



Administration Guide

FortiGate Cloud 25.2.a



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

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

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



September 24, 2025

FortiGate Cloud 25.2.a Administration Guide

32-252a-1151448-20250924

TABLE OF CONTENTS

Change log	7
Introduction	8
Features	8
Requirements	9
Getting started with FortiGate Cloud	10
Port and access control information	12
Subscription types	13
Feature comparison	14
Dashboard	17
Status	18
Network	18
Security	18
SD-WAN	20
FortiView	21
Assets	23
Cloud provisioning	24
Accessing a FortiGate	27
Transferring a FortiGate to another FortiGate Cloud account	29
Sandbox	32
Settings	33
Analytics	35
Reports	35
Reports reference	37
Logs	40
IOC	42
SD-WAN Overlay	44
Prerequisites	44
Creating the initial topology	45
Provisioning the SD-WAN configuration to your sites and viewing tasks	45
Failed configurations	46
Topology	46
Site	47
Creating a site	47
Editing a site	49
Deleting sites	50
Settings	50
Overlay policy	51
Creating a policy	51
Viewing policies	53
Applying policies	54
Managing policies	54
Policy example	55

Addresses	58
Creating an address	59
Creating an address group	59
Managing address objects and groups	60
IPAM	61
Configuring IPAM	61
Managing IPAM	61
Services	62
Creating a service	62
Creating a service group	63
Creating a service category	63
Managing services	63
Schedules	65
Creating a recurring schedule	65
Creating a one-time schedule	65
Creating a schedule group	66
Managing schedules	66
IP Pools	67
Creating an IP pool	68
Managing IP pools	68
Security profiles	69
AntiVirus	69
Web Filter	70
Application Control	71
Intrusion Prevention	72
Application signatures	73
IPS signatures	73
Configuration	74
CLI scripts	76
Administration	77
Automation	77
Firmware management	78
Accounts and users	80
Creating an account	81
User management	81
User settings	82
Audit	85
Multitenancy	86
OU Dashboard	87
OU Asset list	89
API access	92
Frequently asked questions	94
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?	94
Why can I log into the FortiGate Cloud but not activate the FortiGate Cloud	95

account in FortiOS with the same credentials?	
How can I activate my FortiGate Cloud on HA-paired FortiGates?	95
How can I establish a management tunnel connection between my FortiGate and FortiGate Cloud?	95
What do I do if a FortiGate added by its cloud key stays in an inactive state for more than 24 hours?	96
What do I do if the "Device is already in inventory" message appears when importing a FortiGate by key?	96
What do I do if the invalid key message appears when importing a FortiGate by key?	96
What do I do if FortiGate Cloud activation via the FortiOS GUI succeeds, but I cannot find the FortiGate in the FortiGate Cloud portal?	96
How can I move a FortiGate from region A to region B?	97
How can I connect to FortiGate by remote access?	97
How can I activate FortiGate Cloud using a different email FortiCare account when FortiOS does not allow entering another email?	97
What do I do if the migrate notice still appears after successful migration?	97
What do I do if FortiDeploy does not work?	98
What do I do if FortiOS does not upload logs?	98
What do I do if FortiGate Cloud cannot retrieve logs from FortiOS when the data source is set as FortiGate Cloud?	98
How can I export more than 2000 lines of logs?	99
Why does FortiGate Cloud drop some logs from my FortiGate?	99
How can I receive a daily report by email?	99
Why does FortiGate not submit files for Sandbox scanning?	99
What backup retention does FortiGate Cloud provide?	100
How does automatic backup work?	100
What does it mean if a geolocation attribute configuration change log/alert is received?	100
What do I do if FortiGate Cloud does not reflect a new hostname on a FortiGate or FortiGate Cloud overwrites a new FortiGate hostname?	100
Why is my FortiGate provisioned to a region other than global (U.S. or Europe)?	101
How do I check if my FortiGate has been preset for a specific server location? ..	101
Can I change the server location configuration?	101
If my FortiGate's server location is automatic/any, how do I provision it to my preferred region?	102
Can I migrate logs uploaded or reports generated to a different region?	102
What should I do if I accidentally upgrade FortiOS to 7.4.2 or higher on a FortiGate without a FortiGate Cloud Service subscription and remote access to the device becomes read-only?	102
After I transfer my FortiGate to another account in the Asset Management portal, do I still need to transfer it in FortiGate Cloud?	103
Does FortiGate Cloud support data backups and disaster recovery?	103
What happens if you enable the automatic firmware upgrade on FortiGate Cloud and the FortiGate?	103

Can I disable automatic firmware upgrade from FortiOS by logging in directly to the FortiGate that has no FortiGate Cloud subscription to bypass the automatic firmware upgrade enforcement from FortiGate Cloud?	104
How can I activate FortiGate Cloud on a FortiGate provisioned to an OU placeholder account?	104
Why do some of my legacy email users from FortiGate Cloud not appear after going to the Migrate to IAM page?	105
SD-WAN Overlay	105
What is the maximum number of FortiGates that the SD-WAN Overlay feature supports?	105
What is the difference between a branch and DC site?	105
What does the SD-WAN Overlay agent do?	105
When you push SD-WAN Overlay policy changes to a FortiGate, does FortiGate Cloud overwrite other locally changed parameters for an affected policy?	106
Why does pushing some changes from FortiGate Cloud SD-WAN Overlay not create a revision in FortiGate Cloud?	106

Change log

Date	Change description
2025-05-28	Initial release.
2025-06-03	Updated IOC on page 42.
2025-06-04	Updated: <ul style="list-style-type: none">• Assets on page 23• Audit on page 85• Firmware management on page 78
2025-06-05	Updated To provision a FortiGate/FortiWifi to FortiGate Cloud using the FortiCloud key: on page 25.
2025-06-11	Added Transferring a FortiGate to another FortiGate Cloud account on page 29.
2025-06-23	Updated Feature comparison on page 14.
2025-06-27	Updated: <ul style="list-style-type: none">• Requirements on page 9• API access on page 92• Logs on page 40
2025-07-08	Added SD-WAN Overlay on page 105.
2025-07-09	Updated SD-WAN Overlay on page 105.
2025-07-23	Updated Port and access control information on page 12 Added Why do some of my legacy email users from FortiGate Cloud not appear after going to the Migrate to IAM page? on page 105.
2025-08-12	Updated User management on page 81.
2025-09-24	Updated Port and access control information on page 12.

Introduction

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

The cloud-based SaaS offers configuration management for FortiGates, FortiGate-VMs with FortiGate-connected FortiAPs, FortiSwitches, and FortiExtenders. FortiGate Cloud simplifies network and security management with zero-touch provisioning, firewall configuration and policies, cloud backups, firmware upgrades, rich log analytics, reporting, and audit log, and includes one-year log retention.

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

[Features on page 8](#) 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

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.
Assets	Device inventory as list or on map with diagnostic health, network statistics, and subscription information.
Device management	Real-time FortiGate configuration management from the cloud to configure your network interfaces, SD-WAN, firewall policies, security profiles, VPN, and Security Fabric.
Log analysis	Real-time traffic, events, system logs for network activity, and threat analysis.
Centralized reports	Generate on-demand reports or schedule and get predefined reports delivered at intervals for network analytics and monitor usage patterns.
Firmware upgrade	Remotely upgrade FortiOS on FortiGate devices.
AP, FortiSwitch, and FortiExtender management via FortiGate	<ul style="list-style-type: none"> • Manage FortiAPs, AP profiles, SSIDs, and monitor WiFi clients and NAC policies • Manage FortiSwitches, VLANs, ports, and policies • Manage FortiExtenders, profiles, and data plans
FortiSandbox SaaS	Upload and analyze files that FortiGate antivirus marks as suspicious.
Indicators of Compromise	Alerts on newly found infections and threats to devices in the network
Regions	FortiGate Cloud includes the Global (Canada), U.S., and Europe (Germany) regions.
Multitenancy	Multitenancy based on FortiCloud Organizations. FortiGate Cloud does not support subaccount-based multitenancy.
Inline cloud access	Access the GUI for provisioned FortiGates running FortiOS 7.0 and later versions.

Requirements

Requirement	Description
FortiCloud account	Create a FortiCloud account if you do not have one. Launching FortiGate Cloud 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.

Requirement	Description
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 high-end, mid-range, and entry-level FortiGate models up to the FortiGate 3701F. You can find more information about FortiGate models and specifications on the [Fortinet website](#). All FortiWifi models support FortiGate Cloud.

See [Product Life Cycle](#). If the end of support (EOS) of the highest firmware version that a platform can support has been reached, FortiGate Cloud supports this platform until its hardware EOS is also reached.

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

The following summarizes FortiGate Cloud support for older FortiOS versions:

- FortiGate Cloud supported FortiOS 5.X and 6.2 until March 31, 2024.
- FortiOS 6.4:
 - FortiGate Cloud will support FortiGates on FortiOS 6.4 with an Elite subscription until March 31, 2026.
 - Devices with a FortiGate Cloud subscription running FortiOS 6.4 and later versions are exempt from firmware EOS enforcement.

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.

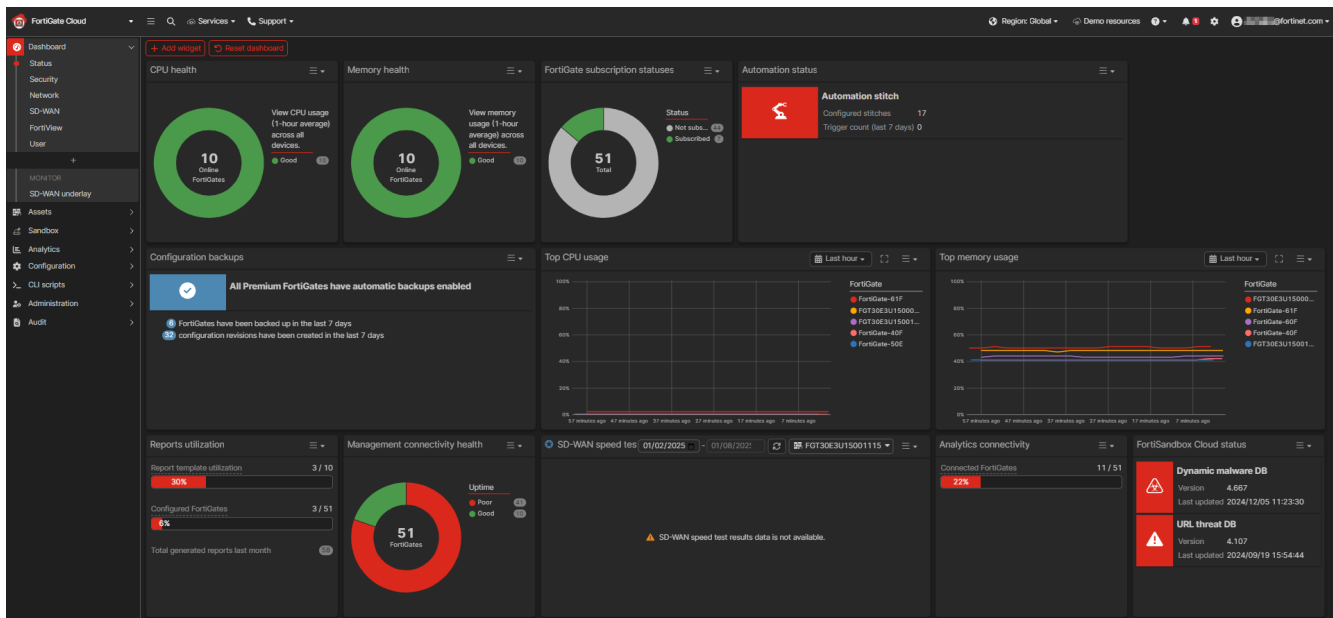
Purpose	Protocol	Port
Portal and controller	TCP	443
Analytic connection		514
Management connection		541

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 27 .
Menu icon	Use the menu icon to collapse or display the left pane, which displays other configuration options.
Search icon	Click the search icon to access a searchbar. You can search for a FortiGate Cloud GUI page or widget with a name that contains your search term. See To search for a GUI page or widget: on page 12 .
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.

To search for a GUI page or widget:

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

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

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

Option	Description
Dashboard	<i>Dashboard</i> displays a variety of widgets. The widgets provide information about the devices that your FortiGate Cloud is managing.
Assets	View a centralized inventory of all FortiGate and FortiWifi devices. See Assets on page 23 .
Sandbox	View the scan results from files that Sandbox submitted to FortiGuard for threat analysis. See Sandbox on page 32 .
Analytics	Create and alter report configurations and their settings. These report configurations are available for all provisioned devices. See Analytics on page 35 .
Configuration	Manage FortiGate Cloud account and Sandbox settings. See Configuration on page 74 .
CLI Scripts	Configure and schedule scripts of CLI commands to run on your FortiGates. See CLI scripts on page 76 .
Administration	Configure automation and firmware management options. See Administration on page 77 .
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

Region	IP address range
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
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:

Description	SKU
FortiGate Cloud subscription	
Management, Analytics, and one-year log retention for FortiGate, FortiGate VM/VM-S, and FortiWiFi	FC-10-00XXX-131-02-DD
FortiGate Cloud Advanced subscription	
Management, Analytics, and one-year log retention, plus SD-WAN overlay-as-a-service and extended security operations (indicators of compromise)	FC-10-XXXXXX-1125-02-DD

The following are add-on subscriptions to enhance your FortiGate Cloud:

Description	SKU
FortiSandbox SaaS (per device)	
FortiSandbox SaaS for FortiGate	FC-10-XXXXXX-811-02-DD
	FC-10-XXXXXX-950-02-DD
	FC-10-XXXXXX-928-02-DD
	FC-10-XXXXXX-100-02-DD
FortiDeploy	
Bulk provisioning	FDP-SINGLE-USE

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

For multitenancy using FortiCloud organizations, see [Standard versus unlimited access to the Organization Portal](#).

For FortiSandbox SaaS upload limits, see [Sandbox on page 32](#).



Provisioning FortiGates to FortiGate Cloud does not require a subscription. For limitations without a subscription, see [Feature comparison on page 14](#). All devices must be registered on the [Fortinet Support site](#).

For pricing information, contact your Fortinet partner or reseller.

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

Feature comparison

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

Feature	No subscription	FortiGate Cloud subscription	FortiGate Cloud Advanced subscription
CLI scripts	No	Yes	Yes
Cloud access	Read-only The following FortiOS versions support read-only cloud access: <ul style="list-style-type: none"> • 7.0.14 and later • 7.2.8 and later • 7.4.2 and later • 7.6 	Read/write The following FortiOS versions support read/write cloud access: <ul style="list-style-type: none"> • 7.0.2 and later • 7.2 • 7.4 • 7.6 	Read/write The following FortiOS versions support read/write cloud access: <ul style="list-style-type: none"> • 7.0.2 and later • 7.2 • 7.4 • 7.6
Cloud management, configurations, and backups	No	Yes	Yes
Cloud provisioning	Yes	Yes	Yes
Customizable patch firmware upgrade	No	Disabled by default and can be enabled	Disabled by default and can be enabled
Event automation	No	Yes	Yes

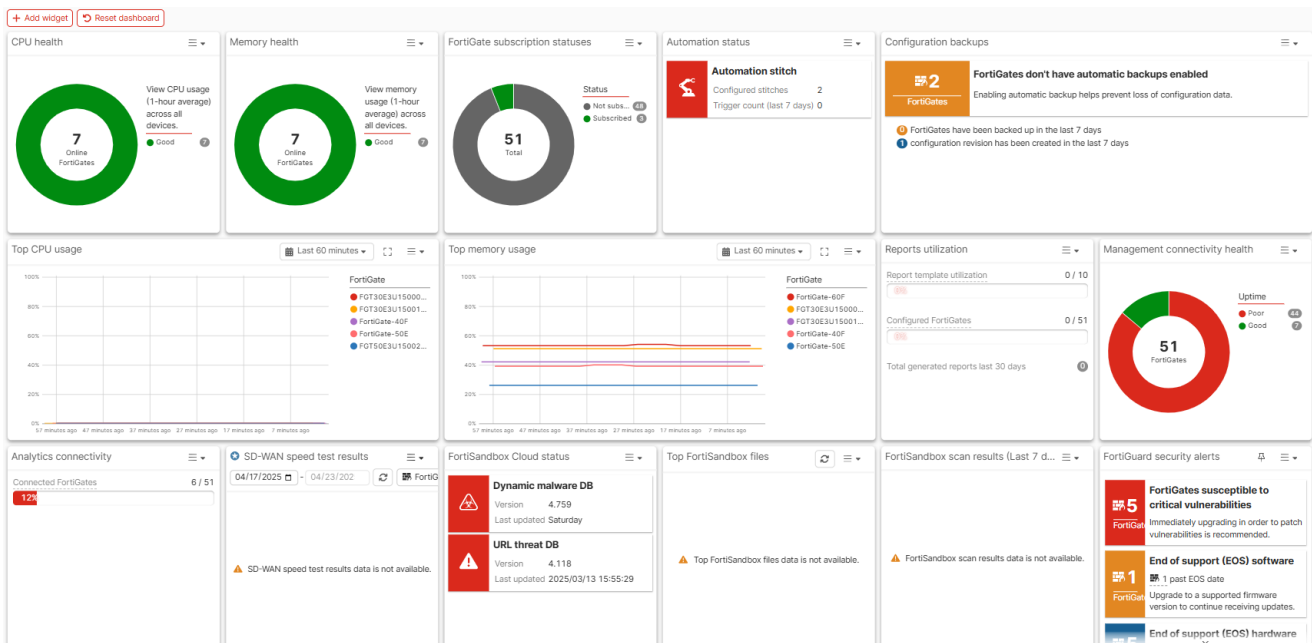
Feature	No subscription	FortiGate Cloud subscription	FortiGate Cloud Advanced subscription
Extended security operations (indicators of compromise)	No	No	Yes
Hosted log retention	Seven days	One year	One year
Manual firmware upgrade	Yes, only to the latest patch available. You must manually upgrade a FortiGate without a paid subscription to the latest patch within seven days of the patch becoming available. If the FortiGate is not upgraded within seven days, log upload and cloud access are restricted. See Firmware management on page 78.	Yes	Yes
Raw log download	No	Yes	Yes
Remote access	Yes (read-only) For the following FortiOS versions, remote access with full permission (read and write) requires a registered FortiGate Cloud Service subscription on the FortiGate. <ul style="list-style-type: none"> • 7.6.0 and later versions • 7.4.2 and later versions • 7.2.8 and later versions • 7.0.14 and later versions 	Yes (read-write)	Yes (read-write)

Feature	No subscription	FortiGate Cloud subscription	FortiGate Cloud Advanced subscription
	Devices without a registered FortiGate Cloud Service Subscription running these FortiOS versions only support read-only remote access.		
Reports	360 degree activity report only	Multiple predefined reports	Multiple predefined reports
SD-WAN monitoring	No	Yes	Yes
SD-WAN overlay-as-a-service	No	No	Yes

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.

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



FortiGate Cloud contains the following dashboards:

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

You can also create a custom dashboard.

The following tables list the widgets available for each dashboard:

Status

Widget	Description
FortiGate subscription statuses	Displays how many FortiGates do not have a paid subscription and how many have a 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.

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.

Security

Widget	Description
FortiSandbox Cloud status	Displays the database versions and last updated dates for the dynamic malware and URL threat databases.

Widget	Description
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)	<p>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.</p> <p>This widget does not display if you are using the new IOC service, which the Advanced subscription supports. See IOC on page 42.</p>
Risk website visitors	Users who visited a website determined as a risk.
Malware victims	Users whose device is affected by malware.
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.

UPGRADE FORTIGATES AFFECTED BY CRITICAL VULNERABILITIES

- Patch upgrades for the FortiGates affected by critical vulnerabilities will be downloaded and installed during the specified upgrade schedule.
- The FortiGates will reboot during the upgrade.
- FortiGates can only be upgraded here if they have a FortiGate Cloud subscription and do not already have upgrades scheduled.

Upgrade schedule

Immediate

Custom

+

Q Search

Q

FortiGate	Firmware	Target version
<div></div> <div>FGT30E</div>	<div></div> <div>v6.2.15 build1378</div>	v6.2.16 build1392
<div></div> <div>FortiGate</div> <div>FGVMEV</div>	<div></div> <div>v5.4.0 build0721 (EOS)</div>	
<div></div> <div>1900</div> <div>FG4H1E</div>	<div></div> <div>v6.4.0 build1579 (EOS)</div>	v6.4.15 build2095
<div></div> <div>FGT30E</div>	<div></div> <div>v6.2.15 build1378</div>	v6.2.16 build1392
<div></div> <div>FGT60D</div>	<div></div> <div>v6.0.17 build0528</div>	v6.0.18 build0549
<div></div> <div>FWF60D</div>	<div></div> <div>v6.0.0 build0076</div>	v6.0.18 build0549
<div></div> <div>FortiGate</div> <div>FGT50E</div>	<div></div> <div>v6.2.14 build1364</div>	v6.2.16 build1392

8

Updated: 13:00:24

OK

Cancel

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.

Widget	Description
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

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

Widget	Description
Top sources	Top traffic sessions aggregated by source.
Top destinations	Top traffic sessions aggregated by destinations.
Top threats	Top traffic sessions aggregated by threats.
Top websites	Top traffic sessions aggregated by websites.
Top attacks	Counts the attacks that the device's IPS most frequently prevents.
Top applications	Compares which applications are most frequently used, based on the device's Application Control settings.
Top application categories	Compares which application categories are most frequently used, based on the device's Application Control settings.
Top applications by threat score	Compares which applications have the most traffic compared to their threat score, based on the device's Application Control settings.
Top DLP by rules	Counts the DLP events that the device detects, sorted by DLP rule.
Top spam	Displays which sources send the most spam email into the network.
Top virus	Counts the viruses that the device's AV most frequently finds.
Top protocols	Compares the traffic volume that has passed through a certain interface, based on which protocol it uses: <ul style="list-style-type: none"> • HTTP • HTTPS • DNS • TCP • UDP • Other

Widget	Description
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.

Assets

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

For instructions on provisioning a FortiGate to FortiGate Cloud, see [Cloud provisioning on page 24](#).

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

- Serial number
- Fortinet product type
- Firmware version
- Management connectivity status (If the device is connected through a management tunnel)
- Current diagnostics (device CPU and memory usage)
- Subscription status
- Configuration save mode. See [Using configuration save mode](#).
- Last log upload time
- Folder name: asset folder that the device belongs to. FortiGate Cloud pulls the folder structure from FortiCloud.

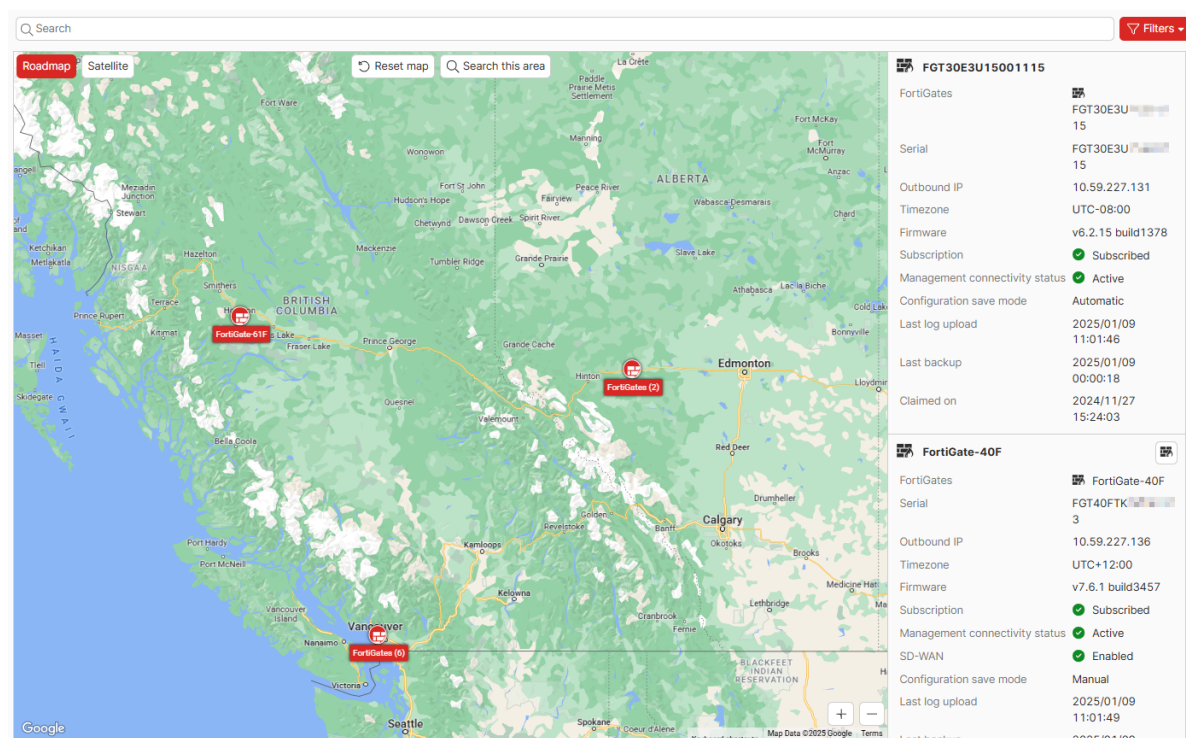
You can use the dropdown list on the right to view FortiGates grouped by subscription status or high availability cluster, or with no grouping. In the example, *Group by subscription* is selected. FortiGate Cloud displays the list of FortiGates separated into two groups: FortiGates with a subscription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

FortiGate	Firmware	Management connectivity	Current diagnostics	Subscription	Configuration save mode	Deployed To
FortiGates with a FortiGate Cloud subscription 7						
FGT30E3	v6.2.15 build1378	Active	0% CPU 41% Memory	Subscribed	Automatic	FortiGateCl
FortiGate FGT40FT	v7.6.1 build3457	Active	0% CPU 42% Memory	Subscribed	Manual	FortiGateCl
FortiGate FGT50E3	v6.2.14 build1364	Active	0% CPU 26% Memory	Subscribed	Automatic	FortiGateCl
FortiGate FGT60FT	v7.6.1 build3457	Active	0% CPU 44% Memory	Subscribed	Automatic	FortiGateCl
FortiGate FGT61FT	v7.6.1 build3457	Active	0% CPU 49% Memory	Subscribed	Automatic	FortiGateCl
FWF60E1	v6.4.15 build2095	Active	0% CPU 28% Memory	Subscribed	Automatic	FortiGateCl
FortiGate FGVM6V	v5.4.0 build0721 (E...	Inactive		Subscribed	Automatic	FortiGateCl
FortiGates without a FortiGate Cloud subscription 44						
FGT30E3U	v6.2.15 build1378	Active	0% CPU 51% Memory	Not subscribed	Automatic	FortiGateCl

To view historical diagnostics data for a device:

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

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



Cloud provisioning

Cloud provisioning 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](#)

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.



For FortiGates that are part of a high availability (HA) pair, you must activate FortiGate Cloud on the primary FortiGate. Activate FortiGate Cloud on the primary FortiGate as [To provision a FortiGate or FortiWifi to FortiGate Cloud in the FortiOS GUI: on page 26](#) 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.

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

1. Log in to [FortiGate Cloud](#).
2. Go to *Assets > Asset list*, then click *Add FortiGate*.
3. Click *Import FortiGate*.
4. In the *FortiCloud or FortiDeploy key* field, enter your key value.
5. For *End user type*, select *A non-government user* or *A government user* as required.
6. From the *Partner* dropdown list, select the affiliated Fortinet partner.
7. To provision your FortiGate to FortiGate Cloud after import, enable *Provision after import*.
8. If desired, you can associate a script with the provisioning. The selected script executes 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 76](#) 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.
9. Click *OK*.



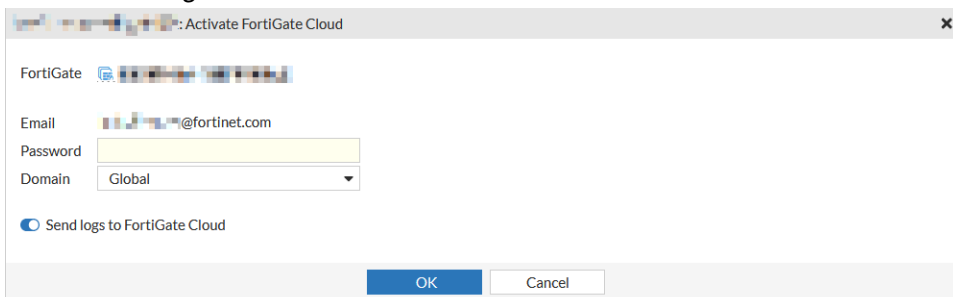
After FortiGate Cloud successfully provisions the device, the device key becomes invalid. You can only use the key once to provision a device.

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

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

To provision a FortiGate or FortiWifi to FortiGate Cloud 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*.



The screenshot shows a dialog box titled "Activate FortiGate Cloud". It contains the following fields and controls:

- FortiGate:** A dropdown menu showing a selected device.
- Email:** A text field containing "@fortinet.com".
- Password:** A text field for entering the password.
- Domain:** A dropdown menu set to "Global".
- Send logs to FortiGate Cloud:** A checkbox that is checked.
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

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
```

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.

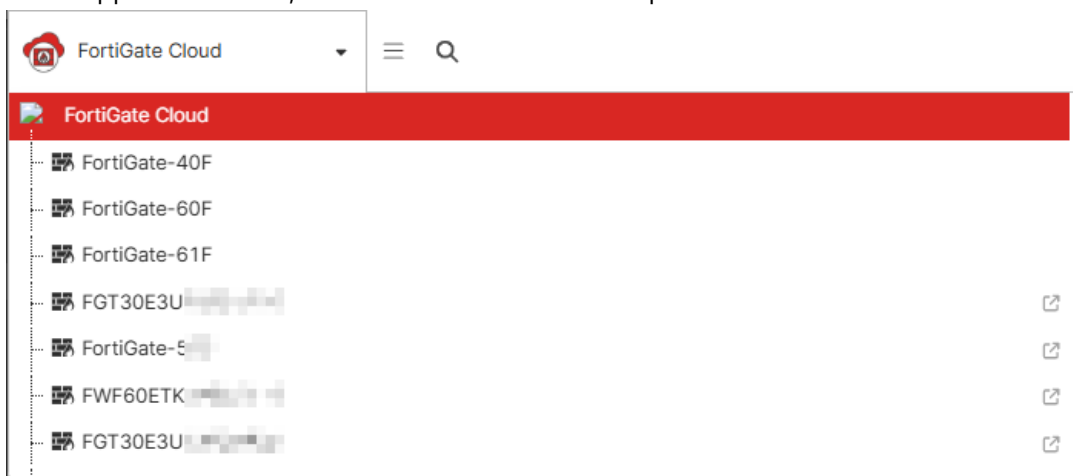
Therefore, when viewing logs on the affected FortiGate, you may see 4aa567e55bc8@fortigatecloud.com or FortiGateCloud as a username. For managed security service provider customers, this provides enhanced security by preventing subusers from seeing the primary account email address in the FortiGate logs.

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](#).

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

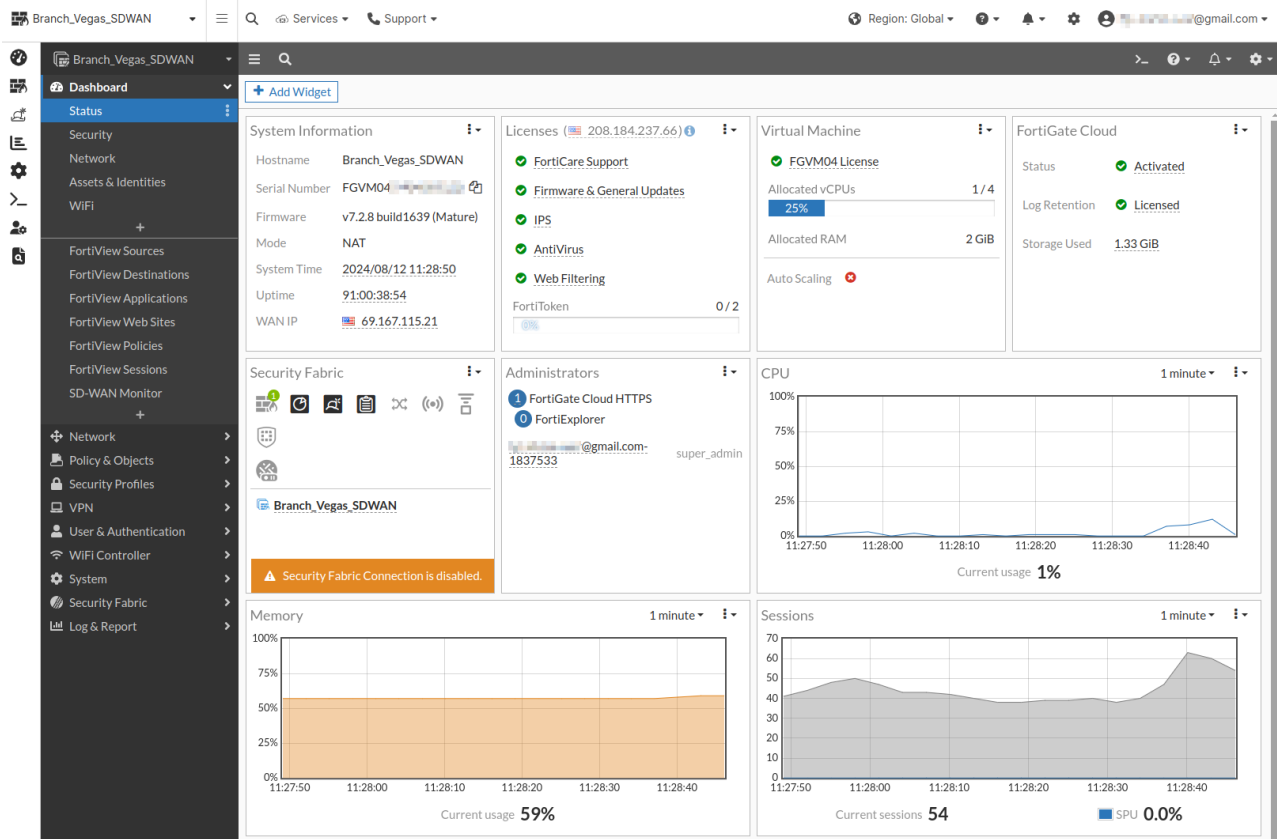
To remotely access and configure a FortiGate:

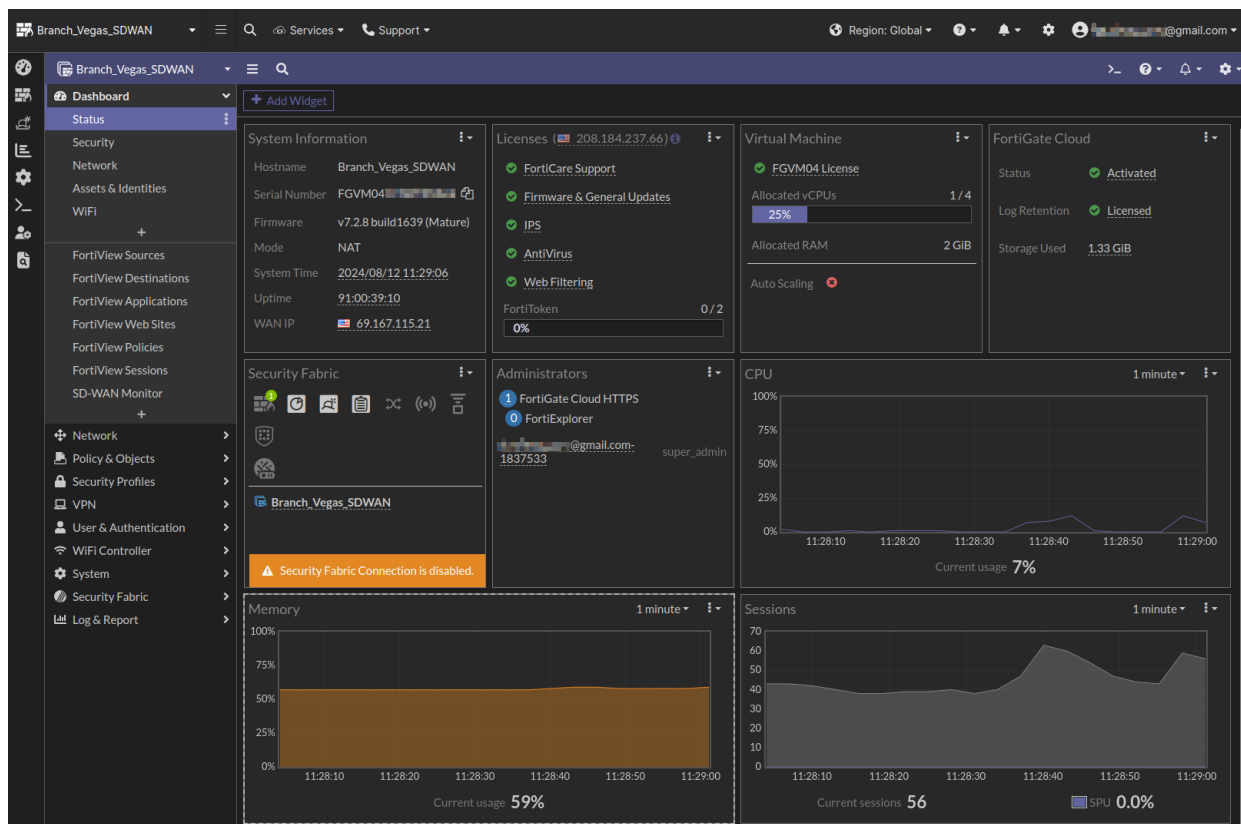
1. Do one of the following:
 - In the upper left corner, click the *FortiGate Cloud* dropdown list and select the desired FortiGate.



- Go to *Assets > Asset list*. Select the desired FortiGate, then click *Cloud access*.

2. If the FortiGate does not have a subscription, FortiGate Cloud displays a warning that you will have read-only access. Click **OK**.
3. FortiGate Cloud displays the FortiOS interface in the browser window. You do not need to enter credentials to log in to the FortiGate. View and make changes as desired. The following shows the FortiOS GUI as shown in FortiGate Cloud, in light and dark modes:





4. 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).


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 *Assets > Asset list*.
 - 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 the email address that you configured in step 6 and your email address. 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.

ASSET TRANSFER

Select FortiGate

 fgtvm-pg-premium02

×

+

Email

me@fortinet.com

History data

Transfer to destination account ▼

End user type

☒ **A non-government user**

☐ **A government user**
In this context, a government end-user is any central, regional or local government department, agency, or other entity performing governmental functions, including:

1. Governmental research institutions.

2. Governmental corporations or their separate business units which are engaged in the manufacture or distribution of items or services controlled on the Wassenaar Munitions List.

3. International governmental organizations.

OK

Cancel

- 2. Log in to FortiGate Cloud using account B credentials.
- 3. Go to *Assets > Asset list*.
- 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.

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.

Settings

SANDBOX SETTINGS

Setting

☒ **Enable Alert Setting**

Log Retention
 Include past day(s) of data. (The limit of max days is 365)
* Data retention: Free - 7 days. Paid: 7 days of clean rating records and 1 year of malicious/suspicious records.

Malware Package Options
 Include job data of the following rating:
☒ Malware
☐ High Risk
☐ Medium Risk
* Please enable FortiSandbox Database on Fortigates to receive this update

URL Package Options
 Include job data of the following rating:
☒ Malware
☐ High Risk
☐ Medium Risk

Device Selections

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

Setting	Description
<i>Enable Alert Setting</i>	<ul style="list-style-type: none"> • Enable alert emails

Setting	Description
	<ul style="list-style-type: none">• Enter multiple email addresses (separated by commas) to receive alerts• Set which severity levels trigger FortiGate Cloud to send alert emails
<i>Log Retention</i>	Set number of days to retain log data.
<i>Malware Package Options</i>	Select the data risk level that FortiGate Cloud automatically submits to FortiGuard to further antithreat research.
<i>URL Package Options</i>	
<i>Device Selections</i>	Select the desired FortiGates to enable Sandbox detection for.

To configure Sandbox alert emails:

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

Analytics

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

Reports

To schedule a report:

1. Go to *Analytics > Scheduled reports*.
2. Select the desired report.
3. Click *Customize*.
4. In the *Select FortiGate* field, select the desired FortiGates to run the report for.
5. 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 > Scheduled reports*.
2. Select the desired report, then click *Run report*.
3. In the *Select FortiGate* field, select the desired FortiGates to run the report for.
4. In the *Start time* and *End time* fields, configure the desired time range to include in the report.
5. If desired, enable *Send report to* and select an email address 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 > Scheduled reports*.
 - b. Click *Manage email groups*.
 - c. Click *Create*.
 - d. In the *Name* field, enter the email group name.
 - e. In the *Subject* field, enter the email subject line.
 - f. In the *Body* field, enter the email body content.
 - g. In the *Description* field, enter the email description.

- h.** In the *To* field, enter the email addresses to send the email to.

NEW EMAIL GROUP

Name

Subject

Body

0/1024

Description

Recipients

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.

CUSTOMIZE SCHEDULE

Name: 360 Degree Activities Report

Description: Overview of user browsing activity.

Select FortiGate: FortiGate-61F

Status: ☒ Enabled ☐ Disabled

Selected devices won't be saved if Status is set as Disabled.

Custom report logo: Upload File. Click to select or drop file here. .jpg Max: 512 KiB. No custom image in use.

Schedule type: ☒ Day(s) ☐ Week(s) ☐ Month(s)

Output: Send report to ☒ Email Security Team

OK Cancel

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

- WiFi 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 > 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.

The screenshot shows the 'Raw logs' interface in FortiGate. At the top, there are buttons for 'Browse logs', 'Download', and a search bar. Below these is a table with columns: 'File name', 'Log period start', and 'Log period end'. The table lists various log files categorized by type (Anomaly, Antivirus, Application, DLP, DNS, Email filter, Event, File filter, IPS, SSH). On the right side, there is a dropdown menu for selecting a FortiGate device, currently showing 'FortiGate-40F'. Below the dropdown is a search bar and a list of subscribed devices.

File name	Log period start	Log period end
Anomaly		
<input checked="" type="checkbox"/> FGT40FTK ..._mlog_20250109-0953-20250111-0953.log.gz	2025/01/08 12:53:11	2025/01/10 12:53:11
Antivirus		
<input type="checkbox"/> FGT40FTK ..._vlog_20250109-0953-20250111-0953.log.gz	2025/01/08 12:53:11	2025/01/10 12:53:12
Application		
<input type="checkbox"/> FGT40FTK ..._rlog_20250109-0952-20250111-0953.log.gz	2025/01/08 12:52:11	2025/01/10 12:53:12
DLP		
<input type="checkbox"/> FGT40FTK ..._dlog_20250109-2354-20250110-0953.log.gz	2025/01/09 02:54:37	2025/01/09 12:53:11
<input type="checkbox"/> FGT40FTK ..._dlog_20250109-0954-20250111-0958.log.gz	2025/01/08 12:54:12	2025/01/10 12:58:15
DNS		
<input type="checkbox"/> FGT40FTK ..._log_20250109-0953-20250111-0953.log.gz	2025/01/08 12:53:11	2025/01/10 12:53:11
Email filter		
<input type="checkbox"/> FGT40FTK ..._slog_20250109-2355-20250110-0953.log.gz	2025/01/09 02:55:38	2025/01/09 12:53:12
<input type="checkbox"/> FGT40FTK ..._slog_20250109-0954-20250111-0958.log.gz	2025/01/08 12:54:12	2025/01/10 12:58:15
Event		
<input type="checkbox"/> FGT40FTK ..._elog_20250109-0953-20250111-0953.log.gz	2025/01/08 12:53:11	2025/01/10 12:53:11
File filter		
<input type="checkbox"/> FGT40FTK ..._llog_20250109-2354-20250110-0953.log.gz	2025/01/09 02:54:37	2025/01/09 12:53:12
<input type="checkbox"/> FGT40FTK ..._llog_20250109-0954-20250111-0958.log.gz	2025/01/08 12:54:12	2025/01/10 12:58:15
IPS		
<input type="checkbox"/> FGT40FTK ..._alog_20250109-0953-20250111-0953.log.gz	2025/01/08 12:53:11	2025/01/10 12:53:11
SSH		

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.

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	<ul style="list-style-type: none">• 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 an Advanced 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 > Threats*. This page displays a table of data for any detected threats.

Indicator of Compromise									
<div><div>Refresh</div><div>Search</div><div>FGT60FTK</div><div>Last 30 days</div><div>Export</div></div>									
Source (IP/User)	Last Detected	Rescanned	Host Name	OS	Log Types	Security Actions	Verdict	# of Threats	Device Name
172.16.15.105	2025/02/27 18:20:33	No	172.16.15.105		dns	pass	Infected	1	FGT60FTK
172.16.68.121/Tom	2025/02/27 18:20:24	No	Lab-PC1	Linux	traffic	accept	Infected	1	FGT60FTK
172.16.68.122/Jack	2025/02/27 18:20:15	No	Office-PC2	Windows	traffic	accept	Infected	1	FGT60FTK
172.16.95.121	2025/02/27 18:19:29	No	172.16.95.121		web filter	passthrough	Infected	1	FGT60FTK
172.16.95.182/Jane	2025/02/27 18:19:26	No	172.16.95.182		web filter	passthrough	Infected	1	FGT60FTK
172.16.95.182/Jane	2025/02/27 18:19:27	No	172.16.95.182		web filter	allow	Infected	1	FGT60FTK
172.16.95.23	2025/02/27 18:19:30	No	172.16.95.23		web filter	passthrough	Infected	1	FGT60FTK
172.16.95.232	2025/02/27 18:19:28	No	172.16.95.232		web filter	passthrough	Infected	1	FGT60FTK
172.16.95.24	2025/02/27 18:19:31	No	172.16.95.24		web filter	passthrough	Infected	1	FGT60FTK
172.16.95.25	2025/02/27 18:19:22	No	172.16.95.25		web filter	passthrough	Infected	1	FGT60FTK

Above the table are the following options:

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

The table displays the following columns of data:

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

You can configure trigger-based automated alerts for IOC events. See [Automation on page 77](#).

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 an Advanced subscription. See [Subscription types on page 13](#).

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.
- FortiGate Cloud Advanced subscription for all spokes.
- 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.

Primary Hub Locations ⓘ	<input type="text" value="USA-Plano-Texas"/>	<input type="button" value="Save"/>
Secondary Hub Locations ⓘ	<input type="text" value="USA-Washington-DC"/>	<input type="button" value="Save"/>
Reserved Subnet	<input type="text" value="10.200.0.0"/>	<input type="button" value="Save"/>
Hub and spoke configurations	<input type="text" value="Up to date"/>	<input type="button" value="Update"/>



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 47](#) describes.
4. Configure the site to include ISP and subnet settings as [Editing a site on page 49](#) 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 47](#), [Editing a site on page 49](#) and [Provisioning the SD-WAN configuration to your sites and viewing tasks on page 45](#).

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 47](#) and [Editing a site on page 49](#)
3. Go to *SDWan Overlay > Overlay policy*. Configure a desired policy. See [Creating a policy on page 51](#).
4. Apply the policy. See [Applying policies on page 54](#). 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*.

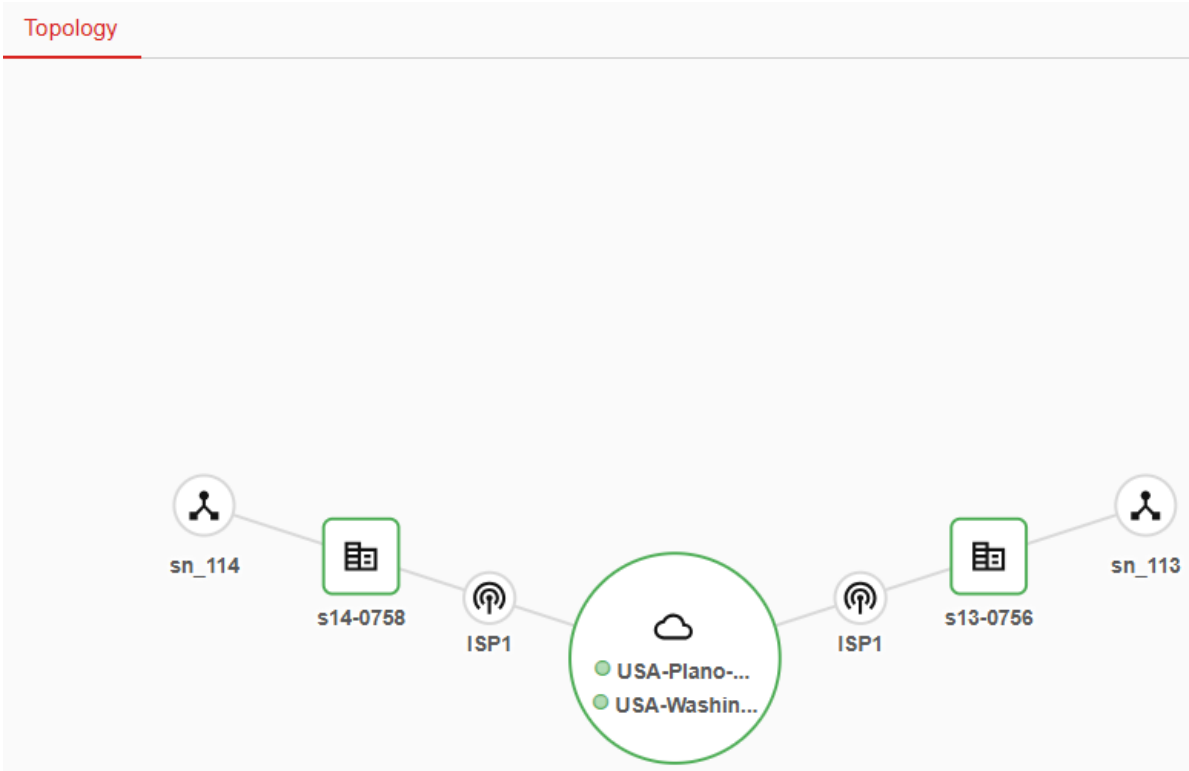
You can retry the connection for each asset from *Tasks* in case the issue has been resolved.

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.

<div><div><div>+ Create</div><div>Edit</div><div>Delete</div></div><div><div>Search</div></div></div>				
<input type="checkbox"/>	Site	Status	Type	Devices
<input type="checkbox"/>	s13-0756	all-pass	Branch	FGVM08TM
<input type="checkbox"/>	s14-0758	all-pass	Branch	FGVM08TM
<input type="checkbox"/>	mySite	disconnected	Branch	FGVM08TM

- This section includes:
- [Creating a site on page 47](#)
 - [Editing a site on page 49](#)
 - [Deleting sites on page 50](#)

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 45](#).

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*.

NEWSITE

Site

Name

Deployment ISP Subnet

Role

Branch Data Center

Description

SLA Latency Threshold

ms

Device

Now only one device or all devices in the same HA cluster are supported per site. To add device, please remove the existing one.

OK

Cancel

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

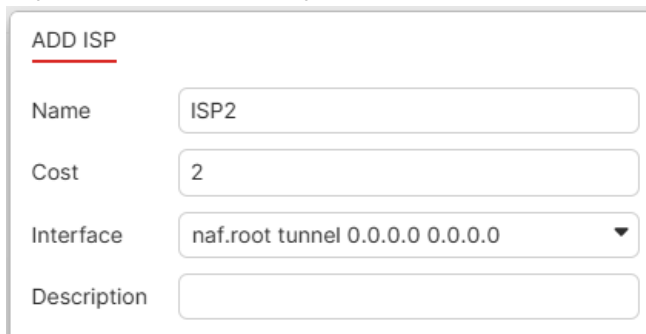
You can edit a site to define the ISP and LAN subnet from the *Site* page.

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.

Primary Hub Locations ⓘ	<input type="text" value="USA-Plano-Texas"/>	<input type="button" value="Save"/>
Secondary Hub Locations ⓘ	<input type="text" value="USA-Washington-DC"/>	<input type="button" value="Save"/>
Reserved Subnet	<input type="text" value="10.200.0.0"/>	<input type="button" value="Save"/>
Hub and spoke configurations	<input type="text" value="Up to date"/>	<input type="button" value="Update"/>

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
<i>Primary Hub Locations</i>	Modify the primary location using the dropdown menus. Click Save .
<i>Secondary Hub Locations</i>	Modify the secondary location using the dropdown menus. Click Save .
<i>Reserved Subnet</i>	Assign a different subnet if you have a network conflict with the default reserved subnet. Click Save .
<i>Hub and spoke configurations</i>	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.

Sequence view		Interface pair view		+ Create		Edit		Delete		Discard Changes		Save		Apply	
+ Search															
	Policy	Source	Destination	Service	Action	Schedule	Security profiles	Status							
<input type="checkbox"/>	all-all-1	all-lans	all-lans	ALL	accept	always	AV: wifi-default WEB: wifi-default APP: wifi-default IPS: IPS-by-Elite-1	synced							
<input type="checkbox"/>	a	all-lans	all-lans	AFS3 AH	accept	always		deleted							

This section includes:

- [Creating a policy on page 51](#)
- [Viewing policies on page 53](#)
- [Applying policies on page 54](#)
- [Managing policies on page 54](#)
- [Policy example on page 55](#)

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 59](#).

- 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 59](#).

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 59](#).

- 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 59](#).

6. Select the *Service*.



You can create a new service in the *SDWan Overlay > Services* page. See [Creating a service on page 62](#).

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 63](#).

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 65](#) and [Creating a one-time schedule on page 65](#).

- 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 66](#).

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 69](#).

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 54](#).

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 *syncd*.

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 *syncd*.

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 45](#) and [Editing a site on page 49](#) for more information.

This section includes:

- [Creating an address on page 59](#)
- [Creating an address group on page 59](#)
- [Managing address objects and groups on page 60](#)

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 59](#).

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 59](#) 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 62](#)
- [Creating a service group on page 63](#)
- [Creating a service category on page 63](#)
- [Managing services on page 63](#)

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 63](#).

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 65](#)
- [Creating a one-time schedule on page 65](#)
- [Creating a schedule group on page 66](#)
- [Managing schedules on page 66](#)

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 65](#) and [Creating a one-time schedule on page 65](#).

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 51](#).



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 68](#)
- [Managing IP pools on page 68](#)

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 Guide for more information.



Sites must be running FortiOS 7.6.0 or later to support security profiles. See [Prerequisites on page 44](#).

The security profiles available include:

- [AntiVirus on page 69](#)
- [Web Filter on page 70](#)
- [Application Control on page 71](#)
- [Intrusion Prevention on page 72](#)
- [Application signatures on page 73](#)
- [IPS signatures on page 73](#)

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 73](#).

- 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 73](#).

- 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 71](#).

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 73](#).

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.

To back up a configuration:

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

To schedule an automatic backup:

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

To compare revisions:

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

To restore the device to a previous configuration:

1. Go to *Configuration > Revisions*.
2. Click the desired FortiGate.

3. Click *Manage revisions*.
4. Select a backup.
5. Click *Actions > Restore*.
6. Click *OK*. Your device reverts to the configuration revision of the selected backup.

CLI scripts



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*.

Administration

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

Automation

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

To configure an event handler stitch:

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

To enable or disable a notification email for a configured event handler stitch:

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

To configure the Sandbox event handler stitch:

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

Firmware management



In 25.2.a, firmware profiles are only available for devices with a paid subscription.

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

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

Firmware upgrade Firmware profiles						
<div> Fabric upgrade Upgrade EOS firmware Schedule Search </div>						
	FortiGate	Subscription	Firmware	Recommended firmware	Schedule summary	Upgrade status
<input type="checkbox"/>	FGT30E	Subscribed	v6.2.15 build1378	v6.2.16 build1392		
<input type="checkbox"/>	FortiGate FGT40F	Subscribed	v7.6.1 build3457		Upgrade to v7.6.0	Failed to upgrade
<input type="checkbox"/>	FortiGate FGT50E	Subscribed	v6.2.14 build1364	v6.2.16 build1392	Upgrade to v6.2.16 at 2025/01/09 23:00:00	Upgrade configure
<input type="checkbox"/>	FortiGate FGT60F	Subscribed	v7.6.1 build3457			
<input type="checkbox"/>	FortiGate FGT61F	Subscribed	v7.6.1 build3457			
<input type="checkbox"/>	FWF60E	Subscribed	v6.4.15 build2095			
<input type="checkbox"/>	FortiGate FGVM6V	Subscribed	v5.4.0 build0721 (E...)			
<input type="checkbox"/>	FGT30E	Not subscribed	v6.2.15 build1378	v6.2.16 build1392	Upgrade to v6.2.16	Upgrade canceled
<input type="checkbox"/>	FGT50E	Not subscribed	v6.2.15 build1378	v6.2.16 build1392	Upgrade to v6.2.16 at 2025/01/10 00:00:00	Upgrade configure
<input type="checkbox"/>	FGT60C	Not subscribed	v6.0.17 build0528	v6.0.18 build0549		
<input type="checkbox"/>	1900 FG4H1E	Not subscribed	v6.4.0 build1579 (E...)	v6.4.15 build2095		
<input type="checkbox"/>	FG40FIT	Not subscribed	Unknown version			

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

To schedule a firmware upgrade:

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

To upgrade EOS firmware:

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

To create a firmware profile:

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

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

CREATE FIRMWARE PROFILE

Name: test-profile

FortiGate model: All supported models **Specify**

FortiGate-30D ×
FortiGate-30E ×
+

Firmware version: **Latest patch** Specify

Upgrade date ⓘ: Delay **Specify days**

Upgrade day preferences:

<input checked="" type="checkbox"/> Sunday	<input checked="" type="checkbox"/> Monday
<input checked="" type="checkbox"/> Tuesday	<input checked="" type="checkbox"/> Wednesday
<input checked="" type="checkbox"/> Thursday	<input checked="" type="checkbox"/> Friday
<input checked="" type="checkbox"/> Saturday	

Preferred upgrade time ⓘ: **11 PM - 2 AM** 12 AM - 3 AM 1 AM - 4 AM

4. Click *OK* to create firmware profile.

To assign a firmware profile:

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

ASSIGN FIRMWARE PROFILE

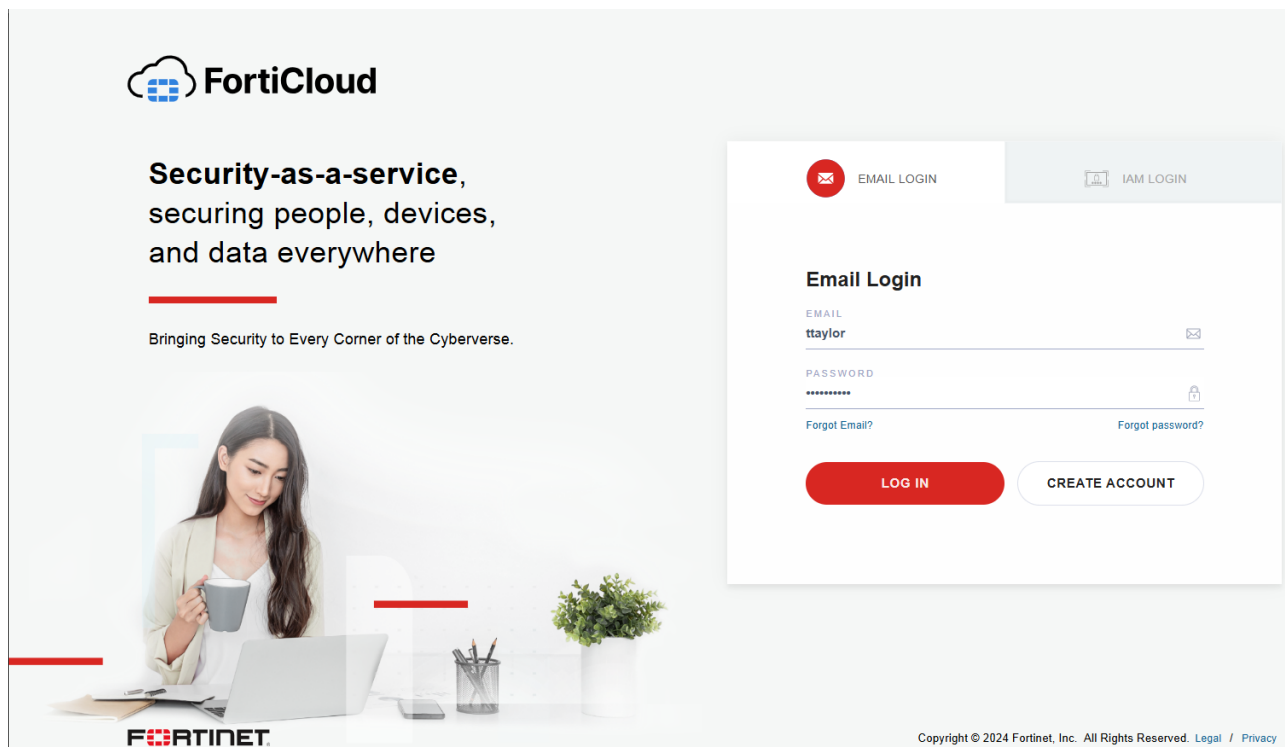
FortiGate: FWF60E

Firmware profile: latest-patch ▼

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

Accounts and users

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



Creating an account

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

User management

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

User type	Method
Identity and Access Management (IAM) user	Add users to the FortiCloud account with role-based access control in FortiGate Cloud using the FortiCloud IAM service . See IAM users on page 81 .

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

IAM users

FortiCloud Identity & Access Management (IAM) supports creating IAM users and allowing access to FortiGate Cloud using resource-based access control using FortiCloud permission profiles. When creating a permission profile in the IAM portal, you must add the FortiGate Cloud portal to the profile and configure the desired permissions.

FortiGate Cloud

Resources	Read Only	Read & Write	No Access
Configuration Management ⓘ		✓	
Logging and Reporting ⓘ		✓	
Cloud Sandbox ⓘ		✓	
IOC ⓘ		✓	
SD-WAN Overlay ⓘ		✓	
Account Settings ⓘ		✓	

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](#).

User settings

You can add and manage users from *Administration > User settings*. *User settings* includes different user types, including Identity & Access Management (IAM) and FortiGate Cloud account users. *User settings* displays a key icon beside the primary account. *User settings* displays a *Legacy Portal* toggle that you can use to revert to the legacy portal.

Account Profile

FortiCloud ID: 1948818

Account ID: [redacted]@gmail.com

Cloud Access Anonymous Mode: ☐

Account User

[+ Add](#) [Edit](#) [Delete](#) [Q Search](#) [Q](#) [Export](#)

Login ID	Role	User Type	Aliases	Status
[redacted]	Admin	FortiGateCloud	user_name_1746385314	Inactive
[redacted]	Admin	FortiGateCloud	[redacted]	Active
[redacted]	Admin	FortiGateCloud	user_name_1746435717	Active
[redacted]	Admin	FortiGateCloud	user_name_1746126135	Active
[redacted]	Admin	FortiGateCloud	[redacted]	Inactive
[redacted]	Admin	FortiGateCloud	[redacted]	Active
[redacted]	Admin	FortiGateCloud	user_name_1746212516	Active
[redacted]	Admin	FortiGateCloud	[redacted]@met.com	Inactive
[redacted]	Admin	FortiGateCloud	[redacted]@mailinator.com	Inactive
[redacted]	Admin	FortiGateCloud	user_name_1747594918	Active
[redacted]	Admin	FortiGateCloud	[redacted]@gmail.com	Inactive
[redacted]	Read-Only	FortiGateCloud	user_name_1745658119	Active
[redacted]	Admin	FortiGateCloud	user_name_1745953318	Inactive
[redacted]	Read-Only	FortiGateCloud	[redacted]@gmail.com	Inactive
[redacted]	Read-Only	FortiGateCloud	[redacted]@gmail.com	Inactive
[redacted]	Read-Only	FortiGateCloud	[redacted]@gmail.com	Inactive
[redacted]	Read-Only	FortiGateCloud	[redacted]@mailinator.com	Inactive
[redacted]	Read-Only	FortiGateCloud	[redacted]@com	Inactive

20

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: <ul style="list-style-type: none"> IAM: see IAM users on page 81. 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 92. 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 <i>Edit</i> icon in the <i>Action</i> column.
Status	Status of the user account. The status can be one of the following: <ul style="list-style-type: none"> Active: user who has activated their account. Inactive: user to whom an activation email has been sent, but has not activated their account yet.

For IAM and IdP users, they can only view their own account and edit their language settings on this page. You can enable or disable cloud access anonymous mode for a user.

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 *Administration > User settings*.
2. Enable or disable *Cloud Access Anonymous Mode*.

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
Backup	<ul style="list-style-type: none">Backing up a device configurationDownloading and disabling backups
Cloud access	Viewing and configuring a device via cloud access
Device deployment	<ul style="list-style-type: none">Provisioning and deprovisioning devicesDeleting 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:

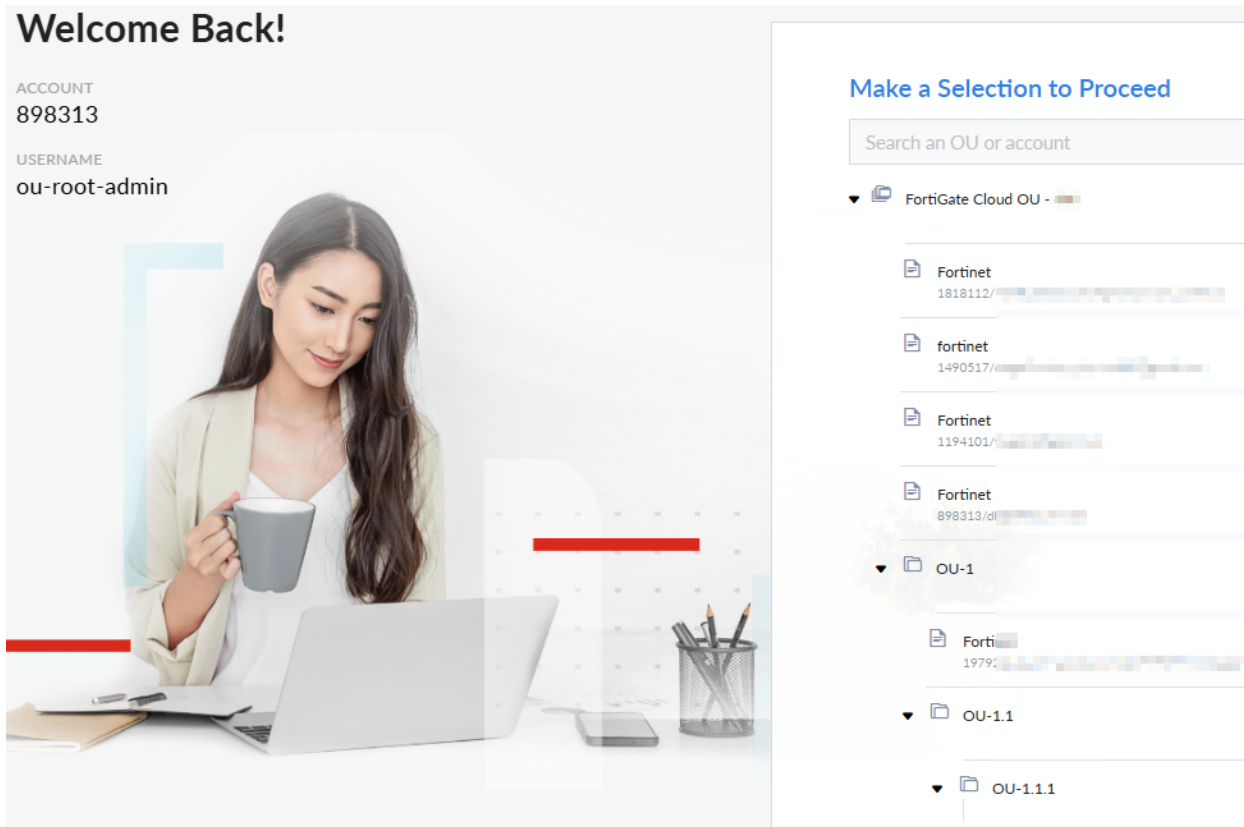
- Email users
- Local or organizational unit Identity & Access Management users
- Users with external identity provider roles

Multitenancy

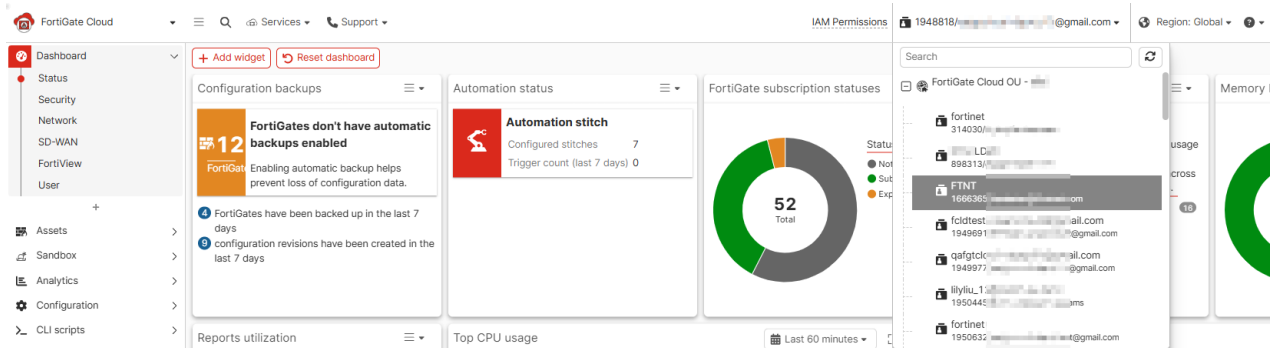
FortiGate Cloud supports FortiCloud Organizations for seamless multitenant features designed for managed security service providers across multiple FortiCloud accounts. With Organizations, Identity & Access Management (IAM) users can view an organizational unit (OU) Dashboard for a single pane of glass 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 81 .
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.



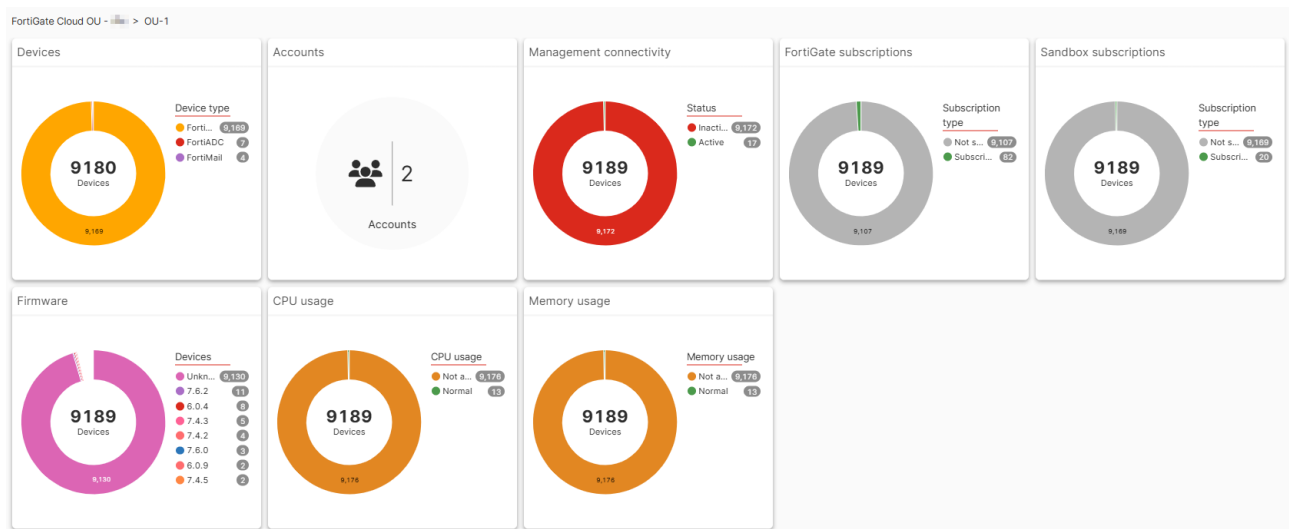
To move to another OU or account, select the desired OU from the dropdown list in the upper right corner.



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...
Devices	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 *Assets*, *Analytics*, *Administration*, *Configuration*, *CLI scripts*, and *Audit* pages. The OU *Assets* page offers some functionalities that the account-level *Assets* page does not. See [OU Asset list on page 89](#).

For the remaining pages, they offer the same functionality as their account-level equivalent pages do. The OU-level pages allow you to view and configure settings for each account in the OU by using the account navigation pane. For descriptions of the functionalities, see the topics for the account-level page in this guide, such as [Analytics on page 35](#).

Search	+ Create new	Edit	Delete	Run	Search
OU-1	Name	Description	Last modified	Owner	
Fortinet 900327	UpdateContract_sub02admin	@mailinator.com_kayla	2024/12/04 17:04:42	@gmail.com	
Fortinet 194861C	change timeout 200		2024/12/04 10:38:24	@gmail.com	
OU-1.1	2222	1: 55	2025/02/24 10:08:37	@gmail.com	
OU-1.1.1	test		2025/02/21 12:20:59	@gmail.com	
OU-1.2	01 @_adminiam		2025/02/12 16:06:04	@gmail.com	
	audit test		2025/02/19 14:20:07	@gmail.com	

OU Asset list

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

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.

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.

Column	Description
Name	(Optional, non-default) Device name.
Serial	(Optional, non-default) Serial number.
Subscription	(Optional, non-default) Subscription status of the device.

You can import and provision FortiGates using OUs.

To import and provision a FortiGate:

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

INVENTORY - 898313/ @FORTINET.COM				
<input type="button" value="+ Import FortiGate"/> <input type="button" value="Provision"/> <input type="button" value="Delete"/> <input type="button" value="Search"/>				
<input type="checkbox"/>	FortiGate	Description	FortiCare registration	Imported date
<input checked="" type="checkbox"/> FortiGates without a FortiGate Cloud subscription 25				
<input type="checkbox"/>	FGT-1000000000000000		Not registered	2024/09/09 11:55:00
<input type="checkbox"/>	FGT-1000000000000000		Not registered	2024/09/09 11:54:00
<input type="checkbox"/>	FGT-1000000000000000		Not registered	2024/09/09 11:54:00
<input type="checkbox"/>	FGT-1000000000000000		Not registered	2024/09/09 11:55:00
<input type="checkbox"/>	FGD-1000000000000000		Not registered	NaN/NaN/NaN NaN:NaN:NaN
<input type="checkbox"/>	FG-1000000000000000		Not registered	2023/12/05 20:27:00
<input type="checkbox"/>	FGT-1000000000000000		Not registered	2024/09/09 11:54:00
<input type="checkbox"/>	FGT-1000000000000000		Not registered	2024/09/09 11:54:00
<input type="checkbox"/>	FGT-1000000000000000		Not registered	2024/09/09 11:54:00
<input type="checkbox"/>	FGD-1000000000000000		Not registered	2024/05/23 16:29:00
<input type="checkbox"/>	FG-1000000000000000		Not registered	2024/08/07 17:38:00
<input type="checkbox"/>	FG-1000000000000000		Not registered	2023/12/05 20:27:00
<input type="checkbox"/>	FGT-1000000000000000		Not registered	2024/07/05 18:57:00
<input type="checkbox"/>	FG-1000000000000000		Not registered	2023/11/18 02:32:00
<input type="checkbox"/>	FG-1000000000000000		Not registered	2023/12/05 20:27:00
<input type="checkbox"/>	FG-1000000000000000		Not registered	2024/02/24 01:44:00
<input type="checkbox"/>	FGT-1000000000000000		Not registered	2024/09/09 11:53:00
<input type="checkbox"/>	FGT-1000000000000000		Not registered	2024/11/06 14:56:00
<input type="checkbox"/>	FGD-1000000000000000		Not registered	2024/05/22 14:41:00

You can transfer FortiGates between accounts in an OU.

To transfer a FortiGate:

1. Go to *Assets > Asset list* in the OU view.
2. Select the account with the source FortiGate(s) you would like the transfer by using the OU tree.

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

TRANSFER FORTIGATES

From

@gmail.com

To

@fortinet.com

End user type

☒ **A non-government user**

☐ **A government user**
In this context, a government end-user is any central, regional or local government department, agency, or other entity performing governmental functions, including:

1. Governmental research institutions.
2. Governmental corporations or their separate business units which are engaged in the manufacture or distribution of items or services controlled on the Wassenaar Munitions List.
3. International governmental organizations.

Data transfer options

☒ **Remove all data**
Permanently delete all log data associated with the FortiGate after transfer.

☐ **Migrate data to new account**
Update log data ownership from the source account to the new account.

☐ **Keep data in original account**
Retain ownership of the log data associated with the FortiGate in the original account.

Search

FortiGate

CSFRoot-Kayla-FGVM01TM

FGVM01TM

OK

Cancel

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

FortiGate Cloud 25.2.a Administration Guide
Fortinet Inc.

91

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
Europe	euapi.fortigate.forticloud.com
Japan	jpapi.fortigate.forticloud.com

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

To make an API call using a server authentication token:

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

Request:

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

Response:

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

Substitute in your FortiGate Cloud account credentials and host address.

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

Request:

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

Response:

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

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

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

Request:

```
curl -H "Content-Type: application/json" -X POST
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": "syIsrAofcHe67bTFdmhT5pInnqCXT", "scope": "read write", "status":
  "success", "token_type": "Bearer" }
```

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

Request:

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

Response:

```
[{"sn":"FG100D3G15803161","name":"FortiGate-100D","timeZone":-
  7.0,"tunnelAlive":true,"contractEndTime":0,"model":"FortiGate
  100D","firmwareVersion":"6.2.8","management":false,"initialized":false,"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://www.forticloud.com/forticloudapi/v1/fgt/<SN>/<FortiOS API>
```

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

Request:

```
curl -H "Content-Type: application/json" -H "Authorization: Bearer EXAMPLETOKEN"
https://www.forticloud.com/forticloudapi/v1/fgt/FGT60D461xxxxxxx/api/v2/monitor/fortiguard/se
vice-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 ping `logctrl1.fortinet.com` or `globallogctrl.fortinet.net`.
3. Connect via Telnet to the resolved IP address from step 2 using port 443.
4. Ensure that the FortiGate Cloud account password length is fewer than 20 characters.
5. If running FortiOS 5.4 or older versions, ensure that the FortiGate Cloud account password does not include special characters, as these FortiOS versions do not support this.
6. If the FortiGate is a member of a high availability (HA) pair, ensure that you activate FortiGate Cloud on the primary device. Activate FortiGate Cloud on the primary FortiGate as [To provision a FortiGate or FortiWifi to FortiGate Cloud in the FortiOS GUI: on page 26](#) 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.
7. 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.
8. If you see the HTTP 400 error, enable HTTP debug with the `diagnose debug application httpsd -1` command.

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

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

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

Activate FortiGate Cloud on the primary FortiGate as [To provision a FortiGate or FortiWifi to FortiGate Cloud in the FortiOS GUI: on page 26](#) 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.

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

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

Do one of the following:

- If you have not activated FortiGate Cloud 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 26](#) 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 26](#) describes instead. If you cannot connect to the FortiOS GUI, contact cs@fortinet.com to reenale the key.

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

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

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

1. Log in to FortiGate Cloud region A.
2. Deprovision the device.
3. Verify that the device has returned to the *Asset list*.
4. Switch the portal to region B.
5. Go to *Assets > Asset list*.
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 95. See [Accessing a FortiGate](#) on page 27.

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

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

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

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

What do I do if FortiDeploy does not work?

1. Ensure that the FortiManager settings are correct and the device can connect to FortiManager.
2. Confirm that the central management setting on the device is set to FortiCloud.
3. Ensure that the device can connect to logctrl1.fortinet.com via port 443.
4. Import the device to the inventory by FortiCloud key. See [To provision a FortiGate/FortiWifi to FortiGate Cloud using the FortiCloud key: on page 25](#).
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 26](#) describes.

What do I do if FortiOS does not upload logs?

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

```
execute telnet <log server IP address> 514
diagnose test application forticldd 1
diagnose test application miglogd 6
diagnose debug application miglogd -1
diagnose debug enable
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 subscription. See [To download a log: on page 41](#).

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 35](#).

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 74](#).

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.

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

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

- 7.6.0 and later versions
- 7.4.2 and later versions
- 7.2.8 and later versions
- 7.0.14 and later versions

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

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 the 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 subscription to bypass the automatic firmware upgrade enforcement from FortiGate Cloud?

FortiGate Cloud does not automatically upgrade devices without a FortiGate Cloud 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 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
```


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 the labeling as a 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.



www.fortinet.com

Copyright© 2025 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.