



FortiClient EMS - Administration Guide

Version 6.4.1

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



December 10, 2020

FortiClient EMS 6.4.1 Administration Guide

04-640-614181-20201210

TABLE OF CONTENTS

Introduction	8
FortiClient EMS components	8
Documentation	10
Getting started	11
Getting started with managing Windows, macOS, and Linux endpoints	11
Deploying FortiClient software to endpoints	11
Pushing configuration information to FortiClient	12
Relationship between FortiClient EMS, FortiGate, and FortiClient	13
Getting started with managing Chromebooks	16
Configuring FortiClient EMS for Chromebooks	16
Configuring the Google Admin console	17
Deploying a profile to Chromebooks	17
How FortiClient EMS and FortiClient work with Chromebooks	17
Installation preparation	19
System requirements	19
License types	19
FortiClient EMS	20
Component applications	21
Required services and ports	22
Management capacity	23
FortiClient Telemetry security features	24
Server readiness checklist for installation	25
Upgrading from an earlier FortiClient EMS version	25
Install preparation for managing Chromebooks	26
Google Workspace account	26
SSL certificates	26
Installation and licensing	27
Downloading the installation file	27
Installing FortiClient EMS	27
Installing FortiClient EMS using the CLI	29
Allowing remote access to FortiClient EMS and using custom port numbers	30
Customizing the SQL Server Express install directory	31
Installing FortiClient EMS to specify SQL Server Enterprise or Standard instance	31
Starting FortiClient EMS and logging in	33
Accessing FortiClient EMS remotely	33
Licensing FortiClient EMS	34
Licensing EMS by logging in to FortiCloud	34
Uploading a license file	36
License status	37
Help with licensing	37
Specifying different ports	37
Upgrading Microsoft SQL Server Express to Microsoft SQL Server Standard or Enterprise	38
Uninstalling FortiClient EMS	39

Installation and setup	40
Google Admin Console setup	40
Service account credentials	47
GUI	53
Banner	53
Left pane	54
Content pane	56
Dashboard	57
Viewing the FortiClient Status	57
System Information widget	58
License Information widget	58
FortiClient Status charts and widgets	59
Viewing the Vulnerability Scan dashboard	60
Viewing current vulnerabilities	62
Viewing the Endpoint Scan Status	64
Viewing the top 10 vulnerable endpoints with high risk vulnerabilities	66
Viewing top ten vulnerabilities on endpoints	68
Viewing Chromebook Status	70
Endpoint management	72
Windows, macOS, and Linux endpoints	72
Managing groups	72
Adding endpoints	72
Viewing endpoints	74
Managing endpoints	85
Google Domains	92
Adding a Google domain	93
Viewing domains	93
Editing a domain	96
Deleting a domain	96
Group assignment rules	96
Group assignment rule types	96
Managing group assignment rule priority levels	97
Adding a group assignment rule	98
Enabling/disabling a group assignment rule	100
Deleting a group assignment rule	100
Quarantine Management	101
Files	101
Viewing quarantined files	101
Allowlisting quarantined files	103
Configuring quarantine management	103
Allowlist	104
Viewing allowlisted files	104
Editing file descriptions	105
Deleting a file from the allowlist	105
Software Inventory	106
Applications	106

Hosts	107
Endpoint Policy	109
Adding an endpoint policy	109
Editing an endpoint policy	110
Deleting an endpoint policy	110
Enabling/disabling an endpoint policy	110
Managing endpoint policy priority levels	110
Editing endpoint policy view	112
FortiClient management based on Active Directory user/user groups	112
Chromebook Policy	115
Endpoint Profiles	116
Configuring profiles	116
Editing a default profile	116
Configuring profiles for Windows, macOS, and Linux endpoints	116
Configuring profiles for Chromebooks	121
Viewing profiles	123
Managing profiles	123
Editing a profile	123
Cloning a profile	124
Syncing profile changes	124
Editing sync schedules	124
Deleting profiles	125
Configuring identity compliance for endpoints	125
Profile references	126
Profile Name	127
Malware Protection	127
Sandbox Detection	134
Web Filter	136
Application Firewall	142
VPN	143
Vulnerability Scan	148
System Settings	150
XML Configuration	157
Deployment	158
Preparing the AD server for deployment	158
Configuring a group policy on the AD server	159
Configuring required Windows services	159
Creating deployment rules for Windows firewall	159
Configuring Windows firewall domain profile settings	159
Preparing Windows endpoints for FortiClient deployment	160
Creating a deployment configuration	161
Managing deployment configuration priority levels	161
Enabling/disabling a deployment configuration	163
Deleting a deployment configuration	163
Deploying initial installations of FortiClient (macOS)	163
Deploying FortiClient upgrades from FortiClient EMS	163

Deploying different installer IDs to endpoints using the same deployment package	164
Managing installers	165
Deployment Packages	165
Adding a FortiClient deployment package	165
Viewing deployment packages	167
Deleting a FortiClient deployment package	168
FortiClient installers	168
Adding a custom FortiClient installer	169
Viewing installers	169
Policy Components	171
CA Certificates	171
Uploading a certificate	171
Importing a certificate	171
On-fabric Detection Rules	172
Determining on-fabric/off-fabric status	174
Telemetry Server Lists	176
Creating a Telemetry server list	176
Exporting a Telemetry gateway list to XML	177
Viewing Telemetry server lists	178
Viewing assigned Telemetry server lists	178
Compliance Verification	179
Compliance Verification Rules	179
Adding a compliance verification rule set	179
Editing a compliance verification rule set	180
Deleting a compliance verification rule	180
Managing tags	180
Compliance verification rule types	181
Host Tag Monitor	184
FortiOS dynamic policies using EMS dynamic endpoint groups	185
Configuring FortiOS 6.4 dynamic policies using EMS dynamic endpoint groups	185
Configuring FortiOS 6.2 dynamic policies using EMS dynamic endpoint groups	188
Fabric Device Monitor	190
Administration	191
Administrators	191
Viewing users	191
Configuring Windows and LDAP user accounts	192
Creating new user accounts	193
Activating a disabled account	193
Admin roles	194
Adding an admin role	194
Cloning an admin role	194
Deleting admin roles	195
Admin role permissions reference	195
User Servers	198
Adding a user server	198
Editing a user server	198

Deleting a user server	199
Viewing user servers	199
Configuring User Settings	200
Fabric Devices	200
Database management	201
Backing up the database	201
Restoring the database	201
Licenses	202
Logs	202
System Settings	203
Configuring Server settings	204
Adding an SSL certificate to FortiClient EMS for Chromebook endpoints	206
Configuring Logs settings	207
Configuring Fortinet Services settings	208
Configuring Endpoints settings	209
Configuring the login banner	209
SAML SSO	210
Alerts	212
Configuring EMS Alerts	212
Configuring Endpoints Alerts	213
Configuring SMTP Server settings	213
Viewing alerts	215
Custom Messages	215
Customizing the endpoint quarantine message	215
Customizing Web Filter messages	216
Feature Select	217
Generating a QR code for centrally managing FortiClient (Android) and (iOS) endpoints	219
Creating a support package	221
Appendix A - Examples	222
Support banned word check in URL	222
Change log	225

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 versions of FortiClient software
- 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.

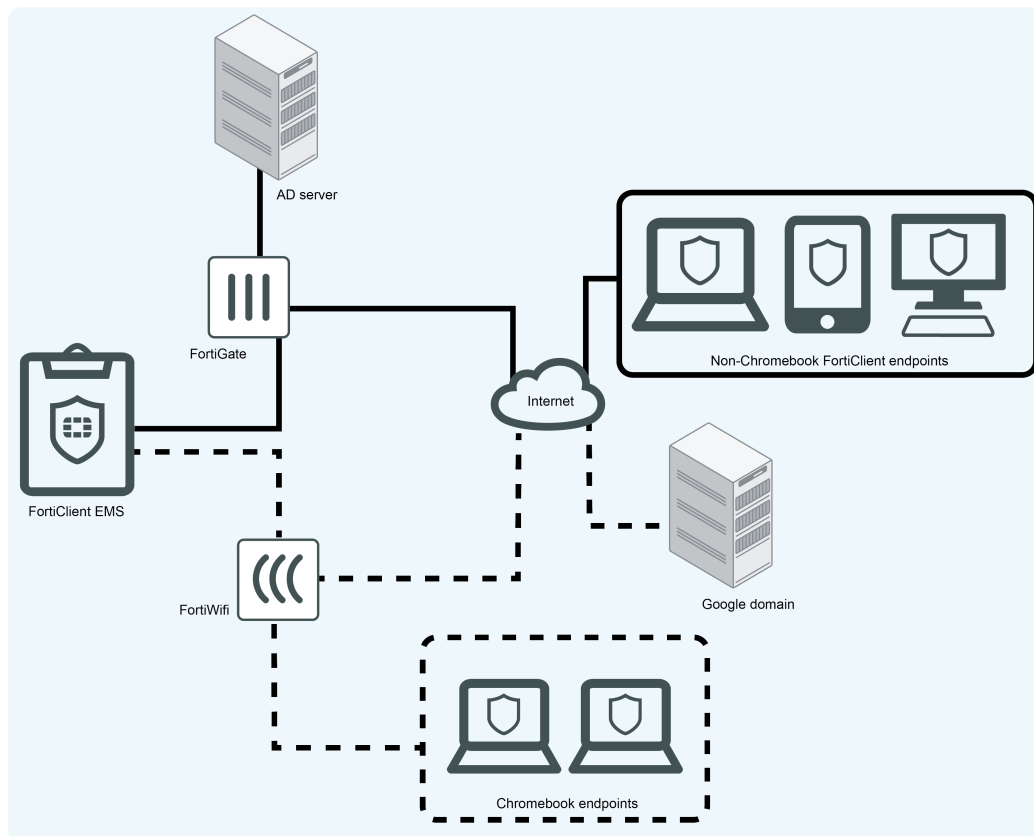
FortiClient EMS also provides the infrastructure to install and manage the FortiClient Web Filter extension on Google Chromebook endpoints. FortiClient protects endpoint users by working with FortiClient EMS to filter web content endpoint users view on Google Chromebooks.

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>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.

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.

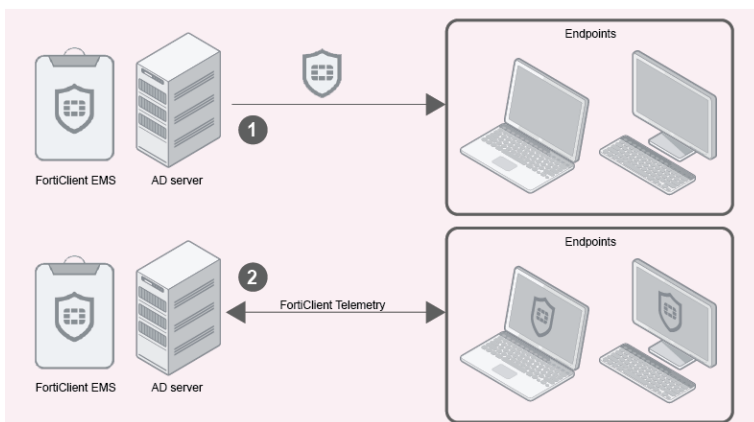
You can deploy FortiClient to endpoints using Active Directory (AD) servers and workgroups. There are differences between using AD servers and workgroups.

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.

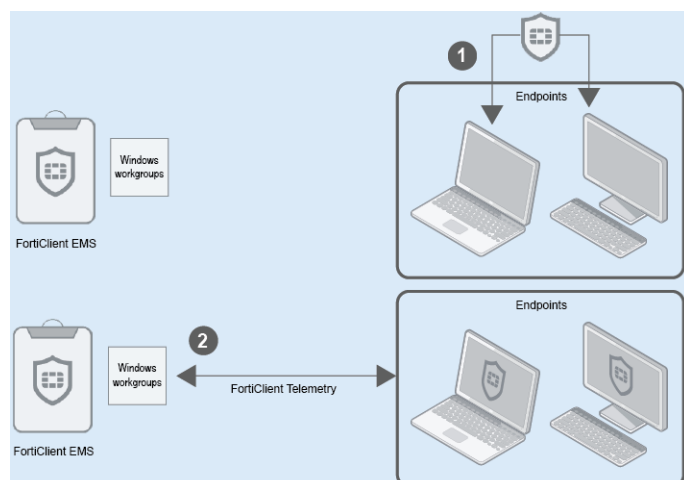
The following shows a deployment of FortiClient using FortiClient EMS with an AD server:

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 167](#).
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 72](#).
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 165](#).
3. Create a profile that includes the desired configuration information for FortiClient software on endpoints. See [Creating a profile to configure FortiClient on page 117](#).
4. Prepare domains and workgroups for deployment. See [Preparing the AD server for deployment on page 158](#).
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 161](#).
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 74](#).

Pushing configuration information to FortiClient

After the endpoints' FortiClient connects 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 profile to configure FortiClient on page 117](#).

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 109](#). 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 74](#).

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 6.4 Compliance Guide](#).

FortiClient in the Security Fabric

In this scenario, FortiClient 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 6.4 does not directly connect to FortiOS. FortiOS receives FortiClient data only from EMS.

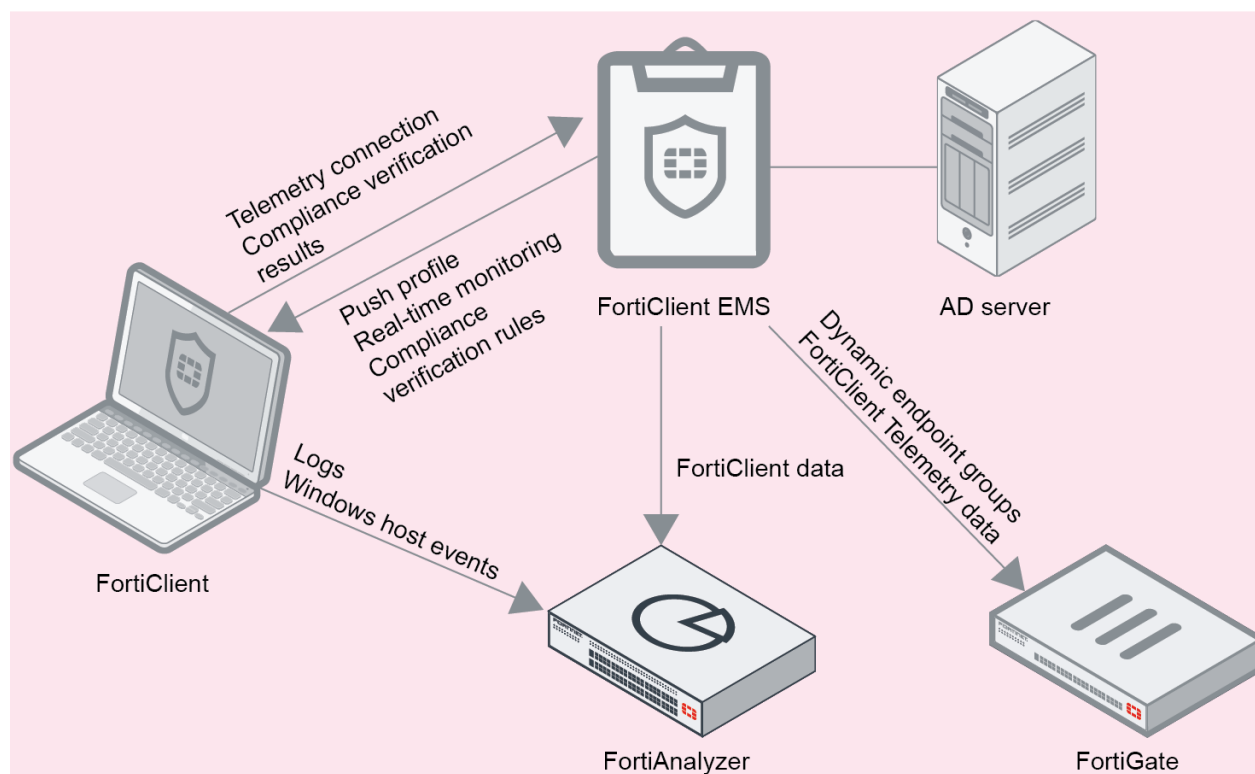


FortiGate does not provide configuration information for FortiClient and the endpoint. An administrator must configure FortiClient using an EMS endpoint policy.

Following is a summary of how the FortiClient Telemetry connection works in this scenario:

1. EMS is connected to the FortiGate as a participant in the Security Fabric.
2. FortiClient Telemetry connects to EMS.
3. EMS sends the endpoint information received via FortiClient Telemetry to FortiOS.
4. FortiClient receives a profile of configuration information from EMS as part of an endpoint policy.
5. EMS sends compliance verification rules to the endpoint.
6. FortiClient checks the endpoint using the provided compliance verification rules and sends the results to EMS.
7. EMS receives the results from FortiClient and dynamically groups the endpoints according to the results.
8. FortiOS pulls the dynamic endpoint group information from EMS. You can use this data to build dynamic firewall policies.
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 185](#).



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

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:

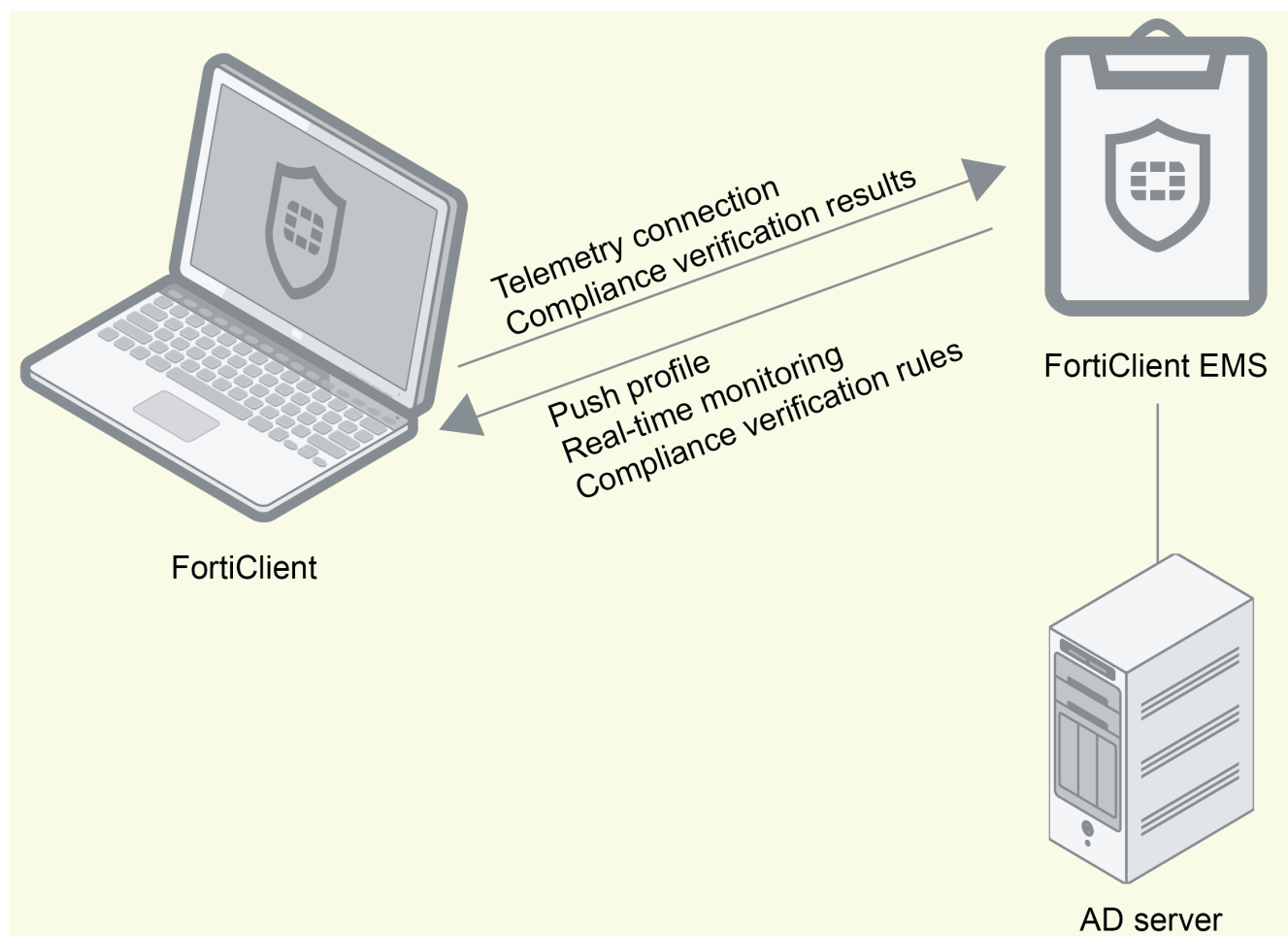
- Logs
- Windows host events

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 compliance verification 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 using the FortiOS CLI to set the following fields: `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 described in [Quarantining an endpoint on page 89](#) 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 33](#).
2. Add SSL certificates. See [Adding an SSL certificate to FortiClient EMS for Chromebook endpoints on page 206](#).
3. Configure FortiClient EMS settings. See [System Settings on page 203](#).
4. Configure user accounts and permissions. See [Administrators on page 191](#). 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 40](#).
2. Configure the FortiClient Web Filter extension. See [Configuring the FortiClient Web Filter extension on page 41](#).
3. Add root certificates. See [Adding root certificates on page 42](#).
4. Configure unique service account credentials. See [Configuring unique service account credentials on page 47](#).
5. Disallow incognito mode. See [Disallowing incognito mode on page 44](#).

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.

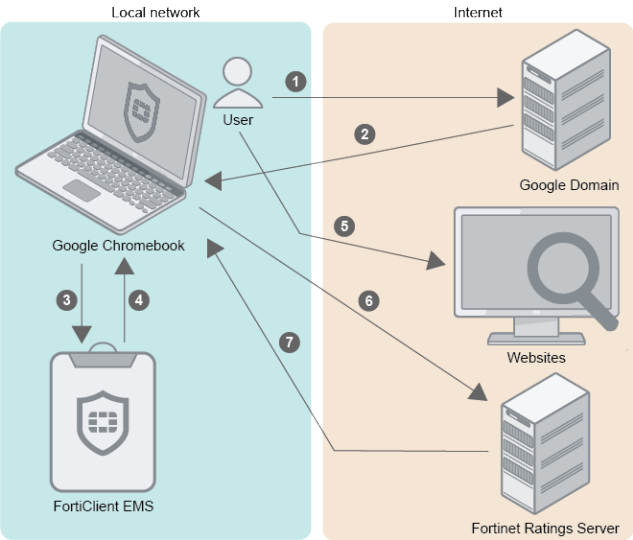
To deploy a profile to Chromebooks:

1. Add the Google domain. See [Adding a Google domain on page 93](#).
2. Define web filtering options in one or more profiles. You can enable Safe Search in profiles. See [Adding a new profile on page 122](#).
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 115](#).
4. Verify the FortiClient Web Filter extension. See [Verifying the FortiClient Web Filter extension on page 46](#).
5. View Google domains and Google users. See [Viewing domains on page 93](#).

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 2019, 2016, or 2012 R2. On Windows Server 2019, preinstalling Microsoft ODBC Driver 17 for SQL Server (x64) is necessary.
- No additional installed services
- 2.0 GHz 64-bit processor, four virtual CPUs (4 vCPU)
- 4 GB RAM (8 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.



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 Fabric Agent license and does not include Sandbox Cloud or FortiSASE support. EMS consumes one license count for each managed endpoint.

See [To apply a trial license to FortiClient EMS: on page 34](#).

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 endpoint licenses

License name	Description
Fabric Agent with Endpoint Protection and Cloud Sandbox	Full license that offers all FortiClient features including endpoint protection and Sandbox Cloud. Includes all features detailed for the Fabric Agent with Endpoint Protection and Sandbox Cloud licenses.
Fabric Agent with Endpoint Protection	Includes support for Telemetry and endpoint protection and management (AV, on-premise FortiSandbox, Web Filter, Application Firewall, Vulnerability Scan, Fortinet Single Sign-On (FSSO), and FortiGate registration). Each purchased Fabric Agent license allows management of one FortiClient Windows, macOS, or Linux endpoint. You must purchase a minimum of 25 endpoint licenses, and you can have these EMS licenses for a maximum three year term. You can specify the number of endpoints and the term duration at time of purchase. The Fabric Agent license also applies for iOS and Android endpoints. You can also use the Fabric Agent license to license Chromebooks if no Chromebook license is present on the EMS instance.
Sandbox Cloud	Adds support for FortiSandbox Cloud for Windows and macOS endpoints.
FortiSASE	Adds support for FortiSASE for Windows, macOS, and Linux endpoints running FortiClient 6.4.1 and later.

When using both Fabric Agent and Sandbox Cloud licenses, you must purchase the same number of licenses for both license types:

- If you already have purchased Fabric Agent licenses for 1000 endpoints, then decide to add the Sandbox Cloud licenses, you must also purchase 1000 Sandbox Cloud licenses.
- If you have purchased Sandbox Cloud licenses for 500 endpoints, then decide to add the Fabric Agent licenses, you must also purchase 500 Fabric Agent licenses.
- If you purchase both Fabric Agent and Sandbox Cloud licenses at the same time, you must purchase the same number of both licenses.
- If the license amounts differ, the lowest common number of licenses is available. For example, if you purchase 500 Fabric Agent licenses and 300 Sandbox Cloud licenses, EMS only has 300 licenses available.



You must purchase a license for each registered endpoint.

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 Fabric Agent 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 Fabric Agent licenses, if available. EMS only licenses Chromebooks using Fabric Agent licenses if no Chromebook license is available. See [Windows, macOS, and Linux endpoint licenses on page 20](#) for information about the Fabric Agent 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	Outgoing	N/A
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
Apache/HTTPS	Web access to FortiClient EMS	TCP	443	Incoming	Installer
FortiGuard	FortiGuard AV, vulnerability, and application version updates	TCP	80	Outgoing	N/A
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

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 (formerly G Suite) 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



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. The following are suggested host system hardware configurations for FortiClient EMS. The suggested configurations depend on the number of endpoints FortiClient EMS is managing.



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

Number of managed endpoints	Number of virtual CPUs	Memory (RAM) (in GB)	Suggested keep alive interval
Up to 10000	2	8	Default (60 seconds)
10000 to 20000	4	8	Default (60 seconds)
20000 to 30000	4	8	120 seconds
30000 to 40000	4	8	120 seconds
40000 to 50000	4	8	120 seconds
50000 to 75000	8	16	120 seconds



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



For the purpose of this table, an Intel i5 processor with two cores and two threads per core is considered to have four virtual CPUs. An Intel i3 processor with two cores and one thread per core has two virtual CPUs.



When managing more than 5000 endpoints, install SQL Server Enterprise 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 31](#).

FortiClient Telemetry security features

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

You can configure Telemetry connections between FortiClient and FortiGate or EMS to require a preshared password or connection key. See [Configuring Endpoints settings on page 209](#) and [Creating a Telemetry server list on page 176](#).

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 22](#) 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 6.4.1 supports upgrading from previous EMS versions as outlined in [FortiClient and FortiClient EMS Upgrade Paths](#).



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



When upgrading FortiClient EMS from 6.0 to 6.4.1, EMS retains the 6.0 license after the upgrade. However, due to the major licensing changes introduced in 6.2.0, you must still convert the license to a 6.4 license by manually converting the license on the [Customer Service & Support site](#) by August 31, 2020, or by contacting the Fortinet Support team. After the converted license expires, you must order and apply 6.2 licenses.

To upgrade from an earlier EMS version:

1. Close FortiClient EMS.
2. Install FortiClient EMS 6.4.1 using the downloaded installer. You may complete the upgrade using one of the following methods. You can download the installer files from [Customer Service & Support](#).
 - a. Fortinet can enable push notifications on FDS for a new EMS GA build. If Fortinet has enabled this, a notification appears on the FortiClient EMS GUI. Click the notification, then review and accept the upgrade message.
 - b. Run the full FortiClient EMS installer as an administrator.
 - c. Run the light FortiClient EMS installer as an administrator. This installer connects to the FDS to check for, download, and run the latest full FortiClient EMS installer.
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 account before you can use the Google service and manage your Chromebook users.

The Google Workspace account differs 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 206](#). 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 42](#).

Installation and licensing

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

- Reviewed [License types on page 19](#)
- Met the requirements listed in [Required services and ports on page 22](#)
- Completed the [Server readiness checklist for installation on page 25](#)
- 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.

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_6.4.1.<build>_x64.exe

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

Installing FortiClient EMS

The FortiClient EMS installation package includes:

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



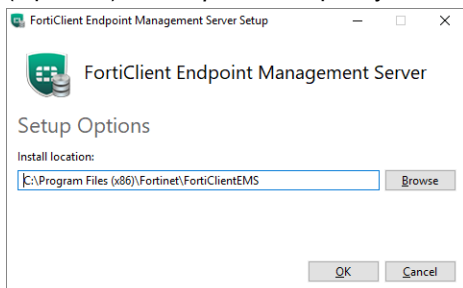
Installing FortiClient EMS requires local administrator rights. Internet access is recommended, but optional, during installation. SQL Server may require some dependencies to be downloaded over the internet. EMS also tries to download information about FortiClient signature updates from FortiGuard.

To install EMS:

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

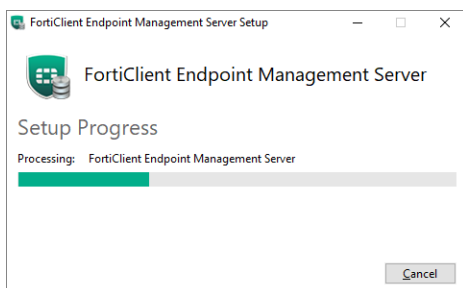


4. (Optional) Click *Options* to specify a custom directory for the FortiClient EMS installation.

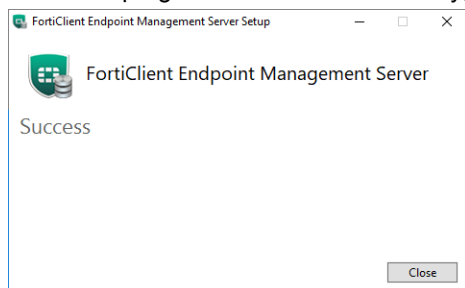


- a. Click *Browse* to locate and select the custom directory.
 - b. Click *OK* to return to the installation wizard.
5. Click *Install*.

The installation may take 30 minutes or longer. It may appear to stop at times, but this is only because certain steps in the installation process take longer than others.



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



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

Installing FortiClient EMS 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.

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

Option	Description
AllowedWebHostnames	The default value is <code>localhost, 127.0.0.1</code> . To clear this value, first enter <code>AllowedWebHostnames=*</code> , then enter the desired <code>AllowedWebHostnames</code> value. Otherwise, the value that you enter is appended to <code>[localhost, 127.0.0.1]</code> , so that <code>AllowedWebHostNames=localhost, 127.0.01, <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 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.

Option	Description
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	Enter the DSN name of the computer where SQL Server is already installed.
SQLServerInstance	Enter the SQL Server instance name.
SQLService	If using a default database instance, enter the instance name. If using a named database instance, enter <code>mssql\$<instance_name></code> . For example, if your instance is named "database000", enter <code>mssql\$database000</code> .
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.

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_6.4.1.XXXX_x64.exe ServerHostname=<preferred_host_name>
ClientDownloadPort=<HTTP_port_number> RemoteManagementPort=<HTTPS_port_number>
AllowedWebHostnames=<allowed_web_host_names> ApacheServerAdminEmail=<Apache_Server_admin_email_address>
```

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

```
FortiClientEndpointManagement_6.4.1.XXXX_x64.exe ServerHostname=emshost.ems.com
ClientDownloadPort=1080 RemoteManagementPort=22443 AllowedWebHostnames=emshost.ems.com
ApacheServerAdminEmail=example@example.com
```

Customizing the SQL Server Express install directory

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

These instructions do not apply for SQL Server Enterprise or Standard, which you must install separately from FortiClient EMS. For information on SQL Server Enterprise or Standard and FortiClient EMS, see [Installing FortiClient EMS to specify SQL Server Enterprise or Standard instance on page 31](#).

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_6.4.1.XXXX_x64 SQLCmdlineOptions="/INSTANCENAME=FCEMS
/INSTANCEDIR=<desired_directory>"
```

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

```
FortiClientEndpointManagement_6.4.1.XXXX_x64 SQLCmdlineOptions="/INSTANCENAME=FCEMS
/INSTANCEDIR=c:\sqlserver"
```

Customizing the SQL Server Express install to a remote directory

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

```
FortiClientEndpointManagement_6.4.1.XXXX_x64 InstallFolder=<desired_directory> SQLServer=<SQL_
Server_name> SQLServerInstance= SQLService=MSSQLSERVER
```

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

```
FortiClientEndpointManagement_6.4.1.XXXX_x64 InstallFolder=c:/sqlserver SQLServer=WIN-0888
SQLServerInstance= SQLService=MSSQLSERVER
```

Installing FortiClient EMS to specify SQL Server Enterprise or Standard instance

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

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_6.4.1.XXXX_x64.exe SQLUser=<username> SQLUserPassword=<password> InstallSQL=0 ScriptDB=1 SQLServerInstance= SQLService=<instance_name> SQLCmdlineOptions="/INSTANCENAME="</pre>
Local default instance using local Windows authentication	<pre>FortiClientEndpointManagement_6.4.1.XXXX_x64.exe SQLServerInstance= SQLService=<instance_name> SQLCmdlineOptions="/INSTANCENAME=" InstallSQL=0 ScriptDB=1</pre>
Local named instance using SQL authentication	<pre>FortiClientEndpointManagement_6.4.1.XXXX_x64.exe SQLUser=<username> SQLUserPassword=<password> InstallSQL=0 ScriptDB=1 SQLServerInstance=<instance_name> SQLService=mssql\$<instance_name> SQLCmdlineOptions="/INSTANCENAME=<instance_name>"</pre>
Local named instance using local Windows authentication	<pre>FortiClientEndpointManagement_6.4.1.XXXX_x64.exe SQLServerInstance=<instance_name> SQLService=mssql\$<instance_name> SQLCmdlineOptions="/INSTANCENAME=<instance_name>" InstallSQL=0 ScriptDB=1</pre>

For example, if installing FortiClient EMS and pointing to a local instance named "database000" using SQL authentication, with SQL username "janedoe", password "password123", the command is as follows:

```
FortiClientEndpointManagement_6.4.1.XXXX_x64.exe SQLUser=janedoe SQLUserPassword=password123
InstallSQL=0 ScriptDB=1 SQLServerInstance=database000 SQLService=mssql$database000
SQLCmdlineOptions="/INSTANCENAME=database000"
```

Remote existing database

To create a backup directory:

Prior to installing FortiClient EMS, create a backup directory on the database server and set the permissions as described:

1. On the database server, create a backup directory.
2. Right-click the directory and select *Properties*.
3. On the *Security* tab, ensure all users have full control of the directory.

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. On the EMS server, open Local Group Policy Editor. Add the domain user to the Log on as a service policy.

Database type	Command
Remote default or named instance using SQL authentication	<pre>FortiClientEndpointManagement_6.4.1.XXXX_x64.exe SQLServer=<SQL_ Server_name> SQLUser=<username> SQLUserPassword=<password> InstallSQL=0 ScriptDB=1 BackupDir=<backupdirectorypath></pre>

Database type	Command
Remote default or named instance using Windows authentication (domain user)	<pre>FortiClientEndpointManagement_6.4.1.XXXX_x64.exe SQLServer=<SQL_Server_name> WindowsUser=<domain name>\<username> WindowsUserPassword=<password> InstallSQL=0 ScriptDB=1 BackupDir=<backupdirectorypath></pre>

For example, if installing FortiClient EMS and pointing to a remote named instance on a computer with DNS name WIN-088 using Windows authentication, with domain name "forticlient.ca", username "janedoe", and password "password123", the command is as follows. This example also includes the optional `SQLEncryptConnection` option:

```
FortiClientEndpointManagement_6.4.1.XXXX_x64.exe SQLServer=WIN-0888
WindowsUser=forticlient.ca\janedoe WindowsUserPassword=password123 InstallSQL=0
ScriptDB=1 BackupDir=c:\backup\ SQLEncryptConnection=no
```

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. Configure FortiClient EMS by going to *System Settings*.

Accessing FortiClient EMS remotely

You can access FortiClient EMS remotely using a web browser instead of the GUI.

To enable remote access to FortiClient EMS:

1. Go to *System Settings > Server*.
2. Enable *Remote HTTPS access*.
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, or Chromebook endpoints. For information on the different license types available, see [License types on page 19](#).

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

- [Licensing EMS by logging in to FortiCloud on page 34](#): You can log in to your FortiCloud account to activate EMS using that account. Once an EMS license expires, EMS uses the FortiCloud account to obtain a new license file, if available on that account. You can use this method to apply a trial or paid license to EMS. This is the primary licensing method for EMS.
- [Uploading a license file on page 36](#): You can upload a license file to EMS. This functions in the same way as EMS versions prior to 6.2.0. You must use this backup licensing method only if you cannot license EMS by logging into FortiCare.

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



Although the option to upload a license file is available in the EMS GUI, FortiCloud does not provide EMS 6.4 license files. You cannot use this option to activate, upgrade, or renew an EMS 6.4 license.

Licensing EMS by logging in to FortiCloud

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

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.

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 > Register/Activate*.
3. In the *Registration Code* field, enter the *Contract Registration Code* from your service registration document. Configure other fields as required, then click *Next*.

FORTINET

PLEASE REMEMBER TO REGISTER YOUR CONTRACT REGISTRATION CODE

Service Entitlement Summary

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

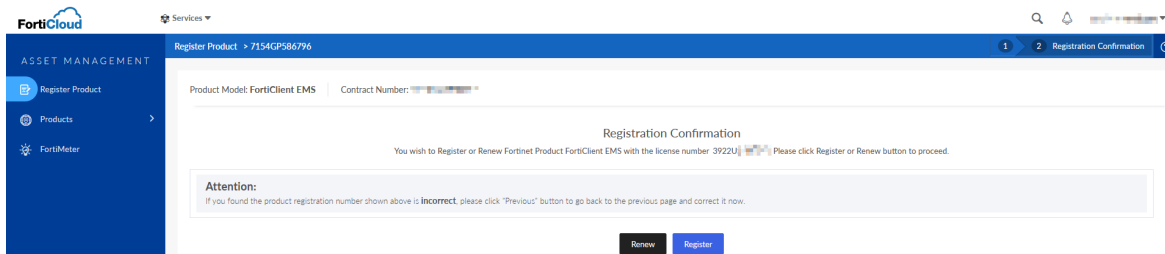
The screenshot shows the FortiCloud 'Register Product' interface. On the left is a sidebar with 'ASSET MANAGEMENT' and 'Register Product' (selected). The main content area is titled 'Register Product' and contains a 'Registration Code' field with the value '3922UW'. Below this is an 'End User Type' section with two radio buttons: 'A government user' and 'A non-government user'.

4. 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 *Administration > Configure 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 *Administration > 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 & Sync License Now*. Once your account information is authenticated, EMS updates the *Configure License* page with the serial number and license information that it retrieved from FortiCloud.
 - b. As described in [Windows, macOS, and Linux endpoint licenses on page 20](#), you can apply multiple license types to the same EMS server. For example, if you have already applied a Fabric Agent license to your EMS server, you can apply another license type, such as a Chromebook 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 *Administration > Configure License* in EMS. Click *Next*.
- iii. Complete the registration, then click *Confirm*.

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

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



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



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

Uploading a license file

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

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

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

1. Go to *Administration > Configure License*.
2. For *License Source*, select *File Upload*.

3. Click *Browse* and locate the license key file.
4. Click *Upload*.

License status

The *Dashboard > FortiClient Status > License Information* widget displays your license statuses. EMS supports multiple licenses, including separate licenses for Telemetry and endpoint protection and management, for FortiSandbox Cloud 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 described in [To apply a paid license to FortiClient EMS: on page 35](#), then click *Sync License Now* in *Administration > Configure License* to apply a paid license to EMS.

Help with licensing

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

- Phone: +1-866-648-4638
- [Technical support](#): support.fortinet.com/

Specifying different ports

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

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

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

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



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

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

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



Upgrading a database edition outside normal production hours is recommended.

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

To upgrade SQL Server Express to Standard or Enterprise:

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

To test the SQL server upgrade:

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

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

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:

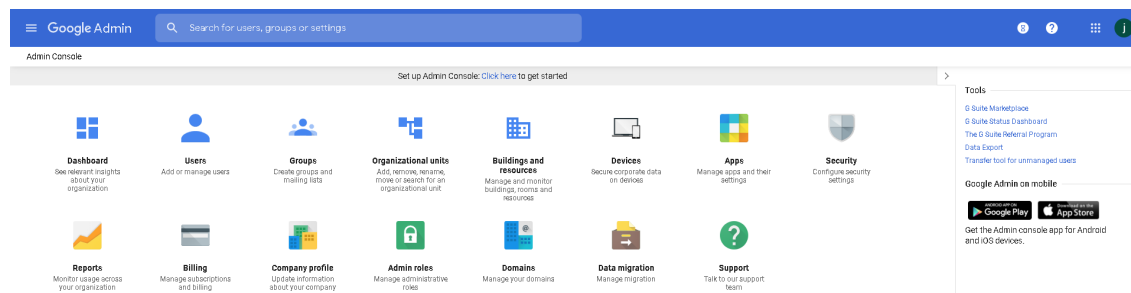
1. Log into the Google Admin console. See [Logging into the Google Admin console on page 40](#).
2. Add the FortiClient Web Filter extension. See [Adding the FortiClient Web Filter extension on page 40](#).
3. Configure the FortiClient Web Filter extension. See [Configuring the FortiClient Web Filter extension on page 41](#).
4. Add the root certificate. See [Adding root certificates on page 42](#).



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.



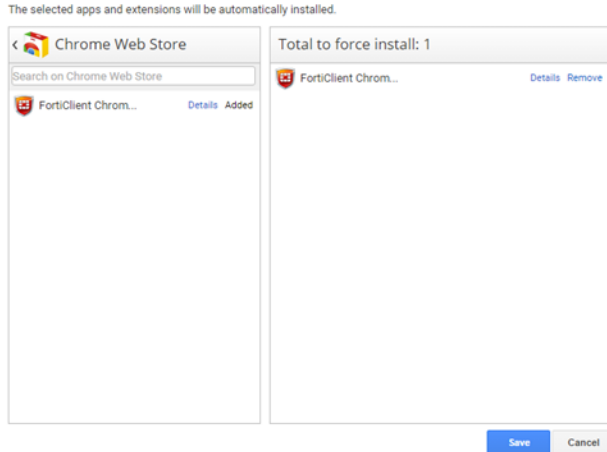
Adding the FortiClient Web Filter extension



FortiClient EMS software is not available for public use. You can only enable the feature using the following extension ID: igbgpehnbmhdgjbhkkpedommgmfbeao

1. In the Google Admin console, go to *Devices > Chrome Management > Settings > User & browser settings > 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. Under *Apps and Extensions*, beside *Force-installed Apps and Extensions*, click *Manage force-installed apps*.
4. Select *Chrome Web Store*, and search for the following extension ID: igbgpehnbmhdgjbhkkpedommgmfbeao.
5. Click *Add*. The extension displays under *Total to force install: 1*. Click *SAVE*.



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.

To configure the FortiClient Web Filter extension:

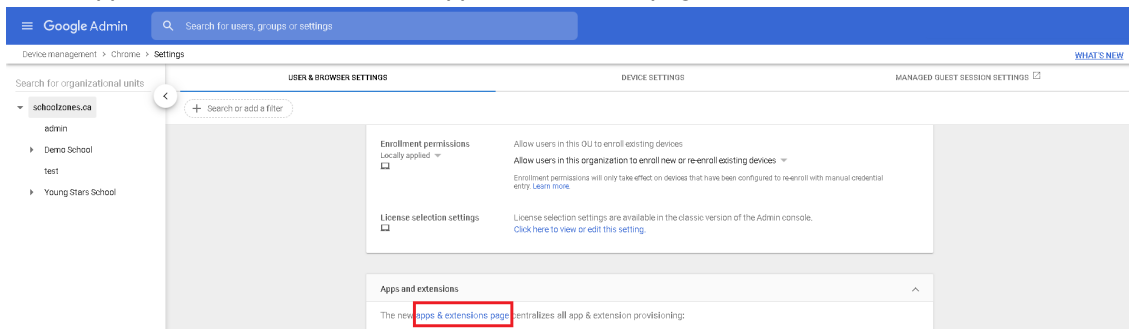
1. In FortiClient EMS, locate the server name and port by going to *System Settings > Server*.
2. Create a text file that contains the following text:

```
{
  "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 management > User & browser settings*.
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. Under *Apps and Extensions*, click the *apps & extensions* page link.



6. Click a domain or organizational unit (OU).
7. In the right pane, under *Policy for extensions*, paste the JSON content from step 2.
8. Click **Save**.
9. Go to *Devices > Chrome management > 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 206](#).

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 44](#).

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 44](#).



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

Scenario	Certificate and CA	Where to add certificates
Allow the FortiClient Chromebook Web Filter extension to trust FortiAnalyzer for logging	Public SSL certificate	<ul style="list-style-type: none"> • 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

1. In the Google Admin console, go to *Device Management > Network > Certificates (root certificate) (cert 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 Management > User & browser 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. For the *Developer Tools* option, select *Never allow use of built-in developer tools*.

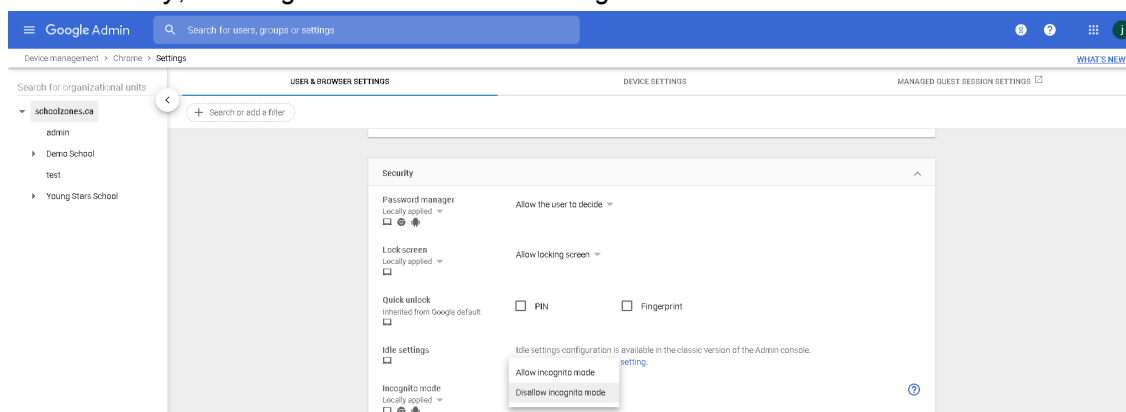
Disallowing incognito mode

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 management > User & browser 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. 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:

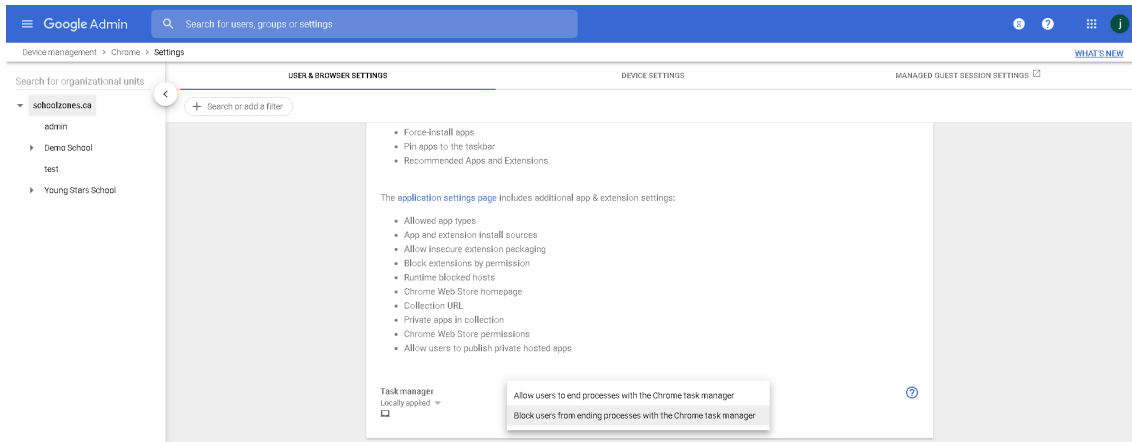
1. In the Google Admin console, go to *Devices > Chrome management > Device settings*.
2. On the left, select the organization that contains the desired users or enrolled browsers. To select all users and browsers, select the top-level organization. Otherwise, select a child.
3. Under *Sign-in settings*, 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 Management > User & browser settings > Apps and extensions*.
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 *Task manager* select *Block users from ending processes with the Chrome task manager* from the dropdown list.

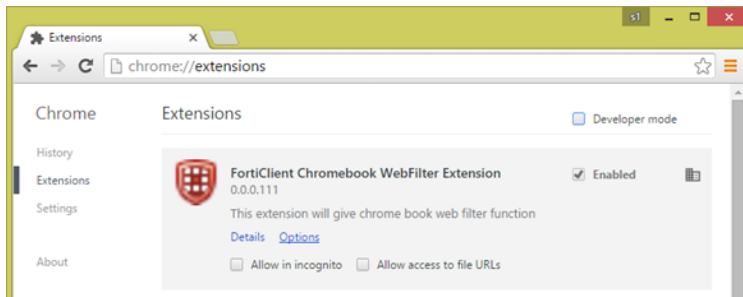


4. Click Save.

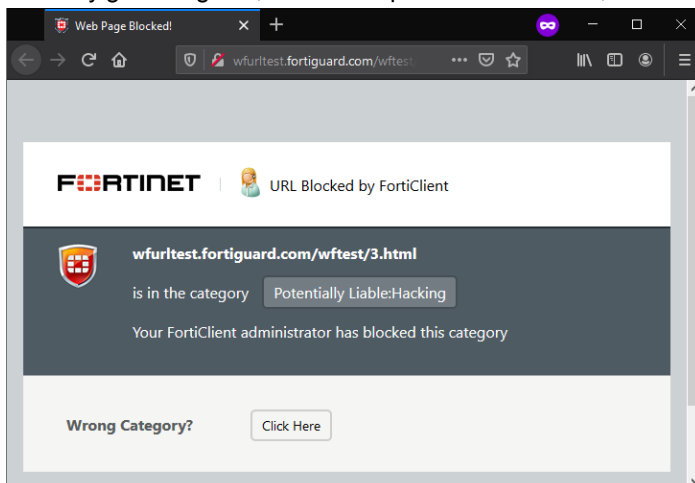
Verifying the FortiClient Web Filter extension

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.

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



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



Service account credentials

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



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

Configuring default service account credentials

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

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



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

To configure the default service account credentials, you must add the client ID's default value to the Google Admin console. Service account credentials do not require other configuration. See [Adding service account credentials to the Google Admin console on page 51](#).

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:

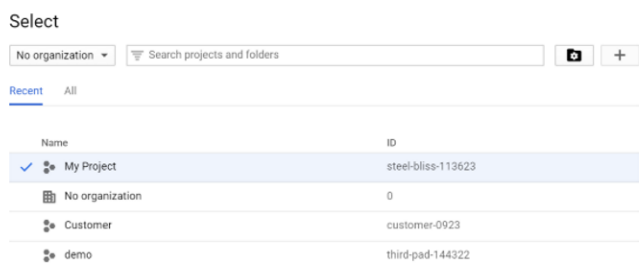
1. Create unique service account credentials using the Google Developer console. See [Creating unique service account credentials on page 48](#).
2. Add the unique service account credentials to the Google Admin console. See [Adding service account credentials to the Google Admin console on page 51](#).
3. Add the unique service account credentials to FortiClient EMS. See [Adding service account credentials to EMS on page 52](#).

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.

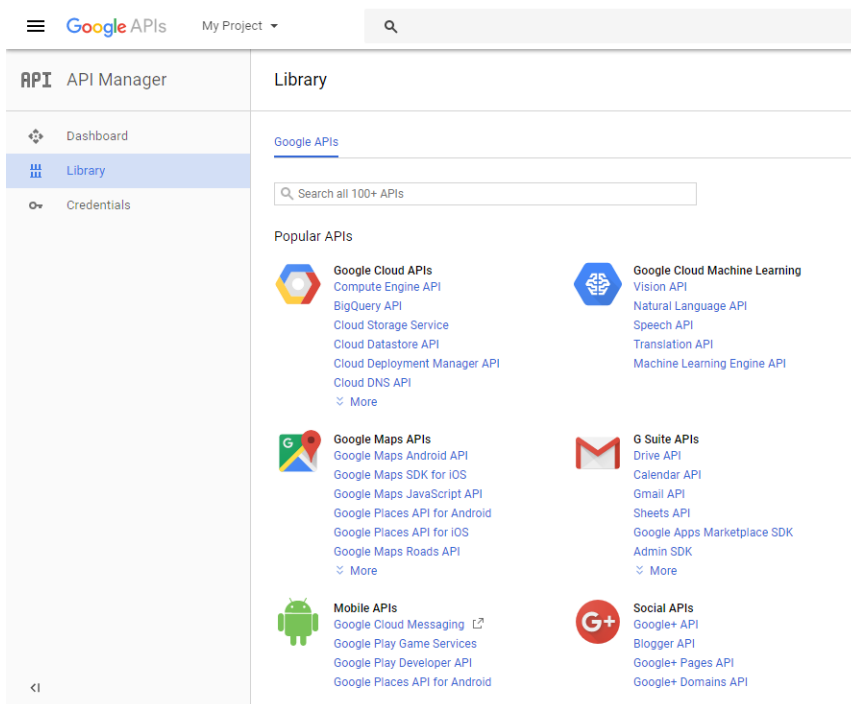


[CANCEL](#) [OPEN](#)

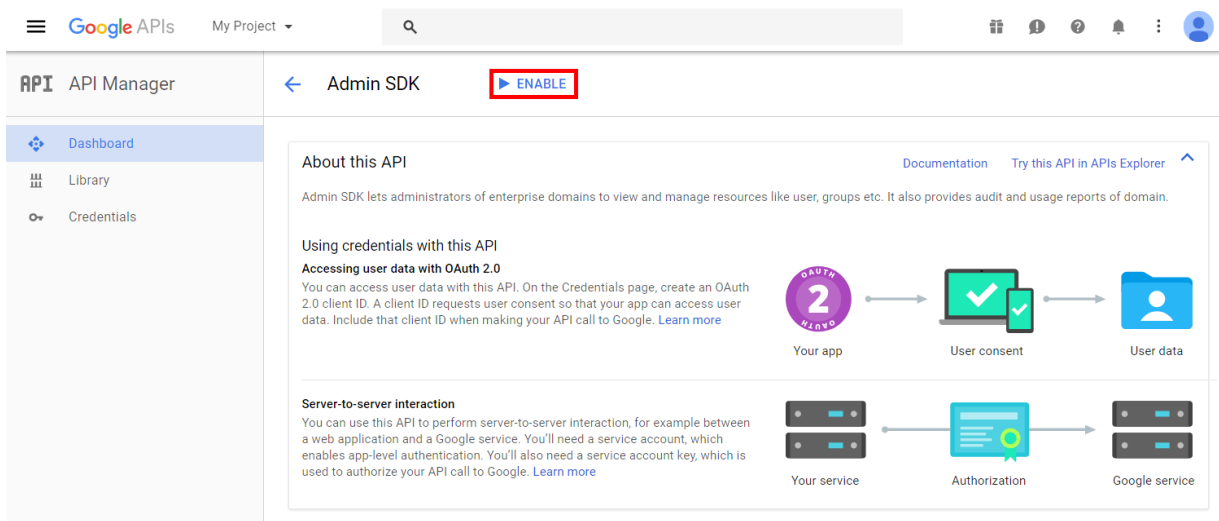
- b. Select your organization, if you see an organization dropdown list.
- c. Click the + button.
- d. In the *Project name* field, enter your project name, then click *Create*.

4. Enable the Admin SDK:

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



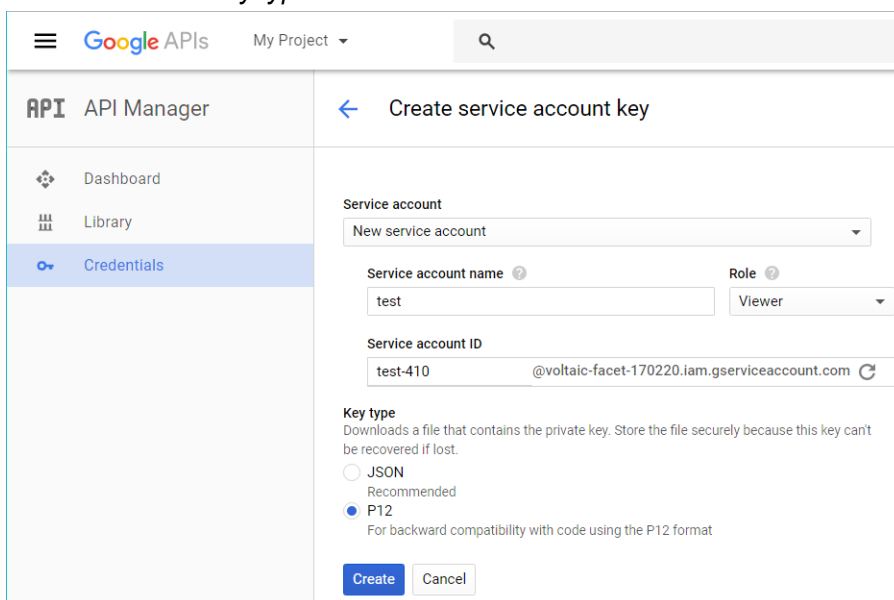
c. Click *ENABLE*.



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

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.

1. In the Google Admin console, go to **Security > Advanced settings > Manage API client access**. You may need to click **show more** to see **Advanced settings**.

2. Set the following options:

- a. For the *Client Name* option, add the client ID from the service account credentials.
- b. For the *API Scopes* option, 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.

3. Click *Authorize*.

Adding service account credentials to EMS

The section describes how to add the service account ID and service account certificate from the service account credentials to FortiClient EMS.

1. In FortiClient EMS, go to *System Settings > Server*.
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.

GUI

The FortiClient EMS GUI consists of the following areas:

Banner

Option	Description
Download icon	Displays if a new version of FortiClient EMS is available on FDS.
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
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.

Option	Description
Dashboard	
FortiClient 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 > Server</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 > Server</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.
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.
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.

Option	Description
Endpoint Policy	Create endpoint policies and manage policy updates for Windows, macOS, and Linux 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 > Server</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.
Deployment	Create deployment configurations to deploy FortiClient to endpoints.
Manage Installers	
Deployment Packages	Add and manage FortiClient deployment packages.
FortiClient Installers	View FortiClient installers available from FortiGuard. Add custom installers.
Policy Components	
CA Certificates	Upload and import CA certificates into FortiClient EMS.
On-fabric Detection Rules	Configure on-fabric detection rules for endpoints.
Telemetry Server Lists	Create and assign Telemetry server lists and manage list updates.
Compliance Verification	
Compliance Verification Rules	Define compliance verification rules.
Host Tag Monitor	View tagged endpoints.
Fabric Device Monitor	View all FortiGates connected to EMS for compliance verification and the list of tags that are shared with each FortiGate.
Administration	
Administrators	Add and manage FortiClient EMS administrators.
Admin Roles	Add and manage FortiClient EMS admin roles and permissions.
User Servers	Configure an AD domain as the user server. EMS uses this to authenticate EMS administrators.
User Settings	Configure the inactivity timeout and other user settings.
Fabric Devices	View Fabric devices connected to EMS.
Back up Database	Back up the FortiClient EMS database.

Option	Description
Restore Database	Restore the FortiClient EMS database.
Configure License	Upgrade or renew the FortiClient EMS license.
Logs	View log messages generated by FortiClient EMS and download raw logs.
System Settings	
Server	Change the IP address and port and configure other server settings for FortiClient EMS, including enabling Chromebook management.
Logs	Specify what level of log messages to capture in FortiClient EMS logs and when to automatically delete logs and alerts.
Fortinet Services	Configure the FortiGuard server location. Configure FortiManager to use for client software/signature updates and configure FortiCloud settings.
Endpoints	Configure endpoint settings.
Login Banner	Enable the pre-login banner to display a message to a user logging into FortiClient EMS.
SAML SSO	Configure SAML SSO authentication.
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

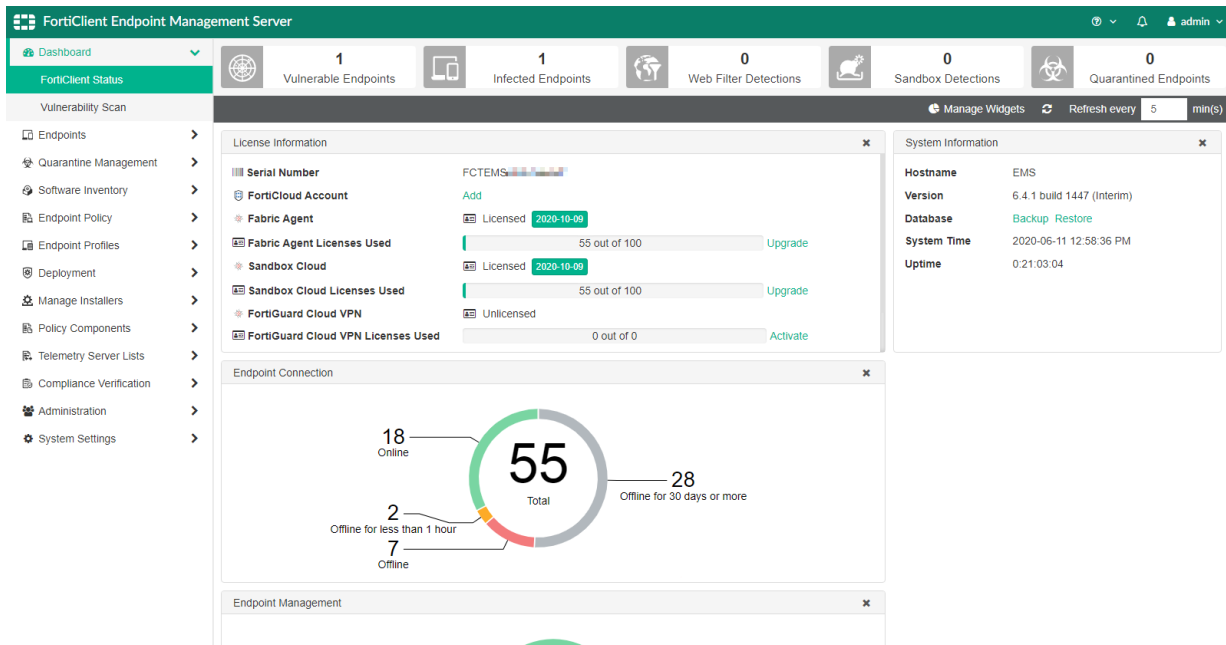
You can use the Dashboard to view summary information about the system and endpoints. You can view summary information about vulnerability scans on endpoints.

Viewing the FortiClient Status

To view the FortiClient Status:

1. In the left pane, click *Dashboard > FortiClient Status*.

A *System Information* widget and charts and widgets of summary information display. See [System Information widget on page 58](#) and [FortiClient Status charts and widgets on page 59](#).



2. For most *FortiClient 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 74](#).
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.

FortiClient Endpoint Management Server

Dashboard > Endpoint Event Summary

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:

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. Click <i>Backup</i> to back up the database. Click <i>Restore</i> to restore a backed up database.
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.

License Information widget

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

Option	Description
Serial Number	Serial number for FortiClient EMS.
FortiCloud Account	FortiCloudaccount that this EMS server is registered to. If EMS is not registered to a FortiCloudaccount, you can log into an existing FortiCloudaccount or create a new FortiCloudaccount from this widget.
Fabric Agent with Endpoint Protection	Status of the FortiClient Security Fabric Agent license. This license includes support for Telemetry and endpoint protection and management.
Sandbox Cloud	Status of the FortiClient Cloud Sandbox license. This license includes support for FortiSandbox Cloud.
FortiSASE	Status of the FortiSASE license.
FortiSASE Licenses Used	Number of FortiSASE licenses used out of the total number of available FortiSASE endpoint licenses. Also displays a button for activating, upgrading, or renewing a license, depending on the license status.
FortiClient Licenses Used	Number of licenses used out of the total number of available Windows, macOS, Linux, iOS, and Android FortiClient endpoint licenses. Also displays a button for activating, upgrading, or renewing a license, depending on the license status.
Chromebook	Status of the Chromebook license for FortiClient EMS. You can use this license for managing Chromebook endpoints.
Chromebook Licenses Used	Number of licenses used out of the total number of available Chromebook endpoint licenses. Also displays a button for activating, upgrading, or renewing a license, depending on the license status.

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 37](#).

FortiClient Status charts and widgets

FortiClient 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.



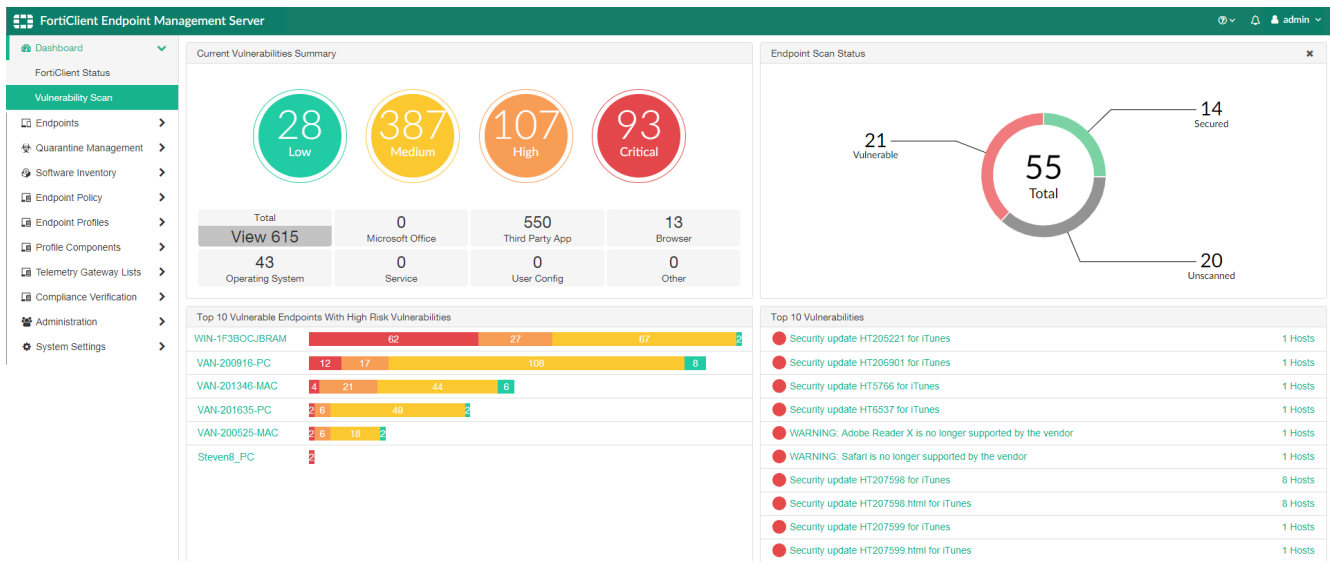
Available options may differ depending on the features you have enabled or disabled in *Feature Select*. See [Feature Select on page 217](#).

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	This chart indicates the percentage of Linux endpoints with each version of FortiClient installed. You can sort the data by version or count.
Endpoint Management	This chart indicates how many endpoints are disconnected and connected.

Option	Description
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>
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.



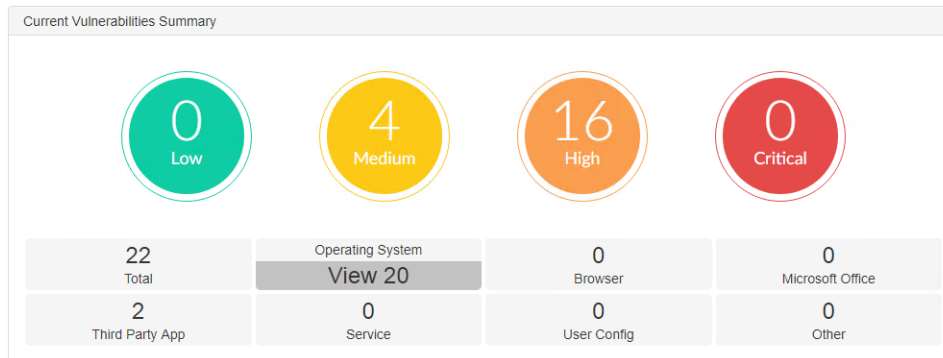
The *Vulnerability Scan* dashboard displays a number of charts. Each chart provides a summary of endpoint information. The sections in each chart are links. You can click sections of the charts or any row in the table to display more details.

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>							
Operating System Vulnerabilities		Patch All					
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>

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

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

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

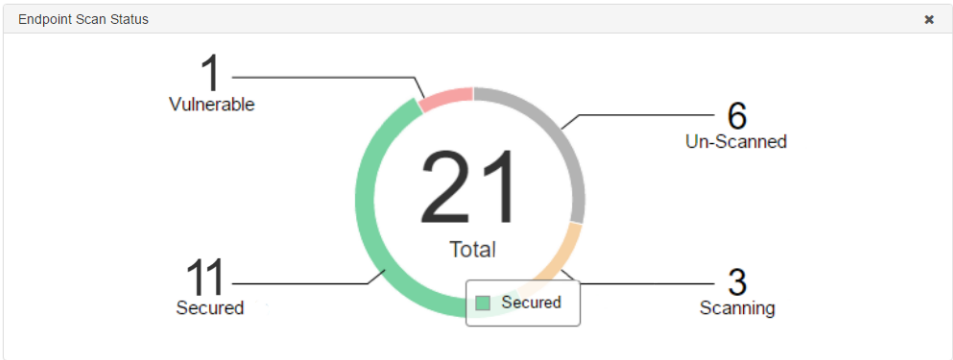
The screenshot shows the FortiClient Endpoint Management Server interface. The left sidebar contains a navigation menu with options: Dashboard, FortiClient Status, Vulnerability Scan, Endpoints, Quarantine Management, Software Inventory, Endpoint Policy, and Endpoint Profiles. The main content area is titled 'Medium Severity Vulnerabilities' and includes a 'Patch All' button. Below the title is a table of vulnerabilities. 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'. Each entry has 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				
admin				
Dashboard	Vulnerability Endpoint Patch All			
FortiClient Status	Hostname	Username	Vulnerability	Patch Status
Vulnerability Scan	WIN-1F3BOCJBRAM	Administrator	11 20 5	Patch
Endpoints	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 <i>Patch</i> button to patch the selected vulnerability with the next Telemetry communication between FortiClient EMS and the endpoint.

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

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

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.

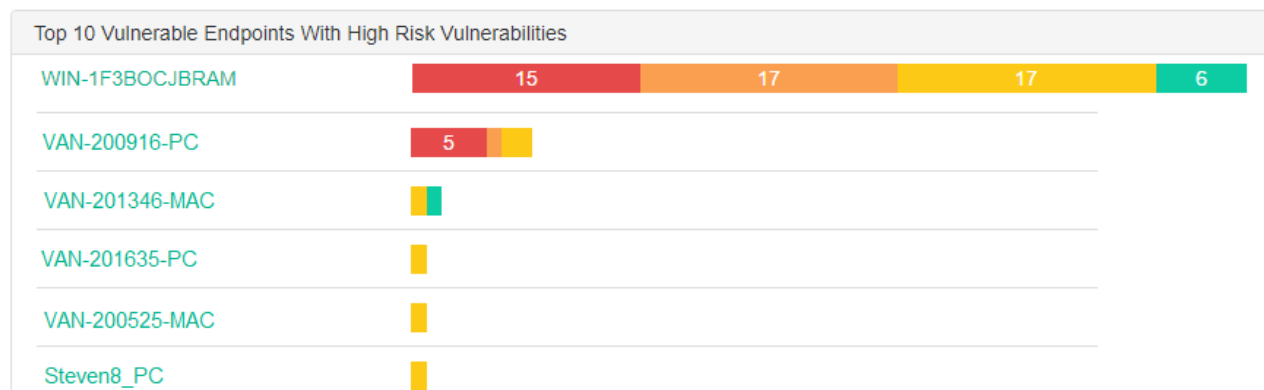
Vulnerability	Category	Severity	Patch Status
Security update HT5766 for iTunes	Application	Critical	Patch
Security update HT5936 for iTunes	Application	Critical	Patch
Security update HT6537 for iTunes	Application	Critical	Patch
Security update HT205221 for iTunes	Application	Critical	Patch
Security update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

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

Viewing the top 10 vulnerable endpoints with high risk vulnerabilities

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

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-1F3BOCJB RAM 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

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.</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>

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

FortiClient Status

Vulnerability Scan

Endpoints

Quarantine Management

Software Inventory

Endpoint Policy

Endpoint Profiles

Profile Components

Telemetry Gateway Lists

Compliance Verification

Administration

Vulnerabilities for WIN-1F3BOCJIBRAM

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

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.

The screenshot shows the FortiGuard Labs website. The header includes the Fortinet logo and navigation links: News / Research, Services, Threat Lookup, Resources, and a search bar labeled 'Search FortiGuard'. The breadcrumb trail reads: Home / Encyclopedia / Endpoint Vulnerability / Security update HT205221 for iTunes.

At a glance:

ID	21883
Created	Aug 02, 2016
Description Updated	Jan 09, 2019
Severity	● ● ● ● ●
Coverage	FortiClient

Endpoint Vulnerability

Security update HT205221 for iTunes

Description

Multiple memory corruption issues existed in the processing of text files. These issues were addressed through improved memory handling. Multiple memory corruption issues existed in the processing of unicode strings. These issues were addressed by updating ICU to version 55. A security issue existed in Microsoft Foundation Class's handling of library loading. This issue was addressed by updating to the latest version of the Microsoft Visual C++ Redistributable Package. Multiple memory corruption issues existed in WebKit. These issues were addressed through improved memory handling. A redirection issue existed in the handling of certain network connections. This issue was addressed through improved resource validation.

Affected Products

- 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 a 'Dashboard' menu with 'FortiClient Status' and 'Vulnerability Scan' options. The main content area is titled 'Affected Endpoints' and contains a table with the following data:

Hostname	Username	Last Seen	Scan Time
WIN-1F3B0CJB RAM	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

Refresh

Clear Filters

FortiClient Status

Vulnerability Scan

Endpoints

Quarantine Management

Software Inventory

Endpoint Policy

Endpoint Profiles

Profile Components

Telemetry Gateway Lists

Compliance Verification

Administration

System Settings

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 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 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.</p> <p>If a patch is already scheduled for the vulnerability, this column displays <i>Scheduled</i>.</p> <p>If the vulnerability must be patched manually, this column displays <i>Manual Patch</i>.</p>

Viewing 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 > Server > EMS for Chromebooks Settings*.

Option	Description
User Charts	
Active Users	Displays active and inactive users.
Managed Users	Displays managed and unmanaged users.
Webfilter Charts	

Option	Description
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 136 .
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 136 .
Others	
System Information	See System Information widget on page 58 .
License Information	See License Information widget on page 58 .

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.

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

Adding endpoints using an AD domain server

You can manually import endpoints from an 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.



A video on how to add a domain is available in the [Fortinet Video Library](#).



You can add the entire domain or an OU from the domain.



EMS does not support importing subdomains if you have already imported the parent domain in to EMS.

To add endpoints using an AD domain server:

1. Go to *Endpoints > Manage Domains > Add*. The *Domain* pane displays.
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.
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> .
Sync every	Enter the sync schedule between FortiClient EMS and the domain in minutes. The default is ten minutes.

3. Click *Test* to test the domain settings connection.
4. 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 edit the endpoints. These changes do not sync back to the AD server.

Connecting manually from FortiClient

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

To manually connect to EMS from FortiClient:

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

For information about FortiClient, see the [FortiClient Administration Guide](#).



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



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

Viewing endpoints

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

Viewing the Endpoints pane

You can view information about endpoints on the *Endpoints* pane.

To view the *Endpoints* pane:

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

Not Installed	Number of endpoints that do not have FortiClient installed. Click to display the list of endpoints without FortiClient installed.
Not Registered	Number of endpoints that are not connected to FortiClient EMS. Click to display the list of disconnected endpoints.
Out-Of-Sync	Number of endpoints with an out-of-sync profile. Click to display the list of endpoints with out-of-sync profiles.

Security Risk	Number of endpoints that are security risks. Click to display the list of endpoints that are security risks.
Quarantined	Number of endpoints that EMS has quarantined. Click to display the list of quarantined endpoints.
Endpoints	Click the checkbox to select all endpoints displayed in the content pane.
Show/Hide Heading	Click to hide or display the following column headings: <i>Device</i> , <i>User</i> , <i>IP</i> , <i>Configurations</i> , <i>Connections</i> , and <i>Alerts and Events</i> .
Show/Hide Full Group Path	Click to hide or display the full path for the group that the endpoint belongs to.
Refresh	Click to refresh the list of endpoints.
Search All Fields	Enter a value and press <i>Enter</i> to search for the value in the list of endpoints.
Filters	Click to display and hide filters you can use to filter the list of endpoints.
Device	Visible when headings are displayed. Displays an icon to represent the OS on the endpoint, the hostname, and the endpoint group.
User	Visible when headings are displayed. Displays the name of the user logged into the endpoint.
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:

- Request FortiClient Logs
- Request Diagnostic Results
- Update Signatures
- Download Available FortiClient Logs
- Download Available Diagnostic Results
- Deregister
- Quarantine
- Un-quarantine
- Exclude from Management
- 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 172 .
Network Status	<p>This section only appears for endpoints running FortiClient 6.4.1 and later versions.</p> <p>Displays the following information for the networks that the endpoint is connected to:</p> <ul style="list-style-type: none"> • MAC address

	<ul style="list-style-type: none"> • 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.
Host Verification Tags	Displays which tags have been applied to the endpoint based on the compliance verification rules. See Compliance Verification on page 179 .
Connection	Displays the connection status between the selected endpoint and FortiClient EMS and between the endpoint and FortiGate.
Configuration	<p>Displays the following information for the selected endpoint:</p> <ul style="list-style-type: none"> • Policy: Endpoint policy assigned to the selected endpoint • Profile: Profile assigned to the selected endpoint • Off-fabric Profile: Off-fabric profile assigned to the selected endpoint • Installer: FortiClient installer used for the selected endpoint. • Telemetry Gateway List: Telemetry gateway list used for the selected endpoint. Displays <i>Not Assigned</i> if no Telemetry gateway list has been assigned to 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 have a maximum of eight custom tags at a time.</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>. See Sending endpoint classification tags to FortiAnalyzer on page 83.</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.	
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 82 .	
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.

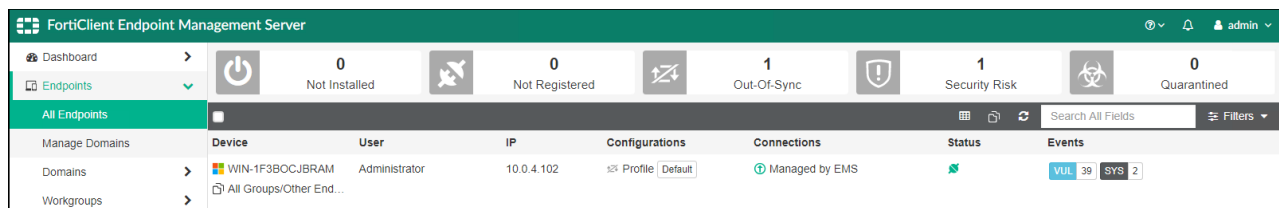
Using the quick status bar

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 74](#).

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 compliance verification and classification tags. See Compliance Verification on page 179 and Viewing the Endpoints pane on page 74 .
FortiClient	Lists the filter options for FortiClient version numbers.
Version	Enter the FortiClient version number to include in the filter.
Deployment Package	Lists the filter options for deployment.
Name	Enter the name(s) of the deployment package to include in the filter.
Status	Click one or more deployment status buttons to include in the filter. Selected status buttons are green. Hover the mouse over each button to view its tooltip. Clear the status button to exclude the status from the filter. Excluded status buttons are gray.
More States	Click to display additional statuses to include in the filter.
Policy	
Name	Enter the name(s) of the policy to include in the filter.
Status	Click the policy status to include in the filter. Selected status buttons are green. Choose between <i>Synced</i> and <i>Out-Of-Sync</i> . Clear the status button to exclude the status from the filter. Excluded status buttons are gray.
Profile	
Name	Enter the name(s) of the profile to include in the filter.
EMS	
Status	Click the status for FortiClient Telemetry connection to EMS to include in the filter. Selected status buttons are green. Clear the status button to exclude the status from the filter. Excluded status buttons are gray.
Events	Select the events to include in the filter. The selected checkboxes beside the events are included in the filter. Clear the checkbox beside the event to exclude the event from the filter.
Features	Enter the AV, Firewall, and/or vulnerability signature and/or engine to filter for.
Bookmarks	Displays the list of saved filter settings. Displays only after you have saved a bookmark. Click the <i>Bookmark</i> button to name and save filter settings. Click a bookmark to use the saved settings. Click the x beside a bookmark to delete it.
Search	Click the <i>Search</i> button to apply the filter setting.
Reset	Click the <i>Reset</i> button to clear the filter settings.
Bookmark	Click the <i>Bookmark</i> button to save the filter settings as a bookmark.

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

Using bookmarks to filter the list of endpoints

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

To create bookmarks to filter endpoints:

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

To use bookmarks to filter the list of endpoints:

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

Viewing Sandbox event details

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

To view Sandbox event details:

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

The screenshot displays the FortiClient Endpoint Management Server interface. The top navigation bar shows the user is logged in as 'admin'. The left sidebar contains a menu with options like Dashboard, Endpoints, Domains, Workgroups, and various management tools. The main content area shows the analysis results for 'credit_report.exe (High Risk)'. The analysis flow is: Threat Detected (2019-03-26 20:38:53) → Sandbox Analysis (2019-03-26 20:38:53) → File Blocked (2019-03-26 20:40:34) → Dynamic Signature Updated (2019-03-26 20:40:34). A 'Download Report' button is available. The endpoint details for 'ledington' (Lola Edington) are shown, including device information (Cherrywood, Microsoft Windows 8.1 Enterprise) and file information (credit_report.exe, 4096 bytes, MD5: e830a79ea311f1915932d3536064f8c0). The process tree is also visible.

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

The screenshot shows the 'Process Tree' view for 'credit_report.exe'. The top navigation bar and left sidebar are the same as in the previous screenshot. The main content area displays the process tree diagram, which shows the parent process '4357810084146248730.exe' spawning two child processes: 'svch' and 'msie'. Below the diagram, the 'Details' section provides information about the processes, including PID, File Path, File Type, CMD Line, and MD5.

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.

The screenshot displays the FortiAnalyzer EMS interface for a specific endpoint, DESKTOP-RIK3OAS, managed by Robert Glazier. The interface is divided into several sections:

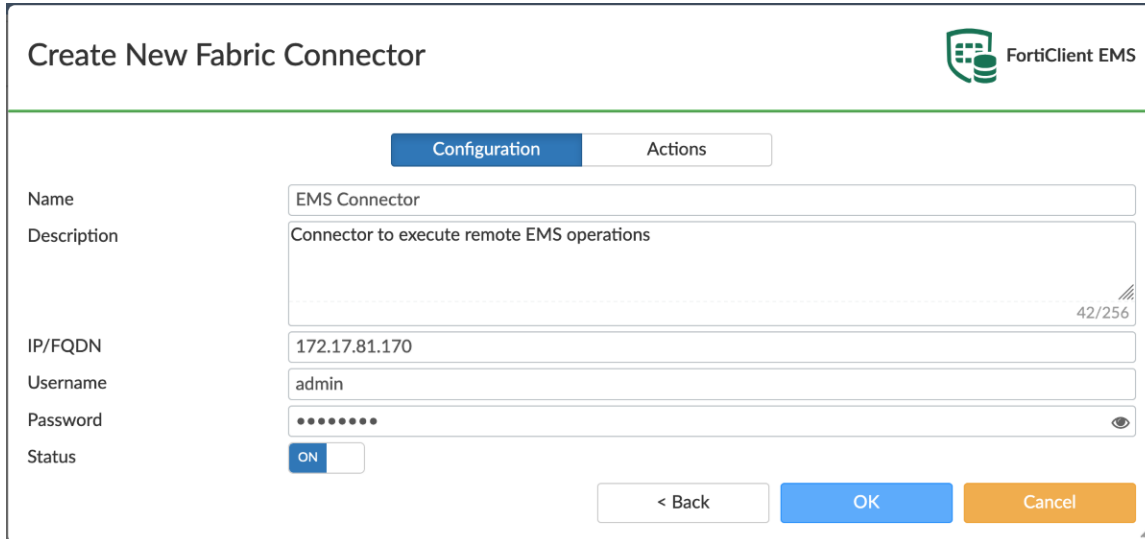
- Header:** Includes navigation tabs (Endpoints, Scan, Patch, Action) and a summary bar showing the endpoint name, user, IP address (192.168.137.243), and policy (Default).
- Summary Tab:** Displays endpoint details:
 - Device:** DESKTOP-RIK3OAS
 - OS:** Microsoft Windows 10 Professional Edit...
 - IP:** 192.168.137.243
 - MAC:** 00-15-5d-90-f2-00
 - Public IP:** 208.91.115.11
 - Status:** Online
 - Location:** On-Fabric
 - Network Status:** Ethernet
 - Hardware Details:**
 - Model:** Virtual Machine
 - Vendor:** Microsoft Corporation
 - CPU:** Intel(R) Core(TM) i7-8705G CPU...
 - RAM:** 2048 MB
 - S/N:** [Redacted]
 - HDD:** 43 GB
- Configuration Tab:** Shows settings managed by EMS:
 - Policy:** Default
 - Profile:** Policy-1
 - Off-net Profile:** Not assigned
 - Telemetry Server List:** Not assigned
 - Installer:** Not assigned
 - FortiClient Version:** 6.4.1.1505
 - FortiClient Serial Number:** [Redacted]
- Classification Tags Tab:**
 - Importance Tags:** A dropdown menu showing options: Low, Medium (selected), High, and Critical.
 - Custom Tags:** A section for creating custom tags. It shows a tag named "Department A" and a text input field labeled "Custom Tag" with a plus button to add new tags.

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*.

- Click the *FortiClient EMS* tile. The *Create New Fabric Connector* dialog opens.
- In the *Configuration* tab, configure the connector settings, enter the EMS IP address and administrator credentials.



The dialog box is titled "Create New Fabric Connector" and features the FortiClient EMS logo in the top right corner. It has two tabs: "Configuration" (selected) and "Actions". The form contains the following fields:

- Name:** EMS Connector
- Description:** Connector to execute remote EMS operations
- IP/FQDN:** 172.17.81.170
- Username:** admin
- Password:** A masked password field with a toggle to show/hide.
- Status:** A toggle switch currently set to "ON".

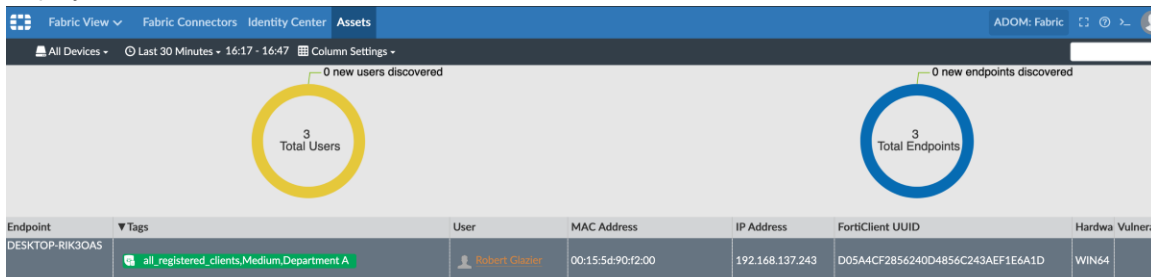
At the bottom right, there are three buttons: "< Back", "OK", and "Cancel".

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

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

- In FortiAnalyzer, in the Fabric ADOM, go to *FortiSoC > Automation > Playbook*.
- Click *Create New*, then *New Playbook created from scratch*.
- 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)
```
- Click **Save**.
- Click **Run**. Accept the *Manually Run Playbook* prompt.
- Go to *Automation > Playbook Monitor*. You can view the running playbook status.
- Once the corresponding playbook job finishes running, go to *Fabric View > Assets*. The endpoint and its tags display.



The screenshot shows the "Assets" tab in the FortiAnalyzer interface. It displays two donut charts: "3 Total Users" and "3 Total Endpoints". Below the charts is a table with the following data:

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

Managing endpoints

You can manage endpoints from the *Endpoints* pane.

Running AV scans on endpoints

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

For the difference between full and quick AV scans, see [AntiVirus Protection on page 127](#).

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.

Reregistering endpoints

You can reregister an endpoint that is currently online and registered to EMS. For example, if a new Telemetry gateway list is assigned to the endpoint but the endpoint did not automatically reregister, you could reregister the endpoint to manually request the endpoint to reread and follow the new Telemetry gateway list while reregistering.

To reregister endpoints:

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 *Re-register*. EMS reregisters the endpoint with the next FortiClient Telemetry communication.

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.

- 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.

Application Firewall must be enabled for this feature to function. See [Feature Select on page 217](#).

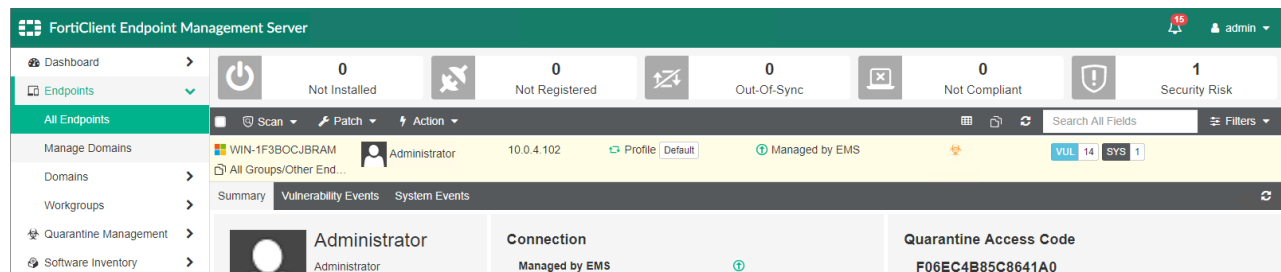
To quarantine an endpoint:

- Go to *Endpoints*.
- Click *All Endpoints*, a domain, or workgroup. A list of endpoints displays.
- Click an endpoint, and from the *Action* menu, select *Quarantine*.

The endpoint status changes to *Quarantined*, and EMS quarantines the endpoint with the next FortiClient Telemetry communication.

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

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



Quarantining an endpoint from FortiOS using EMS

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

- FortiGate
- FortiAnalyzer
- FortiClient EMS
- FortiClient

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

This configuration functions as follows:

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



FortiClient (Linux) does not support this feature.

Prerequisites

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

FortiClient

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

EMS

1. You must create a profile for the endpoint. See [Creating a profile to configure FortiClient on page 117](#).
2. You must create a Telemetry gateway list using the FortiGate's IP address for the endpoint. See [Creating a Telemetry server list on page 176](#)
3. 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 109](#).
4. Enable *Remote HTTPS access*. See [Configuring Server settings on page 204](#).

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.

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.

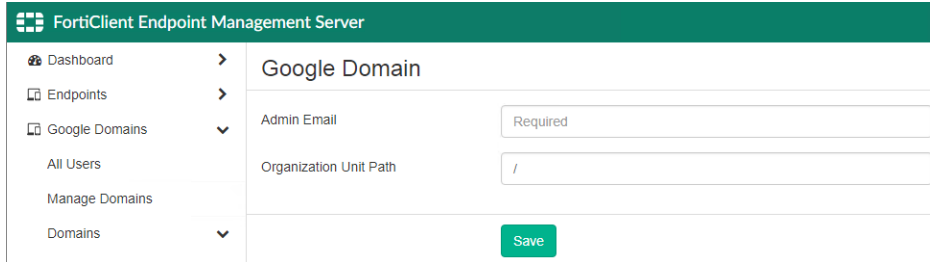
Google Domains

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

Adding a Google domain

To add a Google domain:

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



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



/ stands for the root of the domain.

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

Viewing domains

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

Viewing the Google Users pane

To view the Google Users pane:

You can view Google user information in FortiClient EMS.

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

Google Users Clear Filters ↻					
Name ▼	Email ▼	Last Login ▼	Last Policy Retr ▼	Domain ▼	Organization Path ▼
Art3 Sikes	art3.sikes@s...	8/4/2016 1:1...	Never 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's name.
Email	Chromebook user's email address.
Last Login	Date and time the user last logged into the domain.
Last Policy Retrieval	Date and time that the Google Chromebook last retrieved the endpoint profile.
Domain	Name of the domain to which the user belongs.
Organization Path	Organization path in the domain.

Viewing user details

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

To view user details:

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

User Details

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

Client Statistics

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

Blocked Sites (Past <number> Days)

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

Editing a domain

To edit a domain:

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

Deleting a domain

To delete a domain:

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

Group assignment rules

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

If a newly connected endpoint does not match any group assignment rule and belongs to an imported AD domain, the endpoint is moved into the OU to which it belongs in the AD domain tree. If no AD domain has been imported, or the endpoint also does not belong to the imported AD domain, it is placed in the *Other Endpoints* group.

EMS automatically places endpoints that do not apply for any group assignment rule into the *Other Endpoints* group.

Group assignment rule types

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

Installer ID group assignment rules

Creating a FortiClient 6.0+ deployment package includes an option to specify an installer ID. For example, consider you want all endpoints located in your company's headquarters to be placed in the same endpoint group. You can configure a FortiClient 6.0.1 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 endpoints with the installer ID "HQ" to be placed into the HQ group. The installer ID and group name do not need to match. See [Adding a group assignment rule on page 98](#).
2. Create a FortiClient 6.0+ deployment package. Specify the "HQ" installer ID when creating or uploading the installer. See [Adding a FortiClient deployment package on page 165](#) or [Adding a custom FortiClient installer on page 169](#).

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 98](#).
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 98](#).
2. With the next FortiClient Telemetry communication, endpoints with the specified OS installed are placed in the specified group.

Managing group assignment rule priority levels

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

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

To change rule priority levels:

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

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

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

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

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

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

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

Adding a group assignment rule

To add an installer ID group assignment rule:

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

1. Go to *Endpoints > Group Assignment Rules*.
2. Click *Add*.
3. Under *Type*, select *Installer ID*.
4. In the *Installer ID* field, enter the desired installer ID.
5. In the *Group* field, do one of the following:
 - a. If you want to place the endpoints into an existing group, select the desired group from the dropdown list.
 - b. If you want 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 requires all endpoints with an IP address in the specified subnet or IP address range to be placed 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. If you want to place the endpoints into an existing group, select the desired group from the dropdown list.
 - b. If you want 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 requires all endpoints that have the specified OS installed to be placed 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. If you want to place the endpoints into an existing group, select the desired group from the dropdown list.
 - b. If you want 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*.

Quarantine Management

You can view and allowlist files that FortiSandbox or AV has quarantined from a central management *Files* pane. You can also view and delete allowlisted files from the *Allowlist* pane.



This feature is only supported for Windows endpoints.

Files

FortiClient sends quarantined file information to FortiClient EMS. The FortiClient EMS administrator can view quarantined file information for all managed endpoints on the *Files* pane and allowlist files from FortiClient EMS if needed.

Viewing quarantined files

After FortiClient quarantines files on endpoints and sends the quarantined file information to FortiClient EMS, you can view the list of quarantined files on the *Files* pane. You can also view details about each quarantined file and use filters to access quarantined files with specific qualities.

To view the Files content pane:

You can view information about quarantined files on the *Files* content pane.

1. Go to *Quarantine Management > Files*. The list of quarantined files, a quick status bar, and a toolbar display in the content pane.

Quarantined Files	Number of files that FortiClient has quarantined on endpoints. Click to display the list of quarantined files.
Restored Files	Number of files that have been restored on endpoints. Click to display the list of restored files.
Affected Hosts	Number of hosts where FortiClient has quarantined files. Click to display the list of quarantined files sorted by hostname.
New Detections	Number of new detections. Click to display the list of newly detected threats sorted by date detected.
View	Toggle between the following options: <ul style="list-style-type: none">• View all files or view only quarantined files• Show or hide full path names for files

Display by	Select to display the list of files by instance, host, threat, or date.
Search All Fields	Enter a value and press <i>Enter</i> to search for the value in the list of files.
Filters	Click to display and hide filters you can use to filter the list of files.
Refresh	Click to refresh the list of files in the content pane.
Clear Filters	Click to clear all filters applied to the list of files.
Checkbox	Click to select all files displayed in the content pane.
Host	Hostname of the endpoint. Also shows the group the endpoint belongs to.
File	Name of the file.
Size	Size of the file in bytes.
Threat	Name of threat.
Source	Displays how FortiClient detected the threat: <ul style="list-style-type: none"> • Scheduled Scan • Email Scan • Startup Scan • Manual Scan • Realtime Scan • Rootkit Manual Scan • Sandbox Scan
Status	Status of the file: <i>Quarantined</i> , <i>Quarantined & Allowlisted</i> , <i>Restored</i> , or <i>Deleted</i> . Also shows the time that FortiClient quarantined the file.
Summary	Displays the number of threat instances and number of affected hosts.

To filter the file list:

You can filter the list of files displayed on the *Files* content pane.

1. Go to *Quarantine Management > Files*. The list of files displays.
2. Click the *Filters* menu, and set filters.

The filter options display.

For text values, you can use a comma (,) to separate values and an exclamation mark (!) to exclude a value.

Filename	Enter the file name(s) to include in the filter.
Location	Enter the file location(s) to include in the filter.

Checksum	Enter the checksum(s) to include in the filter.
Threat	Enter the threat(s) to include in the filter. You can also select the desired threat(s) from the dropdown list.
Source	Enter the source(s) to include in the filter. You can also select the desired source(s) from the dropdown list.
Status	Enter the status(es) to include in the filter. You can also select the desired status(es) from the dropdown list.
Date	Enter the range of dates to include in the filter.
Host	Enter the host(s) to include in the filter. You can also select the desired host(s) from the dropdown list.
Group	Enter the endpoint group(s) to include in the filter. You can also select the desired group(s) from the dropdown list.

3. Click *Apply*. The filtered list of files displays.
4. Click *Clear Filters* to clear the filter settings.

Allowlisting quarantined files

You can allowlist and restore quarantined files. This releases the files from quarantine and makes them accessible on the endpoint with the next Telemetry communication between FortiClient EMS and FortiClient.

To allowlist quarantined files:

1. Go to *Quarantine Management > Files*.
2. Select the desired files.
3. Click *Allowlist & Restore*.
4. In the confirmation dialog, click *Yes*, then *Okay*. The file status changes to *Quarantined & Allowlisted*.

Configuring quarantine management

You can configure EMS to delete quarantine records after a configured number of days.

You cannot use EMS to delete quarantined files from endpoints. To configure EMS to delete quarantined files from an endpoint after a specified duration, configure the [<cullage> XML option](#).

To configure quarantine management:

1. Go to *Quarantine Management > Files*.
2. Click the *Quarantine Management Settings* icon on the toolbar.
3. Enter the number of days after which to delete quarantine records from EMS. EMS determines the age of the quarantined file as when its status was last updated. For example, if you configure the duration as 180 days,

EMS deletes the quarantine record 180 days after the file was last updated.

Allowlist

Viewing allowlisted files

You can view the list of allowlisted files in the *Allowlist* pane. You can also view details about each allowlisted file and use filters to access allowlisted files with specific qualities:

Go to *Quarantine Management > Allowlist*. The list of allowlisted files and a toolbar display in the content pane.

Refresh	Click to refresh the list of files in the content pane.
Clear Filters	Click to clear all filters applied to the list of files.
Advanced Information	Click to view the FortiSandbox and AV signature and engine versions.
Date	Date and time the file was allowlisted.
File	Name of the file.
Checksum	File's checksum.
Threat	Name of threat.
Description	The file's description. Blank by default.

To filter allowlisted files:

1. Go to *Quarantine Management > Allowlist*. The list of files displays.
2. You can apply filters by date, file name, checksum, threat, and description. Do the following:
 - a. To filter files by date, click the filter icon beside the *Date* heading. Select the desired date range in the *Start* and *End* fields. You can also enter a start time and end time on the selected dates. The default time is 12:00 PM.
 - b. To filter by file name, checksum, threat, or description, click the filter icon beside the desired heading. Enter the value to include in the filter. You can toggle the *All/Any/Not* button for the following options:
 - *All*: Display all files that match the set filter.
 - *Any*: Display any file that matches the set filter.
 - *Not*: Display only files that do not match the set filter.

The filtered list of files displays.
3. To remove a filter, click the *X* icon beside the filter. To remove all filters, click the *Clear Filters* icon on the toolbar.

Editing file descriptions

You can edit an allowlisted file's description. By default, the file description is blank.

To edit an allowlisted file's description:

1. Go to *Quarantine Management > Allowlist*.
2. Select the desired file.
3. Click *Edit Description*.
4. In the *Required* field, enter the desired description.
5. Click *Confirm*. The description appears under the *Description* heading.

Deleting a file from the allowlist

You can delete files from the allowlist. This reverts the file's status to quarantined on the endpoint with the next Telemetry communication.

To delete a file from the allowlist:

1. Go to *Quarantine Management > Allowlist*.
2. Select the desired file.
3. Click *Delete*.
4. In the confirmation dialog, click *Yes*. EMS deletes the file from the allowlist. FortiClient quarantines the file on the endpoint with the next Telemetry communication. You can view the file on the *Files* pane.

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 150](#).

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.

FortiClient Endpoint Management Server

Dashboard

Endpoints

Quarantine Management

Software Inventory

17

Total Applications

7

Total Vendors

17

New Detections

Display by Application

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

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 106 .
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 107](#) for details on filtering the list of applications.

Endpoint Policy

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

Adding an endpoint policy

To add an endpoint policy:

1. Go to *Endpoint Policy > 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	Search for and select desired domain users to apply the policy to.
Profile	Include an endpoint profile in the policy. From the dropdown list, select the desired endpoint profile.
Profile (Off-Fabric)	<p>Include an endpoint profile in the policy 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 a more restrictive profile to the endpoint when it is determined to be off-fabric. From the dropdown list, select the desired endpoint profile.</p> <p>If including an off-fabric profile in a policy, it is highly recommended to also include on-fabric detection rules in the policy. Otherwise, EMS may not apply on-fabric and off-fabric profiles as desired.</p>
On-Fabric Detection Rules	<p>Select the on-fabric detection rules to include in the policy. You can select multiple rules.</p> <p>You must have already created on-fabric detection rules to include them in an endpoint policy. See On-fabric Detection Rules on page 172.</p>
Telemetry Server List	<p>Include a Telemetry server list in the policy. From the dropdown list, select the desired Telemetry server list.</p> <p>You must have already created a Telemetry server list to include one in an endpoint policy. See Creating a Telemetry server list on page 176.</p>
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 <i>Endpoint Policy > Manage Policies</i> .

- Click **Save**. You can view the newly created policy on the *Endpoint Policy > Manage Policies* page.

Name	Assigned Groups	Profile	Policy Components	Endpoint Count	Enabled
Policy_1	All Groups	PROFILE Profile_1 OFF-NET Default	100% ✓	1 4 endpoints no...	✓
Policy_2	fortitest.burnaby pbuffay rgreen	PROFILE Profile_2 OFF-NET Default	100% ✓	2	✓
Default		PROFILE Default		0	✓

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

Editing an endpoint policy

- Go to *Endpoint Policy > Manage Policies*.
- Select the endpoint policy.
- Click **Edit**.
- Edit as desired.
- Click **Save**.

Deleting an endpoint policy

- Go to *Endpoint Policy > Manage Policies*.
- Click the desired endpoint policy.
- Click **Delete**.
- In the confirmation dialog, click **Yes**.

Enabling/disabling an endpoint policy

- Go to *Endpoint Policy > Manage Policies*.
- 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 > Manage Policies* page.

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

To change endpoint policy priority levels:

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

Name	Endpoint Groups	Endpoint Profile	Policy Components	Telemetry Gateway List	Usage Count	Priority	Enabled
Seattle_general	All Groups/Seattle	PROFILE Seattle_general OFF-NET Seattle_offnet	ON-NET a	FGT_Seattle_floor1	1	1	<input type="checkbox"/>
SF_general	All Groups/SF	PROFILE SF_general	100% ✓		1	2	<input checked="" type="checkbox"/>
Seattle_HR	All Groups/Seattle/HR	PROFILE Seattle_HR		FGT_Seattle_floor2	1	3	<input checked="" type="checkbox"/>

4. Click *Save Priority*.

In the examples, there are three endpoint policies:

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

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

Name	Endpoint Groups	Endpoint Profile	Policy Components	Telemetry Gateway List	Usage Count	Priority	Enabled
Seattle_general	All Groups/Seattle	PROFILE Seattle_general OFF-NET Seattle_offnet	ON-NET a	FGT_Seattle_floor1	1	1	<input type="checkbox"/>
SF_general	All Groups/SF	PROFILE SF_general	100% ✓		1	2	<input checked="" type="checkbox"/>
Seattle_HR	All Groups/Seattle/HR	PROFILE Seattle_HR		FGT_Seattle_floor2	1	3	<input checked="" type="checkbox"/>

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

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

Consider that you then make the following changes:

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

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

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

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

Editing endpoint policy view

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

To edit endpoint policy view:

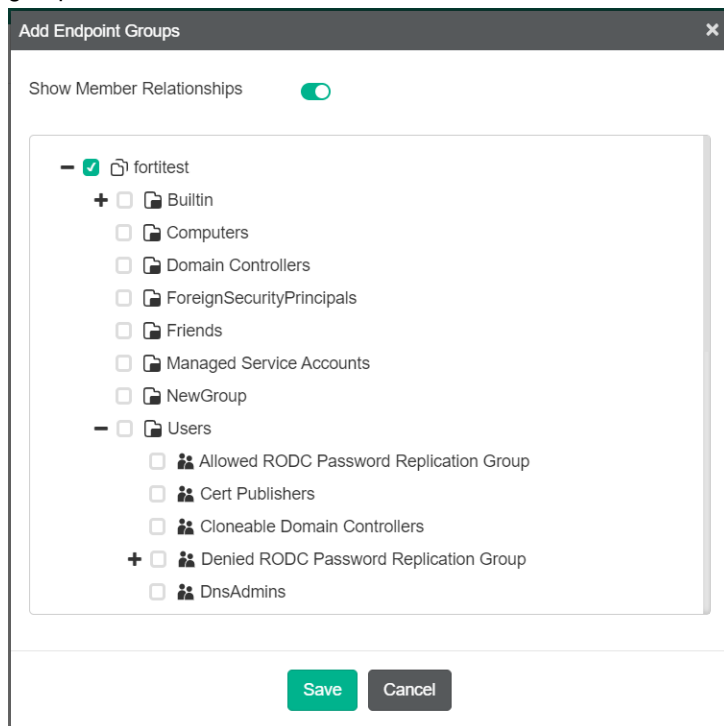
1. Go to *Endpoint Policy > Manage Policies*.
2. Click *Edit Columns*.
3. Enable or disable the columns as desired.
4. Click *Save*.

FortiClient management based on Active Directory user/user groups

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

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

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



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

When FortiClient connects to EMS, the following occurs:

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

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

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

FortiClient Endpoint Management Server

Dashboard

Endpoints

Quarantine Management

Software Inventory

Endpoint Policy

Manage Policies

Endpoint Profiles

Deployment

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><div>OFF-NET</div></div> <div>Profile_1</div> <div>Default</div> <div><div></div>100%</div>	<div><div></div>1</div> <div>4 endpoints not seen for last 30 days</div>	<div></div>	
Policy_2	<div><div>fortitest</div><div>pbufay</div><div>rgreen</div><div>10,00</div></div>				

Click the endpoint count to see the endpoint list.

FortiClient Endpoint Management Server							
Endpoints (4)							
Dashboard	Endpoints	Quarantine Management	Software Inventory	Endpoint Policy	Manage Policies	Endpoint Profiles	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. In 6.4.0, you no longer select available features for each deployment package.
3. Create a deployment package.
4. Create a deployment configuration.

For details on this deployment process, see the [FortiClient EMS Administration Guide](#).

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

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

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 > Server*.

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, not a Telemetry gateway list. For details on configuring a Chromebook policy, refer to the equivalent sections in [Endpoint Policy on page 109](#).

Endpoint Profiles

You can use the default endpoint profile or create endpoint profiles for many configurations and situations. You can also import FortiOS and FortiManager Web Filter profiles to EMS.

Configuring profiles

You can create and configure separate profiles for Windows, macOS, and Linux endpoints and for Chromebook endpoints. You can also edit the default profiles.

When you install FortiClient EMS, a default profile is created. EMS applies this profile to any groups you create. The default profile is designed to provide effective levels of protection. There are separate default profiles for Windows, macOS, and Linux endpoints and for Chromebook endpoints.

Editing a default profile

You can edit the default profile to add or remove settings. You can revert to default settings by clicking *Revert to Default*.

To edit a default profile:

1. Do one of the following:
 - a. To edit the default profile for Windows, macOS, and Linux endpoints, go to *Endpoint Profiles > Local Profiles*, and click the *Default* profile.
 - b. To edit the default profile for Chromebooks, go to *Endpoint Profiles > Local Chromebook Profiles*, and click the *Default - Chromebooks* profile.
2. Configure the settings on the tabs. See [Profile references on page 126](#).
3. Click *Save* to save the profile.

Configuring profiles for Windows, macOS, and Linux endpoints

The default profile is designed to provide effective levels of protection. To use specific features, such as application firewall, create a new profile or change the default profile. Consider the following when creating profiles:

- Use default settings within a profile.
- Consider the endpoint's role when changing the default profile or creating new profiles.
- Create a separate group and profile for endpoints requiring long-term special configuration.
- Use FortiClient EMS for all central profile settings, and set options for within the group instead of for the endpoint itself when possible.

These topics describe creating and configuring profiles for Windows, macOS, and Linux endpoints.

Creating a profile to configure FortiClient

This section describes how to create a profile that excludes any installation or uninstallation of FortiClient software on endpoints. You can use this profile type to configure FortiClient software on endpoints.

To create a profile to configure FortiClient:

1. Go to *Endpoint Profiles > Manage Profiles*, and click the *Add* button. To create a Chromebook profile, click *Add Chrome*.
2. In the *Profile Name* field, enter the profile name.
3. On the *Deployment* tab, leave *FortiClient Deployment* disabled.
4. Configure the settings on the remaining tabs. See [Profile references on page 126](#).
5. 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 217](#).

Importing a Web Filter 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 217](#).

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*.

Import Profiles from FortiGate/FortiManager

Connect to FortiGate/FortiManager Preview and Select Configure Synchronization

Type
☒ FortiGate ☐ FortiManager

IP address/Hostname

VDOM

Username

Password

Quit Back Next Import

3. Under *Type*, select *FortiGate* or *FortiManager*.
4. Complete the following options, and click *Next*.

IP address/Hostname	Enter the IP address and port of the FortiGate or FortiManager from which you are importing the profile, in the format: <ip address>:<port>.
VDOM	Enter a VDOM name from the FortiGate or FortiManager if applicable.
Username	Enter a username for the FortiGate or FortiManager.
Password	Enter the password for the user account entered above.

The list of Web Filter profiles configured on the FortiGate or FortiManager displays.

Import Profiles from FortiGate/FortiManager

Connect to FortiGate/FortiManager Preview and Select Configure Synchronization

☐ default

☒ monitor-all

☐ sniffer-profile

☒ wifi-default

Quit Back Next Import

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 124](#).
 - 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 136](#).

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 that the endpoint requires 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.

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 scope for the setting is for all VPN tunnels for that profile. The following instructions assume that you have already configured a remote SSL or IPsec VPN server in FortiOS. See the [FortiOS documentation](#).

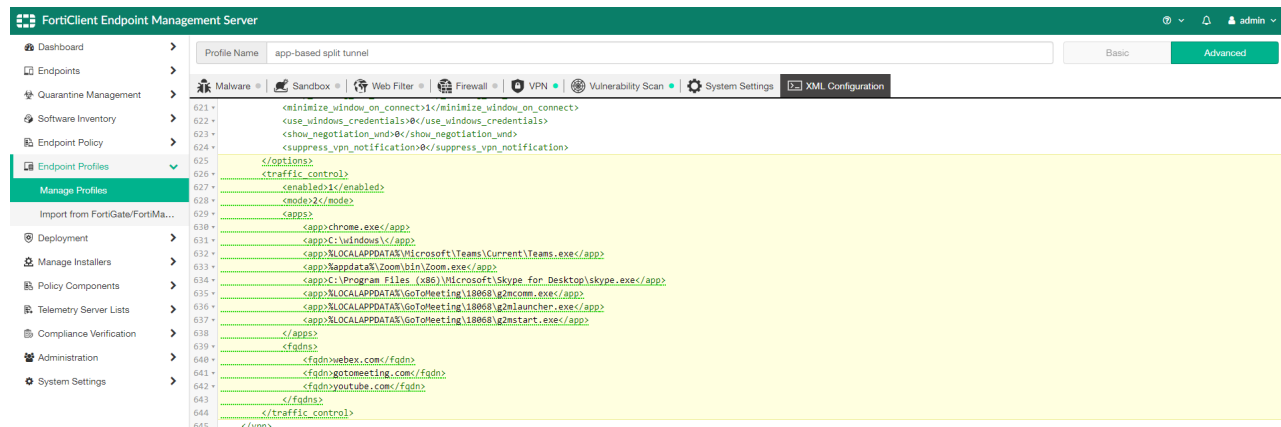
To configure application-based split tunnel:

1. In EMS, go to *Endpoint Profiles*, and select the desired profile. On the *XML Configuration* tab, configure the `<traffic_control>` elements to configure application-based split tunnel. The following provides an example and descriptions of the elements:

```
<vpn>
  <traffic_control>
    <enabled>1</enabled>
    <mode>2</mode>
    <apps>
      <app>chrome.exe</app>
      <app>C:\windows</app>
      <app>%LOCALAPPDATA%\Microsoft\Teams\Current\Teams.exe</app>
      <app>%appdata%\Zoom\bin\Zoom.exe</app>
      <app>C:\Program Files (x86)\Microsoft\Skype for Desktop\skype.exe</app>
      <app>%LOCALAPPDATA%\GoToMeeting\18068\g2mcomm.exe</app>
      <app>%LOCALAPPDATA%\GoToMeeting\18068\g2mlauncher.exe</app>
      <app>%LOCALAPPDATA%\GoToMeeting\18068\g2mstart.exe</app>
    </apps>
    <fqdns>
      <fqdn>webex.com</fqdn>
      <fqdn>gotomeeting.com</fqdn>
      <fqdn>youtube.com</fqdn>
    </fqdns>
  </traffic_control>
</vpn>
```

XML tag	Description
<code><enabled></code>	To enable the feature, enter 1. To disable the feature, enter 0.
<code><mode></code>	Enter 2 so that network traffic for all defined applications and FQDNs do not go through the VPN tunnel. You must configure this value as 2 for the feature to function.

XML tag	Description
<app>	<p>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. 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.</p> <p>To find a running application's full path, on the <i>Details</i> tab in Task Manager, add the <i>Image path name</i> column.</p> <p>Once the VPN tunnel is up, FortiClient binds the specified applications to the physical interface.</p> <p>In the example, for the GoToMeeting path, 18068 refers to the current installed version of the GoToMeeting application.</p>
<fqdn>	<p>Specify which FQDN traffic to exclude from the VPN tunnel and redirect to the endpoint physical interface. The FQDN resolved IP address is dynamically added to the route table when in use, and is removed after disconnection.</p> <p>In the example, youtube.com equals youtube.com and *.youtube.com.</p> <p>After defining an FQDN, such as youtube.com in the example, if you use any popular browser such as Chrome, Edge, or Firefox to access youtube.com, this traffic does not go through the VPN tunnel.</p>



2. 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.

Configuring profiles for Chromebooks

Chromebook profiles support web filtering by categories, blocklists and allowlists, and Safe Search. You can create different profiles and assign them to different groups in the Google domain using Chromebook policies.

These topics describe creating and configuring profiles for Chromebook endpoints.

Adding a new profile

When you install FortiClient EMS, a default profile is created. EMS applies this profile to any Google domains you add to FortiClient EMS.



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

To add a new profile:

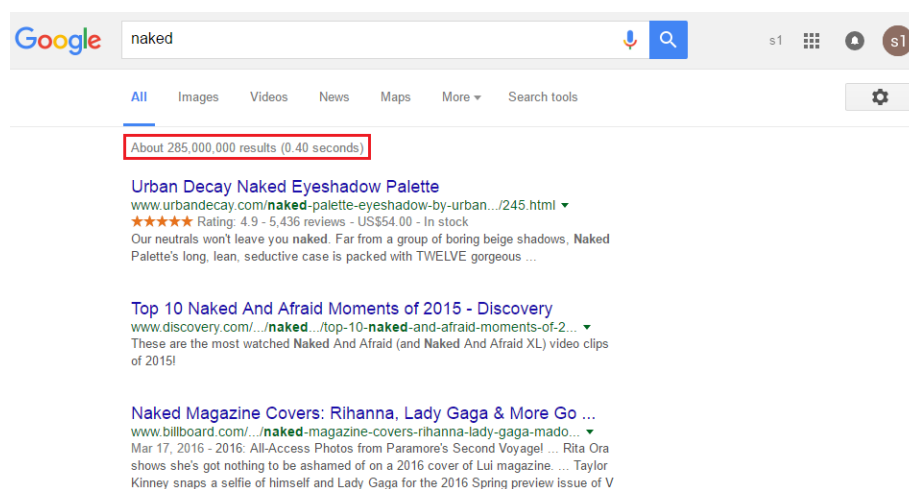
1. Go to *Endpoint Profiles > Manage Profiles*, and click the *Add Chrome* button.
2. In the *Profile Name* field, enter the profile name.
3. On the *Web Filter* tab, enable *Web Filter*, and set the web filtering options.
4. On the *System Settings* tab, set the logging options.
5. Click *Save*.

Enabling and disabling Safe Search

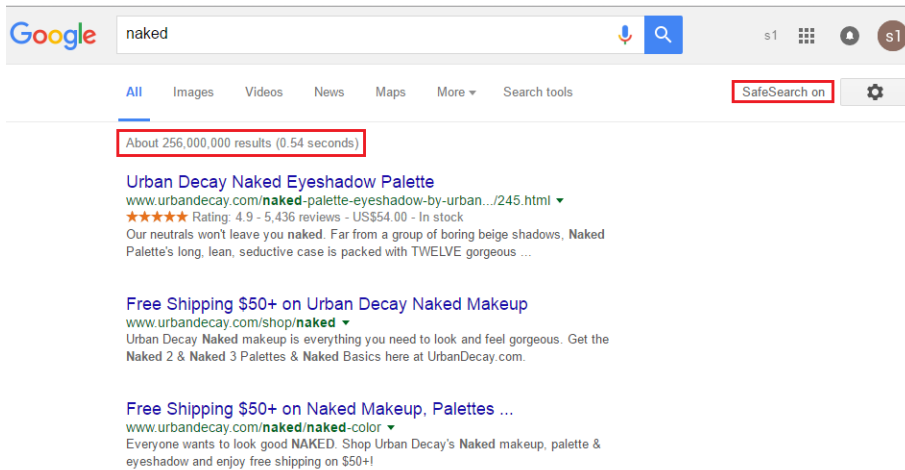
The search engine provides a Safe Search feature that blocks inappropriate or explicit images from search results. The Safe Search feature helps avoid most adult content. FortiClient EMS supports Safe Search for most common search engines, such as Google, Yahoo, and Bing.

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*.

Viewing profiles

When you create endpoint profiles, they are listed under *Endpoint Profiles* in the left pane. You can view endpoint profiles and their settings.

To view profiles:

1. Go to *Endpoint Profiles > Manage Profiles*. The content pane displays the list of profiles.
2. Click a profile name, then click *Edit*. The settings display in the content pane.

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. See [Profile references on page 126](#).
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. See [Profile references on page 126](#).
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 124](#).
 - 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.

Deleting profiles

You cannot delete the default profiles.

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

Configuring identity compliance for endpoints

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

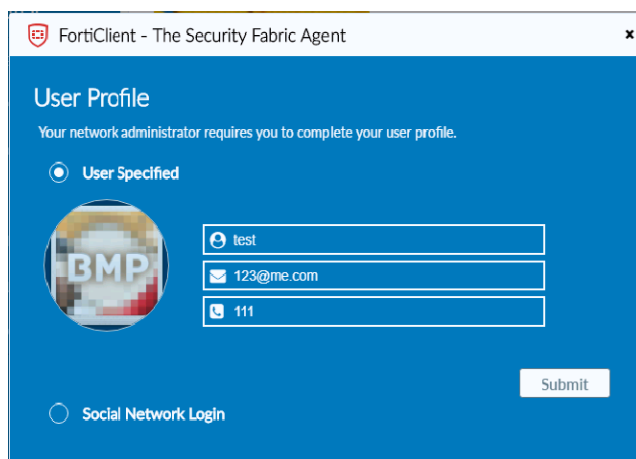
- User Input
- OS
- LinkedIn
- Google
- Salesforce

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.

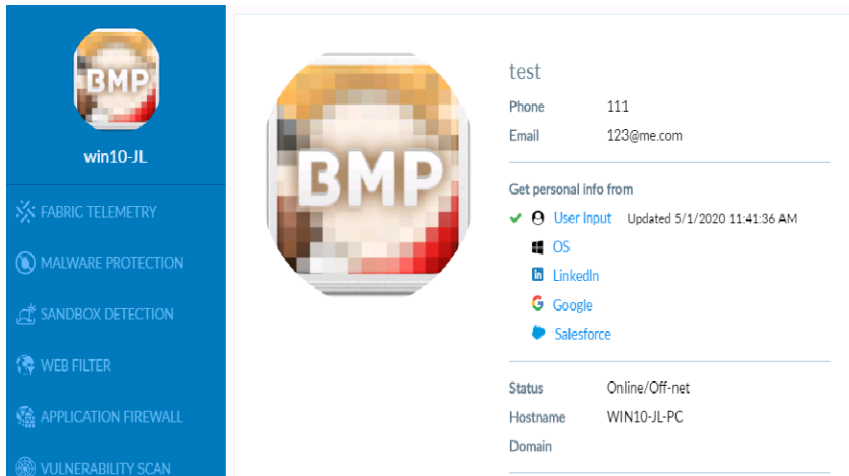
To configure identity compliance:

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*.

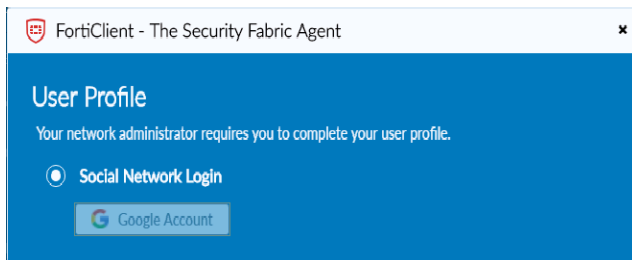
When *Notify Users to Submit User Identity Information* is enabled, the user sees the following notification on the endpoint. If *Manually Enter User Details* is enabled, the user can enter their information manually.

The screenshot shows a window titled "FortiClient - The Security Fabric Agent". Inside, there's a "User Profile" section with the text "Your network administrator requires you to complete your user profile." Below this, there are two radio buttons: "User Specified" (which is selected) and "Social Network Login". Under "User Specified", there's a circular profile picture placeholder with "BMP" text. To the right of the profile picture are three input fields: the first contains "test", the second contains "123@me.com", and the third contains "111". At the bottom right of the form is a "Submit" button.

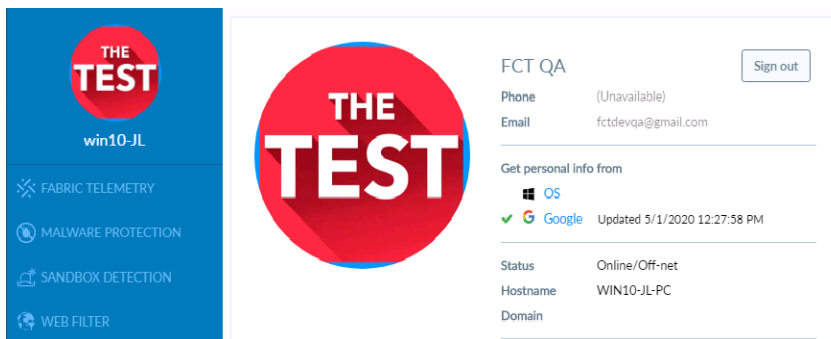
FortiClient displays the entered login information.



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



FortiClient displays the Google login information.



Profile references

This section contains descriptions of the tabs and options used to configure profiles.

For Chromebooks, only the *Web Filter* and *System Settings* tabs are available. All other tabs are exclusive to Windows, macOS, and Linux endpoints.



Available options may differ depending on the features you have enabled or disabled in *Feature Select*. See [Feature Select on page 217](#).

Profile Name

Option	Description
Profile Name	Enter the profile name.
Basic	Select to display basic configuration options.
Advanced	Select to configure the profile using XML on the <i>XML Configuration</i> tab. Displays advanced options for configuration. This option is only available for Windows, macOS, and Linux profiles.

Malware Protection

The *Malware Protection* tab contains options for configuring AV, anti-exploit, cloud-based malware detection, removable media access, exclusions list, and other options. Some options only display if you enable *Advanced* view.

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.
Block Known Communication Channels Used by Attackers	Enable Command and Control (C&C) detection using IP reputation database signatures. Check network traffic against known C&C IP address plus port number combinations.
Block Access to Malicious Websites	Block all access to malicious websites. You must select <i>FortiProxy (Disable Only When Troubleshooting)</i> on the <i>System Settings</i> tab before you can enable this option. If you are syncing the profile's Web Filter settings from a Web Filter profile imported from FortiOS or FortiManager, you cannot configure actions for the security risk site categories in EMS. EMS synchronizes these settings from the FortiOS or FortiManager Web Filter profile. See Web Filter on page 136 .
Security Risk	Configure an action for the security risk site category by selecting one of the following: <ul style="list-style-type: none"> Block Warn Allow Monitor 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 security risk category contains the following subcategories:

Options	Description
	<ul style="list-style-type: none"> • Dynamic DNS • Malicious Websites • Newly Observed Domain • Newly Registered Domain • Phishing • Spam URLs
Use the Exclusion List Defined in the Web Filter Profile	If you enable this option, EMS uses the exclusion list on the <i>Web Filter</i> tab. If you disable this option, you must define exclusions under <i>Exclusions</i> .
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 excludes list default file extensions.
Max Size	Only scan files under the specified size. To allow scanning compressed files of any size, enter 0.
Scan Files Accessed by User Process	Configure when RTP should scan files that a user-initiated process accesses. Select one of the following: <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	Enable system process scanning. Select one of the following: <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

Options	Description
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
Integrate FortiClient into Windows Explorer's Context Menu	Adds a <i>Scan with FortiClient AntiVirus</i> option to the Windows Explorer right-click 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.

Options	Description
Max Size	Only scan files under the specified size (in MB). To allow scanning compressed files of any size, enter 0.
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. • <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.
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	<p>Select one of the following:</p> <ul style="list-style-type: none"> • <i>Quick</i>: 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. • <i>Full</i>: Runs the rootkit detection engine to detect and remove rootkits, then performs a full system scan of all files, executable files, DLLs, and drivers. • <i>Custom</i>: 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.

Options	Description
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-Exploit

Enable anti-exploit engine to detect suspicious processes (payload) running from legitimate applications.

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.

Options	Description
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.

Options	Description
Control removable media access	<p>Configure the action to take with removable media devices. Available options are:</p> <ul style="list-style-type: none"> • <i>Allow</i>: Allow access to all removable media devices connected to the endpoint. • <i>Block</i>: Block access to all removable media devices connected to the endpoint. • <i>Monitor</i>: Log all removable media device connections to the endpoint. <p>This action applies to all USB devices, including keyboards, mice, and webcams. You can configure different actions for different removable media devices using XML configuration. See Removable media access.</p>
Show bubble notifications	Display bubble notifications when FortiClient blocks removable media access.

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 %windir%
- Path variable %allusersprofile%
- Path variable %systemroot%
- Path variable %systemdrive%

Combinations of wildcards and variables are not supported.

Having a longer exclusion list affects AV performance. Keeping the exclusion list as short as possible is advised.



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.
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

Options	Description
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 Detection

Enable Sandbox Detection. Some options only display if you enable *Advanced* view. Configure the following options:

Options	Description
Sandbox Detection	Enable Sandbox Detection. Enable or disable the eye icon to show or hide this feature from the end user in FortiClient.
Server	
FortiSandbox	Select <i>Appliance</i> to configure connection to an on-premise FortiSandbox appliance or <i>Cloud</i> to configure connection to FortiSandbox Cloud. FortiSandbox Cloud 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, FortiSandbox Cloud does not offer the full range of features that a FortiSandbox appliance offers. See Appendix F - FortiCloud Sandbox .
IP address/Hostname	Enter the FortiSandbox's IP address or hostname. Click <i>Test Connection</i> to ensure that EMS can communicate with FortiSandbox. This option is only available for a FortiSandbox appliance.
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 82 .
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 82 .
Region	FortiSandbox Cloud region. See Configuring Fortinet Services settings on page 208 .
Time Zone	FortiSandbox Cloud time zone. See Configuring Fortinet Services settings on page 208 .
License Status	Displays the Sandbox Cloud license status. Using FortiSandbox Cloud requires an additional license. See FortiClient EMS on page 20 .

Options	Description
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. • <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	
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 Sandbox <detect_level> setting.
Exceptions	
Exclude Files from Trusted Sources	<p>Exclude files signed by trusted sources from FortiSandbox submission. Following is a list of sources trusted by FortiSandbox:</p> <ul style="list-style-type: none"> • Microsoft • Fortinet • Mozilla • Windows • Google • Skype • Apple • Yahoo!

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



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.

Web Filter

For Windows, macOS, and Linux profiles, you must enable *FortiProxy (Disable Only When Troubleshooting)* on the *System Settings* tab to use the *Web Filter* options.

Configuration	Description
Web Filter	<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>
Sync web filter profile from FortiGate / FortiManager in the fabric.	<p>From the dropdown list, select the desired FortiOS or FortiManager Web Filter profile. When this option is enabled, you cannot modify the profile's Web Filter settings in EMS. Instead, EMS synchronizes Web Filter settings for this profile from the configured FortiGate or FortiManager depending on the synchronization schedule configured in Importing a Web Filter profile from FortiOS or FortiManager on page 117. You can still modify the profile's settings for other features, such as VPN or AV, from EMS.</p> <p>This option is only available if you have previously imported a Web Filter profile from FortiOS or FortiManager. See Importing a Web Filter profile from FortiOS or FortiManager on page 117.</p>
General	
Client Web Filtering When On-Fabric	Enable client web filtering when on-fabric. This setting affects the <i>Block Access to Malicious Websites</i> setting in Malware Protection on page 127 .
Log All URLs	Log all URLs. When this setting is disabled, FortiClient EMS only logs URLs as specified by per-category or per-URL settings.
Log User Initiated Traffic	Log only user-initiated traffic.
Action On HTTPS Site Blocking	<ul style="list-style-type: none"> Display In-Browser Message

Configuration	Description
Enable Web Browser Plugin for HTTPS Web Filtering	<ul style="list-style-type: none"> • Fail Connection & Show Bubble Notification • Fail Connection <p>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 and Firefox browsers on Windows platforms.</p>
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>When Safe Search is enabled, the endpoint's Google search is set to Restricted mode.</p> <p>For Windows and macOS endpoints, enabling Safe Search also sets YouTube access to Strict Restricted access.</p> <p>For Chromebooks, you can configure the Restriction Level to Strict or Moderate for YouTube access. This setting only affects YouTube access. 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>
Site Categories	<p>Enable site categories from FortiGuard. When you disable site categories, the exclusion list protects FortiClient.</p> <p>See the FortiGuard website for descriptions of the available categories and subcategories.</p> <p>For all categories, you can configure an action for the entire site category by selecting one of the following:</p> <ul style="list-style-type: none"> • Block • Warn • Allow • Monitor <p>You can also click the + button beside the site category to view all subcategories and configure individual actions (Block, Warn, Allow, Monitor) for each subcategory. The following lists each site category's subcategories.</p>
Adult/Mature Content	<ul style="list-style-type: none"> • Abortion • Advocacy Organizations • Alcohol • Alternative Beliefs • Dating • Gambling • Lingerie and Swimsuit

Configuration	Description
	<ul style="list-style-type: none">• 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 Abuse • Discrimination • Drug Abuse • Explicit Violence • Extremist Groups • Hacking • Illegal or Unethical • Plagiarism • Proxy Avoidance
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>
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.

Configuration	Description
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
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>

Configuration	Description
	<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.

Application Firewall

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>

Configuration	Description
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.
Categories	<p>Enable FortiClient firewall to allow, block, or monitor applications based on their signature.</p> <p>Block, allow or monitor the following categories:</p> <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.

VPN

Configuration	Description
VPN	Enable or disable VPN.

Configuration	Description
	Enable or disable the eye icon to show or hide this feature from the end user in FortiClient.
General	
Allow Personal VPN	Allow users to create, modify, and use personal VPN configurations.
Disable Connect/Disconnect	Disable the <i>Connect/Disconnect</i> button when using <i>Auto Connect</i> with VPN.
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.
Current Connection	Select the current VPN tunnel.
Keep Running 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	
DNS Cache Service Control	FortiClient disables Windows DNS cache when an SSL VPN tunnel is established. The DNS cache is restored after the SSL VPN tunnel is disconnected. If it is observed that FSSO clients do not function correctly when an SSL VPN tunnel is up, use <i>Prefer SSL VPN DNS</i> to control the DNS cache.
Prefer SSL VPN DNS	When disabled, EMS does not add the custom DNS server from SSL VPN to the physical interface. When enabled, EMS prepends the custom DNS server from SSL VPN to the physical interface.
IPsec VPN	
	Enable IPsec VPN.

Configuration	Description
	<p>Enable or disable the following:</p> <ul style="list-style-type: none"> • Beep If Connection Fails • Use Windows Store Certificates <ul style="list-style-type: none"> • Current User Windows Store Certificates • Local Computer Windows Store Certificates • Use Smart Card Certificates • Show Auth Certificates Only • Block IPv6 • Enable UDP Checksum • Disable Default Route • Check for Certificate Private Key • Enhanced Key Usage Mandatory

The following options are available in the *Creating VPN Tunnel* window after clicking the *Add Tunnel* button in the *VPN Tunnels* section.

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> or <i>IPsec VPN</i> .
Remote Gateway	Enter the remote gateway IP address/hostname. You can configure multiple remote gateways by clicking the + button. If one gateway is not available, the tunnel connects to the next configured gateway.
Port	Enter the access port. Available if you selected <i>SSL VPN</i> . The default port is 443.
Require Certificate	Require a certificate. Available if you selected <i>SSL VPN</i> .
Authentication Method	Select the authentication method for the VPN. Available if you selected <i>IPsec VPN</i> .
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.
VPN Settings	Available if you selected <i>IPsec VPN</i> for the VPN type.
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>Available if you selected <i>IPsec VPN</i> for the VPN type.</p> <p>Select the encryption and authentication algorithms used to generate keys for protecting negotiations and add encryption and authentication algorithms as required.</p> <p>You need to select a minimum of one and a maximum of two combinations. The remote peer or client must be configured to use at least one of the proposals that you define.</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	<p>Available if you selected <i>IPsec VPN</i> for the VPN type.</p> <p>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.</p>

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. Available if you selected <i>IPsec VPN</i> for the VPN type.
Enable XAuth	Enable IKE Extended Authentication (xAuth). Available if you selected <i>IPsec VPN</i> for the VPN type.
XAuth Timeout	Only available if <i>Enable XAuth</i> is enabled. Configure the IKE Extended Authentication (xAuth) 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. Available if you selected <i>IPsec VPN</i> for the VPN type.
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. Available if you selected <i>SSL VPN</i> for the VPN type.
Save Username	Save your username.
Allow Non-Administrators to Use Machine Certificates	Allow non-administrator users to use local machine certificates. Available if you selected <i>SSL VPN</i> for the VPN type.
Enforce Acceptance of Disclaimer Message	Enable and enter a disclaimer message that appears when the user attempts VPN connection. The user must accept the message to allow connection.

Enable SAML Login	Enable SAML SSO login for this VPN tunnel. See SAML SSO on page 210 .
Redundant Sort Method	How FortiClient determines the order in which to try connection to the SSL VPN servers when more than one is defined. FortiClient calculates the order before each SSL VPN connection attempt. When <i>Server</i> is selected, FortiClient tries the order explicitly defined in the server settings. When <i>Ping Speed</i> is selected, FortiClient determines the order by the ping response speed. When <i>TCP Round Trip Time</i> is selected, FortiClient determines the order by the TCP round trip time.
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.

Vulnerability Scan



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

Configuration	Description
Vulnerability Scan	Enable or disable Vulnerability Scan. Enable or disable the eye icon to show or hide this feature from the end user in FortiClient.
Scanning	
Scan on Registration	Scan endpoints upon connecting to a FortiGate.
Scan on Vulnerability Signature Update	Scan endpoints upon updating a vulnerability signature.
Scan for OS Updates	Scan for OS updates.
Enable Proxy	Enable using proxy settings configured in when downloading updates for vulnerability patches.

Configuration	Description
Automatic Maintenance	Configure settings for automatic maintenance. This configures Vulnerability Scan to run as part of Windows automatic maintenance. Adding FortiClient Vulnerability Scans to the Windows automatic maintenance queue allows the system to choose an appropriate time for the scan that will have minimal impact to the user, PC performance, and energy efficiency. See Automatic Maintenance .
Period	Specify how often Vulnerability Scan needs to be started during automatic maintenance. Enter the desired number of days.
Deadline	Specify when Windows must start Vulnerability Scan during emergency automatic maintenance, if Vulnerability Scan did not complete during regular automatic maintenance. Enter the desired number of days. This value must be greater than the <i>Period</i> value.
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 will start.
Automatic Patching	
Patch Level	Patches are installed automatically when vulnerabilities are detected. Select one of the following: <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. Automatic patching may require the endpoint to reboot.
Exclusions	
Exempt Application Vulnerabilities Requiring Manual Update from Vulnerability Compliance Check	All applications that require the endpoint user to manually patch vulnerabilities are excluded from vulnerability compliance check. This option does not exclude applications from vulnerability scanning.
Exclude Selected Applications from Vulnerability Compliance Check	In the <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.

Configuration	Description
	<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.</p> <p>Applications on the list are not excluded from vulnerability scanning.</p>
Disable Automatic Patching for These Applications	Disable automatic patching for the applications excluded from vulnerability compliance check.

System Settings

The majority of these configuration options are only available for Windows, macOS, and Linux profiles. The table indicates which options are available for Chromebook profiles, such as *Upload Logs to FortiAnalyzer/FortiManager*.

Some options are only available when *Advanced* view is enabled.

Configuration	Description
UI	Specify how the FortiClient user interface appears when installed on endpoints.
Require Password to Disconnect from EMS	Turn on password lock for FortiClient.
Password	Enter a password. The endpoint user must enter this password to disconnect FortiClient from FortiClient EMS.
Do Not Allow User to Back Up Configuration	Disallow users from backing up the FortiClient configuration.
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 Compliance Verification on page 179 .

Configuration	Description
Language	<p>Configure the language that FortiClient uses. By default, FortiClient uses the system operating language. Select one of the following:</p> <ul style="list-style-type: none"> • os-default (System operating language, selected by default) • zh-tw (Taiwanese Mandarin) • cs-cz (Czech) • de-de (German) • en-us (United States English) • fr-fr (French) • hu-hu (Hungarian) • ru-ru (Russian) • ja-jp (Japanese) • ko-kr (Korean) • pt-br (Brazilian Portuguese) • sk-sk (Slovak) • es-es (Spanish) • zh-cn (Chinese (Simplified)) • et-ee (Estonian) • lv-lv (Latvian) • lt-lt (Lithuanian) • fi-fi (Finnish) • sv-se (Swedish) • da-dk (Danish) • pl-pl (Portuguese (Portugal)) • nb-no (Norwegian) • fr-ca (Canadian French)
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: The system becomes unstable. • Alert: Immediate action is required. • Critical: Functionality is affected. • Error: An error condition exists and may affect functionality. • Warning: Functionality could be affected. • Notice: Information about normal events. • Info: General information about system operations. • Debug: Debug FortiClient.

Configuration	Description
Features	<p>Select features to generate logs for:</p> <ul style="list-style-type: none"> • AntiVirus • Application Firewall • Telemetry • FSSOMA • Proxy • IPsec VPN • AntiExploit • SSL VPN • Update • Vulnerability • Web Filter • Sandbox
Client-Based Logging When On-Fabric	Include local log messages when FortiClient is on-fabric. See On-fabric Detection Rules on page 172 .
Upload Logs to FortiAnalyzer/FortiManager	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.
Upload UTM Logs	Upload unified threat management logs to FortiAnalyzer or FortiManager.
Upload Vulnerability Logs	Upload vulnerability logs to FortiAnalyzer or FortiManager.
Upload Event Logs	Upload event logs to FortiAnalyzer or FortiManager.
Send Software Inventory	EMS sends FortiClient software inventory to FortiAnalyzer or FortiManager.
IP Address/Hostname	Enter the FortiAnalyzer IP address or hostname/FQDN. With Chromebook profiles, use the format <i>https://FAZ-IP:port/logging</i> . If using a port other than the default, use <address>:<port>.
SSL Enabled	Enable SSL.
Upload Schedule	Configure the upload schedule in minutes.
Log Generation Timeout	Configure the log generation timeout in seconds.
Log Retention	Configure the duration of time to retain logs in days.
Proxy	
Use Proxy for Updates	Access FortiGuard using the configured proxy.

Configuration	Description
Connect to FDN Directly If Proxy Is Offline	Connect to FDN directly if proxy is offline.
Use Proxy for Virus Submission	Use the configured proxy to submit viruses to FortiGuard.
Type	Configure the type. Options include: <ul style="list-style-type: none"> • http • socks4 • socks5
IP Address/Hostname	Enter the proxy server's IP address/hostname.
Port	Enter the proxy server's port number. The port range is from 1 to 65535.
Username	If the proxy requires authentication, enter the username. Enter the encrypted or non-encrypted username.
Password	If the proxy requires authentication, enter the password. Enter the encrypted or non-encrypted username. Enable <i>Show Password</i> to show the password in plain text.
Update	Specify whether to use FortiManager or Micro-FortiGuard Server for FortiClient to update FortiClient on endpoints.
Use FortiManager for Client Signature Update	Enable FortiClient EMS to obtain AV signatures from the FortiManager or Micro-FortiGuard Server for FortiClient 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 or Micro-FortiGuard Server for FortiClient is not available.
FortiGuard Server Location	Configure the FortiGuard server location. If <i>FortiGuard Anycast</i> is selected for the <i>Server</i> field, you can select from global, U.S., or Europe. If <i>FortiGuard</i> is selected for the <i>Server</i> field, you can select from global or U.S. When <i>Global</i> is selected, FortiClient uses the closest FortiGuard server. FortiClient connects to FortiGuard to query for AV and vulnerability scan engine and signature updates. The URLs connected to for each server location are as follows:

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

Configuration	Description
Last Port	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. The available port range is 65535 to 10000.
Endpoint Control	
Show Bubble Notifications	Show bubble notifications when FortiClient installs new policies on endpoints.
Log off When User Logs Out of Windows	Log off FortiClient when the endpoint user logs out of Windows. Turn off to remain logged in.
Disable Unregister	Forbid users from disconnecting FortiClient from FortiClient EMS.
Disable FortiGate Switch	Disable FortiGate switch. When the FortiGate switch is disabled, the following occurs: <ul style="list-style-type: none"> FortiClient does not probe the default gateway. FortiClient does not automatically connect to the default gateway. FortiClient ignores FortiGate broadcasts. The discovered list displays only predefined FortiGates, if discovered.
Hide Compliance Enforcement Feature Message from Compliance Tab	Hide the compliance enforcement feature message from the <i>Compliance & Telemetry</i> tab. This option is only enforced on FortiClients connected to FortiClient EMS. This option does not apply to monitored clients. This option only applies for endpoints running FortiClient versions earlier than 6.2.0.
On-Fabric Subnets	Turn on to enable on-fabric subnets. FortiClient determines on-/off-fabric status using Determining on-fabric/off-fabric status on page 174 . 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 172 .
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 106 .

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

XML Configuration

Configuration	Description
XML editor	Configure the endpoint profile using the XML editor. See the FortiClient XML Reference Guide .

Deployment

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 158](#).
2. Prepare Windows endpoints for FortiClient. See [Preparing Windows endpoints for FortiClient deployment on page 160](#).
3. Add the AD server to FortiClient EMS. See [Adding endpoints using an AD domain server on page 72](#).
4. Add a profile and configure FortiClient features in the profile. See [Creating a profile to configure FortiClient on page 117](#).
5. Create a deployment package with the profile in step 4 configured. See [Adding a FortiClient deployment package on page 165](#).
6. Create a deployment configuration. See [Creating a deployment configuration on page 161](#).

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.

Preparing the AD server for deployment

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

1. [Configuring a group policy on the AD server on page 159](#)
2. [Configuring required Windows services on page 159](#)
3. [Creating deployment rules for Windows firewall on page 159](#)
4. [Configuring Windows firewall domain profile settings on page 159](#)

Configuring a group policy on the AD server

To configure a group policy on the AD server:

1. On the 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 OUs in the AD server that contains the endpoint computers on which FortiClient will be deployed.

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 the *File and Printer Sharing (SMB-In)* checkbox 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's 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 steps listed in step 2 above 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 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)

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 *Manage Installers > Deployment Packages*.



When adding endpoints using an AD domain server, FortiClient EMS automatically resolves endpoint IP addresses during initial deployment of FortiClient. 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

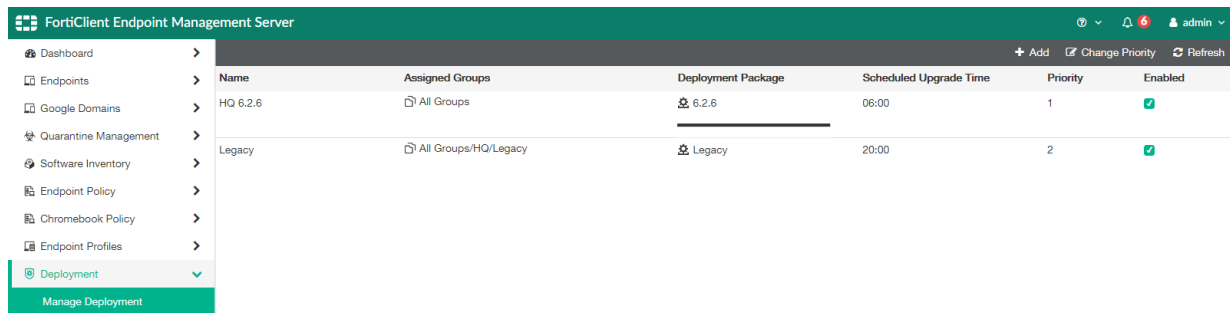
An endpoint may be eligible for multiple deployment configurations. When an endpoint is eligible for multiple endpoint deployment configurations, two factors determine which configuration EMS applies to the endpoint:

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:

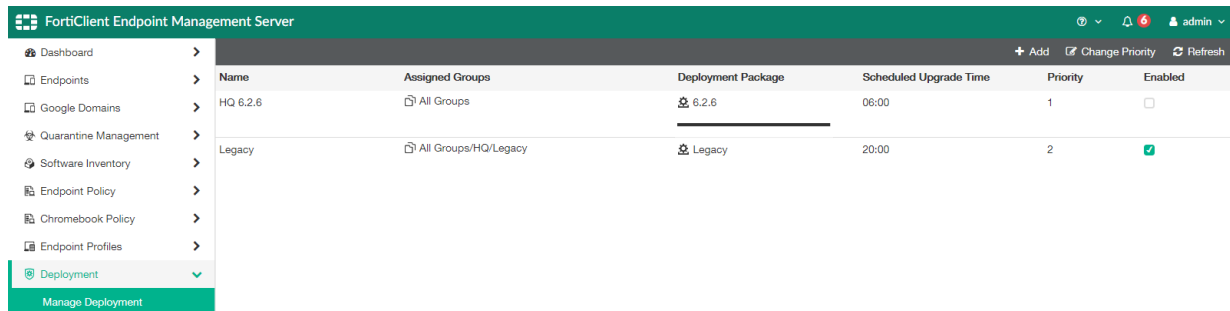
1. Go to *Deployment > Manage Deployment*.
2. Click *Change Priority*.
3. Click and hold the configuration, then drag to the desired position.

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.



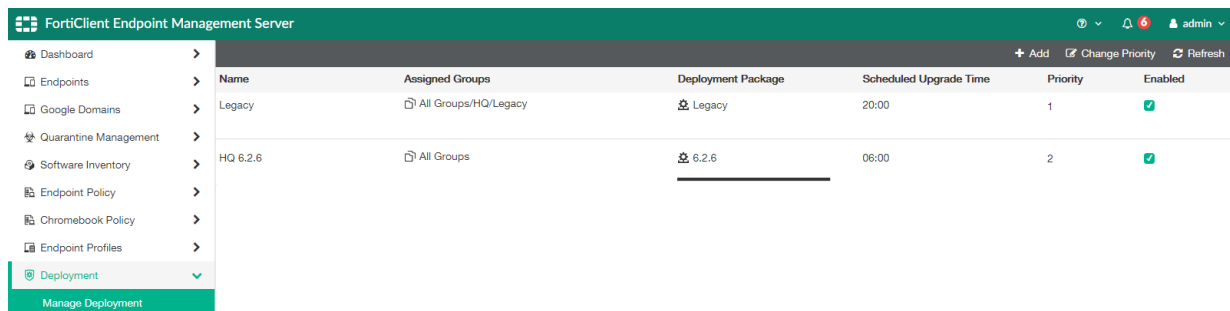
Name	Assigned Groups	Deployment Package	Scheduled Upgrade Time	Priority	Enabled
HQ 6.2.6	All Groups	6.2.6	06:00	1	<input checked="" type="checkbox"/>
Legacy	All Groups/HQ/Legacy	Legacy	20:00	2	<input checked="" type="checkbox"/>

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



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.



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 to be deployed. The prompt requests the user to do one of the following:

1. *Upgrade Now*: If you select this option, FortiClient performs the upgrade and automatically restarts your computer.
2. *Upgrade 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.
3. *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 described in [Installer ID group assignment rules on page 96](#), 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 165](#).
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 98](#).
3. Install FortiClient on endpoints using the following CLI commands:

Installer	CLI command
.msi	<code>msiexec /i forticlient.msi GROUP_TAG=<installer_ID></code>
.exe	<code>FortiClientSetup.exe /v"GROUP_TAG=<installer_ID>"</code>

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.exe /v"GROUP_TAG=<HR>"
FortiClientSetup.exe /v"GROUP_TAG=<Marketing>"
FortiClientSetup.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).

Managing installers

Deployment Packages

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.

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 *Manage Installers > Deployment Packages*.
2. Click *Add*.
3. On the *Version* tab, set the following options:

Installer Type	Use an official or custom FortiClient installer. See FortiClient installers on page 168 .
Release	Select the FortiClient release version to install.
Patch	Select the specific FortiClient patch version to install.
Keep updated to the latest patch	Enable FortiClient to automatically update to the latest patch release when FortiClient is installed on an endpoint.

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 217](#).

Endpoint Telemetry	Enabled by default and cannot be disabled. Installs FortiClient with Telemetry enabled.
Vulnerability Scan	Enabled by default and cannot be disabled. Installs FortiClient with Vulnerability Scan enabled.
Secure Access Architecture Components	<p>Install FortiClient with SSL and IPsec VPN enabled. Disable to omit SSL and IPsec VPN support from the FortiClient deployment package.</p> <p>If you enable this feature for a deployment package and include a preconfigured VPN tunnel in the included endpoint profile, users who use this deployment package to install FortiClient can connect to this preconfigured VPN tunnel for three days after their initial FortiClient installation. This is useful for remote users, as it allows them to connect to the corporate network to activate their FortiClient license. If the user does not activate their FortiClient license within the three days, all FortiClient features, including VPN, stop working on their device.</p> <p>See VPN on page 143 for details on configuring a VPN tunnel.</p>
Advanced Persistent Threat (APT) Components	Install FortiClient with APT components enabled. Disable to omit APT components from the FortiClient deployment package. Includes FortiSandbox detection and quarantine features.
Additional Security Features	<p>Enable any of the following features:</p> <ul style="list-style-type: none"> • AntiVirus • Web Filtering • Application Firewall • Single Sign-On mobility agent • Cloud Based Malware Outbreak Detection. This feature is available for FortiClient 6.2.0 and later versions. <p>Disable to exclude features from the FortiClient deployment package.</p>

If you enable a feature in the deployment package that is disabled in [Feature Select on page 217](#), 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 automatic registration	Configure FortiClient to automatically connect Telemetry to FortiClient EMS after FortiClient installs on the endpoint. Disable to turn off this feature and require endpoint users to manually connect Telemetry to FortiClient EMS.
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 96](#).

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 164](#).

Enable Endpoint Profile

Select an endpoint profile to include in the installer. EMS applies the 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, or if users require VPN connection to connect to EMS.






- Click *Next*. The *Telemetry* tab displays the hostname and IP address of the FortiClient EMS server, which will manage FortiClient once it is installed on the endpoint. Also configure the following option:

Enable telemetry connection to Security Fabric (FortiGate)

Enable this option, and select the name of the gateway list to use. The gateway list defines the IP address for the FortiGate.

If you have not created a gateway list, this option is not available. See [Creating a Telemetry server list on page 176](#).

- Click *Finish*. The FortiClient deployment package is added to FortiClient EMS and displays on the *Manage Installers > Deployment Packages* pane. The deployment package may include .exe (32-bit and 64-bit), .msi, and .dmg files depending on the configuration. The following shows an example of a deployment package that includes .exe, .msi, and .dmg files. The end user can download these files to install FortiClient on their machine with the desired configuration.

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



If the *Sign software packages* option is enabled in *System Settings > Server*, Windows deployment packages display as being from the publisher specified in the certificate file. See [Configuring Server settings on page 204](#).

Viewing deployment packages

After you add FortiClient deployment packages to FortiClient EMS, you can view them on the *Manage Installers > Deployment Packages* 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
- Configured Telemetry gateway list
- Connection to FortiGate and/or 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 *Manage Installers > Deployment Packages*.
2. Click the desired deployment package, then click *Delete*. A confirmation dialog displays.
3. Click *Yes*. FortiClient EMS deletes the FortiClient deployment package.

FortiClient installers

Manage Installers > FortiClient Installers displays FortiClient installers available from FortiGuard and uploaded custom FortiClient installers. These installers are available for selection when creating a FortiClient deployment package. See [Adding a FortiClient deployment package on page 165](#).

FortiClient EMS automatically connects to FortiGuard to provide access to FortiClient installers that you can use with FortiClient EMS profiles. If a connection to FDN is not available, you must manually download FortiClient installers to use with FortiClient EMS.

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.

Adding a custom FortiClient installer

You can create a custom FortiClient installer and add it to FortiClient EMS. Alternately, if a connection to FDN is not available, you may need to manually download a FortiClient installer and add it to FortiClient EMS.

All uploaded Windows installers must be .msi or .zip files. All uploaded macOS installers must be .dmg files.



You cannot upload the FortiClient free VPN client installer into the *Add FortiClient Installer* dialog.

To add a custom FortiClient installer:

1. Download a FortiClient installer. See [FortiClient installers on page 168](#). You can also upload a previously customized installer.
2. Upload the custom installation files:
 - a. Go to *Manage Installers > FortiClient Installers*.
 - b. Click *Add*. The *Add FortiClient Installer* dialog displays.
 - c. Set the following options:

Name	Enter a name for the set of installation files.
Upload Windows Installers	Upload FortiClient installers for the Windows operating system.
Windows 64-Bit Installer (ZIP or MSI)	Click the <i>Browse</i> button to locate and select a custom 64-bit installer for the Windows operating system.
Windows 32-Bit Installer (ZIP or MSI)	Click the <i>Browse</i> button to locate and select a custom 32-bit installer for the Windows operating system.
Upload Mac Installer	Upload a FortiClient installer for the macOS operating system.
Mac Installer (DMG)	Click the <i>Browse</i> button to locate and select a custom installer for the macOS operating system.

- d. Click *Upload*. The custom installers are uploaded to FortiClient EMS.

Viewing installers

After you add FortiClient installers to FortiClient EMS, you can view them in *Manage Installers > FortiClient Installers*.

Manage Installers > FortiClient Installers displays available installers. By default, this page lists installers from FortiGuard first, then uploaded installers. The following information displays for each installer:

Name	For installers from FortiGuard, the name refers to the installer's FortiClient version. For uploaded installers, you configure the name when uploading the installer. You cannot edit the name at a later time. See Adding a custom FortiClient installer on page 169 .
Versions	FortiClient release and patch number for the installer.

If an installer from FortiGuard only has FortiClient (Windows) available, this means there was no FortiClient (macOS) release for that version.

Type

Displays one of the following:

- *Official* for installers from FortiGuard
- *Custom* for uploaded installers

Policy Components

You can manage CA certificates and on-fabric detection rules under *Policy Components*.

CA Certificates

Uploading a certificate

You can locally upload a CA certificate.

To upload a CA certificate:

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

Importing a certificate

To import a certificate:

1. Go to *Policy Components > Manage 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 109](#).



On-fabric detection rules do not apply to endpoints running FortiClient 6.2.1 and earlier versions. Endpoints running FortiClient 6.2.1 and earlier versions determine on-/off-fabric status as [Determining on-fabric/off-fabric status on page 174](#) describes.

To add an on-fabric detection rule set:

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

Determining on-fabric/off-fabric status

This section only applies to endpoints running FortiClient 6.2.1 and earlier versions.

There are two settings in EMS that affect FortiClient on-fabric/off-fabric status:

- *DHCP on-fabric/off-fabric*
- On-fabric detection rules configured for the endpoint's assigned policy.

The table shows how the *DHCP on-fabric/off-fabric* setting, on-fabric detection rules, and Option 224 serial number affect the endpoint's on-fabric/off-fabric status. *DHCP on-fabric/off-fabric* only applies when the endpoint is connected to EMS. You can configure Option 224 with any Fortinet device's serial number. EMS assumes that FortiClient is behind a FortiGate and on-fabric with that FortiGate.

DHCP on-fabric/off-fabric	On-fabric detection rules	Option 224 serial number	Resulting endpoint status
Disabled	Not configured	N/A	Endpoint is on-fabric when registered to EMS.
Enabled	Not configured	Not configured	Endpoint is off-fabric when registered to EMS.
Enabled	Not configured	Configured	On-fabric Since Option 224 is configured with a Fortinet device's serial number, EMS assumes FortiClient is on-fabric with that FortiGate.
N/A	Enabled, with subnet configured. Endpoint IP address is in the configured subnet.	N/A	On-fabric The endpoint is inside the on-fabric networks configured in the applied endpoint policy's on-fabric detection rules.

DHCP on-fabric/off-fabric	On-fabric detection rules	Option 224 serial number	Resulting endpoint status
N/A	Enabled, with subnet configured. Endpoint IP address is not in the configured subnet.	N/A	Off-fabric The endpoint is outside the on-fabric networks configured in the applied endpoint policy's on-fabric detection rules.

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.

Telemetry Server Lists

You can use a Telemetry server list to specify what IP addresses or FQDNs and ports endpoints can use to connect FortiClient Telemetry to FortiClient EMS, or EMS and FortiOS. You can create one or more Telemetry server lists and configure them as part of endpoint policies to assign them to domains or workgroups.

If FortiClient is installed using a deployment package configured with an EMS IP address or FortiClient Cloud invitation code, FortiClient automatically connects to that EMS or FortiClient Cloud after installation. If this is not the case, FortiClient uses the assigned Telemetry server list to try and connect FortiClient Telemetry to EMS or EMS and FortiOS.

Even if the endpoint is already connected to an EMS or an EMS and FortiOS, you can still assign a Telemetry server list to endpoints as part of an endpoint policy. You can also update existing Telemetry server lists as required. EMS pushes the updates to endpoints with the next Telemetry communication.

FortiClient 6.4.0 and later versions cannot directly connect Telemetry to FortiOS. FortiClient 6.4.0 only connects Telemetry to EMS, which then sends FortiClient data to FortiOS. Only endpoints with FortiClient versions older than 6.4.0 installed can connect Telemetry directly to FortiOS.

Creating a Telemetry server list

You can create a Telemetry server list that contains IP addresses for one or multiple EMS servers and FortiGates. FortiClient searches for IP addresses in its subnet in the Telemetry server list and connects to the EMS and FortiGate in the list that is in the same subnet as the host system.

If FortiClient cannot find any EMS or FortiGates in its subnet, it attempts to connect to the first reachable EMS and FortiGate in the list, starting from the top. FortiClient maintains the list order as configured in the Telemetry server list.

FortiClient 6.4.0 and later versions cannot directly connect Telemetry to FortiOS. FortiClient 6.4.0 only connects Telemetry to EMS, which then sends FortiClient data to FortiOS. Only endpoints with FortiClient versions older than 6.4.0 installed can connect Telemetry directly to FortiOS.

To create a Telemetry server list:

1. Go to *Telemetry Server Lists > Manage Telemetry Server Lists*.
2. Click the *Add* button.

3. Configure the following:

Name	Enter the list name.
Comment	Enter additional comments (optional).
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.
New connection key	Enter the connection key.
Confirm new connection key	Reenter the connection key to confirm.
Managed by EMS	Select an option from the dropdown list. Users can configure this IP address in <i>System Settings > Server</i> .
Notify FortiGate	Enter the FortiGates IP address(es) or hostname(s). You can also use an FQDN. Press the <i>Enter</i> key to add additional entries. This option is only available if you enable <i>Show FortiGate Server List</i> in <i>System Settings > Server</i> .

4. Click **Save**.

If you later delete a Telemetry server list, an endpoint that had that Telemetry server list assigned disconnects from the FortiGate configured in that Telemetry server list, but maintains its connection to EMS.

If you disable *Show FortiGate Server List* in *System Settings > Server*, even if you do not delete the Telemetry server list, an endpoint that had that Telemetry server list assigned disconnects from the FortiGate configured in that Telemetry server list.

Exporting a Telemetry gateway list to XML

After you create and save a Telemetry gateway list, the *Export* button displays, and you can export the list to a configuration file in XML format.

To export a Telemetry gateway list to XML:

1. Go to *Telemetry Server Lists > Manage Telemetry Server Lists*.
2. Click a list.
3. Click the *Export* button. EMS downloads a `gateway_list_<list_name>.conf` file to your computer.

Following is an example of the XML:

```
<?xml version="1.0" encoding="utf-8"?>
<forticlient_configuration>
  <endpoint_control>
    <fortigates>
      <fortigate>
        <name>FortiGate</name>
        <registration_password></registration_password>
```

```
<addresses>1.1.1.1:8013</addresses>
</fortigate>
</fortigates>
<notification_server>
  <registration_password></registration_password>
  <address>1.1.1.1:8013</address>
</notification_server>
</endpoint_control>
</forticlient_configuration>
```

Viewing Telemetry server lists

After you create Telemetry server lists, EMS lists them under *Telemetry Server Lists* in the left pane. You can view the Telemetry server lists and their settings.

Viewing assigned Telemetry server lists

To view assigned Telemetry server lists:

1. Go to *Endpoints* and go to the desired endpoint.
2. View the *Configuration* column. The assigned Telemetry server list displays.

Compliance Verification

You can create compliance verification rules for Windows, macOS, and Linux endpoints based on their OS versions, logged in domains, running processes, and other criteria. EMS uses the rules to dynamically group endpoints. FortiOS 6.2.0 and later versions can use the dynamic endpoint groups to build dynamic policy rules.

Compliance Verification Rules

You can create, edit, and delete compliance verification rules for Windows, macOS, and Linux endpoints. You can also view and manage the tags used to dynamically group endpoints.

The following occurs when using compliance verification rules with EMS and FortiClient:

1. EMS sends compliance verification rules to endpoints via Telemetry communication.
2. FortiClient checks endpoints using the provided rules and sends the results to EMS.
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 *Compliance Verification > Host Tag Monitor*. See [Host Tag Monitor on page 184](#).

Adding a compliance verification rule set

To add a compliance verification rule set:

1. Go to *Compliance Verification > Compliance Verification 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 rule:
 - a. For *OS*, select *Windows*, *Mac*, or *Linux*. 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 [Compliance verification rule types on page 181](#) for descriptions of the rule types.
 - c. Click *Save*.
8. Configure additional rules as desired by repeating steps 6-7. Click *Save*.



For some rule types, such as the Running Process rule type, the endpoint must satisfy all conditions to satisfy the rule. There may be situations where you want endpoints that satisfy different conditions to be in the same dynamic group. Consider that you want endpoints that are running Process A or Process B in the "RP" dynamic group. In this case, you can create two rule sets: one for endpoints running Process A and another rule for endpoints running Process B. You can configure both rule sets to apply the "RP" tag to place endpoints running either process in the same dynamic group.

Editing a compliance verification rule set

To edit a compliance verification rule:

1. Go to *Compliance Verification > Compliance Verification Rules*.
2. Select the compliance verification rule.
3. Click *Edit*.
4. Edit as desired.
5. Click *Save*.

Deleting a compliance verification rule

To delete a compliance verification rule:

1. Go to *Compliance Verification > Compliance Verification Rules*.
2. Click the desired compliance verification rule.
3. Click *Delete*.
4. In the confirmation dialog, click *Yes*.

Managing tags

The *Manage Tags* window displays all configured tags and the rules that apply that tag to endpoints that satisfy the rule. You can delete tags that do not have any rules attached.

To manage tags:

1. Go to *Compliance Verification > Compliance Verification Rules*.
2. Click *Manage Tags*. You can see the list of tags and the associated rules. In the example, the BYOD and Local User tags both have two rules attached.

Manage Tags	
Tag Name	Rules
BYOD	Windows File check Windows Registry Key check
Local User	Windows Domain check Mac Domain check
Server 2012	
3 entries loaded	

3. To delete a tag with no rules attached, click the X beside the corresponding tag. In this example, the Server 2012 tag does not have any rules attached.
4. In the confirmation dialog, click **Yes**.

Compliance verification rule types

The following table describes compliance verification rule types and the OSes that they are available for. For all rule types, you can configure multiple conditions using the + button.

Rule type	OS	Description
AD Group	<ul style="list-style-type: none"> Windows macOS 	<p>From the <i>AD Group</i> dropdown list, select the desired 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 also 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 72.</p> <p>Only FortiClient 6.2.2+ endpoints support this rule type.</p>
AntiVirus Software	<ul style="list-style-type: none"> Windows macOS Linux 	<p>From the <i>AV Software</i> dropdown list, select the desired conditions. You can require that an endpoint have AV software installed and running and that the AV signature is up-to-date. You can also use the NOT option for the rule to require that the endpoint does not have AV software installed or running or that the AV signature is not up-to-date. This rule applies for FortiClient AV and third-party AV software that registers to the Windows Security Center. The third-party software notifies the Windows Security Center of the status of its signatures. FortiClient queries the Windows Security Center to determine what third party AV software is installed and if the software reports signatures as up-to-date.</p> <p>The endpoint must satisfy all configured conditions to satisfy this rule.</p> <p>Only FortiClient 6.2.2+ endpoints support this rule type.</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>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 	<p>EMS considers the endpoint as satisfying the rule if the endpoint has FortiClient installed and Telemetry connected to EMS.</p>

Rule type	OS	Description
	<ul style="list-style-type: none"> Android 	
File	<ul style="list-style-type: none"> Windows macOS Linux 	<p>In the <i>File</i> field, enter the file path. You can also use the NOT option to indicate that the rule requires that a certain file is not present on the endpoint.</p> <p>The endpoint must satisfy all configured conditions to satisfy this rule. For example, if the rule is configured to require file A, file B, and NOT file C, then the endpoint must have both files A and B and not file C.</p>
Logged in Domain	<ul style="list-style-type: none"> Windows macOS 	<p>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.</p>
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>
Registry Key	<ul style="list-style-type: none"> Windows 	<p>In the <i>Registry Key</i> field, enter the registry key or registry data value. End the path with \ to indicate a registry key, or without \ to indicate a registry data value. You can also use the NOT option to indicate that the rule requires that a certain registry key or data value 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 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> <p>The following shows examples of registry key values:</p> <p>\HKEY...\Key\ \HKEY...\Key HKEY...\Key\ HKEY...\Key \HKEY...\Key\String\ \HKEY...\Key\String HKEY...\Key\String\ HKEY...\Key\String</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>

Rule type	OS	Description
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>
Vulnerable Devices	<ul style="list-style-type: none"> Windows macOS Linux 	<p>From the <i>Severity Level</i> dropdown list, select the desired vulnerability severity level. If the rule is configured for multiple severity levels, EMS considers the endpoint as satisfying the rule if it has a vulnerability of one of the configured severity levels or higher.</p>
Security	<ul style="list-style-type: none"> macOS 	<p>Select the checkbox to require that File Vault is enabled on the endpoint. You can also use the NOT option to indicate that the rule requires that File Vault is disabled on the endpoint.</p>
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 Windows Defender, Bitlocker Disk Encryption, Exploit Guard, Application Guard, and/or Windows Firewall enabled. You can also use the NOT option for the rule to require that the endpoint have Windows Defender, Bitlocker Disk Encryption, Exploit Guard, Application Guard, and/or Windows firewall disabled.</p> <p>The endpoint must satisfy all configured conditions to satisfy this rule.</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. <i>Specified</i>: enter a specific Google, LinkedIn, or Salesforce account. For example, you can enter joanexample@gmail.com to configure the rule to apply specifically to only that Google account. You can specify multiple social network accounts. <p>EMS considers the endpoint as satisfying the rule if it satisfies one of the conditions.</p> <p>You can also use the NOT option for the rule to require that the endpoint user has not manually entered user details or logged in to a social network account to allow FortiClient to obtain user details.</p> <p>Only FortiClient 6.2.2+ endpoints support this rule type.</p> <p>FortiClient iOS does not support social network login with LinkedIn or Salesforce. FortiClient Android does not support social network login with Salesforce.</p>

Host Tag Monitor

You can view all dynamic endpoint groups in *Compliance Verification > Host Tag Monitor*. EMS creates dynamic endpoint groups based on the tag configured for each rule.

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.
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 compliance verification 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.

EMS supports this feature with FortiOS 6.4 and 6.2. Configuration differs depending on the FortiOS version that you use:

- [Configuring FortiOS 6.4 dynamic policies using EMS dynamic endpoint groups on page 185](#)
- [Configuring FortiOS 6.2 dynamic policies using EMS dynamic endpoint groups on page 188](#)



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.

Configuring FortiOS 6.4 dynamic policies using EMS dynamic endpoint groups

FortiOS 6.4 uses an EMS connector to retrieve dynamic endpoint groups from EMS. The following instructions only apply when using FortiOS 6.4. Configuring this feature requires the following steps:

1. [Checking prerequisites on page 185](#)
2. [Configuring the EMS connector on page 186:](#)
 - a. [Uploading certificates to EMS and FortiOS on page 186](#)
 - b. [Creating the EMS connector in FortiOS on page 186](#)
 - c. [Authorizing the FortiOS EMS connector in EMS on page 187](#)
 - d. [Verifying the FortiOS-EMS connection in FortiOS on page 187](#)
3. [Creating a dynamic firewall policy using dynamic endpoint groups from EMS on page 188](#)

Checking prerequisites

You must ensure that the following prerequisites are met before configuring this feature:

- Create compliance verification rules. See [Adding a compliance verification rule set on page 179](#).
- After FortiClient connects Telemetry to EMS, confirm that EMS dynamically groups endpoints based on the compliance verification rules. See [Host Tag Monitor on page 184](#).
- 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.

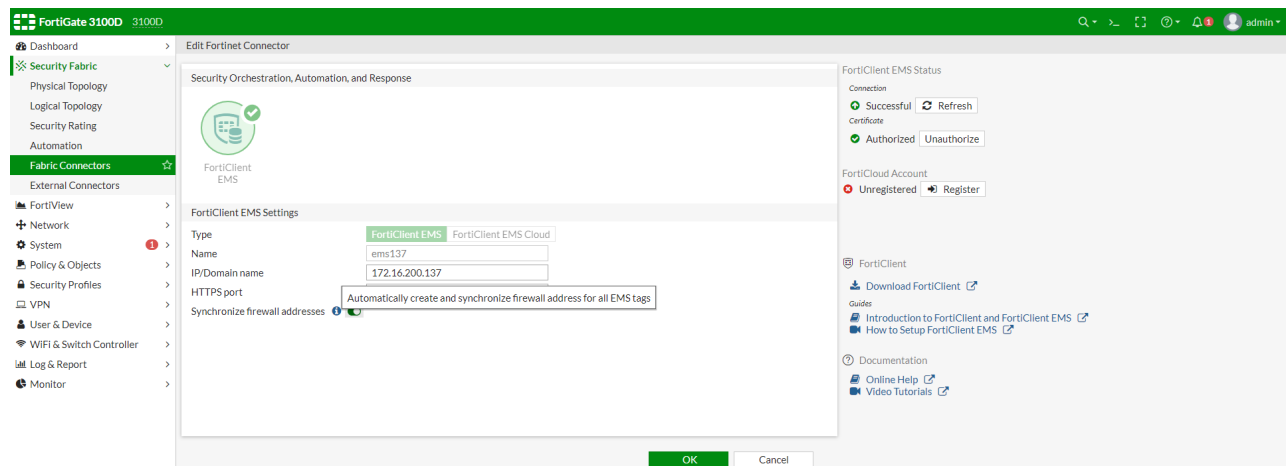
1. Upload the server certificate to EMS:
 - a. Go to *System Settings > Server*.
 - b. Under *Shared Settings*, click the *Upload new SSL certificate* button.
 - c. Upload the server certificate and private key. Click *Test*.
 - d. Click *Save*.
2. Upload the certificate to FortiOS:
 - a. Go to *System > 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.
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 200](#).

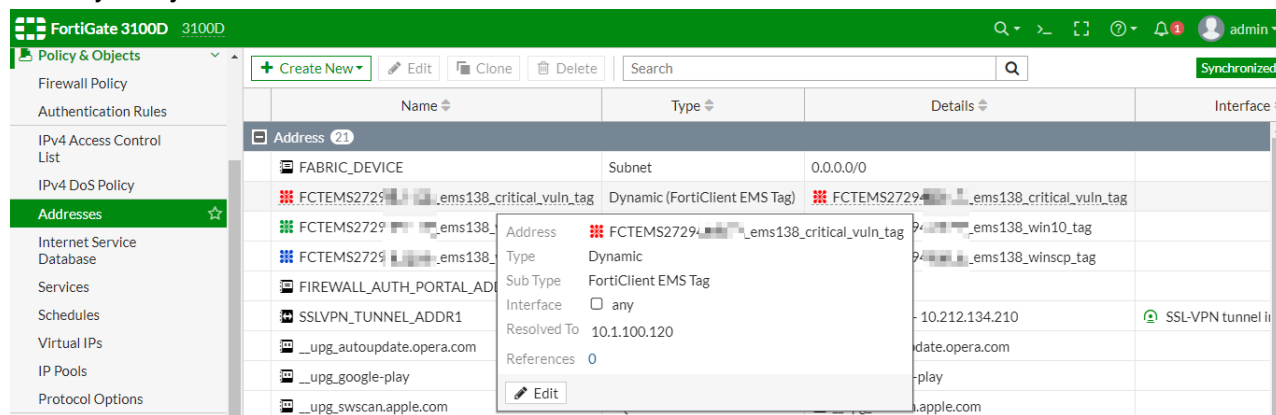
Serial Number	Last Seen IP	Last Seen Time	Certificate Subject	Certificate Expiry	Authorized
FGV...	10.100.88.101	2020-04-24 19:44:51	emailAddress=support@fortinet.com, CN=FGVM01TM19005972, OU=FortiGate, O...	2056-01-18 19:14:07	✓
FGV...	10.100.88.1	2020-04-24 19:44:59	emailAddress=support@fortinet.com, 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=FGVM01TM19005536, OU=FortiGate, O...	2056-01-18 19:14:07	✓
FGV...	10.100.88.102	2020-04-29 13:57:09	emailAddress=support@fortinet.com, CN=FGVM01TM19005743, OU=FortiGate, O...	2056-01-18 19:14:07	✓
FGV...	10.100.88.1	2020-05-15 17:24:01	emailAddress=support@fortinet.com, CN=FGVM01TM19006230, OU=FortiGate, O...	2056-01-18 19:14:07	✓
FGV...	10.100.88.101	2020-05-15 17:23:54	emailAddress=support@fortinet.com, CN=FGVM01TM19005979, OU=FortiGate, O...	2056-01-18 19:14:07	✓
FGV...	10.100.88.102	2020-05-15 17:24:01	emailAddress=support@fortinet.com, CN=FGVM01TM19005948, OU=FortiGate, O...	2056-01-18 19:14:07	✓
FGV...	10.0.11.2	2020-05-15 17:23:53	emailAddress=support@fortinet.com, CN=FGVM01TM19005419, OU=FortiGate, O...	2056-01-18 19:14:07	✓
FGV...	10.0.11.3	2020-05-15 17:23:53	emailAddress=support@fortinet.com, CN=FGVM01TM19004862, OU=FortiGate, O...	2056-01-18 19:14:07	✓
FGV...	10.100.88.1	2020-05-29 15:10:30	emailAddress=support@fortinet.com, CN=FGVM01TM19006550, OU=FortiGate, O...	2056-01-18 19:14:07	✓
FGV...	10.100.88.101	2020-05-29 15:10:35	emailAddress=support@fortinet.com, CN=FGVM01TM19005722, OU=FortiGate, O...	2056-01-18 19:14:07	✓
FGV...	10.0.10.3	2020-05-29 15:10:48	emailAddress=support@fortinet.com, CN=FGVM01TM19004325, OU=FortiGate, O...	2056-01-18 19:14:07	✓
FGV...	10.100.88.102	2020-05-29 15:10:43	emailAddress=support@fortinet.com, CN=FGVM01TM19005157, OU=FortiGate, O...	2056-01-18 19:14:07	✓
FGV...	10.0.11.2	2020-05-29 15:10:43	emailAddress=support@fortinet.com, CN=FGVM01TM19004965, OU=FortiGate, O...	2056-01-18 19:14:07	✓

Verifying the FortiOS-EMS connection in FortiOS

To verify the FortiOS-EMS connection in FortiOS:

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

to **Policy & Objects > Addresses** to view the addresses.



Creating a dynamic firewall policy using dynamic endpoint groups from EMS

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

1. In FortiOS, go to **Policy & Objects > Firewall Policy**. Click **Create New**.
2. In the **Source** field, click **+**. The **Select Entries** pane appears. On the **Address** tab, select the address based on the desired dynamic endpoint group from EMS.
3. Configure other options as desired. Click **OK**.
4. Go to **Policy & Objects > Firewall Policy** to ensure the policy was created. FortiOS updates this policy when it receives updates from EMS.

Configuring FortiOS 6.2 dynamic policies using EMS dynamic endpoint groups

FortiOS 6.2 uses the FSSO protocol to retrieve dynamic endpoint groups from EMS. The following instructions only apply when using FortiOS 6.2.

The following configuration is necessary for this feature:

1. In FortiClient EMS, create compliance verification rules. See [Adding a compliance verification rule set on page 179](#).
2. After Telemetry communication has occurred between EMS and FortiClient, ensure that EMS has dynamically grouped endpoints based on the compliance verification rules. See [Host Tag Monitor on page 184](#).
3. In FortiOS, create the EMS Fabric connector.
4. Configure FSSO settings.
5. In FortiOS, create a user group based on EMS dynamic endpoint groups.
6. In FortiOS, create a dynamic firewall policy for the user group.

EMS can be connected to a maximum of three FortiGates at a time via the FSSO protocol.

To create the EMS Fabric connector in FortiOS:

You can create the EMS Fabric connector in the FortiOS GUI or CLI. If desired, you can optionally configure the Fabric connector with an SSL certificate and a password for FSSO. If configured, you must configure the same certificate and password in EMS to ensure a successful connection.

1. Go to *Security Fabric > Fabric Connectors*.
2. Click *Create New*, then select FortiClient EMS.
3. In the *Name* field, enter the desired name.
4. For *Type*, select FortiClient EMS.
5. In the *Primary Server IP* field, enter the EMS IP address.
6. (Optional) From the *Trusted SSL certificate* dropdown list, select the certificate.
7. (Optional) In the *Password* field, enter the desired password.
8. Click *Apply & Refresh*.

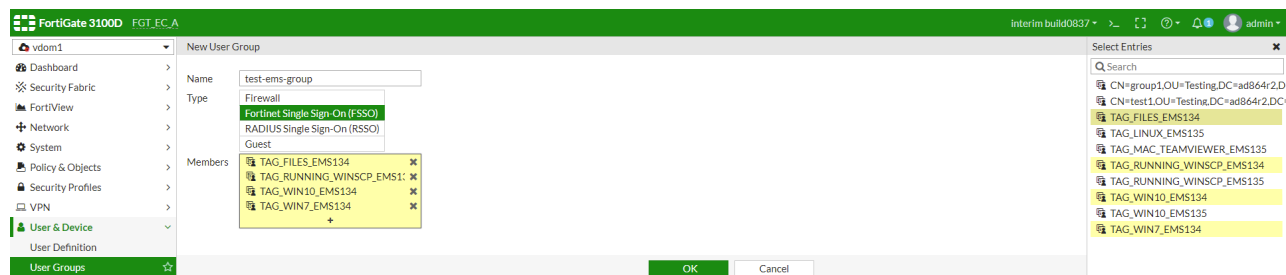
To configure EMS FSSO Settings:

If you configured a certificate and/or password in [To create the EMS Fabric connector in FortiOS: on page 188](#), you must configure the same certificate and password in EMS.

1. If you configured a certificate for the EMS Fabric connector in FortiOS, do the following:
 - a. In FortiOS, go to *System > Certificates*.
 - b. Right-click the configured certificate, then select *Download*.
2. In EMS, go to *System Settings > Server*.
3. For *SSL certificate*, browse to and upload the certificate downloaded in step 1.
4. In the *Configure FSSO Password* field, enter the password.
5. Click *Save*.

To create a user group based on EMS dynamic groups:

1. In FortiOS, go to *User & Device > User Groups*. Click *Create New*.
2. In the *Name* field, enter the desired name.
3. For *Type*, select *Fortinet Single Sign-On (FSSO)*.
4. In the *Members* field, click +. The *Select Entries* pane appears. Select the dynamic endpoint groups pulled from EMS.



5. Select the desired dynamic endpoint groups. Endpoints that currently belong to this EMS dynamic endpoint group will be members of this FortiOS user group.
6. Click *OK*.

To create a dynamic firewall policy for the user group:

You can now create a dynamic firewall policy for the user group. In this example, an IPv4 policy is created for the user group.

1. In FortiOS, go to *Policy & Objects > IPv4 Policy*. Click *Create New*.
2. In the *Source* field, click +. The *Select Entries* pane appears. On the *User* tab, select the user group configured above.
3. Configure other options as desired. Click *OK*.
4. Go to *Policy & Objects > IPv4 Policy* to ensure the policy was created and applied to the desired user group. FortiOS will update this policy when it receives updates from EMS.

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
3	33	all	EMS_server_01 EMS_server_02 EMS_server_03 dns_server	always	ALL	ACCEPT	Enabled	no-inspection	UTM	3.20 GB
1	111	all	pc155_address	always	ALL	ACCEPT	Enabled	no-inspection	UTM	6.68 GB
4	44	all	pc5_address	always	ALL	ACCEPT	Enabled	no-inspection	UTM	21.37 MB

Fabric Device Monitor

On the *Fabric Device Monitor* page, you can view all FortiGates that are connected to EMS. For information on connecting a FortiGate to EMS, see [FortiOS dynamic policies using EMS dynamic endpoint groups on page 185](#).

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

EMS can be connected to a maximum of three FortiGates at a time via the FSSO protocol.

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 an AD domain configured in Adding a user server on page 198.• EMS: User accounts created in FortiClient EMS.
Role	Admin role assigned to the user. See Admin roles on page 194 .
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 193 .
Comments	Comments added when creating/configuring the user.

Configuring Windows and LDAP user accounts

You can configure Windows and LDAP users to have no access or administrator access to FortiClient EMS.

The Windows users list is derived from the host server on which FortiClient EMS is installed. If you want to add more Windows users, you must add them to the host server. The list of LDAP users is derived from those in the AD domain imported into FortiClient EMS using *Administration > User Server*. If you want to add more LDAP users, they must already exist in the AD domain configured as the user server.

1. Go to *Administration > Administrators*.
2. Click the *Add* button.
3. Under *User source*, select *Choose from LDAP/Windows users*. Click *Next*.
4. Configure the permissions:

Option	Description
User	Select the Windows/LDAP user to configure permissions for.
Role	Select the desired admin role for this user. See Admin roles on page 194 .
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.

5. 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.

Creating new user accounts

1. Go to *Administration > Administrators*.
2. Click the *Add* button.
3. Under *User source*, select *Create a new user*. Click *Next*.
4. Configure the account:

Option	Description
Username	Enter the desired username.
Role	Select the desired admin role. See Admin roles on page 194 .
Domain Access	Select or add access to a domain for the user and configure their permissions. If you choose one or more domains in the domain access field, you must select specific permissions.
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 user.

5. Click *Next*.
6. Add a password following the rules shown.
7. Click *Save*.

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 200](#).

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 one of the default admin roles in FortiClient EMS or create a new admin role to assign to an administrator account. Each admin role can include permissions from three categories: endpoint permissions, policy permissions, and settings permissions.

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 has the authority to configure user privileges and permissions. The default admin account is a Super Administrator. You cannot assign another admin role to the admin account.
Standard administrator	Includes all endpoint and policy permissions, and read-only permissions to settings permissions.
Endpoint administrator	Includes all endpoint permissions and read-only permissions to policy and settings permissions.
Read-only administrator	Includes read-only permissions to endpoint, policy, and settings permissions.
Restricted administrator	No permissions enabled.

For admin roles that are not authorized for certain tasks or devices, EMS hides or disables the related menu items, items in content pages, and buttons.

Adding an admin role

To add an admin role:

1. Go to *Administration > Admin Roles*.
2. Click *Add*.
3. In the *Name* field, enter the admin role name.
4. (Optional) In the *Description* field, enter the description.
5. Configure the permissions as desired. See [Admin role permissions reference on page 195](#).
6. Click *Save*.

Cloning an admin role

1. Go to *Administration > Admin Roles*.
2. Select the desired admin role.

3. Click *Clone*.
4. Configure settings for the cloned admin role, then click *Save*.

Deleting admin roles

1. Go to *Administration > Admin Roles*.
2. Select the desired admin role.
3. Click *Delete*.
4. In the confirmation dialog, click *Yes*.

Admin role permissions reference

The following tables list the permissions available when configuring an admin role. The tables also include a description of what the permission allows the user to do and a link to the relevant section in this guide.

Permissions that apply to Chromebook management are denoted with an asterisk (*).

Endpoint permissions

Permission	Link to description
Manage LDAPs	Manage connections to LDAP servers to import users from. See User Servers on page 198 .
Manage Google domains*	Manage connections to Google domains to decide which Chromebooks to manage. See Google Domains on page 92 .
Manage custom groups	Create, rename, and edit groups to manage endpoints. See Managing groups on page 72 .
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 85 .
Block/Unblock/Quarantine/Unquarantine/Reregister endpoints	Manage endpoint access to the network through blocking, quarantine, and registration. See Managing endpoints on page 85 .
Manage and assign endpoint policies	See Endpoint Policy on page 109 .
View group assignment rules	View group assignment rules. See Group assignment rules on page 96 .
Manage group assignment rules	Create, delete, and edit group assignment rules. See Group assignment rules on page 96 .
View endpoint filter bookmarks	View endpoint filter bookmarks. See Using bookmarks to filter the list of endpoints on page 82 .

Permission	Link to description
Manage endpoint filter bookmarks	Create, delete, and edit endpoint filter bookmarks. See Using bookmarks to filter the list of endpoints on page 82 .
View quarantine management	View lists of quarantined and allowlisted files. See Quarantine Management on page 101 .
Manage quarantine management	Allowlist and restore quarantined files and remove files from the allowlist. See Quarantine Management on page 101 .
View software inventory	See Software Inventory on page 106 .
Manage software inventory	See Software Inventory on page 106 .

Policy permissions

Permission	Link to description
View endpoint policies*	View endpoint policies. See Endpoint Policy on page 109 .
View endpoint profiles*	View endpoint profiles. See Endpoint Profiles on page 116 .
Manage endpoint profiles*	Create, delete, and edit endpoint profiles. See Endpoint Profiles on page 116 .
View host verification rules	View compliance verification rules. See Compliance Verification Rules on page 179 .
Manage host verification rules	Create, delete, and edit compliance verification rules. See Compliance Verification Rules on page 179 .
View telemetry server lists	View Telemetry server lists. Telemetry Server Lists on page 176 .
Manage telemetry server lists	Create, delete, and edit Telemetry server lists. See Telemetry Server Lists on page 176 .
View installers	View installers. Managing installers on page 165
Manage installers	Create, delete, and edit installers. See Managing installers on page 165 .
View CA certificates	View CA certificates. See Policy Components on page 171 .
Manage CA certificates	Upload, import, and delete CA certificates. See Policy Components on page 171 .

Setting permissions

Permission	Link to description
View server settings*	View <i>Server</i> settings. See Configuring Server settings on page 204
Manage server settings*	Modify <i>Server</i> settings. See Configuring Server settings on page 204 .
View FortiGuard settings	View <i>FortiGuard</i> settings. See Configuring Fortinet Services settings on page 208 .
Manage FortiGuard settings	Modify <i>FortiGuard</i> settings. See Configuring Fortinet Services settings on page 208 .
View endpoint settings	View <i>Endpoints</i> settings. See Configuring Endpoints settings on page 209 .
Manage endpoint settings	Modify <i>Endpoints</i> settings. See Configuring Endpoints settings on page 209 .
View login banner settings*	View login banner settings. See Configuring the login banner on page 209 .
Manage login banner settings*	Modify login banner settings. See Configuring the login banner on page 209 .
View alert settings*	View <i>Alerts</i> settings. See Alerts on page 212 .
Manage alert settings*	Modify <i>Alerts</i> settings. See Alerts on page 212 .
View custom message settings	View endpoint quarantine message settings. See Customizing the endpoint quarantine message on page 215 .
Manage custom message settings	Modify endpoint quarantine message settings. See Customizing the endpoint quarantine message on page 215 .

User Servers

You can add multiple remote user servers to EMS. This allows you to add users defined in different remote servers as EMS administrators.

Adding a user server

To add a user server:

1. Go *Administration > User Servers*. Click *Add*. The settings display.
2. Configure the following options:

IP address/Hostname	Enter the user server's IP address or name.
Port	Enter the port for EMS to use to connect to the user server.
Distinguished name	Enter the user server's 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.
Sync every	Configure the synchronization schedule between the user server and EMS.

3. Click *Test* to check the LDAP server settings.
4. Click *Save*.

Editing a user server

To edit a user server:

1. Go to *Administration > User Servers*.
2. Select the user server.
3. Click *Edit*.
4. Edit as desired.
5. Click *Save*.

Deleting a user server

To delete a user server:

When you delete a domain, all users added from that domain are removed from EMS.

1. Go to *Administration > User Server*.
2. Click the desired server.
3. Click *Delete*.
4. In the confirmation dialog, click *Yes*.

Viewing user servers

Go to *User Servers*. The list of configured user servers and a toolbar display in the content pane.

Domain Name	User server's domain name.
NetBIOS Name	NetBIOS name for the machine housing the user server.
User Count	Number of users that belong to the user server.
Last Sync	Time of last sync between FortiClient EMS and the user server.
Sync Every	Synchronization schedule in minutes.
Address	User server's IP address.
Distinguished Name	User server's DN.
Username	Username used to connect to the user server.

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 193 .
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 FortiGate devices that the EMS has authorized in *Administration > Fabric Devices*. You can also deny or authorize a FortiGate.

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	

To change the FortiGate authorization status:

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

Database management



EMS cannot create or restore database backups when using a remote SQL database server.

Backing up the database

To back up the database:

1. Go to *Administration > Back up Database*.
2. Set the following options:

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

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

Restoring the database

To restore the database:

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

Licenses

See [Licensing FortiClient EMS on page 34](#).

Logs

To view logs:

1. Go to *Administration > Logs*.
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.

System Settings

Configuring Server 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.

To configure Server settings:

1. Go to *System Settings > Server*.
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	Displays the IP addresses for the FortiClient EMS server. FortiClient connects to FortiClient EMS on the specified IP address. You can generate a QR code for the specified IP address. See Generating a QR code for centrally managing FortiClient (Android) and (iOS) endpoints on page 219 .
Use FQDN	Specify an FQDN for the FortiClient EMS server.
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.
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.
Certificate	Browse and upload a new SSL certificate file.

Password	Configure a new SSL password.
Show FortiGate Server List	<p>When this option is enabled, you can configure FortiGate IP addresses in a Telemetry server list to allow FortiClient to connect directly to FortiOS. FortiClient 6.4.0 and later versions cannot directly connect Telemetry to FortiOS. FortiClient 6.4.0 only connects Telemetry to EMS, which then sends FortiClient data to FortiOS. Only endpoints with FortiClient versions older than 6.4.0 installed can connect Telemetry directly to FortiOS.</p> <p>When this option is disabled, you can only configure EMS IP addresses in a Telemetry server list. See Creating a Telemetry server list on page 176.</p>
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.
Enable TLS 1.0/1.1	<p>Enable TLS 1.0 and 1.1 for file downloads.</p> <p>You must enable this option when upgrading FortiClient on a Windows 7 device via FortiClient EMS.</p>
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.
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.

4. If managing Chromebooks, enable *EMS for Chromebooks Settings*. You may need to restart FortiClient EMS after enabling this option.
5. Configure the following options under *EMS for Chromebooks Settings*. These settings are used by FortiClient EMS managing Chromebook endpoints:

Listen on port	Displays the default port for the FortiClient EMS server for Chromebooks. You can change the port by typing a new port number. The FortiClient Web Filter extension on Chromebooks connects to FortiClient EMS using the specified port number.
----------------	---

User inactivity timeout	Enter the number of hours of inactivity after which to timeout the user.
Profile update interval	Specify the profile update interval (in seconds).
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 206 .
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.

6. Configure the following options under *EMS FSSO Settings*. These settings add SSL encryption to the FSSO 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.

7. Click *Save*.

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 42](#).

To add an SSL certificate to EMS for Chromebook endpoints:

1. In FortiClient EMS, go to *System Settings > Server > 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..."/>
New SSL Password	<input type="text" value="Required"/>

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.
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.
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.
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.
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 now

Click to immediately delete all FortiClient EMS logs or alerts.

3. Click Save.

Configuring Fortinet Services settings

To configure Fortinet Services settings:

1. Go to *System Settings > Fortinet Services*.
2. Configure the following options:

FortiGuard

Server Location Configure FortiGuard server location to *Nearest* or *US*.
If you select *Nearest*, FortiClient EMS connects to the FortiGuard server whose IP address the DNS server provides.
If you select *US*, FortiClient EMS can only connect to FortiGuard servers available in the United States and does not attempt to access a FortiGuard server outside the U.S.

Use FortiManager for client software/signature updates Turn on to use FortiManager or Micro-FortiGuard Server for FortiClient for updating FortiClient software or signatures. You must specify the IP address or hostname for FortiManager or Micro-FortiGuard Server for FortiClient 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 or Micro-FortiGuard Server for FortiClient is unavailable.

FortiCloud

Region Select the FortiCloud region from the dropdown list.

Time Offset Select the FortiCloud time offset from the dropdown list.

Sync FortiSASE

Schedule Type Select the FortiSASE desired synchronization frequency.

Scan On Configure the day the scan will run. This only applies if the schedule type is configured to *Weekly* or *Monthly*. Select a day of the week (Sunday through Monday) or a day of the month (1st through the 31st).

Start At Configure the time the scan will start.

3. Click Save.

Configuring Endpoints settings

To configure Endpoints settings:

1. Go to *System Settings > Endpoints*.
2. Configure the following options:

FortiClient telemetry connection key	Add the FortiClient Telemetry connection key for FortiClient EMS. FortiClient must provide this key during connection. You can generate a QR code for the specified key. See Generating a QR code for centrally managing FortiClient (Android) and (iOS) endpoints on page 219 .
Keep alive interval	Each connected FortiClient endpoint sends a short keep-alive message to FortiClient EMS at the specified interval.
Full keep alive interval	Each connected FortiClient endpoint sends a full keep-alive message to FortiClient EMS at the specified interval.
License timeout	Each connected FortiClient endpoint consumes a license seat. If an endpoint disconnects from FortiClient EMS, EMS retains the license seat in anticipation that the endpoint will reconnect. If the endpoint does not reconnect within the given timeout, EMS removes its connection record. If the endpoint is removed, switched off, or becomes offline, and does not reestablish Telemetry connection to FortiClient EMS within the given timeout, EMS deletes the endpoint even if FortiClient on the endpoint shows that it is still connected to FortiClient EMS. The default license timeout value is 30 days. The maximum allowed value is 45 days.
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.

3. Click **Save**.

Configuring the login banner

When you enable the login banner, a message appears prior to a user logging into FortiClient EMS.

To configure the login banner:

1. Go to *System Settings > Login Banner*.
2. Click *Enable login banner*.
3. In the *Message* field, type your message. The *Preview* section displays a preview of the message.
4. Click **Save**.

SAML SSO

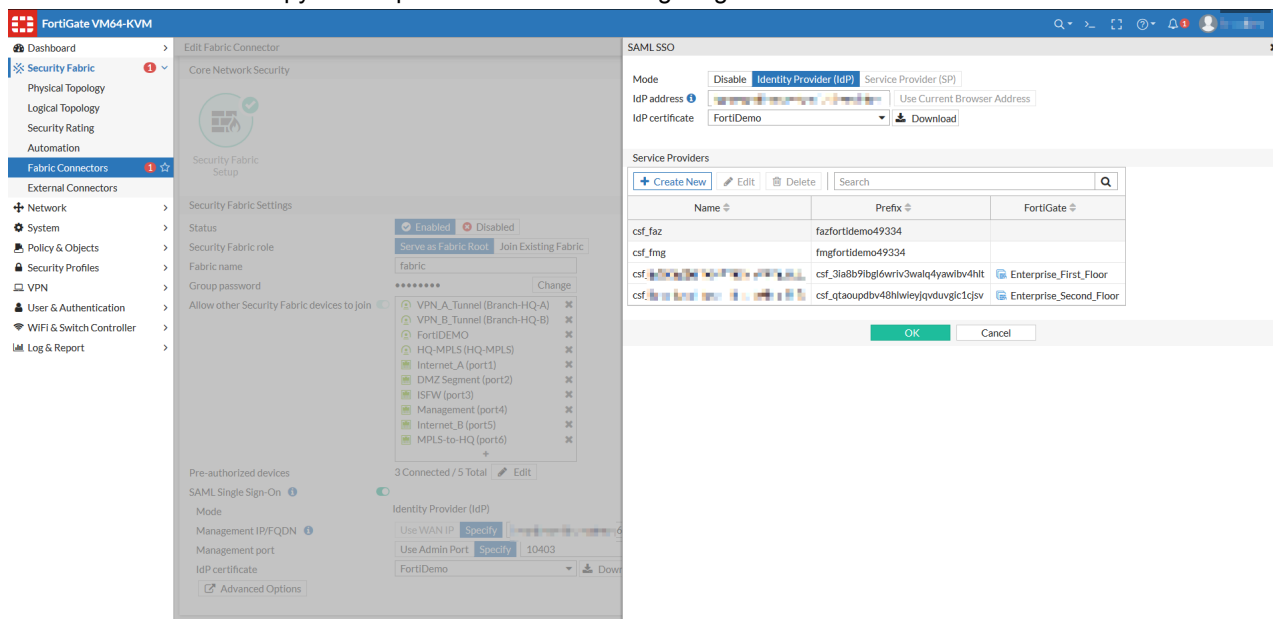
You can enable SAML SSO to allow users to log in to EMS using a FortiGate as an Identity Provider (IdP).



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.

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 Server settings on page 204](#).

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.

Alerts

Configuring EMS Alerts

You can set up an SMTP server to enable alerts for FortiClient EMS or endpoint events. When an alert is triggered, EMS sends an email notification.

To configure EMS Alerts:

1. Go to *System Settings > EMS Alerts*.
2. Set the following options to send an email when the following events happen:

Version Alerts

New EMS version is available for deployment	New FortiClient EMS version is available.
Remind me everyday for 2 weeks	Remind you when a new FortiClient EMS version is available everyday for two weeks.
New FortiClient version is available for deployment	New FortiClient version is available for deployment.
Remind me everyday for 2 weeks	Remind you when a new FortiClient version is available for deployment everyday for two weeks.

FortiClient Alerts

EMS license is expired or about to expire	Expiring or expired FortiClient EMS license.
EMS fails to sync with LDAP domains	FortiClient EMS does not sync with LDAP domains.
Less than 10% of client licenses are left	Be notified when there are less than 10% of client licenses left.
Client licenses have run out	Be notified when you run out of client licenses.
New software is detected	Be notified when new FortiClient software is detected.

FortiClient for Chromebook Alerts

EMS license for Chromebooks is expired or about to expire	Expiring or expired FortiClient EMS license for Chromebooks.
Less than 10% of the client licenses for Chromebooks are left	Be notified when there are less than 10% of client licenses left for Chromebooks.
Client licenses for Chromebooks have run out	Be notified when you run out of client licenses for Chromebooks.

3. Click **Save**. If you have not already set up an SMTP server, the GUI automatically prompts you to configure SMTP server settings. See [Configuring SMTP Server settings on page 213](#).

Configuring Endpoints 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

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**.

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.

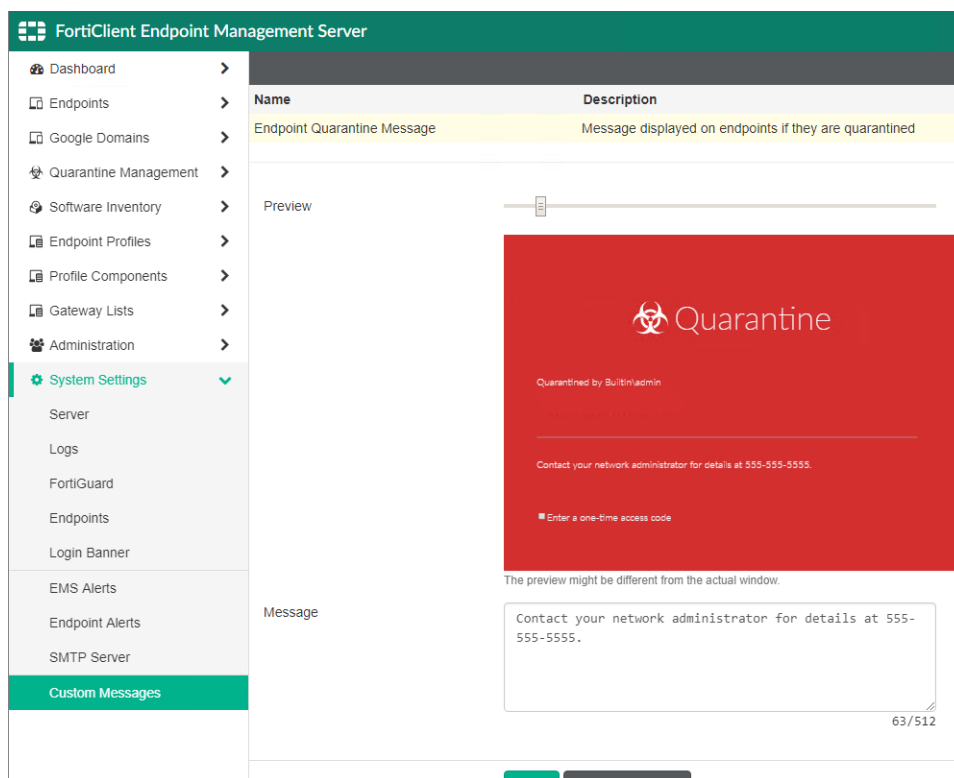
Customizing the endpoint quarantine message

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 types of Web Filter messages:
 - Blocklisted page
 - Blocked page
 - Blocked FortiGuard inaccessible page
 - Warning page
 - Warning FortiGuard inaccessible pageSome customization fields apply to all messages, while others apply to only specific messages. This is indicated beside the field name.
3. In the left pane, enable/disable the fields and enter the desired messages. You can also upload images for logo and icon fields. The right pane displays previews of the messages.
4. Click **Save**.

Feature Select

In Feature Select, you can choose which features to show and hide in EMS. Only features that are enabled in Feature Select are available for configuration in other areas of EMS. For example, disabling Web Filter in Feature Select results in the following:

- Endpoint profiles:
 - The Web Filter tab is not available for configuration.
 - The option to enable Web Filter logs on the System Settings tab is not available.
- If you enable Web Filter in a deployment package, the deployment package installs Web Filter on the endpoint. However, the Web Filter feature is disabled on the endpoint and does not appear in the FortiClient GUI.
- The Web Filter Detection widget is not available on the FortiClient Status dashboard.
- Importing a profile from FortiGate/FortiManager is not available.

Only an EMS superadministrator can enable and disable features in Feature Select. Other EMS users can view which features are enabled and disabled on the Feature Select page, but cannot modify the configuration.

If an endpoint previously had a feature enabled, but you later disable the feature in Feature Select, EMS then disables the feature on the endpoint.

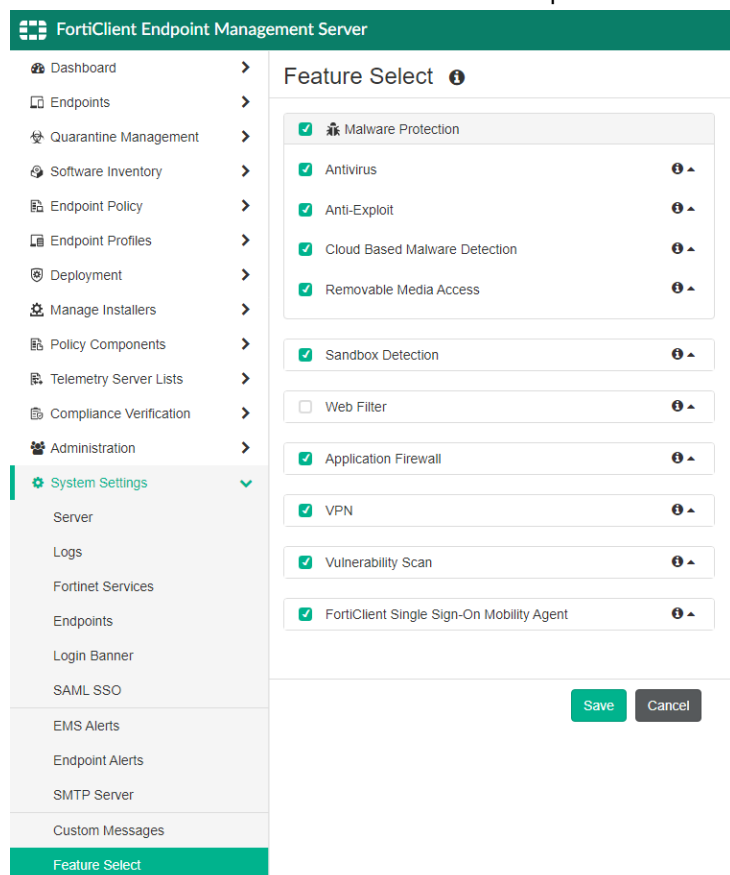
The following table provides details on features that you must enable for certain functionalities to be available in FortiClient. You must enable the feature in *Feature Select*, then configure on the applicable endpoint profile for the functionality to be available in FortiClient. Note that this table 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)

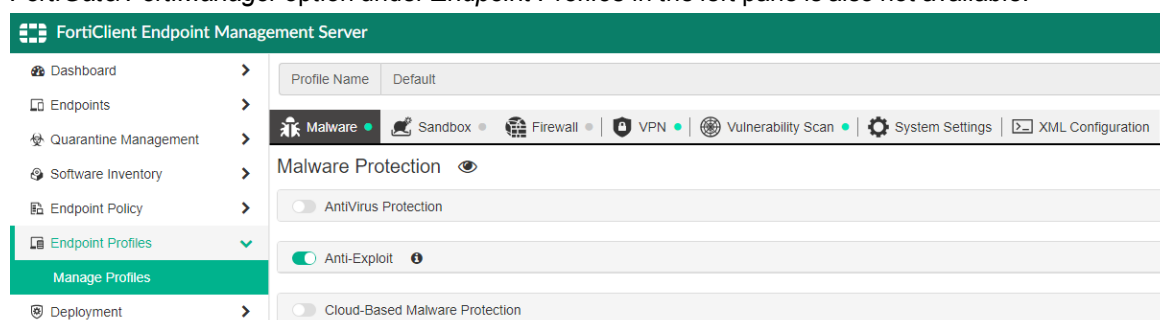
You cannot disable Web Filter if you have applied a Chromebook management license to EMS.

To enable/disable a feature in Feature Select:

1. Go to *System Settings > Feature Select*.
2. Enable or disable features as desired. This example disables Web Filter.



3. Click **Save**. The *Web Filter* tab is not available for configuration in an endpoint profile. The *Import from FortiGate/FortiManager* option under *Endpoint Profiles* in the left pane is also not available.



When creating a deployment package, a warning displays beside Web Filtering that the feature is disabled. You cannot create a deployment package that installs the Web Filter feature on endpoints while Web Filter is disabled in *Feature Select*.

Add Deployment Package

Assigned policies will not be able to enable features that are not installed

1 Version 2 General **3 Features** 4 Advanced 5 Telemetry

Basic Security Features

- ☒ Endpoint Telemetry
Endpoint telemetry and remediation.
- ☒ Vulnerability Scan
Host vulnerability scanning
- ☒ Secure Access Architecture Components
SSL and IPsec VPN
- ☒ Advanced Persistent Threat (APT) Components
FortiSandbox detection and quarantine features

Additional Security Features

- ☒ AntiVirus
- ☐ Web Filtering ▲ This feature is disabled
- ☒ Application Firewall
- ☒ Single Sign-On mobility agent
- ☒ Cloud Based Malware Outbreak Detection

Back **Next**

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

Manage Dashboard Widgets

Endpoint Charts

- ☐ Endpoint Activity
- ☐ Endpoint Alerts
- ☒ Endpoint Connection
- ☐ Managed Mac FortiClient Versions
- ☐ Managed Windows FortiClient Versions
- ☐ Managed Linux FortiClient Versions
- ☒ Endpoint Management
- ☐ Mac Operating Systems
- ☐ Windows Operating Systems
- ☐ Linux Operating Systems

Top 3 Lists

- ☐ Antivirus Detection
- ☐ Sandbox Detection
- ☐ Vulnerability Detection

Others

- ☒ System Information
- ☒ License Information

Save **Cancel**

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 optionally contain the FortiClient telemetry connection key, if desired.

To generate the QR code:

1. Do one of the following:
 - a. To generate the QR code without a connection key, go to *System Settings > Server*. Beside the *Listen on IP* field, click the *View QR Code* button.
 - b. To generate the QR code with a connection key, go to *System Settings > Endpoints*. Ensure that the *FortiClient telemetry connection key* field is populated, then click the *View QR Code* button beside it.
2. In the dialog, select or deselect *Show FortiClient telemetry connection key* as desired.
3. Click *Continue*.
4. Click *Download*.
5. Save the QR code image to your machine.
6. 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 the [FortiClient \(Android\) Administration Guide](#) or [FortiClient \(iOS\) Administration Guide](#).

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*.

Appendix A - Examples

This section includes the following configuration examples for FortiClient EMS:

- [Support banned word check in URL on page 222](#)

Support banned word check in URL

You can configure keyword scanning on search engines for Chromebook endpoints. EMS has a content safeguard service-provided file with a list of words in various languages for different categories. The *Keyword Scanning on Search Engine* feature supports monitoring and blocking searches for banned words that users perform in popular search engines. You can use this feature to protect students from inappropriate and malicious content.

To enable keyword scanning on search engines:

1. In EMS, go to *Endpoint Profiles*. Select the desired Chromebook profile, or create a new one.
2. Enable *Keyword Scanning on Search Engine*.
3. Configure the following features:

Banned Word Search

Enable to configure actions (block or monitor) to take when the user searches for terms that belong to the following categories:

- Violence/Terrorism
- Extremist
- Pornography
- Cyber Bullying
- Self Harm

Custom Banned Words

Configure actions for individual terms. Enable *Custom Banned Words*, type the desired term in the *Add Word* field, then click *Add Word*. Configure the action for the term (*Block*, *Monitor*, or *Allow*), then toggle the *Status* to *On*.

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

The custom term may belong to a category under *Banned Word Search*. If the action configured for the category under *Banned Word Search* and the action configured for the term under *Custom Banned Words* differ, EMS applies the action configured under *Custom Banned Words*.

FortiClient Endpoint Management Server

Profile Name: Default - Chromebooks

Web Filter

☒ Keyword Scanning on Search Engine

☒ Banned Word Search

Category	Block	Monitor	Off
Violence/Terrorism	<input checked="" type="button" value="Block"/>	<input type="button" value="Monitor"/>	<input type="button" value="Off"/>
Extremist	<input checked="" type="button" value="Block"/>	<input type="button" value="Monitor"/>	<input type="button" value="Off"/>
Pornography	<input checked="" type="button" value="Block"/>	<input type="button" value="Monitor"/>	<input type="button" value="Off"/>
Cyber Bullying	<input checked="" type="button" value="Block"/>	<input type="button" value="Monitor"/>	<input type="button" value="Off"/>
Self Harm	<input checked="" type="button" value="Block"/>	<input type="button" value="Monitor"/>	<input type="button" value="Off"/>

☒ Custom Banned Words

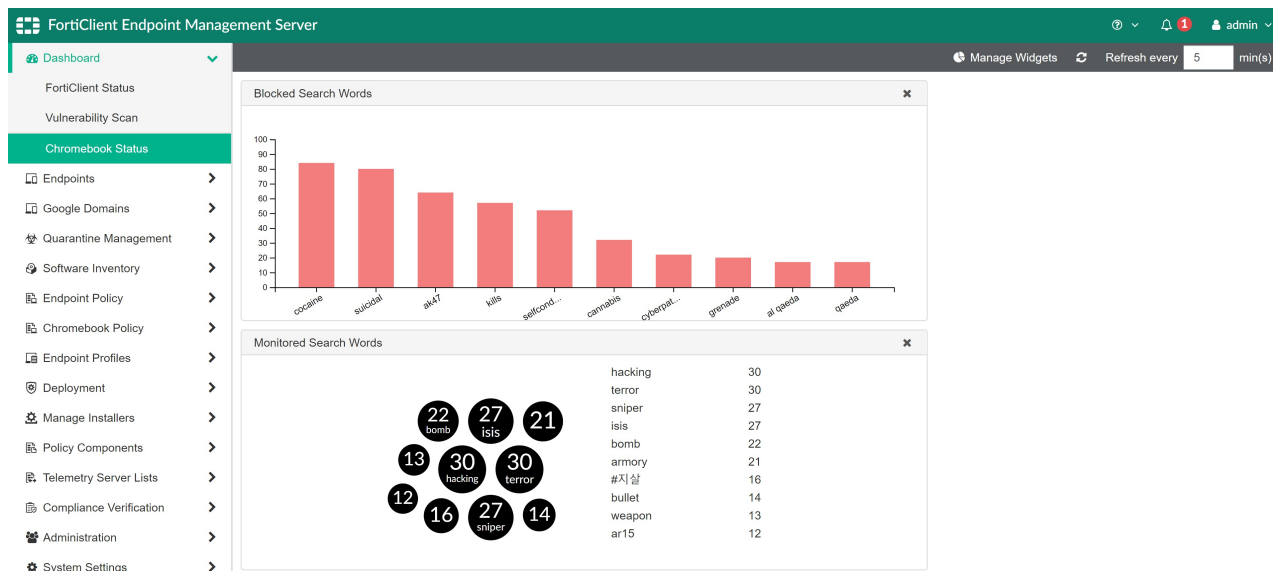
Banned Word	Action	Status
#지살	<input type="button" value="Monitor"/>	<input checked="" type="checkbox"/>
War	<input checked="" type="button" value="Allow"/>	<input checked="" type="checkbox"/>
Rifle	<input checked="" type="button" value="Block"/>	<input checked="" type="checkbox"/>
Bomb	<input type="button"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

Exclusion List

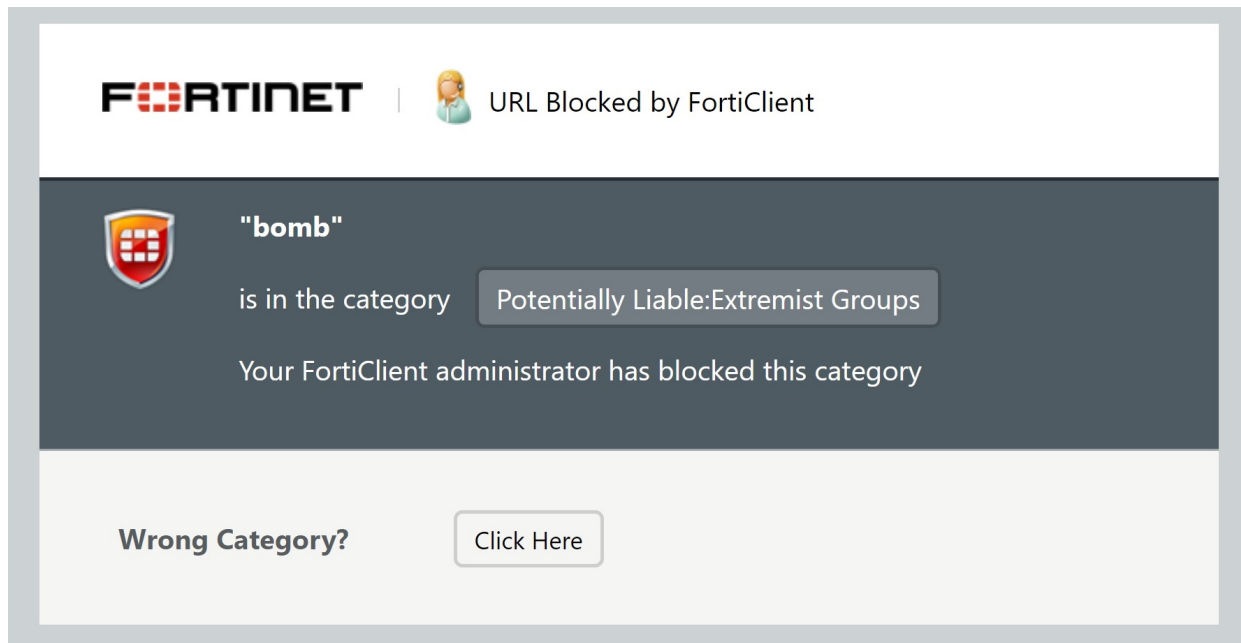
As Simple: Perform a case-insensitive matching against URLs.

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

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.

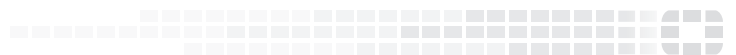


Change log

Date	Change Description
2020-08-24	Initial release.
2020-08-27	Added Configuring a profile with application-based split tunnel on page 120 . Updated To add an IP address group assignment rule: on page 99 and To add an on-fabric detection rule set: on page 172 .
2020-09-22	Updated Compliance verification rule types on page 181 .
2020-10-08	Updated: <ul style="list-style-type: none"> • Filtering the list of endpoints on page 80 • VPN on page 143 • Configuring Server settings on page 204 • Configuring Endpoints settings on page 209. • Generating a QR code for centrally managing FortiClient (Android) and (iOS) endpoints on page 219
2020-10-13	Updated Web Filter on page 136 and System Settings on page 150 .
2020-10-14	Updated Upgrading from an earlier FortiClient EMS version on page 25 . Updated "G Suite" to "Google Workspace".
2020-10-21	Updated Web Filter on page 136 and Configuring Endpoints settings on page 209 .
2020-10-26	Updated Removable Media Access on page 132 .
2020-10-29	Updated Compliance verification rule types on page 181 .
2020-11-04	Updated Licensing EMS by logging in to FortiCloud on page 34 .
2020-11-16	Updated Exclusions on page 132 and Database management on page 201 .
2020-11-23	Updated System requirements on page 19 and Anti-Exploit on page 131 .
2020-11-26	Updated FortiClient installers on page 168 .
2020-11-27	Updated Compliance verification rule types on page 181 .
2020-12-07	Updated Exclusions on page 132 .
2020-12-10	Updated AntiVirus Protection on page 127 .



FORTINET®



Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.