FortiGate Cloud - Administration Guide

Version 3.3.3

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 COOKBOOK
https://cookbook.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: techdocs@fortinet.com

FORTINET®

February 22, 2019
FortiGate Cloud 3.3.3 Administration Guide
32-332-535370-20190128

TABLE OF CONTENTS

FortiGate Cloud 6

User guide 7

Overview 7

Home page 8

Analysis pages 9

FortiView: Summary 9

FortiView: Sections 11

Logs 12

Reports 12

Event Management 14

Management pages 15

Config 15

Backup 16

Upgrade 16

Script 17

Sandbox pages 19

Dashboard 20

Records / On-Demand 20

Setting 21

Frequently asked questions 22

General questions 22

What is FortiGate Cloud? 22

What functions does FortiGate Cloud have? 23

How does FortiGate Cloud work? 23

How does FortiGate Cloud compare with FortiPortal and FortiAnalyzer? 23

How do I confirm which version of FortiGate Cloud is currently in use? 24

Which languages are supported by FortiGate Cloud? 24

Can I choose which data center my logs are stored in? 25

How can I provide feedback or request improvements to FortiGate Cloud? 25

Is there a European FortiGate Cloud instance? 25

If I am an existing customer in EMEA, will my data be transferred to the new data center, or will it remain in its current location? 25

Is there an account designed for MSSP-scale operations? 25

What are the new features in FortiCloud? 26

Licensing and registration 26

Is there an easy way to test drive FortiGate Cloud? 26

What is the price of FortiGate Cloud? 26

Do I need a support contract to enable the service? 27

How do I subscribe to a FortiGate Analysis and Log Retention contract? 27

What features do I get access to for subscribing? 27

What happens if I lose my password? 27

Can I use two-factor authentication for FortiGate Cloud? 28

How do you configure the service once it is activated? 28

How long are logs retained? 28

When a device subscription lapses, what happens to the year’s worth of logs? 28

How can I unsubscribe from the service and stop uploading logs? 28
Technical questions 28
What security and redundancy has been built into the service? 29
How do I verify my network is PCI compliant? 29
Does my FortiGate require a hard drive to use FortiGate Cloud? 29
Does FortiGate Cloud support devices from other vendors? 29
Which FortiGate and FortiWiFi models does FortiGate Cloud support? 29
Which versions of FortiOS does FortiGate Cloud support? 29
What port numbers are used by FortiGate devices connecting to FortiGate Cloud? 30
When are scheduled reports sent to administrators? 30
Why can I not see any management functions? 30
Can I set up high availability (HA) logging with FortiGate Cloud? 30
Do I need to purchase a subscription for each FortiGate in an HA pair? 30
FortiSandbox Cloud 31
How does cloud sandboxing and AV submission work? 31
Why can I not see a function or tab for AV Submission/Sandboxing? 31
What is the turnaround time on Cloud Sandboxing and AV Submission? 31
Is there a service description for FortiSandbox Cloud? 31
Indicator of Compromise (IOC) Service 31
What is the FortiGate Cloud Indicator of Compromise Service? 32
What kind of threats can the IOC Service detect? 32
How do I get access to the IOC Service? 32
Does the IOC Service require a subscription? 32
How do I register my subscription code once I’ve purchased one? 33
FortiDeploy 33
What is FortiDeploy? 33
How does FortiDeploy work? 33
How do I purchase FortiDeploy? 33
What is the price of FortiDeploy? 34
What happens if you forget to order FortiDeploy on the PO? 34
Will my FortiGuard and FortiCare services start automatically? 34
What models are supported by FortiDeploy? 34
Which versions of FortiOS does FortiDeploy support? 34
Are there any complications if I’ve recently upgraded FortiOS? 34
What if I am connected to FortiCloud but the device is not cloud-managed? 35
What if a device is deployed behind a NAT device (such as a cable modem)? 35
FortiGate Cloud Cookbook 36
Basic configuration 36
Basic FortiGate Cloud setup 36
FortiSandbox Cloud setup 36
Indicator of Compromise (IOC) setup 36
FortiGate Cloud device configuration 37
Deploying cloud configuration to devices 37
Device configuration backup to cloud 37
Remote device firmware upgrade 37
Remote device script execution 38
Advanced configuration 38
Adding more administrators/users 38

Creating custom FortiGate Cloud reports 38
Configuring FortiSandbox alert emails 38
Multi-Tenancy configuration 39
Activating Multi-Tenancy feature 39
Basic Multi-Tenancy configuration 39

FortiGate Cloud

This guide provides information about FortiGate Cloud. It's divided into the following sections:

- User guide: information about how you use FortiGate Cloud.
- Frequently asked questions: answers to commonly asked questions about FortiGate Cloud.
- FortiGate Cloud Cookbook: a series of short-form tutorials that teach how to perform tasks in FortiGate Cloud, ranging from basic to complex.

As of FortiCloud 3.2.2, the FortiCloud service has been separated into two distinct parts: FortiGate Cloud, which you use to manage FortiGate devices, and FortiAP Cloud, which you use to manage FortiAP devices (FortiAP Cloud contains functions formerly called FortiAP Network).

This guide contains information about FortiGate Cloud. For information about FortiAP Cloud, please see the FortiAP Cloud Administration Guide.

User guide

This section includes information about how you can use FortiGate Cloud.

Overview

FortiGate Cloud is a cloud-based infrastructure management solution and log retention service for FortiGate and FortiWiFi devices. It gives you centralized reporting, traffic analysis, configuration management, and log retention without the need for additional hardware and software, with the following feature set:

- Simple provisioning of large scale security networks
- Configuration and device management from a single pane of glass
- Hosted log retention and cloud-based storage
- Built-in protection from APTs with FortiGuard sandboxing technology
- Instant security intelligence and analytics with FortiView
- Exceptional network visibility with FortiGate Cloud reporting
- FortiGate Cloud transport security and service availability

FortiGate Cloud also integrates these other Fortinet services: FortiSandbox Cloud and FortiDeploy.

FortiSandbox Cloud

FortiSandbox Cloud is a service that uploads and analyzes files marked as suspicious by the FortiGate AntiVirus.

In a proxy-based antivirus profile on a FortiGate, the administrator selects Inspect Suspicious Files with FortiGuard Analytics to enable a FortiGate unit to upload suspicious files to FortiGuard for analysis. Once uploaded, the file will be 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 antivirus signature database. The next time the FortiGate unit updates its antivirus database it will have the new signature.

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

The FortiCloud 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 FortiCloud subscriptions.

FortiDeploy

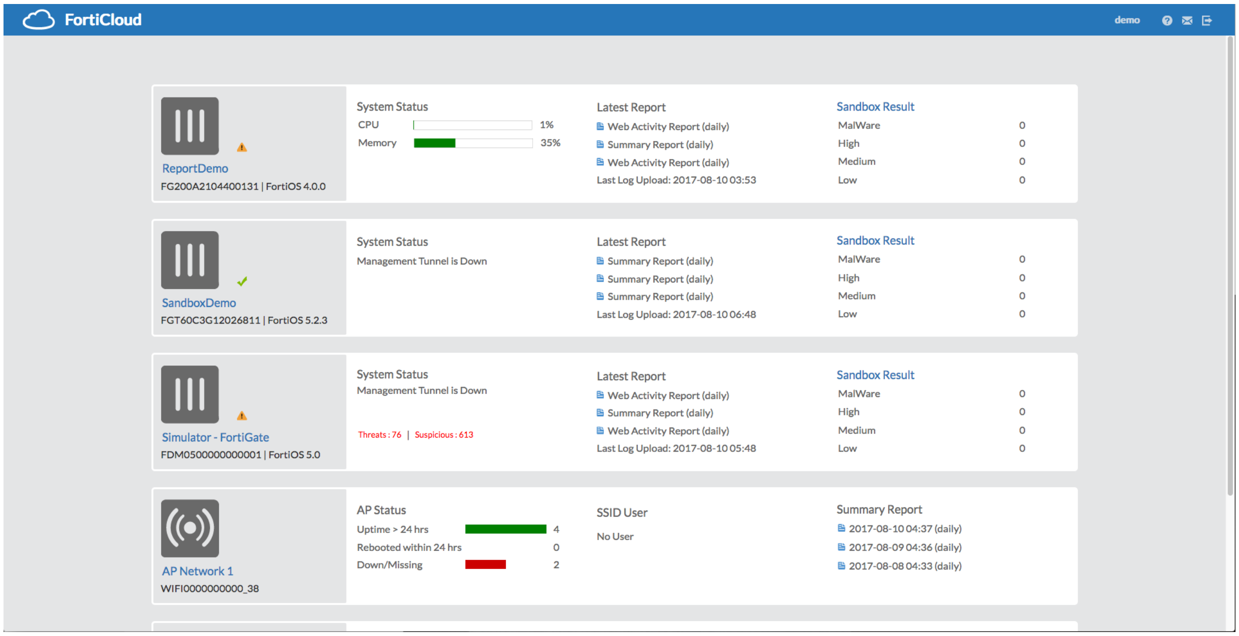
FortiDeploy is a product built into FortiCloud as a feature, for one-touch provisioning when devices are deployed, locally or remotely. FortiDeploy provides deployment for FortiAP devices into a Cloud AP Network, and automatic connection of FortiGates to be managed by FortiCloud or a FortiManager unit.

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

When you visit www.forticloud.com and enter the Bulk FortiCloud Key, you will see a list of serial numbers from the order that contained the FortiDeploy SKU. Once you confirm that the devices are connected, you can perform basic configuration on the devices remotely, such as sending a FortiManager IP to all remote FortiGate devices, so they can be managed remotely.

FortiDeploy support starts the moment you send an email to cs@fortinet.com, which can also be contacted if you have already purchased a FortiCloud subscription and would like to purchase FortiDeploy to add to your existing subscription.

Home page



ReportDemo
FG200A2104400131 | FortiOS 4.0.0

System Status
CPU 1%
Memory 35%

Latest Report
Web Activity Report (daily)
Summary Report (daily)
Web Activity Report (daily)
Last Log Upload: 2017-08-10 03:53

Sandbox Result	
MalWare	0
High	0
Medium	0
Low	0

SandboxDemo
FGT60C3G12026811 | FortiOS 5.2.3

System Status
Management Tunnel is Down

Latest Report
Summary Report (daily)
Summary Report (daily)
Summary Report (daily)
Last Log Upload: 2017-08-10 06:48

Sandbox Result	
MalWare	0
High	0
Medium	0
Low	0

Simulator - FortiGate
FDM0500000000001 | FortiOS 5.0

System Status
Management Tunnel is Down
Threats : 76 | Suspicious : 613

Latest Report
Web Activity Report (daily)
Summary Report (daily)
Web Activity Report (daily)
Last Log Upload: 2017-08-10 05:48

Sandbox Result	
MalWare	0
High	0
Medium	0
Low	0

AP Network 1
WIFI0000000000_38

AP Status	
Uptime > 24 hrs	4
Rebooted within 24 hrs	0
Down/Missing	2

SSID User
No User

Summary Report
2017-08-10 04:37 (daily)
2017-08-09 04:36 (daily)
2017-08-08 04:33 (daily)

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. New devices can be added by selecting **Add Device** and entering a FortiGate Cloud Key.

Each device displays:

- the model/serial number
- the type of Fortinet product
- if the device is connected through a management tunnel
- the last compiled report and the 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)
- a yellow warning symbol, or a green check symbol, to show subscription status.

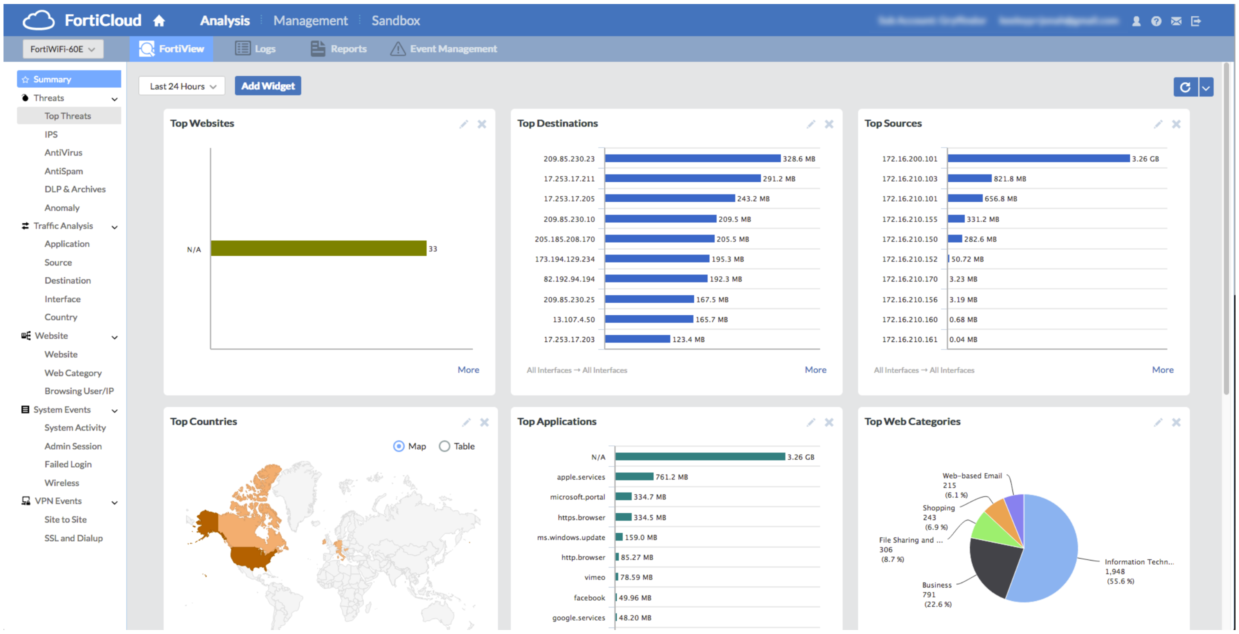
Next to some device icons will be a gear icon, allowing you to delete/rename/configure devices.

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

Analysis pages

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

FortiView: Summary



The default FortiView page is the summary view, general overview of what is happening with your device, using many widgets. New widgets can be added by selecting **Add Widget**.

Each widget is a customizable box, showing certain information about the device.

- You can click on a widget title and drag it to move it around.
- You can customize any widget by selecting the pencil icon.
- You can delete a widget by selecting the X icon.
- You can set the refresh rate of widgets by selecting the refresh icon in the upper right.

All of the types of widgets are listed below, grouped according to function.

Threats

- **Top Threats** displays which Threats are triggering the most detection events on the network. (One or more of the following must be configured on the device: IPS, AntiVirus, AntiSpam, DLP, Anomaly Detection.)
- **Top Spam** displays which Sources are sending the most Spam email into the network. (AntiSpam must be configured on the device.)
- **Top Viruses** counts the viruses most frequently found by the device's AntiVirus. (AntiVirus must be configured on the device.)

- **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 must be configured on the device.)
- **Top Attacks** counts the attacks most frequently prevented by the device's IPS. (IPS must be configured on the device.)
- **Top DLP By Rules** counts the DLP events detected by the device, sorted by DLP rule. (DLP must be configured on the device.)

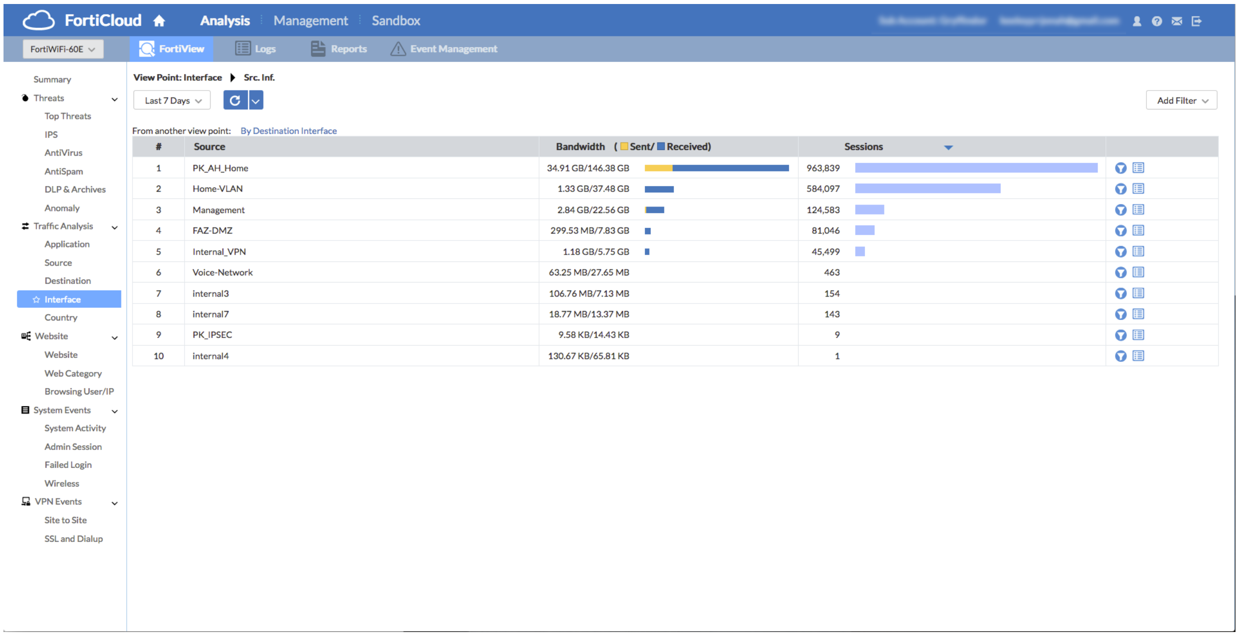
Traffic Analysis

- **Top Applications** compares which Applications are most frequently used, based on the device's Application Control settings. (Application Control must be configured on the device.)
- **Top Application Categories** compares which Application Categories are most frequently used, based on the device's Application Control settings. (Application Control must be configured on the device.)
- **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** is a chart that displays the volume of Incoming and Outgoing traffic over time.

Websites

- **Top Websites** compares which websites are most frequently visited. You can click on a category to see which websites in that category are being visited. (Web Filtering must be configured on the device.)
- **Top Web Categories** compares which Web Filtering Categories are most frequently used, based on the device's Web Filtering settings. (Web Filtering must be configured on the device.)
- **Top Users/IP by Browsing Time In Seconds** compares which IPS are most frequently visited by which users in the greatest ratio. You can click on a user to see which IP addresses they are visiting. (Web Filtering must be configured on the device.)

FortiView: Sections



View Point: Interface ▶ Src. Inf.

Last 7 Days

From another view point: By Destination Interface

#	Source	Bandwidth (🟨 Sent/ 🟦 Received)	Sessions
1	PK_AH_Home	34.91 GB/146.38 GB	963,839
2	Home-VLAN	1.33 GB/37.48 GB	584,097
3	Management	2.84 GB/22.56 GB	124,583
4	FAZ-DMZ	299.53 MB/7.83 GB	81,046
5	Internal_VPN	1.18 GB/5.75 GB	45,499
6	Voice-Network	63.25 MB/27.65 MB	463
7	internal3	106.76 MB/7.13 MB	154
8	internal7	18.77 MB/13.37 MB	143
9	PK_IPSEC	9.58 KB/14.43 KB	9
10	internal4	130.67 KB/65.81 KB	1

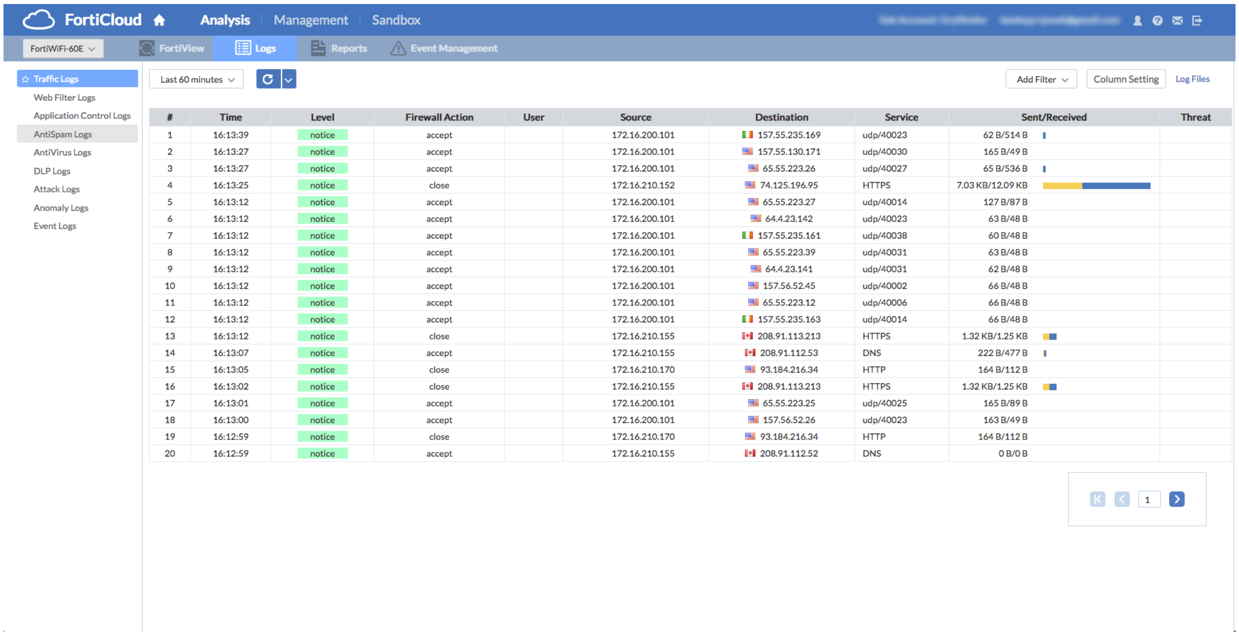
The various **FortiView** subpages offer log information, reformatted into easily navigable charts, in a similar style as the FortiView pages on a FortiGate. Each page is styled differently to suit the information structure. The above screenshot shows the **Interface** subpage, showing source interfaces charted by traffic volume.

The menu to the right of the subpage list allows you to select a time period to view:

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

You can set the refresh rate of the chart by selecting the Refresh icon to the right of the time period. By using the **Add Filter** dropdown menu, 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 (e.g. all log data through that interface.)

Logs



#	Time	Level	Firewall Action	User	Source	Destination	Service	Sent/Received	Threat
1	16:13:39	notice	accept		172.16.200.101	157.55.235.169	udp/40023	62 B/514 B	
2	16:13:27	notice	accept		172.16.200.101	157.55.130.171	udp/40030	165 B/49 B	
3	16:13:27	notice	accept		172.16.200.101	65.55.223.26	udp/40027	65 B/536 B	
4	16:13:25	notice	close		172.16.210.152	74.125.196.95	HTTPS	7.03 KB/12.09 KB	
5	16:13:12	notice	accept		172.16.200.101	65.55.223.27	udp/40014	127 B/87 B	
6	16:13:12	notice	accept		172.16.200.101	64.4.23.142	udp/40023	63 B/48 B	
7	16:13:12	notice	accept		172.16.200.101	157.55.235.161	udp/40038	60 B/48 B	
8	16:13:12	notice	accept		172.16.200.101	65.55.223.39	udp/40031	63 B/48 B	
9	16:13:12	notice	accept		172.16.200.101	64.4.23.141	udp/40031	62 B/48 B	
10	16:13:12	notice	accept		172.16.200.101	157.56.52.45	udp/40002	66 B/48 B	
11	16:13:12	notice	accept		172.16.200.101	65.55.223.12	udp/40006	66 B/48 B	
12	16:13:12	notice	accept		172.16.200.101	157.55.235.163	udp/40014	66 B/48 B	
13	16:13:12	notice	close		172.16.210.155	208.91.113.213	HTTPS	1.32 KB/1.25 KB	
14	16:13:07	notice	accept		172.16.210.155	208.91.112.53	DNS	222 B/477 B	
15	16:13:05	notice	close		172.16.210.170	93.184.216.34	HTTP	164 B/112 B	
16	16:13:02	notice	close		172.16.210.155	208.91.113.213	HTTPS	1.32 KB/1.25 KB	
17	16:13:01	notice	accept		172.16.200.101	65.55.223.25	udp/40025	165 B/89 B	
18	16:13:00	notice	accept		172.16.200.101	157.56.52.26	udp/40023	163 B/49 B	
19	16:12:59	notice	close		172.16.210.170	93.184.216.34	HTTP	164 B/112 B	
20	16:12:59	notice	accept		172.16.210.155	208.91.112.52	DNS	0 B/0 B	

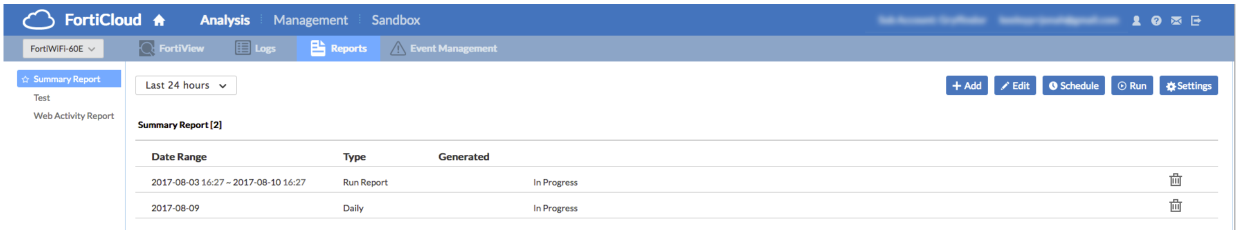
The **Log** pages offer more detailed log information, access to individual log data, and downloadable log files. The above screenshot shows the **Traffic Logs** subpage, showing traffic log data collected by the device. You can select a category of logs to view by selecting from the list on the left.

The menu to the right of the Categories allows you to select a time period to view:

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

You can set the refresh rate of the chart by selecting the refresh icon to the right of the time period. By using the **Add Filter** dropdown menu, you can filter the log list by various factors. Selecting **Column Setting** will allow 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.

Reports

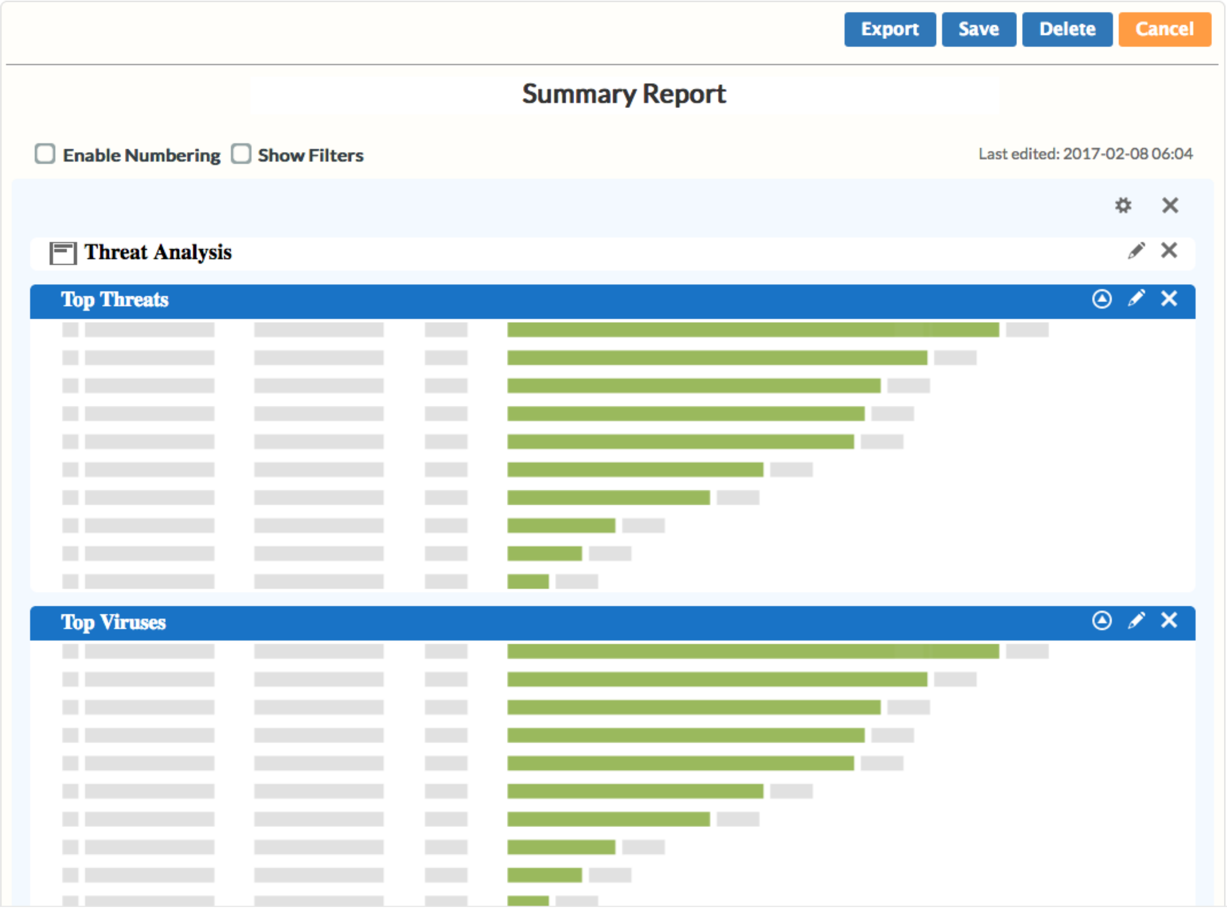


Summary Report [2]

Date Range	Type	Generated
2017-08-03 16:27 ~ 2017-08-10 16:27	Run Report	In Progress
2017-08-09	Daily	In Progress

The **Reports** page generates custom reports of specific traffic data, and can email them to specified addresses. Select a report on the left to see a list of collected reports of that type: there will be a pre-configured **Summary Report** and a **Web Activity Report** by default. Double-click on a report in the list to read it.

You can **Add** new reports or **Edit** existing ones in the upper right. Both of these will open an editing interface, which will allow you to edit the content of the report, adding or removing sections as you choose.



Summary Report

□ Enable Numbering □ Show Filters

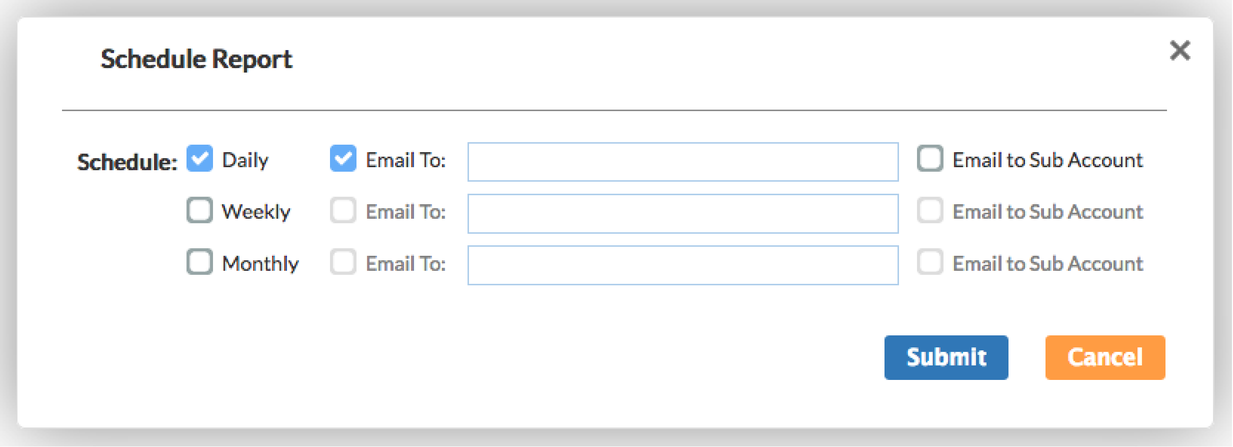
Last edited: 2017-02-08 06:04

Threat Analysis

Top Threats

Top Viruses

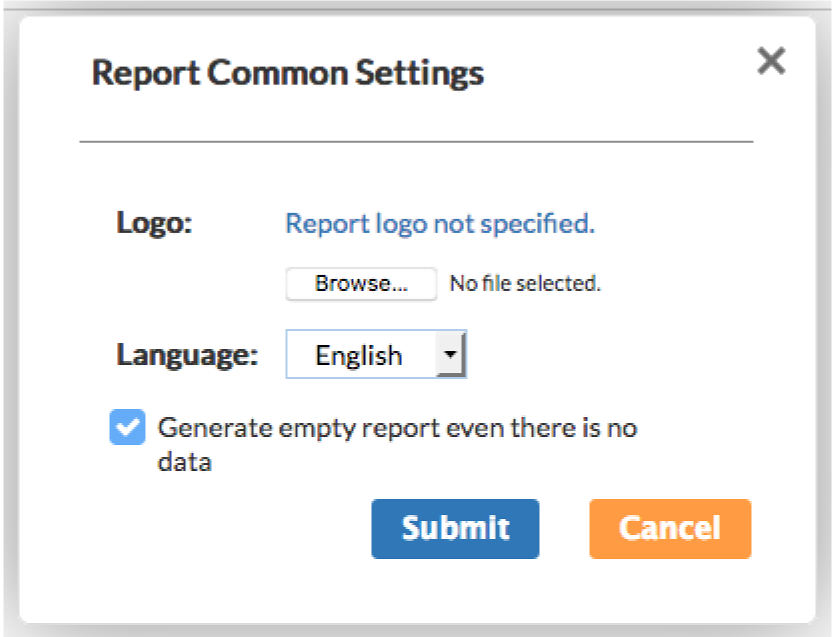
By selecting **Schedule**, you can set how often reports are run: **Daily**, **Weekly** or **Monthly**, and which email the reports are sent to. You can also choose to **Run** a report immediately.



Schedule Report

Schedule: ☑ Daily	☑ Email To:		□ Email to Sub Account
□ Weekly	□ Email To:		□ Email to Sub Account
□ Monthly	□ Email To:		□ Email to Sub Account

Next to the **Run** button is **Settings** where you can upload a report logo, and set the report language.



Report Common Settings

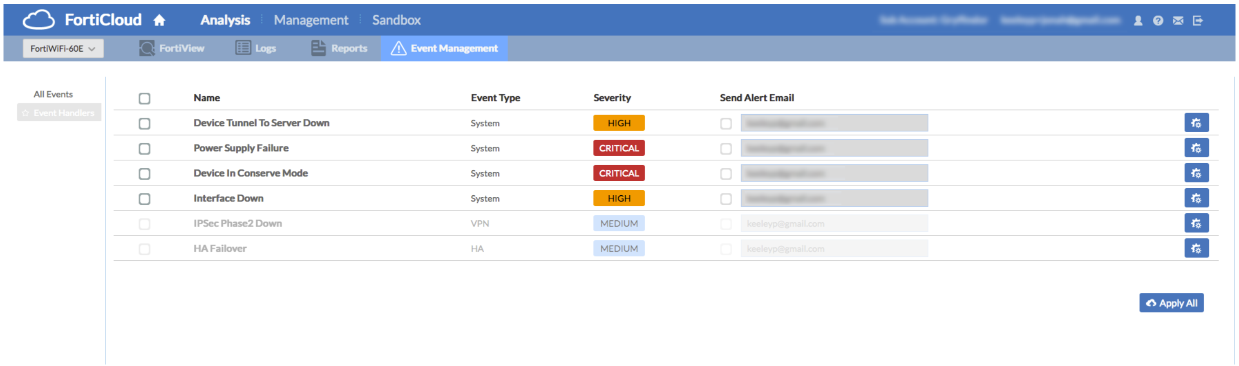
Logo: Report logo not specified.

Browse... No file selected.

Language: English

☑ Generate empty report even there is no data

Event Management



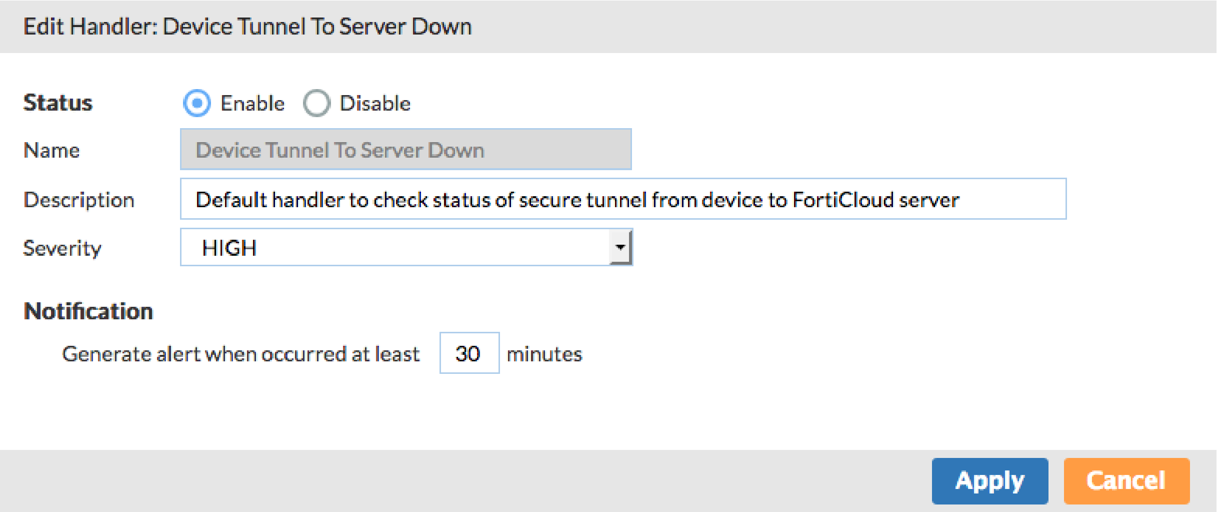
[redacted]

□	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	□	keeleyp@gmail.com
□	HA Failover	HA	MEDIUM	□	keeleyp@gmail.com

The **Event Management** page allows you to 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 will default to **All Events** in the left menu, which will list all past emergency events. Select **Event Handlers** to configure the alert settings.

You can enable events to track by checking them on the left. If you'd like to receive an alert email when they occur, check the mark under **Send Alert Email** and enter the email to send to.

Selecting the gear icon on the far right will allow you to configure each **Event Handler** directly, setting 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

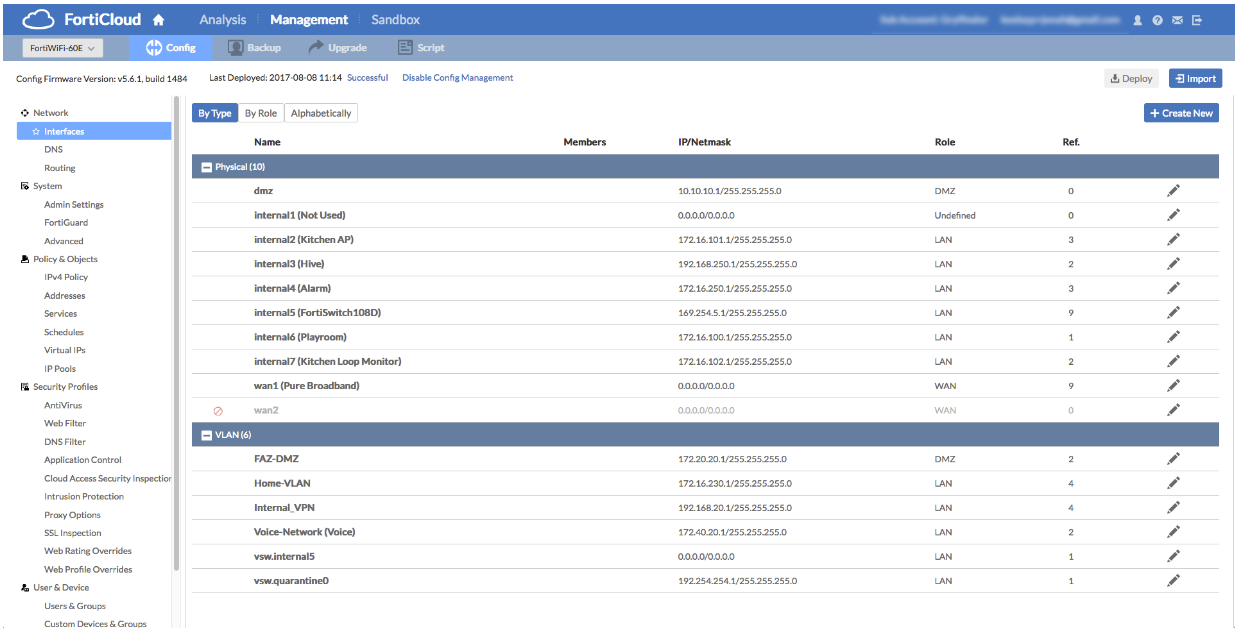
Generate alert when occurred at least 30 minutes

Management pages

The **Management** pages allow you to remotely manage FortiGate, FortiWiFi, and FortiAP devices that are connected to the FortiGate Cloud service.

These pages may only appear if you have purchased a FortiGate Cloud license, as FortiGate Cloud Management is part of the subscription service and will not be available in the free version of FortiGate Cloud from 3.2.1 onwards. It is available in 3.2 on a trial basis.

Config



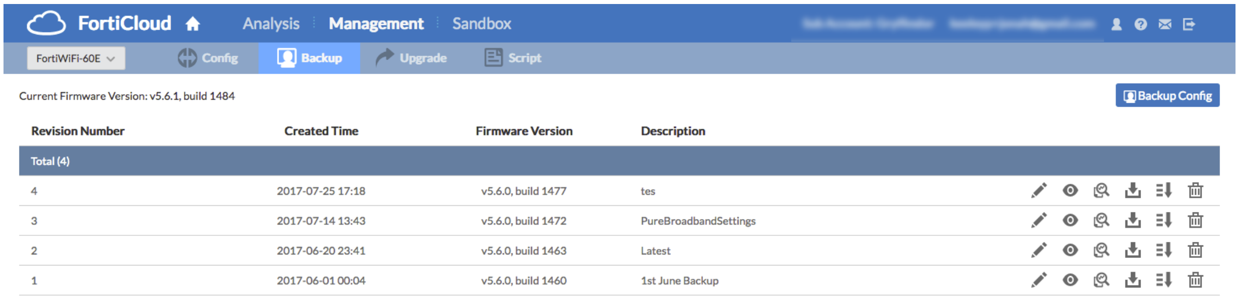
Config Firmware Version: v5.6.1, build 1484   Last Deployed: 2017-08-08 11:14 Successful   Disable Config Management

Name	Members	IP/Netmask	Role	Ref.
Physical (10)				
dmz		10.10.10.1/255.255.255.0	DMZ	0
internal1 (Not Used)		0.0.0.0/0.0.0.0	Undefined	0
internal2 (Kitchen AP)		172.16.101.1/255.255.255.0	LAN	3
internal3 (Hive)		192.168.250.1/255.255.255.0	LAN	2
internal4 (Alarm)		172.16.250.1/255.255.255.0	LAN	3
internal5 (FortiSwitch108D)		169.254.5.1/255.255.255.0	LAN	9
internal6 (Playroom)		172.16.100.1/255.255.255.0	LAN	1
internal7 (Kitchen Loop Monitor)		172.16.102.1/255.255.255.0	LAN	2
wan1 (Pure Broadband)		0.0.0.0/0.0.0.0	WAN	9
⊘ wan2		0.0.0.0/0.0.0.0	WAN	0
VLAN (6)				
FAZ-DMZ		172.20.20.1/255.255.255.0	DMZ	2
Home-VLAN		172.16.230.1/255.255.255.0	LAN	4
Internal_VPN		192.168.20.1/255.255.255.0	LAN	4
Voice-Network (Voice)		172.40.20.1/255.255.255.0	LAN	2
vsw.internal5		0.0.0.0/0.0.0.0	LAN	1
vsw.quarantine0		192.254.254.1/255.255.255.0	LAN	1

The **Config** page gives you access to a pared-down version of the remote device's management interface, allowing you to configure major features as if you were accessing the device itself.

The configuration you see in FortiGate Cloud is not auto-refreshing; you must select **Import** from the upper right to upload the local device's config to the FortiGate Cloud page. You can then make any changes you would like to reflect on the device, and select **Deploy** to push the configuration to the device.

Backup



Current Firmware Version: v5.6.1, build 1484

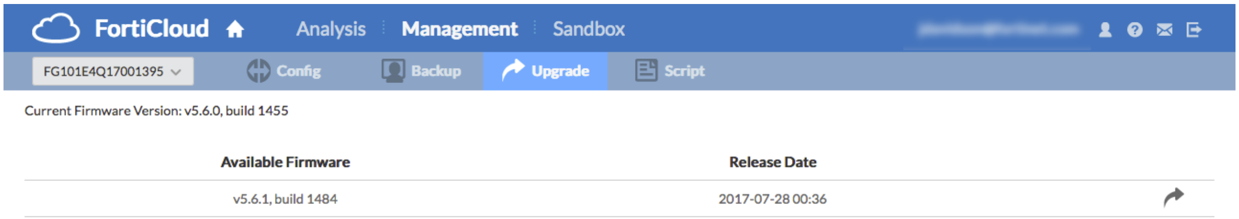
Revision Number	Created Time	Firmware Version	Description
Total (4)			
4	2017-07-25 17:18	v5.6.0, build 1477	tes
3	2017-07-14 13:43	v5.6.0, build 1472	PureBroadbandSettings
2	2017-06-20 23:41	v5.6.0, build 1463	Latest
1	2017-06-01 00:04	v5.6.0, build 1460	1st June Backup

The **Backup** page allows you to back up, track, and compare revisions of your remote device's configuration.

By selecting **Backup Config** in the upper right, you will save a backup to FortiGate Cloud.

The icons on the right allow you to **Edit**, **View**, **Compare** (to other revisions), **Download**, **Restore** (to device), and **Delete** revisions.

Upgrade

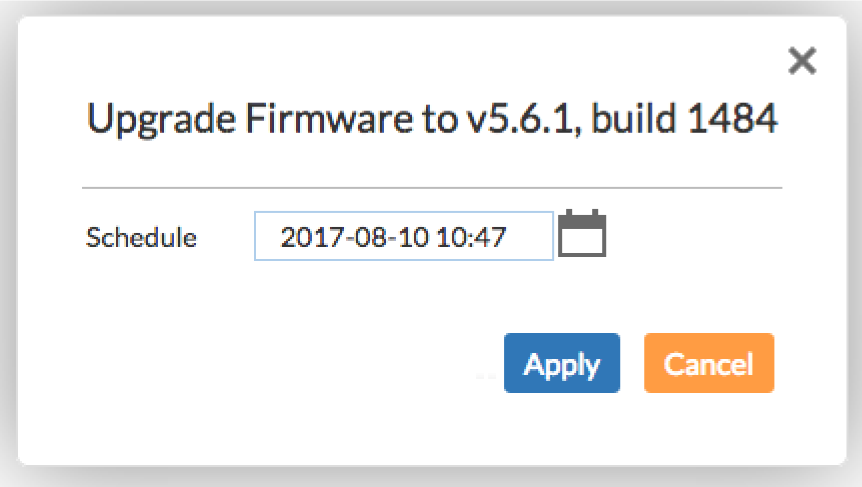


Current Firmware Version: v5.6.0, build 1455

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

The **Upgrade** page allows you to see the current firmware version installed on the device, and update to newer stable versions with one click, if they are available.

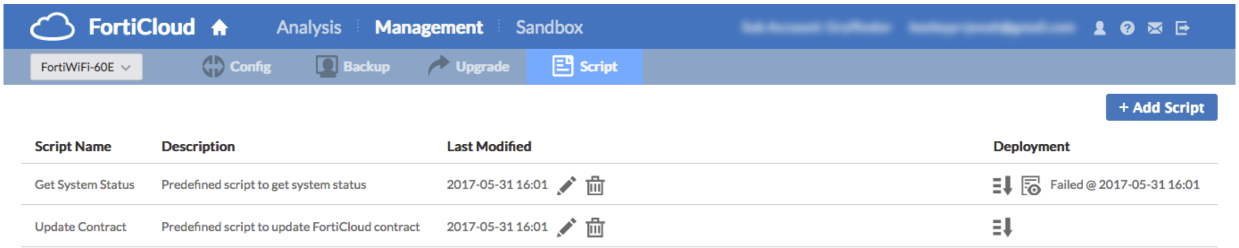
Select the **Upgrade** arrow on the right to upgrade. You can schedule a time and date to perform the remote upgrade, allowing you to schedule it during downtime to minimize disruption.



Upgrade Firmware to v5.6.1, build 1484

Schedule: 2017-08-10 10:47

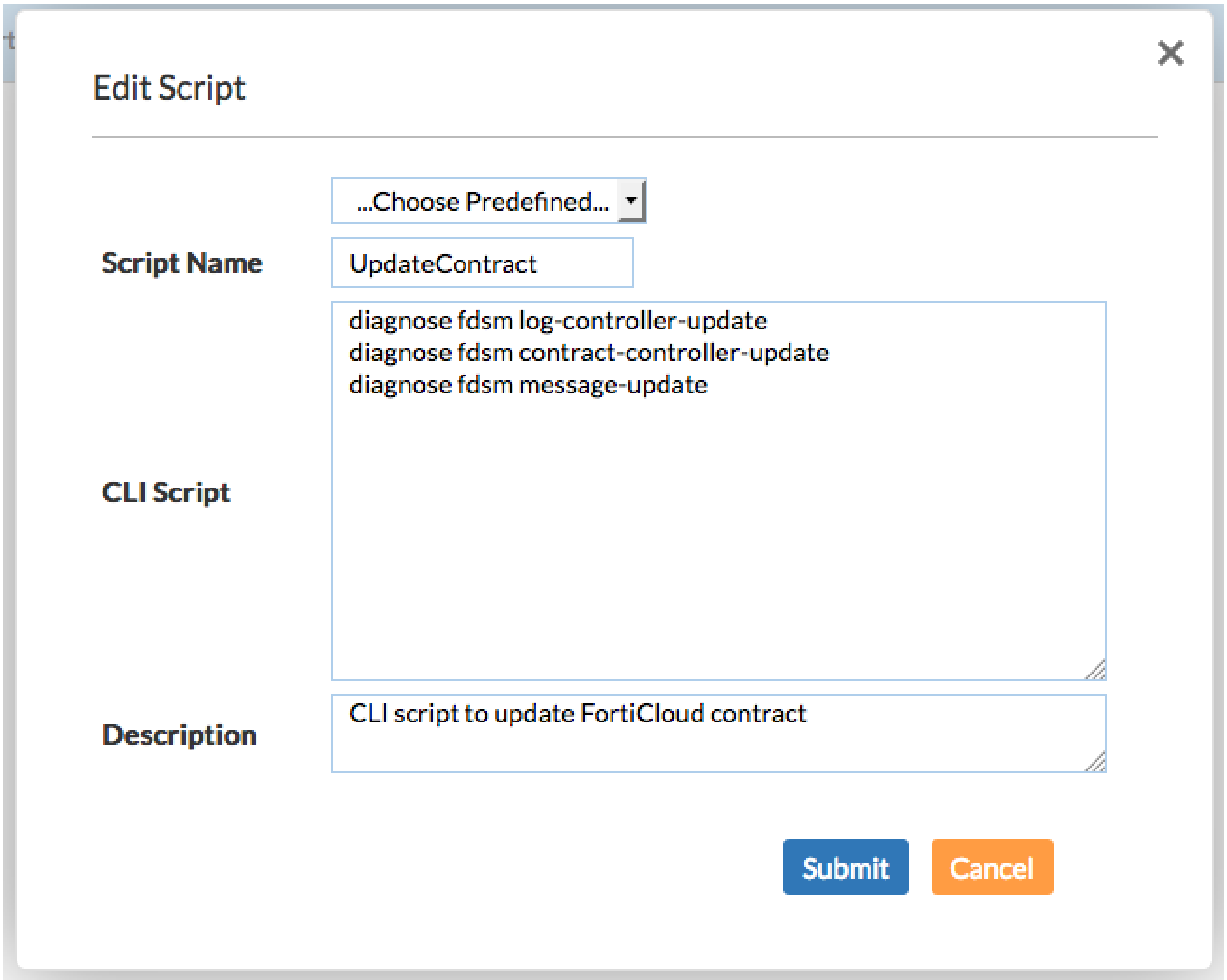
Script



Script Name	Description	Last Modified	Deployment
Get System Status	Predefined script to get system status	2017-05-31 16:01	Failed @ 2017-05-31 16:01
Update Contract	Predefined script to update FortiCloud contract	2017-05-31 16:01	

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

You can click the **Add Script** button to upload a script file, or select a Predefined script, and save it. Each script is a series of CLI commands, one command per line. You can then run it on the device selected in the upper left by selecting the **Deploy** icon on the right. You can also schedule deployment for a later date or time.



Edit Script

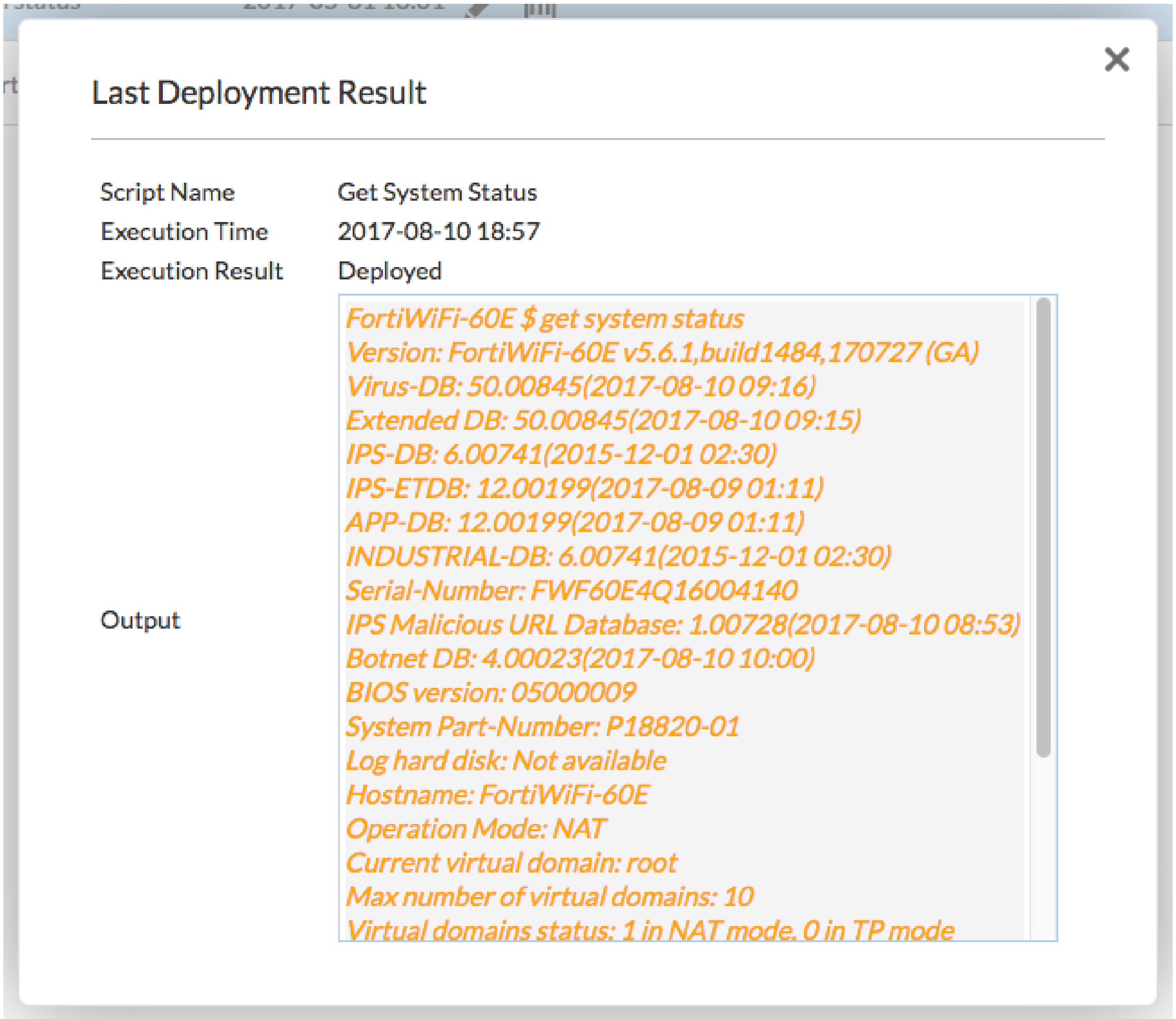
Script Name: UpdateContract

CLI Script:

```
diagnose fdsm log-controller-update
diagnose fdsm contract-controller-update
diagnose fdsm message-update
```

Description: CLI script to update FortiCloud contract

The output of that script will then be recorded, and can be read by clicking the **View Result** icon on the right.



Last Deployment Result

Script Name Get System Status

Execution Time 2017-08-10 18:57

Execution Result Deployed

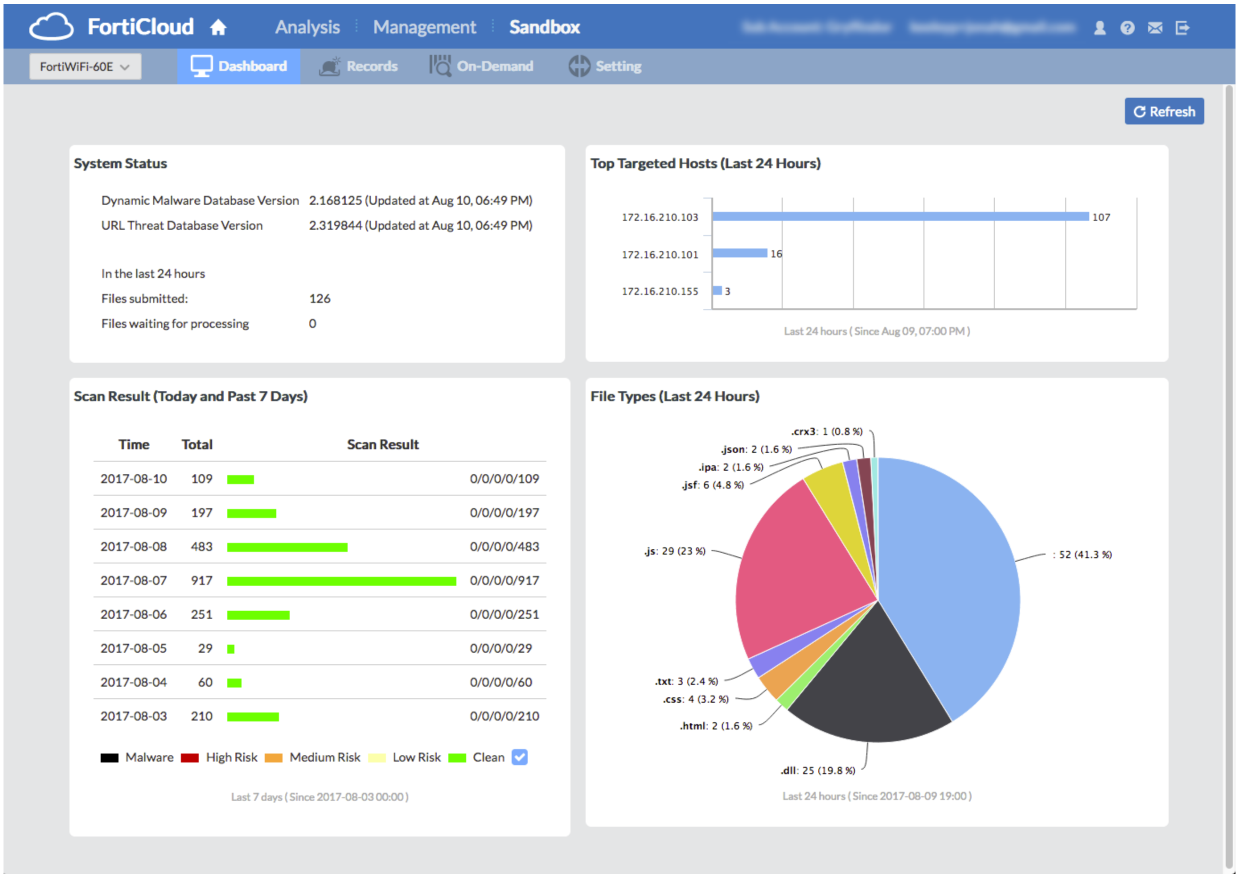
Output

```
FortiWiFi-60E $ get system status
Version: FortiWiFi-60E v5.6.1,build1484,170727 (GA)
Virus-DB: 50.00845(2017-08-10 09:16)
Extended DB: 50.00845(2017-08-10 09:15)
IPS-DB: 6.00741(2015-12-01 02:30)
IPS-ETDB: 12.00199(2017-08-09 01:11)
APP-DB: 12.00199(2017-08-09 01:11)
INDUSTRIAL-DB: 6.00741(2015-12-01 02:30)
Serial-Number: FWF60E4Q16004140
IPS Malicious URL Database: 1.00728(2017-08-10 08:53)
Botnet DB: 4.00023(2017-08-10 10:00)
BIOS version: 05000009
System Part-Number: P18820-01
Log hard disk: Not available
Hostname: FortiWiFi-60E
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
```

Sandbox pages

The **Sandbox** pages collect information compiled by the FortiSandbox Cloud service, which submits files to FortiGuard for threat analysis. They allow you to configure your use of the service, and view results of analyzed files.

Dashboard



System Status

Dynamic Malware Database Version 2.168125 (Updated at Aug 10, 06:49 PM)
URL Threat Database Version 2.319844 (Updated at Aug 10, 06:49 PM)

In the last 24 hours
Files submitted: 126
Files waiting for processing 0

Top Targeted Hosts (Last 24 Hours)
172.16.210.103
107
172.16.210.101
16
172.16.210.155
3
Last 24 hours (Since Aug 09, 07:00 PM)

Scan Result (Today and Past 7 Days)

Time	Total	Scan Result
2017-08-10	109	0/0/0/0/109
2017-08-09	197	0/0/0/0/197
2017-08-08	483	0/0/0/0/483
2017-08-07	917	0/0/0/0/917
2017-08-06	251	0/0/0/0/251
2017-08-05	29	0/0/0/0/29
2017-08-04	60	0/0/0/0/60
2017-08-03	210	0/0/0/0/210

■ Malware 🟥 High Risk 🟧 Medium Risk 🟨 Low Risk 🟩 Clean ☑

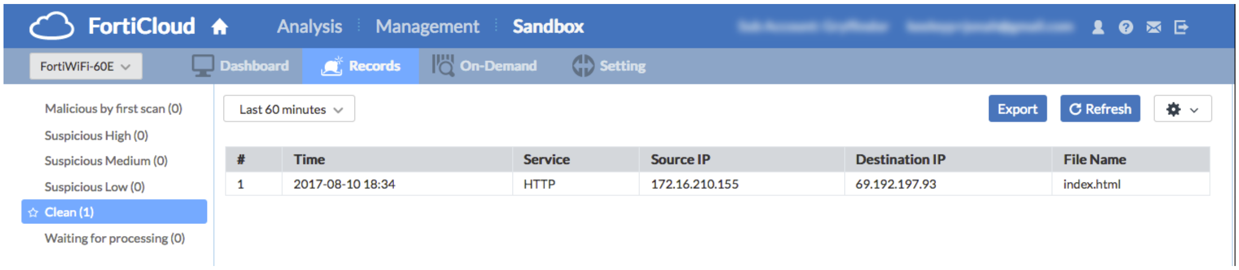
Last 7 days (Since 2017-08-03 00:00)

The **Dashboard** page gives you an overview of the FortiSandbox Cloud results.

The Dashboard contains the following widgets:

- **System Status** gives you a quick view of the current state of the AntiVirus databases and load.
- **Top Targeted Hosts** displays which hosts received the most threats.
- **Scan Result** shows the last 8 days of results and their risk levels (and you can toggle the display of Clean files in the chart by selecting the check mark in the lower right of the widget).
- **File Types** displays the most commonly analyzed file types in the last 24 hours of scanning.

Records / On-Demand



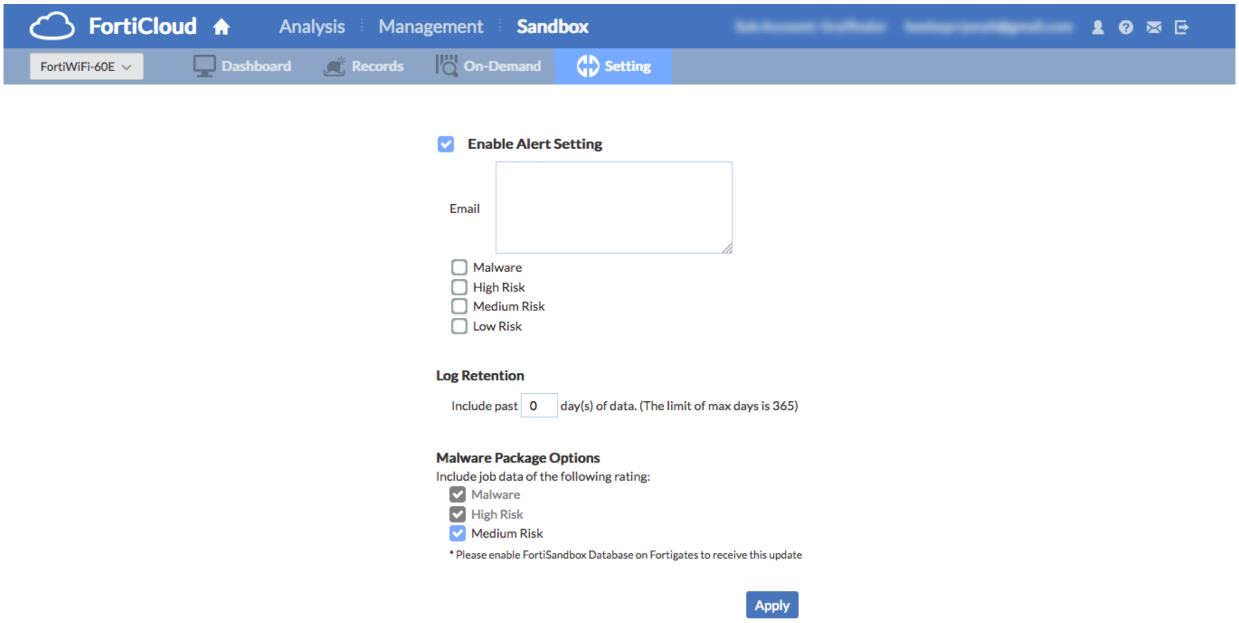
#	Time	Service	Source IP	Destination IP	File Name
1	2017-08-10 18:34	HTTP	172.16.210.155	69.192.197.93	index.html

The **Records** page displays files that have been flagged as suspicious by your connected device's AntiVirus, which have been uploaded to FortiCloud, to be analyzed by FortiGuard services. The **On-Demand** page allows you to manually upload files to FortiGuard services to be analyzed, and displays 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 on the left, and click on the file names for more information. The top right of the **On-Demand** page also has **Export**, which allows you to export a CSV or PDF of On-Demand results, and **Upload File**, where you can manually upload a file to be analyzed.

Maximum file size is 10Mb, and the processing time may vary based on the size of the file.

Setting



☑ Enable Alert Setting

Email

□ Malware
□ High Risk
□ Medium Risk
□ Low Risk

Log Retention

Include past 0 day(s) of data. (The limit of max days is 365)

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

The **Setting** page allows you to configure FortiSandbox Cloud settings:

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

Frequently asked questions

This section includes information about frequently asked questions concerning FortiGate Cloud.

General questions

This section includes the following general questions:

- What is FortiGate Cloud?
- What functions does FortiGate Cloud have?
- How does FortiGate Cloud work?
- How does FortiGate Cloud compare with FortiPortal and FortiAnalyzer?
- How do I confirm which version of FortiGate Cloud is currently in use?
- Which languages are supported by FortiGate Cloud?
- Can I choose which data center my logs are stored in?
- How can I provide feedback or request improvements to FortiGate Cloud?
- Is there a European FortiGate Cloud instance?
- If I am an existing customer in EMEA, will my data be transferred to the new data center, or will it remain in its current location?
- Is there an account designed for MSSP-scale operations?
- What are the new features in FortiCloud?
- General questions

What is FortiGate Cloud?

FortiGate Cloud is a hosted wireless and UTM infrastructure management solution and log retention service for FortiGate and FortiWiFi devices. It gives you centralized configuration management, location-based analytics and reporting, and log retention without the need for additional hardware and software. The feature set includes:

- One-touch provisioning of large scale security and wireless networks
- Configuration and device management from a single pane of glass
- Hosted log retention and cloud-based storage
- Wireless health and oversight at your fingertips
- Cloud management of wireless guest access
- Social media account login for Guest WiFi
- Rogue access point detection and analytics
- Built-in protection from APTs with FortiGuard sandboxing technology
- Location-based analytics with FortiPresence
- Instant security intelligence and analytics with FortiView
- Network health and utilization-based analytics and reporting
- Wireless configuration including security profiles per SSID for the Smart AP

What functions does FortiGate Cloud have?

- 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
- Report Generator: create custom report templates, and schedule reports in different formats to display location-based analytics or illustrate network usage patterns
- Device Management: configuration backup and history, script management, and alert profiles for real-time monitors
- AV Submission: shows the status of suspicious files undergoing cloud-based sandbox analysis
- Wireless Health Monitoring: bandwidth, usage, clients, interference, failed login and rogue APs
- Wireless Security Logs & Events: Authentication, Antivirus, IPS, Web Access, PCI compliance
- Wireless Configuration: SSIDs (including IPS, Antivirus and Web Filtering configuration), Authentication, Captive Portal, Platform Profiles, Tags and Network Settings
- Guest Management: ability to add guests and notify them if credentials via SMS or email
- Social Media Account Integration: ability for guests to connect to wireless accounts via social media

How does FortiGate Cloud work?

One or multiple devices are registered with FortiGate Cloud under a single account. This is done via the licensing widget in the device dashboard or at www.forticloud.com. The logs from each device are periodically sent to FortiGate Cloud and stored.

Logs are sent automatically to FortiGate Cloud for storage and processing. You configure what to log, including just traffic and event logs or including security logs such as antivirus, application control, IPS, etc.

From the recorded logs, reports can be generated to indicate trends within 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 can be used for backup and restore or to provision new devices. A VPN tunnel can be used to bring up the console of a device behind a firewall, allowing you to perform configuration or policy changes remotely.

How does FortiGate Cloud compare with FortiPortal and FortiAnalyzer?

FortiGate Cloud is an ideal solution for customers who do not want to implement a separate hardware solution such as a FortiAnalyzer device. However, it does not have all the features of a FortiAnalyzer. A high-level comparison is shown below:

Feature	FortiGate Cloud	FortiPortal	FortiAnalyzer
Business size	Small Branches/Large Campus/Distributed Enterprise	MSSP	Enterprise/MSSP

Feature	FortiGate Cloud	FortiPortal	FortiAnalyzer
Summary	Fortinet-hosted cloud-based reporting, management and client sandboxing	End customer/MSSP portal, overlaid on existing local infrastructure. Hosted in the MSSP's datacenter	Premises-based log collection, reporting and alerting system
Per-Site Licensing	Licensing is based on a per-device basis.	Licensing is based on number of devices and add-ons. Devices can be FG/VDOM/wireless. No limits on scaling factors, distributed architecture.	Typical licensing for FortiAnalyzer hardware. Max device limit set per model, VM and cloud-based options available.
Sandboxing	FortiSandbox Cloud included in AV bundle. FortiGate Cloud gives visibility in cloud to uploaded files.	No support in the current release. Must use FortiSandbox.	No support. Must use FortiSandbox.
Supports external authentication for administrative access	No	Yes	Yes
Storage quota	Unlimited storage with 1 year log retention.	Based on MSSP's datacenter storage availability.	Depends on model. Up to 48 TB for the appliance, and 24 TB for the VM.
Centralized logging	Real-time for disk-less models. Batch upload for disk models.	Real-time for security and wireless, analytics and reports.	Real-time for disk-less models. Batch upload for disk models. Log aggregation and forwarding. CEF compliant logging.
Aggregated reports	No	Yes	Yes

How do I confirm which version of FortiGate Cloud is currently in use?

Click on the FortiGate Cloud name in the title bar, or the About link to see the build/version number.

Which languages are supported by FortiGate Cloud?

FortiGate Cloud currently supports two languages: English and Japanese. These can be selected via the web portal login page. Other languages may be available in other regions.

Can I choose which data center my logs are stored in?

Yes. When you initially create your account in FortiGate Cloud, it will offer you a choice of data center to use. Data and accounts cannot be transferred between data centers, so migrating will require a new account.

How can I provide feedback or request improvements to FortiGate Cloud?

On the top right of every screen is an envelope icon, which will open a feedback submission form. Feedback is greatly appreciated, but Fortinet cannot guarantee individual responses to any requests.

Is there a European FortiGate Cloud instance?

Yes, the FortiGate Cloud service is available through our new Regional FortiGate Cloud Datacenter, geographically aimed at our European customer base, and is completely isolated from the North American instance.

All analysis, reporting, management and storage capabilities are provided locally, with full access to our global threat intelligence databases, with the dual benefit of isolating intercontinental data and providing performance improvements and lower latency to the end device.

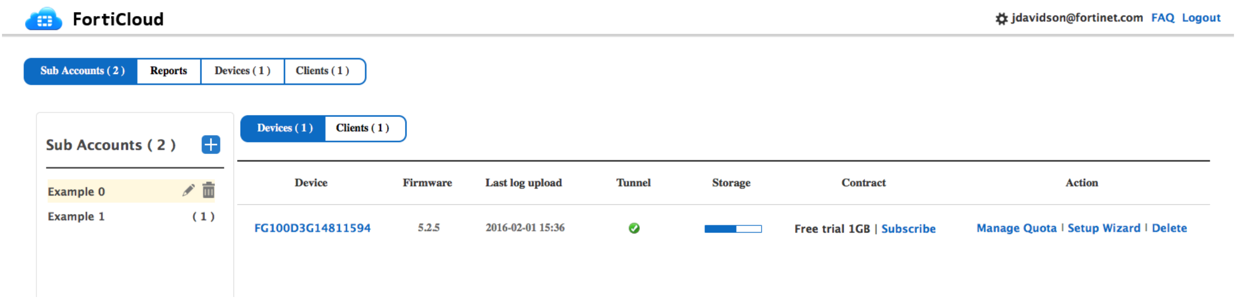
If I am an existing customer in EMEA, will my data be transferred to the new data center, or will it remain in its current location?

Any existing units will remain logging to their original destinations. If you wish to change this, please contact our Customer Services. No existing logs will be moved as part of this process.

Is there an account designed for MSSP-scale operations?

FortiGate Cloud has a premium account type, designed for Managed Security Service Providers: a Multi-Tenancy Account.

A Multi-Tenancy Account is a one-year service for an administrator to create and manage multiple sub-accounts. It also allows devices to be moved between these accounts. Each of the sub accounts can be allocated administrators, with full or read-only access, allowing you more control over the provision of a managed service.



Device	Firmware	Last log upload	Tunnel	Storage	Contract	Action
FG100D3G14811594	5.2.5	2016-02-01 15:36	✓		Free trial 1GB | Subscribe	Manage Quota | Setup Wizard | Delete

To activate a Multi-Tenancy Account, please request a quote for the following SKU through your Fortinet Partner or Reseller: **FCLE-10-FCLD0-161-02-DD**.

What are the new features in FortiCloud?

For information about new features in FortiCloud, refer to the Release Notes, found at the Documentation Library.

Licensing and registration

This section includes the following questions concerning licensing and registration:

- Is there an easy way to test drive FortiGate Cloud?
- What is the price of FortiGate Cloud?
- Do I need a support contract to enable the service?
- How do I subscribe to a FortiGate Analysis and Log Retention contract?
- What features do I get access to for subscribing?
- What happens if I lose my password?
- Can I use two-factor authentication for FortiGate Cloud?
- How do you configure the service once it is activated?
- How long are logs retained?
- When a device subscription lapses, what happens to the year's worth of logs?
- How can I unsubscribe from the service and stop uploading logs?

Is there an easy way to test drive FortiGate Cloud?

Yes, you can test drive FortiGate Cloud by visiting the www.forticloud.com, and selecting **Live Demo**. This will show a FortiGate Cloud account with populated devices and logs to simulate a live environment.

What is the price of FortiGate Cloud?

A no-charge service option is available with unlimited storage is available for one week.

There is also an annual-subscription-based service, with one, two, or three-year service terms. The new service provides 1 year of history, regardless of size. To activate FortiGate Cloud, you need to acquire a subscription license based on the following SKUs, available with 1, 2, and 3-year service terms:

Description	SKU
FortiGate Cloud Analysis and 1-Year Log Retention	
FortiGate & FortiWiFi	FC-10-00XXX-131-02-DD
FortiGate Cloud IOC (Indicator of Compromise)	

Description	SKU
FortiGate 20-90 models	FC-10-90803-142-02-12
FortiGate 100-300 models	FC-10-90804-142-02-12
Other Services	
FortiGate Cloud - Multi-Tenancy	FCLE-10-FCLD0-161-02-12
FortiDeploy Access	FDP-SINGLE-USE

Activation on device requires FortiOS 5.4.2 or newer. The Indicator of Compromise (IOC) Service requires an existing FortiGate Cloud subscription.

For pricing information, please contact your Fortinet partner or reseller.

Do I need a support contract to enable the service?

No, but you do need to register each device on the Fortinet Support website. It's very important to register each device in your network, or the service (free or subscribed) cannot be enabled.

How do I subscribe to a FortiGate Analysis and Log Retention contract?

To upgrade to a subscription, you need to:

1. Obtain a license (contract number) from your Fortinet reseller.
2. Click on the Upgrade icon in the FortiGate/FortiWiFi dashboard licensing widget.
3. Follow the instructions presented. If you are running FortiOS 5.0 and higher, you have the option of receiving a scratch-off card/certificate from your Fortinet reseller.
4. Scratch the card to reveal the hidden activation code. Enter this directly into the FortiGate console in the Licensing widget.
5. Wait about 30 minutes for the backend systems to process the subscription.
6. Check your FortiGate/FortiWiFi Dashboard, and the subscription will have changed from Free to Subscribed.

What features do I get access to for subscribing?

Yes. When you upgrade to a subscription, you will no longer have a daily limit on uploads and will be able to create, schedule, and customize reports. You will also be able to subscribe to more advanced features, like the FortiGate Cloud IOC (Indicator of Compromise) Service, FortiPresence Analytics, and FortiOS Management.

You also gain the ability to analyze more files per day with FortiSandbox Cloud (the free version limits you to 100 files per day.) The actual daily limit of files is based on the model of FortiGate deployed.

What happens if I lose my password?

You can reset your FortinetOne password by selecting **Forget Password?** on the login screen.

Can I use two-factor authentication for FortiGate Cloud?

Yes. As of 3.1, two-factor authentication is offered as part of the base free service, using the FortiToken app available on mobile devices. To enable two-factor authentication, ensure your entered email address is correct, as you will be sent an email withe setup instructions. Then enable **2-Factor** in the **My Account** section.

How do you configure the service once it is activated?

Logs will automatically start appearing in the logs and archives section of FortiGate Cloud. Select the gear icon on any page to edit that page's settings. Select the gear icon next to the administrator email in the top right to edit user settings.

How long are logs retained?

FortiGate Cloud will automatically delete logs older than the length of the support contract to make space for new log data. Email and pop-up reminders will be sent periodically (30 days, 14 days, 7 days, and 24 hours) before logs are deleted and before the contract term comes to an end.

When a device subscription lapses, what happens to the year's worth of logs?

Any logs that are associated with the licensed device older than 1 year will be automatically purged. For the free service, logs older than 7 days will be purged. There is no grace period, so please ensure you are properly renewed so that your logs are retained.

How can I unsubscribe from the service and stop uploading logs?

You can disconnect your account from the dashboard in your FortiGate/FortiWiFi. In the Licensing and Information widget in the FortiGate interface, click on the Log-out button. This will detach the FortiGate/FortiWiFi from the account and stop the logs from uploading.

Technical questions

This section includes the following technical questions:

- What security and redundancy has been built into the service?
- How do I verify my network is PCI compliant?
- Does my FortiGate require a hard drive to use FortiGate Cloud?
- Does FortiGate Cloud support devices from other vendors?
- Which FortiGate and FortiWiFi models does FortiGate Cloud support?
- Which versions of FortiOS does FortiGate Cloud support?
- What port numbers are used by FortiGate devices connecting to FortiGate Cloud?
- When are scheduled reports sent to administrators?

- Why can I not see any management functions?
- Can I set up high availability (HA) logging with FortiGate Cloud?
- Do I need to purchase a subscription for each FortiGate in an HA pair?

What security and redundancy has been built into the service?

Logs are transferred between devices and the FortiGate Cloud storage are transmitted via an encrypted link. All system elements are duplicated for redundancy.

How do I verify my network is PCI compliant?

FortiGate Cloud makes it easy to deploy, monitor and verify PCI compliance. FortiGate Cloud’s security feature set addresses PCI Data Security Standards 3.0, helping customers to build and maintain a secure network, protect cardholder data, maintain a vulnerability management program, implement strong control measures, and monitor network security.

Does my FortiGate require a hard drive to use FortiGate Cloud?

The FortiGate does not require a hard drive if logs are being uploaded to FortiGate Cloud in real-time, which can be enabled in the Log Setting page in the FortiGate interface. FortiGate Cloud is a convenient alternative to a hard drive for devices too small to contain one, such as FortiWiFi units.

Does FortiGate Cloud support devices from other vendors?

FortiGate Cloud only supports FortiGate and FortiWiFi. It does not currently support other company’s products for log retention.

Which FortiGate and FortiWiFi models does FortiGate Cloud support?

FortiGate

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.

FortiWiFi

All FortiWiFi models support FortiGate Cloud.

Which versions of FortiOS does FortiGate Cloud support?

FortiGate Cloud is available for all devices at FortiOS version 4.3 or later, but for full feature support, the most current available version should be deployed. Devices running FortiOS version 4.2 or earlier may not be able to access FortiGate Cloud. Consult your device’s documentation for more information.

What port numbers are used by FortiGate devices connecting to FortiGate Cloud?

Please note that these should be required by outbound traffic only. On request, we can supply the destination IP addresses to add to an outbound policy, if required.

Purpose	Protocol/Port
Syslog, Registration, Quarantine, Log & Report	TCP/443
OFTP	TCP/514
Management	TCP/541
Contract Validation	TCP/443

When are scheduled reports sent to administrators?

Scheduled reports are sent to administrator email addresses between 2 AM and 6 AM if automatic report delivery (Daily/Weekly/Monthly) is enabled.

Why can I not see any management functions?

You must first enable the management tunnel on the your device. On the device, use the following commands in the CLI:

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

Can I set up high availability (HA) logging with FortiGate Cloud?

FortiGate Cloud accepts inbound logs from each device independently, and has no means of detecting that connected devices are in an HA cluster. Though multiple HA clustered devices will theoretically send identical logs to FortiGate Cloud, if one device stops logging or is unable to reach FortiGate Cloud, the other devices will not send logs on its behalf.

Do I need to purchase a subscription for each FortiGate in an HA pair?

Yes. FortiGate Cloud handles each device separately, regardless of configuration.

FortiSandbox Cloud

This section includes the following questions concerning FortiSandbox Cloud:

- How does cloud sandboxing and AV submission work?
- Why can I not see a function or tab for AV Submission/Sandboxing?
- What is the turnaround time on Cloud Sandboxing and AV Submission?
- Is there a service description for FortiSandbox Cloud?

How does cloud sandboxing and AV submission work?

In a proxy-based antivirus profile on a FortiGate, the administrator selects **Send Files to FortiSandbox Cloud for Inspection** to enable a FortiGate unit to upload suspicious files to FortiGuard for analysis. Once uploaded, the file will be 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 antivirus signature database. The next time the FortiGate unit updates its antivirus database it will have the new signature.

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

The FortiCloud 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.

Why can I not see a function or tab for AV Submission/Sandboxing?

You must first enable Cloud Sandboxing on the FortiGate device, and then submit a suspicious file to cause the tab to appear.

What is the turnaround time on Cloud Sandboxing and AV Submission?

It can be anywhere from 10 minutes (for automated sandbox detection) to up to 10 hours (if FortiGuard Labs is involved).

Is there a service description for FortiSandbox Cloud?

Yes, a full current service description is available on the Fortinet Documentation Library.

Indicator of Compromise (IOC) Service

This section includes the following questions concerning the IOC service:

- What is the FortiGate Cloud Indicator of Compromise Service?
- What kind of threats can the IOC Service detect?
- How do I get access to the IOC Service?
- Does the IOC Service require a subscription?
- How do I register my subscription code once I've purchased one?

What is the FortiGate Cloud Indicator of Compromise Service?

FortiGate Cloud Indicator of Compromise (IOC) Service is a new service that alerts administrators about newly-found infections and threats to devices in their network. By analyzing UTM logging and activity, the service can provide a comprehensive overview of threats to the network.

What kind of threats can the IOC Service detect?

IOC can detect three types of threats, based on our evolving FortiGuard database:

- Malware: Malicious programs residing on infected endpoints.
- PUP: Potentially unwanted programs, such as spyware, adware, and toolbars.
- Unknown: Threats detected by signature but not associated with any known malware.

How do I get access to the IOC Service?

The free version of IOC is currently available on all accounts in the North America data center.

Non-Multi-Tenancy Account

In the FortiGate list, look for the label **Threats/Suspicious** underneath **System Status**, which will only appear if the FortiGate has detected any threats. Click on the text to open the IOC interface.

Multi-Tenancy Account

In the FortiGate list, look to the far right. A bomb icon will be visible next to the other configuration icons if your FortiGate has detected any threats. Select the bomb icon to open the IOC interface.

Does the IOC Service require a subscription?

The basic form of the IOC is free, which will alert you to threats and automatically prepare a comprehensive threat report. Threats listed will only provide partial IP addresses of infected devices: server and subnet.

You can purchase a subscription for the complete IOC by opening the **How to Buy** page in the FortiGate Cloud IOC site, and completing the purchase process.

A subscription grants you access to IP whitelisting, which allows you to narrow your malware search by excluding safe IP addresses and domains, and Alert Emails, which notify you directly of detected network threats. It will also allow you to view the full IP addresses of infected devices, allowing you to better control their access to your network.

How do I register my subscription code once I’ve purchased one?

You will receive your subscription code by email. Go to Fortinet Support and log into your customer account. On the Asset page, register the subscription code as if it were a product serial number, and then enter the serial number of the FortiGate Cloud-connected device that you want the service to monitor.

FortiDeploy

This section includes the following questions concerning FortiDeploy:

- What is FortiDeploy?
- How does FortiDeploy work?
- How do I purchase FortiDeploy?
- What is the price of FortiDeploy?
- What happens if you forget to order FortiDeploy on the PO?
- Will my FortiGuard and FortiCare services start automatically?
- What models are supported by FortiDeploy?
- Which versions of FortiOS does FortiDeploy support?
- Are there any complications if I’ve recently upgraded FortiOS?
- What if I am connected to FortiCloud but the device is not cloud-managed?
- What if a device is deployed behind a NAT device (such as a cable modem)?

What is FortiDeploy?

FortiDeploy is a product built into FortiCloud as a feature, for one-touch provisioning when devices are deployed, locally or remotely. FortiDeploy provides automatic connection of FortiGate and FortiWiFi devices to be managed by FortiCloud or a FortiManager unit.

How does FortiDeploy work?

When you enter a bulk FortiCloud Key in FortiGate Cloud, you will see a list of serial numbers from the order that contained the FortiDeploy SKU. Once you confirm that the devices are connected, you can perform some basic configuration on the devices remotely, such as sending a FortiManager IP to all remote FortiGate devices, so they can be managed remotely.

How do I purchase FortiDeploy?

At time of purchase, order a FortiDeploy SKU in addition to your other purchases, and enter it in FortiCloud. Once the FortiGate serial number is associated with your customer account, you have the option to deploy the devices in either FortiCloud or FortiManager. FortiDeploy can also push an IP to each FortiManager. Support starts the moment you send an email to cs@fortinet.com.

What is the price of FortiDeploy?

FortiDeploy must be purchased on every PO using FDP-SINGLE-USE SKU. The nominal fee is $100/PO.

What happens if you forget to order FortiDeploy on the PO?

If you forget to order FortiDeploy on the PO, please send an email to the Fortinet Customer Service and Support Team: cs@fortinet.com, and they can manually register your serial numbers and generate a Bulk FortiCloud Key.

Will my FortiGuard and FortiCare services start automatically?

No. FortiGuard and FortiCare services will start only after you register your serial numbers. Bulk registration of FortiGuard and FortiCare is available, but you will need to send a direct request after registration to cs@fortinet.com.

What models are supported by FortiDeploy?

- While FortiCloud supports all FortiGates up to the high-end models, FortiDeploy is only available up to the 200E, as we recommend that larger deployments be handled by trained personnel.
- All FortiWiFi models.

Which versions of FortiOS does FortiDeploy support?

FortiDeploy is available for FortiGate/FortiWiFi devices running FortiOS 5.2.2 or later.

Are there any complications if I’ve recently upgraded FortiOS?

From FortiOS 5.2.3 onward, the CLI command `auto-join-forticloud` is disabled by default and must be enabled for FortiDeploy to function correctly. If you upgrade from 5.0.x to 5.2.2 or later, you must also enable this function.

You can enable this function using the following command:

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

After changing this setting, restart the device and ensure that traffic is being sent to FortiCloud to verify that it has been configured correctly.

What if I am connected to FortiCloud but the device is not cloud-managed?

Double-check that central management is set to FortiGuard. You can enable central management using the following command:

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

Reboot the device, login to FortiCloud and try to manage the device.

What if a device is deployed behind a NAT device (such as a cable modem)?

The default IP address of the **internal** or **lan** interface is the 192.168.1.0/24 subnet. IP conflicts can occur with FortiDeploy-managed devices. The solution is to unset the default IP for each of the devices in the CLI console:

```
config system interface
   edit internal (or lan, depending on the model)
      unset ip
   end
end
```

You can also change the internal interface's IP in the web-based management interface by going to **Network > Interfaces**.

FortiGate Cloud Cookbook

This series of short tutorials will show you how to enable and set up various FortiGate Cloud services and features.

Basic configuration

FortiGate Cloud has many features available, depending on the size of your network and your interest in monitoring and management. First, devices must be added to the service.

Basic FortiGate Cloud setup

1. Register the FortiGate/FortiWiFi on the Fortinet Support website.
2. Create a FortiGate Cloud account in the FortiGate/FortiWiFi dashboard licensing widget.
3. Activate the FortiGate/FortiWiFi within the dashboard licensing widget.
4. Create a firewall policy with logging enabled. Configure log uploading, if necessary.
5. Log in to FortiGate Cloud using your FortinetOne account.

FortiSandbox Cloud setup

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

Indicator of Compromise (IOC) setup

The basic form of IOC is free and functions for all of your FortiGate Cloud-connected devices. In order to purchase the complete form of IOC, follow the instructions below.

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.

5. The service will automatically take effect.

FortiGate Cloud device configuration

Whether you are creating a FortiGate Cloud AP Network, or just monitoring multiple devices, you can use a variety of features to remotely manage and configure your networked devices.

Deploying cloud configuration to devices

1. Go to **Management > Config**.
2. Before you edit any settings, select **Import** in the upper right to retrieve the most up-to-date configuration from the FortiGate Cloud-connected device.
3. On this page, you have limited access to an analogue 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 will appear, showing you the changes as they appear in the CLI.

Device configuration backup to cloud

1. Go to **Management > Backup**.
2. Select **Backup Config** in the upper right, and enter a name for the backup revision.
3. The new configuration will be added 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 will only appear once you have multiple revisions available.

Remote device firmware upgrade

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 make sure you are following the recommended upgrade path.
4. We also recommend that you back up your device's configuration before upgrading, either in **Management > Backup** or in the device's management interface.
5. Select an Available Firmware from the list that you would like to upgrade the device to, and select **Upgrade**.
6. Wait for the upgrade to take effect.

Remote device script execution

The Script deployment functionality allows you to upload scripts and run them as needed on a schedule basis.

1. Go to **Management > Script**.
2. In the upper right, select **Add Script**.
3. Enter a name and a description, and the content of the CLI script that you want to run. Save the script.
4. On the right, select **Schedule Deployment** icon, and select a time that you'd like the script to be automatically deployed to the device.
5. If you need to cancel the scheduled run, select the blue arrow next to the scheduled time.

Advanced configuration

Some features of FortiGate Cloud are more useful for larger/more distributed networks: more refined oversight, multiple administrators, multiple regions, or other complex setups.

Adding 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 email address and name of the new user/admin.
4. Select whether they are an Admin (total control over the FortiGate Cloud interface) or a User (limited control, monitoring only).
5. Select **Submit**. They will receive an email prompting them to set their account password, and log in.

Creating custom FortiGate Cloud reports

1. Go to **Analysis > Reports**.
2. Select Add in the upper right, and choose whether to create a new report, edit an existing template, or import an external template.
3. Select the gear icon on the right side to add **Charts and Headers** to the current section, or new 1- or 2-column sections.
4. Edit charts by selecting the pencil icon in the upper right of each chart, and selecting a predefined chart style or setting the axis variables manually.
5. When you're finished, select **Save** in the upper right.
6. Select **Run**, and view the finished report.

Configuring FortiSandbox alert emails

1. Go to **Sandbox > Setting**.
2. Select **Enable Alert Setting**.

3. Enter emails into the list that should be contacted in the event of a FortiSandbox Alert.
4. Select the levels of severity that will trigger an Alert.

Multi-Tenancy configuration

A Multi-Tenancy account is a subscription account that allows you to create and manage multiple sub-accounts that are functionally isolated from each other. Devices can be added to and moved between these sub-accounts, and each account can have its own administrators and user s.

Activating Multi-Tenancy feature

1. Contact your Fortinet Partner or Reseller, requesting the following SKU: FCLE-10-FCLD0-161-02-DD.
2. You will receive a Multi-Tenancy activation code from them by email.
3. Open the FortiGate Cloud interface, and select the **My Account** icon in the upper right.
4. Under the admin/user list, select **Activate Multi-Tenancy Feature**.
5. Enter the Activation Code, and **Submit**.

Basic Multi-Tenancy configuration

Once Multi-Tenancy has been activated, the default FortiGate Cloud Home page will be replaced with the Multi-Tenancy page, which has 'FortiGate', 'AP Network', and 'Inventory' at the top.

1. Open the **Inventory** page, and select **Import Key** from the upper right, either **FGT**, **AP**, or **Bulk** if you want to add multiple FortiGate Cloud licenses at once.
2. Import all the devices and/or licenses you like. They will be listed under **FortiGate Inventory**, and **AP Inventory**.
3. On an Inventory subpage, select a device, and select **Deploy** in the upper right to assign it a license. It will be automatically moved to the **Deployed FortiGates**/**APs** subpage.
4. Select either **FortiGate** or **AP Network** from the top, and select a device to individually configure it further.