

DO NOT REPRINT

© FORTINET



FortiSIEM Lab Guide

for FortiSIEM 6.3

FORTINET

NSE Training Institute

Fortinet Training

<https://training.fortinet.com>

Fortinet Document Library

<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 Support

<https://support.fortinet.com>

FortiGuard Labs

<https://www.fortiguards.com>

Fortinet Network Security Expert Program (NSE)

<https://training.fortinet.com/local/staticpage/view.php?page=certifications>

Fortinet | Pearson VUE

<https://home.pearsonvue.com/fortinet>

Feedback

Email: askcourseware@fortinet.com



12/19/2021

TABLE OF CONTENTS

Network Topology	8
Lab 1: FortiSIEM Introduction	9
Exercise 1: Creating Roles	10
Create a New Role	10
Exercise 2: Creating New Users	15
Create New Users	15
Exercise 3: Changing Local User Passwords	19
Change Local User Passwords	19
Lab 2: SIEM and PAM Concepts	21
Exercise 1: Reviewing Incoming Data	22
Create a Search Filter	22
Generate Events	23
View Raw Event Logs	24
Exercise 2: Reviewing Structured Data	25
View Structured Data	25
Exercise 3: Reviewing Event Classification	28
Inspect Event Classification	28
Exercise 4: Reviewing Event Enrichment	31
Configure a Search Filter	31
Generate Events	32
Inspect Event Enrichment	33
Exercise 5: Reviewing Performance Events	37
Configure a Search Filter	37
Generate Performance Event Logs	38
View Performance Event Enrichment	38
Lab 3: Discovery	41
Exercise 1: Inspecting Syslog Data	42
Configure Search Filter Criteria	42
Generate Test Logs	43
Inspect Discovered Devices	43
Exercise 2: Adding Credentials and IP Ranges for a Single Device	47
Configure SNMP Credentials	47
Prepare for Discovery	48

Exercise 3: Discovering a Single Device	50
Configure Discovery	50
Generate Scripted Performance Data	51
Exercise 4: Performing Discovery of Other Lab Devices	54
Populate the Credential and Discovery Ranges of Other Devices	55
Prepare the Simulated Devices for Discovery	56
Exercise 5: Bringing in Scripted Data	61
Pull Data From Devices	61
Lab 4: FortiSIEM Analytics	65
Exercise 1: Getting to Know the Real-Time Search	66
View Raw Logs	66
Exercise 2: Exploring Search Operators	70
Use Search Operators	70
Exercise 3: Using the Historical Keyword Search	72
Perform a Keyword Search	72
Exercise 4: Using Single Search Conditions	74
Configure a Search Condition	74
Exercise 5: Using Multiple Search Conditions	76
Add Multiple Search Conditions	76
Exercise 6: Using the CONTAIN Operator	77
Examine the Use of the CONTAIN Operator	77
Exercise 7: Using the IN and NOT IN Operators	80
Examine the Use of the IN and NOT IN Operators	80
Exercise 8: Using the IS NOT Operator	82
Examine the Use of the IS NOT Operator	82
Exercise 9: Using the Greater Than Operator	85
Examine the Use of the > Operator	85
Lab 5: CMDB Lookups and Filters	87
Exercise 1: Selecting Devices From the CMDB	88
Build a Query Using Devices From the CMDB	88
Exercise 2: Searching for Categories of Events	95
Build a Query Using Categories From the CMDB	95
Exercise 3: Expert Challenge	100
Conduct a Historical Search	100
Lab 6: Group By and Aggregation	103
Exercise 1: Grouping By Single and Multiple Attributes	104
Create a Search Filter Criteria	104
Apply the Group By Criteria	105
Exercise 2: Aggregating Data	110
Create a Search Filter Criteria	110

Configure Display Fields for Aggregation.....	111
Exercise 3: Expert Challenge.....	116
Conduct a Historical Search.....	116
Lab 7: Rules.....	118
Exercise 1: Exploring a Simple Rule.....	119
Examine a Rule.....	119
Configure Search Filter Criteria.....	121
Examine an Incident.....	122
Exercise 2: Exploring a Performance Rule.....	124
Examine a Performance Monitoring Rule.....	124
Generate Scripted Performance Events.....	130
Examine Performance Events and Incidents.....	131
Exercise 3: Creating a Rule.....	133
Configure Search Filter Criteria.....	133
Generate Scripted Events.....	134
Examine the Generated Events.....	134
Create a Rule.....	137
Generate Scripted Events.....	139
Examine the Triggered Incident.....	139
Exercise 4: Enhancing a Rule With a Watch List.....	141
Configure a Watch List.....	141
Generate Scripted Events.....	143
Examine the Generated Events.....	143
Exercise 5: Importing a Rule.....	145
Import a Rule.....	145
Lab 8: Incidents and Notification Policies.....	148
Exercise 1: Reviewing the Incident Table.....	149
View Incidents.....	149
Exercise 2: Grouping and Tuning Incidents.....	157
Examine a Group of Incidents.....	157
Tune Incidents.....	159
Exercise 3: Using the Built-In Ticketing System.....	160
Review Incidents for Suspicious Activity.....	160
Create a Case in the Ticketing System.....	161
Exercise 4: Creating a Custom Email Template.....	165
Configure Email Settings.....	165
Exercise 5: Creating a Notification Policy.....	167
Import a Rule.....	167
Generate Incidents to Trigger a Notification Policy.....	170
Examine the Ticket Created by the Notification Policy.....	171
Lab 9: Reporting.....	173

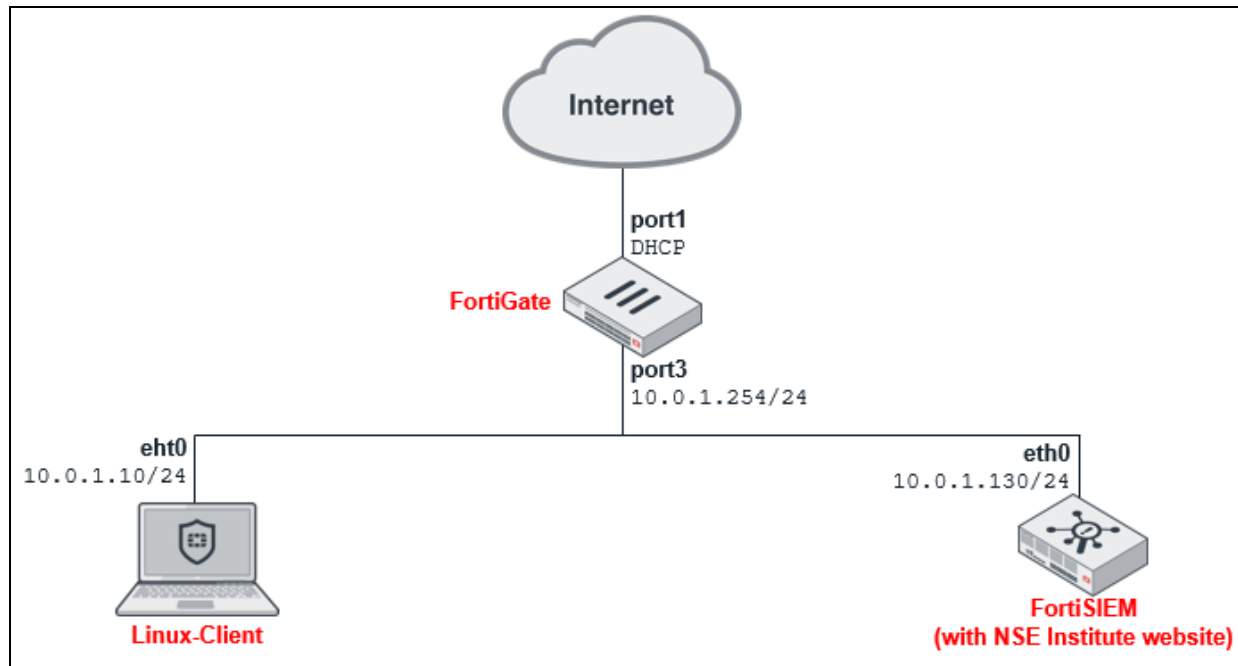
Exercise 1: Opening a Report From the Analytics Page	174
Examine a Report From the Analytics Page	174
Create a Report Template	176
Exercise 2: Opening a Report From the Report Tree	180
Run a Report From the Report Tree	180
Exercise 3: Scheduling a Report	181
Schedule a Report	181
Configure an Alternative Scheduling Method	183
Exercise 4: Creating Custom Dashboards	184
Create a Custom Dashboard	184
Configure a Summary Dashboard	185
Configure a Widget Dashboard	187
Exercise 5: Examining Dashboard Drill-Down Capabilities	192
Drill Down on Dashboard Content	192
Exercise 6: Importing and Exporting Dashboards	195
Export a Dashboard	195
Import a Dashboard	195
Exercise 7: Running CMDB Reports	197
Run a CMDB Report	197
Exercise 8: Building a Custom CMDB Report	199
Create a Custom CMDB Report	199
Lab 10: Business Services	202
Exercise 1: Creating a Business Service	203
Create a Business Service	203
Exercise 2: Monitoring Business Service Incidents	206
Generate Business Service Related Incidents	209
Examine Business Service Incidents	210
Exercise 3: Using the Business Services Dashboard	212
Create a Business Services Dashboard	212
View the Business Services Dashboard Details	214
Reference Business Services in an Analytics Search	216
Lab 11: Troubleshooting	218
Exercise 1: Troubleshooting Device Discovery	219
Configure SNMP on FortiGate	219
Add Credentials for FortiGate	220
Discover FortiGate	221
Configure FortiSIEM for Network Discovery	222
Troubleshoot the Discovery of a FortiGate	223
Verify the Fix	225
Exercise 2: Troubleshooting Privileged Credentials for Configuration Pulling	228
Configure Privileged Credentials	228

Troubleshoot Pull Data Using Privileged Credentials.....229

Resolve the Issue.....231

Appendix: Answer Sheet.....236

Network Topology



Lab 1: FortiSIEM Introduction

In this lab, you will examine role-based access control (RBAC).

Objectives

- Create a role
- Create new users
- Apply roles to users
- Change local passwords

Time to Complete

Estimated: 15 minutes

Exercise 1: Creating Roles

In this exercise, you will create a new manager role.

Create a New Role

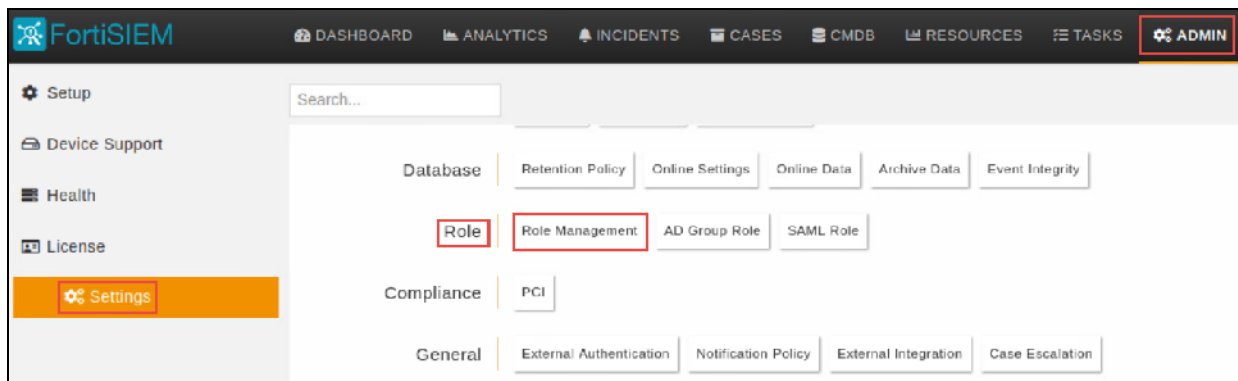
You will create a new role by cloning an existing system-defined role.

To clone a system-defined role

1. On the FortiSIEM GUI, log in with the following credentials:

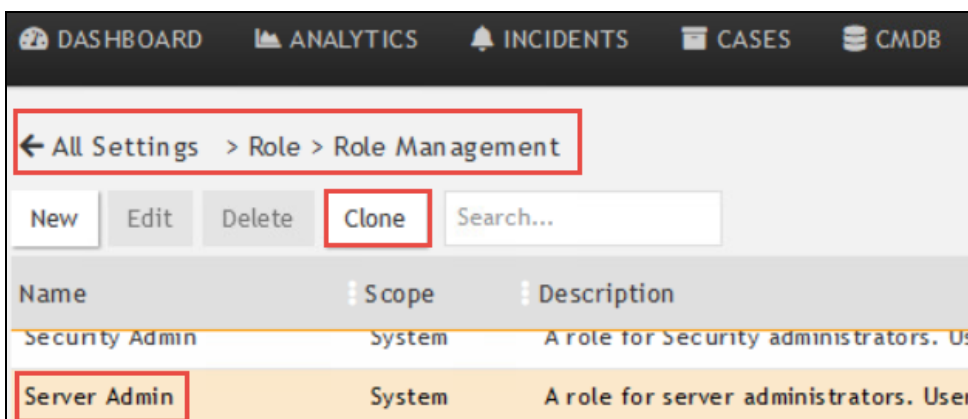
Field	Value
User ID	admin
Password	Fortinet1!
Domain	LOCAL

2. Click **LOG IN**, and then click **Accept** to accept the disclaimer.
3. Click the **ADMIN** tab.
4. In the left pane, select **Settings**, and then under **Role**, click **Role Management**.



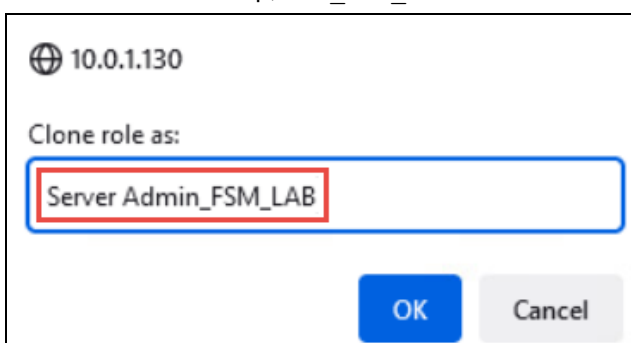
Review the default system roles that are available.

5. Click the **Server Admin** role, and then select **Clone**.



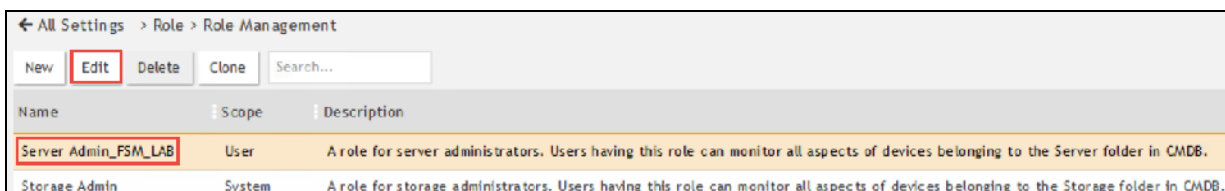
Because FortiSIEM does not allow you to overwrite the out-of-box system roles, the system prompts you to save the role with a different name. By default, it adds a date stamp.

- Remove the date stamp, add `_FSM_LAB` to the role name, and then click **OK**.

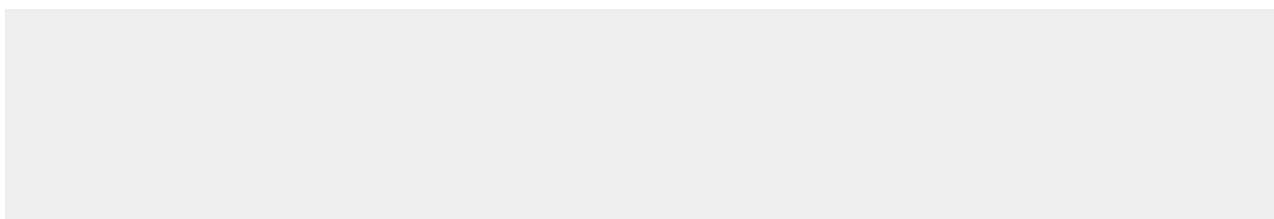


To review the settings for a cloned role

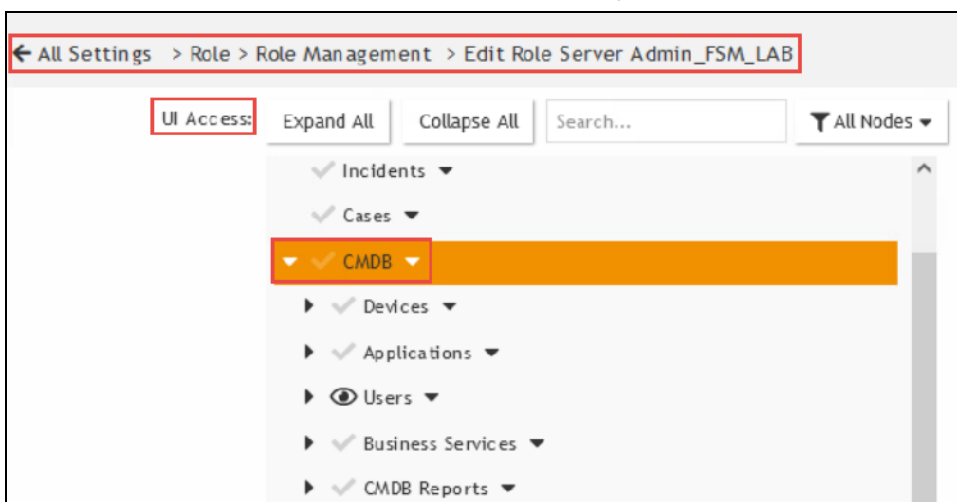
- Continuing on the FortiSIEM GUI, select the cloned role **Server Admin_FSM_LAB**, and then click **Edit**.



- Review the information in the **Data Conditions** and **CMDB Report Conditions** sections for this role. What do you understand about these fields? See ["Appendix: Answer Sheet"](#) on page 236 for the answer.

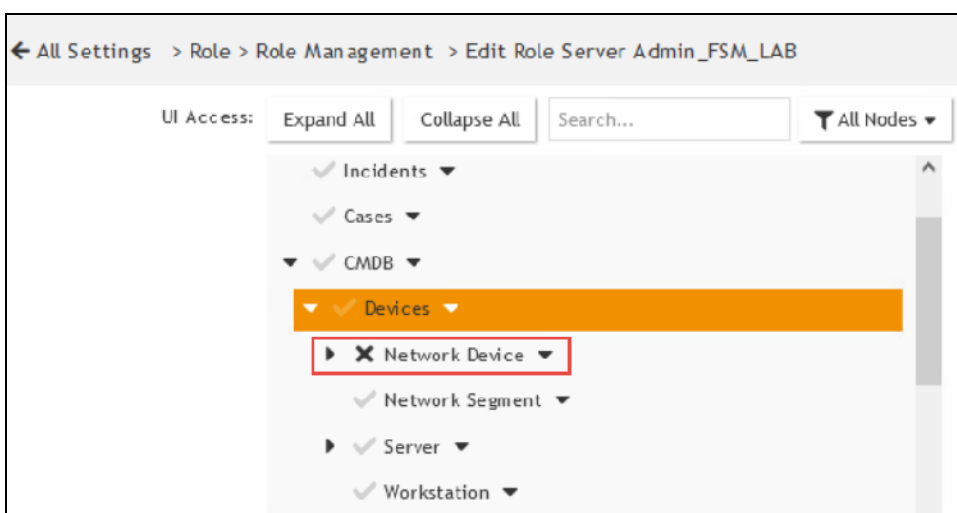


3. Scroll down, review the **UI Access** section, and then expand **CMDB** to see the conditions that apply to this role.



4. Expand **Devices**.

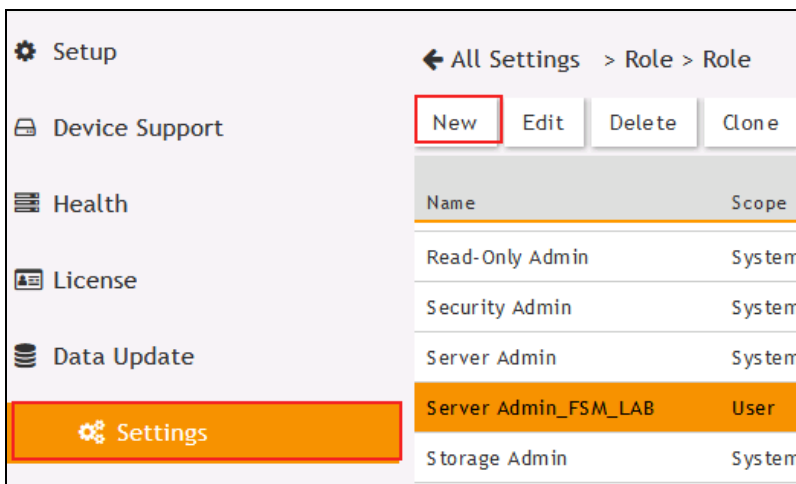
Notice how all network devices are hidden but server devices are accessible.



5. Review the list.
6. Click **Cancel**.

To create a new role

1. Continuing on the FortiSIEM GUI, click **New** to create a role.



- In the **Role Name** field, type `Lab1 - Manager View`.
- In the **Data Conditions** section, configure the following settings:

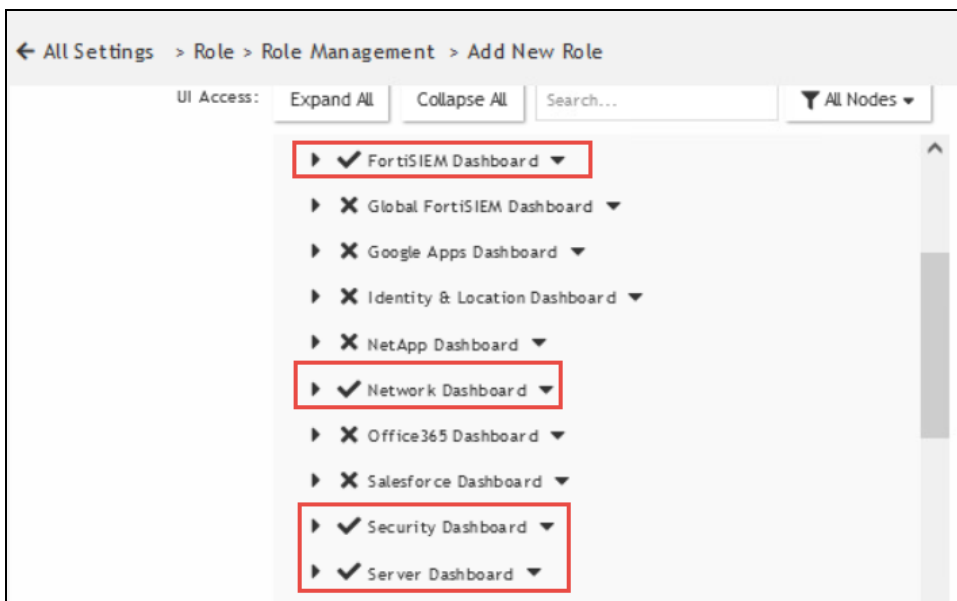
Field	Value
Attribute	Reporting IP
Operator	IN
Value	- Click in the Value search bar, and then select Select from CMDB. - In the left pane, expand Devices, and then expand Network Device. - Select Firewall, and then click >> to move it to the Selections pane. - Click OK.

- Leave the **CMDB Report Conditions** section blank.
- In the **UI Access** section, expand **Dashboard**, and then allow **Full** access to the following dashboards:
 - FortiSIEM Dashboard
 - Network Dashboard
 - Security Dashboard
 - Server Dashboard

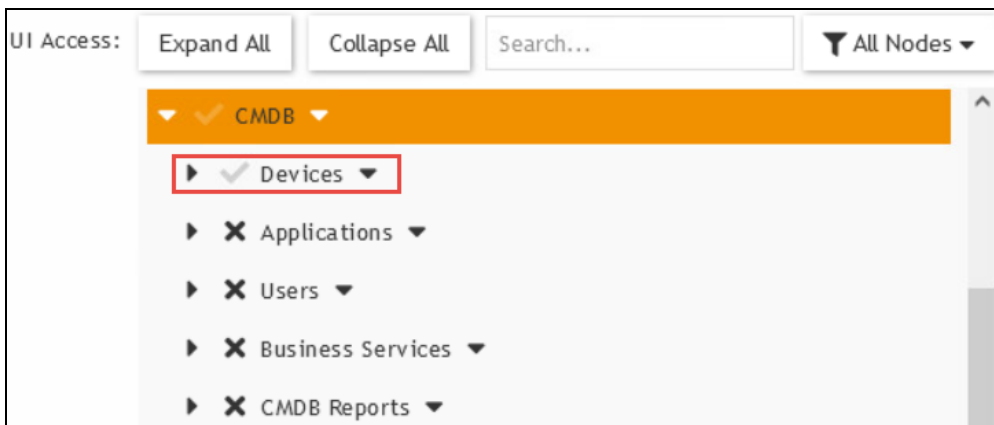


Click the item, and then select the down arrow to change its status.

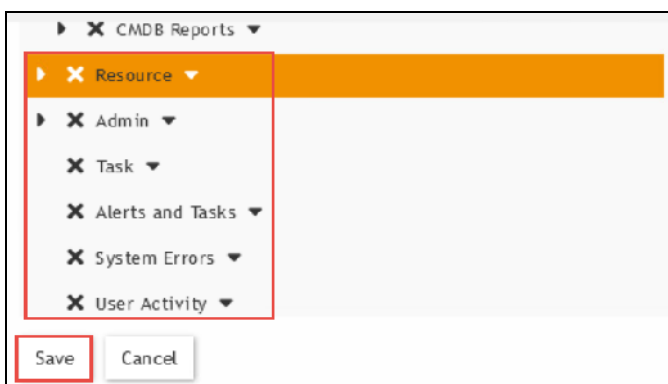
- Hide the rest of the dashboards, and then click **Save**.



7. Leave the **Analytics**, **Incidents**, and **Cases** settings at the default values.
8. Click **CMDB**, and then hide all settings except **Devices**.



9. Hide **Others**.



10. Click **Save**.
11. Log out of the FortiSIEM GUI.

Exercise 2: Creating New Users

In this exercise, you will create two new users: a manager account and your own user account.

Create New Users

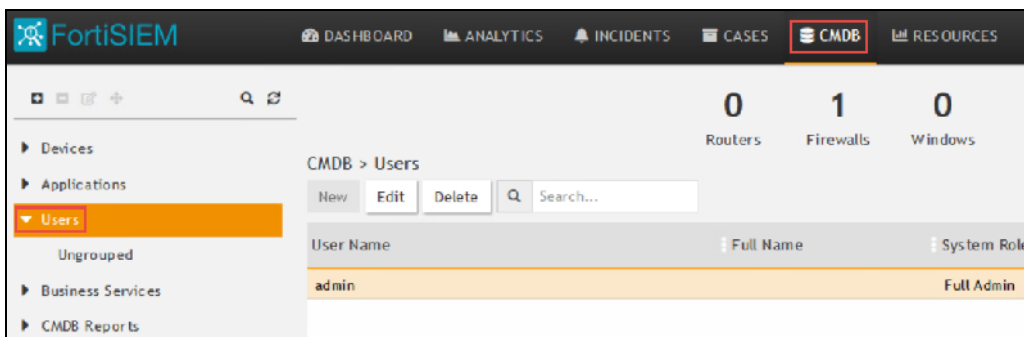
You will create two new users.

To create new users

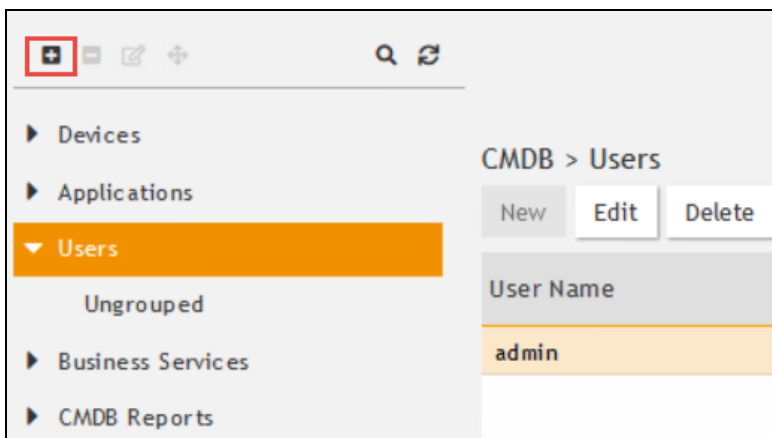
1. On the FortiSIEM GUI, log in with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Domain	LOCAL

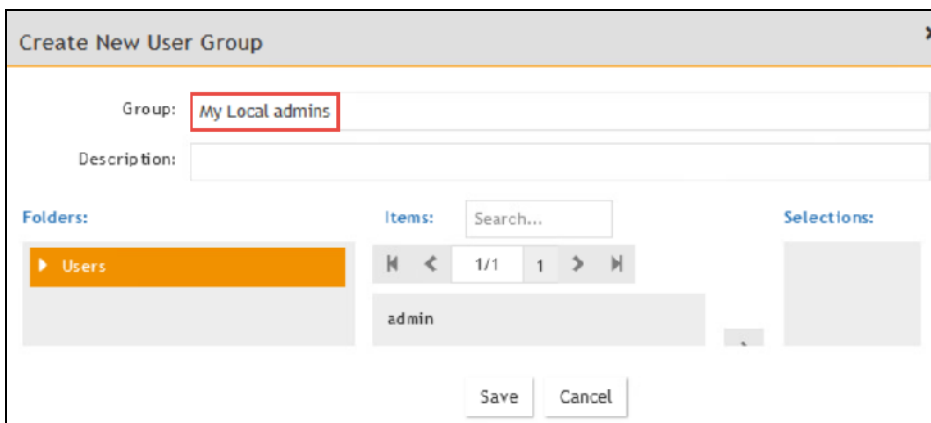
2. Click the **CMDB** tab, and then in the left pane, select **Users**.



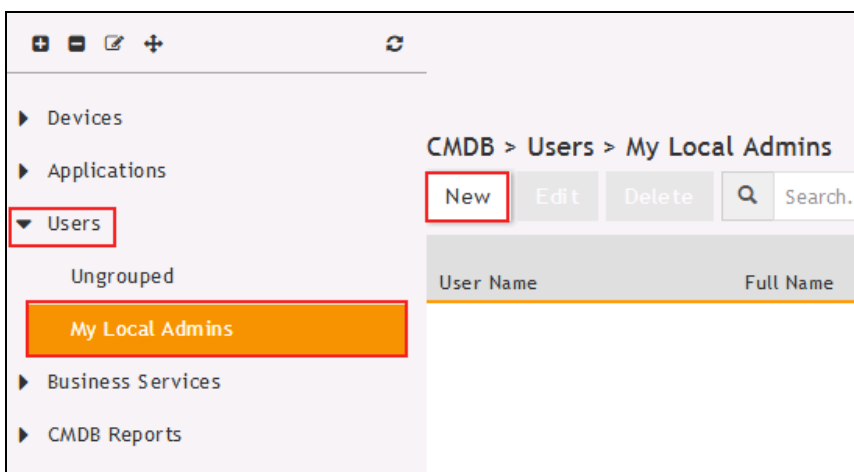
3. At the top of the tree, click the plus icon (+).



4. In the **Group** field, type `My Local admins`, and then click **Save**.



5. Expand the **Users** tree, and then select the new **My Local Admins** folder.
6. Click **New** to create a new user.



7. Configure the following settings:

Field	Value
User Name	manager
System Admin	Click in the empty box to prompt a dialog box to open.
Mode	Local
Password	Fortinet2!
Confirm Password	Fortinet2!
Default Role	Lab1 - Manager View

8. Click **Back**.

New User

Agent Admin: ☐

Mode: Local

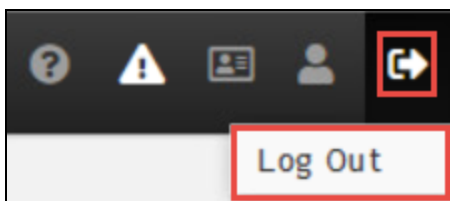
Password:

Confirm Password:

Default Role: Lab1 - Manager View

Back

9. Click **Save**.
10. Click the arrow icon in the top toolbar to log out of the FortiSIEM GUI.



To verify the settings for the newly created account

1. Log in to the FortiSIEM GUI with the following credentials:

Field	Value
User ID	manager
Password	Fortinet2!
Domain	LOCAL
Disclaimer	Accept

Stop and think!

Notice how various parts of the GUI are no longer visible.

2. Click the **Dashboard** tab.
Notice how you can see only the few dashboards you specified previously.
3. Click the **Analytics** tab.

Notice how it contains the **Real-time Search** and **Reports** options. Because of the restrictions on the role, if you were to perform a real-time search, the events returned would come only from devices that the role is allowed to view.

4. Click **CMDB**, and then notice it shows only **Devices**, which you selected previously for the role.
5. Log out of the FortiSIEM GUI as the manager, and then log back in as the admin user with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Domain	LOCAL

6. Click the **CMDB** tab, and then in the left pane, click **Users**.
7. Select **My Local Admins**.
8. Click **New** to create your own user account.
9. Configure the following settings:

Field	Value
User Name	<select a username>
System Admin	Click in the empty box to prompt a dialog box to open.
Mode	Local
Password	Fortinet3!
Confirm Password	Fortinet3!
Default Role	Full Admin

Note that this new user is using the **Full Admin** role.

10. Click **Back**.
11. Click **Save** to save your new user account.
12. Log out of the FortiSIEM GUI.

Exercise 3: Changing Local User Passwords

In this exercise, you will change your user password.

Change Local User Passwords

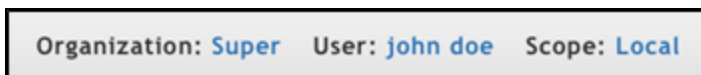
You will change the password for your user account that you created in the previous exercise.

To change local user passwords

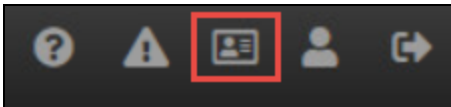
1. Log in to the FortiSIEM GUI with your user account.

Field	Value
User ID	<the name you selected>
Password	Fortinet3!
Domain	LOCAL

Notice that your username and current role are listed at the bottom of the screen.



2. In the upper-right corner of the window, click the user profile icon.



3. In the **Password** and **Confirm Password** fields, type a new password, and then click **Save**.



The password must contain at least one number and one special character (!@#%\$%^*(),.?). You can use Fortinet4!.

The screenshot shows a web-based 'Edit User Profile' window. It has a title bar with a close button. Below the title bar are three tabs: 'Basic', 'Contact', and 'UI Settings'. The 'Basic' tab is active. Under the 'Basic' tab, there are four input fields: 'User Name' (containing 'John doe'), 'Full Name' (empty), 'Password' (masked with dots), and 'Confirm Password' (masked with dots). At the bottom right of the form are two buttons: 'Save' and 'Cancel'. The 'Save' button is highlighted with a red rectangular box.

4. Log out of the FortiSIEM GUI.
5. Log in again using the new password, and then verify that it is working.
6. Log out of the FortiSIEM GUI.

Lab 2: SIEM and PAM Concepts

In this lab, you will explore how FortiSIEM processes each log into an event type.

Objectives

- View raw event logs
- View structured data
- Inspect event classification
- Inspect event enrichment
- Review performance events

Time to Complete

Estimated: 45 minutes

Exercise 1: Reviewing Incoming Data

In this exercise, you will review the raw events that have been received by syslog.

Create a Search Filter

You will create a search filter on FortiSIEM.

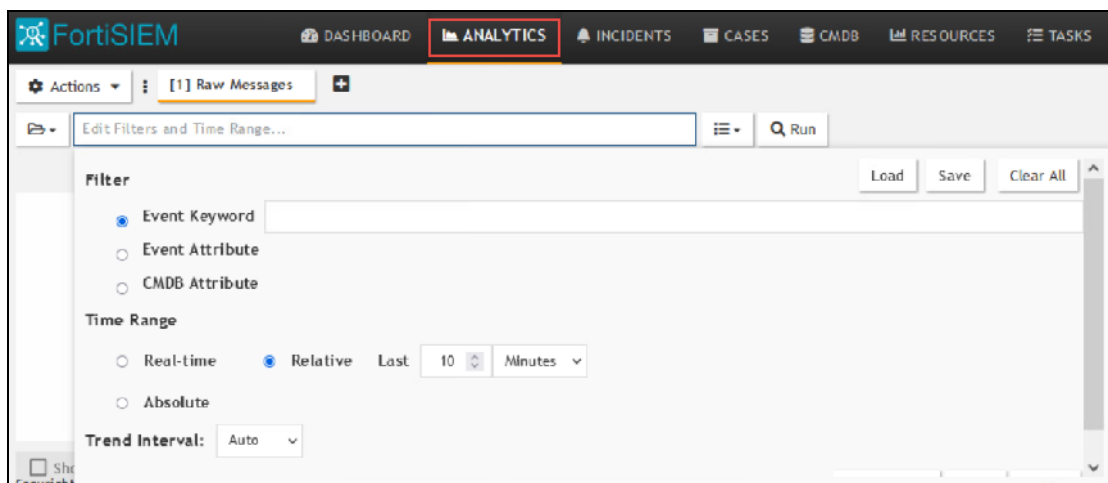
To set search filter criteria

1. Log in to the FortiSIEM GUI with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Domain	LOCAL

2. Click the **ANALYTICS** tab.
3. Click the search field to edit the condition.

The filter editor opens.



4. In the **Filter** section, select the **Event Attribute** option, and then create the following query:

Field	Value
Attribute	Reporting IP
Operator	=
Value	192.168.3.2

5. In the **Time Range** section, select **Real-time**.
6. Click **Apply & Run**.

Filter

Load Save Clear All

☐ Event Keyword

☒ Event Attribute

Paren	Attribute	Operator	Value	Paren	Next	Row
+	Reporting IP	=	192.168.3.2	-	AND	+ -

☐ CMDB Attribute

Time Range

☒ Real-time ☐ Relative

☐ Absolute

Trend Interval: Auto

Apply & Run Apply Cancel

Generate Events

You will generate some scripted events.

To generate logs

1. On the Linux-Client VM, open a browser, and then go to the NSE Institute website.
https://10.0.1.130/NSE_Institute/index.php



There is a link in the browser favorites bar.

2. On the NSE Institute website, click **LABS SET 1**, and then under **Lab 2 – SIEM and PAM Concepts**, click **Exercise 2.1 – Raw Events**.

The output should resemble the following example:

Running Data Input for Lab Exercise 2.1

sending events from file /var/www/html/NSE_Institute/labs/LAB2/A/events_lab2a.dat
5 messages sent

Completed!

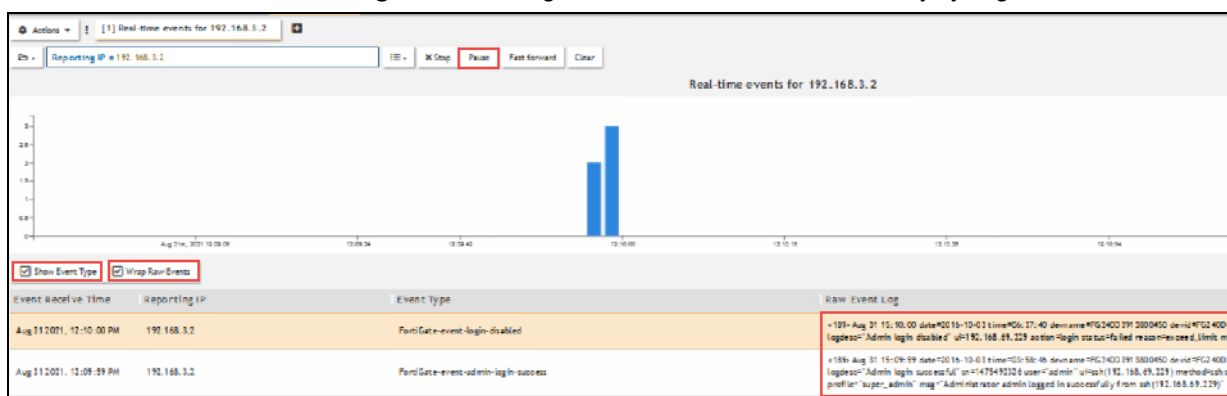
3. Close the Linux-Client VM browser tab.

View Raw Event Logs

You will view the raw event logs of the events you generated from the NSE Institute website.

To view raw event logs

1. Return to the FortiSIEM GUI, and then after five events are received in the table, click **Pause**.
2. To view the type, select **Show Event Type**.
3. To view the full raw log message, select **Wrap Raw Event**.
4. In the table, in the **Raw Event Log**, review the log details for each event received by syslog.



Stop and think!

Can you identify which device they came from?

Which users had failed logins? See "[Appendix: Answer Sheet](#)" on page 236 for the answer.

5. Leave the window that displays the events open, and then continue to the next exercise.

Exercise 2: Reviewing Structured Data

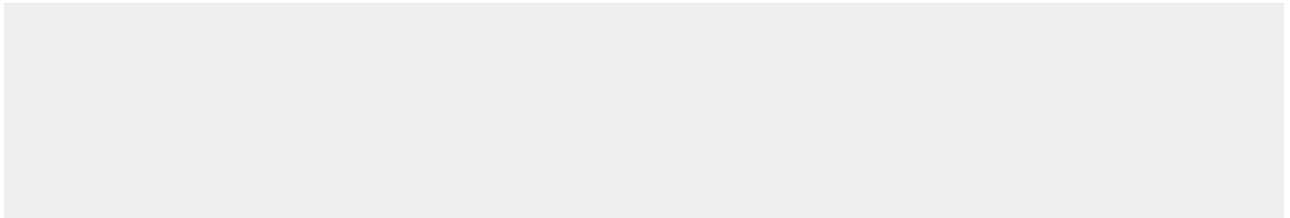
In this exercise, you will review the normalization of raw events into structured data.

View Structured Data

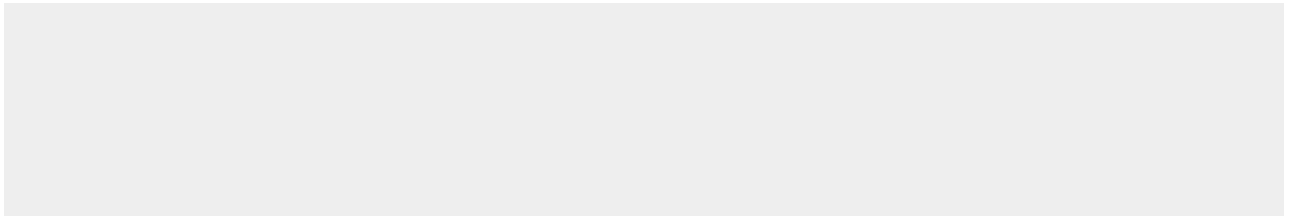
You will examine the raw event log from the previous exercise.

To view structured data

1. Using the analytics results from the previous exercise, make a note of each field header in the table (that is, **Event**, **Receive Time**, and so on).
See "[Appendix: Answer Sheet](#)" on page 236 for the answer.
FortiSIEM refers to these as **Attributes**.

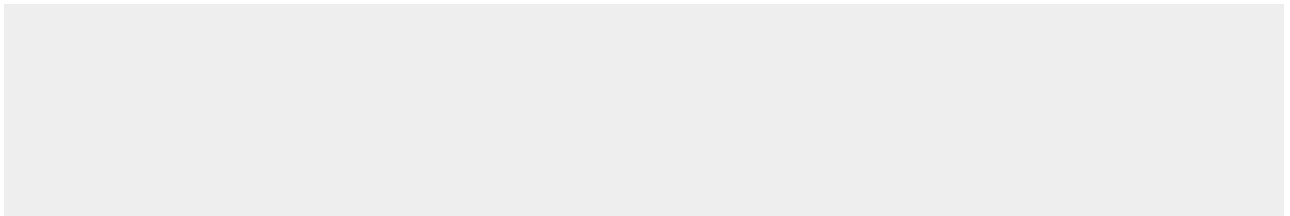


Which attribute relates to the device IP address that sent the data? See "[Appendix: Answer Sheet](#)" on page 236 for the answer.



Notice how each raw event log maps to a specific event type.

Which event type relates to a login failure? See "[Appendix: Answer Sheet](#)" on page 236 for the answer.



2. In the **Raw Event Log** field, select a login event that was successful.
A right arrow icon  appears.

Event Type	Raw Event Log
FortiGate-event-login-disabled	<189>Aug 31 15:10:00 date=2016-10-03 time=06:37:40 devname=FG240D3913800450 devid=FG240D3913800441 logid=0100032021 type=event subtype=system level=alert vd=root logdesc="Admin login disabled" ui=192.168.69.229 action=login status=failed reason=exceed_limit msg="Login disabled from IP 192.168.69.229 for 60 seconds because of 3 bad attempts"
FortiGate-event-admin-login-success	<189>Aug 31 15:09:59 date=2016-10-03 time=03:58:44 devname=FG240D3913800450 devid=FG240D3913800441 logid=0100032001 type=event subtype=system level=information vd=root logdesc="Admin login successful" src=1475492326 user="admin" ui=ssh(192.168.69.229) method=ssh src_ip=192.168.69.229 dst_ip=192.168.3.2 action=login status=success reason=none profile="super_admin" msg="Administrator admin logged in successfully from ssh(192.168.69.229)"

- Click the right arrow icon.

The **Event Details** dialog box opens.

Event Details

```
<189>Aug 31 15:10:00 date=2016-10-03 time=06:37:40 devname=FG240D3913800450
devid=FG240D3913800441 logid=0100032021 type=event subtype=system level=alert vd=root
logdesc="Admin login disabled" ui=192.168.69.229 action=login status=failed
reason=exceed_limit msg="Login disabled from IP 192.168.69.229 for 60 seconds because of
3 bad attempts"
```

Search...

Lines: 34

Display	Filter	Item	Value
☐	☐	Collector ID	1
☐	☐	Count	1
☐	☐	Description	Admin login disabled
☐	☐	Device Time	06:37:40 AM, 03/03/2016
☐	☐	Event Action	0
☐	☐	Event ID	3007137913689548372
☐	☐	Event Parse Status	1
☐	☐	Event Parser Name	FortiGateParser
☒	☐	Event Receive Time	Aug 31 2016, 12:10:00 PM

OK Close

The window includes both the raw log details and a more structured view of the log details.

- In the structured **Event Details** view, review the attributes that FortiSIEM has normalized the raw event log into. Which attribute provides the local time when FortiGate actually logged the event? See "[Appendix: Answer Sheet](#)" on page 236 for the answer.

What are the **Reporting Model** and **Reporting Vendor** attributes of the event? See "[Appendix: Answer Sheet](#)" on page 236 for the answer.

5. Review the raw event log view and look at which protocol was used for the authentication (HTTPS or SSH). What attribute did FortiSIEM map this to in the structured view? See "[Appendix: Answer Sheet](#)" on page 236 for the answer.

Who made a successful authentication? What attribute was this field mapped to in the structured view? See "[Appendix: Answer Sheet](#)" on page 236 for the answer.

6. Close only the **Event Details** window, and then continue to the next exercise.

Exercise 3: Reviewing Event Classification

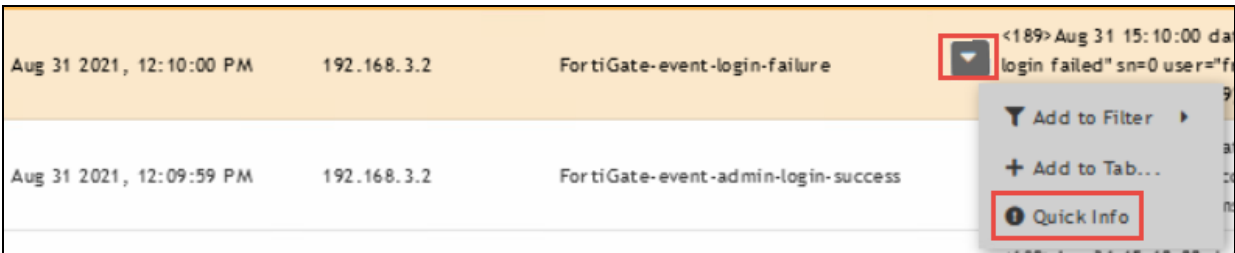
In this exercise, you will review how the events are grouped into event types.

Inspect Event Classification

Using the analytics results from the previous exercise, you will inspect the event classification of **Event Type** and **FortiGate-event-login-success** in the FortiSIEM database (CMDB).

To inspect event classification—method one

1. In the analytics results from the previous exercise, click one of the **FortiGate-event-login-failure** events. A down arrow appears in the **Event Name** column.
2. Click the down arrow, and then select **Quick Info**.

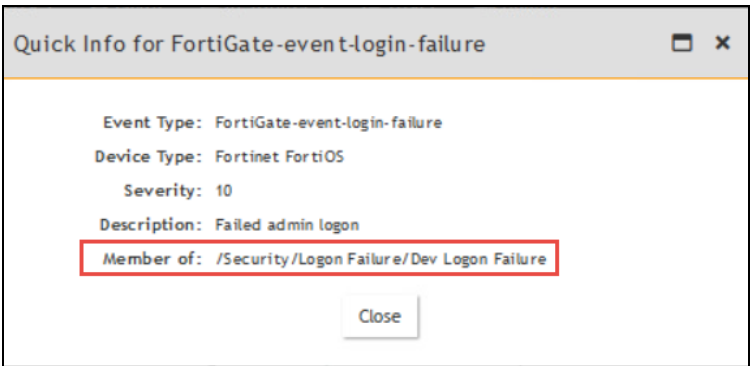


Aug 31 2021, 12:10:00 PM	192.168.3.2	FortiGate-event-login-failure	<189> Aug 31 15:10:00 da login failed" sn=0 user="f
Aug 31 2021, 12:09:59 PM	192.168.3.2	FortiGate-event-admin-login-success	



Notice that the quick info window provides the device type that the event belongs to, with an event severity and description.

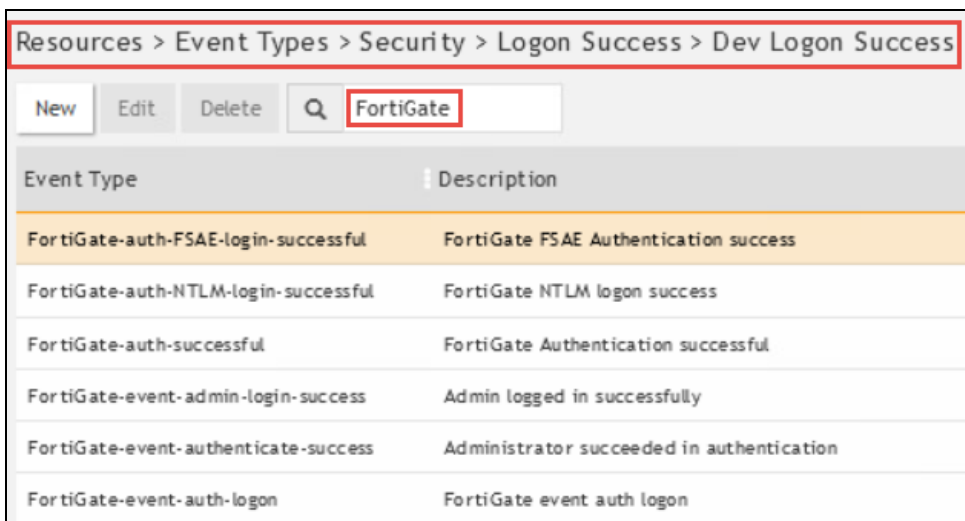
3. Make a note of the **Member of** value, which is related to the CMDB classification for the event.



To inspect event classification—method two

1. Continuing on the FortiSIEM GUI, click the **RESOURCES** tab, and then in the left pane, expand **Event Types**.
2. Click **Security > Logon Success > Dev Logon Success**.

3. In the main window, in the search field, type `FortiGate` to look for all events related to FortiGate.



Resources > Event Types > Security > Logon Success > Dev Logon Success	
New	Edit
Delete	Q FortiGate
Event Type	Description
FortiGate-auth-FSAE-login-successful	FortiGate FSAE Authentication success
FortiGate-auth-NTLM-login-successful	FortiGate NTLM logon success
FortiGate-auth-successful	FortiGate Authentication successful
FortiGate-event-admin-login-success	Admin logged in successfully
FortiGate-event-authenticate-success	Administrator succeeded in authentication
FortiGate-event-auth-logon	FortiGate event auth logon

Stop and think!

Is the **FortiGate-event-login-success** event listed?

4. Select **FortiGate-event-login-success**.
A **Summary** pane opens at the bottom of the screen.
5. Make a note of the **Member of** value.
See "[Appendix: Answer Sheet](#)" on page 237 for the answer.

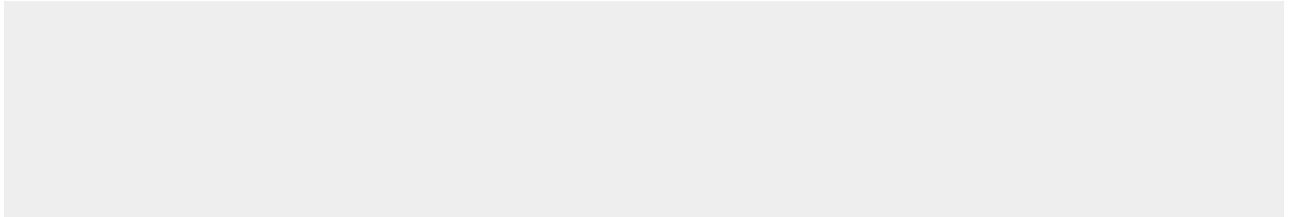
6. Make a note of the **Description**, and then close the window.
See "[Appendix: Answer Sheet](#)" on page 237 for the answer.

7. Remove the search term `FortiGate`, and then review all the other vendor event types that are classified as a **Dev Logon Success** event.
8. In the left pane, continuing under **Security**, click **Logon Failure > Dev Account Locked**, and then review the different event types.
9. Find the event **Win-Security-4740** in the list.



Use the search field to filter the results.

What do you notice about this particular event? See "[Appendix: Answer Sheet](#)" on page 237 for the answer.



10. Log out of the FortiSIEM GUI.

Exercise 4: Reviewing Event Enrichment

In this exercise, you will review how FortiSIEM adds enrichment attributes to events.

Configure a Search Filter

You will configure search filter criteria to filter events.

To set search filter criteria

1. Log in to the FortiSIEM GUI with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Domain	LOCAL

2. Click the **ANALYTICS** tab.
3. Click the search field to edit the condition.



Make sure the search field is empty (it may contain text from another exercise).

The condition editor opens.

4. In the **Filter** editor, select **Event Attribute**.
5. Configure the following settings to create a new query:

Field	Value
Attribute	Reporting IP
Operator	=
Value	172.16.1.3
Next	OR

6. In the **Row** column associated with your existing condition, click the **+** icon to add another row.
7. Configure the following query:

Field	Value
Attribute	Reporting IP
Operator	=
Value	192.168.20.2

Filter

Load Save Clear All

☐ Event Keyword

☒ Event Attribute

Paren	Attribute	Operator	Value	Paren	Next	Row
☐	Reporting IP	=	172.16.1.3	☐	OR	☐
☐	Reporting IP	=	192.168.20.2	☐	AND	☐

☐ CMDB Attribute

Time Range

☒ Real-time ☐ Relative

☐ Absolute

Trend Interval: Auto

Apply & Run Apply Cancel

8. In the **Time Range** section, select **Real-time**.
9. Click **Apply & Run**.

Generate Events

You will generate some scripted events from the Linux-Client VM.

To generate events

1. On the Linux-Client VM, open a browser tab, and then go to the NSE Institute website.
2. On the NSE Institute website, click **LABS SET 1**, and then under **Lab 2 – SIEM and PAM Concepts**, click **Exercise 2.2 – Event Enrichment (Part A)**.

The output should resemble the following example:

Running Data Input for Lab Exercise 2.2A

```
sending events from file /var/www/html/NSE_Institute/labs/LAB2/B/events_lab2b.dat
2 messages sent
```

Completed!

Inspect Event Enrichment

You will examine how FortiSIEM automatically enriches events from various vendor devices. You will also perform manual enrichment on certain device events.

To inspect the event enrichment of a PAN-OS event log

1. Return to the FortiSIEM GUI, and then after two events are received, click **Pause**.
2. Click the **RESOURCES** tab, and then in the left pane, expand **Event Types**.
3. Click **Security > Logon Failure > Dev Logon Failure**.
4. In the main window, in the search field, type **PAN**.
5. Select **PAN-OS-SYSTEM-login-failed**, and then click **Summary** in the bottom pane.

The screenshot shows the FortiSIEM GUI with the breadcrumb path **Resources > Event Types > Security > Logon Failure > Dev Logon Failure** highlighted. Below this, there are buttons for **New**, **Edit**, **Delete**, and a search field containing **PAN**. A table lists three event types:

Event Type	Description	Device Type
PAN-IDP-31732	Telnet Authentication Failed	Palo Alto PAN-OS
PAN-IDP-55873	SSH2 Logon Failure	Palo Alto PAN-OS
PAN-OS-SYSTEM-login-failed	Admin login failure	Palo Alto PAN-OS

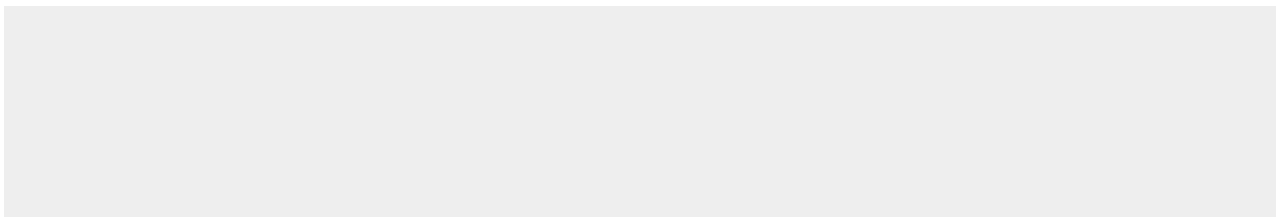
The **PAN-OS-SYSTEM-login-failed** row is highlighted. Below the table, the **Summary** tab is selected, showing the following details:

- Name: PAN-OS-SYSTEM-login-failed
- Description: Admin login failure
- Device Type: Palo Alto PAN-OS
- Severity: 7
- Member Of: /Security/Logon Failure/Dev Logon Failure
- CVE IDs:

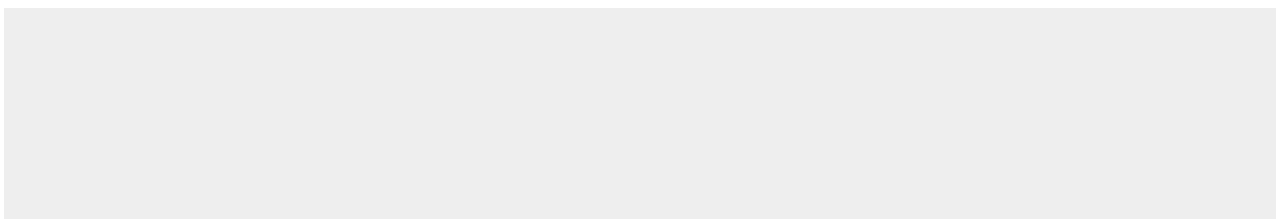
What is the value in the **Member Of** field? See "[Appendix: Answer Sheet](#)" on page 238 for the answer.

6. Return to the **ANALYTICS** tab.
7. Select the **Raw Event Log** field to look at the details for the **PAN-OS-SYSTEM-login-failed** event.
A right arrow icon (➡) appears.

8. Click the right arrow icon to display the **Event Details**, which will enable you to view the details associated with that event.
9. Review the raw event log for that event.
Does it contain any country-related information? See ["Appendix: Answer Sheet" on page 238](#) for the answer.



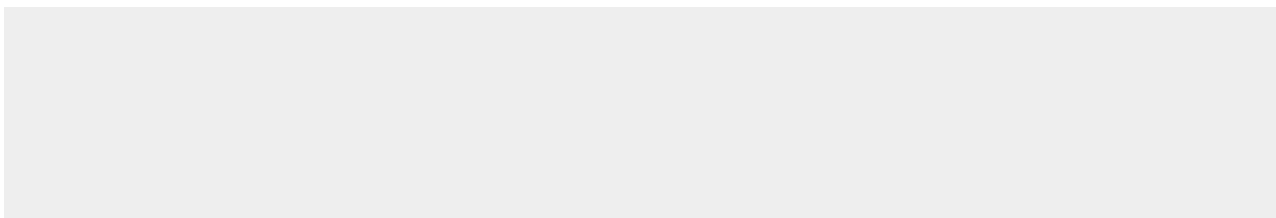
10. Review the attributes in the structured view, and then note the **Source Country**, **Source Organization**, and **Source State**.
Where did this information come from? See ["Appendix: Answer Sheet" on page 238](#) for the answer.



11. Close the **Event Details** window.

To inspect event enrichment in the IOS-SEC event log

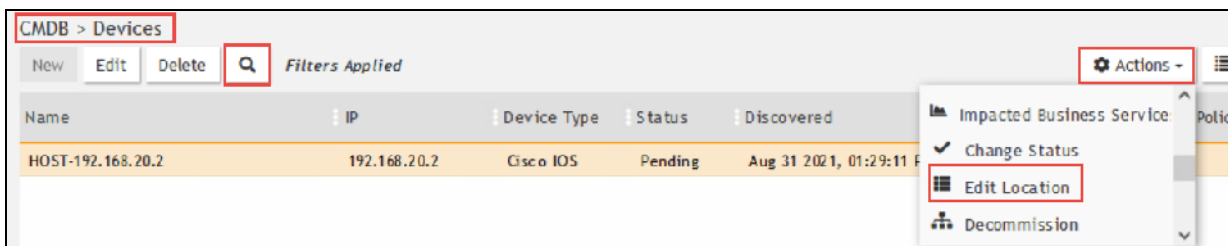
1. Continuing on the FortiSIEM GUI, review the **Event Details** raw event log for the **IOS-SEC_LOGIN-LOGIN_FAILED** event.
Is there a **Source Country** or **Destination Country** populated for this event? If not, why? See ["Appendix: Answer Sheet" on page 238](#) for the answer.



2. Close the **Event Details** window.

To update the geographical location for a device manually

1. Continuing on the FortiSIEM GUI, click the **CMDB** tab.
2. In the left pane, select **Devices**.
3. In the search field, type the IP address 192.168.20.2.



4. In the search results, select the **Name HOST-192.168.20.2** device.
5. Click the down arrow beside **Actions**, and then select **Edit Location**.
The **Edit Device Location** pop-up window opens.



Because FortiSIEM is not configured with a real Google API key, you might see an error message.

6. In the **Edit Device Location** pop-up window, configure the following settings (or configure your own), and then click **OK**:

Field	Value
Location Name	UK Data Center
Country	United Kingdom
State	England
City	London



Because FortiSIEM is not configured with a real Google API key, you might see an error message.

7. Click **Save**.
8. Click the **ANALYTICS** tab, and then click the search field.
Your previous query should still be listed.
9. In the **Time Range** section, select **Real-time**.
10. Click **Apply & Run**.

To generate logs for a manually updated geographical location

1. Return to the Linux-Client VM, and then go to the browser tab connected to the NSE Institute website.
2. Under **LABS SET 1** and **Lab 2 – SIEM and PAM Concepts**, select **Exercise 2.2 – Event Enrichment (Part B)**.
3. Close the Linux-Client VM browser tab.

To inspect event enrichment for a manually updated geographical location

1. Return to the FortiSIEM GUI, and then after two events are received, click **Pause**.
2. Review the **Event Details** for the raw event log **IOS-SEC_LOGIN-LOGIN_FAILED** again.



- Make sure **Wrap Raw Event** is selected.
- Make sure **Show Event Type** is selected.
- Once the **RAW Event log** is selected, a right arrow icon (➡) appears.
- Click the icon to display the **Show Detail** option, which will enable you to view the details associated with that event.

Are the **Reporting City**, **Destination City**, **Destination Country**, and **Destination State** values populated now? If so, why? See "[Appendix: Answer Sheet](#)" on page 238 for the answer.

3. Close the **Event Details** window.
4. Click the **CMDB** tab, select the device with the IP address 192.168.20.2, and then click **Delete**.
5. If a prompt appears instructing you to delete the selected device from the CMDB, click **OK**, or remove it from the group.
6. Log out of the FortiSIEM GUI.

Exercise 5: Reviewing Performance Events

In this exercise, you will examine some of the performance events collected by FortiSIEM.

Configure a Search Filter

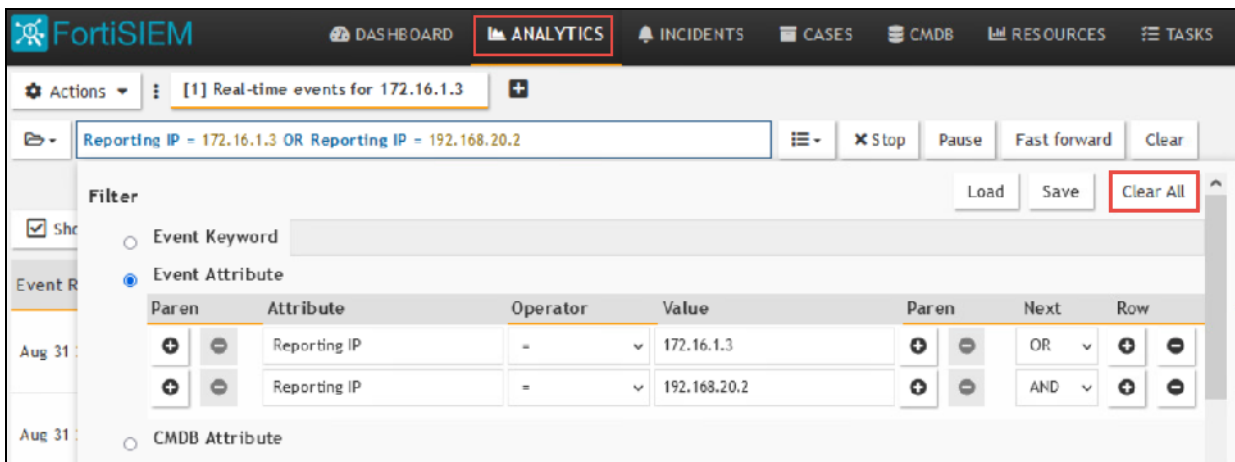
You will configure search filter criteria to filter events.

To set search filter criteria

1. Log in to the FortiSIEM VM with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Domain	LOCAL

2. Click the **ANALYTICS** tab.
3. Click the search field to edit the condition.
The **Filter** editor appears.
4. Click **Clear All** to clear the existing queries.



5. Create the following query:

Field	Value
Attribute	Reporting IP

Field	Value
Operator	=
Value	192.168.20.2

6. In the **Time Range** section, select **Realtime**.
7. Click **Apply & Run**.

Generate Performance Event Logs

You will generate some scripted performance event logs.

To generate performance event logs

1. On the Linux-Client VM, open a browser, and then go to the NSE Institute website.
2. Navigate to **LABS SET 1**, and then under **Lab 2 – SIEM and PAM Concepts**, select **Exercise 2.3 – Performance Events**.

The output should resemble the following example:

Running Data Input for Lab Exercise 2.3
sending events from file /var/www/html/NSE_Institute/labs/LAB2/C/events_lab2_3.dat 10 messages sent
Completed!

3. Close the Linux-Client VM browser tab.

View Performance Event Enrichment

You will examine how FortiSIEM automatically enriches performance events.

To view performance events

1. Return to the FortiSIEM GUI, and then after 10 events are received, click **Pause**.
Notice that there are a number of device monitor events labeled **PH_DEV_MON**.
2. Select **Raw Event Log** for **Event Type PH_DEV_MON_SYS_UPTIME**, and then view **Event Details**.



- Make sure **Wrap Raw Event** is selected.
- Make sure **Show Event Type** is selected.
- Once the **RAW Event log** is selected, a right arrow (➡) icon appears.
- Click the icon to display the **Event Details** window, which will enable you to view the details associated with that event.

3. Review the raw event log and structured data.

Which attributes relate to the uptime and downtime of the device? See ["Appendix: Answer Sheet" on page 239](#) for the answer.



Performance events are also enriched with geolocation data (host, reporting country, and so on), if the CMDB has a location set for an internal device. A host IP is populated for all performance events.

What attribute relates to how often the event is collected? See ["Appendix: Answer Sheet" on page 239](#) for the answer.

4. Close the **Event Details** window.
5. In the **RAW event Log**, select **Event Type PH_DEV_MON_SYS_MEM_UTIL**.
A right arrow (➡) icon appears.

6. Click the right arrow icon (➡).

7. Review the raw event log and structured data.

Which attribute relates to the memory utilization of the device? See ["Appendix: Answer Sheet" on page 239](#) for the answer.

How often is the memory utilization event collected? See ["Appendix: Answer Sheet" on page 239](#) for the answer.

8. Open the **Event Details** dialog box associated with the **PH_DEV_MON_NET_INTF_UTIL** event type.
9. Review the raw event log and structured data.

Which attributes relate to the interface name and interface utilization? See ["Appendix: Answer Sheet" on page 239](#) for the answer.

Why are there four interface utilization events? See ["Appendix: Answer Sheet" on page 239](#) for the answer.

10. Log out of the FortiSIEM GUI.

Lab 3: Discovery

In this lab, you will examine the FortiSIEM discovery processes.

Objectives

- View auto log discovery
- Add credentials and IP ranges for a single device
- Discover a single device
- Perform a discovery on many devices
- Pull performance data from devices

Time to Complete

Estimated: 45 minutes

Exercise 1: Inspecting Syslog Data

In this exercise, you will inspect the type of data that is extracted from the syslogs.

Configure Search Filter Criteria

You will configure search filter criteria to filter events.

To set search criteria for logs

1. Log in to the FortiSIEM GUI with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Domain	LOCAL

2. Click the **ANALYTICS** tab, and then click the search field to edit the condition.
3. In the **Filters** editor, configure the following settings to create a new query:

Field	Value
Event Keyword	ASA or devname

4. In the **Time Range** section, select **Real-time**.
5. Click **Apply & Run**.

The screenshot shows the 'Filter' configuration window in the FortiSIEM GUI. It includes a 'Filter' section with radio buttons for 'Event Keyword' (selected), 'Event Attribute', and 'CMDB Attribute'. The 'Event Keyword' field contains the text 'ASA or devname'. Below this is the 'Time Range' section with radio buttons for 'Real-time' (selected), 'Relative', and 'Absolute'. At the bottom, there is a 'Trend Interval' dropdown menu set to 'Auto'. On the right side of the window, there are buttons for 'Load', 'Save', and 'Clear All'. At the bottom right, there are buttons for 'Apply & Run', 'Apply', and 'Cancel'.



Make sure the search field is empty (it may contain text from another exercise).

Generate Test Logs

You will generate some scripted logs to trigger the discovery processes on FortiSIEM.

To generate test logs

1. On the Linux-Client VM, open a browser, and then go to the NSE Institute website.
2. Navigate to **LABS SET 1**, and then under **Lab 3 – Discovery**, select **Exercise 3.1 – Auto Log Discovery**.

The output should resemble the following example:

```
Running Data Input for Lab Exercise 3.1

sending events from file /var/www/html/NSE_Institute/labs/LAB3/A/events_ciscoasa.dat
sending events from file /var/www/html/NSE_Institute/labs/LAB3/A/events_fortigate.dat
50 messages sent

Completed!
```

3. Close the Linux-Client VM browser tab.

Inspect Discovered Devices

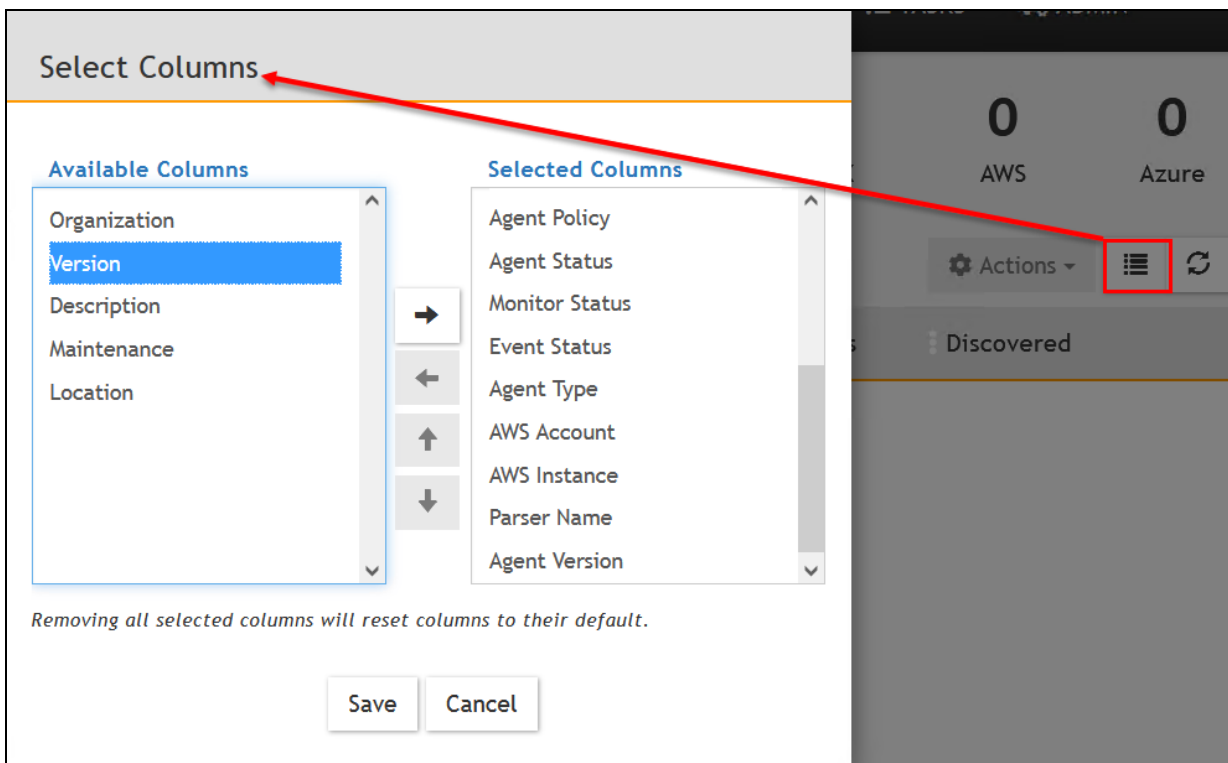
You will inspect the discovered devices on FortiSIEM.

To inspect the syslogs

1. Return to the FortiSIEM GUI, on the **ANALYTICS** tab, wait until at least 25 events are received, and then click **Pause**.

☒ Show Event Type ☐ Wrap Raw Events Search paused. Click Resume or Fast Forward to continue.			
Event Receive Time	Reporting IP	Event Type	Raw Event Log
Sep 30 2021, 12:08:55 PM	192.168.19.56	ASA-602014	<134>Jan 17 2013 01:00:00: %ASA-6-100140: Inbound TCP connection 6476194 for outside:10.1.7.17/13
Sep 30 2021, 12:08:55 PM	192.168.19.56	ASA-602015	<134>Jan 17 2013 01:00:00: %ASA-6-100151: Built inbound UDP connection 64256436 for outside:10.1.2.25/
Sep 30 2021, 12:08:59 PM	192.168.3.1	FortiGate-traffic-forward	<189>Sep 30 15:00:59 date=2016-09-10 time=16:59:49 devname=FG24002913603441 device=FG24002913603
Sep 30 2021, 12:08:59 PM	192.168.3.1	FortiGate-traffic-forward	<189>Sep 30 15:00:59 date=2016-09-10 time=16:59:49 devname=FG24002913603441 device=FG24002913603
Sep 30 2021, 12:08:57 PM	192.168.3.1	FortiGate-traffic-allowed	<189>Sep 30 15:00:57 date=2016-09-10 time=16:59:48 devname=FG24002913603441 device=FG24002913603
Sep 30 2021, 12:08:55 PM	192.168.19.56	ASA-602014	<134>Jan 17 2013 01:00:00: %ASA-6-100140: Inbound TCP connection 6476194 for outside:10.1.7.17/13
Sep 30 2021, 12:08:57 PM	192.168.3.1	FortiGate-traffic-denied	<189>Sep 30 15:00:57 date=2016-09-10 time=16:59:48 devname=FG24002913603441 device=FG24002913603
Sep 30 2021, 12:08:55 PM	192.168.19.56	ASA-602014	<134>Jan 17 2013 01:00:00: %ASA-6-100140: Inbound TCP connection 6476194 for outside:10.1.7.17/13
Sep 30 2021, 12:08:55 PM	192.168.19.56	ASA-602015	<134>Jan 17 2013 01:00:00: %ASA-6-100151: Built inbound UDP connection 64256436 for outside:10.1.2.25/

- Click the **CMDB** tab, and then in the left pane, click **Devices > Network Device > Firewall**.
- In the upper-right corner of the **CMDB** tab, click the columns icon (≡) to add a **Version** column to the display.



- In the **Available Columns** list, select **Version**.
- Click the right arrow icon (➡) to move **Version** to the **Selected Columns** list.
- Click **OK**.
- Drag the **Version** column beside the **Method** column.
- Click the **CMDB** tab, and then in the left pane, click **Devices > Network Device > Firewall**.

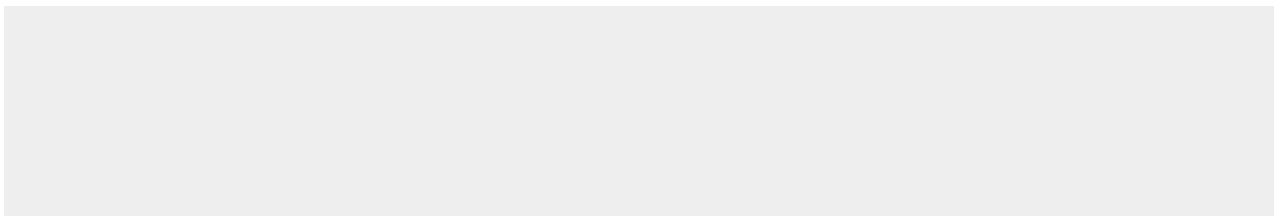
The Cisco ASA device with the name **HOST-192.168.19.65** and a Fortinet FortiOS device with the name **FG240D3913800441** appear in the list.

1 4 0 0 0 0 0						
Routers Firewalls Windows Unix ESX AWS Azure						
CMDB > Devices > Network Device > Firewall						
New Edit Delete Q Actions ≡ ↺						
Name	IP	Device Type	Status	Discovered	Method	Version
FG240D3913800441	192.168.3.1	Fortinet FortiOS	Pending	Oct 05 2021, 02:04:00 AM	LOG	ANY
FG240D3913800450	192.168.3.2	Fortinet FortiOS	Pending	Oct 05 2021, 02:02:33 AM	LOG	ANY
HOST-172.16.1.3	172.16.1.3	Palo Alto PAN-OS	Pending	Oct 05 2021, 02:02:41 AM	LOG	ANY
HOST-192.168.19.65	192.168.19.65	Cisco ASA	Pending	Oct 05 2021, 02:03:57 AM	LOG	ANY

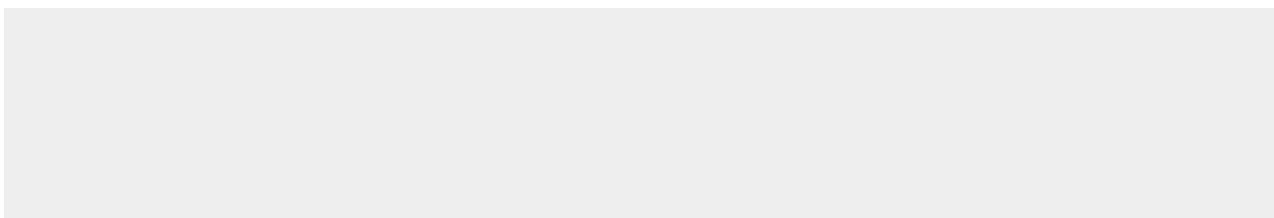


Make sure the search field is empty (it may contain text from another exercise).

Why are the names different? If you are unsure, review some of the raw events on the **ANALYTICS** tab. See ["Appendix: Answer Sheet" on page 240](#) for the answer.



What is displayed under the **Version** and **Discovered** fields for each device? See ["Appendix: Answer Sheet" on page 240](#) for the answer.



- Continuing on the **CMDB** tab, in the lower pane containing the details, select the **Cisco ASA** device, click the **Summary** tab, and then review the details.



You may need to click the up arrow to bring the fields into view.

HOS 1-192.168.19.65		192.168.19.65	Cisco ASA	Pending	Oct 05 2021, 02:03:57 AM	LOG	ANY
Summary Properties Monitor Software Hardware Configuration Relationships File ☐ Auto expand							
General				Health Overview			
Name: HOS 1-192.168.19.65 Device Type: Cisco ASA Importance: Normal				Access IP: 192.168.19.65 Version: ANY Performance Health: ● Normal			
Member of 3 Groups				Statistics			
Group #1: /Network Device/Firewall Group #2: /Network Device/VPN Gateway Group #3: /Network Device/Network IPS				Created: Oct 05 2021, 02:04:17 AM via LOG Last Discovered: Oct 05 2021, 02:03:57 AM via LOG Last Updated: Oct 05 2021, 02:04:17 AM via LOG Interfaces: 0 System Services: 0			

Notice this device has been automatically categorized under three groups.

- Select the **Fortinet FortiOS** device, on the lower pane containing the details, click the **Summary** tab, and then review the details.

CMDB > Devices > Network Device > Firewall

NewEditDeleteQ

Name	IP	Device Type	Status	Discovered	Method	Version
FG240D3913E00441	192.168.3.1	Fortinet FortiOS	Pending	Oct 05 2021, 02:04:00 AM	LOG	ANY
FG240D3913E00450	192.168.3.2	Fortinet FortiOS	Pending	Oct 05 2021, 02:02:33 AM	LOG	ANY
HOST-172.16.1.3	172.16.1.3	Palo Alto PAN-OS	Pending	Oct 05 2021, 02:02:41 AM	LOG	ANY
HOST-192.168.19.65	192.168.19.65	Cisco ASA	Pending	Oct 05 2021, 02:03:57 AM	LOG	ANY

<

SummaryPropertiesMonitorSoftwareHardwareConfigurationRelationshipsFile☐ Auto expand

General

Name: FG240D3913E00441

Device Type: Fortinet FortiOS

Importance: Normal

Access IP: 192.168.3.1

Version: ANY

Member of 4 Groups

Group #1: /Network Device/Firewall

Group #2: /Network Device/Network IPS

Group #3: /Network Device/Security Gateway

Group #4: /Network Device/WLAN Controller

Health Overview

Performance Health: ● Normal

Statistics

Created: Oct 05 2021, 02:04:15 AM via LOG

Last Discovered: Oct 05 2021, 02:04:00 AM via LOG

Last Updated: Oct 05 2021, 02:04:15 AM via LOG

Interfaces: 0

System Services: 0

Running Apps: 0

Notice this device has been automatically categorized under four groups.

- On the same lower pane, review the **Hardware > Interfaces** and **Configuration** tabs for both devices. What do you see and what can you identify about the population of the CMDB from the log discovery alone? See ["Appendix: Answer Sheet"](#) on page 240 for the answer.

- Log out of the FortiSIEM GUI.

Exercise 2: Adding Credentials and IP Ranges for a Single Device

In this exercise, you will add the SNMP credentials used in the discovery process.

Configure SNMP Credentials

You will configure SNMP credentials and assign IP address ranges to the credentials on FortiSIEM.

To add SNMP credentials

1. Log in to the FortiSIEM GUI with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Domain	LOCAL

2. Click the **ADMIN** tab.
3. In the left pane, click **Setup**.
4. In the main window, select the **Credentials** tab.
5. Click **Step 1: Enter Credentials**, and then click **New**.

Access Method Definition

Name:

Device Type: Generic

Access Protocol: SNMP

Port: 161

Password config: Manual

Community String:

Confirm Community String:

Description:

Save

Cancel

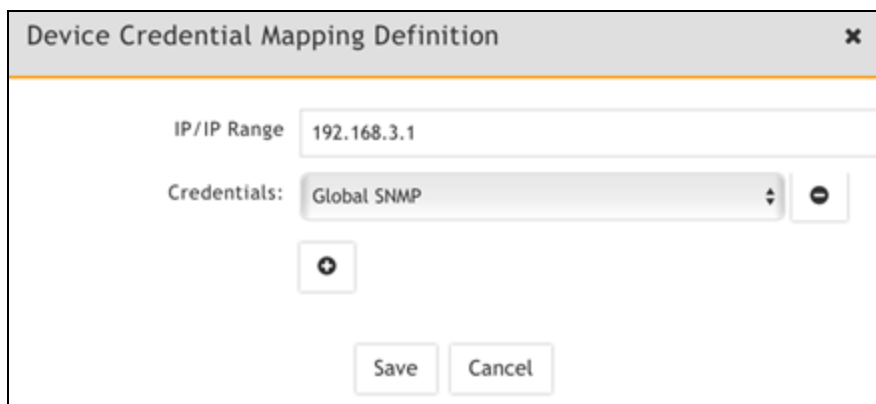
6. Configure the following settings:

Field	Value
Name	Global SNMP
Device Type	Generic
Access Protocol	SNMP
Community String	public
Confirm Comm String	public
Description	FortiSIEM Training SNMP Credentials

7. Click **Save**.

To assign credentials to address ranges

1. Continuing on the FortiSIEM GUI, under **Step 2: Enter IP Range to Credential Associations**, click **New**.
2. In the **IP/IP Range** field, type `192.168.3.1`.
3. In the **Credentials** drop-down list, select **Global SNMP** (it should be listed as the default because there is only one credential defined), and then click **Save**.



4. Log out of the FortiSIEM GUI.

Prepare for Discovery

Because you are working with a system that has scripted data, you must prepare the system before you can perform the discovery.

To create scripted discovery data

1. On the Linux-Client VM, open a browser, and then go to the NSE Institute website.
2. Navigate to **LABS SET 1**, and then under **Lab 3—Discovery**, select **Exercise 3.2—(A) Prepare System for Local File Discovery**.

The output takes approximately one minute to return and should resemble the following example:

Preparing System for Local File Discovery - Lab Exercise 3.2A

This will take around 50 seconds to complete.

```
Waiting 45 seconds for Discovery Process to Restart
admin 14575 1 1 10:05 ? 00:00:00 /opt/phoenix/bin/phDiscover
Discovery Process Restarted OK
```

Completed!

3. Once completed, select **Exercise 3.2—(B) Copy FortiGate Discovery File**.

The output should resemble the following example:

Running Lab Exercise 3.2B

Preparing FortiGate Simulated Device SNMP Walk for Discovery

Made required directories...

Made required directory...

Copied required SNMPwalk file...

Changed file permissions...

Completed! FortiGate Device 192.168.3.1 Ready for Discovery

4. Close the Linux-Client VM browser tab.

Exercise 3: Discovering a Single Device

In this exercise, you will use the credentials from the previous exercise to discover a device and collect data from it.

Configure Discovery

You will configure the discovery settings that FortiSIEM uses to perform discovery.

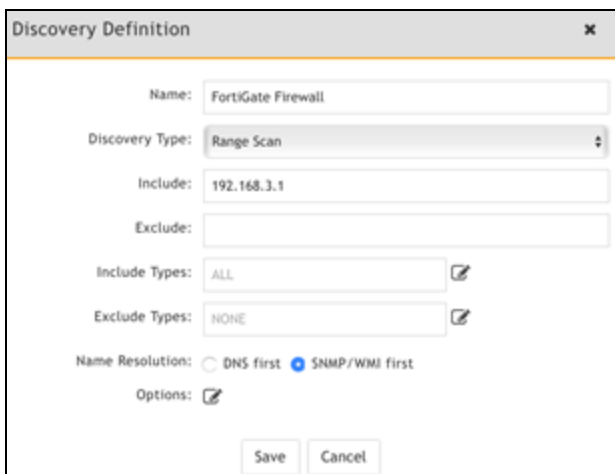
To add a device to be discovered

1. Log in to the FortiSIEM GUI with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Domain	LOCAL

2. Click the **ADMIN** tab.
3. In the left pane, click **Setup**.
4. In the main window, click the **Discovery** tab.
5. Click **New**.
6. Configure the following settings:

Field	Value
Name	FortiGate Firewall
Discovery Type	Range Scan
Include	192.168.3.1
Name Resolution	SNMP/WMI first

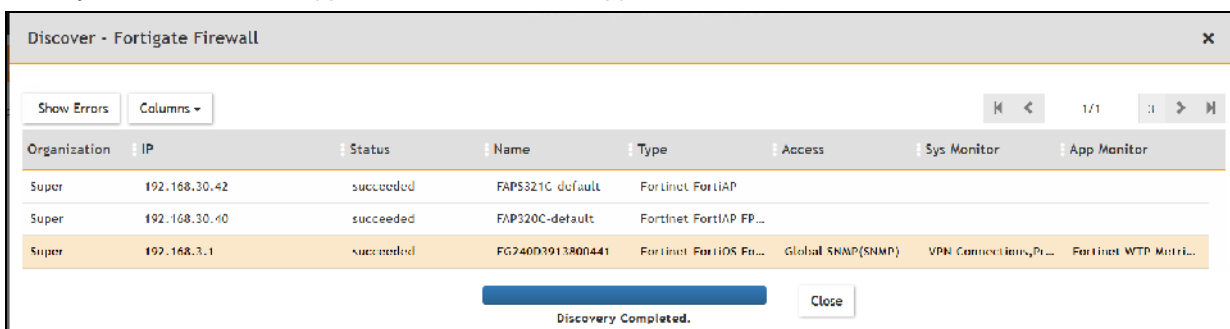


The Discovery Definition dialog box is shown with the following settings:

- Name: FortiGate Firewall
- Discovery Type: Range Scan
- Include: 192.168.3.1
- Exclude: (empty)
- Include Types: ALL
- Exclude Types: NONE
- Name Resolution: ☐ DNS first ☒ SNMP/WMI first
- Options: ☒

Buttons: Save, Cancel

7. Leave all other fields at the default settings, and then click **Save**.
8. In the table, select the **FortiGate Firewall** entry, and then click **Discover**.
9. Once the discovery is complete, review the fields to view what access method was used for the discovery, and what system monitors and application monitors were applied to the device.



The Discover - Fortigate Firewall window shows a table with the following data:

Organization	IP	Status	Name	Type	Access	Sys Monitor	App Monitor
Super	192.168.30.42	succeeded	FAP5321C default	Fortinet FortiAP			
Super	192.168.30.40	succeeded	FAP320C-default	Fortinet FortiAP FP...			
Super	192.168.3.1	succeeded	FG240D391380N441	Fortinet FortiOS Fa...	Global SNMP(SNMP)	VPN Connections,Pr...	Fortinet WTP Metri...

Buttons: Show Errors, Columns, Close

Discovery Completed.

10. Click **Close**.

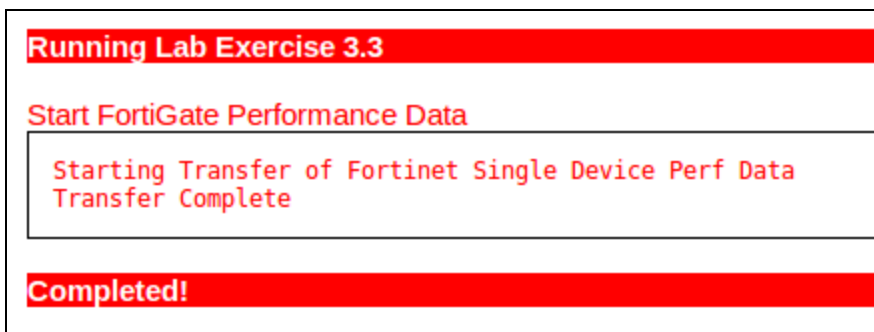
Generate Scripted Performance Data

You will simulate a device by generating scripted performance data that FortiSIEM uses in the discovery process.

To fake the performance data

1. On the Linux-Client VM, open a browser, and then go to the NSE Institute website.
2. Navigate to **LABS SET 1**, and then under **Lab 3—Discovery**, select **Exercise 3.3—Start FortiGate Performance Data**.

The output should resemble the following example:



3. Close the Linux-Client VM browser tab.

To review the performance data

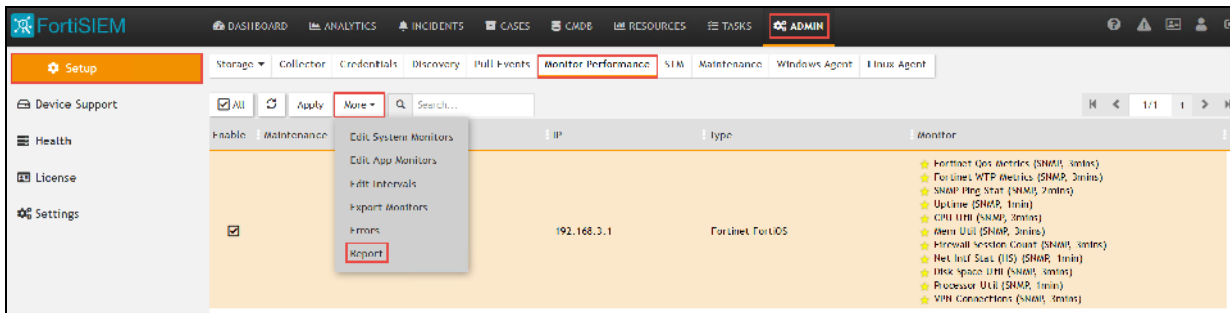
1. Return to the FortiSIEM GUI, and then click the **CMDB** tab.
2. In the left pane, click **Devices > Network Device > Firewall**.
3. Look at the **Fortinet FortiOS** device again (FG240D3913800441).
What does the **Version** field show now? See "[Appendix: Answer Sheet](#)" on page 241 for the answer.

4. Select the **Fortinet FortiOS** device, in the lower pane containing the details, click the **Summary** tab, and then review the details.
How many groups is this device now a member of? See "[Appendix: Answer Sheet](#)" on page 241 for the answer.

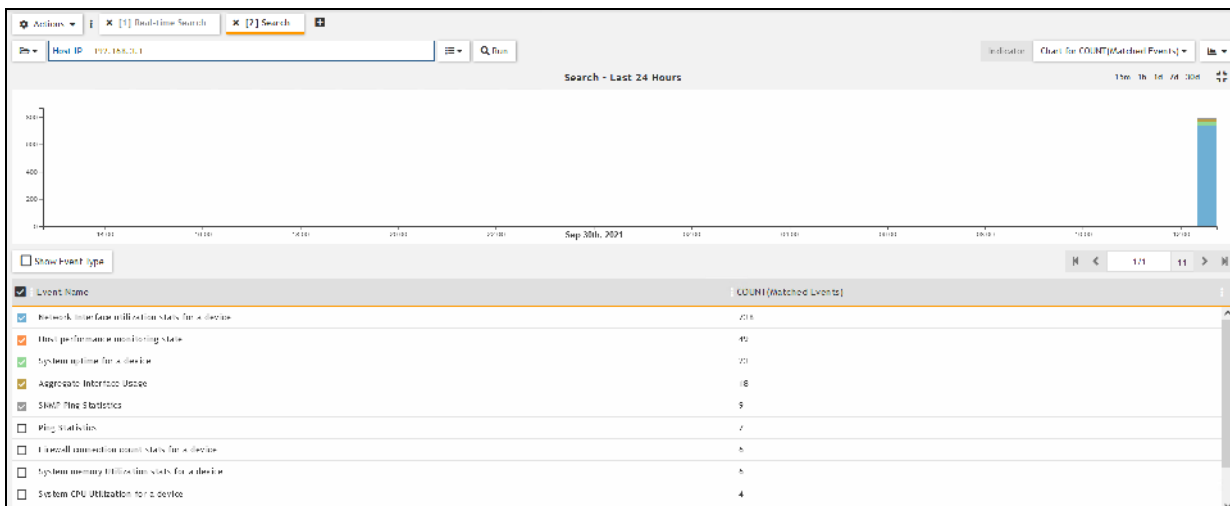
5. Continuing in the lower pane, click **Hardware > Interfaces**.
Notice how it is now populated with a lot of detail.
6. Continuing in the lower pane, click **Hardware > Components**.
Notice how the serial number and software version are recorded.
7. Click the main **ADMIN** tab, and then in the left pane, click **Setup**.
8. In the main window, select the **Monitor Performance** tab.
Notice how the Fortinet FortiOS device lists the system monitors and application monitors under **Monitor**.
9. View the **Monitor** column and make a note of how often **CPU Util**, **Mem Util**, and **Net Intf Stat** jobs are being collected using SNMP.

See "Appendix: Answer Sheet" on page 241 for the answer.

10. Click the device entry for **192.168.3.1**.
11. In the **More** drop-down list, select **Report** to verify if performance data is being collected.



This creates a query and takes you to the **ANALYTICS** tab to view the results.



12. After you review the results, close the search tab.
13. Log out of the FortiSIEM GUI.

Exercise 4: Performing Discovery of Other Lab Devices

In this exercise, you will create discoveries for all other devices in the simulated lab. You will continue to use only SNMP. (You are assuming the same SNMP credential across all devices.)

Other Device List

Type	Make	IP address	Method
Firewall	FortiGate	172.16.255.82	SNMP
Firewall	FortiGate	10.1.1.1	SNMP
Firewall	Palo Alto	172.16.1.2	SNMP
Firewall	Cisco ASA	192.168.19.65	Lab Special
Firewall	Juniper	172.16.3.10	Log Only
Firewall	Juniper	172.16.255.70	SNMP
Firewall	Checkpoint	172.16.0.1	SNMP
Router/Switch	Cisco IOS	10.1.1.5	Log Only
Router/Switch	Cisco IOS	192.168.20.1	SNMP
Router/Switch	Cisco IOS	172.16.3.2	SNMP
Router/Switch	Cisco IOS	192.168.19.1	SNMP
Router/Switch	Foundry	172.16.0.4	SNMP
Router/Switch	Foundry	172.16.10.1	Log Only
Router/Switch	HP Procurve	172.16.22.2	SNMP
Router/Switch	Jun OS	172.16.5.64	SNMP
Wireless Controller	Aruba	192.168.26.7	SNMP
Server	Windows	172.16.10.28	SNMP
Server	Windows	192.168.0.10	SNMP
Server	Windows	192.168.0.40	SNMP

Type	Make	IP address	Method
Server	Windows	172.16.10.9	SNMP
Server	Windows	10.10.100.27	Log Only
Server	Windows	10.1.1.33	SNMP
Server	Windows	10.1.1.41	SNMP
Server	Linux	192.168.0.16	SNMP
Server	AIX	172.16.20.160	SNMP
Server	Solaris	172.16.10.6	SNMP

Populate the Credential and Discovery Ranges of Other Devices

You will execute a script to populate the credential and discovery ranges of all other devices.

To populate the credential and discovery ranges of other devices

- 1. On the Linux-Client VM, open a browser, and then go to the NSE Institute website.
- 2. Navigate to LABS SET 1, and then under Lab 3—Discovery, select Exercise 3.4—(A) To upload the Credentials and Discovery Ranges via the Rest API.

The output takes approximately thirty seconds to return and should resemble the following example:

Scripts To upload the Credential and Discovery Ranges via the Rest API - Lab Exercise 3.4A

This will take around 30 seconds to complete.

Success.
Credentials and Discovery Ranges for Devices Added Successfully
Done!

Completed!

To view the credentials and IP ranges for other devices added by the REST API

- 1. Log in to the FortSIEM GUI with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Domain	LOCAL

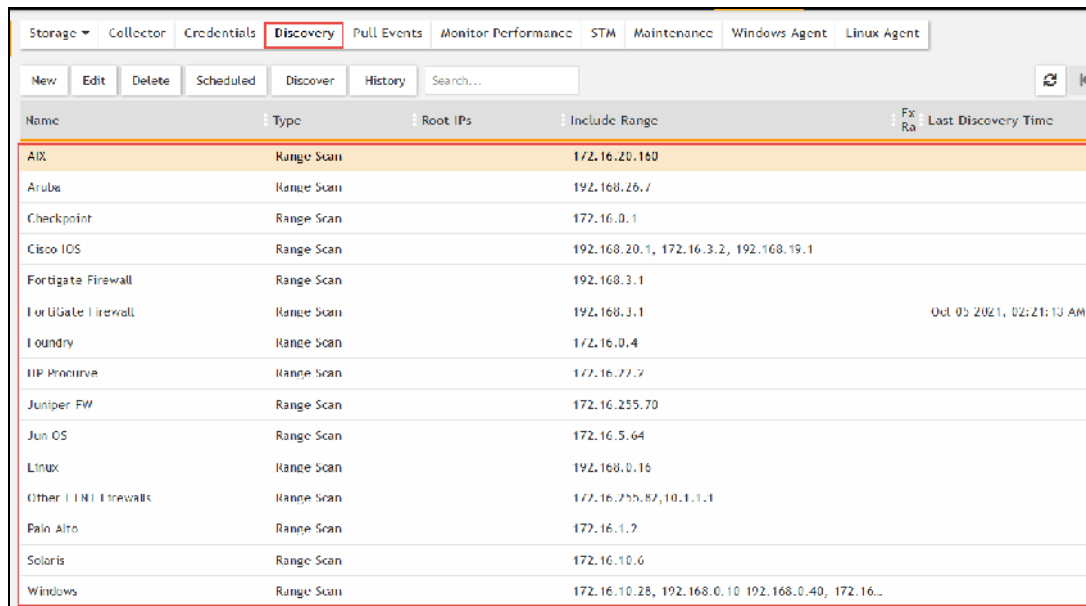
2. Click the **ADMIN** tab.
3. In the left pane, select **Setup**.
4. In the main window, click the **Credentials** tab.

You should see **Step 1: Enter Credentials** and **Step 2: Enter IP Range to Credential Associations** populated for other devices.

To view the discovery task for other devices added by the REST API

1. Continuing on the **Setup** page, click the **Discovery** tab.

You should see discovery tasks with IP ranges populated for other devices.



Name	Type	Root IPs	Include Range	Excl. Range	Last Discovery Time
ADX	Range Scan		172.16.20.160		
Aruba	Range Scan		192.168.26.7		
Checkpoint	Range Scan		172.16.0.1		
Cisco IOS	Range Scan		192.168.20.1, 172.16.3.2, 192.168.19.1		
Fortigate Firewall	Range Scan		192.168.3.1		
FortiGate Firewall	Range Scan		192.168.3.1		Oct 05 2021, 02:21:13 AM
Foundry	Range Scan		172.16.0.4		
HIP Procurve	Range Scan		172.16.22.2		
Juniper FW	Range Scan		172.16.255.70		
Jun OS	Range Scan		172.16.5.64		
Linux	Range Scan		192.168.0.16		
Other Linux Firewalls	Range Scan		172.16.255.82, 10.1.1.1		
Palo Alto	Range Scan		172.16.1.2		
Solaris	Range Scan		172.16.10.6		
Windows	Range Scan		172.16.10.28, 192.168.0.10, 192.168.0.40, 172.16...		

Prepare the Simulated Devices for Discovery

You will prepare the lab system to prepare the simulated devices for discovery.

To prepare the fake devices for discovery

1. Return to the Linux-Client VM, in the browser tab connected to the **NSE Institute** website, navigate to **LABS SET 1**, and then under **Lab 3—Discovery**, select **Exercise 3.4 (B)—Copy All Other Discovery Files**.

The output takes approximately one minute to return and should resemble the following example:

```
Running Lab Exercise 3.4B

Copying Performance Data Files

spawn scp /var/www/html/NSE_Institute/scripts/ASA_Special/disc-328501517-1.xml root@10.0.1.130:/data/cache/discoveryResults/cust-1/new
root@10.0.1.130's password:

disc-328501517-1.xml          0% 0 0.0KB/s --:-- ETA
disc-328501517-1.xml        100% 5500 2.0MB/s 00:00
spawn scp /var/www/html/NSE_Institute/scripts/ASA_Special/disc-328501517-2.xml root@10.0.1.130:/data/cache/discoveryResults/cust-1/new
root@10.0.1.130's password:

disc-328501517-2.xml          0% 0 0.0KB/s --:-- ETA
disc-328501517-2.xml        100% 1319 702.9KB/s 00:00
spawn scp /var/www/html/NSE_Institute/scripts/ASA_Special/disc-328501517-3.xml root@10.0.1.130:/data/cache/discoveryResults/cust-1/new
root@10.0.1.130's password:

disc-328501517-3.xml          0% 0 0.0KB/s --:-- ETA
disc-328501517-3.xml        100% 208 85.3KB/s 00:00
Successfully Delivered Cisco ASA into UMBB

Completed!
```



If you don't see three 100% successful SCP transfers, tell your instructor.

2. Close the Linux-Client VM browser tab.

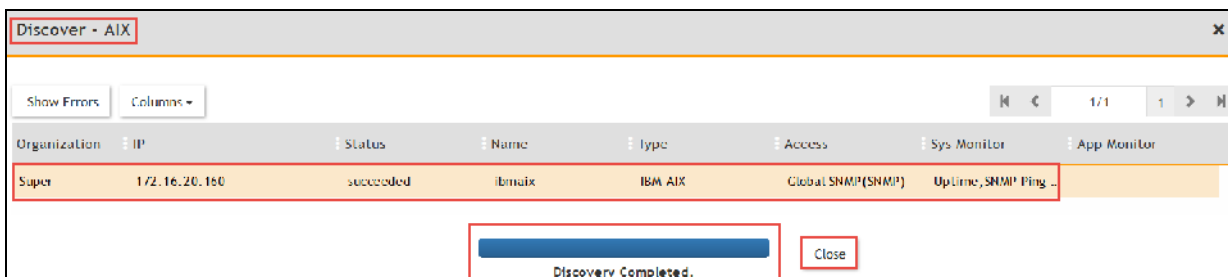
To discover devices

1. Return to the FortiSIEM GUI, and then click **Discover** for each device individually.

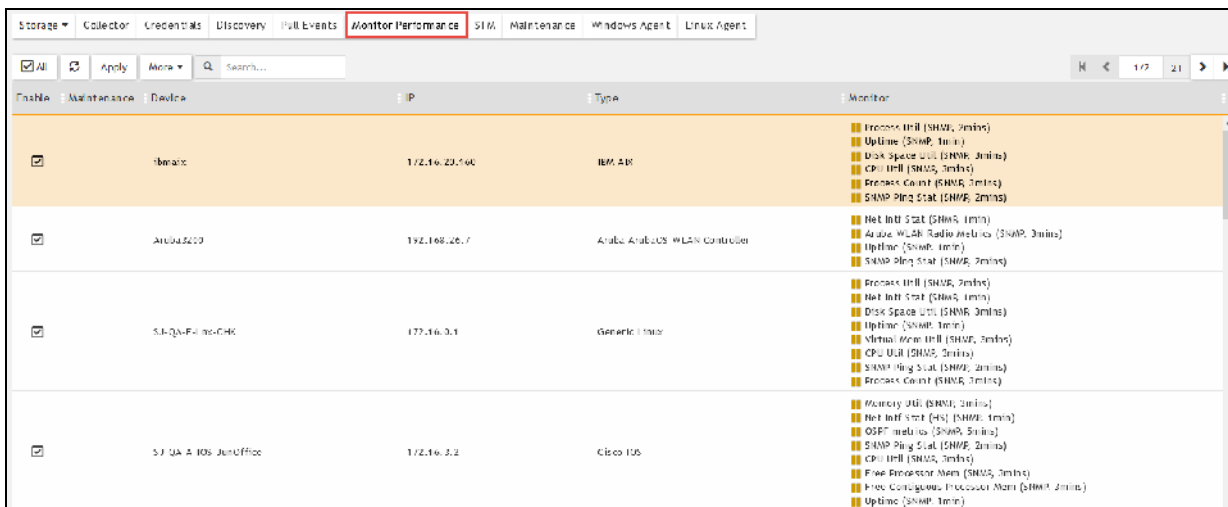
Important: Do not discover them all at once!

Storage ▾ Collector Credentials Discovery Pull Events Monitor Performance STM Maintenance Windows Agent Linux Agent					
New	Edit	Delete	Scheduled	Discover	History Search...
Name	Type	Root IPs	Include Range	Ex Re	Last Discovery time
ADX	Range Scan		172.16.20.160		
Aruba	Range Scan		192.168.26.7		
Checkpoint	Range Scan		172.16.0.1		
Cisco IOS	Range Scan		192.168.20.1, 172.16.3.2, 192.168.10.1		
Fortigate Firewall	Range Scan		192.168.3.1		
FortiGate Firewall	Range Scan		192.168.3.1		Oct 09 2021, 09:21:13 AM
FortiLink	Range Scan		172.16.0.4		
IPsec Peer	Range Scan		172.16.22.2		
Juniper FW	Range Scan		172.16.255.70		
Jun OS	Range Scan		172.16.5.64		
Linux	Range Scan		192.168.0.16		
Other FTNT Firewalls	Range Scan		172.16.255.82, 10.1.1.1		
Palo Alto	Range Scan		172.16.1.2		
Solaris	Range Scan		172.16.10.6		
Windows	Range Scan		172.16.10.28, 192.168.0.10-192.168.0.40, 172.16...		

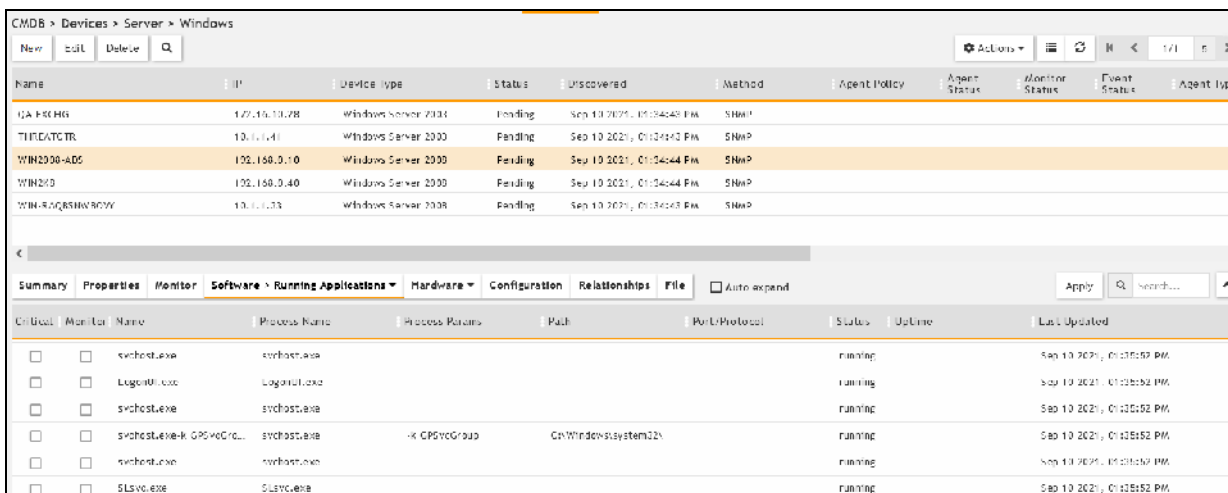
After the discovery task is finished for each device, you should see a message similar to the message in the following image:



2. On the **Monitor Performance** tab, review the system monitors applied to each device.



3. Click the **CMDb** tab, and then review the devices and device categorizations. (You may need to click **Refresh**.)
4. In the left pane, click **Devices > Server > Windows**.
5. In the main window, select the **WIN2008-ADS** device, and then in the lower pane that contains the details, click the **Software** tab.
6. Click the **Running Applications** subtab, and then in the search field, type **iis**.
Notice the list of running applications populated from the discovery for IIS.



7. Make a note of the entries in the **Process Name** and **Process Params** columns.
See "Appendix: Answer Sheet" on page 241 for the answer.

- Type **DNS** in the search field, and then make a note of the entries in the **Process Name** and **Process Param** columns again.

See "Appendix: Answer Sheet" on page 241 for the answer.

- In the left pane, click **Applications > Infrastructure App > DNS**, and then select **Microsoft DNS** in the main window.
- In the lower pane that contains the details, click the **Summary** tab.
Notice how the CMDB knows which devices in the environment are running the DNS process.

CMDB > Applications > Infrastructure App > DNS

App Group	App Name	Process
Bind DNS	Bind DNS	named
DNS Forwarder	DNS Forwarder	dnsmasq
InfoBlox NIOS	InfoBlox NIOS	
Microsoft DNS	Microsoft DNS	dns.exe

Summary Running On ☐ Auto expand

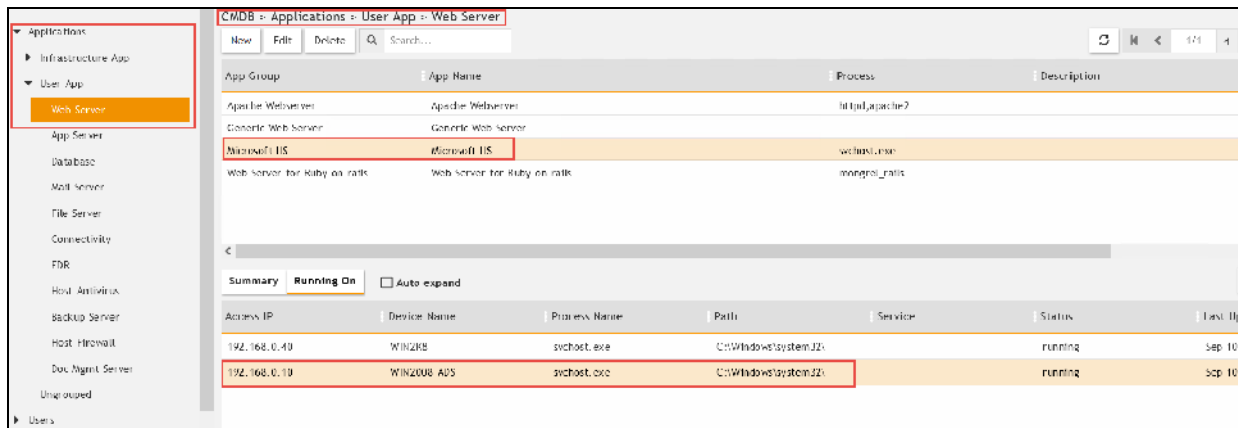
Name: Microsoft DNS

Running On: 2

Process Name: dns.exe

Description:

- In the left pane, click **Applications > User App > Web Server**, and then select **Microsoft IIS** in the main window.
Again, notice how FortiSIEM knows which devices are running IIS by tracking the process names running during discovery.



12. Log out of the FortiSIEM GUI.

Exercise 5: Bringing in Scripted Data

Now that the devices are populated in the CMDB, you will start to bring in scripted performance and security data.

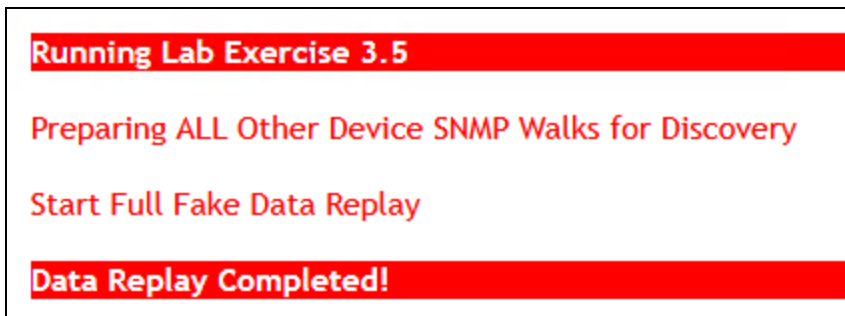
Pull Data From Devices

You will generate some scripted performance and security events, and then view that data on FortiSIEM.

To pull data from devices

1. On the Linux-Client VM, open a browser, and then go to the NSE Institute website.
2. Navigate to **LABS SET 1**, and then under **Lab 3—Discovery**, select **Exercise 3.5—Start All Performance and Device Data**.

The output takes approximately two minutes to return and should resemble the following example:



Leave the Linux-Client VM browser tab open. You will return to it in the next lab.

3. Log in to the FortiSIEM GUI with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Domain	LOCAL

4. Click the **ANALYTICS** tab, and then click the search field to edit the condition.
5. In the **Filters** section, select **Attribute**, and then configure the following settings to create a new query:

Field	Value
Event Attribute	Raw Event Log
Operator	CONTAIN
Value	*

- Beside **Time Range**, select **Real Time**.
- Click **Apply & Run**.



Make sure the search field is empty (it may contain text from another exercise).

Wait a few seconds, and then you will see various events arriving.

Filter

Saved Filters ...

Clear All

☐ Keyword

☒ Attribute

Paren	Attribute	Operator	Value	Paren	Next	Row
+	-	Raw Event Log	CONTAIN	↓	*	

Time

☒ Real Time

☐ Relative

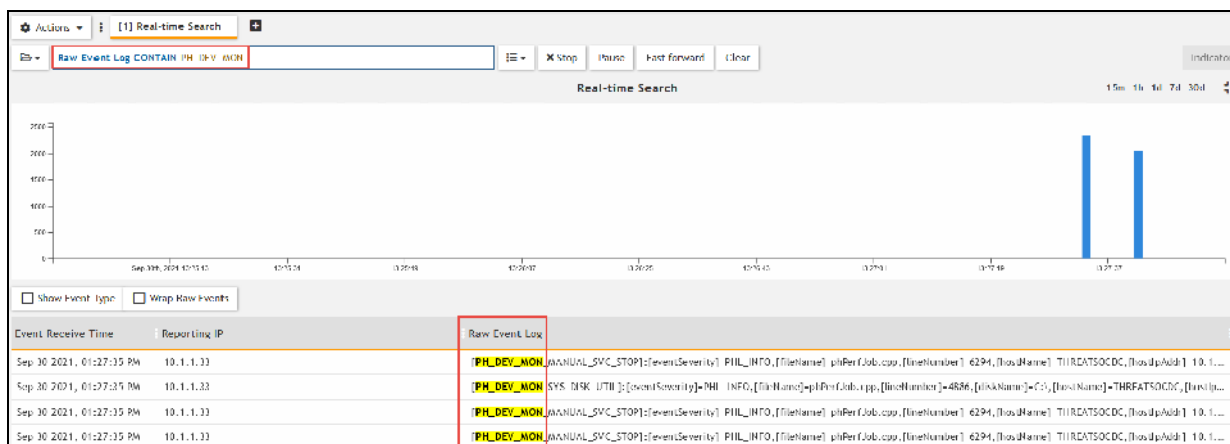
☐ Absolute

Apply & Run

Apply

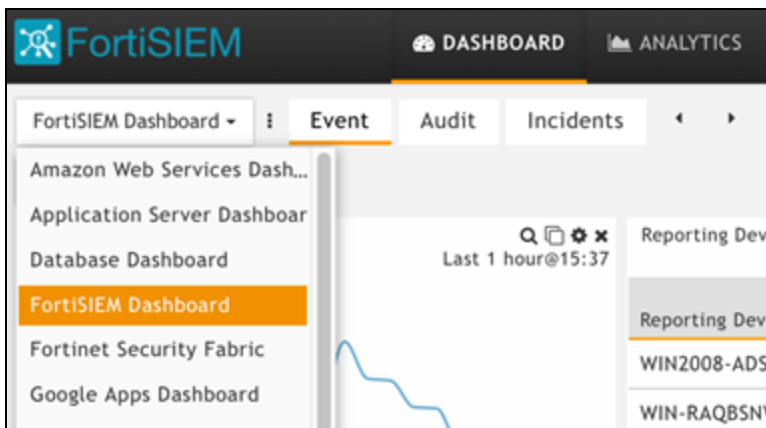
Cancel

- Remove the asterisk from the filter box, type `PH_DEV_MON`, and then click **Apply & Run** again. After waiting a minute or so, you should start to see performance metric events.

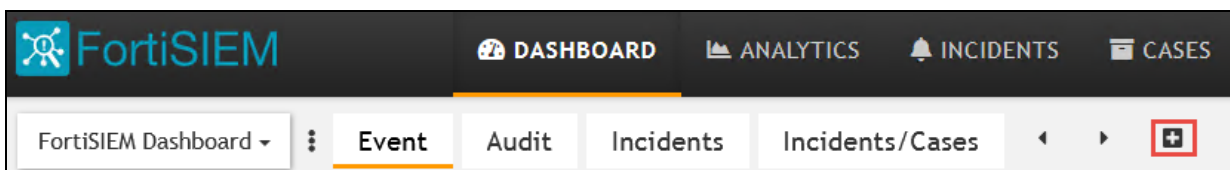


To view all devices on the summary dashboard

1. Continuing on the FortiSIEM GUI, click the **DASHBOARD** tab, and then click the down arrow on the **Application Server Dashboard**.
2. In the drop-down list, select **FortiSIEM Dashboard**.



3. On the FortiSIEM dashboard, select the **+** icon beside the **Incidents/Cases** tab to add a new dashboard.

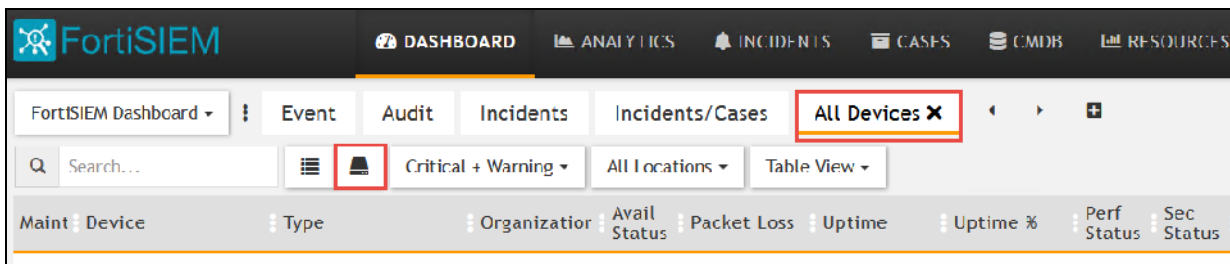


The **Create New Dashboard** pop-up window opens.

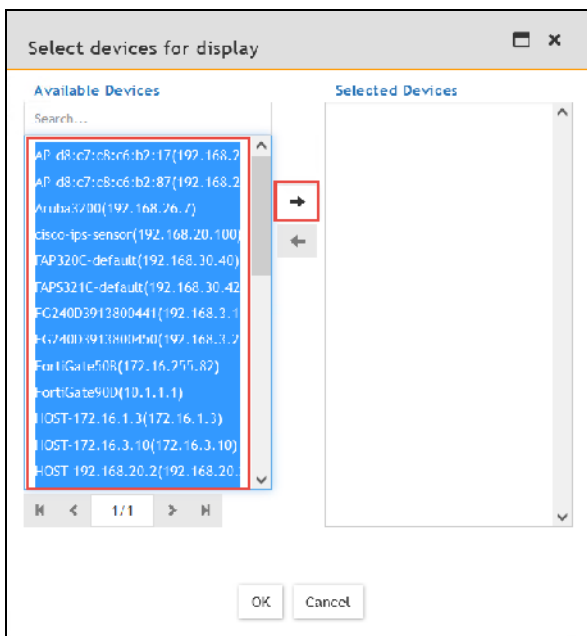
4. Configure the following settings:

Field	Value
Name	All Devices
Type	Summary Dashboard

5. Click **Save**.
6. Select the **All Devices** tab for the dashboard you just created.
7. Click the select devices icon (🖨️) beside the search bar to add all devices.



The **Select devices for display** pop-up window opens.



8. Select all devices in the **Available Devices** column.
9. Use the right-arrow icon to add all selected devices to the **Selected Devices** column.
10. Click **OK**.
11. When the **All Devices** dashboard opens, select **All Severities** in the filter.

Main/Device	Critical	Organization	Avail Status	Packet Loss	Uptime	Uptime %	Perf Status	Sec Status	CPU Util	Mem Util
FortiGate900	Critical - Warning	Super	●	0%	20 days	100%	●	●	100%	41%
WIN-KAGHNSWADYY	All Severities	Super	●	10%	7 hours	100%	●	●	1%	61%
WIN2K8	Microsoft Windows Server 2008	Super	●	0%	979 days	100%	●	●	11%	45%
ibmxa	IBM AIX	Super	●	0%	1048 days	100%	●	●	5%	86%
juniperfir	Juniper SRX JunOS	Super	●	0%	227 days	100%	●	●	20%	79%
THREATCTR	Microsoft Windows Server 2003	Super	●	0%	3 hours	100%	●	●	0%	13%
SLI 124 - Link CDR	Generic Linux	Super	●	10%	1000 days	100%	●	●	1%	15%
SLI Dev A - Edy Platform	Foundry Inware	Super	●	10%	1044 days	100%	●	●	1%	14%
PA-1000-01-accepts	Palo Alto PAN OS	Super	●	10%	778 days	100%	●	●		

Your dashboard should look similar to the example shown above.



Not all devices collect the same system resource metrics, so some columns will be empty. If your system does not resemble the example, tell your instructor.

12. Log out of the FortiSIEM GUI.

Lab 4: FortiSIEM Analytics

In this lab, you will explore the keyword search feature.

Objectives

- Understand the real-time search
- Perform a search for raw log messages
- Perform a historical keyword search
- Employ multiple search conditions
- Explore some of the well-used search operators

Time to Complete

Estimated: 30 minutes

Exercise 1: Getting to Know the Real-Time Search

In this exercise, you will perform a real-time search for raw logs.

View Raw Logs

You will view raw logs on FortiSIEM using a real-time search.

To view all raw logs in a real-time search

1. Log in to the FortiSIEM GUI with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Domain	LOCAL

2. Click the **ANALYTICS** tab.
3. Click the **Group By and Display Fields** drop-down icon.

4. Click **Clear All**, and then click **Apply**.
5. In the pop-up window, click **Use Default**.

6. Click the search field and set it to **Edit Filters and Time Range**.

Action

[1] Real-time Search

Edit Filters and Time Range...

Run

- The **Filter** editor opens.
- Create the following query for an **Event Keyword** type search:

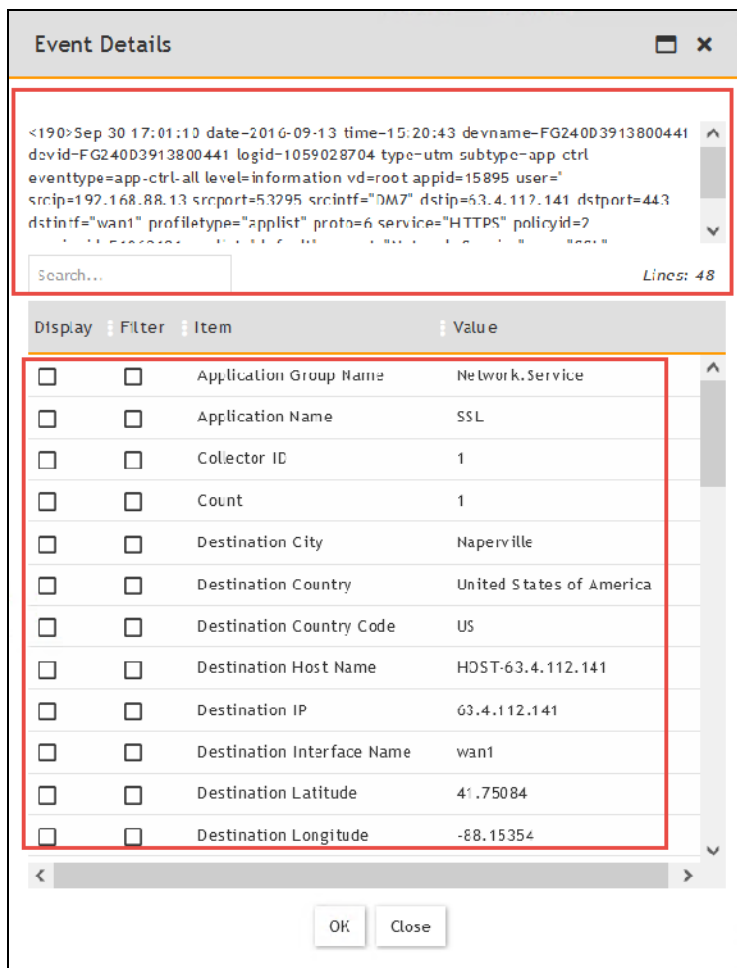
Field	Value
Event Keyword	*

- Beside **Time Range**, select **Real-time**.
- Click **Apply & Run**, let the search run for about 20 seconds, and then click **Pause**.
Notice all the different events being received in real time and the default columns (**Event Receive Time**, **Reporting IP**, **Event Type**, and **Raw Event Log**).



- Make sure **Wrap Raw Event** is selected.
- Make sure **Show Event Type** is selected.

- In the **Raw Event Log** field, select a raw log message.
A right arrow icon appears.
- Click the right arrow icon to display the **Event Details** and view the event details associated with that event.
An **Event Details** dialog box opens.



The top portion of the dialog box includes the raw log that FortiSIEM received.

The bottom portion of the dialog box includes the structured view, which shows all the attributes that FortiSIEM parsed out of the message.

You can use these attributes in structured searches, rules, reports, and on dashboards.

13. Close the **Event Details** dialog box.
14. In the **Filters** section, click **Clear All** to see the functionality of this button.

The screenshot shows a search filter dialog box with the following elements:

- Filter** section with three radio buttons: ☒ **Event Keyword** (with a text input field containing '*'), ☐ **Event Attribute**, and ☐ **CMDB Attribute**.
- Time Range** section with three radio buttons: ☒ **Real-time**, ☐ **Relative**, and ☐ **Absolute**.
- Trend Interval:** A dropdown menu currently set to **Auto**.
- Buttons at the top right: **Load**, **Save**, and **Clear All** (highlighted with a red border).
- Buttons at the bottom right: **Apply & Run**, **Apply**, and **Cancel**.

Notice that as soon as you click **Clear All**, all existing settings are cleared.

15. Click **Apply**.

Exercise 2: Exploring Search Operators

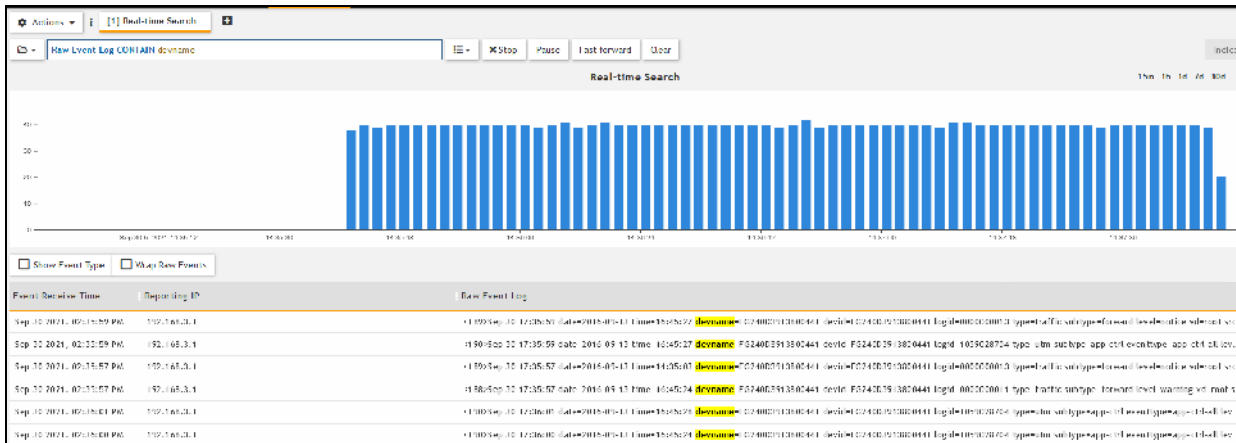
In this exercise, you will explore the use of search operators.

Use Search Operators

You will use various search operators to manipulate FortiSIEM real-time search results.

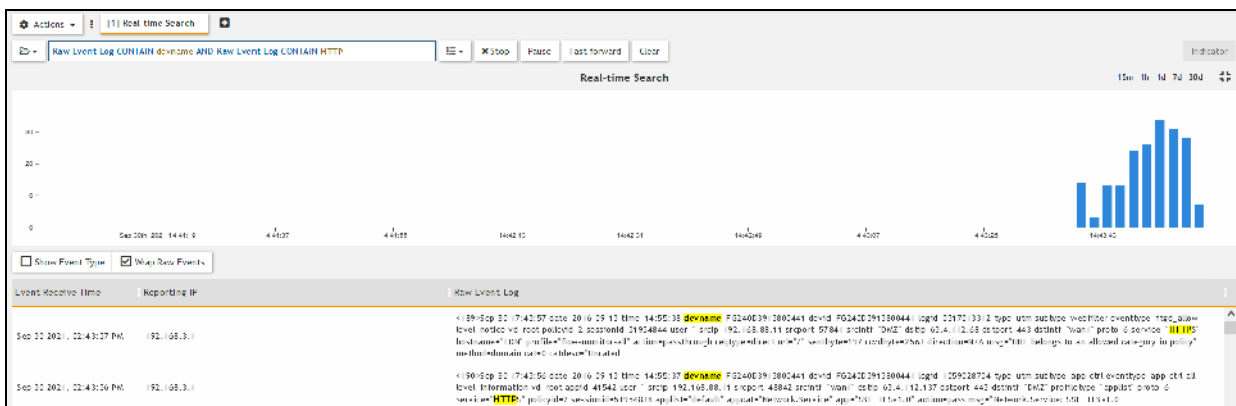
To use search operators

1. Continuing on the FortiSIEM GUI, click the **ANALYTICS** tab, and then click the search field to edit the condition.
2. In the **Filters** section, select **Keyword**, and then type `devname`.
3. Beside **Time Range**, select **Real Time**.
4. Click **Apply & Run**.



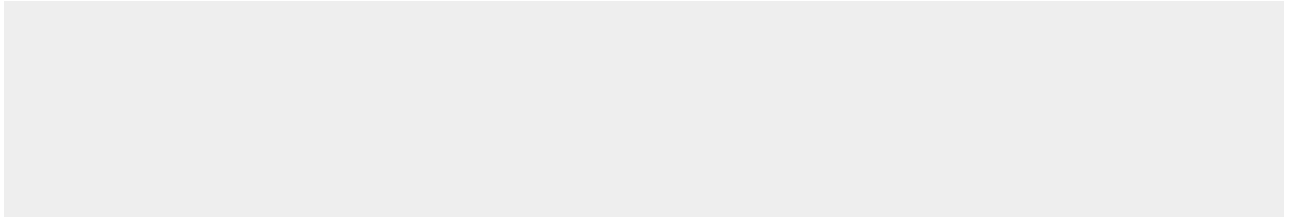
Review the results.

5. Click **Stop**.
6. Modify the search condition again in the **Filter** editor for the **Keyword** condition `devname AND HTTP`.
7. Beside **Time**, select **Real Time**, and then click **Apply & Run**. (Make sure **Wrap Raw Event** is selected.)

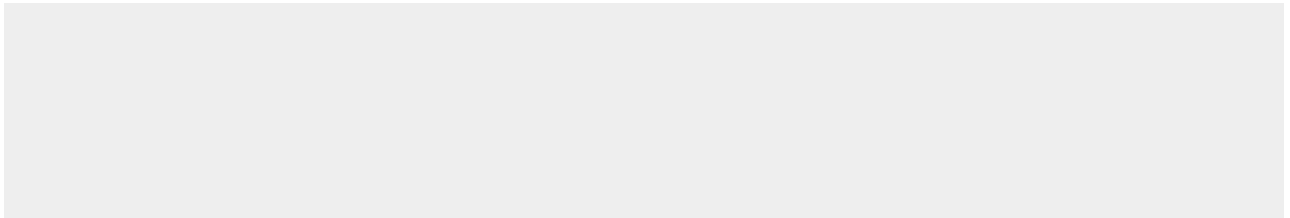


After you receive approximately 50 logs, click **Pause**.

What was the impact of this search? See "[Appendix: Answer Sheet](#)" on page 242 for the answer.



What can you identify about the case sensitivity of keywords? See "[Appendix: Answer Sheet](#)" on page 242 for the answer.



© FORTINET

In this exercise, you will perform a keyword search.

Perform a Keyword Search

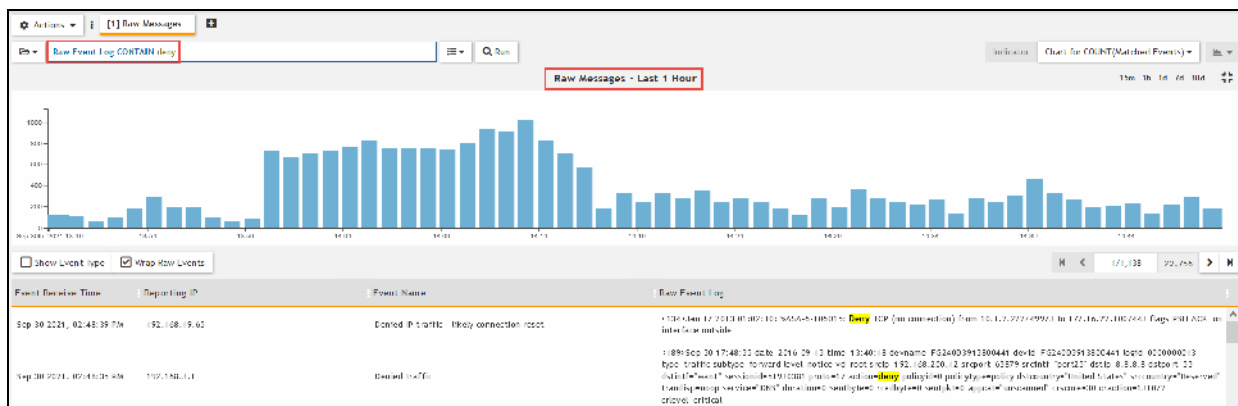
You will use a specific keyword search to filter events on FortiSIEM.

To perform a keyword search

1. Continuing on the FortiSIEM GUI, click the **ANALYTICS** tab, and then click the search field to edit the condition.
2. In the **Filters** editor, configure the following settings to create a new **Event Keyword** query:

Field	Value
Event Keyword	deny

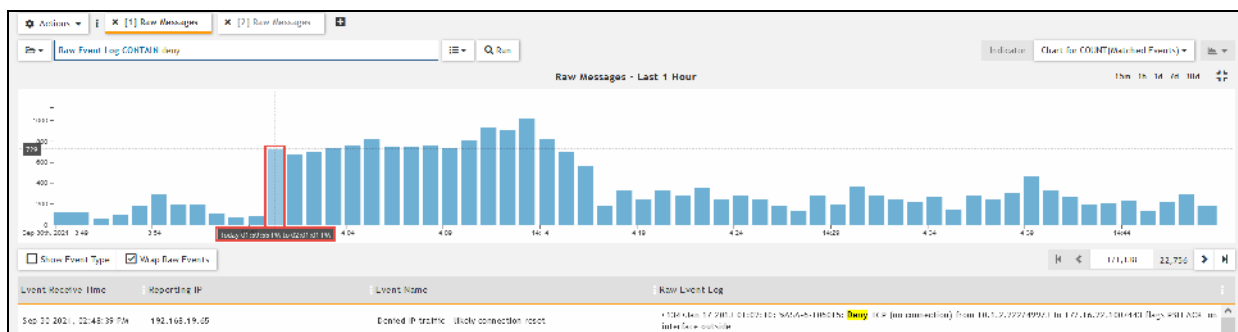
3. Beside **Time Range**, select **Relative**, in the **Last** field, type 1, and then select **Hour**.
4. Click **Apply & Run**.



Events that contain the word **deny** appear.

Notice the graph results show a **COUNT** over time (1 hour in this case) of all the events.

- 5.** Hover over the graph to view the absolute time range for those events during that time period.



- | Time Interval | Message Count (Approx.) |
|---------------------|-------------------------|
| 02:13:00 - 02:13:05 | 190 |
| 02:13:05 - 02:13:10 | 150 |
| 02:13:10 - 02:13:15 | 180 |
| 02:13:15 - 02:13:20 | 160 |
| 02:13:20 - 02:13:25 | 180 |
| 02:13:25 - 02:13:30 | 150 |

- FortiSIEM 6.3 Lab Guide
Fortinet Technologies Inc.

Exercise 4: Using Single Search Conditions

In this exercise, you will explore the use of search conditions.

Configure a Search Condition

You will configure a search condition to narrow down the scope of your search criteria on FortiSIEM.

To add a search condition

- 1. Continuing on the FortiSIEM GUI, click the **ANALYTICS** tab, and then click the search field to edit the condition.
- 2. In the **Filters** editor, click the **Clear All** button to clear any existing conditions, and then configure the following settings to create a new **Event Keyword** query:

Field	Value
Event Keyword	*

- 3. Beside **Time Range**, select **Relative**, in the **Last** field, type 3, and then select **Minutes**.
- 4. Click **Apply & Run**.
Notice all the events received over the specified time period. This could be many lines and pages of data—too many lines to fit on one page. You can jump to any page by entering the page number.

⏮

<

1/2,610

28,709

>

⏭

- 5. Click the search criteria box again, and then select **Attribute**.
This converts a keyword search into an attribute-based search.
- 6. Configure the following settings to change the query:

Field	Value
Attribute	Reporting IP
Operator	=
Value	192.168.3.1

- 7. In the **Last** field, type 5, select **Minutes**, and then click **Apply & Run**.
Notice how all the results include the reporting IP you specified.

Filter Load Save Clear All

☐ Event Keyword *

☒ Event Attribute

Paren	Attribute	Operator	Value	Paren	Next	Row
+	Reporting IP	=	192.168.3.1	+	AND	+

☐ CMDB Attribute

Time Range

☐ Real-time

☒ Relative Last 5 Minutes

☐ Absolute

Trend Interval: Auto

Apply & Run Apply Cancel

Exercise 5: Using Multiple Search Conditions

In this exercise, you will explore the use of multiple search conditions.

Add Multiple Search Conditions

You will configure multiple search conditions to further narrow down the scope of the search on FortiSIEM.

To add multiple search conditions

1. Continuing the search from the last exercise, click the search field to edit the conditions.
2. In the **Next** column associated with your existing condition, select **AND**.
3. In the **Row** column associated with your existing condition, click the **+** icon to add another row.
4. Configure the following settings for your second condition:

Field	Value
Attribute	Destination IP
Operator	=
Value	8.8.8.8

5. Modify the **Time Range** drop-down list to run the search over the last 10 minutes.

Filter

Load Save Clear All

☐ Event Keyword

☒ Event Attribute

Paren	Attribute	Operator	Value	Paren	Next	Row
+	Reporting IP	=	192.168.3.1	+	AND	+
+	Destination IP	=	8.8.8.8	+	AND	+

☐ CMDB Attribute

Time Range

☐ Real-time ☒ Relative Last 10 Minutes ☐ Absolute

Trend Interval: Auto

Apply & Run Apply Cancel

6. Click **Apply & Run**.

Notice how now all the events are reported by a specific device IP going to the destination IP 8.8.8.8.

Exercise 6: Using the CONTAIN Operator

In this exercise, you will explore the use of the CONTAIN operator.

Examine the Use of the CONTAIN Operator

You will use the CONTAIN operator in your search filter, and then observe its effect on the search results.

To use the CONTAIN operator

1. Continuing the search from the last exercise, click the search field, and then click **Clear All** to clear the query.
2. Create the following query for an **Event Attribute** type search:

Field	Value
Attribute	Event Type
Operator	CONTAIN
Value	win-security

3. Leave the search time set to the last 10 minutes, and then click **Apply & Run**.
You should notice that all events returned are related to Windows security.



- Make sure **Wrap Raw Event** is selected.
- Make sure **Show Event Type** is selected.

4. Click the search field to edit the condition.
5. In the **Next** column associated with your existing condition, select **AND**.
6. In the **Row** column associated with your existing condition, click the **+** icon to add another row.
7. Configure the following query to look for only Windows security events that do not have a user with the name **!= svc_monitor**:

Field	Value
Attribute	User
Operator	!=
Value	svc_monitor

Filter Load Save Clear All

☐ Event Keyword

☒ Event Attribute

Paren	Attribute	Operator	Value	Paren	Next	Row
+	Event Type	CONTAIN	win-security	+	-	AND +
+	User	!=	svc_monitor	+	-	AND +

☐ CMDB Attribute

Time Range

☐ Real-time ☒ Relative Last

☐ Absolute

Trend Interval:

Apply & Run Apply Cancel

8. Leave the search time set to the last 10 minutes, and then click **Apply & Run**.
9. Review the **Event Details** of the raw event log for one of the returned events.
10. Scroll to the bottom of the structured view, and then in the row that contains the **User** attribute, select **Display**. This adds an extra display column to the display.

Event Details Close

<13>Sep 30 19:14:19 WIN2008 ADS MSWinEventLog 1 Security 1356822
Mon May 14 12:58:40 2012 4776 Microsoft Windows Security Auditing
administrator N/A Failure Audit WIN2008 ADS Credential Validation
The domain controller attempted to validate the credentials for an account.
Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 Logon

Search... Lines: 30

Display	Filter	Item	Value
☐	☐	Relaying IP	192.168.0.10
☐	☐	Reporting Device	WIN2008-ADS
☒	☐	Reporting IP	192.168.0.10
☐	☐	Reporting Model	Windows
☐	☐	Reporting Vendor	Microsoft
☐	☐	Sequence Number	1356822
☐	☐	Source Host Name	SAA3-CUST111
☐	☐	System Event Category	0 (External)
☐	☐	Time skew	296028939
☐	☐	Type	Failure Audit
☒	☒	User	administrator
☐	☐	Win Logon Fail Code String	0XC000005A (Login failed ...

OK Close

11. Click **OK** to close the **Event Details** dialog box, and then run your search again.
None of the users should be **svc_monitor**.



If you do not get any results for any search, run the search over a longer time period.

Exercise 7: Using the IN and NOT IN Operators

In this exercise, you will explore the use of the IN and NOT IN operators.

Examine the Use of the IN and NOT IN Operators

You will use the IN and NOT IN operators in your search filter, and then observe their effect on the search results.

To use the IN and NOT IN operators

1. Continuing the search from the last exercise, click the search field to modify your query.
2. Modify the existing user condition as follows:

Field	Value
Operator	NOT IN
Value	svc_monitor, administrator

This query is now configured to look for events that are Windows security events, but are not from the administrator or **svc_monitor** user.



Use the **NOT IN** operator when you specify the user (that is, the **User** is **NOT IN** this list).

3. Beside **Time**, select **Relative**, in the **Last** field, type 30, and then select **Minutes**.

4. Click **Apply & Run**.

In your results, you may see many users returned with a \$. These are computer accounts.

Event Receive Time	Reporting IP	Event Name	Raw Event Log	User
Sep 30 2021, 04:23:18 PM	192.168.0.10	Windows logon success	<13>Sep 30 19:23:18 WIN2008-AD5 MSWinEventLog	WIN2008-AD5
Sep 30 2021, 04:23:18 PM	192.168.0.10	Windows logon success	<13>Sep 30 19:23:18 WIN2008-AD5 MSWinEventLog	WIN2008-AD5
Sep 30 2021, 04:23:18 PM	192.168.0.10	Windows logon success	<13>Sep 30 19:23:18 WIN2008-AD5 MSWinEventLog	WIN2008-AD5

5. Modify your search to exclude these computer accounts by adding the following extra condition using the **NOT CONTAIN** operator:
 - a. In the **Next** column associated with the user condition, select **AND**.
 - b. In the **Row** column associated with the user condition, click the **+** icon to add another row.
 - c. Configure the following settings for your new condition:

Field	Value
Attribute	User
Operator	NOT CONTAIN
Value	\$

6. Leave the search time set to the last 30 minutes, and then click **Apply & Run**.

Filter

Load Save Clear All

☐ Event Keyword deny
 ☒ Event Attribute

Parent	Attribute	Operator	Value	Parent	Next	Row
+	Event type	CONTAIN	win-security	+	AND	+
+	User	NOT IN	svc_monitor, administrator	+	AND	+
+	User	NOT CONTAIN	\$	+	AND	+

☐ CMDB Attribute

Time Range
 ☐ Real-time
 ☒ Relative
 Last 30 Minutes

☐ Absolute

Trend Interval: Auto

Apply & Run Apply Cancel

Review the results. You will not see computer accounts.

Exercise 8: Using the IS NOT Operator

In this exercise, you will explore the use of the IS NOT operator.

Examine the Use of the IS NOT Operator

You will use the IS operator in your search filter, and then observe its effect on the search results.

To use the IS NOT operator

1. Continuing on the FortiSIEM GUI, click the **ANALYTICS** tab.
2. Click the **Group By and Display Fields** drop-down icon.

Attribute	Order	Display As	Row	Move
Type in attribute...	▼		+ -	↑ ↓

3. Click **Clear All**, and then click **Apply**.
4. In the pop-up window, click **Use Default**.

Display column cannot be empty. Back to edit or use default?

Go Back Use Default

5. Click the search field, and then click **Clear All** to clear your query.
6. Build an **Event Attribute** search to look for all performance events over a one-hour time period.



All performance events contain the word `PH_DEV_MON`.

Field	Value
Attribute	Event Type
Operator	CONTAIN
Value	ph_dev_mon

- Click **Apply & Run**, and then view the results.
- Add a second condition to your query using the **IS NOT** operator to search only for events that contain the specific attribute you are interested in.

For example:

Field	Value
Attribute	Free Disk MB
Operator	IS NOT
Value	NULL

- Leave the **Time Range** field set to **Relative**, in the **Last** field, type 1, and then select **Hour**.
- Click **Apply & Run**.

The screenshot shows the FortiSIEM Filter dialog box. The 'Event Attribute' section is selected, and two conditions are listed in a table:

Paren	Attribute	Operator	Value	Paren	Next	Row
+	Event Type	CONTAIN	ph_dev_mon	+	AND	+
+	Free Disk MB	IS NOT	NULL	+	AND	+

The 'Time Range' section is set to 'Relative' with 'Last' 1 'Hour'. The 'Apply & Run' button is highlighted.

- Open the **Event Details** dialog box for one of the events, and then select the checkboxes to add the following display columns:
 - **Disk Capacity Util**
 - **Disk Name**
 - **Free Disk MB**



- Once the **RAW Event log** is selected, a right arrow  icon appears.
- Click the icon to display the **Event Details** associated with that event.

Event Details

[PH_DEV_MON_SYS_DISK_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,[lineNumber]=8745,[diskName]=/, [hostName]=SJ-Dev-Core-Srv,[hostIpAddr]=192.168.0.16,[diskUtil]=77.255287,[totalDiskMB]=65652,[usedDiskMB]=50719,[freeDiskMB]=14932,[pollIntv]=176,[phLogDetail]=

Lines: 30

Display	Filter	Item	Value
☐	☐	Collector ID	1
☐	☐	Count	1
☒	☐	Disk Capacity Util	77.26
☒	☐	Disk Name	/
☐	☐	Event ID	3007137913692761017

12. Click **OK** to close the **Event Details** dialog box.

13. Click **Run**.

Actions

[1] Raw Messages

Event Type CONTAIN ph_dev_mon AND Free Disk MB IS NOT NULL

Run

Raw Messages - Last 1 Hour

Review the results. Three new fields were added to the display column for all events.

Disk Capacity Util	Disk Name	Free Disk MB
93.02%	/var	60 MB
77.26%	/	14.58 GB
63.08%	C:\myDisk	14.76 GB
3.31%	/home	31 MB
33.54%	C:\ Label: Serial Number c49509d1	26.58 GB
12.34%	/boot	87 MB

Exercise 9: Using the Greater Than Operator

In this exercise, you will explore the use of the greater than operator.

Examine the Use of the > Operator

You will use the > (greater than) operator in your search filter, and then observe its effect on the search results.

To use the greater than operator

1. Continuing the search from the last exercise, click the search field to modify the query.
2. Add the following additional condition to look only for events where the **Disk Capacity Util** is greater than 80%:

Field	Value
Attribute	Disk Capacity Util
Operator	>
Value	80

Filter

Load Save Clear All

☐ Event Keyword

☒ Event Attribute

Paren	Attribute	Operator	Value	Paren	Next	Row
+	Event Type	CONTAIN	ph_dev_mon	+	AND	+
+	Free Disk MB	IS NOT	NULL	+	AND	+
+	Disk Capacity Util	>	80	+	AND	+

☐ CMDB Attribute

Time Range

☐ Real-time ☒ Relative Last 1 Hour

☐ Absolute

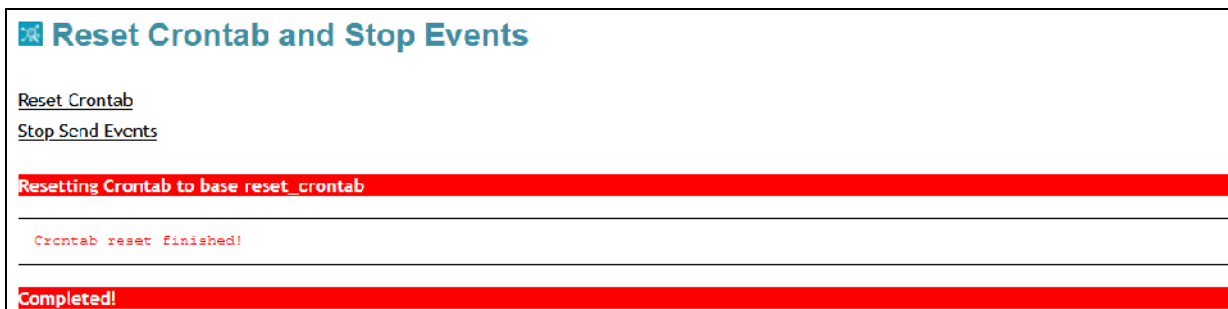
Trend Interval: Auto

Apply & Run Apply Cancel

3. Leave the search time set to the last 1 hour, and then click **Apply & Run**.
4. Review the results.
5. Click the **Group By and Display Fields** icon, and then click **Clear All**.
6. Click **Apply**, and then click **Use Default**.
7. Log out of the FortiSIEM GUI.

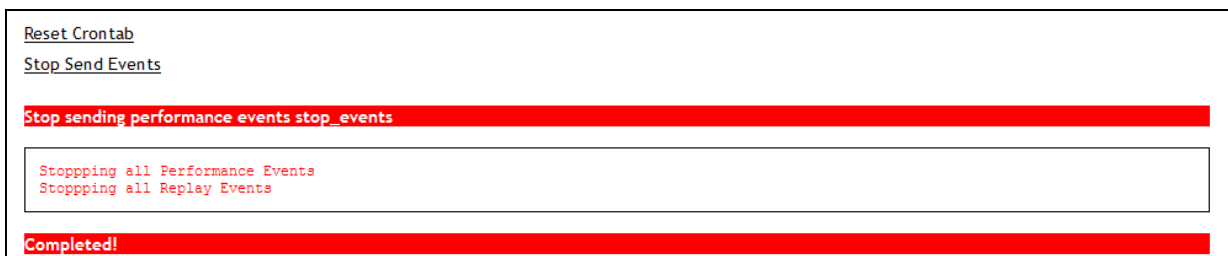
To reset crontab and stop replay events

1. Return to the Linux-Client VM, in the browser tab connected to the **NSE Institute** website, navigate to the **RESET** tab, and then click **Reset Crontab**.



Wait for 10 seconds for the crontab reset to finish.

2. Click **Stop Send Events**.



This stops all performance and replay events.

3. Close the Linux-Client VM browser tab.

Lab 5: CMDB Lookups and Filters

In this lab, you will explore how you can reference the CMDB in searches in FortiSIEM.

Objectives

- Reference CMDB elements in search criteria
- Add and remove display columns
- Use multiple tabs to compare similar search results

Time to Complete

Estimated: 45 minutes

Exercise 1: Selecting Devices From the CMDB

In this exercise, you will reference devices from the CMDB in search criteria.

Build a Query Using Devices From the CMDB

You will create a search query using devices from the CMDB as search criteria.

To select devices from the CMDB

1. Log in to the FortiSIEM GUI with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Domain	LOCAL

2. Click the **ANALYTICS** tab.
3. Click the search field to edit the condition.
The **Filter** editor opens.
4. Click **Clear All** to clear the previous query.

Event Type CONTAIN ph_dev_mon AND Free Disk MB IS NOT NULL AND Disk Capacity Util

Filter

Event Keyword

Event Attribute

Paren	Attribute	Operator	Value	Paren	Next	Row
+	Event Type	CONTAIN	ph_dev_mon	+	AND	1
+	Free Disk MB	IS NOT	NULL	+	AND	2
+	Disk Capacity Util	>	80	+	AND	3

CMDB Attribute

Time Range

Real-time Relative Last 1 Hour

Absolute

Trend Interval: Auto

Apply & Run Apply Cancel

5. Build an **Event Attribute** search to configure the following settings:

Field	Value
Attribute	Reporting IP
Operator	IN

- Click the **Value** field, and then select **Select from CMDB** in the drop-down menu.

The screenshot shows the 'Filter' dialog box with the 'Event Attribute' section active. The 'Value' field is highlighted, and a dropdown menu is open with 'Select from CMDB' selected. The 'Event Keyword' section is also visible.

The **Select Value** dialog box opens.

- In the **Select Value** dialog box, in the **Folders** pane, click **Devices > Network Device > Firewall**.
The firewall devices appear in the middle column.
- Click **>>** to add the folder to the **Selections** pane.
- Click **OK** to close the dialog box.

The screenshot shows the 'Select Value' dialog box. The 'Folders' pane on the left shows 'Devices > Network Device > Firewall' selected. The 'Items' pane in the center shows a list of firewall devices. The 'Selections' pane on the right shows 'Group: Firewall'. The 'OK' button is highlighted.

10. In the **Time Range** section, select **Relative**, in the **Last** field, type 1, and then select **Hour**.
11. Click **Apply & Run**.

Filter

Load Save Clear All

☐ Event Keyword

☒ Event Attribute

Paren	Attribute	Operator	Value	Paren	Next	Row
+	Reporting IP	IN	Group: Firewall	-	AND	+ -

☐ CMDB Attribute

Time Range

☐ Real-time ☒ Relative Last 1 Hour

☐ Absolute

Trend Interval: Auto

Apply & Run Apply Cancel



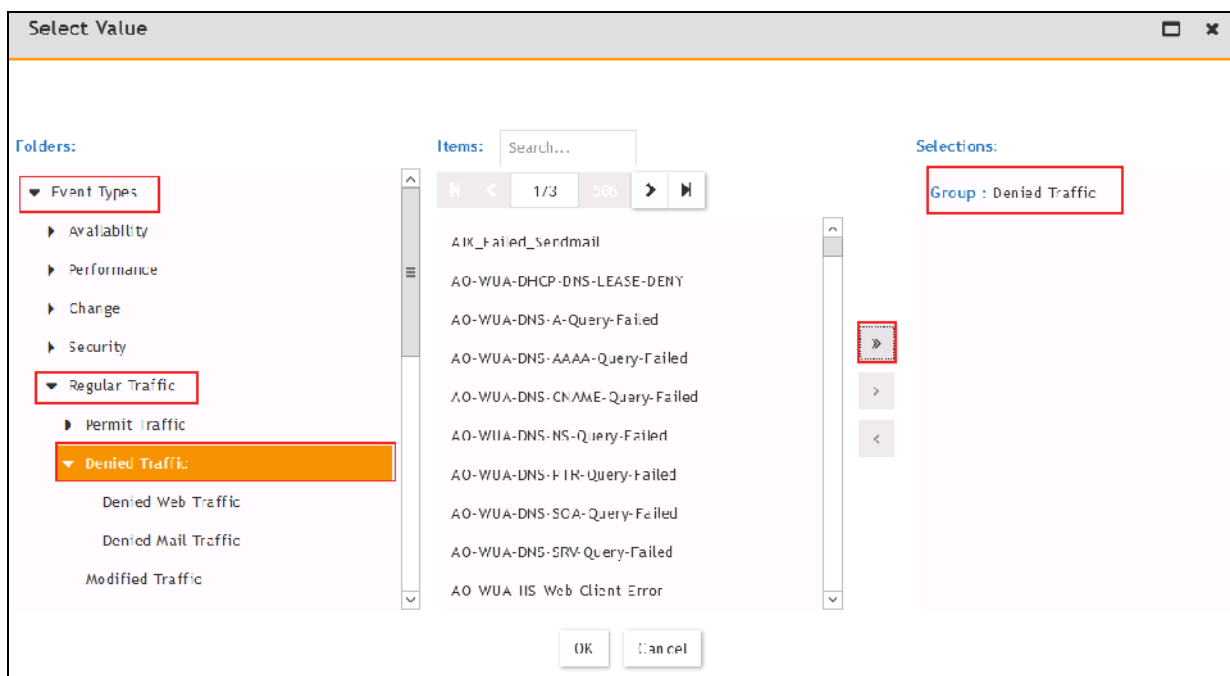
If you do not get any results for any search, run the search over a longer period of time.

To add a second query

1. Continuing on the FortiSIEM GUI, click the search field again to add a second condition to your query.
2. In the **Next** column associated with the existing condition, select **AND**.
3. In the **Row** column associated with the existing condition, click the **+** button.
4. Complete the following for the second condition:

Field	Value
Attribute	Event Type
Operator	IN

5. Click the **Value** field, and then select **Select from CMDB**.
6. Click **Event Types > Regular Traffic > Denied Traffic**, and then click **>>** to add the folder to **Selections**.



7. Click **OK**.
8. Leave **Time Range** set to **Relative**, in the **Last** field, type 1, and then select **Hour**.
9. Click **Apply & Run**.
This narrows your search to denied traffic events only.



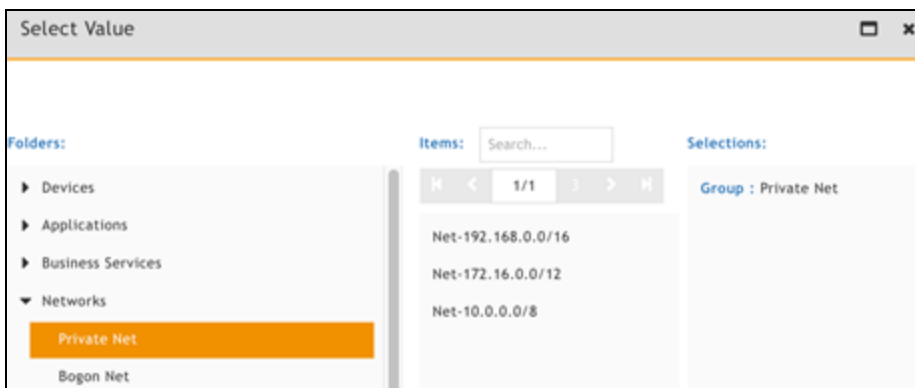
If you do not get any results for any search, run the search over a longer period of time.

To add a third query

1. Continuing on the FortiSIEM GUI, click the search field again to add a third condition to your query.
2. In the **Next** field of the second condition, select **AND**, and then in the **Row** field, click **+** to add a third condition.
3. Add the following third condition to view events where the **Destination IP** is **NOT IN** a private RFC 1918 address:

Field	Value
Attribute	Destination IP
Operator	NOT IN

4. Click the **Value** field, and then select **Select from CMDB**.
5. Click **Networks > Private Net**.
Notice this lists three network entries that relate to the private IP space of RFC 1918.
6. Click **>>** to add the folder to **Selections**.
7. Click **OK**.



8. Leave the **Time** field set to **Relative**, in the **Last** field, type 1, and then select **Hour**.
9. Click **Apply & Run**.

In the results, you should notice that all the destination IP addresses are external to the network, but there may also be some events where the source is also a public IP address.

To add a fourth query

1. Continuing on the FortiSIEM GUI, click the search field again to create a fourth filter condition for your query.
2. In the **Next** field of the third condition, select **AND**, and then in the **Row** field, click **+** to add a fourth condition.
3. Add the following fourth condition to view events where any source IP address is in the private network group:

Field	Value
Attribute	Source IP
Operator	IN

4. Click the **Value** field, and then select **Select from CMDB**.
5. Click **Networks > Private Net**.
6. Click **>>** to add the folder to **Selections**.
7. Click **OK**.
8. Leave the **Time** field set to **Relative**, in the **Last** field, type 1, and then select **Hour**.
9. Click **Apply & Run**.

Your final query should match the following image:

Filter Load Save Clear All

☐ Event Keyword

☒ Event Attribute

Paren	Attribute	Operator	Value	Paren	Next	Row
+	Reporting IP	IN	Group: Firewall	+	AND	+
+	Event Type	IN	Group: Denied Traffic	+	AND	+
+	Destination IP	NOT IN	Group: Private Net	+	AND	+
+	Source IP	IN	Group: Private Net	+	AND	+

☐ CMDB Attribute

Time Range

☐ Real-time

☒ Relative Last 1 Hour

☐ Absolute

Trend Interval: Auto

Apply & Run Apply Cancel

10. Once the search is complete, click the **Group By and Display Fields** drop-down list, and then add a new row to display a column for **Destination TCP/UDP Port**.

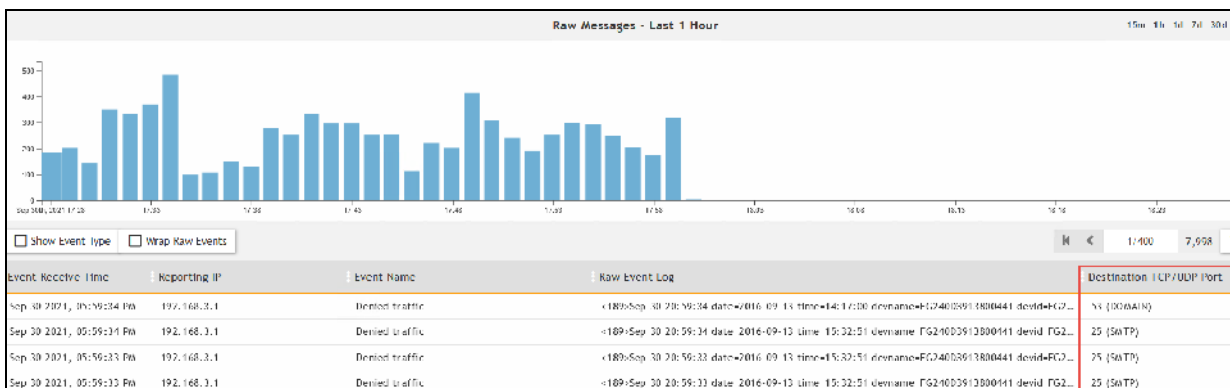
Run Indicator

Group By and Display Fields Load Save Clear All

Attribute	Order	Display As	Row	Move
Event Receive Time	DESC		+ -	↑ ↓
Reporting IP			+ -	↑ ↓
Event Type			+ -	↑ ↓
Raw Event Log			+ -	↑ ↓
Destination TCP/UDP Port			+ -	↑ ↓

Apply & Run Apply Cancel

11. Click **Apply & Run** again, and then see if you can identify the most commonly blocked port.
The search results should look like the following example:



12. Once you have finished reviewing the event logs, click the **Group By and Display Fields** drop-down list again.
13. Click **Clear All** to remove the **Destination TCP UDP/Port** display column.
14. Click **Apply**, and then click **Use Default**.
This reverts the display fields back to the default values.



You can build queries similar to this exercise for other devices like Windows servers, and so on.

15. Log out of the FortiSIEM GUI.

Exercise 2: Searching for Categories of Events

In this exercise, you will select event categories from the CMDB in your search criteria.

Build a Query Using Categories From the CMDB

You will create a search query using event categories from the CMDB as search criteria.

To use an event category from the CMDB

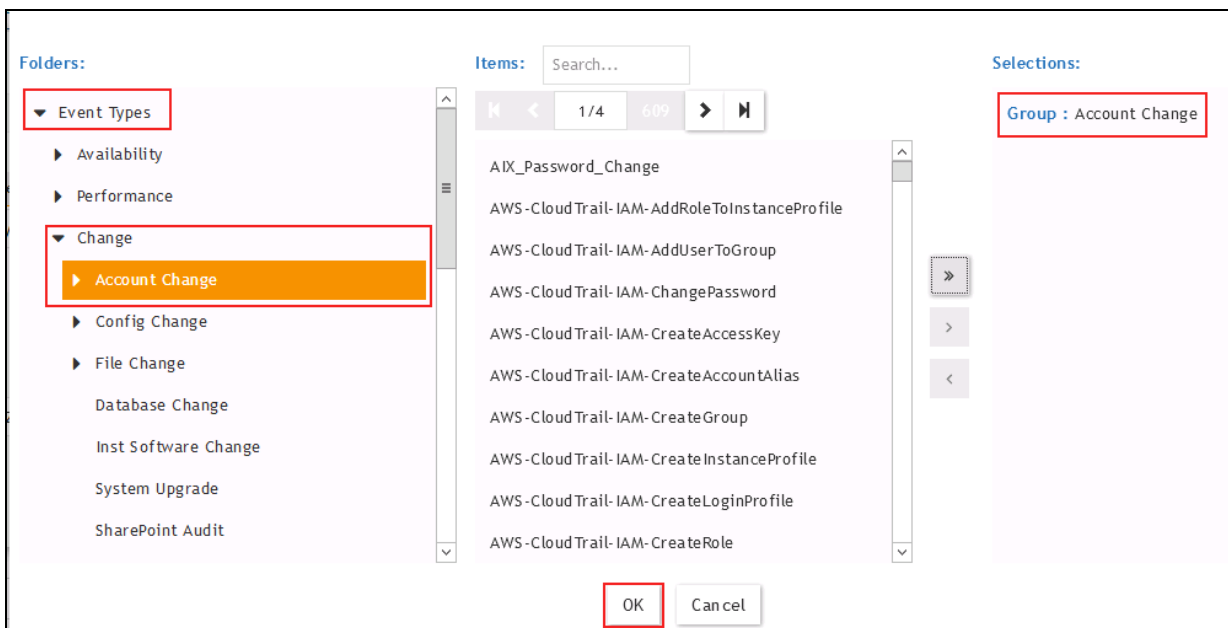
1. Log in to the FortiSIEM GUI with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Domain	LOCAL

2. Click the **ANALYTICS** tab, and then click the search field to edit the condition.
The **Filter** editor opens.
3. Click **Clear All** to clear any existing conditions.
4. Build an **Event Attribute** search, and then add the following condition:

Field	Value
Attribute	Event Type
Operator	IN

5. Click the **Value** field, and then select **Select from CMDB**.
6. Click **Event Types > Change > Account Change**.
7. Click >> to add the folder to **Selections**.



8. Click **OK** to close the CMDB dialog box.
9. Run the search over the last three hours.



If you do not get any results for any search, run the search over a longer period of time. Also, make sure **Wrap Raw Event** and **Show Event Type** are selected.

To add a condition to the existing filter from event logs

1. Continuing on the FortiSIEM GUI, in the received results, select the **Event Type** with the name **Win-Security-4728**.



Win-Security-4728 may not be on the first page of the search results.

2. In the **Event Type** field associated with your selected event type, click the down arrow, in the drop-down menu, select **Add to Filter**, and then in the second drop-down menu, select **=** (equal sign).

- Click the search criteria field.

The **Win-Security-4728** event type is added as a filter to the query.

- Run the search again over the last four hours.

To build a query for investigating an event without losing the existing query

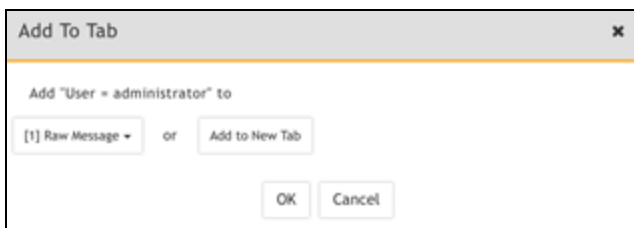
- Continuing on the FortiSIEM GUI, examine the **Event Details** of the raw event log for one of the returned events.



When you select **RAW Event log**, a right arrow icon (→) appears. Click the icon to display the **Event Details** associated with that event.

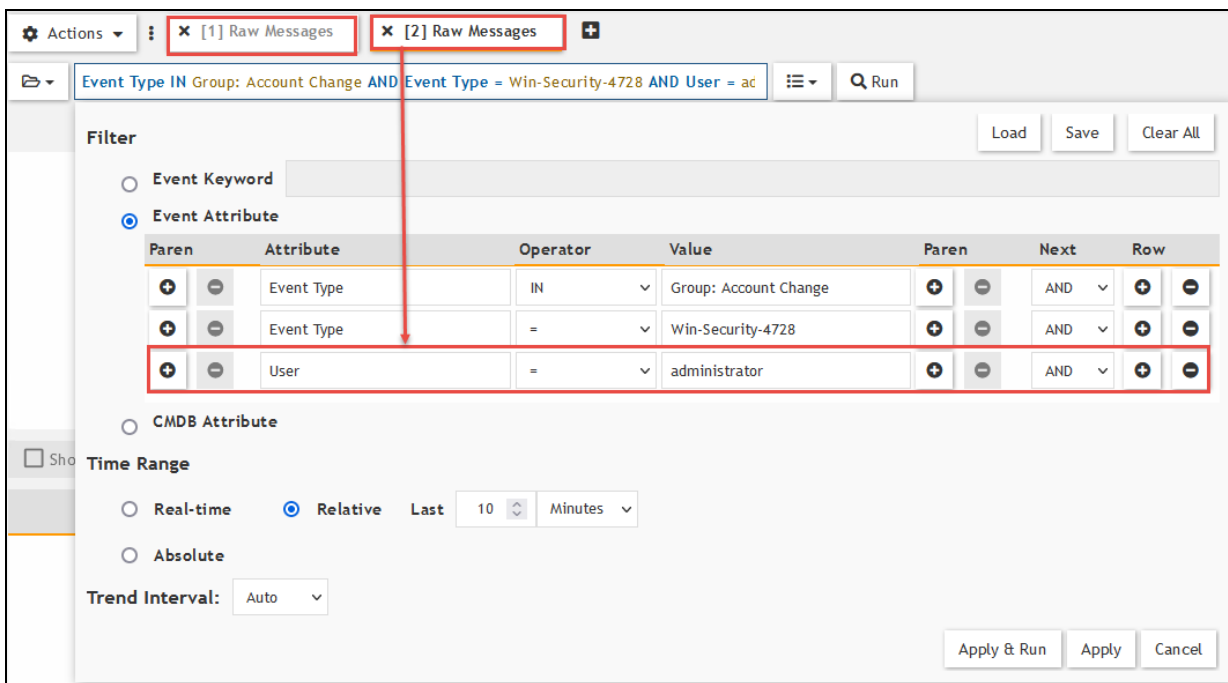
- In the **Event Details** dialog box, in the **Display** column, select the **Target User**, **Target User Group**, **User**, and **Destination IP** checkboxes to add those items as display fields.
- Click **OK**.
- Run the search again over the last four hours.
- Investigate any events with the administrator user in more detail, without losing the existing query.

6. Select an event that has **User** set to **administrator**.
7. In the **User** column, click the down arrow.
8. Select **Add to Tab**.
9. In the **Add To Tab** dialog box, select **Add to New Tab**.

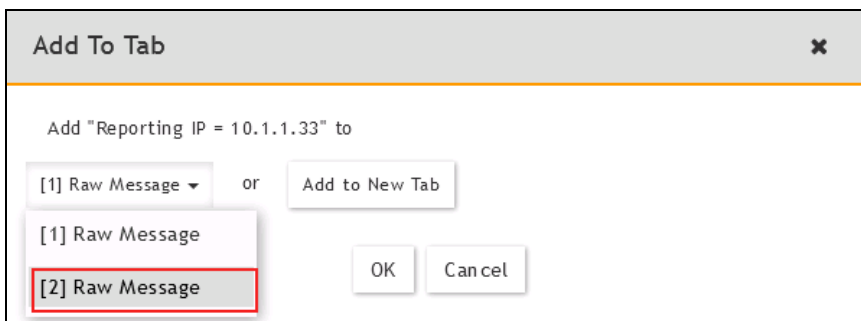


The second tab becomes the active tab in the GUI. You should now have two query tabs.

10. Click the search field on the newly opened second tab.
Your extra filter condition has been added. Your existing query is also still open on the first tab.

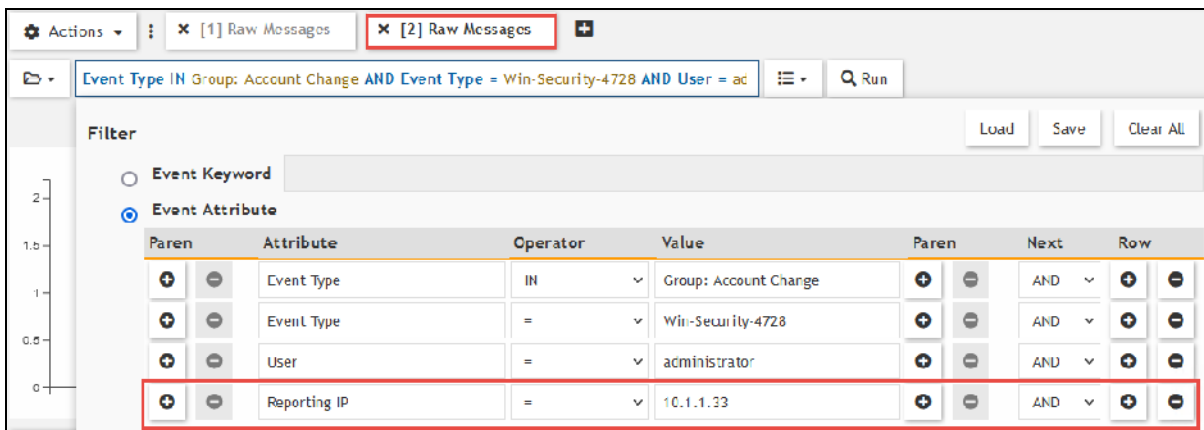


11. Click the first tab, and then select the event with the destination IP address of **10.1.1.33**.
12. In the **Reporting IP** column of that event, click the down arrow, and then click **Add to Tab**.
13. This time, select an existing tab by clicking **[1] Raw Messages**, and then in the drop-down list that appears, select the second tab **[2] Raw Messages**.
14. Click **OK**.



The second tab becomes the active tab in the GUI.

15. Click the search field again to validate that the additional row for the reporting IP filter has been added to the query.



16. In the **Time** section, select **Relative**, in the **Last** field, type 10, and then select **Hours**.
17. Click **Apply & Run**, and then review the results.
18. Once you have reviewed the results, close the search tab that displays your results.
19. Log out of the FortiSIEM GUI.

Exercise 3: Expert Challenge

In this exercise, you will be presented with various scenarios, and you must identify the search criteria that will produce the correct outcome for each scenario.

Conduct a Historical Search

You will create search queries based on the scenarios presented in this section to perform various searches on FortiSIEM.

To conduct scenario-based historical searches

1. Log in to the FortiSIEM GUI with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Domain	LOCAL

2. Click the **ANALYTICS** tab, and then click the search field to edit the condition.
3. Close any search tabs that are open, and then attempt the following searches. For a historic event search, use the **Relative** or **Absolute** options for **Time**.
 - a. There has been some unusual behavior reported by a Solaris administrator. The administrator wants you to create a report of all events reported by the Solaris device with the IP address 172.16.10.6 over the last two hours, and then identify the following:
 - Which user failed an SSH login?
 - Which IP address did the failed login come from?

See "[Appendix: Answer Sheet](#)" on page 242 for the answer.

- b. The firewall team has asked you to perform a search of all events between source IP 68.94.156.1 and destination IP 192.168.0.10 over the last two hours, and display the destination TCP/UDP port. They suspect this machine could have been compromised. Do you see any suspicious port usage in your results?

See "[Appendix: Answer Sheet](#)" on page 242 for the answer.

- c. The firewall team implemented a new firewall, but they are unsure if they configured it correctly. They would like a report of all logs from a source IP in the internal network to an external destination IP that are permitted connections, but not on the common TCP/UDP ports of 80, 443, 53, or 123.
- Produce the report, determine whether they were successful or not over the last three hours, and then display the destination TCP/UDP port as a display column.
 - The firewall should allow only common web traffic (ports 80, 443, 53, or 123) outbound. Do your results indicate the firewall rules are correctly implemented?



Use the CMDB to determine permitted traffic classifications for events and network lists for internal and external traffic.

See ["Appendix: Answer Sheet" on page 242](#) for the answer.

- d. There has been plenty of news in the media about malware attacks originating in Asia. The CISO wants to know if any internal traffic was permitted to any country in Asia in the last two hours that was not on TCP/UDP ports 25, 53, 80, 123, or 443. Add **Sent Bytes**, **Total Bytes**, and **Destination TCP/UDP Port** as display columns to the results.

See ["Appendix: Answer Sheet" on page 242](#) for the answer.

- e. The NOC manager is getting complaints about slow performance to remote sites. These remote sites all connect through the core switch SJ-Main-Cat6500. Produce a list of any events where the **Sent Interface Util** is greater than 20%, and then identify which interfaces on the switch have this issue. Create the search over the last eight hours.



Select the correct device from the CMDB and use the PH_DEV_MON_NET_INTF_UTIL event.

See ["Appendix: Answer Sheet"](#) on page 242 for the answer.

4. Log out of the FortiSIEM GUI.

Lab 6: Group By and Aggregation

In this lab, you will explore the data aggregation features of FortiSIEM.

Objectives

- Group by single and multiple attributes
- Aggregate data

Time to Complete

Estimated: 60 minutes

Exercise 1: Grouping By Single and Multiple Attributes

In this exercise, you will learn how to group similar events based on a single attribute and multiple attributes.

Create a Search Filter Criteria

You will create a search filter on FortiSIEM.

To create the search filter criteria

1. Log in to the FortiSIEM GUI with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Domain	LOCAL

2. Click the **ANALYTICS** tab.
3. Click the **Group By and Display Fields** drop-down icon.

4. Click **Clear All**, and then click **Apply**.
5. In the pop-up window, click **Use Default**.

6. Click the search field, and then click **Clear All** to clear your query.
7. In the **Filters** window, build an **Event Attribute** search, and then configure the following settings to create a new query:

Field	Value
Attribute	Reporting IP
Operator	IN

8. In the **Value** field, click **Select from CMDB**.
9. Click **Devices > Network Device > Firewall**.
10. Click >> to add the folder to **Selections**, and then click **OK**.
11. In the **Time Range** section, select **Relative**, in the **Last** field, type 4, and then select **Hours** in the drop-down list.
12. Click **Apply & Run**.

Filter [Load] [Save] [Clear All]

☐ Event Keyword

☒ Event Attribute

Paren	Attribute	Operator	Value	Paren	Next	Row
[+]	Reporting IP	IN	Group: Firewall	[+]	AND	[+]

☐ CMDB Attribute

Time Range

☐ Real-time ☒ Relative Last 4 Hours

☐ Absolute

Trend Interval: Auto

[Apply & Run] [Apply] [Cancel]

Apply the Group By Criteria

You will configure the **Group By** criteria.

To apply the group by feature

1. Continuing on the FortiSIEM GUI, click **Group By and Display Fields**.
A drop-down list appears.
2. Click the minus icon to remove all the display fields except **Reporting IP**.

Attribute	Order	Display As	Row	Move
Reporting IP	▼		+ -	↑ ↓
Event Type	▼		+ -	↑ ↓

Apply & Run Remove Row Cancel

- Click the plus icon + under the **Row** column to add a new row.
- Click in the **Attribute** field, and then select **COUNT (Matched Events)**.

Attribute	Order	Display As	Row	Move
Reporting IP	▼		+ -	↑ ↓
Type in attribute...	▼		+ -	↑ ↓

* COUNT (Matched Events)

Expression Builder

Apply & Run Apply Cancel

The settings in the **Group By and Display Fields** dialog box should look like the following image:

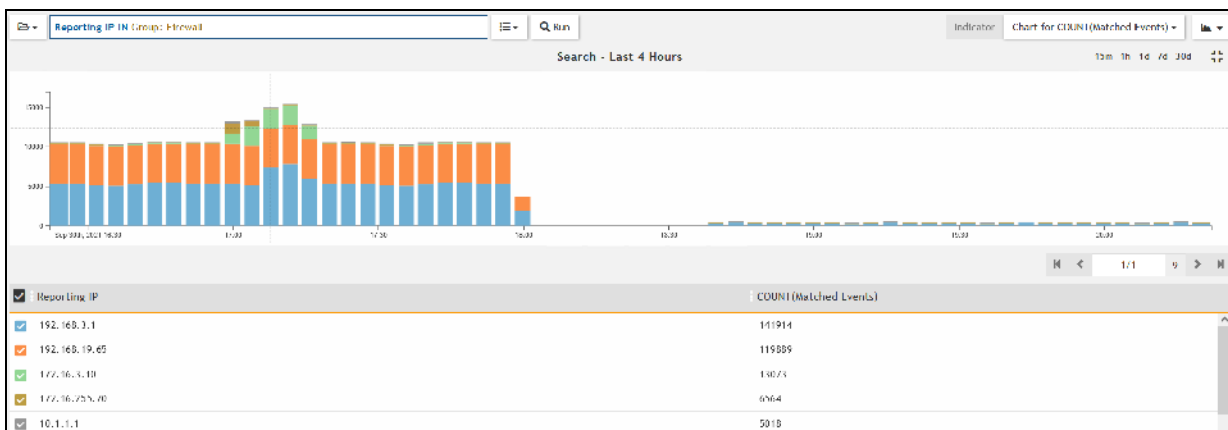
Attribute	Order	Display As	Row	Move
Reporting IP	▼		+ -	↑ ↓
COUNT(Matched Events)	▼		+ -	↑ ↓

Display Conditions

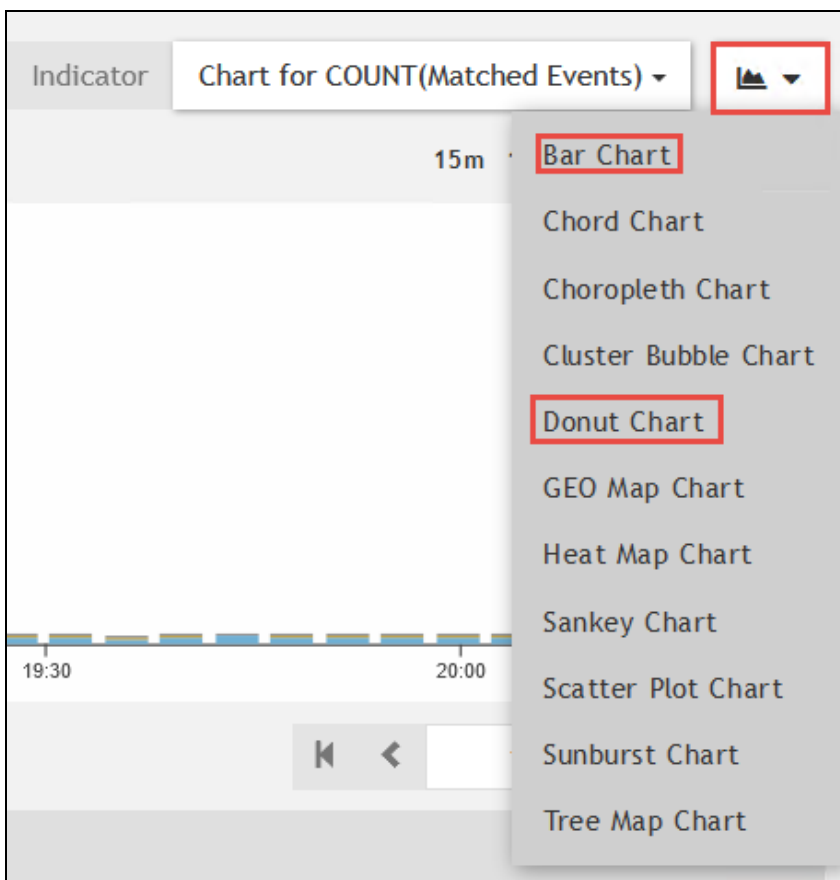
Paren	Attribute	Operator	Value	Paren	Next	Row
+ -	▼	▼		+ -	AND ▼	+ -

Apply & Run Apply Cancel

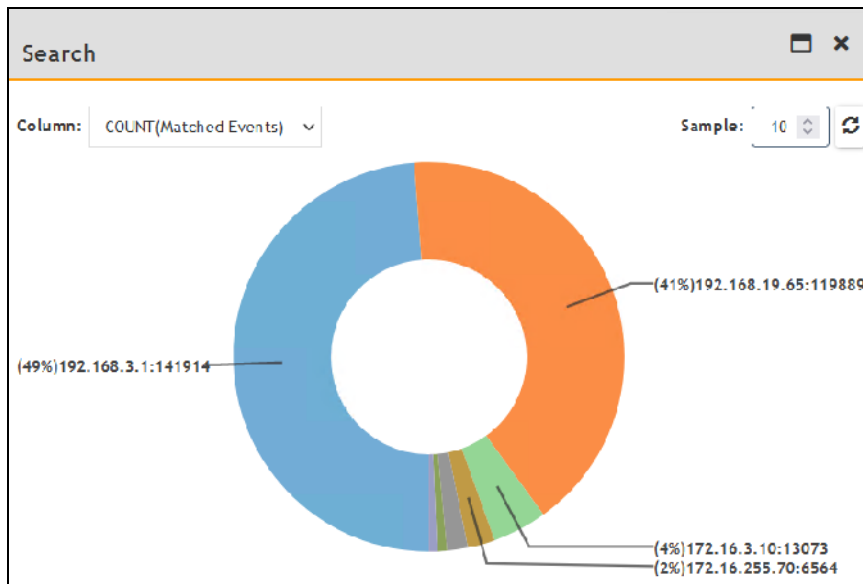
5. In the **Group By and Display Fields** dialog box, click **Apply & Run** to view the **Group By** results. In the results, note the top-down list of the reporting IP addresses that reported the most events in that four hour time period. Notice that the **Reporting IP** attribute column along the **COUNT (Matched Events)** column is returned.



6. Browse the different chart options in the top-right of the graph.
7. Choose and review the following charts:
- **Bar Chart**
 - **Donut Chart**



The following image is an example of a **Donut Chart**:



To add multiple group by attributes

1. Continuing on the FortiSIEM GUI, click the **Group By and Display Fields** icon. A drop-down list appears.
2. In the **Row** column, click the plus icon **+** to add a new row in the **Reporting IP** row, above the **COUNT** expression row.
3. Add the following attributes, one by one. Each time you add an attribute, you must click the plus icon **+** in the **Row** column to add a new row for the new attribute.
 - **Source IP**
 - **Destination IP**
 - **Destination TCP/UDP Port**

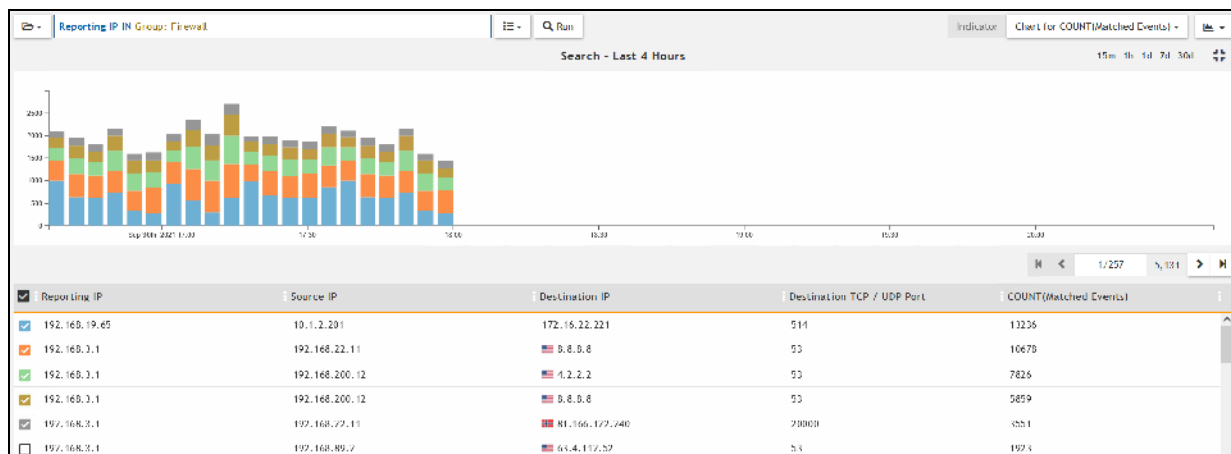
The screenshot shows the 'Group By and Display Fields' configuration window in FortiSIEM. The window has tabs for 'Indicator' and 'Chart for COUNT(Matched Events)'. Below the tabs is a table with columns: Attribute, Order, Display As, Row, and Move. The table contains five rows: Reporting IP, Source IP, Destination IP, Destination TCP/UDP Port, and COUNT(Matched Events). Each row has a plus icon in the 'Row' column. Below the table is a 'Display Conditions' section with a table for adding conditions. The 'Display Conditions' table has columns: Paren, Attribute, Operator, Value, Paren, Next, and Row. The 'Next' column shows 'AND'. At the bottom right, there are buttons for 'Apply & Run', 'Apply', and 'Cancel'.

Attribute	Order	Display As	Row	Move
Reporting IP			+	⬆ ⬇ ⬇ ⬆
Source IP			+	⬆ ⬇ ⬇ ⬆
Destination IP			+	⬆ ⬇ ⬇ ⬆
Destination TCP/UDP Port			+	⬆ ⬇ ⬇ ⬆
COUNT(Matched Events)			+	⬆ ⬇ ⬇ ⬆

Paren	Attribute	Operator	Value	Paren	Next	Row
+				+	AND	⬆ ⬇

4. Click **Apply & Run**.

Review the top-down list of the most reported combination of reporting IP, source IP, destination IP, and destination TCP/UDP port over the time period.



5. Change the time to 10 hours, and then run the search query again to view the results over the increased time period.



To change the time period, in the **ANALYTICS** tab, click the search field to open the **Filters** editor.

You will notice that, even after executing the query for 10 hours, the display fields for group by remain the same.

6. You can use **Clear All** to reset both **Filters** and **Group By and Display Fields** to the default settings.
7. Log out of the FortiSIEM GUI.

Exercise 2: Aggregating Data

In this exercise, you will learn how to add an aggregation condition to your search criteria.

Create a Search Filter Criteria

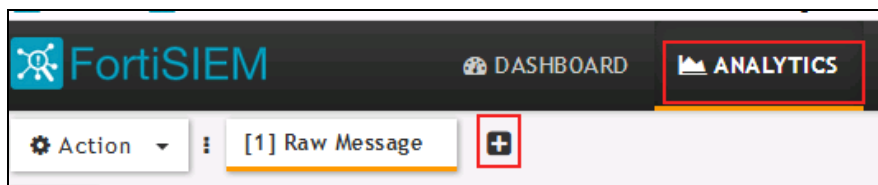
You will create a search filter on FortiSIEM.

To set search filter criteria

1. Log in to the FortiSIEM GUI with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Domain	LOCAL

2. Click the **ANALYTICS** tab, and then click the plus icon **+** to add a new tab for a search.



3. Click the search field to edit the condition.
4. In the **Filters** window, select **Event Attribute**, and then configure the following settings to create a new query:

Field	Value
Attribute	Reporting IP
Operator	=

5. In the **Value** field, click **Select from CMDB**.
6. Click **Devices > Server > Windows**.
7. In the **Items** field, select the **WIN2K8** device.
8. Click **>** to add the device to **Selections**.
9. Click **OK**.
10. In the **Next** column beside the existing condition, select **AND**.
11. In the **Row** column beside the existing condition, click the **+** icon to add another row.
12. Configure the following settings for the second condition:

Field	Value
Attribute	Event Type
Operator	CONTAIN
Value	PH_DEV_MON_SYS

- In the **Time Range** section, select **Relative**, in the **Last** field, type 10, and then select **Hours** in the drop-down list.
- Click **Apply & Run**.

Configure Display Fields for Aggregation

You will configure the display fields for data aggregation.

To configure display fields for aggregation

- Continuing on the FortiSIEM GUI, select the **PH_DEV_MON_SYS_DISK_UTIL** event.



Make sure **Wrap Raw Event** and **Show Event Type** are enabled.

- In the **Event Type** column, click the down arrow, select **Add to Filter**, and then select = (equal sign) as an operator.

☒ Show Event Type

☒ Wrap Raw Events

Event Receive Time	Reporting IP	Event Type	Event Name
Oct 01 2021, 09:24:18 AM	192.168.0.40	PH_DEV_MON_SYS_DISK_UTIL	▼ Disk Utilization stats Add to Filter + Add to Tab... Quick Info
Oct 01 2021, 09:24:18 AM	192.168.0.40	PH_DEV_MON_SYS_UPTIME	

- Run the search again for the last 10 hours.
You should now have your search results filtered to show only disk utilization events.
- Open the **Event Details** dialog box for one of the events, and then add the following columns to the display:
 - Disk Name**
 - Disk Capacity Util**
 - Free Disk MB**
 - Total Disk MB**

Event Details

```
[PH_DEV_MON_SYS_DISK_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,
[lineNumber]=8745,[diskName]=C:\,[hostName]=WIN2K8,[hostIpAddr]=192.168.0.40,
[diskUtil]=36.495039,[totalDiskMB]=40958,[usedDiskMB]=14948,[freeDiskMB]=26010,
[pollIntv]=176,[phLogDetail]=
```

Lines: 30

Display	Filter	Item	Value
☐	☐	Collector ID	1
☐	☐	Count	1
☒	☐	Disk Capacity Util	36.50
☒	☐	Disk Name	C:\
☐	☐	Event ID	3867747654997134315
☐	☐	Event Name	Disk Utilization stats for a device
☐	☐	Event Parse Status	1

- Click **OK** to close the **Event Details** dialog box.
- Click the **Group By and Display Fields** drop-down list arrow icon.
You will notice that the display attributes you have added from **Event Details** are present.

Group By and Display Fields

Attribute	Order	Display As	Row	Move
Event Receive Time	DESC ▼		+ -	↑ ↓
Reporting IP	▼		+ -	↑ ↓
Event Type	▼		+ -	↑ ↓
Raw Event Log	▼		+ -	↑ ↓
Disk Name	▼		+ -	↑ ↓
Disk Capacity Util	▼		+ -	↑ ↓
Total Disk MB	▼		+ -	↑ ↓
Free Disk MB	▼		+ -	↑ ↓

- Click the minus icon - in the **Row** column to remove the following rows from the **Display Fields** window:
 - Event Receive Time**
 - Event Type**

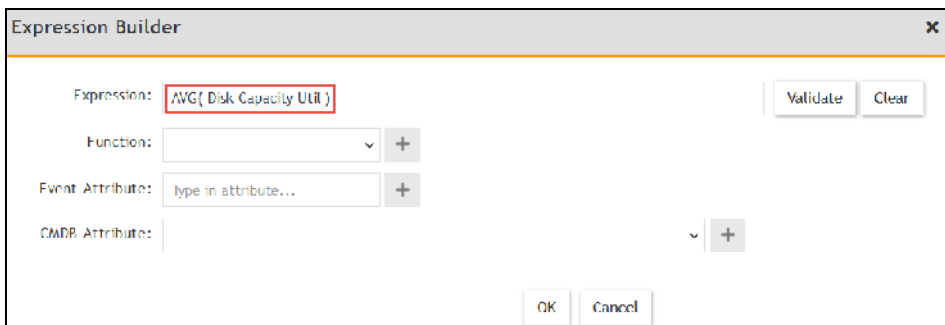
- **Raw Event Log**
8. Run the search again.
Now, you can see disk-related attributes with the reporting IP.

To aggregate events

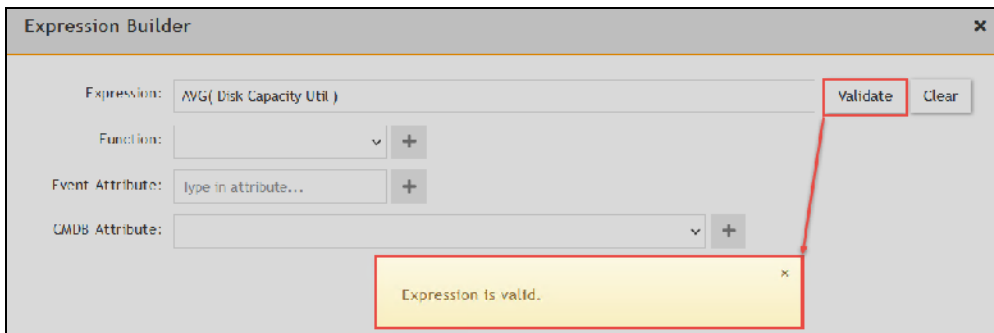
1. Continuing on the FortiSIEM GUI, click the **Group By and Display Fields** drop-down list, and then edit the fields using one of the following methods:
 - Edit the **Disk Capacity Util** attribute by removing text in an existing row, and then clicking **Expression Builder**.
 - Remove the **Disk Capacity Util** row, add a new row at the bottom, and then click **Expression Builder** in the **Attribute** column.

A dialog box appears to build an expression.

2. In the **Function** drop-down list, select **AVG**, and then click the plus icon +.
3. In the **Event Attribute** field, type **Disk Capacity Util**, and then click the plus icon +.



4. Once the expression is added, in the **Expression** field, click **Validate**.
A pop-up message appears.



5. Close the pop-up message, and then click **OK** to close the **Expression Builder** dialog box.
6. Continuing on **Group By and Display Fields**, edit the fields using one of the following methods:
 - Edit the **Free Disk MB** attribute by removing the existing text entry, and then adding the **LAST(Free Disk MB)** expression.
 - Remove the row for the **Free Disk MB** attribute, add a new row, and then add a **LAST(Free Disk MB)** expression using **Expression Builder**.

Indicator Chart

Group By and Display Fields Load Save Clear All

Attribute	Order	Display As	Row	Move
Reporting IP	▼		+	-
Disk Name	▼		+	-
AVG(Disk Capacity Util)	▼		+	-
Total Disk MB	▼		+	-
LAST(Free Disk MB)	▼		+	-

Display Conditions

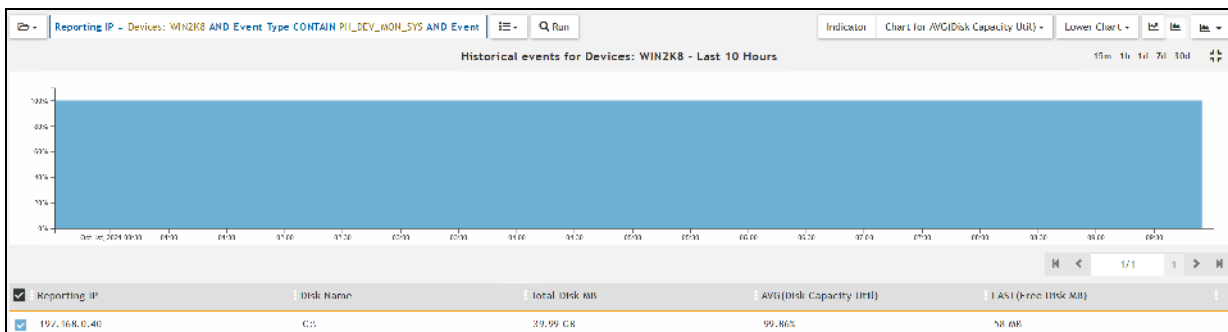
Paren	Attribute	Operator	Value	Paren	Next	Row
+	▼	▼		+	AND	+

Apply & Run Apply Cancel

7. Click **Apply**.

8. Run the search over the last 10 hours.

Results will be aggregated in one line for 10 hours (values shown below may vary).



If you do not get any results for any search, run the search over a longer time period.

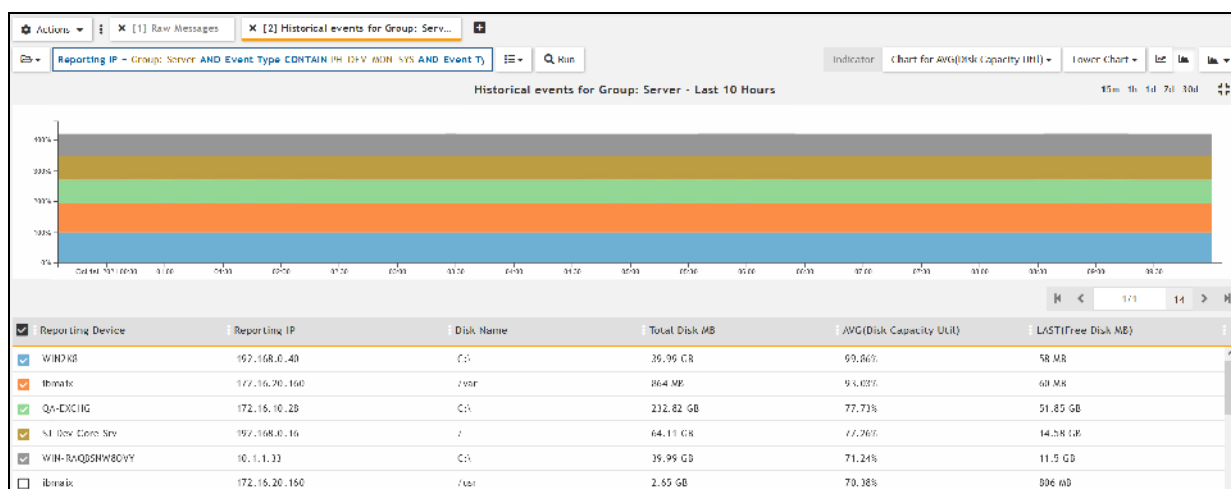
To aggregate disk utilization for all servers

- Continuing on the FortiSIEM GUI, edit the search condition again and remove the entry for **Reporting IP = Device: WIN2K8**.
- Add the following condition:

Field	Value
Attribute	Reporting IP
Operator	IN

3. In the **Value** field, click **Select from CMDB**, and then click **Devices > Server**.
4. Click **>>** to add the folder to **Selections**.
5. Click **OK**.
6. In the **Time Range** section, select **Relative**, in the **Last** field, type **10**, and then select **Hours** in the drop-down list.
7. Click **Apply**.
8. Click the **Group By and Display Fields** icon, and then add a row for **Reporting Device** by clicking the plus icon in the **Row** column of the **Reporting IP**.
9. Click the up arrow icon in the **Move** column of the **Reporting Device** row to move it to the top.
10. Click **Apply & Run**.

The aggregated average disk utilization of all servers in a 10-hour time period displays.



The results may vary because of log simulation.

11. Log out of the FortiSIEM GUI.

Exercise 3: Expert Challenge

In this exercise, you will be presented with various scenarios, and you must determine the search criteria that will produce the correct outcome for each scenario.

Conduct a Historical Search

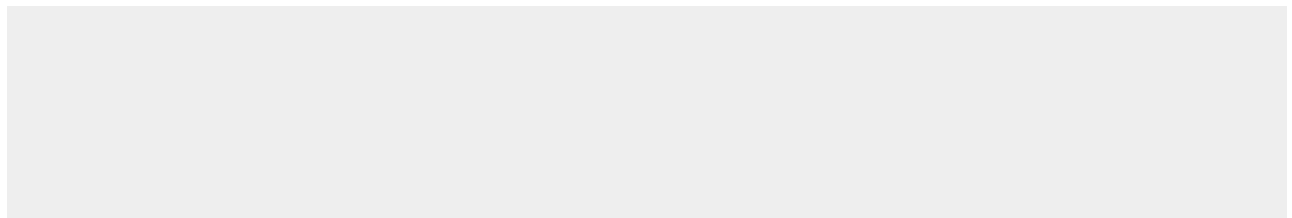
You will create search queries based on the scenarios presented in this section to perform searches on FortiSIEM.

To conduct scenario-based historical searches

1. Log in to the FortiSIEM GUI with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Domain	LOCAL

2. Click the **ANALYTICS** tab, and then click the search field to edit the condition.
3. For a historic event search, in the **Time** section, select the **Relative** or **Absolute** option.
4. Select the appropriate **Display Fields**, and then apply the **Group By** and **Aggregation** expressions to achieve the correct results for the scenarios in this challenge.
5. Close any search tabs that are open, and then attempt the following searches:
 - a. The customer wants to know which firewall device reported the most events over the last 30 minutes.
See "[Appendix: Answer Sheet](#)" on page 243 for the answer.



- b. The customer wants to know which is the most common destination country of firewall events that are not on destination TCP/UDP Port 21, 80, 443, or 53 over the last hour. Also, remove the NULL entry in your results.

See "[Appendix: Answer Sheet](#)" on page 243 for the answer.

- c. The customer wants to know what is the most common source country for denied traffic events reported by a firewall device in the last 30 minutes.

See "[Appendix: Answer Sheet](#)" on page 243 for the answer.

- d. The customer wants to see a list of all the CPU and memory usage for each process on device 192.168.0.16 over the last 30 minutes. Produce a report showing the **Reporting IP**, **Application Name**, **Software Name**, **CPU Util**, and **Memory Util**, and hide all other display columns.



Use the **PH_DEV_MON_PROC_RESOURCE_UTIL** event type.

What events does this report produce? See "[Appendix: Answer Sheet](#)" on page 243 for the answer.

- e. After reviewing the last report, the customer said the report contains the same process over and over again in the results. The customer would like to see a report containing each application name and software name with an average **CPU Util** value and a maximum **Memory Util** value.



Use the **Group By and Display Fields** column expression builder.

- f. Run the report over the last six hours.
6. Log out of the FortiSIEM GUI.

Lab 7: Rules

In this lab, you will configure rules to generate incidents.

Objectives

- Examine a simple rule
- Examine a performance and availability rule
- Create a simple rule to alert you to a specific event
- Add watch lists
- Import rules

Time to Complete

Estimated: 75 minutes

Exercise 1: Exploring a Simple Rule

In this exercise, you will examine the structure of a simple rule.

Examine a Rule

You will examine the out-of-the-box **Account Locked: Domain** rule.

To view a rule

1. Log in to the FortiSIEM GUI with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Domain	LOCAL

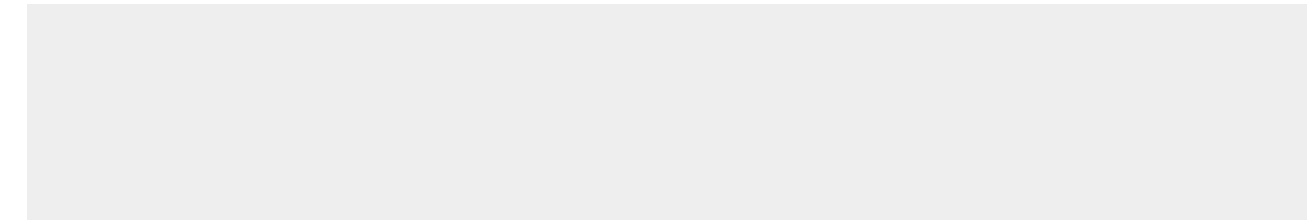
2. Click the **RESOURCES** tab.
3. In the left pane, click **Rules**.
4. In the main window, select **Account Locked: Domain**, and then click **Selected Rule** in the **Edit** drop-down menu.

Resources > Rules

New Edit Delete Clone Test Search...

Active	Name	Description	Tactics
☒	10 - HIGH (s) Account Locked: Domain	Detects account lockout caused by excessive logon failures	Credential Access
☒	10 - HIGH (s) Account Locked: FortiSIEM	Detects system (FortiSIEM) account lockout caused by excessive logon failures	Credential Access

5. Click **Step 2: Define Condition**.
During what time period is the rule evaluating the pattern? See "Appendix: Answer Sheet" on page 244 for the answer.



6. Under the **Subpattern** column, beside **DomainAcctLockout**, click the pencil icon.

Account Locked: Domain - Edit Details

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

Condition: If this Pattern occurs within any 600 second time window

Paren	Subpattern	Paren	Next	Row
(	DomainAcctLockout	)		1

Save Cancel

7. Review the rule subpattern.

The subpattern is looking for a match of one or more events under the **Domain Account Locked** event type in the CMDB, and only those reported by devices that are categorized as a domain controller.

Make a note of the attributes in the **Group By** section. See ["Appendix: Answer Sheet" on page 244](#) for the answer.

8. Click **Cancel** to exit the rule pattern.

9. In the **Step 3: Define Action** section, make a note of the severity of the rule, the category, and the subcategory. See ["Appendix: Answer Sheet" on page 244](#) for the answer.

10. Beside **Action**, click the pencil icon.

Account Locked: Domain - Edit Details

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

Severity: 10 - HIGH Update Status on Summary Dashboard: ☐

Category: Security Notifications: 24 Hours

Subcategory: Credential Access Impacts: Application

Technique: [11110.001] Brute Force: Password Guessing

Tactics: Credential Access

Action: Detined Watch List: Detined

Exception: Untetined Clear: Untetined

log: ☐

Save Cancel

To review received events

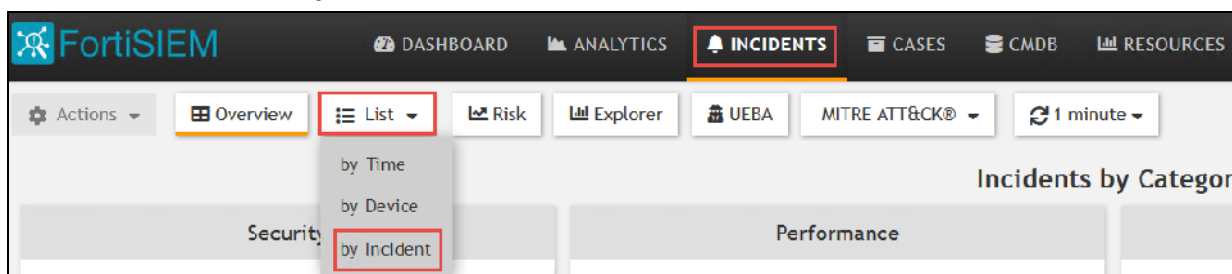
1. Return to the FortiSIEM GUI, and then after the event is received, click **Stop**.
2. Review the **Reporting IP** of the event and the **User** who locked their account.

Examine an Incident

You will examine an incident the **Account Locked: Domain** rule generated.

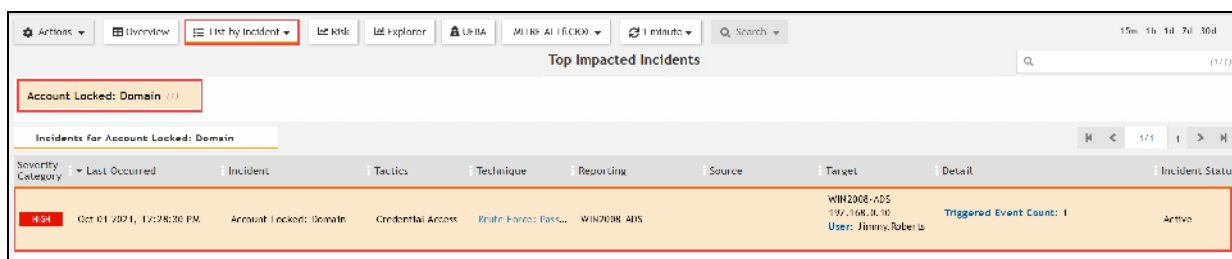
To examine an incident the **Account Locked: Domain** rule generated

1. Continuing on the FortiSIEM GUI, click the **INCIDENTS** tab.
2. Click **List**, and then select **by Incident** to view the incident.



If you do not get any results, change the time to a longer time period.

3. Select the **Account Locked: Domain** incident.



4. Click and hover over the **Target** column for this incident.
Note that it reports an IP address and user that matches what you saw in the real-time search.



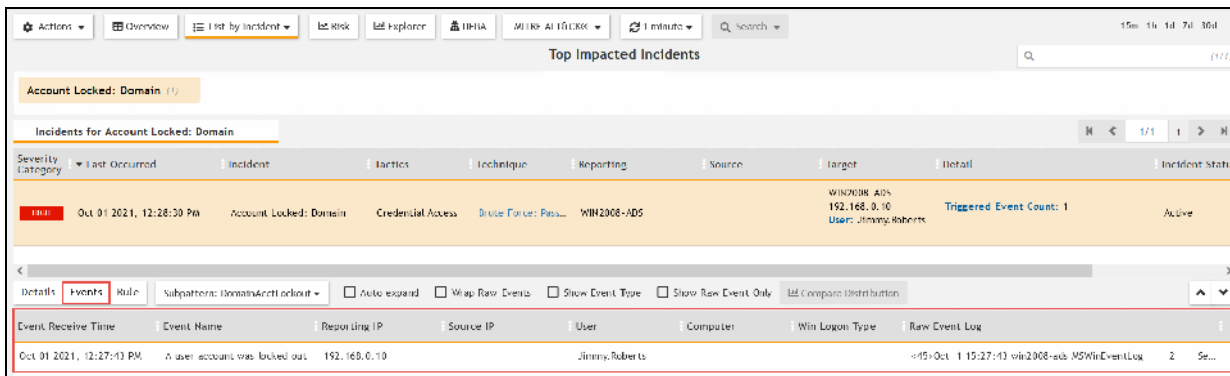
5. Select the incident, and then in the lower pane, review the incident details.



If you select an incident and the lower pane does not appear, you must click the up arrow icon  to expand the lower pane manually.

You can use **Auto expand** in the lower pane, so you don't have to keep manually expanding the lower pane to view incidents.

6. Click the **Events** tab.



The screenshot shows the FortiSIEM GUI interface. At the top, there's a navigation bar with tabs like 'Overview', 'Incident', 'Risk', 'Explorer', 'IRPA', and 'Alerts'. The 'Incident' tab is selected. Below the navigation bar, there's a section titled 'Top Impacted Incidents'. Under this, there's a sub-section 'Incidents for Account Locked: Domain'. A table lists incidents with columns for Severity, Category, Last Occurred, Incident, Tactics, Technique, Reporting, Source, Target, Detail, and Incident Status. One incident is highlighted: 'Account Locked: Domain' on 'Oct 01 2021, 12:28:30 PM'. Below the table, there's a 'Details' section with a 'Events' tab selected. This tab shows a table of events with columns: Event Receive Time, Event Name, Reporting IP, Source IP, User, Computer, Win Logon Type, and Raw Event Log. The first event is: 'Oct 01 2021, 12:27:43 PM', 'A user account was locked out', '192.168.0.10', 'Jimmy.Roberts', 'WIN2008-AD5', '192.168.0.10', 'User: Jimmy.Roberts', 'Triggered Event Count: 1', 'Active'.

Do the details match what you recorded in step 6 of the *To view a rule* procedure in this exercise? See ["Appendix: Answer Sheet" on page 244](#) for the answer.

7. Before proceeding to the next exercise, close the extra browser tab.
8. Log out of the FortiSIEM GUI.

Exercise 2: Exploring a Performance Rule

In this exercise, you will explore an existing performance monitoring rule.

Examine a Performance Monitoring Rule

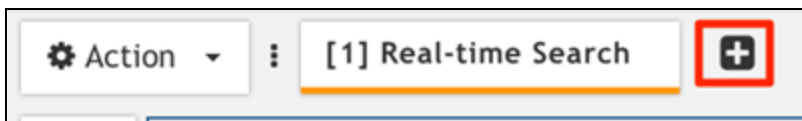
You will examine a performance monitoring rule on FortiSIEM.

To view a performance monitoring rule

1. Log in to the FortiSIEM GUI with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Domain	LOCAL

2. Click the **ANALYTICS** tab.
3. Close all search tabs (if any), and then click the **+** icon to open a new search.



4. Click the search field to edit the condition.
The **Filters** editor opens.
5. Build an **Event Attribute** search, and then configure the following conditions:

Field	Value
Attribute	Reporting IP
Operator	=
Value	192.168.0.40
Next	AND

6. In the **Row** column, click the **+** icon to add the following second condition:

Field	Value
Attribute	Event Type

Field	Value
Operator	CONTAIN
Value	SYS_DISK_UTIL

- In the **Time Range** section, select **Relative**, in the **Last** field, type 10, and then select **Hours** in the drop-down list.
- Click **Apply & Run**.

Filter

Load
Save
Clear All

☐ Event Keyword
☐ Event Attribute

Paren	Attribute	Operator	Value	Paren	Next	Row
+	Reporting IP	-	192.168.0.40	+	AND	+
+	Event Type	CONTAIN	SYS_DISK_UTIL	+	AND	+

☐ CMDB Attribute

Time Range

☐ Real-time
☒ Relative
Last
10
Hours

☐ Absolute

Trend Interval:
Auto

Apply & Run
Apply
Cancel



If you do not get any results for any search, run the search over a longer time period.



Because of the demo system, the results are not strictly correct. In a production system, this event would be collected every three minutes, for each disk. You will probably have more events that are related to the scripted data replay mechanism used.

- Examine the **Event Details** of the raw event log for one of the returned events.

The relevant attributes in this event are:

- Disk Capacity Util
- Disk Name
- Free Disk MB
- Host IP
- Host Name
- Total Disk MB
- Used Disk MB

- Close the **Event Details** dialog box.

To view performance threshold values for a device in the CMDB

1. Continuing on the FortiSIEM GUI, click the **CMDB** tab.
2. In the left pane, click **Devices > Server > Windows**.
3. In the main window, click **WIN2K8** (192.168.0.40), and then click **Edit**.
The **Edit Device** dialog box opens.
4. Click the **Device Properties** tab.
5. In the **Disk Space Util Critical Threshold** field, click **Edit**.

Edit Device

Summary Contacts Interfaces **Device Properties** Parsers Search...

*Note: Only Device Properties are editable.

User Defined

System Defined

ACI Health Score Critical Threshold:

ACI Health Score Warning Threshold:

Business Unit:

CIFS Latency msec Critical Threshold:

CIFS Latency msec Warning Threshold:

Disk Latency msec Critical Threshold: Undefined

Disk Latency msec Warning Threshold: Undefined

Disk Space Util Critical Threshold: Undefined

Disk Space Util Warning Threshold: Undefined

The **Disk Space Util Critical Threshold** dialog box opens.

6. Make a note of the value in the **Default** field and the disk name listed.
See ["Appendix: Answer Sheet"](#) on page 245 for the answer.

Field	Value
Disk Space Util Critical Threshold	
Disk Name	

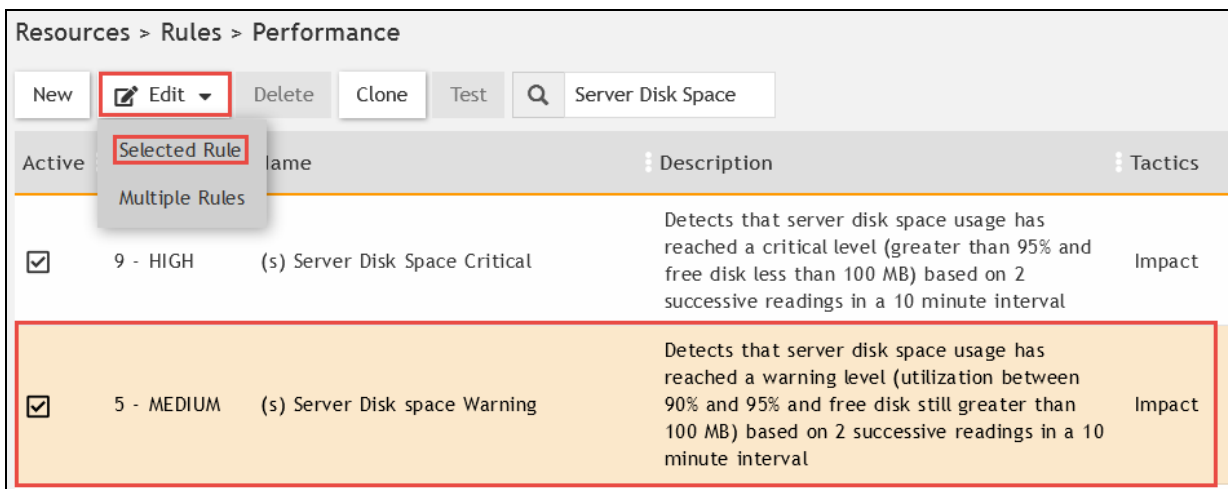
7. Click **Cancel**, and then find the threshold for **Free Disk (MB) Critical Threshold**.
See ["Appendix: Answer Sheet"](#) on page 245 for the answer.

Field	Value
Free Disk (MB) Critical Threshold	
Disk Name	

8. Click **Cancel**.
9. Click **Cancel** again.

To view a performance monitoring rule

1. Continuing on the FortiSIEM GUI, click the **RESOURCES** tab.
2. In the left pane, click **Rules > Performance**.
3. Search for rules with the name **Server Disk Space** (use the search field to filter).
4. Select the **Server Disk space Warning** rule, and then click **Selected Rule** in the **Edit** drop-down menu.



The **Server Disk space Warning - Edit Details** dialog box opens.

5. Click **Step 3: Define Action**.

Make a note of the severity of the rule, the category, and the subcategory. See "[Appendix: Answer Sheet](#)" on [page 245](#) for the answer.

6. Click **Step 2: Define Condition**.
7. In the **Condition** section, note the rule time window and the **ServDiskWarn** subpattern.
8. Beside **ServDiskWarn**, click the pencil icon.
The **Edit SubPattern** window opens.

Edit SubPattern

Name:

Filters:

Paren	Attribute	Operator	Value	Paren	Next	Row
+	Event Type	=	PH_DEV_MON_SYS_DISK_UTIL	+	AND	+
+	Host IP	IN	Devices: Server	+	AND	+
+	Disk Name	NOT IN	/boot	+	AND	+

Aggregate:

Paren	Attribute	Operator	Value	Paren	Next	Row
+	AVG(Disk Capacity Util)	>=	DeviceToCMDBAttr(Host IP : Disk	+	AND	+
+	AVG(Disk Capacity Util)	<=	DeviceToCMDBAttr(Host IP : Disk	+	OR	+
+	AVG(Disk Capacity Util)	>=	DeviceToCMDBAttr(Host IP : Disk	+	AND	+
+	AVG(Free Disk MB)	>	DeviceToCMDBAttr(Host IP : Disk	+	AND	+
+	COUNT(Matched Events)	>=	2	+	AND	+

Group By:

Attribute	Row	Move

Save

Save as Report

Run as Query

Cancel

In the **Filters** section, the subpattern is looking for any events that match the exact event type **PH_DEV_MON_SYS_DISK_UTIL** and only from devices classified as a **Server** in the CMDB, while excluding any events where the disk name is **/boot**.

In the **Aggregate Condition** section, the subpattern is looking for at least two events (two samples) where, during the rule evaluation time window, the following is true for each disk:

- The average **Disk Capacity Util** value is more than or equal to the **Disk Space Util Warning Threshold** and the average **Disk Capacity Util** value is less than or equal to the **Disk Space Util Critical Threshold**, or
- The average **Disk Capacity Util** value is more than or equal to the **Disk Space Util Critical Threshold** and the average **Free Disk MB** value is more than the **Free Disk MB Critical Threshold**.

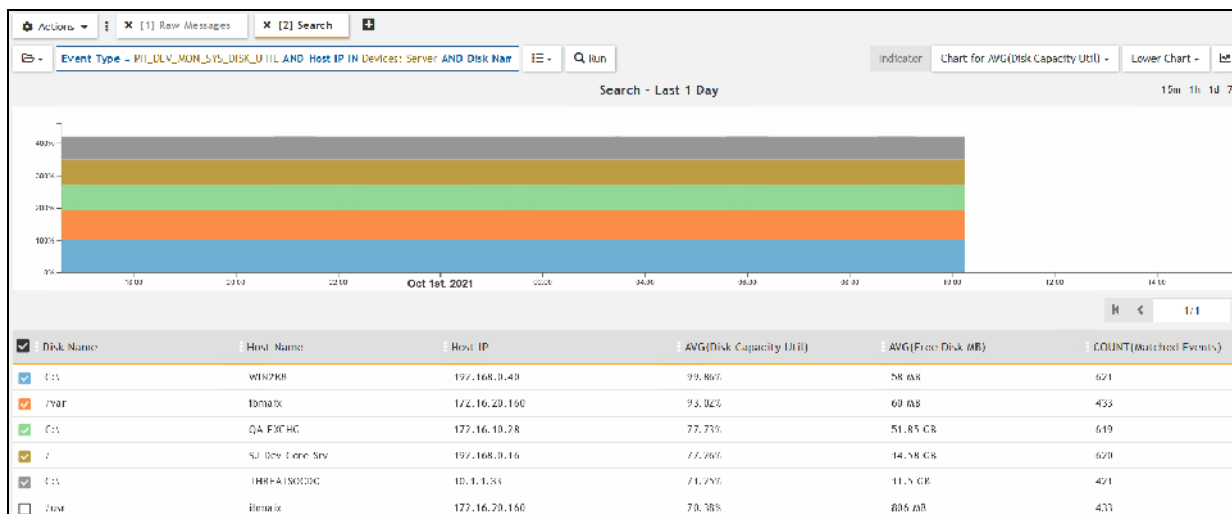
Note that the attributes in the **Edit SubPattern** dialog box in the **Group By** section are **Host IP**, **Host Name**, and **Disk Name**.

- At the bottom of the dialog box, click **Run as Query**.

The **Edit SubPattern > Run As Query** dialog box opens.

- On the **Time Range** tab, select **Relative**, in the **Last** field, type 1, select **Day** in the drop-down list, and then click **Run**.

A new browser tab opens, which displays the **ANALYTICS** tab with the results for the query.



Are there any results where the **AVG(Disk Capacity Util)** is greater than 95% and the **AVG (Free Disk MB)** is less than 100? See ["Appendix: Answer Sheet"](#) on page 245 for the answer.

To modify the performance search query for one device

1. In the new browser tab, under **ANALYTICS**, click the search filter.
2. In the **Next** drop-down list of the last attribute in the list, select **AND**.
3. Add an extra row, and then configure the following condition:

Field	Value
Attribute	Host IP
Operator	=
Value	192.168.0.40

4. In the **Time** section, select **Relative**, in the **Last** field, type 1, and then select **Day** in the drop-down list.

Filter Load Save Clear All

☐ Event Keyword

☒ Event Attribute

Paran	Attribute	Operator	Value	Paran	Next	Row
+	Event Type	-	PIL_DEV_MON_SYS_DISK_UTIL	+	-	AND
+	Host IP	IN	Devices: Server	+	-	AND
+	Disk Name	NOT IN	/boot	+	-	AND
+	Host IP	=	192.168.0.40	+	-	AND

☐ CMDB Attribute

Time Range

☐ Real-time

☒ Relative Last 1 Day

☐ Absolute

Trend Interval: Auto

Apply & Run Apply Cancel

5. Click **Apply & Run**.

You should get a single result for the WIN2K8 machine only, and it should look similar to the following result:



6. Close the old browser tab, and then keep the new tab open to complete the rest of the exercise.

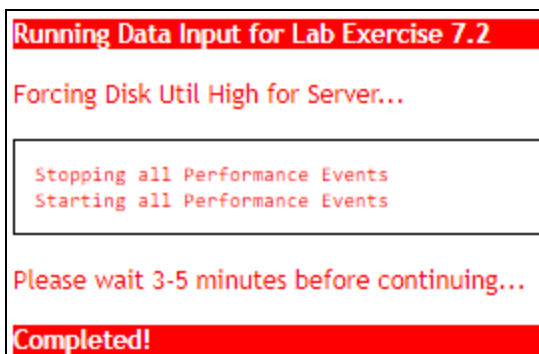
Generate Scripted Performance Events

You will generate some simulated performance events.

To generate performance events

- On the Linux-Client VM, open a browser, and then go to the NSE Institute website.
- Navigate to **LABS SET 2**, and then under **Lab 7—Rules**, select **Exercise 7.2—Trigger Server Critical Disk Rule**.

The output should resemble the following image:



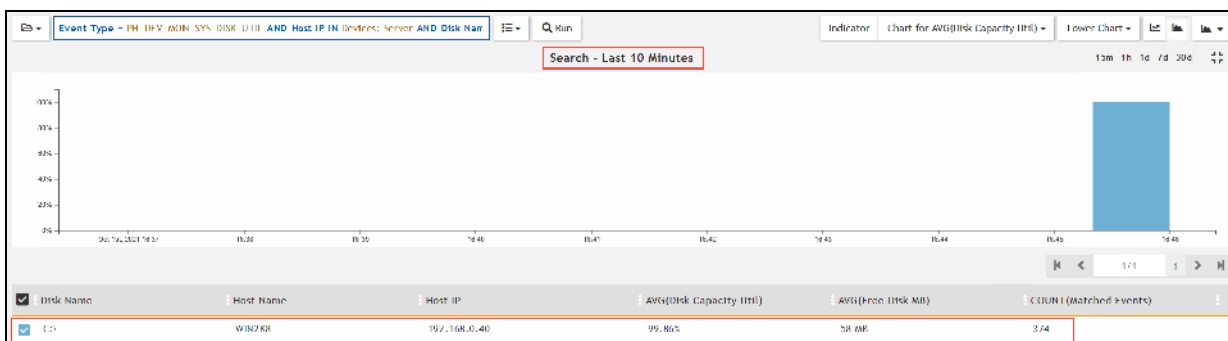
3. Wait approximately three to five minutes before proceeding to the next section.
4. Close the Linux-Client VM browser tab.

Examine Performance Events and Incidents

You will review the performance events and incidents that are generated on FortiSIEM.

To examine the performance events

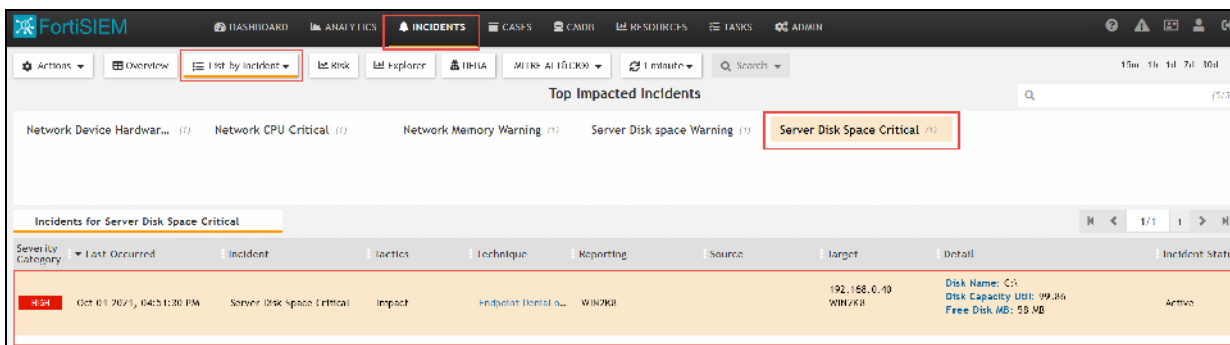
1. Return to the FortiSIEM GUI, and then on the **ANALYTICS** tab, click **Run** to search again for the last 10 minutes.



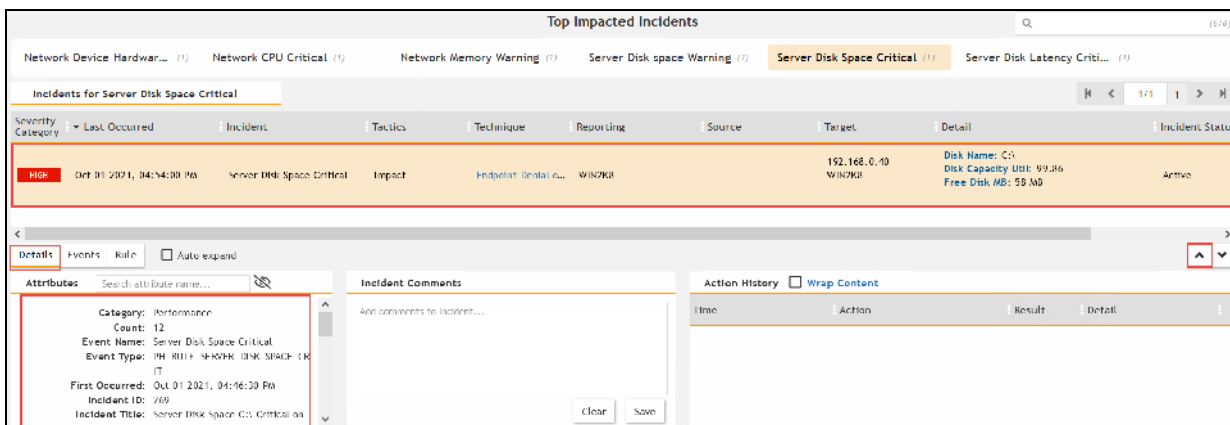
You should now see the **AVG(Disk Capacity Util)** is greater than 95 % and the **AVG(Free Disk MB)** is less than 100 MB events, which should trigger an incident.

To view incidents for the performance rule

1. Continuing on the FortiSIEM GUI, click the **INCIDENTS** tab.
2. Click **List**, and then select **by Incident** to view the incident.
3. Select **Server Disk Space Critical**.



4. Review the details, such as the incident target, incident details, and triggered events.



If you select an incident and the lower pane does not appear, you must click the up arrow icon (⬆) to expand the lower pane manually.

You can use **Auto expand** in the lower pane, so you don't have to keep manually expanding the lower pane to view incidents.

5. Log out of the FortiSIEM GUI.

Exercise 3: Creating a Rule

In this exercise, you will create a simple rule.

In this scenario, a company has strict policies specifying that the administration of a selected FortiGate firewall can be performed from approved workstations only. They would like to detect if administrators are connecting to the FortiGate device from non-approved workstations.

The approved workstations have the following IP addresses:

- 10.1.50.1
- 10.1.50.2
- 10.1.50.3
- 10.1.50.4
- 10.1.50.5

Configure Search Filter Criteria

You will create a search filter on FortiSIEM.

To create the search filter criteria

1. Log in to the FortiSIEM GUI with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Domain	LOCAL

2. Click the **ANALYTICS** tab.
3. Click the **+** icon to open a new search tab, and then close any existing search tabs.
4. Click the search field to edit the condition.
The **Filter** editor opens.
5. Build an **Event Attribute** search, and then configure the following conditions:

Field	Value
Attribute	Reporting IP
Operator	=
Value	192.168.3.1

6. In the **Row** field, click **+** to add a second condition with the following values:

Field	Value
Attribute	Event Type
Operator	CONTAIN
Value	login-success

7. Select **Time** as **Real Time**.
8. Click **Apply & Run**.

Generate Scripted Events

You will generate some simulated performance events.

To generate events

1. On the Linux-Client VM, open a browser, and then go to the NSE Institute website.
2. Navigate to **LABS SET 2**, and then under **Lab 7—Rules**, select **Exercise 7.3—FortiGate Admin Login Events – (Part A)**.

Wait approximately one to two minutes for the output. The output should resemble the following example:

```
Running Data Input for Lab Exercise 7.3A
Now Sending Events for Exercise 7.3 Part A
sending events from file /var/www/html/NSE_Institute/labs/LAB7/C1/events_lab7_ex3_1.dat
3 messages sent
Completed!
```

3. Wait for the **Completed** message before continuing.

Examine the Generated Events

You will review the events that are generated on FortiSIEM.

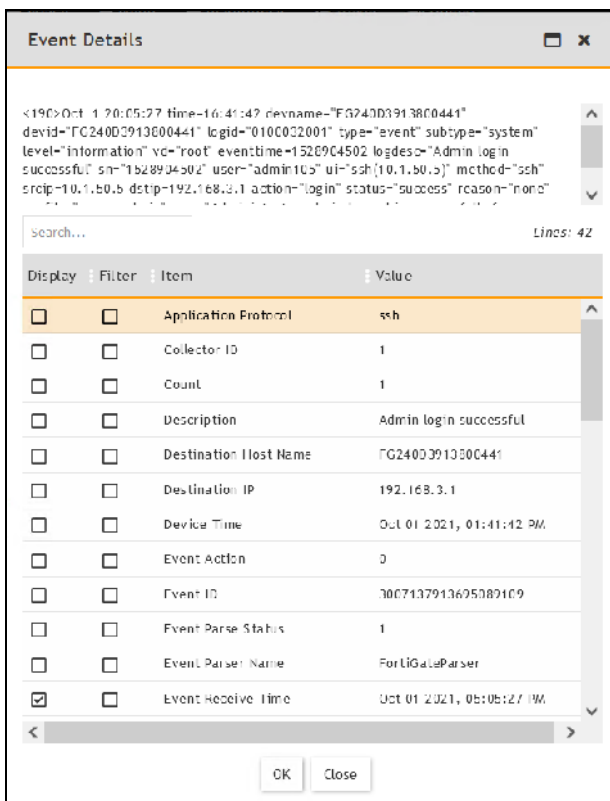
To review generated events

1. Return to the FortiSIEM GUI, and then after all the events are sent, click **Pause**.
You should see only **FortiGate-event-login-success**.



Make sure **Wrap Raw Event** and **Show Event Type** are selected.

2. Examine the **Event Details** of the raw event log for one of the returned events.



Note that these FortiGate admin login events contain the **Application Protocol** (SSH or HTTP), **Source IP**, and **User** who successfully authenticated.

3. After you review the details, close the **Event Details** dialog box.

To configure display fields for analytics

1. Continuing on the FortiSIEM GUI, click the **Group By and Display Fields** icon.
2. Click **Clear All**.
3. Add two new rows for **Source IP** and **User**.
4. Add a third row, and then select * **COUNT(Matched Events)**.

- Click **Apply** to close the dialog box.
- Click the search field.
- In **Filters**, change the search time to be **Relative** over a one hour period.
- Click **Apply & Run**.

Note that all the results so far are for IP addresses that were in the allowed administrator workstation IPs group.

- 9.** Edit the search filters, and then add an extra row for the following condition:

Your search filter should now look like the following example:

Filter [Load] [Save] [Clear All]

☐ Event Keyword

☒ Event Attribute

Paren	Attribute	Operator	Value	Paren	Next	Row
+	Reporting IP	=	192.168.3.1	+	AND	+
+	Event Type	CONTAIN	login-success	+	AND	+
+	Source IP	NOT IN	10.1.50.3, 10.1.50.4, 10.1.50.5	+	AND	+

☐ CMDB Attribute

Time Range

☐ Real-time ☒ Relative Last 1 Hour

- Click **Apply & Run**.

You get no results this time and the message **No report results found** appears.

Create a Rule

You will create a rule using the search filter conditions.

To create a rule

- Continuing on the FortiSIEM GUI, click **Actions**, and then in the drop-down list, select **Create Rule**.

Actions [1] Historical events for 192.168.3.1

- Email Result
- Export Result
- Copy to New Tab
- Save as Report
- Create Rule**

192.168.3.1 AND Event Type CONTAIN login-success AND Source IP NOT IN

- In the **Rule Name** field, type **FortiGate Admin Logon from Non Admin Machine**, and then type an optional **Description**.

Create Rule

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

Rule Name: FortiGate Admin Logon from Non Admin Machine

Description: Admin logons to FortiGate have been detected from non approved administration machines.

Event Type: FortiGate_Admin_Logon_from_Non_Admin_Machine

Remediation Note:

OK Cancel

- Click **Step 2: Define Condition**, and then leave the time window set to **300** seconds.
- Beside the **SubPattern** field for **Filter_1**, click the pencil icon.
- In the **Edit SubPattern** dialog box, note the addition of an **Aggregate** section, which displays **COUNT(Matched Events) >= 1**.
- Click **Cancel** when you are done.
- Click **Step 3: Define Action**.
- For **Category**, select **Security**, and then for **Subcategory**, select **Authentication**.
- Beside **Action: Defined**, click the pencil icon.

Generate Incident for: FortiGate Admin Logon from Non Admin Machine

Incident Attributes:	Event Attribute	Subpattern	Filter Attribute	Row
Source IP	=	Filter_1	Source IP	+
User	=	Filter_1	User	+

Insert Attribute: +

Incident Title:

Triggered Attributes: Available: Search... 1/31

Selected:

- Event Receive Time
- Event Type
- Reporting IP
- Raw Event Log
- Source IP
- User

By default, the rule has the **Group By** fields as **Incident Attributes**.

10. Click **Cancel**.
11. Click **OK**.
12. Click the **RESOURCES** tab.
13. In the left pane, select **Rules**, and then select **Ungrouped**.
14. Select the **FortiGate Admin Logon from Non Admin Machine** rule.
15. In the **Active** column, select the checkbox.
16. In the pop-up window, click **Continue**.

Generate Scripted Events

You will generate some simulated events to trigger the rule.

To generate events for a rule

1. Return to the Linux-Client VM, on the browser connected to the NSE Institute website, navigate to **LABS SET 2**, and then under **Lab 7—Rules**, select **Exercise 7.3—FortiGate Admin Login Events—(Part B)**.

The output should resemble the following example:

Running Data Input for Lab Exercise 7.3B
<pre>sending events from file /var/www/html/NSE_Institute/labs/LAB7/C2/events_lab7_ex3_2.dat 1 messages sent</pre>
Completed!

2. Close the Linux-Client VM.

Examine the Triggered Incident

You will examine the triggered incident on FortiSIEM.

To review an incident triggered by a rule

1. Return to the FortiSIEM GUI, wait for 30 seconds, and then click the **INCIDENTS** tab.
2. Click **List**, and then select **by Incident** to view the incident.
3. Select the **FortiGate Admin Logon from Non Admin Machine** incident.

Severity Category	Last Occurred	Incident	Tactics	Technique	Reporting	Source	Target	Detail	Incident Status	Resolution
HIGH	Oct 01 2021, 06:14:30 PM	FortiGate Admin Logon from Non Admin Machine			FG240D3913800441	10.1.60.5	User: admin101		Active	Open
HIGH	Oct 01 2021, 06:14:30 PM	FortiGate Admin Logon from Non Admin Machine			FG240D3913800441	10.1.60.9	User: admin101		Active	Open
HIGH	Oct 01 2021, 06:14:30 PM	FortiGate Admin Logon from Non Admin Machine			FG240D3913800441	10.1.60.15	User: admin101		Active	Open
HIGH	Oct 01 2021, 05:48:30 PM	FortiGate Admin Logon from Non Admin Machine			FG240D3913800441	10.1.60.7	User: admin101		Active	Open

The new rule has triggered a **FortiGate Admin Logon from Non Admin Machine** incident.

4. Review the incident source, incident target, and details, and then review the events that triggered the rule.
5. Log out of the FortiSIEM GUI.

Exercise 4: Enhancing a Rule With a Watch List

In this exercise, you will add a watch list to your rule.

Configure a Watch List

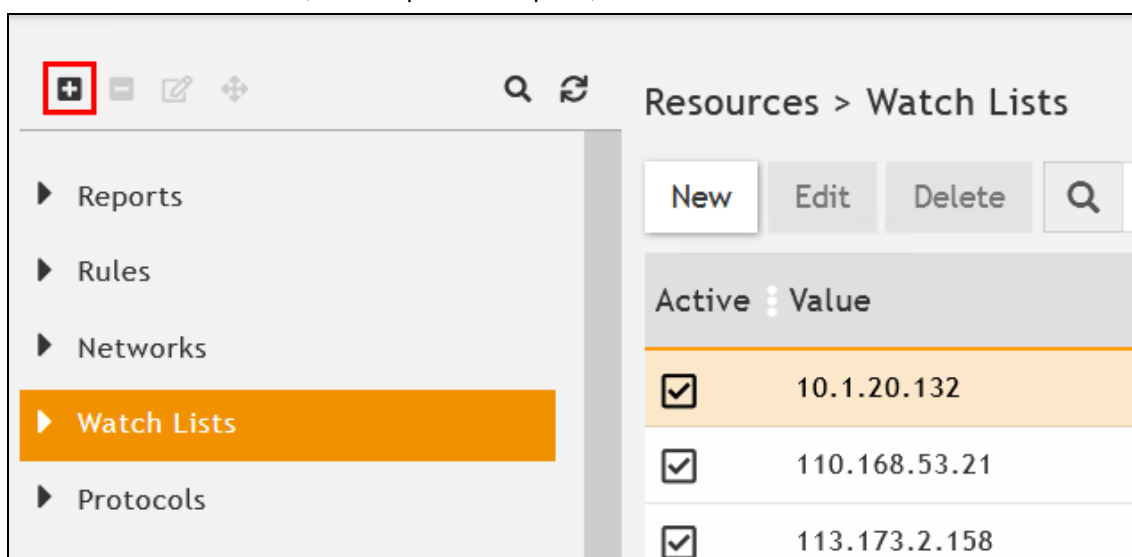
You will configure a watch list on the rule you created in the previous exercise.

To create a watch list

1. Log in to the FortiSIEM GUI with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Domain	LOCAL

2. Click the **RESOURCES** tab.
3. In the left pane, click **Watch Lists**.
4. Review the various watch lists that are provided out-of-the-box.
5. With **Watch Lists** selected, at the top of the left pane, click the add icon **+** to create a new list.



6. Configure the following settings, and then click **Save**:

Field	Value
Group	Suspect Admins
Description	Admin Users who are ignoring compliance rules on FortiGate Administration
Type	String
Expired in	1 Week(s)

Create New Watch List Group

Group:

Suspect Admins

Description:

Admin Users who are ignoring compliance rules on FortiGate Administration

Type:

String

Case Sensitive:

☐

Expired in:

1

Week(s)

Save

Cancel

Your new watch list appears at the bottom of the list.

To add a rule in the watch list

1. Continuing on the FortiSIEM GUI, click **Rules > Ungrouped**.
2. Find and select **FortiGate Admin Logon from Non Admin Machine**, and then click **Selected Rule** in the **Edit** drop-down menu.
3. Click **Step 3: Define Action**.
4. Beside **Watch Lists**, click the pencil icon.
The **Define Watch List** dialog box opens.
5. In the **Incident Attribute** drop-down list, select **User**.
6. Beside **Watch List**, in the **Available** list, select **Suspect Admins**, and then click the right arrow button to move the selection to the **Selected** list.
7. Click **Save**.

Define Watch List

Incident Attribute: User

Watch List: Available:

- Routing Issues
- Suspicious Activity
- Vulnerable Systems
- Wireless LAN Issues
- Ungrouped
- Suspect Admins

Selected:

- Suspect Admins

Save Cancel

8. Click **Save** again.

Generate Scripted Events

You will generate some simulated events.

To generate events for the watch list

1. On the Linux-Client VM, open a browser, and then go to the NSE Institute website.
2. Navigate to **LABS SET 2**, and then under **Lab 7—Rules**, select **Exercise 7.4—FortiGate Admin Login Events – Watch List**.

The output should resemble the following example:

Running Data Input for Lab Exercise 7.4

```
sending events from file /var/www/html/NSE_Institute/labs/LAB7/D/events_lab7_ex4.dat
3 messages sent
```

Completed!

3. Close the Linux-Client VM browser tab.

Examine the Generated Events

You will review the generated event for the watch list on FortiSIEM.

To review events for the watch list

1. Return to the FortiSIEM GUI, and then click the **INCIDENTS** tab.
2. Click **List**, and then select **by Incident** to view the incident.
3. Select **FortiGate Admin Logon from Non Admin Machine**.

Severity Category	Last Occurred	Incident	Tactics	Technique	Reporting	Source	Target	Detail	Incident Status	Resolution
MEDIUM	Oct 01 2021, 06:14:30 PM	FortiGate Admin Logon from Non Admin Machine		FG240D3913800441		10.1.60.5	User: admin101	Active	Open	
MEDIUM	Oct 01 2021, 06:14:30 PM	FortiGate Admin Logon from Non Admin Machine		FG240D3913800441		10.1.60.9	User: admin101	Active	Open	
MEDIUM	Oct 01 2021, 06:14:30 PM	FortiGate Admin Logon from Non Admin Machine		FG240D3913800441		10.1.60.15	User: admin103	Active	Open	
MEDIUM	Oct 01 2021, 05:48:30 PM	FortiGate Admin Logon from Non Admin Machine		FG240D3913800441		10.1.60.7	User: admin101	Active	Open	

Review the incident **Source**, **Target**, **Details**, and the events that triggered the rule.

Make a note of the **Target** column because it indicates the users.

4. Click the **RESOURCES** tab.
5. In the left pane, click **Watch Lists > Suspect Admins**.

Active	Value	Triggering Rules	Count	First Seen	Last Seen
☒	admin101	FortiGate Admin Logon from Non Admin Machine	2	Oct 01 2021, 06:14:30 PM	Oct 01 2021, 06:14:30 PM
☒	admin103	FortiGate Admin Logon from Non Admin Machine	1	Oct 01 2021, 06:14:30 PM	Oct 01 2021, 06:14:30 PM

Notice that **admin101** and **admin103**, which were the admin users referenced in the latest incident, are listed.

6. Log out of the FortiSIEM GUI.

Exercise 5: Importing a Rule

In this exercise, you will import a rule into FortiSIEM.

Import a Rule

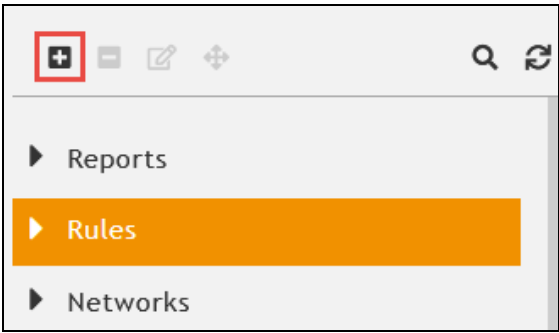
You will import a preconfigured rule into FortiSIEM.

To import a rule

1. Log in to the FortiSIEM GUI from the Linux-Client VM with the following credentials:

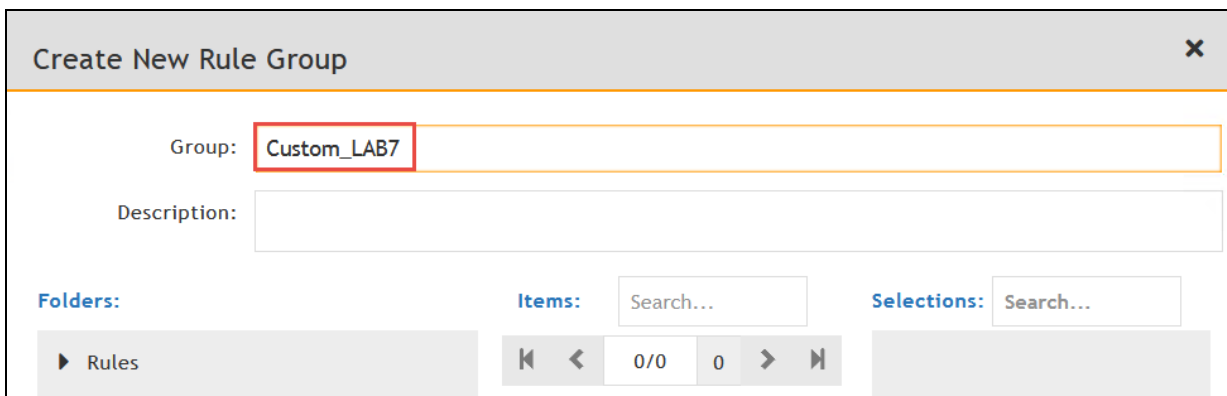
Field	Value
User ID	admin
Password	Fortinet1!
Domain	LOCAL

2. Click the **RESOURCES** tab.
3. In the left pane, click **Rules**.
4. With **Rules** selected, at the top of the left pane, click the add icon (+) to create a new rule group.



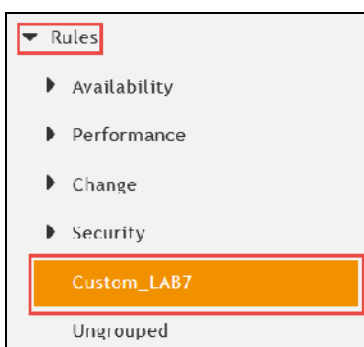
The **Create New Rule Group** dialog box opens.

5. In the **Group** field, type `Custom_LAB7`, and then click **Save**.

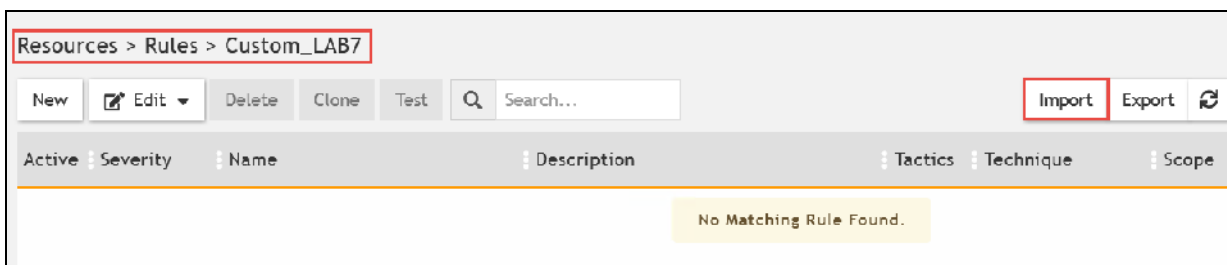


The 'Create New Rule Group' dialog box is shown. It has a title bar with a close button (X). The 'Group:' field contains 'Custom_LAB7'. The 'Description:' field is empty. Below these fields are three search bars labeled 'Folders:', 'Items:', and 'Selections:'. At the bottom, there is a 'Rules' folder icon and a pagination bar showing '0/0' and '0' items.

The left pane now shows a rule group under **Rules** called **Custom_LAB7**.



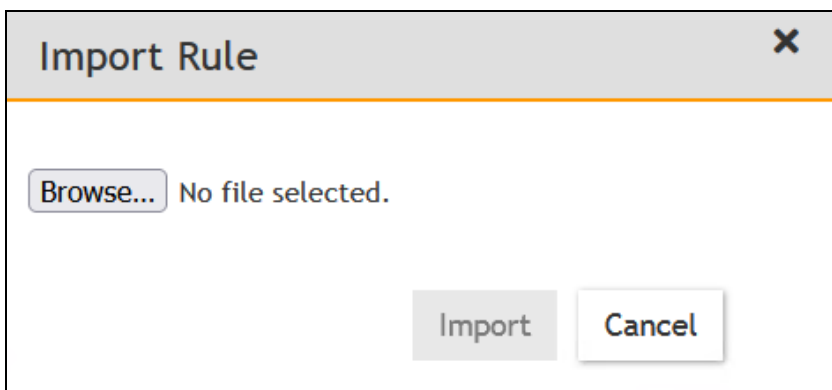
6. In the left pane, click **Custom_LAB7**.
7. In the right pane, click **Import**.



The 'Resources > Rules > Custom_LAB7' view is shown. It has a breadcrumb trail at the top. Below it are buttons for 'New', 'Edit', 'Delete', 'Clone', 'Test', and a search bar. The 'Import' button is highlighted with a red box. Below the buttons is a table with columns: 'Active', 'Severity', 'Name', 'Description', 'Tactics', 'Technique', and 'Scope'. The table is empty, and a message 'No Matching Rule Found.' is displayed at the bottom.

The **Import Rule** dialog box opens.

8. In the **Import Rule** dialog box, click **Browse**.



The 'Import Rule' dialog box is shown. It has a title bar with a close button (X). The 'Browse...' button is highlighted with a red box. Below it is a message 'No file selected.' At the bottom are 'Import' and 'Cancel' buttons.

9. Browse to **Desktop > Resources > LAB-7**, and then select the `newrule.xml` file.
10. Click **Import**.
11. Click **Rules > Custom_LAB7**.
The imported and activated rule appears in this list. You will use this rule in a later lab.
12. Log out of the FortiSIEM GUI.

Lab 8: Incidents and Notification Policies

In this lab, you will configure rules that create events for incidents.

Objectives

- Review the incidents page
- Group and tune incidents
- Use the built-in ticketing system
- Create custom email templates
- Create notification policies

Time to Complete

Estimated: 70 minutes

Exercise 1: Reviewing the Incident Table

In this exercise, you will examine the incident table.

View Incidents

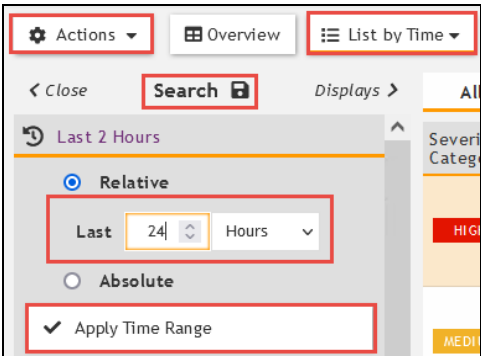
You will explore the **INCIDENTS** page on FortiSIEM, examine the various search capabilities, and clear conditions.

To view the incidents tab

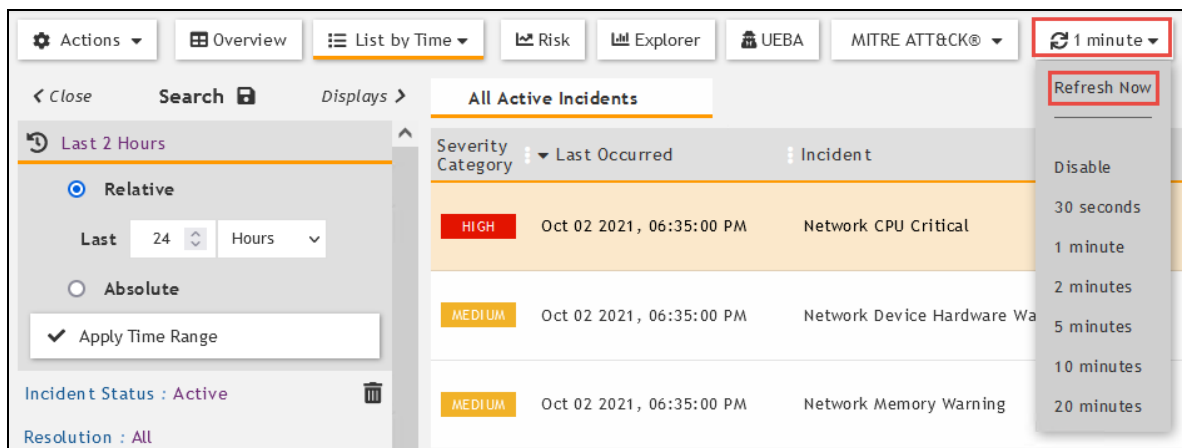
1. Log in to the FortiSIEM GUI with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Domain	LOCAL

2. Click the **INCIDENTS** tab.
3. Click **List**, and then select **by Time** to view the incident.
4. Click **Actions**, and then in the drop-down list, select **Search**.
5. Click **Last 2 Hours** to change the time range.
6. Select **Relative**, in the **Last** field, type 24, and then select **Hours** in the drop-down list.
7. Click **Apply Time Range**.

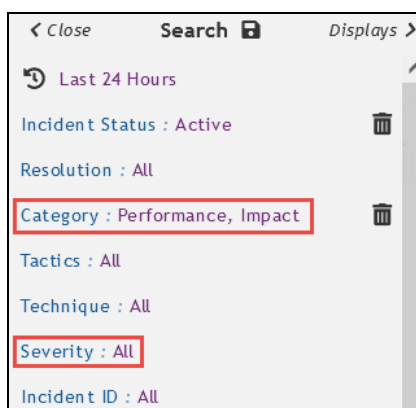


8. Click the refresh icon, and then in the drop-down list, select **Refresh Now**.

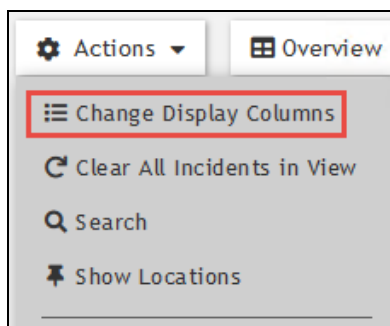


9. In the **Search** pane, click **Severity**, and then select **High**.
The results show a filtered subset of high-severity incidents.
10. In the **Search** pane, change the following settings:

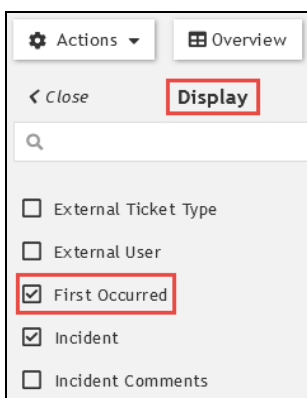
Field	Value
Severity	All (clear HIGH)
Category	Performance



11. In the left **Search** pane, click **Close** to close the left pane.
12. Click **Actions**, and then in the drop-down list, select **Change Display Columns**.



13. In the **Display** list, select **First Occurred**.



14. Click **Close** to close the left pane.
15. In the **First Occurred** column, click and drag the cursor to the **Last Occurred** column.

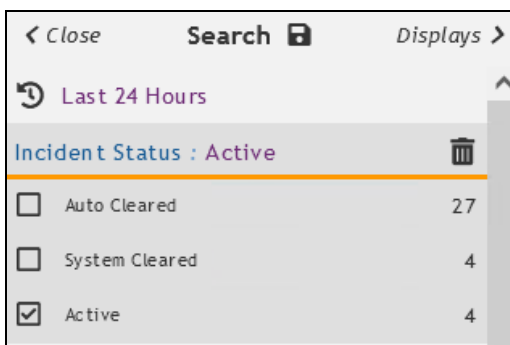
All Active Incidents. Filters Applied										
Severity Category	First Occurred	Last Occurred	Incident	Tactics	Technique	Reporting	Source	Target	Detail	Incident Status
High	Oct 02 2021, 05:43:30 PM	Oct 02 2021, 06:49:00 PM	Server Disk Space Critical	Impact	Endpoint EL...	WIN2K8	192.168.0.40	Disk Na...	Disk Cap...	Active
Medium	Oct 02 2021, 05:43:30 PM	Oct 02 2021, 06:49:00 PM	Server Disk space Warning	Impact	Endpoint EL...	ibm aix	172.16.20.160	Disk Na...	Disk Cap...	Active
Medium	Oct 02 2021, 05:43:30 PM	Oct 02 2021, 06:47:00 PM	Network Memory Warning	Impact	Endpoint EL...	junos perfw	172.16.255.70	Memory		Active
High	Oct 02 2021, 05:43:30 PM	Oct 02 2021, 06:49:00 PM	Network CPU Critical	Impact	Endpoint EL...	FortiGate900	10.1.1.1	CPU Util		Active

The incident dashboard view now contains the column you added, in the position that you placed it in.

To review the incident clear condition

1. Continuing on the FortiSIEM GUI, click **Actions**, and then in the drop-down list, select **Search**.
2. Click **Incident Status**.

Note that only **Active** status incidents are shown.



3. Click **Close** to close the left pane.

There are four different incident statuses available. However, a status type is listed only when incidents with that status exist in the selected time range.

The available statuses are:



- **Active**
- **Cleared**
- **Manually Cleared**
- **System Cleared**

If you cannot find any incidents, change to view **ALL** by clearing the **Active** checkbox.

- For the **WIN2K8** reporting device, select the **Server Disk Space Critical** incident.
- Enable **Auto expand**.
- In the bottom pane, click the up arrow icon.



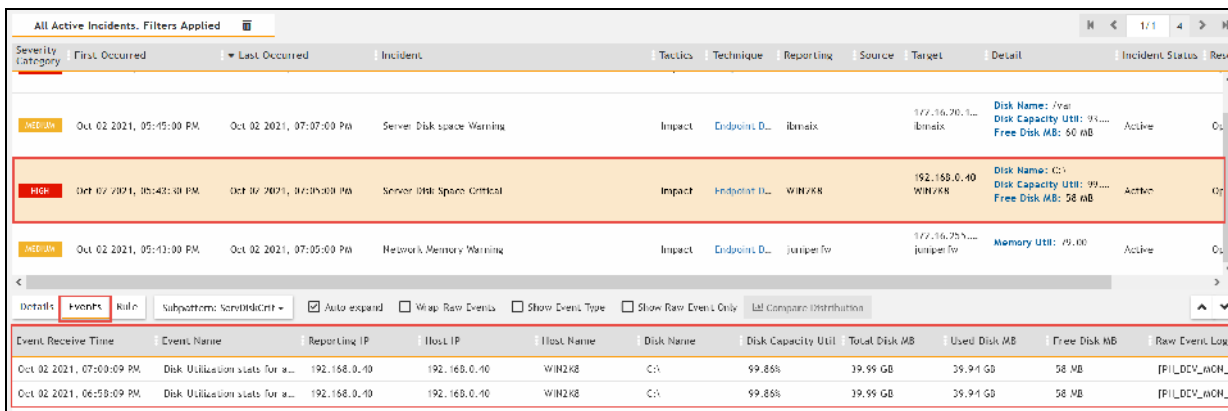
The incident details appear.



If you select an incident and the lower pane does not appear, click the up arrow icon ^ to expand the lower pane manually.

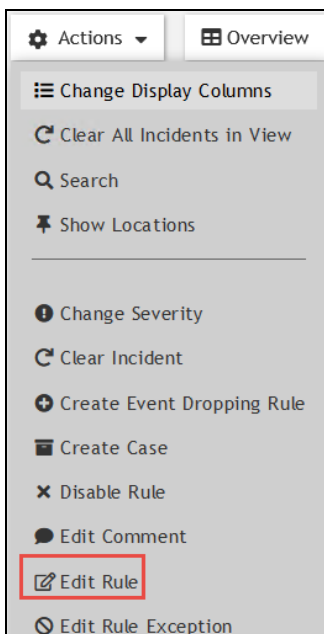
You can select the **Auto expand** option in the lower pane, so you don't have to keep manually expanding the lower pane for incidents.

- Select the **Events** tab to view the events for this incident.



If you don't see the expected result, you may have to change the time range to two days. If you still don't see incidents, they may be cleared by the system. By default, the active incident filter is applied. If the incidents are cleared, you may have to run the scripts again from the NSE Institute website to send events to FortiSIEM.

- With the **Server Disk Space Critical** incident selected, click **Actions**, and then in the drop-down list, select **Edit Rule**.



The **Edit Rule** dialog box opens.

9. Click **Step 3: Define Action**.
10. Beside **Clear: Defined**, click the pencil icon to edit the clear condition.



What do you think this option is actually doing for this rule? See ["Appendix: Answer Sheet" on page 246](#) for the answer.

11. Click **Cancel** to close the **Edit Rule Clear Conditions** dialog box.
12. In the **Edit Rule** dialog box, click **Cancel**.

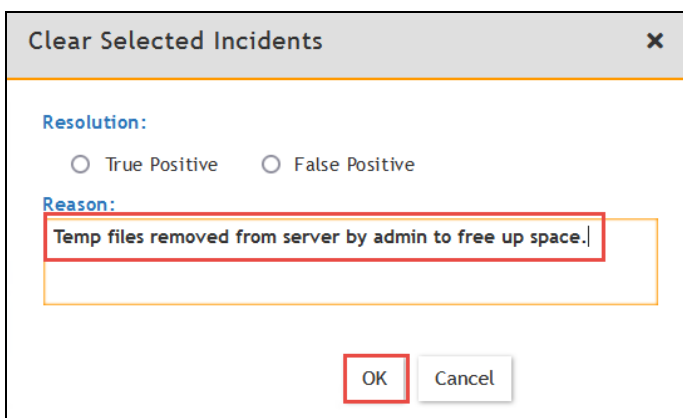
To manually clear an incident

1. Continuing on the FortiSIEM GUI, in the incident **Search** section, in the **Incident Status** drop-down list, ensure that **Active** is selected.
2. Click **Close** to close the left pane.
3. Select the **Server Disk Space Critical** incident, click **Actions**, and then in the drop-down list, select **Clear Incident**.



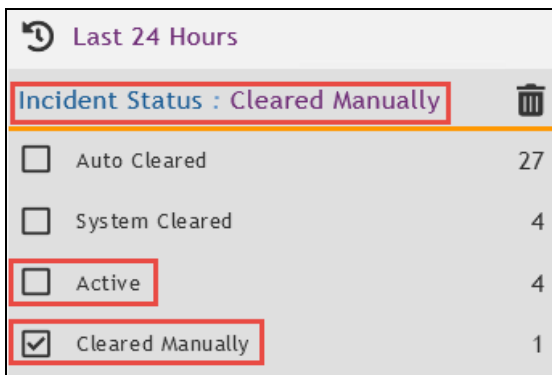
The **Clear Selected Incidents** dialog box opens.

4. In the **Reason** field, type Temp files removed from server by admin to free up space..
5. Optionally, you can choose a **Resolution** option.
6. Click **OK**.
7. Click **Yes**.



Note that the **Server Disk Space Critical** for **WIN2K8** incident will disappear from the list because the incident status is set to show incidents with an **Active** status.

8. Click **Actions**, and then in the drop-down list, click **Search**.
9. Click **Incident Status**, and then in the drop-down list, select the **Cleared Manually** checkbox and clear the **Active** checkbox.



Note that the **Server Disk Space Critical** for **WIN2K8** appears again in the main pane with an incident status of **Manually Cleared**.

10. Click **Close**.
11. Select the **Server Disk Space Critical** incident for **WIN2K8** with the status of **Manually Cleared**.
The bottom pane appears with the incident **Details**.
12. Review the **Cleared Reason** field.

The screenshot shows the 'Details' tab of an incident in FortiSIEM. The incident is 'Server Disk Space Critical' on host 'WIN2K8', with a status of 'Manually Cleared' and a severity of 'HIGH'. The 'Cleared Reason' is 'Temp files removed from server by admin to free up space.' and the 'Cleared User' is 'admin'. Other details include 'Count: 27', 'Event Name: Server Disk Space Critical', 'Event Type: PH_RULE_SERVER_DISK_SPACE_CRIT', 'First Occurred: Oct 02 2021, 05:43:30 PM', 'Incident ID: 323', 'Incident Title: Server Disk Space C:\ Critical on WIN2K8', 'Reporting Device Status: Pending', 'Reporting IP: 192.168.0.40', and 'Tactics: Impact'.

Attribute	Value
Category	Performance
Cleared Reason	Temp files removed from server by admin to free up space.
Cleared Time	Oct 02 2021, 07:29:25 PM
Cleared User	admin
Count	27
Event Name	Server Disk Space Critical
Event Type	PH_RULE_SERVER_DISK_SPACE_CRIT
First Occurred	Oct 02 2021, 05:43:30 PM
Incident ID	323
Incident Title	Server Disk Space C:\ Critical on WIN2K8
Reporting Device Status	Pending
Reporting IP	192.168.0.40
Severity Category	HIGH
Tactics	Impact

13. Click **Actions**, and then in the drop-down list, select **Search**.
14. In the **Incident Status** drop-down list, select **Active**.
15. Click the **INCIDENTS** tab.
16. Click **Actions**, and then in the drop-down list, select **Search**.
17. Clear all of the selections.

Actions

Overview

Close

Search

Last 24 hours

Incident Status : Active

Resolution : All

Category : All

Tactics : All

Technique : All

Severity : All

Incident ID : All

Incident Name : All

Host : All

IP : All

User : All

Reporting Device : All

Reporting IP : All

Reporting Device Status : All

Ticket Status : All

Biz Service : All

18. Log out of the FortiSIEM GUI.

Exercise 2: Grouping and Tuning Incidents

In this exercise, you will group common incidents and fine-tune FortiSIEM to reduce the number of incidents produced.

Examine a Group of Incidents

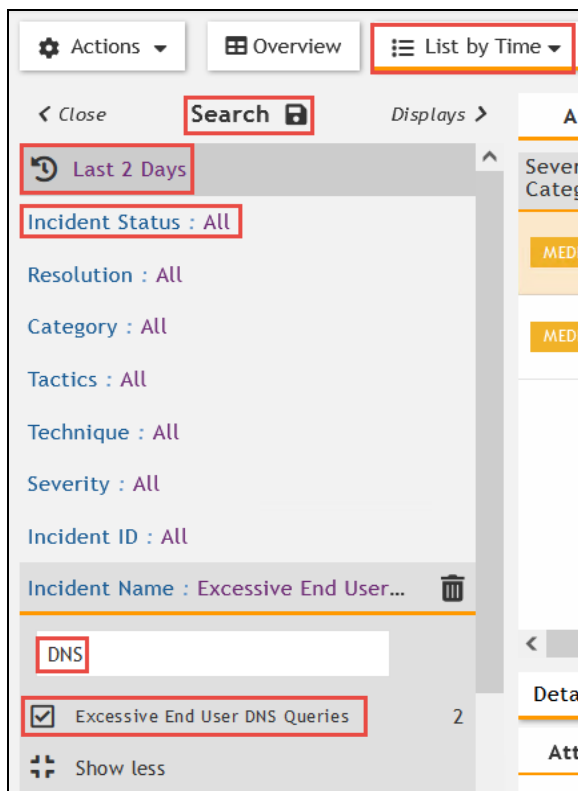
You will review a group of incidents on FortiSIEM.

To review a group of incidents

1. Log in to the FortiSIEM GUI with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Domain	LOCAL

2. Click the **INCIDENTS** tab.
3. Click **List**, and then select **by Time** to view the incident.
4. Click **Actions**, and then in the drop-down list, select **Search**.
5. Click **Last 2 Hours** to change the time range.
6. Select **Relative**, in the **Last** field, type 2, and then in the drop-down list, select **Days**.
7. Click **Apply Time Range**.
8. Beside **Incident Status: Active**, click the clear icon () to change it to **All**.
9. Click the **Incident Name**.
A drop-down list of different incidents appears. The incidents are grouped with a count indicating the number of incidents for the group.
10. In the **Incident Name** section, click **Search**, and then type **DNS**.
This shows a group of incidents with the keyword **DNS**.
11. Select the **Excessive End User DNS Queries** incident, and then click **Close** to close the left pane.



This shows only incidents for the group **Excessive End User DNS Queries**.

Severity Category	First Occurred	Last Occurred	Incident	Tactics	Technique	Reporting	Source	Target	Detail	Incident Status	Resolution
High	Sep 30 2021, 05:02:30 PM	Oct 01 2021, 10:15:30 AM	Excessive End User DNS Queries	Comm...	Dynamic...	FG2400591380...	192.168.22.11		Triggered Event Count: 557	Active	Open
Medium	Sep 30 2021, 05:03:30 PM	Oct 01 2021, 10:15:30 AM	Excessive End User DNS Queries	Comm...	Dynamic...	FG2400591380...	192.168.200.12		Triggered Event Count: 617	Active	Open

12. Select one of the incidents, and then in the **Actions** drop-down list, click **Edit Rule**.
13. In the **Edit Rule** dialog box, click **Step 2: Define Condition**.
14. In the **Conditions** section, beside the **ExcessiveDNSFromFlow** subpattern, click the pencil icon.
15. Review the subpattern.

Explain what the rule pattern is looking for. See "[Appendix: Answer Sheet](#)" on page 246 for the answer.

16. Click **Cancel** to close the **Edit SubPattern**.
17. Click **Cancel** to exit the **Edit Rule** dialog box.

Tune Incidents

To demonstrate the tuning capabilities for an incident, you will analyze incident source 192.168.22.11, which is an application server that produces a huge amount of DNS queries by design.

To tune incidents

- Continuing on the FortiSIEM GUI, select the incident with the IP **192.168.22.11**.
- Click **Actions**, and then in the drop-down list, select **Edit Rule Exception**.
The **Edit Rule Exception** dialog box opens.
- In the condition section, click the **Attribute** drop-down list.
Note that the only attribute that can be used for an exception for this particular incident is the **Source IP**.

Edit Rule Exception

An incident will not be generated if the following conditions match:

Paren	Attribute	Operator	Value	Paren	Next	Row
+ -	attribute...	=	value...	+ -	AND	+ -
	Source IP					

- Add the following condition:

Field	Value
Attribute	Source IP
Operator	=
Value	192.168.22.11

- Click **Save**.
This configuration suppresses any incidents if this rule triggers for the incident source of 192.168.22.11.
- Clear the incident (**192.168.22.11**), and when prompted, enter a reason.
- Before proceeding to the next exercise, click **Actions > Search**, and then clear all of the selections.
- Log out of the FortiSIEM GUI.

Exercise 3: Using the Built-In Ticketing System

In this exercise, you will configure the built-in ticketing system on FortiSIEM.

Review Incidents for Suspicious Activity

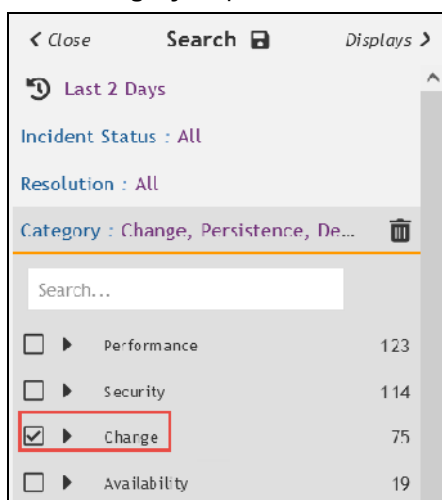
You will review some incidents for suspicious activity on FortiSIEM.

To review incidents for suspicious activity

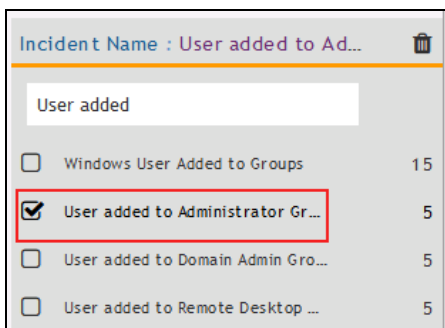
1. Log in to the FortiSIEM GUI with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Domain	LOCAL

2. Click the **INCIDENTS** tab.
3. Click **List**, and then select **by Time** to view the incident.
4. Click **Actions**, and then in the drop-down list, select **Search**.
5. Click **Last 2 Hours** to change the time range.
6. Select **Relative**, in the **Last** field, type 2, and then in the drop-down list, select **Days**.
7. Click **Apply Time Range**.
8. Beside **Incident Status: Active**, click the clear icon (🗑️) to change it to **All**.
9. In the **Category** drop-down list, select **Change**.



10. Click **Incident Name**, and then in the search field, type `User added to Administrator Group`.
11. Select **User added to Administrator Group**.



12. Click **Close** to close the left pane.
Note that now it shows only incidents with the name **User added to Administrator Group**.
13. In the **Target** column, find, and then click the incident with the target user **mike.long**.
This is a suspicious entry.

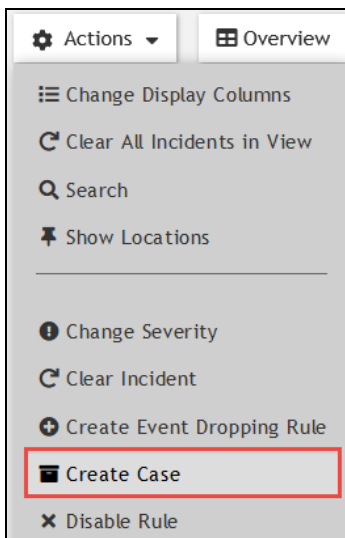
Severity Category	First Occurred	Last Occurred	Incident	Tactics	Technique	Reporting	Source	Target	Detail
MEDIUM	Sep 30 2021, 05:03:00 PM	Oct 01 2021, 10:03:20 AM	User added to Administrator Group	Persist...	Create ...	Threatsocio,th...	Computer: Win2008-ADS	Domain: THREATSOC	5
MEDIUM	Sep 30 2021, 05:04:00 PM	Oct 01 2021, 10:04:00 AM	User added to Administrator Group	Persist...	Create ...	WIN2008-ADS	WIN2008-ADS	User: mike.long Domain: ACCPTO	5
								Host Name: WIN2008-ADS User: mike.long Domain: ACCELOPS Target User: Users Target User Group: Administrators	

Create a Case in the Ticketing System

You will create a new case in the built-in ticketing system on FortiSIEM.

To create a case using the built-in ticketing system

1. Continuing on the FortiSIEM GUI, click **Actions**, and then in the drop-down list, select **Create Case**.



The **New Ticket** dialog box opens. Note that the **Incident ID(s)**, **Summary**, and **Notes** fields are prepopulated.

New Ticket

Incident IDs: 52 Mode: Create a new Ticket

Summary: mike.long added Users to Administrator Group on WIN2008-ADS domain ACCELOPS, in WIN2008-ADS(192.168.0.10)

State: New Assignee:

Escalation: None Selected Priority:

Due Date: 10/04/2021 Attachment:

Assignee Time Zone: Local America/Toronto

CC:

Notes: Incident Name => mike.long added Users to Administrator Group on WIN2008-ADS domain ACCELOPS
Incident Source => computer:
Incident Target => WIN2008-ADS(192.168.0.10)
Incident Detail =>
Incident ID => 52

Save Cancel

2. In the **Assignee** section, click the pencil icon.
3. Click the **Users** folder.
4. Click **admin**, and then click **Save**.

New Ticket

Users

User Name Full Name Email

admin admin@fsm.local

John doe

manager

Save Cancel

5. In the **Priority** section, select **High**.
6. In the **Due Date** field, specify a time in the future.
7. Click **Save**.

8. Click **Actions**, and then in the drop-down list, select **Change Display Columns**.
9. Select **Ticket Status**.
10. Click **Close** to close the left pane.

Observe the **Ticket Status** column, as well as the other default columns.

021, 06:01:00 PM	User added to Administrator Group	Persist...	Create ...	WIN2008-ADS	WIN2008-ADS User: mike.long Domain: ACCELOPS	Active	Open	Assigned
... Show More								

11. Click the **CASES** tab.
- The currently open tickets appear.

FortiSIEM

DASHBOARD

ANALYTICS

INCIDENTS

CASES

CMDB

RESOURCES

TASKS

ADMIN

0

New

1

Assigned

1

High

0

Overdue

0

Late

0

Closed

--

MTR

New

Edit

Export

1 minute

Q

Filters Applied

Elapsed

State

Priority

Ticket ID

Summary

Incident ID

Assignee

Creator

0 %

Assigned

High

961250

mike.long added Users to Administrator Group on WIN2008...

52

admin

admin (admin@fsm.local)

12. Select the ticket, and then click **Edit**.
13. In the lower pane, in the **Notes** field, type Who is this user? Needs to be verified.
14. Click **Save**.
15. Edit the ticket again, and then in the **Notes** field, type New admin in IT. Closing case.
16. In the **State** drop-down list, select **Closed**.
17. In the **Close Code** drop-down list, select **Solved (Permanent)**.

18. Click **Save**.
19. In the warning pop-up window, click **Yes**.

The screenshot shows the 'Edit Ticket' window in the FortiSIEM GUI. The window contains the following fields and values:

- Incident IDs: 52
- Summary: mike.long added Users to Administrator Group on WIN2008-ADS domain ACCELOPS, in WIN2008-ADS(192.168.1.100)
- State: Closed
- Close Code: Solved (Permanent)
- Assignee: admin <admin@fsm.local>
- Due Date: 10/10/2018 10:10:10
- Escalation: None Selected
- Assignee Time Zone: Local
- CC:
- Notes: New admin in IT. Closing case.

A modal dialog box is displayed in the center of the window with the text: "Closing this ticket will also clear related Incidents. Continue?". The dialog has two buttons: "Yes" and "No". The "Yes" button is highlighted with a red box.

At the bottom right of the window, there are two buttons: "Save" and "Cancel". The "Save" button is highlighted with a red box.

Note how the ticket state change is reflected in the table. Also, if you return to the **INCIDENTS** tab, the **Ticket Status** column for that incident displays **Closed**.

20. Log out of the FortiSIEM GUI.

Exercise 4: Creating a Custom Email Template

In this exercise, you will create a custom email template.

Configure Email Settings

You will configure the email gateway settings on FortiSIEM.

To configure email settings

1. Log in to the FortiSIEM GUI with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Domain	LOCAL

2. Click the **ADMIN** tab.
3. In the left pane, click **Settings**.
4. In the main window, click **System > Email**.
5. In the **Email** section, verify that the following values are configured:

Field	Value
Email Gateway Server	10.0.1.10
Default Email Sender	admin@fsm.local

6. Click **Save**.

← All Settings > System > Email

Email Gateway Server: 10.0.1.10 + - Secure Connection (TLS): ☐

Server Account ID: Admin Email IDs:

Account password: Leave empty for unchanged Default Email Sender: admin@fsm.local

Enable S/MIME: ☐ Send Without Key: ☐

Server Port: 25

Test Email Save

To create an email template

1. Continuing on the **Email** tab, in the **Incident Email Template** section, click **New**.
The **Email Template** dialog box opens.
2. In the **Name** field, type `FSM_LAB`.
3. Click the **Email Subject** field, click **Insert Content**, and then in the drop-down list, select **Status**.
4. In the **Email Subject** field, insert a space, then a hyphen (-), then a space, click **Insert Content** again, and then select **Rule Name**.
5. In the **Email Body** field, type some descriptive text.
6. Click **Insert Content**, and then add **Rule Name**, **Rule Description**, **First Seen Time**, **Last Seen Time**, **Incident Source**, **Incident Target**, and **Incident Detail** to the **Email Body** section.

Email Template

Name:

Insert Content: ☐ HTML Tag?

Email Subject:

Email Body: Customised Email_Template for FortiSIEM LAB.
Incident ID: \$incidentId
Incident Severity: \$incident_severity
Rule Name: \$ruleName
Description: \$ruleDescription
First Seen: \$firstSeenTime
Last Seen: \$lastSeenTime

Set as default: ☐

Note that you can enable **HTML Tags** to create HTML-based email templates.

7. Click **Save**.

Incident Email Template

Lines: 1

Name	Subject	Default
FSM_LAB	\$status - \$ruleName	☐

8. Log out of the FortiSIEM GUI.

Exercise 5: Creating a Notification Policy

In this exercise, you will learn how to create a notification policy.

Import a Rule

A system rule was modified for this lab to work. You will import the modified rule.

To import a rule

1. Log in to the FortiSIEM GUI from the Linux-Client VM with the following credentials:

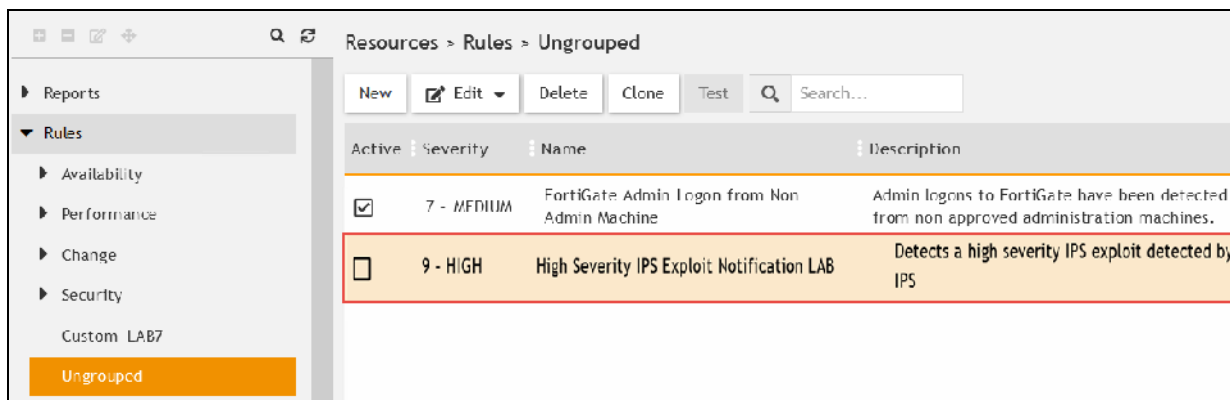
Field	Value
User ID	admin
Password	Fortinet1!
Domain	LOCAL

2. Click the **RESOURCES** tab.
3. In the left pane, select **Rules > Ungrouped**.
4. In the upper-right, click **Import**.



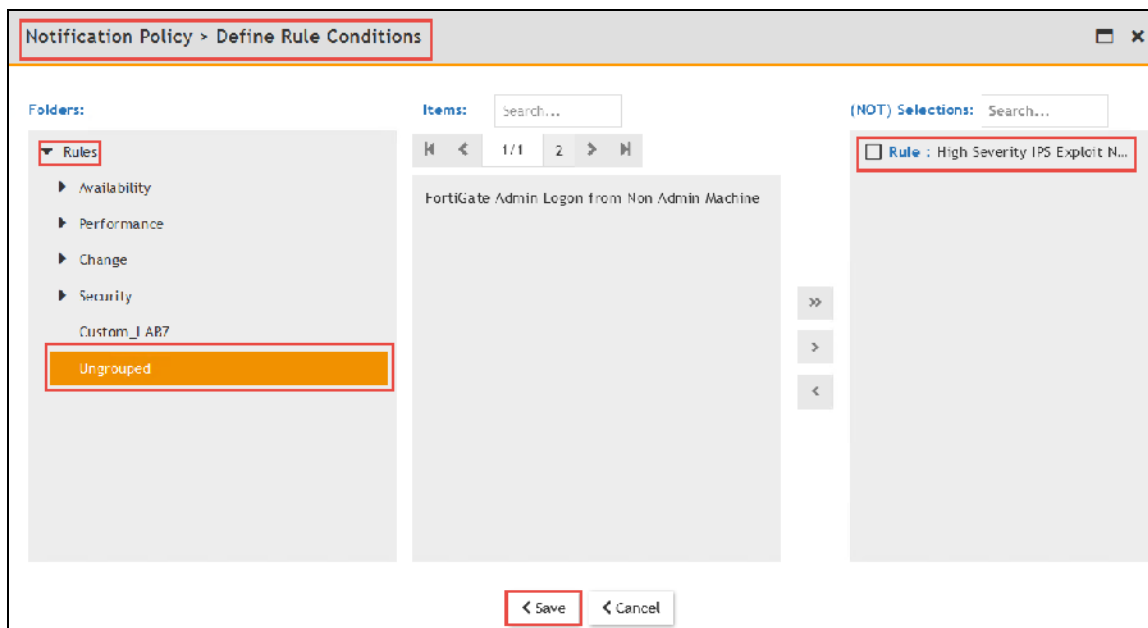
An **Import Rule** dialog box opens.

5. Click **Browse**.
6. Click **Desktop > Resources > LAB-8**, and then select the `Notification_test_rule.xml` file.
7. Click **Import**.
8. In the left pane, click **Rules > Ungrouped**.
Note that the imported rule named **High Severity IPS Exploit Notification LAB** is in an inactive state.



To create a notification policy

1. Continuing on the FortiSIEM GUI, click the **ADMIN** tab.
2. In the left pane, click **Settings**.
3. In the main window, click **General > Notification Policy**.
4. Click **New**.
5. In the **Rules** field, click the down arrow.
The **Notification Policy > Define Rule Conditions** window opens.
6. Click **Rules > Ungrouped**.
7. In the **Items** section, select **High Severity IPS Exploit Notification LAB**.
8. Click **>** to move the item to the **Selections** pane.
9. Click **Save**.



10. In the **Actions** section, beside **Send Email/SMS to the target users**, click the pencil icon to specify a notification action.
The **Notification Policy > Define Notification Actions** dialog box opens.
11. Click the **Add Addr** tab.

The **Notification Policy > Define Notification Actions > Email Address** dialog box opens.

12. In the **Method** drop-down list, select **Email**.
13. In the **To** field, type `student@fsm.local`.
14. In the **Email Template** drop-down list, select **FSM_LAB**.
15. Click **Save**.

Notification Policy > Define Notification Action > Email Address

Method: Email

To: student@fsm.local

CC:

Email Template Organization: Super

Email Template: FSM_LAB

< Save < Cancel

16. In the **Notification Policy > Define Notification Actions** dialog box, click **Save**.

Notification Policy > Define Notification Action

Delete Add Addr Add User Edit Email Template

Method	Name/Address	Email Template
Email	student@fsm.local	FSM_LAB

< Save < Cancel



The lab environment does not have an email server. Therefore, you cannot send notification emails. However, you walked through the steps of creating notification policies with email settings.

To test a notification policy, you will configure FortiSIEM to create a ticket when an incident is created for the selected rule.

17. In the **Notification Policy** dialog box, enable **Create Case when an incident is created**.
18. Click the pencil icon beside **Create Case when an incident is created**, and then configure the following settings:

Field	Value
Priority	High
Expires in	1 Week (s)
Assignee	Click the pencil icon, click Users , select admin , and then click Save .

Notification Policy > Ticket Setting

Escalation: None Selected

Priority: High

Expires in: 1 Week(s)

Assignee: admin

Save Cancel

- Click **Save**.
- In the **Notification Policy** dialog box, click **Save**.
- Enable the notification policy.

← All Settings > General > Notification Policy

New Edit Delete Clone Search... Columns

Enabled	Severity	Rule	Time Range	Affected Item	Action
☒	ANY	RULE:High Severity IPS Exploit Notificat...	ANY	ANY	Create Case Email student@fsm.local [FSM LAB]

To enable the rule for the notification policy

- Continuing on the FortiSIEM GUI, click **Resources > Rules > Ungrouped**.
- Select **High Severity IPS Exploit Notification LAB**.
- Click the **Active** checkbox.
- In the pop-up window, select **Continue**.

Generate Incidents to Trigger a Notification Policy

You will generate scripted events to trigger the notification policy.

To generate incidents to trigger a notification policy

- On the Linux-Client VM, open a browser, and then go to the NSE Institute website.
- Navigate to **LABS SET 1**, and then under **Lab 3—Discovery**, select **Exercise 3.5—Start All Performance and Device Data**.

Wait approximately two minutes for the output. The output should resemble the following example:

Running Lab Exercise 3.5

Preparing ALL Other Device SNMP Walks for Discovery

Start Full Fake Data Replay

Data Replay Completed!

3. Close the Linux-Client VM browser tab.

Examine the Ticket Created by the Notification Policy

You will view the ticket created on FortiSIEM.

To view the ticket created by the notification policy

1. Return to the FortiSIEM GUI, and then click the **CASES** tab.

The ticket created by the notification policy appears. Note that it is assigned to the **admin** user.

			0	1	2	0	0	1	35m
			New	Assigned	High	Overdue	Late	Closed	MTTR
New	Edit	Export	1 minute	Q	Filters Applied				
Elapsed	State	Priority	Ticket ID	Summary	Incident ID	Assignee	Creator	Resolution Time	
0 %	Assigned	High	961051	High Severity IPS Exploit Notification LAB	550	admin	System		
	Closed	High	961050	mike.long added Users to Administrator Group on WIN200...	52	admin	admin cad...	35m 3/s	

Observe the **Creator** column.



It may take up to 10 minutes for the ticket to be created. Once you see the ticket for the **High Severity IPS Exploit Notification LAB** incident, it confirms the notification policy works.

2. You can also check the **Details** column of the **High Severity IPS Exploit Notification LAB** incident.

Active
Overview
1st by Time
Incidents
Explorer
MTR: All Incidents
1 minute
Search

All Active Incidents

Severity Category	First Occurred	Last Occurred	Incident	Tactics	Technique	Reporting	Source	Target	Detail	Incident Status	Resolution	Ticket Status	
High	Oct 04 2021, 10:55:47 PM	Oct 04 2021, 11:10:00 PM	High Severity IPS Exploit Notification LAB				172.400.0.180...	174.36.62.38	172.168.72.10	Compo... Attack... Trigger...	Active	Open	Assigned
High	Sep 30 2021, 05:10:00 PM	Oct 04 2021, 11:10:00 PM	Malware found by firewall but not reme...				172.400.0.180...	172.168.72.10	Malwa...	Active	Open	None	

Details
Events
Rule
Auto expand

Attributes
Search attribute name...

Category: Security
Count: 3
Event Name: High Severity IPS Exploit Notification LAB
Event Type: High_Severity_IPS_Exploit_Inciden...

Incident Comments
Add comments to incident...

Action History
Wrap Content

Time	Action	Result	Detail
Oct 04 2021, 10:55:47 PM	User SYSTEM created (Last 961051)	Success	
Oct 04 2021, 10:55:47 PM	Email sent to (student@f5.com.br)	Failed	Policy:962950



In the **Details** tab, in the **Action History** section, the information confirms that the ticket for the incident was created successfully. However, the email notification is in the **Failed** state because there is no email server configured in the lab environment.

3. Click the **ADMIN** tab.
4. Click **Settings > General > Notification Policy**.
5. Clear the checkbox for the notification policy to disable it.



The policies are disabled in the lab environment because the **High Severity IPS Exploit Notification LAB** rule generates many notifications.

Alternatively, to deactivate only the **High Severity IPS Exploit Notification LAB** rule, click **RESOURCES > Rules > Ungrouped > High Severity IPS Exploit Notification LAB**. Clear the checkbox in the **Active** column.

6. Log out of the FortiSIEM GUI.

Lab 9: Reporting

In this lab, you will run and schedule reports.

Objectives

- Open reports from the **Analytics** and **Reports** trees
- Schedule reports
- Create custom dashboards
- Explore the various options for dashboards and widgets
- Export and import dashboards
- Create custom CMDB reports

Time to Complete

Estimated: 60 minutes

Exercise 1: Opening a Report From the Analytics Page

In this exercise, you will open and save reports from the **Analytics** page.

Examine a Report From the Analytics Page

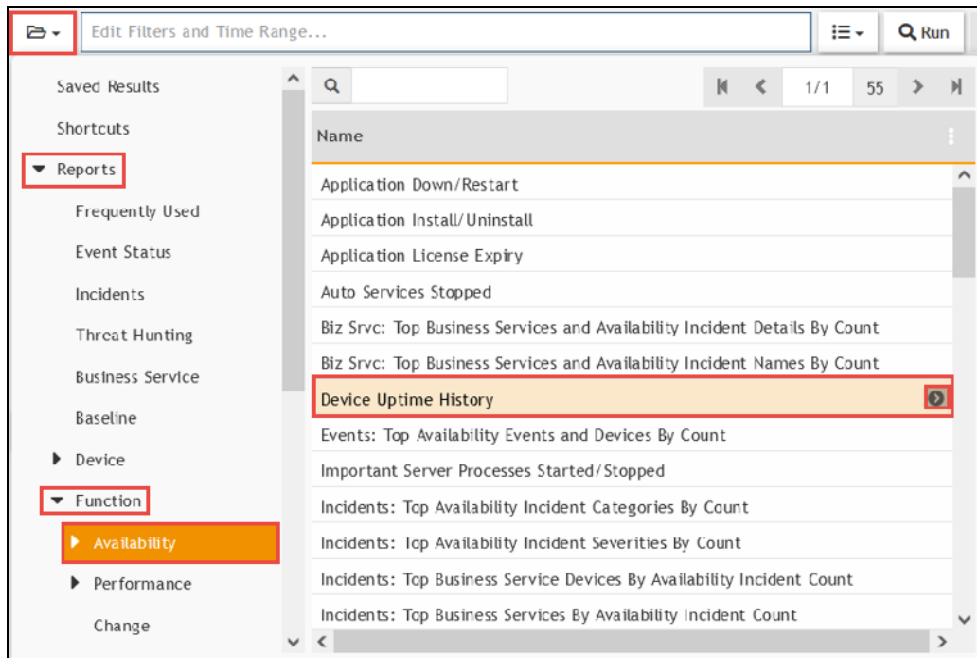
You will load, view, and modify a report on FortiSIEM.

To load a report

1. Log in to the FortiSIEM GUI using the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Domain	LOCAL

2. Click the **ANALYTICS** tab.
3. On the left, click the folder icon (📁).
4. Click **Reports > Function > Availability**.
5. On the right pane, select **Device Uptime History**, and then click the right arrow icon (➡).



When you click the right arrow icon, the report executes.

6. Click the search field.
The **Filters** editor opens. Notice how the query syntax is prepopulated.
7. In the **Time** section, select **Relative**, in the **Last** field, type 5, and then in the drop-down list, select **Hours**.
8. Click **Apply & Run**.
9. When the results open, in the **Actions** drop-down list, select **Save as Report**.
The **Save Report** window opens.
10. In the **Report Name** field, type `Device Uptime History-only-Results`.
11. Leave the **Save Definition** checkbox cleared, and then in the **Save Results for** field, type 1 and select **Hours**.
12. Click **OK**.

Save Report

Save Report Result for: Device Uptime History

Report Name:

Device Uptime History-only-Results

☐ Save Definition

☒ Save Results for: 1 ☒ Hours ☐ Days

☐ Save Report Design Template

OK Cancel

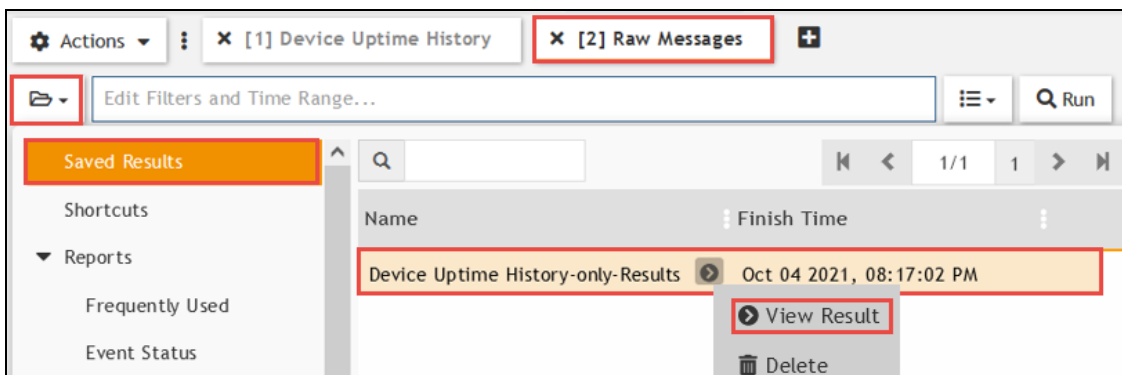
To load saved results for a report

1. Continuing on the FortiSIEM GUI, click the plus icon (+) to open a new search.

Action : [1] Device Uptime History +

Event Type = PH_DEV_MON_SYS_UPTIME

2. Close the **[1] Device Uptime History** search tab.
3. In the new **[1] Raw Messages** tab, on the left, click the folder icon, and then select **Save Results**.
In the right pane, note that the **Device Uptime History-only-Results** report is listed with a date and time stamp.
4. Select the **Device Uptime History-only-Results** report, click the down arrow, and then click **View Result**.



5. Review the results (and the speed at which the results came back) and notice the **Time Range** selection.
6. Close the second search tab.

To modify the search query

1. Continuing on the FortiSIEM GUI, click the search field.
2. In the existing condition, under the **Next** column, select **AND**.
3. In the **Row** column, click the **+** icon.
4. Add a second condition using the following values:

Field	Value
Attribute	Reporting IP
Operator	IN

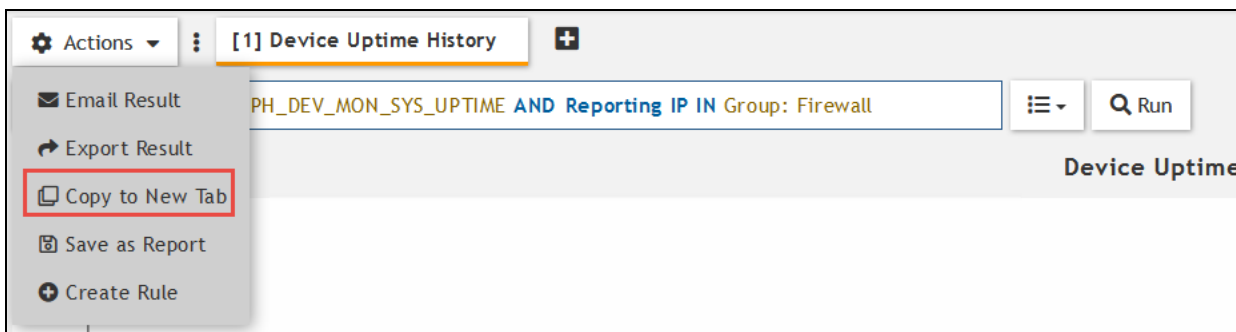
5. In the **Value** field, click and select **Select from CMDB**.
6. Click **Devices > Network Device > Firewall**.
7. In **Folders**, click **>>** to add the **Firewall** folder to **Selections**.
8. Click **OK**.
9. In the **Time** section, select **Relative**, in the **Last** field, type **1**, and then in the drop-down list, select **Day**.
10. Click **Apply & Run**.
Wait for the results.
11. Review the results.

Create a Report Template

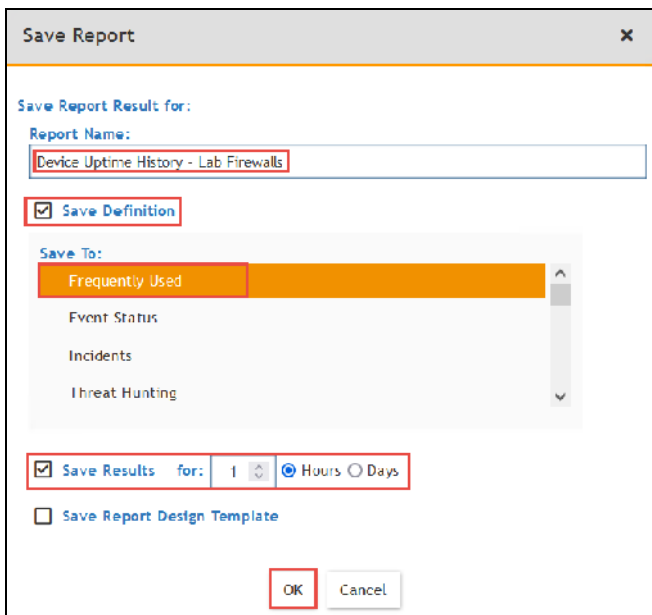
You will create a report template from the report you generated.

To save a copy of the report as a template

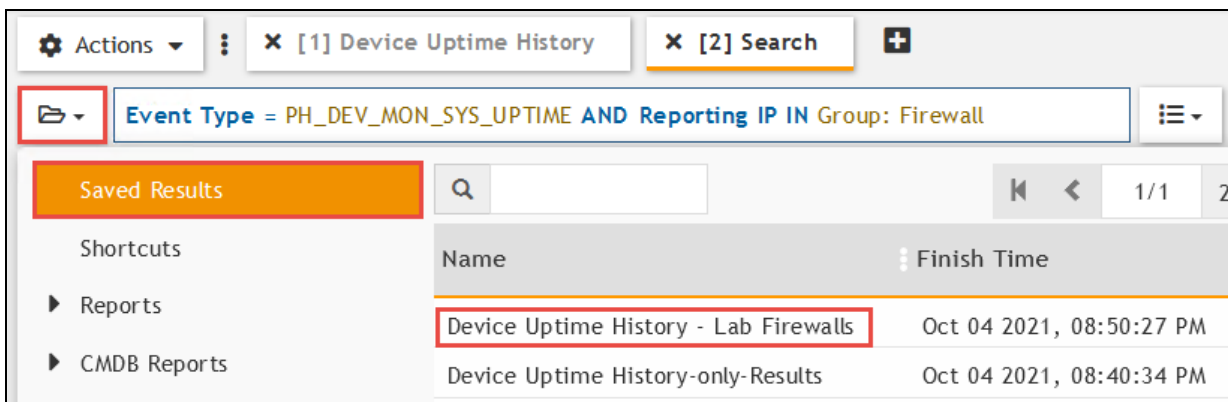
1. Continuing on the FortiSIEM GUI, in the **Actions** drop-down list, select **Copy to New Tab**.



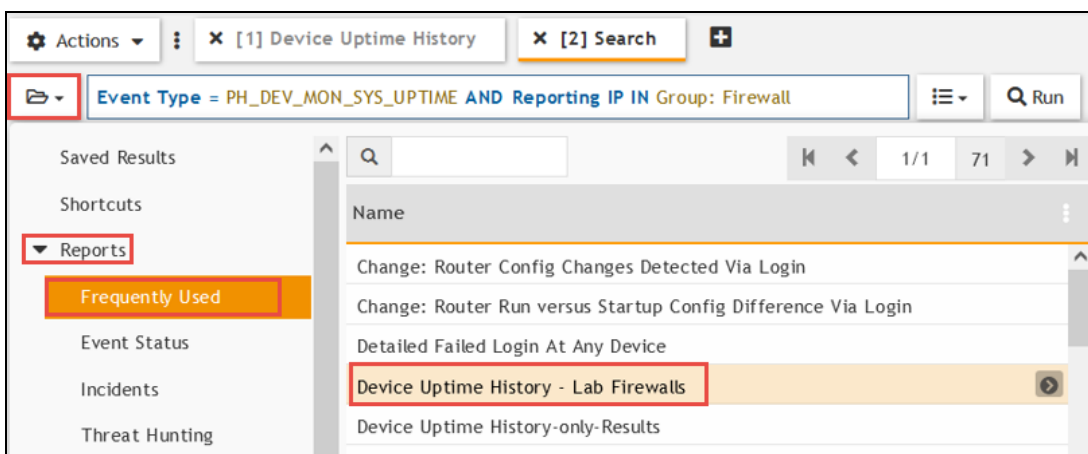
2. Click **Run**.
3. After the results appear, in the **Actions** drop-down list, select **Save as a Report**.
The **Save Report** window opens. The report name follows the format <report name>-<report interval>.
4. In the **Report Name** field, type Device Uptime History - Lab Firewalls.
5. Enable **Save Definition**.
6. In the **Save To** section, select **Frequently Used**.
7. Select **Save Results for**, and then set the value to 1 hour.
8. Click **OK**.



9. Click the folder icon, and then select **Save Results**.

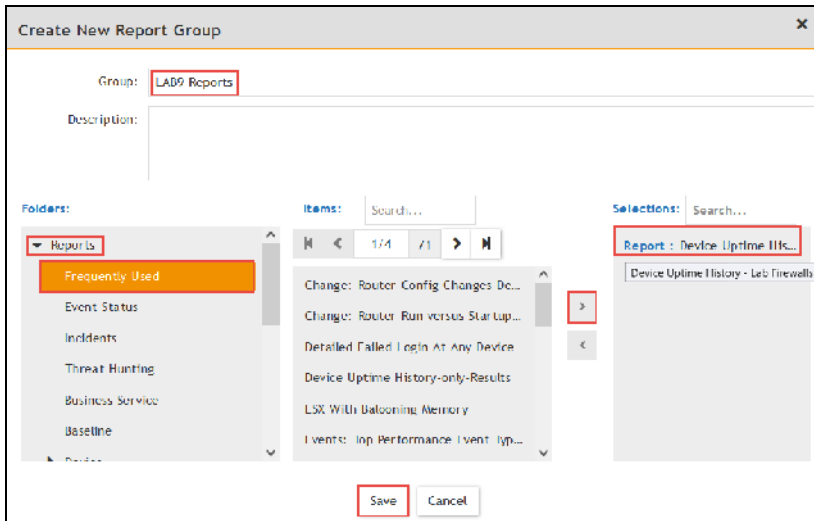


10. In the left pane, click **Reports > Frequently Used**.
11. In the right pane, in the search bar, type Lab Firewalls.
You should see the report you just saved.

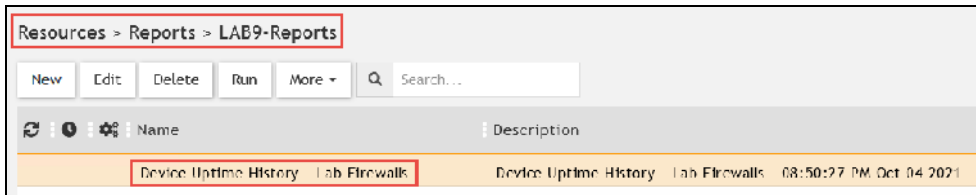


To create a custom report folder

1. Continuing on the FortiSIEM GUI, click the **RESOURCES** tab.
2. In the left pane, select **Reports**.
3. Click the **+** icon at the top of the pane to create a new report group.
4. In the **Group** field, type LAB9-Reports.
5. Click **Reports > Frequently Used**.
6. Under the **Items** column, in the search bar, type lab firewalls.
7. Select **Device Uptime History - Lab Firewalls**.
8. Click **>** to move the report to the **Selections** section.
9. Click **Save**.



You now have a new **LAB9-Reports** folder under **Reports** in the left pane.



10. Log out of the FortiSIEM GUI.

Exercise 2: Opening a Report From the Report Tree

In this exercise, you will explore opening and running reports from the report tree.

Run a Report From the Report Tree

You will run a report from the report tree.

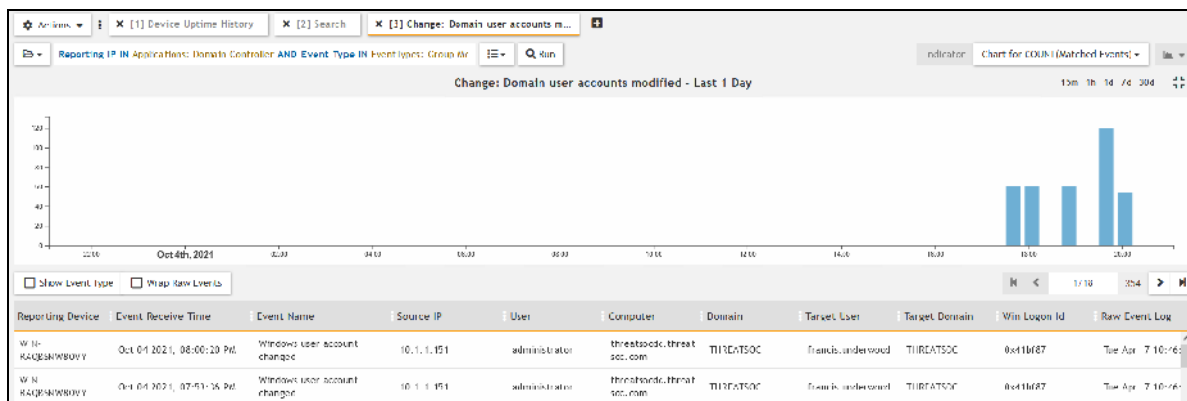
To run a report from the report tree

1. Log in to the FortiSIEM GUI with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Domain	LOCAL

2. Click the **RESOURCES** tab.
 3. In the left pane, click **Reports > Function > Change**.
 4. In the search field, type `user account mod`.
 5. Select the **Change: User Accounts Modified** report.
 6. Click **Run**.
- The **Run** window opens.
7. On the **Report Time Range** tab, make sure that **Relative** is enabled, 1 is entered in the **Last** field, and **Day** is selected in the drop-down list.
 8. Click **OK**.

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



9. Review the results.
10. Log out of the FortiSIEM GUI.

Exercise 3: Scheduling a Report

In this exercise, you will schedule a report.

Schedule a Report

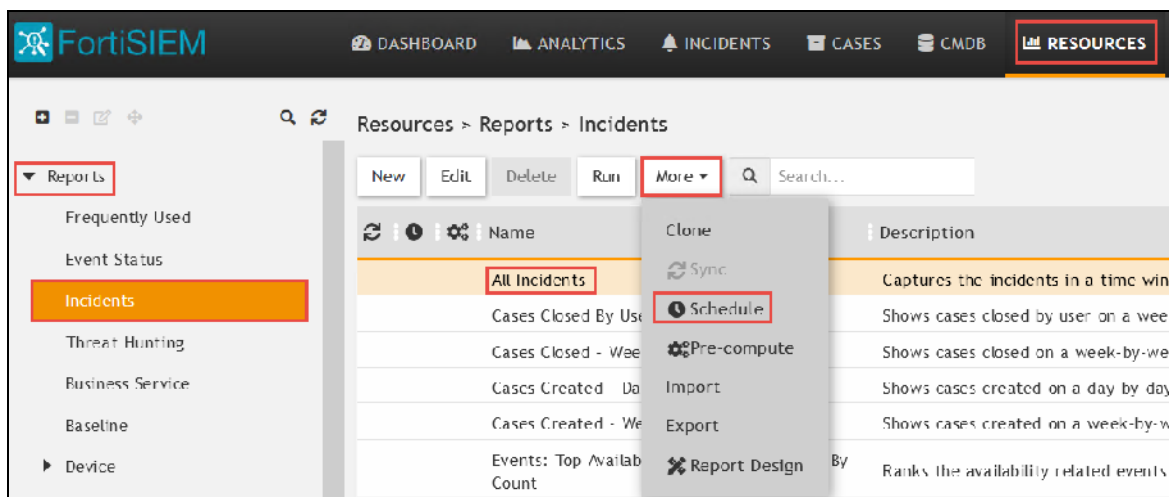
You will configure a scheduled report.

To schedule a report

1. Log in to the FortiSIEM GUI with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Domain	LOCAL

2. Click the **RESOURCES** tab.
3. In the left pane, click **Reports > Incidents**.
4. In the main window, select **All Incidents**.
5. In the **More** drop-down list, select **Schedule**.



6. Configure the following settings—you must click **Next** to view some settings:

Field	Value
Time Zone	Local

Field	Value
Report time range	Relative, last 1 Day
	Set to 10 minutes ahead of the current time and make sure Local is selected.
	Once
	PDF
Notification	Copy to a remote directory
Keep report for	2 hours

The lab environment does not have an email server. The remote directory to save reports is already configured. The reports folder is on the desktop of the **Linux-Client** VM.

To review the settings of the remote directory, click the **ADMIN** tab, and then click **Settings > Analytics > Scheduled Report**.



Scheduled Report Copy

Host: 10.0.1.10

Path: /home/student/Desktop/FortiSIEM_Reports/

User Name: student

Password:

Confirm Password:

Connect Method: SSH

Test

Save

7. Click OK.

The **Scheduled** column for the **All Incidents** report indicates that a report is scheduled.

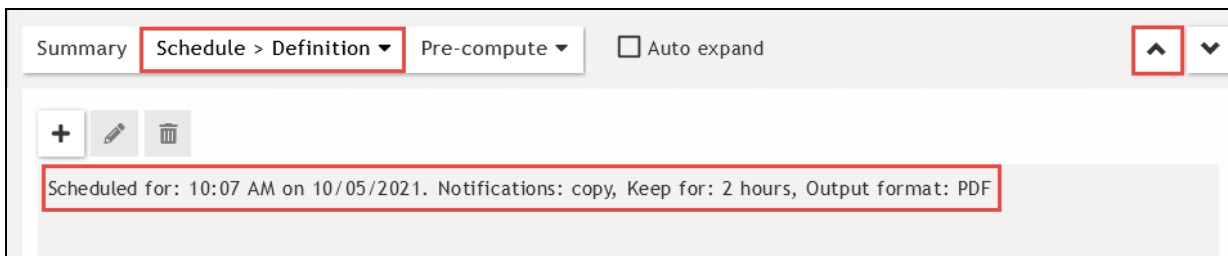
Resources > Reports > Incidents			
New	Edit	Delete	Run More
			Search...
	Name	Description	Report Design Template
☒	All Incidents	Captures the incidents in a time window	Global System Reports Root Template
	Cases Closed By User - Weekly	Shows cases closed by user on a week-by-week basis	Global System Reports Root Template

Configure an Alternative Scheduling Method

You will use an alternative method to schedule a report.

To configure an alternative scheduling method

1. Continuing on the FortiSIEM GUI, select the **All Incidents** report.
2. In the bottom pane, click the **Schedule > Definition** tab. (You may need to click the up arrow in the bottom-right corner of the GUI to see this).



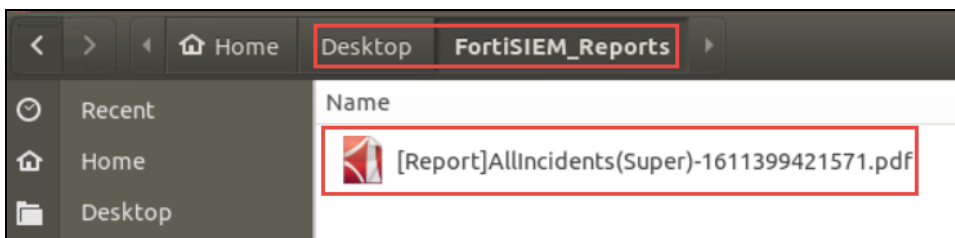
Note that the existing report schedule is already present.

3. Click the **+** icon.
Notice that the same **Schedule** dialog box shown above opens.
4. Click **Cancel**.
5. Click the **Scheduled for:<date>** entry.
Both the pencil and trash icons become active. The pencil icon is used to modify the schedule for the report.
The trash icon is used to delete the schedule for the report.



Do *not* delete the schedule for the report.

6. After ten minutes, go to the Linux-Client VM.
7. Verify the delivery of the scheduled report to the **FortiSIEM_Reports** folder located on the desktop.



8. Open the report, and then review the information.
9. Close the Linux-Client VM browser tab.
10. Log out of the FortiSIEM GUI.

Exercise 4: Creating Custom Dashboards

In this exercise, you will create a custom dashboard.

Create a Custom Dashboard

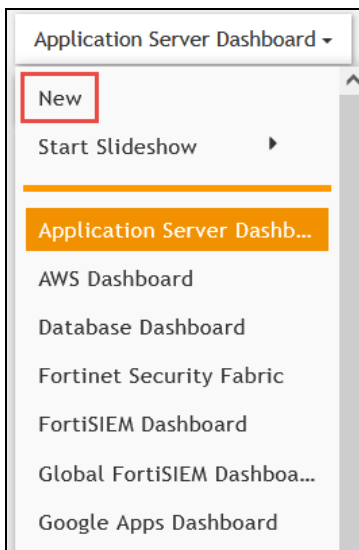
You will create a custom dashboard folder.

To create a custom dashboard folder

1. Log in to the FortiSIEM GUI with the following credentials:

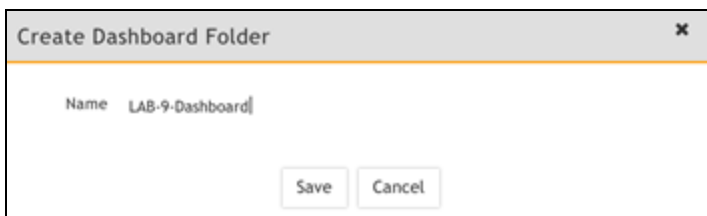
Field	Value
User ID	admin
Password	Fortinet1!
Domain	LOCAL

2. Click the **DASHBOARD** tab.
3. Click the drop-down menu on the left.
4. Click **New**.



The **Create Dashboard Folder** window opens.

5. In the **Name** field, type LAB-9-Dashboard.
6. Enable **Share with**.
7. Click **Save**.

A dialog box titled "Create Dashboard Folder" with a close button (X) in the top right corner. It contains a text field labeled "Name" with the value "LAB-9-Dashboard" entered. At the bottom, there are two buttons: "Save" and "Cancel".

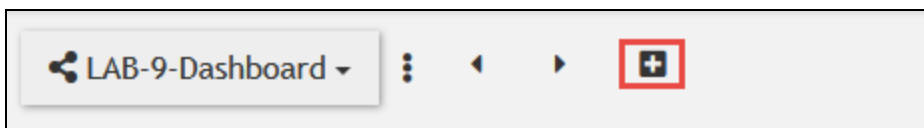
The **LAB-9-Dashboard** group opens and is added to the dashboard type drop-down list.

Configure a Summary Dashboard

You will create a new dashboard that displays an information summary of some devices.

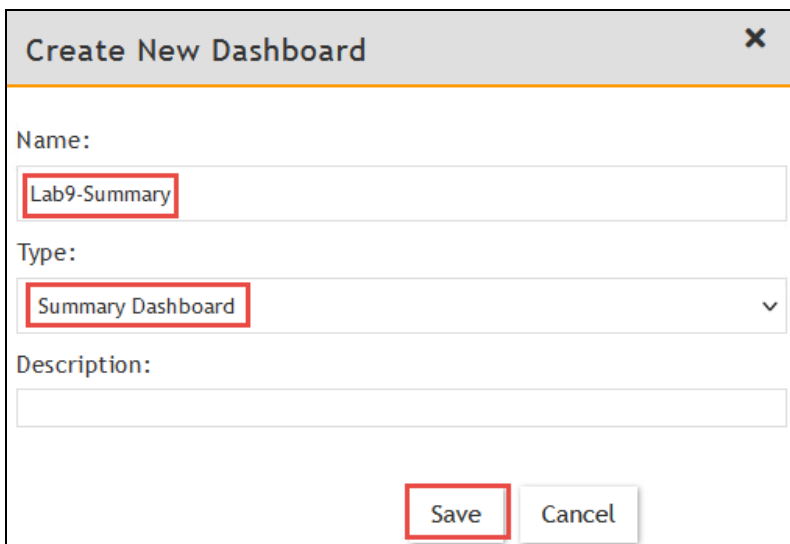
To add a summary dashboard

1. Continuing on the **LAB-9-Dashboard** window, click the plus icon (+) to the right of the dashboard drop-down list.



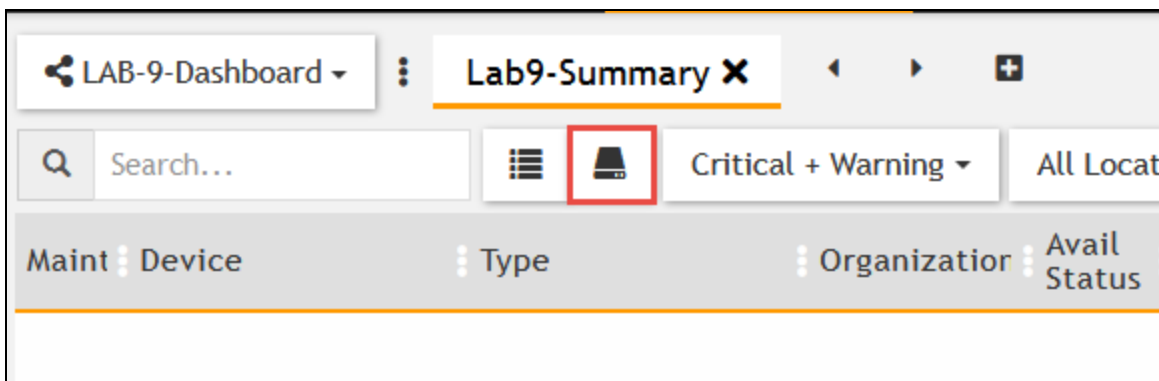
The **Create New Dashboard** dialog box opens.

2. In the **Name** field, type `Lab9-Summary`.
3. In the **Type** drop-down list, select **Summary Dashboard**, and then click **Save**.

A dialog box titled "Create New Dashboard" with a close button (X) in the top right corner. It contains three fields: "Name:" with the value "Lab9-Summary" (highlighted with a red box), "Type:" with a dropdown menu showing "Summary Dashboard" (highlighted with a red box), and "Description:" with an empty text area. At the bottom, there are two buttons: "Save" (highlighted with a red box) and "Cancel".

The **Lab9-Summary** dashboard opens. The **All Device** summary dashboards provide you with a blank page.

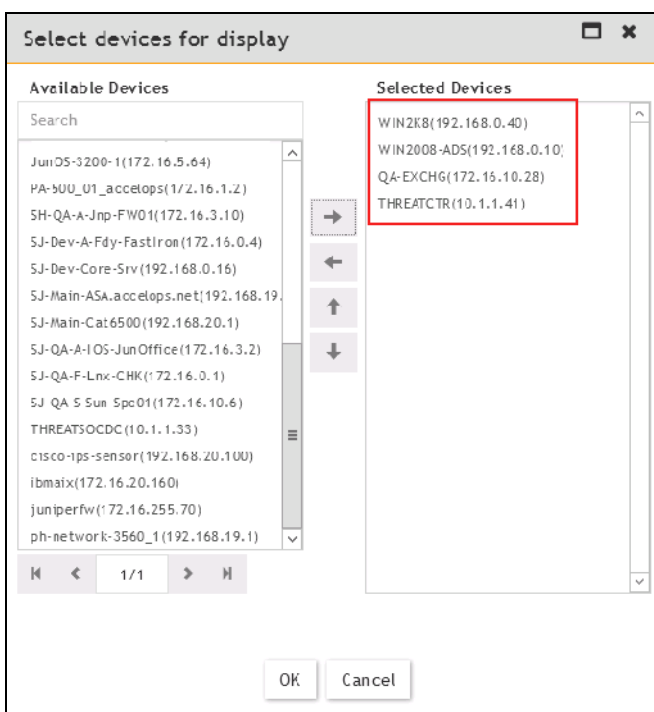
4. In the **Lab9-Summary** tab, click the select devices icon.



The **Select devices for display** dialog box opens.

5. In the **Available Devices** list, search for the following devices:

- WIN2K8(192.168.0.40)
- WIN2008-ADS(192.168.0.10)
- QA-EXCHG(172.16.10.28)
- THREATCTR(10.1.1.41)



6. Click the right arrow icon (➡) to move the devices to the **Selected Devices** list.

7. Click **OK**.

8. In the **Critical + Warning** drop-down list, select **All Severities**.

Your new summary dashboard appears.

The screenshot shows the 'Lab9-Summary' dashboard. At the top, there's a search bar and filters for 'All Severities' and 'All Locations'. Below is a table with columns: Maint, Device, Type, and Avail Status. A dropdown menu is open over the 'Type' column, showing options: 'Critical', 'Critical + Warning', and 'All Severities' (which is highlighted with a red box). The table lists four devices: WIN2K8, WIN2008-ADS, QA-EXCHG, and THREATCTR, all with 'Super' severity.

Maint	Device	Type	Avail Status
	WIN2K8	Microsoft Windows Server 2008	Super
	WIN2008-ADS	Microsoft Windows Server 2008	Super
	QA-EXCHG	Microsoft Windows Server 2003	Super
	THREATCTR	Microsoft Windows Server 2003	Super

9. In the **WIN2K8** device **Perf Status** column, hover over the red icon.

The screenshot shows the 'Lab9-Summary' dashboard with more columns: Organization, Avail Status, Packet Loss, Uptime, Uptime %, Perf Status, and Sec Status. A red icon in the 'Perf Status' column for 'WIN2K8' is highlighted with a red box. A tooltip is visible, showing 'Disk Capacity: Util -> Critical' and 'Free Disk MB -> Critical'.

Maint	Device	Type	Organization	Avail Status	Packet Loss	Uptime	Uptime %	Perf Status	Sec Status
	WIN2K8	Microsoft Windows Server 2008	Super						
	WIN2008-ADS	Microsoft Windows Server 2008	Super						
	QA-EXCHG	Microsoft Windows Server 2003	Super						
	THREATCTR	Microsoft Windows Server 2003	Super						

A pop-up appears indicating why the device is in a non-normal state.



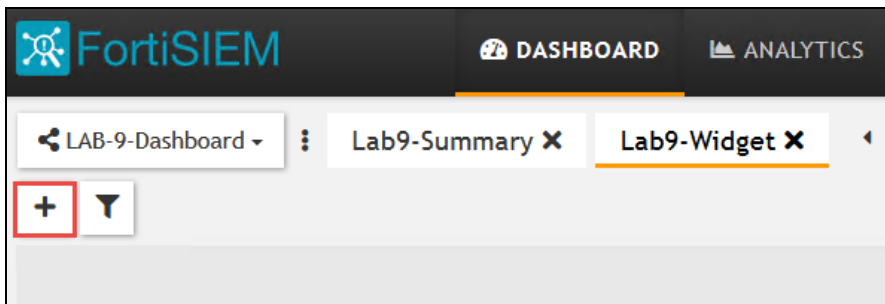
If you don't see the expected result, you may have to change the time range to two days. If you still don't see any incidents, the incidents may be cleared by the system. By default, the active incident filter is applied. If the incidents are cleared, you may have to run the scripts again from the NSE Institute website to send events to FortiSIEM to generate new incidents.

Configure a Widget Dashboard

You will configure a widget dashboard.

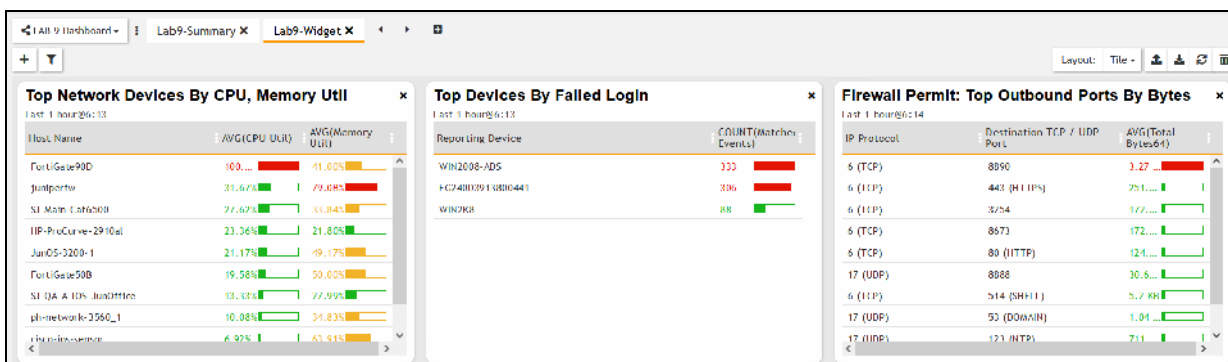
To add a widget dashboard

- Continuing on the **LAB-9-Dashboard** tab, click the plus icon (+) to the right of the dashboard drop-down list. The **Create New Dashboard** dialog box opens.
- In the **Name** field, type **Lab9-Widget**.
- In the **Type** drop-down list, select **Widget Dashboard**.
- Click **Save**.
The **Lab9-Widget** is created.
- In the **Lab9-Widget** tab, click the plus icon.

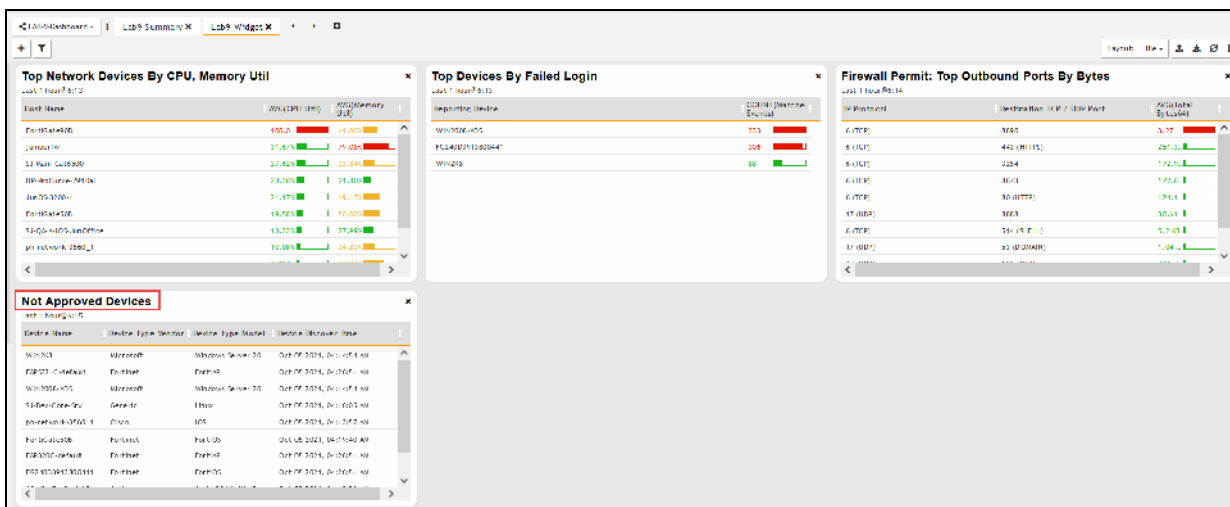


The **Report** selector pop-up appears from the left.

- In the left pane, click the **Reports** folder.
- Use the search field to find the following reports, and then click the right arrow icon to add them. (You must add the reports one at a time.)
 - Top Network Devices By CPU, Memory Util**
 - Top Devices By Failed Login**
 - Firewall Permit: Top Outbound Ports By Bytes**

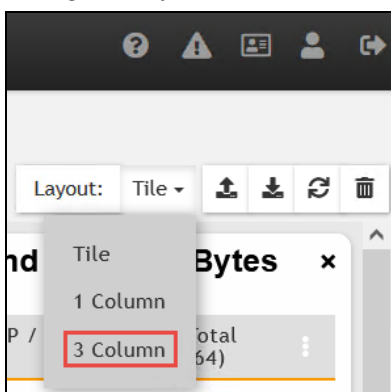


- In the **Lab9-Widget** tab, click the plus icon again.
- Select the **CMD&B Reports** folder.
- Search for the **Not Approved Devices** report.
- Click the right arrow icon to add a widget for the **Not Approved Devices** report.

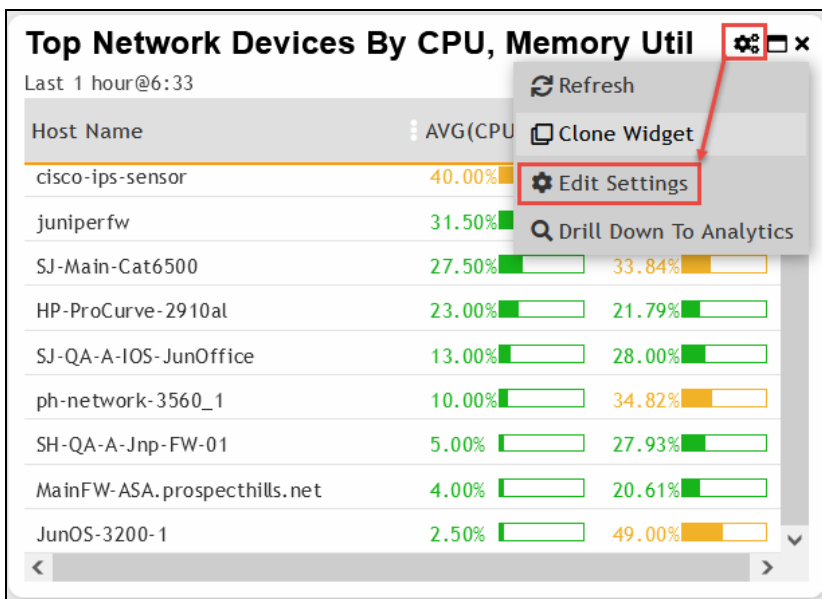


To explore widget dashboard options

1. Continuing on the FortiSIEM GUI, in the upper-right, click the **Layout columns** drop-down list.
2. Change the layout to **3 Column**.



3. Select the **Top Network Devices By CPU, Memory Util** widget, and then hover over the title bar.
4. On the right side of the title bar, click the gears icon (⚙️), and then in the drop-down list, select **Edit settings**.



The **Settings** dialog box opens.

5. In the **Time** drop-down list, select **Last 1 Week**.
6. In the **Display Settings** section:
 - Drag the first **AVG(CPU Util)** slider to about 25%.
 - Drag the second **AVG(CPU Util)** slider to about 60%.

Settings

Title: Top Network Devices By CPU, Memory Util

Display: Table View

Width: 3

Result Limit: 10

Trend Interval: Auto

Time: Last 1 week

Height: 2

Refresh Interval: 5 min

Nested Time: Last 1 hour

Display Settings

Show Bar: ☒

Column: AVG(CPU Util)

Enable Color Setting: ☒

Range Select: 0% 100%

Column: AVG(Mem Util)

Enable Color Setting: ☒

Range Select: 0% 100%

Reverse Color Map: ☐

Save Cancel

7. Click **Save**.

The results are colored to reflect the seriousness of the value.

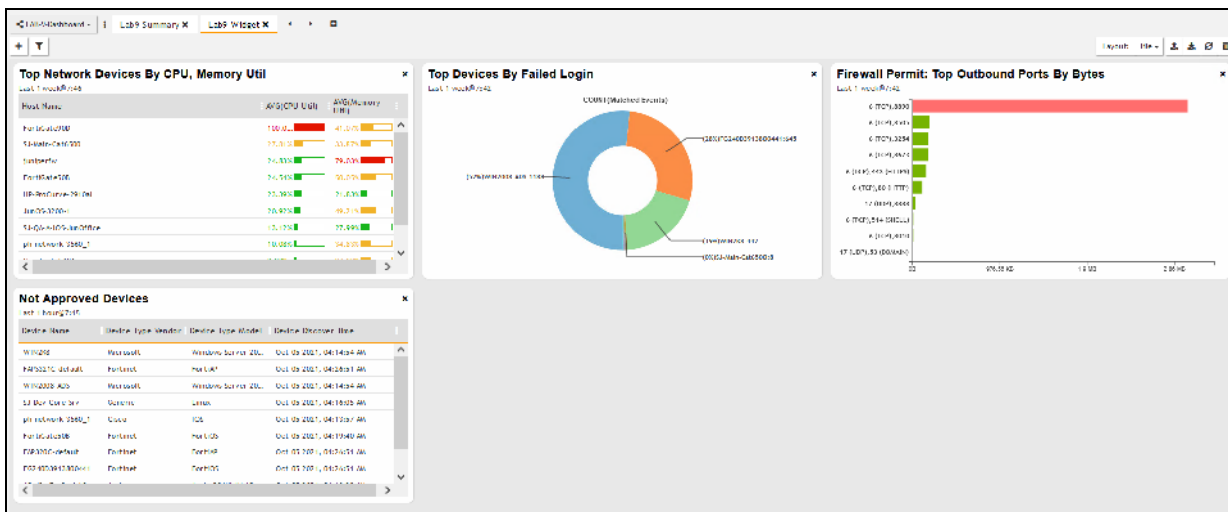
Top Network Devices By CPU, Memory Util

Last 1 hour@6:38

Host Name	AVG(CPU Util)	AVG(Memory Util)
FortiGate90D	100.00%	41.00%
cisco-ips-sensor	40.00%	63.91%
juniperfw	31.50%	79.00%
SJ-Main-Cat6500	27.50%	33.84%
HP-ProCurve-2910al	23.00%	21.79%
SJ-QA-A-IOS-JunOffice	13.00%	28.00%
ph-network-3560_1	10.00%	34.82%
SH-QA-A-Jnp-FW-01	5.00%	27.93%
MainFW-ASA-prospecthills.net	4.00%	20.61%

Will these new adjusted values for AVG CPU determine what thresholds rules will trigger for these devices?
See "Appendix: Answer Sheet" on page 247 for the answer.

- In the **Top Devices By Failed Login** widget, click the settings icon.
- In the **Display** drop-down list, select **Aggregation View (Donut)**.
- In the **Time** drop-down list, select **Last 1 Week**.
- Click **Save**.
- In the **Firewall Permit: Top Outbound Ports By Bytes** widget, click the settings icon.
- In the **Display** drop-down list, select **Aggregation View (Bar)**.
- In the **Time** drop-down list, select **Last 1 Week**.
- Click **Save**.



- Log out of the FortiSIEM GUI.

Exercise 5: Examining Dashboard Drill-Down Capabilities

In this exercise, you will examine the drill-down capabilities of the FortiSIEM dashboards.

Drill Down on Dashboard Content

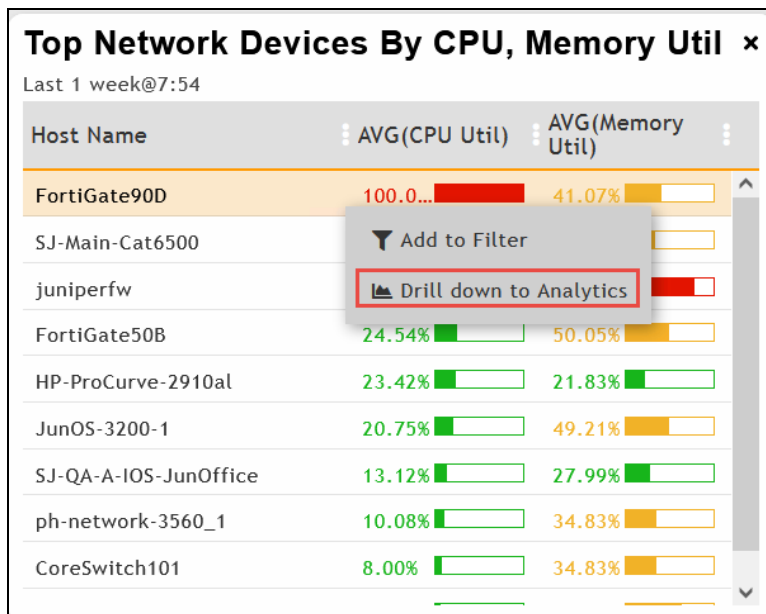
You will examine the FortiSIEM dashboard drill-down capabilities.

To drill down on dashboard content

1. Log in to the FortiSIEM GUI with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Domain	LOCAL

2. Click the **DASHBOARD** tab.
3. Navigate to the **LAB-9-Dashboard** created in the previous exercise.
4. Click **Lab9-Widget**.
5. In the **Top Network Devices By CPU, Memory Util** widget, select **FortiGate90D**.
6. Click the drop-down arrow associated with the **Host Name** column, and then select **Drill down to Analytics**.



This takes you to the **ANALYTICS** tab.

7. Click the search field.

What is the query searching for? See ["Appendix: Answer Sheet" on page 247](#) for the answer.

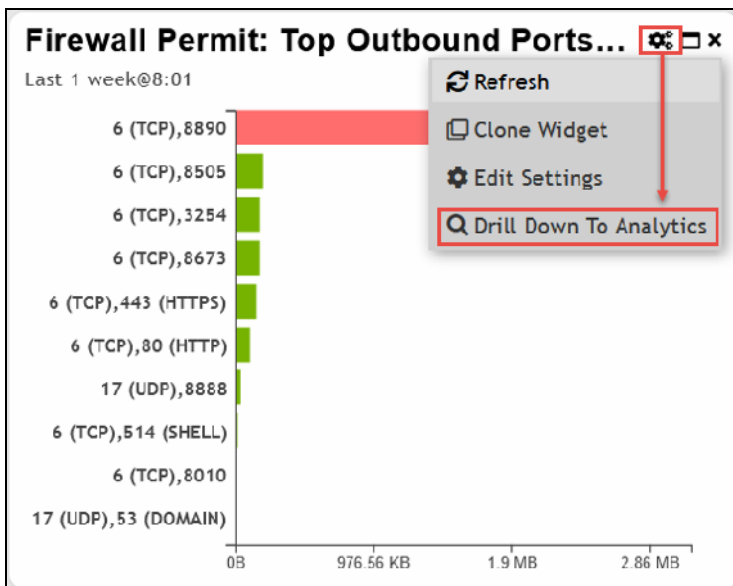
8. Look at the **Time** selection.

What has the time criteria been prepopulated to run over and where did this value come from? See ["Appendix: Answer Sheet" on page 247](#) for the answer.

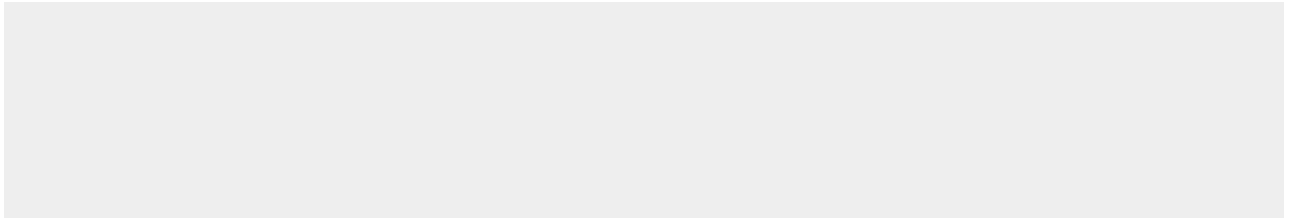
9. View the results.

To explore another dashboard drill-down example

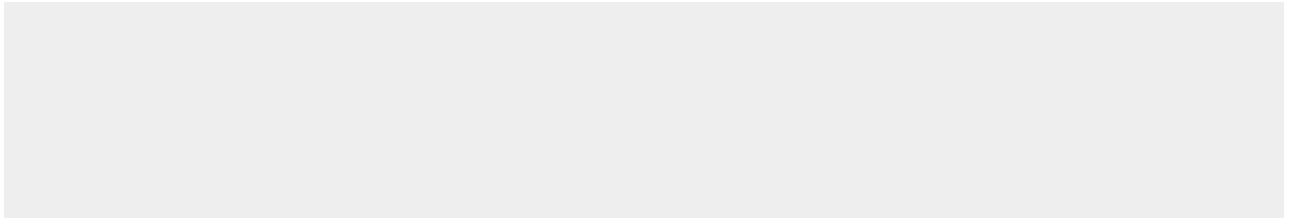
1. Continuing on the FortiSIEM GUI, click **DASHBOARD**.
2. Click **Lab9-Widget**.
3. In the **Firewall Permit: Top Outbound Ports By Bytes** widget, click the gears icon (⚙️), and then in the drop-down list, select **Drill Down To Analytics**.



What is the result of this action? See ["Appendix: Answer Sheet" on page 247](#) for the answer.



How does this differ from the analytic query produced in step 7 of the previous task? See "[Appendix: Answer Sheet](#)" on page 247 for the answer.



4. Log out of the FortiSIEM GUI.

Exercise 6: Importing and Exporting Dashboards

In this exercise, you will export and import dashboards.

Export a Dashboard

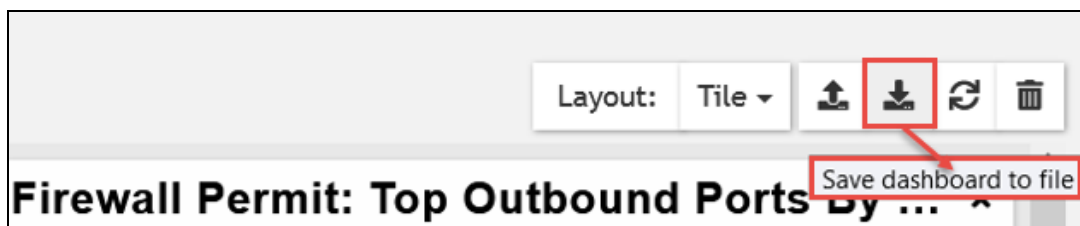
You will export a dashboard out of FortiSIEM.

To export a dashboard

1. Log in to the FortiSIEM GUI with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Domain	LOCAL

2. Click **DASHBOARD**.
3. Click **Lab9-Widget**.
4. In the upper-right of the main window, click the export icon.



5. When prompted, click **Save File**, and then click **OK**.
`Dashboard.xml` is exported to your download folder.

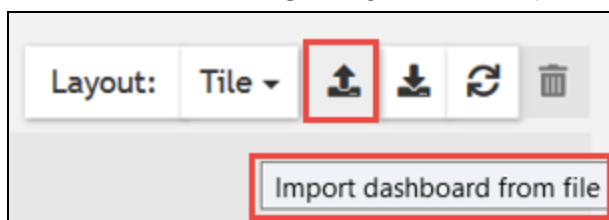
Import a Dashboard

You will import a dashboard into FortiSIEM.

To import a dashboard

1. Continuing on the FortiSIEM GUI, click **DASHBOARD**.
2. On the left, click the dashboard type drop-down list.
3. Click **New**.
The **Create Dashboard Folder** dialog appears.

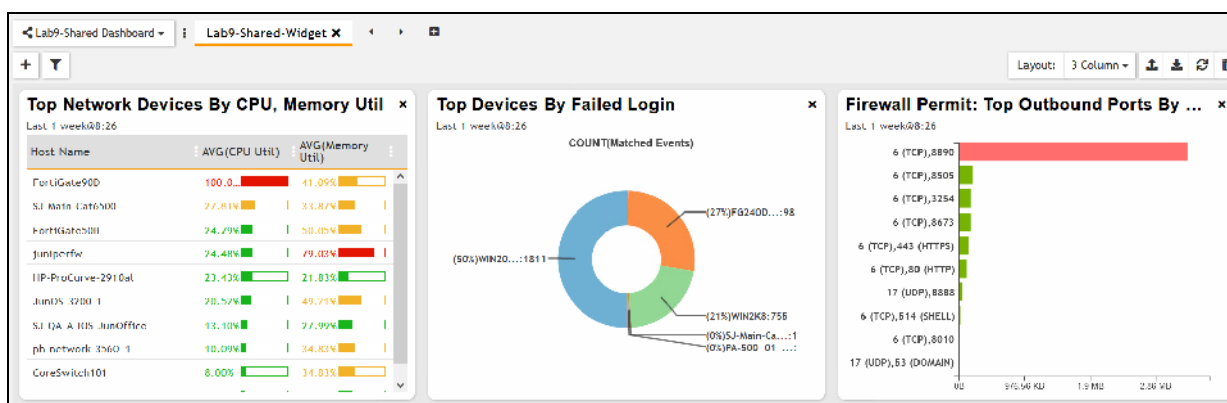
4. In the **Name** field, type `Lab9-Shared Dashboard`.
5. Enable **Share with**.
6. Click **Save**.
7. In the **LAB-9-Shared Dashboard** folder, click the plus icon to the right of the dashboard drop-down list.
8. In the **Name** field, type `Lab9-Shared-Widget`.
9. In the **Type** drop-down list, select **Widget Dashboard**.
10. Click **Save**.
11. In the **Lab9-Shared-Widget** widget, click the import icon.



The **Import Dashboard** dialog box opens.

12. Click **Browse**, and then navigate to the `Dashboard.xml` file you exported in the previous section.
13. Click **Import**.
14. After the import succeeds, click **OK**.
15. Refresh the widget.

The custom dashboard displays.



The imported widget dashboard may not display the CMDB report.

16. Log out of the FortiSIEM GUI.

Exercise 7: Running CMDB Reports

In this exercise, you will run existing CMDB reports.

Run a CMDB Report

You will run the built-in CMDB reports on FortiSIEM.

To run a CMDB report

1. Log in to the FortiSIEM GUI with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Domain	LOCAL

2. Click **CMDB**.
3. In the left pane, click **CMDB Reports**.
4. Find and select the **CIS 1.1,1.2,1.4,1.5: Discovered Network Device Inventory** report.
5. Click **Run**.

CMDB Report Results					
CIS 1.1,1.2,1.4,1.5: Discovered Network Device Inventory X					
Back Export		1/1 23			
Device Name	Device IP	Device Type Vendor	Device Type Model	Device Version	Device Hardware Model
AP d8:c7:c8:c6:b2:17	192.168.26.108	Aruba	ArubaOS WLAN AP	5.0.3.3	
AP d8:c7:c8:c6:b2:87	192.168.26.8	Aruba	ArubaOS WLAN AP	5.0.3.3	
Aruba3200	192.168.26.7	Aruba	ArubaOS WLAN Controller	5.0.3.3	
IAP320C-default	192.168.30.40	Fortinet	FortiAP	IAP320C-v5.0-build450	IAP320C
FG240D3913800441	192.168.3.1	Fortinet	FortiOS	FortiGate-240D v5.4.1,build1064b1064,1605 08 (GA)	FGT_240D
FortiGate50B	177.16.255.82	Fortinet	FortiOS	Fortigate-50B v4.00.1,build0279b279,1005 19	FGT_50B
FortiGate90D	10.1.1.1	Fortinet	FortiOS	Fortigate-90D v4.00.1,build0279b279,1005 19	

The report displays all the different vendors, models, versions, and counts in the CMDB.

6. Click **Back**.
7. Find and select the **Router/Switch Inventory** report.
8. Click **Run**.
9. Review the results, and then click **Back**.

10. Find and select the **Active Rules** report.

11. Click **Run**.

Note that other kinds of data, such as installed software, running applications, users, and device monitoring jobs can also be reported on using this feature.

12. Review the results, and then click **Back**.

13. Log out of the FortiSIEM GUI.

Exercise 8: Building a Custom CMDB Report

In this exercise, you will create a custom CMDB report.

Create a Custom CMDB Report

You will create a custom CMDB report that will report on rules with a remediation action.

To create a CMDB report

1. Log in to the FortiSIEM GUI with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Domain	LOCAL

2. Click **RESOURCES**.
3. In the left pane, click **Rules > Ungrouped**.
4. Find and select the **High Severity IPS Exploit Notification LAB** rule.
5. Click **Edit > Selected Rule**.

Note that there are some remediation steps for an operator to follow if this rule is triggered.

Event Type:	PH_RULE_High_Severity_IPS_Exploit_Notification_LAB
Remediation:	Deactivate this rule once finished with Incident Notification LAB.

6. Once you have reviewed the rule, click **Cancel**.
7. Click the **CMDB** tab, and then return to **CMDB Reports**.
8. Click the **Overall** folder.
9. Click **New**.
10. In the **Report Name** field, type `Rules with Remediation Instructions`.
11. In the **Target** drop-down list, select **RULE**.

New CMDB Report

Step 1: General > Step 2: Define Condition > Step 3: Define Display Column

Report Name: Rules with Remediation Instructions

Description:

Target: RULE

Save Cancel

12. Click **Step 2: Define Condition**.
13. Configure the following settings:

Field	Value
Attribute	Rule Remediation
Operator	IS NOT
Value	NULL

New CMDB Report

Step 1: General > Step 2: Define Condition > Step 3: Define Display Column

Paren	Attribute	Operator	Value	Paren	Next	Row
☐	Rule Remediation	IS NOT	NULL	☐	AND	☐

Save Cancel

14. Click **Step 3: Define Display Column**.
15. In the **Display Columns** section, add the following attributes:
 - Rule Name
 - Rule Description
 - Rule Remediation

New CMDB Report

Step 1: General > Step 2: Define Condition > Step 3: Define Display Column

Attribute	Order	Display As	Row	Move
Rule Name			☐	☐
Rule Description			☐	☐
Rule Remediation			☐	☐

Save Cancel

- 16. Click **Save**.
- 17. In the **CMDB Reports** folder, find and select the **Rules with Remediation Instructions** report.
- 18. Click **Run**.

The **Rules with Remediation Instructions** report is included in the report results.

CMDB Report Results		
CIS 1.1.1.2, 1.4.1.2: Discovered Network Device Inventory X Router/Switch Inventory X Active Rules X Rules with Remediation Instructions X		
Back Export		
1/1 15		
Rule Name	Rule Description	Rule Remediation
High Severity IPS Exploit Notification LAB	Detects a high severity IPS exploit detected by IPS	Deactivate this rule once finished with Incident Notification LAB.
Malicious PowerShell Tool: PSAttack Detected	A malicious powershell tool known as PSAttack has been detected being running on a Windows Host. This rule requires collection of the Windows PowerShell Event Log: Microsoft Windows PowerShell/Operational via the FortiSIFM Agent.	
Powershell Commandlet of Well Known Exploitation Framework Detected	Detects Commandlet names from well-known PowerShell exploitation frameworks, https://adsecurity.org/?p=2921 This rule requires collection of the Windows PowerShell Event Log: Microsoft Windows PowerShell/Operational via the FortiSIFM Agent.	



You can find custom CMDB reports by ordering the **Scope** field. Out-of-the-box reports are itemized as **System** and custom reports are itemized as **User**.

- 19. Log out of the FortiSIEM GUI.

Lab 10: Business Services

In this lab, you will create a business service.

Objectives

- Create a business service
- Monitor a business service
- Report on a business service

Time to Complete

Estimated: 40 minutes

Exercise 1: Creating a Business Service

In this exercise, you will create a new business service.

Create a Business Service

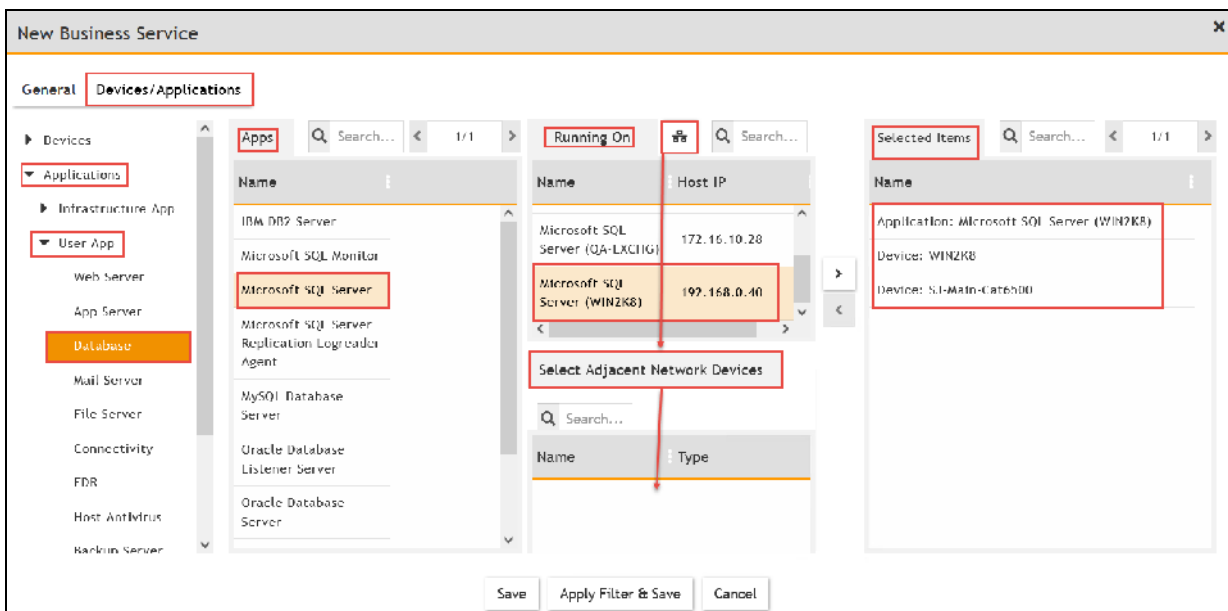
You will create a new business service for a patient services unit.

To create a business service

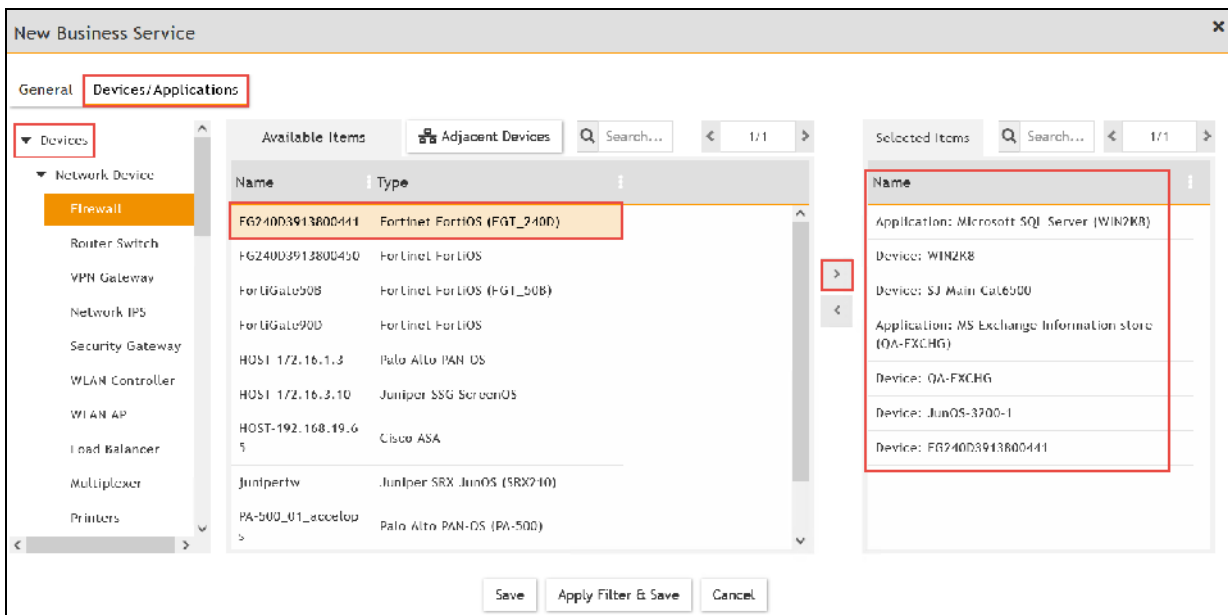
1. Log in to the FortiSIEM GUI with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Domain	LOCAL

2. Click **CMDB**.
3. In the left pane, expand **Business Services**.
4. Click the **Biz Srvc** folder.
5. In the main window, click **New**.
6. In the **Name** field, type `Patient Services`.
7. In the **New Business Service** window, click the **Devices/Applications** tab.
8. In the left pane, click **Applications > User App > Database**.
9. In the **Apps** pane, select **Microsoft SQL Server**.
10. In the **Running On** pane, select **Microsoft SQL Server (WIN2K8) 192.168.0.40**, and then click the **Adjacent Devices** icon beside **Running On**.
11. In the **Select Adjacent Network Devices** pane, select **SJ-Main-Cat6500**.
12. Click **>** to move the selections to the **Selected Items** pane.



13. In the left pane, click **Applications > User App > Mail Server**.
14. In the **Apps** pane, find and select **MS Exchange Information store**.
15. In the **Running On** pane, select the device with access IP **172.16.10.28**.
16. In the **Select Adjacent Network Devices** pane, select **JunOS-3200-1**.
17. Click > to move the selected device to the **Selected Items** pane.
18. In the left pane, click **Devices > Network Device > Firewall**.
19. In the **Available Items** pane, select **FG240D3913800441**.
20. Click > to move the selected device to the **Selected Items** pane.



21. Click **Save**.
22. To review the added devices, click the new **Patient Services** business service, and then on the bottom of the screen, click the up arrow to see the **Members** tab.

CMDB > Business Services > Biz Srvc

New Edit Delete Search...

1/1

Name	Members	Description
Patient Services	/	

Members ☐ Auto expand Search... 1/1

Type	Name	Running On	Access IP	Details	Maintenance
Application	MS Exchange Information store	QA EXCHG	172.16.10.28	store.exe ()	N/A
Application	Microsoft SQL Server	WIN2KR	192.168.0.10	sqlservr.exe ()	N/A
Device	FG240D3913800441		192.168.3.1	Fortinet FortiOS	
Device	SJ Main Cui6500		192.168.20.1	Cisco IOS	

23. Log out of the FortiSIEM GUI.

Exercise 2: Monitoring Business Service Incidents

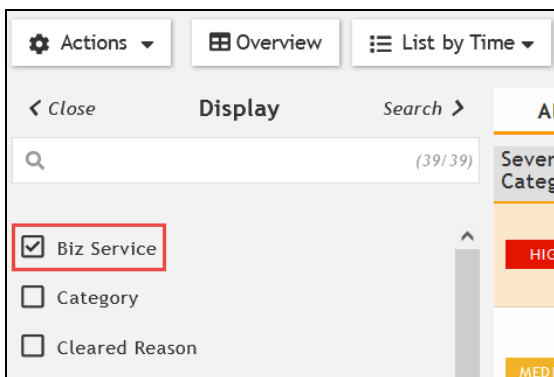
In this exercise, you will monitor business service incidents.

To monitor a business service

1. Log in to the FortiSIEM GUI with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Domain	LOCAL

2. Click the **INCIDENTS** tab.
3. Click **List**, and then select **by Time** to view the incident table.
4. In the main window, in the **Actions** drop-down list, select **Change Display Columns**.
5. Select **BizService**.
6. Click **Close** to close the left pane.



To modify a system rule for business services

1. Continuing on the FortiSIEM GUI, click **RESOURCES**.
2. In the left pane, click **Rules**.
3. In the search field, type `vulnerability`.
4. Select **(s)Scanner found severe vulnerability**.
5. Click **Edit > Selected Rule**.
6. Click **Step 2: Define Condition**.
7. In the **Conditions** section, beside **ScannerHighSev**, click the pencil icon.
8. In the **Group By** section, add a new row.
9. In the new attribute field, type `Host IP`.

Group By:

Attribute	Row	Move
Host Name	 	 
Host IP	 	 
Vulnerability Name	 	 

- Click **Save**.
- Click **Step 3: Define Action**.
- In the **Action: Defined** section, click the pencil icon to edit it.
- Under **Incident Attributes**, add a new row (at the bottom), and then configure the following values:

Field	Value
Event Attribute	Host IP
Subpattern	ScannerHighSev
Filter Attribute	Host IP

Generate Incident for: Scanner found severe vulnerability

Incident Attributes:

Event Attribute		Subpattern		Filter Attribute		Row
Host Name	=	ScannerHighSev	▼	Host Name	▼	 
Vulnerability Name	=	ScannerHighSev	▼	Vulnerability Name	▼	 
Host IP	=	ScannerHighSev	▼	Host IP	▼	 

- Click **Save**.
- Click **Save** again.
Because you changed a system rule, you must save the rule with a different name.
- Remove the date, and then type LAB10, as the following example shows:

The Rule has been Changed

You have made changes to a system rule -- a working copy will be created.
Please select a name for the new rule.

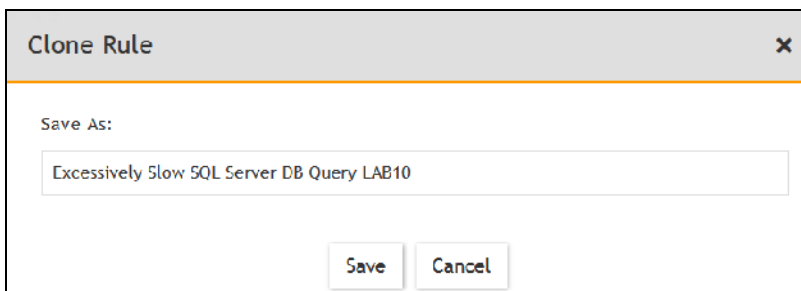
Scanner found severe vulnerability LAB10

OK Cancel

17. Click **OK**.
18. Under the **Active** column, clear the checkbox beside **(s)Scanner found severe vulnerability**.
19. Click **Continue**.
The original system rule is disabled.
20. Under the **Active** column, select the checkbox beside the modified rule you just created (**Scanner found severe vulnerability LAB10**).
21. Click **Continue** when prompted.
This enables and activates the cloned rule.

To modify a second system rule for business services

1. Continuing on the FortiSIEM GUI, in the search field, type `sql server db`.
2. Select the **Excessively Slow SQL Server DB Query** rule.
3. Click **Clone**.
4. Remove the date stamp, and then type `LAB10`.
5. Click **Save**.



The image shows a 'Clone Rule' dialog box with a title bar containing 'Clone Rule' and a close button. Inside the dialog, there is a 'Save As:' label above a text input field. The text input field contains the text 'Excessively Slow SQL Server DB Query LAB10'. At the bottom of the dialog, there are two buttons: 'Save' and 'Cancel'.

6. In the **Active** column, clear the **Original Excessively Slow SQL Server DB Query Rule** checkbox.
7. Click **Continue** when prompted.
8. Select the cloned rule, and then click **Edit > Selected Rule**.
9. Click **Step 2: Define Condition**.
10. In the **Conditions** field, beside the **LongQuery** subpattern, click the pencil icon.
11. In the **Group By** section, add a new row under **Host Name**.
12. In the **Attribute** field, type `Host IP`.



The image shows a 'Group By' table with the following structure:

Attribute	Row	Move
Host Name	+ -	↑ ↓
Host IP	+ -	↑ ↓
DB Name	+ -	↑ ↓
DB Instance Name	+ -	↑ ↓
Command	+ -	↑ ↓

13. Click **Save**.
14. Click **Step 3: Define Action**.

15. In the **Action: Defined** section, click the pencil icon to edit it.
16. In the **Incident Attributes** section, add a new row under **Host Name**.
17. Configure the following settings:

Field	Value
Event Attribute	Host IP
Subpattern	LongQuery
Filter Attribute	Host IP

Generate Incident for: Excessively Slow SQL Server DB Query LAB10

Incident Attributes:

Event Attribute	Subpattern	Filter Attribute	Row
Host Name	= LongQuery	Host Name	+
Host IP	= LongQuery	Host IP	+
DB Name	= LongQuery	DB Name	+
DB Instance Name	= LongQuery	DB Instance Name	+
Command	= LongQuery	Command	+
DB Query Response Time sec	= LongQuery	AVG(DB Query Response)	+

18. Click **Save**.
19. Click **Save**.
20. If you see a warning that the rule has been changed, click **OK** again.
21. In the **Active** column, select the checkbox beside the cloned version of the rule.
22. Click **Continue** when prompted.

Resources > Rules

New
Edit
Delete
Clone
Test
sql server db
Import
Export

Active	Severity	Name	Description	Tactics	Technique	Scope
☒	7 - MEDIUM	Excessively Slow SQL Server DB Query LAB10	Detects that an SQL Server query took more than 5 minute to complete			User
☐	7 - MEDIUM	(s) Excessively Slow SQL Server DB Query	Detects that an SQL Server query took more than 5 minute to complete			System

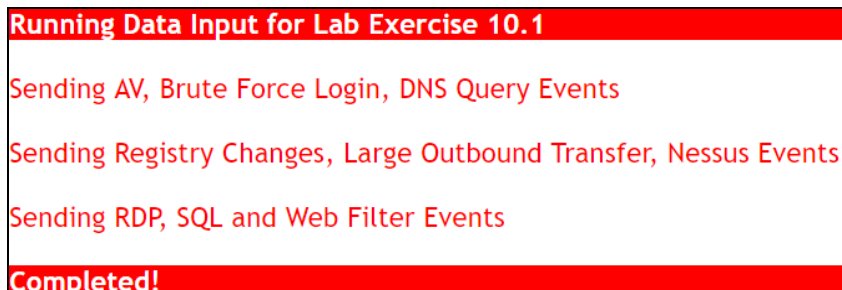
Generate Business Service Related Incidents

You will generate scripted events that will trigger business service related incidents on FortiSIEM.

To trigger business service related incidents

1. On the Linux-Client VM, open a new browser, and then navigate to the NSE Institute website.
2. Under **LABS SET 2** and **Lab 10 – Business Services**, select **Exercise 10.1 – Trigger Business Service Related Incidents**.

Wait for approximately two minutes. The output should resemble the following example:



3. Close the Linux-Client VM browser tab.

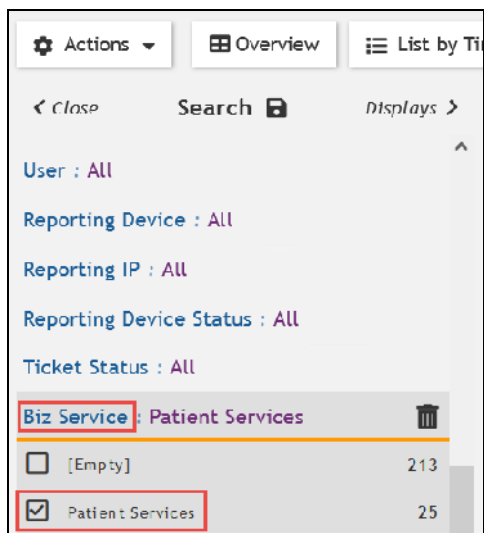
Examine Business Service Incidents

You will examine the business service incidents on FortiSIEM.

To review business service incidents

1. Return to the FortiSIEM GUI, and then click the **INCIDENTS** tab.
In the **BizService** column, incidents with the **Patient Services** name appear.
2. In the main window, in the **Actions** drop-down list, select **Search**.
The **Search** pane opens.
3. In the **Search** pane, click **BizService**.
4. In the drop-down list, select **Patient Services**.

The selection should look like the following example:



5. Click **Close**.
6. Review a few of the incidents.

What service was stopped? See "[Appendix: Answer Sheet](#)" on page 248 for the answer.

Which devices had a severe vulnerability detected? See "[Appendix: Answer Sheet](#)" on page 248 for the answer.

7. Log out of the FortiSIEM GUI.

Exercise 3: Using the Business Services Dashboard

In this exercise, you will create and view business services using dashboards and searches on FortiSIEM.

Create a Business Services Dashboard

You will create a dashboard group, and then add a business services dashboard to it.

To create a business services dashboard group

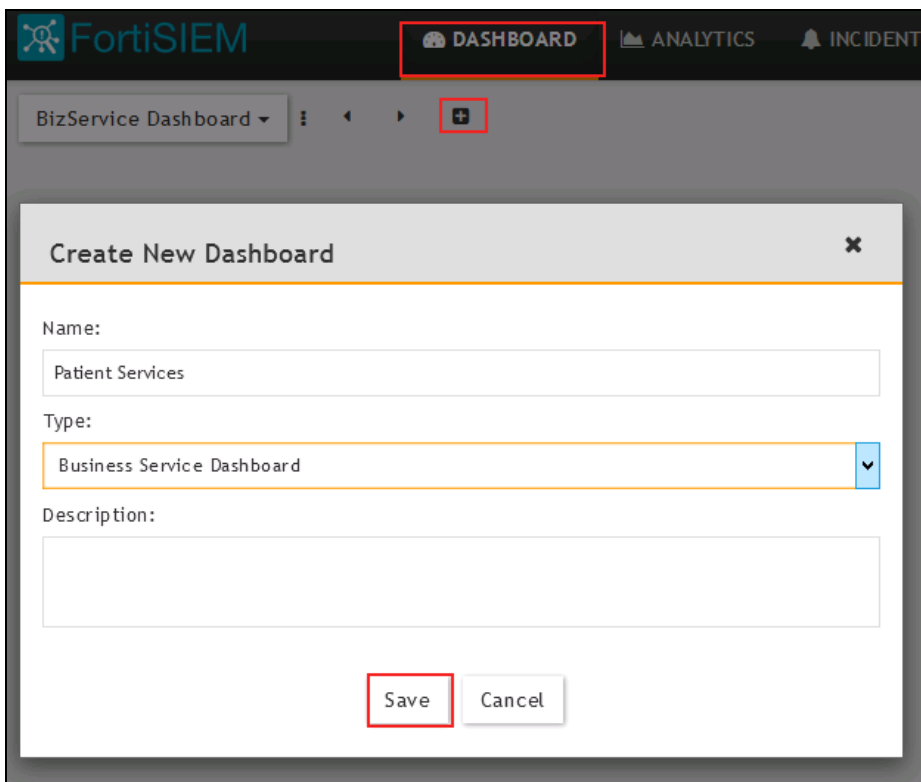
1. Log in to the FortiSIEM GUI with the following credentials:

Field	Value
User ID	admin
Password	Fortinet1!
Domain	LOCAL

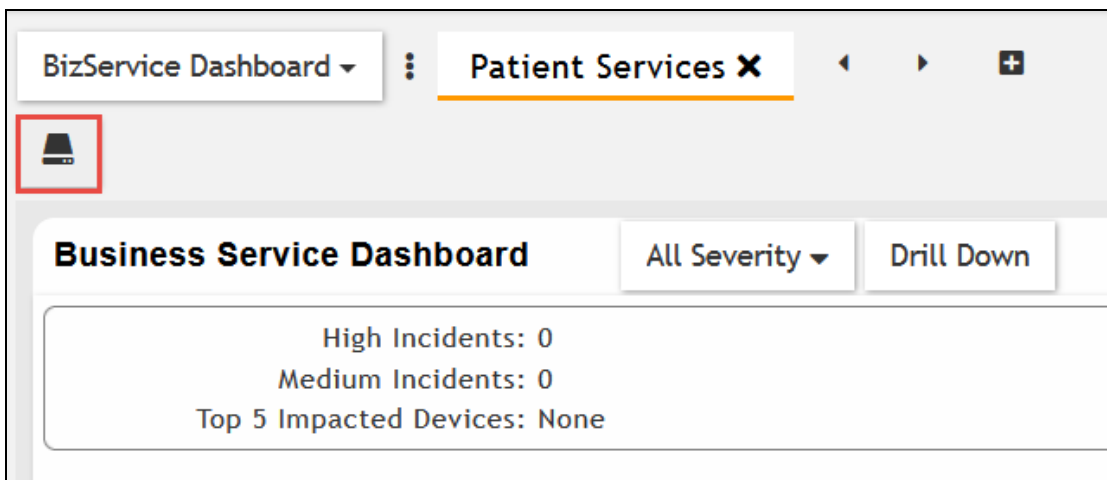
2. Click **DASHBOARD**.
3. On the left side of the window, click the drop-down list.
4. Click **New**.
5. In the **Name** field, type `BizService Dashboard`.
6. Click **Save**.

To create a business services dashboard

1. Continuing on the FortiSIEM GUI, to the right of the dashboard drop-down list, click the plus icon (+).
2. In the **Name** field, type `Patient Services`.
3. In the **Type** drop-down list, select **Business Service Dashboard**.
4. Click **Save**.



5. Under the dashboard selector drop-down list, click the **Select Business Services** icon.
The **Select Business Services** window opens.



6. In the **Available Services** pane, select **Patient Services**, and then click **>** to move **Patient Services** to the **Selected Services** pane.

Select Business Services

Available Services: patient

Selected Services: Patient Services

>

<

Save Cancel

7. Click **Save**.

The summary dashboard for **Patient Services** should match the following example:

BizService Dashboard ▾ Patient Services ✕

Business Service Dashboard All Severity ▾ Drill Down

High Incidents: 16
Medium Incidents: 10
Top 5 Impacted Devices: FG240D3913800441 (93); WIN2K8 (10); QA-EXCHG (4); SJ-Main-Cat6500 (3)

Patient Services

16	10
High	Medium

View the Business Services Dashboard Details

You will examine the business services dashboard details.

To view the business services dashboard details

1. Continuing on the FortiSIEM GUI, on the summary dashboard, select **Patient Services**.

The **Impacted Devices** pane opens at the bottom of the window to display the list of impacted devices.

The screenshot shows the Business Service Dashboard. At the top, there's a 'Patient Services' section with two cards: 'High' with 16 items and 'Medium' with 11 items. Below this is the 'Impacted Devices In Patient Services (Super)' section. It features a search bar and a table with columns: Device, Type, Availability, and Incidents. The table lists two devices: 'SJJ-Main-Cat6500' (Cisco IOS) and 'WIN2K8' (Microsoft Windows Server 2008). The 'WIN2K8' device has a green dot in the Availability column and a list of incidents in the Incidents column.

Device	Type	Availability	Incidents
SJJ-Main-Cat6500	Cisco IOS	●	MEDIUM : No logs from a device MEDIUM : No logs from a device MEDIUM : Running Config Change
WIN2K8	Microsoft Windows Server 2008	●	HIGH : Auto Service Stopped HIGH : Remote Desktop from Internet HIGH : Scanner found severe vulnerability LAB10 HIGH : Server Disk Space Critical MEDIUM : Excessively Slow SQL Server DB Query LAB10 MEDIUM : Suspicious Logon Failure: no following successful login MEDIUM (3) : Agent FIM: Windows File or Directory Created

2. In the **Impacted Devices** section, click **WIN2K8**.
3. Click the **Incidents** column.

The **Incidents for WIN2K8** window opens.

The screenshot shows the 'Incidents for WIN2K8' window. It has a filter bar at the top set to 'Incidents with severity MEDIUM, HIGH'. Below is a table with columns: Severity Category, Last Occurred, Incident, Tactics, Technique, Reporting, Source, and Target. The table lists four incidents. The third incident, 'Excessively Slow SQL Serve...', is highlighted in yellow and has 'WIN2K8' as the target.

Severity Category	Last Occurred	Incident	Tactics	Technique	Reporting	Source	Target
HIGH	Oct 05 2021, 09:58:00 AM	Scanner found severe vuln...	Impact	Endpoint Denial o...	HOST-10.10.100.80		192.168.0.41
HIGH	Oct 05 2021, 09:58:00 AM	Remote Desktop from Inter...	Persistence, Later...	Remote Services: ...	FG240D39138D0441	221.229.172.66	192.168.0.41
MEDIUM	Oct 05 2021, 09:58:00 AM	Excessively Slow SQL Serve...			WIN2K8		WIN2K8 192.168.0.41
HIGH	Oct 05 2021, 09:57:30 AM	Auto Service Stopped	Impact	Service Stop	WIN2K8		192.168.0.41 WIN2K8

Can you identify the SQL query that was running slow? See "[Appendix: Answer Sheet](#)" on page 248 for the answer.

4. Close the **Incidents for WIN2K8** window.

Reference Business Services in an Analytics Search

You will create analytics search filtering criteria that references a business service.

To reference business services in an analytics search

1. Continuing on the FortiSIEM GUI, click **ANALYTICS**.
2. Close all additional search tabs and clear any previous search filters.
3. Click the search field to edit the condition.

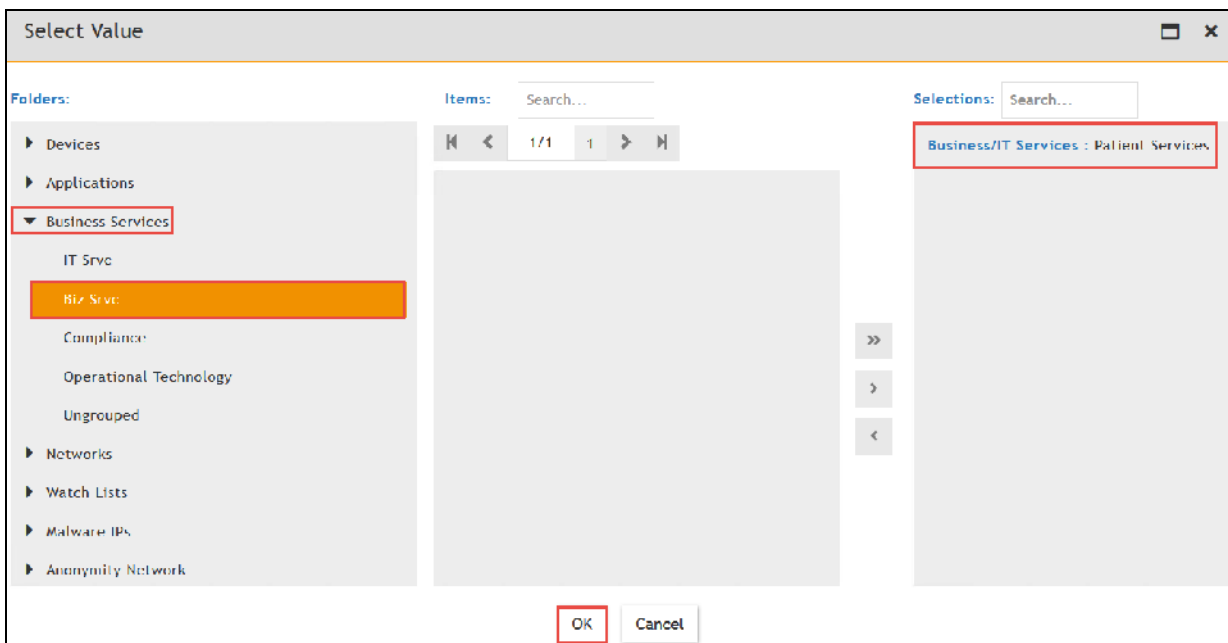


If an existing search is present, clear the search condition and revert any display columns to the default view.

4. In the **Filters** editor, select **Event Attribute**.
5. Configure the following values:

Field	Value
Attribute	Reporting IP
Operator	IN

6. Click the **Value** field, and then in the drop-down list, select **Select from CMDB**.
7. Click **Business Services > Biz Srvc**, and then select **Patient Services**.
8. Click **>** to move **Patient Services** to the **Selections** section.



9. Click **OK**.
10. Add a new row, and then configure the following values:

Field	Value
Attribute	Event Type
Operator	CONTAIN
Value	FileMon

11. In the **Time** section, select **Relative**, in the **Last** field, type 1, and then in the drop-down list, select **Hour**.
12. Click **Apply & Run**.

Filter Load Save Clear All

☐ Event Keyword

☒ Event Attribute

Paren	Attribute	Operator	Value	Paren	Next	Row
+	Reporting IP	IN	Business/IT Services: Patient Servi	+	AND	+
+	Event type	CONTAIN	FileMon	+	AND	+

☐ CMDB Attribute

Time Range

☐ Real-time ☒ Relative Last 1 1 hour

☐ Absolute

Trend Interval: Auto

Apply & Run Apply Cancel

This drills down into the Windows agent events being collected.



If you do not get any results for any search, run the search over a longer time period.

Can you identify the files that were added on the **QA-EXCHG** or **WIN2K8** machines? See "[Appendix: Answer Sheet](#)" on page 248 for the answer.

13. Log out of the FortiSIEM GUI.

Lab 11: Troubleshooting

In this lab, you will troubleshoot the discovery of a FortiGate, view the health status of back-end FortiSIEM processes, and troubleshoot privileged credentials used for configuration pulling.

Objectives

- Troubleshoot the device discovery process
- View the health of back-end FortiSIEM processes
- Troubleshoot privileged credentials used for configuration pulling

Time to Complete

Estimated: 55 minutes

Exercise 1: Troubleshooting Device Discovery

In this exercise, you will troubleshoot the discovery of a FortiGate that is configured as the gateway router for the lab environment.

Configure SNMP on FortiGate

You will configure SNMP on FortiGate. You will enable SNMP events that are critical for FortiSIEM to monitor.

To configure SNMP on FortiGate

1. Log in to the FortiGate GUI with the username `admin` and password `password`.
2. Click **System > SNMP**.
3. Enable **SNMP Agent**.
4. Configure the following settings:

Field	Value
Description	FGT_LAB_Router
Location	Ottawa

5. In the **SNMP v1/v2c** section, click **Create New**.
6. Configure the following settings:

Field	Value
Community Name	public
Enabled	enable
IP Address	0.0.0.0/0
Host Type	Accept queries and send traps

7. Scroll down to the **SNMP Events** section, and then make sure the following traps are enabled:

Field	Value
Configuration change (FM trap)	enable
A new device is found	enable

Leave all other traps at the default settings.

8. Click **OK**.
9. Click **Apply**.

Add Credentials for FortiGate

You will add the FortiGate credentials on FortiSIEM. Using these credentials, FortiSIEM can discover the FortiGate VM.

To add credentials for the FortiGate VM

1. Log in to the FortiSIEM GUI with the following credentials:

Field	Value
User	admin
Password	Fortinet1!
Domain	LOCAL

2. Click **ADMIN**.
3. In the left navigation pane, click **Setup**, and then click **Credentials**.
4. In the **Step 1: Enter Credentials** section, click **New**.
5. Configure the following settings:

Field	Value
Name	FGT_LAB_Router_SNMP
Device Type	Generic
Access Protocol	SNMP
Port	161
Password config	Manual
Community String	public
Confirm Community String	public

6. Click **Save**.
7. In the **Step 2: Enter IP Range to Credential Associations** section, click **New**.
8. Configure the following settings:

Field	Value
IP/IP Range	10.0.1.254
Credential	FGT_LAB_Router_SNMP

9. Click **Save**.

Discover FortiGate

You will discover the FortiGate.

To view live discovery logs

1. Open an SSH session to the FortiSIEM VM.:
2. Enter the following command:

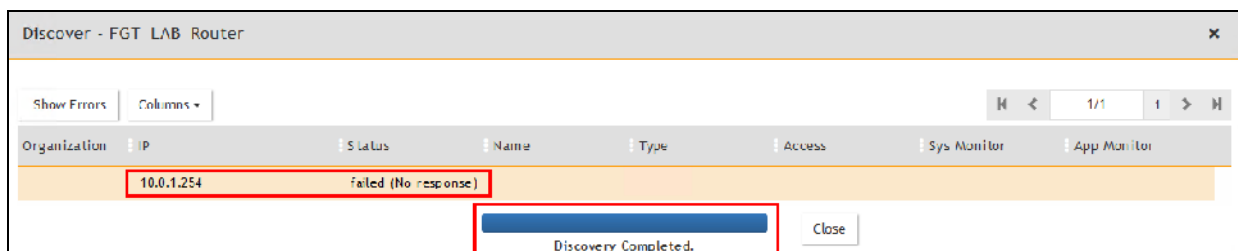
```
tail -f /opt/phoenix/log/phoenix.log | grep -i 10.0.1.254
```
3. Leave the SSH session browser tab open.

To discover the FortiGate VM

1. Return to the FortiSIEM GUI, and then on the **Setup** page, click **Discovery**.
2. Click **New**.
3. Configure the following settings:

Field	Value
Name	FGT_LAB_Router
Discovery Type	Range Scan
Include	10.0.1.254
Name Resolution	SNMP/WMI first

4. Click **Save**.
5. Select the **FGT_LAB_Router** entry, click **Discover**, and then wait for the discovery to complete.



The discovery fails.

6. Click **Close**.
7. Return to the FortiSIEM SSH session, and then view the logs related to device discovery.

```
[root@FSM NSE5 ~]# tail -f /opt/phoenix/log/phoenix.log | grep -i 10.0.1.254
2021-12-09T16:48:58.884921-05:00 FSM NSE5 phDiscover[4285]: [PH DISCOV FILE BASED DISCOV FAILED]:[eventSeverity]=PHL ERROR,[procName]=phDiscover,[fileName]=discover.cpp,[lineNumber]=5038,[hostIpAddr]=10.0.1.254,[filePath]=/opt/phoenix/config/discoverFile/10.0.1.254-snmp.txt,[phLogDetail]=Cannot open file used for file based discovery
2021-12-09T16:48:58.885077-05:00 FSM NSE5 phDiscover[4285]: [PH DISCOV BASIC FAILED]:[eventSeverity]=PHL ERROR,[procName]=phDiscover,[fileName]=discover.cpp,[lineNumber]=5000,[destIpAddr]=10.0.1.254,[phDiscoverFailCode]=No response,[phLogDetail]=Basic device discovery completely failed for 10.0.1.254: reason: No response
```

FortiSIEM is configured to discover from a file instead of network discovery. You made this change as a preparation step in [Discovery on page 41](#).

Configure FortiSIEM for Network Discovery

You will configure FortiSIEM for network discovery.

To enable FortiSIEM for network discovery

1. Return to the FortiSIEM SSH session, and then press **Ctrl+C**.
2. Enter the following command:

```
phstatus
```

All FortiSIEM process statuses are displayed.
3. Make a note of the uptime of the `phDiscover` process.
4. On the Linux-Client VM, open a browser, and then go to the NSE Institute website at https://10.0.1.130/NSE_Institute/index.php.
5. Click **LABS SET 2**, and then under **Lab 11—Troubleshooting**, click **Exercise 11.1—Prepare System for Network Discovery**.



The script changes the configuration of FortiSIEM to discover from the network instead of a file. The script also restarts the `phDiscover` process.

6. Return to the FortiSIEM SSH session, and then observe the output of the `phstatus` command.

```
Every 1.0s: /opt/phoenix/bin/phstatus.py

System uptime: 16:57:25 up 2 days, 17:38, 1 user, load average: 2.20, 2.23, 2.03
Tasks: 28 total, 0 running, 27 sleeping, 1 stopped, 0 zombie
Cpu(s): 8 cores, 7.9%us, 1.2%sy, 0.0%ni, 89.3%id, 0.0%wa, 1.4%hi, 0.1%si, 0.0%st
Mem: 24468876k total, 14227972k used, 433208k free, 10452k buffers
Swap: 26058744k total, 16480k used, 26042264k free, 10634844k cached

PROCESS                UPTIME                CPU%                VIRT_MEM            RES_MEM
phParser                2-17:08:36            0                    2443m                1616m
phQueryMaster           2-17:08:00            0                    1114m                138m
phRuleMaster            2-17:08:00            0                    1588m                892m
phRuleWorker            2-17:08:00            0                    1693m                784m
phQueryWorker           2-17:08:00            0                    1459m                603m
phDataManager           2-17:08:00            0                    3511m                2326m
phDiscover              2-17:08:00            0                    1499m                657m
phReportWorker          2-17:08:00            0                    750m                 88m
phReportMaster          2-17:08:00            0                    1044m                574m
phIpIdentityWorker      2-17:08:00            0                    518m                 47m
phIpIdentityMaster      2-17:08:39            0                    1526m                78m
phAgentManager          2-17:08:00            0                    322m                 58m
phCheckpoint            2-17:08:39            0
```

The `phDiscover` restarts. Compare the current uptime of the process with the one you made a note of earlier.

- Return to the Linux-Client VM, and then in the browser connected to the NSE Institute website, observe the script execution status message.

The output should resemble the following example:

Lab 11 - Troubleshooting

Exercise 11.1 - Prepare System for Network Discovery (page return time, up to 2 minutes)

Preparing System for Network Discovery - Lab Exercise 11.1

This will take around 50 seconds to complete.

Waiting 45 seconds for Discovery Process to Restart

```
admin 3164626 1 1 16:57 ? 00:00:00 /opt/phoenix/bin/phDiscover
Discovery Process Restarted OK
```

Completed!

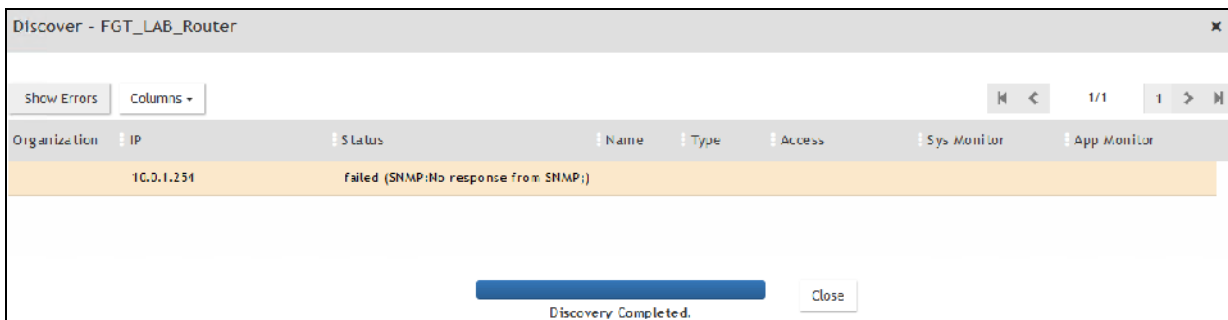
Troubleshoot the Discovery of a FortiGate

You will further troubleshoot the discovery of the FortiGate using the `snmpwalk` command.

To troubleshoot the discovery process

1. Return to the FortiSIEM SSH session, and then press **Ctrl+C**.
2. Enter the following command:

```
tail -f /opt/phoenix/log/phoenix.log | grep -i 10.0.1.254
```
3. Return to the FortiSIEM GUI, and then click **ADMIN**.
4. In the left navigation pane, click **Setup**, and then click **Discovery**.
5. Select **FGT_LAB_Router**, and then click **Discover**.



The discovery of the FortiGate VM fails again.

6. Click **Close**.
7. Return to the FortiSIEM SSH session, and then review the logs.

```
[root@FSM_NSE5 ~]# tail -f /opt/phoenix/log/phoenix.log | grep -i 10.0.1.254
2021-11-04T18:28:42.641525-04:00 FSM_NSE5 phDiscover[3164626]: [PH_DISCOV_BASIC
FAILED]:[eventSeverity]=PHL_ERROR,[procName]=phDiscover,[fileName]=discover.cpp,
[lineNumber]=5909,[destIpAddr]=10.0.1.254,[phDiscovFailCode]=SNMP:No response fr
om SNMP;,[phLogDetail]=Basic device discovery completely failed for 10.0.1.254:
reason: SNMP:No response from SNMP;
```

8. Make a note of the message `Basic device discovery completely failed for 10.0.1.254: reason: SNMP:No response from SNMP`.
9. Press **Ctrl+C** to exit out of the `tail` command output.
10. Enter the following command:

```
snmpwalk -c public -v 2c 10.0.1.254
```

```
[root@FSM_NSE5 ~]# snmpwalk -c public -v 2c 10.0.1.254
Timeout: No Response from 10.0.1.254
```

The `snmpwalk` command fails with the message `Timeout: No Response from 10.0.1.254`. You must review the FortiGate SNMP configuration.



If you configured SNMP as the discovery credential on FortiSIEM, and discovery is failing, you should use the `snmpwalk` command on the FortiSIEM CLI to troubleshoot the issue.

```
snmpwalk -c <community> -v <version> <ip address>
```

If `snmpwalk` fails from the CLI, discovery will not work on the FortiSIEM GUI.

To enable the SNMP service on a FortiGate interface

1. Return to the FortiGate GUI, and then click **Network > Interfaces**.
2. Select **LAN1 (port3)**, and then click **Edit**.
3. In the **Administrative Access** section, select the **SNMP** checkbox.

The screenshot shows the FortiGate GUI configuration for the LAN1 (port3) interface. The 'Administrative Access' section is highlighted with a red box. Within this section, the 'SNMP' checkbox is checked and also highlighted with a red box. Other visible options include HTTPS, HTTP, SSH, PING, FMG-Access, FTM, RADIUS Accounting, and Security Fabric Connection.

4. Click **OK**.
5. Log out of the FortiGate GUI.

Verify the Fix

You will use the `snmpwalk` command to verify the fix.

To verify the fix

1. Return to the FortiSIEM SSH session, and then enter the `snmpwalk` command again:

```
snmpwalk -c public -v 2c 10.0.1.254
```

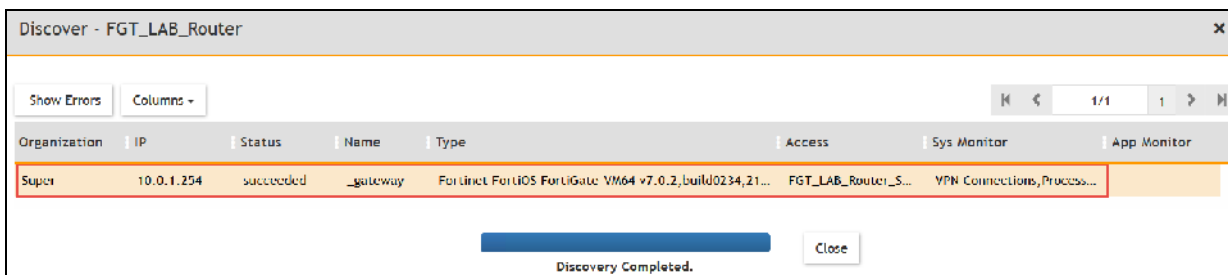
```
SNMPEv2-SMI::mib-2.47.1.1.1.1.1.1.4 = ""
SNMPEv2-SMI::mib-2.47.1.2.1.1.2.1 = STRING: "Fortinet Firewall FortiGate VM64 v7.0.2,build0234,211019 (CA)"
SNMPEv2-SMI::mib-2.47.1.2.1.1.3.1 = OID: SNMPEv2-SMI::enterprises.12356
SNMPEv2-SMI::mib-2.47.1.2.1.1.4.1 = STRING: "public"
SNMPEv2-SMI::mib-2.47.1.2.1.1.5.1 = STRING: "10.0.1.254:161"
SNMPEv2-SMI::mib-2.47.1.2.1.1.6.1 = OID: SNMPEv2-TM::snmpUDPDomain
SNMPEv2-SMI::mib-2.47.1.2.1.1.7.1 = ""
```

This time, the `snmpwalk` command reports a success message.

2. Enter the following command:

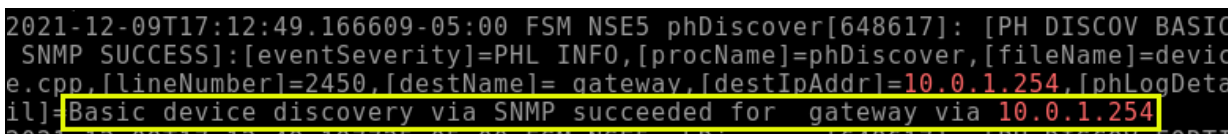
```
tail -f /opt/phoenix/log/phoenix.log | grep -i 10.0.1.254
```
3. Return to the FortiSIEM GUI, and then click **ADMIN**.
4. In the left navigation pane, click **Setup**, and then click **Discovery**.

5. Select **FGT_LAB_Router**, and then click **Discover**.



The discovery for **FGT_LAB_Router** succeeded.

6. Return to the FortiSIEM SSH session, and then observe the logs.



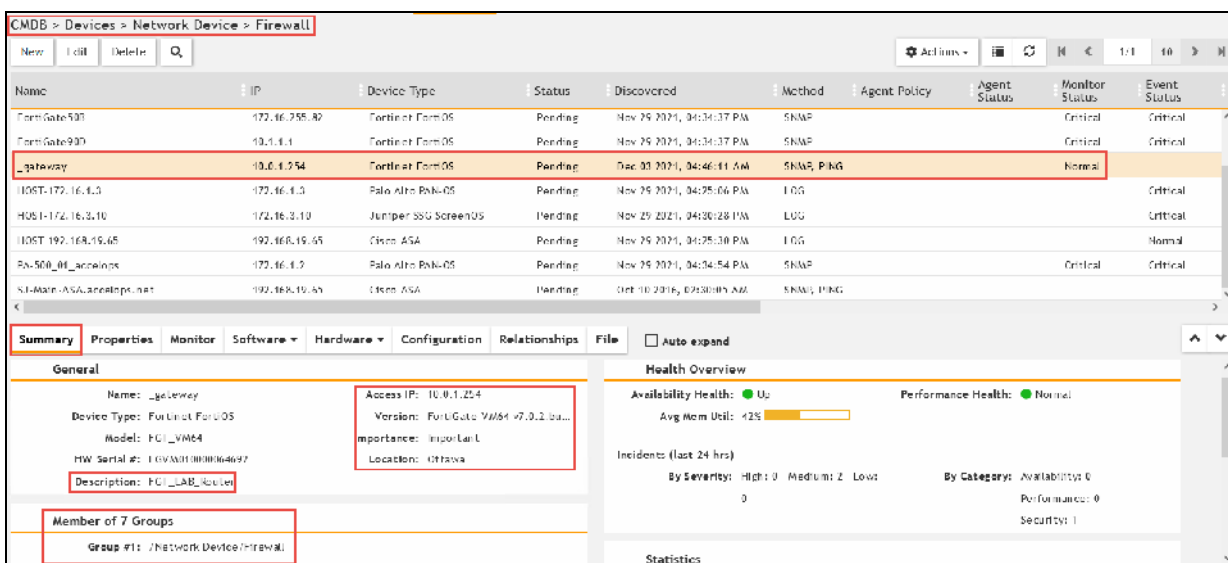
The logs also confirm that the discovery succeeded.

7. Press **Ctrl+C** to exit the **tail** command output.
8. Close the Linux-Client VM browser tab.

To view the FortiGate in the CMDB

1. Return to the FortiSIEM GUI, and then click **CMDB**.
2. In the pane on the left, click **Devices > Network Device > Firewall**.
3. In the main window, click the refresh icon (🔄).
4. Select the Fortinet device named **_gateway**, and then in the lower pane, click the **Summary** tab.

The output should be similar to the following example:



5. Continuing on the lower pane, click the **Configuration** tab.

The **Configuration** tab is empty. You must configure privileged credentials to retrieve the FortiGate VM configuration.

6. Log out of the FortiSIEM GUI.

Exercise 2: Troubleshooting Privileged Credentials for Configuration Pulling

In this exercise, you will examine the configuration pulling functionality, and then if you cannot retrieve the configuration from the device, you will troubleshoot the problem.

Configure Privileged Credentials

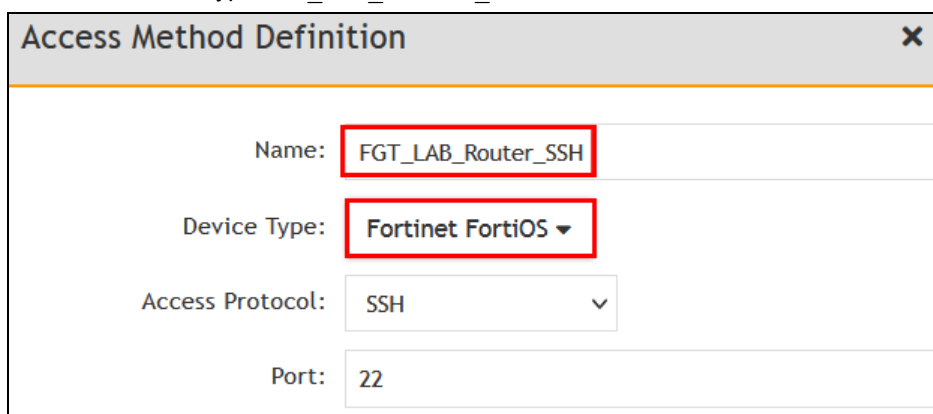
You will configure privileged SSH credentials to retrieve the configuration from FortiGate.

To configure privileged credentials

1. Log in to the FortiSIEM GUI with the following credentials:

Field	Value
User	admin
Password	Fortinet1!
Domain	LOCAL

2. Click **Admin**.
3. In the left navigation pane, click **Setup**.
4. In the main window, select the **Credentials** tab.
5. Under **Step 1: Enter Credentials**, select **FortiGate SSH**, and then click **Edit**.
6. Review the settings.
Notice the **Device Type** value.
7. In the **Name** field, type `FGT_LAB_Router_SSH`.



Access Method Definition

Name: FGT_LAB_Router_SSH

Device Type: Fortinet FortiOS

Access Protocol: SSH

Port: 22

8. Click **Save**.
9. Under **Step 2: Enter IP Range to Credential Associations**, select the **10.0.1.254** entry, and then click **Edit**.

The **Device Credential Mapping Definition** dialog opens.

10. Click the **+** icon near the bottom of the dialog box, and then in the drop-down list, select **FGT_LAB_Router_SSH**.

Device Credential Mapping Definition

IP/Host Name:

10.0.1.254

Credentials:

FGT_LAB_Router_SSNMP

FGT_LAB_ROUTER_SSH

+

Save

Cancel

11. Click **Save**.

Troubleshoot Pull Data Using Privileged Credentials

You will troubleshoot the privileged SSH credentials for configuration pulling.

To pull data using privileged credentials

1. Open an SSH session to the FortiSIEM VM with the username `root` and password `Fortinet1!`, and then enter the following command:

```
tail -f /opt/phoenix/log/phoenix.log | grep -i 10.0.1.254
```
 2. Return to the FortiSIEM GUI, and then click **ADMIN**.
 3. In the left navigation pane, click **Setup**, and then click **Discovery**.
 4. Select **FGT_LAB_Router**, and then click **Discover**.
- The basic SNMP discovery of the device succeeds.

Discover - FGT LAB Router

Show Errors

Columns -

1/1

1

Organization	IP	Status	Name	Type	Access	Sys Monitor	App Monitor
Super	10.0.1.254	succeeded	_gateway	Fortinet FortiOS FortiGate-VMS4 v7.0.2, build 0234, 211619 (CA)	FGT_LAB_Router_SSNMP(S...	VPN Connections, Processo...	

Discovery Completed.

Close

5. Click **Close**, and then click the **CMDB** tab.
6. In the left navigation pane, click **Devices > Network Device > Firewall**.
7. In the main window, click the refresh icon (↻).
8. Select the Fortinet FortiOS device named **_gateway**.
9. Observe the **Method** column.
It displays **SNMP** and **PING** only.

CMDB > Devices > Network Device > Firewall						
NewEditDeleteQ						
Name	IP	Device Type	Status	Discovered	Method	
FG240D3513800441	192.168.3.1	Fortinet FortOS	Pending	Nov 29 2021, 04:30:44 PM	SNMP	
FG240D3513800450	192.168.3.2	Fortinet FortOS	Pending	Nov 29 2021, 04:24:51 PM	LOG	
FortiGate50B	172.16.255.82	Fortinet FortOS	Pending	Nov 29 2021, 04:34:37 PM	SNMP	
FortiGate90D	10.1.1.1	Fortinet FortOS	Pending	Nov 29 2021, 04:34:37 PM	SNMP	
_gateway	10.0.1.254	Fortinet FortOS	Pending	Dec 03 2021, 06:17:25 AM	SNMP, PING	
HOST-172.16.1.3	172.16.1.3	Palo Alto PAN-OS	Pending	Nov 29 2021, 04:25:06 PM	LOG	
HOST-172.16.3.10	172.16.3.10	Juniper SSG ScreenOS	Pending	Nov 29 2021, 04:30:28 PM	LOG	

Although discovery is successful, the CMDB does not show SSH in the **Method** column.

10. Return to the FortiSIEM SSH session, and then press Ctrl+C to exit out of the tail command output.
11. Review the logs.

```
2021-11-04T20:47:06.850681-04:00 FSM_NSE5 phDiscover[3164626]: [PH_DISCOV NEXT_HOP_VIA_SNMP_FAILED]:[eventSeverity], [hostName]=FGVM010000064692, [hostIpAddr]=10.0.1.254, [phLogDetail]=Failed to discover next hop address vis SNMP
2021-11-04T20:47:06.850741-04:00 FSM_NSE5 phDiscover[3164626]: [PH_DISCOV_BASIC_SNMP_SUCCESS]:[eventSeverity]=PE, [hostName]=FGVM010000064692, [destIpAddr]=10.0.1.254, [phLogDetail]=Basic device discovery via SNMP succeeded for FGVM01
2021-11-04T20:48:07.052907-04:00 FSM_NSE5 phDiscover[3164626]: [PH_DISCOV_SSH_ERROR]:[eventSeverity]=PHL_ERROR, [hostName]=FGVM010000064692, [phLogDetail]=SSH discovery failed for FGVM01, [phDiscoverFailCode]=incorrect_user_name / password, [script]=/opt/phoenix/bin/getCmdOutViaSSH_Fortinet.exe failed
```

The logs indicate problems with the SSH credentials.

12. After you have reviewed the logs, enter the following command to restart the performance monitor process:
killall -9 phPerfMonitor
13. Enter the following command to check the status of the processes:
phstatus

```
Every 1.0s: /opt/phoenix/bin/phstatus.py                               FSM_NSE5.local: Fri Dec  3 09:28:03 2021

System uptime: 09:20:04 up 3 days, 14:00,  2 users,  load average: 3.30, 2.09, 2.64
Tasks: 28 total,  1 running, 26 sleeping,  1 stopped,  0 zombie
Cpu(s):  3.3%us,  8.3%sy,  1.0%st,  0.0%ni, 88.8%id,  0.0%wa,  1.8%hi,  0.1%si,  0.0%st
Mem: 24460076k total, 11600892k used, 953044k free, 5240k buffers
Swap: 26058744k total, 344100k used, 25714644k free, 10955400k cached

PROCESS                UPTIME                CPU%                VIRT_MEM            RES_MEM
phParser                3-14:04:08             1                   2443m                1628m
phQueryMaster           3-14:04:26             0                   1093m                118m
phRuleMaster            3-14:04:26             0                   1587m                385m
phRuleWorker            3-14:04:26             0                   1429m                776m
phQueryWorker           3-14:04:26             0                   1459m                600m
phDataManager           3-14:04:26             0                   3678m                1630m
phDiscover              01:51:08              0                    581m                 70m
phReportWorker          3-14:04:26             0                   1491m                691m
phReportMaster          3-14:04:26             0                    758m                 91m
phIdentityWorker        3-14:04:26             0                   1044m                382m
phIdentityWorker        3-14:04:26             0                    518m                 59m
phAgentManager          3-14:04:26             0                   1525m                68m
phCheckpoint            3-14:04:26             0                    322m                 64m
phPerfMonitor           DOWN
phReportLoader          3-14:04:26             0                    835m                335m
phDataPurger            3-14:04:26             0                    756m                199m
phEventForwarder        3-14:04:26             0                    539m                 42m
phMonitor               3-14:04:32             0                   1307m                625m
Apache                 3-14:08:33             0                    306m                 14m
Raynlogd               3-14:07:33             0                    190m                 5144k
Node.js-charting        1-14:01:57             0                    614m                 60m
Node.js-pm2            3-14:07:27             0                    769m                 62m
phFortiInsightAI        3-14:08:33             0                   13996m               358m
AppSvr                 3-14:07:24             6                   11231m               3984m
DBSvr                  3-14:08:33             0                    425m                 36m
phAnomaly              3-14:04:29             0                    782m                 55m
SVNLite                3-14:08:33             0                   9957m                616m
Redis                  3-14:07:27             0                    91m                  50m
```

You may see that the `phPerfMonitor` process is `DOWN`—wait for the process to come back up.

14. Once the `phPerfMonitor` process displays time in the `UPTIME` column, press `Ctrl+C` to exit out of the `phstatus` command output.
15. Close the FortiSIEM SSH session browser tab.

Resolve the Issue

You will fix the credentials, and then verify the fix.

To fix the credentials

1. Return to the FortiSIEM GUI, and then click the **ADMIN** tab.
2. In the left navigation pane, select **Setup**.
3. In the main window, select the **Credentials** tab.
4. Under **Step 1: Enter Credentials**, select **FGT_LAB_Router_SSH**, and then click **Edit**.
5. In the **User Name** field, type `admin`.
6. In the **Password** and **Confirm Password** fields, type `password`.
7. Click **Save**.

To do a configuration pull

1. Continuing on the FortiSIEM GUI, click the **Discovery** tab, and then select **FGT_LAB_Router**.
2. Click **Discover**.
3. After the discovery completes, click **Close**.
4. Click the **CMDB** tab.
5. In the left navigation pane, click **Devices > Network Device > Firewall**.
6. In the main window, click the refresh icon (↻).
7. Select the Fortinet FortiOS device named `_gateway`.
8. Observe the **Method** column.
Now, it displays **SSH** along with **SNMP** and **PING**.
9. In the lower pane, click the **Configuration** tab.
The startup configuration of the FortiGate device appears.

CMDB > Devices > Network Device > Firewall

Name	IP	Device Type	Status	Discovered	Method
FG240D3513800441	192.168.3.1	Fortinet FortiOS	Pending	Nov 29 2021, 04:30:44 PM	SNMP
FG240D3513800450	192.168.3.2	Fortinet FortiOS	Pending	Nov 29 2021, 04:24:51 PM	LOG
FortiGate50B	172.16.255.82	Fortinet FortiOS	Pending	Nov 29 2021, 04:34:37 PM	SNMP
FortiGate90D	10.1.1.1	Fortinet FortiOS	Pending	Nov 29 2021, 04:34:37 PM	SNMP
_gateway	10.0.1.254	Fortinet FortiOS	Pending	Dec 03 2021, 06:41:06 AM	SSH, SNMP, PING
HOST-172.16.1.3	172.16.1.3	Palo Alto PAN-OS	Pending	Nov 29 2021, 04:25:06 PM	LOG
HOST-172.16.3.10	172.16.3.10	Juniper SSG ScreenOS	Pending	Nov 29 2021, 04:30:28 PM	LOG
HOST-192.168.19.65	192.168.19.65	Cisco ASA	Pending	Nov 29 2021, 04:25:30 PM	LOG

Summary Properties Monitor Software Hardware Configuration Relationships File Auto expand

Diff... Delete Export

Rev	Date	Type/File Name
1	Dec 03 2021, 06:08:25 AM	startup-config

Rev #1 - Dec 3, 2021 9:08 AM - startup-config

```
discover Time 1638540496
#config-version=I GYM64-7.0.2-1 W-build02J4-211019:opmode=1:vdom=0:user=admin
#buildno-0234
#global_vdom=1
config system global
set admin-concurrent enable
set admin-console-timeout 0
set admin-forticloud-ssn-login disable
set admin-hsts-max-age 15552000
set admin-https-pki-required disable
```



It can take up to 10 minutes for the configuration to appear. Wait for the configuration to appear before moving to the next section.

To modify intervals for configuration pull

- Continuing on the FortiSIEM GUI, click the **ADMIN > Setup > Monitor Performance** tab, and then select **_gateway**.

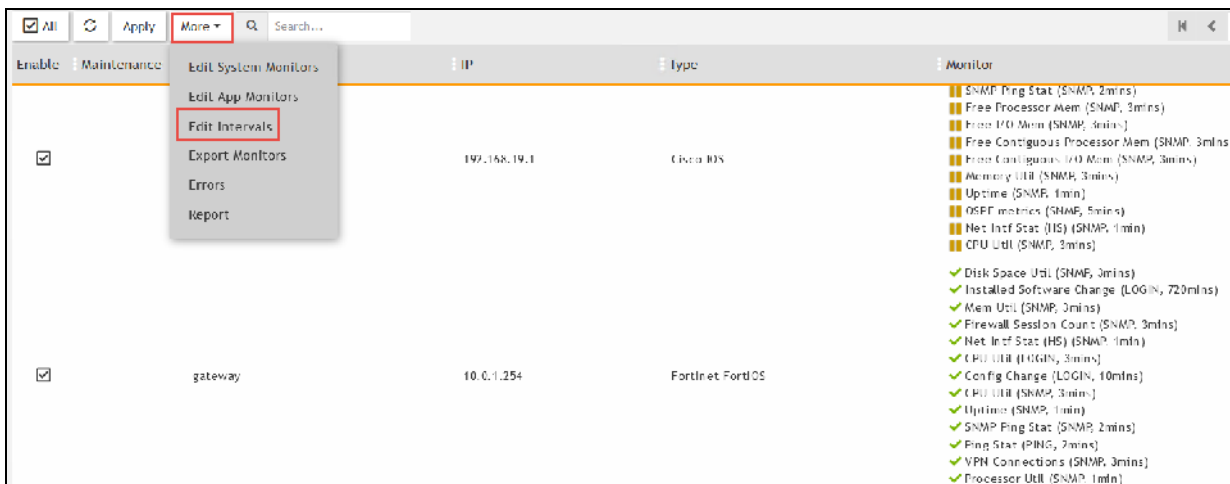
☒	_gateway	10.0.1.254	Fortinet FortiOS	✓ Disk Space Util (SNMP, 3mins) ✓ Installed Software Change (LOGIN, 720mins) ✓ Mem Util (SNMP, 3mins) ✓ Firewall Session Count (SNMP, 3mins) ✓ Net Intf Stat (HS) (SNMP, 1min) ✓ CPU Util (LOGIN, 3mins) ✓ Config Change (LOGIN, 10mins) ✓ CPU Util (SNMP, 3mins) ✓ Uptime (SNMP, 1min) ✓ SNMP Ping Stat (SNMP, 2mins) ✓ Ping Stat (PING, 2mins) ✓ VPN Connections (SNMP, 3mins) ✓ Processor Util (SNMP, 1min)
-------------------------------------	----------	------------	------------------	--



You will see performance monitor jobs applied to the **_gateway** device. All jobs should have a green check mark beside them. If you see a different icon, wait a couple of minutes until a green check mark icon appears. Click the refresh icon (🔄) to refresh the view.

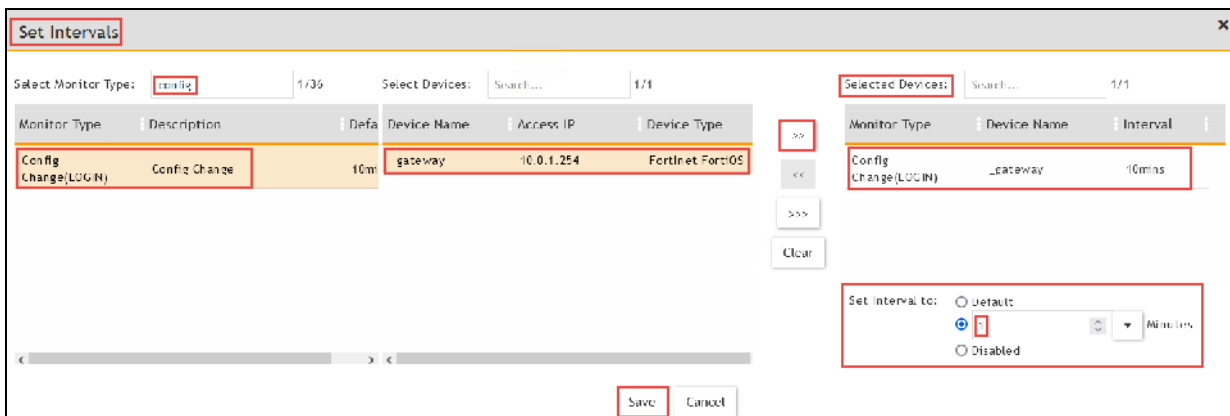
However, if you see the **Config Change(LOGIN, 10 mins)** job, you can move to the next step. While you are in the process of finishing, the next jobs will have a green check mark appear beside them.

- Click **More**, and then click **Edit Intervals**.



The **Set Intervals** pop-up window appears.

- In the **Select Monitor Type** search section, type **config**.
- In the **Select Devices** section, select the **_gateway** device, and then click **>>** to add the monitor to the **Selected Devices** pane.
- In the **Selected Devices** section, select the **Config Change (LOGIN)** entry, and then set the **Set Interval** to to 1 minute.
- Click **Save**.



The **Config Change** monitor should be set to one minute to speed up the configuration change pull from the device for this lab.

Enable	Maintenance	Device	IP	Type	Monitor
☒		_gateway	10.0.1.254	Fortinet FortiOS	✓ Disk Space Util (SNMP, 3mins) ✓ Config Change (LOGIN, 1min) ✓ Mem Util (SNMP, 3mins) ✓ Firewall Session Count (SNMP, 3mins) ✓ Net Intf Stat (HS) (SNMP, 1min) ✓ Installed Software Change (LOGIN, 720mins) ✓ CPU Util (LOGIN, 3mins) ✓ CPU Util (SNMP, 3mins) ✓ Uptime (SNMP, 1min) ✓ SNMP Ping Stat (SNMP, 2mins) ✓ Ping Stat (PING, 2mins) ✓ VPN Connections (SNMP, 3mins) ✓ Processor Util (SNMP, 1min)

To force an SSH configuration revision change on FortiGate

1. Log in to the FortiGate GUI with the username `admin` and password `password`.
2. Click **Policy & Objects > Firewall Policy**.
3. Select the **Internet** firewall policy, and then click **Edit**.
4. Scroll to the bottom of the page, and then in the **Comments** section, type `FSM_SSH_CONFIG_TEST`.
5. Click **OK** to save the changes, and then log out of the FortiGate GUI.

To review the simulated FortiGate SSH configuration change

1. Return to the FortiSIEM GUI, and click **CMDB**.
2. In the left navigation pane, click **Devices > Network Device > Firewall**.
3. Select the **Fortinet FortiOS** device `_gateway`.
4. Click the refresh icon (↻).
5. In the lower pane containing the details, click the **Configuration** tab.

A second revision of the startup configuration should appear. If it does not appear, wait a few minutes, and then refresh again.



It can take up to five minutes for the configuration changes to appear. Wait for the configuration to appear.

4. Depending on your computer, press `Shift` or `Ctrl` to select both revisions, and then click **Diff**.

Summary	Properties	Monitor	Software	Hardware	Configuration	Relationships	File	Auto expand
Diff...	Delete	Export						
Rev	Date	Type/File						
2	Nov 04 2021, 06:52:47 PM	startup-c						
1	Nov 04 2021, 06:29:11 PM	startup-c						

```

Rev #2 - Nov 4, 2021 9:52 PM - startup-config
discoverTime 1636077159
#config-version=FGVM64-7.0.2-FW-build0234-211019:opmode=1:vdom=0:user=admin
#buildno=0234
#global vdom=1
config system global
set admin-concurrent enable
set admin-console-timeout 0
set admin-forticloud-ssologin disable
  
```

If the configuration change is taking longer than five minutes to appear, you can restart the performance monitor process to speed up the configuration change revision.



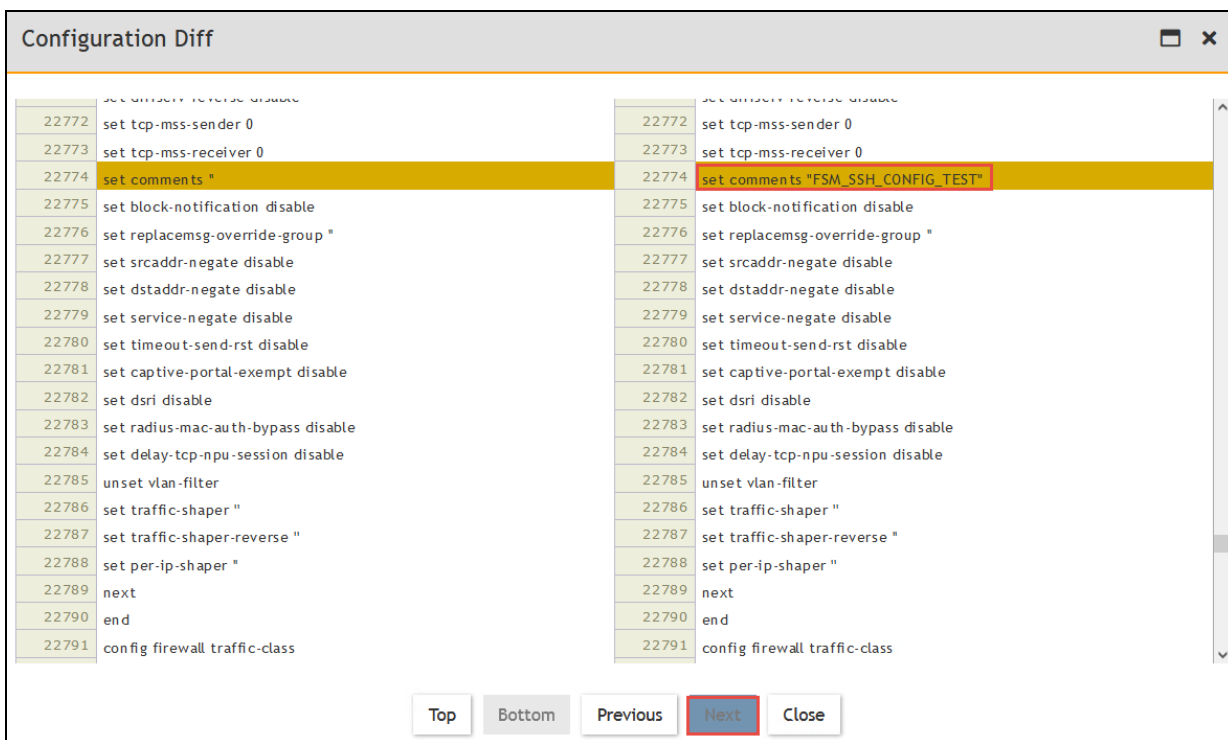
To restart the performance monitor process, enter the following command from the SSH session of FortiSIEM:

```
killall -9 phPerfMonitor
```

The process will start automatically. You can verify this by entering the `phstatus` command.

Once the **phPerfMonitor** process is up, you can force another change from FortiGate by modifying the comment you added in the **Internet** policy, saving the change, and logging out of the FortiGate GUI.

5. Review the configuration changes, click **Next** to move to the next change, and then close the dialog box.



6. Log out of the FortiSIEM GUI.

Appendix: Answer Sheet

Lab 1—Introduction to FortiSIEM

Exercise 1: Creating Roles

Question:

Review the information in the **Data Conditions** and **CMDB Report Conditions** sections for this role. What do you understand about these fields?

Answer:

Data Conditions - Restrict what data a role can see in the GUI, such as restricting auditors to just events reported by Server devices such as Windows devices, or to restrict access to some dashboards for example Network Dashboard.

CMDB Report Conditions - Restrict what data is available in CMDB Reports, such as allowing a device inventory report of only Server devices.

Lab 2—SIEM & PAM Concepts

Exercise 1: Reviewing Incoming Data

Question:

Which users had failed logins?

Answer:

admin and fred

Exercise 2: Structured Data

Question:

Make a note of each field header in the table.

Answer:

Event Receive Time, Reporting IP, Event Type, Raw Event Log.

Question:

Which attribute relates to the device IP that sent the data?

Answer:

Reporting IP

Question:

Which event type relates to a login failure?

Answer:

FortiGate-event-login-failure

Question:

Which attribute provides the local time when FortiGate actually logged the event?

Answer:

Device Time

Question:

What are the **Reporting Model** and **Reporting Vendor** attributes of the event?

Answer:

Reporting Model: FortiOS

Reporting Vendor: Fortinet

Question:

What attribute did FortiSIEM map this to in the structured view?

Answer:

Application Protocol

Question:

Who made a successful authentication? And what attribute was this field mapped to in the structured view?

Answer:

admin was mapped to the User attribute.

Exercise 3: Event Classification

Question:

Make a note of the **Member of** field.

Answer:

/Security/Logon Success/Dev Logon Success

Question:

Make a note of the **Description**

Answer:

Successful admin logon

Question:

What do you notice about this particular event?

Answer:

It's a member of two groups:

/Security/Logon Failure/Dev Account Locked

/Security/Logon Failure/Domain Account Locked

Therefore, events can belong to more than one group/category.

Exercise 4: Event Enrichment

Question:

What is the value in the **Member of** field?

Answer:

/Security/Logon Failure/Dev Logon Failure

Question:

Does it contain any country related information?

Answer:

Yes

Question:

Where did this information come from?

Answer:

The internal geolocation database

Question:

Is there a **Source Country** or **Destination Country** populated for this event? If not, why?

Answer:

No, these are internal RFC 1918 addresses.

Question:

Is there now a **Reporting City**, **Destination City**, **Destination Country**, and **Destination State** populated? If so why?

Answer:

Yes, since country related event enrichment can also occur for internal RFC 1918 addresses if these value are set on an asset in the CMDB.

Exercise 5: Reviewing Performance Events

Question:

Which attributes relate to the up-time and downtime of the device?

Answer:

- RAW: sysUpTime, sysDownTime
- Attribute: System Uptime, System Downtime

Question:

What attribute relates to how often the event is collected?

Answer:

Polling Interval

Question:

Which attribute relates to the memory utilization of the device?

Answer:

Memory Util

Question:

How often is the memory utilization event collected?

Answer:

Every 180 seconds (or 3 minutes)

Question:

Which attributes relate to the interface name and interface utilization?

Answer:

- Host Interface Name
- Recv Interface Util
- Sent Interface Util

Question:

Why are there four interface utilization events?

Answer:

The device has 4 network interfaces (one event per interface).

Lab 3—Discovery

Exercise 1: Auto Log Discovery

Question:

Why are the names different do you think?

Answer:

The FortiGate logs contain the name of the device reporting the data (devname=x), and hence the parser reads this and maps to an attribute named **Reporting Device Name**.

The Cisco ASA logs do not contain the name, so the default behavior is to name the device HOST-<reporting ip>

Question:

What is displayed under the **Version** and **Last Discovered Method** fields for each device?

Answer:

- Version: ANY ... logs alone do not tell the FortiSIEM the version of the device or application.
- Last Discovered Method: LOG .. auto log discovery

Question:

What do you see and what can you determine about the population of the CMDB from log only discovery alone?

Answer:

They are blank. This type of information is not sent as part of the event message.

Exercise 3: Discovery of a Single Device

Question:

What does the **Version** field show now?

Answer:

Version: 5.4.1(1064)

Question:

How many groups is this device now a member of?

Answer:

19 groups. It has also been categorized under various networks by the IP Addresses/Network Masks on the interfaces.

Question:

Make a note of how often **CPU Util**, **Mem Util**, and **Net Intf Stat** jobs are being collected via SNMP.

Answer:

- CPU Util - 3 minutes
- Mem Util - 3 minutes
- Net Intf Stat - 1 minute

Exercise 4: Performing Discovery of other Lab Devices

Question:

Make a note of the entries in the **Process Name** and **Process Param** columns.

Answer:

- Process Name: svchost.exe
- Process Parameter: -k iissvcs

Question:

Now type **DNS** in the search field and again make note of the entries in the **Process Name** and **Process Param** columns.

Answer:

- Process Name: dns.exe
- Process Param: none

Lab 4—Introduction to Analytics

Exercise 2: Search Operators

Question:

What was the impact of this search?

Answer:

Only raw logs with both devname and HTTP keywords are returned

Question:

What can you determine about the case sensitivity of keywords?

Answer:

The keywords are not case sensitive.

Lab 5—CMDB Lookups and Filters

Exercise 3: Expert Challenge

Question A:

- Which user had failed an SSH login?
- From what IP Address?

Answer:

Hacker from source IP 192.168.0.30.

Question B:

Do you see any suspicious port usage in your results?

Answer:

Source IP = 69.94.156.1 AND

Destination IP = 192.168.0.10

Add Column: Destination TCP/UDP

Question C:

Do your results indicate the firewall rules are correctly implemented?

Answer:

There are lots of connections permitted to external destinations on non-standard ports like 135, 199, 445, etc. The firewall rule is incorrectly configured.

Question D:

Was any internal traffic permitted to any country in ASIA in the last 2 hours that was not on TCP/UDP ports 25,53,80,123, or 443?

Answer:

Yes, permitted traffic has been reported to countries in ASIA not on the defined TCP/UDP port list. Time to tighten up those firewall rules!

Question E:

Which interfaces on the switch has this issue?

Answer:

Interface: GigabitEthernet4/48

Lab 6—Group By and Aggregation

Exercise 2: Aggregating Data

Question:

What do your results show?

Answer:

A list of the disk capacity utilization of all the servers, with the highest utilization at the top of the list.

Exercise 3: Expert Challenge

Question A:

Which firewall device reported the most events over the last 30 minute time period?

Answer:

192.168.3.1

Question B:

Which is the most common destination country of any firewall events that are not on Destination TCP/UDP Port of 21,80,443 or 53 over the last 1 hour?

Answer:

United States

Question C:

What is the most common source country for any deny events reported by a firewall device in the last 30 minutes?

Answer:

Top result is NULL (for internal IPs that don't have a country).

Most common country is the United States.

Question D

What events does this report produce?

Answer:

It produces hundreds of events that repeat for the same Application/Software Name. (Since the data is collected every 3 minutes.)

Lab 7—Rules

Exercise 1: Simple Rule Example

Question:

What time period is the rule evaluating the pattern over?

Answer:

600 seconds (or 10 minutes)

Question:

Make a note of the attributes in the **Group By** section.

Answer:

- Reporting Device
- Reporting IP
- User

Question:

Make a note of the severity of the rule and also the function.

Answer:

Severity: 10-High Function: Security

Question:

Make a note of the attributes in the **Selected Attributes** column.

Answer:

- Event Receive Time
- Event Type
- Reporting IP
- Source IP
- User
- Computer
- Win Logon Type
- Raw Event Log

Question:

Do the details match what was recorded in step 6 of **To view a rule** section of this exercise?

Answer:

Yes

Exercise 2: Performance Rule Example

Question:

Make a note of value in the **Default** field and the disk name listed:

Answer:

Disk Space Util Critical Threshold	95
Name	C:\

Question:

Find the threshold for **Free Disk (MB) Critical Threshold**.

Answer:

Free Disk (MB) Critical Threshold	100
Name	C:\

Question:

Make a note of the values associated with the following items.

Answer:

Severity	5 - MEDIUM
Category	Performance
Subcategory	Impact
Evaluation Time Window	600 seconds

Question:

Are there any results where the AVG(Disk Capacity Util) is greater than 95% and the AVG (Free Disk (MB)) is less than 100?

Answer:

Yes

Lab 8—Incidents and Notification Policies

Exercise 1: Reviewing the Incident Table

Question:

What do you think this option is actually doing for this rule?

Answer:

If the original rule does not trigger again for 20 minutes, then the incident will automatically be cleared.

Exercise 2: Grouping and Tuning Incidents

Question:

Explain what the rule pattern is looking for.

Answer:

It is looking for DNS traffic that is not coming from other DNS servers or internal applications. The traffic is originating from the internal private network and is being reported by the firewalls, routers, and/or switches.

Lab 9—Reporting

Exercise 4: Creating your Own Dashboards

Question:

Will these new adjusted values for AVG CPU determine what thresholds rules will trigger for these devices?

Answer:

No

Exercise 5: Dashboard Drill Down

Question:

What is the query looking at?

Answer:

Attribute	Operator	Value	Next Op
Host Name	=	FortiGate90D	
Event Type	IN	PH_DEV_MON_SYS_CPU_UTIL, PH_DEV_MON_SYS_MEM_UTIL AND	AND
Host IP	IN	Devices: Network Device	AND

Question:

What has the time criteria been pre-populated to run over and where did this value come from?

Answer:

The time criteria is set to look at absolute value. These values came from the widget.

Question:

What was the result of this action?

Answer:

It takes you to **ANALYTICS** tab with search field pre-populated.

Question:

How does this differ from the analytic query produced from step 7 of **drill down on dashboard content**?

Answer:

In step 3, it was on a specific device.

Lab 10—Business Services

Exercise 2: Business Service Incidents

Question:

What service was stopped?

Answer:

McAfee Access Scanner

Question:

Which device had a severe vulnerability detected?

Answer:

WIN2K8 192.168.0.40 and QA-EXCHG 172.16.10.28

Exercise 3: Business Service Summary Dashboard

Question:

Can you identify the SQL query that was running slow?

Answer:

```
select * from patient_records
```

Question:

Can you identify the files that were added on the QA-EXCHG or WIN2K8 machines?

Answer:

```
C:\Documents\Contracts\7ogger.exe
```

```
C:\Windows\System32\svchostss.exe
```

```
C:\Documents\Contracts\mcafeeav.pif
```



FORTINET®



No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from Fortinet Inc., as stipulated by the United States Copyright Act of 1976.

Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.