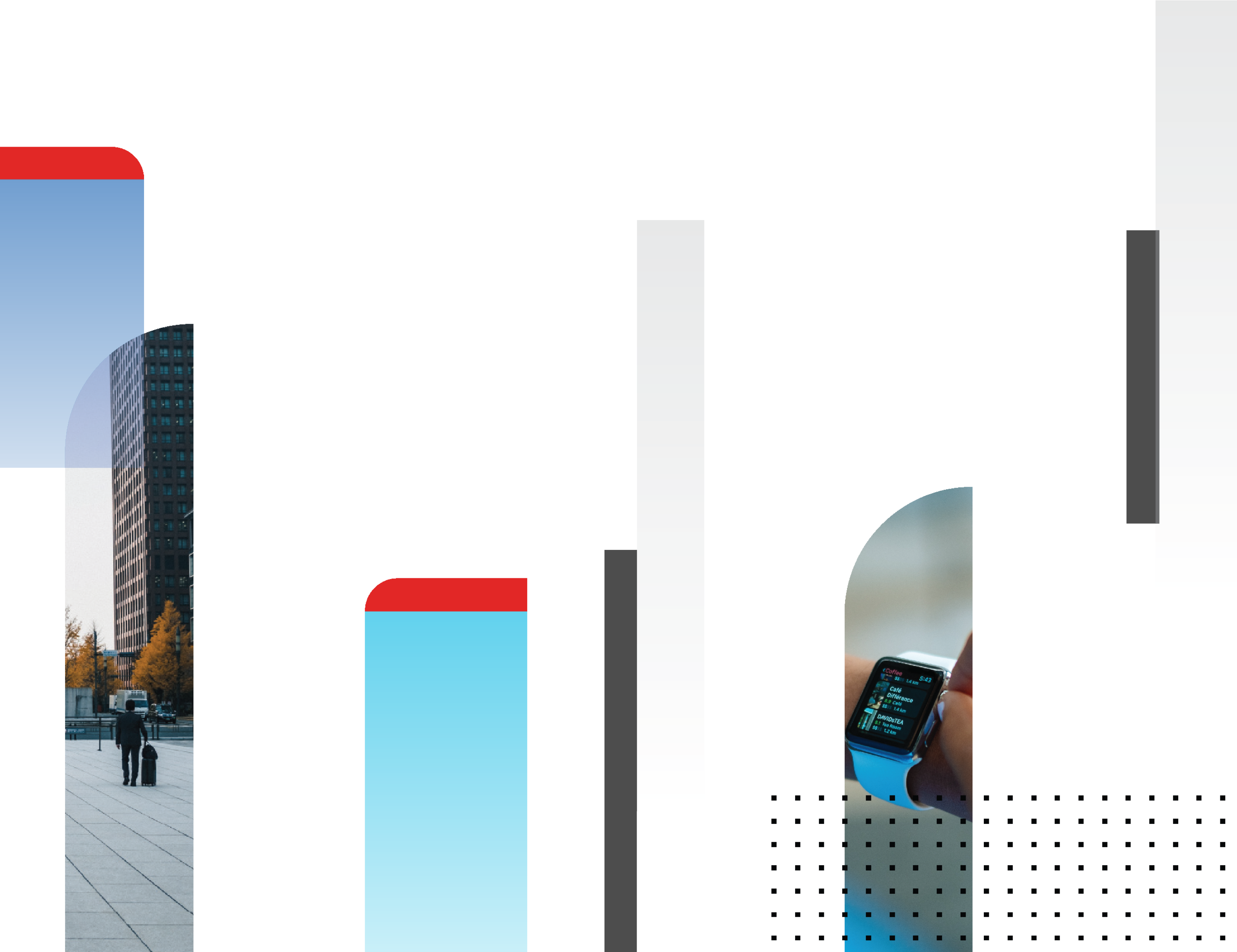
Examples

FortiAnalyzer 7.0.0



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 TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

December 17, 2021
FortiAnalyzer 7.0.0 Examples
05-700-724489-20211217

TABLE OF CONTENTS

Change log

Date	Change Description
2021-06-30	Initial release.
2021-08-13	Added FortiAI logging on FortiAnalyzer on page 47
2021-12-17	Added Configuring an event handler to filter IPS attack direction on page 37.

Introduction

This document serves as a reference guide to common FortiAnalyzer 7.0 configuration and deployment scenarios. The scope of this document is to explain specific examples and include information required for those examples to work. The examples rely on the other documents to provide full product information.

For further FortiAnalyzer information, refer to the FortiAnalyzer Administration Guide available on the Fortinet Docs Library.

This section includes configuration examples for FortiAnalyzer 7.0:

- System settings on page 7
- Reports on page 9
- Real-time dashboards on page 11
- Fabric connectors on page 15
- SOAR and SIEM on page 28
- Logging on page 47
- Troubleshooting on page 51

System settings

This section contains the following topics:

- Setting up a FortiAnalyzer HA cluster on page 7

Setting up a FortiAnalyzer HA cluster

You can configure two or more FortiAnalyzer units in a High Availability (HA) cluster to provide real-time redundancy in case a primary unit fails. High Availability clusters also alleviate the load on the primary unit by using secondary units for processes such as running reports.

The following is an overview of how to configure FortiAnalyzer units in an HA cluster:

1. Go to *System Settings* > *HA*.
2. Set the *Operation Mode* of the primary unit to *High Availability*.
3. Configure the settings for the primary unit.
4. Configure the settings for the secondary units.

All the units must:

- Be of the same FortiAnalyzer series
- Be visible on the network
- Run in the same operation mode: *Analyzer* or *Collector*

To configure the primary unit in an HA cluster:

1. Go to *System Settings* > *HA*.
2. Set the *Operation Mode* to *High Availability*.
3. Set the *Preferred Role* to *Primary*.
4. Configure the *Cluster Virtual IP* settings:

Interface	Select the interface to be used as the clustered Virtual IP.
IP Address	Type the IP address to be used by the HA cluster to provide redundancy.

5. In the *Peer IP and Peer SN* box, type the *Peer IP* and *Peer SN* for each secondary unit. The maximum is three units.
6. Type the *Group Name*, *Group ID*, and *Password*. These settings must be the same for all the units in the cluster.
7. Click *Apply*.

To configure secondary units in an HA cluster:

1. Set the *Preferred Role* to *Secondary*.
2. Configure the *Cluster Virtual IP* settings with the HA cluster's *Interface* and *IP Address*.

Interface	Select the interface being used by the cluster as the Virtual IP.
IP Address	Type the IP address being used by the cluster to provide redundancy.

3. In the *Peer IP and Peer SN* box, type the *Peer IP* and *Peer SN* for the primary unit and each secondary unit.
4. Type the *Group Name*, *Group ID*, and *Password*. These settings must be the same for all the units in the cluster.
5. Click *Apply*.

Reports

This section contains the following topics:

Configuring a report with an LDAP server

You can use report filters to only the show members of a group in an LDAP server.

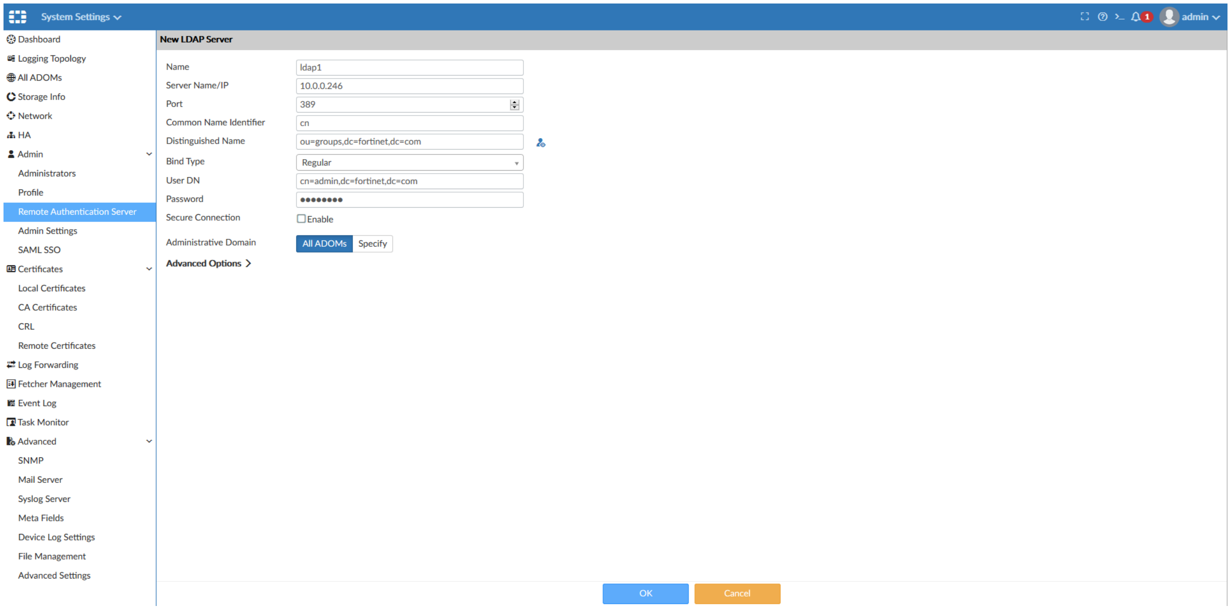
This example demonstrates how to filter the *Admin and System Events Report* to show data for the group members in `Distinguished Name: cn=group1,ou=groups,dc=fortinet,dc=com` in the report output.

Requirements:

- The LDAP server is ready and accessible.
- Group members are configured.

To configure the report:

1. Add the LDAP server to FortiAnalyzer.
   a. Go to *System Settings > Admin > Remote Authentication Server*, and click *Create New > LDAP Server.*
   b. Configure the LDAP server settings, then click *OK*.



New LDAP Server

Name	ldap1
Server Name/IP	10.0.0.246
Port	389
Common Name Identifier	cn
Distinguished Name	ou=groups,dc=fortinet,dc=com
Bind Type	Regular
User DN	cn=admin,dc=fortinet,dc=com
Password	••••••••
Secure Connection	□ Enable
Administrative Domain	All ADOMs / Specify

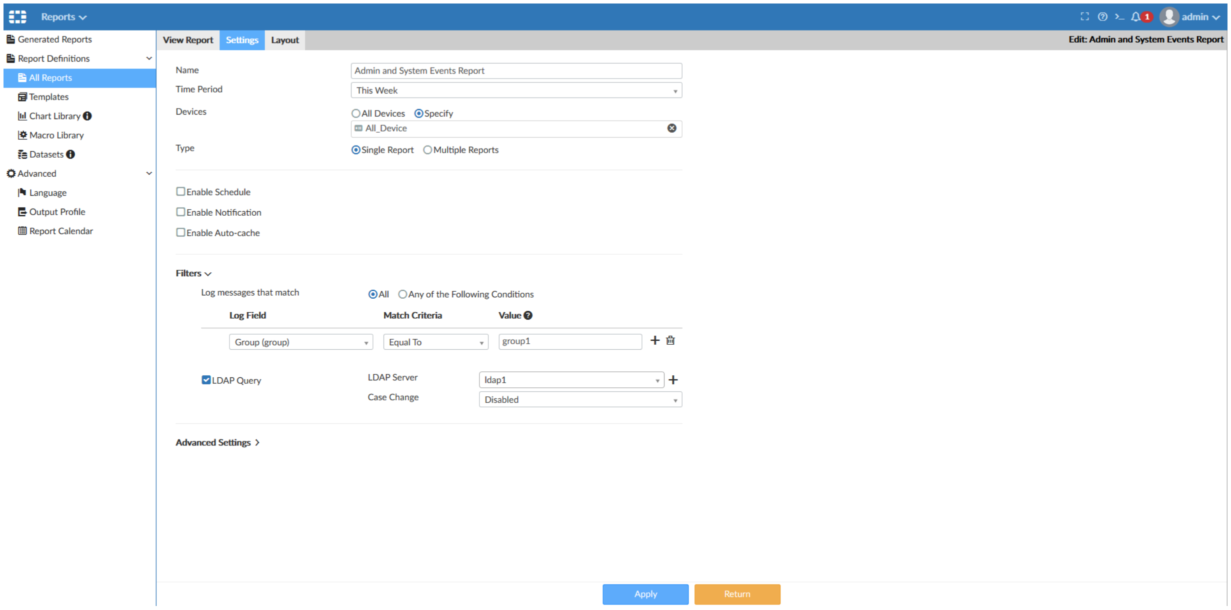
Advanced Options >

2. Apply the LDAP server to the report filter.
   a. Go to *Reports* and select the *Admin and System Events Report*.
   b. Click the *Settings* tab, then expand the *Filters* section.

c. Use the following settings to configure the filter:

Log Field	Select *Group (group)*.
Match Criteria	Select *Equal to*.
Value	Enter `group1`.

d. Click *LDAP Query* and set *LDAP Server* to the LDAP server you created, then click *Apply*.



Name: Admin and System Events Report

Time Period: This Week

Devices: ○ All Devices ● Specify
All_Device

Type: ● Single Report ○ Multiple Reports

□ Enable Schedule

□ Enable Notification

□ Enable Auto-cache

Filters

Log messages that match: ● All ○ Any of the Following Conditions

Log Field	Match Criteria	Value
Group (group)	Equal To	group1

☑ LDAP Query

LDAP Server: ldap1

Case Change: Disabled

3. Select the *View Report* tab and click *Run Report* to run the report and verify the output.
The report displays the users in the group: `cn=group1,ou=groups,dc=fortinet,dc=com` in the *Login Summary* chart and the group name in the *Report Filters*.

Real-time dashboards

This section contains the following topics:

- Configuring FortiAnalyzer to detect FortiSandbox devices on page 11

Configuring FortiAnalyzer to detect FortiSandbox devices

You can use FortiAnalyzer to monitor FortiSandbox devices. Some configurations are required on FortiSandbox to add the device to FortiAnalyzer. After you add the device, go to *FortiView* > *Threats* > *FortiSandbox Detection* to view the scanned files.

To detect FortiSandbox on FortiAnalyzer:

1. Create a firewall policy on FortiSandbox.
2. Create a log server on FortiSandbox.
3. Add FortiSandbox to FortiAnalyzer.

Creating a firewall policy on FortiSandbox

You can use the CLI console in FortiSandbox to configure a firewall policy, then specify the IP address of the FortiAnalyzer you want to monitor the FortiSandbox.

To create a firewall policy on FortiSandbox:

1. In the FortiGate device, click the CLI Console icon on the right-side of the banner on any page.
2. Specify the FortiSandbox in the global configuration:

```
config antivirus profile
   edit "test"
      set ftgd-analytics everything config http
         set options scan avmonitor
      end config ftp
         set options scan avmonitor
      end config imap
         set options scan
      end config pop3
         set options scan
      end config smtp
         set options scan
      end config nntp
         set options scan
      end
   next
end
```

3. Create an antivirus profile to allow FortiGate to submit all files scanned by AntiVirus to FortiSandbox. The following is a sample AntiVirus profile:

```
config firewall policy
   edit 13
      set name "to-server1"
      set uuid 5107b480-3d19-51e8-f1c1-571602a6375b
      set srcintf "lan"
      set dstintf "wan1"
      set srcaddr "net-local"
      set dstaddr "server1"
      set action accept
      set schedule "always"
      set service "ALL"
      set utm-status enable
      set logtraffic all
      set fsso disable
      set av-profile "test"
      set ssl-ssh-profile "certificate-inspection"
      set nat enable
   next
end
```

4. Use the antivirus profile in the firewall policy. The following is a sample firewall policy:

   ```
   config firewall policy
      edit 13
         set name "to-server1"
         set uuid 5107b480-3d19-51e8-f1c1-571602a6375b
         set srcintf "lan"
         set dstintf "wan1"
         set srcaddr "net-local"
         set dstaddr "server1"
         set action accept
         set schedule "always"
         set service "ALL"
         set utm-status enable
         set logtraffic all
         set fsso disable
         set av-profile "test"
         set ssl-ssh-profile "certificate-inspection"
         set nat enable
      next
   end
   ```

5. Specify the IP address of the FortiAnalyzer unit for FortiGate to send logs.

   ```
   configure log fortianalyzer setting
      set status enable
      set server <ip address of FortiAnalyzer> set upload-option realtime
   end
   ```

Creating a log server for FortiAnalyzer

Use FortiSandbox to create a log server to specify the FortiAnalyzer that will monitor the scanned files.

To create a log server on FortiSandbox:

1. On FortiSandbox, go to *Log & Report* > *Log Servers*.
2. Click *Create New* in the toolbar and configure the following settings:

Name	Enter a name for the new server entry.
Type	Select FortiAnalyzer from the dropdown list.
Log Server Address	Enter the log server IP address for the FortiAnalyzer device.
Port	Enter the port number. The default port is 514.
Status	Select Enable to send logs to the server.
Log Level	• Set the logging levels to be forwarded to the log server. The following options are available: Enable *Alert Logs*. By default, only logs of non-Clean rated jobs are sent. Users can choose to send Clean Job Alert Logs by selecting *Include job with Clean Rating*. • Enable *Critical Logs* • Enable *Error Logs* • Enable *Warning Logs* • Enable *Information Logs* • Enable *Debug Logs*

Adding FortiSandbox to FortiAnalyzer

You can use the IP address of the configured FortiSandbox to add it to FortiAnalyzer with *Device Manager*.

To add the FortiSandbox:

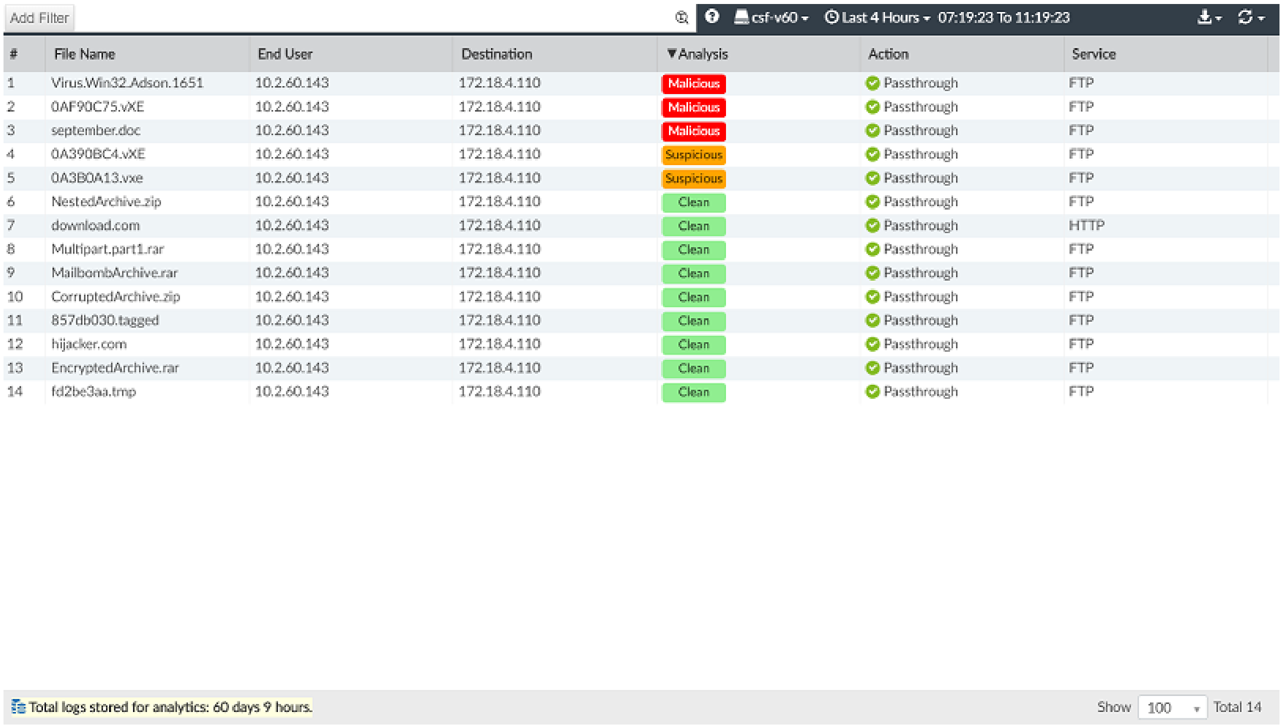
1. In FortiAnalyzer, go to *Device Manager*.
2. Click *Add Device*, and enter the FortiSandbox information into the dialog box.

Device Name	Type a name for the FortiSandbox device.
Link Device By	Serial Number.
Serial Number	Type the serial number for the FortiSandbox device.
Device Model	Select the model of the FortiSandbox device.
Description	Type a description of the FortiSandbox device (optional).

3. Click *Next*.
   The device is added to the ADOM and, if successful, is ready to begin sending logs to the FortiAnalyzer unit.
4. Click *Finish*.
5. In *Device Manager*, select the FortiSandbox you added, and click *Edit* in the toolbar.
6. Enter the *Admin User* and *Password* to allow FortiAnalyzer to access the FortiSandbox, then click *OK*.

To view FortiSandbox scanned files:

1. Go to *FortiView > FortiView > Threats > FortiSandbox Detection* to view the files scanned by FortiSandbox.
2. Click a file to view the *Drilldown Panel*.

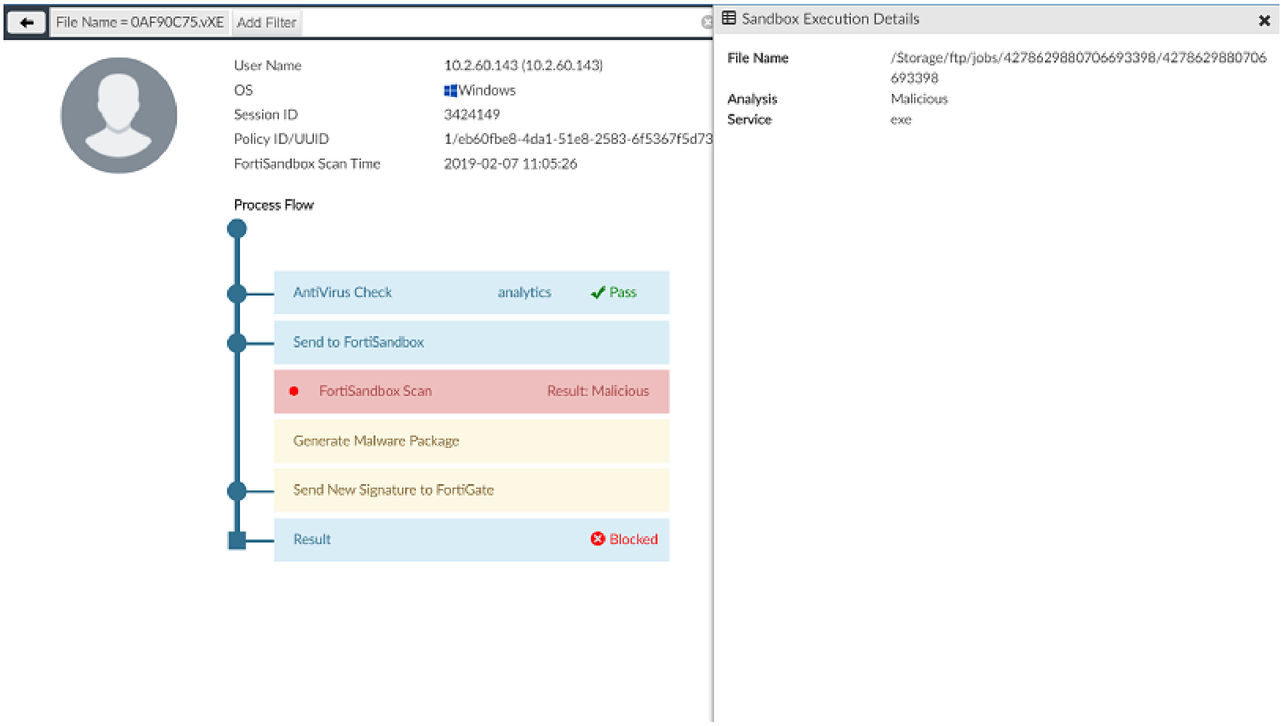


#	File Name	End User	Destination	▼Analysis	Action	Service
1	Virus.Win32.Adson.1651	10.2.60.143	172.18.4.110	Malicious	✓ Passthrough	FTP
2	0AF90C75.vXE	10.2.60.143	172.18.4.110	Malicious	✓ Passthrough	FTP
3	september.doc	10.2.60.143	172.18.4.110	Malicious	✓ Passthrough	FTP
4	0A390BC4.vXE	10.2.60.143	172.18.4.110	Suspicious	✓ Passthrough	FTP
5	0A3B0A13.vxe	10.2.60.143	172.18.4.110	Suspicious	✓ Passthrough	FTP
6	NestedArchive.zip	10.2.60.143	172.18.4.110	Clean	✓ Passthrough	FTP
7	download.com	10.2.60.143	172.18.4.110	Clean	✓ Passthrough	HTTP
8	Multipart.part1.rar	10.2.60.143	172.18.4.110	Clean	✓ Passthrough	FTP
9	MailbombArchive.rar	10.2.60.143	172.18.4.110	Clean	✓ Passthrough	FTP
10	CorruptedArchive.zip	10.2.60.143	172.18.4.110	Clean	✓ Passthrough	FTP
11	857db030.tagged	10.2.60.143	172.18.4.110	Clean	✓ Passthrough	FTP
12	hijacker.com	10.2.60.143	172.18.4.110	Clean	✓ Passthrough	FTP
13	EncryptedArchive.rar	10.2.60.143	172.18.4.110	Clean	✓ Passthrough	FTP
14	fd2be3aa.tmp	10.2.60.143	172.18.4.110	Clean	✓ Passthrough	FTP

Total logs stored for analytics: 60 days 9 hours.

Show 100 Total 14

3. Click the *FortiSandbox Scan* link to view the *Sandbox Execution Details* panel.



User Name 10.2.60.143 (10.2.60.143)
OS Windows
Session ID 3424149
Policy ID/UUID 1/eb60fbe8-4da1-51e8-2583-6f5367f5d73
FortiSandbox Scan Time 2019-02-07 11:05:26

Sandbox Execution Details

File Name /Storage/ftp/jobs/4278629880706693398/4278629880706693398
Analysis Malicious
Service exe

Fabric connectors

This section contains the following topics:

- Configuring a ServiceNow connector on page 15
- Creating a Google Cloud connector on page 18

Configuring a ServiceNow connector

Admins can use ServiceNow to manage incidents and events with the FortiAnalyzer App. To notify ServiceNow when an incident is raised in FortiAnalyzer, create a fabric connector, then enable notifications for the fabric connector you created.

Before you begin, ensure you have completed the following tasks in ServiceNow:

- Install the ServiceNow FortiAnalyzer App.
- Go to *FortiAnalyzer App* > *FortiAnalyzer System Properties*, and create a connection for the ServiceNow API.

To integrate FortiAnalyzer with ServiceNow:

1. Record the ServiceNow API URL.
2. Create a fabric connector for ServiceNow.
3. Enable notifications to notify ServiceNow when an incident is raised.

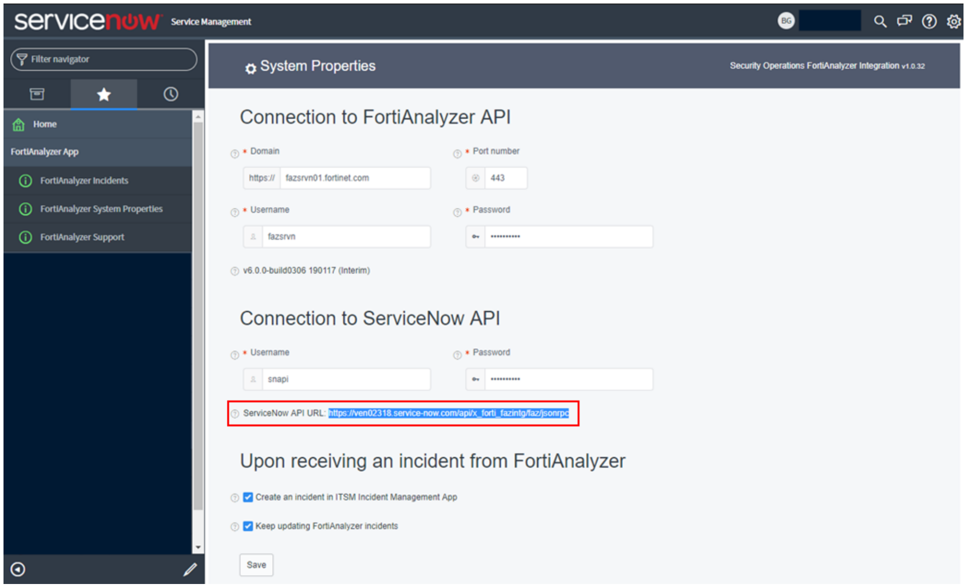
Locating your ServiceNow API URL

You will need to know the ServiceNow API URL and login credentials to create a fabric connector in FortiAnalyzer.

To locate your ServiceNow API URL:

1. Open ServiceNow and go to *FortiAnalyzer App* > *FortiAnalyzer System Properties*.

2. In the *Connection to ServiceNow API* section, copy the URL in the *ServiceNow API URL* field.


servicenow Service Management
BG [redacted]
Filter navigator
Home
FortiAnalyzer App
FortiAnalyzer Incidents
FortiAnalyzer System Properties
FortiAnalyzer Support
System Properties
Security Operations FortiAnalyzer Integration v1.0.32

Connection to FortiAnalyzer API

* Domain: https:// fazsrvn01.fortinet.com

* Port number: 443

* Username: fazsrvn

* Password: **********

v6.0.0-build0306 190117 (Interim)

Connection to ServiceNow API

* Username: snapi

* Password: **********

ServiceNow API URL: https://ven02318.service-now.com/api/x_forti_fazintg/faz/jsonrpc

Upon receiving an incident from FortiAnalyzer

☑ Create an incident in ITSM Incident Management App

☑ Keep updating FortiAnalyzer incidents

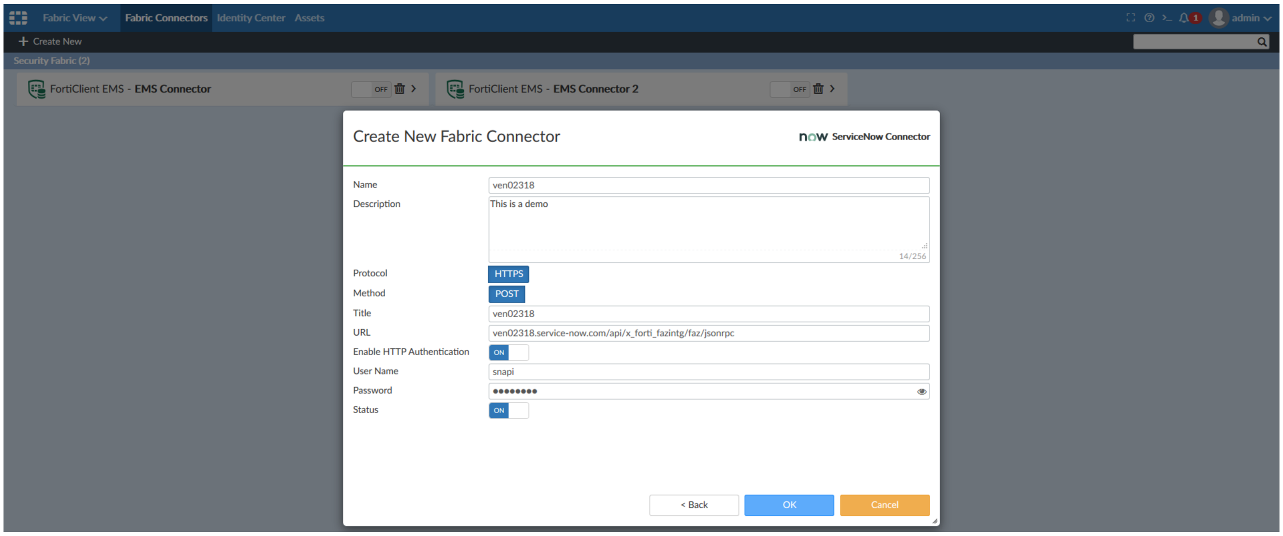
Save

Creating a fabric connector for ServiceNow

You will need to create a fabric connector to notify ServiceNow when an incident is raised in FortiAnalyzer.

To create a fabric connector for ServiceNow:

1. Open FortiAnalyzer and go to *Fabric View* > *Fabric* > *Connectors*.
2. Click *Create New*.
   The *Create New Fabric Connector* dialog opens.
3. Select the *ServiceNow* connector type.
4. Configure the fabric connector:



Create New Fabric Connector

Name: ven02318

Description: This is a demo (14/256)

Protocol: HTTPS

Method: POST

Title: ven02318

URL: ven02318.service-now.com/api/x_forti_fazintg/faz/jsonrpc

Enable HTTP Authentication: ON

User Name: snapi

Password: ••••••••

Status: ON

Name	Type a name for the fabric connector. The name cannot be changed once the fabric connector is created.
Description	(Optional) Type a description for the fabric connector. You can change the description after the fabric connector is created.
Protocol	Select HTTPS.
Method	Select POST.
Title	Type a title for the fabric connector. You can change the title after the fabric connector is created.
URL	Type the ServiceNow API URL located in *FortiAnalyzer App* > *FortiAnalyzer System Propertie*s.
User Name	Type the Username located in *FortiAnalyzer App* > *FortiAnalyzer System Properties*.
Password	Type the Password located in *FortiAnalyzer App* > *FortiAnalyzer System Properties*.
Status	Toggle *ON* to enable the fabric connector.

5. Click *OK*.

Sending notifications to ServiceNow

You will need to enable notifications in FortiAnalyzer to trigger an incident in ServiceNow:

To enable notifications in FortiAnalyzer:

1. Go to *FortiSoC* > *Incidents*.
2. Click *Settings* in the toolbar.
3. From the *Fabric Connector 1* dropdown, select the fabric connector you created for ServiceNow.
4. Select the notification icon settings, and click *OK*.

Creating a Google Cloud connector

When logs hit a certain size, they rollover and begin deleting the earliest entries to make room for additional logs. To prevent losing any log entries, FortiAnalyzer can periodically back up older logs to an external object storage location in Google Cloud. This off-site log archive will help ensure compliance and data redundancy in case there is a local storage or outage in FortiAnalyzer.

To create a Google Cloud connector:

1. Create a storage bucket on Google Cloud. See Configuring a Google Cloud storage bucket on page 18
2. Locate your Google Cloud Platform information. See Locating your Google Cloud information on page 20
3. Import the required CA certificates on FortiAnalyzer. See Importing the CA certificate on page 23
4. Create a cloud connector on FortiAnalyzer. See Creating the cloud connector on page 24
5. Test the connector. See Testing the Google Cloud connector on page 26.

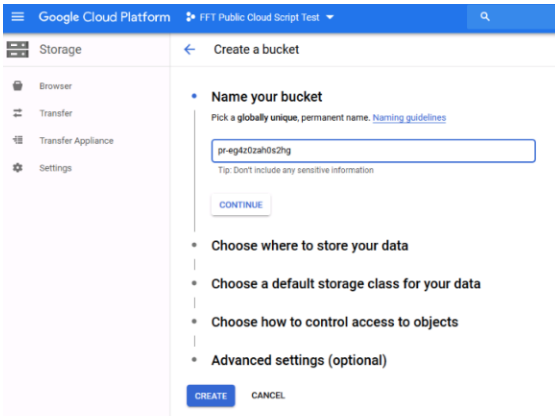
Configuring a Google Cloud storage bucket

Google storage buckets must be globally unique. For simplicity, this example uses the project name. However, you can use any name you like.

For more information about creating Google storage buckets, see the product help.

To create a Google storage bucket:

1. Open the Cloud Storage browser in the Google Cloud Console and click *Create Bucket.*
2. Enter a name for the bucket.



Name your bucket

Pick a **globally unique**, permanent name. Naming guidelines

pr-eg4z0zah0s2hg

Tip: Don't include any sensitive information

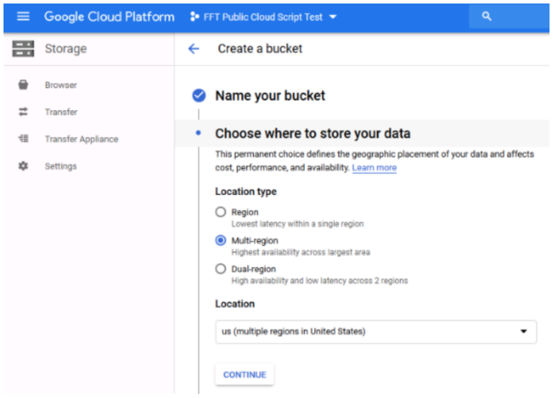
Choose where to store your data

Choose a default storage class for your data

Choose how to control access to objects

Advanced settings (optional)

3. Select a region for the bucket. You will need this location when you create a cloud connector in FortiAnalyzer.



Name your bucket

Choose where to store your data

This permanent choice defines the geographic placement of your data and affects cost, performance, and availability. Learn more

Location type

○ Region
Lowest latency within a single region

● Multi-region
Highest availability across largest area

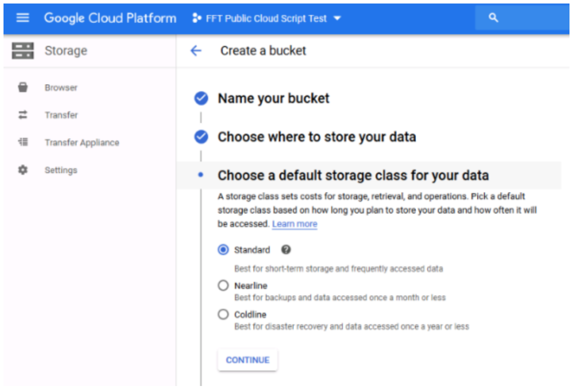
○ Dual-region
High availability and low latency across 2 regions

Location

us (multiple regions in United States)

CONTINUE

4. Set the object storage type to standard.



Name your bucket

Choose where to store your data

Choose a default storage class for your data

A storage class sets costs for storage, retrieval, and operations. Pick a default storage class based on how long you plan to store your data and how often it will be accessed. Learn more

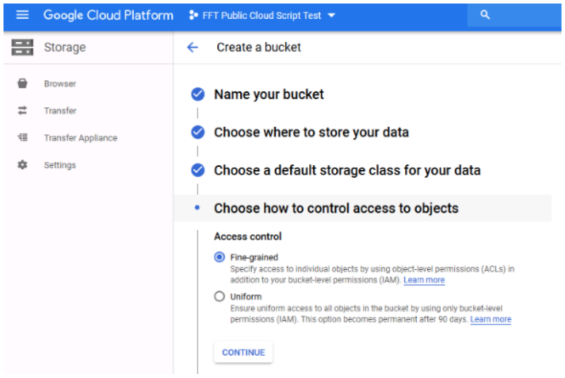
● Standard
Best for short-term storage and frequently accessed data

○ Nearline
Best for backups and data accessed once a month or less

○ Coldline
Best for disaster recovery and data accessed once a year or less

CONTINUE

5. Set the access control to *Fine grained*.



Name your bucket

Choose where to store your data

Choose a default storage class for your data

Choose how to control access to objects

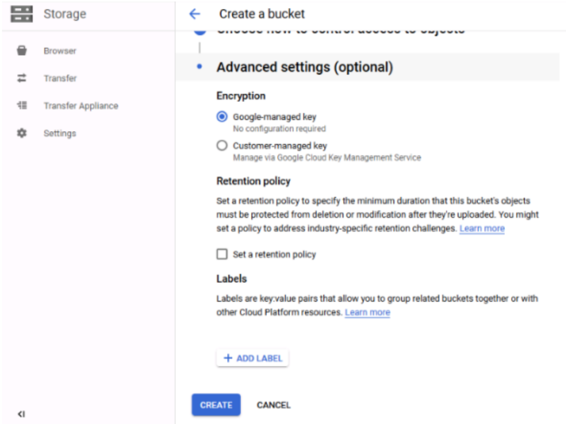
Access control

● Fine-grained
Specify access to individual objects by using object-level permissions (ACLs) in addition to your bucket-level permissions (IAM). Learn more

○ Uniform
Ensure uniform access to all objects in the bucket by using only bucket-level permissions (IAM). This option becomes permanent after 90 days. Learn more

CONTINUE

6. Set the encryption to *Google-managed key*.



Advanced settings (optional)

Encryption

● Google-managed key
No configuration required

○ Customer-managed key
Manage via Google Cloud Key Management Service

Retention policy

Set a retention policy to specify the minimum duration that this bucket's objects must be protected from deletion or modification after they're uploaded. You might set a policy to address industry-specific retention challenges. Learn more

□ Set a retention policy

Labels

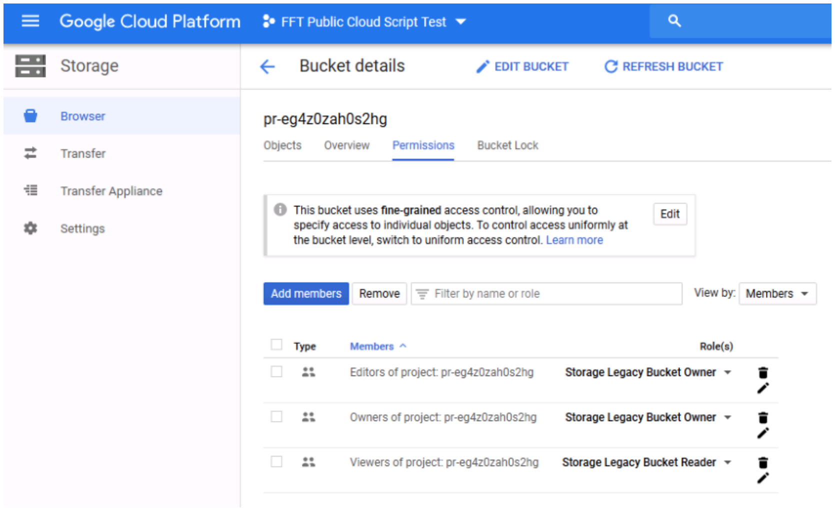
Labels are key:value pairs that allow you to group related buckets together or with other Cloud Platform resources. Learn more

7. Click *Create*.

To view the bucket details:

Go to *Storage* > *Browser*.

- Use the *Objects* tab to test the cloud connector. See Testing the Google Cloud connector on page 26.
- Use the *Permissions* tab to see who can access this bucket. The Google account JSON key will be tied to these permissions. See Locating your Google Cloud information on page 20.



pr-eg4z0zah0s2hg

This bucket uses **fine-grained** access control, allowing you to specify access to individual objects. To control access uniformly at the bucket level, switch to uniform access control. Learn more

□	Type	Members	Role(s)
□	👥	Editors of project: pr-eg4z0zah0s2hg	Storage Legacy Bucket Owner
□	👥	Owners of project: pr-eg4z0zah0s2hg	Storage Legacy Bucket Owner
□	👥	Viewers of project: pr-eg4z0zah0s2hg	Storage Legacy Bucket Reader

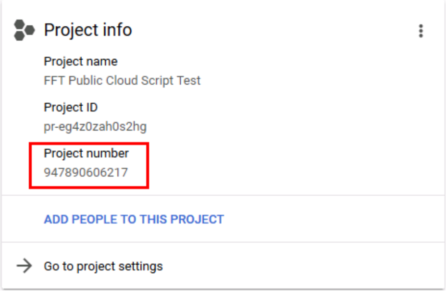
Locating your Google Cloud information

Some information is required from Google Cloud in order to create a storage connector on FortiAnalyzer.

To locate a Google project number:

1. Open the project in Google Cloud Platform.
2. Open the *Home* page.

3. Locate the *Project Info* widget and copy the *Project Number*.



Project info

Project name
FFT Public Cloud Script Test

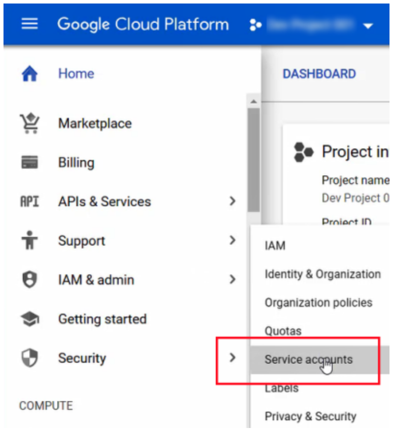
Project ID
pr-eg4z0zah0s2hg

Project number
947890606217

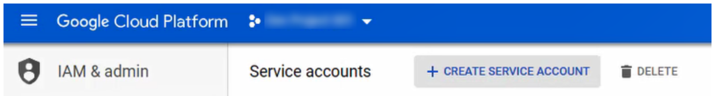
To create a Google service account key:

A private key is required to create a fabric connector for Google Cloud. After you create the key, save it to your computer and paste the entire contents of the JSON file in the *Service Account Credentials* field when you create the cloud connector. You can download an existing service account key from the bucket details page.

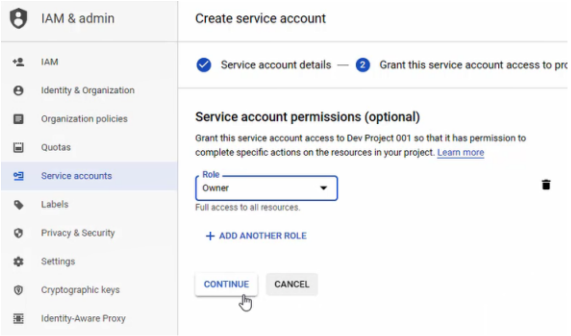
1. Open your project in Google Cloud Platform.
2. In the Navigation pane, go to *IAM & admin* > *Service Accounts*. The *Service accounts* page opens.



3. Click *Create Service Account*. The *Create service account* page opens.



4. Type the *Service account name*, *Service account ID*, and *Service account description*, then click *Create*.
5. Select the account permissions from the *Role* dropdown, then click *Continue*.

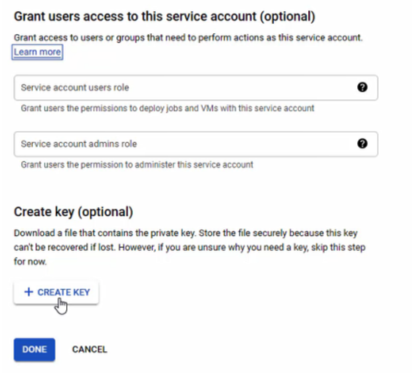


Service account permissions (optional)

Grant this service account access to Dev Project 001 so that it has permission to complete specific actions on the resources in your project. Learn more

Role
Owner
Full access to all resources.

6. In the *Grant users access to this service account* section, click *Create Key*.



Grant users access to this service account (optional)

Grant access to users or groups that need to perform actions as this service account. Learn more

Service account users role

Grant users the permissions to deploy jobs and VMs with this service account

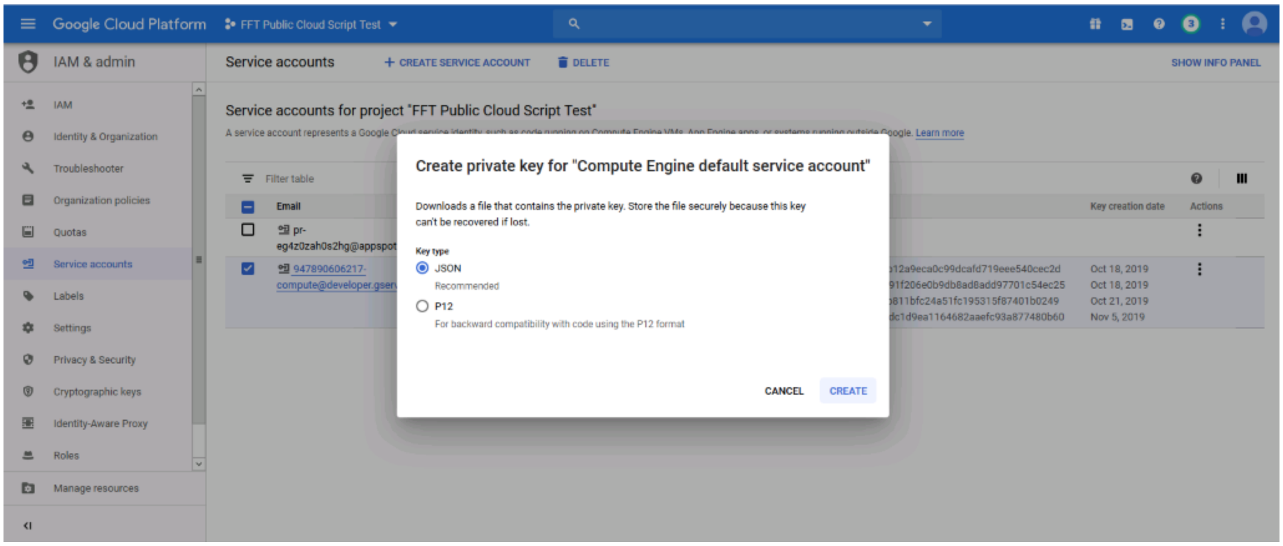
Service account admins role

Grant users the permission to administer this service account

Create key (optional)

Download a file that contains the private key. Store the file securely because this key can't be recovered if lost. However, if you are unsure why you need a key, skip this step for now.

7. Click *Create* and save your key to your computer.



Service accounts for project "FFT Public Cloud Script Test"

A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. Learn more

Email		Key creation date	Actions
☐ pr-eg4z0zah0s2hg@appspot			⋮
☑ 947890606217-compute@developer.gser	12a9eca0c99dcafd719eee540cec2d 91f206e0b9db8ad8add97701c54ec25 811bfc24a51fc195315f87401b0249 dc1d9ea1164682aaefc93a877480b60	Oct 18, 2019 Oct 18, 2019 Oct 21, 2019 Nov 5, 2019	⋮

Create private key for "Compute Engine default service account"

Downloads a file that contains the private key. Store the file securely because this key can't be recovered if lost.

Key type

● JSON
Recommended

○ P12
For backward compatibility with code using the P12 format

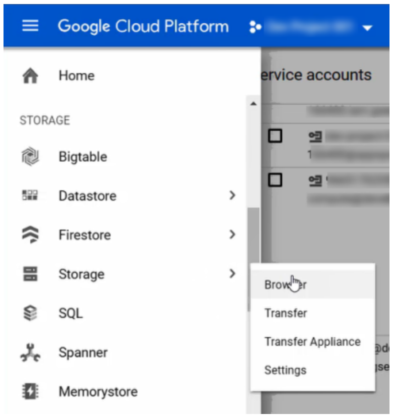
CANCEL CREATE

8. Paste the entire contents of the JSON file in the *Service Account Credentials* field when you create the cloud connector.

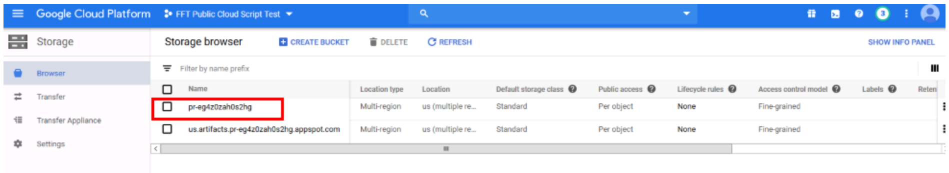
To locate the remote path in Google Cloud:

Use the Google bucket name for the Remote Path in the Device Logs Settings. The bucket name is also the name of the fabric connector.

1. In the navigation pane, go to *Storage* > *Browser*.



2. Copy the name of the bucket as it appears in the *Name* column and paste it into the *Remote Path* field when you create the cloud connector.



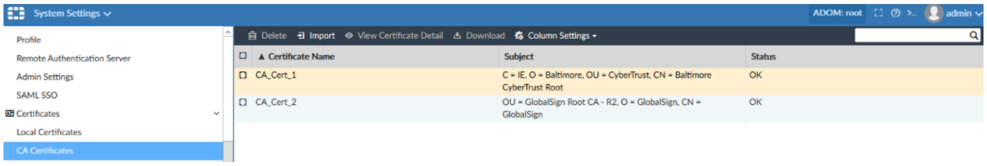
Name	Location type	Location	Default storage class	Public access	Lifecycle rules	Access control model	Labels	Reten
pr-eg4z0zah0s2hg	Multi-region	us (multiple re...	Standard	Per object	None	Fine-grained		
us.artifacts.pr-eg4z0zah0s2hg.appspot.com	Multi-region	us (multiple re...	Standard	Per object	None	Fine-grained		

Importing the CA certificate

Google requires you provide CyberTrust and GlobalSign certificates when creating a cloud object.

To import a CA certificate:

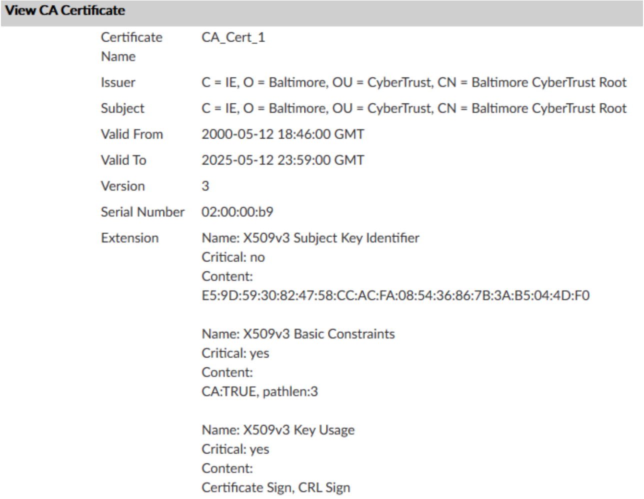
1. Go to *System Settings* > *Certificates* > *CA Certificates*.
2. Click *Import* in the toolbar, or right-click and select *Import*. The Import dialog box opens.
3. Click *Browse...* and locate the certificate file on the management computer, or drag and drop the file onto the dialog box.
4. Click *OK* to import the certificate.



Certificate Name	Subject	Status
CA_Cert_1	C = IE, O = Baltimore, OU = CyberTrust, CN = Baltimore CyberTrust Root	OK
CA_Cert_2	OU = GlobalSign Root CA - R2, O = GlobalSign, CN = GlobalSign	OK

To view a CA certificate's details:

1. Go to *System Settings* > *Certificates* > *CA Certificates*.
2. Select the certificates you need to see details about.
3. Click *View Certificate Detail* in the toolbar, or right-click and select *View Certificate Detail*. The *View CA Certificate* page opens.



View CA Certificate

Certificate Name	CA_Cert_1
Issuer	C = IE, O = Baltimore, OU = CyberTrust, CN = Baltimore CyberTrust Root
Subject	C = IE, O = Baltimore, OU = CyberTrust, CN = Baltimore CyberTrust Root
Valid From	2000-05-12 18:46:00 GMT
Valid To	2025-05-12 23:59:00 GMT
Version	3
Serial Number	02:00:00:b9
Extension	Name: X509v3 Subject Key Identifier Critical: no Content: E5:9D:59:30:82:47:58:CC:AC:FA:08:54:36:86:7B:3A:B5:04:4D:F0 Name: X509v3 Basic Constraints Critical: yes Content: CA:TRUE, pathlen:3 Name: X509v3 Key Usage Critical: yes Content: Certificate Sign, CRL Sign

4. Click *OK* to return to the CA certificates list.

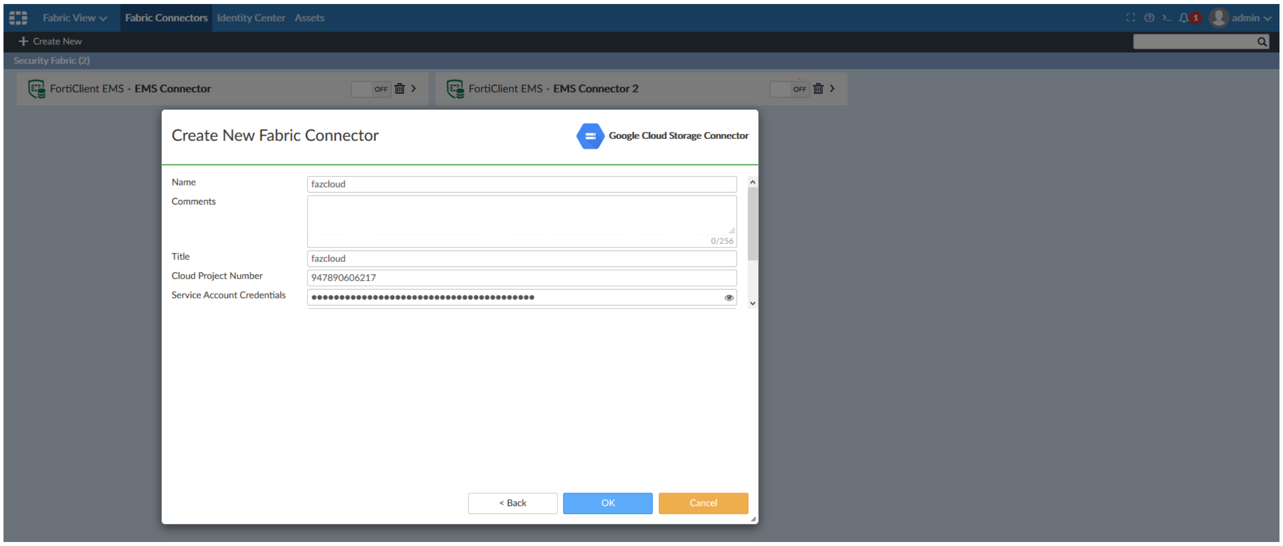
Creating the cloud connector

Before you begin creating a Google Cloud connector, ensure you have:

- Imported the required CA certificates.
- Downloaded the private key from Google Cloud.

To create a Google Cloud connector:

1. Go to *Fabric View* > *Fabric* > *Connectors*, and click *Create New* in the toolbar. The *Create New Fabric Connector* dialog opens.
2. In the *Storage* section, click *Google Cloud Storage Connector*.
3. Configure the fabric connector settings, then click *OK*.



Create New Fabric Connector

Name: fazcloud

Comments: 0/256

Title: fazcloud

Cloud Project Number: 947890606217

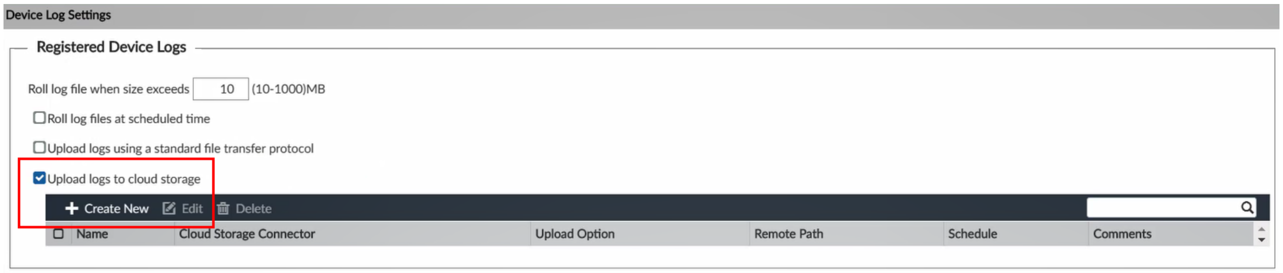
Service Account Credentials: ••

Property	Description
Name	Type a name for the fabric connector.
Comments	(Optional) Add comments about the connector.
Title	Type a title for the fabric connector.
Cloud Project Number	Type the project number from the Google Cloud Platform dashboard. See Locating your Google Cloud information on page 20.
Service Account Credentials	Paste the entire Google account JSON key into the field. Click the eye icon to *Show* or *Hide* the key. See Locating your Google Cloud information on page 20.
Cloud Location	Type the bucket region. See Creating a Google storage bucket See Locating your Google Cloud information on page 20.

The fabric connector appears in the *Fabric Connectors* pane.

To roll the logs to Google Cloud:

1. Go to *System Settings* > *Advanced* > *Device Log Settings*.
2. In the *Registered Device Logs* section, click *Upload logs to cloud storage* > *Create New*.



Device Log Settings

Registered Device Logs

Roll log file when size exceeds 10 (10-1000)MB

□ Roll log files at scheduled time

□ Upload logs using a standard file transfer protocol

☑ Upload logs to cloud storage

□	Name	Cloud Storage Connector	Upload Option	Remote Path	Schedule	Comments

3. Configure the following cloud storage settings and click *OK*.

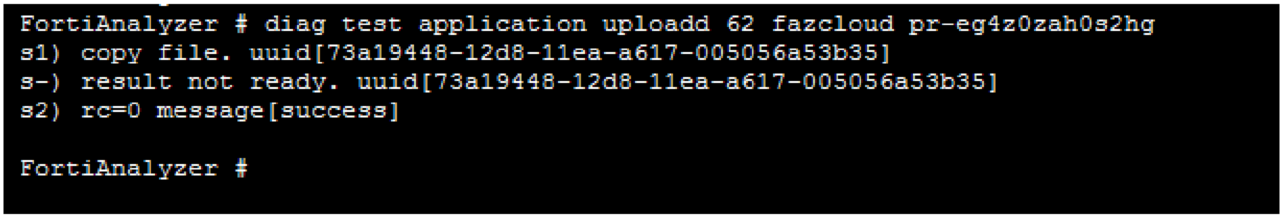
Property	Description
Cloud Storage Connector	Type the name you gave to the fabric connector.
Remote Path	Type the globally unique name you gave to your bucket. For simplicity use the project name. See Locating your Google Cloud information on page 20.
Upload option	Choose between *Rolling* or *Schedule*.

Testing the Google Cloud connector

You can use the CLI console to test the cloud connector before the logs have rolled over or a scheduled backup is performed.

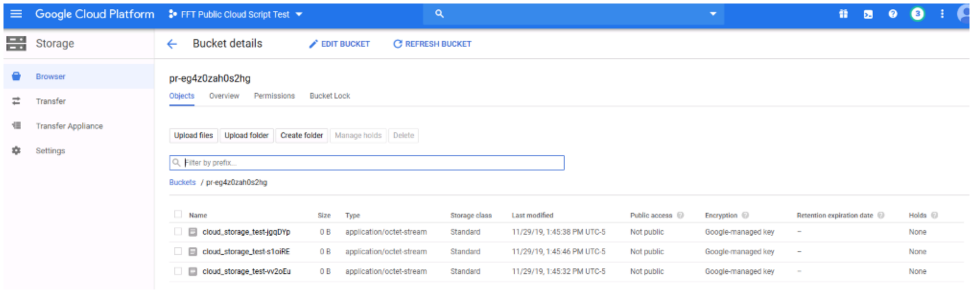
To test a cloud connector:

1. Open the CLI console and type: `diag test application uploadd 62 <connector name> <bucket name>`.
   If the connector is working, the output will show `success`.



```
FortiAnalyzer # diag test application uploadd 62 fazcloud pr-eg4z0zah0s2hg
s1) copy file. uuid[73a19448-12d8-11ea-a617-005056a53b35]
s-) result not ready. uuid[73a19448-12d8-11ea-a617-005056a53b35]
s2) rc=0 message[success]

FortiAnalyzer #
```

2. Go to the storage bucket on Google Cloud and look for the test files you uploaded.



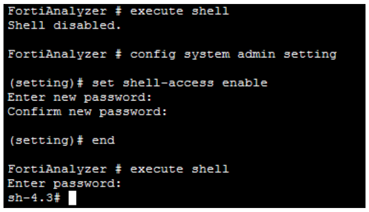
pr-eg4z0zah0s2hg

Buckets / pr-eg4z0zah0s2hg

Name	Size	Type	Storage class	Last modified	Public access	Encryption	Retention expiration date	Holds
cloud_storage_test-jgqDYp	0 B	application/octet-stream	Standard	11/29/19, 1:45:38 PM UTC-5	Not public	Google-managed key	–	None
cloud_storage_test-s1oiRE	0 B	application/octet-stream	Standard	11/29/19, 1:45:46 PM UTC-5	Not public	Google-managed key	–	None
cloud_storage_test-vv2oEu	0 B	application/octet-stream	Standard	11/29/19, 1:45:32 PM UTC-5	Not public	Google-managed key	–	None

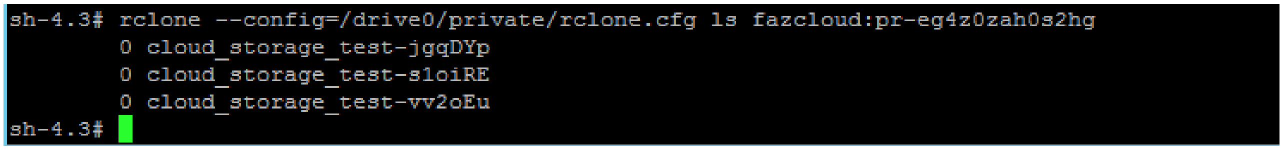
To test a cloud connector with a shell prompt:

1. With the default settings, access to shell will give the following message:
```
FAZ1000D # execute shell
   Shell disabled.
```
2. Use the following commands to enable shell on the FortiAnalyzer:
```
FAZ1000D # config system admin setting
   (setting)# set shell-access enable
      Enter new password: *****
      Confirm new password: *****
   FAZ1000D # end
```
3. The shell is now enabled.
```
FAZ1000D # execute shell
   Enter password:
      sh-4.3#
      sh-4.3#
```
Open the CLI console on any page and type: `rclone --config=/drive0/private/rclone.cfg ls <connector-name>:<bucketname>`



```
FortiAnalyzer # execute shell
Shell disabled.

FortiAnalyzer # config system admin setting

(setting)# set shell-access enable
Enter new password:
Confirm new password:

(setting)# end

FortiAnalyzer # execute shell
Enter password:
sh-4.3#
```

If the connector is working, you will not see any errors.



```
sh-4.3# rclone --config=/drive0/private/rclone.cfg ls fazcloud:pr-eg4z0zah0s2hg
        0 cloud_storage_test-jgqDYp
        0 cloud_storage_test-s1oiRE
        0 cloud_storage_test-vv2oEu
sh-4.3#
```

SOAR and SIEM

This section contains the following topics:

Event handler example scenarios

Custom event handler example

Event handlers can be created to trigger events based on a variety of conditions. By viewing logs in a raw format, you can identify notable log fields and apply corresponding filters in event handlers so that similar logs will trigger an event. For more information on viewing raw logs in FortiAnalyzer, see the FortiAnalyzer Administration Guide.

In this scenario, information from the following raw log is used to create a custom event handler.

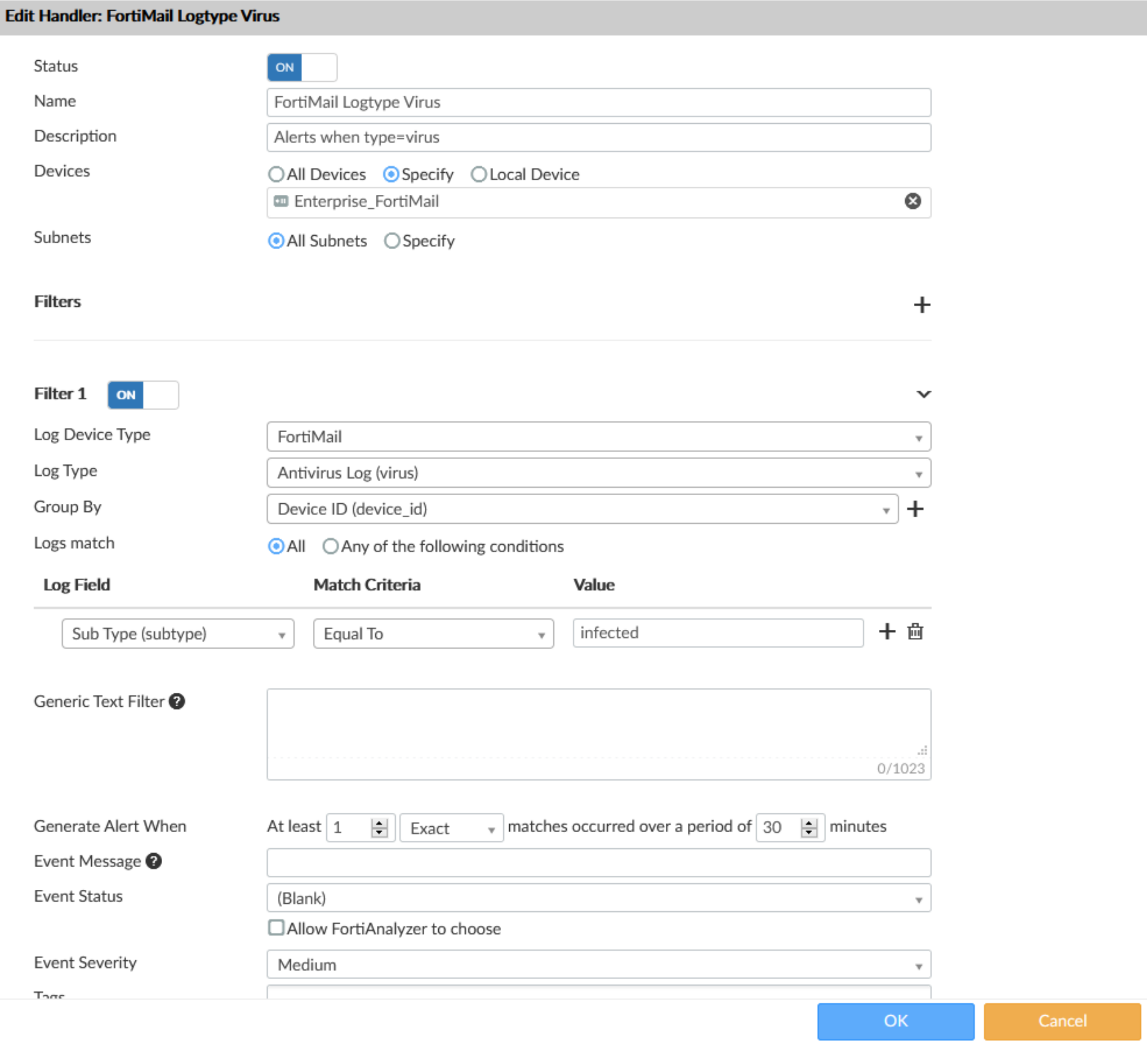
```
date="2020-08-02" time="09:49:57" id=6856321710715568162 bid=8050516 dvid=1039
itime=1596361797 euid=1 epid=1 dsteuid=1 dstepid=1 log_id="0100026477" type="virus"
subtype="infected" pri="information" from="qa200@qa.ca" to="user10@6.ca"
src="172.20.140.108" session_id="s7Q4T9no026475-s7Q4T9pw026475" msg="The file virus_
samples/sandbox/1385973112552098.172.16.92.92.3 is infected with W32/DomaIQ.AN!tr."
device_id="FE-2KB3R09690010" vd="root" devname="FE-2KB3R09690010"
```

This log contains information about malware detected by FortiMail. Two notable fields are the log type, `type=virus`, and the subtype, `subtype=infected`.

Using this information, you can create an event handler which identifies these fields and generates an alert whenever FortiMail logs include these definitions, indicating the presence of an infection.

To create the custom event handler:

1. Go to *FortiSoC* > *Handlers* > *Event Handler List*, and click *Create New*.
2. Enter a name and description (optional) for the event handler.
3. For *Devices*, select your FortiMail device, and for *Subnets* select *All Subnets*.
4. Configure a filter with the following information:
   a. Log Device Type: FortiMail
   b. Log Type: Antivirus Log (virus)
   c. Group By: Device ID
   d. Logs match: All
   e. Log Field: *Subtype (subtype) Equal To Infected*.
   The remaining settings can be left in their default state. Click *OK* to save the event handler.



Edit Handler: FortiMail Logtype Virus

Status	ON
Name	FortiMail Logtype Virus
Description	Alerts when type=virus
Devices	○ All Devices ● Specify ○ Local Device Enterprise_FortiMail
Subnets	● All Subnets ○ Specify

Filters

Filter 1 ON

Log Device Type	FortiMail
Log Type	Antivirus Log (virus)
Group By	Device ID (device_id)
Logs match	● All ○ Any of the following conditions

Log Field	Match Criteria	Value
Sub Type (subtype)	Equal To	infected

Generic Text Filter	0/1023
Generate Alert When	At least 1 Exact matches occurred over a period of 30 minutes
Event Message	
Event Status	(Blank) □ Allow FortiAnalyzer to choose
Event Severity	Medium
Tags	

When enabled, logs from the selected FortiMail device which include the *Log Type: virus* and *Sub Type: Infected* will generate an event.

Predefined event handler example

In addition to custom event handlers, FortiAnalyzer includes predefined event handlers. Below are example logs that will trigger predefined event handlers when enabled.

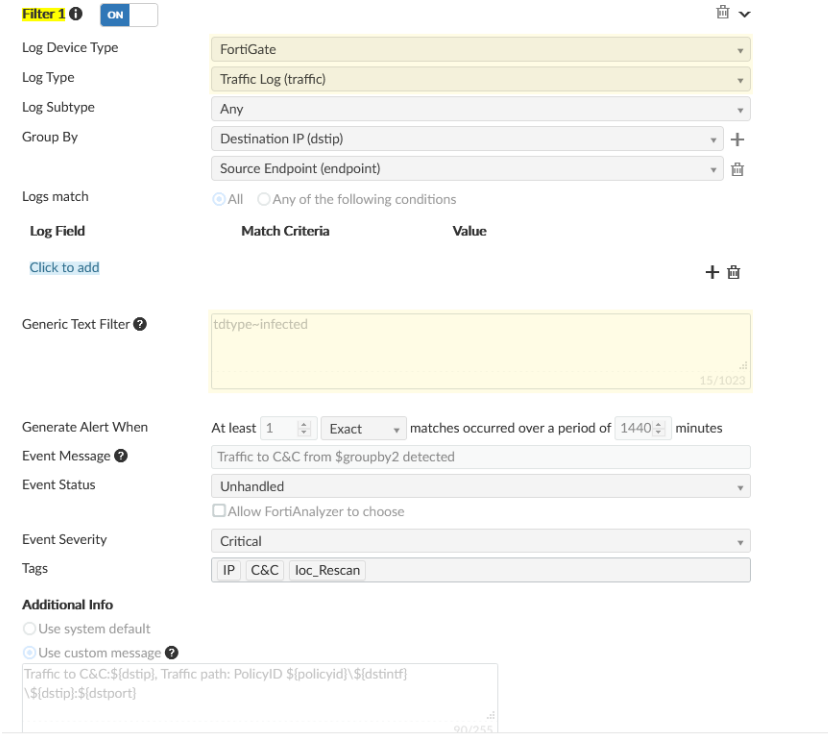
These examples use the *Generic Text filter* field to include specific log information, such as *logid="0422016400*, in the event handler filters.

Default-Compromised Host-Detection-by IOC-By-Threat:

Example log:

```
date="2020-10-02" time="12:54:41" id=6879113766412222465 bid=152167 dvid=1046
itime=1601668486 euid=3 epid=1072 dsteuid=3 dstepid=101 logflag=1 logver=604021723
type="traffic" subtype="forward" level="notice" action="close" policyid=5
sessionid=2126025 srcip="10.200.1.8" dstip="148.81.111.122" srcport=34094 dstport=80
trandisp="noop" duration=1 proto=6 sentbyte=346 rcvdbyte=397 sentpkt=5 rcvdpkt=5
logid="0000000013" srcname="LAN-FSW-GUEST" service="HTTP" app="HTTP" appcat="unscanned"
srcintfrole="lan" dstintfrole="wan" srcserver=0 policytype="policy"
eventtime=1601668481582497121 srcuuid="2de7756a-0343-51eb-c0b5-0d5602c3ecc6"
dstuuid="2de7756a-0343-51eb-c0b5-0d5602c3ecc6" poluuid="528f5f54-0343-51eb-bae9-
3c63f22ce0df" srcmac="00:03:93:6d:8f:fd" mastersrcmac="00:03:93:6d:8f:fd"
srchwvendor="Apple" osname="Linux" srccountry="Reserved" dstcountry="Poland"
srcintf="vsw.port5" dstintf="port1" tdinfoid=7317936224723035242 tdtype="infected-ip"
tdscantime=1601668440 tdthreattype=0 tdthreatname=2 tdwfcate=0 tz="-0700"
devid="FGVM02TM20001234" vd="root" devname="Enterprise_Second_Floor"
```

The above example log triggers Filter 1 in the *Default-Compromised Host-Detection-by IOC-By-Threat* event handler:



Filter 1 ON

Log Device Type: FortiGate

Log Type: Traffic Log (traffic)

Log Subtype: Any

Group By: Destination IP (dstip)
Source Endpoint (endpoint)

Logs match: ● All ○ Any of the following conditions

Log Field	Match Criteria	Value
Click to add		

Generic Text Filter: tdtype~infected (15/1023)

Generate Alert When: At least 1 Exact matches occurred over a period of 1440 minutes

Event Message: Traffic to C&C from $groupby2 detected

Event Status: Unhandled

□ Allow FortiAnalyzer to choose

Event Severity: Critical

Tags: IP C&C Ioc_Rescan

Additional Info

○ Use system default

● Use custom message

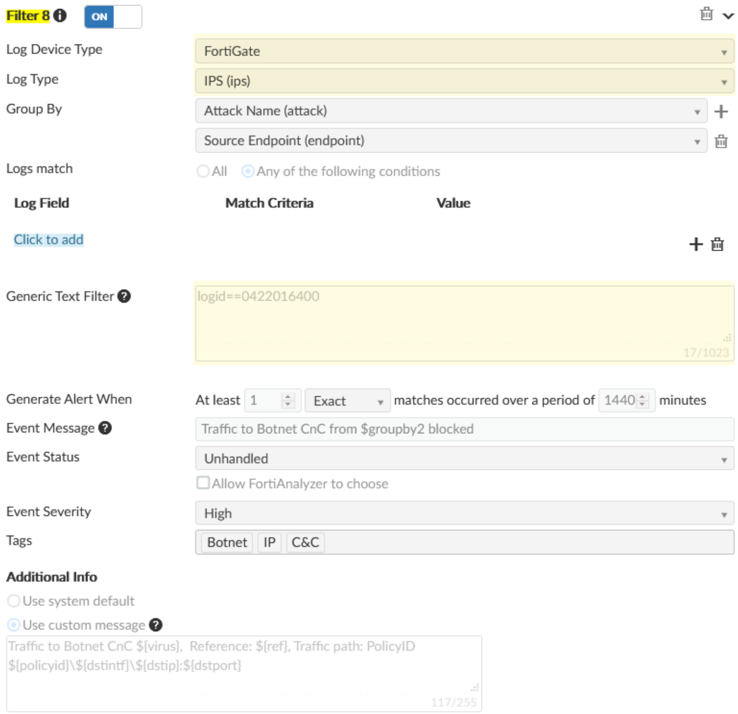
Traffic to C&C:${dstip}, Traffic path: PolicyID ${policyid}\${dstintf}\${dstip}:${dstport} (90/255)

Default-Botnet-Communication-Detection-By-Threat:

Example log:

```
date="2020-10-02" time="12:44:16" id=6879111064877793339 bid=151784 dvid=1043
itime=1601667857 euid=3 epid=1083 dsteuid=3 dstepid=101 logflag=16 logver=604021723
type="utm" subtype="ips" level="warning" action="dropped" sessionid=4398915
srcip="10.100.91.100" dstip="103.226.154.43" srcport=8725 dstport=80 attackid=7630075
severity="critical" proto=6 logid="0422016400" service="HTTP"
eventtime=1601667857379929845 policyid=13 crscore=50 craction=4 crlevel="critical"
srcintfrole="lan" dstintfrole="wan" direction="outgoing" profile="default"
srcintf="port3" dstintf="port1" ref="http://www.fortinet.com/be?bid=7630075"
attack="BlackMoon" eventtype="botnet" srccountry="Reserved" msg="Botnet C&C
Communication." tz="-0700" tdthreatname=20432 devid="FGVM02TM20001234" vd="root"
devname="Enterprise_Core"
```

The above example log triggers Filter 8 in the *Default-Botnet-Communication-Detection-By-Threat* event handler:



Filter 8 ON

Log Device Type: FortiGate

Log Type: IPS (ips)

Group By: Attack Name (attack)
Source Endpoint (endpoint)

Logs match: ○ All ● Any of the following conditions

Log Field	Match Criteria	Value
Click to add		

Generic Text Filter: logid==0422016400 (17/1023)

Generate Alert When: At least 1 Exact matches occurred over a period of 1440 minutes

Event Message: Traffic to Botnet CnC from $groupby2 blocked

Event Status: Unhandled

□ Allow FortiAnalyzer to choose

Event Severity: High

Tags: Botnet IP C&C

Additional Info

○ Use system default

● Use custom message

Traffic to Botnet CnC ${virus}, Reference: ${ref}, Traffic path: PolicyID ${policyid}\${dstintf}\${dstip}:${dstport} (117/255)

Configuring an EMS connector for use in FortiSoC playbooks

Configuring an EMS connector on FortiAnalyzer allows FortiSoC automation playbooks to reach out to endpoints and collect information or take containment actions.

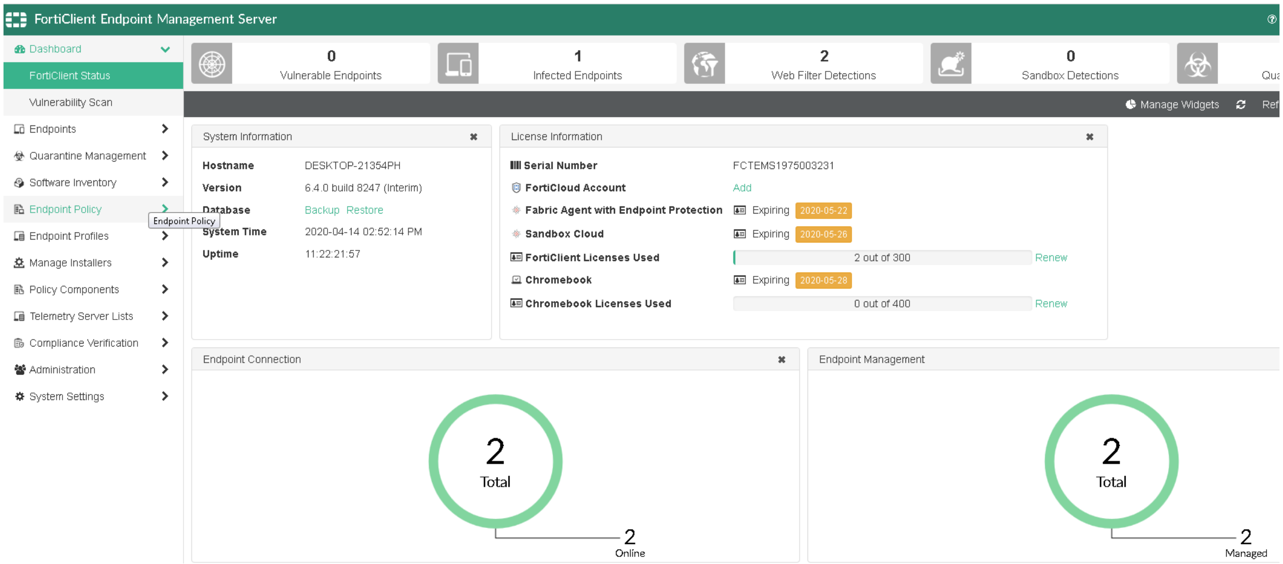
To use EMS connectors in FortiSoC Playbooks:

1. Configure the EMS connector on page 32
2. Create a playbook using the EMS connector on page 35

Configure the EMS connector

To configure an EMS connector for use in FortiSoC playbooks:

1. Configure a FortiClient EMS 6.4.0 server which supports the FortiAnalyzer EMS connector feature.



System Information

Hostname DESKTOP-21354PH
Version 6.4.0 build 8247 (Interim)
Database Backup Restore
System Time 2020-04-14 02:52:14 PM
Uptime 11:22:21:57

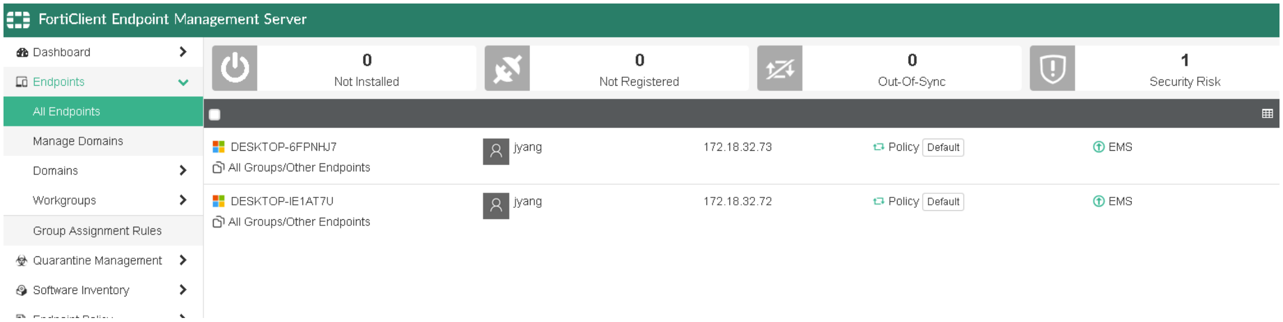
License Information

Serial Number FCTEMS1975003231
FortiCloud Account Add
Fabric Agent with Endpoint Protection Expiring 2020-05-22
Sandbox Cloud Expiring 2020-05-26
FortiClient Licenses Used 2 out of 300 Renew
Chromebook Expiring 2020-05-28
Chromebook Licenses Used 0 out of 400 Renew

Endpoint Connection

Endpoint Management

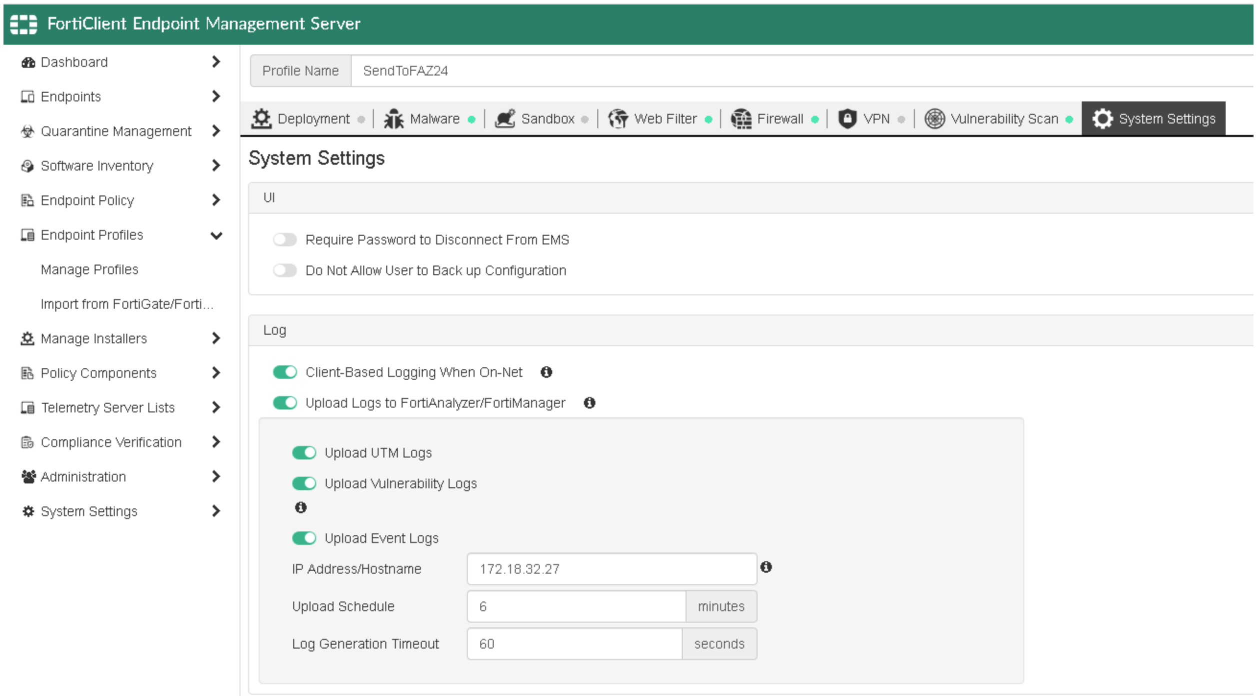
2. Register FortiClient to the EMS server.
   In the example below, two FortiClients have been registered.



DESKTOP-6FPNHJ7 jyang 172.18.32.73 Policy Default EMS
All Groups/Other Endpoints

DESKTOP-IE1AT7U jyang 172.18.32.72 Policy Default EMS
All Groups/Other Endpoints

3. In FortiClient EMS *System Settings*, configure FortiClient EMS to send logs to FortiAnalyzer.



Profile Name: SendToFAZ24

System Settings

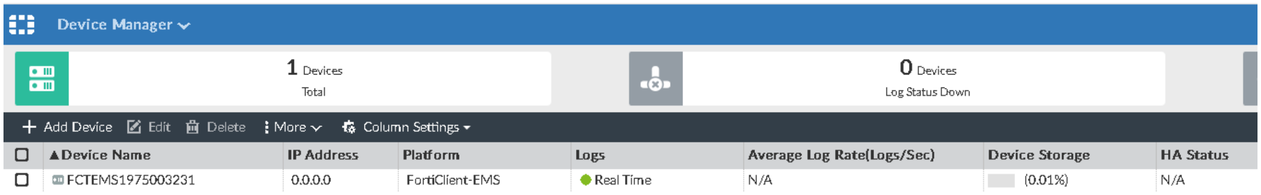
UI

- Require Password to Disconnect From EMS (off)
- Do Not Allow User to Back up Configuration (off)

Log

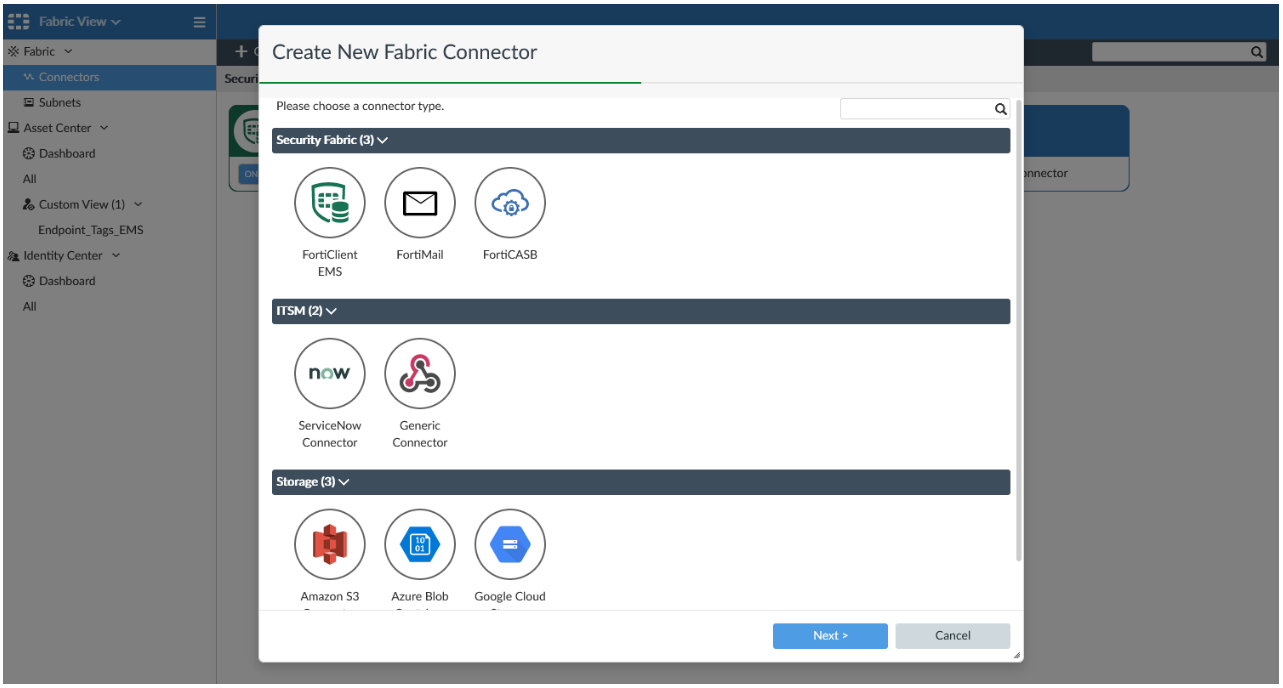
- Client-Based Logging When On-Net (on)
- Upload Logs to FortiAnalyzer/FortiManager (on)
  - Upload UTM Logs (on)
  - Upload Vulnerability Logs (on)
  - Upload Event Logs (on)
  - IP Address/Hostname: 172.18.32.27
  - Upload Schedule: 6 minutes
  - Log Generation Timeout: 60 seconds

4. In FortiAnalyzer, register the EMS device to a Fabric ADOM.

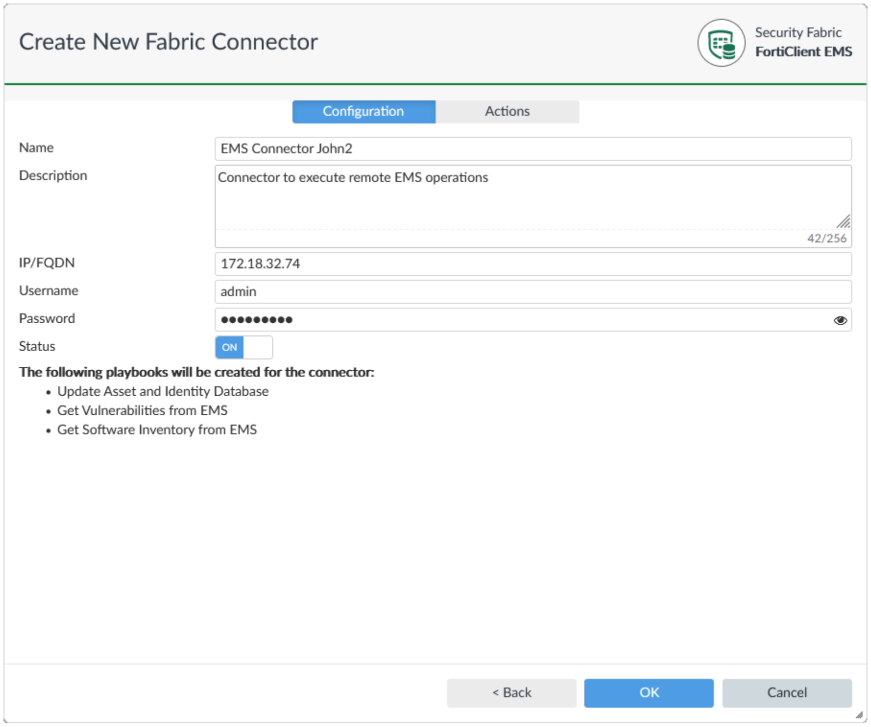


□	▲Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)	Device Storage	HA Status
□	FCTEMS1975003231	0.0.0.0	FortiClient-EMS	● Real Time	N/A	(0.01%)	N/A

5. In the Fabric ADOM, go to *Fabric View* > *Fabric* > *Connectors*. Click *Create New*, and select *FortiClient EMS*.



Configure the EMS connector, and click *OK*.

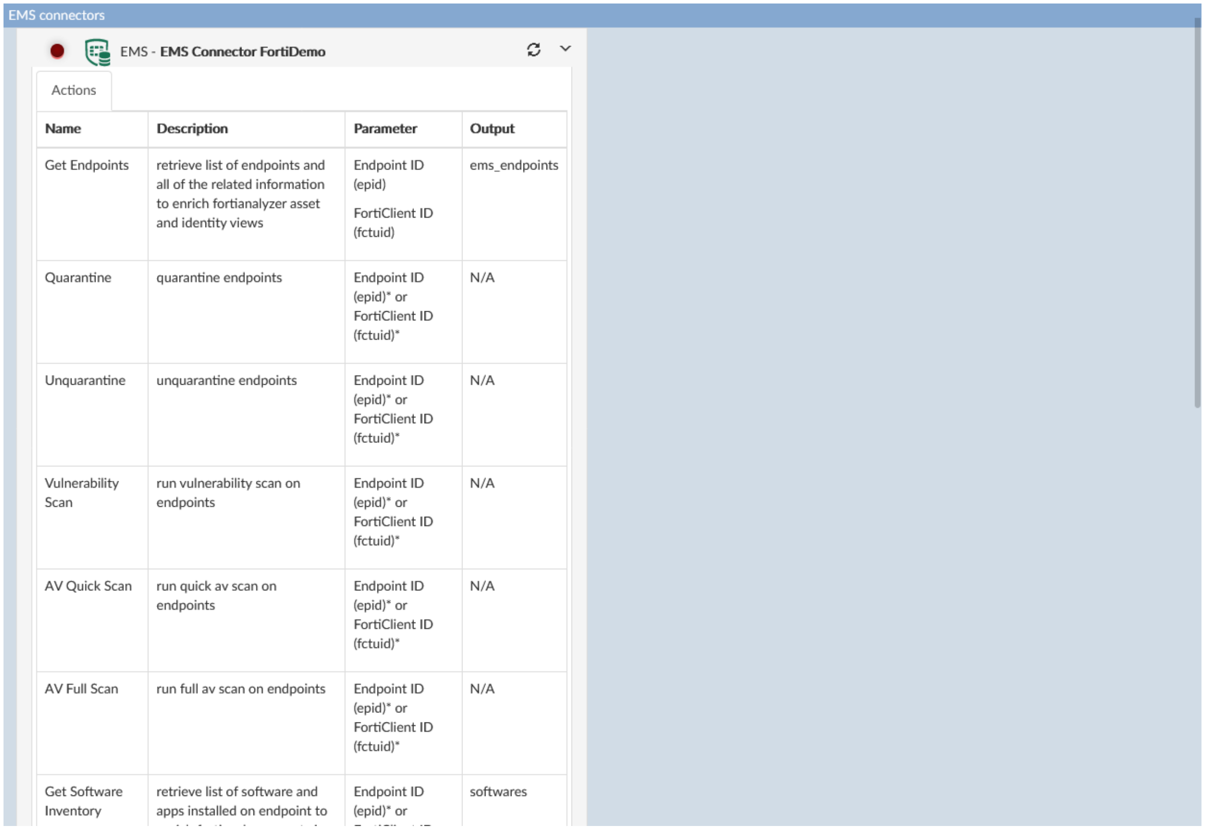


Name	EMS Connector John2
Description	Connector to execute remote EMS operations 42/256
IP/FQDN	172.18.32.74
Username	admin
Password	●●●●●●●●●
Status	ON

The following playbooks will be created for the connector:

- Update Asset and Identity Database
- Get Vulnerabilities from EMS
- Get Software Inventory from EMS

6. Go to *FortiSoC* > *Automation* > *Connectors*. Here you can view the actions FortiAnalyzer can take on endpoints using the EMS connector.



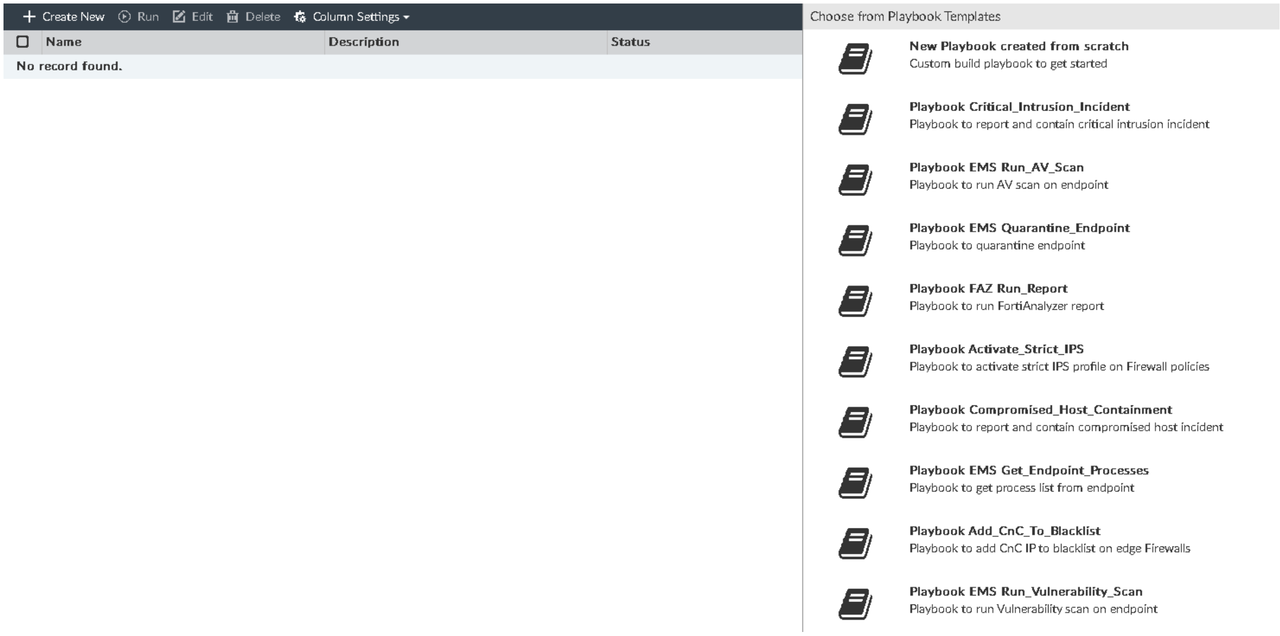
Name	Description	Parameter	Output
Get Endpoints	retrieve list of endpoints and all of the related information to enrich fortianalyzer asset and identity views	Endpoint ID (epid) FortiClient ID (fctuid)	ems_endpoints
Quarantine	quarantine endpoints	Endpoint ID (epid)* or FortiClient ID (fctuid)*	N/A
Unquarantine	unquarantine endpoints	Endpoint ID (epid)* or FortiClient ID (fctuid)*	N/A
Vulnerability Scan	run vulnerability scan on endpoints	Endpoint ID (epid)* or FortiClient ID (fctuid)*	N/A
AV Quick Scan	run quick av scan on endpoints	Endpoint ID (epid)* or FortiClient ID (fctuid)*	N/A
AV Full Scan	run full av scan on endpoints	Endpoint ID (epid)* or FortiClient ID (fctuid)*	N/A
Get Software Inventory	retrieve list of software and apps installed on endpoint to	Endpoint ID (epid)* or	softwares

Create a playbook using the EMS connector

Below are two examples of how FortiSoC playbooks can be configured to use the FortiClient EMS connector to enable actions in FortiAnalyzer.

To create a playbook from a template:

1. Go to *FortiSoC > Automation > Playbook*, and click *Create New*.



□	Name	Description	Status
No record found.			

Choose from Playbook Templates

New Playbook created from scratch
Custom build playbook to get started

Playbook Critical_Intrusion_Incident
Playbook to report and contain critical intrusion incident

Playbook EMS Run_AV_Scan
Playbook to run AV scan on endpoint

Playbook EMS Quarantine_Endpoint
Playbook to quarantine endpoint

Playbook FAZ Run_Report
Playbook to run FortiAnalyzer report

Playbook Activate_Strict_IPS
Playbook to activate strict IPS profile on Firewall policies

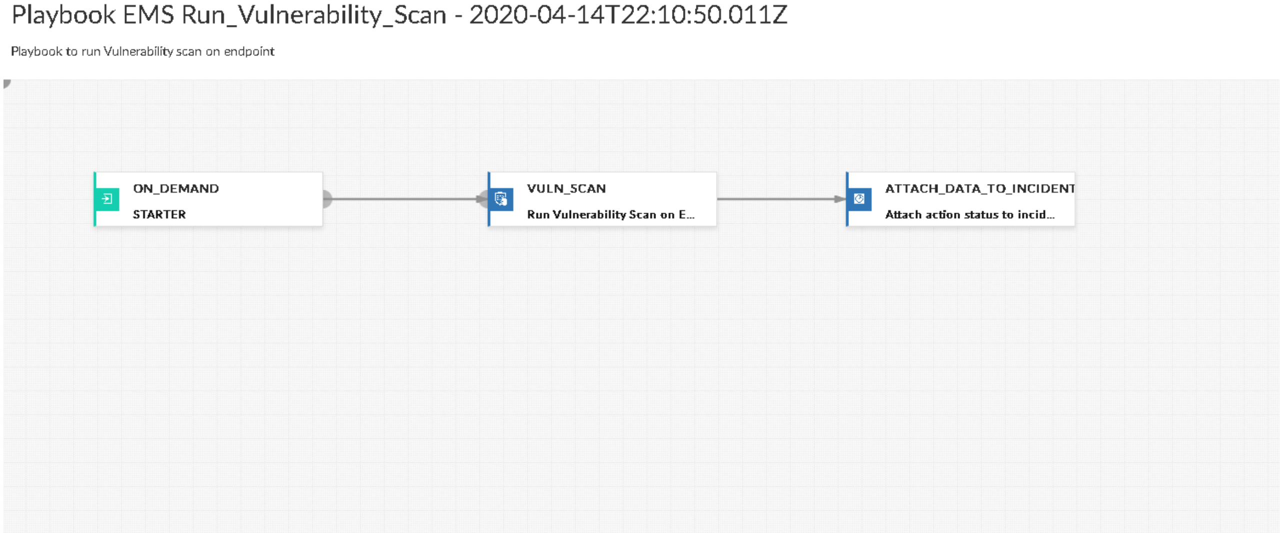
Playbook Compromised_Host_Containment
Playbook to report and contain compromised host incident

Playbook EMS Get_Endpoint_Processes
Playbook to get process list from endpoint

Playbook Add_CnC_To_Blacklist
Playbook to add CnC IP to blacklist on edge Firewalls

Playbook EMS Run_Vulnerability_Scan
Playbook to run Vulnerability scan on endpoint

2. From the list of templates, select *Playbook EMS Run_Vulnerability_Scan*.
   This template will run a vulnerability scan on an endpoint. Save the playbook.

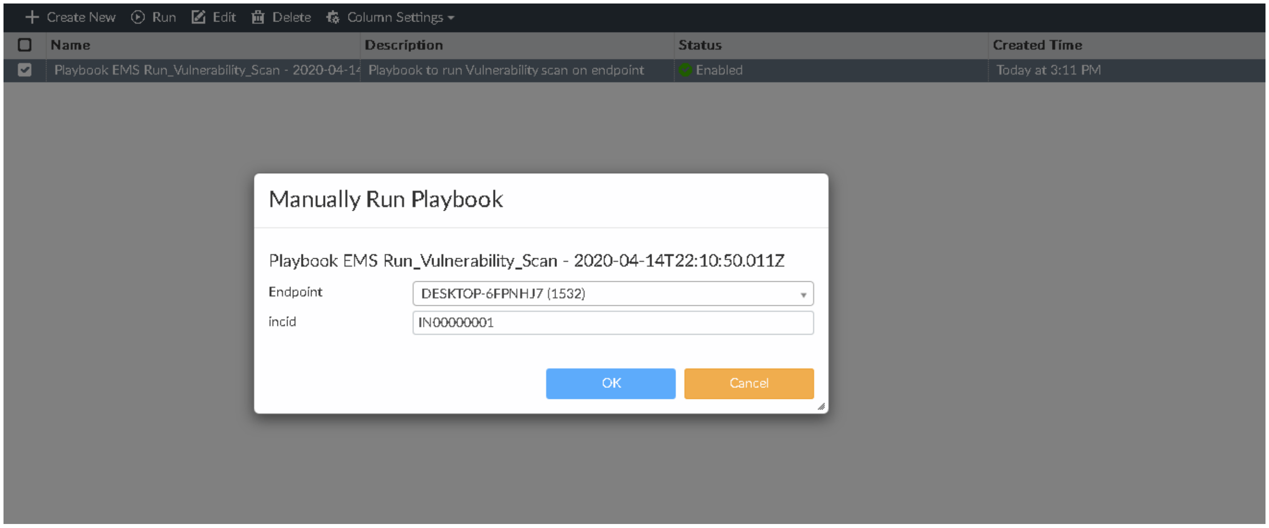


Playbook EMS Run_Vulnerability_Scan - 2020-04-14T22:10:50.011Z

Playbook to run Vulnerability scan on endpoint

ON_DEMAND
STARTER
VULN_SCAN
Run Vulnerability Scan on E...
ATTACH_DATA_TO_INCIDENT
Attach action status to incid...

3. From the Playbook menu, run the playbook.



☐	Name	Description	Status	Created Time
☑	Playbook EMS Run_Vulnerability_Scan - 2020-04-14	Playbook to run Vulnerability scan on endpoint	Enabled	Today at 3:11 PM

Manually Run Playbook

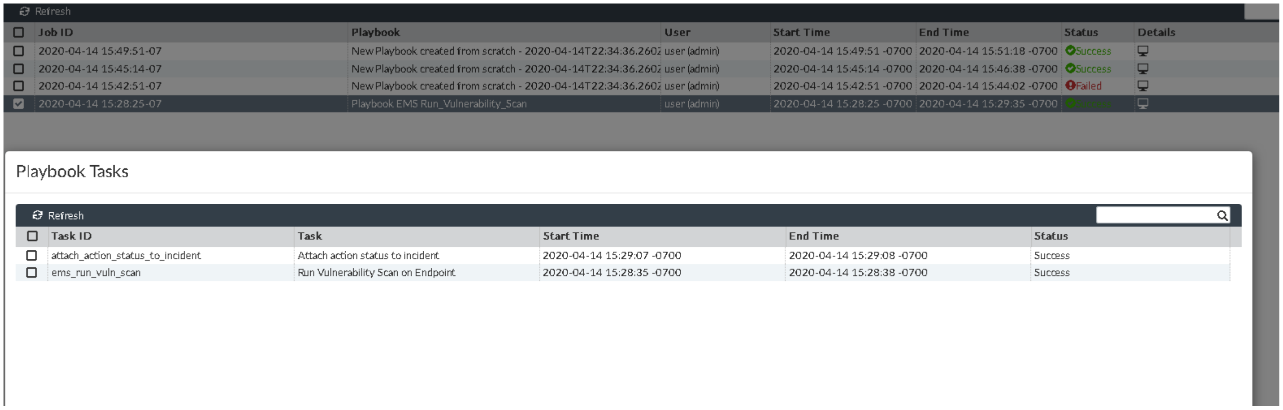
Playbook EMS Run_Vulnerability_Scan - 2020-04-14T22:10:50.011Z

Endpoint: DESKTOP-6FPNHJ7 (1532)

incid: IN00000001

A prompt appears to select the endpoint on which to perform the vulnerability scan. Select the endpoint and enter the ID of the incident that will be updated with information from the scan.

4. Go to *FortiSoC > Automation > Playbook Monitor* to view the running status of the playbook job and confirm it has completed successfully.



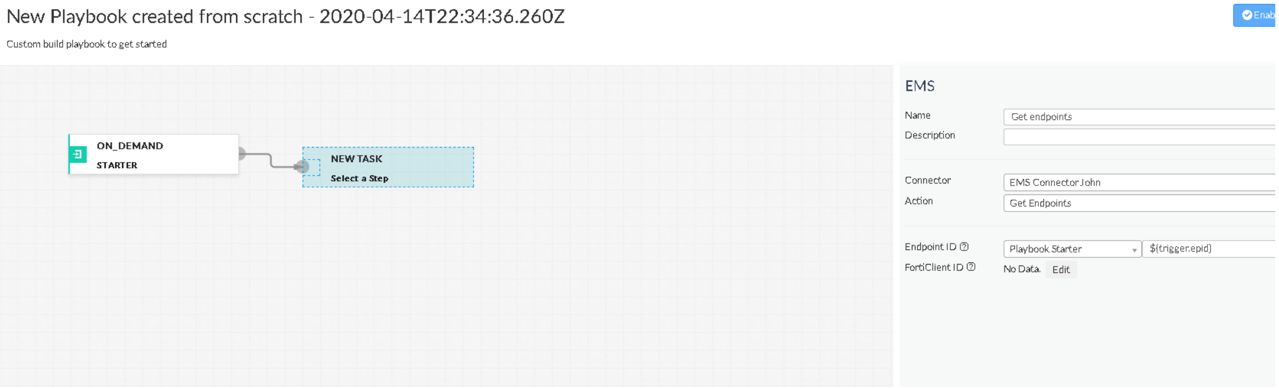
☐	Job ID	Playbook	User	Start Time	End Time	Status	Details
☐	2020-04-14 15:49:51-07	New Playbook created from scratch - 2020-04-14T22:34:36.260Z	user (admin)	2020-04-14 15:49:51 -0700	2020-04-14 15:51:18 -0700	✓Success	🖵
☐	2020-04-14 15:45:14-07	New Playbook created from scratch - 2020-04-14T22:34:36.260Z	user (admin)	2020-04-14 15:45:14 -0700	2020-04-14 15:46:38 -0700	✓Success	🖵
☐	2020-04-14 15:42:51-07	New Playbook created from scratch - 2020-04-14T22:34:36.260Z	user (admin)	2020-04-14 15:42:51 -0700	2020-04-14 15:44:02 -0700	!Failed	🖵
☑	2020-04-14 15:28:25-07	Playbook EMS Run_Vulnerability_Scan	user (admin)	2020-04-14 15:28:25 -0700	2020-04-14 15:29:35 -0700	✓Success	🖵

Playbook Tasks

☐	Task ID	Task	Start Time	End Time	Status
☐	attach_action_status_to_incident	Attach action status to incident	2020-04-14 15:29:07 -0700	2020-04-14 15:29:08 -0700	Success
☐	ems_run_vuln_scan	Run Vulnerability Scan on Endpoint	2020-04-14 15:28:35 -0700	2020-04-14 15:28:38 -0700	Success

To create a playbook from scratch

1. Go to *FortiSoC > Automation > Playbook*, and click *Create New*.
From the list of templates, select *New Playbook created from scratch*.



New Playbook created from scratch - 2020-04-14T22:34:36.260Z

Custom build playbook to get started

EMS

Name: Get endpoints

Description:

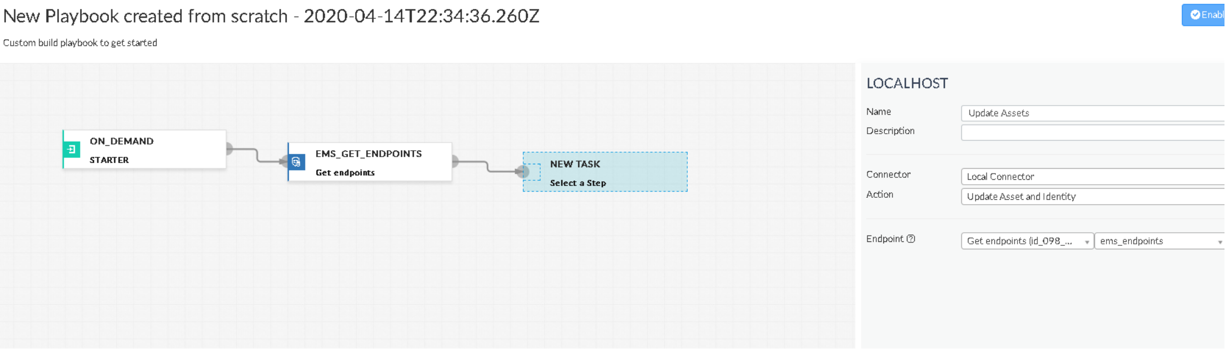
Connector: EMS Connector John

Action: Get Endpoints

Endpoint ID: Playbook Starter ${trigger.epid}

FortiClient ID: No Data. Edit

2. Configure the playbook:
   a. Select a playbook trigger. For example, the *On Demand* trigger.
   b. Add a task with the EMS connector *Get Endpoints* action.
   c. Add a task with the Local connector *Update Asset and Identity* action.



New Playbook created from scratch - 2020-04-14T22:34:36.260Z

Custom build playbook to get started

LOCALHOST

Name: Update Assets

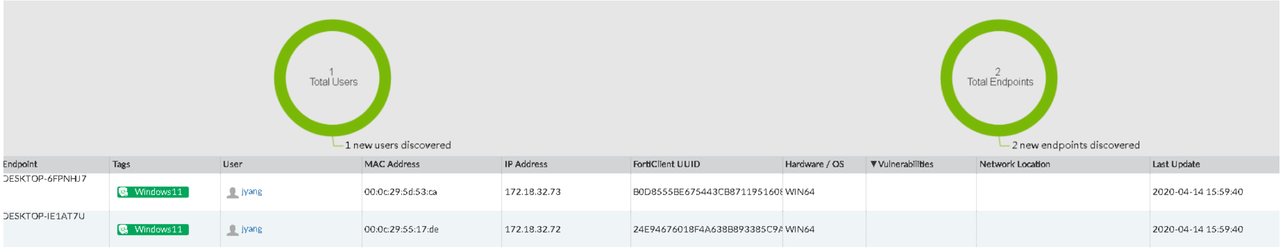
Description:

Connector: Local Connector

Action: Update Asset and Identity

Endpoint: Get endpoints (id_098_... ems_endpoints

3. Click *Save Playbook*.
4. Run the playbook, and go to *Fabric View* > *Assets* to view the collected endpoint information.



Endpoint	Tags	User	MAC Address	IP Address	FortiClient UUID	Hardware / OS	▼Vulnerabilities	Network Location	Last Update
DESKTOP-6FPNHJ7	Windows11	jyang	00:0c:29:5d:53:ca	172.18.32.73	B0D8555BE675443CB871195160	WIN64			2020-04-14 15:59:40
DESKTOP-IE1AT7U	Windows11	jyang	00:0c:29:55:17:de	172.18.32.72	24E94676018F4A638B893385C9A	WIN64			2020-04-14 15:59:40

Configuring an event handler to filter IPS attack direction

The example below demonstrates how you can create a FortiAnalyzer event handler for filtering the IPS attack direction based on the user's network environment.

You can configure this event handler based on network subnet information or interface roles:

- Event handler setup based on user network subnet on page 37
- Event handler setup based on interface role on page 42

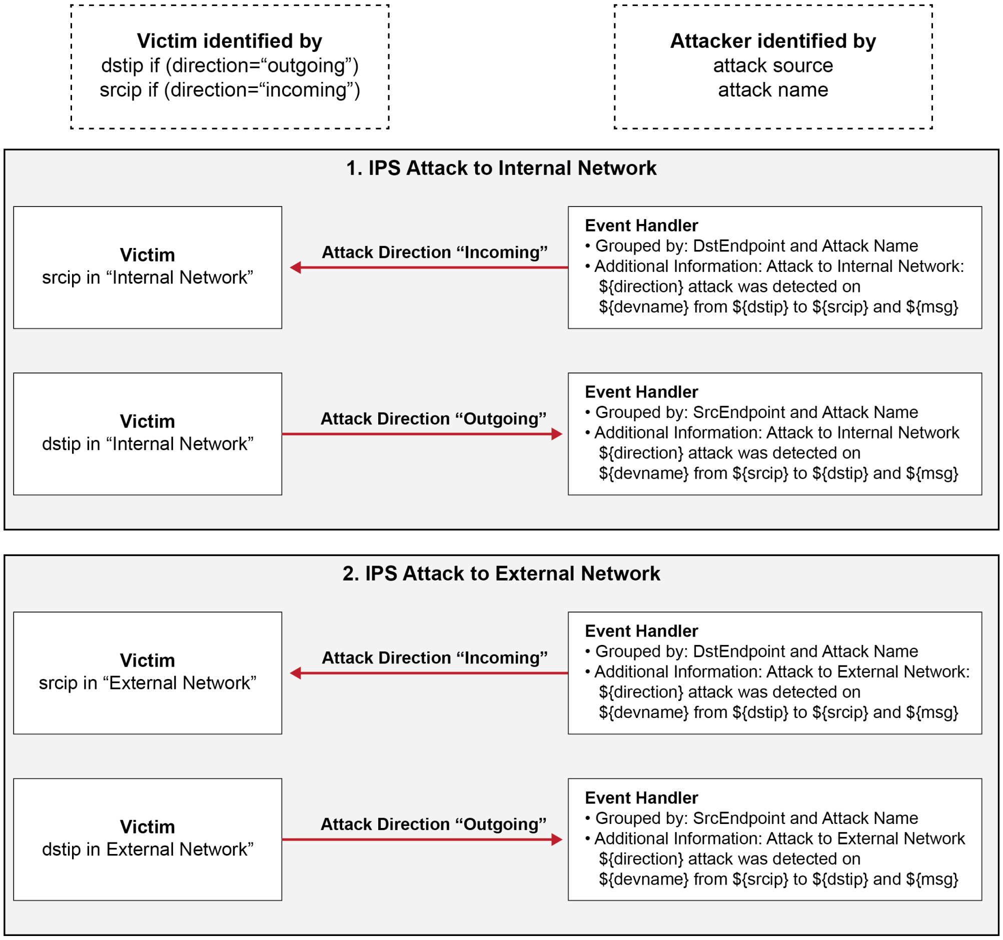
Event handler setup based on user network subnet

In this example, the following IP range includes the internal IPs for users. IPs outside of this range are considered external IPs.

- 192.168.0.0 - 192.168.255.255

The victim and attacker are identified as follows:

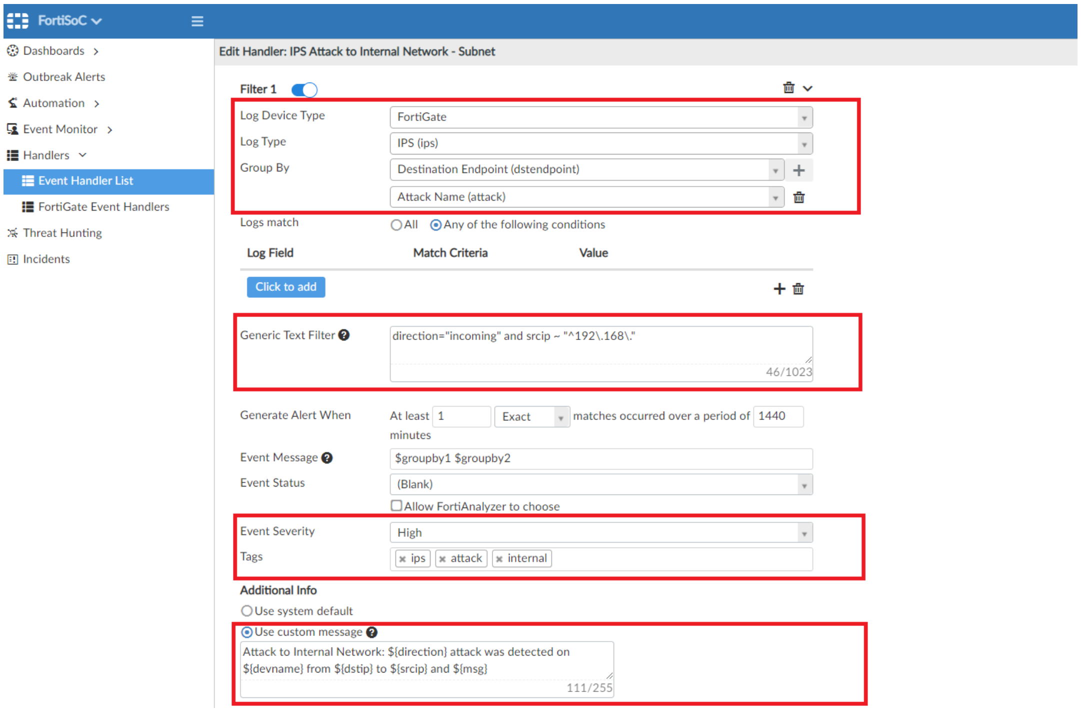
- The victim is identified by the IP of the traffic's origin (*srcip*) if the direction is incoming or the destination IP (*dstip*) if the direction is outgoing.
- The attacker is identified by *Attack Source* and *Attack Name*.


Victim identified by
dstip if (direction="outgoing")
srcip if (direction="incoming")
Attacker identified by
attack source
attack name
1. IPS Attack to Internal Network
Victim
srcip in "Internal Network"
Attack Direction "Incoming"
Event Handler
• Grouped by: DstEndpoint and Attack Name
• Additional Information: Attack to Internal Network: ${direction} attack was detected on ${devname} from ${dstip} to ${srcip} and ${msg}
Victim
dstip in "Internal Network"
Attack Direction "Outgoing"
Event Handler
• Grouped by: SrcEndpoint and Attack Name
• Additional Information: Attack to Internal Network ${direction} attack was detected on ${devname} from ${srcip} to ${dstip} and ${msg}
2. IPS Attack to External Network
Victim
srcip in "External Network"
Attack Direction "Incoming"
Event Handler
• Grouped by: DstEndpoint and Attack Name
• Additional Information: Attack to External Network: ${direction} attack was detected on ${devname} from ${dstip} to ${srcip} and ${msg}
Victim
dstip in External Network"
Attack Direction "Outgoing"
Event Handler
• Grouped by: SrcEndpoint and Attack Name
• Additional Information: Attack to External Network ${direction} attack was detected on ${devname} from ${srcip} to ${dstip} and ${msg}

To create an "IPS attack to internal network" event handler:

1. Go to *FortiSoC* > *Handlers* > *Event Handler List*, and click *Create New* to create a new event handler.
2. Based on the previously described example IP range, create an event handler to filter the alert as an attack to the internal network when the source IP is within the internal network and the direction is incoming.
   In this example, the filter is configured as follows:

Log Device Type	FortiGate
Log Type	IPS (ips)
Group By	Destination Endpoint (dstendpoint) Attack Name (attack)
Generic Text Filter	`direction="incoming" and srcip ~ "^192\.168\."`
Event Severity	High
Tags	ips, attack, internal
Additional Info	`Attack to Internal Network: ${direction} attack was detected on ${devname} from ${dstip} to ${srcip} and ${msg}`



Edit Handler: IPS Attack to Internal Network - Subnet

Filter 1

Log Device Type	FortiGate
Log Type	IPS (ips)
Group By	Destination Endpoint (dstendpoint) Attack Name (attack)
Logs match	○ All ● Any of the following conditions

Log Field	Match Criteria	Value

Generic Text Filter	direction="incoming" and srcip ~ "^192\.168\." 46/1023
Generate Alert When	At least 1 Exact matches occurred over a period of 1440 minutes
Event Message	$groupby1 $groupby2
Event Status	(Blank) □ Allow FortiAnalyzer to choose
Event Severity	High
Tags	ips, attack, internal

Additional Info

○ Use system default

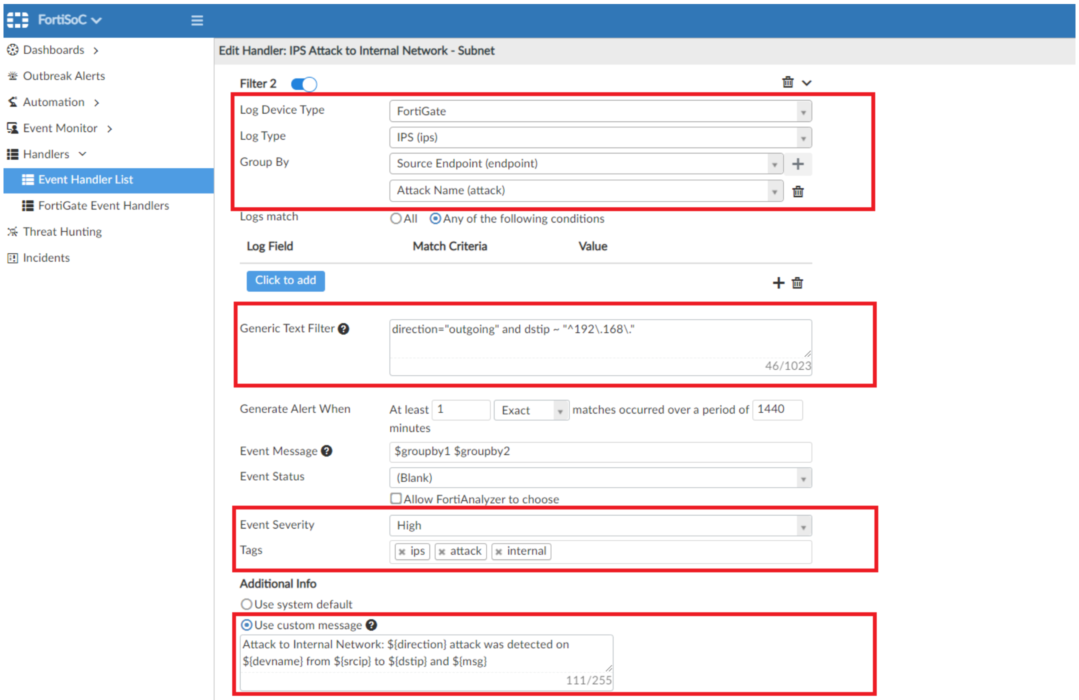
● Use custom message

Attack to Internal Network: ${direction} attack was detected on ${devname} from ${dstip} to ${srcip} and ${msg}

111/255

3. Add an additional filter for when the destination IP is within the internal network and the direction is outgoing. In this example, the filter is configured as follows:

Log Device Type	FortiGate
Log Type	IPS (ips)
Group By	Source Endpoint (endpoint) Attack Name (attack)
Generic Text Filter	`direction="outgoing" and dstip ~ "^192\.168\."`
Event Severity	High
Tags	ips, attack, internal
Additional Info	`Attack to Internal Network: ${direction} attack was detected on ${devname} from ${srcip} to ${dstip} and ${msg}`



Edit Handler: IPS Attack to Internal Network - Subnet

Filter 2

Log Device Type	FortiGate
Log Type	IPS (ips)
Group By	Source Endpoint (endpoint) Attack Name (attack)
Logs match	○ All ● Any of the following conditions

Log Field	Match Criteria	Value

Click to add

Generic Text Filter	direction="outgoing" and dstip ~ "^192\.168\." 46/1023
Generate Alert When	At least 1 Exact matches occurred over a period of 1440 minutes
Event Message	$groupby1 $groupby2
Event Status	(Blank) □ Allow FortiAnalyzer to choose
Event Severity	High
Tags	ips, attack, internal

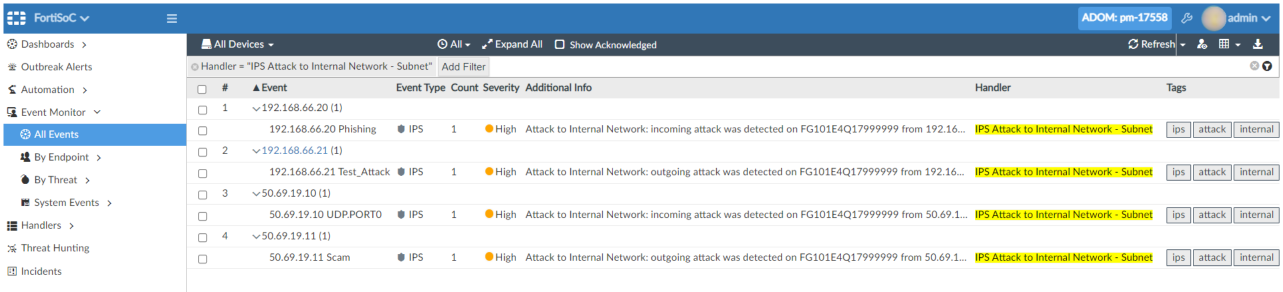
Additional Info

○ Use system default

● Use custom message

Attack to Internal Network: ${direction} attack was detected on ${devname} from ${srcip} to ${dstip} and ${msg} 111/255

4. Click *OK* to save the event handler.
5. Triggered alerts for this event handler are grouped by the attack source and attack name. This example includes additional custom information and tags to help recognize them.



Handler = "IPS Attack to Internal Network - Subnet"

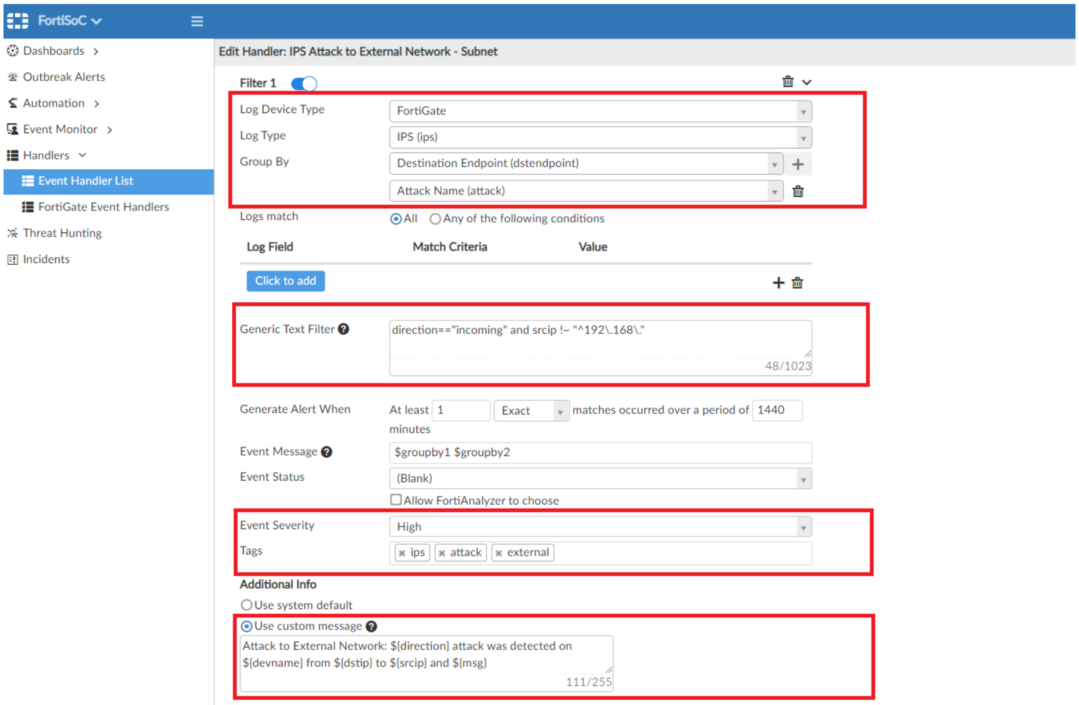
#	▲Event	Event Type	Count	Severity	Additional Info	Handler	Tags
1	192.168.66.20 (1)						
	192.168.66.20 Phishing	IPS	1	High	Attack to Internal Network: incoming attack was detected on FG101E4Q17999999 from 192.16...	IPS Attack to Internal Network - Subnet	ips attack internal
2	192.168.66.21 (1)						
	192.168.66.21 Test_Attack	IPS	1	High	Attack to Internal Network: outgoing attack was detected on FG101E4Q17999999 from 192.16...	IPS Attack to Internal Network - Subnet	ips attack internal
3	50.69.19.10 (1)						
	50.69.19.10 UDP.PORT0	IPS	1	High	Attack to Internal Network: incoming attack was detected on FG101E4Q17999999 from 50.69.1...	IPS Attack to Internal Network - Subnet	ips attack internal
4	50.69.19.11 (1)						
	50.69.19.11 Scam	IPS	1	High	Attack to Internal Network: outgoing attack was detected on FG101E4Q17999999 from 50.69.1...	IPS Attack to Internal Network - Subnet	ips attack internal

To create an "IPS attack to external network" event handler:

1. Go to *FortiSoC* > *Handlers* > *Event Handler List*, and click *Create New* to create a new event handler.
2. Based on the previously described example IP range, create an event handler to filter the alert as an attack to the external network when the source IP is external and the direction is incoming.
   In this example, the filter is configured as follows:

Log Device Type	FortiGate
Log Type	IPS (ips)
Group By	Destination Endpoint (dstendpoint) Attack Name (attack)
Generic Text Filter	`direction=="incoming" and srcip !~ "^192\.168\."`
Event Severity	High

Tags	ips, attack, external
Additional Info	`Attack to External Network: ${direction} attack was detected on ${devname} from ${dstip} to ${srcip} and ${msg}`



Edit Handler: IPS Attack to External Network - Subnet

Filter 1

Log Device Type	FortiGate
Log Type	IPS (ips)
Group By	Destination Endpoint (dstendpoint) Attack Name (attack)
Logs match	● All ○ Any of the following conditions

Log Field	Match Criteria	Value

Generic Text Filter	direction=="incoming" and srcip !~ "^192\.168\." 48/1023
Generate Alert When	At least 1 Exact matches occurred over a period of 1440 minutes
Event Message	$groupby1 $groupby2
Event Status	(Blank) □ Allow FortiAnalyzer to choose
Event Severity	High
Tags	ips, attack, external

Additional Info

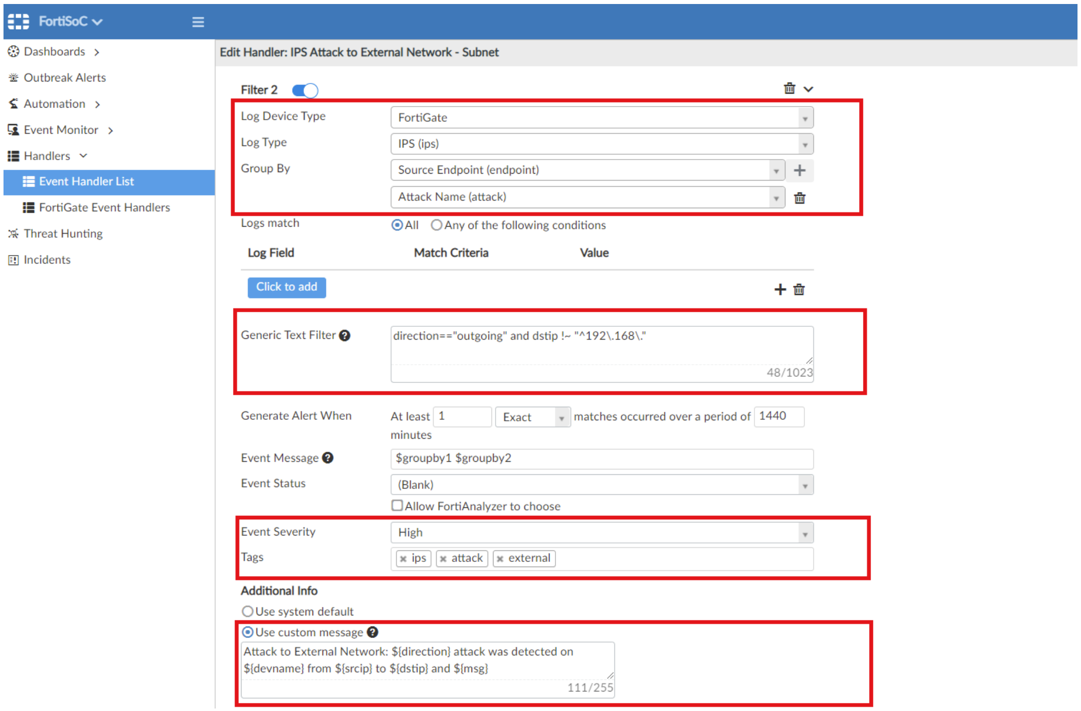
○ Use system default

● Use custom message

Attack to External Network: ${direction} attack was detected on ${devname} from ${dstip} to ${srcip} and ${msg} 111/255

3. Add an additional event handler filter for when the destination IP is external and the direction is outgoing.
   In this example, the filter is configured as follows:

Log Device Type	FortiGate
Log Type	IPS (ips)
Group By	Source Endpoint (endpoint) Attack Name (attack)
Generic Text Filter	`direction=="outgoing" and dstip !~ "^192\.168\."`
Event Severity	High
Tags	ips, attack, external
Additional Info	`Attack to External Network: ${direction} attack was detected on ${devname} from ${srcip} to ${dstip} and ${msg}`



Edit Handler: IPS Attack to External Network - Subnet

Filter 2

Log Device Type	FortiGate
Log Type	IPS (ips)
Group By	Source Endpoint (endpoint)
	Attack Name (attack)
Logs match	● All ○ Any of the following conditions

Log Field	Match Criteria	Value

Click to add

Generic Text Filter: direction=="outgoing" and dstip !~ "^192\.168\." 48/1023

Generate Alert When: At least 1 Exact matches occurred over a period of 1440 minutes

Event Message: $groupby1 $groupby2

Event Status: (Blank)

□ Allow FortiAnalyzer to choose

Event Severity: High

Tags: ips, attack, external

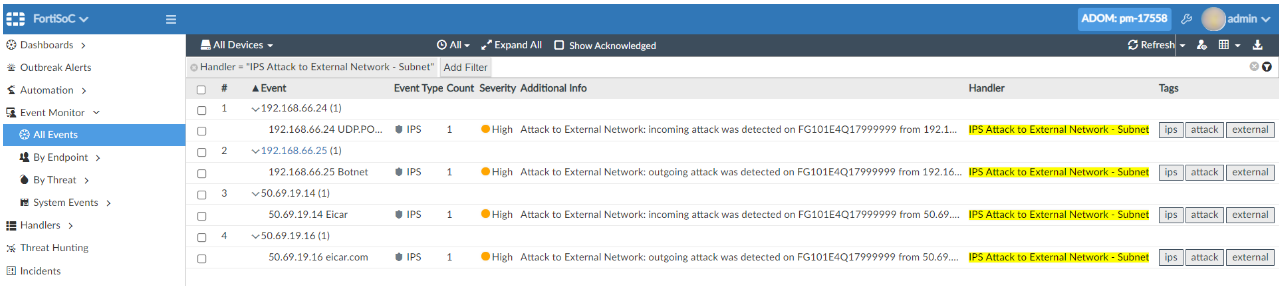
Additional Info

○ Use system default

● Use custom message

Attack to External Network: ${direction} attack was detected on ${devname} from ${srcip} to ${dstip} and ${msg} 111/255

4. Click *OK* to save the event handler.
5. Triggered alerts for this event handler are grouped by the attack source and attack name. This example includes additional custom information and tags to help recognize them.



Handler = "IPS Attack to External Network - Subnet"

#	Event	Event Type	Count	Severity	Additional Info	Handler	Tags
1	192.168.66.24 (1)						
	192.168.66.24 UDP.PO...	IPS	1	High	Attack to External Network: incoming attack was detected on FG101E4Q17999999 from 192.1...	IPS Attack to External Network - Subnet	ips attack external
2	192.168.66.25 (1)						
	192.168.66.25 Botnet	IPS	1	High	Attack to External Network: outgoing attack was detected on FG101E4Q17999999 from 192.16...	IPS Attack to External Network - Subnet	ips attack external
3	50.69.19.14 (1)						
	50.69.19.14 Eicar	IPS	1	High	Attack to External Network: incoming attack was detected on FG101E4Q17999999 from 50.69....	IPS Attack to External Network - Subnet	ips attack external
4	50.69.19.16 (1)						
	50.69.19.16 eicar.com	IPS	1	High	Attack to External Network: outgoing attack was detected on FG101E4Q17999999 from 50.69....	IPS Attack to External Network - Subnet	ips attack external

Event handler setup based on interface role

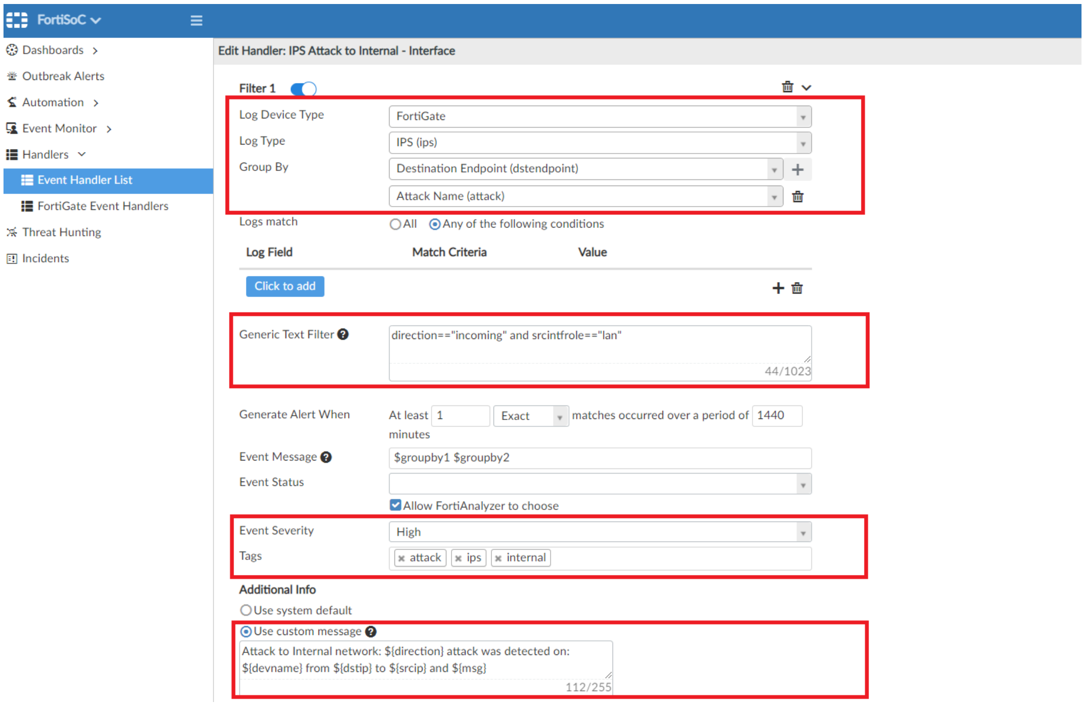
In this example, interface roles are set up in FortiGate, where the internal network is connected with the "lan" interface, and the external network is connected with the "wan" interface.
Traffic follows the below situations between the internal and external networks.

- Traffic from internal to internal: srcintfrole="lan", dstintfrole="lan".
- Traffic from internal to external: srcintfrole="lan", dstintfrole="wan".
- Traffic from external to external: srcintfrole="wan", dstintfrole="wan".
- Traffic from external to internal: srcintfrole="wan", dstintfrole="lan".

To create an "IPS attack to internal interface" event handler:

1. Go to *FortiSoC* > *Handlers* > *Event Handler List*, and click *Create New* to create a new event handler.
2. Based on the previously described interface roles, create an event handler to filter the alert as an attack to the internal interface when the source interface role is "lan" and the direction is incoming.
   In this example, the filter is configured as follows:

Log Device Type	FortiGate
Log Type	IPS (ips)
Group By	Destination Endpoint (dstendpoint) Attack Name (attack)
Generic Text Filter	`direction=="incoming" and srcintfrole=="lan"`
Event Severity	High
Tags	ips, attack, internal
Additional Info	`Attack to Internal Network: ${direction} attack was detected on: ${devname} from ${dstip} to ${srcip} and ${msg}`



Edit Handler: IPS Attack to Internal - Interface

Filter 1

Log Device Type	FortiGate
Log Type	IPS (ips)
Group By	Destination Endpoint (dstendpoint) Attack Name (attack)
Logs match	○ All ● Any of the following conditions

Log Field	Match Criteria	Value

Generic Text Filter	direction=="incoming" and srcintfrole=="lan" 44/1023
Generate Alert When	At least 1 Exact matches occurred over a period of 1440 minutes
Event Message	$groupby1 $groupby2
Event Status	☑ Allow FortiAnalyzer to choose
Event Severity	High
Tags	attack, ips, internal

Additional Info

○ Use system default

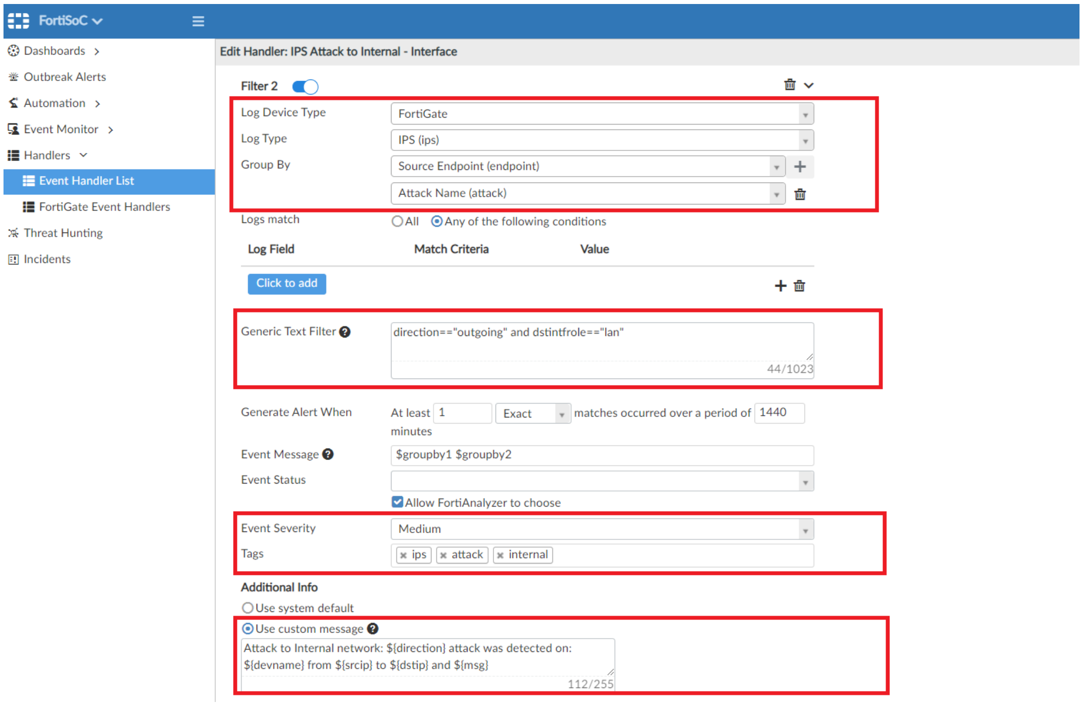
● Use custom message

Attack to Internal network: ${direction} attack was detected on: ${devname} from ${dstip} to ${srcip} and ${msg} 112/255

3. Add an additional filter for when the destination interface role is "lan" and the direction is outgoing.
   In this example, the filter is configured as follows:

Log Device Type	FortiGate
Log Type	IPS (ips)
Group By	Source Endpoint (endpoint) Attack Name (attack)

Generic Text Filter	`direction=="outgoing" and dstintfrole=="lan"`
Event Severity	Medium
Tags	ips, attack, internal
Additional Info	`Attack to Internal Network: ${direction} attack was detected on: ${devname} from ${srcip} to ${dstip} and ${msg}`



Edit Handler: IPS Attack to Internal - Interface

Filter 2

Log Device Type	FortiGate
Log Type	IPS (ips)
Group By	Source Endpoint (endpoint) Attack Name (attack)
Logs match	○ All ● Any of the following conditions

Log Field	Match Criteria	Value

Generic Text Filter	direction=="outgoing" and dstintfrole=="lan" 44/1023
Generate Alert When	At least 1 Exact matches occurred over a period of 1440 minutes
Event Message	$groupby1 $groupby2
Event Status	☑ Allow FortiAnalyzer to choose
Event Severity	Medium
Tags	ips, attack, internal

Additional Info

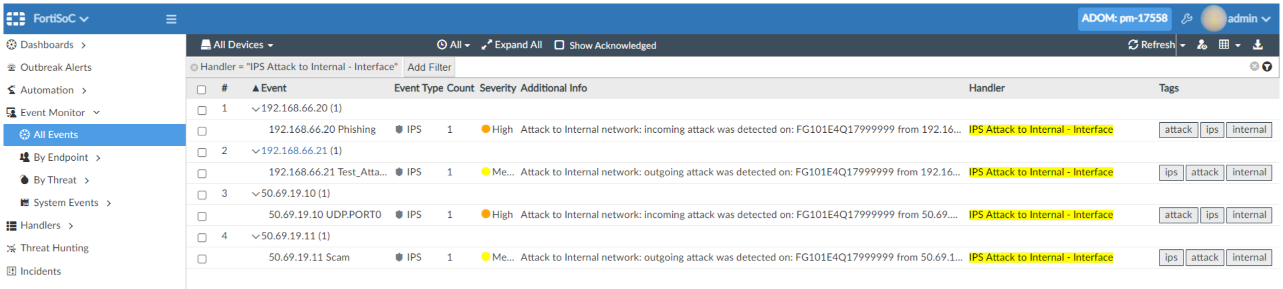
○ Use system default

● Use custom message

Attack to Internal network: ${direction} attack was detected on: ${devname} from ${srcip} to ${dstip} and ${msg}

112/255

4. Click *OK* to save the event handler.
5. Triggered alerts for this event handler are grouped by the attack source and attack name. This example includes additional custom information and tags to help recognize them.



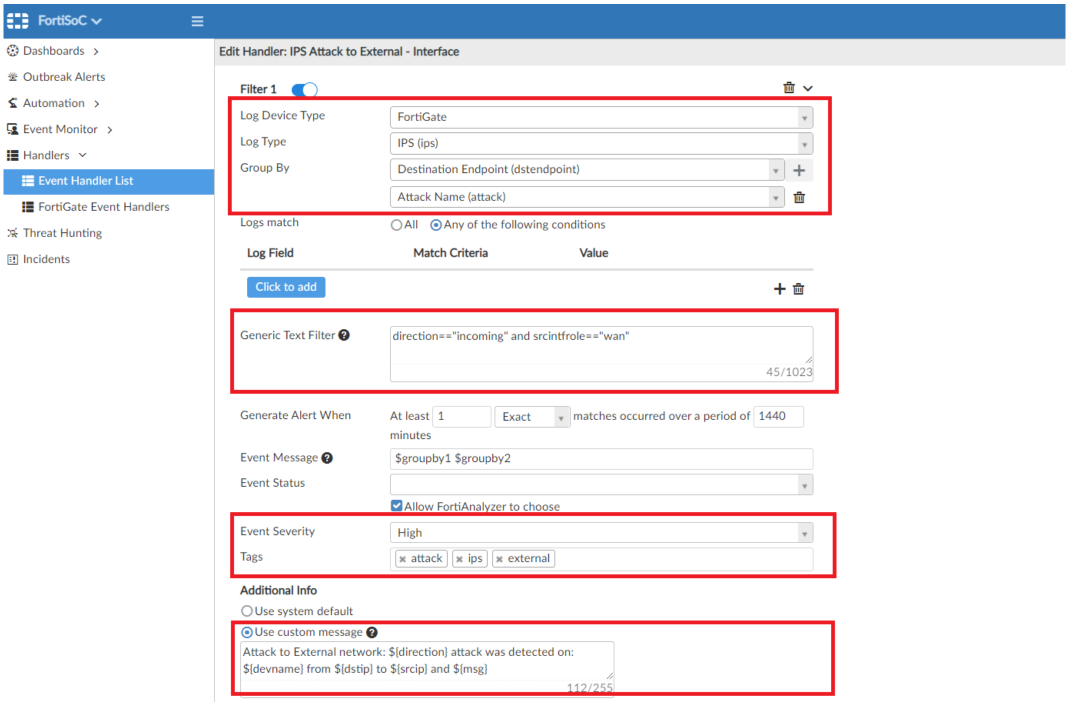
Handler = "IPS Attack to Internal - Interface"

#	Event	Event Type	Count	Severity	Additional Info	Handler	Tags
1	192.168.66.20 (1)						
	192.168.66.20 Phishing	IPS	1	High	Attack to Internal network: incoming attack was detected on: FG101E4Q17999999 from 192.16...	IPS Attack to Internal - Interface	attack ips internal
2	192.168.66.21 (1)						
	192.168.66.21 Test_Atta...	IPS	1	Me...	Attack to Internal network: outgoing attack was detected on: FG101E4Q17999999 from 192.16...	IPS Attack to Internal - Interface	ips attack internal
3	50.69.19.10 (1)						
	50.69.19.10 UDP.PORT0	IPS	1	High	Attack to Internal network: incoming attack was detected on: FG101E4Q17999999 from 50.69....	IPS Attack to Internal - Interface	attack ips internal
4	50.69.19.11 (1)						
	50.69.19.11 Scam	IPS	1	Me...	Attack to Internal network: outgoing attack was detected on: FG101E4Q17999999 from 50.69.1...	IPS Attack to Internal - Interface	ips attack internal

To create an "IPS attack to external interface" event handler:

1. Go to *FortiSoC* > *Handlers* > *Event Handler List*, and click *Create New* to create a new event handler.
2. Based on the previously described interface roles, create an event handler to filter the alert as an attack to the external interface when the source interface role is "wan" and the direction is incoming. In this example, the filter is configured as follows:

Log Device Type	FortiGate
Log Type	IPS (ips)
Group By	Destination Endpoint (dstendpoint) Attack Name (attack)
Generic Text Filter	`direction=="incoming" and srcintfrole=="wan"`
Event Severity	High
Tags	ips, attack, external
Additional Info	`Attack to External Network: ${direction} attack was detected on: ${devname} from ${dstip} to ${srcip} and ${msg}`



Edit Handler: IPS Attack to External - Interface

Filter 1

Log Device Type: FortiGate

Log Type: IPS (ips)

Group By: Destination Endpoint (dstendpoint)
Attack Name (attack)

Logs match: ○ All ● Any of the following conditions

Log Field	Match Criteria	Value

Generic Text Filter: direction=="incoming" and srcintfrole=="wan" 45/1023

Generate Alert When: At least 1 Exact matches occurred over a period of 1440 minutes

Event Message: $groupby1 $groupby2

Event Status:

☑ Allow FortiAnalyzer to choose

Event Severity: High

Tags: attack, ips, external

Additional Info

○ Use system default

● Use custom message

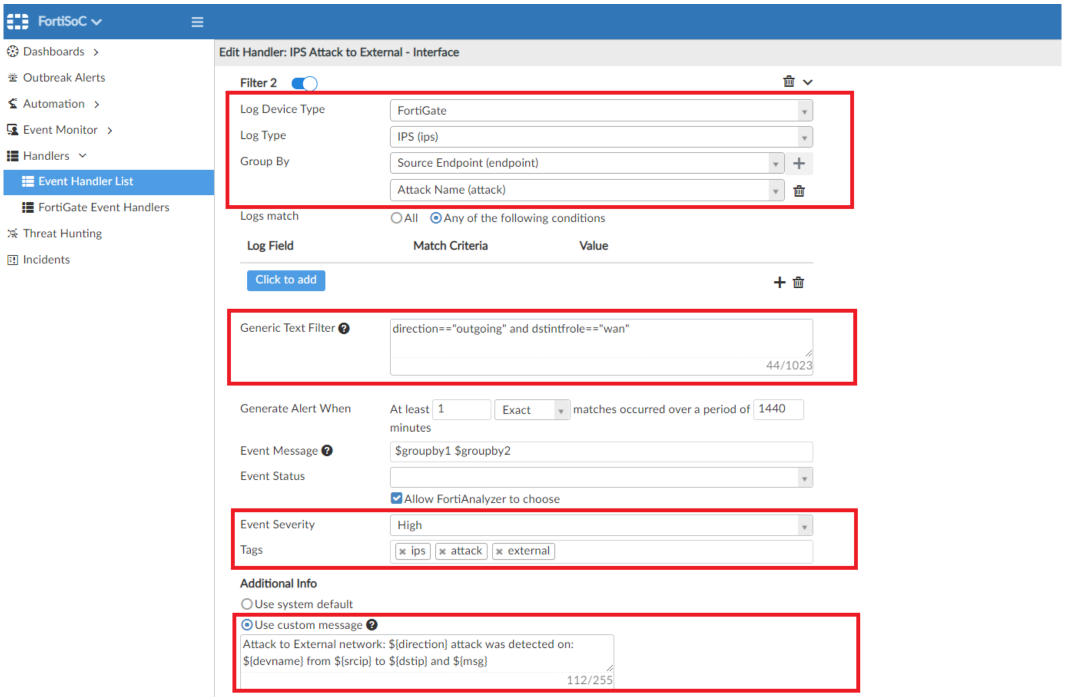
Attack to External network: $(direction) attack was detected on: $(devname) from $(dstip) to $(srcip) and $(msg)

112/255

3. Add an additional filter for when the destination interface role is "wan" and the direction is outgoing.
   In this example, the filter is configured as follows:

Log Device Type	FortiGate
Log Type	IPS (ips)
Group By	Source Endpoint (endpoint) Attack Name (attack)
Generic Text Filter	`direction=="outgoing" and dstintfrole=="wan"`
Event Severity	High
Tags	ips, attack, external

Additional Info	`Attack to External Network: ${direction} attack was detected on: ${devname} from ${srcip} to ${dstip} and ${msg}`



Edit Handler: IPS Attack to External - Interface

Filter 2

Log Device Type	FortiGate
Log Type	IPS (ips)
Group By	Source Endpoint (endpoint) Attack Name (attack)
Logs match	○ All ● Any of the following conditions

Log Field	Match Criteria	Value

Click to add

Generic Text Filter	direction=="outgoing" and dstintfrole=="wan" 44/1023
Generate Alert When	At least 1 Exact matches occurred over a period of 1440 minutes
Event Message	$groupby1 $groupby2
Event Status	
	☑ Allow FortiAnalyzer to choose
Event Severity	High
Tags	ips, attack, external

Additional Info

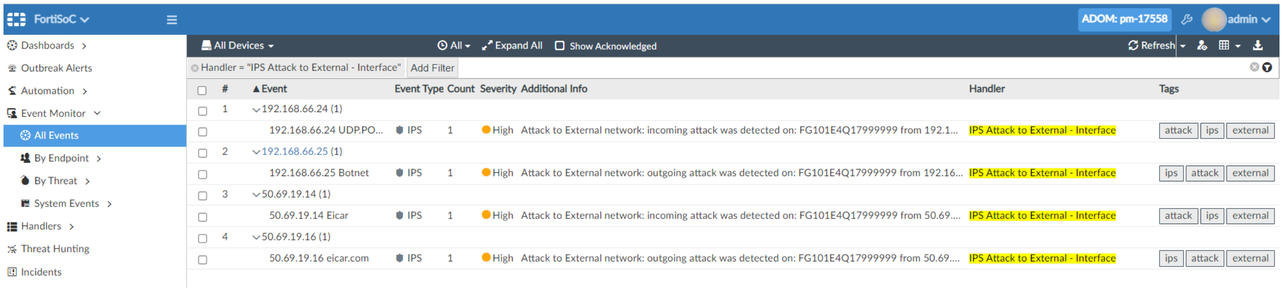
○ Use system default

● Use custom message

Attack to External network: ${direction} attack was detected on: ${devname} from ${srcip} to ${dstip} and ${msg}

112/255

4. Click *OK* to save the event handler.
5. Triggered alerts for this event handler are grouped by the attack source and attack name. This example includes additional custom information and tags to help recognize them.



Handler = "IPS Attack to External - Interface"

#	Event	Event Type	Count	Severity	Additional Info	Handler	Tags
1	192.168.66.24 (1)						
	192.168.66.24 UDP.PO...	IPS	1	High	Attack to External network: incoming attack was detected on: FG101E4Q17999999 from 192.1...	IPS Attack to External - Interface	attack ips external
2	192.168.66.25 (1)						
	192.168.66.25 Botnet	IPS	1	High	Attack to External network: outgoing attack was detected on: FG101E4Q17999999 from 192.16...	IPS Attack to External - Interface	ips attack external
3	50.69.19.14 (1)						
	50.69.19.14 Eicar	IPS	1	High	Attack to External network: incoming attack was detected on: FG101E4Q17999999 from 50.69....	IPS Attack to External - Interface	attack ips external
4	50.69.19.16 (1)						
	50.69.19.16 eicar.com	IPS	1	High	Attack to External network: outgoing attack was detected on: FG101E4Q17999999 from 50.69....	IPS Attack to External - Interface	ips attack external

Logging

This section contains the following topics:

- FortiAI logging on FortiAnalyzer on page 47

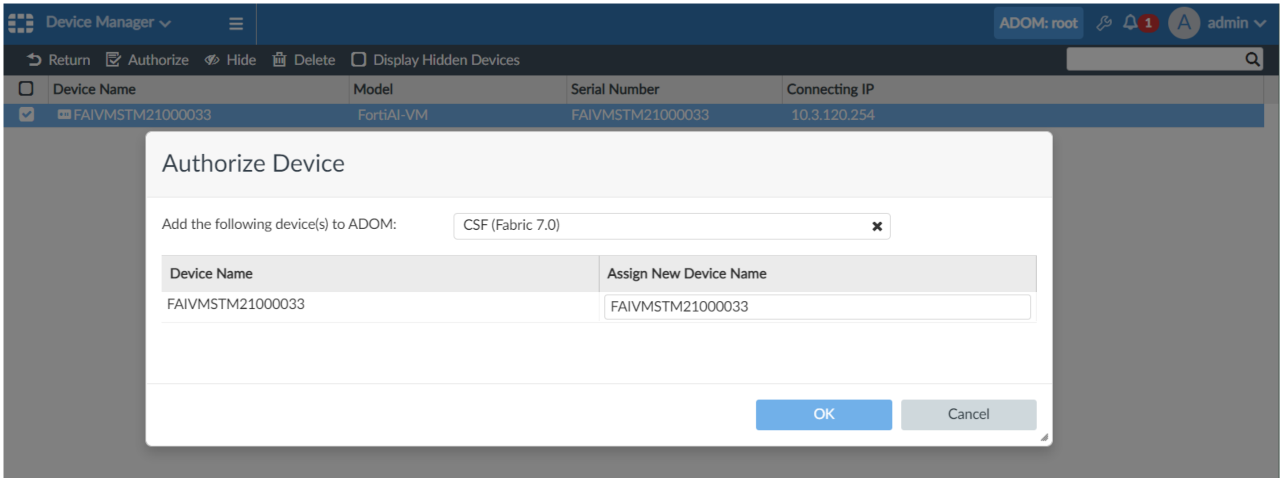
FortiAI logging on FortiAnalyzer

Starting in FortiAnalyzer 7.0.1, you can configure FortiAnalyzer to accept logs from a FortiAI device for use in the following ways:

- FortiAnalyzer can recognize FortiAi devices.
- FortiAI logs can be stored in Fabric ADOM.
- FortiAI can be viewed in LogView.
- FortiAI Device Type and Log Types are available in event handlers and report data sets.

To add a FortiAI device to FortiAnalyzer:

1. On FortiAnalyzer, ensure you in are in the correct ADOM.
2. Go to *Device Manager* and add the FortiAI device.
   Prior to FortiAnalyzer 7.0.1, FortiAnalyzer could not recognize FortiAI devices. In 7.0.1 and later, FortiAnalyzer is able to recognize the FortiAI device and will display it in the *Unauthorized Device* list once added.



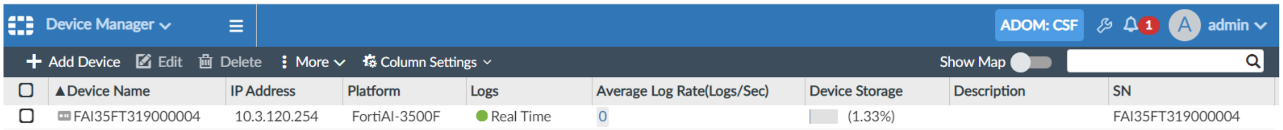
☐	Device Name	Model	Serial Number	Connecting IP
☑	FAIVMSTM21000033	FortiAI-VM	FAIVMSTM21000033	10.3.120.254

Authorize Device

Add the following device(s) to ADOM: CSF (Fabric 7.0)

Device Name	Assign New Device Name
FAIVMSTM21000033	FAIVMSTM21000033

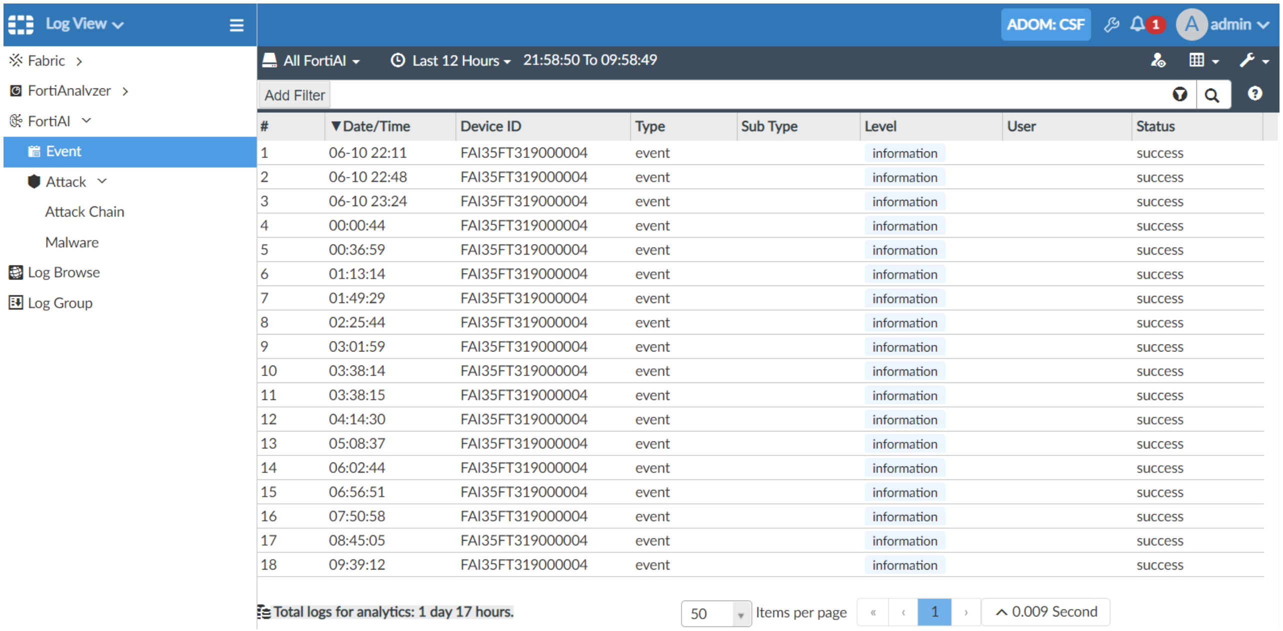
3. Select *Unauthorized Devices* and authorize the FortiAI device.
   When the FortiAI device is authorized on FortiAnalyzer, it is listed in the FortiAnalyzer *Device Manager* with information including its device name, IP, serial number, and logging status.



☐	▲Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)	Device Storage	Description	SN
☐	FAI35FT319000004	10.3.120.254	FortiAI-3500F	● Real Time	0	(1.33%)		FAI35FT319000004

To view FortiAI logs in FortiAnalyzer:

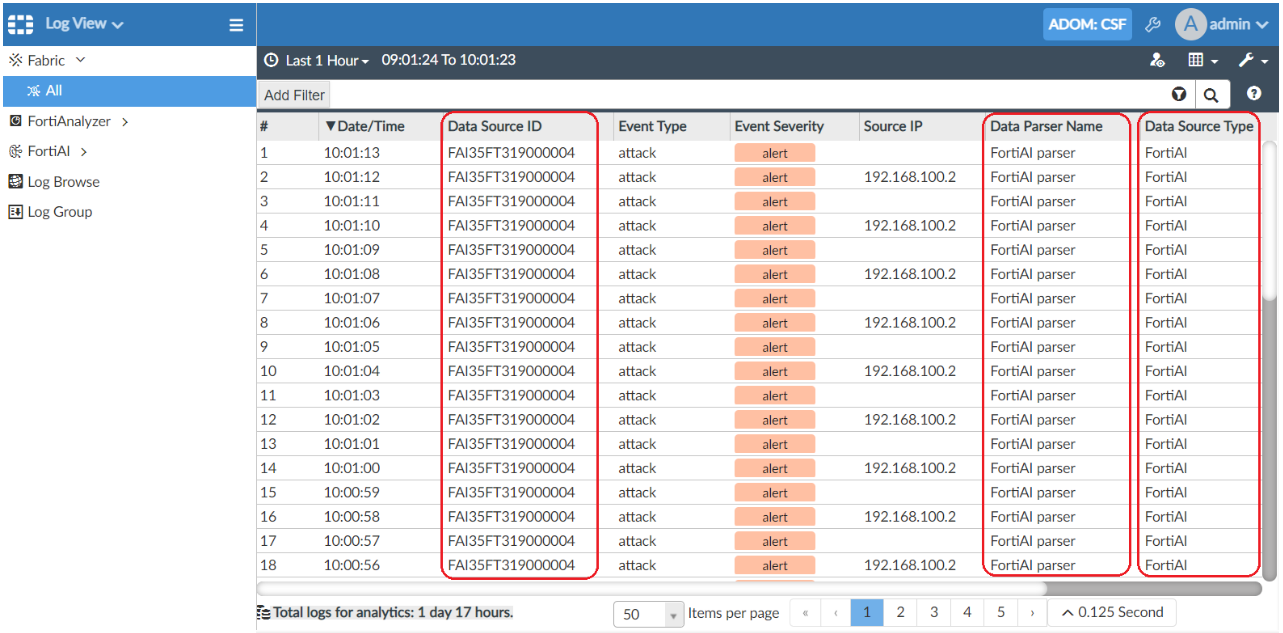
1. On FortiAnalyzer, ensure you are in the correct ADOM.
2. Go to *Log View > FortiAI*.
   There is a new *FortiAI* log type created for the FortiAI device. When FortiAI logs are received, they are displayed in *Log View*.



#	Date/Time	Device ID	Type	Sub Type	Level	User	Status
1	06-10 22:11	FAI35FT319000004	event		information		success
2	06-10 22:48	FAI35FT319000004	event		information		success
3	06-10 23:24	FAI35FT319000004	event		information		success
4	00:00:44	FAI35FT319000004	event		information		success
5	00:36:59	FAI35FT319000004	event		information		success
6	01:13:14	FAI35FT319000004	event		information		success
7	01:49:29	FAI35FT319000004	event		information		success
8	02:25:44	FAI35FT319000004	event		information		success
9	03:01:59	FAI35FT319000004	event		information		success
10	03:38:14	FAI35FT319000004	event		information		success
11	03:38:15	FAI35FT319000004	event		information		success
12	04:14:30	FAI35FT319000004	event		information		success
13	05:08:37	FAI35FT319000004	event		information		success
14	06:02:44	FAI35FT319000004	event		information		success
15	06:56:51	FAI35FT319000004	event		information		success
16	07:50:58	FAI35FT319000004	event		information		success
17	08:45:05	FAI35FT319000004	event		information		success
18	09:39:12	FAI35FT319000004	event		information		success

Total logs for analytics: 1 day 17 hours.

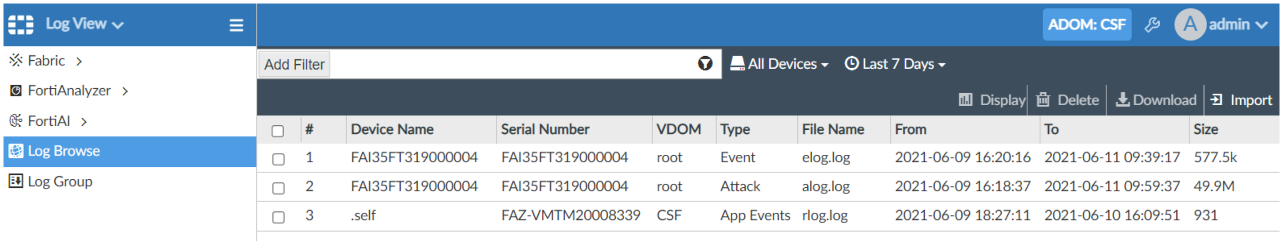
3. Go to *Log View > Fabric*.
   FortiAnalyzer adds a SIEM parser to FortiAI logs so that they can be viewed in the Fabric SIEM database correctly.



#	Date/Time	Data Source ID	Event Type	Event Severity	Source IP	Data Parser Name	Data Source Type
1	10:01:13	FAI35FT319000004	attack	alert		FortiAI parser	FortiAI
2	10:01:12	FAI35FT319000004	attack	alert	192.168.100.2	FortiAI parser	FortiAI
3	10:01:11	FAI35FT319000004	attack	alert		FortiAI parser	FortiAI
4	10:01:10	FAI35FT319000004	attack	alert	192.168.100.2	FortiAI parser	FortiAI
5	10:01:09	FAI35FT319000004	attack	alert		FortiAI parser	FortiAI
6	10:01:08	FAI35FT319000004	attack	alert	192.168.100.2	FortiAI parser	FortiAI
7	10:01:07	FAI35FT319000004	attack	alert		FortiAI parser	FortiAI
8	10:01:06	FAI35FT319000004	attack	alert	192.168.100.2	FortiAI parser	FortiAI
9	10:01:05	FAI35FT319000004	attack	alert		FortiAI parser	FortiAI
10	10:01:04	FAI35FT319000004	attack	alert	192.168.100.2	FortiAI parser	FortiAI
11	10:01:03	FAI35FT319000004	attack	alert		FortiAI parser	FortiAI
12	10:01:02	FAI35FT319000004	attack	alert	192.168.100.2	FortiAI parser	FortiAI
13	10:01:01	FAI35FT319000004	attack	alert		FortiAI parser	FortiAI
14	10:01:00	FAI35FT319000004	attack	alert	192.168.100.2	FortiAI parser	FortiAI
15	10:00:59	FAI35FT319000004	attack	alert		FortiAI parser	FortiAI
16	10:00:58	FAI35FT319000004	attack	alert	192.168.100.2	FortiAI parser	FortiAI
17	10:00:57	FAI35FT319000004	attack	alert		FortiAI parser	FortiAI
18	10:00:56	FAI35FT319000004	attack	alert	192.168.100.2	FortiAI parser	FortiAI

Total logs for analytics: 1 day 17 hours.

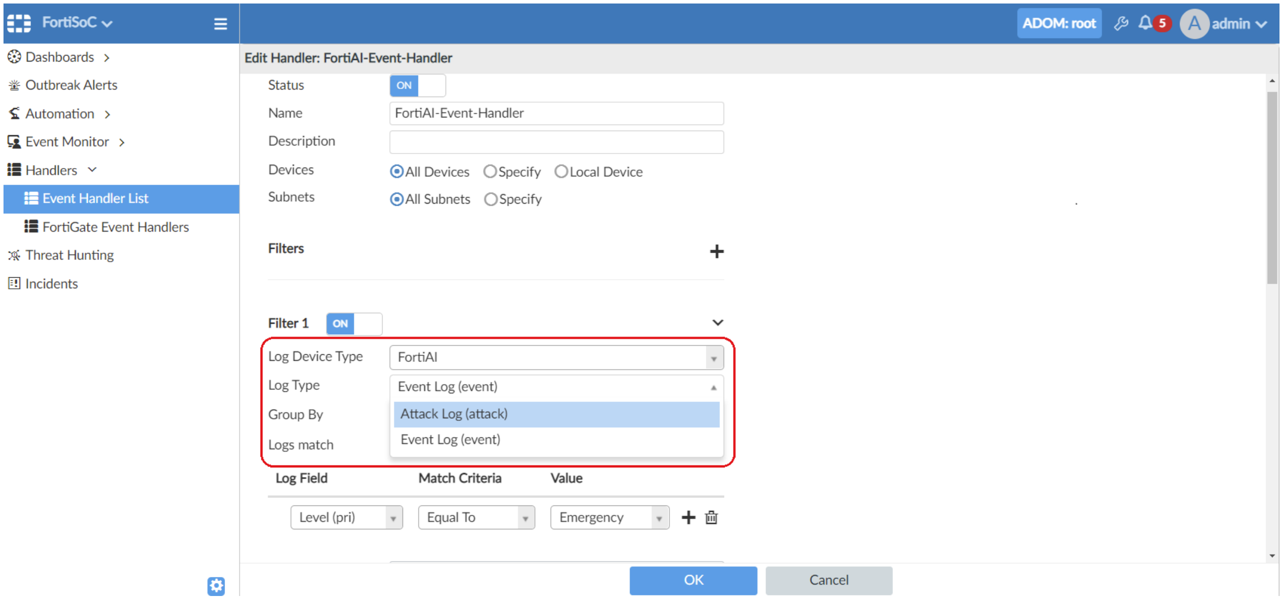
4. Go to *Log View* > *Log Browse*.
   In *Log Browse*, you can see the FortiAI device logs listed. You can download or import FortiAI logs.



□	#	Device Name	Serial Number	VDOM	Type	File Name	From	To	Size
□	1	FAI35FT319000004	FAI35FT319000004	root	Event	elog.log	2021-06-09 16:20:16	2021-06-11 09:39:17	577.5k
□	2	FAI35FT319000004	FAI35FT319000004	root	Attack	alog.log	2021-06-09 16:18:37	2021-06-11 09:59:37	49.9M
□	3	.self	FAZ-VMTM20008339	CSF	App Events	rlog.log	2021-06-09 18:27:11	2021-06-10 16:09:51	931

To create a custom event handler using FortiAI logs:

1. Go to *FortiSoC* > *Handlers* > *Event Handler List*, and create a new event handler.
2. Enter a name for the event handler, for example *FortiAI-Event-Handler*.
3. Enable a filter, and select *FortiAI* as the *Log Device Type*.
4. In *Log type*, select a FortiAI log type.
5. Configure the remaining settings as required, and click *OK* to save the event handler.



Edit Handler: FortiAI-Event-Handler

Status	ON
Name	FortiAI-Event-Handler
Description	
Devices	● All Devices ○ Specify ○ Local Device
Subnets	● All Subnets ○ Specify

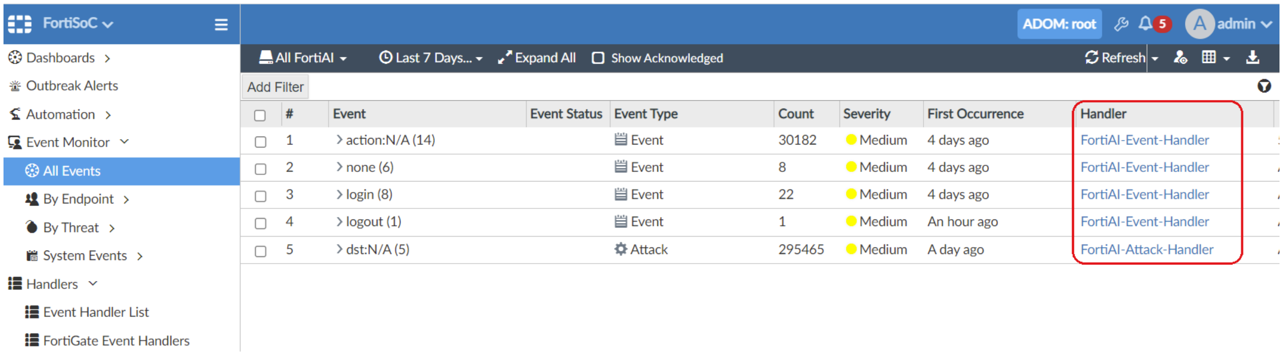
Filters

Filter 1 ON

Log Device Type	FortiAI
Log Type	Event Log (event) Attack Log (attack) Event Log (event)
Group By	
Logs match	

Log Field	Match Criteria	Value
Level (pri)	Equal To	Emergency

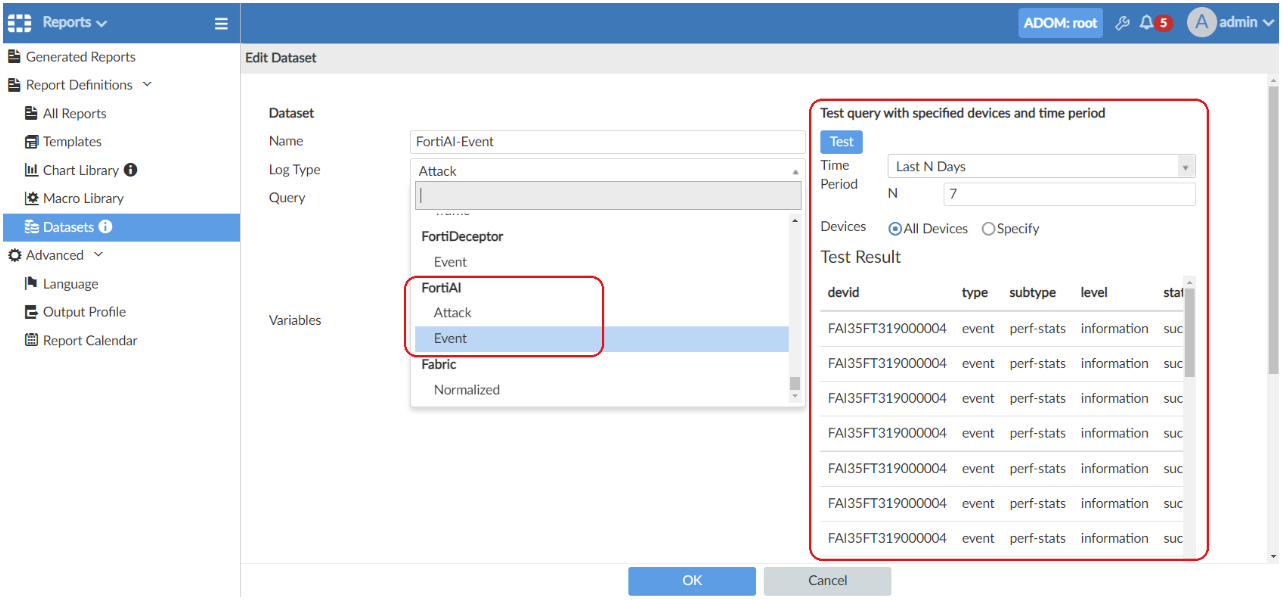
6. Events triggered by the event handler appear in *FortiSoC* > *Event Monitor* > *All Events*. The name of the event handler is displayed in the table.



□	#	Event	Event Status	Event Type	Count	Severity	First Occurrence	Handler
□	1	> action:N/A (14)		Event	30182	● Medium	4 days ago	FortiAI-Event-Handler
□	2	> none (6)		Event	8	● Medium	4 days ago	FortiAI-Event-Handler
□	3	> login (8)		Event	22	● Medium	4 days ago	FortiAI-Event-Handler
□	4	> logout (1)		Event	1	● Medium	An hour ago	FortiAI-Event-Handler
□	5	> dst:N/A (5)		Attack	295465	● Medium	A day ago	FortiAI-Attack-Handler

To create a custom report using FortiAI logs:

1. Go to *Reports* > *Report Definitions* > *Datasets*, and create or edit a dataset.
2. Select a FortiAI log type in the Log Type dropdown.
3. Configure the remaining settings as required, and click *OK* to save the dataset.
   The dataset can now be used when configuring charts used in FortiAnalyzer reports.



Dataset

Name: FortiAI-Event

Log Type: Attack

Query

Test query with specified devices and time period

Time Period: Last N Days

N: 7

Devices: ● All Devices ○ Specify

Test Result

devid	type	subtype	level	stat
FAI35FT319000004	event	perf-stats	information	suc
FAI35FT319000004	event	perf-stats	information	suc
FAI35FT319000004	event	perf-stats	information	suc
FAI35FT319000004	event	perf-stats	information	suc
FAI35FT319000004	event	perf-stats	information	suc
FAI35FT319000004	event	perf-stats	information	suc
FAI35FT319000004	event	perf-stats	information	suc

Troubleshooting

This section contains the following topics:

- Troubleshooting report performance issues on page 51
- Troubleshooting a dataset query on page 59
- Troubleshooting an empty chart on page 61

Troubleshooting report performance issues

The following topics provide guidance when troubleshooting report performance issue:

- Check the report diagnostic log on page 51
- Check hardware and software status on page 54
- Check data policy and log storage policy on page 55
- Check report and chart settings on page 55
- Check and adjust report auto-cache daemon on page 56
- Check and adjust report hcache on page 57
- Report performance troubleshooting commands on page 58

Check the report diagnostic log

For reports that take a long time to run, check the report diagnostic log to troubleshoot performance issues.

To retrieve a report diagnostic log, go to *Reports > Generated Report*, right-click the report and select *Retrieve Diagnostic* to download the log to your computer. Use a text editor to open the log and check the log for possible causes of performance issues.

Following are parts of a sample report diagnostic log and what to look for when troubleshooting report performance.

```
NAME  SCHEDULED  AUTO-CACHE  REPORT GROUP  REPORT TITLE
==================================================================================
1     V          V           -             Security Analysis

per-device option: disable
hostname-resolve: disable

Report Status
   Max pending rpts: 100000
   Current pendings: 0
   Max running rpts: 10
   Current runnings: 2
```

Section	What to look for
NAME / SCHEDULED / AUTO-CACHE / REPORT GROUP / REPORT TITLE	Check the `SCHEDULED`, `AUTO-CACHE`, and `REPORT GROUP` columns. • Schedule the reports that run regularly. To configure report schedules, see *Scheduling reports* in the *FortiAnalyzer Administration Guide*. • Enable auto-cache for reports that run regularly, especially schedule reports. See *How auto-cache works* and *Enabling auto-cache* in the *FortiAnalyzer Administration Guide*. • Group reports that run regularly. To group reports, see *Grouping reports* in the *FortiAnalyzer Administration Guide*.
`hostname-resolve`	Ensure `hostname-resolve` is set to `disable`. Resolving hostnames usually takes a long time. If the DNS server is slow or does not support reverse DNS, report generation might hang.

```
Total Quota Summary:
     Total Quota   Allocated   Available   Allocate%
     27201.3GB     1024.0GB    26177.3GB   3.8 %

System Storage Summary:
     Total         Used        Available   Use%
     27501.3GB     1117.6GB    26383.6GB   4.1 %

----------------------------------------
System Performance
Fri Aug 25 12:00:02 2017
----------------------------------------
CPU
     Used:  34.4%
     Used(Excluded NICE):  34.4%
Memory
     Total:  34939888 KB
     Used 23899636 KB 68.4%
Hard Disk
     Total:  28837161872 KB
     Used:  11171927688 KB 38.7%
     IoStat:
Log Rate
     logs/sec: 20326.8, logs/30sec: 20395.6, logs/60sec: 20274.2
Message Rate
     msgs/sec: 3057.4, msgs/30sec: 3068.1, msgs/60sec: 3039.1
```

Section	What to look for
Total Quota Summary and **System Storage Summary**	• Ensure there is enough disk quota and disk space for logging and reporting. Insufficient disk quota might affect report accuracy. Disk quota must be big enough so that quota enforcement does not affect logs used for reporting. If quota enforcement trims the logs or tables used for the reporting period, there might be empty charts or incorrect data.
System Performance	• Check that there is enough system resources including CPU, memory, and disk space. • Check that the log rate and message rate is not so high that it slow report

Section	What to look for
	generation. • If the log rate is higher than the sustained rates for your FortiAnalyzermodel, the hardware is overloaded and needs an upgrade. The sustained rates for FortiAnalyzermodels are listed in the Data Sheet on the FortiAnalyzer web page.

```
------------------------------------------
Run Report
Fri Aug 25 12:00:03 2017
------------------------------------------
[12:00:03] Request hcaches for 9 log tables
chart Traffic-Bandwidth-Summary-Day-Of-Month done, 1 subqrys
   1/1 took 17.88s, 0 hcaches ready, 2 hcaches requested
   overall time used 18.13s
chart Session-Summary-Day-Of-Month done, 1 subqrys
   1/1 took 15.54s, 0 hcaches ready, 2 hcaches requested
   overall time used 15.80s
chart Traffic-History-By-Active-User done, 1 subqrys
   1/1 took 12.79s, 0 hcaches ready, 2 hcaches requested
   overall time used 13.07s
chart Top-Attack-Victim done, 1 subqrys
   1/1 took 1.71s, 0 hcaches ready, 1 hcaches requested
   overall time used 1.71s
chart Top-Attack-Source done, 1 subqrys
   1/1 took 1.51s, 0 hcaches ready, 1 hcaches requested
   overall time used 1.51s
chart Top-Attacks-Detected done, 1 subqrys
   1/1 took 1.91s, 0 hcaches ready, 1 hcaches requested
   overall time used 1.94s
…
…
…
chart System-Summary-By-Severity done, 1 subqrys
   1/1 took 1.22s, 0 hcaches ready, 1 hcaches requested
   overall time used 1.22s
chart System-Critical-Severity-Events done, 1 subqrys
   1/1 took 1.18s, 0 hcaches ready, 1 hcaches requested
   overall time used 1.18s
chart System-High-Severity-Events done, 1 subqrys
   1/1 took 0.46s, 0 hcaches ready, 1 hcaches requested
   overall time used 0.46s
```

Section	What to look for
Run Report	• Check the number of log tables. • Check the number of hcaches requested vs ready. If many hcaches are not ready, then those charts will take a long time. If the number of log tables is high but the number of hcaches ready is low, retrieve the diagnostic log after five minutes. A change in the number of hcaches ready means the report is still running. Since the diagnostic log is updated every five minutes, you can check this log to view reporting progress.

Section	What to look for
	• Check which charts take a long time to generate and reconfigure those charts to improve performance.

```
------------------------------------------
Report Summary
Fri Aug 25 12:00:56 2017
------------------------------------------
Number of charts: 58
Number of tables: 9
Number of hcaches requested: 109

HCACHE building time: 53.32s
Rendering time: 13.33s
Total time: 1m7.67s
```

Section	What to look for
Report Summary	• Check the number of hcaches requested, hcache building time, and rendering time. The `number of hcaches requested` = number of charts per report * number of primary tables * number of reports.

Check hardware and software status

get system status

This command shows the system status such as platform type (hardware or VM), firmware version, system time, disk usage, and file system format.

Use this information to check if the hardware is overloaded. This information also helps you and customer support to quickly identify any issues and narrow down the investigation.

Following is a sample result of running this command.

```
Platform Type : FAZ3500E
Platform Full Name : FortiAnalyzer-3500E
Version : v5.4.3-build1187 170517 (GA)
Serial Number : FL99999999999999
BIOS version : 00010001
System Part-Number : P15168-01
Hostname : SAMPLEFZ350
Max Number of Admin Domains : 4000
Admin Domain Configuration : Disabled
FIPS Mode : Disabled
Branch Point : 738
Release Version Information : GA
Current Time : Tue May 23 10:22:53 PST 2017
Daylight Time Saving : Yes
Time Zone : (GMT-8:00) Pacific Time (US & Canada).
x86-64 Applications : Yes
Disk Usage : Free 17020.10GB, Total 40314.71GB
File System : Ext4
```

Line	Notes
`Current Time`	This is the SQL insert start time.
`File System`	Ensure the file system is `Ext4`. Other file systems will likely cause performance issues.

What to look for:

- Check the hardware `Platform Type`. Consider upgrading older hardware, especially older hardware running newer software such as 5.2 or later.
- `Version` shows the software version. Ensure you are running the latest software version with the newest report engine.
- Ensure `File System` is `Ext4`. Other file systems will likely cause performance issues.

diagnose fortilogd lograte

This command shows the log receive rate.

Following is a sample result of running this command.

```
logs/sec: 121091.0, logs/30sec: 119613.9, logs/60sec: 116695
```

What to look for

- If the log rate is higher than the sustained rates for your FortiAnalyzer model, the hardware is overloaded and needs an upgrade. The sustained rates for FortiAnalyzer models are listed in the Data Sheet on the FortiAnalyzer web page.

Check data policy and log storage policy

Check that the data policy and log storage policy are configured properly for each ADOM in each FortiAnalyzer unit. The data policy specifies how long to keep logs. The log storage policy affects logs and the SQL database. For details, see the *FortiAnalyzer Administration Guide*.

Check report and chart settings

Resolving hostnames usually takes a long time. If the DNS server is slow or does not support reverse DNS, report generation might hang. Check that `Resolve Hostname` is disabled:

- In *Reports Settings tab > Advanced Settings*, check that `Resolve Hostname` is not selected.
- In the *Chart Library*, check that `Resolve Hostname` is set to `Disabled`.

If you do not need to show all results, specify a lower maximum number of entries:

- In the *Chart Library*, check that the chart's `Show Top (0 for all results)` is not set too high. Setting this field to `0` for all results causes FortiAnalyzer to list all logs for the chart.

Check and adjust report auto-cache daemon

get system performance

This command shows system performance statistics such as CPU, memory, and I/O usage.

Following is a sample result of running this command.

```
CPU:
   Used:                   49.51%
   Used(Excluded NICE):   49.51%
        %used  %user  %nice  %sys  %idle %iowait  %irq %softirq
   CPU0 27.89  20.60   0.00  5.40  96.42    0.80   0.00     1.79
   CPU1 21.62  12.61   0.00  8.20  98.38    0.40   0.00     0.40
Memory:
   Total:  6,134,200 KB
   Used:   3,770,260 KB   61.5%
Hard Disk:
   Total:   82,434,736 KB
   Used:    65,283,648 KB  79.2%
   IOStat:  tps r_tps w_tps r_kB/s w_kB/s queue wait_ms  svc_ms %util sampling_sec
            4.7   0.2   4.4   27.5  144.2   0.2    52.5     8.4   3.9    599578.78
Flash Disk:
   Total:   499,656 KB
   Used:    314,416 KB     62.9%
   IOStat:  tps r_tps w_tps r_kB/s w_kB/s queue wait_ms  svc_ms %util sampling_sec
            0.0   0.0   0.0    0.0    0.0   0.0    13.6     4.6   0.0    599578.78
```

Following is a sample result of high `%iowait`. To see the `iowait` usage and limit, first enable debug messages for SQL commands (`diagnose debug enable`) and set the debug level (`diagnose debug application sqlrptcached 8`).

```
FAZVM64 # [530] iowait usage (27.5%) is over limit (23%).
[530] iowait usage (25.9%) is over limit (23%).
[530] iowait usage (28.3%) is over limit (23%).
```

What to look for

- Check the `Used` and `IOStat` lines to see if I/O is busy.
- If both CPU `%used` and `%iowait` are high, check if the report cache daemon is running:
  ```
  diagnose debug enable
  diagnose debug application sqlrptcached 8
  ```
- If `iowait` is over the limit, cache building (by `sqlrptcached`) will be paused until `iowait` drops below the limit. In this case, do one or both of the following:
  - Change the report schedule to run at a less busy time. To see scheduled reports, run `execute sql-report list-schedule <ADOM>`. To configure report schedules, see *Scheduling reports* in the *FortiAnalyzer Administration Guide*.
  - Enable `aggressive-schedule` so the report auto-cache daemon does not stop even under heavy system load:
    ```
    config system report auto-cache
       set aggressive-schedule enable
    end
    ```

Check and adjust report hcache

diagnose test application sqlrptcached 2

This command shows if hcache creation is able to catch up.

Following is a sample result of running this command.

```
Number of log table read: all=6453(fortiview=0, rpt=6453) pending=1
Number of log table done: all=6453(fortiview=0, rpt=6453) rpt=6453
Current hcache table entries: 155750
Number of hcache requests sent: 70999
Number of log table vacuums: 39401, pending=2
FortiView hcache load: rounds=817, tbl=653600
ncmdb:
cache hit: sch=0, config=27, chart=140, macro=0, dataset=140 config=27
calls : sch=130, config=11, chart=23, macro=0, dataset=23
```

The following table provides notes about some output lines in the example.

Line	Notes
`Number of log table read`	`pending`=0 means hcache creation is able to catch up. If `pending` is above 0, see What to look for below.
`Number of log table done`	The number of primary tables used to calculate the `Number of hcache requests sent`.
`Current hcache table entries`	Total hcache on the system.
`Number of hcache requests sent`	The number of charts per report * the number of primary tables * the number of reports.
`Number of log table vacuums`	The postgres built-in status. A `pending` number above 0 indicates insufficient postgres resources.
`FortiView hcache load`	`rounds` is the number of FortiView caches proactively loaded into memory.
`ncmdb`	Report configuration database.
`cache hit`	`config` is the number of enabled auto cache.

What to look for

- In `Number of log table read`, if the `pending` number is continuously above 0 or is increasing, that indicates there are too many pending log tables to read and the system lacks resources to create cache. In this case, consider disabling auto-cache on some reports. See *Enabling auto-cache* and *Reports Settings tab* in the *FortiAnalyzer Administration Guide*.
- Run `execute sql-report list-schedule <ADOM>` and check if there are too many scheduled reports and if auto-cache is enabled. See *Scheduling reports* and *Enabling auto-cache* in the *FortiAnalyzer Administration Guide*.
- Run `execute top` to check which applications are using the most system resources.

execute sql-report hcache-check <ADOM> <schedule-id>

This command shows a specific report’s hcache status.

If necessary, check the hcache status of a specific report that you think might be a problem.

For example, if the `ADOM` is `root` and `schedule-id` is `10004`, then run `execute sql-report hcache-check root 10004`.

To get the `schedule-id`, run `execute sql-report list-schedule root` and see the `NAME` column.

Following is a sample result of running the `execute sql-report hcache-check <ADOM> <schedule-id>` command.

```
layout_num:1
start [0] get layout-id:10004.
start report_process, layout-id:10004, layout title:Admin and System Events Report.
device list:All_FortiGates.
reports num:1.


device list[0].FWF60C3G13006291[root].
device list[1].FG3K2C3Z11800039[root].
......


> checking (10004_t10004-Admin and System Events Report) ...
checking chart Admin-Login-Summary...
8/8 (100%) done 0.131 secs used.
checking chart Admin-Login-Summary-By-Date...
8/8 (100%) done 0.128 secs used.
...
```

What to look for

- If a few reports are causing a bottleneck, check those reports’ Check the report diagnostic log on page 51 and consider reconfiguring those reports. See also Check and adjust report auto-cache daemon on page 56.

Report performance troubleshooting commands

CLI	Description
`diagnose debug application sqlrptcached 8`	Set the debug level of the SQL report cache daemon.
`diagnose debug crashlog read`	Print information of all crashed daemons. If daemons crash frequently, contact customer support for assistance.
`diagnose debug disable`	Disable debug message.
`diagnose debug enable`	Enable debug messages to run SQL diagnostic commands.
`diagnose fortilogd lograte`	Show the log receive rate.

CLI	Description
`diagnose fortilogd msgrate`	Show message receive rate. One message might contain multiple logs.
`diagnose log device`	Show disk quota for all logging devices.
`diagnose report status`	Show the maximum number of pending and running reports, and the current number of pending and running reports.
`diagnose test application sqlrptcached 2`	Show if hcache creation is able to catch up.
`diagnose sql show hcache-size`	Show the hcache size.
`diagnose sql status run-sql-rpt`	List the number of log tables, hcaches, and the time to generate each chart in the report.
`diagnose sql status sqlreportd`	Show SQL query connections and hcache status.
`execute sql-report hcache-check <ADOM> <schedule-id>`	Show a specific report's hcache status.
`execute sql-report list-schedule <ADOM>`	Show a summary table of all configured reports with their configuration status.
`execute top`	List the processes running on the FortiAnalyzer system.
`get system performance`	Show system performance statistics such as CPU, memory, and I/O usage.
`get system status`	Show the system status such as platform type (hardware or VM), firmware version, system time, disk usage, and file system format. Use this information to check if the hardware is overloaded. This information also helps you and customer support to quickly identify any issues and narrow down the investigation. • Ensure `Version` is the latest software version. • Check the hardware `Platform Type`. Consider upgrading older hardware, especially older hardware running newer software such as 5.2 or later. • Ensure `File System` is `Ext4`. Other file systems will likely cause performance issues.

`show system report auto-cache`	Show non-default settings in the report auto-cache.
	Ensure auto-cache is enabled by running these commands:
	`config system report auto-cache`
	`    set status enable`
	`end`

Troubleshooting a dataset query

The following topics provide guidance when troubleshooting a dataset query:

- Troubleshooting a custom dataset on page 60
- SQL functions for formatting and converting data types on page 60
- Macros for formatting date and time in a dataset on page 61

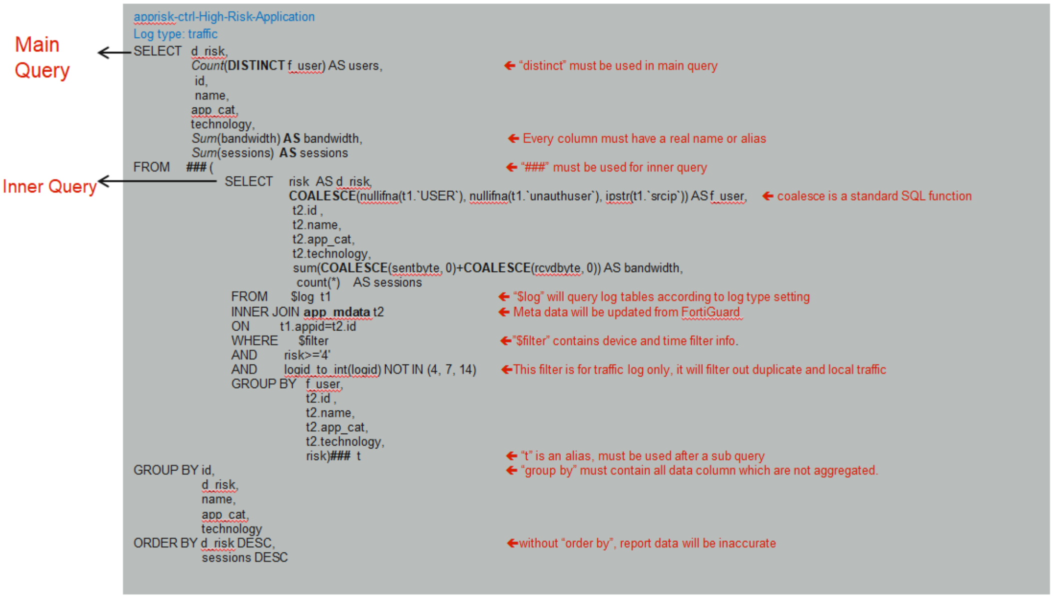
Troubleshooting a custom dataset

This topic provides a list and an example of common issues in a custom dataset that cannot be identified by the dataset test console.

Common issues:

- `$filter` is not applied.
- No `###` for inner query.
- `distinct` is used in inner query.
- No column alias for column with function.
- no hcache merge for `count distinct`.
- No *group by* or `order by`.
- Log tables are not joined. For example, join traffic log with IPS log.
- Dataset test console is out of memory.

The image below indicates where common issues may appear in the dataset:



```
apprisk-ctrl-High-Risk-Application
Log type: traffic
SELECT  d_risk,
        Count(DISTINCT f_user) AS users,                          ← "distinct" must be used in main query
         id,
         name,
        app_cat,
        technology,
        Sum(bandwidth) AS bandwidth,                               ← Every column must have a real name or alias
        Sum(sessions)  AS sessions
FROM    ### (                                                      ← "###" must be used for inner query
            SELECT    risk  AS d_risk,
                      COALESCE(nullifna(t1.`USER`), nullifna(t1.`unauthuser`), ipstr(t1.`srcip`)) AS f_user,   ← coalesce is a standard SQL function
                       t2.id ,
                       t2.name,
                       t2.app_cat,
                       t2.technology,
                       sum(COALESCE(sentbyte, 0)+COALESCE(rcvdbyte, 0)) AS bandwidth,
                        count(*)    AS sessions
            FROM      $log  t1                                     ← "$log" will query log tables according to log type setting
            INNER JOIN app_mdata t2                                ← Meta data will be updated from FortiGuard
            ON       t1.appid=t2.id
            WHERE     $filter                                      ←"$filter" contains device and time filter info.
            AND      risk>='4'
            AND      logid_to_int(logid) NOT IN (4, 7, 14)         ←This filter is for traffic log only, it will filter out duplicate and local traffic
            GROUP BY  f_user,
                      t2.id ,
                      t2.name,
                      t2.app_cat,
                      t2.technology,
                      risk)###  t                                  ← "t" is an alias, must be used after a sub query
GROUP BY id,                                                       ← "group by" must contain all data column which are not aggregated.
         d_risk,
         name,
         app_cat,
         technology
ORDER BY d_risk DESC,                                              ←without "order by", report data will be inaccurate
         sessions DESC
```

SQL functions for formatting and converting data types

The following SQL functions can be used to format or convert different data types:

SQL function	Description
`from_itime / from_dtime`	Converts timestamp to formatted date/time.
`ipstr`	Converts `srcip/dstip` field from `inet` to string.
`app_group_name`	Groups similar application names.
root_domain	Groups similar `hostnames`.
`vpn_trim`	Groups similar VPN tunnels.
`nullifna`	Converts `N/A` to `null`.
`logid_to_int`	Trims `logid`.

Macros for formatting date and time in a dataset

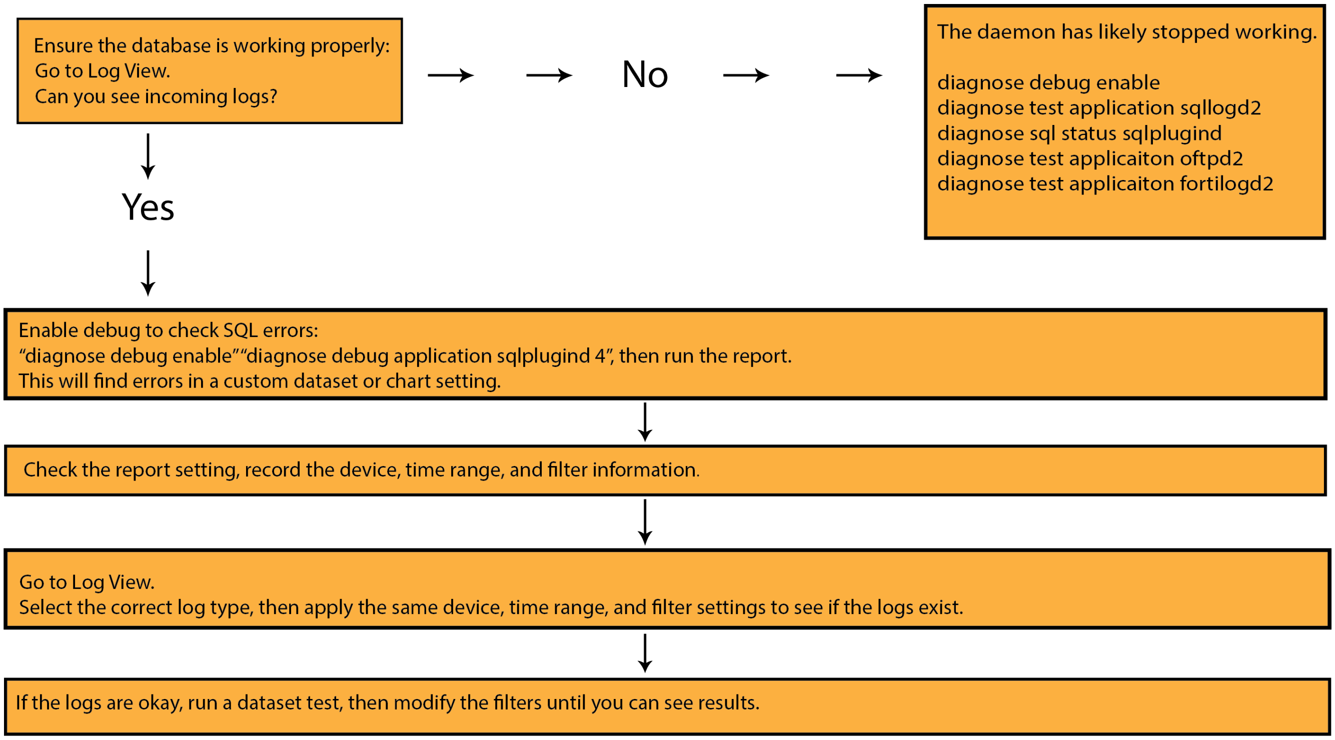
The following macros can be used to fine tune date and time formatting in a dataset:

Macros	Description	Example
$flex_timescale	Time scale changes according to the report time period: • Time period > 28 days • Time period > 12 hours and <= 28 days • Time period > 4 hours and <= 12 hours • Time period > 1 hour • <= hour	• Display day: 2018-02-25 • Display hour: 2018-02-25 14:00 • Display 30 min granularity: 2018-02-25 14:30 • Display 5 min granularity: 2018-02-25 14:40 • display 1 min granularity: 2018-02-25 14:42
$hour_of_day	Displays hour in 24 hr format.	18:00
$HOUR_OF_DAY	Displays date (YYYY-MM-DD) and hour in 24 hr format.	2018-01-13 18:00
$DAY_OF_MONTH	Displays month in format YYYY-MM-DD (2017-01-10).	2018-01-01
$day_of_month	Displays day of the month in two digits format 01-12.	01
$day_of_week	Displays number and name of the day of the week (WDAY 2-Mon).	Mon

Troubleshooting an empty chart

To troubleshoot an empty chart in a report, go to Log View to verify logs are incoming.

- If you see logs check for SQL errors.
- If you don't see any logs the daemon may have stopped working.



Ensure the database is working properly:
Go to Log View.
Can you see incoming logs?

No

The daemon has likely stopped working.

diagnose debug enable
diagnose test application sqllogd2
diagnose sql status sqlplugind
diagnose test applicaiton oftpd2
diagnose test applicaiton fortilogd2

Yes

Enable debug to check SQL errors:
“diagnose debug enable”“diagnose debug application sqlplugind 4”, then run the report.
This will find errors in a custom dataset or chart setting.

Check the report setting, record the device, time range, and filter information.

Go to Log View.
Select the correct log type, then apply the same device, time range, and filter settings to see if the logs exist.

If the logs are okay, run a dataset test, then modify the filters until you can see results.

CLI commands for troubleshooting

The following table provides a list of CLI commands to troubleshoot an empty chart in a report:

Command	Description
Check report running/pending status	`diagnose report status {running | pending}`

Debug sql query	`diagnose debug enable`
	`diagnose debug application sqlplugind 4  -----errors only`
	`diagnose debug application sqlplugind 8`

List current SQL process	`diagnose sql process list`
Configure global report automatic cache setting	`config system report auto-cache`
List report schedule/auto-cache status by ADOM	`execute sql-report list-schedule <ADOM-name>`
Diagnose report hcache working status	`diagnose test application sqlrptcached 2`
Check individual report hcache status	`execute sql-report hcache-check <ADOM-name> <schedule-id>`

Check report status during report running	`diagnose debug enable`
	`diagnose sql status sqlreportd`

Common issues

The following table provides a list of common issues that may produce an empty chart in a report:

Issue	Description
Wrong report filter applied	Go to *Log View* and search for: • Field “status” changed to “action” (since 5.0.6) • Data type of `srcip` and `dstip` changed from string to `inet`.
Log field changed after upgrade	This can be identified by a dataset test console or SQL debug.
Hcache corrupt	Clear hcache before running the report (`dia sql remove hcache`).
Log traffic	• High log rate (`diagnose fortilogd lograte`) • Device or ADOM quota reached (`diagnose log device`)
“logver” issue	Some datasets are using field “logver” to identify FOS log version. Go to *Log View* and search for `logver=*` If there are no records, you may need to upgrade.
"out of memory”	File system error. This occurs mostly in 5.2.

FORTINET®

www.fortinet.com