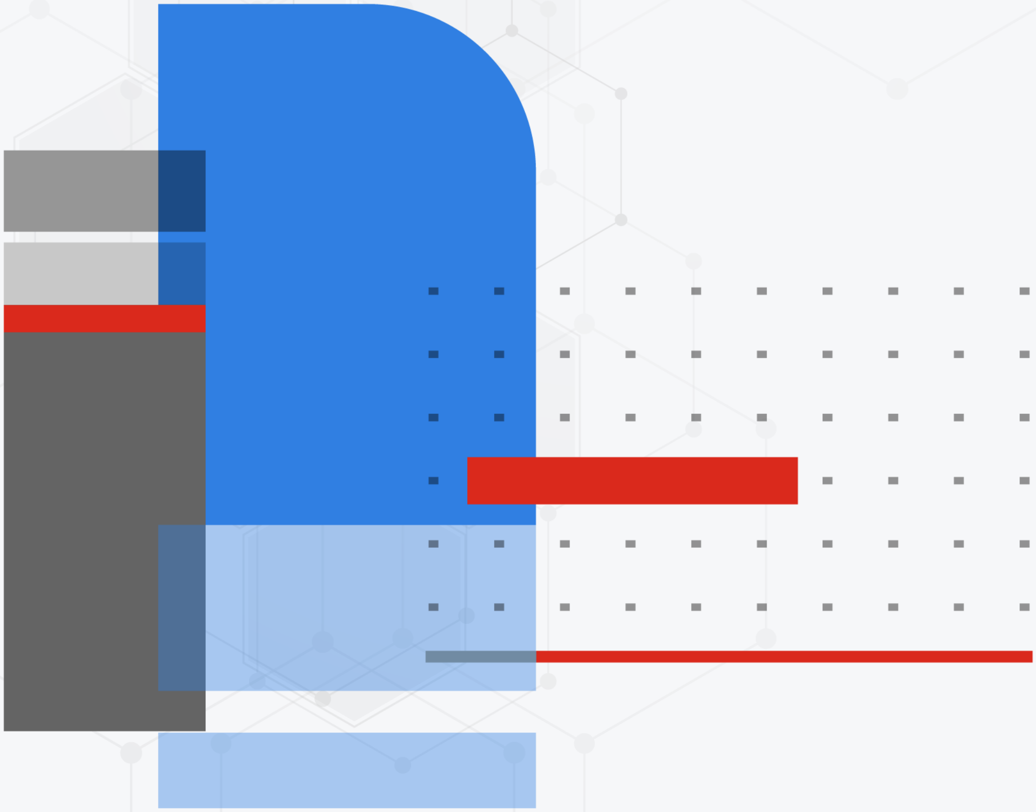
Cloud Deployment Guide

FortiClient 24.1



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

April 11, 2024
FortiClient 24.1 Cloud Deployment Guide
04-241-995168-20240411

TABLE OF CONTENTS

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 license contract for management by FortiClient Cloud to your FortiCloud account.

The management capacity data for the latest EMS 7.2 or 7.0 version applies to FortiClient Cloud depending on your instance. See the management capacity for your instance:

- 7.2
- 7.0

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

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

FortiClient Cloud 24.1 runs EMS 7.2 or 7.0.

FortiClient Cloud is hosted in the following regions:

- U.S.
- EMEA
  - U.K.
- APAC

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*.

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 Service Organization Controls (SOC2) certified. See SOC2 compliance standard.

Requirements

The following items are required before you can initialize your FortiClient 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 7.
Internet access	You must have Internet access to create a FortiClient Cloud instance.
Browser	Device with a browser to access FortiClient 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.
- Licensing FortiClient Cloud does not require a FortiCloud Premium subscription. You can purchase a FortiCloud Premium license for a trial of FortiClient Cloud. See the FortiCloud datasheet for details.
- 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.

  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 7 describes.

  Registering a ZTNA license for FortiClient Cloud management does not support all features supported for on-premise EMS. See Limitations on page 31 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 supports the following products:

- FortiClient:
  - 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.

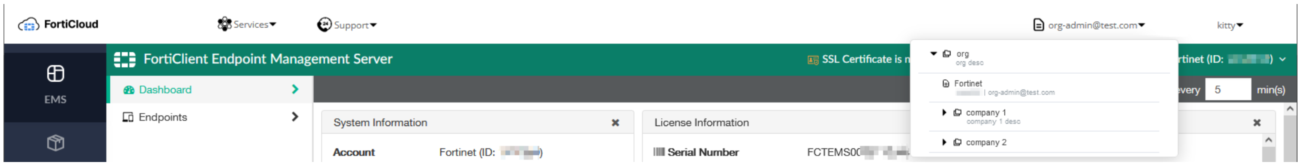
2. Register the FortiClient endpoint licenses for management by FortiClient Cloud:
   a. On the Customer Service & Support site, go to *Asset Management* > *Register Now*.
   b. In the *Registration Code* field, enter your license activation code and select *Next* to continue registering the product.
   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 portal, ensure that you enable access to forticlient.forticloud.com:443. Refer to the list of required services and ports for FortiClient.

4. When you first log in to FortiClient Cloud, you can select the region to store your FortiClient Cloud data. Select North America, EMEA, 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 with FortiClient Cloud

Adding a FortiClient deployment package

FortiClient Cloud allows a maximum of ten deployment packages.

To add a deployment package:

1. Go to *Manage Installers* > *Deployment Packages*.
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.
Keep updated to the latest patch	Select to enable FortiClient to automatically update to the latest patch release when FortiClient is installed on an endpoint.
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.
Expiry Date	Enter this deployment package's expiry date. After this date, users cannot use this deployment package to install FortiClient.
Notes	(Optional) Enter any notes about the FortiClient deployment package.

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

Security Fabric Agent	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.
Advanced Persistent Threat (APT) Components	Install FortiClient with APT components enabled. Disable to omit APT components from the FortiClient deployment package. Includes FortiSandbox detection and quarantine features.

Additional Security Features	Enable any of the following features: • AntiVirus • Web Filtering • Application Firewall • Single Sign-On (SSO) mobility agent • Cloud Based Malware Outbreak Detection 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 31.

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

Enable automatic registration	FortiClient automatically connects Telemetry to FortiClient 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 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 *Next*. The *Telemetry* tab displays the hostname and IP address of the FortiClient server, which will manage FortiClient once it is installed on the endpoint. Also configure the following option:

Enable telemetry connection to Security Fabric (FortiGate)	Enable this option, and select the name of the gateway list to use. The gateway list defines the IP address for the FortiGate. If you have not created a gateway list, select the checkbox, then click the *No telemetry server lists are available, create one here* link to create a gateway list for this deployment package to use. See *FortiClient EMS Administration Guide* for details on configuring a gateway list.

8. Click *Finish*. The FortiClient deployment package is added to FortiClient 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 on an endpoint and registering to FortiClient Cloud

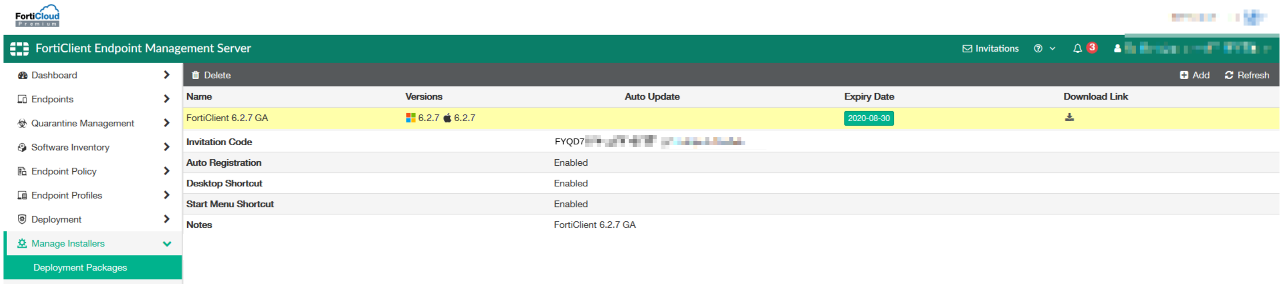
To deploy FortiClient to Windows and macOS endpoints:

Deploying FortiClient to Windows and macOS endpoints is the same in FortiClient Cloud as for on-premise EMS. See Deployment for more details.

To install FortiClient on an endpoint:

When installing FortiClient 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 EMS, go to *Manage Installers* > *Deployment Packages*. Note the invitation code for the desired deployment package.



Name	Versions	Auto Update	Expiry Date	Download Link
FortiClient 6.2.7 GA	6.2.7 6.2.7		2020-08-30	

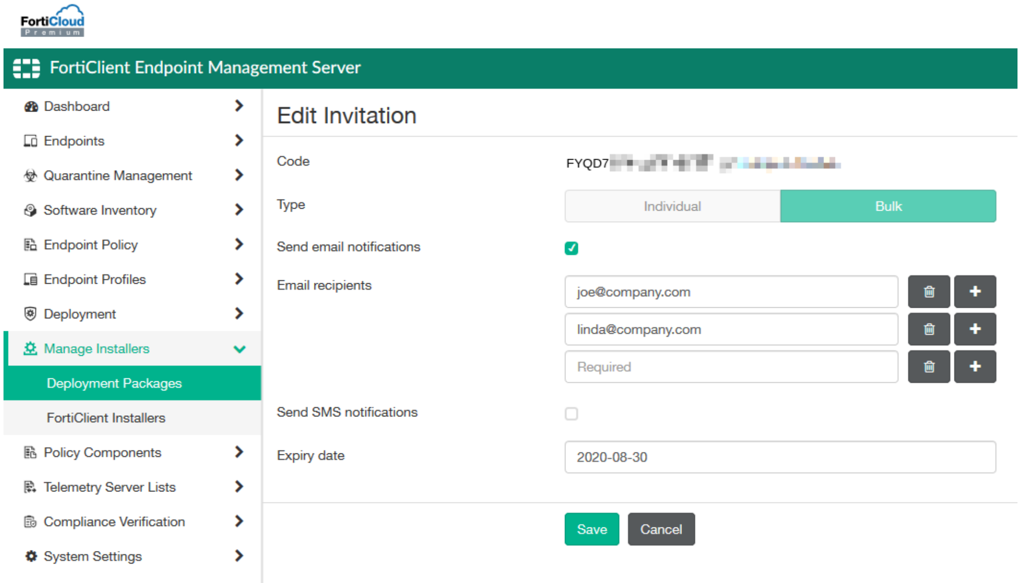
Invitation Code	FYQD7[redacted]
Auto Registration	Enabled
Desktop Shortcut	Enabled
Start Menu Shortcut	Enabled
Notes	FortiClient 6.2.7 GA

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*.



Edit Invitation

Code: FYQD7[redacted]

Type: Individual / Bulk (selected)

Send email notifications: ☑

Email recipients: joe@company.com; linda@company.com; Required

Send SMS notifications: ☐

Expiry date: 2020-08-30

5. (Administrator) The email that users receive for an individual invitation code does not include a FortiClient 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 on your device. The FortiClient Cloud invitation email or text message that you received may include a FortiClient download link. Otherwise, your administrator should have provided the installer files or a link where you can download them.
7. (End user) Your FortiClient may automatically register to FortiClient Cloud after installation. If your FortiClient did not automatically register to FortiClient Cloud, use the instructions in Connecting an endpoint to FortiClient Cloud on page 12 to register to FortiClient Cloud.

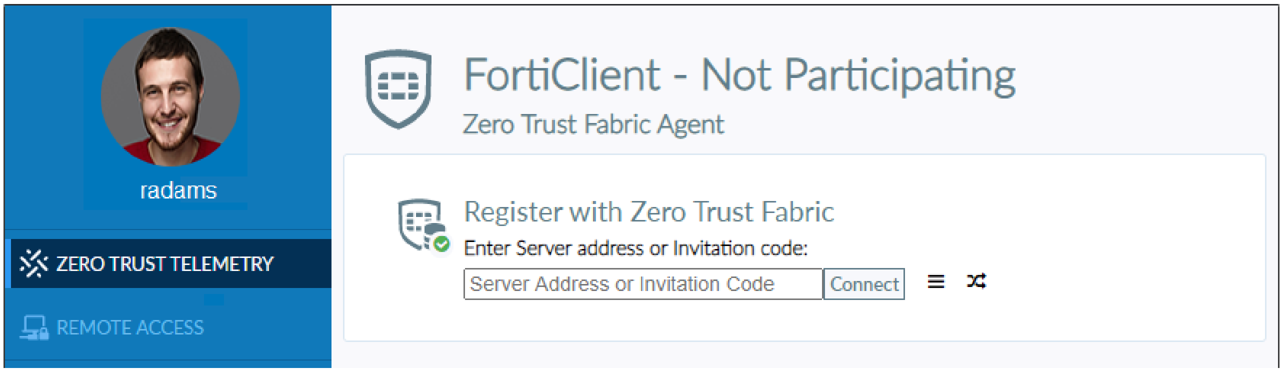
Connecting an endpoint to FortiClient Cloud

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

- If you want to connect a FortiClient 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 your FortiClient did not automatically register to FortiClient Cloud after installation.

To register FortiClient Windows, macOS, or Linux 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 Cloud, enter the invitation code in the *Join FortiClient Cloud* field on the *Zero Trust Telemetry* tab in FortiClient.



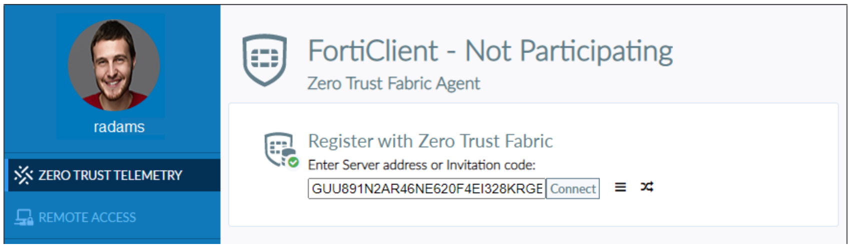
FortiClient - Not Participating

Zero Trust Fabric Agent

Register with Zero Trust Fabric

Enter Server address or Invitation code:

Server Address or Invitation Code



FortiClient - Not Participating

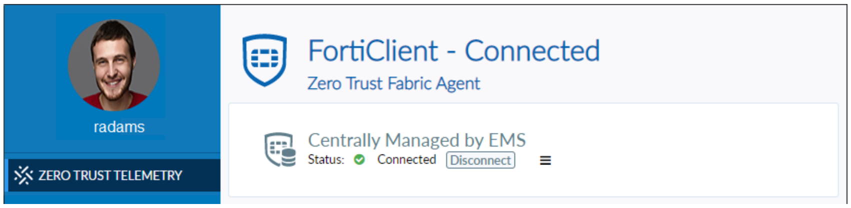
Zero Trust Fabric Agent

Register with Zero Trust Fabric

Enter Server address or Invitation code:

GUU891N2AR46NE620F4EI328KRGE

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



FortiClient - Connected

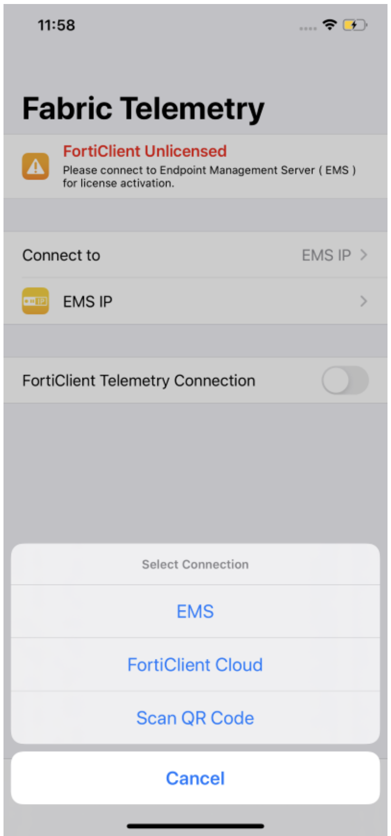
Zero Trust Fabric Agent

Centrally Managed by EMS

Status: Connected

To register FortiClient iOS or Android to FortiClient Cloud:

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



11:58

Fabric Telemetry

FortiClient Unlicensed
Please connect to Endpoint Management Server (EMS) for license activation.

Connect to — EMS IP

EMS IP

FortiClient Telemetry Connection

Select Connection

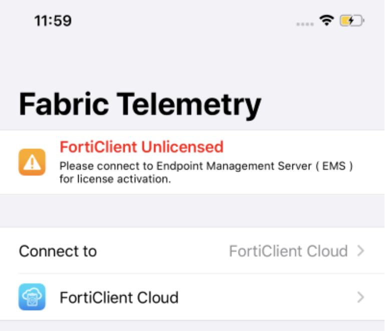
EMS

FortiClient Cloud

Scan QR Code

Cancel

2. Do one of the following:
   a. If using FortiClient (iOS), tap *FortiClient Cloud*.



11:59

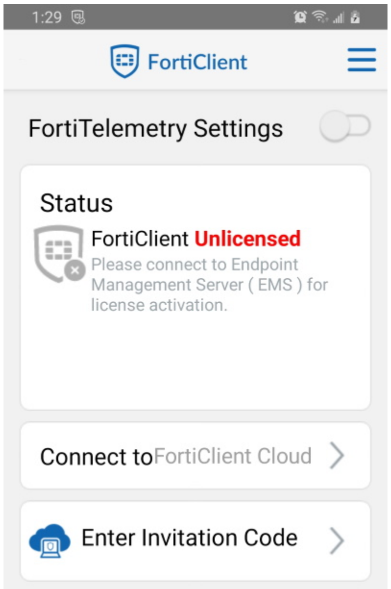
Fabric Telemetry

FortiClient Unlicensed
Please connect to Endpoint Management Server (EMS) for license activation.

Connect to — FortiClient Cloud

FortiClient Cloud

b. If using FortiClient (Android), tap *Enter Invitation Code*.



1:29

FortiClient

FortiTelemetry Settings

Status

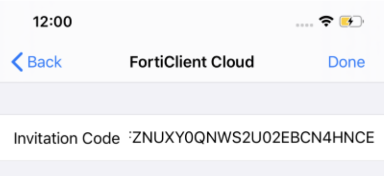
FortiClient **Unlicensed**

Please connect to Endpoint Management Server (EMS) for license activation.

Connect to FortiClient Cloud

Enter Invitation Code

3. Enter the invitation code.

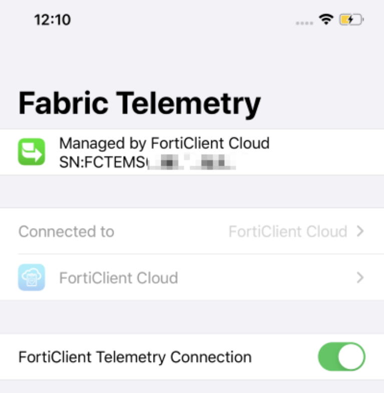


12:00

< Back FortiClient Cloud Done

Invitation Code ZNUXY0QNWS2U02EBCN4HNCE

FortiClient Cloud is now managing FortiClient.



12:10

Fabric Telemetry

Managed by FortiClient Cloud
SN:FCTEMS[redacted]

Connected to FortiClient Cloud >

FortiClient Cloud >

FortiClient Telemetry Connection

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.

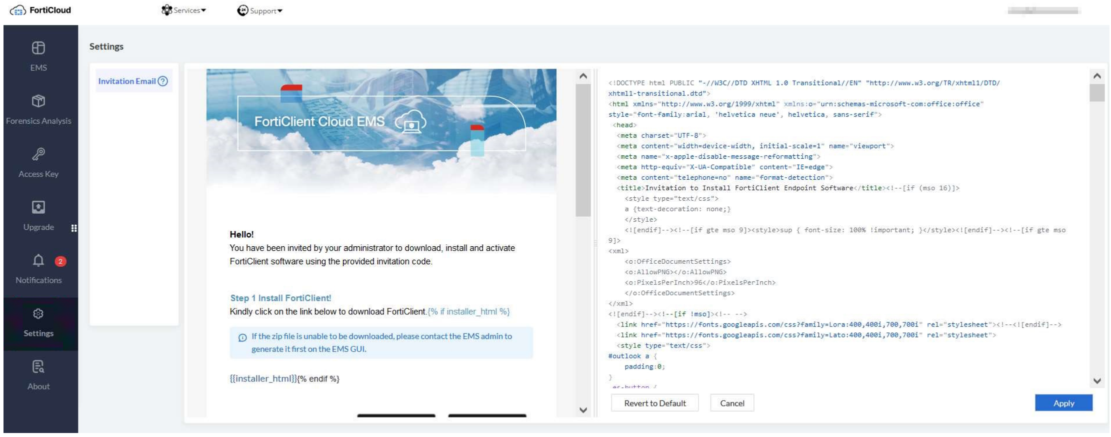
5. Click *Save*. You see a new invitation code for the deployment package.

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.



Hello!
You have been invited by your administrator to download, install and activate FortiClient software using the provided invitation code.

Step 1 Install FortiClient!
Kindly click on the link below to download FortiClient.{% if installer_html %}

If the zip file is unable to be downloaded, please contact the EMS admin to generate it first on the EMS GUI.

{{installer_html}}{% endif %}

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/
xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xmlns:o="urn:schemas-microsoft-com:office:office"
style="font-family:arial, 'helvetica neue', helvetica, sans-serif">
 <head>
  <meta charset="UTF-8">
  <meta content="width=device-width, initial-scale=1" name="viewport">
  <meta name="x-apple-disable-message-reformatting">
  <meta http-equiv="X-UA-Compatible" content="IE=edge">
  <meta content="telephone=no" name="format-detection">
  <title>Invitation to Install FortiClient Endpoint Software</title><!--[if (mso 16)]>
    <style type="text/css">
    a {text-decoration: none;}
    </style>
    <![endif]--><!--[if gte mso 9]><style>sup { font-size: 100% !important; }</style><![endif]--><!--[if gte mso
9]>
<xml>
    <o:OfficeDocumentSettings>
    <o:AllowPNG></o:AllowPNG>
    <o:PixelsPerInch>96</o:PixelsPerInch>
    </o:OfficeDocumentSettings>
</xml>
<![endif]--><!--[if !mso]><!-- -->
  <link href="https://fonts.googleapis.com/css?family=Lora:400,400i,700,700i" rel="stylesheet"><!--<![endif]-->
  <link href="https://fonts.googleapis.com/css?family=Lato:400,400i,700,700i" rel="stylesheet">
  <style type="text/css">
#outlook a {
    padding:0;
}
```

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 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 use FortiClient Cloud running 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 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.

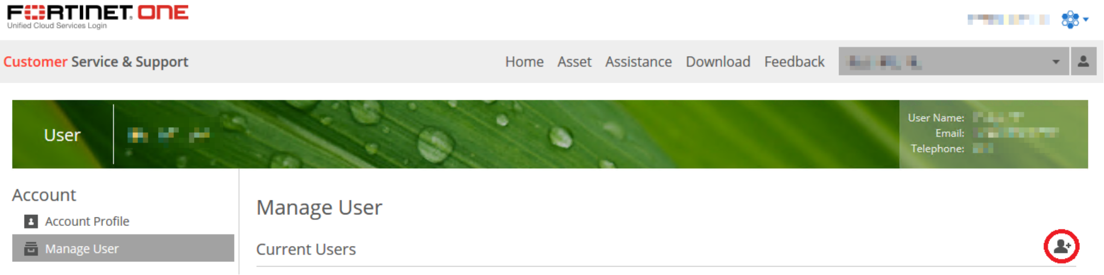
Accounts

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 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 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

On the *Access Key* tab, you can manage access keys for FortiClient Cloud API access. The access keys are your gateway to access FortiClient Cloud APIs.

To view FortiClient Cloud API details in the GUI:

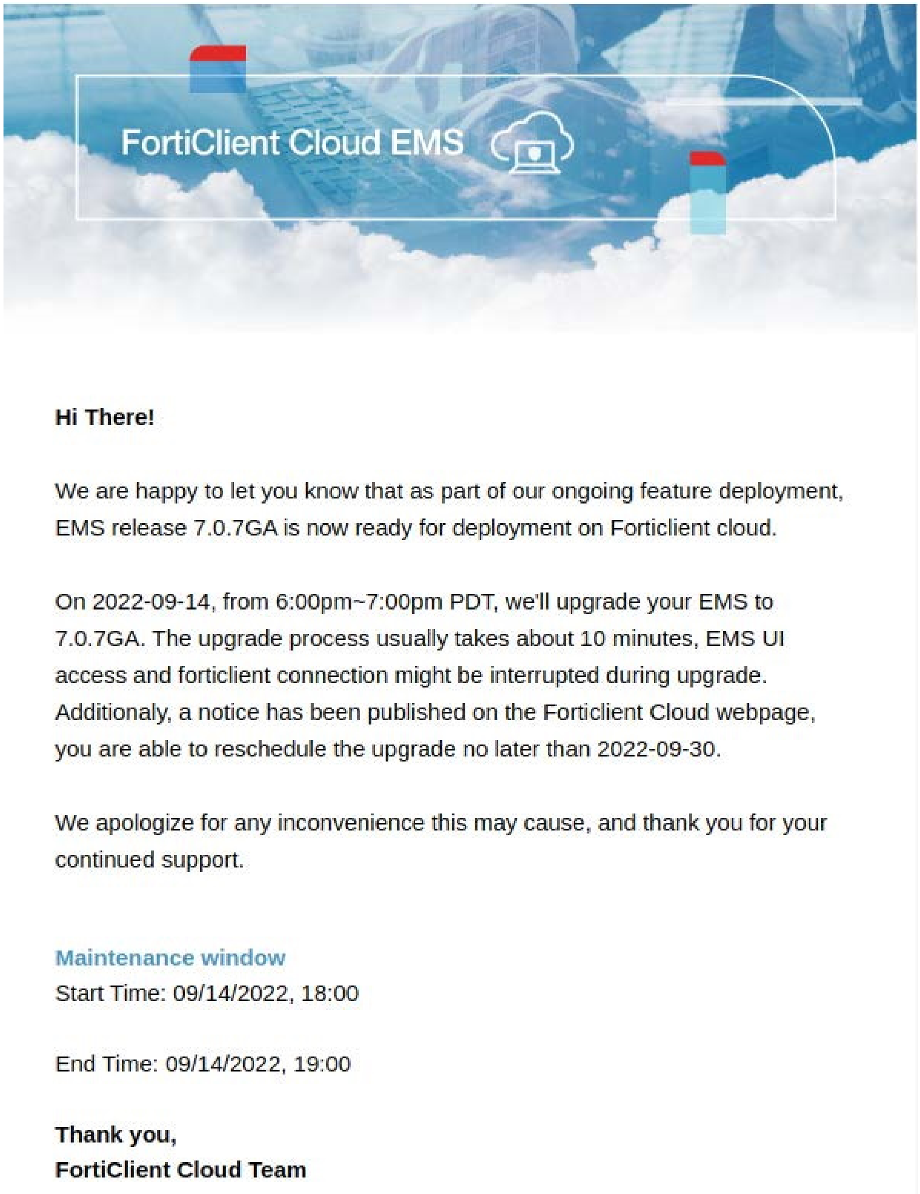
1. In FortiClient Cloud, go to *Access Key*.
2. Beside *Managing access keys for EMS API access*, click the question mark (?). An *Access Key Usage for EMS APIs* dialog opens with instructions on accessing the APIs.

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

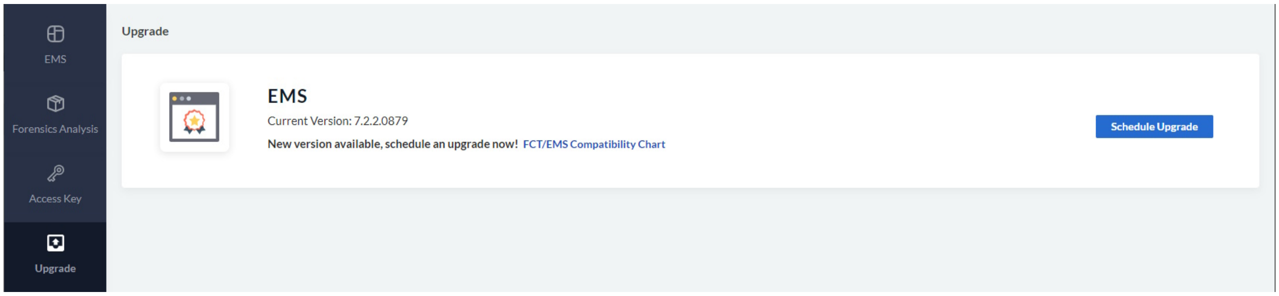
End Time: 09/14/2022, 19:00

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, go to *Upgrade*.
2. Click *Schedule Upgrade*.



EMS

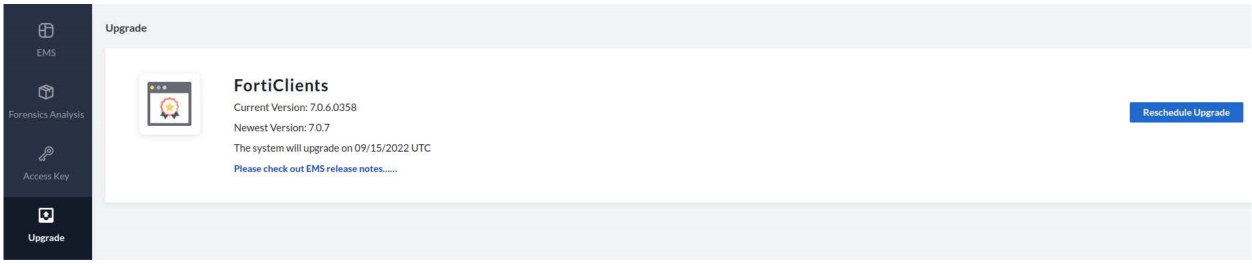
Current Version: 7.2.2.0879

New version available, schedule an upgrade now! FCT/EMS Compatibility Chart

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, go to *Upgrade*.
2. Click *Reschedule Upgrade*.



FortiClients

Current Version: 7.0.6.0358

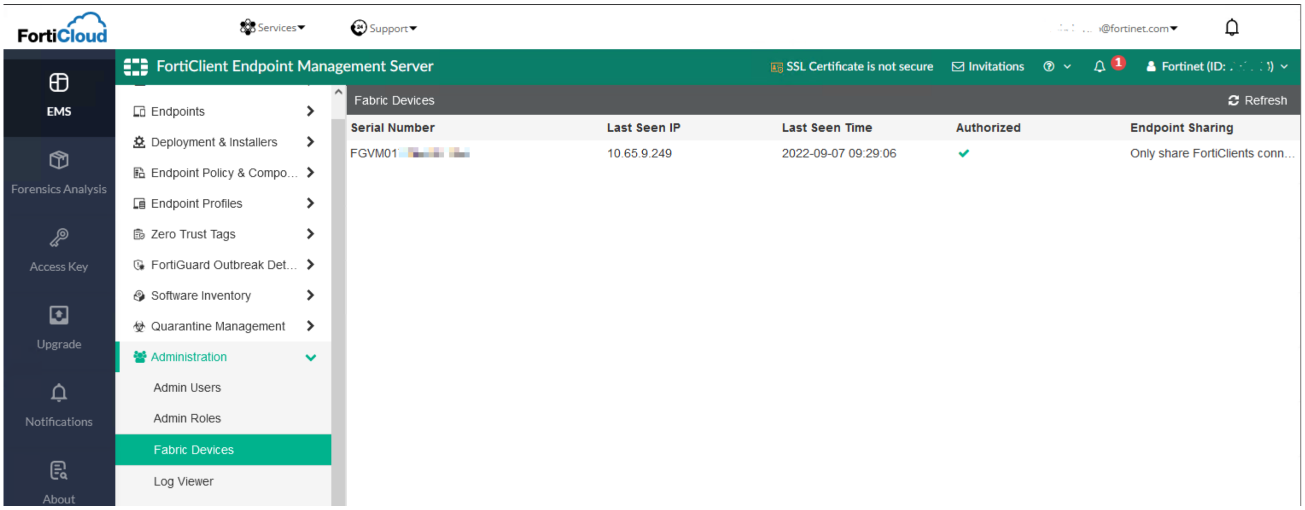
Newest Version: 7.0.7

The system will upgrade on 09/15/2022 UTC

Please check out EMS release notes......

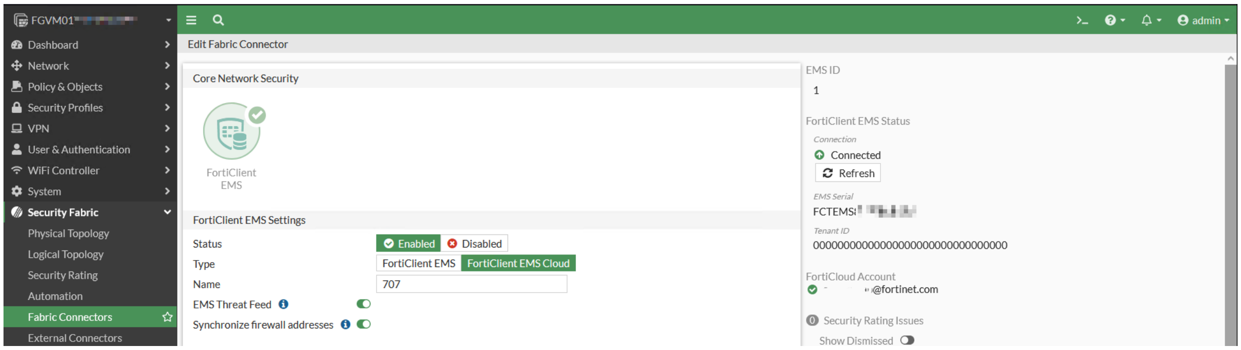
3. In the *System Upgrade Time* field, select the desired date. You must select a date before the displayed last day to upgrade. If you need to upgrade on a day after the displayed last day to upgrade, or you want to cancel the upgrade, contact Fortinet Support.
4. Click *OK*.

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.



Fabric Devices

Serial Number	Last Seen IP	Last Seen Time	Authorized	Endpoint Sharing
FGVM01[redacted]	10.65.9.249	2022-09-07 09:29:06	✓	Only share FortiClients conn...



Edit Fabric Connector

Core Network Security

FortiClient EMS Settings

Status: Enabled | Disabled

Type: FortiClient EMS | FortiClient EMS Cloud

Name: 707

EMS Threat Feed

Synchronize firewall addresses

EMS ID
1

FortiClient EMS Status

Connection
Connected
Refresh

EMS Serial
FCTEMS[redacted]

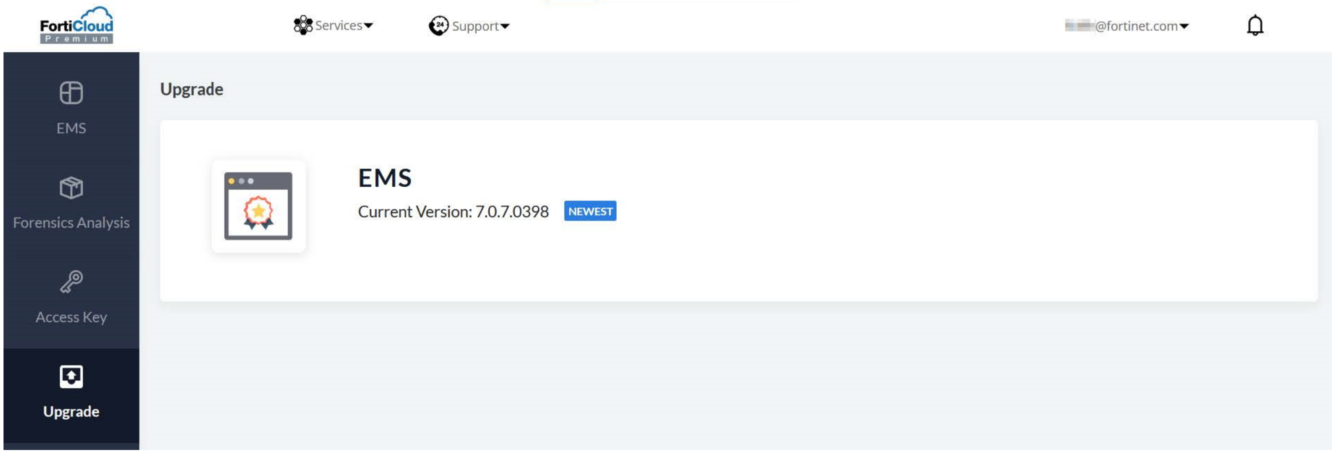
Tenant ID
00000000000000000000000000000000

FortiCloud Account
[redacted]@fortinet.com

Security Rating Issues

Show Dismissed

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



Upgrade

EMS

Current Version: 7.0.7.0398 NEWEST

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

You must allowlist the IP address 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

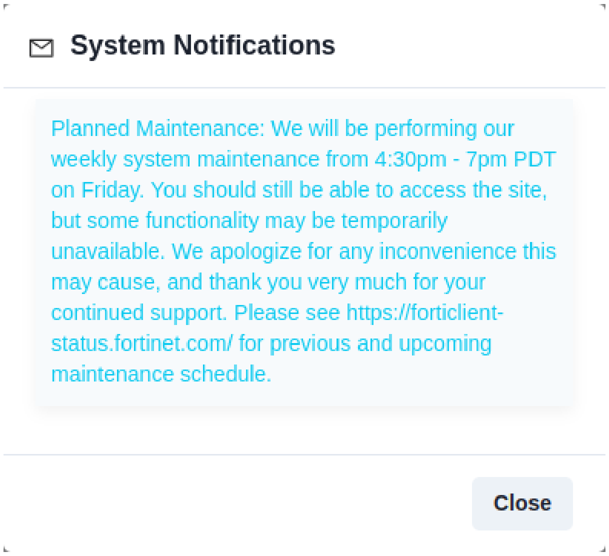
In the FortiClient Cloud portal, go to *About*. The IP address row displays the IP address that you must allowlist for the listed features.

Notifications

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

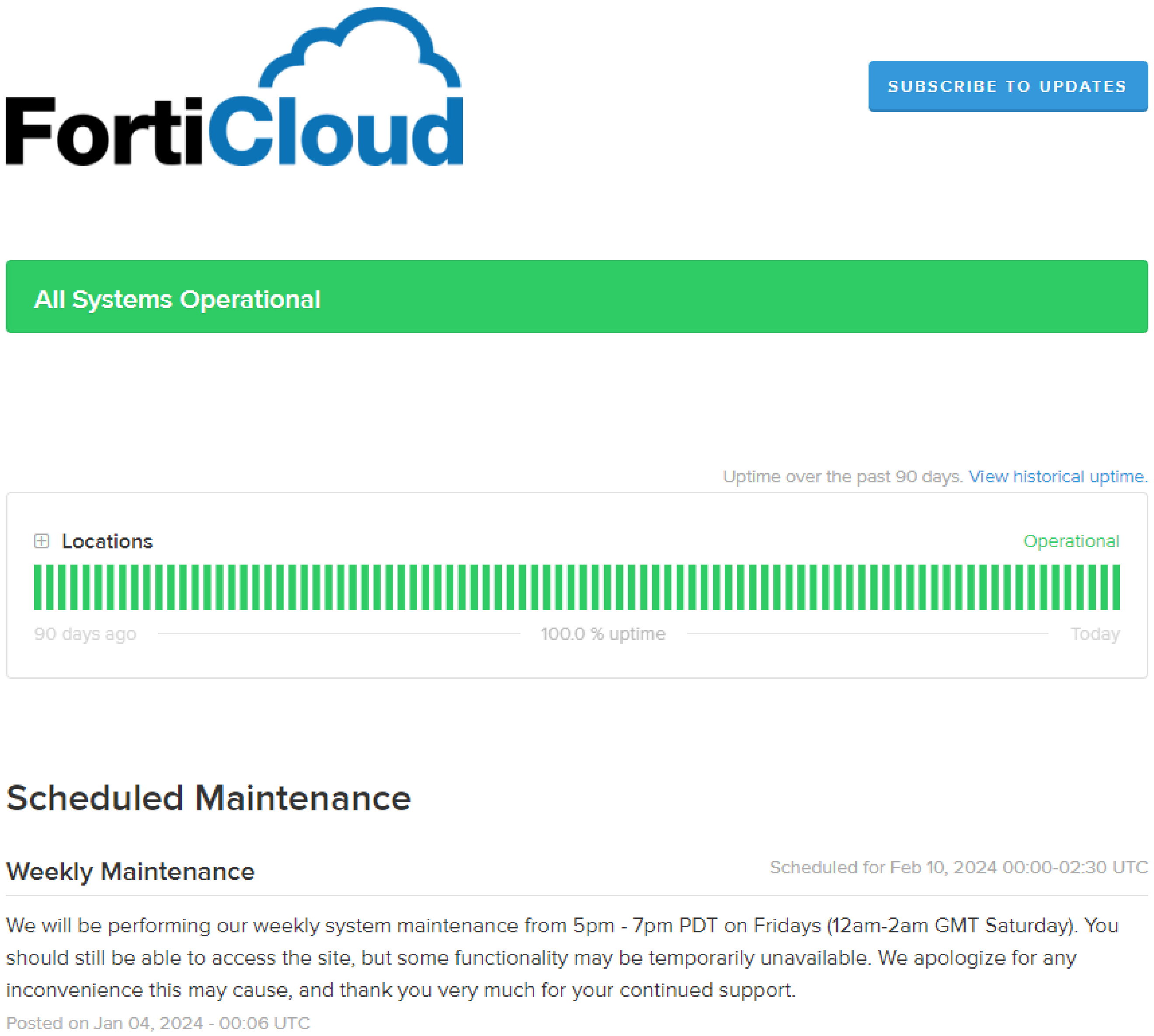
System maintenance

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



Planned Maintenance: We will be performing our weekly system maintenance from 4:30pm - 7pm PDT on Friday. You should still be able to access the site, but some functionality may be temporarily unavailable. We apologize for any inconvenience this may cause, and thank you very much for your continued support. Please see https://forticlient-status.fortinet.com/ for previous and upcoming maintenance schedule.

You can also view this notification from FortiClientCloud Status.



All Systems Operational

Uptime over the past 90 days. View historical uptime.

Locations — Operational

90 days ago — 100.0 % uptime — Today

Scheduled Maintenance

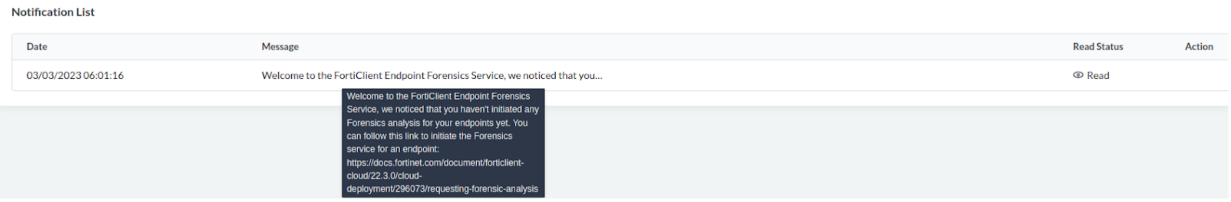
Weekly Maintenance — Scheduled for Feb 10, 2024 00:00-02:30 UTC

We will be performing our weekly system maintenance from 5pm - 7pm PDT on Fridays (12am-2am GMT Saturday). You should still be able to access the site, but some functionality may be temporarily unavailable. We apologize for any inconvenience this may cause, and thank you very much for your continued support.

Posted on Jan 04, 2024 - 00:06 UTC

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:

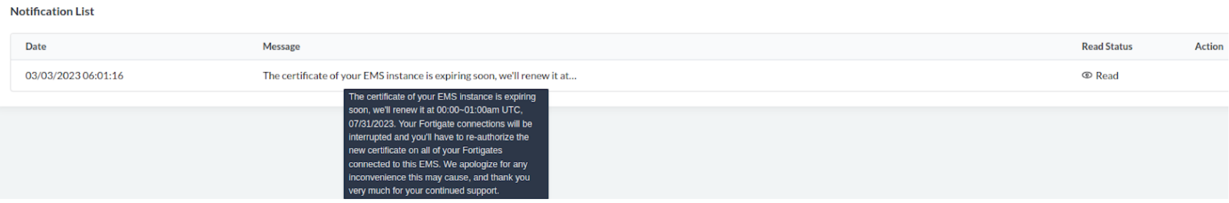


Notification List

Date	Message	Read Status	Action
03/03/2023 06:01:16	Welcome to the FortiClient Endpoint Forensics Service, we noticed that you...	Read	

Welcome to the FortiClient Endpoint Forensics Service, we noticed that you haven't initiated any Forensics analysis for your endpoints yet. You can follow this link to initiate the Forensics service for an endpoint: https://docs.fortinet.com/document/forticlient-cloud/22.3.0/cloud-deployment/296073/requesting-forensic-analysis

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



Notification List

Date	Message	Read Status	Action
03/03/2023 06:01:16	The certificate of your EMS instance is expiring soon, we'll renew it at...	👁 Read	

The certificate of your EMS instance is expiring soon, we'll renew it at 00:00~01:00am UTC, 07/31/2023. Your Fortigate connections will be interrupted and you'll have to re-authorize the new certificate on all of your Fortigates connected to this EMS. We apologize for any inconvenience this may cause, and thank you very much for your continued support.

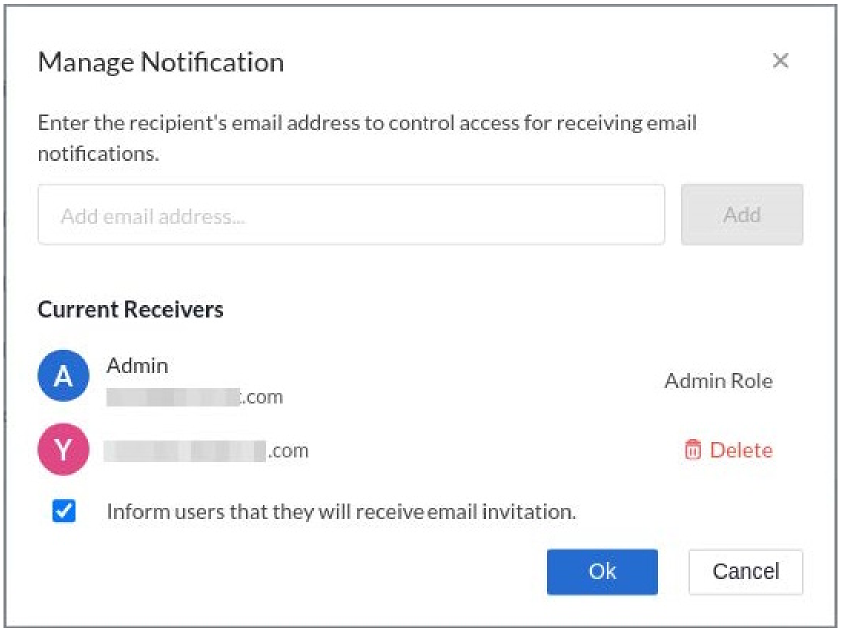
Managing notifications in the FortiClient Cloud portal

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 current notification recipients. Add new recipients by entering their email address in the *Add email address* field or remove current recipients by clicking *Delete*. If you are adding a new recipient, you can select *Inform users that they will receive email invitation.* to notify them that they will receive notifications.



Manage Notification ×

Enter the recipient's email address to control access for receiving email notifications.

Add email address... [Add]

Current Receivers

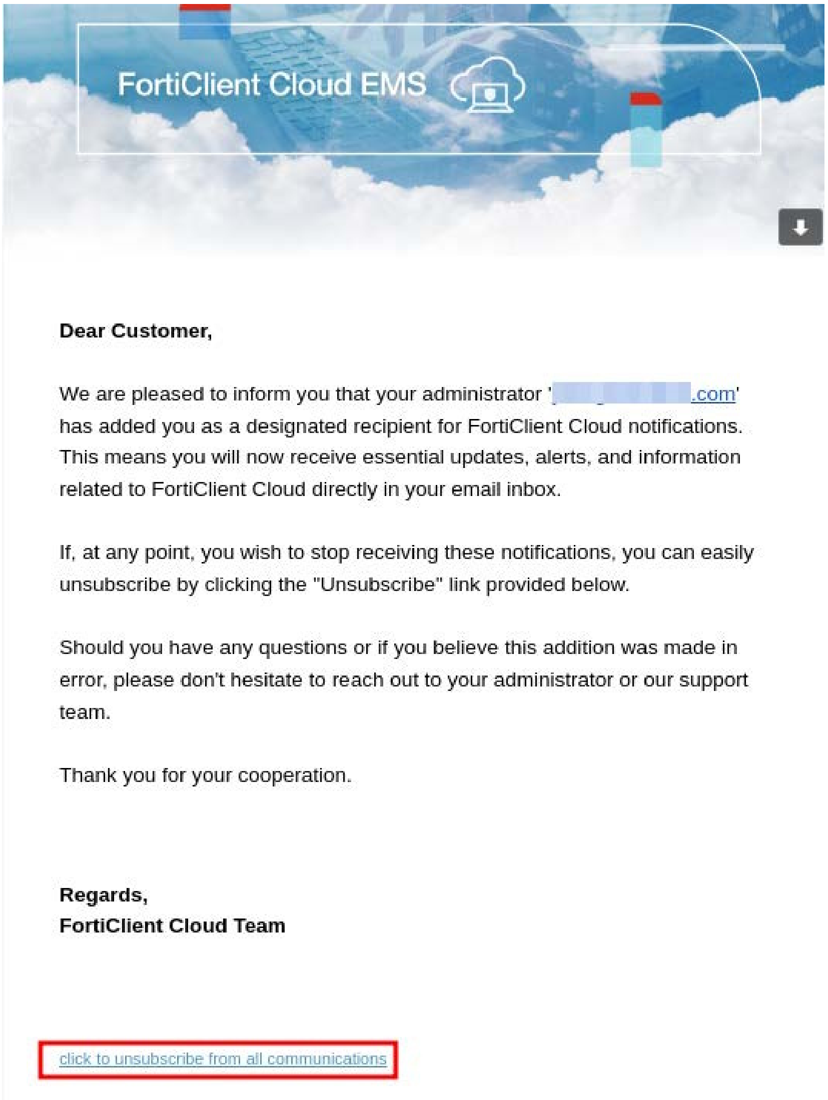
A Admin [redacted].com — Admin Role

Y [redacted].com — 🗑 Delete

☑ Inform users that they will receive email invitation.

[Ok] [Cancel]

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

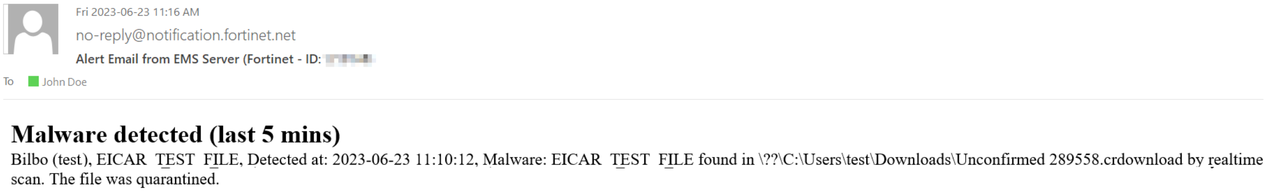
By default, FortiClient Cloud uses the Fortinet built-in email server to send email alerts. This eliminates the need to specify your own SMTP/mail server before sending alert emails. You only need to configure the recipient email addresses.

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.



Fri 2023-06-23 11:16 AM
no-reply@notification.fortinet.net
Alert Email from EMS Server (Fortinet - ID: [redacted]

To 🟩 John Doe

Malware detected (last 5 mins)

Bilbo (test), EICAR_TEST_FILE, Detected at: 2023-06-23 11:10:12, Malware: EICAR_TEST_FILE found in \??\C:\Users\test\Downloads\Unconfirmed 289558.crdownload by realtime scan. The file was quarantined.

Limitations

The management capacity data for the latest EMS 7.2 or 7.0 version applies to FortiClient Cloud depending on your instance. See the management capacity for your instance:

- 7.2
- 7.0

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

The following provides a comparison between FortiClient Cloud and EMS 7.2 and 7.0:

Feature	FortiClient Cloud	EMS 7.2 and 7.0
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
Zero Trust 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 iOS and Android	Yes	Yes
Import web filter policy from FortiOS	Yes	Yes
Browser plugin support	Yes Browser support depends on the endpoint OS and installed FortiClient version.	Yes Browser support depends on the endpoint OS and installed FortiClient version.
Endpoint hardening, visibility, and discovery		
Vulnerability scan	Yes	Yes

Feature	FortiClient Cloud	EMS 7.2 and 7.0
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 Windows Server machine
EMS version	• 7.2 • 7.0	• 7.2 • 7.0
Supported FortiClient agent versions	• 7.2 • 7.0 • 6.4	• 7.2 • 7.0 • 6.4
Active Directory integration	Yes	Yes
Supported platforms	• Windows • macOS • Linux • iOS • Android • Chromebook	• Windows • macOS • Linux • iOS • Android • Chromebook
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 7.

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 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.

Question	Answer
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
2024-01-30	Initial release.
2024-02-08	Added API access keys on page 21.
2024-03-14	Updated: - Introduction on page 4 - Limitations on page 31
2024-04-11	Updated: - Deploying FortiClient Cloud on page 7 - Limitations on page 31

FORTINET®

www.fortinet.com