



FortiAnalyzer - Cookbook

Version 5.4.0

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: techdoc@fortinet.com



May 06, 2019

FortiAnalyzer 5.4.0 Cookbook

05-540-556125-20190506

TABLE OF CONTENTS

Change Log	4
Introduction	5
FortiAnalyzer recipes	5
FortiAnalyzer Analyzer-Collector configuration	5
Setting up the Collector	6
Setting up the Analyzer	8
Results	10
Adding FortiAnalyzer to the Security Fabric	10
Connecting the External FortiGate and the FortiAnalyzer	11
Configuring OSPF routing to the FortiAnalyzer	12
Allowing internal FortiGates to access the FortiAnalyzer	12
Sending log information to the FortiAnalyzer	13
Review Results	14
Log data migration from an old to new FortiAnalyzer	14
Migrating prerequisites	15
Setting up the aggregation client	15
Setting up the aggregation server	15
Running aggregation in the client CLI	16
Checking the aggregation progress on the client	16
Rebuilding the database	16
Debugging log aggregation	16
Replacing FortiGate HA pairs with logging enabled	16
Replacing the primary unit	17

Change Log

Date	Change Description
2019-05-06	Initial release.

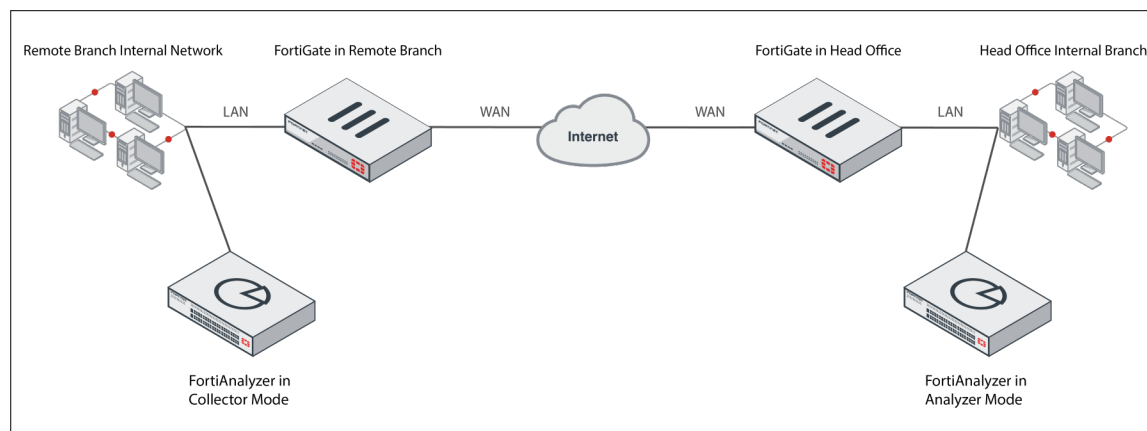
Introduction

FortiAnalyzer units securely aggregate log data from Fortinet security appliances, allowing you to quickly analyze and visualize network threats, inefficiencies, and usage. FortiAnalyzer is one of several versatile Fortinet Management Products that provide a diversity of deployment types, growth flexibility, advanced customization through APIs, and simple licensing.

FortiAnalyzer recipes

- [FortiAnalyzer Analyzer-Collector configuration on page 5](#)
- [Adding FortiAnalyzer to the Security Fabric on page 10](#)
- [Log data migration from an old to new FortiAnalyzer on page 14](#)
- [Replacing FortiGate HA pairs with logging enabled on page 16](#)

FortiAnalyzer Analyzer-Collector configuration



This example illustrates how to set up FortiAnalyzer *Analyzer* and *Collector* modes and make them work together to increase the overall performance of log receiving, analysis, and reporting.

FortiAnalyzer provides two operation modes: *Analyzer* and *Collector*. Analyzer mode is the default mode that supports the full FortiAnalyzer features, while the primary task of a Collector is receiving logs from connected devices and uploading the logs to an Analyzer. Instead of writing logs to the database, the Collector retains the logs in their original (binary) format and sends the logs to the Analyzer. The following table shows a comparison of the supported features of the Analyzer and Collector modes.

FortiAnalyzer Feature	Analyzer Mode	Collector Mode
FortiView	Yes	No
Event Monitor	Yes	No

FortiAnalyzer Feature	Analyzer Mode	Collector Mode
Reports	Yes	No
Log View	Yes	Compressed logs only; indexed logs not available.
Device Manager	Yes	Yes
System Settings	Yes	Yes

In this example, Company A has a branch network with a FortiGate and a FortiAnalyzer 400E deployed in Collector mode. In its head office, Company A has another FortiGate and FortiAnalyzer 3000D deployed in Analyzer mode. Collector mode forwards the FortiGate logs in the remote branch to the Analyzer in the head office for data analysis and report generation. The Collector will also be used to archive logs.

Setting up the Collector

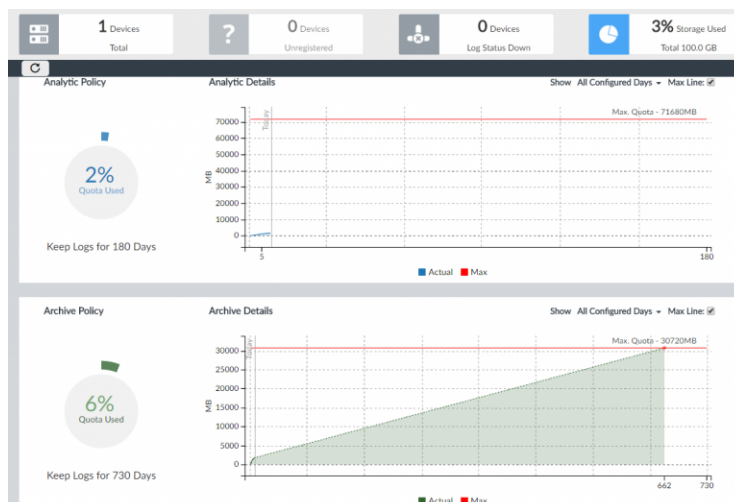
To set up the Collector:

- Configure the operation mode.
 - Go to *System Settings > Dashboard*.
 - In the *System Information* widget, select *Collector* as the *Operation Mode*.

System Information 🔄 ✕

Host Name	FAZ400E	✎
Serial Number	FL-4HE3R15900006	
System Time	Sat Apr 09 14:47:42 PDT 2016	✎
Firmware Version	v5.4.0-build1024 160324 (Interim)	⬆
System Configuration	N/A	📄 📄
Current Administrators	admin /1 in total	👤
Up Time	7 days 23 hours 57 minutes 13 seconds	
Administrative Domain	<input checked="" type="checkbox"/> ON	
Operation Mode	<div> <div>Analyzer</div> <div>Collector</div> </div>	

- Go to *Device Manager* and click the *Storage Used* tab in the quick status bar to check the storage policy of the Collector.



3. Configure the storage policy of the Collector.

- To edit the date policy when ADOMs are enabled:
 - i. Go to *System Settings > All ADOMs*.
 - ii. Double click the ADOM your Analyzer/Collector belongs to.
 - iii. On the *Edit ADOM Storage Configurations* page, edit the log storage policy.
- To edit the storage settings when ADOMs are disabled:
 - i. Go to *System Settings > Dashboards*.
 - ii. In the *System Information widget*, click the *edit* icon for *Log Storage Policy*. In the *Edit Log Storage Policy* dialog box, change the settings.

4. You can use the default admin account of the Analyzer or create a custom administrator account on the Analyzer. The Collector will need to provide the login credentials of this administrator account to get authenticated by the Analyzer for log aggregation.



For the Collector, you should allocate most of the disk space for *compressed* logs. You should keep the compressed logs long enough to meet the regulatory requirements of your organization. After this initial configuration, you can monitor the storage usage and adjust it as you go.

To configure log forwarding:

1. On the Collector, go to *System Settings > Log Forwarding*. Click *Create New*.
2. Set the following settings:
 - Set *Server Name* to a name you prefer.
 - Set *Remote Server Type* to FortiAnalyzer.
 - Set *Server IP* to the IP address of the Analyzer to which this Collector will forward logs.
 - Click *Select Device* and select the FortiGate device of the branch office.
 - Select both *Enable Real-time Forwarding* and *Enable Log Aggregation*.
 - Provide the username and password of the Administrator account of the Analyzer.

3. Click OK.

Create New Log Forwarding

Server Name

Head Office

Remote Server Type

☒ FortiAnalyzer
 ☐ Syslog
 ☐ Comment Event Format(CEF)

Server IP

192.168.1.99

Devices

All FortiGates

Select Device +

☒ Enable Real-time Forwarding

Server Port

514

Enable Filters

☐

☒ Enable Log Aggregation

User

admin

Password

Upload daily at

22:00



We recommend that you enable real-time forwarding to optimize performance. If you want the Collector to upload content files, which include DLP (data leak prevention) files, antivirus quarantine files, and IPS (intrusion prevention system) packet captures, you should also enable Log Aggregation so the Collector will send content files to the Analyzer at a scheduled time.



Log forwarding is enabled by default. If you cannot see *System Settings > Log Forwarding* in the GUI, you will have to enable it first. Go to *System Settings > Dashboard*. In the CLI Console widget, enter the following CLI commands:

```
config system admin setting
    set show-log-forwarding enable
end
```

Setting up the Analyzer

To set up the Analyzer:

- Configure the operation mode.
 - Go to *System Settings > Dashboard*.
 - In the *System Information* widget, select *Analyzer* as the *Operation Mode*.

System Information

Host Name

FAZ3000D

Serial Number

FL-3KD3R13000001

System Time

Sat Apr 09 14:36:03 PDT 2016

Firmware Version

v5.4.0-build1024 160324 (Interim)

System Configuration

Thu Mar 17 12:00:27 2016

Current Administrators

admin /1 in total

Up Time

12 days 2 hours 30 minutes 36 seconds

Administrative Domain

ON

Operation Mode

Analyzer

Collector

- Go to *Device Manager* and click the *Storage Used* tab in the quick status bar to check the storage policy of the Analyzer.

3. Configure the storage policy of the Analyzer using the corresponding instructions above for the Collector.



For the Analyzer, you should allocate most of the disk space for *indexed* logs. You may want to keep the indexed logs for 30-90 days. After this initial configuration, you can monitor the storage usage and adjust it as you go.

4. Add the branch office FortiGate to the Analyzer.

- a. Go to *Device Manager* and click *Unregistered Device* in the quick status bar.

Device Name	Model	Serial Number	Connecting IP
310b-ha	FortiGate-310B	FG300B3908604043	192.168.125.1
FG100D3G00000011	FortiGate-100D	FG100D3G00000011	192.168.125.1
FG100D3G00000012	FortiGate-100D	FG100D3G00000012	192.168.125.1
FGT-VM-50	FortiGate-VM	FGVM020000040131	10.2.125.61
<input checked="" type="checkbox"/> FGT92D3G14001099	FortiGate-92D	FGT92D3G14001099	192.168.125.1
FGVM020000042041	FortiGate-VM	FGVM020000042041	10.2.125.60
FW80CM3914602656	FortiWiFi-80CM	FW80CM3914602656	10.2.125.31

- b. Select the FortiGate device, and click *Add*.
- c. In the *Add Device* dialog box, select the ADOM you want to add to the FortiGate device (if ADOM is disabled, select root), and give the device a name. Once the FortiGate device is added, you can see it under the *Device Total* tab.

Add Device

Device Name	Assign New Device Name
FGT92D3G14001099	Branch_FGT

5. Make sure that the log aggregation service is enabled on the Analyzer.

- a. Go to *System Settings > Dashboard*.
- b. In the CLI Console widget, enter the following commands:

```
config system aggregation-service
    set accept-aggregation enable
end
```

6. Make sure the Analyzer interface receiving the logs allows aggregator access.
 - a. Go to *System Settings > Network*.
 - b. In the *System Network Management Interface* pane, select *Aggregator* under *Administrator Access*.

System Network Management Interface

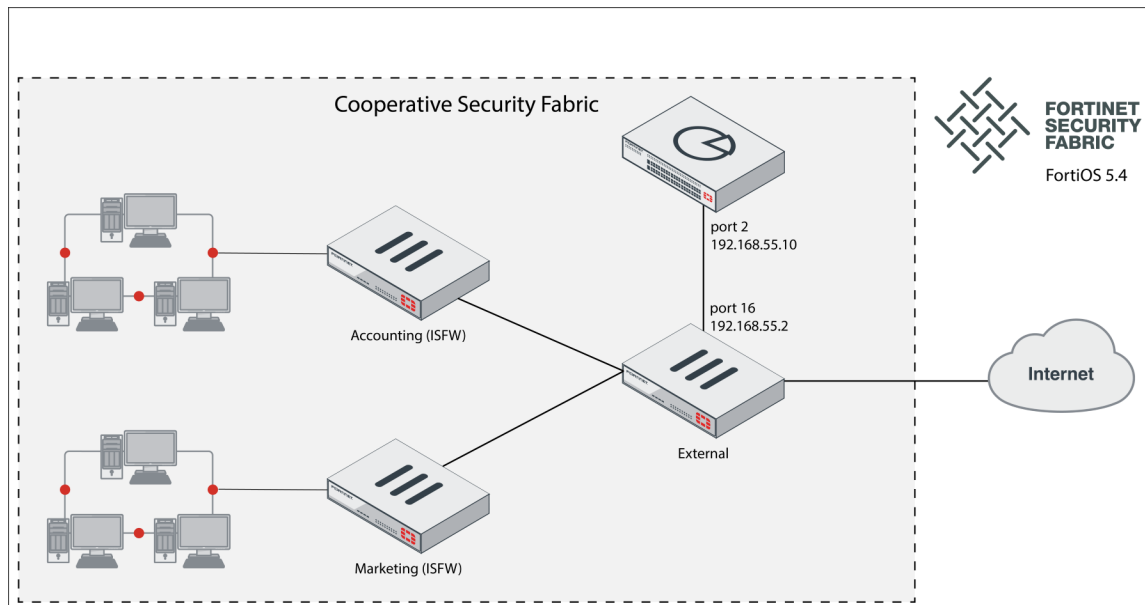
Name	port1
IP Address/Netmask	192.168.1.99/255.255.255.0
IPv6 Address	::/0
Administrative Access	<input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> HTTP <input checked="" type="checkbox"/> PING <input checked="" type="checkbox"/> SSH <input checked="" type="checkbox"/> TELNET <input checked="" type="checkbox"/> SNMP <input checked="" type="checkbox"/> Web Service <input checked="" type="checkbox"/> Aggregator <input type="checkbox"/> FortiManager
IPv6 Administrative Access	<input type="checkbox"/> HTTPS <input type="checkbox"/> HTTP <input type="checkbox"/> PING <input type="checkbox"/> SSH <input type="checkbox"/> TELNET <input type="checkbox"/> SNMP <input type="checkbox"/> Web Service <input type="checkbox"/> Aggregator <input type="checkbox"/> FortiManager
Default Gateway	192.168.1.1
Primary DNS Server	208.91.112.53
Secondary DNS Server	208.91.112.63

Apply

Results

At this point, the Collector will start to forward logs to the Analyzer. Log in to the Analyzer GUI and go to *Log View*. Select the branch office FortiGate device from the device list, and select *Real-time Log* from the *Tools* dropdown. You will see real-time logs arriving from the branch office FortiGate.

Adding FortiAnalyzer to the Security Fabric



In this recipe, you will add a FortiAnalyzer to a network that is already configured as a Cooperative Security Fabric (CSF). This will simplify network logging by storing and displaying all log information in one place.

In this example, a FortiGate called *External* is the upstream FortiGate. There are also two ISFWs, called *Accounting* and *Marketing*. OSPF routing is used between the FortiGates in the CSF.

To add FortiAnalyzer to the Security Fabric:

1. Connect the *External* FortiGate and the FortiAnalyzer.
2. Configure OSPF routing to the FortiAnalyzer.
3. Allow internal FortiGates to access the FortiAnalyzer.
4. Send log information to the FortiAnalyzer.
5. Review results.

Connecting the *External* FortiGate and the FortiAnalyzer

In this example, the *External* FortiGate's port 16 will connect to port 2 on the FortiAnalyzer.

To connect the External FortiGate and FortiAnalyzer:

1. On the *External* FortiGate, go to *Network > Interfaces* and edit *port 16*.
2. Set an IP/Network Mask for the interface (in the example, 192.168.55.2).

Interface Name: port16 (90:6C:AC:45:6C:6A)

Alias: FortiAnalyzer

Link Status: Up

Type: Physical Interface

Role: DMZ

Address

Addressing mode: Manual DHCP One-Arm Sniffer Dedicated to FortiSwitch

IP/Network Mask: 192.168.55.2/255.255.255.0

Restrict Access

Administrative Access: ☐ HTTPS ☒ PING ☐ FMG-Access ☐ CAPWAP ☒ SSH ☐ SNMP ☐ RADIUS Accounting ☒ FortiTelemetry

3. Configure *Administrative Access* to allow FortiTelemetry, required for communication between devices in the CSF. Configure other services as required.
4. On the FortiAnalyzer, go to *System Settings > Network*, select *All Interfaces*, and edit *port2*.
5. Set IP/Netmask to an internal IP (in the example, 192.168.55.10/255.255.255.0).

Name: port2

Alias:

IP Address/Netmask: 192.168.55.10/255.255.255.0

IPv6 Address: ::/0

Administrative Access: ☒ HTTPS ☒ HTTP ☒ PING ☒ SSH ☐ TELNET ☐ SNMP ☐ Web Service ☐ FortiManager

IPv6 Administrative Access: ☐ HTTPS ☐ HTTP ☐ PING ☐ SSH ☐ TELNET ☐ SNMP ☐ Web Service ☐ FortiManager

Service Access: ☒ FortiGate Updates

Status: Enable Disable

6. Connect the *External* FortiGate and the FortiAnalyzer. On the FortiAnalyzer, go to *System Settings > Network*. Port 2 is now shown as the management interface.

7. Add a *Default Gateway*, using the IP address of the External FortiGate's port 16.

Name	port2
IP Address/Netmask	192.168.55.10/255.255.255.0
IPv6 Address	::/0
Administrative Access	<input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> HTTP <input checked="" type="checkbox"/> PING <input checked="" type="checkbox"/> SSH <input type="checkbox"/> TELNET <input type="checkbox"/> SNMP <input type="checkbox"/> Web Service <input type="checkbox"/> FortiManager
IPv6 Administrative Access	<input type="checkbox"/> HTTPS <input type="checkbox"/> HTTP <input type="checkbox"/> PING <input type="checkbox"/> SSH <input type="checkbox"/> TELNET <input type="checkbox"/> SNMP <input type="checkbox"/> Web Service <input type="checkbox"/> FortiManager
Default Gateway	192.168.55.2

Configuring OSPF routing to the FortiAnalyzer

To configure OSPF routing to the FortiAnalyzer:

1. On the *External* FortiGate, go to *Network > OSPF*.
2. Click *Create New* to create a new network.
3. Set *IP/Netmask* to 192.168.55.0/255.255.255.0 (the subnet that includes FortiAnalyzer's port 2) and *Area* to 0.0.0.0.

Networks		
Create New	Edit	Delete
	Network	Area
<input type="checkbox"/>	192.168.10.0/255.255.255.0	0.0.0.0
<input type="checkbox"/>	192.168.200.0/255.255.255.0	0.0.0.0
<input type="checkbox"/>	192.168.55.0/255.255.255.0	0.0.0.0

Allowing internal FortiGates to access the FortiAnalyzer

To allow internal FortiGates to access the FortiAnalyzer:

1. On the *External* FortiGate, go to *System > Feature Select*.
2. Under *Additional Features*, select *Multiple Interface Policies*.

☒ Multiple Interface Policies [+](#)

3. Go to *Policy & Objects > IPv4 Policy* and create a policy allowing the internal FortiGates (*Accounting* and *Marketing*) to access the FortiAnalyzer.
4. Do *not* enable NAT.

Name	FortiAnalyzer-access
Incoming Interface	<input checked="" type="checkbox"/> Accounting (port10) <input checked="" type="checkbox"/> Marketing (port11) <input checked="" type="checkbox"/>
Outgoing Interface	<input checked="" type="checkbox"/> FortiAnalyzer (port16) <input checked="" type="checkbox"/>
Source	<input checked="" type="checkbox"/> all <input checked="" type="checkbox"/>
Destination Address	<input checked="" type="checkbox"/> all <input checked="" type="checkbox"/>
Schedule	<input checked="" type="checkbox"/> always
Service	<input checked="" type="checkbox"/> ALL <input checked="" type="checkbox"/>
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> LEARN

Firewall / Network Options

NAT ☐

Sending log information to the FortiAnalyzer

To send log information to the FortiAnalyzer:

1. On the FortiAnalyzer, go to *Device Manager* and add a device.
2. Enter all information about the *External* FortiGate, then select *Next*.
The FortiAnalyzer will now add the device, and the *External* FortiGate will be listed on the FortiAnalyzer.

Add Device

Please input the following information to add a device.

IP Address	<input type="text" value="192.168.55.2"/>
SN	<input type="text" value="FGT6HD3916800525"/>
Device Name	<input type="text" value="External"/>
Device Model	<input type="text" value="FortiGate-600D"/>
Firmware Version	<input type="text" value="5.4"/>
Description	<input type="text" value="Upstream FortiGate in CSF"/>

3. On the *External* FortiGate, go to *Log & Report Settings*. Under *Remote Logging and Archiving*, enable *Send Logs to FortiAnalyzer/FortiManager*.

Remote Logging and Archiving

Send Logs to FortiAnalyzer/FortiManager ☒

IP Address

Upload Option

Encrypt Log Transmission ☐

4. Enter the IP Address of the FortiAnalyzer.
In the example image above, logs are set to be uploaded in *Realtime* because there is no bandwidth limitations. Also, since log traffic is occurring within the CSF, encryption is not enabled.
5. Select *Test Connectivity* to view information about the connection.

FortiAnalyzer(Hostname)	FortiGate(Device ID)	Registration Status	Connection Status
FAZ400E	FGT6HD3916800525	Registered	✓

Allocated Space	Used Space	Total Free Space
Unlimited	0	5630624

Privileges							
Log		DLP Archive		Quarantine		IPS	
Traffic Out	Traffic In	Traffic Out	Traffic In	Traffic Out	Traffic In	Traffic Out	Traffic In
✓	✓	✓	✓	✓	✓	✓	✓

6. Under *GUI Preferences*, select *Display Logs From FortiAnalyzer*.

GUI Preferences

Display Logs From

Resolve Hostnames ☒

Resolve Unknown Applications ☒

7. Repeat this process on both the *Accounting* and *Marketing* FortiGates.

Review Results

- All three FortiGates are listed in the FortiAnalyzer's *Device Manager*.

<input type="checkbox"/>	▲ Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)	Device Storage	Description
<input type="checkbox"/>	Accounting	192.168.10.10	FortiGate-140D	Real Time	0	0.04%	FortiGate for Accounting Department.
<input type="checkbox"/>	External	192.168.55.2	FortiGate-600D	Real Time	0	0.52%	Upstream FortiGate in CSF.
<input type="checkbox"/>	Marketing	192.168.200.10	FortiGate-90D	Real Time	0	0.05%	FortiGate for Marketing Department.

- Go to *FortiView > System > System Events*. Events from all FortiGates in the CSF are shown, allowing you to have a complete view of the network.

Event Name (Description)	Severity	▼ Counts
System performance statistics	Low	19
FortiAnalyzer connection up	Low	8
SSL connection established	Info	6
SSL connection closed	Info	5
FortiAnalyzer connection down	Low	5
SSL connection failed	Info	3
Attribute configured	Info	3
FortiGate updated	Low	1

- You can select a type of system event, such as *System performance statistics*, to view information about the individual events. Events are shown from all three FortiGates (the Device ID shown for each FortiGate is that unit's serial number).

#	▼ Date/Time	Level	Device ID	Message
1	19:43:13	notice	FGT90D3Z15019631	Performance statistics: average CPU: 51, memory: 43, concurrent sessions: 3...
2	19:42:53	notice	FG140D3G13804256	Performance statistics: average CPU: 17, memory: 32, concurrent sessions: 4...
3	19:42:20	notice	FGT6HD3916800525	Performance statistics: average CPU: 0, memory: 28, concurrent sessions: 78...
4	19:38:14	notice	FGT90D3Z15019631	Performance statistics: average CPU: 0, memory: 42, concurrent sessions: 29...
5	19:37:53	notice	FG140D3G13804256	Performance statistics: average CPU: 0, memory: 31, concurrent sessions: 33...
6	19:37:20	notice	FGT6HD3916800525	Performance statistics: average CPU: 0, memory: 27, concurrent sessions: 69...
7	19:33:14	notice	FGT90D3Z15019631	Performance statistics: average CPU: 0, memory: 42, concurrent sessions: 29...
8	19:32:52	notice	FG140D3G13804256	Performance statistics: average CPU: 0, memory: 31, concurrent sessions: 33...
9	19:32:19	notice	FGT6HD3916800525	Performance statistics: average CPU: 0, memory: 27, concurrent sessions: 67...
10	19:28:14	notice	FGT90D3Z15019631	Performance statistics: average CPU: 0, memory: 42, concurrent sessions: 31...
11	19:27:52	notice	FG140D3G13804256	Performance statistics: average CPU: 0, memory: 31, concurrent sessions: 32...
12	19:27:23	notice	FGT6HD3916800525	Performance statistics: average CPU: 0, memory: 27, concurrent sessions: 67...
13	19:23:14	notice	FGT90D3Z15019631	Performance statistics: average CPU: 0, memory: 42, concurrent sessions: 33...
14	19:22:51	notice	FG140D3G13804256	Performance statistics: average CPU: 0, memory: 31, concurrent sessions: 34...
15	19:22:22	notice	FGT6HD3916800525	Performance statistics: average CPU: 0, memory: 27, concurrent sessions: 69...
16	19:18:14	notice	FGT90D3Z15019631	Performance statistics: average CPU: 0, memory: 42, concurrent sessions: 32...
17	19:17:50	notice	FG140D3G13804256	Performance statistics: average CPU: 0, memory: 31, concurrent sessions: 33...
18	19:17:22	notice	FGT6HD3916800525	Performance statistics: average CPU: 0, memory: 27, concurrent sessions: 69...

Log data migration from an old to new FortiAnalyzer

This example illustrates how to migrate logs from an old FortiAnalyzer to a new FortiAnalyzer.



When migrating logs, the firmware version must be the same. For example, if you are migrating logs from an old FortiAnalyzer running 5.2 to a new FortiAnalyzer running 5.4, you must upgrade the 5.2 FortiAnalyzer to 5.4 firmware before aggregating and migrating logs to the new 5.4 FortiAnalyzer.

Migrating prerequisites

To migrate prerequisites:

1. Make the old and new FortiAnalyzer the same firmware version. 5.4.0 or later is preferred.
2. Migrate the Device Manager settings from the old FortiAnalyzer to the new one.
3. Enable the GUI display by using the following command:

```
conf sys admin setting > show-device-import-export: enable
```

4. In the old FortiAnalyzer, *export* the Device List from the Device Manager.
5. In the new FortiAnalyzer, *import* the Device List from the Device Manager.

Setting up the aggregation client



For FortiAnalyzer 5.6.0 and later, Log Aggregation is only available from the CLI.

To set up the aggregation client in the CLI:

```
config system aggregation-client
  edit 1
    set mode aggregation
    set agg-user [ENTER ADMIN USER FOR NEW FORTIANALYZER]
    set agg-password [ENTER PASSWORD FOR NEW FORTIANALYZER]
    set agg-time 1 [LOG AGGREGATION START TIME]
    set server-ip [ENTER NEW FORTIANALYZER IP ADDRESS]
  next
end
```

Setting up the aggregation server

To set up the aggregation server in the CLI:

1. Use the following command in the CLI:

```
config system aggregation-service
  set accept-aggregation enable
end
```

2. After running the command, take note of the *Instance ID*. You will need to enter the Instance ID when running the aggregation command in the client CLI.



Log Aggregation is not supported on all FortiAnalyzer models. Check your specific device's datasheet.

Running aggregation in the client CLI

You can initiate log aggregation via the GUI or the CLI console.

To initiate log aggregation in the GUI:

1. Go to *System > Log Forwarding*.
2. Select *Aggregation Profile*.
3. Click *Aggregate Now*.

To initiate log aggregation in the CLI:

```
exec log-aggregation all
```

Checking the aggregation progress on the client

To check the aggregation progress on the client:

1. On the old FortiAnalyzer, go to *System Settings > Event Log*.
2. When the log aggregation is completed, the following message will be displayed:
Log aggregation session completed.

Rebuilding the database

If you are migrating a large amount of logs, you will need to rebuild the database after log aggregation.

To rebuild the database:

```
exec sql-local rebuild-db
```

Debugging log aggregation

To debug log aggregation:


```
dia debug application log-aggregate 255  
dia deb en
```

Replacing FortiGate HA pairs with logging enabled

This recipe describes how to replace the primary and secondary FortiGate units in a high-availability (HA) pair, that are sending logs to FortiAnalyzer, when the connection to FortiAnalyzer goes down.

When the FortiGate units in an HA pair are synchronized and added to FortiAnalyzer, two members are displayed in the HA Cluster list in FortiAnalyzer.

HA Cluster List:

#	Device Name	Action
1	FGT60D4614007024 (FGT60D4614007024)	
2	FGT60D4614007595	

In this example, *FGT 60D4614007024* is the primary unit, but the connection to FortiAnalyzer is down.

Replacing the primary unit

In FortiAnalyzer, do not delete the original primary FortiGate unit; if you do, you will lose logs associated with the device being replaced. Instead, add the new primary FortiGate unit to the *HA Cluster* list.



You can delete the original primary FortiGate unit at a later time, when the logs are no longer needed.

HA Cluster ☒

Add existing device

Add other device



HA Cluster List:

#	Device Name	Action
1	FGT60D4614007024 (FGT60D4614007024)	
2	FGT60D4614007595	
3	FGT60D4Q16025640	

The FortiAnalyzer GUI displays three units in the *HA Cluster* list. It appears that the original FortiGate unit remains the primary unit in the HA cluster.

However, the new primary FortiGate unit in the HA cluster informs FortiAnalyzer which of the three units is the master.

HA Cluster List:

#	Device Name	Action
1	FGT60D4Q16025640 (FGT60D4614007024)	
2	FGT60D4614007595	
3	FGT60D4Q16025640	

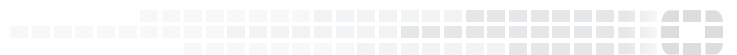
If you would like to see the new primary FortiGate unit as the current device, change the device name in the FortiAnalyzer. If the unit being replaced was the original master, the cluster's device name may show the serial number of this device. If you wish, you can edit the cluster to reflect the serial number of the new device.



The process is the same if you want to replace the secondary unit in an HA pair.



FORTINET®



Copyright© 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.