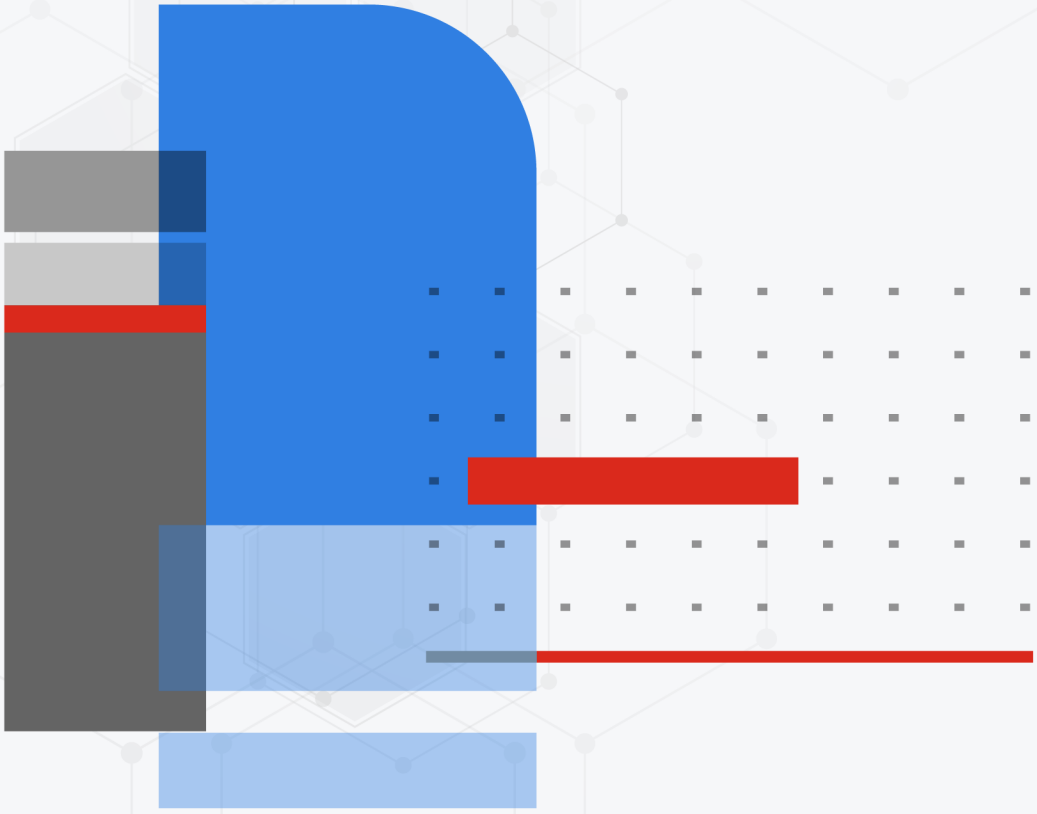
QuickStart Guide

FortiClient EMS 7.4.3



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

August 27, 2025
FortiClient EMS 7.4.3 QuickStart Guide
04-743-1010850-20250827

TABLE OF CONTENTS

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.

Supported installation platforms

You can install FortiClient EMS on Ubuntu 22.04 LTS Server and Desktop.

For information about minimum system requirements and supported platforms, see Product integration and support.

Because implementing or migrating to EMS 7.4.0 on the Linux platform can be complex, Fortinet highly recommends FortiClient Best Practices Service (BPS).

FortiClient Best Practices Service is an account-based annual subscription providing access to a specialized team that delivers remote guidance on deployment, upgrades, and operations. The service allows customers to share information about their deployment, user requirements, resources, and other related items. Based on the information provided, the BPS experts can provide recommended best practices, sample code, links to tools, and other materials or assistance to speed adoption and guide the customer towards best practice deployments. The team does not log into customer devices to make changes for them. This is a consulting and guidance service which may include sample configurations or playbooks. This is not an on-site professional services offer.

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 certificates to support communication between FortiClient Web Filter extension and the following products:
  - FortiClient EMS
  - 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 or outgoing	How to customize
ACME	EMS can use certificates that are managed by Let's Encrypt and other certificate management services that use the ACME protocol. This feature also requires port 443. See Adding an SSL certificate to FortiClient EMS.	TCP	80	Incoming	N/A
Active Directory (AD) server connection	Retrieving workstation and user information	TCP	389 (LDAP) or 636 (LDAPS)	Outgoing	GUI
Antivirus (AV) allowlist signature download	Downloading AV allowlist signatures	TCP	10443 (default)	Incoming	N/A
Apache/HTTPS	Web access to FortiClient EMS. Also required for the ACME feature.	TCP	443	Incoming	Installer

Communication	Usage	Protocol	Port	Incoming or outgoing	How to customize
Communication between EMS AD connector and AD servers	Enables synchronization of AD groups and users with EMS for endpoint management, policy enforcement, and SAML-based authentication.	TCP	8871	Incoming	N/A
Communication with FortiOS	EMS is the server that opens up the port for FortiOS to connect to as a client.	TCP	8015	Incoming	N/A
FortiClient download	Downloading FortiClient deployment packages that FortiClient EMS created	TCP	10443 (default)	Incoming	Installer
FortiClient endpoint probing	FortiClient EMS uses ICMP for endpoint probing during FortiClient initial deployment.	ICMP	N/A	Outgoing	N/A
FortiClient Telemetry	FortiClient endpoint management	TCP	8013 (default)	Incoming	Installer or GUI
FortiCloud	FortiCloud services (forticlient.forticloud.com)	TCP	443	Outgoing	N/A
License synchronization	FortiCare login (support.fortinet.com) to synchronize licenses	TCP	443	Outgoing	N/A
SCEP service	Installing zero trust network access certificate	TCP	4001, 4002	Incoming	N/A
SMTP server, email	Alerts for FortiClient EMS and endpoint events. When an alert is triggered, EMS sends an email notification.	TCP	25 (default)	Outgoing	GUI
Web Filter custom page download	Downloading custom Web Filter pages that the administrator created in EMS	TCP	10443 (default)	Incoming	N/A

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

Communication	Usage	Protocol	Port	Incoming or 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 or 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

EMS uses the following FQDN for installer creation:

Usage	Server URL	Protocol	Port	Incoming or outgoing
Create installers on Fortinet-hosted servers and download them locally to EMS for deployment to endpoints	forticlient-rs.forticloud.com	TCP	443	Incoming/outgoing

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

Usage	Server URL			Protocol	Port	Incoming or outgoing	How to customize
	Global	U.S.	Europe				
AV and vulnerability signature update and FortiClient installer downloads	• forticlient.fortinet.net • myforticlient.fortinet.net	usforticlient.fortinet.net	N/A	TCP	80	Outgoing	N/A
AV and vulnerability signature updates with FortiGuard Anycast and FortiClient installer package download	fctupdate.fortinet.net	fctusupdate.fortinet.net	fcteuupdate.fortinet.net	TCP	443	Outgoing	N/A

FortiClient EMS can also connect to FortiClient Cloud Sandbox (SaaS) for integration with FortiSandbox. The following table summarizes required services for FortiClient EMS to communicate with FortiClient Cloud Sandbox (SaaS):

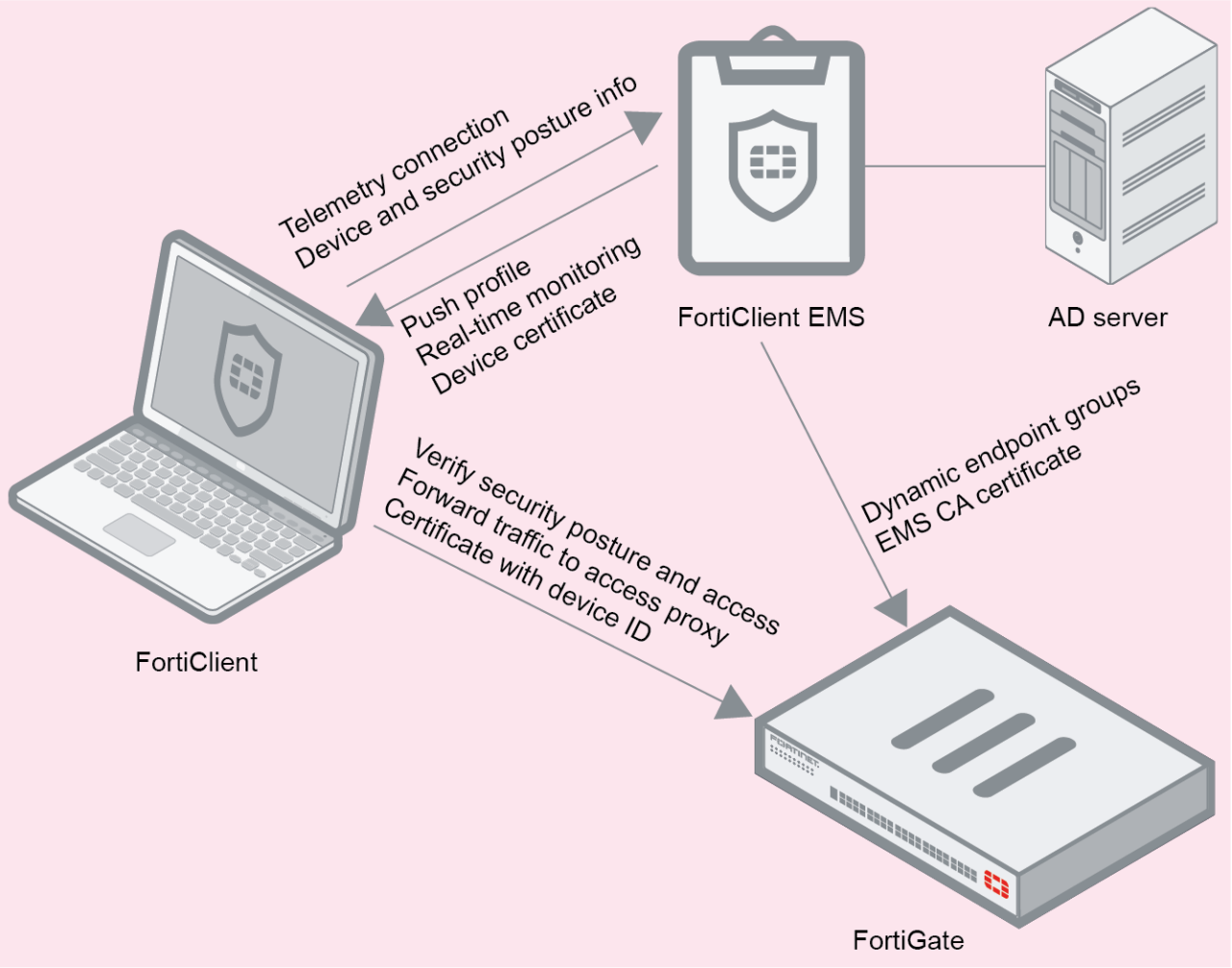
Usage	Server URL	Protocol	Port	Incoming or outgoing	How to customize
FortiClient EMS Cloud Sandbox (SaaS) connection	aptctrl1.fortinet.com	TCP	443 (default)	Outgoing	N/A

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.

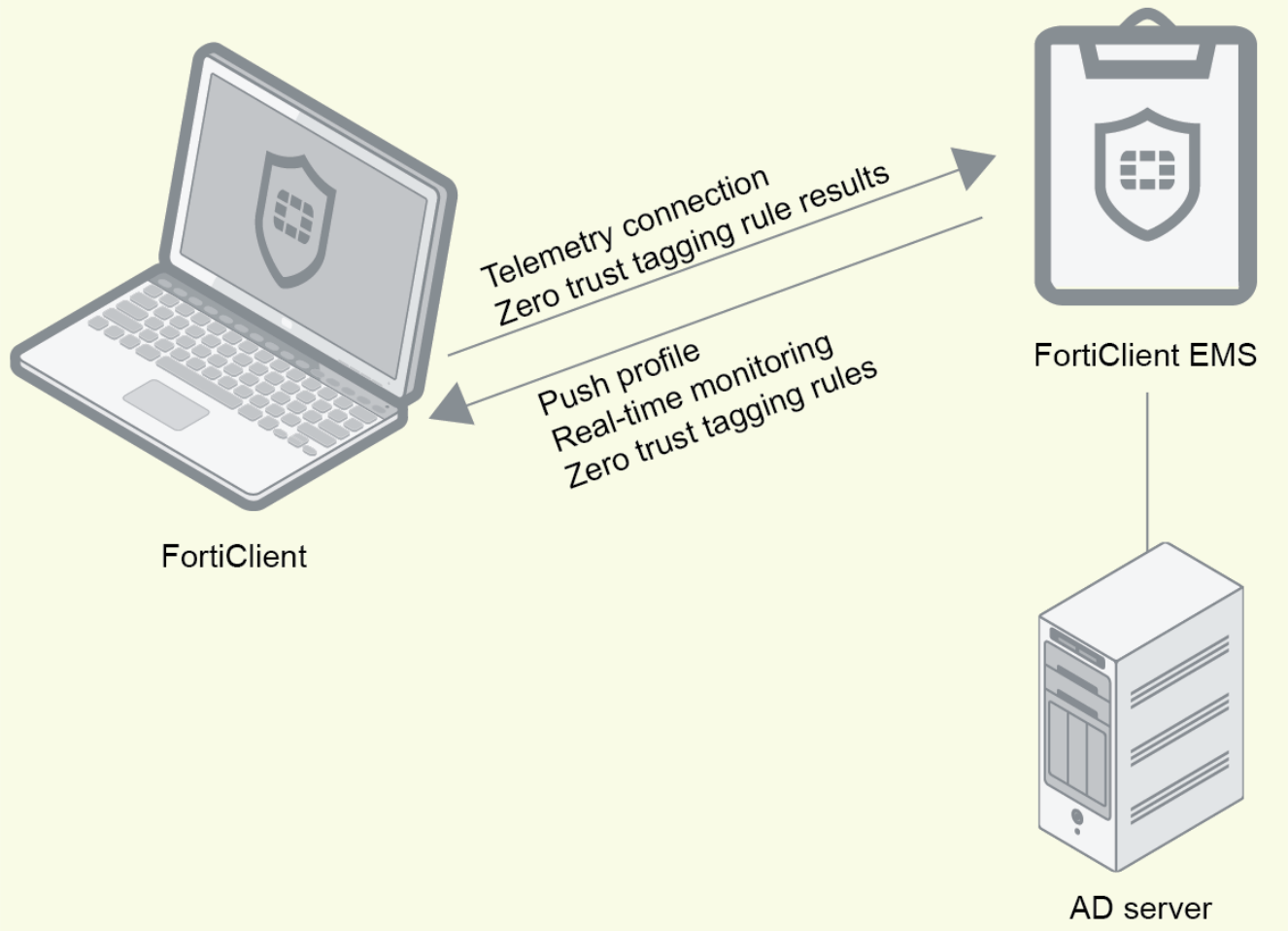
Security Fabric



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 security posture 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 security posture 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 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 that a Certificate Authority (CA) signed 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. You do not need to add the root certificate to the Google Admin console.

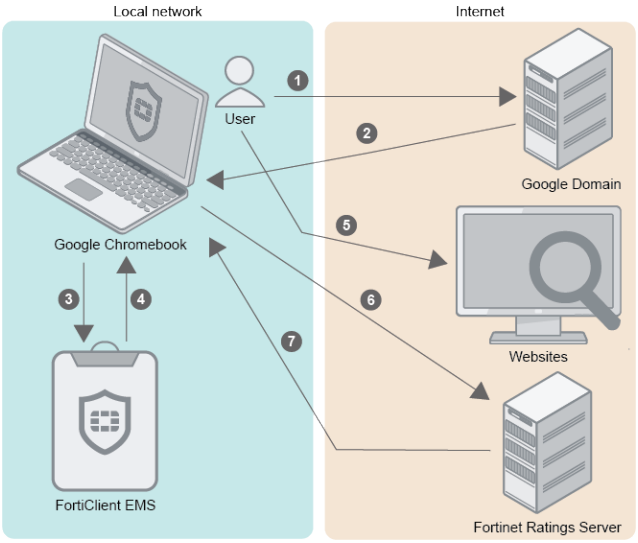
If you are using a self-signed certificate (non-public SSL certificate), your certificate's *Subject Alternative Name* must include `DNS:<FQDN>`, for example, `DNS:ems.forticlient.com`. You must add the SSL certificate to FortiClient EMS and the root certificate to the Google Admin console to allow the extension to trust FortiClient EMS. See Adding root certificates on page 48.

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 14.
2. Install FortiClient EMS. See Installing EMS in standalone mode on page 14.
3. Start FortiClient EMS and log in. See Starting FortiClient EMS and logging in on page 20.

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 installation files from a sales representative.

The following installation files are available for FortiClient EMS:

- forticlientems_7.4.3.xxxx.bin
- forticlientems_7.4.3.xxxx_migration_tool.zip
- forticlientems_7.4.3.xxxx_postgres-ha.tar.gz
- forticlientems_7.4.3.xxxx_postgresql15.tar.gz

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

Installing EMS in standalone mode

The following provides instructions for installing EMS in standalone mode with a local database (DB) and assumes that you have a machine with Ubuntu installed. You can install EMS in other scenarios, such as high availability, with a remote DB, and so on. See Installation.

To install standalone EMS:

1. Download the forticlientems_7.4.3.XXXX.arm64.bin or forticlientems_7.4.3.XXXX.amd64.bin file from the Fortinet Support site.

2. Run `sudo -i` to log in to the shell with root privileges.
3. Change permissions and add execute permissions to the installation file:
   `chmod +x forticlientems_7.4.3.XXXX.XXX64.bin`
   ```
   root@emsnode2:/home/ems/Downloads# chmod +x forticlientems_7.4.0.1745.bin
   ```
4. Set umask to 022 if the existing umask setting is more restrictive.
5. Run the following command to install EMS:
   `./forticlientems_7.4.3.XXXX.XXX64.bin -- --allowed_hosts '*' --enable_remote_https`
   Run the installer to and from any directory other than `/tmp`. Running the installer to or from `/tmp` causes issues.
6. After installation completes, check that all EMS services are running by entering the following command:
   `systemctl --all --type=service | grep -E 'fcems|apache|redis|postgres'`
   ```
   root@emsnode2:/home/ems/Downloads# systemctl --all --type=service | grep -E 'fcems|apache|redis|postgres'
     apache2.service                              loaded    active   running The Apache HTTP Server
     fcems_adconnector.service                    loaded    active   running adconnector service
     fcems_addaemon.service                       loaded    active   running addaemon service
     fcems_adevtsrv.service                       loaded    active   running adevtsrv service
     fcems_adtask.service                         loaded    active   running adtask service
     fcems_chromebook.service                     loaded    active   running chromebook worker service
     fcems_das.service                            loaded    active   running das service
     fcems_dbop.service                           loaded    active   running dbop worker service
     fcems_deploy.service                         loaded    active   running deploy worker service
     fcems_ecsocksrv.service                      loaded    active   running ecsocksrv service
     fcems_forensics.service                      loaded    active   running forensics worker service
     fcems_ftntdbimporter.service                 loaded    active   running FTNT DB importer worker service
     fcems_installer.service                      loaded    active   running installer worker service
     fcems_ka.service                             loaded    active   running kaworker service
     fcems_mdmproxy.service                       loaded    active   running MDM proxy service
     fcems_monitor.service                        loaded    active   running monitor worker service
     fcems_notify.service                         loaded    active   running FOS notify service
     fcems_pgbouncer.service                      loaded    active   running pgBouncer for EMS service
     fcems_probe.service                          loaded    active   running probeworker service
     fcems_reg.service                            loaded    active   running regworker service
     fcems_scep.service                           loaded    active   running SCEP service
     fcems_sip.service                            loaded    active   running software inventory processor service
     fcems_tag.service                            loaded    active   running tagworker service
     fcems_task.service                           loaded    active   running taskworker service
     fcems_update.service                         loaded    active   running update worker service
     fcems_upload.service                         loaded    active   running upload worker service
     fcems_wspgbouncer.service                    loaded    active   running pgBouncer for EMS WebServer service
     fcems_ztna.service                           loaded    active   running ztna worker service
     postgresql.service                           loaded    active   exited  PostgreSQL RDBMS
     postgresql@15-main.service                   loaded    active   running PostgreSQL Cluster 15-main
     redis-server.service                         loaded    active   running Advanced key-value store
   ```
   The output shows that postgresql.service status displays as `exited`. This is the expected status. EMS does not create this service, which only exists to pass commands to version-specific Postgres services. It displays as part of the output as the command filters for all services that contain "postgres" in the name.
7. Access the EMS GUI and log in.
8. If after initially installing EMS 7.4.3 you need to upgrade to a newer build, repeat the process with the new installation file.

Licensing EMS by logging in to FortiCloud

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

Applying a trial license to FortiClient EMS

To apply a trial license to FortiClient EMS:

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

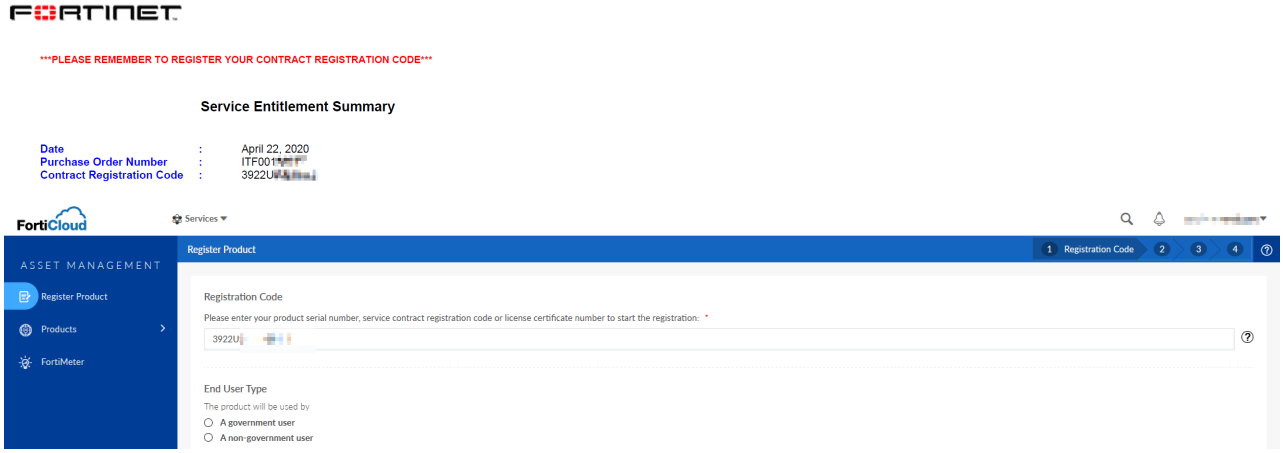
1. In EMS, in the *License Information* widget, click *Add* beside *FortiCloud Account*.
2. In the *FortiCloud Registration* dialog, enter your FortiCloud account credentials. If you do not have a FortiCloud account, create one.
3. Read and accept the license agreement terms.
4. Click *Login & Sync License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

Applying paid licenses to FortiClient EMS

To apply a paid license to FortiClient EMS:

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

1. Log in to your FortiCloud account on Customer Service & Support.
2. Go to *Asset Management*.
3. Click *Register More*.
4. In the *Registration Code* field, enter the *Contract Registration Code* from your service registration document. Configure other fields as required, then click *Next*.



5. Do one of the following:
   - 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.

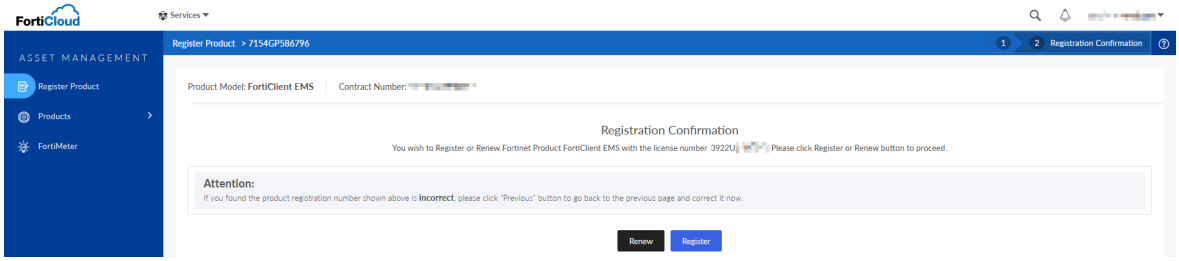
viii. Click *Login & Update License*. Once your account information is authenticated, EMS updates *Configure License* with the serial number and license information that it retrieved from FortiCloud.

- As the *FortiClient EMS Administration Guide* describes, you can apply multiple license types to the same EMS server. For example, if you have already applied an EPP license to your EMS server, you can apply another license type, such as a ZTNA license, to the same EMS server. If desired, add another license type:

  i. On the *Registration Confirmation* page, when applying an additional license type, you must select *Renew* on the contract registration screen, regardless of the license types of the first and subsequent licenses. Selecting *Renew* combines the new 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 cannot apply the new and existing licenses to the same EMS server.

  ii. In the *Serial Number* field, enter the EMS serial number or select the EMS instance from the list. You can find the serial number in *Dashboard* > *Status* > *License Information widget* > *Configure License* in EMS. Click *Next*.

  iii. Complete the registration, then click *Confirm*.

EMS reports the following information to 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.

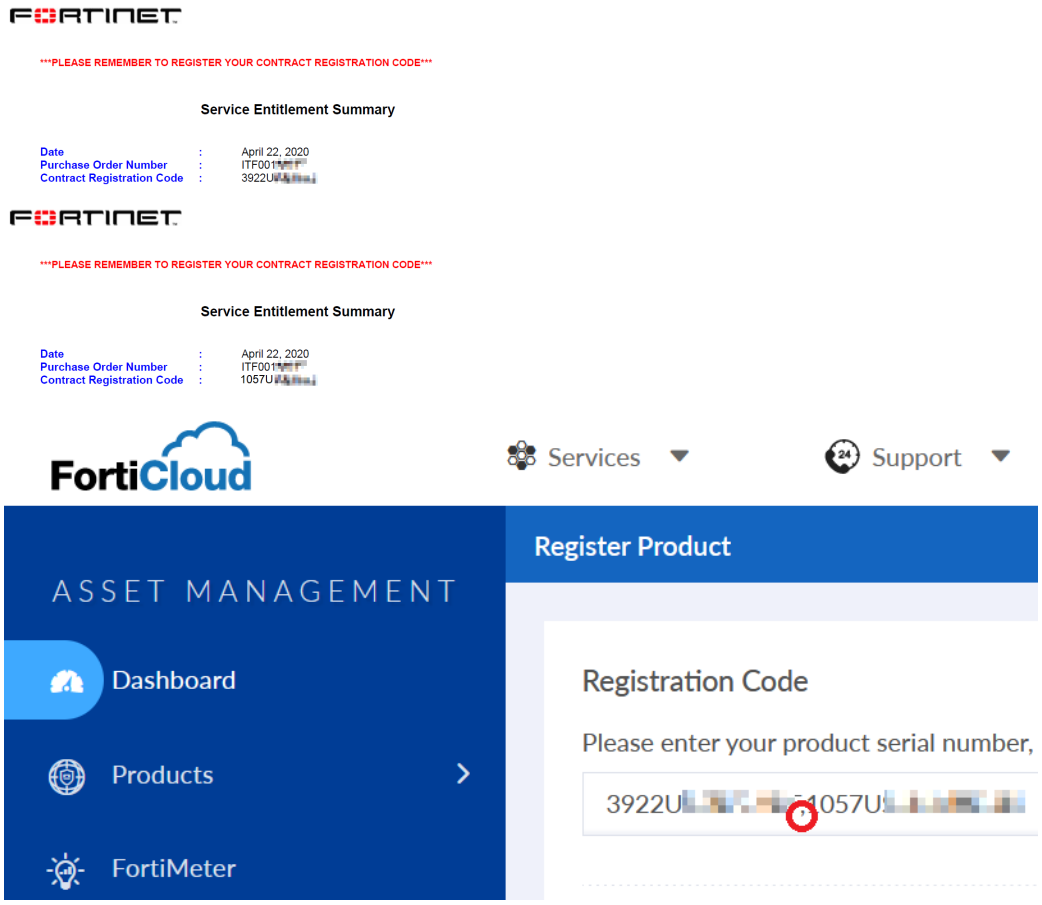
If you previously activated another license with the same EMS hardware ID, you receive a duplicated UUID error. In this case, contact Customer Support to remove the hardware ID from the old license.

To apply multiple paid licenses to FortiClient EMS:

You may want to apply multiple paid licenses of the same type to at the same time. For example, if you want EMS to manage 525 ZTNA endpoints, you can purchase two ZTNA licenses: one for 500 endpoints, and another for 25 endpoints. In this scenario, you need to register the licenses at the same time.

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

1. Log in to your FortiCloud account on Customer Service & Support.
2. Go to *Register Product*.
3. In the *Registration Code* field, enter the *Contract Registration Code*s from your service registration documents. Separate the codes with a comma. For example, to register the 3922U and 1057U codes in the following screenshots, you would enter 3922U,1057U in the *Registration Code* field. Configure other fields as required, then click *Next*.



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

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

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

EMS reports the following information to 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 Linux computers.

The post-install setup wizard facilitates rapid EMS setup for users immediately following installation, prioritizing license provisioning. You must have a license to proceed and use EMS.

EMS requires you to authenticate via FortiCloud for license entitlement immediately after install. You must log in to EMS, validate your FortiCloud account, and EMS must retrieve the license for you to proceed further. Access to EMS is contingent on the validation and connection of your FortiCloud account information.

In air-gapped instances, EMS allows you to upload a license file. However, this only applies in rare cases. In the majority of deployments, you must provide FortiCloud account information and EMS retrieves the license directly from FortiCloud.

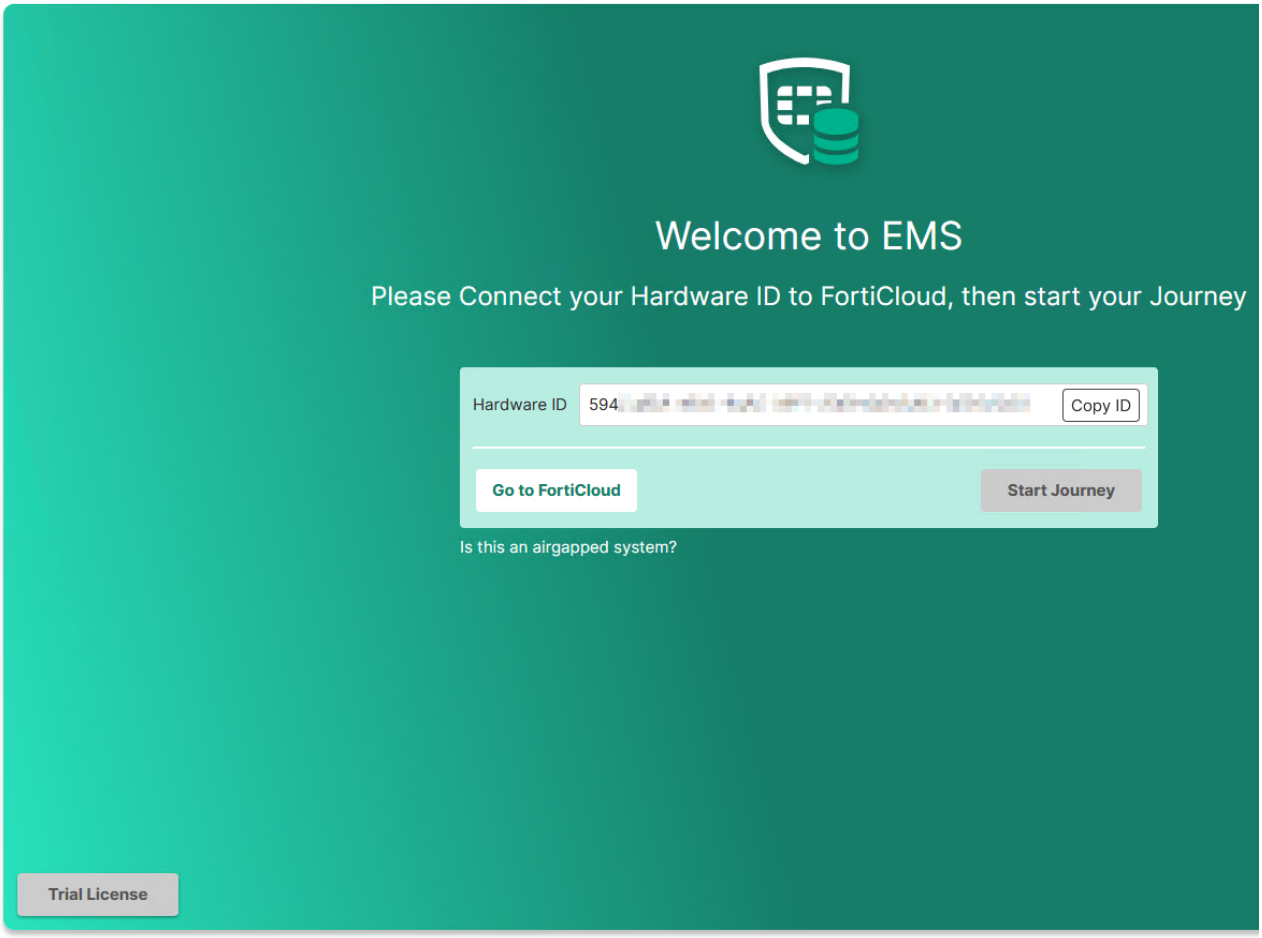
The post-install setup wizard streamlines the EMS post-install setup process.

To license EMS using the post-install setup wizard:

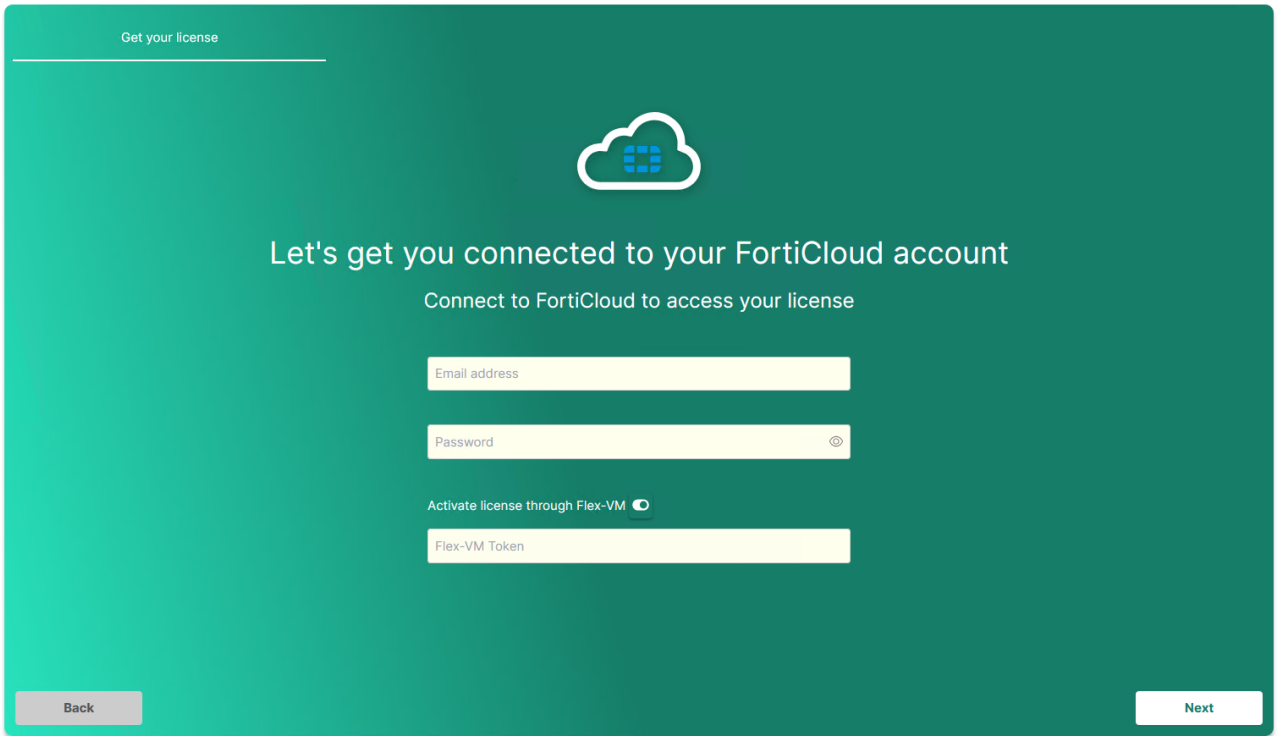
1. After installing EMS, launch it for the first time. EMS displays a *Welcome to EMS* page that displays the hardware ID of the machine that EMS is installed on. Registering and licensing EMS requires the hardware ID. Do one of the following:
   - If you have a registered license, click *Start Journey*.
   - If you do not have a registered license, click *Go to FortiCloud*. This opens the FortiCloud website, where you can register and license your EMS instance. See Licensing EMS by logging in to FortiCloud on page 15 for details on licensing EMS.
   - To try EMS on a temporary basis, click *Trial License* in the bottom left. This prompts you to enter your email address and password for trial license registration.
   - If you are using an air-gapped system or isolated network where EMS cannot access the Internet, click *Is this an airgapped system?* The wizard displays a page where you can manually upload a license file to activate EMS.

     You can obtain the license file in FortiCloud by selecting *Products > My Assets*, clicking the EMS serial number, and then *License File Download*.

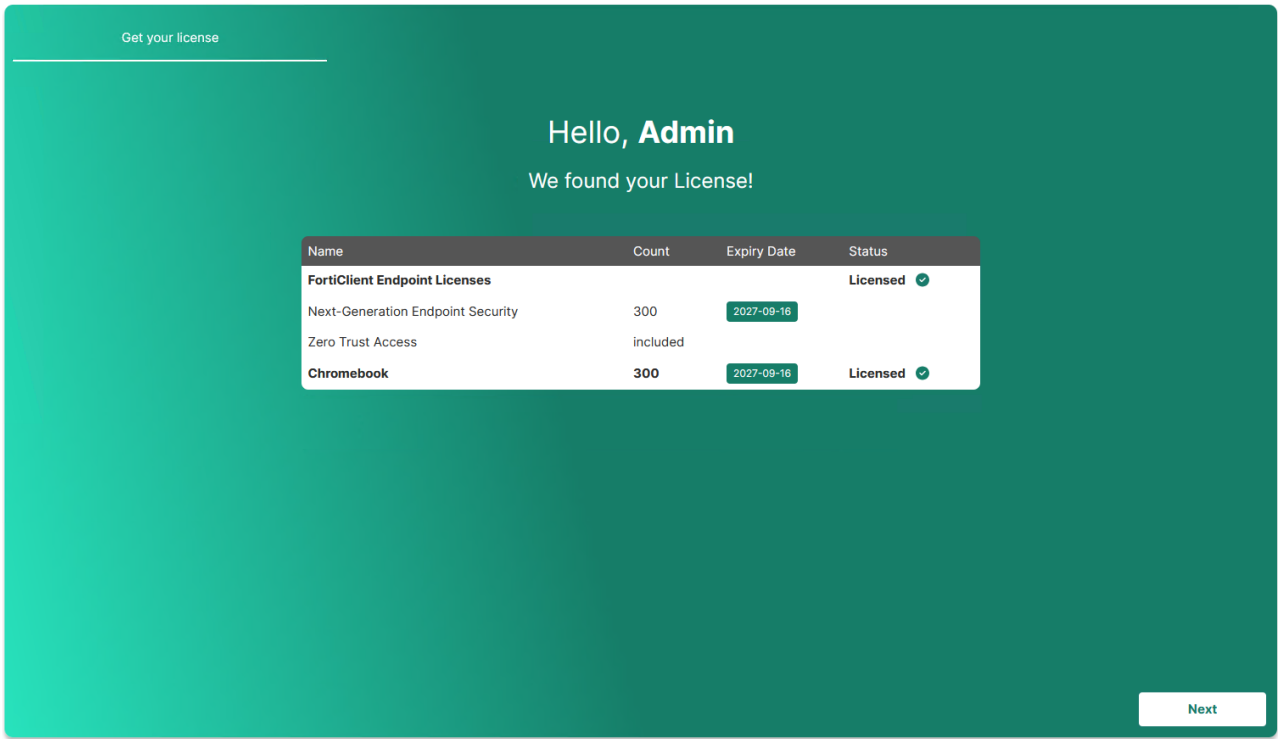


2. On the *Let's get you connected to your FortiCloud account* page, do one of the following, then click *Next*:
   - Enter your FortiCloud account credentials to retrieve your EMS license from FortiCloud.
   - Activate your EMS using FortiFlex licensing by enabling *Activate license through Flex-VM* and entering your FortiCloud account credentials and FortiFlex token.



If you enter incorrect credentials or do not have licensing registered to your account, the install wizard displays a page with *Reset password* and *Create new FortiCloud account* buttons. You can use these buttons to access FortiCloud for assistance.

3. EMS connects to FortiCloud to retrieve the license. The wizard displays the retrieved license type and entitlements and displays them. Click *Next*.



4. The wizard prompts you to enter a preferred hostname for the EMS server. If desired, configure a custom hostname, then click *Next*.
5. The wizard prompts you to enter a new admin username. Configure as desired, then click *Next*.
6. Configure a password for the new user. Click *Finish*. You can now access EMS with these credentials.

Configuring EMS after installation

You can configure a fully qualified domain name (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 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 requires 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 disconnected from 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*. Enter the desired FQDN.
3. If desired, enable Remote HTTPS Access.
4. If desired, in the *Custom Hostname* field, enter the hostname or IP address. Otherwise, EMS uses the *Pre-defined Hostname*.
5. If desired, select *Redirect HTTP request to HTTPS*. If this option is enabled, if you attempt to remotely access EMS at *http://<server_name>*, this automatically redirects to *https://<server_name>*.
6. 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.

Following is a summary of how to use FortiClient EMS:

1. Configure user accounts. See Configuring user accounts on page 25.
2. Create an endpoint profile. See Creating a new profile on page 26.
3. Add a FortiClient deployment package to EMS and configure it with the profile that you created in step 3. See Adding a FortiClient installer on page 26.
4. Deploy the FortiClient deployment package. See Deploying the FortiClient deployment package to endpoints on page 34.
   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.
5. View the endpoint status. See Viewing endpoints on page 34.

Configuring user accounts

You can configure Windows and LDAP users to have no access or administrator access to FortiClient EMS. You can also create a new user account in EMS.

EMS derives the Windows users from the host server that it is installed on. To add more Windows users, you must add them to the host server. EMS derives the list of LDAP users from those in the Active Directory (AD) domain imported into FortiClient EMS. If you want to add more LDAP users, they must already exist in the AD domain configured as the user server.

To configure Windows and LDAP user accounts:

1. Go to *Administration > Admin Users*.
2. Click *Add*.
3. Under *User source*, select *Choose from Windows users* or *Choose from LDAP*.
4. If you selected *Choose from LDAP*, select the desired server from the *Authentication Server* dropdown list. You must have already configured an authentication server.
5. Click *Next*.

6. Configure the user:

Option	Description
Username	(New user account only) enter the desired username.
User	(Windows/LDAP only) Select the user to configure permissions for.
Role	Select the desired admin role for this user.
Domain Access	Select or add access to a domain for the user. If desired, enable *Allow all domains* to allow this user access to all domains connected to EMS.
Restrict Login to Trusted Hosts	When this option is enabled, users can only log into this account from a trusted host machine. In the *Trusted Hosts* field, enter a trusted host machine's IP address. Use the + button to add multiple trusted host machines.
Comment	Enter optional comments/information for the Windows/LDAP user.

7. Click *Save*.

When an admin user from an AD domain logs into EMS, they must provide the domain name as part of their username to log in successfully. For example, if the domain name is "example-domain" and the username is "admin", the user must enter "example-domain/admin" when logging into EMS.

Creating a new profile

This section describes how to create a profile. You can use this profile to configure FortiClient software on endpoints by including it in an endpoint policy and deploying the policy to endpoints.

To create a profile to configure FortiClient:

1. Go to *Endpoint Profiles*.
2. Select the desired profile type.
3. Click the *Add* button.
4. Configure the settings as desired.
5. Click *Save* to save the profile.

Adding a FortiClient installer

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

You can create an installer or installer config file, or upload a packaged installer to add a FortiClient deployment package.

If *Sign Software Packages* 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.

To create an installer or install config file:

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

Option	Description
Online Installer Name	Enter the desired installer name.
Add Note	Click to add a note to the installer. In the *Notes* field, enter any details about the installer.
Release	Select the FortiClient release version to install.
Patch	Select the specific FortiClient patch version to install.
Build	Available if you select *This EMS has no internet connection*. Enter the FortiClient build number to install.
Hotfix	If a hotfix is available for the selected patch, the *Hotfix* dropdown list appears. See Adding a FortiClient hotfix installer.
Auto update to the	If a hot fix is not available for the selected patch, this field displays *Auto update to the Latest Patch*. Enable to repackage the installer to the latest patch release. If a hotfix is available for the selected patch, you can select several options. See Adding a FortiClient hotfix installer.
This EMS has no internet connection	Enable if you want to create an install config file.

4. Click *Next*. On the *Features* tab, set the following options. For features that are not available for all operating systems, the dialog displays the icons for the operating systems that the feature is available:

Available options may differ depending on the features you have enabled or disabled in *Feature Select*. See Feature Select.

Option	Description
Zero Trust Telemetry	Enabled by default and cannot be disabled. Installs FortiClient with Telemetry enabled.

Option	Description
Secure Access Architecture Components	Install FortiClient with SSL and IPsec VPN enabled. Disable to omit SSL and IPsec VPN support from the FortiClient deployment package. If you enable this feature for a deployment package and include a preconfigured VPN tunnel in the included endpoint profile, users who use this deployment package to install FortiClient can connect to this preconfigured VPN tunnel for three days after their initial FortiClient installation. This is useful for remote users, as it allows them to connect to the corporate network to activate their FortiClient license. If the user does not activate their FortiClient license within the three days, all FortiClient features, including VPN, stop working on their device.
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.
Malware	Enable any of the following features: • AntiVirus, Anti-Exploit, Removable Media Access • Anti-Ransomware • Cloud Based Malware Outbreak Detection Disable to exclude features from the FortiClient installer.
Web and Video Filtering	Enable any of the following features: • Web Filtering • Video Filtering Disable to exclude features from the FortiClient installer.
Application Firewall	Enable or disable Application Firewall in the FortiClient installer.
Single Sign-On Mobility Agent	Enable or disable single sign-on mobility agent in the FortiClient installer.
Zero Trust Network Access	Enable or disable zero trust network access (ZTNA) in the FortiClient installer. The ZTNA feature is always installed on a macOS endpoint, regardless of whether this option is enabled or disabled.

Option	Description
Privileged Access Agent	Enable or disable privileged access agent in the FortiClient installer.

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.

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

Option	Description
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.
Installer Files	Enable to include MSI installer files for FortiClient (Windows).
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.
Enable Endpoint VPN Profile	Select an endpoint VPN profile to include in the installer. EMS applies the VPN profile to the endpoint once it has installed FortiClient. This option is necessary if users require VPN connection to connect to EMS.
Enable Endpoint System Profile	Select an endpoint system profile to include in the installer. EMS applies the system profile to the endpoint once it has installed FortiClient. This option is necessary if it is required to have certain security features enabled prior to contact with EMS.
Invalid Certificate Action	Select the action to take when FortiClient attempts to connect to EMS with an invalid certificate: • **Warn**: warn the user about the invalid server certificate. Ask the user whether to proceed with connecting to EMS, or terminate the connection attempt. FortiClient remembers the user's decision for this EMS, but displays the warning prompt

Option	Description
	if FortiClient attempts to connect to another EMS (using a different EMS FQDN/IP address and certificate) with an invalid certificate. • **Allow**: allows FortiClient to connect to EMS with an invalid certificate. • **Deny**: block FortiClient from connecting to EMS with an invalid certificate.
Invitation	Select an invitation to include in the deployment package. If you have not created an invitation, you can create one by clicking *Create Invitation*. See Invitations.

6. Click *Next*. The *Telemetry* tab displays the hostname and IP address of the FortiClient EMS server, which manage FortiClient once it is installed on the endpoint.
7. Do one of the following:
   - If you selected *Create* installer, 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 (64-bit), .msi, .dmg, .rpm, and .deb files depending on the configuration. The end user can download these files to install FortiClient on their machine with the desired configuration.
   - If you selected *Create installer config* file, click *Download*. This downloads a config.json file to your device. You can upload this file to a cloud server to create a custom deployment package.

To upload packaged installers:

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

Option	Description
Online Installer Name	Enter the desired installer name.
Add Note	Click to add a note to the installer. In the *Notes* field, enter any details about the installer.
Release	Select *Upload packaged installer*.
Repackaged installer	Browse to and select the installer file.
This EMS has no internet connection	Enable.

4. Click *Next*. On the *Features* tab, set the following options. For features that are not available for all operating systems, the dialog displays the icons for the operating systems that the feature is available:

Available options may differ depending on the features you have enabled or disabled in *Feature Select*. See Feature Select.

Option	Description
Zero Trust Telemetry	Enabled by default and cannot be disabled. Installs FortiClient with Telemetry enabled.
Secure Access Architecture Components	Install FortiClient with SSL and IPsec VPN enabled. Disable to omit SSL and IPsec VPN support from the FortiClient deployment package. If you enable this feature for a deployment package and include a preconfigured VPN tunnel in the included endpoint profile, users who use this deployment package to install FortiClient can connect to this preconfigured VPN tunnel for three days after their initial FortiClient installation. This is useful for remote users, as it allows them to connect to the corporate network to activate their FortiClient license. If the user does not activate their FortiClient license within the three days, all FortiClient features, including VPN, stop working on their device.
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.
Malware	Enable any of the following features: • AntiVirus, Anti-Exploit, Removable Media Access • Anti-Ransomware • Cloud Based Malware Outbreak Detection Disable to exclude features from the FortiClient installer.
Web and Video Filtering	Enable any of the following features: • Web Filtering • Video Filtering Disable to exclude features from the FortiClient installer.
Application Firewall	Enable or disable Application Firewall in the FortiClient installer.

Option	Description
Single Sign-On Mobility Agent	Enable or disable single sign-on mobility agent in the FortiClient installer.
Zero Trust Network Access	Enable or disable zero trust network access (ZTNA) in the FortiClient installer. The ZTNA feature is always installed on a macOS endpoint, regardless of whether this option is enabled or disabled.
Privileged Access Agent	Enable or disable privileged access agent in the FortiClient installer.

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.

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

Option	Description
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.
Installer Files	Enable to include MSI installer files for FortiClient (Windows).
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.
Enable Endpoint VPN Profile	Select an endpoint VPN profile to include in the installer. EMS applies the VPN profile to the endpoint once it has installed FortiClient. This option is necessary if users require VPN connection to connect to EMS.

Option	Description
Enable Endpoint System Profile	Select an endpoint system profile to include in the installer. EMS applies the system profile to the endpoint once it has installed FortiClient. This option is necessary if it is required to have certain security features enabled prior to contact with EMS.
Invalid Certificate Action	Select the action to take when FortiClient attempts to connect to EMS with an invalid certificate: • **Warn**: warn the user about the invalid server certificate. Ask the user whether to proceed with connecting to EMS, or terminate the connection attempt. FortiClient remembers the user's decision for this EMS, but displays the warning prompt if FortiClient attempts to connect to another EMS (using a different EMS FQDN/IP address and certificate) with an invalid certificate. • **Allow**: allows FortiClient to connect to EMS with an invalid certificate. • **Deny**: block FortiClient from connecting to EMS with an invalid certificate.
Invitation	Select an invitation to include in the deployment package. If you have not created an invitation, you can create one by clicking *Create Invitation*. See Invitations.

6. Click *Next*. The *Telemetry* tab displays the hostname and IP address of the FortiClient EMS server, which manage FortiClient once it is installed on the endpoint.
7. Do one of the following:
   - If you selected *Create* installer, 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 (64-bit), .msi, .dmg, .rpm, and .deb files depending on the configuration. The end user can download these files to install FortiClient on their machine with the desired configuration.
   - If you selected *Create installer config* file, click *Download*. This downloads a config.json file to your device. You can upload this file to a cloud server to create a custom deployment package.

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

Installer Type	Select *Upload packaged installers*.

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.

Repacked installers	Upload a zip file that contains 64-bit Windows, macOS, and/or Linux 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, macOS, or Linux installation file. The installation files on the Fortinet Customer Service & Support and FortiClient.com websites are not available in .zip format. You must package the installer as a .zip file to upload it.

5. Click *Next*. The *Telemetry* tab displays the hostname and IP address of the FortiClient EMS server, which manage FortiClient once it is installed on the endpoint.
6. 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 (64-bit), .msi, .dmg, .rpm, or .deb files depending on the configuration. The end user can download these files to install FortiClient on their machine with the desired configuration.

Deploying the FortiClient deployment package to endpoints

To deploy the FortiClient deployment package to endpoints:

Deploy the FortiClient deployment package to desired endpoints using one of the following:

- SCCM: see Deploy applications with Configuration Manager.
- GPO: Use Group Policy to remotely install software.

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 in *Endpoints*.

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.

Option	Description
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: *Device*, *User*, *IP*, *Configurations*, *Connections*, and *Alerts and Events*.
Show/Hide Full Group Path	Click to hide or display the full path for the group that the endpoint belongs to.
Refresh	Click to refresh the list of endpoints.
Search All Fields	Enter a value and press *Enter* to search for the value in the list of endpoints.
Filters	Click to display and hide filters you can use to filter the list of endpoints.
Device	Visible when headings are displayed. Displays an icon to represent the OS on the endpoint, the hostname, and the endpoint group.
User	Visible when headings are displayed. Displays the name and icon of the user logged into the endpoint. Also displays the endpoint status: • **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. When using user-based licensing, you can use the dropdown list to view all registered users for this endpoint. The dropdown list displays the verified user and device username.
IP	Visible when headings are displayed. Displays the endpoint IP address.
Configurations	Visible when headings are displayed. Displays the name of the policy assigned to the endpoint and its synchronization status.

Option	Description
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.  For Web Filter events, only events of the *Block* and *Warn* categories are displayed here. Events of the *Allow* and *Monitor* categories are not displayed.

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: • Selected Vulnerabilities on Selected Clients • Selected Vulnerabilities on All Affected Clients • All Critical and High Vulnerabilities
Move to	Move the endpoint to a different group.

Action	Click to perform one of the following actions on the selected endpoint: • Request FortiClient Logs • Request Diagnostic Results • Update Signatures • Download Available FortiClient Logs • Download Available Diagnostic Results • Deregister • Quarantine • Un-quarantine • Exclude from Management • Revoke Client Certificate. This action is only available if the ZTNA or EPP license is applied and for endpoints running FortiClient 7.0.0 and later versions. Revoke the certificate that FortiClient is using to securely encrypt and tunnel TCP traffic through HTTPS to the FortiGate. You may want to revoke a certificate if it becomes compromised and can no longer be trusted. When a certificate is revoked, EMS prompts FortiOS and FortiClient with a new certificate signing request. • Clear Events • Mark as Uninstalled • Set Importance • Set Custom Tags. This option is only available if you have already created a custom tag. • Delete Stale Verified Users. This option deletes stale verified users and only keeps the last seen record for each machine user on an endpoint. For example, if two users onboarded on FortiClient on an endpoint, this option removes the user who onboarded earlier one. This option does not affect license seats. • Delete Device • Send Message. See Send endpoints one-way message 7.2.1.

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.
	Network Status	Displays the following information for the networks that the endpoint is connected to: • 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.
	Security Posture Tags	Displays which tags have been applied to the endpoint based on the security posture tagging rules.
	FortiGuard Outbreak Detections	Displays which FortiGuard Outbreak tags have been applied to the endpoint based on the FortiGuard Outbreak Alerts service rules.
	Connection	Displays the connection status between the selected endpoint and FortiClient EMS.

	Configuration	Displays the following information for the selected endpoint: • Policy: Endpoint policy 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. • FortiClient ID • ZTNA Serial Number: serial number for the zero trust network access certificate provisioned to the endpoint. • MDM Enrolled: whether the endpoint is enrolled on a mobile device management (MDM) platform. • MDM Deployment Status: whether a ZTNA certificate provisioned through MDM has been installed on the endpoint.
	Classification Tags	Displays classification tags that are 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 *Add* 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. You can assign a classification tag to multiple endpoints by selecting the endpoints, then selecting *Action > Set Importance* or *Set Custom Tags*. Tags that FortiClient EMS receives from FortiAnalyzer also display under *Classification Tags*. Configuring a maximum of eight custom tags is recommended. Configuring more than eight custom tags may result in performance or management issues.
	Classification Tags - Fabric	Displays Fabric classification tags that are currently assigned to the endpoint. In a Fabric deployment, FortiEDR can detect suspicious or compromised endpoint behavior, share that endpoint's security status with EMS, and tag the affected endpoint on EMS. You can view these tags under *Classification Tags - Fabric*. You can also unassign a tag from the endpoint. The following lists the predefined tags for FortiEDR use: • **FortiEDR_Malicious**: FortiEDR has classified this endpoint as malicious. • **FortiEDR_PUP**: FortiEDR has detected a potentially

		unwanted program on this endpoint. • **FortiEDR_Suspicious**: FortiEDR has detected suspicious activity on this endpoint. • **FortiEDR_Likely_Safe**: FortiEDR has detected this endpoint as likely to be safe. • **FortiEDR_Probably_Good**: FortiEDR has determined that this endpoint is not a safety risk. See Identity Management integration.

	Forensic Analysis	Displays statuses for forensic analysis tasks:
		• **Ticket Status**: status of the ticket. Possible statuses are:
		  • **Request Submitted**
		  • **Pending**: Forensic analysis request has been initiated. The Forensics team has not yet assigned it to an analyst.
		  • **Running**
		  • **In Progress**: Forensics team has assigned the request to an analyst, who has begun working on it.
		  • **Failed**: analyst could not connect to the endpoint.
		  • **Cancelled**: indicates one of the following:
		  • The analyst needed more information about the endpoint to perform the analysis.
		  • The EMS administrator canceled the request.
		  • **Completed**: analyst has completed analysis on the endpoint and shared the result in a PDF document. You can download the report from the endpoint summary's *Forensic Analysis* section.
		• **Agent Status**: status of the forensic agent collecting logs on the endpoint. Possible statuses are:
		  • **Pending**: EMS has notified FortiClient that a forensic analysis request is submitted, but the forensic agent is not running yet.
		  • **Running**: forensics agent starts collecting forensics logs.
		  • **Collection Completed**: forensics agent has completed collecting forensics logs.
		  • **Upload Started**: FortiClient has started to upload the logs to the cloud.
		  • **Upload Completed**: FortiClient has completed uploading the logs to the cloud.
		  • **Upload Failed**: FortiClient failed to upload the logs to the cloud.
		• **Verdict**: forensic analysis verdict as determined by the FortiGuard analyst.
		• **Task ID**: Request ID in the FortiGuard forensics system.
		• **Request Analysis**: request forensic analysis on the

		endpoint. See Requesting forensic analysis on an endpoint. • **Download Report**: download the forensic analysis report.
	Status	Displays one of the following statuses: • Managed: Endpoint is managed by EMS. • Quarantined: If quarantined, displays access code. The user can enter this access code in the affected endpoint's FortiClient to remove the endpoint from quarantine. • Excluded: Endpoint is excluded from management by EMS.
	Features	Displays which features are enabled for FortiClient.
	Third Party Features	Displays which third party features are installed and running on the endpoint. This section includes the status of FortiEDR on the endpoint. This information is only available for Windows endpoints.
Antivirus Events		
	Date	Displays the AV event's date and time.
	Count	Displays the number of occurrences for this event.
	Message	Displays the AV event's message.
	Actions	Mark the event as read or delete it.
Cloud Scan Events		
	Date	Displays the cloud-based malware detection event's date and time.
	Count	Displays the number of occurrences for this event.
	Message	Displays the cloud-based malware detection event's message.
	Actions	Mark the event as read or delete it.
Anti-Ransomware Events		
	Date	Displays the anti-ransomware event's date and time.
	Count	Displays the number of occurrences for this event.
	Message	Displays the anti-ransomware event's message. The message may say that FortiClient detected ransomware on the endpoint, or that FortiClient restored a file that the detected ransomware encrypted.
	Actions	Mark the event as read or delete it.
AntiExploit Events		
	Date	Displays the AntiExploit event's date and time.
	Count	Displays the number of occurrences for this event.

	Message	Displays the AntiExploit event's message.
	Actions	Mark the event as read or delete it.
USB Device Events		
	Date	Displays the USB device event's date and time.
	Count	Displays the number of occurrences for this event.
	Message	Displays the USB device event's message.
	Actions	Mark the event as read or delete it.
Sandbox Events		
	Date	Displays the sandbox event's date and time.
	Message	Displays the sandbox event's message.
	Rating	Displays the file's risk rating as retrieved from FortiSandbox.
	Checksum	Displays the checksum for the file.
	Download	Download a PDF version of the detailed report.
	Magnifying glass	Click to view a more detailed report.
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.
Videofilter Events		
	Date	Displays the video filter event's date and time.
	Count	Displays the number of occurrences for this event.
	Message	Displays the video filter event's message.
	Actions	Mark the event as read or delete it.
Vulnerability Events		

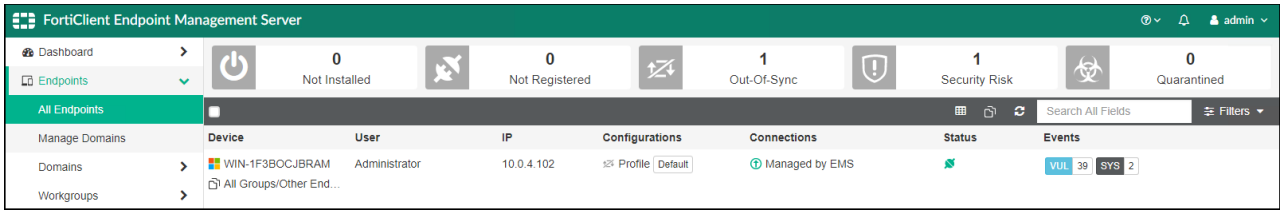
	Vulnerability	Displays the vulnerability's name. For example, *Security update available for Adobe Reader*.
	Category	Displays the vulnerability's category. For example, *Third Party App*.
	Application	Displays the name of the application with the vulnerability.
	Detected Paths	Path where FortiClient detected the vulnerability.
	Severity	Displays the vulnerability's severity.
	Patch Type	Displays the patch type for this vulnerability: *Auto* or *Manual*.
	FortiGuard	Displays the FortiGuard ID number. If you click the FortiGuard ID number, it redirects you to FortiGuard where further information is provided if available.
PUA Events		
	Name	Displays the potentially unwanted application (PUA) name.
	Vendor	Displays the PUA vendor name.
	Version	Displays the PUA version number.
	Category	Displays the PUA category that the application belongs to. PUA categories are as follows: • Illegal or unethical • Cryptomining • Hacking • Unpopular • Phishing • Malicious
	Date	Displays the date that EMS detected the PUA. This column is available in *Events* view.
	Event Type	Displays the event type, such as *Detected* (EMS detected the PUA) or *Uninstalled* (the PUA was uninstalled from the endpoint). This column is available in *Events* view.
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 34.

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 62.
2. Add the Google domain. See Adding a Google domain on page 64.
3. Create an endpoint profile. See Adding a new Chromebook profile on page 64.
4. Create an endpoint policy configured with the endpoint profile. See Adding a Chromebook policy on page 66.
5. View the status. See Viewing domains on page 67.

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.

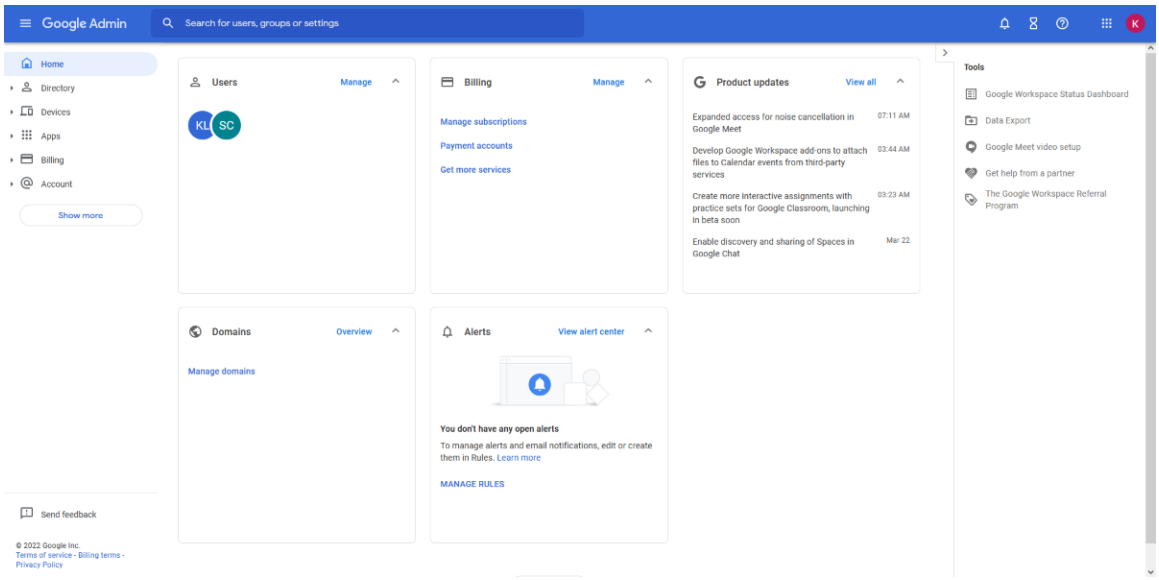
Following is a summary of how to set up the Google Admin console:

1. Log into the Google Admin console. See Logging into the Google Admin console on page 46.
2. Add the FortiClient Web Filter extension. See Adding the FortiClient Web Filter extension on page 46.
3. Configure the FortiClient Web Filter extension. See Configuring the FortiClient Web Filter extension on page 47.
4. Add the root certificate. See Adding root certificates on page 48.
5. Disable access to Chrome developer tools.
6. Disallow incognito mode.
7. Disallow guest mode.
8. Block Chrome task manager.
9. Verify the FortiClient Web Filter extension.

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

Logging into the Google Admin console

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



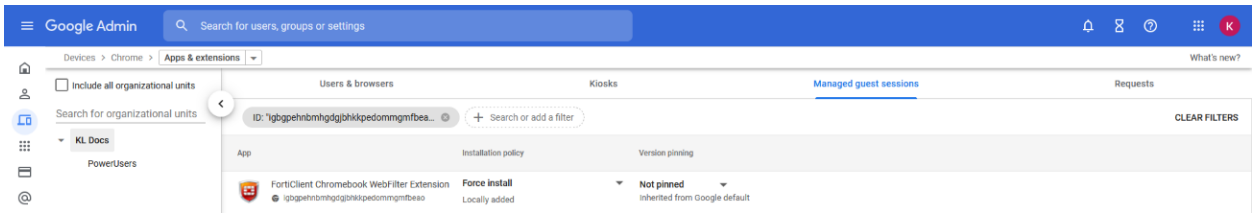
Adding the FortiClient Web Filter extension

FortiClient EMS software is unavailable for public use. You can only enable the feature using the following extension ID: igbgpehnbmhgdgjbhkkpedommgmfbeao

To add the FortiClient Web Filter extension:

1. In the Google Admin console, go to *Devices > Chrome > Settings > Users & browsers > Managed Guest Session Settings*.
2. On the left, select the organization that contains the desired users or enrolled browsers. To select all users and browsers, select the top-level organization. Otherwise, select a child.
3. From the breadcrumbs, select the dropdown list beside *Settings*, and select *Apps & extensions*.
4. In the bottom right corner, hover over the + icon, then select *Add Chrome app or extension by ID*.
5. In the *Extension ID* field, enter the following extension ID: igbgpehnbmhgdgjbhkkpedommgmfbeao.

6. Click *SAVE*. The extension displays, with the Force install installation policy.



Configuring the FortiClient Web Filter extension

You must configure the FortiClient Chromebook Web Filter extension to enable the Google Admin console to communicate with FortiClient EMS.

FortiClient EMS hosts the services that assign endpoint profiles of web filtering policies to groups in the Google domain. FortiClient EMS also handles the logs and web access statistics that the FortiClient Web Filter extensions send.

FortiClient EMS is the profile server.

For instructions on configuring the extension for connection to FortiClient Cloud, see Managing Chromebooks with FortiClient Cloud.

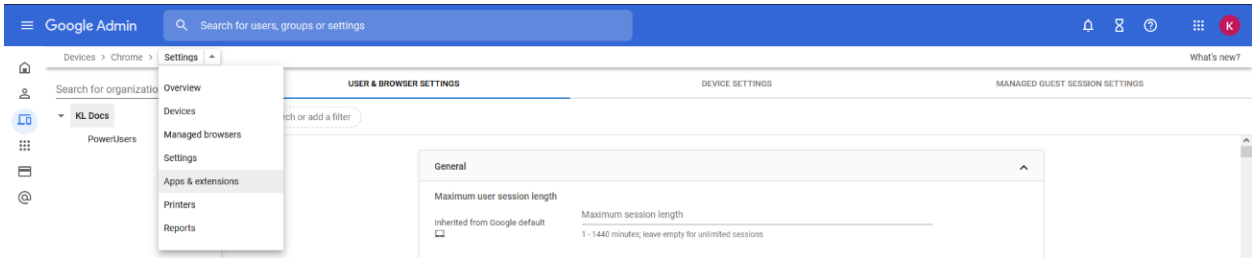
To configure the FortiClient Web Filter extension:

1. In FortiClient EMS, locate the server name and port by going to *System Settings > EMS Settings*.
2. Create a text file that contains either set of the following text, depending on your deployment mode:

Deployment Mode	Text	Example
Regular	{ "ProfileServerUrl": { "Value": "https://< ProfileServer >:< port for Profile Server >"} }	{ "ProfileServerUrl": { "Value": "https://ems.mydomain.com:8443"} }
Multi-tenancy	{ "ProfileServerUrl": { "Value": "https://< ProfileServer >:< port for Profile Server >"} }, "SiteName": {	{ "ProfileServerUrl": { "Value": "https://ems.mydomain.com:8443"} }, "SiteName": { "Value": "Site1"} }

Deployment Mode	Text	Example
	"Value": "SiteName"} }	

3. In the Google Admin console, go to *Devices* > *Chrome* > *Settings* > *Users & browsers*.
4. On the left, select the organization that contains the desired users or enrolled browsers. To select all users and browsers, select the top-level organization. Otherwise, select a child.
5. From the breadcrumbs, select the dropdown list beside *Settings*, and select *Apps & extensions*.



6. Click a domain or organizational unit (OU), then click the FortiClient Web Filter extension.
7. In the right pane, under *Policy for extensions*, paste the JSON content from step 2.
8. Click *SAVE*.
9. Go to *Devices* > *Chrome* > *Apps & extensions* to view your configured Chrome applications.

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.

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 50.

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. You can add FortiClient EMS as a device to the FortiClient or Fabric 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 50.

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

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

In FortiAnalyzer CLI, enter the following command:

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

Adding an SSL certificate to FortiAnalyzer

To add an SSL certificate to FortiAnalyzer:

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

Selecting a certificate for HTTPS connections

To select a certificate for HTTPS connections:

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

Summary of where to add certificates

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

Scenario	Certificate and CA	Where to add certificates
Allow the FortiClient Chromebook Web Filter extension to trust EMS	Public SSL certificate	Add SSL certificate to FortiClient EMS.
	SSL certificate not from a common CA	• 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 upload root certificates to the Google Admin console:

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

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

Disabling access to Chrome developer tools

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

To disable access to Chrome developer tools:

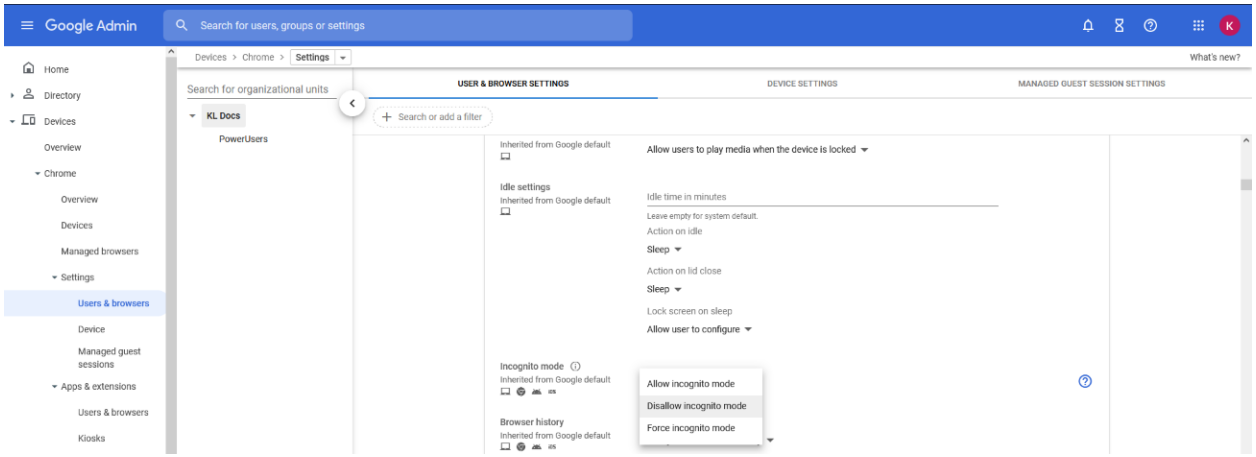
1. In the Google Admin console, go to *Devices > Chrome > Settings > Users & browsers*.
2. On the left, select the organization that contains the desired users or enrolled browsers. To select all users and browsers, select the top-level organization. Otherwise, select a child.
3. In *User & Browser Settings*,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

Disallowing incognito mode

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

To disallow incognito mode:

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



4. Click *Save*.

Disabling guest mode

You should disallow guest mode for managed Google domains.

To disallow guest mode:

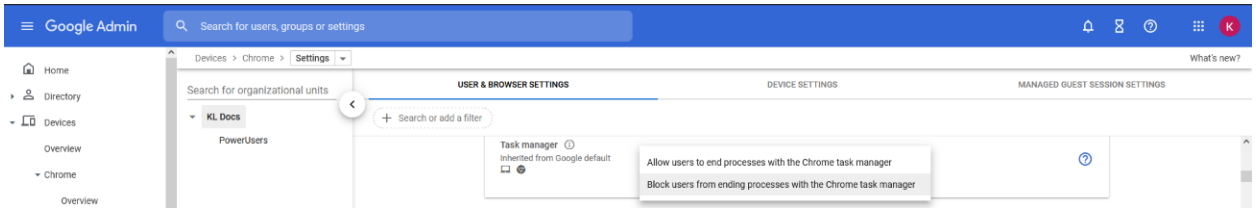
1. In the Google Admin console, go to *Devices > Chrome > Settings > Device*.
2. On the left, select the organization that contains the desired users or enrolled browsers. To select all users and browsers, select the top-level organization. Otherwise, select a child.
3. Under *Sign-in settings*, for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

Blocking the Chrome task manager

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

To block the Chrome task manager:

1. In the Google Admin console, go to *Devices > Chrome > Settings > Users & browsers*.
2. On the left, select the organization that contains the desired users or enrolled browsers. To select all users and browsers, select the top-level organization. Otherwise, select a child.
3. In *User & Browser Settings*, under *Task manager* select *Block users from ending processes with the Chrome task manager* from the dropdown list.



4. Click *Save*.

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

Option	Default setting	Where used
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 Delegating domain-wide authority to the service account on page 60.

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 53.
2. Add the unique service account credentials to the Google Admin console. See Delegating domain-wide authority to the service account on page 60.
3. Add the unique service account credentials to FortiClient EMS. See Adding service account credentials to EMS on page 62.

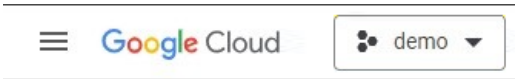
Creating unique service account credentials

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

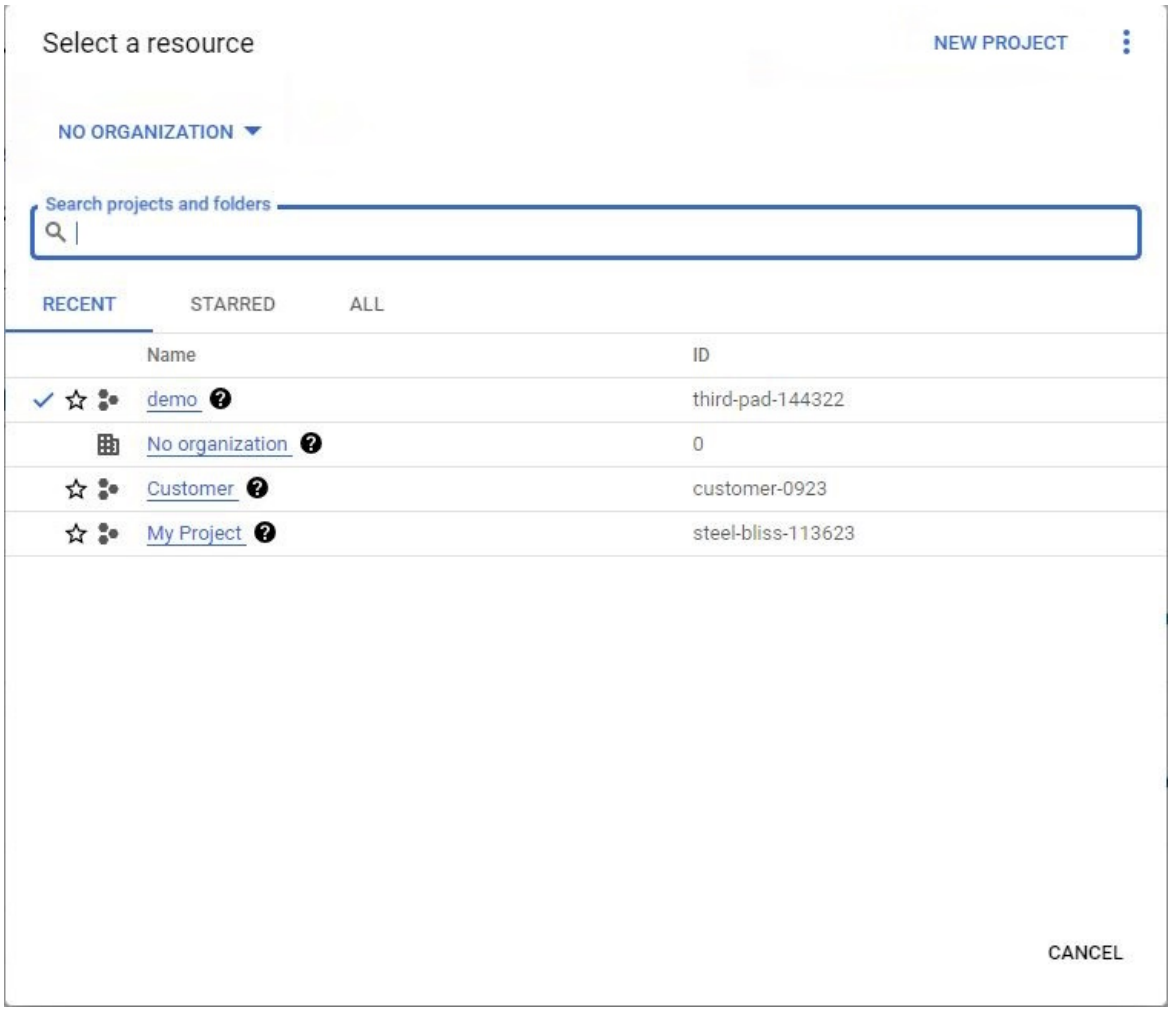
- Client ID (a long number)
- Service account ID (email address)
- Service account certificate (a certificate in `.pem` format)

To create unique service account credentials:

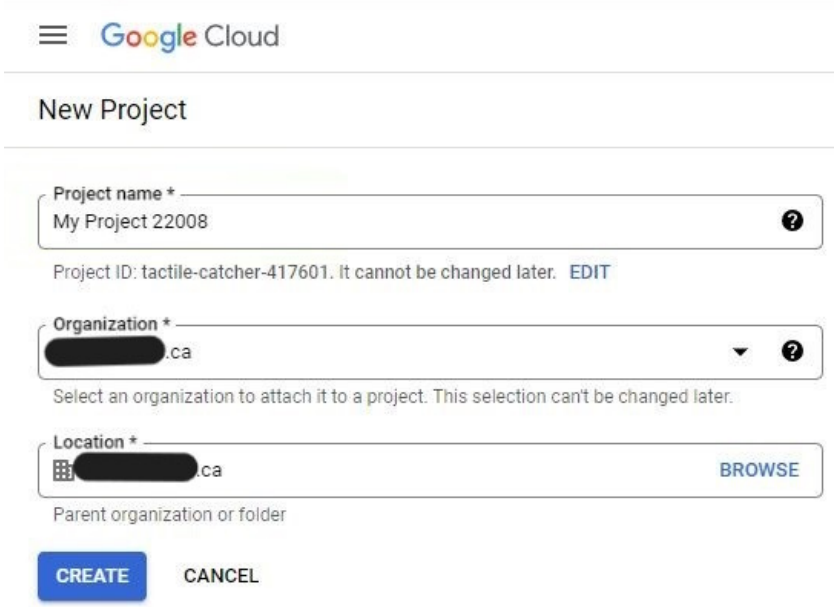
1. Go to Google API Console.
2. Log in with your Google Workspace account credentials.
3. Create a new project:
   a. Click the toolbar list. The browser displays the following dialog.



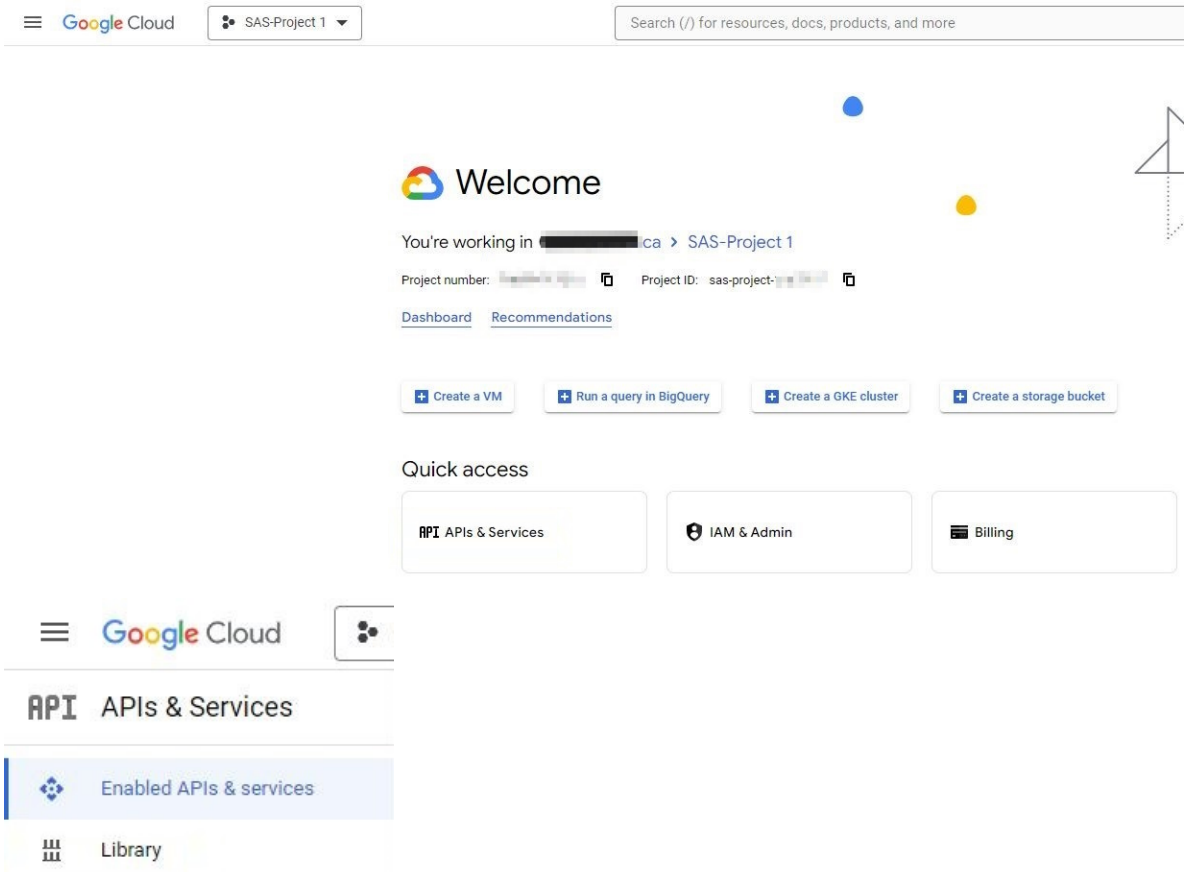
b. Select your organization, if you see an organization dropdown list. Click *New Project*.



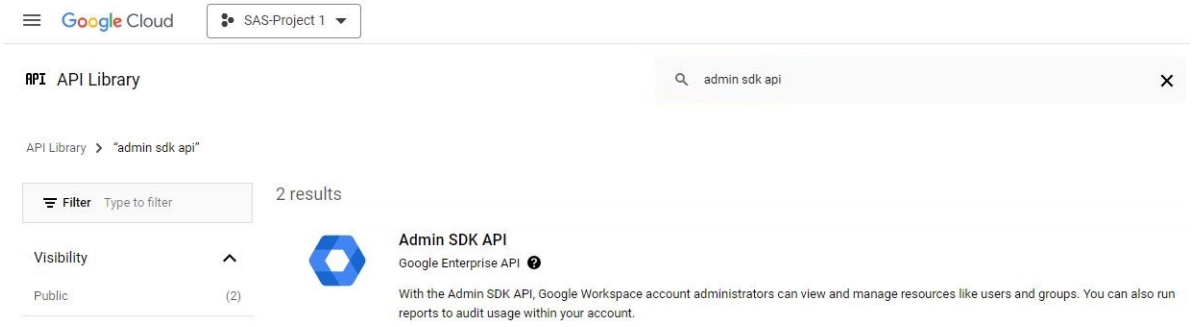
c. In the *Project name* field, enter your project name, then click *Create*.

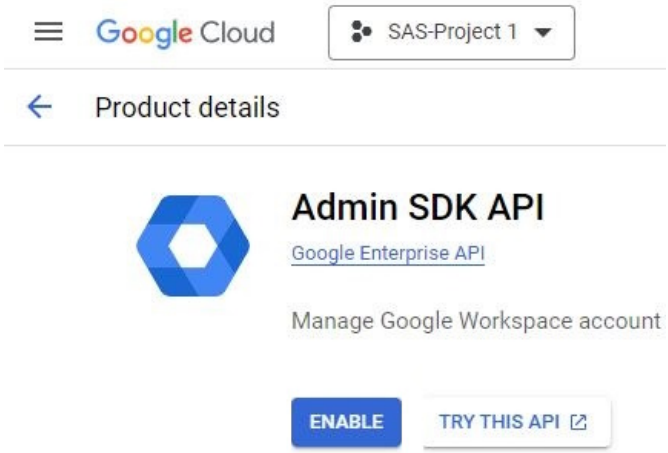


4. Enable the Admin SDK:
   a. Select your project from the toolbar list, then click *APIs & Services*.

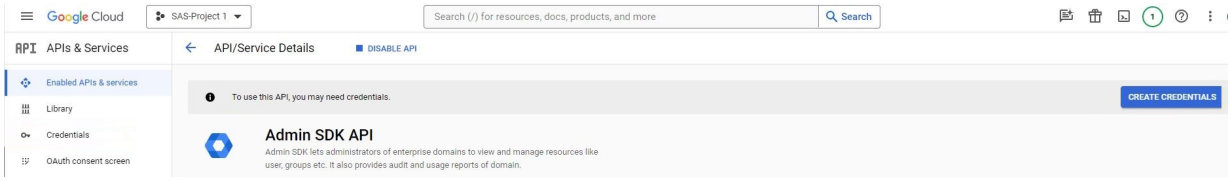


   b. Under *Google Workspace APIs*, search for *Admin SDK API* and enable it.

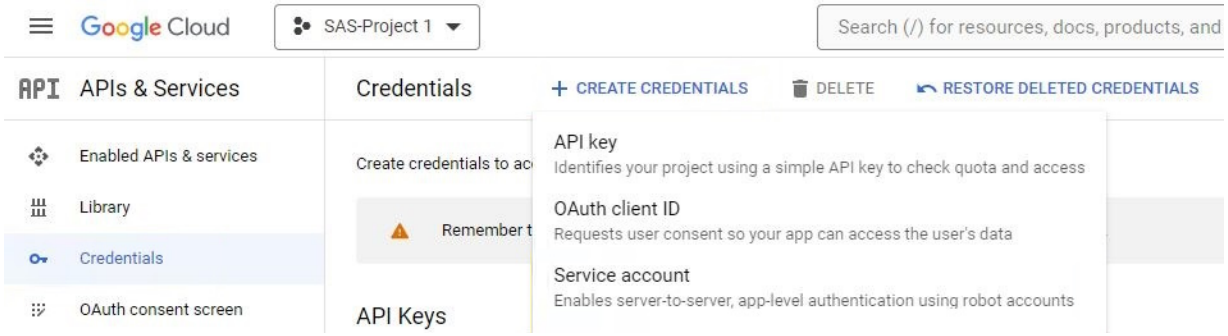




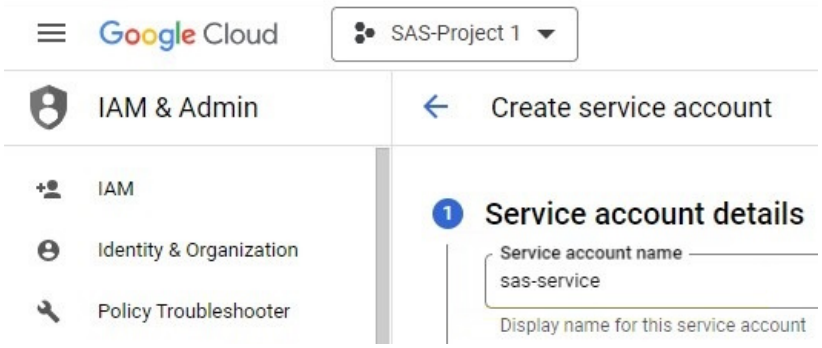
After enabling the Admin SDK API, the console displays a message indicating: *To use this API, you may need credentials*.



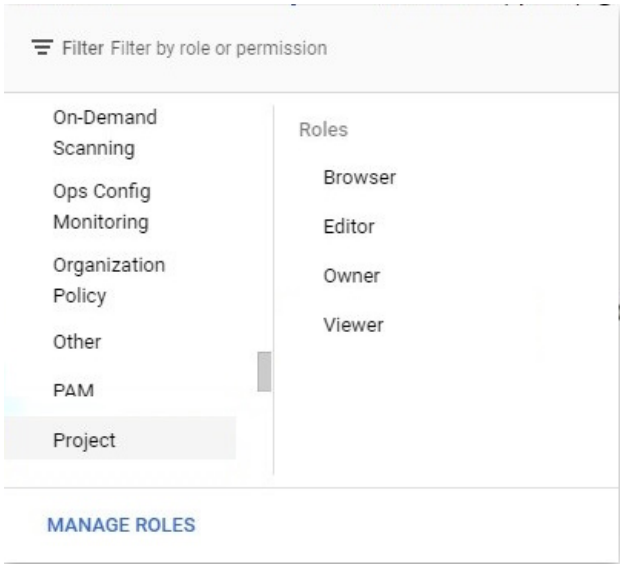
5. Create a service account:
   a. Go to the *Credentials* tab and select *Create Credentials* > *Service account*.



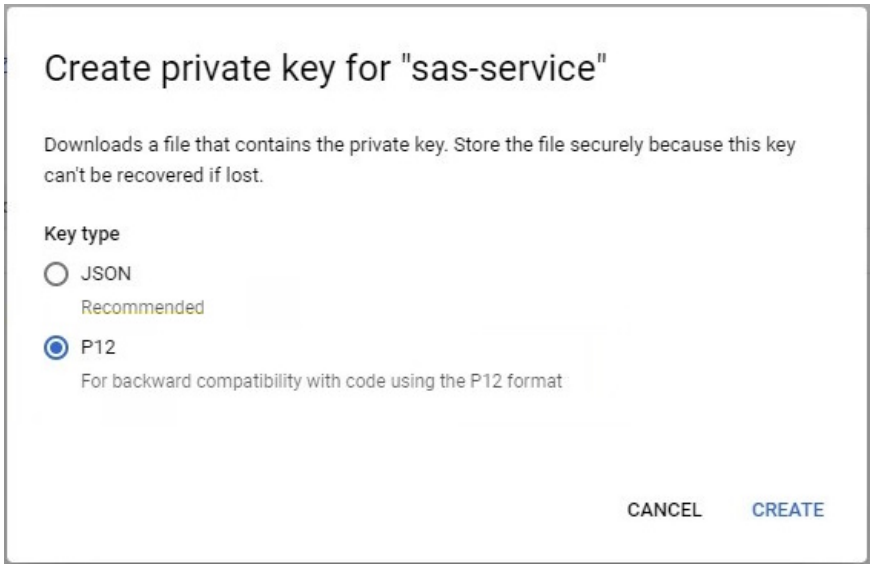
   b. From the *Service account* list, select *New Service Account*. Enter a service account name.



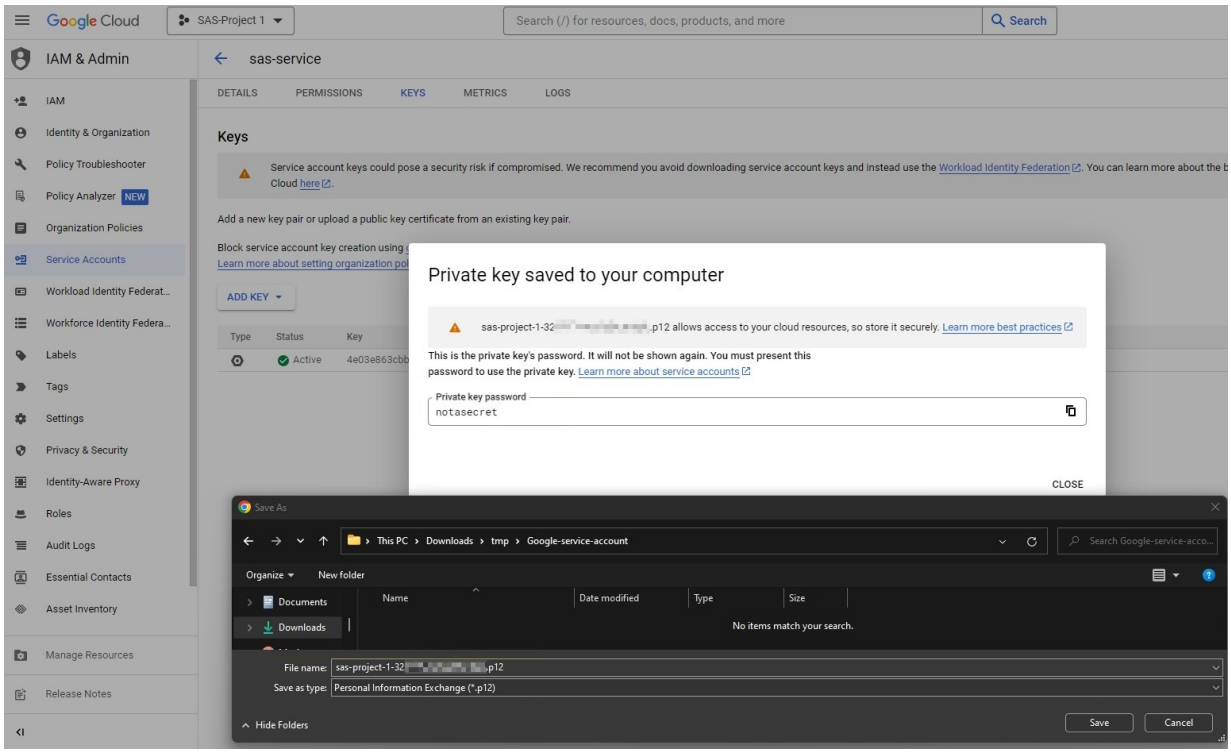
c. From the *Role* list, select *Project > Viewer*.



d. Edit the created service account and go to *Keys*. Click *Add Key* to create a P12 private key.

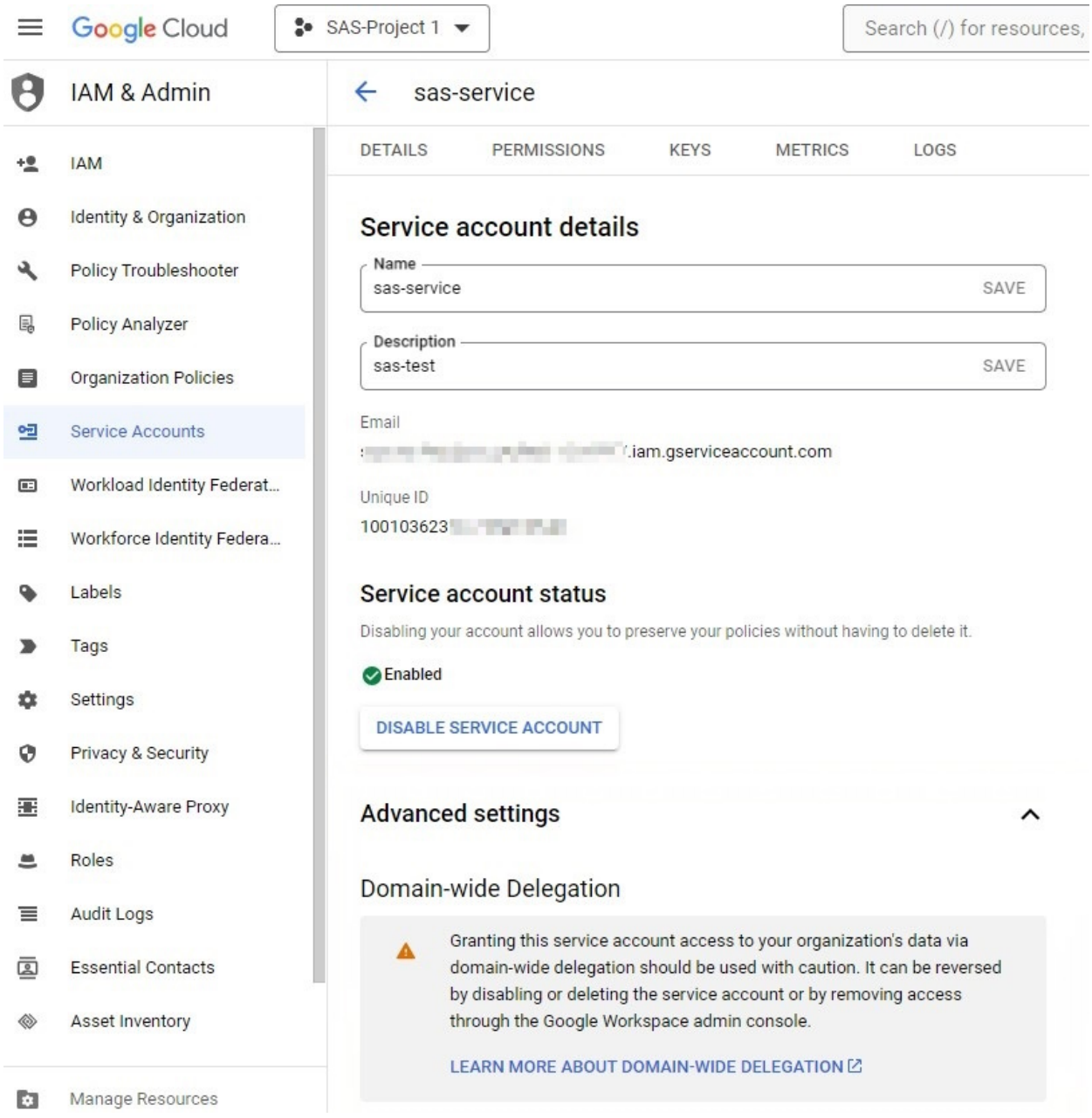


e. Save the private key and note the private key password, "notasecret".



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**.

6. *Edit* the service account you just created and expand *Advanced settings*. There is a *Domain-wide Delegation* message and step-by-step guide.



To use the private key in EMS, you must convert it to `.pem` format. You can use the following `openssl` command to convert it. Remember to use the notasecret password.

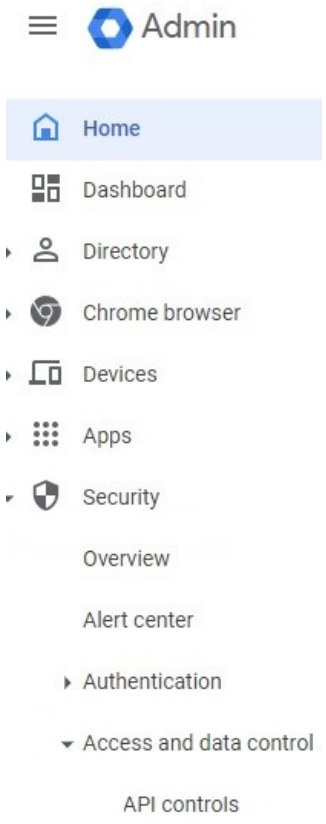
```
C:\OpenSSL-Win64\bin>openssl pkcs12 -in demo-976b9d6e9328.p12 -out
      serviceAccount-demo.pem -nodes -nocerts
Enter Import Password:
```

Delegating domain-wide authority to the service account

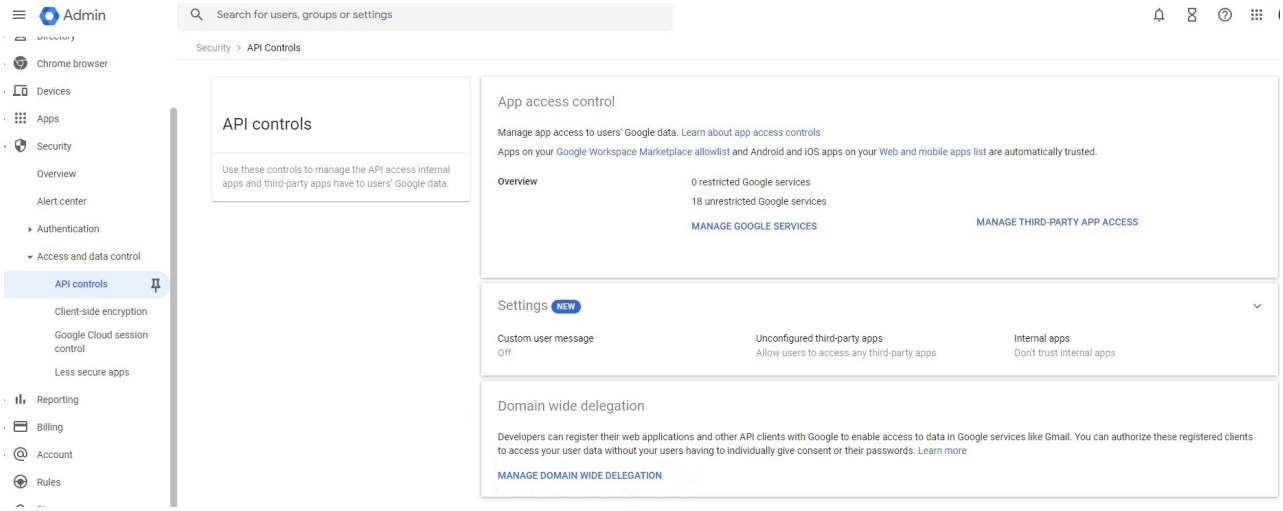
This section describes how to delegate domain-wide authority to the service account in the Google Admin console. These settings allow Google to trust FortiClient EMS, which enables FortiClient EMS to retrieve information from the Google domain.

To delegate domain-wide authority to the service account:

1. In the Google Admin console, go to *Menu* > *Security* > *Access and data control* > *API controls*.



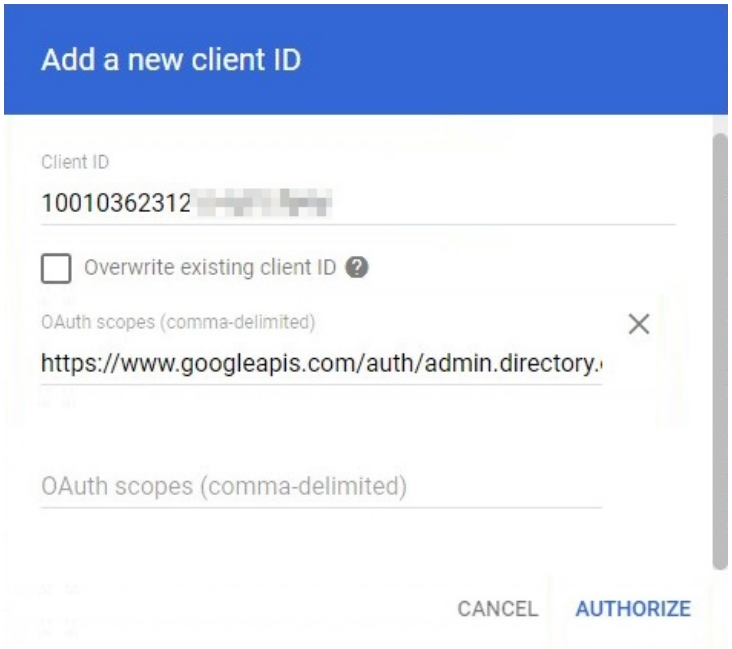
2. Click *Manage Domain Wide Delegation*, then click *Add New*.



3. Set the following options:
   a. In the *Client ID* field, add the client ID from the service account credentials.
   b. In the *OAuth Scopes* field, add the following string:
   https://www.googleapis.com/auth/admin.directory.orgunit.readonly,https://www.googleapis.com/auth/admin.directory.user.readonly

   The API scopes are case-sensitive and must be lowercase. You may need to copy the string into a text editor and remove spaces created by words wrapping to the second line in the PDF.

   c. Click *Authorize*.



Adding service account credentials to EMS

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

To add service account credentials to EMS:

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

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

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

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

4. Click *Save*.

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 48
- Communication with FortiAnalyzer for logging on page 48

It includes the following procedures:

- Required: Adding an SSL certificate to FortiClient EMS for Chromebook endpoints on page 63
- Required only when sending logs to FortiAnalyzer: Adding SSL certificates to FortiAnalyzer on page 63

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.

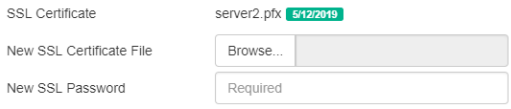
If you are using a public SSL certificate, add the certificate to FortiClient EMS. You do not need to add the certificate to the Google Admin console.

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 48.

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.



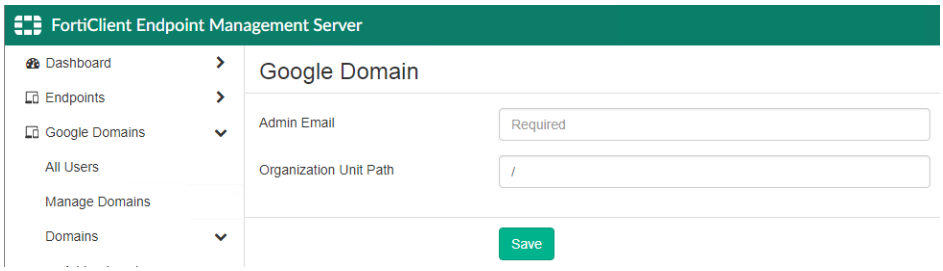
Adding SSL certificates to FortiAnalyzer

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 enable Chromebook management on EMS, EMS creates default Web Filter and System Settings profiles for Chromebooks. By default, EMS includes these profiles in the default Chromebook policy, which it applies to any Google domains you add to FortiClient EMS.

You can add new Chromebook profiles to deploy different settings to Chomebook endpoints.

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

To add a new profile:

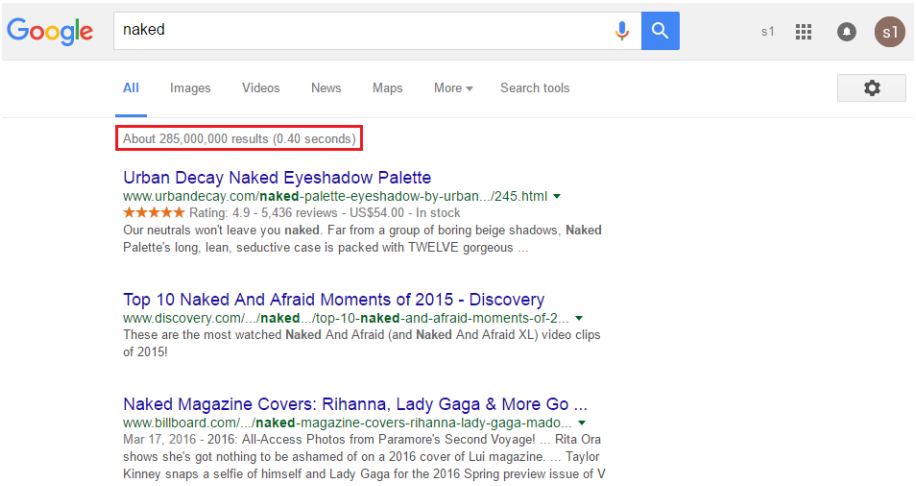
1. Go to *Endpoint Profiles*.
2. Go to *Web Filter* or *System Settings*.
3. Click *Add*, then click *Add Chrome Profile*.
4. Configure the profile as desired.
5. Click *Save*.

Enabling and disabling Safe Search

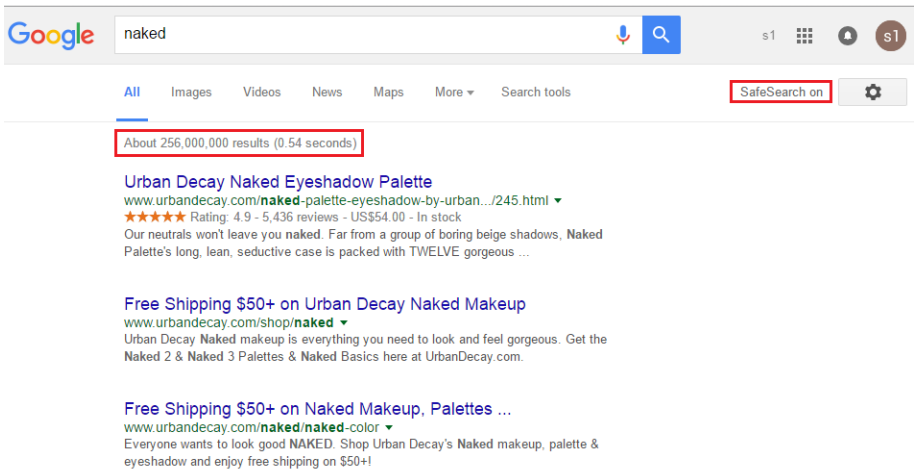
The search engine provides a Safe Search feature that blocks inappropriate or explicit images from search results. The Safe Search feature helps avoid most adult content. FortiClient EMS supports Safe Search for most common search engines, such as Google, Yahoo, and Bing.

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*.

You can enable Safe Search on the Video Filter and Web Filter profiles. When Safe Search is enabled on both profiles, the more restrictive settings are applied to YouTube

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 64.
Comments	Enter any comments desired for the endpoint policy.
Enable the policy	Toggle to enable or disable the endpoint policy. You can enable or disable the policy at a later time from *Endpoint Policy & Components Manage Policies*.

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

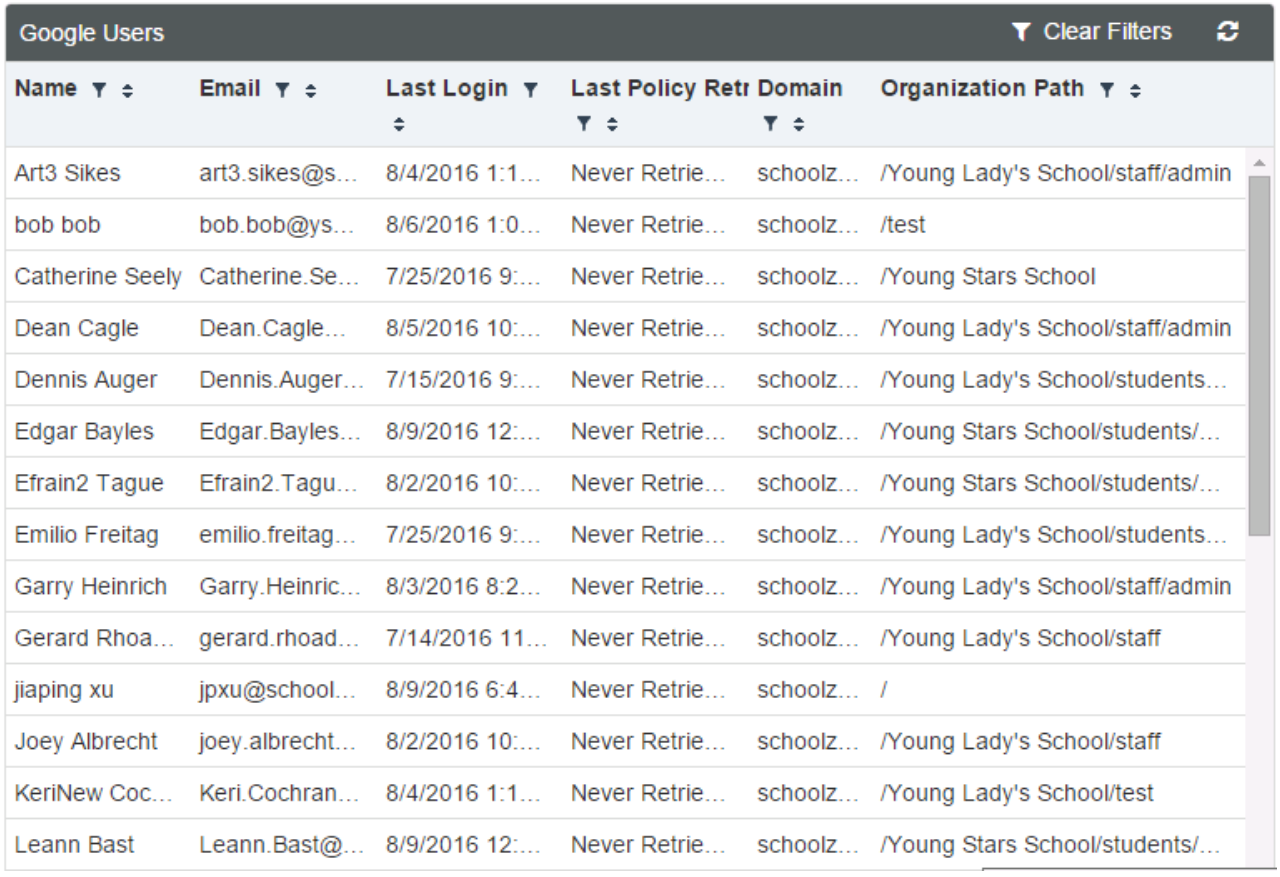
After you add domains to FortiClient EMS, you can view the list of domains in *Google Domains*. You can also view the list of Google users in each domain and details about each Google user in the *User Details*, *Client Statistics*, and *Blocked Sites* panes.

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.



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

Blocked Sites (Past <number> Days)

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

Change log

Date	Change description
2025-03-20	Initial release.
2025-04-22	Updated Viewing endpoints on page 34.
2025-06-05	Updated Viewing the Endpoints pane on page 34.
2025-06-19	Updated: • Required services and ports on page 6
2025-06-30	Updated Viewing the Endpoints pane on page 34.
2025-08-08	Updated Configuring the FortiClient Web Filter extension on page 47.
2025-08-20	Updated Starting FortiClient EMS and logging in on page 20.
2025-08-27	Updated Viewing the Endpoints pane on page 34.

www.fortinet.com