FORTINET
NSE
7
ARCHITECT

OT Security
Lab Guide

for FortiOS 7.2

FORTINET®
Training Institute

Fortinet Training Institute - Library

https://training.fortinet.com

Fortinet Product Documentation

https://docs.fortinet.com

Fortinet Knowledge Base

https://kb.fortinet.com

Fortinet Fuse User Community

https://fusecommunity.fortinet.com/home

Fortinet Forums

https://forum.fortinet.com

Fortinet Product Support

https://support.fortinet.com

FortiGuard Labs

https://www.fortiguard.com

Fortinet Training Program Information

https://www.fortinet.com/nse-training

Fortinet | Pearson VUE

https://home.pearsonvue.com/fortinet

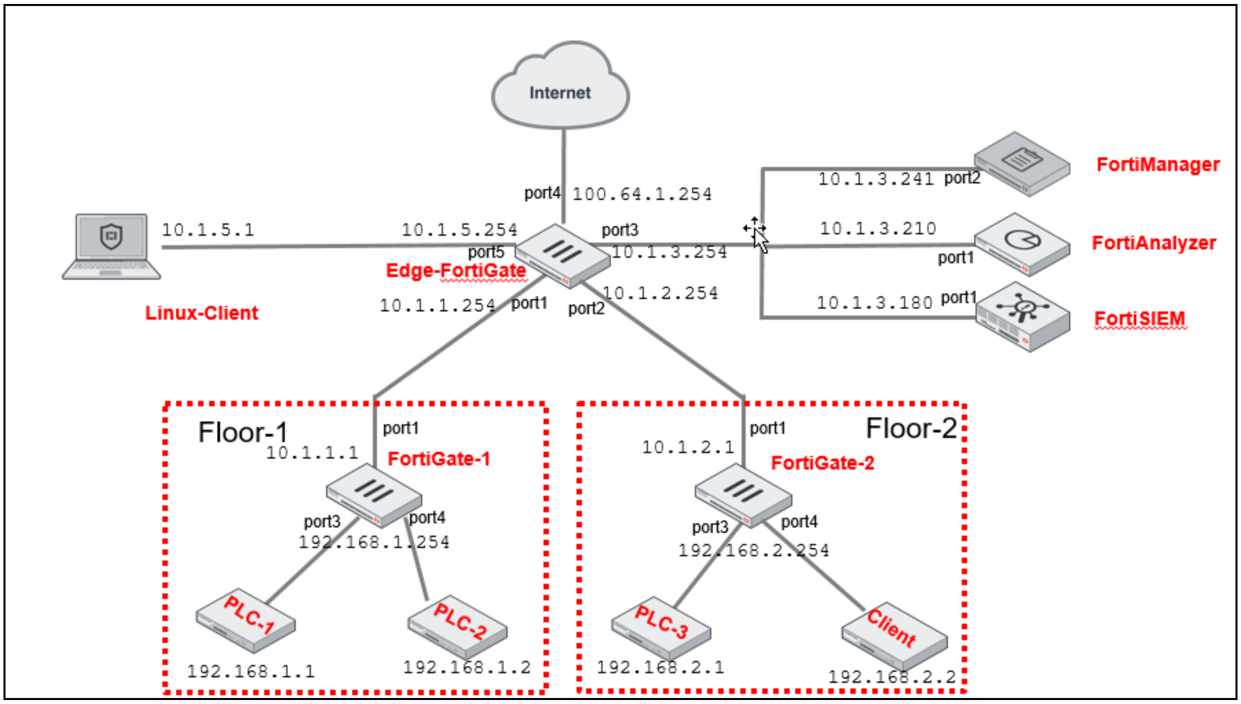
Fortinet Training Institute Helpdesk (training questions, comments, feedback)

https://helpdesk.training.fortinet.com/support/home

11/22/2022

TABLE OF CONTENTS

Network Topology



Lab 1: Introduction

There is no lab associated with this lesson.

Lab 2: Device Detection

In this lab, you will learn to configure the Fortinet Security Fabric with device detection. After you configure the Security Fabric, you will access the physical and logical topology views.

Objectives

- Configure the Security Fabric on Edge-FortiGate (root), FortiGate-1, and FortiGate-2
- Use the Security Fabric topology views to have logical and physical views of your network topology

Time to Complete

Estimated: 30 minutes

VM Username and Passwords

VM	Username	Password
Linux-Client	Supervisor	password
Edge-FortiGate	admin	password
FortiGate-1	admin	password
FortiGate-2	admin	password
FortiAnalyzer	admin	password
FortiSIEM	admin	Fortinet1!
PLC-1	sysadmin	Fortinet1!
PLC-2	sysadmin	Fortinet1!
PLC-3	sysadmin	Fortinet1!
Client	sysadmin	Fortinet1!

Exercise 1: Configuring Device Detection on FortiGate

In this exercise, you will configure the Security Fabric between Edge-FortiGate (root), FortiGate-1 (leaf), and FortiGate-2 (leaf).

Configure FortiAnalyzer Logging on Edge-FortiGate (Root)

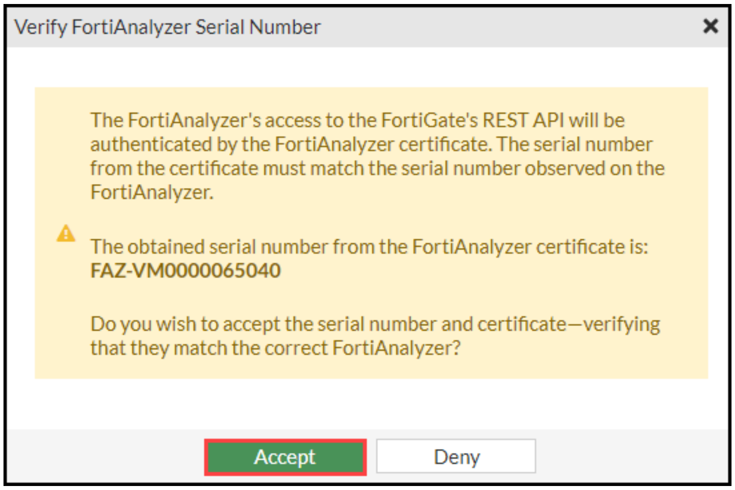
You will configure the root of the Security Fabric to send all logs to FortiAnalyzer. These settings are automatically replicated to all downstream devices when they become members of the Security Fabric.

To configure Edge-FortiGate (root) to send logs to FortiAnalyzer

1. Log in to the Edge-FortiGate GUI with the username `admin` and password `password`.
2. Click **Security Fabric** > **Fabric Connectors**.
3. Select **FortiAnalyzer Logging**, and then click **Edit**.
4. In the **FortiAnalyzer Settings** section, configure the following settings:

Field	Value
Status	Enable
IP address	10.1.3.210
Upload option	Real Time

5. Click **OK**.
6. In the verification window that appears, click **Accept**.



Verify FortiAnalyzer Serial Number

The FortiAnalyzer's access to the FortiGate's REST API will be authenticated by the FortiAnalyzer certificate. The serial number from the certificate must match the serial number observed on the FortiAnalyzer.

The obtained serial number from the FortiAnalyzer certificate is: **FAZ-VM0000065040**

Do you wish to accept the serial number and certificate—verifying that they match the correct FortiAnalyzer?

A warning appears that states FortiGate isn't authorized on FortiAnalyzer yet. You will configure this authorization on FortiAnalyzer in a later step.

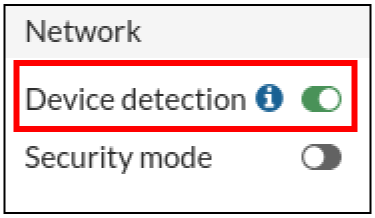
7. Click **Close**.

Configure the Security Fabric on Edge-FortiGate (Root)

You will configure the root of the Security Fabric tree.

To enable the Security Fabric connection on the Edge-FortiGate interfaces

1. On the Edge-FortiGate GUI, click **Network** > **Interfaces**.
2. Click **port5**, and then click **Edit**.
3. In the **Network** section, enable **Device detection**.



Network

Device detection ℹ ●

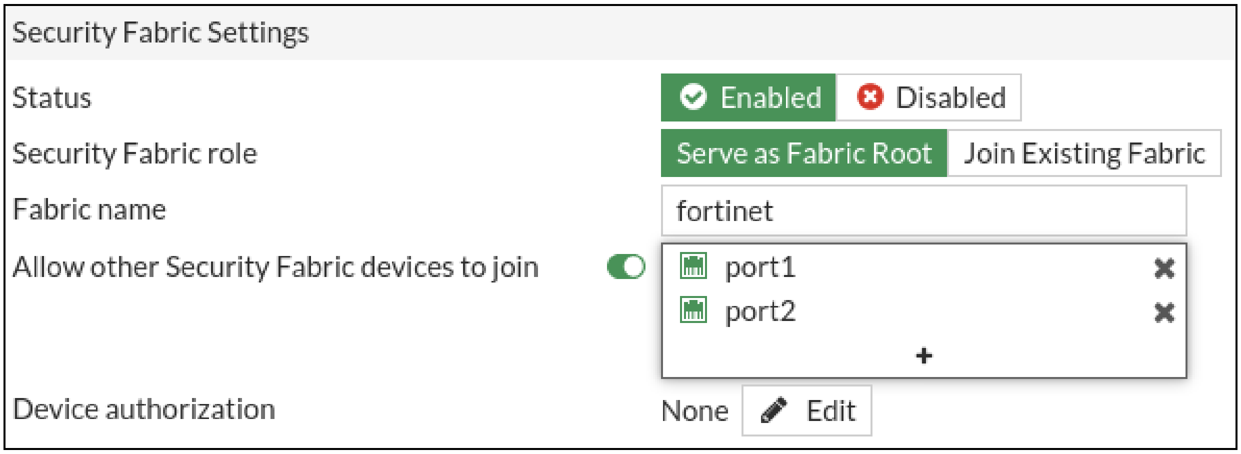
Security mode ○

4. Click **OK**.

To enable the Security Fabric on Edge-FortiGate

1. On the Edge-FortiGate GUI, click **Security Fabric** > **Fabric Connectors**.
2. Click **Security Fabric Setup**, and then click **Edit**.
3. In the **Security Fabric role** field, select **Serve as Fabric Root**.
4. Configure the following settings:

Field	Value
Status	Enable
Security Fabric role	Serve as Fabric Root
Fabric name	fortinet
Allow other Security Fabric devices to join	Enable, and then ensure that both interfaces (**port1** and **port2**) are selected.



Security Fabric Settings

Status: Enabled | Disabled

Security Fabric role: Serve as Fabric Root | Join Existing Fabric

Fabric name: fortinet

Allow other Security Fabric devices to join: port1, port2

Device authorization: None Edit

5. Click **OK**.

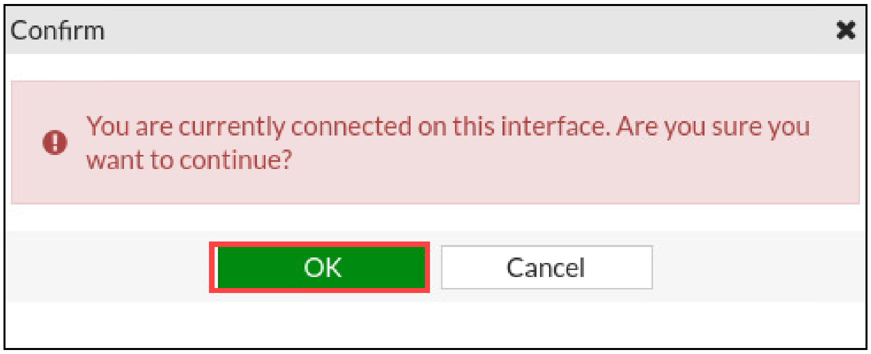
Configure the Security Fabric on FortiGate-1

You will configure a leaf of the Security Fabric tree.

To enable the Security Fabric connection on the FortiGate-1 interfaces

1. Log in to the FortiGate-1 GUI with the username `admin` and password `password`.
2. Click **Network** > **Interfaces**.
3. Click **port1**, and then click **Edit**.
4. In the **Administrative Access** section, select the **Security Fabric Connection** checkbox.
5. In the **Network** section, enable **Device detection**.
6. Click **OK**.

If the following warning appears, click **OK**:



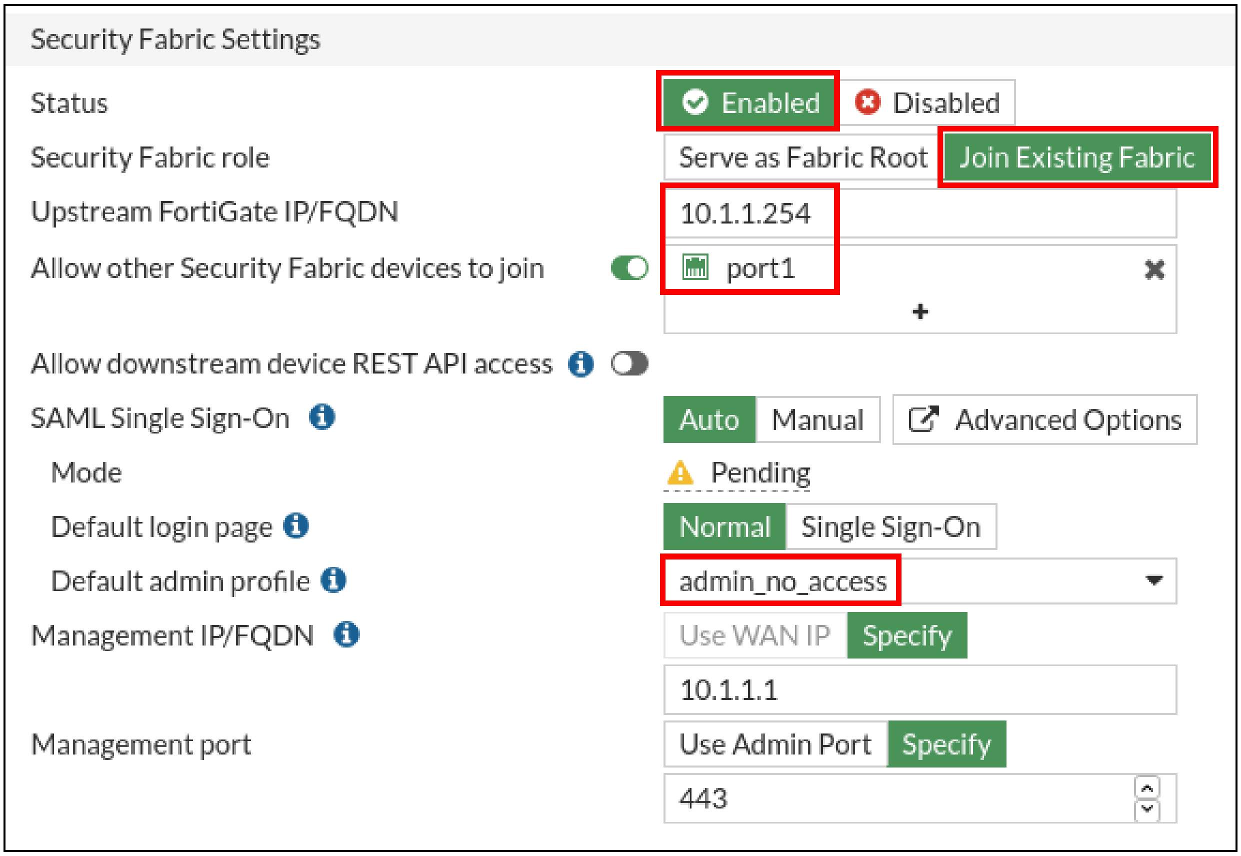
Confirm

You are currently connected on this interface. Are you sure you want to continue?

To enable the Security Fabric on FortiGate-1 (leaf)

1. On the FortiGate-1 GUI, click **Security Fabric** > **Fabric Connectors**.
2. Click **Security Fabric Setup**, and then click **Edit**.
3. In the **Security Fabric Settings** section, in the **Status** field, select **Enabled**.
4. In the **Security Fabric role** field, confirm that **Join Existing Fabric** is selected.

5. In the **Upstream FortiGate IP/FQDN** field, make sure the IP address is `10.1.1.254`.
6. In the **Default admin profile** field, select **admin_no_access**.



Security Fabric Settings

Status: ✓ Enabled | Disabled

Security Fabric role: Serve as Fabric Root | Join Existing Fabric

Upstream FortiGate IP/FQDN: 10.1.1.254

Allow other Security Fabric devices to join: port1

Allow downstream device REST API access

SAML Single Sign-On: Auto | Manual | Advanced Options

Mode: Pending

Default login page: Normal | Single Sign-On

Default admin profile: admin_no_access

Management IP/FQDN: Use WAN IP | Specify

10.1.1.1

Management port: Use Admin Port | Specify

443

7. Click **OK**.
8. Click **OK**.

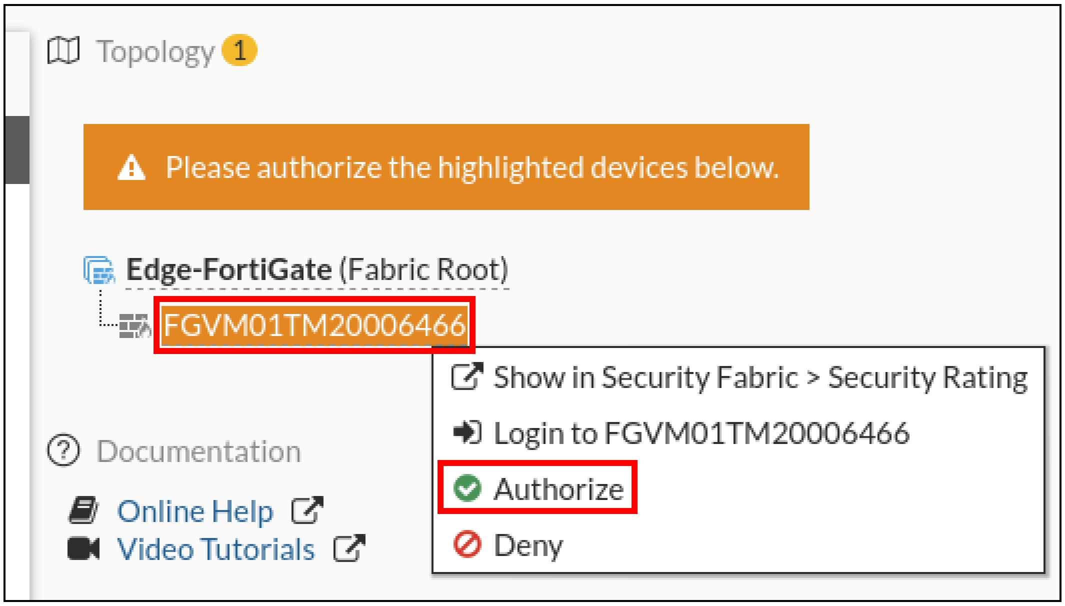
FortiAnalyzer logging is enabled after FortiTelemetry is enabled. FortiAnalyzer settings are retrieved from the root Edge-FortiGate when FortiGate-1 connects to the root Edge-FortiGate.

Authorize the Downstream FortiGate (FortiGate-1) on the Root FortiGate (Edge-FortiGate)

You will authorize FortiGate-1 on the root Edge-FortiGate to join the Security Fabric.

To authorize the downstream FortiGate-1 on the root Edge-FortiGate

1. On the Edge-FortiGate GUI, click **Security Fabric** > **Fabric Connectors**.
2. In the **Topology** section, click the highlighted FortiGate serial number, and then click **Authorize**.


Topology 1
Please authorize the highlighted devices below.
Edge-FortiGate (Fabric Root)
FGVM01TM20006466
Show in Security Fabric > Security Rating
Login to FGVM01TM20006466
Authorize
Deny
Documentation
Online Help
Video Tutorials

3. In the **Device Registration** window, in the **Devices** field, ensure the FortiGate serial number is selected, and then click **Authorize**.

If the serial number is not displayed, refresh the page, and then repeat step 2.

4. Click **Close**.

After authorization, FortiGate-1 appears in the Security Fabric topology section, which means FortiGate-1 joined the Security Fabric successfully.

5. Hover over the **FortiGate-1** icon to display a summary of the firewall settings, and then verify that it is correctly registered in the Security Fabric.

Configure the Security Fabric on FortiGate-2

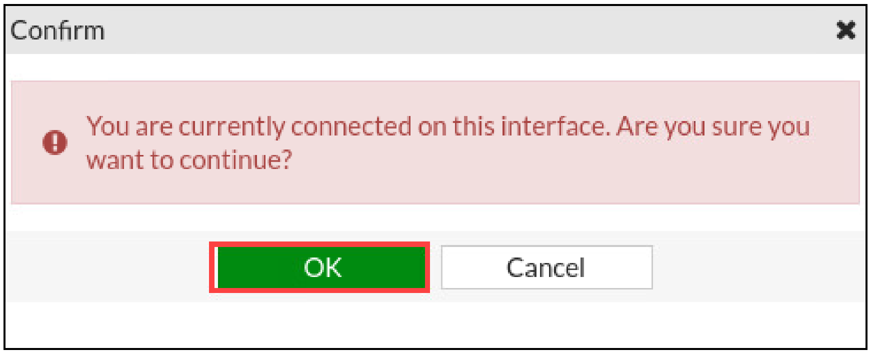
You will configure a leaf of the Security Fabric tree.

To enable the Security Fabric connection on the FortiGate-2 interfaces

1. Log in to the FortiGate-2 GUI with the username `admin` and password `password`.
2. Click **Network** > **Interfaces**.
3. Click **port1**, and then click **Edit**.
4. In the **Administrative Access** section, select the **Security Fabric Connection** checkbox.

5. In the **Network** section, enable **Device detection**.
6. Click **OK**.

If the following warning appears, click **OK**:



Confirm

You are currently connected on this interface. Are you sure you want to continue?

To enable the Security Fabric on FortiGate-2 (leaf)

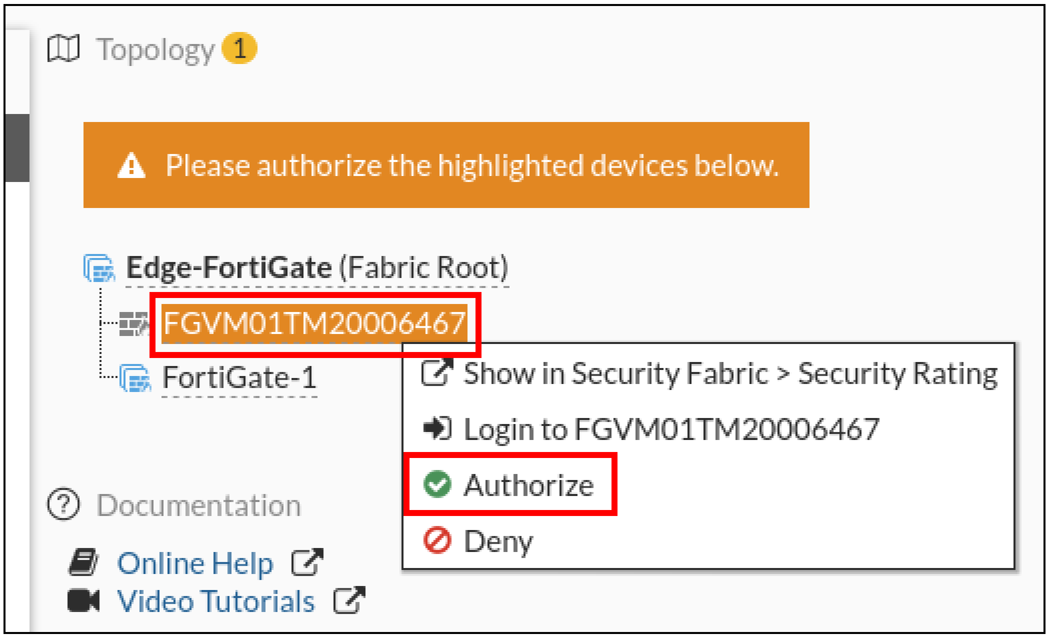
1. On the FortiGate-2 GUI, click **Security Fabric** > **Fabric Connectors**.
2. Click **Security Fabric Setup**, and then click **Edit**.
3. In the **Security Fabric Settings** section, in the **Status** field, select **Enabled**.
4. In the **Security Fabric role** field, confirm that **Join Existing Fabric** is selected.
5. In the **Upstream FortiGate IP/FQDN** field, make sure the IP address is `10.1.2.254`.
6. In the **Default admin profile** field, select **admin_no_access**.
7. Click **OK**.
8. Click **OK**.

Authorize the Downstream FortiGate (FortiGate-2) on the Root FortiGate (Edge-FortiGate)

You will authorize FortiGate-2 on the root Edge-FortiGate to join the Security Fabric.

To authorize the downstream FortiGate-2 on the root Edge-FortiGate

1. On the Edge-FortiGate GUI, click **Security Fabric** > **Fabric Connectors**.
2. In the **Topology** section, click the highlighted FortiGate serial number, and then click **Authorize**.


Topology 1
Please authorize the highlighted devices below.
Edge-FortiGate (Fabric Root)
FGVM01TM20006467
FortiGate-1
Show in Security Fabric > Security Rating
Login to FGVM01TM20006467
Authorize
Deny
Documentation
Online Help
Video Tutorials

3. In the **Device Registration** window, in the **Devices** field, ensure the FortiGate serial number is selected, and then click **Authorize**.

If the serial number is not displayed, refresh the page, and then repeat step 2.

4. Click **Close**.

After authorization, FortiGate-2 appears in the Security Fabric topology section, which means FortiGate-2 joined the Security Fabric successfully.

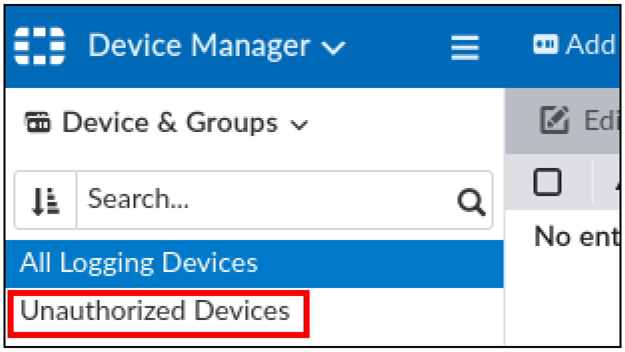
5. Hover over the **FortiGate-2** icon to display a summary of the firewall settings, and then verify that it is correctly registered in the Security Fabric.

Authorize All Security Fabric FortiGate Devices on FortiAnalyzer

You will authorize all Security Fabric devices on FortiAnalyzer.

To authorize Edge-FortiGate, FortiGate-1, and FortiGate-2 on FortiAnalyzer

1. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. Click **Device Manager**.
3. In the **Device & Groups** section, click **Unauthorized Devices**.



All three FortiGate devices appear as unauthorized devices.

4. Select the **Edge-FortiGate**, **FortiGate-1**, and **FortiGate-2** checkboxes, and then click **Authorize**.
5. Click **OK** to keep the default FortiGate device names.
6. In the **Authorize Device** wizard, click **Close**.

   All three devices are added to the FortiAnalyzer root ADOM.

7. Wait a few seconds until the **Logs** status for all FortiGate devices turns green.

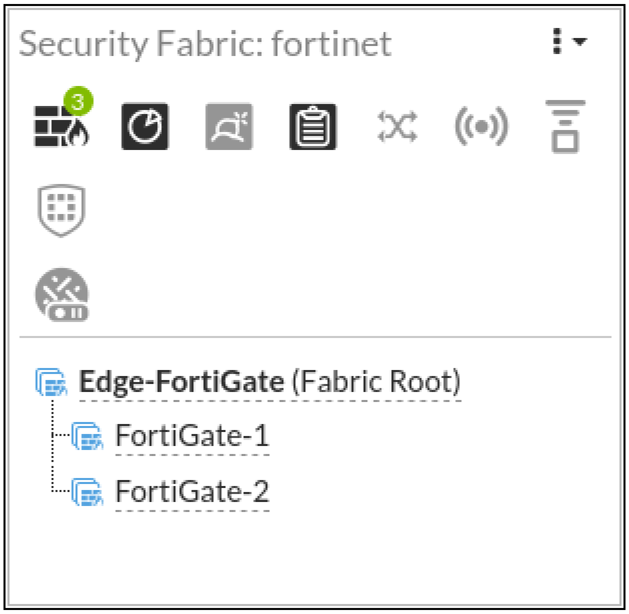
Check the Security Fabric Deployment Result

You will check the Security Fabric deployment result on the root Edge-FortiGate.

To check the Security Fabric on Edge-FortiGate

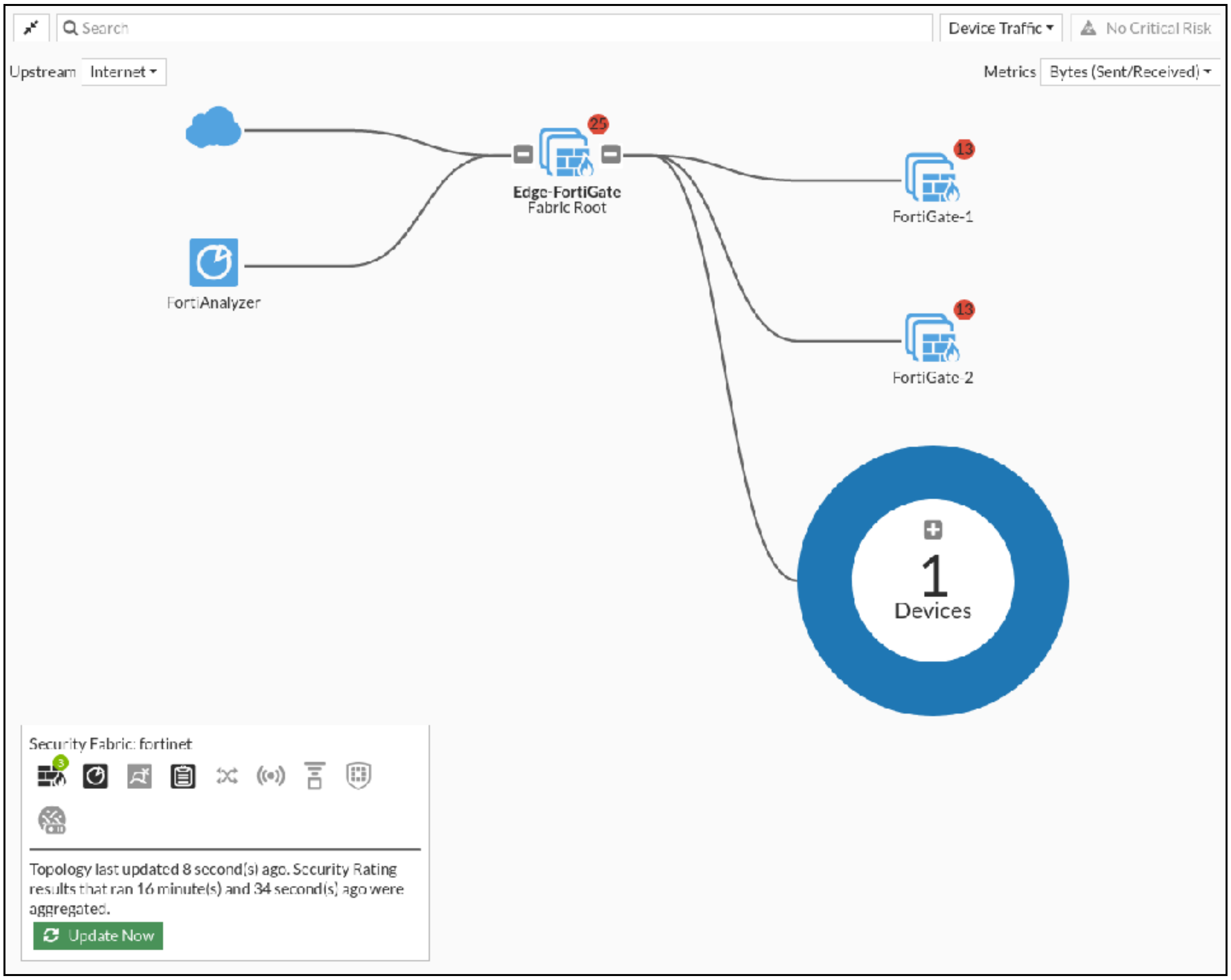
1. On the Edge-FortiGate GUI, click **Dashboard** > **Status**.

   The **Security Fabric** widget displays all FortiGate devices in the Security Fabric.



2. On the Edge-FortiGate GUI, click **Security Fabric** > **Physical Topology**.

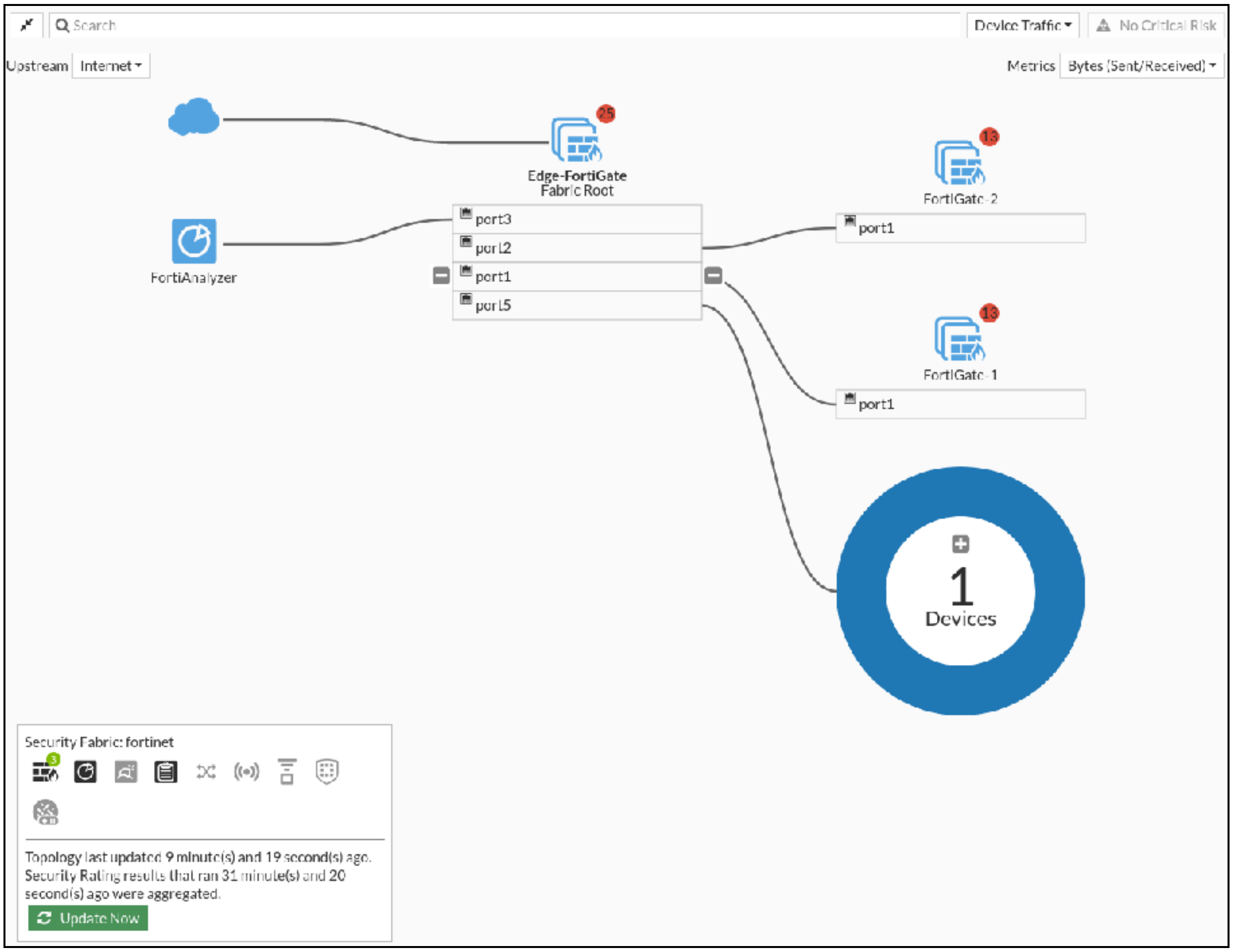
   This page shows a visualization of access layer devices in the Security Fabric.



Topology last updated 8 second(s) ago. Security Rating results that ran 16 minute(s) and 34 second(s) ago were aggregated.

3. On the Edge-FortiGate GUI, click **Security Fabric** > **Logical Topology**.

   This dashboard displays information about the interfaces that each device in the Security Fabric connects to.



Topology last updated 9 minute(s) and 19 second(s) ago. Security Rating results that ran 31 minute(s) and 20 second(s) ago were aggregated.

Lab 3: Access Control

In this lab, you will configure local authentication on FortiGate-1 and FortiGate-2.

This lab uses a demo environment to emulate the behavior of an active FSSO DC agent from the Linux-Client VM using a Python script. Therefore, you will not configure a DC agent to send logon events from the Linux-Client VM.

Objectives

- Configure local authentication and apply it to policies
- Review the SSO configuration on FortiGate
- Test the transparent or automatic user identification by generating user logon events
- Monitor the SSO status and operation

Time to Complete

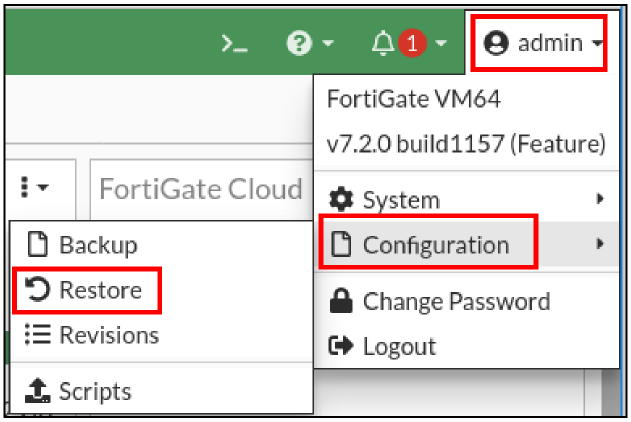
Estimated: 30 minutes

Prerequisites

Before you begin this lab, you must restore the initial configuration files to the FortiGate devices. The configuration files are located on the desktop of the Linux-Client VM.

To restore the FortiGate-1 configuration file

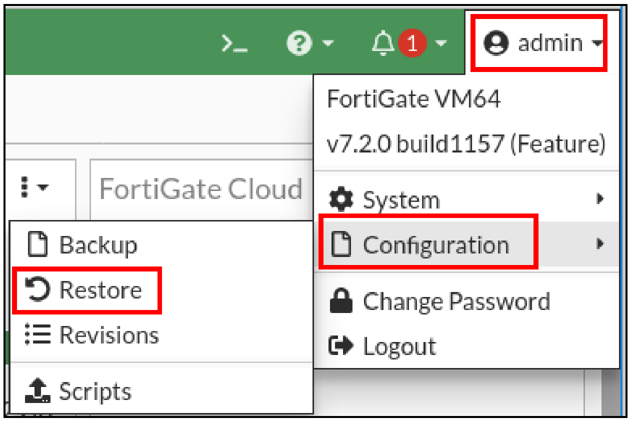
1. Log in to the FortiGate-1 GUI at `10.1.1.1` with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **Access_Control**, select `FortiGate-1_access_control.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

To restore the FortiGate-2 configuration file

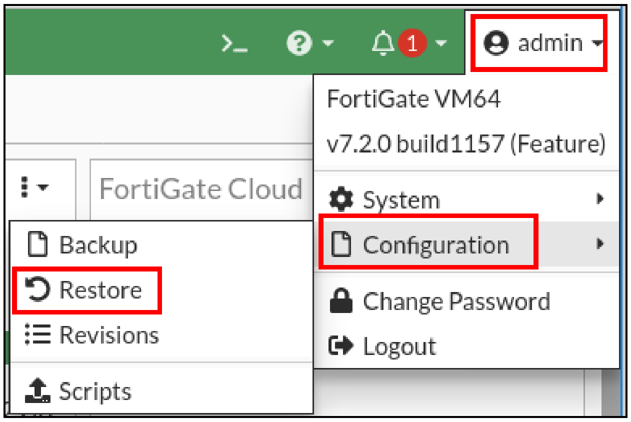
1. Log in to the FortiGate-2 GUI at `10.1.2.1` with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **Access Control**, select `FortiGate-2_access_control.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

To restore the Edge-FortiGate configuration file

1. On the Linux-Client VM, open a browser, and then log in to the Edge-FortiGate GUI at `10.1.5.254` with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **Access Control**, select `Edge-FortiGate_access_control.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

Exercise 1: Configuring Local Authentication

In this exercise, you will configure local users and use them as part of policy-based authentication to allow access to programmable logic controllers (PLCs).

Configure Local Users

You will configure local users on FortiGate-1 and FortiGate-2.

To configure local users

1. Log in to the FortiGate-1 GUI with the username `admin` and password `password`.
2. Click **User & Authentication** > **User Definition**, and then click **Create New**.
3. Configure the following settings:

Field	Value
User Type	Local User
Username	supervisor
Password	password

4. Click **Submit**.
5. Click **Create New**.
6. Configure the following settings:

Field	Value
User Type	Local User
Username	PLC1admin
Password	password

7. Click **Submit**.
8. Log in to the FortiGate-2 GUI with the username `admin` and password `password`.
9. Click **User & Authentication** > **User Definition** > **Create New**.
10. Configure the following settings:

Field	Value
User Type	Local User
Username	supervisor
Password	password

11. Click **Submit**.

Configure Firewall Policy Authentication

You will configure firewall policy authentication to allow authorized users to access the PLCs.

To configure firewall policies

1. On the FortiGate-1 GUI, click **Policy & Objects** > **Firewall Policy**.
2. Click **Create New**, and then configure the following settings:

Field	Value
Name	PLC-2_Access
Incoming Interface	port1
Outgoing Interface	Floor-1_Switch
Source	all supervisor (located under **User**)
Destination	PLC-2
Service	ALL
NAT	disable

3. Click **OK**.
4. Click **Create New**, and then configure the following settings:

Field	Value
Name	PLC-1_Access
Incoming Interface	port1
Outgoing Interface	Floor-1_Switch
Source	all supervisor and PLC1admin (located under **User**)
Destination	PLC-1
Service	ALL
NAT	disable

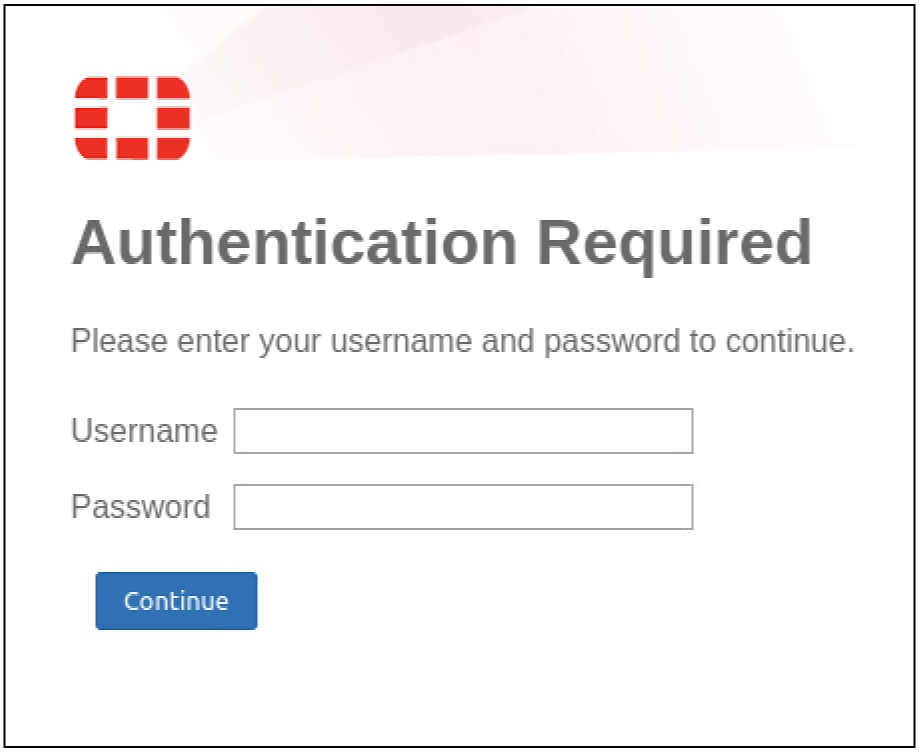
5. Click **OK**.
6. On the Linux-Client VM, close all browsers that are open.

Test the Policy-Based Authentication

You will test the policy-based authentication from the Linux-Client VM.

To test the policy-based authentication

1. On the Linux-Client VM, open a browser, and then access PLC-1 at `http://192.168.1.1`.
   FortiGate sends an authentication page for user authentication.
2. Type the username `PLC1admin` and password `password`, and then click **Continue**.



Authentication Required

Please enter your username and password to continue.

   You are redirected to the PLC-1 web page.
3. Open another browser tab, and then open the PLC-2 web page at `http://192.168.1.2`.

Notice that you cannot connect to the PLC-2 page. This is because the user is already registered with the IP address and is not allowed to access PLC-2.

4. Close the browser to clear the cache.
5. Log in to the FortiGate-1 GUI with the username `admin` and password `password`.
6. Click **Dashboard** > **Users & Devices**.
7. Expand **Firewall Users**.
8. If the PLC1admin user is still logged in, deauthenticate this user.
9. On the Linux-Client VM, close all browsers.
10. On the Linux-Client VM, open a new browser, and then access PLC-1 at `http://192.168.1.1`.

FortiGate sends an authentication page for user authentication.

11. Type the username `supervisor` and password `password`, and then click **Continue**.

    You are redirected to the PLC-1 web page.

12. Open another browser tab, and then open the PLC-2 web page at `http://192.168.1.2`.

Notice that this time, you are not required to authenticate the user. Because the `supervisor` user also has access to PLC-2, you can access PLC-2 without having to authenticate the user.

Exercise 2: Configuring FSSO Authentication

In this exercise, you will assign FSSO users to a firewall policy and test the user authentication to access PLCs protected by FortiGate.

This lab uses a demo environment to emulate the behavior of an active FSSO DC agent from the Linux-Client VM using a Python script. Therefore, you will not configure a DC agent to send logon events from the Linux-Client VM.

In the real world, you must configure FortiGate to identify users by polling their logon events using an FSSO agent, and you must install and configure a collector agent. FSSO agents are available on the Fortinet Support website (http://support.fortinet.com).

For FortiGate to communicate and poll information from the FSSO collector agent, you must assign the polled user to a firewall user group, and then add the user group as a source on a firewall policy.

Finally, you can verify the user logon event that FortiGate collects. This event is generated after a user logs in to the Windows Active Directory domain. Therefore, no firewall authentication is required.

Review the FSSO Configuration on FortiGate

You will review the FSSO configuration and FSSO user groups on Edge-FortiGate. FSSO allows FortiGate to automatically identify the users who connect using SSO. Then, you will add FSSO user groups to the firewall policies.

To review the FSSO server and FSSO user group configuration on FortiGate

1. Log in to the Edge-FortiGate GUI with the username `admin` and password `password`.
2. Click **Security Fabric** > **External Connectors**.
3. Select **TrainingDomain**, and then click **Edit**.
4. In the upper-right corner, review the **Endpoint/Identity** status, and see that the status is **Disconnected**.

   Leave the window open.

To run a script to simulate a user logon event

1. On the Linux-Client VM, open a terminal window, and then run the following commands to simulate a user logon event:

   ```
   cd Desktop/FSSO/
   python2 fssoreplay.py -l 8000 -f sample.log
   ```

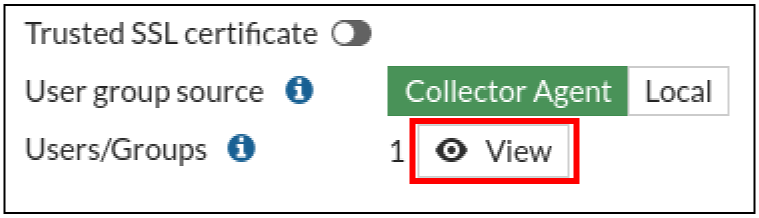
   Keep the terminal window open. The script will continue to run in the background.

To review the FSSO connection and FSSO user groups

1. Continuing on the **TrainingDomain** window, click **Apply & Refresh**.

The **Security Fabric** > **External Connectors** window is displayed.

2. Select **TrainingDomain**, and then click **Edit**.
3. In the **Users/Groups** field, click **View**.



You can see the **TRAININGAD/Management_Users** monitored group.

4. Click **X** to close the **Collector Agent Group Filters** window.
5. Click **OK**.
   A green up arrow confirms that communication with the FSSO collector agent is up.

To assign the FSSO user to an FSSO user group

1. On the Edge-FortiGate GUI, click **User & Authentication** > **User Groups**.
2. Click **Create New**, and then configure the following settings:

Field	Value
Name	Management
Type	Fortinet Single Sign-On (FSSO)
Members	TRAININGAD/Management_Users

The FSSO user is automatically listed because of the selected group type—FSSO.

3. Click **OK**.

Assign FSSO Users to a Firewall Policy

You will assign your FSSO user group as a source on a firewall policy. This allows you to control access to network resources based on user identity.

To add the FSSO user group to the firewall policy

1. Log in to the Edge-FortiGate GUI with the username `admin` and password `password`.
2. Click **Policy & Objects** > **Firewall Policy**.
3. Click **Create New**, and then configure the following settings:

Field	Value
Name	Floor-2_Access
Incoming Interface	port5
Outgoing Interface	port2
Source	all Management (located under **User**)
Destination	all
Service	ALL
NAT	disable
Log Allowed Traffic	All Sessions

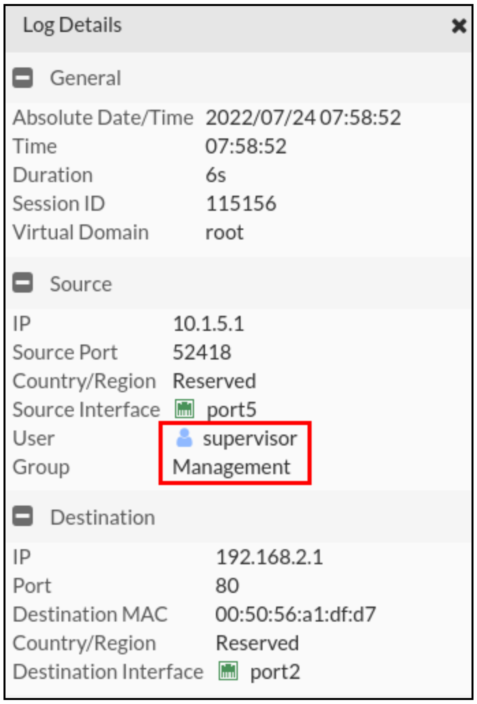
4. Click **OK**.

Test the User Authentication

You will test the user authentication from the Linux-Client VM.

To test the user authentication

1. On the Linux-Client VM, open a new browser, and then access PLC-3 at `http://192.168.2.1`.
   You are redirected to the PLC-3 web page without an authentication prompt.
2. Log in to the Edge-FortiGate GUI with the username `admin` and password `password`.
3. Click **Log & Report** > **Forward Traffic**.
4. Select a log, and then click **Details** to view more information about it.



Log Details

General

```
Absolute Date/Time  2022/07/24 07:58:52
Time                07:58:52
Duration            6s
Session ID          115156
Virtual Domain      root
```

Source

```
IP                10.1.5.1
Source Port       52418
Country/Region    Reserved
Source Interface  port5
User              supervisor
Group             Management
```

Destination

```
IP                     192.168.2.1
Port                   80
Destination MAC        00:50:56:a1:df:d7
Country/Region         Reserved
Destination Interface  port2
```

Lab 4: Segmentation

In this lab, you will configure microsegmentation with Edge-FortiGate, FortiGate-1, and FortiGate-2.

Objectives

- Configure software switches on FortiGate-1 and FortiGate-2
- Allow traffic between software switch members based on requirements

Time to Complete

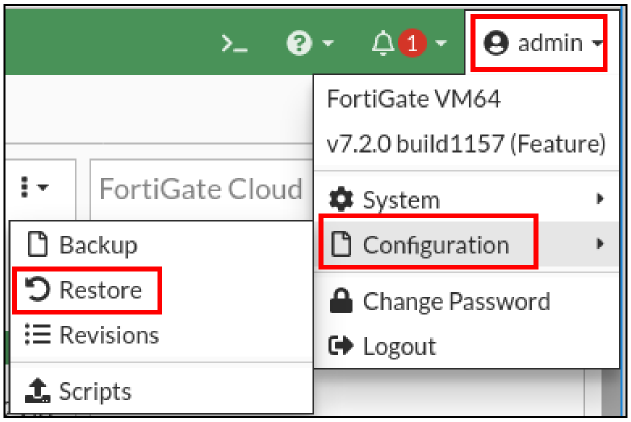
Estimated: 30 minutes

Prerequisites

Before you begin this lab, you must restore the initial configuration files to the FortiGate devices. The configuration files are located on the desktop of the Linux-Client VM.

To restore the FortiGate-1 configuration file

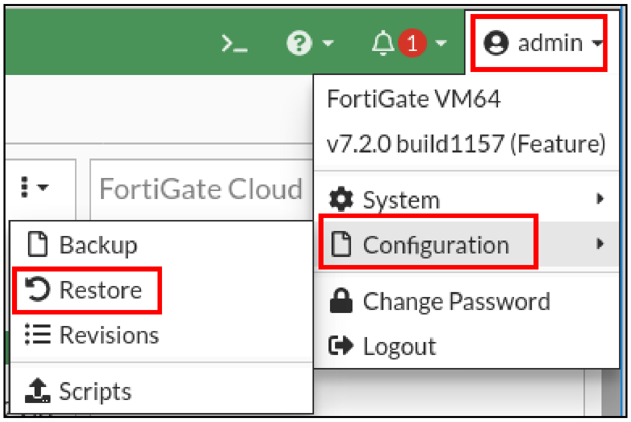
1. On the Linux-Client VM, open a browser, and then log in to the FortiGate-1 GUI at `10.1.1.1` with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **Segmentation**, select `FortiGate-1_segmentation.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

To restore the FortiGate-2 configuration file

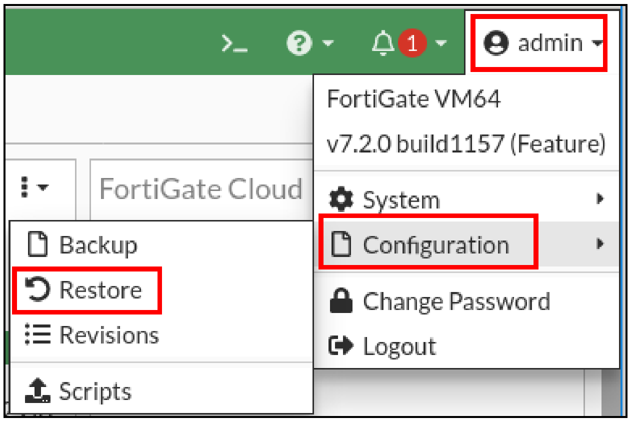
1. On the Linux-Client VM, open a browser, and then log in to the FortiGate-2 GUI at `10.1.2.1` with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **Segmentation**, select `FortiGate-2_segmentation.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

To restore the Edge-FortiGate configuration file

1. On the Linux-Client VM, open a browser, and then log in to the Edge-FortiGate GUI at `10.1.5.254` with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **Segmentation**, select `Edge-FortiGate_segmentation.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

Exercise 1: Configuring Microsegmentation

In this exercise, you will configure software switches on FortiGate-1 and FortiGate-2. You will use the software switches to control traffic between devices that belong to the same broadcast domain. You will use firewall policies to allow traffic based on the requirements.

Configure a Software Switch on FortiGate-1

You will configure a software switch on FortiGate-1. You will add port3 and port4 as members of the switch.

To configure a software switch on FortiGate-1

1. Connect over SSH to FortiGate-1.
2. Log in with the username `admin` and password `password`.
3. Enter the following commands to create a software switch:

```
config system switch-interface
     edit Floor_1_Switch
          set vdom root
          set member port3 port4
          set intra-switch-policy explicit
          next
     end
```

4. Enter the following commands to configure the switch interface:

```
config system interface
     edit Floor_1_Switch
          set ip 192.168.1.254 255.255.255.0
          set allowaccess ping
          next
     end
```

5. Log in to the FortiGate-1 GUI with the username `admin` and password `password`.
6. Click **Policy & Objects** > **Firewall Policy**.
7. Click **Create New**, and then configure the following settings to allow Linux-Client access to PLC-1 and PLC-2:

Field	Value
Name	Linux_Client_To_PLC_Access
Incoming Interface	port1
Outgoing Interface	Floor_1_Switch
Source	Linux-Client
Destination	all
Service	ALL
NAT	disable

8. Click **OK**.

Manage Traffic Between PLC-1 and PLC-2

You configured a software switch and now PLC-1 and PLC-2 belong to the same broadcast domain. Now, you will test the connectivity between PLC-1 and PLC-2.

To test the connection

1. Connect to the Linux-Client VM.
2. On the Linux-Client VM, open PuTTY.
3. Click **PLC-1** to select the saved session, and then click **Open**.
4. Log in with the username `sysadmin` and password `Fortinet1!`.
5. Enter the following command to start a ping:

   `ping 192.168.1.2` (after a few seconds, press `Ctrl`+`C` to stop the ping)
6. Minimize the PuTTY window for PLC-1.
7. On the Linux-Client VM, open PuTTY, and then open the **PLC-2** saved session.
8. Log in with the username `sysadmin` and password `Fortinet1!`.
9. Enter the following command to start a ping:

   `ping 192.168.1.1` (after a few seconds, press `Ctrl`+`C` to stop the ping)

You will notice that even if PLC-1 and PLC-2 are in the same broadcast domain, they cannot ping each other.

To allow access from PLC-1 to PLC-2

1. Log in to the FortiGate-1 GUI with the username `admin` and password `password`.
2. Click **Policy & Objects** > **Firewall Policy**.
3. Click **Create New**, and then configure the following settings to allow access from PLC-1 to PLC-2:

Field	Value
Name	PLC-1_To_PLC-2
Incoming Interface	port3
Outgoing Interface	port4
Source	all
Destination	all
Service	ALL
NAT	disable

4. Click **OK**.

To test the connection

1. Connect to the Linux-Client VM.
2. On the Linux-Client VM, open PuTTY.
3. Click **PLC-1** to select the saved session, and then click **Open**.
4. Log in with the username `sysadmin` and password `Fortinet1!`.
5. Enter the following command to generate a ping:

   `ping 192.168.1.2` (after a few seconds, press `Ctrl`+`C` to stop the ping)
6. Minimize the PuTTY window for PLC-1.
7. On the Linux-VM, open PuTTY, and then open the **PLC-2** saved session.
8. Log in with the username `sysadmin` and password `Fortinet1!`.
9. Enter the following command to generate a ping:

   `ping 192.168.1.1` (after a few seconds, press `Ctrl`+`C` to stop the ping)

Because you only have a policy that allows traffic from PLC-1 to PLC-2, the communication is active from PLC-1 to PLC-2 only, but not the other way around.

Configure a Software Switch on FortiGate-2

You will configure a software switch on FortiGate-2. You will add port3 and port4 as members of the switch.

To configure a software switch on FortiGate-2

1. Connect over SSH to FortiGate-2.
2. Log in with the username `admin` and password `password`.
3. Enter the following commands to create a software switch:

```
config system switch-interface
     edit Floor_2_Switch
          set vdom root
          set member port3 port4
          set intra-switch-policy explicit
          next
     end
```

4. Enter the following commands to configure the switch interface:

```
config system interface
     edit Floor_2_Switch
          set ip 192.168.2.254 255.255.255.0
          set allowaccess ping
          next
     end
```

5. Log in to the FortiGate-2 GUI with the username `admin` and password `password`.
6. Click **Policy & Objects** > **Firewall Policy**.

7. Click **Create New**, and then configure the following settings to allow Linux-Client access to PLC-3 and the Client VM:

Field	Value
Name	Linux_Client_Access
Incoming Interface	port1
Outgoing Interface	Floor_2_Switch
Source	Linux-Client
Destination	all
Service	ALL
NAT	disable

8. Click **OK**.

Exercise 2: Configuring Internal Segmentation

In this exercise, you will manage the traffic from one floor to another using firewall policies on Edge-FortiGate. Floor-1 and Floor-2 are already segmented using two different subnets and two different interfaces. Any communication between the floors must be allowed by a supervisor on Edge-FortiGate.

Configure Firewall Policies to Allow Traffic Between Floors

You will configure firewall policies to allow traffic from the Client VM to PLC-2. You will also allow traffic from PLC-1 to PLC-3. You will restrict the allowed traffic as much as possible to allow only essential traffic, to avoid security risks.

To allow traffic from the Client VM to PLC-2

1. Log in to the FortiGate-2 GUI with the username `admin` and password `password`.
2. Click **Policy & Objects** > **Firewall Policy**.
3. Click **Create New**, and then configure the following settings to allow the Client VM access to PLC-2:

Field	Value
Name	Client_To_PLC-2
Incoming Interface	Floor_2_Switch
Outgoing Interface	port1
Source	Client
Destination	PLC-2
Service	ALL
NAT	disable

4. Click **OK**.
5. Log in to the Edge-FortiGate GUI with the username `admin` and password `password`.
6. Click **Policy & Objects** > **Firewall Policy**.
7. Click **Create New**, and then configure the following settings to allow the Client VM access to PLC-2:

Field	Value
Name	Client_To_PLC-2
Incoming Interface	port2
Outgoing Interface	port1

Field	Value
Source	Client
Destination	PLC-2
Service	ALL
NAT	disable
Log Allowed Traffic	All Sessions

8. Click **OK**.
9. Log in to the FortiGate-1 GUI with the username `admin` and password `password`.
10. Click **Policy & Objects** > **Firewall Policy**.
11. Click **Create New**, and then configure the following settings to allow the Client VM access to PLC-2:

Field	Value
Name	Client_To_PLC-2
Incoming Interface	port1
Outgoing Interface	Floor_1_Switch
Source	Client
Destination	PLC-2
Service	ALL
NAT	disable

12. Click **OK**.

To test the connection

1. Connect to the Linux-Client VM.
2. On the Linux-Client VM, open PuTTY.
3. Click **CLIENT** to select the saved session, and then click **Open**.
4. Log in with the username `sysadmin` and password `Fortinet1!`.
5. Enter the following command to generate a ping:
   `ping 192.168.1.2` (after a few seconds, press `Ctrl`+`C` to stop the ping)

To allow traffic from PLC-1 to PLC-3

1. On the FortiGate-1 GUI, click **Policy & Objects** > **Firewall Policy**.
2. Click **Create New**, and then configure the following settings to allow PLC-1 access to PLC-3:

Field	Value
Name	PLC-1_To_PLC-3
Incoming Interface	Floor_1_Switch
Outgoing Interface	port1
Source	PLC-1
Destination	PLC-3
Service	ALL
NAT	disable

3. Click **OK.**
4. On the Edge-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
5. Click **Create New**, and then configure the following settings to allow PLC-1 access to PLC-3:

Field	Value
Name	PLC-1_To_PLC-3
Incoming Interface	port1
Outgoing Interface	port2
Source	PLC-1
Destination	PLC-3
Service	ALL
NAT	disable
Log Allowed Traffic	All Sessions

6. Click **OK.**
7. On the FortiGate-2 GUI, click **Policy & Objects** > **Firewall Policy**.
8. Click **Create New**, and then configure the following settings to allow PLC-1 access to PLC-3:

Field	Value
Name	PLC-1_To_PLC-3
Incoming Interface	port1
Outgoing Interface	Floor_2_Switch
Source	PLC-1
Destination	PLC-3

Field	Value
Service	ALL
NAT	disable

9. Click **OK**.

To test the connection

1. Connect to the Linux-Client VM.
2. On the Linux-Client VM, open PuTTY.
3. Click **PLC-1** to select the saved session, and then click **Open**.
4. Log in with the username `sysadmin` and password `Fortinet1!`.
5. Enter the following command to generate a ping:
   `ping 192.168.2.1` (after a few seconds, press `Ctrl`+`C` to stop the ping)

Lab 5: Protection

In this lab, you will configure Edge-FortiGate to monitor industrial protocol signatures using application filters. You will also create an application filter to allow specific signatures to pass through.

Objectives

- Configure an application filter to monitor industrial signatures
- Generate industrial signatures on PLCs and Client VMs
- Monitor logs for industrial traffic signatures
- Use application control to allow only specific signatures

Time to Complete

Estimated: 45 minutes

Prerequisites

You must complete the previous lab before you start this one. If you haven't done so, tell your instructor.

Exercise 1: Configuring Industrial Signatures

In this exercise, you will perform basic industrial control system (ICS) honeypot communication by simulating common industrial control protocols. You will generate Modbus TCP with Conpot from the Client VM to PLC-2. You will log the traffic on Edge-FortiGate, and then review the logs.

Generate Modbus Traffic

You will configure application control on Edge-FortiGate. You will also generate Modbus TCP traffic from the Client VM to PLC-2.

To configure application control

1. Connect over SSH to Edge-FortiGate.
2. Log in with the username `admin` and password `password`.
3. Enter the following commands to include industrial signatures:

```
config ips global
      set exclude-signature none
end
```

4. Log in to the Edge-FortiGate GUI with the username `admin` and password `password`.
5. Click **Policy & Objects** > **Firewall Policy**.
6. Select the **Client_To_PLC-2** policy, and then click **Edit**.
7. Enable **Application Control**, and then select the **default** profile.
8. Click **OK**.

To generate Modbus traffic

1. Connect to the Linux-Client VM.
2. On the Linux-Client VM, open PuTTY.
3. Click **PLC-2** to select the saved session, and then click **Open**.
4. Log in with the username `sysadmin` and password `Fortinet1!`.
5. Enter the following command:

```
./Uploads/start-conpot.sh
```

6. Leave the PuTTY session open.
7. On the Linux-Client VM, open a new PuTTY window.
8. Click **CLIENT** to select the saved session, and then click **Open**.
9. Log in with the username `sysadmin` and password `Fortinet1!`.
10. Enter the following command:

```
./Uploads/synchronous_client_ext.py
```

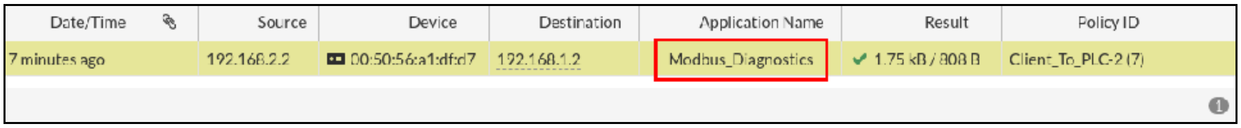
11. Leave the PuTTY session open.

Review Logs

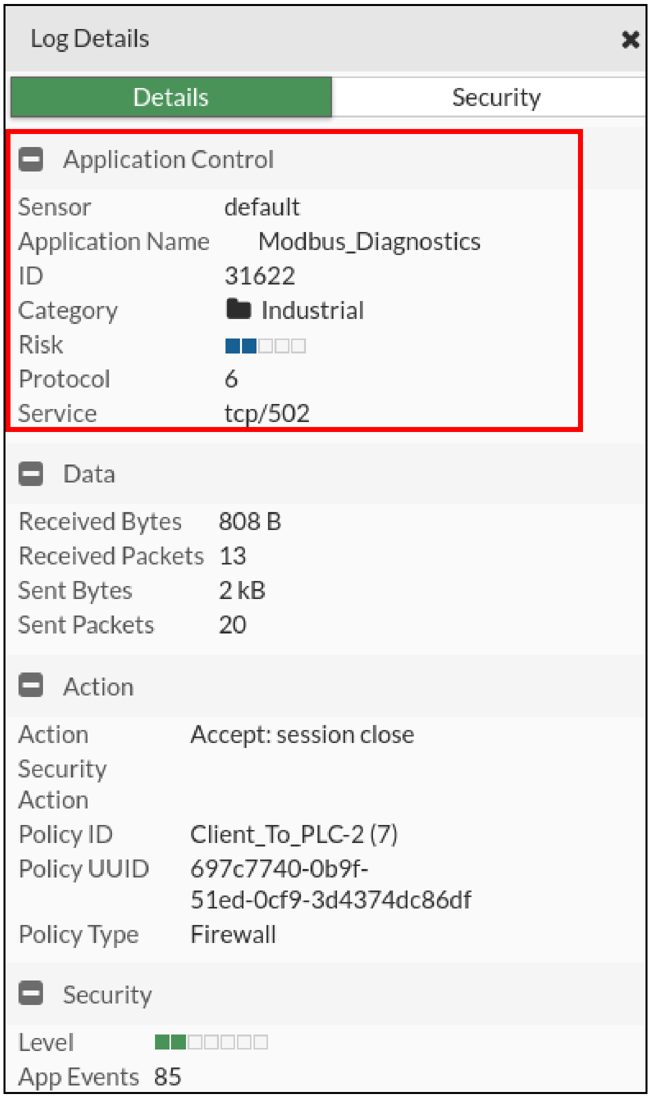
You will review logs being captured by Edge-FortiGate for the Modbus traffic that you generated.

To review logs

1. Log in to the Edge-FortiGate GUI with the username `admin` and password `password`.
2. Click **Log & Report** > **Forward Traffic**.
3. Review the log with the **Modbus_Diagnostics** signature.



Date/Time	Source	Device	Destination	Application Name	Result	Policy ID
7 minutes ago	192.168.2.2	00:50:56:a1:df:d7	192.168.1.2	Modbus_Diagnostics	✓ 1.75 kB / 808 B	Client_To_PLC-2 (7)



Log Details

Details | Security

Application Control

Sensor	default
Application Name	Modbus_Diagnostics
ID	31622
Category	Industrial
Risk	■■□□□
Protocol	6
Service	tcp/502

Data

Received Bytes	808 B
Received Packets	13
Sent Bytes	2 kB
Sent Packets	20

Action

Action	Accept: session close
Security Action	
Policy ID	Client_To_PLC-2 (7)
Policy UUID	697c7740-0b9f-51ed-0cf9-3d4374dc86df
Policy Type	Firewall

Security

Level	■■□□□□□
App Events	85

Generate IEC 104 Communication Traffic

You will start IEC 104 communication from PLC-1 to PLC-3, and then monitor the traffic.

To configure application control

1. Log in to the Edge-FortiGate GUI with the username `admin` and password `password`.
2. Click **Policy & Objects** > **Firewall Policy**.
3. Select the **PLC-1_To_PLC-3** policy, and then click **Edit**.
4. Enable **Application Control**, and then select the **default** profile.
5. Click **OK**.

To generate IEC 104 traffic

1. Connect to the Linux-Client VM.
2. On the Linux-Client VM, open PuTTY.
3. Click **PLC-3** to select the saved session, and then click **Open**.
4. Log in with the username `sysadmin` and password `Fortinet1!`.
5. Enter the following command:

   ```
   cd Uploads/iecsim/
   python3 demo_server.py 1000 2000
   ```
6. Leave the PuTTY session open.
7. On the Linux-Client VM, open a new PuTTY window.
8. Click **PLC-1** to select the saved session, and then click **Open**.
9. Log in with the username `sysadmin` and password `Fortinet1!`.
10. Enter the following command:

    ```
    cd Uploads/iecsim/
    python3 demo_client.py 192.168.2.1 1000 1010
    ```
11. Leave the PuTTY session open.

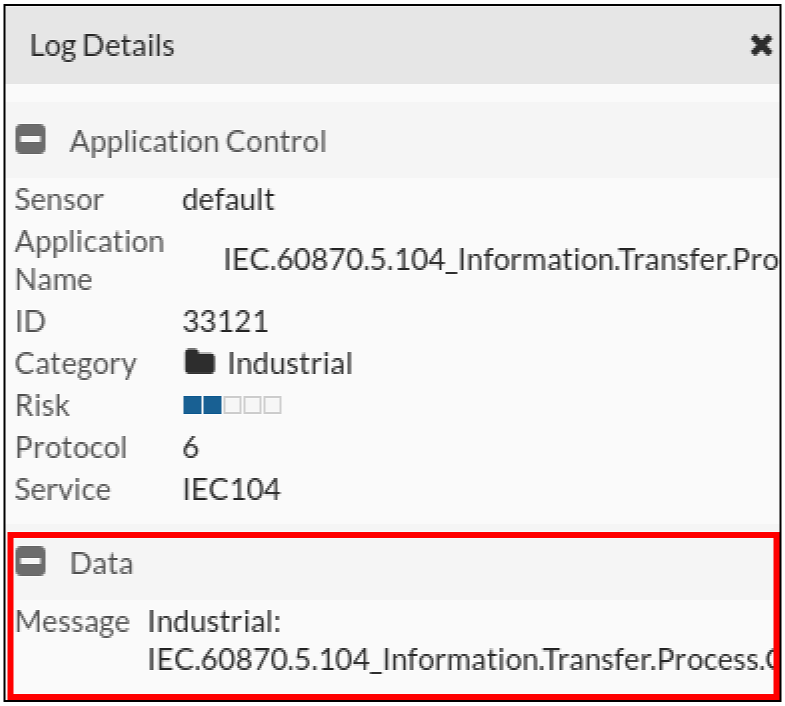
After you run the Python command, notice the data model on PLC-3. You also simulated a similar data model on PLC-1.

Review Logs

You will review the logs being captured by Edge-FortiGate for the IEC 104 traffic that you generated.

To review logs

1. Log in to the Edge-FortiGate GUI with the username `admin` and password `password`.
2. Click **Log & Report** > **Security Events**.
3. Review the security widgets, and then click the **Application Control** widget.
4. Review the logs for IEC traffic.



Log Details

Application Control

Sensor	default
Application Name	IEC.60870.5.104_Information.Transfer.Pro
ID	33121
Category	Industrial
Risk	■■□□□
Protocol	6
Service	IEC104

Data

Message	Industrial: IEC.60870.5.104_Information.Transfer.Process.(

Press `Ctrl+C` to stop the scripts on the PLC-1, PLC-2, and PLC-3 PuTTY sessions before beginning the next exercise.

Exercise 2: Configuring an Application Filter Sensor

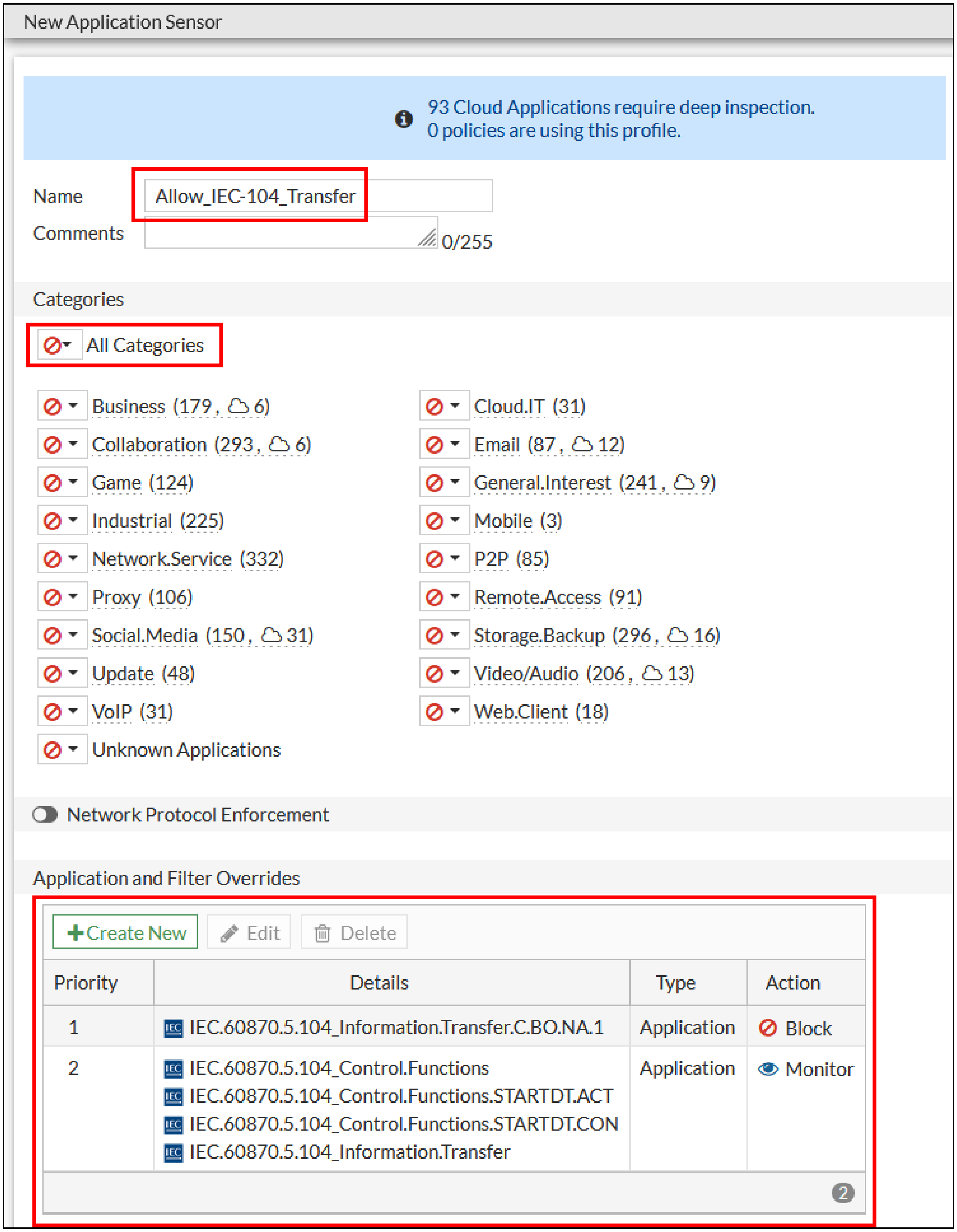
In this exercise, you will create an application sensor to allow only specific traffic and block all other traffic from PLC-1 to PLC-3.

Create an Application Sensor

You will create an application sensor using signatures to allow IEC 104 transfer only. You will also block the signature for the C_BO_NA_1 command.

To create an application sensor

1. Log in to the Edge-FortiGate GUI with the username `admin` and password `password`.
2. Click **Security Profiles** > **Application Control** > **Create New**.
3. In the **Name** field, type `Allow_IEC-104_Transfer`.
4. Under **Categories**, select **Block** for **All Categories**.
5. In the **Application and Filter Overrides** section, click **Create New**.
6. In the search field, type `IEC.60870.5.104` to list all matching signatures.
7. Right-click the **IEC.60870.5.104_Information.Transfer.C.BO.NA.1** signature to select it.
8. Click **Add selected**, and then click **OK** to save the filter.
9. Under **Application and Filter Overrides**, click **Create New** again.
10. Change the **Action** field to **Monitor**.
11. In the search field, type `IEC.60870.5.104` to list all matching signatures.
12. Press `Ctrl`, and then select the following signatures:
    ```
    IEC.60870.5.104_Control.Functions
    IEC.60870.5.104_Control.Functions.STARTDT.ACT
    IEC.60870.5.104_Control.Functions.STARTDT.CON
    IEC.60870.5.104_Information.Transfer
    ```
13. Right-click each of the selected signatures, and then click **Add selected**.
14. Click **OK** to save the filter.



New Application Sensor

93 Cloud Applications require deep inspection.
0 policies are using this profile.

Name: Allow_IEC-104_Transfer

Comments: 0/255

Categories

⊘ All Categories

⊘ Business (179, ☁ 6)	⊘ Cloud.IT (31)
⊘ Collaboration (293, ☁ 6)	⊘ Email (87, ☁ 12)
⊘ Game (124)	⊘ General.Interest (241, ☁ 9)
⊘ Industrial (225)	⊘ Mobile (3)
⊘ Network.Service (332)	⊘ P2P (85)
⊘ Proxy (106)	⊘ Remote.Access (91)
⊘ Social.Media (150, ☁ 31)	⊘ Storage.Backup (296, ☁ 16)
⊘ Update (48)	⊘ Video/Audio (206, ☁ 13)
⊘ VoIP (31)	⊘ Web.Client (18)
⊘ Unknown Applications	

○ Network Protocol Enforcement

Application and Filter Overrides

Priority	Details	Type	Action
1	IEC.60870.5.104_Information.Transfer.C.BO.NA.1	Application	⊘ Block
2	IEC.60870.5.104_Control.Functions IEC.60870.5.104_Control.Functions.STARTDT.ACT IEC.60870.5.104_Control.Functions.STARTDT.CON IEC.60870.5.104_Information.Transfer	Application	Monitor

15. Click **OK**.

To apply an application sensor to a policy

1. Log in to the Edge-FortiGate GUI with the username `admin` and password `password`.
2. Click **Policy & Objects** > **Firewall Policy**.
3. Select the **PLC-1_To_PLC-3** policy, and then click **Edit**.
4. Enable **Application Control**, and then select the **Allow_IEC-104_Transfer** profile.
5. Click **OK**.

Generate and Monitor Traffic

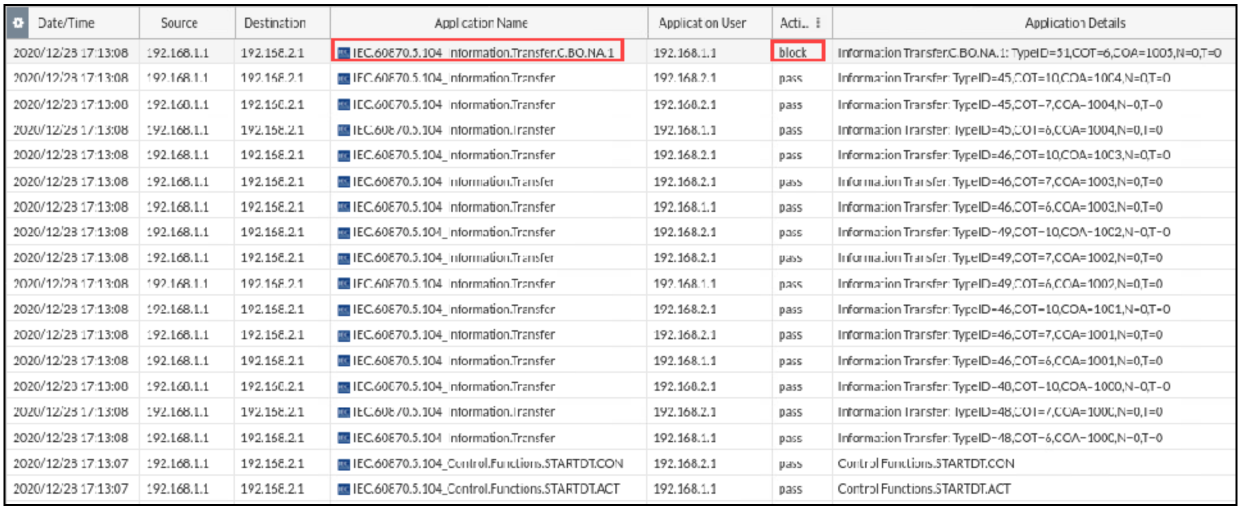
You will generate IEC 104 communication, and then review the logs.

To generate traffic

1. Connect to the Linux-Client VM.
2. On the Linux-Client VM, open PuTTY.
3. Click **PLC-3** to select the saved session, and then click **Open**.
4. Log in with the username `sysadmin` and password `Fortinet1!`.
5. Enter the following command:
   ```
   cd Uploads/iecsim/
   python3 demo_server.py 1000 2000
   ```
6. Leave the PuTTY session open.
7. Connect to the Linux-Client VM.
8. On the Linux-Client VM, open PuTTY.
9. Click **PLC-1** to select the saved session, and then click **Open**.
10. Log in with the username `sysadmin` and password `Fortinet1!`.
11. Enter the following command:
    ```
    cd Uploads/iecsim/
    python3 demo_client.py 192.168.2.1 1000 1010
    ```
12. Leave the PuTTY session open.

To review logs

1. Log in to the Edge-FortiGate GUI with the username `admin` and password `password`.
2. Click **Log & Report** > **Security Events**, then click the **Application Control** widget.
3. Review the logs for IEC traffic.



Date/Time	Source	Destination	Application Name	Application User	Acti..	Application Details
2020/12/23 17:13:08	192.168.1.1	192.168.2.1	IEC.60870.5.104_Information.Transfer.C.BO.NA.1	192.168.1.1	block	Information Transfer.C.BO.NA.1: TypeID=51,COT=6,COA=1005,N=0,T=0
2020/12/23 17:13:08	192.168.1.1	192.168.2.1	IEC.60870.5.104_Information.Transfer	192.168.2.1	pass	Information Transfer: TypeID=45,COT=10,COA=1004,N=0,T=0
2020/12/23 17:13:08	192.168.1.1	192.168.2.1	IEC.60870.5.104_Information.Transfer	192.168.2.1	pass	Information Transfer: TypeID=45,COT=7,COA=1004,N=0,T=0
2020/12/23 17:13:08	192.168.1.1	192.168.2.1	IEC.60870.5.104_Information.Transfer	192.168.1.1	pass	Information Transfer: TypeID=45,COT=6,COA=1004,N=0,T=0
2020/12/23 17:13:08	192.168.1.1	192.168.2.1	IEC.60870.5.104_Information.Transfer	192.168.2.1	pass	Information Transfer: TypeID=46,COT=10,COA=1003,N=0,T=0
2020/12/23 17:13:08	192.168.1.1	192.168.2.1	IEC.60870.5.104_Information.Transfer	192.168.2.1	pass	Information Transfer: TypeID=46,COT=7,COA=1003,N=0,T=0
2020/12/23 17:13:08	192.168.1.1	192.168.2.1	IEC.60870.5.104_Information.Transfer	192.168.1.1	pass	Information Transfer: TypeID=46,COT=6,COA=1003,N=0,T=0
2020/12/23 17:13:08	192.168.1.1	192.168.2.1	IEC.60870.5.104_Information.Transfer	192.168.2.1	pass	Information Transfer: TypeID=49,COT=10,COA=1002,N=0,T=0
2020/12/23 17:13:08	192.168.1.1	192.168.2.1	IEC.60870.5.104_Information.Transfer	192.168.2.1	pass	Information Transfer: TypeID=49,COT=7,COA=1002,N=0,T=0
2020/12/23 17:13:08	192.168.1.1	192.168.2.1	IEC.60870.5.104_Information.Transfer	192.168.1.1	pass	Information Transfer: TypeID=49,COT=6,COA=1002,N=0,T=0
2020/12/23 17:13:08	192.168.1.1	192.168.2.1	IEC.60870.5.104_Information.Transfer	192.168.2.1	pass	Information Transfer: TypeID=46,COT=10,COA=1001,N=0,T=0
2020/12/23 17:13:08	192.168.1.1	192.168.2.1	IEC.60870.5.104_Information.Transfer	192.168.2.1	pass	Information Transfer: TypeID=46,COT=7,COA=1001,N=0,T=0
2020/12/23 17:13:08	192.168.1.1	192.168.2.1	IEC.60870.5.104_Information.Transfer	192.168.1.1	pass	Information Transfer: TypeID=46,COT=6,COA=1001,N=0,T=0
2020/12/23 17:13:08	192.168.1.1	192.168.2.1	IEC.60870.5.104_Information.Transfer	192.168.2.1	pass	Information Transfer: TypeID=48,COT=10,COA=1000,N=0,T=0
2020/12/23 17:13:08	192.168.1.1	192.168.2.1	IEC.60870.5.104_Information.Transfer	192.168.2.1	pass	Information Transfer: TypeID=48,COT=7,COA=1000,N=0,T=0
2020/12/23 17:13:08	192.168.1.1	192.168.2.1	IEC.60870.5.104_Information.Transfer	192.168.1.1	pass	Information Transfer: TypeID=48,COT=6,COA=1000,N=0,T=0
2020/12/23 17:13:07	192.168.1.1	192.168.2.1	IEC.60870.5.104_Control.Functions.STARTDT.CON	192.168.2.1	pass	Control Functions.STARTDT.CON
2020/12/23 17:13:07	192.168.1.1	192.168.2.1	IEC.60870.5.104_Control.Functions.STARTDT.ACT	192.168.1.1	pass	Control Functions.STARTDT.ACT

⚠ Press `Ctrl+C` to stop the scripts on the PLC-1 and PLC-3 PuTTY sessions before beginning the next lab.

Lab 6: Logging and Monitoring Configuration

In this lab, you will configure FortiGate to send logs to FortiAnalyzer and FortiSIEM. You will configure FortiAnalyzer to accept logs from FortiGate, and configure a rule to monitor industrial protocols on FortiSIEM.

You will also configure FortiSIEM to monitor and send alerts for changes in the performance of industrial devices. After you complete these exercises, you will understand how single and multiple pattern performance rules for industrial devices work and how to create your own.

Objectives

- Configure FortiGate to send logs to both FortiAnalyzer and FortiSIEM
- Configure FortiAnalyzer to send security events to FortiSIEM
- Examine logs on FortiAnalyzer for industrial protocols and signatures
- Examine logs and alerts on FortiSIEM for industrial protocols and signatures
- Configure a performance single pattern rule on FortiSIEM to send alerts for industrial devices
- Enhance performance rules for multiple patterns to send alerts for industrial devices on FortiSIEM

Time to Complete

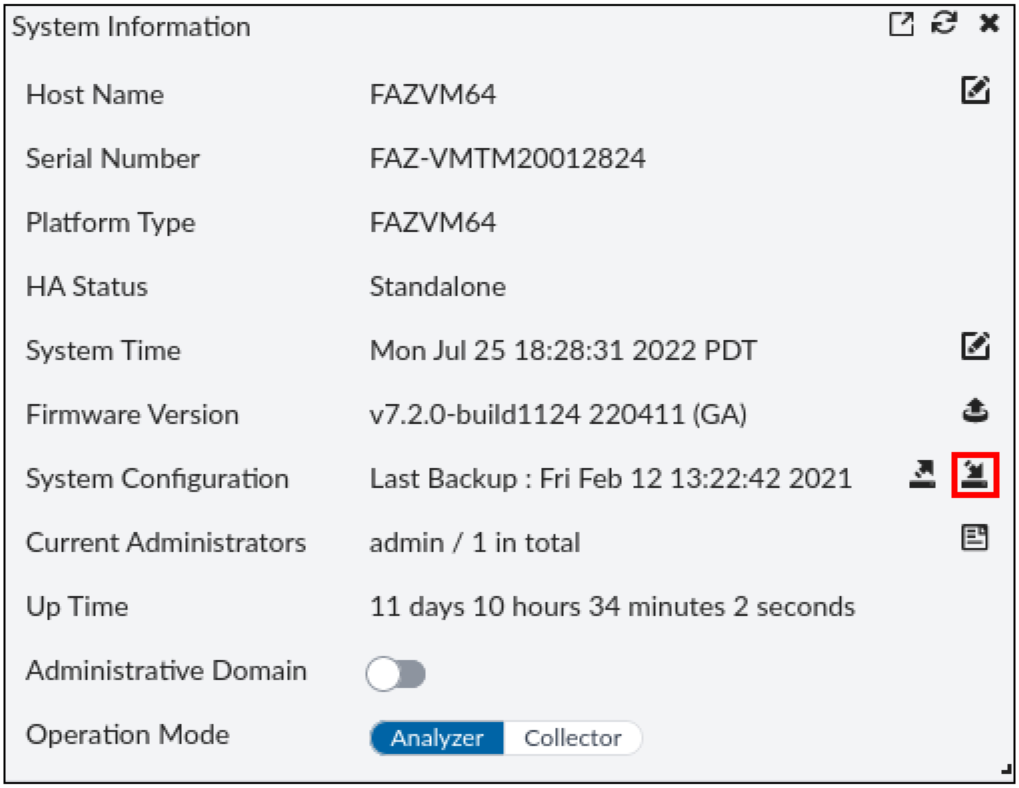
Estimated: 120 minutes

Prerequisites

Before you begin this lab, you must restore the initial configuration files to FortiAnalyzer and Edge-FortiGate. The configuration files are located in the **Resources** folder on the desktop of the Linux-Client VM.

To restore the FortiAnalyzer configuration file

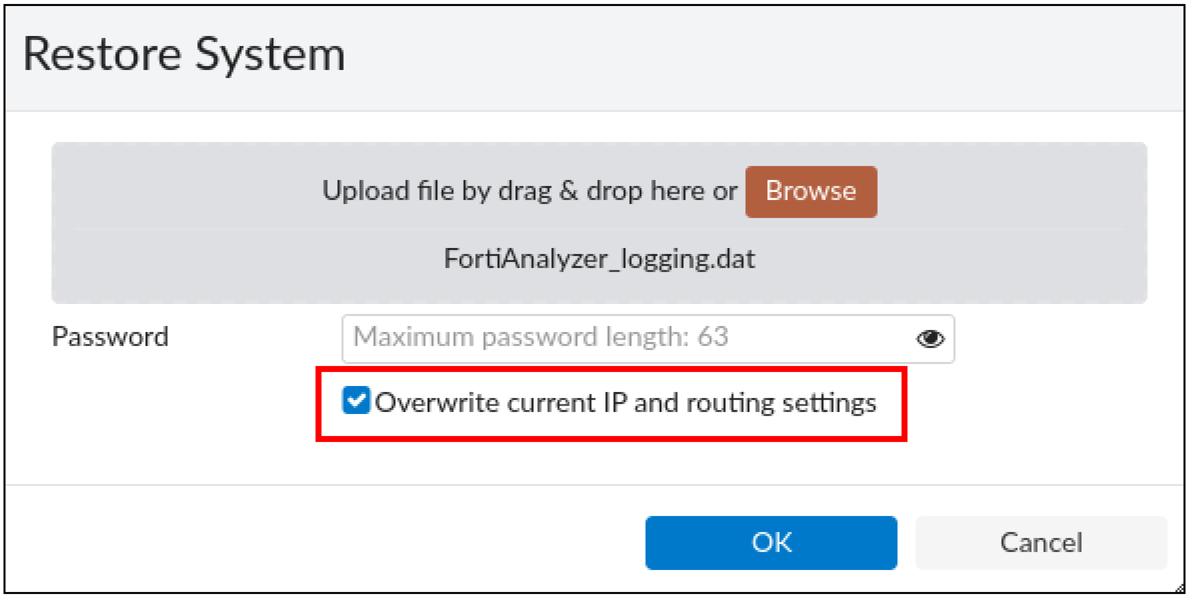
1. On the Linux-Client VM, open a browser, and then log in to the FortiAnalyzer GUI at `10.1.3.210` with the username `admin` and password `password`.
2. Click **System Settings**.
3. In the **System Information** widget, in the **System Configuration** field, click the **Restore** icon.



System Information

Host Name	FAZVM64
Serial Number	FAZ-VMTM20012824
Platform Type	FAZVM64
HA Status	Standalone
System Time	Mon Jul 25 18:28:31 2022 PDT
Firmware Version	v7.2.0-build1124 220411 (GA)
System Configuration	Last Backup : Fri Feb 12 13:22:42 2021
Current Administrators	admin / 1 in total
Up Time	11 days 10 hours 34 minutes 2 seconds
Administrative Domain	○
Operation Mode	● Analyzer ○ Collector

4. Click **Browse**.
5. Click **Desktop** > **Resources** > **Logging and Monitoring**, and then select `FortiAnalyzer_logging.dat`. You do not have to enter a password because the file is not encrypted.
6. Leave the **Overwrite current IP and routing settings** checkbox selected.



Restore System

Upload file by drag & drop here or Browse

FortiAnalyzer_logging.dat

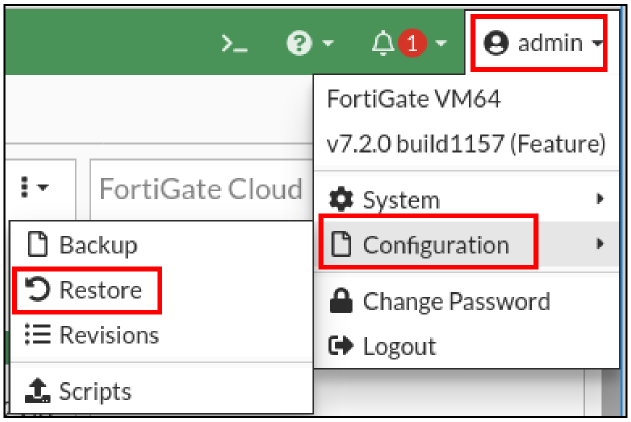
Password: Maximum password length: 63

☑ Overwrite current IP and routing settings

7. Click **OK**.

To restore the Edge-FortiGate configuration file

1. On the Linux-Client VM, open a browser, and then log in to the Edge-FortiGate GUI at `10.1.5.254` with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **Logging and Monitoring**, select `Edge-FortiGate_logging.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

Follow the directions in the lab guide and do not make changes to any other devices unless your instructor tells you to.

Exercise 1: Preparing Devices for Logs and Alerts

In this exercise, you will configure FortiGate to send logs to FortiAnalyzer and FortiSIEM. You will configure FortiAnalyzer to accept logs from FortiGate, and configure an event handler to send events to FortiSIEM. You will also configure a rule to monitor industrial protocols on FortiSIEM, by generating traffic from PLC simulations.

Configure Edge-FortiGate to Send Logs to FortiAnalyzer and FortiSIEM

You will configure FortiGate to send logs to both FortiAnalyzer and FortiSIEM.

To enable FortiAnalyzer logging on Edge-FortiGate

1. Log in to the Edge-FortiGate GUI with the username `admin` and password `password`.
2. On the Edge-FortiGate GUI, click **Security Fabric** > **Fabric Connectors**.
3. Click **FortiAnalyzer logging**, and then click **Edit**.
4. In the **FortiAnalyzer Settings** section, in the **Status** field, select **Enabled**.
5. Configure the following settings:

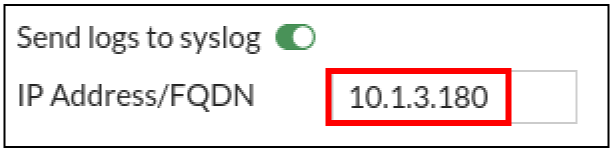
Field	Value
IP address	10.1.3.210
Upload option	Real Time

6. Click **OK**.
7. Click **Accept**.
8. Click **Close**.

A warning appears that states FortiGate isn't yet authorized on FortiAnalyzer. You will configure this authorization on FortiAnalyzer in a later step.

To enable syslog on Edge-FortiGate for FortiSIEM

1. On the Edge-FortiGate GUI, click **Log & Report** > **Log Settings**.
2. In the **Remote Logging and Archiving** section, enable **Send logs to syslog**.
3. In the **IP Address/FQDN** field, type `10.1.3.180`.



Send logs to syslog ●
IP Address/FQDN 10.1.3.180

4. Click **Apply**.
5. Click **OK** to dismiss the warning message.

6. Click **Close**.

Configure FortiAnalyzer

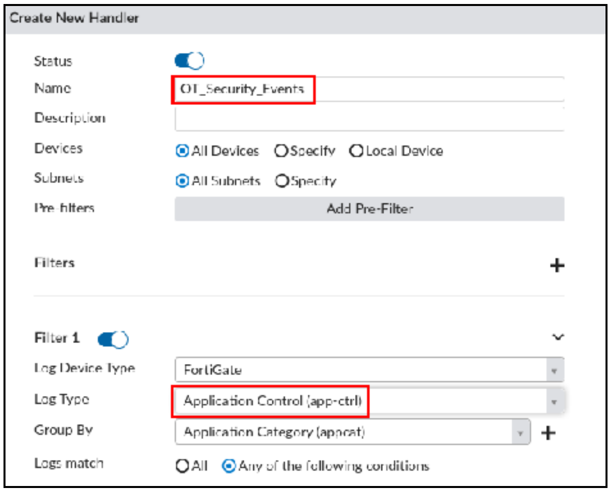
You will configure FortiAnalyzer to accept logs from FortiGate. You will also configure an event handler to send events to FortiSIEM.

To accept a device registration request

1. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. Click **Device Manager**.
3. In the **Device & Groups** section, click **Unauthorized Devices**.
4. Select the **Edge-FortiGate** checkbox, and then click **Authorize**.
5. Click **OK**, and then click **Close**.

To configure an event handler

1. Continuing on the FortiAnalyzer GUI, in the drop-down list on the left, click **FortiSOC**.
2. Click **Handlers** > **Event Handler List**.
3. Click **Create New**, and then in the **Name** field, type `OT_Security_Events`.
4. In the **Log Type** field, select **Application Control (app-ctrl)**, and then in the **Confirm Reset** window, click **OK**.



Create New Handler

Status

Name: OT_Security_Events

Description

Devices: ● All Devices ○ Specify ○ Local Device

Subnets: ● All Subnets ○ Specify

Pre-filters: Add Pre-Filter

Filters +

Filter 1

Log Device Type: FortiGate

Log Type: Application Control (app-ctrl)

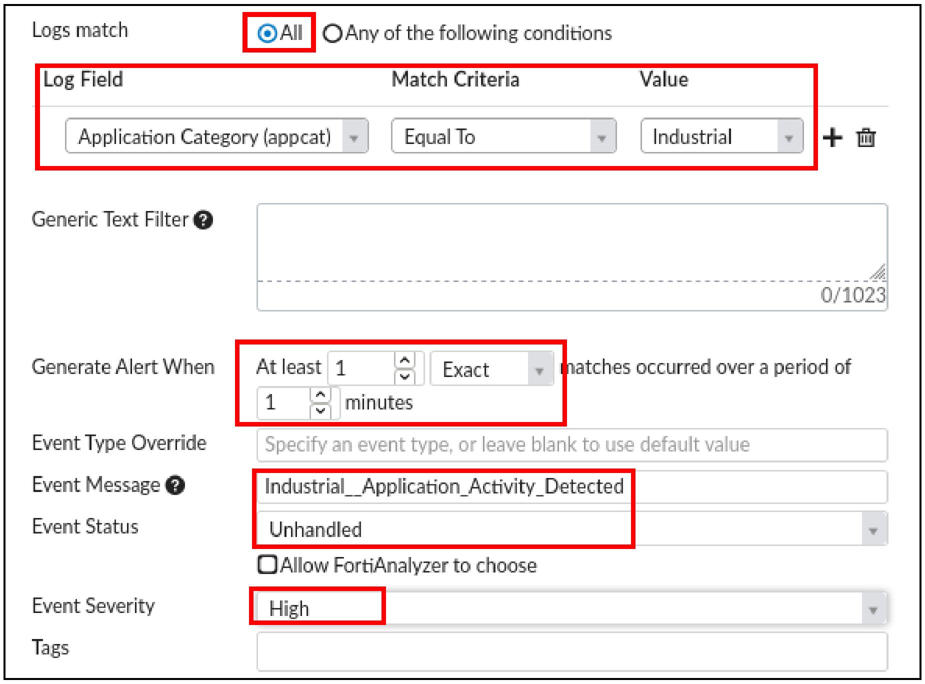
Group By: Application Category (appcat) +

Logs match: ○ All ● Any of the following conditions

5. In the **Logs match** field, select **All**, and then configure the following settings:

Field	Value
Log Field	Application Category (appcat)
Value	Industrial
Generate Alert When	1, Exact, 1
Event Message	Industrial_Application_Activity_Detected

Field	Value
Event Status	Unhandled
Event Severity	High



Logs match ● All ○ Any of the following conditions

Log Field	Match Criteria	Value
Application Category (appcat)	Equal To	Industrial

Generic Text Filter 0/1023

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

Event Type Override: Specify an event type, or leave blank to use default value

Event Message: Industrial__Application_Activity_Detected

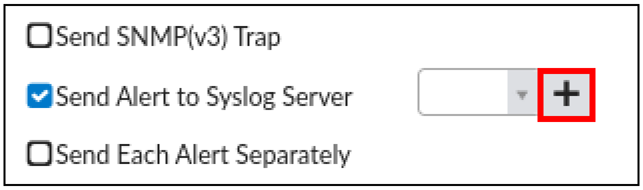
Event Status: Unhandled

□ Allow FortiAnalyzer to choose

Event Severity: High

Tags

6. In the **Notification** section, select the **Send Alert to Syslog Server** checkbox, and then click **+** to configure the syslog server settings.



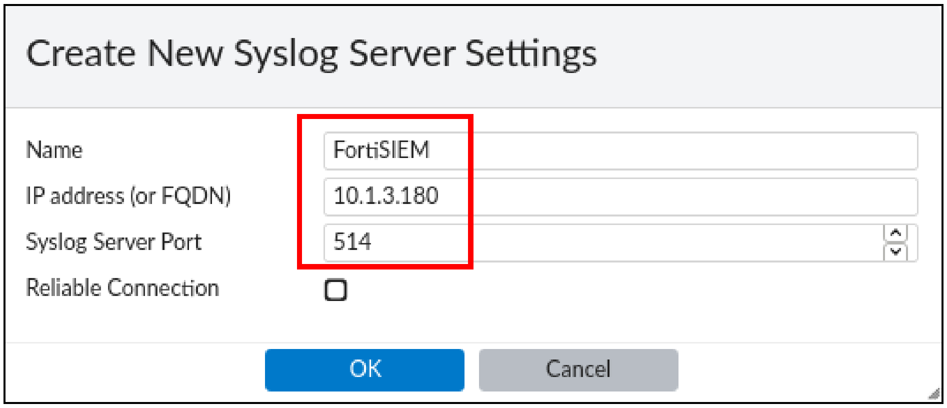
□ Send SNMP(v3) Trap

☑ Send Alert to Syslog Server +

□ Send Each Alert Separately

7. In the **Create New Syslog Server Settings** window, configure the following settings:

Field	Value
Name	FortiSIEM
IP address (or FQDN)	10.1.3.180
Syslog Server Port	514


Create New Syslog Server Settings

Name: FortiSIEM

IP address (or FQDN): 10.1.3.180

Syslog Server Port: 514

Reliable Connection: □

8. Click **OK**, and then in the drop-down list, select **FortiSIEM** as the syslog server.
9. Click **OK** to finish the event handler configuration.

Configure a Rule on FortiSIEM for Incidents

You will configure a rule on FortiSIEM to monitor industrial protocols and trigger an incident if a match is found.

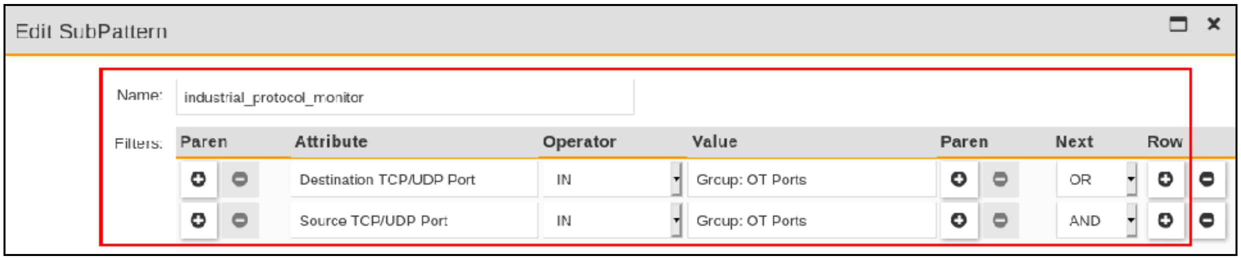
To configure a rule to monitor industrial protocols

1. Log in to the FortiSIEM GUI with the username `admin` and password `Fortinet1!`.
2. Click **Accept** to dismiss the warning message.
3. Click the **RESOURCES** tab, and then expand the **Protocols** section on the left.
4. Click **OT Ports**.

   Review the entries including **Modbus** and **IEC.60870.5.104** ports.
5. Click **Rules** > **Security** > **Operation Technology**, and then click **New**.
6. In the **Add New Rule** window, under **Step 1: General**, in the **Rule Name** field, type `Monitor Industrial Protocols`.
7. Select **Step 2: Define Condition**, and then leave the default time interval set to 300 seconds (5 minutes).
8. In the **Subpattern** field, click the pencil icon, type the name `industrial_protocol_monitor`, and then create the following **Filters**:

Field	Value
Attribute	Destination TCP/UDP Port
Operator	IN
Value	Select **CMDB** > **Protocols** > **OT Ports**, add the **OT Ports** group to **Selections**, and then click **OK**.
Next	OR
Row	+

Field	Value
Attribute	Source TCP/UDP Port
Operator	IN
Value	Select **CMDB** > **Protocols** > **OT Ports**, add the **OT Ports** group to **Selections**, and then click **OK**.



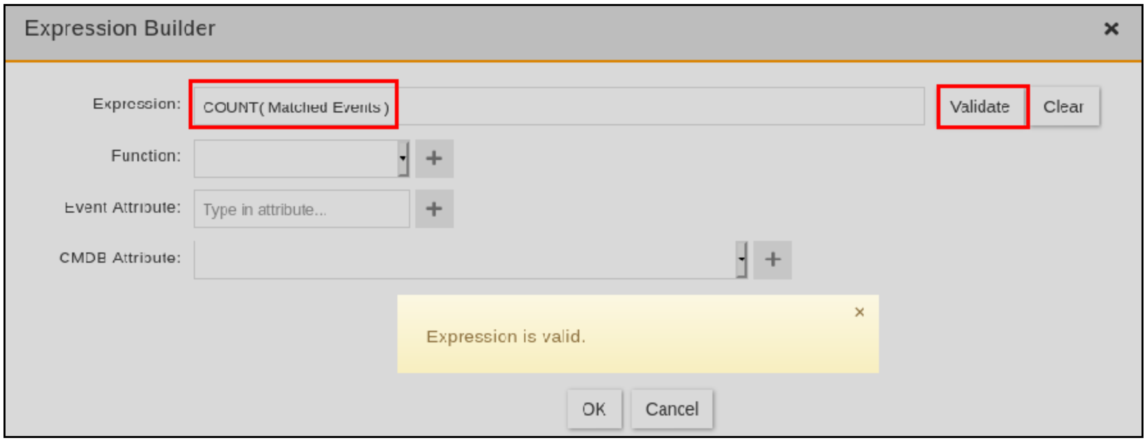
Name: industrial_protocol_monitor

Filters:

Paren	Attribute	Operator	Value	Paren	Next	Row
⊕ ⊖	Destination TCP/UDP Port	IN	Group: OT Ports	⊕ ⊖	OR	⊕ ⊖
⊕ ⊖	Source TCP/UDP Port	IN	Group: OT Ports	⊕ ⊖	AND	⊕ ⊖

9. In the **Aggregate** section, use the **Expression Builder** in the **Attribute** field.
10. In the **Function** field, select **COUNT**, and then click **+**.
11. In the **Event Attribute** field, select **Matched Events**, click **+**, and then click **Validate**.

    An **Expression is valid** message appears.



Expression: COUNT(Matched Events)

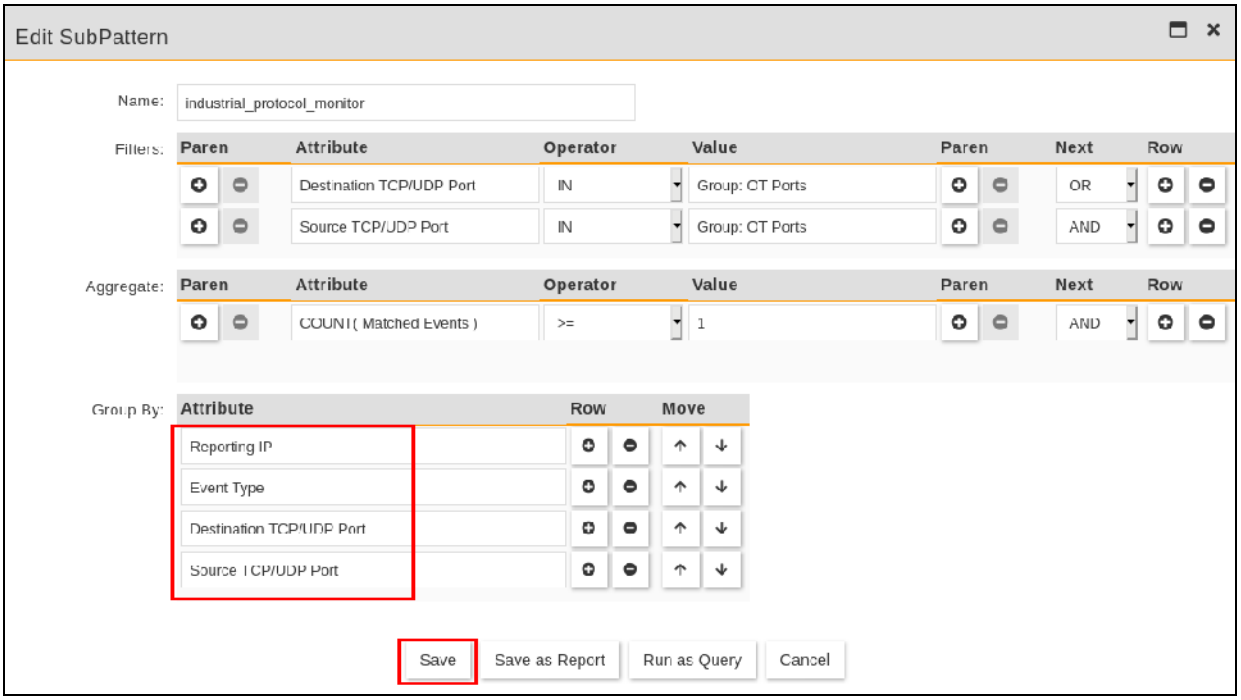
Function:

Event Attribute: Type in attribute...

CMDB Attribute:

Expression is valid.

12. Close the window, and then click **OK**.
13. In the **Operator** field, select **>=**, and then type a value of `1`.
14. In the **Group By** section, add the **Source TCP/UDP Port**, **Destination TCP/UDP Port**, **Event Type**, and **Reporting IP** attributes, and then click **Save**.



Edit SubPattern

Name: industrial_protocol_monitor

Filters:

Paren	Attribute	Operator	Value	Paren	Next	Row
⊕ ⊖	Destination TCP/UDP Port	IN	Group: OT Ports	⊕ ⊖	OR	⊕ ⊖
⊕ ⊖	Source TCP/UDP Port	IN	Group: OT Ports	⊕ ⊖	AND	⊕ ⊖

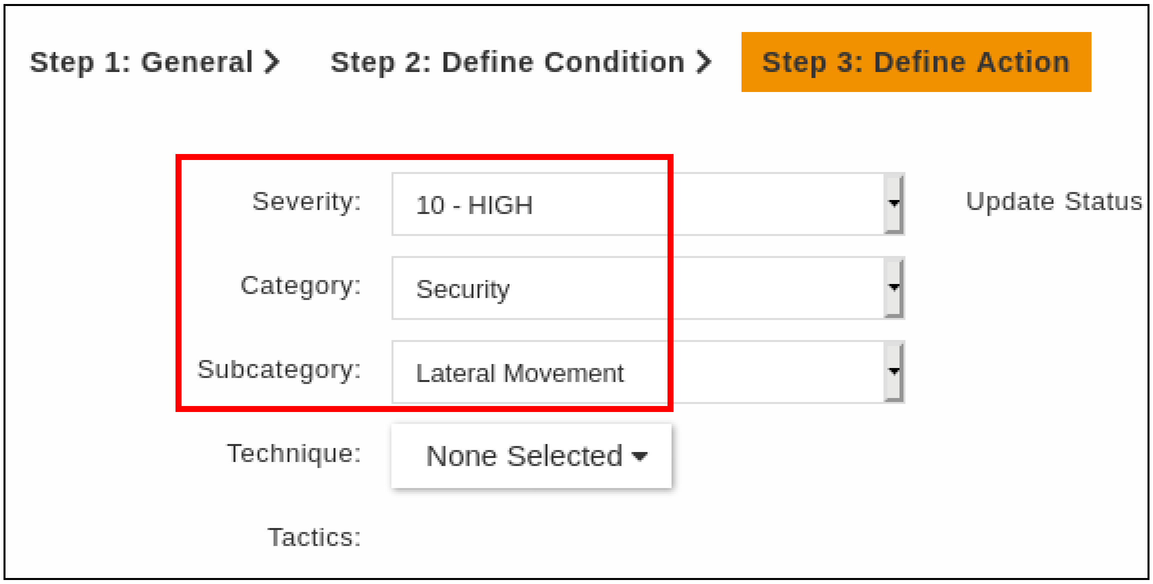
Aggregate:

Paren	Attribute	Operator	Value	Paren	Next	Row
⊕ ⊖	COUNT(Matched Events)	>=	1	⊕ ⊖	AND	⊕ ⊖

Group By:

Attribute	Row	Move
Reporting IP	⊕ ⊖	↑ ↓
Event Type	⊕ ⊖	↑ ↓
Destination TCP/UDP Port	⊕ ⊖	↑ ↓
Source TCP/UDP Port	⊕ ⊖	↑ ↓

15. Click **Step 3: Define Action**, set the **Severity** to **10 - HIGH**, the **Category** to **Security**, and the **Subcategory** to **Lateral Movement**.



Severity: 10 - HIGH

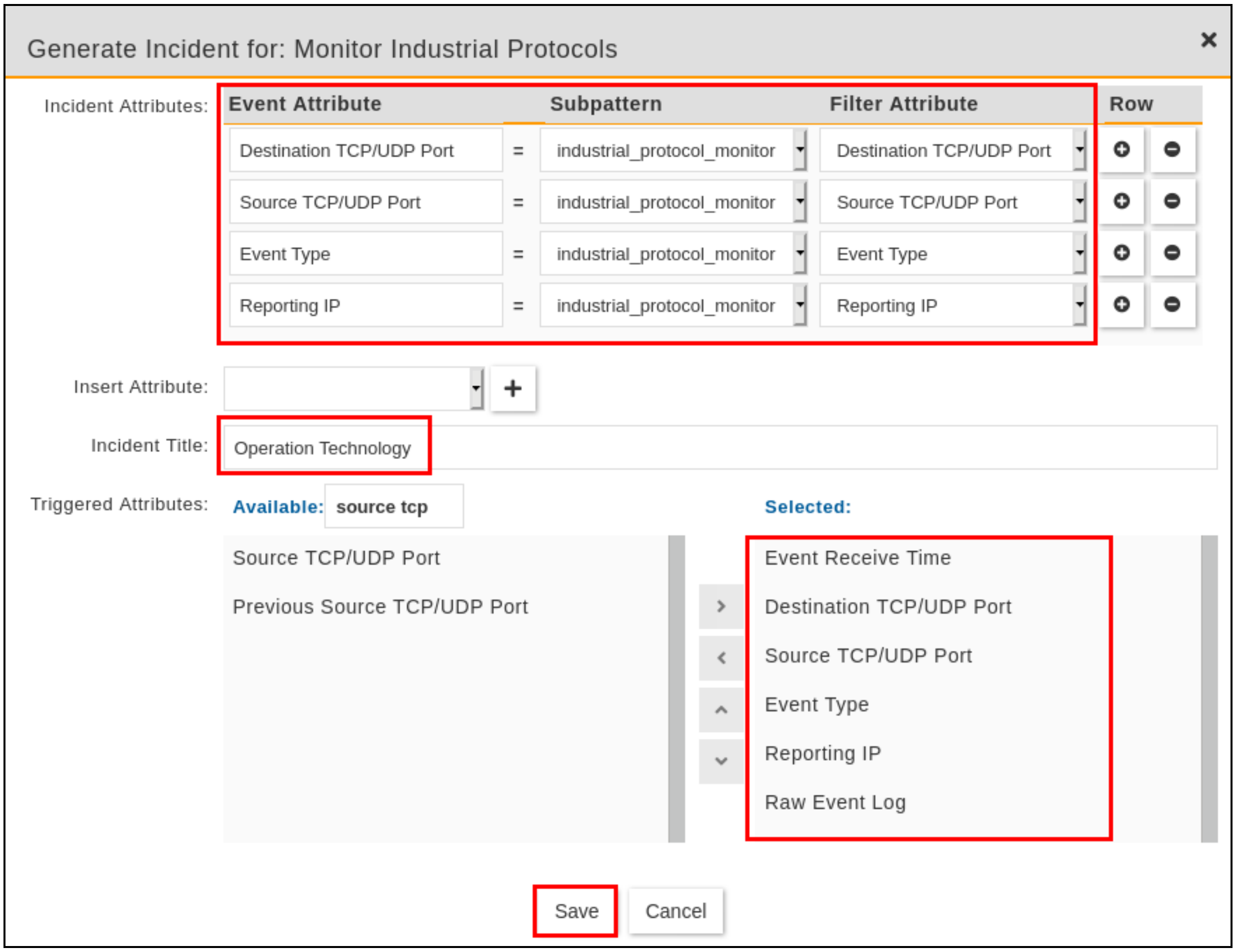
Category: Security

Subcategory: Lateral Movement

Technique: None Selected

Tactics:

16. In the **Action** section, click the pencil icon, in the **Incident Title** field, type `Operational Technology`, complete the **Incident Attributes** and **Triggered Attributes** fields as shown in the following image, and then click **Save**.



Generate Incident for: Monitor Industrial Protocols

Incident Attributes:

Event Attribute		Subpattern	Filter Attribute	Row	
Destination TCP/UDP Port	=	industrial_protocol_monitor	Destination TCP/UDP Port	⊕	⊖
Source TCP/UDP Port	=	industrial_protocol_monitor	Source TCP/UDP Port	⊕	⊖
Event Type	=	industrial_protocol_monitor	Event Type	⊕	⊖
Reporting IP	=	industrial_protocol_monitor	Reporting IP	⊕	⊖

Insert Attribute: +

Incident Title: Operation Technology

Triggered Attributes: Available: source tcp

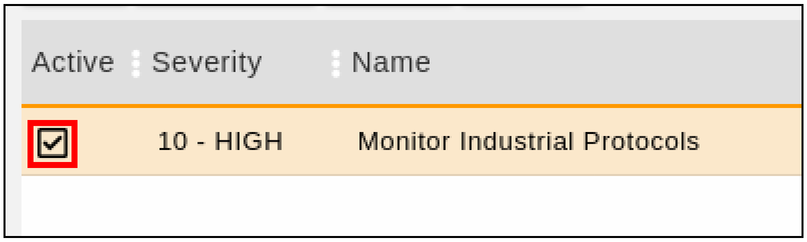
- Source TCP/UDP Port
- Previous Source TCP/UDP Port

Selected:

- Event Receive Time
- Destination TCP/UDP Port
- Source TCP/UDP Port
- Event Type
- Reporting IP
- Raw Event Log

Save Cancel

17. Click **Save** to save the rule.
18. Select the **Active** checkbox to enable the rule, and then in the **Activation** window, click **Continue**.



Active	Severity	Name
☑	10 - HIGH	Monitor Industrial Protocols

Generate Logs

You will generate Modbus and IEC 104 communication.

To generate Modbus traffic

1. Connect to the Linux-Client VM.
2. On the Linux-Client VM, open PuTTY.
3. Click **PLC-2** to select the saved session, and then click **Open**.

4. Log in with the username `sysadmin` and password `Fortinet1!`.
5. Enter the following command:

```
./Uploads/start-conpot.sh
```

6. Leave the PuTTY session open.

The output may report a failure to allocate a new port. This is because of the previous lab. It should not impact the results to continue and generate Modbus traffic.

7. On the Linux-Client VM, open a new PuTTY window.
8. Click **CLIENT** to select the saved session, and then click **Open**.
9. Log in with the username `sysadmin` and password `Fortinet1!`.
10. Enter the following command:

```
./Uploads/synchronous_client_ext.py
```

11. Leave the PuTTY session open.

To generate IEC 104 traffic

1. On the Linux-Client VM, open a new PuTTY window.
2. Click **PLC-3** to select the saved session, and then click **Open**.
3. Log in with the username `sysadmin` and password `Fortinet1!`.
4. Enter the following command:

```
cd Uploads/iecsim/
python3 demo_server.py 1000 2000
```

5. Leave the PuTTY session open.
6. On the Linux-Client VM, open a new PuTTY window.
7. Click **PLC-1** to select the saved session, and then click **Open**.
8. Log in with the username `sysadmin` and password `Fortinet1!`.
9. Enter the following command:

```
cd Uploads/iecsim/
python3 demo_client.py 192.168.2.1 1000 2000
```

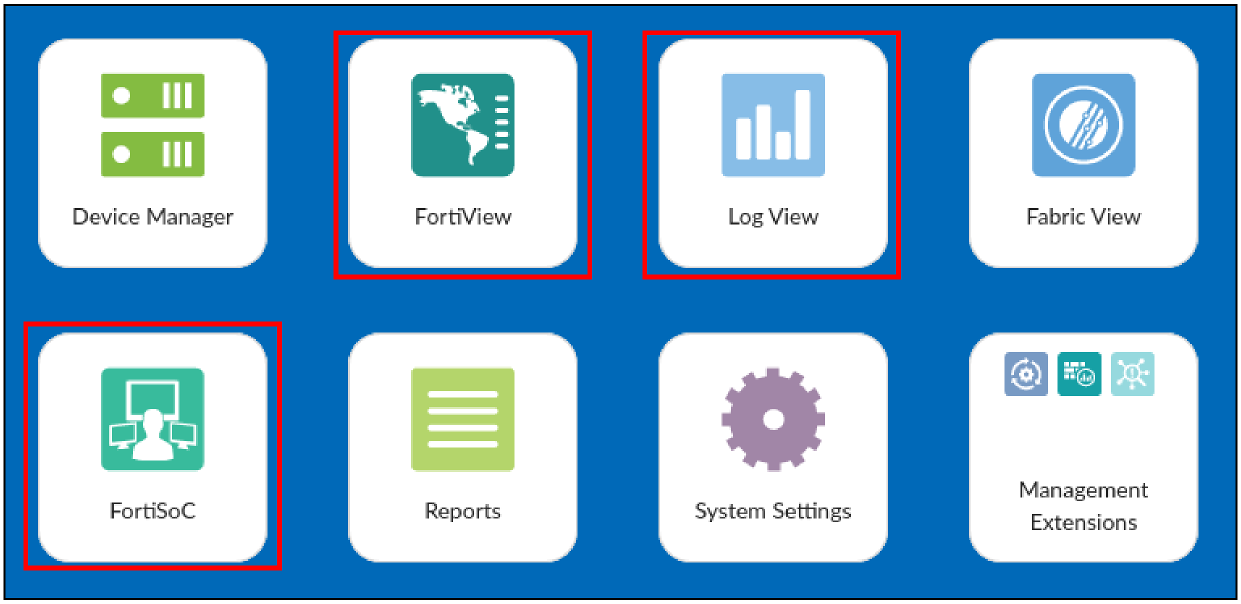
10. Leave the PuTTY session open.

Notice the data model on PLC-3 after running the Python command. You also simulated a similar data model on PLC-1.

Exercise 2: Examining Logs and Events on FortiAnalyzer

There are many ways to view logs and events on FortiAnalyzer. In this exercise, you will explore the following different views and log management features:

- **Log View**
- **FortiView**
- **FortiSOC**



Because of simulated traffic limitations in this lab, not all views will be populated.

Explore Log View

Log View allows you to view traffic logs (also referred to as firewall policy logs), event logs, and security logs for each device or for each log group, which is a feature we are not using in this lab.

When ADOMs are enabled, **Log View** displays information for each ADOM.

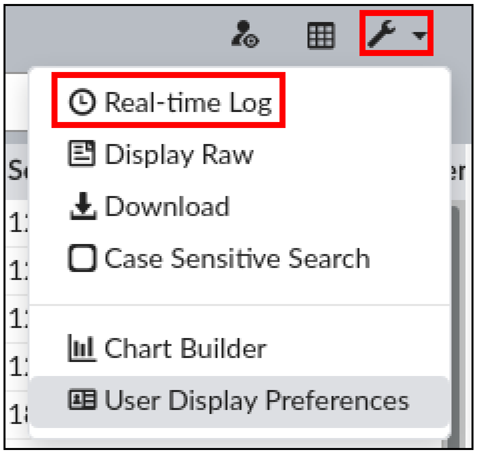
Log View displays log messages from analytics logs and archive logs.

- Historical logs and real-time logs in **Log View** are from analytics logs.
- **Log Browse** can display logs from both the current, active log file and any of the compressed log files.

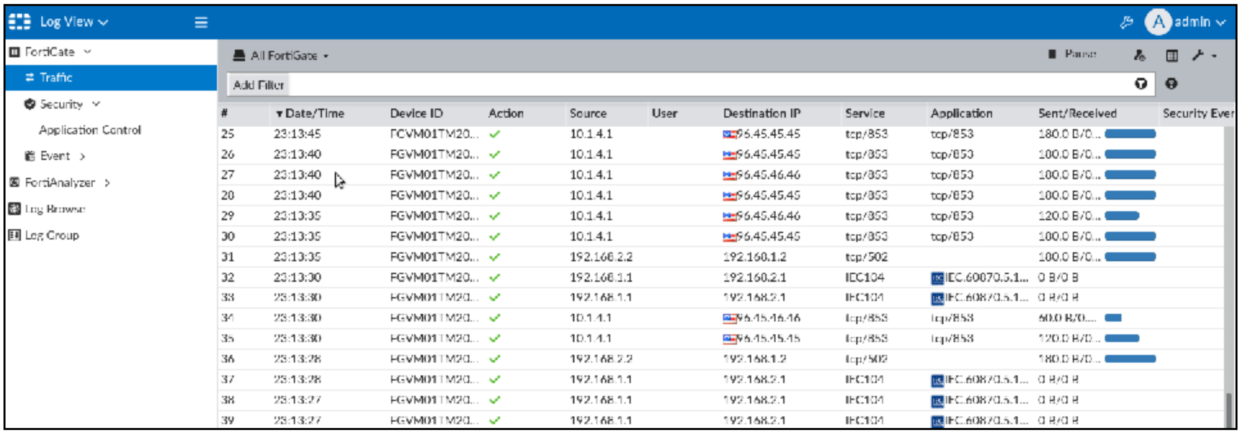
You will examine traffic logs and security logs related to industrial protocols and signatures only.

To view logs in Log View

1. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. Click **Log View**.
3. In the menu on the left, click **FortiGate** > **Traffic**.
4. Explore the different ways of viewing logs, such as real time, historical, and raw.
    - On the right side of the GUI, click **Tools** > **Real-time Log**.



You should see traffic logs in real time and in the formatted view.



#	▾Date/Time	Device ID	Action	Source	User	Destination IP	Service	Application	Sent/Received	Security Ever
25	23:13:45	FCVM01TM20...	✓	10.1.4.1		96.45.45.45	tcp/853	tcp/853	180.0 B/0...	
26	23:13:40	FGVM01TM20...	✓	10.1.4.1		96.45.45.45	tcp/853	tcp/853	100.0 B/0...	
27	23:13:40	FGVM01TM20...	✓	10.1.4.1		96.45.46.46	tcp/853	tcp/853	100.0 B/0...	
20	23:13:40	FGVM01TM20...	✓	10.1.4.1		96.45.45.45	tcp/853	tcp/853	100.0 B/0...	
29	23:13:35	FGVM01TM20...	✓	10.1.4.1		96.45.46.46	tcp/853	tcp/853	120.0 B/0...	
30	23:13:35	FGVM01TM20...	✓	10.1.4.1		96.45.45.45	tcp/853	tcp/853	100.0 B/0...	
31	23:13:35	FGVM01TM20...	✓	192.168.2.2		192.160.1.2	tcp/502		100.0 B/0...	
32	23:13:30	FGVM01TM20...	✓	192.168.1.1		192.160.2.1	IEC104	IEC.60870.5.1...	0 B/0 B	
33	23:13:30	FGVM01TM20...	✓	192.168.1.1		192.168.2.1	IEC104	IEC.60870.5.1...	0 B/0 B	
34	23:13:30	FGVM01TM20...	✓	10.1.4.1		96.45.46.46	tcp/853	tcp/853	60.0 B/0...	
35	23:13:30	FGVM01TM20...	✓	10.1.4.1		96.45.45.45	tcp/853	tcp/853	120.0 B/0...	
36	23:13:28	FGVM01TM20...	✓	192.168.2.2		192.168.1.2	tcp/502		180.0 B/0...	
37	23:13:28	FGVM01TM20...	✓	192.168.1.1		192.168.2.1	IEC104	IEC.60870.5.1...	0 B/0 B	
38	23:13:27	FGVM01TM20...	✓	192.168.1.1		192.168.2.1	IEC104	IEC.60870.5.1...	0 B/0 B	
39	23:13:27	FGVM01TM20...	✓	192.168.1.1		192.168.2.1	IEC104	IEC.60870.5.1...	0 B/0 B	

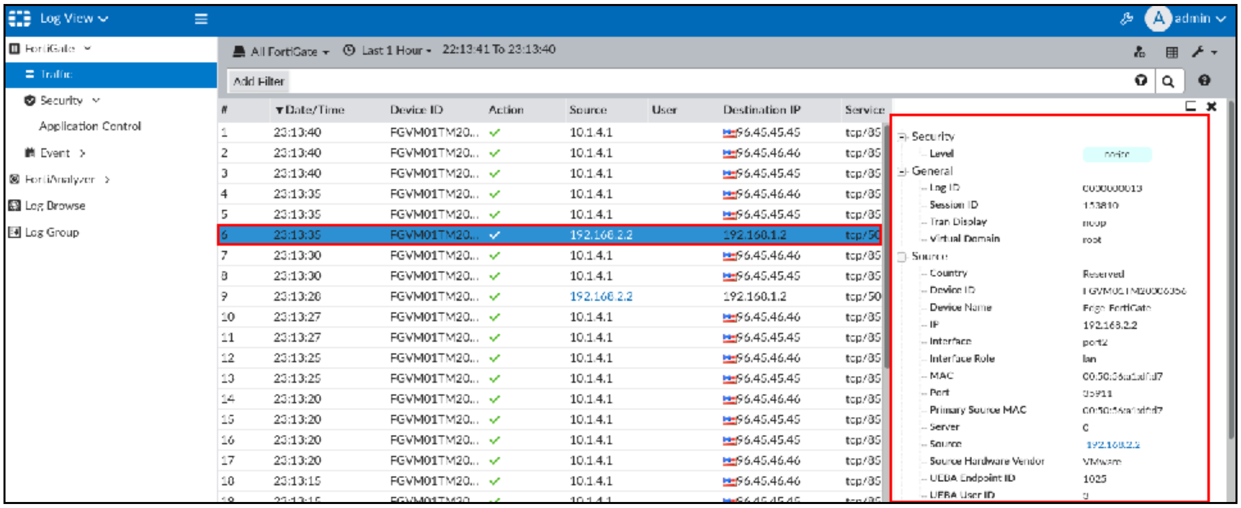
Note that you can click **Pause** to stop the traffic if you want to look at one or more logs without losing them among all the real-time logs constantly dropping in. Click **Resume** to resume.

Real-time logs are temporarily considered compressed, but are indexed as soon as FortiAnalyzer has available CPU and memory.

- Click **Tools** > **Historical Log**.

  You should see formatted, historical logs according to the filters that are set. For example, **All FortiGate** and **Last 1 hour**. Double-click a log to see more details.

The indexing process may take a few minutes to show all historical logs.



22:13:41 To 23:13:40

#	Date/Time	Device ID	Action	Source	User	Destination IP	Service
1	23:13:40	FGVM01TM20...	✓	10.1.4.1		96.45.45.45	tcp/85
2	23:13:40	FGVM01TM20...	✓	10.1.4.1		96.45.46.46	tcp/85
3	23:13:40	FGVM01TM20...	✓	10.1.4.1		96.45.45.45	tcp/85
4	23:13:35	FGVM01TM20...	✓	10.1.4.1		96.45.46.46	tcp/85
5	23:13:35	FGVM01TM20...	✓	10.1.4.1		96.45.45.45	tcp/85
6	23:13:35	FGVM01TM20...	✓	192.168.2.2		192.168.1.2	tcp/50
7	23:13:30	FGVM01TM20...	✓	10.1.4.1		96.45.46.46	tcp/85
8	23:13:30	FGVM01TM20...	✓	10.1.4.1		96.45.45.45	tcp/85
9	23:13:28	FGVM01TM20...	✓	192.168.2.2		192.168.1.2	tcp/50
10	23:13:27	FGVM01TM20...	✓	10.1.4.1		96.45.46.46	tcp/85
11	23:13:27	FGVM01TM20...	✓	10.1.4.1		96.45.45.45	tcp/85
12	23:13:25	FGVM01TM20...	✓	10.1.4.1		96.45.46.46	tcp/85
13	23:13:25	FGVM01TM20...	✓	10.1.4.1		96.45.45.45	tcp/85
14	23:13:20	FGVM01TM20...	✓	10.1.4.1		96.45.46.46	tcp/85
15	23:13:20	FGVM01TM20...	✓	10.1.4.1		96.45.45.45	tcp/85
16	23:13:20	FGVM01TM20...	✓	10.1.4.1		96.45.45.45	tcp/85
17	23:13:20	FGVM01TM20...	✓	10.1.4.1		96.45.46.46	tcp/85
18	23:13:15	FGVM01TM20...	✓	10.1.4.1		96.45.46.46	tcp/85

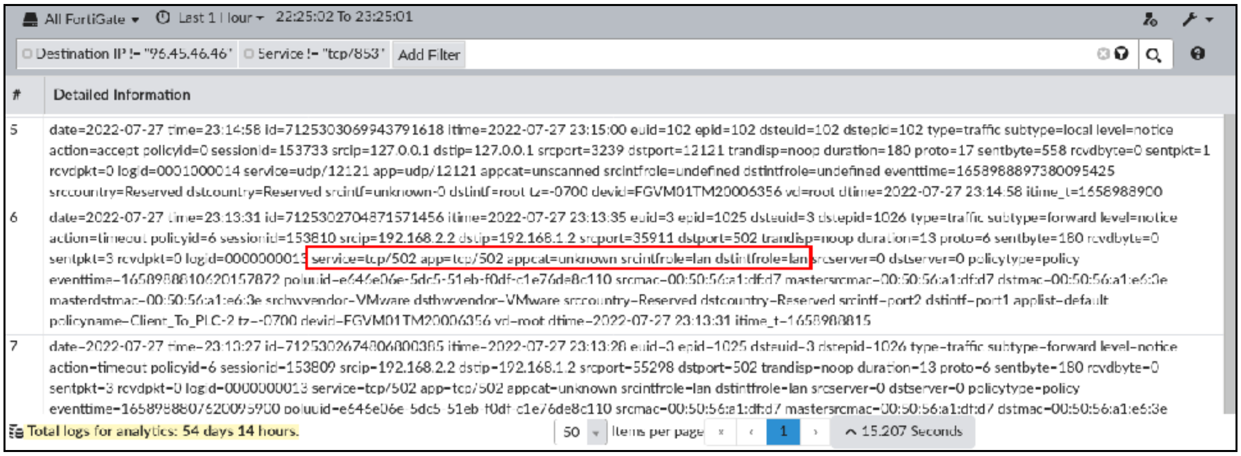
Security	
Level	notice
General	
Log ID	0000000013
Session ID	153810
Tran Display	noop
Virtual Domain	root
Source	
Country	Reserved
Device ID	FGVM01TM20006356
Device Name	Edge-FortiGate
IP	192.168.2.2
Interface	port2
Interface Role	lan
MAC	00:50:56:a1:df:d7
Port	35911
Primary Source MAC	00:50:56:a1:df:d7
Server	0
Source	192.168.2.2
Source Hardware Vendor	VMware
UEBA Endpoint ID	1025
UEBA User ID	3

You can view details about historical logs, because they have been indexed in the SQL database.

- Click **Tools** > **Display Raw**.

  You should see the raw logs (not formatted).

While logs are compressed, they are considered offline, and you cannot view details about the logs in Log View (or FortiView). Also, you cannot customize the columns.



22:25:02 To 23:25:01

Destination IP != "96.45.46.46" Service != "tcp/853"

#	Detailed Information
5	date=2022-07-27 time=23:14:58 id=7125303069943791618 itime=2022-07-27 23:15:00 euid=102 epid=102 dsteuid=102 dstepid=102 type=traffic subtype=local level=notice action=accept policyid=0 sessionid=153733 srcip=127.0.0.1 dstip=127.0.0.1 srcport=3239 dstport=12121 trandisp=noop duration=180 proto=17 sentbyte=558 rcvdbyte=0 sentpkt=1 rcvdpkt=0 logid=0001000014 service=udp/12121 app=udp/12121 appcat=unscanned srcintfrole=undefined dstintfrole=undefined eventtime=1658988897380095425 srccountry=Reserved dstcountry=Reserved srcintf=unknown-0 dstintf=root tz=-0700 devid=FGVM01TM20006356 vd=root dtime=2022-07-27 23:14:58 itime_t=1658988900
6	date=2022-07-27 time=23:13:31 id=7125302704871571456 itime=2022-07-27 23:13:35 euid=3 epid=1025 dsteuid=3 dstepid=1026 type=traffic subtype=forward level=notice action=timeout policyid=6 sessionid=153810 srcip=192.168.2.2 dstip=192.168.1.2 srcport=35911 dstport=502 trandisp=noop duration=13 proto=6 sentbyte=180 rcvdbyte=0 sentpkt=3 rcvdpkt=0 logid=0000000013 service=tcp/502 app=tcp/502 appcat=unknown srcintfrole=lan dstintfrole=lan srcserver=0 dstserver=0 policytype=policy eventtime=1658988810620157872 poluuid=e646e06e-5dc5-51eb-f0df-c1e76de8c110 srcmac=00:50:56:a1:df:d7 mastersrcmac=00:50:56:a1:df:d7 dstmac=00:50:56:a1:e6:3e masterdstmac=00:50:56:a1:e6:3e srchwvendor=VMware dsthwvendor=VMware srccountry=Reserved dstcountry=Reserved srcintf=port2 dstintf=port1 applist=default policyname=Client_To_PLC-2 tz=-0700 devid=FGVM01TM20006356 vd=root dtime=2022-07-27 23:13:31 itime_t=1658988815
7	date=2022-07-27 time=23:13:27 id=7125302674806800385 itime=2022-07-27 23:13:28 euid=3 epid=1025 dsteuid=3 dstepid=1026 type=traffic subtype=forward level=notice action=timeout policyid=6 sessionid=153809 srcip=192.168.2.2 dstip=192.168.1.2 srcport=55298 dstport=502 trandisp=noop duration=13 proto=6 sentbyte=180 rcvdbyte=0 sentpkt=3 rcvdpkt=0 logid=0000000013 service=tcp/502 app=tcp/502 appcat=unknown srcintfrole=lan dstintfrole=lan srcserver=0 dstserver=0 policytype=policy eventtime=1658988807620095900 poluuid=e646e06e-5dc5-51eb-f0df-c1e76de8c110 srcmac=00:50:56:a1:df:d7 mastersrcmac=00:50:56:a1:df:d7 dstmac=00:50:56:a1:e6:3e

Total logs for analytics: 54 days 14 hours.

50 Items per page 1 15.207 Seconds

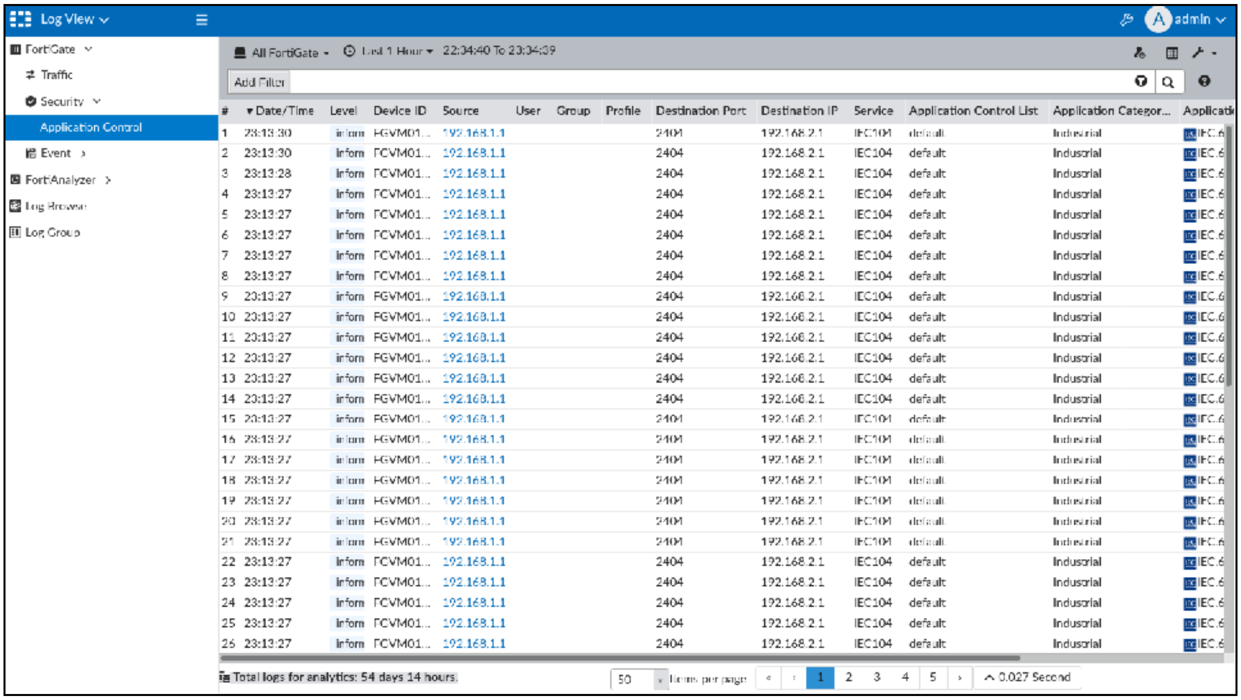
5. Click **Tools** > **Formatted Log** to return the view to formatted logs.
6. In the menu on the left, click **Security** to examine the security logs.

   Security logs from FortiAnalyzer include antivirus, web filtering, application control, intrusion prevention, email filtering, data leak prevention, SSL/SSH scan, and VoIP. The logs displayed on FortiAnalyzer are dependent on the device type logging to it, the traffic, and the features that are enabled. In this lab, only web filter, application control, and intrusion prevention logs are triggered.

You can also view security logs in real-time or historical views, and in raw or formatted formats.

- Click **Security** > **Application Control**.

  You should see all logs that match application control traffic. Double-click a log for more details.



22:34:40 To 23:34:39

#	Date/Time	Level	Device ID	Source	User	Group	Profile	Destination Port	Destination IP	Service	Application Control List	Application Categor...	Applicati
1	23:13:30	inform	FGVM01...	192.168.1.1				2404	192.168.2.1	IEC104	default	Industrial	IEC.6
2	23:13:30	inform	FGVM01...	192.168.1.1				2404	192.168.2.1	IEC104	default	Industrial	IEC.6
3	23:13:28	inform	FGVM01...	192.168.1.1				2404	192.168.2.1	IEC104	default	Industrial	IEC.6
4	23:13:27	inform	FGVM01...	192.168.1.1				2404	192.168.2.1	IEC104	default	Industrial	IEC.6
5	23:13:27	inform	FGVM01...	192.168.1.1				2404	192.168.2.1	IEC104	default	Industrial	IEC.6
6	23:13:27	inform	FGVM01...	192.168.1.1				2404	192.168.2.1	IEC104	default	Industrial	IEC.6
7	23:13:27	inform	FGVM01...	192.168.1.1				2404	192.168.2.1	IEC104	default	Industrial	IEC.6
8	23:13:27	inform	FGVM01...	192.168.1.1				2404	192.168.2.1	IEC104	default	Industrial	IEC.6
9	23:13:27	inform	FGVM01...	192.168.1.1				2404	192.168.2.1	IEC104	default	Industrial	IEC.6
10	23:13:27	inform	FGVM01...	192.168.1.1				2404	192.168.2.1	IEC104	default	Industrial	IEC.6
11	23:13:27	inform	FGVM01...	192.168.1.1				2404	192.168.2.1	IEC104	default	Industrial	IEC.6
12	23:13:27	inform	FGVM01...	192.168.1.1				2404	192.168.2.1	IEC104	default	Industrial	IEC.6
13	23:13:27	inform	FGVM01...	192.168.1.1				2404	192.168.2.1	IEC104	default	Industrial	IEC.6
14	23:13:27	inform	FGVM01...	192.168.1.1				2404	192.168.2.1	IEC104	default	Industrial	IEC.6
15	23:13:27	inform	FGVM01...	192.168.1.1				2404	192.168.2.1	IEC104	default	Industrial	IEC.6
16	23:13:27	inform	FGVM01...	192.168.1.1				2404	192.168.2.1	IEC104	default	Industrial	IEC.6
17	23:13:27	inform	FGVM01...	192.168.1.1				2404	192.168.2.1	IEC104	default	Industrial	IEC.6
18	23:13:27	inform	FGVM01...	192.168.1.1				2404	192.168.2.1	IEC104	default	Industrial	IEC.6
19	23:13:27	inform	FGVM01...	192.168.1.1				2404	192.168.2.1	IEC104	default	Industrial	IEC.6
20	23:13:27	inform	FGVM01...	192.168.1.1				2404	192.168.2.1	IEC104	default	Industrial	IEC.6
21	23:13:27	inform	FGVM01...	192.168.1.1				2404	192.168.2.1	IEC104	default	Industrial	IEC.6
22	23:13:27	inform	FGVM01...	192.168.1.1				2404	192.168.2.1	IEC104	default	Industrial	IEC.6
23	23:13:27	inform	FGVM01...	192.168.1.1				2404	192.168.2.1	IEC104	default	Industrial	IEC.6
24	23:13:27	inform	FGVM01...	192.168.1.1				2404	192.168.2.1	IEC104	default	Industrial	IEC.6
25	23:13:27	inform	FGVM01...	192.168.1.1				2404	192.168.2.1	IEC104	default	Industrial	IEC.6
26	23:13:27	inform	FGVM01...	192.168.1.1				2404	192.168.2.1	IEC104	default	Industrial	IEC.6

Total logs for analytics: 54 days 14 hours.

0.027 Second

Use Log Filters

You can use log filters to narrow down search results and locate specific logs.

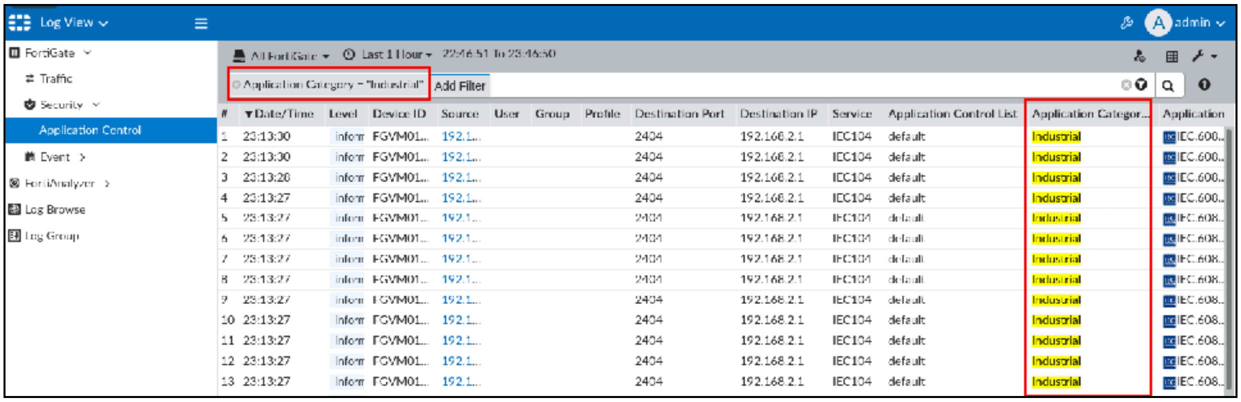
Tips:

- If you are not sure what the correctly formed column name is, add the column name that you want to search for in the **Column Settings** drop-down list.
- Ensure your time filter covers the logs that you are searching for.
- Ensure the device is set accordingly for the logs you want to return.
- Verify whether case-sensitive search is enabled or disabled (**Tools**).

- Ensure you are searching on the appropriate log type for the logs you want to return (for example, traffic, web filter, application control, IPS, and so on).
- Ensure you are not in the raw log view, because you cannot filter on raw logs (only historical and real-time).
- Ensure you are not filtering on real-time logs if you want to search on historical logs.

To use log filters

1. Continuing on the FortiAnalyzer GUI, click **Log View**.
2. Locate the following logs:
   - Application control logs on all FortiGate devices over the past hour with a specific application category (for example, **Industrial**)



#	Date/Time	Level	Device ID	Source	User	Group	Profile	Destination Port	Destination IP	Service	Application Control List	Application Categor...	Application
1	23:13:30	inform	FGVM01...	192.1...				2404	192.168.2.1	IEC104	default	Industrial	IEC.600...
2	23:13:30	inform	FGVM01...	192.1...				2404	192.168.2.1	IEC104	default	Industrial	IEC.600...
3	23:13:28	inform	FGVM01...	192.1...				2404	192.168.2.1	IEC104	default	Industrial	IEC.600...
4	23:13:27	inform	FGVM01...	192.1...				2404	192.168.2.1	IEC104	default	Industrial	IEC.600...
5	23:13:27	inform	FGVM01...	192.1...				2404	192.168.2.1	IEC104	default	Industrial	IEC.608...
6	23:13:27	inform	FGVM01...	192.1...				2404	192.168.2.1	IEC104	default	Industrial	IEC.608...
7	23:13:27	inform	FGVM01...	192.1...				2404	192.168.2.1	IEC104	default	Industrial	IEC.608...
8	23:13:27	inform	FGVM01...	192.1...				2404	192.168.2.1	IEC104	default	Industrial	IEC.608...
9	23:13:27	inform	FGVM01...	192.1...				2404	192.168.2.1	IEC104	default	Industrial	IEC.608...
10	23:13:27	inform	FGVM01...	192.1...				2404	192.168.2.1	IEC104	default	Industrial	IEC.608...
11	23:13:27	inform	FGVM01...	192.1...				2404	192.168.2.1	IEC104	default	Industrial	IEC.608...
12	23:13:27	inform	FGVM01...	192.1...				2404	192.168.2.1	IEC104	default	Industrial	IEC.608...
13	23:13:27	inform	FGVM01...	192.1...				2404	192.168.2.1	IEC104	default	Industrial	IEC.608...

Ensure your time filter is set correctly (includes the time you have been generating traffic).

Create a Custom View

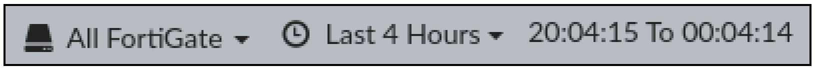
You will create a custom view for industrial protocols and application categories.

To create a custom view

1. Continuing on the FortiAnalyzer GUI, click **Log View** > **Security** > **Application Control**.

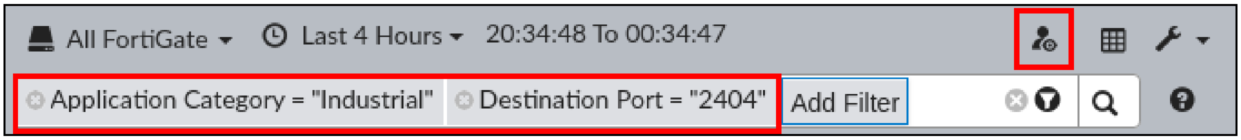
Ensure your time filter is set correctly (includes the time you have been generating traffic).

Set your time filters appropriately, and if required, increase the time range from 1 to 4 hours.



2. Click **Add Filter**, type `Application`, in the drop-down list, select **Application Category**, and then select **"Industrial"**.

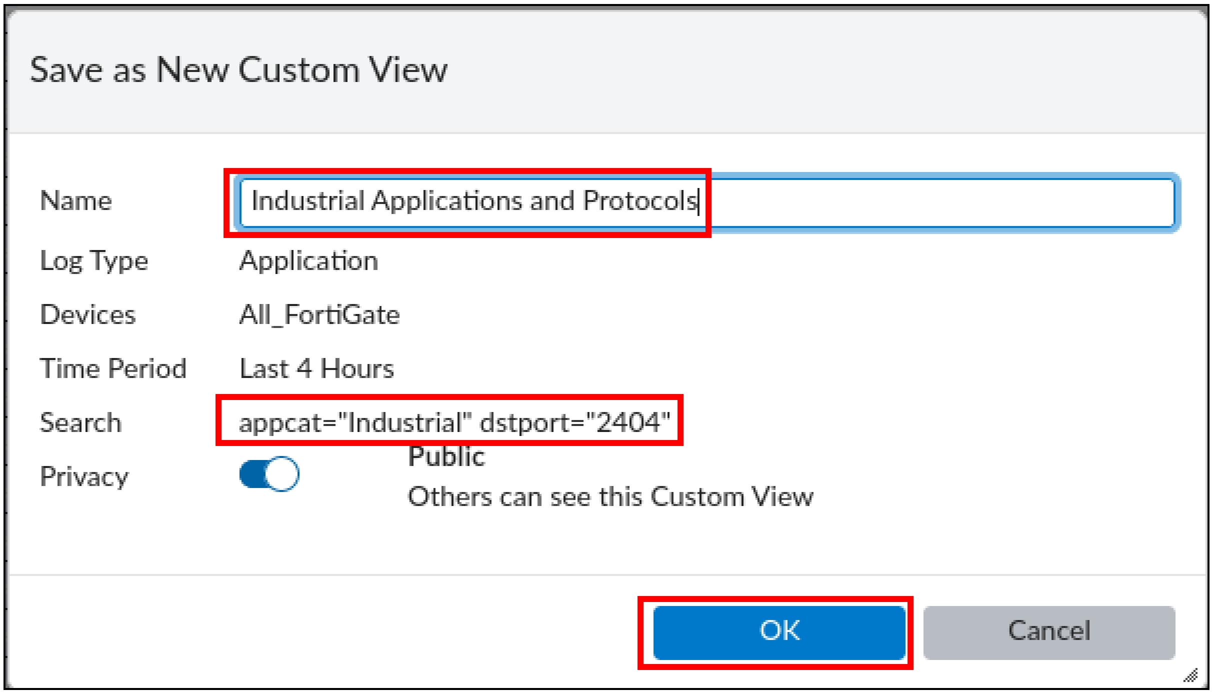
3. Click **Add Filter** again, type `Destination`, in the drop-down list, select **Destination Port**, and then type `"2404"`.
4. To the right of the filters, click the custom view icon.



All FortiGate ▾ Last 4 Hours ▾ 20:34:48 To 00:34:47

Application Category = "Industrial" Destination Port = "2404" Add Filter

5. In the **Name** field, type `Industrial Applications and Protocols`.
6. Click **OK**.



Save as New Custom View

Name: Industrial Applications and Protocols

Log Type: Application

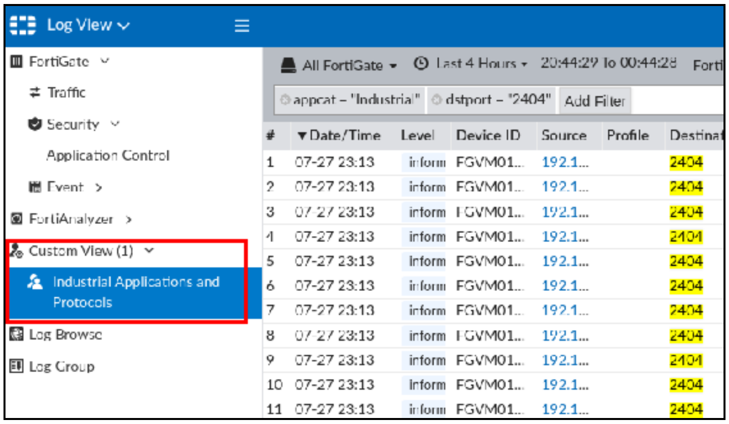
Devices: All_FortiGate

Time Period: Last 4 Hours

Search: appcat="Industrial" dstport="2404"

Privacy: Public
Others can see this Custom View

7. In the **Custom View** section, you can review the **Industrial Applications and Protocols** custom view.



All FortiGate ▾ Last 4 Hours ▾ 20:44:29 To 00:44:28 Forti

appcat = "Industrial" dstport = "2404" Add Filter

#	Date/Time	Level	Device ID	Source	Profile	Destinat
1	07-27 23:13	inform	FGVM01...	192.1...		2404
2	07-27 23:13	inform	FGVM01...	192.1...		2404
3	07-27 23:13	inform	FGVM01...	192.1...		2404
4	07-27 23:13	inform	FGVM01...	192.1...		2404
5	07-27 23:13	inform	FGVM01...	192.1...		2404
6	07-27 23:13	inform	FGVM01...	192.1...		2404
7	07-27 23:13	inform	FGVM01...	192.1...		2404
8	07-27 23:13	inform	FGVM01...	192.1...		2404
9	07-27 23:13	inform	FGVM01...	192.1...		2404
10	07-27 23:13	inform	FGVM01...	192.1...		2404
11	07-27 23:13	inform	FGVM01...	192.1...		2404

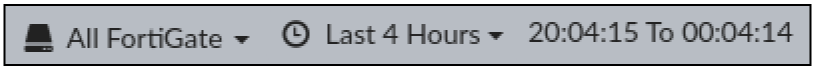
Explore FortiView

You can view summaries of log data in FortiView in both tabular and graphical formats. For example, you can view top applications and websites, top threats to your network, top sources of network traffic, and top destinations of network traffic. For each summary view, you can drill down into details.

To view logs in FortiView

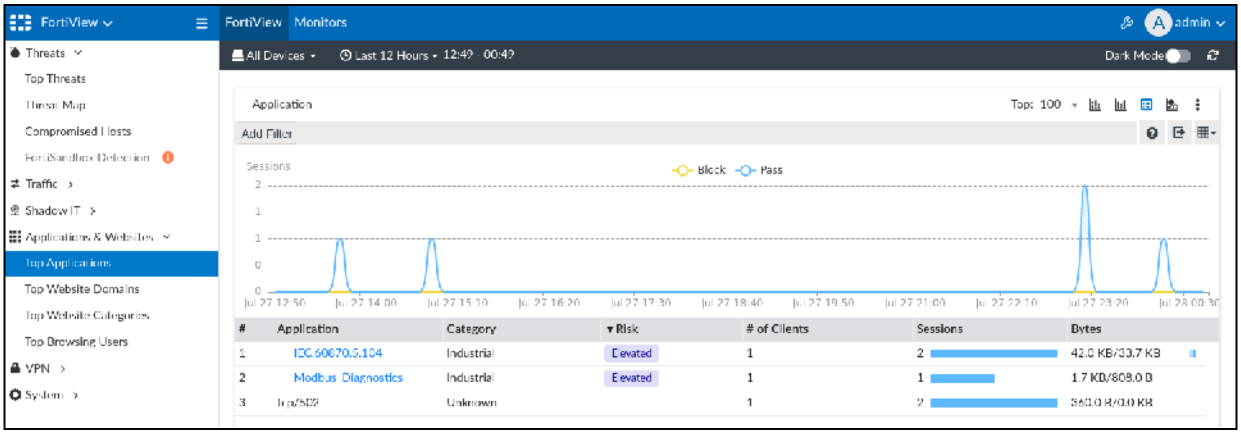
1. Click **Log View** > **FortiView**.
2. Examine (and experiment with) the following views and feel free to add notes:

Set your time filters appropriately!



All FortiGate ▾ Last 4 Hours ▾ 20:04:15 To 00:04:14

Category	View	Notes
Applications & Websites	Top Applications Displays information about the top applications being used on the network, including the application name, category, and risk level.	



#	Application	Category	▾Risk	# of Clients	Sessions	Bytes
1	IEC.60870.5.104	Industrial	Elevated	1	2	42.0 KB/33.7 KB
2	Modbus_Diagnostics	Industrial	Elevated	1	1	1.7 KB/808.0 B
3	tcp/502	Unknown		1	2	360.0 B/0.0 KB

Explore FortiSOC

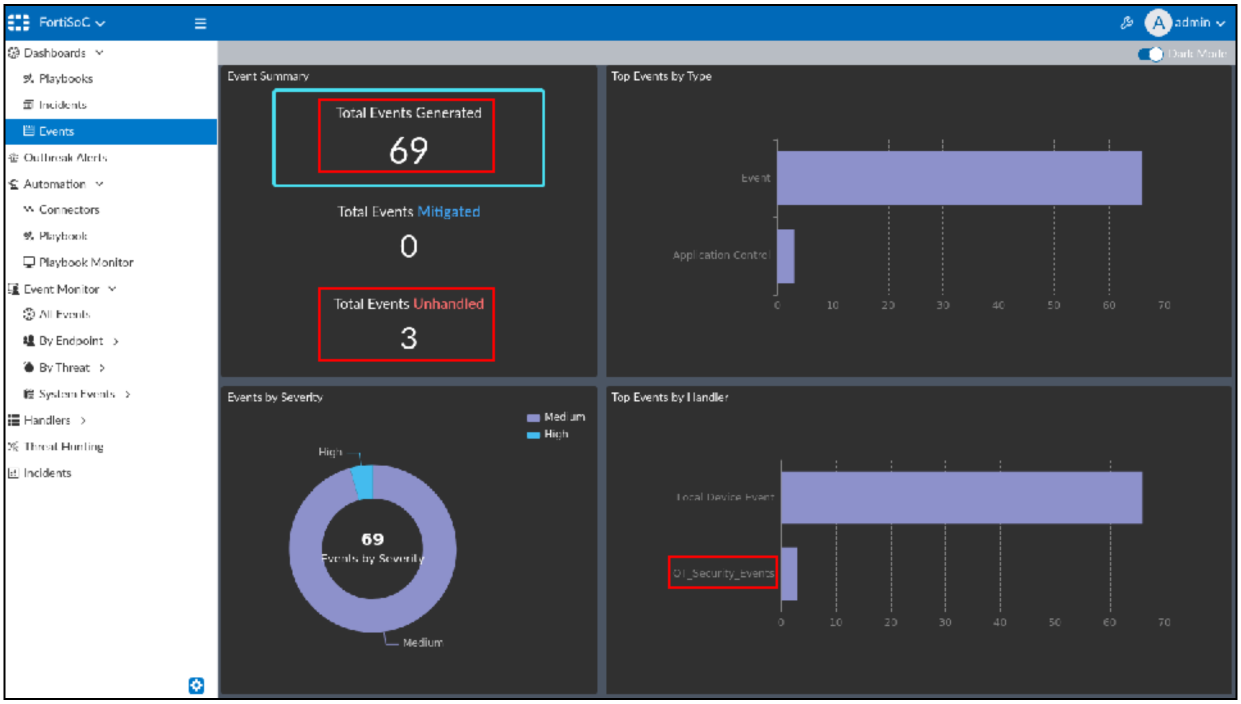
FortiSoC provides events and incident management capabilities. You will review the OT security events that the event handler created, and you will also create an incident for the OT security event.

View OT Security Events and Incidents

You will view the OT security event that the event handler you configured in the first exercise created, and then you will create an incident for the event.

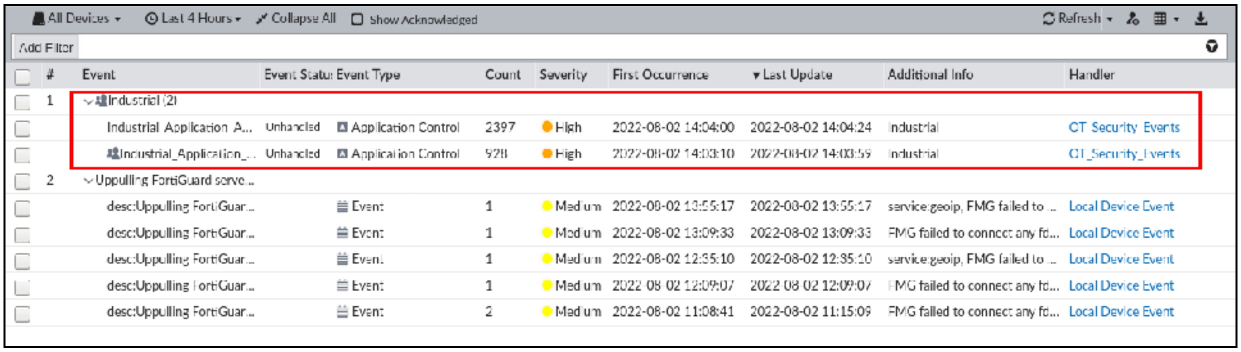
To view events and create an incident

1. Click **FortiView** > **FortiSOC**.
2. Click **Dashboards** > **Events** to verify two **OT_Security_Events**.



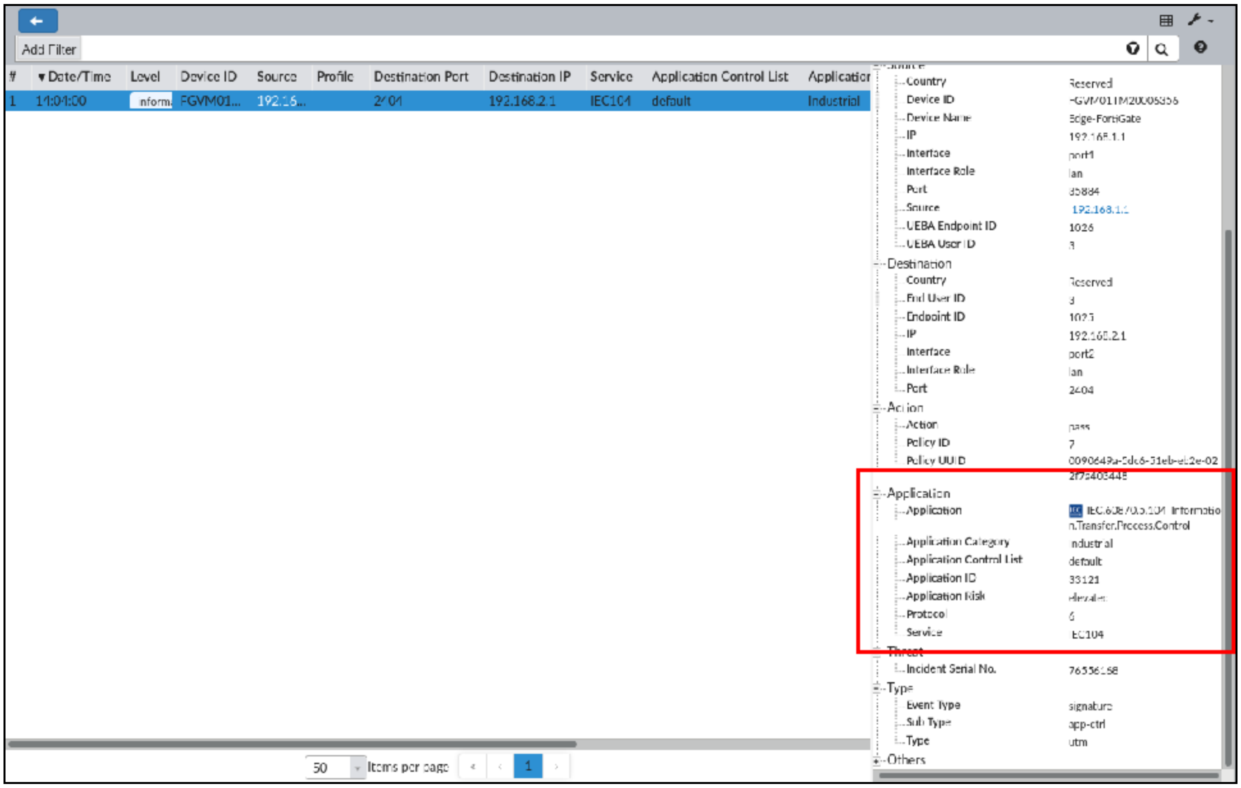
3. Click **Event Monitor** > **All Events**, and then expand the **Industrial** event.

   You should see at least two grouped events for the industrial category—one for the Modbus application and one for IEC 104.



□	#	Event	Event Status	Event Type	Count	Severity	First Occurrence	▾ Last Update	Additional Info	Handler
□	1	Industrial (2)								
□		Industrial Application A...	Unhandled	Application Control	2397	● High	2022-08-02 14:04:00	2022-08-02 14:04:24	industrial	CT Security Events
□		Industrial_Application_...	Unhandled	Application Control	928	● High	2022-08-02 14:03:10	2022-08-02 14:03:59	industrial	OT_Security_Events
□	2	Uppulling FortiGuard serve...								
□		desc:Uppulling FortiGuar...		Event	1	● Medium	2022-08-02 13:55:17	2022-08-02 13:55:17	service:geoip, FMG failed to ...	Local Device Event
□		desc:Uppulling FortiGuar...		Event	1	● Medium	2022-08-02 13:09:33	2022-08-02 13:09:33	FMG failed to connect any fd...	Local Device Event
□		desc:Uppulling FortiGuar...		Event	1	● Medium	2022-08-02 12:35:10	2022-08-02 12:35:10	service:geoip, FMG failed to ...	Local Device Event
□		desc:Uppulling FortiGuar...		Event	1	● Medium	2022-08-02 12:09:07	2022-08-02 12:09:07	FMG failed to connect any fd...	Local Device Event
□		desc:Uppulling FortiGuar...		Event	2	● Medium	2022-08-02 11:08:41	2022-08-02 11:15:09	FMG failed to connect any fd...	Local Device Event

4. Double-click one of the events to view logs for the event, and then double-click the log again to view log details.



Add Filter

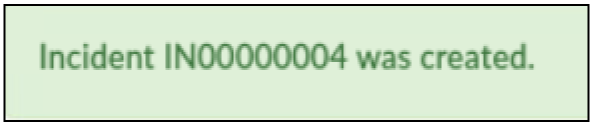
#	Date/Time	Level	Device ID	Source	Profile	Destination Port	Destination IP	Service	Application Control List	Applicatior
1	14:04:00	inform.	FGVM01...	192.16...		2404	192.168.2.1	IEC104	default	Industrial

Country	Reserved
Device ID	FGVM01TM20005356
Device Name	Edge-FortiGate
IP	192.168.1.1
Interface	port1
Interface Role	lan
Port	35884
Source	192.168.1.1
UEBA Endpoint ID	1026
UEBA User ID	3
Destination	
Country	Reserved
End User ID	3
Endpoint ID	1023
IP	192.168.2.1
Interface	port2
Interface Role	lan
Port	2404
Action	
Action	pass
Policy ID	7
Policy UUID	0090649a-5dc6-51eb-eb2e-022f75403445
Application	
Application	IEC.60870.5.104_Information.Transfer.Process.Control
Application Category	Industrial
Application Control List	default
Application ID	33121
Application Risk	elevated
Protocol	6
Service	IEC104
Threat	
Incident Serial No.	76556158
Type	
Event Type	signature
Sub Type	app-ctrl
Type	utm
Others	

5. Click the back arrow icon to go back to **All Events**, select one of the events, right-click the event, and then click **Create New Incident** to manually create an incident for the selected event.
6. In the **Raise Incident** window, configure the following settings:

Field	Value
Incident Category	Unauthorized Access
Severity	High
Status	New
Description	Investigate: Industrial_Application_Activity_Detected
Assigned To	admin

7. Click **OK** to create the incident.

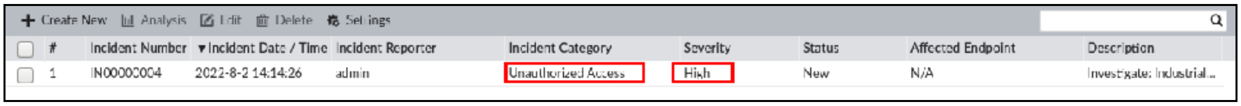


Incident IN00000004 was created.

A window appears, to confirm that the incident was created. The window will disappear by itself.

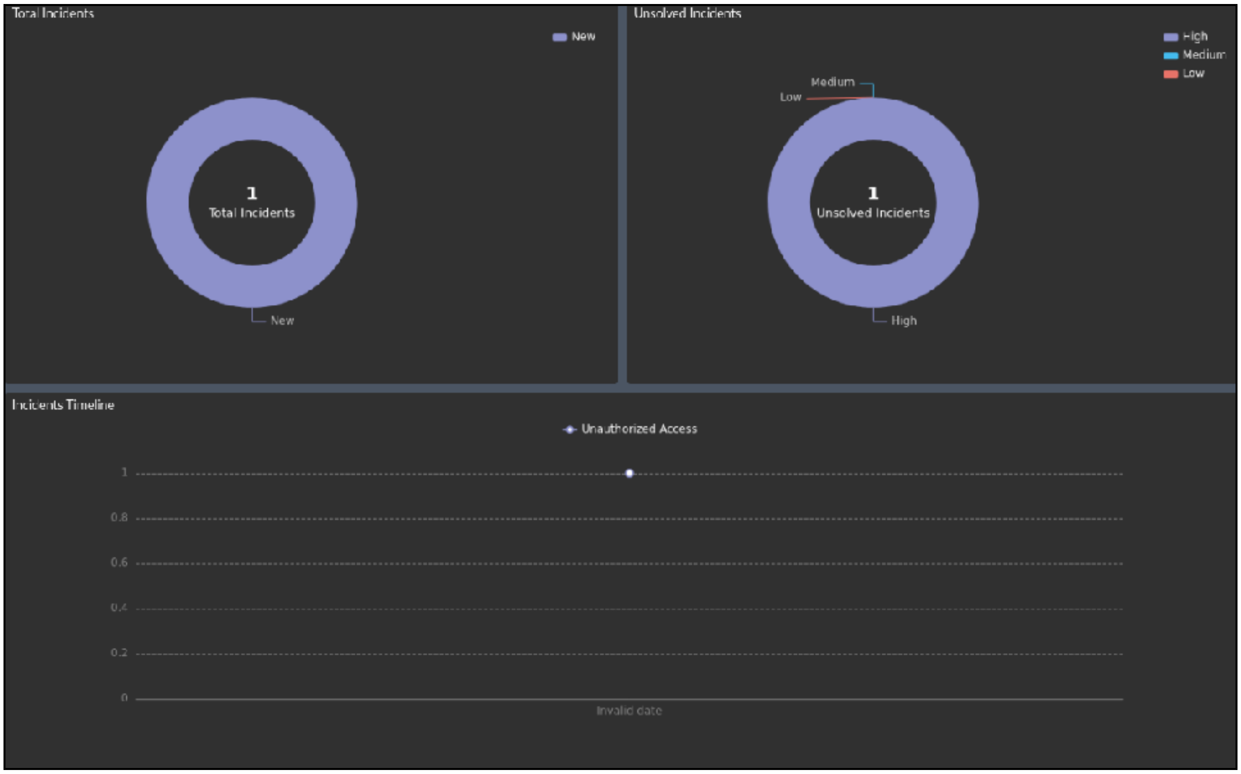
8. Click **Incidents** to view the incident table and verify the incident.

You should see an incident listed in the table.



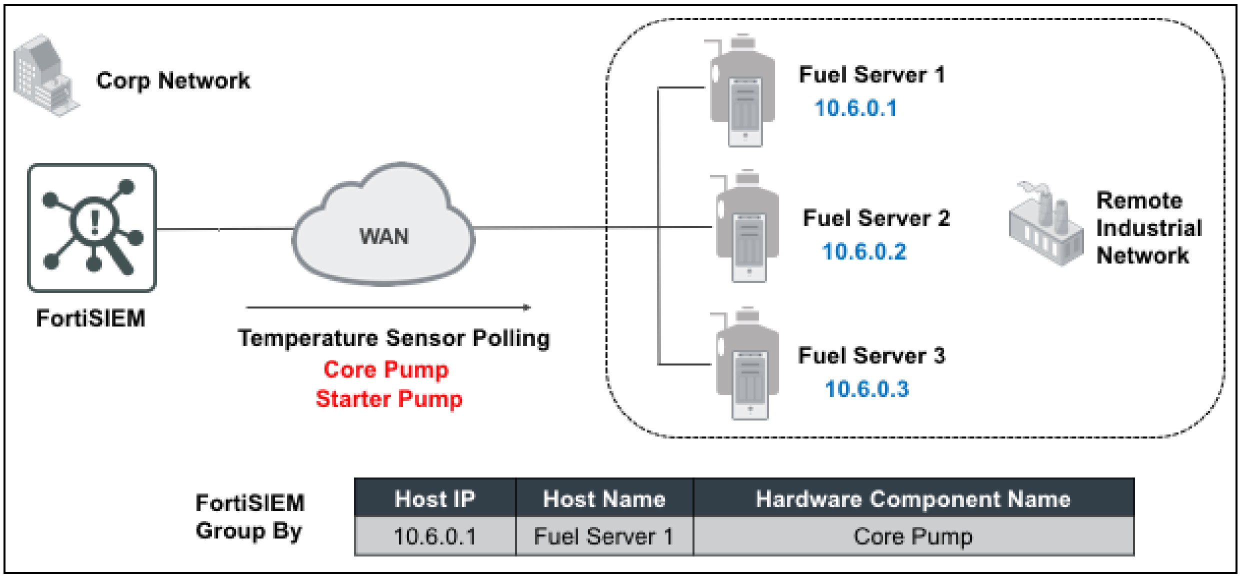
☐	#	Incident Number	▾Incident Date / Time	Incident Reporter	Incident Category	Severity	Status	Affected Endpoint	Description
☐	1	IN00000004	2022-8-2 14:14:26	admin	Unauthorized Access	High	New	N/A	Investigate: Industrial...

9. Click **Dashboards** > **Incidents** to view the count and status of incidents on the **Incidents** dashboard.



Exercise 3: Configuring a Rule to Monitor Performance

In this exercise, you will build a single pattern performance rule to monitor the temperature of some fuel pump sensors, and trigger alerts if the average temperature over a 5-minute time period goes above or below a set threshold (80 degrees Fahrenheit).



Host IP	Host Name	Hardware Component Name
10.6.0.1	Fuel Server 1	Core Pump

FortiSIEM collects temperature events every 60 seconds, and appear as:

Event Type: `PH_DEV_MON_HW_TEMP`

Raw Event Sample:

```
[PH_DEV_MON_HW_TEMP]:[eventSeverity]=PHL_INFO,
[fileName]=deviceCustom.cpp,[lineNumber]=2227,[hostName]=Fuel
Server1,[hostIpAddr]=10.6.0.1,[hwComponentName]=CorePump,
[envTempDegF]=47,[phLogDetail]=
```

Configure a Rule to Monitor Fuel Pump Server Temperature Sensors

You will configure a rule to monitor fuel pump temperature sensors. You will also generate logs to trigger an incident according to your rule.

To configure filters

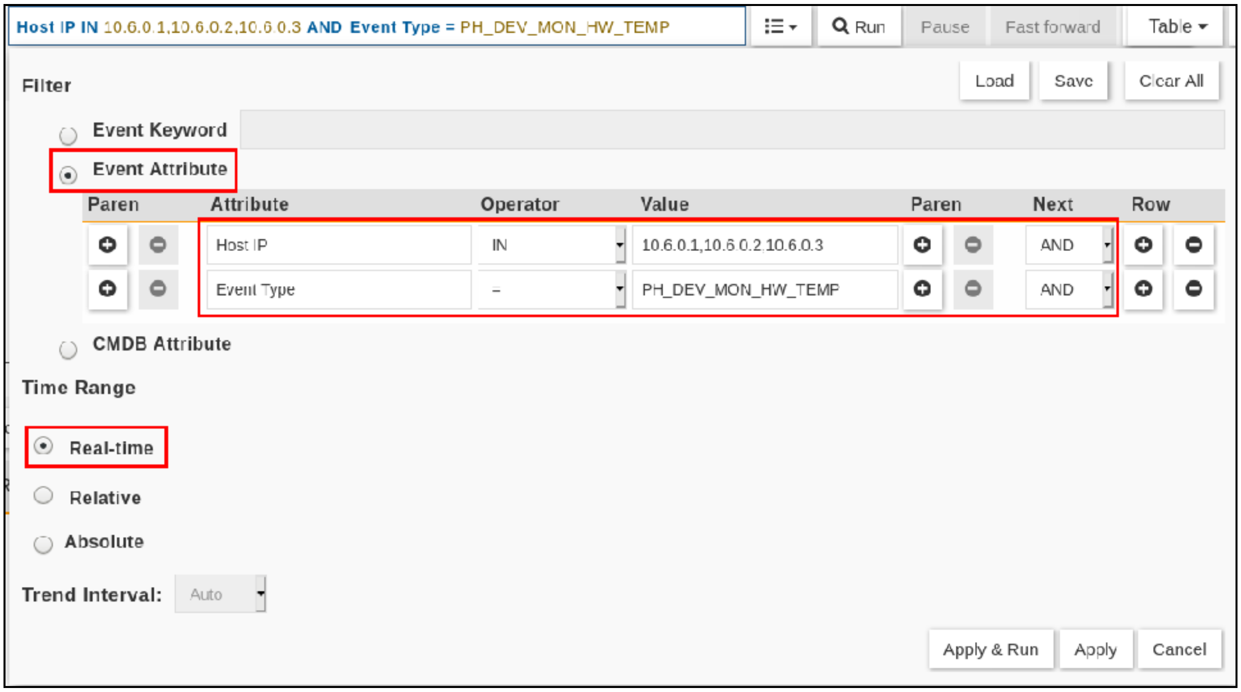
1. Log in to the FortiSIEM GUI, click the **ANALYTICS** tab, and then clear the display filters.
2. Click the change field display icon beside the **Run** icon, and then click **Clear All** to clear any existing fields.
3. Click **Apply**, and then click **Use Default**.
4. In the **Edit Filters and Time Range** field, click the field, and when the **Filter** editor opens, click **Clear All** to clear any existing conditions, and then add the following condition:

Field	Value
Filter	Event Attribute
Attribute	Host IP
Operator	IN
Value	10.6.0.1,10.6.0.2,10.6.0.3
NEXT	AND

5. In the **Row** column associated with the condition, click **+** to add another row.
6. In the second condition row, configure the following settings:

Field	Value
Attribute	Event Type
Operator	=
Value	PH_DEV_MON_HW_TEMP

7. In the **Time Range** section, select **Real Time**.
8. Click **Apply & Run**.



Host IP IN 10.6.0.1,10.6.0.2,10.6.0.3 AND Event Type = PH_DEV_MON_HW_TEMP

Filter

○ Event Keyword
● Event Attribute

Paren	Attribute	Operator	Value	Paren	Next	Row
	Host IP	IN	10.6.0.1,10.6.0.2,10.6.0.3		AND	
	Event Type	=	PH_DEV_MON_HW_TEMP		AND	

○ CMDB Attribute

Time Range

● Real-time
○ Relative
○ Absolute

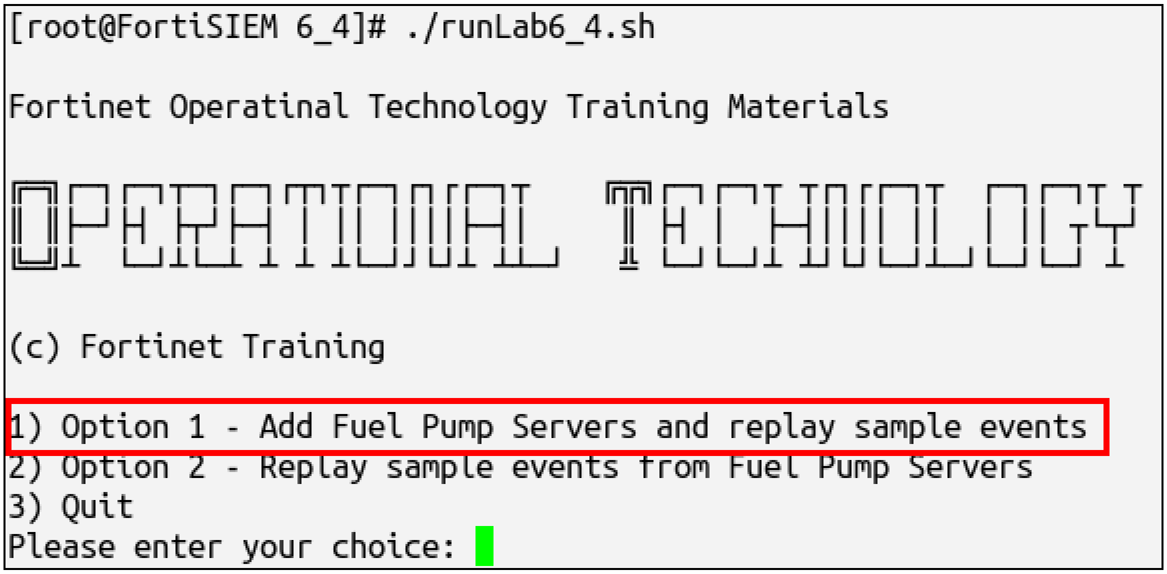
Trend Interval: Auto

To add and generate logs for fuel servers

1. On **Linux-Client**, open PuTTY, create a new SSH session to the **FortiSIEM** device using the **Host Name** `10.1.3.180` and **Port** `22`, and then click **Open**.

2. Log in with the username `root` and password `Fortinet1!`.
3. Enter the following commands, and then when prompted, enter `1` for **Option 1**:

```
cd /root/labs/lab6/6_4

./runLab6_4.sh
```



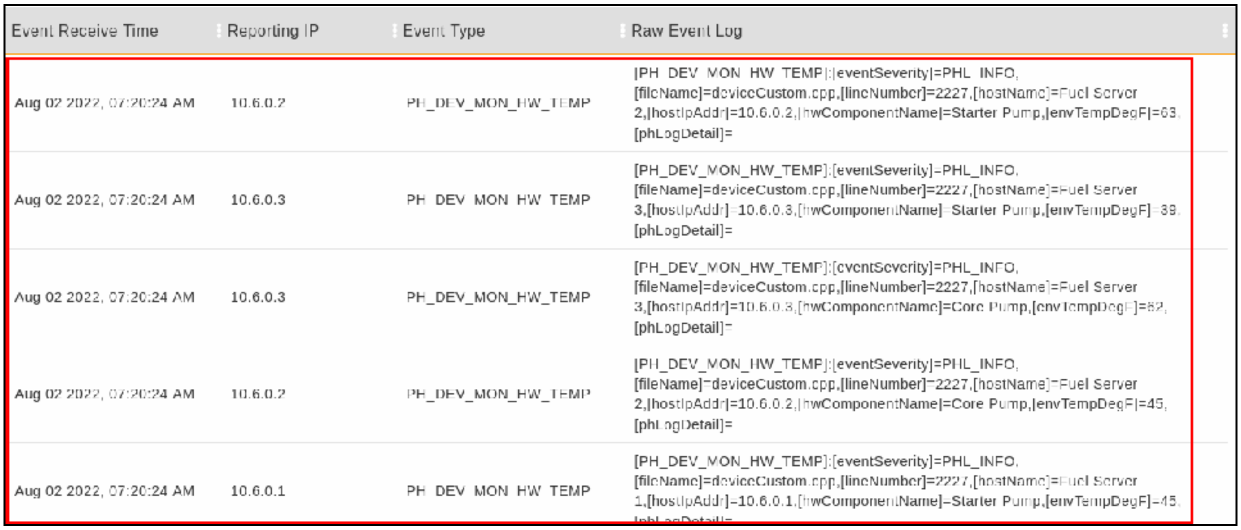
```
[root@FortiSIEM 6_4]# ./runLab6_4.sh

Fortinet Operational Technology Training Materials

OPERATIONAL TECHNOLOGY

(c) Fortinet Training

1) Option 1 - Add Fuel Pump Servers and replay sample events
2) Option 2 - Replay sample events from Fuel Pump Servers
3) Quit
Please enter your choice:
```

This script adds three generic Linux devices to FortiSIEM and replays some temperature events.

On the **CMDB** tab, you can view the devices that were added: Fuel Server 1 – 10.6.0.1, Fuel Server 2 – 10.6.0.2, and Fuel Server 3 – 10.6.0.3.

To view logs

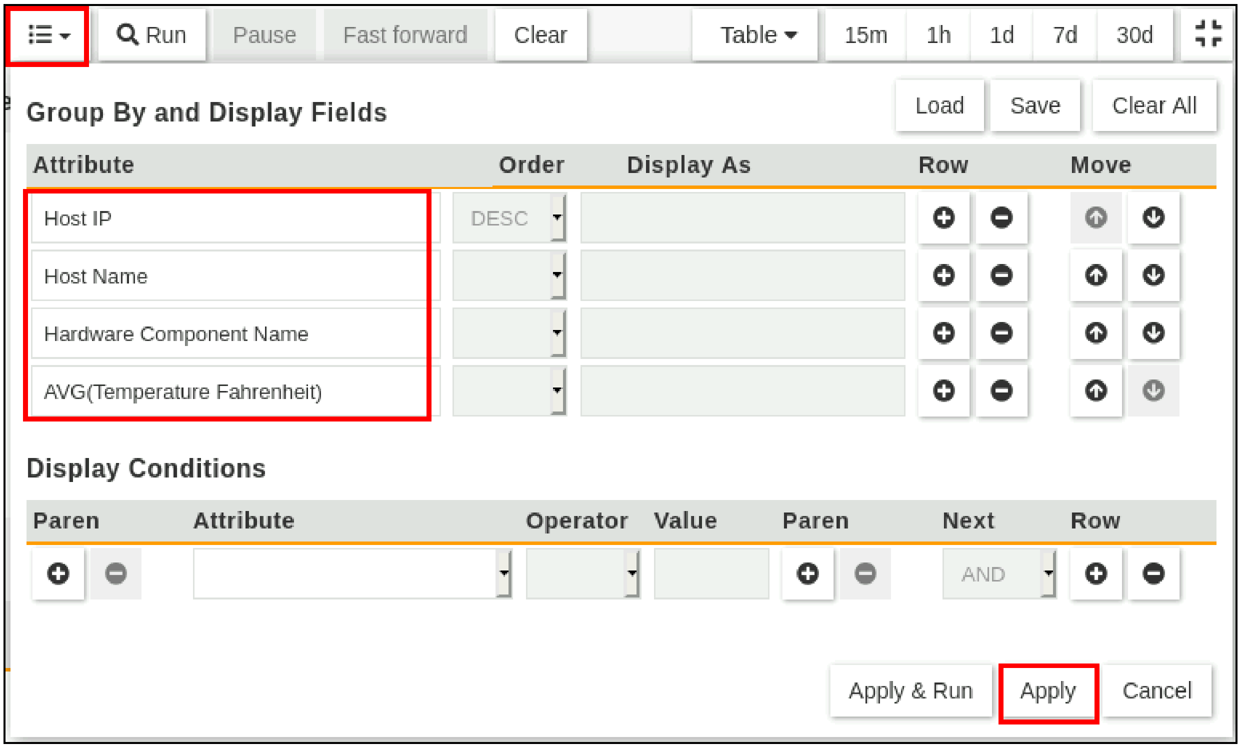
1. On the FortiSIEM GUI, you should see results from the **Real Time** search—review the raw event logs to see their content.



Event Receive Time	Reporting IP	Event Type	Raw Event Log
Aug 02 2022, 07:20:24 AM	10.6.0.2	PH_DEV_MON_HW_TEMP	[PH_DEV_MON_HW_TEMP]:[eventSeverity]=PHL_INFO,[fileName]=deviceCustom.cpp,[lineNumber]=2227,[hostName]=Fuel Server 2,[hostIpAddr]=10.6.0.2,[hwComponentName]=Starter Pump,[envTempDegF]=63,[phLogDetail]=
Aug 02 2022, 07:20:24 AM	10.6.0.3	PH_DEV_MON_HW_TEMP	[PH_DEV_MON_HW_TEMP]:[eventSeverity]=PHL_INFO,[fileName]=deviceCustom.cpp,[lineNumber]=2227,[hostName]=Fuel Server 3,[hostIpAddr]=10.6.0.3,[hwComponentName]=Starter Pump,[envTempDegF]=39,[phLogDetail]=
Aug 02 2022, 07:20:24 AM	10.6.0.3	PH_DEV_MON_HW_TEMP	[PH_DEV_MON_HW_TEMP]:[eventSeverity]=PHL_INFO,[fileName]=deviceCustom.cpp,[lineNumber]=2227,[hostName]=Fuel Server 3,[hostIpAddr]=10.6.0.3,[hwComponentName]=Core Pump,[envTempDegF]=82,[phLogDetail]=
Aug 02 2022, 07:20:24 AM	10.6.0.2	PH_DEV_MON_HW_TEMP	[PH_DEV_MON_HW_TEMP]:[eventSeverity]=PHL_INFO,[fileName]=deviceCustom.cpp,[lineNumber]=2227,[hostName]=Fuel Server 2,[hostIpAddr]=10.6.0.2,[hwComponentName]=Core Pump,[envTempDegF]=45,[phLogDetail]=
Aug 02 2022, 07:20:24 AM	10.6.0.1	PH_DEV_MON_HW_TEMP	[PH_DEV_MON_HW_TEMP]:[eventSeverity]=PHL_INFO,[fileName]=deviceCustom.cpp,[lineNumber]=2227,[hostName]=Fuel Server 1,[hostIpAddr]=10.6.0.1,[hwComponentName]=Starter Pump,[envTempDegF]=45,[phLogDetail]=

The script may take a couple of minutes to process and display the logs. If you cannot see logs on the FortiSIEM GUI, run the scripts again.

2. Edit the **Group By and Display Fields** section to match the following image, and then click **Apply**:



Group By and Display Fields

Attribute	Order	Display As
Host IP	DESC	
Host Name		
Hardware Component Name		
AVG(Temperature Fahrenheit)		

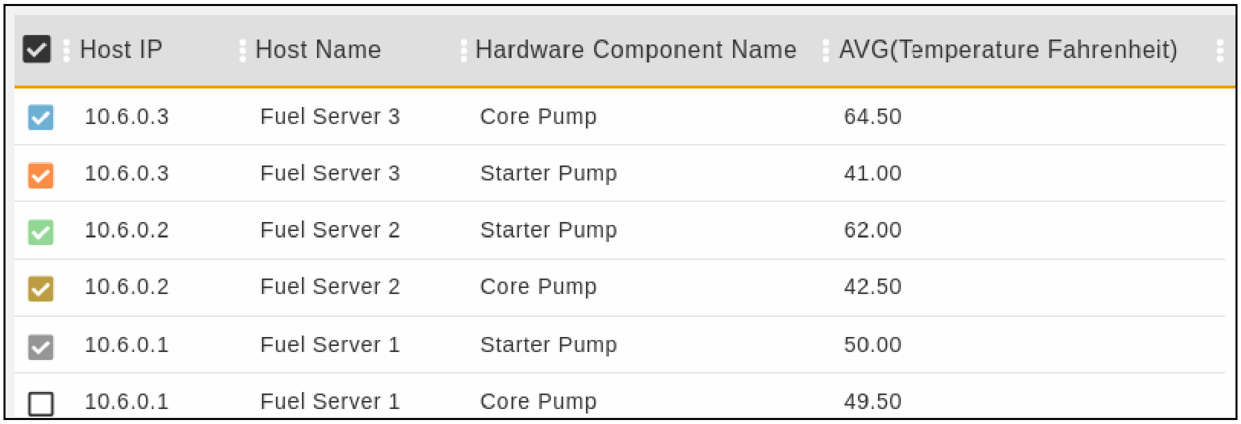
Display Conditions

Paren	Attribute	Operator	Value	Paren	Next	Row
					AND	

Use the **Expression Builder** to create the **AVG(Temperature Fahrenheit)** field for the **Group By and Display fields**.

3. Perform the search again using a **Relative** time period of 10 minutes.

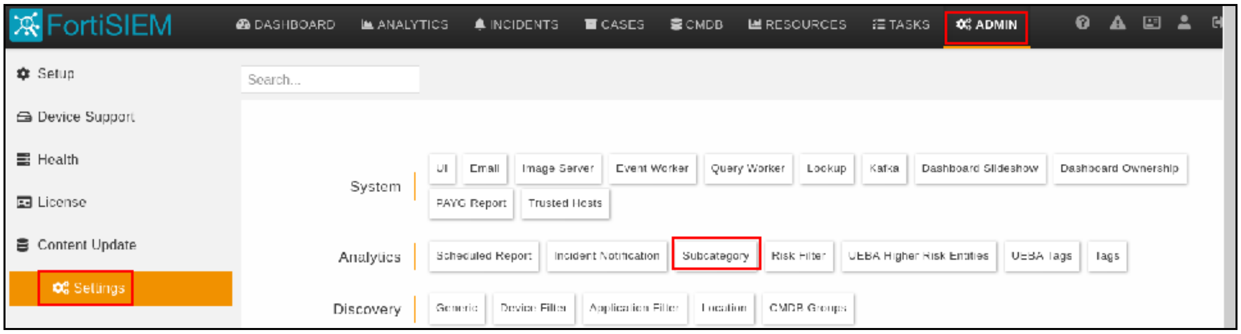
   The results should be similar to the following example. Notice that for the same **Host IP**, **Host Name**, and **Hardware Component Name**, the average temperature in Fahrenheit is now reported.



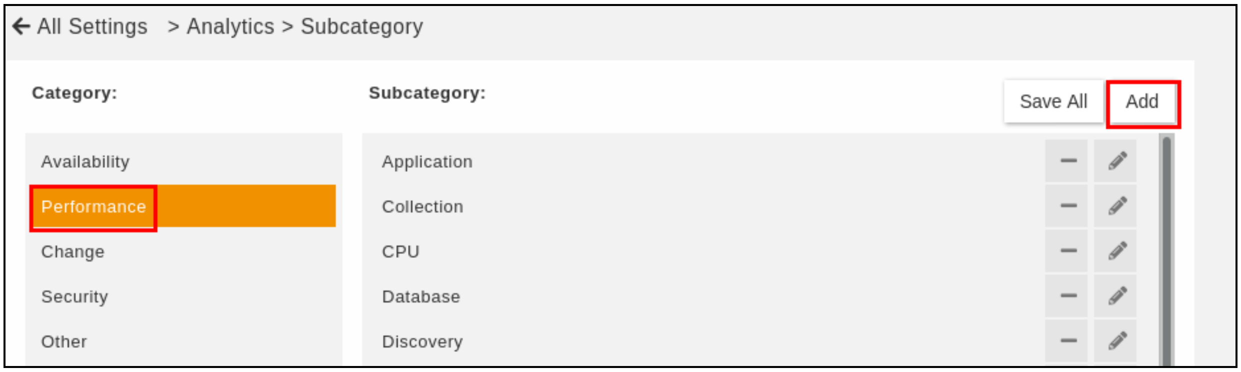
☑	Host IP	Host Name	Hardware Component Name	AVG(Temperature Fahrenheit)
☑	10.6.0.3	Fuel Server 3	Core Pump	64.50
☑	10.6.0.3	Fuel Server 3	Starter Pump	41.00
☑	10.6.0.2	Fuel Server 2	Starter Pump	62.00
☑	10.6.0.2	Fuel Server 2	Core Pump	42.50
☑	10.6.0.1	Fuel Server 1	Starter Pump	50.00
□	10.6.0.1	Fuel Server 1	Core Pump	49.50

To configure a rule

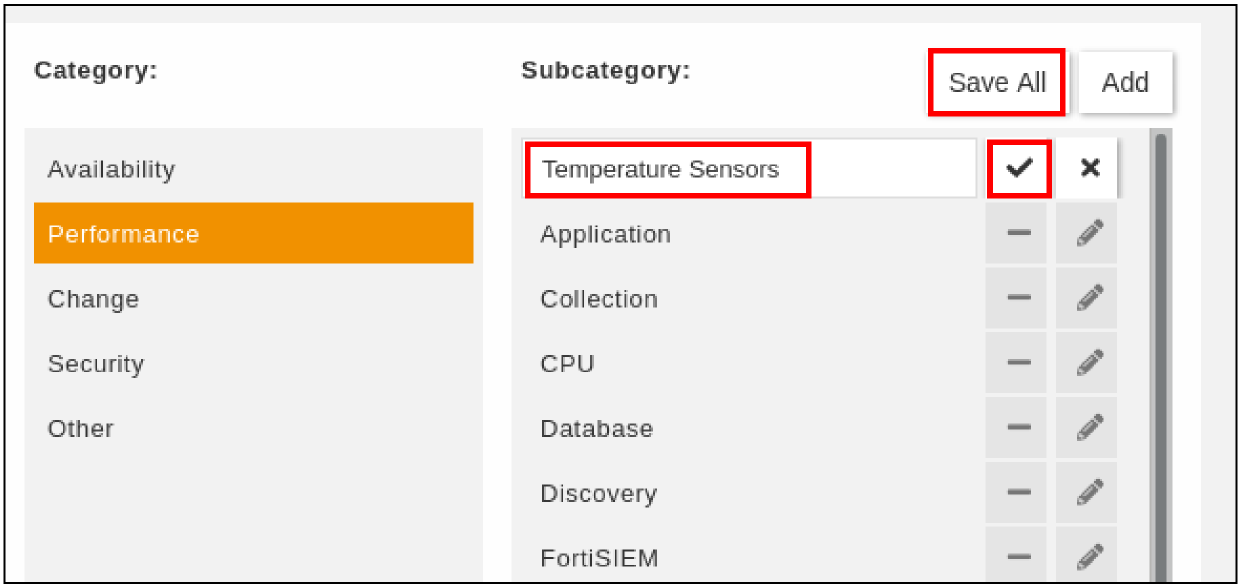
1. On the FortiSIEM GUI, click the **ADMIN** tab, click **Settings**, and then in the **Analytics** section, click **Subcategory**.



2. In the left pane, under **Category**, select **Performance**, and then in the **Subcategory** section, click **Add**.

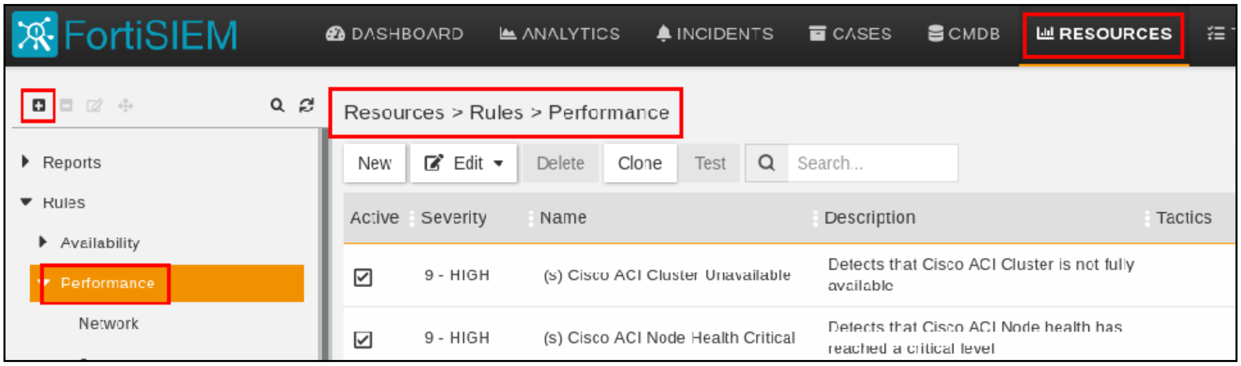


3. In the new empty entry box, type `Temperature Sensors`, click the check mark icon, and then click **Save All**.



If an empty entry is created above, click **X** to delete it.

4. Click the **RESOURCES** tab, and in the left pane, open the **Rules** tree, and then click **Performance**.

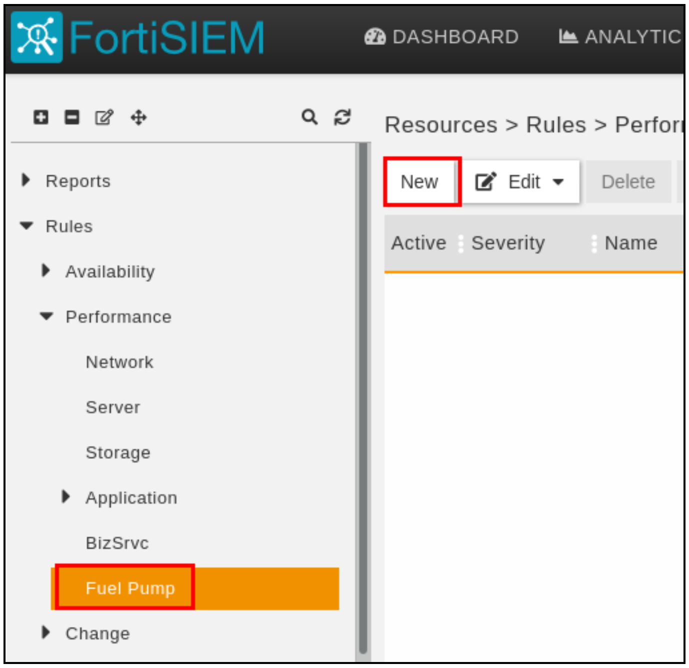


Resources > Rules > Performance

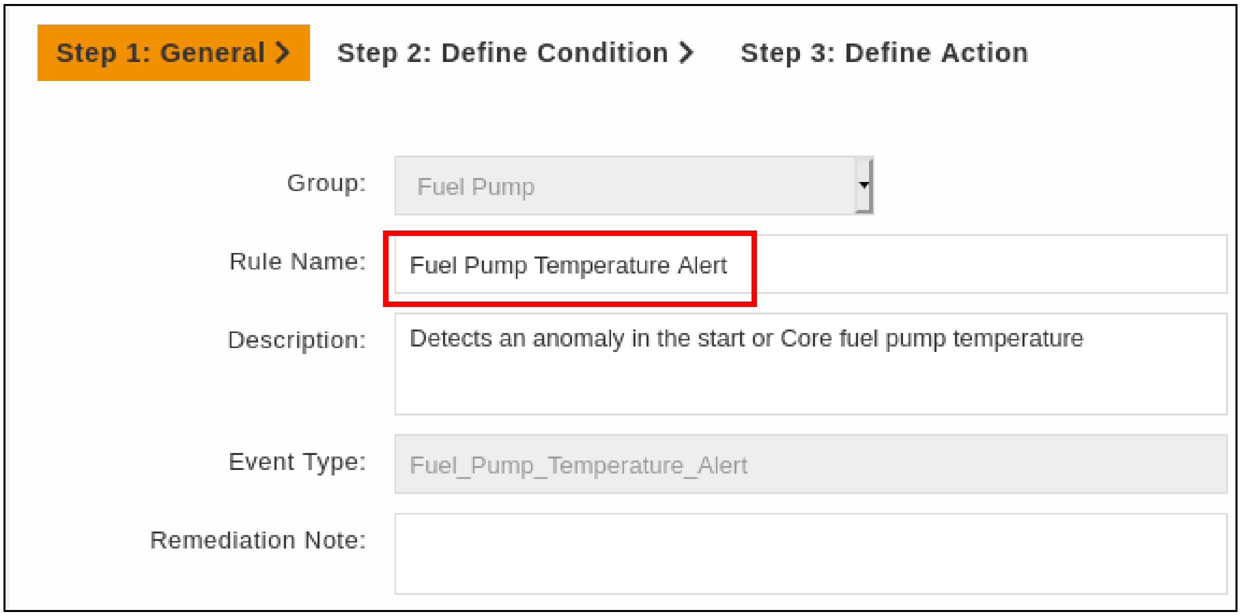
Active	Severity	Name	Description	Tactics
☑	9 - HIGH	(s) Cisco ACI Cluster Unavailable	Detects that Cisco ACI Cluster is not fully available	
☑	9 - HIGH	(s) Cisco ACI Node Health Critical	Detects that Cisco ACI Node health has reached a critical level	

5. Click **+** at the top of the tree to create a new folder, in the **Group** field, type `Fuel Pump`, and then click **Save**.

6. Select the new **Fuel Pump** subgroup, and then click **New** to create a new rule.



7. Under **Step 1: General**, in the **Rule Name** field, type `Fuel Pump Temperature Alert`, and then if you want, type a description.



Group: Fuel Pump

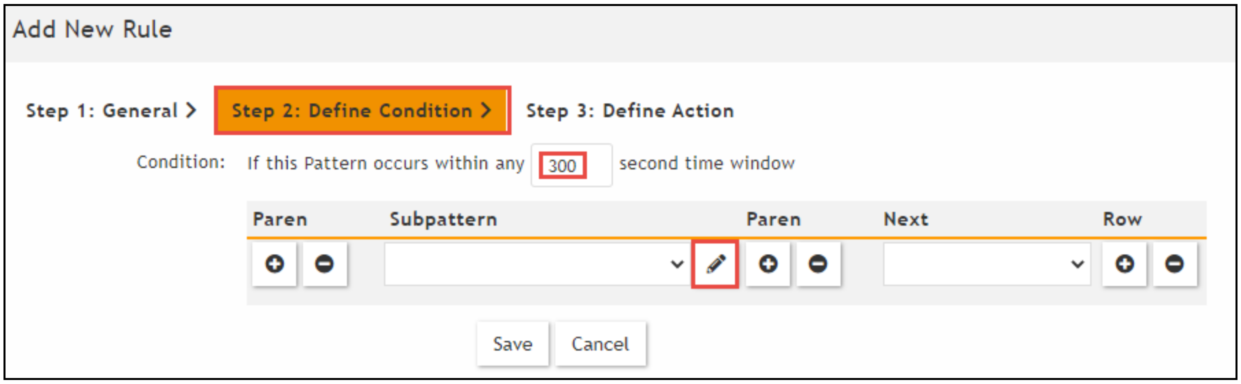
Rule Name: Fuel Pump Temperature Alert

Description: Detects an anomaly in the start or Core fuel pump temperature

Event Type: Fuel_Pump_Temperature_Alert

Remediation Note:

8. Click **Step 2: Define Condition**, and then leave the default time interval at 300 seconds (5 minutes).



Add New Rule

Step 1: General > **Step 2: Define Condition >** Step 3: Define Action

Condition: If this Pattern occurs within any 300 second time window

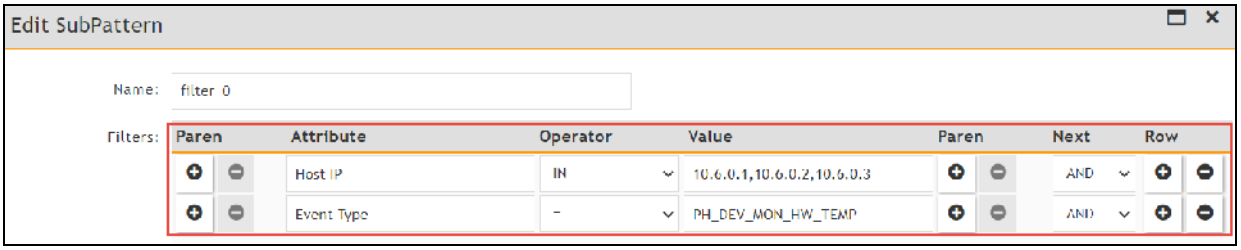
Paren	Subpattern	Paren	Next	Row
⊕ ⊖		⊕ ⊖		⊕ ⊖

9. Click the pencil icon, and then in the **Subpattern** field, create the following **Filters**:

Field	Value
Attribute	Host IP
Operator	IN
Value	10.6.0.1,10.6.0.2,10.6.0.3
NEXT	AND

10. In the **Row** column associated with the condition, click **+** to add another row.
11. In the second condition row, configure the following settings:

Field	Value
Attribute	Event Type
Operator	=
Value	PH_DEV_MON_HW_TEMP



Edit SubPattern

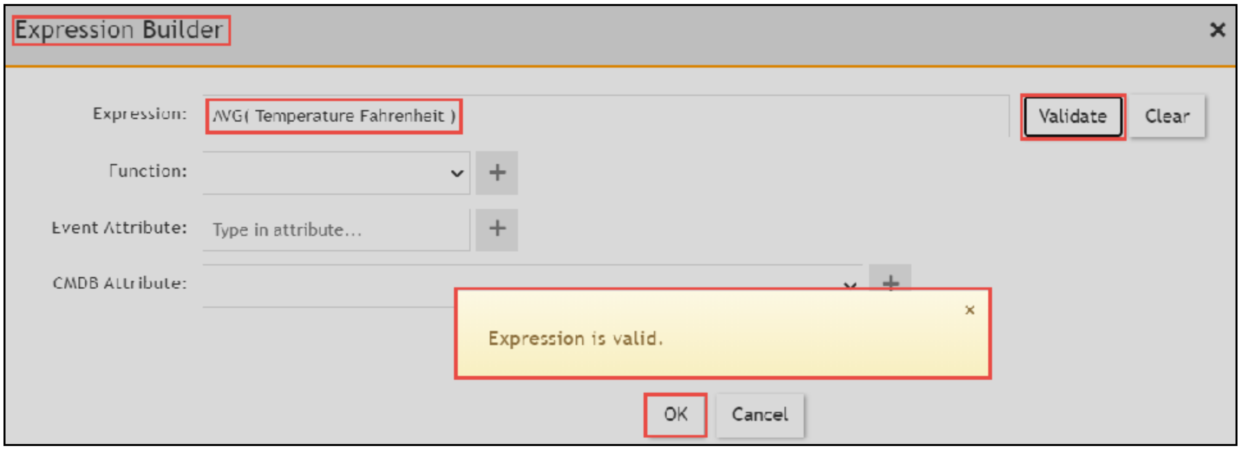
Name: filter 0

Filters:

Paren	Attribute	Operator	Value	Paren	Next	Row
⊕ ⊖	Host IP	IN	10.6.0.1,10.6.0.2,10.6.0.3	⊕ ⊖	AND	⊕ ⊖
⊕ ⊖	Event Type	-	PH_DEV_MON_HW_TEMP	⊕ ⊖	AND	⊕ ⊖

12. For the **Aggregate** condition, use the **Expression Builder** in the **Attribute** section.
13. In the **Function** drop-down list, select **AVG**, and then click **+**.
14. In the **Event Attribute** field, type `Temperature`, select **Temperature Fahrenheit**, click **+**, and then click **Validate**.

    An **Expression is valid** message appears.



Expression: AVG(Temperature Fahrenheit)

Function:

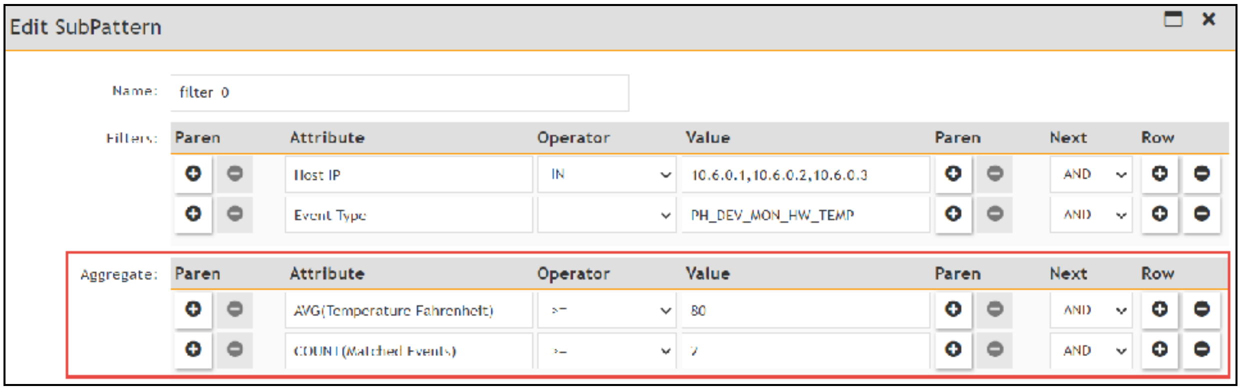
Event Attribute: Type in attribute...

CMDB Attribute:

Expression is valid.

15. Close the message, and then click **OK**.
16. In the **Operator** field, select **>=**, and then type a value of `80` to complete the first row.
17. Add a second row to the **Aggregate** condition.
18. Use the **Expression Builder** with the following settings:

Field	Value
Attribute	COUNT(Matched Events)
Operator	>=
Value	2



Name: filter 0

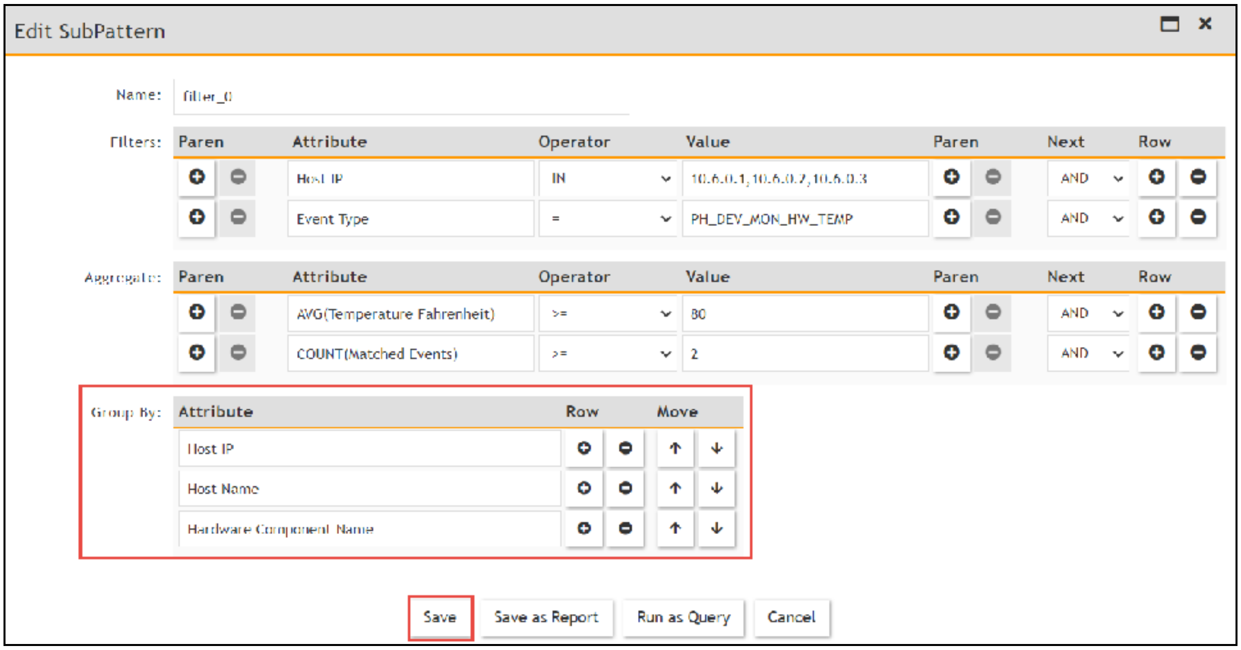
Filters:

Paren		Attribute	Operator	Value	Paren		Next	Row	
⊕	⊖	Host IP	IN	10.6.0.1,10.6.0.2,10.6.0.3	⊕	⊖	AND	⊕	⊖
⊕	⊖	Event Type		PH_DEV_MON_HW_TEMP	⊕	⊖	AND	⊕	⊖

Aggregate:

Paren		Attribute	Operator	Value	Paren		Next	Row	
⊕	⊖	AVG(Temperature Fahrenheit)	>=	80	⊕	⊖	AND	⊕	⊖
⊕	⊖	COUNT(Matched Events)	>=	2	⊕	⊖	AND	⊕	⊖

19. In the **Group By** section, add the **Host IP**, **Host Name**, and **Hardware Component Name** attributes, and then click **Save**.



Edit SubPattern

Name: filter_0

Filters:

Paren	Attribute	Operator	Value	Paren	Next	Row
	Host IP	IN	10.6.0.1,10.6.0.2,10.6.0.3		AND	
	Event Type	=	PH_DEV_MON_HW_TEMP		AND	

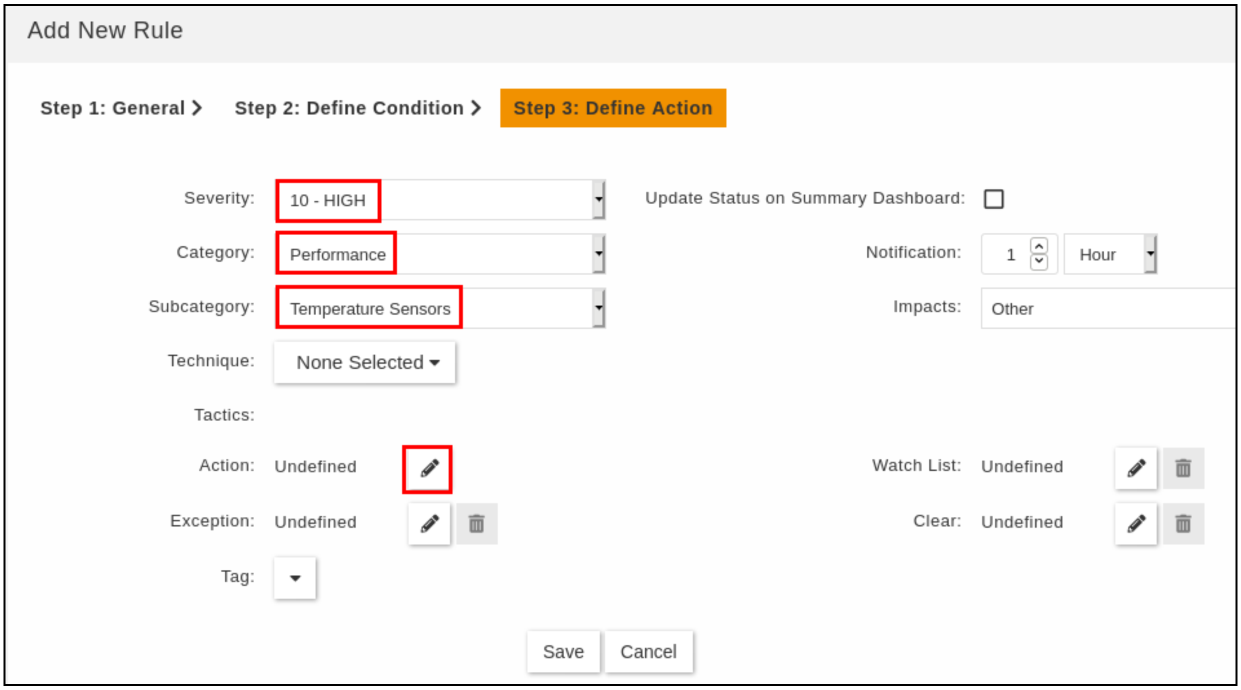
Aggregate:

Paren	Attribute	Operator	Value	Paren	Next	Row
	AVG(Temperature Fahrenheit)	>=	80		AND	
	COUNT(Matched Events)	>=	2		AND	

Group By:

Attribute	Row	Move
Host IP		
Host Name		
Hardware Component Name		

20. Click **Step 3: Define Action**, set **Severity** to **10-HIGH**, **Category** to **Performance**, and **Subcategory** to **Temperature Sensors**.



Add New Rule

Severity: 10 - HIGH

Update Status on Summary Dashboard: □

Category: Performance

Notification: 1 Hour

Subcategory: Temperature Sensors

Impacts: Other

Technique: None Selected

Tactics:

Action: Undefined

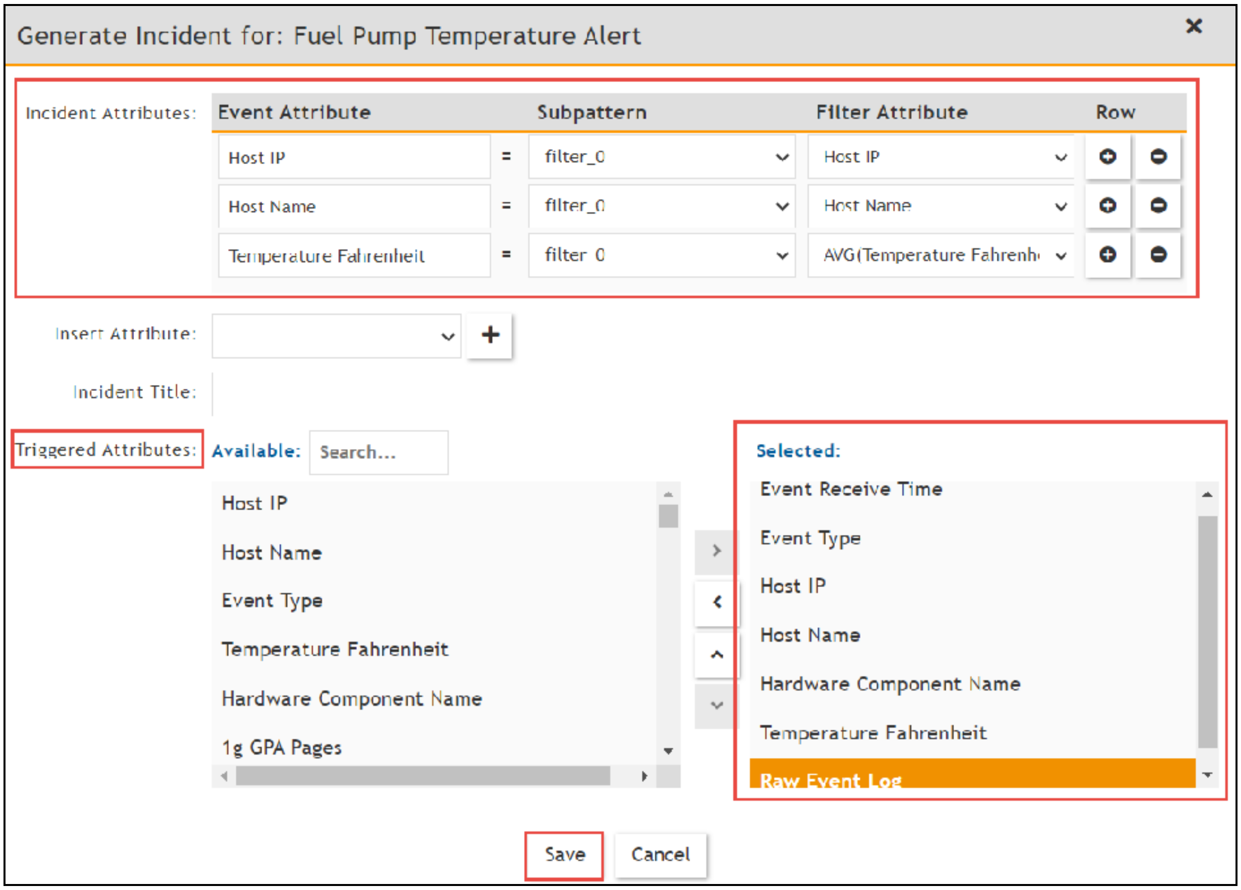
Watch List: Undefined

Exception: Undefined

Clear: Undefined

Tag:

21. In the **Action: Undefined** section, click the pencil icon, complete the **Incident** and **Triggered Attributes** as shown in the following image, and then click **Save**:



Generate Incident for: Fuel Pump Temperature Alert

Incident Attributes:

Event Attribute		Subpattern	Filter Attribute	Row
Host IP	=	filter_0	Host IP	⊕ ⊖
Host Name	=	filter_0	Host Name	⊕ ⊖
Temperature Fahrenheit	=	filter_0	AVG(Temperature Fahrenh	⊕ ⊖

Insert Attribute:

Incident Title:

Triggered Attributes: Available: Search...

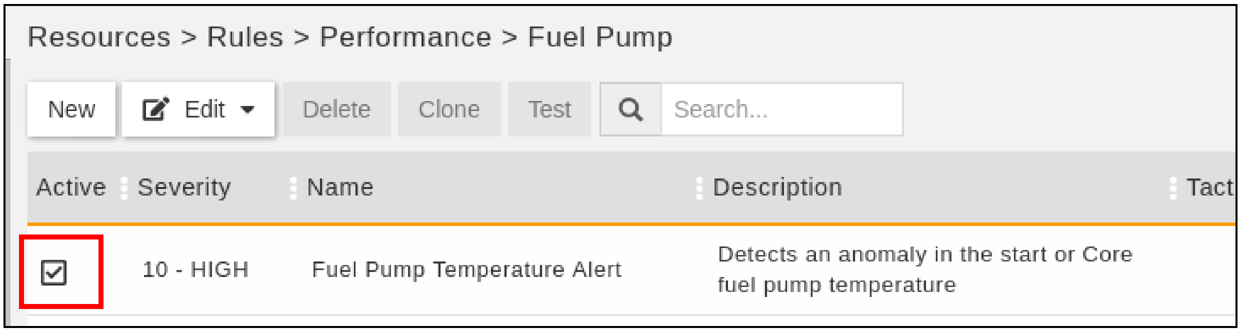
Host IP
Host Name
Event Type
Temperature Fahrenheit
Hardware Component Name
1g GPA Pages

Selected:

Event Receive Time
Event Type
Host IP
Host Name
Hardware Component Name
Temperature Fahrenheit
Raw Event Log

22. Click **Save** to save the rule.

23. Click the **Active** checkbox to enable the rule, and then in the activation window, click **Continue**.

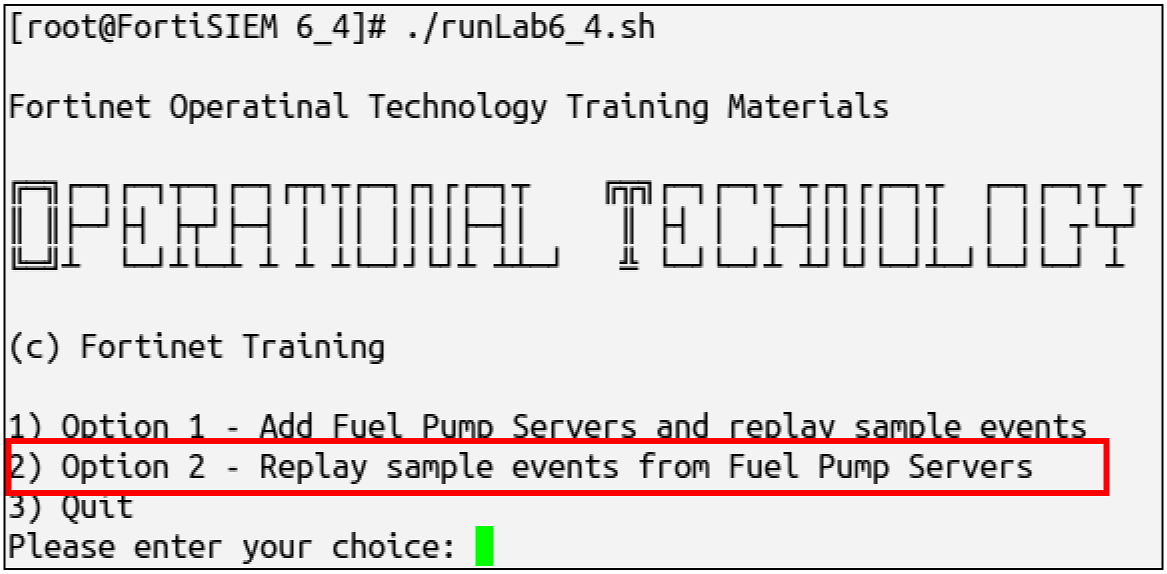


Resources > Rules > Performance > Fuel Pump

Active	Severity	Name	Description	Tact
☑	10 - HIGH	Fuel Pump Temperature Alert	Detects an anomaly in the start or Core fuel pump temperature	

To generate logs to test the rule

1. On the FortiSIEM CLI, enter 2 for **Option 2** to replay new events.



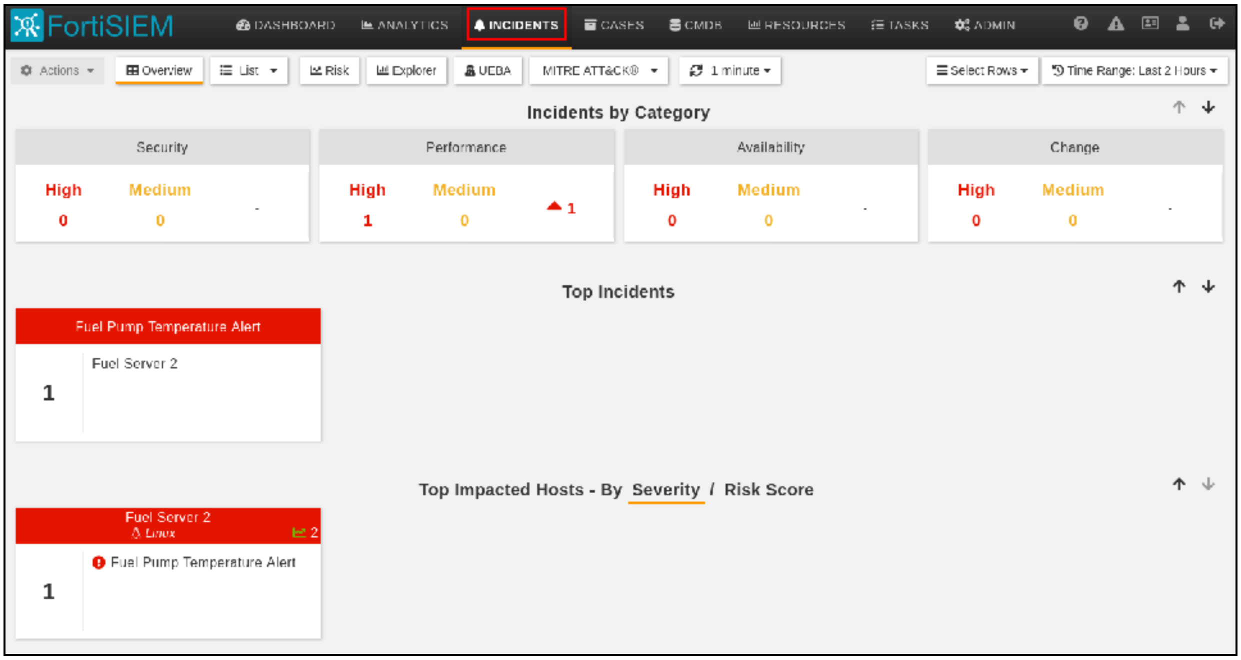
```
[root@FortiSIEM 6_4]# ./runLab6_4.sh

Fortinet Operatinal Technology Training Materials

OPERATIONAL TECHNOLOGY

(c) Fortinet Training

1) Option 1 - Add Fuel Pump Servers and replay sample events
2) Option 2 - Replay sample events from Fuel Pump Servers
3) Quit
Please enter your choice:
```

If the Lab 6.4 tool is not open, launch it again.

2. Wait for the **Simulation - All Done!** message (in approximately 3 minutes), and then enter 3 to **Quit** the script.

To view the incident triggered by the rule

1. On the FortiSIEM GUI, select the **INCIDENTS** tab to see if your new rule triggered an incident.



Incidents by Category

Security		Performance			Availability		Change	
High	Medium	High	Medium		High	Medium	High	Medium
0	0	1	0	▲ 1	0	0	0	0

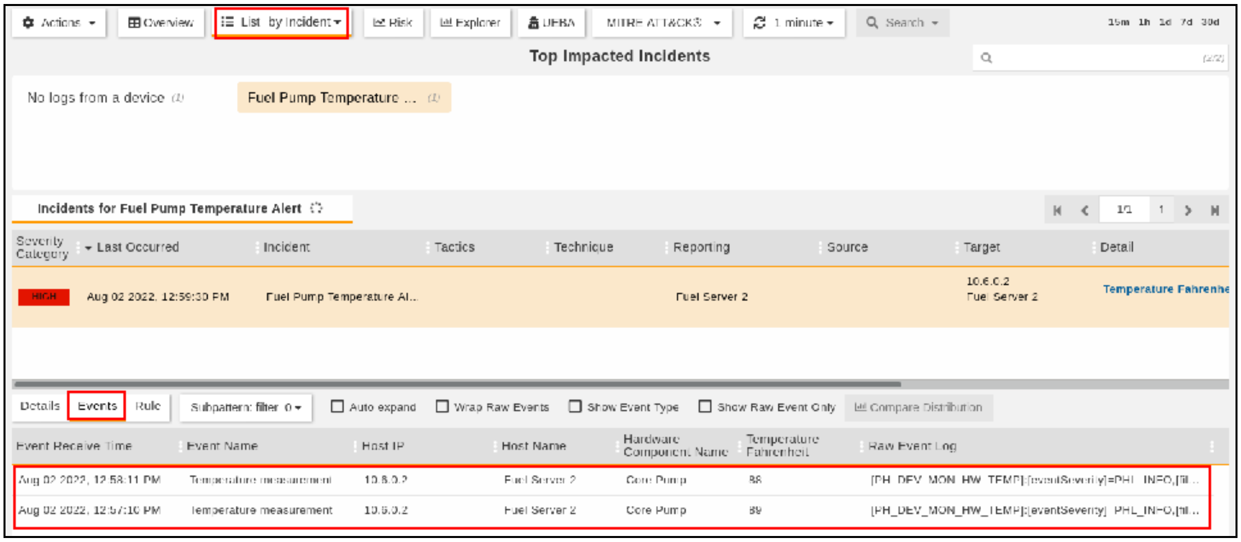
Top Incidents

Fuel Pump Temperature Alert
1 Fuel Server 2

Top Impacted Hosts - By Severity / Risk Score

Fuel Server 2
Linux 2
1 Fuel Pump Temperature Alert

2. Select **List by Incident** to view the **Events** that triggered the incident.



Incidents for Fuel Pump Temperature Alert

Severity Category	Last Occurred	Incident	Tactics	Technique	Reporting	Source	Target	Detail
HIGH	Aug 02 2022, 12:59:30 PM	Fuel Pump Temperature Al...			Fuel Server 2		10.6.0.2 Fuel Server 2	Temperature Fahrenhe

□ Auto expand □ Wrap Raw Events □ Show Event Type □ Show Raw Event Only

Event Receive Time	Event Name	Host IP	Host Name	Hardware Component Name	Temperature Fahrenheit	Raw Event Log
Aug 02 2022, 12:58:11 PM	Temperature measurement	10.6.0.2	Fuel Server 2	Core Pump	88	[PH_DEV_MON_HW_TEMP]:[eventSeverity]=PHL_INFO,[fil...
Aug 02 2022, 12:57:10 PM	Temperature measurement	10.6.0.2	Fuel Server 2	Core Pump	89	[PH_DEV_MON_HW_TEMP]:[eventSeverity]=PHL_INFO,[fil...

Review the incident (there should be an incident for Fuel Server 2 only) and notice the incident **Target** and **Details**, and then click the **Events** tab to view the individual events that triggered the rule.

Lab 7: Risk Assessment

In this lab, you will generate a default report, build a chart based on a log search, and perform some diagnostic checks on FortiAnalyzer. You will also create reports and dashboards for operational technology (OT) security on FortiSIEM.

Objectives

- Generate a default report on FortiAnalyzer
- Run report diagnostics on FortiAnalyzer
- Build a chart-based report on a log search on FortiAnalyzer
- Execute default reports on FortiSIEM
- Create reports on FortiSIEM from analytics
- Create an OT dashboard on FortiSIEM

Time to Complete

Estimated: 75 minutes

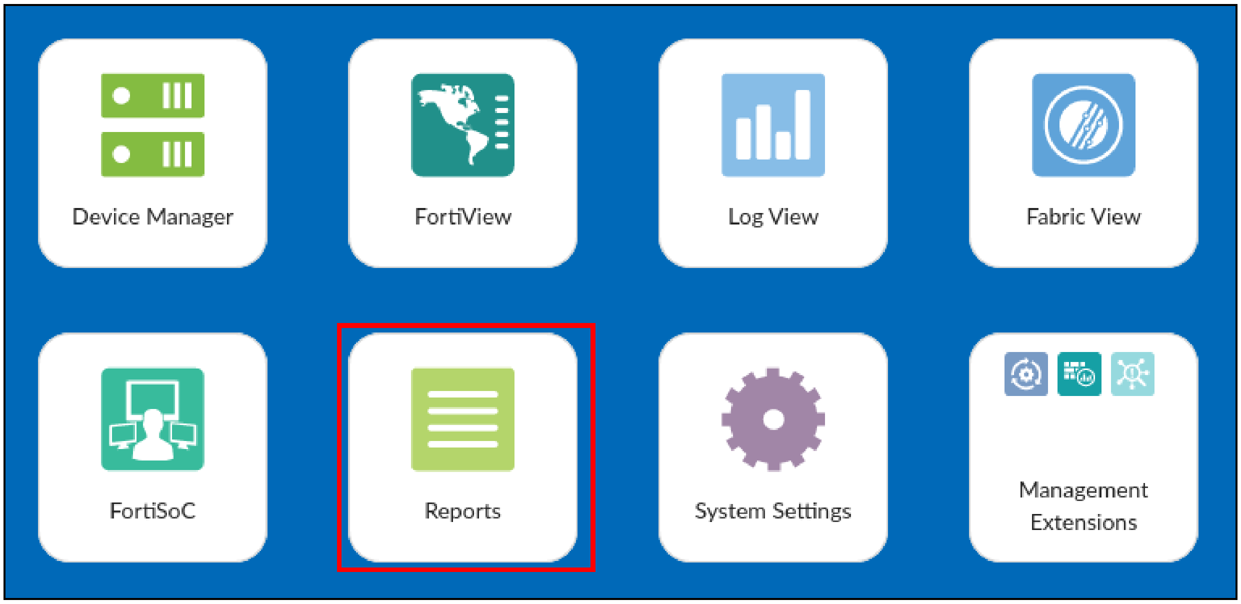
Prerequisites

Before you begin this lab, you must complete the previous lab. If you haven't done so, tell your instructor.

Follow the directions in the lab guide and do not make changes to any other devices unless the course instructor tells you to.

Exercise 1: Running a Default Report

In this exercise, you will run one of the default reports on demand. This will allow you to see the report immediately. You will also run diagnostics for this report.

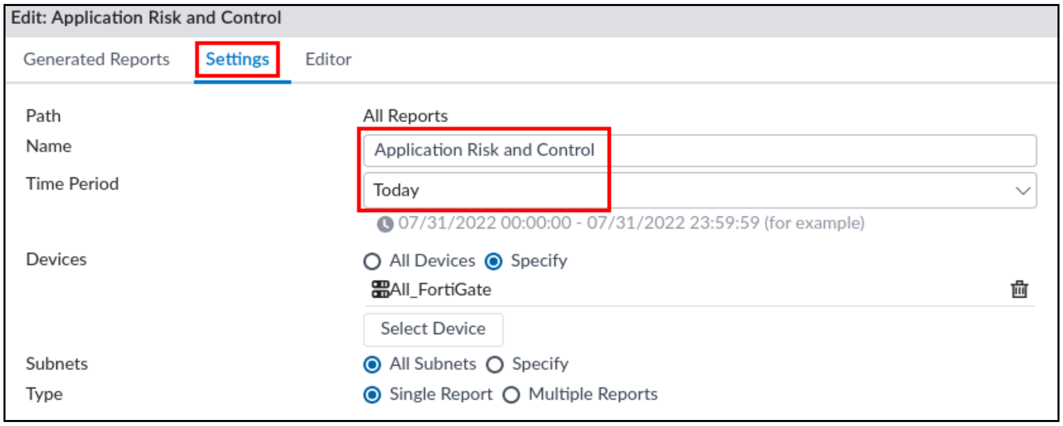


Because of simulated traffic limitations in this lab, not all report fields are populated.

To generate a default report

1. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. Click **Reports**.
3. Click **Report Definitions** > **All Reports**.

   This page provides all available default reports.
4. Double-click the **Application Risk and Control** report.
5. Click the **Settings** tab, and then in the **Time Period** field, select **Today**.

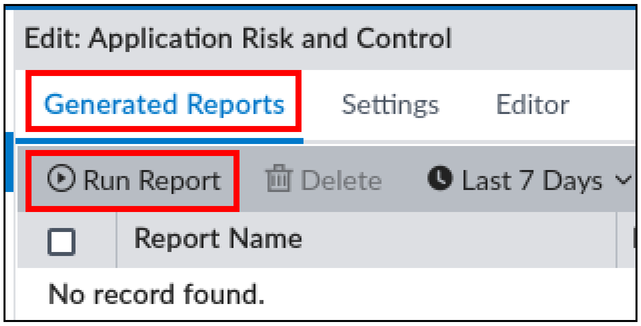


Edit: Application Risk and Control

Path	All Reports
Name	Application Risk and Control
Time Period	Today
	07/31/2022 00:00:00 - 07/31/2022 23:59:59 (for example)
Devices	○ All Devices ● Specify
	All_FortiGate
	Select Device
Subnets	● All Subnets ○ Specify
Type	● Single Report ○ Multiple Reports

Ensure your time filter is set correctly (includes the time you have been generating traffic).

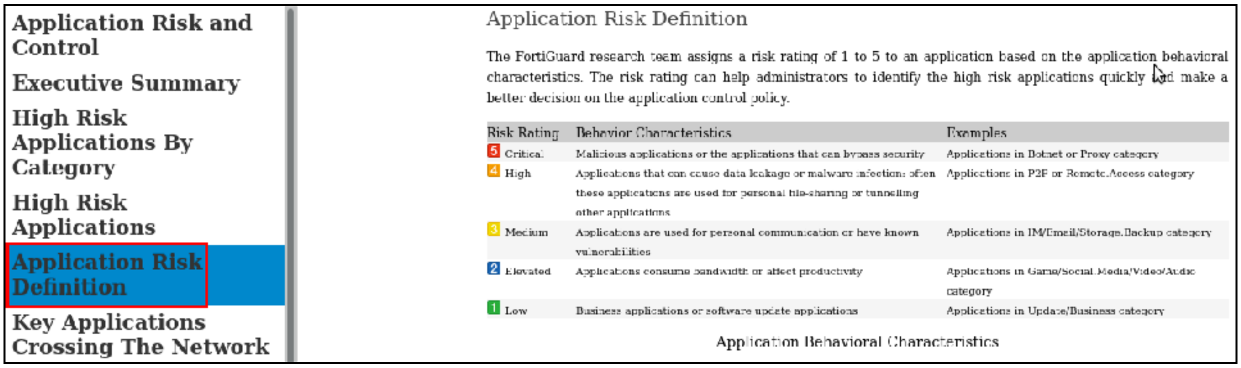
6. Click **Apply**.
7. Click the **Generated Reports** tab, and then click **Run Report** to run the report on demand.



Edit: Application Risk and Control

No record found.

8. When the report is ready, view the report in **HTML** format.
9. Scroll down, click **Application Risk Definition**, and then review the **Risk Rating** for applications.



Application Risk and Control
Executive Summary
High Risk Applications By Category
High Risk Applications
Application Risk Definition
Key Applications Crossing The Network

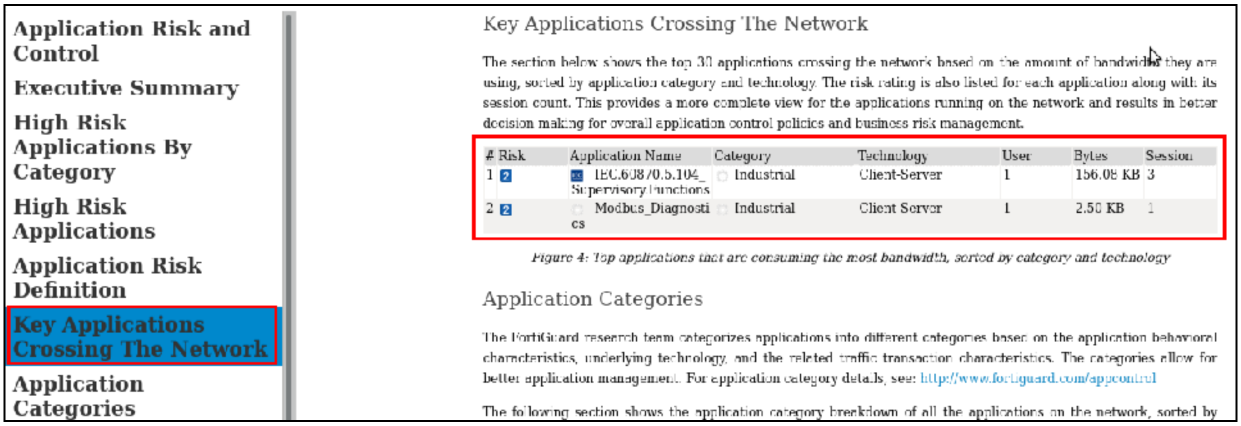
Application Risk Definition

The FortiGuard research team assigns a risk rating of 1 to 5 to an application based on the application behavioral characteristics. The risk rating can help administrators to identify the high risk applications quickly and make a better decision on the application control policy.

Risk Rating	Behavior Characteristics	Examples
5 Critical	Malicious applications or the applications that can bypass security	Applications in Botnet or Proxy category
4 High	Applications that can cause data leakage or malware infection: often these applications are used for personal file-sharing or tunnelling other applications	Applications in P2P or Remote.Access category
3 Medium	Applications are used for personal communication or have known vulnerabilities	Applications in IM/Email/Storage.Backup category
2 Elevated	Applications consume bandwidth or affect productivity	Applications in Game/Social.Media/Video/Audio category
1 Low	Business applications or software update applications	Applications in Update/Business category

Application Behavioral Characteristics

10. Scroll down, and then click **Key Applications Crossing The Network**.



Application Risk and Control
Executive Summary
High Risk Applications By Category
High Risk Applications
Application Risk Definition
Key Applications Crossing The Network
Application Categories

Key Applications Crossing The Network

The section below shows the top 30 applications crossing the network based on the amount of bandwidth they are using, sorted by application category and technology. The risk rating is also listed for each application along with its session count. This provides a more complete view for the applications running on the network and results in better decision making for overall application control policies and business risk management.

#	Risk	Application Name	Category	Technology	User	Bytes	Session
1	2	IEC.60870.5.104_Supervisory.Functions	Industrial	Client-Server	1	156.08 KB	3
2	2	Modbus_Diagnostics	Industrial	Client Server	1	2.50 KB	1

Figure 4: Top applications that are consuming the most bandwidth, sorted by category and technology

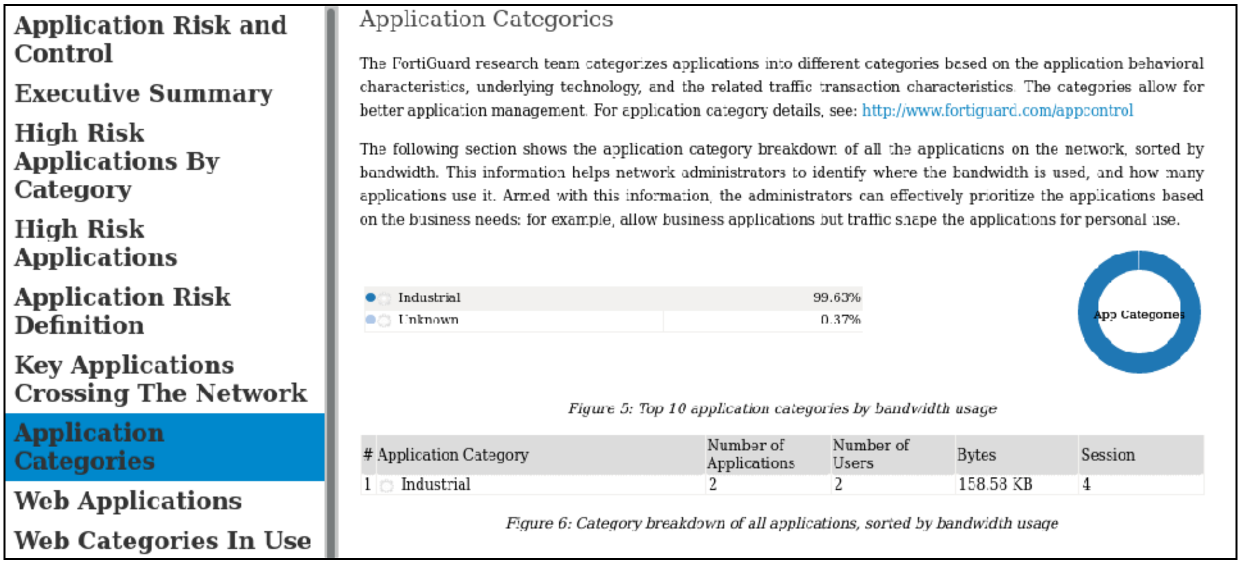
Application Categories

The FortiGuard research team categorizes applications into different categories based on the application behavioral characteristics, underlying technology, and the related traffic transaction characteristics. The categories allow for better application management. For application category details, see: http://www.fortiguard.com/appcontrol

The following section shows the application category breakdown of all the applications on the network, sorted by

The report shows key industrial applications going through your network.

11. Click **Application Categories**.



Application Risk and Control
Executive Summary
High Risk Applications By Category
High Risk Applications
Application Risk Definition
Key Applications Crossing The Network
Application Categories
Web Applications
Web Categories In Use

Application Categories

The FortiGuard research team categorizes applications into different categories based on the application behavioral characteristics, underlying technology, and the related traffic transaction characteristics. The categories allow for better application management. For application category details, see: http://www.fortiguard.com/appcontrol

The following section shows the application category breakdown of all the applications on the network, sorted by bandwidth. This information helps network administrators to identify where the bandwidth is used, and how many applications use it. Armed with this information, the administrators can effectively prioritize the applications based on the business needs: for example, allow business applications but traffic shape the applications for personal use.

● Industrial	99.63%
● Unknown	0.37%

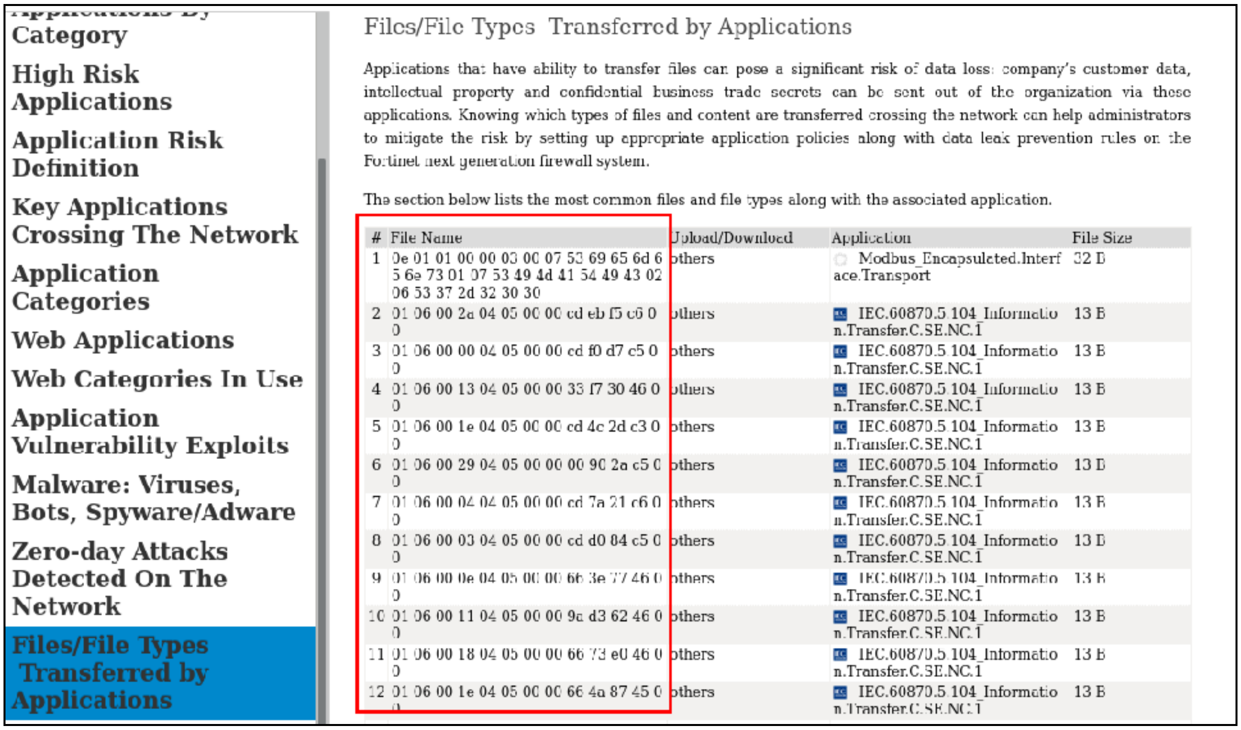
Figure 5: Top 10 application categories by bandwidth usage

#	Application Category	Number of Applications	Number of Users	Bytes	Session
1	Industrial	2	2	158.58 KB	4

Figure 6: Category breakdown of all applications, sorted by bandwidth usage

You can view the latest available applications in the industrial category by clicking the http://fortiguard.com/appcontrol link.

12. Scroll down, click **Files/File Types Transferred by Applications**, and then review the contents of the **File Name** column to see the industrial application data.


Applications By
Category
High Risk Applications
Application Risk Definition
Key Applications Crossing The Network
Application Categories
Web Applications
Web Categories In Use
Application Vulnerability Exploits
Malware: Viruses, Bots, Spyware/Adware
Zero-day Attacks Detected On The Network
Files/File Types Transferred by Applications

Files/File Types Transferred by Applications

Applications that have ability to transfer files can pose a significant risk of data loss: company's customer data, intellectual property and confidential business trade secrets can be sent out of the organization via these applications. Knowing which types of files and content are transferred crossing the network can help administrators to mitigate the risk by setting up appropriate application policies along with data leak prevention rules on the Fortinet next generation firewall system.

The section below lists the most common files and file types along with the associated application.

#	File Name	Upload/Download	Application	File Size
1	0e 01 01 00 00 03 00 07 53 69 65 6d 65 6e 73 01 07 53 49 4d 41 54 49 43 02 06 53 37 2d 32 30 30	others	Modbus_Encapsulated.Interface.Transport	32 B
2	01 06 00 2a 04 05 00 00 cd eb f5 c6 00	others	IEC.60870.5.104_Information.Transfer.C.SE.NC.1	13 B
3	01 06 00 00 04 05 00 00 cd f0 d7 c5 00	others	IEC.60870.5.104_Information.Transfer.C.SE.NC.1	13 B
4	01 06 00 13 04 05 00 00 33 f7 30 46 00	others	IEC.60870.5.104_Information.Transfer.C.SE.NC.1	13 B
5	01 06 00 1e 04 05 00 00 cd 4c 2d c3 00	others	IEC.60870.5.104_Information.Transfer.C.SE.NC.1	13 B
6	01 06 00 29 04 05 00 00 00 90 2a c5 00	others	IEC.60870.5.104_Information.Transfer.C.SE.NC.1	13 B
7	01 06 00 04 04 05 00 00 cd 7a 21 c6 00	others	IEC.60870.5.104_Information.Transfer.C.SE.NC.1	13 B
8	01 06 00 03 04 05 00 00 cd d0 84 c5 00	others	IEC.60870.5.104_Information.Transfer.C.SE.NC.1	13 B
9	01 06 00 0e 04 05 00 00 66 3e 77 46 00	others	IEC.60870.5.104_Information.Transfer.C.SE.NC.1	13 B
10	01 06 00 11 04 05 00 00 9a d3 62 46 00	others	IEC.60870.5.104_Information.Transfer.C.SE.NC.1	13 B
11	01 06 00 18 04 05 00 00 66 73 e0 46 00	others	IEC.60870.5.104_Information.Transfer.C.SE.NC.1	13 B
12	01 06 00 1e 04 05 00 00 66 4a 87 45 00	others	IEC.60870.5.104_Information.Transfer.C.SE.NC.1	13 B

To run diagnostics on a report

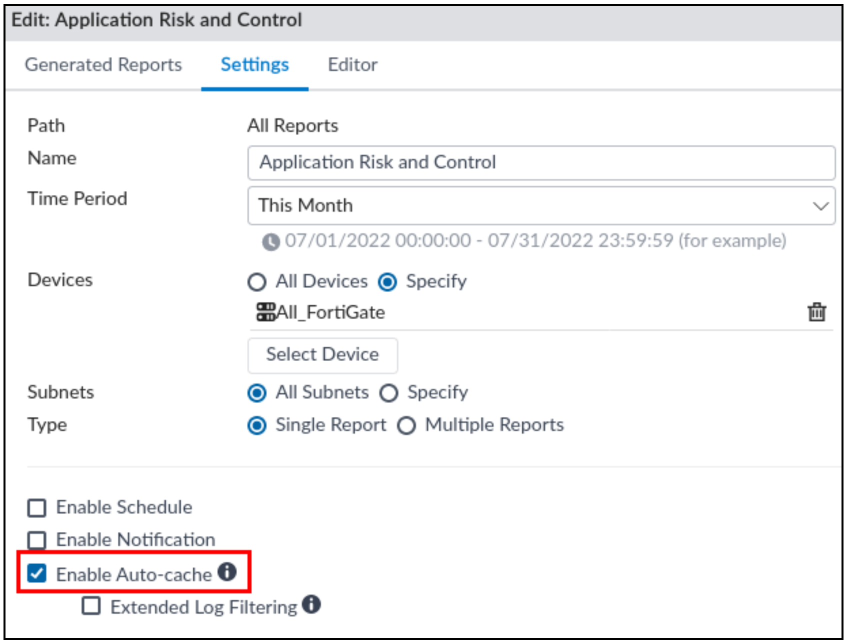
1. Return to the FortiAnalyzer GUI, right-click the report you just ran, and then select **Retrieve Diagnostic**.
2. Save the file to your downloads folder.
3. Open the `rpt_status.log` file in Notepad++.
4. Scroll down to the `Report Summary` section, and then record the following information:

HCACHE building time
Rendering time
Total time

For example:

```
HCACHE building time: 0.69s
Rendering time: 4.14s
Total time: 4.84s
```

5. Return to the FortiAnalyzer GUI, and then click **All Reports**.
6. Double-click the **Application Risk and Control** report.
7. Click the **Settings** tab, and then select the **Enable Auto-cache** checkbox.



Edit: Application Risk and Control

Path: All Reports
Name: Application Risk and Control
Time Period: This Month
07/01/2022 00:00:00 - 07/31/2022 23:59:59 (for example)
Devices: ○ All Devices ● Specify
All_FortiGate

Subnets: ● All Subnets ○ Specify
Type: ● Single Report ○ Multiple Reports

□ Enable Schedule
□ Enable Notification
☑ Enable Auto-cache
□ Extended Log Filtering

FortiAnalyzer updates the HCACHE when new logs come in and new log tables generate. If you do not enable auto-cache, the report generates the HCACHE for the current log tables only. Remember, you are currently generating traffic in your lab.

8. Click **Apply**.
9. Run the report again, and then run diagnostics again.

   What is the output this time?

HCACHE building time
Rendering time
Total time

For example:

```
HCACHE building time: 0.19s
Rendering time: 3.72s
Total time: 3.91s
```

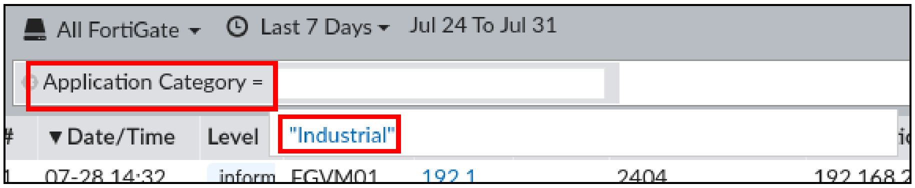
Although your lab environment does not have a large number of logs, you can still see that by enabling auto-cache, the report builds faster. This is more noticeable if you have higher log volumes.

Exercise 2: Building a Chart-Based Report on a Log Search

In this exercise, you will create a chart based on the industrial application category, add the chart to a report, and then run the report.

To create a chart based on a log search

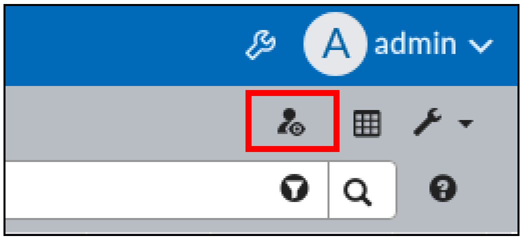
1. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. Click **Log View**.
3. Click **FortiGate** > **Security** > **Application Control**.
4. Click **Last 1 Hour**, and then in the drop-down list, select **Last 7 Days** to change the duration.
5. Click **Add Filter**, type `Application`, and then select **Application Category**.
6. Click **"Industrial"** as the filter value.



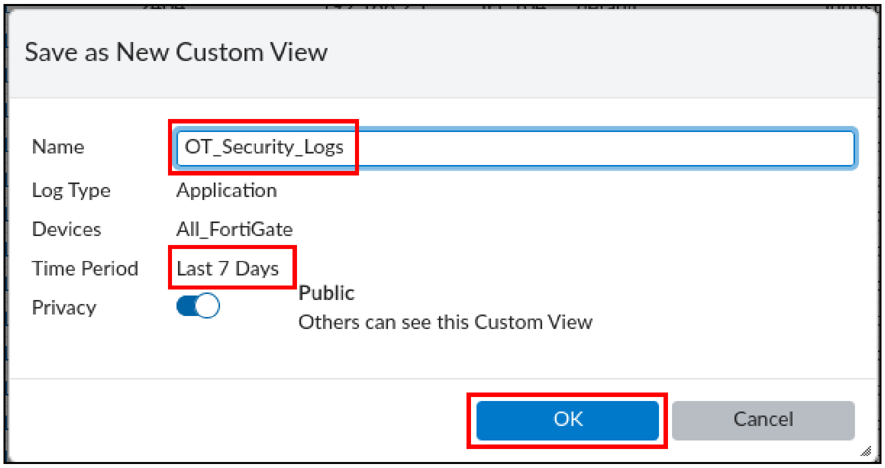
Ensure your time filter is set correctly (includes the time you have been generating traffic).

7. Click the custom view icon to save the current view as a custom view.

Although a custom view isn't required to build a chart, it's a nice feature that allows you to save your filtered searches. The custom view option is available only in the historical log view.

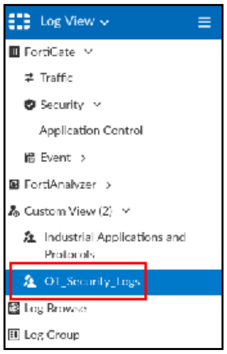


8. In the **Name** field, type `OT_Security_Logs`, and then click **OK**.



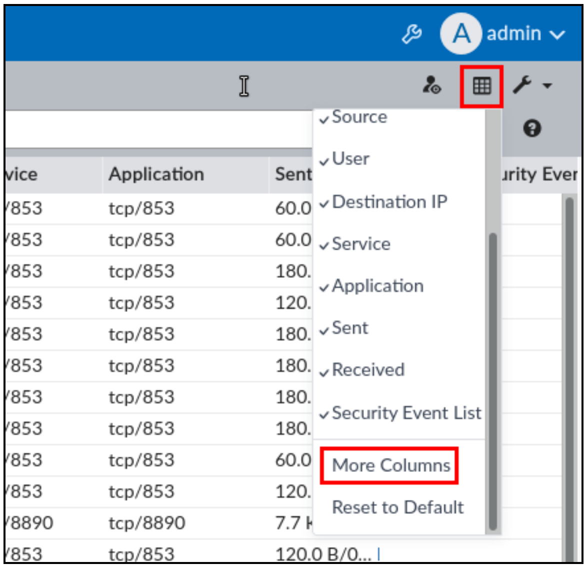
Save as New Custom View

Name	OT_Security_Logs
Log Type	Application
Devices	All_FortiGate
Time Period	Last 7 Days
Privacy	Public Others can see this Custom View



Ensure your time filter is set correctly (includes the time you have been generating traffic).

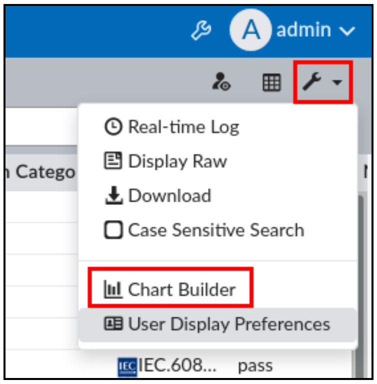
9. In your **OT_Security_Logs** custom view, click the custom view icon, and then click **More Columns**.



vice	Application	Sent	urity Ever
/853	tcp/853	60.0	
/853	tcp/853	60.0	
/853	tcp/853	180.	
/853	tcp/853	120.	
/853	tcp/853	180.	
/853	tcp/853	180.	
/853	tcp/853	180.	
/853	tcp/853	180.	
/853	tcp/853	60.0	
/853	tcp/853	120.	
/8890	tcp/8890	7.7 k	
/853	tcp/853	120.0 B/0...	

10. In **Column Settings**, select the **Application Risk** and **File Name** column names, and then click **OK**.
11. In your **OT_Security_Logs** custom view, click the tools icon, and then click **Chart Builder**.

Chart Builder is available only in the historical log view.



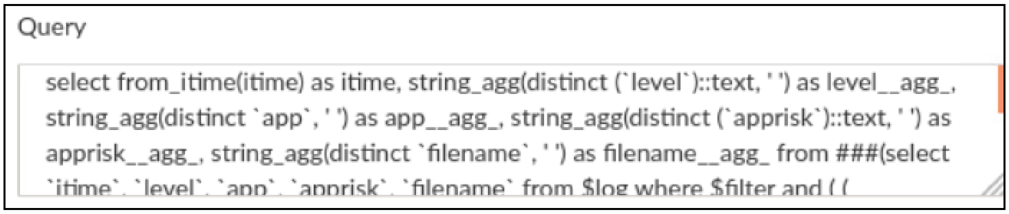
The dataset query is generated in advance based on your search filters. The **Preview** window indicates what the results will look like in a report.

12. Configure the following settings to fine-tune your results:

Field	Value
Name	OT_Security_Chart
Columns	Select: • Date/Time • Level • Application • Application Risk • File Name This setting allows you to select only five columns. If other columns are selected by default, deselect them.
Group By	Date/Time
Order By	Application
Show Limit	200

13. Click **Preview**.

The dataset query updates based on your modifications. Review the following example of a dataset query:



Query

```
select from_itime(itime) as itime, string_agg(distinct (`level`)::text, ' ') as level__agg_,
string_agg(distinct `app`, ' ') as app__agg_, string_agg(distinct (`apprisk`)::text, ' ') as
apprisk__agg_, string_agg(distinct `filename`, ' ') as filename__agg_ from ###(select
`itime`, `level`, `app`, `apprisk`, `filename` from $log where $filter and ((
```

14. View the preview, and then click **Save**.

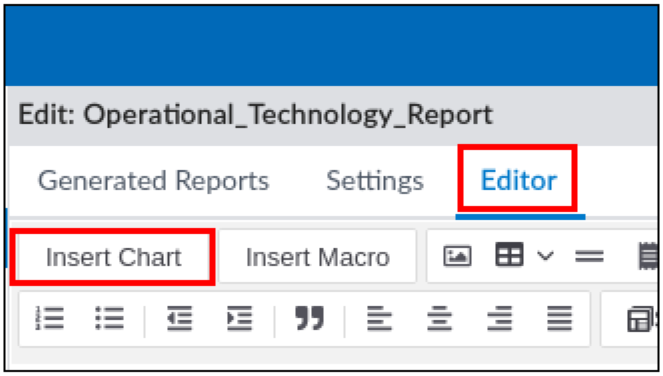
    Your dataset and chart are created.

To run a report on the custom chart

1. Continuing on the FortiAnalyzer GUI, click **Log View** > **Reports**.
2. Click **All Reports**, and then click **Report** > **Create New**.
3. Configure the following settings:

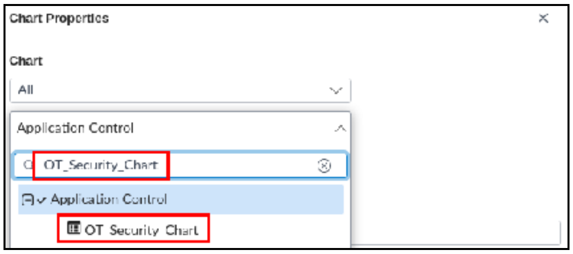
Field	Value
Name	Operational_Technology _Report
Create from	Blank

4. Click **OK**.
5. Click **Settings**.
6. In the **Time Period** field, select **Today**.
7. Click the **Editor** tab, and then click **Insert Chart**.



Edit: Operational_Technology_Report

8. Click the second **Chart** drop-down list, in the text field, start typing `OT_Security_Chart`, and then when it appears in the list, select it.



9. Click **OK**.
10. Click **Apply**.

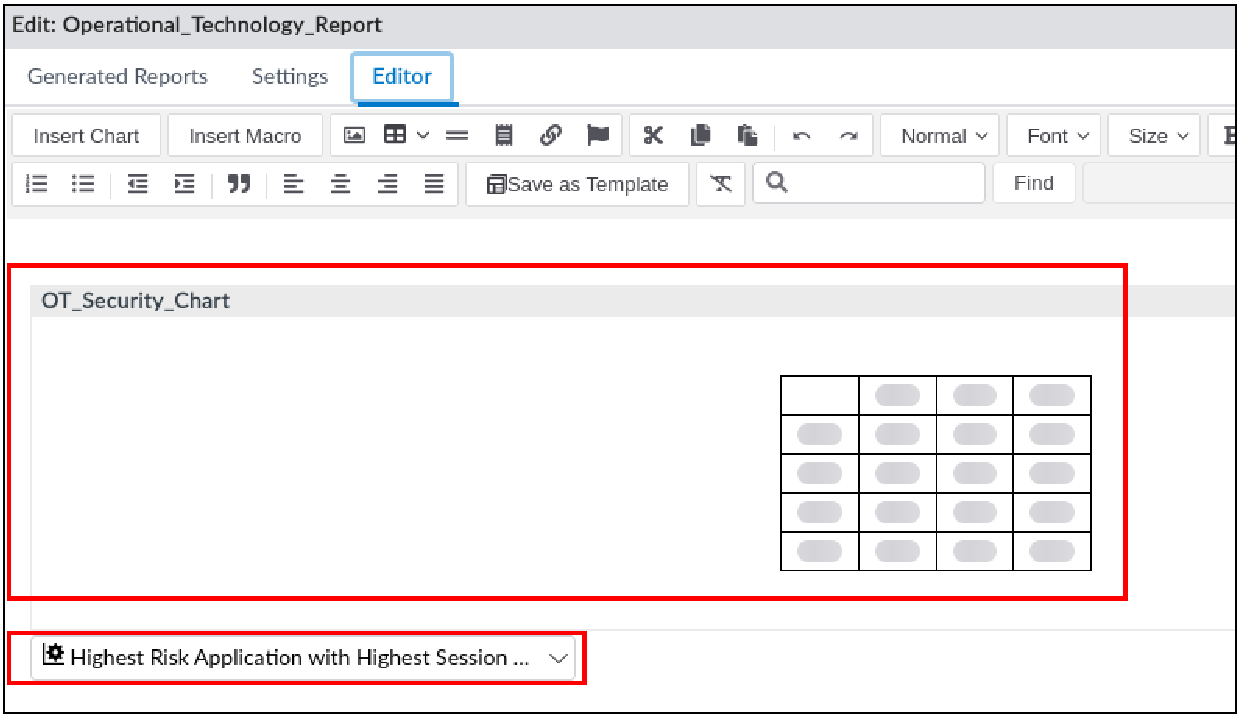
11. Optionally, try inserting one of the **Traffic** macros:

    a. Click to insert your cursor below the chart you just added to the layout.

    b. Click **Insert Macro**.

    c. In the inserted macro drop-down list, scroll up to the **Traffic** section, and then select any of the default macros. For example, you can select the **Highest Risk Application with Highest Session Count** macro.

    d. Click **Apply**.



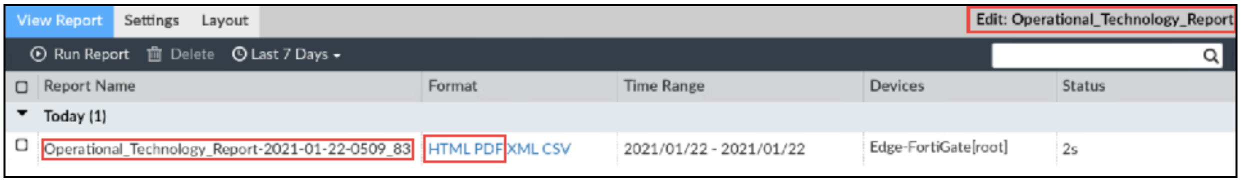
Edit: Operational_Technology_Report

OT_Security_Chart

Highest Risk Application with Highest Session ...

12. Click the **Generated Reports** tab, and then click **Run Report**.

13. In the **Format** column, click **HTML** or **PDF** to view the report.



□	Report Name	Format	Time Range	Devices	Status
▾	Today (1)				
□	Operational_Technology_Report-2021-01-22-0509_83	HTML PDF XML CSV	2021/01/22 - 2021/01/22	Edge-FortiGate[root]	2s

Operational_Technology_Report

Report Date: August 1, 2022 08:51

Data Range: 2022-08-01 00:00:00 2022-08-01 08:51:12PDT (FAZ local)

You successfully created a report based on a chart and dataset created from a filtered search result.

Exercise 3: Executing Default Reports on FortiSIEM

In this exercise, you will run one of the default reports on demand. You will explore the opening and running of reports from the report tree. You will explore a default report on all incidents. FortiSIEM is placed in Purdue level 3.5, and it will trigger incidents based on events for devices from level 0 to 5. The **All incidents** report provides an incident summary from all Purdue levels. You will also learn how to schedule a report on FortiSIEM.

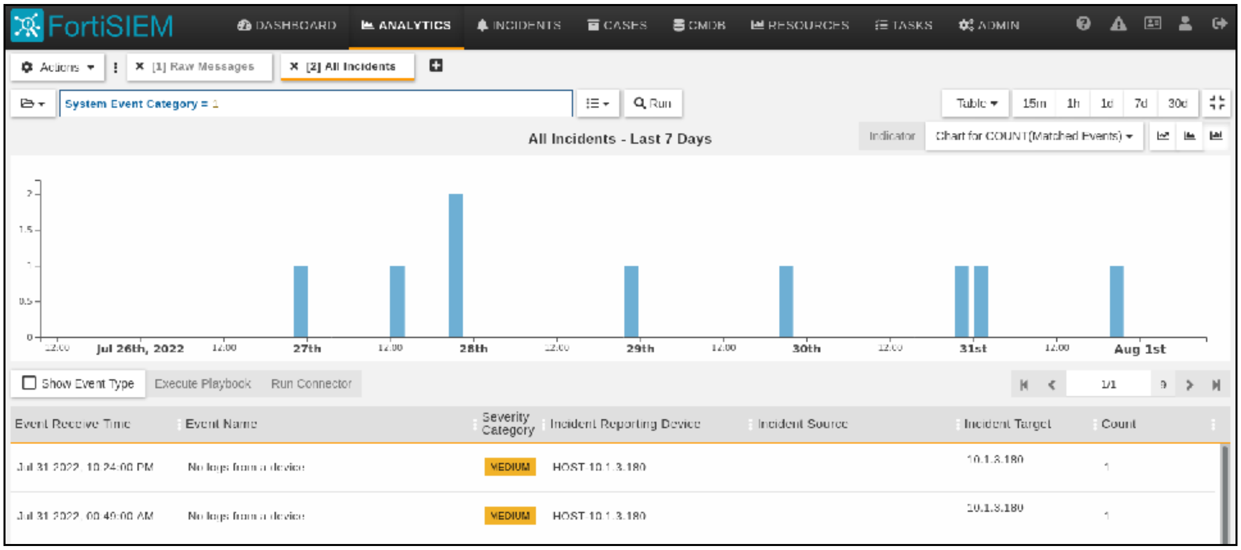
To run a report from the report tree

1. Log in to the FortiSIEM GUI, and then click the **RESOURCES** tab.
2. Click **Reports** > **Incidents**.
3. In the main window, select **All Incidents**.
4. Click **Run**.

   The **Run** window opens.

5. On the **Report Time Range** tab, select **Relative**, in the **Last** field, type `7`, and then in the drop-down list, select **Days**.
6. Click **OK**.

   The report automatically runs and populates the results in a new tab on the **ANALYTICS** tab.

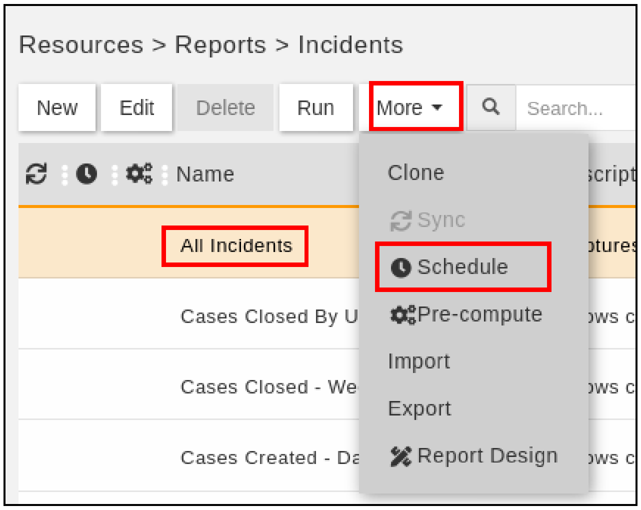


Event Receive Time	Event Name	Severity Category	Incident Reporting Device	Incident Source	Incident Target	Count
Jul 31 2022, 10:24:00 PM	No logs from a device	MEDIUM	HOST 10.1.3.180		10.1.3.180	1
Jul 31 2022, 00:49:00 AM	No logs from a device	MEDIUM	HOST 10.1.3.180		10.1.3.180	1

Review the results. Results may vary.

To schedule a report

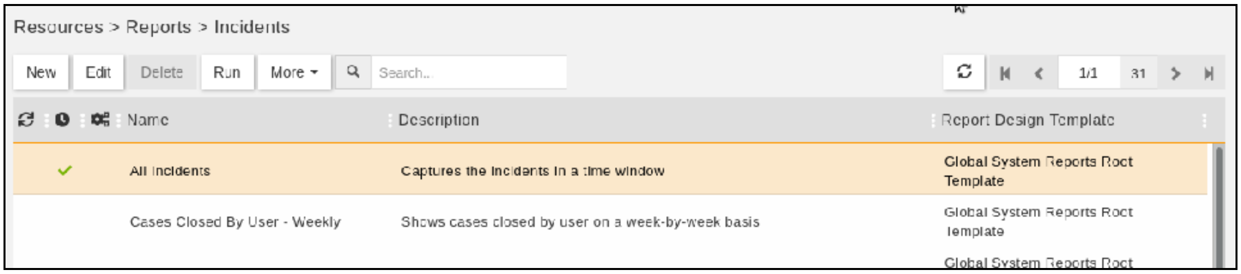
1. Click the **RESOURCES** tab.
2. Click **Reports** > **Incidents**.
3. Select **All Incidents**.
4. Click **More**.
5. In the **More** drop-down list, select **Schedule**.



6. Configure the following settings (you must click **Next** to view some of the settings), and then click **OK**:

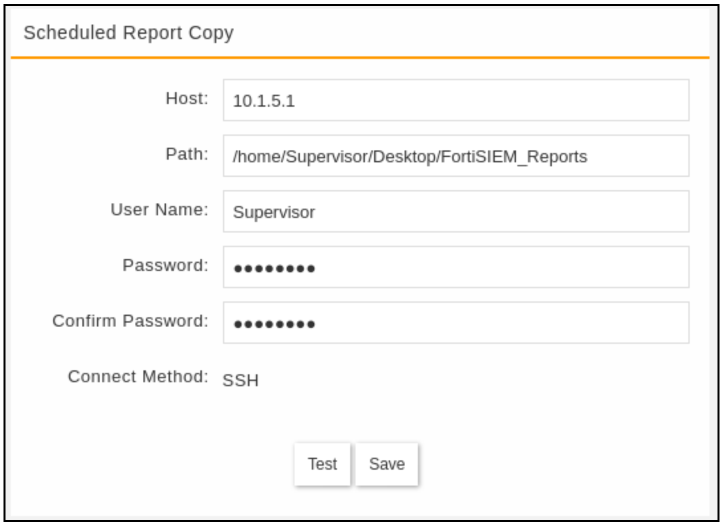
Field	Value
Time Zone	Local
Report time range	Relative, last 7 Days
Schedule Time Range (Start Time:)	Set this field to 10 minutes ahead of the current time, and then make sure **Local** is selected.
Schedule Recurrence Pattern	Once
Output Format	PDF
Notification	Copy to a remote directory
Keep report for	2 hours

The remote directory to save reports is already configured. The **Scheduled** column for the **All Incidents** report indicates that a report is scheduled.



	Name	Description	Report Design Template
✓	All Incidents	Captures the incidents in a time window	Global System Reports Root Template
	Cases Closed By User - Weekly	Shows cases closed by user on a week-by-week basis	Global System Reports Root Template
			Global System Reports Root

7. Click the **ADMIN** tab, and then click **Settings** > **Analytics** > **Scheduled Report** > **Scheduled Report Copy** to review the settings of the remote directory.



Scheduled Report Copy

Host: 10.1.5.1

Path: /home/Supervisor/Desktop/FortiSIEM_Reports

User Name: Supervisor

Password: ••••••••

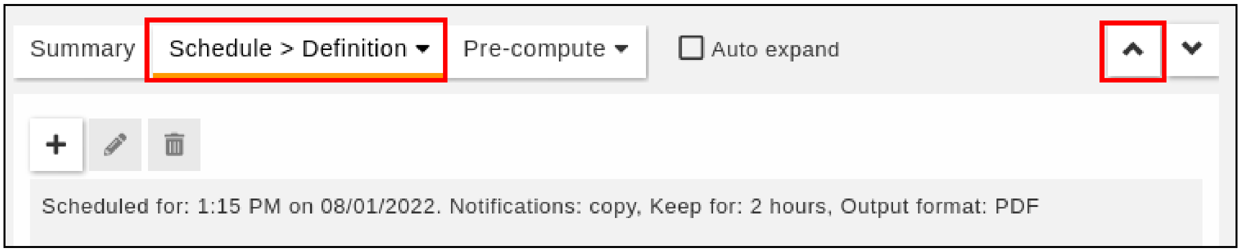
Confirm Password: ••••••••

Connect Method: SSH

The **FortiSIEM _Reports** folder is on the desktop of the **Linux-Client** VM.

To explore other options to schedule a report

1. On the FortiSIEM GUI, click the **RESOURCES** tab.
2. Click **Reports** > **Incidents**.
3. Select the **All Incidents** report, and then in the lower section, click the **Schedule** tab (you may need to click the up arrow in the lower-right corner of the GUI to see this).



Scheduled for: 1:15 PM on 08/01/2022. Notifications: copy, Keep for: 2 hours, Output format: PDF

Notice the existing report schedule is already present.

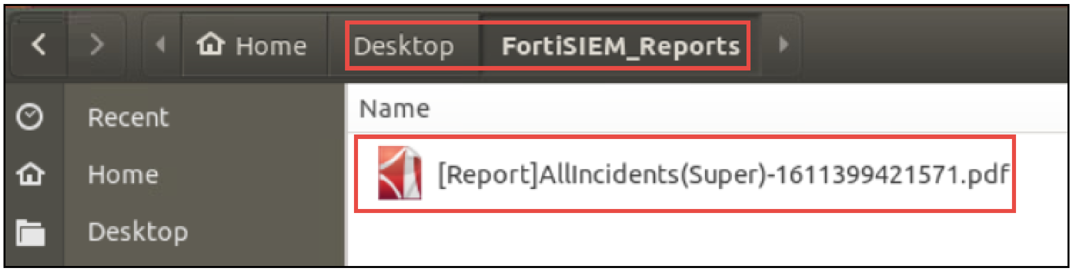
4. Click **+**.

   Notice that the same **Schedule** dialog box shown above opens.
5. Click **Cancel**.
6. Click the scheduled entry **Scheduled for:<date>**.

   Both the pencil and trash icons become active.
7. Click the pencil icon to modify the schedule of the report.

Do *not* delete the schedule for the report.

8. After 10 minutes, verify the delivery of the scheduled report to the **FortiSIEM_Reports** folder on the desktop of the **Linux-Client** VM.



[Report]AllIncidents(Super)-1611399421571.pdf

All Incidents

Organization : Super/Local
Report Start Time : Jul 25 2022 01:14:59 PM EDT
Report End Time: Aug 01 2022, 01:14:50 PM EDT
Generated On: Aug 01 2022, 01:15:00 PM EDT
Device Time Zone: America/New_York

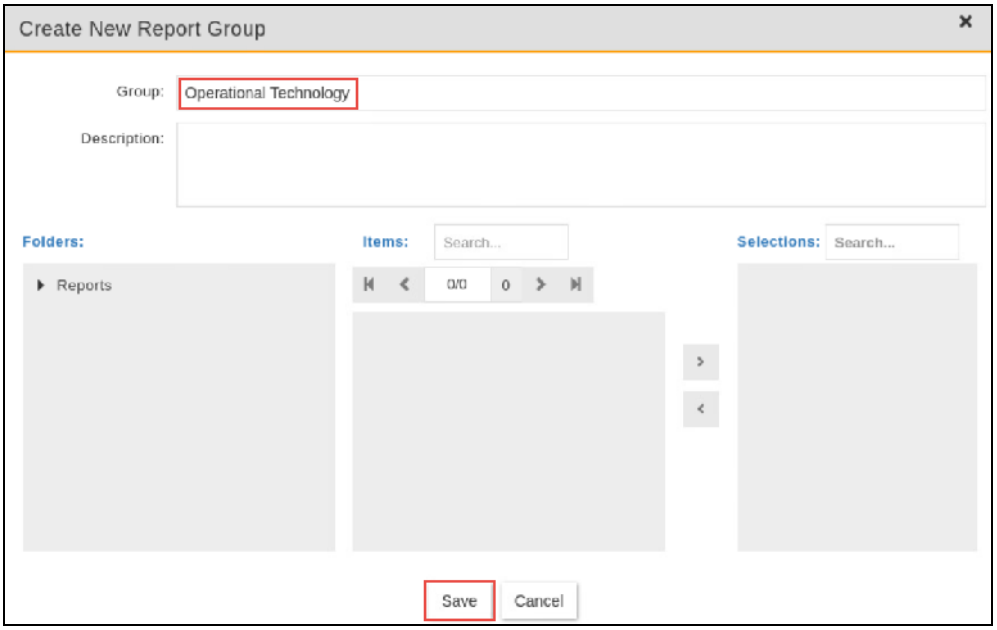
The **All Incidents** report should be available in PDF format after approximately 10 minutes.

Exercise 4: Building Reports From Analytics on FortiSIEM

In this exercise, you will learn to save reports from the **ANALYTICS** tab. You will create search filters to capture events on various OT, security, and performance events, and then save them as reports.

To create a custom report folder for OT

1. On the FortiSIEM GUI, click the **RESOURCES** tab.
2. Click **Reports**.
3. Click **+** to create a new report group.
4. In the **Group** field, type `Operational Technology`.
5. Click **Save**.



Create New Report Group

Group: Operational Technology

Description:

Create a Report on Performance for OT Devices

You will build search filters to capture the temperature performance of fuel pump servers, add aggregate log data for average temperatures, and then save it as a report.

To configure search filters and save a report

1. On the FortiSIEM GUI, click the **ANALYTICS** tab, and then click the search field.

   The **Filter** editor opens.

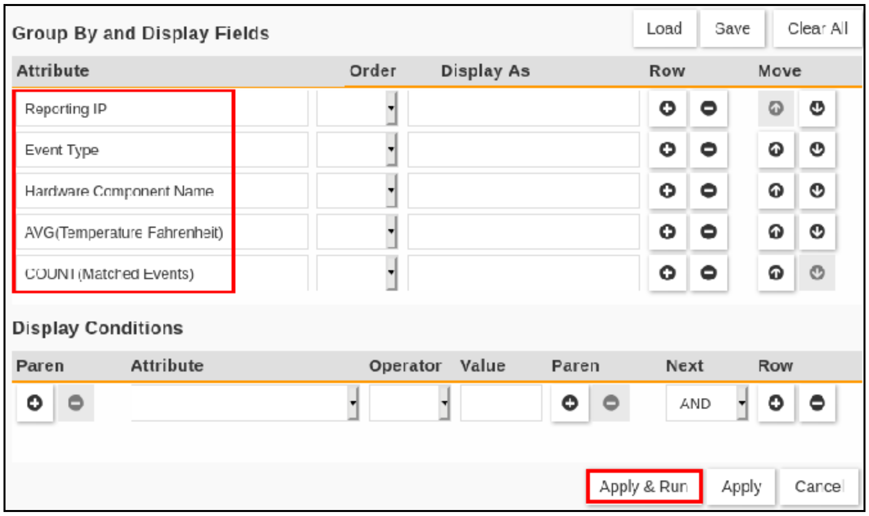
2. Click the **Clear All** button to clear any existing conditions, and then add the following condition:

Field	Value
Filter	Event Attribute
Attribute	Host IP
Operator	IN
Value	10.6.0.1,10.6.0.2,10.6.0.3
NEXT	AND

3. In the **Row** column associated with the condition, click **+** to add another row.
4. In the second condition row, configure the following settings:

Field	Value
Attribute	Event Type
Operator	=
Value	PH_DEV_MON_HW_TEMP

5. In the **Time Range** section, select **Relative**, in the **Last** field, type `1`, select **Day** in the drop-down list, and then click **Apply**.
6. Click the change field display icon beside the **Run** icon.
7. In the **Group By and Display Fields** window, click **Clear All** to clear any existing fields, and then configure the display fields with the following attributes:
    - **Reporting IP**
    - **Event Type**
    - **Hardware Component Name**
    - **AVG(Temperature Fahrenheit)**
    - **COUNT(Matched Events)**



Group By and Display Fields

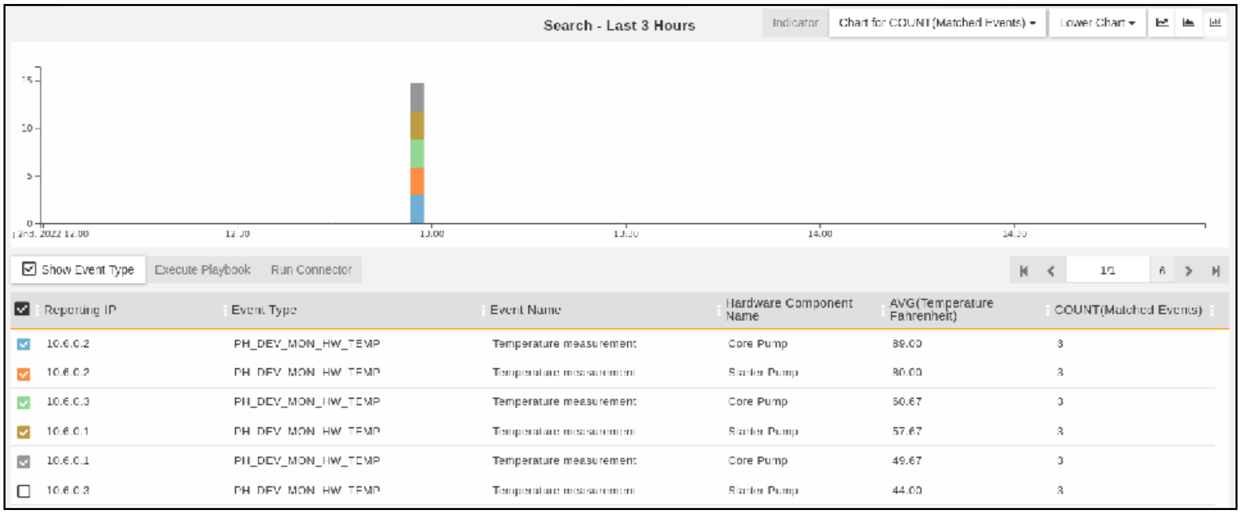
Reporting IP
Event Type
Hardware Component Name
AVG(Temperature Fahrenheit)
COUNT(Matched Events)

Display Conditions

Use **Expression Builder** where required.

8. Click **Apply & Run**.

   The search results should look similar to the following example:



☑	Reporting IP	Event Type	Event Name	Hardware Component Name	AVG(Temperature Fahrenheit)	COUNT(Matched Events)
☑	10.6.0.2	PH_DEV_MON_HW_TEMP	Temperature measurement	Core Pump	89.00	3
☑	10.6.0.2	PH_DEV_MON_HW_TEMP	Temperature measurement	Starter Pump	80.00	3
☑	10.6.0.3	PH_DEV_MON_HW_TEMP	Temperature measurement	Core Pump	60.67	3
☑	10.6.0.1	PH_DEV_MON_HW_TEMP	Temperature measurement	Starter Pump	57.67	3
☑	10.6.0.1	PH_DEV_MON_HW_TEMP	Temperature measurement	Core Pump	49.67	3
□	10.6.0.3	PH_DEV_MON_HW_TEMP	Temperature measurement	Starter Pump	44.00	3

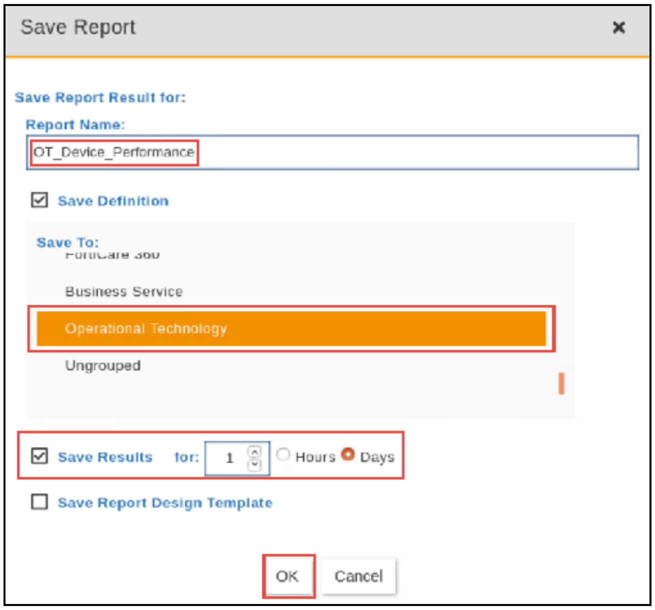
Results may vary, because of log simulation.

Event Name is not an attribute that you can search for—it appears automatically when the **Event Type** attribute is selected.

9. In the upper-left corner, click **Actions**, and then click **Save as Report** to save the results as a report.

   The default report name is **Search Result - <report interval>**.

10. Replace the **Report Name** with `OT_Device_Performance`.
11. Select the **Save Definition** checkbox, and then in the **Save To** section, select the **Operational Technology** folder.
12. Select the **Save Results** checkbox, in the **for** field, select **1** and **Days**, and then click **OK** to save the report.



Save Report ×

Save Report Result for:

Report Name: OT_Device_Performance

☑ Save Definition

Save To:
FortiCare 360
Business Service
Operational Technology
Ungrouped

☑ Save Results for: 1 ○ Hours ● Days

□ Save Report Design Template

A window should appear that confirms the report was saved successfully.

Save Report definition successful

The window disappears automatically. You can view the saved report in the **Reports** > **Operational Technology** folder.

Create a Report on Traffic for Purdue Level 1 Devices

You will build search filters to capture security events from Purdue level 1 devices (traffic from PLC-1 to PLC-3), and then save it as a report.

To configure search filters and save a report

1. On the FortiSIEM GUI, click the **ANALYTICS** tab, and then click the search field.

   The **Filter** editor opens.

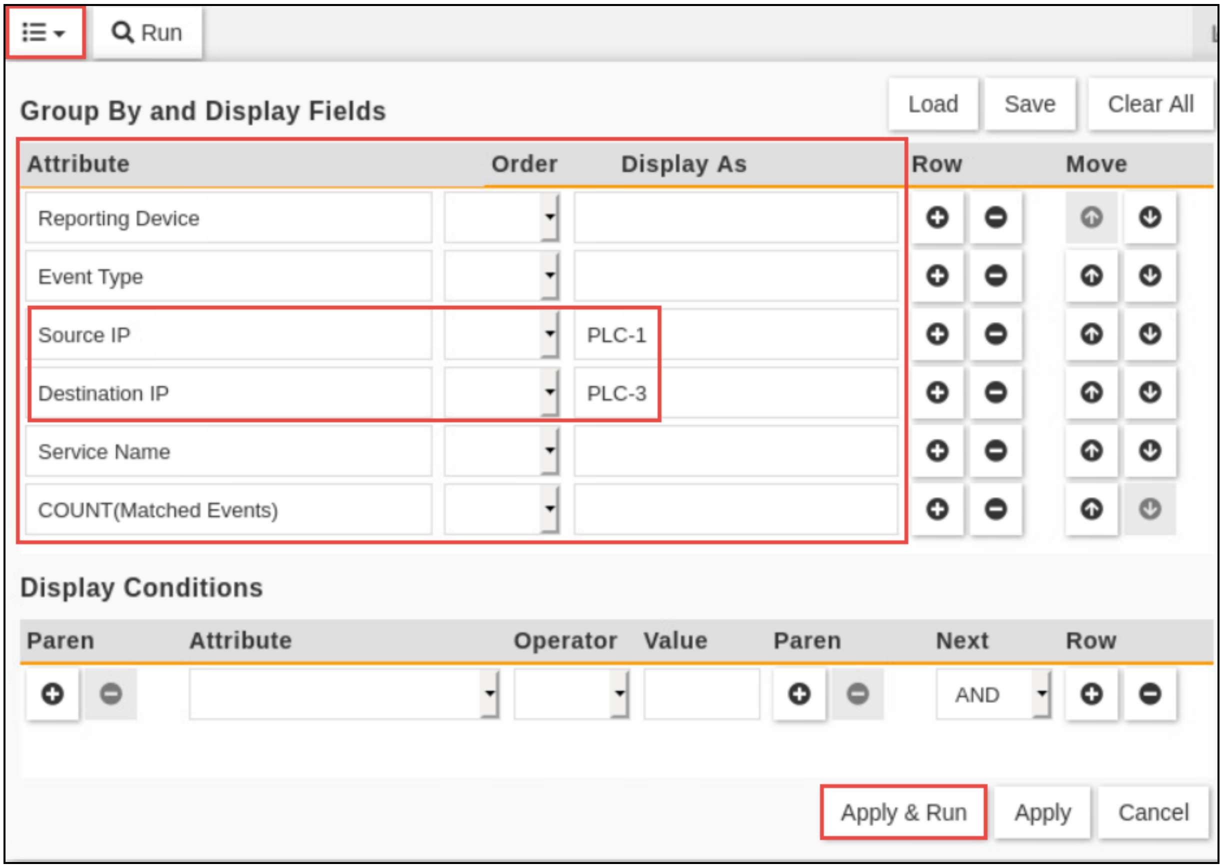
2. Click **Clear All** to clear any existing conditions, and then add the following condition:

Field	Value
Filter	Event Attribute
Attribute	Source IP
Operator	=
Value	192.168.1.1
NEXT	AND

3. In the **Row** column associated with the condition, click **+** to add another row.
4. In the second condition row, configure the following settings:

Field	Value
Attribute	Destination IP
Operator	=
Value	192.168.2.1

5. In the **Time Range** section, select **Relative**, in the **Last** field, type `1`, in the drop-down list, select **Day**, and then click **Apply**.
6. In the **Group By and Display Fields** window, click **Clear All** to clear any existing fields, and then configure the display fields with the following attributes:
   - **Reporting Device**
   - **Event Type**
   - **Source IP** > **Display AS** > `PLC-1`
   - **Destination IP** > **Display AS** > `PLC-3`
   - **Service Name**
   - **COUNT(Matched Events)**



Group By and Display Fields

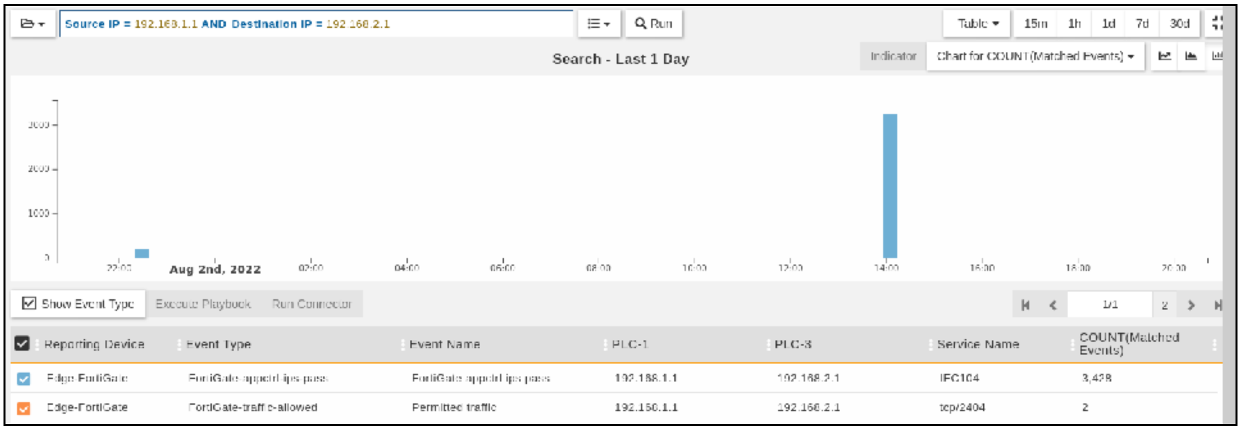
Attribute	Order	Display As	Row	Move
Reporting Device				
Event Type				
Source IP		PLC-1		
Destination IP		PLC-3		
Service Name				
COUNT(Matched Events)				

Display Conditions

Paren	Attribute	Operator	Value	Paren	Next	Row
					AND	

7. Click **Apply & Run**.

   The search results should look like the following example:



☑ Reporting Device	Event Type	Event Name	PLC-1	PLC-3	Service Name	COUNT(Matched Events)
☑ Edge-FortiGate	FortiGate-appctrl-ips-pass	FortiGate appctrl ips pass	192.168.1.1	192.168.2.1	IEC104	3,428
☑ Edge-FortiGate	FortiGate-traffic-allowed	Permitted traffic	192.168.1.1	192.168.2.1	tcp/2404	2

Event Name is not an attribute that you can search for—it appears automatically when the **Event Type** attribute is selected.

8. In the upper-left corner, click **Actions**, and then click **Save as Report** to save the results as a report.

   The default report name is **Search Result - <report interval>**.

9. Replace the **Report Name** with `Traffic From PLC-1 to PLC-3 - Purdue Level 1_Security Events`.
10. Select the **Save Definition** checkbox, and then in the **Save To** section, select the **Operational Technology** folder.
11. Select the **Save Results** checkbox, in the **for** field, select **1** and **Days**, and then click **OK** to save the report.

Create a Report on Modbus and IEC 104 service

You will build search filters to capture security events for Modbus and IEC 104 service, and then save it as a report.

To configure search filters and save a report

1. On the FortiSIEM GUI, continuing on the **ANALYTICS** tab, click the search field.

   The **Filter** editor opens.

2. Click **Clear All** to clear any existing conditions, and then add the following condition:

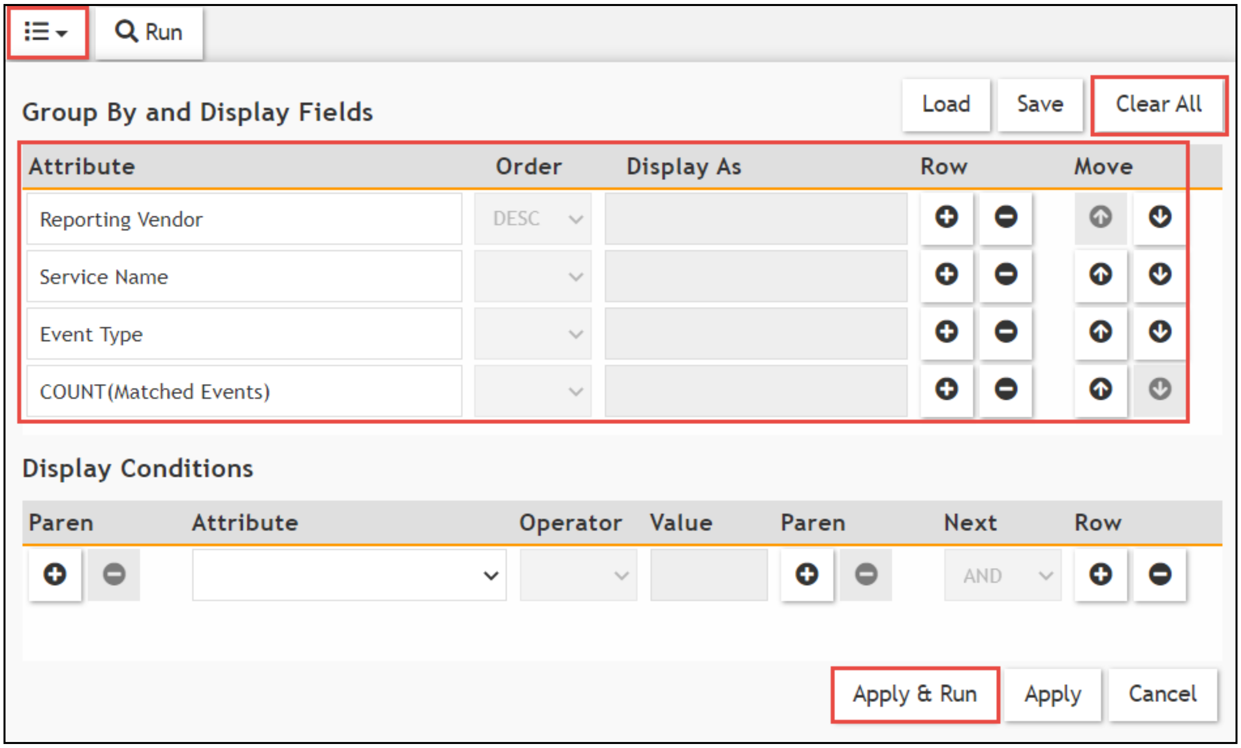
Field	Value
Filter	Event Attribute
Attribute	Destination TCP/UDP Port
Operator	IN

Field	Value
Value	Click **CMDB** > **Protocols** > **OT Ports**, add the **OT Ports** group to **Selections**, and then click **OK**.
NEXT	OR

3. In the **Row** column associated with the condition, click **+** to add another row.
4. In the second condition row, configure the following settings:

Field	Value
Attribute	Source TCP/UDP Port
Operator	IN
Value	Click **CMDB** > **Protocols** > **OT Ports**, add the **OT Ports** group to **Selections**, and then click **OK**.

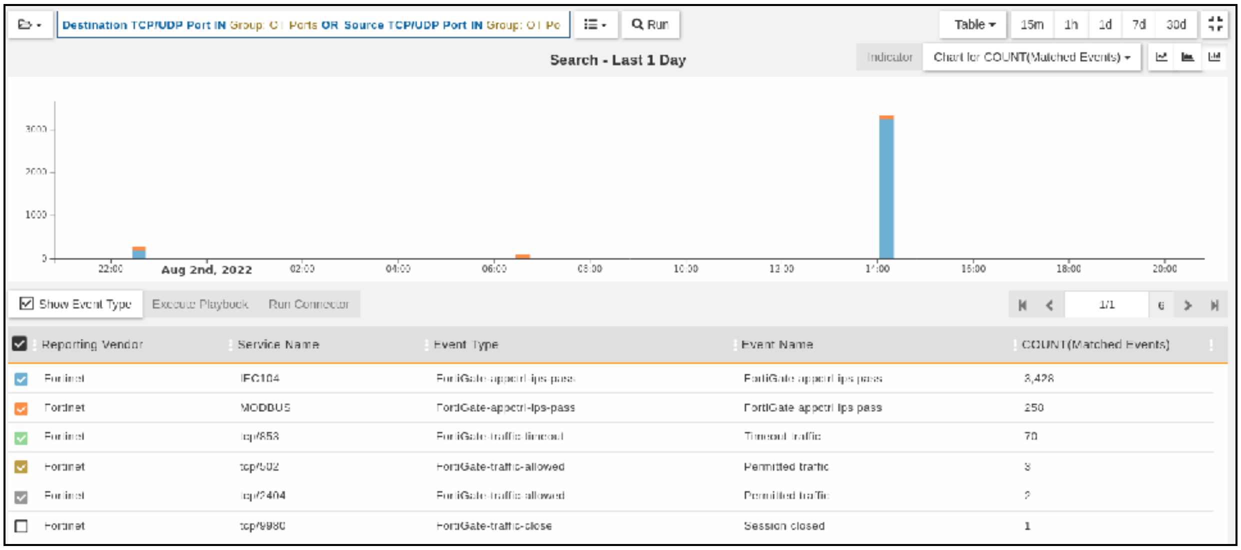
5. In the **Time Range** section, select **Relative**, in the **Last** field, type `1`, in the drop-down list, select **Day**, and then click **Apply**.
6. In the **Group By and Display Fields** window, click **Clear All** to clear any existing fields, and then configure the display fields with the following attributes:
   - **Reporting Vendor**
   - **Service Name**
   - **Event Type**
   - **COUNT(Matched Events)**



Attribute	Order	Display As
Reporting Vendor	DESC	
Service Name		
Event Type		
COUNT(Matched Events)		

7. Click **Apply & Run**.

   The search results should look like the following example:



☑	Reporting Vendor	Service Name	Event Type	Event Name	COUNT(Matched Events)
☑	Fortinet	IEC104	FortiGate-appctrl-ips-pass	FortiGate appctrl ips pass	3,428
☑	Fortinet	MODBUS	FortiGate-appctrl-ips-pass	FortiGate appctrl ips pass	250
☑	Fortinet	tcp/853	FortiGate-traffic-timeout	Timeout traffic	70
☑	Fortinet	tcp/502	FortiGate-traffic-allowed	Permitted traffic	3
☑	Fortinet	tcp/2404	FortiGate-traffic-allowed	Permitted traffic	2
□	Fortinet	tcp/9980	FortiGate-traffic-close	Session closed	1

Event Name is not an attribute that you can search for—it appears automatically when the **Event Type** attribute is selected.

8. In the upper-left corner, click **Actions**, , and then click **Save as Report** to save the results as a report.

   The default report name is **Search Result - <report interval>**.

9. Replace the **Report Name** with `MODBUS and IEC104_OT_Security_Events`.
10. Select the **Save Definition** checkbox, and then in the **Save To** section, select the **Operational Technology** folder.
11. Select the **Save Results** checkbox, in the **for** field, select **1** and **Days**, and then click **OK** to save the report.

Create a Report on OT Security Events From FortiAnalyzer

You will build search filters to capture security events that FortiAnalyzer (IP 10.1.3.210) reports, and you will add display fields to display the application risk level, and then save it as a report.

To configure search filters and save a report

1. On the FortiSIEM GUI, continuing on the **ANALYTICS** tab, click the search field.

   The **Filter** editor opens.

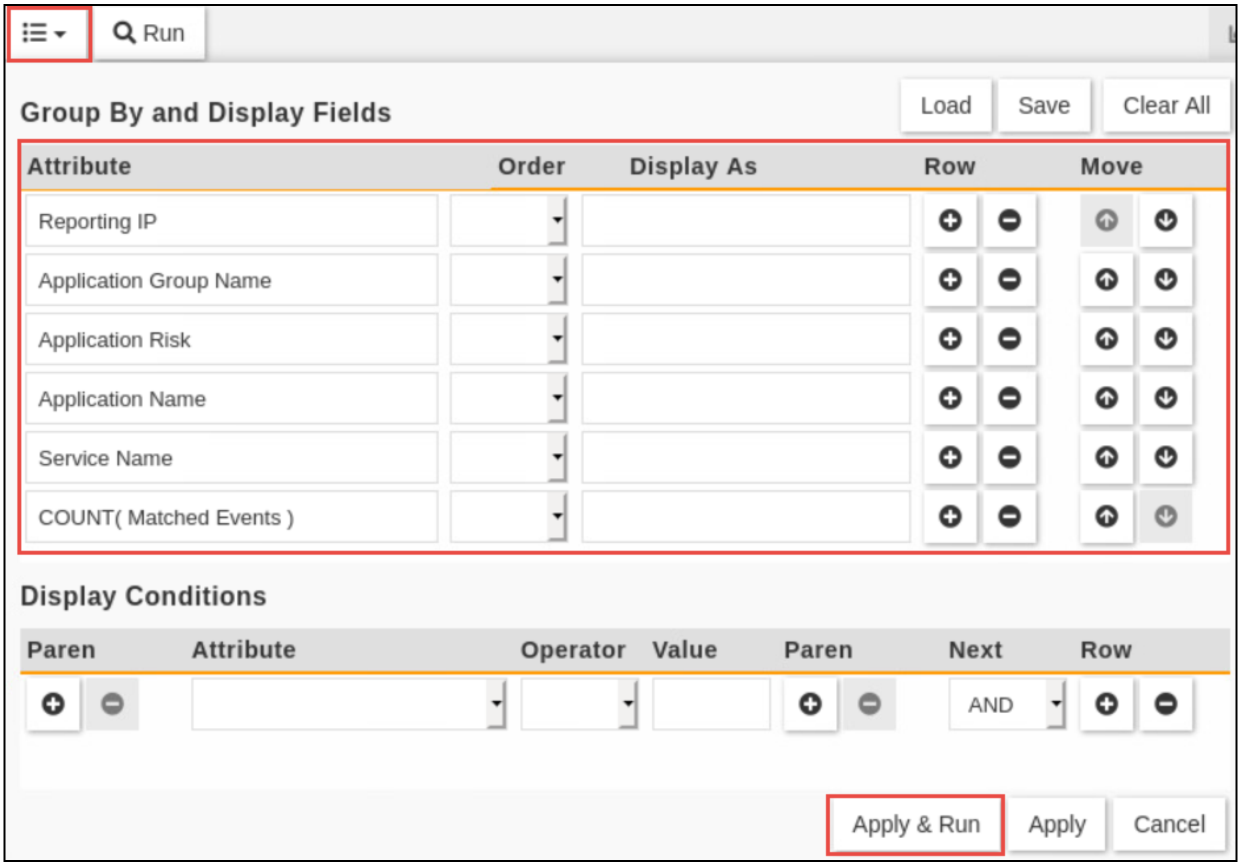
2. Click **Clear All** to clear any existing conditions, and then add the following condition:

Field	Value
Filter	Event Attribute
Attribute	Reporting IP
Operator	=
Value	10.1.3.210
NEXT	AND

3. In the **Row** column associated with the condition, click **+** to add another row.
4. In the second condition row, configure the following settings:

Field	Value
Attribute	Application Group Name
Operator	=
Value	Industrial

5. In the **Time Range** section, select **Relative**, in the **Last** field, type `1`, in the drop-down list, select **Day**, and then click **Apply**.
6. In the **Group By and Display Fields** window, click **Clear All** to clear any existing fields, and then configure the display fields with the following attributes:
   - **Reporting IP**
   - **Application Group Name**
   - **Application Risk**
   - **Application Name**
   - **Service Name**
   - **COUNT(Matched Events)**



Group By and Display Fields

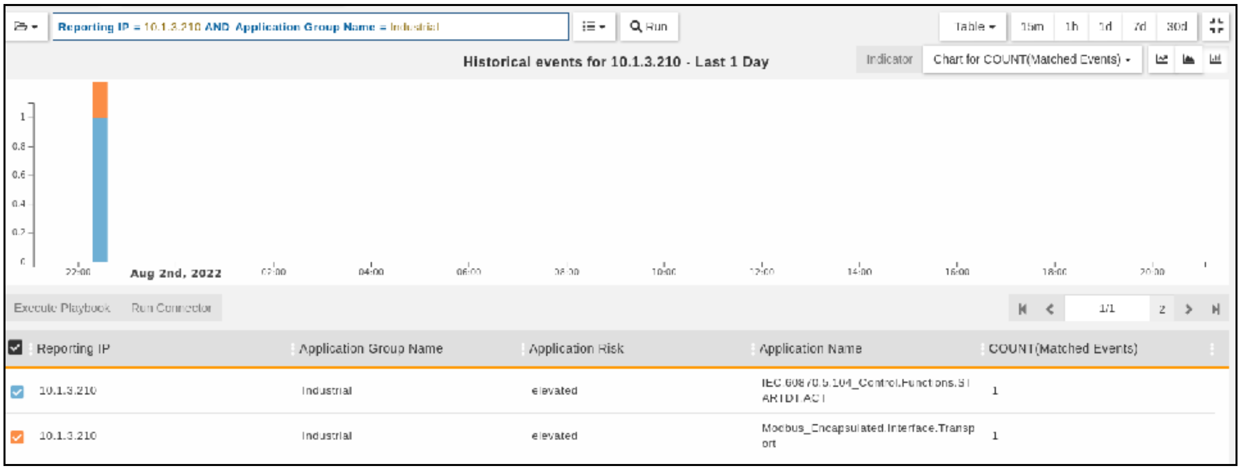
Attribute	Order	Display As	Row	Move
Reporting IP				
Application Group Name				
Application Risk				
Application Name				
Service Name				
COUNT(Matched Events)				

Display Conditions

Paren	Attribute	Operator	Value	Paren	Next	Row
					AND	

7. Click **Apply & Run**.

   The search results should look like the following example:



☑	Reporting IP	Application Group Name	Application Risk	Application Name	COUNT(Matched Events)
☑	10.1.3.210	Industrial	elevated	IEC 60870.5.104_Control.Functions.STARTDT.ACT	1
☑	10.1.3.210	Industrial	elevated	Modbus_Encapsulated.Interface.Transport	1

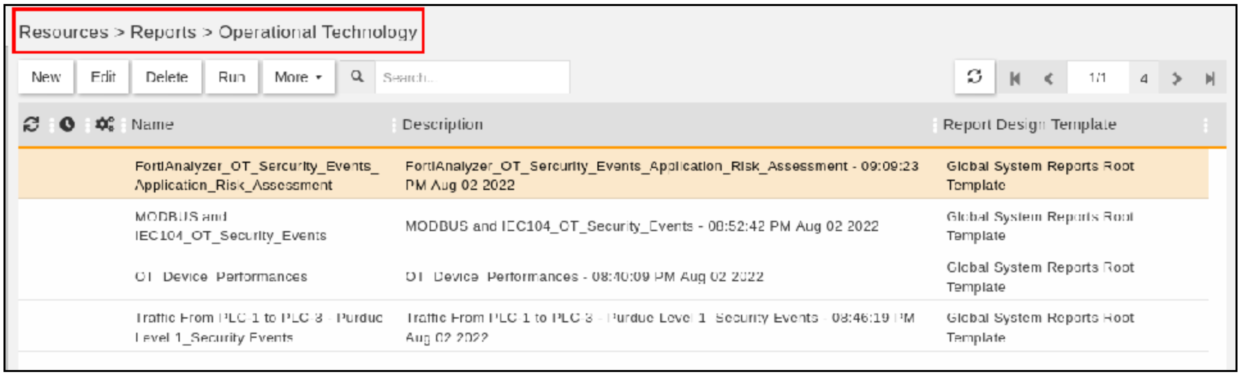
8. In the upper-left corner, click **Actions**, and then click **Save as Report** to save the results as a report.

   The default report name is **Search Result - <report interval>**.

9. Replace the **Report Name** with `FortiAnalyzer_OT_Security_Events_Application_Risk_Assessment`.

10. Select the **Save Definition** checkbox, and then in the **Save To** section, select the **Operational Technology** folder.

11. Select the **Save Results** checkbox, in the **for** field, select **1** and **Days**, and then click **OK** to save the report.
12. Navigate to the **RESOURCES** > **Reports** > **Operational Technology** folder to view all four reports.



Resources > Reports > Operational Technology

Name	Description	Report Design Template
FortiAnalyzer_OT_Sercurity_Events_Application_Risk_Assessment	FortiAnalyzer_OT_Sercurity_Events_Application_Risk_Assessment - 09:09:23 PM Aug 02 2022	Global System Reports Root Template
MODBUS and IEC104_OT_Security_Events	MODBUS and IEC104_OT_Security_Events - 08:52:42 PM Aug 02 2022	Global System Reports Root Template
OT_Device_Performances	OT_Device_Performances - 08:40:09 PM Aug 02 2022	Global System Reports Root Template
Traffic From PLC-1 to PLC-3 - Purdue Level 1_Security Events	Traffic From PLC-1 to PLC-3 - Purdue Level 1_Security Events - 08:46:19 PM Aug 02 2022	Global System Reports Root Template

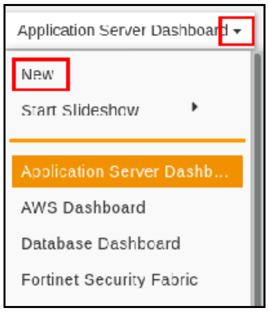
You will use these reports in the next exercise to build an OT dashboard.

Exercise 5: Building an OT Dashboard on FortiSIEM

In this exercise, you will create a custom dashboard by adding dashboard widgets for OT.

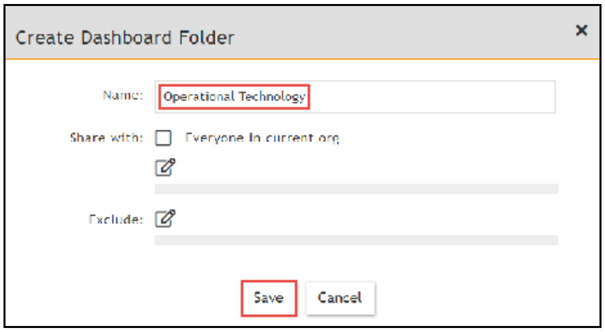
To create a custom dashboard folder

1. On the FortiSIEM GUI, click the **DASHBOARD** tab.
2. In the **Application Server Dashboard** drop-down menu, select **New**.



The **Create Dashboard Folder** window opens.

4. In the **Name** field, type `Operational Technology`, and then click **Save**.



Name: Operational Technology

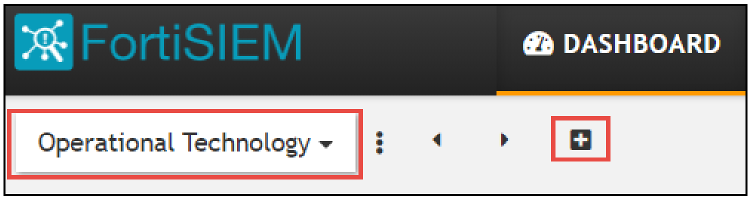
Share with: □ Everyone In current org

Exclude:

The **Operational Technology** group opens, and is added to the dashboard drop-down list.

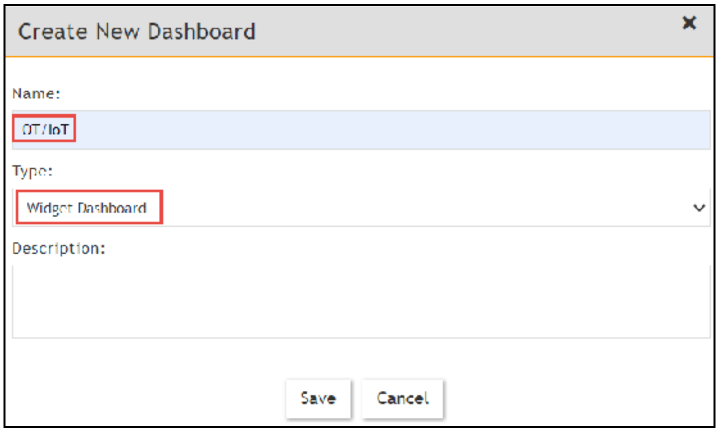
To add widget dashboards

1. In the **Operational Technology** dashboard group, to the right of the dashboard drop-down list, click **+**.



The **Create New Dashboard** window opens.

2. In the **Name** field, type `OT/IoT`.
3. In the **Type** field, select **Widget Dashboard**.
4. Click **Save**.



Create New Dashboard

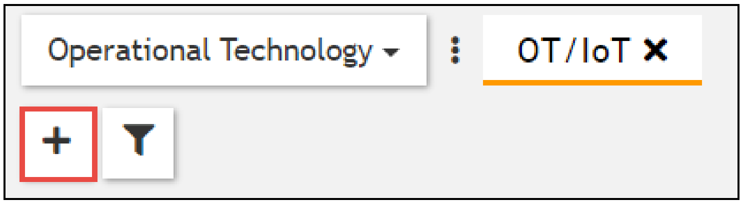
Name: OT/IoT

Type: Widget Dashboard

Description:

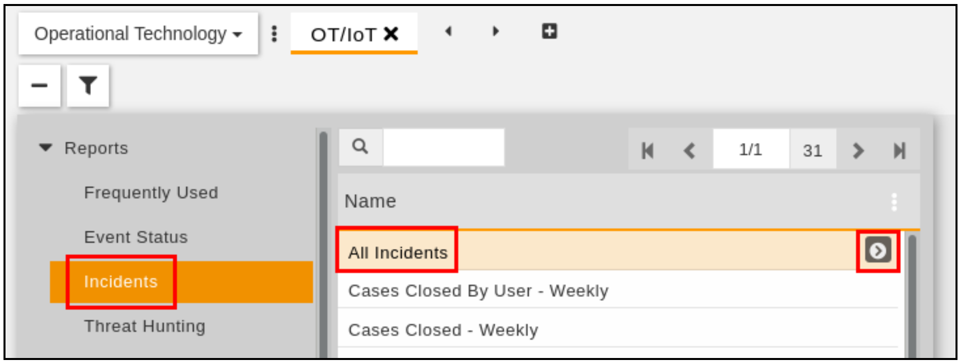
The OT/IoT widget is created, and the main window displays an empty widget.

5. On the **OT/IoT** tab, click **+**.

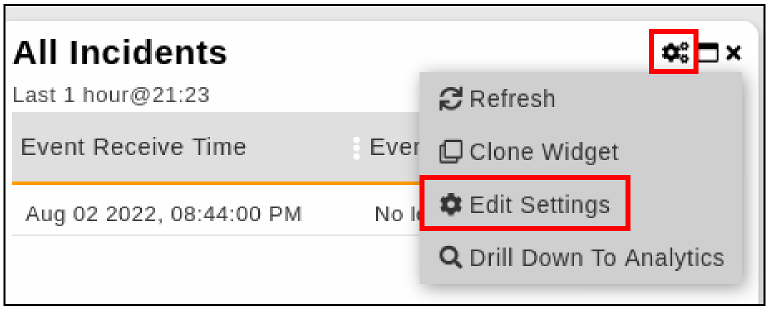


The **Report** selector window appears.

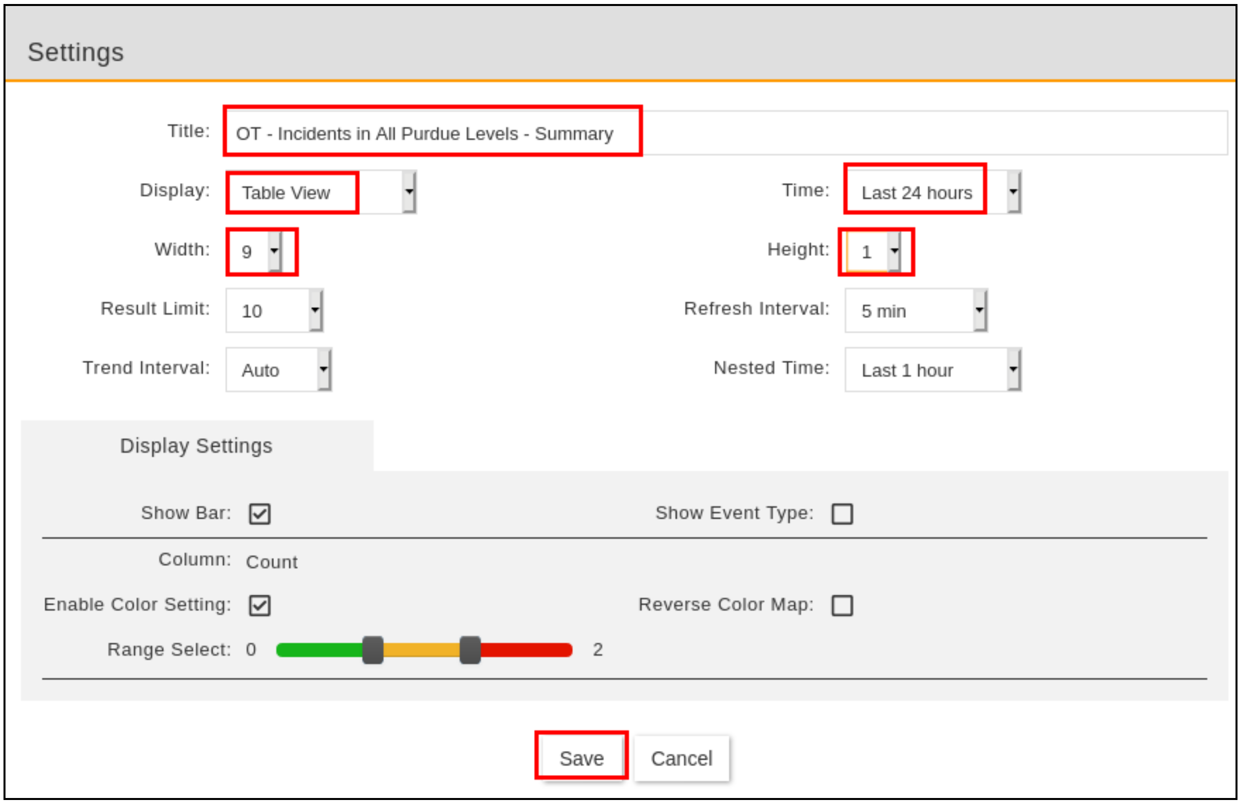
6. Click the **Reports** folder, and then select the **Incidents** folder.
7. Select the **All Incidents** report, and then when the right arrow icon appears, click the icon to add the **All Incidents** report widget.



8. Hover over the title bar of the **All Incidents** widget, on the right side, click the settings icon, and then click **Edit Settings**.



9. Adjust the widget settings to match the following image, and then click **Save**:



Settings

Title: OT - Incidents in All Purdue Levels - Summary

Display: Table View

Time: Last 24 hours

Width: 9

Height: 1

Result Limit: 10

Refresh Interval: 5 min

Trend Interval: Auto

Nested Time: Last 1 hour

Display Settings

Show Bar: ☑

Show Event Type: □

Column: Count

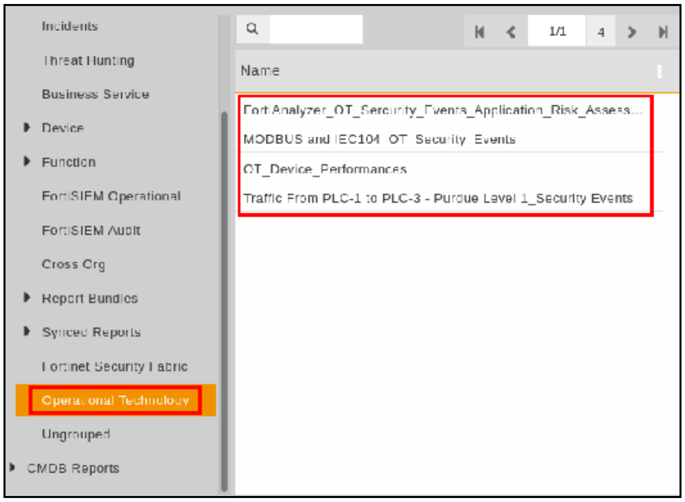
Enable Color Setting: ☑

Reverse Color Map: □

Range Select: 0 2

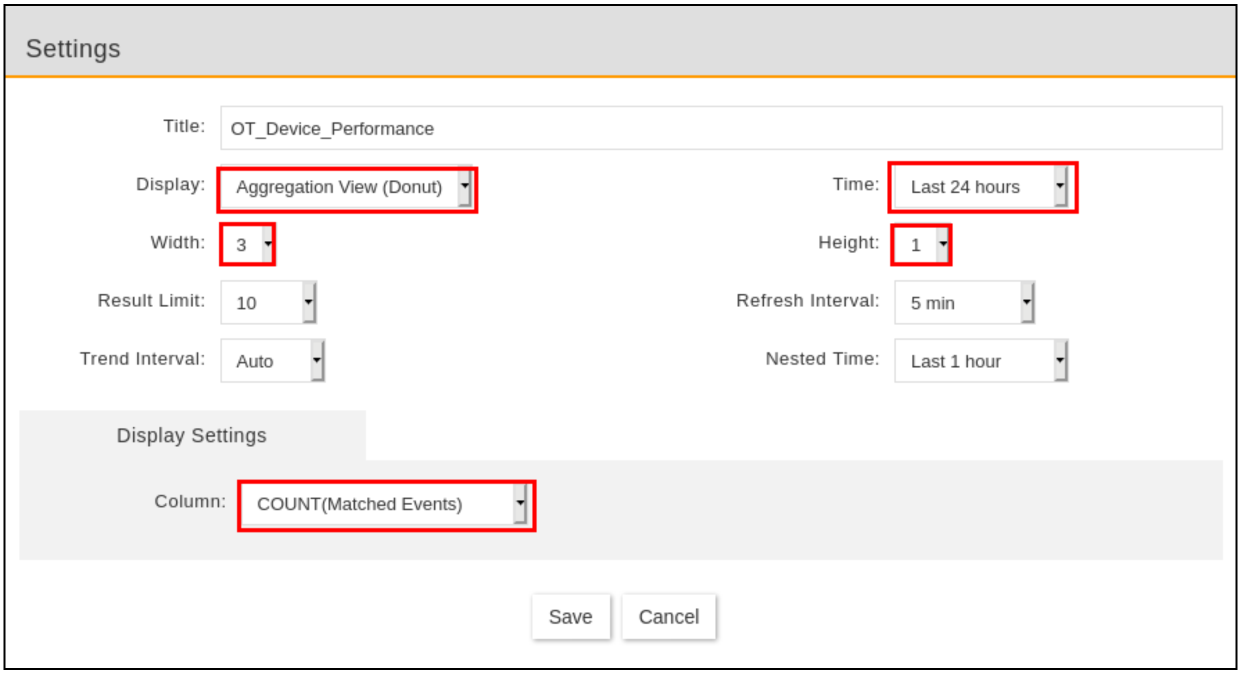
If the **Display Settings** fields are empty, click **Save**, and then click the widget settings icon again to open the widget settings. The **Display Settings** fields should now be populated. Network lag can cause this issue, which you may not experience.

10. On the **OT/IoT** tab, click **+** again, and add the report widgets from the **Operational Technology** folder, in the following order:
    - **OT_Device_Performance**
    - **FortiAnalyzer_OT_Security_Events_Application_Risk_Assessment**
    - **MODBUS and IEC104_OT_Security_Events**
    - **Traffic From PLC-1 to PLC-3 - Purdue Level 1_Security Events**



FortiAnalyzer_OT_Sercurity_Events_Application_Risk_Assess...
MODBUS and IEC104 OT Security Events
OT_Device_Performances
Traffic From PLC-1 to PLC-3 - Purdue Level 1_Security Events

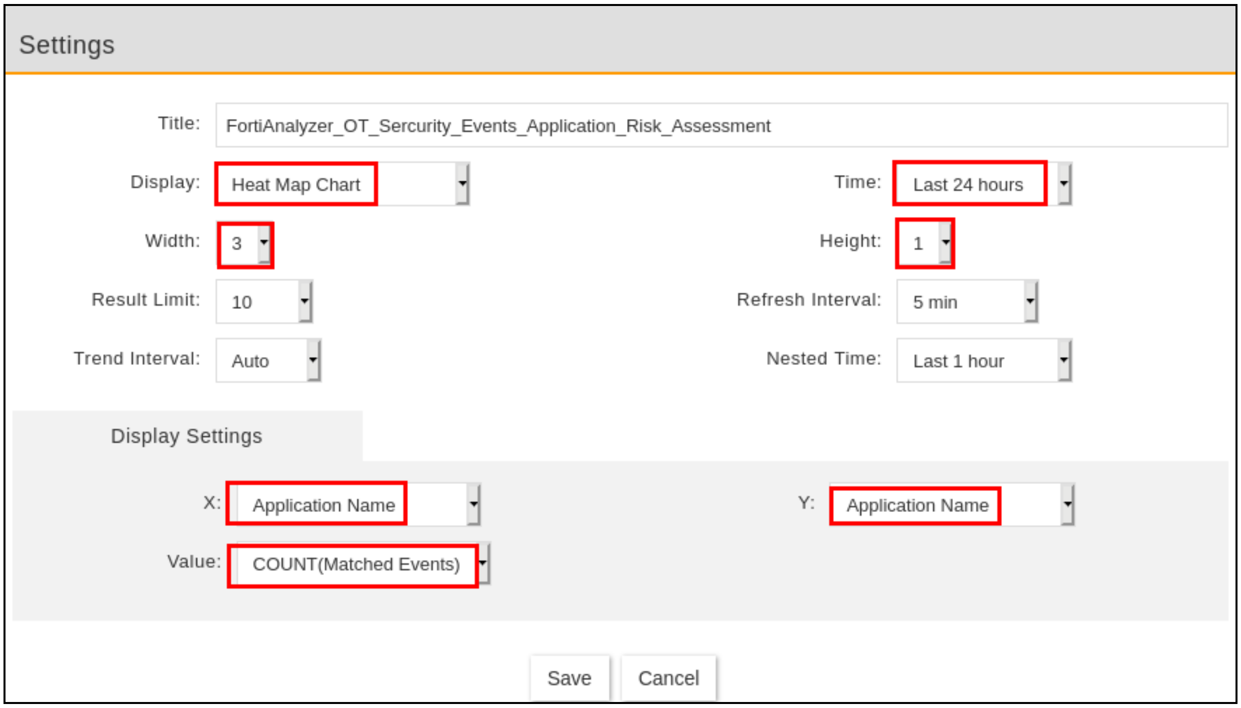
10. Hover over the title bar of the **OT_Device_Performance** widget, and then on the right, click the settings icon to edit the settings.
11. Adjust the widget settings to match the following image, and then click **Save**:



Title: OT_Device_Performance
Display: Aggregation View (Donut)
Time: Last 24 hours
Width: 3
Height: 1
Result Limit: 10
Refresh Interval: 5 min
Trend Interval: Auto
Nested Time: Last 1 hour
Column: COUNT(Matched Events)

If the **Display Settings** fields in the widget settings are empty, click **Save**, and then click the widget settings icon again to open the widget settings. The **Display Settings** fields should now be populated. Network lag can cause this issue, which you may not experience.

12. Hover over the title bar of the **FortiAnalyzer_OT_Security_Events_Application_Risk_Assessment** widget, and then on the right, click the settings icon to edit the settings.
13. Adjust the widget settings to match the following image, and then click **Save**:



Settings

Title: FortiAnalyzer_OT_Sercurity_Events_Application_Risk_Assessment

Display: Heat Map Chart

Time: Last 24 hours

Width: 3

Height: 1

Result Limit: 10

Refresh Interval: 5 min

Trend Interval: Auto

Nested Time: Last 1 hour

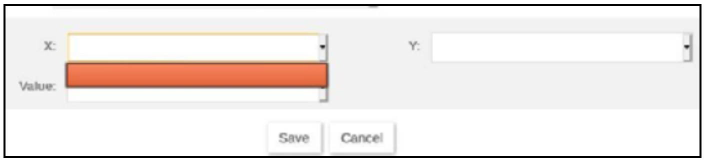
Display Settings

X: Application Name

Y: Application Name

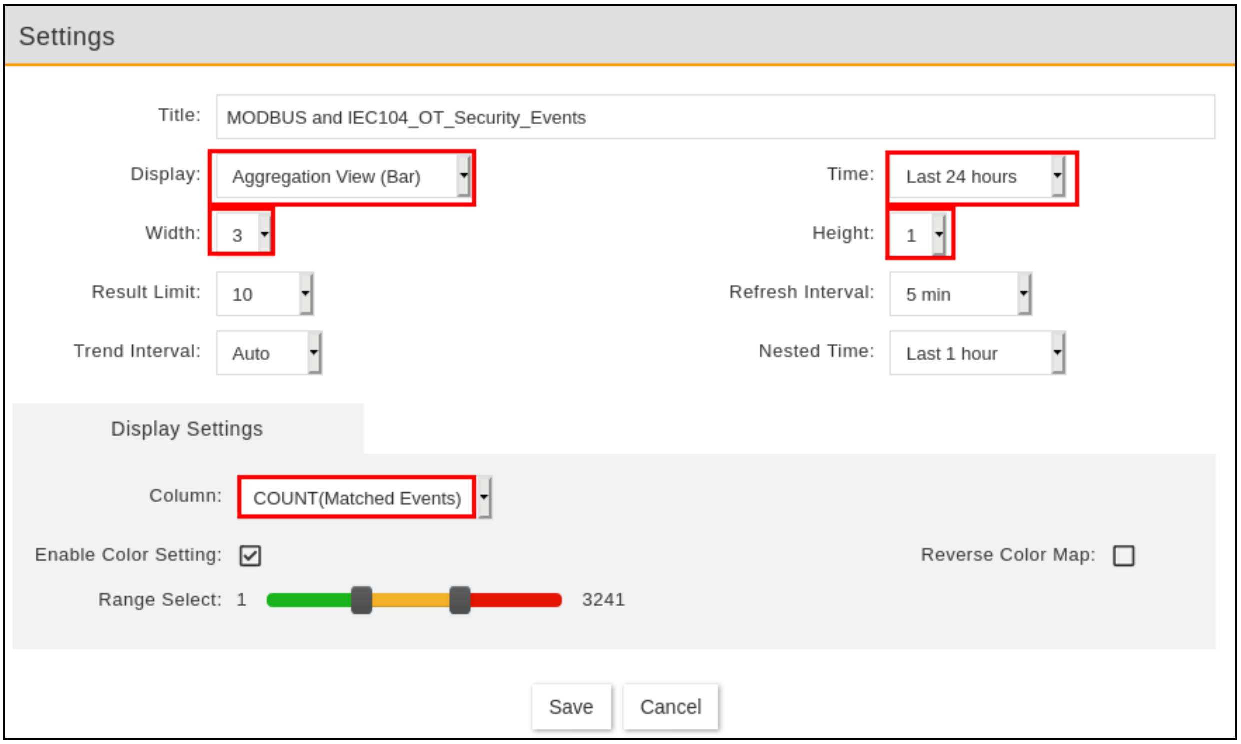
Value: COUNT(Matched Events)

If the **Display Settings** fields in the widget settings are empty, click **Save**, and then click the widget settings icon again to open the widget settings. The **Display Settings** fields should now be populated. Network lag can cause this issue, which you may not experience.



14. Hover over the title bar of the **MODBUS and IEC104_OT_Security_Events** widget, and on the right side, click the settings icon to edit the settings.

15. Adjust the widget settings to match the following image, and then click **Save**:



Settings

Title: MODBUS and IEC104_OT_Security_Events

Display: Aggregation View (Bar)

Time: Last 24 hours

Width: 3

Height: 1

Result Limit: 10

Refresh Interval: 5 min

Trend Interval: Auto

Nested Time: Last 1 hour

Display Settings

Column: COUNT(Matched Events)

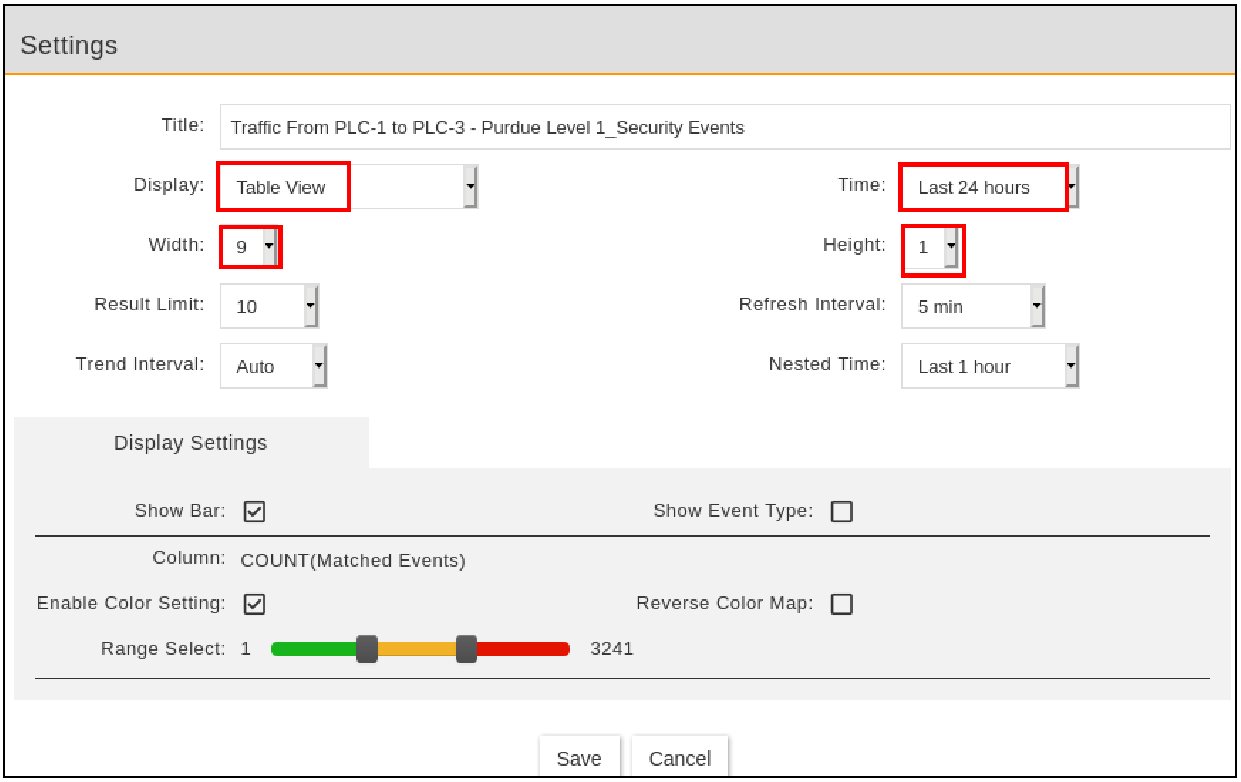
Enable Color Setting: ☑

Reverse Color Map: □

Range Select: 1 3241

If the **Display Settings** fields in the widget settings are empty, click **Save**, and then click the widget settings icon again to open the widget settings. The **Display Settings** fields should now be populated. Network lag can cause this issue, which you may not experience.

16. Hover over the title bar of the **Traffic From PLC-1 to PLC-3 - Purdue Level 1_Security Events** widget, and then on the right, click the settings icon to edit the settings.
17. Adjust the widget settings to match the following image, and then click **Save**:



Settings

Title: Traffic From PLC-1 to PLC-3 - Purdue Level 1_Security Events

Display: Table View

Time: Last 24 hours

Width: 9

Height: 1

Result Limit: 10

Refresh Interval: 5 min

Trend Interval: Auto

Nested Time: Last 1 hour

Display Settings

Show Bar: ☑

Show Event Type: □

Column: COUNT(Matched Events)

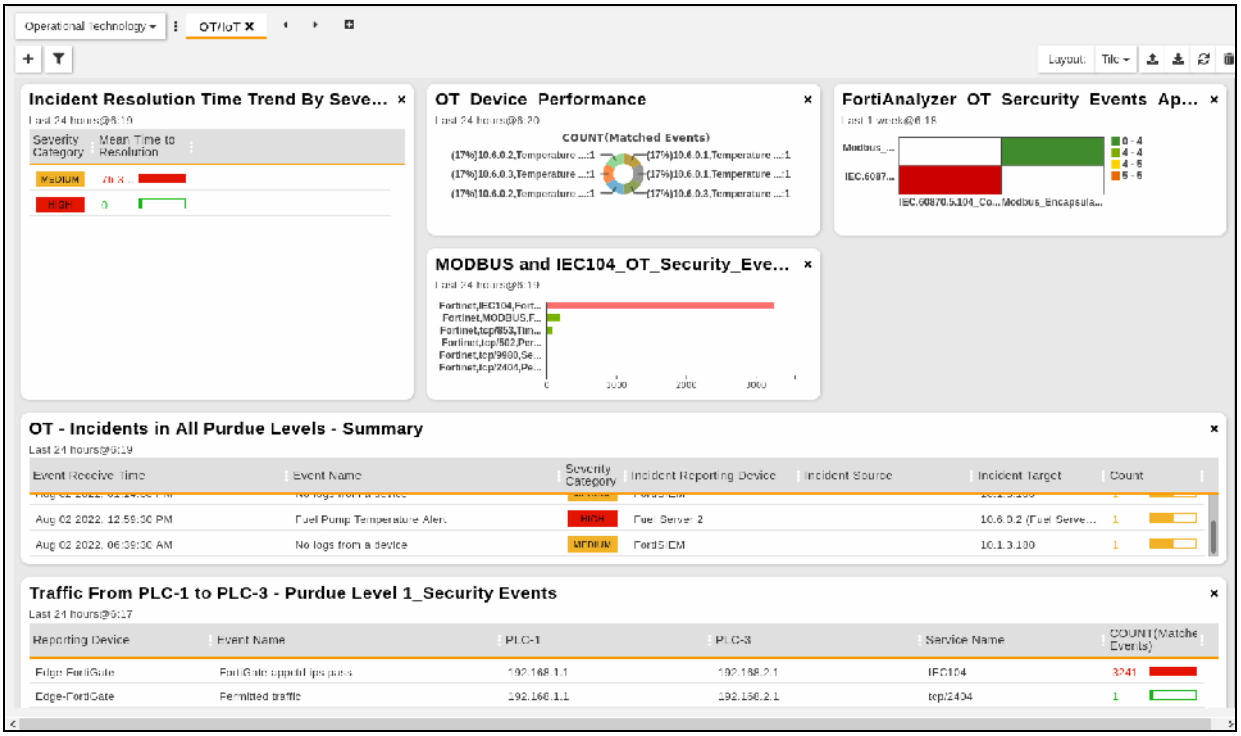
Enable Color Setting: ☑

Reverse Color Map: □

Range Select: 1 3241

If the **Display Settings** fields are empty, click **Save**, and then click the widget settings icon again to open the widget settings. The **Display Settings** fields should now be populated. Network lag can cause this issue, which you may not experience.

18. Review the **Operational Technology** > **OT/IOT** dashboard, which appears similar to the following image:



OT - Incidents in All Purdue Levels - Summary

Last 24 hours@6:19

Event Receive Time	Event Name	Severity Category	Incident Reporting Device	Incident Source	Incident Target	Count
Aug 02 2022, 12:59:30 PM	Fuel Pump Temperature Alert	HIGH	Fuel Server 2		10.6.0.2 (Fuel Serve...	1
Aug 02 2022, 06:39:30 AM	No logs from a device	MEDIUM	FortiSIEM		10.1.3.100	1

Traffic From PLC-1 to PLC-3 - Purdue Level 1_Security Events

Last 24 hours@6:17

Reporting Device	Event Name	PLC-1	PLC-3	Service Name	COUNT(Matched Events)
Edge-FortiGate	FortiGate appctrl ips pass	192.168.1.1	192.168.2.1	IEC104	3241
Edge-FortiGate	Permitted traffic	192.168.1.1	192.168.2.1	tcp/2404	1

Results may vary, because of log simulation.

Lab 8: Use Case 1

In this lab, you will configure Fortinet devices based on requirements that a customer provides. The lab is preconfigured with IP addresses.

Objectives

- Complete all tasks to configure the network based on customer requirements

Time to Complete

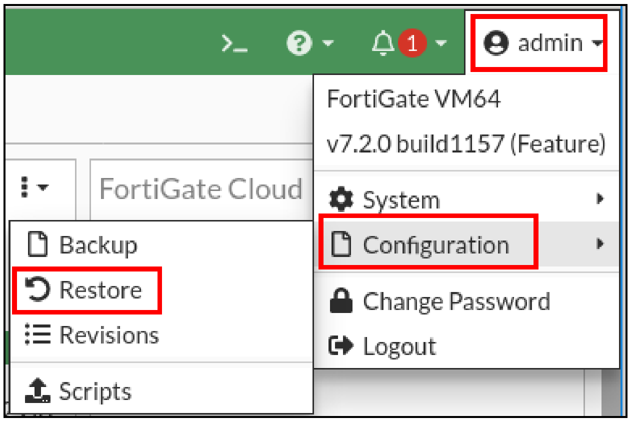
Estimated: 150 minutes

Prerequisites

Before you begin this lab, you must restore the initial configuration files to the FortiGate devices. The configuration files are located on the desktop of the Linux-Client VM.

To restore the FortiGate-1 configuration file

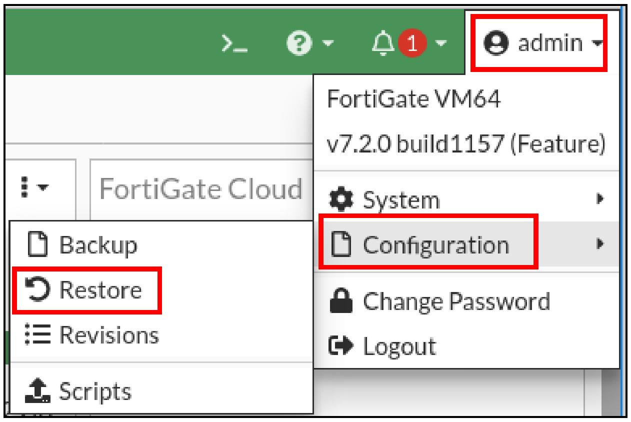
1. Log in to the FortiGate-1 GUI at `10.1.1.1` with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **Use Case-1**, select `FortiGate-1_usecase1.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

To restore the FortiGate-2 configuration file

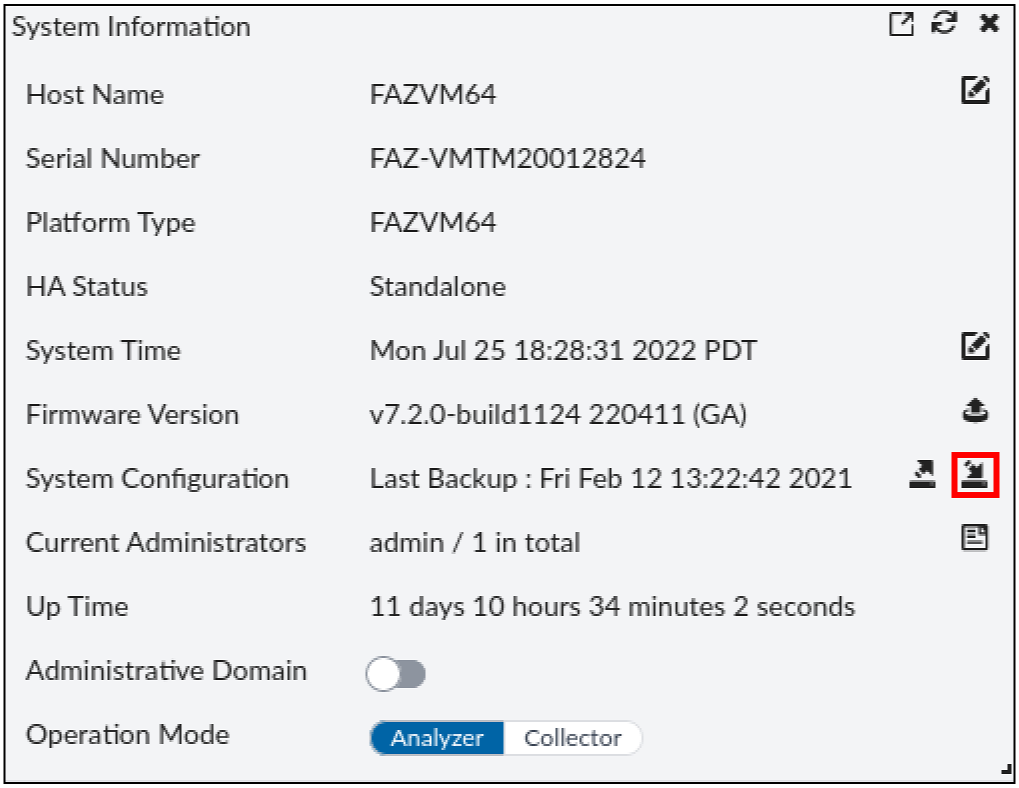
1. Log in to the FortiGate-2 GUI at `10.1.2.1` with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **Use Case-1**, select `FortiGate-2_usecase1.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

To restore the FortiAnalyzer configuration file

1. On the Linux-Client VM, open a browser, and then log in to the FortiAnalyzer GUI at `10.1.3.210` with the username `admin` and password `password`.
2. Click **System Settings**.
3. In the **System Information** widget, in the **System Configuration** field, click the restore icon.



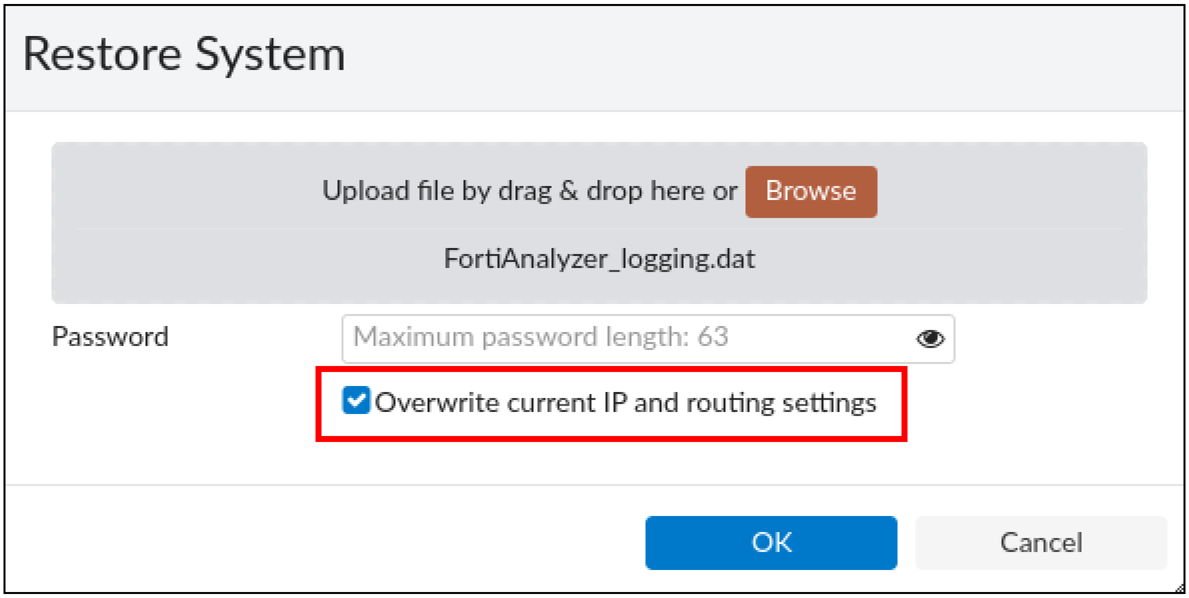
System Information

Host Name	FAZVM64
Serial Number	FAZ-VMTM20012824
Platform Type	FAZVM64
HA Status	Standalone
System Time	Mon Jul 25 18:28:31 2022 PDT
Firmware Version	v7.2.0-build1124 220411 (GA)
System Configuration	Last Backup : Fri Feb 12 13:22:42 2021
Current Administrators	admin / 1 in total
Up Time	11 days 10 hours 34 minutes 2 seconds
Administrative Domain	○
Operation Mode	● Analyzer ○ Collector

4. Click **Browse**.
5. Click **Desktop** > **Resources** > **Use Case-1**, and then select `FortiAnalyzer_usecase1.dat`.

You do not have to enter a password because the file is not encrypted.

6. Leave the **Overwrite current IP and routing settings** checkbox selected.



Restore System

Upload file by drag & drop here or Browse

FortiAnalyzer_logging.dat

Password: Maximum password length: 63

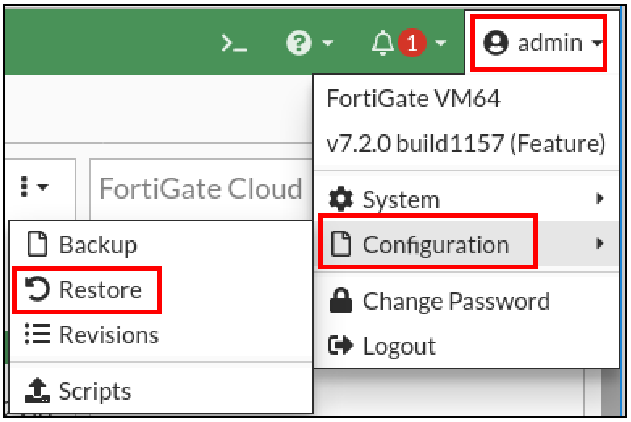
☑ Overwrite current IP and routing settings

OK | Cancel

7. Click **OK**.

To restore the Edge-FortiGate configuration file

1. On the Linux-Client VM, open a browser, and then log in to the Edge-FortiGate GUI at `10.1.5.254` with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



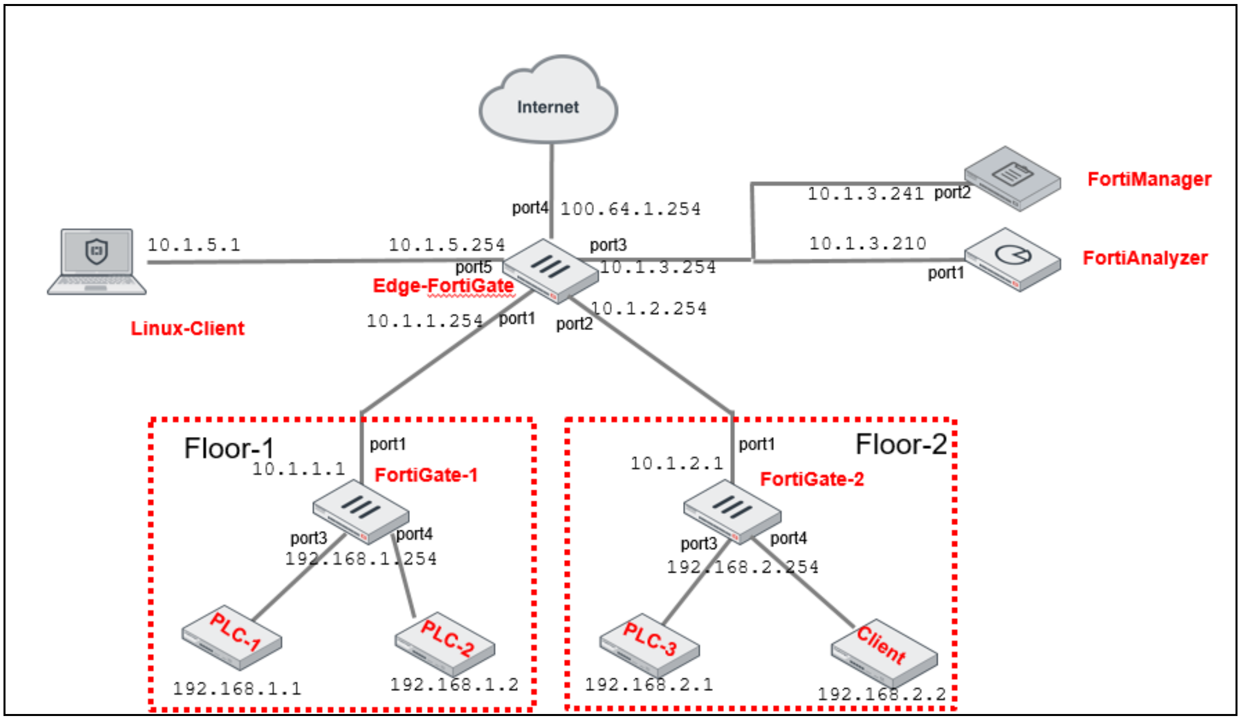
3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **Use Case-1**, select `Edge-FortiGate_usecase1.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

Exercise 1: Configuring Devices

In this exercise, you will configure the OT network based on the following basic customer requirements:

- Achieve microsegmentation within floors
- Implement segmentation between floors
- Implement access control to limit access to Fortinet devices and PLCs
- Allow only Modbus traffic between PLCs based on requirements
- Log traffic on FortiGate and FortiAnalyzer

Network Topology



Review the current configuration before proceeding to the next step. You have basic connectivity from Fortinet products to FortiManager so that you can perform license verification. Do not make changes to the policies that allow this traffic.

Requirements

To configure basic connectivity

Ensure that Linux-Client is able to access the following devices without access control:

- FortiGate-1
- FortiGate-2
- FortiAnalyzer

To achieve microsegmentation within floors

- On Floor-1, make sure that PLC-1 and PLC-2 are in the same broadcast domain.
- Allow only ping traffic from PLC-1 to PLC-2.
- Do not allow any other traffic between PLC-1 and PLC-2.
- On Floor-2, make sure that PLC-3 and the Client VM are in the same broadcast domain.
- Configure FortiGate-1 to allow the Client VM to send all traffic to PLC-3.
- Allow only ping traffic from PLC-3 to the Client VM.

To segment floors

- Ensure that all traffic between floors is controlled through Edge-FortiGate.
- Allow Linux-Client to access PLC-1, PLC-2, PLC-3, and the Client VM over SSH without access control.

To implement access control

Create the following local users on Edge-FortiGate:

Username	Password
supervisor	supervisor
jradmin	jradmin
sradmin	sradmin
client1	client1

Create policies to allow traffic from the Linux-Client VM to the following devices using access control:

- Allow supervisor to access PLC-1, PLC-2, PLC-3, and the Client VM over HTTP.
- Allow jradmin to access PLC-3 over HTTP.
- Allow sradmin to access all PLCs on Floor-1 over HTTP.
- Allow client1 to access the Client VM over HTTP.

To log traffic

Configure the devices so that Edge-FortiGate can send logs in real time to FortiAnalyzer for storage and reporting.

To protect the OT network

- Allow all Modbus traffic from the Client VM to PLC-2, except for traffic that matches the **Modbus_Exception.Illegal.Function** signature.
- Log all traffic from the Client VM to PLC-2.

Exercise 2: Testing the Configuration

Make sure you complete all of the configuration steps before you test the configuration.

To test basic connectivity

From the Linux-Client VM, you must be able to access the following devices:

- FortiGate-1 at `10.1.1.1` over HTTP and SSH
- FortiGate-2 at `10.1.2.1` over HTTP and SSH
- FortiAnalyzer at `http://10.1.3.210` over HTTP and SSH

To test internal segmentation

- You must not be able to ping PLC-3 from PLC-1.
- You must not be able to ping the Client VM from PLC-1.
- PLC-3 must not be able to ping any devices on Floor-1.
- Linux-Client must be able to connect to PLC-1, PLC-2, PLC-3, and the Client VM over SSH.

To test microsegmentation within floors

- You should be able to ping PLC-2 from PLC-1.
- You must not be able to ping PLC-1 from PLC-2.
- You should be able to ping the Client VM from PLC-3.
- You should be able to ping and connect over SSH to PLC-3 from the Client VM.

To test access control

- On the Linux-Client VM, when you access PLC-1, PLC-2, PLC-3, and the Client VM over HTTP, you must receive a login prompt.
- The following users must be able to access the allowed devices over HTTP only:

Username	Allowed devices over HTTP
supervisor	PLC1, PLC-2, PLC-3, and the Client VM
jradmin	PLC-3
sradmin	PLC-1 and PLC-2
client1	The Client VM

After you are logged in with one user, if you do not see another login prompt, do the following:

1. Click **Dashboard** > **Users & Devices**, and then expand **Firewall Users** to deauthenticate the user.
2. Close all browsers to clear the caches.

To test application filter and logging

1. Connect to the Linux-Client VM.
2. Open PuTTY.
3. Click **PLC-2** to select the saved session, and then click **Open**.
4. Log in with the username `sysadmin` and password `Fortinet1!`.
5. Enter the following command:

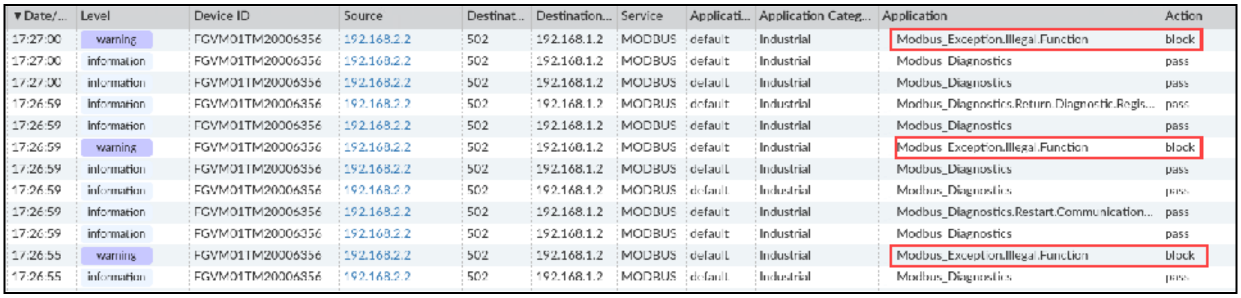
```
./Uploads/start-conpot.sh
```

If you receive an error when you try to run the script, this may be due to a previous session. Enter the `docker ps` command to check the process ID of the running script, and then enter the `docker kill <container_id>` command to stop the script.

6. Leave the PuTTY session open.
7. Connect to the Linux-Client VM.
8. On the Linux-Client VM, open PuTTY.
9. Click **Client** to select the saved session, and then click **Open**.
10. Log in with the username `sysadmin` and password `Fortinet1!`.
11. Enter the following command:

```
./Uploads/synchronous_client_ext.py
```

12. Leave the PuTTY session open.
13. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
14. Click **Log View**.
15. Click **FortiGate** > **Security** > **Application Control**.
16. Ensure that you see the following results:



▼Date/...	Level	Device ID	Source	Destinat...	Destination...	Service	Applicati...	Application Categ...	Application	Action
17:27:00	warning	FGVM01TM20006356	192.168.2.2	502	192.168.1.2	MODBUS	default	Industrial	Modbus_Exception.Illegal.Function	block
17:27:00	information	FGVM01TM20006356	192.168.2.2	502	192.168.1.2	MODBUS	default	Industrial	Modbus_Diagnostics	pass
17:27:00	information	FGVM01TM20006356	192.168.2.2	502	192.168.1.2	MODBUS	default	Industrial	Modbus_Diagnostics	pass
17:26:59	information	FGVM01TM20006356	192.168.2.2	502	192.168.1.2	MODBUS	default	Industrial	Modbus_Diagnostics.Return.Diagnostic.Regis...	pass
17:26:59	information	FGVM01TM20006356	192.168.2.2	502	192.168.1.2	MODBUS	default	Industrial	Modbus_Diagnostics	pass
17:26:59	warning	FGVM01TM20006356	192.168.2.2	502	192.168.1.2	MODBUS	default	Industrial	Modbus_Exception.Illegal.Function	block
17:26:59	information	FGVM01TM20006356	192.168.2.2	502	192.168.1.2	MODBUS	default	Industrial	Modbus_Diagnostics	pass
17:26:59	information	FGVM01TM20006356	192.168.2.2	502	192.168.1.2	MODBUS	default	Industrial	Modbus_Diagnostics	pass
17:26:59	information	FGVM01TM20006356	192.168.2.2	502	192.168.1.2	MODBUS	default	Industrial	Modbus_Diagnostics.Restart.Communication...	pass
17:26:59	information	FGVM01TM20006356	192.168.2.2	502	192.168.1.2	MODBUS	default	Industrial	Modbus_Diagnostics	pass
17:26:55	warning	FGVM01TM20006356	192.168.2.2	502	192.168.1.2	MODBUS	default	Industrial	Modbus_Exception.Illegal.Function	block
17:26:55	information	FGVM01TM20006356	192.168.2.2	502	192.168.1.2	MODBUS	default	Industrial	Modbus_Diagnostics	pass

Lab 9: Use Case 2

In this lab, you will configure Fortinet devices based on requirements provided by a customer. The lab is preconfigured with IP addresses.

Objectives

- Complete all tasks to configure the network based on customer requirements

Time to Complete

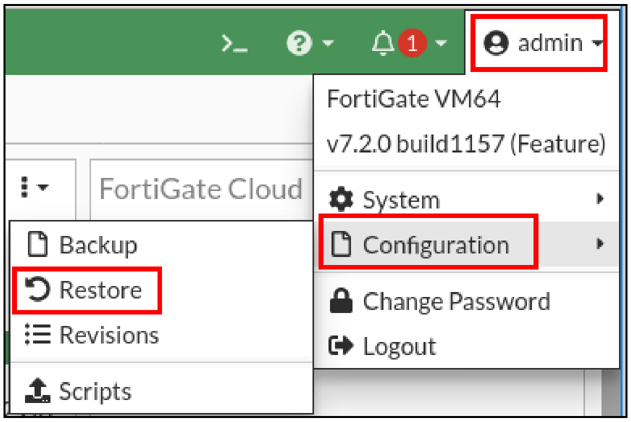
Estimated: 150 minutes

Prerequisites

Before you begin this lab, you must restore the initial configuration files to the FortiGate devices. The configuration files are located on the desktop of the Linux-Client VM.

To restore the FortiGate-1 configuration file

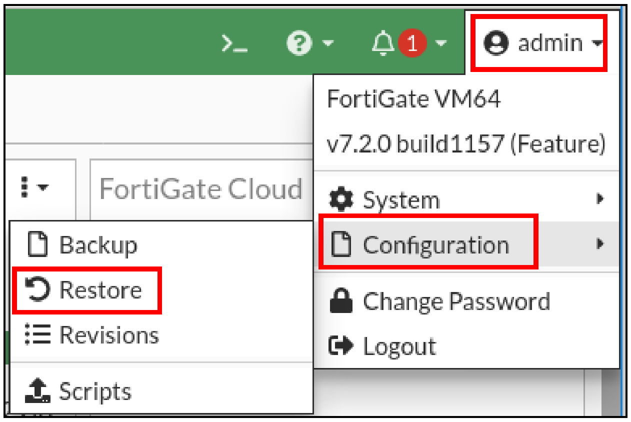
1. Log in to the FortiGate-1 GUI at `10.1.1.1` with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **Use Case-2**, select `FortiGate-1_usecase2.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

To restore the FortiGate-2 configuration file

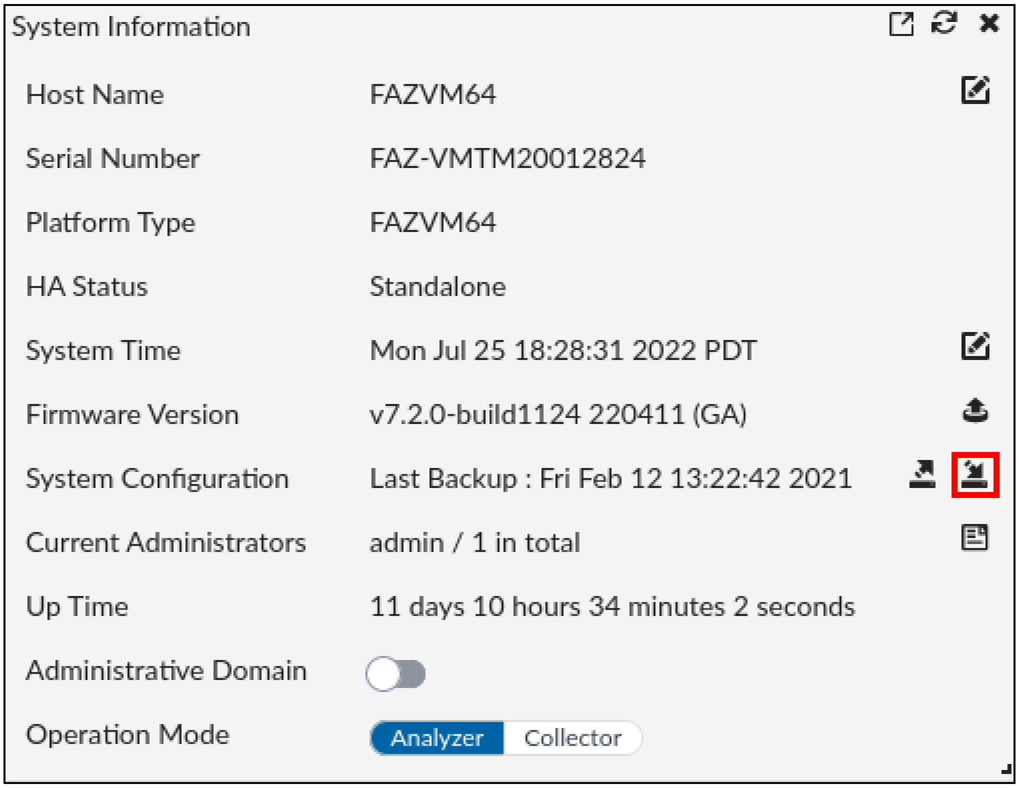
1. Log in to the FortiGate-2 GUI at `10.1.2.1` with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **Use Case-2**, select `FortiGate-2_usecase2.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

To restore the FortiAnalyzer configuration file

1. On the Linux-Client VM, open a browser, and then log in to the FortiAnalyzer GUI at `10.1.3.210` with the username `admin` and password `password`.
2. Click **System Settings**.
3. In the **System Information** widget, in the **System Configuration** field, click the restore icon.



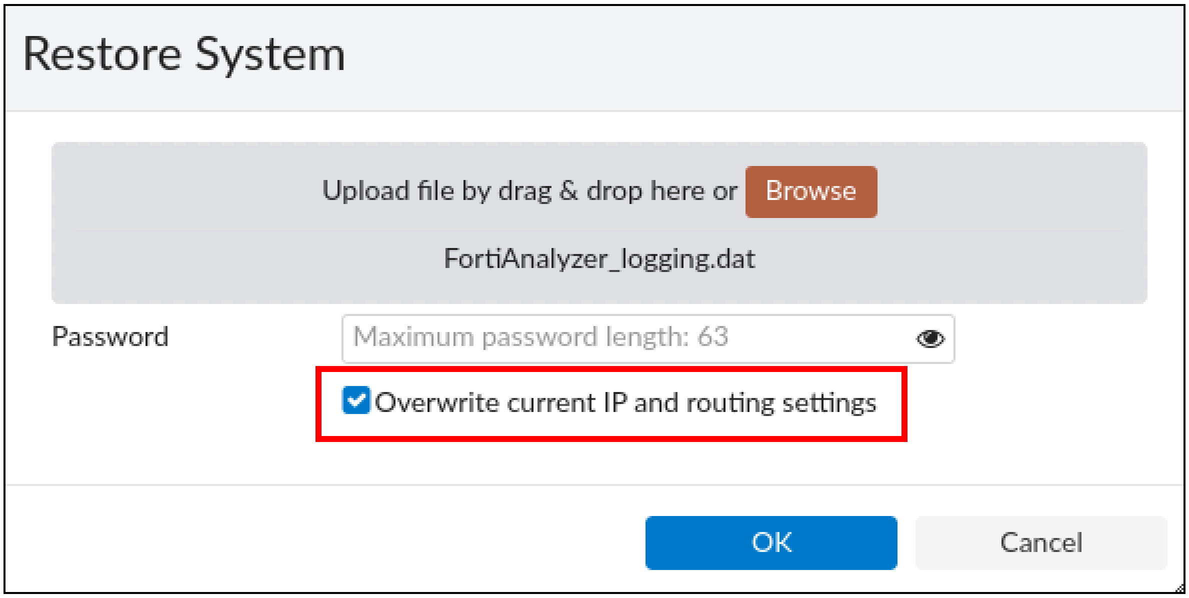
System Information

Host Name	FAZVM64
Serial Number	FAZ-VMTM20012824
Platform Type	FAZVM64
HA Status	Standalone
System Time	Mon Jul 25 18:28:31 2022 PDT
Firmware Version	v7.2.0-build1124 220411 (GA)
System Configuration	Last Backup : Fri Feb 12 13:22:42 2021
Current Administrators	admin / 1 in total
Up Time	11 days 10 hours 34 minutes 2 seconds
Administrative Domain	○
Operation Mode	Analyzer Collector

4. Click **Browse**.
5. Click **Desktop** > **Resources** > **Use Case-2**, and then select `FortiAnalyzer_usecase2.dat`.

You do not have to enter a password because the file is not encrypted.

6. Leave the **Overwrite current IP and routing settings** checkbox selected.



Restore System

Upload file by drag & drop here or Browse

FortiAnalyzer_logging.dat

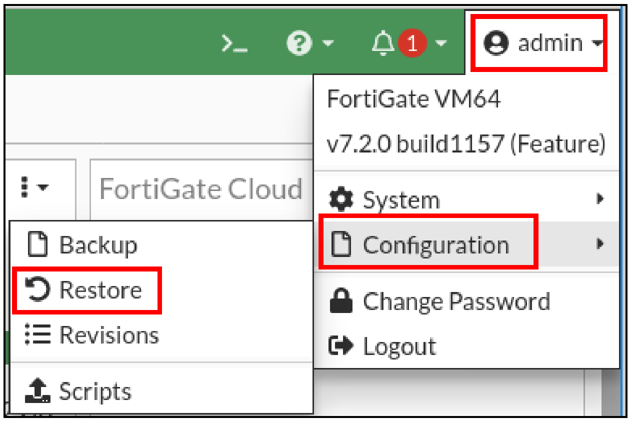
Password: Maximum password length: 63

☑ Overwrite current IP and routing settings

7. Click **OK**.

To restore the Edge-FortiGate configuration file

1. On the Linux-Client VM, open a browser, and then log in to the Edge-FortiGate GUI at `10.1.5.254` with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



FortiGate VM64
v7.2.0 build1157 (Feature)

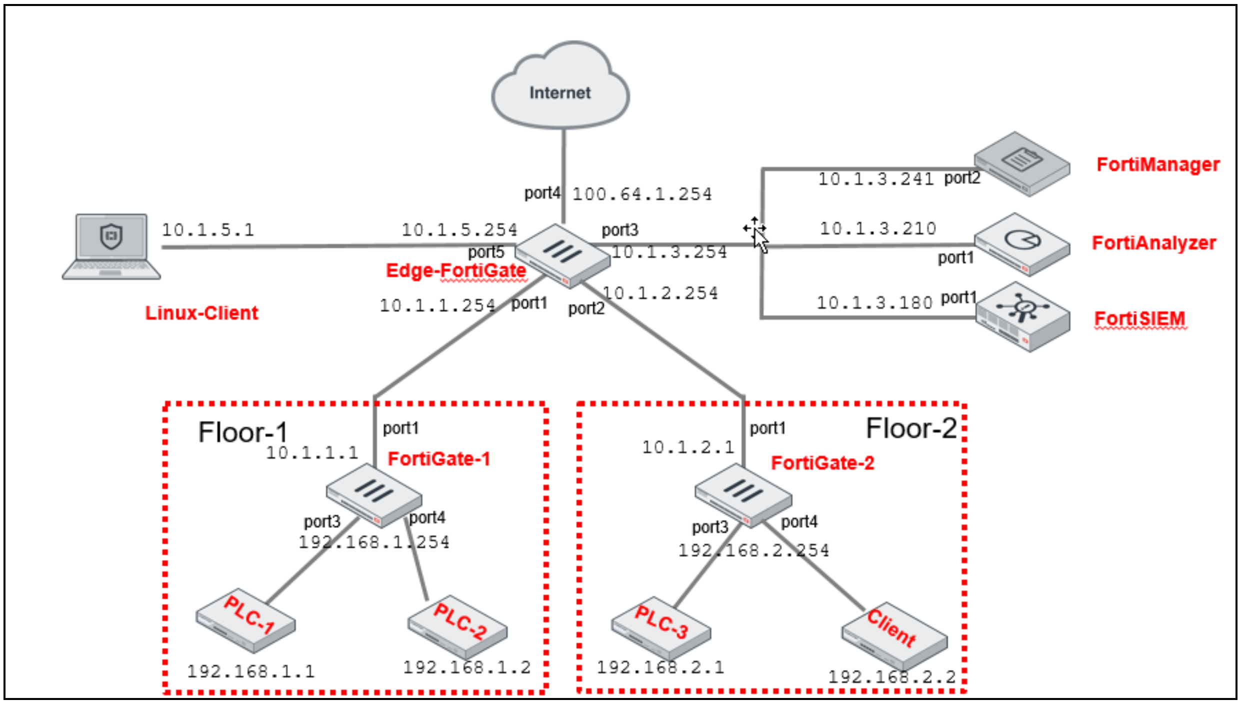
3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **Use Case-2**, select `Edge-FortiGate_usecase2.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

Exercise 1: Configuring Devices

In this exercise, you will configure the OT network based on the following basic customer requirements:

- Configure administrator accounts on the FortiGate devices
- Configure microsegmentation within Floor-1
- Implement segmentation between floors
- Implement access control to limit access to Fortinet devices and PLCs
- Allow only IEC-104 traffic between PLCs based on requirements
- Log traffic on FortiGate, FortiAnalyzer, and FortiSIEM

Network Topology



Review the current configuration before proceeding to the next step. You will have basic connectivity from Fortinet products to FortiManager so that you can perform license verification. Do not make changes to the policies that allow this traffic.

Requirements

To configure administrator accounts

Create the following administrator accounts on FortiGate-1 and FortiGate-2:

Username	Password	Access
supervisor	fortinet	Super admin
admin_1	fortinet	Super admin read-only

To configure basic connectivity

Ensure that the Linux-Client can access the following devices without access control:

- FortiGate-1
- FortiGate-2
- FortiAnalyzer
- FortiSIEM

To achieve microsegmentation within floors

- On Floor-1, make sure that PLC-1 and PLC-2 are in the same broadcast domain.
- Allow only ICMP and SSH traffic from PLC-2 to PLC-1.
- Do not allow any other traffic between PLC-1 and PLC-2.
- On Floor-2, make sure that PLC-3 and the Client VM are in the same broadcast domain.
- Allow all traffic between PLC-3 and the Client VM without using firewall policies.

To segment floors

- Ensure that all traffic between floors is controlled through Edge-FortiGate.
- Configure firewall policies and routes to allow Linux-Client to access PLC-1, PLC-2, PLC-3, and the Client VM over SSH without access control.

To implement access control

Create the following local users on Edge-FortiGate:

Username	Password
supervisor	supervisor
jradmin	jradmin
sradmin	sradmin

Create policies to allow traffic from the Linux-Client VM to the following devices using access control:

- Allow supervisor to access PLC-1, PLC-2, PLC-3, and the Client VM over HTTP.
- Allow jradmin to access PLC-1 over HTTP.
- Allow sradmin to access PLC-3 on Floor-2 over HTTP.

To log traffic

Configure devices so that Edge-Fortigate can:

- Send logs in real time to FortiAnalyzer for storage and reporting
- Send logs to FortiSIEM

To protect the OT network

- Allow and monitor only IEC-104 traffic from PLC-2 to PLC-3, except traffic that matches the **IEC.60870.5.104_Information.Transfer.C.BO.NA.1** signature.
- Block all other industrial signatures from PLC-2 to PLC-3.
- Log all traffic from PLC-2 to PLC-3.

Exercise 2: Testing the Configuration

Make sure you have completed all of the configuration steps before testing the configuration.

To configure administrator accounts

- You must be able to log in to FortiGate-1 and FortiGate-2 with the username `supervisor` and password `fortinet`.
  - After you log in, you must have read and write access to all features on the FortiGate devices.
- You must be able to log in to FortiGate-1 and FortiGate-2 with the username `admin_1` and password `fortinet`.
  - After you log in, you must have read-only access to all features on the FortiGate devices.

To test basic connectivity

From the Linux-Client VM, you must be able to access the following devices:

- FortiGate-1 at `10.1.1.1` over HTTP and SSH
- FortiGate-2 at `10.1.2.1` over HTTP and SSH
- FortiAnalyzer at `http://10.1.3.210` over HTTP and SSH
- FortiSIEM at `https://10.1.3.180`

To test microsegmentation within floors

- From PLC-2, you should be able to ping and connect over SSH to PLC-1.
- You must not be able to ping PLC-2 from PLC-1.
- You should be able to send any traffic between PLC-3 and the Client VM.
- Firewall policies on FortiGate-2 must not allow or deny traffic between PLC-3 and the Client VM.

To test internal segmentation

- You must not be able to ping PLC-3 from PLC-1.
- You must not be able to ping the Client VM from PLC-1.
- PLC-3 must not be able to ping any devices on Floor-1.
- Linux-Client must be able to connect to PLC-1, PLC-2, PLC-3, and the Client VM over SSH.

To test access control

- On the Linux-Client VM, when you access PLC-1, PLC-2, PLC-3, and the Client VM over HTTP, you must receive a login prompt.
- The following users must be able to access the allowed devices over HTTP only:

Username	Allowed devices over HTTP
supervisor	PLC1, PLC-2, PLC-3, and the Client VM
jradmin	PLC-1
sradmin	PLC-3

If you do not see another login prompt after you are logged in with one user, do the following:

1. Click **Dashboard** > **Users & Devices**, and then expand **Firewall Users** to deauthenticate the user.
2. Close all browsers to clear the caches.

To test application filter and logging

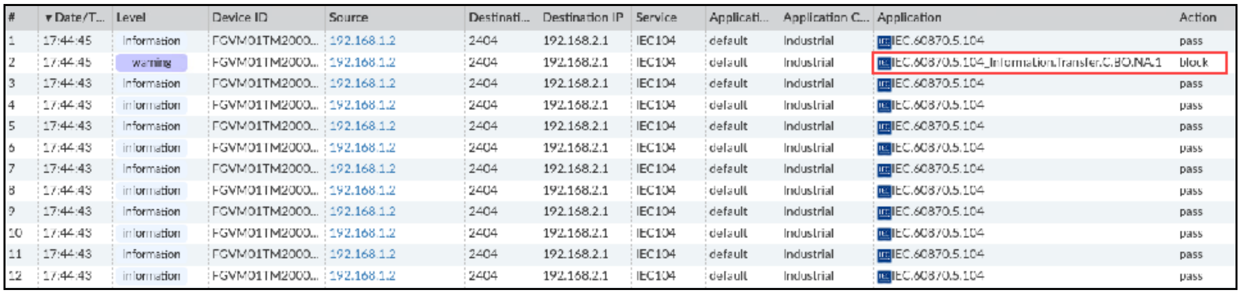
1. Connect to the Linux-Client VM.
2. On the Linux-Client VM, open PuTTY.
3. Click **PLC-3** to select the saved session, and then click **Open**.
4. Log in with the username `sysadmin` and password `Fortinet1!`.
5. Enter the following command:

```
cd Uploads/iecsim/
python3 demo_server.py 1000 2000
```

6. Leave the PuTTY session open.
7. Connect to the Linux-Client VM.
8. On the Linux-Client VM, open PuTTY.
9. Click **PLC-2** to select the saved session, and then click **Open**.
10. Log in with the username `sysadmin` and password `Fortinet1!`.
11. Enter the following command:

```
cd Uploads/iecsim/
python3 demo_client.py 192.168.2.1 1000 1010
```

12. Leave the PuTTY session open.
13. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
14. Click **Log View**.
15. In the menu on the left, click **FortiGate** > **Security** > **Application Control**.
16. Ensure that you see the following result:



#	▾Date/T...	Level	Device ID	Source	Destinati...	Destination IP	Service	Applicati...	Application C...	Application	Action
1	17:44:45	Information	FGVM01TM2000...	192.168.1.2	2404	192.168.2.1	IEC104	default	Industrial	IEC.60870.5.104	pass
2	17:44:45	warning	FGVM01TM2000...	192.168.1.2	2404	192.168.2.1	IEC104	default	Industrial	IEC.60870.5.104_Information.Transfer.C.BO.NA.1	block
3	17:44:43	Information	FGVM01TM2000...	192.168.1.2	2404	192.168.2.1	IEC104	default	Industrial	IEC.60870.5.104	pass
4	17:44:43	information	FGVM01TM2000...	192.168.1.2	2404	192.168.2.1	IEC104	default	Industrial	IEC.60870.5.104	pass
5	17:44:43	Information	FGVM01TM2000...	192.168.1.2	2404	192.168.2.1	IEC104	default	Industrial	IEC.60870.5.104	pass
6	17:44:43	information	FGVM01TM2000...	192.168.1.2	2404	192.168.2.1	IEC104	default	Industrial	IEC.60870.5.104	pass
7	17:44:43	Information	FGVM01TM2000...	192.168.1.2	2404	192.168.2.1	IEC104	default	Industrial	IEC.60870.5.104	pass
8	17:44:43	information	FGVM01TM2000...	192.168.1.2	2404	192.168.2.1	IEC104	default	Industrial	IEC.60870.5.104	pass
9	17:44:43	Information	FGVM01TM2000...	192.168.1.2	2404	192.168.2.1	IEC104	default	Industrial	IEC.60870.5.104	pass
10	17:44:43	information	FGVM01TM2000...	192.168.1.2	2404	192.168.2.1	IEC104	default	Industrial	IEC.60870.5.104	pass
11	17:44:43	Information	FGVM01TM2000...	192.168.1.2	2404	192.168.2.1	IEC104	default	Industrial	IEC.60870.5.104	pass
12	17:44:43	information	FGVM01TM2000...	192.168.1.2	2404	192.168.2.1	IEC104	default	Industrial	IEC.60870.5.104	pass

FORTINET