FortiGate Cloud - Administration Guide

Version 4.3

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

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

FORTINET BLOG
https://blog.fortinet.com

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

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

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

FEEDBACK
Email: techdoc@fortinet.com

November 20, 2019
FortiGate Cloud 4.3 Administration Guide
32-430-535370-20191120

TABLE OF CONTENTS

Change log

Date	Change Description
2019-11-08	Initial release.
2019-11-20	Updated To assign a device to a subaccount on the homepage: on page 37.

Introduction

FortiGate Cloud is a SaaS UTM infrastructure management and log retention service available for FortiGate and FortiWiFi devices. With FortiGate Cloud, you can do the following:

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

FortiGate Cloud also integrates other Fortinet services: FortiSandbox Cloud and FortiDeploy. See Sandbox on page 33 and FortiDeploy on page 45.

Functions

FortiGate Cloud has the following functions:

Function	Description
Centralized dashboard	System and log widgets plus real-time monitors.
FortiView log viewer	Real-time log viewing with filters and download capability.
Drilldown analysis	Real-time location, user, and network activity analysis, and alert profiles.
Report generator	Create custom report templates and schedule reports in different formats to display location-based analytics or illustrate network usage platforms.
Device management	Scheduled configuration backup and history and script management. If using multitenancy license, includes group management.
Antivirus (AV) submission	Shows the status of suspicious files undergoing cloud-based sandbox analysis.

AP and FortiSwitch management via FortiGate	• Wireless configuration:
	  ◦ View, add, and remove APs managed by FortiGates
	  ◦ Create and edit SSID settings
	  ◦ Create and edit FortiAP profiles
	  ◦ Create and edit WIDS profiles
	• Guest management: Add guests and notify them of credentials via SMS or email.

Zero-touch deployment	Automatic connection of FortiGate devices for FortiGate Cloud management using FortiDeploy.
Multitenancy templates	Create templates and push to multiple devices.

Function	Description
Remote access	Import local configuration to web browser and push changes to device through network.
FortiGate virtual domain (VDOM) support	Support for VDOMs configured in FortiGate devices.
Active Directory (AD) management	Integration with AD.
Firmware upgrade	Remotely upgrade FortiOS on FortiGate devices.
Event management	Set up email alerts for specific network structure emergencies, such as FortiGate Cloud losing connection to the device, or the device's power supply failing.
Regional datacenters	Datacenters located in Canada and Germany for better performance and GDPR compliance for international customers.

How FortiGate Cloud works

You can register one or multiple devices with FortiGate Cloud under a single account on the FortiGate Cloud portal.

Each device periodically sends logs to FortiGate Cloud for storage. You can configure log settings. For example, you can configure devices to send only traffic and event logs, or include security logs such as AV, application control, and IPS.

From the recorded logs, you can generate reports to identify trends in network traffic, individual user activity, and security threats across different applications. Drilldown capability and real-time alerting are also available.

FortiGate Cloud also creates copies of configurations that you can use for backup, restoration, or provisioning new devices. You can use a VPN tunnel to bring up the console of a device behind a firewall to perform configuration or policy changes remotely.

FortiGate Cloud is integrated with FortinetOne single sign on. After you create a FortinetOne SSO account, you can enable the FortiGate Cloud global or European service. You can also enable both services. You can deploy FortiGate devices to the global or Europe cloud service from the unified device inventory in the FortiGate Cloud portal. See Inventory on page 15. You can migrate historical data such as logs, reports, and backups between accounts under the same service (global or Europe), but you cannot migrate such data from one service to another. To migrate a FortiGate device from one service to the other, you must undeploy the device, then deploy the device again from *Inventory* on the desired service portal.

When you initially create your account in FortiGate Cloud, you choose the data center to use. You cannot transfer data and accounts between data centers, so migration requires a new account.

To confirm which version of FortiGate Cloud is currently in use, on the Fortinet website, use your FortinetOne account to access FortiGate Cloud. The version details are at the bottom of the FortiGate Cloud homepage.

FortiGate Cloud currently supports two languages: English and Japanese. You can select a language from the web portal login page. Other languages may be available in other regions.

You can provide feedback or request improvements to FortiGate Cloud using the envelope icon on the top-right of every screen. Fortinet cannot guarantee individual responses to requests.

Requirements

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

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

For Management, FortiGate Cloud supports FortiOS 5.0.0 through 6.2.1. For devices that are running unsupported FortiOS versions, you can use the Remote Access feature.

For Analysis, FortiGate Cloud supports all FortiOS versions.

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

The FortiGate does not require a hard drive if it uploads logs to FortiGate Cloud in real-time, which you can enable under *Log Settings* in FortiOS.

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

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

What's new

For information about FortiGate Cloud new features, see the *FortiGate Cloud Release Notes*.

Licensing and registration

Demo

You can access a demo of FortiGate Cloud by visiting the FortiGate Cloud portal and selecting the *Live Demo* button. The demo shows a FortiGate Cloud account with populated devices and logs to simulate a live environment.

License types

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

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

You can enjoy the free subscription of FortiGate Cloud on any FortiGate or FortiWifi device, or purchase an annual-subscription-based license with a one-, two-, or three-year service term. A FortiGate Cloud license entitles devices to advanced features including the IOC service and FortiPresence analytics, as well as one-year log retention compared to the seven-day log retention with the free subscription. With the Sandbox feature, a device can upload up to 100 suspicious files/URLs per day to FortiSandbox Cloud through FortiGate Cloud without a FortiSandbox Cloud license. You can increase the daily limit by adding a FortiSandbox Cloud service license.

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

Description	SKU
FortiGate Cloud analysis and one-year log retention	
FortiGate and FortiWifi	FC-10-00XXX-131-02-DD
FortiGate Cloud IOC (Indicator of Compromise)	
FortiGate 20 to 90 models	FC-10-90803-142-02-12
FortiGate 100 to 300 models	FC-10-90804-142-02-12
Other services	
FortiGate Cloud multitenancy	FCLE-10-FCLD0-161-02-12
FortiDeploy access	FDP-SINGLE-USE

Activation on device requires FortiOS 5.4.2 or later. The IOC service requires an existing FortiGate Cloud subscription.

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

For pricing information, contact your Fortinet partner or reseller.

Deploying a FortiGate/FortiWifi to FortiGate Cloud

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

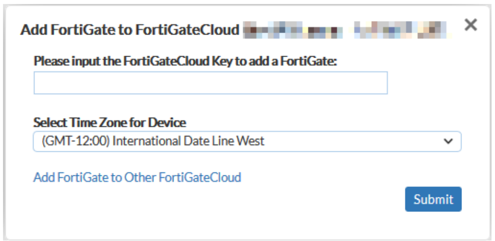
- FortiGate key
- Bulk key
- Zero-touch deployment
- FortiOS GUI

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

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

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

1. Log in to the FortiGate Cloud portal, then click *Add FortiGate*.
2. In the *Add FortiGate* dialog, enter the key printed on your FortiGate.
3. From the *Select Time Zone for Device* dropdown list, select the desired time zone.
4. Click *Submit*.



Add FortiGate to FortiGateCloud [redacted]

Please input the FortiGateCloud Key to add a FortiGate:

Select Time Zone for Device

(GMT-12:00) International Date Line West

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

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

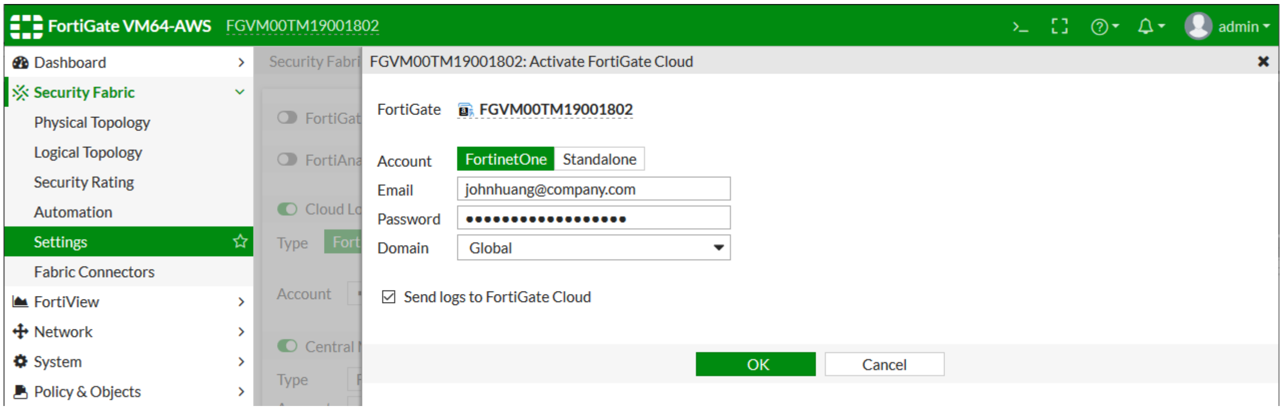
1. Log in to the FortiGate Cloud portal, then click *Inventory*.
2. Click *Import Bulk Key*.
3. In the *Please input the Bulk Key:* field, enter the bulk key.
4. Click *Submit*. The portal displays a list of the FortiGate/FortiWifi serial numbers associated with the bulk key.

To deploy multiple FortiGate/FortiWifi devices to FortiGate Cloud using zero-touch deployment:

See FortiDeploy on page 45.

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

1. In the FortinetOne portal, ensure that you have a product entitlement for FortiGate Cloud for the desired FortiGate or FortiWifi.
2. In FortiOS, do one of the following:
   a. Go to *Security Fabric* > *Settings*, and enable *Central Management*. Click *FortiGate Cloud*.
   b. 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, for *Account*, select *FortinetOne*.
5. In the *Email* and *Password* fields, enter the email address and password associated with the FortinetOne account.
6. Enable *Send logs to FortiGate Cloud*. Click *OK*.



FGVM00TM19001802: Activate FortiGate Cloud

FortiGate FGVM00TM19001802

Account [✓ FortinetOne] Standalone

Email johnhuang@company.com

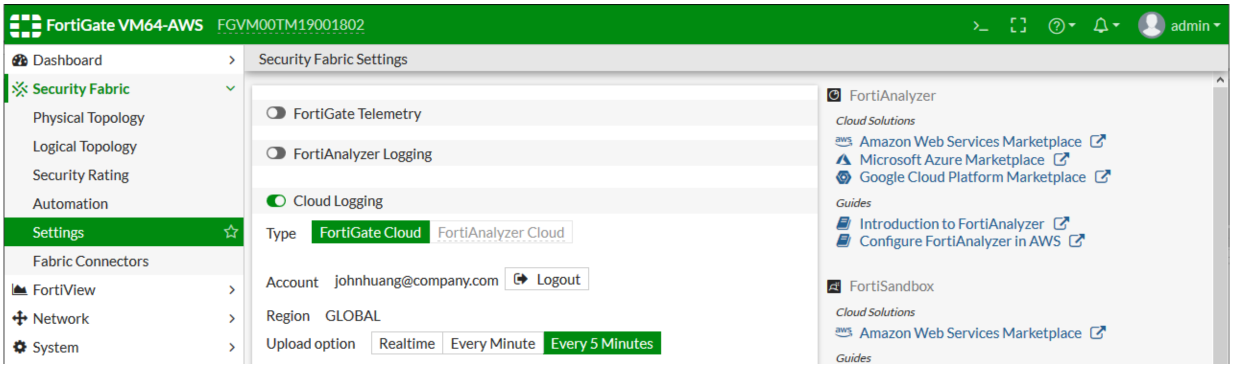
Password ••••••••••••••••••

Domain Global

☑ Send logs to FortiGate Cloud

OK Cancel

7. This should have automatically enabled *Cloud Logging*. Ensure that *Cloud Logging* was enabled. If it was not enabled, enable it, then set *Type* to *FortiGate Cloud*.


FortiGate VM64-AWS FGVM00TM19001802
admin
Dashboard
Security Fabric
Physical Topology
Logical Topology
Security Rating
Automation
Settings
Fabric Connectors
FortiView
Network
System
FortiAnalyzer
Cloud Solutions
Amazon Web Services Marketplace
Microsoft Azure Marketplace
Google Cloud Platform Marketplace
Guides
Introduction to FortiAnalyzer
Configure FortiAnalyzer in AWS
FortiSandbox
Cloud Solutions
Amazon Web Services Marketplace
Guides

Security Fabric Settings

FortiGate Telemetry

FortiAnalyzer Logging

Cloud Logging

Type [✓ FortiGate Cloud] FortiAnalyzer Cloud

Account johnhuang@company.com Logout

Region GLOBAL

Upload option Realtime Every Minute [✓ Every 5 Minutes]

8. At this point, in FortiGate Cloud, you can access Analysis and Sandbox features for this device. To access Management features, you must authorize the FortiGate in FortiGate Cloud by entering the a local superadministrator username and password when prompted. After authorization, you can manage that FortiGate from FortiGate Cloud.

To unsubscribe from FortiGate Cloud:

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

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

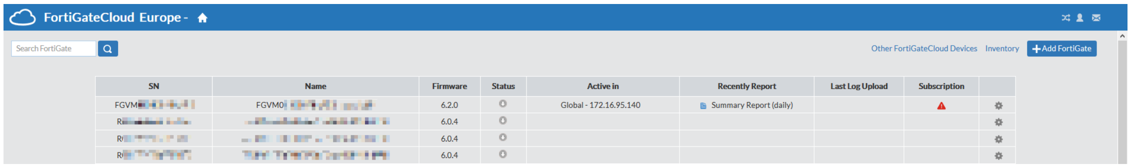
Homepage

You see the *Home* page when you first open the FortiGate Cloud interface. On this page is a list of Fortinet devices connected to the FortiGate Cloud service. You can add new devices by selecting *Add FortiGate* and entering a FortiGate Cloud key.

To view Fortinet devices that you have deployed using the same FortinetOne account under a different service, you can click *Other FortiGateCloud Devices*. This displays a dropdown list of devices deployed using the same FortinetOne account under a different service. For example, if you are currently logged in to the Europe service, this link displays a dropdown list of devices deployed under the global service. If there are more than 20 devices deployed to the other service, the dropdown list only displays 20. You can go to the other service homepage using the link at the bottom of the dropdown list.

The homepage also displays currently active devices that you previously deployed to the current service, but later deployed to another service. For example, if you deployed a FortiGate to the global service, then deployed it to the Europe service, it shows up in the homepage for both services.

In the example shown, the user has logged in to the Europe service. The first device in the table, FGVM, is deployed under the FortiGate Cloud global service, as shown in the *Active in* column. This FortiGate is shown because it was previously deployed to the Europe service. The other devices in the table are deployed under the Europe service, and have no values in the *Active in* column, since the user is logged in to the Europe service.



SN	Name	Firmware	Status	Active in	Recently Report	Last Log Upload	Subscription	
FGVM[redacted]	FGVM0[redacted]	6.2.0	○	Global - 172.16.95.140	Summary Report (daily)		⚠	⚙
R[redacted]	[redacted]	6.0.4	○					⚙
R[redacted]	[redacted]	6.0.4	○					⚙
R[redacted]	[redacted]	6.0.4	○					⚙

Each device displays:

- Model/serial number
- Fortinet product type
- If the device is connected through a management tunnel
- Last compiled report and last log uploaded
- What percentage of the FortiGate Cloud quota has been filled (and a *Manage Quota* button, that allows you to delete old logs and make space on the server)
- Subscription expiry date

Next to some device icons is a gear icon, allowing you to delete, rename, or configure devices.

Click a device name or icon to go to the FortiGate Cloud dashboard for that device.

If you enable multitenancy, FortiGate Cloud displays a different homepage when you log in. See Multitenancy on page 37.

To add more administrators/users:

1. In the upper right of the FortiGate Cloud interface, select the *My Account* icon.
2. Select *Add User* in the window.
3. Enter the new admin/user's email address and name.
4. Select whether they are an admin (total control over the FortiGate Cloud interface) or a regular user (limited control, monitoring only).
5. Select *Submit*. The admin/user receives an email prompting them to set their account password and log in.

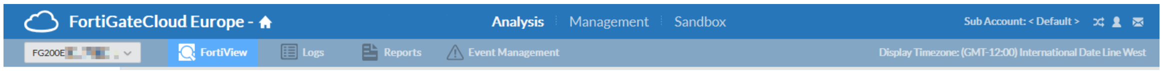
To undeploy the FortiGate:

1. Click the *Config* icon for the desired device.
2. Click *Undeploy*.
3. In the confirmation dialog, click *YES*.

You have the option to place an unit where the FortiGate was deployed. The unit contains historical data and a serial number that starts with U.

To set the display timezone for the FortiGate:

1. You must set the display timezone for the FortiGate before you can access the dashboard for that device. This timezone only affects log data view for the FortiGate and does not affect the FortiGate's configured timezone. You can also modify the FortiGate's display timezone after it has already been set. Go to the homepage and do one of the following:
   a. If you have previously configured the display timezone, click the *Config* icon beside the desired device, then click *Display Timezone*.
   b. If you have not previously configured a display timezone, click the desired device. FortiGate Cloud displays a Please set display time zone for device <FortiGate name> before proceeding message. Click *OK*.
2. From the *Display Timezone for Device* dropdown list, select the desired timezone. Click *Submit*. The FortiGate Cloud GUI shows the FortiGate's display timezone in the upper right corner.



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

Inventory

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

Inventory is divided into tabs: *FortiGate Inventory*, *FortiCare Inventory*, *FortiGate Cloud Deployed*, and *FortiManager Deployed*. You can filter each list by searching for the device serial number in the *SN* searchbar or selecting the desired bulk key from the *Bulk Key* dropdown list.

FortiGate Inventory

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

To deploy devices to FortiGate Cloud:

1. On the homepage, go to *Inventory*.
2. Select the desired devices.
3. Click *Deploy to FortiGate Cloud*.
4. In the *Deploy to FortiGate Cloud* dialog, do one of the following:
   a. If multitenancy is enabled, configure the following options:

Option	Description
Sub Account	Select the desired subaccount to add the devices to.
Task Name	Enter the desired task name.
Template	From the dropdown list, select the desired template. This dialog only displays templates applicable for the selected devices. If you select a template, this enables configuration management for the devices. For details on creating and configuring a template, see Templates on page 42.
Auto Upgrade Firmware to Match Template Version	Enable to automatically upgrade FortiOS on these devices to the template version, if the template FortiOS version is newer. Ensure that you review the FortiOS Upgrade Path to ensure that upgrade is supported before enabling this option.

   b. If multitenancy is not enabled, configure the timezone for the selected devices.
5. Click *Deploy*. These devices are deployed to FortiGate Cloud, and you can now access them on the *FortiGate Cloud Deployed* tab.

To deploy a device to FortiManager:

1. On the homepage, go to *Inventory*.
2. Click *FortiManager Setup* .
3. In the *FortiManager Setup* dialog, enter the desired FortiManager IP address/FQDN and serial number. Click *Submit*.
4. Select the desired devices.
5. Click *Deploy to FortiManager*.
6. Click *Deploy*. These devices are deployed to FortiManager, and you can now view their serial numbers on the *FortiManager Deployed* tab. Once deployed to FortiManager, FortiGate Cloud has no control over the device. You cannot manage the device in FortiGate Cloud until you set central management back to FortiGate Cloud.

To delete a device from inventory:

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

FortiCare Inventory

FortiCare Inventory displays the devices that are registered to FortiCare under the account's primary administrator email address. Only the primary administrator can view and deploy these devices from the FortiCare Inventory to FortiGate Cloud. To deploy FortiCare devices to FortiGate Cloud, follow the same instructions as described in To deploy devices to FortiGate Cloud: on page 15, from the *FortiCare Inventory* tab.

FortiGate Cloud Deployed and FortiManager Deployed

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

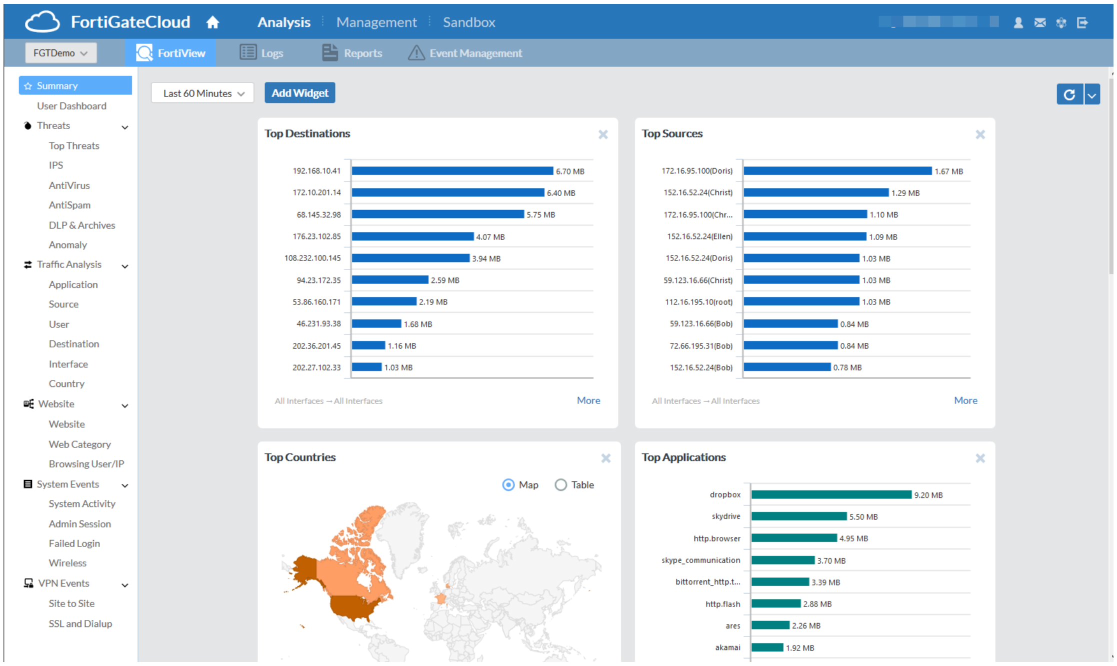
The *FortiGate Inventory* tab provides a centralized view of all devices imported into the Europe and global services. However, after you deploy a FortiGate to FortiGate Cloud, you can only view the FortiGates deployed to the service that you are currently logged in to on the *FortiGate Cloud Deployed*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

Analysis

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

When using a free subscription, you can only view FortiView data, logs, and reports for the past seven days.

FortiView



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

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

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

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

Threats

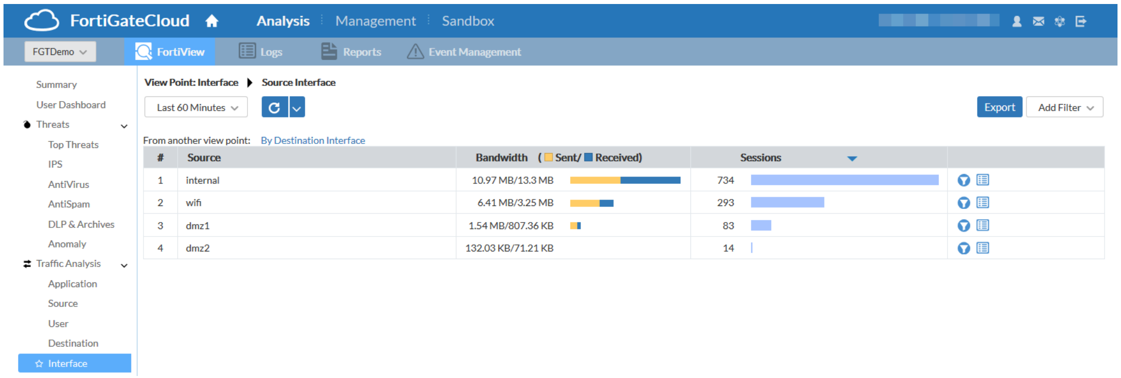
Widget	Description	Feature required to be enabled on device
Top Threats	Displays which threats trigger the most detection events on the network.	At least one of the following: IPS, AV, AntiSpam, DLP, or Anomaly Detection.
Top Spam	Displays which sources send the most spam email into the network.	AntiSpam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

Traffic Analysis

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

Websites

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



View Point: Interface ▸ Source Interface

From another view point: By Destination Interface

#	Source	Bandwidth (🟨 Sent/ 🟦 Received)	Sessions
1	internal	10.97 MB/13.3 MB	734
2	wifi	6.41 MB/3.25 MB	293
3	dmz1	1.54 MB/807.36 KB	83
4	dmz2	132.03 KB/71.21 KB	14

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

You can select a time period to view data for:

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

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

FortiView charts reference

The following provides descriptions of all FortiView charts.

User Dashboard

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

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

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

FSBP Dashboard

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

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

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

Threats

Chart	Description
Top Threats	Lists the top threats to your network. The following incidents are considered threats: • Risk applications detected by application control. • Intrusion incidents detected by IPS. • Malicious web sites detected by web filtering. • Malware/botnets detected by antivirus.
IPS	Lists intrusion incidents detected by IPS.
AntiVirus	Lists the malware/botnets detected by AV.
AntiSpam	Lists the spam detected by AntiSpam.
DLP & Archives	Lists the DLP and archives incidents.
Anomaly	Lists network anomalies.

Traffic Analysis

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

Website

Chart	Description
Website	Displays the top allowed and blocked website domains on the network. You can also view by source. You can filter by threat level.
Web Category	Displays the top website categories. You can filter by threat level.
Browsing User/IP	Displays the top web-browsing users and their IP addresses by total browsing time duration. You can also view by category or domain. You can filter by threat level.

System Events

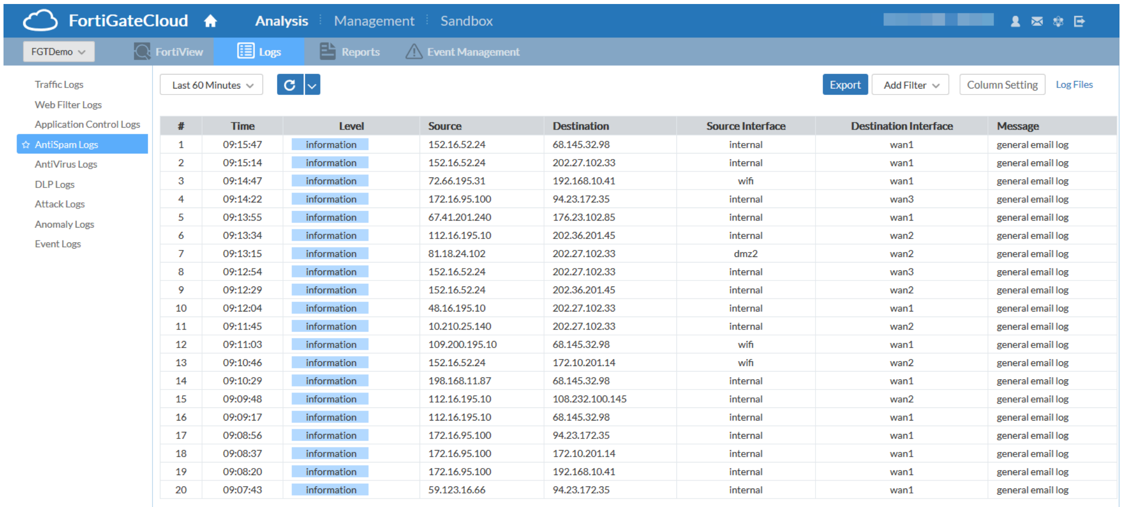
Chart	Description
System Activity	Displays events on the managed devices, their severity, and number of incidents. You can filter by user or severity level.

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

VPN Events

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

Logs



#	Time	Level	Source	Destination	Source Interface	Destination Interface	Message
1	09:15:47	information	152.16.52.24	68.145.32.98	internal	wan1	general email log
2	09:15:14	information	152.16.52.24	202.27.102.33	internal	wan1	general email log
3	09:14:47	information	72.66.195.31	192.168.10.41	wifi	wan1	general email log
4	09:14:22	information	172.16.95.100	94.23.172.35	internal	wan3	general email log
5	09:13:55	information	67.41.201.240	176.23.102.85	internal	wan1	general email log
6	09:13:34	information	112.16.195.10	202.36.201.45	internal	wan2	general email log
7	09:13:15	information	81.18.24.102	202.27.102.33	dmz2	wan2	general email log
8	09:12:54	information	152.16.52.24	202.27.102.33	internal	wan3	general email log
9	09:12:29	information	152.16.52.24	202.36.201.45	internal	wan2	general email log
10	09:12:04	information	48.16.195.10	202.27.102.33	internal	wan1	general email log
11	09:11:45	information	10.210.25.140	202.27.102.33	internal	wan2	general email log
12	09:11:03	information	109.200.195.10	68.145.32.98	wifi	wan1	general email log
13	09:10:46	information	152.16.52.24	172.10.201.14	wifi	wan2	general email log
14	09:10:29	information	198.168.11.87	68.145.32.98	internal	wan1	general email log
15	09:09:48	information	112.16.195.10	108.232.100.145	internal	wan2	general email log
16	09:09:17	information	112.16.195.10	68.145.32.98	internal	wan1	general email log
17	09:08:56	information	172.16.95.100	94.23.172.35	internal	wan1	general email log
18	09:08:37	information	172.16.95.100	172.10.201.14	internal	wan1	general email log
19	09:08:20	information	172.16.95.100	192.168.10.41	internal	wan1	general email log
20	09:07:43	information	59.123.16.66	94.23.172.35	internal	wan1	general email log

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

You can select a time period to view data for:

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

- Last 30 days
- Specified time period

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

You can download various types of raw logs from FortiGate Cloud. The log filename format is as follows:

<FortiGate serial number>_<log type>_<beginning of log date range>-<time of first log>-<end of log date range>-<time of last log>.log.gz

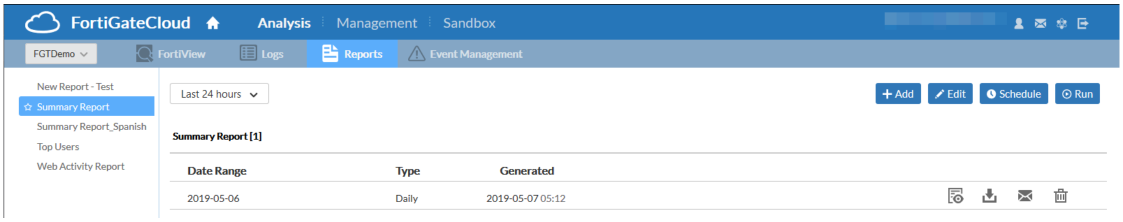
The log filename format uses a shortened identifier for each log type:

Log type	Identifier
Traffic	tlog
Web Filter	wlog
Application Control	rlog
AntiSpam	slog
AntiVirus	vlog
DLP	dlog
Attack	alog
Anomaly	mlog
DNS	olog
Event (including all subtypes)	elog

For example, consider an Application Control log that is generated for the period between October 23, 2019 and November 2, 2019 for a FortiGate with the serial number "FGT123". The first log in the file has a timestamp of 6:09 PM, while the last log in the file has a timestamp of 9:32 AM. The log file name is as follows:

FGT123_rlog_20191023-1809-20191101-0932.log.gz

Reports



Summary Report [1]

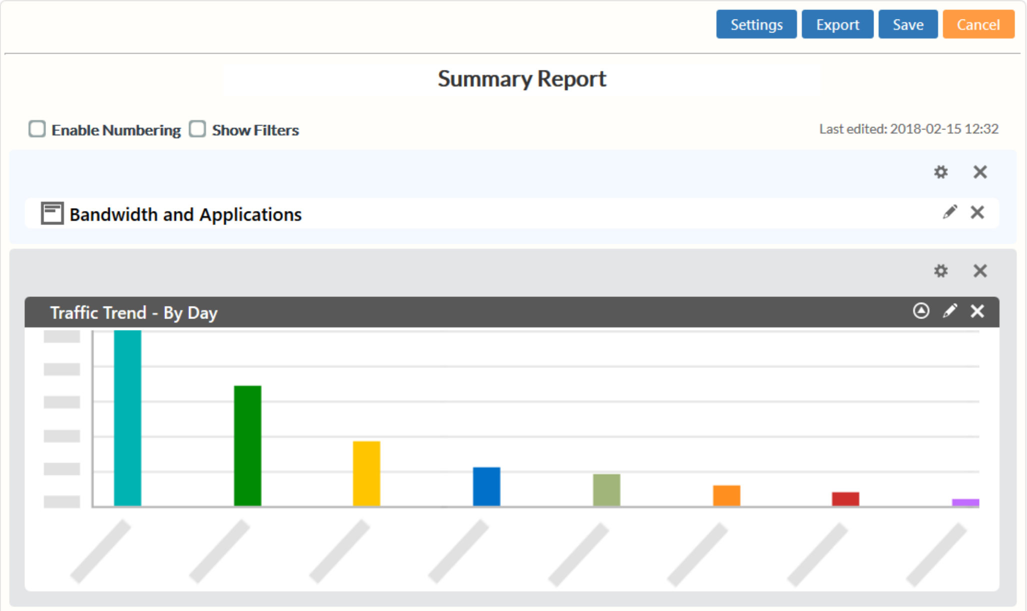
Date Range	Type	Generated
2019-05-06	Daily	2019-05-07 05:12

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

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

To create a custom report:

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



Summary Report

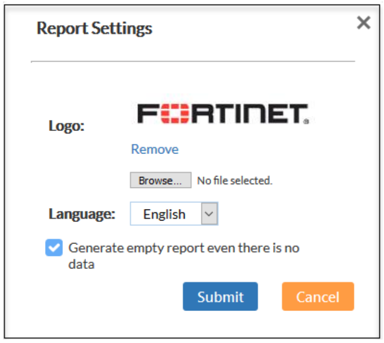
□ Enable Numbering □ Show Filters

Last edited: 2018-02-15 12:32

Bandwidth and Applications

Traffic Trend - By Day

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



Report Settings

Logo: FURTINET

No file selected.

Language: English

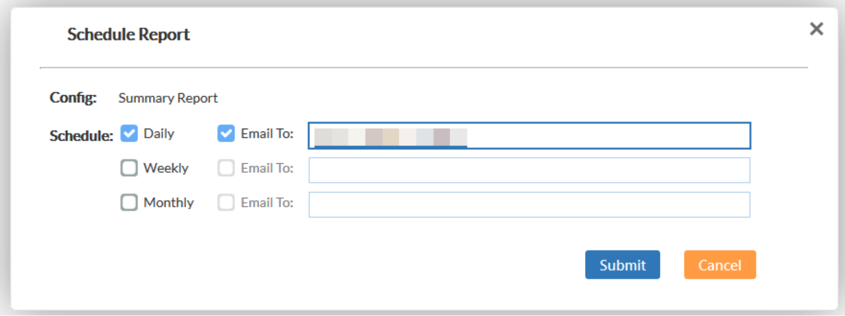
☑ Generate empty report even there is no data

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

To schedule a report:

1. Go to *Analysis* > *Reports*.
2. Click the desired report from the left pane.

3. Click *Schedule* to determine the range of time for which to generate reports: *Daily*, *Weekly* or *Monthly*, and which email to send the reports to. For example, if you want to generate a report for a month of data, you can select *Monthly* and FortiGate Cloud will run and send the report once a month. You can also run a report immediately.



Schedule Report

Config: Summary Report

Schedule: ☑ Daily ☑ Email To: [redacted]

□ Weekly □ Email To:

□ Monthly □ Email To:

To configure report settings:

If you have enabled multitenancy, you can access these options in *Group Management* > *Manage Report Configs*.

1. Go to *Analysis* > *Reports*.
2. Click the desired report from the left pane.
3. Click *Settings*. You can upload a report logo and set the report language. *Click Submit*.

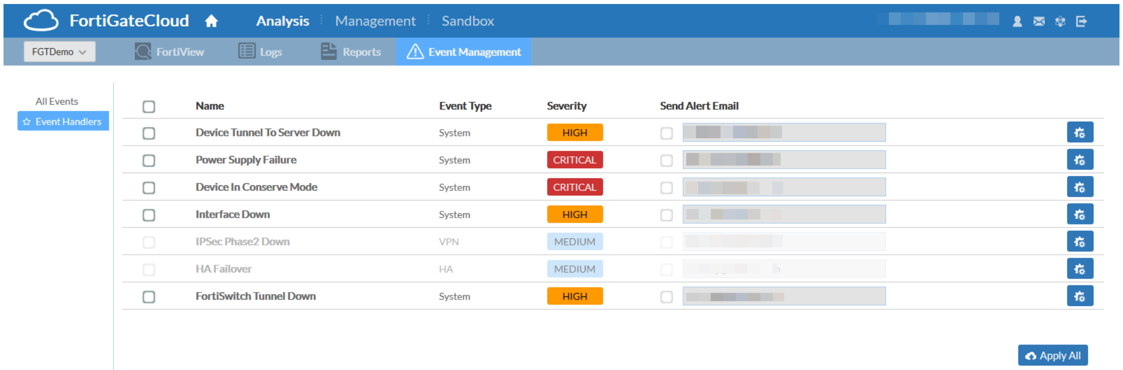
Reports reference

The following provides descriptions of preconfigured reports:

Report	Description
DNS	The default version of this report displays the following charts: • Queried Botnet C&C domains and IP addresses • High risk sources • Top queried domains • Top domain lookup block • Top domain lookup timeout
FSBP	The default version of this report displays results based on the device's security rating result: • Fabric components audited • Score history (industry average and industry range) • Maturity milestones • Achievements and to-do list The FSBP Dashboard is only available for devices that support the Security Rating feature. If the device does not have any Security Rating results, all charts show no data.
High Bandwidth Application Usage	Shows you applications that may affect network performance by using high bandwidth, allowing you to quickly pinpoint high bandwidth usage and violation of corporate policies.

Report	Description
	This report focuses on peer-to-peer applications (such as BitTorrent, Xunlei, Gnutella, Filetopia), file sharing and storage applications (such as Onebox, Google Drive, Dropbox, Apple Cloud), and voice/video applications (such as YouTube, Skype, Spotify, Vimeo, Netflix). You cannot edit this report.
Summary	The default version of this report displays the following sections: • Threat Analysis • Traffic Analysis • Web Activities • VPN Analysis • System Activity
Web Activity	The default version of this report displays the following charts: • Most Visited Web Categories • Most Visited Websites • Most Visited Web Categories and Web Sites • Most Active Web Users • Most Visited Web Sites by Most Active Users • Most Active Users of Most Visited Web Sites
360 Degree Activities	Displays the following sections: • Application Visibility • Web Traffic Analysis • User Behavior Analysis You cannot edit this report.
Cyber Threat Assessment	An enhanced version of the Summary Report. Displays the following sections: • User Productivity • Application Usage • Web Usage • Security and Threat Prevention • Application Vulnerability Exploits • Virus Prevention • At-Risk Devices and Hosts • High Risk Application • Network Utilization • Bandwidth You cannot edit this report.

Event Management

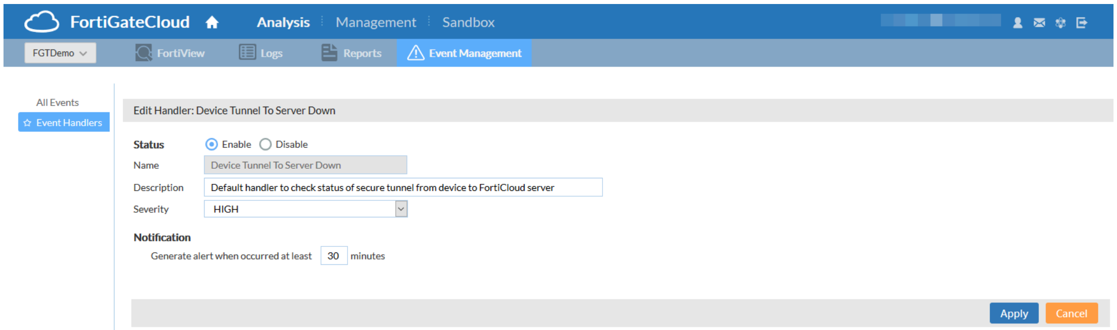


□	Name	Event Type	Severity	Send Alert Email	
□	Device Tunnel To Server Down	System	HIGH	□ [redacted]	⚙
□	Power Supply Failure	System	CRITICAL	□ [redacted]	⚙
□	Device In Conserve Mode	System	CRITICAL	□ [redacted]	⚙
□	Interface Down	System	HIGH	□ [redacted]	⚙
□	IPSec Phase2 Down	VPN	MEDIUM	□ [redacted]	⚙
□	HA Failover	HA	MEDIUM	□ [redacted]	⚙
□	FortiSwitch Tunnel Down	System	HIGH	□ [redacted]	⚙

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

You can enable events to track by selecting their checkboxes. If you want to receive an alert email when they occur, select the checkbox under *Send Alert Email* and enter the email address to send the alert email to.

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



Edit Handler: Device Tunnel To Server Down

Status ● Enable ○ Disable

Name: Device Tunnel To Server Down

Description: Default handler to check status of secure tunnel from device to FortiCloud server

Severity: HIGH

Notification

Generate alert when occurred at least 30 minutes

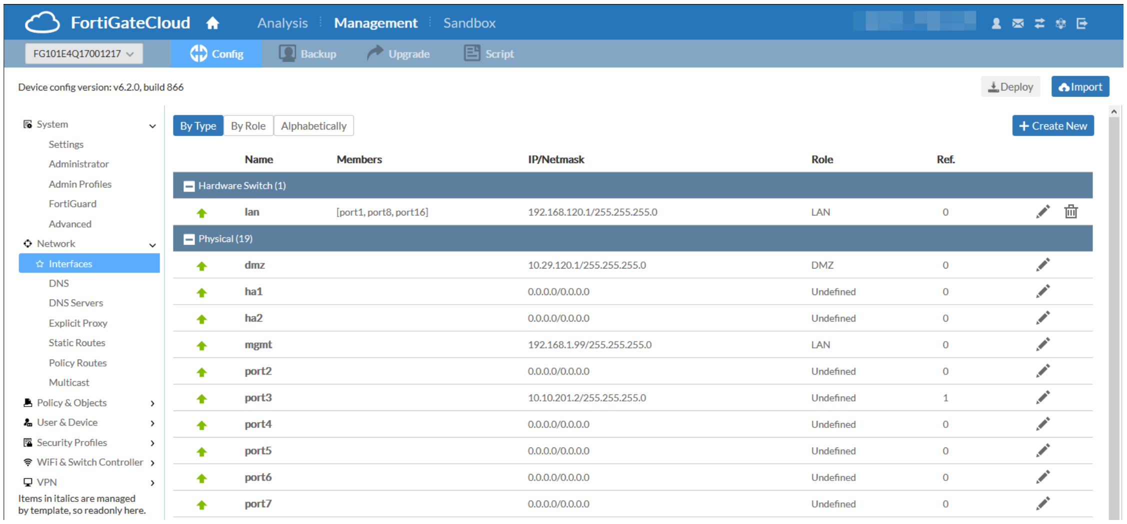
Management

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

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

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

Config



Device config version: v6.2.0, build 866

Name	Members	IP/Netmask	Role	Ref.
Hardware Switch (1)				
lan	[port1, port8, port16]	192.168.120.1/255.255.255.0	LAN	0
Physical (19)				
dmz		10.29.120.1/255.255.255.0	DMZ	0
ha1		0.0.0.0/0.0.0.0	Undefined	0
ha2		0.0.0.0/0.0.0.0	Undefined	0
mgmt		192.168.1.99/255.255.255.0	LAN	0
port2		0.0.0.0/0.0.0.0	Undefined	0
port3		10.10.201.2/255.255.255.0	Undefined	1
port4		0.0.0.0/0.0.0.0	Undefined	0
port5		0.0.0.0/0.0.0.0	Undefined	0
port6		0.0.0.0/0.0.0.0	Undefined	0
port7		0.0.0.0/0.0.0.0	Undefined	0

Items in italics are managed by template, so readonly here.

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

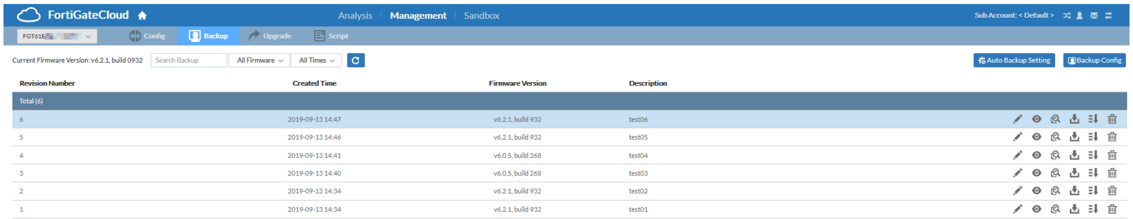
The configuration you see in FortiGate Cloud does not autorefresh. FortiGate Cloud displays a notification if the current local FortiGate configuration differs from the latest configuration uploaded to FortiGate Cloud. You can overwrite the FortiGate Cloud configuration with the current local FortiGate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

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

To deploy cloud configuration to devices:

1. Go to *Management* > *Config*.
2. Before you edit any settings, click the *Import* button to retrieve the most up-to-date configuration from the FortiGate Cloud-connected device.
3. On this page, you have limited access to a pared-down version of the FortiGate interface, allowing you to edit interfaces, routes, policies, etc. Edit the FortiGate configuration as needed.
4. When you are ready to push your updated configuration back to the device, select *Deploy* in the upper right.
5. Wait for the configuration to download to the device. When it completes, a deployment log appears, showing you the changes as they appear in the CLI.

Backup



Current Firmware Version: v6.2.1, build 0932

Revision Number	Created Time	Firmware Version	Description
Total (6)			
6	2019-09-13 14:47	v6.2.1, build 932	test06
5	2019-09-13 14:46	v6.2.1, build 932	test05
4	2019-09-13 14:41	v6.0.5, build 268	test04
3	2019-09-13 14:40	v6.0.5, build 268	test03
2	2019-09-13 14:34	v6.2.1, build 932	test02
1	2019-09-13 14:34	v6.2.1, build 932	test01

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

You cannot restore backups for FortiGates that are running FortiOS 6.2 and FortiGates with VDOMs enabled.

To back up the device configuration to the cloud:

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

To enable auto backup:

1. Go to *Management* > *Backup* > *Auto Backup Setting*.
2. Click *Enable Auto Backup*. Only setting changes on the FortiGate (locally from the FortiGate or from FortiGate

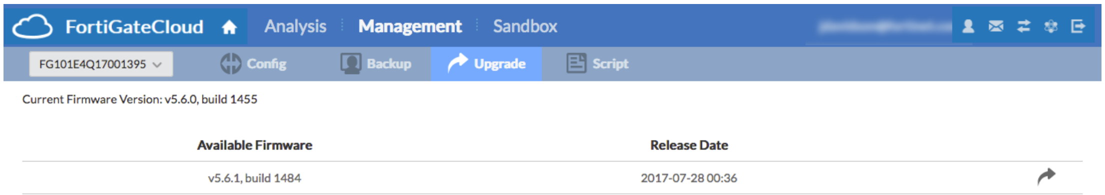
Cloud) trigger auto backup. You can select one of the following auto back up settings:

Option	Description
Per Session	By default, the session duration is 600 seconds. For example, if you modify FortiGate settings at 10:00 AM, FortiGate Cloud schedules an auto backup in 600 seconds. If no other setting changes occur within the 600 seconds, FortiGate Cloud performs an auto backup at 10:10 AM. However, if you further modify settings, for example, at 10:05 AM, this resets the timer and FortiGate Cloud schedules an auto backup for 600 seconds after 10:05 AM. FortiGate Cloud keeps every backup revision for all sessions in one day. You can only configure an alert email for this option. The alert email does not contain a copy of the backup revision.
Per Day	This option operates the same as *Per Session*, except that FortiGate Cloud only keeps one latest backup revision per day.

3. Click *Apply*.

Auto backup only occurs if the device's settings have changed since the last backup.

Upgrade



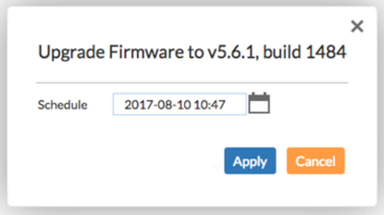
Current Firmware Version: v5.6.0, build 1455

Available Firmware	Release Date
v5.6.1, build 1484	2017-07-28 00:36

In *Upgrade*, you can see the current firmware version installed on the device, and update to newer stable versions if they are available.

To upgrade remote device firmware:

1. Go to *Management* > *Upgrade*.
2. Verify your device's current firmware version in the upper left before continuing.
3. If you are concerned about the effects of upgrading or have not upgraded recently, use the Upgrade Path Tool to ensure you are following the recommended upgrade path.
4. It is recommended to back up your device's configuration before upgrading, in *Management* > *Backup* or in the device's management interface.
5. Select an available firmware from the list, and select *Upgrade*. You can schedule a time and date to perform the remote upgrade. For example, you can schedule it during downtime to minimize disruption. A caution icon may also display to indicate that the upgrade path may not be supported.

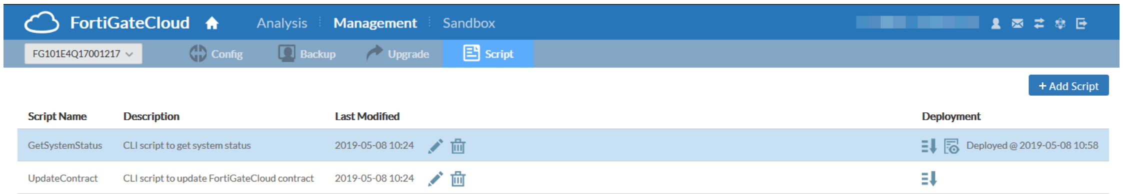


Upgrade Firmware to v5.6.1, build 1484

Schedule: 2017-08-10 10:47

6. Wait for the upgrade to take effect.

Script

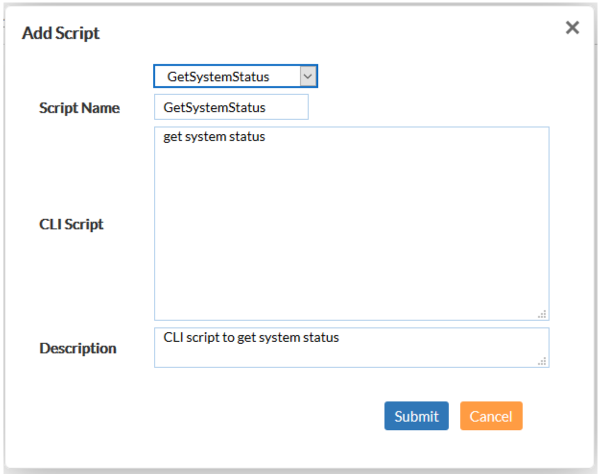


Script Name	Description	Last Modified	Deployment
GetSystemStatus	CLI script to get system status	2019-05-08 10:24	Deployed @ 2019-05-08 10:58
UpdateContract	CLI script to update FortiGateCloud contract	2019-05-08 10:24	

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

To execute a script on a remote device:

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



Add Script

GetSystemStatus

Script Name: GetSystemStatus

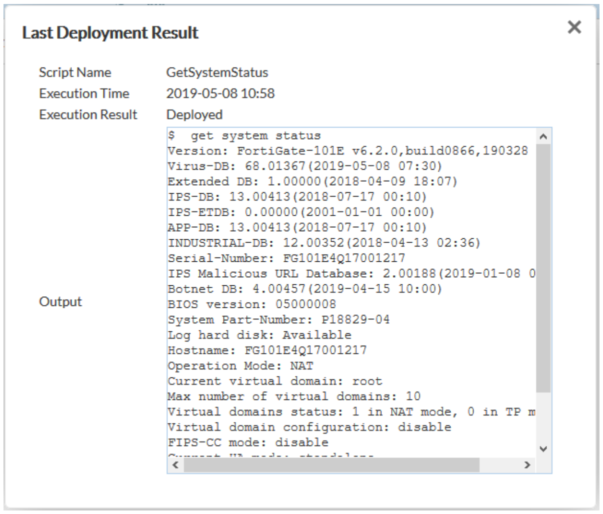
CLI Script:

```
get system status
```

Description: CLI script to get system status

4. Click the *Deploy* icon, and select a time to automatically deploy the script to the device.
5. To cancel the scheduled run, click the *Cancel* icon next to the scheduled time.

6. FortiGate Cloud records that script's output. You can read it by clicking *View Result*.



Last Deployment Result

Script Name GetSystemStatus

Execution Time 2019-05-08 10:58

Execution Result Deployed

Output

```
$  get system status
Version: FortiGate-101E v6.2.0,build0866,190328
Virus-DB: 68.01367(2019-05-08 07:30)
Extended DB: 1.00000(2018-04-09 18:07)
IPS-DB: 13.00413(2018-07-17 00:10)
IPS-ETDB: 0.00000(2001-01-01 00:00)
APP-DB: 13.00413(2018-07-17 00:10)
INDUSTRIAL-DB: 12.00352(2018-04-13 02:36)
Serial-Number: FG101E4Q17001217
IPS Malicious URL Database: 2.00188(2019-01-08 0
Botnet DB: 4.00457(2019-04-15 10:00)
BIOS version: 05000008
System Part-Number: P18829-04
Log hard disk: Available
Hostname: FG101E4Q17001217
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP m
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: standalone
```

Sandbox

FortiSandbox Cloud is a service that uploads and analyzes files that FortiGate AV marks as suspicious.

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

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

The FortiGate Cloud console enables administrators to view the status of any suspicious files uploaded: Pending, Clean, Malware, or Unknown. The console also provides data on time, user, and location of the infected file for forensic analysis. Sandboxing is available in both free and paid FortiGate Cloud subscriptions.

You can view the *FortiSandbox Cloud Service Description* for details.

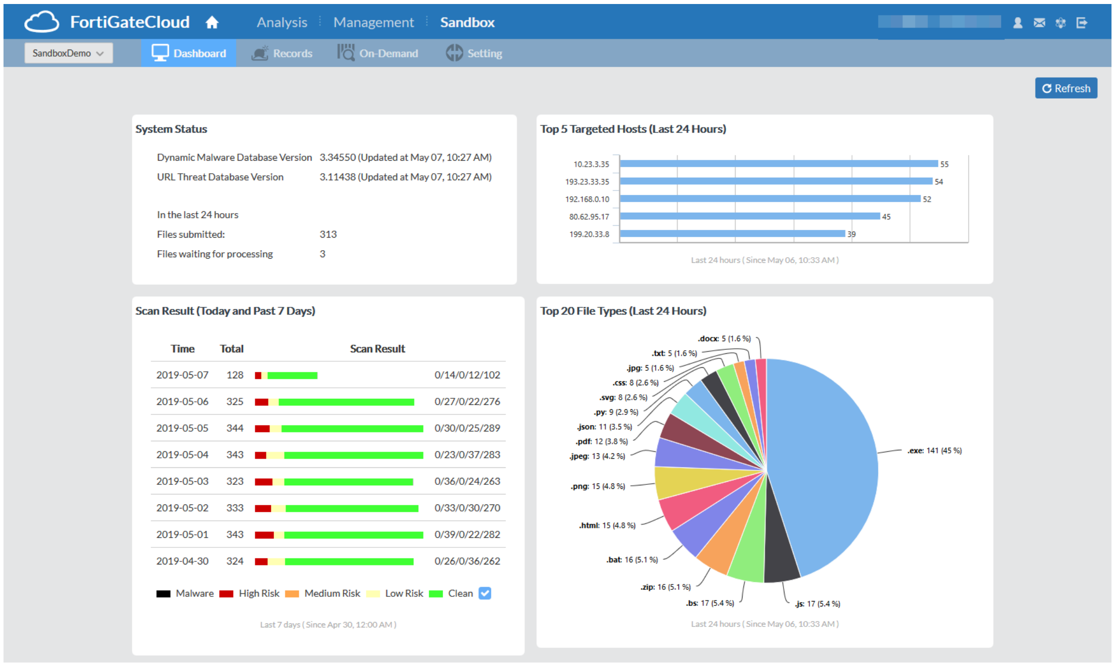
The *Sandbox* tab collects information that the FortiSandbox Cloud service compiles. FortiSandbox Cloud submits files to FortiGuard for threat analysis. You can configure your use of the service and view analyzed files' results.

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

To set up FortiSandbox:

1. Go to *Security Fabric* > *Settings* and enable *Sandbox Inspection*. Set *Sandbox type* to *FortiSandbox Cloud*. The associated FortiGate Cloud account appears.
2. In *Security Profiles* > *AntiVirus*, create a profile that has *Send Files To FortiSandbox Cloud For Inspection* configured.
3. Create a firewall policy with logging enabled that uses the FortiSandbox-enabled AV profile.
4. Once devices have uploaded some files to FortiSandbox Cloud, log in to the FortiGate Cloud portal to see the results.

Dashboard



System Status

Dynamic Malware Database Version 3.34550 (Updated at May 07, 10:27 AM)
URL Threat Database Version 3.11438 (Updated at May 07, 10:27 AM)

In the last 24 hours
Files submitted: 313
Files waiting for processing 3

Top 5 Targeted Hosts (Last 24 Hours)

Scan Result (Today and Past 7 Days)

Time	Total	Scan Result
2019-05-07	128	0/14/0/12/102
2019-05-06	325	0/27/0/22/276
2019-05-05	344	0/30/0/25/289
2019-05-04	343	0/23/0/37/283
2019-05-03	323	0/36/0/24/263
2019-05-02	333	0/33/0/30/270
2019-05-01	343	0/39/0/22/282
2019-04-30	324	0/26/0/36/262

■ Malware 🟥 High Risk 🟧 Medium Risk 🟨 Low Risk 🟩 Clean ☑
Last 7 days (Since Apr 30, 12:00 AM)

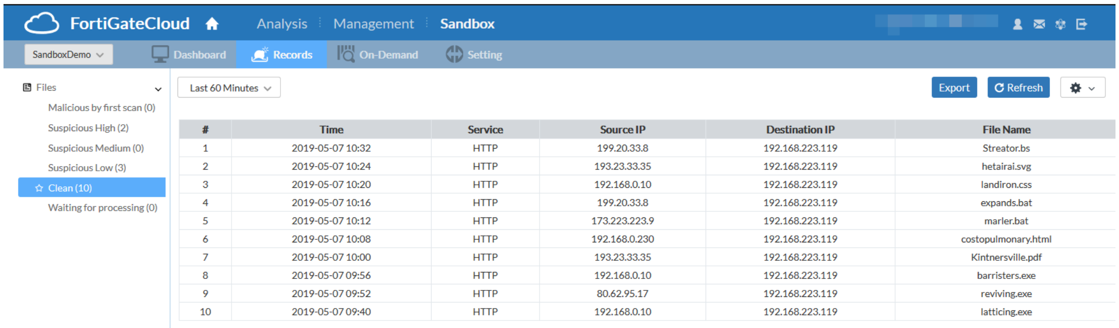
Top 20 File Types (Last 24 Hours)

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

The Dashboard contains the following widgets:

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

Records and On-Demand



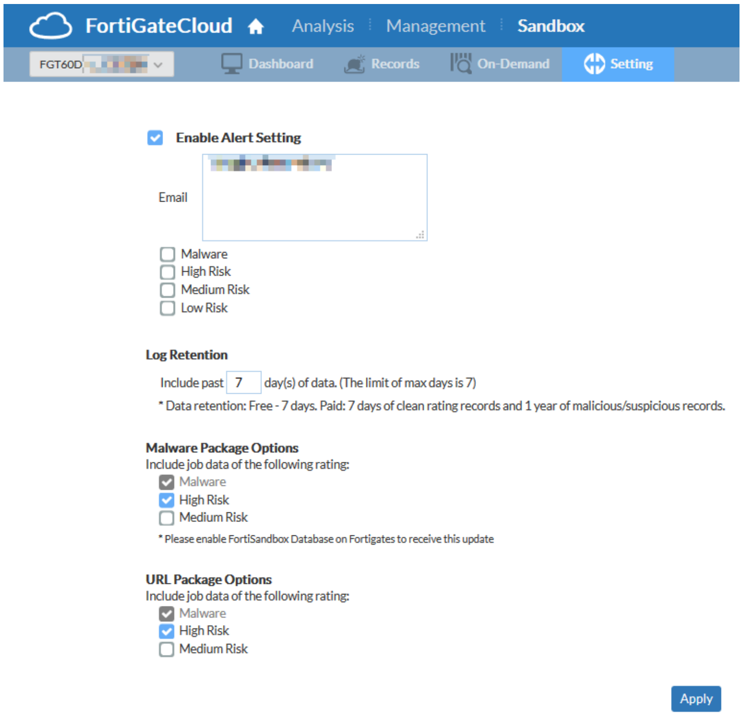
#	Time	Service	Source IP	Destination IP	File Name
1	2019-05-07 10:32	HTTP	199.20.33.8	192.168.223.119	Streator.bs
2	2019-05-07 10:24	HTTP	193.23.33.35	192.168.223.119	hetairai.svg
3	2019-05-07 10:20	HTTP	192.168.0.10	192.168.223.119	landiron.css
4	2019-05-07 10:16	HTTP	199.20.33.8	192.168.223.119	expands.bat
5	2019-05-07 10:12	HTTP	173.223.223.9	192.168.223.119	marler.bat
6	2019-05-07 10:08	HTTP	192.168.0.230	192.168.223.119	costopulmonary.html
7	2019-05-07 10:00	HTTP	193.23.33.35	192.168.223.119	Kintnersville.pdf
8	2019-05-07 09:56	HTTP	192.168.0.10	192.168.223.119	barristers.exe
9	2019-05-07 09:52	HTTP	80.62.95.17	192.168.223.119	reviving.exe
10	2019-05-07 09:40	HTTP	192.168.0.10	192.168.223.119	latticing.exe

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

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

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

Setting



☑ Enable Alert Setting

Email [redacted]

□ Malware
□ High Risk
□ Medium Risk
□ Low Risk

Log Retention

Include past 7 day(s) of data. (The limit of max days is 7)

* 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

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

- *Enable Alert Setting:* to enable alert emails, enter multiple emails (one per line) to receive alerts, and set which severity level triggers sending alert emails.
- *Log Retention*: set number of days to retain log data.
- *Malware Package Options* and *URL Package Options*: select the risk level of data that will be automatically submitted to FortiGuard to further antithreat research.

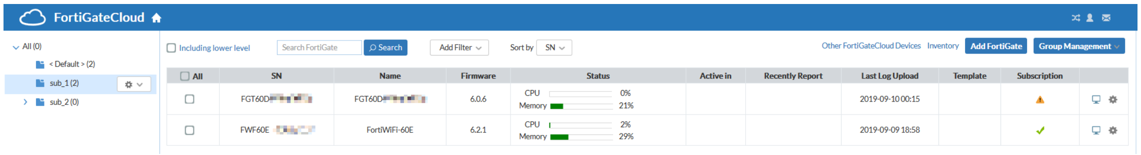
To configure FortiSandbox alert emails:

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

Multitenancy

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

After you activate multitenancy, FortiGate Cloud replaces the default homepage with the multitenancy homepage.



□ All	SN	Name	Firmware	Status	Active in	Recently Report	Last Log Upload	Template	Subscription	
□	FGT60D[redacted]	FGT60D[redacted]	6.0.6	CPU 0% Memory 21%			2019-09-10 00:15		⚠	
□	FWF60E [redacted]	FortiWiFi-60E	6.2.1	CPU 2% Memory 29%			2019-09-09 18:58		✓	

You can access management actions from the multitenancy homepage. Some actions are not unique to multitenancy and are described elsewhere in this document. For descriptions of these functions, see Homepage on page 13.

To activate multitenancy:

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

To configure basic multitenancy:

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

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

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

To assign a device to a subaccount on the homepage:

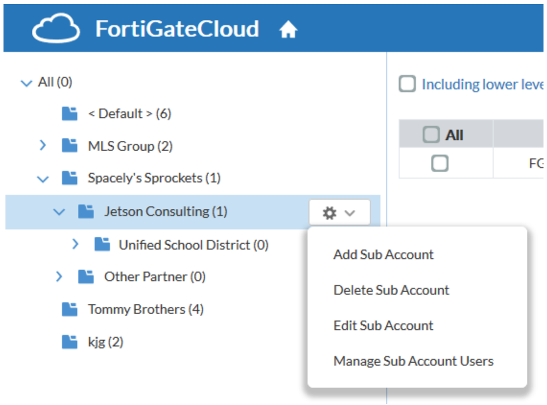
Assigning a device to a new subaccount keeps the device data in FortiGate Cloud, including logs, reports, and configuration backup and moves this data to the new subaccount. To delete this data, you must undeploy your device from FortiGate Cloud, then assign it to the desired subaccount.

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

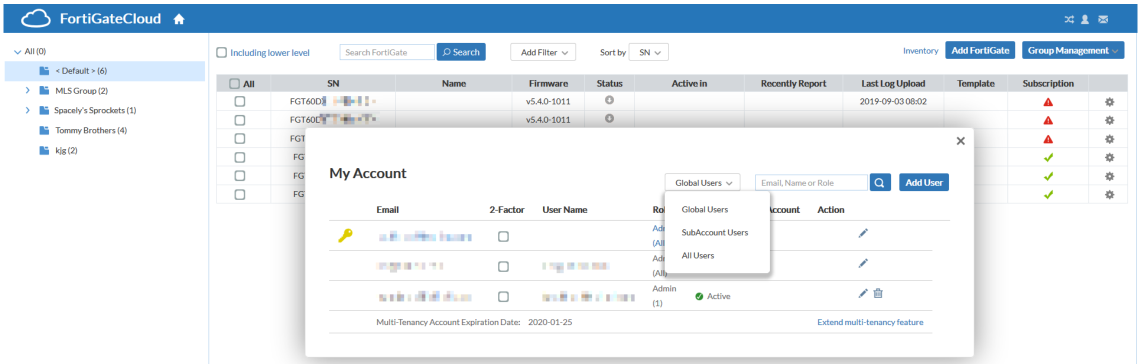
1. On the multitenancy homepage, click the *Config* icon beside the desired device, then click *Assign To*.
2. In the *Assign To* dialog, select the desired subaccount, then click *Submit*.
3. In the confirmation dialog, click *YES*.

To manage subaccounts:

1. The multitenancy homepage lists subaccounts on the left panel. To manage a subaccount, click the desired subaccount. From the dropdown list, select the desired management action.



2. On the multitenancy page, click the *My Account* icon. You can view all accounts associated with this FortiGate Cloud. Use the dropdown list to view *Global*, *SubAccount*, or *All Users*. You can see in this dialog that users have different roles. For descriptions of the roles, see User roles on page 39.



All	SN	Name	Firmware	Status	Active in	Recently Report	Last Log Upload	Template	Subscription
□	FGT60D[redacted]		v5.4.0-1011				2019-09-03 08:02		▲
□	FGT60D[redacted]		v5.4.0-1011						▲
□	FGT								▲
□	FG								✓
□	FG								✓
□	FG								✓

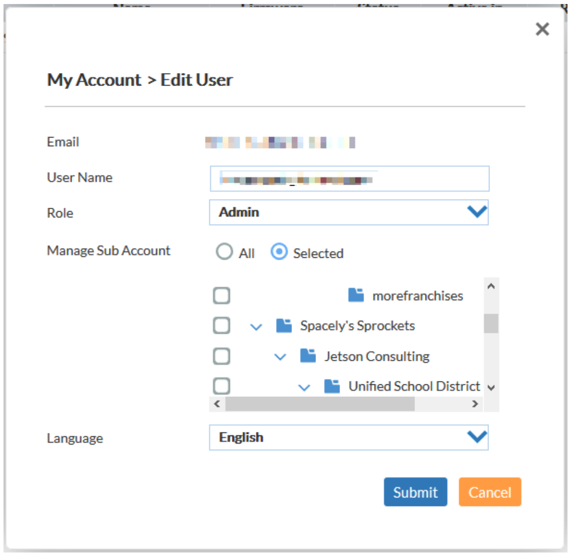
My Account

Email	2-Factor	User Name	Ro	ccount	Action
[redacted]	□		Adı (All		
[redacted]	□	[redacted]	Adı (All)		
[redacted]	□	[redacted]	Admin (1)	Active	

Multi-Tenancy Account Expiration Date: 2020-01-25

3. Click the *Edit* icon for the desired account.
4. In the *My Account* > *Edit User* dialog, for *Manage Sub Account*, select *Selected*. Select the desired subaccounts

for this user to manage.



My Account > Edit User

Email [redacted]

User Name [redacted]

Role: Admin

Manage Sub Account: ○ All ● Selected

- □ morefranchises
- □ Spacely's Sprockets
  - □ Jetson Consulting
    - □ Unified School District

Language: English

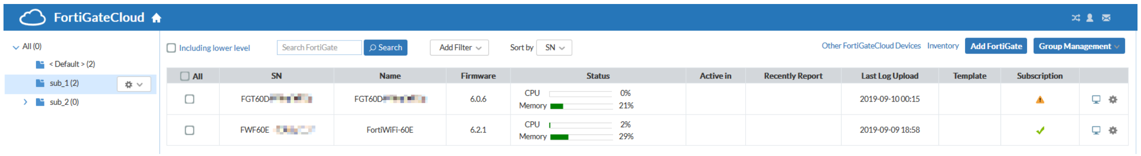
User roles

The multitenancy account includes different user roles. You can view users and their roles by clicking the *My Account* icon.

User role	Description
Admin (All)	Administrator who can access devices under all subaccounts.
Admin (1)	Administrator who can only access devices under the one subaccount that is assigned to them, including the assigned subaccount's child subaccounts.
Regular (All)	Regular user who has view-only access to all subaccounts.
Regular (1)	Regular user who has view-only access to all subaccounts, including the assigned subaccount's child subaccounts.

Admin (All)

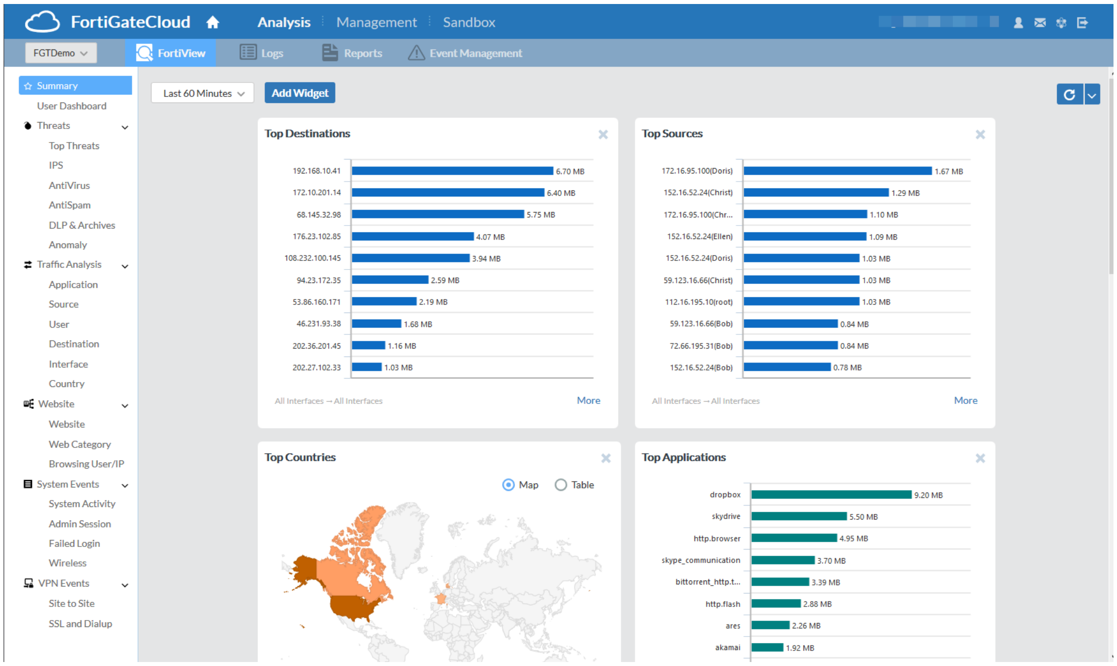
The Admin (All) user can view and access all subgroups on the left pane, and use Management functions.



- All (0)
  - < Default > (2)
  - sub_1 (2)
  - sub_2 (0)

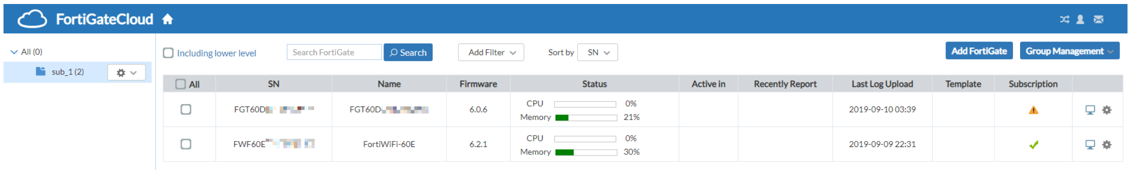
□ Including lower level | Search FortiGate | Sort by SN

□ All	SN	Name	Firmware	Status	Active in	Recently Report	Last Log Upload	Template	Subscription	
□	FGT60D[redacted]	FGT60D[redacted]	6.0.6	CPU 0% Memory 21%			2019-09-10 00:15		⚠	
□	FWF60E [redacted]	FortiWiFi-60E	6.2.1	CPU 2% Memory 29%			2019-09-09 18:58		✓	



Admin (1)

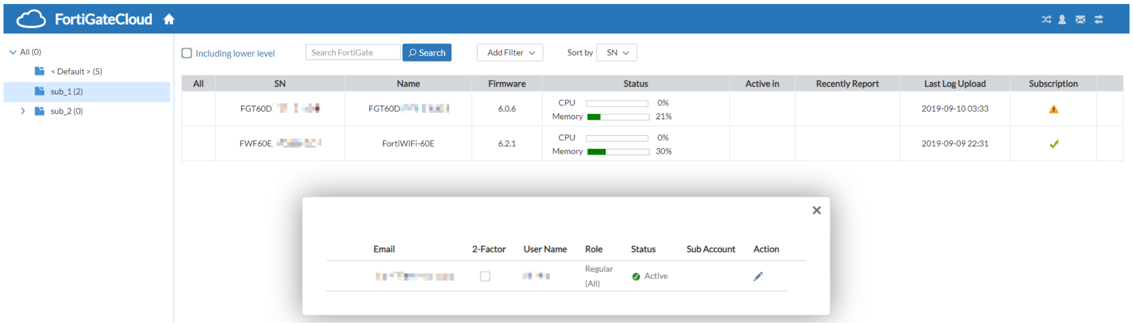
The Admin (1) user can only access devices under the one subaccount assigned to them (and any child subaccounts), as shown in the left pane. They can access Management functions.



All	SN	Name	Firmware	Status	Active in	Recently Report	Last Log Upload	Template	Subscription
□	FGT60D[redacted]	FGT60D[redacted]	6.0.6	CPU 0% Memory 21%			2019-09-10 03:39		⚠
□	FWF60E[redacted]	FortiWiFi-60E	6.2.1	CPU 0% Memory 30%			2019-09-09 22:31		✓

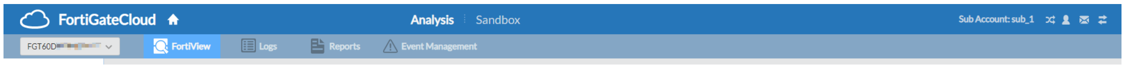
Regular (All)

The Regular (All) user has view-only access to all subgroups, but has no access to Management functions.



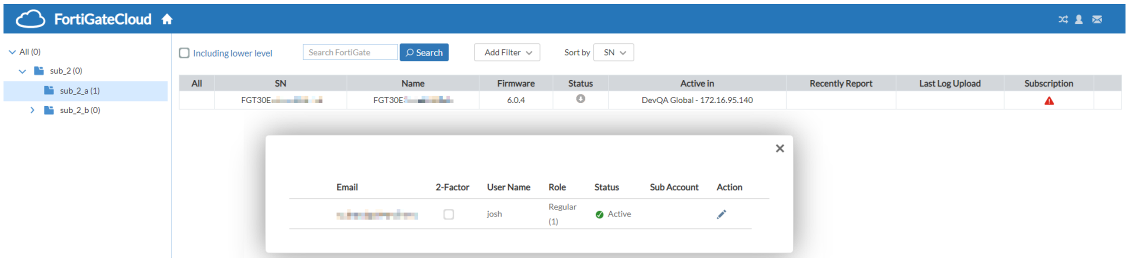
All	SN	Name	Firmware	Status	Active in	Recently Report	Last Log Upload	Subscription
	FGT60D[redacted]	FGT60D[redacted]	6.0.6	CPU 0% Memory 21%			2019-09-10 03:33	⚠
	FWF60E[redacted]	FortiWiFi-60E	6.2.1	CPU 0% Memory 30%			2019-09-09 22:31	✓

Email	2-Factor	User Name	Role	Status	Sub Account	Action
[redacted]	□	[redacted]	Regular (All)	Active		✎



Regular (1)

The Regular (1) user has view-only access to devices under the subaccount assigned to them (and any child subaccounts), as shown in the left pane. In this example, the user is assigned access to the sub_2 subaccount, which means they can also view devices assigned to the sub_2_a and sub_2_b subaccounts, which are children of the sub_2 subaccount. The Regular (1) user cannot access Management functions.



All	SN	Name	Firmware	Status	Active in	Recently Report	Last Log Upload	Subscription
	FGT30E[redacted]	FGT30E[redacted]	6.0.4		DevQA Global - 172.16.95.140			⚠

Email	2-Factor	User Name	Role	Status	Sub Account	Action
[redacted]	□	josh	Regular (1)	✓ Active		✎

Group management

Multitenancy also enables group management actions. You can apply actions to a group of FortiGate and FortiWifi devices, simplifying administrative tasks.

Some group management actions require that you enable management on the selected device. See Management on page 28.

You can access group management actions from the multitenancy homepage. Some actions are not unique to group management and are described elsewhere in this document in the context of use on a single device; the multitenancy homepage simply offers the ability to apply the action to multiple devices. For descriptions of these functions, see the following topics:

Schedule Report	To schedule a report: on page 24
Deploy Config	To deploy cloud configuration to devices: on page 29
Upgrade Firmware	To upgrade remote device firmware: on page 30
Run Script	To execute a script on a remote device: on page 31
Set Auto Backup	To enable auto backup: on page 29
Manage Report Configs	Reports on page 23
Manage Scripts	Script on page 31

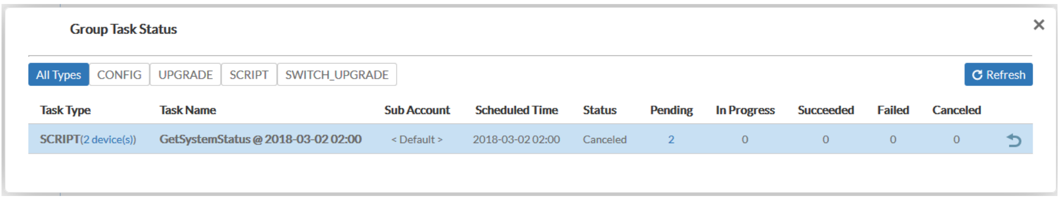
The following describes actions exclusive to group management:

To view group task status:

You can view the current status of group management actions.

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

that the group management action was applied to.



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

Templates

You can create device configuration templates and deploy different templates to applicable devices to simplify device management. FortiGate Cloud applies the template to the selected devices.

To create a template:

1. On the multitenancy homepage, click *Group Management* > *Manage Templates*.
2. Click *Create Template*.
3. In the *Name* field, enter the desired template name.
4. In the *Description* field, enter the desired template description.
5. For *Create template based on*, select one of the following:

Option	Description
In-cloud config copy of sampling device	Create a template based on a sample device that has already been added to FortiGate Cloud. Select the desired device from the dropdown list. Only devices from the subaccount selected in *Sub Account* are available.
Platform and version	Create a template based on a specific FortiGate or FortiWifi platform and FortiOS version.
Config file	Create a template based on a configuration file. You must upload a .conf file.

6. For *Feature set*, select the desired features.
7. For *Sub Account*, select the desired sub account for this template.
8. Click *Apply*.

To apply a template to devices:

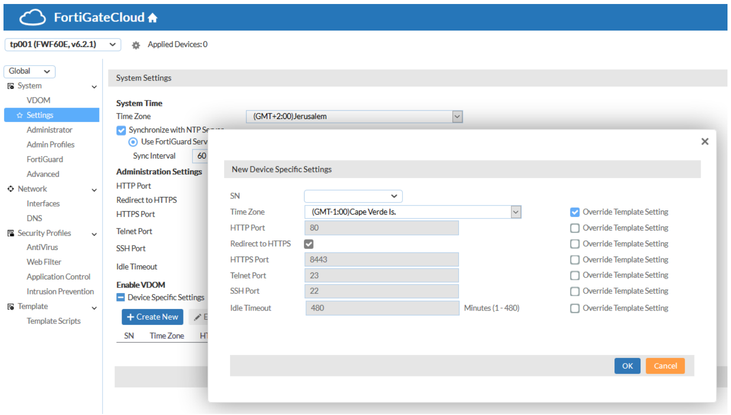
1. On the multitenancy homepage, select the desired devices
2. Click *Group Management* > *Use Templates*.
3. In the *Use Templates* dialog, select the desired template. The dialog only shows templates applicable for the current selected devices.
4. Click *Apply*. FortiGate Cloud applies the template to the selected devices.

To revoke templates from devices:

1. On the multitenancy homepage, select the desired devices.
2. Click *Group Management* > *Un-use Templates*.
3. Click *Apply*. FortiGate Cloud revokes the templates from the selected devices.

To edit a template:

1. On the multitenancy homepage, go to *Group Management* > *Manage Templates*.
2. Click the *Edit* icon for the desired template.
3. For a template that has already been applied to devices, you can configure device-specific settings:
   a. Go to the desired configuration page, then expand *Device Specific Settings*.
   b. Click *Create New*.
   c. In the *New Device Specific Settings* dialog, select the desired device's serial number from the *SN* dropdown list.
   d. To configure a device-specific setting, enable *Override Template Setting*, then configure the desired option. Otherwise, FortiGate Cloud applies the template setting to the device. Click *OK*.
      The example configures a device-specific setting for the time zone using Cape Verde Island time, which differs from the template setting, which uses Jerusalem time.



Time Zone: (GMT+2:00)Jerusalem

☑ Synchronize with NTP Se

● Use FortiGuard Serv

Sync Interval: 60

▬ Device Specific Settings

New Device Specific Settings

SN		
Time Zone	(GMT-1:00)Cape Verde Is.	☑ Override Template Setting
HTTP Port	80	☐ Override Template Setting
Redirect to HTTPS	☑	☐ Override Template Setting
HTTPS Port	8443	☐ Override Template Setting
Telnet Port	23	☐ Override Template Setting
SSH Port	22	☐ Override Template Setting
Idle Timeout	480 Minutes (1 - 480)	☐ Override Template Setting

IOC

FortiGate Cloud IOC alerts administrators about newly found infections and threats to devices in their network. By analyzing UTM logging and activity, IOC provides a comprehensive overview of threats to the network.

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

Threat type	Description
Malware	Malicious programs residing on infected endpoints
Potentially unwanted programs	Spyware, adware, and toolbars
Unknown	Threats that the signature has detected but are not associated with any known malware

The free version of IOC is currently available on all accounts in the North America datacenter. The free version alerts you to threats and automatically prepares a comprehensive threat report. Threats listed only provide infected devices' partial IP addresses: server and subnet.

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

To purchase an IOC subscription:

1. Open the *Plan* page in the FortiGate Cloud IOC site, and select *Buy Online*.
2. Complete the purchase process, and wait for the key to arrive by email.
3. Log into the Fortinet Support website.
4. On the *Asset* page, register the code as if it were a new product's serial number, and then enter the serial number of the FortiGate Cloud-connected device that you want the service to monitor. The service automatically takes effect.

To access IOC using a non-multitenancy account:

1. In the FortiGate list, click the *Threats/Suspicious* label under *System Status*. This only appears if the FortiGate has detected any threats.

To access IOC using a multitenancy account:

1. In the FortiGate list, look to the right. If your FortiGate has detected any threats, a bomb icon is visible. Click the bomb icon.

FortiDeploy

FortiDeploy is a product built into FortiGate Cloud for one-touch provisioning when devices are deployed locally or remotely. FortiDeploy provides automatic connection of FortiGates to be managed by FortiGate Cloud or a FortiManager.

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

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

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

FortiDeploy is available for FortiGate, FortiWiFi, and PoE desktop and 1U models up to the 900D. It is recommended for trained personnel to handle larger deployments. FortiDeploy is available for devices running FortiOS 5.2.2 and later.

To enable autojoining FortiGate Cloud:

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

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

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

To set central management to FortiGuard:

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

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

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

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

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

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

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

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