DO NOT REPRINT
© FORTINET

FortiAnalyzer Lab Guide

for FortiAnalyzer 7.0

FORTINET NSE Training Institute

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET

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.fortiguard.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

FORTINET

2/15/2022

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET

Brave-Dumps.com

TABLE OF CONTENTS

Change Log 6
Network Topology 7
Lab 1: Initial Configuration 8
Exercise 1: Examining the Network Settings 12
Lab 2: Administration and Management 17
Exercise 1: Configuring ADOMs 18
View ADOM Information 19
Create Custom ADOMs 20
Exercise 2: Configuring an External Server to Validate Administrators 23
Configure an LDAP Server on FortiAnalyzer 23
Create a Wildcard LDAP Administrator 25
Test External Administrator Access 26
View the Event Logs 29
Lab 3: Device Registration and Communication 30
Exercise 1: Registering Devices on FortiAnalyzer 32
Register a Device Using the Add Device Wizard 32
Accept a Device Registration Request 34
Exercise 2: Troubleshooting Device Communication 37
Verify Device Registration 37
Verify Device Communication 38
Troubleshoot Device Communication 38
Resolve a Connection That Is Down 39
Lab 4: Logs 43
Exercise 1: Gathering Benchmark Diagnostics 44
View System Resource Information 44
Gather Data Policy and Disk Utilization Information 45
Exercise 2: Generating Traffic 47
Generate Traffic Using FIT 47
Generate Traffic Using Nikto 48
Exercise 3: Examining Logs 51
View Logs in Log View 51
Use Log Filters 54
View Logs in FortiView 55

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 4: Viewing Log Statistics and Used Storage Space 59
View the Raw Log Receiving Rate 59
View the Insert Rate Versus the Receive Rate 60
View Used Storage Statistics 61
Exercise 5: Modifying Disk Quotas 63
Compare Storage Space Between ADOMs 63
Modify the Disk Quota 63
Exercise 6: Moving Devices With Logs Between ADOMs 65
Gather Log and ADOM Information 65
Move a Device to a Different ADOM 66
Rebuild the ADOM Database to Migrate the Device Logs 67
Lab 5: Events and Incidents Management 70
Exercise 1: Examining and Managing Events 71
Examine Existing Events 71
Exercise 2: Cloning and Customizing Event Handlers 74
Find the Event Handler and the Log That Generated an Event 74
Clone and Customize an Event Handler 77
Generate Traffic to Create Events 79
Verify the New Event Handler Works 80
Exercise 3: Creating a Custom Event Handler 82
Create an Event and Find the Log That Generated It 82
Create a Custom Event Handler 83
Test the Custom Event Handler 84
Expert Challenge 85
Exercise 4: Managing Incidents 86
Create New Incidents Manually 86
Exercise 5: Exploring Threat Hunting 93
Explore the Threat Hunting Tools 93
Example of a Threat Hunting Scenario 94
Lab 6: Playbook Management 95
Exercise 1: Creating a Playbook With an On-Demand Trigger 97
Create a New Playbook With an On-Demand Trigger 97
Verify the Current Number of Incidents 100
Run and Troubleshoot a Playbook 101
Exercise 2: Creating a Playbook With an Incident Trigger 104
Create a Playbook With an Incident Trigger 104
Verify the Playbook Runs Successfully 107
Exercise 3: Importing and Customizing a Playbook 109
Import and Customize a Playbook 109
Generate Traffic to Trigger the Playbook 113
Verify the Successful Execution of the Playbook 113

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 4: Using FortiOS Connectors 115
Examine Existing FortiOS Connectors 115
Add a Playbook Task That Disables a Firewall Policy 115
Verify the FortiGate Configuration Before Running the Playbook 117
Generate Traffic to Trigger the Playbook 118
Verify the Effect of Running the Playbook 118
Create a Playbook to Enable a Firewall Policy 119
Exercise 5: Exporting and Importing Playbooks 121
Add a Connector in Fabric View 121
Create a Playbook With the FortiClient EMS Connector 122
Export a Playbook 125
Import a Playbook 126
Lab 7: Reports 128
Exercise 1: Running a Default Report 129
Generate a Default Report 129
Run Diagnostics on a Report 131
Exercise 2: Cloning and Customizing a Default Report 133
Exercise 3: Building a Custom Dataset From Scratch 134
Create a Dataset 134
Exercise 4: Building a Custom Chart From Log View 136
Create a Custom Chart 136
Create and Run a Report Using a Custom Chart 138
Exercise 5: Scheduling a Report 142
Create and Configure an Output Profile 142
Schedule Reports 143

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Change Log

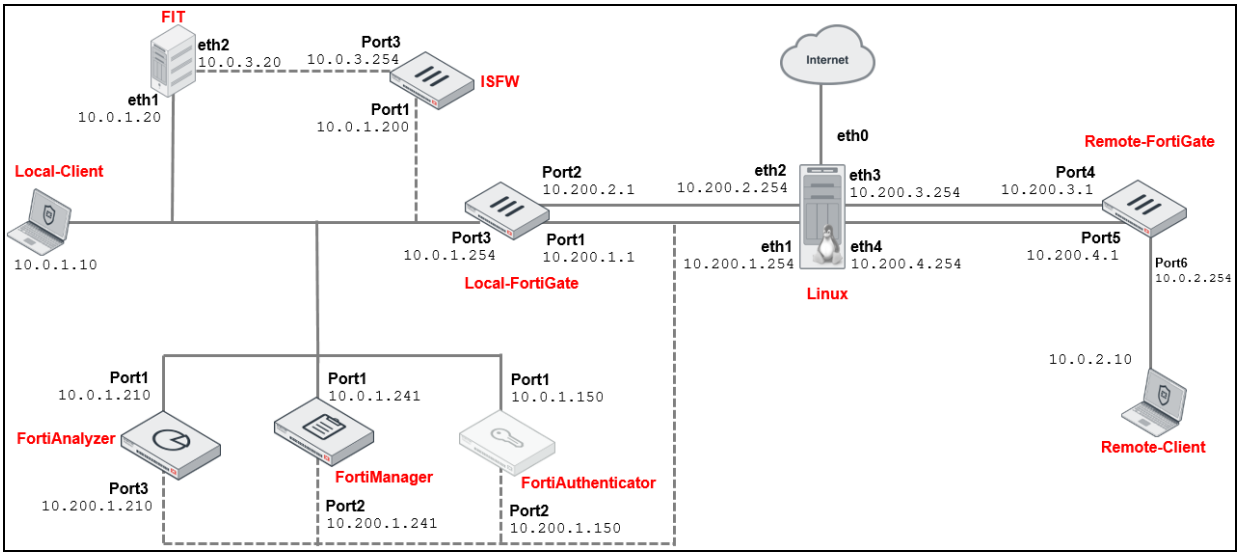
This table includes updates to the *FortiAnalyzer Lab Guide 7.0* dated 12/01/2021 to the updated document version dated 2/15/2022.

Change	Location
Removed following exercise from lab 5: Examining the FortiSoC Dashboards	Lab 5
Clarified instructions for Instructor Led and Self-paced students	Lab 7 exercise 1

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Network Topology



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Lab 1: Initial Configuration

In this lab, you will examine the network settings of FortiAnalyzer from the CLI and GUI.

Objectives

- Examine the network settings

Time to Complete

Estimated: 25 minutes

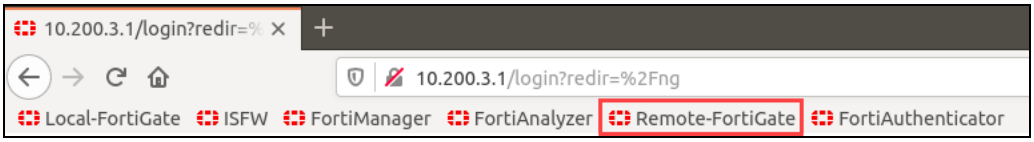
Prerequisites

Before beginning this lab, you must update the firmware and initial configuration on Local-FortiGate, ISFW, and Remote-FortiGate.

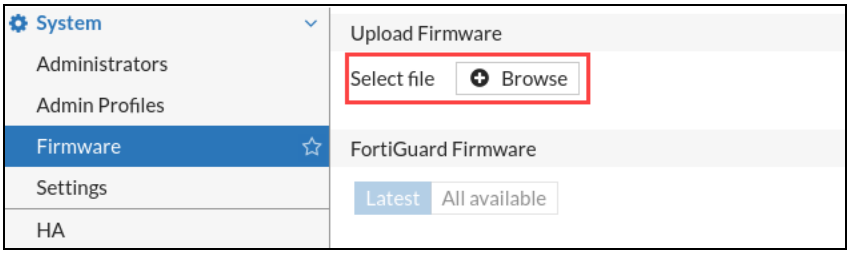
This lab environment is also used for the FortiGate Security and FortiGate Infrastructure 7.0.0 training, and initializes in a different state from what is required for the FortiAnalyzer 7.0.2 training.

To update the FortiGate firmware on all FortiGate devices

1. On the Local-Client VM, open a browser, and then log in to the Remote-FortiGate GUI at `10.200.3.1` with the username `admin` and password `password`.
   You can use the links in the favorites bar to access all devices, as shown in the following image:



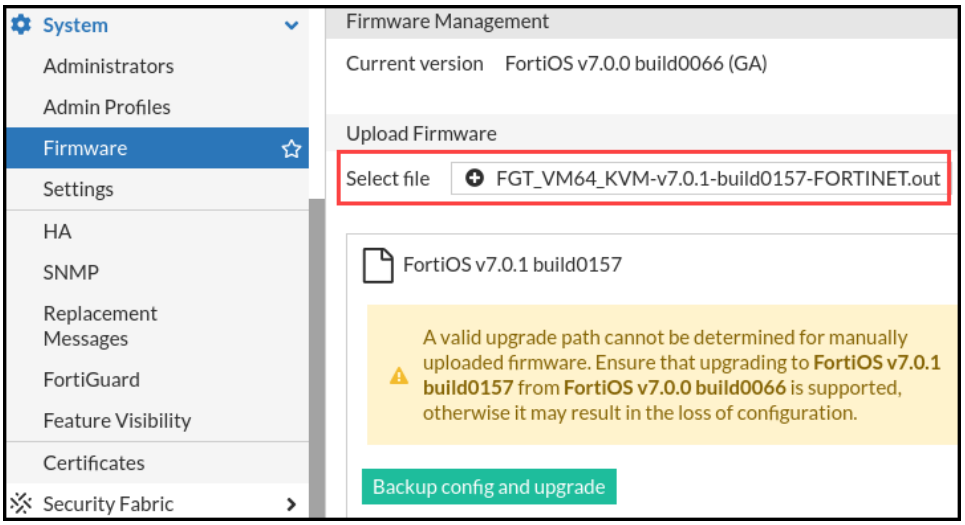
2. Click **System** > **Firmware**, and then click **Browse** under **Upload Firmware**.



3. Browse to **Desktop** > **Resources** > **FortiAnalyzer** > **FGT-firmware**, select `FGT_VM64_KVM-v7.0.1-build0157-FORTINET.out`, and then click **Open** to load the file.
4. Click **Backup config and upgrade**, and then click **Continue** on the warning window to initiate the upgrade.

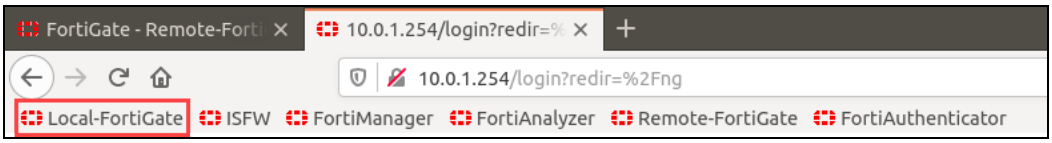
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

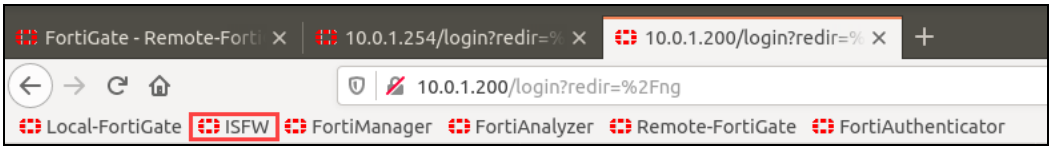


The system starts rebooting.

5. Click **Cancel** to not save the configuration backup file.
6. Open another browser tab, and then log in to the Local-FortiGate GUI at `10.0.1.254` with the username `admin` and password `password`.



7. Repeat this procedure to update the firmware for Local-FortiGate.
8. Open a third browser tab, and then log in to the ISFW GUI at `10.0.1.200` with the username `admin` and password `password`.



9. Repeat this procedure to update the firmware for ISFW.

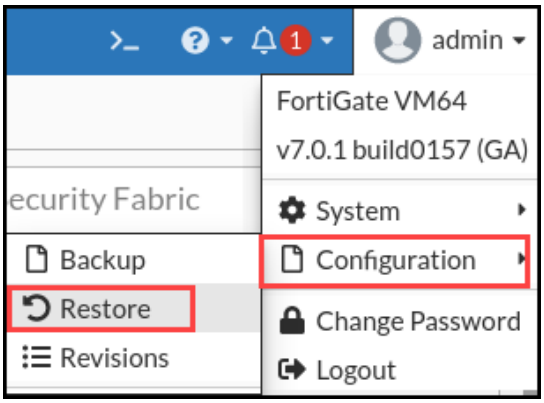
To restore the Remote-FortiGate configuration file

Make sure you restore the correct configuration file on the correct device. The name of the configuration file matches the name of the device that it must be restored on.

1. On the Local-Client VM, open a browser, and then log in to the Remote-FortiGate GUI at `10.200.3.1` with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

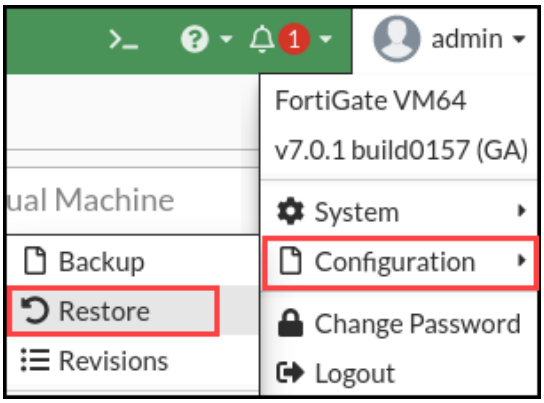
DO NOT REPRINT
© FORTINET
Brave-Dumps.com



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **FortiAnalyzer** > **LAB-1** > `Remote-FortiGate-initial.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

To restore the Local-FortiGate configuration file

1. On the Local-Client VM, open a browser, and then log in to the Local-FortiGate GUI at `10.0.1.254` with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



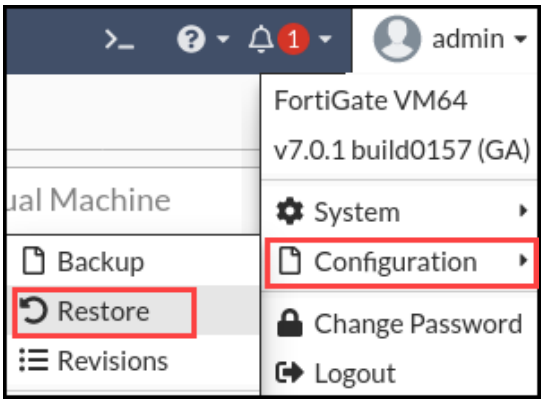
3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **FortiAnalyzer** > **LAB-1** > `Local-FortiGate-initial.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

To restore the ISFW configuration file

1. On the Local-Client VM, open a browser, and then log in to the ISFW GUI at `10.0.1.200` with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **FortiAnalyzer** > **LAB-1** > `ISFW-initial.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 1: Examining the Network Settings

In this exercise, you will examine the initial configuration of FortiAnalyzer from the CLI and GUI.

To examine the network settings using the CLI

1. On the FortiAnalyzer CLI, log in with the username `admin` and password `password`.
2. Enter the following command to display basic status information about FortiAnalyzer:

CLI command	Data	Result
`# get system status`	What is the firmware version? Knowing the FortiAnalyzer firmware version is important because it determines what Fortinet products—and associated firmware versions—are supported.	
	What is the administrative domain (ADOM) configuration? By default, ADOMs are disabled.	
	What is the time zone? For proper log correlation, it is important that the system time on FortiAnalyzer and all registered devices is synchronized.	
	What is the license status? To ensure FortiAnalyzer continues to collect and store logs, a valid license is required.	

3. Enter the following command to display information about the FortiAnalyzer interface configuration:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

CLI command	Diagnostic	Result
`# show system interface`	What is the IP address of port1? Port1 is the management port and has the IP address of FortiAnalyzer.	
	What administrative access protocols are configured for port1? This will help troubleshoot any access issues you may experience.	
	What is the IP address of port3? According to the network topology diagram, port3 is used to route traffic between Remote-FortiGate and FortiAnalyzer. Remote-FortiGate, therefore, will connect to FortiAnalyzer using the port3 IP address.	
	What administrative access protocols are configured for port3?	

4. Enter the following command to display DNS setting information:

CLI command	Diagnostic	Result
`# show system dns`	What are the primary and secondary DNS settings? Several FortiAnalyzer functions use DNS, such as sending alert emails and resolving host names in the logs. By default, FortiAnalyzer uses FortiGuard DNS servers.	

5. Enter the following commands to display NTP setting information:

CLI command	Diagnostic	Result
`# get system ntp`	Is NTP enabled? NTP is recommended on FortiAnalyzer and all registered devices for proper log correlation.	
	How often does FortiAnalyzer synchronize its system time with the NTP server?	
`# show system ntp`	What server is configured for NTP? By default, Fortinet servers are configured.	

6. Enter the following command to display information about the FortiAnalyzer routing configuration:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

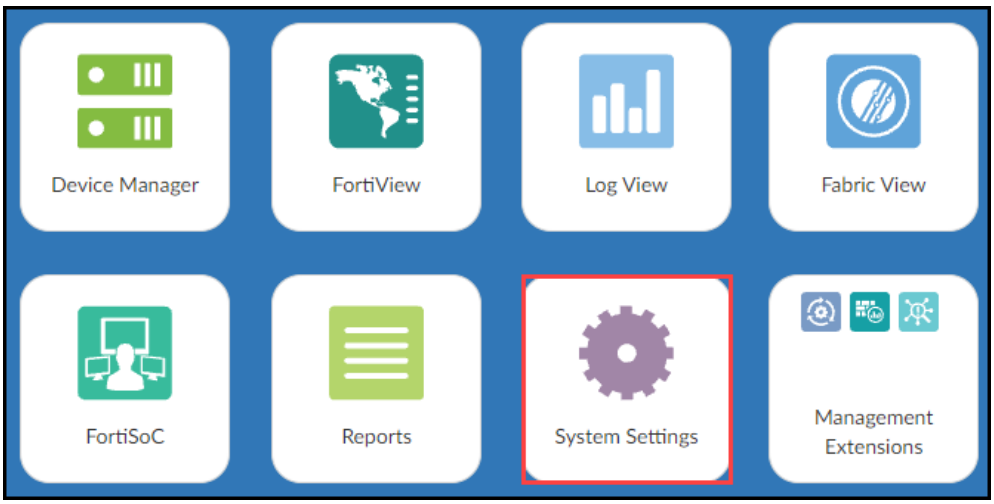
DO NOT REPRINT
© FORTINET
Brave-Dumps.com

CLI command	Diagnostic	Result
`# show system route`	What is the gateway route associated with port3? According to the network topology diagram, this IP address is the route to use to reach Remote-FortiGate.	

7. Close the FortiAnalyzer CLI session.

To examine the network settings using the GUI

1. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. On the main tiles, click **System Settings**.



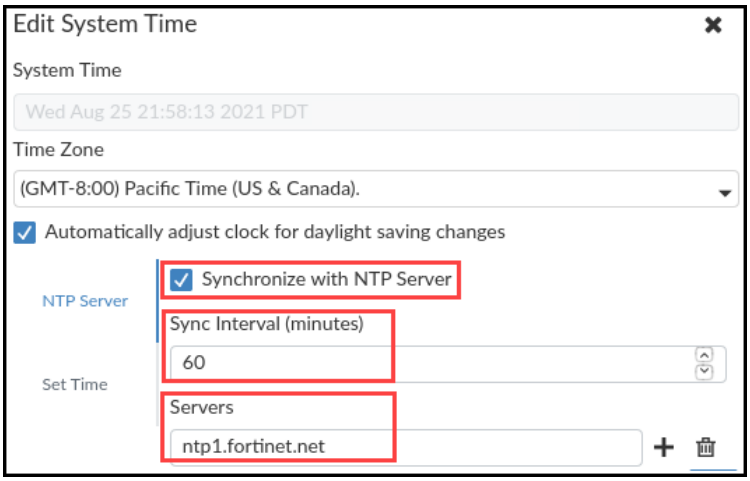
The dashboard appears.

3. Examine the **System Information** and **License Information** widgets to display the information shown below. This displays the same information available from the `get system status` CLI command.
   - Firmware version
   - ADOM status
   - System time and time zone
   - License status (VM)
4. On the **System Information** widget, click the edit pencil icon beside **System Time** to view the NTP information.

This displays the same information available from the `get system ntp` and `show system ntp` CLI commands.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

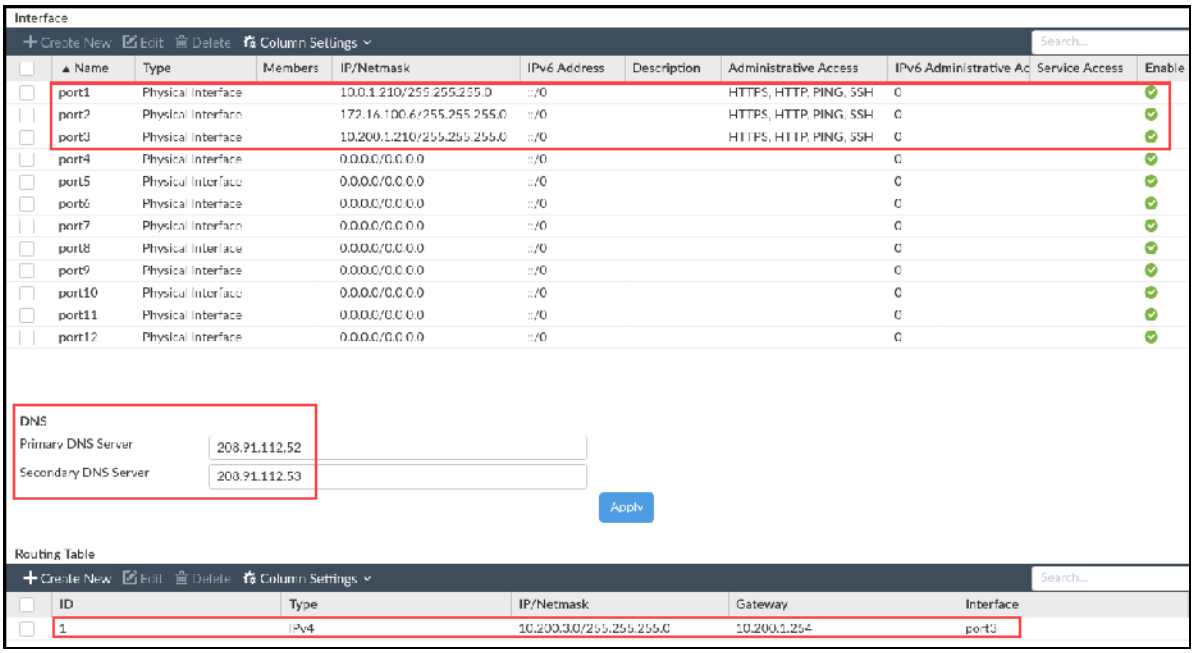
DO NOT REPRINT
© FORTINET
Brave-Dumps.com



5. Click **X** to go back to the **System Information** widget.
6. In the menu on the left, click **Network**.

   This page displays information about all FortiAnalyzer interfaces, including their configured IP addresses and administrative access protocols. This page also shows the DNS servers and the routing table.

   The information displayed here is the same information available from the `show system interface`, `show system dns`, and `show system route` CLI commands. For example, according to the `show system interface` CLI command, you should see that port 2 and port 3 are also configured.



7. To modify the settings of an interface, or the routing table, select the checkbox for the entry that you want to change, and then click **Edit**.
8. To modify the DNS settings, type new values in the DNS server fields, and then click **Apply**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

To examine the Local-FortiGate system time

1. Log in to the Local-FortiGate GUI with the username `admin` and password `password`.
2. In the menu on the left, click **System** > **Settings**, and then check **System Time**.
   Does Local-FortiGate have the same system time settings as FortiAnalyzer?

   This is important to ensure log correlation between Local-FortiGate and FortiAnalyzer.

Setting	FortiAnalyzer	Local-FortiGate
Time Zone	(GMT-8:00) Pacific Time (US & Canada)	
Set time	NTP	
Select server	FortiGuard	

3. Close the browser.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Lab 2: Administration and Management

In this lab, you will configure FortiAnalyzer for administrative domains (ADOMs). You will also configure an external server to validate non-local (external) administrators.

You will configure the external administrator to have access to a specific ADOM only.

Objectives

- Configure ADOMs
- Configure an external server to validate administrators

Time to Complete

Estimated: 25 minutes

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

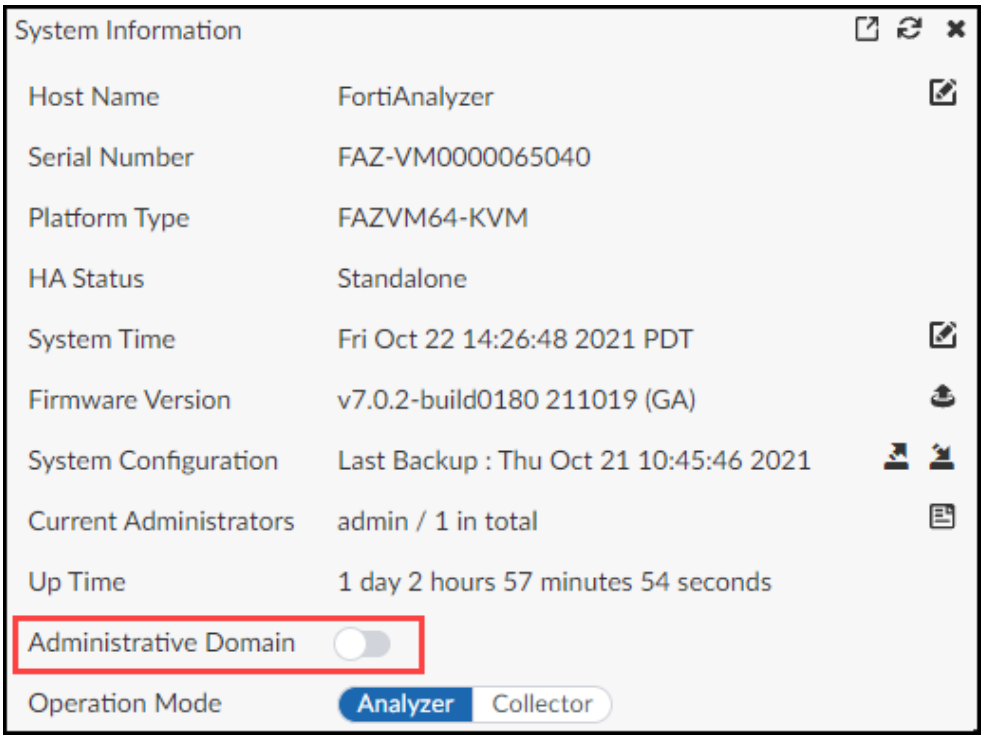
Exercise 1: Configuring ADOMs

In this exercise, you will enable ADOMs, view default ADOM information, and create two custom ADOMs.

A use case for employing ADOMs is to restrict the access privileges of other administrators to a subset of devices in the device list.

To enable ADOMs

1. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. Click **System Settings**.
3. On the dashboard, in the **System Information** widget, turn on **Administrative Domain**.



4. Click **OK** to confirm.
   You are automatically logged out of the GUI.
5. Log back in to the FortiAnalyzer GUI with the username `admin` and password `password`.
   Since ADOMs are now enabled, you must select an ADOM to log in to. The ADOMs that you are presented with are based on your administrator permissions.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

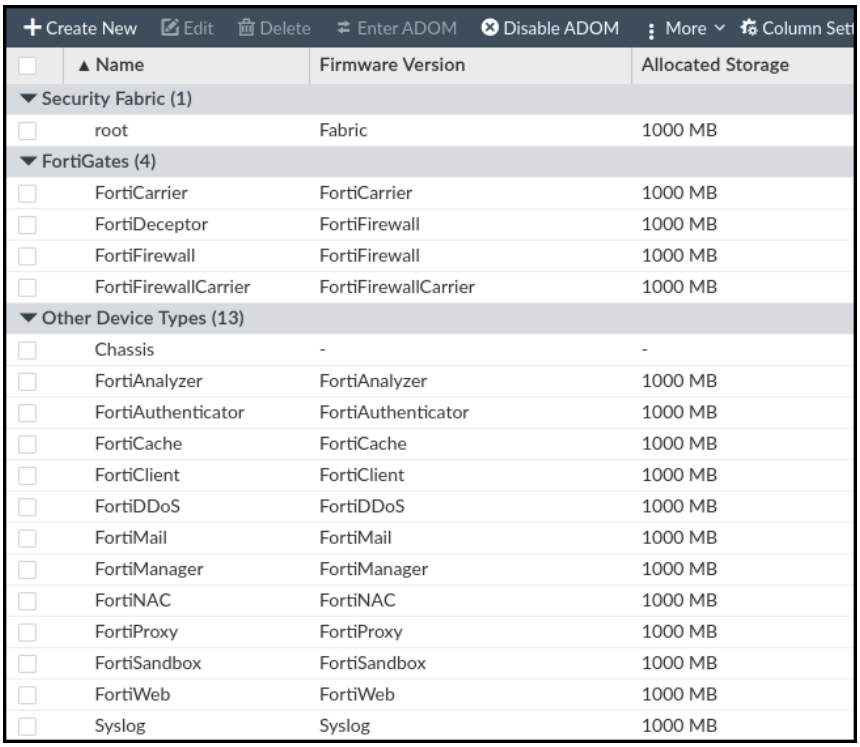
6. Select the **root** ADOM.

View ADOM Information

Before you create new ADOMs, you should be aware of what ADOM types are available to you. You will view ADOM information on both the GUI and CLI.

To view ADOM information

1. After you log in to the root ADOM on FortiAnalyzer, click **System Settings**.
2. In the menu on the left, click **All ADOMs**.
   This page lists all available ADOMs and any devices that are added to those ADOMs.



Name	Firmware Version	Allocated Storage
Security Fabric (1)		
root	Fabric	1000 MB
FortiGates (4)		
FortiCarrier	FortiCarrier	1000 MB
FortiDeceptor	FortiFirewall	1000 MB
FortiFirewall	FortiFirewall	1000 MB
FortiFirewallCarrier	FortiFirewallCarrier	1000 MB
Other Device Types (13)		
Chassis	-	-
FortiAnalyzer	FortiAnalyzer	1000 MB
FortiAuthenticator	FortiAuthenticator	1000 MB
FortiCache	FortiCache	1000 MB
FortiClient	FortiClient	1000 MB
FortiDDoS	FortiDDoS	1000 MB
FortiMail	FortiMail	1000 MB
FortiManager	FortiManager	1000 MB
FortiNAC	FortiNAC	1000 MB
FortiProxy	FortiProxy	1000 MB
FortiSandbox	FortiSandbox	1000 MB
FortiWeb	FortiWeb	1000 MB
Syslog	Syslog	1000 MB

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

3. On the FortiAnalyzer CLI, log in with the username `admin` and password `password`.
4. Run the following command to view the ADOMs that are currently enabled on FortiAnalyzer and the type of device that you can register to each ADOM:

```
diagnose dvm adom list
```

The CLI output is easier to read if you maximize your window. If you already executed the command, once the window is maximized, press the up arrow to show the last command you entered, and then press `Enter` to run the command again.

```
FAZVM64-KVM # diagnose dvm adom list
There are currently 20 ADOMs:
OID      STATE    PRODUCT OSVER MR  NAME                 MODE    VPN MANAGEMENT        IPS       ISDB
122      enabled  FAZ     6.0   4   FortiAnalyzer        Normal  Policy & Device VPNs  18.175    7.1704
138      enabled  FAC     6.0   0   FortiAuthenticator   Normal  Policy & Device VPNs  18.175    7.1924
126      enabled  FCH     4.0   2   FortiCache           Normal  Policy & Device VPNs  0.0       0.0
118      enabled  FOC     6.0   4   FortiCarrier         Normal  Policy & Device VPNs  18.175    7.1704
128      enabled  FCT     6.0   2   FortiClient          Normal  Policy & Device VPNs  18.175    7.1924
136      enabled  FDD     5.0   3   FortiDDoS            Normal  Policy & Device VPNs  18.175    7.1924
144      enabled  FFW     3.0   1   FortiDeceptor        Normal  Policy & Device VPNs  0.0       0.0
175      enabled  FFW     6.0   2   FortiFirewall        Normal  Policy & Device VPNs  18.175    7.1924
181      enabled  FWC     6.0   2   FortiFirewallCarrier Normal  Policy & Device VPNs  18.175    7.1924
120      enabled  FML     6.0   0   FortiMail            Normal  Policy & Device VPNs  18.175    7.1924
132      enabled  FMG     6.0   4   FortiManager         Normal  Policy & Device VPNs  18.175    7.1704
142      enabled  FNA     8.0   7   FortiNAC             Normal  Policy & Device VPNs  0.0       0.0
140      enabled  FPX     1.0   2   FortiProxy           Normal  Policy & Device VPNs  0.0       0.0
134      enabled  FSA     3.0   1   FortiSandbox         Normal  Policy & Device VPNs  0.0       0.0
124      enabled  FWB     6.0   3   FortiWeb             Normal  Policy & Device VPNs  18.175    7.1924
130      enabled  LOG     0.0   0   Syslog               Normal  Policy & Device VPNs  0.0       0.0
155      enabled  FSF     6.0   4   Unmanaged_Devices    Normal  Policy & Device VPNs  18.175    7.1704
116      enabled  Chassis 6.0   0   Chassis              Normal  Policy & Device VPNs  18.175    7.1924
3        enabled  FSF     6.0   4   root                 Normal  Policy & Device VPNs  18.175    7.1704
10       enabled  FOS     6.0   4   Global               Normal  Policy & Device VPNs  18.175    7.1704
---End ADOM list---
```

As you can see, there are several ADOMs that FortiAnalyzer supports, each associated with different device types.

5. Close the FortiAnalyzer CLI window.

Create Custom ADOMs

Now that you enabled ADOMs on FortiAnalyzer, you can create your own custom ADOMs. In this exercise, you will create a Fabric ADOM and a FortiGate ADOM. (In *Lab 3*, you will add FortiGate devices to these ADOMs.)

You do not have to create ADOMs before you register devices to FortiAnalyzer—you can register devices to the default ADOMs first, and then move those devices into custom ADOMs later.

The benefit of creating custom ADOMs before device registration is that logs collected for the device that you add to the ADOM are stored on the ADOM from the beginning. If log collection begins in one ADOM, and then you move the device to a different ADOM, the analytics (indexed) logs are not automatically moved with the device. We will explore this scenario in *Lab 4*.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

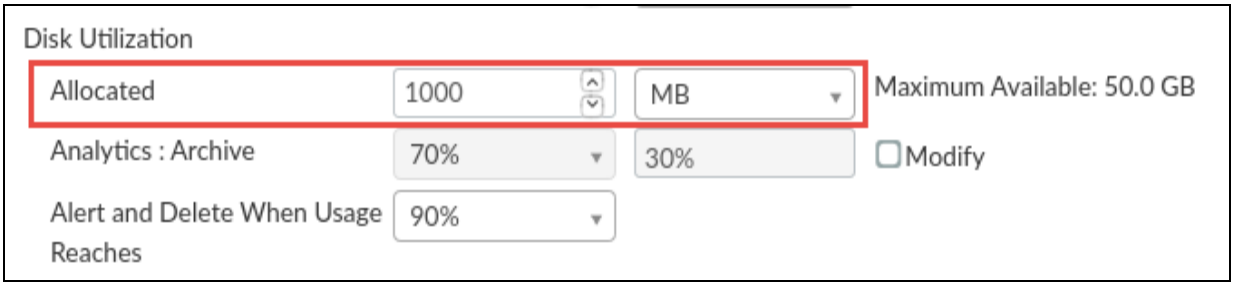
DO NOT REPRINT
© FORTINET
Brave-Dumps.com

To create custom ADOMs for FortiGate devices

1. Continuing on the FortiAnalyzer GUI, click **All ADOMs**.
2. Click **Create New** to create a custom ADOM.
3. On the **Create ADOM** window, configure the following settings:

Field	Value
Name	ADOM1
Type	Fabric

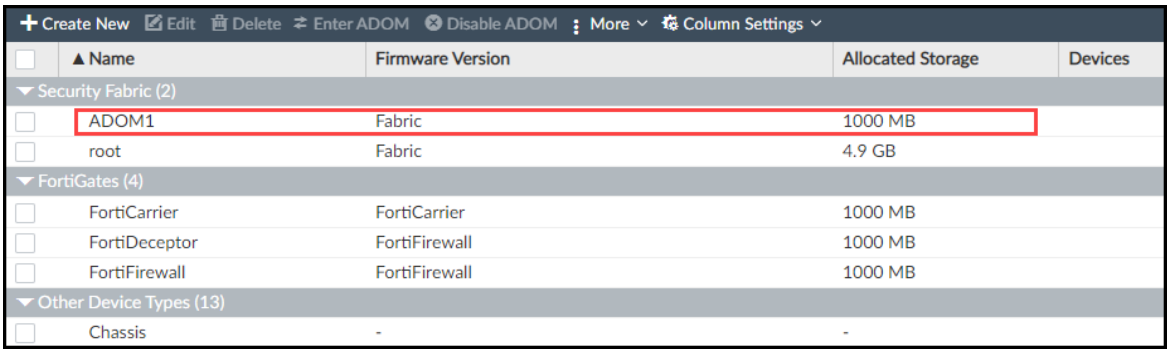
4. Click **Select Device**.
   If you had any devices registered to FortiAnalyzer, you could select them in the list, and then add them to the ADOM at this time. However, in this lab, you have not registered any devices yet, so the list is empty.
5. Click **Cancel**.
6. Review the information in the **Disk Utilization** section for the new ADOM.
   The default allocated space depends on the maximum available space.
7. Change the **Allocated** setting to **1000 MB**, and then click **OK**.



ADOM1, the Fabric ADOM you just created, now appears in the ADOM list. No registered devices are associated with **ADOM1** yet.

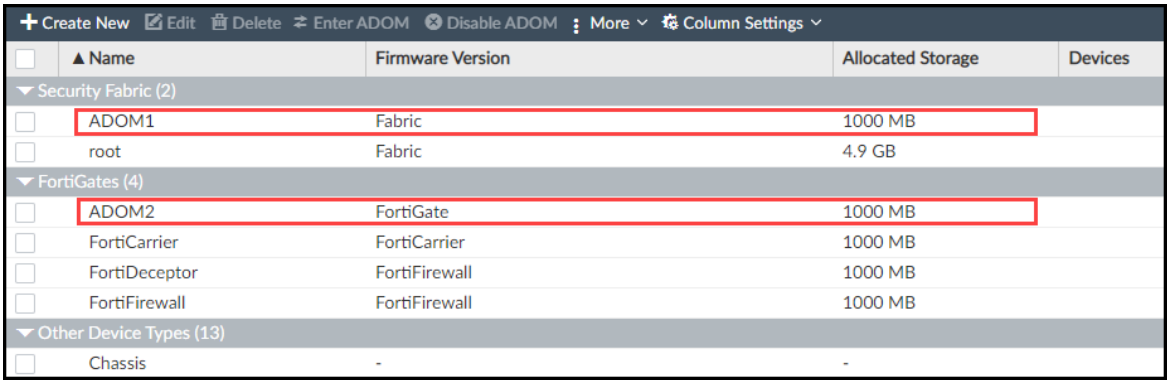
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



8. Repeat this procedure, but this time create a FortiGate ADOM called `ADOM2`, set **Type** to **FortiGate**, and set **Allocated** to **1000 MB**.

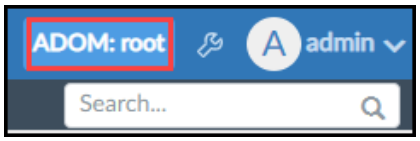
   Your ADOMs should now appear the same as the following example:



   You will add FortiGate devices to these ADOMs in *Lab 3*.

By default, FortiAnalyzer includes a root ADOM that is the Fabric type. Only FortiGate devices and devices in a Security Fabric can register to the root ADOM. Therefore, with ADOMs disabled, you cannot register a standalone device that is not a FortiGate on FortiAnalyzer.

You can switch between ADOMs on the GUI—you do not have to log out and log back in. To switch ADOMs on the GUI, click **ADOM** in the top-right corner of the GUI. Your administrator privileges determine which ADOMs you have access to.



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

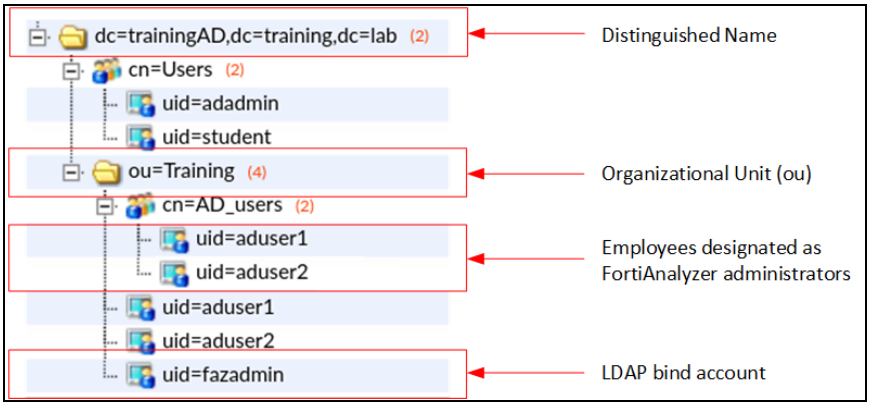
DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 2: Configuring an External Server to Validate Administrators

In this exercise, you will configure an external LDAP server on FortiAnalyzer to validate administrator logins. You will also create a new administrator account and permit LDAP group access by enabling the wildcard administrator account feature. You will also configure a wildcard administrator account for accessing a specific ADOM only.

Most companies, especially medium to large-sized companies, have employee accounts located in a central database, with employees as members of specific groups. As such, instead of managing employees designated as FortiAnalyzer administrators locally on FortiAnalyzer across multiple administrator accounts (as well as managing these employees in the organization's central database), you can configure one wildcard administrator account on FortiAnalyzer to point to an LDAP group the FortiAnalyzer administrators are members of. This allows you to have centralized control over your administrators.

For the purpose of this lab, an LDAP server with the following directory tree has been configured using FortiAuthenticator (10.0.1.150):



After you complete the configuration, you will verify that you can access FortiAnalyzer, and then you will check the event logs for details.

Configure an LDAP Server on FortiAnalyzer

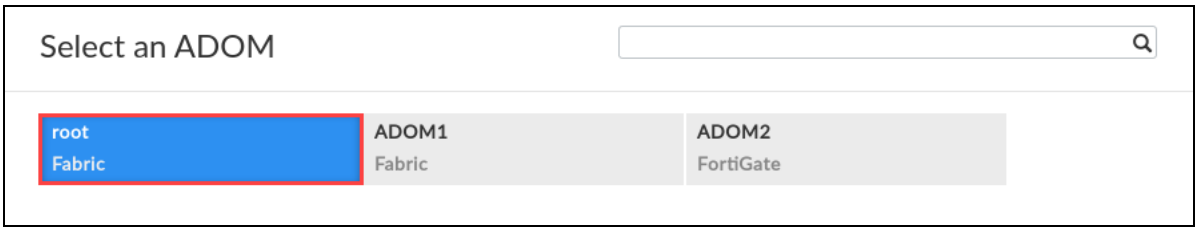
You will configure FortiAnalyzer to point to a preconfigured LDAP server.

To configure an LDAP server on FortiAnalyzer

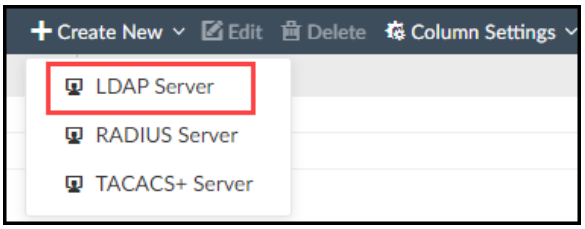
1. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. Click **root**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



3. Click **System Settings**.
4. In the menu on the left, click **Admin** > **Remote Authentication Server**.
5. Click **Create New**, and then in the dialog box that opens, click **LDAP Server**.



6. Configure the following settings:

You can copy the distinguished name (DN) and user DN from the `ADserver-info.txt` file by clicking **Desktop** > **Resources** > **FortiAnalyzer** > **LAB2**, opening the file, copying the information, and then pasting the information directly into the fields.

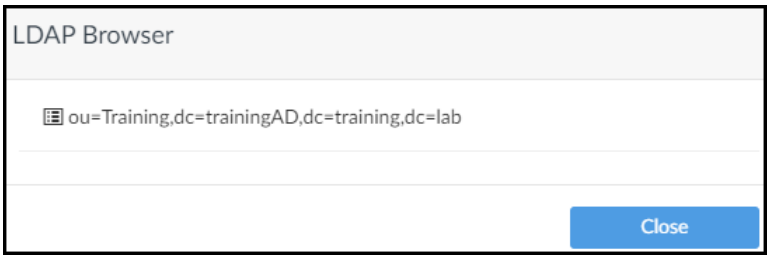
Field	Value
Name	External_Server
Server Name/IP	10.0.1.150 This is the IP address of the FortiAuthenticator acting as the LDAP server. For more information, see Network Topology on page 7.
Common Name Identifier	uid
Distinguished Name	ou=Training,dc=trainingAD,dc=training,dc=lab This is the domain name for the LDAP directory on FortiAuthenticator, with all users located under the **Training** organizational unit (ou).
Bind Type	Regular
User DN	uid=fazadmin,ou=Training,dc=trainingAD,dc=training,dc=lab fazadmin is the LDAP bind account. FortiAnalyzer uses these account credentials to authenticate against the LDAP server.
Password	Training!

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Field	Value
Administrative Domain	All ADOMs While this ensures that the LDAP server can provide administrator access to all ADOMs, it is ultimately the LDAP administrator account that determines which ADOMs are accessible.

7. Click the icon at the end of the **Distinguished Name** field to query the DN, and test your LDAP connection.
   If the connection is successful, you will see the DN in the **LDAP Browser** window. If you do not see the DN, verify that you configured the correct LDAP server information as outlined in the previous step.



8. Click **Close** to close the **LDAP Browser** window.
9. Click **OK** to accept your configuration.
   Your remote LDAP authentication server is added to FortiAnalyzer.

Create a Wildcard LDAP Administrator

You will create a new administrator account, and permit LDAP group access by enabling the wildcard administrator account feature.

To create a wildcard LDAP administrator

1. Continuing on the FortiAnalyzer GUI, click **Admin** > **Administrators**.
2. Click **Create New**.
3. Configure the following settings:

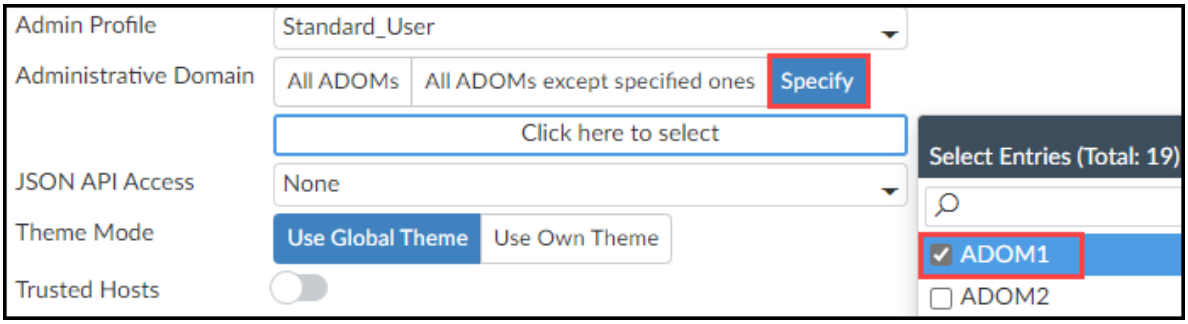
Field	Value
User Name	remote-admins
Admin Type	LDAP
LDAP Server	External_Server This is the LDAP server you created in the previous procedure.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

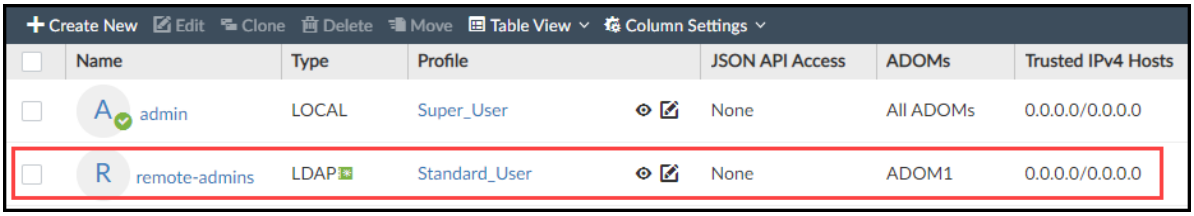
Field	Value
Match all users on remote server	<enable> This ensures that any user account located in the LDAP group (ou) you specified in the LDAP server configuration can authenticate.
Admin Profile	Standard_User This provides read/write access for all device privileges, but disables system privileges.

4. Beside **Administrative Domain**, click **Specify**, and then click **Click here to select**.
5. Select **ADOM1** in the drop-down list, and then click **OK**.



Even though you configured the LDAP server to access all ADOMs, this LDAP administrator account limits access to **ADOM1** only. This provides you with more flexibility and security because you can create additional LDAP administrator accounts for different ADOM access rights, if required.

6. Click **OK**.
   You successfully created a wildcard LDAP administrator.



7. Log out of FortiAnalyzer.

Test External Administrator Access

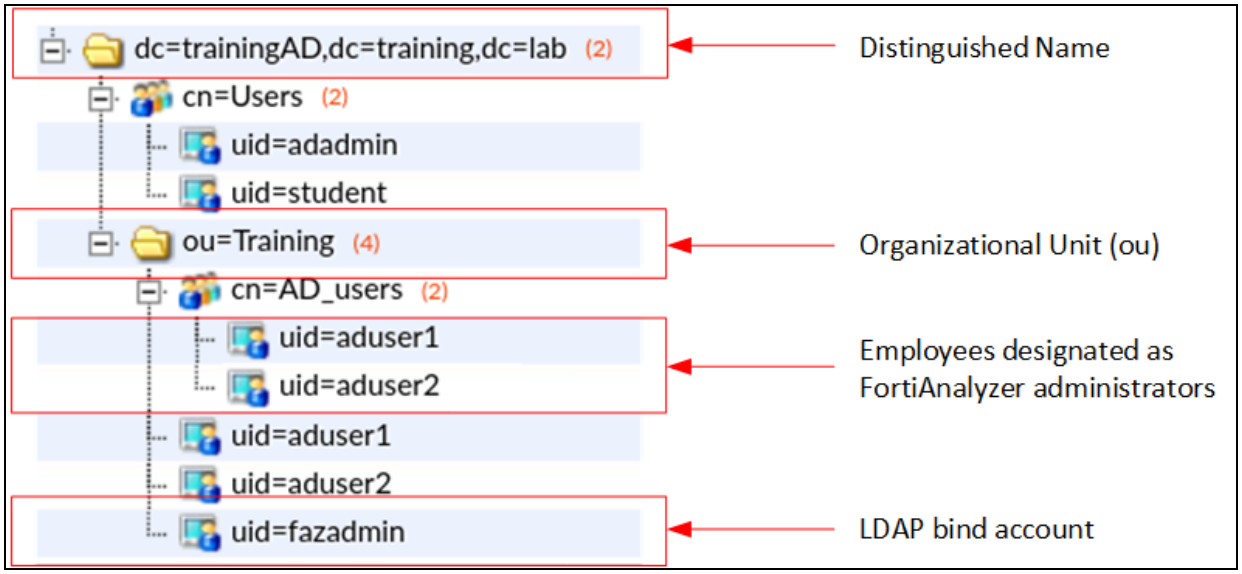
Now that you configured an external server, and created a wildcard administrator account that points to that external server, you are ready to test your configuration.

Based on the preconfigured LDAP server, you should be able to successfully authenticate with the following two users:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

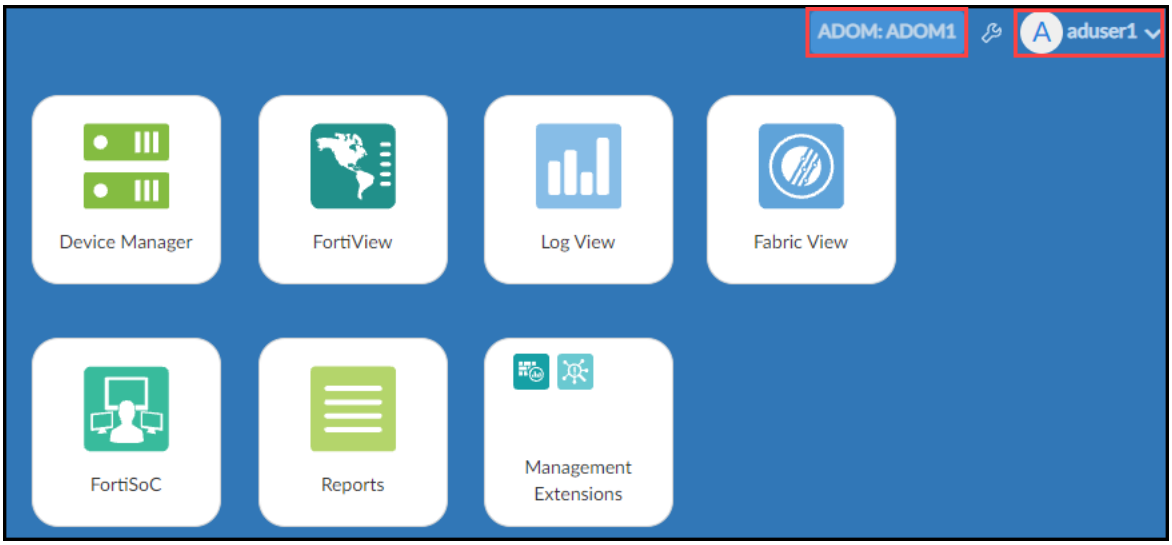
- aduser1
- aduser2



Also, since you gave this account the **Standard_User** profile and access to **ADOM1** only, you will notice a reduction in permissions (compared to the admin user account with the **Super_User** profile).

To test external administrator account access

1. Log in to the FortiAnalyzer GUI with the username `aduser1` and password `Training!`.
   You successfully logged in as an external administrator!



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Stop and think!

Since ADOMs are enabled, why do you not have to select an ADOM to log in to after authenticating?

You configured the **remote-admins** account with permission to access **ADOM1** only. Therefore, you are logged directly in to **ADOM1** (your only option).

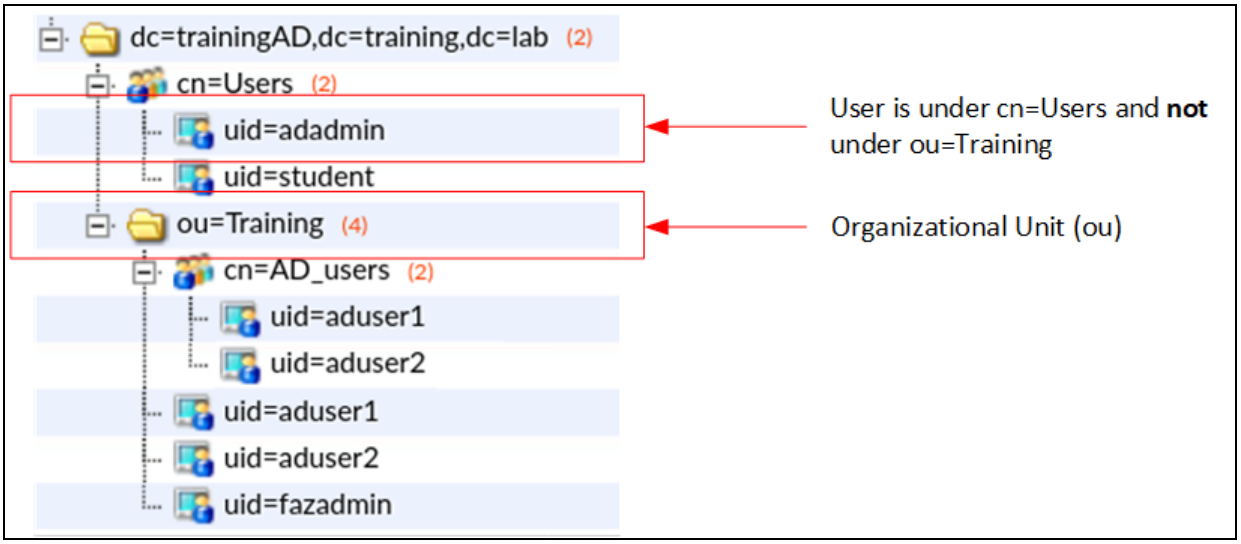
Why do you not have access to **System Settings**?

You configured the **remote-admins** account with the **Standard_User** profile. This profile does not provide system privileges.

2. Log out as **aduser1**, and then log in with the following credentials:
   - Username: `aduser2`
   - Password: `Training!`

   You successfully logged in as an external administrator.

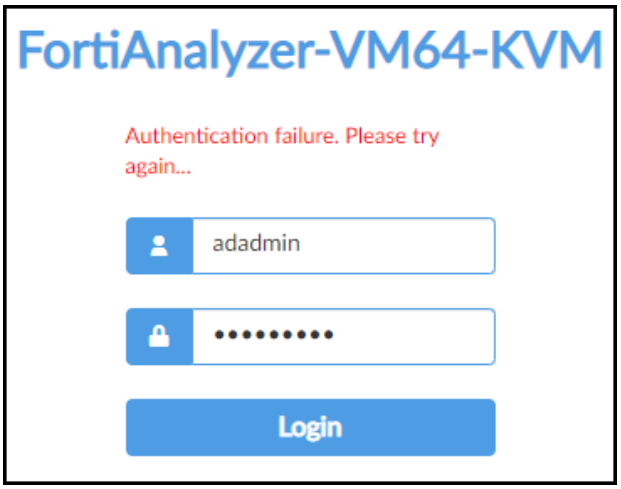
   Since you configured wildcard access on the **remote-user** administrator account, any user account located in the LDAP group (ou) you specified in the LDAP server configuration can authenticate. ADOM permissions and administrator privileges are the same for each user in the LDAP group.
3. Log out as **aduser2**.
4. Try to log in as a user located in the same LDAP server (`trainingAD.training.lab`), but in the **Users** organizational unit, not the **Training** organizational unit that you configured on FortiAnalyzer.
   - Username: `adadmin`
   - Password: `Training!`



Access is denied, because **adadmin** is not in an allowed LDAP group.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



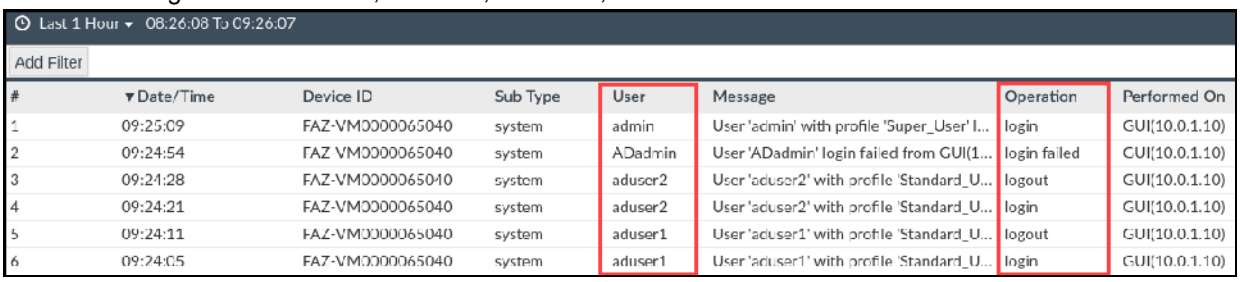
You successfully tested the external validation of administrators.

View the Event Logs

FortiAnalyzer audits administrator activity, so changes can be tracked. Review the event logs to see your recent administrator user activity.

To view the event logs

1. Log back in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. Click **root**.
3. Click **System Settings**.
4. In the menu on the left, select **Event Log**.
5. Examine the logins from **aduser1**, **aduser2**, **adadmin**, and **admin**.



6. Close your browser.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Lab 3: Device Registration and Communication

In this lab, you will register Local-FortiGate, ISFW, and Remote-FortiGate on FortiAnalyzer for the purpose of log collection.

After you register the devices, you will add them to the custom ADOMs you created in *Lab 2:* Administration and Management on page 17

Finally, you will run some diagnostics to troubleshoot device connection issues.

Objectives

- Register devices on FortiAnalyzer
- Troubleshoot device communication

Time to Complete

Estimated: 30 minutes

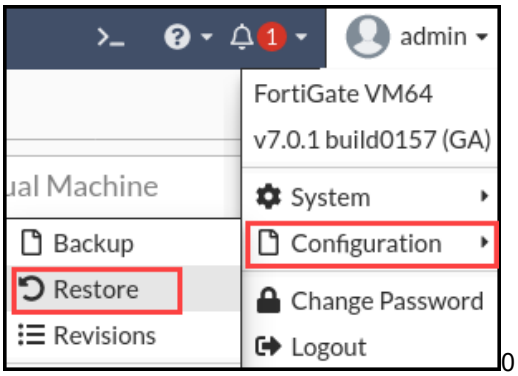
Prerequisites

Before beginning this lab, you must restore a configuration file to Local-FortiGate and ISFW.

To restore the ISFW configuration file

Make sure you restore the correct configuration file on the correct device. The name of the configuration file matches the name of the device that it must be restored on.

1. On the Local-Client VM, open a browser, and then log in to the ISFW GUI at `10.0.1.200` with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **FortiAnalyzer** > **LAB-3** > `ISFW.conf`, and then click **Open**.

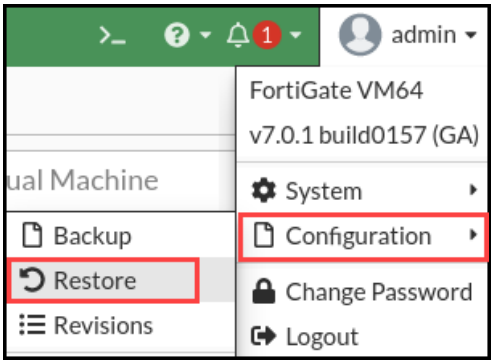
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

5. Click **OK**.
6. Click **OK** to reboot.

To restore the Local-FortiGate configuration file

1. On the Local-Client VM, open a browser, and then log in to the Local-FortiGate GUI at `10.0.1.254` with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



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

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 1: Registering Devices on FortiAnalyzer

In this exercise, you will register Remote-FortiGate on one ADOM, and Local-FortiGate and ISFW on another ADOM, using different methods of device registration.

One use case for adding FortiGate devices to different ADOMs is to manage data policies and disk space allocation more efficiently, because these features are set for each ADOM, and not for each device.

For example, if you know (or have identified over time) that one of your FortiGate devices receives a higher volume of traffic than another (such as a core FortiGate rather than an internal FortiGate), you may not want both devices to share the allocated disk space.

Register a Device Using the Add Device Wizard

You will use the **Add Device** wizard to add Remote-FortiGate to **ADOM2** in FortiAnalyzer.

You will need the serial number of Remote-FortiGate for device registration. You can gather this information by logging in to the Remote-FortiGate GUI at `10.200.3.1` with the username `admin` and password `password`.

To register Remote-FortiGate from FortiAnalyzer

1. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. Click **ADOM2**.

This ensures that Remote-FortiGate will be registered to ADOM2.

3. Click **Device Manager**.
4. Click **Add Device**.

5. Configure the following settings:

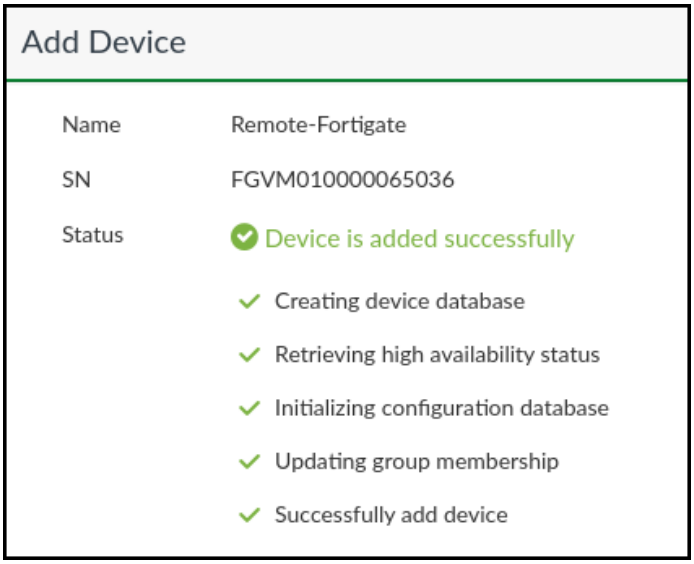
Field	Value
Name	Remote-FortiGate

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

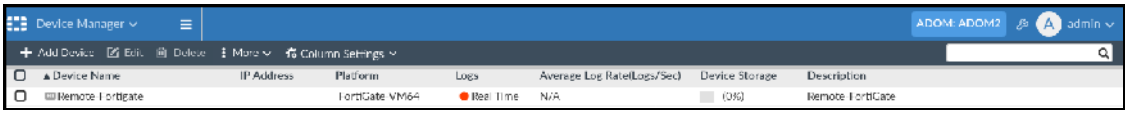
DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Field	Value
Link Device by	Serial Number
Serial Number	This is the serial number of the FortiGate. You can find this serial number on the dashboard of Remote-FortiGate.
Device Model	This is automatically populated as you type the serial number.
Description	Remote-FortiGate. (This field is optional but recommended.)

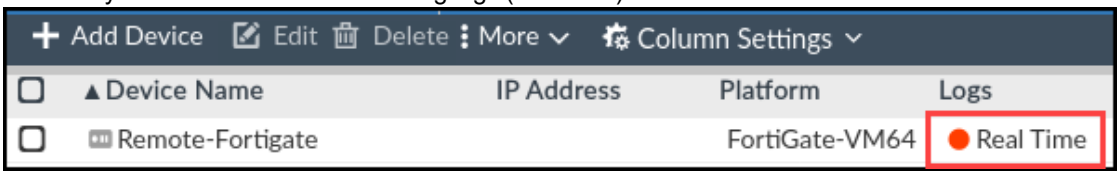
6. Click **Next**.
   A success message appears.



7. Click **Finish**.
   Device Manager indicates that Remote-FortiGate is now a registered device.



8. Examine the **Logs** column.
   FortiAnalyzer indicates it is not receiving logs (red circle).



   You will diagnose this issue later in this lab.

9. Log out of FortiAnalyzer.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

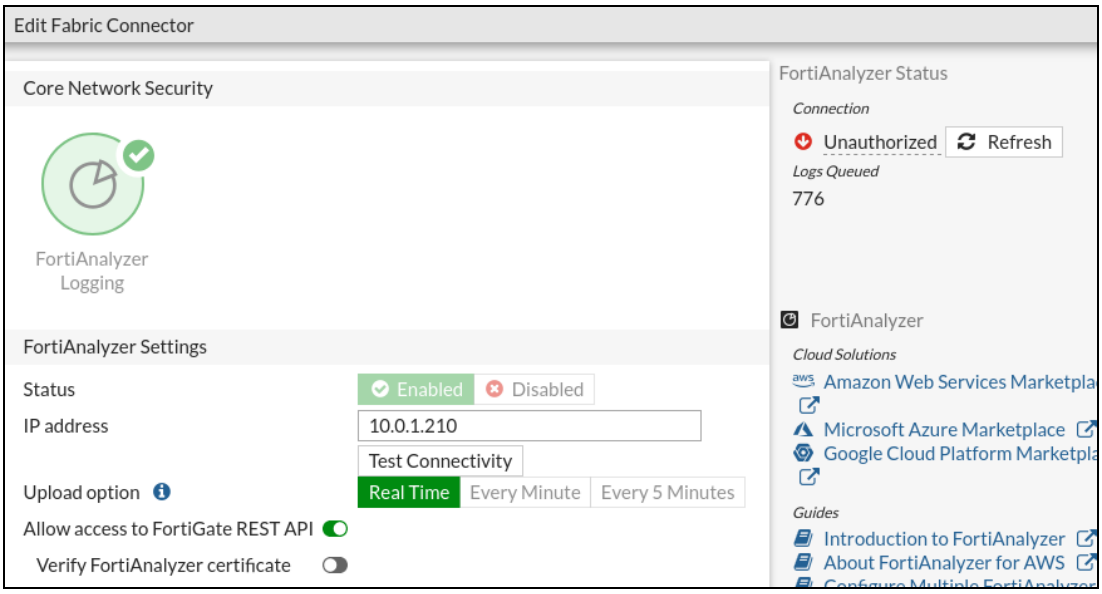
Accept a Device Registration Request

In this scenario, you will review the preconfigured Fortinet Security Fabric on ISFW and Local-FortiGate. Both FortiGate devices have requested registration on FortiAnalyzer. This was part of the configuration you restored at the beginning of this lab. You must review and accept the connection requests. After you accept the requests, the devices will be registered.

If you use this registration method, you do not need to use the **Add Device** wizard to register a device, as you did in the previous procedure.

To review the Security Fabric settings on ISFW and Local-FortiGate

1. Log in to the Local-FortiGate GUI with the username `admin` and password `password`.
2. In the menu on the left side of the window, click **Security Fabric** > **Fabric Connectors**.
3. Select **FortiAnalyzer Logging**, and then click **Edit** to review the configuration on Local-FortiGate.



4. Log out of Local-FortiGate.
5. Log in to the ISFW GUI with the username `admin` and password `password`.
6. In the menu on the left, click **Security Fabric** > **Fabric Connectors**.
7. Select **FortiAnalyzer Logging**, and then click **View** to review the configuration.
8. Log out of ISFW.

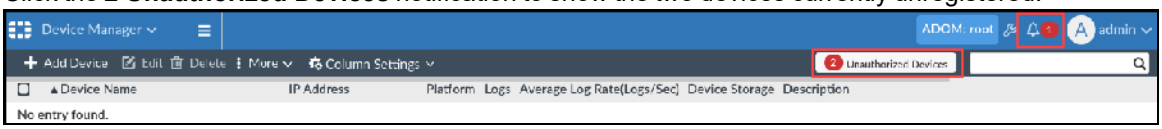
To accept a device registration request

1. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. Click **root**.
   All FortiGate registration requests go to the root ADOM.
3. Click **Device Manager**.
   A notification about the unregistered devices is displayed in two locations.

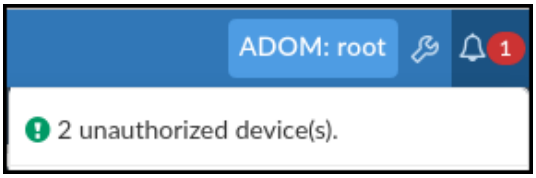
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

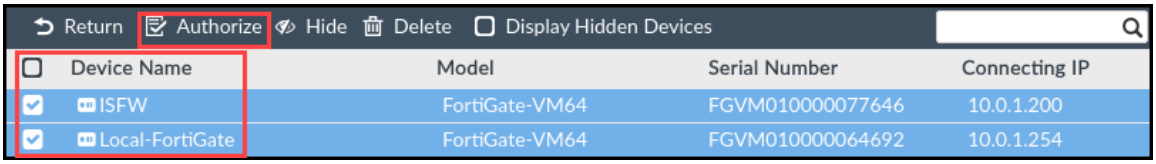
4. Click the **2 Unauthorized Devices** notification to show the two devices currently unregistered.



You can also click the notification bell, and then click the warning message to display the devices.

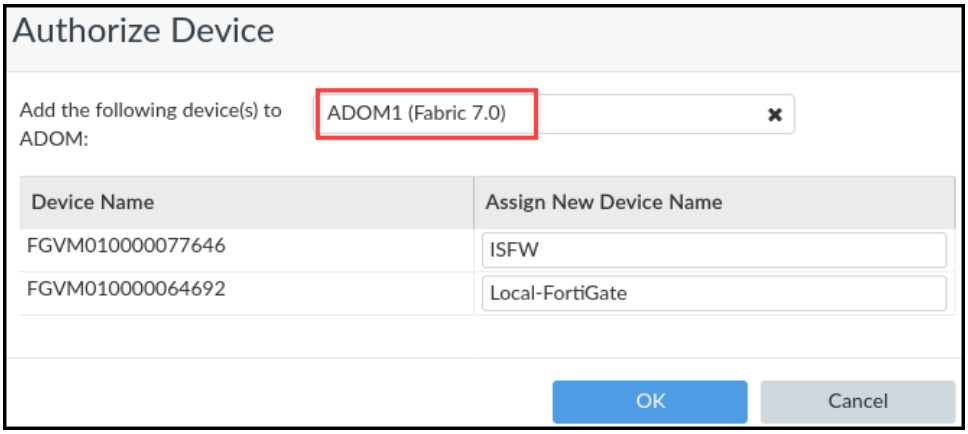


5. Select both FortiGate devices, and then click **Authorize**.

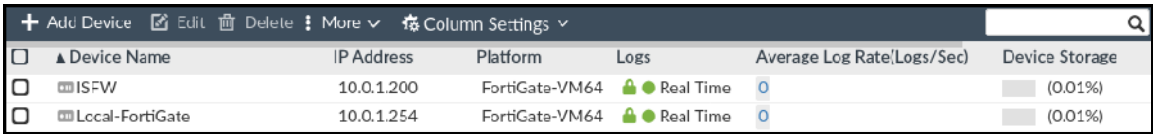


The **Authorize Device** window opens. Since ADOMs are enabled, and you created additional ADOMs, you now have the ability to select which ADOM you want to register the devices on.

6. Select **ADOM1**, and then click **OK**.



7. Click **Close**.
8. Switch to **ADOM1**.



Both devices are now registered.

Initially, the values under the **Logs** and **Average Log Rate** columns might be different from the image above. You may need to refresh the page a couple of times to get the same results.

FortiAnalyzer indicates that it is now receiving logs (green circle) from both devices.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Stop and think!

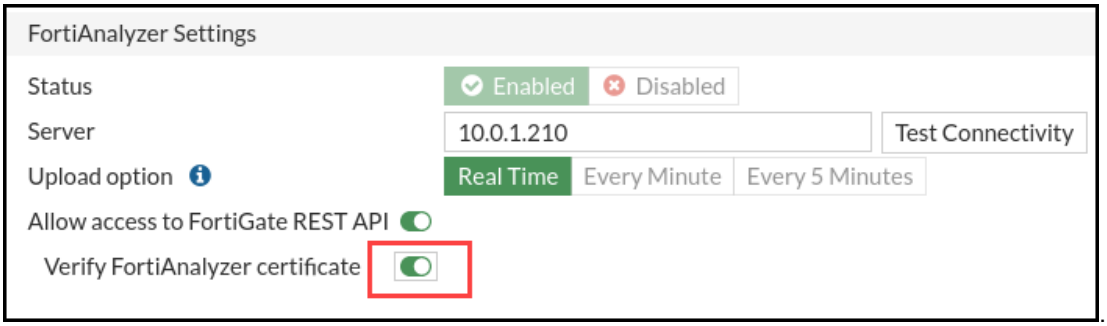
Why does FortiAnalyzer indicate that it is receiving logs from Local-FortiGate and ISFW (green circle), but not from Remote-FortiGate (red circle)? You will diagnose this issue next.

What is indicated by the green lock under the **Logs** columns for ISFW and Local-FortiGate?

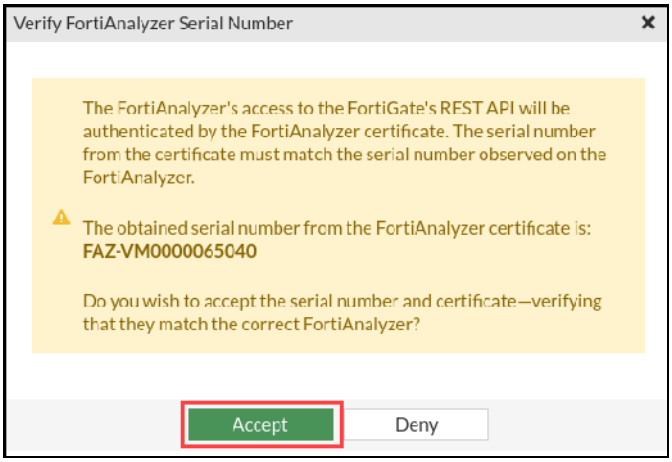
This means that the logs are being encrypted so they are transferred securely to FortiAnalyzer.

To validate the FortiAnalyzer certificate

1. Log in to the Local-FortiGate GUI with the username `admin` and password `password`.
2. In the menu on the left, click **Security Fabric** > **Fabric Connectors**.
3. Select **FortiAnalyzer Logging**, and then click **Edit** to review the configuration on Local-FortiGate.
4. Enable **Verify FortiAnalyzer certificate**, and then click **OK**.



5. Click **Accept**.



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 2: Troubleshooting Device Communication

In the Device Manager of all the registered devices, you saw an indication that Local-FortiGate, ISFW, and Remote-FortiGate have different statuses with FortiAnalyzer.

FortiAnalyzer showed it was receiving logs successfully from Local-FortiGate and ISFW, but not from Remote-FortiGate.

Now, you will troubleshoot the issue.

Verify Device Registration

A quick way to verify device registration with FortiAnalyzer is to use the `diagnose dvm device list` command. This command provides the serial number, IP address, name, and registered ADOM for each device added.

To verify device registration information

1. On the FortiAnalyzer CLI, log in with the username `admin` and password `password`.
2. Run the following command to view which ADOM your devices are currently registered on:

The CLI output formatting is easier to read if you maximize your window.

```
# diagnose dvm device list
```

```
FAZVM64-KVM # diagnose dvm device list
--- There are currently 3 devices/vdoms managed ---
    There are currently 3 devices/vdoms count for license

TYPE            OID    SN              HA      IP              NAME                            ADOM    IPS    FIRMWARE
faz-managed     207    FGVM010000077546 -      10.0.1.200      ISFW                            ADOM1   N/A    7.0 MR0 (157)
                |- STATUS: dev-db: unknown; conf: unknown; cond: unknown; dm: none; conn: unknown
                |  vdom:[3]root flags:0 adom:ADOM1 pkg:[never installed]
faz-managed     219    FGVM010000064692 -      10.0.1.254      Local-FortiGate                 ADOM1   N/A    7.0 MR0 (157)
                |- STATUS: dev-db: unknown; conf: unknown; cond: unknown; dm: none; conn: unknown
                |- vdom:[3]root flags:0 adom:ADOM1 pkg:[never-installed]
faz-managed     231    FGVM010000065036 -                      Remote-FortiGate                ADOM2   N/A    6.0 MR0 (443)
                |  STATUS: dev db: unknown; conf: unknown; cond: unknown; dm: unknown; conn: unknown
                |- vdom:[3]root flags:0 adom:ADOM2 pkg:[never-installed]

--- There are currently 0 FortiAP managed ---

--- There are currently 0 FortiSwitch managed ---

--- There are currently 0 FortiExtender managed ---
--- End device list ---
```

The output indicates that there are three devices currently registered: ISFW (`10.0.1.200`) and Local-FortiGate (`10.0.1.254`) on **ADOM1**, and Remote-FortiGate (IP is not displayed) on **ADOM2**.

Initially, the entry for Remote-FortiGate displays a firmware version 6.0 because it was added from FortiAnalyzer using the add device wizard. The correct firmware version will be displayed after completing the registration process later in the lab.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Verify Device Communication

Just because a device is successfully added to FortiAnalyzer, does not mean there is successful communication between the devices. As you have identified, Remote-FortiGate is registered with FortiAnalyzer, but log communication is down.

To verify FortiAnalyzer log connectivity from the FortiGate side

1. On the Remote-FortiGate CLI, log in with the username `admin` and password `password`.
2. Run the following command to view log connectivity to FortiAnalyzer:

```
# execute log fortianalyzer test-connectivity
```

The output should indicate that logging to FortiAnalyzer is not enabled.

```
Remote-FortiGate # execute log fortianalyzer test-connectivity
No FAZ is enabled.
```

This result should be enough to conclude the problem is with Remote-FortiGate. However, we will run a few more commands to verify this conclusion.

3. Leave the Remote-FortiGate CLI session open because you will use it again soon.
4. On the ISFW CLI, log in with the username `admin` and password `password`.
5. Run the following command to view log connectivity to FortiAnalyzer:

```
# execute log fortianalyzer test-connectivity
```

The output should indicate that logging connectivity is allowed.

```
ISFW # execute log fortianalyzer test-connectivity
FortiAnalyzer Host Name: FortiAnalyzer
FortiAnalyzer Adom Name: ADOM1
FortiGate Device ID: FGVM010000077646
Registration: registered
Connection: allow
Adom Disk Space (Used/Allocated): 602908B/1048576000B
Analytics Usage (Used/Allocated): 582428B/734003200B
Analytics Usage (Data Policy Days Actual/Configured): 0/60 Days
Archive Usage (Used/Allocated): 20480B/314572800B
Archive Usage (Data Policy Days Actual/Configured): 76/365 Days
Log: Tx & Rx (2 logs received since 16:06:27 08/26/21)
IPS Packet Log: Tx & Rx
Content Archive: Tx & Rx
Quarantine: Tx & Rx
```

These results confirm that the issue exists on the Remote-FortiGate side, not the FortiAnalyzer side.

Troubleshoot Device Communication

So far, diagnostics indicate that logging connectivity is not enabled on Remote-FortiGate.

A quick way to verify connectivity between FortiAnalyzer and the logging devices is to run some tests for the `oftpd` process. This should also confirm the logging connectivity results from the previous steps.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

To verify which devices are connecting to FortiAnalyzer

1. Continuing on the FortiAnalyzer CLI session, enter the following command to display the devices that are communicating with FortiAnalyzer:

```
# diagnose test application oftpd 3
```

2. Is Remote-FortiGate listed in the output?

```
FortiAnalyzer # diagnose test application oftpd 3
 #   SN                HOSTNAME          IP           UPTIME      IDLETIME   #PKTS
-------------------------------------------------------------------------------------
 1   FGVM010000077646  ISFW              10.0.1.200   11h36m21s   4s         8653
 2   FGVM010000064692  Local-FortiGate   10.0.1.254   11h36m50s   3s         8642
 3   FGVM010000077646  ISFW              10.0.1.200   11h36m21s   5s         8896
 4   FGVM010000064692  Local-FortiGate   10.0.1.254   11h36m50s   3s         9373

FortiAnalyzer #
```

Only ISFW and Local-FortiGate have established a connection with FortiAnalyzer—Remote-FortiGate has not.

Resolve a Connection That Is Down

Since Remote-FortiGate was the device you registered on the FortiAnalyzer side (using the **Add Device** wizard), you should check the following:

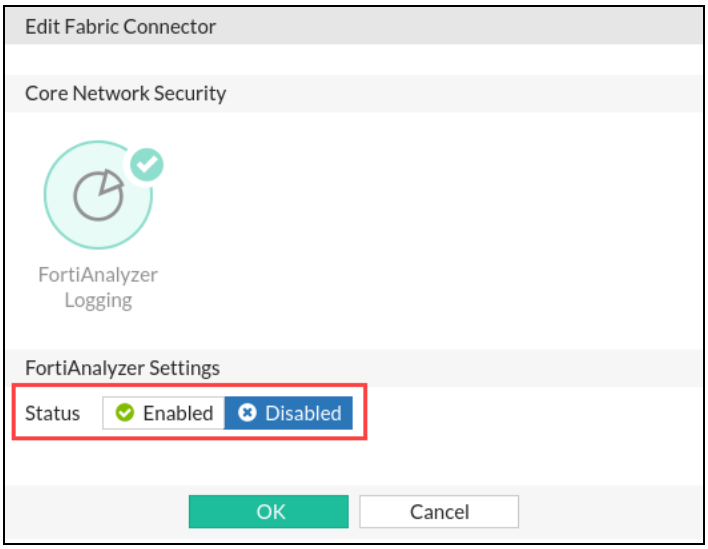
- Is Remote-FortiGate enabled for remote logging to FortiAnalyzer?
- What are the logging filters on Remote-FortiGate?

To resolve a connection that is down

1. Log in to the Remote-FortiGate GUI with the username `admin` and password `password`.
2. In the menu on the left, click **Security Fabric** > **Fabric Connectors**.
3. Select **FortiAnalyzer Logging**, and then click **Edit** to examine the **FortiAnalyzer Logging** settings.
   Is remote logging to FortiAnalyzer enabled and configured?

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



FortiAnalyzer logging is not enabled.

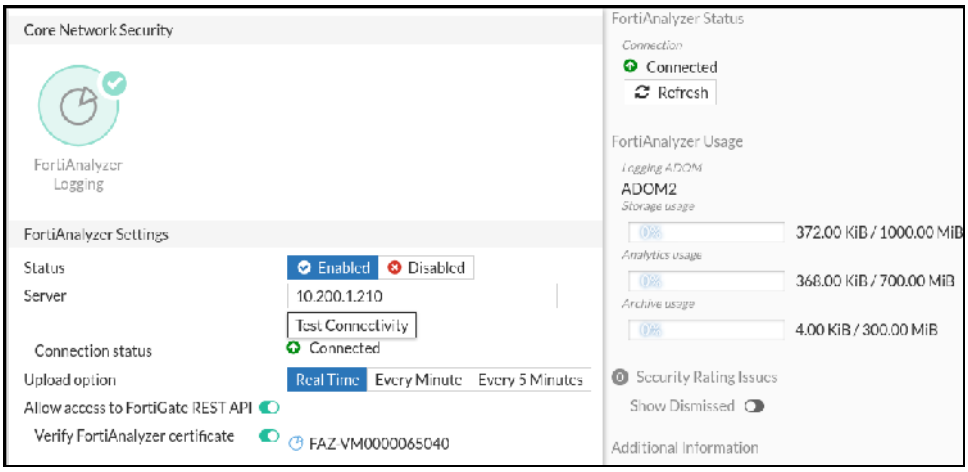
4. Enable **FortiAnalyzer Logging**.
5. Configure the following settings:

Field	Setting
IP Address	`10.200.1.210` This is the IP address of the FortiAnalyzer for Remote-FortiGate.
Upload Option	Realtime For the purposes of this lab, we are using real-time so you can see the logs instantly.
Verify FortiAnalyzer certificate	Enabled

6. Click **OK**, and then click **Accept** to save the settings.
7. Click **FortiAnalyzer Logging** > **Edit**.
8. In the **FortiAnalyzer Settings** section, click **Test Connectivity**.
   The test should be successful, which proves the devices are connected.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

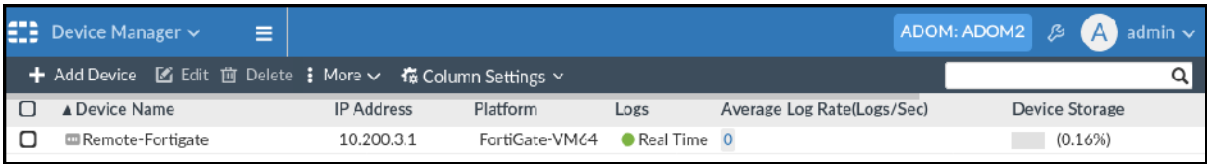


9. Run the `# diagnose test application oftpd 3` command again to verify Remote-FortiGate is now listed in the output.

```
FortiAnalyzer # diagnose test application oftpd 3
 #   SN                 HOSTNAME          IP           UPTIME      IDLETIME   #PKTS
---------------------------------------------------------------------------------------
 1   FGVM010000065036   Remote-FortiGate  10.200.3.1   18s         13s        3
 2   FGVM010000077646   ISFW              10.0.1.200   11h54m19s   1s         8875
 3   FGVM010000064692   Local-FortiGate   10.0.1.254   11h54m48s   5s         8863
 4   FGVM010000065036   Remote-FortiGate  10.200.3.1   18s         17s        3
 5   FGVM010000077646   ISFW              10.0.1.200   11h54m19s   2s         9115
 6   FGVM010000064692   Local-FortiGate   10.0.1.254   11h54m48s   5s         9592
```

10. Log out of Remote-FortiGate.
11. Continuing on the FortiAnalyzer GUI, select **ADOM2**.
12. Click (or refresh) **Device Manager**.

    In the registered device **Logs** column, does FortiAnalyzer indicate it is receiving logs from Remote-FortiGate (green circle)?



Stop and think!

If you followed all steps in the lab, you will notice that the logs sent from Remote-FortiGate are not encrypted. What must you do to secure the log traffic?

To encrypt the log traffic, you must run the following commands on Remote-FortiGate:

```
# config log fortianalyzer setting
(setting)# set reliable enable
```

These commands were included in the configurations that you restored at the beginning of the lab for Local-FortiGate and ISFW.

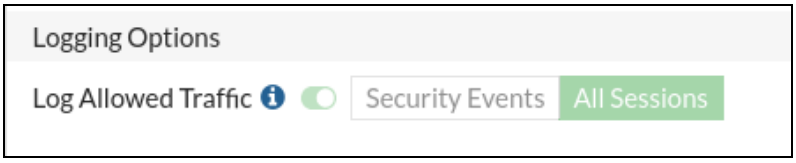
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

You can run the `execute log fortianalyzer test-connectivity` command on Remote-FortiGate again to see that log connectivity is enabled.

13. **Optional** It is always a good idea to check your logging filters on the FortiGate firewall policies to ensure you receive the logs you are expecting:
    a. Log in to the Local-FortiGate GUI with the username `admin` and password `password`.
    b. Click **Policy & Objects** > **Firewall Policy**.
    c. Review the **Logging Options** section for all the policies.

    You should see **All Sessions** enabled for both policies, and some security profiles enabled. While logging all sessions requires more system resources and storage space, it is a good option when you want to verify that logging was set up successfully.



14. Close the browser.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Lab 4: Logs

In this lab, you will generate some traffic so you can see where logs are stored on FortiAnalyzer, what information is included in logs, and different ways of viewing log data. Before you generate traffic, you will gather information about your FortiAnalyzer performance benchmarks and log storage policies.

After traffic has passed through the network for a while, you will examine the used storage statistics, and then modify the ADOM disk quota based on this information.

Objectives

- Gather benchmark diagnostics
- Examine logs
- Gather logs statistics and used storage information
- Modify the disk quota
- Move a device to a different ADOM

Time to Complete

Estimated: 75 minutes

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 1: Gathering Benchmark Diagnostics

Before you start generating traffic, you should be aware of the system resources for FortiAnalyzer and the log storage policies. This can help you correctly manage your device and the logs that are stored.

View System Resource Information

You can view the real-time and historical usage status of the CPU, memory, and hard disk on FortiAnalyzer. You can monitor these statistics over time to see how your device is performing.

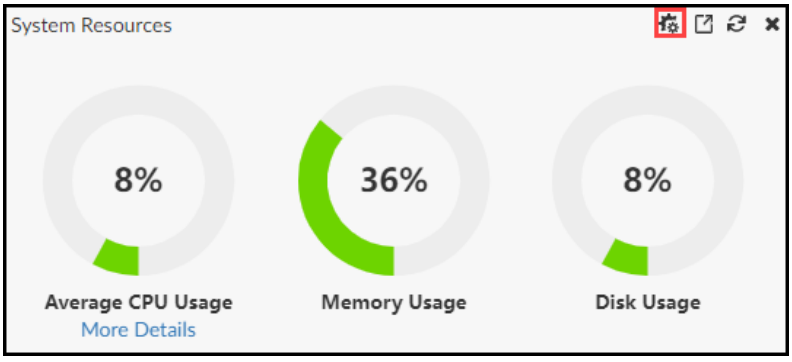
You can also use the FortiAnalyzer `get system status` and `get system performance` CLI commands to view this information.

To view system performance information

1. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. Click **ADOM1**.
3. Click **System Settings**.
4. On the dashboard, examine the **System Resources** widget.
   You can click the refresh icon to get the latest statistics.

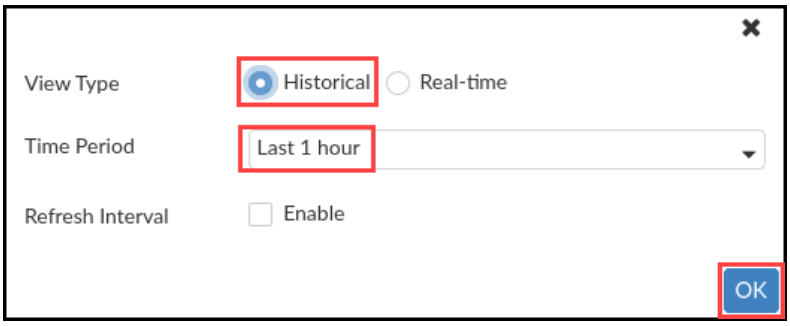
Diagnostic	Result
What is the average CPU usage?	
What is the memory usage?	
What is the disk usage?	

5. Click the **Settings** icon to view the historical usage over the past hour.



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



6. Click **OK**.

Gather Data Policy and Disk Utilization Information

You should also be aware of your disk quota for each ADOM. This can help prevent any log storage issues that may occur, especially if some devices produce a high volume of logs.

You can also use the `diagnose log device` CLI command to obtain this information.

To check log storage information

1. Continuing on the FortiAnalyzer GUI (ADOM1), click **System Settings**.
2. In the menu on the left, click **Storage Info**.
3. Double-click (or edit) **ADOM1**, and then view the data policy and disk utilization policies.

How long are logs configured to be kept in the SQL database (**Keep Logs for Analytics**)? This is the number of days that you can view information about the logs on **FortiView**, **Event Monitor**, and **Reports**. After the specified amount of time expires, logs are automatically purged from the SQL database.
How long are logs configured to be kept in the compressed state (**Keep Logs for Archive**)? When logs are in the compressed state, you cannot view information about the log messages on **FortiView**, **Event Monitor**, and **Reports**. After the specified amount of time expires, archive logs are automatically deleted from FortiAnalyzer.
What is the maximum amount of FortiAnalyzer disk space available to use for logs (**Maximum Available**)? Note: The reserved space is already deducted from this total.
How much disk space is allocated to ADOM1?

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

What is the allotted disk space percentage available for indexed (analytics) and compressed (archive) logs? Analytics logs require more space than archive logs.
At what percentage are alert messages to be generated and logs automatically deleted? The oldest archive log files or analytics database tables are deleted first.

The log storage information for ADOM2 is the same because both ADOMs are configured with the same data policy and disk utilization settings.

4. Click **Cancel** to close the window.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 2: Generating Traffic

For the purposes of this lab, you must generate traffic so you can see the logs that FortiAnalyzer receives.

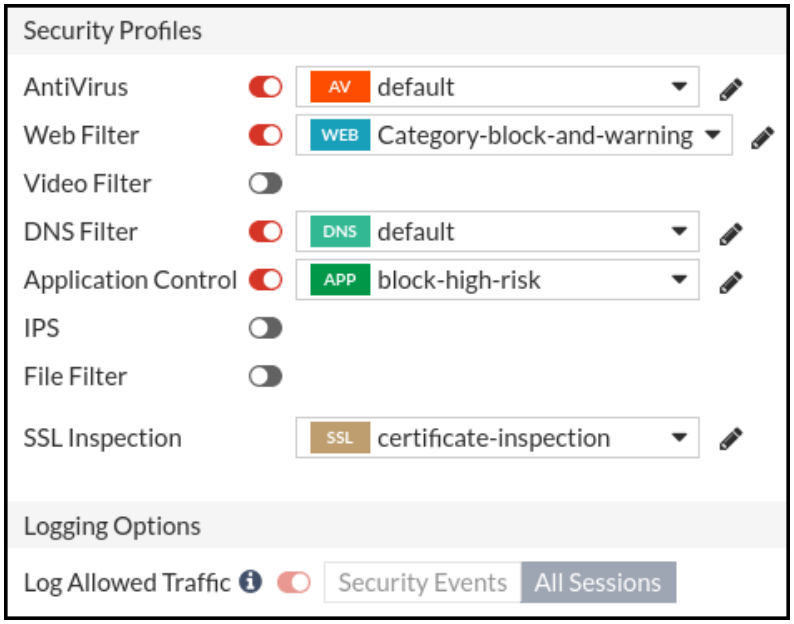
The traffic you generate will go through ISFW and Local-FortiGate. The firewall policies were preconfigured for you, and logging for all sessions is enabled. To view the firewall policies on the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.

You will use two different tools to generate different types of traffic.

Generate Traffic Using FIT

The firewall inspection tester (FIT) VM generates web browsing traffic, application control, botnet IP hits, malware URLs, and malware downloads.

In this lab, you will direct FIT-generated traffic through the ISFW **Full_Access** firewall policy. This firewall policy was preconfigured for you, and includes the following security policies and logging options:



Because FIT-generated traffic will originate from the IP address of the FIT VM (`10.0.3.20`), all of these logs will show the same source IP address in the FortiAnalyzer logs. This is a limitation of the lab environment. In a real-world scenario, you will likely see many different source IP addresses for your traffic.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

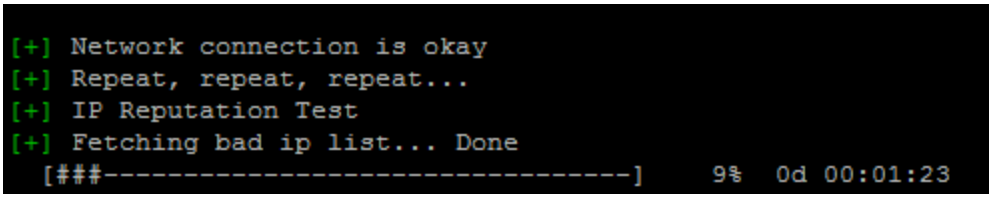
DO NOT REPRINT
© FORTINET
Brave-Dumps.com

To generate traffic using FIT

1. On the Local-Client VM, open PuTTY, and then connect to the FIT saved session (connect over SSH).
2. Log in with the username `student` and password `password`.
3. Enter the following command to run a script that changes the default route of FIT to send traffic through ISFW (see Network Topology on page 7):
   ```
   $ sudo ./default3
   ```
4. When prompted, enter the password again.
5. Enter the following command to check the default route:
   ```
   $ ip route
   ```
   You should see the default route through `10.0.3.254`.
6. Enter the following commands:

   ```
   # cd FIT

   # ./fit.py all --repeat
   ```

   Traffic will begin to generate, and the script will repeat each time it completes.

7. Leave the PuTTY session open (you can minimize it), so that traffic continues to generate. This will run throughout the remainder of the lab.

Do not close the FIT PuTTY session or traffic will stop generating.

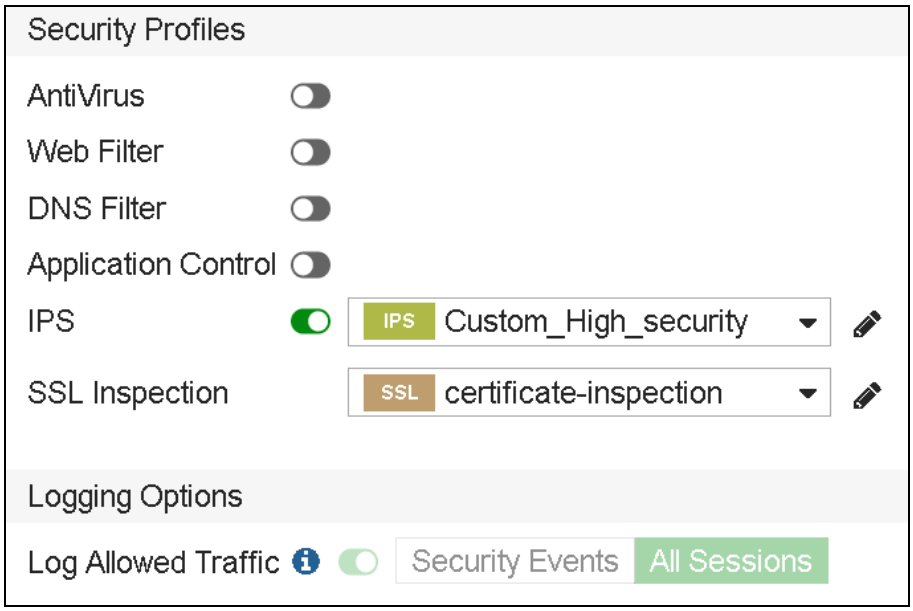
Generate Traffic Using Nikto

Nikto generates intrusion prevention system (IPS) traffic.

You will direct the traffic that Nikto generates through the Local-FortiGate **IPS-traffic-policy** firewall policy. This firewall policy was preconfigured for you, and includes the following security policies and logging options:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



Because the traffic that Nikto generates originates from the IP address of the Linux VM where Nikto is installed (`10.200.1.254`), all of these logs will show the same source IP address in the FortiAnalyzer logs. This is a limitation of the lab environment. In a real-world scenario, you will likely see many different source IP addresses for your traffic. Note that `10.200.1.10` is a virtual IP configured on Local-FortiGate.

To generate traffic using Nikto

1. Continuing on the Local-Client VM, open a second PuTTY application, and then connect to the LINUX saved session (connect over SSH).
2. Log in with the username `student` and password `password`.
3. Enter the following command:

   ```
   nikto.pl -host 10.200.1.10
   ```

   The script starts generating traffic.

```
- ***** SSL support not available (see docs for SSL install) *****
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          10.200.1.10
+ Target Hostname:    10.200.1.10
+ Target Port:        80
+ Start Time:         2017-03-17 06:58:33 (GMT-7)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/8.5
+ Server leaks inodes via ETags, header found with file /, fields: 0x35e578bc95b
2d11:0
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server banner has changed from 'Microsoft-IIS/8.5' to 'Microsoft-HTTPAPI/2.0'
which may suggest a WAF, load balancer or proxy is in place
```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

The scan will continue for approximately 25 minutes. When the scan is complete, the window displays an end time and indication that one host has been tested.

```
+ End Time:           2017-03-17 07:33:35 (GMT-7) (2102 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

You can run the command again. Press the up arrow, and then press `Enter` to generate more logs—however, this is not required. One cycle provides enough logs for the purposes of this lab.

4. Leave the PuTTY session open (you can minimize it), so that traffic continues to generate. This will run for the remainder of the lab.

Do not close the LINUX PuTTY session or traffic will stop generating.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 3: Examining Logs

There are many ways to view logs in FortiAnalyzer. In this exercise, to familiarize yourself with the options available, you will explore the following different views:

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

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

View Logs in Log View

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

When ADOMs are enabled, each ADOM has its own information displayed in **Log View**.

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

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

In this exercise, you will examine traffic logs and security logs only.

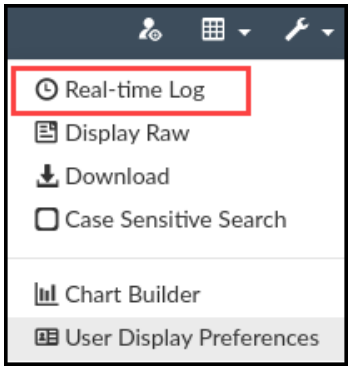
To view logs in Log View

1. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. Select **ADOM 1**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

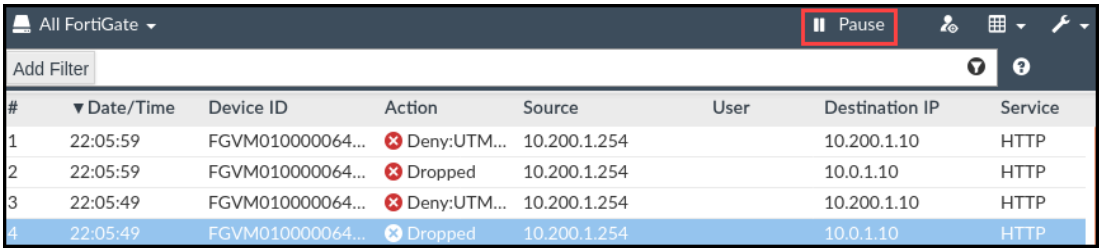
3. Click **Log View**.
4. In the menu on the left, select **FortiGate** > **Traffic**.
5. Explore the different ways of viewing logs, such as real time, historical, and raw.
   - On the upper-right side of the GUI, click **Tools** > **Real-time Log**.



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

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

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



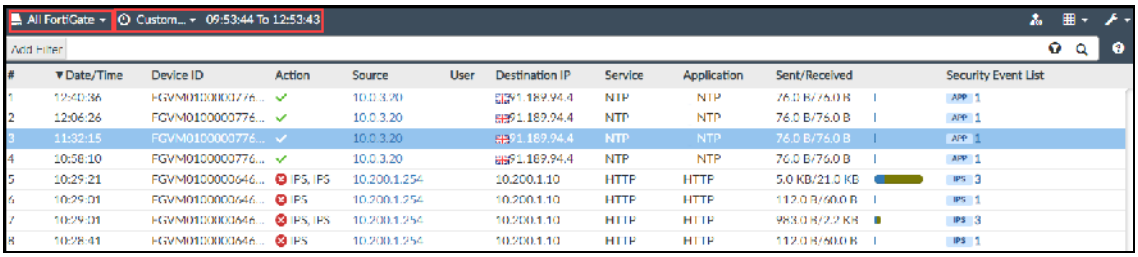
- Click **Tools** > **Historical Log**.

  You should see formatted, historical logs according to the filters that are set. For example, **All FortiGate**, **Custom**. Historical logs are the default view. Double-click a log to see more details.

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

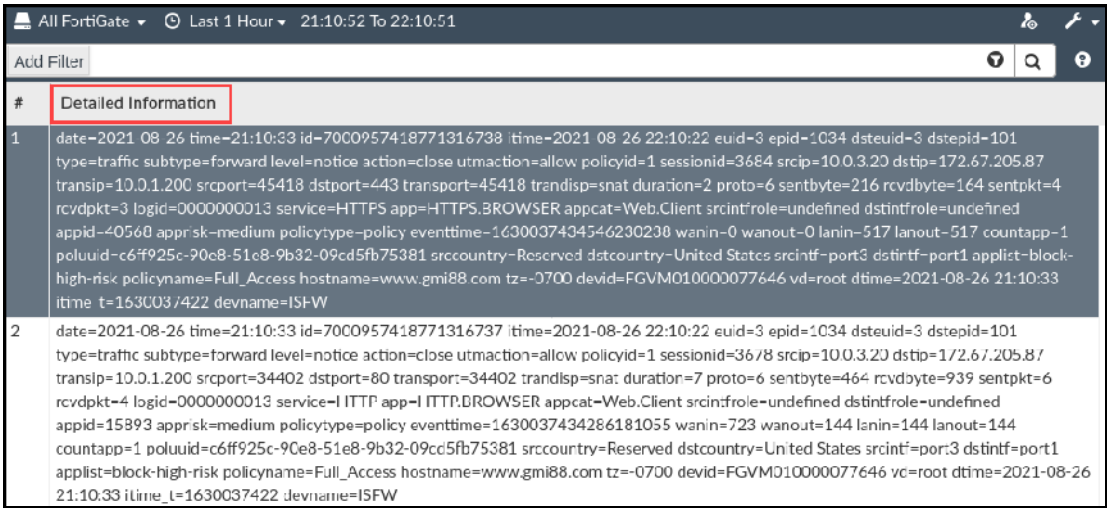
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



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

  You should see the raw logs (not formatted).

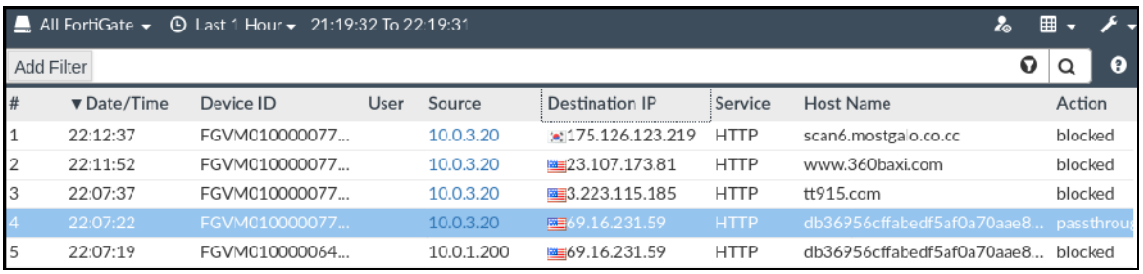


6. Click **Tools** > **Formatted Log** to return the view to formatted logs.
7. Security logs from FortiAnalyzer include antivirus, web filtering, application control, intrusion prevention, email filtering, data leak prevention, SSL/SSH scan, and VoIP. The logs displayed on FortiAnalyzer are dependent on the device type logging to it, the traffic, and the features enabled. In this lab, only web filter, application control, and intrusion prevention logs are triggered.

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

- In the menu on the left, click **Security** > **Web Filter**.

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

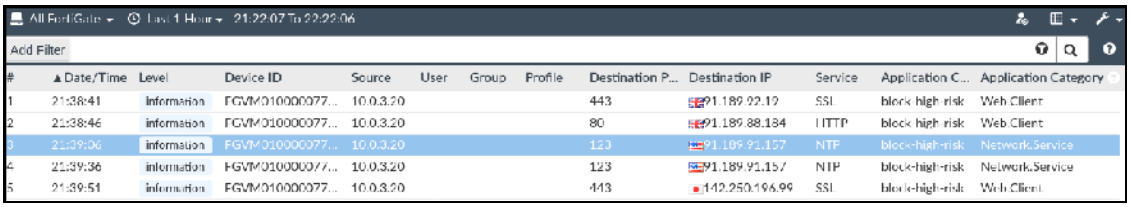


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

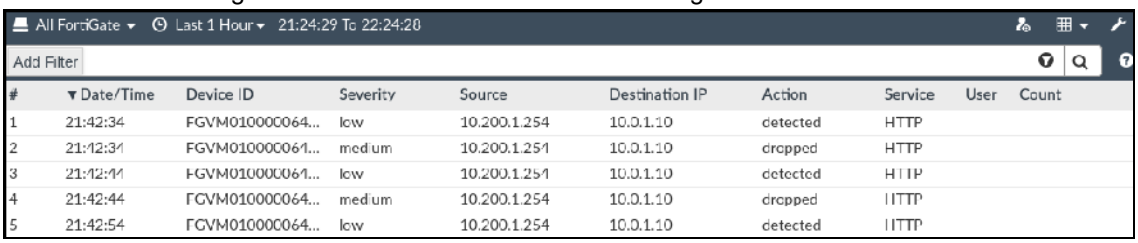
- Click **Security** > **Application Control**.

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



- Click **Security** > **Intrusion Prevention**.

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



Use Log Filters

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

Tips:

- Check the filter drop-down list first to select the SQL column filter name that you want to filter on.
- You can right-click a column value to use that value as a filter. Add the columns that you want from the **Column Settings** drop-down list.
- Ensure the time filter covers the logs that you are searching for.
- Ensure the device is set accordingly for the logs you want to return.
- Verify whether case-sensitive search is enabled or disabled (**Tools**).
- Ensure you are searching on the appropriate log type for the logs you want to return (for example, traffic, web filter, application control, IPS, and so on).
- Ensure you are not in the raw log view, because you cannot filter on raw logs (only historical and real-time logs).
- Ensure you are not filtering on real-time logs if you want to search on historical logs.

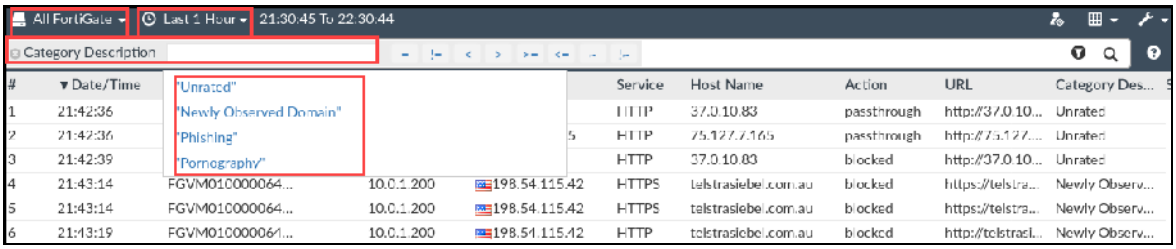
Use filters to find the following logs in ADOM1.

To use log filters

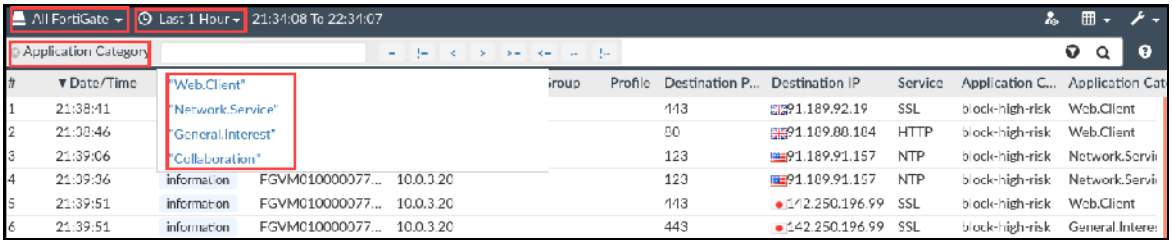
1. Continuing on the FortiAnalyzer GUI (ADOM1), click **Log View**.
2. Locate the following logs:
   - Web filter logs for the **All FortiGate** device group over the past **1** hour with a specific **Category Description** (for example, gambling, phishing, malicious websites)

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

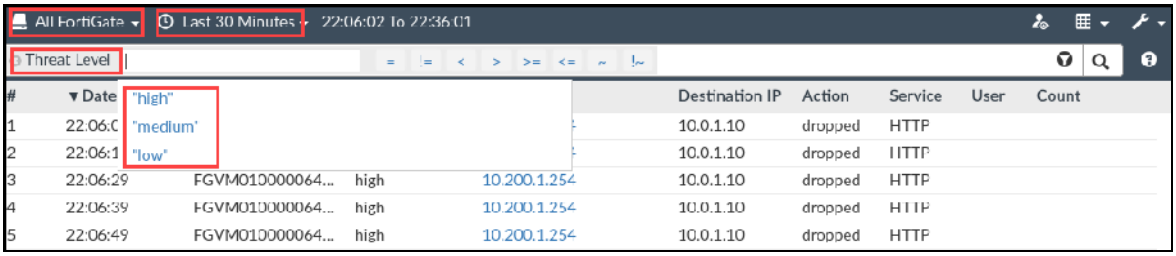
DO NOT REPRINT
© FORTINET
Brave-Dumps.com



- Application control logs for the **All FortiGate** device group over the past **1** hour with a specific application category (for example, general interest, web client)



- Intrusion prevention logs for the **All FortiGate** device group over the last **30** minutes with a **Threat Level** of **high**, **medium**, or **low**



View Logs in FortiView

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

When ADOMs are enabled, each ADOM has its own data analysis in FortiView.

To view logs in FortiView

1. In the drop-down menu in the upper-left, click **Log View** > **FortiView**.
2. Examine (and experiment with) the following views, and feel free to add any notes:

Set your time filters appropriately!

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

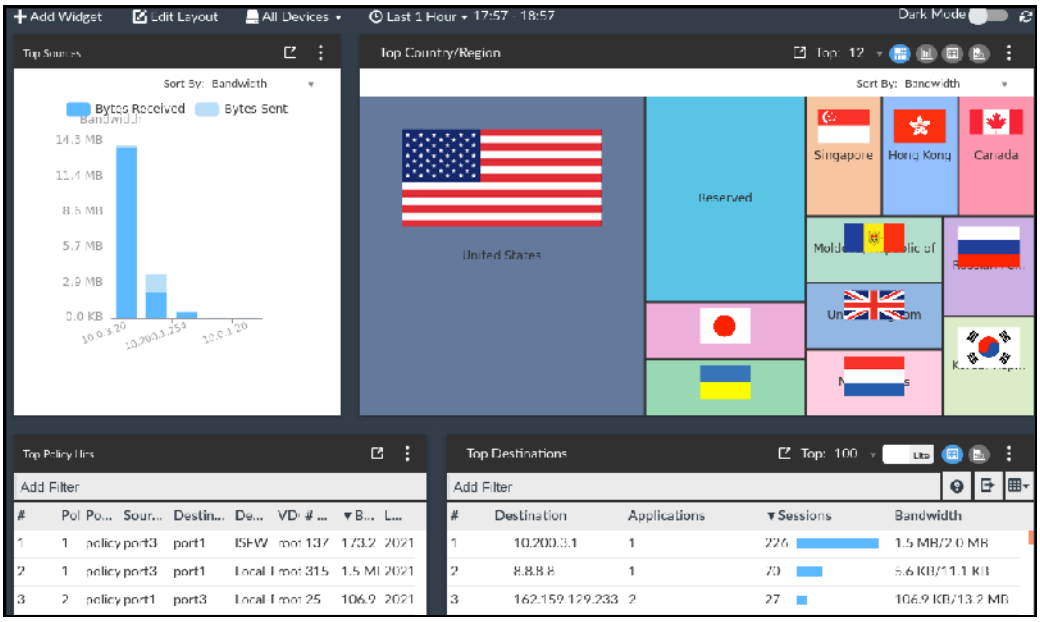
Category	View	Notes
Threats	Top Threats Displays a list of the top threats to your network.	
	Compromised Hosts Displays any hits using fresh threat intelligence against current logs. If there are no hits, try coming back later after FortiAnalyzer has collected more logs.	
Traffic	Top Sources Displays information about the sources of network traffic by source IP address and interface.	
	Top Destinations Displays information about the top destinations of network traffic by destination IP addresses and the application used to access the destination.	
	Top Country/Region Displays information about top countries in terms of traffic sessions, including threat score and destination.	
	Policy Hits Displays information about the FortiGate policy hits. Displays the name of the policy, the name of the FortiGate device, and the number of hits.	
Applications & Websites	Top Applications Displays information about the top applications being used on the network, including the application name, category, and risk level.	
	Top Websites Categories Displays information about the top categories, browsing time, threat score, and sessions.	

To view FortiView monitoring

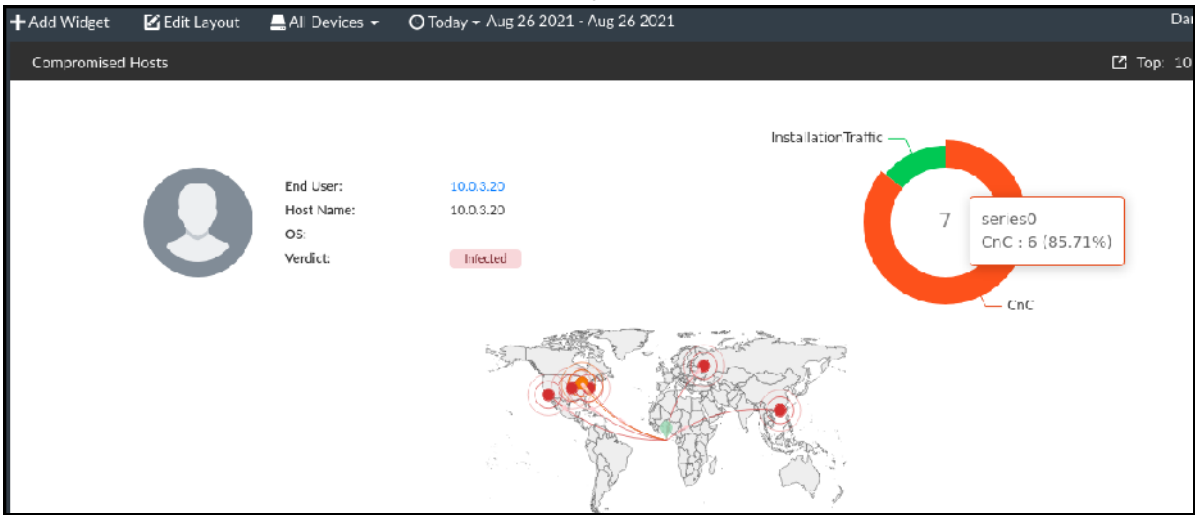
1. Return to the FortiAnalyzer GUI (ADOM1), and then click **FortiView** > **Monitors**.
2. In the menu on the left, click **Traffic**.
   You will be able to see and review the **Top Sources**, **Top Country/Region**, **Top Policy Hits**, and **Top Destinations** information.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



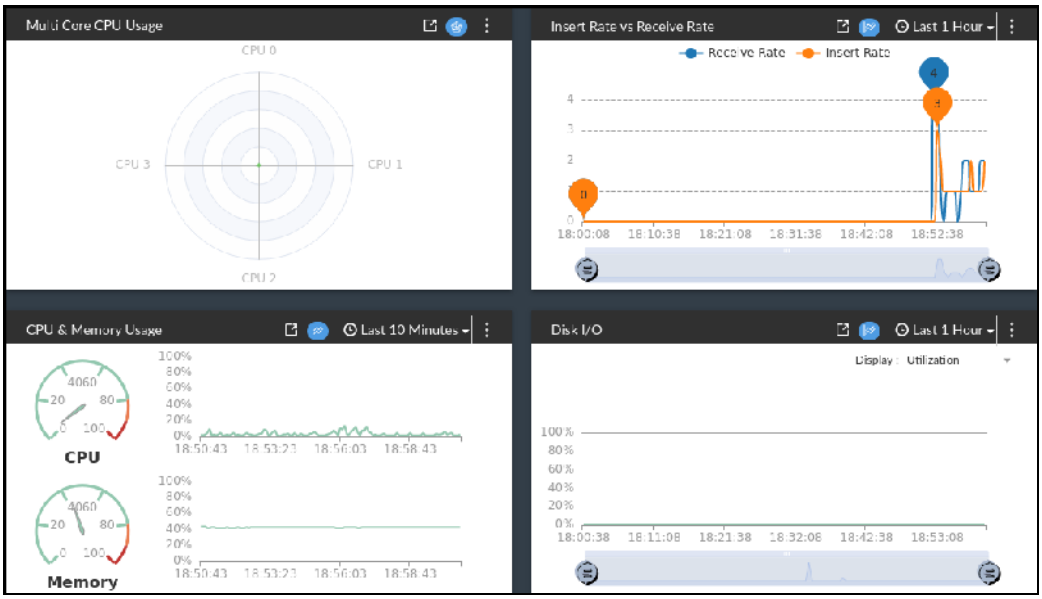
3. In the menu on the left, click **Compromised Hosts Monitor**.
This monitor will show the IP addresses of all the compromised hosts in the network.



4. In the menu on the left, click **Local System Performance**.
This dashboard monitors the system performance of the FortiAnalyzer device, not the logging devices.
5. Review all the widgets and notice that each one can be configured with a separate time period independently from the dashboard settings.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



6. Log out of FortiAnalyzer.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 4: Viewing Log Statistics and Used Storage Space

Now that FortiAnalyzer is collecting logs, you should view the log statistics and used storage space to determine whether FortiAnalyzer is adequately configured to store the logs it receives from the registered devices in your network.

View the Raw Log Receiving Rate

The fortilogd daemon is the process responsible for receiving the raw logs at FortiAnalyzer. Multiple diagnostic commands show the rate at which the logs and messages are received and the status of the process.

This allows you to identify and understand the following:

- The log rate
- The log message rate
- The log message volumes and whether they are well-balanced among the devices
- The log message type distribution (traffic, event, and so on)

To view the raw log receiving rate

1. On the FortiAnalyzer CLI, log in with the username `admin` and password `password`.
2. Enter the following commands to view fortilog daemon information:

Diagnostic	Command
What is the log rate every second/30 seconds/60 seconds?	`diagnose fortilogd lograte`
What is the message log rate every second/30 seconds/60 seconds?	`diagnose fortilogd msgrate` One log message can consist of multiple logs in LZ4 format. Therefore, the rate should be lower for `msgrate` than `lograte`.
What is the log message rate per device per second?	`diagnose fortilogd lograte-device` Since all traffic is going through Local-FortiGate and ISFW, the totals for the Local-FortiGate and ISFW should be higher than Remote-FortiGate.
What is the log type distribution per second?	`diagnose fortilogd lograte-type` FortiGate sends only two types of log files to FortiAnalyzer: `tlog` (traffic) and `elog` (event). All UTM logs are sent with `tlog`.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

3. Close the FortiAnalyzer CLI session.

View the Insert Rate Versus the Receive Rate

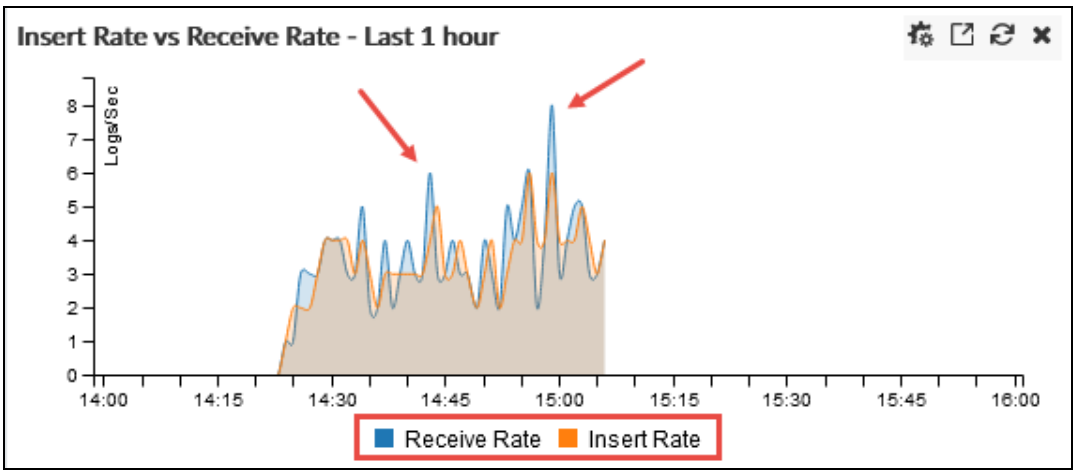
The FortiAnalyzer dashboard includes a widget that shows the rate at which raw logs are reaching FortiAnalyzer (receive rate) and the rate at which they are indexed by the SQL database (insert rate) by the sqlplugind daemon.

Another widget displays the log insert lag time (how many seconds the database is behind in processing the logs).

To view log rates

1. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. Click **ADOM1**.
3. Click **System Settings**.
4. On the dashboard, view the information in the following widgets:
   - **Insert Rate vs. Receive Rate**

     If at any point the log receive rate is higher than the log insert rate, this indicates that the raw logs are being received faster than they can be indexed (inserted) in the database.

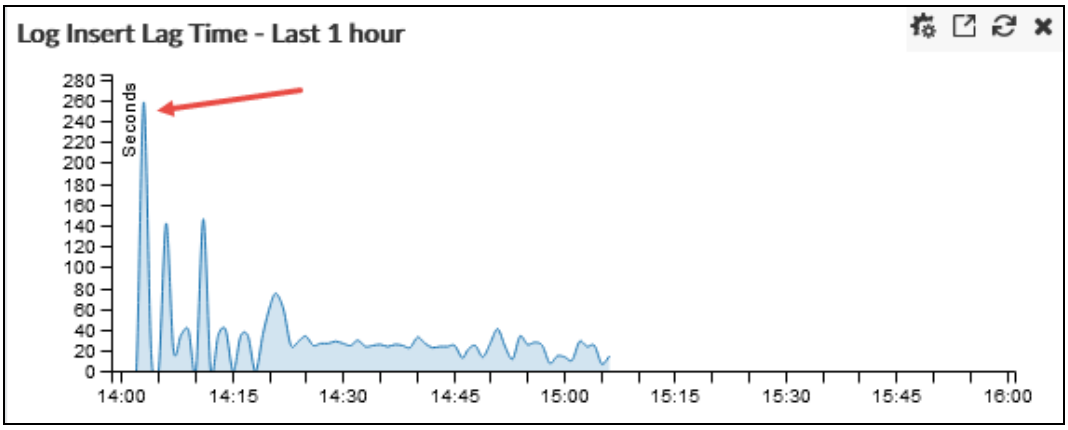


   - **Log Insert Lag Time**

     If at any point there is a high lag time, this indicates how many seconds the database is behind in processing the logs.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



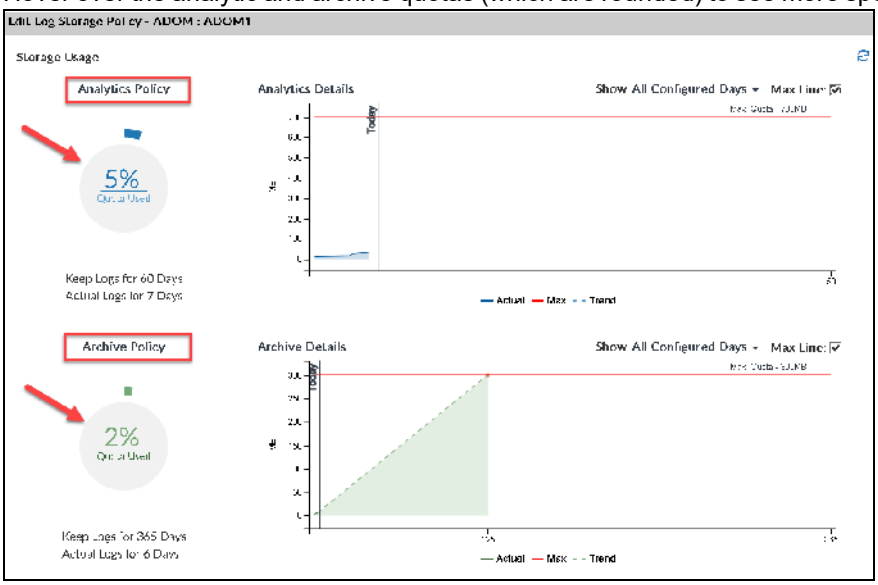
View Used Storage Statistics

Earlier, you obtained your data policy and disk utilization information. Now that FortiAnalyzer has collected some logs, you will view the current status for the used storage.

You can also use the `diagnose log device` CLI command to obtain this information.

To view the current used storage

1. Continuing on the FortiAnalyzer GUI (ADOM1), in the drop-down menu on the left, click **System Settings** > **Storage Info**.
2. Edit **ADOM1**.
3. Hover over the analytic and archive quotas (which are rounded) to see more specific statistics.



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Due to the relatively low volume of logs being generated in the lab environment, you may see that very little storage is being used.

4. Click **Cancel** to close the window.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 5: Modifying Disk Quotas

In this exercise, you will compare the storage space available on both ADOMs. Then, you will modify the disk quota on one of the ADOMs to reflect what is happening.

Compare Storage Space Between ADOMs

You will run a CLI command so you can compare the used storage space between ADOM1 and ADOM2. Remember, you ran all your traffic through Local-FortiGate and ISFW, which is located in ADOM1.

To compare storage space

1. On the FortiAnalyzer CLI, log in with the username `admin` and password `password`.
2. Enter the following command to check the storage space for each ADOM:

The CLI output formatting is easier to read if you maximize your window or copy and paste the output to a Notepad file.

```
# diagnose log device
```

You should see that ADOM1 is using more of its log storage and database storage than ADOM2.

```
AdomName          AdomOID  Type                                  Logs                                                                                  Database
                           [Retention    Quota    UsedSpace(logs / quarantine / content / IPS) Used%]  [Retention    Quota      Used    Used%]
ADOM1             131      FGT      365days   300.0MB   25.1MB(   25.1MB/    0.0KB/    0.0KB/    0.0KB)  8.4%      60days   700.0MB   53.6MB    7.7%
ADOM2             133      FGT      365days   300.0MB  148.0KB(  148.0KB/    0.0KB/    0.0KB/    0.0KB)  0.0%      60days   700.0MB 1000.0KB    0.1%
FortiAnalyzer     107      FAZ      365days   400.0MB    0.0KB(    0.0KB/    0.0KB/    0.0KB/    0.0KB)  0.0%     365days   600.0MB    0.0KB    0.0%
FortiAuthenticator 129       FAC      365days   300.0MB    0.0KB(    0.0KB/    0.0KB/    0.0KB/    0.0KB)  0.0%      60days   700.0MB    0.0KB    0.0%
FortiCache        111      FCH      365days   400.0MB    0.0KB(    0.0KB/    0.0KB/    0.0KB/    0.0KB)  0.0%     365days   600.0MB    0.0KB    0.0%
FortiCarrier      103      FGT      365days   400.0MB    0.0KB(    0.0KB/    0.0KB/    0.0KB/    0.0KB)  0.0%     365days   600.0MB    0.0KB    0.0%
FortiClient       113      FCT      365days   400.0MB    0.0KB(    0.0KB/    0.0KB/    0.0KB/    0.0KB)  0.0%     365days   600.0MB    0.0KB    0.0%
FortiDDoS         126      FDD      365days   400.0MB    0.0KB(    0.0KB/    0.0KB/    0.0KB/    0.0KB)  0.0%     365days   600.0MB    0.0KB    0.0%
FortiMail         105      FML      365days   400.0MB    0.0KB(    0.0KB/    0.0KB/    0.0KB/    0.0KB)  0.0%     365days   600.0MB    0.0KB    0.0%
FortiManager      116      FMG      365days   400.0MB    0.0KB(    0.0KB/    0.0KB/    0.0KB/    0.0KB)  0.0%     365days   600.0MB    0.0KB    0.0%
FortiSandbox      118      FSA      365days   400.0MB    0.0KB(    0.0KB/    0.0KB/    0.0KB/    0.0KB)  0.0%     365days   600.0MB    0.0KB    0.0%
FortiWeb          109      FWB      365days   400.0MB    0.0KB(    0.0KB/    0.0KB/    0.0KB/    0.0KB)  0.0%     365days   600.0MB    0.0KB    0.0%
Syslog            114      SYS      365days   400.0MB    0.0KB(    0.0KB/    0.0KB/    0.0KB/    0.0KB)  0.0%     365days   600.0MB    0.0KB    0.0%
root              3        FGT      365days   400.0MB    0.0KB(    0.0KB/    0.0KB/    0.0KB/    0.0KB)  0.0%     365days   600.0MB    0.0KB    0.0%
Total usage: 14 ADOMs, logs=25.2MB database=106.3MB(ADOMs usage:54.6MB + Internal Usage:51.7MB)
```

Modify the Disk Quota

The `diagnose log device` output indicated that ADOM1 is receiving more traffic than ADOM2. In the real world, if you were consistently seeing a high log volume in a specific ADOM over a reasonable amount of time, it might cause your disk to fill up and result in lost logs. In that case, you would do one of the following:

- Modify the firewall policies to reduce the amount of traffic you are monitoring
- Modify the disk quotas

The easiest way to resolve this imbalance between ADOM disk usage is to modify the disk quotas, because it allows you to keep the firewall policies intact.

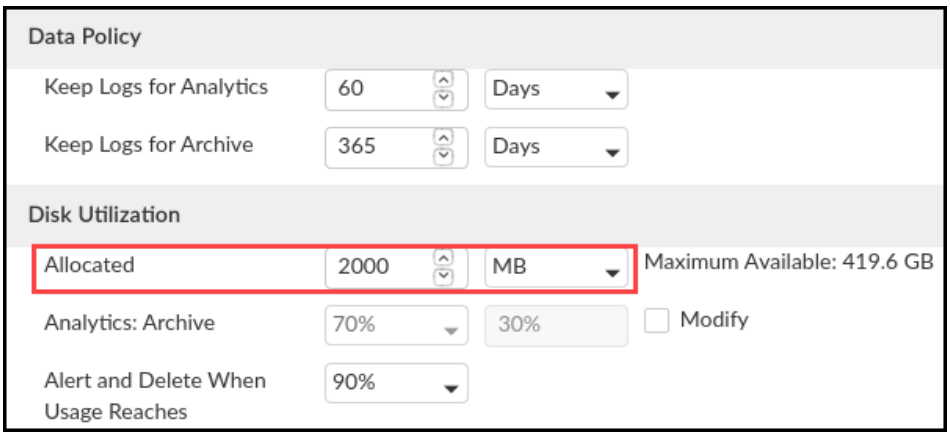
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

You will increase the disk quota in ADOM1, which is the ADOM receiving the most traffic.

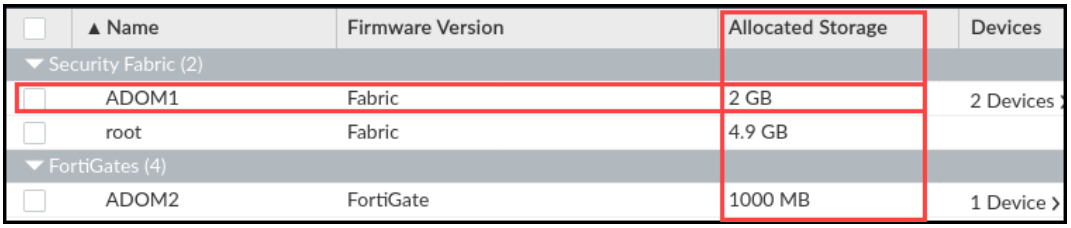
To modify the disk quota

1. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. Click **ADOM1**.
3. Click **System Settings**.
4. In the menu on the left, select **All ADOMs**, and then edit **ADOM1**.
5. Change the allocated disk utilization from 1000 MB to 2000 MB.



6. Click **OK**.

   You successfully increased the disk storage in ADOM1.



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 6: Moving Devices With Logs Between ADOMs

As you expand your network, or as your organizational structure changes, you may need to reorganize your devices in ADOMs. In this exercise, you will move two devices out of one ADOM and into another ADOM.

As mentioned in the *Device Registration and Communication* lesson, when you move a device into a different ADOM, the archive (compressed) logs are migrated to that ADOM, but the analytics (indexed) logs are not migrated.

Therefore, you must rebuild the ADOMs to move the analytics logs into the new ADOM, and delete them from the old ADOM.

In a real-world scenario, you would perform this procedure during a low maintenance time, when little traffic is passing through the device you are moving.

Gather Log and ADOM Information

Before you move a device out of an ADOM, you should be aware of the following information:

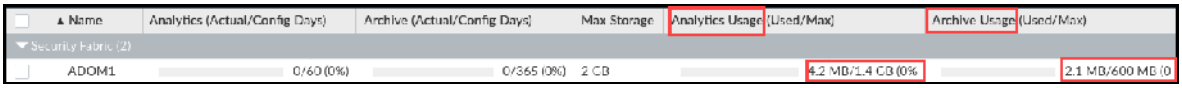
- The disk quota set on the current ADOM (**System Settings** > **All ADOMs**)

  Since the disk quota is set for each ADOM and not for each device, you do not necessarily need to match the disk quota from the current ADOM to the new ADOM. This is because, for example, the new ADOM may contain less devices than the current one. However, you must ensure that your new ADOM has enough space for the device you are moving into it.

  In this lab environment, ADOM1 currently has a 2000 MB disk quota.

- The volume of logs (**System Settings** > **Storage Info** or `# diagnose log device`)

  Although the disk quota is set for each ADOM, it is important to know the actual log volume associated with the device you are moving. You must ensure that the new ADOM, at a minimum, has enough space to store the device's current logs. You will still need to select a disk quota with future logs in mind.



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
Brave-Dumps.com
© FORTINET

AdomName	AdomID	Type	Logs						Database				
			Retention	Quota	Used	Logs/quaranti/	content/	IPS	Used%	Retention	Quota	Used	SiemDB/ hcache)	Used%
ADOM1	255	FSF	365days	600.0MB	2.1MB	2.1MB/	0.0KB/	0.0KB/	0.4%	60days	1.4GB	4.2MB	694.5KB/ 0.0KB)	0.3%
ADOM2	194	FGT	365days	300.0MB	96.0KB	96.0KB/	0.0KB/	0.0KB/	0.0%	60days	700.0MB	2.0MB	0.0KB/ 11.2KB)	0.3%
FortiAnalyzer	122	FAZ	365days	300.0MB	0.0KB	0.0KB/	0.0KB/	0.0KB/	0.0%	60days	700.0MB	0.0KB	0.0KB/ 0.0KB)	0.0%
FortiAuthenticator	138	FAC	365days	300.0MB	0.0KB	0.0KB/	0.0KB/	0.0KB/	0.0%	60days	700.0MB	0.0KB	0.0KB/ 0.0KB)	0.0%
FortiCache	126	FCH	365days	300.0MB	0.0KB	0.0KB/	0.0KB/	0.0KB/	0.0%	60days	700.0MB	0.0KB	0.0KB/ 0.0KB)	0.0%
FortiCarrier	118	FGT	365days	300.0MB	0.0KB	0.0KB/	0.0KB/	0.0KB/	0.0%	60days	700.0MB	0.0KB	0.0KB/ 0.0KB)	0.0%
FortiClient	128	FCT	365days	300.0MB	0.0KB	0.0KB/	0.0KB/	0.0KB/	0.0%	60days	700.0MB	0.0KB	0.0KB/ 0.0KB)	0.0%
FortiDDoS	136	FDD	365days	300.0MB	0.0KB	0.0KB/	0.0KB/	0.0KB/	0.0%	60days	700.0MB	0.0KB	0.0KB/ 0.0KB)	0.0%
FortiDeceptor	144	FDC	365days	300.0MB	0.0KB	0.0KB/	0.0KB/	0.0KB/	0.0%	60days	700.0MB	0.0KB	0.0KB/ 0.0KB)	0.0%
FortiFirewall	154	FFW	365days	300.0MB	0.0KB	0.0KB/	0.0KB/	0.0KB/	0.0%	60days	700.0MB	0.0KB	0.0KB/ 0.0KB)	0.0%
FortiMail	120	FML	365days	300.0MB	0.0KB	0.0KB/	0.0KB/	0.0KB/	0.0%	60days	700.0MB	0.0KB	0.0KB/ 0.0KB)	0.0%
FortiManager	132	FMG	365days	300.0MB	0.0KB	0.0KB/	0.0KB/	0.0KB/	0.0%	60days	700.0MB	0.0KB	0.0KB/ 0.0KB)	0.0%
FortiNAC	142	FNA	365days	300.0MB	0.0KB	0.0KB/	0.0KB/	0.0KB/	0.0%	60days	700.0MB	0.0KB	0.0KB/ 0.0KB)	0.0%
FortiProxy	140	FPX	365days	300.0MB	0.0KB	0.0KB/	0.0KB/	0.0KB/	0.0%	60days	700.0MB	0.0KB	0.0KB/ 0.0KB)	0.0%
FortiSandbox	134	FSA	365days	300.0MB	0.0KB	0.0KB/	0.0KB/	0.0KB/	0.0%	60days	700.0MB	0.0KB	0.0KB/ 0.0KB)	0.0%
FortiWeb	124	FWB	365days	300.0MB	0.0KB	0.0KB/	0.0KB/	0.0KB/	0.0%	60days	700.0MB	0.0KB	0.0KB/ 0.0KB)	0.0%
Syslog	130	SYS	365days	300.0MB	0.0KB	0.0KB/	0.0KB/	0.0KB/	0.0%	60days	700.0MB	0.0KB	0.0KB/ 0.0KB)	0.0%
Unmanaged Devices	156	FSF	365days	300.0MB	0.0KB	0.0KB/	0.0KB/	0.0KB/	0.0%	60days	700.0MB	0.0KB	0.0KB/ 0.0KB)	0.0%
root	3	FSF	365days	1.5GB	0.0KB	0.0KB/	0.0KB/	0.0KB/	0.0%	60days	3.4GB	2.1MB	0.0KB/ 0.0KB)	0.1%

Move a Device to a Different ADOM

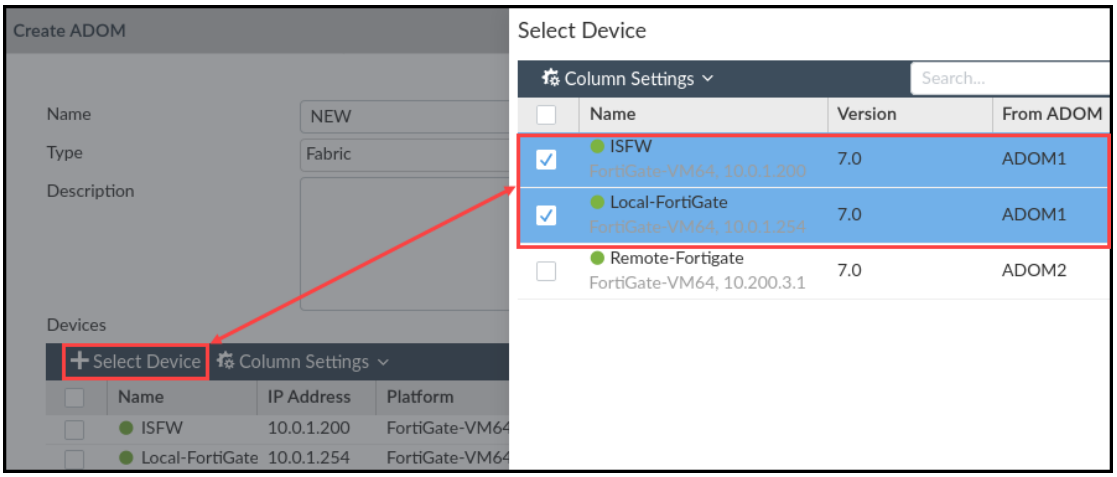
Since Local-FortiGate and ISFW in ADOM1 contain the logs from all the traffic you have been generating through FIT and Nikto, you will move both FortiGate devices out of ADOM1 and into a new ADOM called NEW.

To move a device to a different ADOM

1. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. Click **ADOM1**.
3. Click **System Settings**.
4. In the menu on the left, select **All ADOMs**, and then click **Create New**.
5. Configure the following settings to create a new ADOM for Local-FortiGate and ISFW:

Field	Value
Name	NEW
Type	Fabric

6. Click **Select Device**.
7. In the **Select Device** pane that opens, select **Local-FortiGate** and **ISFW**.



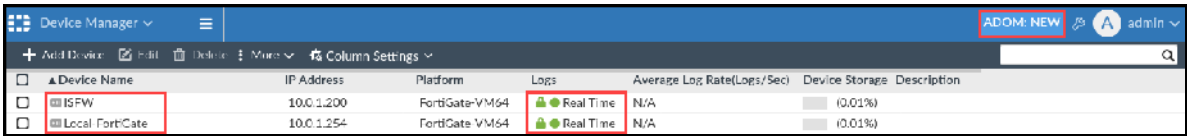
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

8. Click **Add to ADOM**.
   Local-FortiGate and ISFW are added to the **Devices** list for the **NEW** ADOM.
9. Under **Disk Utilization**, change the **Allocated** setting to 1000 MB.

At a minimum, the disk quota should support the volume of logs that you are moving into it.

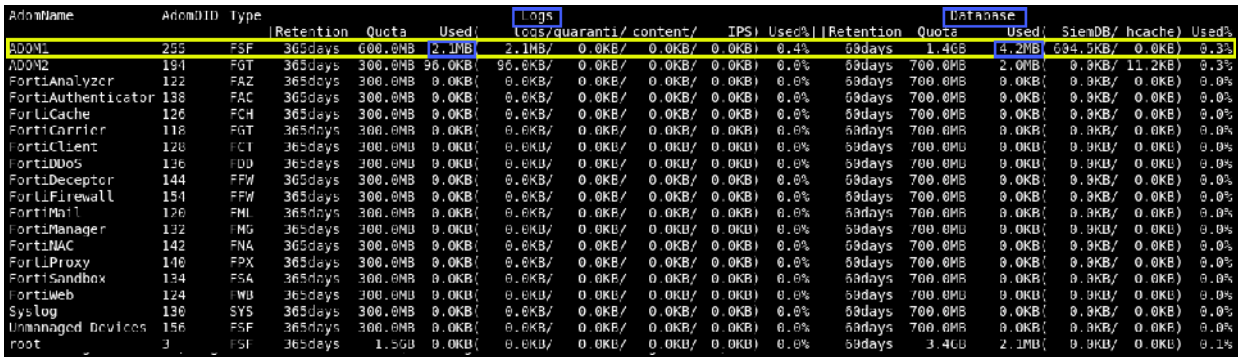
10. Click **OK**.
11. Click **Close**.
    Both FortiGate devices move from ADOM1 to NEW ADOM.
12. Switch into the **NEW** ADOM, and then under **Device Manager**, verify **Local-FortiGate** and **ISFW** are registered and still collecting logs.



Rebuild the ADOM Database to Migrate the Device Logs

Assuming you want the old logs (analytics logs) in the new ADOM so you can run reports against them, and no longer want to see the device logs in the old ADOM, you must rebuild the new ADOM database and the old ADOM database.

Ensure that you remember the log volume associated with your Local-FortiGate and ISFW devices (`# diagnose log device`).



To verify the location of the Local-FortiGate logs

1. On the FortiAnalyzer CLI, log in with the username `admin` and password `password`.
2. Enter the following commands to display log information for each ADOM:

```
# diagnose test application logfiled 4 ADOM1
# diagnose test application logfiled 4 NEW
```

3. Confirm the location of the logs by examining ADOM1 (the old ADOM) and NEW ADOM (the new ADOM).

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com


```
ADOM [ADOM1 FSFADOM183] last-dvm-update:4m19s(ago) (1633401070)
  quota          : 2.0GB(log=600.0MB, db=1.4GB), split_ratio=70%(db), trim_thres=90%
  retention      : log=365 days, db=60 days(actual from 2021/10/04 19:23:32 to 2021/10/04 19:31:04),
  log-db         : 3.6MB(SIEM-DB:159.9KB) 0.3%, prev_scan=4m13s(ago), next_scan=10m47s(later), rate=
    by-retention: requests=0 last-req=n/a
    by-quota    : requests=0 last-req=n/a
  log-files      : 0.0KB 0.0%
    usage        : log=n/a(0.0KB), quar=0(0.0KB), content=0(0.0KB), ips=0(0.0KB), total=0(0.0KB)
    by-retention: log=n/a(0.0KB), quar=0(0.0KB), content=0(0.0KB), ips=0(0.0KB), total=0(0.0KB)
    by-quota    : log=n/a(0.0KB), quar=0(0.0KB), content=0(0.0KB), ips=0(0.0KB), total=0(0.0KB)
    by-inode    : log=n/a(0.0KB), quar=0(0.0KB), content=0(0.0KB), ips=0(0.0KB), total=0(0.0KB)
```

Analytics Logs

Archive Logs

```
ADOM [NEW FSFADOM242] last-dvm-update:4m19s(ago) (1633401070)
  quota          : 1000.0MB(log=300.0MB, db=700.0MB), split_ratio=70%(db), trim_thres=90%
  retention      : log=365 days, db=60 days(no data), last_chk=4m11s(ago) next_chk=11h55m49s(later)
  log-db         : 0.0KB(SIEM-DB:0.0KB) 0.0%, prev_scan=4m11s(ago), next_scan=10m49s(later), rate=0(Bps)
    by-retention: requests=0 last-req=n/a
    by-quota    : requests=0 last-req=n/a
  log-files      : 600.0KB 0.2%
    usage        : log=n/a(600.0KB), quar=0(0.0KB), content=0(0.0KB), ips=0(0.0KB), total=0(600.0KB)
    by-retention: log=n/a(0.0KB), quar=0(0.0KB), content=0(0.0KB), ips=0(0.0KB), total=0(0.0KB)
    by-quota    : log=n/a(0.0KB), quar=0(0.0KB), content=0(0.0KB), ips=0(0.0KB), total=0(0.0KB)
    by-inode    : log=n/a(0.0KB), quar=0(0.0KB), content=0(0.0KB), ips=0(0.0KB), total=0(0.0KB)
```

Analytics Logs

Archive Logs

As you can see, the log-files (archive logs) have moved from **ADOM1** to **NEW**, but **ADOM1** still contains the `log-db` (analytics logs) logs.

To rebuild the ADOM database

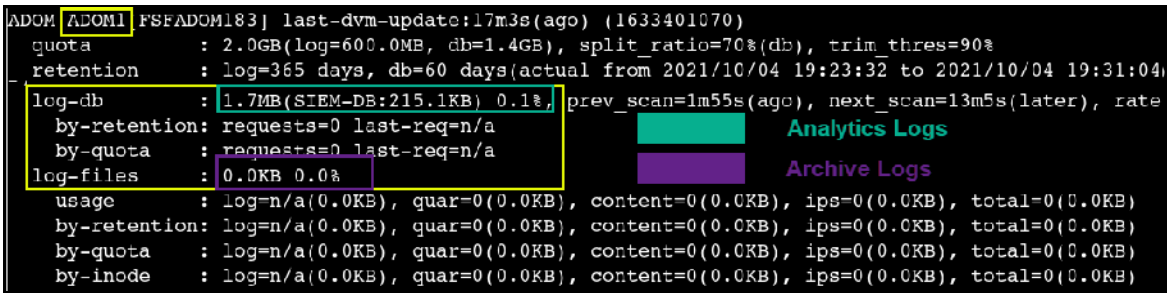
1. Continuing on the FortiAnalyzer CLI session, enter the following command to rebuild the two ADOMs, and transfer the analytics logs:
   ```
   # execute sql-local rebuild-adom NEW ADOM1
   ```
2. Type `y` to continue with the operation.
   ```
   FAZVM # execute sql-local rebuild-adom NEW ADOM1
   Rebuild log SQL database of ADOM 'NEW,ADOM1' has been requested.
   This operation will remove the log SQL database for ADOM 'NEW,ADOM1' and rebuild from log data.
   Do you want to continue? (y/n)y

   Request to rebuild ADOM 'NEW,ADOM1' submitted successfully.
   ```
3. Wait a few minutes for the databases to rebuild.
   The FortiAnalyzer GUI shows the rebuild progress.

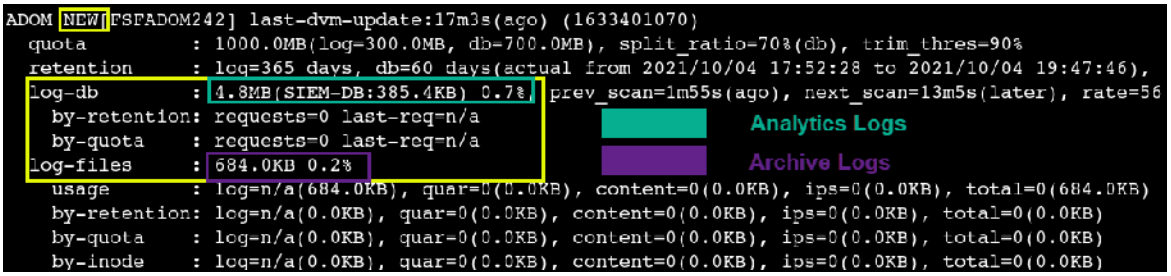
4. Enter the following command to recheck log storage for both ADOM1 and NEW:
   ```
   # diagnose test application logfiled 4
   ```

If you do not see the logs move, wait a few minutes, and then try again.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com





The `log-db` (analytics logs) successfully migrated from `ADOM1` to `NEW ADOM`.

You can also see that the `log-files` (archive logs) in `NEW` were reduced. This is because the logs were compressed.

You can also see that the `log-db` in `ADOM1` still contains some data, even after the rebuild. This data is used for the system (management) tables.

5. Close the FortiAnalyzer CLI session.
6. Return to Local-Client, and then press `Ctrl+Z` on each PuTTY session to stop the scripts.
7. Close both PuTTY sessions.
8. Close the browser.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Lab 5: Events and Incidents Management

In this lab, you will examine some of the components included in the FortiSoC feature on FortiAnalyzer. You will gain experience managing events, event handlers, and tools that you can use to analyze incidents on FortiAnalyzer. For some of the tasks, you must generate traffic that will trigger the creation of new events. Finally, you will explore how you can be proactive in a SOC environment, with the help of the available threat hunting capabilities.

Objectives

- Examine the FortiSoC dashboards
- Examine and manage events
- Clone and customize event handlers
- Create a custom event handler
- Manage incidents
- Explore threat hunting

Time to Complete

Estimated: 90 minutes

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 1: Examining and Managing Events

In this exercise, you will examine how you can find the details of existing events in FortiAnalyzer and the logs that generated them. You will also explore how you can use filters to display only the events with specific parameters.

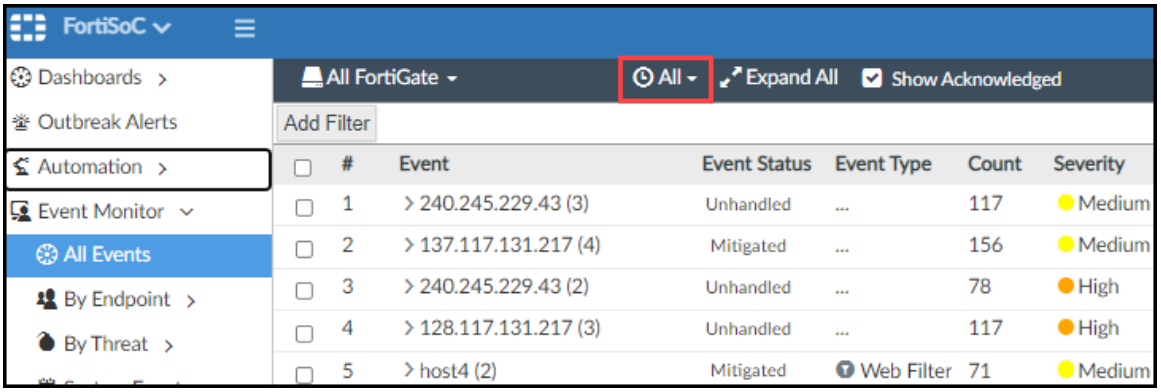
Examine Existing Events

Examining events allows you to identify existing and potential security threats in your environment. You will use the filtering capabilities included in FortiAnalyzer to help you with this task.

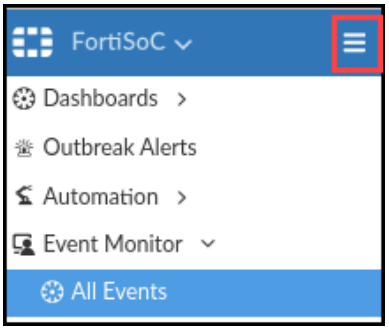
To examine events

1. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. Click **NEW**.
3. Click **FortiSoC**.
4. Click **Event Monitor** > **All Events**.

   On the panel on the right, you should see multiple events that were created by the traffic generated in a previous lab. If you don't see any events, set the filter to **All**.



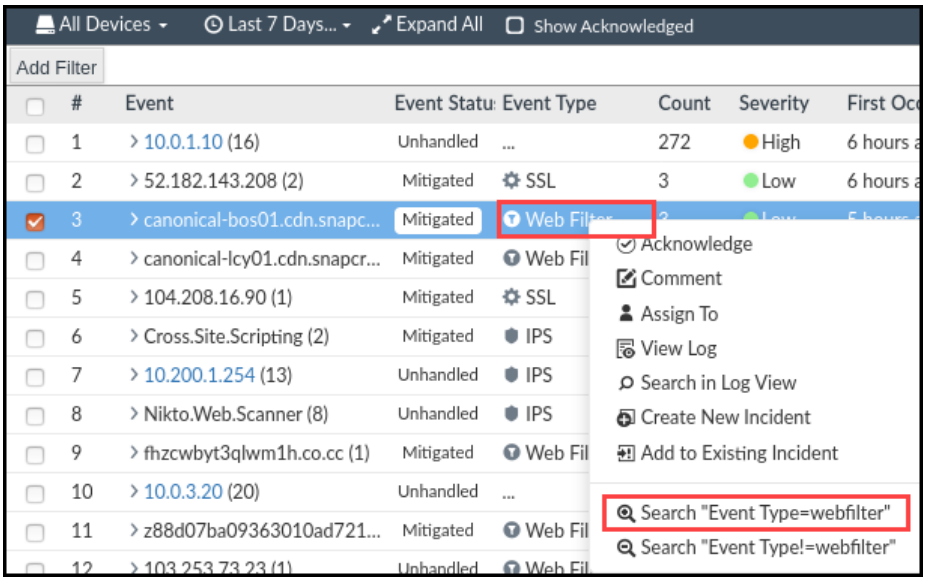
5. Optionally, if you need more room to see all the columns, click the button to hide the side menu.



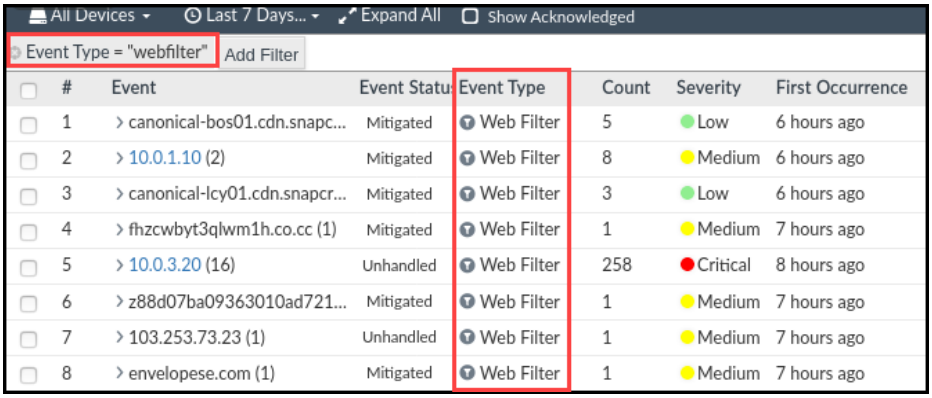
6. Under the **Event Type** column, right-click one of the **Web Filter** entries, and then select **Search "Event Type=webfilter"** to filter the events displayed.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



The resulting view includes only those events that match the filter you selected.



Notice there is a **>** symbol beside each entry. This is because the event handlers group multiple events based on different criteria, such as threat or endpoint.

If you need to narrow down the information displayed further, you can repeat the process to add more filters based on additional columns.

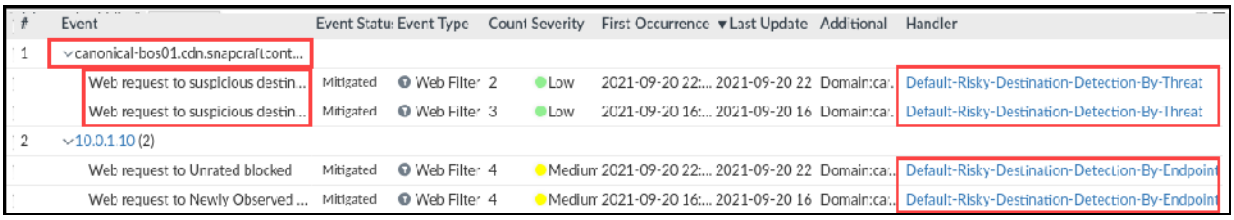
7. Select one of the entries listed, and then scroll to the right to see the name of the event handler that created it.

   For example, in the following image, the first entry was generated by the **Default-Risky-Destination-By-Threat** handler and the second entry was generated by the **Default-Risky-Destination-By-Endpoint**

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

handler.



The top-level containers are not the actual events—they are just the parameters used to group similar events.

In the example above, each of the entries shown has two events within it.

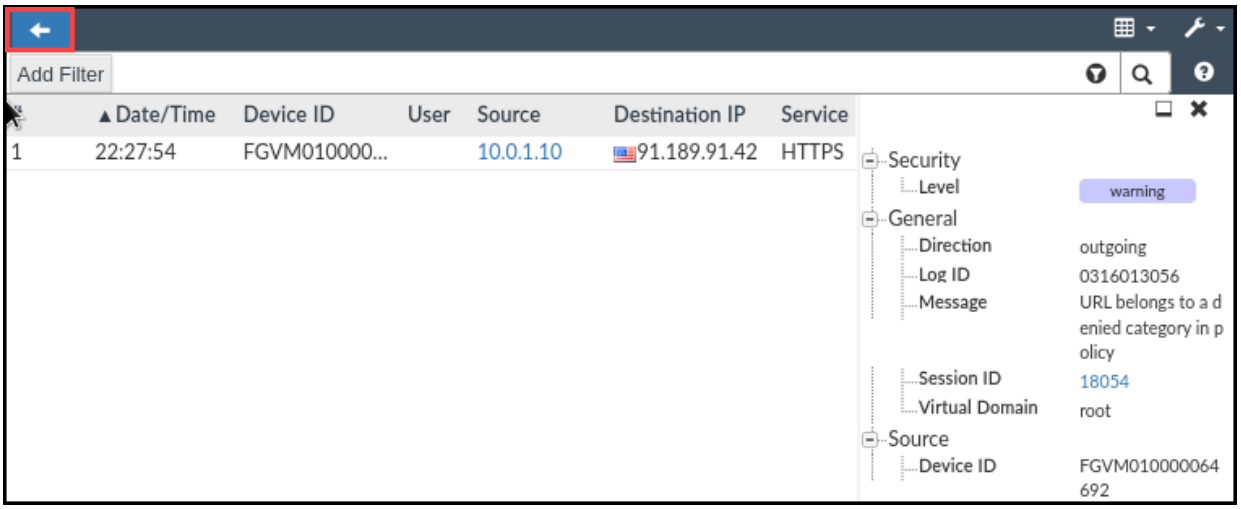
Depending on the event handlers enabled, you may find the same event in more than one of these containers.

8. Notice the **Event Status** and **Severity** columns.

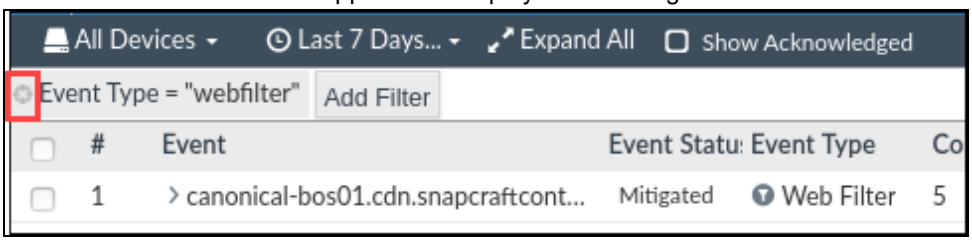
   In general, **Mitigated** events should not result in any harm to your network. However, an **Unhandled** event could be a reason for concern, and should be investigated.

9. Double-click an event to see which log generated it.
   This will take you to a new view where you can see details about that log.

10. Click the back arrow to return to the **All Events** view.



11. Click the **X** to clear the filters applied and display all events again.



12. Log out of FortiAnalyzer.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 2: Cloning and Customizing Event Handlers

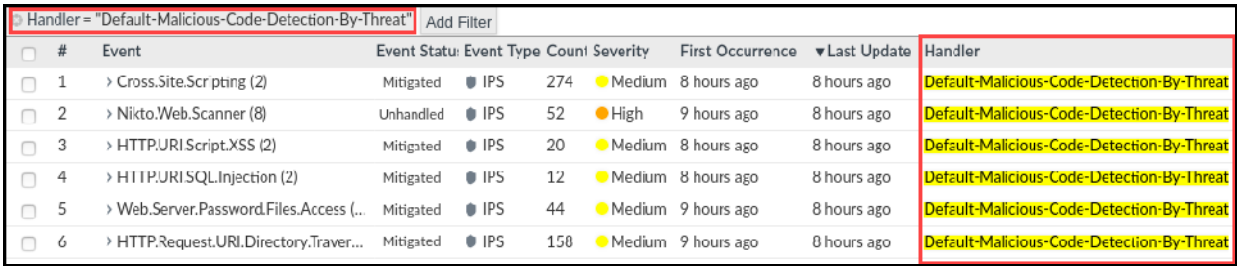
In this exercise, you will examine which event handler generated an event. You will then create a new handler by cloning the original one, and then customizing the cloned version to send a notification email every time it generates a new event.

Find the Event Handler and the Log That Generated an Event

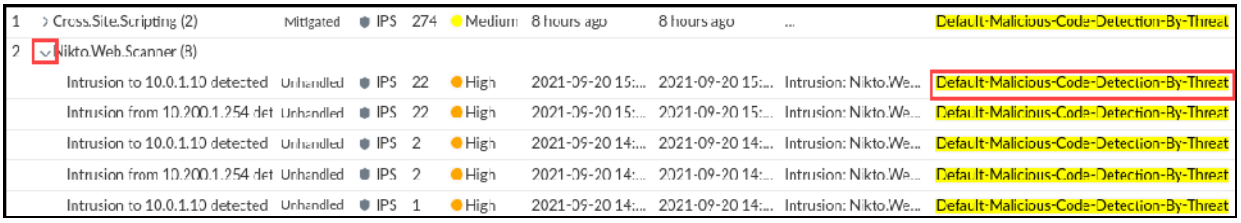
You will get important details about an event by finding what event handler and traffic log generated it.

To find the event handler and the log that generated an event

1. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. Click **NEW**.
3. Click **FortiSoC**.
4. Click **Event Monitor** > **All Events**.
   In a previous exercise, you saw that the event handler information is shown in one of the columns in **All Events**.
   Event handlers search for specific criteria in the logs received and, if a match is found, they generate an event.
5. Find an event that was generated by the **Default-Malicious-Code-Detection-By-Threat** handler.
   This handler generates IPS-related events. You can scroll down until you find one or use a filter like the one in the following image:



6. Find the entry labeled **Nikto.Web.Scanner**.
7. Click the **>** sign to expand it, and then find the event labeled **Intrusion to 10.0.1.10 detected**.

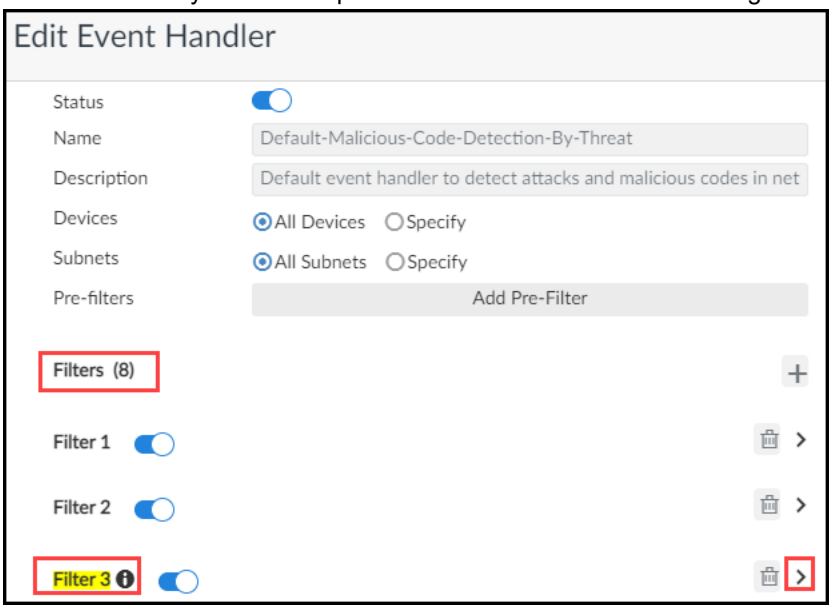


8. Click the handler name, listed on the right.
   The **Edit Event Handler** window opens and you can see how many filters are included in this handler.

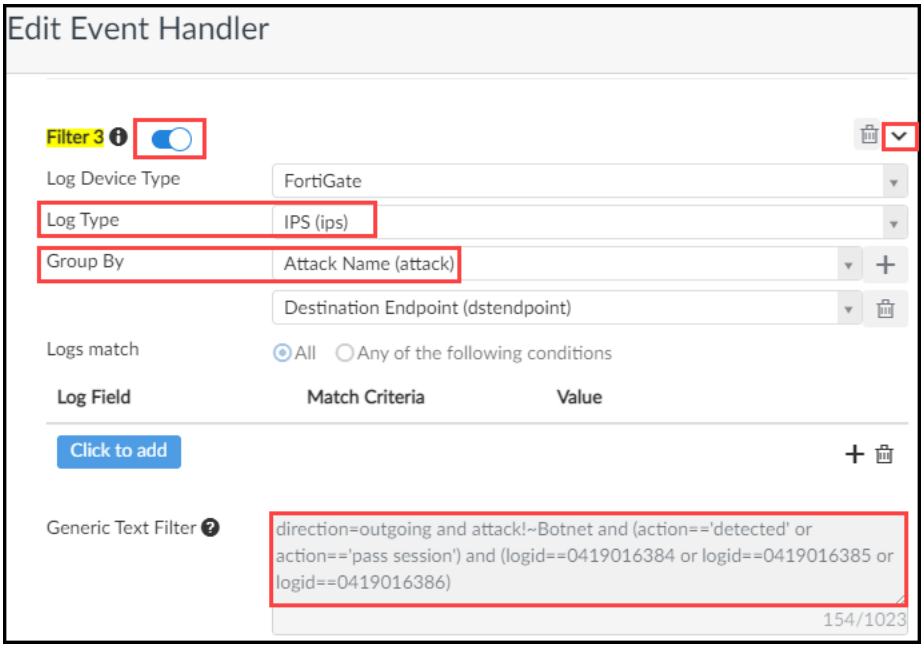
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

9. Scroll down until you see the specific filter that found the match that generated this event, highlighted in yellow.



10. Click the **>** symbol on the right to expand that filter and see all its settings.



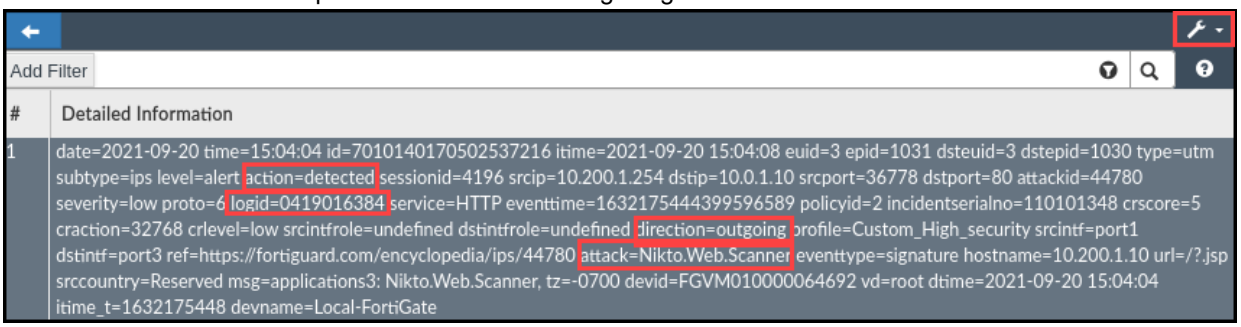
The handler shown here is one of several predefined handlers that come with FortiAnalyzer. You can disable any of the filters they include, but you cannot make other changes.

11. Notice the **Generic Text Filter** section.
    This is a good reference to have when you create custom filters.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

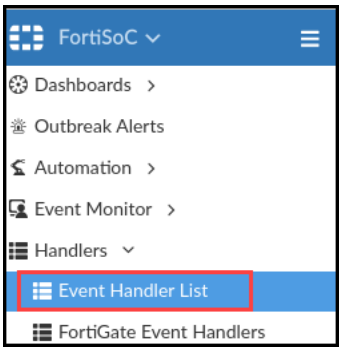
12. Click **OK** to close the handler settings window.
13. Return to the **Intrusion to 10.0.1.10 detected** event that you found in Step 6.
14. Double-click the event to open its associated log, and then click the tool icon to change the view to **Raw**.
    The view should include the parameters in the following image:



15. Click the arrow to return to the event view.

To view the predefined event handler settings

1. Click **FortiSoC** > **Handlers** > **Event Handler List** to see all the predefined event handlers.



2. Observe on the right pane that all the predefined handlers are listed.

Not all predefined event handlers are enabled by default.

You cannot delete any of these handlers. However, you can disable them so they don't generate events.

3. Note that each entry listed shows the status of the handler, how many filters it has, from which devices it will be examining logs, and the number of events it has generated so far.

4. Find the **Default-Malicious-Code-Detection-By-Threat** handler that you used earlier in this lab, and then double-click it to see its settings.
   The window displayed is the same one you saw before, except now it doesn't show any matched filters.
5. Close the handler settings window.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Clone and Customize an Event Handler

You will create a custom event handler by cloning an existing one, and then making the required changes to the clone.

To clone and customize an event handler

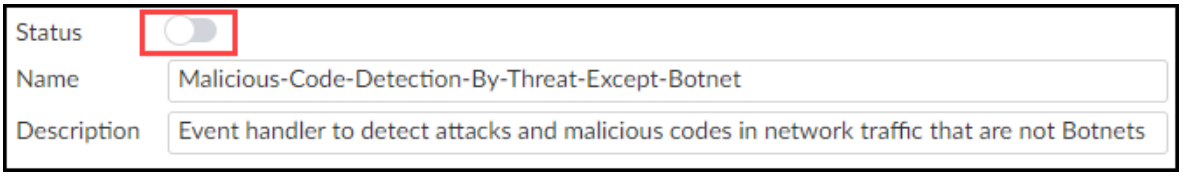
Stop and think!

You now know which predefined event handler created the event we are interested in.

For this exercise, let's pretend that this specific event requires special attention, and an email notification must be sent every time it is detected. To achieve this, you will create a new, custom event handler.

1. Continuing in the **Event Handlers List**, right-click **Default-Malicious-Code-Detection-By-Threat**, and then select **Clone**.

   A new window opens with all the settings now available for editing.
2. Change the name of the new handler to `Malicious-Code-Detection-By-Threat-Except-Botnet`. This name is based on the generic text filter that is part of the current **Filter 3**.
3. Change the description to `Event handler to detect attacks and malicious codes in network traffic that are not Botnets`.
4. Verify that the top section of the new handler looks like the following image:



5. Click the trash icons to the right of **Filter 4** to **Filter 8** to delete them, and then click the button to disable **Filter 1** and **Filter 2**.

Stop and think!

We determined earlier that **Filter 3**, in the predefined event handler, is generating the events we are concerned about. That is why we are disabling or deleting the rest.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

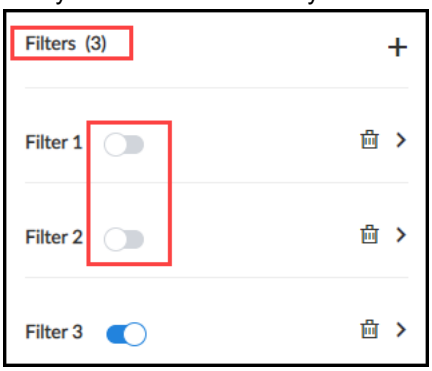
DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Be careful when you delete filters because the numbers are automatically adjusted and you can get them mixed up.

You should always start deleting the filters with the higher numbers first to avoid confusion.

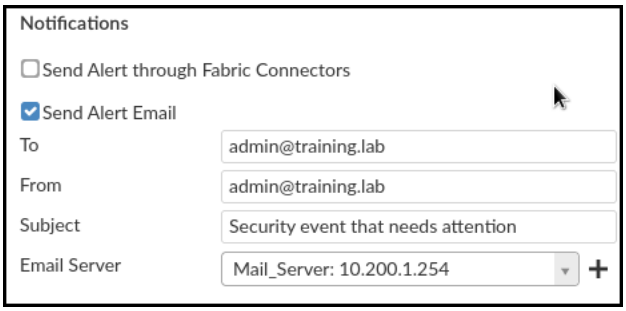
In general, it is recommended that you disable filters instead of deleting them.

6. Verify the **Filters** section in your cloned handler looks like the following image:



7. Edit **Filter 3** to set the amount of time between matches that will generate events to 5 minutes.

8. Edit the **Notifications** section at the bottom to look like the following image:



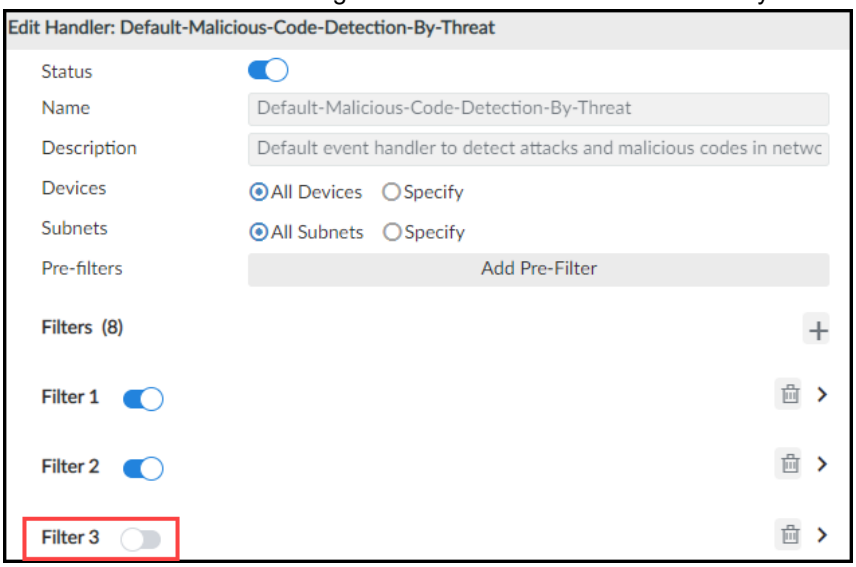
Note that the email server at `10.200.1.254` was already configured for you.

9. Click **OK** to close the handler settings page and return to the **Event Handlers List**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

10. Open the original handler, **Default-Malicious-Code-Detection-By-Threat**, and then disable its **Filter 3**.
We don't want this handler to generate events based on that filter anymore.



11. Click **OK** to save the changes.
12. Find the new handler that you created.
Since it is disabled, it will be at the bottom of the list.
You can also use the search bar in the upper-right corner.

When you use the search bar, try to be as specific as possible because the **Filters** column will be expanded for all matches.

13. Notice the email address under the **Send Alert to** column.
14. Right-click the handler, and then select **Enable**.
The handler will be moved higher in the list and join the other handlers with the same status.

Generate Traffic to Create Events

You will generate some traffic to test the functionality of the new event handler.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

To generate traffic using Nikto

1. On Local-Client, open the PuTTY application, and then connect to the LINUX saved session.
2. Log in with the username `student` and password `password`.
3. Enter the following command:
   ```
   nikto.pl -host 10.200.1.10
   ```
4. Leave the script running.

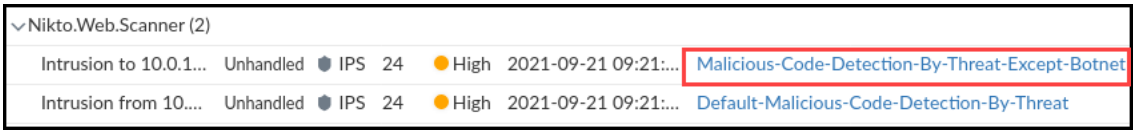
Verify the New Event Handler Works

The traffic being generated should trigger the new event handler to create new events. You will verify the new event handler generated new events.

To verify the custom handler generated new events and sent a notification email

1. Return to **FortiSoC** > **Event Monitor** > **All Events**.
2. Filter the view to the last 30 minutes and change the refresh rate to 10 seconds.

3. Verify that new events are showing while paying close attention to the **Event** column and looking for an entry called **Nikto.Web.Scanner**.
   Once you see that entry, expand it, and then wait until at least one of the events listed is generated by the custom handler you created.



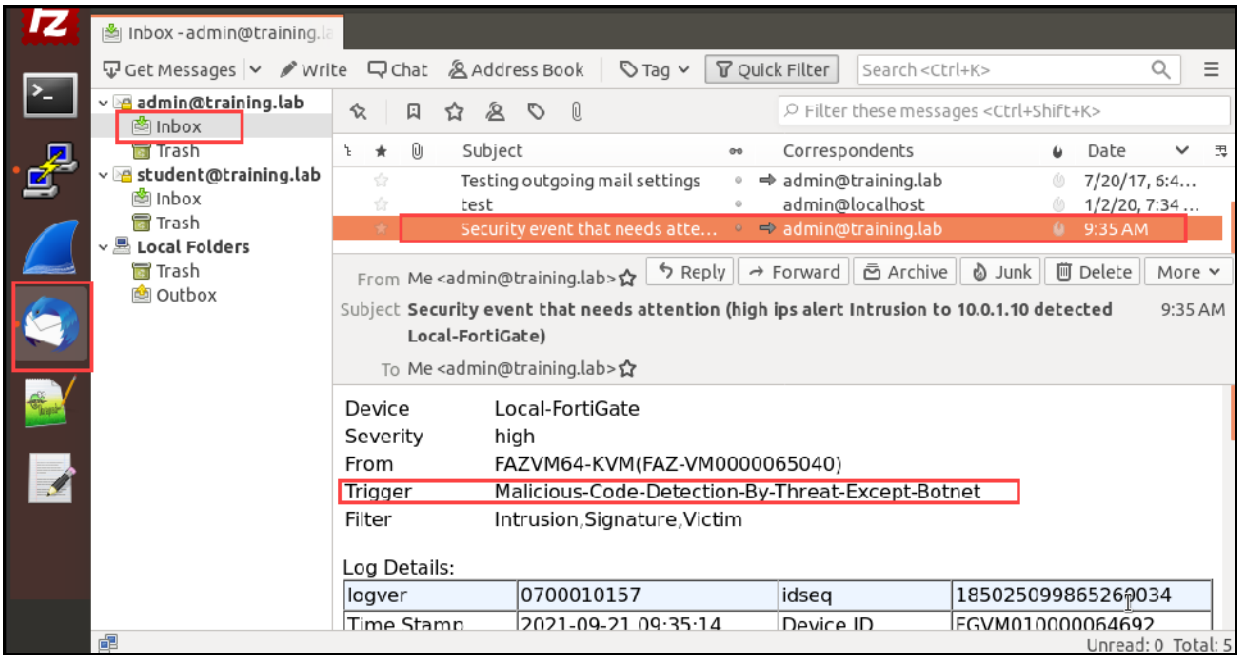
4. Return to the PuTTY session, and then press `Ctrl+Z` to stop the script.
5. Return to the **Event Handlers List** to verify there is at least one event generated by the new handler.

   You may have more than one, depending on how long you left the Linux script running.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

6. Open the Thunderbird email client, and then verify you received an email notification with the configured subject in the **admin** mailbox.



Note that it may take several seconds for the email to appear in Thunderbird.

7. Log out of FortiAnalyzer.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 3: Creating a Custom Event Handler

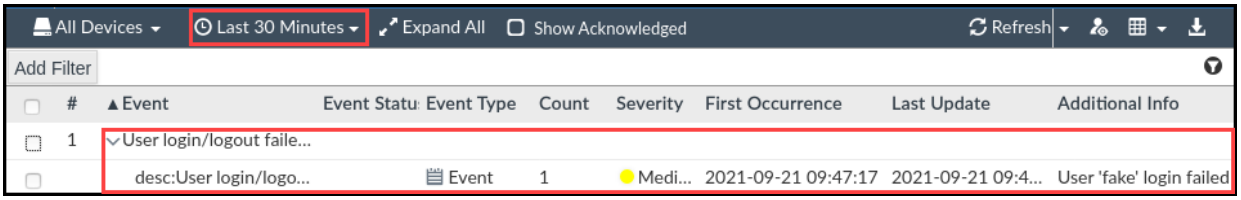
In this exercise, you will generate an event by using a wrong set of credentials to log in to FortiAnalyzer. Then, you will verify that the log generated, and then create a new handler that will send a notification email when another event like that occurs.

Create an Event and Find the Log That Generated It

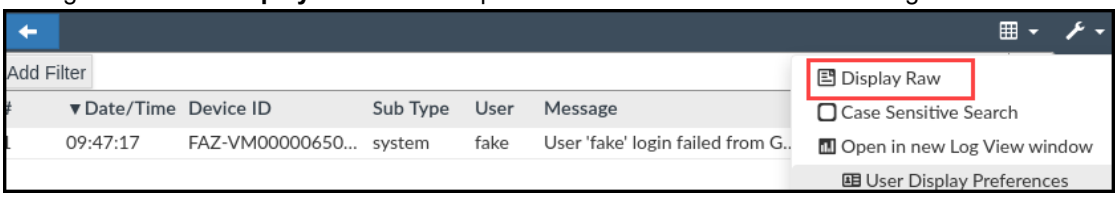
You can view the details of existing events to use them as a reference when you create custom event handlers.

To force the generation of an event and view the log that generated it

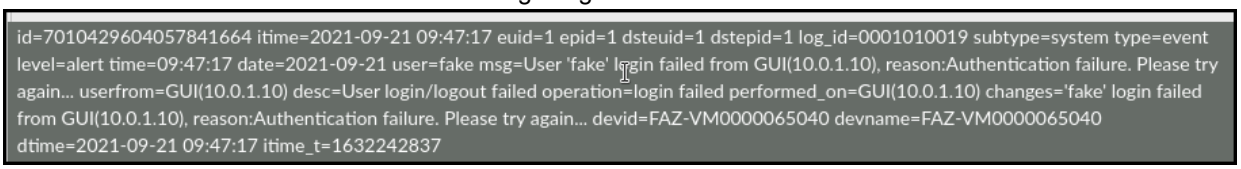
1. Log in to the FortiAnalyzer GUI with the username `fake` and password `fake`.
   This user does not exist, so you will receive an error that prevents you from logging in.
2. Log in with the correct credentials—`admin` and `password`—and then click the **root** ADOM.
3. Click **FortiSoC** > **Event Monitor** > **System Events** > **Local Device**.
4. Filter the view to include only the **Last 30 Minutes**.
   You should see the event that the failed login attempt generated.



5. Double-click the event to see the details of the log that generated it.
6. Change the view to **Display Raw** to find all parameters that can be used to create generic text filters.



The raw view should look similar to the following image:



Each of the fields in this view can be used as part of a generic text filter. You will use a very simple example to learn how to use them.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

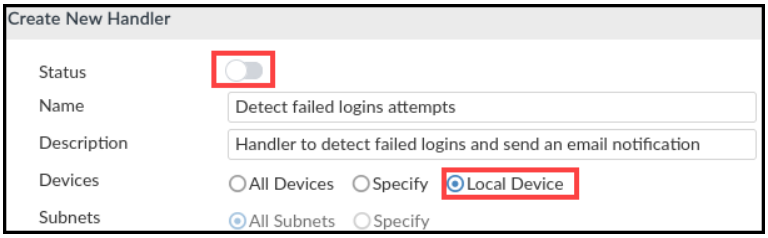
DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Create a Custom Event Handler

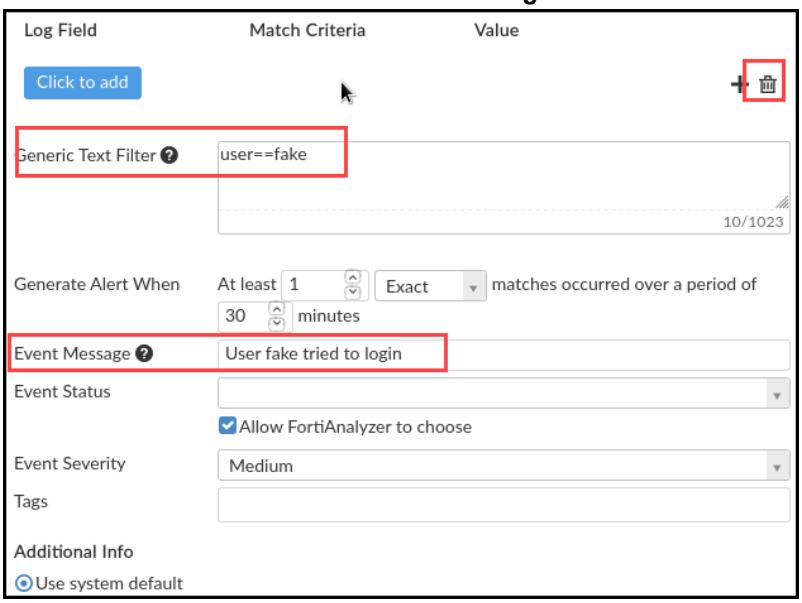
Now that you know the details of the log created after a failed login attempt, you will create a custom event handler based on those details.

To create a new event handler

1. Click **Handlers** > **Events Handler list**.
2. Click **Create new**.
3. Disable the new handler while you edit it.
4. Change the handler name to `Detect failed logins attempts`.
5. Change the handler description to `Handler to detect failed logins and send an email notification`.
6. Select **Local Device**, and then click **OK** to accept the **Reset Filters** warning.
   This warning states that the filters available depend on the type of device that you select.



7. Click the trash icon to the right of the **Log Field** filter to remove it.
8. Edit the **Generic Text Filter** and **Event Message** fields to match the following image:

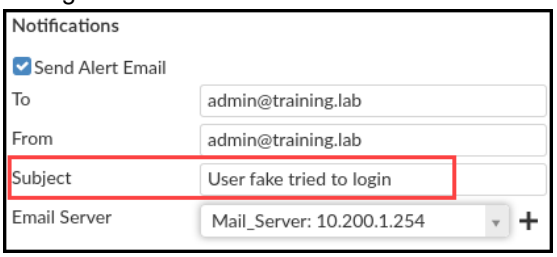


This filter will match only when a user tries to log in with the username **fake**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

9. Configure this handler to send an email with the **Subject** of `User fake tried to login`.



10. Enable the new handler, and then click **OK**.

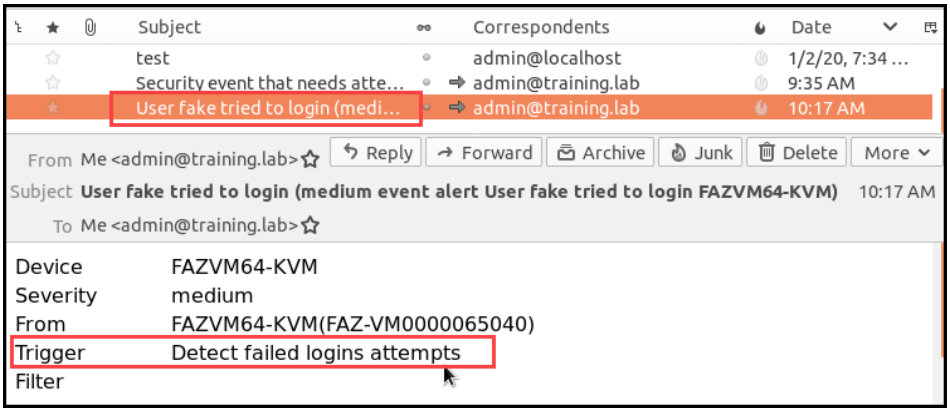
Test the Custom Event Handler

You will test the custom event handler by attempting to log in with the wrong credentials.

To verify the new event handler works

1. Log out of the FortiAnalyzer GUI, and then try to log in again using the username `fake`.
2. Log in to the **root** ADOM again with the username `admin` and password `password`.
   You should see that one event was generated by the new handler.

3. Open the Thunderbird email client, and then verify that a new email was received with the correct subject.



4. Close the email client, and then log out of FortiAnalyzer.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Expert Challenge

Take the Expert Challenge!

Create another generic text filter.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

Edit the generic text filter in the custom event handler that you created in this exercise so it generates an event when a potential intruder tries to log in as the `admin` user, from any device other than the Local-Client VM.

Challenge solution

1. Review the original raw log.

```
id=7010429604057841664 itime=2021-09-21 09:47:17 euid=1 epid=1 dsteuid=1 dstepid=1 log_id=0001010019 subtype=system type=event level=alert time=09:47:17 date=2021-09-21 user=fake msg=User 'fake' login failed from GUI(10.0.1.10), reason:Authentication failure. Please try again... userfrom=GUI(10.0.1.10) desc=User login/logout failed operation=login failed performed_on=GUI(10.0.1.10) changes='fake' login failed from GUI(10.0.1.10), reason:Authentication failure. Please try again... devid=FAZ-VM0000065040 devname=FAZ-VM0000065040 dtime=2021-09-21 09:47:17 itime_t=1632242837
```

2. Notice the **user**, **performed_on**, and **operation** fields in the log.
3. Edit the generic text filter with `user==admin` to match any login attempts with that user.
4. Add the text `operation=="login failed"` to match only failed login attempts.
   If you don't include this condition, you will get more matches than what is required.
5. Add the text `performed_on!~10.0.1.10`.
   This includes any attempts coming from devices with an IP address that is not the one configured on the Local-Client computer.

You need this syntax because the requirements do not specify the method the attacker uses to try to access FortiAnalyzer.

If you were looking only for attempts using a browser, you could use `performed_on!="GUI(10.0.1.10)"` instead.

If you were looking only for attempts using SSH, you could use `performed_on!="ssh(10.0.1.10)"` instead.

6. Combine the three conditions with a logical `and`.
   `operation=="login failed" & user==admin & performed_on!~10.0.1.10`

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 4: Managing Incidents

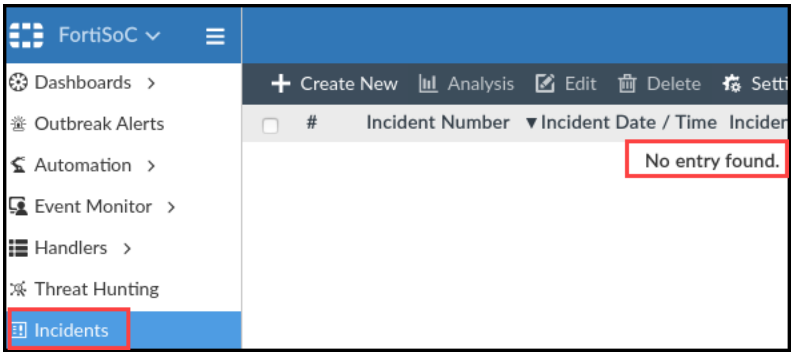
In this exercise, you will practice how to create, or raise, an incident manually in FortiAnalyzer, and you will explore some of the tools available to security analysts to work with existing incidents.

Create New Incidents Manually

You will create a new incident from several events that must be investigated.

To create an incident manually

1. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. Click **NEW**.
3. Click **FortiSoC**.
4. Click **Incidents**.
   As you saw before in the dashboard with the same name, no incidents have been created in this environment yet.

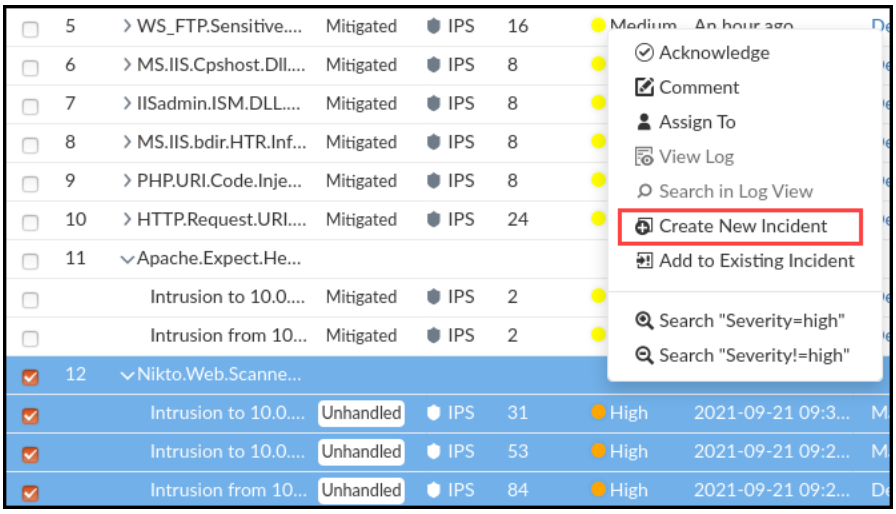


   Incidents can be raised from events the SOC analysts think require further investigation. For example, an event that appears as **Unhandled** should always be examined.

5. Click **FortiSoC** > **Event Monitor** > **All Events**.
6. Find the entry labeled **Nikto.Web.Scanner**.
   Remember you can adjust the filter to help you with your search.
7. Right-click the **Nikto.Web.Scanner** entry, and then select **Create New Incident**.
   This creates an incident that contains all the events within that entry.

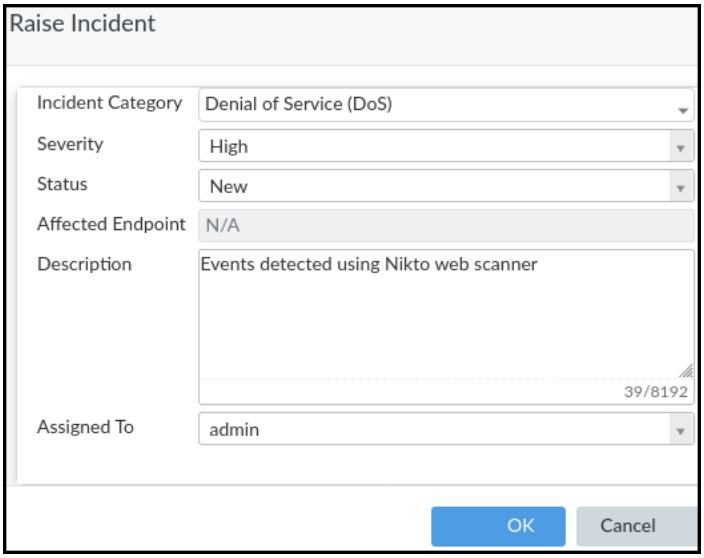
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



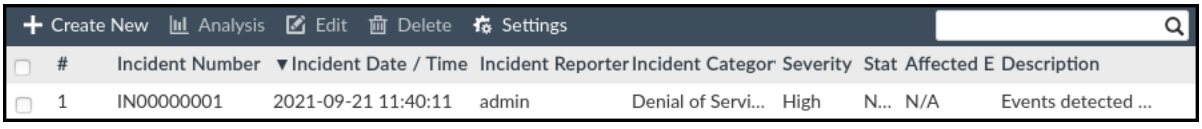
When creating an incident from a filtered view, the number of events included in the incident depends on the time period filter set and how many were generated during that time frame.

8. Explore the available options on the **Raise Incident** window.
9. Edit each field to match the following image, and then click **OK**.



In a production scenario, these values must be adjusted according to the severity and urgency of the event.

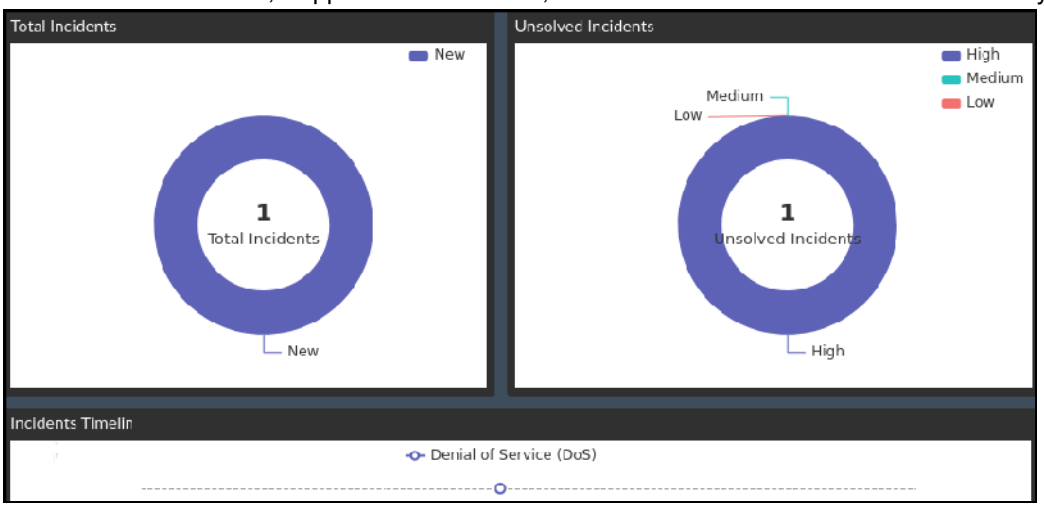
10. Click **Incidents**.
Now, you should see the incident you just created.



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

11. Verify the new incident appears in the **Incidents** dashboard.
Since it's a new incident, it appears as **Unsolved**, and the color code used indicates its severity.



This dashboard allows SOC analysts to easily get an overview of how up to date, or not, their team is in dealing with security incidents.

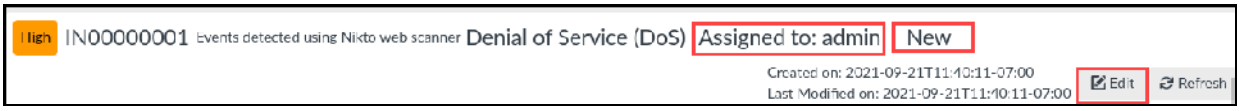
For example, depending on how many unsolved incidents are present, and what their severity is, higher priority can be given to the most important ones.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

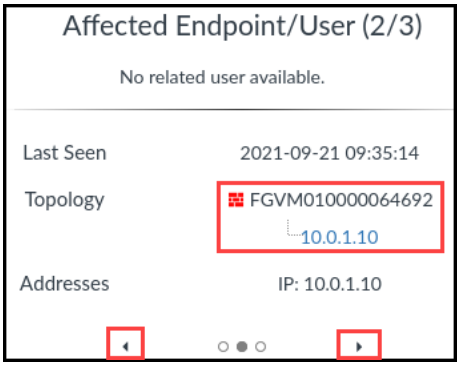
DO NOT REPRINT
© FORTINET
Brave-Dumps.com

To examine the incident analysis window

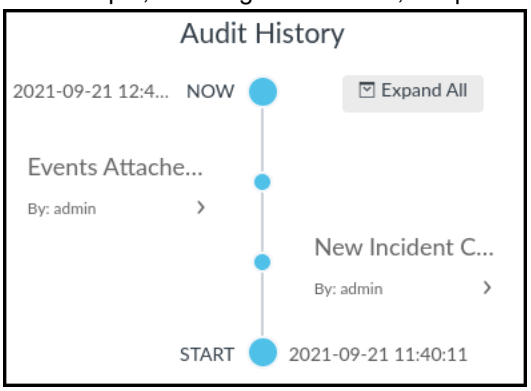
1. Return to **FortiSoC** > **Incidents**, and then double-click the current incident to open its **Analysis** page.
2. Examine the top of this page.
   This section provides general information about the incident, and the ability to edit its settings.



3. Examine the **Affected Endpoint/User** section.
   This section shows all devices and users (if available) involved in the incident. You can change which one is displayed by clicking on the navigation buttons. Clicking on the device IP will open **Fabric View** in a new window.



4. Examine the **Executed Playbooks** section.
   This section includes any playbooks associated with the incident, and allows you to execute them, if required.
5. Examine the **Audit History** section.
   This section allows you to keep track of all the activity since the incident was created.
   For example, following our scenario, this panel should look like the following image:

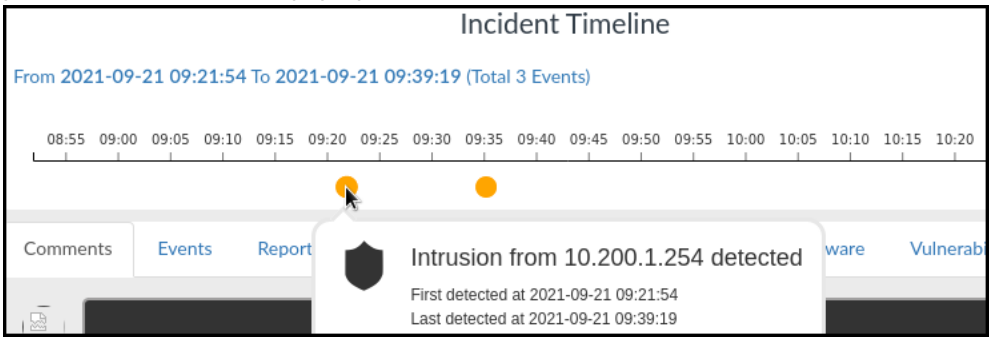


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

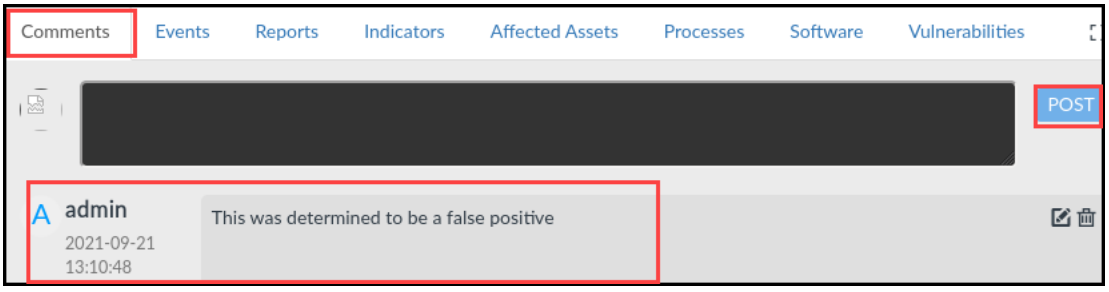
DO NOT REPRINT
© FORTINET
Brave-Dumps.com

6. Click **Edit**, change the status of the incident to **Analysis**, and then click **OK**.
This change is reflected in the **Audit History**. You might need to refresh the **Analysis** page to see the update.

7. Examine the **Incident Timeline** section.
This section provides the exact dates and times the suspicious traffic was detected. Hovering over the yellow dots provides more details in a pop-up window. You can also use the mouse to zoom in or out on the timeline.



8. Examine the different tabs available at the bottom.
9. Click the **Comments** tab, start typing your comment in the text box, and then click **Post** when you are done.
In the following example, the analyst determined this incident was only a false positive:

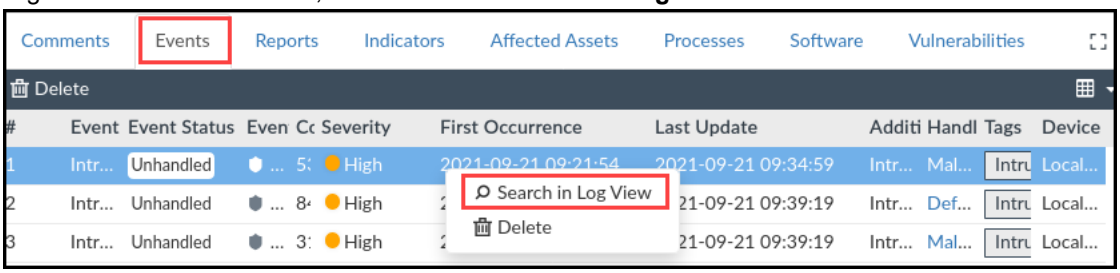


10. Verify that this action is also reflected in **Audit History**.
11. Click the **Events** tab to see all associated events.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

12. Right-click one of the events, and then select **Search in Log View**.

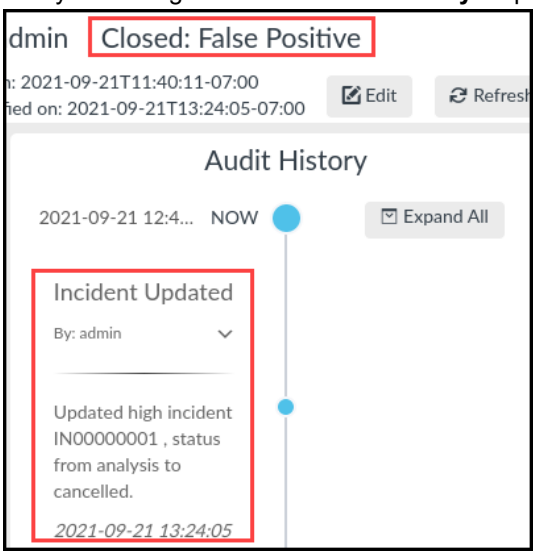


This opens **Log View** in a new window with the related filter already applied.

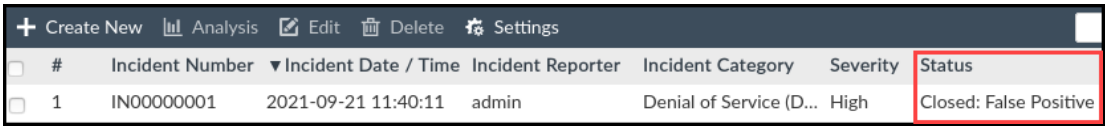
13. Explore the other tabs to see the information they include.
Depending on the type of events associated with the incident, some of them may not have any data available.

14. Change the incident status to **Closed: False Positive**.

15. Verify the change is reflected on the **Analysis** page.



16. Verify the change is also reflected in **FortiSoC** > **Incidents**.



Closing an incident does not remove it from the list. The time to remove it depends on the security policy in place.

You should remove a closed incident only when you are sure it will not need to be reopened again. This is especially important in environments dealing with a high volume of security related activity.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

17. Return to the **Incidents** dashboard, and then see that the number of unsolved incidents is now zero.

18. Log out of FortiAnalyzer.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 5: Exploring Threat Hunting

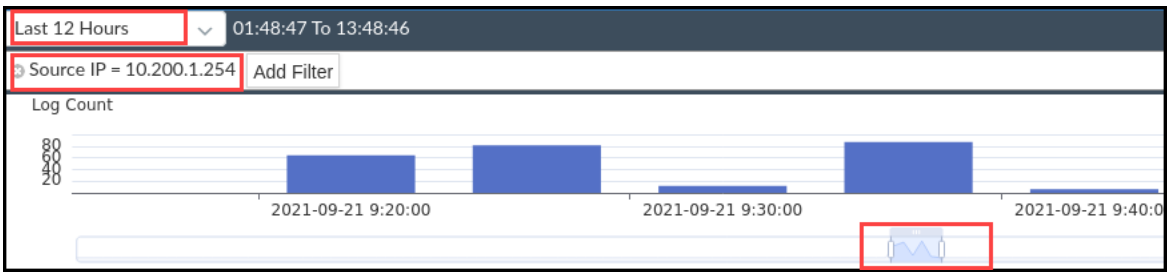
In this exercise, you will explore the threat hunting tools available on FortiAnalyzer.

Threat hunting uses a proactive approach when dealing with security threats. Many times, an apparently harmless event can precede a dangerous attack. For example, intensive network activity at unexpected times of the day can be a sign of something worse coming later.

Explore the Threat Hunting Tools

To access the tools

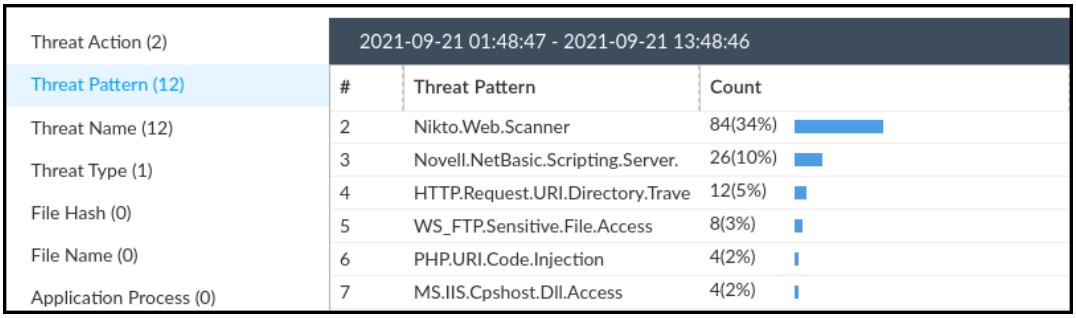
1. Click **FortiSoC** > **Threat Hunting**.
2. On the right pane, observe the **Log Count**.
3. Use the time filter to specify a time frame, and then use your mouse or the time bar below to focus on logs received at those times.



When you use the **Log Count** chart, you apply the same filters available in **Log View** to narrow down the details displayed.

For example, you can apply a filter to include traffic during the weekend or outside of office hours, and from specific IP addresses.

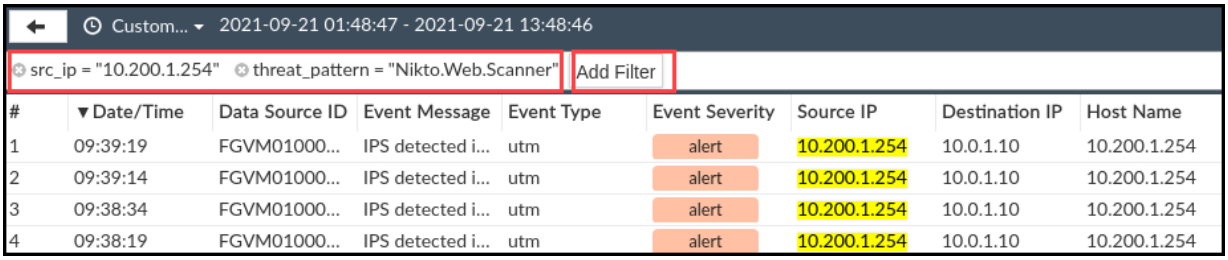
4. Observe the **SIEM Analytics table** under the **Log Count** chart.
This panel provides more details about the logs included in the selected time frame and filters.



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

5. Double-click an entry to show the same information available in **Log View**, including all the filtering capabilities.

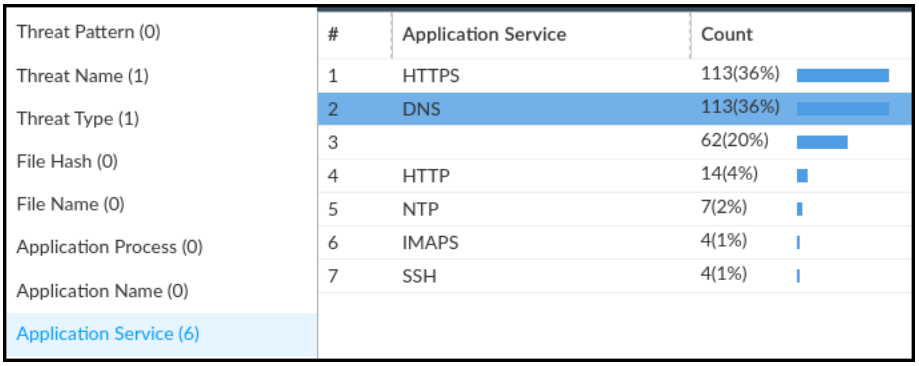


#	Date/Time	Data Source ID	Event Message	Event Type	Event Severity	Source IP	Destination IP	Host Name
1	09:39:19	FGVM01000...	IPS detected i...	utm	alert	10.200.1.254	10.0.1.10	10.200.1.254
2	09:39:14	FGVM01000...	IPS detected i...	utm	alert	10.200.1.254	10.0.1.10	10.200.1.254
3	09:38:34	FGVM01000...	IPS detected i...	utm	alert	10.200.1.254	10.0.1.10	10.200.1.254
4	09:38:19	FGVM01000...	IPS detected i...	utm	alert	10.200.1.254	10.0.1.10	10.200.1.254

Example of a Threat Hunting Scenario

Note: The images shown here do not represent a real attack. They are used only to illustrate the scenario described.

- With the help of the **Log Count** chart, an analyst discovered an unusual amount of DNS traffic was occurring during the weekend.
- The **SIEM Analytics table** showed that, during that time, 72% of the traffic consisted of HTTPS and DNS queries originating from one of the headquarter offices.



- After double-clicking the DNS entry, the logs showed that the device with the IP address `10.0.1.10` was sending continuous queries in the middle of the night.
  The same host was responsible for the unexpected HTTPS traffic.

Data Source ID	Event Message	Event Type	Event Severity	Source IP	Destination IP	Host Name
FGVM01000...		traffic	notice	10.0.1.10	8.8.8.8	10.0.1.10
FGVM01000...		traffic	notice	10.0.1.10	8.8.8.8	10.0.1.10
FGVM01000...		traffic	notice	10.0.1.10	8.8.8.8	10.0.1.10
FGVM01000...		traffic	notice	10.0.1.10	8.8.8.8	10.0.1.10
FGVM01000...		traffic	notice	10.0.1.10	8.8.8.8	10.0.1.10
FGVM01000...		traffic	notice	10.0.1.10	8.8.8.8	10.0.1.10
FGVM01000...		traffic	notice	10.0.1.10	8.8.8.8	10.0.1.10
FGVM01000...		traffic	notice	10.0.1.10	8.8.8.8	10.0.1.10
FGVM01000...		traffic	notice	10.0.1.10	8.8.8.8	10.0.1.10

- All the queries were considered normal traffic by the firewall, but further investigation brought to light that the host with IP address `10.0.1.10` had been compromised and was being used as part of a DDoS attack.
- A new incident was created, and the SOC team started to follow the procedures in the company security policy to resolve the issue.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Lab 6: Playbook Management

In this lab, you will examine the use of playbooks on FortiAnalyzer. You will learn how to create, customize, and export playbooks, and then import them to a different ADOM.

Objectives

- Create simple playbooks with an on-demand trigger
- Create and customize simple playbooks with incident triggers or event triggers
- Import and customize playbooks with multiple tasks
- Create simple playbooks using a FortiOS connector
- Examine the effect of including connectors when you export and import playbooks

Time to Complete

Estimated: 90 minutes

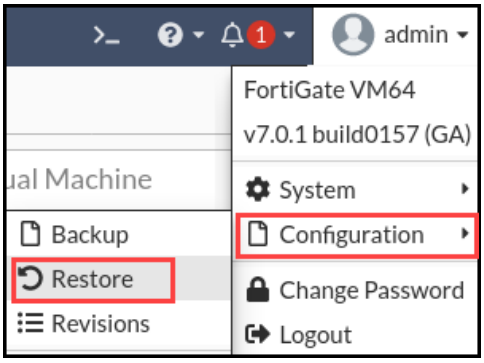
Prerequisites

Before beginning this lab, you must restore a configuration file to Local-FortiGate and ISFW.

To restore the ISFW configuration file

Make sure you restore the correct configuration file on the correct device. The name of the configuration file matches the name of the device that it must be restored on.

1. On the Local-Client VM, open a browser, and then log in to the ISFW GUI at `10.0.1.200` with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



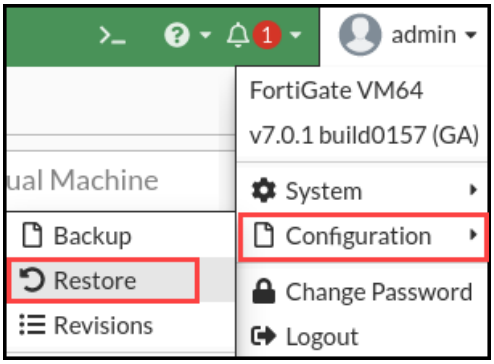
3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **FortiAnalyzer** > **LAB-6** > `ISFW.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

To restore the Local-FortiGate configuration file

1. On the Local-Client VM, open a browser, and then log in to the Local-FortiGate GUI at `10.0.1.254` with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



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

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 1: Creating a Playbook With an On-Demand Trigger

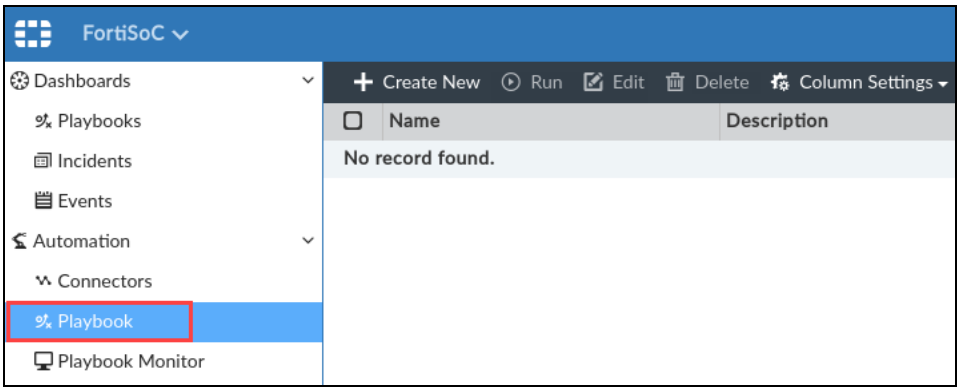
In this exercise, you will create a simple playbook to generate an incident. The playbook will use an on-demand trigger and one task. You will also explore how to check the log associated with the playbook run, and verify it was executed as intended.

Create a New Playbook With an On-Demand Trigger

The creation of new playbooks is very simple. You will create a new playbook.

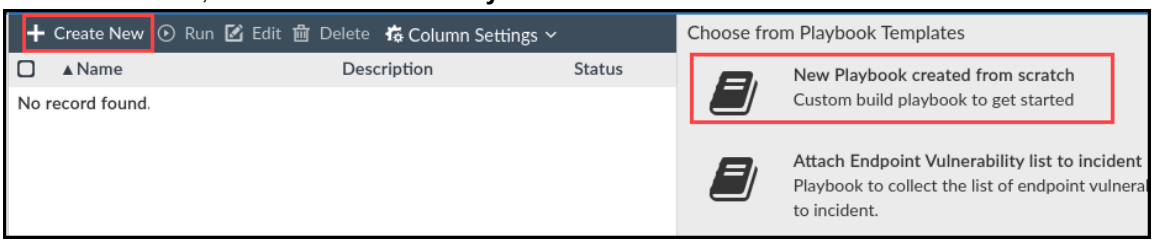
To create a new playbook from scratch

1. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. Click **NEW**.
3. Click **FortiSoC**.
4. Click **Automation** > **Playbook**.



There are no playbooks created by default.

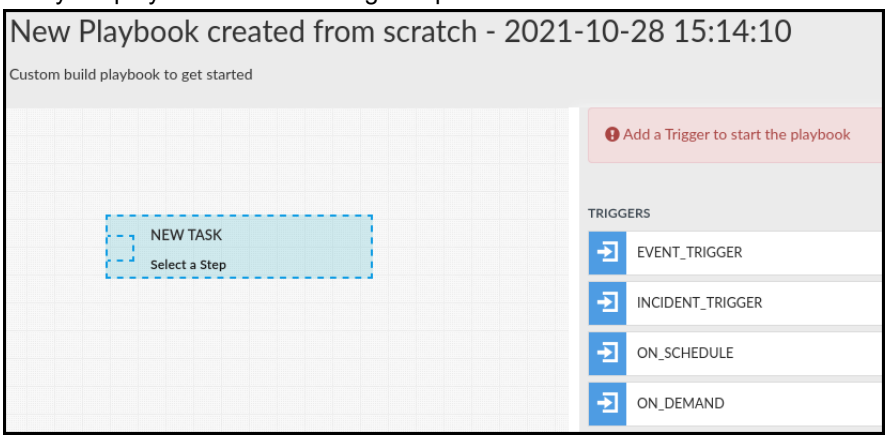
5. Click **Create New**, and then select **New Playbook created from scratch**.



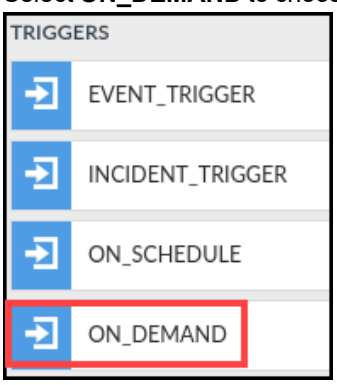
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

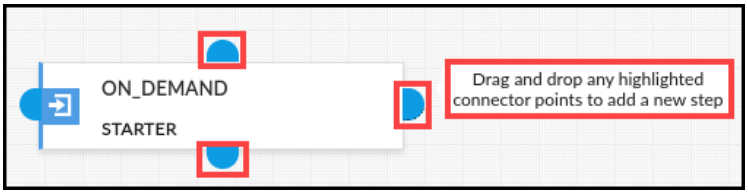
6. Verify the playbook editor or designer opens.



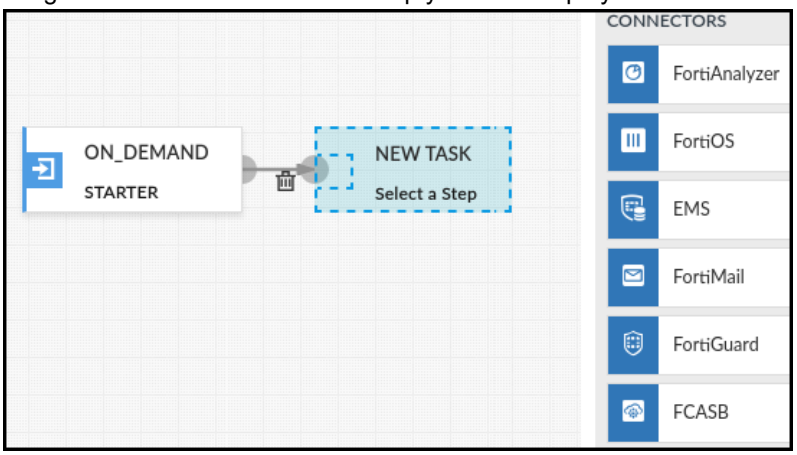
7. Select **ON_DEMAND** to choose that trigger type.



8. Verify the playbook editor displays your choice, and then notice the hint provided about how to add a new task.



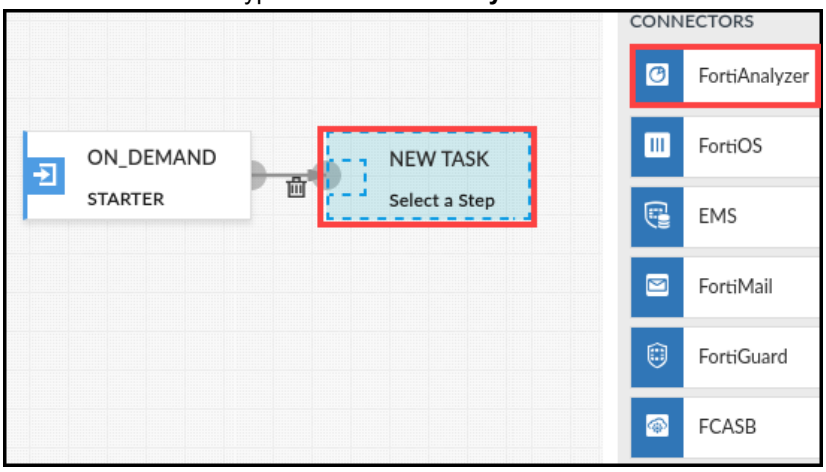
9. Drag one of the connectors to an empty area in the playbook editor.



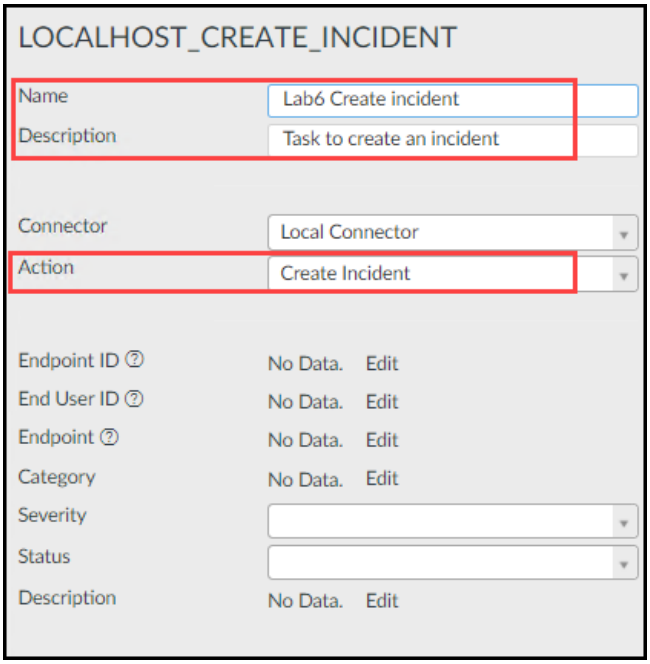
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

10. Select the connector type labeled **FortiAnalyzer** for the new task.



11. Configure the task settings exactly as shown in the following image:

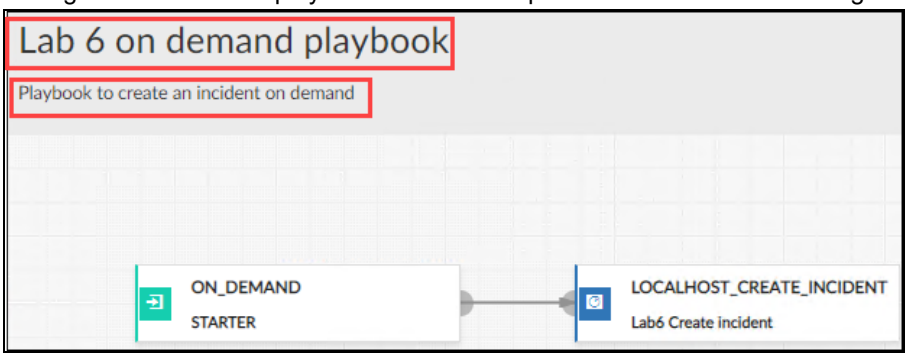


The other fields in this task are not configured intentionally. This way, you will see the playbook fail, and then explore how you can find out why it happened.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

12. Click **OK** to save the task settings and return to the playbook editor.
13. Change the name of the playbook and its description as shown in the following image:



It is important to change the default name used for playbooks.

When you have many playbooks, using poor naming conventions makes it difficult to find specific playbooks.

14. Click **Save Playbook**.
15. Return to **Automation** > **Playbook**, and then verify the new playbook is listed there.

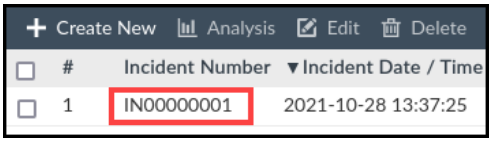
Do not try to run the playbook now because FortiAnalyzer requires some time to parse the playbook.

If you try to run the playbook before FortiAnalyzer parses it, you will receive an error like the one in the following image:

Verify the Current Number of Incidents

To verify the current number of incidents

1. Click **Incidents**, and then make a note of the number assigned to the newest incident in the list.
For example, in the following image, the newest incident is number **IN00000001**:



This step is included so you can easily identify the new incidents that are created after you run the playbooks in this lab.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

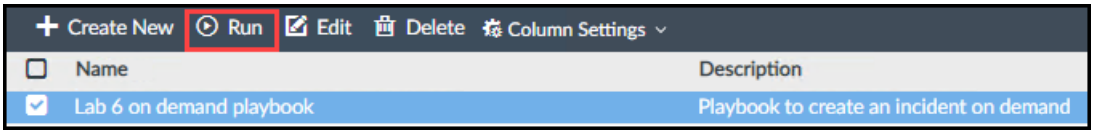
DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Run and Troubleshoot a Playbook

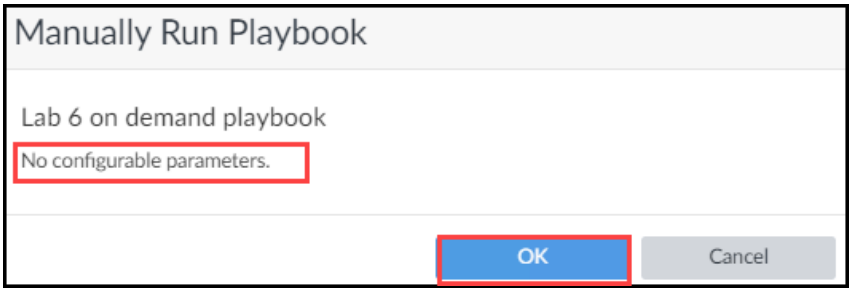
You will use the log information provided to troubleshoot a playbook that fails to run.

To run and troubleshoot a playbook

1. Return to **Automation** > **Playbook**.
2. Select the playbook you created, and then click **Run**.



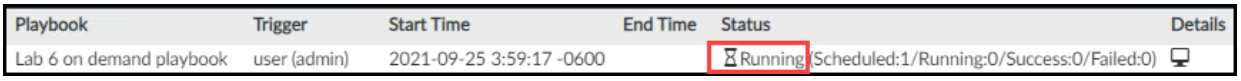
3. Click **OK** to run the playbook manually.



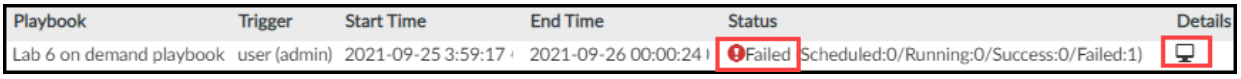
Notice there are no parameters that you can configure. This is the reason this playbook will fail, which you will verify later.

The required parameters vary depending on the type of task.

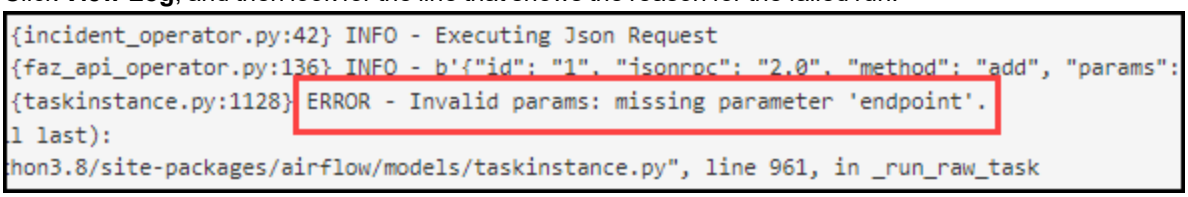
4. Click **Playbook Monitor**.
The status of the new playbook should be **Running**.



5. Click **Refresh** a few times to see the status change.
It will take several seconds.
6. Verify the playbook fails, and then click **Details**.



7. Click **View Log**, and then look for the line that shows the reason for the failed run.



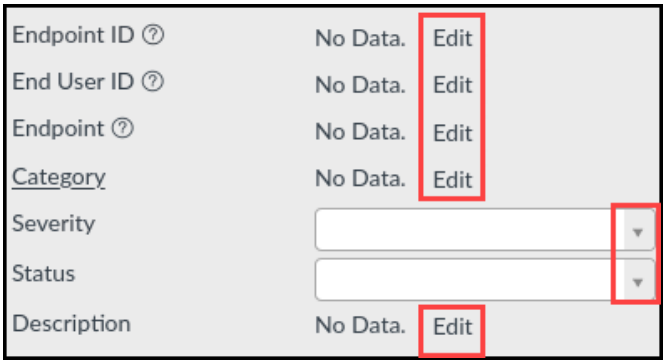
8. Click **Close** twice to return to **Playbook Monitor**.
9. Return to **Automation** > **Playbook**.
10. Double-click the playbook to open it in the editor.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

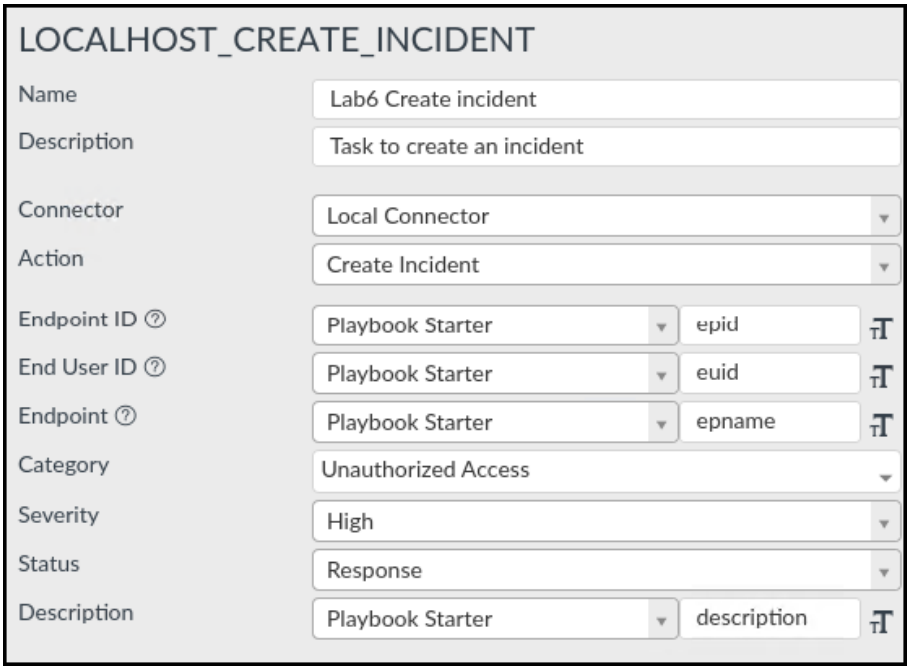
DO NOT REPRINT
Brave-Dumps.com
© FORTINET

11. Click the edit button on the task.

12. Click **Edit** for each of the parameters and the drop-down menus as shown in the following image:



13. Verify the final settings match those shown in the following image:



The **Playbook Starter** option used here prompts you to select, or type, the parameters manually.

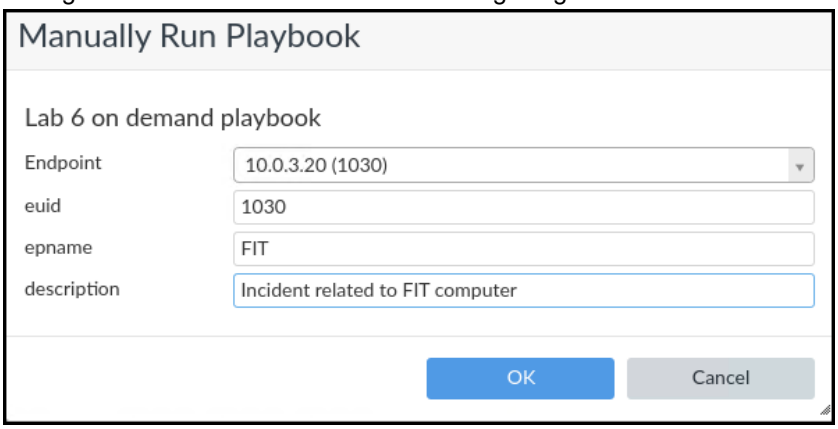
Although it may not look very automated, this option can be useful if, for example, you want to run the same playbook for different endpoints or users.

14. Click **OK** to save the changes.
15. Click **Save Playbook**.
16. Return to **Automation** > **Playbook**.

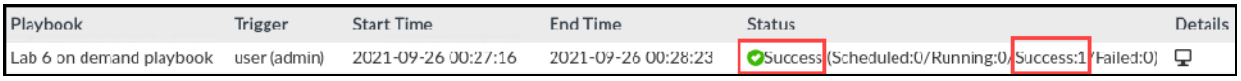
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

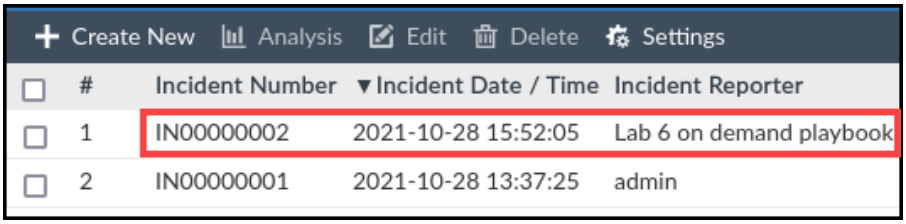
17. Click the playbook, and then run it again.
    This time you are prompted to configure some parameters.
18. Configure each field as shown in the following image:



    Note that the value shown in parentheses in the **Endpoint** field is the **euid**, and it may be different in your environment.
19. Click **OK**.
20. Click **Playbook Monitor**.
21. Click **Refresh** every couple of seconds until the status is **Success**.



22. Click **Incidents**, and then verify a new incident was created.



23. Double-click the new incident, and then verify its settings match the settings in the playbook task.
24. Log out of FortiAnalyzer.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 2: Creating a Playbook With an Incident Trigger

In this exercise, you will create a playbook that uses an incident trigger and contains a task that updates an existing incident.

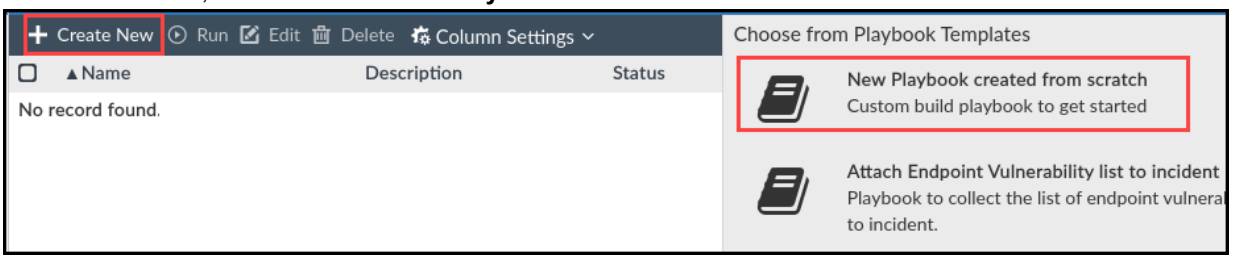
You will also explore how trigger variables are used to allow a task to use parameters provided by the trigger.

Create a Playbook With an Incident Trigger

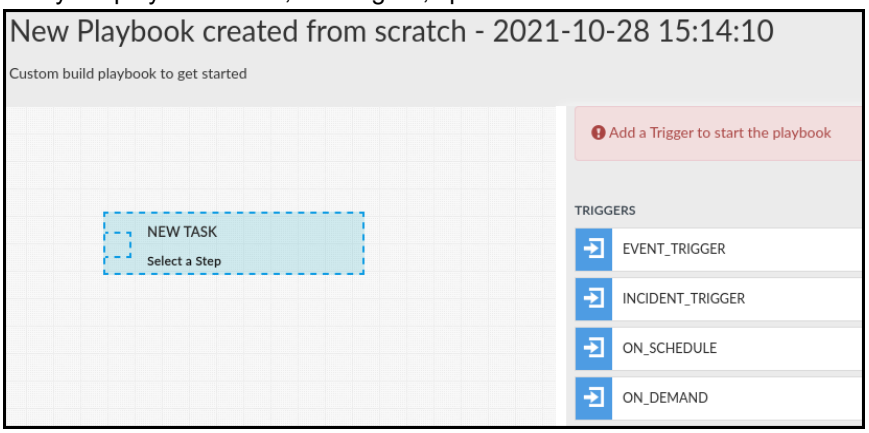
Using an incident trigger makes a playbook run when an incident with the specified criteria is detected. You will create a playbook with an incident trigger.

To create a playbook with an incident trigger

1. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. Click **NEW**.
3. Click **FortiSoC**.
4. Click **Automation** > **Playbook**.
5. Click **Create New**, and then select **New Playbook created from scratch**.



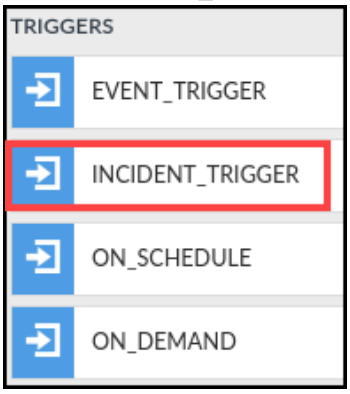
6. Verify the playbook editor, or designer, opens.



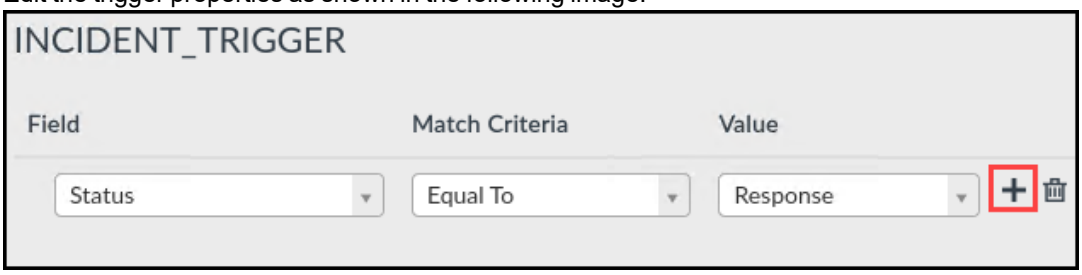
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

7. Select **INCIDENT_TRIGGER** to choose that trigger type.



8. Edit the trigger properties as shown in the following image:



Response is the incident status that you configured for the **On_Demand** playbook in the previous exercise.

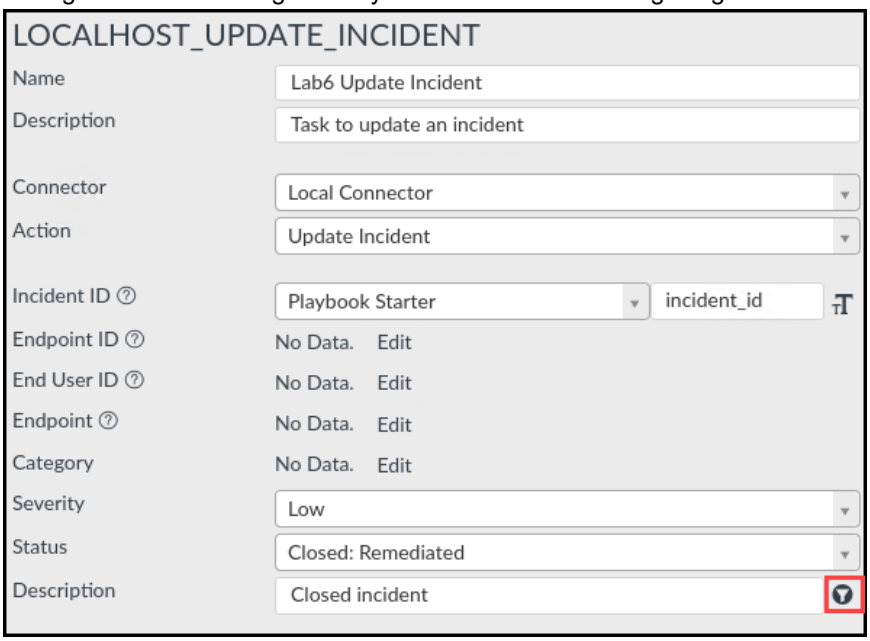
You will run that playbook again, and that will trigger this playbook to make some changes to the incident created by the former playbook.

9. Click **OK** to save the changes.
10. Drag one of the connectors to an empty area in the playbook editor.
11. Select the connector type labeled **FortiAnalyzer** for the new task.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

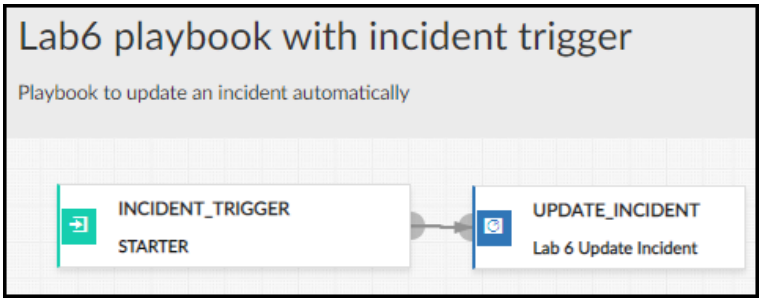
12. Configure the task settings exactly as shown in the following image:



Note that to complete the **Description** field, you must click **Edit**, and then click the icon on the right to change to text mode.

> **Stop and think!**
>
> In this case, only the **Incident ID** parameter is required—the trigger provides this parameter. This means the trigger tells this task the incident that must be updated using a trigger variable.
>
> Notice the changes in the bottom three fields, since they are reflected in the incident once it is updated.

13. Click **OK** to save the changes and return to the playbook editor.
14. Change the name and description of the playbook as shown in the following image:



15. Click **Save Playbook**.
16. Return to **Automation** > **Playbook**, and then verify the new playbook is listed.

17. Wait for five minutes to make sure FortiAnalyzer finishes the parsing process, and then continue to the next step.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Verify the Playbook Runs Successfully

You will test the new playbook by running the playbook you created in the previous exercise.

To test the execution of the playbook

1. Run the **Lab 6 on demand playbook** you created in the previous exercise.
2. Click **Playbook Monitor**.
3. Click **Refresh** every few seconds to see the progress.

Stop and think!

This time, two playbooks will be executed.

First, **Lab 6 on demand playbook** will create an incident, and then **Lab6 playbook with incident trigger** will update that incident.

4. Verify both playbooks were executed successfully.

Playbook	Trigger	Start Time	End Time	Status	Details
Lab6 playbook with incident trigger	incident: (IN00000003)	2021-10-28 16:23:30 -0700	2021-10-28 16:24:3	Success (Scheduled:0/Running:0/Success:1/Failed:0)	
Lab 6 on demand playbook	user (admin)	2021-10-28 16:22:35 -0700	2021-10-28 16:23:1	Success (Scheduled:0/Running:0/Success:1/Failed:0)	

The incident number shown in brackets on the second playbook refers to the incident created by the previous playbook.

5. Click **Incidents** to verify the new incident was added and updated by the **Lab6 playbook with incident trigger**.

#	Incident Number	▼Incident Date / Time	Incident Reporter	Incident Category	Severity	Status
1	IN00000003	2021-10-28 16:23:10	Lab6 playbook with incid...	Unauthorized Access	Low	Closed: Reme...
2	IN00000002	2021-10-28 15:52:05	Lab 6 on demand playbook	Unauthorized Access	High	Response
3	IN00000001	2021-10-28 13:37:25	admin	Denial of Service (DoS)	High	Closed: False ...

6. Double-click the incident to open its **Analysis** page.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

7. In the **Audit History** pane, verify the incident activity.

8. Log out of FortiAnalyzer.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 3: Importing and Customizing a Playbook

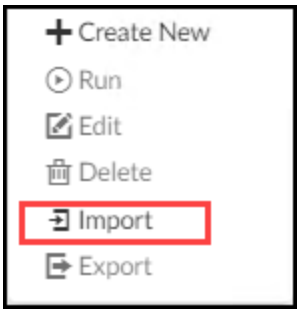
In this exercise, you will examine how to import and customize a playbook that includes multiple tasks and uses an event trigger. You will also explore how you can use output variables for one task to use the output of another task as its input.

Import and Customize a Playbook

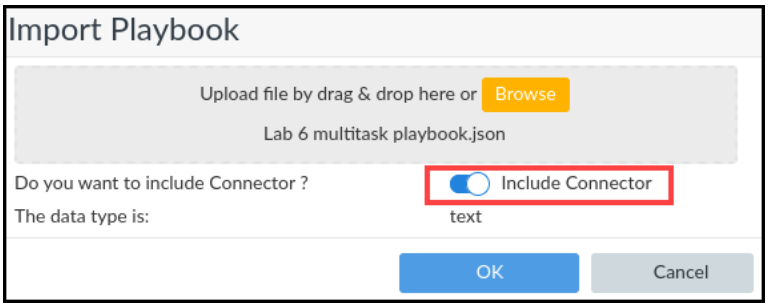
You can import a playbook created in a different ADOM or on a different FortiAnalyzer. After you import it, you can modify it to meet your needs.

To import and customize a playbook

1. On the Local-Client VM, log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. Click **NEW**.
3. Click **FortiSoC**.
4. Click **Automation** > **Playbook**.
5. Right-click an empty space in this pane, and then select **Import**.



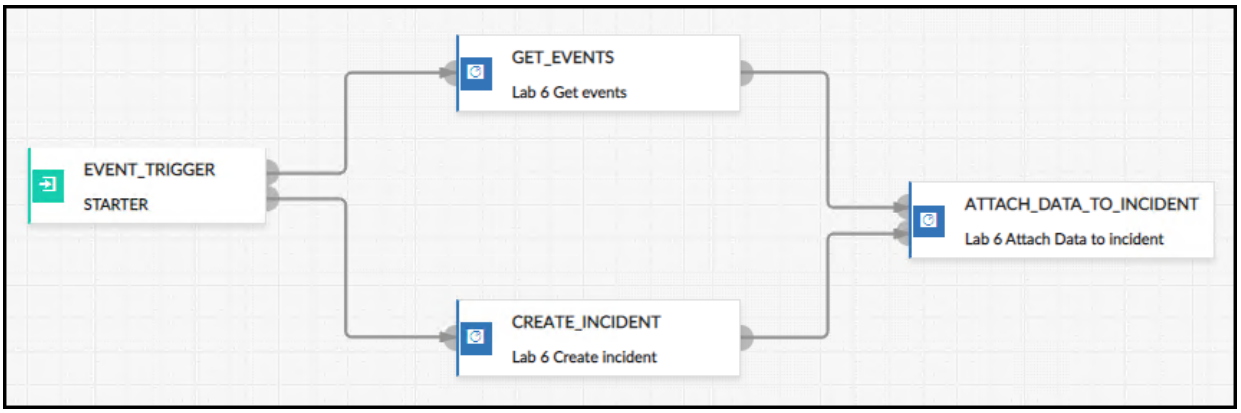
6. Click **Browse**.
7. Click **Desktop** > **Resources** > **FortiAnalyzer** > **LAB-6** > `Lab 6 multitask playbook.json`, and then click **Open**.
8. Enable the **Include Connector** option with the import.



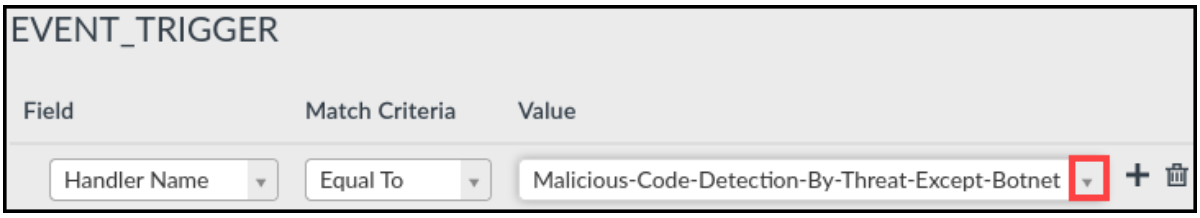
9. Click **OK** to import the playbook.
10. Double-click the playbook you just imported.
    It looks like the following image:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



11. Open, and then examine the trigger settings.

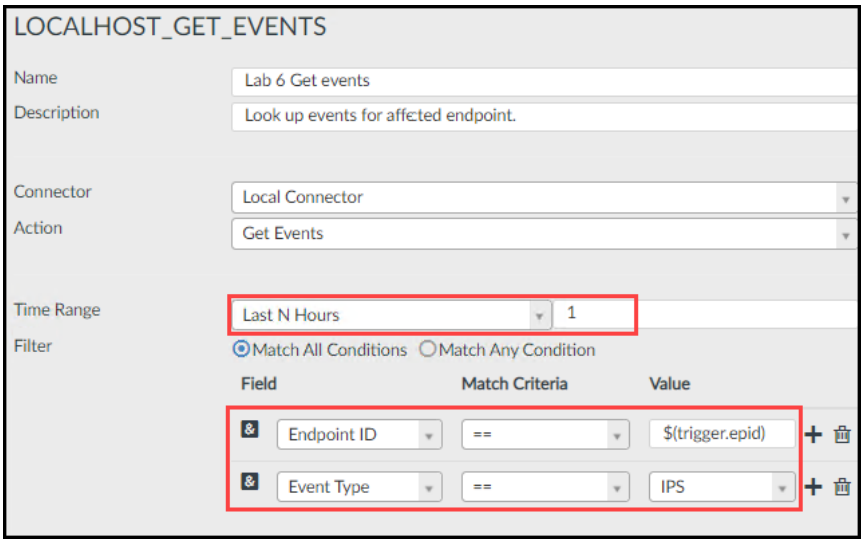


This playbook uses an **Event_Trigger** that runs when the system detects an event generated by the **Malicious-Code-Detection-By-Threat-Except-Botnet** event handler.

You created this event handler in a previous lab.

If the handler name is not displayed automatically under **Value**, click the drop-down menu, and then select it in the list.

12. Click **OK**.
13. Examine the settings of the **Lab 6 Get events** task.



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

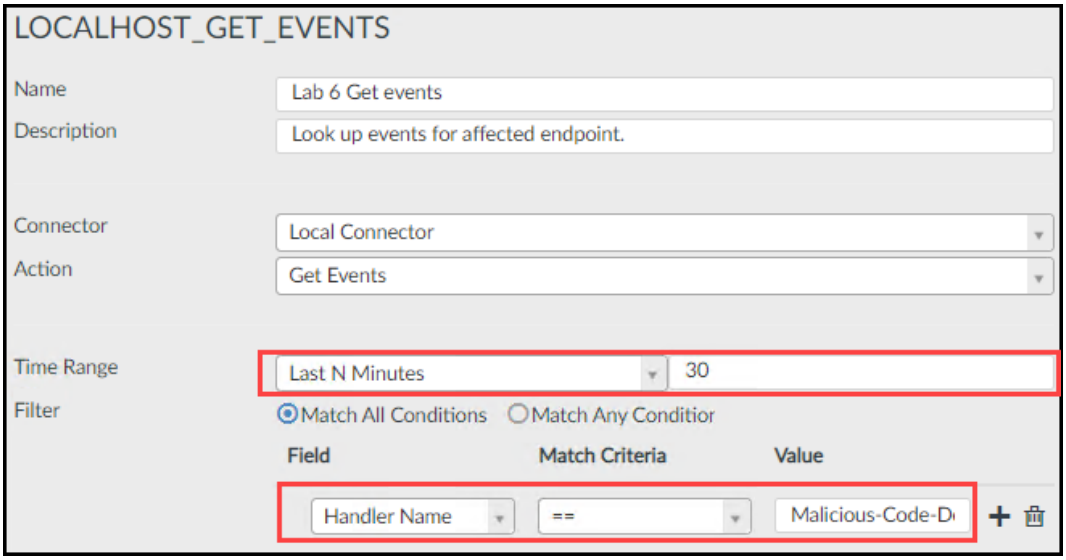
You will simplify this task so it only receives events created by the **Malicious-Code-Detection-By-Threat-Except-Botnet** handler during the last 30 minutes.

The original settings of the task would include many more events.

Notice that a **Get_Events** task is *not* restricted to the events that triggered the playbook.

Any events that match the filters in the task are fetched.

14. Edit the settings of the **Lab 6 Get events** task to match the following image:

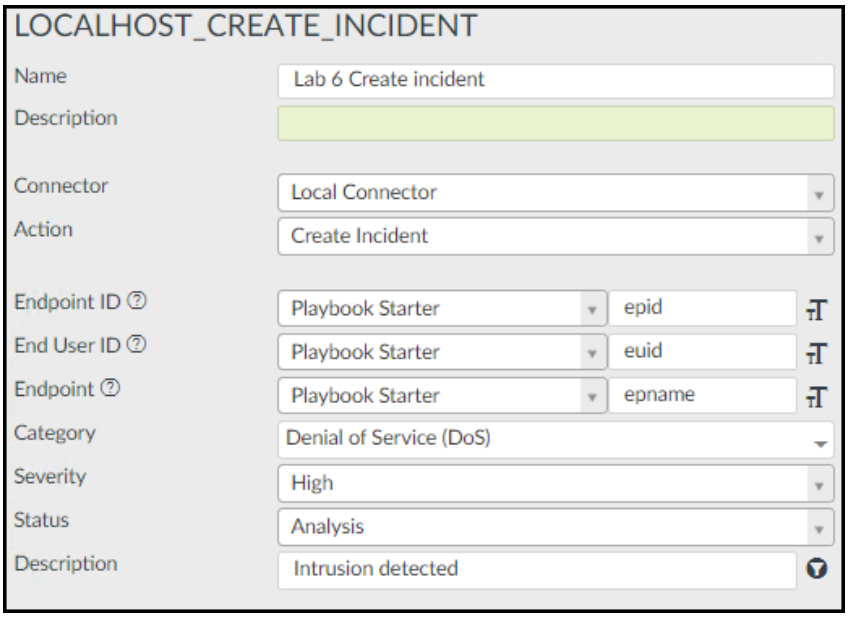


Ensure you type the name of the handler correctly, or the playbook will fail to run. The handler name should be **Malicious-Code-Detection-By-Threat-Except-Botnet**.

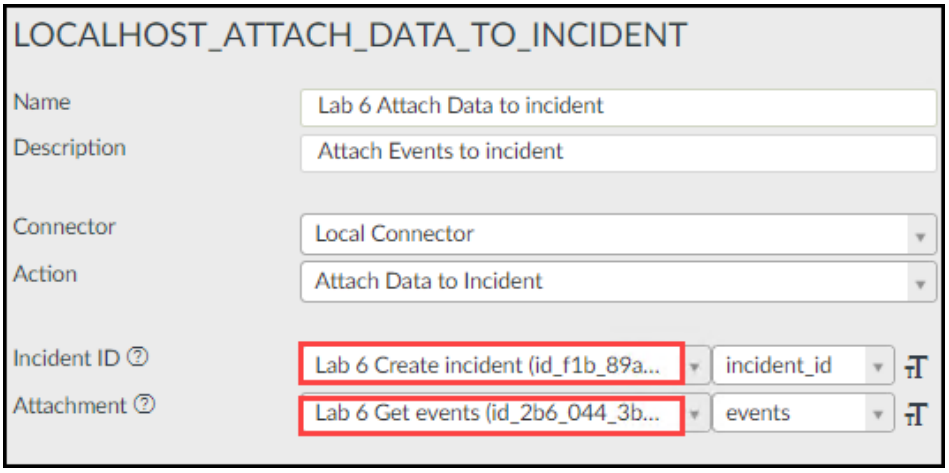
15. Click **OK** to save the changes.
16. Open the properties of the **Lab 6 Create incident** task, and then verify they match the following image:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
Brave-Dumps.com
© FORTINET



17. Click **OK**.
18. Examine the settings of the **Lab 6 Attach Data to incident** task.



> **Stop and think!**
>
> This task adds some information to an existing incident, and uses two output variables to achieve that goal.
>
> The incident that is updated is provided by the **Lab 6 Create incident** task.
>
> The information that is added to that incident are the events provided by the **Lab 6 Get events** task.

19. Click **OK** to return to the playbook editor.
20. Click **Save Playbook**.
21. Wait for five minutes to ensure FortiAnalyzer has enough time to parse the imported playbook.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

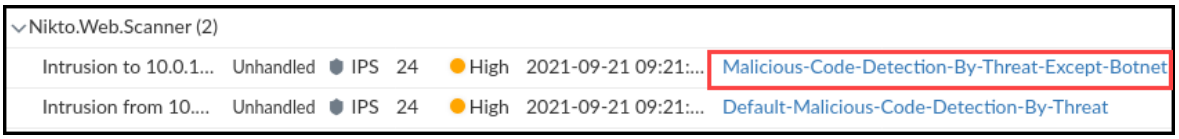
Generate Traffic to Trigger the Playbook

You will generate some traffic to trigger the execution of the imported playbook.

To generate traffic and watch for the new events

1. Open the PuTTY application, and then connect to the LINUX saved session.
2. Log in with the username `student` and password `password`.
3. Enter the following command:
   ```
   nikto.pl -host 10.200.1.10
   ```
4. Leave the command running.
5. Return to **FortiSoC** > **Event Monitor** > **All Events**.
6. Filter the view to the **Last 30 Minutes**, and then change the refresh rate to 10 seconds.

7. Verify that new events are appearing—pay close attention to the **Event** column, and look for a `Nikto.Web.Scanner` entry.
8. Once you see that entry, expand it, and then wait until at least one of the events listed is generated by the custom handler (**Malicious-Code-Detection-By-Threat-Except-Botnet**) you created.



9. Return to the PuTTY session, and then press `Ctrl+Z` to stop the script.

Verify the Successful Execution of the Playbook

After a few seconds, the traffic generated in the previous step should trigger the playbook. You will verify the execution of the playbook.

To verify the playbook execution

1. Return to the **Playbook Monitor**, and then verify the playbook was executed successfully.

This indicates that the three tasks were completed correctly.

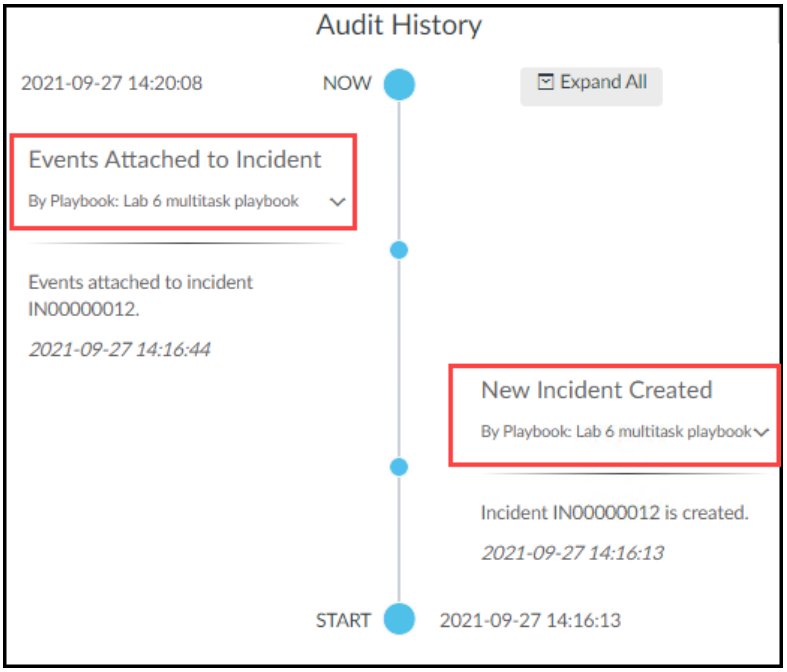
If at least one task fails, the playbook is considered to have failed its execution. You can check which task fails by clicking **Details**.

2. Click **Incidents** to verify a new incident was created.
3. Double-click the new incident to open its analysis page.
4. Examine the **Audit History** pane.

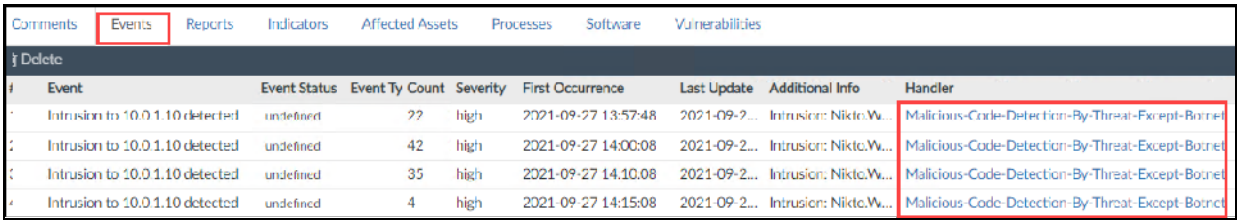
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

It should look similar to the following image:



5. Continuing on the **Analysis** page, examine the **Events** tab.
   All events included should be the ones generated by the handler you specified before.



6. Log out of FortiAnalyzer.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 4: Using FortiOS Connectors

In this exercise, you will examine the process of creating an on-demand playbook that uses a FortiOS (FOS) connector.

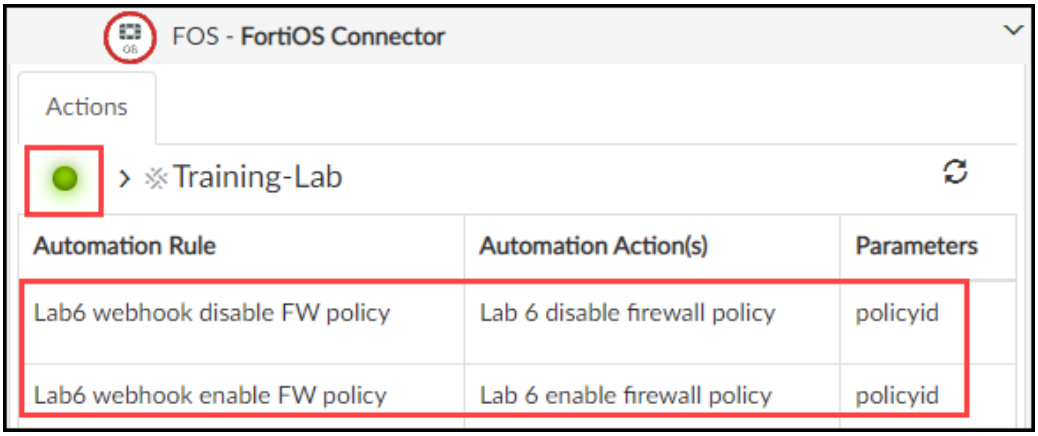
When executed, the playbook instructs a FortiGate to run a simple script.

Examine Existing FortiOS Connectors

Before you start this exercise, you must verify that the FortiOS connectors are ready to be used by FortiAnalyzer.

To examine the FortiOS connectors available

1. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. Click **NEW**.
3. Click **FortiSoC**.
4. Click **Automation** > **Connectors**.
5. Verify the indicator for the FOS connector is green and shows two automation rules.



The automation rules displayed above were preconfigured for you on the FortiGate side.

Each rule consists of a CLI script that will be executed when FortiGate receives a webhook call from FortiAnalyzer. The call is made during the execution of a playbook.

One script disables a firewall policy, and the other script enables it. The affected policy is determined by the **policyid** parameter.

Add a Playbook Task That Disables a Firewall Policy

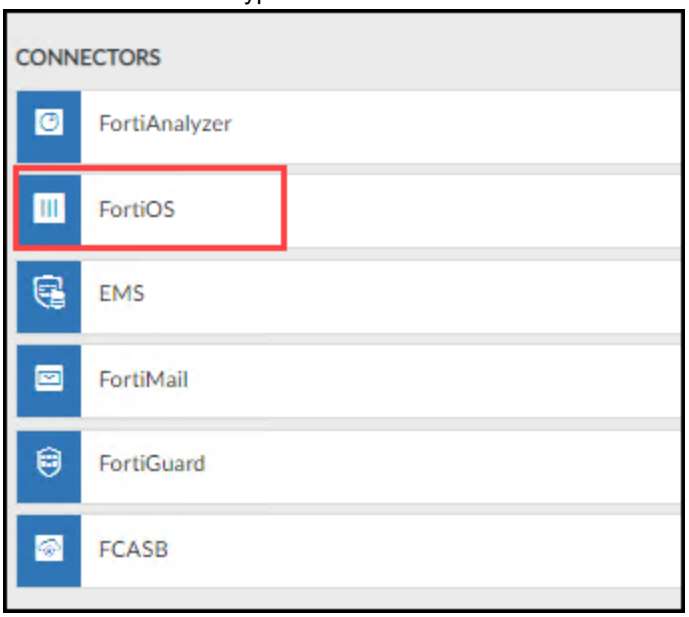
You will edit one of the existing playbooks to include a task that disables a firewall policy when executed.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

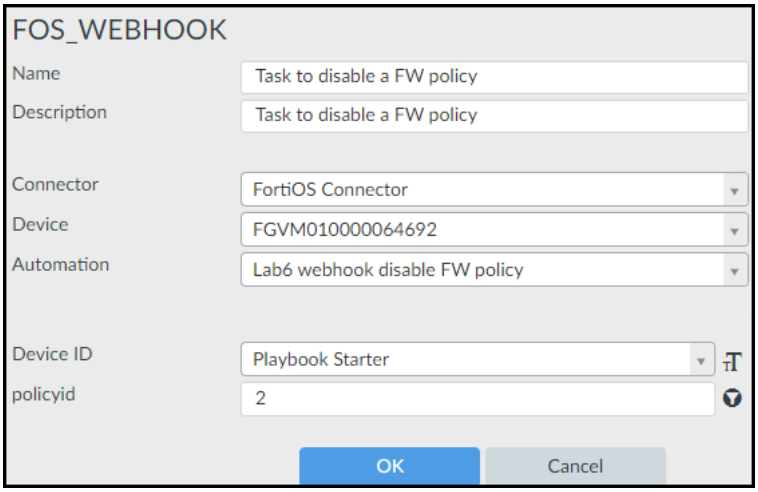
DO NOT REPRINT
© FORTINET
Brave-Dumps.com

To add a new task to an existing playbook

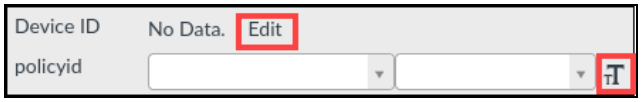
1. Click **Automation** > **Playbook**.
2. Double-click the playbook named **Lab 6 multitask playbook** to edit its settings.
3. Drag one of the connectors in the trigger to an empty area in the playbook editor.
4. Select the connector type labeled **FortiOS** for the new task.



5. Edit the new task as shown in the following image:



You must click **Edit** to configure the **Device ID** parameter, and then click the convert to text button to configure the **policyid**.

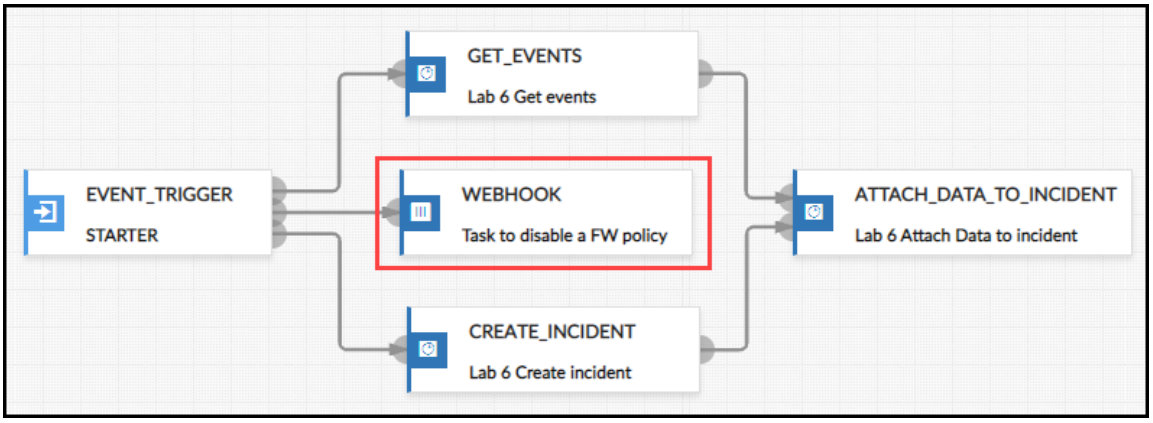


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

The device listed in this task is Local-FortiGate, and **2** is the `policyid` of the **IPS-traffic-policy** firewall policy on that device.

6. Click **OK**.
7. The playbook should now look similar to the following image:



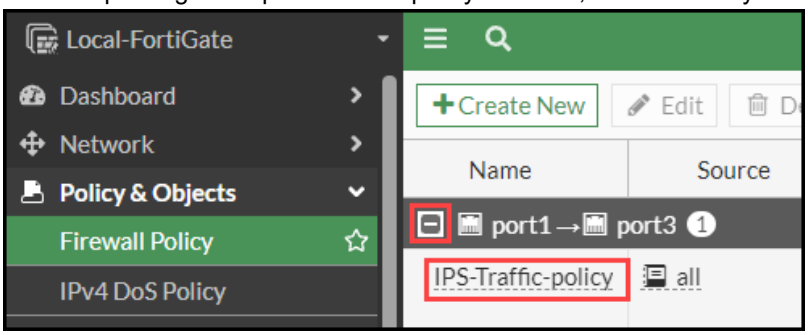
8. Click **Save Playbook**, and then return to **Automation** > **Playbook**.

Verify the FortiGate Configuration Before Running the Playbook

Before proceeding to the next step, you must verify the configuration of the FortiGate that will be modified by the playbook.

To verify the current FortiGate configuration

1. On the Local-Client VM, open a browser, and then log in to the Local-FortiGate GUI at `10.0.1.254` with the username `admin` and password `password`.
2. In the left panel, click **Policy & Objects**, and then click **Firewall Policy**.
3. Click the plus sign to expand the first policy in the list, and then verify it is enabled.



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Generate Traffic to Trigger the Playbook

As in previous exercises, you will generate some traffic to trigger the playbook.

To generate traffic that will trigger the playbook

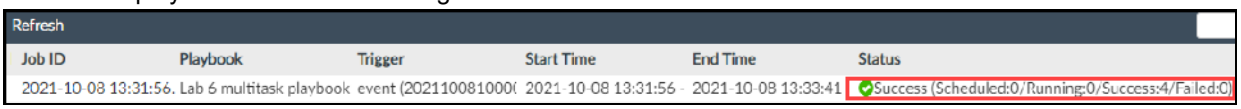
1. On the Local-Client VM, open the PuTTY application, and then connect to the LINUX saved session.
2. Log in with the username `student` and password `password`.
3. Enter the following command:
   ```
   nikto.pl -host 10.200.1.10
   ```
4. Leave the command running.

Verify the Effect of Running the Playbook

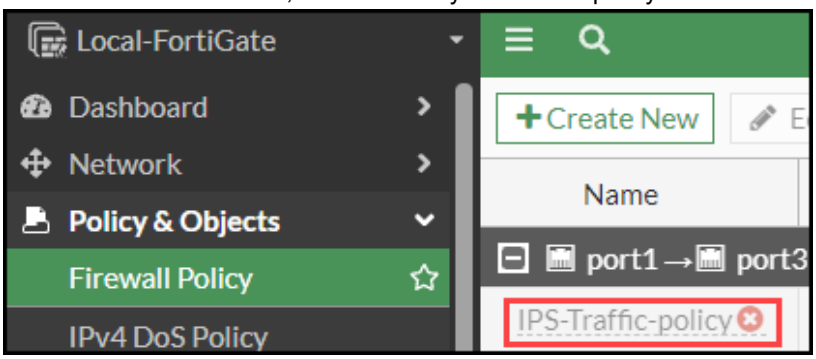
After the successful execution of the playbook, the firewall policy you examined before should now be disabled. You will verify that the firewall policy is disabled.

To verify that the playbook execution disabled the firewall policy

1. On FortiAnalyzer, click **Automation** > **Playbook Monitor**.
2. Wait for the playbook to run until it changes its status to **Success**.



3. Return to Local-FortiGate, and then verify the firewall policy is disabled.



Stop and think!

You successfully configured FortiAnalyzer to instruct a FortiGate to change its configuration based on a detected event.

Although this is a very simple example, it should give you a good idea of how powerful it can be to use playbooks to automate tasks.

4. Return to the PuTTY session, and then press `Ctrl+Z` to stop the script.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

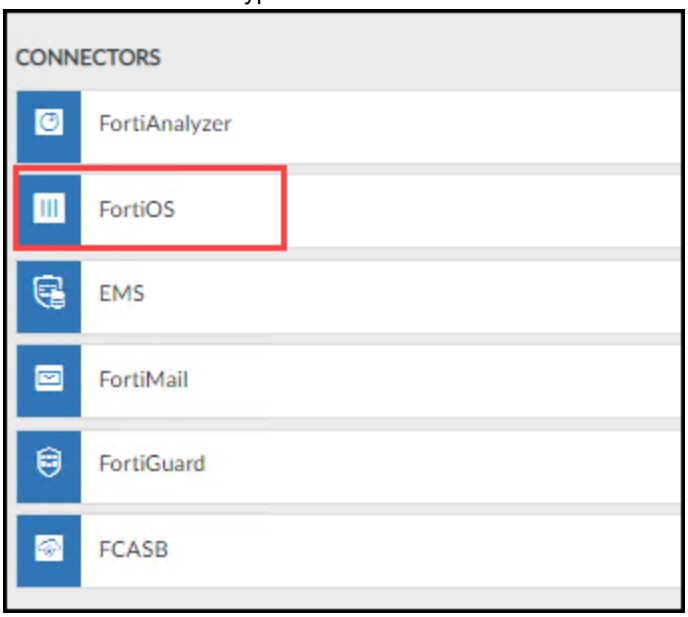
DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Create a Playbook to Enable a Firewall Policy

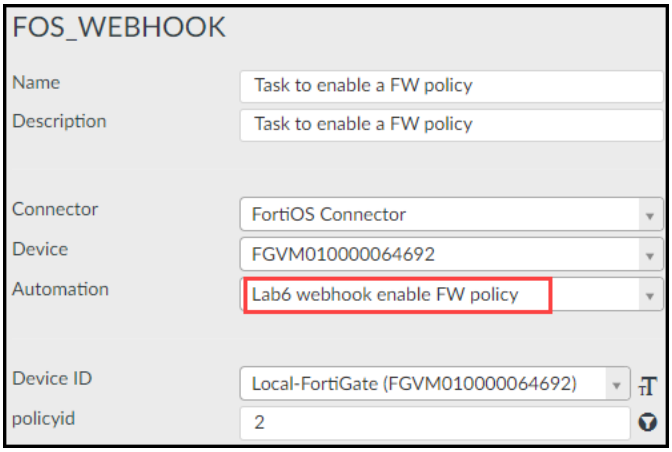
To enable the firewall policy again, you will create a new playbook to be executed on demand.

To create a playbook that enables a firewall policy

1. On FortiAnalyzer, click **Automation** > **Playbook**.
2. Click **Create New**, and then select **New Playbook created from scratch**.
3. Select **On_Demand** to choose that trigger type.
4. Drag one of the connectors to an empty area in the playbook editor.
5. Select the connector type labeled **FortiOS** for the new task.



6. Configure the task settings exactly as shown in the following image:

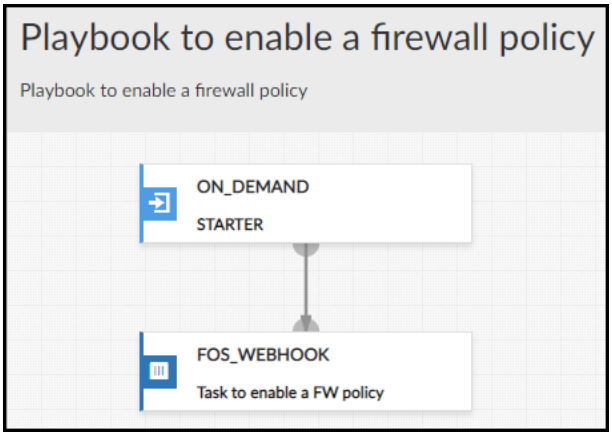


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

When executed, this task enables the same policy that was disabled in the previous section.

7. Click **OK**.
8. Change the name and description of the playbook as shown in the following image:



9. Click **Save Playbook**.

Do not run the playbook immediately.

Remember, it takes about five minutes for FortiAnalyzer to finish parsing a new playbook.

10. Run the playbook.
11. Click **Automation** > **Playbook Monitor**.
12. Wait for the playbook to run until it changes its status to **Success**.
13. Return to Local-FortiGate, and then verify the firewall policy is now enabled.
14. Log out of Local-FortiGate.
15. Log out of FortiAnalyzer.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

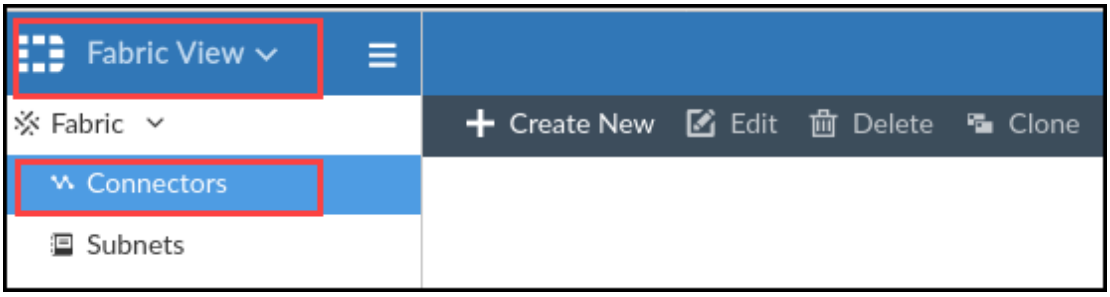
Exercise 5: Exporting and Importing Playbooks

In this exercise, you will examine how to export a playbook, and then import it on a different ADOM. You will also explore the effect of including connectors during the export and import process.

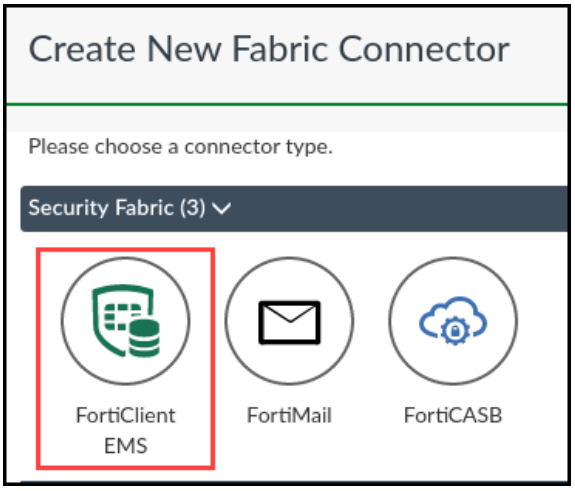
Add a Connector in Fabric View

To add a FortiClient EMS connector

1. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. Click **NEW**.
3. Click **Fabric View**.
4. Click **Fabric** > **Connectors**.
5. Verify there are no connectors present.



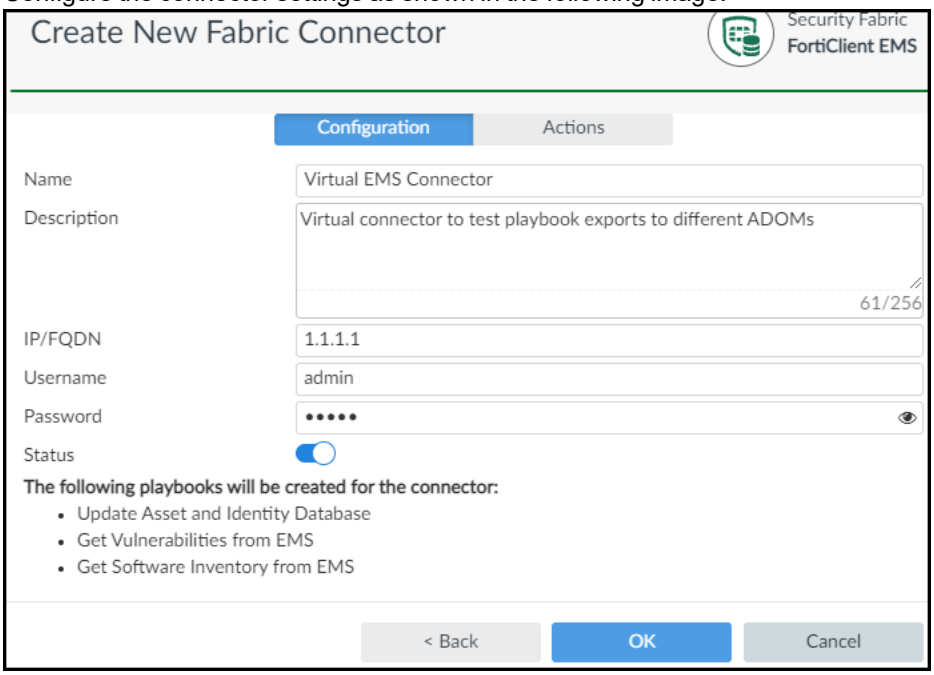
6. Click **Create New**, and then select **FortiClient EMS**.



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

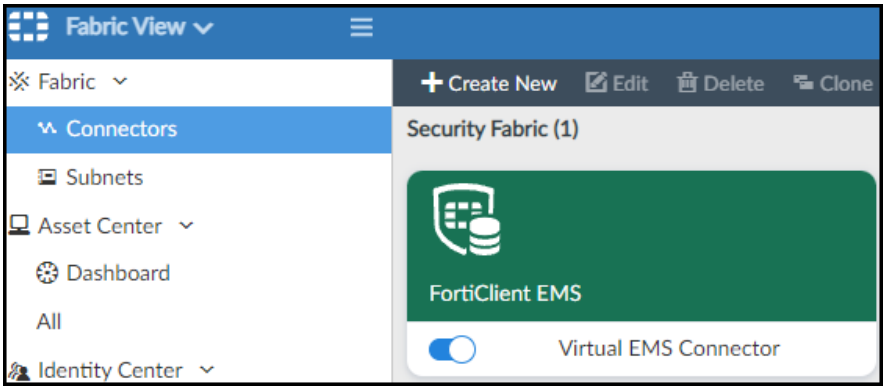
DO NOT REPRINT
© FORTINET
Brave-Dumps.com

7. Configure the connector settings as shown in the following image:



This is only a virtual connector that you will use to examine the export and import process later in this exercise. It does not add any real functionality to the lab environment, therefore the values you use in the IP, username, and password fields are not important.

8. Click **OK** to save the changes.
9. Verify the new connector is added and enabled.



Create a Playbook With the FortiClient EMS Connector

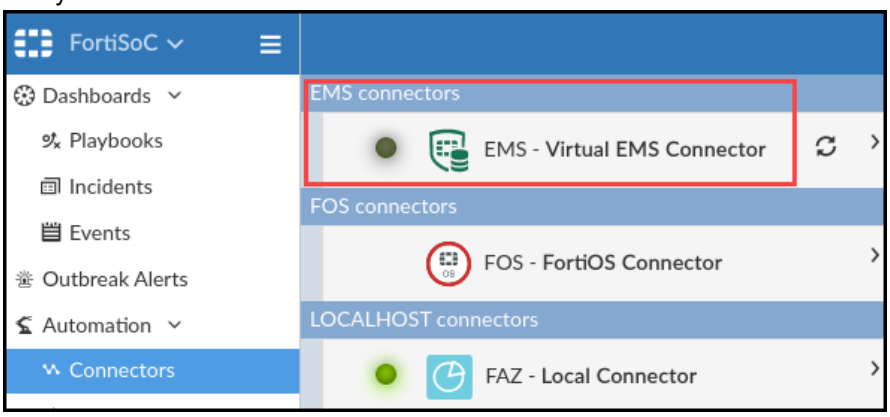
Now that you created the FortiClient EMS connector, you will use it in a playbook.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

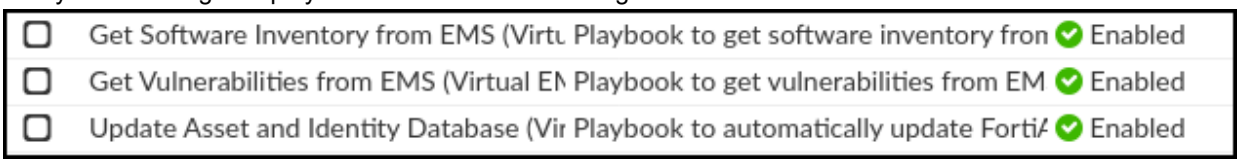
DO NOT REPRINT
© FORTINET
Brave-Dumps.com

To create a playbook with the new connector

1. Return to **FortiSoC** > **Automation** > **Connectors**.
2. Verify the new EMS connector is listed.



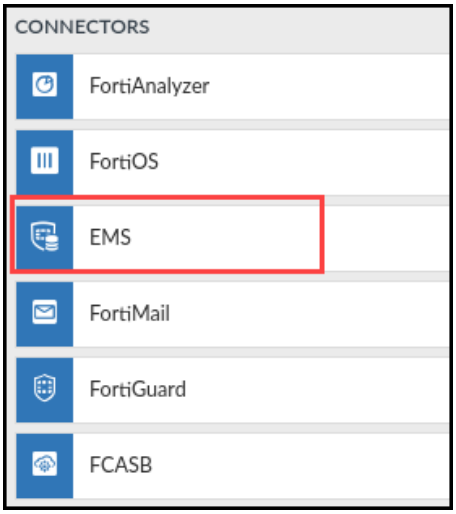
3. Click **Automation** > **Playbook**.
4. Verify the following new playbooks are listed after adding the virtual EMS connector:



The playbooks added with the EMS connector use on-schedule triggers, and are set to run daily.

In this lab environment, the execution of these playbooks will fail because the connector is configured to use a server that doesn't exist.

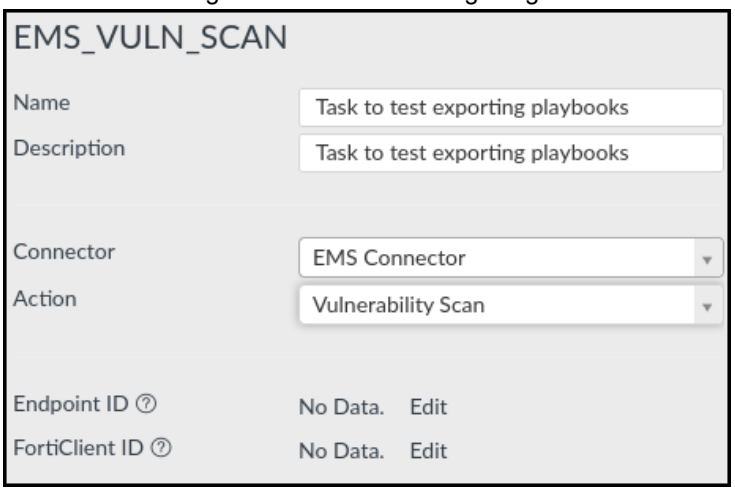
5. Click **Create New**, and then select **New Playbook created from scratch**.
6. Select **On_Demand** to choose that trigger type.
7. Drag one of the connectors to an empty area in the playbook editor.
8. Select the connector type labeled **EMS** for the new task.



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

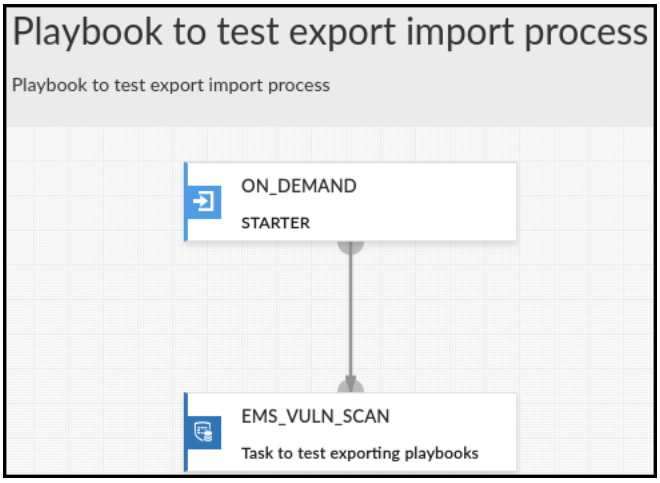
9. Edit the task settings to match the following image:



This connector is not functional and you will not be running this playbook.

We are using it only to demonstrate the export and import processes including connectors.

10. Click **OK** to save the changes.
11. Change the name and description of the playbook as shown in the following image:



12. Click **Save Playbook**.

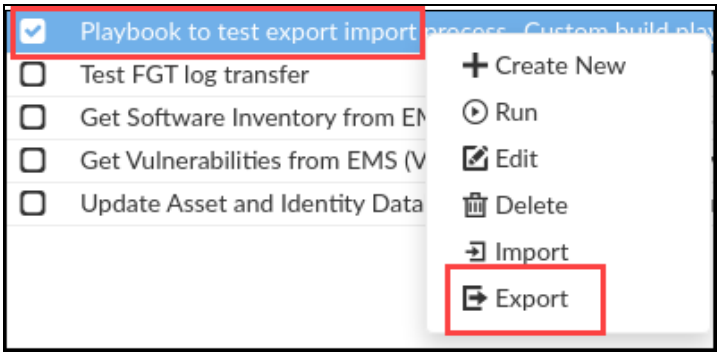
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

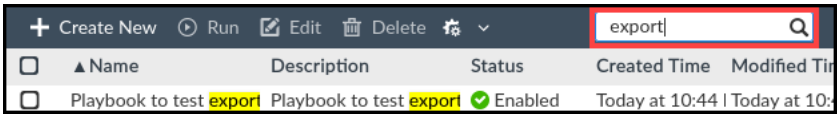
Export a Playbook

To export the playbook

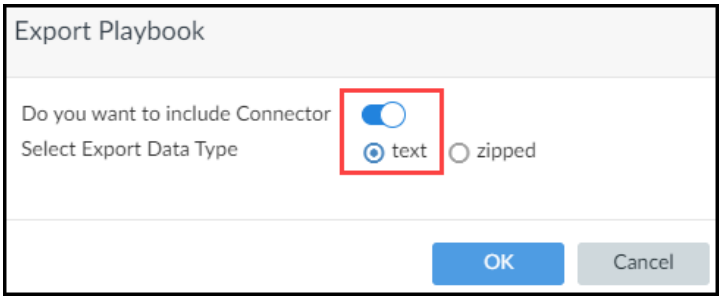
1. Return to **Automation** > **Playbook**.
2. Right-click the new playbook, and then select **Export**.



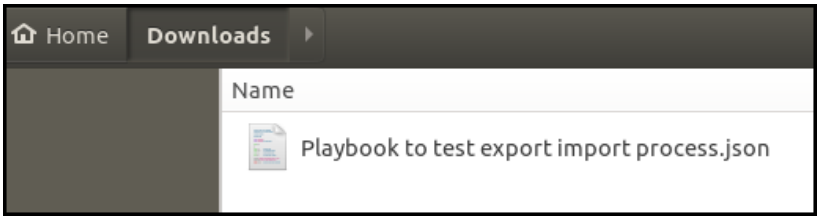
You can use the search bar to locate a playbook.



3. Click to enable the option labeled **Do you want to include Connector**, and then in the **Select Export Data Type** field, select **text** to export the playbook as plaintext.



4. Click **OK**
5. Select **Save File**, and then click **OK**.
6. Verify the exported file is in the **Downloads** folder.



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

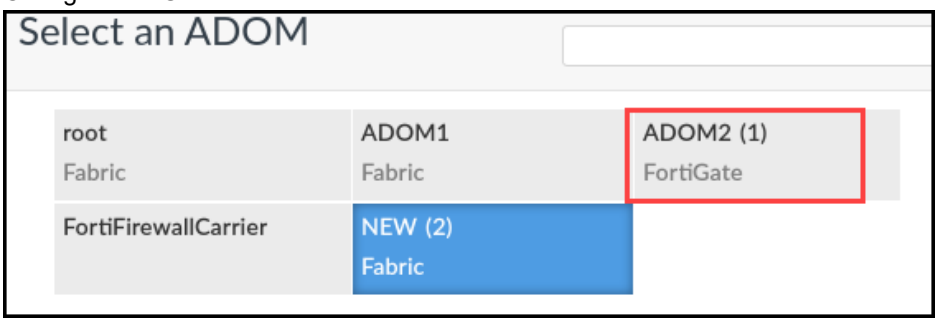
DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Import a Playbook

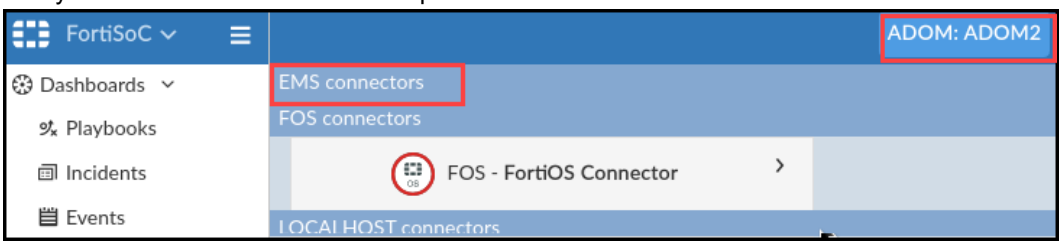
After you export a playbook, you can import it to another ADOM or FortiAnalyzer.

To import the playbook in a different ADOM

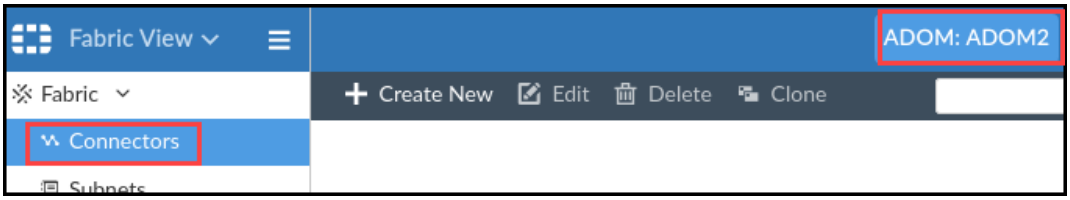
1. Change to **ADOM2**.



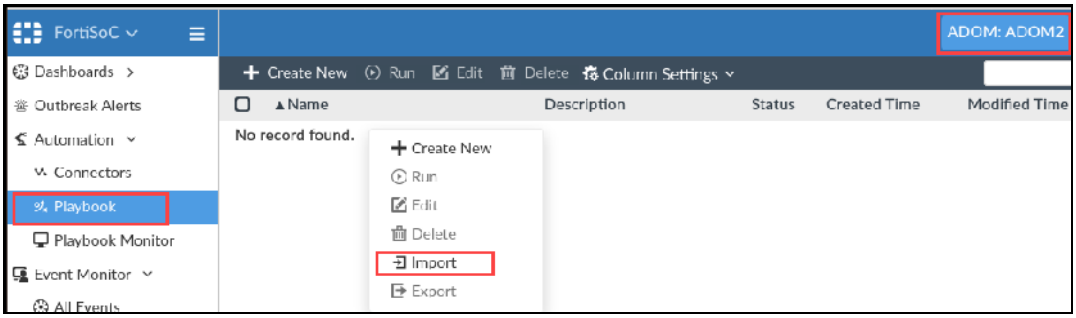
2. Verify that there is no EMS connector present in **FortiSoC** > **Automation** > **Connectors**.



3. Verify that there is no connector present in **Fabric View**.



4. Return to **FortiSoC** > **Automation** > **Playbook**.
5. Right-click anywhere on the empty pane, and then select **Import**.

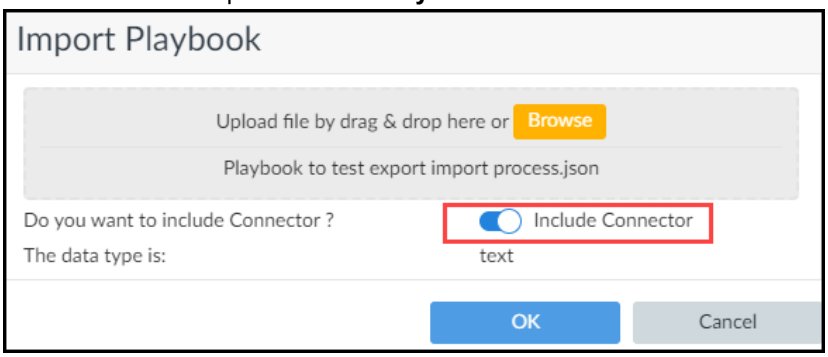


6. Click **Browse**, and then go to the **Downloads** folder.
7. Select the exported file, and then click **Open**.

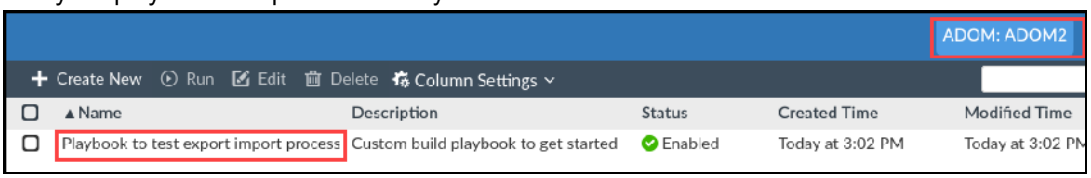
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

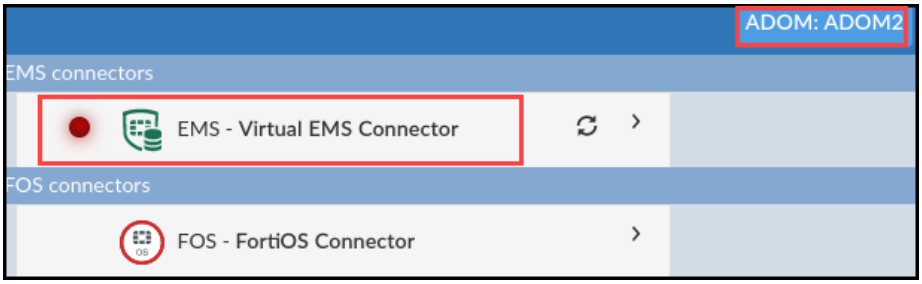
8. Click to enable the option labeled **Do you want to include Connector**.



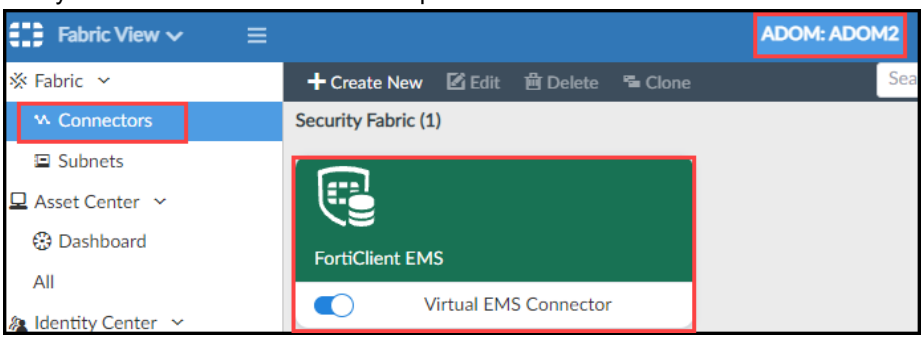
9. Click **OK**.
10. Verify the playbook is imported correctly.



11. Verify that there is an EMS connector present in **FortiSoC**.



12. Verify that there is an EMS connector present in **Fabric View**.



Stop and think!

Including the connectors when exporting and importing allows you to transfer fully functional playbooks to different ADOMs, or even different devices, as long as the connector settings are still valid on their destination.

You can choose to not include the connectors, but then you must manually configure most of the tasks settings.

13. Log out of FortiAnalyzer.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Lab 7: Reports

In this lab, you will examine the reporting capabilities included in FortiAnalyzer. You will generate a default report, build a chart based on a log search, and perform some diagnostic checks.

Objectives

- Generate one of the predefined reports
- Clone and customize a predefined report
- Build a custom dataset
- Build a custom chart based on a log search
- Create a schedule for a report
- Configure an output profile to include a report in an email

Time to Complete

Estimated: 45 minutes

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 1: Running a Default Report

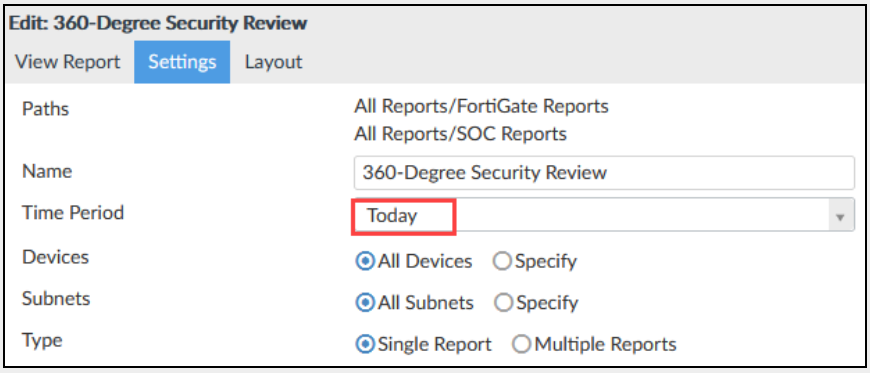
In this exercise, you will run one of the predefined reports on demand. You will also examine the effect of enabling **Auto-cache** in a report.

Generate a Default Report

FortiAnalyzer includes many predefined reports to serve a wide variety of scenarios. You will generate one of the default reports.

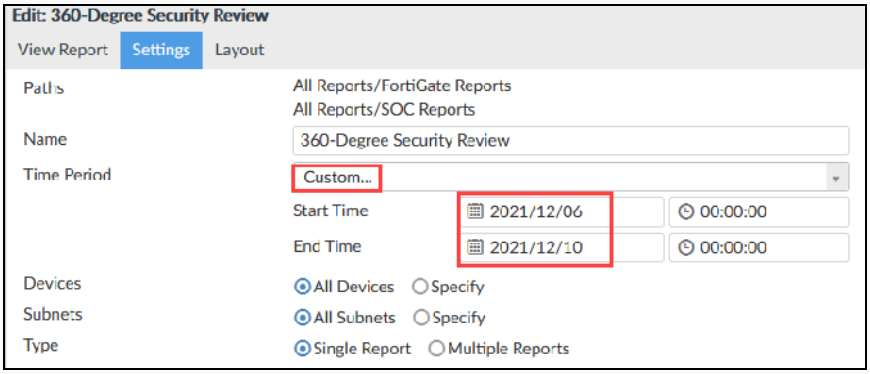
To generate a default report

1. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. Click **NEW**.
3. Click **Reports**.
4. In the left menu, select **All Reports**.
   This page provides all available default reports.
5. Double-click the report at **SOC Reports** > **360-Degree Security Review**.
6. Depending on the class format, do one of the following:

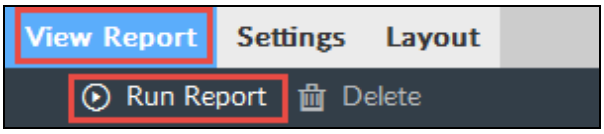
Class Format	Do This...
Instructor Led class	Click the **Settings** tab, and then in the **Time Period** drop-down list, select **Today**.  **Note**: If you didn't do the previous labs the same day you are doing this one, adjust the **Time Period** accordingly to avoid a report with little or no data.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Class Format	Do This...
Self paced class	Click the **Settings** tab, and then in the **Time Period** drop-down list, select **Custom** and specify the time range shown in the image.  **Note**: Some traffic was generated during the time range specifed to ensure that the resulting report is not empty.

7. Click **Apply**.
8. Click the **View Report** tab, and then click **Run Report** to run the report on demand.



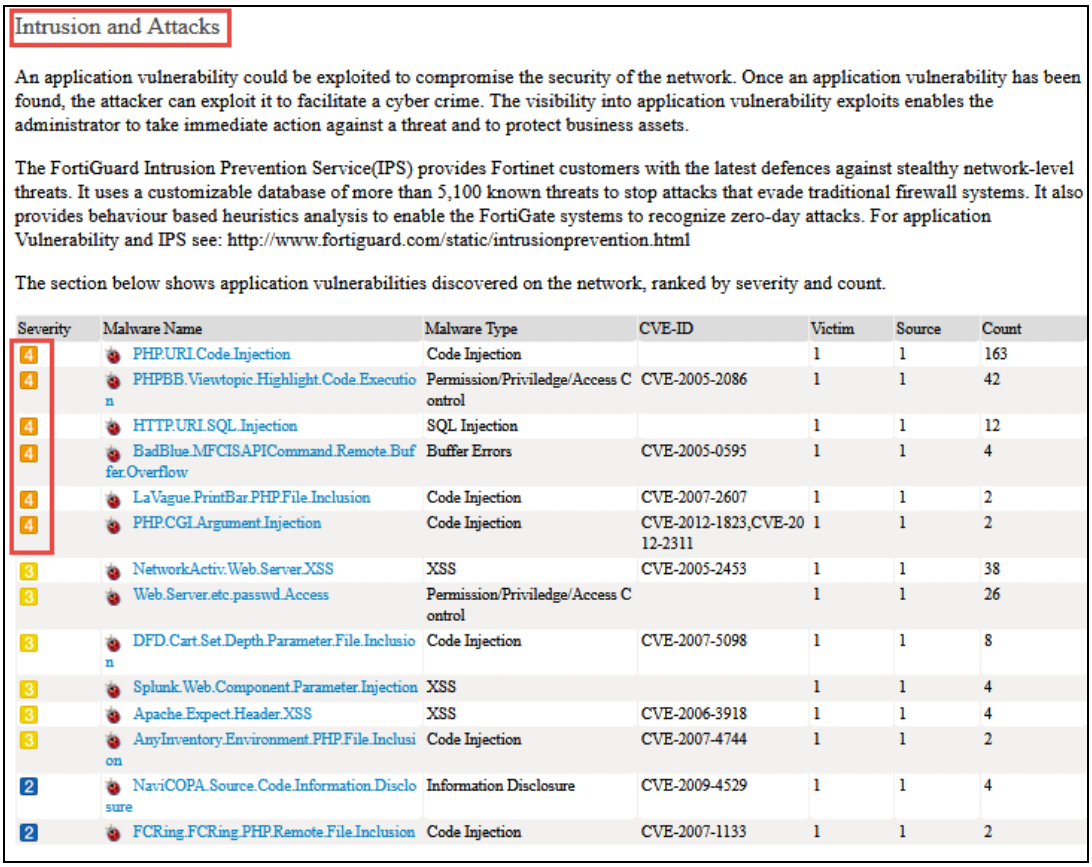
9. When the report is ready, in the **Format** column, click **HTML** to view the report in HTML format.
10. In the left menu, select **Intrusion and Attacks**.

As you can see from the report, several types of attacks are occurring in your network.

11. Look for any severity 4 attacks.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



Intrusion and Attacks

An application vulnerability could be exploited to compromise the security of the network. Once an application vulnerability has been found, the attacker can exploit it to facilitate a cyber crime. The visibility into application vulnerability exploits enables the administrator to take immediate action against a threat and to protect business assets.

The FortiGuard Intrusion Prevention Service(IPS) provides Fortinet customers with the latest defences against stealthy network-level threats. It uses a customizable database of more than 5,100 known threats to stop attacks that evade traditional firewall systems. It also provides behaviour based heuristics analysis to enable the FortiGate systems to recognize zero-day attacks. For application Vulnerability and IPS see: http://www.fortiguard.com/static/intrusionprevention.html

The section below shows application vulnerabilities discovered on the network, ranked by severity and count.

Severity	Malware Name	Malware Type	CVE-ID	Victim	Source	Count
4	PHP.URI.Code.Injection	Code Injection		1	1	163
4	PHPBB.Viewtopic.Highlight.Code.Execution	Permission/Priviledge/Access Control	CVE-2005-2086	1	1	42
4	HTTP.URI.SQL.Injection	SQL Injection		1	1	12
4	BadBlue.MFCISAPICommand.Remote.Buffer.Overflow	Buffer Errors	CVE-2005-0595	1	1	4
4	LaVague.PrintBar.PHP.File.Inclusion	Code Injection	CVE-2007-2607	1	1	2
4	PHP.CGI.Argument.Injection	Code Injection	CVE-2012-1823,CVE-2012-2311	1	1	2
3	NetworkActiv.Web.Server.XSS	XSS	CVE-2005-2453	1	1	38
3	Web.Server.etc.passwd.Access	Permission/Priviledge/Access Control		1	1	26
3	DFD.Cart.Set.Depth.Parameter.File.Inclusion	Code Injection	CVE-2007-5098	1	1	8
3	Splunk.Web.Component.Parameter.Injection	XSS		1	1	4
3	Apache.Expect.Header.XSS	XSS	CVE-2006-3918	1	1	4
3	AnyInventory.Environment.PHP.File.Inclusion	Code Injection	CVE-2007-4744	1	1	2
2	NaviCOPA.Source.Code.Information.Disclosure	Information Disclosure	CVE-2009-4529	1	1	4
2	FCRing.FCRing.PHP.Remote.File.Inclusion	Code Injection	CVE-2007-1133	1	1	2

12. Click the malware name associated with one of the severity 4 entries.
    This takes you to the FortiGuard website, where you can view more information about the attack.

Run Diagnostics on a Report

FortiAnalyzer creates a diagnostic log for each report that generates. You can examine this log, for example, to troubleshoot a report that is very slow to generate.

To run diagnostics on a report

1. Return to the FortiAnalyzer GUI, right-click the report you just ran, and then select **Retrieve Diagnostic**.
2. Save the file.
3. Open the `rpt_status.log` file that was saved to your **Downloads** folder.
4. Scroll down to the `Report Summary` section at the bottom of the file, and then record the following:

HCACHE building time
Rendering time
Total time

For example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com


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

5. Return to the FortiAnalyzer GUI, click the **Settings** tab for the report, and then enable **Enable Auto-cache**.
   The hcache is updated when new logs come in, and new log tables are generated. If you do not enable auto-cache, the report generates only the hcache for the current log tables.
6. Click **Apply**.
7. Run the report one more time, and then run the diagnostics again. What is the output this time?

HCACHE building time
Rendering time
Total time

For example:

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

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

8. Log out of FortiAnalyzer.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

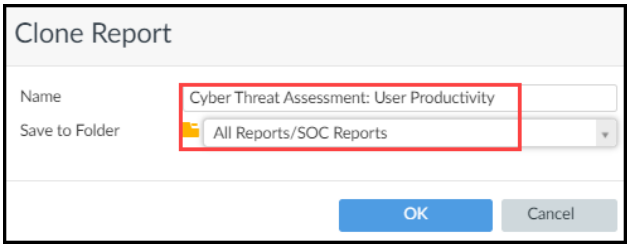
DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 2: Cloning and Customizing a Default Report

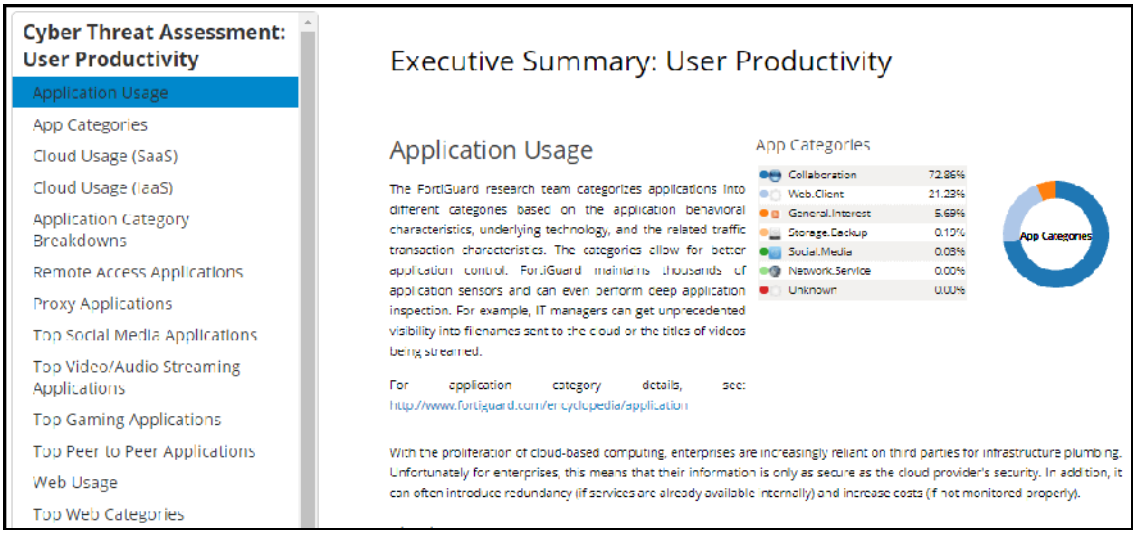
In this exercise, you will clone one of the predefined reports, and then you will customize the report settings.

To clone and customize a default report

1. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. Click **NEW**.
3. Click **Reports**.
4. In the left menu, select **All Reports**.
5. Right-click the report **SOC Reports** > **Cyber Threat Assessment**, and then select **Clone**.
   This is a very comprehensive, high-level report that can be useful for executive summaries.
6. Name the cloned report `Cyber Threat Assessment: User Productivity`, and then save it in the **SOC Reports** folder.



7. Click **OK**.
8. Click the **Layout** tab, and then examine the different sections included.
   This pane is a WYSIWYG (what you see is what you get) editor.
9. Change the top header to **Executive Summary: User Productivity**.
10. Remove all sections except the **User Productivity** one located near the bottom.
11. Click **Apply** to save the changes.
12. Click the **View Report** tab, and then click **Run Report** to run the report on demand.
13. View the report in **HTML** format—it should look similar to the following image:



14. Log out of FortiAnalyzer.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 3: Building a Custom Dataset From Scratch

In this exercise, you will build a custom dataset that will query the database for traffic destined to websites in the `Gambling` category.

Create a Dataset

Datasets are the component that queries the database for specific logs. Although FortiAnalyzer comes with many predefined datasets, in some scenarios you may need to create custom ones.

To create a dataset from scratch

1. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. Click **NEW**.
3. Click **Reports**.
4. Navigate to **Report Definitions** > **Datasets**.
5. Click **Create New**.
6. Configure each setting as shown in the following image:

Hovering your mouse over the underlined **from $log** section, displays all the fields available for you to use in queries.

7. Click the **Test** button on the right, and then verify there are some matches under **Test Result** for this query.

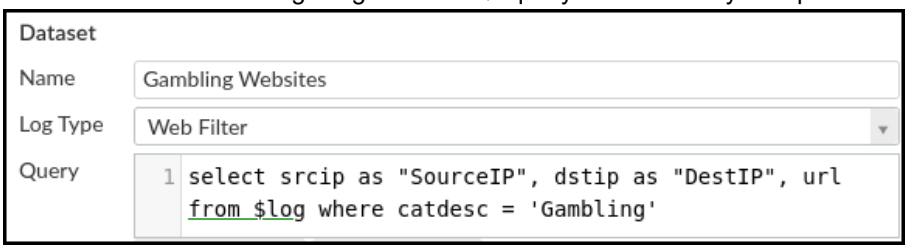
The word `Gambling` in this query is case sensitive.

Do not proceed to the next step until **Test Result** displays some matches.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

8. Add the text in the following image to the SQL query to include only the specified columns:



9. Click **Test** again, and then verify there are some matches under **Test Result**.
Your results should look similar to the following image:

Test Result

SourceIP	DestIP	url
10.0.1.200	156.245.113.108	http://bjmzw.net/
10.0.1.200	172.80.53.239	http://www.bn915.com/
10.0.1.200	3.64.163.50	http://dalotto.com/
10.0.1.200	206.119.87.32	http://www.464446.com/
10.0.1.200	212.16.185.86	http://bordella.com/
10.0.3.20	3.64.163.50	http://dalotto.com/
10.0.3.20	172.80.53.239	http://www.bn915.com/
10.0.3.20	156.245.113.108	http://bjmzw.net/

10. Click **OK** to save the custom dataset.

Stop and think!

The dataset you created queries the database for entries with the value `Gambling` in the **catdesc** column. From those results, it retrieves only the columns that contain the source IP address, destination IP address, and URL.

Creating a dataset from scratch, or customizing a predefined dataset, requires some knowledge of the syntax used for SQL queries.

11. Log out of FortiAnalyzer.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 4: Building a Custom Chart From Log View

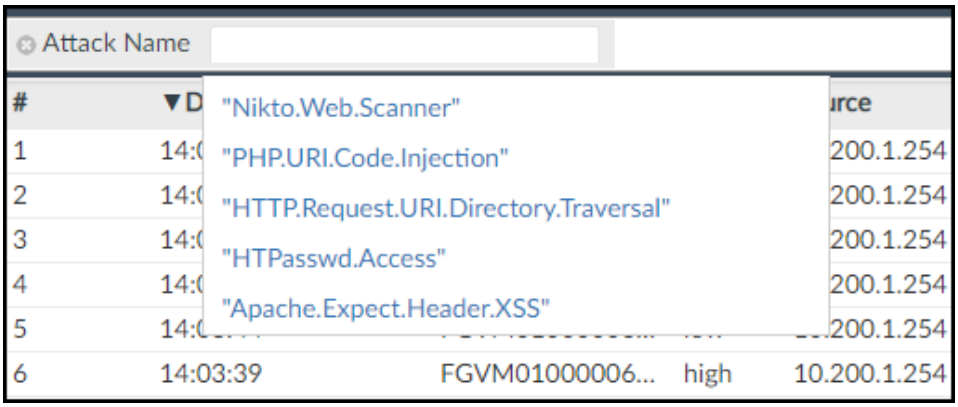
In this exercise, you will build a custom chart based on log filters. This process allows you to create a new dataset without requiring you to know the syntax used for SQL queries.

Create a Custom Chart

You can create custom charts that include only the information you need. The chart builder makes this process very easy. You will create a custom chart based on a log search.

To create a chart based on a log search

1. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. Click **NEW**.
3. Click **Log View**.
4. In the menu on the left, click **FortiGate** > **Security** > **Intrusion Prevention**.
5. Add a filter for any **Attack Name**.



You may need to adjust the time filter so it includes the traffic that you want. If you are not sure, select **Any time**.

6. Click the icon for **Custom View**.

Although a custom view isn't required to build a chart, it's a nice feature that allows you to save your filtered searches.

Custom View is available in the historical log view only.

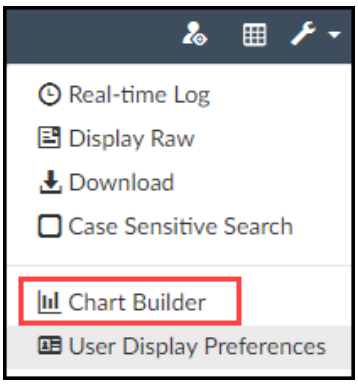
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

7. Name your custom view `Lab7_Custom_View`, and then click **OK**.
   The new custom view is added to the panel on the left.
8. Click **Lab7_Custom_View**, and then click **Column Settings** > **More Columns**.

9. In **Column Settings**, find and select the columns named **Attack Name** and **Source IP**, and then click **OK**.
10. Click the **Lab7_Custom_View** custom view, and then click **Tools** > **Chart Builder**.

Chart Builder is available in the historical log view only.



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

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

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Field	Value
Name	Lab7_Chart
Columns	Select: • Date/Time • Device ID • Severity • Source IP • Attack Name The chart builder allows you to select only five columns. Cancel the selection of any other columns, if they are selected by default. This is not a limitation when building custom datasets manually.
Order By	Date/Time
Sort By	Descending
Show Limit	500

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

Your resulting query depends on which attack you chose.

In the example above, the attack name selected was `Nikto.Web.Scanner`.

13. View the preview, and then click **Save**.
    Your dataset and chart are created, both with the same name.

Create and Run a Report Using a Custom Chart

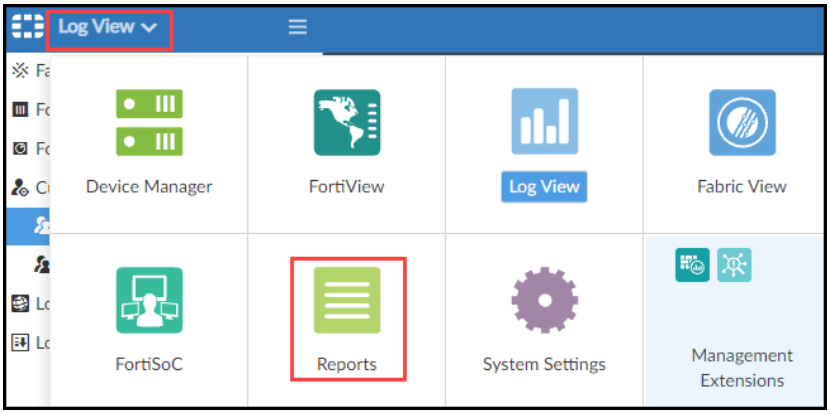
You will create a new report that uses the custom chart you built.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

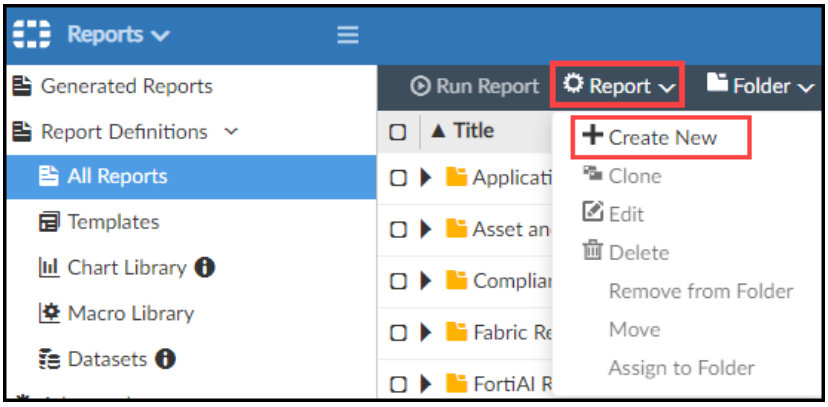
DO NOT REPRINT
© FORTINET
Brave-Dumps.com

To create a report using a custom chart

1. In the drop-down list on the left, click **Log View** > **Reports**.



2. Click **All Reports**, and then click **Report** > **Create New**.



3. Configure the following settings:

Field	Value
Name	Lab7_Report
Create from	Blank

4. Click **OK**.
   The **Settings** tab for the report appears.
5. In the **Time Period** drop-down list, select **Today**.

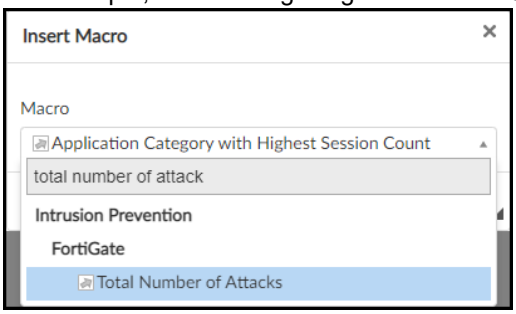
If you didn't do the previous labs the same day you are doing this one, adjust the **Time Period** accordingly to avoid a report with little or no data.

6. Click the **Layout** tab, and then click **Insert Chart**.

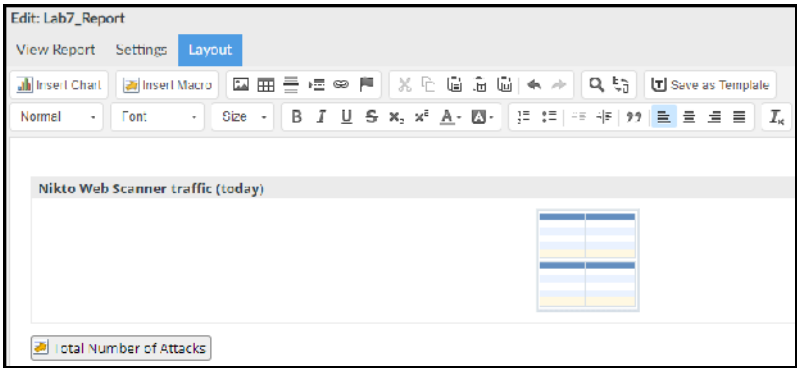
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

7. Click the **Chart** drop-down list, in the text field start typing `Lab7_Chart`, and then select it when it appears in the list.
8. In the title box, type `Nikto Web Scanner (traffic)`. Adjust the attack name to the one you used to build the chart.
9. Click **OK**.
10. Click **Apply**.
11. Optionally, complete the following steps to insert one of the IPS macros:
    a. Click to insert your cursor below the chart you just added to the layout.
    b. Click **Insert Macro**.
    c. Click the **Macro** drop-down list, scroll up to the **Intrusion Prevention** section, and then select any of the default macros.
    For example, the following image shows the **Total Number of Attacks** macro selected:



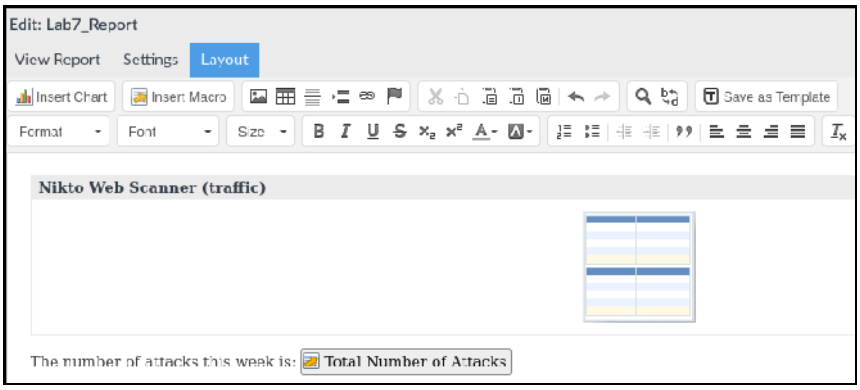
    d. Click **OK**.
    e. Click **Apply**.



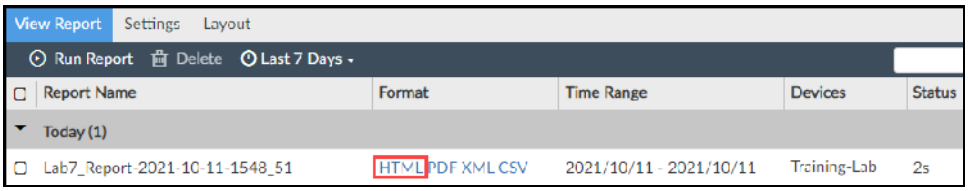
12. Add a new line of text to describe the information provided by the macro, and then drag the macro at the end of the text.
    The result should look similar to the following image:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



13. Click **Apply**.
14. Click the **View Report** tab, and then click **Run Report**.
15. In the **Format** column, click **HTML** to view the report in HTML format.



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

16. Log out of FortiAnalyzer.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 5: Scheduling a Report

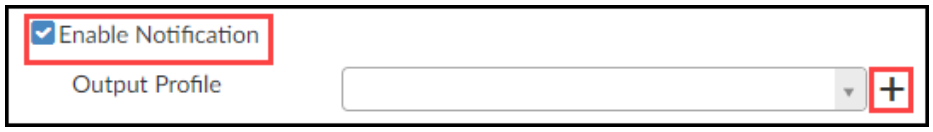
In this exercise, you will schedule a report to be generated daily, and configure it to be sent in an email using an output profile.

Create and Configure an Output Profile

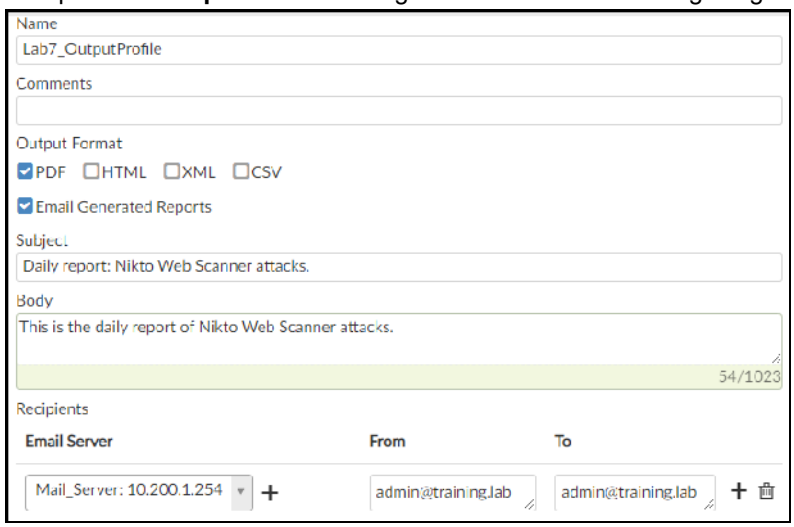
Output profiles allow you to send a copy of generated reports to other servers. You will create an output profile.

To configure an output profile

1. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. Click **NEW**.
3. Click **Reports**.
4. Find and double-click the report named **Lab7_Report**, and then click the **Settings** tab.
5. Select the **Enable Notification** checkbox, and then click the plus sign to add a new output profile.



6. Complete the **Output Profile** settings as shown in the following image:



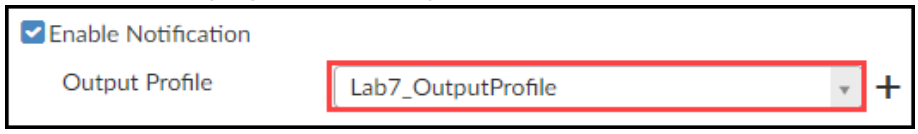
Adjust the subject to the attack name and time period you selected earlier.

Click the plus sign to add the email server.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

7. Click **OK**.
8. Select the new output profile in the drop-down list.

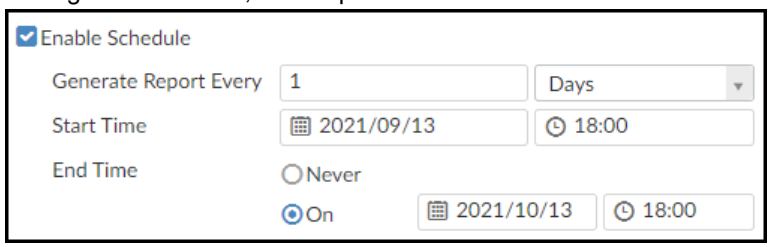


Schedule Reports

When you need to generate the same report periodically, you can enable the report schedule feature using a very intuitive interface. You will schedule a report.

To schedule a report

1. Select the **Enable Schedule** checkbox.
2. Configure the report to be generated every day, starting today, and to end one month after today. Adjust the start time so the first occurrence is five minutes from the current time.
   For example, the following image shows a schedule that will run daily, starting on September 13, at 6:00 pm, and ending on October 13, at 6:00 pm.



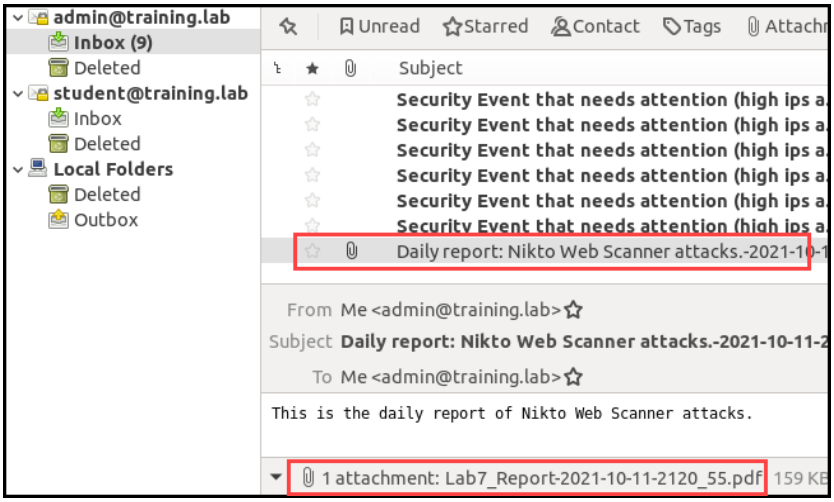
3. Click **Apply** to save the changes.
4. In the menu on the left, click **Report Calendar**, and then verify the report is added and is **Pending** to run today.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

To verify an email was received with the report

1. Wait five minutes.
2. On Local-Client, open the Thunderbird email client, and then verify an email was received with the daily report attached.



In this exercise, you used the option to send a report as an email attachment. However, if they are available, you can also upload a report to an FTP, SFTP, or SCP server.

This is done by selecting and configuring the **Upload Report to Server** option in the output profile.

Congratulations! You successfully completed the FortiAnalyzer labs.

You can now close your browser.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© 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© 2022 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.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com