FORTINET

Administration Guide

FortiGate Cloud Premium 24.1

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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

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

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

March 08, 2024
FortiGate Cloud Premium 24.1 Administration Guide
32-241-991318-20240308

TABLE OF CONTENTS

Change log

Date	Change description
2024-02-02	Initial release.
2024-03-08	Updated: • OU Asset list on page 12 • Logs on page 28

Introduction

FortiGate Cloud is a cloud-based software-as-a-service offering a range of management, reporting, and analytics for FortiGate next generation firewalls. FortiGate Cloud Premium is the latest version, which includes various user experience (UX) and feature enhancements.

FortiGate Cloud Premium is a redesigned version of FortiGate Cloud with enhanced UX and features. The cloud-based software-as-a-service offers configuration management for FortiGate(s), FortiGate VMs along with FortiGate-connected FortiAP(s), FortiSwitch(s), and FortiExtender(s). 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 exclusive 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 6. Features on page 6 includes the full list of FortiGate Cloud Premium features.

FortiGate Cloud Premium 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 environment to FortiGate Cloud Premium.

FortiGate Cloud Premium does not support multitenancy-enabled accounts.

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

Features

FortiGate Cloud Premium 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.

Requirements

You can only access FortiGate Cloud Premium by upgrading an existing FortiGate Cloud environment. Before upgrading to FortiGate Cloud Premium, you must upgrade all FortiGates with a subscription to FortiOS 7.0.2 or a later version. For eligibility requirements, see Upgrading to FortiGate Cloud Premium Portal (Beta).

Requirement	Description
FortiCloud account	Create a FortiCloud account if you do not have one. Launching FortiGate Cloud 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 account, merging your account to your FortiCloud account is recommended.

Requirement	Description
FortiGate/FortiWifi license	You must register all FortiGate/FortiWifi devices on FortiCloud.
FortiGate Cloud Premium Subscription	Purchase FortiGate Cloud Management, Analysis, and 1 Year Log Retention license for each device or VM. See License types on page 9.
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.

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.

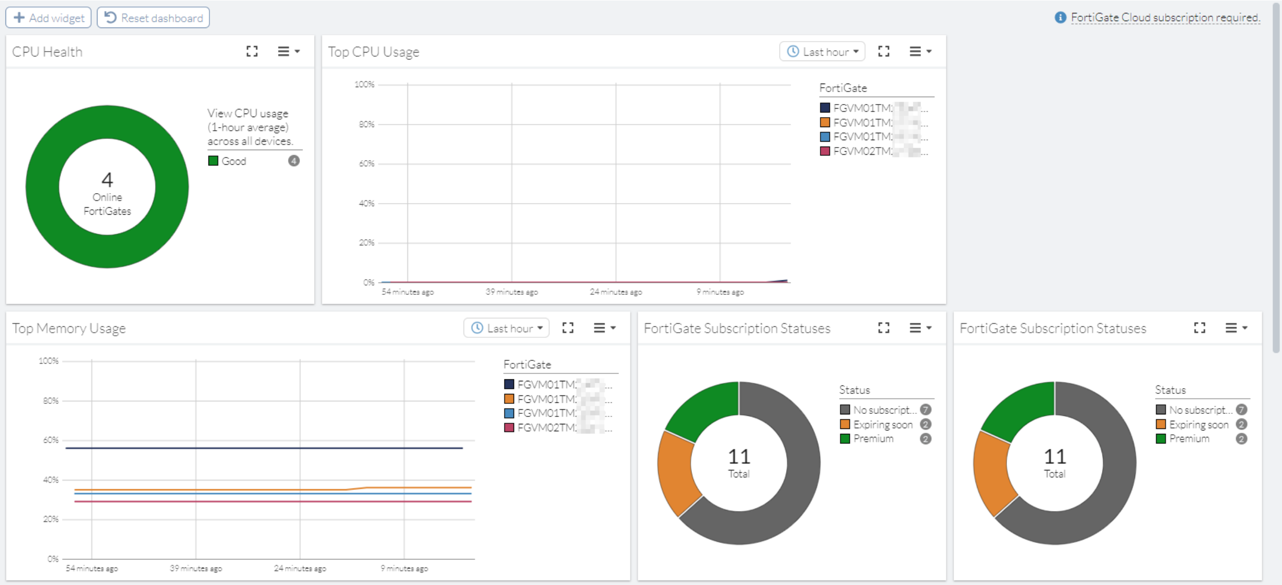
Purpose	Protocol	Port
Syslog, registration, quarantine, log, and report	TCP	443
OFTP	TCP	514
Management	TCP	541
Contract validation	TCP	443
Config portal	TCP	8443

Getting started with FortiGate Cloud Premium

After upgrading to FortiGate Cloud Premium, go to https://fortigate.forticloud.com to access FortiGate Cloud Premium.

After you log in, the FortiGate Cloud Premium portal displays the *Dashboard* > *Status* page. You can switch regions and access FortiGate Cloud Premium documentation from the ? icon on the FortiCloud banner at the top of the page.

The *Dashboard* > *Status* page displays a variety of widgets. The widgets provide information about the devices that your FortiGate Cloud Premium 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 21.
Menu icon	Use the menu icon to collapse or display the left pane, which displays other configuration options.
Services	Access another Fortinet service.
Support	Access Fortinet support options, such as contacting the Fortinet support team.
Region selection	Select another region to access FortiGate Cloud Premium in.
Documentation link	Access FortiGate Cloud documentation.
Preferences	Configure dark or light theme and the language to display FortiGate Cloud Premium in.
User menu dropdown	Displays the current logged in user. You can use the dropdown list to switch accounts or view account settings.

From the left pane, you can access other options including inventory, 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 Premium is managing.
Assets	View a centralized inventory of all FortiGate and FortiWifi devices. See Assets on page 18.

Option	Description
Sandbox	View the scan results from files that Sandbox submitted to FortiGuard for threat analysis. See Sandbox on page 23.
Analytics	Create and alter report configurations and their settings. These report configurations are available for all deployed devices. See Analytics on page 24.
Configuration	Manage FortiGate Cloud Premium account and Sandbox settings. See Configuration on page 30.
CLI Scripts	Configure and schedule scripts of CLI commands to run on your FortiGates. See CLI scripts on page 31.
Administration	Configure automation and firmware management options. See Administration on page 32.

The FortiGate Cloud Premium landing page also offers the option of accessing a demo site, from which you can experience the benefits of FortiGate Cloud Premium without registering for an account. Click *Premium Portal Demo Site*.

License types

To activate FortiGate Cloud Premium, you must acquire a subscription license and add-ons as needed based on the SKUs that the following table lists:

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 FC-10-XXXXX-950-02-DD FC-10-XXXXX-928-02-DD FC-10-XXXXX-100-02-DD
FortiDeploy	
Bulk provisioning	FDP-SINGLE-USE

The FortiGate Cloud Premium 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, the FortiCloud Premium license (for FortiCloud Organizations) is required at the account level on the admin account managing the tenants.

For FortiSandbox SaaS upload limits, see Sandbox on page 23.

Provisioning FortiGates to FortiGate Cloud Premium does not require a subscription. For limitations without a subscription, see Feature comparison on page 10. 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

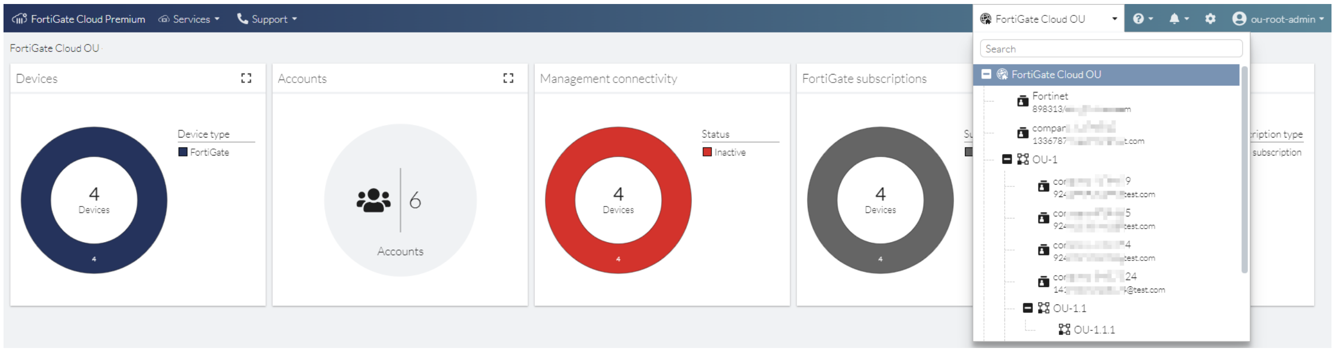
FortiGate Cloud Premium offers a different feature set depending on whether or not the device has a paid subscription. The following chart shows the features available for FortiGate Cloud Premium for these scenarios:

Feature	Device without paid subscription	Device with paid subscription
Cloud provisioning	Yes	Yes
Federated firmware upgrade	No	Yes
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

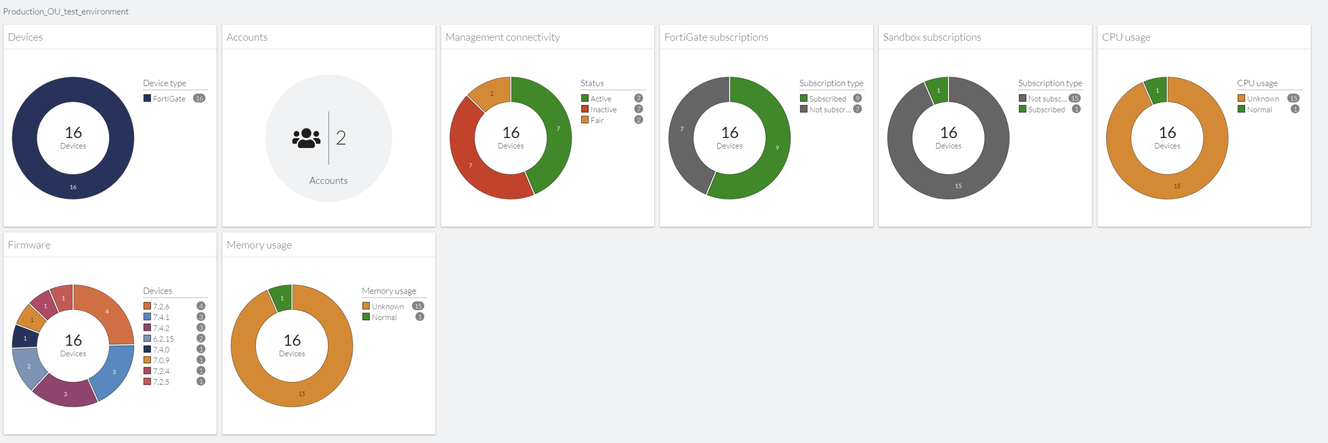
OU

FortiGate Cloud Premium supports organizational unit (OU) account selection and switching. OU support is currently in beta and available to external customers with FortiCloud Premium Account licenses (FC-15-CLDPS-219-02-DD). 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 Premium 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 15.

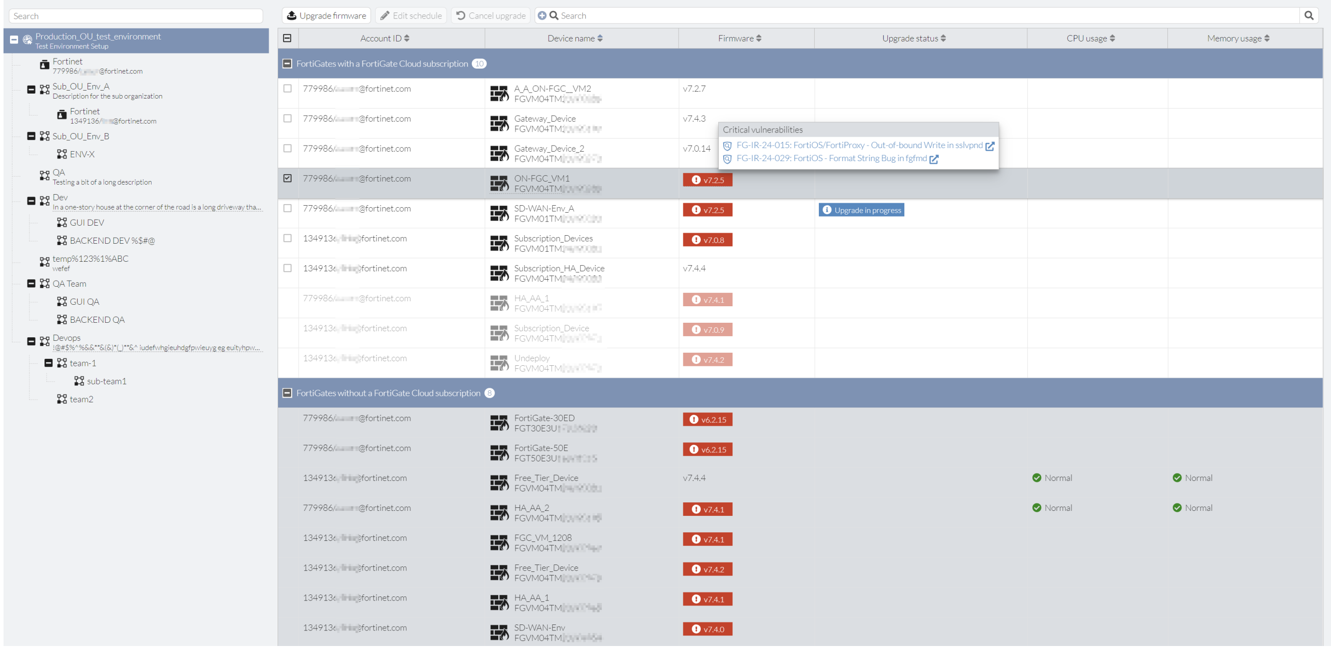


Widget	Description
Devices	Displays a donut chart that details the device type breakdown and total number of devices in this OU. To display the list of devices for each account in the OU, see OU Asset list on page 12.
Accounts	Displays a donut chart that details the total number of accounts in this OU. You can expand the widget to display the list of accounts in the OU.
Management connectivity	Displays a donut chart that details the management connectivity status breakdown and total number of devices in this OU.

Widget	Description
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.



- Production_OU_test_environment
  Test Environment Setup
  - Fortinet
    779986/[redacted]@fortinet.com
  - Sub_OU_Env_A
    Description for the sub organization
    - Fortinet
      1349136/[redacted]@fortinet.com
  - Sub_OU_Env_B
    - ENV-X
  - QA
    Testing a bit of a long description
  - Dev
    In a one-story house at the corner of the road is a long driveway tha...
    - GUI DEV
    - BACKEND DEV %$#@
  - temp%123%1%ABC
    wefef
  - QA Team
    - GUI QA
    - BACKEND QA
  - Devops
    !@#$%^%&&**&(&)*(_)**&^ iudefwhgieuhdgfpwieuyg eg euityhpw...
    - team-1
      - sub-team1
    - team2

⊟	Account ID	Device name	Firmware	Upgrade status	CPU usage	Memory usage
⊟	FortiGates with a FortiGate Cloud subscription 10					
□	779986/[redacted]@fortinet.com	A_A_ON-FGC__VM2 FGVM04TM[redacted]	v7.2.7			
□	779986/[redacted]@fortinet.com	Gateway_Device FGVM04TM[redacted]	v7.4.3			
□	779986/[redacted]@fortinet.com	Gateway_Device_2 FGVM04TM[redacted]	v7.0.14			
☑	779986/[redacted]@fortinet.com	ON-FGC_VM1 FGVM04TM[redacted]	v7.2.5			
□	779986/[redacted]@fortinet.com	SD-WAN-Env_A FGVM01TM[redacted]	v7.2.5	Upgrade in progress		
□	134913[redacted]fortinet.com	Subscription_Devices FGVM01TM[redacted]	v7.0.8			
□	134913[redacted]fortinet.com	Subscription_HA_Device FGVM04TM[redacted]	v7.4.4			
	779986/[redacted]@fortinet.com	HA_AA_1 FGVM04TM[redacted]	v7.4.1			
	134913[redacted]fortinet.com	Subscription_Device FGVM04TM[redacted]	v7.0.9			
	134913[redacted]fortinet.com	Undeploy FGVM04TM[redacted]	v7.4.2			
⊟	FortiGates without a FortiGate Cloud subscription 8					
	779986/[redacted]@fortinet.com	FortiGate-30ED FGT30E3U[redacted]	v6.2.15			
	779986/[redacted]@fortinet.com	FortiGate-50E FGT50E3U[redacted]	v6.2.15			
	134913[redacted]fortinet.com	Free_Tier_Device FGVM04TM[redacted]	v7.4.4		✓ Normal	✓ Normal
	779986/[redacted]@fortinet.com	HA_AA_2 FGVM04TM[redacted]	v7.4.1		✓ Normal	✓ Normal
	134913[redacted]fortinet.com	FGC_VM_1208 FGVM04TM[redacted]	v7.4.1			
	134913[redacted]fortinet.com	Free_Tier_Device FGVM04TM[redacted]	v7.4.2			
	134913[redacted]fortinet.com	HA_AA_1 FGVM04TM[redacted]	v7.4.1			
	134913[redacted]fortinet.com	SD-WAN-Env FGVM04TM[redacted]	v7.4.0			

Critical vulnerabilities
FG-IR-24-015: FortiOS/FortiProxy - Out-of-bound Write in sslvpnd
FG-IR-24-029: FortiOS - Format String Bug in fgfmd

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.

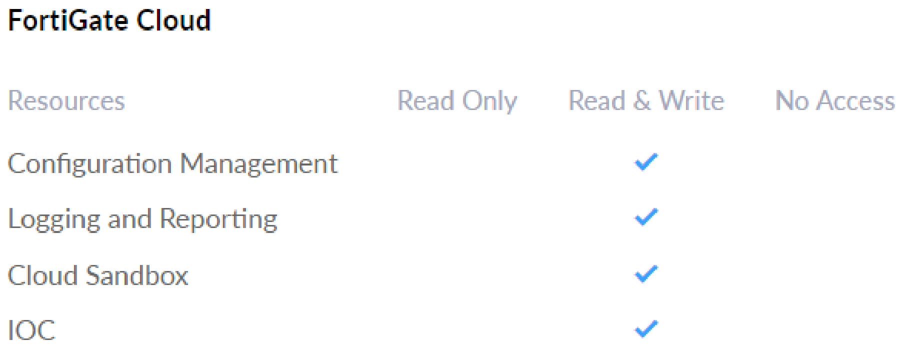
Column	Description
Firmware	Firmware version installed on the device.
Upgrade status	Displays if the FortiGate is currently performing a firmware upgrade.
CPU usage	CPU usage level on the device.
Memory usage	Memory usage level on the device.

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 31.

IAM users

FortiCloud Identity & Access Management (IAM) supports creating IAM users and allowing access to FortiGate Cloud Premium 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.



FortiGate Cloud

Resources	Read Only	Read & Write	No Access
Configuration Management		✓	
Logging and Reporting		✓	
Cloud Sandbox		✓	
IOC		✓	

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.

Dashboard

You see the *Dashboard* > *Status* page when you first open the FortiGate Cloud Premium interface. The widgets provide information about the devices that your FortiGate Cloud Premium 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 Premium then displays the *Assets* > *Asset list* filtered to only display FortiGates that have a subscription.

FortiGate Cloud Premium contains the following dashboards:

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

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.

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.

Network

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

Security

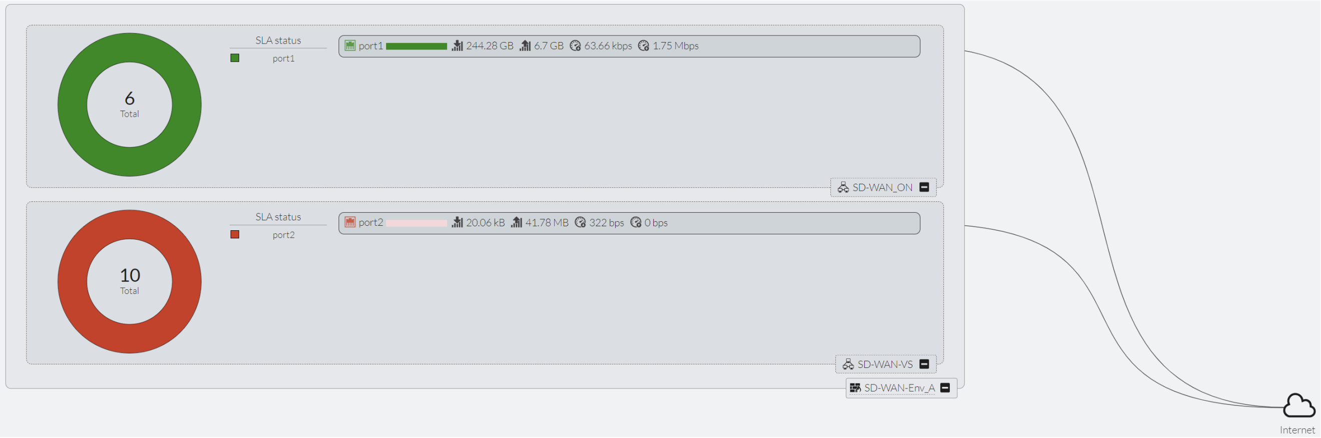
Widget	Description
FortiSandbox Cloud status	Displays the database versions and last updated dates for the dynamic malware and URL threat databases.
Top FortiSandbox files	Displays the most commonly analyzed file types in the last 24 hours of scanning.
FortiSandbox scan results	Shows the last seven days 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.

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.
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.

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



Assets

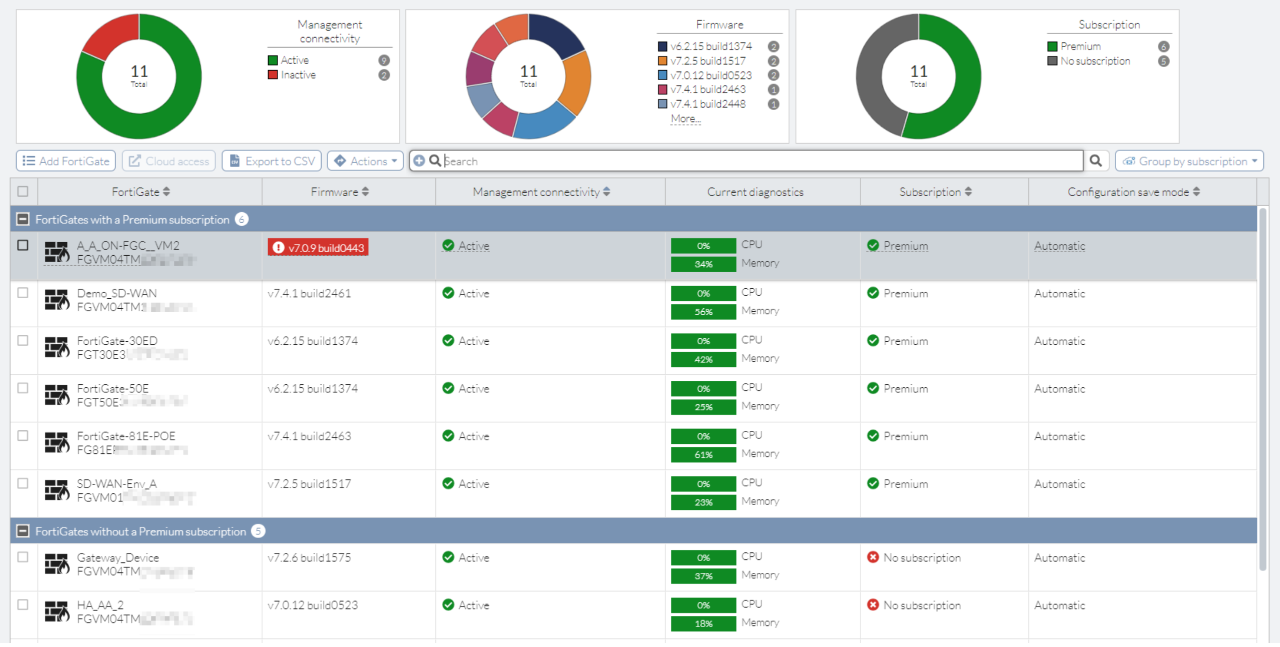
Assets > *Asset list* displays a centralized inventory of all FortiGate and FortiWifi devices from all FortiGate Cloud Premium instances in a domain group, regardless of region. For example, if you access *Assets* from the Europe region, you see the region of a connected FortiGate Cloud Premium instance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

For instructions on deploying a FortiGate to FortiGate Cloud Premium, see Cloud provisioning on page 19.

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:

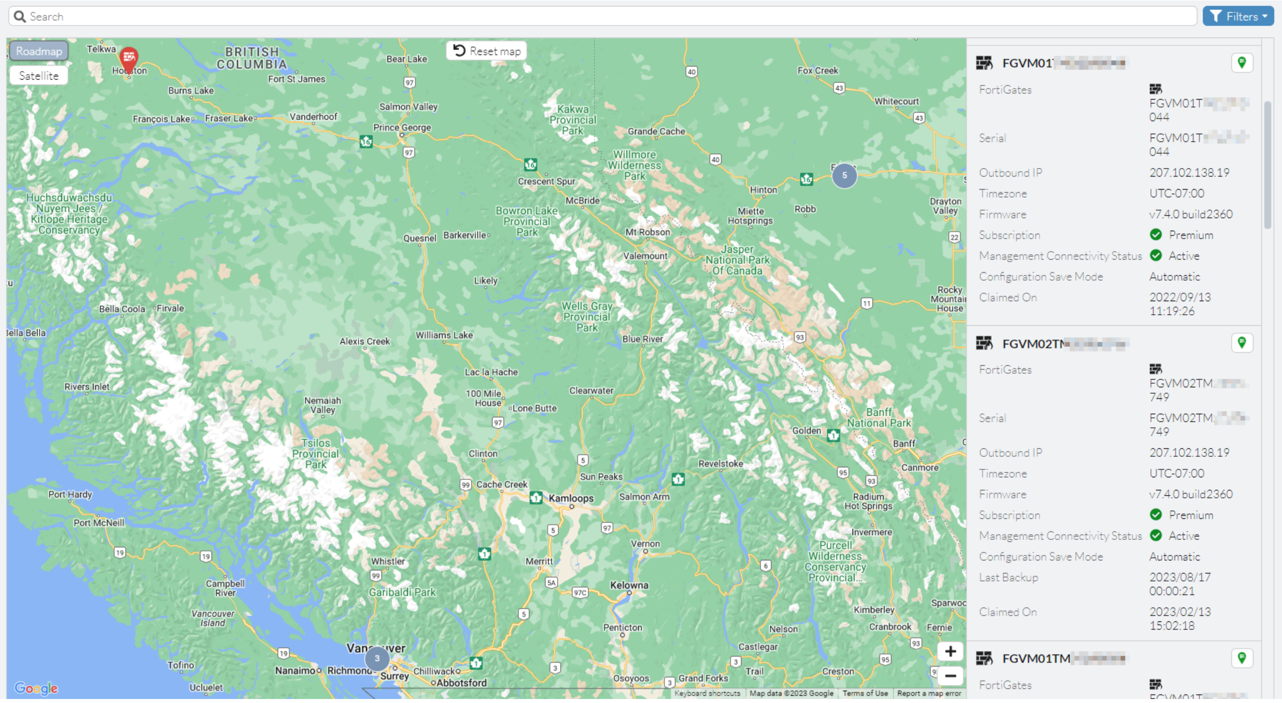
- Serial number
- Fortinet product type
- Firmware version
- Management connectivity status (If the device is connected through a management tunnel)
- Current diagnostics (device CPU and memory usage)
- Subscription status
- Configuration save mode. See Using configuration save mode.
- Last log upload 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 Premium displays the list of FortiGates separated into two groups: FortiGates with a premium subscription and FortiGates without a subscription.



□	FortiGate	Firmware	Management connectivity	Current diagnostics	Subscription	Configuration save mode
⊟	FortiGates with a Premium subscription 6					
□	A_A_ON-FGC__VM2 FGVM04TM[redacted]	v7.0.9 build0443	✓ Active	0% CPU 34% Memory	✓ Premium	Automatic
□	Demo_SD-WAN FGVM04TM[redacted]	v7.4.1 build2461	✓ Active	0% CPU 56% Memory	✓ Premium	Automatic
□	FortiGate-30ED FGT30E3[redacted]	v6.2.15 build1374	✓ Active	0% CPU 42% Memory	✓ Premium	Automatic
□	FortiGate-50E FGT50E[redacted]	v6.2.15 build1374	✓ Active	0% CPU 25% Memory	✓ Premium	Automatic
□	FortiGate-81E-POE FG81E[redacted]	v7.4.1 build2463	✓ Active	0% CPU 61% Memory	✓ Premium	Automatic
□	SD-WAN-Env_A FGVM01[redacted]	v7.2.5 build1517	✓ Active	0% CPU 23% Memory	✓ Premium	Automatic
⊟	FortiGates without a Premium subscription 5					
□	Gateway_Device FGVM04TM[redacted]	v7.2.6 build1575	✓ Active	0% CPU 37% Memory	✗ No subscription	Automatic
□	HA_AA_2 FGVM04TM[redacted]	v7.0.12 build0523	✓ Active	0% CPU 18% Memory	✗ No subscription	Automatic

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*.



FGVM01[redacted]

FortiGates	FGVM01T[redacted] 044
Serial	FGVM01T[redacted] 044
Outbound IP	207.102.138.19
Timezone	UTC-07:00
Firmware	v7.4.0 build2360
Subscription	✓ Premium
Management Connectivity Status	✓ Active
Configuration Save Mode	Automatic
Claimed On	2022/09/13 11:19:26

FGVM02TM[redacted]

FortiGates	FGVM02TM[redacted] 749
Serial	FGVM02TM[redacted] 749
Outbound IP	207.102.138.19
Timezone	UTC-07:00
Firmware	v7.4.0 build2360
Subscription	✓ Premium
Management Connectivity Status	✓ Active
Configuration Save Mode	Automatic
Last Backup	2023/08/17 00:00:21
Claimed On	2023/02/13 15:02:18

FGVM01TM[redacted]

FortiGates	FGVM01T[redacted]

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 Premium displays historical diagnostics data for the device.

Cloud provisioning

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

- FortiCloud key
- FortiOS GUI

After provisioning a FortiGate to FortiGate Cloud Premium 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 Premium using your FortiCloud account.

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

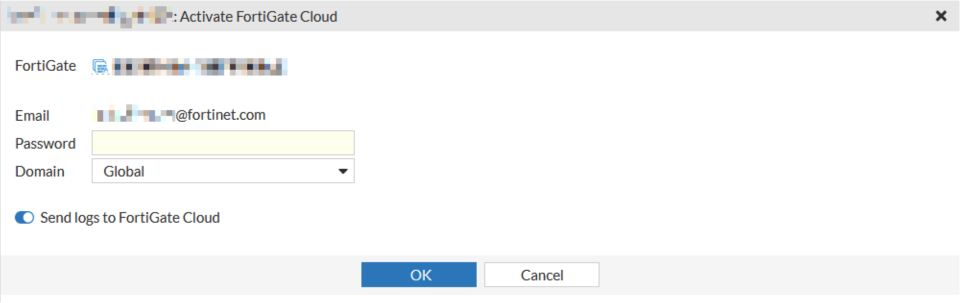
To provision a FortiGate/FortiWifi to FortiGate Cloud Premium using the FortiCloud key:

1. Log in to the FortiGate Cloud Premium portal.
2. Go to *Assets* > *Asset list*, then click *Add FortiGate*. If the device is available on the list shown on the inventory slide, select the device and click *Provision*. If else, click *Import FortiGate*.
3. In the *FortiCloud or FortiDeploy key* field, enter the key printed on your FortiGate.
4. From the *Select Display Timezone for Device* dropdown list, select the desired time zone.
5. Click *Submit*.

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/FortiWifi to FortiGate Cloud Premium 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*.



[redacted]: Activate FortiGate Cloud ✕

FortiGate [redacted]

Email [redacted]@fortinet.com

Password

Domain Global

● Send logs to FortiGate Cloud

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 Premium:

FortiGate-VMs require additional configuration to ensure that they function with FortiGate Cloud Premium. Run the following commands in the FortiOS CLI:

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

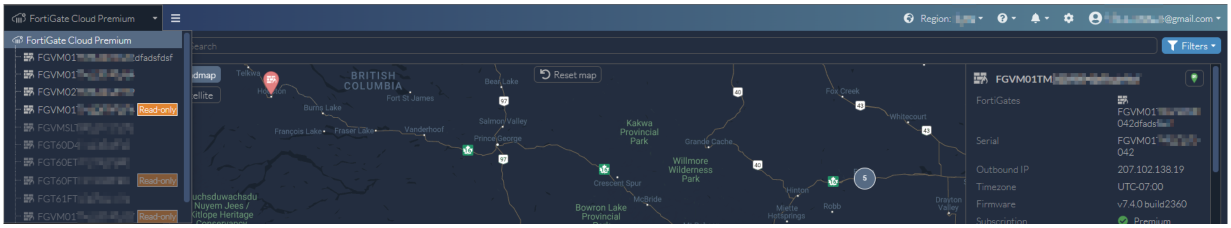
Accessing a FortiGate

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.

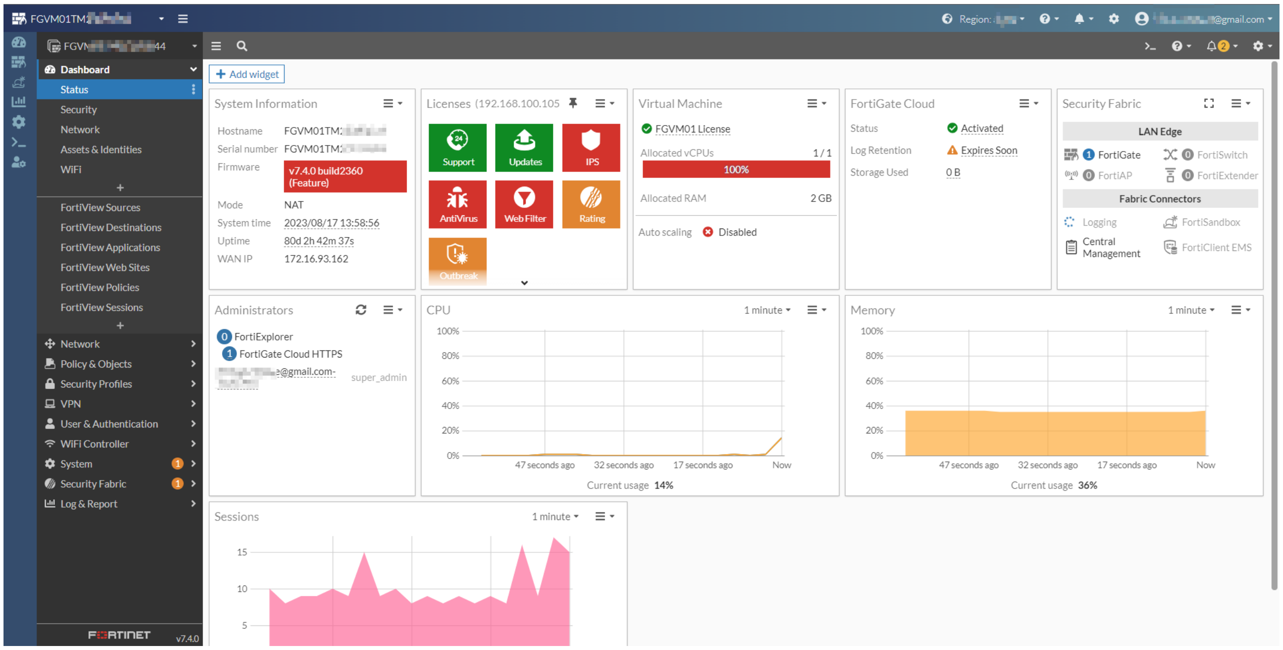
For devices with a subscription that are upgraded to FortiOS 7.0.2 or a later version, you have full access to configure features. For devices without a subscription, you have a read-only view of the configuration.

To remotely access and configure a FortiGate:

1. Do one of the following:
   - In the upper left corner, click the *FortiGate Cloud Premium* 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 Premium displays a warning that you will have read-only access. Click *OK*.
3. FortiGate Cloud Premium 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 Premium (Beta), in light and dark modes:



System Information

Hostname	FGVM01TM[redacted]
Serial number	FGVM01TM[redacted]
Firmware	v7.4.0 build2360 (Feature)
Mode	NAT
System time	2023/08/17 13:58:56
Uptime	80d 2h 42m 37s
WAN IP	172.16.93.162

Licenses (192.168.100.105

Virtual Machine

FGVM01 License

Allocated vCPUs	1 / 1
	100%
Allocated RAM	2 GB
Auto scaling	Disabled

FortiGate Cloud

Status	Activated
Log Retention	Expires Soon
Storage Used	0 B

Security Fabric

Administrators

0 FortiExplorer
1 FortiGate Cloud HTTPS
[redacted]@gmail.com- super_admin

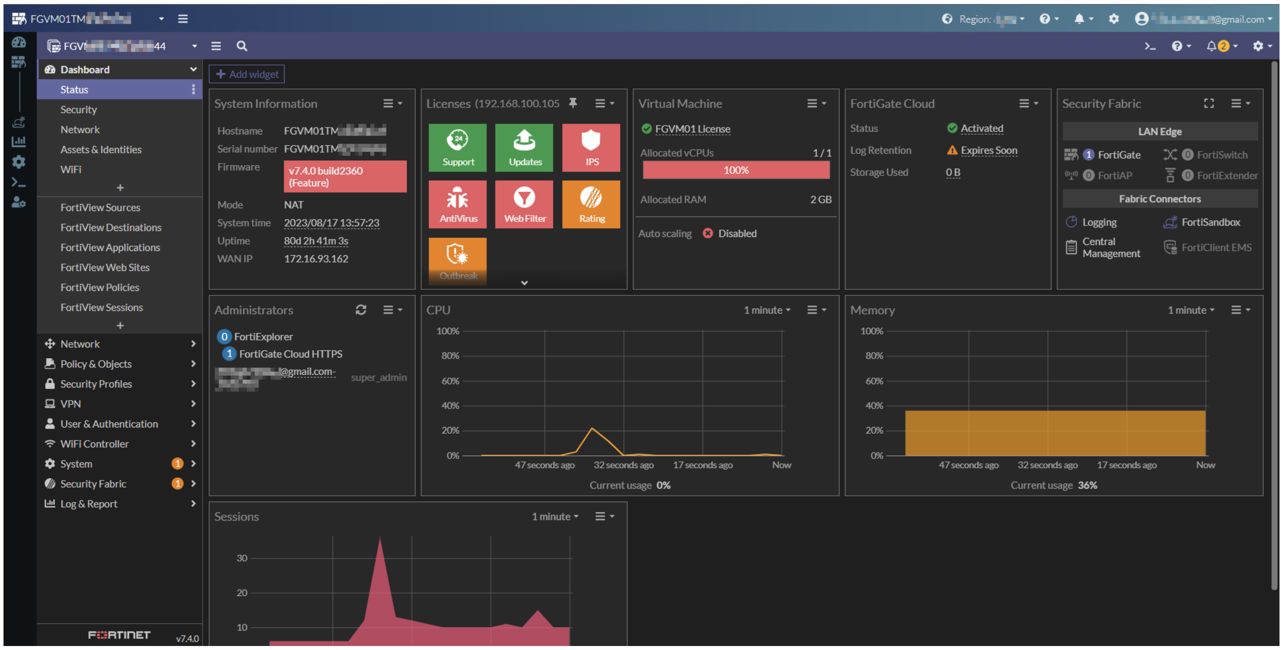
CPU

Current usage 14%

Memory

Current usage 36%

Sessions



System Information

Hostname	FGVM01TM[redacted]
Serial number	FGVM01TM[redacted]
Firmware	v7.4.0 build2360 (Feature)
Mode	NAT
System time	2023/08/17 13:57:23
Uptime	80d 2h 41m 3s
WAN IP	172.16.93.162

Licenses (192.168.100.105

Virtual Machine

FGVM01 License

Allocated vCPUs	1 / 1
	100%
Allocated RAM	2 GB
Auto scaling	Disabled

FortiGate Cloud

Status	Activated
Log Retention	Expires Soon
Storage Used	0 B

Security Fabric

Administrators

0 FortiExplorer
1 FortiGate Cloud HTTPS
[redacted]@gmail.com- super_admin

CPU

Current usage 0%

Memory

Current usage 36%

Sessions

4. Return to FortiGate Cloud Premium using the icons on the left pane.

Sandbox

Sandbox 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 configures *Send files to FortiSandbox for inspection* to enable a FortiGate to upload suspicious files to FortiSandbox 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 Premium Analytics considers suspicious change depending on the current threat climate and other factors.

The FortiGate Cloud Premium 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.

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

For devices with a paid FortiSandbox SaaS license, FortiGate Cloud supports 365 days of records and file submission limits, based on the model. For devices without a paid FortiSandbox SaaS license, FortiGate Cloud supports limited file submissions (100 per day/2 per minute) and up to seven days of records for FortiGates running FortiOS 6.2 and earlier versions.

To set up Sandbox:

1. Complete the FortiSandbox SaaS steps.
2. In *Security Profiles* > *AntiVirus*, create a profile that has *Send files to FortiSandbox 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 Premium portal 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.

To configure Sandbox settings:

1. Go to *Sandbox* > *Sandbox settings*.
2. In the *Days to retain data* field, configure the number of days to retain log data.
3. 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 Premium 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 report*.
4. In the *Select FortiGate* field, select the desired FortiGates to run the report for.
5. In the *Consolidation method* field, select whether to generate one report for all selected devices, or a separate report for each selected device.
6. If desired, in *Custom report logo*, upload an image as the custom logo for the report.
7. From the *Time period* dropdown list, determine the range of time for which to generate the report.
8. In the *Schedule* fields, configure the desired schedule for the report.
9. Click *OK*. FortiGate Cloud Premium 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*. FortiGate Cloud Premium generates the report. You can view these reports in *Analytics* > *Generated reports*.

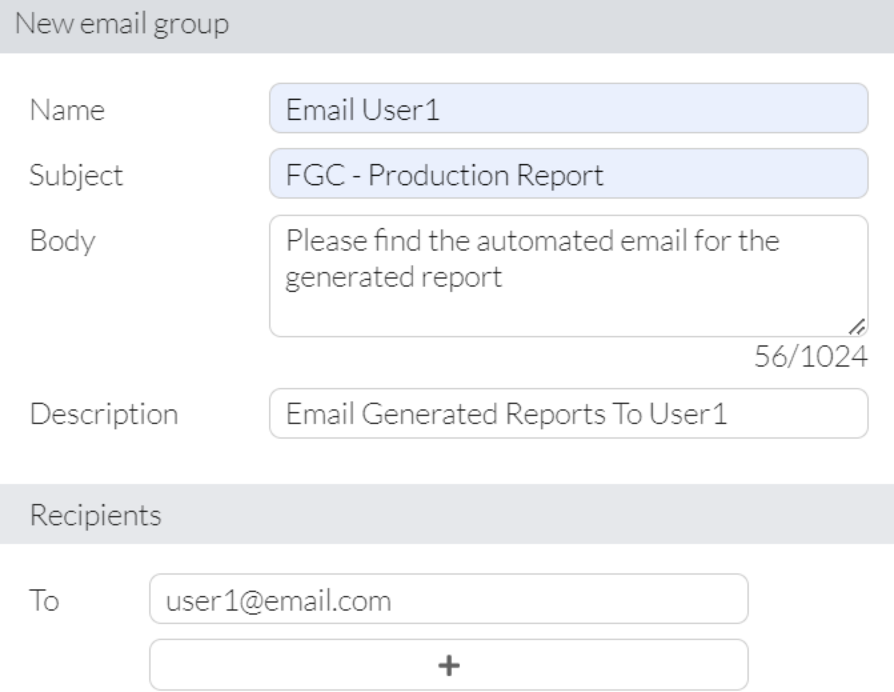
You must enable a report to be able to run it on-demand.

To unschedule a report:

1. Go to *Analytics* > *Scheduled reports*.
2. Select the desired report.
3. Click *Unschedule*.
4. The *Included devices* field displays all devices that the report is currently scheduled for. Modify the device list as necessary. Click *OK*.

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.



New email group

Name: Email User1

Subject: FGC - Production Report

Body: Please find the automated email for the generated report

56/1024

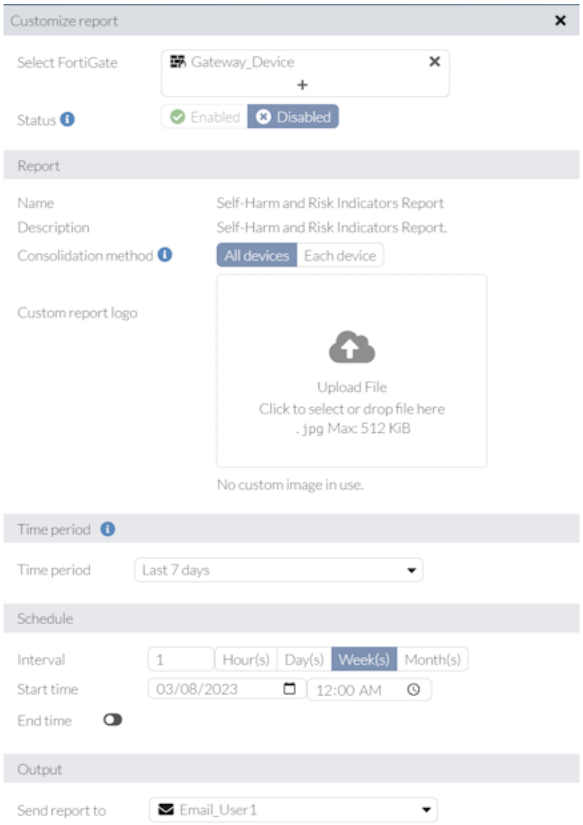
Description: Email Generated Reports To User1

Recipients

To: user1@email.com

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

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



Customize report ✕

Select FortiGate: Gateway_Device ✕ +

Status: ○ Enabled ● Disabled

Report

Name: Self-Harm and Risk Indicators Report

Description: Self-Harm and Risk Indicators Report.

Consolidation method: [✓ All devices] Each device

Custom report logo: Upload File
Click to select or drop file here
.jpg Max: 512 KiB

No custom image in use.

Time period

Time period: Last 7 days

Schedule

Interval: 1 Hour(s) Day(s) [✓ Week(s)] Month(s)

Start time: 03/08/2023 12:00 AM

End time: ○

Output

Send report to: Email_User1

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 Premium 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
- 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.

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 Premium 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. For *Backup interval*, select *Session*, *Daily*, or *Weekly*.
6. (Optional) If you selected a daily or weekly interval, you can enable *Backup when config change*. If no configuration changed, FortiGate Cloud Premium does not perform the daily or weekly backup.
7. (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.
8. 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.

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* and *Firmware management*.

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. To configure email notifications, do the following:
   a. Enable *Email*.
   b. Configure the desired email addresses to send the notification from and to.
4. To configure webhooks, do the following:
   a. Enable *Webhook*.
   b. For *Type*, select *Generic* or *MS Teams*. Webhooks only support the HTTPS protocol.
   c. Do one of the following:
      - If you selected *Generic*, configure the following:

Field	Value
Port	Enter the port that FortiGate Cloud Premium uses to send the webhook. Enter a value between 0 and 65535.
Method	Select *POST* or *PUT*.
Title	Enter the desired title for the webhook to display.
URL	Enter a URL for the webhook.
HTTP body	Enter the webhook HTTP body.
HTTP authentication	Enable HTTP authentication to view the webhook.

      - If you selected *MS Teams*, configure the following:

Field	Value
Method	Select *POST* or *PUT*.
Title	Enter the desired title for the webhook to display in Microsoft Teams.
URL	Enter a URL for the webhook.

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 Premium takes the configured action and sends notifications as configured.

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*.
   b. Configure the desired email addresses to send the notification from and to.
7. To configure webhooks, do the following:
   a. Enable *Webhook*.
   b. For *Type*, select *Generic* or *MS Teams*. Webhooks only support the HTTPS protocol.
   c. Do one of the following:
      - If you selected *Generic*, configure the following:

Field	Value
Port	Enter the port that FortiGate Cloud uses to send the webhook. Enter a value between 0 and 65535.
Method	Select *POST* or *PUT*.
Title	Enter the desired title for the webhook to display.
URL	Enter a URL for the webhook.
HTTP body	Enter the webhook HTTP body.
HTTP authentication	Enable HTTP authentication to view the webhook.

      - If you selected *MS Teams*, configure the following:

Field	Value
Method	Select *POST* or *PUT*.
Title	Enter the desired title for the webhook to display in Microsoft Teams.
URL	Enter a URL for the webhook.

8. Under *Triggers*, enable the desired file types to send notifications for.
9. Click *OK*. When the trigger occurs, FortiGate Cloud Premium takes the configured action and sends notifications as configured.

Firmware management

Firmware management lists FortiGates deployed to FortiGate Cloud Premium. It groups FortiGates that belong to the same Fortinet Security Fabric. You can manage firmware upgrades to a Fabric on this page.

To schedule a firmware upgrade:

1. Go to *Administration* > *Firmware management*.
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 Premium 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*.
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.

Audit log

Audit log displays a log of actions that users have performed on FortiGate Cloud Premium. To access Audit log, use the account dropdown list in the upper right corner of the GUI, and select *Audit log*. 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

Question	Answer
How can I customize reports in FortiGate Cloud Premium?	FortiGate Cloud Premium supports centralized reporting across all or selected devices in the account. You can enable reports can and customize them with the devices, consolidation method (all or per device), interval, and dates. You cannot change the report layout. FortiGate Cloud Premium supports 20 additional (30 in total) predefined templates, of which you can actively schedule 10 reports at any point in time. To view the report templates list and scheduling, go to *Analytics > Scheduled Reports* to enable the report and customize the parameters.
Can I use FortiGate Cloud Premium simultaneously in multiple regions (e.g. U.S. and EU)?	At the moment, the FortiGate Cloud Premium upgrade is available for one region per account. Upgrading to the Premium portal in your primary region is recommended. For secondary regions, you can continue to use the v1.0 portal.
What is the difference between a FortiGate Cloud license and a premium subscription?	"FortiGate Cloud license" and "premium subscription" refer to the same license. The FortiGate Cloud Premium GUI refers to the license as "premium subscription" while other materials, such as the price list, refer to the same license as the "FortiGate Cloud license".
Does FortiGate Cloud Premium require an additional license?	The upgrade to FortiGate Cloud Premium does not require an additional license. If the upgrade button does not display, confirm that your instance fulfills the requirements. See Requirements on page 6.

FORTINET®

www.fortinet.com