</div> </div> Seattle_general Seattle_offnet 100% ✓	ON-NET a	FGT_Seattle_floor1	1	1	<input type="checkbox"/>
SF_general	All Groups/SF	<div> <div>PROFILE</div> </div> SF_general			1	2	<input checked="" type="checkbox"/>
Seattle_HR	All Groups/Seattle/HR	<div> <div>PROFILE</div> </div> 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	<div> <div>PROFILE</div> <div>OFF-NET</div> </div> Seattle_general Seattle_offnet 100% ✓	ON-NET a	FGT_Seattle_floor1	1	1	<input checked="" type="checkbox"/>
SF_general	All Groups/SF	<div> <div>PROFILE</div> </div> SF_general			1	2	<input checked="" type="checkbox"/>
Seattle_HR	All Groups/Seattle/HR	<div> <div>PROFILE</div> </div> 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	<div> <div>PROFILE</div> <div>OFF-NET</div> </div> Seattle_general Seattle_offnet 100% ✓	ON-NET a	FGT_Seattle_floor1	1	1	<input type="checkbox"/>
SF_general	All Groups/SF	<div> <div>PROFILE</div> </div> SF_general			1	2	<input checked="" type="checkbox"/>
Seattle_HR	All Groups/Seattle/HR	<div> <div>PROFILE</div> </div> 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 ineligible 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:

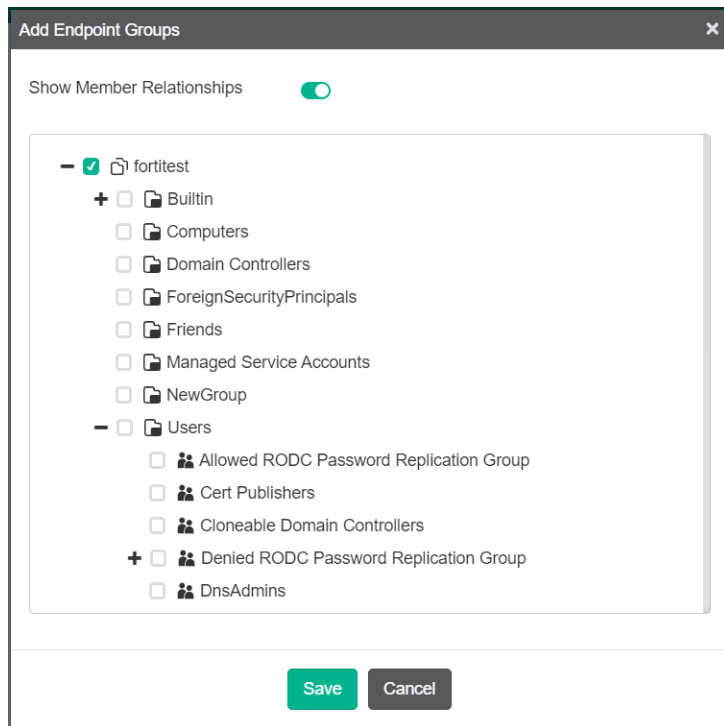
1. Go to *Endpoint Policy & Components > Manage Policies*.
2. Click *Edit Columns*.
3. Enable or disable the columns as desired.
4. Click *Save*.

Managing FortiClient based on AD 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.

Edit Delete		Add Change Priority Refresh Clear Filters Edit Columns				
Name	Assigned Groups	Profile	Policy Components	Endpoint Count	Enabled	
Policy_1	All Groups	<div><div>PROFILE</div>Profile_1</div> <div><div>OFF-NET</div>Default</div> <div><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><div>PROFILE</div>Profile_2</div> <div><div>OFF-NET</div>Default</div> <div><div></div>100%</div>		<div> 2</div>		
Default		<div><div>PROFILE</div>Default</div>		<div> 0</div>		

Click the endpoint count to see the endpoint list.

Endpoints (4) Refresh						
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-RHock	 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.
3. Create a deployment package.
4. Create a deployment configuration.

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

+ Add Change Priority Refresh					
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 Fortinet Security 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 201](#). 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 201](#).

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 128](#).

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 138.</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 the serial number "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 128](#).

Endpoint Profiles

FortiClient EMS has separate endpoint profiles for the following features:

- [Remote Access on page 144](#)
- [ZTNA Destinations on page 173](#)
- [Web Filter on page 174](#)
- [Vulnerability Scan on page 185](#)
- [Malware Protection on page 188](#)
- [Sandbox on page 197](#)
- [Firewall on page 200](#)
- [System Settings on page 201](#)

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 128](#).

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 143](#).
 - 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 a profile

You cannot delete the default profiles.

To delete a profile:

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.

Configuration	Description
Disable Connect/Disconnect	Disable the <i>Connect/Disconnect</i> button when using <i>Auto Connect</i> with VPN.
Show VPN before Logon	Allow users to select a VPN connection before logging into the system.
Use Windows Credentials	If allowing users to select a VPN connection before logging into the system, enable this option to allow them to use their current Windows username and password.
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 149 .
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 136 .
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.

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.

Configuration	Description
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 unavailable, 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.
Show Passcode	Display Passcode instead of Password in the <i>VPN</i> tab in FortiClient.
Enable Invalid Server Certificate Warning	Display a warning to the user that the certificate is invalid before attempting VPN connection.
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.

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 255 .
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> <p>Only FortiClient (Windows) supports this feature. FortiClient (macOS) and (Linux) do not support this feature.</p>
Host Tag	<p>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 214.</p> <p>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:</p> <ol style="list-style-type: none"> 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 214. 2. For the VPN tunnel settings, select <i>Prohibit</i>, then select the configured tag from the <i>Select a Tag</i> dropdown list. <p>Endpoints without up-to-date AV signatures are prohibited from connecting to the VPN tunnel.</p> <p>FortiClient (macOS) and (Linux) do not support this feature.</p>
Customize Host Check Fail Warning	<p>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.</p> <p>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.</p>
Show "Remember Password" Option	Show option to have the VPN tunnel remember the password. You must also enable this option on the FortiGate.
Show "Always Up" Option	Show option to have the VPN tunnel always up. You must also enable this option on the FortiGate.
Show "Auto Connect" Option	Automatically connect the VPN tunnel. You must also enable this option on the FortiGate. Automatic connection to the VPN tunnel may fail if the endpoint boots up with a user profile set to automatic logon.
On Connect Script	Enable the on connect script. Enter your script.

**On
Disconnect
Script**

Enable the disconnect script. Enter your script.

IPsec VPN

This topic contains descriptions of IPsec VPN settings.

Configuration	Description
IPsec VPN	Enable IPsec VPN.
Beep If Connection Fails	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.
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 unavailable, 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 • 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. 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	<p>Select the encryption and authentication algorithms used to generate keys for protecting negotiations and add encryption and authentication algorithms as required. You must 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.</p>
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 255 .
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.

	<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> <p>Only FortiClient (Windows) supports this feature. FortiClient (macOS) and (Linux) do not support this feature.</p>
Host Tag	<p>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 214.</p> <p>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:</p> <ol style="list-style-type: none"> 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 214. 2. For the VPN tunnel settings, select <i>Prohibit</i>, then select the configured tag from the <i>Select a Tag</i> dropdown list. <p>Endpoints without up-to-date AV signatures are prohibited from connecting to the VPN tunnel.</p>
Customize Host Check Fail Warning	<p>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.</p> <p>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.</p>
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	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: <ul style="list-style-type: none">• Microsoft Office 365• Microsoft Teams• Skype• GoToMeeting• Zoom• WebEx• YouTube Once the VPN tunnel is up, FortiClient binds the specified excluded applications to the physical interface.
Type	Select <i>Exclude</i> to configure whether to exclude certain application traffic from the VPN tunnel.

Configuration	Description
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 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 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)

teams.exe;C:\Users\<username>\appData\Local\Microsoft\Teams\

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

For example:
 Application Name: chrome.exe
 Full Path: C:\Program Files\Internet Explorer\ieplorer.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

Type: Include Exclude

Local Applications

Name
<input type="checkbox"/> teams.exe
<input type="checkbox"/> %localappdata%\Microsoft\Teams\current\Teams.exe
<input type="checkbox"/> C:\Program Files\Mozilla Firefox\firefox.exe
<input type="checkbox"/> %localappdata%\Microsoft\Teams\current\
<input type="checkbox"/> C:\Program Files\Mozilla Firefox\

Remove Add

Cloud Applications

Name
<input type="checkbox"/> Microsoft-Skype_Teams
<input type="checkbox"/> Cisco-Webex
<input type="checkbox"/> Cisco-Webex.FedRAMP
<input type="checkbox"/> Zoom.us-Zoom.Meeting

Remove Add

Domain

Domain
No Content Found

Remove Add

Add Tunnel Cancel

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

Configuring a profile to allow or block endpoint from VPN tunnel connection based on the applied 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	CriticalVuln
Tag Endpoint As ⓘ	Vulnerable Devices ▼
Enabled	<input checked="" type="checkbox"/>
Comments	Optional

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

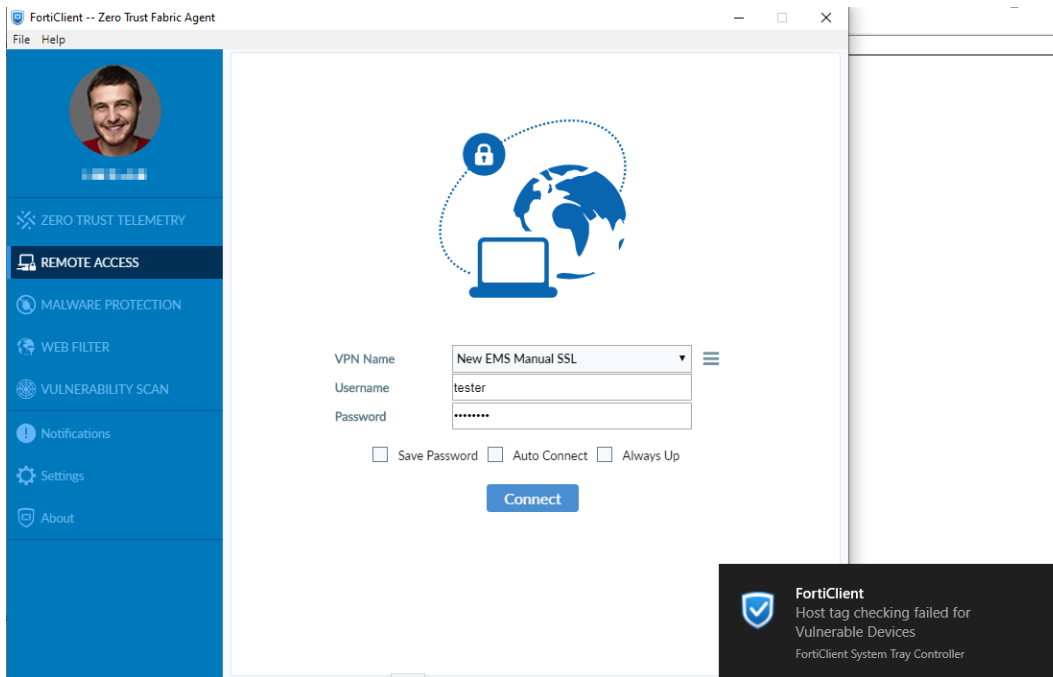
Save **Cancel**

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.

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 performs IPsec VPN NAT incorrectly.

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

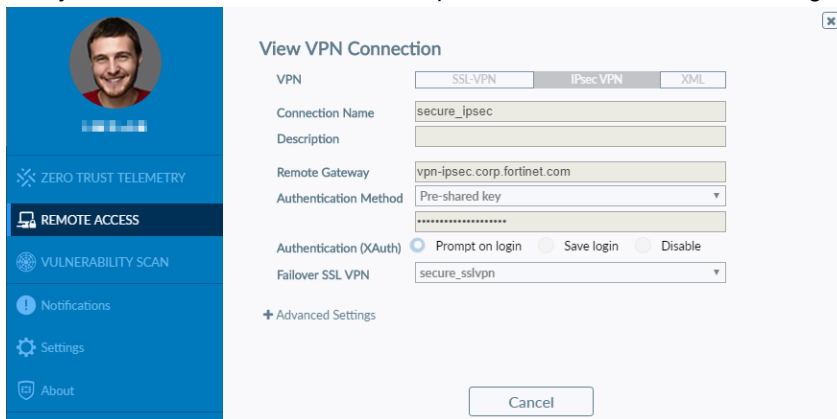
To configure a backup VPN connection:

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:

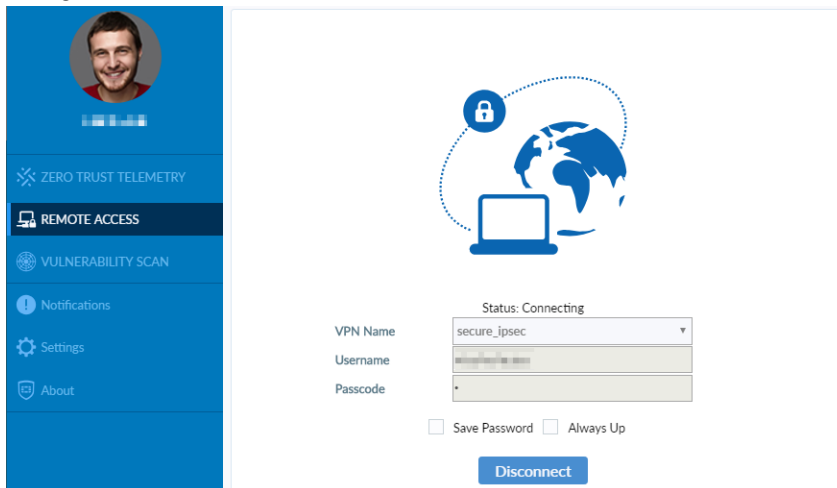

```
<forticlient_configuration>
  <vpn>
    <ipsecvpn>
      <connections>
        <connection>
          <ike_settings>
            <failover_sslvpn_connection>secure_sslvpn</failover_sslvpn_
              connection>
          <ike_settings>
        <connection>
      </connections>
    </ipsecvpn>
  </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) 7.0.7 and EMS 7.0.7 support this feature. FortiClient (Linux) 7.0.7 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 that FortiAuthenticator provides:

```
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

```

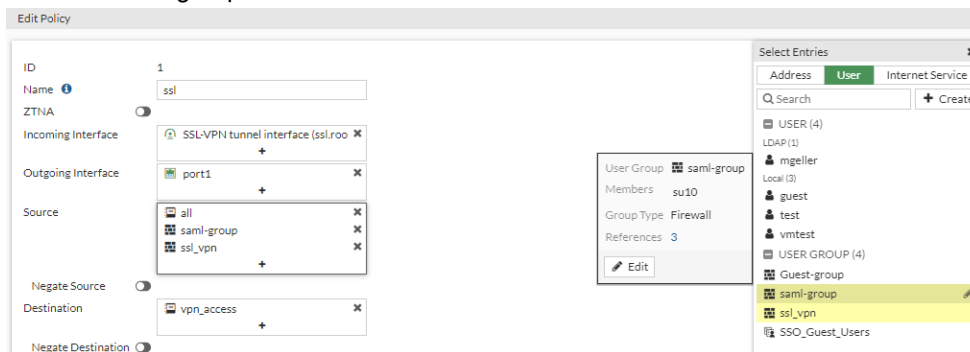
2. Ensure that the SAML redirect port is set to 8020. SAML external browser authentication uses port 8020 by default. If another service or application occupies this port, FortiClient displays a message showing that the SAML redirect port is unavailable:

```

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

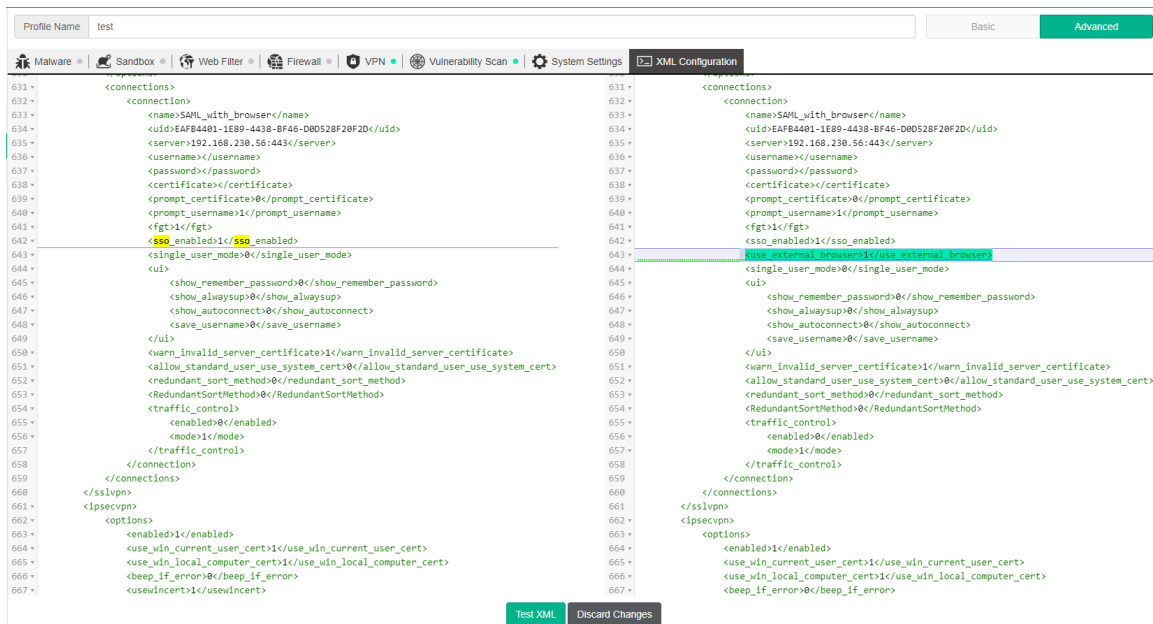
```

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 prelogon VPN connection without user interaction

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

XML tag	Description	Default value
<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

```

<ipseccvpn>
  <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 does not intend to cover all possible VPN tunnel configuration combinations.

Autoconnect on logging in as an Entra ID user

You can configure FortiClient to automatically connect to a specified VPN tunnel immediately after it installs and receives its configuration from EMS. In this example, FortiClient authenticates the connection using Microsoft Entra ID 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 Entra ID environment, that your FortiClient EMS and FortiGate are part of a Fortinet Security Fabric, and that the FortiGate has been configured in Azure as an enterprise application for SAML single sign on. See [Tutorial: Microsoft Entra 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 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:

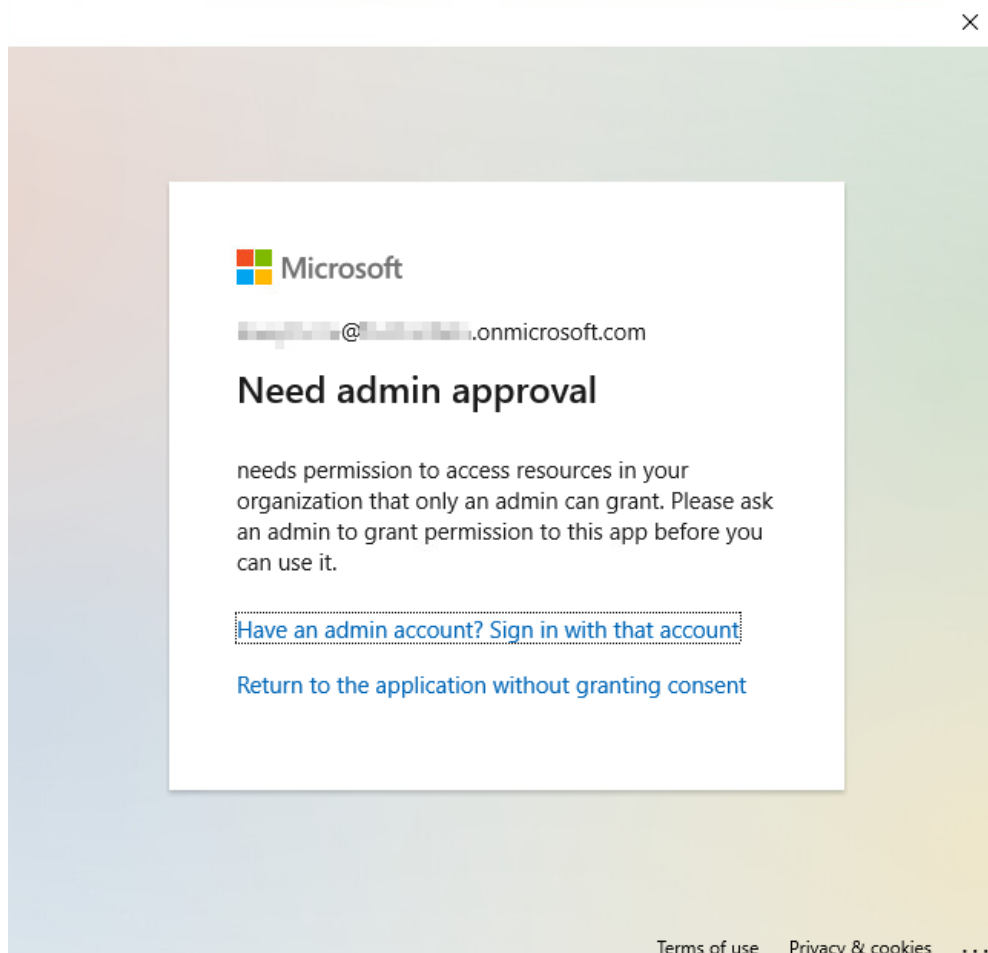
```
<vpn>
  <sslvpn>
    <connections>
      <connection>
        <name>SSL VPN HQ</name>
        <sso_enabled>1</sso_enabled>
        <azure_auto_login>
          <enabled>1</enabled>
          <azure_app>
            <tenant_name>Domain name obtained from the Azure portal</tenant_name>
           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

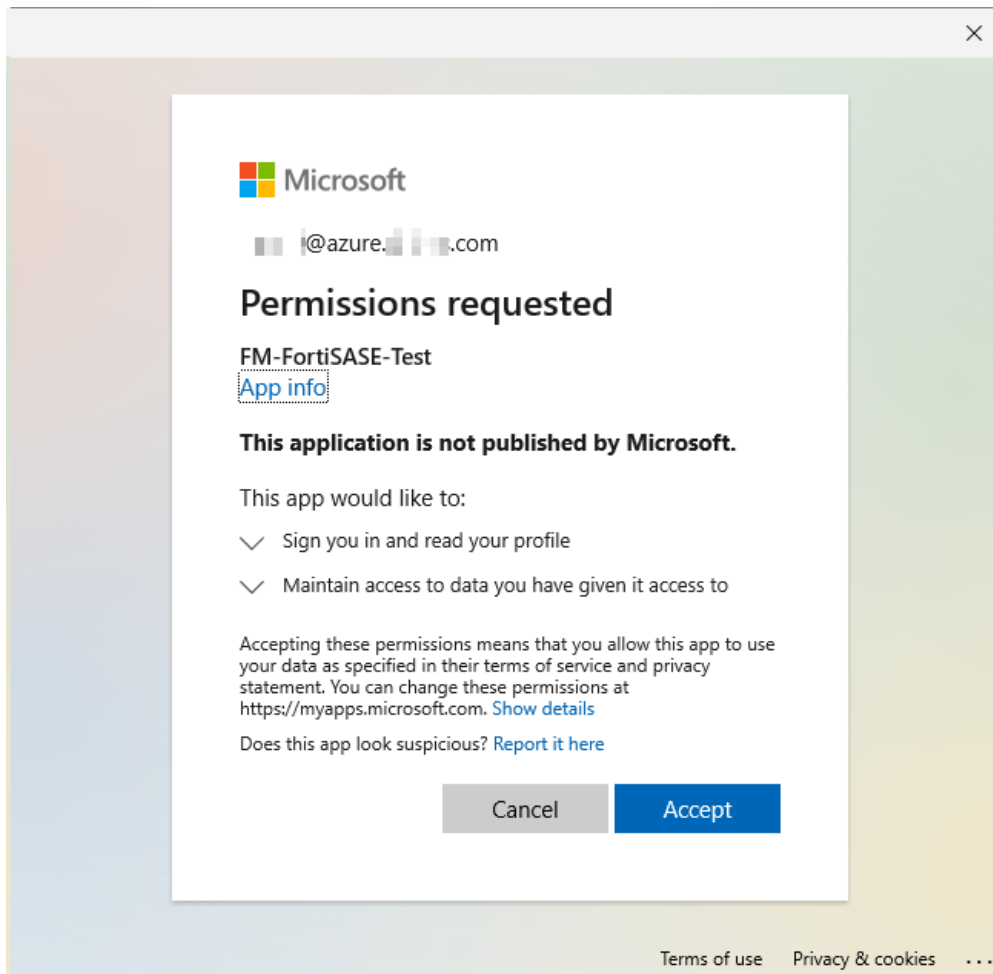
To manage application permissions:

1. As an end user, log in to an endpoint that has the profile configured in [To configure EMS: on page 169](#) 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. You should now configure one of the following permission options. These steps assume that you have already configured Azure SAML SSL/IPsec VPN autoconnect as this document describes and you are signed in as a global administrator of the same tenant.
3. To have *Need admin approval* shown to users, do the following:
 - a. In the Azure portal, go to *Enterprise Application* > <Your VPN application> > (sidebar) *Manage* > *Properties*.
 - b. Set *Assignment required?* to *Yes*.
 - c. Add the desired users to *Users & Groups*.
 - d. Remove any permissions in *App Registration*.
 - e. Go to *Home* > *App Registration* > <Your VPN application> > (sidebar) *Manage* > *API permissions*.
 - f. Right-click and remove permission.
- g. If you want to disallow user consent for all applications, you can disable this by doing the following:
 - i. Go to *Home* > *Enterprise Application* > <Your VPN application> > (sidebar) *Security* > *Consent and permissions* > *Manage* > *User consent settings*.
 - ii. For *User consent for applications*, select *Do not allow user consent*.



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

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



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

- *User > User.Read*
 - v. Add the permissions.
 - vi. After the permissions are added, they appear in the table on the same screen. Click *Grant admin consent for <Tenant name>*.
 - vii. Return to *Enterprise Applications Permissions* by clicking *Enterprise applications* in the sentence *To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try Enterprise applications*.
 - viii. The *Grant admin consent for <Tenant name>* button is blue instead of being grayed out. Click the button. A popup opens that requires you to sign in as a global administrator and to allow the application permissions. The permissions that you used in *App Permissions* fill in the following table.
- After you complete either step, users no longer need to request consent and can autoconnect to VPN without having to give consent.



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

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 [Zero Trust Network Access](#) 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.

To add a ZTNA destination:

1. Go to *Endpoint Profiles > ZTNA Destinations*.
2. Click *Add*.
3. Click *Advanced*.
4. Enable or disable the eye icon to show or hide this feature from the end user in FortiClient.
5. In the *Name* field, enter the desired name.
6. If desired, enable *Allow Personal Destinations*. This feature allows end users to configure personal ZTNA destinations.
7. Add a destination:
 - a. Under *Rules*, click *Add Destination*.
 - b. In the *Destination Name* field, enter the desired destination name.
 - c. In the *Destination Host* field, enter the IP address/FQDN and port of the destination host in the format *<IP address or FQDN>:<port>*.
 - d. In the *Proxy Gateway* field, enter the FortiGate access IP address and port in the same format.

- e. From the *Mode* dropdown list, select *Transparent*.
 - f. Enable or disable encryption. By default, encryption is disabled. When encryption is enabled, traffic between FortiClient and the FortiGate is always encrypted, even if the original traffic is already encrypted. When encryption is disabled, traffic between FortiClient and the FortiGate is unencrypted.
 - g. Enable or disable *User External Browser as User-agent for Saml User Authentication*. When you enable this feature, FortiClient presents a SAML authentication request to the end user in a web browser for traffic that is eligible for this rule.
 - h. Click **Save**.
8. Repeat the steps to configure multiple destinations for this profile as desired, then click **Save**.

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. If the webpage matches a given signature where the action is set to block or if *Block Access to Malicious Websites* is enabled on the *Application Firewall* profile, FortiClient blocks the webpage. See [Firewall on page 200](#). 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. 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 136.</p> <p>This setting affects the <i>Block Access to Malicious Websites</i> setting in Malware Protection on page 188.</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. Those logs are only logged locally or sent 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

Configuration		Description
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.
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.</p> <p>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>
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

Configuration	Description
	<ul style="list-style-type: none">• Lingerie and Swimsuit• Marijuana• Nudity and Risque• Other Adult Materials• Pornography• Sex Education• Sports Hunting and War Games• Tobacco• Weapons (Sales)
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	
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> <p>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.</p>

Configuration	Description
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	<p>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.</p> <p>Available options are:</p> <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	<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 URL ratings.</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: 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	<p>Enable to configure actions (block or monitor) to take when the user searches for terms that belong to the following categories:</p> <ul style="list-style-type: none"> • Violence/Terrorism • Extremist • Pornography • Cyber Bullying • Self Harm

Configuration	Description
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	
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 292](#).

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.

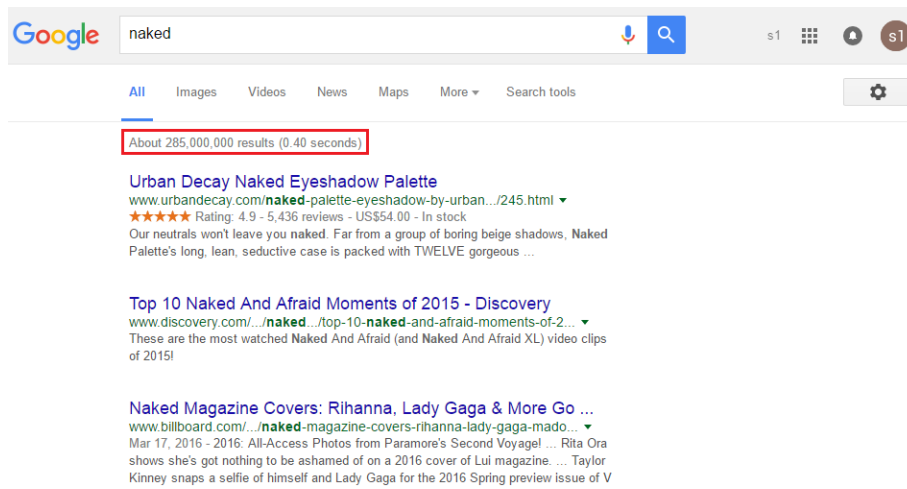
- a. **One Time Pull:** FortiClient EMS does not automatically sync profile changes from the FortiGate or FortiManager. You can manually sync profile changes after importing the profile. See [Syncing profile changes on page 143](#).
 - b. **Group Schedule:** Configure a group synchronization schedule 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 174](#).
 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

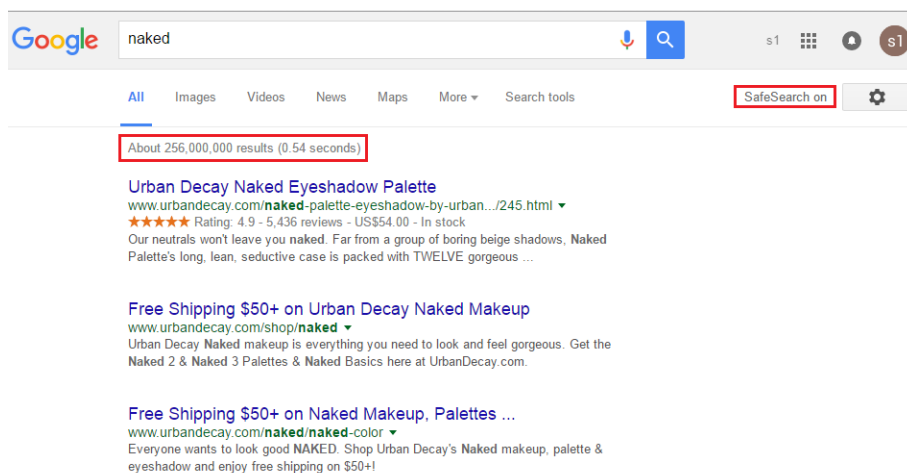
The search engine provides a Safe Search feature that blocks inappropriate or explicit images from search results. The Safe Search feature helps avoid most adult content. FortiClient EMS supports Safe Search for most common search engines, such as Google, Yahoo, and Bing.

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*.

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*.

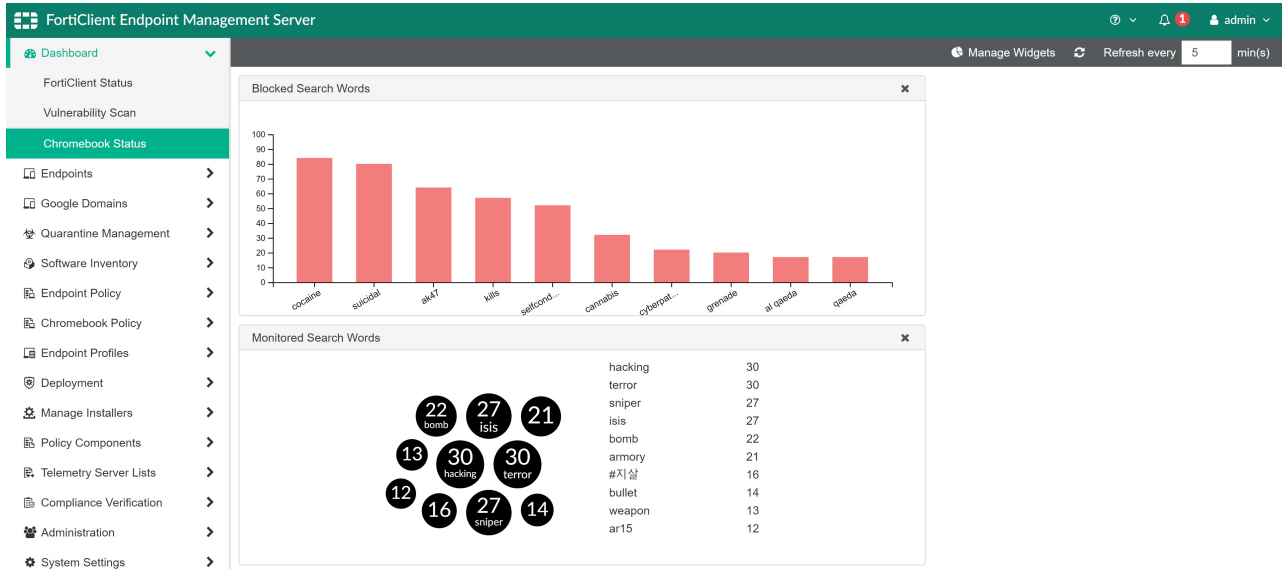
You can remove a term from the *Custom Banned Word* list by selecting the checkbox beside the term, then clicking the *Remove Word* button.

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*.

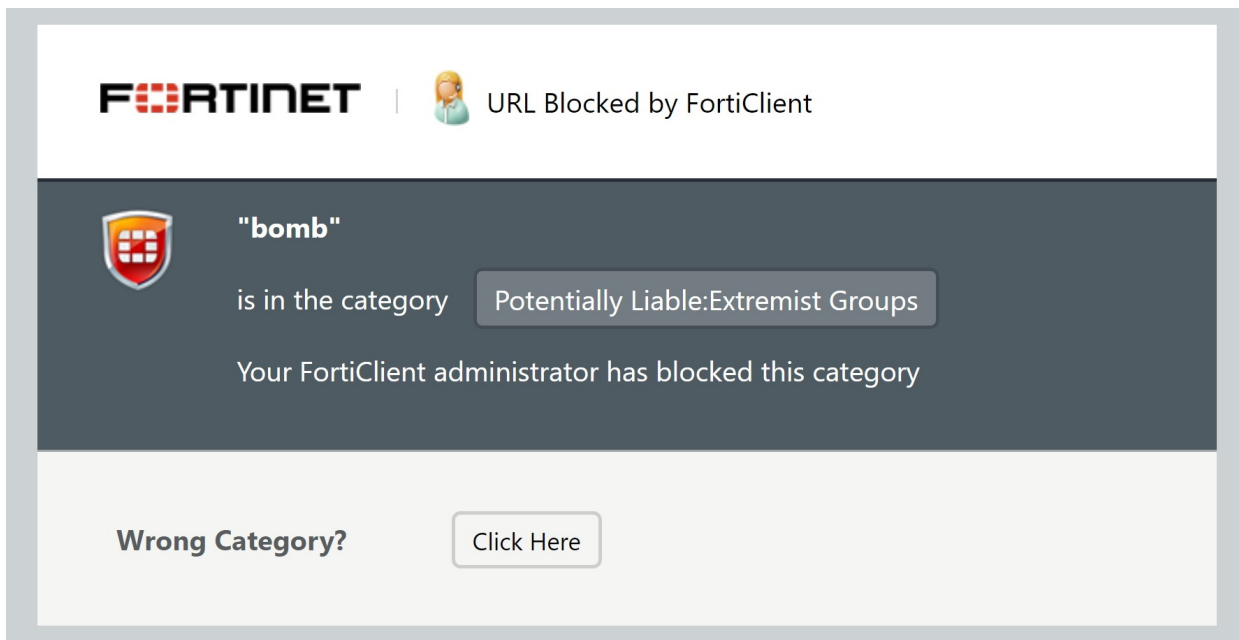
The screenshot displays the FortiClient Endpoint Management Server interface. The left sidebar shows the navigation menu with 'Endpoint Profiles' selected. The main content area shows the configuration for 'Default - Chromebooks' profile. The 'Web Filter' section is expanded, and 'Keyword Scanning on Search Engine' is enabled. Under 'Banned Word Search', five categories are listed: Violence/Terrorism, Extremist, Pornography, Cyber Bullying, and Self Harm. Each category has three buttons: 'Block' (green), 'Monitor' (blue), and 'Off' (grey). The 'Custom Banned Words' section is also enabled, showing a table with columns for 'Banned Word', 'Action', and 'Status'. The table contains several entries, including '#지살', 'War', 'Rifle', 'Bomb', 'Hacking', and 'Attack'. Each entry has a checkbox, an action dropdown, and a status toggle. At the bottom, there is an 'Exclusion List' section with a description and a 'Save' button.

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

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



When the user searches for a banned word, they see the following. In the example, the user searched for "bomb", which belongs to the Extremist category.



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> .
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	

Configuration	Description
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	<p>Disable automatic patching for the applications excluded from vulnerability compliance check.</p>

Malware Protection

The *Malware Protection* tab contains options for configuring antivirus (AV), antiransomware, antiexploit, 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.

Antiexploit

Enable antiexploit engine to detect suspicious processes (payload) running from legitimate applications. You must enable *Real-Time Protection* for the antiexploit 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	Configure the action to take with removable media devices connected to the endpoint that match this rule. Available options are: <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	Select <i>Simple</i> or <i>Regular Expression</i> for the rule type. When <i>Simple</i> is selected, FortiClient performs case-insensitive matching against classes, manufacturers, vendor IDs, product IDs, and revisions. 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.
Class	Enter the device class.
Manufacturer	Enter the device manufacturer.
Vendor ID	Enter the device vendor ID.
Product ID	Enter the device product ID.
Revision	Enter the device revision number.
Remove this rule	Remove this rule from the profile.
Add a new rule	Add a new removable media access rule.
Move this rule up/down	Move this rule up or down. If a connected device is eligible for multiple rules, FortiClient applies the highest rule to the device.
Default removable media access	Configure the action to take with removable media devices that do not match any configured rules. Available options are: <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 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. If multiple files are submitted around the same time, FortiClient sends one file to FortiClient Cloud Sandbox, waits until it receives the verdict for that file, then sends the next file to FortiClient Cloud Sandbox.



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.</p> <p>FortiClient Cloud Sandbox 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 does not offer the full range of features that a FortiSandbox appliance offers. FortiClient Cloud Sandbox is a service that uploads and analyzes files that FortiClient antivirus (AV) marks as suspicious.</p> <p>If FortiClient Cloud Sandbox 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 detection to ten hours if FortiGuard Labs is involved. FortiGuard Labs considers a file suspicious if it exhibits some unusual behavior, yet does not contain a known virus. The behaviors that it considers suspicious change depending on the current threat climate and other factors.</p> <p>FortiClient Cloud Sandbox is only available with the Endpoint Protection Platform license.</p>
IP address/Hostname	For a FortiSandbox appliance, enter the FortiSandbox's IP address, FQDN, or hostname.

Options	Description
	<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 99 .
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 99 .
Region	FortiClient Cloud Sandbox region. See Configuring FortiGuard Services settings on page 285 .
Time Offset	FortiClient Cloud Sandbox time offset. See Configuring FortiGuard Services settings on page 285 .
License Status	Displays the Sandbox Cloud license status. Using FortiClient Cloud Sandbox 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, html, 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.
File Submission Options	

Options	Description
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 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 address reputation database signatures. Check network traffic against known C&C IP address plus port number combinations.
Categories	Enable FortiClient firewall to allow, block, or monitor applications based on their signature.

Configuration	Description
	Block, allow or monitor the following categories: <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.
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.
Require Password to Disconnect from EMS	Turn on password lock for FortiClient.

Configuration	Description
Password	Enter a password. The endpoint user must enter this password to disconnect FortiClient from FortiClient EMS.
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) endpoints.
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 214 .
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	From the dropdown list, select the tab for FortiClient to display by default when the user opens the console.

Configuration	Description
Log	Specify FortiClient log settings.
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: system becomes unstable. Alert: immediate action is required. Critical: functionality is affected. Error: error condition exists and may affect functionality. Warning: functionality could be affected. Notice: information about normal events. Info: general information about system operations. Debug: debug FortiClient. Detailed debug logs for the selected features are generated on the endpoint. You can request the creation and download of the diagnostic tool output, which includes these logs.
Features	Select features to generate logs for.
Client-Based Logging When On-Fabric	<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 136.</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>
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.

Configuration		Description
	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.
	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.

Configuration	Description
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 unavailable.
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

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

Configuration	Description
Show Bubble Notifications	Show bubble notifications when FortiClient installs new policies on endpoints.
Log off When User Logs Out of Windows	Log off FortiClient when the endpoint user logs out of Windows. Turn off to remain logged in.
Disable Disconnect	Forbid users from disconnecting FortiClient from FortiClient EMS.
On-Fabric Subnets	Turn on to enable on-fabric subnets. 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 136 .
IP Addresses/Subnet Masks	Enter IP addresses/subnet mask to connect to on-fabric subnets.
Gateway MAC Address	Enable gateway MAC address.
MAC Addresses	Enter MAC addresses.
Send Software Inventory	Send installed application information to FortiClient EMS. If the <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 237 . This feature requires the EPP license. See FortiClient EMS on page 21 .
Invalid Certificate Action	Select the action to take when FortiClient attempts to connect to EMS with an invalid certificate: <ul style="list-style-type: none"> • Allow: allows FortiClient to connect to EMS with an invalid certificate. • Warn: warn the user about the invalid server certificate. Ask the user whether to proceed with connecting to EMS, or terminate the connection attempt. FortiClient remembers the user's decision for this EMS, but displays the warning prompt if FortiClient attempts to connect to another EMS (using a different EMS FQDN/IP address and certificate) with an invalid certificate. • Deny: block FortiClient from connecting to EMS with an invalid certificate.
User Identity Settings	
Allow Users to Specify Identity Using	Enable users to specify their identity in FortiClient using the following methods: <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

Configuration	Description
	<ul style="list-style-type: none"> • 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	Displays a notification on the endpoint for the user to specify their identity. If the user closes the notification without specifying their identity, the notification displays every ten minutes until the user submits their identity information.
Other	
Install CA Certificate on Client	Turn on to select and install a CA certificate on the FortiClient endpoint. You can add certificates by going to <i>Endpoint Policy & Components > CA Certificates</i> .
FortiClient Single Sign-On Mobility Agent	Enable single sign-on mobility agent (SSOMA) for FortiAuthenticator. To use this feature you must apply a FortiClient SSOMA license to your FortiAuthenticator.
IP Address/Hostname	Enter the FortiAuthenticator IP address or hostname.
Port	Enter the port number.
Pre-Shared Key	Enter the preshared key (PSK). The PSK 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.

Configuring identity compliance for endpoints

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

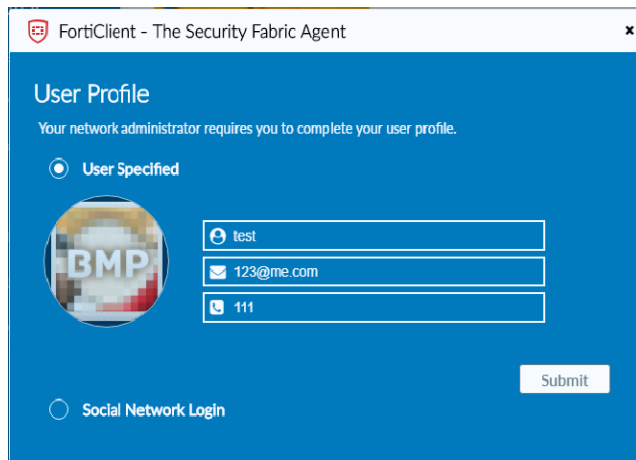
- User Input
- OS
- LinkedIn
- Google
- Salesforce

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 10 minutes.

To configure identity compliance:

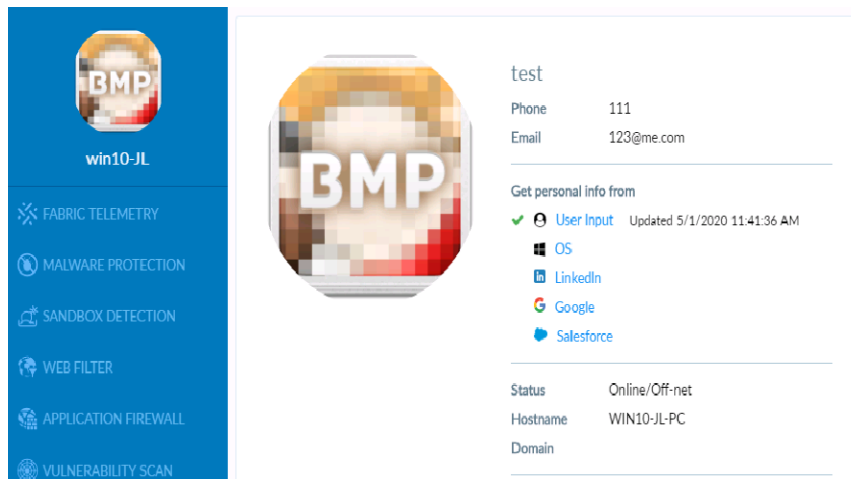
1. In EMS, go to *Endpoint Profiles*. Select the desired profile, or create a new one.
2. On the *System Settings* tab, under *User Identity Settings*, enable the desired user identification method.
3. If desired, enable *Notify Users to Submit User Identity Information*.
4. Click *Save*.

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.



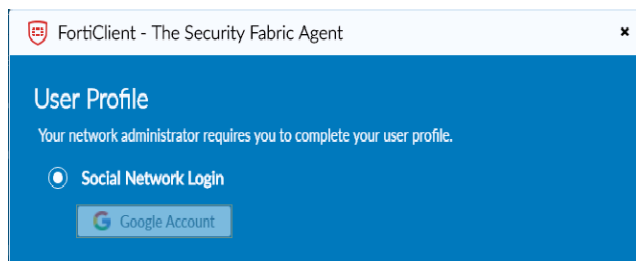
The screenshot shows the 'User Profile' dialog box in FortiClient. The title bar reads 'FortiClient - The Security Fabric Agent'. The main heading is 'User Profile' with a subtext: 'Your network administrator requires you to complete your user profile.' There are two radio buttons: 'User Specified' (selected) and 'Social Network Login'. Under 'User Specified', there are three input fields: a name field with 'test', an email field with '123@me.com', and a phone field with '111'. A 'Submit' button is at the bottom right. The 'Social Network Login' option is unselected.

FortiClient displays the entered login information.

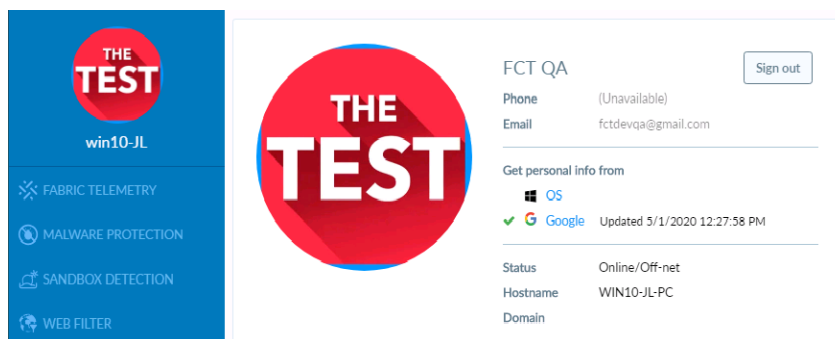


The screenshot shows the FortiClient user profile page. On the left is a blue sidebar with the FortiClient logo (BMP) and the text 'win10-JL'. Below the logo are several security features: FABRIC TELEMETRY, MALWARE PROTECTION, SANDBOX DETECTION, WEB FILTER, APPLICATION FIREWALL, and VULNERABILITY SCAN. The main area has a white background. At the top left is a large circular profile picture (BMP). To its right, the username 'test' is displayed. Below the username, the phone number '111' and email '123@me.com' are listed. A section titled 'Get personal info from' shows a green checkmark next to 'User Input' with the text 'Updated 5/1/2020 11:41:36 AM'. Below this are icons for OS, LinkedIn, Google, and Salesforce. At the bottom, a table shows the user's status: 'Status: Online/Off-net', 'Hostname: WIN10-JL-PC', and 'Domain'.

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



FortiClient displays the Google login information.



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*.

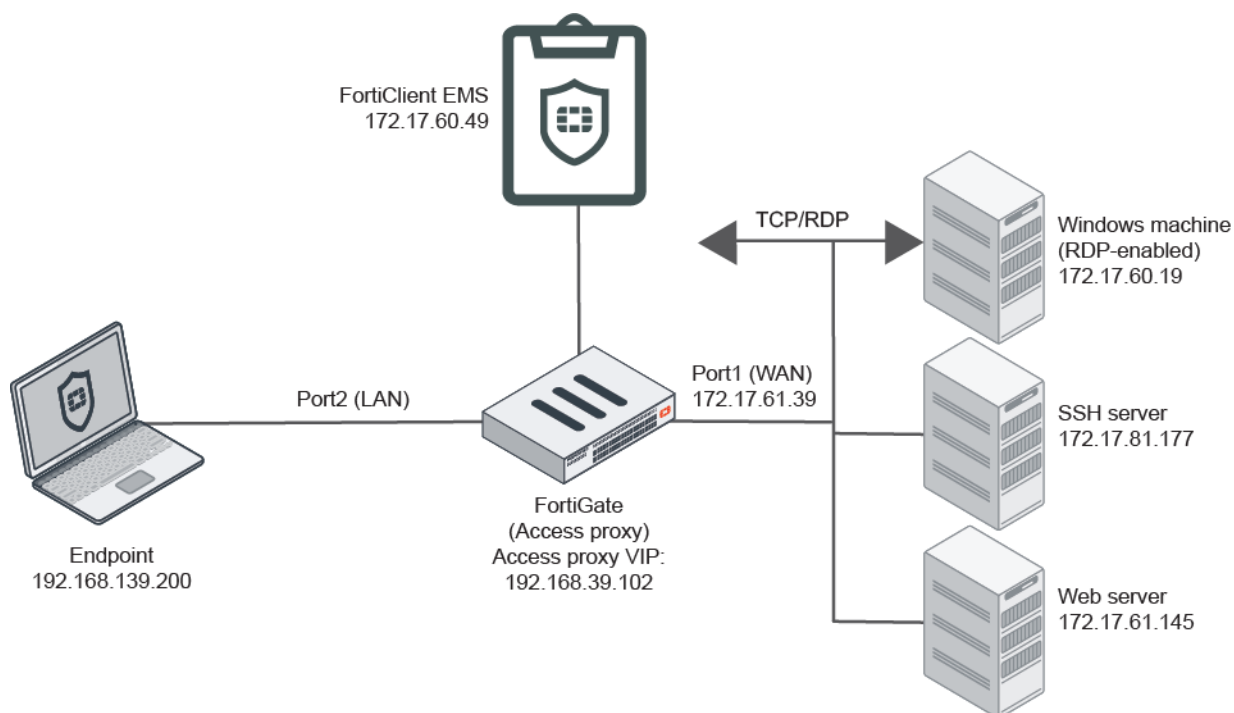
If the profile has a feature enabled that is disabled in Feature Select, EMS displays a warning that the feature will not be enabled on endpoints that the profile is deployed to. To enable this feature on the endpoint, you must enable the feature in Feature Select. See [Feature Select on page 292](#).

Configuring encrypted ZTNA rules

FortiClient supports encryption and non-encryption modes for Zero Trust Network Access (ZTNA) via a toggle switch. You can manually add ZTNA rules in the FortiClient GUI or receive rules from EMS. This feature requires the prerequisites:

- A Security Fabric connector between FortiOS and EMS must be configured.
- FortiOS ZTNA-related settings must be configured properly. See [ZTNA TCP forwarding access proxy example](#).
- FortiClient must be registered to EMS.
- You must add ZTNA rules in EMS or FortiClient.

The following shows the topology for the example configuration. In this topology, RDP access is configured to one server, and SSH access to another.



To configure ZTNA rules in EMS:

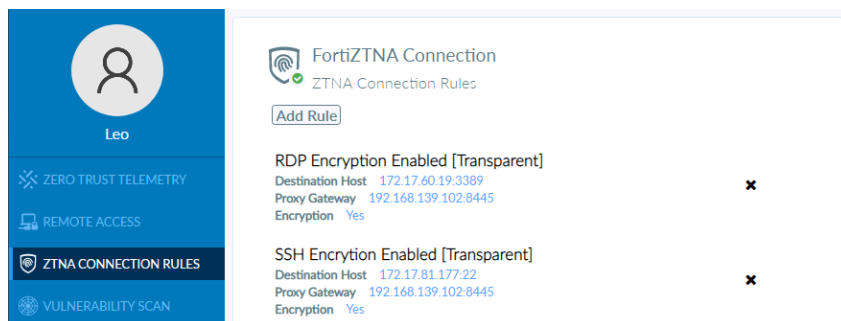
1. In EMS, go to *Endpoint Profiles > Manage Profiles*.
2. Edit the desired profile.
3. On the *XML Configuration* tab, add the following configuration:

```
<ztna>
  <enabled>1</enabled>
  <rules>
    <rule>
      <name>RDP Forwarding</name>
      <destination>172.17.60.19:3389</destination>
      <gateway>192.168.139.102:8445</gateway>
      <encryption>1</encryption>
      <mode>transparent</mode>
    </rule>
    <rule>
      <name>SSH Forwarding</name>
      <destination>172.17.81.177:22</destination>
      <gateway>192.168.139.102:8445</gateway>
      <encryption>1</encryption>
      <mode>transparent</mode>
    </rule>
  </rules>
</ztna>
```

4. Save the configuration.

To configure ZTNA rules in FortiClient:

1. In FortiClient, go to the *ZTNA Connection Rules* tab.
2. Create the RDP forwarding rule:
 - a. Click *Add Rule*.
 - b. In the *Rule Name* field, enter RDP Encryption Enabled.
 - c. In the *Destination Host* field, enter 172.17.60.19:3389.
 - d. In the *Proxy Gateway* field, enter 192.168.139.102:8445.
 - e. For *Mode*, select *Transparent*.
 - f. Select the *Encryption* checkbox.
3. Create the SSH forwarding rule:
 - a. Click *Create*.
 - b. Click *Add Rule*.
 - c. In the *Rule Name* field, enter SSH Encryption Enabled.
 - d. In the *Destination Host* field, enter 172.17.81.177:22.
 - e. In the *Proxy Gateway* field, enter 192.168.139.102:8445.
 - f. For *Mode*, select *Transparent*.
 - g. Select the *Encryption* Checkbox.
 - h. Click *Create*.



To verify the configuration:

1. Start an SSH connection to 172.17.81.177 via ZTNA.
2. Run debug commands in FortiOS:

```
diagnose wad debug enable category all
diagnose wad debug enable level verbose
diagnose debug enable
```
3. Check the debug logs to verify whether encryption is enabled. When encryption is enabled, the debug logs contain the line `GET tcpaddress=172.17.81.177&port=22&tls=1 HTTP1.1`. When encryption is disabled, the debug logs contain the line `GET tcpaddress=172.17.81.177&port=22&tls=0 HTTP1.1`.

Zero Trust Tags

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.

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 277](#).
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 222](#).

You can enable a maximum of ten rule sets.

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 217](#) 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:

- Click *Edit Logic*.
- 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

Type	Value
Windows (2)	
AntiVirus Software	1 AV Software is installed and running
OS Version	2 Windows 7 3 Windows 10

Rule Logic

- Click *Save*.

Editing a Zero Trust tagging rule set

To edit a Zero Trust tagging rule:

- Go to *Zero Trust Tags > Zero Trust Tagging Rules*.
- Select the Zero Trust tagging rule.
- Click *Edit*.
- Edit as desired.
- 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*.

FortiClient Endpoint Management Server

</

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*.

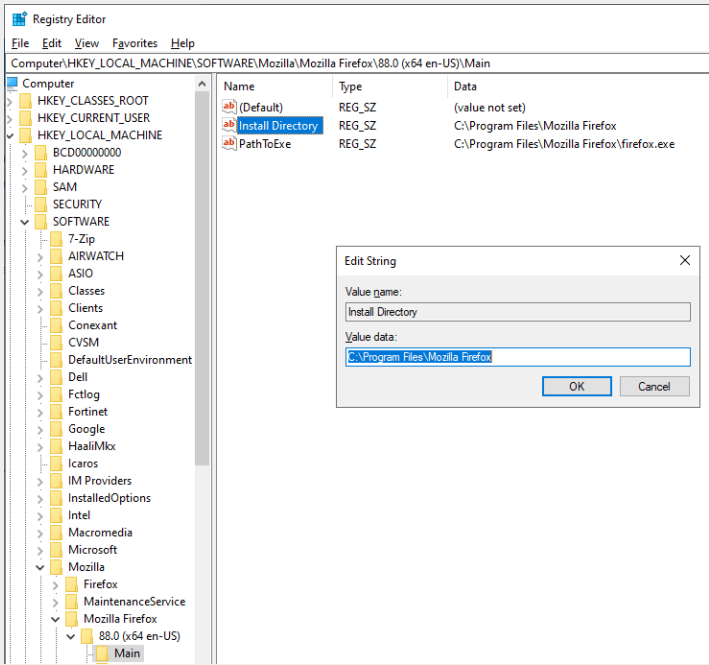
Zero Trust tagging rule types

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 	<p>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.</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>

Rule type	OS	Description
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> <p>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.</p>
EMS Management	<ul style="list-style-type: none"> Windows macOS Linux iOS Android 	<p>EMS considers the endpoint as satisfying the rule if the endpoint has FortiClient installed and Telemetry connected to EMS.</p>
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>

Rule type	OS	Description
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 	<p>In the <i>Registry Key</i> field, enter the registry path or value name. End the path with \ to indicate a registry path, or without \ to indicate a registry value name. You can also use the NOT option to indicate that the rule requires that a certain registry path or value name is not present on the endpoint. This rule does not support using the value data.</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\88.0 (x64 en-US)\Main</code>. The value name is <code>Install Directory</code>, and the value data is <code>C:\Program Files\Mozilla Firefox</code>. You can configure a registry key rule to match <code>HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox\88.0 (x64 en-US)\Main</code> as the path or <code>Install Directory</code> as the registry value name, but you cannot configure a rule to match <code>C:\Program Files\Mozilla Firefox</code>.</p>

Rule type	OS	Description
		 <p>The endpoint must satisfy all configured conditions to satisfy this rule. For example, if the rule is configured to require registry key A, registry key B, and NOT registry key C, then the endpoint must have both registry keys A and B and not registry key C.</p>
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> <p>Only FortiClient 6.2.2+ endpoints support this rule type.</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.

Rule type	OS	Description
		<ul style="list-style-type: none"> • Specified: enter a specific Google, LinkedIn, or Salesforce account. For example, you can enter joanexample@gmail.com to configure the rule to apply specifically to only that Google account. You can specify multiple social network accounts. • Verified User: endpoint user must be a verified user that has authenticated their connection to EMS as a member of an authorized user group. See User Management on page 260. <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. 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 	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.
Security	<ul style="list-style-type: none"> • macOS 	Select the checkbox to require that File Vault is enabled on the endpoint. You can also use the NOT option to indicate that the rule requires that File Vault is disabled on the endpoint.
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.

Rule type	OS	Description
		<ul style="list-style-type: none"> • 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>

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 214 .
FortiGuard outbreak alert tags	See FortiGuard Outbreak Alerts on page 235 .
Classification tags	See Viewing the Endpoints pane on page 90 .
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 an endpoint profile. See System Settings on page 201. 2. FortiClient connects to EMS and receives FortiAnalyzer connection information from the endpoint 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>. Note that this tag displays as a

Tag	Description
	<p>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 90.</p> <p>7. If FortiGate is configured to receive all tags for this specific endpoint, EMS sends the tag to FortiGate.</p> <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 224](#)
2. [Configuring the EMS connector on page 225](#):
 - a. [Uploading certificates to EMS and FortiOS on page 225](#)
 - b. [Creating the EMS connector in FortiOS on page 225](#)
 - c. [Authorizing the FortiOS EMS connector in EMS on page 226](#)
 - d. [Verifying the FortiOS-EMS connection in FortiOS on page 227](#)
3. [Creating a dynamic firewall policy using dynamic endpoint groups from EMS on page 227](#)



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 214](#).
- 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 222](#).

- 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.

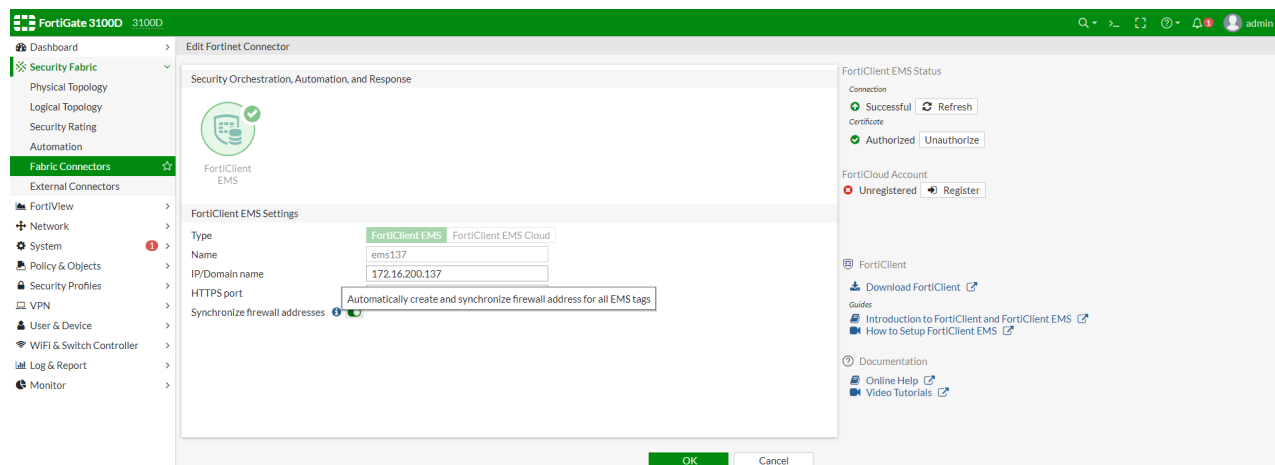
Creating the EMS connector in FortiOS

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. Click *Create New*, then select *FortiClient EMS*.
3. For *Type*, select *FortiClient EMS*.
4. In the *Name* field, enter the desired name.
5. 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 `side.fqdn` to integrate the FortiGate to the a specific EMS multitenancy site. For example, if the site name is site A, enter `sitea.ems.example.com`. See [Multitenancy on page 295](#).
6. Ensure that *Synchronize firewall addresses* is enabled. This allows FortiOS to automatically create and synchronize firewall addresses for dynamic endpoint groups received from EMS.

7. 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 252](#).

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=FGVM01TM19005986, 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:

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

Name	Type	Details	Interface
FABRIC_DEVICE	Subnet	0.0.0.0/0	
FCTEMS2729..._ems138_critical_vuln_tag	Dynamic (FortiClient EMS Tag)	FCTEMS2729..._ems138_critical_vuln_tag	
FCTEMS2729..._ems138...	Address	FCTEMS2729..._ems138_critical_vuln_tag	
FCTEMS2729..._ems138...	Type	Dynamic	
FIREWALL_AUTH_PORTAL_AD	Sub Type	FortiClient EMS Tag	
SSLVPN_TUNNEL_ADDR1	Interface	any	
_upg_autoupdate.opera.com	Resolved To	10.1.100.120	
_upg_google-play	References	0	
_upg_swscan.apple.com			

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 Fortinet 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 224](#)
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.
 - 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 are 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.

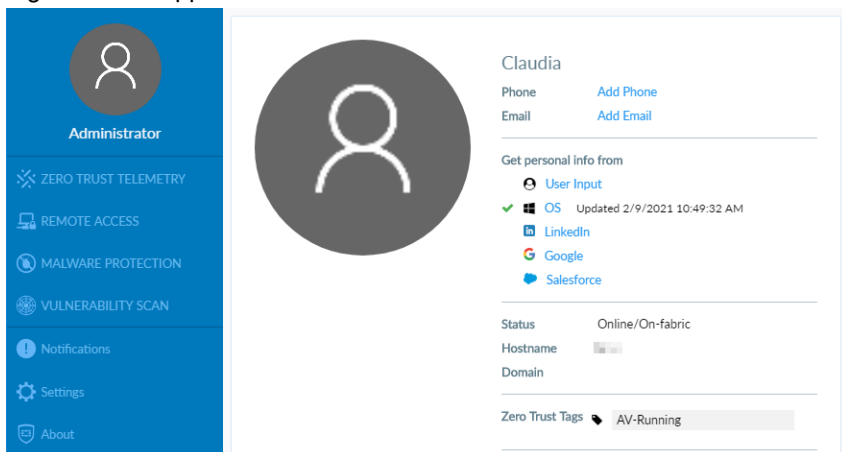
ID	Name	Source	Destination	Schedule	Service	Action	NAT
<div> Create New Edit Delete Policy Lookup <input type="text"/> <input type="button" value="Q"/> </div>							
<div> GuestWiFi (guestwifi) → wan </div>							
2		all	all	always	ALL	✓ ACCEPT	✓ Enabled
<div> internal → wan </div>							
1		all	all	always	ALL	✓ ACCEPT	✓ Enabled
<div> internal → wwan </div>							
3		all	all	always	ALL	✓ ACCEPT	✓ Enabled
<div> SSL-VPN tunnel interface (ssl.root) → internal </div>							
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

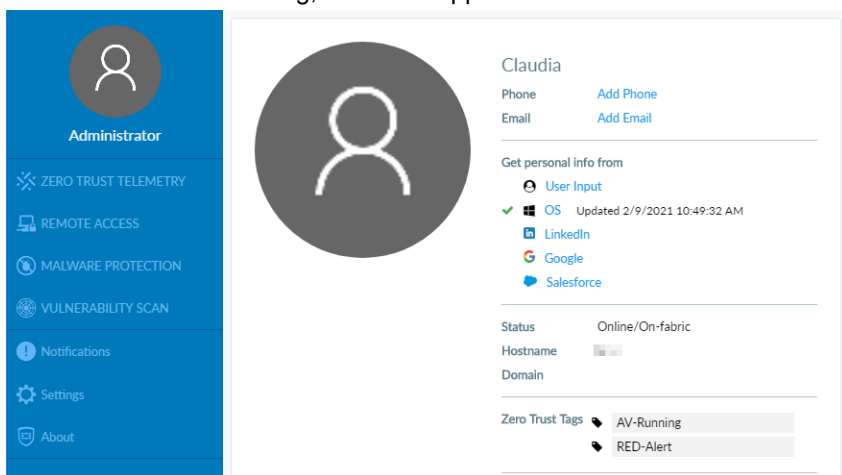
To verify the configuration for IPsec VPN on FortiClient:

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

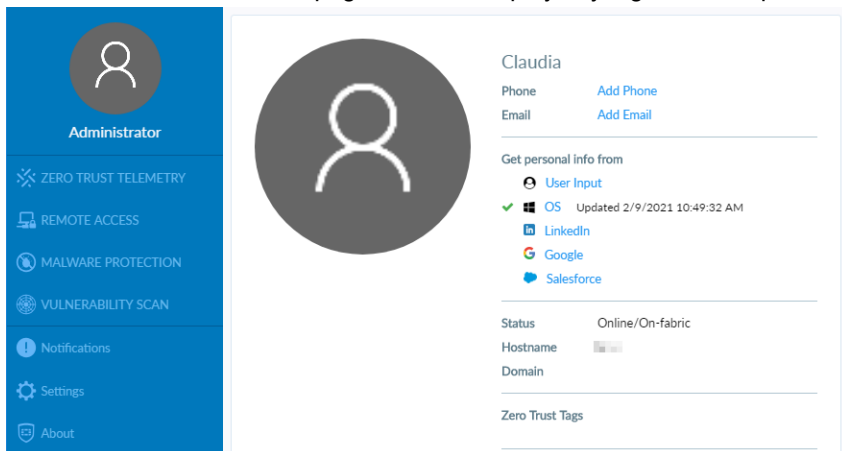
3. Ensure that EMS and FortiOS apply the correct tags and policies for a compliant endpoint:
 - a. On the user details page, ensure that EMS has applied the appropriate tag. In this example, the AV-Running tag should be applied.



- 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.

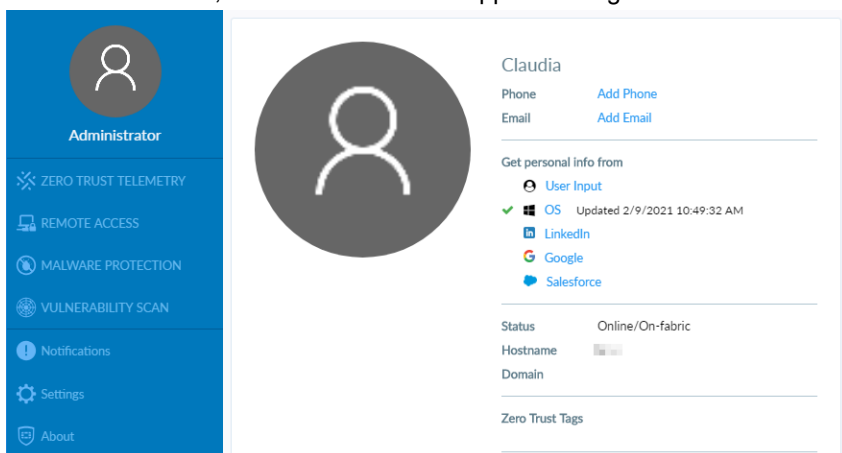


5. Ensure that EMS and FortiOS apply the correct tags and policies for a rogue endpoint:
 - a. Delete the risk.txt file, and stop AV services.
 - b. Ensure that the user details page does not display any tags. The endpoint should lose network access.



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

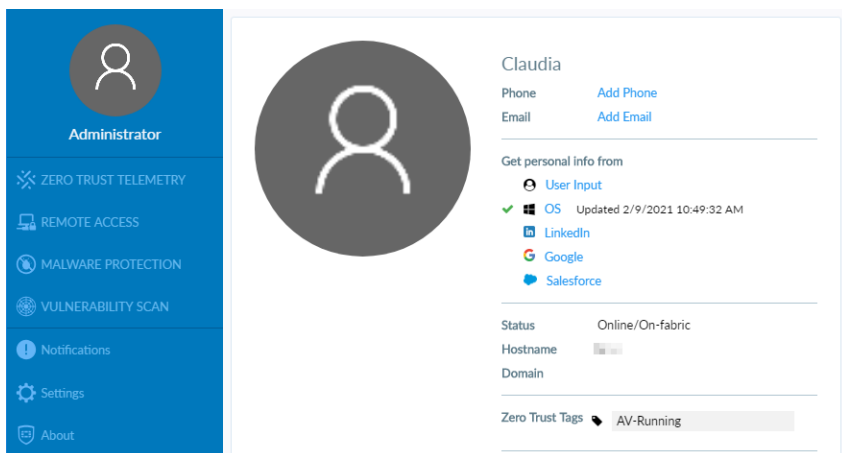
Deauthenticate

Show all FSSO Logons

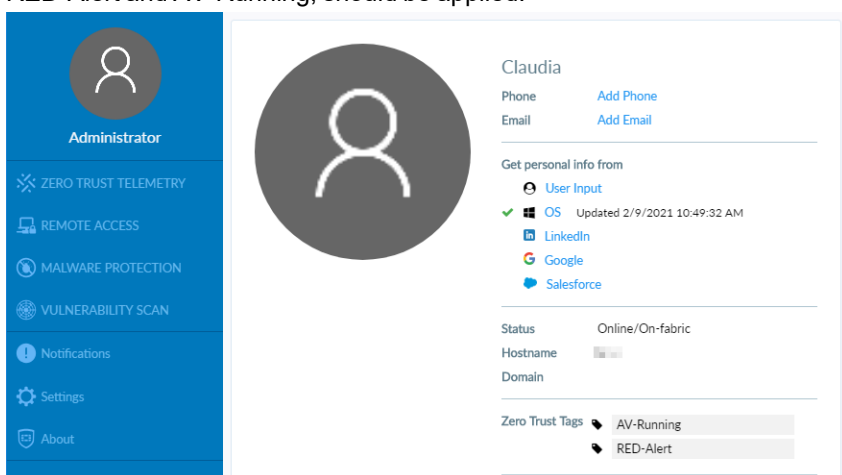
Search

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

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 FortiGate devices that are connected to EMS. For information on connecting a FortiGate to EMS, see [FortiOS dynamic policies using EMS dynamic endpoint groups on page 224](#).

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 224](#).

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

☒

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	1	CVE-2022-24508
	2	CVE-2021-34523
	3	CVE-2021-31207
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 201](#).

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

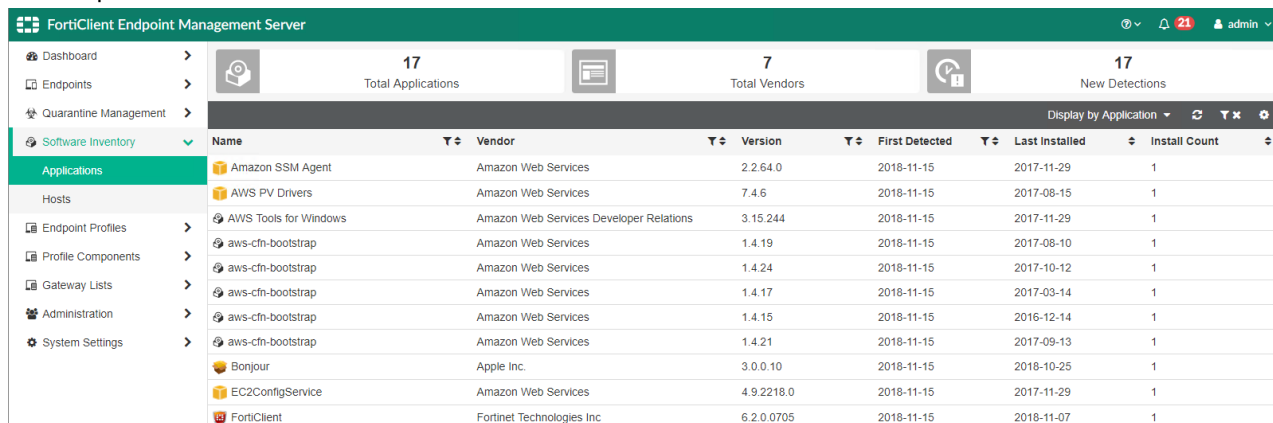
Applications

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 237 .
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 238](#) 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.

The screenshot shows the 'Filters' panel in the FortiClient EMS interface. It contains a grid of filter categories, each with a search input field and a 'Clear' button. The categories are: Filename, Threat, Date, Location, Source, Host, Checksum, Status, and Group. The Date field is expanded to show 'Start' and 'End' input fields with a 'to' separator. At the bottom right of the panel are 'Apply' and 'Clear' buttons.

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 248 .
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 247 .
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*, do the following to connect to a new LDAP server:
 - a. Configure the following:

Option		Description
IP address/Hostname		Enter the user server IP address or name.
Port		Enter the port for EMS to use to connect to the user server.
Distinguished name		Enter the user server distinguished name (DN). You must use only capital letters when configuring the DN.
Bind type		Select <i>Simple</i> , <i>Anonymous</i> , or <i>Regular</i> for the bind type.
Username		Appears only when the <i>Regular</i> bind type is selected. Enter the username.
Password		Appears only when the <i>Regular</i> bind type is selected. Enter the password.
Show Password		Show the password.
LDAPS connection		Enable LDAPS connection.

- b. Click *Test* to check the LDAP server settings.
5. Click *Next*.

6. Configure the permissions:

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 248 .
Domain Access	Select or add access to a domain for the Windows/LDAP user.
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 *User Settings > Allowed inactive days*. See [Configuring User Settings on page 252](#).

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 unauthorized 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 249](#).
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.

The table denotes permissions that apply to Chromebook management 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 246 .
Manage Google domains*	Manage connections to Google domains to decide which Chromebooks to manage. See Google Domains on page 112 .
Manage custom groups	Create, rename, and edit groups to manage endpoints. See Managing groups on page 88 .
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 102 .
Block/Unblock/Quarantine/Unquarantine/Reregister endpoints	Manage endpoint access to the network through blocking, quarantine, and registration. See Managing endpoints on page 102 .
Manage and assign endpoint policies	See Endpoint Policy & Components on page 128 .
View group assignment rules	View group assignment rules. See Group assignment rules on page 109 .
Manage group assignment rules	Create, delete, and edit group assignment rules. See Group assignment rules on page 109 .
View endpoint filter bookmarks	View endpoint filter bookmarks. See Using bookmarks to filter the list of endpoints on page 98 .
Manage endpoint filter bookmarks	Create, delete, and edit endpoint filter bookmarks. See Using bookmarks to filter the list of endpoints on page 98 .
View quarantine management	View lists of quarantined and allowlisted files. See Quarantine Management on page 240 .

Permission	Link to description
Manage quarantine management	Allowlist and restore quarantined files and remove files from the allowlist. See Quarantine Management on page 240 .
View software inventory	See Software Inventory on page 237 .
Manage software inventory	See Software Inventory on page 237 .

Policy permissions

Permission	Link to description
View endpoint policies*	View endpoint policies. See Endpoint Policy & Components on page 128 .
View endpoint profiles*	View endpoint profiles. See Endpoint Profiles on page 141 .
Manage endpoint profiles*	Create, delete, and edit endpoint profiles. See Endpoint Profiles on page 141 .
View Zero Trust tagging rules	View Zero Trust tagging rules. See Zero Trust Tagging Rules on page 214 .
Manage Zero Trust tagging rules	Create, delete, and edit Zero Trust tagging rules. See Zero Trust Tagging Rules on page 214 .
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 123 .
Manage installers	Create, delete, and edit installers. See FortiClient Installer on page 123 .
View CA certificates	View CA certificates. See CA Certificates on page 134 .
Manage CA certificates	Upload, import, and delete CA certificates. See CA Certificates on page 134 .
View on-fabric detection rules	View on-fabric detection rules. See On-fabric Detection Rules on page 136 .
Manage on-fabric detection rules	Create, delete, and edit on-fabric detection rules. See On-fabric Detection Rules on page 136 .

Setting permissions

Permission	Link to description
View server settings*	View <i>Server</i> settings. See Configuring EMS settings on page 277
Manage server settings*	Modify <i>Server</i> settings. See Configuring EMS settings on page 277 .
View Fortinet services settings	View <i>FortiGuard Services</i> settings. See Configuring FortiGuard Services settings on page 285 .
Manage Fortinet services settings	Modify <i>FortiGuard Services</i> settings. See Configuring FortiGuard Services settings on page 285 .
View endpoint settings	View <i>Endpoints</i> settings. See Configuring EMS settings on page 277 .
Manage endpoint settings	Modify <i>Endpoints</i> settings. See Configuring EMS settings on page 277 .
View login banner settings*	View login banner settings. See Configuring EMS settings on page 277 .
Manage login banner settings*	Modify login banner settings. See Configuring EMS settings on page 277 .
View alert settings*	View <i>Alerts</i> settings. See Alerts on page 287 .
Manage alert settings*	Modify <i>Alerts</i> settings. See Alerts on page 287 .
View custom message settings	View endpoint quarantine message settings. See Customizing the endpoint quarantine message on page 290 .
Manage custom message settings	Modify endpoint quarantine message settings. See Customizing the endpoint quarantine message on page 290 .
View feature select settings	View feature select settings. See Feature Select on page 292 .
Manage feature select settings	Modify feature select settings. See Feature Select on page 292 .

Configuring User Settings

To configure User Settings:

1. Go to *Administration > 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 this field is specified 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 247 .
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 Fabric devices that the EMS has authorized in *Administration > Fabric Devices*. You can also deny or authorize a Fabric device. These Fabric devices receive endpoint data from EMS. FortiClient does not directly connect to Fabric devices listed on this page.

FortiClient Endpoint Management Server

Dashboard

Endpoints

Quarantine Management

Software Inventory

Endpoint Policy

Endpoint Profiles

Deployment

Manage Installers

Policy Components

Telemetry Server Lists

Compliance Verification

Administration

Administrators

































Admin Roles

User Servers

User Settings

Fabric Devices

Refresh

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=FGVM01TM19005986, 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	

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](#). The communication between EMS and FortiAnalyzer is unencrypted.

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 Fabric device receives all endpoints' resolved IP or MAC addresses (hereafter referred to as "host tag"), regardless of whether the gateways point to the selected Fabric device.
Only share FortiClients connected to this fabric device (Recommended)	This is the default setting. The selected Fabric device only receives the host tags for endpoints whose gateways point to the selected Fabric device.
Share FortiClients connected to selected fabric devices	The selected Fabric device receives host tags for the following: <ul style="list-style-type: none"> • Endpoints whose gateways point to the selected Fabric device • Endpoints whose gateways point to the configured additional Fabric devices. You can configure up to four additional Fabric devices.

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 214 .
FortiGuard outbreak alert tags	See FortiGuard Outbreak Alerts on page 235 .
Classification tags	See Viewing the Endpoints pane on page 90 .
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 an endpoint profile. See System Settings on page 201. 2. FortiClient connects to EMS and receives FortiAnalyzer connection information from the endpoint 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>. Note that this tag displays as a 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 90. 7. If FortiGate is configured to receive all tags for this specific endpoint, EMS sends the tag to FortiGate.

Tag	Description
	See EMS API support for FortiAnalyzer to notify and tag suspicious endpoints.

5. Click **Save**.

To change the Fabric device authorization status:

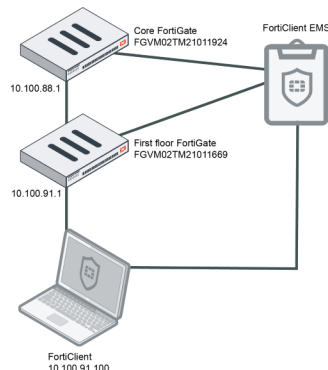
1. Go to *Administration > Fabric Devices*.
2. Select the desired Fabric device.
3. Click *Deny* or *Authorize*. The Fabric device status in the *Authorized* column changes.

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:

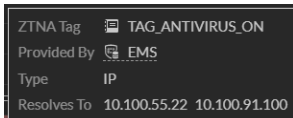
- Both FortiGates are connected to EMS as part of a Security Fabric.
- FortiClient is registered to EMS.
- The FortiClient gateway points to the first floor FortiGate.
- The FortiClient endpoint has the TAG_ANTIVIRUS_ON Zero Trust tag applied.
- The host tag of the FortiClient endpoint with TAG_ANTIVIRUS_ON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



SAML SSO

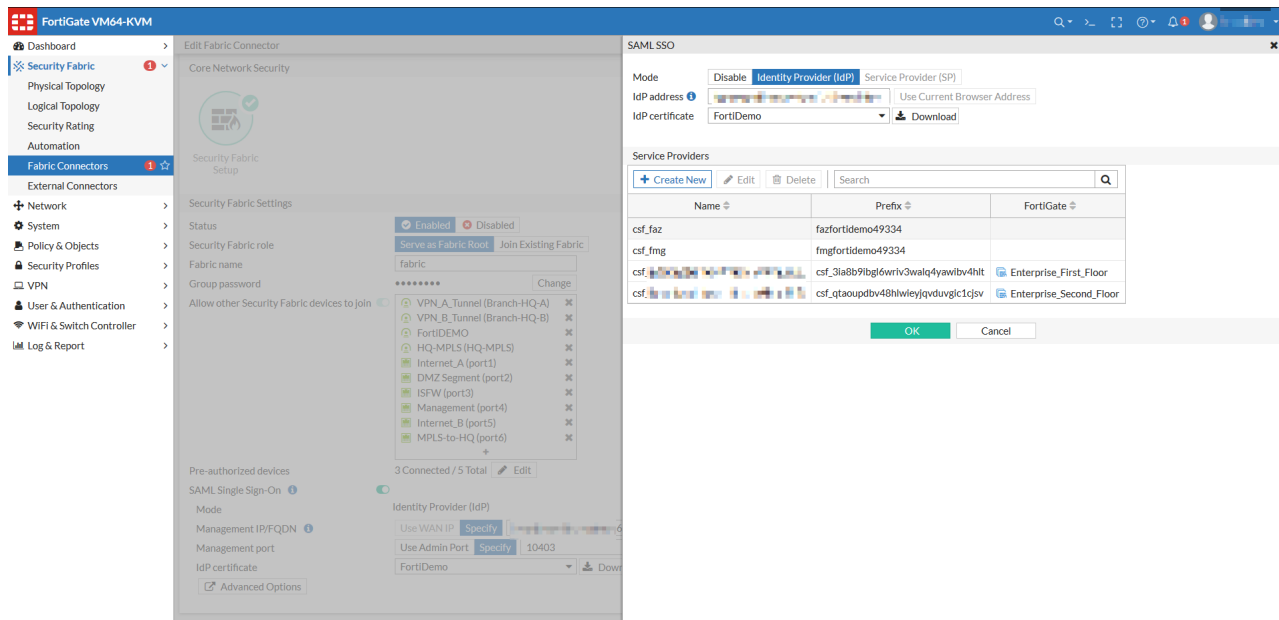
You can enable SAML SSO to allow users to log in to EMS using a FortiGate as an Identity Provider (IdP).



You can only use the SAML SSO feature in EMS with a FortiGate as the IdP. EMS does not support using FortiAuthenticator as an IdP or custom IdPs.

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

FortiClient Endpoint Management Server

SAML SSO

Enable SAML SSO ☒

⚠ SAML SSO is designed to be used with FortiGate. Custom IdP's are not supported

Service Provider Settings

SP Address

SP Certificate

Identity Provider Settings

IDP Address

Prefix

IDP Certificate 2029-05-21

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 277](#).

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 44](#).

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 263 .
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 264 .

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 260](#).
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 265](#).
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 user groups from all imported LDAP servers.

+ Add				Refresh	Clear Filters
Group Name	Server	Distinguished Name	Users	Last Synced	Invitation Status
Administrators	172.16.1.1	DC=qa,DC=fortinet,DC=local	4	2022-05-24 14:49:47	None
Administrators	172.16.1.1	DC=ztnademo1,DC=net	2	2022-05-24 14:52:47	Created
Business	172.16.1.1	OU=Los Angeles,OU=United States,OU=End Points,...	50	2022-05-24 15:11:48	None
City	172.16.1.1	OU=Los Angeles,OU=United States,OU=End Points,...	50	2022-05-24 15:11:48	None
Domain Admins	172.16.1.1	DC=ztnademo1,DC=net	1	2022-05-24 14:52:47	Created
Domain Admins	172.16.1.1	DC=qa,DC=fortinet,DC=local	5	2022-05-24 14:49:47	None
Economics	172.16.1.1	OU=Los Angeles,OU=United States,OU=End Points,...	50	2022-05-24 15:11:48	None
EMS196	172.16.1.1	DC=qa,DC=fortinet,DC=local	4	2022-05-24 14:49:47	None
EMS48	172.16.1.1	DC=qa,DC=fortinet,DC=local	3	2022-05-24 14:49:47	None
Engineering	172.16.1.1	DC=qa,DC=fortinet,DC=local	1	2022-05-24 14:49:47	None
Enterprise Admins	172.16.1.1	DC=qa,DC=fortinet,DC=local	3	2022-05-24 14:49:47	None
Enterprise Admins	172.16.1.1	DC=ztnademo1,DC=net	1	2022-05-24 14:52:47	Created
Estester-Group	172.16.1.1	DC=qa,DC=fortinet,DC=local	3	2022-05-24 14:49:47	None
Fire Department	172.16.1.1	OU=Los Angeles,OU=United States,OU=End Points,...	50	2022-05-24 15:11:48	None
Friends_OU	172.16.1.1	OU=Friends_OU,DC=fortinet,DC=burnaby	7	2022-05-24 14:52:48	Created
Group Policy Creator Owners	172.16.1.1	DC=ztnademo1,DC=net	1	2022-05-24 14:52:47	Created
Group Policy Creator Owners	172.16.1.1	DC=qa,DC=fortinet,DC=local	2	2022-05-24 14:49:47	None
Health	172.16.1.1	OU=Los Angeles,OU=United States,OU=End Points,...	50	2022-05-24 15:11:48	None
IIS_IUSRS	172.16.1.1	DC=qa,DC=fortinet,DC=local	1	2022-05-24 14:49:47	None
Idap	172.16.1.1	DC=qa,DC=fortinet,DC=local	1	2022-05-24 14:49:47	None
Legal	172.16.1.1	OU=Los Angeles,OU=United States,OU=End Points,...	50	2022-05-24 15:11:48	None
LocalAdmins	172.16.1.1	DC=qa,DC=fortinet,DC=local	2	2022-05-24 14:49:47	None
Organization Management	172.16.1.1	DC=qa,DC=fortinet,DC=local	2	2022-05-24 14:49:47	None
Police	172.16.1.1	OU=Los Angeles,OU=United States,OU=End Points,...	50	2022-05-24 15:11:48	None
Production	172.16.1.1	DC=qa,DC=fortinet,DC=local	1	2022-05-24 14:49:47	None
Radius	172.16.1.1	DC=qa,DC=fortinet,DC=local	1	2022-05-24 14:49:47	None
Showing: 40 Total: 40					

This page displays the following columns of information:

Column	Description
Group Name	Group name.
Server	LDAP server IP address.
Distinguished Name	LDAP server distinguished name.
Users	Number of users that belong to the group.
Last Synced	Time that EMS and the LDAP server last synchronized configurations.
Invitation Status	Whether an invitation was created for this user group.

You can click *Add* on this page to add a domain to EMS. See [Adding endpoints using an AD domain server on page 89](#).

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 Action									
Refresh	Clear Filters								
User	Invitation	Domain	SAML	Device Count	Email/Phone	Last Seen	User Type	Status	
bwoiowitz@em... SAML_Okta			SAML_None_Okta	verified: 0 total: 1		2022-05-11 16:52:55	SAML	Managed	
Device Name Platform Group FortiClient ID Last Seen Device Status									
1014-MacBookPro	Mac OS X 10.15.7	Other Endpoints	246			2022-05-11 16:52:55		Managed, Not Verified	
c	Installer_LDAP, Install...	fortitest.burnaby	SAML_Single_AD	verified: 0 total: 1	c@fortitest.com 123456789	2022-05-15 12:34:52	LDAP	Managed	
l	bulk_local_mobile, de...			verified: 0 total: 1		2022-05-14 12:53:30	Local	Managed	
l	bulk_local_mobile, de...			verified: 0 total: 1		2022-05-12 12:49:55	Local	Managed	
n	Installer_LDAP, Install...	fortitest.burnaby	SAML_Single_AD	verified: 0 total: 2	m@fortitest.com 987654321	2022-05-13 12:51:40	LDAP	Managed	
p	Installer_LDAP, Install...	fortitest.burnaby	SAML_Single_AD	verified: 0 total: 1	p@fortitest.com 999888777	2022-05-15 12:34:26	LDAP	Managed	
r	Installer_LDAP, Install...	fortitest.burnaby	SAML_Single_AD	verified: 0 total: 2	r@fortitest.com 555555555	2022-05-17 11:09:29	LDAP	Managed	

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 288](#).
 - 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 they 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 263 .
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 264 .

- 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 AD credentials.

To add the LDAP server to EMS:

1. Go to *User Management > Authorized User Groups*.
2. Click *Add*.
3. In the *IP address/Hostname* field, enter the server IP address.
4. For *Bind type*, select *Regular*.
5. In the *Username* and *Password* fields, provide the credentials required to access the LDAP server.
6. Enable *LDAPS connection* and upload a certificate authority certificate or server certificate file in PEM or DER format.
7. If needed, configure other fields.
8. Click *Test*.
9. 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 email address of the desired user.
 - 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@redacted.com"/>  </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

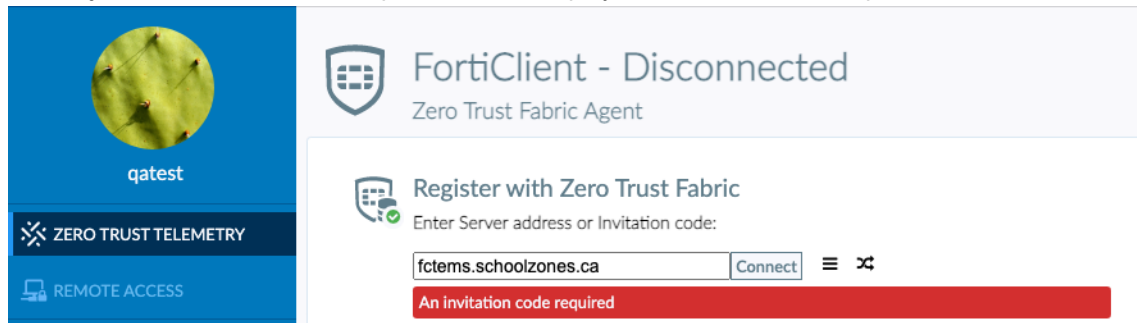
- h. Go to *Zero Trust Tags > Zero Trust Tagging Rules*. Add a Zero Trust tagging rule to tag registered endpoints with verified users.

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"/>

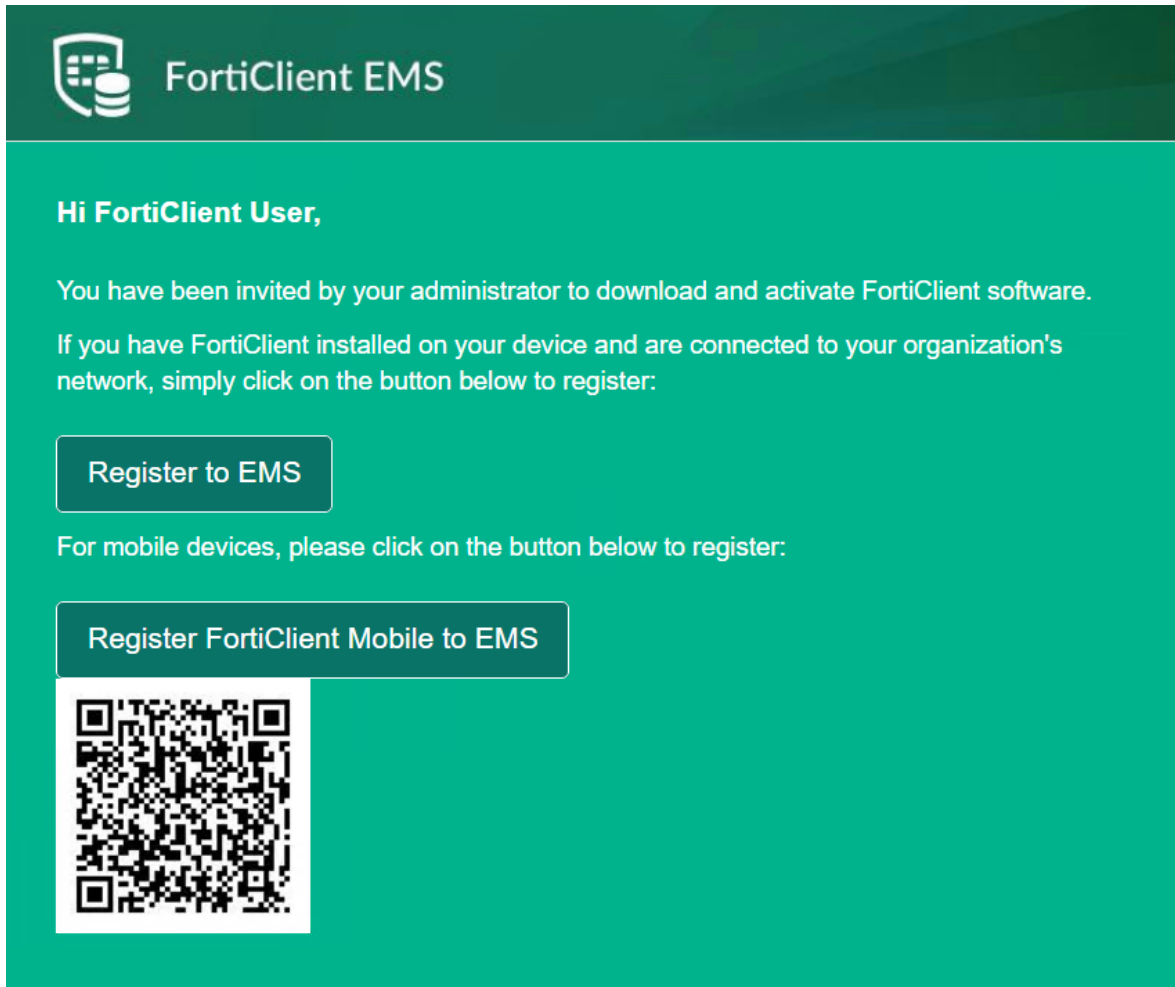
Rules		 Edit Logic	 Add Rule
Type	Value		
 Windows (1)			
User Identity	 Verified User		
 Mac (1)			
User Identity	 Verified User		
 Linux (1)			
User Identity	 Verified User		

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.



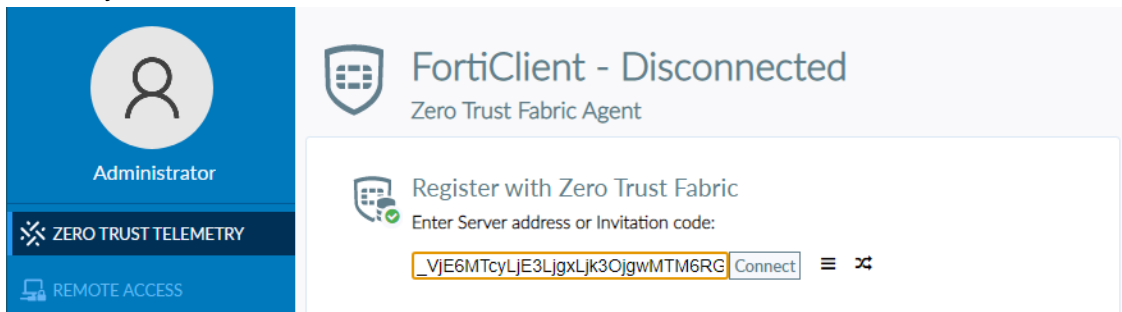
Register to EMS Manually

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

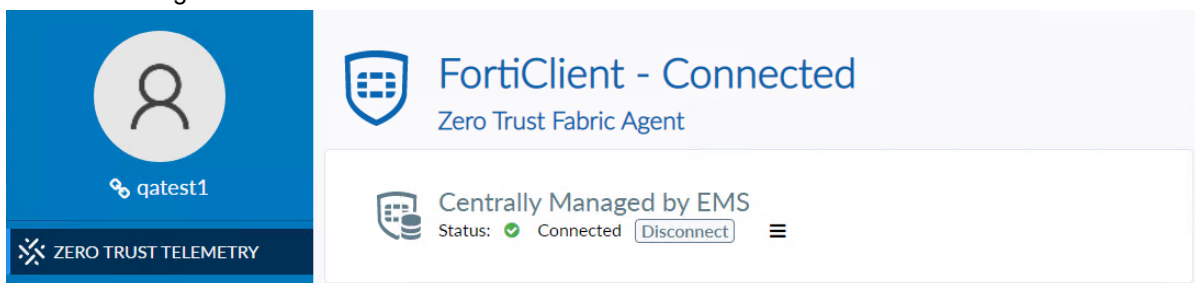
`_VjE6ZmN0ZW1zLnNjaG9vbHpvbmVzLmNhOjgwMTM6RGVmYXVsdDpENzY5NTY4Ny00RjkwLTlTRCMUitQjVlYXQ1FNUQxOTYyNTczNUU=`

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

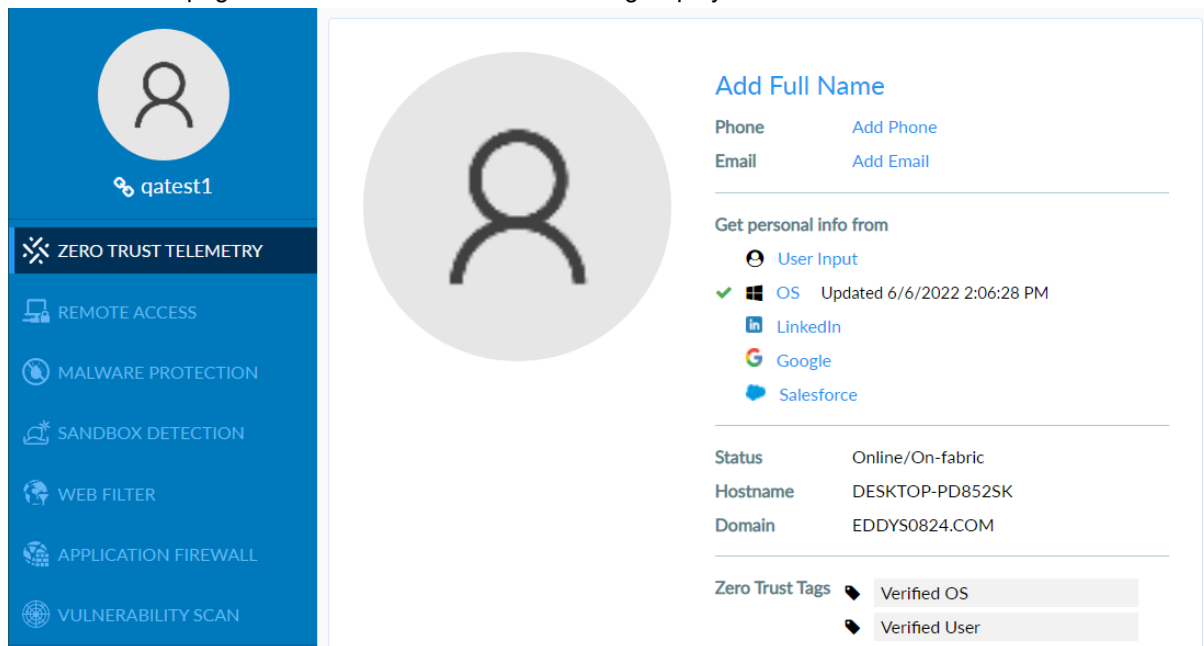
Telemetry tab, and click **Connect**.



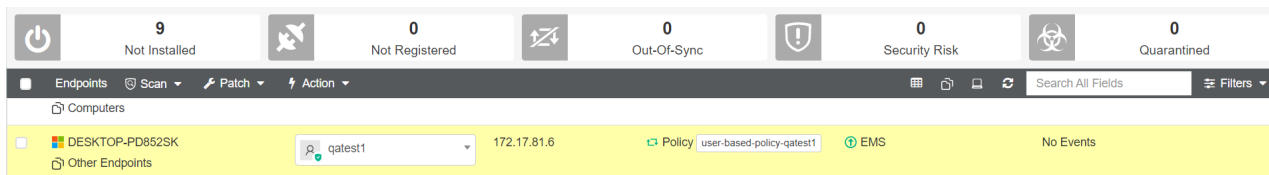
- b. In the popup, provide your LDAP user credentials, then click **Login**. FortiClient proceeds with the registration process after authentication succeeds. After FortiClient successfully registers to EMS, the username in FortiClient changes to the verified user account, and a chain icon appears beside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



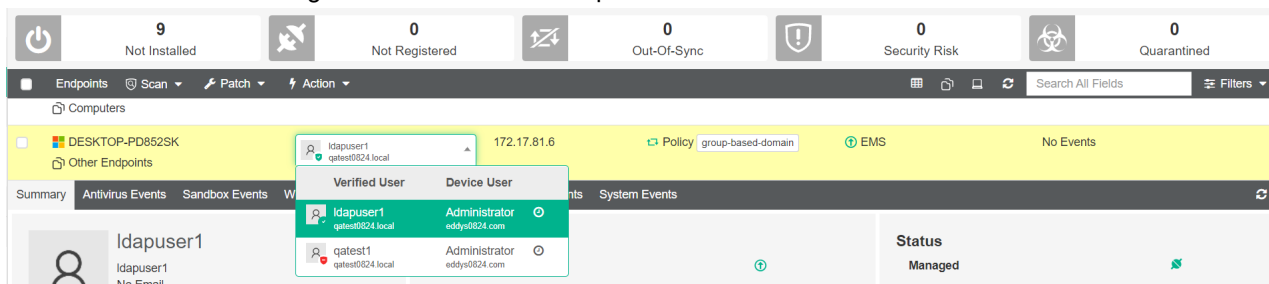
4. Go to the About page to confirm that the Verified User tag displays.



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.



- 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.



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 296](#).

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 283.</p>
Use FQDN	<p>Specify an FQDN for the FortiClient EMS server.</p> <p>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 fully qualified domain name (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 would require 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 not connected to 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> .
SSL certificate	Displays the currently imported SSL certificate. If you have already uploaded an SSL certificate, a <i>Replace</i> button displays. See Adding an SSL certificate to FortiClient EMS on page 281 .
Use SSL certificate for Endpoint Control	Enable to use the certificate uploaded in the <i>SSL certificate</i> field on port 8013. 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 14 .

Click the *Revoke and Update* button to revoke and update the certificate. You may want to revoke a certificate if it is compromised and can no longer be trusted. When a certificate is revoked, EMS prompts FortiOS and FortiClient with a new certificate signing request. This may affect existing connections.

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.
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 265 .
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).
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. See Adding an SSL certificate to FortiClient EMS for Chromebook endpoints on page 282 .
Password	Configure a new SSL password.
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.

- Configure the following options under *Endpoints Settings*:

FortiClient telemetry connection key	<p>Add the FortiClient Telemetry connection key for FortiClient EMS. FortiClient must provide this key during connection.</p> <p>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 283.</p>
--------------------------------------	---

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**.

Adding an SSL certificate to FortiClient EMS

You can add an SSL certificate to FortiClient EMS in one of the following ways:

Method	Description
Automated	The public Let's Encrypt certificate authority uses the Automated Certificate Management Environment (ACME), as RFC 8555 defines, 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.
Upload	Manually upload an SSL certificate.

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. In the *SSL certificate* field, click the *Import SSL certificate* button.
4. Select *Automated*.
5. In the *Domain* field, enter the EMS FQDN. For the Let's Encrypt server to issue the certificate, the public DNS server must resolve the EMS FQDN to the EMS public IP address.
6. In the *Email* field, enter a valid email address.
7. If desired, enable *Auto Renew*. When *Auto Renew* is enabled, FortiClient EMS automatically renews the certificate before expiry.
8. Select the checkbox to agree to Let's Encrypt's terms of service.
9. Click *Import*.

To manually upload an SSL certificate in FortiClient EMS:

1. Go to *System Settings > EMS Settings*.
2. In the *SSL certificate* field, click the *Import SSL certificate* button.
3. Select *Upload*.
4. In the *Certificate* field, browse to and select the desired certificate.
5. In the *Certificate Password* field, configure the desired password for the certificate.
6. Click *Upload*.

Adding an SSL certificate to FortiClient EMS for Chromebook endpoints

You must add an SSL certificate to FortiClient EMS to allow Chromebooks to connect to FortiClient EMS.

If you are using a public SSL certificate, add the certificate to FortiClient EMS. You do not need to add the certificate to the Google Admin console.

If you are not using a public SSL certificate, you must add the SSL certificate to FortiClient EMS, and the root certificate to the Google Admin console. See [Adding root certificates on page 55](#).

To add an SSL certificate to EMS for Chromebook endpoints:

1. In FortiClient EMS, go to *System Settings > EMS Settings > EMS for Chromebooks Settings*.
2. Do one of the following:
 - a. To replace an existing SSL certificate, beside *SSL certificate*, click *Update SSL certificate*.
 - b. If no SSL certificate has been added yet, click the *Upload new SSL certificate* button.
3. Click *Browse* and locate the certificate file (<name>.pfx).
4. In the *Password* field, enter the password.
5. Click *Test*.
6. Click *Save*.



If the SSL certificate expires in less than three months, the expiry date label is yellow. If it is expired, the label is red. Otherwise, it is green.

SSL Certificate	server2.pfx 5/12/2019
New SSL Certificate File	<input type="button" value="Browse..."/> <input type="text"/>
New SSL Password	<input type="text" value="Required"/>

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](#).

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. The communication between EMS and FortiAnalyzer is unencrypted. • <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

System log messages include information regarding date, time, hostname, device IP and MAC addresses, event time, operating system, message (online/offline/IP address change, and so on), policy name, and EMS name and serial number.

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 that FortiClient status updates report. EMS can also send an email when this happens. See [Configuring Endpoint Alerts on page 288](#).

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 labeled 'Search FortiGuard'. Below the navigation bar, on the left, a large blue circle contains the text '1.8M' and 'Number of new and updated anti-virus definitions every week'. To the right of this is a world map with several blue dots indicating FortiGuard hubs. Below the map, text states: 'FortiGuard hubs are globally situated to provide fast real time updates and signature data for any network.' In the center, there's a 'Search' section with a magnifying glass icon and three radio buttons: 'CVE Lookup' (selected), 'Threat ID Lookup', and 'Encyclopedia'. Below the search bar, it says 'Found a suspicious file? Try the Online Scanner.' On the left side of the main content area, there's a section for 'Version 84.00441' (highlighted with a red box) and 'Updated: 34 minutes ago'. Below this is a list of versions and their update times: 84.00441 (34 minutes ago), 84.00440 (1 hour ago), 84.00439 (2 hours ago), 84.00438 (3 hours ago), and 84.00437 (4 hours ago). To the right of this 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; and December 18, 2020. On the far right, there are two circular icons with text: one showing a shield with a virus icon and text 'Protects against latest malware variants with proactive technologies to block new threats', and another showing a clock icon and text 'Keeps your protection up-to-date with hourly updates'.

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

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**.

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:

- Go to *System Settings > EMS Alerts*.
- 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 288](#).

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.

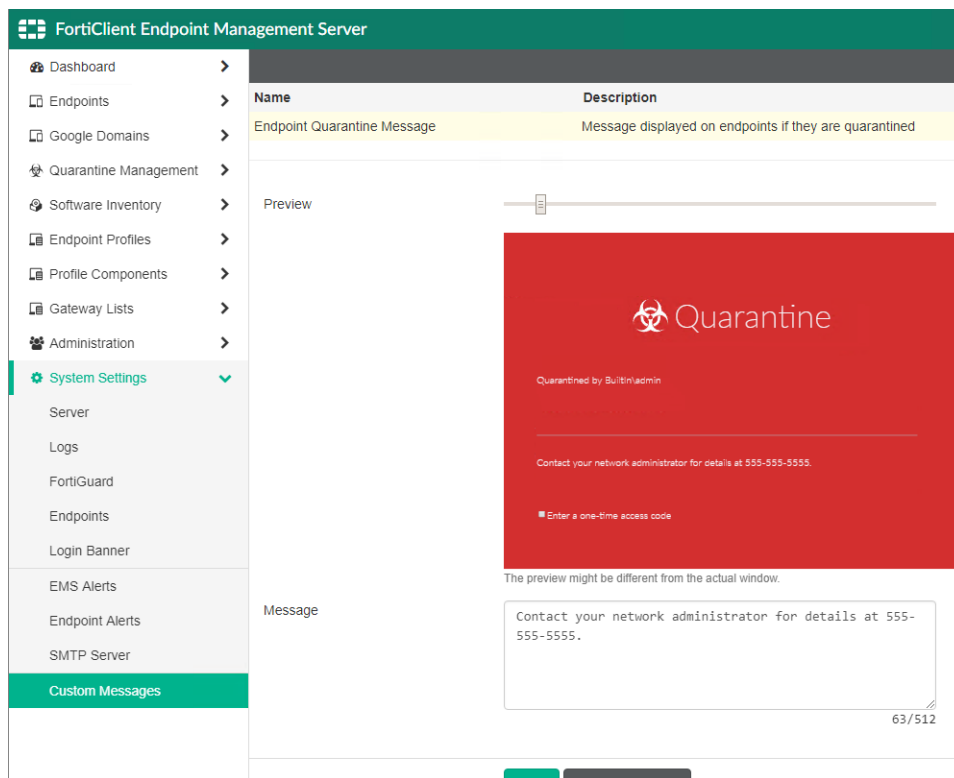
Customizing the endpoint quarantine message

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 will appear in a web browser when using the latest version of FortiClient. There are different Web Filter message types:
 - 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 unavailable for configuration.
 - The option to enable Web Filter logs on the System Settings tab is unavailable.
- If you enable Web Filter in a deployment package, the deployment package installs Web Filter on the endpoint. However, the Web Filter feature is disabled on the endpoint and does not appear in the FortiClient GUI.
- The Web Filter Detection widget is unavailable on the Status dashboard.
- Importing a profile from FortiGate/FortiManager is unavailable.

Only an EMS superadministrator can enable and disable features in Feature Select. Other EMS users can view which features are enabled and disabled 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. Note that 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 ⓘ

<input checked="" type="checkbox"/> Malware Protection ⓘ
<input checked="" type="checkbox"/> Antivirus ⓘ
<input checked="" type="checkbox"/> Anti-Ransomware ⓘ
<input checked="" type="checkbox"/> Anti-Exploit ⓘ
<input checked="" type="checkbox"/> Cloud Based Malware Detection ⓘ
<input checked="" type="checkbox"/> Removable Media Access ⓘ
<input checked="" type="checkbox"/> Sandbox Detection ⓘ
<input type="checkbox"/> Web Filter ⓘ
<input checked="" type="checkbox"/> Application Firewall ⓘ
<input checked="" type="checkbox"/> VPN ⓘ
<input checked="" type="checkbox"/> Vulnerability Scan ⓘ
<input checked="" type="checkbox"/> Zero Trust Network Access ⓘ
<input checked="" type="checkbox"/> FortiClient Single Sign-On Mobility Agent ⓘ
<input type="checkbox"/> Chromebook Features ⓘ

Save Cancel

3. Click **Save**. The *Web Filter* tab is unavailable for configuration in an endpoint profile. The *Import from FortiGate/FortiManager* option under *Endpoint Profiles* in the left pane is also unavailable.

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 unavailable 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.

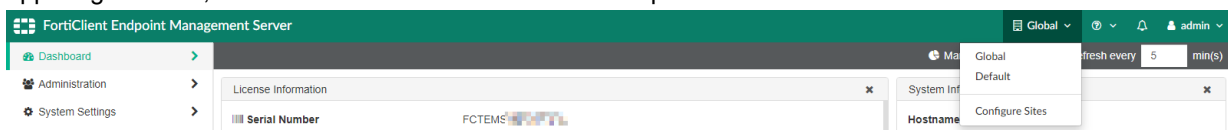
When multitenancy is enabled, Fabric connectors must use an FQDN to connect to EMS, where the FQDN hostname matches a site name in EMS (including "Default"). The following are examples of FQDNs to provide when configuring the connector to connect to the default site and to a site named SiteA, respectively: `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 301](#).
- 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 301](#).

- 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.
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.

Option	Description
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.
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	

Option	Description
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	
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.

Option	Description
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:

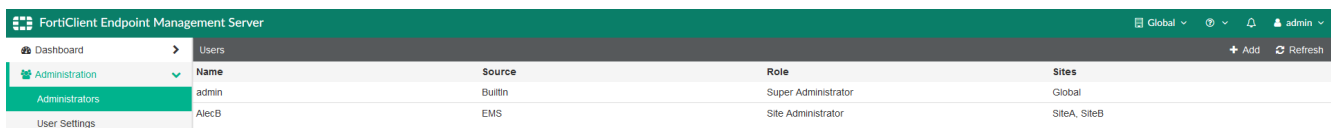
1. From the global site, go to *Administration > Administrators*.
2. Click *Add*.
3. Configure the administrator as [Configuring user accounts on page 246](#) describes. When adding a new administrator from the global site, you can create a local administrator or configure a Windows or LDAP user. When 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.

Administrator role	Description
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 248 .

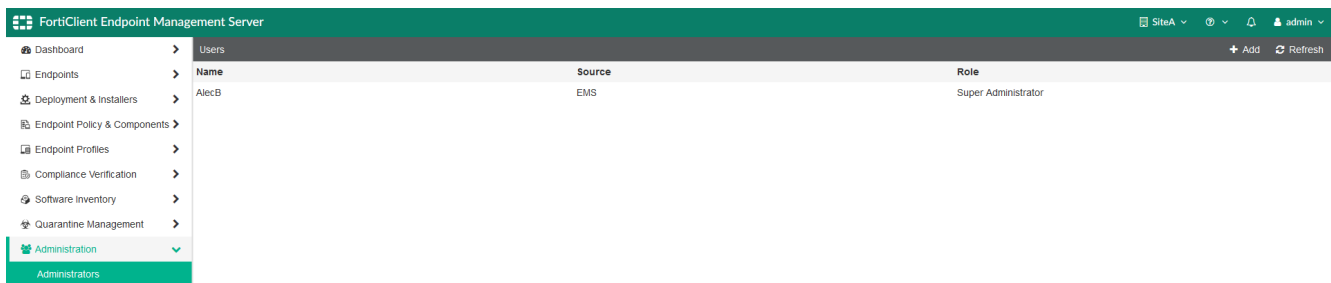
4. Click *Finish*. The new administrator appears on the *Administrators* page.

The following example shows a site administrator, AlecB. The *Global Administration > Administrators* page shows that AlecB has access to two sites, SiteA and SiteB.



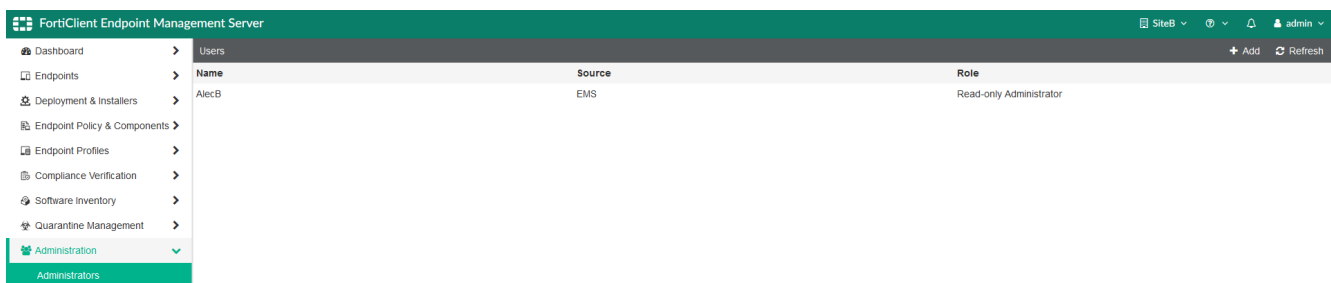
Name	Source	Role	Sites
admin	Builtin	Super Administrator	Global
AlecB	EMS	Site Administrator	SiteA, SiteB

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 248](#).



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 248](#).



Name	Source	Role
AlecB	EMS	Read-only Administrator

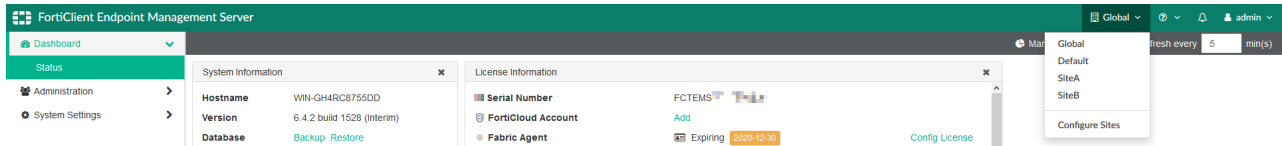


If you had configured a SAML SSO administrator prior to enabling multitenancy, enabling multitenancy causes this administrator to become a global superadministrator. You can configure a different role for this administrator. You can only have one SAML SSO administrator for the entire EMS server.

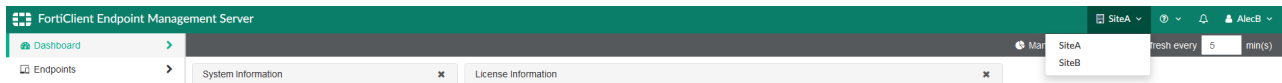
Logging into EMS with multitenancy enabled

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.



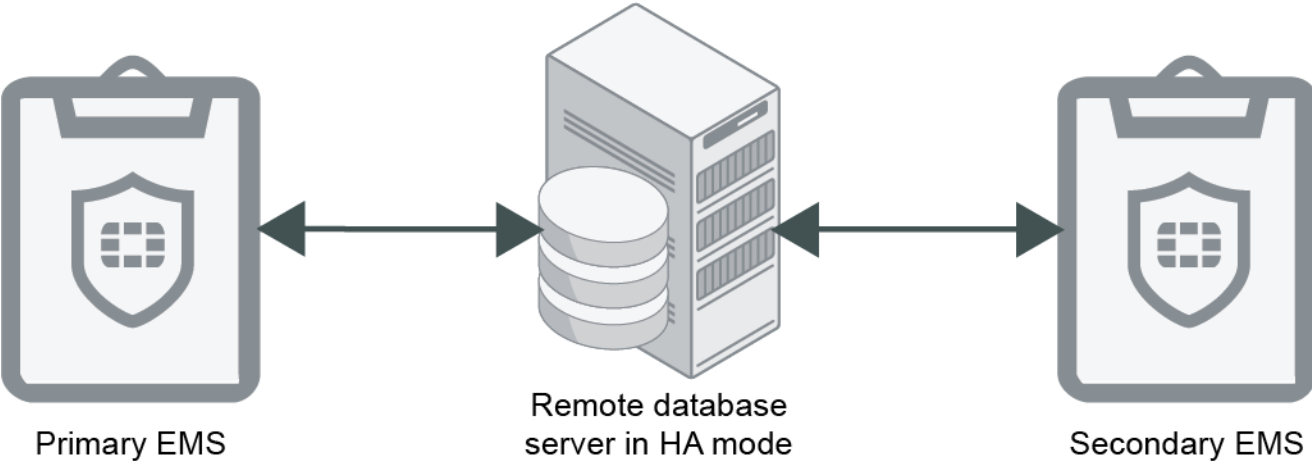
Redundancy

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:

- For file synchronization between HA nodes, you must enable FILESTREAM on the SQL Server Database Engine instance. See [Enable and configure FILESTREAM](#).
- 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 310 and Fabric connection setup using FortiGate as a load balancer on page 312 .

- 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.

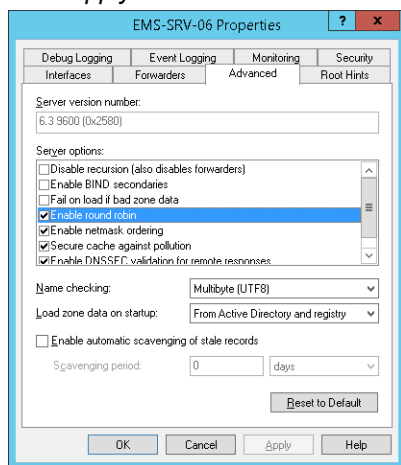


This configuration uses DNS round robin, which may cause endpoints and/or Fabric Connector connections to send data to the failover node, which by design has all but the monitor FCEMS services off. This causes FortiClient data to not reach the EMS database.

To configure DNS round robin on the database 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*.



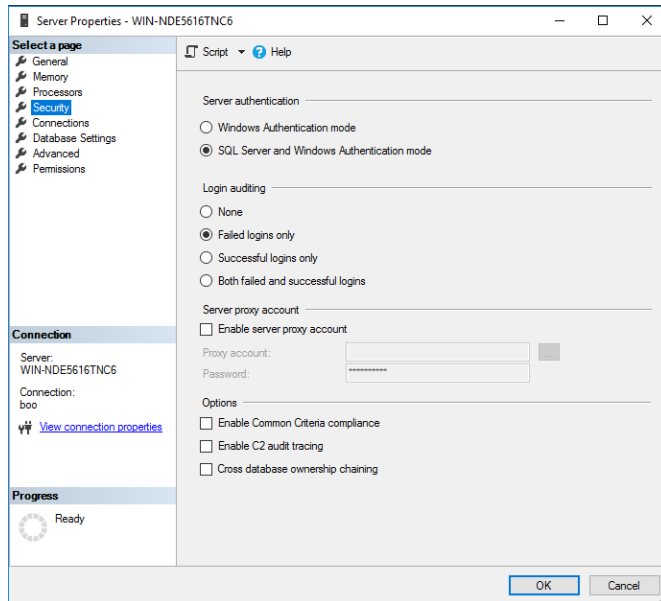
To configure SQL Server options on the remote database server:

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 (SSMS) 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 SSMS 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.

1. On the primary node, install EMS by opening Command Prompt as an administrator and running the following command:

```
FortiClientEndpointManagementServer_7.0.7.0398_x64.exe SQLServer=WIN-NDE5616TNC6
SQLUser=cbreaux SQLUserPassword=MyPassword SQLPort=1445 InstallSQL=0 ScriptDB=1
BackupDir=\\EMSServer38\backup\ DBInitialSize=31MB DBInitialLogSize=4MB
DBGrowth=11MB DBLogGrowth=11% DBLoginTimeout=31 DBQueryTimeout=61
```

This command enters the remote database server name in the *SQLServer* field. This field also supports entering FQDNs.

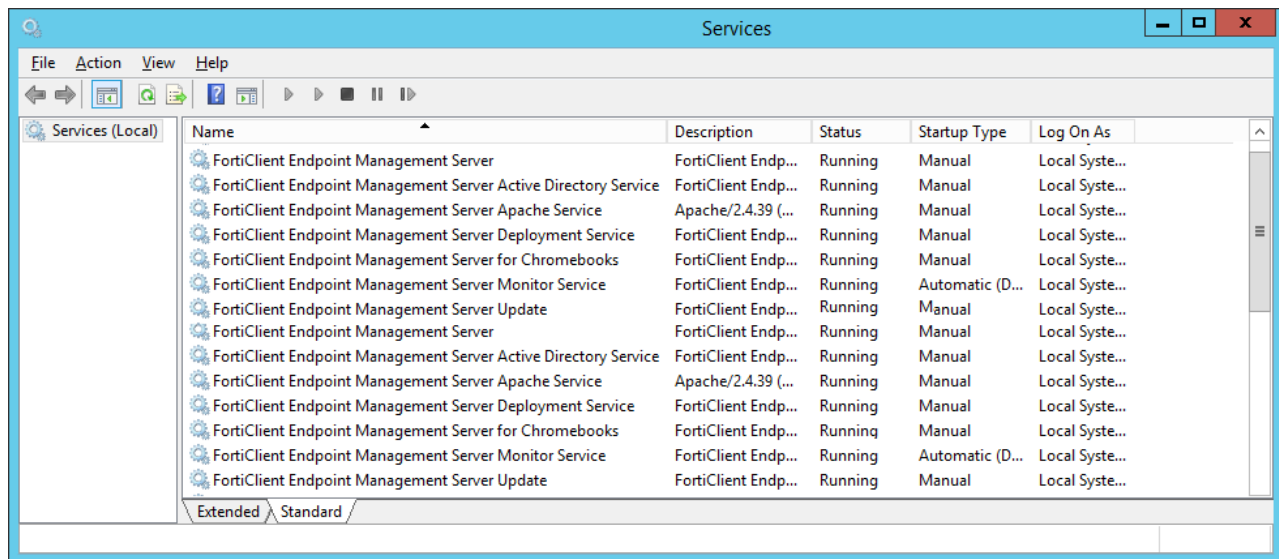
ScriptDB=1 indicates that this is the primary node.

BackUpDir=UNC_PATH\\backup indicates the shared backup directory on the local EMS server or any other accessible servers. The following lists requirements for the backup directory:

- The backup directory must not be on the remote database server.
- The backup directory must not be local to the SQL server, as SQL Server applies access control lists to the encryption key file and prevents Apache running on the other server to delete the key file.
- The SQL server should require at least write permissions to the backup directory. The EMS servers should have read/write permissions for the backup directory.
- The backup directory must be share accessible and writable by the SQL Server process user.

Ensure that you specify `SQLPort` to match the database that you want to use for your EMS server.

After installation completes, all EMS services should be running. In HA, the FortiClient Endpoint Management Server Monitor Service can be considered as the heartbeat.

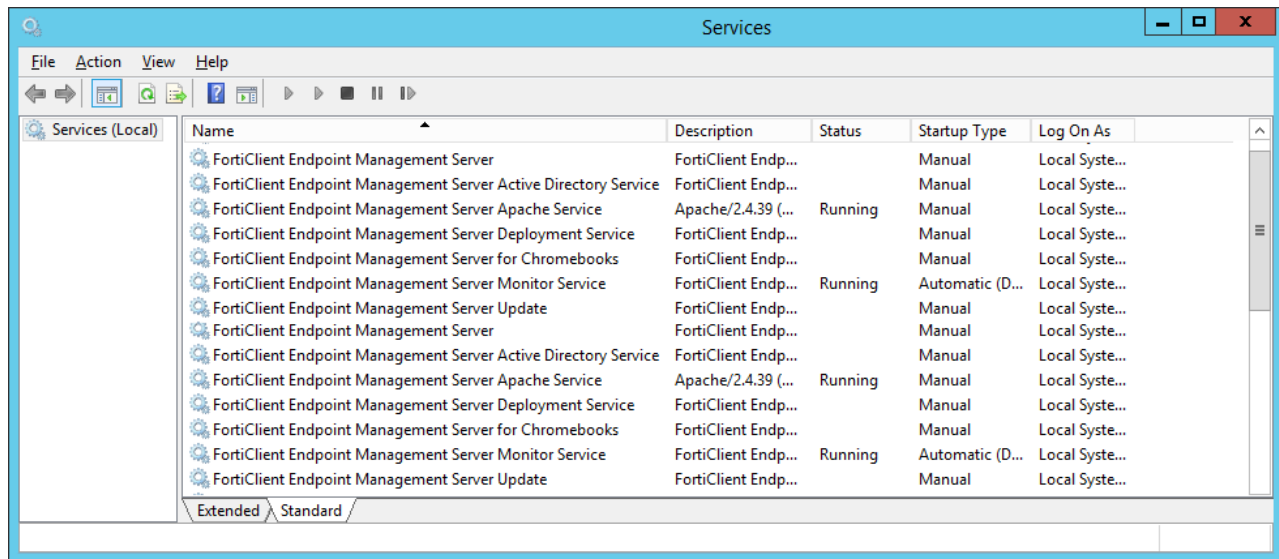


2. Install EMS on the secondary node by running the following command:

```
FortiClientEndpointManagementServer_7.0.7.0398_x64.exe SQLServer=WIN-NDE5616TNC6
  SQLUser=cbreaux SQLUserPassword=MyPassword SQLPort=1445 InstallSQL=0 ScriptDB=0
  BackupDir=\\EMSServer38\\backup\\ DBInitialSize=31MB DBInitialLogSize=4MB
  DBGrowth=11MB DBLogGrowth=11% DBLoginTimeout=31 DBQueryTimeout=61
```

`ScriptDB=0` indicates that this is the secondary node.

After installation completes, only the FortiClient Endpoint Management Server Monitor Service and FortiClient Endpoint Management Server Apache Service should be running on the secondary node.



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	FCTEMS00000992
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 File Upload
FortinetOne Account	@fortinet.com

[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.

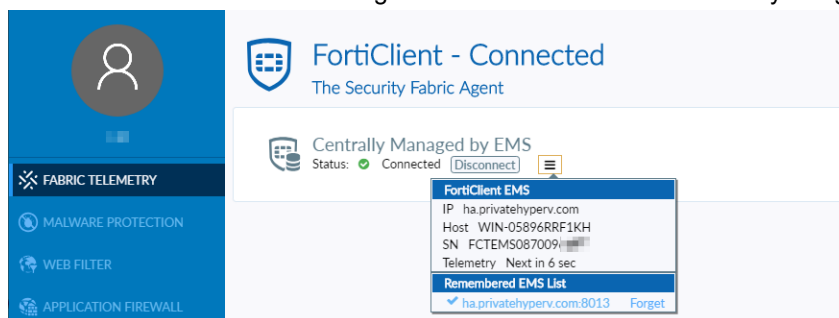


As this HA deployment uses DNS round robin, when you attempt to log in to EMS, you may be directed to the passive EMS. If this occurs, the browser displays *ERR_CONNECTION_CLOSED*. The login succeeds if DNS resolves the FQDN to the active EMS.

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.

- 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 current 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:

- Log in to the Azure portal.
- Select the desired resource group.
- 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.
- You must add traffic manager profile endpoints. In this example, the endpoints are EMS nodes. On the *Endpoints* tab, select *Add*.
- 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 with the following details:

- Resource group (browse): [TCTDM_Release](#)
- Status: Enabled
- Subscription (browse): [Software Development/Engineering](#)
- Subscription ID: 3f4a7f4e-5eda-408f-8b5b-cbfefb836628
- Tags (edit): Name: Harkamal Singh, Username: sharkamal, ExpectedUseThrough: 2022-12, VMState: ShutdownAtNight, CostCenter: 4310
- DNS name: http://emsharelease.trafficmanager.net
- Monitor status: Degraded
- Routing method: Performance

Below the essentials, there is a table titled 'Search endpoints' with the following data:

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 (highlighted), Real user measurements, Traffic view, Endpoints, Properties, Locks, Monitoring (Alerts, Metrics, Diagnostic settings, Logs). The main content area shows configuration options for the 'Routing method' (Performance), 'DNS time to live (TTL)' (20 seconds), 'Endpoint monitor settings' (Protocol: TCP, Port: 8013, Path: empty), 'Fast endpoint failover settings' (Probing interval: 10, Tolerated number of failures: 2, Probe timeout: 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.

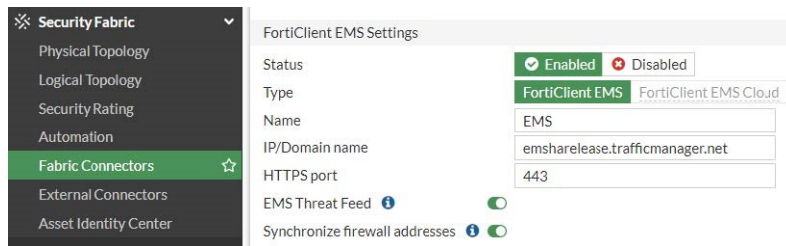
The screenshot shows the 'emsharelease' Traffic Manager profile page. The 'Endpoints' section displays a table with the following data:

Name	Status	Monitor status	Type	Location
emsnode1	Enabled	Degraded	Azure endpoint	West US 2
emsnode2	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. Under **FortiClient EMS Settings**, in the **IP/Domain name** field, enter the traffic manager 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 fully qualified domain name (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 FQDN has a new IP address and switch

to it after EMS failover.

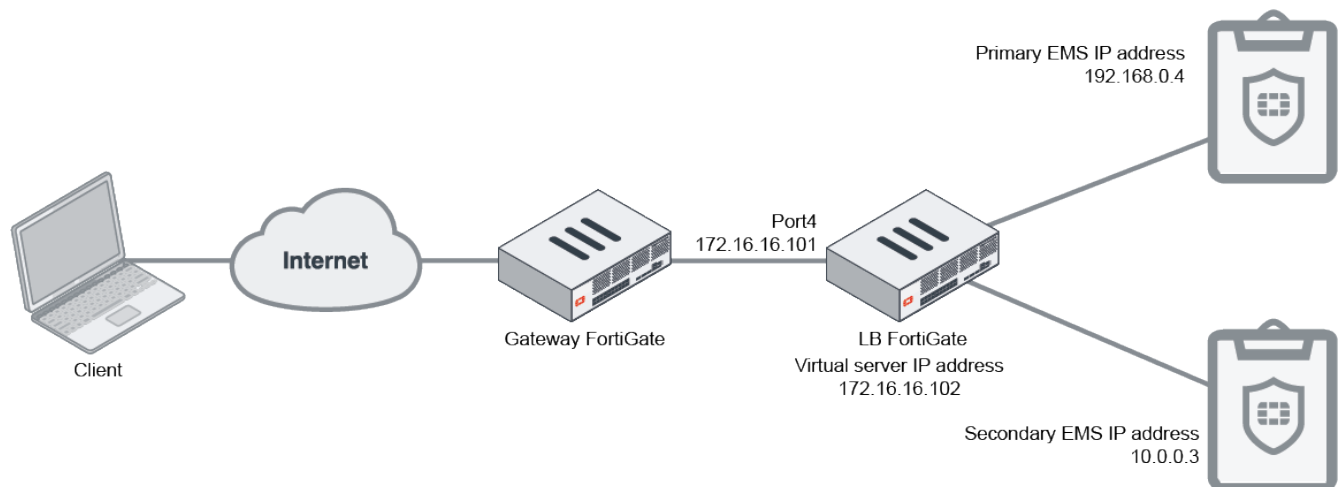


Fabric connection setup using FortiGate as a load balancer

The current 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 failure.
- 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 7.0.6 nodes configured in an HA environment
- FortiGate running FortiOS 7.0.6, acting as the LB
- FortiGate running FortiOS 7.0.6, acting as the gateway
- Endpoint running FortiClient 7.0.6

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. 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.

FortiClient EMS Settings

Status	<input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Disabled
Type	<input checked="" type="radio"/> FortiClient EMS <input type="radio"/> FortiClient EMS Cloud
Name	EMS
IP/Domain name	emsha.lab.local
HTTPS port	443
EMS Threat Feed	<input checked="" type="checkbox"/>
Synchronize firewall addresses	<input checked="" type="checkbox"/>

Similarly, the end user uses the FQDN to connect FortiClient to EMS.

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

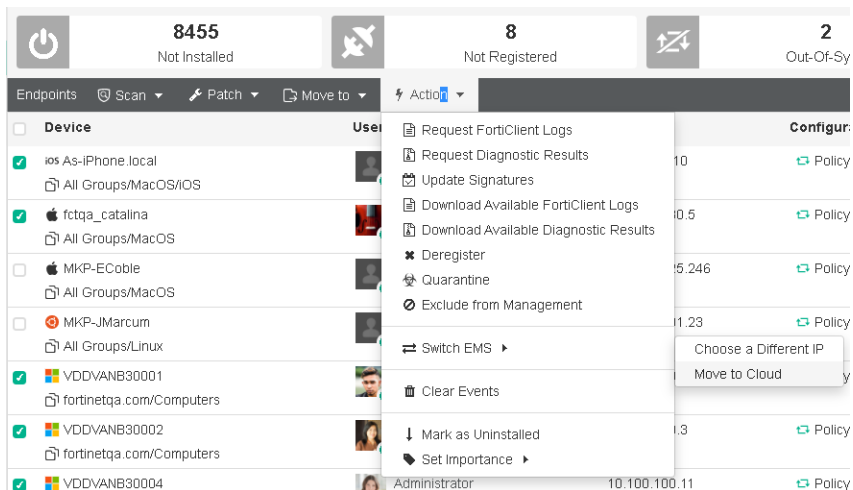
You can simply and efficiently move configurations, data, and endpoint connections between EMS instances without disrupting FortiClient endpoint functionality. This document describes migrating one EMS on-premise environment to another. This migration requires the following:

- 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>								<div><div>Search All Fields</div><div>Filters</div></div>	
<input type="checkbox"/>	<div>ios As-iPhone local</div> <div>Other Endpoints</div>	<div> A.R</div> <div>192.168.4.10</div>	<div> Policy</div> <div>Default</div>	<div> EMS</div> <div>Migrating</div>	<div>No Events</div>				
<input type="checkbox"/>	<div>apple fctqa_catalina</div> <div>Other Endpoints</div>	<div> fctqa</div> <div>192.168.130.5</div>	<div> Policy</div> <div>Default</div>	<div> EMS</div> <div>Migrating</div>	<div>No Events</div>				
<input type="checkbox"/>	<div>msi VDDVNB30001</div> <div>Other Endpoints</div>	<div> Administrator</div> <div>10.100.100.7</div>	<div> Policy</div> <div>Default</div>	<div> EMS</div> <div>Migrating</div>	<div>VUL 5</div>				
<input type="checkbox"/>	<div>msi VDDVNB30010</div> <div>Other Endpoints</div>	<div> Administrator</div> <div>10.100.100.17</div>	<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
2022-08-31	Initial release.
2022-09-07	Updated Deploying different installer IDs to endpoints using the same deployment package on page 122 .
2022-09-20	Updated Configuring a profile with application-based split tunnel on page 153 .
2022-10-11	Updated ZTNA Destinations on page 173 .
2022-11-02	Added Exporting a profile on page 143 .
2022-11-03	Updated: <ul style="list-style-type: none">• Windows, macOS, and Linux licenses on page 22• Chromebook licenses on page 23• License Information widget on page 73• Viewing the Endpoints pane on page 90• Fabric connection setup using traffic manager on page 310
2022-11-04	Updated Management capacity on page 27 .
2022-11-24	Updated Management capacity on page 27 .
2023-01-10	Updated Management capacity on page 27 .
2023-02-15	Updated Redundancy on page 304 .
2024-02-12	Updated Configuring a backup VPN connection on page 160 .
2024-02-20	Updated To manage application permissions: on page 170 .



www.fortinet.com

Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.