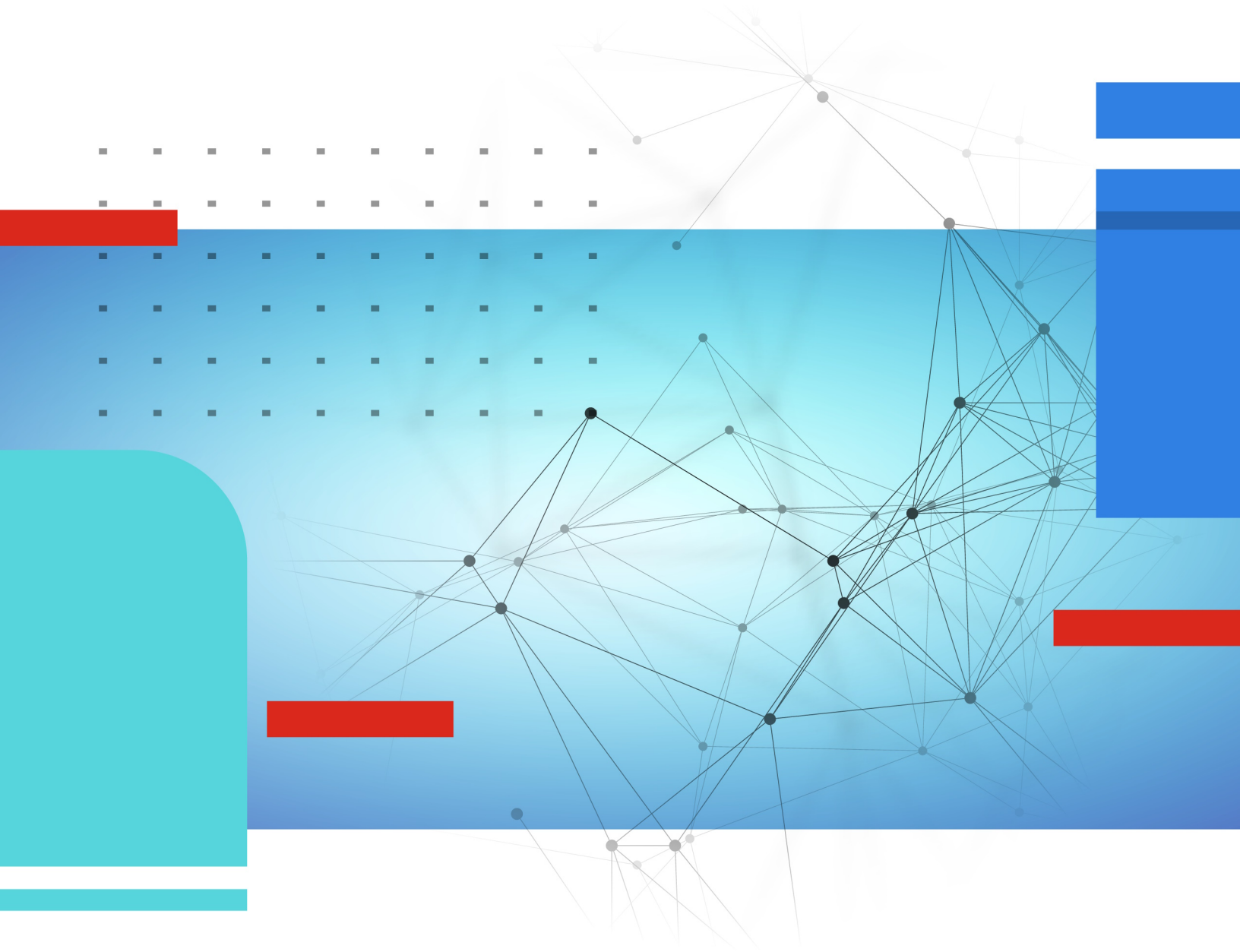
Administration Guide

FortiGate Cloud 25.1.a Portal (Beta) 25.1.a



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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

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

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

February 19, 2025
FortiGate Cloud 25.1.a Portal (Beta) 25.1.a Administration Guide
32-251a-1113632-20250219

TABLE OF CONTENTS

Change log

Date	Change description
2025-02-03	Initial release.
2025-02-04	Added Frequently asked questions on page 51.
2025-02-19	Added How can I activate FortiGate Cloud 25.1.a Portal (Beta) on a FortiGate provisioned to an OU placeholder account? on page 60.

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 25.1.a Portal (Beta) is the latest version, which includes various user experience (UX) and feature enhancements.

FortiGate Cloud 25.1.a Portal (Beta) is a redesigned version of FortiGate Cloud with enhanced UX and features. It combines the standard FortiGate Cloud and FortiGate Cloud Premium offerings. The cloud-based SaaS offers configuration management for FortiGates, FortiGate-VMs with FortiGate-connected FortiAPs, FortiSwitches, and FortiExtenders. FortiGate Cloud simplifies network and security management with zero-touch provisioning, firewall configuration and policies, cloud backups, firmware upgrades, rich log analytics, reporting, and audit log, and includes one-year log retention.

This latest revision includes modern look and feel enhancements, improved navigation and access, and features such as centralized and customizable dashboards, full-featured FortiOS configuration management from the cloud, centralized reporting with 30 report templates, log views, Fortinet Security Fabric firmware upgrades, and so on.

There is no additional license required to upgrade. For upgrade eligibility and requirements, see Requirements on page 9. Features on page 8 includes the full list of FortiGate Cloud 25.1.a Portal (Beta) features.

FortiGate Cloud 25.1.a Portal (Beta) provides the following features:

- Centralized dashboard with widgets to view Fortinet Security Fabric devices, health, licenses, and other information
- Real-time FortiOS configuration management
- Centralized logging, analytics, and reports
- Ability to create and schedule a full range of reports
- FortiCloud account support, including multifactor authentication
- User management (FortiCloud Identity & Access Management)
- Configuration backup and restore
- Log download
- Firmware management
- CLI scripts
- Audit logs to view user actions
- FortiSandbox SaaS
- FortiGuard Indicators of Compromise
- Role-based access to read-only views
- Multiple languages
- SD-WAN dashboard

You can upgrade your FortiGate Cloud or FortiGate Cloud Premium environment to FortiGate Cloud 25.1.a Portal (Beta).

FortiGate Cloud 25.1.a Portal (Beta) supports multitenancy with FortiCloud Organizations.

- You cannot activate a legacy subaccount-based multitenancy license (SKU FCLE-10-FCLD0-161-02-DD) in FortiGate Cloud 25.1.a Portal (Beta).
- You cannot upgrade an account with subaccount-based multitenancy enabled to FortiGate Cloud 25.1.a Portal (Beta).

See Upgrading to FortiGate Cloud Premium (Beta) for details.

Features

FortiGate Cloud 25.1.a Portal (Beta) has the following functions:

Function	Description
Centralized dashboards	Network overview dashboard includes widgets for the status of Fortinet Security Fabric devices, device health, licenses, Sandbox, and other information. Customizable status, network, and security widgets plus real-time monitors for each FortiGate.
Assets	Device inventory as list or on map with diagnostic health, network statistics, and license information.
Device management	Real-time FortiGate configuration management from the cloud to configure your network interfaces, SD-WAN, firewall policies, security profiles, VPN, and Security Fabric.
Log analysis	Real-time traffic, events, system logs for network activity, and threat analysis.
Centralized reports	Generate on-demand reports or schedule and get predefined reports delivered at intervals for network analytics and monitor usage patterns.
Firmware upgrade	Remotely upgrade FortiOS on FortiGate devices.
AP, FortiSwitch, and FortiExtender management via FortiGate	• Manage FortiAPs, AP profiles, SSIDs, and monitor WiFi clients and NAC policies • Manage FortiSwitches, VLANs, ports, and policies • Manage FortiExtenders, profiles, and data plans
FortiSandbox SaaS	Upload and analyze files that FortiGate antivirus (AV) marks as suspicious.
Indicators of Compromise	Alerts on newly found infections and threats to devices in the network
Regions	FortiGate Cloud includes the Global (Canada), U.S., and Europe (Germany) regions.
Multitenancy	Multitenancy based on FortiCloud Organizations. FortiGate Cloud 25.1.a Portal (Beta) does not support subaccount-based multitenancy.
In-portal cloud access	Access the GUI for provisioned FortiGates running FortiOS 7.0 and later versions.

Requirements

Requirement	Description
FortiCloud account	Create a FortiCloud account if you do not have one. Launching FortiGate Cloud 25.1.a Portal (Beta) requires a FortiCloud account. A FortiCloud account administrator can add Identity and Access Management users to the access the account with admin or read-only roles. If you are using a legacy FortiGate Cloud 25.1.a Portal (Beta) account, merging your account to your FortiCloud account is recommended.
FortiGate or FortiWifi license	You must register all FortiGate or FortiWifi devices on FortiCloud.
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 25.1.a Portal (Beta).
Browser	FortiGate Cloud supports Firefox, Chrome, Edge, and Safari.

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.

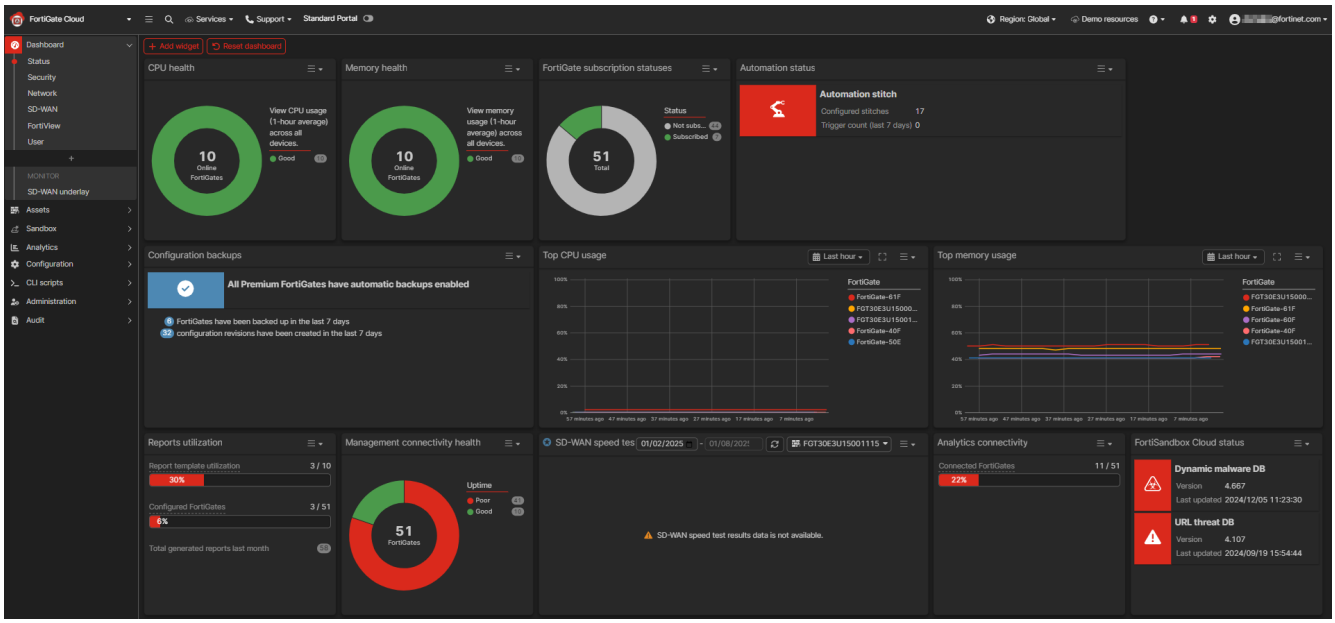
Purpose	Protocol	Port
Syslog, registration, quarantine, log, and report	TCP	443
OFTP	TCP	514
Management	TCP	541
Contract validation	TCP	443
Config portal	TCP	8443

Getting started with FortiGate Cloud 25.1.a Portal (Beta)

After toggling on FortiGate Cloud 25.1.a Portal (Beta), go to https://fortigate.forticloud.com to access FortiGate Cloud 25.1.a Portal (Beta).

After you log in, the FortiGate Cloud 25.1.a Portal (Beta) portal displays the *Dashboard* > *Status* page. You can switch regions using the region selector and access FortiGate Cloud 25.1.a Portal (Beta) documentation from the *?* icon.

The *Dashboard* > *Status* page displays a variety of widgets. The widgets provide information about the devices that your FortiGate Cloud 25.1.a Portal (Beta) is managing, such as how many FortiGates have subscriptions. *Dashboard* > *Security* provides details on the current FortiSandbox URL threat database version.



From the banner, you can access options including the following:

Option	Description
FortiGate quick selection menu	Select a FortiGate from the dropdown list to access it. See Accessing a FortiGate on page 28.
Menu icon	Use the menu icon to collapse or display the left pane, which displays other configuration options.
Search icon	Click the search icon to access a searchbar. You can search for a FortiGate Cloud 25.1.a Portal (Beta) GUI page or widget with a name that contains your search term. See To search for a GUI page or widget: on page 11.
Services	Access another Fortinet service.
Support	Access Fortinet support options, such as contacting the Fortinet support team.
Standard Portal toggle	Toggle on to return to using FortiGate Cloud standard portal.
Region selection	Select another region to access FortiGate Cloud 25.1.a Portal (Beta) in.
Demo resources	View use case videos and access FortiGate Cloud 25.1.a Portal (Beta) documentation for accounts created within the past 90 days.
Documentation link	Access FortiGate Cloud documentation.
Notifications	View and acknowledge notifications, such as for upcoming automatic FortiGate firmware upgrades.
Preferences	Configure dark or light theme, language to display FortiGate Cloud 25.1.a Portal (Beta) in, and other settings.
User menu dropdown	Displays the current logged in user. You can use the dropdown list to switch accounts or view account settings.

To search for a GUI page or widget:

1. In the banner, click the search icon.
2. In the *Search* field, enter the desired search term. FortiGate Cloud 25.1.a Portal (Beta) searches for GUI page names and Dashboard widget names that contain your search term.
3. FortiGate Cloud 25.1.a Portal (Beta) displays the search results. You can filter the results by *Navigation menu* or *Dashboard* widget on the left pane, and sort by relevance or ascending or descending alphabetical order in the upper right corner. Use the search results to navigate to the desired page or widget.

From the left pane, you can access other options including assets, Sandbox, analytics, and configuration features.

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

Option	Description
Dashboard	*Dashboard* displays a variety of widgets. The widgets provide information about the devices that your FortiGate Cloud 25.1.a Portal (Beta) is managing.
Assets	View a centralized inventory of all FortiGate and FortiWifi devices. See Assets on page 25.
Sandbox	View the scan results from files that Sandbox submitted to FortiGuard for threat analysis. See Sandbox on page 31.
Analytics	Create and alter report configurations and their settings. These report configurations are available for all deployed devices. See Analytics on page 34.
Configuration	Manage FortiGate Cloud 25.1.a Portal (Beta) account and Sandbox settings. See Configuration on page 40.
CLI Scripts	Configure and schedule scripts of CLI commands to run on your FortiGates. See CLI scripts on page 42.
Administration	Configure automation and firmware management options. See Administration on page 43.
Audit	View a log of actions that users have performed on FortiGate Cloud Premium.

License types

Description	SKU
Management, Analytics, and one-year log retention	
FortiGate and FortiWifi	FC-10-00XXX-131-02-DD
Multitenancy	
Multitenancy with FortiCloud Organizations	FC-15-CLDPS-219-02-DD
FortiSandbox SaaS (per device)	
FortiSandbox Saas for FortiGate	FC-10-XXXXX-811-02-DD

Description	SKU
	FC-10-XXXXX-950-02-DD FC-10-XXXXX-928-02-DD FC-10-XXXXX-100-02-DD
FortiDeploy	
Bulk provisioning	FDP-SINGLE-USE
SD-WAN Cloud Assisted Monitoring	
Optional/add-on license needed for SD-WAN widgets	FC-10-*-288-02-12

The FortiGate Cloud 25.1.a Portal (Beta) subscription for management, analytics, and one-year log retention is available for FortiGates or FortiWiFi devices (per device) with a one-, three- or five- year service term. For high availability clusters, a subscription is required for each device.

For multitenancy using FortiCloud organizations, see Standard versus unlimited access to the Organization Portal.

For FortiSandbox SaaS upload limits, see Sandbox on page 31.

Provisioning FortiGates to FortiGate Cloud 25.1.a Portal (Beta) does not require a subscription. For limitations without a subscription, see Feature comparison on page 12. All devices must be registered on the Fortinet Support site.

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 25.1.a Portal (Beta) 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 25.1.a Portal (Beta) for these scenarios:

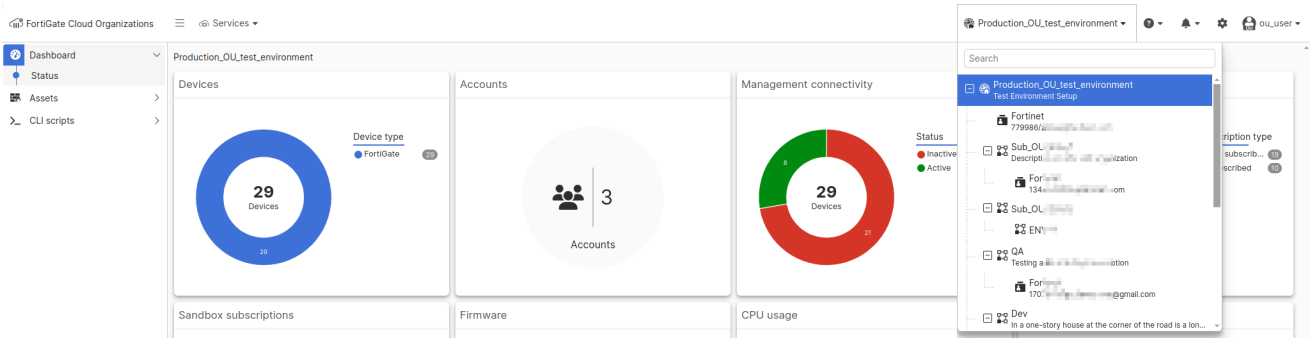
Feature	Device without paid subscription	Device with paid subscription
Cloud provisioning	Yes	Yes
Manual firmware upgrade	Yes.	Yes

Feature	Device without paid subscription	Device with paid subscription
	You must manually upgrade a FortiGate without a paid subscription to the latest patch within seven days of the patch becoming available. If the FortiGate is not upgraded within seven days, it remains connected to FortiGate Cloud 25.1.a Portal (Beta) but cannot use any FortiGate Cloud 25.1.a Portal (Beta) features and stops uploading logs to FortiGate Cloud Premium Portal (Beta). See Firmware management on page 44.	
Customizable patch firmware upgrade	No	Disabled by default and can be enabled
Cloud management, configurations, and backups	No	Yes
Reports	360 degree activity report only	Multiple predefined reports
CLI scripts	No	Yes
Event automation	No	Yes
Hosted log retention	Seven days	One year
SD-WAN monitoring	No	Yes
Security analytics	Yes	Yes
Cloud access	Read-only	Read/write
Remote access	Yes (read-only) For the following FortiOS versions, remote access with full permission (read and write) requires a registered FortiGate Cloud Service subscription on the FortiGate. • 7.6.0 and later versions • 7.4.2 and later versions • 7.2.8 and later versions • 7.0.14 and later versions Devices without a registered FortiGate Cloud 25.1.a Portal (Beta) Service Subscription running these FortiOS versions only support read-only remote access.	Yes (read-write)

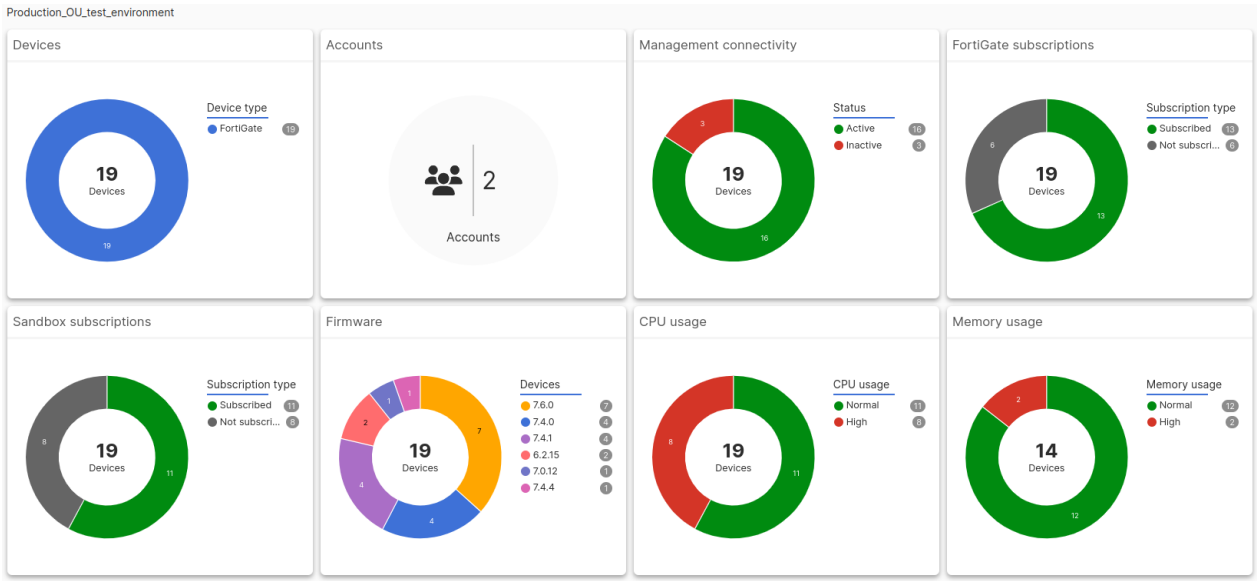
OU

FortiGate Cloud 25.1.a Portal (Beta) supports organizational unit (OU) account selection and switching. OU support is currently in beta. 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.



FortiGate Cloud 25.1.a Portal (Beta) opens to the OU Dashboard, which displays a variety of widgets that you can use to monitor your products and services. When you log in to an OU, the available widgets differ than when you log in to an account. The following table only lists OU dashboard widgets. For other widgets, see Dashboard on page 19.

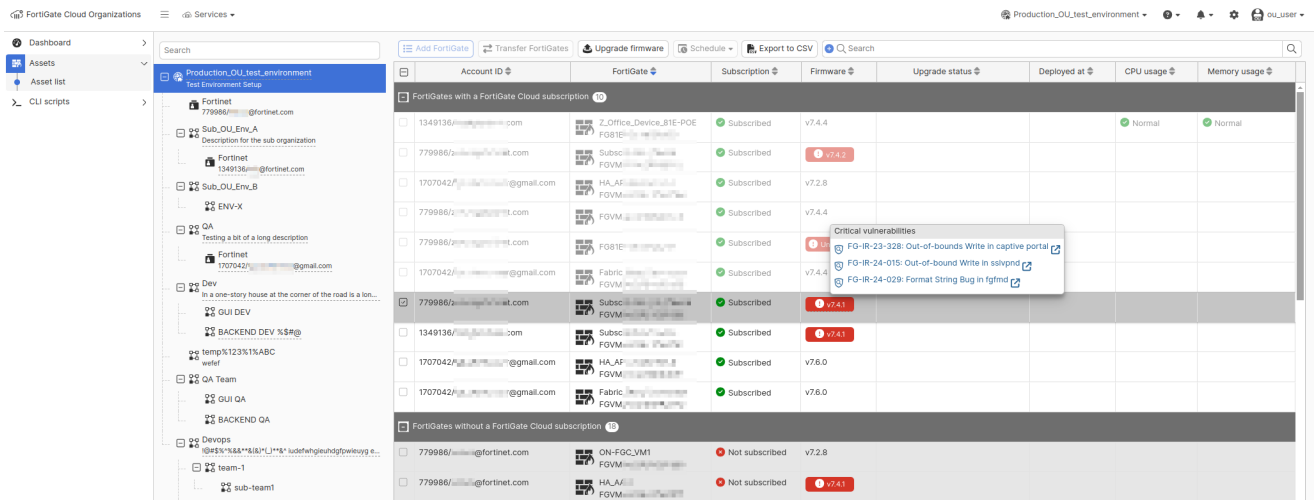


Widget	Description
Devices	Displays a donut chart that details the device type breakdown and total number of devices in this OU. To display the list of devices for each account in the OU, see OU Asset list on page 15.
Accounts	Displays a donut chart that details the total number of accounts in this OU. You can expand the widget to display the list of accounts in the OU.

Widget	Description
Management connectivity	Displays a donut chart that details the management connectivity status breakdown and total number of devices in this OU.
FortiGate subscriptions	Displays a donut chart that details the FortiGate Cloud license type breakdown and total number of devices in this OU.
Sandbox subscriptions	Displays a donut chart that details the Sandbox license type and total number of devices in this OU.
CPU usage	Displays a donut chart that details the CPU usage level of devices in the OU.
Memory usage	Displays a donut chart that details the memory usage level of devices in the OU.
Firmware	Displays a donut chart that details the firmware versions installed on devices in the OU.

OU Asset list

The OU Asset list displays the list of devices for each account in the organizational unit (OU). You can view device information for different OUs and accounts by using the navigation pane. The device list is separated into FortiGates that have a FortiGate Cloud subscription and FortiGates without a subscription. You can also manage firmware upgrades for FortiGates across the OU. The *Firmware* column also warns of potential critical vulnerabilities associated with your FortiGates' firmware versions. You can export the OU asset list and its data using *Export to CSV*.



This list displays the following information about the devices:

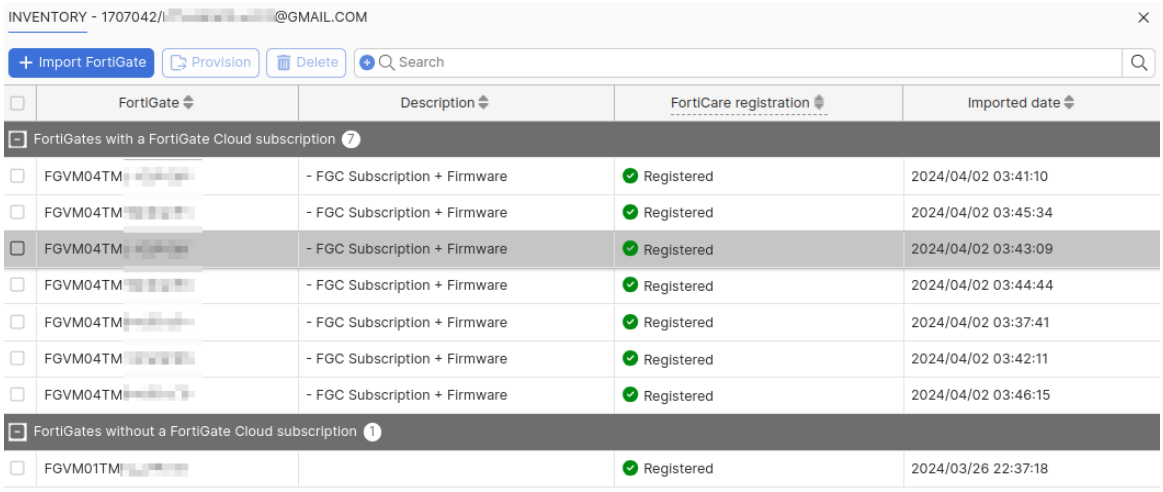
Column	Description
Account ID	FortiCloud account that the device is registered to.
Device name	Device name and serial number.

Column	Description
Firmware	Firmware version installed on the device.
Upgrade status	Displays if the FortiGate is currently performing a firmware upgrade.
Transfer status	Transfer status on the device.
CPU usage	CPU usage level on the device.
Memory usage	Memory usage level on the device.
Claimed on	(Optional, non-default) Date the device was claimed.
Deployment key	(Optional, non-default) Key used to deploy device.
Last backup	(Optional, non-default) Date and time of last configuration backup on the device.
Last log upload	(Optional, non-default) Date and time of last log uploaded by device.
Name	(Optional, non-default) Device name.
Serial	(Optional, non-default) Serial number.
Subscription	(Optional, non-default) Subscription status of the device.

You can import and provision FortiGates using OUs.

To import and provision a FortiGate:

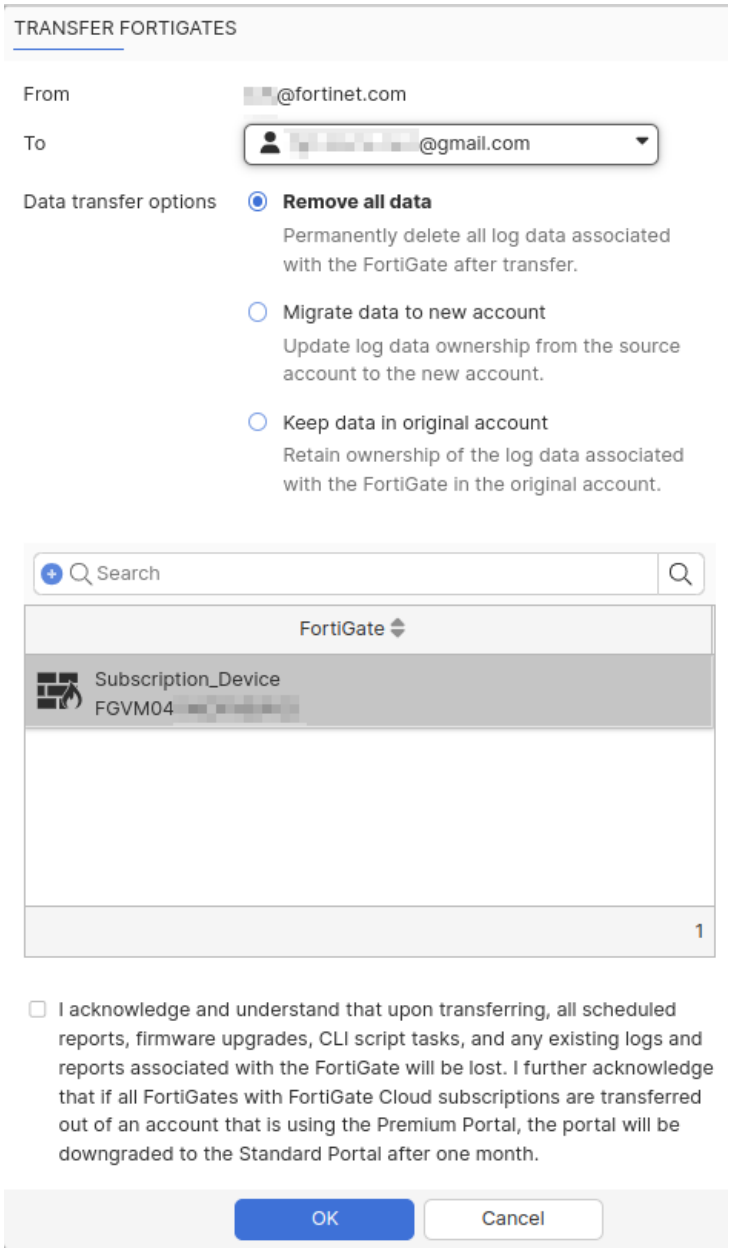
1. Go to *Assets* > *Asset list* in the OU view.
2. Select the account to add a FortiGate to by using the OU tree.
3. Click *Add FortiGate*.
4. On the *Inventory* slide, click *Import FortiGate*.
5. Enter a FortiCloud or FortiDeploy key(s), select a partner, and click *OK*.
6. Select the devices to provision on the *Inventory* slide and click *Provision*. The provisioned devices now are on the OU Asset list.



You can transfer FortiGates between accounts in an OU.

To transfer a FortiGate:

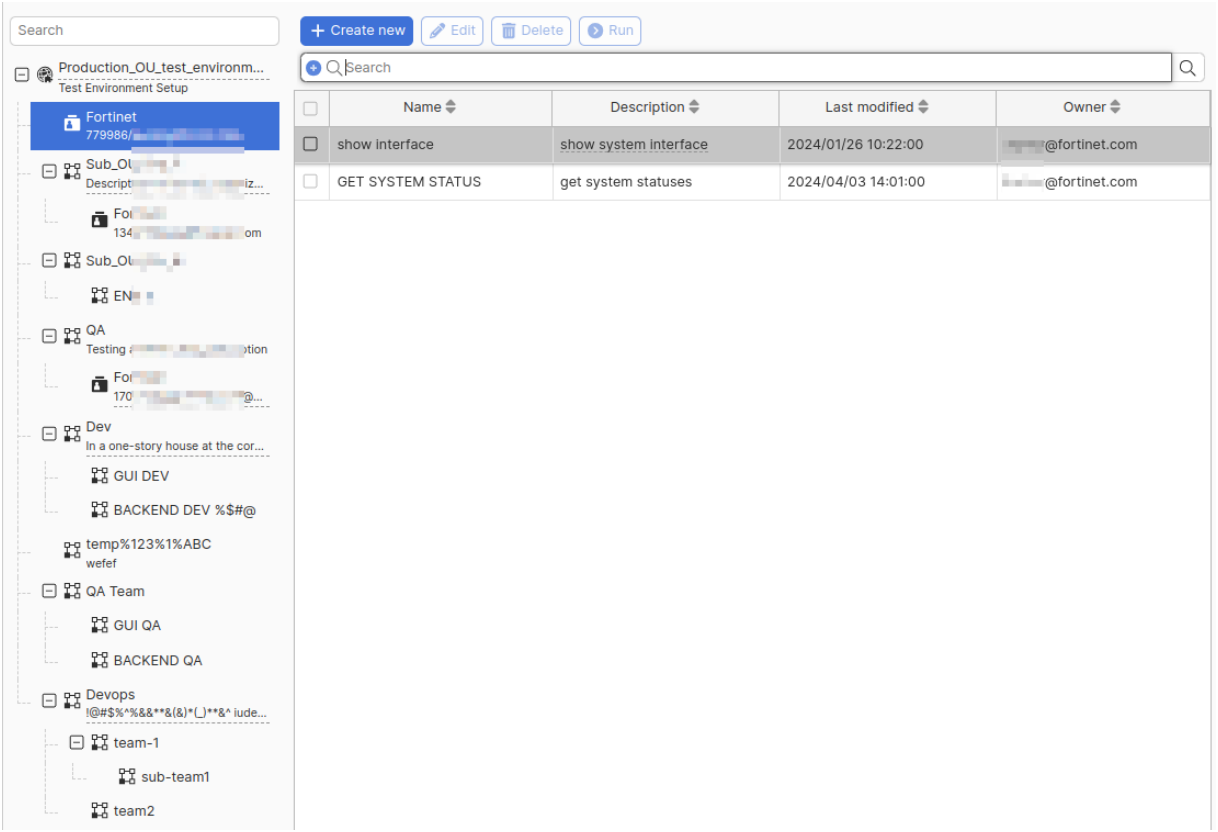
1. Go to *Assets* > *Asset list* in the OU view.
2. Select the account with the source FortiGate(s) you would like the transfer by using the OU tree.
3. Select the source FortiGate(s) on the table.
4. Click the *Transfer FortiGates* button.
5. On the *Transfer FortiGates* slide, select the destination account, data transfer option, click the acknowledgment, then click *OK*. The selected FortiGate(s) will now be transferred to from the source account to the destination account.



FortiGate Cloud 25.1.a Portal (Beta) supports transfers from and to FortiGate Cloud standard and premium portals.

OU CLI scripts

OU *CLI scripts* displays the list of CLI scripts for each account in the organizational unit (OU). You can view, manage, and schedule scripts for different OUs and accounts by using the navigation pane. For script management and scheduling instructions, see CLI scripts on page 42.



Dashboard

You see the *Dashboard* > *Status* page when you first open the FortiGate Cloud 25.1.a Portal (Beta) interface. The widgets provide information about the devices that your FortiGate Cloud 25.1.a Portal (Beta) manages, such as how many FortiGates have subscriptions.

For most widgets, you can click in to a section of the widget's displayed chart to view more details. For example, for the *FortiGate subscription statuses* widget, you can click the green portion of the donut chart, which represents the FortiGates that have a subscription. FortiGate Cloud 25.1.a Portal (Beta) then displays the *Assets* > *Asset list* filtered to only display FortiGates that have a subscription.

FortiGate Cloud 25.1.a Portal (Beta) contains the following dashboards:

- Status
- Security
- Network
- SD-WAN
- FortiView
- User

You can also create a custom dashboard. A star icon identifies widgets that require a subscription.

The following tables list the widgets available for each dashboard:

Status

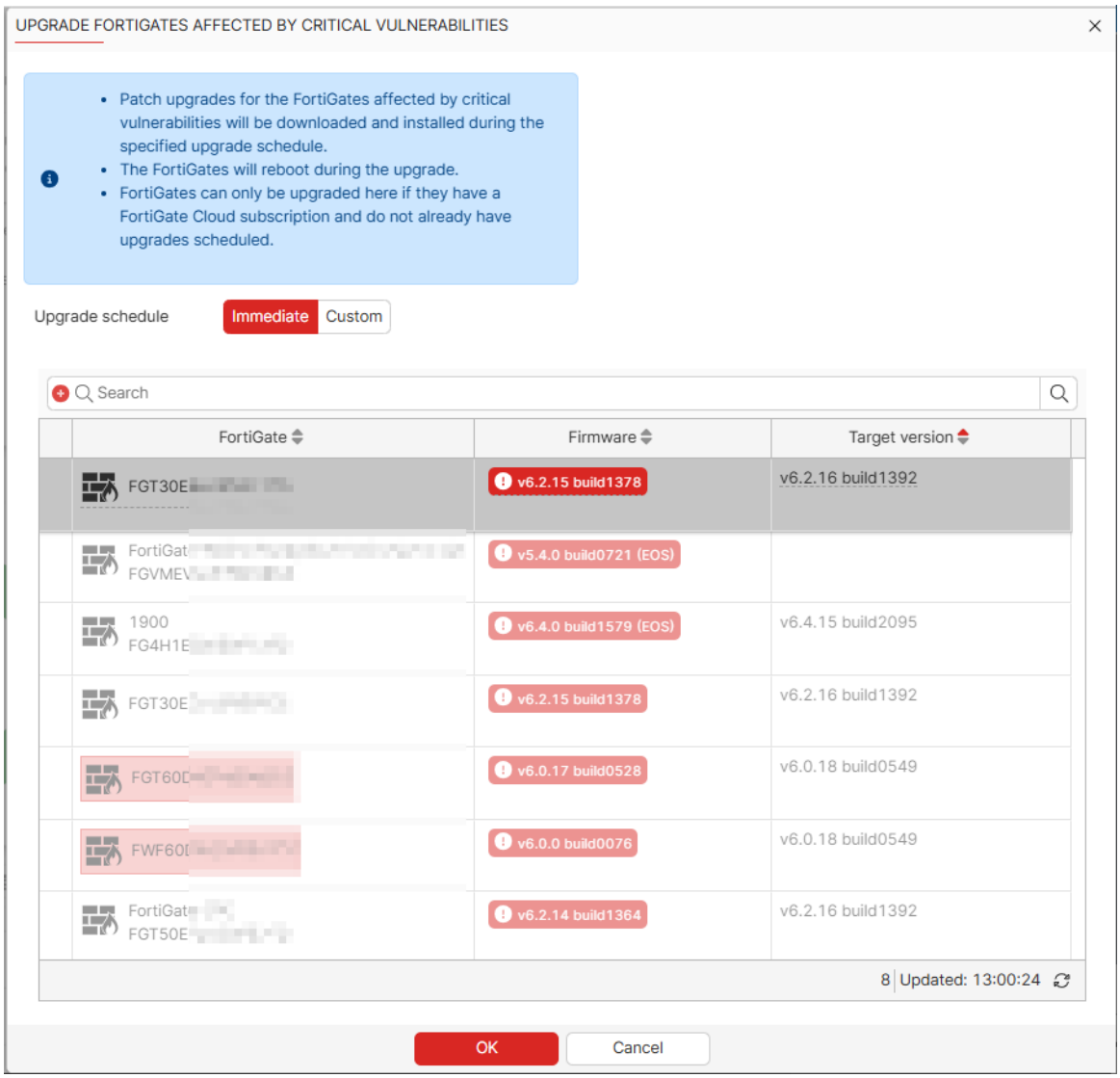
Widget	Description
FortiGate subscription statuses	Displays how many FortiGates do not have a paid subscription and how many have a premium subscription. Some features, such as the SD-WAN dashboard, require a premium subscription.
CPU health	Displays CPU usage statistics for the last hour for the connected FortiGates.
Top CPU usage	Displays FortiGates with the top CPU usage.
Memory health	Displays memory usage statistics for the last hour for the connected FortiGates.
Top memory usage	Displays FortiGates with the top memory usage.
Reports utilization	Shows a summary of the utilization of analytic reports.
Configuration backups	Shows status of FortiGate configuration backups.
Automation status	Shows number of configured automation stitches and trigger counts.

Network

Widget	Description
Management connectivity health	Displays tunnel uptime and the number of FortiGates that are online and offline.
Fabric device overview	Displays the platforms for the Fortinet Security Fabric devices connected to FortiGate Cloud 25.1.a Portal (Beta).
Analytics connectivity	Displays the status of the Analytics services.

Security

Widget	Description
FortiSandbox Cloud status	Displays the database versions and last updated dates for the dynamic malware and URL threat databases.
Top FortiSandbox files	Displays the most commonly analyzed file types in the last 24 hours of scanning.
FortiSandbox scan results	Shows the last seven days of results and their risk levels.
Compromised hosts	Displays compromised hosts data from the devices with Premium Subscription.
FortiGuard security alerts	Displays FortiGuard security alert information and schedule upgrades for FortiGates susceptible to critical vulnerabilities.



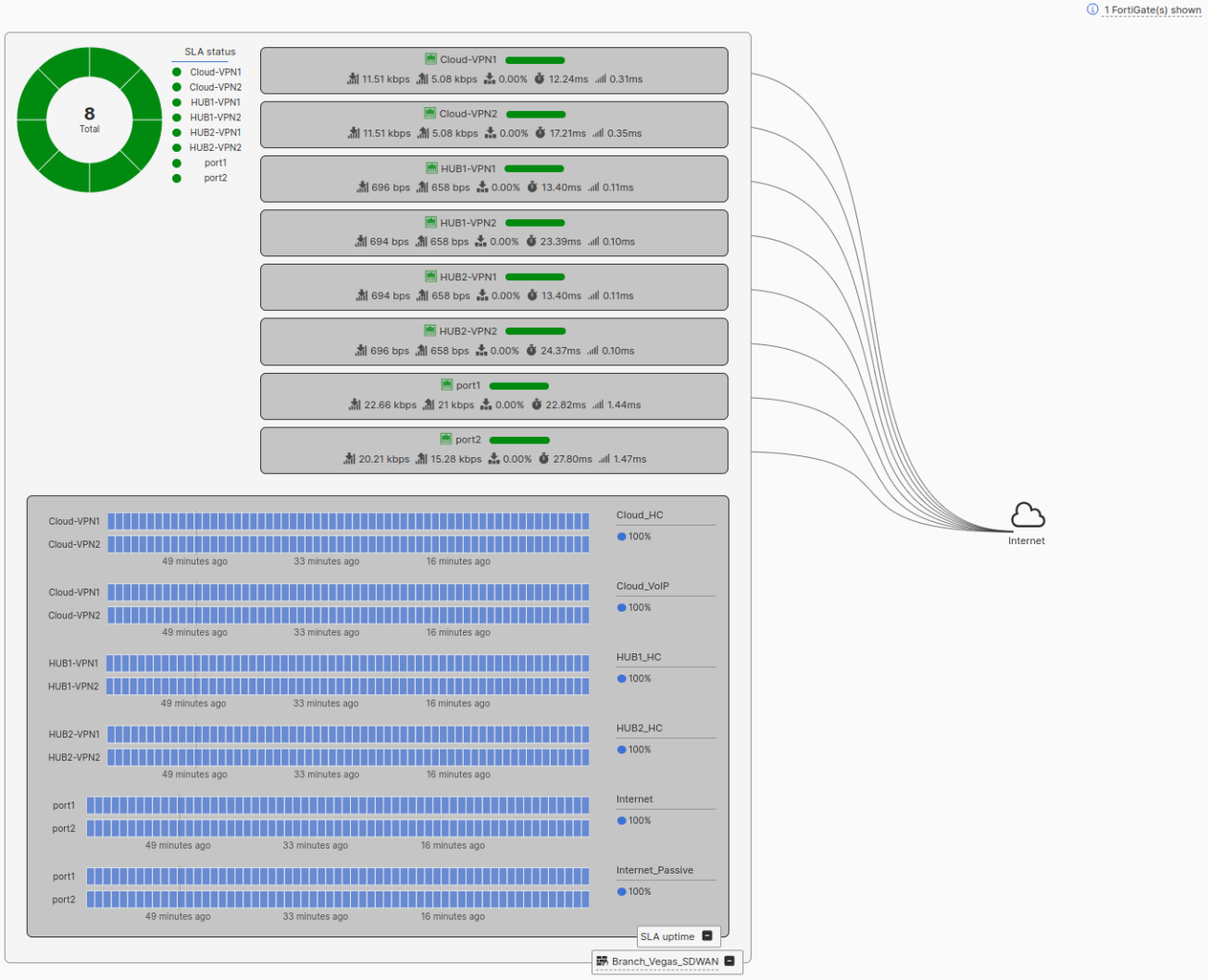
SD-WAN

The widgets on this dashboard only display information for FortiGates with a premium subscription.

Widget	Description
SD-WAN interfaces	Displays SD-WAN interface statistics.
SD-WAN performance SLA - all FortiGates	Displays SD-WAN performance SLA status across all FortiGates with a premium subscription.
SD-WAN QoE	Displays SD-WAN quality of experience status.
SD-WAN performance SLA	Displays SD-WAN performance SLA status.

Widget	Description
SD-WAN utilization by rule	Sankey chart to visualize traffic flows from rules to applications and SD-WAN members.
SD-WAN utilization by application	Bar chart to visualize most used applications for each SD-WAN member.
SD-WAN speed test results	View SD-WAN speed test results within a specified seven-day range.

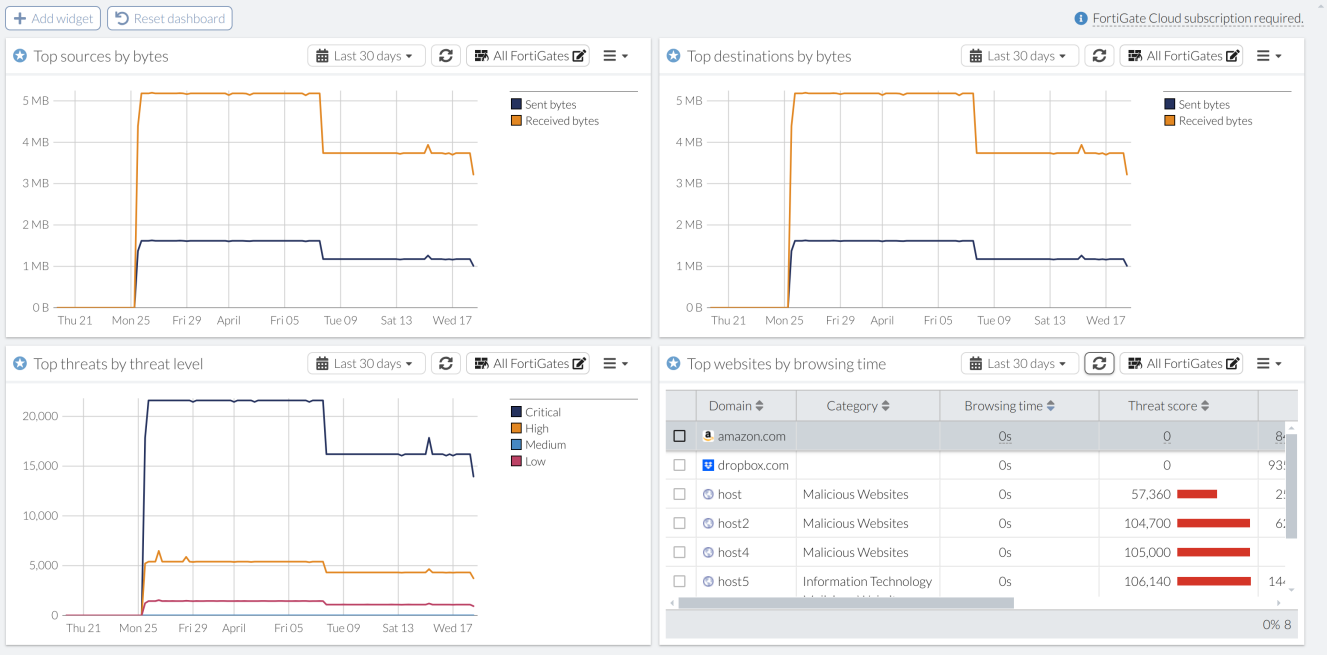
Dashboard also contains an SD-WAN Underlay Monitor, where you can access SD-WAN underlay bandwidth information and quality monitoring.



FortiView

The widgets on this dashboard only display information for FortiGates with a premium subscription.

Widget	Description
Top sources	Top traffic sessions aggregated by source.
Top destinations	Top traffic sessions aggregated by destinations.
Top threats	Top traffic sessions aggregated by threats.
Top websites	Top traffic sessions aggregated by websites.
Top Attacks	Counts the attacks that the device's IPS most frequently prevents.
Top Applications	Compares which applications are most frequently used, based on the device's Application Control settings.
Top Application Categories	Compares which application categories are most frequently used, based on the device's Application Control settings.
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.
Top DLP By Rules	Counts the DLP events that the device detects, sorted by DLP rule.
Top Spam	Displays which sources send the most spam email into the network.
Top Virus	Counts the viruses that the device's AV most frequently finds.
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
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.
Top Web Categories	Compares which web filtering categories are most frequently used, based on the device's Web Filtering settings.



User

The widgets on this dashboard only display information for users.

Widget	Description
Risk Website Visitors	?
Malware Victims	?
Malware Targets	?
Spam Targets	?
View data rule violators	?
Risk Application Users	?
Attack Targets	?
Intrusion Targets	?

Assets

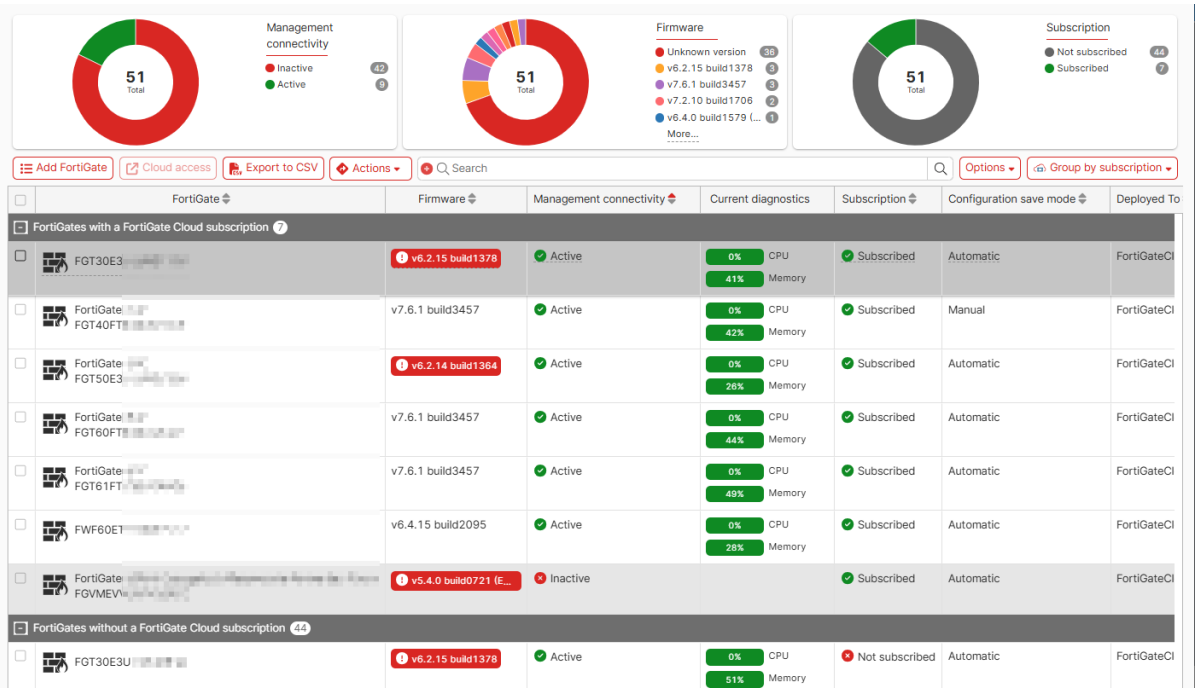
Assets > *Asset list* displays a centralized inventory of all FortiGate and FortiWifi devices from all FortiGate Cloud 25.1.a Portal (Beta) instances in a domain group. For example, if you access *Assets* from the Europe region, you see the region of a connected FortiGate Cloud 25.1.a Portal (Beta) instance from the Europe region.

For instructions on deploying a FortiGate to FortiGate Cloud 25.1.a Portal (Beta), see Cloud provisioning on page 26.

You can view the device CPU and memory usage under the *Current diagnostics* column. The *Asset list* page provides the following information about devices. *Asset list* displays the following device information, among others:

- Serial number
- Fortinet product type
- Firmware version
- Management connectivity status (If the device is connected through a management tunnel)
- Current diagnostics (device CPU and memory usage)
- Subscription status
- Configuration save mode. See Using configuration save mode.
- Last log upload time

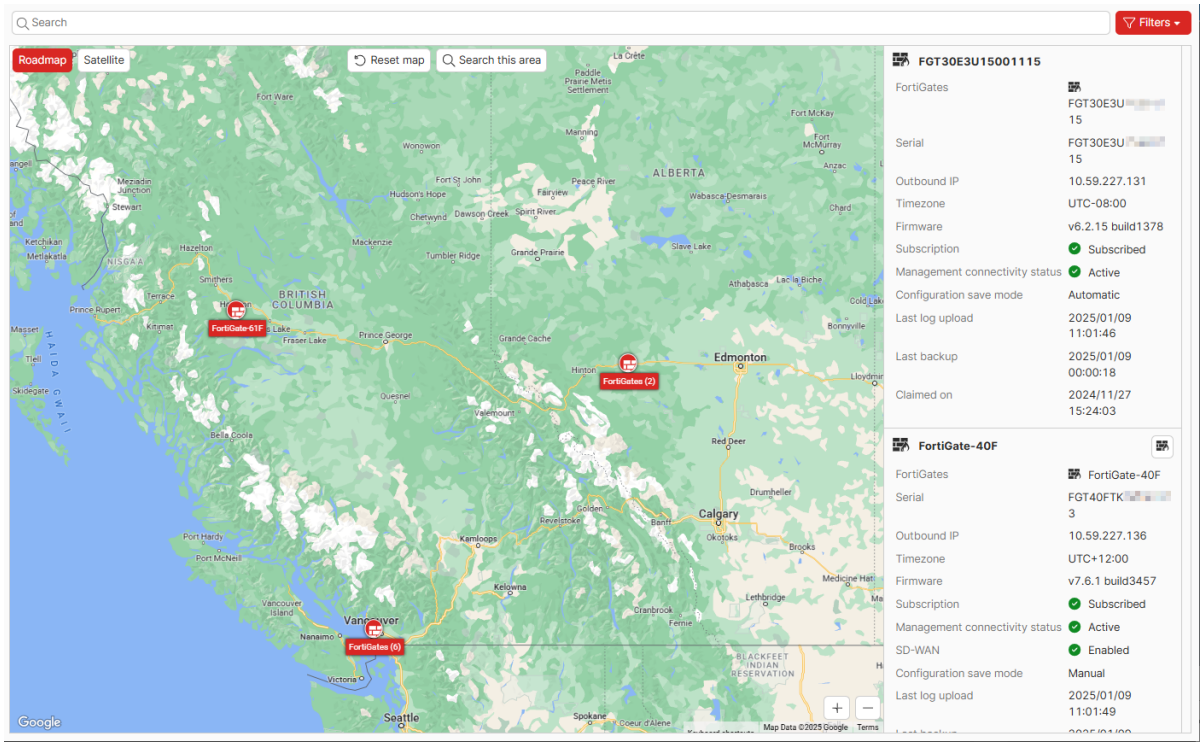
You can use the dropdown list on the right to view FortiGates grouped by subscription status or high availability cluster, or with no grouping. In the example, *Group by subscription* is selected. FortiGate Cloud 25.1.a Portal (Beta) displays the list of FortiGates separated into two groups: FortiGates with a premium subscription and FortiGates without a subscription.



To view historical diagnostics data for a device:

1. Go to *Assets* > *Asset list*.
2. Right-click the desired device, then select *View diagnostics*. FortiGate Cloud 25.1.a Portal (Beta) displays historical diagnostics data for the device.

You can select go to *Assets* > *Asset map* to view the device list as a map. This allows you to see the geographic location of the deployed devices. The right panel displays a list of FortiGates that includes similar information as you can find in *Asset list*. You can click the *Locate on map* icon for each device to zoom in to the device's location on the map. You can zoom in and out on the map using the + and - buttons in the lower right corner of the map. To return the map to the global view, click *Reset map*. For devices with a subscription, you can update their geolocation by dragging the device icon to the desired location on the map.



Cloud provisioning

Cloud provisioning or deployment is the mechanism to connect a FortiGate to FortiGate Cloud 25.1.a Portal (Beta) and configure it for cloud management and logging. You can provision a FortiGate to FortiGate Cloud 25.1.a Portal (Beta) using one of the following methods:

- FortiCloud key
- FortiCloud inventory
- FortiOS GUI

After provisioning a FortiGate to FortiGate Cloud 25.1.a Portal (Beta) 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 25.1.a Portal (Beta) using your FortiCloud account.

For FortiGates that are part of a high availability (HA) pair, you must activate FortiGate Cloud 25.1.a Portal (Beta) on the primary FortiGate. Activate FortiGate Cloud 25.1.a Portal (Beta) on the primary FortiGate as To provision a FortiGate or FortiWifi to FortiGate Cloud 25.1.a Portal (Beta) in the FortiOS GUI: on page 27 describes. FortiGate Cloud 25.1.a Portal (Beta) activation on the primary FortiGate activates FortiGate Cloud 25.1.a Portal (Beta) on the secondary FortiGate. Local FortiGate Cloud 25.1.a Portal (Beta) activation on the secondary FortiGate will fail.

To provision a FortiGate/FortiWifi to FortiGate Cloud 25.1.a Portal (Beta) using the FortiCloud key:

1. Log in to the FortiGate Cloud 25.1.a Portal (Beta).
2. Go to *Assets* > *Asset list*, then click *Add FortiGate*.
3. Click *Import FortiGate*.
4. In the *FortiCloud or FortiDeploy key* field, enter your key value.
5. For *End user type*, select *A non-government user* or *A government user* as required.
6. From the *Partner* dropdown list, select the affiliated Fortinet partner.
7. To provision your FortiGate to FortiGate Cloud 25.1.a Portal (Beta) after import, enable *Provision after import*.
8. Click *OK*.

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

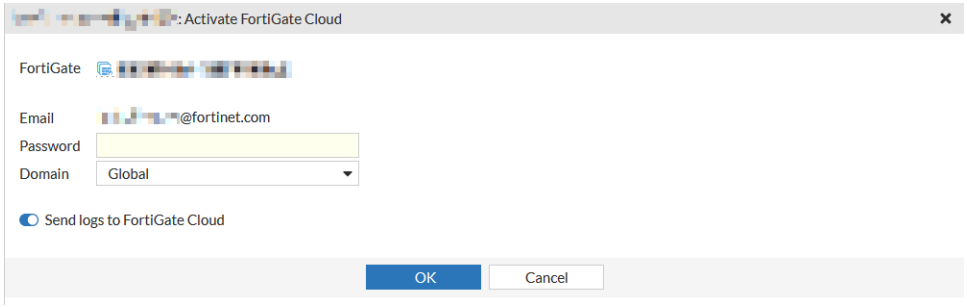
To provision a FortiGate or FortiWifi to FortiGate Cloud 25.1.a Portal (Beta) using the inventory:

1. Log in to the FortiGate Cloud 25.1.a Portal (Beta).
2. Go to *Assets* > *Asset list*, then click *Add FortiGate*. Do one of the following:
3. Select the desired device from the displayed inventory. This displays all assets from the logged-in FortiCloud account. Click *Provision* > *Provision to FortiGate Cloud*.
4. From the *Select Display Timezone for Device* dropdown list, select the desired time zone.
5. Click *Submit*.

To provision a FortiGate or FortiWifi to FortiGate Cloud 25.1.a Portal (Beta) 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, in the *Dashboard*, in the FortiGate Cloud widget, the *Status* displays as *Not Activated*. Click *Not Activated*.
3. Click the *Activate* button.
4. In the *Activate FortiGate Cloud* panel, the *Email* field is already populated with the FortiCloud account that this FortiGate is registered to.
5. In the *Password* field, enter the password associated with the FortiCloud account.

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



7. This should have automatically enabled *Cloud Logging*. Ensure that *Cloud Logging* was enabled. If it was not enabled, go to *Security Fabric* > *Fabric Connectors* > *Cloud Logging*, enable it, then set *Type* to FortiGate Cloud.
8. You must set the central management setting to FortiCloud, as this is the initial requirement for enabling device management features.

To configure a FortiGate-VM for FortiGate Cloud 25.1.a Portal (Beta):

FortiGate-VMs require additional configuration to ensure that they function with FortiGate Cloud 25.1.a Portal (Beta). Run the following commands in the FortiOS CLI:

```
config system fortiguard
   unset update-server-location
end
```

Accessing a FortiGate

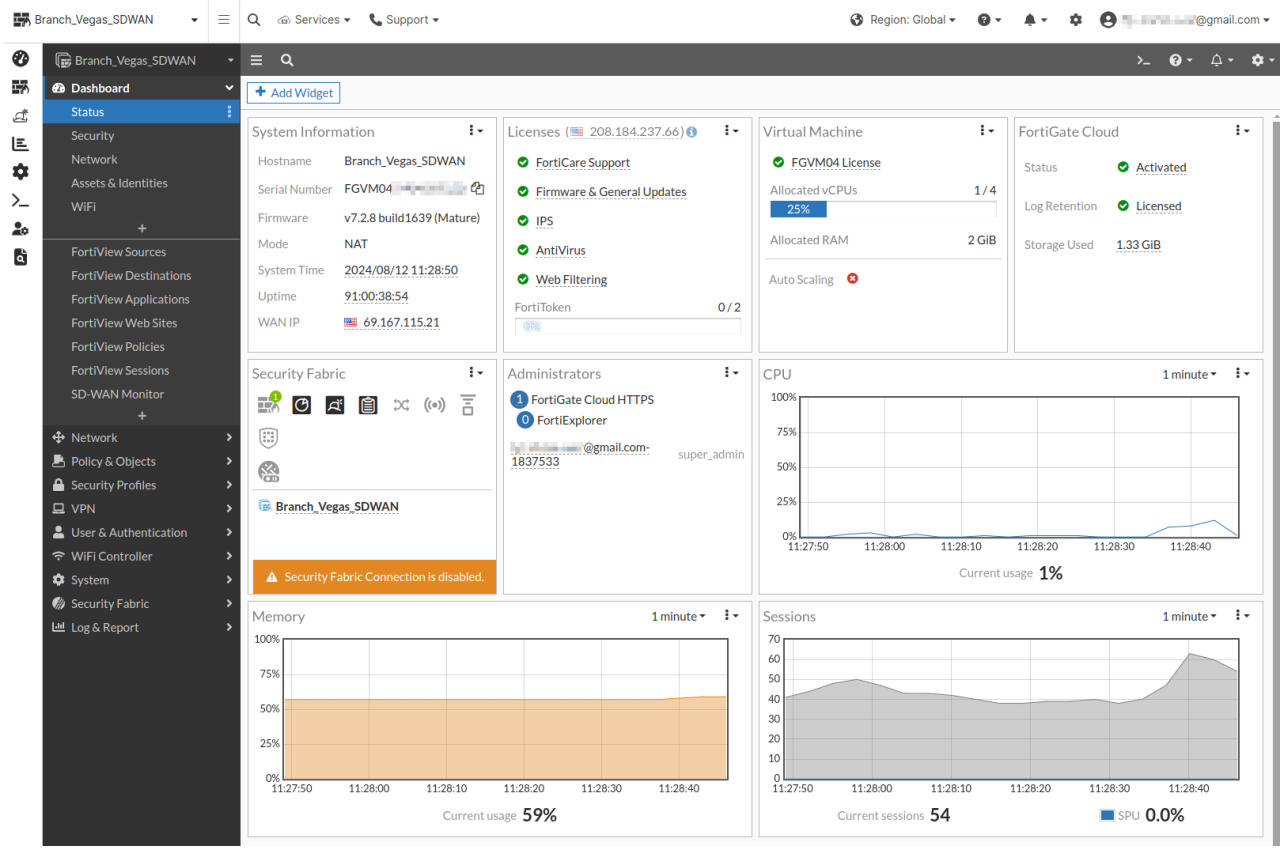
You can access the remote device's management interface to configure major features as if you were accessing the device itself. For configuration option descriptions, see the FortiOS documentation.

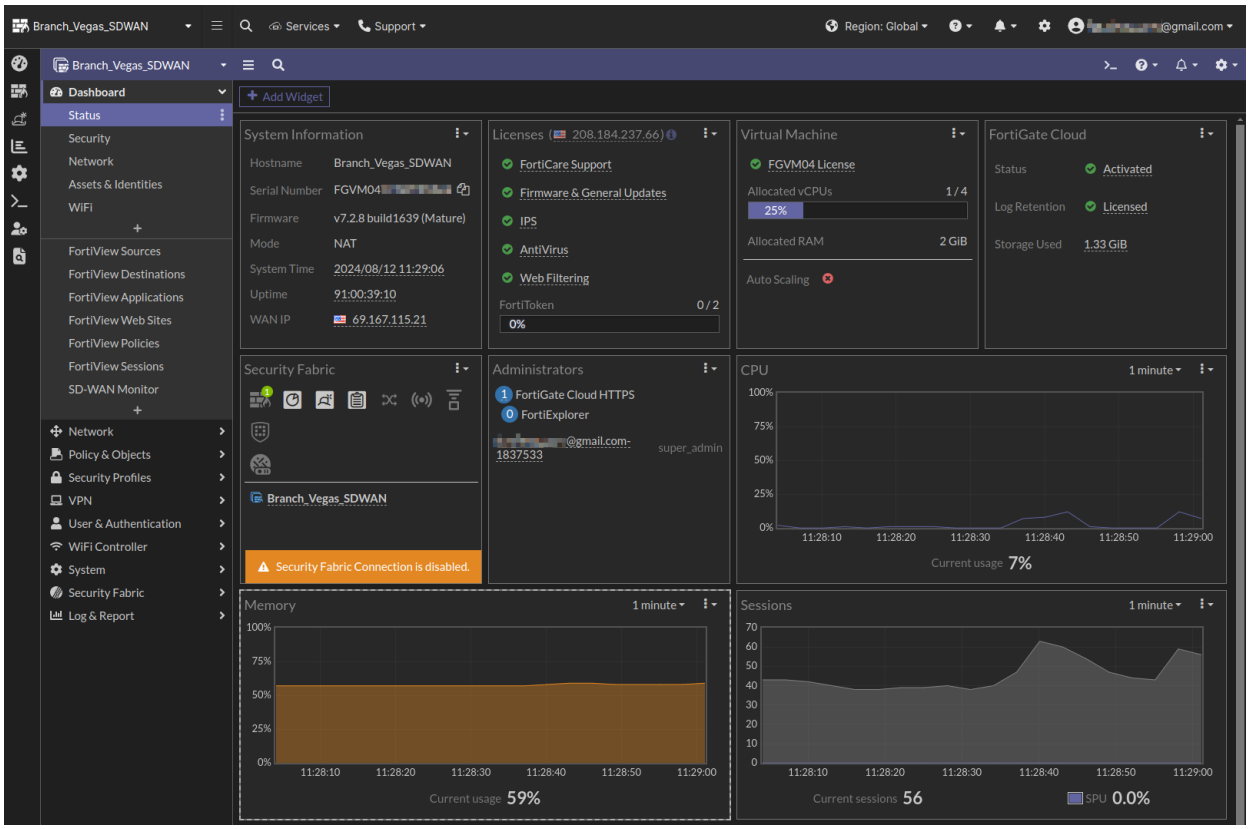
For devices with a subscription that are upgraded to FortiOS 7.0.2 or a later version, you have full access to configure features. For devices without a subscription, you have a read-only view of the configuration.

To remotely access and configure a FortiGate:

1. Do one of the following:
   - In the upper left corner, click the *FortiGate Cloud* dropdown list and select the desired FortiGate.

   - Go to *Assets* > *Asset list*. Select the desired FortiGate, then click *Cloud access*.
2. If the FortiGate does not have a subscription, FortiGate Cloud 25.1.a Portal (Beta) displays a warning that you will have read-only access. Click *OK*.
3. FortiGate Cloud 25.1.a Portal (Beta) displays the FortiOS interface in the current browser window. You do not need to enter credentials to log in to the FortiGate. View and make changes as desired. The following shows the FortiOS GUI as shown in FortiGate Cloud 25.1.a Portal (Beta), in light and dark modes:





4. Return to FortiGate Cloud 25.1.a Portal (Beta) using the icons on the left pane.

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 25.1.a Portal (Beta) Analytics considers suspicious change depending on the current threat climate and other factors.

The FortiGate Cloud 25.1.a Portal (Beta) 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.

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.

The FortiSandbox SaaS feature allows the following file upload sources:

- File uploads from FortiGate:
  - For a FortiGate without a FortiSandbox SaaS subscription (see License types), FortiSandbox SaaS supports up to 100 uploads per day or two uploads per minute.
  - For FortiGates with a FortiSandbox SaaS subscription, the below upload limits apply:

FortiGate model	Per minute	Per day
FortiGate 30-90/VM00	5	7 200
FortiGate 100-400/VM01	10	14 400
FortiGate 500-900/VM02, VM04	20	28 880
FortiGate 1000-2000/VM08, VM16	50	72 000
FortiGate 3000/VM32 and higher models	100	144 000

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

To set up Sandbox:

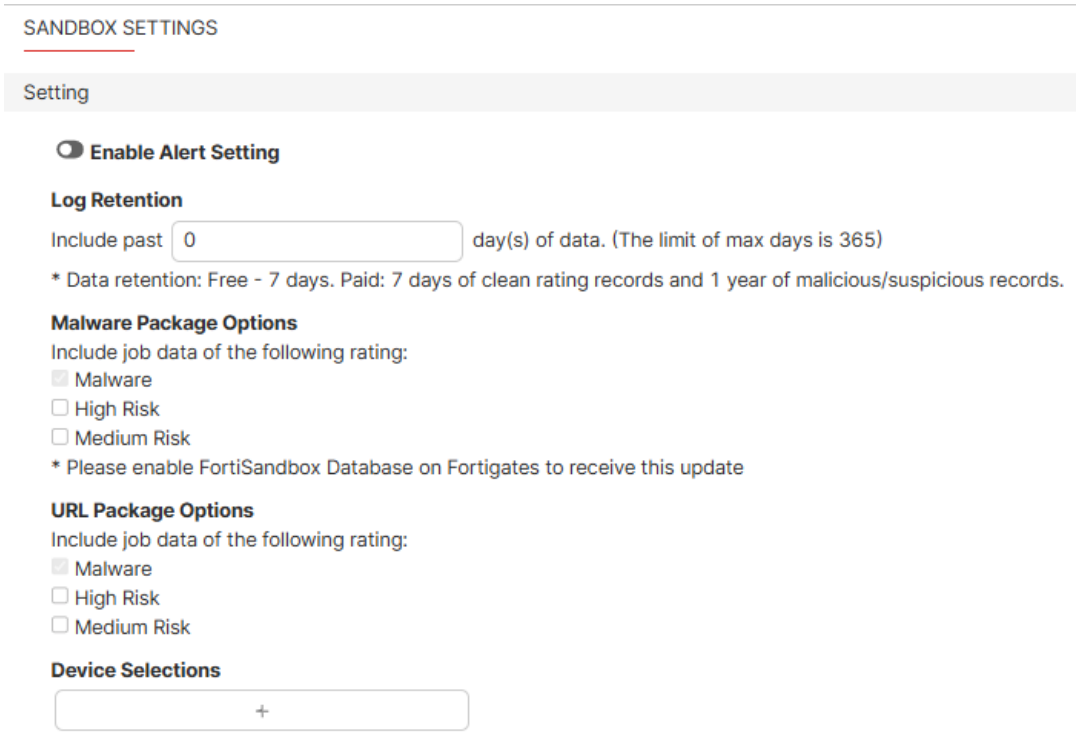
1. Complete the FortiGate Cloud Sandbox steps.
2. In *Security Profiles* > *AntiVirus*, create a profile that has *Send files to FortiSandbox Cloud for inspection* configured.
3. Create a firewall policy with logging enabled that uses the Sandbox-enabled AV profile.

4. Once devices have uploaded some files to FortiSandbox SaaS, log in to the FortiGate Cloud 25.1.a Portal (Beta) to see the results.

To upload a sample to Sandbox:

1. Go to *Sandbox* > *Scan Results*.
2. Click *Upload Sample*.
3. Browse to and select a file to upload, then click *Submit*. Once analysis completes, *Scan Results* displays the results.

Settings



In *Settings* > *Sandbox Settings*, you can configure FortiSandbox SaaS settings:

Setting	Description
Enable Alert Setting	• Enable alert emails • Enter multiple email addresses (separated by commas) to receive alerts • Set which severity levels trigger FortiGate Cloud 25.1.a Portal (Beta) to send alert emails
Log Retention	Set number of days to retain log data.

Setting	Description
Malware Package Options	Select the data risk level that is automatically submitted to FortiGuard to further antithreat research.
URL Package Options	
Device Selections	Select the desired FortiGates to enable Sandbox detection for.

If multitenancy is enabled, you can also configure the target subaccount to apply Sandbox settings to. You can also choose to apply the Sandbox settings to all lower-level subaccounts of that subaccount, or not.

To configure Sandbox alert emails:

1. Go to *Settings* > *Sandbox Setting*.
2. Select *Enable Alert Setting*.
3. Enter email addresses into the list to contact in the event of a Sandbox alert.
4. Select the severity levels to trigger an alert.
5. Click *Apply*.

Analytics

Analytics provide tools for monitoring and logging your device's traffic, providing you centralized oversight of traffic and security events. You can generate and view reports of specific traffic data. You can configure FortiGate Cloud 25.1.a Portal (Beta) to generate reports at scheduled times and run reports on-demand as desired.

Reports

To schedule a report:

1. Go to *Analytics* > *Scheduled reports*.
2. Select the desired report.
3. Click *Customize*.
4. In the *Select FortiGate* field, select the desired FortiGates to run the report for.
5. For *Status*, select *Enabled*.
6. If desired, in *Custom report logo*, upload an image as the custom logo for the report.
7. In the *Schedule type* field, configure the desired schedule for the report.
8. If desired, enable *Send report to* and select an email address to email group to send the report to.
9. Click *OK*. FortiGate Cloud 25.1.a Portal (Beta) generates the report as per the configured schedule. You can view these reports in *Analytics* > *Generated reports*.

To run a report on-demand:

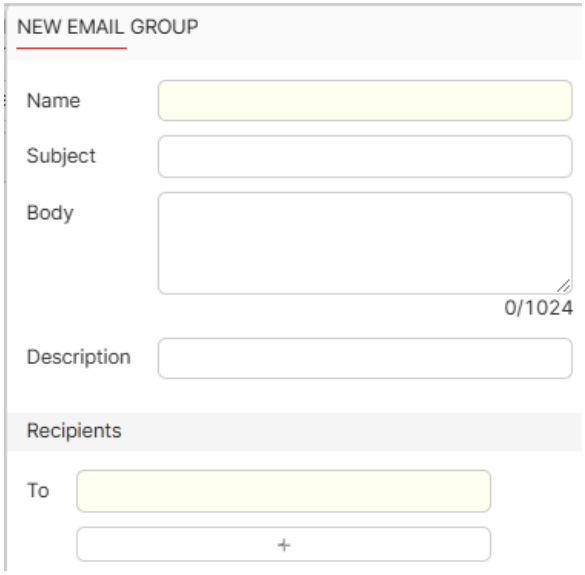
1. Go to *Analytics* > *Scheduled reports*.
2. Select the desired report, then click *Run report*.
3. In the *Select FortiGate* field, select the desired FortiGates to run the report for.
4. In the *Start time* and *End time* fields, configure the desired time range to include in the report.
5. If desired, enable *Send report to* and select an email address to email group to send the report to.
6. Click *OK*. FortiGate Cloud 25.1.a Portal (Beta) generates the report. You can view these reports in *Analytics* > *Generated reports*.

To customize a report:

1. Go to *Analytics* > *Scheduled reports*.
2. Select a report in the *Scheduled reports* table.
3. Click *Customize* button.
4. Customize report settings in the *Customize schedule* pane.
5. Once customization is complete, click *OK* to save settings.

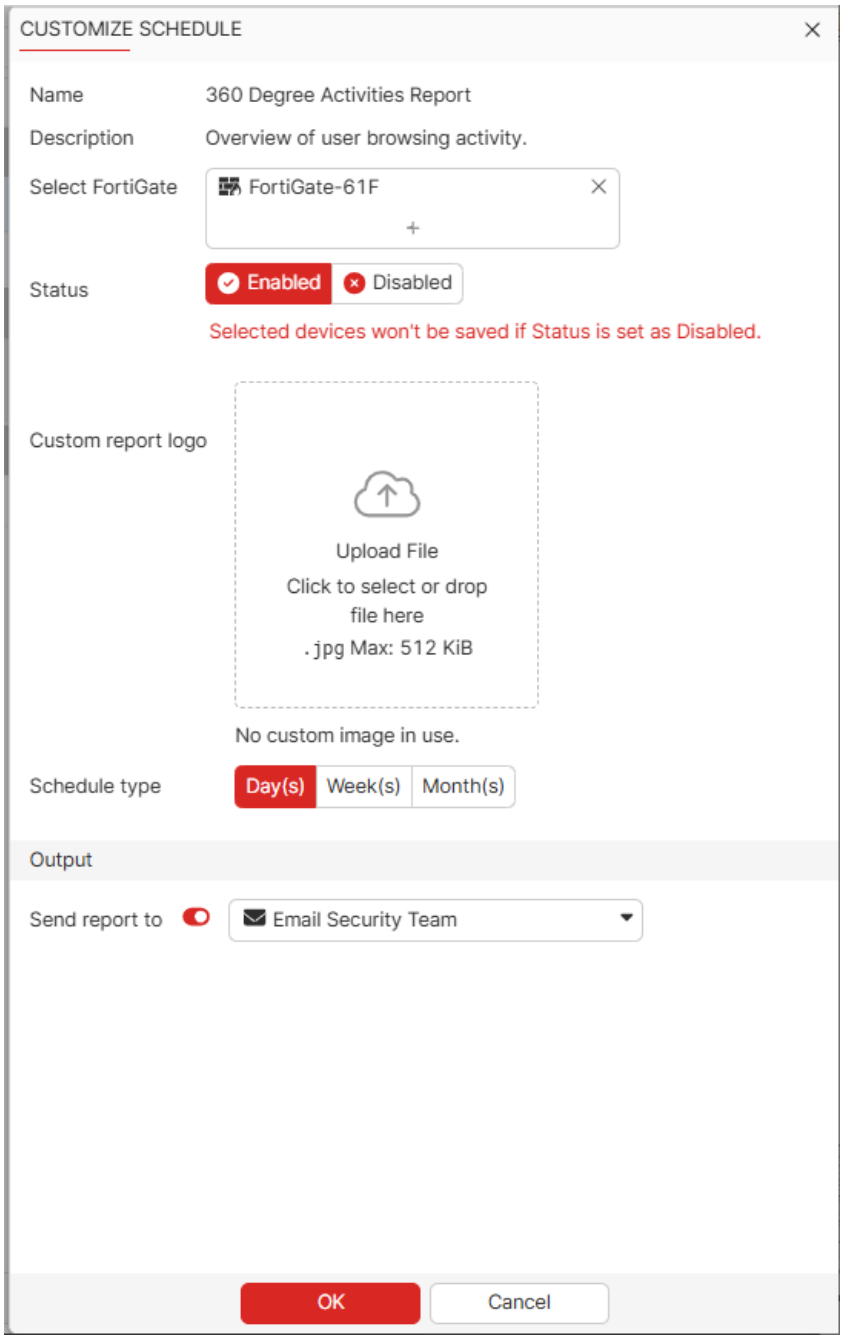
To configure an email group to send a report to:

1. Create an email group:
   a. Go to *Analytics* > *Scheduled reports*.
   b. Click *Manage email groups*.
   c. Click *Create*.
   d. In the *Name* field, enter the email group name.
   e. In the *Subject* field, enter the email subject line.
   f. In the *Body* field, enter the email body content.
   g. In the *Description* field, enter the email description.
   h. In the *To* field, enter the email addresses to send the email to.



   i. Click *OK*.
2. Select the desired report, then click *Customize*.

3. Enable the *Send report to* toggle. From the *Send report to* dropdown list, select the desired email group.



4. Click *OK*.

Reports reference

The following provides descriptions of report templates:

Reports for FortiGates without a paid subscription

The 360 Degree Activities Report is the only report available for FortiGates without a paid subscription. It is a general activities report on all FortiGates without a paid subscription. You cannot customize or schedule this report. FortiGate Cloud 25.1.a Portal (Beta) automatically runs this report weekly.

Reports for FortiGates with a premium subscription

You can configure a maximum of ten report templates for FortiGates with a premium subscription. The following lists all available report templates:

- 360 Degree Activities Report
- 360-Degree Security Review
- 360 Protection Report
- Admin and System Events Report
- Application Risk and Control
- Bandwidth and Applications Report
- Cyber-Bullying Indicators Report
- Cyber Threat Assessment
- Daily Summary Report
- Detailed Application Usage and Risk
- DNS Report
- DNS Security Report
- High Bandwidth Application Usage
- PCI DSS Compliance Review
- SaaS Application Usage Report
- Secure SD-WAN Assessment Report
- Secure SD-WAN Report
- Security Analysis
- Security Events and Incidents Summary
- Self-Harm and Risk Indicators Report
- Threat Report
- Top 20 Categories and Applications (Bandwidth)
- Top 20 Categories and Applications (Session)
- Top 20 Category and Websites (Bandwidth)
- Top 20 Category and Websites (Session)
- Top 500 Sessions by Bandwidth
- User Detailed Browsing Log
- User Security Analysis
- User Top 500 Websites by Bandwidth
- VPN Report
- Web Usage Report
- What is New Report

Logs

In *Logs*, you can view and download FortiOS traffic, security, and event logs. You can use the dropdown list on the upper right corner to select the desired FortiGate(s), and the time dropdown list to filter data for the desired time period. You can also use the log category dropdown list to filter data for the desired log category.

The following provides a list of the available log types and subtypes:

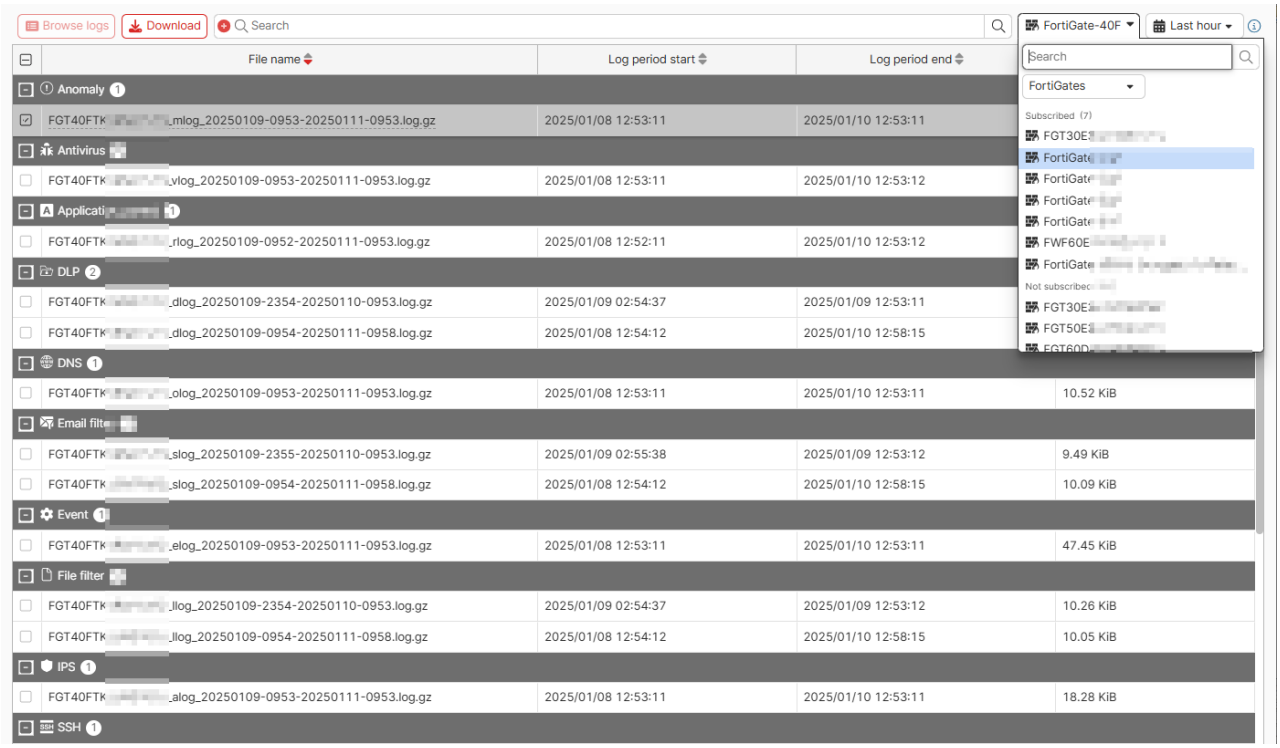
- Traffic:
  - Forward traffic
  - Local traffic
  - Multicast traffic
  - Sniffer traffic
  - ZTNA traffic
- Security:
  - Anomaly
  - Anti-spam
  - Antivirus
  - Application control
  - Data loss prevention
  - DNS query
  - File filter
  - Intrusion prevention
  - SSH
  - SSL
  - VoIP
  - Web application firewall
  - Web filter
- Events:
  - CIFS events
  - Endpoint events
  - General system events
  - HA events
  - Router events
  - SD-WAN events
  - SDN connector events
  - Security rating events
  - User events
  - VPN
  - Web proxy events
  - WiFi events

To download a log:

1. Go to *Analytics* > *LOG ARCHIVES* > *Raw logs*.
2. Select the desired logs.
3. Click *Download*. The log downloads to your device.

To browse raw logs:

1. 1. Go to *Analytics* > *LOG ARCHIVES* > *Raw logs*.
2. 2. Select a subscription FortiGate from the dropdown list on the right, then select the desired log file.
3. 3. Click *Browse logs*.



Configuration

In *Configuration* > *Revisions*, you can manage FortiGate revisions. This feature is only available for FortiGates with a premium subscription. For a FortiGate with a premium subscription, *Configuration* > *Revisions* displays the number of revisions and last backup time.

You can click a FortiGate, then click *Manage revisions* to view detailed revision history for that FortiGate.

To back up a configuration:

1. Go to *Configuration* > *Revisions*.
2. Click the desired FortiGate.
3. Click *Manage revisions*.
4. Click *Backup config*. FortiGate Cloud 25.1.a Portal (Beta) grays out this button if the current configuration on the FortiGate is already backed up.

To schedule an automatic backup:

1. Go to *Configuration* > *Revisions*.
2. Click the desired FortiGate.
3. Click *Manage revisions*.
4. Click *Schedule auto-backup*.
5. If automatic backup is disabled, click *Enable*.
6. For *Backup interval*, select *Session*, *Daily*, or *Weekly*.
7. (Optional) If you selected a daily or weekly interval, you can enable *Backup when config change*. If no configuration changed, FortiGate Cloud 25.1.a Portal (Beta) does not perform the daily or weekly backup.
8. (Optional) Enable *Backup mail notification*, and enter the desired email addresses to receive the notification. From the *Mail notification language* dropdown list, select the desired language of the email.
9. Click *OK*.

To compare revisions:

1. Go to *Configuration* > *Revisions*.
2. Click the desired FortiGate.
3. Click *Manage revisions*.
4. Select two revisions.
5. Click *Compare*. The *Revision comparison* panel shows the configuration differences between the two revisions.
6. Click *Close*.

To restore the device to a previous configuration:

1. Go to *Configuration* > *Revisions*.
2. Click the desired FortiGate.
3. Click *Manage revisions*.
4. Select a backup.

5. Click *Actions* > *Restore*.
6. Click *OK*. Your device reverts to the configuration revision of the selected backup.

CLI scripts

You can configure and schedule scripts of CLI commands to run on your FortiGates. For FortiOS CLI command information, see the FortiOS CLI Reference.

To create a script:

1. Go to *CLI scripts* > *Script list*.
2. Click *Create new*.
3. In the *CLI script* field, enter the desired FortiOS CLI commands to run on the FortiGates.
4. Configure other fields as desired, then click *OK*.

To run a script:

1. Go to *CLI scripts* > *Script list*. Select the desired script, then click *Run*.
2. In *FortiGates*, select the desired FortiGates.
3. In the *Execution schedule* toggle, select one of the following:
   - To run the script immediately, click *Immediate*.
   - To schedule the script to run at a desired time, select *Scheduled*. Configure the desired time to run the script. Click *OK*.

You can view and edit scheduled script runs in *CLI Scripts* > *Script tasks* > *Scheduled scripts*. You can view the script run results in *CLI scripts* > *Script tasks* > *Run results*.

Administration

In Administration, you can access *Automation*, *Firmware management*, and *User settings*.

Automation

In *Automation*, you can enable trigger-based automation for alerts and receive notifications.

To configure an event handler stitch:

1. Go to *Administration* > *Automation*.
2. On the *Actions* tab, click *Create new*.
3. Enable *Email*.
4. Configure the desired email addresses to send the notification from and to.
5. Configure other fields as desired, then click *OK*.
6. On the *Stitches* tab, click *Create new*.
7. Click *Add trigger*. From the *Select Entries* pane, select the desired event to send notifications for.
8. Click *Add action*. From the *Select Entries* pane, select the desired action to take.
9. Click *OK*. When the trigger occurs, FortiGate Cloud 25.1.a Portal (Beta) takes the configured action and sends notifications as configured.

To enable or disable a configured event handler stitch:

1. Go to *Administration Automation* > *Stitches* tab.
2. Right-click the desired automation stitch.
3. On the tooltip menu, click *Enable* or *Disable*.

To configure the Sandbox event handler stitch:

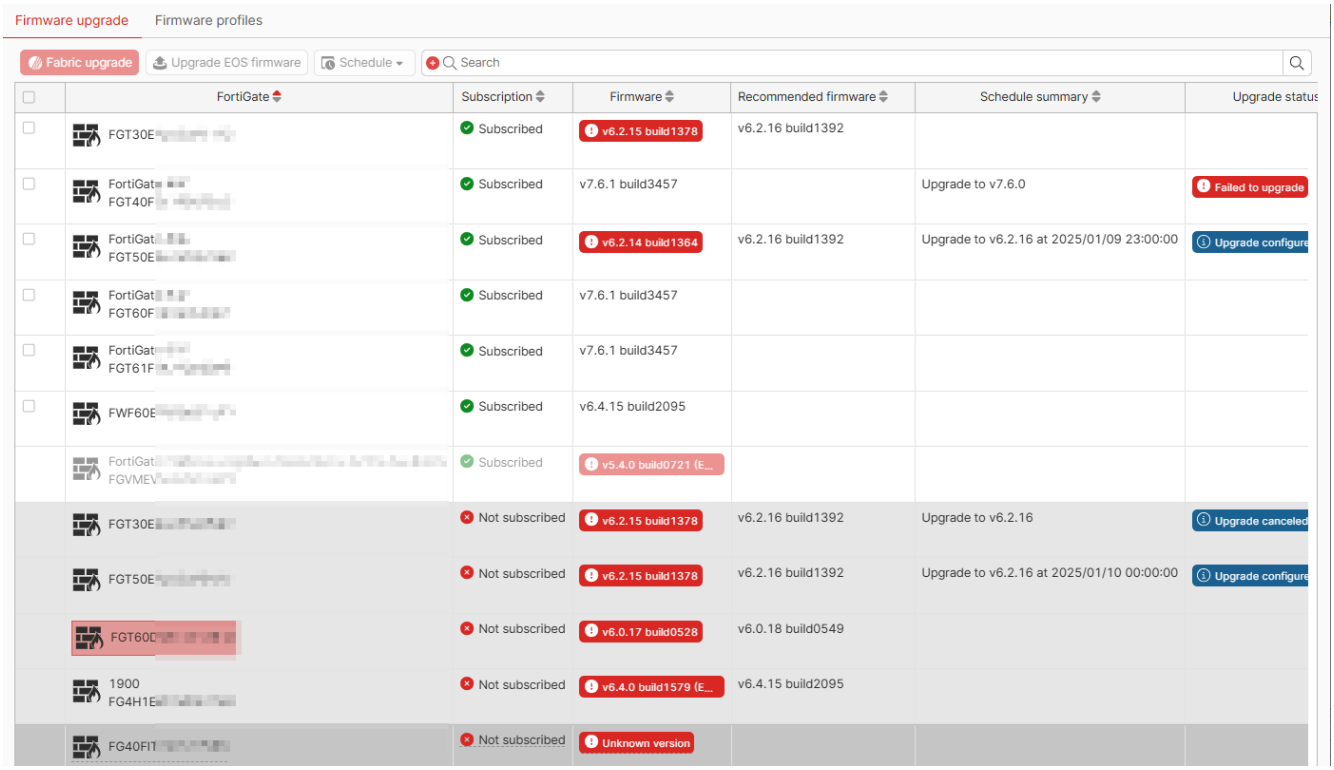
1. Go to *Administration* > *Automation*.
2. On the *Actions* tab, click *Create new*.
3. Configure the desired email addresses to send the notification from and to.
4. Configure other fields as desired, then click *OK*.
5. On the *Stitches* tab, edit the *Sandbox* stitch.
6. To configure email notifications, do the following:
   a. Enable *Email alert*.
   b. Configure the desired email addresses to send the notification from and to.
7. Under *Triggers*, enable the desired file types to send notifications for.
8. Click *OK*. When the trigger occurs, FortiGate Cloud 25.1.a Portal (Beta) takes the configured action and sends notifications as configured.

Firmware management

In 25.1.a, firmware profiles are only available for devices with a paid subscription.

Firmware management lists FortiGates deployed to FortiGate Cloud and groups FortiGates that belong to the same Fortinet Security Fabric. You can manage firmware upgrades in the *Firmware upgrade* tab. Firmware profiles allow you to easily control device firmware for multiple FortiGates with a subscription from one central interface and automate firmware upgrades.

FortiGates set to automatic patch upgrade perform firmware upgrades to the latest patch of the same major minor release version during the selected time.



When a new FortiOS patch becomes available, FortiGate Cloud 25.1.a Portal (Beta) sends an email to notify the user that they must upgrade the firmware within seven days of the release date of the patch for FortiGates running an older patch of that FortiOS version. For a FortiGate with a paid subscription, you can postpone the upgrade if desired. For a FortiGate without a paid subscription, if you do not upgrade it within seven days, it remains connected to FortiGate Cloud 25.1.a Portal (Beta) but cannot use any FortiGate Cloud 25.1.a Portal (Beta) features. It stops uploading logs to FortiGate Cloud 25.1.a Portal (Beta).

If a FortiGate without a paid subscription is not running the latest patch available of its FortiOS version when it initially connects to FortiGate Cloud, you must also upgrade it within seven days of the release date of the latest patch. If the latest patch was released more than seven days earlier, you must upgrade the FortiGate immediately. The FortiGate cannot use FortiGate Cloud 25.1.a Portal (Beta) features and does not upload logs to FortiGate Cloud until it is upgraded.

If the FortiOS version on a FortiGate reaches end of support, you must upgrade the FortiGate to the latest patch of a supported major release.

Updating to the latest patch is not required for the following devices:

- FortiGate that is a member of one of the following:
  - High availability cluster
  - Cooperative Security Fabric
- FortiGate that is running a special build (if the build number is greater than or equal to 8000)

To schedule a firmware upgrade:

1. Go to *Administration* > *Firmware management* > *Firmware upgrade*.
2. Select the desired FortiGates.
3. Click *Fabric upgrade*.
4. For *Upgrade schedule*, select *Immediate* or *Custom*. If you select *Custom*, configure the desired upgrade time.
5. Confirm that the dialog displays the desired firmware versions for each FortiGate. Click *OK*. FortiGate Cloud 25.1.a Portal (Beta) backs up the FortiGate configurations and upgrades the firmware as per the schedule that you configured. The upgrade reboots the FortiGates.

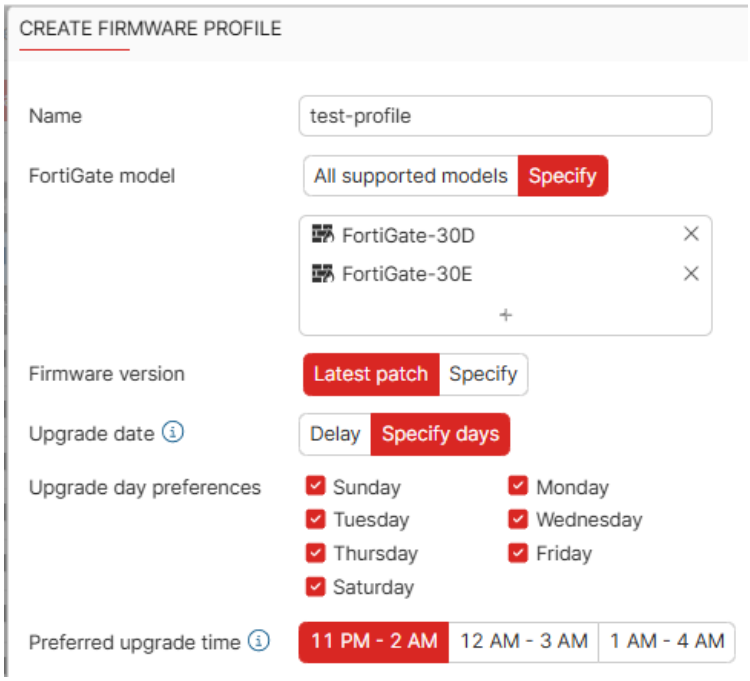
To upgrade EOS firmware:

1. Go to *Administration* > *Firmware management* > *Firmware upgrade*.
2. Select the desired FortiGates.
3. Click *Upgrade EOS firmware*. If the current firmware is at end of support (EOS), this upgrades it to a supported version.

To create a firmware profile:

1. Go to *Administration* > *Firmware management* > *Firmware profiles*.
2. Click *Create*.

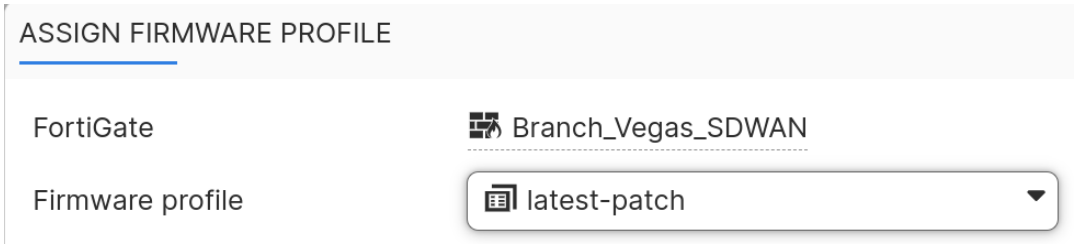
3. In the *Create firmware profile* slide-in, configure firmware profile settings.



4. Click *OK* to create firmware profile.

To assign a firmware profile

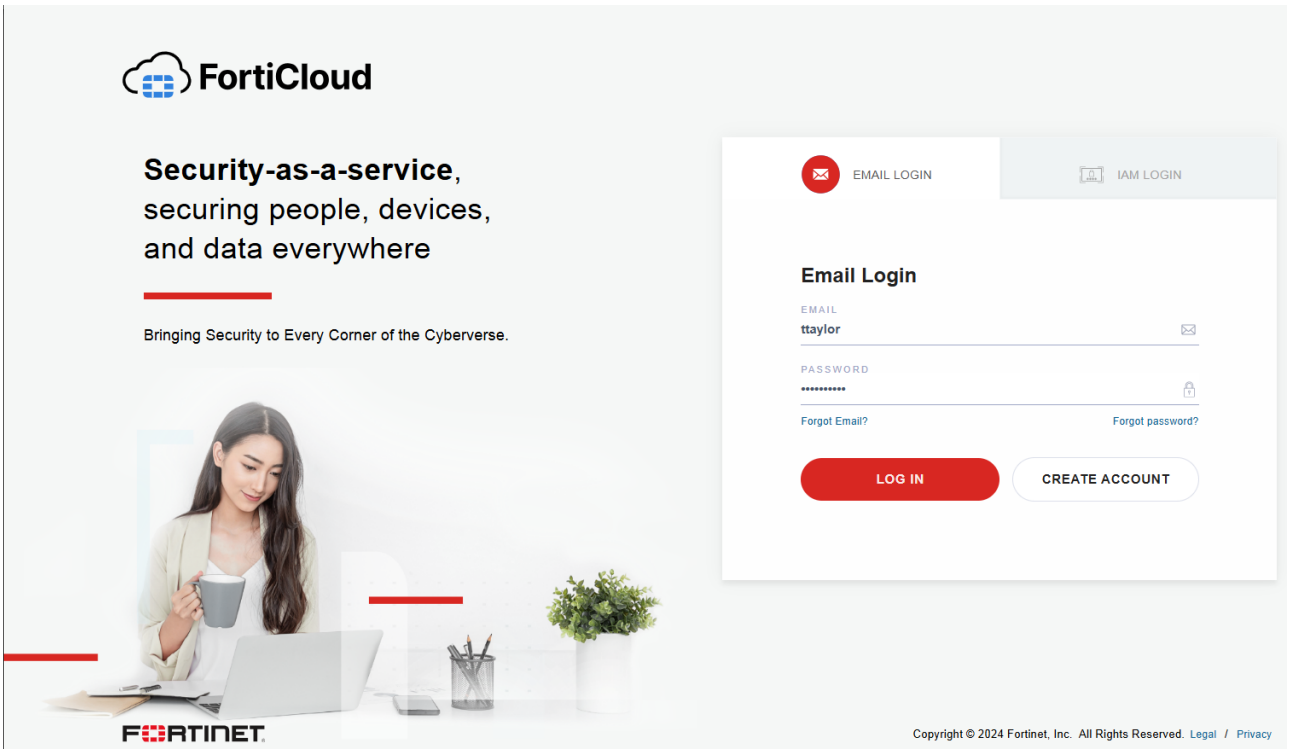
1. Go to *Administration* > *Firmware management* > *Firmware upgrade*.
2. Select device(s) and click *Assign firmware profile*.
3. On the *Assign firmware profile* slider-in, select the desired firmware profile.



4. Click *OK* to assign a firmware profile.

Accounts and users

FortiGate Cloud 25.1.a Portal (Beta) 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 25.1.a Portal (Beta) using their email ID as the username and the password that they chose when creating the account.



Creating an account

You can register a new FortiCloud account using the *Create account* button on the landing page.

User management

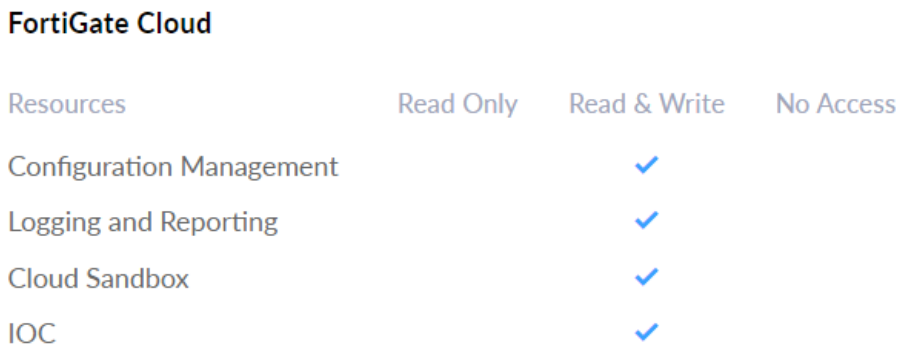
The primary user can add users to the account using the following methods:

User type	Method
Identity and Access Management (IAM) user	Add users to the FortiCloud account with role-based access control in FortiGate Cloud 25.1.a Portal (Beta) using the FortiCloud IAM service. See IAM users on page 47.

FortiGate Cloud 25.1.a Portal (Beta) 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 25.1.a Portal (Beta) using resource-based access control using FortiCloud permission profiles. When creating a permission profile in the IAM portal, you must add the FortiGate Cloud portal to the profile and configure the desired permissions.



For details on creating a permission profile in the IAM portal, see Creating a permission profile.

See Adding IAM users for details on configuring IAM users.

FortiCloud organizations

FortiGate Cloud 25.1.a Portal (Beta) supports organizational unit (OU) account selection and switching. See Organization Portal for details on creating an OU.

Creating an IAM user with OU scope

See User permissions.

User settings

You can add and manage users from *Administration* > *User settings*. *User settings* includes different user types, including Identity & Access Management (IAM) and FortiGate Cloud 25.1.a Portal (Beta) account users. *User settings* displays a key icon beside the primary account.

The *User settings* page contains the following columns:

Column	Description
Login ID	Email address that the user uses to log in to the FortiGate Cloud 25.1.a Portal (Beta). This column also displays the region that each user can access and their role.
Role	Displays the user role.
User Type	Displays the type of user. User types include the following: • **IAM**: see IAM users on page 47. • **API**: an API user only has the ability to call the FortiGate Cloud 25.1.a Portal (Beta) API. FortiCare manages API users and their access permissions. API users are subusers of the primary account. See API access. • **Third Party**: user who authenticates using an external identity provider (IdP). Configuring an external IdP requires FortiCare and FortiAuthenticator support.

Column	Description
Aliases	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 *Edit* icon in the *Action* column.
Status	Status of the user account. The status can be one of the following: • **Active**: user who has activated their account. • **Inactive**: user to whom an activation email has been sent, but has not activated their account yet.

For IAM and IdP users, they can only view their own account and edit their language settings on this page.

Audit

Audit > *Activities* displays a log of actions that users have performed on FortiGate Cloud 25.1.a Portal (Beta). 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	Account activities
Backup	• Backing up a device configuration • Downloading and disabling backups
Cloud access	Viewing and configuring a device via cloud access
Device deployment	• Deploying and undeploying devices • Deleting deployments
Log	Exporting logs
Report	Downloading, scheduling, and running reports
Sandbox	Uploading files to Sandbox for analysis
Script	Creating, editing, deleting, and deploying scripts
Upgrade	Scheduling and running upgrades

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

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 25.1.a Portal (Beta) on the primary FortiGate as To provision a FortiGate or FortiWifi to FortiGate Cloud 25.1.a Portal (Beta) in the FortiOS GUI: on page 27 describes. FortiGate Cloud 25.1.a Portal (Beta) activation on the primary FortiGate activates FortiGate Cloud 25.1.a Portal (Beta) on the secondary FortiGate. Local FortiGate Cloud 25.1.a Portal (Beta) activation on the secondary FortiGate will fail.
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 activate my FortiGate Cloud on HA-paired FortiGates?

Activate FortiGate Cloud 25.1.a Portal (Beta) on the primary FortiGate as To provision a FortiGate or FortiWifi to FortiGate Cloud 25.1.a Portal (Beta) in the FortiOS GUI: on page 27 describes. FortiGate Cloud 25.1.a Portal (Beta) activation on the primary FortiGate activates FortiGate Cloud 25.1.a Portal (Beta) on the secondary FortiGate. Local FortiGate Cloud 25.1.a Portal (Beta) activation on the secondary FortiGate will fail.

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?

Do one of the following:

- If you have not activated FortiGate Cloud 25.1.a Portal (Beta) in FortiOS for the first time, follow the steps in FortiCare and FortiGate Cloud login.
- Otherwise, if you have already activated FortiGate Cloud 25.1.a Portal (Beta), run the following commands in FortiOS to establish a connection manually:

```
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 provision a FortiGate or FortiWifi to FortiGate Cloud 25.1.a Portal (Beta) in the FortiOS GUI: on page 27 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 provision a FortiGate or FortiWifi to FortiGate Cloud 25.1.a Portal (Beta) in the FortiOS GUI: on page 27 describes instead. If you cannot connect to the FortiOS GUI, contact cs@fortinet.com to reenable 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 52. See Accessing a FortiGate on page 28.

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 provision a FortiGate/FortiWifi to FortiGate Cloud 25.1.a Portal (Beta) using the FortiCloud key: on page 27.
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 provision a FortiGate or FortiWifi to FortiGate Cloud 25.1.a Portal (Beta) in the FortiOS GUI: on page 27 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 a log: on page 39.

Why does the FortiGate Cloud server drop some logs from my FortiGate?

A FortiGate with implicit policy logging settings enabled uploads a large amount of redundant logs, causing processing delays and overloading on the log server. The amount of redundant logs uploaded can be large enough to block all log uploads from the FortiGate. Therefore, FortiGate Cloud drops logs matching the following conditions:

- `policyid=0`
- `sentbyte=0`
- `rcvdbyte=0`
- `no crscore`
- `subtype="local"`

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.

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.

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 schedule an automatic 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.

Why am I logging into the Premium Portal in one region and the Standard Portal in another?

Upgrading to the Premium Portal is done on a region-by-region basis. If your account meets the upgrade requirements in another region, you see the *Upgrade* button after logging in and can upgrade to the Premium Portal for that region.

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.

What should I do if I accidentally upgrade FortiOS to 7.4.2 or higher on a FortiGate without a FortiGate Cloud Service subscription and remote access to the device becomes read-only?

For the following FortiOS versions, the remote access feature requires a FortiGate Cloud Service subscription license on the FortiGate to have read and write access:

(missing or bad snippet)

If you are considering or in the process of purchasing the license, contact our Support team. They can apply a short-term trial license to your device to resolve the issue. Alternatively, you can access your FortiGate via its web interface. If you do not have access to the FortiGate's web interface, contact our Support team with a description of the situation.

After my FortiGate is transferred to another account in the Asset Management portal, do I still need to transfer it again in the FortiGate Cloud portal?

After a FortiGate is transferred from account A to B in the Asset Management portal, it is undeployed from account A with existing data retained under account A. The FortiGate will be available for deployment under the *FortiCare Inventory* tab of account B in the FortiGate Cloud portal.

Does FortiGate Cloud 25.1.a Portal (Beta) support data backups and disaster recovery?

FortiGate Cloud 25.1.a Portal (Beta) is ISO 27001- and SOC2-compliant and supports standard procedures for data backup, data redundancy, and disaster recovery.

What happens if you enable the automatic firmware upgrade feature on both FortiGate Cloud 25.1.a Portal (Beta) and the FortiGate?

The firmware profile assignment within FortiGate Cloud 25.1.a Portal (Beta) disables the local automatic firmware upgrade configuration on the FortiGate.

Can I disable the automatic firmware upgrade from FortiOS by logging in directly to the FortiGate that has no FortiGate Cloud 25.1.a Portal (Beta) subscription to bypass the automatic firmware upgrade enforcement from FortiGate Cloud 25.1.a Portal (Beta)?

In 25.1.a, FortiGate Cloud 25.1.a Portal (Beta) does not automatically upgrade devices without a FortiGate Cloud 25.1.a Portal (Beta) subscription to the latest patch. For devices without a subscription to continue using cloud features, you must manually upgrade the device to the latest patch, such as upgrading the device manually via FortiGate Cloud 25.1.a Portal (Beta) or by using the automatic firmware upgrade feature in FortiOS. If you do not upgrade the device to the latest patch, the device cannot use FortiGate Cloud 25.1.a Portal (Beta) features and stops uploading logs to FortiGate Cloud 25.1.a Portal (Beta).

For devices with a FortiGate Cloud 25.1.a Portal (Beta) subscription, automatic firmware upgrades using a firmware profile is available as an optional feature. If you have configured a firmware profile in FortiGate Cloud 25.1.a Portal (Beta) for a device, you do not need to disable the automatic firmware upgrade feature in FortiOS.

How can I activate FortiGate Cloud 25.1.a Portal (Beta) on a FortiGate provisioned to an OU placeholder account?

To activate FortiGate Cloud 25.1.a Portal (Beta), run the following in the CLI:

```
execute fortiguard-log join
```

To refresh the management tunnel connection, run the following in the CLI:

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

www.fortinet.com