FortiClient EMS - Administration Guide

Version 6.2.0

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

January 29, 2020
FortiClient EMS 6.2.0 Administration Guide
04-620-546494-20200129

TABLE OF CONTENTS

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- Identifying outdated versions of FortiClient software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.

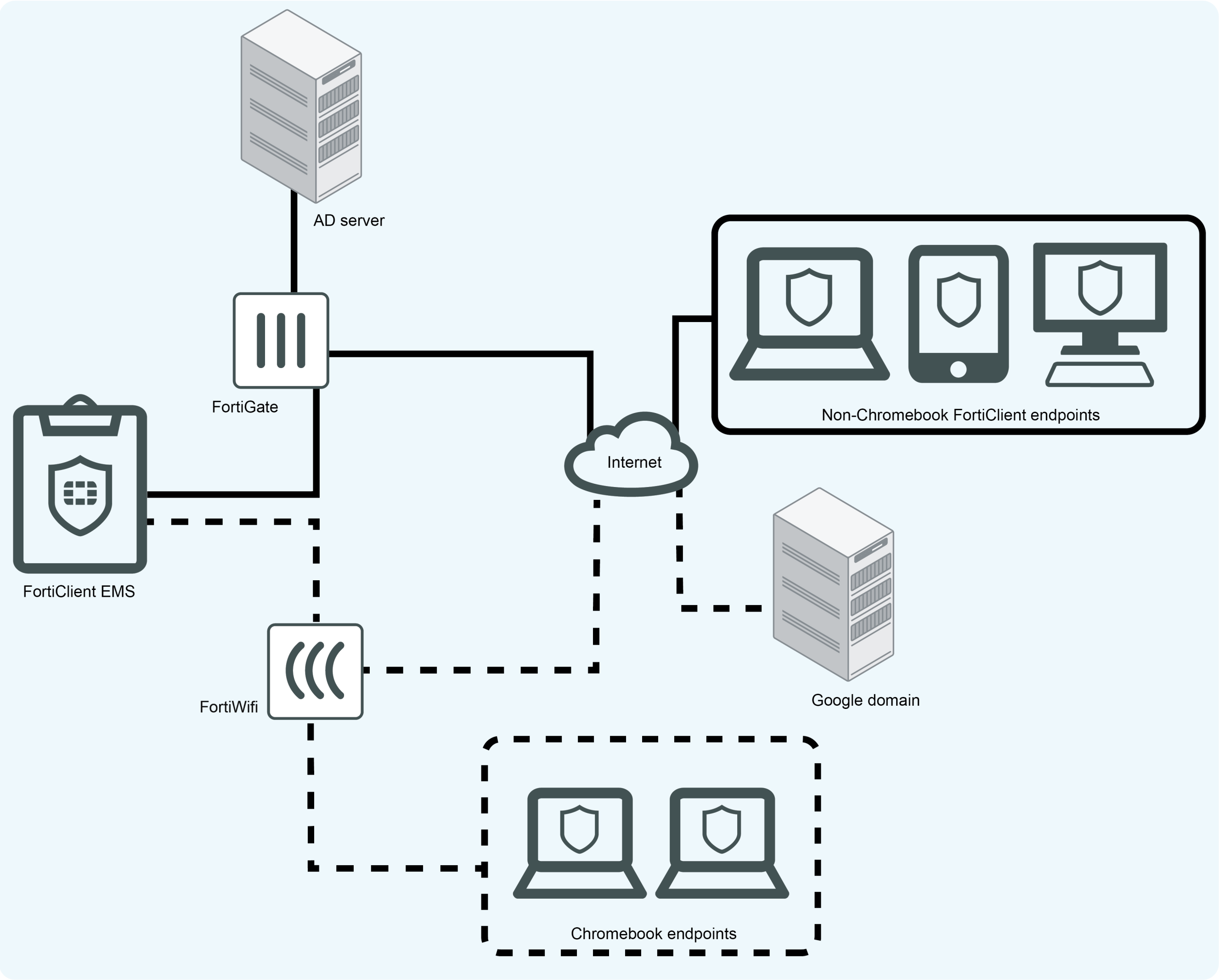
FortiClient EMS also provides the infrastructure to install and manage the FortiClient Web Filter extension on Google Chromebook endpoints. FortiClient protects endpoint users by working with FortiClient EMS to filter web content endpoint users view on Google Chromebooks.

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: • 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 below, the undotted lines shows how different components are connected to manage Windows, macOS, and Linux endpoints using FortiClient EMS. The dotted lines represent how components are used 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
Administration Guide	Describes how to set up FortiClient EMS and use it to manage endpoints. It includes information on how to configure multiple endpoints, configure and manage profiles for the endpoints, and view and monitor endpoints.
New Features Guide	Describes new features and enhancements in FortiClient EMS for the release, including configuration information.
QuickStart Guide	Describes how to install and begin working with the FortiClient EMS system. It provides instructions on installation and deployment, and includes a high-level task flow for using the FortiClient EMS system.
Release Notes	Lists any known issues and limitations for the release. This document also defines supported platforms and minimum system requirements.
Upgrade Paths	Provides upgrade path information for different versions of FortiClient EMS.

Getting started

This section provides information on getting started with managing Windows, macOS, and Linux endpoints and managing Chromebooks:

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.

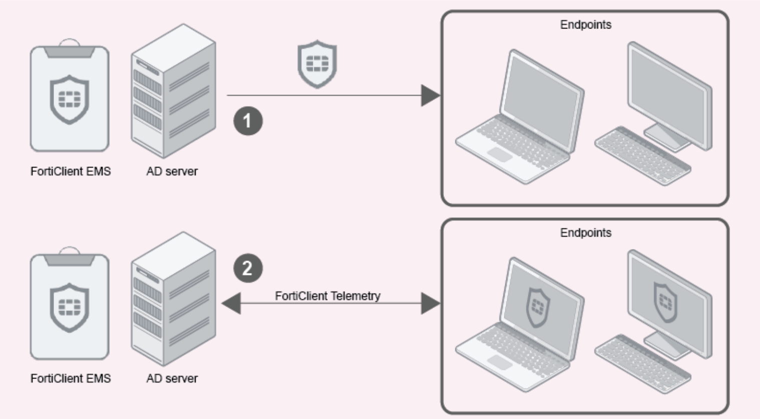
You can deploy FortiClient to endpoints using Active Directory (AD) servers and workgroups. There are differences between using AD servers and workgroups.

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 is installed 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 is installed on endpoints and endpoints are connected to FortiClient EMS, you can use workgroups to uninstall and update FortiClient on endpoints.

The image below 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.

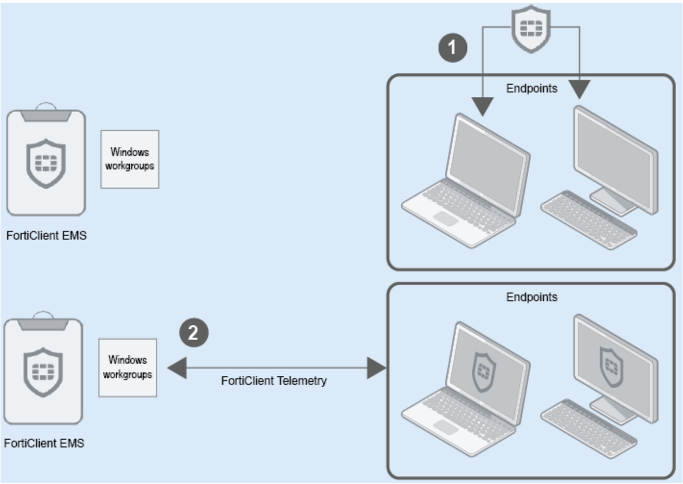


The image below shows a deployment of FortiClient (Windows) using FortiClient EMS with Windows workgroups:

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 148.

2. The endpoints now have FortiClient installed and FortiClient Telemetry is connected to FortiClient EMS.



1. Add endpoints with an AD server or Windows workgroups. See Adding endpoints on page 71.
   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 on the profile's *Deployment* tab 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 credentials on the *Deployment* tab in FortiClient EMS are not taken into account.
2. Create FortiClient deployment packages in FortiClient EMS, and specify which FortiClient features each deployment package will install on endpoints. See Adding FortiClient deployment packages on page 146.
3. Create a profile to select the FortiClient deployment package and include configuration information for FortiClient software on endpoints. See Creating profiles to deploy FortiClient on page 109.
4. Prepare domains and workgroups for deployment. See Preparing the AD server for deployment on page 161.
5. Create an endpoint policy that is configured with desired profile. Configure the endpoint policy to apply to domains and workgroups to deploy FortiClient on endpoints. See Adding an endpoint policy on page 105.
   See Deploying FortiClient on endpoints on page 163.

   After you apply the endpoint policy to endpoint groups, EMS pushes profile changes to endpoints with the next Telemetry communication. FortiClient is installed on endpoints, and FortiClient connects Telemetry to FortiClient EMS.
6. Monitor the installation process using the *Endpoints* content pane. See Viewing the Endpoints content pane on page 73.

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.

1. Edit an existing profile or create a new profile to configure FortiClient software on endpoints. See Creating profiles to configure FortiClient on page 109.
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 domains and workgroups to deploy FortiClient on endpoints. See Adding an endpoint

policy on page 105.
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* content pane. See Viewing the Endpoints content pane on page 73.

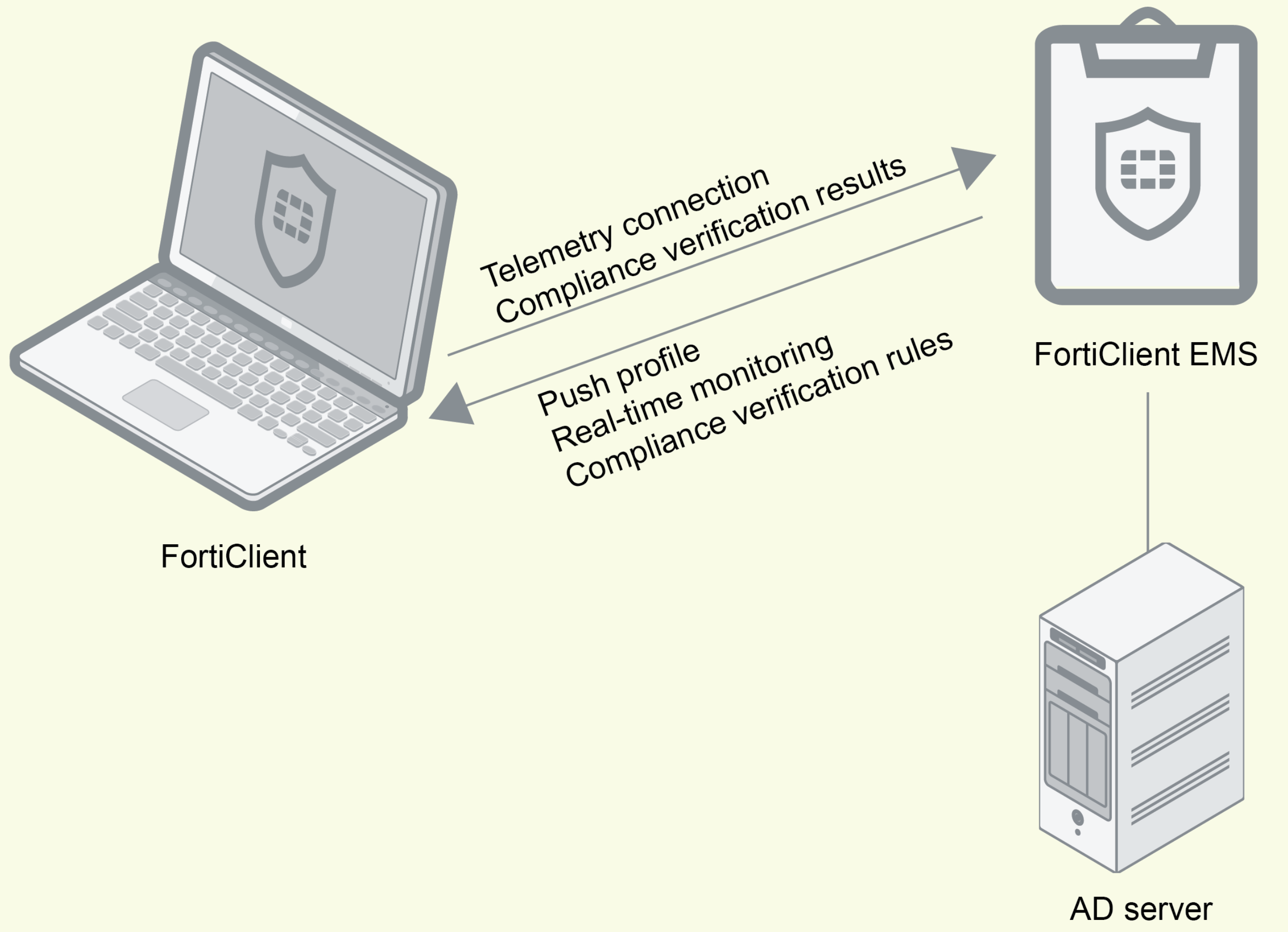
Relationship between FortiClient EMS, FortiGate, and FortiClient

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

For details, see the *FortiClient 6.2 Compliance Guide*.

Standalone FortiClient EMS

The diagram below shows the topology when using FortiClient EMS in standalone mode.

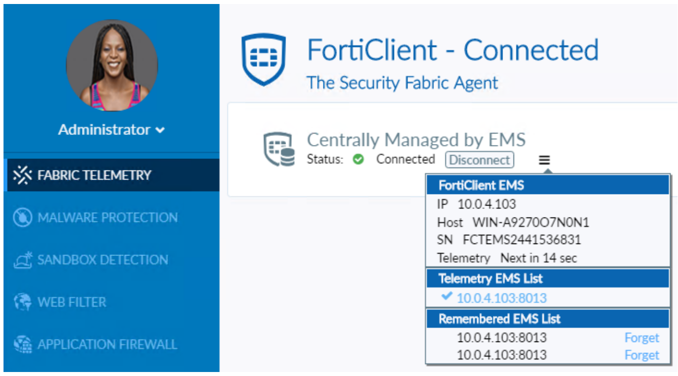


In this scenario, EMS provides FortiClient endpoint provisioning. FortiClient connects Telemetry to EMS to receive configuration information in an endpoint profile as part of an endpoint policy from EMS. EMS also sends compliance verification rules to FortiClient, and use the results from FortiClient to dynamically group endpoints in EMS. Only EMS can control the connection between FortiClient and EMS. Any changes to the connection must be made from EMS, not

FortiClient. When FortiClient is connected to EMS, FortiClient settings are locked so the endpoint user cannot change any configuration. To disconnect FortiClient from EMS, the EMS administrator must deregister the endpoint in EMS.

When viewing the endpoint in the EMS GUI, the endpoint's connection is shown as *Managed by EMS*.

The below shows the FortiClient GUI when FortiClient is connected to FortiClient EMS. You can also view the IP address, hostname, and serial number of the FortiClient EMS to which FortiClient Telemetry is connected. This means FortiClient EMS can push profiles to FortiClient. FortiClient EMS is providing endpoint provisioning to FortiClient.



Status: Connected

IP 10.0.4.103
Host WIN-A9270O7N0N1
SN FCTEMS2441536831
Telemetry Next in 14 sec

✓ 10.0.4.103:8013

10.0.4.103:8013
10.0.4.103:8013

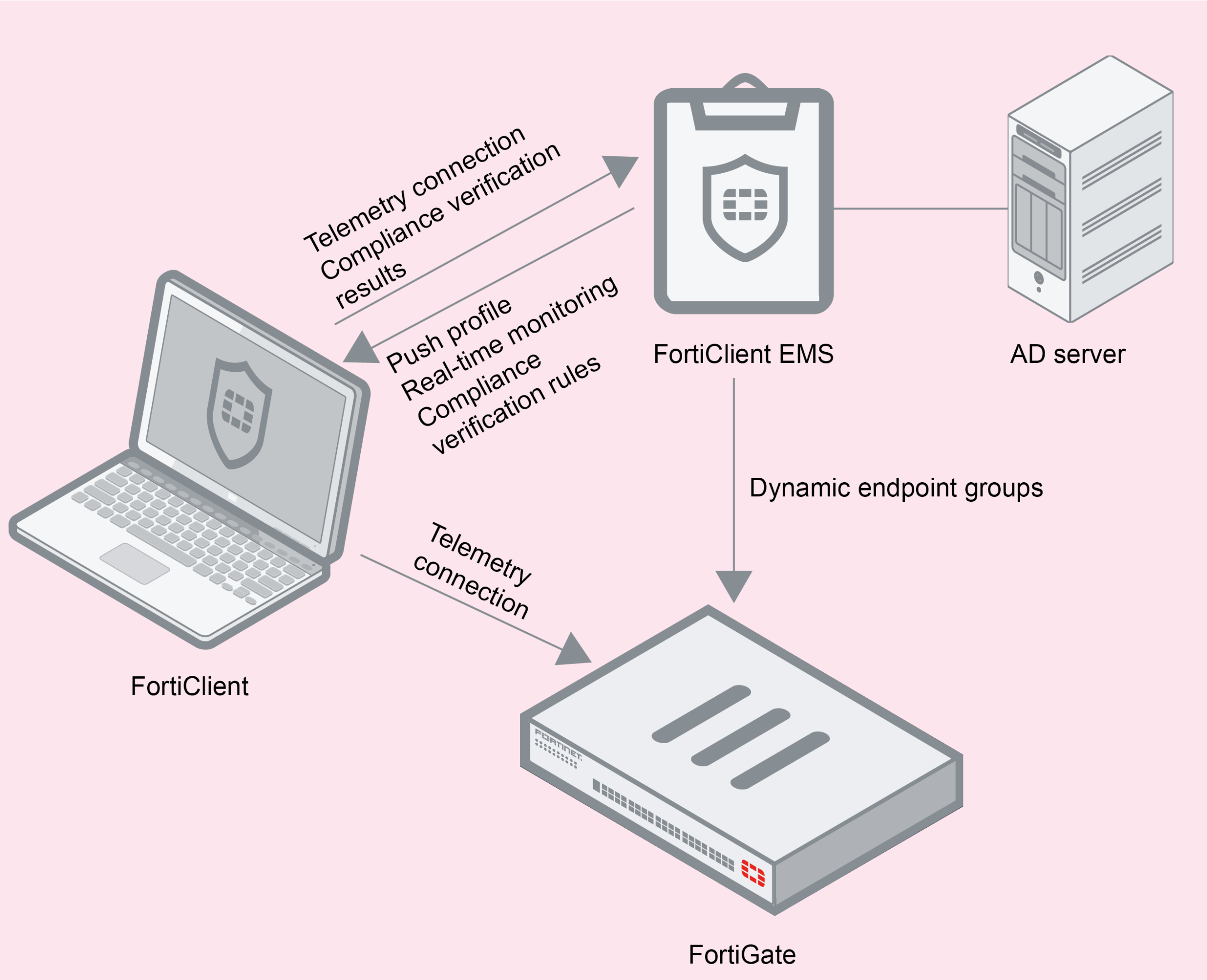
FortiClient EMS integrated with FortiGate

In this scenario, FortiClient Telemetry connects to EMS to receive a profile of configuration information as part of an endpoint policy and to FortiGate to participate in the Fortinet Security Fabric. 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. See Configuring FortiOS dynamic policies using EMS dynamic endpoint groups on page 158.

FortiClient only registers to a FortiGate if all of the following is true:

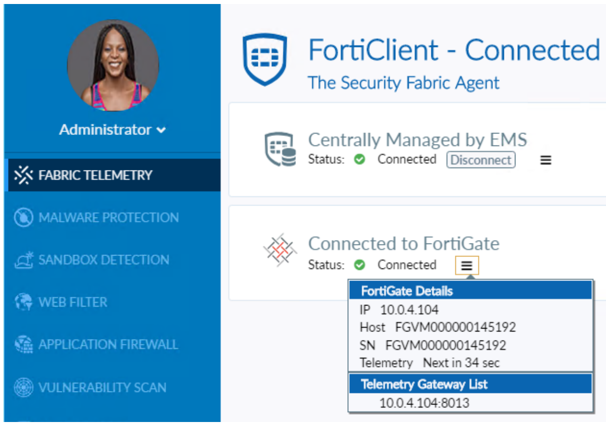
- FortiClient is registered to EMS.
- FortiClient has received a Telemetry gateway list from EMS.
- EMS has allocated a Fabric Agent license seat to the endpoint. A Fabric Agent license is required to register to the FortiGate. If the EMS server has only Sandbox Cloud licenses, FortiClient cannot register to FortiGates. See FortiClient EMS on page 20.

If using a version of FortiOS earlier than 6.2.0, FortiClient endpoints can connect to the Security Fabric, but compliance enforcement is not supported.



When viewing the endpoint in the FortiClient EMS GUI, the endpoint's connection is shown as *Managed by EMS* and *FortiTelemetry to <FortiGate hostname>*.

When FortiClient Telemetry is connected to both EMS and FortiGate, the FortiClient GUI shows the connection status for both the EMS and FortiGate.



FortiClient - Connected
The Security Fabric Agent

Centrally Managed by EMS
Status: Connected

Connected to FortiGate
Status: Connected

FortiGate Details
IP 10.0.4.104
Host FGVM000000145192
SN FGVM000000145192
Telemetry Next in 34 sec

Telemetry Gateway List
10.0.4.104:8013

Depending on the EMS compliance verification rules and policies configured in FortiOS, the FortiClient endpoint may be blocked from accessing the network. The EMS administrator can adjust the endpoint configuration so that the endpoint regains network access.

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 server 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 endpoints on page 84 or using FortiOS by following the procedure described below:

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

1. Start and log into FortiClient EMS. See Starting FortiClient EMS and logging in on page 34.
2. Add SSL certificates. See Adding SSL certificates to FortiClient EMS for Chromebook endpoints on page 180.

3. Configure FortiClient EMS settings. See System Settings on page 177.
4. Configure user accounts and permissions. See Administrators on page 165.

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.

1. Add the FortiClient Web Filter extension. See Adding the FortiClient Web Filter extension on page 41.
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 46.
5. Disallow incognito mode. See Disallowing incognito mode on page 44.

Deploying profiles to Chromebooks

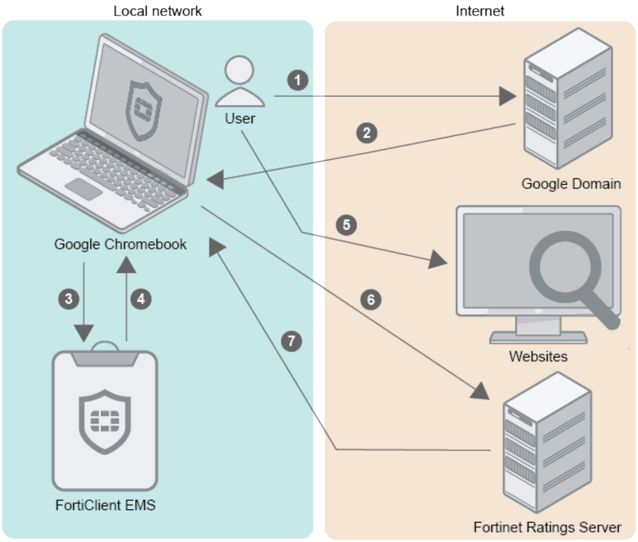
Following is an overview of how to add a Google domain, configure profiles, and push profiles to Google Chromebooks. After you add the extension in the Google Admin console, the extension is downloaded to the Google Chromebook when the Chromebook user logs into the Chromebook.

1. Add the Google domain. See Adding Google domains on page 89.
2. Define web filtering options in one or more profiles. See Adding new profiles on page 116.
   You can enable Safe Search in profiles.
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 107.
4. Verify the FortiClient Web Filter extension. See Verifying the FortiClient Web Filter extension on page 45.
5. View Google domains and Google users. See Viewing domains on page 89.

How FortiClient EMS and FortiClient work with Chromebooks

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

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


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

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, it is recommended you read the *FortiClient EMS Release Notes* to become familiar with relevant software components and other important information about the product.

System requirements

The minimum system requirements for FortiClient EMS are as follows.

- Microsoft Windows Server 2012 R2 or newer
- No additional installed services
- 2.0 GHz 64-bit processor, dual core (or two virtual CPUs)
- 4 GB RAM (8 GB RAM or more is recommended)
- 40 GB free hard disk
- Gigabit (10/100/1000baseT) Ethernet adapter
- Internet access

Internet access is required during installation. This becomes optional once installation is complete. FortiClient EMS accesses the Internet to obtain information about FortiGuard engine and signature updates.

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.

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

Windows, macOS, and Linux endpoint licenses

There are three types of licenses for Windows, macOS, and Linux endpoints:

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 below 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, 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.
Sandbox Cloud	Adds support for FortiSandbox Cloud for Windows endpoints.

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.

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.

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.

During the installation of common services required for FortiClient EMS, you are not asked for license information.

Required services and ports

You must ensure required ports and services are enabled 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)	The FortiClient EMS server connects to endpoints using RPC for FortiClient initial deployment.	TCP	135	Outgoing	N/A
AD 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

Communication	Usage	Protocol	Port	Incoming/Outgoing	How to customize
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
G suite API/Google domain directory	Retrieving Google domain information using API calls	TCP	443	Outgoing	N/A

The following ports and services should be enabled 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
FortiAnalyzer	Sending logs to FortiAnalyzer	TCP	8443	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 use by enterprises. It 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.

It is recommended to have at least 200 GB of disk space available.

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 is installed with EMS by default. Otherwise, you may experience database deadlocks. See Installing FortiClient EMS to specify SQL Server Enterprise or Standard instance on page 32.

FortiClient Telemetry security features

FortiClient connects to the FortiGate and EMS 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.

Telemetry connections between FortiClient and FortiGate or EMS may be configured to require a preshared password or connection key. See Configuring Endpoints settings on page 182 and Creating Telemetry gateway lists on page 152.

The default Telemetry port number is 8013. This may be changed 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 will lock out endpoints that are still using the default.

The EMS administrator may at anytime disconnect a rogue endpoint from EMS and prevent it from reconnecting to EMS in the future.

A list of TCP/IP ports used by the EMS is provided in Required services and ports on page 22. The network administrator may 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, it is recommended to sync the time to the Google server time.
	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 6.2.0 supports upgrading from previous EMS versions as outlined in*FortiClient and FortiClient EMS Upgrade Paths*.

To ensure a successful upgrade, it is recommended you perform the upgrade on a staging server before upgrading the production server. The staging server is a test environment where you can run the latest FortiClient EMS version using your own configuration. You can create it before upgrading the production server, then shut it down after successfully upgrading the production server.

When upgrading FortiClient EMS from 6.0 to 6.2.0, 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 6.2 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 the staging server:

1. Back up the database from the FortiClient EMS production server.
2. Install FortiClient EMS on the staging server. Ensure this is the same version of FortiClient EMS as currently installed on the production server.

3. Import the FortiClient EMS database from the production server.
4. Connect a few endpoints to the staging server by disconnecting them from the production server, then entering the staging server's FortiClient EMS IP address in FortiClient on the endpoints. This is for testing purposes; keep most endpoints connected to the production server.
5. Close FortiClient EMS.
6. Install FortiClient EMS 6.2.0 on the staging server using the downloaded installer. You may complete the upgrade using one of the following methods. The installer files can be downloaded from Customer Service & Support.
    a. If Fortinet has enabled upgrade on the FDS, 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.
7. Monitor FortiClient EMS performance on the staging server for at least two days, including testing use cases.

To upgrade the production server:

1. Upgrade the production server to FortiClient EMS 6.2.0 by repeating step 5 to 7 from the instructions above on the production server.
2. If you performed the upgrade on the staging server prior to the production server, do the following after successfully upgrading the production server:
    a. Disconnect endpoints from the staging server, then connect them to the production server.
    b. Shut down the staging server.

Install preparation for managing Chromebooks

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

G Suite account

You need to sign up for your G Suite account before you can use the Google service and manage your Chromebook users.

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

You can sign up for a G Suite 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 FortiClient EMS is installed 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 SSL certificates to FortiClient EMS for Chromebook endpoints on page 180. 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 20
- 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.

It is recommended you install FortiClient EMS on a dedicated server in a controlled environment. 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_6.2.0.<build>_x64.exe
```

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

Installing FortiClient EMS

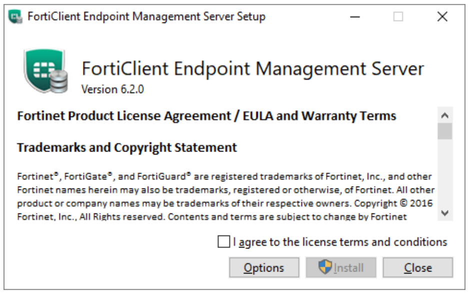
The FortiClient EMS installation package includes:

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

Local administrator rights and Internet access are required to install FortiClient EMS.

1. If you are logged into the system as an administrator, double-click the downloaded installation file.
   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.



FortiClient Endpoint Management Server Setup

FortiClient Endpoint Management Server
Version 6.2.0

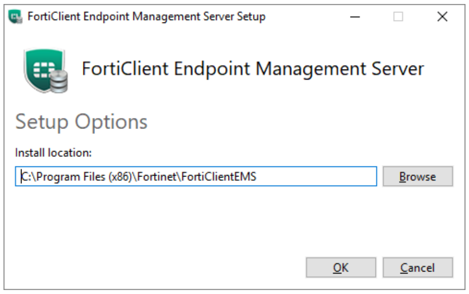
Fortinet Product License Agreement / EULA and Warranty Terms

Trademarks and Copyright Statement

Fortinet®, FortiGate®, and FortiGuard® are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks, registered or otherwise, of Fortinet. All other product or company names may be trademarks of their respective owners. Copyright © 2016 Fortinet, Inc., All Rights reserved. Contents and terms are subject to change by Fortinet

□ I agree to the license terms and conditions

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



FortiClient Endpoint Management Server Setup

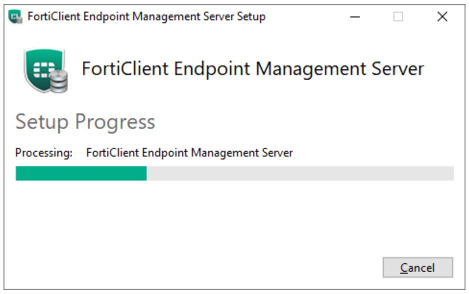
FortiClient Endpoint Management Server

Setup Options

Install location: C:\Program Files (x86)\Fortinet\FortiClientEMS

   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.



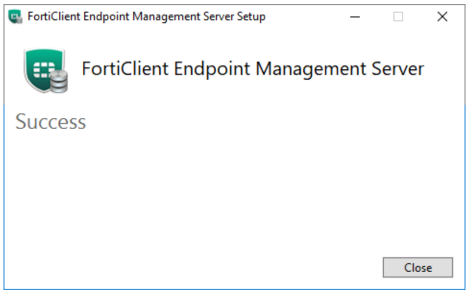
FortiClient Endpoint Management Server Setup

FortiClient Endpoint Management Server

Setup Progress

Processing: FortiClient Endpoint Management Server

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



FortiClient Endpoint Management Server Setup

FortiClient Endpoint Management Server

Success

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 localhost, 127.0.0.1. To clear this value, first enter `AllowedWebHostnames=*`, then enter the desired AllowedWebHostnames value. Otherwise, the value entered will be appended to [localhost, 127.0.0.1], so that AllowedWebHostNames=localhost, 127.0.01, <new_value>.
`ApacheServerAdminEmail`	Enter the Apache Server administrator's email address. By default, this is admin@yourcompany.com.
`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 will install SQL Server Express on the same server as FortiClient EMS. Enter `1` to install SQL Server Express; otherwise, enter `0`. By default, SQL Server Express is installed with FortiClient EMS.
`ScriptDB`	Controls where the installer will attempt to create the database from db scripts. Enter `1` to create the database from db scripts. `0` should only be entered if databases have already been set up on the server and you are only installing EMS components locally.
`ServerHostname`	Enter the preferred hostname (the remote hostname). The default is the local host.
`SQLAuthType`	Enter `sql`.
`SQLCmdlineOptions="/INSTANCEDIR"`	Enter the desired directory to install SQL Server Express to.
`SQLCmdlineOptions="/INSTANCENAME"`	Enter the SQL Server instance name.
`SQLEncryptConnection`	(Optional) Enter `yes` to encrypt the connection to SQL Server. Otherwise, enter `no`. The default is `yes`.
`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.

Option	Description
SQLService	If using a default database instance, enter the instance name. If using a named database instance, enter mssql$<instance_name>. For example, if your instance is named "database000", enter mssql$database000.
SQLTrustServerCertificate	(Optional) Enter yes to trust the SQL Server certificate on the machine where FortiClient EMS is installed. If entering no, 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. This must be pre-configured in SQL Server as described in .
SQLUserPassword	Enter the SQL password used to connect to the database instance.
WindowsUser	Enter the Windows username used to connect to the database instance. This must be pre-configured in SQL Server as described in .
WindowsUserPassword	Enter the Windows password used to connect to the database instance.

The following topics describe how to use the options above for specific use cases.

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_6.2.0.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 below 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. In this example, the HTTP and HTTPS ports are changed to 1080 and 22443, respectively.

```
FortiClientEndpointManagement_6.2.0.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, FortiClient EMS is installed with 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 must be installed 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 32.

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_6.2.0.XXXX_x64 SQLCmdlineOptions="/INSTANCENAME=FCEMS
     /INSTANCEDIR=<desired_directory>"
```

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

```
FortiClientEndpointManagement_6.2.0.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_6.2.0.XXXX_x64 InstallFolder=<desired_directory> SQLServer=<SQL_
     Server_name> SQLServerInstance= SQLService=MSSQLSERVER
```

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

```
FortiClientEndpointManagement_6.2.0.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	`FortiClientEndpointManagement_6.2.0.XXXX_x64.exe SQLUser=<username> SQLUserPassword=<password> InstallSQL=0 ScriptDB=1 SQLServerInstance= SQLService=<instance_name> SQLCmdlineOptions="/INSTANCENAME="`
Local default instance using local Windows authentication	`FortiClientEndpointManagement_6.2.0.XXXX_x64.exe SQLServerInstance= SQLService=<instance_name> SQLCmdlineOptions="/INSTANCENAME=" InstallSQL=0 ScriptDB=1`
Local named instance using SQL authentication	`FortiClientEndpointManagement_6.2.0.XXXX_x64.exe SQLUser=<username> SQLUserPassword=<password> InstallSQL=0 ScriptDB=1 SQLServerInstance=<instance_name> SQLService=mssql$<instance_name> SQLCmdlineOptions="/INSTANCENAME=<instance_name>"`

Database type	Command
Local named instance using local Windows authentication	`FortiClientEndpointManagement_6.2.0.XXXX_x64.exe SQLServerInstance=<instance_name> SQLService=mssql$<instance_name> SQLCmdlineOptions="/INSTANCENAME=<instance_name>" InstallSQL=0 ScriptDB=1`

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 would be as follows:

```
FortiClientEndpointManagement_6.2.0.XXXX_x64.exe SQLUser=janedoe SQLUserPassword=password123
     InstallSQL=0 ScriptDB=1 SQLServerInstance=database000 SQLService=mssql$database000
     SQLCmdlineOptions="/INSTANCENAME=database000"
```

Remote existing database

Creating a backup directory

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

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. In 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	`FortiClientEndpointManagement_6.2.0.XXXX_x64.exe SQLServer=<SQL_Server_name> SQLUser=<username> SQLUserPassword=<password> InstallSQL=0 ScriptDB=1 BackupDir=<backupdirectorypath>`
Remote default or named instance using Windows authentication (domain user)	`FortiClientEndpointManagement_6.2.0.XXXX_x64.exe SQLServer=<SQL_Server_name> WindowsUser=<domain name>/<username> WindowsUserPassword=<password> InstallSQL=0 ScriptDB=1 BackupDir=<backupdirectorypath>`

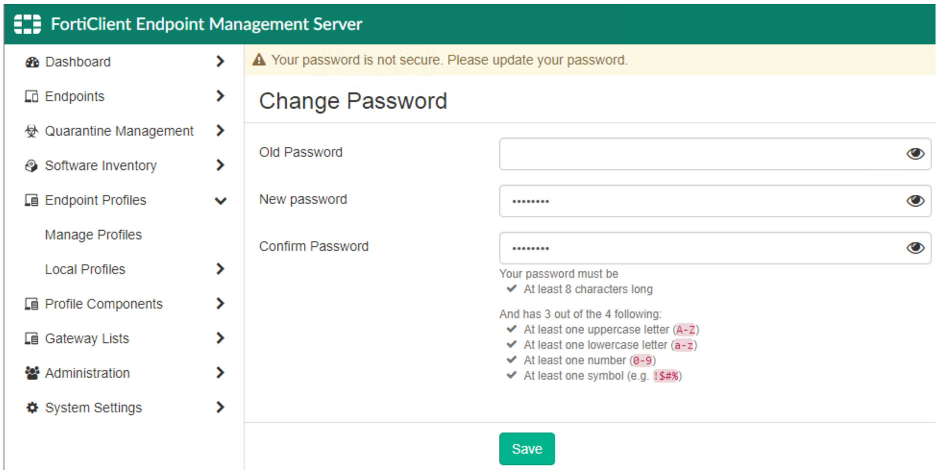
For example, if installing FortiClient EMS and pointing to a remote named instance on a computer with DNS name WIN-088 using Windows authentication, with domain name "forticlient.ca", username "janedoe", and password "password123", the command would be as follows. This example also includes the optional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

```
FortiClientEndpointManagement_6.2.0.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.

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. EMS now directs you to add a password for increased security. Change the password following the rules shown. Click *Save*.



Your password is not secure. Please update your password.

Change Password

Old Password

New password ••••••••

Confirm Password ••••••••

Your password must be
✓ At least 8 characters long

And has 3 out of the 4 following:
✓ At least one uppercase letter (A-Z)
✓ At least one lowercase letter (a-z)
✓ At least one number (0-9)
✓ At least one symbol (e.g. !$#%)

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

If you do not add the *admin* password upon initial login, EMS directs you to add a password each time the *admin* user account logs in.

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* box, enter the hostname or IP address. Otherwise, the *Pre-defined hostname* is used.
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

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

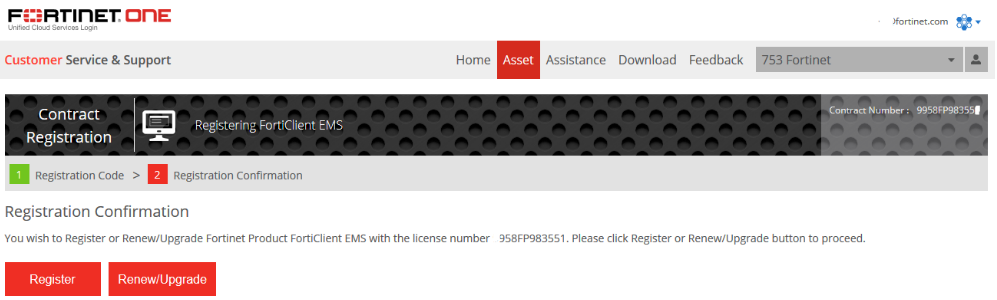
To license FortiClient EMS:

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

1. Log into your FortiCare account.
2. On your FortiCare account, register the EMS installation.
3. Register your FortiClient licenses on your FortiCare account.
   As described in FortiClient EMS 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.

   When applying an additional license type, you must select *Renew/Upgrade* on the contract registration screen, regardless of the license types of the first and subsequent licenses. Selecting *Renew/Upgrade* 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/Upgrade* creates an additional license file instead of combining the new license with the existing license(s). You will not be able to have the new license and existing licenses both applied to the same EMS server.


FORTINET ONE
Unified Cloud Services Login
)fortinet.com
Customer Service & Support
Home
Asset
Assistance
Download
Feedback
753 Fortinet
Contract Registration
Registering FortiClient EMS
Contract Number : 9958FP98355
1 Registration Code
>
2 Registration Confirmation

Registration Confirmation

You wish to Register or Renew/Upgrade Fortinet Product FortiClient EMS with the license number 958FP983551. Please click Register or Renew/Upgrade button to proceed.

4. License FortiClient EMS. See Activating, upgrading, and renewing licenses on page 175.

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.

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 into your FortiCare account or upload a license file to update the license status.
Non-expired license	You can upgrade the license. See Uploading a license file for activation, upgrade, or renewal on page 175.
Expired license	You can renew the license. See Uploading a license file for activation, upgrade, or renewal on page 175. You have ten days after the license expiry date to renew the license. During this grace period, the *License Information* widget displays the expiry date, which has already passed, and FortiClient EMS functions as if the license has not expired. FortiClient EMS also displays a daily notification that the license has expired and that you are currently using FortiClient EMS as part of the ten day grace period. After ten days, FortiClient EMS reverts to unlicensed mode for that license.

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	Description
`ClientDownloadPort`	Port used to download FortiClient from FortiClient EMS.
`RemoteManagementPort`	Port used for EMS administration.

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

FortiClient EMS is installed with 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.

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.

It is recommended to do a database edition upgrade outside normal production hours.

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*.

Testing the SQL server upgrade

It is recommended to run a short test on FortiClient EMS after the upgrade to verify proper operations. 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

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

Chromebook-only 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.

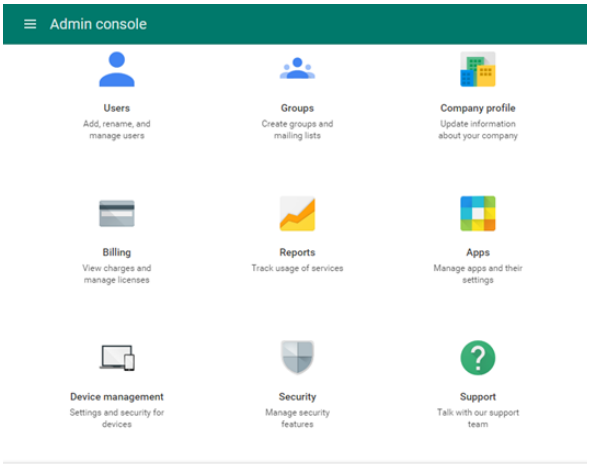
Following is a summary of how to set up the Google Admin console:

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 41.
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

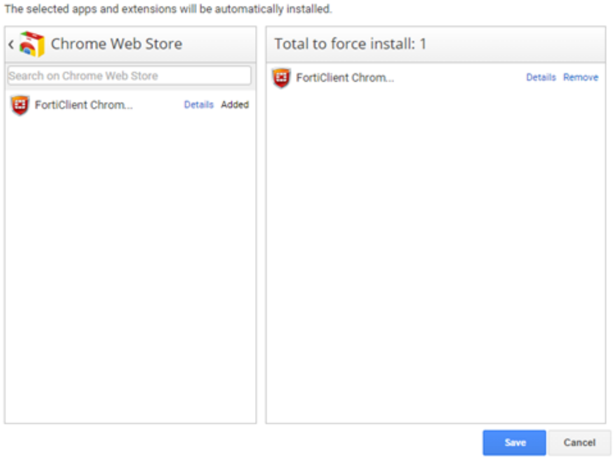
Log into the Google Admin console using your Google domain admin account. The Admin console displays.


≡ Admin console
Users
Add, rename, and manage users
Groups
Create groups and mailing lists
Company profile
Update information about your company
Billing
View charges and manage licenses
Reports
Track usage of services
Apps
Manage apps and their settings
Device management
Settings and security for devices
Security
Manage security features
Support
Talk with our support team

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: igbgpehnbmhgdgjbhkkpedommgmfbeao

1. In the Google Admin console, go to *Device management* > *Chrome Management* > *User Settings* > *Apps and Extensions* > *Force-installed Apps and Extensions* > *Manage force-installed apps*.
2. Select *Chrome Web Store*, and search for the following extension ID: igbgpehnbmhgdgjbhkkpedommgmfbeao.
3. Add the extension ID and save.
   The extension name displays as *FortiClient Chromebook Web Filter Extension*.



The selected apps and extensions will be automatically installed.

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 sent from the FortiClient Web Filter extensions.

FortiClient EMS is the profile server.

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 *Device management* > *Chrome Management* > *App Management* > *FortiClient Chrome Web Filter Extension* > *User settings*.
4. Click a domain or organizational unit (OU).
5. In the right pane, under *Configure*, upload a new configuration file. You can also view the current settings here.
6. Click *Save*.
7. Go to *Device Management* > *Chrome* > *App Management* to view your configured Chrome apps.

Adding root certificates

This section includes the following information:

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 SSL certificates to FortiClient EMS for Chromebook endpoints on page 180.

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 will 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 EMS 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 EMS supports logging to FortiAnalyzer. If you have a FortiAnalyzer and configure FortiClient EMS 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 SSL certificates 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 will 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 EMS.

In FortiAnalyzer CLI, enter the following command:

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

Adding SSL certificates 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 certificates for HTTPS connections

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

Summary of where to add certificates

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

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

Uploading root certificates to the Google Admin console

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

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

Disabling access to Chrome developer tools

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

1. In the Google Admin console, go to *Device management* > *Chrome Management* > *User Settings*.
2. 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. Incognito mode should be disallowed for managed Google domains.

1. In the Google Admin console, go to *Device management* > *Chrome management* > *User settings*.
2. From the left panel, select the organization.
3. In the *Security* section, set *Incognito Mode* to *Disallow incognito mode*.
4. Click *Save*.

Disallowing guest mode

You should disallow guest mode for managed Google domains.

1. In the Google Admin console, go to *Device management* > *Chrome management* > *Device settings* > *Sign-in settings*.
2. From the left panel, select the organization.
3. Under *Guest Mode*, select *Do not allow guest mode* from the *Allow Guest Mode* dropdown list.
4. Click *Save*.

Blocking Task Manager

You should block Task Manager for managed Google domains.

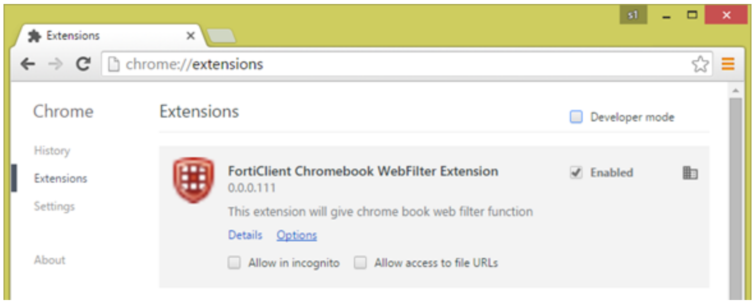
1. In the Google Admin console, go to *Device Management* > *Chrome Management* > *User settings* > *Apps and Extensions*.
2. From the left panel, select the organization.

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.

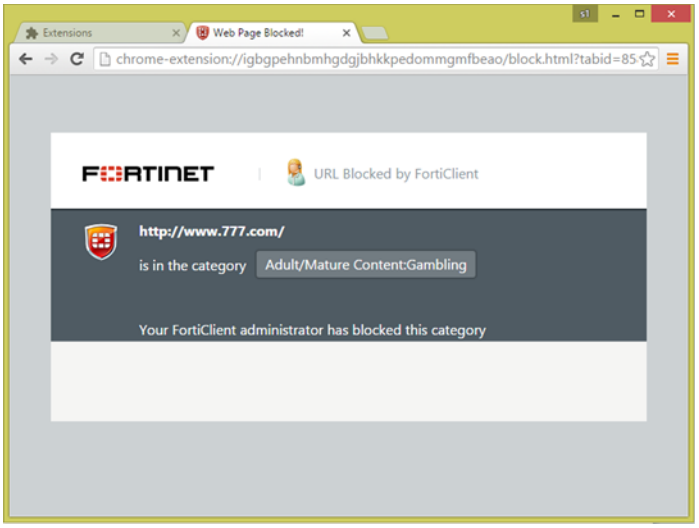
1. Open the Google Chrome browser.
2. Enter the following in the address bar: *chrome://extensions*



Extensions □ Developer mode

FortiClient Chromebook WebFilter Extension
0.0.0.111
This extension will give chrome book web filter function
Details Options
☑ Enabled
□ Allow in incognito □ Allow access to file URLs

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



chrome-extension://igbgpehnbmhgdgjbhkkpedommgmfbeao/block.html?tabid=85

FORTINET | URL Blocked by FortiClient

http://www.777.com/
is in the category Adult/Mature Content:Gambling

Your FortiClient administrator has blocked this category

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 50.

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:

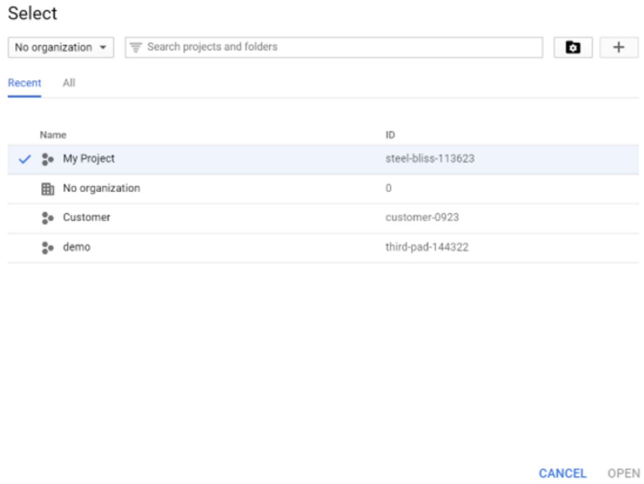
1. Create unique service account credentials using the Google Developer console. See Creating unique service account credentials on page 46.
2. Add the unique service account credentials to the Google Admin console. See Adding service account credentials to the Google Admin console on page 50.
3. Add the unique service account credentials to FortiClient EMS. See Adding service account credentials to EMS on page 50.

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



Select

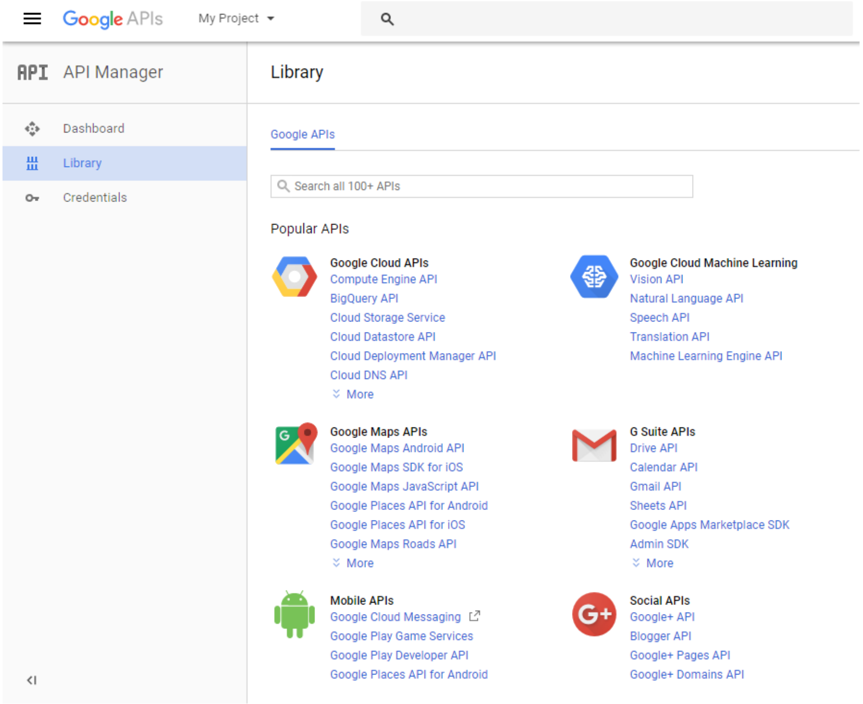
No organization ▾ | Search projects and folders

Recent | All

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

CANCEL OPEN

   b. Select your organization, if you see an organization dropdown list.
   c. Click the + button.
   d. In the *Project name* field, enter your project name, then click *Create*.
4. Enable the Admin SDK:
   a. Select your project from the toolbar list, then go to the *Library* tab.
   b. Under *G Suite APIs*, click *Admin SDK*.



Google APIs | My Project ▾

API Manager | Library

Dashboard
Library
Credentials

Google APIs

Search all 100+ APIs

Popular APIs

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

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

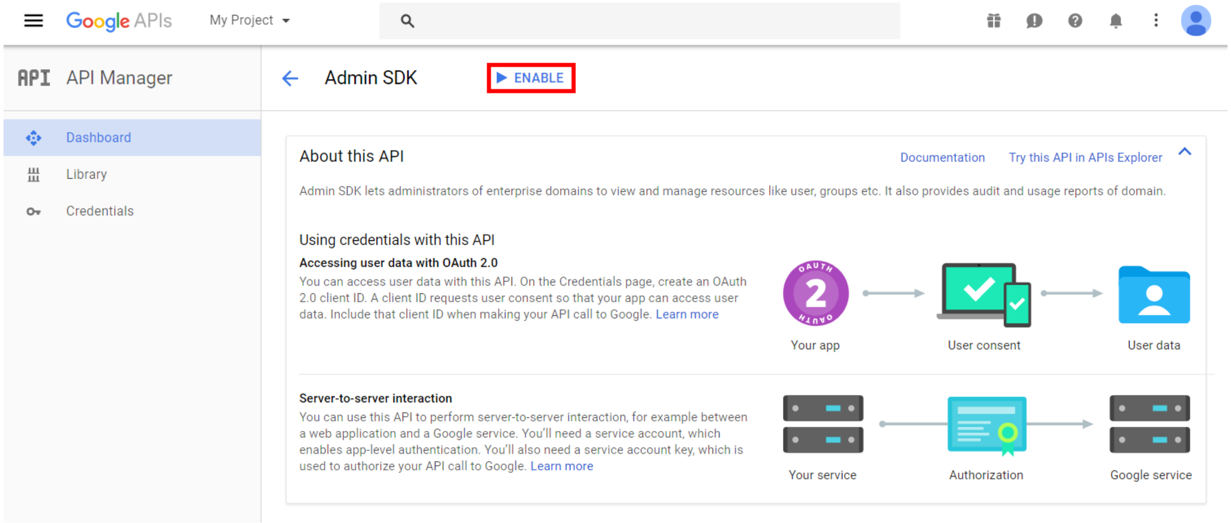
Google Maps APIs
Google Maps Android API
Google Maps SDK for iOS
Google Maps JavaScript API
Google Places API for Android
Google Places API for iOS
Google Maps Roads API
More

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

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

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

c. Click *ENABLE*.



About this API

Admin SDK lets administrators of enterprise domains to view and manage resources like user, groups etc. It also provides audit and usage reports of domain.

Using credentials with this API

Accessing user data with OAuth 2.0

You can access user data with this API. On the Credentials page, create an OAuth 2.0 client ID. A client ID requests user consent so that your app can access user data. Include that client ID when making your API call to Google. Learn more

Server-to-server interaction

You can use this API to perform server-to-server interaction, for example between a web application and a Google service. You'll need a service account, which enables app-level authentication. You'll also need a service account key, which is used to authorize your API call to Google. Learn more

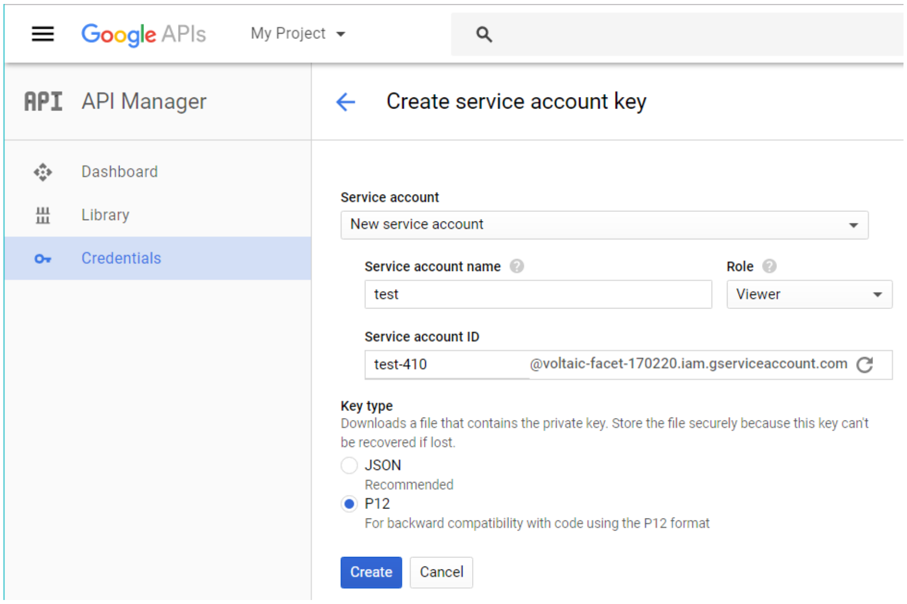
5. Create a service account:

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

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

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

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



Create service account key

Service account: New service account

Service account name: test

Role: Viewer

Service account ID: test-410 @voltaic-facet-170220.iam.gserviceaccount.com

Key type

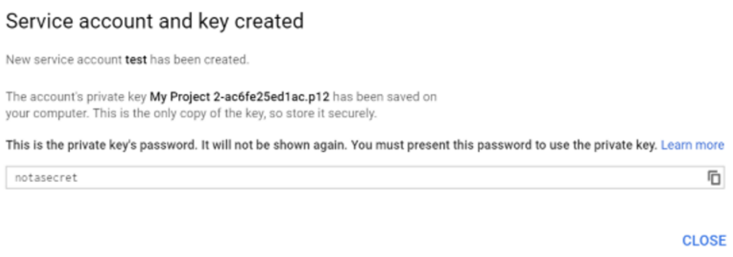
Downloads a file that contains the private key. Store the file securely because this key can't be recovered if lost.

○ JSON
Recommended

● P12
For backward compatibility with code using the P12 format

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 will 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

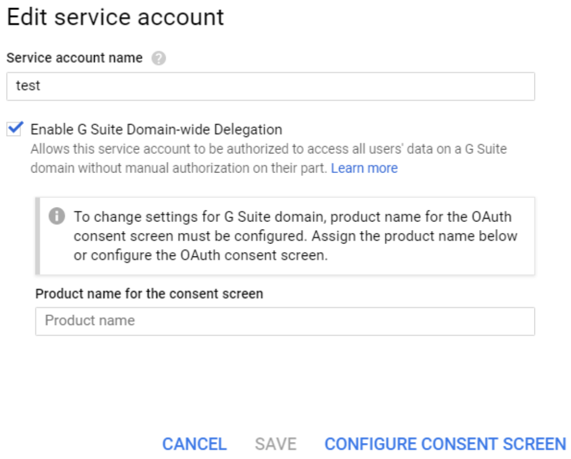
New service account **test** has been created.

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

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

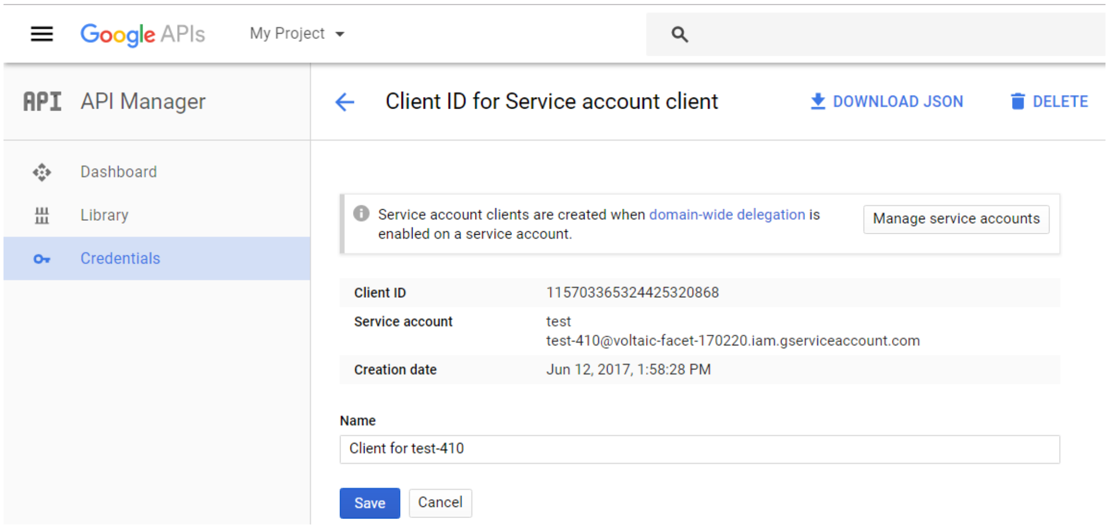
Service account name: test

☑ 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

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

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).



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

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

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 *Browse* 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 *Release Notes* and other resources.
	Technical Documentation	Link to the FortiClient EMS documentation.
	How-To Videos	Link to the Fortinet Video Library.
	Forums	Link to Fortinet Customer Service and Support forum.
	Product Videos	Links to the following FortiClient EMS videos: • Introduction to FortiClient EMS: introductory video for FortiClient EMS, which gives an overview of features, modes, and system requirements for FortiClient EMS 1.0. • How to License FortiClient EMS: shows how to license or renew FortiClient EMS 1.0 with more endpoints. • Adding a Domain to FortiClient EMS: shows how to add an AD domain to FortiClient EMS
	Create Support Package	Create a support package to provide to the Fortinet technical support team for troubleshooting.
	FortiGuard	View list of engine and signature versions for this version of FortiClient EMS.
Bell icon		Click the bell icon to display all alert logs.
<Logged in username>		Click the dropdown list beside the <logged in username> to do one of the following: • Change the password for this user. Enter a new password that complies with the displayed rules. • Log out of FortiClient EMS.

Left pane

The left navigation pane is used to display content in the right content 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 *EMS for Chromebooks Settings* option is enabled in *System Settings* > *Server*.
Endpoints		
	All Endpoints	Manage all endpoints.
	Manage Domains	Add and manage AD domains.
	Domains	Manage endpoints from AD domains. You can also add an AD domain if none exist.
	Workgroups	Manage endpoints from workgroups.
	Group Assignment Rules	Configure rules to automatically place endpoints into custom groups based on their installer ID, IP address, or OS.
Google Domains		Only available if the *EMS for Chromebooks Settings* option is enabled in *System Settings* > *Server*.
	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.
	Whitelist	View and delete allowlisted files from the *Whitelist* 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 *EMS for Chromebooks Settings* option is enabled in *System Settings > Server*.
Endpoint Profiles		
	Manage Profiles	Create profiles and manage profile updates for all profiles.
	Local Profiles	Create profiles and manage profile updates for local Windows, macOS, and Linux profiles.
	Local Chromebook Profiles	Create profiles and manage profile updates for local Chromebook profiles. Only available if the *EMS for Chromebooks Settings* option is enabled in *System Settings > Server*.
Manage Installers		
	Deployment Packages	Add and manage FortiClient deployment packages.
	FortiClient Installers	View FortiClient installers available from FortiGuard. Add custom installers.
Profile Components		
	Manage CA Certificates	Import CA certificates into FortiClient EMS.
Telemetry Gateway Lists		Create and assign Telemetry gateway 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 through the FSSO protocol, 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. This is used to authenticate FortiClient EMS administrators.
	User Settings	Configure the inactivity timeout and other user settings.
	Back up Database	Back up the FortiClient EMS database.
	Restore Database	Restore the FortiClient EMS database.

Option		Description
	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.
	FortiGuard	Configure the FortiGuard server location. Configure the FortiManager to use for client software/signature updates.
	Endpoints	Configure endpoint settings.
	Login Banner	Enable the pre-login banner to display a message to a user logging into FortiClient EMS.
	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

Content pane

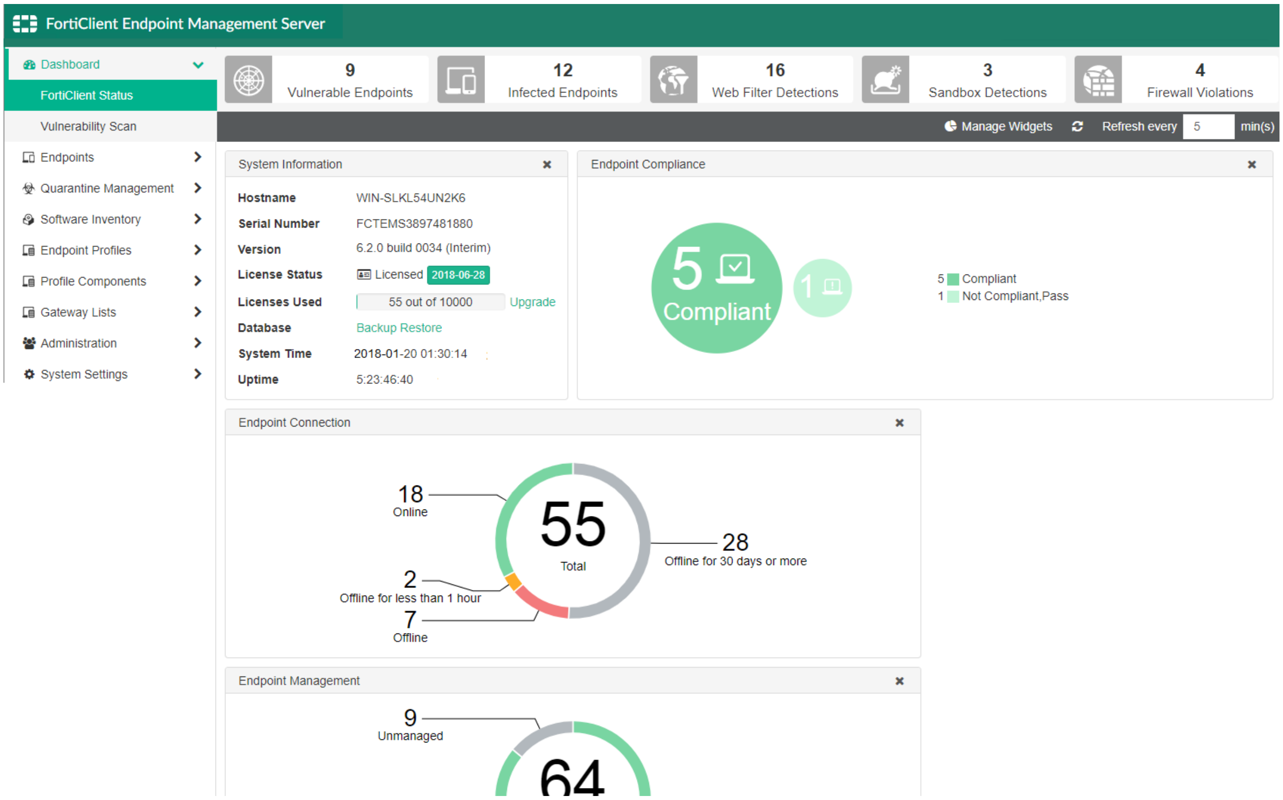
The right content pane displays the user interface controls that correspond to the selection made in the left pane. The status and menu icons in the top-right display controls what you can use to configure additional settings for user management and each individual endpoint.

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

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 57 and FortiClient Status charts and widgets on page 58.



Hostname	WIN-SLKL54UN2K6
Serial Number	FCTEMS3897481880
Version	6.2.0 build 0034 (Interim)
License Status	Licensed 2018-06-28
Licenses Used	55 out of 10000 Upgrade
Database	Backup Restore
System Time	2018-01-20 01:30:14
Uptime	5:23:46:40

2. Click an event summary.
   The list of endpoints for the summary displays.
3. Click the *Back* button to return to the *FortiClient Status* pane.
4. Click a pie chart.
   The *Endpoints* content pane displays with more details about the endpoints related to the pie charts. See also Viewing the Endpoints content pane on page 73.

System Information widget

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

Option	Description
Hostname	Name of the computer on which FortiClient EMS is installed.
Serial Number	Serial number for FortiClient EMS.
Version	Version number for FortiClient EMS. Also displays the build number. If the current build is an interim build, also displays *(Interim)* beside the build number.
Database	Options to back up and restore the database. Click *Backup* to back up the database. Click *Restore* to restore a backed up database.
System Time	Time and date used by the computer on which FortiClient EMS is installed.
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
FortiCare Support Account	FortiCare account that this EMS server is registered to. If EMS is not registered to a FortiCare account, you can log into an existing FortiCare account or create a new FortiCare account 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.
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. This license is used 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 *Activate* to upload your license file. If you have a non-expired license, but want to upgrade your license, click the *Upgrade* button to upgrade your license file. If your current license is expiring, the *Renew* button is enabled for you to upload your new license file. See License status on page 36.

FortiClient Status charts and widgets

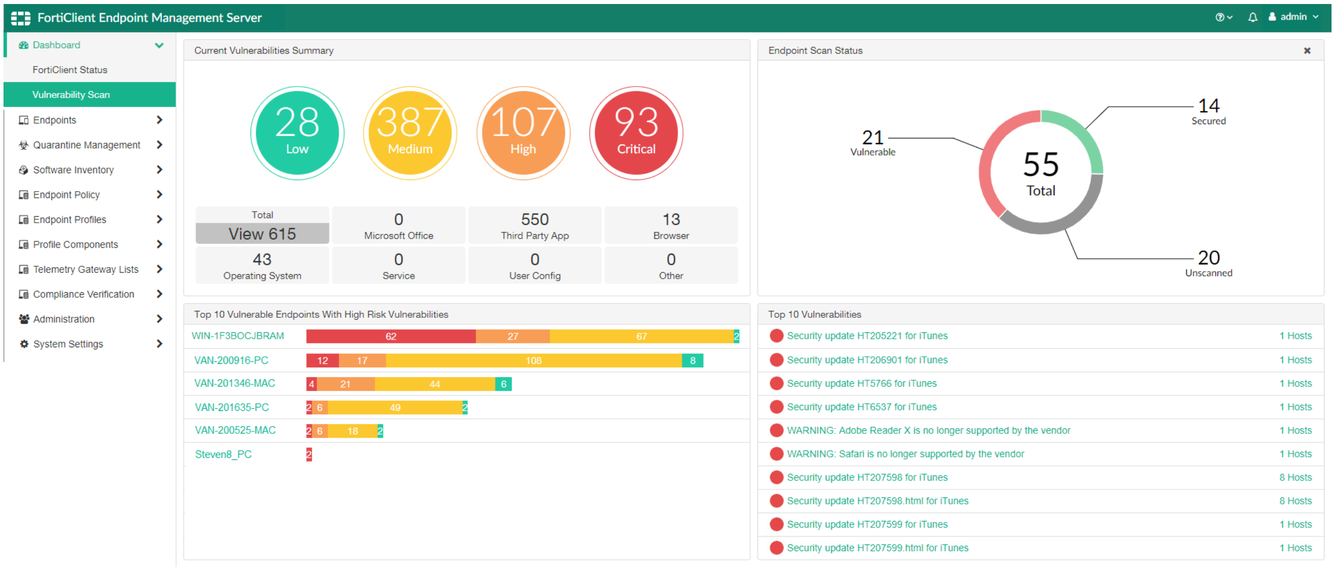
FortiClient Status displays a number of pie charts. Each pie chart provides a summary of endpoint information. The sections in each chart are links. You can click any section of the pie charts or any row in the table to display more details.

Option	Description
Endpoint Charts	
Endpoint Activity	Shows a summary of endpoint activity information. Categories are: • FortiGate On-net • FortiGate Off-net • FortiGate Offline • FortiGate Not Registered • EMS On-net • EMS Off-net
Endpoint Alerts	Shows the number of endpoints with alerts, including pending software updates, out-of-date protection, and out-of-sync profiles.
Endpoint Connection	Shows the number of endpoints that are: • Online • Offline for less than one hour • Offline • Offline for 30 days or more
Managed Mac FortiClient Versions	This chart indicates the percentage of macOS endpoints with each version of FortiClient installed. Sorting by version lists FortiClient versions from most recent to least recent. For example, FortiClient 6.2.0 is listed first, then FortiClient 6.0.0, and so on. Sorting by count lists FortiClient versions from the version with the largest number of endpoints to the version with the smallest number of endpoints. For example, if there are 600 endpoints with FortiClient 6.0.0 installed and 40 endpoints with FortiClient 6.2.0 installed, FortiClient 6.0.0 is listed first.
Managed Windows FortiClient Versions	This chart indicates the percentage of Windows endpoints with each version of FortiClient installed. You can sort the data by version or count. Sorting by version lists FortiClient versions from most recent to least recent. For example, FortiClient 6.2.0 is listed first, then FortiClient 6.0.0, and so on. Sorting by count lists FortiClient versions from the version with the largest number of endpoints to the version with the smallest number of endpoints. For example, if there are 600 endpoints with FortiClient 6.0.0 installed and 40 endpoints with FortiClient 6.2.0 installed, FortiClient 6.0.0 is listed first.
Managed Linux FortiClient Versions	This chart indicates the percentage of Linux endpoints with each version of FortiClient installed. You can sort the data by version or count.
Endpoint Management	This chart indicates how many endpoints are disconnected and connected.

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



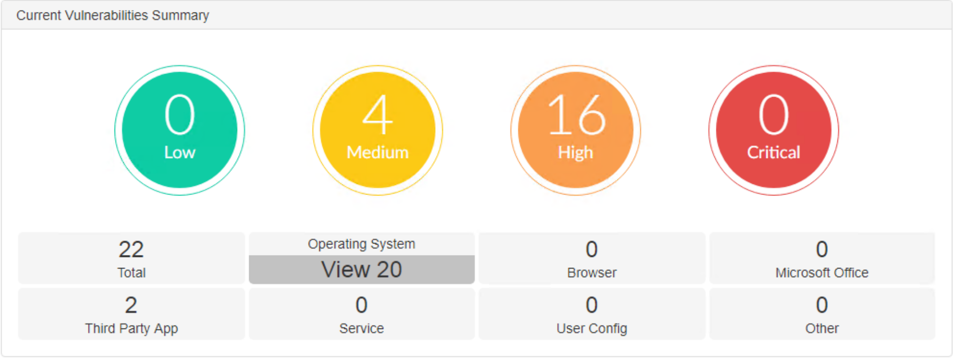
● Security update HT205221 for iTunes	1 Hosts
● Security update HT206901 for iTunes	1 Hosts
● Security update HT5766 for iTunes	1 Hosts
● Security update HT6537 for iTunes	1 Hosts
● WARNING: Adobe Reader X is no longer supported by the vendor	1 Hosts
● WARNING: Safari is no longer supported by the vendor	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

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

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

Viewing current vulnerabilities

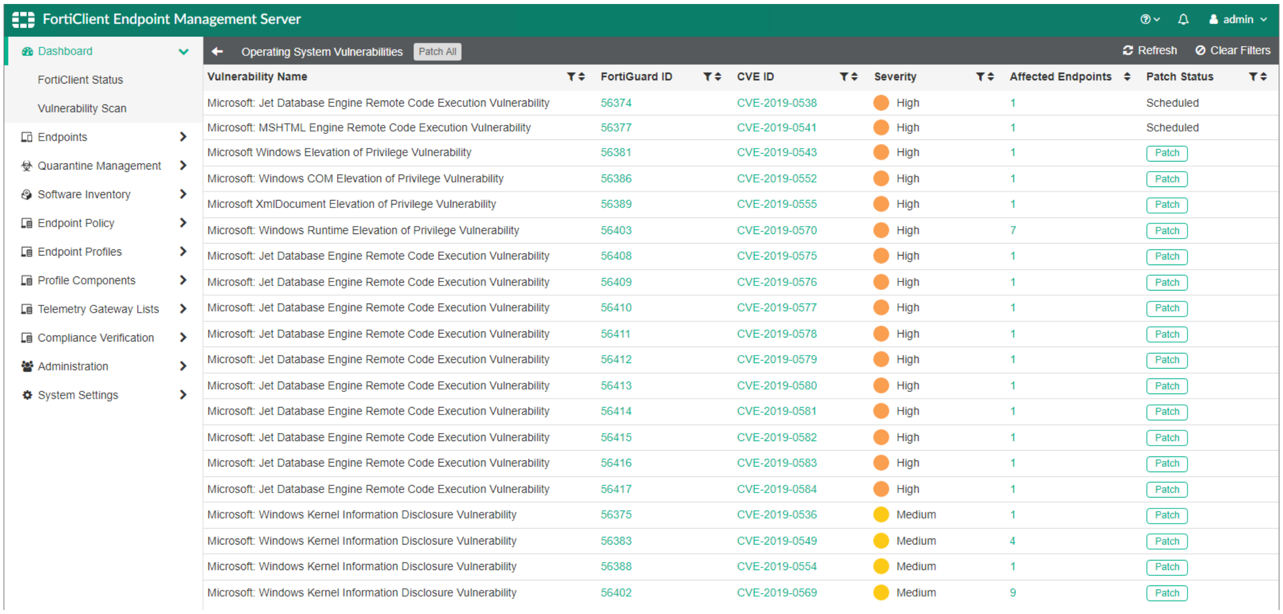
1. Go to *Dashboard* > *Vulnerability Scan*.
2. Under *Current Vulnerabilities Summary*, click a vulnerability tile.
3. When you click a vulnerability tile, the colored circles update to display the number of vulnerabilities that correspond to each severity level in the selected category.
   In this 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:



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

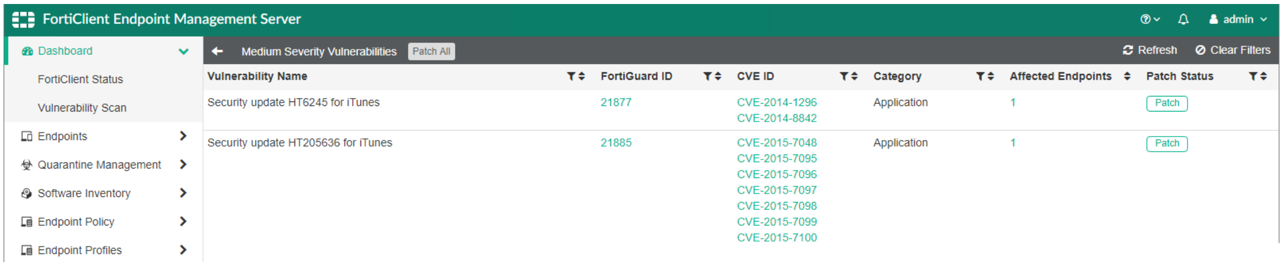
Patch All	Click this button to patch all vulnerabilities currently displayed on the content pane. The vulnerabilities are patched with the next Telemetry communication between FortiClient EMS and the endpoint.

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

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.

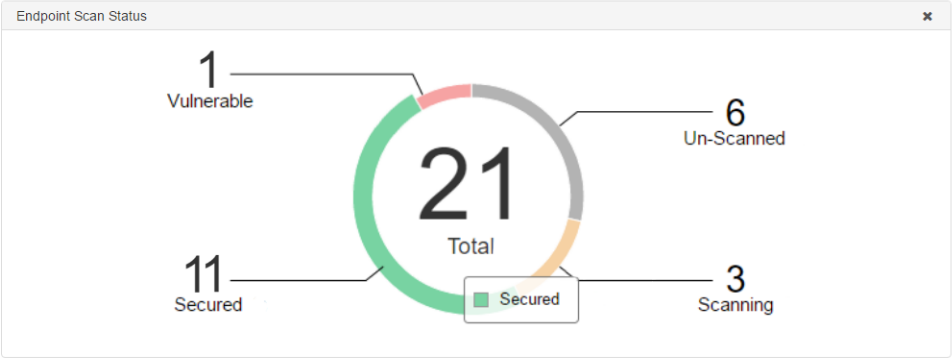
5. Return to *Dashboard* > *Vulnerability Scan*. You can also click a colored circle to view all vulnerabilities of the selected severity level. The following shows all medium severity third party application vulnerabilities:



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

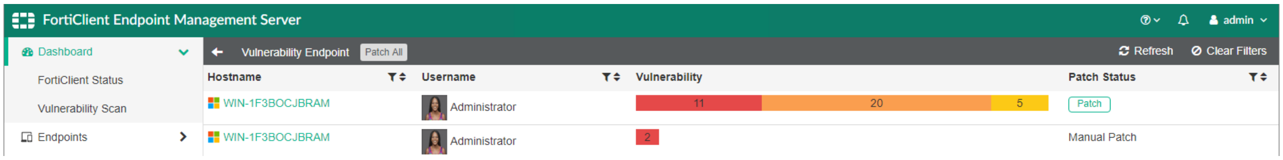
1. Go to *Dashboard* > *Vulnerability Scan*.



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:



Hostname	Username	Vulnerability	Patch Status
WIN-1F3BOCJBRAM	Administrator	11 20 5	Patch
WIN-1F3BOCJBRAM	Administrator	2	Manual Patch

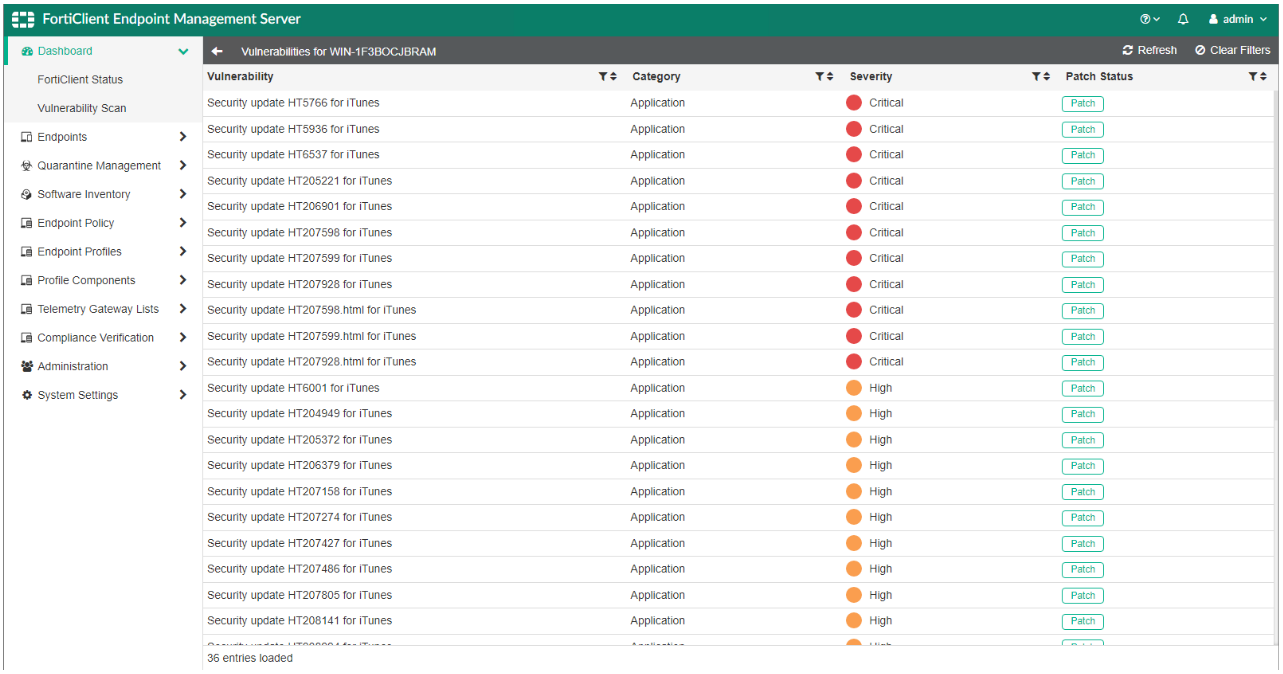
Patch All	Click this button to patch all vulnerabilities currently displayed on the content pane. The vulnerabilities are patched with the next Telemetry communication between FortiClient EMS and the endpoint.
Refresh	Click to refresh the list of vulnerabilities in the content pane.
Clear Filters	Click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

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

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.

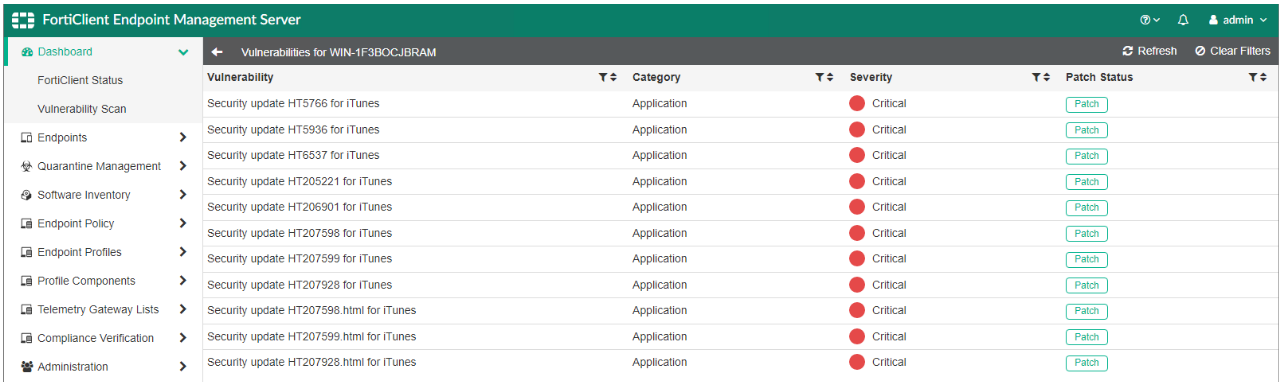
3. Click a hostname. You can view all vulnerabilities detected on that endpoint. You can filter the list of vulnerabilities in the same way that you can filter the list of vulnerable endpoints in step 2.



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.



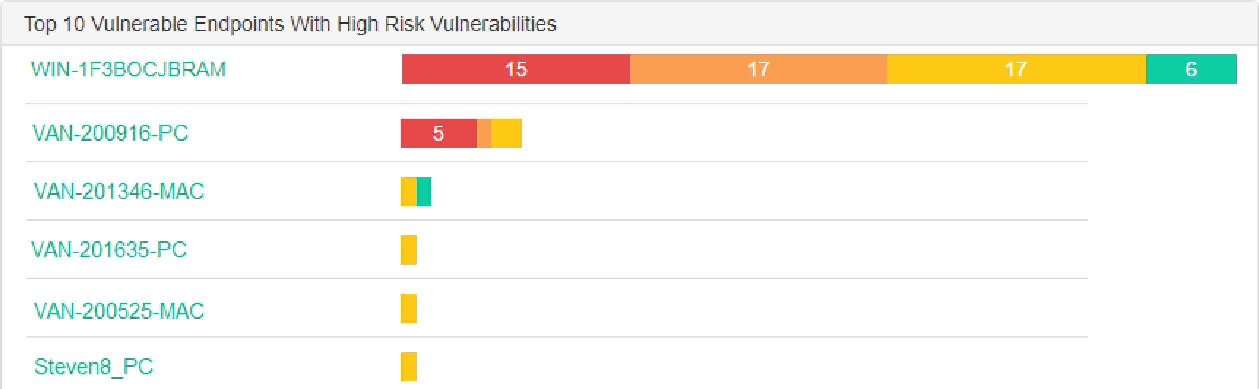
Vulnerability	Category	Severity	Patch Status
Security update HT5766 for iTunes	Application	Critical	Patch
Security update HT5936 for iTunes	Application	Critical	Patch
Security update HT6537 for iTunes	Application	Critical	Patch
Security update HT205221 for iTunes	Application	Critical	Patch
Security update 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	You can click the *Patch* button to patch the selected vulnerability with the next Telemetry communication between FortiClient EMS and the endpoint. If a patch is already scheduled for the vulnerability, this column displays *Scheduled*. If the vulnerability must be patched manually, this column displays *Manual Patch*.

Viewing the top 10 vulnerable endpoints with high risk vulnerabilities

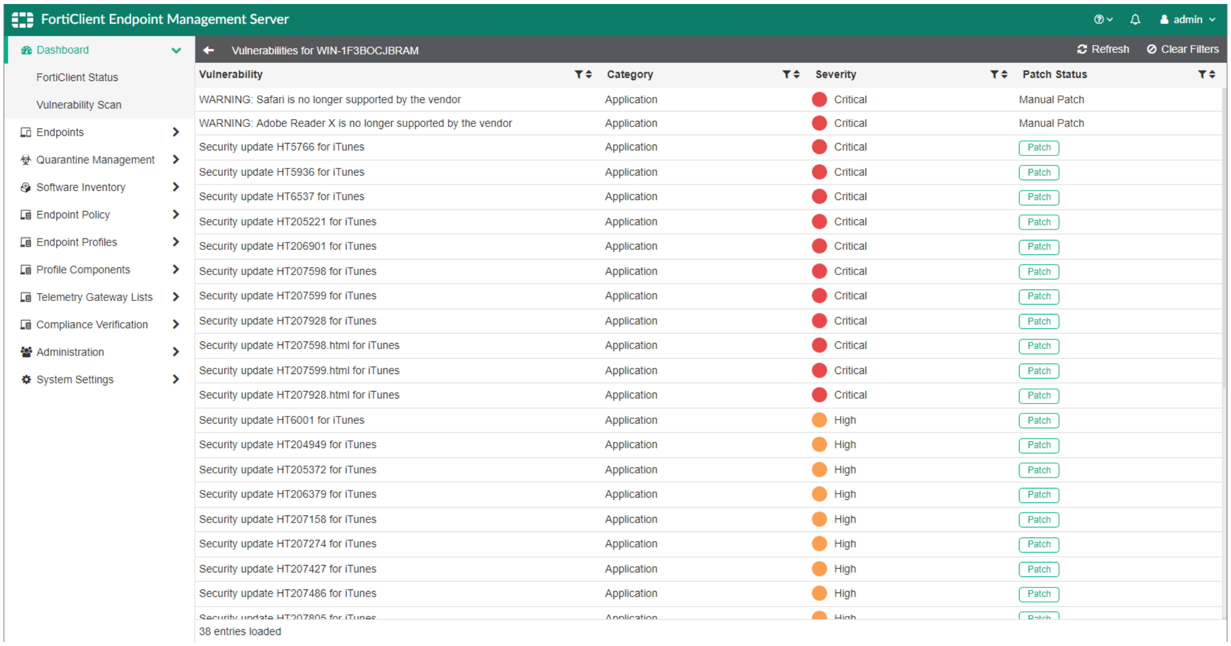
1. Go to *Dashboard* > *Vulnerability Scan*. The *Top 10 Vulnerable Endpoints With High Risk Vulnerabilities* chart displays vulnerabilities per endpoint in a segmented bar graph and organized by severity.



WIN-1F3BOCJBRAM has the following:

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

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



Vulnerabilities for WIN-1F3BOCJBRAM

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

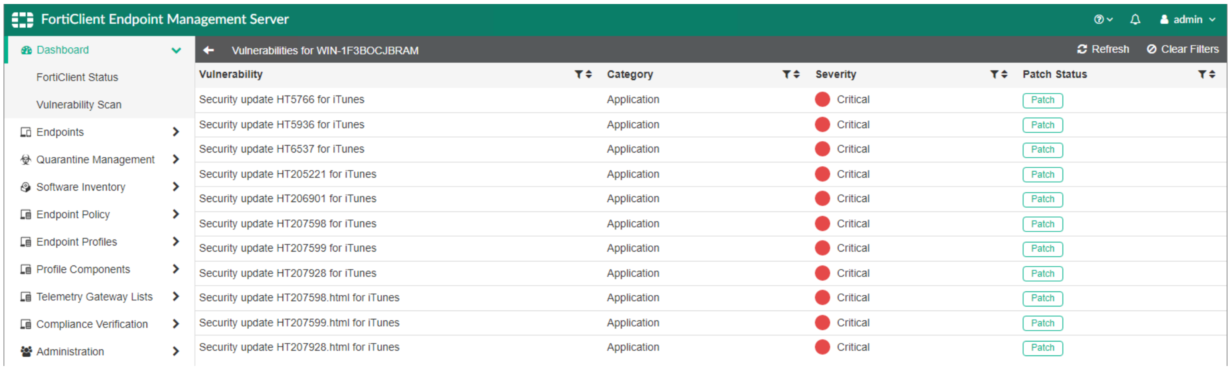
Vulnerability	Name of the vulnerability.
Category	Category of the vulnerability.
Severity	Severity level of the vulnerability.
Patch Status	You can click the *Patch* button to patch the selected vulnerability with the next Telemetry communication between FortiClient EMS and the endpoint. If a patch is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

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.

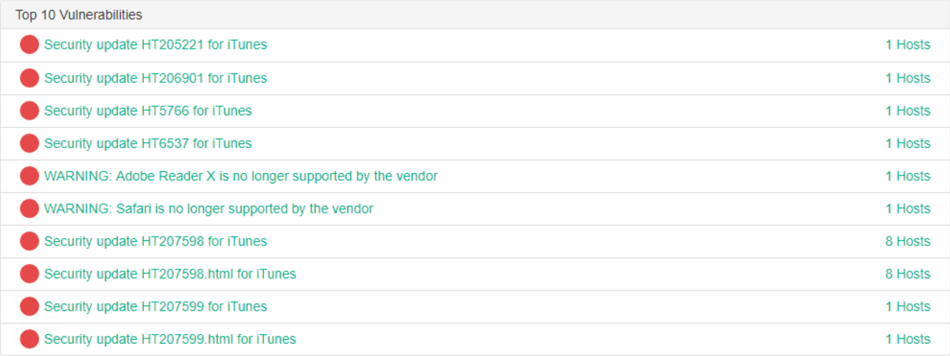
You can filter the list of vulnerabilities in the same way that you can filter the list of vulnerabilities in option a.



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

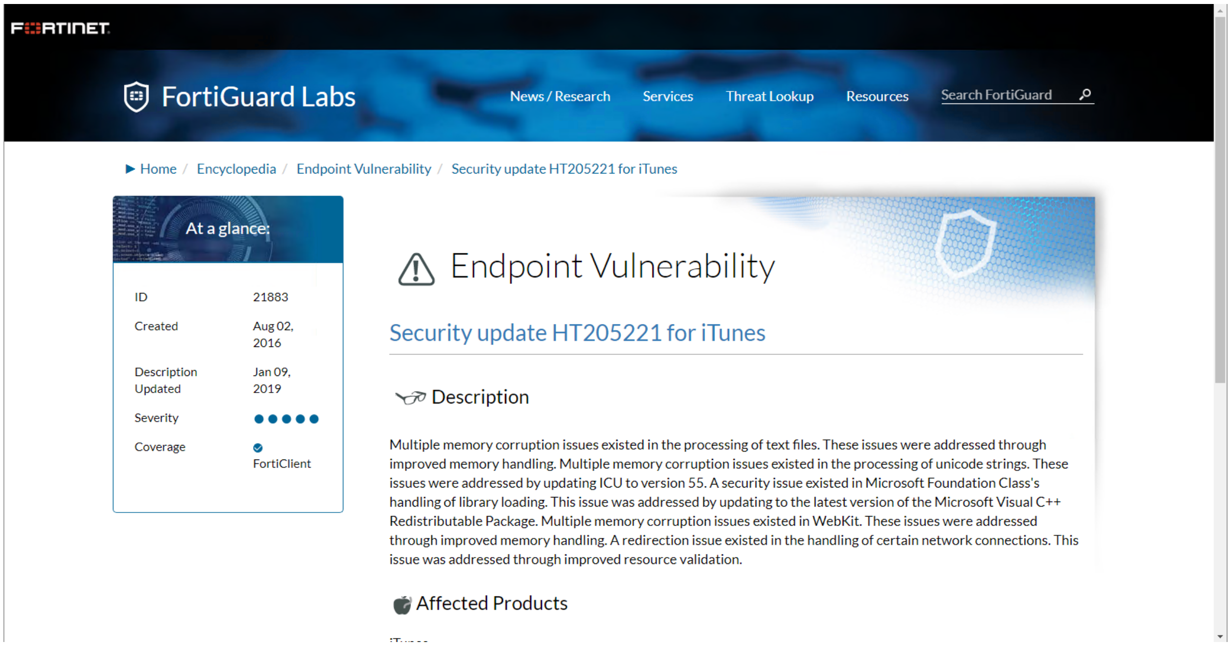
Viewing top ten vulnerabilities on endpoints

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.



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

Endpoint Vulnerability

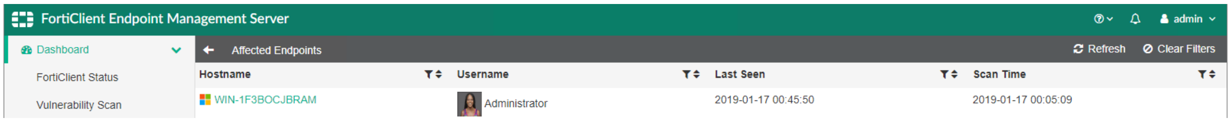
Security update HT205221 for iTunes

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.



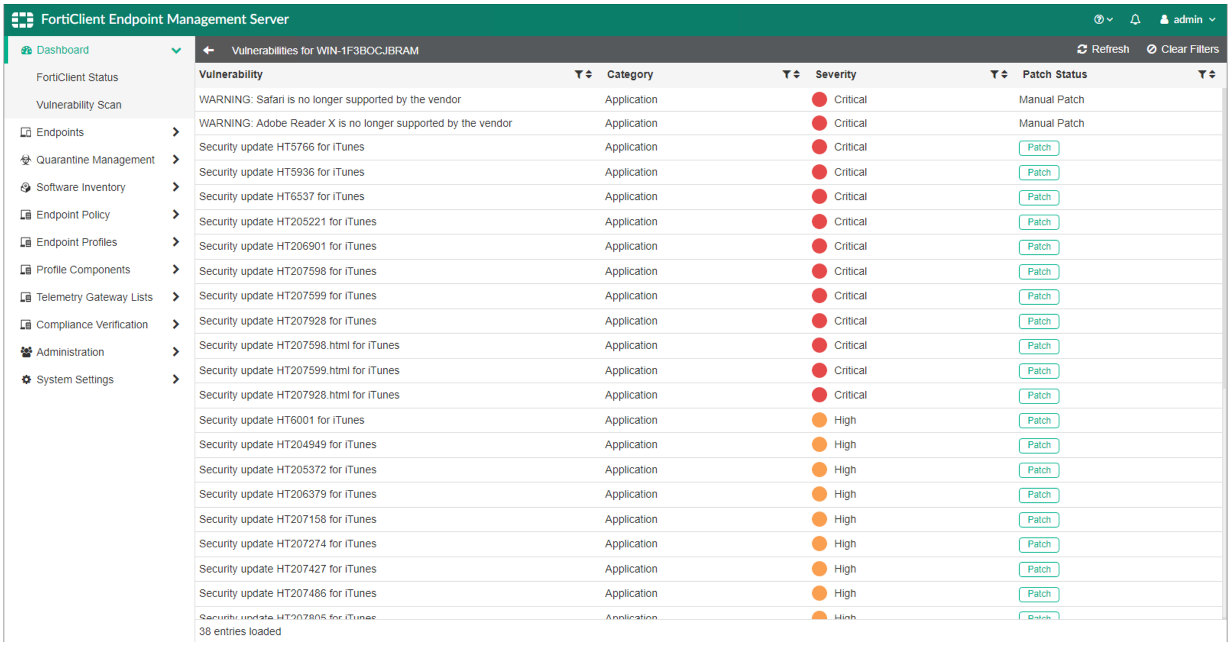
Hostname	Username	Last Seen	Scan Time
WIN-1F3BOCJBRAM	Administrator	2019-01-17 00:45:50	2019-01-17 00:05:09

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.



Vulnerabilities for WIN-1F3BOCJBRAM

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

Viewing Chromebook Status

Chromebook Status displays a number of pie charts. Each pie chart provides a summary of Chromebook 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. Chromebook Status is only available if *EMS for Chromebooks Settings* is selected in *System Settings > Server*.

Option	Description
User Charts	
Active Users	This chart displays the active and inactive users.
Managed Users	This chart displays the managed and unmanaged users.

Option	Description
Webfilter Charts	
Top 10 Violations by Category	The chart displays the top ten web filter violations by category in the past few days. You can configure the number of days. Go to *System Settings* > *Logs*.
Top 10 Violations by User	The chart displays the top web filter violations by user in the past few days. You can configure the number of days. Go to *System Settings* > *Logs*.
Others	
System Information	This widget displays summary information for the system.

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.

Creating 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* box, 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* box, 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.

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's IP address or hostname.
Port	Enter the port number.
Distinguished name	Enter the distinguished name (optional). You must use only capital letters when configuring the DN.
Bind type	Select the bind type: *Simple*, *Anonymous*, or *Regular*. When you select *Regular*, you must enter the *Username* and *Password*.
Username	Available when *Bind type* is set to *Regular*. Enter the username.
Password	Available when *Bind type* is set to *Regular*. Enter the user password.
Show Password	Available when *Bind type* is set to *Regular*. Turn on and off to show or hide the password.
LDAPS connection	Turn on to enable a secure connection protocol when *Bind Type* is set to *Regular*.
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 is successful, select *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* box, 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.

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

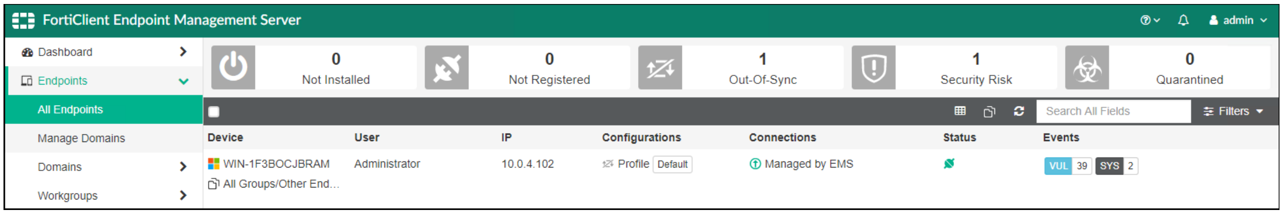
Viewing endpoints

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 content pane

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

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

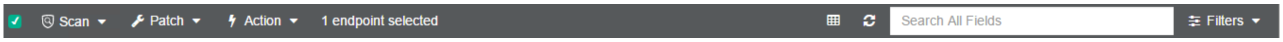


Device	User	IP	Configurations	Connections	Status	Events
WIN-1F3BOCJBRAM All Groups/Other End...	Administrator	10.0.4.102	Profile Default	Managed by EMS		VUL 39 SYS 2

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.
Checkbox	Click to select all endpoints displayed in the content pane.
Show/Hide Heading	Click to hide or display the following column headings: *Device*, *User*, *IP*, *Configurations*, *Connections*, *Status*, and *Events*.
Show/Hide Full Group Path	Click to hide or display the full path for the group that the endpoint belongs to.
Refresh	Click to refresh the list of endpoints.
Search All Fields	Enter a value and press *Enter* to search for the value in the list of endpoints.
Filters	Click to display and hide filters you can use to filter the list of endpoints.
Device	Visible when headings are displayed. Displays an icon to represent the OS on the endpoint, the hostname, and the endpoint group.
User	Visible when headings are displayed. Displays the name 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 profile and Telemetry gateway list assigned to the endpoint and their synchronization statuses.
Connections	Visible when headings are displayed. Displays the connection status between FortiClient and FortiClient EMS: *Managed by EMS* or *Not Managed*. If the endpoint is connected to a FortiGate, displays *FortiTelemetry to <FortiGate hostname>*.
Status	Visible when headings are displayed. Displays one of the following Telemetry statuses for the endpoint. • Registered • Quarantined • Excluded • Not registered
Events	Visible when headings are displayed. Displays FortiClient events for the endpoint.

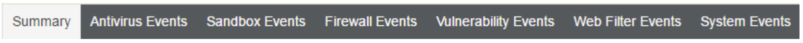
2. Click an endpoint to display its details in the content pane. The following dropdown lists display in the toolbar for the selected endpoint:



Checkbox	Click to select and deselect all endpoints in the content pane. You can then select or clear the checkbox for individual endpoints to fine-tune the list of selected endpoints.
Scan	Click to start a Vulnerability or AV scan on the selected endpoint.

Patch	Click to patch all critical and high vulnerabilities on the selected endpoint. Choose one of the following options: • Selected Vulnerabilities on Selected Clients • Selected Vulnerabilities on All Affected Clients • All Critical and High Vulnerabilities
Action	Click to perform one of the following actions on the selected endpoint: • Upload FortiClient Logs • Request Diagnostic Results • Update Signatures • Re-register • Deregister • Register • Quarantine • Un-quarantine • Exclude from Management • Clear Events • Mark as Uninstalled • Delete Device

The following tabs are available in the content pane toolbar when you select an endpoint, depending on which FortiClient features have been 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.
	Device	Displays the selected endpoint's hostname.
	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 onnet or offnet.
	Host Verification Tags	Displays which tags have been applied to the endpoint based on the compliance verification rules. See Compliance Verification on page 155.

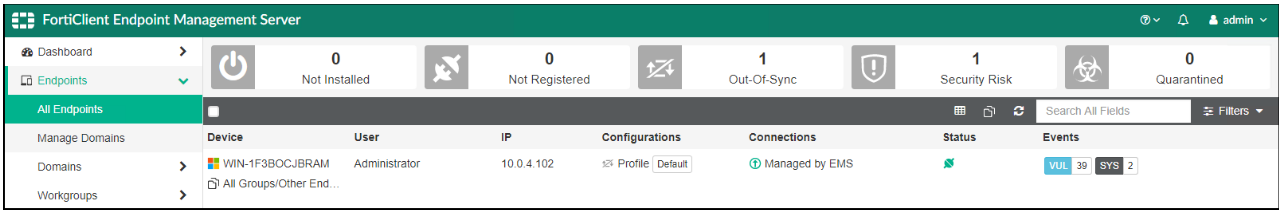
	Connection	Displays the connection status between the selected endpoint and FortiClient EMS and between the endpoint and FortiGate.
	Configuration	Displays the following information for the selected endpoint: • Profile: Name of the profile assigned to the selected endpoint • Installer: Name of the FortiClient installer used for the selected endpoint. Displays *Not Assigned* if no FortiClient installer has been assigned to the selected endpoint. • Telemetry Gateway List: Name of the Telemetry gateway list used for the selected endpoint. Displays *Not Assigned* 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.
	Status	Displays if the endpoint is registered to EMS.
	Features	Displays which features are enabled for FortiClient.
Antivirus Events		
	Date	Displays the AV event's date and time.
	Message	Displays the AV event's message.
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. This option is only available for an on-premise FortiSandbox appliance.
	Malware	Displays the malware name. This option is only available for an on-premise FortiSandbox appliance.
	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 80.
Firewall Events		
	Date	Displays the firewall event's date and time.
	Message	Displays the firewall event's message.
Web Filter Events		
	Date	Displays the web filter event's date and time.
	Message	Displays the web filter event's message.

Vulnerability Events		
	Vulnerability	Displays the vulnerability's name. For example, *Security update available for Adobe Reader*.
	Category	Displays the vulnerability's category. For example, *Third Party App*.
	Application	Displays the name of the application with the vulnerability.
	Severity	Displays the vulnerability's severity.
	Patch Type	Displays the patch type for this vulnerability: *Auto* or *Manual*.
	FortiGuard	Displays the FortiGuard ID number. If you click the FortiGuard ID number, it redirects you to FortiGuard where further information is provided if available.
	Bulletin	Displays a link to a bulletin about the software vulnerability.
System Events		
	Date	Displays the system event's date and time.
	Message	Displays the system event's message.

Using the quick status bar

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

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



Device	User	IP	Configurations	Connections	Status	Events
WIN-1F3BOCJBRAM All Groups/Other End...	Administrator	10.0.4.102	Profile Default	Managed by EMS		VUL 39 SYS 2

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 content pane on page 73.

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.

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. You can exclude a name or names from the filter using an exclamation mark (!).
	User	Enter the name of the user(s) to include in the filter. You can exclude a name or names from the filter using an exclamation mark (!).
	Group	Enter the name of the group(s) to include in the filter. You can also exclude a name or names from the filter using an exclamation mark (!).
	IP	Enter the IP address to include in the filter. You can exclude an IP address from the filter using an exclamation mark (!).
	OS	Enter the name of the operating system(s) to include in the filter. You can exclude a name or names from the filter using an exclamation mark (!).
	Tag	Enter the tag(s) to include in the filter. You can exclude a name or names from the filter using an exclamation mark (!).
FortiClient		Lists the filter options for FortiClient version numbers.
	Version	Enter the FortiClient version number to include in the filter. You can exclude a version or versions from the filter using an exclamation mark (!).
Installer		Lists the filter options for deployment.
	Name	Enter the name(s) of the installer to include in the filter. You can exclude a name or names from the filter using an exclamation mark (!).

	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.
Profile		
	Name	Enter the name(s) of the profile to include in the filter. You can also exclude a name or names from the filter by using an exclamation mark (!).
	Status	Click the profile status to include in the filter. Selected status buttons are green. Choose between *Synced* and *Out-Of-Sync*. Clear the status button to exclude the status from the filter. Excluded status buttons are gray.
Telemetry Gateway List		
	Name	Enter the name(s) of the Telemetry gateway list to include in the filter. You can also exclude a name or names from the filter by using an exclamation mark (!).
	Status	Click the Telemetry gateway list status to include in the filter. Selected status buttons are green. Choose between *Synced* and *Out-Of-Sync*. Clear the status button to exclude the status from the filter. Excluded status buttons are gray.
FortiTelemetry		
	Serial	Select the FortiGate serial number to include in the filter.
	Status	Click the status for FortiClient Telemetry connection to FortiGate to include in the filter. Choose between *Online*, *Offline*, and *Not Registered*.
EMS		
	Status	Click the status for FortiClient Telemetry connection to EMS to include in the filter. Selected status buttons are green. Choose between *Online*, *Offline*, and *Not Registered*. Clear the status button to exclude the status from the filter. Excluded status buttons are gray.
Status		Click the endpoint status to include in the filter. Selected status buttons are green. Choose between *Registered*, *Excluded*, *Not Registered*, *Quarantined*, and *Not Installed*. 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.

Bookmarks	Displays the list of saved filter settings. Displays only after you have saved a bookmark. Click the *Bookmark* button to name and save filter settings. Click a bookmark to use the saved settings. Click the *x* beside a bookmark to delete it.
Search	Click the *Search* button to apply the filter setting.
Reset	Click the *Reset* button to clear the filter settings.
Bookmark	Click the *Bookmark* button to save the filter settings as a bookmark.

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

Using bookmarks to filter the list of endpoints

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

To create bookmarks to filter endpoints:

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

To use bookmarks to filter the list of endpoints:

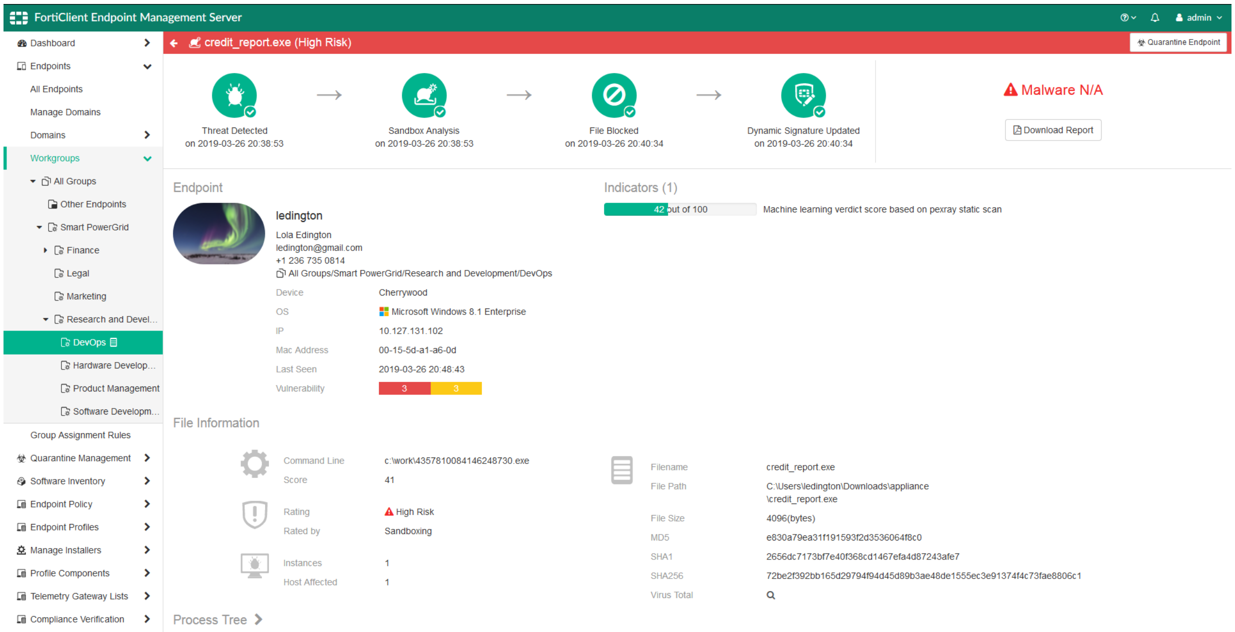
1. Go to *Endpoints*.
2. Click *All Endpoints*, a domain, or workgroup. The list of endpoints displays.
3. Click the *Filters* menu.
4. In the *Bookmarks* list, click a bookmark. The bookmark settings are used to filter the list of endpoints.

Viewing Sandbox event details

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

This option is only available when using an on-premise FortiSandbox appliance that you have configured a username and password for in the endpoint profile. FortiSandbox Cloud does not support this option. See Sandbox Detection on page 124.

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



credit_report.exe (High Risk)

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

Malware N/A

Endpoint

ledington
Lola Edington
ledington@gmail.com
+1 236 735 0814
All Groups/Smart PowerGrid/Research and Development/DevOps

Device	Cherrywood
OS	Microsoft Windows 8.1 Enterprise
IP	10.127.131.102
Mac Address	00-15-5d-a1-a6-0d
Last Seen	2019-03-26 20:48:43
Vulnerability	3 3

Indicators (1)

42 out of 100 Machine learning verdict score based on pexray static scan

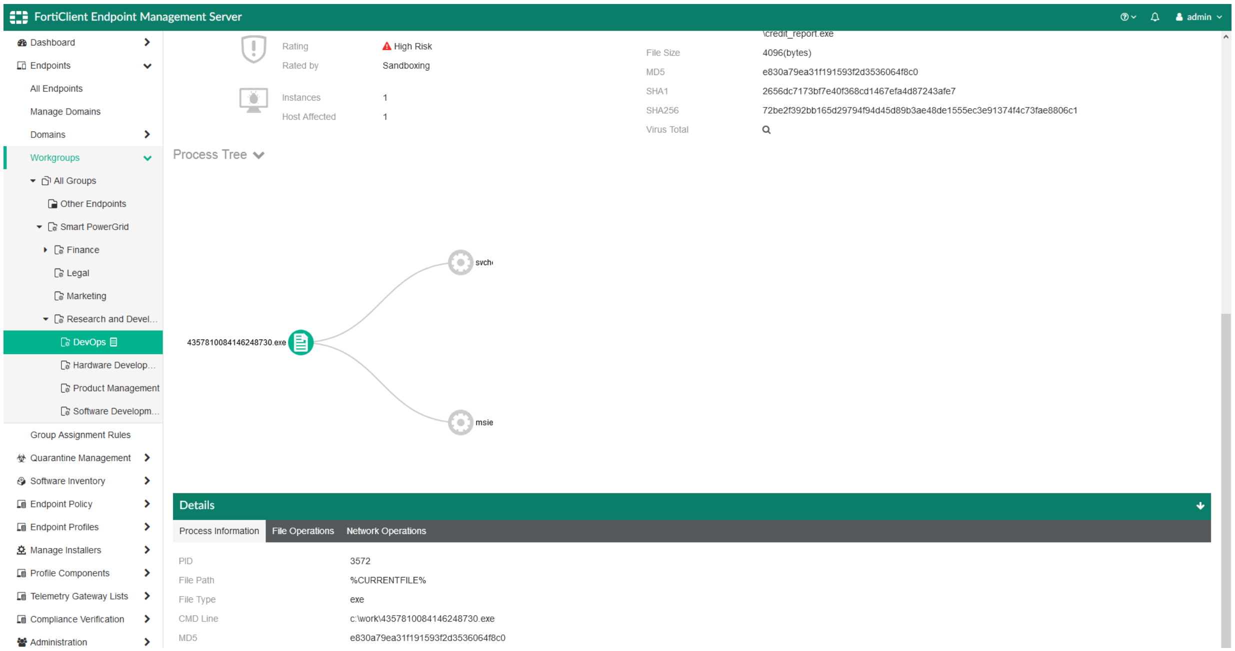
File Information

Command Line	c:\work\4357810084146248730.exe
Score	41
Rating	High Risk
Rated by	Sandboxing
Instances	1
Host Affected	1

Filename	credit_report.exe
File Path	C:\Users\ledington\Downloads\appliance \credit_report.exe
File Size	4096(bytes)
MD5	e830a79ea31f191593f2d3536064f8c0
SHA1	2656dc7173bf7e40f368cd1467efa4d87243afe7
SHA256	72be2f392bb165d29794f94d45d89b3ae48de1555ec3e91374f4c73fae8806c1
Virus Total	

Process Tree

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



Rating	High Risk
Rated by	Sandboxing
Instances	1
Host Affected	1

	\credit_report.exe
File Size	4096(bytes)
MD5	e830a79ea31f191593f2d3536064f8c0
SHA1	2656dc7173bf7e40f368cd1467efa4d87243afe7
SHA256	72be2f392bb165d29794f94d45d89b3ae48de1555ec3e91374f4c73fae8806c1
Virus Total	

Process Tree

PID	3572
File Path	%CURRENTFILE%
File Type	exe
CMD Line	c:\work\4357810084146248730.exe
MD5	e830a79ea31f191593f2d3536064f8c0

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 119.

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.

Disconnecting and connecting endpoints

You can manually disconnect and connect endpoints using EMS.

To disconnect endpoints:

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

To connect 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 *Register*. EMS connects the endpoint with the next FortiClient Telemetry communication.

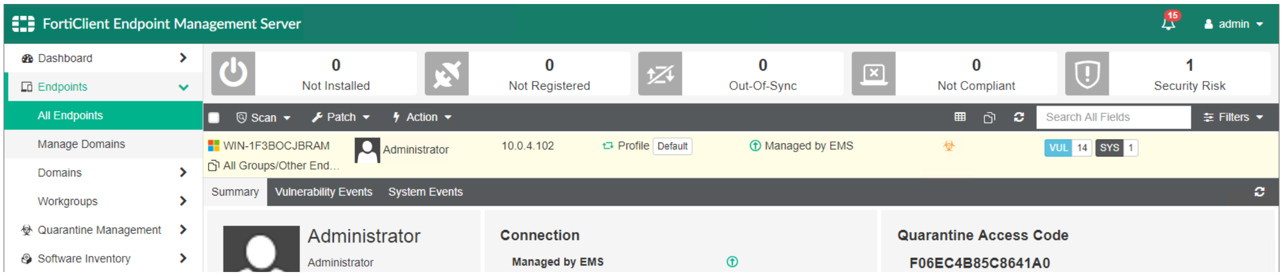
Quarantining endpoints

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

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

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

   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 as seen below.



FortiClient Endpoint Management Server

0 Not Installed | 0 Not Registered | 0 Out-Of-Sync | 0 Not Compliant | 1 Security Risk

WIN-1F3BOCJBRAM | Administrator | 10.0.4.102 | Profile Default | Managed by EMS | VUL 14 | SYS 1

All Groups/Other End...

Administrator

Administrator

Connection

Managed by EMS

Quarantine Access Code

F06EC4B85C8641A0

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 both EMS and the FortiGate.

EMS

1. You must create a profile for the endpoint. See Creating profiles to configure FortiClient on page 109.
2. You must create a Telemetry gateway list using the FortiGate's IP address for the endpoint. See Creating Telemetry gateway lists on page 152
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 105.
4. Enable *Remote HTTPS access*. See Configuring Server settings on page 177.

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 commands below, <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*, a domain, or 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.

Provisioning FortiClient (Android) endpoints for central management

You can use a third-party QR code generator to create a QR code to distribute to FortiClient (Android) users. FortiClient (Android) users can scan the QR code from their device to automatically enable FortiTelemetry and attempt connection to the specified FortiClient EMS server and FortiGate.

QR codes can contain the FortiClient EMS server's hostname or IP address, port number, and a connection key. Only the FortiClient EMS hostname/IP address is required; all other fields are optional. The following table summarizes the possible syntax used to generate the QR code:

Scenario	Format	Example
Includes hostname or IP address, port number, and connection key.	fortitelemetry://<EMS hostname or IP address>:<port number> <connection key>	fortitelemetry://192.168.128.12:8013 11111
Includes hostname or IP address, port number, with no connection key.	fortitelemetry://<EMS hostname or IP address>:<port number>	fortitelemetry://192.168.128.12:8013
Includes hostname or IP address only. Uses the default port and has no connection key.	fortitelemetry://<EMS hostname or IP address>:	fortitelemetry://192.168.128.12:

1. Open the QR code generator of your choice.
2. Enter the hostname/IP address, port number, and/or connection key information as desired, using one of the formats above.
3. Generate the plain text QR code.
4. Email the QR code to FortiClient (Android) users.

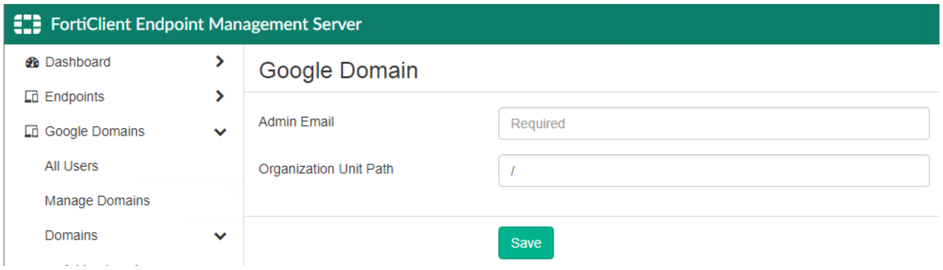
For instructions on scanning the QR code from an Android device, see the *FortiClient (Android) User Guide*.

Google Domains

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

Adding Google domains

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



Google Domain

Admin Email: Required

Organization Unit Path: /

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

/ stands for the root of the domain.

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

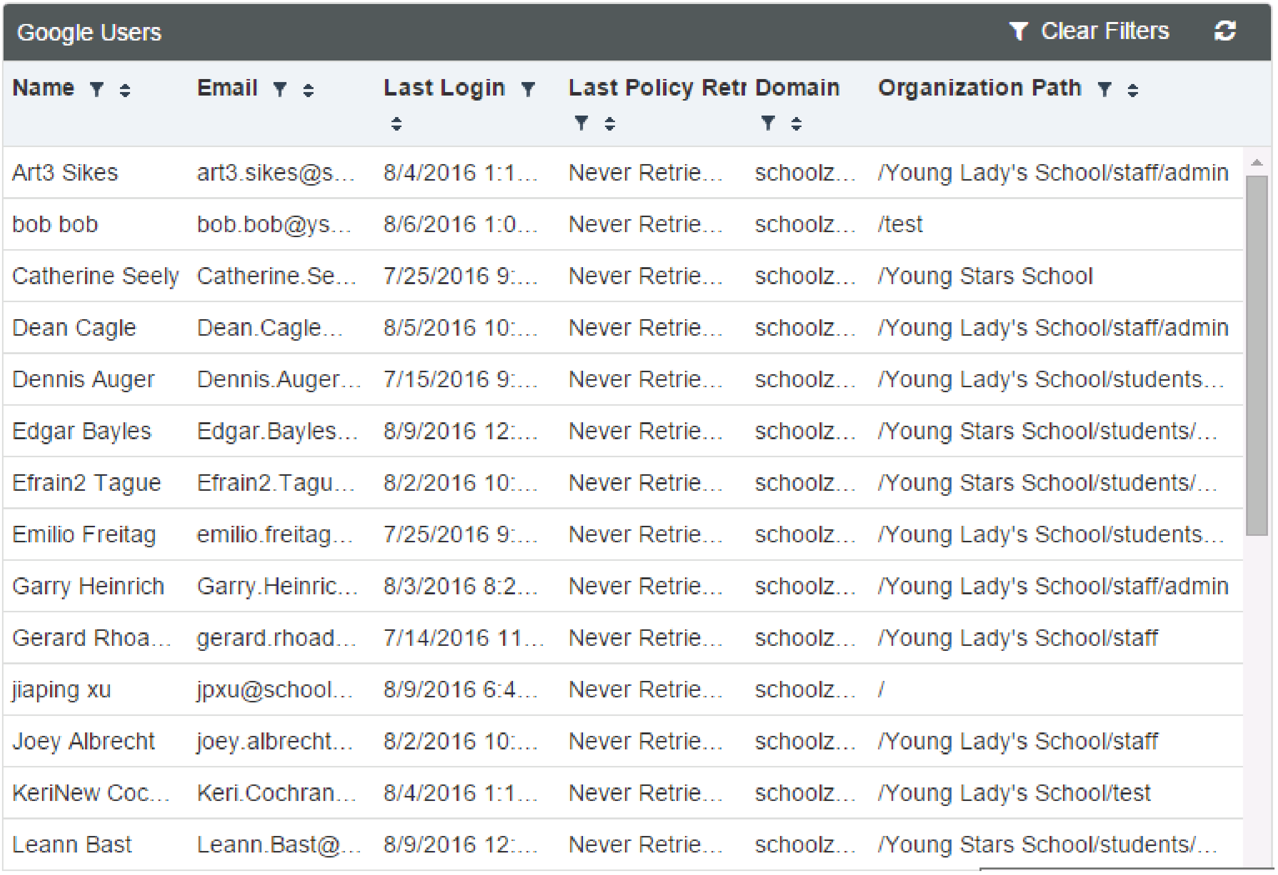
Viewing domains

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

You can view Google users' information in FortiClient EMS.

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



Google Users

Name	Email	Last Login	Last Policy Retr	Domain	Organization Path
Art3 Sikes	art3.sikes@s...	8/4/2016 1:1...	Never Retrie...	schoolz...	/Young Lady's School/staff/admin
bob bob	bob.bob@ys...	8/6/2016 1:0...	Never Retrie...	schoolz...	/test
Catherine Seely	Catherine.Se...	7/25/2016 9:...	Never Retrie...	schoolz...	/Young Stars School
Dean Cagle	Dean.Cagle...	8/5/2016 10:...	Never Retrie...	schoolz...	/Young Lady's School/staff/admin
Dennis Auger	Dennis.Auger...	7/15/2016 9:...	Never Retrie...	schoolz...	/Young Lady's School/students...
Edgar Bayles	Edgar.Bayles...	8/9/2016 12:...	Never Retrie...	schoolz...	/Young Stars School/students/...
Efrain2 Tague	Efrain2.Tagu...	8/2/2016 10:...	Never Retrie...	schoolz...	/Young Stars School/students/...
Emilio Freitag	emilio.freitag...	7/25/2016 9:...	Never Retrie...	schoolz...	/Young Lady's School/students...
Garry Heinrich	Garry.Heinric...	8/3/2016 8:2...	Never Retrie...	schoolz...	/Young Lady's School/staff/admin
Gerard Rhoa...	gerard.rhoad...	7/14/2016 11...	Never Retrie...	schoolz...	/Young Lady's School/staff
jiaping xu	jpxu@school...	8/9/2016 6:4...	Never Retrie...	schoolz...	/
Joey Albrecht	joey.albrecht...	8/2/2016 10:...	Never Retrie...	schoolz...	/Young Lady's School/staff
KeriNew Coc...	Keri.Cochran...	8/4/2016 1:1...	Never Retrie...	schoolz...	/Young Lady's School/test
Leann Bast	Leann.Bast@...	8/9/2016 12:...	Never Retrie...	schoolz...	/Young Stars School/students/...

The following options are available in the toolbar:

Clear Filter (filter icon)	Click the *Clear Current Filter* icon to clear the currently used filter.
Refresh	Click the *Refresh* icon to 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.
Organizational Path	Organization path in the domain.

Viewing user details

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

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

Client Statistics

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

Blocked Sites (Past <number> Days)

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

Editing domains

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

Deleting domains

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, OS, or AD group.

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 group assignment rules on page 94.
2. Create a FortiClient 6.0+ deployment package. Specify the "HQ" installer ID when creating or uploading the installer. See Adding FortiClient deployment packages on page 146 or Adding a custom FortiClient installer on page 149.
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.

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 group assignment rules on page 94.
2. With the next FortiClient Telemetry communication, endpoints within the specified subnet or IP address range are placed in the specified group.

OS group assignment rules

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

1. In 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 group assignment rules on page 94.
2. With the next FortiClient Telemetry communication, endpoints with the specified OS installed are placed in the specified group.

AD group assignment rules

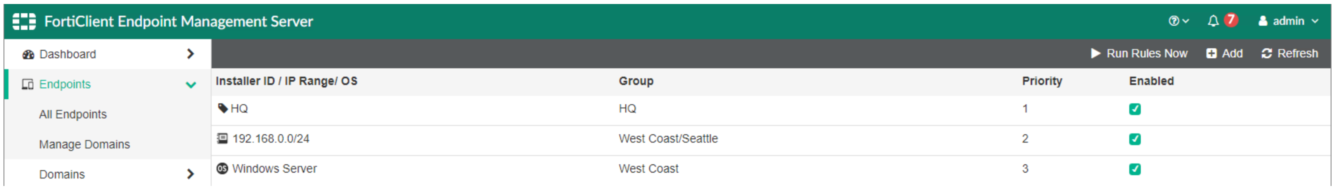
You can create a group assignment rule to automatically place all endpoints in an AD group into the same custom group. In this situation, the process is as follows:

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

Group assignment rule priority levels

The *Priority* column on the *Group Assignment Rules* page shows the order in which EMS applies group assignment rules.

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



Installer ID / IP Range/ OS	Group	Priority	Enabled
HQ	HQ	1	☑
192.168.0.0/24	West Coast/Seattle	2	☑
Windows Server	West Coast	3	☑

Adding group assignment rules

Adding 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 already 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*.

Adding 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. EMS will automatically place 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 already 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*.

Adding 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 already 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*.

Adding an AD group assignment rule

An AD group assignment rule requires all endpoints in the specified AD group to be placed into the specified endpoint group.

1. Go to *Endpoints* > *Group Assignment Rules*.
2. Click *Add*.
3. Under *Type*, select *AD Group*.
4. From the *AD Group* dropdown list, select the desired AD group. EMS automatically places endpoints in the specified AD groups into the specified group.
5. In the *Group* field, do one of the following:
    a. If you want to place the endpoints into an already 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

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

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 *Whitelist* 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.

Viewing the Files content pane

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

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

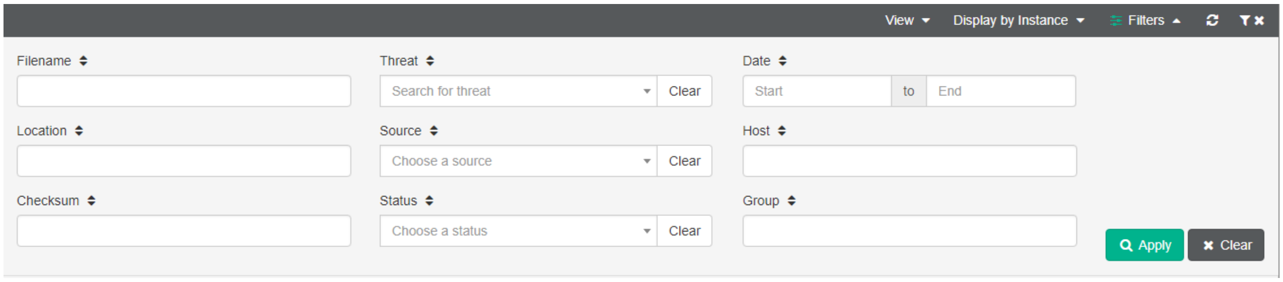
Quarantined Files	Number of files that FortiClient has quarantined on endpoints. Click to display the list of quarantined files.
Restored Files	Number of files that have been restored on endpoints. Click to display the list of restored files.
Affected Hosts	Number of hosts where FortiClient has quarantined files. Click to display the list of quarantined files sorted by hostname.
New Detections	Number of new detections. Click to display the list of newly detected threats sorted by date detected.
View	Toggle between the following options: • View all files or view only quarantined files • Show or hide full path names for files

Display by	Select to display the list of files by instance, host, threat, or date.
Search All Fields	Enter a value and press *Enter* to search for the value in the list of files.
Filters	Click to display and hide filters you can use to filter the list of files.
Refresh	Click to refresh the list of files in the content pane.
Clear Filters	Click to clear all filters applied to the list of files.
Checkbox	Click to select all files displayed in the content pane.
Host	Hostname of the endpoint. Also shows the group the endpoint belongs to.
File	Name of the file.
Size	Size of the file in bytes.
Threat	Name of threat.
Source	Displays how FortiClient detected the threat: • Scheduled Scan • Email Scan • Startup Scan • Manual Scan • Realtime Scan • Rootkit Manual Scan • Sandbox Scan
Status	Status of the file: *Quarantined*, *Quarantined & Whitelisted*, *Restored*, or *Deleted*. Also shows the time that FortiClient quarantined the file.
Summary	Displays the number of threat instances and number of affected hosts.

Filtering files 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. You can exclude a name or names from the filter using an exclamation mark (!).
Location	Enter the file location(s) to include in the filter. You can exclude a location or locations from the filter using an exclamation mark (!).
Checksum	Enter the checksum(s) to include in the filter. You can exclude a checksum or checksums from the filter using an exclamation mark (!).
Threat	Enter the threat(s) to include in the filter. You can exclude a threat or threats from the filter using an exclamation mark (!). You can also select the desired threat(s) from the dropdown list.
Source	Enter the source(s) to include in the filter. You can exclude a source or sources from the filter using an exclamation mark (!). You can also select the desired source(s) from the dropdown list.
Status	Enter the status(es) to include in the filter. You can exclude a status or statuses from the filter using an exclamation mark (!). You can also select the desired statuse(s) from the dropdown list.
Date	Enter the range of dates to include in the filter.
Host	Enter the host(s) to include in the filter. You can exclude a host or hosts from the filter using an exclamation mark (!). 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 exclude a group or groups from the filter using an exclamation mark (!). 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.

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

Whitelist

Viewing allowlisted files

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

Go to *Quarantine Management* > *Whitelist*. 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.

Filtering allowlisted files

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

1. Go to *Quarantine Management* > *Whitelist*. 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.

1. Go to *Quarantine Management* > *Whitelist*.
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 files 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.

1. Go to *Quarantine Management* > *Whitelist*.
2. Select the desired file.
3. Click *Delete*.
4. In the confirmation dialog, click *Yes*. EMS deletes the file from the allowlist. The file will be quarantined 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.

If enabled, FortiClient also sends software inventory logs to FortiAnalyzer for real-time and historic logging and reporting. FortiClient sends the software inventory information when it first registers to EMS and when it first sends data to FortiAnalyzer. 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 FortiAnalyzer. See System Settings on page 138.

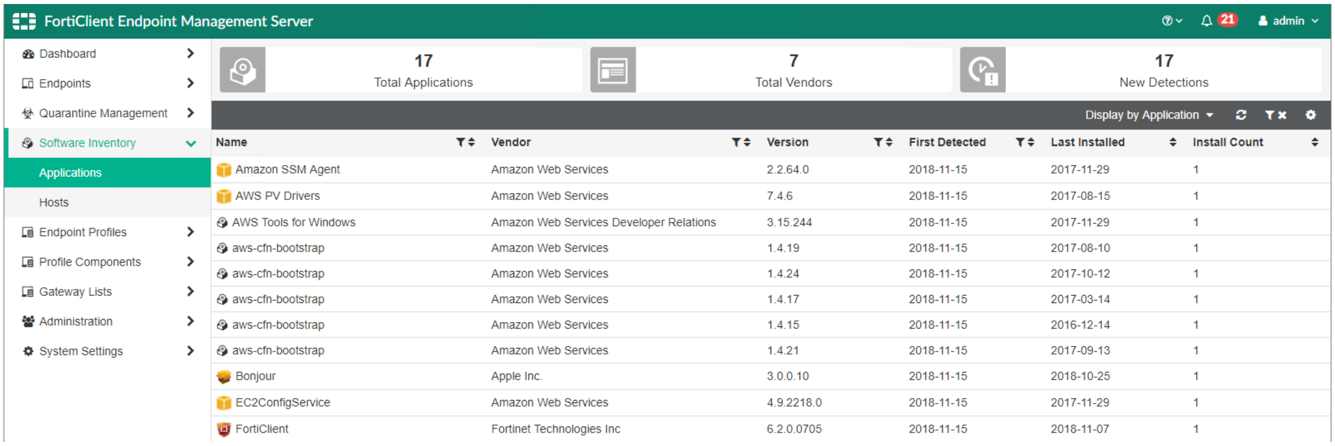
Applications

The FortiClient EMS administrator can view installed application information for all managed endpoints on the *Applications* pane.

Viewing the Applications content pane

You can view information about installed applications on the *Applications* content pane.

Go to *Software Inventory* > *Applications*. The list of applications, a quick status bar, and a toolbar display in the content pane.



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

Total Applications	Number of applications that have been installed on all managed endpoints. Click to display the list of installed applications.
Total Vendors	Number of vendors whose applications have been installed on managed endpoints. Click to display the list of installed applications sorted by vendor.

New Detections	Number of applications that have been detected as newly installed since the last Telemetry communication. Click to display newly detected applications sorted by date detected.
Display by	Select to toggle between the following options: • 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.

Filtering 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.

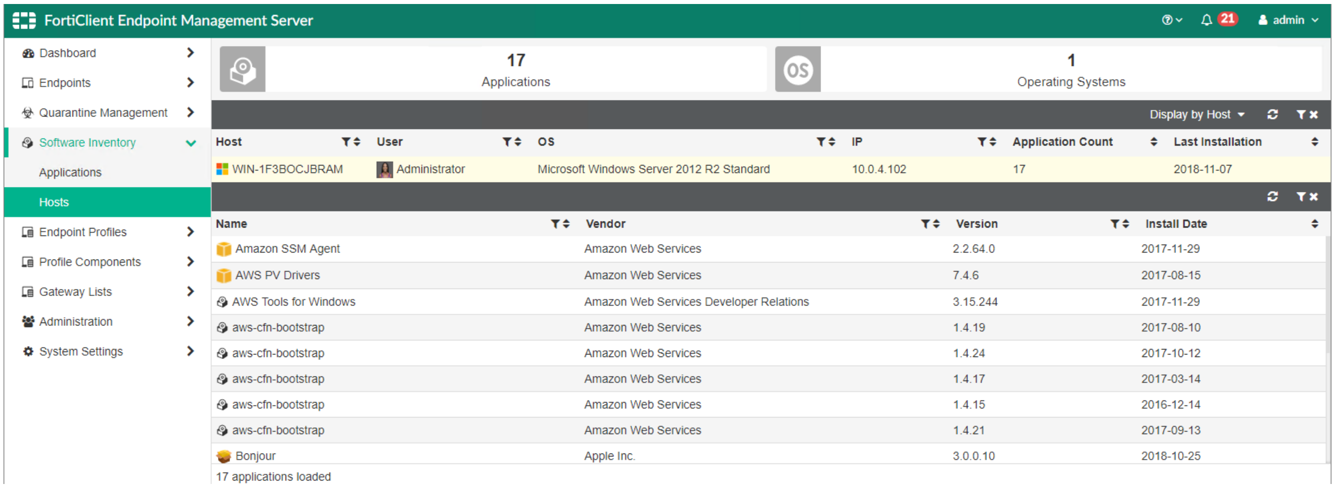
Hosts

The FortiClient EMS administrator can view installed application information for all managed endpoints by host on the *Hosts* pane.

Viewing the Hosts content pane

You can view information about installed applications by host on the *Hosts* content pane.

Go to *Software Inventory* > *Hosts*. The list of hosts, a quick status bar, and a toolbar display in the content pane.



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

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

17 applications loaded

Applications	Number of applications that have been installed on all managed endpoints.
Operating Systems	Number of different operating systems on managed endpoints.
View Details	Displays list of software installed on the selected endpoint. For details on the application list headings, see Viewing the Applications content pane on page 102.
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.

Filtering 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 Filtering applications on page 103 for details on filtering the list of applications.

Endpoint Policy

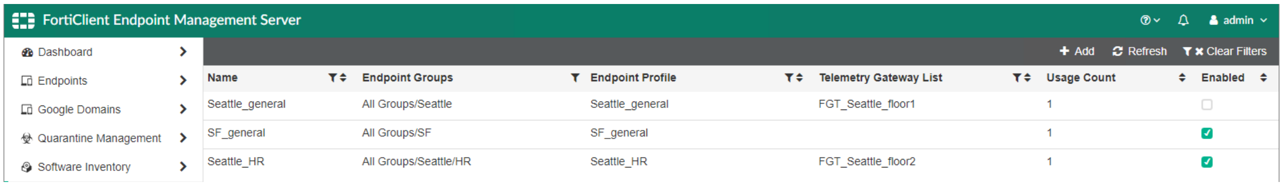
You can create endpoint policies to assign endpoint profiles and Telemetry gateway lists to groups of Windows, macOS, and Linux endpoints. The *Endpoint Policy > Manage Policies* page provides a comprehensive summary of which endpoint policies are applied to which endpoint groups.

Adding an endpoint policy

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

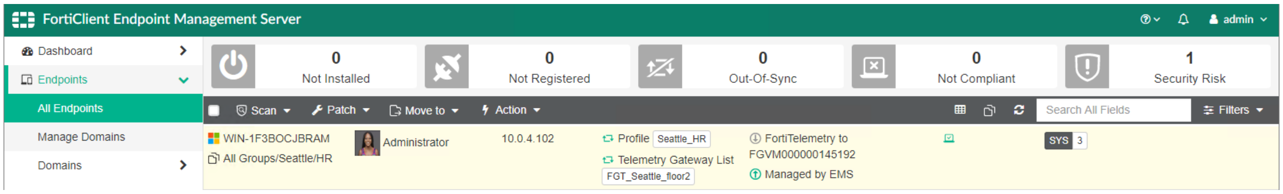
Endpoint policy name	Enter the desired name for the endpoint policy.
Endpoint domains	Select the domains to apply the policy to. Domains for which an endpoint policy has already been created are grayed out and you cannot select them.
Endpoint workgroups	Select the workgroup of endpoints to apply the policy to. Groups for which an endpoint policy has already been created are grayed out and you cannot select them.
Endpoint profile	Include an endpoint profile in the policy. From the dropdown list, select the desired endpoint profile.
Telemetry gateway list	Include a Telemetry gateway list in the policy. From the dropdown list, select the desired Telemetry gateway list. You must have already created a Telemetry gateway list to include one in an endpoint policy. See Creating Telemetry gateway lists on page 152.
Comments	Enter any comments desired for the endpoint policy.
Enable the policy	Toggle to enable or disable the endpoint policy. You can enable or disable the policy at a later time from *Endpoint Policy > Manage Policies*.

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



Name	Endpoint Groups	Endpoint Profile	Telemetry Gateway List	Usage Count	Enabled
Seattle_general	All Groups/Seattle	Seattle_general	FGT_Seattle_floor1	1	☐
SF_general	All Groups/SF	SF_general		1	☑
Seattle_HR	All Groups/Seattle/HR	Seattle_HR	FGT_Seattle_floor2	1	☑

On the *Endpoints* pane, you can see that endpoints that belong to the All Groups/Seattle/HR group have the endpoint profile and Telemetry gateway list configured in the endpoint policy (Seattle_HR and FGT_Seattle_floor2, respectively) applied:



WIN-1F3BOCJBRAM
All Groups/Seattle/HR
Administrator
10.0.4.102
Profile Seattle_HR
Telemetry Gateway List FGT_Seattle_floor2
FortiTelemetry to FGVM000000145192
Managed by EMS

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

In this example, endpoints in the All Groups/Seattle/HR group are applicable for the Seattle_HR policy. If both the Seattle_general policy (applied to the All Groups/Seattle group) and the Seattle_HR policy (applied to the All Groups/Seattle/HR group) are enabled, EMS applies only the Seattle_HR policy to the All Groups/Seattle/HR group, since the Seattle_HR policy is the most specific policy that is applicable for that group. If the Seattle_HR policy is disabled, EMS applies the Seattle_general policy to endpoints in the All Groups/Seattle/HR group.

Editing an endpoint policy

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

Deleting an endpoint policy

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

You cannot delete an endpoint policy that is currently assigned to endpoints. If the policy is currently assigned to endpoints, disable the policy, then delete it.

Enabling/disabling an endpoint policy

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

Chromebook Policy

You can create Chromebook policies to assign endpoint profiles and Telemetry gateway lists to groups 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 the *EMS for Chromebooks Settings* option is enabled in *System Settings > Server*.

Chromebook policies function identically to Windows, macOS, and Linux endpoint policies except that they are applied 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 105.

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 the default profile

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

1. Do one of the following:
   a. To edit the default profile for Chromebooks, go to *Endpoint Profiles > Local Chromebook Profiles*, and click the *Default - Chromebooks* profile.
   b. To edit the default profile for other endpoints, go to *Endpoint Profiles > Local Profiles*, and click the *Default* profile.
2. Configure the settings on the tabs. See Profile references on page 119.
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 profiles to configure FortiClient

This section describes how to create a profile that excludes any installation or uninstallation of FortiClient software on endpoints. This type of profile is used to configure FortiClient software on endpoints.

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* box, 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 119.
5. Click *Save* to save the profile.

Creating profiles to deploy FortiClient

You must create a new profile to deploy FortiClient to endpoints. You cannot add a FortiClient deployment package to the default profile.

You must add FortiClient deployment packages to FortiClient EMS before you can select the deployment packages in a profile. See Adding FortiClient deployment packages on page 146.

The selected FortiClient deployment package in a profile controls what tabs display for configuration in the profile. Only the tabs for the features in the selected deployment package display for configuration in the profile. For example, if the deployment package includes only the VPN feature, only the *VPN* tab displays for you to configure. The *System Settings* tab always displays.

You can disable a feature included in the deployment package, then enable the feature in the profile later. For example, if the deployment package includes the Web Filter and VPN features, you can disable the Web Filter feature and keep the VPN feature enabled. When FortiClient is installed on the endpoint, the Web Filter is installed, but disabled.

1. Go to *Endpoint Profiles > Manage Profile*, and click the *Add* button.
2. On the *Deployment* tab, enable *FortiClient Deployment*. The FortiClient deployment options display.
3. Set the following options on the *Deployment* tab:

Action		
	Action	Click *Install*.
	Deployment Package	In the *Deployment Package* list, select the desired FortiClient deployment package. If you have not added a FortiClient deployment package to FortiClient EMS, see Adding FortiClient deployment packages on page 146. The selected FortiClient deployment package affects what tabs display for configuration. Only tabs related to features enabled in the FortiClient deployment package display for configuration.
Schedule		
	Start At	Specify what time to start installing FortiClient on endpoints.
	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 the user decide when to reboot when they 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.
Credentials		
	Username	Enter the username to perform deployment on AD. You must enter the admin credentials for the AD in the profile. Enter the appropriate credentials in the profile to assign to 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.

4. Set the options on the remaining tabs.
5. Click *Save*.

Creating profiles to uninstall FortiClient

You can configure a profile to uninstall FortiClient from endpoints. You must create a new profile for this configuration. You cannot use the default profile to uninstall FortiClient from endpoints.

1. Go to *Endpoint Profiles* > *Manage Profiles*, and click the *Add* button.
2. On the *Deployment* tab, enable *FortiClient Deployment*. The FortiClient deployment options display.
3. Set the following options on the *Deployment* tab:

Action		
	Action	Click *Uninstall*.
Schedule		
	Start At	Specify what time to start uninstalling FortiClient from endpoints.
	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 the user decide when to reboot when they 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.
Credentials		

	Username	Enter the username to perform deployment on AD or workgroups. If you are using an AD to uninstall FortiClient on endpoints, you must enter the admin credentials for the AD in the profile. If you are using a workgroup to uninstall FortiClient on endpoints, FortiClient must be connected to FortiClient EMS. Admin credentials are not required. When configuring the profile, know what method (AD or workgoup) is being used to uninstall FortiClient on endpoints. If using an AD, enter the appropriate credentials in the profile you will assign to the AD. The credentials allow FortiClient EMS to uninstall FortiClient on endpoints by using AD. If the credentials are wrong, the uninstallation fails, and an error displays in FortiClient EMS.
	Password	Enter the password to perform the uninstall on AD or workgroups.

4. Click *Save*. When you apply this profile to a group of endpoints and the profile takes effect, Microsoft Security Center on the endpoint alerts the user that FortiClient is off and advises to enable AV and other protection. The system must reboot to complete the uninstall process, and will reboot as configured above. Once the reboot process has begun on the endpoint, the *Endpoints > System Events* tab for the endpoint displays a *FortiClient Telemetry-<hostname> has manually disconnected* message.

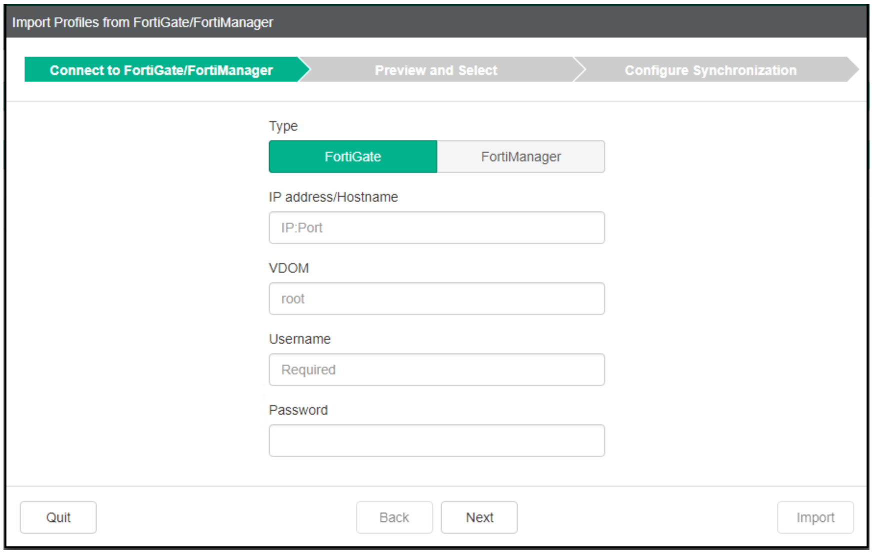
   Once the uninstall is complete, the endpoint appears on the *Endpoints* pane with only the uninstaller applied. The endpoint is shown as having no connection to EMS.

Importing FortiGate Web Filter profiles

You can import a Web Filter profile from FortiOS into FortiClient EMS, then edit the profile in FortiClient EMS to add a FortiClient installer or other configuration details.

To import Web Filter profiles successfully from FortiOS to FortiClient EMS, FortiGate must be open to HTTPS access. In FortiOS, go to *Network > Interfaces*, select the desired port, and under *Administrative Access*, enable the *HTTPS* checkbox.

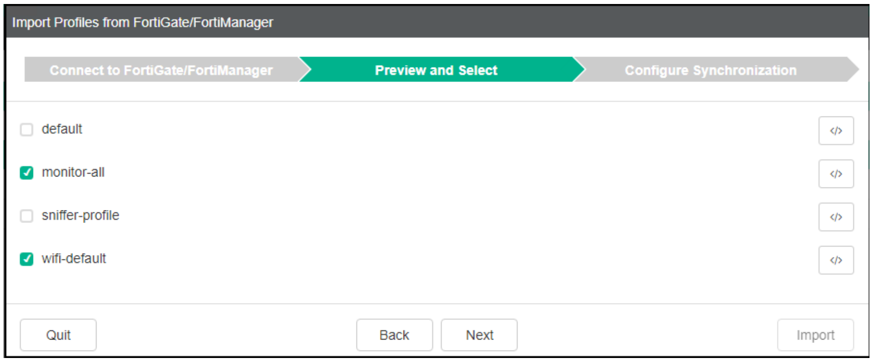
1. Click *Endpoint Profiles > Manage Profiles > Import > From FortiGate / FortiManager*. The *Import Profiles from FortiGate/FortiManager* window opens.



2. Under *Type*, select *FortiGate*.
3. Complete the following options, and click *Next*.

IP address/Hostname	Enter the IP address and port of the FortiGate from which the profile is being imported, in the format: `<ip address>:<port>`.
VDOM	Enter a VDOM name from the FortiGate if applicable.
Username	Enter the FortiGate's login username.
Password	Enter the FortiGate's login password.

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


Import Profiles from FortiGate/FortiManager
Connect to FortiGate/FortiManager
Preview and Select
Configure Synchronization
</>
</>
</>
</>
Quit
Back
Next
Import

□ default

☑ monitor-all

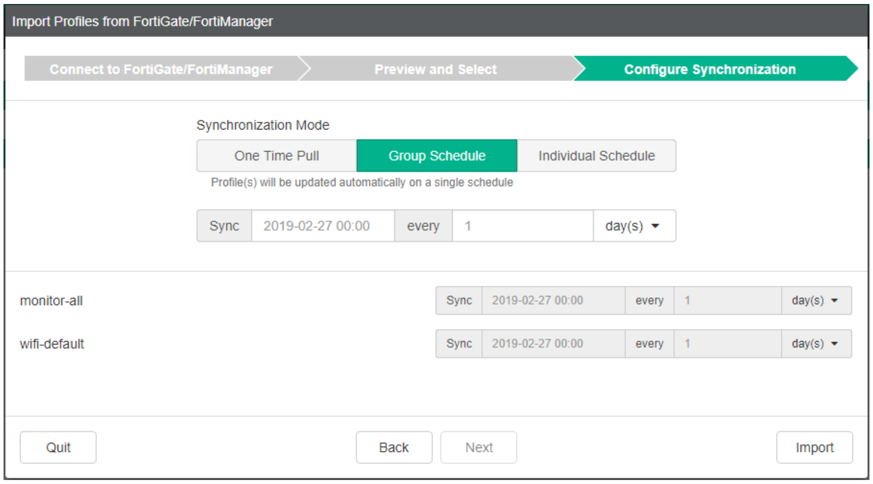
□ sniffer-profile

☑ wifi-default

You can click the </> icon beside each profile to preview the settings in XML format.

4. Select the profiles to import into FortiClient EMS and click *Next*.

5. Under *Synchronization Mode*, select one of the following options.



Import Profiles from FortiGate/FortiManager

Synchronization Mode

Profile(s) will be updated automatically on a single schedule

Sync 2019-02-27 00:00 every 1 day(s)

monitor-all	Sync	2019-02-27 00:00	every	1	day(s)
wifi-default	Sync	2019-02-27 00:00	every	1	day(s)

   a. *One Time Pull*: If selected, FortiClient EMS does not automatically sync profile changes from the FortiGate. You can manually sync profile changes after importing the profile. See Syncing profile changes on page 118.
   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.
6. Click *Import*. The selected profiles are imported into FortiClient EMS and display in *Endpoint Profiles > Manage Profiles* in a group named after the FortiGate from which they were imported.
7. In the *Endpoint Profiles* page, select an imported profile. Click *Edit*.

   You can modify settings on the *Web Filter* tab. When the next profile synchronization occurs between FortiOS and EMS, any Web Filter settings modified in EMS are overwritten with the settings from the Web Filter profile in FortiOS. For Web Filter settings that are available in EMS but are not available for configuration in FortiOS, the EMS settings are preserved.

   You can edit other tabs on the profile to provide additional configuration information. You can also add a FortiClient deployment package to the profile by using the *Deployment* tab. Custom installers can be created. See Adding FortiClient deployment packages on page 146.
8. Edit the options on the tabs.
9. Click *Save Profile*.

Importing Web Filter profiles from FortiManager

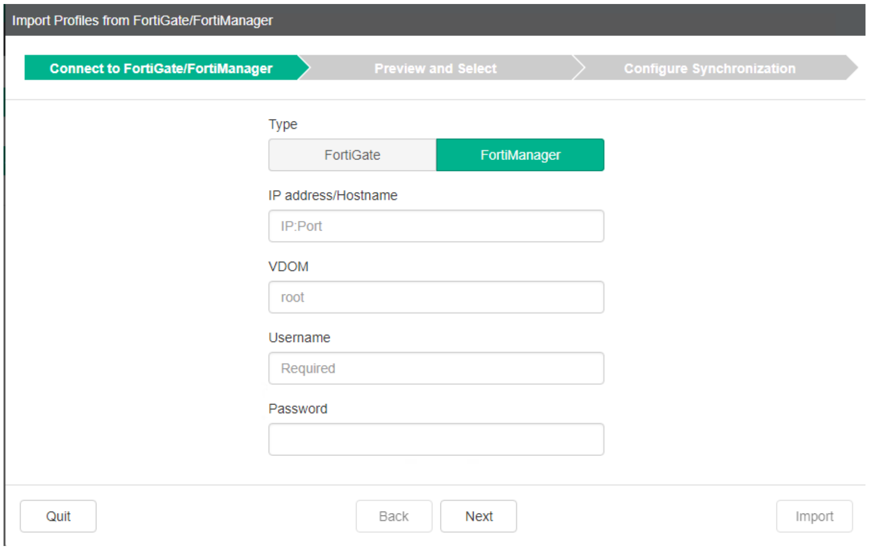
You can import Web Filter profiles from FortiManager into FortiClient EMS, then edit the profile in FortiClient EMS to add a FortiClient deployment package or add configuration information.

1. Configure FortiManager to allow EMS profile importation:
   a. Go to *System Settings > Network* and enable the *HTTPS* checkbox.
   b. Remote Procedure Call must be set to `read`. Run the `get system admin user admin` command. Ensure that `rpc-permit` is set to `read-write`.
   c. If `rpc-permit` is not set to `read`, run the following commands to configure it:

```
config system admin user
   edit "admin"
      set rpc-permit read
```

```
end
```

2. Click *Endpoint Profiles > Manage Profiles > Import > From FortiGate / FortiManager*. The *Import Profiles from FortiGate/FortiManager* window opens.



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

IP address/Hostname	Enter the IP address and port of the FortiManager from which the profile is being imported, in the format: `<ip address>:<port>`.
VDOM	Enter a VDOM name from the FortiManager if applicable.
Username	Enter the FortiManager's login username.
Password	Enter the FortiManager's login password.

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

You can click the </> icon beside each profile to preview the settings in XML format.

5. Select the profiles to import into FortiClient EMS and click *Next*.
Select the name of the profile to import all profiles for it into FortiClient EMS. You can also clear the checkbox beside the profiles you do not want to import into FortiClient EMS.
6. Under *Synchronization Mode*, select one of the following options.
   a. *One Time Pull*: If selected, FortiClient EMS does not automatically sync profile changes from the FortiManager. You can manually sync profile changes after importing the profile. See Syncing profile changes on page 118.
   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.
7. Click *Import*. The selected profiles are imported into FortiClient EMS and display under the *Endpoint Profiles* pane in a group named after the FortiManager from which they were imported.
8. In the *Endpoint Profiles* page, select an imported profile to edit it.
You can edit additional options to provide configuration information. You can also add a FortiClient deployment package to the profile by using the *Deployment* tab. You can create custom deployment packages. See Adding

FortiClient deployment packages on page 146.

9. Edit the options on the tabs.
10. Click *Save Profile*.

Creating profiles with XML

You can configure FortiClient profile settings in FortiClient EMS by using XML or a custom XML configuration file. The custom XML file must include all settings required by the endpoint at the time of deployment. For more information about how to configure a profile with XML, see the *FortiClient XML Reference*.

1. Go to *Endpoint Profiles* > *Manage Profiles*, and click the *Add* button.
2. In the *Profile Name* box, 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.

Creating profiles to automatically upgrade FortiClient

You can create a profile to automatically upgrade FortiClient to the latest patch release. The profile must be configured with a deployment package that meets the following requirements:

- The FortiClient deployment package was created in FortiClient EMS 1.2.0 or later.
- The FortiClient deployment package was created with the latest FortiClient version available for selection in FortiClient EMS at the time the deployment package was created.
- The FortiClient deployment package was created with the *Keep software updated to the latest patch release* option enabled.

See Adding FortiClient deployment packages on page 146.

With this configuration, when an upgrade is available, FortiClient downloads it directly from FortiClient EMS. Offline FortiClients remain without the upgrade until they contact FortiClient EMS.

1. Go to *Endpoint Profiles* > *Manage Profiles*, and click the *Add* button.
2. In the *Profile Name* box, enter a name for the profile.
3. On the *Deployment* tab, enable *FortiClient Deployment*.
4. Beside *Action*, click *Install*.
5. From the *Deployment Package* dropdown list, select the desired deployment package.
6. Configure the profile as desired, then click *Save*.

If deploying an upgrade to a FortiClient endpoint running Windows 7, you must enable *Enable TLS 1.0/1.1*. See Configuring Server settings on page 177.

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 new profiles

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

It is recommended to add Yandex search engine to the blocklist in the profile.

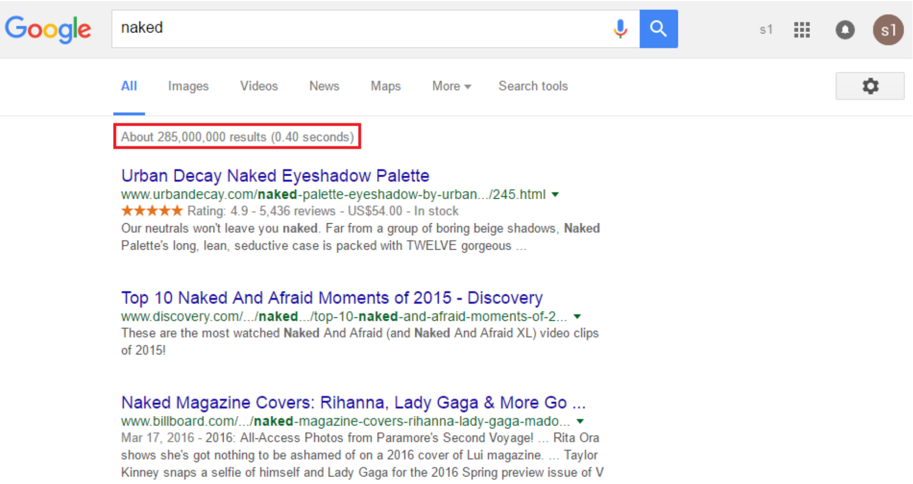
1. Go to *Endpoint Profiles > Manage Profiles*, and click the *Add Chrome* button.
2. In the *Profile Name* box, enter the profile name.
3. On the *Web Filter* tab, enable *Web Filter*, and set the web filtering options.
4. On the *System Settings* tab, set the logging options.
5. Click *Save*.

Enabling/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:



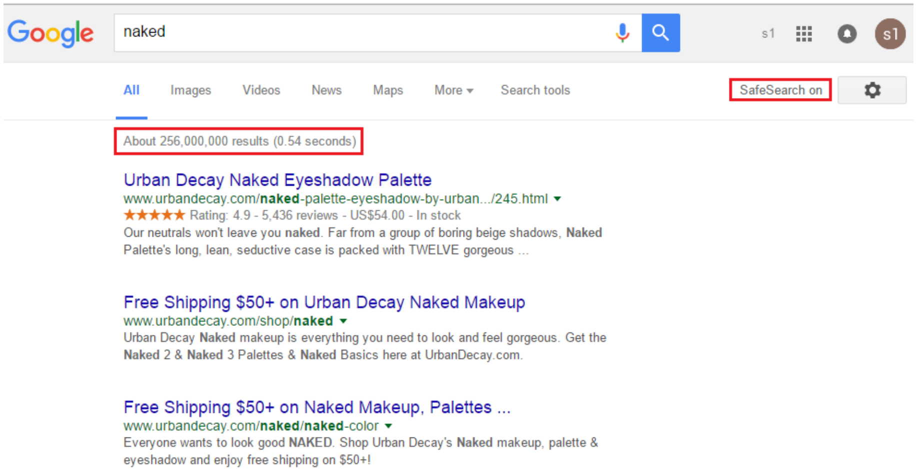
About 285,000,000 results (0.40 seconds)

Urban Decay Naked Eyeshadow Palette
www.urbandecay.com/**naked**-palette-eyeshadow-by-urban.../245.html ▾
★★★★★ Rating: 4.9 - 5,436 reviews - US$54.00 - In stock
Our neutrals won't leave you **naked**. Far from a group of boring beige shadows, **Naked** Palette's long, lean, seductive case is packed with TWELVE gorgeous ...

Top 10 Naked And Afraid Moments of 2015 - Discovery
www.discovery.com/.../**naked**.../top-10-**naked**-and-afraid-moments-of-2... ▾
These are the most watched **Naked** And Afraid (and **Naked** And Afraid XL) video clips of 2015!

Naked Magazine Covers: Rihanna, Lady Gaga & More Go ...
www.billboard.com/.../**naked**-magazine-covers-rihanna-lady-gaga-mado... ▾
Mar 17, 2016 - 2016: All-Access Photos from Paramore's Second Voyage! ... Rita Ora shows she's got nothing to be ashamed of on a 2016 cover of Lui magazine. ... Taylor Kinney snaps a selfie of himself and Lady Gaga for the 2016 Spring preview issue of V

Here are the search results when the Safe Search feature is enabled, which has about 256000000 results.



About 256,000,000 results (0.54 seconds)

Urban Decay Naked Eyeshadow Palette
www.urbandecay.com/**naked**-palette-eyeshadow-by-urban.../245.html ▾
★★★★★ Rating: 4.9 - 5,436 reviews - US$54.00 - In stock
Our neutrals won't leave you naked. Far from a group of boring beige shadows, **Naked** Palette's long, lean, seductive case is packed with TWELVE gorgeous ...

Free Shipping $50+ on Urban Decay Naked Makeup
www.urbandecay.com/shop/**naked** ▾
Urban Decay **Naked** makeup is everything you need to look and feel gorgeous. Get the **Naked** 2 & **Naked** 3 Palettes & **Naked** Basics here at UrbanDecay.com.

Free Shipping $50+ on Naked Makeup, Palettes ...
www.urbandecay.com/**naked**/**naked**-color ▾
Everyone wants to look good **NAKED**. Shop Urban Decay's **Naked** makeup, palette & eyeshadow and enjoy free shipping on $50+!

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.

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 profiles

When you edit a profile that is assigned to endpoints or domains as part of an endpoint policy, the changes are automatically pushed to the endpoints or Chromebooks with the next Telemetry communication after you save the 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 119.
4. Click *Save*.

Cloning profiles

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* box, enter a name for the profile.
4. Configure the settings on the tabs. See Profile references on page 119.
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* > *Manage Profiles*.
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 118.
   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.

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.

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 *XML Configuration* 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.

Options	Description
Real-Time Protection	Enable real-time protection (RTP).
Action On Virus Discovery	• Quarantine Infected Files. You can use FortiClient to view the quarantined file, virus name, and logs, as well as submit the file to FortiGuard. • Deny Access to Infected Files • Ignore Infected Files
Alert When Viruses Are Detected	Displays the *Virus Alert* dialog when RTP detects a virus while attempting to download a file via a web browser. The dialog allows you to view recently detected viruses, their locations, and statuses.
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 *Sandbox Detection* tab is enabled. Enter the number of minutes after which to update signatures.

Options		Description
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 *FortiProxy (Disable Only When Troubleshooting)* on the *System Settings* tab before you can enable this option.
	Security Risk	Configure an action for the security risk site category by selecting one of the following: • 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: • Dynamic DNS • Malicious Websites • Newly Observed Domain • Newly Registered Domain • Phishing • Spam URLs
	Use the Exclusion List Defined in the Web Filter Profile	If this option is enabled, the exclusion list on the *Web Filter* tab is used. If this option is not enabled, you must define exclusions under *Exclusions*.
Scan Compressed Files		Scan archive files, including zip, rar, and tar files, for threats. Default file extensions are listed in RTP exclusions below.
	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 user-initiated processes access. Select one of the following: • Scan Files When Processes Read or Write Them • Scan Files When Processes Read Them • Scan Files When Processes Write Them
	Scan Network Files	Scan network files for threats when a user-initiated process accesses them.

Options	Description
System Process Scanning	Enable system process scanning. Select one of the following: • Scan Files When System Processes Read or Write Them • Scan Files When System Processes Read Them • Scan Files When System Processes Write Them • Do Not Scan Files When System Processes Read or Write Them
On Demand Scanning	
Action On Virus Discovery	Select one of the following from the dropdown list: • Warn the User If a Process Attempts to Access Infected Files • Quarantine Infected Files. You can use FortiClient to view the quarantined file, virus name, and logs, as well as submit the file to FortiGuard. • Ignore Infected Files
Integrate FortiClient into Windows Explorer's Context Menu	Adds a *Scan with FortiClient AntiVirus* option to the Windows Explorer right-click menu.
Pause Scanning When Running on Battery Power	Pause scanning when the computer is running on battery power.
Allow Admin Users to Terminate Scheduled and On-Demand Scans from FortiClient Console	Control whether the local administrator can stop a scheduled or on-demand AV scan initiated by the EMS administrator. A user who is not a local administrator cannot stop a scheduled or on-demand AV scan regardless of this setting.
Automatically Submit Suspicious Files to FortiGuard for Analysis	Automatically submit suspicious files to FortiGuard for analysis. You do not receive feedback for files submitted for analysis. The FortiGuard team can create signatures for any files that are submitted for analysis and determined to be malicious.
Scan Compressed Files	Scan archive files, including zip, rar, and tar files, for threats.
Max Size	Only scan files under the specified size (in MB). To allow scanning compressed files of any size, enter 0.
Max Scan Speed on Computers With	Select the minimum amount of memory that must be installed on a computer to maximize scan speed. AV maximizes scan speed by loading signatures on computers with a minimum amount of memory: • 4 GB • 6 GB • 8 GB • 12 GB • 16 GB
Scheduled Scan	Enable scheduled scans.
Schedule Type	Select *Daily*, *Weekly*, or *Monthly*.

Options	Description
Scan On	If *Weekly* is selected, select the day of the week to perform the scan. If *Monthly* is selected, select the day of the month to perform the scan. If you configure monthly scans to occur on the 31st of each month, the scan occurs on the first day of the month for months with fewer than 31 days.
Start At	Configure the start time for the scheduled scan.
Scan Type	Select one of the following: • *Quick*: Runs the rootkit detection engine to detect and remove rootkits. The quick scan only scans executable files, DLLs, and drivers that are currently running for threats. • *Full*: Runs the rootkit detection engine to detect and remove rootkits, then performs a full system scan of all files, executable files, DLLs, and drivers. • *Custom*: Runs the rootkit detection engine to detect and remove rootkits. In the *Scan Folder* field, enter the full path of the folder on your local hard disk drive that will be scanned.
Scan Priority	Set to *Low*, *Normal*, or *High*. This refers to the amount of processing power that the scan uses and its impact on other processes.
Scan Removable Media	Scan connected removable media, such as USB drives, for threats, if present.
Scan Network Drives	Scan attached or mounted network drives for threats.
Enable Scheduled Scans Even When a Third-Party AV Product Is Present	Enable scheduled scans even when a third party AV product is present.

Anti-Exploit

Enable anti-exploit engine to monitor commonly used applications for attempts to exploit known vulnerabilities.

Options	Description
Show System Tray Notifications	Show system tray notifications when anti-exploit engine detects an exploit.
Application Exclusion List	Exclude applications from anti-exploit detection.

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.

Removable Media Access

Control access to removable media devices, such as USB drives.

Options	Description
Control removable media access	Configure the action to take with removable media devices. Available options are: • *Allow*: Allow access to all removable media devices connected to the endpoint. • *Block*: Block access to all removable media devices connected to the endpoint. • *Monitor*: Log all removable media device connections to the endpoint.
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%

Having a longer exclusion list affects AV performance. It is advised to keep the exclusion list as short as possible.

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: • Text in character sets other than ASCII • Non text attachments (audio, video, images, applications) • Message bodies with multiple parts
Enable FortiGuard Analytics	Automatically sends suspicious files to FortiGuard for analysis.
Notify Logged in Users if Their AV Signatures Expired	Notify logged in users if their AV signatures expired.

Sandbox 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	

Options	Description
FortiSandbox	Select *Appliance* to configure connection to an on-premise FortiSandbox appliance or *Cloud* to configure connection to FortiSandbox Cloud. FortiSandbox Cloud offers a more affordable alternative to a FortiSandbox appliance, since it is a cloud service that does not need to be hosted 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 *Test Connection* 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. The username is necessary to view detailed FortiSandbox reports on the *Sandbox Events* tab. See Viewing Sandbox event details on page 80.
Password	Optional. Enter the FortiSandbox password. This option is only available for a FortiSandbox appliance. The password is necessary to view detailed FortiSandbox reports on the *Sandbox Events* tab. See Viewing Sandbox event details on page 80.
Region	Select the desired region. This option is only available for FortiSandbox Cloud.
License Status	Displays the Sandbox Cloud license status. Using FortiSandbox Cloud requires an additional license. See FortiClient EMS on page 20.
Inspection Mode	Select one of the following: • *None*: FortiClient does not send any files to FortiSandbox for inspection. • *All High-Risk Exts*: FortiClient inspects all supported high-risk file extensions and sends to FortiSandbox as appropriate. • *All Supported Extensions*: FortiClient inspects all supported file extensions and sends to FortiSandbox as appropriate.
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.

Options	Description
Remediation Actions	
Action	Choose *Quarantine* or *Alert & Notify* for infected files. The user can access the file after FortiClient submits the file to FortiSandbox for analysis. FortiClient quarantines the file only if FortiSandbox reports the file as malicious.
Exceptions	
Exclude Files from Trusted Sources	Exclude files signed by trusted sources from FortiSandbox submission.
Exclude Specified Folders/Files	Exclude specified folders/files from FortiSandbox submission. You must also create the exclusion 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	Enable web filtering. Enable or disable the eye icon to show or hide this feature from the end user in FortiClient.
General	
Client Web Filtering When On-Net	Enable client web filtering when onnet. Only available for Windows and macOS profiles. This setting affects the *Block Access to Malicious Websites* setting in Malware Protection on page 119.
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.
Show Bubble Notification When HTTPS Site Is Blocked	Show a bubble notification when Web Filter blocks an HTTPS site.
Enable Web Browser Plugin for HTTPS Web Filtering	Enable a web browser plugin for HTTPS web filtering. This improves detection and enforcement of Web Filter rules on HTTPS sites. After this option is enabled, the user must open the browser to approve installing the new plugin. The web browser plugin is installed only for the Google Chrome browser on Windows platforms.

Configuration		Description
	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		Enable Safe Search. When Safe Search is enabled, the endpoint's Google search is set to Restricted mode, and YouTube access is set to Strict Restricted access. To set YouTube access to Moderate Restricted or Unrestricted YouTube access, you can disable Safe Search and configure Google Search and YouTube access with the Google Admin Console instead of FortiClient EMS.
Site Categories		Select to enable site categories from FortiGuard. When site categories are disabled, FortiClient is protected by the exclusion list. See the FortiGuard website for descriptions of the available categories and subcategories. For all categories below, you can configure an action for the entire site category by selecting one of the following: • 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. Each site category's subcategories are listed below.
Adult/Mature Content		• Abortion • Advocacy Organizations • Alcohol • Alternative Beliefs • Dating • Gambling • Lingerie and Swimsuit • Marijuana • Nudity and Risque • Other Adult Materials • Pornography • Sex Education • Sports Hunting and War Games • Tobacco • Weapons (Sales)
Bandwidth Consuming		• File Sharing and Storage

Configuration	Description
	• Freeware and Software Downloads • Internet Radio and TV • Internet Telephony • Peer-to-peer File Sharing • Streaming Media and Download
General Interest-Business	• Armed Forces • Business • Charitable Organizations • Finance and Banking • General Organizations • Government and Legal Organizations • Information Technology • Information and Computer Security • Online Meeting • Remote Access • Search Engines and Portals • Secure Websites • Web Analytics • Web Hosting • Web-based Applications

Configuration	Description
General Interest-Personal	- Advertising - Arts and Culture - Auction - Brokerage and Trading - Child Education - Content Servers - Digital Postcards - Domain Parking - Dynamic Content - Education - Entertainment - Folklore - Games - Global Religion - Health and Wellness - Instant Messaging - Job Search - Meaningless Content - Medicine - News and Media - Newsgroups and Message Boards - Personal Privacy - Personal Vehicles - Personal Websites and Blogs - Political Organizations - Real Estate - Reference - Restaurant and Dining - Shopping - Social Networking - Society and Lifestyles - Sports - Travel - Web Chat - Web-based Email

Configuration	Description
Potentially Liable	• Child Abuse • Discrimination • Drug Abuse • Explicit Violence • Extremist Groups • Hacking • Illegal or Unethical • Plagiarism • Proxy Avoidance
Security Risk	• Dynamic DNS • Malicious Websites • Newly Observed Domain • Newly Registered Domain • Phishing • Spam URLs
Unrated	
Rate IP Addresses	Have FortiClient request the rating of the site by URL and IP address separately, providing additional security against attempts to bypass the FortiGuard Web Filter. If the rating determined by the domain name and the rating determined by the IP address differ, a weighting assigned to the different categories determines the action that FortiClient enforces. The higher weighted category will take precedence in determining the action. This will have 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. 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. An example of how this would work would be if a URL's rating based on the domain name indicated that it belonged 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.
Allow websites when rating error occurs	Configure the action to take with all websites when FortiGuard is temporarily unavailable. This may occur when an endpoint is forced to access a network via a captive portal. FortiClient takes the configured action until contact is reestablished with FortiGuard. Available options are:

Configuration	Description
	- 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
Exclusion List	
Action	Select one of the following actions: - Allow - Block - Monitor
URL	Enter specific URLs to allow, block, or monitor.
Type	Select one of the following types: - Simple - Wildcard - Regular Expression Wildcard characters and Perl Compatible Regular Expressions (PCRE) can be used.

Application Firewall

Configuration	Description
Application Firewall	Enable application control. Enable or disable the eye icon to show or hide this feature from the end user in FortiClient.
General	
Notification Bubbles on User's Desktop When Applications Are Blocked	Enable notification bubbles when applications are blocked.
Detect & Block Exploits	Inspect network traffic for intrusions attempting to exploit known vulnerabilities.
Categories	Enable FortiClient firewall to allow, block or monitor applications based on their signature.

Configuration	Description
	Block, allow or monitor the following categories: - Botnet - Business - Cloud.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. Enable or disable the eye icon to show or hide this feature from the end user in FortiClient.
General	
Allow Personal VPN	Allow users to create, modify, and use personal VPN configurations.
Disable Connect/Disconnect	Disable the *Connect/Disconnect* button when using *Auto Connect* with VPN.

Configuration	Description
Show VPN before Logon	Allow users to select a VPN connection before logging into the system.
Use Windows Credentials	If allowing users to select a VPN connection before logging into the system, enable this option to allow them to use their current Windows username and password.
Minimize FortiClient Console On Connect	Minimize FortiClient after successfully establishing a VPN connection.
Show Connection Progress	Display information on FortiClient dashboard while establishing connections.
Use Vendor ID	Use vendor ID. Enter the vendor ID in the *Vendor ID* field.
Current Connection	Select the current VPN tunnel.
Keep Running Max Tries	The maximum number of attempts to retry a VPN connection that was lost due to network issues. If set to 0, it will retry indefinitely
SSL VPN	Enable 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 *Prefer SSL VPN DNS* to control the DNS cache.
Prefer SSL VPN DNS	When disabled, custom DNS server from SSL VPN will not be added to physical interface. When enabled, custom DNS server from SSL VPN will be prepended to physical interface.
IPsec VPN	Enable IPsec VPN.
	Enable or disable the following: • Beep If Connection Fails • Use Windows Store Certificates ◦ 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 *SSL VPN* or *IPsec VPN*.
Remote Gateway	Enter the IP address/hostname of the remote gateway. You can configure multiple remote gateways by separating each entry with a semicolon. If one gateway is not available, the VPN will connect to the next configured gateway.
Port	Enter the access port. Available if *SSL VPN* is selected. The default port is 443.
Require Certificate	Require a certificate. Available if *SSL VPN* is selected.
Authentication Method	Select the authentication method for the VPN. Available if *IPsec VPN* is selected.
Pre-Shared Key	Enter the preshared key required. Available if *Pre-Shared Key* is selected for *Authentication Method*.
Prompt for Username	Prompt for the username when accessing VPN.
VPN Settings	Available if *IPsec VPN* is selected for the VPN type.
IKE	Select *Version 1* or *Version 2*.
Mode	Select *Main* or *Aggressive*.
Options	Select *Mode Config*, *Manual Set*, or *DHCP over IPsec*.
Specify DNS Server (IPv4)	Specify the DNS server for the VPN tunnel. Available if *Manual Set* is selected.
Assign IP Address (IPv4)	Enter the IP address to assign for the VPN tunnel. Available if *Manual Set* is selected.
Split Table	Enter the IP address and subnet mask for the VPN tunnel. Available if *Manual Set* or *DHCP over IPsec* is selected.
Phase 1	Available if *IPsec VPN* is selected for the VPN type. Select the encryption and authentication algorithms used to generate keys for protecting negotiations and add encryption and authentication algorithms as required. You need to select a minimum of one and a maximum of two combinations. The remote peer or client must be configured to use at least one of the proposals that you define.
Encryption	Select the encryption standard.
Authentication	Select the authentication method.

DH Groups	Select one or more Diffie-Hellman (DH) groups from groups 1, 2, 5, 14, 15, 16, 17, 18, 19 and 20. 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 can use local machine certificates to connect IPsec VPN.
Phase 2	Available if *IPsec VPN* is selected for the VPN type. Select the encryption and authentication algorithms that will be proposed to the remote VPN peer. You can specify up to two proposals. To establish a VPN connection, at least one of the proposals that you specify must match configuration on the remote peer.
Encryption	Select the encryption standard.
Authentication	Select the authentication method.
DH Group	Select one DH group (1, 2, 5, 14, 15, 16, 17, 18, 19, 20, or 21). This must match the DH group that the remote peer or dialup client uses.
Key Life	Set a limit on the length of time that a phase 2 key can be used. The default units are seconds. Alternatively, you can set a limit on the number of kilobytes (KB) of processed data, or both. If you select both, the key expires when the time has passed or the number of KB have been processed. When the phase 2 key expires, a new key is generated without interrupting service.
Enable Replay Detection	Replay detection enables the unit to check all IPsec packets to see if they have been received before. If any encrypted packets arrive out of order, the unit discards them.

Enable Perfect Forward Secrecy (PFS)	Enable PFS. PFS forces a new DH exchange when the tunnel starts and whenever the phase 2 key life expires, causing a new key to be generated each time.
Advanced Settings	
Enable One-Time Password	Enable one-time password. Available if *IPsec VPN* is selected for the VPN type.
Enable XAuth	Enable IKE Extended Authentication (xAuth). Available if *IPsec VPN* is selected for the VPN type.
XAuth Timeout	Only available if *Enable XAuth* 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 *IPsec VPN* is selected for the VPN type.
Enable Single User Mode	Enable single user mode.
Show Passcode	Display Passcode instead of Password in the *VPN* 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 *SSL VPN* is selected 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 *SSL VPN* is selected 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.
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.
On Connect Script	Enable the on connect script. Enter your script. You must also enable this option on the FortiGate.
On Disconnect Script	Enable the disconnect script. Enter your script. You must also enable this option on the FortiGate.

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 proxy.
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 *Period* value.
Scheduled Scan	Configure settings for scheduled scanning.
Schedule Type	Select *Daily*, *Weekly*, *Monthly*.
Scan On	Configure the day the scan will run. This only applies if the schedule type is configured to *Weekly* or *Monthly*. Select a day of the week (Sunday through Monday) or a day of the month (1st through the 31st).
Start At	Configure the time the scan will start.
Automatic Patching	

Configuration		Description
Patch Level		Patches are installed automatically when vulnerabilities are detected. Select one of the following: • Critical: Patch critical vulnerabilities only • High: Patch high severity and above vulnerabilities • Medium: Patch medium severity and above vulnerabilities • Low: Patch low severity and above vulnerabilities • All: Patch all vulnerabilities. Automatic patching may require the endpoint to reboot.
Exclusions		
Exempt Application Vulnerabilities Requiring Manual Update from Vulnerability Compliance Check		All applications that require the endpoint user to manually patch vulnerabilities are excluded from vulnerability compliance check. This option does not exclude applications from vulnerability scanning.
Exclude Selected Applications from Vulnerability Compliance Check		In the *<number> Applications* list, click the applications to exclude from vulnerability compliance check, and they are automatically moved to the *<number> Excluded Applications* list. In the *<number> Excluded Applications* list, click the applications to remove from the exclusion list. Applications on the exclusion list are exempt from needing to install software patches within the time frame specified in FortiGate compliance rules to maintain compliant status and network access. Applications on the list are not excluded from vulnerability scanning.
	Disable Automatic Patching for These Applications	Disable automatic patching for the applications excluded from vulnerability compliance check.

System Settings

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

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.

Configuration	Description
Do Not Allow User to Back Up Configuration	Disallow users from backing up the FortiClient configuration.
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 155.
Language	Configure the language that FortiClient uses. By default, FortiClient uses the system operating language. Select one of the following: • os-default (System operating language, selected by default) • zh-tw (Taiwanese Mandarin) • cs-cz (Czech) • de-de (German) • en-us (United States English) • fr-fr (French) • hu-hu (Hungarian) • ru-ru (Russian) • ja-jp (Japanese) • ko-kr (Korean) • pt-br (Brazilian Portuguese) • sk-sk (Slovak) • es-es (Spanish) • zh-cn (Chinese (Simplified)) • et-ee (Estonian) • lv-lv (Latvian) • lt-lt (Lithuanian) • fi-fi (Finnish) • sv-se (Swedish) • da-dk (Danish) • pl-pl (Portuguese (Portugal)) • nb-no (Norwegian)
Log	Specify FortiClient log settings.

Configuration		Description
Level		This option is available for Chromebook profiles. Generates logs equal to and more critical than the selected level. Select one of the following: • Emergency: The system becomes unstable. • Alert: Immediate action is required. • Critical: Functionality is affected. • Error: An error condition exists and may affect functionality. • Warning: Functionality could be affected. • Notice: Information about normal events. • Info: General information about system operations. • Debug: Debug FortiClient.
Features		Select features to generate logs for: • AntiVirus • Application Firewall • Telemetry • FSSOMA • Proxy • IPsec VPN • AntiExploit • SSL VPN • Update • Vulnerability • Web Filter • Sandbox
Client-Based Logging When On-Net		Include local log messages when FortiClient is onnet. For information about the onnet feature, see the *FortiClient Administration Guide*.
Upload Logs to FortiAnalyzer/FortiManager		This option and all nested options are available for Chromebook profiles. Configure endpoints to sends logs to the FortiAnalyzer or FortiManager at the specified address or hostname. If the *Send Software Inventory* option below is also enabled, FortiClient also sends software inventory information to FortiAnalyzer or FortiManager.
	Upload UTM Logs	Upload unified threat management logs to FortiAnalyzer.
	Upload Vulnerability Logs	Upload vulnerability logs to FortiAnalyzer.
	Upload Event Logs	Upload event logs to FortiAnalyzer.
	Send Software Inventory	Send software inventory to FortiAnalyzer.

Configuration		Description
	IP Address/Hostname	Enter the FortiAnalyzer IP address or hostname/FQDN. With Chromebook profiles, use the format *https://FAZ-IP:port/logging*. If using a port other than the default, use <address>:<port>.
	SSL Enabled	Enable SSL.
	Upload Schedule (minutes)	Configure the upload schedule in minutes.
	Log Generation Timeout (seconds)	Configure the log generation timeout in seconds.
	Log Retention (days)	Configure the duration of time to retain logs in days.
Proxy		
Use Proxy for Updates		Access FortiGuard using the configured proxy.
	Connect to FDN Directly If Proxy Is Offline	Connect to FDN directly if proxy is offline.
Use Proxy for Virus Submission		Use the configured proxy to submit viruses to FortiGuard.
	Type	Configure the type. Options include: • http • socks4 • socks5
	IP Address/Hostname	Enter the proxy server's IP address/hostname.
	Port	Enter the proxy server's port number. The port range is from 1 to 65535.
	Username	If the proxy requires authentication, enter the username. Enter the encrypted or non-encrypted username.
	Password	If the proxy requires authentication, enter the password. Enter the encrypted or non-encrypted username. Enable *Show Password* to show the password in plain text.
Update		Specify whether to use FortiManager 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.

Configuration		Description
	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.
Software Update		Automatically update FortiClient software on endpoints.
	Update Action	Select the option to implement when new software updates are available: • Notify Only The Update Action is set to *Disabled*. The Advanced XML configuration should be: `<update_action>disable</update_action>` • Download And Install
Scheduled Updates		Configure the schedule to check for new software updates and signatures.
	Schedule Type	Select *Interval* or *Daily* for your schedule time.
	Update Every	Configure the interval to check for new software updates and signatures.
FortiGuard Server Location		Configure FortiGuard server location to *Nearest* or *US*. If *Nearest* is selected, the endpoint connects to the FortiGuard server whose IP address is provided by the DNS server. If *US* is selected, the endpoint can only connect to FortiGuard servers available in the United States and does not attempt to access a FortiGuard server outside the U.S.
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. This may be used in a situation where FortiClient is installed on a mail server.

Configuration	Description
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	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. Enable self tests. FortiProxy periodically checks its own connectivity to determine if it is able to proxy other applications' traffic.
Notify	Display a bubble notification when self-testing detects that a third party program has blocked HTTP/HTTPS filtering and SMTP/POP3 AV scanning.
Last Port	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.
Silent Registration	Enable silent connection of endpoints, which means that endpoints are connected to FortiGate or EMS without user interaction. Turn off to require user interaction to connect 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: • 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 *Compliance & Telemetry* tab. This option is only enforced on FortiClients connected to FortiClient EMS. This option does not apply to monitored clients.

Configuration		Description
		This option only applies for endpoints running FortiClient versions earlier than 6.2.0.
On-Net Subnets		Turn on to enable onnet subnets. For details on how FortiClient determines onnet/offnet status, see the *FortiClient Administration Guide*.
	IP Addresses/Subnet Masks	Enter IP addresses/subnet mask to connect to onnet subnets.
	Gateway MAC Address	Enable gateway MAC address.
	MAC Addresses	Enter MAC addresses.
Send Software Inventory		Send installed application information to FortiClient EMS. If the *Upload Logs to FortiAnalyzer/FortiManager* option is enabled, the endpoint also sends the software inventory information to FortiAnalyzer. See Software Inventory on page 102.
Other		
Install CA Certificate on Client		Turn on to select and install a CA certificate on the FortiClient endpoint. You can add certificates by going to *Profile Components > Manage CA Certificates*.
FortiClient Single Sign-On Mobility Agent		Select to 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 `.mobileconfig` file to distribute the configuration profile.
Privacy		
Send Usage Statistics to Fortinet		Submit virus information to FDS. This information is used to improve Fortinet's 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*.

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, as well as which FortiClient features are installed on the endpoint. Deployment packages can also include a Telemetry gateway list for connection to a FortiGate.

Adding FortiClient deployment packages

When you create a FortiClient deployment package in FortiClient EMS, you can specify what FortiClient features to include in the deployment package for the endpoint. You can include a feature in the deployment package, then disable the feature in the profile. Because the feature is included in the deployment package, you can update the profile later to enable the feature on the endpoint.

For example, consider that you create a deployment package that has SSL VPN and IPsec VPN enabled. You then assign the deployment package to a profile where VPN is disabled. The endpoints that the profile is deployed to will have VPN disabled. At a later time, if you enable VPN on the profile, the endpoints will then have VPN enabled, since it was included in the 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.

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

Installer Type	Configure the deployment package to use an official FortiClient installer or a custom FortiClient installer. See FortiClient installers on page 149.
Release	Select the FortiClient release version to install.
Patch	Select the specific FortiClient patch version to install.
Keep updated to the latest patch	Select to 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 installer's name.
Notes	(Optional) Enter any notes about the FortiClient installer.

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

Security Fabric Agent	Enabled by default and cannot be disabled. Installs FortiClient with Telemetry and Vulnerability Scan enabled.
Secure Access Architecture Components	Install FortiClient with SSL and IPsec VPN enabled. Disable to omit SSL and IPsec VPN support from the FortiClient deployment package.
Advanced Persistent Threat (APT) Components	Install FortiClient with APT components enabled. Disable to omit APT components from the FortiClient installer. Includes FortiSandbox detection and quarantine features.
Additional Security Features	Enable any of the following features: • 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. Disable to exclude the features from the FortiClient deployment package.

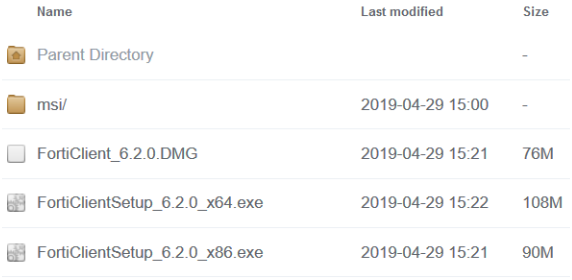
6. Click *Next*. On the *Advanced* tab, set the following options:

Enable automatic registration	Configure FortiClient to automatically connect Telemetry to FortiClient EMS after FortiClient is installed 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 installer to create a desktop shortcut on the endpoint.
Enable start menu shortcut	Configure the FortiClient installer 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 92.
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.

7. 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 Telemetry gateway lists on page 152.

8. 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 177.

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 Telemetry gateway list
- Connection to FortiGate and/or FortiClient EMS
- Auto registration enabled/disabled
- Desktop shortcut enabled/disabled
- Start menu shortcut enabled/disabled
- Notes included when creating the deployment package

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

Deleting FortiClient deployment packages

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 FortiClient deployment packages on page 146.

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. 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 available for download at forticlient.com into the *Add FortiClient Installer* dialog.

To add a custom FortiClient installer:

1. Download a FortiClient installer. See FortiClient installers on page 149. 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 *Browse* button to locate and select a custom 64-bit installer for the Windows operating system.
Windows 32-Bit Installer (ZIP or MSI)	Click the *Browse* 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 *Browse* button to locate and select a custom installer for the macOS operating system.

⚠ Do not upload the installer file for the FortiClient free VPN client as a custom FortiClient installer.

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 149.
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

Profile Components

You can manage CA certificates under *Profile Components*.

Uploading certificates

You can locally upload a CA certificate.

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

Importing certificates

1. Go to *Profile 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.

Telemetry Gateway Lists

Gateway lists are useful when using FortiClient EMS integrated with FortiGate. If using FortiClient EMS without FortiGate, you are not required to use gateway lists.

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

After deploying FortiClient to endpoints, FortiClient uses the gateway list to try and connect FortiClient Telemetry to FortiGate or FortiClient EMS. This connection is based on the gateway list that FortiClient received from FortiClient EMS.

Even if the endpoint is already connected to a FortiGate, you can still assign a gateway list to endpoints as part of an endpoint policy. You can also update existing gateway lists as required. The updates are pushed to endpoints with the next Telemetry communication.

Creating Telemetry gateway lists

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

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

1. Go to *Telemetry Gateway Lists > Manage Telemetry Gateway 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 *System Settings* > *Server*.
Notify FortiGate		Enter the IP address(es) or hostname(s) of the FortiGates. You can also use an FQDN. Press the *Enter* key to add additional entries.

4. Click *Save*.

Exporting Telemetry gateway lists 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.

1. Go to *Telemetry Gateway Lists* > *Manage Telemetry Gateway 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 gateway lists

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

Viewing assigned Telemetry gateway lists

1. Go to *Endpoints* and go to the desired endpoint.
2. View the *Configuration* column. The assigned Telemetry gateway 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 157.

Adding a compliance verification rule

1. Go to *Compliance Verification* > *Compliance Verification Rules*, and click *Add*.
2. In the *Name* field, enter the desired rule name.
3. Toggle *Status* on or off to enable or disable the rule.
4. For *Type*, select *Windows*, *Mac*, or *Linux*. This affects what rule types are available.
5. From the *Rule* dropdown list, select the rule type and configure the related options. Ensure that you click the + button after entering each criterion.

Rule type	Description
Certificate	In the *Subject CN* and *Issuer CN* fields, enter the certificate subject and issuer. You can enter multiple certificates using the + button. You can also use the NOT option to indicate that the rule requires that a certain certificate is not present for the endpoint. 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.
Logged in Domain	In the *Domain* field, enter the domain name. You can enter multiple domain names using the + button. If the rule is configured for multiple domains, the endpoint is considered as satisfying the rule if it belongs to one of the configured domains. This option is not available for Linux endpoints.

Rule type	Description
File	In the *File* field, enter the file path. You can enter multiple files using the + button. You can also use the NOT option to indicate that the rule requires that a certain file is not present on the endpoint. The endpoint must satisfy all 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.
OS Version	From the *OS Version* field, select the OS version. You can enter multiple OS versions using the + button. If the rule is configured for multiple OS versions, the endpoint is considered as satisfying the rule if it has one of the configured OS versions installed.
Running Process	In the *Running Process* field, enter the process name. You can enter multiple processes using the + button. You can also use the NOT option to indicate that the rule requires that a certain process is not running on the endpoint. The endpoint must satisfy all 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.
Registry Key	In the *Registry Key* field, enter the registry key value. You can enter values using the + button. You can also use the NOT option to indicate that the rule requires that a certain registry key is not present on the endpoint. The endpoint must satisfy all 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. This option is only available for Windows endpoints.
Vulnerable Devices	From the *Severity Level* dropdown list, select the desired vulnerability severity level. You can select multiple severity levels using the + button. If the rule is configured for multiple severity levels, the endpoint is considered as satisfying the rule if it has vulnerabilities of one of the configured severity levels present.

6. Under *Assign to*, select *All*.
7. 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.
8. 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 rules: one for endpoints running Process A and another rule for endpoints running Process B. You can configure both rules to apply the "RP" tag to place endpoints running either process in the same dynamic group.

Editing 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*.

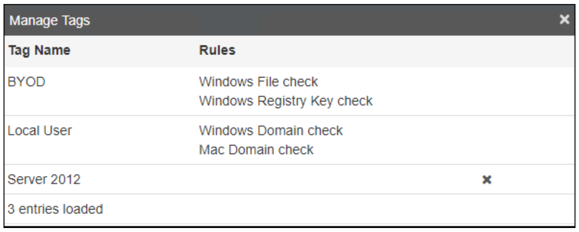
Deleting a compliance verification rule

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.

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.



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*.

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.

Configuring FortiOS dynamic policies using EMS dynamic endpoint groups

After defining compliance verification rules as described in Adding a compliance verification rule on page 155, you can configure FortiOS to receive the dynamic endpoint groups from EMS via the FSSO protocol, using the new "fortiems" FSSO agent type which supports SSL and imports trusted certificates. When a change to the dynamic endpoint groups occurs, EMS sends the update to FortiOS, and FortiOS updates its dynamic policies accordingly. This feature is only available for FortiOS 6.2.0 or a later version.

The following configuration is necessary for this feature:

1. In FortiClient EMS, create compliance verification rules.
2. After Telemetry communication has occurred between EMS and FortiClient, ensure that EMS has dynamically grouped endpoints based on the compliance verification rules.
3. In FortiOS, configure the following options to allow FortiOS to pull dynamic endpoint groups from EMS:
    a. Create the fortiems FSSO agent.
    b. Configure EMS FSSO groups.
    c. Create a user group based on EMS dynamic endpoint groups.
4. In FortiOS, create a dynamic firewall policy for the user group.

When a dynamic endpoint group event occurs (such as an endpoint being added to or removed from a dynamic endpoint group), EMS sends the updates to FortiOS. FortiOS updates firewall policies accordingly, providing dynamic access control based on endpoint status.

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

To add a compliance verification rule in EMS:

Create a compliance verification rule to dynamically group endpoints. See Adding a compliance verification rule on page 155.

To ensure EMS has dynamically grouped endpoints:

After Telemetry communication has occurred between EMS and FortiClient, ensure that EMS has dynamically grouped endpoints using tags by going to *Compliance Verification* > *Host Tag Monitor*. See Host Tag Monitor on page 157.

To create the fortiems FSSO agent:

Run the following commands in the FortiOS CLI:

```
config user fsso
   edit "<agent_name>"
      set server "<EMS_IP_address>"
      set type fortiems
      set ssl enable
      set ssl-trusted-cert "Fortinet_CA"
   next
end
```

In the above CLI sample, `set ssl-trusted cert` is optional. For this option to function, you must upload a certificate in *System Settings* > *Server* > *EMS FSSO Settings*.

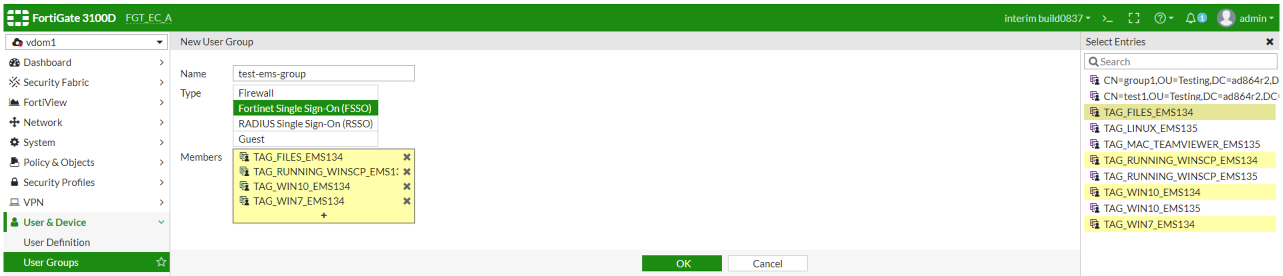
To configure EMS FSSO groups in FortiOS:

In the FortiOS CLI, run the following commands. For the FSSO group name, use the format `TAG_<tag_name>`, where `<tag_name>` is the tag name configured in EMS as described in Adding a compliance verification rule on page 155. For example, if you configured the tag with the name "WIN10_EMS134" in EMS, the FSSO group name is `TAG_WIN10_EMS134`. For `server-name`, enter the FSSO agent name configured in To create the fortiems FSSO agent.

```
config user adgrp
   edit "TAG_<tag_name>"
      set server-name "<agent_name>"
   next
end
```

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. You can identify the dynamic endpoint groups pulled from EMS because the names begin with TAG_, followed by the tag name from EMS.



Name: test-ems-group

Type: Firewall / Fortinet Single Sign-On (FSSO) / RADIUS Single Sign-On (RSSO) / Guest

Members: TAG_FILES_EMS134, TAG_RUNNING_WINSCP_EMS1:, TAG_WIN10_EMS134, TAG_WIN7_EMS134

Select Entries:
- CN=group1,OU=Testing,DC=ad864r2,D
- CN=test1,OU=Testing,DC=ad864r2,DC
- TAG_FILES_EMS134
- TAG_LINUX_EMS135
- TAG_MAC_TEAMVIEWER_EMS135
- TAG_RUNNING_WINSCP_EMS134
- TAG_RUNNING_WINSCP_EMS135
- TAG_WIN10_EMS134
- TAG_WIN10_EMS135
- TAG_WIN7_EMS134

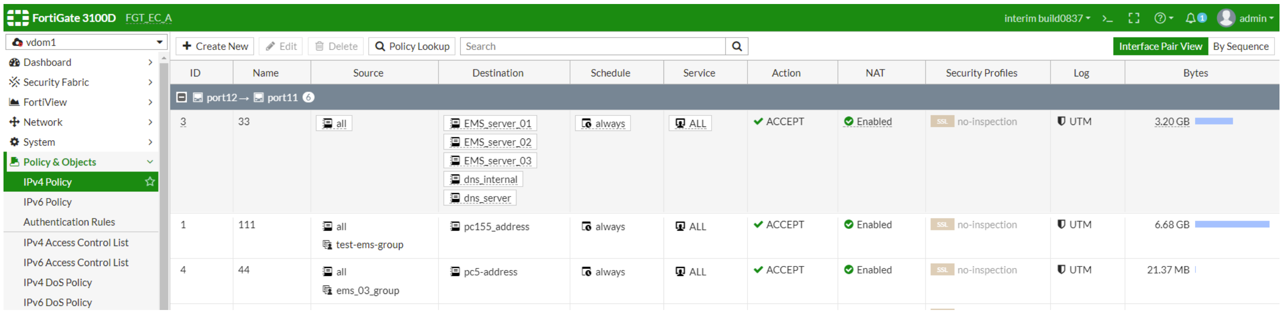
5. Select the desired dynamic endpoint groups. Endpoints that currently belong to this EMS dynamic endpoint group will be members of this FortiOS user group.
6. Click *OK*.

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
port12 → port11 6										
3	33	all	EMS_server_01 EMS_server_02 EMS_server_03 dns_internal dns_server	always	ALL	✓ ACCEPT	✓ Enabled	SSL no-inspection	UTM	3.20 GB
1	111	all test-ems-group	pc155_address	always	ALL	✓ ACCEPT	✓ Enabled	SSL no-inspection	UTM	6.68 GB
4	44	all ems_03_group	pc5-address	always	ALL	✓ ACCEPT	✓ Enabled	SSL 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 using the FSSO protocol. For information on connecting a FortiGate to EMS using the FSSO protocol, see Configuring FortiOS dynamic policies using EMS dynamic endpoint groups on page 158.

For each connected FortiGate, you can view the following information:

- 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.

Deployment

You can use FortiClient EMS to deploy FortiClient on endpoints that are part of an AD server. This does not apply to Chromebooks. Deploying FortiClient from FortiClient EMS requires the following steps:

1. Preparing the AD server for deployment
2. Deploying FortiClient on endpoints

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 that are part of an AD server.

You cannot use workgroups to deploy an initial installation of FortiClient to endpoints. However, after FortiClient is installed 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 161
2. Configuring required Windows services on page 161
3. Creating deployment rules for Windows firewall on page 162
4. Configuring Windows firewall domain profile settings on page 162

Configuring 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

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

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)* box 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

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.

Deploying FortiClient on endpoints

Before you can successfully deploy a FortiClient installation from FortiClient EMS using an AD server, you must have prepared the AD server. See Preparing the AD server for deployment on page 161.

1. Add the AD server to FortiClient EMS by adding a domain. See Adding endpoints using an AD domain server on page 71.
2. Add a FortiClient deployment package to FortiClient EMS. See Adding FortiClient deployment packages on page 146.
3. Add a profile, select the FortiClient deployment package, and configure FortiClient features in the profile. See Creating profiles to deploy FortiClient on page 109.
4. Create an endpoint policy that is configured with desired profile. Configure the endpoint policy to apply to a branch of the AD domain to push the FortiClient installation process on the endpoints. See Adding an endpoint policy on page 105.
5. Verify the deployment by monitoring FortiClient connections to the FortiClient EMS.

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.

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: • 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 172. • EMS: User accounts created in FortiClient EMS.
Role	Admin role assigned to the user. See Configuring admin roles on page 168.
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 disabled accounts on page 167.
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 Configuring admin roles on page 168.
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 *Trusted Hosts* field, enter a trusted host machine's IP address. Use the + button to add multiple trusted host machines.
Comment	Enter optional comments/information for the Windows/LDAP user.

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 Configuring admin roles on page 168.
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 *Trusted Hosts* field, enter a trusted host machine's IP address. Use the + button to add multiple trusted host machines.
Comment	Enter optional comments/information for the user.

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

Activating disabled accounts

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 174.

When an account is disabled, 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 account is activated, 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.

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.

Configuring admin roles

You can use admin roles to define the permissions each administrator account has in FortiClient EMS. You can use one of the four default admin roles in FortiClient EMS (super administrator, standard administrator, endpoint administrator, restricted administrator) 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 four default admin roles in FortiClient EMS. You cannot edit or delete these admin roles.

Name	Description
Super administrator	Most privileged admin role. Complete access to all FortiClient EMS permissions, including modification, user permissions, approval, discovery, and deployment. Only built-in role that has access to the *Administration* section of the GUI. Has access to all configured Windows and LDAP servers and users and has the authority to configure user privileges and permissions. The default admin account is configured as a Super Administrator and cannot be changed to another admin role.
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.
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

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 169.
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 172.
Manage Google domains*	Manage connections to Google domains to decide which Chromebooks to manage. See Google Domains on page 88.
Manage custom groups	Create, rename, and edit groups to manage endpoints. See Creating groups on page 71.
Run commands on endpoints	Perform actions to endpoints on the *Endpoints* pane, including uploading FortiClient logs, requesting diagnostic results, and so on. See Managing endpoints on page 81.
Block/Unblock/Quarantine/Unquarantine/Reregister endpoints	Manage endpoint access to the network through blocking, quarantine, and registration. See Managing endpoints on page 81.
Manage and assign endpoint policies	See Endpoint Policy on page 105.
View group assignment rules	View group assignment rules. See Group assignment rules on page 92.
Manage group assignment rules	Create, delete, and edit group assignment rules. See Group assignment rules on page 92.
View endpoint filter bookmarks	View endpoint filter bookmarks. See Using bookmarks to filter the list of endpoints on page 80.
Manage endpoint filter bookmarks	Create, delete, and edit endpoint filter bookmarks. See Using bookmarks to filter the list of endpoints on page 80.
View quarantine management	View lists of quarantined and allowlisted files. See Quarantine Management on page 97.

Permission	Link to description
Manage quarantine management	Allowlist and restore quarantined files and remove files from the allowlist. See Quarantine Management on page 97.
View software inventory	See Software Inventory on page 102.
Manage software inventory	See Software Inventory on page 102.

Policy permissions

Permission	Link to description
View endpoint policies*	View endpoint policies. See Endpoint Policy on page 105.
View endpoint profiles*	View endpoint profiles. See Endpoint Profiles on page 108.
Manage endpoint profiles*	Create, delete, and edit endpoint profiles. See Endpoint Profiles on page 108.
View host verification rules	View compliance verification rules. See Compliance Verification Rules on page 155.
Manage host verification rules	Create, delete, and edit compliance verification rules. See Compliance Verification Rules on page 155.
View gateway lists	View gateway lists. Telemetry Gateway Lists on page 152.
Manage gateway lists	Create, delete, and edit gateway lists. See Telemetry Gateway Lists on page 152.
View installers	View installers. Managing installers on page 146
Manage installers	Create, delete, and edit installers. See Managing installers on page 146.
View CA certificates	View CA certificates. See Profile Components on page 151.
Manage CA certificates	Upload, import, and delete CA certificates. See Profile Components on page 151.

Setting permissions

Permission	Link to description
View server	View *Server* settings. See Configuring Server settings on page 177

Permission	Link to description
settings*	
Manage server settings*	Modify *Server* settings. See Configuring Server settings on page 177.
View FortiGuard settings	View *FortiGuard* settings. See Configuring FortiGuard settings on page 181.
Manage FortiGuard settings	Modify *FortiGuard* settings. See Configuring FortiGuard settings on page 181.
View endpoint settings	View *Endpoints* settings. See Configuring Endpoints settings on page 182.
Manage endpoint settings	Modify *Endpoints* settings. See Configuring Endpoints settings on page 182.
View login banner settings*	View login banner settings. See Configuring the login banner on page 183.
Manage login banner settings*	Modify login banner settings. See Configuring the login banner on page 183.
View alert settings*	View *Alerts* settings. See Alerts on page 183.
Manage alert settings*	Modify *Alerts* settings. See Alerts on page 183.
View custom message settings	View endpoint quarantine message settings. See Customizing the endpoint quarantine message on page 186.
Manage custom message settings	Modify endpoint quarantine message settings. See Customizing the endpoint quarantine message on page 186.

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

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 distinguished name. You must use only capital letters when configuring the DN.
Bind type		Select *Simple*, *Anonymous* or *Regular* for the bind type.
	Username	Appears only when the *Regular* bind type is selected. Enter the username.
	Password	Appears only when the *Regular* 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

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

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 configured in minutes when adding the user server.
Address	User server's IP address.
Distinguished Name	User server's distinguished name.
Username	Username used to connect to the user server.

Configuring 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 user with Super Administrator permissions can reactivate their account. See Activating disabled accounts on page 167.
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*.

Database management

You can back up and restore the FortiClient EMS database.

Backing 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

1. Go to *Administration* > *Restore Database*.
2. Click *Browse*.
3. Locate the database backup file, and click *Open*.
4. In the *Password* box, 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.

Activating, upgrading, and renewing licenses

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 20.

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

- Logging into FortiCare on page 175. You can log into your FortiCare account to activate EMS using that account. Once an EMS license expire, EMS uses the FortiCare account to obtain a new license file, if available on that account.
- Uploading a license file for activation, upgrade, or renewal on page 175. You can upload a license file to EMS. This functions in the same way as in EMS versions prior to 6.2.0.

You must use one of the above methods to activate an EMS license before you can manage any endpoints with EMS.

Logging into FortiCare

To retrieve license information from FortiCare:

1. Go to *Administration* > *Configure License*.
2. For *License Source*, select *FortiCare*.
3. In the *Account ID/Email* field, enter your FortiCare account ID or email address.
4. In the *Password* field, enter your FortiCare account password.
5. Click *Login & Update License*. Once your account information is authenticated, EMS updates the *Configure License* page with the serial number and license information that it retrieved from FortiCare.

EMS reports the following information to FortiCare. FortiCare 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.

Uploading a license file for activation, upgrade, or renewal

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*.

Logs

Viewing 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.

Downloading logs

You can download the logs generated by FortiClient EMS.

1. Go to *Administration* > *Logs*.
2. Click *Download*.
   A zip of the raw logs is downloaded to your computer.

System Settings

This section describes FortiClient EMS 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.

1. Go to *System Settings* > *Server*.
2. Configure the following options under *Shared Settings*. These settings are shared between 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.
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 *Listen on IP Addresses* 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 *Custom hostname* box 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.
	Pre-defined hostname	Available when *Remote HTTPS Access* is enabled. Displays the predefined hostname. You cannot change the name.
	Custom hostname	Available when *Remote HTTPS Access* 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 *Remote HTTPS Access* is turned on. If this option is enabled, if you attempt to remotely access FortiClient EMS at *http://<server_name>*, this automatically redirects to *https://<server_name>*.
SSL certificate		Displays the currently imported SSL certificate. If you have already uploaded an SSL certificate, a *Replace* button displays.
Certificate		Browse and upload a new SSL certificate file.
Password		Configure a new SSL password.

3. Configure the following options under *EMS Settings*. These settings are used by FortiClient EMS 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.
DHCP onnet/offnet		Monitor endpoints within the company network (onnet). Endpoints that are connected to FortiClient EMS from outside the company network are offnet endpoints. See Determining onnet/offnet status.
Enable TLS 1.0/1.1		Enable TLS 1.0 and 1.1 for file downloads. You must enable this option when upgrading FortiClient on a Windows 7 device via FortiClient EMS.
FortiClient download URL		FortiClient deployment packages created in FortiClient EMS are available for download at this URL.
	Open port 10443 in Windows Firewall	Open port 10443 or close port 10443. Port 10443 is used to download FortiClient.
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 *Replace* button displays.
Certificate	Browse and upload a new SSL certificate file. See Adding SSL certificates to FortiClient EMS for Chromebook endpoints on page 180.

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 *Reset* button. This restores the default service account. You need to *Save* the settings for the change to take effect.
ID	Available if the *Update service account* button is clicked. Enter a new service account ID.
Private key	Available if the *Update service account* button is clicked. Upload a new service account private key.

6. Configure the following options under *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 *Replace* button displays.
Certificate	Browse and upload a new SSL certificate file.
Password	Configure a new SSL password.

7. Click *Save*.

Determining onnet/offnet status

There are two settings in EMS that affect FortiClient onnet/offnet status:

- *DHCP onnet/offnet*
- *System Settings* > *Endpoint Control* > *On-Net Subnets* on the endpoint's assigned profile. See System Settings on page 138.

The table below shows how the *DHCP onnet/offnet* and *On-Net Subnets* settings and Option 224 serial number affect the endpoint's onnet/offnet status. You can configure Option 224 with any Fortinet device's serial number. EMS assumes that FortiClient is behind a FortiGate and onnet with that FortiGate.

DHCP onnet/offnet	On-Net Subnets	Option 224 serial number	Resulting endpoint status
Disabled	Disabled	N/A	When onnet subnets are not configured, onnet/offnet status is related to the endpoint's online/offline status (whether it is connected to EMS). An online status causes the endpoint to be onnet, while an offline status causes the endpoint to be offnet.
Enabled	Disabled	Not configured	Same as above.
Enabled	Disabled	Configured	Onnet

DHCP onnet/offnet	On-Net Subnets	Option 224 serial number	Resulting endpoint status
			Since Option 224 is configured with a Fortinet device's serial number, EMS assumes FortiClient is onnet with that FortiGate.
Disabled or enabled	Enabled, with subnet configured. Endpoint IP address is in the configured subnet.	Configured or not	Onnet The endpoint is inside the onnet networks configured in *On-Net Subnets*.
Disabled or enabled	Enabled, with subnet configured. Endpoint IP address is not in the configured subnet.	Configured or not	Offnet The endpoint is outside the onnet networks configured in *On-Net Subnets*.

The following are examples on how FortiClient determines the endpoint status when connected to EMS only. For details on how FortiClient determines onnet/offnet status in managed mode with FortiGate and EMS, see the *FortiClient Administration Guide*.

An endpoint has an offline offnet status when it cannot connect FortiClient Telemetry to EMS and is outside one of the onnet networks.

An endpoint has an offline onnet status when it cannot connect FortiClient Telemetry to EMS but is inside one of the onnet networks.

Adding SSL certificates to FortiClient EMS for Chromebook endpoints

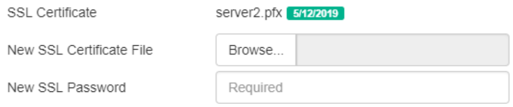
You must add an SSL certificate to FortiClient EMS to allow Chromebooks to connect to FortiClient EMS.

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.

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* box, enter the password.
5. Click *Test*.
6. Click *Save*.

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



SSL Certificate: server2.pfx 5/12/2019

New SSL Certificate File: Browse...

New SSL Password: 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.

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

Log level	Select the level of messages to include in FortiClient EMS logs. For example, if you select *Info*, all log messages from *Info* to *Emergency* are added to the FortiClient EMS logs.
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 daysthat 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 FortiGuard settings

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

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 not available.

3. Click *Save*.

Configuring 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.
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.
Automatically upload avatars	FortiClient uploads user avatars to all FortiGates, FortiAnalyzers, and FortiClient EMS servers it is connected to.

Allow duplicate FortiClient registrations	Allows duplicate FortiClient registrations by assigning the duplicate registrations new UIDs. Enabling this feature requires all devices to reregister, and EMS loses their historical event data. This setting is only supported for FortiClient 6.2 endpoints.

3. Click *Save*.

Configuring the login banner

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

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

Alerts

Configuring EMS Alerts

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

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 184.

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
   k. Endpoint is not compliant

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).

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 *None*, *STARTTLS*, or *SMTPS* for the security type, or select the *Auto Detect* button to automatically select the security type. If *STARTTLS* or *SMTPS* is selected, the *Username* and *Password* boxes 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 *Enter* to add more email addresses.
Test subject		Test email's subject.
Test message		Test email's message.
Test recipient		Email address to send the test email to.
Send Test Email		Click the button to test the configured email settings.

3. Click *Save*.

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

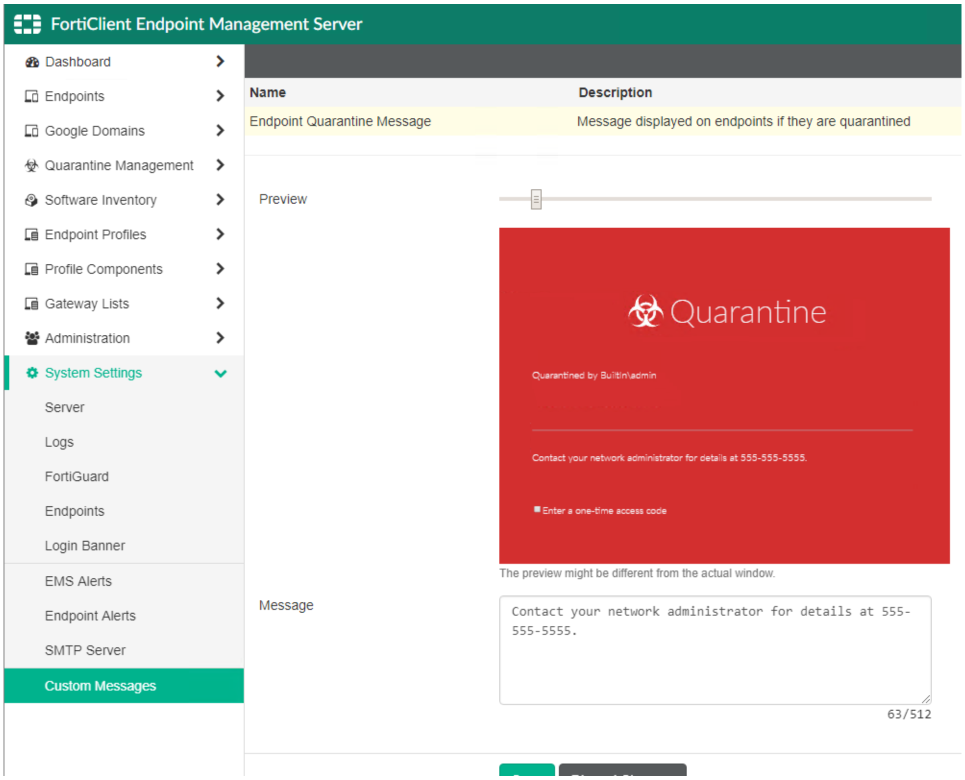
You can customize messages that display on endpoints in certain situations, such as if EMS has quarantined the endpoint. For example, you can customize the message to include your organization's help desk phone number so that users can contact the network administration about their machine.

Customizing the endpoint quarantine message

You can customize the message that displays on an endpoint when FortiClient EMS has quarantined it.

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*.



Name	Description
Endpoint Quarantine Message	Message displayed on endpoints if they are quarantined

Quarantined by Builtin\admin

Contact your network administrator for details at 555-555-5555.

■ Enter a one-time access code

The preview might be different from the actual window.

Message: Contact your network administrator for details at 555-555-5555.

63/512

Customizing Web Filter messages

You can customize the messages that display on an endpoint in in-browser Web Filter result pages.

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 page

   Some customization fields apply to all messages, while others apply to only specific messages. This is indicated beside the field name.
3. In the left pane, enable/disable the fields and enter the desired messages. You can also upload images for logo and icon fields. The right pane displays previews of the messages.
4. Click *Save*.

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.

1. Go to *Help* > *Create Support Package*.
2. In the *Password* box, 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* box, enter the password again.
4. Click *Create*.

Change log

Date	Change Description
2019-04-16	Initial release.
2019-04-18	Updated Upgrading Microsoft SQL Server Express to Microsoft SQL Server Standard or Enterprise on page 37 and Uninstalling FortiClient EMS on page 39.
2019-04-29	Updated FortiClient EMS on page 20.
2019-05-08	Updated Adding FortiClient deployment packages on page 146.
2019-05-22	Updated Configuring Server settings on page 177.
2019-05-23	Updated Required services and ports on page 22.
2019-06-07	Updated Licensing FortiClient EMS on page 36.
2019-06-12	Updated for licensing information.
2019-06-18	Updated Configuring Endpoints settings on page 182.
2019-07-03	Updated Adding endpoints on page 71 and Adding a user server on page 172.
2019-07-12	Updated Adding a custom FortiClient installer on page 149.
2019-07-15	Updated Configuring FortiOS dynamic policies using EMS dynamic endpoint groups on page 158.
2019-07-31	Updated System requirements on page 20.
2019-08-07	Updated Licensing FortiClient EMS on page 36.
2019-12-20	Updated FortiClient EMS on page 20 and Upgrading from an earlier FortiClient EMS version on page 25.
2020-01-29	Updated Installation commands for remote existing databases on page 33.