FORTINET

Administration Guide

FortiGate Cloud 26.2

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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

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

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

May 1, 2026
FortiGate Cloud 26.2 Administration Guide
32-262-1179633-20260501

TABLE OF CONTENTS

Change log **7**
Introduction **8**
Features 9
Requirements 10
Getting started with FortiGate Cloud 11
Port and access control information 13
Subscription types 13
Feature add-ons 14
Feature comparison 15
Dashboard **17**
Status 18
Security 18
Network 20
SD-WAN 20
FortiView 20
ZTNA 22
Devices and Provisioning **23**
Cloud provisioning 23
Cloud provisioning for HA pairs 26
Device list 26
FortiGate device list 27
FortiAP device list 30
FortiSwitch device list 31
FortiExtender device list 33
Device Map 35
Manage devices 35
Accessing a FortiGate 36
Transferring a FortiGate to another FortiGate Cloud account 38
Authorizing managed devices 40
Managing the device address book 40
Provisioning targets 42
Assigning provisioning targets 43
Firmware management **44**
Configuration **47**
SD-WAN Overlay **49**
Prerequisites 49
Creating the initial topology 50
Provisioning the SD-WAN configuration to your sites and viewing tasks 50
Failed configurations 51
Topology 51
Site 52
Creating a site 52

Editing a site 54
Deleting sites 55
Settings 55
Overlay policy 56
Creating a policy 56
Viewing policies 58
Applying policies 59
Managing policies 59
Policy example 60
Addresses 63
Creating an address 64
Creating an address group 64
Managing address objects and groups 65
IPAM 66
Configuring IPAM 66
Managing IPAM 66
Services 67
Creating a service 67
Creating a service group 67
Creating a service category 68
Managing services 68
Schedules 69
Creating a recurring schedule 70
Creating a one-time schedule 70
Creating a schedule group 70
Managing schedules 71
IP Pools 72
Creating an IP pool 72
Managing IP pools 73
Security profiles 73
AntiVirus 74
Web Filter 75
Application Control 75
Intrusion Prevention 76
Application signatures 77
IPS signatures 77
Analytics 78
Reports 78
Reports reference 80
Logs 83
Incidents & Events 85
Incidents 85
Event Monitor 87
Event Handler 88
Automation 89
IoC 90

Sandbox **92**
CLI scripts **94**
FortiConverter **95**
Creating tickets for third-party configuration migration 95
Creating tickets for FortiGate configuration migration 97
Viewing FortiConverter tickets 98
Downloading converted configuration files 99
Settings **100**
FortiCloud Subscriptions 100
Activating free seats 101
General Settings 102
User management 103
IAM users 103
FortiCloud account 104
Creating an account 105
Audit **106**
Multitenancy **107**
Multitenancy with FortiCloud Organizations 108
OU Dashboard 109
OU Device list 111
OU General settings 114
API access **115**
Frequently asked questions **117**
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? 117
Why can I log into the FortiGate Cloud but not activate the FortiGate Cloud account in FortiOS with the same credentials? 118
How can I activate my FortiGate Cloud on HA-paired FortiGates? 118
How can I establish a management tunnel connection between my FortiGate and FortiGate Cloud? 118
What do I do if a FortiGate added by its cloud key stays in an inactive state for more than 24 hours? 119
What do I do if the "Device is already in inventory" message appears when importing a FortiGate by key? 119
What do I do if the invalid key message appears when importing a FortiGate by key? 119
What do I do if FortiGate Cloud activation via the FortiOS GUI succeeds, but I cannot find the FortiGate in the FortiGate Cloud portal? 119
How can I use the CLI to access the root VDOM on FortiOS 7.6.4? 120
How can I move a FortiGate from region A to region B? 121
How can I connect to FortiGate by remote access? 121
How can I activate FortiGate Cloud using a different email FortiCare account when FortiOS does not allow entering another email? 121
What do I do if the migrate notice still appears after successful migration? 121

What do I do if FortiDeploy does not work? 122
What do I do if FortiOS does not upload logs? 122
What do I do if FortiGate Cloud cannot retrieve logs from FortiOS when the data source is set as FortiGate Cloud? 122
How can I export more than 2000 lines of logs? 123
Why does FortiGate Cloud drop some logs from my FortiGate? 123
How can I receive a daily report by email? 123
Why does FortiGate not submit files for Sandbox scanning? 123
What backup retention does FortiGate Cloud provide? 124
How does automatic backup work? 124
What does it mean if a geolocation attribute configuration change log/alert is received? 124
What do I do if FortiGate Cloud does not reflect a new hostname on a FortiGate or FortiGate Cloud overwrites a new FortiGate hostname? 124
Why is my FortiGate provisioned to a region other than global (U.S. or Europe)? 125
How do I check if my FortiGate has been preset for a specific server location? 125
Can I change the server location configuration? 125
If my FortiGate's server location is automatic/any, how do I provision it to my preferred region? 126
Can I migrate logs uploaded or reports generated to a different region? 126
After I transfer my FortiGate to another account in the Asset Management portal, do I still need to transfer it in FortiGate Cloud? 126
Does FortiGate Cloud support data backups and disaster recovery? 126
What happens if you enable automatic firmware upgrade on FortiGate Cloud and the FortiGate? 127
Can I disable automatic firmware upgrade from FortiOS by logging in directly to the FortiGate that has no FortiGate Cloud Basic subscription to bypass the automatic firmware upgrade enforcement from FortiGate Cloud? 127
How can I activate FortiGate Cloud on a FortiGate provisioned to an OU placeholder account? 127
Why do some of my legacy email users from FortiGate Cloud not appear after going to the Migrate to IAM page? 128
SD-WAN Overlay 129
- What is the maximum number of FortiGates that the SD-WAN Overlay feature supports? 129
- What is the difference between a branch and DC site? 129
- What does the SD-WAN Overlay agent do? 129
- When you push SD-WAN Overlay policy changes to a FortiGate, does FortiGate Cloud overwrite other locally changed parameters for an affected policy? 129
- Why does pushing some changes from FortiGate Cloud SD-WAN Overlay not create a revision in FortiGate Cloud? 129
- How do I set the SD-WAN Overlay permission for an IAM user with the RBAC profile? 130

How do I set the FortiConverter permission for an IAM user with the RBAC profile? 130
Why has log uploading stopped with an alert icon under Last Log Upload column? 131

Change log

Date	Change description
2026-05-01	Initial release.

Introduction

FortiGate Cloud is a cloud-based software-as-a-service (SaaS) offering with a range of management, reporting, and analytics for FortiGate next generation firewalls.

The cloud-based SaaS offering provides 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 report templates, log views, Fortinet Security Fabric firmware upgrades, and so on.

Features on page 9 includes the full list of FortiGate Cloud features.

FortiGate Cloud provides the following features:

- Centralized dashboard with widgets to view Fortinet Security Fabric devices, health, subscriptions, 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
- SD-WAN overlay-as-a-service
- FortiConverter Service
- Event handlers and incident management

FortiGate Cloud supports multitenancy with FortiCloud Organizations.

Features

FortiGate Cloud has the following functions:

Function	Description
Centralized dashboards	Network overview dashboard includes widgets for the status of Fortinet Security Fabric devices, device health, subscriptions, Sandbox, and other information. Customizable status, network, and security widgets plus real-time monitors for each FortiGate.
Devices list	Device inventory as list or on map with diagnostic health, network statistics, and subscription information.
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
Firmware management	Remotely upgrade FortiOS on FortiGate devices.
Configuration	Real-time FortiGate configuration management from the cloud to configure your network interfaces, SD-WAN, firewall policies, security profiles, VPN, and Security Fabric.
Analytics	• Centralized reports: Generate on-demand reports or schedule and get predefined reports delivered at intervals for network analytics and monitor usage patterns. • Log analysis: Real-time traffic, events, system logs for network activity, and threat analysis. • Incidents and events: View and analyze incidents, view and edit event handlers, monitor events, and configure automation of events and actions. • Indicators of Compromise: Alerts on newly found infections and threats to devices in the network.
FortiSandbox SaaS	Upload and analyze files that FortiGate antivirus marks as suspicious.
Regions	FortiGate Cloud includes the Global (Canada), U.S., Japan, and Europe (Germany) regions.
Multitenancy	Multitenancy based on FortiCloud Organizations. FortiGate Cloud does not support subaccount-based multitenancy.
Inline Cloud Access / Cloud Access	Choose either Inline Cloud Access or Cloud Access with FortiGate local authentication.
FortiConverter Service	Create tickets to migrate configuration files from third-party vendors to FortiGate or from FortiGate to FortiGate.

Requirements

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.
FortiGate/FortiWifi subscription	You must register all FortiGate/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.
Browser	FortiGate Cloud supports Firefox, Chrome, Edge, and Safari.

FortiGate Cloud supports all high-end, mid-range, and entry-level FortiGate models up to the FortiGate 3701F. See the Fortinet website for information about FortiGate models and specifications. All FortiWifi models support FortiGate Cloud.

FortiGate Cloud enforces the End of Support (EoS) date for FortiOS firmware. See Product Life Cycle for information about EoS dates.

How FortiGate Cloud supports EoS dates depends on whether the connected FortiGate has a subscription to FortiGate Cloud.

For FortiGates connected to FortiGate Cloud with a subscription:

- FortiGates are exempt from firmware EoS enforcement and can run any firmware supported by FortiGate Cloud (FortiOS 6.4 and later).
- Supported FortiGate hardware models that cannot be upgraded to supported firmware versions will instead be supported by FortiGate Cloud on the latest available firmware until the hardware EoS date has been reached.
- Support for FortiOS 5.x and 6.2 ended March 31, 2024.

For FortiGates connected to FortiGate Cloud without a subscription:

- FortiGates must run supported firmware that has not exceeded the EoS date to retain access to all FortiGate Cloud functionality.
- When FortiGate devices are running EoS firmware, FortiGate Cloud continues to receive submitted event logs and generate reports, but no longer sends report emails to administrators, and administrators cannot access FortiView or Log View. However, administrators can access firmware upgrade and deprovision functionality.
- When a new patch of supported firmware becomes available, you must upgrade FortiGates to the latest patch within 7 days to retain access to all FortiGate Cloud functionality. When not upgraded, FortiGate Cloud temporarily stops receiving submitted logs and blocks access to FortiView and Log View until you upgrade FortiGate.

Following are exceptions to EoS enforcement for FortiGates without a subscription:

- FortiGates running FortiOS 6.4 with Elite support contracts will be supported by FortiGate Cloud until March 31, 2026.
- FortiGates with FIPS-CC mode enabled (using either GA firmware or the FIPS-CC certified firmware) are exempt from EoS enforcement by FortiGate Cloud.

For FortiDeploy, FortiGate Cloud supports FortiGate/FortiWiFi/POE desktop and 1U models up to the 900 series running FortiOS 6.4 and later.

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.

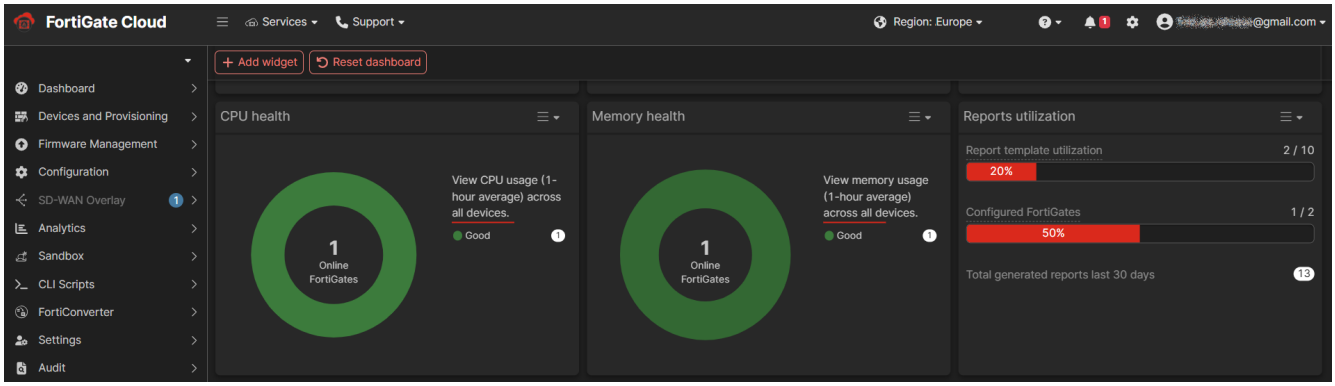
Purpose	Protocol	Port
Portal and controller	TCP	443
Analytic connection		514
Management connection		541

Getting started with FortiGate Cloud

Go to https://fortigate.forticloud.com to access FortiGate Cloud.

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

The *Dashboard* > *Status* page displays a variety of widgets. The widgets provide information about the devices that your FortiGate Cloud manages, such as how many FortiGates have subscriptions. *Dashboard* > *Security* provides details on the 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 36.
Menu icon	Use the menu icon to collapse or display the left pane, which displays other

Option	Description
	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 in.
Demo resources	View use case videos and access FortiGate Cloud 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 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.

From the left pane, you can access other options including devices, 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 is managing.
Devices and Provisioning	View a centralized inventory of all FortiGate and FortiWifi devices. See Devices and Provisioning on page 23.
Firmware management	View FortiGates provisioned to FortiGate Cloud and managed devices connected to FortiGates. Manage firmware upgrades and use firmware profiles. See Firmware management on page 44.
Configuration	Manage FortiGate Cloud account and Sandbox settings. See Configuration on page 47.
SD-WAN Overlay	Provision new SD-WAN overlay networks from FortiGate Cloud. See SD-WAN Overlay on page 49.
Analytics	Create and alter report configurations and their settings. These report configurations are available for all provisioned devices. See Analytics on page 78.
Sandbox	View the scan results from files that Sandbox submitted to FortiGuard for threat analysis. See Sandbox on page 92.
CLI Scripts	Configure and schedule scripts of CLI commands to run on your FortiGates. See CLI scripts on page 94.

Option	Description
FortiConverter	Create tickets to migrate a configuration from a third-party vendor or a FortiGate to a target FortiGate. See FortiConverter on page 95.
Settings	Configure general FortiGate Cloud settings, including users. View and activate FortiCloud subscriptions. See Settings on page 100.
Audit	View a log of actions that users have performed on FortiGate Cloud.

Port and access control information

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

FortiGate Cloud can also use internet service database (ISDB) objects. To use ISDB to allowlist control outgoing traffic to FortiGate Cloud, you must use both Fortinet-FortiCloud and Fortinet-FortiSandbox. See Internet service database objects.

Region	IP address range
Global	208.91.113.0/24, 173.243.132.0/24
Japan	148.230.40.0/24
EU	154.52.10.0/24, 154.45.6.0/24
US	154.52.4.0/24,209.40.117.0/24

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

Region	IP address range
Global	173.243.139.0/24, 184.94.112.0/24, 154.52.26.0/24, 141.109.166.192/26
Japan	210.7.96.0/24, 154.52.7.0/24
EU	83.231.212.128/25, 154.52.11.0/24, 209.40.96.192/26
US	209.40.106.192/26, 209.66.107.0/24

Subscription types

The following are essential subscriptions to use FortiGate Cloud:

Type	Description	SKU
FortiGate Cloud Standard Subscription	Cloud Management, Analytics and 1 Year Log Retention for FortiGate, FortiGate VM and FortiWiFi devices	FC-10-00XXX-131-02-DD

- Devices without a FortiGate Cloud standard subscription can be provisioned to FortiGate Cloud as *Basic tier*, which provides limited features, including 7-day log retention, remote access and one default report.
- An active FortiCare Premium support contract is required.
- For high availability clusters, a subscription is required for each device.

Feature add-ons

The following are add-on subscriptions to enable additional features in FortiGate Cloud:

Feature	Description	Bundles/SKUs
FortiDeploy (per PO)	Bulk provisioning	FDP-SINGLE-USE
FortiSandbox SaaS (per device)	SaaS based Cloud Sandbox for FortiGate devices	Included in ENT, UTP, ATP and AMP bundles. SKUs: ENT: FC-10-XXXXX-809-02-DD UTP: FC-10-XXXXX-950-02-DD ATP: FC-10-XXXXX-928-02-DD AMP: FC-10-XXXXX-100-02-DD
FortiConverter Service (per each service request)	Configuration conversion service	Standalone or included in Enterprise bundle. SKUs: FC-10-XXXXX-189-02-DD ENT Bundle: FC-10-XXXXX-809-02-DD)
SD-WAN Overlay-as-a-Service (included in SD-WAN Bundle)	SaaS based overlay network provisioning	FortiGates: SD-WAN bundles or FortiGate Cloud Advanced subscription includes FortiGate Cloud Standard and SD-WAN Overlay-as-a-service. FortiGate SKUs:

Feature	Description	Bundles/SKUs
		FC-10-XXXXX-1337-02-DD FC-10-XXXXX-1329-02-DD FortiGate VM SKU: FCX-10-FGVVS-1125-02-DD

For pricing information, contact your Fortinet partner or reseller.

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

Feature comparison

FortiGate Cloud offers a different feature set for Basic and Standard subscriptions. The following chart summarizes the features available with each subscription:

Feature	Basic*	Standard
Zero Touch Cloud Provisioning	✓	✓
Remote Access to FortiOS GUI	✓	✓
Federated Firmware Management	Latest Patch only	✓
Centralized Configuration Management	X	✓
Configuration Backup and Restore	X	✓
Security Analytics	7 days	1 Year
Hosted Log Retention	7 days	1 Year
Realtime log views and download	X	✓
Incident Management	X	✓
Event Handlers and Automation	X	✓
Reports	1 default report	Multiple
API Access	X	✓
Indicators of Compromise	X	✓
SD-WAN Overlay-as-a-Service**	X	✓
FortiConverter***	✓	✓
Cloud Sandbox****	✓	✓

* Basic subscription requires FortiCare Premium

** SD-WAN Bundle includes FortiGate Cloud Standard, SD-WAN Overlay-as-a-Service

*** Available as separate addon or limited free license

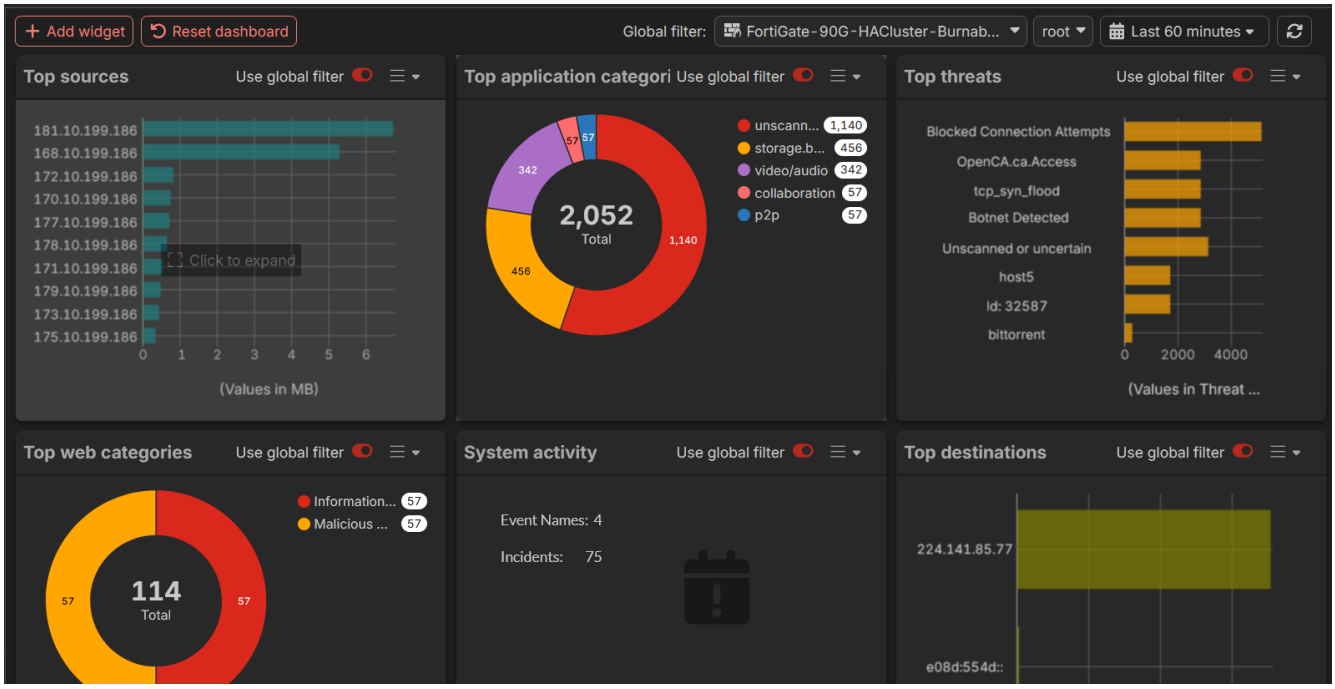
**** Cloud Sandbox requires UTP/Enterprise bundle

Dashboard

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

Within the widgets, you can enable the *Use global filter* toggle. When enabled, this toggle activates the *Global filter* at the top of the page, which can then be used to apply the same filters to multiple widgets on the same page.

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 portion of the donut chart that represents FortiGates with a FortiGate Cloud Basic subscription or Standard subscription. FortiGate Cloud then displays the *Devices and Provisioning > Device List > FortiGate* page filtered to only display FortiGates with the Basic or Standard subscription.



FortiGate Cloud contains the following dashboards:

- Status on page 18
- Security on page 18
- Network on page 20
- SD-WAN on page 20
- FortiView on page 20
- ZTNA on page 22

You can also create a custom dashboard.

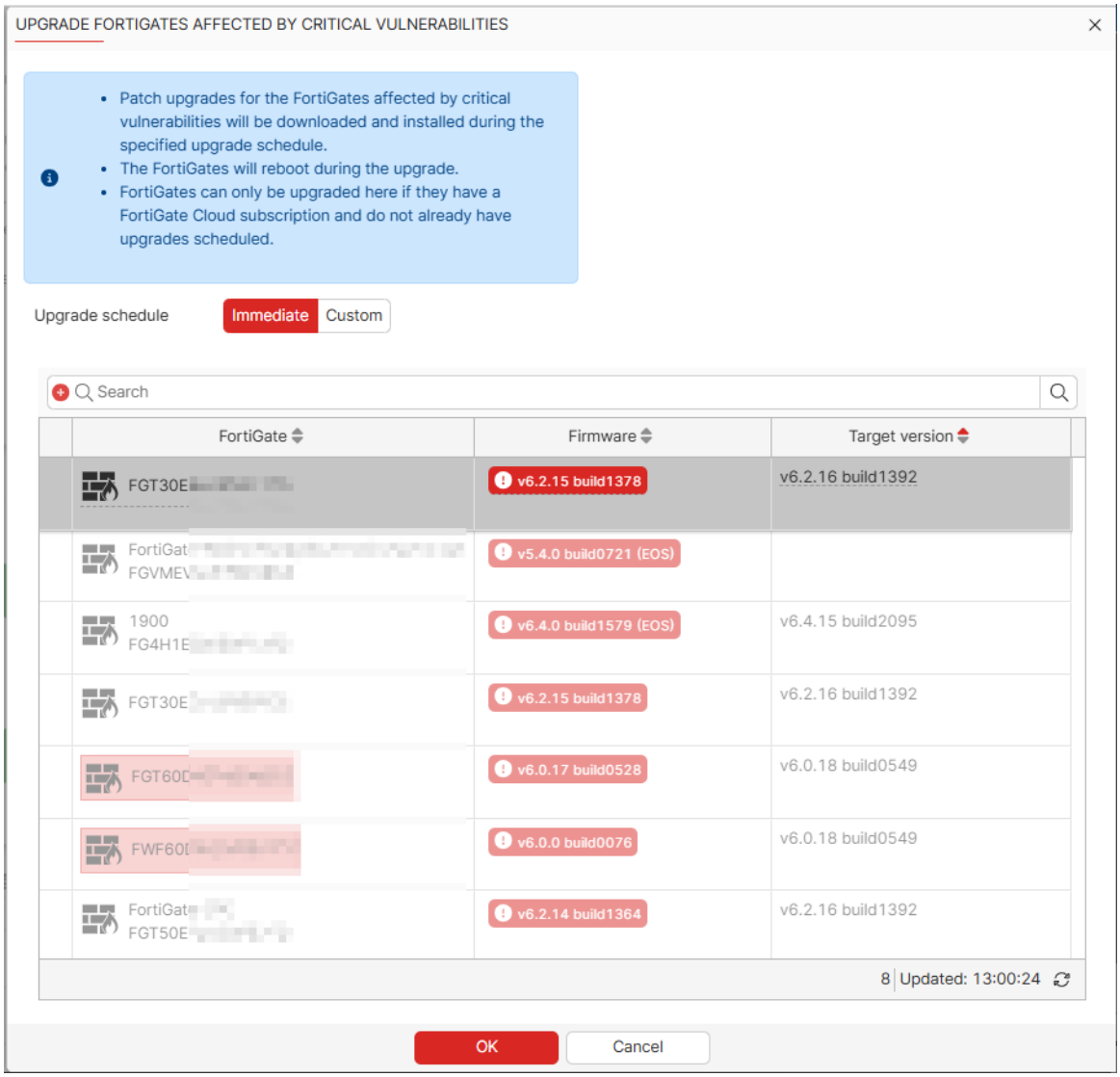
Status

Widget	Description
FortiGate subscription statuses	Displays how many FortiGates have a FortiGate Cloud Basic or FortiGate Cloud Standard subscription. Some features, such as the SD-WAN dashboard, require a separate subscription. See Subscription types on page 13.
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.

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.
FortiGuard security alerts	Displays FortiGuard security alert information and schedule upgrades for FortiGates susceptible to critical vulnerabilities.
Indicators of compromise (standalone)	Only applies if you have a FortiGate with a legacy standalone indicator of compromise (IOC) subscription which has not reached expiry. If so, this widget displays compromised hosts data from devices with a standalone IOC contract and a link to the IOC portal. This widget does not display if you are using the new IOC service, which the Standard subscription supports. See IoC on page 90.
Risk website visitors	Users who visited a website determined as a risk.
Malware victims	Users whose device is affected by malware.

Widget	Description
Malware targets	??
Spam targets	User whose device is affected by spam.
Data rule violators	Users who violated data rules.
Risk application users	Users who used an application determined as a risk.
Attack targets	Users whose device is affected by an attack.
Intrusion targets	Users whose device is affected by an intrusion.



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.
Analytics connectivity	Displays the status of the Analytics services.

SD-WAN

The widgets on this dashboard only display information for FortiGates with an SD-WAN underlay and application monitoring subscription (SKU: FC-10-*-288-02-12).

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 an SD-WAN underlay and application monitoring 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.
SD-WAN speed test results	View SD-WAN speed test results within a specified seven-day range.

FortiView

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.

Widget	Description
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.
System activity	System events that occurred on the device.
Admin session	Admin sessions on the device.
Failed login	Failed admin login attempts on the device.
Wireless	Wireless network connection events on the device.
VPN - site to site	Site-to-site VPN connections and related incidents.
VPN - SSL and dialup	SSL and dialup VPN connections and users using these connections.
Failed VPN login	Failed VPN tunnel login attempts on the device.
ZTNA servers	Information on FortiGates acting as zero trust network access (ZTNA) servers, such as number of sessions.

ZTNA

Widget	Description
Public cloud App access	ZTNA public cloud app access attempts.
Private App access	ZTNA private cloud app access attempts.
Private & public application access failure history	ZTNA private and public app access failed attempts.
Bandwidth trends	ZTNA bandwidth usage trends.
CASB App access	ZTNA CASB app access attempts.
Connection attempts	ZTNA connection attempts.
Device statistics	Device statistics.
Top users by connections	Top users by number of ZTNA connections.
Users	Users who have connected to ZTNA.
User statistics	Statistics for users who have connected to ZTNA.
User overview	Overview for users who have connected to ZTNA.
Policy overview	ZTNA policy overview.
Session statistics	ZTNA session statistics.

Devices and Provisioning

Devices and Provisioning displays a device list and map of all FortiGates and managed devices, providing a centralized inventory of all devices from all FortiGate Cloud instances in a domain group.

For instructions on provisioning a device to FortiGate Cloud, see Cloud provisioning on page 23.

You can see different device types using the *FortiGates*, *FortiAPs*, *FortiSwitches*, and *FortiExtenders* menus. When you add a FortiGate to FortiGate Cloud that is managing these devices, the managed devices also display in FortiGate Cloud. Therefore, this guide does not provide instructions on provisioning these devices. See the relevant product's documentation for provisioning information.

Expand the *Device List* to access the following menu options:

FortiGate	Click the *FortiGate* menu to view all FortiGates from all FortiGate Cloud instances in a domain group. For example, if you access *Devices and Provisioning* from the Europe region, you see the region of a connected FortiGate Cloud instance from the Europe region. See FortiGate device list on page 27.
FortiAP	Click the *FortiAP* menu to view all managed FortiAPs. See FortiAP device list on page 30.
FortiSwitch	Click the *FortiSwitch* menu to view all managed FortiSwitch devices. See FortiSwitch device list on page 31.
FortiExtender	Click the *FortiExtender* menu to view all managed FortiExtender devices. See FortiExtender device list on page 33.

Click *Device Map* to view the device list as a map. See Device Map on page 35.

Cloud provisioning

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

- FortiCloud key
- FortiCloud inventory
- FortiOS GUI

> If a device has not yet been registered in the Asset Management portal, performing a cloud provisioning action automatically registers the device.

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

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

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

1. Log in to FortiGate Cloud.
2. Go to *Devices and Provisioning* > *Provisioning*, then click *Add*.
3. In the *FortiCloud or FortiDeploy key* field, enter your key value.
4. For *End user type*, select *A non-government user* or *A government user* as required.
5. From the *Partner* dropdown list, select the affiliated Fortinet partner.
6. To provision your FortiGate to FortiGate Cloud after import, enable *Provision after import*.
7. If desired, you can associate a script with the provisioning. The selected script is executed automatically once the FortiGate establishes a management tunnel with its management server. This feature is limited to FortiGates that have an active FortiGate Cloud subscription. If the script depends on a specific FortiOS version, you must specify the target FortiOS version to ensure compatibility. From the *Pre-run Script* dropdown list, select the desired script. CLI scripts configured in CLI scripts on page 94 are available for selection. The *Description* and *CLI Scripts* fields populate according to the selected script. If needed, from the *Enforce Firmware* dropdown list, select the desired FortiOS version.
8. Click *OK*.

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

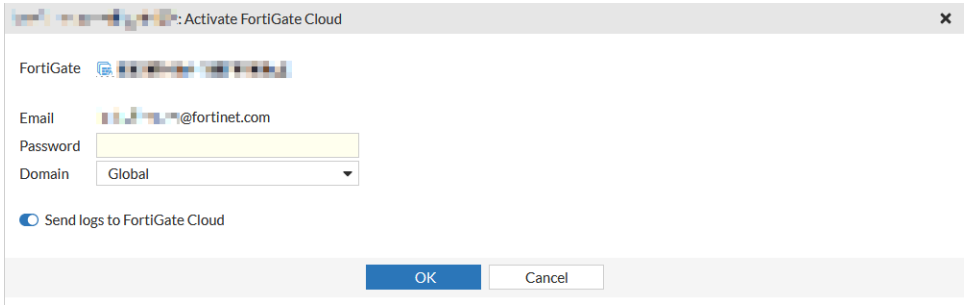
To provision a FortiGate or FortiWifi to FortiGate Cloud using the inventory:

1. Log in to the FortiGate Cloud.
2. Go to *Devices and Provisioning* > *Provisioning* , then click *Add*.
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 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:

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

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

To provision Fabric Devices (FortiAP (FAP), FortiSwitch (FSW), and FortiExtender (FEXT)):

1. Log in to the FortiGate Cloud.
2. Go to *Devices and Provisioning* > *Provisioning* . All FAP, FSW, and FEXT devices registered in the account's Asset Management portal are displayed on the *Provisioning* page.
3. Select the device(s) to provision and click *Provision*.
4. In the *Provision Device* pane, configure the device and click OK.

When a FortiGate is deprovisioned, its connected fabric devices will also be deprovisioned.

If multiple provisioning targets are detected for a Fabric device, a *Conflict Target* pop-up window is displayed, where you can select the intended provisioning target.

When a Fabric device is deprovisioned from its root FortiGate, it is also deauthorized on the FortiGate.

Cloud provisioning for HA pairs

Activate FortiGate Cloud for an Existing HA Pair/Group

For FortiGate devices configured in a High Availability (HA) pair or group, activate FortiGate Cloud only on the primary unit.

Activate FortiGate Cloud on the primary FortiGate as described in To provision a FortiGate or FortiWiFi to FortiGate Cloud in the FortiOS GUI. After activation on the primary unit, FortiGate Cloud is automatically activated on all secondary units.

Activating FortiGate Cloud directly on a secondary unit is not supported and will fail.

Before activating FortiGate Cloud on the primary unit, ensure that all HA members are already provisioned to your FortiGate Cloud account.

Add a new member to an HA Group (including RMA)

When adding or replacing an HA member, provision the new FortiGate to FortiGate Cloud before it joins the HA group.

To add a member to an HA Group:

1. Add and provision the new FortiGate to your FortiGate Cloud account.
2. Confirm the device appears in FortiGate Cloud.
3. Join the new FortiGate to the HA group.

After joining the HA group, the device automatically synchronizes its FortiGate Cloud status with the primary unit.

Device list

Expand the *Devices and Provisioning* > *Device List* menu to access the following device lists:

- FortiGate device list on page 27
- FortiAP device list on page 30
- FortiSwitch device list on page 31
- FortiExtender device list on page 33

FortiGate device list

On the *Devices and Provisioning* > *Device List* > *FortiGate* page, you can view all FortiGates. In addition to the charts, buttons, and tables on the page, you can right-click each FortiGate to access additional options.

Charts at the top of the page display:

Chart	Description
Management Connectivity	Displays the total number of FortiGates being managed and how many devices are actively connected. It also displays the number of inactive FortiGates. Click the chart to filter the page. Click the *Filter* icon beside *Management Connectivity* to remove the filter.
Firmware	Displays the total number of FortiGates and how many devices are running each version of FortiOS firmware. Click the chart to filter the page. Click the *Filter* icon beside *Firmware* to remove the filter.
Subscription	Displays the total number of FortiGates with subscriptions and how many devices have a FortiGate Cloud Basic description and a FortiGate Cloud Standard description. Click the chart to filter the page. Click the *Filter* icon beside *Subscription* to remove the filter.

Below the charts, you can access the following buttons:

Button	Description
Cloud Access	Select a FortiGate, and click *Cloud Access* to access the FortiGate. See Accessing a FortiGate on page 36.

Button	Description
Export to CSV	Click the *Export to CSV* to export the *Devices and Provisioning* > *Device List* > *FortiGate* page to a CSV file named `Asset_List_<year>_<month>_<day>.csv`.
Actions	Select a FortiGate, and click *Actions* to access the following options: • Change hostname • Deprovision • Manage Configuration • Show Matching Generated Reports • Show Matching Scheduled Reports • Set Configuration Save Mode • View Diagnostics • Upgrade Subscriptions using FortiPoints • Set Auto Backup • Set Display Timezone • Asset Transfer Some of these options are also available when you right-click a FortiGate.
Options	Access the following options: • *FortiManager Provisioned*: Toggle on to display FortiGates provisioned by FortiManager. • *RMA'd and Deprovisioned*: Toggle on to display deprovisioned FortiGates.
Group by	Select how to group the list of displayed devices: • *Group by Subscription*: Groups FortiGates by type of subscription. FortiGates with a FortiGate Cloud Basic subscription are grouped together, and FortiGates with a FortiGate Cloud Standard subscription are grouped together. • Group by HA Cluster • Group by Tunnel Status • No Grouping

The table displays the following information about each FortiGate:

Column	Description
FortiGate	Displays the name and serial number. Hover the mouse over each FortiGate to display a tooltip of information. Hover the mouse over a column heading to display: • *Configure Table* icon: Click to choose which columns to display in the table. • *Filter* icon: Click to access filter options for the column. May not be available for all columns.
Firmware	Displays the FortiOS version and build number running on the FortiGate.

Column	Description
Management Connectivity	Displays the status of the FortiGate: • *Active*: The device is connected through a management tunnel. • *Inactive*: The device is not connected through a management tunnel.
Current Diagnostics	Displays device CPU and memory usage.
Subscription	Displays the subscription status of the FortiGate: • *Basic*: The device has a FortiCare Premium subscription. • *Standard*: The device has a FortiGate Cloud Standard subscription.
Configuration Save Mode	Displays the configured save mode for each FortiGate: • *Automatic*: Configuration changes are automatically saved to the device. • *Manual*: Administrators save changes to the device. See Using configuration save mode.
Provisioned to	Displays where the FortiGate is provisioned, for example, FortiGate Cloud.
Device Type	Displays the type of device, such as FortiGate.
Folder Name	Displays the name of the asset folder to which the device belongs. FortiGate Cloud pulls the folder structure from FortiCloud.
Last Backup	Displays the date and time of the last configuration backup.
Last Log Upload	Displays the date and time of the last log upload.
Outbound IP	Displays the outbound IP address for the device
SD-WAN	Displays whether SD-WAN is enabled or disabled on the device.

To use the right-click menu for a FortiGate:

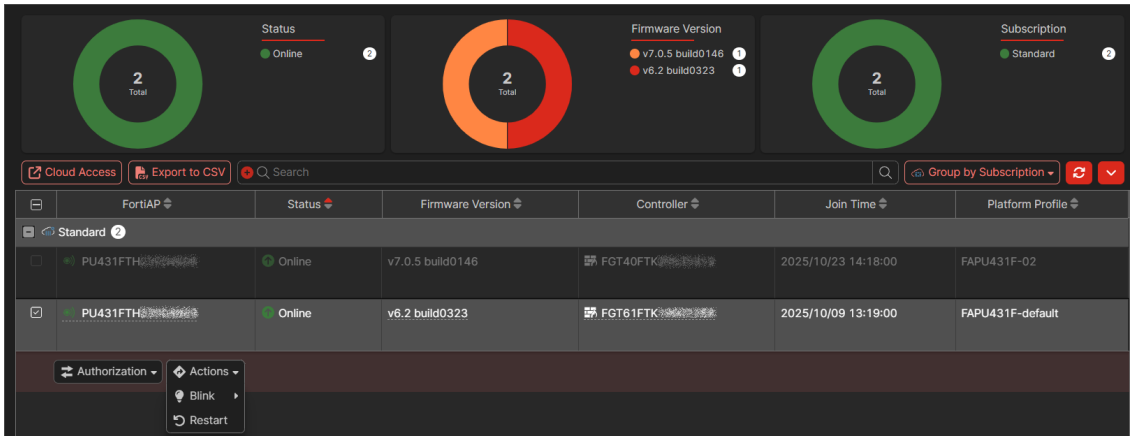
1. Go to *Devices and Provisioning* > *Device List* > *FortiGate*.
2. Right-click the FortiGate, to display and access the following menu items:

Menu	Description
Cloud Access	Select to access the FortiGate GUI. See Accessing a FortiGate on page 36.
Change hostname	Select to display the *Change Hostname* pane, type a new name, and click *OK*.
Manage configuration	Select to display the *Configuration* > *Revisions* page.
Show matching generated reports	Select to display matching reports on the *Reports* > *Generated Reports* page.
Show matching scheduled reports	Select to display scheduled reports on the *Reports* > *Scheduled Reports* page.
Set configuration save mode	Select to display the *Set Configuration Save Mode* pane, select a mode, and click *OK*. See Using configuration save mode.

Menu	Description
View diagnostics	Select to display the *Diagnostics* pane. Scroll down to view historical data organized on the following tabs: *Outages*, *Outages Chart*, and *CPU/Memory/Disk*.

FortiAP device list

On the *Devices and Provisioning* > *Device List* > *FortiAP* page, you can see FortiAP devices managed by FortiGates with a FortiGate Cloud Standard subscription.



Charts at the top of the page display:

Chart	Description
Status	Displays the total number of FortiAPs and how many devices have a status of Online. Click the chart to filter the page. Click the *Filter* icon beside *Status* to remove the filter.
Firmware Version	Displays the total number of FortiAPs and how many devices are running each firmware version. Click the chart to filter the page. Click the *Filter* icon beside *Firmware Version* to remove the filter.

Below the charts, you can access the following buttons:

Button	Description
Cloud Access	Select a FortiAP, and click *Cloud Access* to access the FortiGate that is managing the FortiAP.
Export to CSV	Click the *Export to CSV* to export the *Devices and Provisioning* > *Device List* > *FortiAP* page to a CSV file.
Group by	Select how to group the list of displayed devices:

Button	Description
	• *Group by Controller* • *No Grouping*

The table displays the following information about each FortiAP:

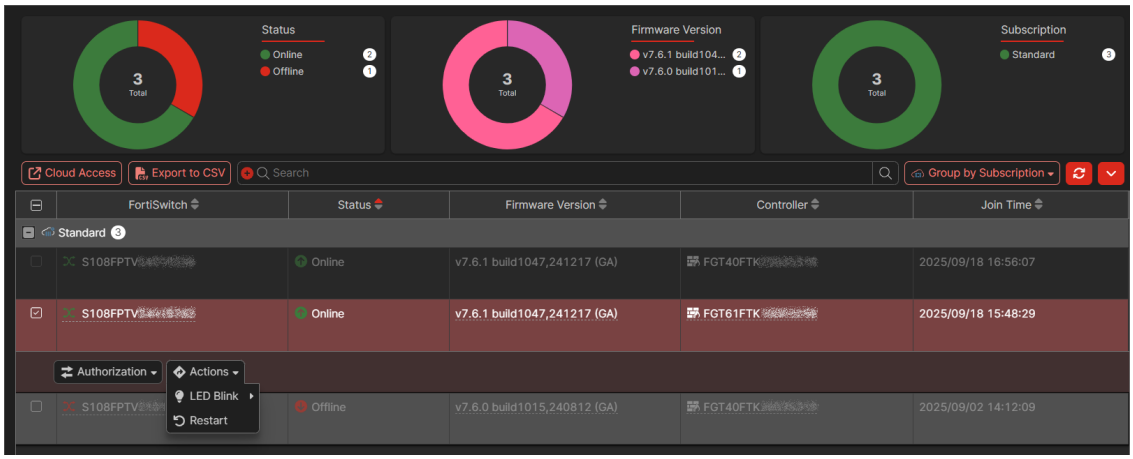
Column	Description
FortiAP	Displays the name and serial number. Hover the mouse over a column heading to display: • *Configure Table* icon: Click to choose which columns to display in the table. • *Filter* icon: Click to access filter options for the column. May not be available for all columns.
Status	Displays whether the FortiAP is online.
Firmware Version	Displays the firmware version and build number running on the FortiAP.
Controller	Indicates that the FortiAP belongs to a Fortinet Security Fabric by displaying a FortiGate serial number.
Platform Profile	Displays the name of the configuration profile assigned to the FortiAP.

Select a FortiAP to display and access the following options:

Option	Description
Authorize	Select a FortiAP to display and access the following buttons to authorize, reject, or deauthorize the selected FortiAP. See Authorizing managed devices on page 40.
Actions	Access the following options: • *Blink*: Select to start or stop blinking on the FortiAP for a specified period of time. • *Restart*: Select to restart the selected FortiAP.

FortiSwitch device list

On the *Devices and Provisioning* > *Device List* > *FortiSwitch* page, you can see FortiSwitch devices managed by FortiGates with a FortiGate Cloud Standard subscription.



Charts at the top of the page display:

Chart	Description
Status	Displays the total number of FortiSwitch devices and how many devices have a status of Online and Offline. Click the chart to filter the page. Click the *Filter* icon beside *Status* to remove the filter.
Firmware Version	Displays the total number of FortiSwitch devices and how many devices are running each firmware version. Click the chart to filter the page. Click the *Filter* icon beside *Firmware Version* to remove the filter.

Below the charts, you can access the following buttons:

Button	Description
Cloud Access	Select a FortiSwitch, and click *Cloud Access* to access the FortiGate that is managing the FortiSwitch.
Export to CSV	Click the *Export to CSV* to export the *Devices and Provisioning* > *Device List* > *FortiSwitch* page to a CSV file.
Group by	Select how to group the list of displayed devices: • *Group by Controller* • *No Grouping*

The table displays the following information about each FortiSwitch:

Column	Description
FortiSwitch	Displays the name and serial number. Hover the mouse over a column heading to display: • *Configure Table* icon: Click to choose which columns to display in the table. • *Filter* icon: Click to access filter options for the column. May not be

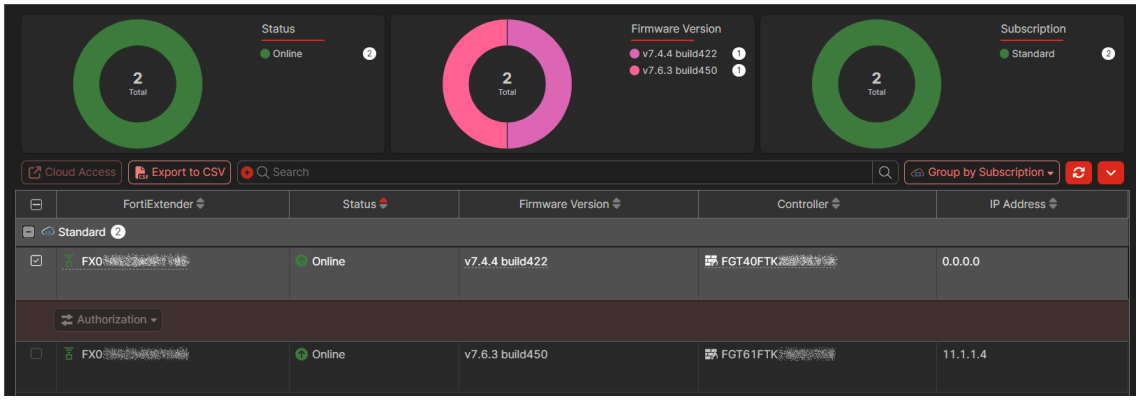
Column	Description
	available for all columns.
Status	Displays whether the FortiSwitch is Online or Offline.
Firmware Version	Displays the firmware version and build number running on the FortiSwitch.
Controller	Indicates that the FortiSwitch belongs to a Fortinet Security Fabric by displaying a FortiGate serial number.
Folder Name	Displays the name of the asset folder to which the device belongs. FortiGate Cloud pulls the folder structure from FortiCloud.
Model	Displays the FortiSwitch model.

Select a FortiSwitch to display and access the following options:

Option	Description
Authorize	Select a FortiSwitch to display and access the following buttons to authorize, reject, or deauthorize the selected FortiSwitch. See Authorizing managed devices on page 40.
Actions	Select a FortiSwitch to display and access the following options: • *LED Blink*: Select to start or stop blinking on the FortiSwitch for a specified period of time. • *Restart*: Select to restart the selected FortiSwitch.

FortiExtender device list

On the *Devices and Provisioning* > *Device List* > *FortiExtender* page, you can see FortiExtender devices managed by FortiGates with a FortiGate Cloud Standard subscription.



Charts at the top of the page display:

Chart	Description
Status	Displays the total number of FortiExtender devices and how many devices have a status of Online and Offline. Click the chart to filter the page. Click the *Filter* icon beside *Status* to remove the filter.
Firmware Version	Displays the total number of FortiExtender devices and how many devices are running each firmware version. Click the chart to filter the page. Click the *Filter* icon beside *Firmware Version* to remove the filter.

Below the charts, you can access the following buttons:

Button	Description
Cloud Access	Select a FortiExtender, and click *Cloud Access* to access the FortiGate that is managing the FortiExtender.
Export to CSV	Click the *Export to CSV* to export the *Devices and Provisioning > Device List > FortiExtender* page to a CSV file.
Group by	Select how to group the list of displayed devices: • *Group by Controller* • *No Grouping*

The table displays the following information about each FortiExtender:

Column	Description
FortiExtender	Displays the serial number of the FortiExtender. Hover the mouse over a column heading to display: • *Configure Table* icon: Click to choose which columns to display in the table. • *Filter* icon: Click to access filter options for the column. May not be available for all columns.
Status	Displays whether the FortiExtender is Online or Offline.
Firmware Version	Displays the firmware version and build number running on the FortiExtender.
Controller	Indicates that the FortiExtender belongs to a Fortinet Security Fabric by displaying a FortiGate serial number.
IP Address	Displays the FortiExtender IP address.
Folder Name	Displays the name of the asset folder to which the device belongs. FortiGate Cloud pulls the folder structure from FortiCloud.

Select a FortiExtender to display and access the following options:

Option	Description
Authorize	Select a FortiExtender to display and access the following buttons to authorize, reject, or deauthorize the selected FortiExtender. See Authorizing managed devices on page 40.

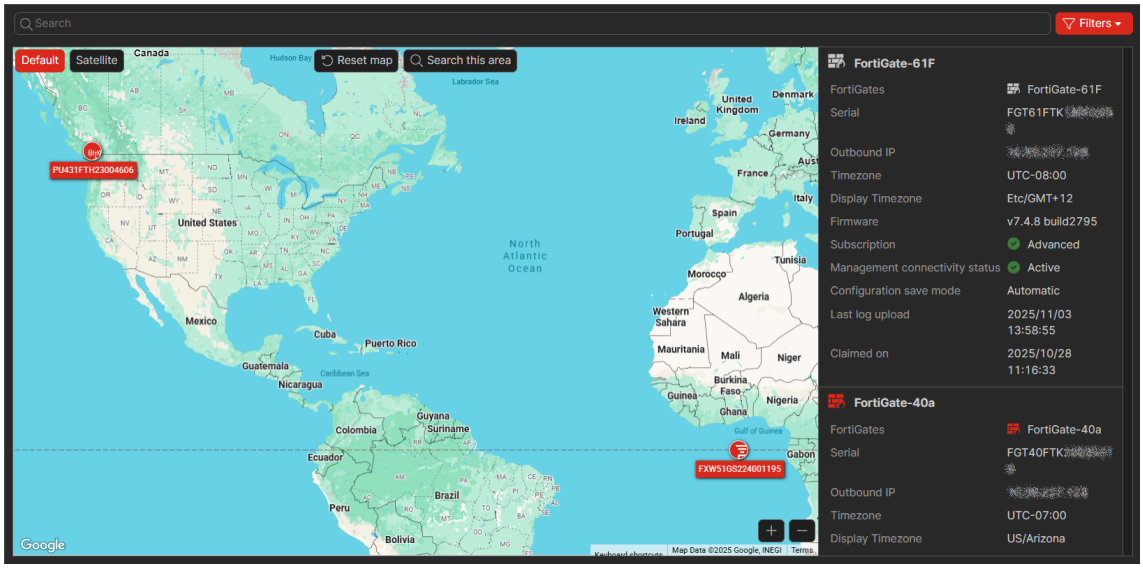
Device Map

Go to *Devices and Provisioning* > *Device Map* to view provisioned devices on a map. The map shows the geographic location of each device based on assigned or user-defined coordinates.

When you assign an address to a device, the device location is set using the address coordinates. You can manually move a device icon on the map to fine-tune its location without changing or removing the associated address. If the coordinates from an assigned address or a user-defined (drag-and-drop) location differ from coordinates configured locally on the device, the FortiGate Cloud portal uses the assigned or user-defined coordinates to determine the device's position on the map. For information about device addresses, see Managing the device address book on page 40.

The right panel displays a list of FortiGates with information similar to the *Device List*. Click the *Locate on map* icon for a device to center the map on its location.

Use the **+** and **–** buttons to zoom in and out of the map. Click *Reset map* to return to the global view. You can also filter the map by device type, such as displaying only FortiAPs.



Manage devices

From the *Devices and Provisioning* menu, you can perform the following actions:

- Accessing a FortiGate on page 36
- Transferring a FortiGate to another FortiGate Cloud account on page 38
- Authorizing managed devices on page 40

Accessing a FortiGate

When you run a function in FortiGate Cloud that applies to FortiGates, such as running a script, FortiGate Cloud may not pass the actual username of the user who performed the action to FortiOS:

When remotely accessing a FortiGate from FortiGate Cloud, one of the following occurs:

- If *Cloud Access Anonymous Mode* is enabled, FortiGate Cloud passes the username of the FortiGate Cloud user who performed the action as a randomized @fortigatecloud.com email address, such as 4aa567e55bc8@fortigatecloud.com, to FortiOS.
- If *Cloud Access Anonymous Mode* is disabled, FortiGate Cloud passes the actual username of the FortiGate Cloud user who performed the action to FortiOS.

For other management features that a user can perform from FortiGate Cloud, such as running a script, FortiGate Cloud passes the username of the FortiGate Cloud user who performed the action as FortiGateCloud to FortiOS.

Therefore, when viewing logs on the affected FortiGate, you may see 4aa567e55bc8@fortigatecloud.com or FortiGateCloud as a username. For managed security service provider customers, this provides enhanced security by preventing subusers from seeing the primary account email address in the FortiGate logs.

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

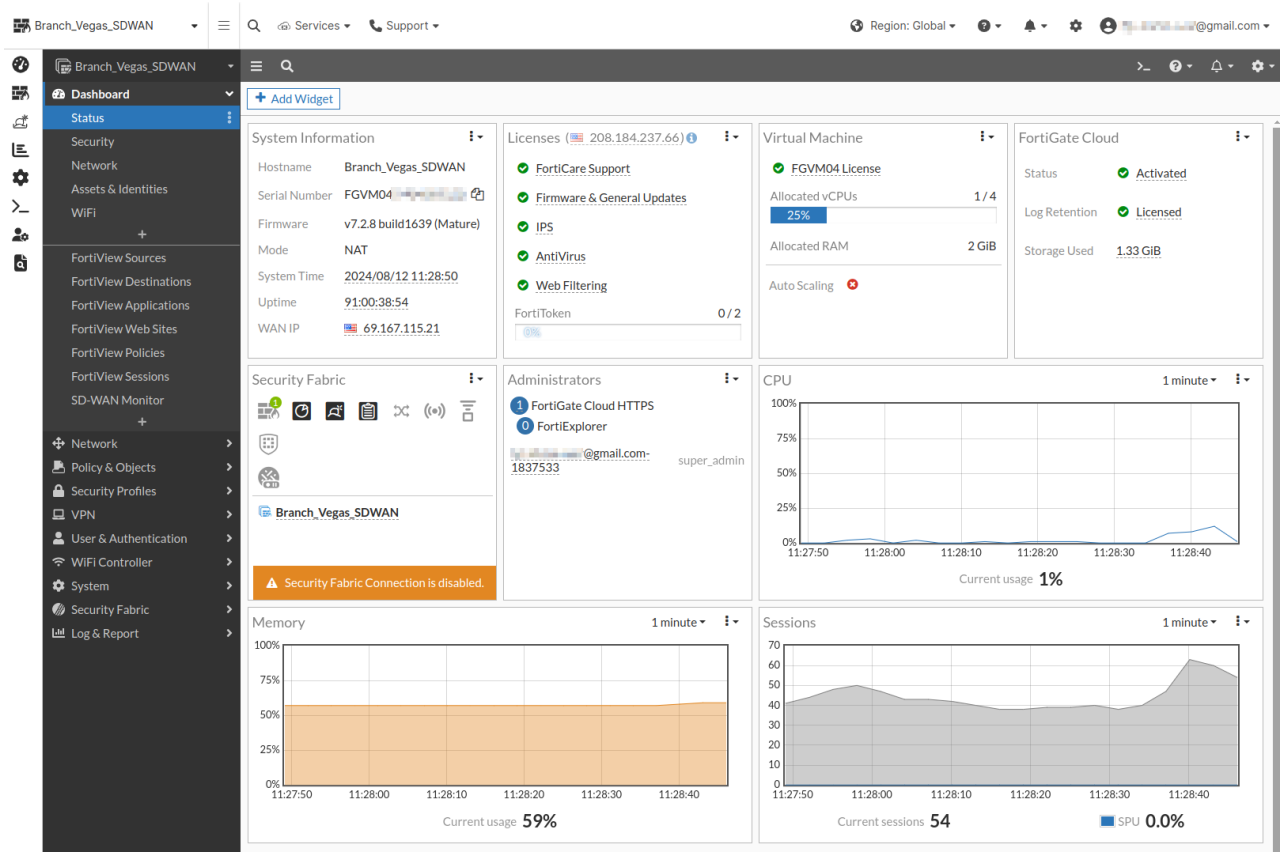
Cloud Access with read/write permission is available to FortiGates with a valid FortiCare Premium subscription; however, these devices must use the Cloud Access Local Authentication method to log in.

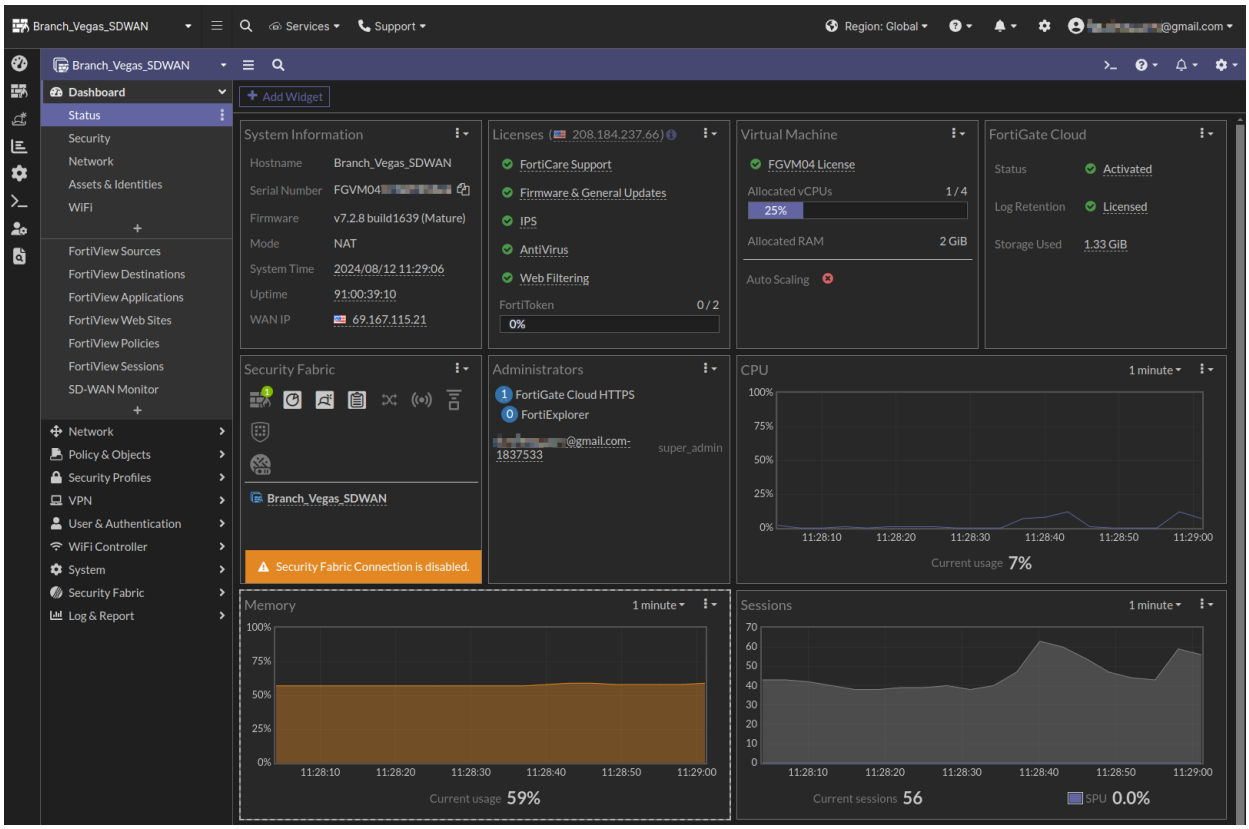
For FortiGates with a FortiGate Cloud Standard subscription, users can choose either Inline Cloud Access or Cloud Access Local Authentication under *Settings* > *General Settings*.

For devices with a subscription that are upgraded to FortiOS 7.0.2 or a later version, you have full access to configure features.

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 *Devices and Provisioning* > *Device List* > *FortiGate*. Select the desired FortiGate, then click *Cloud access*.
2. FortiGate Cloud displays the FortiOS interface in the browser window. When *Cloud Access Local Authentication* is enabled, Cloud Access opens a new browser tab where you must enter FortiGate local credentials to log in. When it is disabled, no credentials are required. View and make changes as desired. The following shows the FortiOS GUI as shown in FortiGate Cloud, in light and dark modes:


Branch_Vegas_SDWAN
Services
Support
Region: Global
Dashboard
Status
Security
Network
Assets & Identities
WiFi
FortiView Sources
FortiView Destinations
FortiView Applications
FortiView Web Sites
FortiView Policies
FortiView Sessions
SD-WAN Monitor
Policy & Objects
Security Profiles
VPN
User & Authentication
WiFi Controller
System
Security Fabric
Log & Report
Add Widget
System Information
Hostname Branch_Vegas_SDWAN
Serial Number FGVM04
Firmware v7.2.8 build1639 (Mature)
Mode NAT
System Time 2024/08/12 11:28:50
Uptime 91:00:38:54
WAN IP 69.167.115.21
Licenses (208.184.237.66)
FortiCare Support
Firmware & General Updates
IPS
AntiVirus
Web Filtering
FortiToken 0 / 2
Virtual Machine
FGVM04 License
Allocated vCPUs 1 / 4
25%
Allocated RAM 2 GiB
Auto Scaling
FortiGate Cloud
Status Activated
Log Retention Licensed
Storage Used 1.33 GiB
Security Fabric
Branch_Vegas_SDWAN
Security Fabric Connection is disabled.
Administrators
FortiGate Cloud HTTPS
FortiExplorer
@gmail.com-1837533 super_admin
CPU 1 minute
Current usage 1%
Memory 1 minute
Current usage 59%
Sessions 1 minute
Current sessions 54
SPU 0.0%


Branch_Vegas_SDWAN
Services
Support
Region: Global
Dashboard
Status
Security
Network
Assets & Identities
WiFi
FortiView Sources
FortiView Destinations
FortiView Applications
FortiView Web Sites
FortiView Policies
FortiView Sessions
SD-WAN Monitor
Policy & Objects
Security Profiles
VPN
User & Authentication
WiFi Controller
System
Security Fabric
Log & Report
Add Widget
System Information
Hostname Branch_Vegas_SDWAN
Serial Number FGVM04
Firmware v7.2.8 build1639 (Mature)
Mode NAT
System Time 2024/08/12 11:29:06
Uptime 91:00:39:10
WAN IP 69.167.115.21
Licenses (208.184.237.66)
FortiCare Support
Firmware & General Updates
IPS
AntiVirus
Web Filtering
FortiToken 0 / 2
0%
Virtual Machine
FGVM04 License
Allocated vCPUs 1 / 4
25%
Allocated RAM 2 GiB
Auto Scaling
FortiGate Cloud
Status Activated
Log Retention Licensed
Storage Used 1.33 GiB
Security Fabric
Branch_Vegas_SDWAN
Security Fabric Connection is disabled.
Administrators
FortiGate Cloud HTTPS
FortiExplorer
@gmail.com-1837533 super_admin
CPU 1 minute
Current usage 7%
Memory 1 minute
Current usage 59%
Sessions 1 minute
Current sessions 56
SPU 0.0%

3. Return to FortiGate Cloud using the icons on the left pane.

Transferring a FortiGate to another FortiGate Cloud account

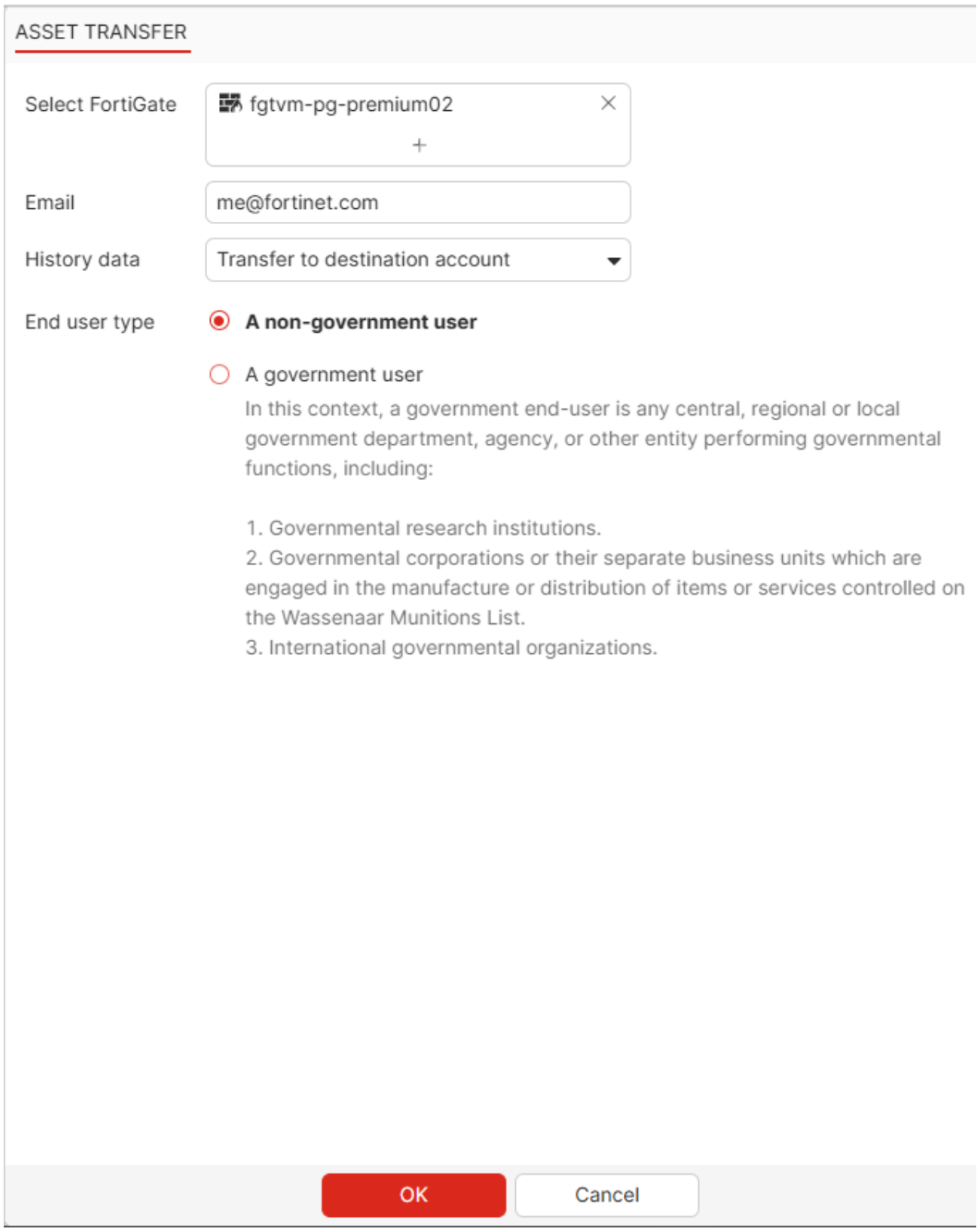
The following instructions describe transferring a FortiGate from one account (account A) to another FortiGate Cloud account (account B).

After a transfer request is initiated, the FortiGates involved are hidden from the device list, and an email is sent to both the requester and the receiver.

The requester can send a reminder email to the receiver by selecting the transfer and clicking the *Remind* button.

To transfer a FortiGate from account A to account B:

1. Initiate the transfer request from account A:
   a. Log in to FortiGate Cloud using account A credentials.
   b. Go to *Devices and Provisioning* > *Device List* > *FortiGate*.
   c. Select *Actions* > *Asset Transfer*.
   d. Click *Transfer*.
   e. In *Select FortiGate*, click *+*, then select the desired FortiGate(s) to transfer to account B. A FortiGate where the log status is suppressed or the FortiOS version has reached end of support in FortiGate Cloud is not eligible for transfer.
   f. In the *Email* field, enter the email address associated with account B.
   g. From the *History data* dropdown list, select the desired action to perform on the FortiGate(s)' historical data.
   h. For *End user type*, select the appropriate user type.
   i. Click *OK*. FortiGate Cloud sends an email notification to your email address and to the email address that you configured earlier. From the *Asset Transfer Overview* pane, you have the option to cancel the transfer request and to send an additional reminder email to account B.



2. Log in to FortiGate Cloud using account B credentials.
3. Go to *Devices and Provisioning* > *Device List* > *FortiGate*.
4. Select *Actions* > *Asset Transfer*.
5. On the *Receive* tab, select the FortiGate, then click *Accept*. You also have the option to decline the transfer. The FortiGate is now transferred to account B.

Authorizing managed devices

You can view different device types using the *FortiGates*, *FortiAPs*, *FortiSwitches*, and *FortiExtenders* tabs. The *Provisioning* page will list all supported fabric device types that are registered to your account in FortiCare, regardless of whether a fabric device has already connected to a FortiGate. From the *Provisioning* page, you can select a device and provision it to its controller. The fabric device is authorized automatically on its controller as part of the provisioning process.

If a device is provisioned to a FortiGate with a FortiGate Cloud Standard subscription, the fabric device is listed on the *Device list* > *FortiAP* page after provisioning.

You can set the device authorization status by clicking the device, then selecting the desired action from the *Authorization* dropdown list. The device authorization status displays as synced from the FortiGate. For example, if the device was authorized from the FortiGate, FortiGate Cloud displays its status as authorized. When you change the authorization status of a device from FortiGate Cloud, the new status is pushed to the FortiGate.

To change the device authorization status:

1. Go to *Devices and Provisioning* > *Device List*.
2. Go to the *FortiAP*, *FortiSwitch*, or *FortiExtender*.
3. Click the desired device.
4. From the *Authorization* dropdown list, select the desired action:

Action	Description
Authorize	Authorize the device. When a device is authorized, you can perform actions on it and update its firmware in FortiGate Cloud.
Reject	Device continues displaying in FortiGate Cloud and is connected to the FortiGate, but displays as rejected.
Deauthorize	Deauthorize the device. You cannot perform any actions on the device, including updating its firmware.

Managing the device address book

The device address book stores addresses at the account level and makes them available for association with devices. Each address includes coordinate information that can be used for location mapping. Address book entries are static and are not automatically updated after they are created, which helps maintain consistent address data. You can manage address book entries from the *Device List*, *Device Details*, and the *Device Map*.

To add a device address to the address book:

1. Do one of the following:
   - In the *Device list*:
     - Select a device, click the *Actions* menu and select *Update Device Information*.
     - Hover over a device to view the device details and click *Update Device Information*.

- In the *Device Map*, hover over a device on the map to view the device details and click *Update Device Information*.

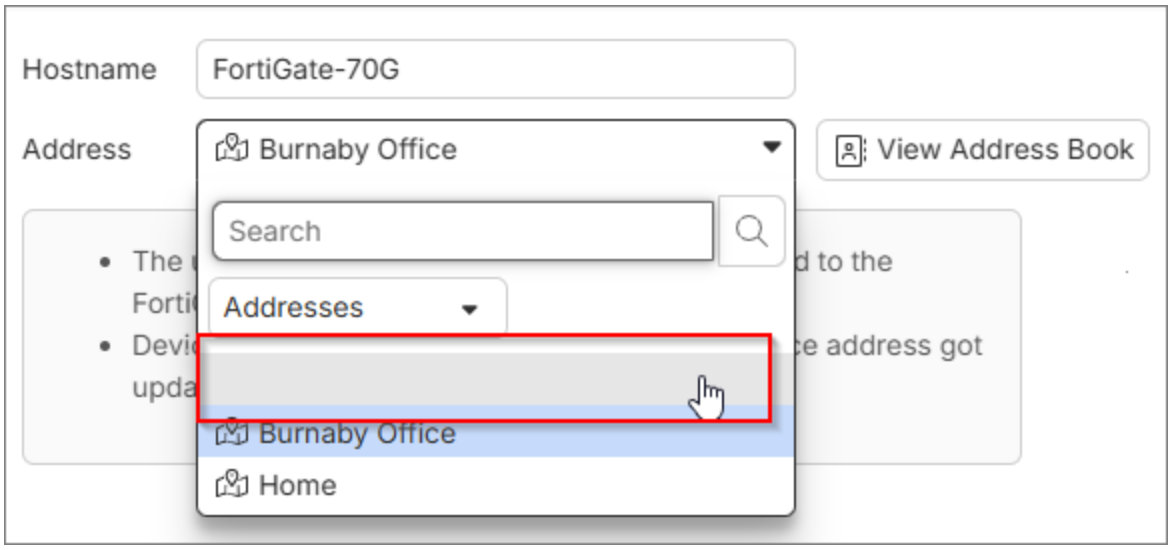
2. In the *Update Device Information* pane, click *View address book*.
3. In the address book dialog, click *Create new* to add a new address.
4. Enter the *Location name* (such as a region or site), the device address and country, then click *OK*.

To associate a device with an address:

1. Do one of the following:
   - In the *Device list*:
     - Select a device, click the *Actions* menu and select *Update Device Information*.
     - Hover over a device to view the device details and click *Update Device Information*.
   - In the *Device Map*, hover over a device on the map to view the device details and click *Update Device Information*.
2. In the *Update Device Information* pane, click the *Address* and select a location from the list.
3. Click *OK*.

To remove an associated address:

Select the top empty entry in the address drop-down list.



To edit an address:

1. In the *Update Device Information* pane, click *View address book*.
2. In the address book dialog, click *Edit* to modify an existing address.
3. Edit the device address and click *OK*.

Provisioning targets

The *Provisioning Targets* page lets you define where fabric managed devices will be provisioned to. After the target is created, the device will appear in the Provision target dropdown when you provision a FortiGate.

To create a provisioning target for FortiGate:

1. Go to *Devices and Provisioning* > *Provisioning Targets*.
2. Enable *FortiManager Cloud* or *FortiManager*.
3. Click *Add*.
4. In the *Serial Number* and *IP Address/FQDN* fields, enter the FortiManager details. If you are provisioning FortiGate to FortiManagers in a high availability (HA) pair, enter both nodes' serial numbers separated by a comma in the Serial Number field and one IP address (the virtual IP address or hostname) in the *IP Address/FQDN* field. FortiGate Cloud supports provisioning for FortiManager 7.2 HA.
5. Optionally, enable *Pre-run CLI* Script to choose a previously configured pre-run CLI script as the default for this FortiManager.
6. Click *OK*.

To create a provisioning target for FortiAP:

1. Go to *Devices and Provisioning* > *Provisioning Targets*.
2. Click the *FortiAP* tab.
3. Enable *FortiSASE*.
4. (Optional) Enable *External Controller*.
5. Click *Add*.
6. In the *IP Address/FQDN* fields, enter the address.
7. Click *OK*.

To create a provisioning target for FortiSwitch:

1. Go to *Devices and Provisioning* > *Provisioning Targets*.
2. Click the *FortiSwitch* tab.
3. Enable *FortiSASE*.
4. Click *OK*.

To create a provisioning target for FortiExtender:

1. Go to *Devices and Provisioning* > *Provisioning Targets*.
2. Click the *FortiExtender* tab.
3. Enable *FortiSASE*.

4. (Optional) Enable *External Controller*.

   FortiGate Cloud supports provisioning a FortiExtender to a FortiGate when the FortiExtender is operating in LAN extension mode. When LAN extension is enabled, only FortiExtenders running supported FortiOS versions with external LAN functionality are displayed.

5. Click *Add*.
6. In the *IP Address/FQDN* fields, enter the address.
7. Click *OK*.

Assigning provisioning targets

To assign a provisioning target:

1. Go to *Devices and Provisioning* > *Provisioning Targets*.
2. Select a device an *Unprovisioned* device in the list and click *Provision*.
3. Configure the *Serial Number(s)* and *Portal display time zone*.
4. Assign a target from the *Provision target* dropdown.
5. Click *OK*.

Firmware management

In 26.2, firmware profiles are only available for devices with a paid subscription.

Firmware management > *Firmware upgrade* lists FortiGates provisioned to FortiGate Cloud and groups FortiGates that belong to the same Fortinet Security Fabric. You can also view managed devices connected to the FortiGates. You can manage firmware upgrades. 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 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 but cannot use any FortiGate Cloud features. It stops uploading logs to FortiGate Cloud.

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 released more than seven days earlier, you must upgrade the FortiGate immediately. The FortiGate cannot use FortiGate Cloud features and does not upload logs to FortiGate Cloud until you upgrade it.

If the FortiOS version on a FortiGate reaches end of support (EOS), 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:
  - 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 *Firmware management* > *Firmware upgrade*.
2. Go to the desired tab.
3. Select the desired devices.
4. Click *Fabric upgrade*. For a non-FortiGate managed device, this option is only available if the device is authorized. See Authorizing managed devices on page 40.
5. For a non-FortiGate managed device, for *Select Firmware*, select one of the following:

Option	Description
Recommended	Upgrade the device to a recommended firmware version. The *Target version* dropdown list displays the recommended version to upgrade to.

Option	Description
File Upload	Browse to and upload the install file for the desired firmware version to upgrade to.

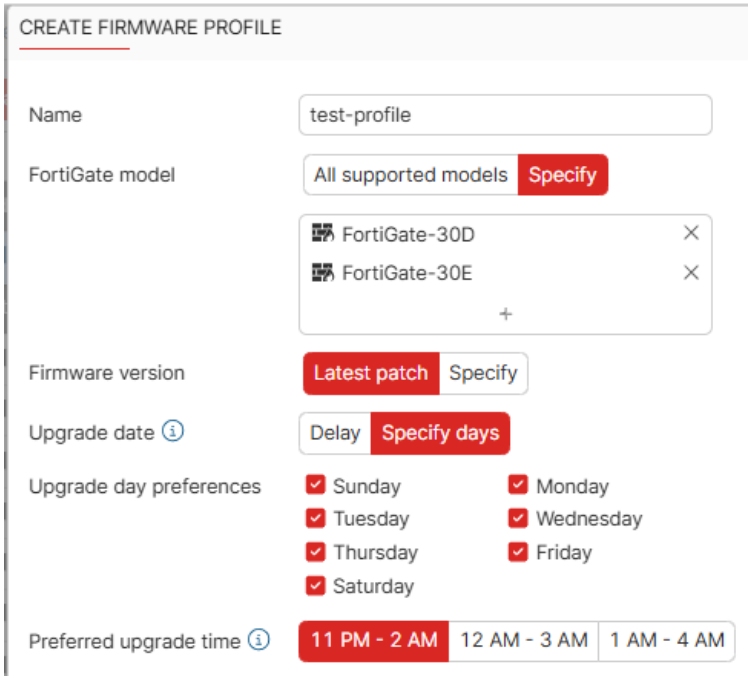
6. For *Upgrade schedule*, select *Immediate* or *Custom*. If you select *Custom*, configure the desired upgrade time.
7. Confirm that the dialog displays the desired firmware versions for each FortiGate. Click *OK*. FortiGate Cloud backs up the FortiGate configurations and upgrades the firmware as per the schedule that you configured. The upgrade reboots the FortiGates.

To upgrade EOS firmware:

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

To create a firmware profile:

1. Go to *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 *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.

To view firmware upgrade history:

Go to *Firmware management* > *Firmware upgrade history*. You can view a list of firmware upgrade tasks and information about them, such as the upgrade path and whether the task succeeded or failed. The list is sorted by device name, then date and time.

Configuration

In *Configuration* > *Revisions*, you can manage FortiGate revisions. This feature is only available for FortiGates with a subscription. For a FortiGate with a 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.

FortiGate Cloud masks user passwords and sensitive configuration data in backups that are downloaded or viewed.

To back up a configuration:

1. Go to *Configuration* > *Revisions*.
2. Click the desired FortiGate.
3. Click *Manage revisions*.
4. Click *Backup config*.

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*.

Option	Description
Session	The default session duration is 600 seconds. For example, if you modify FortiGate settings at 10:00 AM, FortiGate Cloud schedules an auto backup in 600 seconds. If no further setting changes occur within the 600 seconds, FortiGate Cloud performs an auto backup at 10:10 AM. However, if you make additional changes to the settings, for example, at 10:05 AM, this resets the timer and FortiGate Cloud schedules an auto backup for 600 seconds *after* 10:05 AM. FortiGate Cloud keeps every backup revision for all sessions in one day.
Daily	Automatically backs up the configuration once per day.
Weekly	Automatically backs up the configuration once per week.

7. (Optional) When a *Daily* or *Weekly* interval is selected, you can enable *Backup when config change* to perform an auto backup only if the configuration has changed. If no configuration changes occur during the interval, FortiGate Cloud does not perform the daily or weekly backup.

8. (Optional) Enable *Backup mail notification* to specify an email address that will receive a notification when a backup occurs. The notification email does not include a copy of the backup revision. From the *Mail notification language* dropdown list, select the desired language for the notification email.

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.

SD-WAN Overlay

SD-WAN overlay allows FortiGate devices to easily provision new SD-WAN overlay networks from FortiGate Cloud. SD-WAN overlay provides an easy-to-use GUI wizard that simplifies the process of configuring an SD-WAN overlay within a single region.

This feature requires a Standard subscription. See Subscription types on page 13.

The SD-WAN Overlay feature is supported only on FortiGate devices running FortiOS 7.4.4 or later.

The SD-WAN overlay hub acts as a bridge to allow overlay shortcuts to be formed between your spokes.

SD-WAN overlay and the spokes rely on Fortinet Technologies Inc.'s Auto-Discovery VPN (ADVPN), which allows the central hub to dynamically inform spokes about a better path for traffic between two spokes. ADVPN shortcut tunnels, also known as shortcuts, are formed between spokes, such as between branches and the data center, or between branches themselves so that traffic does not need to pass through the hub.

An Identity & Access Management user must have full read-write permission in the role-based access control profile to have admin access to SD-WAN overlay features.

Starting May 3, 2025, the FortiCloud IAM portal supports an individual SD-WAN Overlay role control under the FortiGate Cloud permission profile. Therefore, to have read-write or read-only access to the feature, you can configure it accordingly in the IAM portal.

This feature is available in the Global, U.S., and Europe regions. Availability for Japan will be announced at a later time.

Prerequisites

The prerequisites of using the SD-WAN overlay in the FortiGate Cloud portal are as follows:

- FortiOS 7.4.4 and later on the FortiGates acting as spokes.
- SD-WAN Overlay bundle subscriptions for all spokes.
- All spokes must be provisioned in FortiGate Cloud to the same account to which they are registered in FortiCare.
- Sites must be running FortiOS 7.6.0 or later to support security profiles.

For successful setup of ADVPN tunnels, the spokes' ISPs must allow traffic over UDP port 500 and UDP port 4500 for NAT traversal (NAT-T).

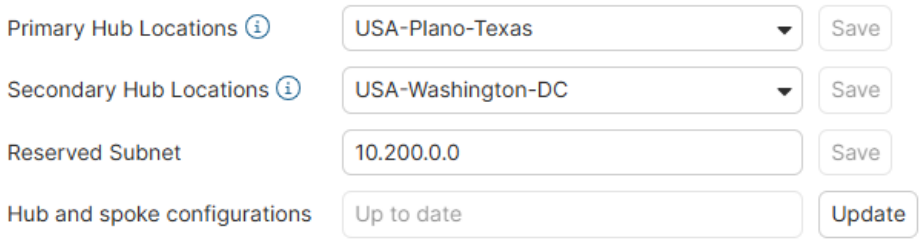
The SD-WAN overlay feature does not support FortiOS 7.6.1 or 7.6.2.

Creating the initial topology

The following provides instructions for creating a topology to provision the SD-WAN overlay configuration to your FortiGates.

To create the initial topology:

1. Go to *SDWan Overlay* > *Settings*.
2. Set up the hub locations:
   a. Use the *Primary Hub Locations* and *Secondary Hub Locations* dropdown lists to select your locations.



> Select locations that are nearest to your site as this provides the best connectivity and backup.

3. Add a site as Creating a site on page 52 describes.
4. Configure the site to include ISP and subnet settings as Editing a site on page 54 describes.
5. Repeat these steps to add another site configuration.

> Not all FortiGate sites must be configured at once. You can add new sites, ISPs, and LAN subnets after you apply the initial configuration. See Creating a site on page 52, Editing a site on page 54 and Provisioning the SD-WAN configuration to your sites and viewing tasks on page 50.

Provisioning the SD-WAN configuration to your sites and viewing tasks

You can add several sites with their corresponding ISP and subnets in *Site*. When you apply the changes, the configuration is provisioned to the FortiGates, and the SD-WAN network is configured. The status of each configuration within the topology is displayed in the *Tasks*.

To apply changes and view tasks:

1. Go to *SDWan Overlay* > *Site*.
2. Add the desired sites and their corresponding configuration. See Creating a site on page 52 and Editing a site on page 54
3. Go to *SDWan Overlay* > *Overlay policy*. Configure a desired policy. See Creating a policy on page 56.
4. Apply the policy. See Applying policies on page 59. The sync process runs in the background.
5. Go to *SDWan Overlay* > *Tasks* icon to view the status of each configuration task.

Failed configurations

If a configuration in the topology fails, the configuration will appear as red in *Tasks*. You can review information on the configuration to identify troubleshooting scenarios:

- For suggestions on how to successfully connect an asset, select *Details*.
- For information on the configuration, click *View Config*.

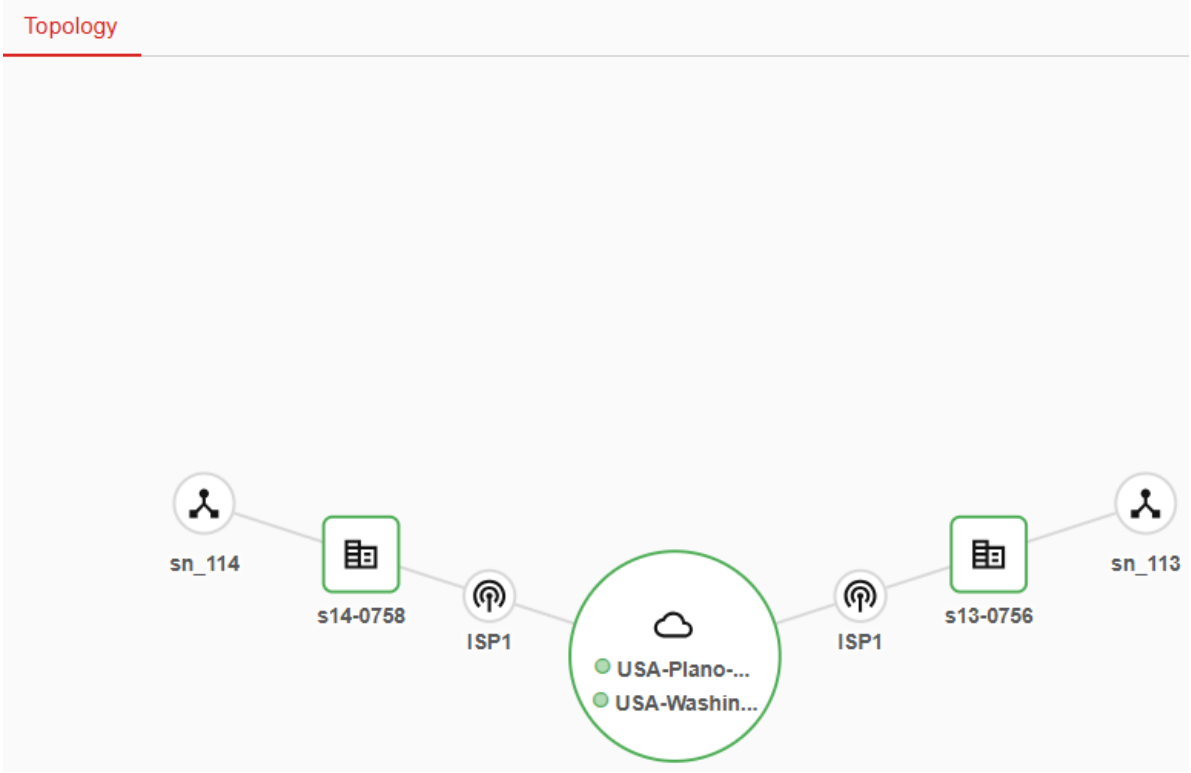
You can retry the connection for each asset from *Tasks* in case the issue has been resolved.

To retry a failed connection:

1. Go to *SDWan Overlay* > *Tasks* icon to view the status of each configuration task.
2. Identify the failed connection.
3. Click *Retry*. The *Retry Task* dialog is displayed.
4. Click *OK*.

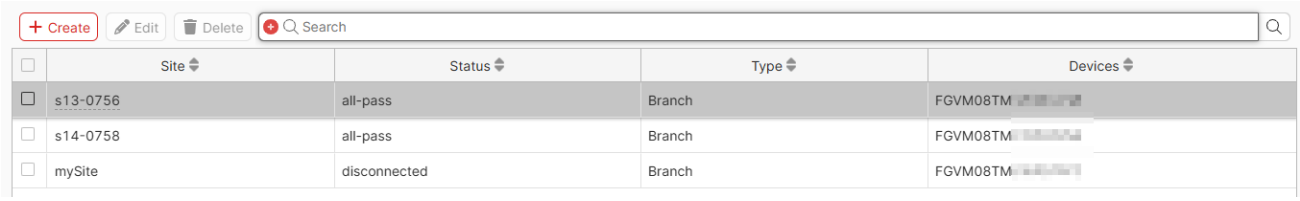
Topology

The *Topology* page displays the current configuration of the SD-WAN overlay hub and site FortiGates.



Site

In the *Site* page, you can view a table of the sites that have been added. You can also add more sites by clicking *Create* to enter the *New Site* dialog.



This section includes:

- Creating a site on page 52
- Editing a site on page 54
- Deleting sites on page 55

Creating a site

You can create a new site from the *Site*. SD-WAN sites are authorized FortiGate devices. Use SD-WAN overlay to add your FortiGates to the site. You can assign the site as:

Role	Description
Branch	Organization site that needs to access headquarter applications
Data center	Organization headquarters that maintain business applications

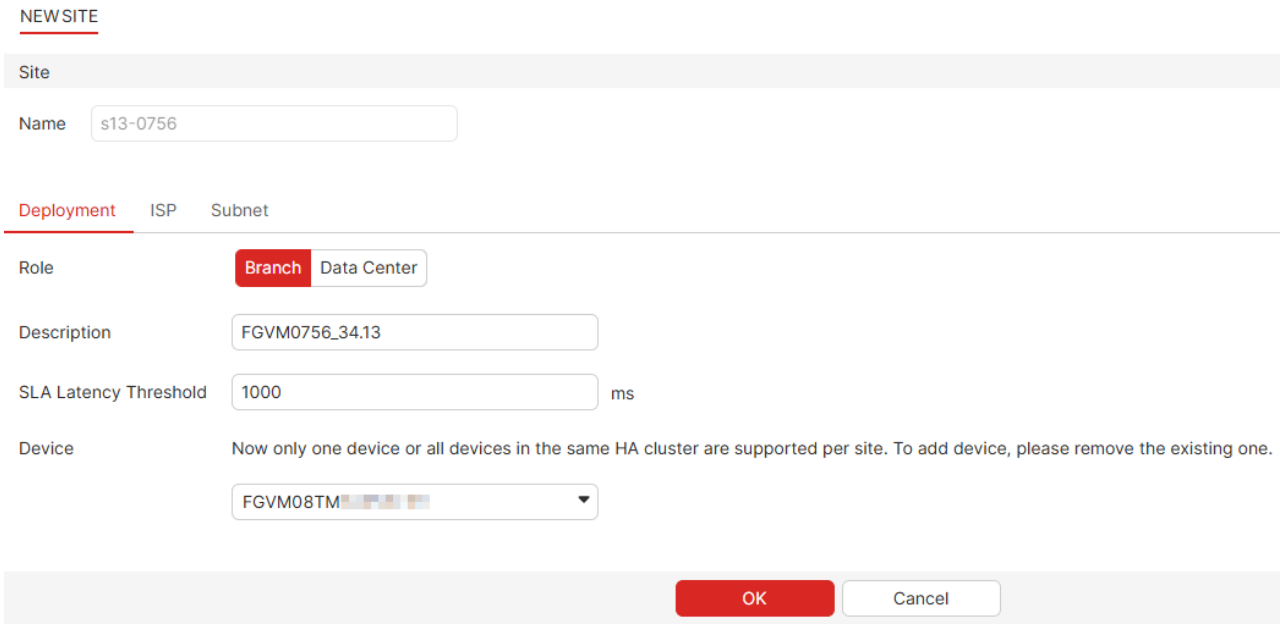
You must set the hub locations before you can add a new site. See Creating the initial topology on page 50.

To create a new site:

1. Go to *SDWan Overlay* > *Site*.
2. Click *Create*.
3. Enter the *Name*.
4. On the *Deployment* tab, set the site as a *Branch* or *Data Center*.
5. (Optional) Enter a *Description*.
6. Enter the *SLA Latency Threshold*.
7. Select the FortiGate device to provision from the *Device* dropdown menu.

   It is critical for the added FortiGate device to appear with a status of *Online*. If the device lacks a status of *Online*, check whether the device is:
   - Powered on.
   - Activated or logged in to FortiGate Cloud.
   - Configured and properly connected to its internet service provider's WAN link.

8. Click *OK*.



Adding HA clusters to sites

HA clusters that have been set up outside of FortiGate Cloud can be added to a site when selecting the *Device*. To implement an HA cluster in FortiGate Cloud, select the primary FortiGate as the *Device* when adding a site. The secondary FortiGate in the HA cluster will be added to the *Device List for Deployment*.

See High Availability in the FortiOS Administration guide for more information on HA clusters.

Editing a site

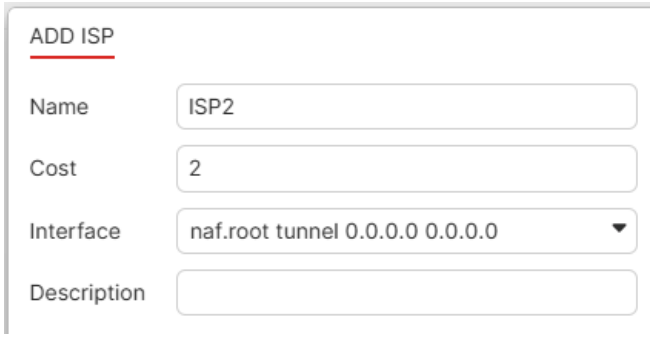
You can edit a site to define the ISP and LAN subnet from the *Site* page.

You can add LAN subnets that will communicate within your SD-WAN region. You can define subnets as either *direct* or *indirect*:

- *direct*: Directly select the subnet assigned to a FortiGate interface.
- *indirect*: Use a Classless Inter-Domain Routing (CIDR) prefix to input a network summary address behind the interface. You can create multiple indirect subnets behind the same interface, if needed.

To edit a new site:

1. Go to *SDWAN Overlay* > *Site*.
2. Select the desired site, then click *Edit*.
3. Configure how the SD-WAN device connects to the region by selecting the ISP link for external access.
   a. On the *ISP* tab, select *Create*. The *Add ISP* dialog opens.
   b. Enter a *Name* for the ISP.
   c. Enter the cost assigned to the ISP in the *Cost* field.
   d. Select the interface from the *Interface* dropdown list.
   e. (Optional) Enter a *Description*.



   f. Click *OK*. The ISP is added between the hub and site.
   g. Repeat the above steps to add another ISP configuration. SD-WAN overlay allows a maximum of three ISPs for each site.
4. Select the *Subnet* tab. Configure the following:
   a. Select *Create*. The *Add subnet* dialog opens.
   b. Enter a *Name*.
   c. Select *direct* or *indirect* for the subnet definition.

   d. Select the interface from the *Interface* dropdown list.
   e. If you select indirect, configure the CIDR as needed.
   f. Enable or disable *Advertise to Overlay*.
   g. (Optional) Enter a *Description*.
   h. Click *OK*. The subnet is added to the topology.
5. Click *OK*.

Deleting sites

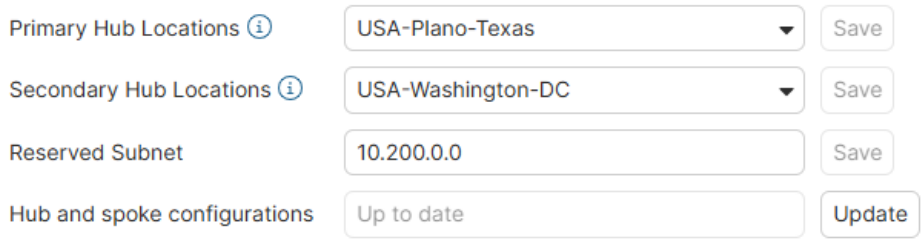
You can permanently remove a site FortiGate and connected LAN subnets from the *Site* page.

To delete a site:

1. Go to *SDWAN Overlay* > *Site* and identify the site you want to delete.
2. Select *Delete*. A confirmation message displays.
3. Click *OK*.

Settings

In *Settings*, you can view the hub locations and the reserved subnet. You can modify settings as needed.



SD-WAN overlay uses a reserved subnet to provide IP addresses for the overlay network. Customers should not use this reserved subnet in their networks.

By default, SD-WAN overlay has reserved 10.200.0.0/16 for overlay IP addressing of all spokes, and you should not use this network in either the LAN subnets or WAN network. If you have a network conflict, you can modify the reserved subnet in the *Settings* within FortiGate Cloud.

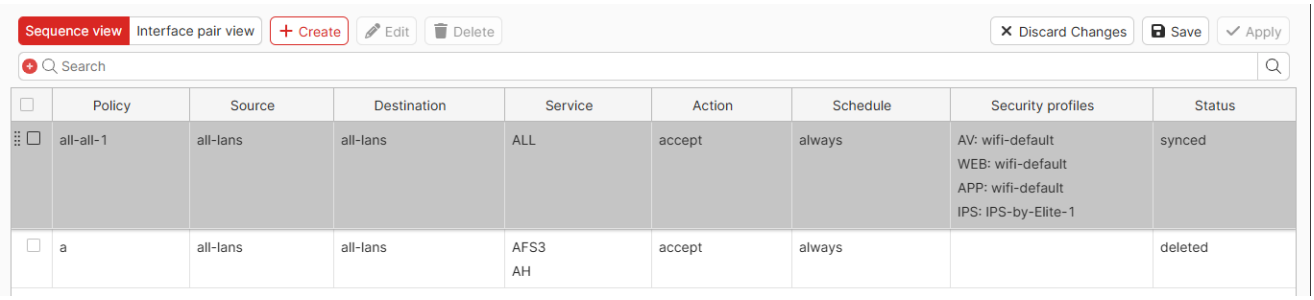
To edit settings:

1. Go to *SDWAN Overlay* > *Settings*.
2. Modify the following settings as desired:

Setting	Description
Primary Hub Locations	Modify the primary location using the dropdown menus. Click *Save*.
Secondary Hub Locations	Modify the secondary location using the dropdown menus. Click *Save*.
Reserved Subnet	Assign a different subnet if you have a network conflict with the default reserved subnet. Click *Save*.
Hub and spoke configurations	Push changes to the configuration of the hub and spokes. Confirm in the warning dialog.

Overlay policy

Centralized SD-WAN overlay policies can be created and managed in the *SDWAN Overlay* > *Overlay Policy* page. Overlay policies are policies whose source and destination can be in different sites, crossing overlay networks. For more information on policies, see Policies in the FortiOS Administration Guide.



This section includes:

- Creating a policy on page 56
- Viewing policies on page 58
- Applying policies on page 59
- Managing policies on page 59
- Policy example on page 60

Creating a policy

You can create new central policies from the *SDWan Overlay* > *Overlay Policy* page.

To create a new policy:

1. Go to *SDWan Overlay* > *Overlay Policy*.
2. Click *Create*.
3. Enter a *Name*.
4. Define the source:
   - To define a source address, select *Address*:
     i. Select the *Site* from the dropdown list.
     ii. Select the *Interface* from the dropdown list.
     iii. Select the *Address* from the dropdown list.

     > You can create a new address in the *SDWan Overlay* > *Addresses* page. See Creating an address on page 64.

   - To define a source address group, select *Address Group*:
     i. Select the *Address group* from the dropdown menu.

     > If there are no address groups listed, you can create a new address group in the *SDWan Overlay* > *Addresses* page. See Creating an address group on page 64.

5. Define the destination:
   - To define a destination address, select *Address*:
     i. Select the *Site* from the dropdown list.
     ii. Select the *Interface* from the dropdown list.
     iii. Select the *Address* from the dropdown list.

     > You can create a new address in the *SDWan Overlay* > *Addresses* page. See Creating an address on page 64.

   - To define a destination address group, select *Address Group*:
     i. Select the *Address Group* from the dropdown menu.

     > If there are no address groups listed, you can create a new address group in the *SDWan Overlay* > *Addresses* page. See Creating an address group on page 64.

6. Select the *Service*.

   > You can create a new service in the *SDWan Overlay* > *Services* page. See Creating a service on page 67.

7. Select the *Service Group*.

   > If there are no service groups listed, you can create a new service group in the *SDWan Overlay* > *Services* page. See Creating a service group on page 67.

8. Define the schedule of the policy:

- To define the schedule, select *Schedule*:
  i. Select the *Schedule* from the dropdown list.

  > You can create a new schedule in the *SDWan Overlay > Schedules* page. See Creating a recurring schedule on page 70 and Creating a one-time schedule on page 70.

- To define the schedule group, select *Schedule Group*:
  i. Select the *Schedule Group* from the dropdown list.

  > If there are no schedule groups listed, you can create a new schedule group in the *SDWan Overlay > Schedules* page. See Creating a schedule group on page 70.

9. Set the *Action* as *accept* or *deny*.
10. Select the *Security Profiles*.

    > Security profiles can be configured in the *SDWan Overlay > Security profiles* page. See Security profiles on page 73.

11. Define the *Logging Options*:
    a. Toggle *Log Allowed Traffic* and select *Security Events* or *All Sessions* to define which events to log.
    b. Enable *Generate Logs when Session Starts*, if needed.
12. (Optional) Enter a description for the policy.
13. Toggle *Enable this policy* to enable or disable the policy.
14. Click *OK*.

    > Once a policy has been created, it will appear in the *SDWan Overlay > Overlay policy* list with the *new* status. You must save and apply the policy to the spoke FortiGates before they will take effect. See Applying policies on page 59.

Viewing policies

Overlay policies are displayed in the in the *SDWan Overlay > Overlay Policy* page. Policies can be viewed in:

- *Sequence view*: Displays policies in the order that they are checked for matching traffic. The order can be changed by dragging and dropping policies into a new location in the list.
- *Interface pair view*: Displays policies in the order by the pairs of incoming and outgoing interfaces in collapsible sections.

For more information on *Sequence view* and *Interface pair view*, see Policy views in the FortiOS Administration Guide.

To filter policies:

1. Go to *SDWan Overlay > Overlay policy*.
2. In the *Search* bar, do one of the following:

   a. Click +, then select the filter criteria from the dropdown list. Select the filter definition from the dropdown list or enter the desired value to filter on.
   b. Type in the filter definition and value.
3. Configure additional filters as desired.
4. Click *Apply*.

Applying policies

The overlay policies must be saved and applied to the spoke FortiGates before they can take effect. Any edits made to a policy will not be pushed to the spokes until they have been applied.

To apply a policy:

1. Go to *SDWan Overlay* > *Overlay policy*.
2. Right-click the desired policy, then click *Save*. The *Status* will change to *unapplied*.
3. Right-click the policy, then click *Apply*. The *Status* will change to *synced*.

Managing policies

Policies can be edited and deleted in the *SDWan Overlay* > *Overlay policy* page.

To edit a policy:

1. Go to *SDWan Overlay* > *Overlay policy*.
2. Find the policy you want to update, then select *Edit*.
3. Make the edits and click *OK*. The Status will change to *modified*.

   Right-click the policy, then select *Discard Changes* to undo any edits made.

4. Right-click the policy, then click *Save*. The *Status* will change to *unapplied*.
5. Right-click the policy, then click *Apply*. The *Status* will change to *synced*.

To delete a policy:

1. Go to *SDWan Overlay* > *Overlay policy*.
2. In *Sequence View*, select the policy you want to delete.
3. Click *Delete*.
4. Click *OK* in the confirmation dialog.

Policy example

Given a topology that has already been previously orchestrated using the *SDWan Overlay*, the following example demonstrates how to create overlay policies between two FortiGate sites in that topology using these steps:

1. Configure an overlay policy to allow traffic from the Datacenter LAN (10.1.100.0/24) to the Branch 1 LAN (10.1.1.0/24).
2. Test and verify connectivity from the Datacenter LAN to the Branch 1 LAN.
3. Test and verify connectivity from the Branch 1 LAN and the Datacenter LAN is not allowed by the overlay policy configured in Step 1.
4. Configure an overlay policy to allow traffic from the Branch 1 LAN (10.1.1.0/24) to the Datacenter LAN (10.1.100.0/24).
5. Test and verify connectivity from the Branch 1 LAN to the Datacenter LAN.

For granularity, overlay policies are destined for the source and destination specified only. Therefore, an overlay policy from site A crossing overlay networks to site B does not automatically allow traffic in the opposite direction from site B to site A. You must create a separate overlay policy for traffic in the opposite direction between sites.

To configure an overlay policy to allow traffic from the Datacenter LAN to the Branch 1 LAN:

1. Go to *SDWan Overlay* > *Overlay policy*.
2. Click *Create*.
3. Configure the policy as follows:

Name		DCport3-to-Br1port3
Source		Address
	Site	Datacenter
	Interface	port3 10.1.100.0/24
	Address	port3@Datacenter
Destination		Address
	Site	Branch-1
	Interface	port3 10.1.1.0/24
	Address	port3@Branch-1
Service		ALL
Service Group		
Schedule/Schedule Group		Schedule
Schedule		always

Action		accept
Security Profiles		
	AntiVirus	default
	Web Filter	default
	Application Control	default
	Intrusion Prevention	default
Logging Options		
	Log Allowed Traffic	Enabled, All Sessions
	Generate Logs when Session Starts	Disabled
	Description	DC port3 to Br1 port3
Enable this policy		Enabled

4. Click *OK*.
5. In *SDWan Overlay > Overlay policy*:
   a. Status is *new*. Right-click the policy, then click *Save*.
   b. Status is *unsynced*. Right-click the policy, then click *Apply*.
   c. Status is *synced*. The policy has been applied to the FortiGate devices in the specified sites.

To test and verify connectivity from the Datacenter LAN to the Branch 1 LAN:

1. Run these CLI commands on the Datacenter FortiGate:

```
# execute ping-options source <IP address in Datacenter LAN>
# execute ping <IP address in Branch 1 LAN>
```

2. Observe the following output:

```
Datacenter# execute ping-options source 10.1.100.1

Datacenter# execute ping 10.1.1.99
PING 10.1.1.99 (10.1.1.99): 56 data bytes
64 bytes from 10.1.1.99: icmp_seq=0 ttl=255 time=0.7 ms
64 bytes from 10.1.1.99: icmp_seq=1 ttl=255 time=2.7 ms
64 bytes from 10.1.1.99: icmp_seq=2 ttl=255 time=1.2 ms
64 bytes from 10.1.1.99: icmp_seq=3 ttl=255 time=1.9 ms
64 bytes from 10.1.1.99: icmp_seq=4 ttl=255 time=0.6 ms

--- 10.1.1.99 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.6/1.4/2.7 ms
```

To test and verify connectivity from the Branch 1 LAN and the Datacenter LAN is not allowed by the overlay policy:

1. Run these CLI commands on the Branch 1 FortiGate:

```
# execute ping-options source <IP address in Branch 1 LAN>
# execute ping <IP address in Datacenter LAN>
```

2. Observe the following output:

```
Branch-1# execute ping-options source 10.1.1.99

Branch-1# execute ping 10.1.100.1
PING 10.1.100.1 (10.1.100.1): 56 data bytes

--- 10.1.100.1 ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss
```

To configure an overlay policy to allow traffic from the Branch 1 LAN to the Datacenter LAN:

1. Go to *SDWan Overlay > Overlay policy*.
2. Configure the policy as follows:

Name		Br1port3-to-DCport3
Source		Address
	Site	Branch-1
	Interface	port3 10.1.1.0/24
	Address	port3@Branch-1
Destination		Address
	Site	Datacenter
	Interface	port3 10.1.100.0/24
	Address	port3@Datacenter
Service		ALL
Service Group		
Schedule/Schedule Group		Schedule
Schedule		always
Action		accept
Logging Options		
	Log Allowed Traffic	Enabled, All Sessions

	Generate Logs when Session Starts	Disabled
	Description	
Enable this policy		Enabled

3. Click *OK*.
4. In *SDWan Overlay* > *Overlay policy*:
   a. Status is *new*. Right-click the policy, then click *Save*.
   b. Status is *unsynced*. Right-click the policy, then click *Apply*.
   c. Status is *synced*. The policy has been applied to the FortiGate devices in the specified sites.

To test and verify connectivity from the Branch 1 LAN to the Datacenter LAN:

1. Run these CLI commands on the Branch 1 FortiGate:

```
# execute ping-options source <IP address in Branch 1 LAN>
# execute ping <IP address in Datacenter LAN>
```

2. Observe the following output:

```
Branch-1# execute ping-options source 10.1.1.99

Branch-1# execute ping 10.1.100.1
PING 10.1.100.1 (10.1.100.1): 56 data bytes
64 bytes from 10.1.100.1: icmp_seq=0 ttl=254 time=50.6 ms
64 bytes from 10.1.100.1: icmp_seq=1 ttl=255 time=0.4 ms
64 bytes from 10.1.100.1: icmp_seq=2 ttl=255 time=0.5 ms
64 bytes from 10.1.100.1: icmp_seq=3 ttl=255 time=0.7 ms
64 bytes from 10.1.100.1: icmp_seq=4 ttl=255 time=0.4 ms

--- 10.1.100.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.4/10.5/50.6 ms
```

Addresses

Address objects and groups can be creating and managed in the *Addresses* pages. The addresses can be used in an overlay policy to identify the source and destination of the traffic flow. For more information about address objects and groups, see Address objects in the FortiOS Administration Guide.

Addresses created in the *Addresses* > *Address* page can be added to address groups in the *Address Group* tab.

Subnet addresses will be automatically added to the address list when you add a subnet to your topology. See Creating the initial topology on page 50 and Editing a site on page 54 for more information.

This section includes:

- Creating an address on page 64
- Creating an address group on page 64
- Managing address objects and groups on page 65

Creating an address

You can create new addresses to add to overlay policies in the *Addresses* > *Address* page.

You can implement addresses in an address group. See Creating an address group on page 64.

To create a new address:

1. Go to *SDWan Overlay* > *Addresses*.
2. Select the *Address* tab.
3. Click *Create*.
4. Enter a *Name*.
5. Select the *Type* from the dropdown list.
6. Select the *Site* from the dropdown list.
7. Select the *Interface* from the dropdown list.
8. If you selected *IP Range*, enter the IP address range in the *IP/Netmask* field.
9. (Optional) Enter a *Description* for the address.
10. Click *OK*.

Creating an address group

You can create a new address group to be used in an overlay policy in the *Addresses* > *Address group* page. An address group is a group of address objects that can be used in an overlay policy to identify the source and destination of traffic flow.

To create a new address group:

1. Go to *SDWan Overlay* > *Addresses*.
2. Select the *Address Group* tab.
3. Click *Create*.
4. Enter a *Name*.
5. In the *Members* field, click *+* to add address objects.

6. In the *Select Entries* pane, select the desired addresses. See Creating an address on page 64 for how to create an address.
7. (Optional) Enter a *Description* for the address group.
8. Click *OK*.

Managing address objects and groups

You can edit or delete existing addresses and address groups in the *Addresses* page.

To edit an address:

1. Go to *SDWan Overlay* > *Addresses*.
2. Select the *Address* tab.
3. For the address you want to edit, select *Edit*.
4. Make your updates.
5. Click *OK*.

To edit an address group:

1. Go to *SDWan Overlay* > *Addresses*.
2. Select the *Address Group* tab.
3. For the address group you want to edit, select *Edit*.
4. Make your updates.
5. Click *OK*.

To delete an address:

1. Go to *SDWan Overlay* > *Addresses*.
2. Select the *Address* tab.
3. For the address you want to delete, select *Delete*.
4. Click *OK* in the confirmation dialog.

You cannot delete an address if it is being used in an address group.

To delete an address group:

1. Go to *SDWan Overlay* > *Addresses*.
2. Select the *Address Group* tab.
3. For the address you want to delete, select *Delete*.
4. Click *OK* in the confirmation dialog.

IPAM

This feature requires a site to be running FortiOS 7.4.5 and above. Major version 7.6.0 and above is not currently supported.

IP address management (IPAM) can be configured in the *SDWan Overlay > IPAM* page. For information on IPAM, see Configure IPAM locally on the FortiGate in the FortiOS Administration Guide.

Configuring IPAM

New IPAM can be configured in the *SDWan Overlay > IPAM* page.

To configure IPAM:

1. Go to *SDWan Overlay > IPAM*.
2. Click *Create*.
3. Enter the *Name*.
4. Enter the *IP/Mask*.
5. Enter a *Description*, if desired.
6. Click *OK*.

Managing IPAM

You can edit and delete existing IPAM instances from the *SDWan Overlay > IPAM* page. When editing an IPAM instance, you can also reset the IPAM landscape.

To edit an IPAM instance:

1. Go to *SDWan Overlay > IPAM*.
2. Select the desired IPAM instance.
3. Click *Edit*.
4. Edit the configuration.
5. Click *OK*.

To delete an IPAM instance:

1. Go to *SDWan Overlay > IPAM*.
2. Select the desired IPAM instance.
3. Click *Delete*. A confirmation dialog is displayed.
4. Click *OK*.

Services

Services can be managed from the *SDWan Overlay* > *Services* page. See Firewall policy in the FortiOS Administration guide for more information on services.

Services created in the *SDWan Overlay* > *Services* page can be implemented in service groups displayed in the *Service group* tab.

This section includes:

- Creating a service on page 67
- Creating a service group on page 67
- Creating a service category on page 68
- Managing services on page 68

Creating a service

Service protocols can be created in the *SDWan Overlay* > *Services* page.

To create a service:

1. Go to *SDWan Overlay* > *Services*.
2. Select the *Service* tab.
3. Click *Create*.
4. Enter a *Name*.
5. Select a *Category* from the dropdown list.

   Service categories can be created in the *Service Category* tab. See Creating a service category on page 68.
6. Select a *Protocol Type* from the dropdown list:
7. Enter the protocol particulars in the new fields.
8. (Optional) Enter a *Description* of the protocol.
9. Click *OK*.

Creating a service group

Service protocols can be combined into a service group.

To create a service group:

1. Go to *SDWan Overlay* > *Services*.
2. Select the *Service group* tab.
3. Click *Create*.

4. Enter a *Name*.
5. In the *Service Group Members* field, click + to add service group members.
6. In the *Select Entries* pane, select the desired services.
7. (Optional) Enter a *Description* for the address group.
8. Click *OK*.

Creating a service category

You can create new service categories to be used in service protocols.

To create a new service category:

1. Go to *SDWan Overlay* > *Services*.
2. Select the *Service category* tab.
3. Click *Create*.
4. Enter a *Name*.
5. Enter a description of the service category.
6. Click *OK*.

Managing services

You can edit or delete services, service groups, and service categories in the *SDWan Overlay* > *Services* page.

To edit a service:

1. Go to *SDWan Overlay* > *Services*.
2. Select the *Service* tab.
3. Find the service you want to edit and select *Edit*.
4. Make your updates.
5. Click *OK*.

To edit a service group:

1. Go to *SDWan Overlay* > *Services*.
2. Select the *Service group* tab.
3. Find the service group you want to edit and select *Edit*.
4. Make your updates.
5. Click *OK*.

To edit a service category:

1. Go to *SDWan Overlay* > *Services*.
2. Select the *Service category* tab.

3. Find the category you want to edit and select *Edit*.
4. Make your updates.
5. Click *OK*.

To delete a service:

1. Go to *SDWan Overlay* > *Services*.
2. Select the *Service* tab.
3. Find the service you want to delete and select *Delete*.
4. Click *OK* in the confirmation dialog.

You cannot delete a service if it is being used in a service group.

To delete a service group:

1. Go to *SDWan Overlay* > *Services*.
2. Select the *Service group* tab.
3. Find the service group you want to delete and select *Delete*.
4. Click *OK* in the confirmation dialog.

To delete a service category:

1. Go to *SDWan Overlay* > *Services*.
2. Select the *Service category* tab.
3. Find the category you want to delete and select *Delete*.
4. Click *OK* in the confirmation dialog.

You cannot delete a category if it is being used in a service.

Schedules

Policy schedules can be created and managed in the *SDWan Overlay* > *Schedules* page. Schedules can be recurring or one-time occurrences, or a combination in a schedule group.

This section includes:

- Creating a recurring schedule on page 70
- Creating a one-time schedule on page 70
- Creating a schedule group on page 70
- Managing schedules on page 71

Creating a recurring schedule

You can create a policy schedule that recurs at specific days and times in the *SDWan Overlay > Schedules* page. This schedule will continue to recur in the assigned policy until it is removed or edited.

To create a recurring schedule:

1. Go to *SDWan Overlay > Schedules*.
2. Select the *Recurring schedule* tab.
3. Click *Create*.
4. Enter a *Name*.
5. Specify the *Days*:
   - Select *All days* if the schedule should occurs every day of the week.
   - Select *Specify* to select specific days of the week for the schedule to occur.
6. Specify the *Time*:
   - Select *All day* if the schedule should occurs for 24 hours.
   - Select *Specify* to set a *Start* and *Stop* time.
7. Click *OK*.

Creating a one-time schedule

You can create a one-time schedule event in the *SDWan Overlay > Schedules* page.

To create a one-time schedule:

1. Go to *SDWan Overlay > Schedules*.
2. Select the *One-Time schedule* tab.
3. Click *Create*.
4. Enter a *Name*.
5. Specify the *Start Date* and time.
6. Specify the *End Date* and time.
7. If you would like an event log to occur before the expiration of the schedule, enable *Pre-expiration event log* and specify the *Number of days before* expiration.
8. Click *OK*.

Creating a schedule group

You can create a schedule group from a combination of recurring and one-time schedules in the *SDWan Overlay > Schedules* page.

To create a schedule group:

1. Go to *SDWan Overlay > Schedules*.
2. Select the *Schedule group* tab.
3. Click *Create*.
4. Enter a *Name*.
5. In the *Schedule Group Members* field, click *+* to select the desired schedules from the *Select Entries* pane.

   For information on creating schedules that can be added to an schedule group, see Creating a recurring schedule on page 70 and Creating a one-time schedule on page 70.

6. Click *OK*.

Managing schedules

You can edit and delete schedules and schedule groups from the *SDWan Overlay > Schedules* page.

To edit a recurring schedule:

1. Go to *SDWan Overlay > Schedules*.
2. Select the *Recurring schedule* tab.
3. Find the schedule you want to edit and select *Edit*.
4. Make your updates.
5. Click *OK*.

To edit a one-time schedule:

1. Go to *SDWan Overlay > Schedules*.
2. Select the *One-Time schedule* tab.
3. Find the schedule you want to edit and select *Edit*.
4. Make your updates.
5. Click *OK*.

To edit a schedule group:

1. Go to *SDWan Overlay > Schedules*.
2. Select the *Schedule group* tab.
3. Find the schedule group you want to edit and select *Edit*.
4. Make your updates.
5. Click *OK*.

To delete a recurring schedule:

1. Go to *SDWan Overlay > Schedules*.
2. Select the *Recurring schedule* tab.

3. Find the schedule you want to delete and select *Delete*.
4. Click *OK* in the confirmation dialog.

> You cannot delete a schedule if it is being used in a schedule group.

To delete a one-time schedule:

1. Go to *SDWan Overlay* > *Schedules*.
2. Select the *One-Time schedule* tab.
3. Find the schedule you want to delete and select *Delete*.
4. Click *OK* in the confirmation dialog.

> You cannot delete a schedule if it is being used in a schedule group.

To delete a schedule group:

1. Go to *SDWan Overlay* > *Schedules*.
2. Select the *Schedule group* tab.
3. Find the schedule group you want to delete and select *Delete*.
4. Click *OK* in the confirmation dialog.

IP Pools

IP pools are a mechanism that allows sessions leaving the FortiGate firewall to use NAT. IP pools can be configured in the *SDWan Overlay* > *IP Pools* page. For more information on IP pools, see Static SNAT, Dynamic SNAT, and Central SNAT in the FortiOS Administration Guide.

Once an IP pool is configured, it can be implemented when configuring overlay policies to be applied to the FortiGate devices. See Creating a policy on page 56.

> This feature requires a site to be running FortiOS 7.4.5 and above. Major version 7.6.0 and above is not currently supported.

This section includes:

- Creating an IP pool on page 72
- Managing IP pools on page 73

Creating an IP pool

You can create a new IP pool in the *SDWan Overlay* > *IP Pools* page.

To create an IP pool:

1. Go to *SDWan Overlay > IP Pools*.
2. Click *Create*.
3. Enter the *Name*.
4. Enter a *Description*, if desired.
5. Select the *Type*.
6. Enter the IP address and range information as needed.

   The IP address and range field differ depending on the selected *Type*. For more information on each *Type*, see Dynamic SNAT in the FortiOS Administration Guide.

7. Enable or disabled *ARP Reply*.
8. Click *OK*.

Managing IP pools

You can edit or delete existing IP pools in the *SDWan Overlay > IP Pools* page.

To edit an IP pool:

1. Go to *SDWan Overlay > IP Pools*.
2. Select the desired IP pool.
3. Click *Edit*.
4. Edit the fields as desired.
5. Click *OK*.

To delete an IP pool:

1. Go to *SDWan Overlay > IP Pools*.
2. Select the desired IP pool.
3. Click *Delete*. A confirmation dialog is displayed.
4. Click *OK*.

Security profiles

Security profiles configurations can be managed from *SDWan Overlay > Security profiles*. See Security Profiles in the FortiOS Administration Gudide for more information.

Sites must be running FortiOS 7.6.0 or later to support security profiles. See Prerequisites on page 49.

The security profiles available include:

- AntiVirus on page 74
- Web Filter on page 75
- Application Control on page 75
- Intrusion Prevention on page 76
- Application signatures on page 77
- IPS signatures on page 77

AntiVirus

Antivirus security profiles can be created and managed from *SDWan Overlay* > *Security profiles* > *AntiVirus* tab. See Antivirus in the FortiOS Administration Guide for more information.

To create an antivirus security profile:

1. Go to the *SDWan Overlay* > *Security profiles* > *AntiVirus* tab.
2. Click *Create*. The *New AntiVirus Profile* page is displayed.
3. Enter the *Name*.
4. Enter a *Description*.
5. Enable *AntiVirus scan*. This feature cannot be enabled until the security profile is inspecting at least one protocol.
6. Enable the desired *Inspected Protocols*. An error is displayed until the scan options are defined in the next step.
7. Enable the desired *APT Protection Options*.
8. Enable the desired *Virus Outbreak Prevention* fields.
9. Click *OK*.

To edit a security profile:

1. Go to the *SDWan Overlay* > *Security profiles* > *AntiVirus* tab.
2. Select the desired profile.
3. Click *Edit*.
4. Edit the security profile as desired.
5. Click *OK*.

To delete a security profile:

1. Go to the *SDWan Overlay* > *Security profiles* > *AntiVirus* tab.
2. Select the desired profile.
3. Click *Delete*. A confirmation dialog is displayed.
4. Click *OK*.

Web Filter

Web filter security profiles can be created and managed from *SDWan Overlay > Security profiles > Web filter* tab. See Web filter in the FortiOS Administration Guide for more information.

To create a new web filter security profile:

1. Go to the *SDWan Overlay > Security profiles > Web filter* tab.
2. Click *Create*. The *New Web Filter Profile* page is displayed.
3. Enter the *Name*.
4. Enter a *Description*.
5. Enable the *FortiGuard Category Based Filter* and configure the filters. See FortiGuard filter in the FortiOS Administration Guide. To configure non-default actions for certain categories, select the category, then select the desired action.
6. Enable and configure the desired *Search Engines* parameters. See Search engines in the FortiOS Administration Guide.
7. Enable and configure the desired *Static URL Filter* parameters. See Static URL filter in the FortiOS Administration Guide.

   The *URL Filter* and *Content Filter* features require a site to be running FortiOS 7.4.6 and above. Major version 7.6.0 and above is not currently supported.

8. Enable the desired *Rating Options*.
9. Click *OK*.

To edit a security profile:

1. Go to the *SDWan Overlay > Security profiles > Web filter* tab.
2. Select the desired profile.
3. Click *Edit*.
4. Edit the security profile as desired.
5. Click *OK*.

To delete a security profile:

1. Go to the *SDWan Overlay > Security profiles > Web filter* tab.
2. Select the desired profile.
3. Click *Delete*. A confirmation dialog is displayed.
4. Click *OK*.

Application Control

Application control sensors can be created and managed from *SDWan Overlay > Security profiles > Application Control* tab. See Application control in the FortiOS Administration Guide for more information.

To create a new application control sensor:

1. Go to the *SDWan Overlay > Security profiles > Application Control* tab.
2. Click *Create*. The *New Application Sensor* page is displayed.
3. Enter the *Name*.
4. Enter a *Description*.
5. Edit the *Categories* as desired.
6. Enable *Network Protocol Enforcement*.
   a. Click *Create*.
   b. Configure the network service.
   c. Click *OK*.
7. Click *Create* for *Application Overrides*. See Basic category filters and overrides in the FortiOS Administration Guide.
   a. Configure the override.

      Application signatures can also be viewed in the *Policy > Security Profiles > Application Signatures* tab. See Application signatures on page 77.

   b. Click *OK*.
8. Enable the desired *Options*.
9. Click *OK*.

To edit a sensor:

1. Go to the *SDWan Overlay > Security profiles > Application Control* tab.
2. Select the desired sensor.
3. Click *Edit*.
4. Edit the sensor as desired.
5. Click *OK*.

To delete a sensor:

1. Go to the *SDWan Overlay > Security profiles > Application Control* tab.
2. Select the desired sensor.
3. Click *Delete*. A confirmation dialog is displayed.
4. Click *OK*.

Intrusion Prevention

Intrusion prevention security profiles can be created and managed from *SDWan Overlay > Security profiles > Intrusion prevention* tab. See Intrusion prevention in the FortiOS Administration Guide for more information.

To create a new IPS sensor:

1. Go to the *SDWan Overlay > Security profiles > Intrusion prevention* tab.
2. Click *Create*. The *New IPS Sensor* page is displayed.
3. Enter the *Name*.
4. Enter a *Description*.
5. Enable *Block malicious URLs*.
6. Click *Create* for *IPS Signatures and Filters*.
   a. Select the *Type*.
   b. Configure the filter or signature as required.

      IPS signatures are also listed in the *SDWan Overlay > Security profiles > IPS signatures* tab. See IPS signatures on page 77.

   c. Click *OK*.
7. Configure the *Botnet C&C* as desired.
8. Click *OK*.

To edit a sensor:

1. Go to the *Policy > Security Profiles > Intrusion Prevention* tab.
2. Select the desired sensor.
3. Click *Edit*.
4. Edit the security profile as desired.
5. Click *OK*.

To delete a sensor:

1. Go to the *SDWan Overlay > Security profiles > Intrusion Prevention* tab.
2. Select the desired sensor.
3. Click *Delete*. A confirmation dialog is displayed.
4. Click *OK*.

Application signatures

Application signatures can be viewed in the *SDWan Overlay > Security profiles > Application signatures* tab. Application signatures are required when configuring overrides in application control profiles. See Application Control on page 75.

IPS signatures

IPS signatures can be viewed in the *SDWan Overlay > Security profiles > IPS signatures* tab. IPS signatures are required when configuring signatures in IPS sensors. See IPS signatures on page 77.

Analytics

Analytics provide tools for monitoring and logging your device's traffic, providing you with centralized oversight of traffic and security events:

Reports	Generate and view reports of specific traffic data. You can configure FortiGate Cloud to generate reports at scheduled times and run reports on-demand as desired. See Reports on page 78.
Logs	View and download FortiOS traffic, security, and event logs. See Logs on page 83.
Incidents & Events	View event handlers and create notification profiles. Combine event handlers and notification profiles to create event handler stitches to add events to the *Event Monitor*. Raise select events to incidents for assignment and tracking. See Incidents & Events on page 85.
Log Archives	View an archive of raw logs. See Logs on page 83.
IoC	View alerts about newly found infections and threats to devices in the network. See IoC on page 90.

Reports

To schedule a report:

1. Go to *Analytics* > *Reports* > *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. If desired, in *Custom report logo*, upload an image as the custom logo for the report.
6. In the *Schedule type* field, configure the desired schedule for the report.
7. If desired, enable *Send report to* and select an email address or email group to send the report to.
8. Click *OK*. FortiGate Cloud generates the report as per the configured schedule. You can view these reports in *Analytics* > *Generated reports*.

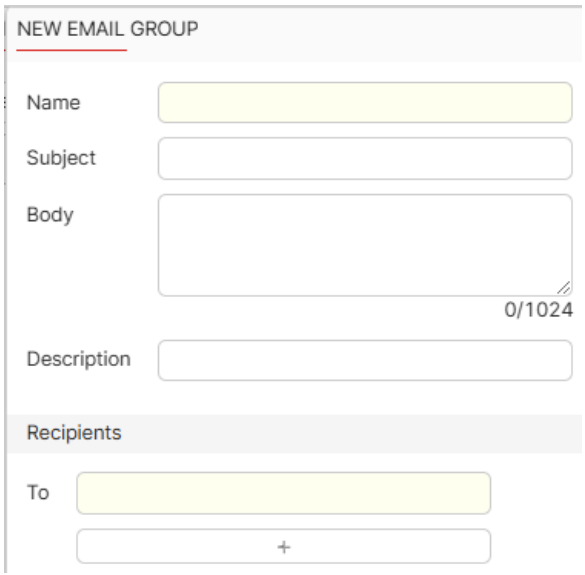
To run a report on-demand:

1. Go to *Analytics* > *Reports* > *Scheduled reports*.
2. Select the desired report, and 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 or email group to send the report to.

6. Click *OK*. FortiGate Cloud generates the report. You can view these reports in *Analytics* > *Generated reports*.

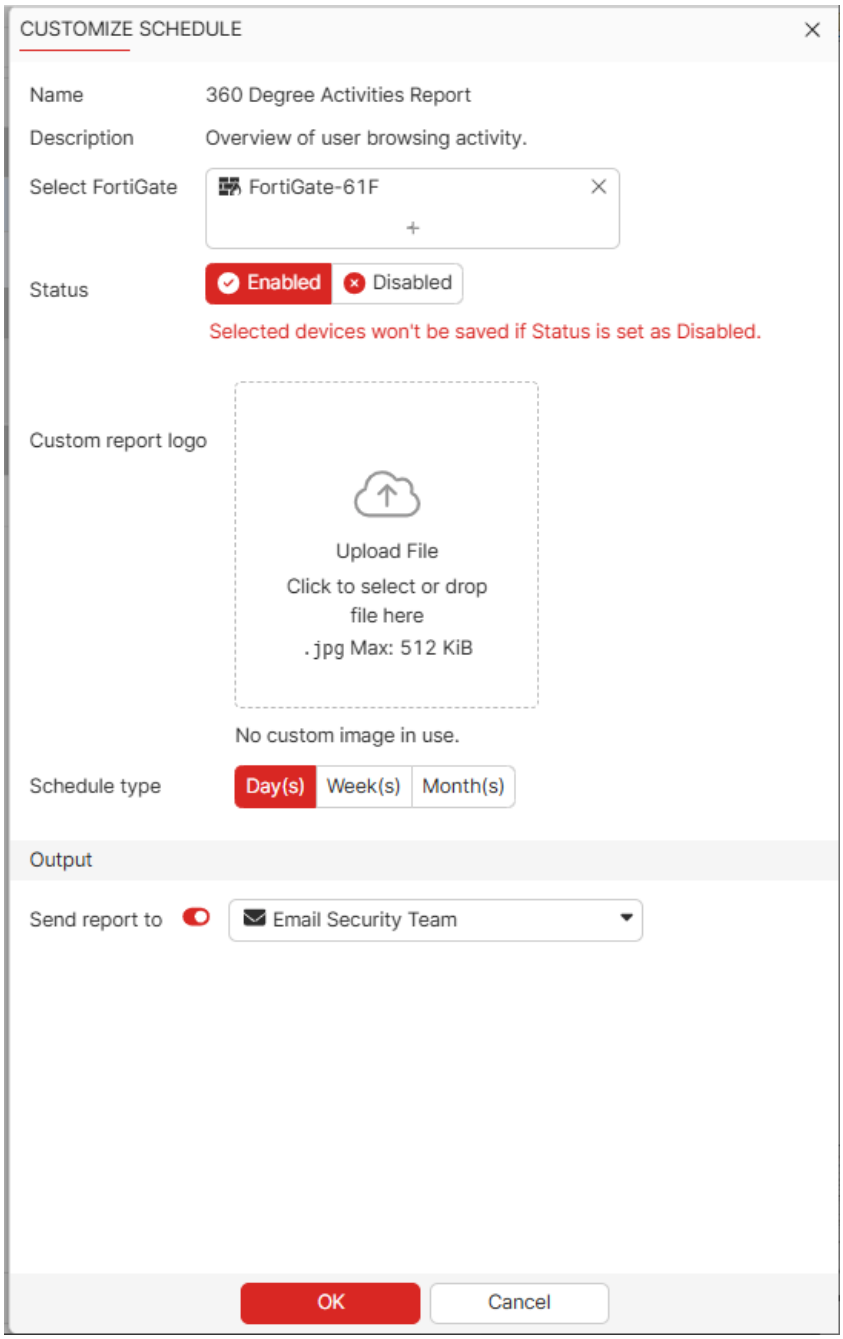
To configure an email group to send a report to:

1. Create an email group:
   a. Go to *Analytics* > *Reports* > *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 automatically runs this report weekly.

Reports for FortiGates with a subscription

You can schedule reports using a maximum of 10 report templates with a subscription. The following lists all available report templates:

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

- WiFi Report
- ZTNA 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.

FortiGate Cloud can display and export a maximum of 2000 rows of log data. If desired, you can download 40000 rows per log type (traffic, system, security, and so on) from the FortiGate itself by going to *Log & Report* and setting the source to FortiGate Cloud.

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

- Traffic:
  - Forward traffic
  - Local traffic
  - Multicast traffic
  - Sniffer traffic
  - Zero trust network access traffic
- Security:
  - Anomaly
  - Antispam
  - Antivirus
  - Application control
  - Data loss prevention
  - DNS query
  - File filter
  - Intrusion prevention
  - SSH
  - SSL
  - VoIP
  - Web application firewall
  - Web filter
- Events:
  - CIFS
  - Endpoint
  - General system
  - High availability
  - Router
  - SD-WAN
  - SDN connector
  - Security rating
  - User

- VPN
- Web proxy
- WiFi

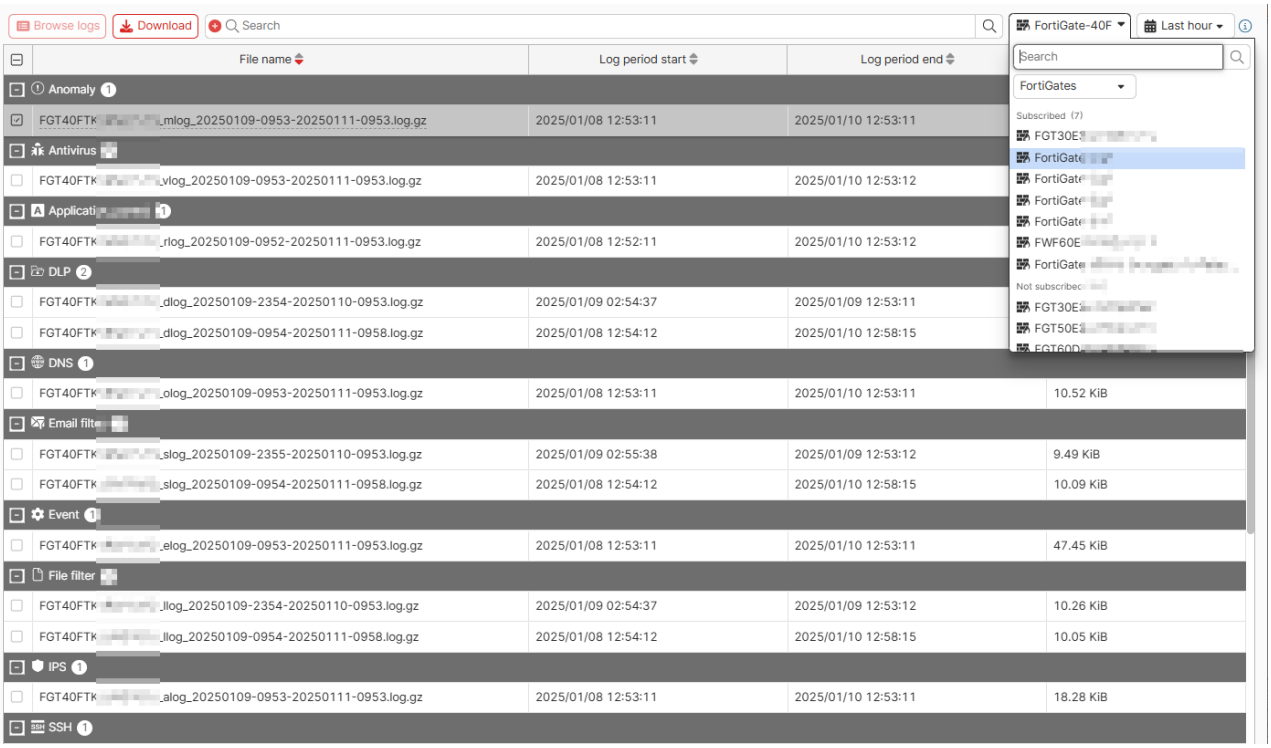
To download a log:

Downloading raw logs is available for FortiGates with a subscription.

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. Go to *Analytics* > *Log Archives* > *Raw logs*.
2. Select a subscription FortiGate from the dropdown list on the right, then select the desired log file.



3. Click *Browse logs*.

To export log data as a CSV file:

1. Go to *Analytics* > *Logs* and select the desired log type.
2. Click *Export to CSV*. A CSV file of the log data downloads to your device.

Incidents & Events

In *Incidents & Events*, you can generate, monitor, and manage alerts and events from logs.

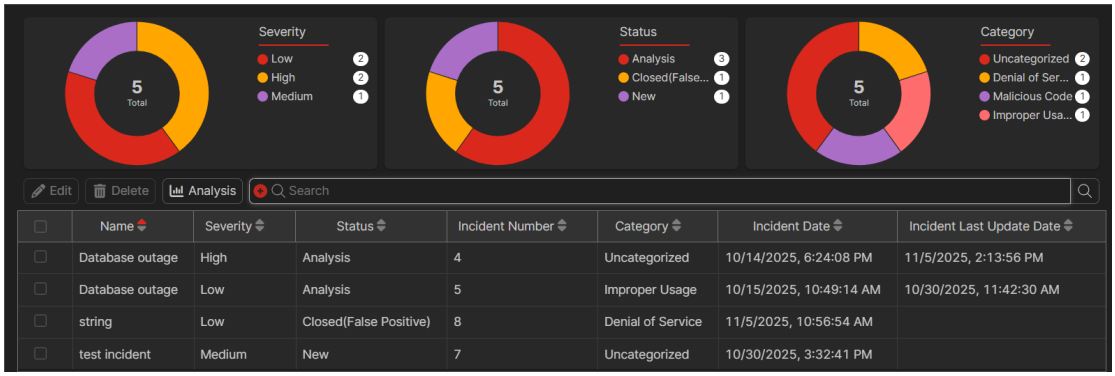
Incidents	View, edit, and analyze incidents created for events. See Incidents on page 85.
Event Monitor	View and monitor events generated by event handlers, and create incidents. See Event Monitor on page 87.
Event Handler	View predefined event handlers and create notification profiles. See Event Handler on page 88.
Automation	Create event handler stitches for FortiGates. Each stitch specifies what action to automatically take for an event handler on a FortiGate. See Automation on page 89.

Following is a summary of the workflow:

1. On the *Event Handler* page, create a notification profile.
2. On the *Automation* page, create an event handler stitch to combine an event handler with an action. The event handler stitches are used to create events on the *Event Monitor* page.
3. On the *Event Monitor* page, review events and create incidents.
4. On the *Incidents* page, assign and track incidents.

Incidents

The *Analytics* > *Incidents & Events* > *Incidents* page displays all incidents created to track and analyze events.



Charts at the top of the page display:

Chart	Description
Severity	Displays the total number of incidents and the number of incidents for each severity: • Low

Chart	Description
	• Medium • High • Critical Click the chart to filter the page. Click the *Filter* icon beside *Severity* to remove the filter.
Status	Displays the total number of incidents and the number of incidents for each status: • Analysis • Response • Closed (Remediated) • Closed (False Positive) • Not Assigned Click the chart to filter the page. Click the *Filter* icon beside *Status* to remove the filter.
Category	Displays the total number of incidents and the number of incidents per category: • Unauthorized Access • Denial of Service • Malicious Code • Improper Usage • Scans/Probes/Attempted Access • Uncategorized Click the chart to filter the page. Click the *Filter* icon beside *Category* to remove the filter.

Hover the mouse over a column heading to display:

- *Configure Table* icon: Click to choose which columns to display in the table.
- *Filter* icon: Click to access filter options for the column. May not be available for all columns.

To view incident analysis:

1. Go to *Analytics* > *Incidents & Events* > *Incidents*.
2. Select an incident and click *Analysis*.
   A summary of the incident is displayed as well as the associated event(s).
3. When done, click *Back*.

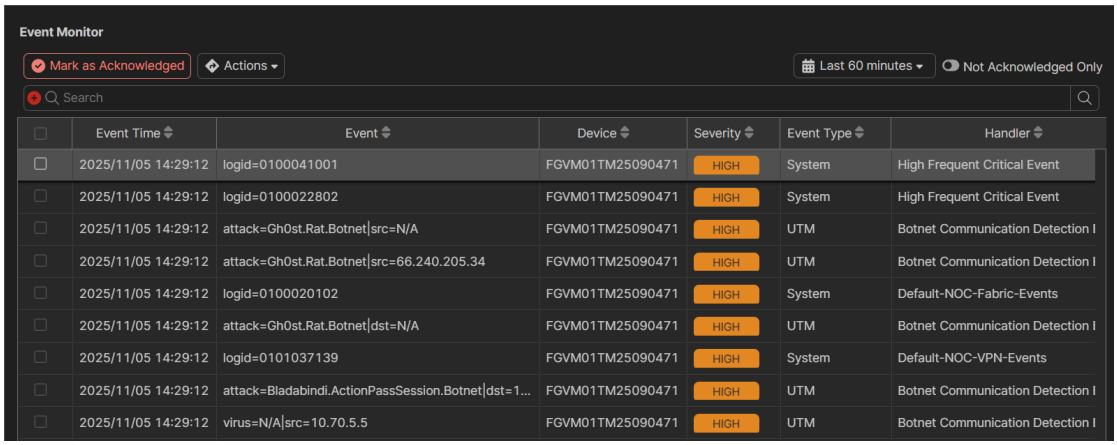
To edit an incident:

1. Go to *Analytics* > *Incidents & Events* > *Incidents*.
2. Select an incident and click *Edit*.
3. Edit the following options, and click *OK*:

- Name
- Incident Category
- Severity
- Status
- Description
- Assigned To

Event Monitor

After event handlers start generating events, the events display on *Event Monitor*.



To create an incident:

1. Go to *Analytics* > *Incidents & Events* > *Event Monitor*.
2. Select one or more incidents, and click *Actions*.
3. Choose one of the following options:
   - *Create New Incident*
   - *Add to Existing Incident*

To acknowledge an event:

1. Go to *Analytics* > *Incidents & Events* > *Event Monitor*.
2. Select one or more incidents and click *Acknowledge*. A confirmation dialog box displays.
3. Click *OK*.

To clone a preconfigured event handler:

1. Go to *Analytics* > *Incidents & Events* > *Event Monitor*.
2. Select one or more incidents and click *Clone*. A confirmation dialog box displays.
3. Click *OK*.

Event Handler

On *Analytics* > *Incidents & Events* > *Event Handler*, you can view event handlers and create notification profiles for events.

To view event handlers:

1. Go to *Analytics* > *Incidents & Events* > *Event Handler*. The list of event handlers is displayed.
2. Hover the mouse over each event handler to display a tooltip of information.

To create a notification profile:

1. Go to *Analytics* > *Incidents & Events* > *Event Handler*.
2. On the *Notification Profile* tab, click *Create New*.
3. Enter a name for the profile.
4. If desired, enable *Email*.
   a. Configure the desired email addresses to send the notification to.
   b. Configure the *Subject* field as desired, then click *OK*.

5. If desired, enable *Webhook*.
   a. Configure the webhook options as follows:

Field	Description
Type	Select *Generic* or *MS Teams*.
Port	Available if you selected *Generic*. Enter the port number that FortiGate Cloud uses to communicate with the platform.
Method	Select *POST* or *PUT* for the REST API call method.
Title	Enter the title for the message.
URL	Enter the webhook URL from the desired platform.
HTTP body	Available if you selected *Generic*. Enter the message body text.
HTTP authentication	Available if you selected *Generic*. Select *Basic* or *OAuth2* to configure and allow HTTP authentication between FortiGate Cloud and the platform.
Username	Available if you selected *Basic* for *HTTP authentication*. Enter the username to use for HTTP authentication between FortiGate Cloud and the platform.
Password	Available if you selected *Basic* for *HTTP authentication*. Enter the password to use for HTTP authentication between FortiGate Cloud and the platform.
Authorization server	Available if you selected *OAuth2* for *HTTP authentication*. Enter the IP address of the authorization server to use for HTTP authentication between FortiGate Cloud and the platform.
Auth client ID	Available if you selected *OAuth2* for *HTTP authentication*. Enter the client ID to use for HTTP authentication between FortiGate Cloud and the platform.
Auth client secret	Available if you selected *OAuth2* for *HTTP authentication*. Enter the client secret to use for HTTP authentication between FortiGate Cloud and the platform.

   b. Click OK.

Automation

On the *Analytics > Incidents & Events > Automation* page, you can create, edit, and enable/disable automation stitches.

To configure an automation stitch:

1. Go to *Analytics > Incidents & Events > Automation*.
2. Click *Create new*.
3. Click *Add event handler*. From the *Select Entries* pane, select the desired event to send notifications for.

4. Click *Add action*. From the *Select Entries* pane, select the desired action to take.
5. Beside *Select FortiGate*, click *+* to select a FortiGate.
6. Click *OK*. When the trigger occurs, FortiGate Cloud takes the configured action and sends notifications as configured.

To edit an automation stitch:

1. Go to *Analytics* > *Incidents & Events* > *Automation*.
2. Select an event handler, and click *Edit*.
3. Click *Action*, select a different action, and click *Close*.
4. Beside *Select FortiGate*, click *+* to change the FortiGate selection, and click *Close*.
5. Click *OK* to save the changes.

To enable or disable an automation stitch:

1. Go to *Analytics* > *Incident & Events* > *Automation*.
2. Right-click the desired event handler to display the tooltip menu.
3. On the tooltip menu, click *Enable* or *Disable*.

IoC

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

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

Threat type	Description
Malware	Malicious programs residing on infected endpoints
Potentially unwanted programs	• Spyware • Adware • Toolbars
Unknown	Threats that the signature detected but does not associate with any known malware

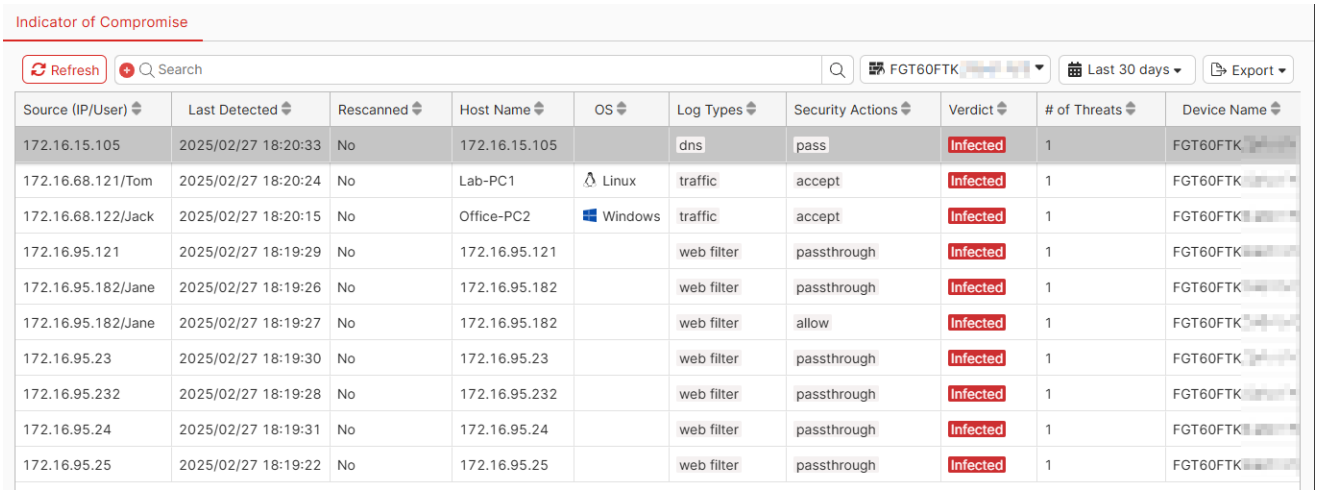
You can view infected devices' full IP addresses, allowing you to better control their access to your network.

This feature requires a Standard subscription. See Subscription types on page 13.

When a compromised host is detected, FortiGate Cloud triggers an alert to the FortiGate with the automation stitch type set to *Compromised Host*. You can configure an automation stitch on your FortiGate to determine the appropriate action for handling the compromised host in response to the alert. For detailed instructions on setting up an automation stitch, see Creating automation stitches.

To access IoC:

Go to *Analytics* > *IoC* > *Threats*. This page displays a table of data for any detected threats.



Above the table are the following options:

Option	Description
Refresh	Refresh the data in the table.
Search	Search for the desired threat. You can filter on the columns and values.
FortiGate	Select the desired FortiGate from the dropdown list.
Time range	Select the desired time range from the dropdown list.
Export	Export the data in the table to a CSV or JSON file.

The table displays the following columns of data:

Column	Description
Source (IP/User)	IP address and username of the device where the threat was detected.
Last Detected	Last time that the threat was detected.
Rescanned	Whether the device was rescanned for the threat.
Host Name	Hostname of the device where the threat was detected.
OS	OS of the device where the threat was detected.
Log Types	Log types associated with the threat.
Security Actions	Security action taken with the traffic.
Verdict	Status of the device.
# of Threats	Number of threats present on the device.
Device Name	Device name where the threat was detected.

You can configure trigger-based automated alerts for IoC events. See Event Handler on page 88.

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 *Send files to FortiSandbox for inspection* 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 10 minutes for automated SandBox detection to 10 hours if FortiGuard Labs is involved.

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

FortiGate Cloud enables you to view the status of any suspicious files uploaded: pending, clean, identified as malware, or unknown. The console also provides data on the time, user, and location of the infected file for forensic analysis.

The *Sandbox* page 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.

FortiSandbox SaaS allows the following file upload sources:

- File uploads from FortiGate:
  - For a FortiGate without a FortiSandbox SaaS subscription, FortiSandbox SaaS supports up to 100 uploads per day or two uploads per minute. See Subscription types on page 13
  - For FortiGates with a FortiSandbox SaaS subscription, the following upload limits apply:

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

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

To set up Sandbox:

1. Complete the FortiGate Cloud Sandbox (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 FortiGate Cloud 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.

CLI scripts

When you run a function in FortiGate Cloud that applies to FortiGates, such as running a script, FortiGate Cloud may not pass the actual username of the user who performed the action to FortiOS:

When remotely accessing a FortiGate from FortiGate Cloud, one of the following occurs:

- If *Cloud Access Anonymous Mode* is enabled, FortiGate Cloud passes the username of the FortiGate Cloud user who performed the action as a randomized @fortigatecloud.com email address, such as 4aa567e55bc8@fortigatecloud.com, to FortiOS.
- If *Cloud Access Anonymous Mode* is disabled, FortiGate Cloud passes the actual username of the FortiGate Cloud user who performed the action to FortiOS.

For other management features that a user can perform from FortiGate Cloud, such as running a script, FortiGate Cloud passes the username of the FortiGate Cloud user who performed the action as FortiGateCloud to FortiOS.

Therefore, when viewing logs on the affected FortiGate, you may see 4aa567e55bc8@fortigatecloud.com or FortiGateCloud as a username. For managed security service provider customers, this provides enhanced security by preventing subusers from seeing the primary account email address in the FortiGate logs.

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*.

FortiConverter

FortiConverter lets you create and monitor tickets for the FortiConverter Service and download converted configuration files. See About FortiConverter Service for information about business hours for the FortiConverter service team.

The FortiConverter Service:

- Helps migrate your network to Fortinet network security solutions by translating configuration files from other vendors' firewall products to a valid FortiGate configuration file.
- Helps migrate a configuration from one FortiGate to another FortiGate. A free opt-in license is available for the target FortiGate configuration conversion.

The FortiConverter Service provides FortiOS configuration files of command line syntax, and you can upload the configuration files to the target FortiGate.

From the *FortiConverter* > *Tickets* page, you can:

Create a ticket	Use to create a FortiConverter ticket to migrate a configuration from a third-party vendor to a FortiGate. See Creating tickets for third-party configuration migration on page 95.
Get a free license	Use to create a FortiConverter ticket to migrate a configuration from one FortiGate to another FortiGate and request a free opt-in license for the target FortiGate. See Creating tickets for FortiGate configuration migration on page 97.
View tickets	View the number and status of all FortiConverter tickets. Access the details of each ticket, and download the converted configuration files provided by the FortiConverter Service. See Viewing FortiConverter tickets on page 98.
Download converted configuration files	When the ticket status is *Service Delivered*, the converted configuration file is available for download. See Downloading converted configuration files on page 99.

See also FortiConverter Service.

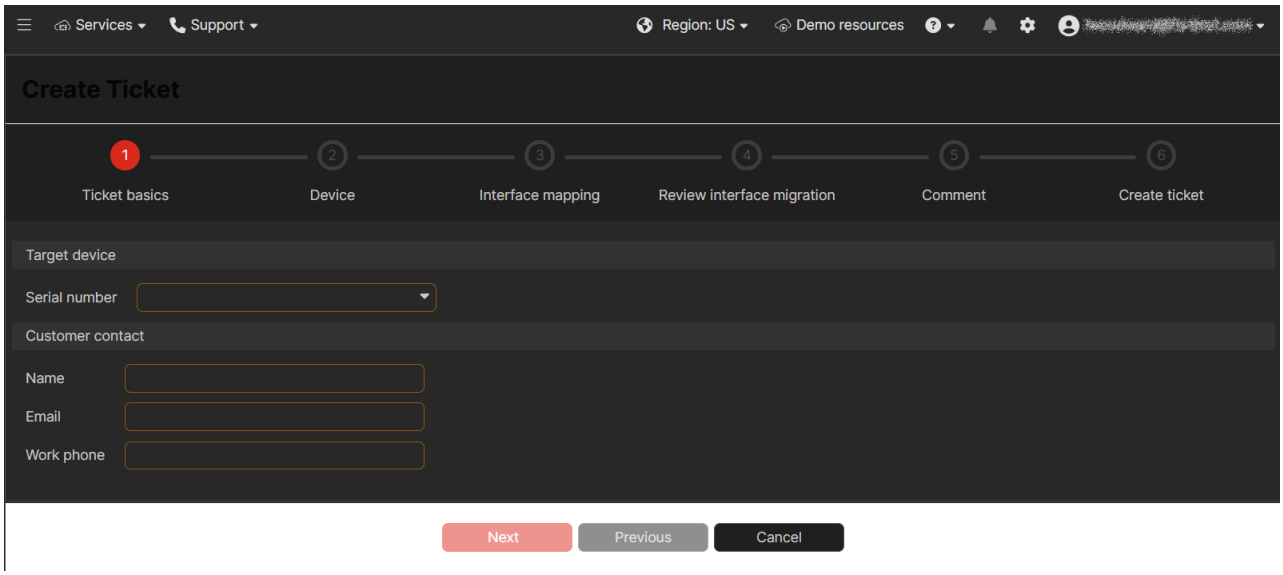
Creating tickets for third-party configuration migration

Use this procedure to create a FortiConverter ticket to migrate a configuration from a third-party vendor to a FortiGate.

See Third-party Security Vendors Conversion for a list of supported third-party vendors.

To create a FortiConverter ticket:

1. Go to *FortiConverter* > *Tickets* and click *Create ticket*. The Create Ticket wizard is displayed.



2. On the *Ticket basics* page, complete the following options and then click *Next*.

Option		Description
Target device	Serial number	Select the serial number of the target FortiGate.
Customer contact	Name	Your name.
	Email	Your email address.
	Work phone	Your work phone number.

If a FortiGate serial number is missing from the *Serial Number* list, confirm the missing FortiGate is registered to the same account in FortiCare. If the missing FortiGate is registered to the same FortiCare account, contact Fortinet Customer Service and Support at https://support.fortinet.com.

3. On the *Device* page, complete the following options and then click *Next*.

Option		Description
From	Config file	Click *Choose File* and upload an existing configuration file.
	Vendor	The vendor is automatically selected based on the configuration file.
To	Target SN	Displays the serial number for the target FortiGate.
	Target version	Select a target FortiOS version for the conversion.

4. On the *Interface mapping* page, complete the *From* and *To* mappings on each tab and then click *Next*. Some tabs may be automatically populated for you.

- Physical Interface tab
- VDOM Link
- 802.3 Aggreate
- EMAC VLAN
- PPPoE
- Redundant
- Software Switch
- Tunnel
- VLAN
- Hardware Switch
- WiFi SSID

5. On the *Review interface mapping* page, expand each section to review the mappings and then click *Next*.
6. On the *Comment* page, optionally add a comment for the support team and then click *Next*.
7. On the *Create ticket* page, an estimated delivery date and time is displayed:
   a. Click *Create ticket* to create the FortiConverter ticket.
   b. After the ticket is created, click *View Ticket Detail* to display the details. See Viewing FortiConverter tickets on page 98 for more information.

Creating tickets for FortiGate configuration migration

Use this procedure to create a FortiConverter ticket to migrate a configuration from a FortiGate to a FortiGate and receive a free opt-in license for the target FortiGate.

Only configuration migration from FortiGate to FortiGate supports the free opt-in license. Only FortiGates without a license can be selected as the target FortiGate.

All FortiGate to FortiGate configurations are fully supported with a few exceptions. See FortiGate Configuration Migration for more information.

To create a FortiConverter ticket:

1. Go to *FortiConverter > Tickets* and click *Get free license*. The *Get Free License* pane is displayed.
2. In the *Target device serial number* list, select a FortiGate.
   Only devices without a license can be selected. Devices that already have a license cannot be selected for free license.
3. Read the terms and conditions, and select *I Agree to the following terms and conditions*.
4. Click *OK*. The *Create Ticket* pane is displayed.
5. On the *Create Ticket* pane, complete the *Customer contact* options, and click *Next*.
6. On the *Device* pane, complete the options and click *Next*.
7. On the *Device* page, complete the following options and click *Next*.

Option	Description
Vendor	Select Fortinet. Only Fortinet is available in the list.
Config file	Click *Choose File* and upload an existing FortiGate configuration file.
Target SN	Displays the serial number for the target FortiGate.
Target version	Select a target FortiOS version for the conversion.

If a FortiGate serial number is missing from the *Serial Number* list, confirm the missing FortiGate is registered to the same account in FortiCare. If the missing FortiGate is registered to the same FortiCare account, contact Fortinet Customer Service and Support at https://support.fortinet.com.

8. Follow the wizard to complete the remaining steps to create a ticket.
   The remaining steps are the same as creating a ticket for a third-party migration. See Creating tickets for third-party configuration migration on page 95 for more information.
   See also Viewing FortiConverter tickets on page 98.

Viewing FortiConverter tickets

The *FortiConverter > Tickets* page displays all existing FortiConverter tickets. Charts at the top of the page provide a summary of the tickets and their statuses:

- *New*: A FortiConverter ticket has been created and is in the queue for processing.
- *In Progress*: The provided configuration file is being converted for the target FortiGate model and FortiOS version.
- *Service Delivered*: The conversion process is complete, and a converted configuration file is available for download.

Select a ticket, and click *Edit* to view its details and access associated configuration files.

A *Search* bar is available to help you find tickets. In addition, each column can be filtered.

To view a ticket:

1. Go to *FortiConverter > Tickets*. The top of the page displays:
   - *Status*: The number of tickets and how many tickets are at each status
   - *Source Vendor*: The number of tickets for each source vendor
2. In the *Search* bar:
   - Type a search term, and press `Enter`.
   - Click + to select a column and specify the search terms. Click *Apply*.
3. Select a ticket to display the *Edit* button and then click *Edit*. The ticket details displayed on the following tabs:

Option	Description
Summary	Displays a summary of the ticket and customer contact information. Ticket summary fields include: • Estimated Delivery • Priority • Name • Assigned to • Target FortiOS version • Current Status • Target Model • Free License • Source Vendor • Support Level
Files	Displays the uploaded configuration file and the FortiConverter config file when available. For the source config file, you can delete an existing source config file and upload a new file. You can also download all files. For the FortiConverter config file, you can download the file when available. See Downloading converted configuration files on page 99.
Message	Displays the communication between you and the Fortinet service team.

To edit a ticket:

1. Go to *FortiConverter* > *Tickets*, and select a ticket. The *Edit* button is displayed.
2. Click *Edit* to display the ticket details.
3. Add changes, and click *OK*.

Downloading converted configuration files

Converted configuration files for a ticket are available when the ticket status is *Service Delivered*.

To download converted configuration files:

1. Go to *FortiConverter* > *Tickets*.
2. Locate and select your ticket with a status of *Service Delivered*. An *Edit* button is displayed.
3. Click *Edit* to display ticket details on the following tabs: *Summary*, *Files*, *Message*.
4. Click *Files*.
   The converted configuration files are displayed under *Converted config files*.
5. Download the files by using one of the following options:
   - Select a file, and click *Download*.
   - Click *Download All Files*.

Settings

In *Settings*, you can access the following menus:

- FortiCloud Subscriptions on page 100
- General Settings on page 102

FortiCloud Subscriptions

On the *Settings* > *FortiCloud Subscriptions* page, you can view activated and available seats for FortiClient EMS Cloud and FortiIdentity Cloud. You can also activate seats.

Charts at the top of the page display:

Chart	Description
Seat activation status	Displays the number of activated FortiClient EMS Cloud and FortiIdentity Cloud seats as well as the number of seats available for activation.
Seat count timeline	Displays the timeline for activated FortiClient EMS Cloud and FortiIdentity Cloud seats.

Below the charts, you can access the following buttons:

Button	Description
Activate seats	Select *FortiClient EMS Cloud* or *FortiIdentity Cloud*, and click *Activate seats* to activate seats.

The table displays the following information about FortiCloud subscriptions:

Column	Description
Subscriptions	Displays the name of available subscriptions. Hover the mouse over the *Subscriptions* column to display and click the *Configure Table* gear icon to customize the column headings.
Seats Available for Activation	Displays how many seats are not yet activated.
Seats Activated	Displays how many seats have been activated.

Activating free seats

The following information explains how to activate free entitlements for FortiClient EMS Cloud and FortiIdentity Cloud in the FortiGate Cloud portal.

FortiGate devices registered with a FortiCare Premium or Elite contract are eligible for free service seats:

FortiCloud service	Eligible FortiCare subscription	Free seats granted	Seat maximum per FortiCloud account
FortiClient EMS Cloud	FortiCare Premium or FortiCare Elite	3 seats per device subscription	No maximum
FortiIdentity Cloud			48 seats maximum (16 subscriptions maximum)

After logging in to FortiGate Cloud, a notification appears informing you free seats are available for activation. The notification provides details about the available seats and a link to the *FortiCloud Subscriptions* page, where the free seats can be activated. Alternatively, go to *Dashboard* > *Status*, where the *FortiCloud Subscriptions* widget displays the number of available free seats. Click *View full details* to open the *FortiCloud Subscriptions* page.

To activate the free seats for your account, register the device in FortiCloud from the *Asset Management* page using a FortiCare Premium or Elite license, then open FortiGate Cloud and go to the *FortiCloud Subscriptions* page to review and activate the available free entitlement. After activation, log in to FortiIdentity Cloud or FortiClient EMS Cloud with your FortiCloud account and use the service with the activated free entitlement.

To activate free seats:

1. Register a FortiGate if you have not done so already. See Registering assets.
2. Register your FortiCare Premium or FortiCare Elite license. On the *Registration Info* page, assign the license to a FortiGate in your account.
3. After registration, return to the *FortiGate Cloud Portal*.
4. Go to *Settings* > *FortiGate Cloud Subscriptions*. Verify that the number *Seats Available for Activation* has increased.
5. Select a subscription and click *Activate Seats*. The *Pending Activation* tab displays:
   - Devices with eligible FortiCare contracts
   - The number of seats granted per device

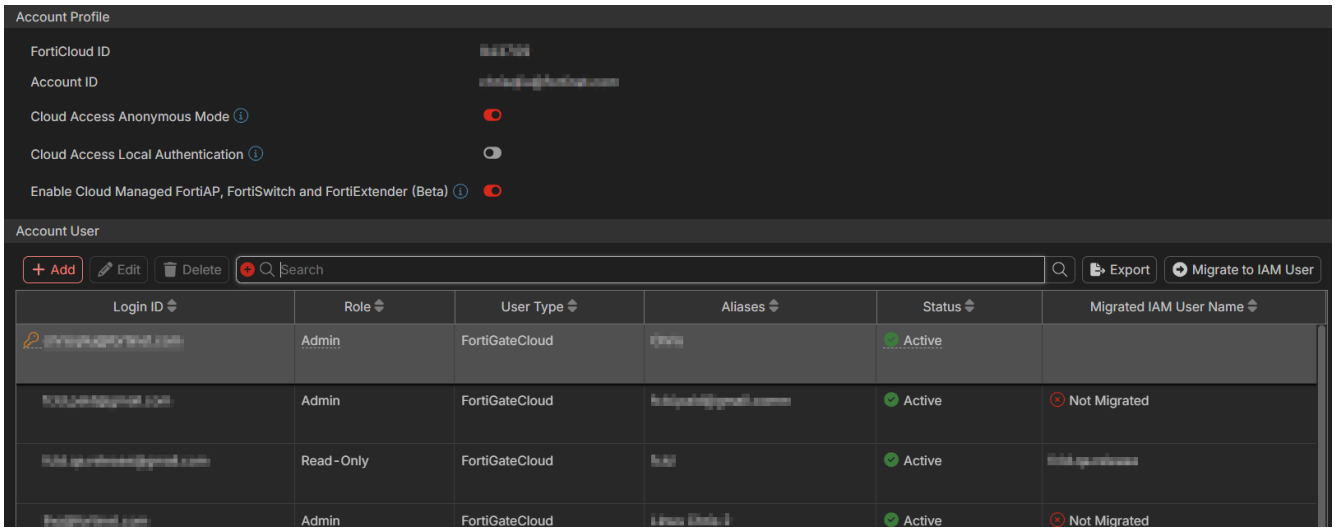
   Devices are grouped by contract expiration date. Newly registered devices are listed at the bottom.
6. Select the device.
7. Click *OK* to activate the seats.

To view activated seats:

- In FortiGate Cloud, open the *FortiCloud Subscriptions* page, select a subscription, click *Activate Seats*, and then open the *Activated* tab.
- In FortiIdentity Cloud, log in and go to the *Dashboard*. The activated seats appear in the *Users / Max Users* section.
- In FortiClient EMS Cloud, the activated seats appear in *Dashboard* > *Status*, under *Licensed*.

General Settings

You can add and manage users from *Settings* > *General Settings*. The *General Settings* page includes different user types, including Identity & Access Management (IAM) and FortiGate Cloud account users. *General 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. 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: • **API**: an API user only has the ability to call the FortiGate Cloud API. FortiCare manages API users and their access permissions. API users are subusers of the primary account. See API access on page 115. • FortiGate Cloud: Local FortiGate Cloud user. • **IAM**: see IAM users on page 103. • **Third Party**: user who authenticates using an external identity provider (IdP). Configuring an external IdP requires FortiCare and FortiAuthenticator support.
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.

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

You can enable or disable cloud access anonymous mode for a user. Alternately Cloud access anonymous mode can be configured at the organization level. See OU General settings on page 114.

When you run a function in FortiGate Cloud that applies to FortiGates, such as running a script, FortiGate Cloud may not pass the actual username of the user who performed the action to FortiOS:

When remotely accessing a FortiGate from FortiGate Cloud, one of the following occurs:

- If *Cloud Access Anonymous Mode* is enabled, FortiGate Cloud passes the username of the FortiGate Cloud user who performed the action as a randomized @fortigatecloud.com email address, such as 4aa567e55bc8@fortigatecloud.com, to FortiOS.
- If *Cloud Access Anonymous Mode* is disabled, FortiGate Cloud passes the actual username of the FortiGate Cloud user who performed the action to FortiOS.

For other management features that a user can perform from FortiGate Cloud, such as running a script, FortiGate Cloud passes the username of the FortiGate Cloud user who performed the action as FortiGateCloud to FortiOS.

Therefore, when viewing logs on the affected FortiGate, you may see 4aa567e55bc8@fortigatecloud.com or FortiGateCloud as a username. For managed security service provider customers, this provides enhanced security by preventing subusers from seeing the primary account email address in the FortiGate logs.

To enable or disable cloud access anonymous mode:

1. Go to *Settings* > *General Settings*.
2. Enable or disable *Cloud Access Anonymous Mode*.
   You may be unable to change this setting when the organization administrator has enabled/disabled the setting at the organization level.

User management

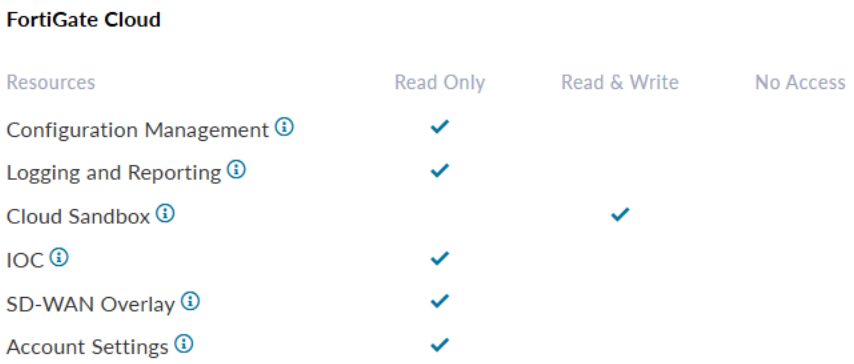
The primary user can add users to the account using the following methods:

User type	Method
Identity and Access Management (IAM) user	Add users to the FortiCloud account with role-based access control in FortiGate Cloud using the FortiCloud IAM service. See IAM users on page 103.

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

IAM users

FortiCloud supports creating IAM users and allowing access to FortiGate Cloud 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

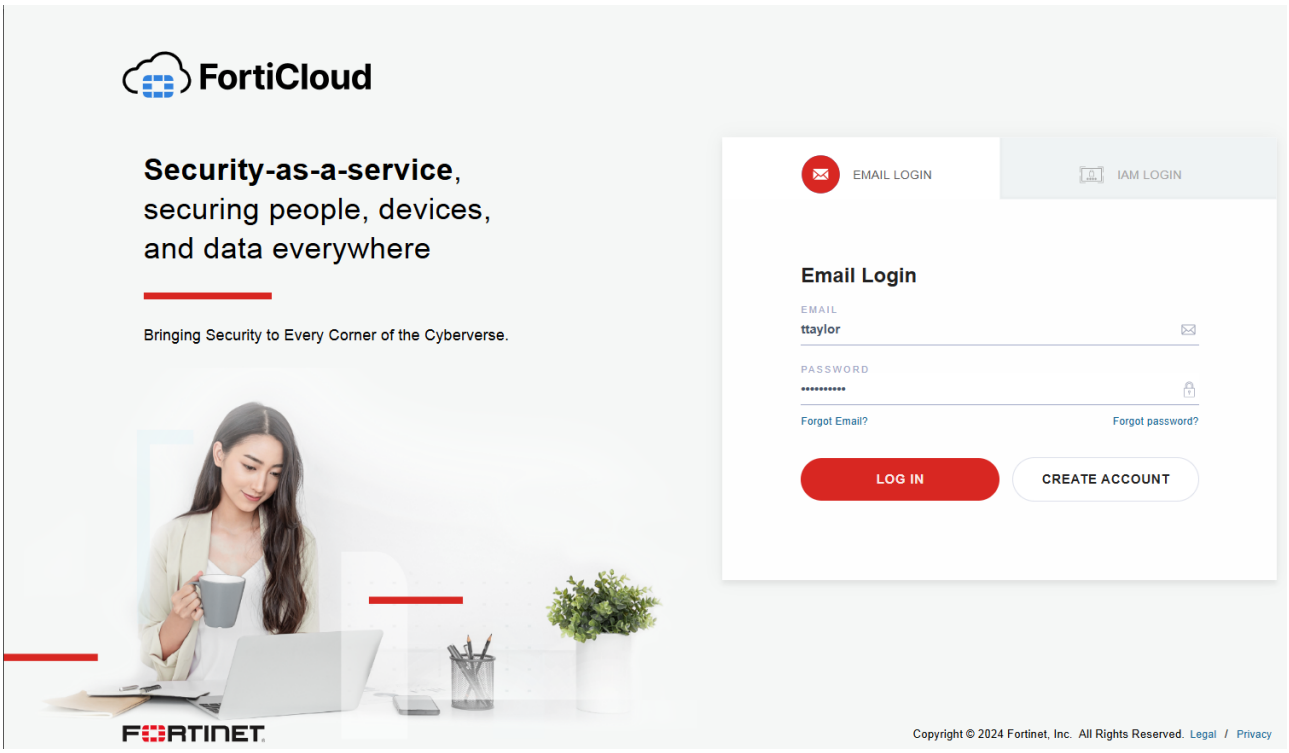
FortiGate Cloud supports organizational unit (OU) account selection and switching. See Organization Portal for details on creating an OU.

Creating an IAM user with OU scope

See User permissions.

FortiCloud account

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



Creating an account

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

Audit

Audit > *Activities* displays a log of actions that users have performed on FortiGate Cloud. 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 include user login and logout events, user edit actions, and updates to account settings.
Backup	• Backing up a device configuration • Downloading and disabling backups
Cloud access	Viewing and configuring a device via cloud access
Device deployment	• Provisioning and deprovisioning devices • Deleting provisionings
Log	Exporting logs
Report	Downloading, scheduling, and running reports
Sandbox	Uploading files to Sandbox for analysis
Script	Creating, editing, deleting, and provisioning 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

The audit feature is available to the following user types that have read-write permission over all role-based access control resources for all assets in the account:

- Email users
- Local or organizational unit Identity & Access Management users
- Users with external identity provider roles

Multitenancy

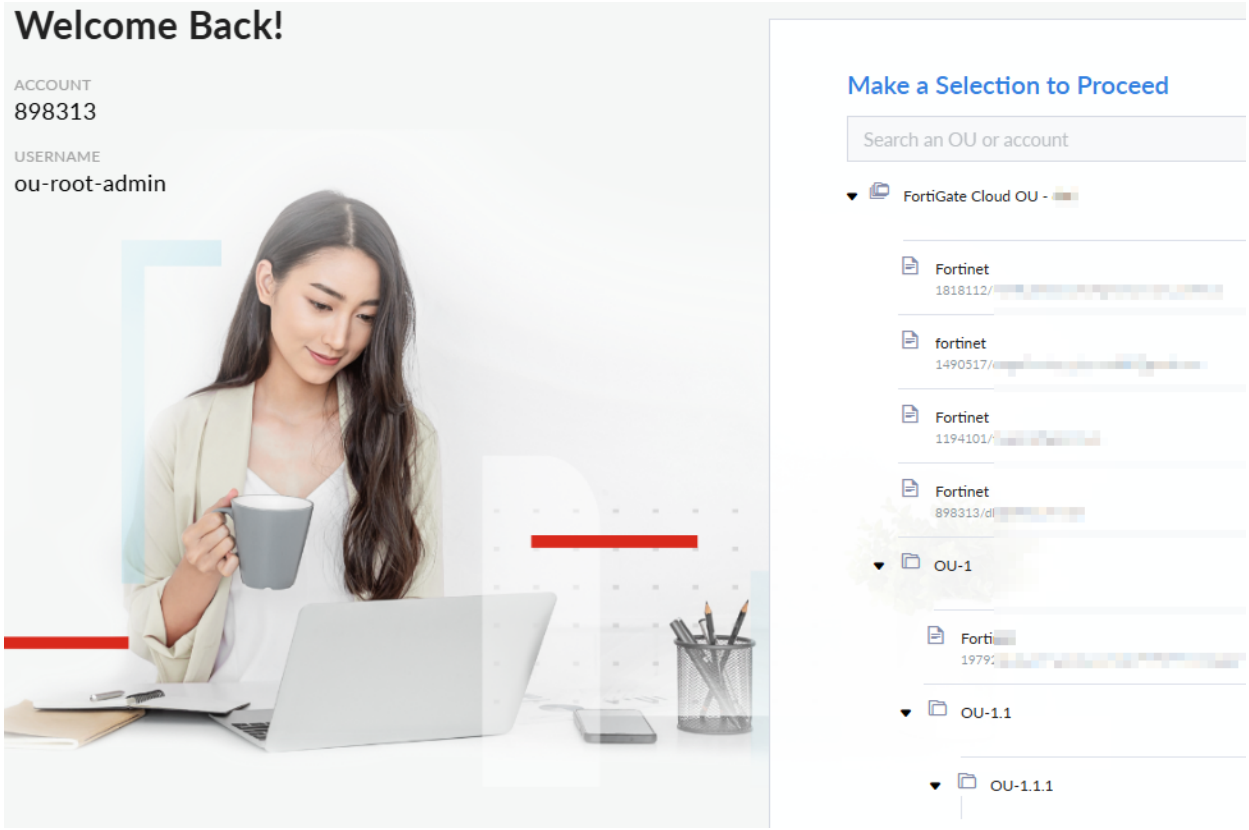
FortiGate Cloud supports Multitenancy with FortiCloud Organizations. See Multitenancy with FortiCloud Organizations on page 108.

Multitenancy with FortiCloud Organizations

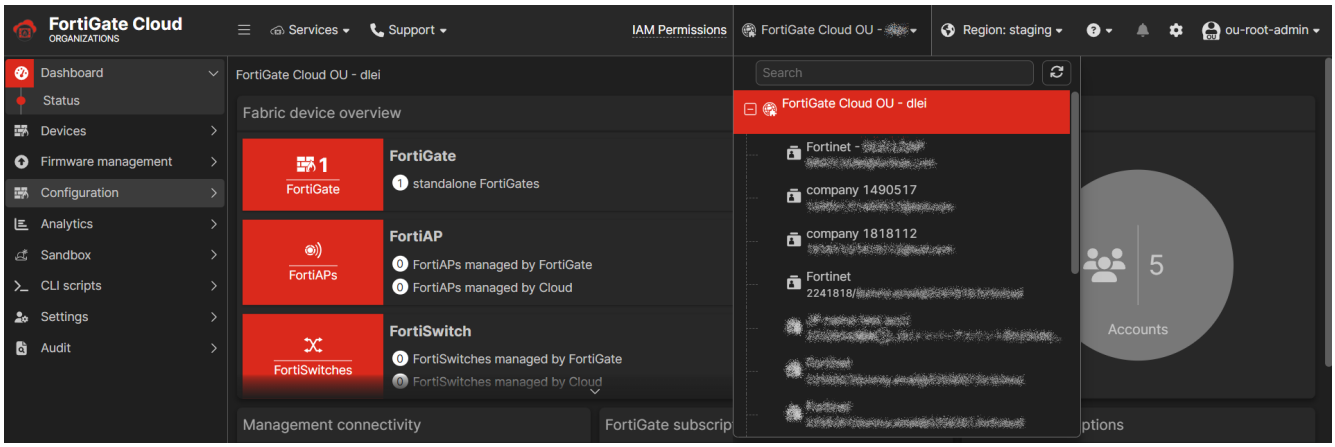
FortiGate Cloud supports FortiCloud Organizations for seamless multitenant features designed for managed security service providers across multiple FortiCloud accounts. With Organizations, Identity & Access Management (IAM) users can view an organizational unit (OU) Dashboard for a single pane of glass view of assets across the entire Organization or OU. Administrators can add additional users with a fine grained permission model (IAM permission profile) and manage the visibility and access to full Organization or specific OU or OU member accounts. You can create an Organization and manage up to 10 accounts. For managing more than 10 accounts, Organization root account can create a Fortinet Developer Network basic account. This requires no additional subscription. See the following for details on various OU tasks:

Task	Instructions
Creating an OU	Adding and deleting OUs
Creating an OU IAM user	Organization user management When creating a permission profile in the IAM portal, you must add the FortiGate Cloud portal to the profile, and configure the desired permissions. See IAM users on page 103.
Log in as an OU IAM user	Logging into an OU account

When you log in to FortiGate Cloud, if OUs are enabled on the account, a OU/account selection screen displays. You can select an OU or account to access from this tree. The folder icon denotes OUs, while the file icon denotes accounts.



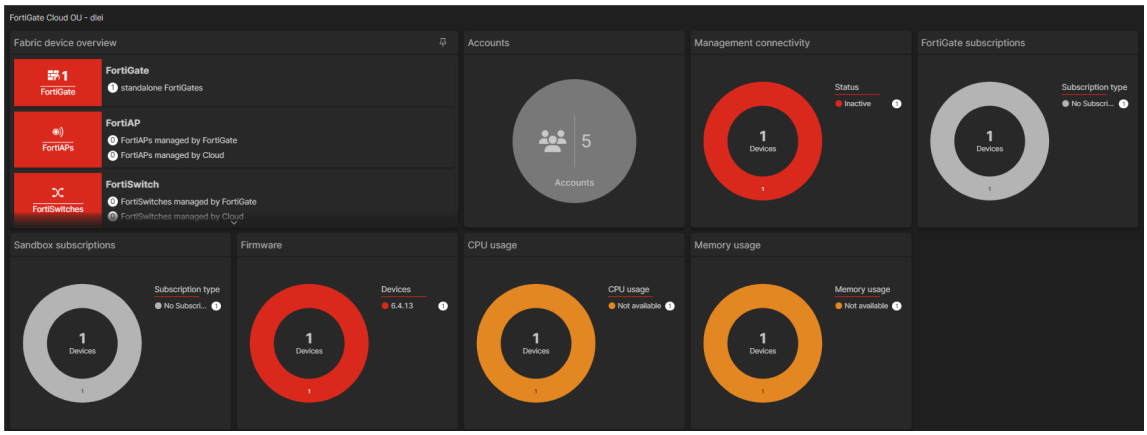
To move to another OU or account, select the desired OU from the dropdown list in the upper right corner.



OU Dashboard

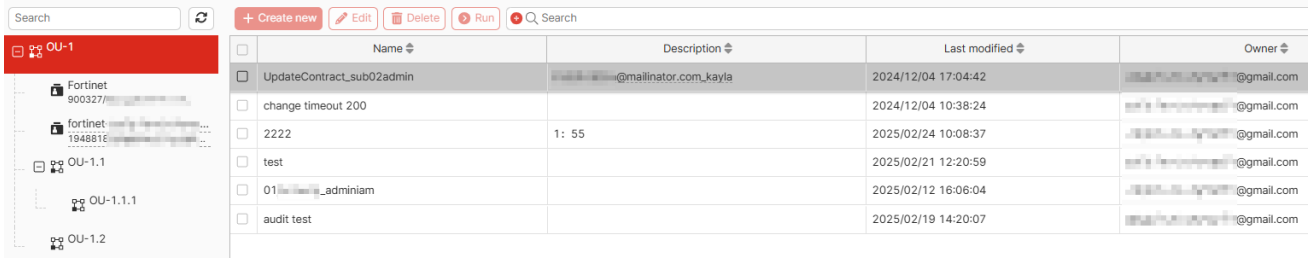
The OU Dashboard provides a consolidated view of accounts and assets in the given scope of the Organization. The dashboard is available for Organization type IAM users and the visibility of accounts and assets depends on the OU scope selected for the IAM user.

When you access an OU from the OU tree, FortiGate Cloud displays an OU dashboard. The following lists OU dashboard widgets:



Widget	Displays a donut chart that details...
Fabric Device Overview	Device type breakdown and total number of devices in this OU.
Accounts	Total number of accounts in this OU.
Management connectivity	Management connectivity status breakdown and total number of devices in this OU.
FortiGate subscriptions	FortiGate Cloud subscription type breakdown and total number of devices in this OU.
Sandbox subscriptions	Sandbox subscription type and total number of devices in this OU.
Firmware	Firmware version installed on devices in this OU.
CPU usage	CPU usage levels on devices in this OU.
Memory usage	Memory usage levels on devices in this OU.

When logged in to an OU, you can also access the same pages that you can access from within an account. When accessing one of these pages from an OU, there is a panel where you can select an account or sub-OU. The content pane then displays content from the selected account or OU.



The following lists configuration pages that are available when logged into an OU. See the relevant topic in this guide as linked in the table:

Page	Description
Dashboard	OU Dashboard on page 109

Page	Description
Devices	Offers some functionalities that the account-level *Assets* page does not. See OU Device list on page 111.
Firmware management	Firmware management on page 44
Configuration	Configuration on page 47
Analytics	Analytics on page 78
Sandbox	Sandbox on page 92
CLI scripts	CLI scripts on page 94
Settings	Settings on page 100
Audit	Audit on page 106

OU Device list

The OU *Devices* > *Device 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:

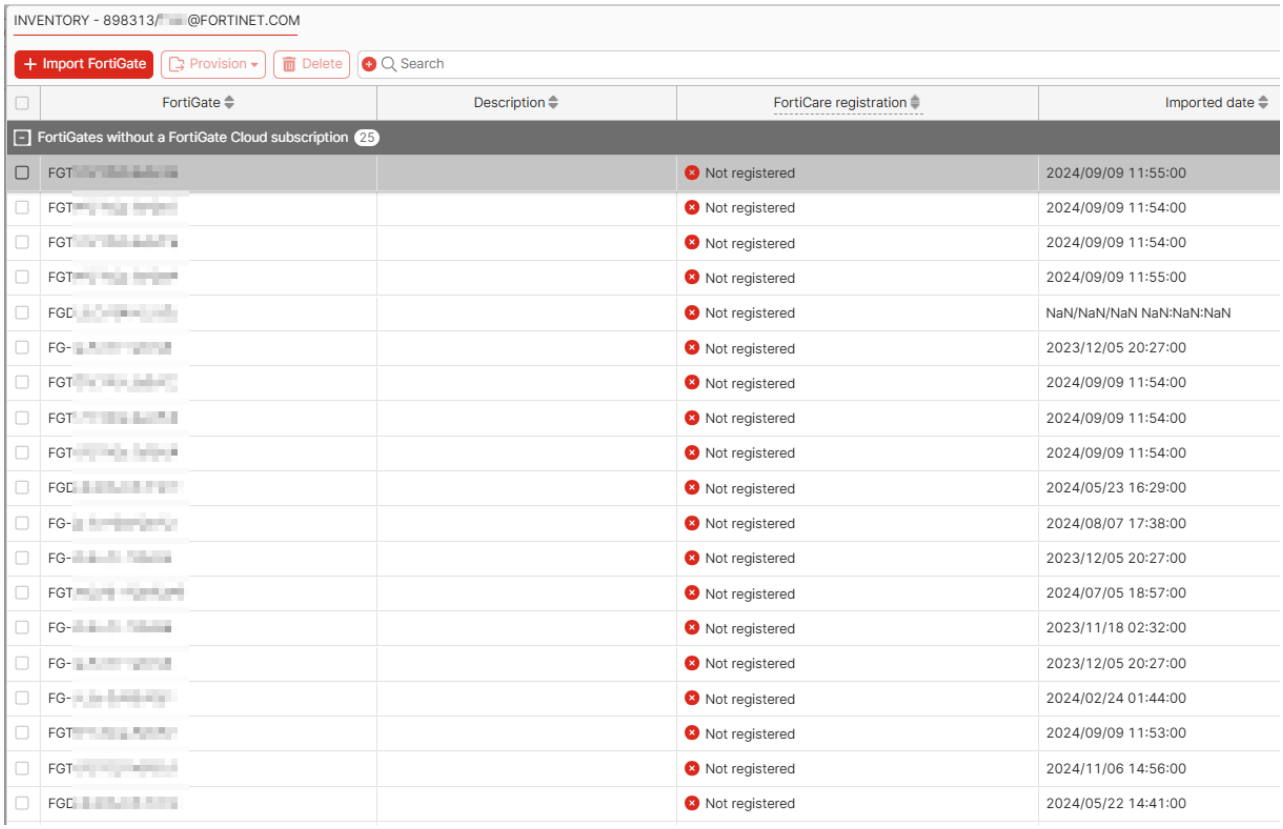
Column	Description
Account ID	FortiCloud account that the device is registered to.
Device name	Device name and serial number.
Firmware	Firmware version installed on the device.
Upgrade status	Displays if the FortiGate is currently performing a firmware upgrade.
Transfer status	Transfer status on the 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 provision 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.

Column	Description
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 *Devices* > *Device 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.

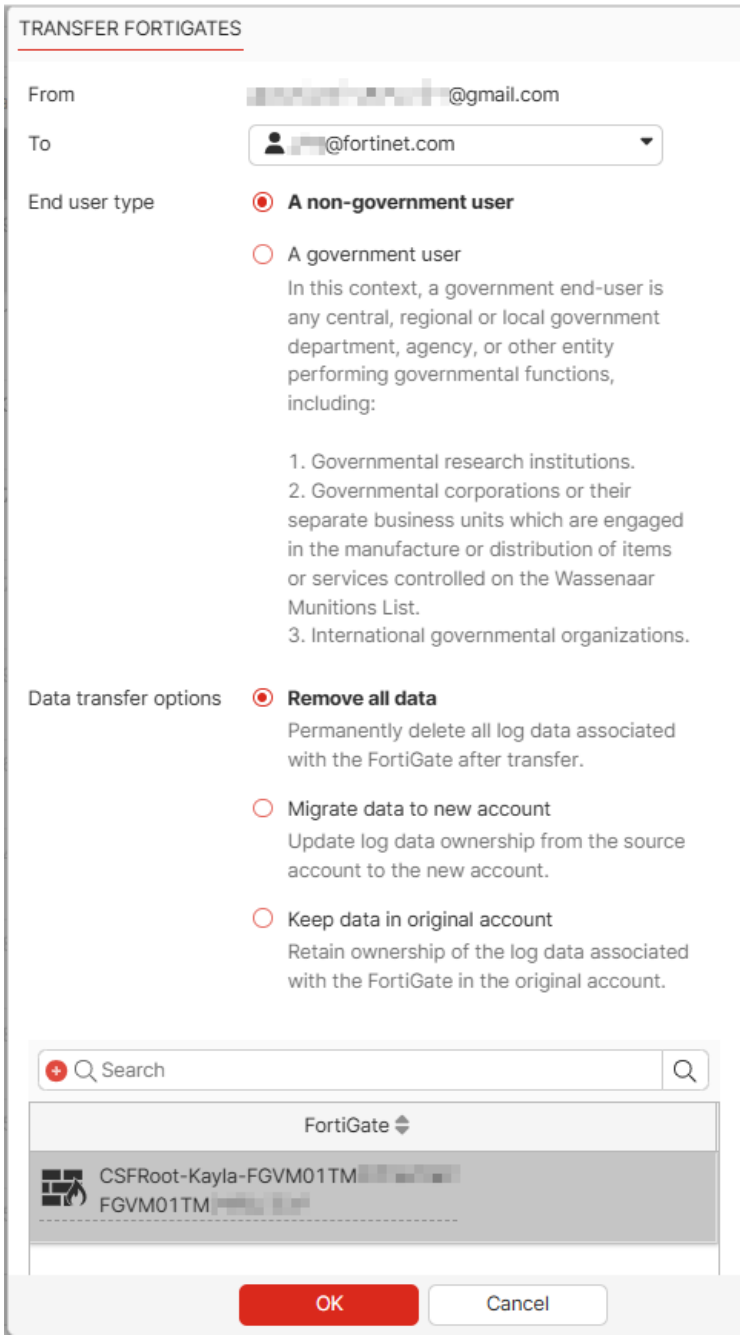


You can transfer FortiGates between accounts in an OU.

To transfer a FortiGate:

1. Go to *Devices* > *Device 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.

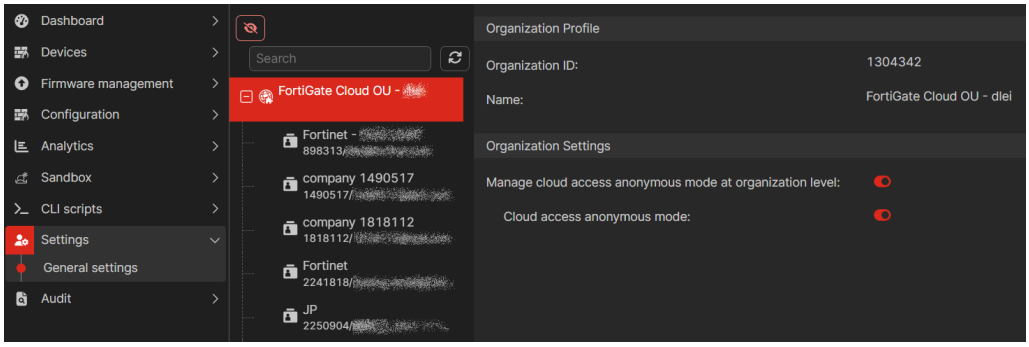
4. Click the *Transfer FortiGates* button.
5. On the *Transfer FortiGates* slide, select the destination account, data transfer option, click the acknowledgment, then click *OK*. The selected FortiGate(s) will now be transferred to from the source account to the destination account.



FortiGate Cloud supports transfers from and to the and legacy FortiGate Cloud portal.

OU General settings

The OU *Settings* > *General settings* page lets you set anonymous cloud access for all accounts in the OU.



To set anonymous cloud access:

1. Go to *Settings* > *General Settings*.
2. Select the OU.
3. Enable *Manage cloud access anonymous mode at the organization level*.
4. Enable *Cloud access anonymous mode*.
   Anonymous cloud access is enabled for all accounts in the OU.
5. Select an account to see *Cloud Access Anonymous Mode* is enabled and controlled by the organization administrator.

API access

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

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

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

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

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

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

1. If you do not already have one, create an Identity & Access Management (IAM) API user:
   a. Log in to the IAM portal using your FortiGate Cloud account credentials.
   b. Go to *API Users*, then click *ADD API USER*. Click *Next*.
   c. Under *Effective Portal Permissions*, select *FortiGate*, then *ADD*. Click *Next*.
   d. Click *Edit*. Toggle *Allow Portal Access* to *YES*. Under *Access Type*, select *Admin*. Click *CONFIRM*.
   e. Click *DOWNLOAD CREDENTIALS*. Open the downloaded file to view your username and password.
2. Retrieve the access token by calling the FortiAuthenticator token retrieval API: `/oauth/token/`. The following provides an example where the FortiAuthenticator IP address is customerapiauth.fortinet.com:
   Request:
   ```
   curl -H "Content-Type: application/json" -X POST
        https://customerapiauth.fortinet.com/api/v1/oauth/token/ -d '{"username":"AC0F1454-3CCD-
        4523-8B3C-4412156CB197","password":"a679bc11d6011e6ea3a7390cef0cd66b!1Aa","client_
        id":"fortigatecloud","grant_type":"password"}'
   ```
   Response:
   ```
   {"access_token": "EXAMPLETOKEN", "expires_in": 14400, "message": "successfully authenticated",
        "refresh_token": "syIsrAofcHe67bTFdmhhT5pInnqCXT", "scope": "read write", "status":
        "success", "token_type": "Bearer"}
   ```
3. You can query all supported FortiGate Cloud APIs using the access token that you retrieved from step 2. The following provides an example:
   Request:
   ```
   curl -H "Content-Type: application/json" -H "Authorization: Bearer EXAMPLETOKEN" -X GET
        https://api.fortigate.forticloud.com/forticloudapi/v1/devices -k
   ```
   Response:

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


To call FortiOS APIs via FortiGate Cloud:

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

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

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

Request:

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

For FortiOS API information, see the FortiOS REST API documentation.

Frequently asked questions

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

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 telnet logctrl1.fortinet.com or globallogctrl.fortinet.net via port 443.
3. Ensure that the FortiGate Cloud account password length is fewer than 20 characters.
4. If the FortiGate is a member of a high availability (HA) pair, ensure that you activate FortiGate Cloud on the primary device. Activate FortiGate Cloud on the primary FortiGate as To provision a FortiGate or FortiWifi to FortiGate Cloud in the FortiOS GUI: on page 24 describes. FortiGate Cloud activation on the primary FortiGate activates FortiGate Cloud on the secondary FortiGate. Local FortiGate Cloud activation on the secondary FortiGate will fail.
5. Enable FortiGate Cloud debugging 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.
6. 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?

To activate FortiGate Cloud for an HA pair, all members of the cluster, including both primary and secondary units, must be provisioned to the same FortiGate Cloud account.

If an HA unit is replaced, the replacement device must be provisioned to the same FortiGate Cloud account before it joins and forms the new HA cluster.

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 in FortiOS for the first time, follow the steps in FortiCare and FortiGate Cloud login.
- Otherwise, if you have already activated FortiGate Cloud, 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 in the FortiOS GUI: on page 24 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 in the FortiOS GUI: on page 24 describes instead. If you cannot connect to the FortiOS GUI, contact cs@fortinet.com to reenable the key.

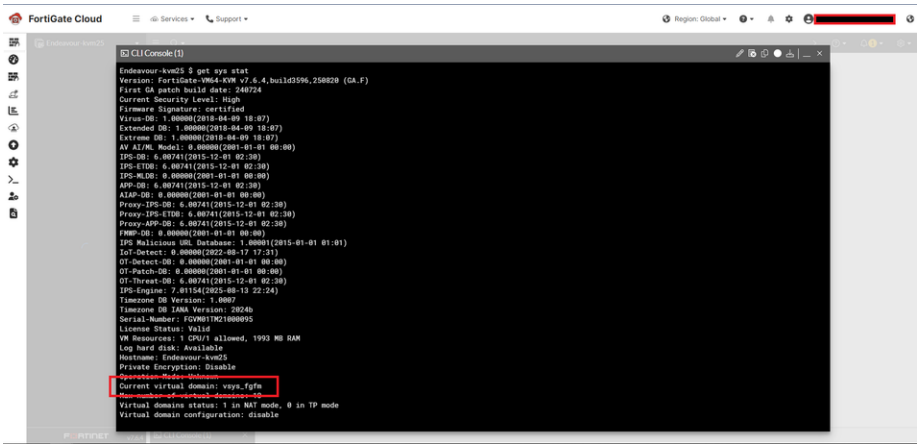
What do I do if FortiGate Cloud activation via the FortiOS GUI succeeds, but I cannot find the FortiGate in the FortiGate Cloud portal?

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 use the CLI to access the root VDOM on FortiOS 7.6.4?

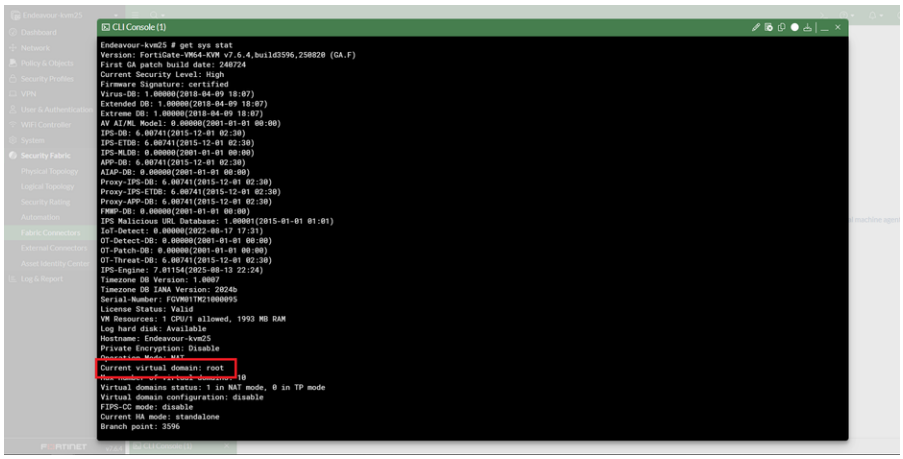
When accessing the CLI inside FortiGate Cloud, the default VDOM is not the usual `root` VDOM if FortiGate is running FortiOS 7.6.4.

To check the current VDOM, run `get sys stat`. The following example shows the output when accessing the device through FortiGate Cloud:



Under `Current virtual domain`, the VDOM is `vsys_fgfm`, which is usually an internal VDOM. The output for most commands will be unexpected until the correct VDOM is selected.

The following example shows the output when accessing the device directly. Notice the default is `root`:



To select the correct VDOM when using FortiGate Cloud, run `exec enter root` to manually move the CLI session to the correct VDOM.

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

1. Log in to FortiGate Cloud region A.
2. Deprovision the device.
3. Verify that the device has returned to the *Devices and Provisioning* > *Device List* > *FortiGate* list.
4. Switch the portal to region B.
5. Go to *Devices and Provisioning* > *Device List* > *FortiGate*.
6. Click *Add FortiGate*.
7. Search for the device, then click *Provision to FortiGate Cloud*.

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 118. See Accessing a FortiGate on page 36.

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 differfent 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 using the FortiCloud key: on page 24.
5. Provision 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 in the FortiOS GUI: on page 24 describes.
7. If the FortiGate is running an older version of FortiOS and has just been factory-reset, wait a few moments after it boots up to allow the certificates to download properly from FortiGuard.

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
diagnose test application forticldd 3
show full log fortiguard setting
```

What do I do if FortiGate Cloud cannot retrieve logs from FortiOS when the 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
```

You may use the Fortinet support tool Chrome extension to troubleshoot issues. See Technical Tip: Fortinet Support Tool - Google Chrome Extension for troubleshooting GUI issues.

How can I export more than 2000 lines of logs?

FortiGate Cloud only supports raw log download for FortiGates with a FortiGate Cloud Basic subscription. See To download a log: on page 84.

Why does FortiGate Cloud 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 on page 78.

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 devices with an active subscription, 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 47.

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 following in the CLI after changing the hostname:

```
diagnose fdsm contract-controller-update
```

Why is my FortiGate provisioned 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 provisions 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 provision 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 provision 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.

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

After you transfer a FortiGate from account A to B in the Asset Management portal, it is deprovisioned from account A with existing data retained under account A. The FortiGate is available for provisioning under *Asset list > Add FortiGate > Inventory* in account B in FortiGate Cloud. After reactivating FortiGate Cloud using account B, you must ensure that the FortiGate central management and log destination are configured as FortiGate Cloud in *Security Fabric > Fabric Connectors*.

Does FortiGate Cloud support data backups and disaster recovery?

FortiGate Cloud is ISO 27001- and SOC2-compliant and supports standard procedures for data backup and redundancy and disaster recovery.

What happens if you enable automatic firmware upgrade on FortiGate Cloud and the FortiGate?

The firmware profile assignment within FortiGate Cloud disables the local automatic firmware upgrade configuration on the FortiGate.

Can I disable automatic firmware upgrade from FortiOS by logging in directly to the FortiGate that has no FortiGate Cloud Basic subscription to bypass the automatic firmware upgrade enforcement from FortiGate Cloud?

FortiGate Cloud does not automatically upgrade devices without a FortiGate Cloud Basic 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 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 features and stops uploading logs to FortiGate Cloud.

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

How can I activate FortiGate Cloud on a FortiGate provisioned to an OU placeholder account?

To activate FortiGate Cloud, 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
```

OU scope member accounts (i.e., accounts without a real email address) cannot be used to provision a FortiGate to Fabric Managed mode directly from the FortiOS GUI, as these accounts do not have passwords.

Instead, use the following procedures:

Scenario	Procedure
Device is NOT yet provisioned to Fabric Managed	1. Ensure the device is registered to the OU scope member account in FortiCare. 2. Switch to the OU scope member account. 3. Navigate to *Devices & Provisioning* and provision the device to Fabric Managed. 4. Reboot the device, or run the CLI command: `execute fortiguard-log join`
Device is ALREADY provisioned under a different account	1. Use the *OU dashboard asset transfer* feature to move the device to the target OU scope member account. 2. Reboot the device, or run the CLI command: `execute fortiguard-log join`

Why do some of my legacy email users from FortiGate Cloud not appear after going to the Migrate to IAM page?

When you click the *Migrate to IAM* button in *Administration > User Settings*, FortiGate Cloud redirects to the IAM portal *Migrate to IAM* page. After clicking *Next*, all eligible legacy email users from your FortiGate Cloud account are listed for migration.

However, some users may be excluded from the list due to the following reasons:

- Duplicate across regions: if the same email address exists in multiple FortiGate Cloud regions and has already been migrated in one region, it does not appear.
- Subaccount user in a multitenancy account: if your FortiGate Cloud account has a valid multitenancy subscription and a user is assigned to only some (but not all) subaccounts, the migration list does not include that user.

SD-WAN Overlay

What is the maximum number of FortiGates that the SD-WAN Overlay feature supports?

There is no limit on the number of FortiGates supported.

What is the difference between a branch and DC site?

There is no configuration difference between a branch and DC site. You can use it as site identification method.

What does the SD-WAN Overlay agent do?

The agent is a FortiOS component that preprocesses the configuration pushed from FortiGate Cloud SD-WAN Overlay via the FGFM management tunnel and applies it to the device. The agent must be running properly after device bootup for SD-WAN Overlay to function.

When you push SD-WAN Overlay policy changes to a FortiGate, does FortiGate Cloud overwrite other locally changed parameters for an affected policy?

FortiGate Cloud SD-WAN Overlay does not read or overwrite firewall policy configurations for policies previously configured on devices. Managing all required firewall policies through SD-WAN Overlay is considered best practice.

Why does pushing some changes from FortiGate Cloud SD-WAN Overlay not create a revision in FortiGate Cloud?

Pushing SD-WAN Overlay configuration changes that do not affect the FortiGate device configuration does not trigger a device revision. For example, modifying certain SD-WAN Overlay policies does not result in policy changes on devices.

How do I set the SD-WAN Overlay permission for an IAM user with the RBAC profile?

For more information about configuring portal-based permissions, refer to the Fortinet Identity & Access Management (IAM) guide.

To grant an IAM user access to SD-WAN Overlay features in FortiGate Cloud:

1. Log in to the Fortinet IAM portal.
2. In the left navigation panel, go to *Permission Profile*.
3. Either edit an existing profile or click *Add New* to create a new one.
4. Under the *Permission Profile* section, click *Add Portal* if FortiGate Cloud has not yet been added.
5. In the *Resources* list for FortiGate Cloud, locate and set the SD-WAN Overlay permission according to the desired access level.
6. Apply the updated permission profile to the appropriate IAM user.

If the IAM user still cannot access SD-WAN Overlay after updating permissions, try clearing the browser cache to ensure the latest permission settings are applied.

How do I set the FortiConverter permission for an IAM user with the RBAC profile?

For more information about configuring portal-based permissions, refer to the Fortinet Identity & Access Management (IAM) guide.

To grant an IAM user access to FortiConverter features in FortiGate Cloud:

1. Log in to the Fortinet IAM portal.
2. In the left navigation panel, go to *Permission Profile*.
3. Either edit an existing profile or click *Add New* to create a new one.
4. Under the *Permission Profile* section, click *Add Portal* if FortiGate Cloud has not yet been added.
5. In the *Resources* list for FortiGate Cloud, locate and set the FortiConverter permission according to the desired access level.
6. Apply the updated permission profile to the appropriate IAM user.

If the IAM user still cannot access FortiConverter after updating permissions, try clearing the browser cache to ensure the latest permission settings are applied.

Why has log uploading stopped with an alert icon under Last Log Upload column?

A free-tier FortiGate managed by FortiGate Cloud is required to run the latest FortiOS patch version. If the FortiGate is not upgraded within seven (7) days after a new FortiOS patch becomes available, an alert icon will be displayed. This indicates that log uploading has been suppressed, and other FortiGate Cloud features may also be impacted.

If the FortiGate is already running the latest FortiOS patch version but FortiGate Cloud does not reflect the updated status, please ensure that the device is properly managed by FortiGate Cloud. You may also run the following CLI commands to refresh the FortiGuard status:

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

diagnose fdsm contract-controller-update
```

This requirement does not apply to FortiGate devices registered with a valid FortiGate Cloud subscription.

This requirement does not apply to FortiGate devices registered with a valid FortiGate Cloud subscription.

www.fortinet.com

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