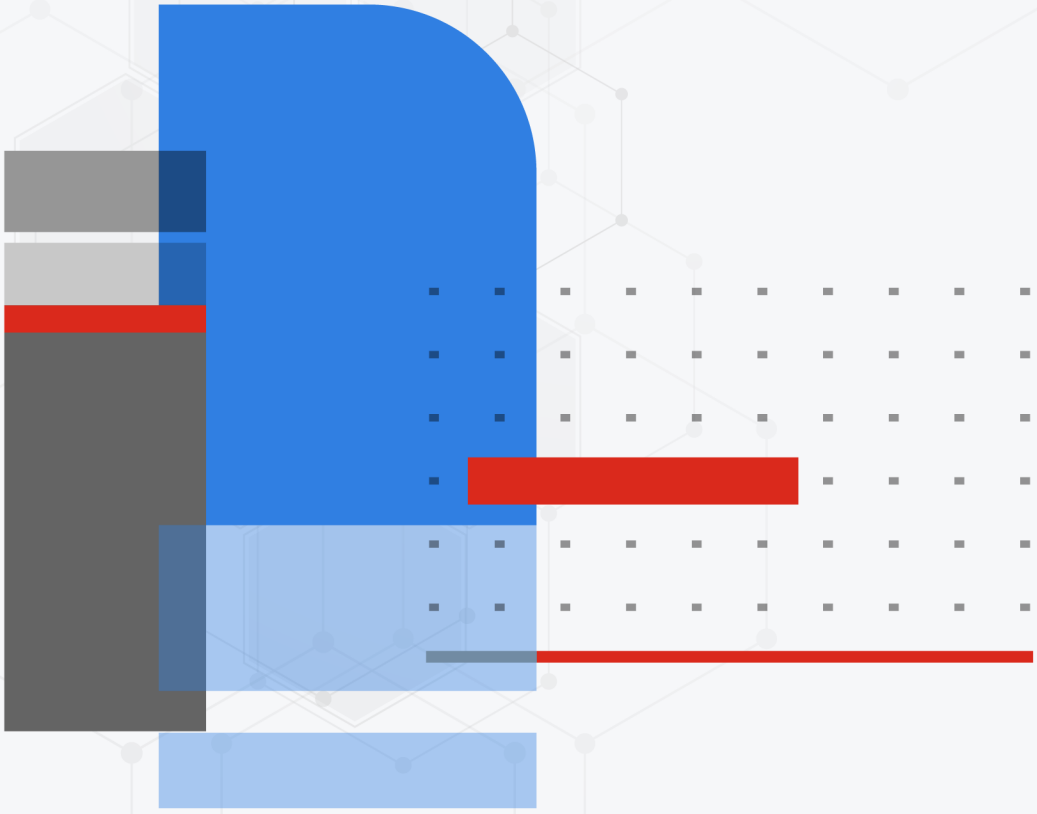
# QuickStart Guide

## FortiClient EMS 7.4.6



**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

March 17, 2026
FortiClient EMS 7.4.6 QuickStart Guide
04-746-1010850-20260317

# 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 the following Linux distributions:

- Ubuntu 22.04 or 24.04 LTS Server and Desktop
- Red Hat Enterprise Linux 9
- CentOS Stream 9

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

Because implementing or migrating to EMS 7.4 on Linux can be complex, Fortinet highly recommends the FortiClient Best Practices Service (BPS).

FortiClient BPS is an account-based annual subscription providing access to a specialized team that delivers remote guidance on deployment, upgrades, and operations. The service allows you to share information about your deployment, user requirements, resources, and other related items. Based on the information provided, BPS experts can provide recommended best practices, sample code, links to tools, and other materials or assistance to speed adoption and guide you towards best practice deployments. The team does not log into your devices to make changes. 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.<br>This feature also requires port 443.<br>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. | TCP | 443 | Incoming | Installer |

| Communication | Usage | Protocol | Port | Incoming or outgoing | How to customize |
|---|---|---|---|---|---|
| | Also required for the ACME feature. | | | | |
| 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 Telemetry | FortiClient endpoint management | TCP | 8013 (default) | Incoming | Installer/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 |

# Chromebooks management

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

| Communication | Usage | Protocol | Port | Incoming/Outgoing | How to customize |
|---|---|---|---|---|---|
| FortiClient on Chrome OS | Connecting to FortiClient EMS | TCP | 8443 (default)<br>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 |

When using FortiClient for Chromebooks, you should enable the following ports and services for use on Chromebooks:

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

# EMS installer creation

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 installation

Access to the following destination addresses are required for EMS installation:

- `*.archive.ubuntu.com`
- `*.canonical.com`
- `*.cdn.snapcraftcontent.com`
- `*.forticloud.com`
- `*.fortinet.com`

- *.fortinet.net
- *.fwupd.org
- *.launchpad.net
- *.launchpadcontent.net
- *.packages.redis.io
- *.postgresql.org
- *.pypi.org
- *.python.org
- *.pythonhosted.org
- *.redis.io
- *.snapcraft.io
- *.ubuntu.com
- *.winehq.org

# FortiGuard

EMS connects to FortiGuard to download AV and vulnerability scan engine and signature updates and FortiClient and EMS installer downloads. FortiClient EMS can connect to legacy FortiGuard or FortiGuard Anycast.

The following table summarizes required services for FortiClient EMS to communicate with FortiGuard:

| Usage | Server URL | | | Protocol | Port | Incoming/Outgoing | How to customize |
|---|---|---|---|---|---|---|---|
| | Global | U.S. | Europe | | | | |
| AV/vulnerability signature update and FortiClient installer downloads | forticlient.fortinet.net<br>myforticlient.fortinet.net | usforticlient.fortinet.net | N/A | TCP | 80 | Outgoing | N/A |

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

# FortiClient Cloud Sandbox (SaaS)

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):

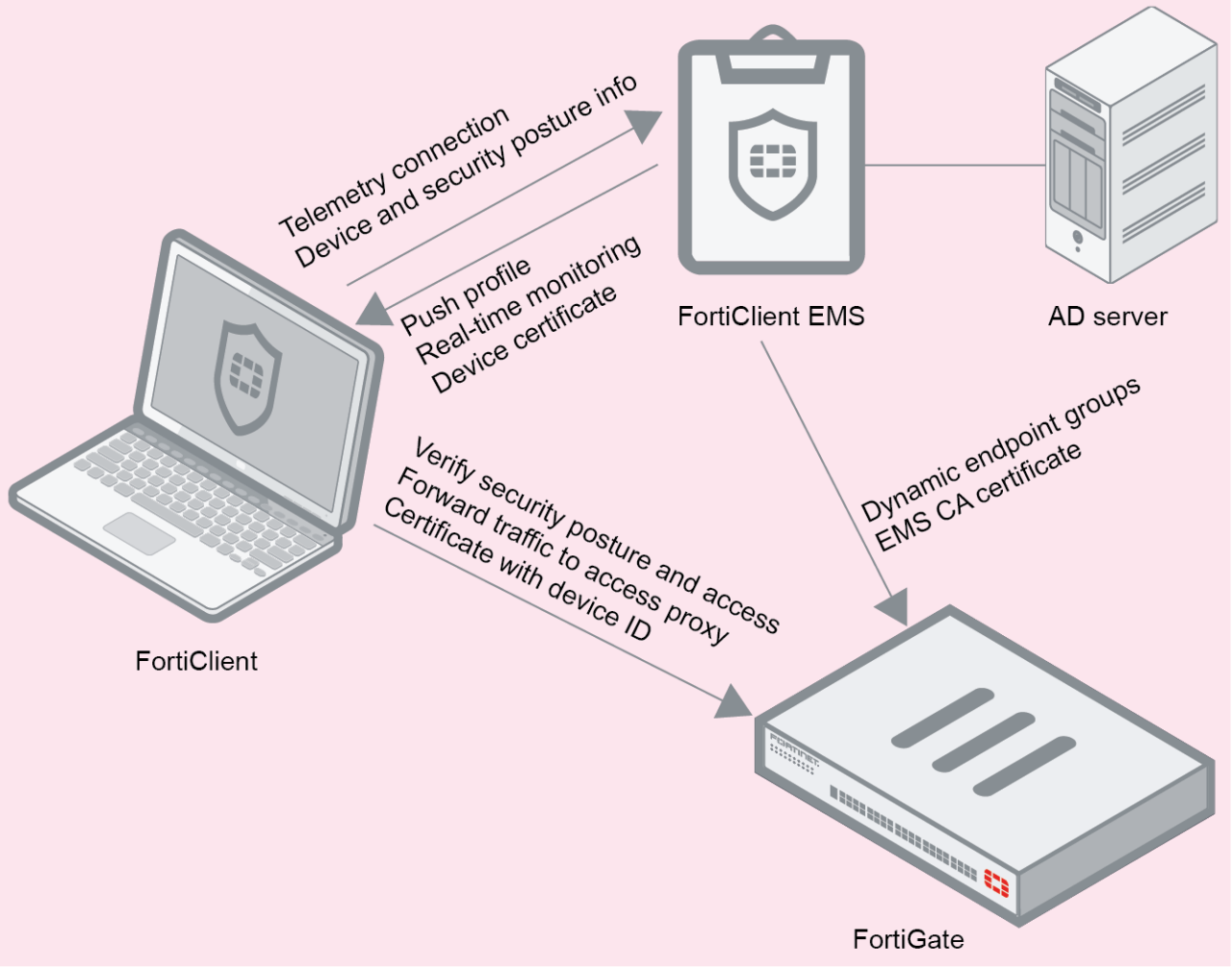
| Usage | Server URL | Protocol | Port | Incoming/Outgoing | How to customize |
|---|---|---|---|---|---|
| FortiClient EMS Cloud Sandbox (SaaS) connection | aptctrl1.fortinet.com | TCP | 443 (default) | Outgoing | N/A |

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

# Deployment options

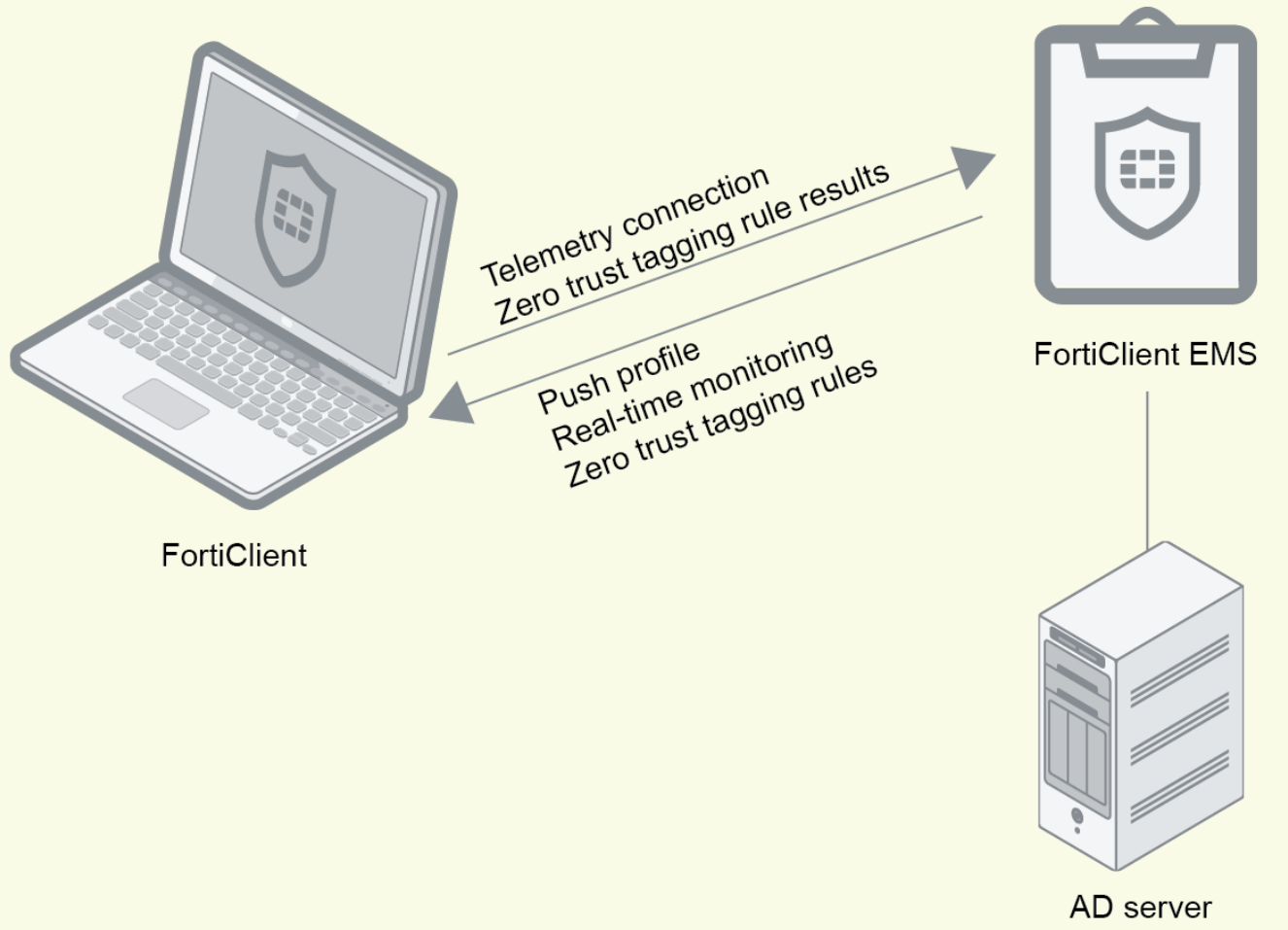
FortiClient EMS supports the following deployment scenarios: participating in the Fortinet Security Fabric or standalone.

## 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.

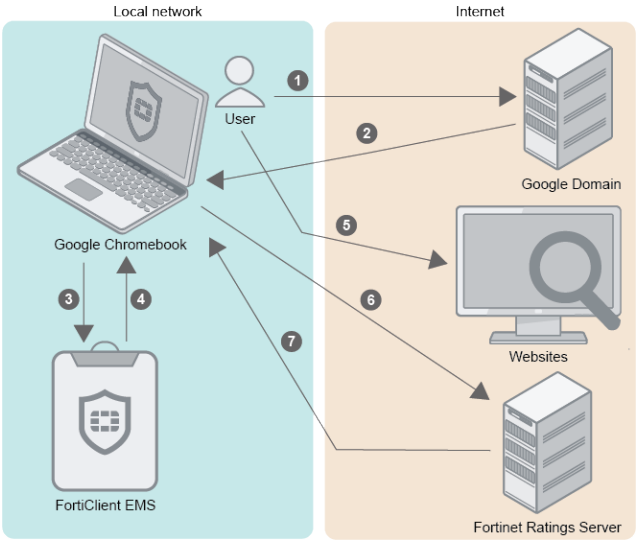
If you are using a self-signed certificate (non-public SSL certificate), your certificate's *Subject Alternative Name* must include `DNS:<FQDN>`, for example, `DNS:ems.forticlient.com`. You must add the SSL certificate to FortiClient EMS and the root certificate to the Google Admin console to allow the extension to trust FortiClient EMS. See Adding root certificates on page 51.

# 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 15.
2. Install FortiClient EMS. See Installing EMS in standalone mode with a local DB on page 16.
3. Start FortiClient EMS and log in. See Starting FortiClient EMS and logging in on page 24.

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_7.4.6.2170.M.bin`
- `forticlientems_7.4.6.2170.M_migration_tool.zip`
- `forticlientems_7.4.6.2170.M_postgres-ha.tar.gz`
- `forticlientems_7.4.6.2170.M_postgresql15.tar.gz`
- `FORTINET-FORTICLIENTEMS-build2170.M.mib`

Released firmware images use tags to indicate the following maturity levels:

- The *Feature (F)* tag indicates that the firmware release includes new features. It can also include bug fixes and vulnerability patches where applicable.
- The *Mature (M)* tag indicates that the firmware release includes no new major features. Mature firmware contains bug fixes and vulnerability patches where applicable.

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

# Installing EMS in standalone mode with a local DB

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

Installing EMS on Red Hat Enterprise Linux (RHEL) requires an active Red Hat subscription.

**To install standalone EMS:**

1. Download the `forticlientems_7.4.6.2170.M.arm64.bin` or `forticlientems_7.4.6.2170.M.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_7.4.6.2170.M.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. If you are installing EMS on Red Hat Enterprise Linux (RHEL) 9, do one of the following. :
   - If you are installing EMS on RHEL on Azure, run the following:

     ```
     sudo dnf repolist enabled
     ```

     Verify if `codeready-builder-for-rhel-9-x86_64-eus-rhui-rpms` is in the list. If it is in the list, it is enabled. If it is not in the list, then run the following:

     ```
     sudo subscription-manager repos --enable codeready-builder-for-rhel-9-x86_64-eus-rhui-rpms
     ```

     Run the following commands:

     ```
     sudo dnf install -y https://download.postgresql.org/pub/repos/yum/reporpms/EL-$(rpm -E
     %rhel)-$(uname -m)/pgdg-redhat-repo-latest.noarch.rpm
     sudo dnf config-manager --disable pgdg17 pgdg16
     sudo dnf install -y https://rpms.remirepo.net/enterprise/remi-release-$(rpm -q --qf "%
     {VERSION}\n" redhat-release).rpm
     sudo curl -o /etc/pki/rpm-gpg/RPM-GPG-KEY-remi2021 https://rpms.remirepo.net/RPM-GPG-KEY-
     remi2021
     sudo rpm --import /etc/pki/rpm-gpg/RPM-GPG-KEY-remi2021
     sudo ln -sf /etc/pki/rpm-gpg/RPM-GPG-KEY-remi2021 /etc/pki/rpm-gpg/RPM-GPG-KEY-
     remi.el$(rpm -q --qf "%{VERSION}\n" redhat-release)
     ```

   - If you are installing EMS on RHEL on AWS, run the following command:

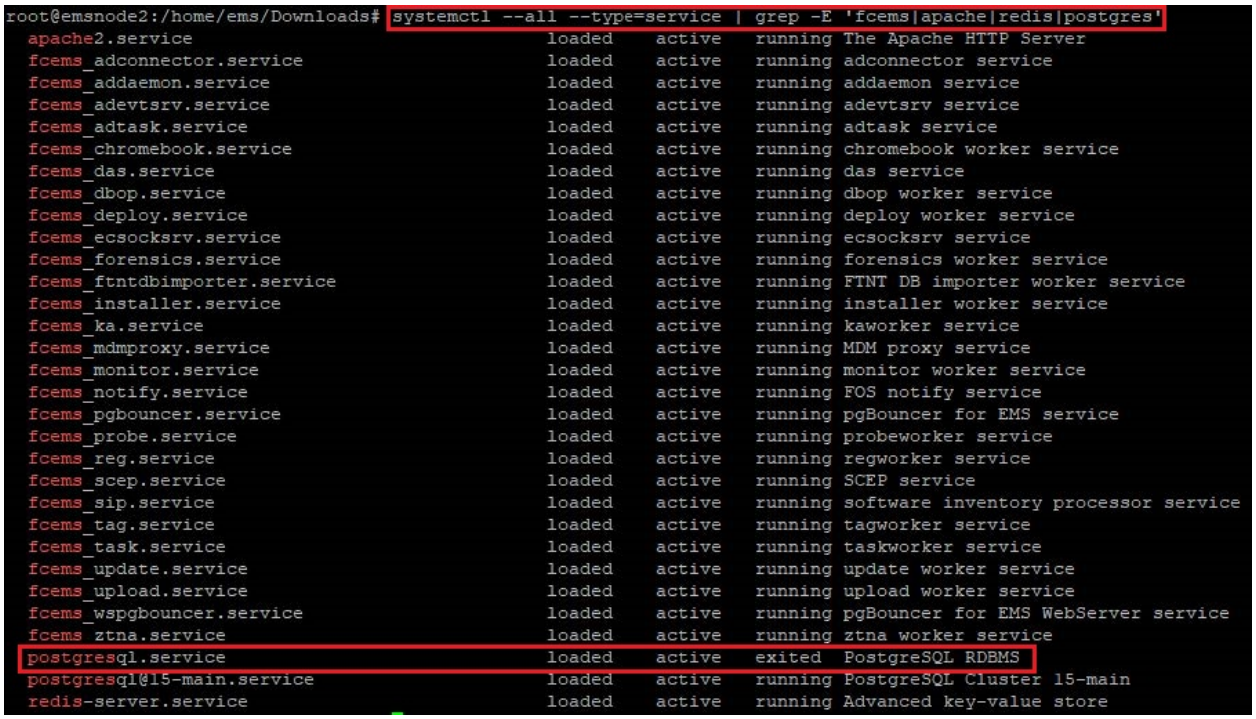
     ```
     sudo dnf config-manager --set-enabled codeready-builder-for-rhel-9-rhui-rpms
     ```

6. Run the following command to install EMS:
   `./forticlientems_7.4.6.2170.M.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.

7. After installation completes, verify that `/etc/timezone` and `/etc/localtime` are configured with the same time zone on the Linux system. Check that all EMS services are running by entering the following command:

```
systemctl --all --type=service | grep -E 'fcems|apache|redis|postgres'
```




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.

8. Access the EMS GUI and log in.
9. If after initially installing EMS 7.4.6 you need to upgrade to a newer build, repeat the process with the new installation file.

# Configuring the IP address

After deploying EMS in standalone mode, you may want to configure the IP address. Refer to one of the following procedures, depending on your platform.

An alternative way to configure the IP address is using the `emscli` tool:

- `emscli system set network ip`
- `emscli system set network domain`

## Ubuntu:

On Ubuntu, you configure the IP address by modifying the Netplan configuration files.

1. On the Ubuntu machine, locate the Netplan configuration files. Ubuntu stores Netplan configuration files in `/etc/netplan`. The files typically have a .yaml extension, such as 01-netcfg.yaml or 50-cloud-init.yaml. Run the following to list the files:

   ```
   ls /etc/netplan/
   ```

2. Use a text editor such as nano or vim to open the yaml file for editing:

   ```
   sudo nano /etc/netplan/01-netcfg.yaml
   ```

3. In the yaml file, find the section for your desired network interface. Do one of the following:
   - If you are using a static IP address, modify the file, setting `addresses` with your desired static IP address and subnet mask. Update the IP address under `routes: - to: default via:` with your desired gateway, and modify `nameservers` with search domains as needed. The following provides an example configuration where the static IP address is 192.168.1.100/24:

     ```
     network:
         version: 2
         renderer: networkd
         ethernets:
             enp3s0:
                 addresses:
                     - 192.168.1.100/24
                 nameservers:
                     addresses: [8.8.8.8, 1.1.1.1]
                     search: [mydomain1.local, mydomain2.local]
                 routes:
                     - to: default
                       via: 192.168.1.1
     ```

   - If you are using DHCP, ensure that `dhcp4` is set to `yes`. The following provides an example configuration:

     ```
     network:
       version: 2
       renderer: networkd
       ethernets:
         enp0s3:
           dhcp4: yes
     ```

4. Before applying the changes permanently, run the following to test the configuration. This command temporarily applies the configuration and gives you 120 seconds to confirm the changes. If the configuration does not work, it rolls back automatically.

   ```
   sudo netplan try
   ```

5. If the test succeeds, apply the changes permanently:

   ```
   sudo netplan apply
   ```

6. To verify the configuration, check that the IP address is updated as you configured:

```
ip addr show
```

## RHEL:

You can utilize several methods to configure a network interface with a static IP address on Red Hat Enterprise Linux (RHEL) 9. The following approach uses the nmcli command-line tool, which allows you to manage network connections from the command line.

1. Run the following command to list all network interfaces and identify the one you want to configure:

```
nmcli device status
```

2. Modify the connection using the following command (this example modifies the interface *enp0s3*):

```
sudo nmcli con mod 'enp0s3' ipv4.method manual ipv4.addresses 192.168.1.100/24 ipv4.gateway
192.168.1.1 ipv4.dns "8.8.8.8 8.8.4.4"
```

   Replace *enp0s3* with your actual interface name and adjust the IP address, gateway, and DNS servers as per your network configuration.
3. Apply the network interface changes by restarting the connection using the following command:

```
sudo nmcli con down 'enp0s3' && sudo nmcli con up 'enp0s3'
```

4. Verify the IP configuration using the following commands:

```
ip addr show enp0s3
ip route show
```

## CentOS:

To configure the IP address on CentOS:

1. Run the following command to list all network interfaces and identify the one you want to configure:

```
nmcli connection show
```

2. Modify the connection to set a static IP address using the following commands (this example modifies the interface *enp0s3*):

```
sudo nmcli connection modify enp0s3 \
ipv4.method manual \
ipv4.addresses 192.168.1.100/24 \
ipv4.gateway 192.168.1.1 \
ipv4.dns "8.8.8.8 8.8.4.4" \
connection.autoconnect yes
```

   Replace *enp0s3* with your actual interface name and adjust the IP address, gateway, and DNS servers as per your network configuration.
3. Apply the network interface changes by restarting the connection using the following command:

```
sudo nmcli connection down enp0s3 && sudo nmcli connection up enp0s3
```

4. Verify the IP configuration using the following commands:

```
ip addr show enp0s3
ip route show
```

# Licensing EMS by logging in to FortiCloud

You must license 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.

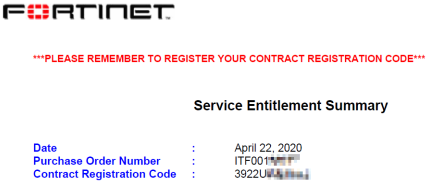
1. In EMS, in the *License Information* widget, click *Add* beside *FortiCloud Account*.
2. In the *FortiCloud Registration* dialog, enter your FortiCloud account credentials. If you do not have a FortiCloud account, create one.
3. Click *Login & Sync License Now*. If your FortiCloud account is eligible 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.

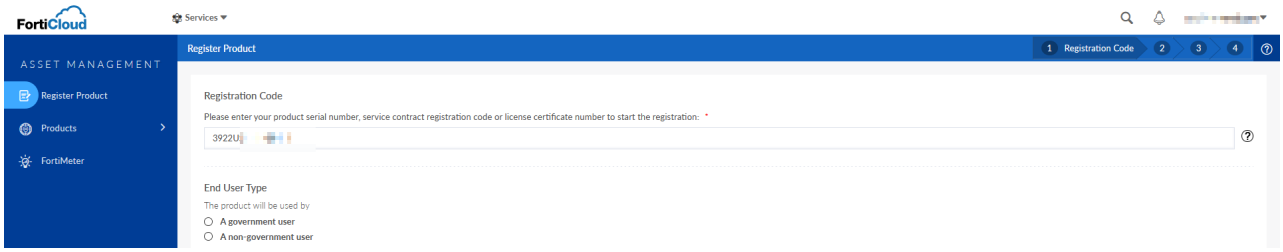
1. Log in to FortiCloud.
2. Click *Register Now*.
3. In the *Registration Code* field, enter the *Contract Registration Code* from your service registration document. Configure other fields as required, then click *Next*.



***PLEASE REMEMBER TO REGISTER YOUR CONTRACT REGISTRATION CODE***

**Service Entitlement Summary**

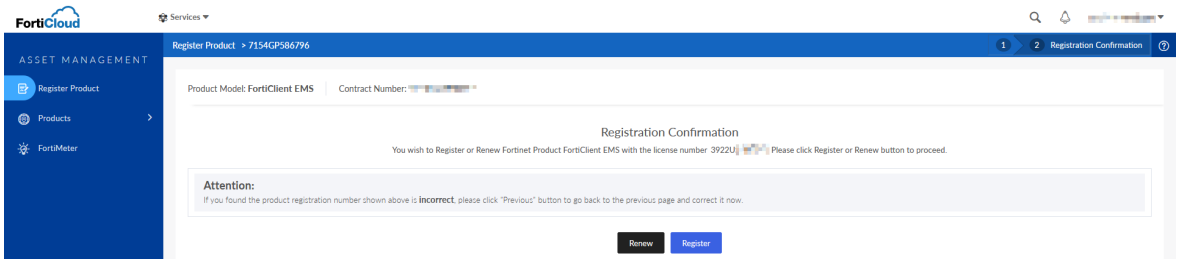
| | | |
|---|---|---|
| Date | : | April 22, 2020 |
| Purchase Order Number | : | ITF001 |
| Contract Registration Code | : | 3922U |




4. 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.

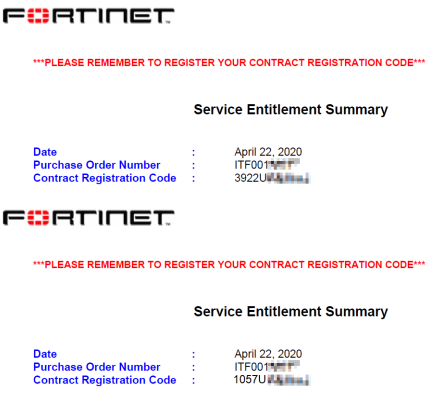
If you previously activated another license with the same EMS hardware ID, you receive a duplicated UUID error. In this case, contact Customer Support to remove the hardware ID from the old license.

**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*.



FORTINET

***PLEASE REMEMBER TO REGISTER YOUR CONTRACT REGISTRATION CODE***

Service Entitlement Summary

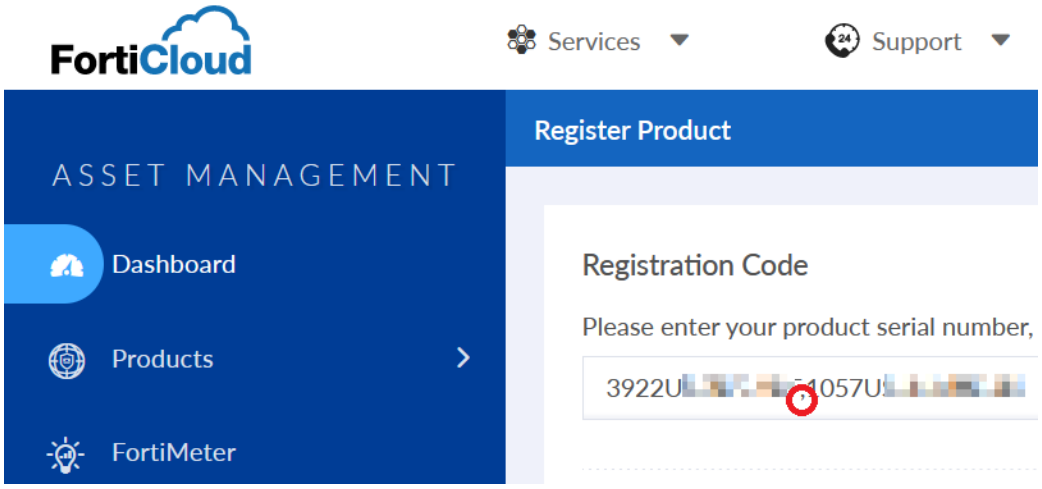
Date : April 22, 2020
Purchase Order Number : ITF001
Contract Registration Code : 3922U

FORTINET

***PLEASE REMEMBER TO REGISTER YOUR CONTRACT REGISTRATION CODE***

Service Entitlement Summary

Date : April 22, 2020
Purchase Order Number : ITF001
Contract Registration Code : 1057U




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.

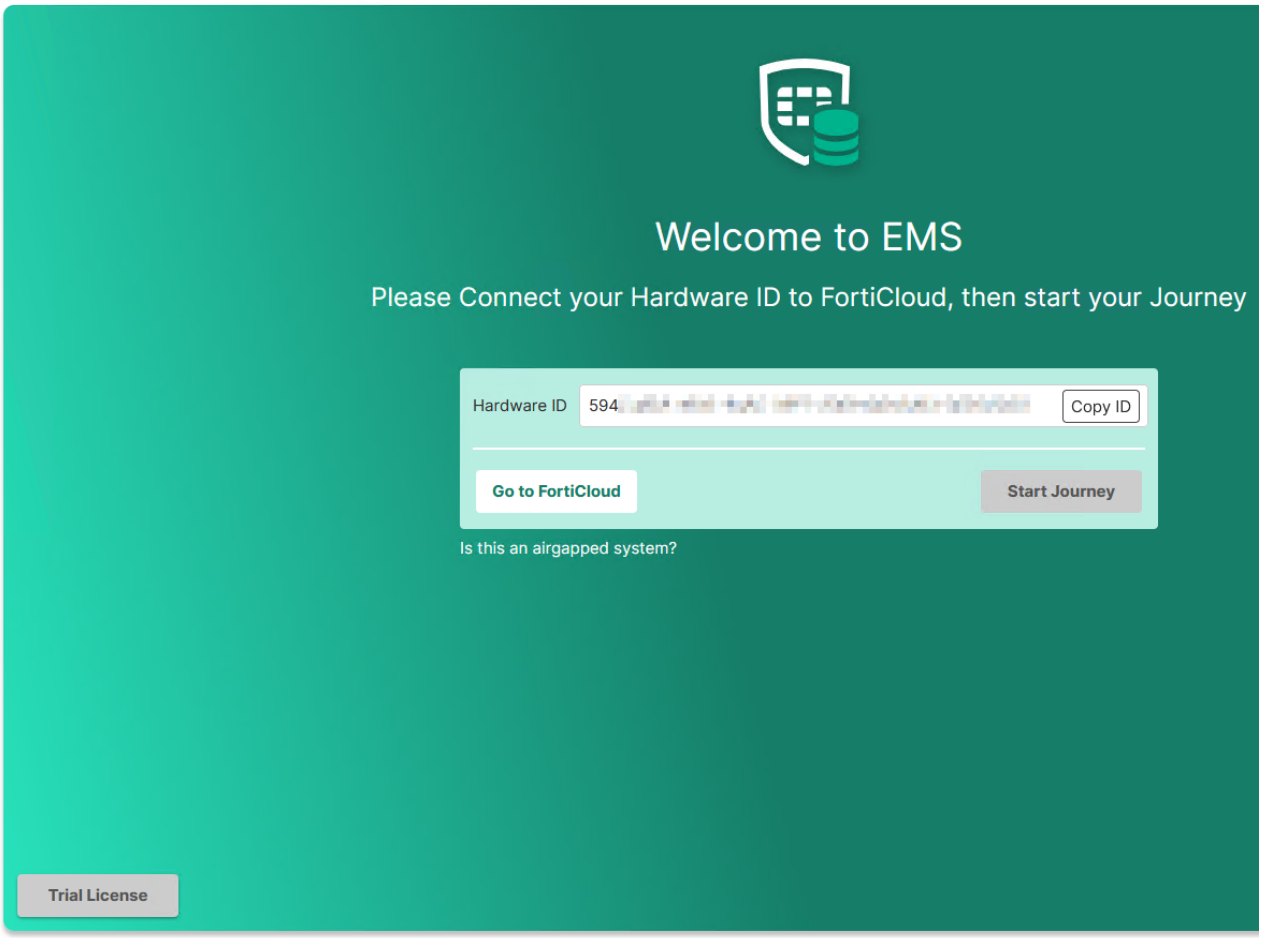
The post-install setup wizard streamlines the EMS post-install setup process.

**To license EMS using the post-install setup wizard:**

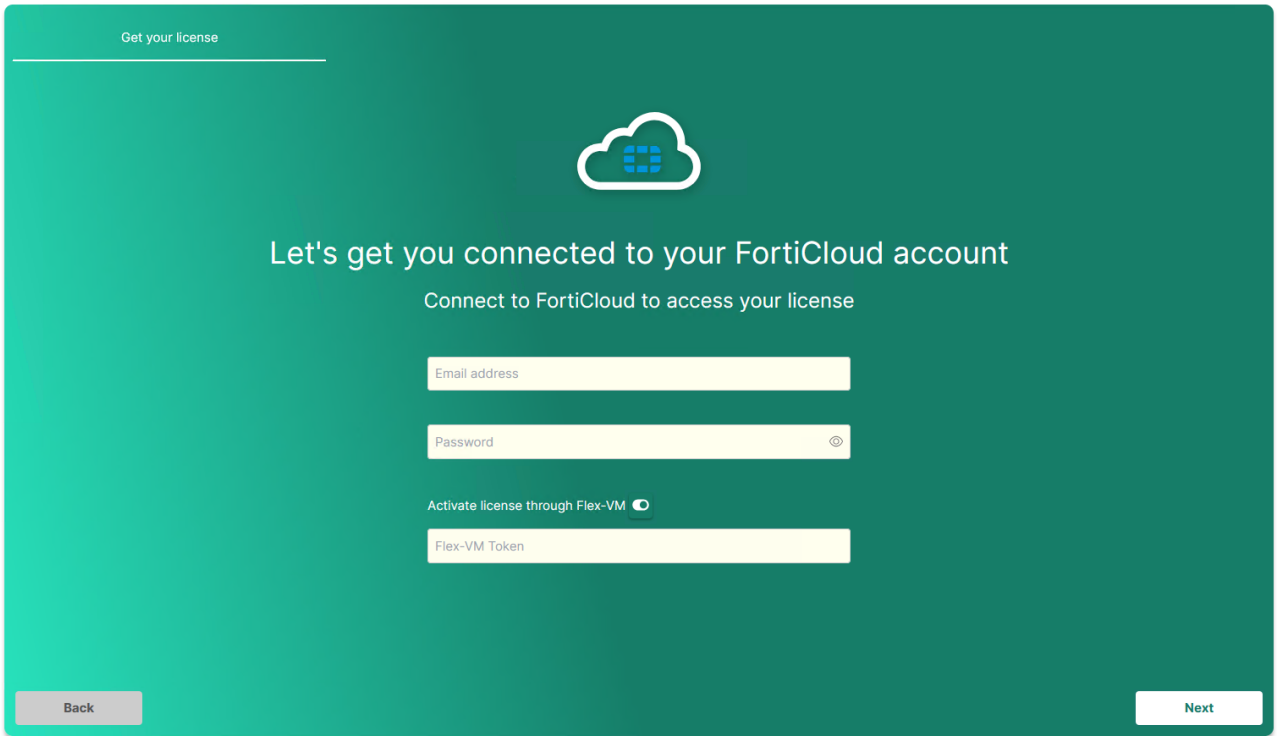
1. After installing EMS, launch it for the first time. EMS displays a *Welcome to EMS* page that displays the hardware ID of the machine that EMS is installed on. Registering and licensing EMS requires the hardware ID. Do one of the following:
   - If you have a registered license, click *Start Journey*.
   - 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 20 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*.

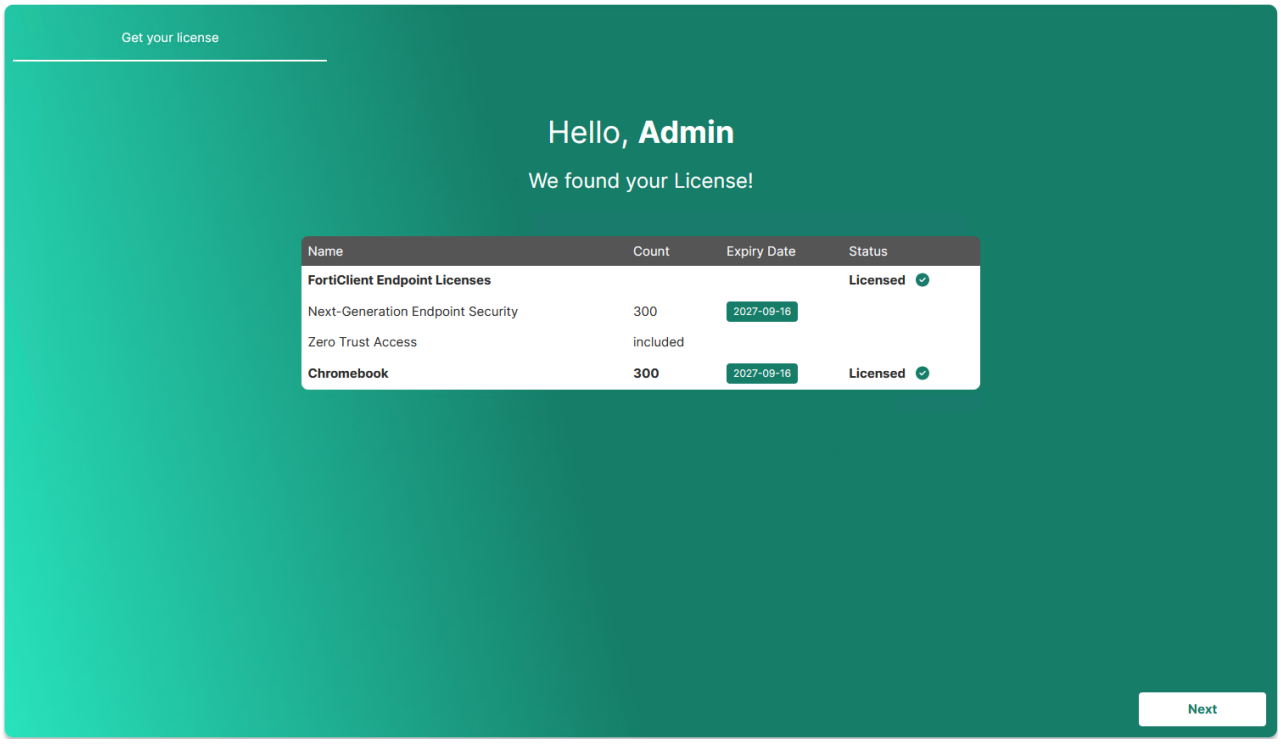



2. On the *Let's get you connected to your FortiCloud account* page, do one of the following, then click *Next*:
   - Enter your FortiCloud account credentials to retrieve your EMS license from FortiCloud.
   - Activate your EMS using FortiFlex licensing by enabling *Activate license through Flex-VM* 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*. In the *FQDN* field, enter the desired FQDN.
3. If desired, in the *Custom hostname* field, enter the hostname or IP address. Otherwise, EMS uses the *Pre-defined hostname*.
4. If desired, select the *Redirect HTTP request to HTTPS* checkbox. If this option is enabled, if you attempt to remotely access EMS at *http://<server_name>*, this automatically redirects to *https://<server_name>*.
5. Click *Save*.

**To remotely access FortiClient EMS:**

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

# Windows, macOS, and Linux endpoint management setup

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

Following is a summary of how to use FortiClient EMS:

1. Configure user accounts. See Configuring user accounts on page 28.
2. Create an endpoint profile. See Creating a new profile on page 29.
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 30.
4. Deploy the FortiClient deployment package. See Deploying the FortiClient deployment package to endpoints on page 37.
   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 37.

# 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.<br>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. Do one of the following:
   a. To create a Windows, macOS, and Linux profile, click *Add Profile*.
   b. To create a Chromebook profile, click *Add Chrome Profile*.
5. Configure the settings as desired.
6. 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 the *Sign software packages* option is enabled in *System Settings > EMS Settings*, Windows deployment packages display as being from the publisher specified in the certificate file. See the*FortiClient EMS Administration Guide*.

**To create an installer or install config file:**

1. Go to *Deployment & Installers > FortiClient Installer* and click *Add*.
2. On the *General* tab, configure the options depending on the type of FortiClient installer you are using:
   - To use an official FortiClient installer, keep the *Create a manual installer* option disabled under *Advanced Options* at the bottom and 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. |
| *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 Latest Patch* | Select to enable FortiClient to automatically update to the latest patch release when FortiClient is installed on an endpoint.<br>For more information about the FortiClient upgrade process on the endpoint, see Upgrading FortiClient. |
| *Repackaged Installer Files* | Configure which installer files to include. |

   - To manually create a FortiClient installer, enable the *Create a manual installer* option under *Advanced Options* at the bottom and set the following options:

| Option | Description |
|---|---|
| *Release* | Select from the following options:<br>• *Upload packaged installer*—Manually upload a repackaged installer provided by TAC. |

| Option | Description |
|---|---|
| | • *Use custom installer*—Select from a list of previously uploaded custom installers or upload a new custom installer as follows:<br>**a.** Click *Add*.<br>**b.** Specify the custom installer name.<br>**c.** Browse to select 64-bit/32-bit Window and/or Linux/macOS custom installers in ZIP or MSI format.<br>You can download FortiClient installers (in ZIP format) from Fortinet Customer Service & Support., which requires a support account with a valid support contract. To upload an `.msi` file, you must package the installer as an `.msi` file.<br>**d.** For Windows and Linux, you can also select *Include ARM* and browse to select the ARM installer files.<br>**e.** Click *Upload*. |
| *Manual Installer Name* | Enter the desired custom installer name. |

3. 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.<br>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. |

| Option | Description |
|---|---|
| *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:<br>• AntiVirus, Anti-Exploit, Removable Media Access<br>• Anti-Ransomware<br>• Cloud Based Malware Outbreak Detection<br>Disable to exclude features from the FortiClient installer. |
| *Web and Video Filtering* | Enable any of the following features:<br>• Web Filtering<br>• Video Filtering<br>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. |
| *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.

4. 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. |
| *Include MSI installer files* | Enable to include MSI installer files for FortiClient (Windows). |

| Option | Description |
|---|---|
| *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.<br>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.<br>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:<br>• **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.<br>• **Allow**: allows FortiClient to connect to EMS with an invalid certificate.<br>• **Deny**: block FortiClient from connecting to EMS with an invalid certificate. |

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. 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. |

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.<br>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. |

| Option | Description |
|---|---|
| *Malware* | Enable any of the following features:<br>• AntiVirus, Anti-Exploit, Removable Media Access<br>• Anti-Ransomware<br>• Cloud Based Malware Outbreak Detection<br>Disable to exclude features from the FortiClient installer. |
| *Web and Video Filtering* | Enable any of the following features:<br>• Web Filtering<br>• Video Filtering<br>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. |
| *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. |

| Option | Description |
|---|---|
| | 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.<br>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:<br>• **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.<br>• **Allow**: allows FortiClient to connect to EMS with an invalid certificate.<br>• **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.

# 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.

| | |
|---|---|
| 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:<br>• **Online**: endpoint has been seen within less than three keep alive timeouts.<br>• **Away**: endpoint has been offline for less than eight hours.<br>• **Offline**: endpoint has been offline for more than eight hours.<br>• **Never Seen**: endpoint has never been registered to EMS.<br>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. |
| 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.<br>  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:<br>• Selected Vulnerabilities on Selected Clients<br>• Selected Vulnerabilities on All Affected Clients<br>• 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:<br>• Request FortiClient Logs<br>• Request Diagnostic Results<br>• Update Signatures<br>• Download Available FortiClient Logs<br>• Download Available Diagnostic Results<br>• Deregister<br>• Quarantine<br>• *Un-quarantine*<br>• *Exclude from Management*<br>• *Revoke Client Certificate*: only available if the ZTNA or EPP license is applied. 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.<br>• Clear Events<br>• Mark as Uninstalled<br>• Set Importance<br>• Set Custom Tags. This option is only available if you have already created a custom tag.<br>• 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.<br>• Delete Device<br>• 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 keepalive (KA) message to EMS. This information is useful if FortiClient is offline because it indicates when the last KA 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:<br>• MAC address<br>• IP address<br>• Gateway IP address<br>• Gateway MAC address<br>• 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. You can also view tag evaluation and rule matching details by clicking the *View All Security Posture Tags* link. |
| | *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:<br>• Policy: Endpoint policy assigned to the selected endpoint<br>• Installer: FortiClient installer used for the selected endpoint.<br>• FortiClient Version: FortiClient version installed on the selected endpoint.<br>• FortiClient Serial Number: Serial number for the selected endpoint's FortiClient license.<br>• FortiClient ID<br>• ZTNA Serial Number: serial number for the zero trust network access certificate provisioned to the endpoint.<br>• MDM Enrolled: whether the endpoint is enrolled on a mobile device management (MDM) platform.<br>• 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 *Add*, enter the desired tag, then click the *+* button. When you create a tag, it is available for assignment to all endpoints in the site.<br>You can assign a classification tag to multiple endpoints by selecting the endpoints, then selecting *Action > Set Importance* or *Set Custom Tags*.<br>Tags that FortiClient EMS receives from FortiAnalyzer also display under *Classification Tags*.<br>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:<br>• **FortiEDR_Malicious**: FortiEDR has classified this endpoint as malicious.<br>• **FortiEDR_PUP**: FortiEDR has detected a potentially unwanted program on this endpoint.<br>• **FortiEDR_Suspicious**: FortiEDR has detected suspicious activity on this endpoint.<br>• **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.<br>See Identity Management integration. |
| | *Forensic Analysis* | Displays statuses for forensic analysis tasks:<br>• **Ticket Status**: status of the ticket. Possible statuses are:<br>  • **Request Submitted**<br>  • **Pending**: Forensic analysis request has been initiated. The Forensics team has not yet assigned it to an analyst.<br>  • **Running**<br>  • **In Progress**: Forensics team has assigned the request to an analyst, who has begun working on it.<br>  • **Failed**: analyst could not connect to the endpoint.<br>  • **Cancelled**: indicates one of the following:<br>  • The analyst needed more information about the endpoint to perform the analysis.<br>  • The EMS administrator canceled the request.<br>  • **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.<br>• **Agent Status**: status of the forensic agent collecting logs on the endpoint. Possible statuses are:<br>  • **Pending**: EMS has notified FortiClient that a forensic analysis request is submitted, but the forensic agent is not running yet.<br>  • **Running**: forensics agent starts collecting forensics logs.<br>  • **Collection Completed**: forensics agent has completed collecting forensics logs.<br>  • **Upload Started**: FortiClient has started to upload the logs to the cloud.<br>  • **Upload Completed**: FortiClient has completed uploading the logs to the cloud.<br>  • **Upload Failed**: FortiClient failed to upload the logs to the cloud.<br>• **Verdict**: forensic analysis verdict as determined by the FortiGuard analyst.<br>• **Task ID**: Request ID in the FortiGuard forensics system.<br>• **Request Analysis**: request forensic analysis on the endpoint. See Requesting forensic analysis on an endpoint.<br>• **Download Report**: download the forensic analysis report. |
| | *Status* | Displays one of the following statuses:<br>• Managed: Endpoint is managed by EMS.<br>• 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.<br>• Excluded: Endpoint is excluded from management by EMS. |
| | *FortiDeceptor Campaign Deployment* | Displays the status of the FortiDeception token if enabled on the endpoint:<br>• When the token is deployed to FortiClient, the field progresses from *Pending* to *Notified* to *Deployed*.<br>• When the token is removed from FortiClient, the field progresses from *Pending to uninstall* to *Notified to uninstall* to *Clean*. The *FortiDeceptor Campaign Deployment* field will eventually no longer be visible for the endpoint.<br>See FortiDeceptor Campaign. |
| | *Endpoint Health* | Provides a comprehensive view of feature statuses, such as whether a feature is installed, not installed, enabled, or disabled. It also reports any warnings or error messages associated with a feature. For example, if FortiClient cannot connect to VPN, an error displays under *Remote Access*. This enhanced visibility significantly improves the ability to diagnose and troubleshoot feature-related issues. You can effectively identify and resolve problems specifically linked to endpoint feature configurations and statuses.<br>A feature may have one of the following statuses:<br>• *OK*<br>• *Warning*<br>• *Error*<br>• *Disabled*<br>• *Not Installed*<br>Clicking the status opens a slide-in with detailed information about the status. For the *Warning* and *Error* statuses, the *Description* may provide details to explain the cause, which you can investigate. |
| | *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 antivirus (AV) event 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. |
| | *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.<br>PUA categories are as follows:<br>• Illegal or unethical<br>• Cryptomining<br>• Hacking<br>• Unpopular<br>• Phishing<br>• 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. |

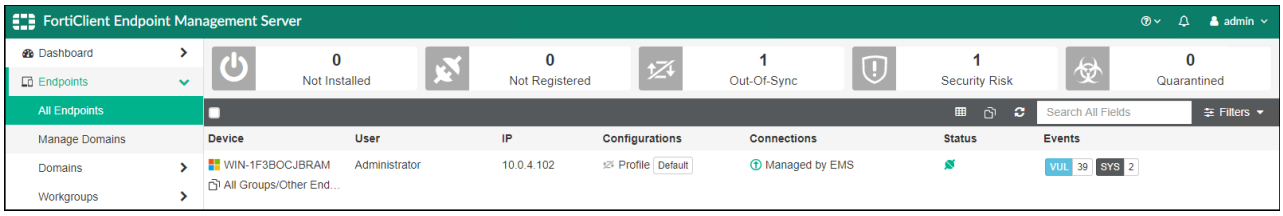
| | | |
|---|---|---|
| *Data Protection Events* | | |
| | *Date* | Displays the date the end user triggered the data protection event. |
| | *Count* | Displays the number of occurrences for this event. |
| | *Message* | Displays the event message. |
| | *Actions* | Mark the event as read or delete it. |
| *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 37.

**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 65.
2. Add the Google domain. See Adding a Google domain on page 67.
3. Create an endpoint profile. See Adding a new Chromebook profile on page 67.
4. Create an endpoint policy configured with the endpoint profile. See Adding a Chromebook policy on page 69.
5. View the status. See Viewing domains on page 70.

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.

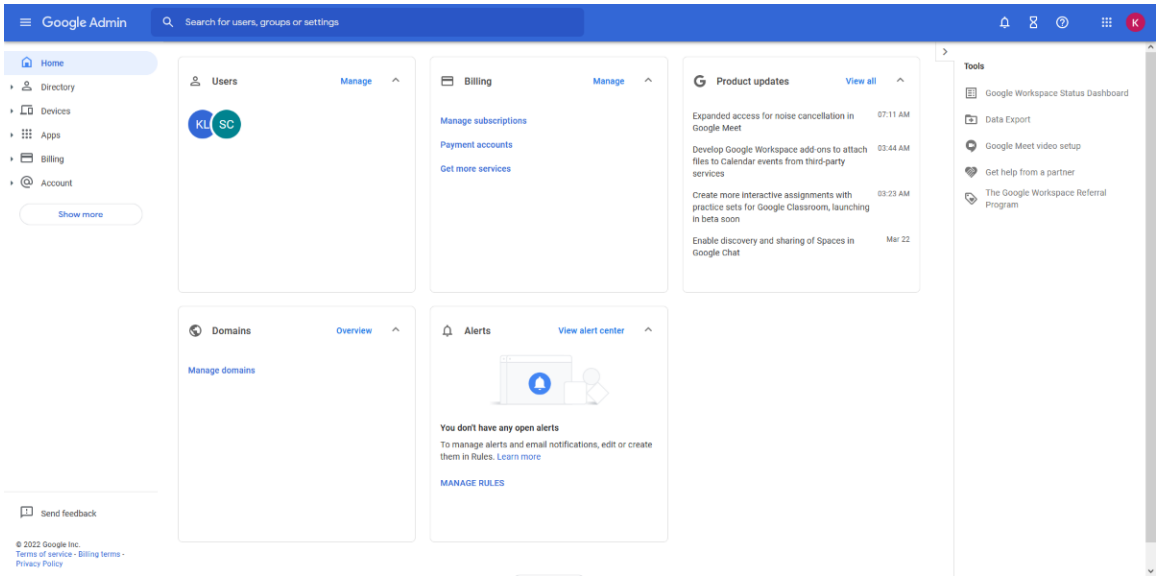
Following is a summary of how to set up the Google Admin console:

1. Log into the Google Admin console. See Logging into the Google Admin console on page 49.
2. Add the FortiClient Web Filter extension. See Adding the FortiClient Web Filter extension on page 49.
3. Configure the FortiClient Web Filter extension. See Configuring the FortiClient Web Filter extension on page 50.
4. Add the root certificate. See Adding root certificates on page 51.
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.

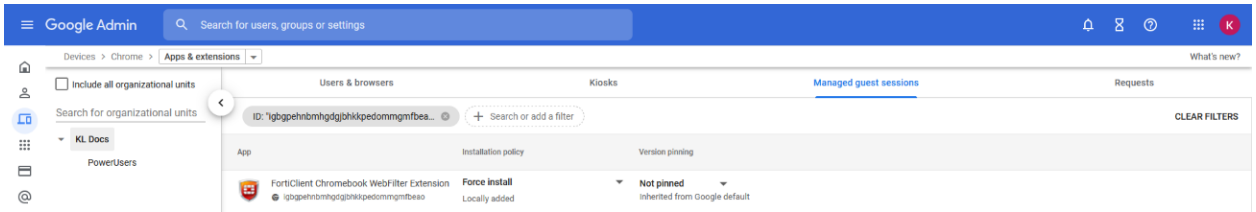



# Adding the FortiClient Web Filter extension

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.

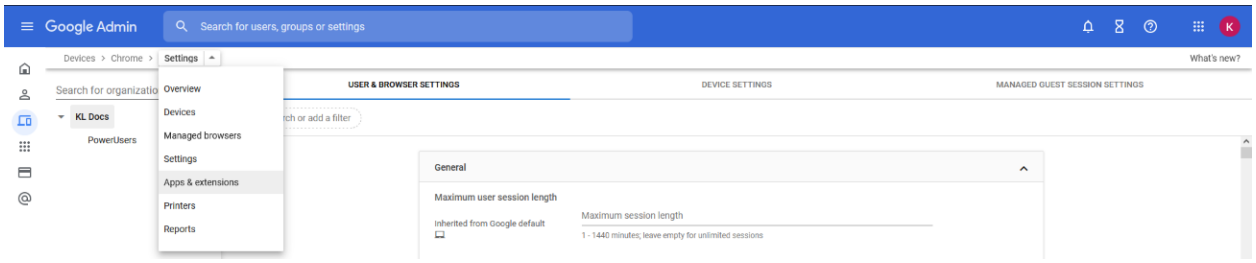
**To configure the FortiClient Web Filter extension:**

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": { "Value": "SiteName"} }` | `{ "ProfileServerUrl": { "Value": "https://ems.mydomain.com:8443"} }, "SiteName": { "Value": "Site1"} }` |

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 53.

## 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 53.

The FortiAnalyzer FQDN address can be assigned to *Common Name* or *Alternative Name*.

FortiAnalyzer also supports one-level wildcard FQDNs for certificates. For example, for certificates with wildcard FQDN `*.fortinet.com`, FortiAnalyzer accepts certificates with the `ems.fortinet.com` FQDN but not certificates with the `test.ems.fortinet.com` FQDN.

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.<br>• 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.<br>• 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:**

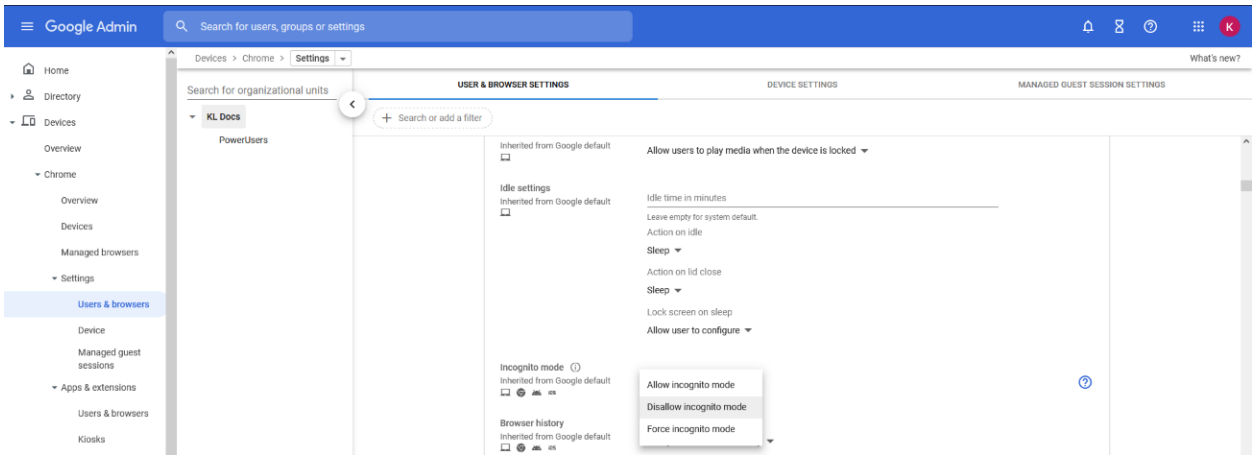
1. In the Google Admin console, go to *Devices > Chrome > Settings > Users & browsers*.
2. On the left, select the organization that contains the desired users or enrolled browsers. To select all users and browsers, select the top-level organization. Otherwise, select a child.
3. In *User & Browser Settings*,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

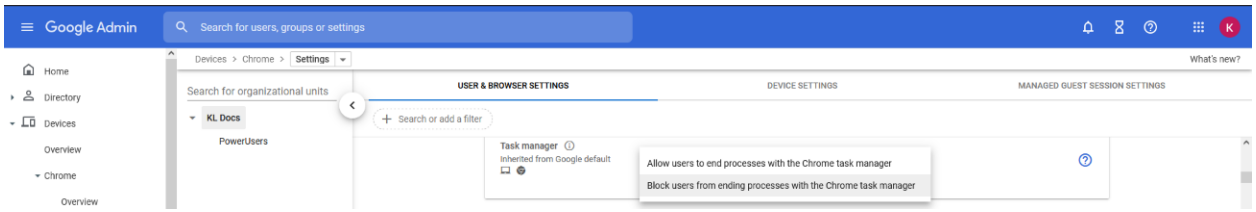
1. In the Google Admin console, go to *Devices* > *Chrome* > *Settings* > *Device*.
2. On the left, select the organization that contains the desired users or enrolled browsers. To select all users and browsers, select the top-level organization. Otherwise, select a child.
3. Under *Sign-in settings*, 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 |
| 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 63.

# 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 56.
2. Add the unique service account credentials to the Google Admin console. See Delegating domain-wide authority to the service account on page 63.
3. Add the unique service account credentials to FortiClient EMS. See Adding service account credentials to EMS on page 65.

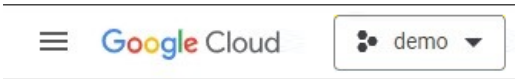
## Creating unique service account credentials

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

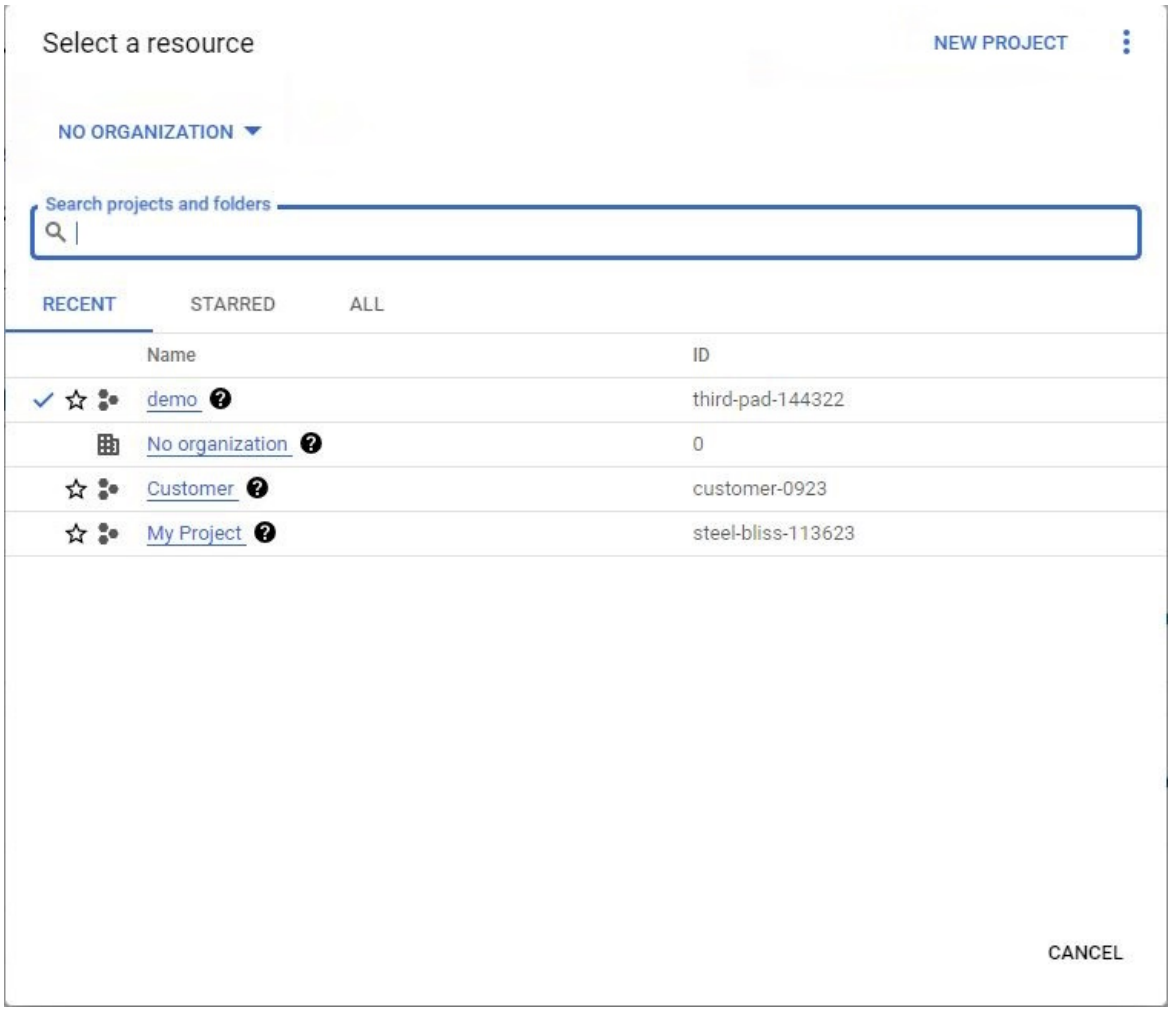
- Client ID (a long number)
- Service account ID (email address)
- Service account certificate (a certificate in `.pem` format)

**To create unique service account credentials:**

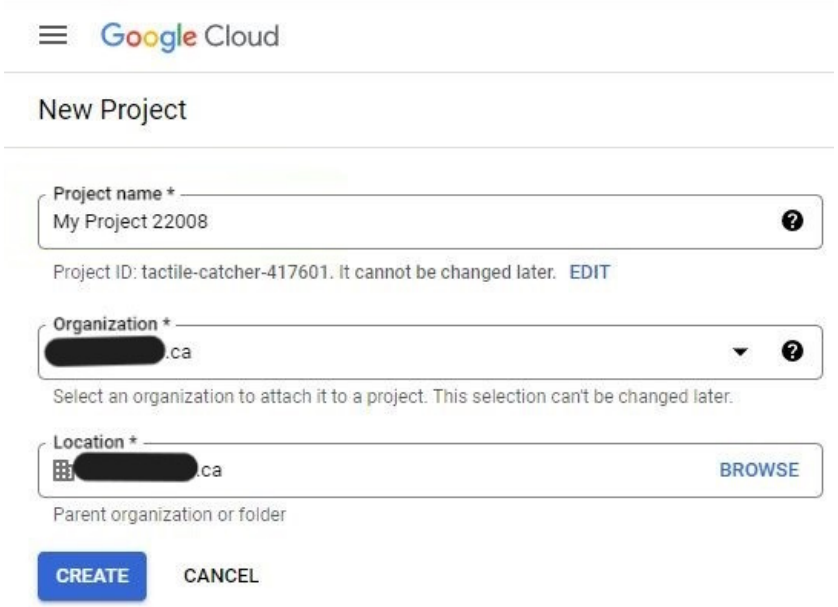
1. Go to Google API Console.
2. Log in with your Google Workspace account credentials.
3. Create a new project:
   a. Click the toolbar list. The browser displays the following dialog.



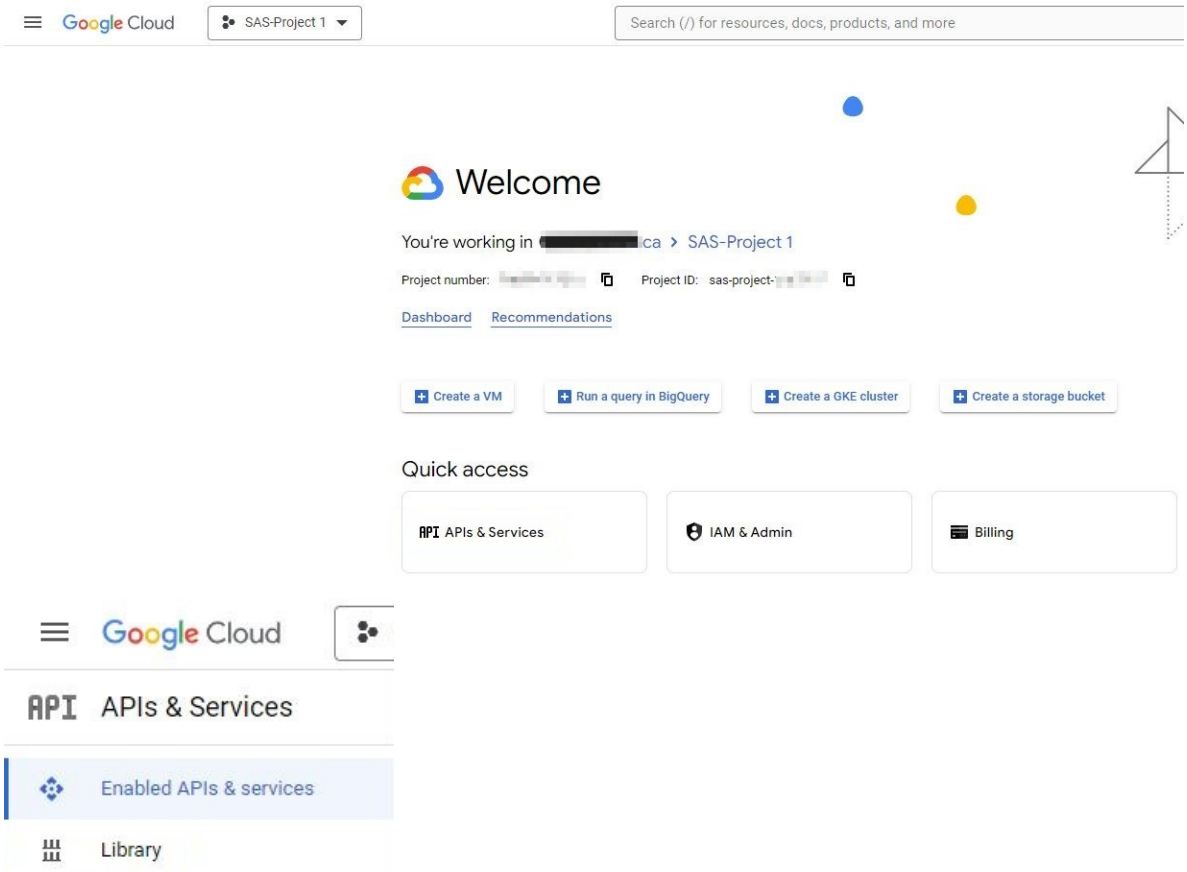
**b.** Select your organization, if you see an organization dropdown list. Click *New Project*.



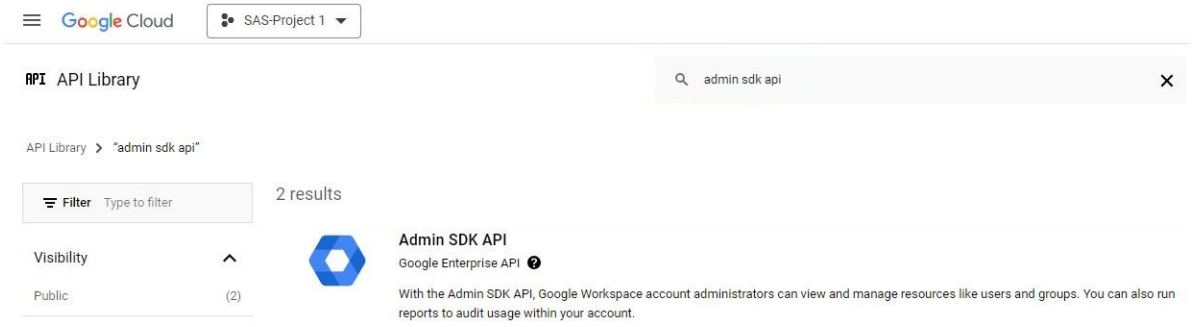

**c.** In the *Project name* field, enter your project name, then click *Create*.

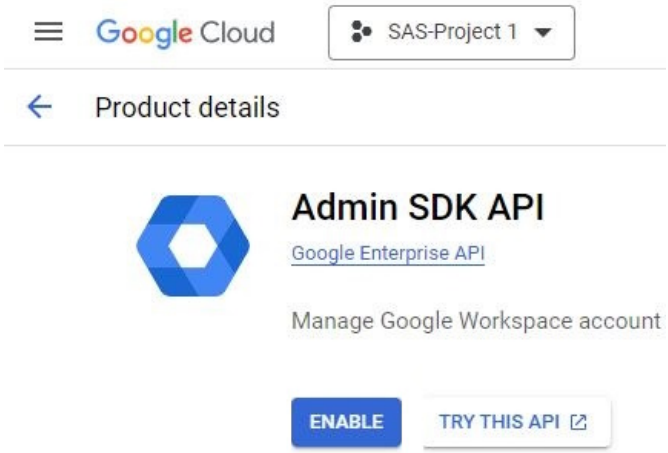


4. Enable the Admin SDK:
   a. Select your project from the toolbar list, then click *APIs & Services*.

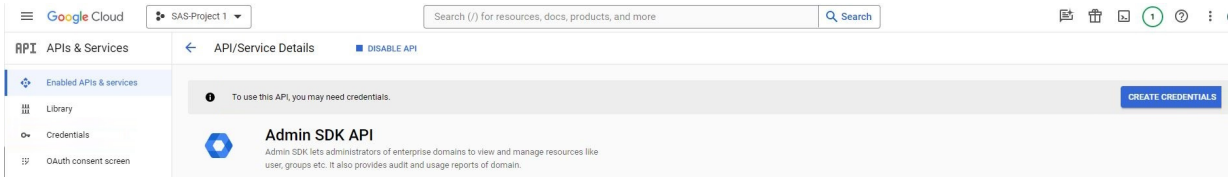



   b. Under *Google Workspace APIs*, search for *Admin SDK API* and enable it.

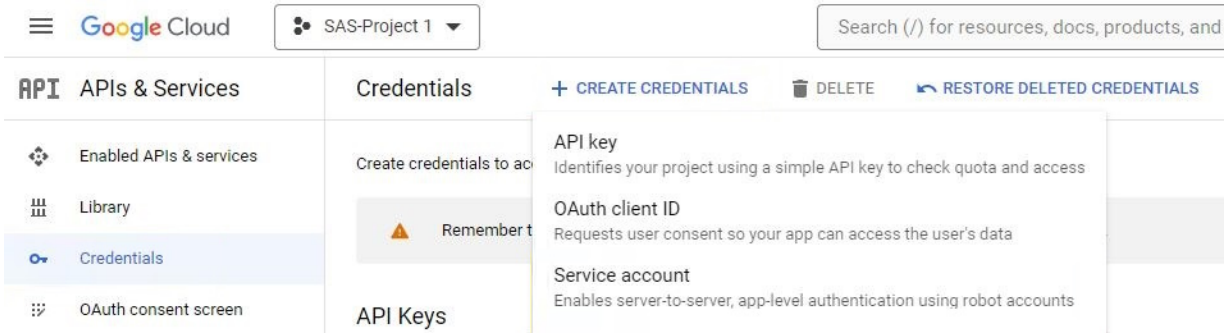




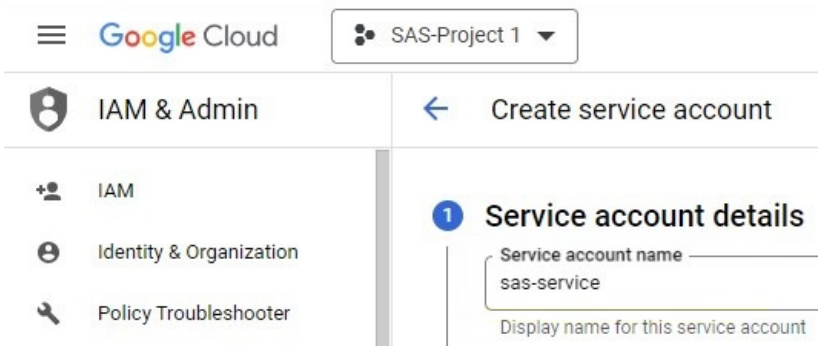

After enabling the Admin SDK API, the console displays a message indicating: *To use this API, you may need credentials*.



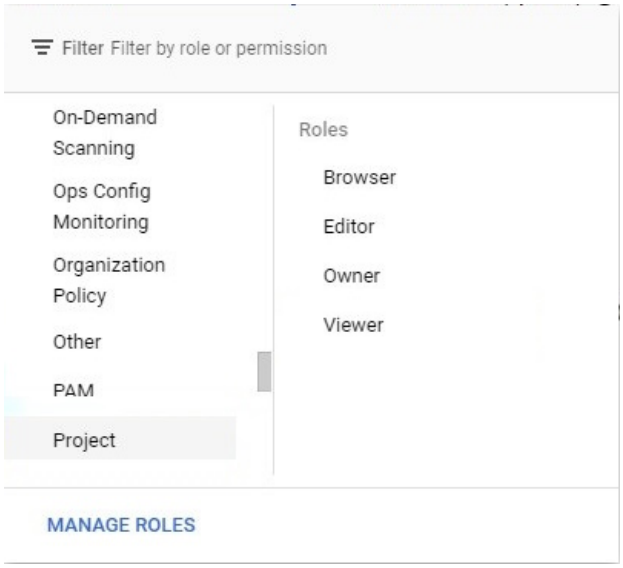

5. Create a service account:
   a. Go to the *Credentials* tab and select *Create Credentials* > *Service account*.



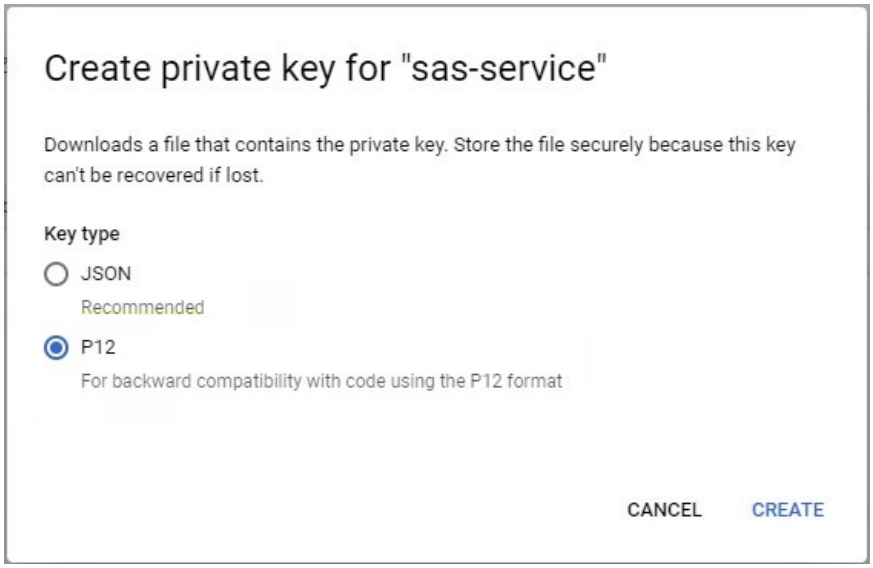

   b. From the *Service account* list, select *New Service Account*. Enter a service account name.



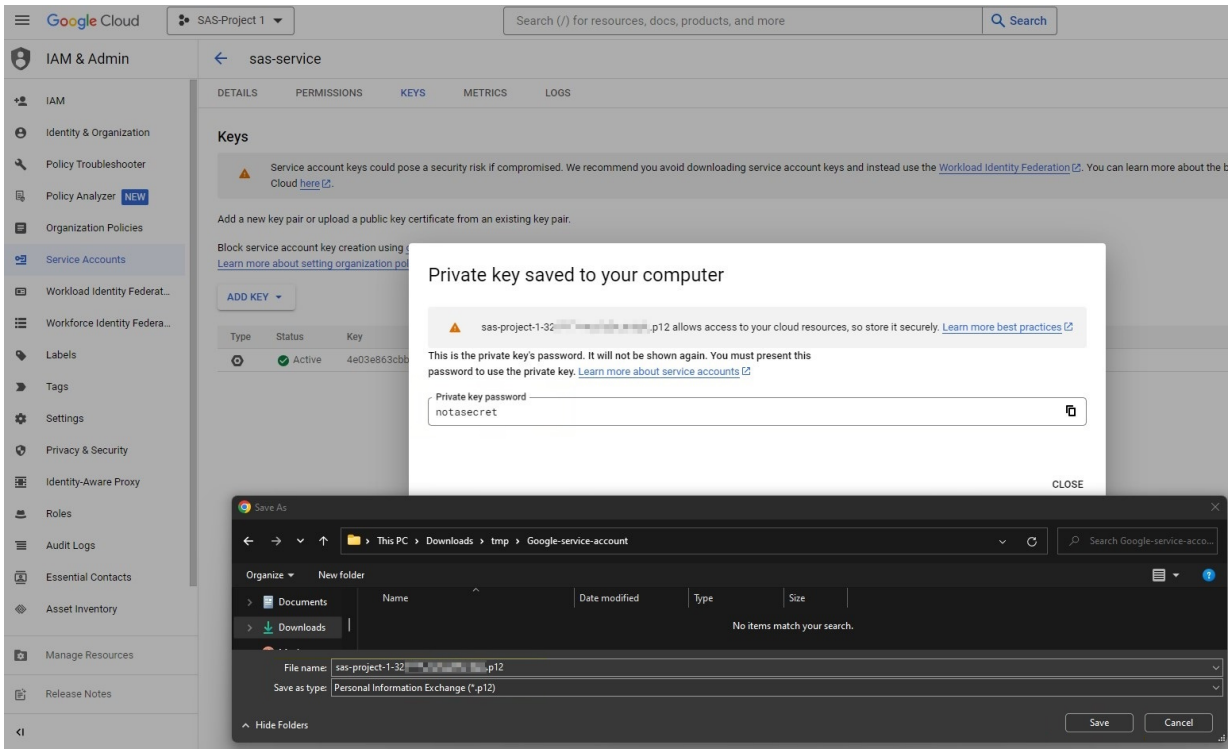
**c.** From the *Role* list, select *Project* > *Viewer*.




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

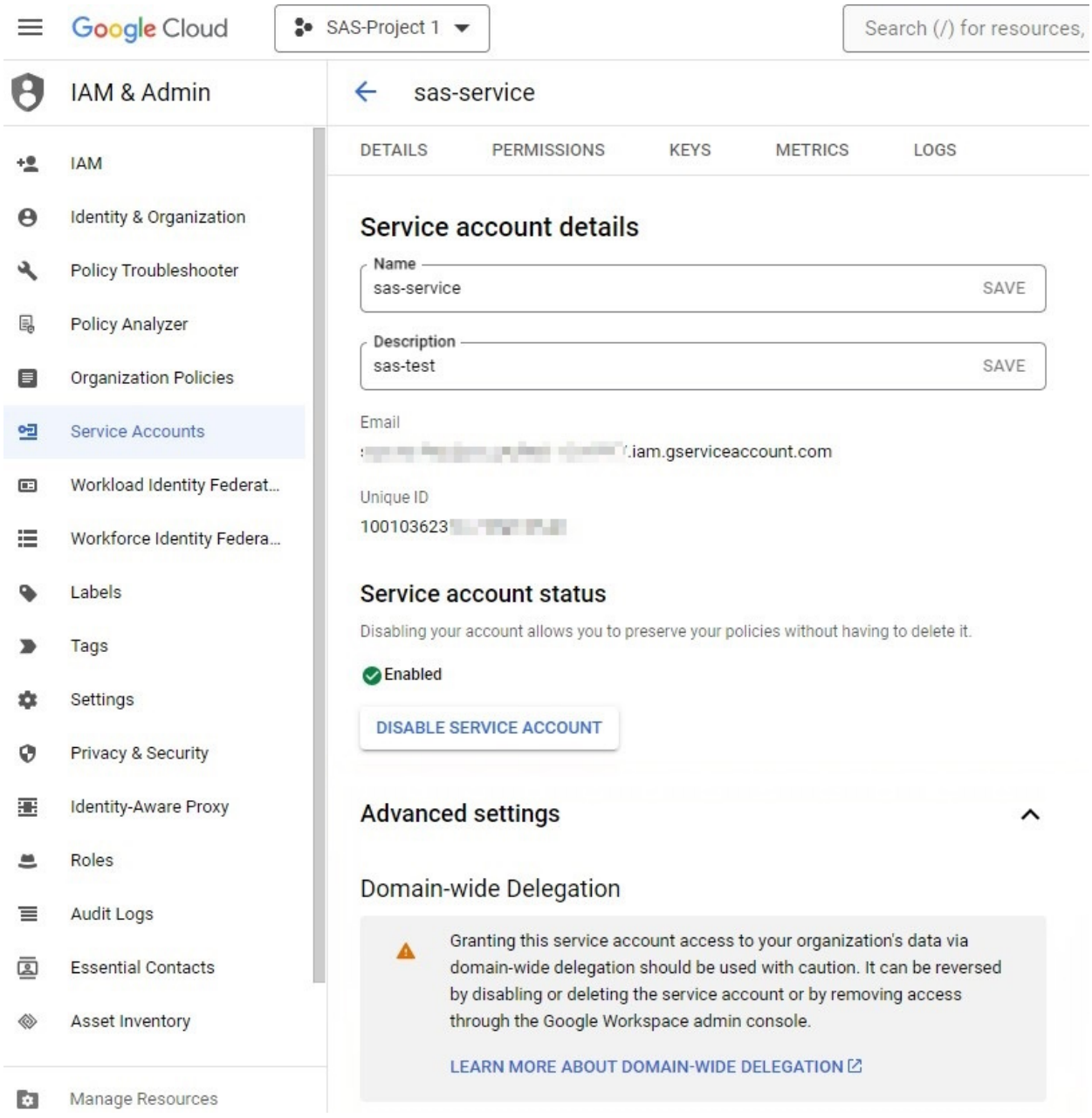


**e.** Save the private key and note the private key password, "notasecret".




> 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.

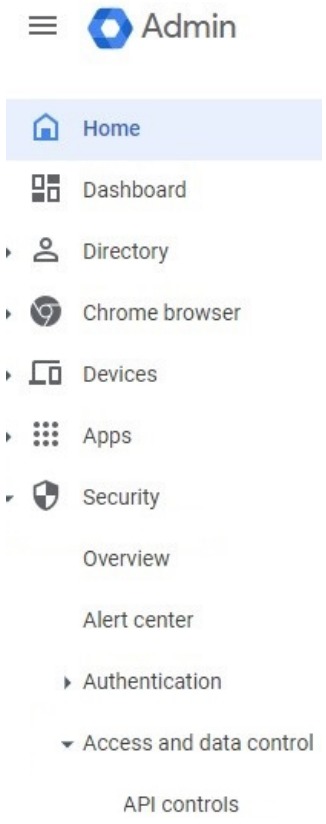
```
C:\OpenSSL-Win64\bin>openssl pkcs12 -in demo-976b9d6e9328.p12 -out
      serviceAccount-demo.pem -nodes -nocerts
Enter Import Password:
```

# Delegating domain-wide authority to the service account

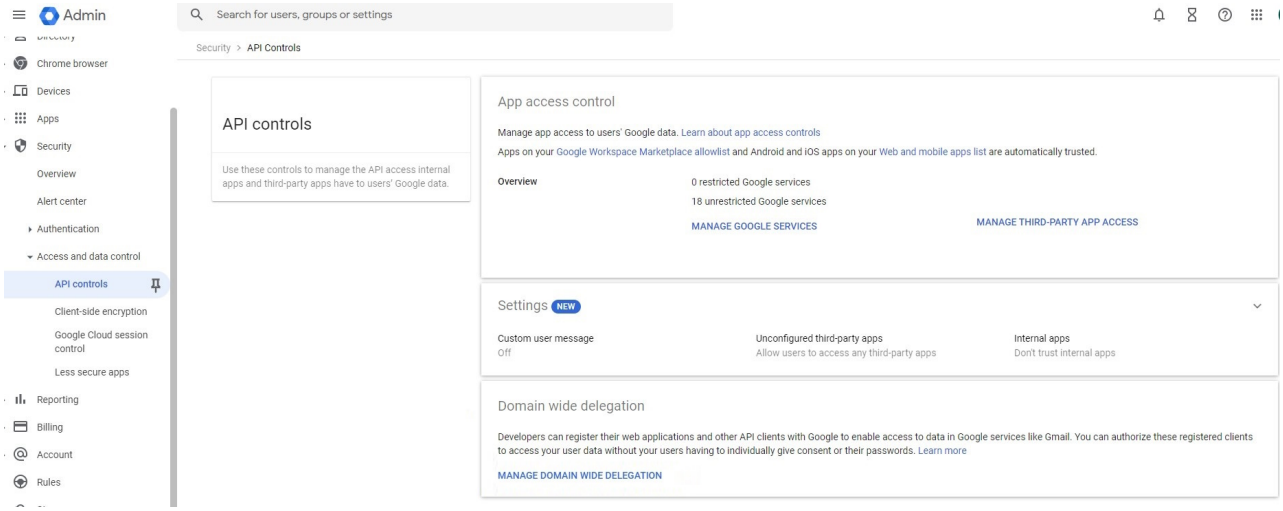
This section describes how to delegate domain-wide authority to the service account in the Google Admin console. These settings allow Google to trust FortiClient EMS, which enables FortiClient EMS to retrieve information from the Google domain.

**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*.



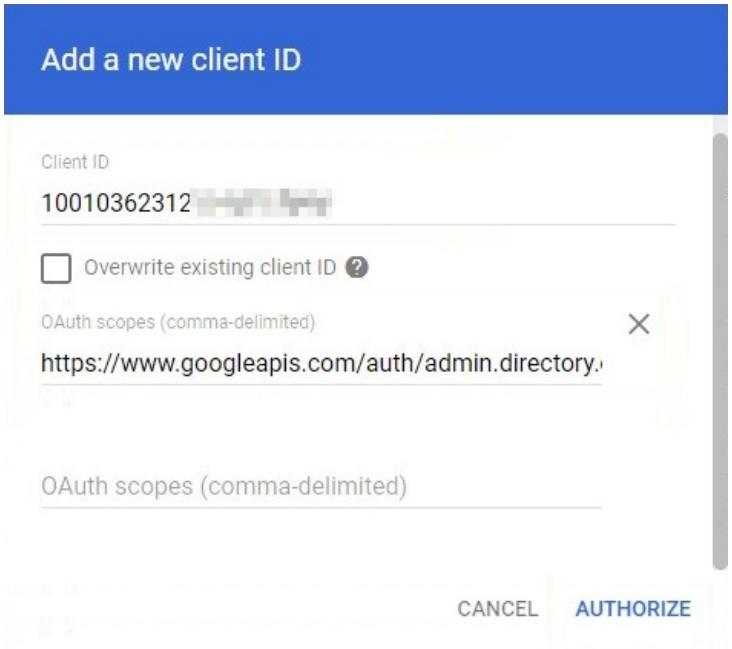
2. Click *Manage Domain Wide Delegation*, then click *Add New*.




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 51
- Communication with FortiAnalyzer for logging on page 51

It includes the following procedures:

- Required: Adding an SSL certificate to FortiClient EMS for Chromebook endpoints on page 65
- Required only when sending logs to FortiAnalyzer: Adding SSL certificates to FortiAnalyzer on page 66

# 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.

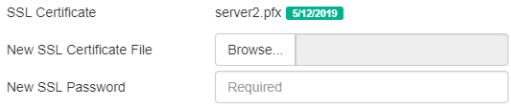
If you are using a public SSL certificate, add the certificate to FortiClient EMS. You do not need to add the certificate to the Google Admin console.

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 51.

**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.



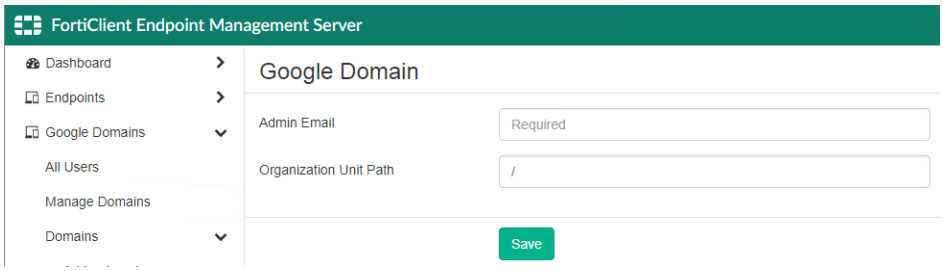

# Adding SSL certificates to FortiAnalyzer

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:**

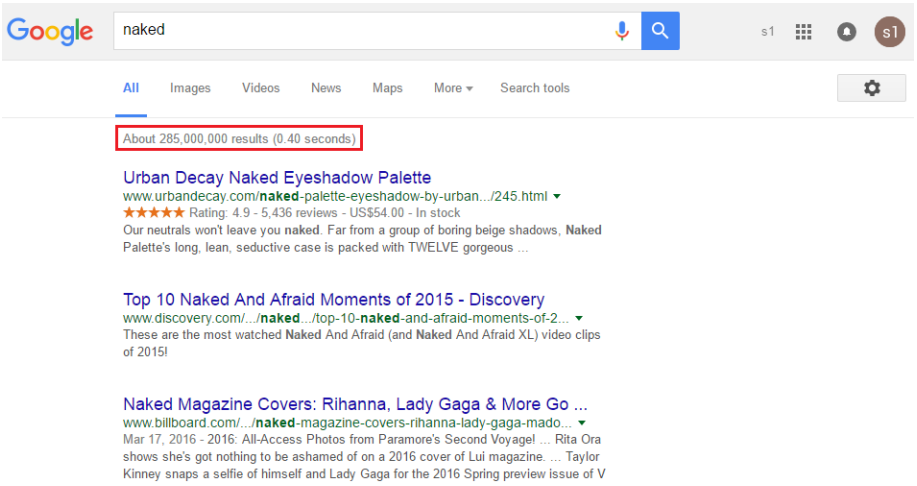
1. Go to *Endpoint Profiles*.
2. Go to *Web Filter* or *System Settings*.
3. Click *Add*, then click *Add Chrome Profile*.
4. Configure the profile as desired.
5. Click *Save*.

# Enabling and disabling Safe Search

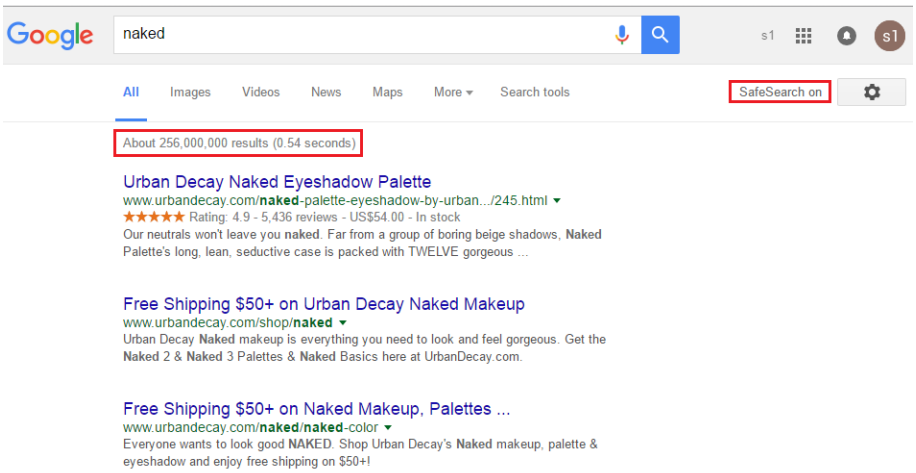
The search engine provides a Safe Search feature that blocks inappropriate or explicit images from search results. The Safe Search feature helps avoid most adult content. FortiClient EMS supports Safe Search for most common search engines, such as Google, Yahoo, and Bing.

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.<br>You must have already created a profile to include one in an endpoint policy. See Adding a new Chromebook profile on page 67. |
| **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

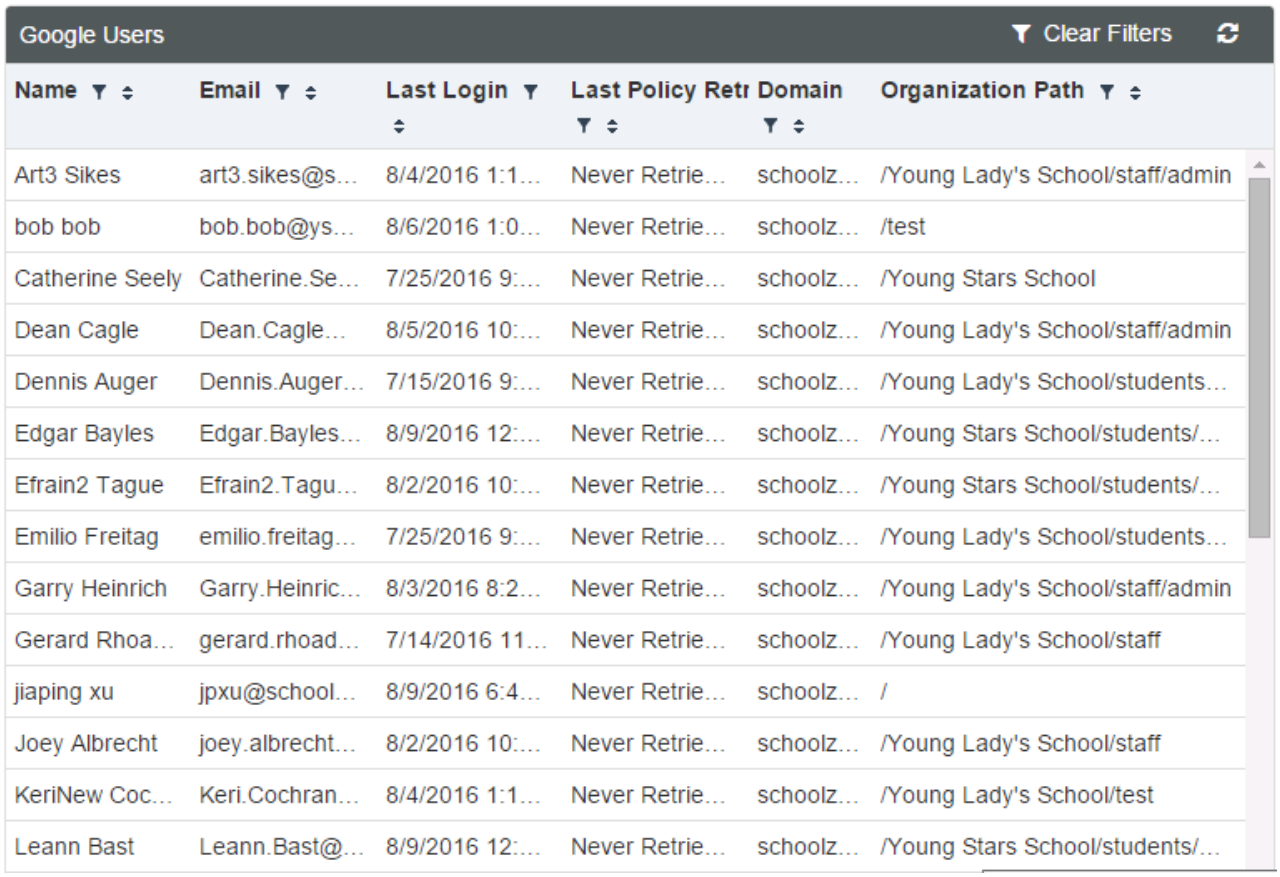
After you add domains to FortiClient EMS, you can view the list of domains in *Google Domains*. You can also view the list of Google users in each domain and details about each Google user in the *User Details*, *Client Statistics*, and *Blocked Sites* panes.

# 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. |

# Troubleshooting IPsec VPN IKEv2 with SAML authentication

This document focuses on multiple scenarios of IPsec VPN IKEv2 with SAML authentication failures. This document provides details regarding FortiGate diagnostics and FortiClient log highlights.

When troubleshooting IPsec VPN IKEv2 SAML authentication failures, use the following logs for troubleshooting:

- FortiClient diagnostics
- FortiGate CLI diagnostics
- FortiGate system events (VPN events)

The following provides the FortiOS commands to enable debugging to view the aforementioned logs for troubleshooting:

```
diagnose debug reset
diagnose debug console timestamp enable
diagnose debug app ike -1
diagnose debug app fnbamd -1
diagnose debug enable
```

You can also complete the diagnostics with the following commands, depending on your use case:

```
diagnose debug app eap_proxy -1
diagnose debug app authd -1
diagnose debug app samld -1
```

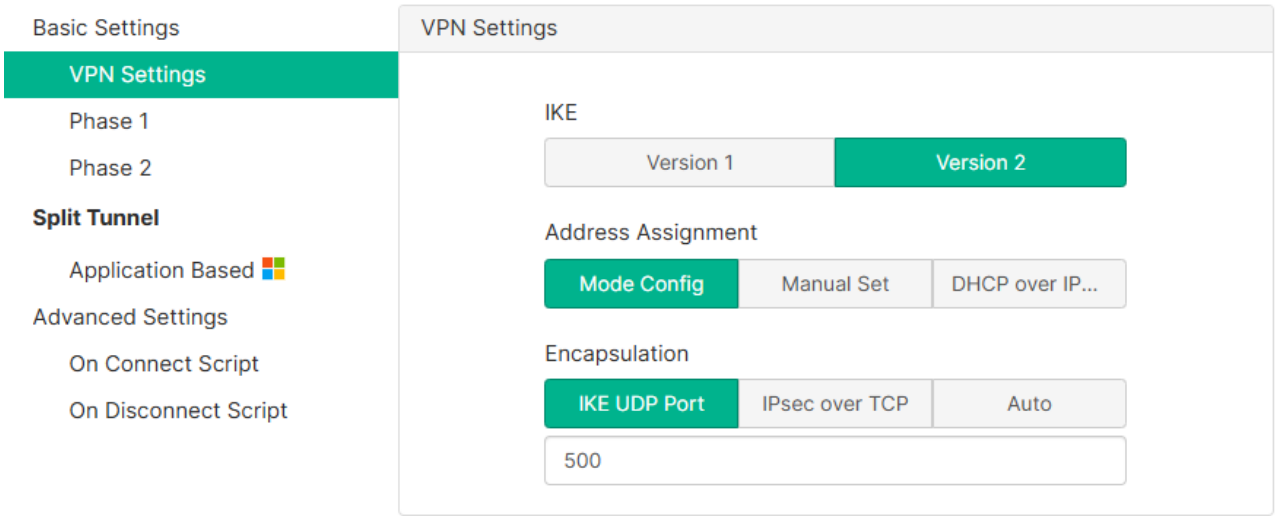
# Verifying SAML configuration

Verify that SAML is configured correctly on EMS and FortiOS.

**To verify the SAML configuration on EMS:**

1. In EMS, go to *Endpoint Profiles* > *Remote Access*.
2. Edit the desired profile.
3. Under *VPN Tunnels*, edit the desired IPsec VPN tunnel.

4. In *Basic Settings* > *VPN Settings*, confirm that *Version 2* is selected under *IKE*.




5. Go to *Advanced Settings*.
6. Confirm that *EAP* is enabled.
7. Confirm that *Enable SAML Login* is toggled on and that you defined a custom port in *SAML Port*.

**To verify the SAML configuration in FortiOS:**

1. Confirm that `auth-ike-saml-port` is configured under `config system global` and matched to SAML port defined on EMS.
2. Ensure that the SAML user group is referenced in the firewall IPsec VPN policy or under `config vpn ipsec phase1-interface` as the `authusrgrp` parameter.
3. Confirm that the SAML server is mapped to an external port serving VPN connections, such as the WAN interface:

```
config system interface
       edit "port1"
               set ike-saml-server "<SAML server>"
       next
end
```

4. Verify that EAP is enabled:

```
config vpn ipsec phase1-interface
       set eap enable
       set eap-identity send-request
end
```

For a complete configuration guide, see IPsec VPN SAML-based authentication.

# IPsec VPN SAML connection sequence

Understanding the sequence of the IPsec SAML connection process is crucial before beginning troubleshooting. See SAML-based authentication for FortiClient remote access dialup IPsec VPN clients.

# Troubleshooting use cases

The majority of failures are results of misconfiguration. Therefore, it is critical to verify your SAML configuration prior to troubleshooting. See Verifying SAML configuration on page 73.

## PSK mismatch

Peer authentication via a preshared key (PSK) occurs during the IKE_AUTH phase (`exchange=AUTH` in FortiGate IKE diagnostics).

If there is a PSK mismatch, the authentication process between FortiClient and FortiGate does not proceed beyond AUTH exchange.

In this case, the FortiGate IKE debug logs ends at `AUTH_RESPONSE`:

```
ike V=root:0:FSTP_SAML:33: received FCT-UID : 2665C39D4EE1467383FB49594AF45B38
ike V=root:0:FSTP_SAML:33: received EMS SN : FCTEMS8825002288
ike V=root:0:FSTP_SAML:33: received EMS tenant ID : 00000000000000000000000000000000
ike V=root:0:FSTP_SAML:33: re-validate gw ID
ike V=root:0:FSTP_SAML:33: gw validation OK
ike V=root:0:FSTP_SAML:33: responder preparing EAP identity request
ike 0:FSTP_SAML:33: enc
2700000C010000000A80CCE03000002802000000FCAFD5785CFDFC91EC4C6C4F3DE8F191DB3097928025144317E1A3F51F
1F23740000000901960005010201 02
ike 0:FSTP_SAML:33: out F6F0BE78E3ECDF1D55FC35815C84...
ike V=root:0:FSTP_SAML:33: sent IKE msg (AUTH_RESPONSE): 10.128.204.224:500->10.10.11.2:500,
len=128, vrf=0, id=f6f0be78e3ecdf1d/55fc35815c843162:00000001, oif=5
diag debug disable
```

This is because the FortiClient does not follow up in the authentication process due to authentication failure:

```
[FortiIKE  4553   debug] 0:FSTP IPsec (SAML):0: initiator received AUTH msg
[FortiIKE  1224   debug] 0:FSTP IPsec (SAML):0: peer identifier IPV4_ADDR 10.128.204.224
[FortiIKE  1494   debug] ikev2_verified: iph1 0x0000022290B63A80 auth verify done
[FortiIKE  4738   debug] 0:FSTP IPsec (SAML):0: initiator AUTH continuation
[FortiIKE  4765   debug] 0:FSTP IPsec (SAML):0: authentication failed
[FortiIKE  481   debug] 0:FSTP IPsec (SAML):0: schedule delete of IKE SA
```

```
f6f0be78e3ecdf1d:55fc35815c843162 iph1 0x0x0000022290B63A80
[FortiIKE  481   debug] 0:FSTP IPsec (SAML):0: schedule delete of IKE SA
f6f0be78e3ecdf1d:55fc35815c843162 iph1 0x0x0000022290B63A80
```

**To resolve this issue:**

Ensure that the PSK is identical between the FortiGate and FortiClient.

On newer FortiOS versions, you can download a FortiClient-compatible XML file for each IPsec VPN tunnel using the *Download tunnel XML* button. You can then insert this XML into EMS to ensure that the PSK value is the same between your FortiGate and FortiClient.

# EAP response is empty

You may observe the following error due to user group misconfiguration.

```
ike V=root:0:FSTP_SAML:53: initiating EAP authentication
ike V=root:0:FSTP_SAML: EAP user "2665C39D4EE1467383FB49594AF45B38"
ike V=root:0:FSTP_SAML: EAP failed for user "2665C39D4EE1467383FB49594AF45B38"
ike V=root:0:FSTP_SAML: EAP response is empty
ike V=root:0:FSTP_SAML: connection expiring due to EAP failure
```

**To resolve this issue:**

Do one of the following in FortiOS:

- In the applicable IPsec VPN firewall policy, reference the applicable user group.
- In the CLI, configure the applicable user group under `config vpn ipsec phase1-interface` as follows:

```
config vpn ipsec phase1-interface
       edit <name>
               set authusrgrp "<SAML user group>"
       next
end
```

Do not apply both of the listed configurations.

# gw validation failed

There can be multiple reasons for this error and most of them are configuration-related. Therefore, once observed, it is critical to verify your SAML configuration prior to troubleshooting. See Verifying SAML configuration on page 73.

```
ike V=root:0:FSTP_SAML:41: gw validation failed
ike V=root:FSTP_SAML Negotiate SA Error: gateway validation failed
```

## Local or peer ID misconfiguration

Ensure that the local ID defined on EMS matches `peerid` on the FortiGate.

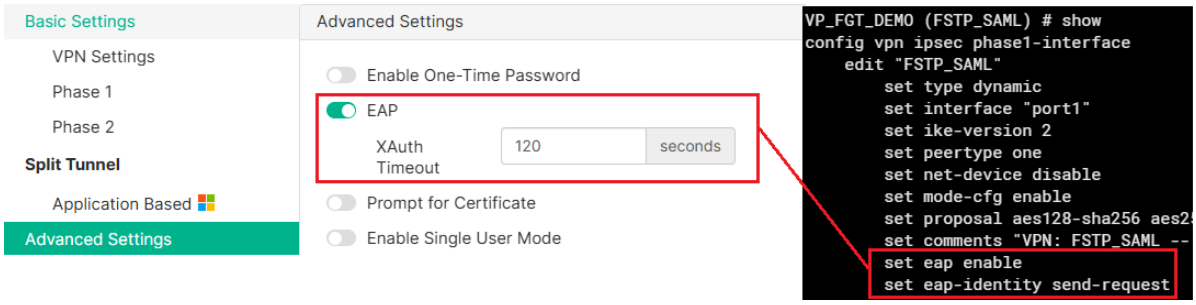
**To verify the local and peer ID configuration:**

1. In EMS, go to *Endpoint Profiles* > *Remote Access*.
2. Edit the desired profile.
3. Under *VPN Tunnels*, edit the desired IPsec VPN tunnel.
4. In *Phase 1*, observe the value under *Local ID*.
5. In FortiOS, run the following commands. Confirm that the value in `set peerid` matches the local ID configured on EMS:

```
config vpn ipsec phase1-interface
       edit <name>
       show
```

## EAP misconfiguration

When EAP is disabled in EMS or the FortiGate, FortiGate IKE diagnostics may present `gw validation failed` error. Ensure that EAP is enabled for both EMS and FortiOS. See Verifying SAML configuration on page 73.




# No SAML method found

When FortiClient does not open a browser for SAML authentication and simply reverts to login, include `diagnose debug app authd -1` in the FortiGate diagnostics.

An error like this may appear:

```
[authd_local_saml_auth:5844]: SAML login with UID '2665C39D4EE1467383FB49594AF45B38'.
[authd_local_saml_auth:5857]: No SAML method found.
```

**To resolve this issue:**

Ensure that the FortiGate interface that acts as a first point of contact for incoming traffic from the FortiClient dialup connections has `set ike-saml-server` configured. This interface may or may not be the WAN interface.

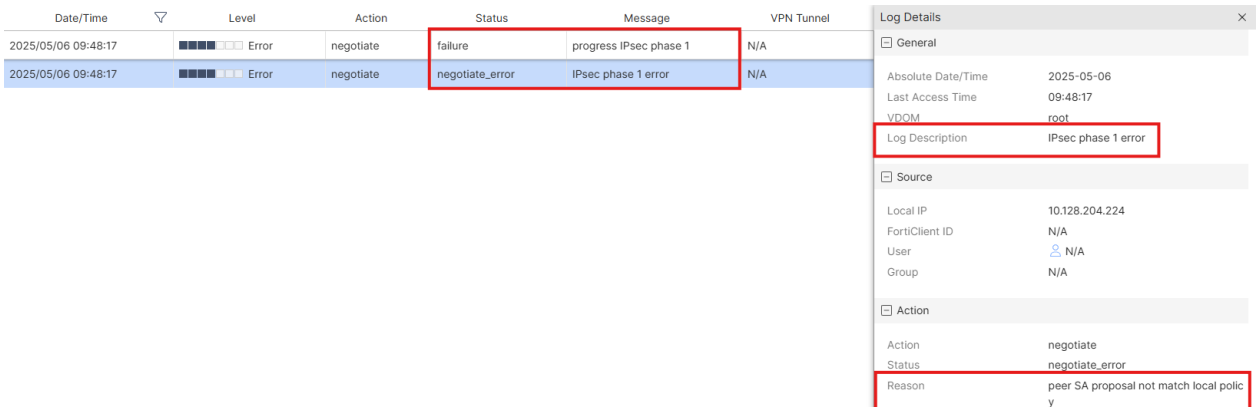
# No proposal chosen

This error may appear during two phases of IKEv2 connection - IKE_SA_INIT (phase 1 configuration on FortiClient) and IKE_AUTH (phase 2 configuration on FortiClient).

The following shows an example of the FortiOS CLI output for this issue:

```
ike V=root:0:d8196d424283cd4e/0000000000000000:36: no proposal chosen
ike V=root:d8196d424283cd4e/0000000000000000 Negotiate SA Error: peer SA proposal not match local
policy
ike V=root:0:d8196d424283cd4e/0000000000000000:36: no proposal chosen, send error response
```

The following shows an example of a VPN *System Event* log view showing IPsec VPN phase 1 (IKE_SA_INIT) negotiation failure. A similar message shows for phase 2.



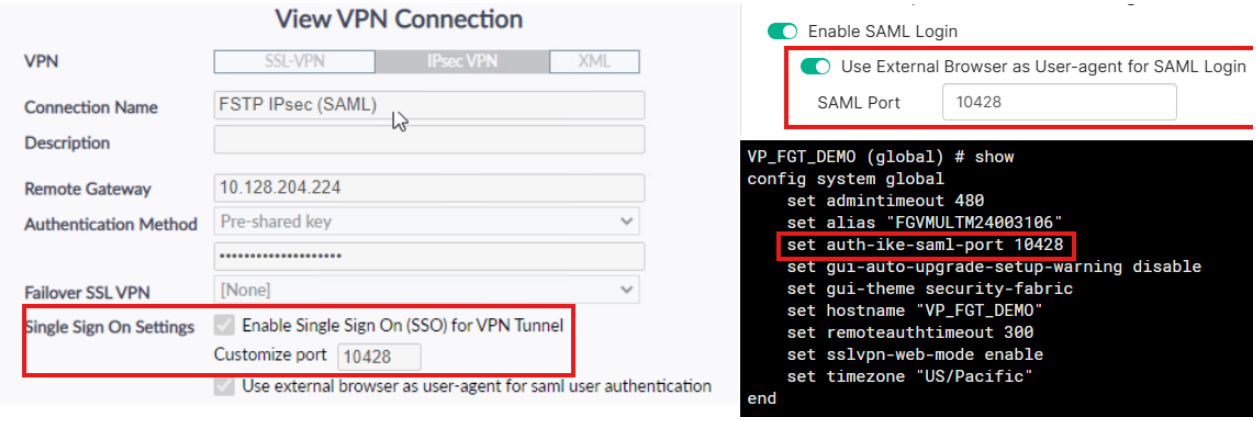

**To resolve this issue:**

1. Validate that the IPsec VPN tunnels have IKEv2 enabled on EMS and FortiOS.
2. Ensure that the incoming SA (FortiClient IKE proposal) is accurately matched to the phase 1 configuration under `config vpn ipsec phase1-interphase` on FortiGate.
3. Verify the security parameters of phase 1 SAs match on FortiClient and FortiGate.
4. Verify the security parameters of phase 2 SAs match on FortiClient and FortiGate.

# Browser issues

When user clicks *Connect*, FortiClient sends a request to the FortiGate port defined by `auth-ike-saml-port` as SAML-based authentication for FortiClient remote access dialup IPsec VPN clients describes.

When the browser does not open, FortiClient gets stuck, or no authentication window displays, it can mean `auth-ike-saml-port` is misconfigured or, more generally, FortiClient fails to reach the FortiGate over that port.




The web framework used for SAML authentication affects the logs. See Technical Tip: FortiClient SAML Authentication Configuration Demystified. Depending on the framework used, verify the following logs:

# External browser

## FortiTray

```
[580:12804] [fortitray  220   debug] SamlAuth::QueryIpsecSamlDataExtBrowser() called.
[580:12804] [fortitray  4713   error] CFortiTrayDlg::RequestMissingVPNCredentials() could not get
saml data.
[580:12804] [fortitray  4753   debug] CFortiTrayDlg::RequestMissingVPNCredentials() ends. res=3
[580:7416] [fortitray  192   debug] cbPIPEMSG_VPN_CONNECTION_ERROR 2053
```

## FortiTray.exe_FortiAuth.log

```
[580:12804] [FortiAuth  101   error] GetHttpResponse() WinHttpSendRequest failed.
[580:12804] [FortiAuth  458   error] QueryIpsecExtBrowserSamlStartUrl() could not extract the
start url in response.()
[580:12804] [FortiAuth  528   error] GetIpsecSamlDataExternalBrowser() Failed to get ipsec saml
external browser start url.
```

# WebView2

## FortiTray

```
[2025-05-07 11:25:05.7873592 UTC-07:00] [7804:11976] [fortitray  251   debug]
SamlAuth::PickSamlAuthProvider() saml auth provided: 0
[2025-05-07 11:25:13.6196951 UTC-07:00] [7804:8008] [fortitray  311   info]
SamlAuth::QuerySamlData::<lambda_2737bdf304228843c31873ebb86af054>::operator ()() Response
```

```
returned.
[2025-05-07 11:25:13.6197081 UTC-07:00] [7804:8008] [fortitray  350   debug]
SamlGetResponse=0xa7000006
[2025-05-07 11:25:13.6197098 UTC-07:00] [7804:8008] [fortitray  359   error]
SamlAuth::QuerySamlData() Get Saml Response ERROR ret=0xa7000006
[2025-05-07 11:25:13.6199290 UTC-07:00] [7804:8008] [fortitray  4591   debug]
CFortiTrayDlg::StartIPSecSAML() lRet=0xa7000006
[2025-05-07 11:25:13.6199343 UTC-07:00] [7804:8008] [fortitray  4593   error] QuerySamlData()
failed. lRet=0xa7000006
```

**FortiTray.exe_FortiAuth.log**

```
[7804:11692] [FortiAuth  228   debug] RunFortiAuthInSession() CMD to start auth module:  --
provider-name=WebView2 --receiver=2844  --object="saml:ipsecvpn:2665C39D4EE1467383FB49594AF45B38"
--object-name="FSTP IPsec (SAML)" --url="https://10.128.204.224:10429/saml_login?" --
description="FortiClient SAML Authentication" --ignore-certificate=1 --timeout=300 --delete-
cookies
[7804:11692] [FortiAuth  245    info] CreateProcessW() returned 1
[7804:11692] [FortiAuth  248   debug] Process Id: 3584
[7804:11692] [FortiAuth  292    info] Caller deliberately terminates auth process.
[7804:11692] [FortiAuth  224   error] RunFortiAuthInSession=0xa7000007
[7804:11692] [FortiAuth  261    info] SamlGetResponseUsingExternalAuthProvider exit with
HRESULT=0x0xa7000007
```

# Electron

## FortiTray.exe_FortiAuth.log

```
[7804:7224] [FortiAuth  228   debug] RunFortiAuthInSession() CMD to start auth module:  --
provider-name=Electron --receiver=2936  --
object="saml:ipsecvpn:2665C39D4EE1467383FB49594AF45B38" --object-name="FSTP IPsec (SAML)" --
url="https://10.128.204.224:10429/saml_login?" --description="FortiClient SAML
Authentication" --ignore-certificate=1 --timeout=300 --delete-cookies
[7804:7224] [FortiAuth  245    info] CreateProcessW() returned 1
[7804:7224] [FortiAuth  248   debug] Process Id: 6316
[7804:7224] [FortiAuth  276   debug] Daemon exit code: 0xa7000006
[7804:7224] [FortiAuth  234   debug] decode base64 to cipher binary, cipher len=304
[7804:7224] [FortiAuth  224   error] RunFortiAuthInSession=0xa7000006
[7804:7224] [FortiAuth  261    info] SamlGetResponseUsingExternalAuthProvider exit with
HRESULT=0x0xa7000006
```

## FortiTray

```
[7804:8008] [fortitray  4573   debug] CFortiTrayDlg::StartIPSecSAML() connection_name=FSTP
IPsec (SAML) remote_gateway=10.128.204.224 dwSSOPort=10429
[7804:8008] [fortitray  231   debug] szRetUrl=https://10.128.204.224:10429/saml_login?
```

```
[7804:8008] [fortitray  301   debug] Reset cancel event.
[7804:7224] [fortitray  36   debug] ThreadGetResponse() called.
[7804:7224] [fortitray  251   debug] SamlAuth::PickSamlAuthProvider() saml auth provided: 1
[7804:8008] [fortitray  311    info] SamlAuth::QuerySamlData::<lambda_
2737bdf304228843c31873ebb86af054>::operator ()() Response returned.
[7804:8008] [fortitray  350   debug] SamlGetResponse=0xa7000006
[7804:8008] [fortitray  359   error] SamlAuth::QuerySamlData() Get Saml Response ERROR
ret=0xa7000006
[7804:8008] [fortitray  4591   debug] CFortiTrayDlg::StartIPSecSAML() lRet=0xa7000006
[7804:8008] [fortitray  4593   error] QuerySamlData() failed. lRet=0xa7000006
```

### samlauth.log

```
[info]  doSAMLConnect - saml_auth_request={"saml_auth_
url":"https://10.128.204.224:10429/saml_login?","saml_auth_
object":"saml:ipsecvpn:2665C39D4EE1467383FB49594AF45B38","saml_auth_object_name":"FSTP IPsec
(SAML)","saml_auth_ignore_certificate":1,"saml_auth_timeout":"300","saml_auth_
description":"FortiClient SAML Authentication","saml_auth_delete_cookies":true,"saml_auth_
receiver":"2936"}
[info]  deleteSAMLTunnelCookies tunnel_name=FSTP IPsec (SAML) tunnel_type=ipsecvpn
[info]  deleteSAMLTunnelCookies tunnel_cookies=
[info]  doSAMLConnect saml_auth_request={"saml_auth_url":"https://10.128.204.224:10429/saml_
login?","saml_auth_object":"saml:ipsecvpn:2665C39D4EE1467383FB49594AF45B38","saml_auth_
object_name":"FSTP IPsec (SAML)","saml_auth_ignore_certificate":1,"saml_auth_
timeout":"300","saml_auth_description":"FortiClient SAML Authentication","saml_auth_delete_
cookies":true,"saml_auth_receiver":"2936"}
[info]  SAMLAUTH - openURL url=https://10.128.204.224:10429/saml_login?
type=saml:ipsecvpn:2665C39D4EE1467383FB49594AF45B38
[info]  SAMLAUTH - loadUrlWithType Obj=saml:ipse url=https://10.128.204.224:10429/saml_login?
[info]  load ipsec saml uid=2665C39D4EE1467383FB49594AF45B38
[info]  SAMLAUTH - did-fail-load errorCode=-118 errorDescription=ERR_CONNECTION_TIMED_OUT
validatedURL=https://10.128.204.224:10429/saml_login?
[info]  saveSAMLResponse saml_auth_receiver=2936 saml_response.length=282
[info]  SAMLAUTH - exit with code=-1493172218
```

## Web browser

### FortiTray

```
[fortitray  251   debug] SamlAuth::PickSamlAuthProvider() saml auth provided: 2
[fortitray  311    info] SamlAuth::QuerySamlData::<lambda_
2737bdf304228843c31873ebb86af054>::operator ()() Response returned.
[fortitray  350   debug] SamlGetResponse=0xa7000000
[fortitray  353   error] FCT_AUTH_UNKNOWN, tries=0
[fortitray  359   error] SamlAuth::QuerySamlData() Get Saml Response ERROR ret=0xa7000000
```

### FortiAuth.log

```
[FortiAuthExe] [Info] [4594s] [4594:1] Auth start
[FortiAuthExe] [Info] --provider-name=WebBrowser
[FortiAuthExe] [Info] --receiver=2796
[FortiAuthExe] [Info] --object=saml:ipsecvpn:2665C39D4EE1467383FB49594AF45B38
[FortiAuthExe] [Info] --object-name=FSTP IPsec (SAML)
[FortiAuthExe] [Info] --url=https://10.128.204.224:10429/saml_login?
[FortiAuthExe] [Info] --description=FortiClient SAML Authentication
[FortiAuthExe] [Info] --ignore-certificate=1
[FortiAuthExe] [Info] --timeout=300
[FortiAuthExe] [Info] --delete-cookies
[FormSamlAuth] [Info] WebBrowserMajorVersion=11
[FormSamlAuth] [Info] ShowForm=False
[FormSamlAuth] [Error] Program.FCT_AUTH_UNKNOWN->The operation has timed out
```

### FortiTray.exe_FortiAuth.log

```
[FortiAuth  228   debug] RunFortiAuthInSession() CMD to start auth module:  --provider-
name=WebBrowser --receiver=2796  --object="saml:ipsecvpn:2665C39D4EE1467383FB49594AF45B38" --
object-name="FSTP IPsec (SAML)" --url="https://10.128.204.224:10429/saml_login?" --
description="FortiClient SAML Authentication" --ignore-certificate=1 --timeout=300 --delete-
cookies
[FortiAuth  245    info] CreateProcessW() returned 1
[FortiAuth  248   debug] Process Id: 1304
[FortiAuth  276   debug] Daemon exit code: 0xa7000000
[FortiAuth  234   debug] decode base64 to cipher binary, cipher len=0
[FortiAuth  285   error] Could not decrypt saml data. nRet=-10
[FortiAuth  224   error] RunFortiAuthInSession=0xa7000000
```

# SAML authentication issues

Most authentication issues, if not on the identity provider (Microsoft Entra ID, Okta, FortiAuthenticator, and so on) side are group-related, such as a group mismatch, unless EAP is misconfigured, as in EAP response is empty.

When troubleshooting SAML authentication issues, ensure to include the following FortiGate CLI commands on top of `ike` diagnostics:

```
diagnose debug app fnbamd -1
diagnose debug app samld -1
```

# Change log

| Date | Change description |
| --- | --- |
| 2026-03-17 | Initial release. |

www.fortinet.com