



FortiClient EMS - QuickStart Guide

Version 6.4.7

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

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

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



November 25, 2021

FortiClient EMS 6.4.7 QuickStart Guide

04-647-614182-20211125

TABLE OF CONTENTS

Introduction	5
Supported installation platforms	5
Requirements for managing Chromebooks	5
Required services and ports	5
Deployment options	8
Chromebook setup	10
Install preparation for managing Chromebooks	11
How FortiClient EMS and FortiClient work with Chromebooks	11
Installation	13
Downloading the installation file	13
Installing FortiClient EMS	13
Licensing EMS by logging in to FortiCloud	15
Starting FortiClient EMS and logging in	17
Configuring EMS after installation	17
Windows, macOS, and Linux endpoint management setup	19
FortiClient EMS	19
FortiClient EMS integrated with FortiGate	20
Configuring user accounts	20
Adding endpoints	21
Adding a FortiClient deployment package	22
Preparing Windows endpoints for FortiClient deployment	25
Creating a deployment configuration	25
Viewing endpoints	26
Viewing the Endpoints pane	26
Using the quick status bar	31
Viewing endpoint details	32
FortiClient EMS for Chromebooks setup	33
Google Admin Console setup	33
Logging into the Google Admin console	33
Adding the FortiClient Web Filter extension	34
Configuring the FortiClient Web Filter extension	34
Adding root certificates	35
Disabling access to Chrome developer tools	37
Disallowing incognito mode	37
Disabling guest mode	38
Blocking the Chrome task manager	38
Service account credentials	39
Configuring default service account credentials	39
Configuring unique service account credentials	40
Adding SSL certificates	44
Adding an SSL certificate to FortiClient EMS for Chromebook endpoints	45
Adding SSL certificates to FortiAnalyzer	45
Adding a Google domain	46

Configuring Chromebook profiles	46
Adding a new Chromebook profile	46
Enabling and disabling Safe Search	47
Adding a Chromebook policy	48
Viewing domains	48
Viewing the Google Users pane	48
Viewing user details	49
Change log	51

Introduction

This guide describes how to install and set up FortiClient Endpoint Management Server (EMS) for the first time. You can use FortiClient EMS to deploy and manage FortiClient endpoints. This guide also describes how to set up the Google Admin console to use the FortiClient Web Filter extension. Together the products also provide web filtering for Google Chromebook users.



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

Supported installation platforms

You can install FortiClient EMS on Microsoft Windows Server 2012 R2 or newer.



For information about minimum system requirements and supported platforms, see the [FortiClient EMS Release Notes](#).

Requirements for managing Chromebooks

Using FortiClient EMS for managing Chromebooks requires the following components and knowledge:

- FortiClient EMS installer
- FortiClient Web Filter extension available in the Google Web Store for Chrome OS
- Google Workspace account
- Knowledge of administering the Google Admin console
- Domain configured in the Google Admin console
- SSL certificate to support communication between FortiClient Web Filter extension and FortiClient EMS
- SSL certificate to support communication between FortiClient Web Filter extension and FortiAnalyzer for logging, if using
- Unique set of service account credentials

Required services and ports

You must ensure that you enable required ports and services for use by FortiClient EMS and its associated applications on your server. The required ports and services enable FortiClient EMS to communicate with endpoints and servers

running associated applications. You do not need to enable ports 8013 and 10443 as the FortiClient EMS installation opens these.

Communication	Usage	Protocol	Port	Incoming/Outgoing	How to customize
FortiClient Telemetry	FortiClient endpoint management	TCP	8013 (default)	Incoming	Installer/GUI
Samba (SMB) service	FortiClient EMS uses the SMB service during FortiClient initial deployment.	TCP	445	Outgoing	N/A
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC)	FortiClient EMS connects to endpoints using RPC for FortiClient initial deployment.	TCP	135 1024-5000* 49152-65535*	Outgoing	You can configure ranges noted with *. See How to configure RPC dynamic port allocation to work with firewalls.
Active Directory server connection	Retrieving workstation and user information	TCP	389 (LDAP) or 636 (LDAPS)	Outgoing	GUI
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
SMTP server/email	Alerts for FortiClient EMS and endpoint events. When an alert is triggered, EMS sends an email notification.	TCP	25 (default)	Outgoing	GUI
FortiClient endpoint probing	FortiClient EMS uses ICMP for endpoint probing during FortiClient initial deployment.	ICMP	N/A	Outgoing	N/A

Communication	Usage	Protocol	Port	Incoming/Outgoing	How to customize
FSSO	Connection to FortiOS.	TCP	8000	Incoming	N/A

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

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

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

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

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

Usage	Server URL			Protocol	Port	Incoming/Outgoing	How to customize
	Global	U.S.	Europe				
AV/vulnerability signature update	forticlient.fortinet.net myforticlient.fortinet.net	usforticlient.fortinet.net	N/A	TCP	80	Outgoing	N/A

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

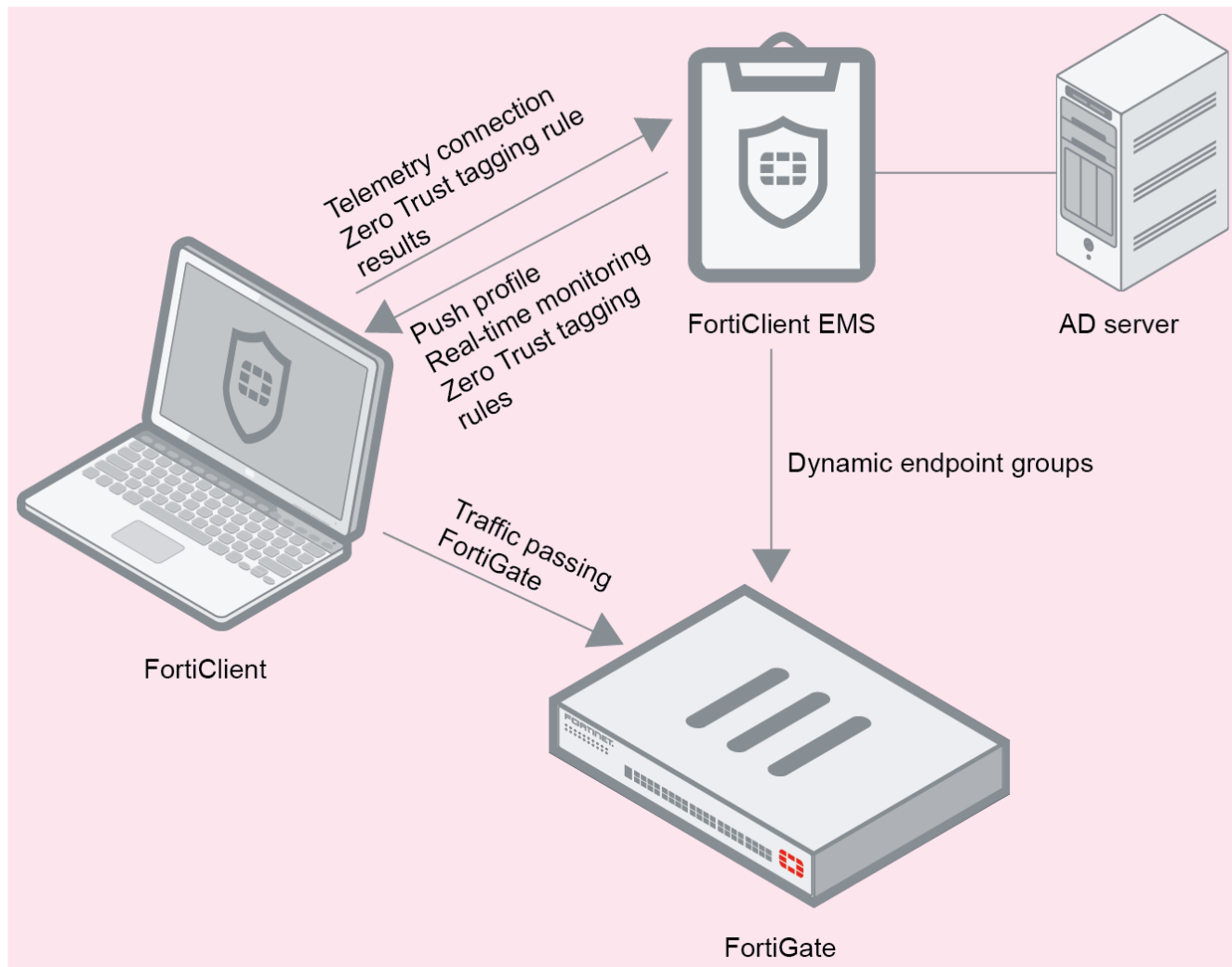


For the list of required services and ports for FortiClient, see the [FortiClient Administration Guide](#).

Deployment options

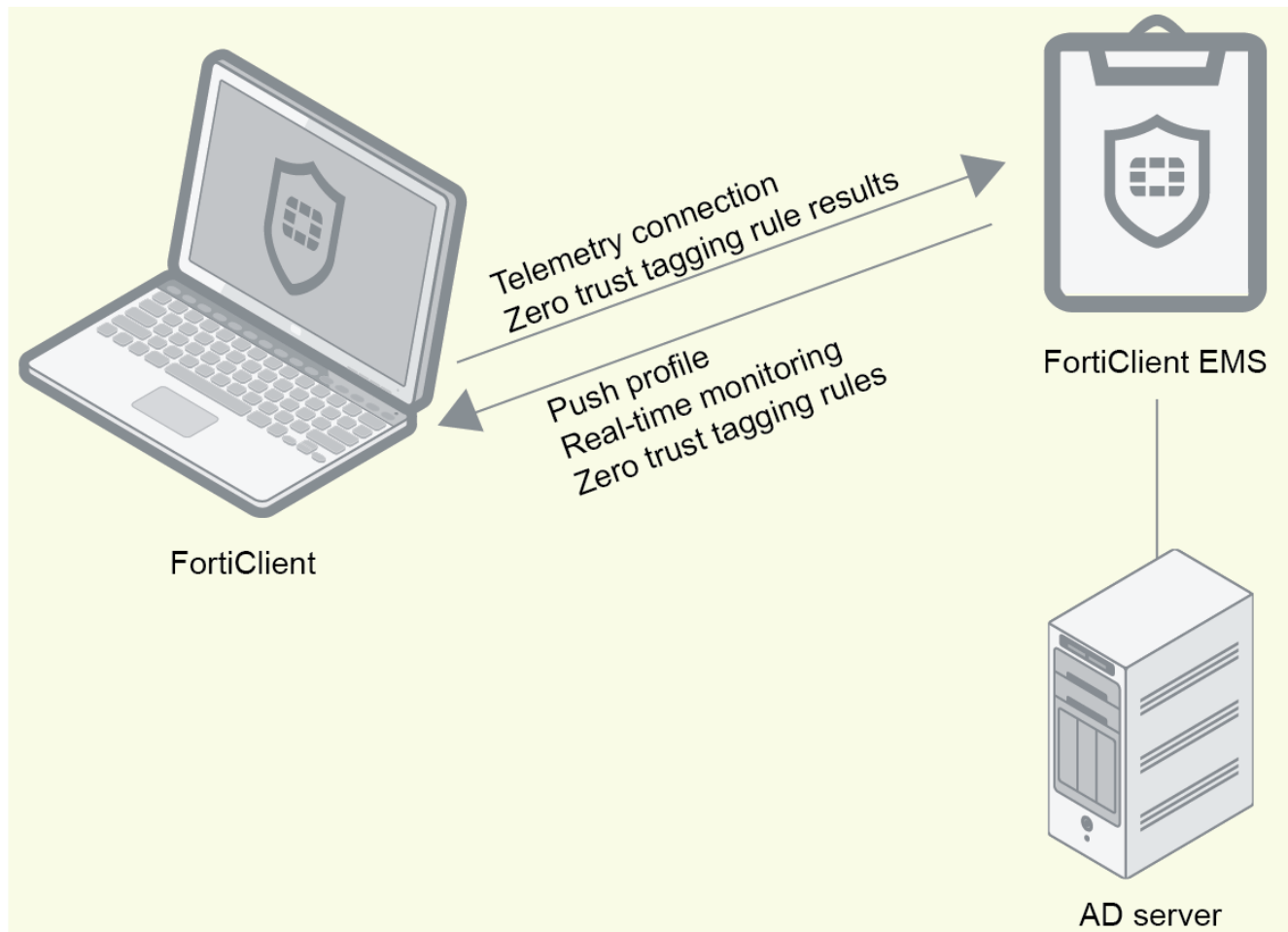
FortiClient EMS supports the following deployment scenarios: participating in the Fortinet Security Fabric or standalone.

Security Fabric



This deployment requires a FortiGate and supports NAC. In this scenario, FortiClient Telemetry connects to EMS to receive a profile of configuration information as part of an endpoint policy. EMS connects to FortiGate to participate in the Security Fabric and allow endpoints to participate in the Fabric. The FortiGate can also receive dynamic endpoint group lists from EMS and use them to build dynamic firewall policies. Depending on the EMS Zero Trust tagging rules and policies configured in FortiOS, the FortiClient endpoint may be blocked from accessing the network.

Standalone



Standalone mode does not require a FortiGate. In standalone mode, EMS deploys FortiClient on endpoints, and endpoints connect Telemetry to EMS to receive configuration information from EMS. EMS also sends Zero Trust tagging rules to FortiClient, and uses the results from FortiClient to dynamically group endpoints in EMS. You use EMS to deploy, configure, and monitor FortiClient endpoints.

Chromebook setup

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

Install preparation for managing Chromebooks

Google Workspace account

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

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

You can sign up for a Google Workspace account [here](#).

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

SSL certificates

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

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

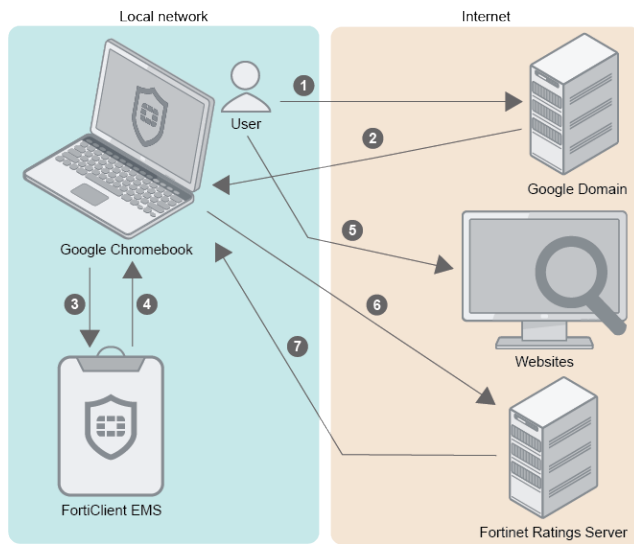
If you are using a public SSL certificate, the FQDN can be included in *Common Name* or *Subject Alternative Name*. You must add the SSL certificate to FortiClient EMS. See [Adding an SSL certificate to FortiClient EMS for Chromebook endpoints on page 45](#). You do not need to add the root certificate 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 35](#).

How FortiClient EMS and FortiClient work with Chromebooks

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

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



Installation

FortiClient EMS is necessary to install on endpoints. For a complete endpoint solution, use FortiClient EMS for central management and provisioning of endpoints.

Following is a summary of how to install and start FortiClient EMS:

1. Download the installation file. See [Downloading the installation file on page 13](#).
2. Install FortiClient EMS. See [Installing FortiClient EMS on page 13](#).
3. Start FortiClient EMS and log in. See [Starting FortiClient EMS and logging in on page 17](#).

For information about upgrading FortiClient EMS, see the [FortiClient EMS Release Notes](#).



A video on how to install, log in, and change your administrator password is available in the [Fortinet Video Library](#).

Downloading the installation file

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

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

The following installation file is available for FortiClient EMS:

`FortiClientEndpointManagement_6.4.7.<build>_x64.exe`

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

Installing FortiClient EMS

The FortiClient EMS installation package includes:

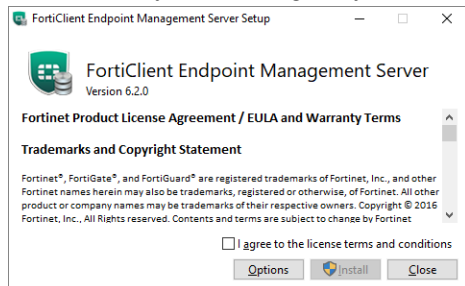
- FortiClient EMS
- Microsoft SQL Server 2017 Express Edition
- Apache HTTP server



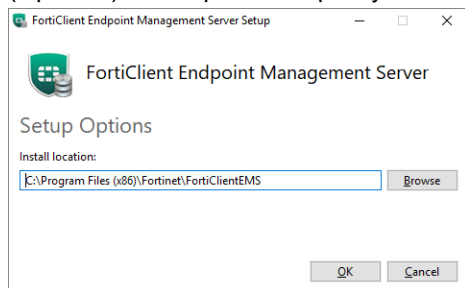
Installing FortiClient EMS requires local administrator rights. Internet access is recommended, but optional, during installation. SQL Server may require some dependencies to be downloaded over the internet. EMS will also try to download information about FortiClient signature updates from FortiGuard.

To install EMS:

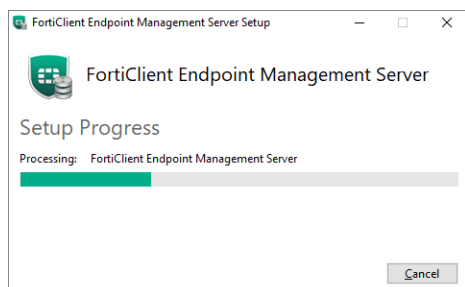
1. Do one of the following:
 - a. If you are logged into the system as an administrator, double-click the downloaded installation file.
 - b. If you are not logged in as an administrator, right-click the installation file, and select *Run as administrator*.
2. If applicable, select **Yes** in the *User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



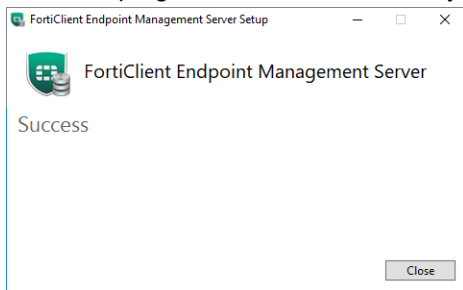
4. (Optional) Click *Options* to specify a custom directory for the FortiClient EMS installation.



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



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



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

Licensing EMS by logging in to FortiCloud

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

To apply a trial license to FortiClient EMS:

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

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

To apply a paid license to FortiClient EMS:

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

1. Log in to your FortiCloud account on [Customer Service & Support](#).
2. Go to *Asset > Register/Activate*.
3. In the *Registration Code* field, enter the *Contract Registration Code* from your service registration document. Configure other fields as required, then click *Next*.

FORTINET

PLEASE REMEMBER TO REGISTER YOUR CONTRACT REGISTRATION CODE

Service Entitlement Summary

Date	:	April 22, 2020
Purchase Order Number	:	ITF0017881
Contract Registration Code	:	3922UW44334

4. Do one of the following:

- a. If this is the first license that you are applying to this EMS server, do the following:
 - i. Click *Register*.
 - ii. In the *Hardware ID* field, enter the hardware ID found in *Dashboard > Status > License Information widget > Config License* in EMS. If you register the license prior to installing EMS, you must enter the hardware ID after installation. Configure other fields as required, then click *Next*.
 - iii. Complete the registration, then click *Confirm*.
 - iv. In EMS, go to *Dashboard > Status > License Information widget > Config License*.
 - v. For *License Source*, select *FortiCare*.
 - vi. In the *FortiCloud Account* field, enter your FortiCloud account ID or email address.
 - vii. In the *Password* field, enter your FortiCloud account password.
 - viii. Click *Login & Update License*. Once your account information is authenticated, EMS updates the *Configure License* page with the serial number and license information that it retrieved from FortiCloud.
- b. As described in the [FortiClient EMS Administration Guide](#), you can apply multiple license types to the same EMS server. For example, if you have already applied a Fabric Agent license to your EMS server, you can apply another license type, such as a Chromebook license, to the same EMS server. If desired, add another license type:
 - i. On the *Registration Confirmation* page, when applying an additional license type, you must select *Renew* on the contract registration screen, regardless of the license types of the first and subsequent licenses. Selecting *Renew* combines the new license with any existing licenses for the EMS server and allows you to add the new license type to EMS while retaining previously applied license(s).



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

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

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

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



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



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

Starting FortiClient EMS and logging in

FortiClient EMS runs as a service on Windows computers.

To start FortiClient EMS and log in:

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

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

Configuring EMS after installation

You can configure an FQDN for EMS.

FortiClient's connection to EMS is critical to managing endpoint security. Managing this is relatively easy for internal devices. For external devices or devices that may leave the internal network, you must consider how to maintain this

connection. FortiClient can connect to EMS using an IP address or fully qualified domain name (FQDN). An FQDN is preferable for the following reasons:

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

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

Alternatively, you can use a private IP address for the connection. This configuration would require external clients to establish a VPN connection to reach the EMS (VPN policies permitting). This configuration can be problematic if all endpoints need an urgent update but some are not connected to VPN at that time.

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

To enable remote access to FortiClient EMS:

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

To remotely access FortiClient EMS:

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

Windows, macOS, and Linux endpoint management setup

This section describes how to set up FortiClient EMS for Windows, macOS, and Linux endpoint management. It provides an overview of using FortiClient EMS and FortiClient EMS integrated with FortiGate.

FortiClient EMS

Following is a summary of how to use FortiClient EMS without FortiGate:

1. Configure user accounts. See [Configuring user accounts on page 20](#).
2. Add domains and/or discover local endpoints. See [Adding endpoints on page 21](#)
3. Create an endpoint profile. See [Creating a profile to configure 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 the EMS server. To allow initial deployment, EMS must be able to resolve the endpoint IP address via the DNS configured on the server.



You can use with workgroups only to upgrade FortiClient (Windows) on endpoints after they connect Telemetry. When using workgroups, you must separately install FortiClient (Windows) on endpoints.



You can use FortiClient EMS to replace, upgrade, and uninstall FortiClient (macOS) after they connect Telemetry to EMS and FortiClient connects to FortiClient EMS. You cannot use FortiClient EMS to initially deploy FortiClient (macOS) and must separately install it on endpoints. See the [FortiClient EMS Administration Guide](#).

-
4. Add a FortiClient deployment package to EMS and configure it with the profile that you created in step 3. See [Adding a FortiClient deployment package on page 22](#).
 5. Prepare Windows endpoints for FortiClient deployment. See [Preparing Windows endpoints for FortiClient deployment on page 25](#).
You must also prepare the Windows AD server for deployment. See the [FortiClient EMS Administration Guide](#).
 6. Create a deployment configuration with the desired deployment package. Configure the deployment configuration for the desired workgroup, domain, endpoint group, or organizational group. See [Creating a deployment configuration on page 25](#).
Depending on the selected profile's configuration, FortiClient is installed on the endpoints to which the profile is applied.
After FortiClient installation, the endpoint connects FortiClient Telemetry to FortiClient EMS to receive the profile configuration and complete endpoint management setup.
 7. View the endpoint status. See [Viewing endpoints on page 26](#).

FortiClient EMS integrated with FortiGate

Following is a summary of how to use FortiClient EMS when integrated with FortiGate. This deployment only applies for endpoints with a version of FortiClient earlier than 6.4.0 installed:

1. Configure user accounts. See [Configuring user accounts on page 20](#).
2. Add domains and/or discover local endpoints. See [Adding endpoints on page 21](#)
3. Create an endpoint profile. See [Creating a profile to configure 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 the EMS server. To allow initial deployment, EMS must be able to resolve the endpoint IP address via the DNS configured on the server.



You can use with workgroups only to upgrade FortiClient (Windows) on endpoints after they connect Telemetry to EMS. When using workgroups, you must separately install FortiClient (Windows) on endpoints.



You can use FortiClient EMS to replace, upgrade, and uninstall FortiClient (macOS) after they connect Telemetry to EMS and FortiClient connects to FortiClient EMS. You cannot use FortiClient EMS to initially deploy FortiClient (macOS) and must separately install it on endpoints. See the [FortiClient EMS Administration Guide](#).

-
4. Add a FortiClient deployment package to EMS and configure it with the profile that you created in step 3. See [Adding a FortiClient deployment package on page 22](#).
 5. Prepare Windows endpoints for FortiClient deployment. See [Preparing Windows endpoints for FortiClient deployment on page 25](#).
You must also prepare the Windows AD server for deployment. See the [FortiClient EMS Administration Guide](#).
 6. Create a deployment configuration with the desired deployment package. Configure the deployment configuration for the desired workgroup, domain, endpoint group, or organizational group. See [Creating a deployment configuration on page 25](#).
Depending on the selected profile's configuration, FortiClient is installed on the endpoints to which the profile is applied.
After FortiClient installation, the endpoint connects FortiClient Telemetry to FortiClient EMS to receive the profile configuration and complete endpoint management setup.
 7. View the endpoint status. See [Viewing endpoints on page 26](#).

Configuring user accounts

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

For EMS users, you create a new user account from EMS.

For local Windows users, the user list is derived from the server where FortiClient EMS is installed. If you want to add more users, you must add them to the server.

For LDAP users, you must add an LDAP server to FortiClient EMS, then configure users.

To add an LDAP server:

1. Go *Administration > User Servers*. Click *Add*.
2. Configure the options, and click *Test*.
3. If the test succeeds, click *Save*.

To configure users:

1. Go to *Administration > Administrators*.
2. Click *Add* from the toolbar.
3. In the *User* list, select *Choose from LDAP/Windows users* or *Create a new user*.
4. Configure the user's administrator role. See the [FortiClient EMS Administration Guide](#).
5. Select the user's specific domain access.
6. Click *Save*.

Adding endpoints

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.

The LDAP connection is read-only.



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



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



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

To add endpoints using an AD domain server:

1. Go to *Endpoints > Manage Domains > Add*. The *Domain* pane displays.
2. Configure the following options:

IP address/Hostname	Enter the domain server IP address or hostname.
Port	Enter the port number.

Distinguished name	Enter the distinguished name (DN) (optional). You must use only capital letters when configuring the DN. You cannot import domains and OUs that have a DN with more than 256 characters.
Bind type	Select the bind type: <i>Simple</i> , <i>Anonymous</i> , or <i>Regular</i> . When you select <i>Regular</i> , you must enter the <i>Username</i> and <i>Password</i> .
Username	Available when <i>Bind type</i> is set to <i>Regular</i> . Enter the username.
Password	Available when <i>Bind type</i> is set to <i>Regular</i> . Enter the user password.
Show Password	Available when <i>Bind type</i> is set to <i>Regular</i> . Turn on and off to show or hide the password.
LDAPS connection	Enable a secure connection protocol when <i>Bind Type</i> is set to <i>Regular</i> .
Sync every	Enter the sync schedule between FortiClient EMS and the domain in minutes. The default is ten minutes.

3. Click *Test* to test the domain settings connection.
4. If the test succeeds, click *Save* to save the new domain. If not, correct the information as required, then test the settings again.



After importing endpoints from an AD server, you can move them to custom created groups. These groups are not seen in AD and EMS does not have the ability to modify the AD server in any way. See [Managing groups](#).

Adding a FortiClient deployment package



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

To add a deployment package:

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

Installer Type	Use an official or custom FortiClient installer. When using a custom FortiClient installer, you can select from a list of previously uploaded installers, or upload a new custom installer. You can also remove previously created installers.
-----------------------	---

To upload a new custom FortiClient installer, enter the desired name, then upload Windows (64-bit and 32-bit) and/or macOS custom installers. You can download FortiClient installers to use with FortiClient EMS from [Fortinet Customer Service & Support](#). This requires a support account with a valid support contract. You can also download installers from [FortiClient.com](#). Download the Windows or macOS installation file. The installation files on the Fortinet Customer Service & Support and FortiClient.com websites are not available in .msi or .zip format. You must package the installer as an .msi or .zip file to upload it.

Release	Select the FortiClient release version to install.
Patch	Select the specific FortiClient patch version to install.
Keep updated to the latest patch	Enable EMS to repackage EMS created FortiClient deployment package to the latest patch release.

4. Click *Next*. On the *General* tab, set the following options:

Name	Enter the FortiClient deployment package name.
Notes	(Optional) Enter notes about the FortiClient deployment package.

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



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

Zero Trust Telemetry	Enabled by default and cannot be disabled. Installs FortiClient with Telemetry enabled.
Secure Access Architecture Components	<p>Install FortiClient with SSL and IPsec VPN enabled. Disable to omit SSL and IPsec VPN support from the FortiClient deployment package.</p> <p>If you enable this feature for a deployment package and include a preconfigured VPN tunnel in the included endpoint profile, users who use this deployment package to install FortiClient can connect to this preconfigured VPN tunnel for three days after their initial FortiClient installation. This is useful for remote users, as it allows them to connect to the corporate network to activate their FortiClient license. If the user does not activate their FortiClient license within the three days, all FortiClient features, including VPN, stop working on their device.</p> <p>See VPN for details on configuring a VPN tunnel.</p>
Vulnerability Scan	Enabled by default and cannot be disabled. Installs FortiClient with Vulnerability Scan enabled.
Advanced Persistent Threat (APT) Components	Install FortiClient with APT components enabled. Disable to omit APT components from the FortiClient deployment package. Includes FortiSandbox detection and quarantine features.

Additional Security Features

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 features from the FortiClient deployment package.

If you enable a feature in the deployment package that is disabled in [Feature Select](#), the feature is installed on the endpoint, but is disabled and does not appear in the FortiClient GUI. For example, when Web Filter is disabled in Feature Select, if you enable Web Filtering in a deployment package, the deployment package installs Web Filter on the endpoint. However, the Web Filter feature is disabled on the endpoint and does not appear in the FortiClient GUI.

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

Enable desktop shortcut

Configure the FortiClient deployment package to create a desktop shortcut on the endpoint.

Enable start menu shortcut

Configure the FortiClient deployment package to create a Start menu shortcut on the endpoint.

Enable Installer ID

Configure an installer ID. Select an existing installer ID or enter a new installer ID. If creating an installer ID, select a group path or create a new group in the *Group Path* field. FortiClient EMS automatically groups endpoints according to installer ID group assignment rules.






If you manually move the endpoint to another group after EMS places it into the group defined by the installer ID group assignment rule, EMS returns the endpoint to the group defined by the installer ID group assignment rule.

In an environment with a large number of endpoints, since you can configure each deployment package with only one installer ID, it may be inefficient to create a deployment package for each installer ID. See [Deploying different installer IDs to endpoints using the same deployment package](#).

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

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



If the *Sign software packages* option is enabled in *System Settings > EMS Settings*, Windows deployment packages display as being from the publisher specified in the certificate file. See the *FortiClient EMS Administration Guide*.

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 *Deployment & Installers > FortiClient Installer*.



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

Creating a deployment configuration

To create a deployment configuration:

1. Go to *Deployment > Manage Deployment*.
2. Click *Add*.

3. Configure the fields as desired:

Field	Description
Name	Required. Enter the desired name.
Endpoint Groups	Optional. Select the desired endpoint group. The list includes device groups for all imported domains and workgroups.
Action	Select <i>Install</i> or <i>Uninstall</i> .
Deployment Package	Select the desired deployment package from the dropdown list.
Start at a Scheduled Time	Specify what time to start installing FortiClient on endpoints.
Unattended Installation	When enabled, the end user cannot modify the installation schedule. If needed, the device reboots without warning logged-in users.
Reboot When Needed	Reboot the endpoint to install FortiClient when needed.
Reboot When No Users Are Logged In	Allow the endpoint to reboot without prompt if no endpoint user is logged into FortiClient.
Notify Users and Let Them Decide When To Reboot When Users Are Logged In	Notify the end user if a reboot of the endpoint is needed and allow the user to decide what time to reboot the endpoint. Disable to reboot the endpoint without notifying the user.
Username	Enter the username to perform deployment on AD. You must enter the admin credentials for the AD. The credentials allow FortiClient EMS to install FortiClient on endpoints using AD. If the credentials are wrong, the installation fails, and an error displays in FortiClient EMS.
Password	Enter the password to perform deployment on AD.
Enable the Deployment	Enable or disable.

4. Click Save.

Viewing endpoints

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

Viewing the Endpoints pane

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

To view the *Endpoints* pane:

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

Not Installed	Number of endpoints that do not have FortiClient installed. Click to display the list of endpoints without FortiClient installed.
Not Registered	Number of endpoints that are not connected to FortiClient EMS. Click to display the list of disconnected endpoints.
Out-Of-Sync	Number of endpoints with an out-of-sync profile. Click to display the list of endpoints with out-of-sync profiles.
Security Risk	Number of endpoints that are security risks. Click to display the list of endpoints that are security risks.
Quarantined	Number of endpoints that EMS has quarantined. Click to display the list of quarantined endpoints.
Endpoints	Click the checkbox to select all endpoints displayed in the content pane.
Show/Hide Heading	Click to hide or display the following column headings: <i>Device</i> , <i>User</i> , <i>IP</i> , <i>Configurations</i> , <i>Connections</i> , and <i>Alerts and Events</i> .
Show/Hide Full Group Path	Click to hide or display the full path for the group that the endpoint belongs to.
Refresh	Click to refresh the list of endpoints.
Search All Fields	Enter a value and press <i>Enter</i> to search for the value in the list of endpoints.
Filters	Click to display and hide filters you can use to filter the list of endpoints.
Device	Visible when headings are displayed. Displays an icon to represent the OS on the endpoint, the hostname, and the endpoint group.
User	Visible when headings are displayed. Displays the name and icon of the user logged into the endpoint. Also displays the status of the endpoint: <ul style="list-style-type: none"> • Online: Endpoint has been seen within less than three keep alive timeouts. • Away: Endpoint has been offline for less than eight hours. • Offline: Endpoint has been offline for more than eight hours. • Never Seen: Endpoint has never been registered to EMS.
IP	Visible when headings are displayed. Displays the endpoint's IP address.
Configurations	Visible when headings are displayed. Displays the name of the policy assigned to the endpoint and its synchronization status.
Connections	Visible when headings are displayed. Displays the connection status between FortiClient and FortiClient EMS. If the endpoint is connected to a FortiGate, displays the FortiGate hostname.
Alerts and Events	Visible when headings are displayed. Displays FortiClient alerts and events for the endpoint.

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

Scan	Click to start a Vulnerability or AV scan on the selected endpoint.
------	---

Patch	Click to patch all critical and high vulnerabilities on the selected endpoint. Choose one of the following options: <ul style="list-style-type: none"> Selected Vulnerabilities on Selected Clients Selected Vulnerabilities on All Affected Clients All Critical and High Vulnerabilities
Move to	Move the endpoint to a different group.
Action	Click to perform one of the following actions on the selected endpoint: <ul style="list-style-type: none"> Request FortiClient Logs Request Diagnostic Results Update Signatures Download Available FortiClient Logs Download Available Diagnostic Results Deregister Quarantine Un-quarantine Exclude from Management Clear Events Mark as Uninstalled Set Importance Set Custom Tags. This option is only available if you have already created a custom tag. Delete Device

The following tabs are available in the content pane toolbar when you select an endpoint, depending on which FortiClient features are installed on the endpoint and enabled via the assigned profile:

Summary	
<user name>	Displays the name of the user logged into the selected endpoint. Also displays the user's avatar, email address, and phone number if these are provided to FortiClient on the endpoint. If the user's LinkedIn, Google, Salesforce, or other cloud app account is linked in FortiClient, the username from the cloud application displays. Also displays the group that the endpoint belongs to in EMS.
Device	Displays the selected endpoint's hostname. You can enter an alias if desired.
OS	Displays the selected endpoint's operating system and version number.
IP	Displays the selected endpoint's IP address.
MAC	Displays the selected endpoint's MAC address.
Last Seen	Displays the last date and time that FortiClient sent a keep-alive message to EMS. This information is useful if FortiClient is offline because it indicates when the last keep-alive message occurred.

Location	Displays whether the selected endpoint is on- or off-fabric. You can also view any on-fabric detection rules that the endpoint is applicable for. See On-fabric Detection Rules .
Network Status	<p>This section only appears for endpoints running FortiClient 6.4.1 and later versions.</p> <p>Displays the following information for the networks that the endpoint is connected to:</p> <ul style="list-style-type: none">• MAC address• IP address• Gateway IP address• Gateway MAC address• SSID for Wi-Fi connections
Hardware Details	Displays the hardware model, vendor, CPU, RAM, and serial number information for the endpoint device, if available.
Zero Trust Tags	Displays which tags have been applied to the endpoint based on the Zero Trust tagging rules. See Zero Trust Tags .
Connection	Displays the connection status between the selected endpoint and FortiClient EMS.
Configuration	<p>Displays the following information for the selected endpoint:</p> <ul style="list-style-type: none">• Policy: Endpoint policy assigned to the selected endpoint• Profile: Profile assigned to the selected endpoint• Off-fabric Profile: Off-fabric profile assigned to the selected endpoint• Installer: FortiClient installer used for the selected endpoint.• FortiClient Version: FortiClient version installed on the selected endpoint.• FortiClient Serial Number: Serial number for the selected endpoint's FortiClient license.
Classification Tags	<p>Displays classification tags that are currently assigned to the endpoint. You can also assign a classification tag to the endpoint. Classification tags include the default importance level tags (low, medium, high, or critical), and custom tags. An endpoint can only have one default importance tag assigned, but can have multiple custom tags assigned. You can also unassign a tag from the endpoint, and create, assign, or delete a custom tag. To create a new custom tag, click the <i>Add</i> button, enter the desired tag, the click the + button. When you create a tag, it is available for assignment to all endpoints in the current site.</p> <p>You can assign a classification tag to multiple endpoints by selecting the endpoints, then selecting <i>Action > Set Importance</i> or <i>Set Custom Tags</i>. See Sending endpoint classification tag to FortiAnalyzer.</p>
Status	<p>Displays one of the following statuses:</p> <ul style="list-style-type: none">• Managed: Endpoint is managed by EMS.• Quarantined: If quarantined, displays access code. The user can enter this access code in the affected endpoint's FortiClient to remove the

	<p>endpoint from quarantine.</p> <ul style="list-style-type: none"> Excluded: Endpoint is excluded from management by EMS.
Features	Displays which features are enabled for FortiClient.
Third Party Features	Displays which software is in use on the endpoint for virus and threat protection and disk encryption. This may list FortiClient or third party AV software that registers with Microsoft Security Center.
Antivirus Events	
Date	Displays the AV event's date and time.
Count	Displays the number of occurrences for this event.
Message	Displays the AV event's message.
Actions	Mark the event as read or delete it.
Cloud Scan Events	
Date	Displays the cloud-based malware detection event's date and time.
Count	Displays the number of occurrences for this event.
Message	Displays the cloud-based malware detection event's message.
Actions	Mark the event as read or delete it.
AntiExploit Events	
Date	Displays the AntiExploit event's date and time.
Count	Displays the number of occurrences for this event.
Message	Displays the AntiExploit event's message.
Actions	Mark the event as read or delete it.
USB Device Events	
Date	Displays the USB device event's date and time.
Count	Displays the number of occurrences for this event.
Message	Displays the USB device event's message.
Actions	Mark the event as read or delete it.
Sandbox Events	
Date	Displays the sandbox event's date and time.
Message	Displays the sandbox event's message.
Rating	Displays the file's risk rating as retrieved from FortiSandbox.
Checksum	Displays the checksum for the file.
Download	Download a PDF version of the detailed report.

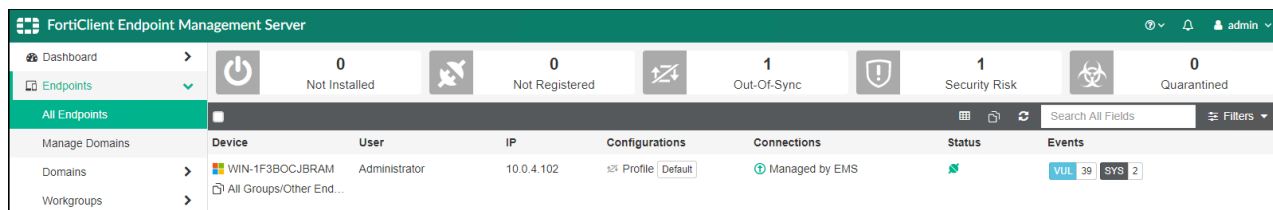
Magnifying glass	Click to view a more detailed report. See Viewing Sandbox event details .
Firewall Events	
Date	Displays the firewall event's date and time.
Count	Displays the number of occurrences for this event.
Message	Displays the firewall event's message.
Actions	Mark the event as read or delete it.
Web Filter Events	
Date	Displays the web filter event's date and time.
Count	Displays the number of occurrences for this event.
Message	Displays the web filter event's message.
Actions	Mark the event as read or delete it.
Vulnerability Events	
Vulnerability	Displays the vulnerability's name. For example, <i>Security update available for Adobe Reader</i> .
Category	Displays the vulnerability's category. For example, <i>Third Party App</i> .
Application	Displays the name of the application with the vulnerability.
Severity	Displays the vulnerability's severity.
Patch Type	Displays the patch type for this vulnerability: <i>Auto</i> or <i>Manual</i> .
FortiGuard	Displays the FortiGuard ID number. If you click the FortiGuard ID number, it redirects you to FortiGuard where further information is provided if available.
System Events	
Date	Displays the system event's date and time.
Count	Displays the number of occurrences for this event.
Message	Displays the system event's message.
Actions	Mark the event as read.

Using the quick status bar

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

To use the quick status bar:

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



3. Click one of the following buttons in the quick status bar:

- Not Installed
- Not Registered
- Out-Of-Sync
- Security Risk
- Quarantined

The list of affected endpoints displays.

4. Click an endpoint to display its details.

5. In the *Events* column, click the *AV <number>*, *SB <number>*, *FW <number>*, *VUL<number>*, *WEB <number>* and *SYS<number>* buttons to display the associated tab of details for the selected endpoint.

6. Click the *Total* button to clear the filters. The unfiltered list of endpoints displays.

Viewing endpoint details

You can view each endpoint's details on the *Endpoints* content pane. For a description of the options on the *Endpoints* content pane, see [Viewing the Endpoints pane on page 26](#).

To view endpoint details:

1. Go to *Endpoints*, and select *All Domains*, a domain, or workgroup. The list of endpoints for the selected domain or workgroup displays.
2. Click an endpoint to display details about it in the content pane. Details about the endpoint display in the content pane.

FortiClient EMS for Chromebooks setup

This section describes how to set up FortiClient EMS for Chromebooks. Following is a summary of how to set up FortiClient EMS for Chromebooks:

1. Add an SSL certificate. See [Adding SSL certificates on page 44](#).
2. Add the Google domain. See [Adding a Google domain on page 46](#).
3. Create an endpoint profile. See [Adding a new Chromebook profile on page 46](#).
4. Create an endpoint policy configured with the endpoint profile. See [Adding a Chromebook policy on page 48](#).
5. View the status. See [Viewing domains on page 48](#).

Additional configuration procedures are also included in this section.

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:

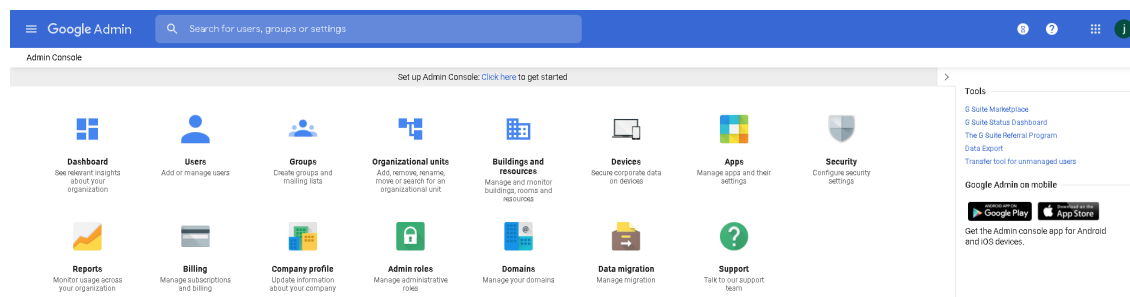
1. Log into the Google Admin console. See [Logging into the Google Admin console on page 33](#).
2. Add the FortiClient Web Filter extension. See [Adding the FortiClient Web Filter extension on page 34](#).
3. Configure the FortiClient Web Filter extension. See [Configuring the FortiClient Web Filter extension on page 34](#).
4. Add the root certificate. See [Adding root certificates on page 35](#).



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

Logging into the Google Admin console

Log into the [Google Admin console](#) using your Google domain admin account. The Admin console displays.



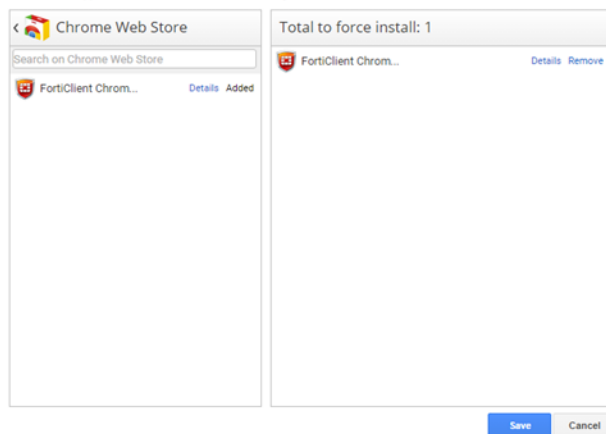
Adding the FortiClient Web Filter extension



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

1. In the Google Admin console, go to *Devices > Chrome Management > Settings > User & browser settings > Managed Guest Session Settings*.
2. On the left, select the organization that contains the desired users or enrolled browsers. To select all users and browsers, select the top-level organization. Otherwise, select a child.
3. Under *Apps and Extensions*, beside *Force-installed Apps and Extensions*, click *Manage force-installed apps*.
4. Select *Chrome Web Store*, and search for the following extension ID: igbgpehnbmhdgdgjbhkkpedommgmfbeao.
5. Click *Add*. The extension displays under *Total to force install: 1*. Click *SAVE*.

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 that the FortiClient Web Filter extensions send.



FortiClient EMS is the profile server.

To configure the FortiClient Web Filter extension:

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

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

}

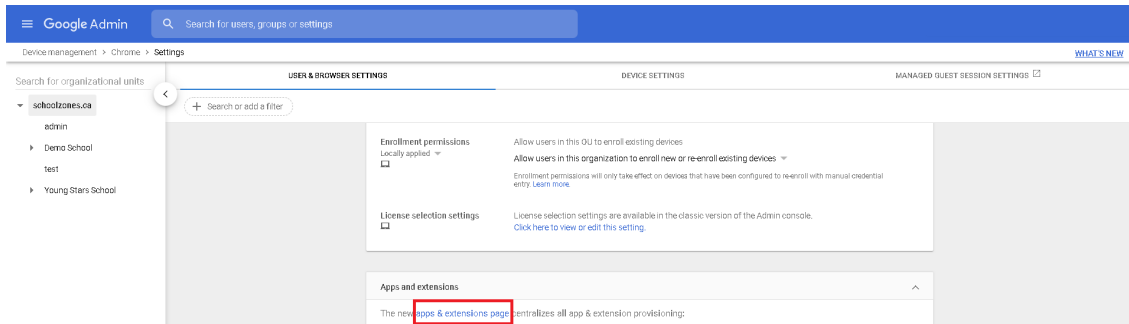
For example:

{

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

}

3. In the Google Admin console, go to *Devices > Chrome management > User & browser settings*.
4. On the left, select the organization that contains the desired users or enrolled browsers. To select all users and browsers, select the top-level organization. Otherwise, select a child.
5. Under *Apps and Extensions*, click the *apps & extensions* page link.



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

Adding root certificates

Communication with the FortiClient Chromebook Web Filter extension

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

If you use a public SSL certificate, you only need to add the public SSL certificate to FortiClient EMS. See [Adding an SSL certificate to FortiClient EMS for Chromebook endpoints on page 45](#).

However, if you prefer to use a certificate not from a common CA, you must add the SSL certificate to FortiClient EMS and push your certificate's root CA to the Google Chromebooks. Otherwise, the HTTPS connection between the FortiClient Chromebook Web Filter extension and FortiClient EMS does not work. See [Uploading root certificates to the Google Admin console on page 37](#).

Communication with FortiAnalyzer for logging

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



Sending logs to FortiAnalyzer requires you enable ADOMs in FortiAnalyzer and add FortiClient EMS to FortiAnalyzer. FortiClient EMS is added as a device to the FortiClient ADOM in FortiAnalyzer. See the [FortiAnalyzer Administration Guide](#).

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

If you use a public SSL certificate, you only need to add the public SSL certificate to FortiAnalyzer. See [Adding an SSL certificate to FortiAnalyzer](#).

However, if you prefer to use a certificate not from a common CA, you must add the SSL certificate to FortiAnalyzer and push your certificate's root CA to the Google Chromebooks. Otherwise, the HTTPS connection between the FortiClient Chromebook Web Filter extension and FortiAnalyzer does not work. See [Uploading root certificates to the Google Admin console on page 37](#).



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

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

In FortiAnalyzer CLI, enter the following command:

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

Adding an SSL certificate to FortiAnalyzer

To add an SSL certificate to FortiAnalyzer:

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

Selecting a certificate for HTTPS connections

To select a certificate for HTTPS connections:

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

Summary of where to add certificates

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

Scenario	Certificate and CA	Where to add certificates
Allow the FortiClient Chromebook Web Filter extension to trust EMS	Public SSL certificate	<ul style="list-style-type: none"> Add SSL certificate to FortiClient EMS.
	SSL certificate not from a common CA	<ul style="list-style-type: none"> Add SSL certificate to FortiClient EMS. Add your certificate's root CA to the Google Admin console.
Allow the FortiClient Chromebook Web Filter extension to trust FortiAnalyzer for logging	Public SSL certificate	<ul style="list-style-type: none"> Add SSL certificate to FortiAnalyzer.
	SSL certificate not from a common CA	<ul style="list-style-type: none"> Add SSL certificate to FortiAnalyzer. Add your certificate's root CA to the Google Admin console.

Uploading root certificates to the Google Admin console

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



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

Disabling access to Chrome developer tools

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

To disable access to Chrome developer tools:

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

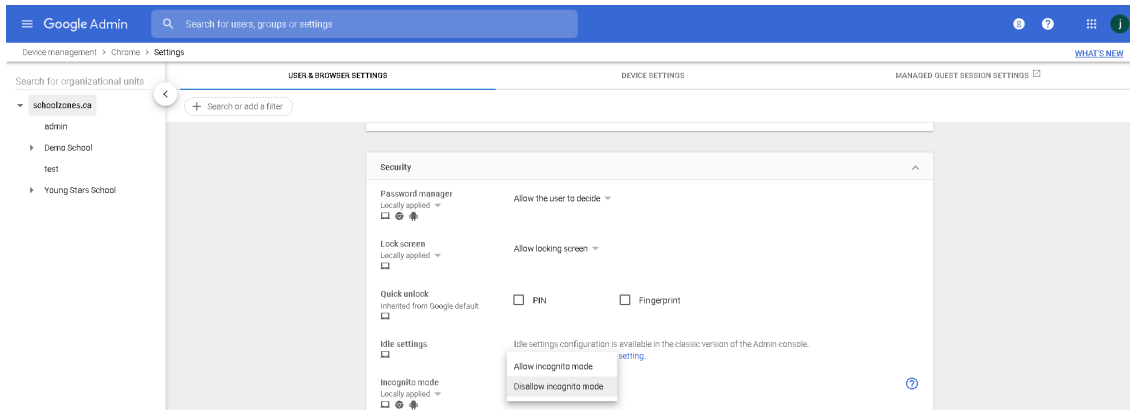
Disallowing incognito mode

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

To disallow incognito mode:

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

- Under *Security*, set *Incognito mode* to *Disallow incognito mode*.



- Click **Save**.

Disabling guest mode

You should disallow guest mode for managed Google domains.

To disallow guest mode:

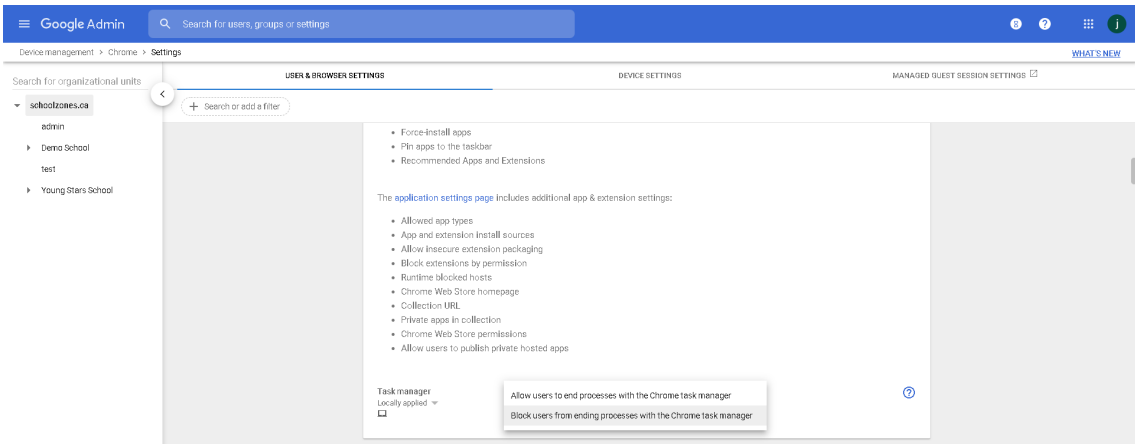
- In the Google Admin console, go to *Devices > Chrome management > Device settings*.
- On the left, select the organization that contains the desired users or enrolled browsers. To select all users and browsers, select the top-level organization. Otherwise, select a child.
- Under *Sign-in settings*,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

Blocking the Chrome task manager

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

To block the Chrome task manager:

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



4. Click Save.

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 43](#).

Configuring unique service account credentials

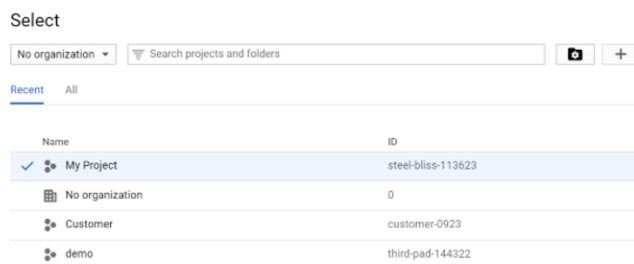
When using unique service account credentials for improved security, you must complete the following steps to add the unique service account credentials to the Google Admin console and FortiClient EMS:

1. Create unique service account credentials using the Google Developer console. See [Creating unique service account credentials on page 40](#).
2. Add the unique service account credentials to the Google Admin console. See [Adding service account credentials to the Google Admin console on page 43](#).
3. Add the unique service account credentials to FortiClient EMS. See [Adding service account credentials to EMS on page 44](#).

Creating unique service account credentials

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

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

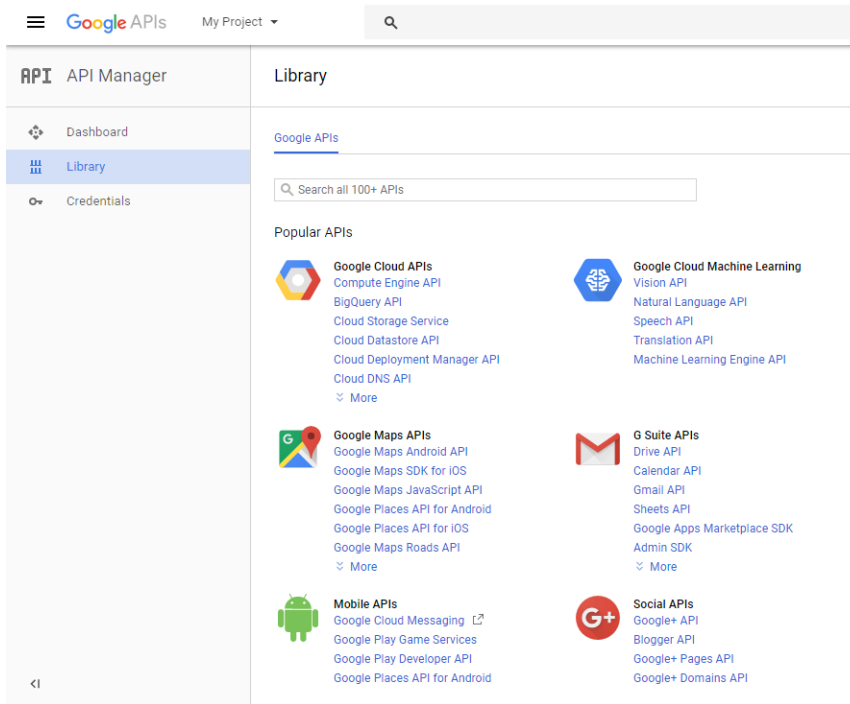
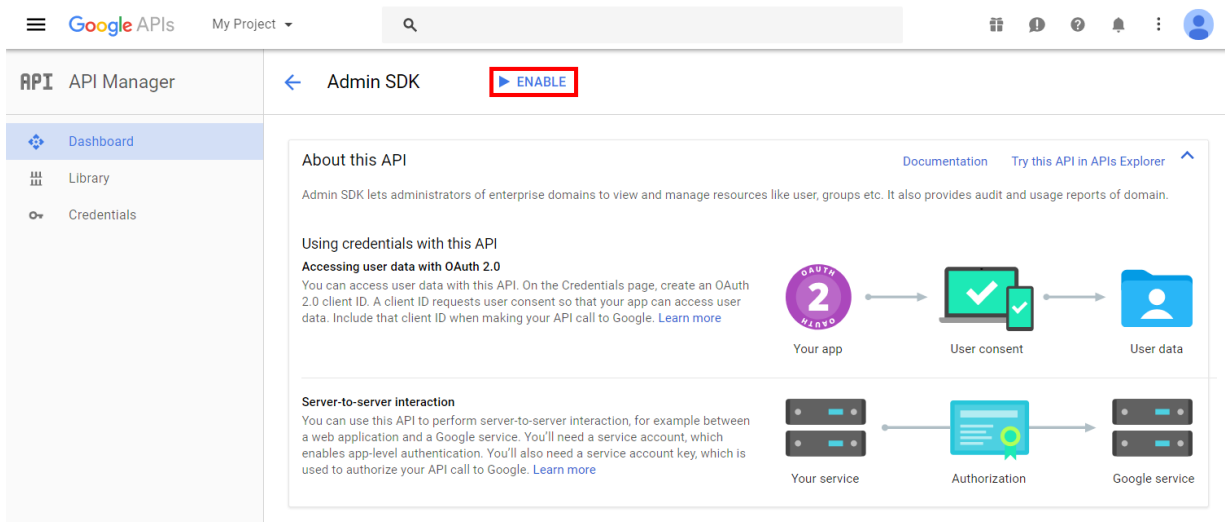


CANCEL OPEN

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

4. Enable the Admin SDK:

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

c. Click *ENABLE*.

5. Create a service account:

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

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

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



The private key with the *P12* extension is the only copy you receive. Keep it in a safe place. You should also remember the password prompted on the screen. At this time, that password should be **notasecret**.

Service account and key created

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

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

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

notasecret

[CLOSE](#)

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

Edit service account

Service account name ?

test

☒ Enable G Suite Domain-wide Delegation

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

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

Product name for the consent screen

Product name

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

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

The screenshot shows the Google APIs console interface. On the left is a sidebar with 'API Manager' and 'Credentials' selected. The main area is titled 'Client ID for Service account client' and includes buttons for 'DOWNLOAD JSON' and 'DELETE'. A message states: 'Service account clients are created when domain-wide delegation is enabled on a service account.' Below this, a table shows the following details:

Client ID	115703365324425320868
Service account	test-410@voltaic-facet-170220.iam.gserviceaccount.com
Creation date	Jun 12, 2017, 1:58:28 PM

Below the table, there is a 'Name' field with the value 'Client for test-410' and 'Save' and 'Cancel' buttons.



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 > EMS Settings*.
2. Enable *EMS for Chromebooks Settings*.



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

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

Service Account Email	Enter a new email address for the service account credentials.
Private key	Click <i>Browse</i> and select the certificate provided with the service account credentials.

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



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

Adding SSL certificates

This section includes information about the required SSL certificates to support the following types of communication:

- [Communication with the FortiClient Chromebook Web Filter extension on page 35](#)
- [Communication with FortiAnalyzer for logging on page 35](#)

It includes the following procedures:

- Required: [Adding an SSL certificate to FortiClient EMS for Chromebook endpoints on page 45](#)
- Required only when sending logs to FortiAnalyzer: [Adding SSL certificates to FortiAnalyzer on page 45](#)

Adding an SSL certificate to FortiClient EMS for Chromebook endpoints

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

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

If you are not using a public SSL certificate, you must add the SSL certificate to FortiClient EMS, and the root certificate to the Google Admin console. See [Adding root certificates on page 35](#).

To add an SSL certificate to EMS for Chromebook endpoints:

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



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

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

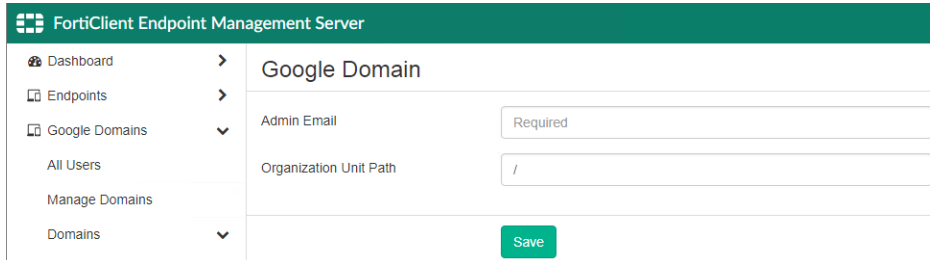
Adding SSL certificates to FortiAnalyzer

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*.

Adding a Google domain

To add a Google domain:

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



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



/ stands for the root of the domain.

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

Configuring Chromebook profiles

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 as part of an endpoint policy.

Adding a new Chromebook profile

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



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

To add a new profile:

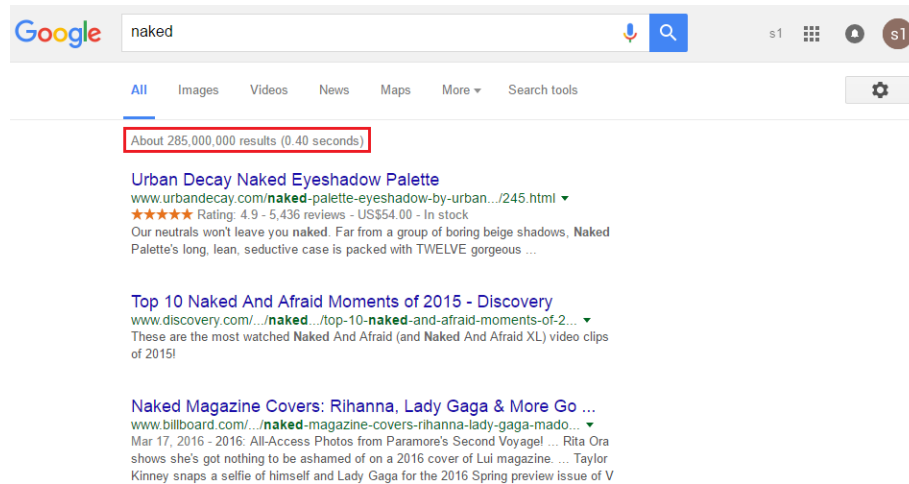
1. Go to *Endpoint Profiles > Manage Profiles*, and click the *Add Chrome* button.
2. In the *Profile Name* field, enter the profile name.
3. On the *Web Filter* tab, enable *Web Filter*, and set the web filtering options.
4. On the *System Settings* tab, set the logging options.
5. Click *Save*.

Enabling and disabling Safe Search

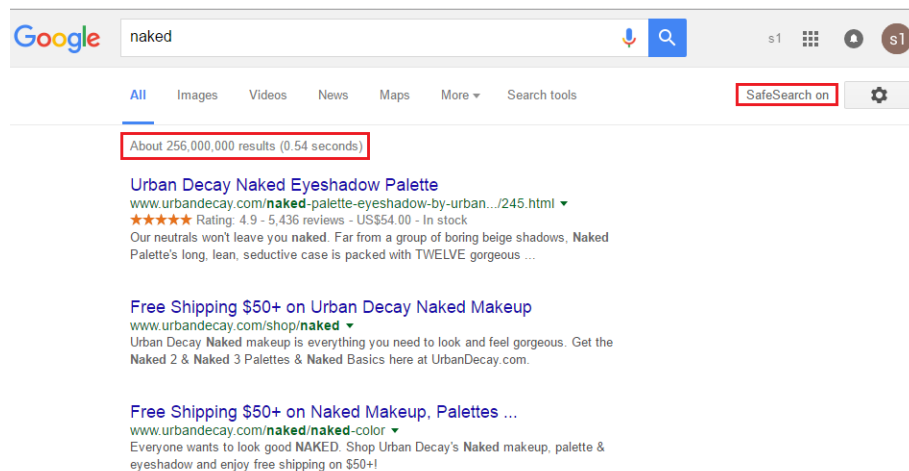
The search engine provides a Safe Search feature that blocks inappropriate or explicit images from search results. The Safe Search feature helps avoid most adult content. FortiClient EMS supports Safe Search for most common search engines, such as Google, Yahoo, and Bing.

The profile in FortiClient EMS controls the Safe Search feature.

Following are examples of search results with the Safe Search feature disabled and enabled. Notice the difference between the number of results. Here are the search results when the Safe Search feature is disabled, which has about 285000000 results:



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



To enable or disable Safe Search:

1. In FortiClient EMS, in the *Endpoint Profiles > Manage Profiles* area, click the *Default - Chromebooks* profile or another profile.
2. On the *Web Filter* tab, enable or disable *Enable Safe Search*.

Adding a Chromebook policy

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

Chromebook policy name	Enter the desired name for the Chromebook policy.
Google domains	Select the Google domain to apply the policy to. Domains for which an endpoint policy has already been created are grayed out and you cannot select them.
Chromebook profile	Include a Chromebook profile in the policy. From the dropdown list, select the desired profile. You must have already created a profile to include one in an endpoint policy. See Adding a new Chromebook profile on page 46 .
Comments	Enter any comments desired for the endpoint policy.
Enable the policy	Toggle to enable or disable the endpoint policy. You can enable or disable the policy at a later time from <i>Endpoint Policy & Components Manage Policies</i> .

4. Click *Save*. You can view the newly created policy on the *Chromebook Policy > Manage Chromebook Policies* page.
EMS pushes these settings to the endpoint with the next Telemetry communication.

Viewing domains

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

Viewing the Google Users pane

To view the Google Users pane:

You can view Google user information in FortiClient EMS.

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

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

The following options are available in the toolbar:

Clear Filters	Clear the currently used filter(s).
Refresh	Refresh the page.

The following columns of information display for Google users:

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

Viewing user details

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

To view user details:

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

User Details

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

Client Statistics

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

Blocked Sites (Past <number> Days)

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

Change log

Date	Change Description
2021-11-25	Initial release.



FORTINET®



Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.