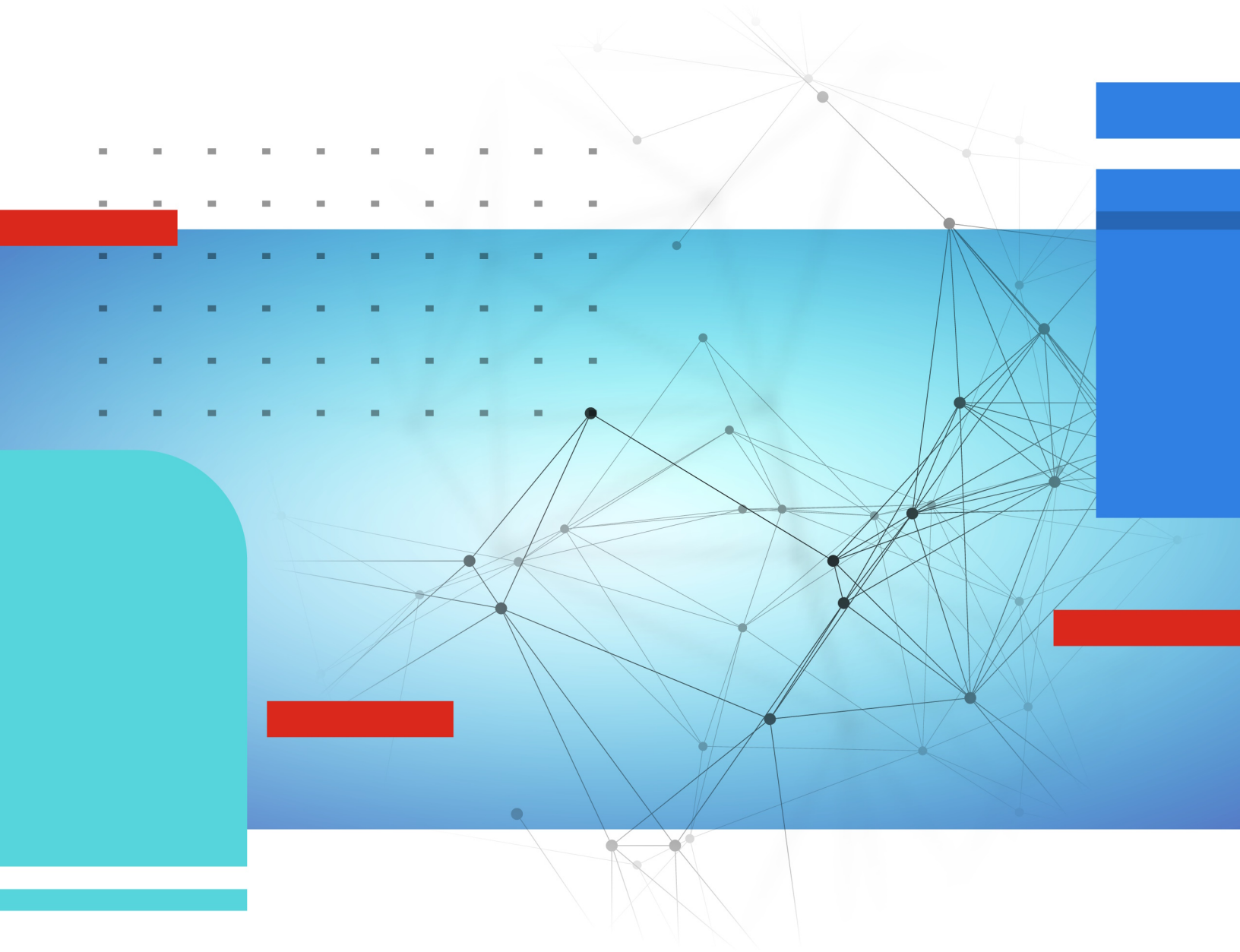
Deployment Guide

FortiClient Cloud 25.2



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

February 13, 2026
FortiClient Cloud 25.2 Deployment Guide
04-252-1134986-20260213

TABLE OF CONTENTS

Introduction **4**
Requirements 5
Licensing 6
Product integration and support 7
Deploying FortiClient Cloud **8**
Managing endpoints using FortiClient Cloud **10**
Adding a FortiClient deployment package 10
Installing FortiClient Cloud on an endpoint and registering to FortiClient Cloud EMS 12
Connecting an endpoint to FortiClient Cloud 13
Adding a new invitation for a deployment package 16
Customizing invitation code email content 17
Managing Chromebooks with FortiClient Cloud 18
Accounts **19**
Adding a secondary admin account 19
IAM users 20
API access keys **21**
Upgrading FortiClient Cloud **23**
Allowlisting the FortiClient Cloud IP addresses **27**
Communication from endpoints to FortiClient Cloud 27
Communication from FortiClient Cloud to endpoints 27
Notifications **28**
System maintenance 28
Targeted notifications 29
Managing notifications in the FortiClient Cloud portal 30
Using the Fortinet email server for sending alerts **33**
Limitations **34**
Privacy **37**
Backup and restore strategy **39**
Local reliability 39
Disaster recovery 39
Change log **40**

Introduction

A cloud-based software-as-a-service endpoint management service called FortiClient Cloud is available. This is a Fortinet-hosted EMS solution.

You can execute EMS functions from the cloud-based EMS. You must complete the following steps to create a cloud-based EMS instance under your FortiCloud user account:

1. Register a FortiClient Cloud subscription to your FortiCloud account.
2. Register a FortiClient Cloud license contract for management by FortiClient Cloud to your FortiCloud account.

The management capacity data for the latest EMS 7.4 or 7.2 version applies to FortiClient Cloud depending on your instance. See the management capacity for your instance:

- 7.4
- 7.2

You can use FortiClient Cloud to manage the following FortiClient Cloud endpoint types:

- Windows
- macOS
- Linux
- iOS
- Android
- Chromebook

FortiClient Cloud 25.2 runs EMS 7.4 or 7.2.

FortiClient Cloud is hosted in the following regions:

- North America:
  - United States:
    - San Jose
    - Plano
  - Toronto
  - Vancouver
- EMEA:
  - Frankfurt
  - Madrid
  - U.K.:
    - London
- APAC:
  - Tokyo
  - Sydney
  - Singapore

- Middle East:
  - Dubai

All customer FortiClient Cloud data, including backup instances for redundancy or data recovery, are kept in the region selected when provisioning the cloud instance.

This guide only provides information specific to FortiClient Cloud. For information about EMS features that this guide does not include, see the *EMS Administration Guide*:
- 7.2
- 7.4

You can use the FortiClient Cloud Service monitoring site to check the status of the FortiClient Cloud service and any scheduled maintenance times.

FortiClient Cloud is ISO/IEC 27001 certified. See ISO 27001 compliance standard.

Requirements

The following items are required before you can initialize your FortiClient Cloud Cloud instance:

Requirement	Description
FortiCloud account with FortiClient Cloud subscription	Create a FortiCloud account if you do not have one and register a FortiClient Cloud subscription to this account. Launching FortiClient Cloud requires a primary FortiCloud account with a FortiClient Cloud subscription. A primary FortiCloud account with a FortiClient Cloud subscription can invite other users to launch FortiClient Cloud. Each FortiCloud account that will access FortiClient Cloud must be registered with its own FortiClient Cloud subscription. See Deploying FortiClient Cloud on page 8.
Internet access	You must have Internet access to create a FortiClient Cloud Cloud instance.
Browser	Device with a browser to access FortiClient Cloud Cloud.

If you are using a new FortiCloud account:

- If the account has a FortiClient Cloud subscription and an endpoint license (ZTNA/VPN or EPP/ATP), you can launch a FortiClient Cloud instance.
- If the account has only a FortiClient Cloud subscription, you can launch a FortiClient Cloud instance that can manage up to three endpoints.

If you are using an existing FortiCloud account with a FortiClient Cloud instance that was launched prior to the FortiClient Cloud subscription requirement, the FortiClient Cloud instance continues to run without the FortiClient Cloud subscription.

Licensing

FortiClient Cloud requires the following licenses:

- **FortiClient Cloud subscription:** Each FortiCloud account that will access FortiClient Cloud must be registered with its own FortiClient Cloud subscription.
- **Per-endpoint or per-user licensing:** FortiClient Cloud supports per-endpoint and per-user licensing. You cannot use both license types on one FortiClient Cloud environment. You must select per-endpoint or per-user licensing. You must purchase a license for each endpoint or user that FortiClient Cloud will manage. Purchase the following FortiClient license types from Fortinet. All licenses are available for both per-endpoint and per-user licensing:
  - Zero Trust Network Access (ZTNA)
  - Endpoint Protection Platform/Advanced Persistent Threat
  - Managed Endpoint Security Services
  - FortiGuard Endpoint Forensic Analysis. See Requesting forensic analysis on an endpoint.
  - Endpoint Detection & Response (EDR)
  - Extended Detection & Response (XDR)

  When registering the license contract, you must specify that the endpoints or users will be managed using FortiClient Cloud, as Deploying FortiClient Cloud on page 8 describes.

  Registering a ZTNA license for FortiClient Cloud management does not support all features supported for on-premise EMS. See Limitations on page 34 for the list of supported features.

FortiClient Cloud is available in the following locations:

- U.S.
- Canada
- Europe
- U.K.
- Japan
- Australia

Product integration and support

FortiClient Cloud Cloud supports the following products:

- FortiClient Cloud:
  - 7.0.0 and later versions
  - 6.4.4 and later versions
- FortiOS:
  - 7.0.0 and later versions
  - 6.4.0 and later versions
- FortiAnalyzer:
  - 7.0.0 and later versions
  - 6.4.0 and later versions

To import a profile from FortiManager to FortiClient Cloud, FortiManager must be reachable over the public Internet.

FortiClient Cloud is a component of FortiSASE, a cloud-based SaaS service that offers protection for remote, off-net endpoints. FortiSASE only works with a new FortiClient Cloud instance. You cannot apply a FortiSASE license to an existing FortiClient Cloud instance. See the FortiSASE documentation.

Deploying FortiClient Cloud

This topic explains how to deploy FortiClient Cloud. This topic assumes that you already purchased the desired subscription licenses for your deployment from a Fortinet partner or reseller and received your license activation codes.

You can create only one FortiClient Cloud instance per FortiCloud account.

To deploy FortiClient Cloud:

1. Register the FortiClient Cloud subscription contract to your FortiCloud account:
   a. On the Customer Service & Support site, go to *Asset Management* > *Register Now*.
   b. In the *Registration Code* field, enter your license activation code and select *Next* to continue registering the product.
   c. Enter your details in the other fields and complete the registration. This is a yearly subscription.

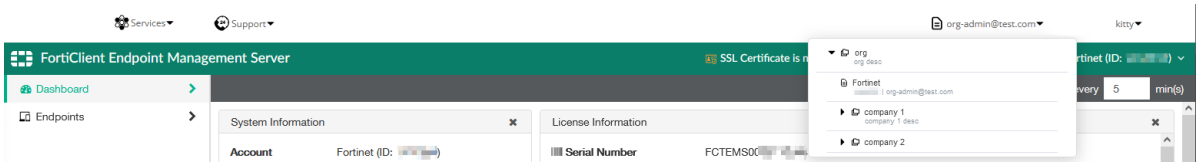
   You may need to wait a few minutes for the cloud instance to initialize before you can proceed to step 2 or 3.

2. Register the FortiClient Cloud endpoint licenses for management by FortiClient Cloud:
   a. On the Customer Service & Support site, go to *Asset Management* > *Register Now*.
   b. In the *Registration Code* field, enter your license activation code and select *Next* to continue registering the product.
   c. Select the *Used for Cloud Purpose* checkbox.
   d. Enter your details in the other fields and complete the registration.
3. Access FortiClient Cloud in one of the following ways:
   - Access FortiClient Cloud from FortiCloud.
   - Access FortiClient Cloud from the FortiClient Cloud portal:
     i. In a browser, go to the FortiClient Cloud portal.
     ii. Log in with your FortiCloud credentials.
   - Access FortiClient Cloud from the link in the welcome email.

   If you cannot access the FortiClient Cloud EMS portal, ensure that you enable access to `forticlient.forticloud.com:443`. See Allowlisting the FortiClient Cloud IP addresses on page 27.

4. When you first log in to FortiClient Cloud, you can select the region to store your FortiClient Cloud data. Select North America, EMEA, U.K., or APAC.
5. Select the desired account from the organizational unit (OU) tree to access FortiClient Cloud.

If you are logged in as an IAM user with OUs enabled, you can return to the OU tree by selecting the dropdown list in the upper right corner of the GUI, which displays the OU account that you are currently logged in, then selecting the desired OU account from the dropdown list. If you are not logged in as an IAM user, you can select your account in the upper right corner of the GUI and then select *Switch Accounts* to switch to other accounts that you belong to as a subuser.



For information about multitenancy with FortiCloud Organizations and Identity & Access Management, see Organization Portal. You will need a FortiCloud Premium account for this feature. There is no *Manage Multiple Customer Sites* option in System *Settings* > *EMS Settings* as there is in on-premise EMS.

Managing endpoints using FortiClient Cloud

Adding a FortiClient deployment package

FortiClient Cloud allows a maximum of ten deployment packages.

To add a deployment package:

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

Installer Type	Use an official FortiClient installer or a custom FortiClient installer. See Adding a custom FortiClient installer for details on uploading a custom installer.
Release	Select the FortiClient release version to install.
Patch	Select the specific FortiClient patch version to install.
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. For more information about the FortiClient upgrade process on the endpoint, see Upgrading FortiClient.
Custom installer	Select the desired custom FortiClient installer.

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

Name	Enter the FortiClient deployment package's name.
Invitation	Select the desired invitation to include in the installer. Once installed, FortiClient Cloud uses the invitation to connect to FortiClient Cloud. You can click *Create Invitation* to create a new invitation. See Adding a new invitation for a deployment package on page 16. Each invitation can only be used by one deployment package.
Notes	**(Optional)** Enter any notes about the FortiClient deployment package.

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

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.
Vulnerability Scan	Enabled by default and cannot be disabled. Installs FortiClient with Vulnerability Scan enabled.
Advanced Persistent Threat (APT) Components	Install FortiClient with APT components enabled. Disable to omit APT components from the FortiClient deployment package. Includes FortiSandbox detection and quarantine features.

Additional Security Features	Enable any of the following features:
	• Malware:
	  • AntiVirus, Anti-Exploit, Removable Media Access
	  • Anti-Ransomware
	  • Cloud Based Malware Outbreak Detection
	• Web and Video Filtering:
	  • Web Filtering
	  • Video Filtering
	• Application Firewall
	• Single Sign-On (SSO) mobility agent
	• Zero Trust Network Access
	• Privileged Access Agent
	Disable to exclude features from the FortiClient deployment package.

FortiClient Cloud does not support all the features that an on-premise EMS supports. See Limitations on page 34.

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

Enable automatic registration	FortiClient automatically connects Telemetry to FortiClient Cloud after FortiClient installs on the endpoint. You cannot disable this option.
Enable desktop shortcut	Configure the FortiClient deployment package to create a desktop shortcut on the endpoint.
Enable start menu shortcut	Configure the FortiClient deployment package to create a Start menu shortcut on the endpoint.
Enable Installer ID	Configure an installer ID. Select an existing installer ID or enter a new installer ID. If creating an installer ID, select a group path or create a new group in the *Group Path* field. FortiClient Cloud automatically groups endpoints according to installer ID group assignment rules.
Enable Endpoint Profile	Select an endpoint profile to include in the installer. EMS applies the profile to the endpoint once it has installed FortiClient. This option is necessary if it is required to have certain security features enabled prior to contact with EMS, or if users require VPN connection to connect to EMS.

7. Click *Finish*. The FortiClient deployment package is added to FortiClient Cloud and displays on the *Manage Installers* > *Deployment Packages* pane. The deployment package may include .exe (32-bit and 64-bit), .msi, and .dmg files depending on the configuration.

Installing FortiClient Cloud on an endpoint and registering to FortiClient Cloud EMS

After Creating a FortiClient installer for FortiClient Cloud deployment, you must push the FortiClient installer to applicable endpoints which will install FortiClient and the EDR Collector on the endpoint if it is not already installed.

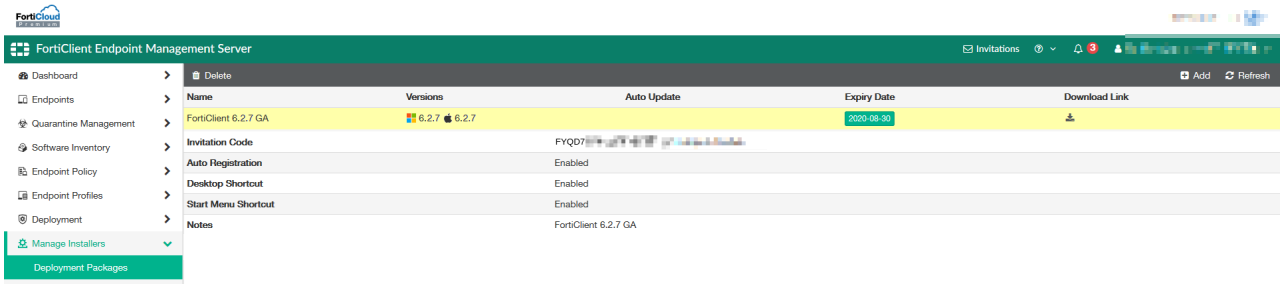
To deploy FortiClient Cloud to Windows and macOS endpoints:

Deploying FortiClient Cloud to Windows and macOS endpoints is the same in FortiClient Cloud as for on-premise EMS. See Initially deploying FortiClient Cloud software to endpoints.

To install FortiClient Cloud on an endpoint:

When installing FortiClient Cloud on an endpoint from a deployment package created in FortiClient Cloud, the administrator carries out some actions, while the endpoint user carries out others.

1. (Administrator) In FortiClient Cloud EMS, go to *Manage Installers* > *Deployment Packages*. Note the invitation code for the desired deployment package.

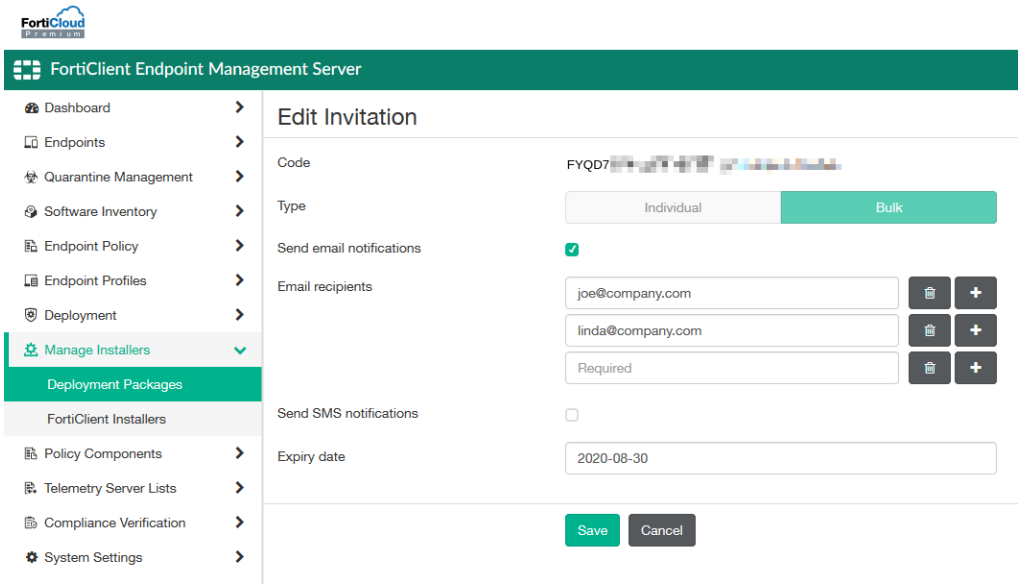


2. (Administrator) Go to *Invitations* in the upper right corner or in *Endpoints* > *Invitations*.
3. (Administrator) Select the invitation code that was noted in step 2. Click *Edit*.
4. (Administrator) Configure the invitation code:
   a. (Administrator) To send the code to a single recipient, select *Individual*. Otherwise, select *Bulk*.

   Sending individual invitation codes is considered best practice, as it can limit unexpected endpoints from connecting to FortiClient Cloud.

   b. (Administrator) In the *Email recipients* field, enter the email addresses of the desired end users.
   c. (Administrator) If desired, enable *Send SMS notifications*.
   d. (Administrator) In the *SMS recipients* field, enter the phone numbers of the desired end users.

e. (Administrator) In the *Expiry date* field, set the expiry date. Click *Save*.



5. (Administrator) The email that users receive for an individual invitation code does not include a FortiClient Cloud download link. You must share the installer files with users, or send them the link to FortiClient.com, from where they can download the installer files.
6. (End user) Install FortiClient Cloud on your device. The FortiClient Cloud invitation email or text message that you received may include a FortiClient Cloud download link. Otherwise, your administrator should have provided the installer files or a link where you can download them.
7. (End user) Your FortiClient Cloud may automatically register to FortiClient Cloud after installation. If not, use the instructions in Connecting an endpoint to FortiClient Cloud on page 13 to register to FortiClient Cloud.

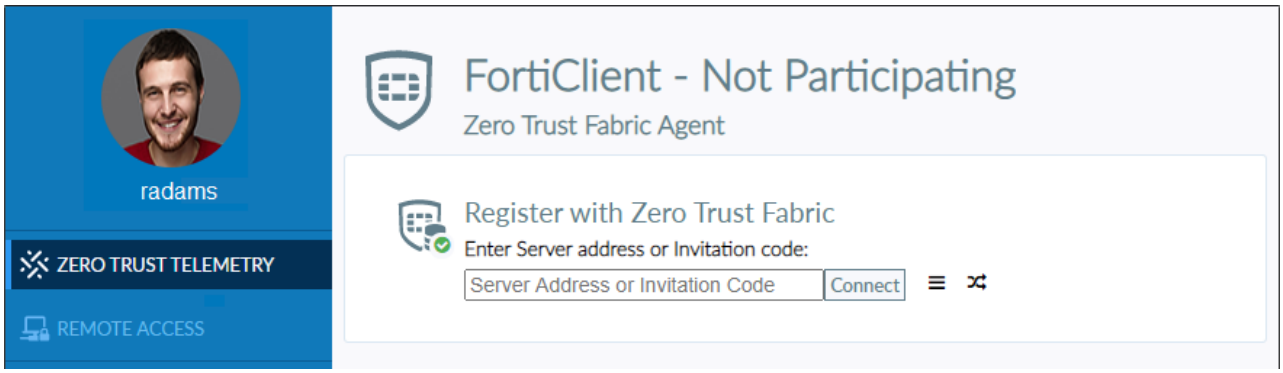
Connecting an endpoint to FortiClient Cloud

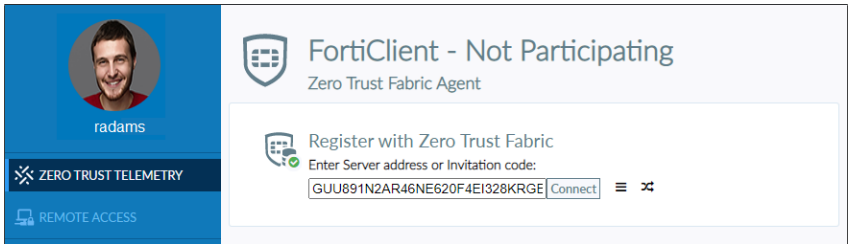
You can use the following instructions to connect to FortiClient Cloud in one of the following scenarios:

- If you want to connect a Linux, iOS, or Android endpoint to FortiClient Cloud. Since you cannot create a deployment package for these operating systems in FortiClient Cloud, this is the only way to register these endpoints to FortiClient Cloud.
- If an endpoint did not automatically register to FortiClient Cloud after FortiClient installation.

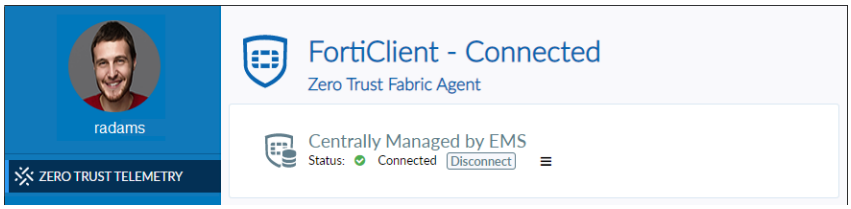
To register Windows, macOS, or Linux endpoints to FortiClient Cloud:

1. If your administrator is using FortiClient Cloud, you should receive an invitation email. Use the link in the invitation email to download FortiClient to your device.
2. Run the downloaded installer to install FortiClient .
3. After initial installation, FortiClient should automatically register to FortiClient Cloud. If FortiClient does not automatically register to FortiClient , enter the invitation code in the *Join FortiClient Cloud* field on the *Zero Trust Telemetry* tab in FortiClient Cloud.



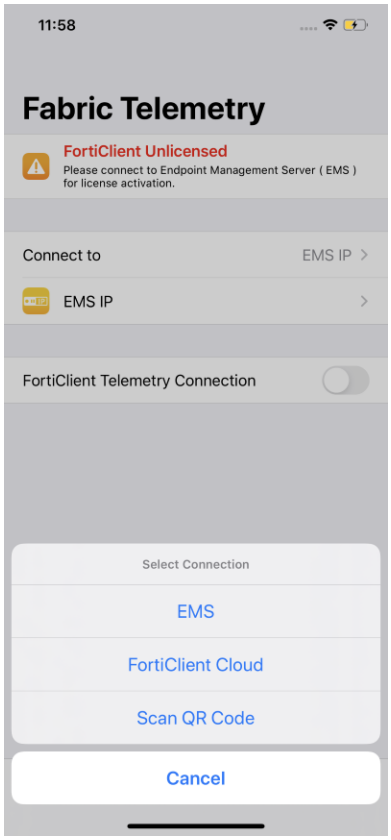


4. Click *Connect*. Ensure that the *Status* displays as *Connected*. FortiClient software is now licensed and activated.

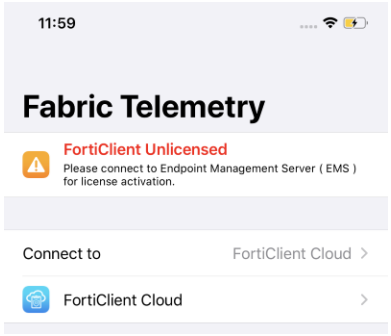


To register iOS or Android endpoints to FortiClient Cloud:

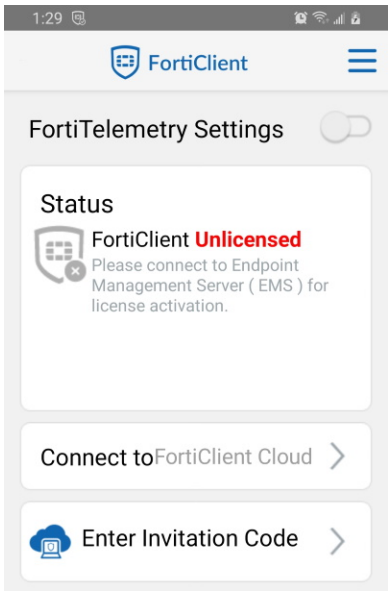
1. Tap *Connect to*, then select *FortiClient Cloud*.



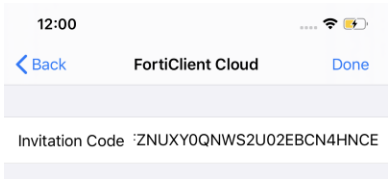
2. Do one of the following:
   a. For iOS, tap *FortiClient Cloud*.



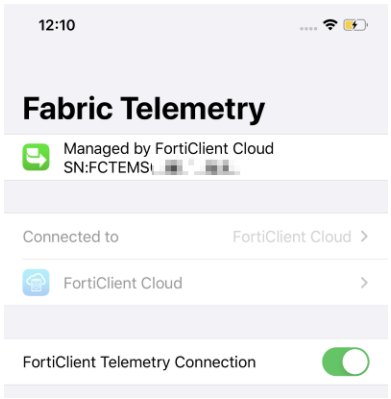
b. For Android, tap *Enter Invitation Code*.



3. Enter the invitation code.



FortiClient Cloud is now managing FortiClient .



Adding a new invitation for a deployment package

To add a new invitation for a deployment package:

1. Go to *Invitations* in the upper right corner or in *Endpoints* > *Invitations*.
2. Select an existing invitation code for the desired deployment package.
3. Click *Add*.

4. Configure the invitation:
   a. To send the code to a single recipient, select *Individual*. Otherwise, select *Bulk*.

Sending individual invitation codes is considered best practice, as it can limit unexpected endpoints from connecting to FortiClient Cloud.

   b. If desired, select *Send Email Notifications*.
   c. In the *Email Recipients* field, enter the desired end users' email addresses.
   d. If desired, enable *Send SMS Notifications*.
   e. In the *SMS Recipients* field, enter the desired end users' phone numbers.
   f. If desired, enable Expiring.
   g. In the *Expiry Date* field, set the expiry date.
   h. For *Verification Type*, select one of the following:

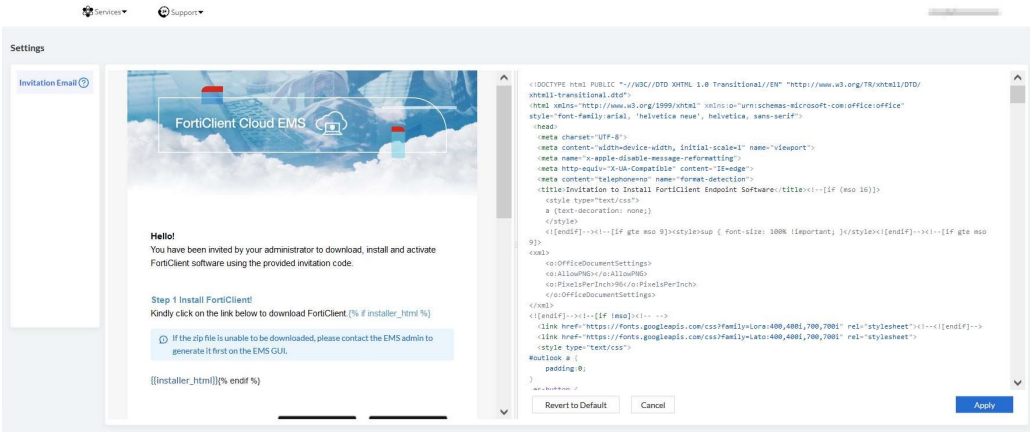
Verification type	Description
None	End user does not need to provide any credentials to connect to FortiClient Cloud.
Local	End user must provide credentials that match a local user configured in *User Management > Local Users* to connect to EMS. You must create a local user to configure this option.
LDAP	End user must provide their domain credentials to connect to FortiClient Cloud. You must configure an LDAP domain to configure this option.
SAML	End user must provide their credentials for an SAML identity provider, such as Azure Active Directory, to connect to EMS. You must configure SAML settings to configure this option.

5. Click *Save*. You see a new invitation code for the deployment package.

Customizing invitation code email content

To customize invitation code email content:

1. Log in to FortiClient Cloud using your primary account credentials.
2. Go to *Settings*.
3. Edit and preview email content. You can edit email content on the right pane and preview your changes on the left pane. Click *Apply* to save your changes or click *Revert to Default* to get revert content to the default email template. Ensure that your email content contains {{invitation_code}} since it is used to render the invitation code in the email.



If you log in as a non-primary user, such as a subuser or Identity & Access Management user, you have read-only permissions and cannot edit the email content.

Managing Chromebooks with FortiClient Cloud

You can use FortiClient Cloud to manage Chromebooks. After you deploy and configure FortiClient Cloud, the Google Admin console, and the FortiClient Cloud Web Filter extension, the products work together to provide web filtering security for Google Chromebook users logged into the Google domain.

For a new deployment, ensure that you select FortiClient 7.2.1 or later. This section only provides instructions for 7.2.1 or a later version.

To configure FortiClient Cloud for Chromebook management:

You can configure FortiClient Cloud for Chromebook management by following the instructions in Installation and setup for managing Chromebooks. While these topics are for on-premise EMS, they also apply to FortiClient Cloud, except for one difference. In step 2 of Configuring the FortiClient Web Filter extension, instead of `ProfileServerUrl`, the text file must contain the following text:

```
{
"InvitationCode": { "Value": "<FortiClient Cloud invitation code>"}
}
```

The following provides an example:

```
{
"InvitationCode": { "Value": "6LY209RIP8NE6J1JR0FIF97LEVJVBKT2"}
}
```

You do not need to create an SSL certificate as a public certificate is used.

Accounts

The following provides account-related information:

- Adding a secondary admin account on page 19
- IAM users on page 20

You cannot control the admin role for the following user types from FortiClient Cloud EMS:

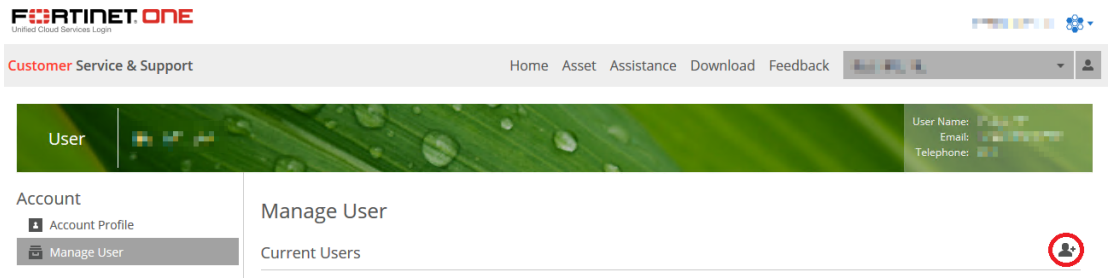
- When a user is configured as Admin or Viewer in FortiCloud. In FortiClient Cloud EMS, these users become super administrators and restricted administrators, respectively.
- Secondary user who has full access permission in FortiCloud

Adding a secondary admin account

The FortiClient Cloud primary administrator (the user who created the FortiClient Cloud instance) can add secondary administrators from their FortiCloud account.

To create a secondary admin account:

1. Log in to Fortinet Service & Support with your FortiCloud account.
2. Click your account name in the top right corner, then select *My Account*.
3. Select *Manage User*.
4. Click the *Add User* icon.



5. Enter the user information as required. If the new user does not have a FortiCloud account, they must create one. Click *Save*. A user added on this page becomes visible on the FortiClient Cloud GUI in *Administrators* and can log in to FortiClient Cloud with their FortiCloud account. These users have limited permissions. For details on configuring permissions for these administrators, see Admin roles.

FortiClient Cloud supports resource-based access control using FortiCloud permission profiles. See Creating a permission profile.

IAM users

FortiCloud Identity & Access Management (IAM) supports creating IAM users and allowing access to FortiClient Cloud using the admin role.

See Adding IAM users for details on configuring IAM users.

Creating an IAM user with OU scope

See User permissions.

Logging in to FortiClient Cloud and accessing OU accounts

To log in to FortiClient Cloud and access OU accounts:

1. In the FortiClient Cloud landing page, click *Login*.
2. Select *IAM Login*.
3. Enter your account ID/alias, username, and password, then click *Log In*.
4. Select the desired account/organizational unit.

API access keys

FortiClient Cloud supports an option for the administrator to define an access code to identify an instance. A Fabric device can establish connection to a FortiClient Cloud instance by providing one of the following in the SNI:

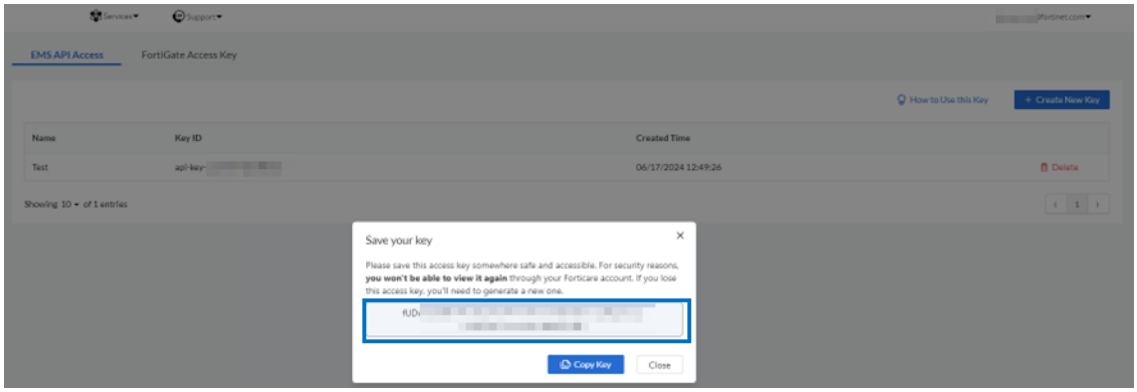
- FortiCloud account ID. The connection succeeds if the FortiCloud account has only one FortiClient Cloud instance and there is no organizational unit structure.
- FortiCloud account ID and FortiClient Cloud access key

This feature supports the following key types:

- EMS API access key. Only a primary account can create EMS API access keys. These keys do not expire.
- FortiGate access key. This feature requires FortiOS 7.4.4 or later.

To create an EMS API access key:

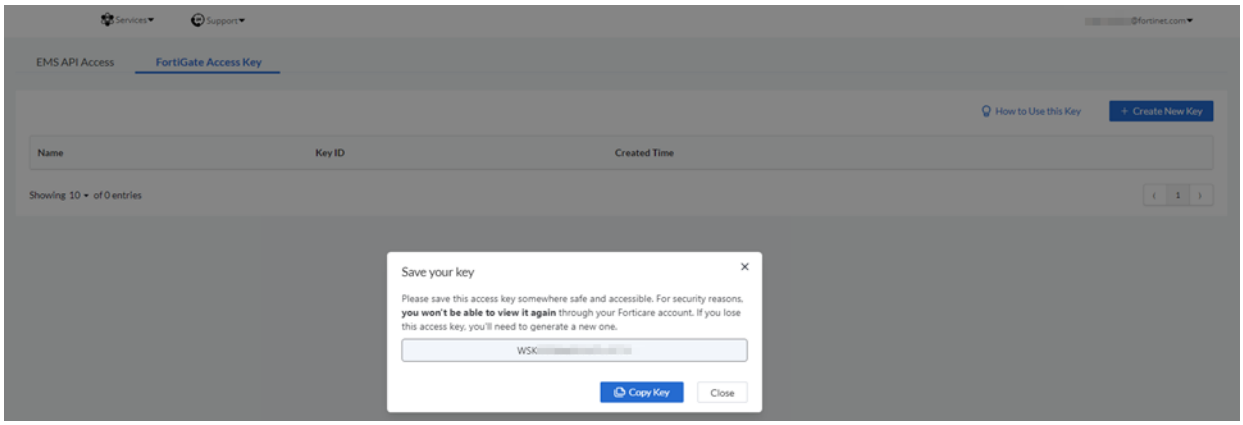
1. In FortiClient Cloud, go to *Access Key* > *EMS API Access*.
2. Click *Create New Key*.
3. In the *Name* field, enter a unique name, then click *OK*.
4. Once the key is created, copy it to a safe location, as it does not display again after you close the dialog. Click *Close*.



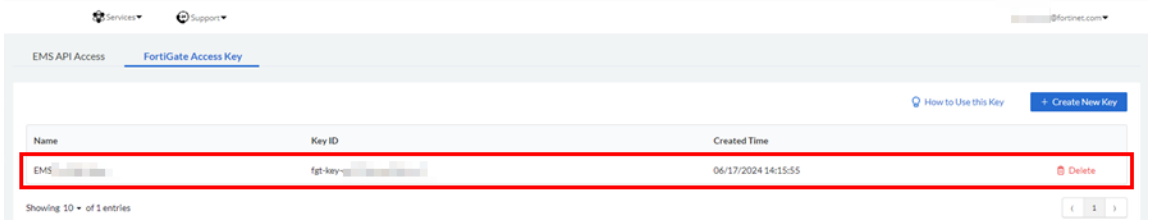
5. The EMS API keys display in the *EMS API Access* table. Note that the key ID is not the same as the generated API key that you copied in step 4. To view information about the keys, click *How to Use this Key*.

To create a FortiGate access key:

1. In FortiClient Cloud, go to *Access Key* > *FortiGate Access Key*.
2. Click *Create New Key*.
3. In the *Name* field, enter a unique name, then click *OK*.
4. Once the key is created, copy it to a safe location, as it does not display again after you close the dialog. Click *Close*.



5. The FortiGate keys display in the *FortiGate Access Key* table. Note that the key ID is not the same as the generated API key that you copied in step 4. To view information about the keys, click *How to Use this Key*.



6. On the FortiGate, configure the key on the EMS Fabric connector:

```
config endpoint-control fctems
                                        edit 1
                                        set status enable
                                        set name "ems-cloud"
                                        set fortinetone-cloud-authentication enable
                                        set cloud-authentication-access-key "<FortiGate key>"
                                        next
                    end
```

7. In EMS, authorize the FortiGate to complete the connection. Standalone FortiGates or separate virtual domains from the same FortiGate can establish Fabric connection with FortiClient Cloud.

Upgrading FortiClient Cloud

FortiClient Cloud is a SaaS service where Fortinet continuously updates the version for all customers. You can expect a FortiClient Cloud upgrade to be available two to four weeks after a stable minor GA version release announcement.

A FortiClient Cloud upgrade can occur in one of the following ways:

- You can schedule the upgrade yourself from the FortiClient Cloud portal.
- You can send an upgrade request to Fortinet Support.
- Fortinet forces an upgrade. This generally occurs to avoid compatibility issues. Fortinet sends an email notification seven to ten business days prior to the upgrade. The email includes the upgrade time and version information. You can also view the upgrade schedule on the FortiClient Cloud portal.

Hi There!

We are happy to let you know that as part of our ongoing feature deployment, EMS release 7.0.7GA is now ready for deployment on Forticlient cloud.

On 2022-09-14, from 6:00pm~7:00pm PDT, we'll upgrade your EMS to 7.0.7GA. The upgrade process usually takes about 10 minutes, EMS UI access and forticlient connection might be interrupted during upgrade. Additionaly, a notice has been published on the Forticlient Cloud webpage, you are able to reschedule the upgrade no later than 2022-09-30.

We apologize for any inconvenience this may cause, and thank you for your continued support.

Maintenance window
Start Time: 09/14/2022, 18:00

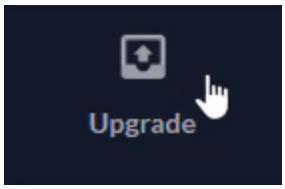
End Time: 09/14/2022, 19:00

Thank you,
FortiClient Cloud Team

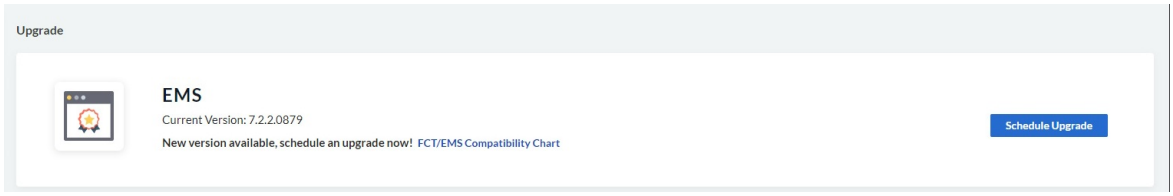
To schedule an upgrade:

If your FortiClient Cloud is not at the latest version, you can schedule to upgrade to the latest version.

1. In the FortiClient Cloud portal, click the menu icon ( ) at the bottom right corner and then select *Upgrade*.



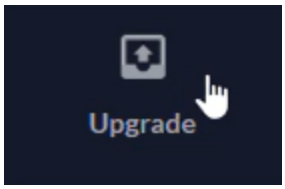
2. Click *Schedule Upgrade*.



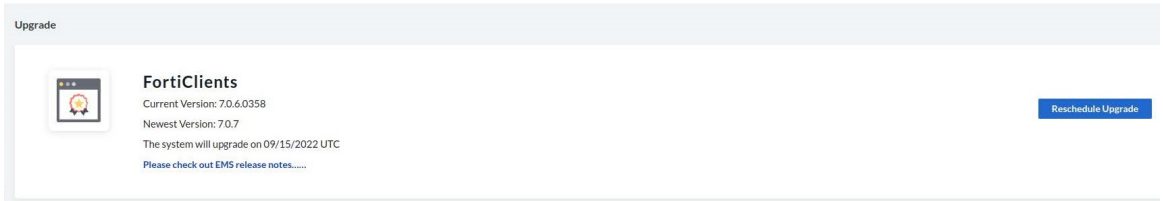
3. From the *Upgrade Version* dropdown list, select the desired version to upgrade to.
4. In the *Scheduled Upgrade Time* field, select the desired date. You must select a date before the displayed last day to upgrade. If you need to upgrade on a day after the displayed last day to upgrade, or you have a specific critical issue, contact Fortinet Support to discuss if the upgrade can be delayed to a future date.
5. Click *OK*.

To reschedule an upgrade:

1. In the FortiClient Cloud portal, click the menu icon ( ) at the bottom right corner and then select *Upgrade*.

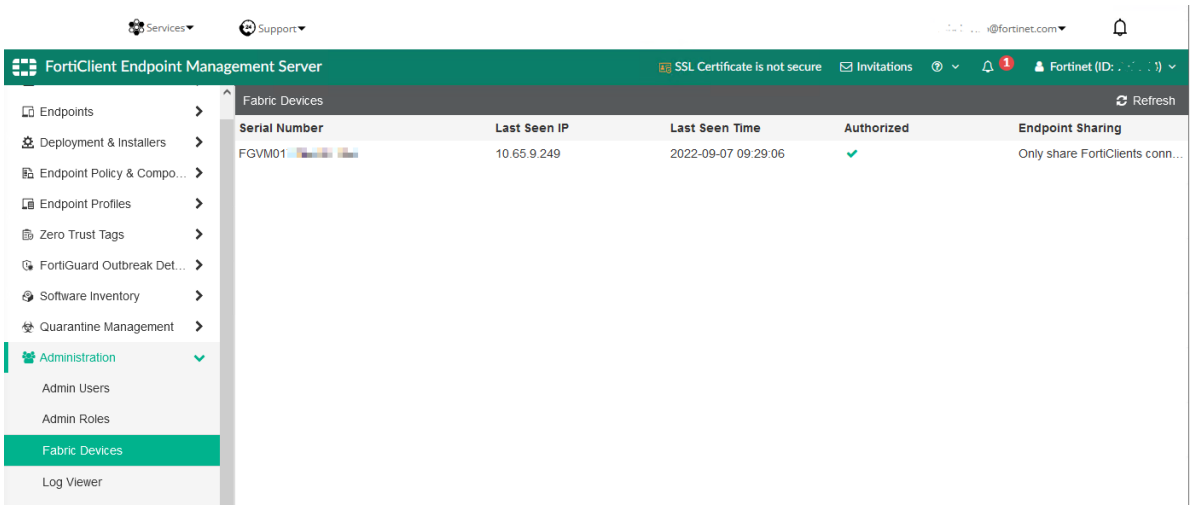


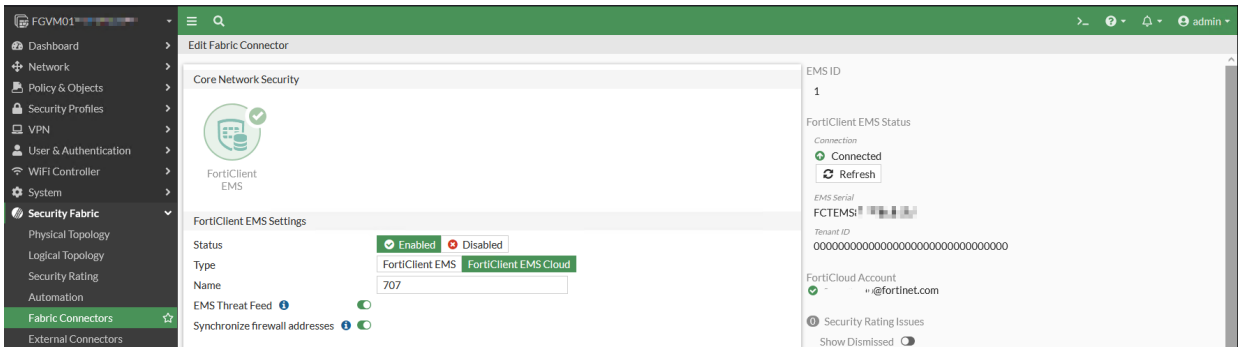
2. Click *Reschedule Upgrade*.



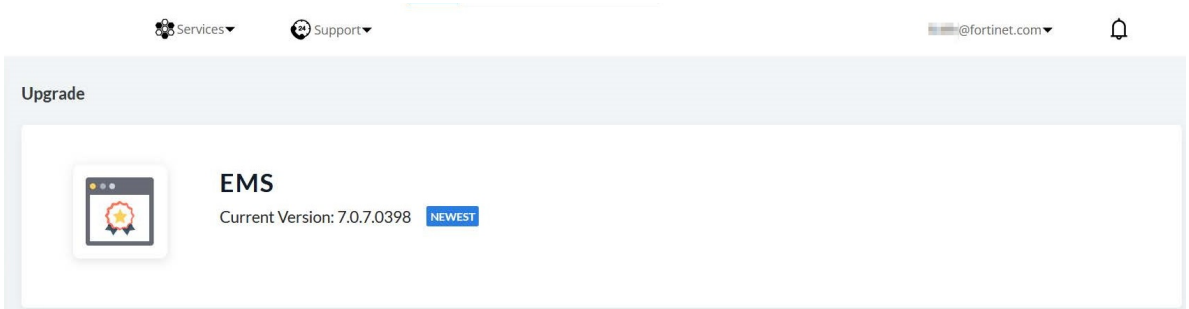
3. In the *System Upgrade Time* field, select the desired date. You must select a date before the displayed last day to upgrade. If you need to upgrade on a day after the displayed last day to upgrade, or you want to cancel the upgrade, contact Fortinet Support.
4. Click *OK*.

After the upgrade, view your FortiOS connectors to ensure that they are functioning correctly and that the desired FortiGates are authorized on FortiClient Cloud and vice-versa.





The following shows the *Upgrade* page when EMS is at the latest version. In this case, there is no need to upgrade.



Allowlisting the FortiClient Cloud IP addresses

Communication from endpoints to FortiClient Cloud

The following are public domains involved in the communication from endpoints to FortiClient Cloud:

- `forticlient.forticloud.com` (browser, FortiClient Cloud)
- `*.ems.forticlient.forticloud.com` (browser)
- `forticlient-emsproxy.forticloud.com` (FortiClient Cloud, FortiGate, Active Directory (AD) connector)

You must allowlist the IP addresses of the aforementioned domains.

Communication from FortiClient Cloud to endpoints

You must allowlist the FortiClient Cloud external IP address to allow communication from FortiClient Cloud to endpoints for the following features:

- AD integration
- Importing a profile from FortiGate or FortiManager
- SMTP server configuration

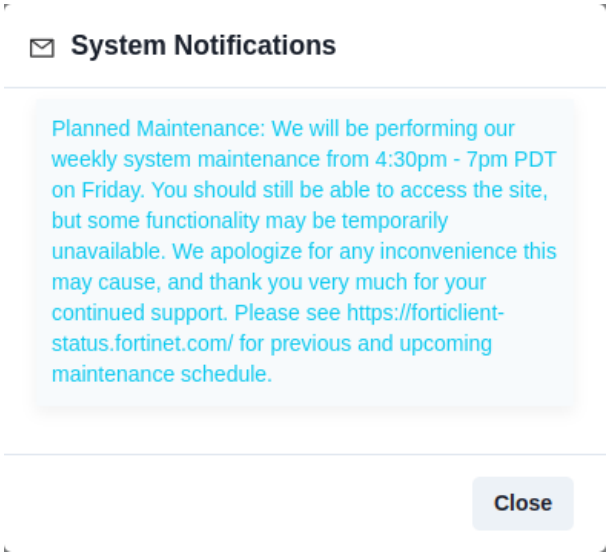
In the FortiClient Cloud portal, go to *About*. The IP address row displays the IP address that you must allowlist for the listed features.

Notifications

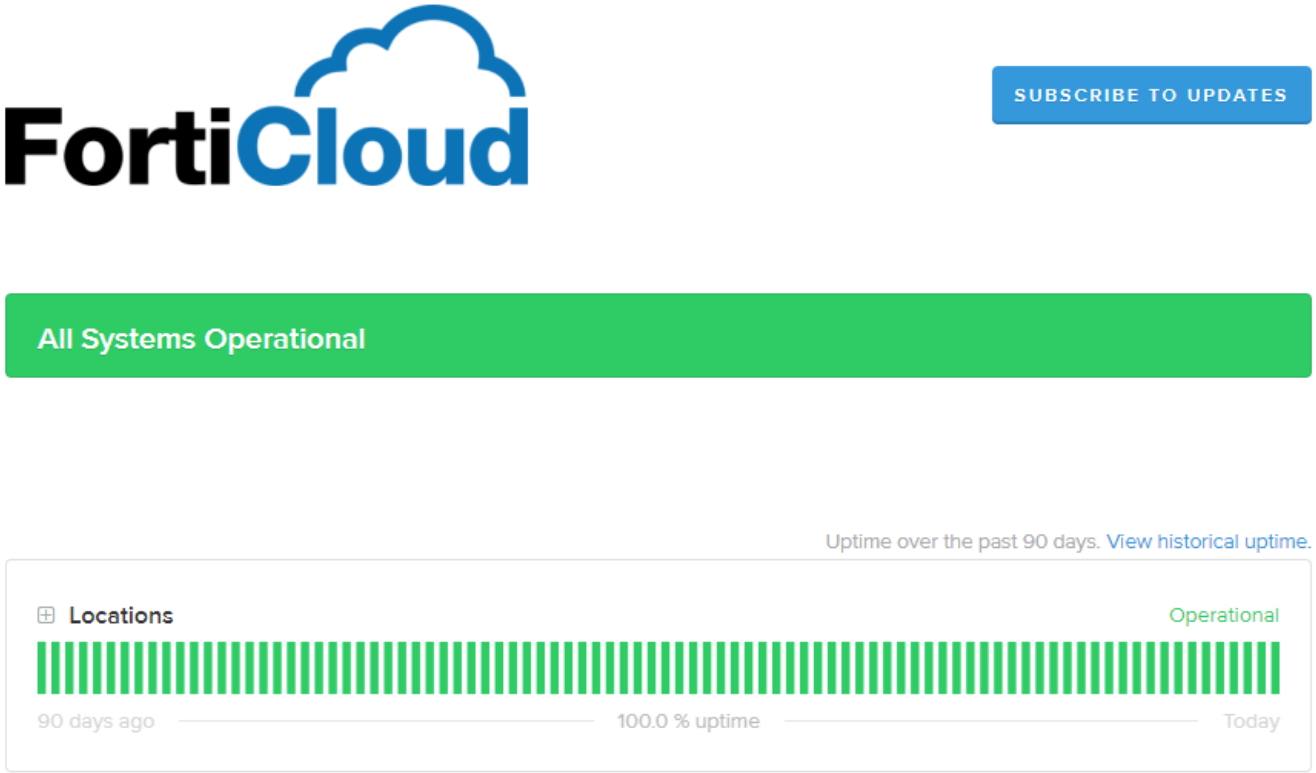
The following summarizes types of notifications that you may observe on FortiClient Cloud:

System maintenance

These notifications alert you to system maintenance that is planned for all users in that datacenter due to a release, backend environment issue, or maintenance need. There is no action required for customers. You can view this notification from the GUI:

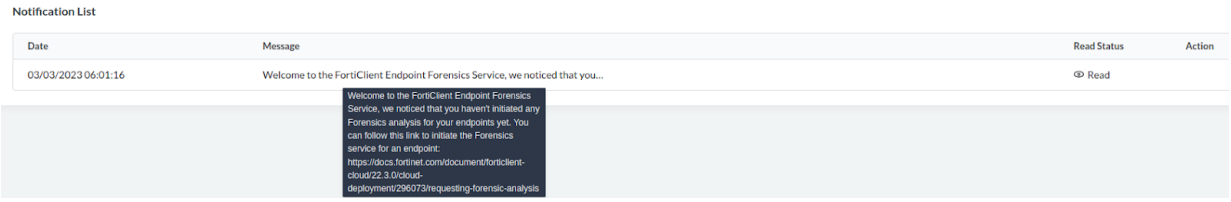


You can also view this notification from FortiClient Cloud Status.

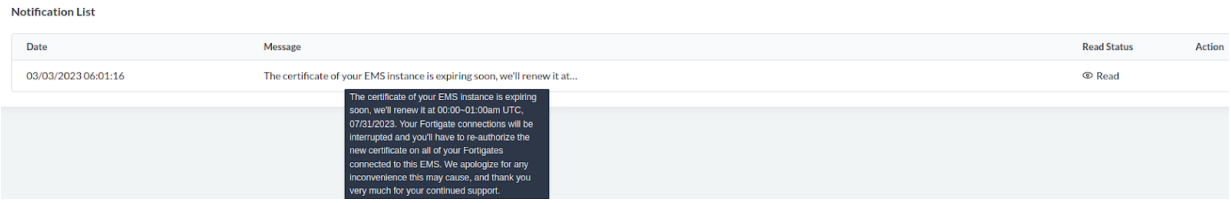


Targeted notifications

These notifications target specific customers and may require an action from the user. You can find them in the *Notifications* tab on the left panel. The following shows an example of a targeted notification for a new Forensics service user:



The following shows an example of a targeted notification for EMS certificate renewal:



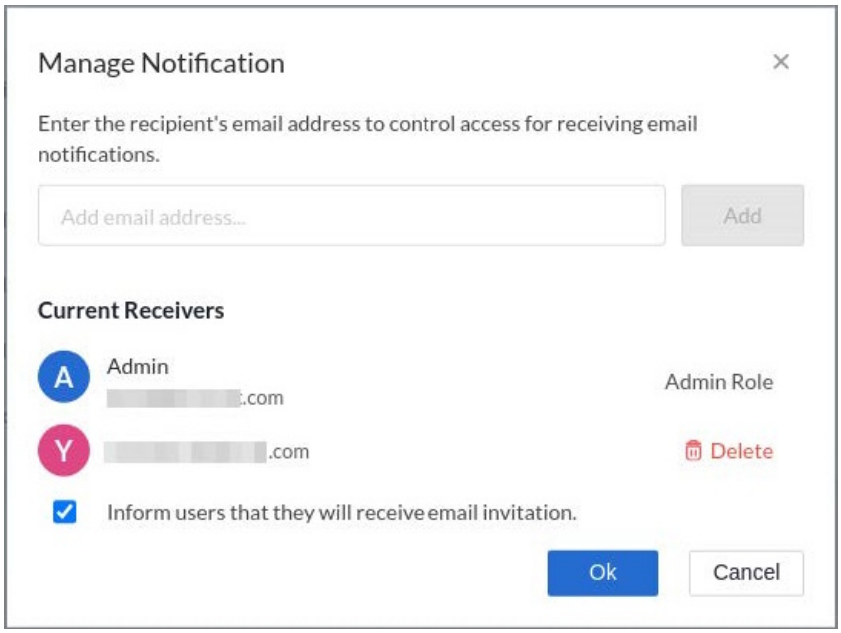
Managing notifications in the FortiClient Cloud portal

To configure notification recipients:

1. Log in to the FortiClient Cloud portal using your primary account credentials.

   If you log in as a non-primary user (subuser or Identity & Access Management user), you have read-only permissions and cannot edit the recipient list.

2. Go to *Notifications*.
3. Click *Manage Notification*.
4. The *Manage Notification* dialog displays the list of notification recipients. Add new recipients by entering their email address in the *Add email address* field or remove recipients by clicking *Delete*. If adding a new recipient, you can select *Inform users that they will receive email invitation.* to notify them that they will receive notifications.



If desired, the recipient can unsubscribe by using a link in the subscription notice email.

Dear Customer,

We are pleased to inform you that your administrator '[redacted].com' has added you as a designated recipient for FortiClient Cloud notifications. This means you will now receive essential updates, alerts, and information related to FortiClient Cloud directly in your email inbox.

If, at any point, you wish to stop receiving these notifications, you can easily unsubscribe by clicking the "Unsubscribe" link provided below.

Should you have any questions or if you believe this addition was made in error, please don't hesitate to reach out to your administrator or our support team.

Thank you for your cooperation.

Regards,
FortiClient Cloud Team

click to unsubscribe from all communications

Using the Fortinet email server for sending alerts

By default, FortiClient Cloud uses the Fortinet built-in email server to send email alerts. This eliminates the need to specify your own SMTP or mail server before sending alert emails. You only need to configure the recipient email addresses.

If desired, you can still manually specify your own SMTP server.

To configure email settings:

1. In FortiClient Cloud, go to *System Settings* > *SMTP Server*.
2. By default, *Fortinet* is selected as *Mail Server*. Configure recipients and test recipient settings as desired. Save.

The following shows an example alert email. The sender email address is no-reply@notification.fortinet.net.

Limitations

The management capacity data for the latest EMS 7.4 or 7.2 version applies to FortiClient Cloud depending on your instance. See the management capacity for your instance:

- 7.4
- 7.2

FortiClient Cloud supports the majority of features that on-premise EMS supports.

The following provides a comparison between FortiClient Cloud and EMS 7.4 and 7.2:

Feature	FortiClient Cloud	EMS 7.4 and 7.2
Fortinet Security Fabric integration		
Share endpoint telemetry data with FortiGate and FortiAnalyzer	Updated connector for FortiGate and FortiAnalyzer	Updated connector for FortiGate and FortiAnalyzer
Dynamic access control	Yes	Yes
Security posture tags	Yes	Yes
FortiSASE support	Yes	No
Secure remote access		
IPsec and SSL VPN agents	Yes	Yes
Single sign on	Yes	Yes
Web Filter		
Web Filter	Yes	Yes
Chromebook support, including filtering based on keyword searches	Yes	Yes
Web Filter for FortiClient Cloud iOS and Android	Yes	Yes
Import web filter policy from FortiOS	Yes	Yes
Import web filter profile from FortiManager Cloud	Yes	Yes
Browser plugin support	Yes	Yes

Feature	FortiClient Cloud	EMS 7.4 and 7.2
	Browser support depends on the endpoint OS and installed FortiClient Cloud version.	Browser support depends on the endpoint OS and installed FortiClient Cloud version.
Endpoint hardening, visibility, and discovery		
Vulnerability scan	Yes	Yes
Patching	Yes	Yes
Application inventory	Yes	Yes
Application Firewall	Yes	Yes
Endpoint protection and prevention		
Antimalware	Yes (Content pattern recognition language (CPRL) and machine learning)	Yes (CPRL and machine learning)
Antiexploit	Yes	Yes
Antiransomware	Yes	Yes
Application Firewall (SaaS control, botnet protection)	Yes	Yes
Fileless malware scanning through AMSI	Yes	Yes
Sandbox integration	Yes	Yes
Deployment and management console		
Management console	Cloud-based management console hosted by Fortinet	On-premise, self-hosted by customer. Requires a Linux (7.4) or Windows Server (7.2) machine
EMS version	• 7.4 • 7.2	• 7.4 • 7.2
Supported FortiClient agent versions	• 7.4 • 7.2 • 7.0	• 7.4 • 7.2 • 7.0
Active Directory integration	Yes	Yes
Supported platforms	• Windows • macOS • Linux • iOS • Android • Chromebook	• Windows • macOS • Linux • iOS • Android • Chromebook

Feature	FortiClient Cloud	EMS 7.4 and 7.2
Multitenancy	Yes via FortiCloud organizational units. You will need a FortiCloud Premium account for this feature. There is no *Manage Multiple Customer Sites* option in System *Settings* > *EMS Settings* as there is in on-premise EMS.	Yes

Privacy

You can find information around privacy, including the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) at the following:

Link	Description
https://www.fortinet.com/content/dam/fortinet/assets/legal/EULA.pdf	End User License Agreement (EULA)
https://www.fortinet.com/corporate/about-us/privacy	Privacy Policy. Referenced in the EULA, contains information for not only the European Economic Area but for the CCPA as well.
https://www.fortinet.com/corporate/about-us/gdpr	How Fortinet supports and complies with GDPR. As this document mentions, a data processing agreement can be made available upon request.
https://www.fortinet.com/solutions/industries/regulatory-compliance/GDPR	Fortinet Solutions for GDPR
https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/checklist-gdpr.pdf	STATE-OF-THE-ART DATA PROTECTION FOR GDPR 7 Considerations and Where Fortinet Can Help
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/Fortinet_Data_Privacy_Practices.pdf	Data privacy datasheet

When registering the FortiClient Cloud license on the FortiCloud portal, you can choose where your instance resides:

- North America
- EMEA
- APAC

See Deploying FortiClient Cloud on page 8.

To obtain a data processing agreement signed to comply with GDPR, EMEA customers can contact their Fortinet sales contact.

See the following frequently asked questions regarding GDPR and privacy:

Question	Answer
Is data accessible through or shared with other regions?	Each customer chooses the region that their FortiClient Cloud is hosted in. The data stays in that

Question	Answer
	region.
How long is FortiClient Cloud data retained for?	Data is retained inside the FortiClient Cloud instance. The customer controls much of the data, such as log retention. The FortiClient data is retained in the FortiClient Cloud database in the instance.
What happens if a license expires or FortiClient Cloud is decommissioned?	Fortinet has a grace period of 60 days, where the FortiClient Cloud instance is retained, after which one backup is kept for one year.
Can a customer trigger a purge of all of their data?	The customer can call Fortinet Support to initiate purging of data at any time. Fortinet verifies the customer's identify before proceeding with the request.
Do FortiClient Cloud customers need the Data Processing Agreement (DPA) to comply with GDPR?	You can request DPA to be signed for FortiClient Cloud by contacting your sales team or emailing privacy@fortinet.com.
Is FortiClient Cloud instance data regularly backed up?	Yes, FortiClient Cloud keeps a backup of customer data for five business days. If a critical event occurs, Fortinet can restore data from up to five days prior to the event.
Does FortiClient Cloud support disaster recovery?	A copy of FortiClient Cloud data is stored in multiple data centers in same geographic location for data redundancy and disaster recovery. Data backups are updated daily. In the event of a disaster, FortiClient Cloud can quickly fall back to a backup data center and recover your organization's instance.
How does disaster recovery work?	A snapshot of the customer's FortiClient Cloud instance/data is stored in backup data centers. The snapshot is delta synced daily so that in the event of disaster, Fortinet can restore or spin up backup instances quickly for a fast recovery.
Is FortiClient Cloud data at rest encrypted?	FortiClient Cloud instances reside on encrypted storage arrays.
How can I request a backup of my FortiClient Cloud data?	You can export endpoint details, endpoint security profiles, and application inventory data from the FortiClient Cloud GUI. You can also open a ticket with Technical Support to request a full backup of your FortiClient Cloud data.

For questions regarding Fortinet's privacy efforts, contact privacy@fortinet.com.

Backup and restore strategy

As reliability is a critical concern, robust backup and disaster recovery strategies are in place for FortiClient Cloud.

Local reliability

- Daily database backups for each FortiClient Cloud instance with a 15-day retention period to ensure that data can be recovered in case of issues
- Snapshots taken before upgrades or instance termination

Disaster recovery

- AWS is set up as a backup site. Each user's FortiClient Cloud instance is duplicated on AWS with the same configuration as their primary instance on private cloud. Regular data synchronization from the primary node to the backup node ensures data consistency.
- In case of a region failure, the AWS backup instance can easily be activated, ensuring minimal downtime and data loss. Once the issue is resolved, you can be switched back to the primary FortiClient Cloud instance on private cloud.

Change log

Date	Change description
2025-03-20	Initial release.
2025-04-02	Updated Installing FortiClient Cloud on an endpoint and registering to FortiClient Cloud EMS on page 12.
2025-04-22	Updated Adding a FortiClient deployment package on page 10.
2025-07-09	Updated Accounts on page 19.
2025-08-12	Updated Introduction on page 4.
2025-10-20	Updated Introduction on page 4.
2025-10-21	Updated Requirements on page 5.

www.fortinet.com

Copyright© 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.