

# Exercise 1: Configuring a Collector to Forward Logs

In this exercise, you will configure a FortiAnalyzer to operate in collector mode, which will forward logs to an upstream FortiAnalyzer that is working in analyzer mode. You will also generate some test logs to confirm that the collector is configured correctly.

## Configure a Collector to Forward Logs to an Analyzer

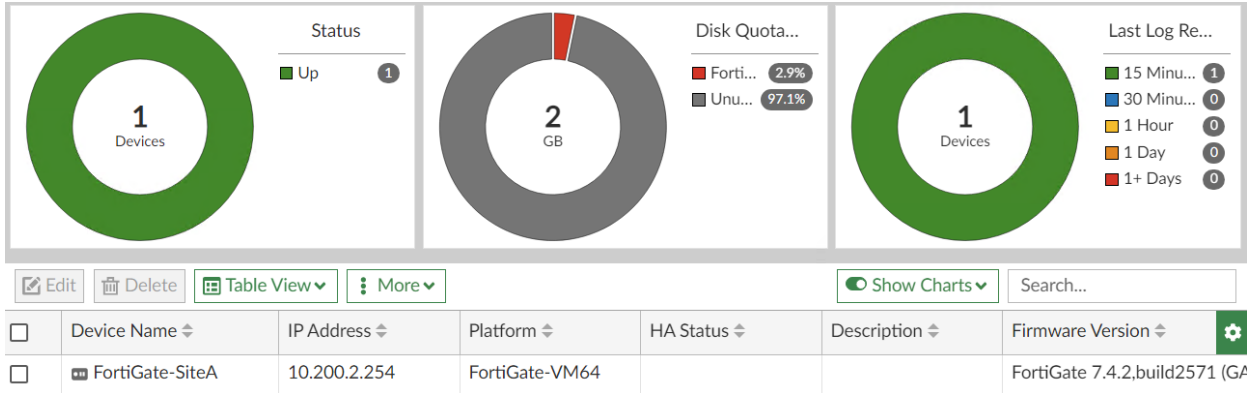
A FortiAnalyzer can be configured to operate in collector mode, which forwards logs to a FortiAnalyzer in analyzer mode. The FortiAnalyzer in collector mode is designed to forward logs and host archive logs, and the FortiAnalyzer in analyzer mode is designed to provide analytics. Analyzer mode is the default operation mode.

In this scenario, FAZ-SiteA is the collector, and FAZ-MSSP is the analyzer.

To review logging devices

- On the bastion host, open Google Chrome, and then log in to the FAZ-SiteA GUI (10.200.4.237) with the following credentials:
  - Username: admin
  - Password: Fortinet1!
- Click **Device Manager**.
- Click **All Logging Devices**.

One device is registered: **FortiGate-SiteA**.



## To change the operation mode

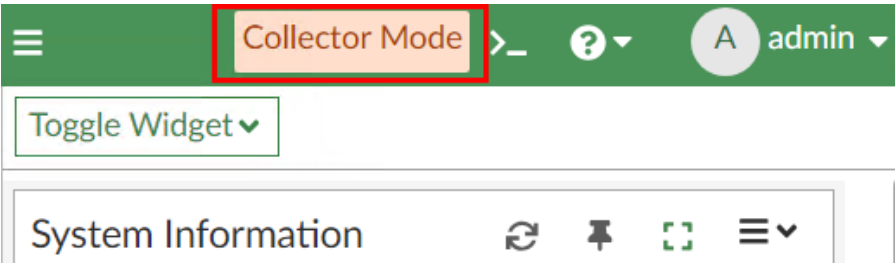
- Continuing on the FAZ-SiteA GUI, click **Dashboard**.
- In the **System Information** widget, in the **Operation Mode** field, select **Collector**.

By default, **Analyzer** is selected.

# System Information

Host Name	FAZ-SiteA
Serial Number	FAZ-VMTM24000906
Platform Type	FAZVM64
HA Status	Standalone
System Time	Sun Aug 11 19:33:18 2024 PDT
Firmware Version	v7.4.3-build2487 240514 (GA)
System Configuration	Last Backup: Wed Jun 12 15:11:54 2024
Current Administrators	admin / 1 in total
Up Time	2 days 2 hours 43 minutes 2 seconds
Administrative Domain	<input type="checkbox"/>
Operation Mode	<div><div>Analyzer</div><div>Collector</div></div>

- 3. Click **OK**.
- 4. Log out of the FAZ-SiteA GUI.
- 5. Log in to the FAZ-SiteA GUI again, and then near the upper-right corner, ensure that **Collector Mode** is displayed to confirm that the FortiAnalyzer is now working in collector mode.



## To change the data policy and allocated quota

- 1. Continuing on the FAZ-SiteA GUI, click **System Settings > ADOMs**.
- 2. Double-click **root**.
- 3. Configure the following settings:

Field	Value
Keep Logs for Analytics	0 Days
Keep Logs for Archive	365 Days
Modify	Select the checkbox.
Analytics: Archive	5%:95%

Data Policy			
Keep Logs for Analytics	0	Days	
Keep Logs for Archive	365	Days	

Disk Utilization			
Allocated	50	GB	Maximum Available: 441.0 GB
Analytics: Archive	5%	95%	<input checked="" type="checkbox"/> Modify
Alert and Delete When Usage Reaches	90%		

4. Click **OK**.

If you see a warning regarding the analytics logs being kept for unlimited days, click **OK** to ignore the warning and proceed.



When FortiAnalyzer is operating in collector mode, the analytics database is disabled. Therefore, the **Keep Logs for Analytics** setting is not used.

FAZ-SiteA, as a collector, does not handle analytics, which is reflected in the configuration above. FAZ-MSSP, in analyzer mode, handles analytics.

## To configure log forwarding

1. Continuing on the FAZ-SiteA GUI, click **System Settings > Advanced > Log Forwarding**.
2. Click **Create New**.
3. Configure the following settings:

Field	Value
Name	FAZ-MSSP
Status	Enabled
Remote Server Type	FortiAnalyzer
Server FQDN/IP	10.0.1.236
Compression	Enabled
Reliable Connection	Enabled
Sending Frequency	Real-time

Name	<input type="text" value="FAZ-MSSP"/>
Status	<input checked="" type="checkbox"/>
Remote Server Type	<input type="text" value="FortiAnalyzer"/>
Server FQDN/IP	<input type="text" value="10.0.1.236"/>
Compression	<input checked="" type="checkbox"/>
Reliable Connection	<input checked="" type="checkbox"/>
Peer Certificate CN	<input type="text"/>
Sending Frequency	<div><input checked="" type="radio"/> Real-time</div> <div><input type="radio"/> Every 1 Minute</div> <div><input type="radio"/> Every 5 Minutes</div>

4. Click **OK**.

Enabling the log message compression setting reduces the bandwidth required on the network.



If the **Reliable Connection** setting is enabled, TCP is used. If this setting is disabled, UDP is used. If there are connection problems, logs are buffered, and then automatically forwarded when the connection is restored. The default buffer size depends on the system reserved disk space and the platform.

## Configure the Analyzer

You will enable administrative domains (ADOMs) on FAZ-MSSP. You will configure one of the ADOMs for analytics only, and the other ADOM for both analytics and archive. Then, you will add the collector that you configured in the previous task to the analytics-only ADOM. To verify that log forwarding from the collector is functional, you will generate test logs on FortiGate-SiteA, and then confirm that FAZ-MSSP received the logs. You will also verify that the logs are able to generate events.

## To enable ADOMs

1. Continuing on the bastion host, in Chrome, log in to the FAZ-MSSP GUI (10.200.4.236) with the following credentials:
  - Username: admin

- Password: Fortinet1!

2. Click **Dashboard**.

3. In the **System Information** widget, enable **Administrative Domain**.

By default, this setting is disabled.

## System Information

Host Name	FAZ-MSSP
Serial Number	FAZ-VMTM24000905
Platform Type	FAZVM64
HA Status	Standalone
System Time	Sun Aug 11 19:46:05 2024 PDT
Firmware Version	v7.4.3-build2487 240514 (GA)
System Configuration	Last Backup: Wed Jun 12 15:11:34 2024
Current Administrators	admin / 1 in total
Up Time	2 days 2 hours 55 minutes 54 seconds
Administrative Domain	<input type="checkbox"/>
Operation Mode	<span>Analyzer</span> <span>Collector</span>

4. Click **OK**.

You will be logged out of the FAZ-MSSP GUI.

5. Log in to the FAZ-MSSP GUI again, and then click **root**.

6. Click **System Settings > ADOMs**.

7. Click **Create New**.

8. Configure the following settings:

Field	Value
Name	SiteA
Keep Logs for Analytics	60 Days
Keep Logs for Archive	0 Days
Allocated	50 GB
Modify	Select the checkbox.
Analytics: Archive	95%:5%

9. Click **OK**.

10. Click **OK** again.

11. Continuing on the **System Settings > ADOMs** page, click **Create New** again.

12. Configure the following settings:

Field	Value
Name	MSSP-Local
Keep Logs for Analytics	60 Days
Keep Logs for Archive	365 Days
Allocated	50 GB
Analytics: Archive	70%:30%

13. Click **OK**.

The SiteA ADOM will be used for analytics only. The archiving will be handled by the collector. FortiGate-SiteA will send logs to FAZ-SiteA first, which will then forward logs to FAZ-MSSP under the SiteA ADOM. This is why you configure the data policy and disk utilization for analytics.



The MSSP-Local ADOM will be used for both analytics logs and archive logs. FortiGate-MSSP is configured to send logs directly to FAZ-MSSP, so there is no collector involved. As a result, the data policy

for MSSP-Local should not be 0 for analytics or archive, and the default 70%:30% ratio is not changed.

## To register devices with FAZ-MSSP

1. Continuing on the FAZ-MSSP GUI, in the root ADOM, click **Device Manager**.



You can change the ADOM by clicking **ADOM: root**.



2. Click **Unauthorized Devices**.

There should be two unauthorized devices: FortiGate-SiteA and FortiGate-MSSP.

3. Select the checkbox for **FortiGate-SiteA**, and then click **Authorize**.

☒ Authorize ☐ Hide ☐ Delete ☐ Display Hidden Devices

<input type="checkbox"/>	Device Name ▾	Platform ▾	Serial Number ▾	IP Address ▾
<input type="checkbox"/>	FortiGate-MSSP	FortiGate-VM64	FGVMSLTM2400045	10.0.1.254
<input checked="" type="checkbox"/>	FortiGate-SiteA	FortiGate-VM64	FGVMSLTM2400045	10.200.2.254

4. In the **Add the following device(s) to ADOM** field, select **SiteA (Fabric 7.4)**.

Authorize Device ✕

Add the following device(s) to ADOM: SiteA (Fabric 7.4) ▾

Search...

Name ▾	Assign New Device Name ▾	⚙
FortiGate-SiteA	FortiGate-SiteA	

1

OK

Cancel

5. Click **OK**.
6. In the **Authorize Device** window, click **Close**.
7. Continuing on the **Device Manager** page, select the checkbox for **FortiGate-MSSP**, and then click **Authorize**.

☒ Authorize ☐ Hide ☐ Delete ☐ Display Hidden Devices

<input type="checkbox"/>	Device Name ▾	Platform ▾	Serial Number ▾	IP Address ▾
<input checked="" type="checkbox"/>	FortiGate-MSSP	FortiGate-VM64	FGVMSLTM2400045	10.0.1.254

8. In the **Add the following device(s) to ADOM** field, select **MSSP-Local (Fabric 7.4)**.



All Devices

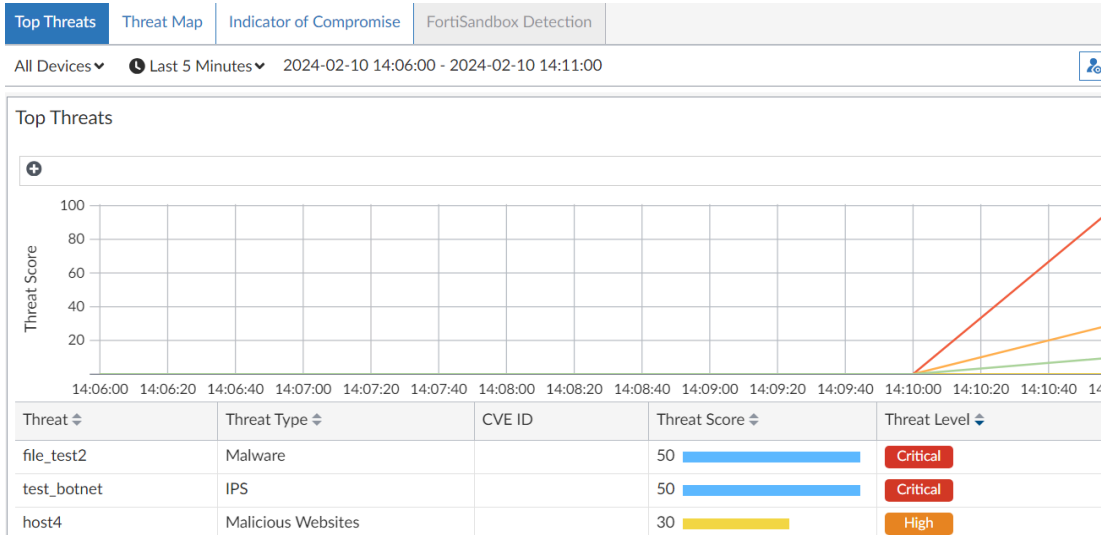
Last 5 Minutes

13:56:56 To 14:01:55

+

#	↓Date/Time	Device ID	Source	Action
1	14:01:21	FGVMSLTM24000454	168.10.199.186	✓
2	14:01:21	FGVMSLTM24000454	172.16.100.2	✓
3	14:01:20	FGVMSLTM24000454	172.16.100.2	✓
4	14:01:20	FGVMSLTM24000454	178.10.199.186	✗ Deny:UTM

- Click **FortiView** > **Threats**.
- Confirm that security threats are displayed—if necessary, adjust the log time period filter.



- Click **Incidents & Events** > **Event Monitor**.
- Confirm that generated events are displayed—if necessary, adjust the log time period filter.

All Events

By Endpoint

By Threat

System Events

Toggle Views

All Devices

Last 30 Minutes

Show Acknowledged

Expand All

Search or type filters...

<input type="checkbox"/>	Event	Event Status	Event Type	Count	Severity
<input type="checkbox"/>	+ 168.10.199.186 (6)	Unhandled	...	12	High
<input type="checkbox"/>	+ test_botnet (1)	Unhandled	IPS	2	High
<input type="checkbox"/>	+ 224.141.85.77 (3)	Unhandled	...	6	Medium
<input type="checkbox"/>	+ 178.10.199.186 (4)	Mitigated	...	8	Medium
<input type="checkbox"/>	+ virus:N/A (2)	Mitigated	Antivirus	4	Medium
<input type="checkbox"/>	+ host4 (1)	Mitigated	Web Filter	2	Medium

The **FortiView** and **Incident & Events** features are not available on the collector because they require analytics logs. This is why you must access FAZ-MSSP, the analyzer, to view these items.

### To verify log forwarding statistics on the collector

- Continuing on the bastion host, in Chrome, return to the FAZ-SiteA GUI, and then click the icon to open the FortiAnalyzer CLI.
- Enter the following commands:

```
diagnose test application logfwd 3
```

```
diagnose test application logfwd 4
```



```

FAZ-SiteA # diagnose test application logfwd 3
Usage: <devf (show up to 30 devices that passed expression filters)|devf-all (show all devices that passed expression filters)

Config disk-cache-size: 15 GB

#1: FAZ-MSSP => FortiAnalyzer @ 10.0.1.236:514 token=1483262000804368994 Reliable Running Updt=1723431552 cfg-id=1
tlvm-ver=2 logfwd-ver=1.1 logfmt=Lz4 v5c compress firmware-ver=7.2487
Grp=ld-FAZ-MSSP Qid=21 Updt=1723431552 Hash=1.54f6e499f5add59a.0.0.0

FAZ-SiteA # diagnose test application logfwd 4

** Loader: ld-FAZ-MSSP
Pos=(1723430709.60569631-106483.0)
lag-behind=0.00% (751) bytes-discarded=0
msg-load=134 msg-pass_devf=134 msg-pass_logf=134 log-to/pass_logf=0/0
Cvtr-Q: in-queue=0
Fwdr-Q: in-queue=0 idle=1023 q-get-timeout=0
lbuf-cvtr-get-wait=0 lbuf-get-wait=0 lbuf-get-forced=0
grp-refcnt=3 curr-Qsz-max=64
lfwd_parse_err=0 lfwd_msg_err=0 msglen-err=0 cfile-read-err=0

** Server#1: FAZ-MSSP ld-FAZ-MSSP Qid=21 Connected src-intf:port1 bind: from 14m4s ago
curr-msg-seqno=1723431553244
nmsg-sent=132 nlog-sent=206 send timeout=0 send_err=0
conn_err=0 msg_append_err=0 unreliable-errno=0
compress_overthres=0 compress_err=0 adaptive_bufsz=65536
rate in last 5sec, 30sec, 60sec
msg/sec: 0.0 0.1 0.1
log/sec: 0.0 0.1 0.1

```




You can find information, such as log positions, log and log message rates, timeouts, connection errors, and other important values, if you need to troubleshoot.

Note that error values may not necessarily indicate an issue if they are low and do not increment.

3. Close the CLI.

## To verify log forwarding statistics on the analyzer

1. Continuing on the bastion host, in Chrome, return to the FAZ-MSSP GUI, and then click the  icon to open the FortiAnalyzer CLI.
2. Enter the following command:

diagnose test application oftpd 7

```

FAZ-MSSP # diagnose test application oftpd 7
Reliable logging stats:
log=0 log(>4k)=0

Reliable log-forward stats:
log=0 log(>4k)=0 reg=0 ack=0 ack_back=0 thr=0 optcode_err=0

Reliable log-forward gen2 stats:
Connections:
From FAZ-VMTM24000906 @ 10.200.2.237 sig.14959aee5ac79262 Connected 16m55.062s ago fc.0x7f9430007a38
Pos=1723430709.60569631.120666.1 tlvm-ver=2 lfwd-ver=1.1 last_rcv=1723431709 n_flushed=153 n_compressed=0
Stats:
add=1 del=0 replace=0
inactive=0 expired=0
msg-rcv=153
msg-dropped=0(seq error)
Errors:
conn=0 conn_info=0 discard=0 unknow-option=0
epoll.add=0 epoll.del=0
rcv_tlvm=0 rcv_oversize=0 parse_msg=0 build_resp=0

Internal log-forward stats:
queued=0 (max=2048) update=3331 (now=3347)

errors
fortilogd-not-running=0 no-init=0 socket=0 no-rcv=0 unknown=0

Internal-forward stats by source:
fwd-reliable : 153

```



You can use this command to compare the log positions in order to see how far behind (if at all) the analyzer is compared to the collector.

LAB-2 > Configuring a Collector to Forward Logs