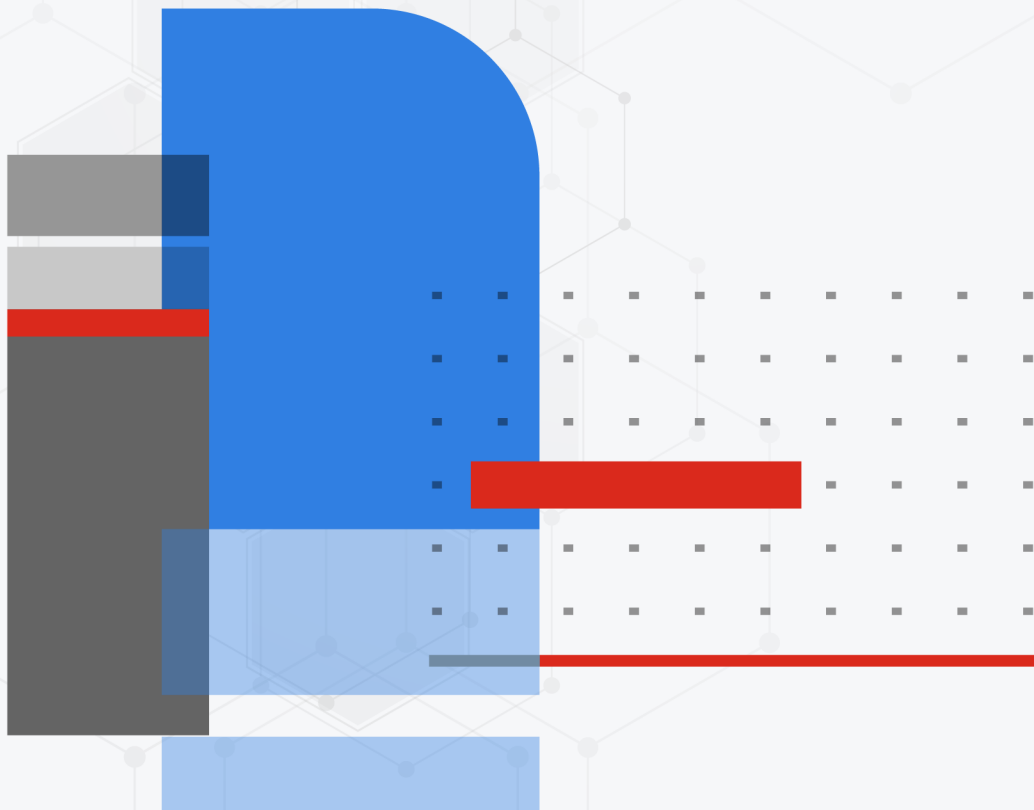




Administration Guide

FortiGate Cloud 23.2



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



May 23, 2023

FortiGate Cloud 23.2 Administration Guide

32-232-903541-20230523

TABLE OF CONTENTS

Change log	6
Introduction	7
Functions	7
Requirements	9
Getting started with FortiGate Cloud	10
Port and access control information	12
License types	14
Feature comparison	15
Upgrading to FortiGate Cloud Premium Portal (Beta)	16
OU	18
Deployment	19
Inventory	22
FortiDeploy	24
FortiCloud and FortiDeploy keys	26
FortiCloud key	26
FortiDeploy key	27
Network Overview	28
Group management	31
Management	34
Config	35
Managing FortiAP, FortiSwitch, and FortiExtender devices	36
Backup	39
Upgrade	40
Script	42
Manage Scripts	43
Analysis	45
FortiView	45
Threats	46
Traffic Analysis	46
Websites	47
DNS	47
FortiView charts reference	48
Monitor	50
Logs from FortiGate	50
Logview	51
Event Management	53
Reports	54
Reports reference	54
Report configurations	57
SandBox	59
Dashboard	60

Files and On-Demand Records	60
Setting	61
Accounts and users	62
Creating an account	62
User management	62
IAM users	62
FortiCloud organizations	63
FortiGate Cloud users	64
Signing in as a FortiGate Cloud user	65
Replacing a FortiGate Cloud user account ID with a new email address	65
Account Setting	66
Audit Log	68
Multitenancy	70
User roles	72
IOC	73
API access	74
Frequently asked questions	77
What do I do if FortiOS returns an Invalid Username or Password/FortiCloud Internal Error/HTTP 400 error when activating FortiGate Cloud on the FortiOS GUI?	77
Why can I log into the FortiGate Cloud but not activate the FortiGate Cloud account in FortiOS with the same credentials?	77
How can I change the FortiGate Cloud account ID from A to B?	78
How can I move a FortiGate from account A to account B in the same region?	78
How can I activate my FortiGate Cloud on HA-paired FortiGates?	78
How can I establish a management tunnel connection between my FortiGate and FortiGate Cloud?	78
What do I do if a FortiGate added by its cloud key stays in an inactive state for more than 24 hours?	78
What do I do if the "Device is already in inventory" message appears when importing a FortiGate by key?	79
What do I do if the invalid key message appears when importing a FortiGate by key?	79
What do I do if FortiGate Cloud activation via the FortiOS GUI succeeds, but I cannot find the FortiGate in the FortiGate Cloud portal?	79
How can I move a FortiGate from region A to region B?	79
How can I connect to FortiGate by remote access?	79
How can I activate FortiGate Cloud using a different email FortiCare account when FortiOS does not allow entering another email?	80
What do I do if the migrate notice still appears after successful migration?	80
What do I do if FortiDeploy does not work?	80
What do I do if FortiOS does not upload logs?	80
What do I do if FortiGate Cloud cannot retrieve logs from FortiOS when data source is set as FortiGate Cloud?	81
How can I export more than 1000 lines of logs?	81
How can I receive a daily report by email?	81

Why does FortiGate not submit files for Sandbox scanning?	81
What backup retention does FortiGate Cloud provide?	81
How does automatic backup work?	82
What does it mean if a geolocation attribute configuration change log/alert is received? ...	82
What do I do if FortiGate Cloud does not reflect a new hostname on a FortiGate or FortiGate Cloud overwrites a new FortiGate hostname?	82
Can I revert back from FortiGate Cloud 2.0 after upgrade?	82
Why is my FortiGate deployed to a region other than global (U.S. or Europe)?	83
How do I check if my FortiGate has been preset for a specific server location?	83
Can I change the server location configuration?	83
If my FortiGate's server location is automatic/any, how do I deploy it to my preferred region?	83
Can I migrate logs uploaded or reports generated to a different region?	84
How do I choose my region for the FortiGate Cloud (Premium) portal?	84
How do I change my region in the FortiGate Cloud (Premium) portal?	84

Change log

Date	Change Description
2023-04-25	Initial release. See What's new for a list of enhancements for this release.
2023-05-11	Updated: • Introduction on page 7 • Functions on page 7 • Getting started with FortiGate Cloud on page 10 • Port and access control information on page 12 • License types on page 14 • SandBox on page 59
2023-05-23	Updated Feature comparison on page 15 .

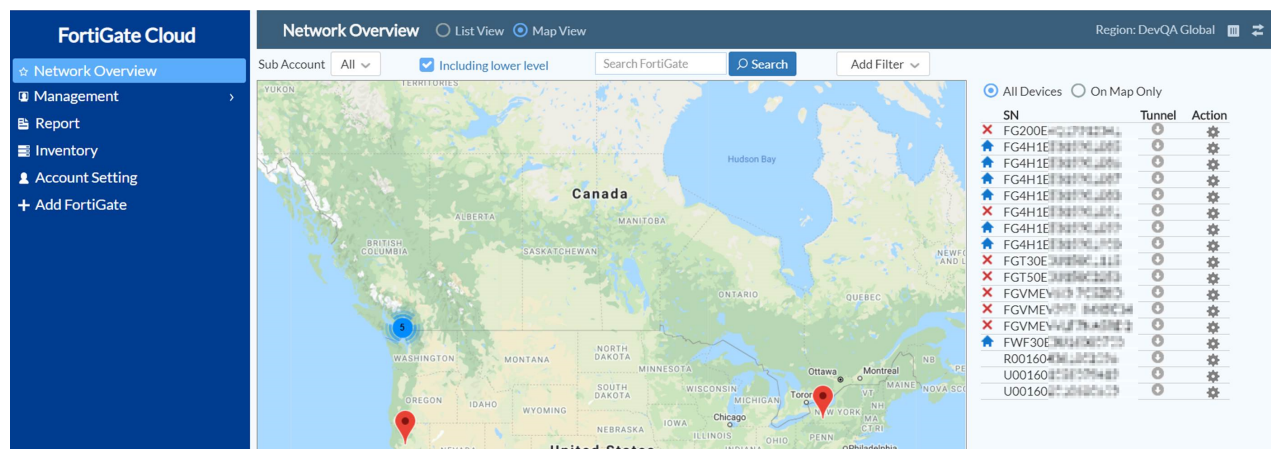
Introduction

FortiGate Cloud is a cloud-based software-as-a-service (SaaS) offering a range of management, reporting, and analytics for FortiGate next generation firewalls. FortiGate Cloud simplifies the initial deployment, setup, and ongoing management of FortiGate with SD-WAN functions, FortiSwitch, FortiAP, and FortiExtender with zero-touch provisioning, providing you with visibility of your entire deployment. FortiGate Cloud grows with your requirements from a single FortiGate to a complete managed security services management solution for thousands of devices across multiple customers. With FortiGate Cloud, you can do the following:

- Manage FortiGate and FortiWifi devices, including configuration, backup, firmware upgrade, and running scripts
- Use Remote Access to easily connect to a device without physical connection
- Run full web, event, and traffic analysis on your FortiGates
- Review different types of past-date logs from your FortiGates
- Create, schedule, and customize a full range of reports
- Receive email alerts on device and network events as configured

To add subaccounts and subaccount users under your primary account, you can upgrade your regular account to a multitenancy account. See [Multitenancy on page 70](#).

FortiGate Cloud also integrates other Fortinet services: FortiSandbox SaaS and FortiDeploy. See [SandBox on page 59](#) and [FortiDeploy on page 24](#).



For information about FortiGate Cloud new features, see the [FortiGate Cloud Release Notes](#).

Functions

FortiGate Cloud has the following functions:

Function	Description
Centralized dashboard	System and log widgets plus real-time monitors.

Function	Description
FortiView log viewer	Real-time log viewing with filters and download capability.
Drilldown analysis	Real-time location, user, and network activity analysis, and alert profiles.
Report generator	Create custom report templates and schedule reports in different formats to display location-based analytics or illustrate network usage platforms.
Device management	Scheduled configuration backup and history and script management. If using multitenancy license, includes group management.
Antivirus (AV) submission	Shows the status of suspicious files undergoing cloud-based sandbox analysis.
AP, FortiSwitch, and FortiExtender management via FortiGate	- Wireless configuration: - View, add, and remove APs managed by FortiGates - View WiFi user statistics and health monitor - Create and edit SSID settings - Create and edit FortiAP profiles - Create and edit WIDS profiles - FortiSwitch management: add, delete, configure, create, and edit FortiSwitch profiles - FortiExtender management: add, delete, deploy, create, and edit FortiExtender profiles
Remote access	Access device configuration from web browser, modify configuration, and push changes through to device through the network.
FortiGate virtual domain (VDOM) support	Support for VDOMs configured in FortiGate devices.
Active Directory (AD) management	Integration with AD.
Firmware upgrade	Remotely upgrade FortiOS on FortiGate devices and FortiAP, FortiSwitch, and FortiExtender devices connected to the FortiGate.
Event management	Set up email alerts for specific network structure emergencies, such as FortiGate Cloud losing connection to the device, or the device's power supply failing.
Regions	Datacenters located in Canada, Germany, the United States, and Japan for better performance and GDPR compliance for international customers. FortiGate Cloud includes the Global, Europe, U.S., and Japan regions. FortiSandbox SaaS includes the Global, Europe, U.S., and Japan regions. For U.S. government devices, the default datacenter is the U.S. datacenter, and the device is provisioned to FortiGate Cloud's U.S. region. The U.S. datacenter stores the data of FortiGates with the US-Government license key or that are provisioned to the U.S. region with a paid FortiGate Cloud Service subscription. FortiGates that are provisioned to the U.S. region without paid FortiGate Cloud Service subscriptions use the Canada datacenter.

Requirements

The following items are required before you can initialize FortiGate Cloud:

Requirement	Description
FortiCloud account	Create a FortiCloud account if you do not have one. Launching FortiGate Cloud requires a FortiCloud account. A primary FortiCloud account can invite other users to launch FortiGate Cloud as secondary administrator/regular users. Some customers may be using their FortiCloud or FortiCare account. Merging these accounts to your FortiCloud account is strongly recommended.
FortiGate/FortiWifi license	You must register all FortiGate/FortiWifi devices on FortiCloud.
FortiGate Cloud entitlement	Purchase FortiGate Cloud licenses from Fortinet.
Internet access	You must have Internet access to create a FortiGate Cloud instance and to enable devices to communicate with and periodically send logs to FortiGate Cloud.
Browser	FortiGate Cloud supports Firefox, Chrome, and Edge.

FortiGate Cloud supports all high-end, mid-range, and entry-level FortiGate models. You can find more information about FortiGate models and specifications on the [Fortinet website](#). All FortiWifi models support FortiGate Cloud.

See [Product Life Cycle](#). FortiGate Cloud supports the following:

- FortiGate Cloud supports 30E, 50E, and 240D models, where 7.0 is unavailable, until the hardware EOS.
- For devices with a free subscription, FortiGate Cloud supports the latest three major.minor versions.

Upgrading your device to the latest firmware or replacing EOS hardware is recommended for continued support and security.

The following summarizes FortiGate Cloud support for older FortiOS versions:

- FortiGate Cloud will support FortiOS 5.X and 6.2 until March 31, 2024.
- FortiOS 6.4:
 - FortiGate Cloud will support FortiGates on FortiOS 6.4 with a FortiCare Elite license until March 31, 2026.
 - Otherwise, FortiGate Cloud will support FortiGates on FortiOS 6.4 until June 30, 2024.

For FortiDeploy, FortiGate Cloud supports FortiGate/FortiWifi/POE desktop and 1U models up to 900D running FortiOS 5.2.2 and later. See [FortiDeploy on page 24](#).

The following table lists port numbers that outbound traffic requires. On request, Fortinet can supply the destination IP addresses to add to an outbound policy, if required.

Purpose	Protocol	Port
Syslog, registration, quarantine, log, and report	TCP	443
OFTP	TCP	514
Management	TCP	541

Purpose	Protocol	Port
Contract validation	TCP	443
Config portal	TCP	8443

Getting started with FortiGate Cloud

After activating your FortiCloud single sign on account and ensuring that you have met all requirements in [Requirements on page 9](#), go to one of the following to access FortiGate Cloud:

Region	URL
Global	https://forticloud.com
Europe	https://europe.forticloud.com
U.S.	https://us.forticloud.com

When you initially log in to the FortiGate Cloud portal, the login page displays. The login page displays all accounts that you have access to. The page lists regions that each account can access. You can also search for an account using the serial number of a FortiGate deployed on that account. Click the *Access* link beside the desired account.

FortiGateCloud Search accounts by SN 		
Account  @gmail.com	Region FortiGate Cloud Global	Access
Account  @fortinet.com	Region All Region	Access
Account  @fortinet.com	Region All Region	Access

If the FortiGate Cloud account does not have a FortiCloud ID or does not exist in FortiCare, FortiGate Cloud displays a registration dialog when you log in to the account. After you enter all required information and click *Register*, the account is registered to FortiCare.

Register your FortiCloud Account

Company:

Address:

Country:

Select a Country

City:

State/Province:

ZIP/Postal Code:

Phone:

Fax:

Industry:

Select an organization industry

Organization Size:

Select an organization size

Master User: @gmail.com

First Name:

Last Name:

Password for Verification:

Register

Close

After you access the desired account, the FortiGate Cloud portal displays the *Network Overview* page. You can access notifications regarding maintenance, multitenancy expiration, and unregistered devices from the FortiCloud banner at the top of the page. You can access FortiGate Cloud documentation from the ? icon on the lower banner.

The *Network Overview* page displays the list of devices that are currently deployed to FortiGate Cloud. From the left pane, you can access other options including scripts, reporting, and account settings features.

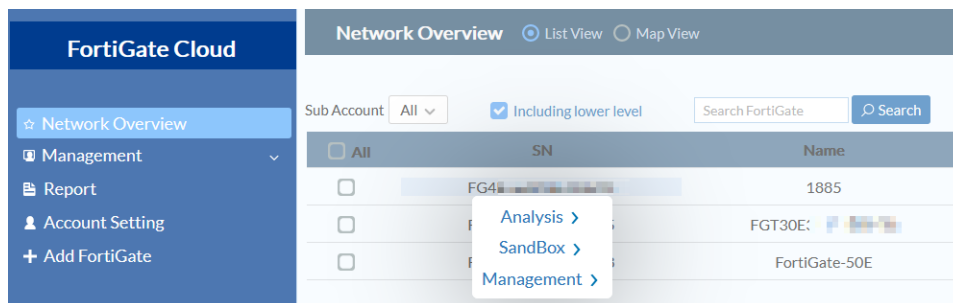
SN	Name	Sub Account	Firmware	Status	Management Connectivity
FG4		sub_2			
FG4		< Default >			
FG4		< Default >			
FG4		< Default >			
FGT5	FGT50E	< Default >	6.2.6		
FGT6	FGT60C	< Default >	5.6.13		
FGT6		< Default >			
U00	S248EFTF1	< Default >			
U001	FGT30E3U1	< Default >			

The following describes the portal options available from the left pane:

Option	Description
Network Overview	<i>Network Overview</i> displays a list of devices that are currently deployed to FortiGate Cloud. For details on actions available in <i>Network Overview</i> , see Network Overview on page 28 .
Management	<i>Manage Scripts</i> : Create script files to check device status or get bulk configuration information quickly. See Manage Scripts on page 43 .

Option	Description
Report	Create and alter report configurations and their settings. These report configurations are available for all deployed devices. See Report configurations on page 57 .
Inventory	View a centralized inventory of all FortiGate and FortiWiFi devices from all FortiGate Cloud instances in a domain group, regardless of datacenter. See Inventory on page 22 .
Account Setting	Add and manage FortiGate Cloud administrator accounts. See Account Setting on page 66 .
Add FortiGate	Add a FortiGate or FortiWiFi device to FortiGate Cloud using a FortiCloud key. See To deploy a FortiGate/FortiWiFi to FortiGate Cloud using the FortiCloud key: on page 19 .

FortiGate Cloud also provides the device-specific *Analysis*, *SandBox*, and *Management* modules. To access *Analysis*, *SandBox*, and *Management*, select the desired device in *Network Overview*, then click the desired link.



The following describes the device-specific modules available:

Option	Description
Analysis	Monitor and log your device's traffic for centralized oversight of traffic and security events. See Analysis on page 45
SandBox	Upload and analyze files that FortiGate AV marks as suspicious to FortiSandbox SaaS. See SandBox on page 59 .
Management	Remotely manage FortiGate and FortiWiFi devices that are connected to the FortiGate Cloud service. See Management on page 34 . For details on remotely accessing a device, see To remotely access a device: on page 34 .

Port and access control information

FortiGate Cloud uses TCP ports 80, 443, 514, 541, and UDP ports 5246/5247. IP address ranges differ depending on the region:

Region	IP address range
Global	208.91.113.0/24, 173.243.132.0/24
Japan	208.91.113.0/24, 173.243.132.0/24 Subnet is 210.7.96.0/24. Gateway IP address is 210.7.96.1.
Germany	154.52.10.0/24
France	154.45.6.0/24

The following summarizes FortiSandbox SaaS (SaaS) information for FortiGate Cloud:

Region	IP address range
Global	173.243.139.0/24, 184.94.112.0/24, 154.52.26.0/24
Japan	210.7.96.0/24, 154.52.7.0/24
EU	83.231.212.128/25, 154.45.1.0/24, 154.52.11.0/24
US	208.184.237.0/24, 209.66.107.0/24

License types

You can use FortiGate Cloud for free or with a subscription.



You do not need a support contract to enable the service. However, you must register each device on the [Fortinet Support site](#). You cannot enable FortiGate Cloud (free or subscribed) without registering each device in your network.

You can enjoy the free subscription of FortiGate Cloud on any FortiGate or FortiWifi device, or purchase an annual-subscription-based license with a one-, two-, or three-year service term. A FortiGate Cloud license entitles devices to advanced features including the Indicator of Compromise (IOC) service, as well as one-year log retention compared to the seven-day log retention with the free subscription.

To activate FortiGate Cloud, you must acquire a subscription license based on the SKUs listed in the following table:

Description	SKU
FortiGate Cloud management, analysis, and one-year log retention	
FortiGate and FortiWifi	FC-10-00XXX-131-02-DD
FortiGate Cloud IOC	
FortiGate 20 to 90 models	FC-10-90803-142-02-12
FortiGate 100 to 300 models	FC-10-90804-142-02-12
Other services	
FortiGate Cloud multitenancy	FCLE-10-FCLD0-161-02-12
FortiDeploy access	FDP-SINGLE-USE
FortiGate Cloud Sandbox	FC-10-XXXX-811-02-DD
	FC-10-XXXXX-879-02-DD
	FC-10-XXXXX-950-02-DD
	FC-10-XXXXX-928-02-DD
	FC-10-XXXXX-100-02-DD

For the IOC license, activation on device requires FortiOS 5.4.2 or later.

You must purchase a subscription for each FortiGate in a high availability (HA) cluster. FortiGate Cloud handles each device separately regardless of configuration. FortiGate Cloud accepts inbound logs from each device independently and cannot detect whether connected devices are in an HA cluster. Though multiple HA clustered devices theoretically send identical logs to FortiGate Cloud, if one device stops logging or cannot reach FortiGate Cloud, the other devices do not send logs on its behalf.

The FortiSandbox SaaS feature allows the following file upload sources:

- File uploads from FortiGate:
 - For a FortiGate with a free subscription, FortiSandbox SaaS supports up to 100 uploads per day or two uploads per minute.
 - For a FortiGate with a paid subscription, the limits are as follows:

FortiGate model	Per minute	Per day
FortiGate 30-90/VM00	5	7200
FortiGate 100-400/VM01	10	14400
FortiGate 500-900/VM02, VM04	20	28880
FortiGate 1000-2000/VM08, VM16	50	72000
FortiGate 3000/VM32 and higher models	100	144000

- For manual uploads from FortiGate Cloud, FortiSandbox SaaS supports up to 50 uploads per day per account.

For pricing information, contact your Fortinet partner or reseller.

FortiGate Cloud reserves the right to impose limits upon detection of abnormal or excessive traffic originating from a certain device and perform preventive measures including blocking the device and restricting log data.

Feature comparison

FortiGate Cloud offers a different feature set depending on whether or not the device has a paid subscription. The following chart shows the features available for FortiGate Cloud for these scenarios:

Feature	Device without paid subscription	Device with paid subscription
Analysis	Yes	Yes
FortiView	Yes	Yes
Monitor	Yes	Yes
Logview	Yes	Yes
Log retention	Seven days	One year
Raw log download	No	Yes
Event Management	No	Yes
360 Degree Activity Report	Yes	Yes
All other reports	No	Yes
Sandbox	Yes	Yes
Audit Log	Yes	Yes
Management	No	Yes

Feature	Device without paid subscription	Device with paid subscription
Configuration management	No	Yes
Configuration backup and restoration	No	Yes
Scripts	No	Yes
Remote access	Yes In FortiGate Cloud 23.3, remote access with read and write rights will require registered FortiGate Cloud Service subscription on FortiGate (enforcement starting from the following FortiOS versions: • 7.4.1 • 7.2.6 • 7.0.13	Yes
Firmware upgrade	No	Yes
Multitenancy	No	No

You can enable multitenancy features by activating a multitenancy license on a regular account. For details, see [Multitenancy on page 70](#).

Upgrading to FortiGate Cloud Premium Portal (Beta)

FortiGate Cloud Premium Portal (Beta) is available to upgrade your FortiGate Cloud environment to. The FortiGate Cloud Premium Portal (Beta) provides the following features:

- Centralized dashboard
- Enhanced user experience with a modern theme and smoother performance
- Full real-time FortiOS configuration management and log analysis for paid tier devices
- Centralized logging, analytics, and reports powered by [FortiAnalyzer Cloud](#)
- Read-only configuration view for free tier devices

The following summarizes eligibility requirements for FortiGate Cloud Premium Portal (Beta):

- All FortiGates in the FortiGate Cloud account must be registered to the same account in FortiCloud Asset Management.
- For FortiGate Cloud accounts in the global/Europe region, the account must have been created within the last six months.
- FortiGate Cloud Premium Portal (Beta) is unavailable in the Japan region.
- You must migrate a multitenancy account to organizational unit to use FortiGate Cloud Premium Portal (Beta).

To upgrade your environment:

1. Add FortiGates with a FortiGate Cloud subscription (FortiGate Cloud Management, Analysis, and 1 Year Log Retention) to your FortiCloud account.

-
2. Upgrade all FortiGates with a subscription to FortiOS 7.0.2 or a later version. FortiGate Cloud Premium Portal (Beta) allows FortiGates without a subscription to have any version of FortiOS installed.
 3. Log in to your FortiGate Cloud environment.
 4. The portal displays an upgrade dialog. Read and select the acknowledgment checkboxes, then click *Proceed with Upgrade*. The dialog only displays for the first user who logs in to an account that is eligible for upgrade. If you do not see the upgrade dialog, click the *Upgrade* button in the upper right corner. The upgrade typically takes five minutes. If the upgrade cannot complete after 30 minutes, it times out and you can restart the upgrade procedure.

When accounts in the U.S. region upgrade to FortiGate Cloud Premium Portal (Beta), the upgrade migrates existing logs and reports to the FortiGate Cloud Premium Portal (Beta) portal. This migration does not occur for accounts in other regions.

See the [FortiGate Cloud Premium Portal \(Beta\) Administration Guide](#) for details on FortiGate Cloud Premium Portal (Beta).

OU

FortiGate Cloud supports organizational unit (OU) account selection and switching. OU support is currently in beta and available to external customers with FortiCloud Premium license accounts. See [Organization Portal](#) for details on creating an OU.

To move to another OU or account, select the desired OU from the dropdown list in the upper right corner.

When you log in to an OU, FortiGate Cloud displays an OU dashboard. The following lists OU dashboard widgets:

Widget	Description
Devices	Displays a donut chart that details the device type breakdown and total number of devices in this OU.
Accounts	Displays a donut chart that details the total number of accounts in this OU.
Management Connectivity	Displays a donut chart that details the management connectivity status breakdown and total number of devices in this OU.
FortiGate Cloud License	Displays a donut chart that details the FortiGate Cloud license type breakdown and total number of devices in this OU.
Sandbox License	Displays a donut chart that details the Sandbox license type and total number of devices in this OU.

Deployment

You can deploy FortiGate Cloud using one of the following methods:

- [FortiCloud key](#)
- [FortiDeploy bulk key](#)
- [FortiOS GUI](#)

After deploying FortiGate Cloud using one of the methods described, complete basic configuration by doing the following:

1. Create a firewall policy with logging enabled. Configure log uploading if necessary.
2. Log in to FortiGate Cloud using your FortiCloud account.



For FortiGates that are part of a high availability (HA) pair, you must activate FortiGate Cloud on the primary FortiGate. Activate FortiGate Cloud on the primary FortiGate as [To deploy a FortiGate/FortiWifi to FortiGate Cloud in the FortiOS GUI: on page 20](#) describes. FortiGate Cloud activation on the primary FortiGate activates FortiGate Cloud on the secondary FortiGate. Local FortiGate Cloud activation on the secondary FortiGate fails.

For a FortiGate with a US-Government license to use the US region service of FortiGate Cloud, you must import the device into your US region FortiGate Cloud account by a cloud/FortiDeploy key or use the CLI login command `execute fortiguard-log login <email> <password> US` if cloud/FortiDeploy key is unavailable.

To deploy a FortiGate/FortiWifi to FortiGate Cloud using the FortiCloud key:

1. Log in to the [FortiGate Cloud portal](#).
2. Do one of the following:
 - a. Click *Add Fortigate*.

FortiGate Cloud

- Network Overview
- Management
 - Manage Scripts
- Report Configuration
- Add Fortigate**
- Inventory
- My Account

Add Fortigate

Please input the FortiGate Cloud Key to add a FortiGate:

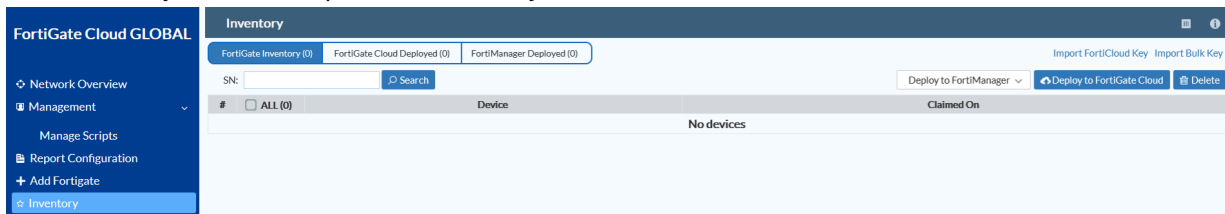
Select Display Timezone for Device
(GMT-12:00) International Date Line West

Select Sub Account

- ☒ < Default >
- ☐ 100E
- ☐ 60D
- ☐ 60F
- ☐ 61E
- ☐ vm

Submit

- b. Go to *Inventory*, then click *Import FortiCloud Key*.



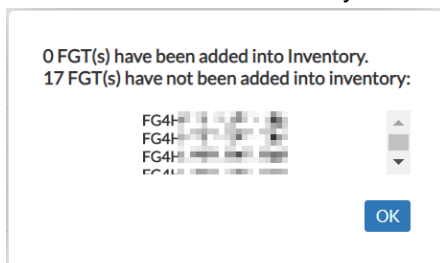
3. Enter the key printed on your FortiGate.
4. From the *Select Display Timezone for Device* dropdown list, select the desired time zone.
5. Under *Select Sub Account*, select the desired subaccount.
6. Click *Submit*.



After the device successfully deploys, the device key becomes invalid. You can only use the key once to deploy a device.

To deploy multiple FortiGate/FortiWifi devices to FortiGate Cloud using a FortiDeploy bulk key:

1. Log in to the FortiGate Cloud portal, then click *Inventory*.
2. Click *Import Bulk Key*.
3. In the *Please input the Bulk Key:* field, enter the FortiDeploy bulk key.
4. Click *Submit*. The portal displays a list of the FortiGate/FortiWifi serial numbers associated with the bulk key. If FortiGate Cloud fails to add any FortiGate/FortiWifi devices, it lists those failed devices' serial numbers.



To deploy a FortiGate/FortiWifi to FortiGate Cloud in the FortiOS GUI:

1. In the FortiCloud portal, ensure that you have a product entitlement for FortiGate Cloud for the desired FortiGate or FortiWifi.
2. In FortiOS, do one of the following:
 - a. Go to *Security Fabric > Fabric Connectors*, and enable *Central Management*. For *Type*, select *FortiGate Cloud*.
 - b. In the *Dashboard*, in the *FortiGate Cloud* widget, the *Status* displays as *Not Activated*. Click *Not Activated*.
3. Click *Activate*.
4. In the *Activate FortiGate Cloud* panel, for *Account*, select *FortinetOne*.
5. In the *Email* and *Password* fields, enter the email address and password associated with the FortiCloud account.

6. Enable *Send logs to FortiGate Cloud*. Click *OK*.

FGVM: Activate FortiGate Cloud

FortiGate

Account **FortinetOne** Standalone

Email

Password

Domain

☒ Send logs to FortiGate Cloud

OK Cancel

7. This automatically enables *Cloud Logging*. Ensure that *Cloud Logging* is enabled. If it is disabled, enable it, then set *Type* to *FortiGate Cloud*.

Security Fabric Settings

☐ FortiGate Telemetry

☐ FortiAnalyzer Logging

☒ Cloud Logging

Type **FortiGate Cloud** FortiAnalyzer Cloud

Account johnhuang@company.com [Logout](#)

Region GLOBAL

Upload option Realtime Every Minute **Every 5 Minutes**

FortiAnalyzer

Cloud Solutions

[Amazon Web Services Marketplace](#)

[Microsoft Azure Marketplace](#)

[Google Cloud Platform Marketplace](#)

Guides

[Introduction to FortiAnalyzer](#)

[Configure FortiAnalyzer in AWS](#)

FortiSandbox

Cloud Solutions

[Amazon Web Services Marketplace](#)

Guides

8. At this point you can access Analysis and SandBox features for this device. To access Management features, you must authorize the FortiGate in FortiGate Cloud by entering the a local superadministrator username and password when prompted. After authorization, you can manage that FortiGate from FortiGate Cloud.
9. You must set the central management setting to FortiCloud, as this is the initial requirement for enabling device management features.

To unsubscribe from FortiGate Cloud:

You can disconnect your account from the dashboard in your FortiGate/FortiWifi.

1. In the FortiOS *Dashboard FortiGate Cloud* widget, the *Status* appears as *Activated*. Click *Activated*, then click the *Logout* button.
2. In the confirmation dialog, click *OK*. This detaches the FortiGate/FortiWifi from the account and stops uploading logs.

To move a FortiGate/FortiWifi deployed to FortiGate Cloud to another account:

To move a FortiGate/FortiWifi that is already deployed to FortiGate Cloud to another account and retain its historical data, you must follow these instructions.

1. Log in to the FortiGate Cloud portal using the account that the FortiGate/FortiWifi is currently deployed on.
2. Click the *Config* icon for the desired device.
3. Click *Migrate Existing Data*.
4. In the *Account ID* field, enter the desired new account. Click *Submit*.

5. In FortiOS, go to *Security Fabric > Settings*. Log out of the FortiGate Cloud account that the FortiGate/FortiWifi is currently deployed on.
6. Deploy the device to FortiGate Cloud using the new account by following the instructions for [To deploy a FortiGate/FortiWifi to FortiGate Cloud in the FortiOS GUI: on page 20](#).

After moving a FortiGate to another FortiGate Cloud account, you must also transfer that FortiGate to the same account in FortiCloud.

Inventory

Inventory displays a centralized inventory of all FortiGate and FortiWifi devices from all FortiGate Cloud instances in a domain group, regardless of region. For example, if you access Inventory from the European region, you see the region of a connected FortiGate Cloud instance from the global region.

Inventory is divided into tabs: *FortiGate Inventory*, *FortiCare Inventory*, *FortiGate Cloud Deployed*, *FortiManager Deployed*, and *FortiManager Cloud Deployed*. You can filter each list by searching for the device serial number (SN) in the SN searchbar.

If you add devices using the FortiDeploy bulk key, the *FortiGate Inventory*, *FortiGate Cloud Deployed*, and *FortiManager Deployed* tabs allow you to filter the device list by the FortiDeploy bulk key, and display a *Bulk Key* column in the device list.

FortiGate Inventory

FortiGate Inventory displays the inventory of all FortiGate and FortiWifi devices imported by FortiCloud key or FortiDeploy bulk key to FortiGate Cloud, including each device's subscription status. The inventory provides a centralized view of all devices imported into the Europe and global services. From here, you can deploy devices to FortiGate Cloud or FortiManager, if configured. You can also delete an imported device from the inventory.

To deploy a device to FortiGate Cloud:

1. On the homepage, go to *Inventory*.
2. Select the desired devices.
3. Click *Deploy to FortiGate Cloud*.
4. From the *Select Display Timezone for Device* dropdown list, select the desired time zone. Click *Next*.
5. For a multitenancy account, you can select the desired subaccount to add the devices to. Select the subaccount, then click *Next*.
6. Click *Apply*. These devices deploy to FortiGate Cloud, and you can now access them on the *FortiGate Cloud Deployed* tab.

To deploy a device to FortiManager:

1. On the homepage, go to *Inventory*.
2. From the *Deploy to FortiManager* dropdown list, select *FortiManager Setup*.
3. Enter the desired FortiManager IP address/FQDN and SN. Click *Submit*.
4. Select the desired devices.
5. Click *Deploy to FortiManager*.
6. Click *Deploy*.

7. Go to *FortiManager Deployed*. The *Status* column displays the deployment process current status. Once the *Status* column displays that the process is complete, these devices deploy to FortiManager, and you can view their SNs on the *FortiManager Deployed* tab. Once deployed to FortiManager, FortiGate Cloud has no control over the device. You cannot manage the device in FortiGate Cloud until you set central management back to FortiGate Cloud.

To delete a device from inventory:

1. On the homepage, go to *Inventory*.
2. Select the desired devices.
3. Click *Delete*.
4. In the confirmation dialog, click *YES*.

FortiCare Inventory

FortiCare Inventory displays the devices that are registered to FortiCare under the account's primary administrator email address with a verified key. Only the primary administrator can view and deploy these devices from the FortiCare Inventory to FortiGate Cloud. To deploy FortiCare devices to FortiGate Cloud, follow the instructions in [To deploy a device to FortiGate Cloud: on page 22](#), from the *FortiCare Inventory* tab. To deploy FortiCare devices to FortiManager, follow the instructions in [To deploy a device to FortiManager: on page 22](#) from the *FortiCare Inventory* tab.

FortiGate Cloud Deployed and FortiManager Deployed

The *FortiGate Cloud Deployed* and *FortiManager Deployed* tabs displays all FortiGate and FortiWifi devices deployed to FortiGate Cloud and FortiManager, respectively. The tabs also display the devices' subscription statuses and the date and time that they were deployed to FortiGate Cloud or FortiManager. Click a device SN to access Analysis, Management, and SandBox functions for that device.

The *FortiGate Inventory* tab provides a centralized view of all devices imported into the Europe and global services. However, after you deploy a FortiGate to FortiGate Cloud, you can only view the FortiGates deployed to the service that you are currently logged in to on the *FortiGate Cloud Deployed* tab. For example, if you are currently logged in to the Europe service, the *FortiGate Cloud Deployed* tab only displays FortiGates deployed to the FortiGate Cloud Europe service.

FortiDeploy

FortiDeploy is a product built into FortiGate Cloud for zero-touch provisioning (ZTP) when devices are deployed locally or remotely. FortiDeploy provides automatic connection of FortiGates for management by FortiGate Cloud or FortiManager.

At time of purchase, you can order a FortiDeploy SKU in addition to your FortiGate Cloud subscription.

When you visit the [FortiGate Cloud portal](#) and enter the FortiDeploy bulk key, you see a list of serial numbers from the order that contained the FortiDeploy SKU. After you confirm that the devices are connected, you can perform basic configuration on the devices remotely, such as sending a FortiManager IP address to all remote FortiGates, so that the FortiManager can manage them remotely.

FortiDeploy support starts the moment you send an email to cs@fortinet.com. You can also contact cs@fortinet.com if you already purchased a FortiGate Cloud subscription and want to purchase FortiDeploy to add to your existing subscription.

FortiDeploy requires a FortiGate model that supports the ZTP (autojoin) feature. FortiGate/FortiWiFi/POE desktop and 1U models up to 100F support the ZTP feature. For other models, FortiDeploy supports one-touch provisioning. For these models, you must configure DHCP on the port of choice. The FortiDeploy server can push FortiManager settings to devices that fulfill this requirement. Having trained personnel handle larger deployments is recommended. FortiDeploy is available for devices running FortiOS 5.2.2 and later.

To enable autojoining FortiGate Cloud:

From FortiOS 5.2.3 and later, the `auto-join-forticloud` option is enabled by default. It must be enabled for FortiDeploy to function correctly. You can ensure that the option is enabled by running the following commands:

```
config system fortiguard
    set auto-join-forticloud enable
end
```

After changing this setting, restart the device and ensure that the device sends traffic to FortiGate Cloud to verify that you configured it correctly.

To set central management to FortiGuard:

If your device is connected to FortiGate Cloud but not cloud-managed, ensure that central management is set to FortiGuard:

```
config system central-management
    set type fortiguard
end
```

Reboot the device, log into FortiGate Cloud, and see if you can manage the device.

To use FortiDeploy with a device deployed behind a NAT device:

The internal or LAN interface default address is the 192.168.1.0/24 subnet. IP address conflicts can occur with departmentalization devices. You can unset each device's default IP address:

```
config system interface
    edit internal
```

```
        unset ip
    end
end
config system interface
    edit lan
        unset ip
    end
end
end
```

You can change the web-based management interface's internal interface IP address in *Network > Interfaces*.

To set a port to DHCP mode:

```
config system interface
    edit "portX"
        set mode dhcp
        set role wan
    next
end
```

FortiCloud and FortiDeploy keys

The following table summarizes the differences between FortiCloud and FortiDeploy key usage:

Account type	Key type	Key reuse policy	Autojoin policy
Regular	FortiCloud	Valid until a new device is deployed	24 hours from first autojoin (grace period) If join request is from the same IP address: 15 minutes after reenabling autojoin.
	FortiDeploy	Valid only once	Always
Multitenancy	FortiCloud	Valid until a new device is deployed	Always
	FortiDeploy	Valid only once	Always

A FortiGate that is imported by FortiCloud or FortiDeploy key which has not been registered in FortiCare is registered upon deployment to either FortiGate Cloud or FortiManager.

You can reenable autojoin for a device in *Network Overview* or *Inventory*.

The image displays two screenshots of the FortiGate Cloud web interface. The top screenshot shows the 'Network Overview' page with a table of devices. One device, FGT61E, is highlighted with a red warning icon and a tooltip that reads: 'The device auto-join had been rejected. Click to re-enable the auto-join.' The bottom screenshot shows the 'Inventory' page with a table of devices. One device, FGT61E, is highlighted with a red warning icon and a tooltip that reads: 'The device auto-join had been rejected. Click to re-enable the auto-join.'

FortiCloud key

A FortiCloud key is printed on a sticker attached to a FortiGate/FortiWifi's top surface. You can use this key for one of the following:

- Directly add a new individual device to a FortiGate Cloud account.
- Import the key to a FortiGate Cloud account inventory.

See [To deploy a FortiGate/FortiWifi to FortiGate Cloud using the FortiCloud key: on page 19](#)

Either action allows the next autojoin request from the device. After the device successfully connects to FortiGate Cloud, its FortiCloud key becomes invalid.

If you load a device by FortiCloud key to a regular account, FortiGate Cloud always allows the device's autojoin request if the source IP address is the same as the last time it autojoined. If the device source IP address differs from the last time it successfully autojoined, you have the option to reenable autojoin for 15 minutes. You must reboot the device within that time to finish the autojoin process. You have a maximum of five attempts to reenable autojoin and reboot the device. After you reach five attempts, you must contact [Customer Service & Support](#) to reset the number of attempts. When the device successfully completes the autojoin process, this resets the number of attempts.

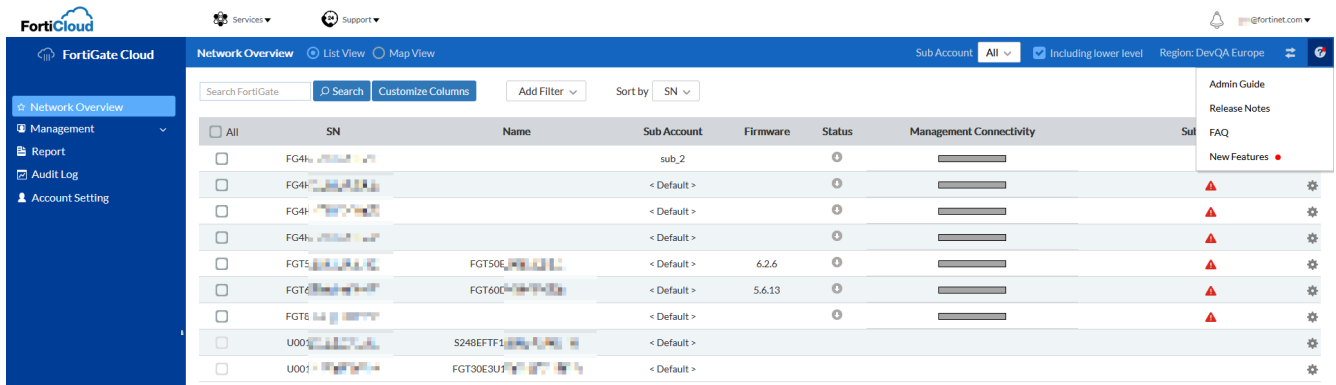
For multitenancy accounts, autojoin is always allowed.

FortiDeploy key

A FortiDeploy key is purchased with a SKU to load one or multiple new FortiGate/FortiWiFi(s) to a FortiGate Cloud account inventory. See [To deploy multiple FortiGate/FortiWifi devices to FortiGate Cloud using a FortiDeploy bulk key: on page 20](#). This load action allows autojoin requests from all devices on the FortiDeploy key. Once you use a FortiDeploy key to load devices to a FortiGate Cloud account, you cannot reuse it to reload the devices. FortiGate Cloud always allows autojoin for a device added by FortiDeploy key.

Network Overview

You see the *Network Overview* page when you first open the FortiGate Cloud interface. From the *Network Overview* page, you can add a FortiGate as [To deploy a FortiGate/FortiWifi to FortiGate Cloud using the FortiCloud key: on page 19](#) describes. A user with an admin role can also go to the [Inventory on page 22](#) pages or the device-specific [Analysis on page 45](#), [Management on page 34](#), [SandBox on page 59](#) pages. A user with a regular role or subaccount admin role (multitenancy) can only go to the [Analysis on page 45](#) and [SandBox on page 59](#) pages. You can view the device CPU and memory usage under the *Status* column.



	SN	Name	Sub Account	Firmware	Status	Management Connectivity	
☐	FG4h...		sub_2				
☐	FG4h...		< Default >				
☐	FG4h...		< Default >				
☐	FG4h...		< Default >				
☐	FGT5...	FGT50C...	< Default >	6.2.6			
☐	FGT6...	FGT60C...	< Default >	5.6.13			
☐	FGT8...		< Default >				
☐	U005...	S248EFTF1...	< Default >				
☐	U001...	FGT30E3U1...	< Default >				

The Network Overview page provides the following information about devices. You can select a device's serial number or name to access analysis tools for that device. Network Overview displays the following device information in both list and map views. To configure which information to be visible in list view, click *Customize Columns*.

- Model/serial number
- Fortinet product type
- Firmware version
- Status (If the device is connected through a management tunnel)
- SD-WAN status
- Last compiled report and last log uploaded
- Subscription expiry date
- DHCP clients
- In/out traffic
- Indicators of compromise
- Configuration status
- Public IP address
- Subaccount
- Last time a configuration backup was created
- For devices that are paired in a high availability configuration, a peer icon appears beside the serial number. You

can click the icon to view the HA information.

The screenshot shows the FortiGate Cloud interface. On the left is a sidebar with 'FortiGate Cloud' and navigation links: Network Overview, Management, Report, Inventory, Account Setting, and Add FortiGate. The main panel is titled 'Network Overview' with tabs for 'List View' and 'Map View'. Below the title bar, there are filters for 'Sub Account' (sub2), 'Including lower level', a search bar, and a 'Search' button. A table lists devices with columns: All, SN, Name, Sub Account, Firmware, Status, SD-WAN, IOC, and Subscription. Three devices are listed: FGT61E4, FGT61E4Q17006243 (PRIMARY), and FGT61E4Q17006508 (SECONDARY). A modal dialog titled 'HA Group: FGT61E4Q17006243 - PRIMARY' is open, showing a table with two rows: FGT61E4Q17006243 (PRIMARY) and FGT61E4Q17006508 (SECONDARY).

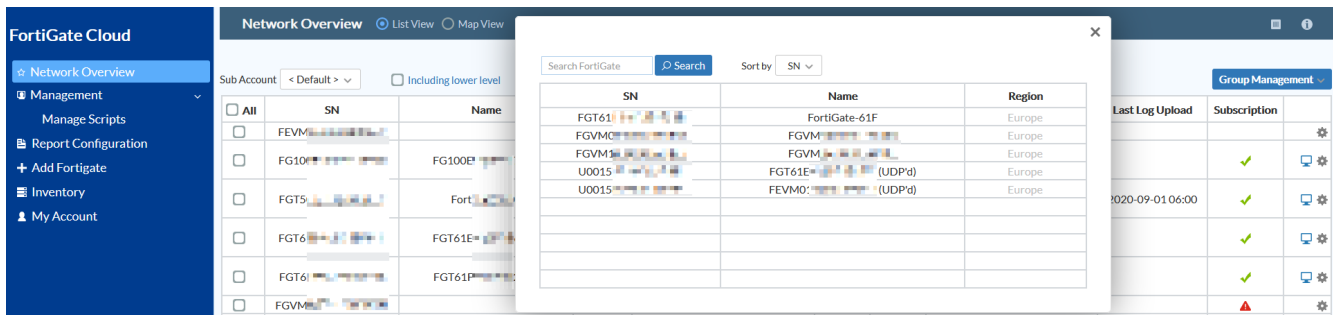
You can download a .csv file of device information by clicking the *Export* button.

You can select *Map View* to view the device list as a map. This allows you to see the geographic location of the deployed devices. You can also place a device at a desired location on the map that does not need to correspond to the device's actual geographic location. You can also view the map in satellite view.

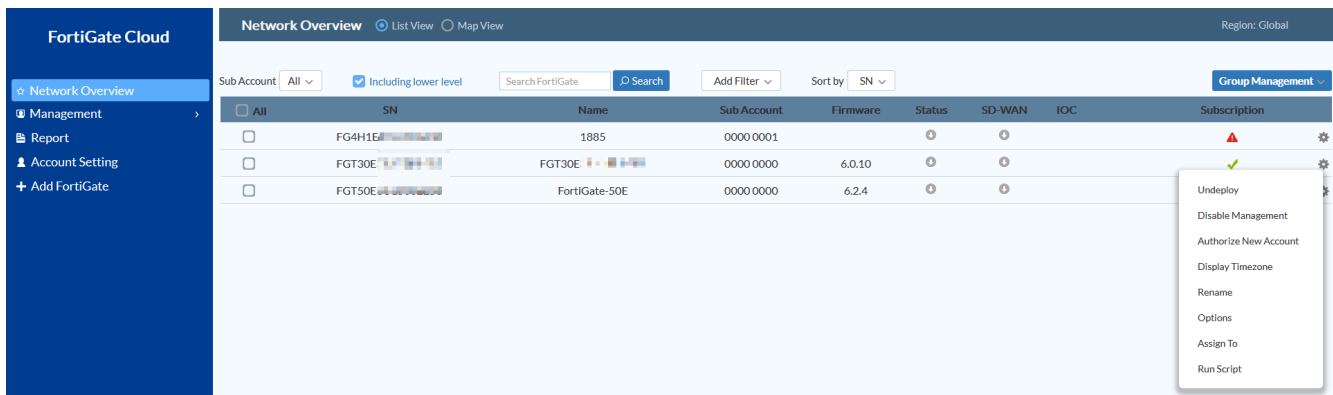
The screenshot shows the FortiGate Cloud interface in 'Map View'. The main panel displays a map of the Pacific Northwest region, including Washington, Oregon, and Idaho. Several red location pins are placed on the map. A sidebar on the left shows the 'FortiGate Cloud' navigation menu. On the right, there is a legend titled 'All Devices' and 'On Map Only' with a table listing devices: SN, Device Name, Model, Version, Tunnel, CPU, Memory, and Last Log Upload. A modal dialog is open over the map, showing details for a device: SN (FEVM1E4Q17006243), Device Name (FEVM1E4Q17006243), Model (Unknown), Version (Unknown), Tunnel (N/A), CPU (N/A), Memory (N/A), and Last Log Upload (N/A). Below the map, there is a 'Show FortiManager Deployed' checkbox and a 'Sandbox' button.

You can toggle on *Show FortiManager Deployed* to view devices deployed to FortiManager. You can then click on a displayed device to access its Sandbox page.

To access devices deployed to another region, click the *Devices in Other Regions* icon in the upper right corner. FortiGate Cloud displays a dialog with a list of devices deployed in other regions.



You can use the gear icon to access additional functions:



To undeploy the FortiGate:

1. Go to *Network Overview*.
2. Click the *Config* icon for the desired device.
3. Click *Undeploy*.
4. In the confirmation dialog, click *YES*.
5. You have the option to place a unit where the FortiGate was deployed. The unit contains historical data and a serial number that starts with U.

An admin user can undeploy a device from one service, then deploy it from another service. For example, an admin user can undeploy a device from the global service, then deploy the same device to the Europe service.

The device may automatically join back to the account due to the autojoin feature. See [FortiCloud and FortiDeploy keys on page 26](#).

To authorize a new account to access the FortiGate's historical data:

You can use this function to transfer historical data to an authorized new account when moving the device to that account.

1. Click the *Config* icon for the desired device.
2. Click *Migrate Existing Data*.
3. In the *Account ID* field, enter the desired account ID.
4. Click *Submit*.

To set the display timezone for the FortiGate:

The display timezone only affects log data view for the FortiGate and does not affect the FortiGate's configured timezone. You can modify the FortiGate's display timezone after it has already been set.

1. Go to *Network Overview*.
2. Click the *Config* icon beside the desired device, then click *Display Timezone*.
3. From the *Display Timezone for Device* dropdown list, select the desired timezone. Click *Submit*. The FortiGate Cloud GUI shows the FortiGate's display timezone in the upper right corner.



To rename the FortiGate:

1. Go to *Network Overview*.
2. Click the *Config* icon for the desired device, then click *Rename*.
3. In the *Device Name* field, enter the desired name. Click *Submit*.

To move a FortiGate from the global service to the Europe service:

You can move a FortiGate from the global service to the Europe service, or vice-versa. The example illustrates moving a FortiGate Cloud from the global service to the Europe service.

1. Log in to the FortiGate Cloud global service.
2. Undeploy the FortiGate:
 - a. Click the *Config* icon for the desired device.
 - b. Click *Undeploy*.
 - c. In the confirmation dialog, click *YES*.
 - d. You have the option to place a unit where the FortiGate was deployed. The unit contains historical data and a serial number that starts with U.

An admin user can undeploy a device from one service, then deploy it from another service. For example, an admin user can undeploy a device from the global service, then deploy the same device to the Europe service.

After a device under a non-multitenancy account is undeployed, the device cannot automatically join back to any account due to the autojoin feature being disabled, even after an admin user deploys the device to another service. You must reactivate FortiGate Cloud on the device GUI using your account email address and password.

3. Go to *Inventory* and confirm that the FortiGate is now listed under inventory.
4. Log in to the FortiGate Cloud Europe service.
5. Go to *Inventory*. Select the desired FortiGate, then click *Deploy to FortiGate Cloud*.
6. Log in to the FortiOS GUI. Reactivate FortiGate Cloud by following [To deploy a FortiGate/FortiWifi to FortiGate Cloud in the FortiOS GUI: on page 20](#).

Group management

When you select multiple devices on the *Network Overview* page, you can perform group management actions. You can apply actions to a group of FortiGate and FortiWifi devices, simplifying administrative tasks. If you only select paid devices, the dropdown list displays all available actions. If your selection includes a free device, only the *Schedule*

Report and *Set Display Time Zone* options are available. Some group management actions require that you enable management on the selected device. See [Management on page 34](#).

Some actions are not unique to group management and this document describes them elsewhere in the context of use on a single device. For descriptions of these functions, see the following topics:

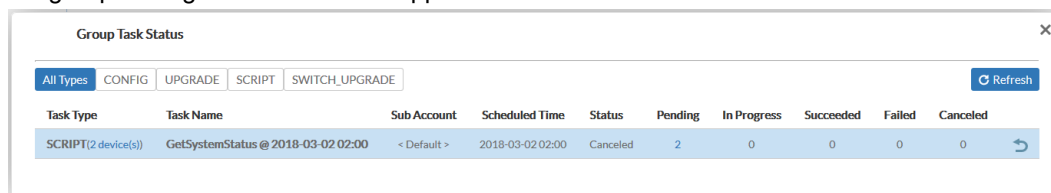
Schedule Report	To schedule a report: on page 54
Deploy Config	To deploy cloud configuration to devices: on page 35
Upgrade Firmware	To upgrade remote device firmware: on page 41
Run Script	To execute a script on a remote device: on page 42
Set Auto Backup	To enable auto backup: on page 40
Manage Report Configs	Reports on page 54
Manage Scripts	Script on page 42

The following describes actions exclusive to group management:

To view group task status:

You can view the current status of group management actions.

1. On the *Management* homepage, click *Group Management > Task Status*. The *Group Task Status* displays the group management actions and their statuses. You can click *# devices* beside the task type to view the devices that the group management action was applied to.



All Types CONFIG UPGRADE SCRIPT SWITCH_UPGRADE Refresh									
Task Type	Task Name	Sub Account	Scheduled Time	Status	Pending	In Progress	Succeeded	Failed	Canceled
SCRIPT(2 device(s))	GetSystemStatus @ 2018-03-02 02:00	< Default >	2018-03-02 02:00	Canceled	2	0	0	0	0

To download a deployment log:

1. On the *Management* homepage, click *Group Management > Task Status*.
2. Click the task for which you want to download a deployment log. You may need to go to the *CONFIG* or *SCRIPT* tab to select the desired task.

3. Click *log*, then *Download*.

The screenshot displays the FortiGate Cloud Management interface. The main panel shows a table of devices with columns for SN, Name, Firmware, CPU, Memory, Status, Active in, and Template. A 'Log' dialog box is open, showing the command 'diagnose fdm log-controller-update' and its output. A 'Group Run Script' dialog box is also visible, showing a list of tasks. The 'Log' dialog box contains the following text:

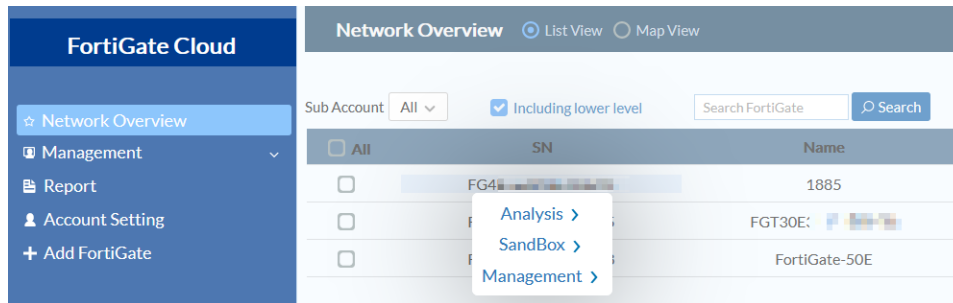
```
diagnose fdm log-controller-update
Protocol=2.0|Response=202|Firmware=FAZ-4K-FW-2.50-100|SerialNumber=FAZ000000000000|Result=Success
diagnose fdm log-controller-update
Protocol=2.0|Response=202|Firmware=FAZ-4K-FW-2.50-100|SerialNumber=FAZ000000000000|Result=Success
```

The 'Group Run Script' dialog box shows a table with columns for Task Type and Task Name. The task type is 'SCRIPT' and the task name is 'diag fdm'. The 'Log' dialog box has a 'Download' button at the bottom right.

Management

On the *Management* tab, you can remotely manage FortiGate and FortiWiFi devices that are connected to the FortiGate Cloud service.

To access the *Management* tab, select the desired device in *Network Overview*, then click *Management*.



When you access the *Management* tab for a new or newly factory reset device with no password configured, you must configure the device admin password to access the *Management* interface.

The template feature is discontinued, except for accounts that have a paid device license and template already in use.

In 23.3, a FortiGate device without a FortiGate Cloud subscription license that is running FortiOS 7.0 or later will have read-only remote access.

To remotely access a device:

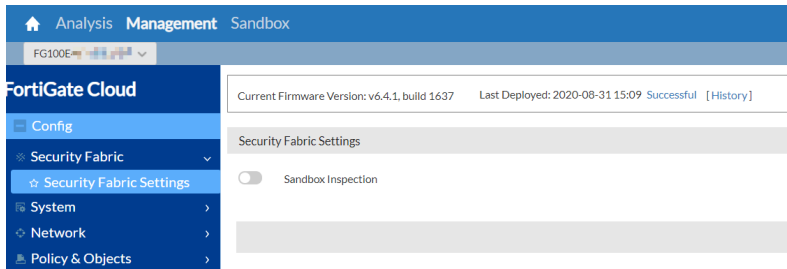
Remote access is only available for a device that has Management enabled and the management tunnel is up.

1. Click the *Remote Access* icon for the desired device.
2. Enter the username and password of a user with super_admin profile.
3. FortiGate Cloud displays a popup where you can provide the FortiGate web GUI port. The popup is prepopulated with the default value of 443 or the last updated port number from the device. If the port value in the popup is correct, click *OK* to remotely access the FortiGate. Otherwise, enter the correct value in the popup to remotely access the FortiGate from FortiGate Cloud.
4. Click *OK*.
5. A login page pops up for the user to enter the local username and password. A user with a prof_admin profile is allowed to remotely access a virtual domain (VDOM)-enabled device only if the user profile has access to the management VDOM.

You must first enable the management tunnel on your device before you can see any management functions. On the device, run the following CLI commands:

```
config system central-management
  set mode backup
  set type fortiguard
end
```

Config



In *Config*, you can access a pared-down version of the remote device's management interface to configure major features as if you were accessing the device itself. For configuration option descriptions, see the [FortiOS documentation](#).

The configuration you see in FortiGate Cloud does not autorefresh. FortiGate Cloud displays a notification if the current local FortiGate configuration differs from the latest configuration uploaded to FortiGate Cloud. You can overwrite the FortiGate Cloud configuration with the current local FortiGate configuration by clicking *Import*, or merge the two configurations by clicking *Merge*. If you merge the configurations and there is a conflict between them (for example, an option is enabled locally on the FortiGate but disabled in FortiGate Cloud), FortiGate Cloud keeps the local FortiGate Cloud configuration for that option. You can then make any changes you want to reflect on the device and click *Deploy* to push the configuration to the device.

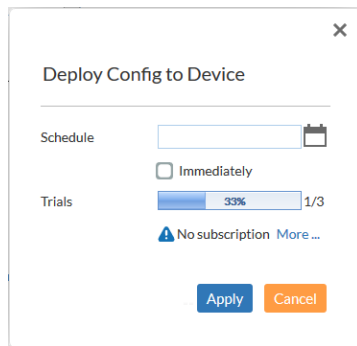
In the case that your device configuration version does not match the firmware version, FortiGate Cloud may display a *Device config version does not match device firmware version* message. You can click the *Import* button to synchronize the configurations.

FortiGate Cloud also supports CLI configuration using FortiExplorer over websocket with FortiOS 6.4.1 and later versions.

FortiGate Cloud supports configuring and deploying SD-WAN for FortiOS 5.6, 6.0, and 6.2, and SD-WAN zones for 6.4, 7.0, and 7.2.

To deploy cloud configuration to devices:

1. Go to *Management > Config*.
2. Before you edit any settings, click the *Import* button to retrieve the most up-to-date configuration from the FortiGate Cloud-connected device.
3. On this page, you have limited access to a pared-down version of the FortiOS interface, allowing you to edit interfaces, routes, policies, and so on. Edit the FortiOS configuration as needed.
4. When you are ready to push your updated configuration back to the device, click the *Deploy* button in the upper right.
5. In the *Schedule* field, select the date and time to deploy the configuration to the device.
6. Select *Immediately* if desired.
7. Click *Apply*. When using the free version of FortiGate Cloud, you are limited to three successful configuration deployments per device. The GUI displays the number of deployments left on the *Deploy* button on the *Config* page and in the *Trials* field in the *Deploy Config to Device* dialog. Once you reach the limit for a device, FortiGate Cloud grays out the *Apply* button in the *Deploy Config to Device* dialog and you cannot deploy the configuration.



8. Wait for the configuration to download to the device. When it completes, a deployment log appears, showing you the changes as they appear in the CLI.

To download a deployment log:

1. Go to *Management > Config*.
2. Do one of the following:
 - a. To download the log for the last successful deployment, beside *Last Deployed: <yyyy-mm-dd hh:mm>*, click *Successful*.
 - b. To download the log for another deployment, beside *Last Deployed: <yyyy-mm-dd hh:mm>*, click *History*. Beside the desired deployment instance, click *log*.
3. Click *Download*.

Managing FortiAP, FortiSwitch, and FortiExtender devices

You can use FortiGate Cloud to manage FortiAP, FortiSwitch, and FortiExtender devices that are connected to a FortiGate deployed to FortiGate Cloud. If these devices are already connected to the FortiGate when the FortiGate connects to FortiGate Cloud, and FortiGate Cloud creates the FortiSwitch and FortiExtender profiles based on their uploaded configurations, while the FortiAP profile is predefined. If these devices are not already connected to FortiGate, you can preauthorize them by adding their serial number and selecting a predefined profile.

Managing FortiAPs

To create a managed FortiAP:

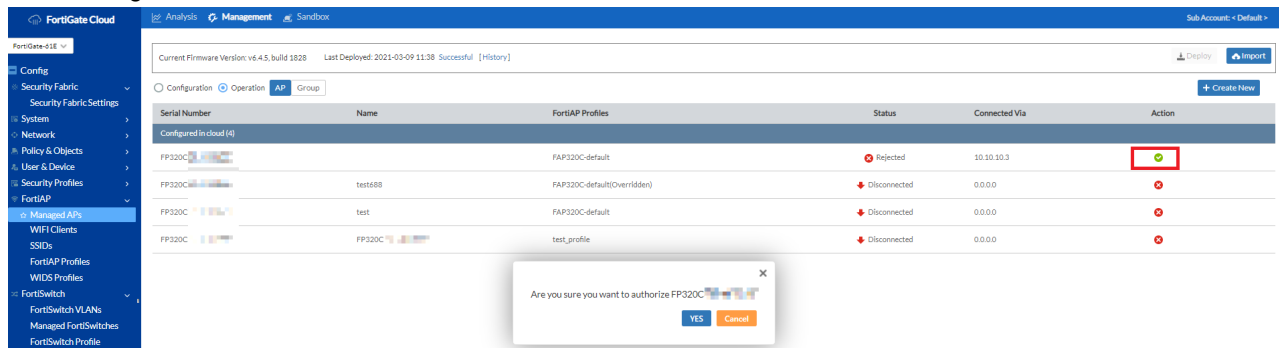
1. (Optional) Create an SSID by going to *Management > Config > FortiAP > SSIDs*. Creating an SSID is only necessary if a radio on the FortiAP profile is configured to use a manual SSID.
2. (Optional) Create a FortiAP profile by going to *Management > Config > FortiAP > FortiAP Profiles*. You can also use the default profile instead of creating a new profile. To configure the SSID that you created, select *Manual* for *SSIDs*, then select the SSID from the dialog.
3. Create the managed FortiAP:
 - a. Go to *Management > Config > FortiAP > Managed APs*.
 - b. Select *Create New > Managed APs*.
 - c. Configure the FortiAP as desired, then click *Save*.
4. The new managed FortiAP displays in *Management > Config > FortiAP > Managed APs*. Deploy the configuration to the FortiGates.

To configure a newly joined FortiAP:

1. Go to *Management > Config > FortiAP > Managed APs*.
2. Select the newly joined FortiAP, then select *Edit*.
3. Edit as desired, then click *Save*.

To authorize a managed FortiAP:

1. Go to *Management > Config > FortiAP > Managed APs*.
2. Select the *Authorize* icon for the desired FortiAP.
3. In the dialog, select *YES*.



Managing FortiSwitches

To create a managed FortiSwitch:

1. Create a FortiSwitch profile by going to *Management > Config > FortiSwitch > FortiSwitch Profile*, then clicking *Create New*.
2. Create the managed FortiSwitch:
 - a. Go to *Management > Config > FortiSwitch > Managed FortiSwitches*.
 - b. Select *Create New*.
 - c. Configure the FortiSwitch as desired, then click *Save*.
3. The new managed FortiSwitch displays in *Management > Config > FortiSwitch > Managed FortiSwitches*. Deploy the configuration to the FortiGates.

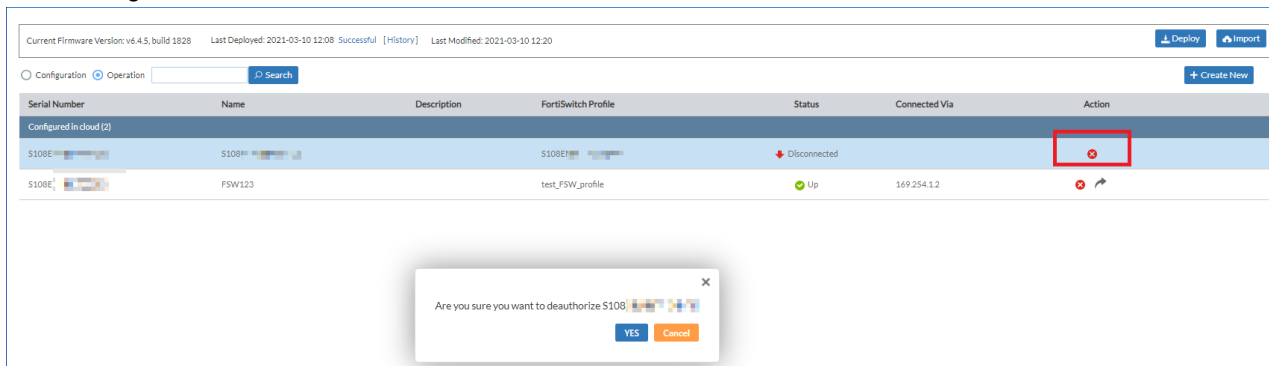
To configure a newly joined FortiSwitch:

1. Go to *Management > Config > FortiSwitch > Managed FortiSwitches*.
2. Select the newly joined FortiSwitch, then select *Edit*.
3. Edit as desired, then click *Save*.

To authorize or deauthorize a managed FortiSwitch:

1. Go to *Management > Config > FortiSwitch > Managed FortiSwitches*.
2. Select the *Authorize* or *Deauthorize* icon for the desired FortiSwitch.

3. In the dialog, select **YES**.



Managing FortiExtenders

To create a managed FortiExtender:

1. Create a FortiExtender interface by going to *Management > Config > Network > Interfaces*, then clicking *Create New > FortiExtender*.
2. Create a FortiExtender profile by going to *Management > Config > FortiExtender > FortiExtender Profiles*, then clicking *Create New*.
3. Create the FortiExtender:
 - a. Go to *Management > Config > FortiExtender*.
 - b. Select *Create New*.
 - c. From the *FortiExtender Profiles* dropdown list, select the profile that you configured in step 2. Configure other fields as desired, then click *Save*.
4. The new managed FortiSwitch displays in *Management > Config > FortiSwitch > Managed FortiSwitches*. Deploy the configuration to the FortiGates.

To configure a newly joined FortiExtender:

1. Create a FortiExtender interface by going to *Management > Config > Network > Interfaces*, then clicking *Create New > FortiExtender*.
2. Create a FortiExtender profile by going to *Management > Config > FortiExtender > FortiExtender Profiles*, then clicking *Create New*.
3. Go to *Management > Config > FortiExtender*.
4. Select the newly joined FortiSwitch, then select *Edit*.
5. From the *FortiExtender Profiles* dropdown list, select the profile that you configured in step 2. Edit other fields as desired, then click *Save*.

To edit a FortiExtender device:

1. Go to *Management > Config > FortiExtender > FortiExtender*.
2. For the desired device, click *Edit*.

3. Edit the fields as desired, then click *Save*.

To authorize or deauthorize a FortiExtender:

1. Go to *Management > Config > FortiExtender > FortiExtender*.
2. Select the *Authorize* or *Deauthorize* icon for the desired FortiExtender.
3. In the dialog, select *YES*.

Backup

In *Backup*, you can back up, *Edit*, *View*, *Compare* (to other revisions), *Download*, *Restore* (to device), and *Delete* revisions. You can filter the revision list by firmware version or created time. You can also search for a specific backup.



You cannot restore backups for FortiGates that are running FortiOS 6.2.3.

To back up the device configuration to the cloud:

1. Go to *Management > Backup*.
2. Select *Backup Config* in the upper right, and enter the backup revision name. FortiGate Cloud adds the new configuration to the list. By selecting the icons on the right side, you can rename, view, compare, download, restore, and delete configuration files. The compare icon only appears once you have multiple revisions available.

To enable auto backup:

1. Go to *Management > Backup > Auto Backup Setting*.
2. Click *Enable Auto Backup*. Only setting changes on the FortiGate (locally from the FortiGate or from FortiGate Cloud) trigger auto backup. You can select one of the following auto back up settings:

Option	Description
Per Session	By default, the session duration is 600 seconds. For example, if you modify FortiGate settings at 10:00 AM, FortiGate Cloud schedules an auto backup in 600 seconds. If no other setting changes occur within the 600 seconds, FortiGate Cloud performs an auto backup at 10:10 AM. However, if you further modify settings, for example, at 10:05 AM, this resets the timer and FortiGate Cloud schedules an auto backup for 600 seconds after 10:05 AM. FortiGate Cloud keeps every backup revision for all sessions in one day.
Daily	Automatically backup the configuration once per day. You can also configure the auto backup to only occur if the configuration has changed.
Weekly	Automatically backup the configuration once per week. You can also configure the auto backup to only occur if the configuration has changed.
Send Email To	Configure an email address to send a notification to when the backup occurs. The email does not contain a copy of the backup revision.

3. Click *Apply*.

Upgrade

FortiGate Cloud

Config Backup Upgrade Script

Current Firmware Version: v6.4.1, build 1637 [History]

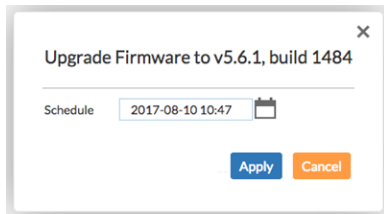
Available Firmware	Release Date
v6.4.2, build 1723	2020-07-30

Only if device's firmware version is below template's version, e.g., device version is 6.0.6, template version is 6.2. And firmware will be upgraded to template's Auto Upgrade version.
 Upgrade path might not be supported. Please read the release notes of the firmware you are upgrading to.
 Upgrading the firmware will cause the system to reboot.

In *Upgrade*, you can see the current firmware version installed on the device, and update to newer stable versions if they are available. The upgrade path that FortiGate Cloud displays may differ from the upgrade path that FortiGuard displays.

To upgrade remote device firmware:

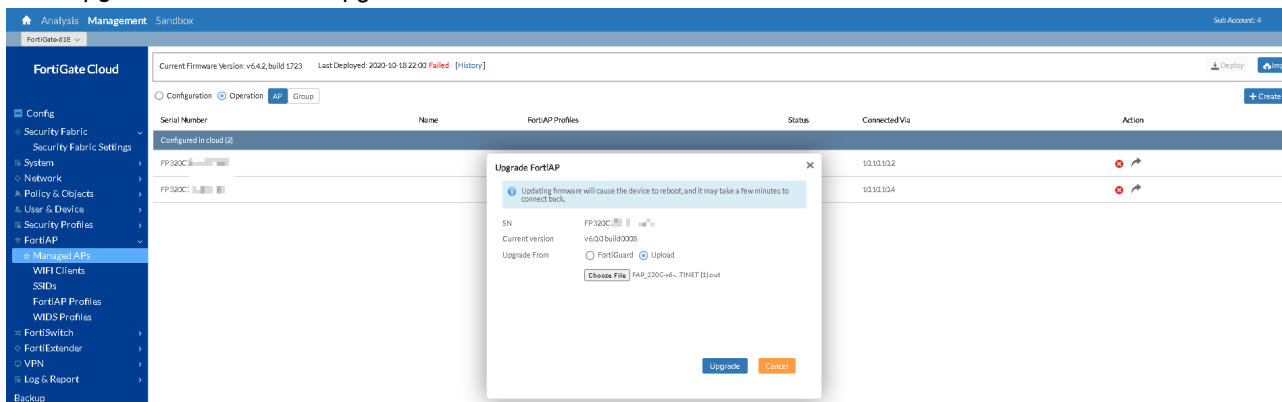
1. Go to *Management > Upgrade*.
2. Verify your device's current firmware version in the upper left before continuing.
3. If you are concerned about the effects of upgrading or have not upgraded recently, use the [Upgrade Path Tool](#) to ensure you follow the recommended upgrade path.
4. Backing up your device configuration before upgrading in *Management > Backup* or in the device's management interface is recommended.
5. Select an available firmware version from the list, and select *Upgrade*. Schedule a time and date to perform the remote upgrade. Scheduling the upgrade during downtime is recommended to minimize disruption. A caution icon may also display to indicate that FortiOS does not support the upgrade path.



6. Wait for the upgrade to take effect.

To upgrade FortiAP, FortiSwitch, or FortiExtender firmware:

1. Go to *Management > Config > FortiAP > Managed APs*, *FortiSwitch > Managed FortiSwitches*, or *FortiExtender > FortiExtender*.
2. For the desired device, click *Upgrade*.
3. In the *Upgrade* dialog, select *Upload*.
4. Click *Choose File*.
5. Browse to and upload the desired firmware file.
6. Click *Upgrade*. The device is upgraded to the selected firmware version.



Script

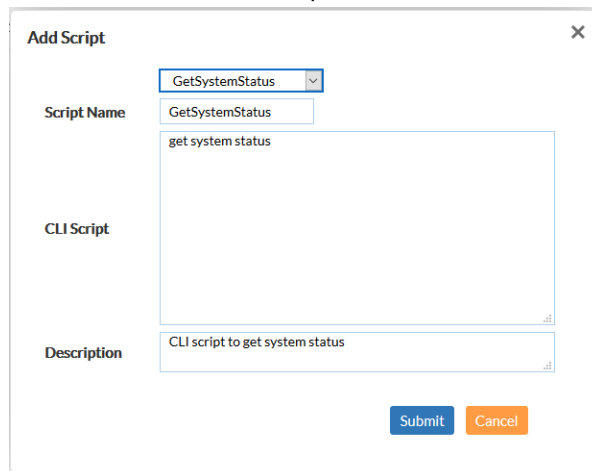
Script Name	Description	Last Modified
1.RadiusServer		2020-07-06 15:48
2.LDAPServer		2020-07-06 15:48
3.User		2020-07-06 15:48
4.UserGroup		2020-07-06 15:48
5.SSID		2020-07-06 15:49
6.SecurityProfil		2020-07-06 15:49
7.VPN		2020-07-06 15:49
8.SSID60X		2020-07-06 16:11
GetSystemStatus	CLI script to get system status	2020-08-31 13:29

In *Script*, you can create and run script files on connected remote devices to check device status or get bulk configuration information quickly.

To execute a script on a remote device:

1. Go to *Management > Script*.
2. (Optional) To create a new script, do the following:
 - a. In the upper right, select *Add Script*.
 - b. Enter a name and a description, and the CLI script content that you want to run. Each script is a series of CLI

commands, one command per line. Click *Submit*.

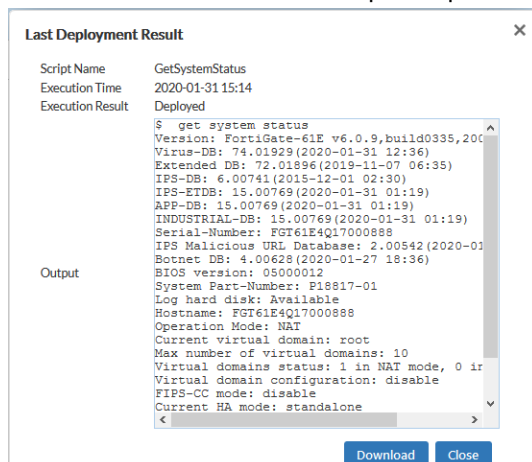


The **Add Script** dialog box contains the following fields:

- Script Name:** A dropdown menu showing "GetSystemStatus" and a text input field containing "GetSystemStatus".
- CLI Script:** A large text area containing the command "get system status".
- Description:** A text input field containing "CLI script to get system status".

At the bottom right are **Submit** and **Cancel** buttons.

- For the desired script, click the *Deploy* icon, and select a time to automatically deploy the script to the device.
- To cancel the scheduled run, click the *Cancel* icon next to the scheduled time.
- FortiGate Cloud records that script's output. You can read it by clicking *View Result*.



The **Last Deployment Result** dialog box displays the following information:

- Script Name:** GetSystemStatus
- Execution Time:** 2020-01-31 15:14
- Execution Result:** Deployed

The **Output** section shows a scrollable list of system status details:

```
$ get system status
Version: FortiGate-61E v6.0.9,build0335,200
Virus-DB: 74.01929(2020-01-31 12:36)
Extended DB: 72.01896(2019-11-07 06:35)
IPS-DB: 6.00741(2015-12-01 02:30)
IPS-ETDB: 15.00769(2020-01-31 01:19)
APP-DB: 15.00769(2020-01-31 01:19)
INDUSTRIAL-DB: 15.00769(2020-01-31 01:19)
Serial-Number: FGT61E4Q17000888
IPS Malicious URL Database: 2.00542(2020-01-31 01:19)
Botnet DB: 4.00628(2020-01-27 18:36)
BIOS version: 05000012
System Part-Number: F18817-01
Log hard disk: Available
Hostname: FGT61E4Q17000888
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: standalone
```

At the bottom are **Download** and **Close** buttons.

To download a deployment log:

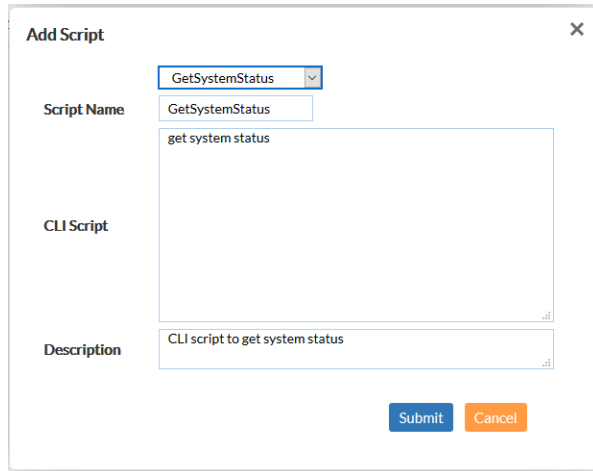
- Go to *Management > Script*.
- Do one of the following:
 - To download the log for a script's last successful deployment, click *View Result* for the desired script.
 - To download the log for another deployment, click *History*. Beside the desired deployment instance, click *Log*.
- Click *Download*.

Manage Scripts

In *Manage Scripts*, you can create script files to check device status or get bulk configuration information quickly.

To add a script:

1. Go to *Management > Script*.
2. In the upper right, select *Add Script*.
3. Enter a name and a description, and the CLI script content that you want to run. Each script is a series of CLI commands, one command per line. Click *Submit*.

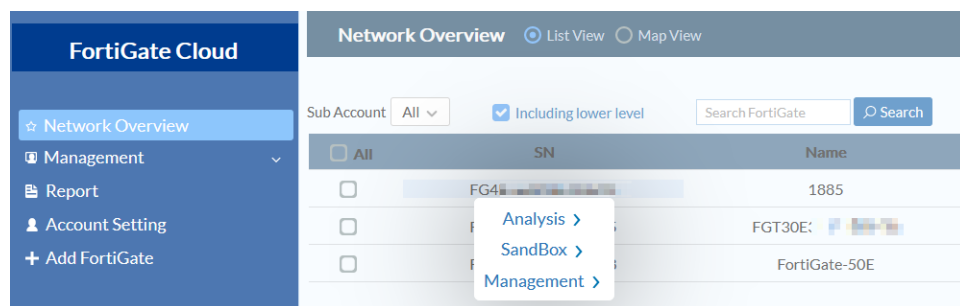


The image shows a modal dialog box titled "Add Script" with a close button (X) in the top right corner. The dialog contains four labeled input fields: "Script Name" (a dropdown menu showing "GetSystemStatus"), "CLI Script" (a large text area containing "get system status"), and "Description" (a text field containing "CLI script to get system status"). At the bottom right of the dialog are two buttons: "Submit" (blue) and "Cancel" (orange).

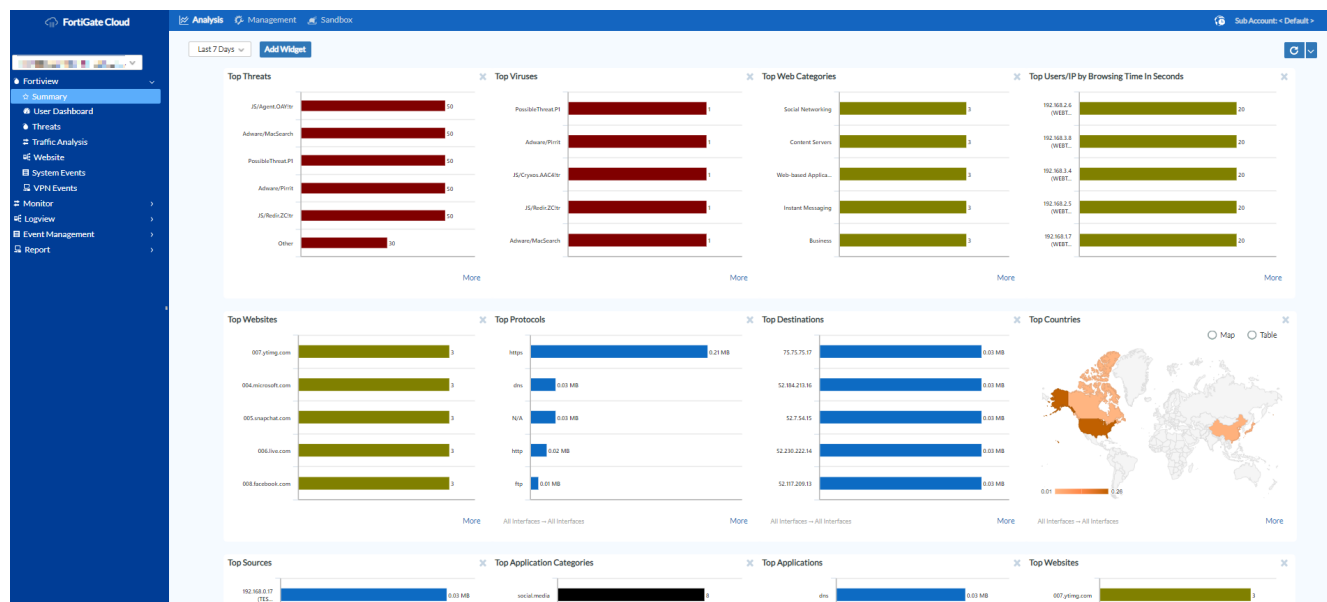
Analysis

The *Analysis* tab provide tools for monitoring and logging your device's traffic, providing you centralized oversight of traffic and security events.

To access the *Analysis* tab, select the desired device in *Network Overview*, then click *Analysis*.



FortiView



The default FortiView page is the summary view, which uses widgets to show a general overview of what is happening with your device. You can add new widgets by selecting *Add Widget*.

Each widget is a customizable box, showing certain information about the device. You can do the following with widgets:

- Click a widget title and drag it to move it around.
- Delete a widget by selecting the X icon.
- Set the widget refresh rate by selecting the dropdown list beside the refresh icon.

The following lists all widget types, grouped according to function:

Threats

Widget	Description	Feature required to be enabled on device
Top Threats	Displays which threats trigger the most detection events on the network.	At least one of the following: IPS, AV, AntiSpam, DLP, or Anomaly Detection.
Top Spam	Displays which sources send the most spam email into the network.	AntiSpam
Top Viruses	Counts the viruses that the device's AV most frequently finds.	AV
Top Applications by Threat Score	Compares which applications have the most traffic compared to their threat score, based on the device's Application Control settings.	Application Control
Top Attacks	Counts the attacks that the device's IPS most frequently prevents.	IPS
Top DLP By Rules	Counts the DLP events that the device detects, sorted by DLP rule.	DLP

Traffic Analysis

Widget	Description	Feature required to be enabled on device
Top Applications	Compares which applications are most frequently used, based on the device's Application Control settings.	Application Control
Top Application Categories	Compares which application categories are most frequently used, based on the device's Application Control settings.	Application Control
Top Sources	Displays which sources have the most traffic from or to the device.	
Top Destinations	Displays which destinations have the most traffic from or to the device.	
Top Protocols	Compares the traffic volume that has passed through a certain interface, based on which protocol it uses (HTTP, HTTPS, DNS, TCP, UDP, other).	

Widget	Description	Feature required to be enabled on device
Top Countries	Displays which countries have the most traffic from or to the device.	
Traffic History	Displays volume of incoming and outgoing traffic over time.	
Bandwidth	Displays utilization per interface in bps.	

Websites

Widget	Description	Feature required to be enabled on device
Top Websites	Compares which websites are most frequently visited. You can click a category to see which websites in that category are being visited.	Web Filtering
Top Web Categories	Compares which web filtering categories are most frequently used, based on the device's Web Filtering settings.	Web Filtering
Top Users/IP by Browsing Time in Seconds	Compares which users visit which IP addresses most frequently in the greatest ratio. You can click a user to see which IP addresses they visit.	Web Filtering

DNS

Widget	Description	Feature required to be enabled on device
Top Queried Domain	Compares which domains are most frequently queried.	
Queried Botnet C-and-C Domains	Displays which botnet C-and-C domains were queried.	
High Risk Domains	Displays which high risk domains were visited.	
Top Domain Lookup Failures	Displays domains with highest number of lookup failures.	

FortiView offers log information, reformatted into easily navigable charts, in a style similar to FortiView in FortiOS.

You can select a time period to view data for:

- Last 60 minutes
- Last 24 hours
- Last 7 days

You can set the chart's refresh rate by clicking the *Refresh* icon. By using the *Add Filter* dropdown list, you can filter the chart by various factors. Individual chart entries may also allow you to filter by that entry's data by selecting a filter icon on the right, or drill down to see all related log data, such as all log data through that interface.

FortiView charts reference

The following provides descriptions of all FortiView charts.

User Dashboard

The User Dashboard displays the number of users/entities that fit into the following security categories:

- Visited high risk websites
- Infected by malware
- Targeted by malware
- Targeted by spam
- Violated data leak rules
- Used high-risk applications
- Targeted by attacks
- Attacked by protocol intrusion

You can click each category to view the list of users/entities affected. You can drill down further to view the list of incidents for each user/entity and the logs for each incident.

FSBP Dashboard

The FSBP Dashboard displays security rating results for the device in the following categories:

- Overall Score
- Maturity Milestones
- Top Achievement
- Top Todo
- History Trend

The FSBP Dashboard is only available for devices that support the Security Rating feature.

Threats

Chart	Description
Top Threats	Lists the top threats to your network. FortiGate Cloud considers the following incidents threats: • Risk applications detected by application control

Chart	Description
	• Intrusion incidents detected by IPS • Malicious web sites detected by web filtering • Malware/botnets detected by antivirus (AV)
IPS	Lists intrusion incidents detected by IPS.
AntiVirus	Lists the malware/botnets detected by AV.
AntiSpam	Lists the spam detected by AntiSpam.
DLP & Archives	Lists the DLP and archives incidents.
Anomaly	Lists network anomalies.

Traffic Analysis

Chart	Description
Application	Displays the top applications used on the network including the application name, category, bandwidth (sent/received), sessions, and risk level.
Cloud Application	Displays the top cloud applications used on the network.
Source	Displays the highest network traffic by source IP address and name, bandwidth (sent/received), sessions, and risk level.
User	Displays the highest network traffic by user in terms of bandwidth sent/received, sessions, and risk level.
Destination	Displays the highest network traffic by destination IP addresses, the applications used to access the destination, bandwidth sent/received, sessions, and risk level.
Interface	Displays the highest network traffic by interface in terms of bandwidth sent/received, traffic sessions, and risk level. You can view by source or destination interface.
Country	Displays the highest network traffic by country in terms of bandwidth sent/received, traffic sessions, and risk level. You can view by source or destination country.
Policy Hits	Lists the policy hits by policy, device name, VDOM, number of hits, bytes, and last used time and date.

Website

Chart	Description
Website	Displays the top allowed and blocked website domains on the network. You can also view by source. You can filter by threat level.
Web Category	Displays the top website categories. You can filter by threat level.

Chart	Description
Browsing User/IP	Displays the top web-browsing users and their IP addresses by total browsing time duration. You can also view by category or domain. You can filter by threat level.

System Events

Chart	Description
System Activity	Displays events on the managed devices, their severity, and number of incidents. You can filter by user or severity level.
Admin Session	Displays the users who logged into managed devices, the number of configuration changes they performed, number of admin sessions, and their total duration of logged-in time. You can also view by login interface. You can filter by severity level.
Failed Login	Displays the users who failed to log into managed devices. You can also view by login interface. You can filter by severity level.
Wireless	Displays wireless events. You can filter by severity level.

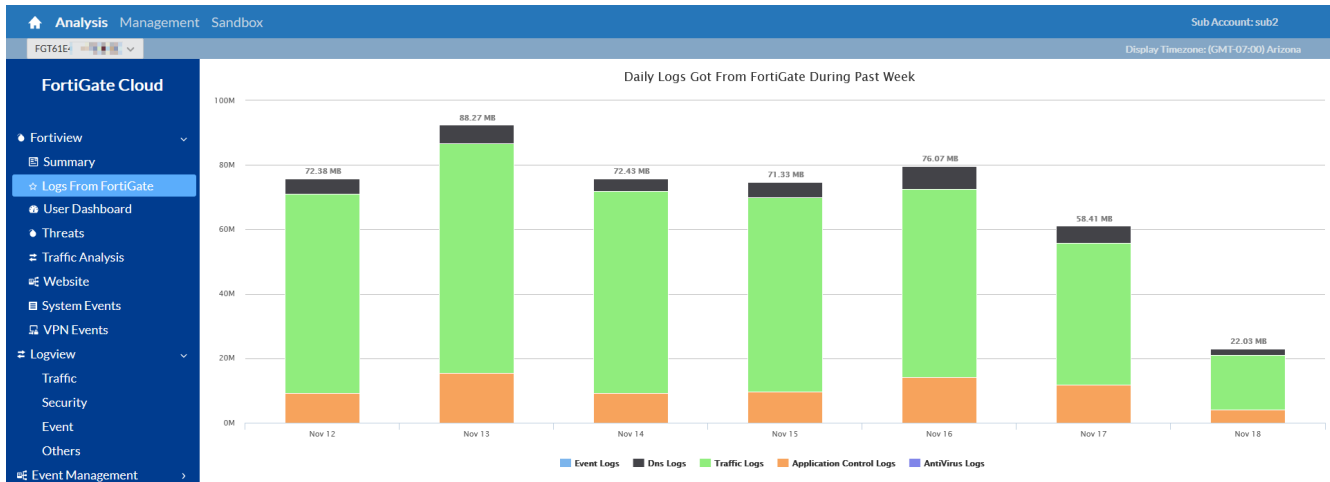
VPN Events

Chart	Description
Site to Site	Displays the names of VPN tunnels with IPsec that are accessing the network.
SSL and Dialup	Displays the users who are accessing the network by using an SSL or IPsec VPN tunnel.
Failed VPN Login	Displays the users who failed to log in successfully via VPN.

Monitor

Logs from FortiGate

The Logs from FortiGate chart displays the daily amount of logs that FortiGate Cloud has received from the FortiGate for the past seven days. For each day of data, the chart also displays the type of logs that FortiGate Cloud has received, such as traffic, antivirus, and so on.



Logview

Event Logs Last 30 Days

#	Time	User	Level	User Interface	Action	Message
1	08-26 17:53:05	admin	Information	https(172.16.93.68)	login	Administrator admin logged in successfully from https(172.16.93.68)
2	08-26 16:58:58		Information	N/A	N/A	DHCP statistics
3	08-26 16:58:58		Information	N/A	N/A	DHCP statistics
4	08-26 16:58:58		Information	N/A	N/A	DHCP statistics
5	08-26 16:43:20	Fortimanager_Access	Warning	fgfmd	download	System config file has been downloaded by user Fortimanager_Access via fgfmd
6	08-26 16:43:20	Fortimanager_Access	Warning	fgfmd	download	System config file has been downloaded by user Fortimanager_Access via fgfmd
7	08-26 16:43:00	Fortimanager_Access	Warning	fgfmd	download	System config file has been downloaded by user Fortimanager_Access via fgfmd
8	08-26 16:42:53	Fortimanager_Access	Information	fgfm_tunnel	Delete	Delete application.list block-high-risk
9	08-26 16:42:53	Fortimanager_Access	Information	fgfm_tunnel	Delete	Delete webfilter.profile monitor-all
10	08-26 16:42:51	Fortimanager_Access	Warning	fgfmd	download	System config file has been downloaded by user Fortimanager_Access via fgfmd
11	08-26 16:42:45	Fortimanager_Access	Information	fgfm_tunnel	Edit	Edit system.settings
12	08-26 16:42:43	Fortimanager_Access	Warning	fgfmd	download	System config file has been downloaded by user Fortimanager_Access via fgfmd
13	08-26 16:42:36	Fortimanager_Access	Warning	fgfmd	download	System config file has been downloaded by user Fortimanager_Access via fgfmd
14	08-26 16:42:34	Fortimanager_Access	Warning	fgfmd	download	System config file has been downloaded by user Fortimanager_Access via fgfmd
15	08-26 16:42:28	Fortimanager_Access	Warning	fgfmd	download	System config file has been downloaded by user Fortimanager_Access via fgfmd
16	08-26 16:40:18	Fortimanager_Access	Warning	fgfmd	download	System config file has been downloaded by user Fortimanager_Access via fgfmd
17	08-26 16:39:54	Fortimanager_Access	Warning	fgfmd	download	System config file has been downloaded by user Fortimanager_Access via fgfmd
18	08-26 16:39:50	admin	Information	GUI(172.16.93.68)	Edit	Edit system.settings
19	08-26 16:39:09		Notice	N/A	N/A	N/A
20	08-26 16:32:28	Fortimanager_Access	Warning	fgfmd	download	System config file has been downloaded by user Fortimanager_Access via fgfmd

Logview offers more detailed log information, access to individual log data, and downloadable log files. You can select a log category to view from the list on the left.

You can select a time period to view data for. You can view log data older than seven days only for devices that have a FortiGate Cloud subscription. For devices with a free subscription, FortiGate Cloud grays out any dates beyond a seven-day period:

- Last 60 minutes
- Last 24 hours
- Last 7 days
- Last 30 days
- Specified time period

The *Time* column displays the raw log time, which may not correspond to the display time zone that you configured for FortiGate Cloud. To convert the raw log time to the FortiGate Cloud display time zone, add or subtract the time offset provided in the *Time* column. In the example, log 1 was recorded at 03:10:56. The *(-0700)* in the *Time* column shows the time difference between the raw log time and Greenwich mean time (GMT). Since in the example, the display time zone is the same as GMT, you can conclude that log 1 was recorded at 10:10:56 (03:10:56 + 07:00:00) in the display time zone.

You can set the chart's refresh rate by selecting the *Change Refresh Period* icon. By using the *Add Filter* dropdown list, you can filter the log list by various factors. Selecting *Column Setting* allows you to customize the default log view. By selecting *Log Files*, you can see the raw log data files and manually download them. The box in the lower right allows you to move through pages of log data by clicking the arrows or entering a page number.

To download logs:

1. In *Analysis > Logview*, go to the desired log in the left navigation pane.
2. Click *Log Files* in the upper right corner.
3. Select the checkboxes for the desired logs. You can download up to five log files at once.
4. Click the *Download* button. A .gz archive file containing the logs that you selected in step 3 is downloaded.

You can download various raw log types from FortiGate Cloud. The log filename format is <log type>_MultiLogs_<download timestamp>.gz

For example, for a traffic log, the filename would be tlog_MultiLogs_1592503586.gz.

The log filename format uses a shortened identifier for each log type:

Log type	Identifier
Anomaly	mlog
AntiSpam	slog
AntiVirus	vlog
Application Control	rlog
Attack	alog
CIFS	ilog
Content	clog
DLP	dlog
DNS	olog
Event (including all subtypes)	elog
File filter	fflog
GTP	glog
Netscan	nscan
SSH/SSL	hlog
Traffic	tlog

Log type	Identifier
VOIP	plog
Web Application Firewall (WAF)	flog
Web Filter	wlog

For example, consider an Application Control log that is generated for the period between October 23, 2021 and November 2, 2021 for a FortiGate with the serial number "FGT123". The first log in the file has a timestamp of 6:09 PM, while the last log in the file has a timestamp of 9:32 AM. The log file name is as follows:

FGT123_rlog_20211023-1809-20211101-0932.log.gz

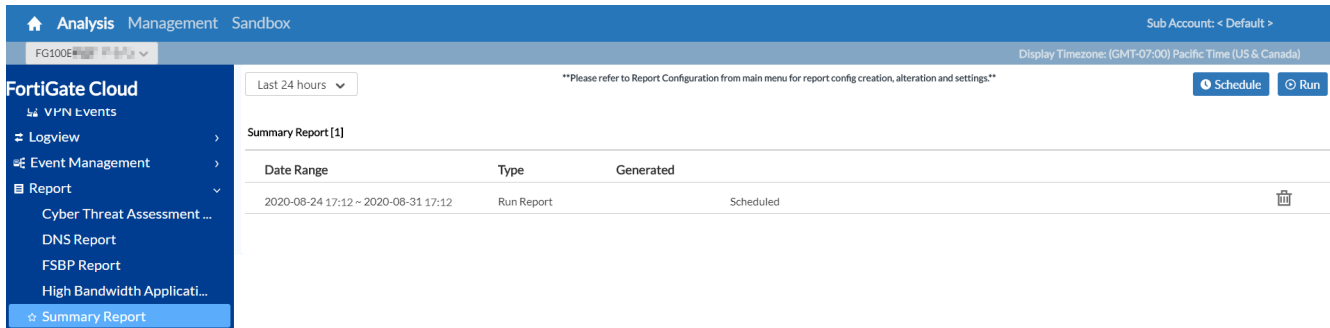
Event Management

In *Event Management*, you can set up email alerts for specific network structure emergencies, such as the device's power supply failing. The page defaults to *All Events* in the left menu, which lists all past emergency events. Select *Event Handlers* to configure the alert settings.

You can enable events to track by selecting their checkboxes. If you want to receive an alert email when they occur, select the checkbox under *Send Alert Email* and enter the email address to send the alert email to. To send the alert email to multiple email addresses, you can enter multiple email addresses in the *Send Alert Email* fields, separating each email address with a comma.

Select the gear icon to configure each *Event Handler* directly and set the logged severity level.

Reports



Reports generates custom reports of specific traffic data, and can email them to specified addresses. Select a report to see a list of collected reports of that type. By default, there is a preconfigured *Summary Report* and a *Web Activity Report*.

To schedule a report:

1. Go to *Analysis > Reports*.
2. Click the desired report from the left pane.
3. Click *Schedule* to determine the range of time for which to generate reports: *Daily*, *Weekly* or *Monthly*, and which email to send the reports to. For example, if you want to generate a report for a month of data, you can select *Monthly* and FortiGate Cloud runs and sends the report once a month.
4. Under *Aggregation Devices*, add devices to schedule the report for. You can use this option to generate a report with aggregated data from multiple devices, which is useful for providing a network status overview. FortiGate Cloud supports report aggregation for the following:
 - FortiGates in a high availability cluster
 - Virtual domains on the same FortiGate

Reports reference

The following provides descriptions of preconfigured reports:

Report	Description
DNS	The default version of this report displays the following charts: • Queried Botnet C&C domains and IP addresses • High risk sources • Top queried domains • Top domain lookup block • Top domain lookup timeout
FSBP	The default version of this report displays results based on the device's security rating result: • Fortinet Security aFbric components audited • Score history (industry average and industry range) • Maturity milestones

Report	Description
	Achievements and to-do list The FSBP Dashboard is only available for devices that support the Security Rating feature. If the device does not have any Security Rating results, all charts show no data.
High Bandwidth Application Usage	Shows you applications that may affect network performance by using high bandwidth, allowing you to quickly pinpoint high bandwidth usage and violation of corporate policies. This report focuses on peer-to-peer applications (such as BitTorrent, Xunlei, Gnutella, Filetopia), file sharing and storage applications (such as Onebox, Google Drive, Dropbox, Apple Cloud), and voice/video applications (such as YouTube, Skype, Spotify, Vimeo, Netflix). You cannot edit this report.
Summary	The default version of this report displays the following sections: - Threat Analysis - Traffic Analysis - Web Activities - VPN Analysis - System Activity
Web Activity	The default version of this report displays the following charts: - Most Visited Web Categories - Most Visited Websites - Most Visited Web Categories and Web Sites - Most Active Web Users - Most Visited Web Sites by Most Active Users - Most Active Users of Most Visited Web Sites
360 Degree Activities	Displays the following sections: - Application Visibility - Web Traffic Analysis - User Behavior Analysis You cannot edit this report.
Cyber Threat Assessment	Enhanced version of the Summary Report. Displays the following sections: - User Productivity - Application Usage - Web Usage - Security and Threat Prevention - Application Vulnerability Exploits - Virus Prevention - At-Risk Devices and Hosts - High Risk Application - Network Utilization - Bandwidth

Report	Description
	You cannot edit this report.
What is New Weekly Report	This report displays new emerging devices, applications, vulnerabilities, and viruses during the past week. You can only schedule FortiGate Cloud to run this report weekly. Displays the following sections: • New Device • New Applications • New Vulnerability • New Virus All sections display all findings from the past week. You cannot edit this report.
Admin and System Events Report	This report displays admin login information and system event information. Displays the following sections: • Admin Login • Login Summary • Login Summary By Date • List of Failed Logins • System Events • Events by Severity • Critical Severity Events • High Severity Events • Medium Severity Events You cannot edit this report.
VPN Report	This report displays VPN-related information. Displays the following sections: • Summary • VPN Traffic Usage Trend • VPN User Logins • Failed Login Attempts • Top Dialup VPN Users • SSL VPN • Top Sources of SSL VPN Tunnels by Bandwidth • Top SSL VPN Tunnel Users by Bandwidth • Top SSL VPN Web Mode Users by Duration • Top SSL VPN Users by Duration • IPsec VPN • Top Site-to-Site IPsec Tunnels by Bandwidth • Top Dialup IPsec Tunnels by Bandwidth • Top Dialup IPsec Users by Bandwidth • Top Dialup IPsec Users by Duration You cannot edit this report.

Report configurations

You can create and alter report configurations and their settings from *Report*. You can *Add* new reports or *Edit* existing ones. Both open an editing interface, which allows you to edit the report content and add or remove sections.

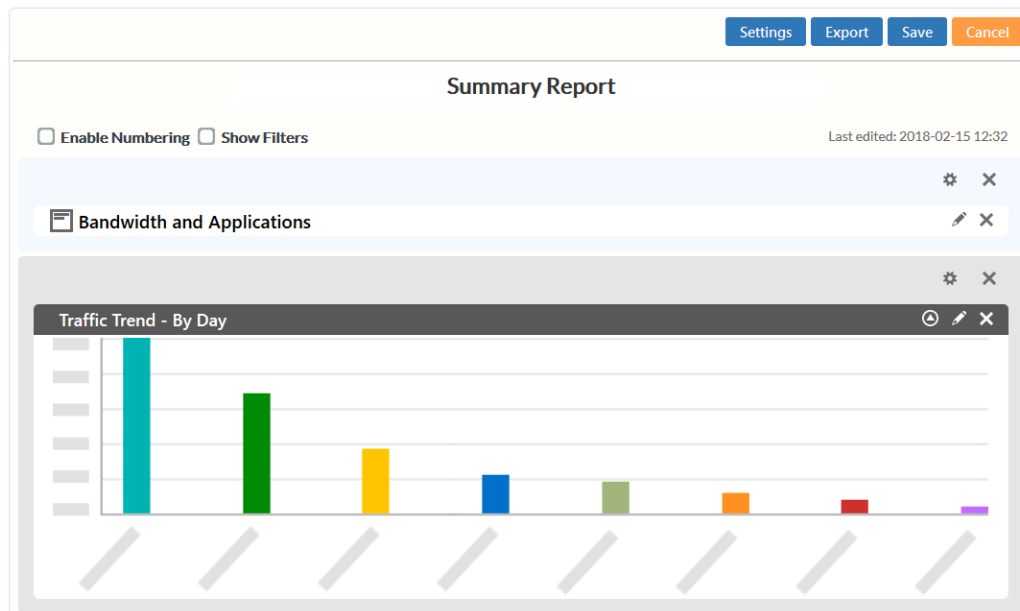
This feature is available for devices with FortiGate Cloud Service subscriptions.

When a report configuration is scheduled for more than 15 devices, you can click ... in the *Scheduled Devices* column to open a window where you can view all scheduled devices.

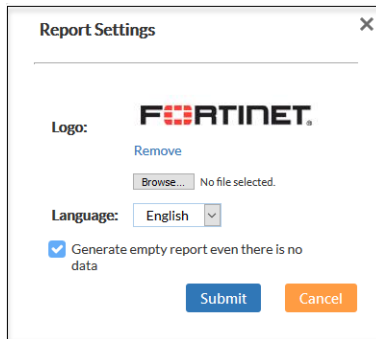
Network Overview Management Report Inventory Account Setting Add FortiGate	Report Config	Sub Account	Total Scheduled	Scheduled Devices			Last Modified		
	Total (16)								
	300 Degree Activities Report	ALL	19	FGT61E	FGT61E	FGT61E		2020-10-21 17:35	
				FGT61E	FGT61E	FGT61E			
				FGT61E	FGT61E	FGT61E			
				FGT61E	FGT61E	FGT61E			
				FGT61E	FGT61E	FGT61E			
	Cyber Threat Assessment Report	ALL	1	FGT61E				2020-10-07 15:55	
	DNS Report	ALL	1	FGT61E				2020-10-07 15:55	
	FSBP Report	ALL	1	FGT61E				2020-10-07 15:55	
High Bandwidth Application Usage Report	ALL	1	FGT61E				2020-10-07 15:55		
Summary Report	ALL	33	FG100E	FG30H	IRE-GL (FG30H)	FG600E	FG600E (FG600E)	2020-10-26 09:45	
			FGT61E	FGT61E	FGT61E	FGT61E	FGT61E		
			FGT61E	FGT61E	FGT61E	FGT61E	FGT61E		
			FGT61E	FGT61E	FGT61E	FGT61E	FGT61E		
			FGT61E	FGT61E	FGT61E	FGT61E	FGT61E		

To create a custom report:

1. Go to *Report*.
2. Click *Create Report Config* in the upper right, and choose to create a blank report, default Summary or Web Activity Report, copy an existing report, or import an external template. Click *Submit*.
3. To add a chart, click the gear icon and select *Add Chart*.
4. In the *Predefined Chart List* dialog, select the desired chart. You can further customize the chart by clicking *Customize*. Click *Save*.
5. Click the gear icon to add *Descriptions*, and *Titles* to the current section, or new 1- or 2-column sections.



6. Click *Settings*. You can upload a report logo and set the report language.



The image shows a 'Report Settings' dialog box with a close button (X) in the top right corner. Inside the dialog, there is a 'Logo:' section with the Fortinet logo and a 'Remove' link below it. Below the logo section is a 'Browse...' button and the text 'No file selected.' Underneath that is a 'Language:' section with a dropdown menu currently set to 'English'. At the bottom left, there is a checked checkbox labeled 'Generate empty report even there is no data'. At the bottom right, there are two buttons: 'Submit' (blue) and 'Cancel' (orange).

7. Click *Save*.
8. Select *Run*, and view the finished report.

To configure report settings:

1. Go to *Report*.
2. Click *Settings* for the desired report. You can upload a report logo and set the report language. *Click Submit*.

To delete a report config:

1. Go to *Report*.
2. Click *Delete* for the desired report. Deleting the report configuration deletes all associated reports from FortiGate Cloud. Click *YES* in the confirmation dialog to continue with the deletion.

SandBox

FortiSandbox SaaS is a service that uploads and analyzes files that FortiGate antivirus (AV) marks as suspicious.

In a proxy-based AV profile on a FortiGate, the administrator selects *Inspect Suspicious Files with FortiGuard Analytics* to enable a FortiGate to upload suspicious files to FortiGuard for analysis. Once uploaded, the file is executed and the resulting behavior analyzed for risk. If the file exhibits risky behavior or is found to contain a virus, a new virus signature is created and added to the FortiGuard AV signature database. The next time the FortiGate updates its AV database it has the new signature. The turnaround time on Cloud SandBoxing and AV submission ranges from ten minutes for automated SandBox detection to ten hours if FortiGuard Labs is involved.

FortiGuard Labs considers a file suspicious if it exhibits some unusual behavior, yet does not contain a known virus. The behaviors that FortiGate Cloud Analytics considers suspicious change depending on the current threat climate and other factors.

The FortiGate Cloud console enables administrators to view the status of any suspicious files uploaded: pending, clean, malware, or unknown. The console also provides data on time, user, and location of the infected file for forensic analysis. SandBoxing is available in both free and paid FortiGate Cloud subscriptions.

The *SandBox* tab collects information that the FortiSandbox SaaS service compiles. FortiSandbox SaaS submits files to FortiGuard for threat analysis. You can configure your use of the service and view analyzed files' results.

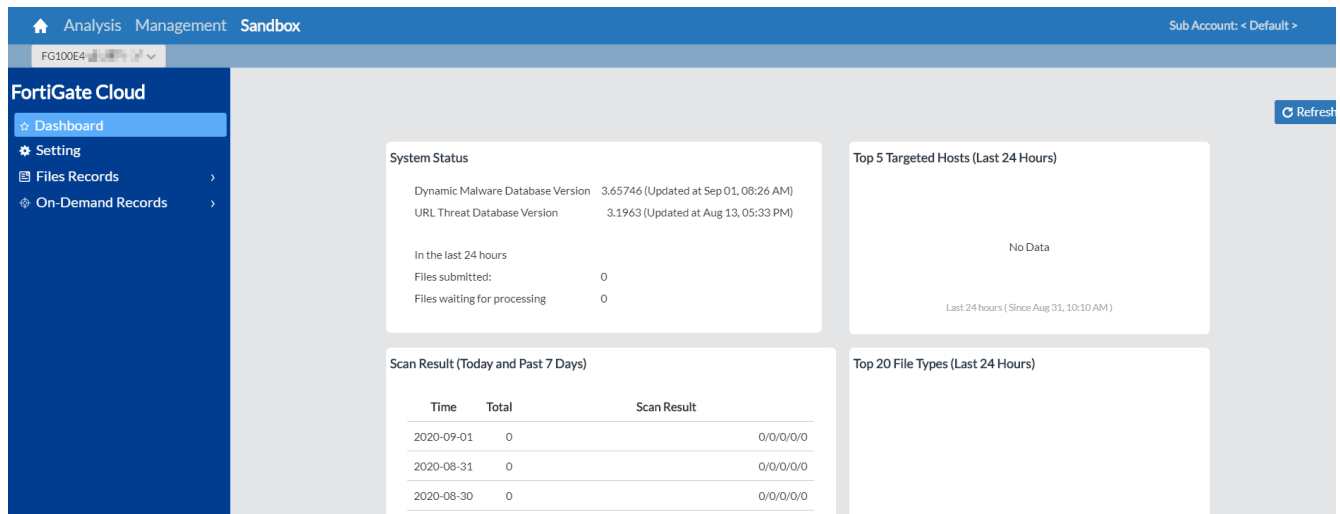
You must enable Cloud SandBoxing on the FortiGate and submit a suspicious file for the *SandBox* tab to become visible.

FortiSandbox SaaS regions include Global, Europe, U.S., and Japan.

To set up Sandbox:

1. Complete the [FortiSandbox SaaS](#) steps.
2. In *Security Profiles > AntiVirus*, create a profile that has *Send files to FortiSandbox Cloud for inspection* configured.
3. Create a firewall policy with logging enabled that uses the Sandbox-enabled AV profile.
4. Once devices have uploaded some files to FortiSandbox SaaS, log in to the [FortiGate Cloud portal](#) to see the results.

Dashboard

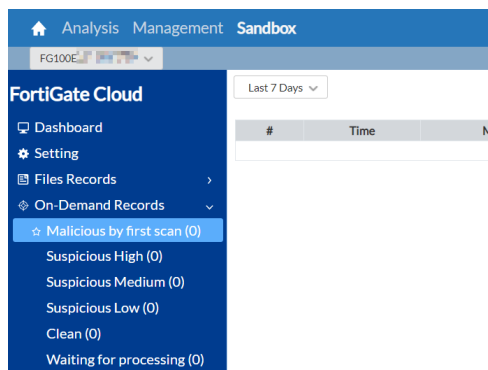


You can see an overview of the Sandbox results on the *Dashboard*.

The Dashboard contains the following widgets:

Widget	Description
System Status	Quick view of the current state of the AV databases and load.
Top 5 Targeted Hosts (Last 24 Hours)	Displays which hosts received the most threats during the last 24 hours.
Scan Result (Today and Past 7 Days)	Shows the last eight days of results and their risk levels. You can toggle the display of clean files in the chart by selecting the checkmark in the lower right of the widget.
Top 20 File Types (Last 24 Hours)	Displays the most commonly analyzed file types in the last 24 hours of scanning.

Files and On-Demand Records

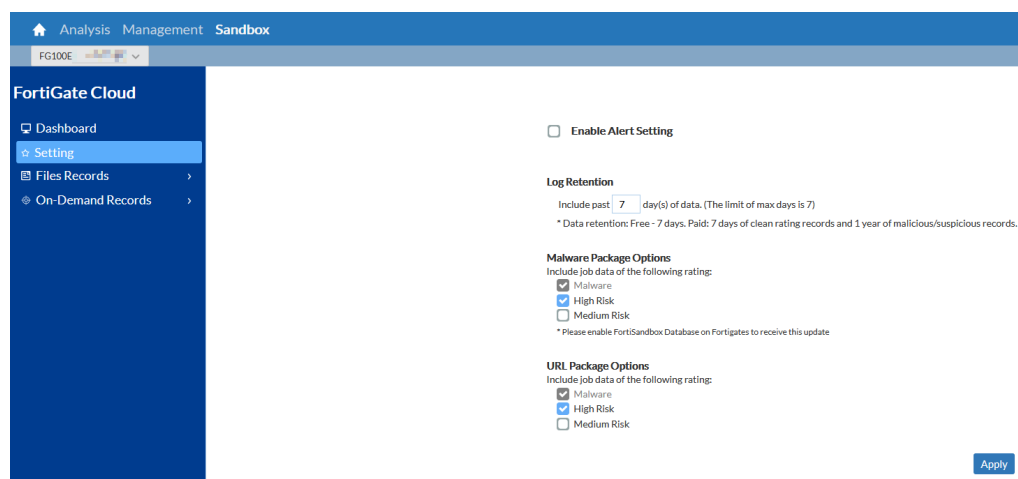


Files Records displays files that your connected device's AV has flagged as suspicious, which have been uploaded to FortiGate Cloud for FortiGuard analysis. In *On-Demand*, you can manually upload files for FortiGuard analysis, and view the analysis results. These pages may not appear if you do not have the FortiSandbox SaaS service enabled on the connected device.

You can select an analysis level and click the file names for more information. *On-Demand* also has an *Export* option, which allows you to export a CSV or PDF of on-demand results, and *Upload File*, where you can manually upload a file for analysis.

The maximum file size is 10 MB. The processing time may vary based on the file size.

Setting



In *Setting*, you can configure FortiSandbox SaaS settings:

Setting	Description
Enable Alert Setting	• Enable alert emails • Enter multiple emails (one per line) to receive alerts • Set which severity level triggers sending alert emails
Log Retention	Set number of days to retain log data.
Malware Package Options	Select the risk level of data that is automatically submitted to FortiGuard to further antithreat research.
URL Package Options	

To configure Sandbox alert emails:

1. Go to *SandBox > Setting*.
2. Select *Enable Alert Setting*.
3. Enter emails into the list to contact in the event of a Sandbox alert.
4. Select the severity levels to trigger an alert.

Accounts and users

FortiGate Cloud supports the unified FortiCloud account for login to access the portal. The user who created the account, which this guide refers to as the primary user, can log in to FortiGate Cloud using their email ID as the username and the password that they chose when creating the account.

Creating an account

See [Creating a FortiCloud account](#).

User management

The primary user can add users to the account using the following methods:

User type	Method
Identity and Access Management (IAM) user	Add users to the FortiCloud account with role-based access control in FortiGate Cloud using the FortiCloud IAM service . See IAM users on page 62 .
FortiGate Cloud user	Add FortiGate Cloud-only users. See FortiGate Cloud users on page 64 .

FortiGate Cloud does not support subusers added via the FortiCare legacy user management system. IAM users are the recommended approach.

IAM users

FortiCloud Identity & Access Management (IAM) supports creating IAM users and allowing access to FortiGate Cloud using the admin or read-only access role. The following summarizes the functions available for each access role:

Function	Admin	Read-only
Network Overview	Yes	Yes
Import and provision devices	Yes	
Configuration management	Yes	
View logs and reports	Yes	Yes
Generate reports	Yes	
View audit logs	Yes	

See [Adding IAM users](#) for details on configuring IAM users.

FortiCloud organizations

FortiGate Cloud supports organizational unit (OU) account selection and switching. OU support is currently in beta and available to external customers with FortiCloud Premium license accounts. See [Organization Portal](#) for details on creating an OU.

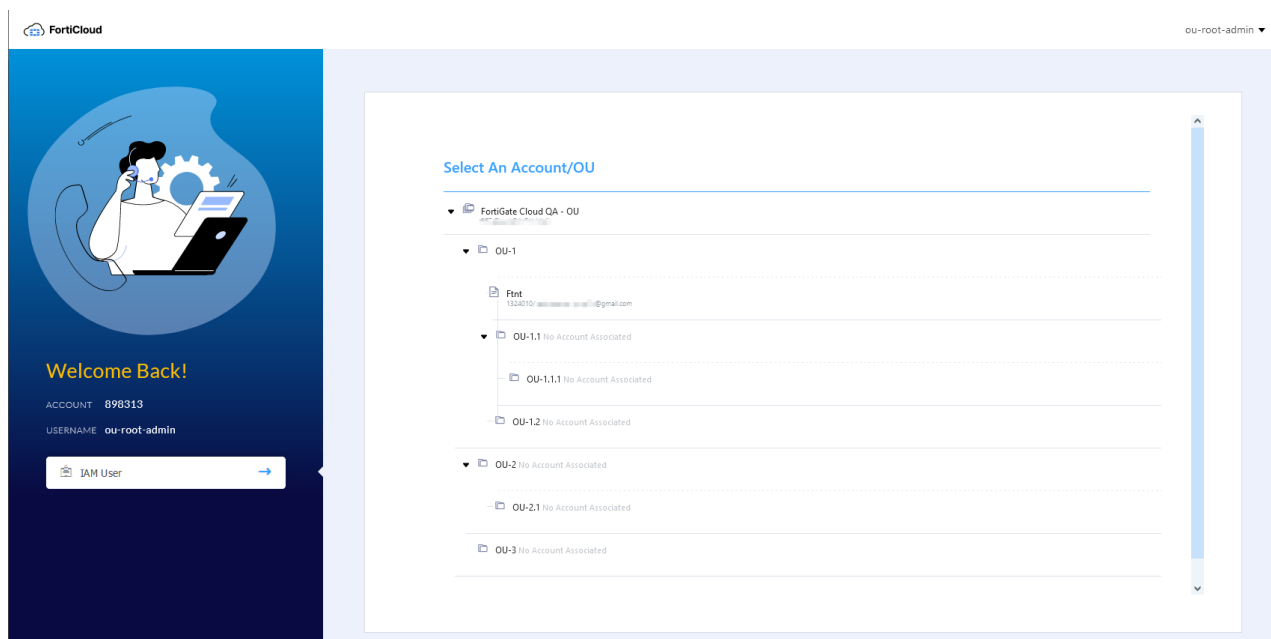
Creating an IAM user with OU scope

See [User permissions](#).

Logging in to FortiGate Cloud and accessing OU accounts

To log in to FortiGate Cloud and access OU accounts:

1. In the FortiGate 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/OU.

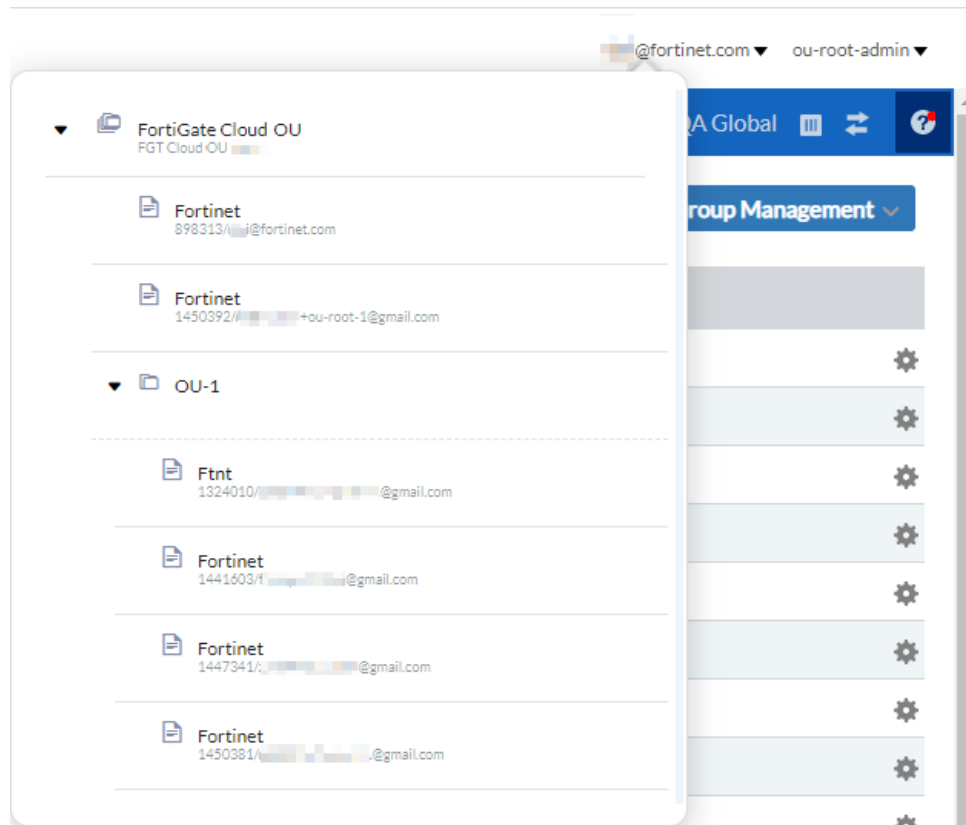


Returning to the OU tree

To return to the OU tree, select your username in the upper right corner of the GUI, then select *Switch Accounts*.

Switching OUs or accounts

To switch the OU or account that you are using to access FortiGate Cloud, select your account in the upper right corner of the GUI, then select the desired OU or account from the dropdown list.



FortiGate Cloud users

Primary users can create FortiGate Cloud users with admin and regular (read-only) permission roles with access to different functionalities.

For information on multitenancy-enabled accounts and adding subaccounts and users to subaccounts, see [Multitenancy on page 70](#).

To add more FortiGate Cloud users:

1. Go to *Account Setting*.
2. Click the *Add User* button.
3. Enter the new admin/user's email address and name.
4. From the *Region* dropdown list, select the desired region for this user to have access to.
5. From the *Role* dropdown list, select whether they are an admin (total control over the FortiGate Cloud interface) or a regular user (limited control, monitoring only).

6. For *Manage Sub Account*, select *All*, or select *Selected* to decide which subaccounts the admin/user has access to.

The screenshot shows the FortiGate Cloud interface. On the left is a dark blue sidebar with the 'FortiGate Cloud' logo and a menu containing 'Network Overview', 'Management', 'Report', 'Account Setting' (highlighted), and 'Add FortiGate'. The main content area is titled 'Account Setting' and 'My Account > Add User'. It contains a form with the following fields: 'Email' and 'Re-type Email' (password fields with a strength indicator), 'User Name' (text field with 'Eric'), 'Region' (dropdown menu with 'Global' selected), and 'Role' (dropdown menu with 'Admin' selected). Below these is the 'Manage Sub Account' section with radio buttons for 'All' and 'Selected' (which is selected). Under 'Selected', there are two checkboxes: the first is checked and labeled '0000 0000', the second is unchecked and labeled '0000 0001'. At the bottom right are 'Submit' and 'Cancel' buttons.

7. Select *Submit*. The admin/user receives an email prompting them to set their account password and log in.

Signing in as a FortiGate Cloud user

To sign in as a FortiGate Cloud user:

1. Go to the [FortiGate Cloud portal](#).
2. In the *Email* and *Password* fields, enter the account email address and password.
3. Click *Login*.

Replacing a FortiGate Cloud user account ID with a new email address

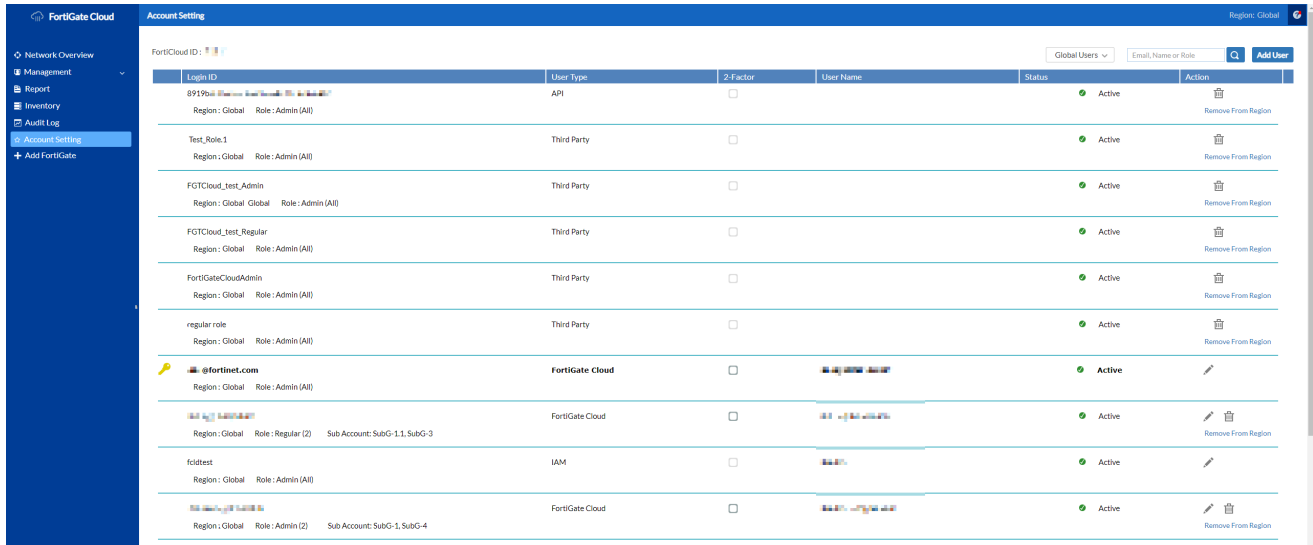
To replace a FortiGate Cloud user account ID with a new email address:

1. Log in to FortiGate Cloud using the FortiGate Cloud account that you want to replace. In the upper right of the FortiGate Cloud interface, click *Account Setting*. In the list of users, ensure that the new email address is not already in use.
2. Add a new admin user, using the desired new email address. Follow the instructions in [To add more FortiGate Cloud users: on page 64](#) to add the new admin user.
3. Select *Set as primary*.
4. Log out of FortiGate Cloud.
5. Log in to FortiGate Cloud as the admin user added in step 2.
6. Click the *Account Setting* icon.
7. In the list of users, click the *Delete* icon beside the old account to remove it from FortiGate Cloud.

After replacing the account ID, you must reactivate the FortiGate Cloud account on each device under the account.

Account Setting

You can add and manage users from *Account Setting*. *Account Setting* includes different user types, including IAM and FortiGate Cloud account users. *Account Setting* displays a key icon beside the primary account.



Login ID	User Type	2-Factor	User Name	Status	Action
89190a... Region: Global Role: Admin (All)	API	☐		Active	
Test_Role.1 Region: Global Role: Admin (All)	Third Party	☐		Active	
FGTCloud_test_Admin Region: Global Global Role: Admin (All)	Third Party	☐		Active	
FGTCloud_test_Regular Region: Global Role: Admin (All)	Third Party	☐		Active	
FortiGateCloudAdmin Region: Global Role: Admin (All)	Third Party	☐		Active	
regular role Region: Global Role: Admin (All)	Third Party	☐		Active	
@fortinet.com Region: Global Role: Admin (All)	FortiGate Cloud	☐		Active	
 Region: Global Role: Regular (2) Sub-Account: SubG-1.1, SubG-3	FortiGate Cloud	☐		Active	
fcldtest Region: Global Role: Admin (All)	IAM	☐		Active	
 Region: Global Role: Admin (2) Sub-Account: SubG-1, SubG-4	FortiGate Cloud	☐		Active	

The *Account Setting* page contains the following columns:

Column	Description
Login ID	Email address that the user uses to log in to the FortiGate Cloud portal. This column also displays the region that each user can access and their role. If multitenancy is activated, this column also displays the subaccounts that the user can access.
User Type	Displays the type of user. User types include the following: IAM: see IAM users on page 62. FortiGate Cloud: see FortiGate Cloud users on page 64. API: an API user only has the ability to call the FortiGate Cloud API. FortiCare manages API users and their access permissions. API users are subusers of the primary account. See API access on page 74. Third Party: user who authenticates using an external identity provider (IdP). Configuring an external IdP requires FortiCare and FortiAuthenticator support.
2-Factor	Enable two-factor authentication for the user. Two-factor authentication is only available for FortiGate Cloud and IAM users. Enabling two-factor authentication by selecting the checkbox in this column is only available for FortiGate Cloud users. For IAM users, you can enable two-factor authentication by selecting <i>Security Credentials</i> from the top-right dropdown list.
User Name	Name of the user associated with the user account. You may want to edit a username to make it easier to identify who is using that account. You can edit the username by clicking the <i>Edit</i> icon in the <i>Action</i> column.

Column	Description
Status	Status of the user account. The status can be one of the following: • Active: user who has activated their account. • Pending: user to whom an activation email has been sent, but has not activated their account yet.
Action	Edit or delete the user, or remove them from their current region. Available options depend on the role of the user account that you are currently logged in to FortiGate Cloud with.

Audit Log

The Audit Log displays a log of actions that users performed on the FortiGate Cloud portal. You can filter the page to only view logs for actions for a certain date range, module, or action type. The log displays information for the following modules:

Module	Actions
Account	• Adding, deleting, and editing subaccounts, account users, and subaccount users • Moving devices to subaccounts • Setting an account as the primary account
Report	• Adding, deleting, editing, downloading, scheduling, and running reports • Adding, deleting, and editing report configurations
Log	Downloading and exporting logs
FortiView	Exporting charts
Event Handler	Enabling and disabling event handlers
Summary widget	Adding and deleting summary widgets
Management	Enabling, disabling, and authenticating management on devices
Script	Adding, editing, and deploying scripts
Remote Access	Viewing a device via Remote Access
Config	Importing and merging device configurations
Backup	Downloading, running, restoring, and deleting backups
Device deployment	Undeploying, deleting, adding, bulk adding, and deploying devices to FortiGate Cloud or FortiManager
Sandbox	Uploading files to Sandbox for analysis

The following information is available for each action. You can configure which columns display:

- Time when the action occurred
- User who completed the action
- Module that the action falls under
- Action type
- Subject that the action was performed on
- Other details as available

FortiGate Cloud

Audit Log

Region: Global

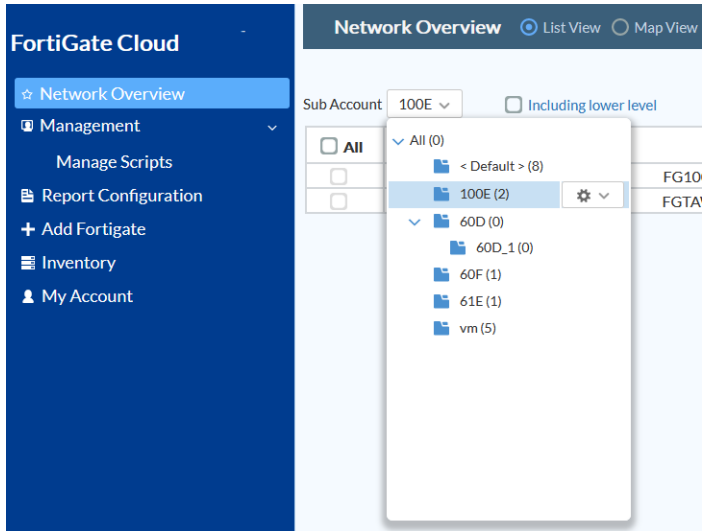
Network Overview
Management
Report
Inventory
Audit Log
Account Setting
Add FortiGate

Select date...
Module
Action

	Time	User	Module	Action	Subject	Message
☐	5:47	@fortinet.com	Backup	Run	FWF60E7	
☒	1:06	@fortinet.com	Config	Deploy	FWF60E7	
☒	0:47	@fortinet.com	Config	Edit	FWF60E7	{ "object operation":"new", ...
☒	0:47	@fortinet.com	Config	Edit	FWF60E7	{ "object operation":"new", ...
☒	0:47	@fortinet.com	Config	Edit	FWF60E7	{ "object operation":"new", ...
☒	7:27	@fortinet.com	Template	Upgrade	template_61F_FOS62_BAKUP_BAKUP	
☒	6:03	@fortinet.com	Template	Delete	Template_11111111111111111111111111111111	
☒	0:40	@fortinet.com	Backup	Download	FWF60E7	
	2021-03-04 11:52:52	@fortinet.com	Management	Enable	FORTIGATE_SET - [FGT30E	

Multitenancy

The multitenancy account is designed for managed security service providers. A multitenancy account is a one- or five-year service for an administrator to create and manage multiple subaccounts. It also allows you to move devices between these accounts. You can allocate administrators to each subaccount with full or read-only access, allowing more control over a managed service's provisioning.



To activate multitenancy:

1. Contact your Fortinet partner or reseller, requesting the following SKU: FCLE-10-FCLD0-161-02-DD. They email you a multitenancy activation code.
2. In FortiGate Cloud, select *Account Setting*.
3. Under the admin/user list, select *Activate multi-tenancy feature*.
4. Enter the activation code, and click *Submit*.

To configure basic multitenancy:

1. On the *Inventory* page, select *Import FortiCloud Key* or *Import Bulk Key* to add multiple FortiGate Cloud licenses at once.



After the device successfully deploys, the device key becomes invalid. You can only use the key once to deploy a device.

2. On the *FortiGate Inventory* subpage, select one or multiple devices, and select *Deploy to FortiGate Cloud*. Select the subaccount for the selected devices. You can also select a timezone for the devices.
3. Click *Deploy*. FortiGate Cloud moves the devices to the *FortiGate Cloud Deployed* subpage.

To assign a device to a subaccount on the homepage:



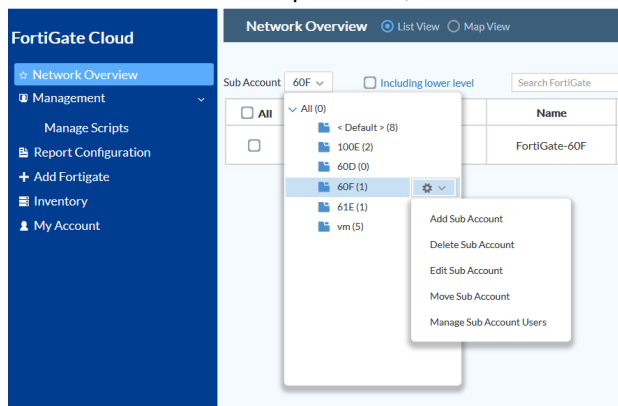
Assigning a device to a new subaccount keeps the device data in FortiGate Cloud, including logs, reports, and configuration backup, and moves this data to the new subaccount. To delete this data, you must undeploy your device from FortiGate Cloud, then assign it to the desired subaccount.

You can assign a device to a different subaccount, including RMA devices.

1. On the *Network Overview* page, click the *Config* icon beside the desired device, then click *Assign To*.
2. In the *Assign To* dialog, select the desired subaccount, then click *Submit*.
3. In the confirmation dialog, click *YES*.

To manage subaccounts:

1. The *Network Overview* page lists subaccounts in a dropdown list. To manage a subaccount, click the desired subaccount. From the dropdown list, select the desired management action.

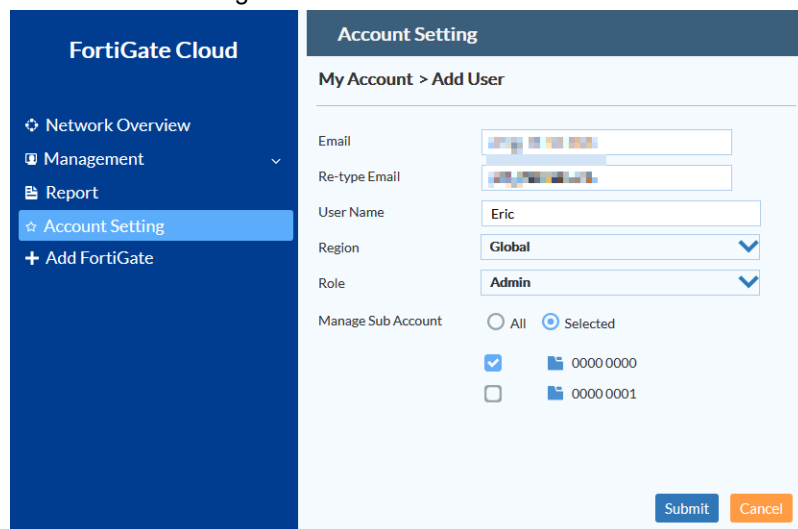


2. Go to *Account Setting*. You can view all accounts associated with this FortiGate Cloud. Use the dropdown list to view *Global*, *SubAccount*, or *All Users*. You can see that users have different roles. For role descriptions, see [User roles on page 72](#).

Login ID	User Type	2-Factor	User Name	Status	Action
89190a1b-8b8e-4b8e-8b8e-8b8e8b8e8b8e Region: Global Role: Admin (All)	API	☐		Active	Remove From Region
Test_Role1 Region: Global Role: Admin (All)	Third Party	☐		Active	Remove From Region
FTGCloud_test_Admin Region: Global Global Role: Admin (All)	Third Party	☐		Active	Remove From Region
FTGCloud_test_Regular Region: Global Global Role: Admin (All)	Third Party	☐		Active	Remove From Region
FortiGateCloudAdmin Region: Global Role: Admin (All)	Third Party	☐		Active	Remove From Region
regular role Region: Global Role: Admin (All)	Third Party	☐		Active	Remove From Region
@fortinet.com Region: Global Role: Admin (All)	FortiGate Cloud	☐		Active	Remove From Region
 Region: Global Role: Regular (2) Sub Account: SubG-1, SubG-3	FortiGate Cloud	☐		Active	Remove From Region
fcidtest Region: Global Role: Admin (All)	IAM	☐		Active	
 Region: Global Role: Admin (2) Sub Account: SubG-1, SubG-4	FortiGate Cloud	☐		Active	Remove From Region

3. Click the *Edit* icon for the desired account.

4. In the *Account Setting > Edit User* dialog, for *Manage Sub Account*, select *Selected*. Select the desired subaccounts for this user to manage.



The screenshot shows the FortiGate Cloud interface. On the left is a dark blue sidebar with the 'FortiGate Cloud' logo and a menu containing 'Network Overview', 'Management', 'Report', 'Account Setting' (highlighted), and 'Add FortiGate'. The main area is titled 'Account Setting' and 'My Account > Add User'. It contains a form with the following fields: 'Email' and 'Re-type Email' (password fields with a strength indicator), 'User Name' (text field with 'Eric'), 'Region' (dropdown menu with 'Global' selected), and 'Role' (dropdown menu with 'Admin' selected). Below these is the 'Manage Sub Account' section with two radio buttons: 'All' and 'Selected' (which is selected). Under 'Selected', there are two checkboxes, each with a subaccount icon and ID: the first is checked and labeled '0000 0000', the second is unchecked and labeled '0000 0001'. At the bottom right are 'Submit' and 'Cancel' buttons.

User roles

The multitenancy account includes different user roles. You can view users and their roles by clicking the *Account Setting* icon. For multitenancy accounts, admins and regular users can select single or multiple subaccounts.

User role	Description
Admin	Can access and manage devices under all subaccounts.
Regular	View-only access to devices under all subaccounts.

IOC

The indicators of compromise (IOC) service alerts administrators about newly found infections and threats to devices in their network. By analyzing unified threat management logging and activity, IOC provides a comprehensive overview of threats to the network.

IOC detects the following threat types, based on the evolving FortiGuard database:

Threat type	Description
Malware	Malicious programs residing on infected endpoints
Potentially unwanted programs	• Spyware • Adware • Toolbars
Unknown	Threats that the signature detected but are unassociated with any known malware

A subscription grants access to IP address allowlisting, which allows you to narrow your malware search by excluding safe IP addresses and domains, and alert emails to notify you directly of detected network threats. You can also view infected devices' full IP addresses, allowing you to better control their access to your network.

You must enable the IOC column in Network Overview. See [Network Overview on page 28](#).

To purchase an IOC subscription:

1. Go to [FortiGate Cloud Indicators of Compromise](#) for purchase options.
2. Complete the purchase process and wait for the key to arrive by email.
3. Log into the [Fortinet Support website](#).
4. On the *Asset* page, register the code as if it is a new product's serial number, and then enter the serial number of the FortiGate Cloud-connected device that you want the service to monitor. The service automatically takes effect.

To access IOC:

In the FortiGate list, look to the right. A bomb icon is visible. Click the bomb icon.

API access

The following provides instructions on how to access and call the FortiGate Cloud API. You can find all supported API calls at the [FortiGate Cloud REST API documentation](#).

FortiOS version 7.0 and later versions return Gzipped binary file responses by default. For CURL, you can add the `- -compressed` tag in your query to get the unzipped plain response.

For FortiGate Cloud API calls, the host address depends on the server environment as follows:

Environment	Host address
Global	api.fortigate.forticloud.com
Europe	euapi.fortigate.forticloud.com
Japan	jpapi.fortigate.forticloud.com

All API calls that this guide includes use the global environment as an example.

To make an API call using a server authentication token:

1. Call the token retrieval API. The following provides an example:

Request:

```
curl -H "Content-Type: application/json" -X POST -d '{
  "accountId": "xxx", "userName": "xxx", "password": "xxxxxxxxx"
}' https://www.forticloud.com/forticloudapi/v1/auth
```

Response:

```
{
  "access_token": "EXAMPLETOKEN", "expires_in": 14400, "message": "successfully authenticated", "refresh_token": "syIsrAofcHe67bTFdmhhT5pInnqCXT", "scope": "read write", "status": "success", "token_type": "Bearer"
}
```

Substitute in your FortiGate Cloud account credentials and host address.

2. You can query all supported FortiGate Cloud APIs using the access token that you retrieved from step 1. The following provides an example:

Request:

```
curl -H "Content-Type: application/json" -H "Authorization: Bearer EXAMPLETOKEN" -X GET https://www.forticloud.com/forticloudapi/v1/devices
```

Response:

```
[{"sn": "", "name": "FortiGate-100D", "timeZone": "-7.0", "tunnelAlive": true, "contractEndTime": 0, "model": "FortiGate 100D", "firmwareVersion": "6.2.8", "management": false, "initialized": false, "subAccountOid": 793, "ip": "172.16.30.193", "latitude": null, "longitude": null, "total": 8, "trial": false}, {"sn": "FG60DP4614004455", "name": "FG60DP4614004455-Daniel-FGT", "timeZone": "-7.0", "tunnelAlive": false, "contractEndTime": 0, "model": "FortiGate", "firmwareVersion": "6.0.9", "management": true, "initialized": false, "subAccountOid": 1, "ip": "172.16.93.119", "latitude": null, "longitude": null, "total": 8, "trial": true}, {"sn": "FGT60ETK1809A1GX", "name": "FGT60ETK1809A1GX", "timeZone": "-8.0", "tunnelAlive": false, "contractEndTime": 0, "model": "FortiGate", "firmwareVersion": ...}]
```

To make an API call using an IAM user authentication token:

1. If you do not already have one, create an Identity & Access Management (IAM) API user:
 - a. Log in to the [IAM portal](#) using your FortiGate Cloud account credentials.
 - b. Go to *API Users*, then click *ADD API USER*. Click *Next*.
 - c. Under *Effective Portal Permissions*, select *FortiGate*, then *ADD*. Click *Next*.
 - d. Click *Edit*. Toggle *Allow Portal Access* to *YES*. Under *Access Type*, select *Admin*. Click *CONFIRM*.
 - e. Click *DOWNLOAD CREDENTIALS*. Open the downloaded file to view your username and password.
2. Retrieve the access token by calling the FortiAuthenticator token retrieval API: `/oauth/token/`. The following provides an example where the FortiAuthenticator IP address is `customerapiauth.fortinet.com`:

Request:

```
curl -H "Content-Type: application/json" -X POST -d
https://customerapiauth.fortinet.com/api/v1/oauth/token/ '{"username":"AC0F1454-
3CCD-4523-8B3C-
4412156CB197","password":"a679bc11d6011e6ea3a7390cef0cd66b!1Aa","client_
id":"fortigatecloud","grant_type":"password"}'
```

Response:

```
{"access_token": "EXAMPLETOKEN", "expires_in": 14400, "message": "successfully
authenticated", "refresh_token": "syIsrAofcHe67bTFdmhhT5pInnqCXT", "scope": "read
write", "status": "success", "token_type": "Bearer"}
```

3. You can query all supported FortiGate Cloud APIs using the access token that you retrieved from step 2. The following provides an example:

Request:

```
curl -H "Content-Type: application/json" -H "Authorization: Bearer EXAMPLETOKEN" -X GET
https://www.forticloud.com/forticloudapi/v1/devices -k
```

Response:

```
[{"sn":"FG100D3G15803161","name":"FortiGate-100D","timeZone":-
7.0,"tunnelAlive":true,"contractEndTime":0,"model":"FortiGate
100D","firmwareVersion":"6.2.8","management":false,"initialized":false,"subAccountO
id":793,"ip":"172.16.30.193","latitude":null,"longitude":null,"total":8,"trial":fal
se},{ "sn":"FG60DP4614004455","name":"FG60DP4614004455-Daniel-FGT","timeZone":-
7.0,"tunnelAlive":false,"contractEndTime":0,"model":"FortiGate","firmwareVersion":"
6.0.9","management":true,"initialized":false,"subAccountOid":-
1,"ip":"172.16.93.119","latitude":null,"longitude":null,"total":8,"trial":true},
{ "sn":"FGT60ETK1809A1GX","name":"FGT60ETK1809A1GX","timeZone":-
8.0,"tunnelAlive":false,"contractEndTime":0,"model":"FortiGate","firmwareVersion
...}
```

To call FortiOS APIs via FortiGate Cloud:

1. If the management feature is disabled on the desired FortiGate, enable it by calling `devices/{sn}/management`. The following provides an example:

Request:

```
curl -H "Content-Type: application/json" -H "Authorization: Bearer EXAMPLETOKEN" -X PUT
-d '{"management":true, "username":"xxx", "password":"xxx"}'
https://www.forticloud.com/forticloudapi/v1/devices/FGT60D461xxxxxxx/management
```

2. You can proxy any FortiOS API via FortiGate Cloud. The format for calling FortiOS APIs from FortiGate Cloud is as follows:

```
https://www.forticloud.com/forticloudapi/v1/fgt/<SN>/<FortiOS API>
```

The following provides an example request where the FortiGate serial number is `FGT60D461xxxxxxx` and the API being called is `/api/v2/monitor/fortiguard/service-communication-stats`, which retrieves historical statistics for communication with FortiGuard services.

Request:

```
curl -H "Content-Type: application/json" -H "Authorization: Bearer EXAMPLETOKEN"  
https://www.forticloud.com/forticloudapi/v1/fgt/FGT60D461xxxxxxx/api/v2/monitor/for  
tiguard/service-communication-stats
```

For FortiOS API information, see the [FortiOS REST API documentation](#).

Frequently asked questions

What do I do if FortiOS returns an *Invalid Username or Password/FortiCloud Internal Error/HTTP 400* error when activating FortiGate Cloud on the FortiOS GUI?

Do the following:

1. Ensure that you can log into FortiGate Cloud via a web browser using the same username and password that you attempted to activate FortiGate Cloud with on the FortiOS GUI.
2. Confirm that the FortiGate can ping `logctrl1.fortinet.com` or `globallogctrl.fortinet.net`.
3. Connect via Telnet to the resolved IP address from step 2 using port 443.
4. Ensure that the FortiGate Cloud account password length is less than 20 characters.
5. If running FortiOS 5.4 or older versions, ensure that the FortiGate Cloud account password does not include special characters, as these FortiOS versions do not support this.
6. If the FortiGate is a member of a high availability (HA) pair, ensure that you activate FortiGate Cloud on the primary device. Activate FortiGate Cloud on the primary FortiGate as [To deploy a FortiGate/FortiWifi to FortiGate Cloud in the FortiOS GUI: on page 20](#) describes. FortiGate Cloud activation on the primary FortiGate activates FortiGate Cloud on the secondary FortiGate. Local FortiGate Cloud activation on the secondary FortiGate fails.
7. Enable FortiGate Cloud debug in the CLI. The `get` command displays the device timezone, while the `diagnose debug console timestamp enable` command shows the date timestamp for the debug logs.

```
config system global
  get
end
diagnose debug console timestamp enable
execute fortiguard-log domain
diagnose debug application forticldd -1
diagnose debug enable
execute fortiguard-log login email password
```

Email any debug output to admin@forticloud.com.
8. If you see the HTTP 400 error, enable HTTP debug with the `diagnose debug application httpsd -1` command.

Why can I log into the FortiGate Cloud but not activate the FortiGate Cloud account in FortiOS with the same credentials?

FortiOS 5.4 and older versions do not support passwords with special characters. If you are running FortiOS 5.4 or an older version and attempting to activate a FortiGate Cloud account with a password that includes special characters, the activation fails. You must remove special characters from the password, or upgrade to FortiOS 5.6 or a later version.

How can I change the FortiGate Cloud account ID from A to B?

See [To replace a FortiGate Cloud user account ID with a new email address](#): on page 65.

How can I move a FortiGate from account A to account B in the same region?

See [To move a FortiGate/FortiWifi deployed to FortiGate Cloud to another account](#): on page 21.

How can I activate my FortiGate Cloud on HA-paired FortiGates?

Activate FortiGate Cloud on the primary FortiGate as [To deploy a FortiGate/FortiWifi to FortiGate Cloud in the FortiOS GUI: on page 20](#) describes. FortiGate Cloud activation on the primary FortiGate activates FortiGate Cloud on the secondary FortiGate. Local FortiGate Cloud activation on the secondary FortiGate fails.

You can also disable HA on both devices, activate FortiGate Cloud on each device, then enable HA.

How can I establish a management tunnel connection between my FortiGate and FortiGate Cloud?

```
config system central-management
  set type fortiguard
end
diagnose fdsm contract-controller-update
fnsysctl killall fgfmd
```

What do I do if a FortiGate added by its cloud key stays in an inactive state for more than 24 hours?

1. Check the FortiGate network settings and ensure that port 443 is not blocked.
2. Connect via Telnet to `logctrl1.fortinet.com` or `globallogctrl.fortinet.net` (if FortiOS supports Anycast) through port 443.
3. In the FortiOS GUI, activate FortiGate Cloud as [To deploy a FortiGate/FortiWifi to FortiGate Cloud in the FortiOS GUI: on page 20](#) describes.

What do I do if the "Device is already in inventory" message appears when importing a FortiGate by key?

This message means that the device has already been added to an account inventory. Another user may have tried to add the device to another account. If you cannot find the device on the Inventory page, contact cs@fortinet.com.

What do I do if the invalid key message appears when importing a FortiGate by key?

The FortiCloud key is for one-time use only. Log into the FortiGate and activate FortiGate Cloud as [To deploy a FortiGate/FortiWifi to FortiGate Cloud in the FortiOS GUI: on page 20](#) describes instead. If you cannot connect to the FortiOS GUI, contact cs@fortinet.com to reenale the key.

What do I do if FortiGate Cloud activation via the FortiOS GUI succeeds, but I cannot find the FortiGate in the FortiGate Cloud portal?

When a new FortiGate is added to FortiGate Cloud, FortiGate Cloud dispatches it to the global or Europe region based on its IP address geolocation. If the FortiGate warranty region is Japan, FortiGate Cloud dispatches it to the Japan region.

How can I move a FortiGate from region A to region B?

1. Log in to FortiGate Cloud region A.
2. Undeploy the device.
3. Verify that the device has returned to the Inventory page.
4. Switch the portal to region B.
5. Go to Inventory and deploy the device.

How can I connect to FortiGate by remote access?

You must set the FortiOS central management setting to FortiCloud. The management tunnel status must be up. See [How can I establish a management tunnel connection between my FortiGate and FortiGate Cloud? on page 78](#). See [To remotely access a device: on page 34](#).

How can I activate FortiGate Cloud using a different email FortiCare account when FortiOS does not allow entering another email?

```
execute fortiguard-log login <email> <password>
```

What do I do if the migrate notice still appears after successful migration?

The migrate notice appears when FortiOS detects different email addresses used for FortiCare and FortiGate Cloud. FortiOS has a known issue that it is case-sensitive when verifying an email address. For example, FortiOS may consider example@mail.com and Example@mail.com as different email addresses. Contact cs@fortinet.com to ensure both accounts use all lower-case letters.

What do I do if FortiDeploy does not work?

1. Ensure that the FortiManager settings are correct and the device can connect to FortiManager.
2. Confirm that the central management setting on the device is set to FortiCloud.
3. Ensure that the device can connect to logctrl1.fortinet.com via port 443.
4. Import the device to the inventory by FortiCloud key. See [To deploy a FortiGate/FortiWifi to FortiGate Cloud using the FortiCloud key: on page 19](#).
5. Deploy the device to FortiManager, then power up the device. If the device is already powered up, run `execute fortiguard-log join`.
6. If the FortiCloud key has been used and is invalid for reuse, log into the device GUI and activate FortiGate Cloud as [To deploy a FortiGate/FortiWifi to FortiGate Cloud in the FortiOS GUI: on page 20](#) describes.

What do I do if FortiOS does not upload logs?

Gather debug logs for the following commands, then send the debug output to fortigatecloud@forticloud.com. Check log upload settings on the FortiGate and ensure that it is configured to send logs to FortiGate Cloud:

```
execute telnet <log server IP address> 514
diagnose test application forticldd 1
diagnose test application miglogd 6
diagnose debug application miglogd -1
diagnose debug enable
```

What do I do if FortiGate Cloud cannot retrieve logs from FortiOS when data source is set as FortiGate Cloud?

Ensure that you can see logs in the FortiGate Cloud portal.

In poor network conditions, increase the timeout period to avoid connection timeout:

```
config log fortiguard setting
    set conn-timeout 120
end
```

How can I export more than 1000 lines of logs?

See [To download logs](#): on page 52.

How can I receive a daily report by email?

Ensure that FortiGate Cloud generated the scheduled report and that you have added the email address. See [Reports on page 54](#).

Why does FortiGate not submit files for Sandbox scanning?

Check the FortiGate settings:

- For FortiOS 6.2 and later versions:
 - Ensure that FortiGate Cloud has been activated.
 - Go to *Security Profiles > AntiVirus*. Ensure that *Suspicious Files Only* or *All Supported Files* is enabled.
- For FortiOS 6.0 and earlier versions:
 - Go to *System > Feature Visibility*, then enable *FortiSandbox Cloud*.
 - Go to *Security Fabric > Settings*. Enable *Sandbox Inspection*.
 - Go to *Security Profiles > AntiVirus*. Ensure that *Suspicious Files Only* or *All Supported Files* is enabled.
 - Go to *Policy & Objects > IPv4 Policy*. Enable antivirus for the policy in use.

What backup retention does FortiGate Cloud provide?

Backup does not have storage limits. For licensed devices, the retention period is one year. For unlicensed devices, the retention period is seven days.

How does automatic backup work?

Automatic backup is either per session or day. FortiGate setting changes from FortiOS or FortiGate Cloud trigger backup. If there is no changes to FortiGate settings, FortiGate Cloud does not perform a backup. See [To enable auto backup: on page 40](#).

What does it mean if a geolocation attribute configuration change log/alert is received?

This is a feature to sync a FortiGate device's geolocation information between the FortiOS GUI, FortiGate Cloud, and the Asset Management portal. When a new device is being provisioned, or there is a change in a provisioned device's IP address, or a user moves a device to another location on the map view, its new geolocation attributes are pushed to the device via the management tunnel with username as *FortiGateCloud*. Since the geolocation database may not be entirely accurate, it is possible that a device is placed at a wrong location on the map, but you can move the device to its correct location on Map View.

What do I do if FortiGate Cloud does not reflect a new hostname on a FortiGate or FortiGate Cloud overwrites a new FortiGate hostname?

To synchronize the local hostname on a FortiGate and in FortiGate Cloud, compare the times of the FortiGate Cloud portal change and the local hostname modification on the device GUI. Use whichever time is the latest.

- When you change the hostname within the FortiGate Cloud portal, FortiGate Cloud pushes the change to the device via the management tunnel.
- When you change the hostname within the device GUI, the device only sends the new hostname to FortiGate Cloud with its next FCP UpdateMgr request.

To ensure that FortiGate Cloud can immediately reflect hostname changes, you can run the `diagnose fdsm contract-controller-update` command in the CLI after changing the hostname:

Can I revert back from FortiGate Cloud 2.0 after upgrade?

Once the upgrade to FortiGate Cloud 2.0 is complete, you cannot revert back within the FortiGate Cloud portal. If you want to revert your FortiGate Cloud environment, contact the [support team](#) as soon as possible.

Why is my FortiGate deployed to a region other than global (U.S. or Europe)?

There are several possible cases:

- The FortiGate has a physical IP address outside of North America, and thus FortiGate Cloud's dispatcher server deploys the device according to its IP address's geolocation.
- When activating FortiGate Cloud from the web UI, for some FortiOS versions, the user could choose a region to deploy the device. The default region is global, and the user could optionally select Europe or U.S.
- For U.S. government orders, the FortiGate has a US-Government license key burnt in BIOS, and therefore such a device could only be provisioned to the US region of FortiGate Cloud. For a FortiGate VM instance, the default server location is usa, and therefore, to provision a VM instance to another region other than US, you must first change its server location configuration to 'automatic'.

How do I check if my FortiGate has been preset for a specific server location?

In CLI, browse for `update-server-location` under `system fortiguard` settings. For a device with a USG license key, `update-server-location` does not apply, so you can use the `get system status` to check for `License Status: US-Government (USG)`.

Can I change the server location configuration?

Yes, for non-USG FortiGates, run the following commands in CLI to change this configuration:

```
config system fortiguard
  set update-server-location <usa>|<automatic/any>|<eu>
end
```

If my FortiGate's server location is automatic/any, how do I deploy it to my preferred region?

You may choose the preferred region from the web UI FortiGate Cloud activation page, or run the following commands in the CLI: `exe fortiguard-log login <email> <password> <GLOBAL|EUROPE|US>`.

Can I migrate logs uploaded or reports generated to a different region?

No, you cannot migrate existing data cannot to another region. FortiGate Cloud only uploads new data to the new region from the time that you updated the region settings.

How do I choose my region for the FortiGate Cloud (Premium) portal?

FortiGate Cloud (Premium)'s region is the region from which the upgrade is initiated. Once upgraded, you cannot simultaneously use other regions in the FortiGate Cloud (Premium) portal. Using a different account or enabling multitenancy is recommended for multiregion scenarios.

How do I change my region in the FortiGate Cloud (Premium) portal?

Migrating to another region for the same account is not permitted as the data cannot be allowed to move across the regions. Instead, creating a new account and reprovisioning the devices to the new account is recommended.



www.fortinet.com

Copyright© 2023 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 General Counsel, 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.