FortiClient EMS - QuickStart Guide

Version 6.0.1

FORTINET DOCUMENT LIBRARY

https://docs.fortinet.com

FORTINET VIDEO GUIDE

https://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTINET COOKBOOK

https://cookbook.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: techdocs@fortinet.com

TABLE OF CONTENTS

Change Log

Date	Change Description
2018-07-23	Initial release.

Introduction

This guide describes how to install and set up FortiClient Enterprise Management Server (EMS) for the first time. FortiClient EMS is used 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 the following platforms:

- Microsoft Windows Server 2008 R2 or newer

For information about minimum system requirements and supported platforms, see the *FortiClient EMS Release Notes*, available in the Fortinet Document Library.

Requirements

The following components and knowledge are required to use FortiClient EMS for managing Chromebooks:

- FortiClient EMS installer
- FortiClient Web Filter extension available in the Google Web Store for Chrome OS
- G Suite account
- Knowledge of administering the Google Admin console
- A 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 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
FortiClient upload	Used for FortiClient to upload events, logs, and diagnostics to FortiClient EMS.	TCP	8014 (default)	Incoming	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 EMS server connects to endpoints using RPC for FortiClient initial deployment.	TCP	135	Outgoing	N/A
Active Directory server connection	Retrieving workstation and user information	TCP	389 (LDAP) or 636 (LDAPS)	Outgoing	GUI
FortiClient download	Downloading FortiClient installer created by the EMS server	TCP	10443 (default)	Incoming	Installer
Apache/HTTPS	Web access to EMS	TCP	443	Incoming	Installer
FortiGuard	FortiGuard antivirus, vulnerability, and application version updates	TCP	80	Outgoing	N/A
SMTP server/email	Alerts for EMS and endpoint events. When an alert is triggered, an email notification is sent	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

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

Communication	Usage	Protocol	Port	Incoming/Outgoing	How to customize
FortiClient on Chrome OS	Connection to EMS	TCP	8443 (default) You can customize this port.	Incoming	GUI
G suite API/Google domain directory	API calls to retrieve Google domain information	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	Connection to profile server	TCP	8443 (default)	Outgoing	Via Google Admin console when adding the profile
FortiGuard	URL rating	TCP	443, 3400	Outgoing	N/A
FortiAnalyzer	Send logs to FortiAnalyzer	TCP	8443	Outgoing	N/A

For the list of required services and ports for FortiClient, see the *FortiClient Administration Guide* on the Fortinet Document Library.

Deployment options

The following deployment options for EMS are supported: standalone or integrated with FortiGate.

Standalone
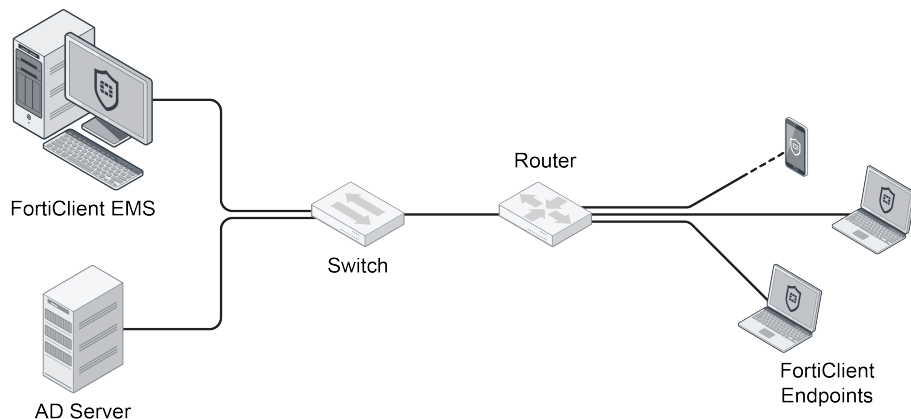
In standalone mode, a FortiGate device is not required, and network access control (NAC) is not supported. In standalone mode, EMS deploys FortiClient software on endpoints, and FortiClient endpoints connect FortiClient Telemetry to EMS to receive configuration information from EMS. EMS is used to deploy, configure, and monitor FortiClient endpoints.

Integrated with FortiGate
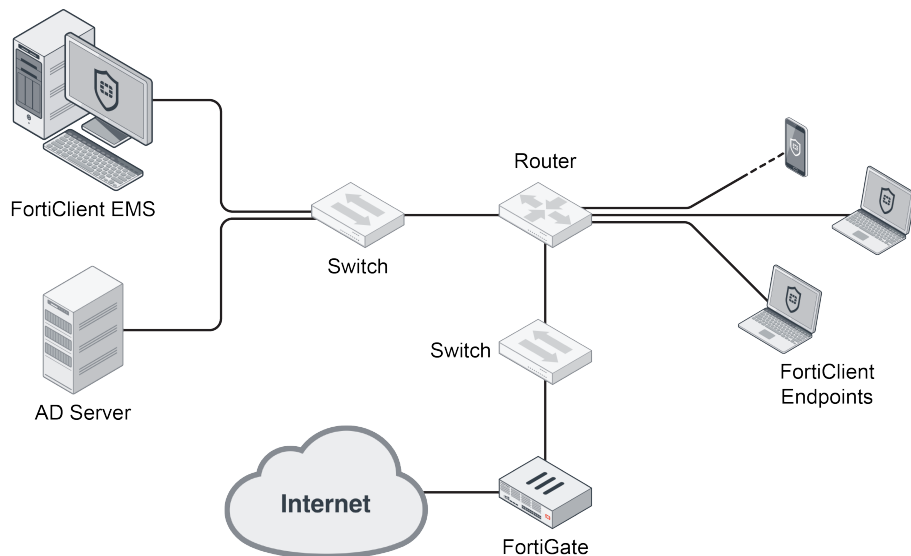
In integrated mode, a FortiGate device is required, and NAC is supported. In integrated mode, EMS deploys FortiClient software on endpoints, and FortiClient endpoints connect FortiClient Telemetry to FortiGate to receive compliance rules. FortiClient endpoints also connect to EMS to be managed. After FortiClient endpoints are connected, compliance rules are downloaded from FortiGate to the endpoint. EMS might also push a profile of FortiClient configuration information to endpoints. FortiClient endpoints are now managed, and NAC is enforced.

FortiClient uses the compliance rules from FortiGate to communicate whether the endpoint is compliant. If an endpoint fails to meet the compliance rules, the steps required to remain compliant are communicated. For more information, see the *FortiClient Administration Guide*.

Chromebook setup

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

- G Suite account on page 10
- SSL certificates on page 10
- How FortiClient EMS and FortiClient work with Chromebooks on page 10

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: https://gsuite.google.com/signup/basic/welcome#0

In the sign up 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 a fully qualified domain name (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 on page 46. 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.
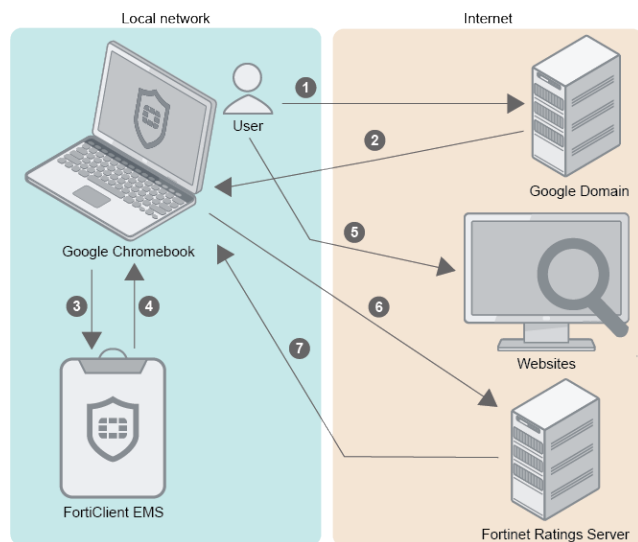
Installation

For a complete endpoint solution, FortiClient should be installed on all endpoints, and FortiClient EMS should be installed 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 12.
2. Install FortiClient EMS. See Installing FortiClient EMS on page 12.
3. Start FortiClient EMS and log in. See Starting FortiClient EMS and logging in on page 14.

For information about upgrading FortiClient EMS, see the FortiClient EMS *Release Notes*.

An instructional 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 following location:

Fortinet Support website: https://support.fortinet.com/

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

The following installation file is available for FortiClient EMS:

`FortiClientEnterpriseManagement_6.0.1.<build>_x64.exe`

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

Installing FortiClient EMS

The FortiClient EMS installation package includes:

- FortiClient EMS
- Microsoft SQL Server 2014 Express Edition
- Apache HTTP server

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

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.

4. (Optional) Click *Options* to specify a custom directory for the FortiClient EMS installation.
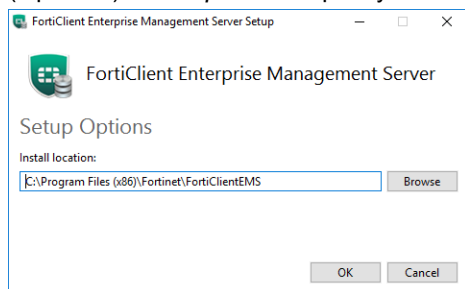
   a. Click *Browse* to locate and select the custom directory.
   b. Click *OK* to return to the installation wizard.
5. Click *Install*.
   The installation may take 30 minutes or longer. It may appear to stop at times, but this is only because certain steps in the installation process take longer than others.
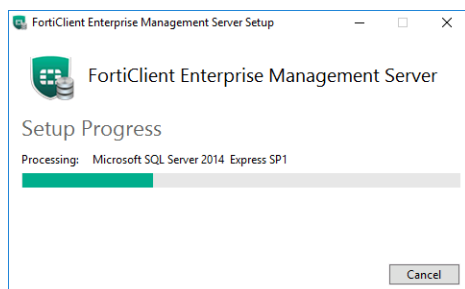
6. When the program has installed correctly, the *Success* window displays. Click *Close*.
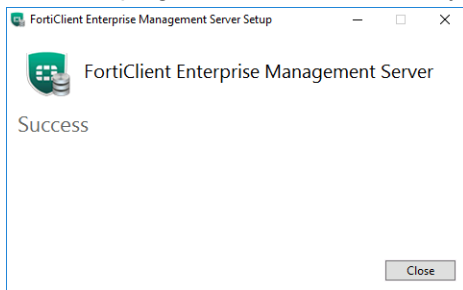
A *FortiClient Enterprise Management Server* icon is added to the desktop.

Extending license expiries

You can apply multiple licenses to your FortiClient EMS to extend the license expiry. For example, consider you purchase two one-year licenses for FortiClient EMS. After you register and apply the first license, FortiClient EMS has an expiry date of August 1, 2018. You can register and apply the second license as a renewal, after which FortiClient EMS has an expiry date of August 1, 2019.

Note you must upload the second license file to FortiClient EMS using the GUI. Registering the license does not automatically update the license expiry in FortiClient EMS.

> 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.

For details, see the *FortiClient EMS Administration Guide*.

Starting FortiClient EMS and logging in

FortiClient EMS runs as a service on Windows computers.

To start FortiClient EMS:

1. Double-click the *FortiClient Enterprise Management Server* icon.
2. Sign in with the username *admin* and no password.
3. Change the username and password by going to *Administration > Administrators*.
4. Configure FortiClient EMS by going to *System Settings*.

Accessing FortiClient EMS remotely

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

To enable remote access to FortiClient EMS:

1. Go to *System Settings > Server*.
2. Enable *Remote HTTPS access*.
3. If desired, in the *Custom hostname* box, type the host name 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 is automatically redirected 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. This can be achieved by adding it into a DNS entry or to the Windows hosts file. You may have to modify the Windows firewall rules to allow the connection.

Windows, Mac, and Linux Endpoint Management Setup

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

When FortiClient EMS is integrated with FortiGate, you can use gateway lists to help FortiClient endpoints connect to FortiClient EMS and FortiGate. You can also import FortiClient profiles from FortiGate to FortiClient EMS.

FortiClient EMS

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

1. Configure user accounts. See Configuring user accounts on page 17.
2. Add domains and/or discover local endpoints. See Adding endpoints on page 18
3. Add a FortiClient installer to EMS. See Adding FortiClient installers on page 21.
4. Create an endpoint profile and select a FortiClient installer. See Creating profiles to deploy FortiClient on page 23.

> You can use FortiClient EMS with an Active Directory server to install and upgrade FortiClient (Windows) on endpoints before and after endpoints connect Telemetry to EMS. You can use FortiClient EMS with workgroups only to upgrade FortiClient (Windows) on endpoints after they connect Telemetry to EMS and FortiClient connects to FortiClient EMS. When using workgroups, you must separately install FortiClient (Windows) on endpoints. See the *FortiClient EMS Administration Guide*.

> 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*.

5. Prepare Windows endpoints for FortiClient deployment. See Preparing Windows endpoints for FortiClient deployment on page 26.
   You must also prepare the Windows AD server for deployment. See the *FortiClient EMS Administration Guide*.
6. Assign a profile to a workgroup, domain, endpoint group, or organizational group. See Assigning profiles to Windows, Mac, and Linux endpoints on page 27.
   Depending on the selected profile's configuration, FortiClient is installed on the endpoints to which the profile is applied.
   After FortiClient installation, the endpoint user must connect FortiClient Telemetry to FortiGate or FortiClient EMS to receive the profile configuration and complete endpoint management setup. See Connecting manually from FortiClient on page 19.
7. View the endpoint status. See Viewing endpoints on page 27.

FortiClient EMS integrated with FortiGate

Following is a summary of how to use FortiClient EMS when integrated with FortiGate:

1. Configure user accounts. See Configuring user accounts on page 17.
2. Add domains and/or discover local endpoints. See Adding endpoints on page 18
3. Create gateway lists. See Creating gateway lists on page 20.
4. Assign the lists to domains or workgroups. See Assigning gateway lists to endpoints on page 21.
   Alternately, you can add a FortiClient Telemetry gateway list to a custom FortiClient installer using the FortiClient Configurator tool.
5. Add a FortiClient installer to EMS. See Adding FortiClient installers on page 21.
6. Create an endpoint profile and select a FortiClient installer. See Creating profiles to deploy FortiClient on page 23.

> You can use FortiClient EMS with an Active Directory server to install and upgrade FortiClient (Windows) on endpoints before and after endpoints connect Telemetry to EMS. You can use FortiClient EMS with workgroups only to upgrade FortiClient (Windows) on endpoints after they connect Telemetry to EMS and FortiClient connects to FortiClient EMS. When using workgroups, you must separately install FortiClient (Windows) on endpoints. See the *FortiClient EMS Administration Guide*.

> 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*.

7. Prepare Windows endpoints for FortiClient deployment. See Preparing Windows endpoints for FortiClient deployment on page 26.
   You must also prepare the Windows AD server for deployment. See the *FortiClient EMS Administration Guide*.
8. Assign a profile to a workgroup, domain, endpoint group, or organizational group. See Assigning profiles to Windows, Mac, and Linux endpoints on page 27.
   Depending on the selected profile's configuration, FortiClient is installed on the endpoints to which the profile is applied.

   After FortiClient installation, the endpoint user must connect FortiClient Telemetry to FortiGate or FortiClient EMS to receive the profile configuration and complete endpoint management setup. See Connecting manually from FortiClient on page 19.
9. View the endpoint status. See Viewing endpoints on page 27.

Configuring user accounts

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

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 Server*.
2. Configure the options, and click *Test*.
3. If the test is successful, click *Save*.

To configure users:

1. Go to *Administration > Administrators*.
2. Click *Add* from the toolbar.
3. In the *User* list, select *Windows* or *LDAP*.
   The *LDAP* option is available only after you add an LDAP server to FortiClient EMS.
4. Select the user's specific domain access.
5. Configure the permissions.
6. Click *Save*.

Adding endpoints

You can add endpoints using an Active Directory service. Endpoints are also added when endpoint users manually connect FortiClient Telemetry to FortiClient EMS.

Adding endpoints using an Active Directory domain server

Endpoints can be manually imported from an Active Directory (AD) domain 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.

	An instructional video on how to add a domain is available in the Fortinet Video Library.

	You can add the entire domain or an organizational unit (OU) from the domain.

To add endpoints using an Active Directory domain service:

1. Click *Endpoints > Manage Domains > Add*. The *Domain* pane displays.

2. Configure the following options:

IP address/Hostname	Type the IP address or name.
Port	Type the port number.
Distinguished name	Type the distinguished name (optional).
Bind type	Select the bind type: *Simple*, *Anonymous*, or *Regular*. When you select *Regular*, enter the *User DN* and *Password*.
Username	Available when *Bind Type* is set to *Regular*. Type the user DN.
Password	Available when *Bind Type* is set to *Regular*. Type 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*.

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.

Connecting manually from FortiClient

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

To connect FortiClient Telemetry to FortiClient EMS:

1. In FortiClient Console on the endpoint, go to the *Compliance & Telemetry* tab.
2. In the *FortiGate or EMS IP* box, type the EMS IP address, and click *Connect*. FortiClient connects to FortiClient EMS.

For information about FortiClient, see the *FortiClient Administration Guide* available on
docs.fortinet.com/forticlient/admin-guides.

	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 5.2 is 8010 and in FortiClient 5.4 is 8013. By default, FortiClient EMS listens for connection on port 8013.

	Note it is considered best practice to add endpoints using the method in Adding endpoints using an Active Directory domain server on page 18. Connecting FortiClient to FortiClient EMS manually is only recommended for troubleshooting purposes.

Creating 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 create one or more gateway lists. Each list can contain IP addresses for multiple FortiGate units.

To create gateway lists:

1. Go to *Gateway Lists > Manage Gateway Lists*.
2. Click the *Add* button.
3. Configure the following:

Name		Enter the list name.
Comment		Enter additional comments (optional).
IP addresses/hostnames		Enter the IP address and port for FortiGate devices using the following format: IP:port. You can also use an FQDN. Press the *Enter* key to add additional IP addresses.
Connect to local subnets only		Enable to only allow to connect to local subnets.
Use connection key		Enable the connection key endpoints can use to connect to FortiGate units.
	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*.

4. Click *Save*.

Assigning gateway lists to endpoints

After creating a gateway list, you can assign the list to endpoints. When you assign the IP list and FortiClient Telemetry data connection process has started, the endpoint connects to a FortiGate or EMS, based on the gateway list.

To assign gateway lists to endpoints:

1. Go to *Endpoints*.
2. Right-click a domain or workgroup, and select *Assign gateway list*.
3. Select the desired list or create a new gateway list.

Adding FortiClient installers

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

When you add a FortiClient installer to FortiClient EMS, an installer for the Windows operating system and an installer for the macOS operating system are added to FortiClient EMS.

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

To add FortiClient installers:

1. Go to *Profile Components > Manage Installers*.
2. Click *Add*.
3. On the *General* tab, set the following options:

Name	Type the FortiClient installer's name.
Notes	(Optional) Type any notes about the FortiClient installer.
Version	Select the FortiClient version to install. Click *Upload* to add a custom FortiClient installer.
Patch version	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. This field is only available for the latest FortiClient version FortiClient EMS can access from FortiGuard. This option is not available if an older FortiClient version is selected.

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

Security Fabric Agent (Mandatory Feature)	Enabled by default and cannot be disabled. Installs FortiClient with Telemetry and Vulnerability Scanning enabled.
Secure Access Architecture Components	Enable to install FortiClient with SSL VPN and IPsec VPN enabled. Disable to omit SSL VPN and IPsec VPN support from the FortiClient installer.
Advanced Persistent Threat (APT) Components	Enable to 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 to select one, two, or all of the following features: • AntiVirus • Web Filtering • Application Firewall • Single Sign-On mobility agent Disable to exclude the features from the FortiClient installer.

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

Enable automatic registration	Enable to configure FortiClient to automatically connect Telemetry to EMS or FortiGate after FortiClient is installed on the endpoint. Disable to turn off this feature and require endpoint users to manually connect Telemetry to EMS or FortiGate.
Enable desktop shortcut	Enable to configure the FortiClient installer to create a desktop shortcut on the endpoint.
Enable start menu shortcut	Enable to configure the FortiClient installer to create a Start menu shortcut on the endpoint.
Enable endpoint tag	Enable to configure an endpoint tag to assign to endpoints. Under *Endpoint Tag*, select an existing tag or enter a new tag. FortiClient EMS automatically groups tagged endpoints according to group assignment rules. See Group assignment rules on page 1. This option is not available when the FortiClient installer selected or uploaded in step 3 is a version prior to 6.0.0.

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

EMS	Click *EMS* to configure the FortiClient installer to connect Telemetry to EMS.
FortiGate	Click *FortiGate*, and select the name of the gateway list to use. The gateway list defines the IP address for FortiGate and includes the IP address for EMS. You must define a FortiClient Telemetry gateway list to select FortiGate. If you have not created a list, the *No Gateway IPs have been defined* dialog box is displayed, and you can click *OK* to create a list.

7. Click *Save*. The FortiClient installer is added to FortiClient EMS and displays on the *Manage Installers* pane.

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

Configuring endpoint profiles

When you install FortiClient EMS, a default profile is created. This profile is applied to any groups you create. 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.

Creating profiles to deploy FortiClient

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

You must add FortiClient installers to FortiClient EMS before you can select the installers in a profile. See Adding FortiClient installers on page 21.

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

You can disable a feature included in the installer, then enable the feature in the profile later. For example, if the installer 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.

To create profiles for FortiClient deployment:

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		
	Assign an	Click *Installer*.
	Installer	In the *Installer* list, select a FortiClient installer. If you have not added a FortiClient installer to FortiClient EMS, see Adding FortiClient installers on page 21.
		The selected FortiClient installer affects what tabs display for configuration. Only tabs related to features enabled in the FortiClient installer display for configuration.
Schedule		
	Start At	Specify what time to start installing FortiClient on endpoints.

	Reboot When Needed	Enable to reboot the endpoint to install FortiClient when needed.
	Reboot when no users is logged in	Enable to 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	Enable to 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	Type 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 EMS to install FortiClient on endpoints using AD. If the credentials are wrong, the installation fails, and an error displays in EMS.
	Password	Type the password to perform deployment on AD.

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

Importing FortiGate profiles

In FortiOS, endpoint profiles are called FortiClient Compliance profiles. You can import a FortiClient Compliance profile into EMS, then edit the profile in FortiClient EMS to add a FortiClient installer or add configuration information that supports the FortiGate compliance rules.

> To import profiles successfully from FortiOS to FortiClient EMS, FortiGate must have the HTTPS port open. In FortiOS, go to *Network > Interfaces > Administrative Access* and enable the *HTTPS* checkbox.

To import profiles:

1. Click *Endpoint Profiles > Manage Profiles > Import*. 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 device 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 FortiClient Compliance profiles configured on the FortiGate displays.

Under each profile name is the list of profiles created for different operating systems, such as desktops running a Windows or Mac operating system or devices running an Android operating system. In the example, under the test profile, *Android*, *Desktop*, and *iOS* profiles are listed. You can click the *</>* icon beside each profile to preview the settings in XML format.

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

   Select the name of the profile to import all profiles for it into EMS. You can also clear the checkbox beside the profiles you do not want to import into EMS. For example, you can import the Android and desktop profiles, but not the iOS profile for a given profile name.

5. 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 FortiGate. You can manually sync profile changes after importing the profile. See 0730_Sync profile changes on page 1.

   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 EMS and display under the *Endpoint Profiles* pane in a group named after the FortiGate device from which they were imported.

7. In the *Endpoint Profiles* page, select an imported profile to edit it.

   The options configured in the profile by the FortiGate administrator are read-only compliance rules. You cannot change them. You can edit additional options to provide configuration information to support the compliance rules. You can also add a FortiClient installer to the profile by using the *Deployment* tab. Custom installers can be created. See Adding FortiClient installers on page 21.

8. Edit the options on the tabs.

9. Click *Save Profile*.

Preparing Windows endpoints for FortiClient deployment

The following services must be enabled and configured on each Windows endpoint before FortiClient is deployed to them:

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

> The Windows Firewall must be configured to allow the following inbound connections:
> - File and Printer Sharing (SMB-In)
> - Remote Scheduled Tasks Management (RPC)

For AD group deployments, an AD administrator account is required. For non-AD deployments, the installer URL can be shared with users, who can then download and install FortiClient manually. You can locate the installer URL in *Manage Installers*. Go to *Profile Components > Manage Installers*.

Assigning profiles to Windows, Mac, and Linux endpoints

After creating the profile, you can assign the profile to domains or workgroups. When you assign the profile to domains or workgroups, the profile settings are automatically pushed to the endpoints in the domain or workgroup.

If you do not assign a profile to a specific domain or workgroup, the default profile is automatically applied.

To assign profiles:

1. Go to *Endpoints*.
2. Right-click a domain or group, select *Assign profile*, then the profile. A confirmation dialog box displays.
3. Click *Yes*. The profile is assigned.

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 in the *Client Details* pane 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.

To view 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.

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 not connected to FortiClient EMS or FortiGate. 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.
Not Compliant	Number of endpoints not compliant with the FortiGate compliance rules. Click to display the list of not compliant endpoints.
Security Risk	Number of endpoints that are a security risk. Click to display the list of 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 in the content pane.
Search All Fields	Type 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 operating system on the endpoint and the device name.
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 assigned to the endpoint and the profile's synchronization status.
Connections	Visible when headings are displayed. Displays whether the endpoint is connected to FortiClient EMS or FortiGate and the connection status of *Online*, *Offline*, or *Not Registered*.
Status	Visible when headings are displayed. Displays one of the following compliance statuses for the endpoint. • Compliant • Not compliant • Not participating in compliance • Quarantined • Excluded • Not registered • Not installed
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 AntiVirus 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 • De-register • Register • Quarantine • Un-quarantine • Exclude from Management • Mark as Uninstalled • Delete Device

The following tabs are available in the content pane toolbar when you select an endpoint:

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 device name.
	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.
	Connection	Displays when the selected endpoint is connected to FortiClient EMS or FortiGate. Also displays the connection status.
	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. • Gateway List: Name of the gateway list used for the selected endpoint. Displays *Not Assigned* if no 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.
	Compliance	Displays if the endpoint is compliant. If the endpoint is not compliant, displays the features for which FortiClient is not compliant.
	Features	Displays which features are enabled for FortiClient.
Antivirus Events		
	Date/Time	Displays the antivirus event's date and time.
	Message	Displays the antivirus event's message.
Sandbox Events		
	Date/Time	Displays the sandbox event's date and time.
	Message	Displays the sandbox event's message.
Firewall Events		
	Date/Time	Displays the firewall event's date and time.
	Message	Displays the firewall 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.
	FortiGuard ID	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.

Web Filter Events		
	Date/Time	Displays the web filter event's date and time.
	Message	Displays the web filter event's message.
System Events		
	Date/Time	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.

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
   - Not Compliant
   - Security Risk

   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 endpont.
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 .

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 46.
2. Add the Google domain. See Adding Google domains on page 47.
3. Create an endpoint profile. See Adding new profiles on page 47.
4. Assign the endpoint profile to the Google domain. See Assigning profiles to Chromebooks on page 49.
5. View the status. See Viewing domains on page 49.

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.

Logging into the Google Admin console

To log into the Google Admin console:

1. Log into the Google Admin console (https://admin.google.com) using your Google domain admin account. The Admin console displays.
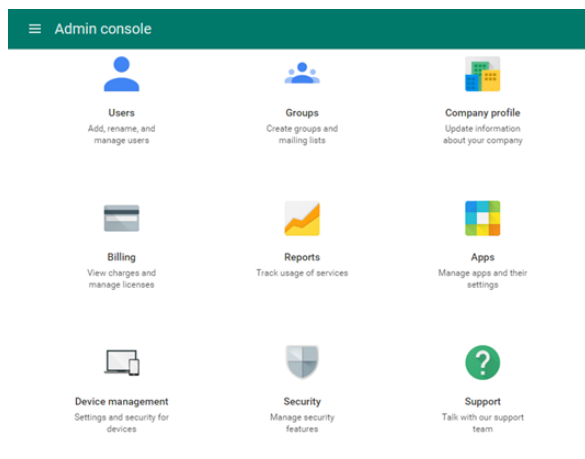
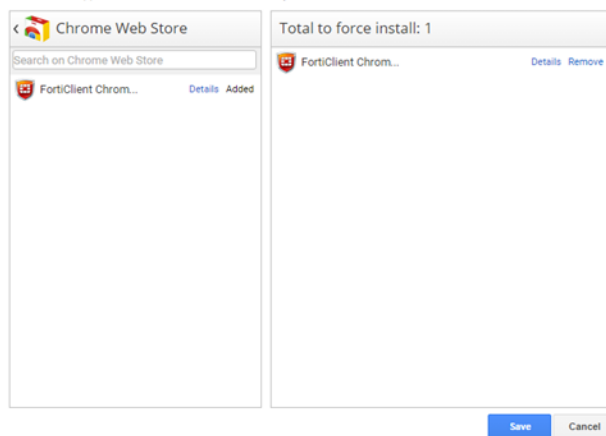## Adding the FortiClient Web Filter extension

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

To add the FortiClient Web Filter extension:

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*.

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.

To configure the FortiClient Web Filter extension:

1. In FortiClient EMS, locate the server name and port by going to *System Settings > Server*.
2. Create a text file that contains the following text:
    ```
    {
        "ProfileServerUrl": { "Value": "https://< ProfileServer >:< port for Profile Server >"}
    }
    ```

For example:

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

3. In the Google Admin console, go to *Device management > Chrome Management > App Management > FortiClient Chrome Web Filter Extension > User settings*.

4. Click a domain or organization unit (OU).

5. In the right pane, under *Configure*, upload a new configuration file.
    You can also view the current settings.

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 on page 46.

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 37.

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 device 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 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>`.

Enabling HTTPS logging access to FortiAnalyzer

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

To add 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*.

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

To add root certificates:

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.
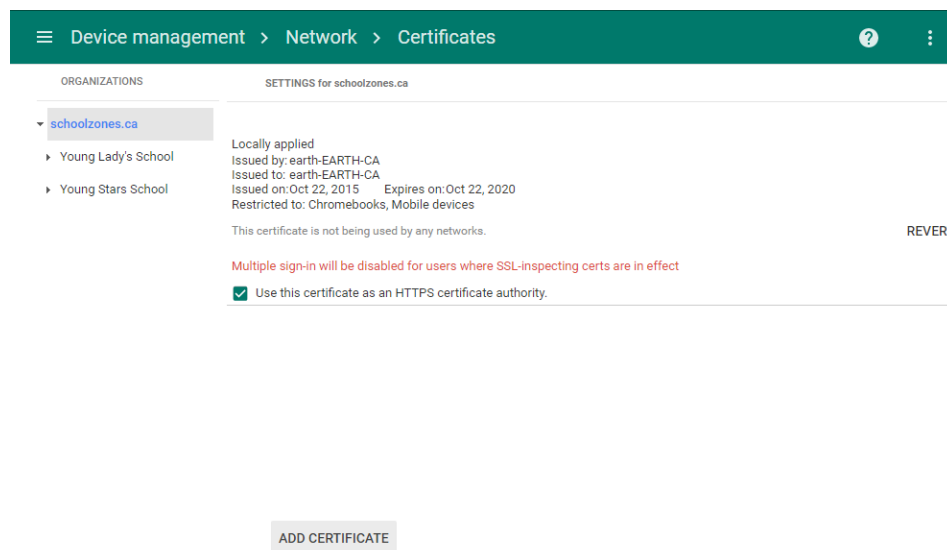
Disabling access to Chrome developer tools

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

To disable access to Chrome developer tools:

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, extensions are bypassed. Incognito mode should be disallowed for managed Google domains.

To disallow incognito mode:

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*.
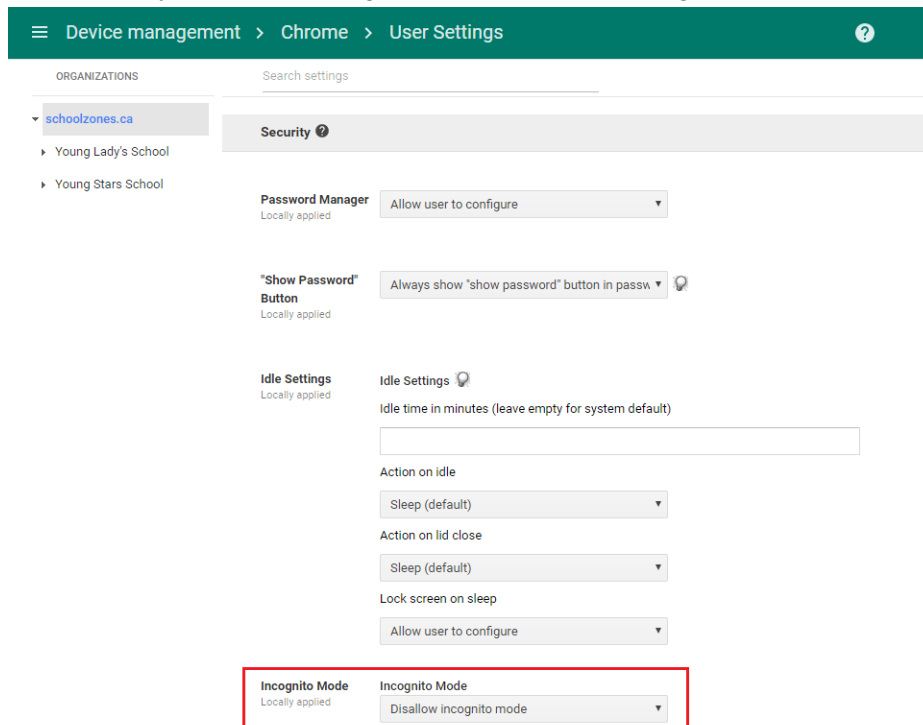
4. Click *Save*.

Disallowing guest mode

Guest mode should be disallowed for managed Google domains.

To disallow guest mode:

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.
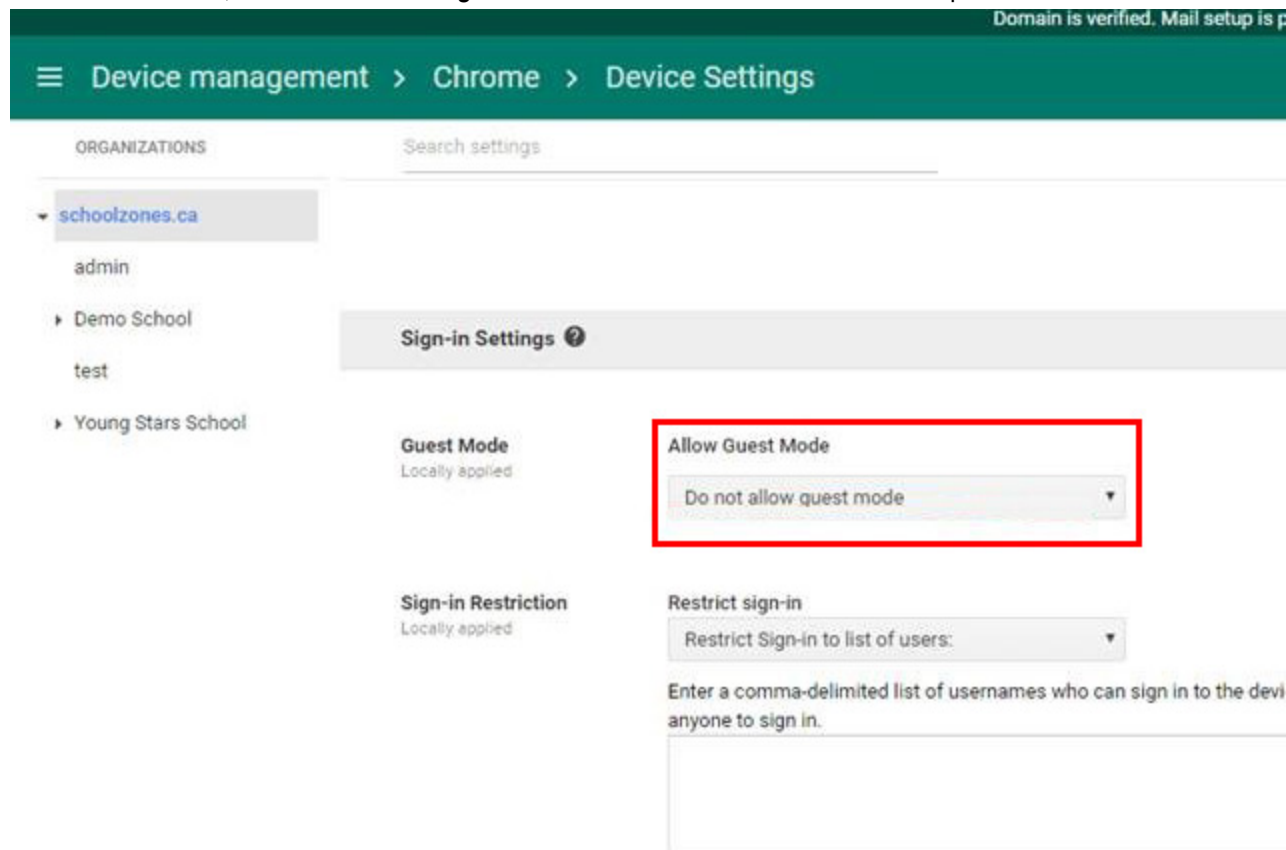
4. Click *Save*.

Blocking Task Manager

Task Manager should be blocked for managed Google domains.

To block Task Manager:

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.
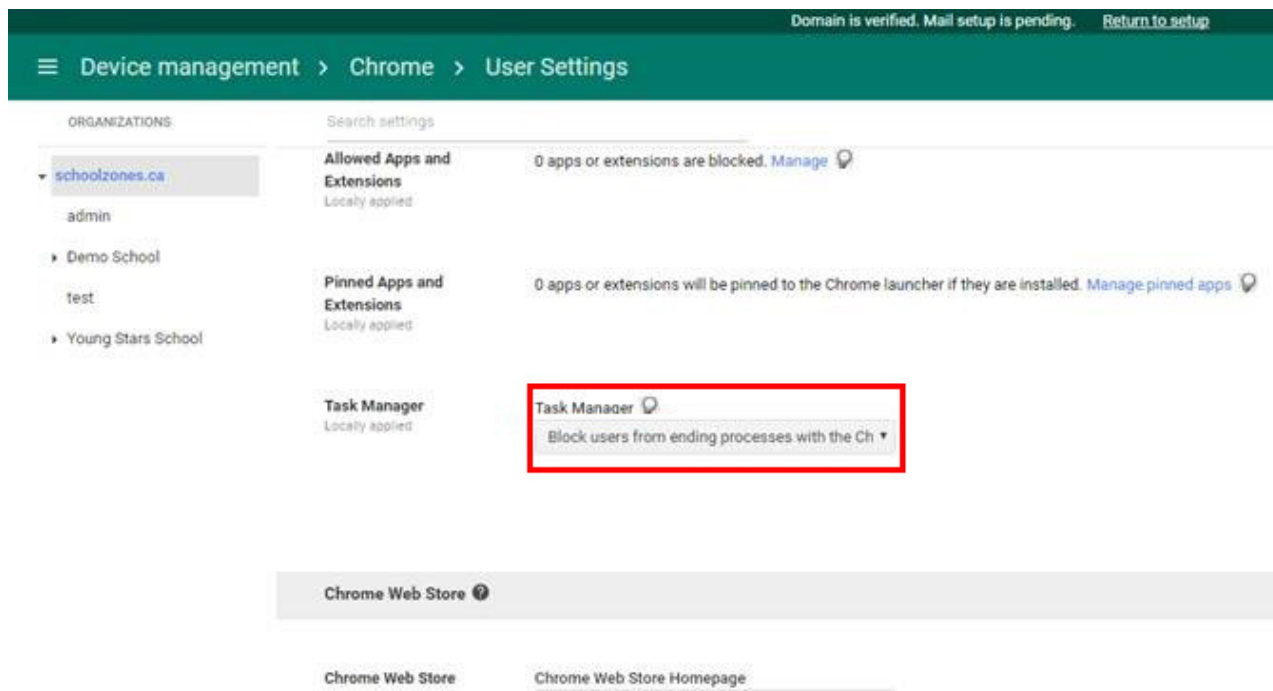
4. Click *Save*.

Service account credentials

FortiClient EMS requires service account credentials generated by the Google Developer console. 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.

This section describes how to configure default and unique service account credentials. See the following sections.

Configuring default service account credentials

FortiClient EMS includes the following default service account credentials generated by the Google Developer console:

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	FortiClient EMS

Option	Default setting	Where used
	credentials	

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

Adding the default service account client ID to the Google Admin console

To configure the default service account credentials, you must add the client ID's default value to the Google Admin console. No other configuration for service account credentials is required. See Adding service account credentials to the Google Admin console on page 45.

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 41.
2. Add the unique service account credentials to the Google Admin console. See Adding service account credentials to the Google Admin console on page 45.
3. Add the unique service account credentials to FortiClient EMS. See Adding service account credentials to EMS on page 45.

Creating unique service account credentials

Creating a unique set of service account credentials provides more security. Unique service account credentials include the following:
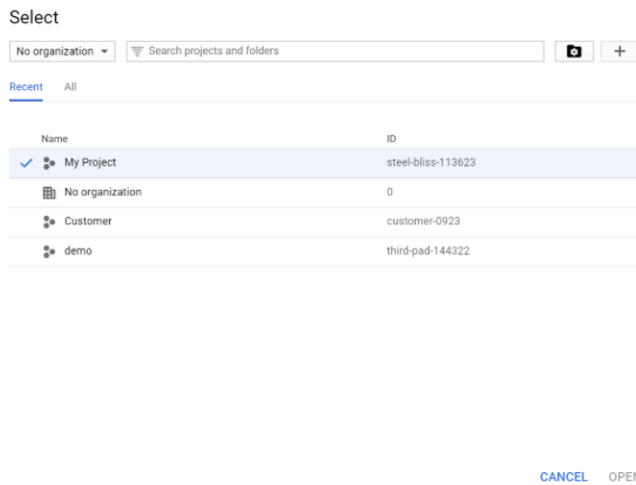
- Client ID (a long number)
- Service account ID (email address)
- Service account certificate (a certificate in `.pem` format)

To create a unique service account:

1. Go to https://console.developers.google.com.
2. Log in with your G Suite account credentials.
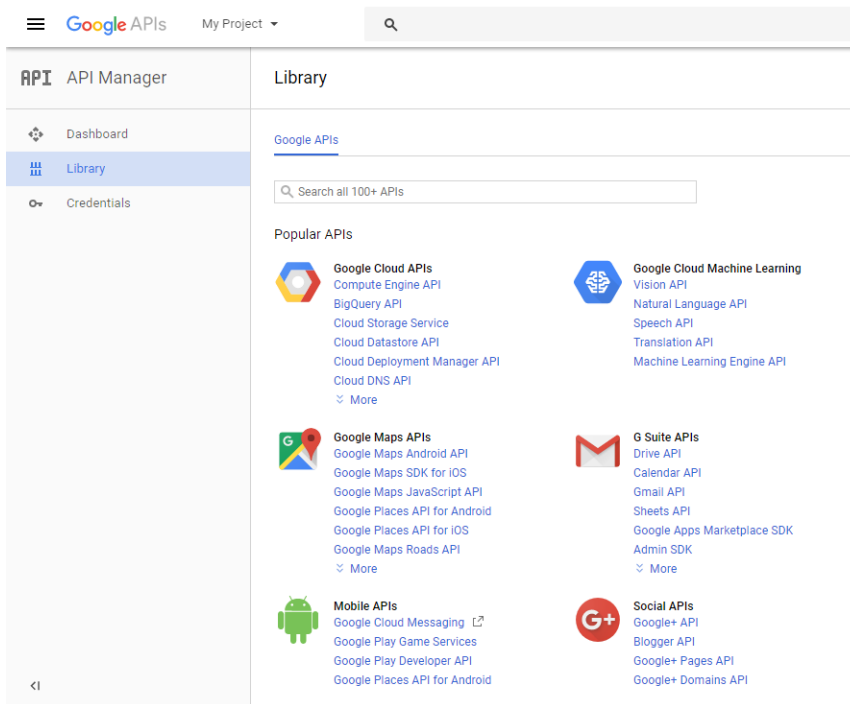
3. Create a new project:

    a. Click the toolbar list. The browser displays the following dialog.

    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*.

c. Click *ENABLE*.

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*.

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   ⧉

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

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

Product name for the consent screen

Product name

CANCEL   SAVE   **CONFIGURE CONSENT SCREEN**

8. Click *Save*.

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

☰ **Google** APIs   My Project ▾   🔍

API API Manager   ← Client ID for Service account client   ⬇ DOWNLOAD JSON   🗑 DELETE

◈ Dashboard

⛁ Library   ⓘ Service account clients are created when domain-wide delegation is   [Manage service accounts]
                                        enabled on a service account.
🔑 Credentials

                                    Client ID   115703365324425320868

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

                                    Creation date   Jun 12, 2017, 1:58:28 PM

                                    Name

                                    Client for test-410

                                    [Save]   [Cancel]

> To use the private key in EMS, it needs to be converted to `.pem` format. You can use the following `openssl` command to convert it. Remember to use the notasecret password.
> ```
> C:\OpenSSL-Win64\bin>openssl pkcs12 -in demo-976b9d6e9328.p12 -out
>         serviceAccount-demo.pem -nodes -nocerts
> Enter Import Password:
> ```

Adding service account credentials to the Google Admin console

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

To add the client ID:

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

To add service account credentials:

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

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

2. 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:

ID	Type a new email address for the service account credentials.
Private key	Click *Browse* and select the certificate provided with the service account credentials.

3. Click *Save*.

4. 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 SSL certificates to FortiClient EMS on page 46
- Required only when sending logs to FortiAnalyzer: Adding SSL certificates to FortiAnalyzer on page 36

Adding SSL certificates to FortiClient EMS

You must add an SSL certificate to FortiClient EMS to allow HTTPS connections with the Google Admin console.

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 or replace SSL certificates:

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

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, type the password.
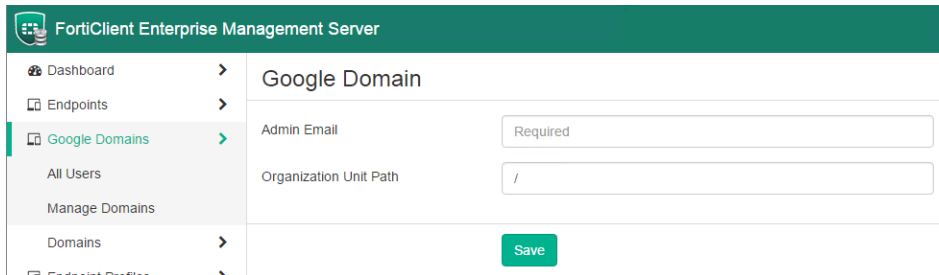
5. Click *Test*.

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 |

Adding Google domains

To add Google domains:

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

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

> / stands for the root of the domain.

4. Click *Save*.
   The Google domain information and users are imported into FortiClient EMS.

Configuring Chromebook profiles

Chromebook profiles support web filtering by categories, black and white lists, and safe search. You can create different profiles and assign them to different groups in the Google domain.

Adding new profiles

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

> It is recommended to add Yandex search engine to the black list in the profile.

To create new profiles:

1. Go to *Endpoint Profiles > Manage Profiles*, and click the *Add Chrome* button.
2. In the *Profile Name* box, type 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:
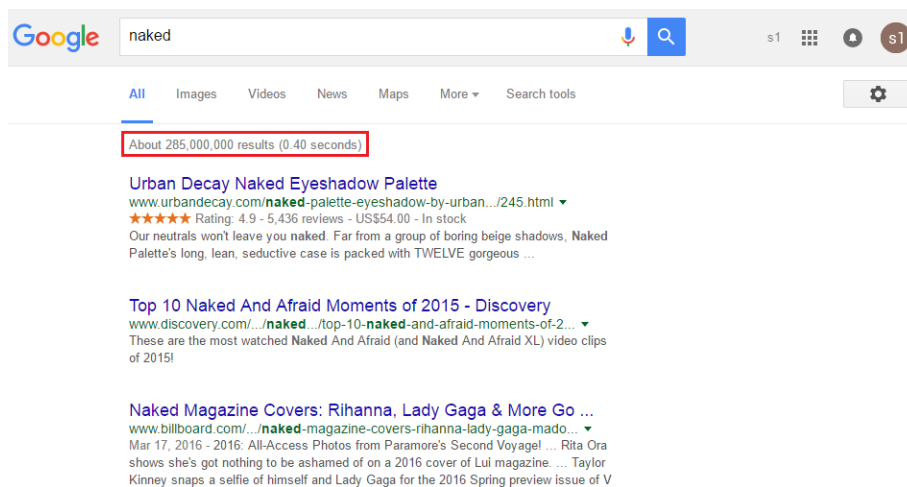
Here are the search results when the Safe Search feature is enabled, which has about 256000000 results.
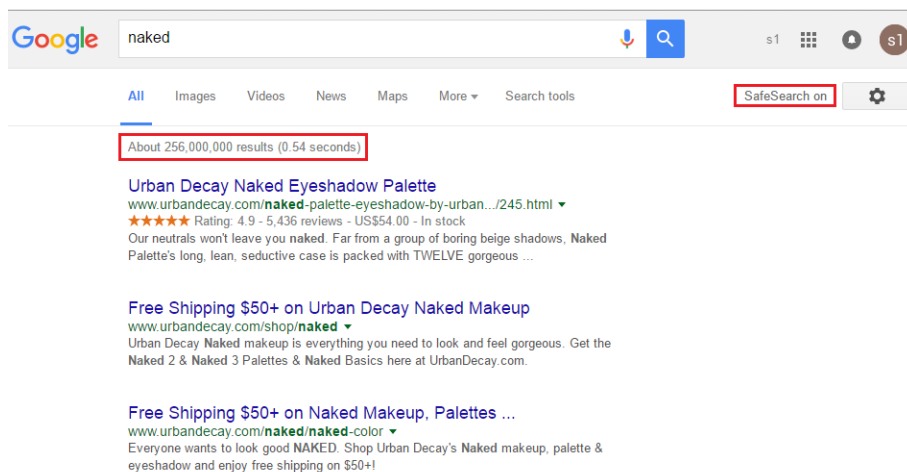
To enable or disable Safe Search:

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*.

Assigning profiles to Chromebooks

After creating the profile, you can assign the profile to Google domains. When you assign the profile to domains, the profile settings are automatically pushed to the Chromebooks in the domain.

To assign profiles:

1. Go to *Google Domains*.
2. Right-click a domain, select *Assign Profile*, then the profile. The profile is assigned.
3. Hover the mouse over the name of the domain to view the name of the assigned profile.

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.

To view the Google Users pane:

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

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

The following options are available in the toolbar:

Clear 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 are displayed for Google users:

Name	Chromebook user's name.
Email	Chromebook user's email address.
Last Login	Date and time when the user last logged into the domain.
Last Policy Retrieval	Date and time of the last endpoint profile retrieved by the Google Chromebook.
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.

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	User's name.
Email	User's email address.
Last Login	Date and time when the user last logged into the domain.
Last Policy Retrieval	Date and time of the last endpoint profile retrieved by the Google Chromebook.
Organization Path	Organization path of the user in the domain.
Effective Policy	Name of the profile 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 the blocked site was visited.
Threat	Threat type detected.
Client Version	Chromebook user's current version.
OS	Type of OS used by the Chromebook user.

Fields	Information
URL	Blocked site's URL.
Port	Port number currently listening.
User Initiated	User initiated visitation to the blocked site.