FortiNAC

Lab Guide

for FortiNAC 7.2

FORTINET
Training Institute

Fortinet Training Institute - Library

https://training.fortinet.com

Fortinet Product Documentation

https://docs.fortinet.com

Fortinet Knowledge Base

https://kb.fortinet.com

Fortinet Fuse User Community

https://fusecommunity.fortinet.com/home

Fortinet Forums

https://forum.fortinet.com

Fortinet Product Support

https://support.fortinet.com

FortiGuard Labs

https://www.fortiguard.com

Fortinet Training Program Information

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

Fortinet | Pearson VUE

https://home.pearsonvue.com/fortinet

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

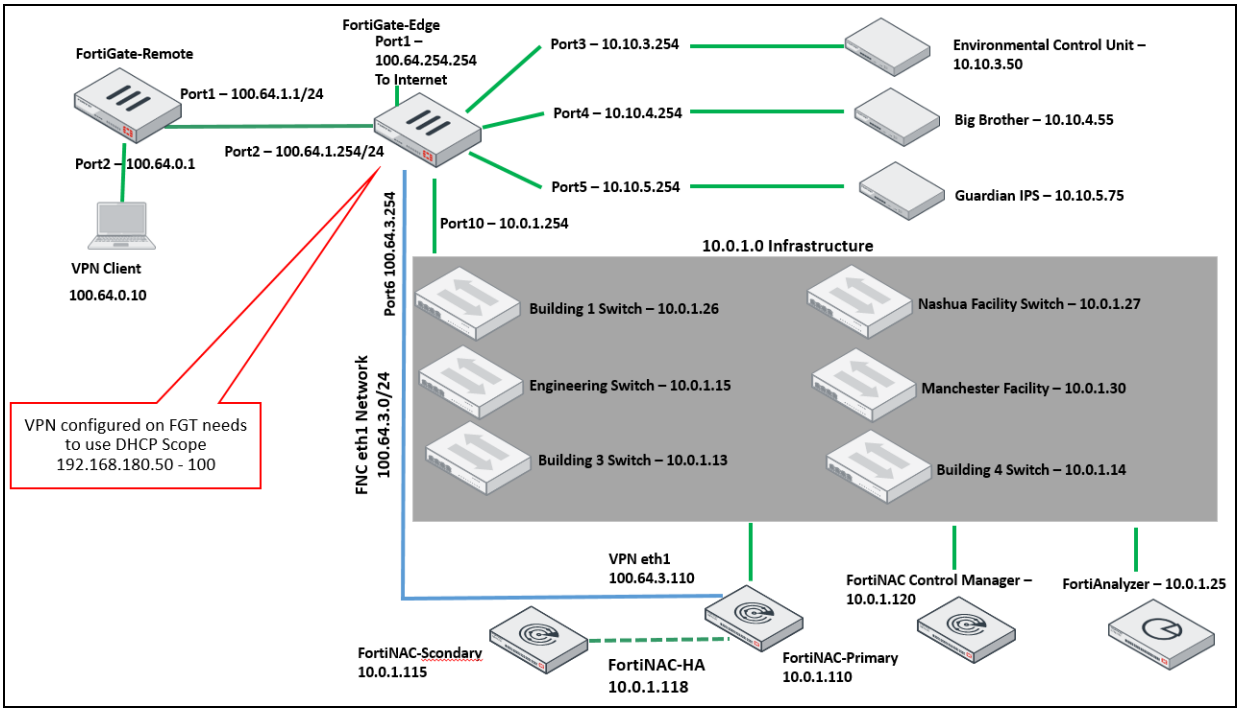
https://helpdesk.training.fortinet.com/support/home

FORTINET

3/10/2023

TABLE OF CONTENTS

Network Topology



Lab 1: Initial FortiNAC Configuration

In this lab, you will examine some initial device configurations necessary to prepare FortiNAC for deployment. Next, you will create an administrative user for FortiNAC management.

Objectives

- Access the FortiNAC configuration wizard and examine the configuration views
- Create an administrative user account

Time to Complete

Estimated: 20 minutes

Exercise 1: Examining the Initial Configuration

In this exercise, you will access the FortiNAC configuration wizard and examine the configuration options. First, you will examine the basic network settings that configure the FortiNAC administrative interface (eth0). Next, you will examine the captive network settings that will be applied to the captive interface (eth1) for each of the different contexts (registration, remediation, and so on).

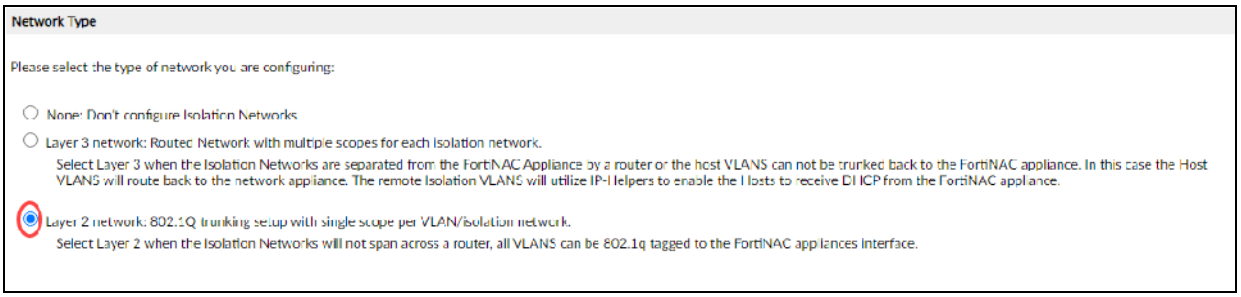
Examine the Initial Configuration Views

The FortiNAC configuration wizard is what you use to perform initial device configuration and configure isolation network type designations and settings. You will examine the initial configuration views.

To examine the initial configuration views

1. Log in to the jump box, and then open Firefox.
2. Select the **FortiNAC-Secondary** bookmark.
3. Log in to the FortiNAC-Secondary GUI with the username `admin` and password `password`.
4. Click **System** > **Config Wizard**.
5. In the **Basic Network** step, examine the settings for the **Host Name**, **eth0 IP Address**, **Mask in dotted decimal**, and **Default Gateway**, as well as the other configuration options.

   These fields have been preconfigured for this lab.
6. In the **Network Type** section, select **Layer 2 network**, and then click **Next**.



7. In the **Layer 2 Isolation** step, examine the settings.

   This is where you configure the eth1 VLAN subinterface settings for the isolation captive network.

Each Layer 2 captive network (registration, remediation, and so on) must have an IP address, mask, gateway, VLAN ID, lease pool, domain, and lease time defined. Lease pool and interface IP addresses are on the same subnet.

8. Continue to click **Next** and examine the settings for each of the wizard steps until you get to the **Layer 2 Virtual Private Network** step.
9. In the **Mask in dotted decimal** field, type `255.255.255.0`.
10. In the **VLAN ID** field, type `250`.

You will not save the changes, but the last two settings are required to continue in the wizard.

11. Continue to click **Next** and examine the settings for each of the wizard steps until you get to the **Layer 2 Access Point Management** step.

Each window except **Layer 2 Access Point Management** looks the same. Because it functions a little differently, access point management requires two lease pools.

12. Click the **Basic Network** step to return to that step.
13. In the **Network Type** section, select **Layer 3 network**, and then click **Next**.
14. In the **Layer 3 Isolation** step, examine the available options.
    This is where you will configure eth1 interface settings for the isolation captive network.
15. In the **Isolation Scopes** section, click **Add**.
    The **Add/Modify Scope** window opens. This is where you define DHCP scopes for hosts in the captive networks.
16. Click **Cancel** to close the **Add/Modify Scope** window.

Layer 3 captive networks may require more than one lease pool because FortiNAC may manage captive hosts from different captive networks.

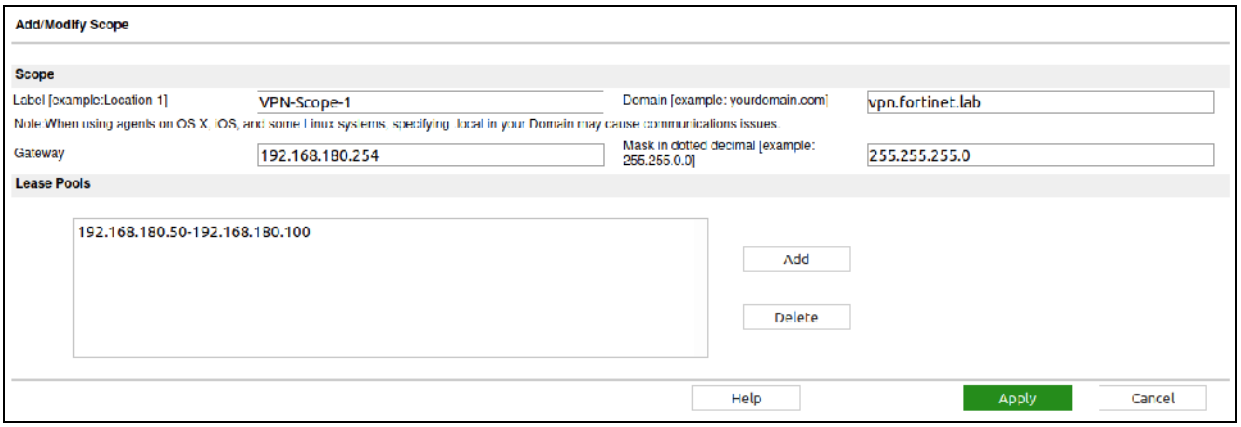
17. Continue to click **Next** and examine the settings for each of the wizard steps until you get to the **Layer 3 Virtual Private Network** step.
18. In the **Layer 3 Virtual Private Network** step, in the **Virtual Private Network Scopes** section, click **Add**, and then configure the following settings:

Field	Value
Label	VPN-Scope-1
Gateway	192.168.180.254
Mask in dotted decimal	255.255.255.0

19. In the **Lease Pools** section, click **Add**.
20. In the **Add IP Range** window, configure the following settings, and then click **Add**:

Field	Value
Start	192.168.180.50
End	192.168.180.100

21. Click **Apply**.



22. Continue to click **Next** until you get to the **Additional Routes** step.

    FortiNAC requires entries for additional routes so that it can communicate with captive networks that it is not directly connected to, using the appropriate interface (eth1).

23. Click **Next**.
24. Review the information in the **Summary** step.

    All configurations you made in the configuration wizard appear here for you to review before you apply them.

25. Click **Apply**, and then click **OK** to confirm.

    The process of applying the configurations may take 2–3 minutes.

26. Click **Reboot**.
27. Allow 3–4 minutes for the reboot to complete before continuing to the next exercise.

Exercise 2: Creating an Administrative Account

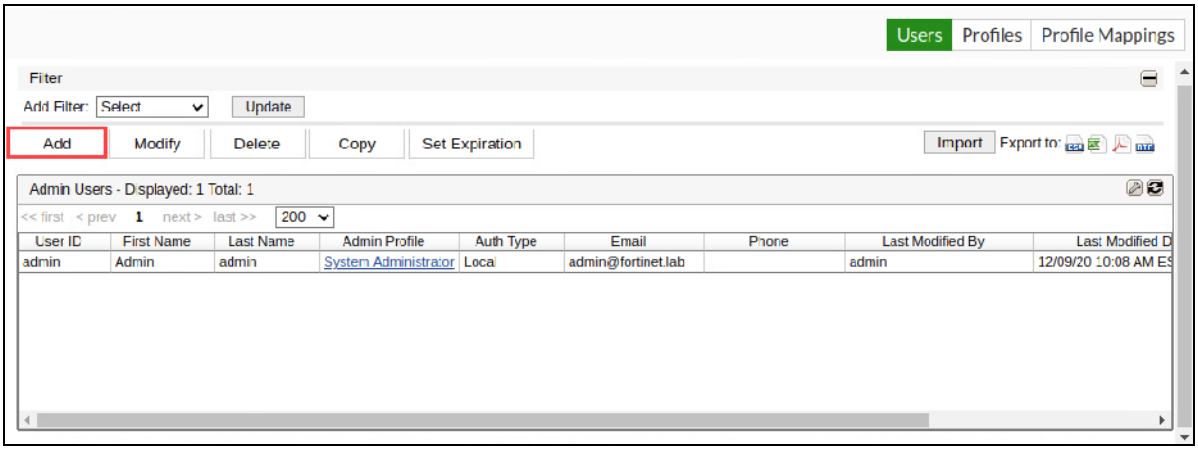
In this exercise, you will access the FortiNAC GUI using a browser, and create a new administrative user account. The FortiNAC GUI is where you perform all administrative functions. Administrative user accounts provide customized access and capabilities to FortiNAC administrators. You will log in to the FortiNAC GUI throughout this lab with the login credentials that you create in the following procedure.

Access the FortiNAC GUI and Create an Administrative User Account

Administrative user accounts provide customized access and capabilities to FortiNAC administrators. You will create an administrative user account to use in this lab.

To access the FortiNAC GUI and create an administrative user account

1. Log in to the FortiNAC-Primary GUI with the username `admin` and password `password`.
2. Click **Users & Hosts** > **Administrators**, and then click **Add**.



3. In the **Enter User ID** window, type `User1`, and then click **OK**.
   The **Add User** window opens.
4. In the **Authentication Type** field, select **Local**.
5. In the **Admin Profile** field, select **System Administrator**.
6. Click in the **Password** field, in the **Change Password** window, type `password`, confirm `password` , and then click **OK**.
7. In the **Last Name** field type `User`.
8. In the **Add User** window, click **OK**.
9. Log out of the FortiNAC-Primary GUI, and then log back in using the account that you created to test your access to the account.
10. Accept the **End User License Agreement**, and then click **OK**.
11. Log out of the FortiNAC-Primary GUI.

Lab 2: Network Discovery and Group Creation

In this lab, you will discover the network infrastructure devices to begin achieving device and endpoint visibility. You will also create groups that are used to organize elements.

Objectives

- Access the FortiNAC GUI
- Model network devices
- Create groups

Time to Complete

Estimated: 30 minutes

Exercise 1: Discovering Network Devices

In this exercise, you will discover wired components of the lab network infrastructure for visibility purposes, and organize these components, using containers in the FortiNAC inventory view.

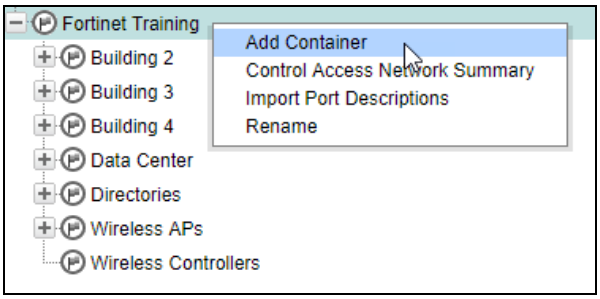
Discover Network Devices

In FortiNAC, infrastructure devices are discovered for the visibility and control of both the devices and the endpoints that connect to them.

You will add several infrastructure devices to the inventory view, while following best practices for device modeling.

To discover network devices

1. Log in to the FortiNAC-Primary GUI with the username `admin` and password `password`.
2. Click **Network** > **Inventory**, right-click the **Fortinet Training** container, and then select **Add Container**.

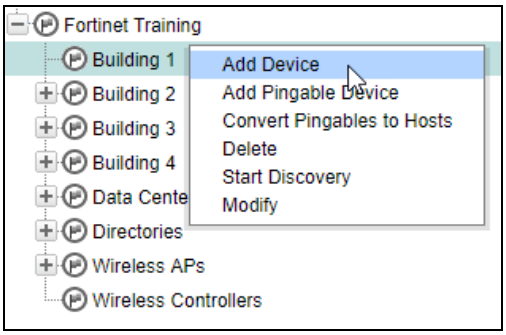


   The **Add Container** window opens.

3. Configure the following settings:

Field	Value
Name	Building 1
Note	Building 1 infrastructure devices

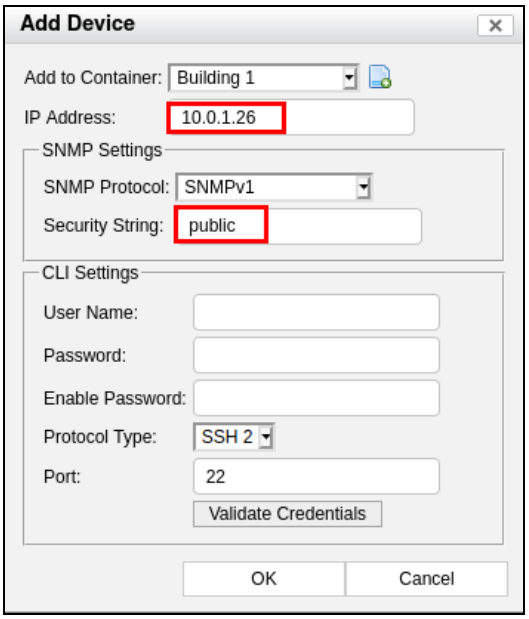
4. Click **OK**.
5. Right-click the **Building 1** container, and then select **Add Device**.
   The **Add Device** window opens.



6. Configure the following settings:

Field	Value
IP Address	10.0.1.26
Security String	public

The completed fields should look like the following image:



The ability of FortiNAC to communicate with the network infrastructure is fundamental to its ability to achieve visibility and provide control and automation.

7. Click **OK**.
   The device appears in the container.
8. Expand the **Building 1** container, and then select the **Building 1 Switch** device.
9. Right-click **Building 1 Switch**, and then select **Poll for L2 (Hosts) Info**.

The **Ports** tab shows all physical ports discovered on the device. It also shows the ports that have devices connected to them and the ports that are uplinks (small cable icon). Hosts should populate on some of the ports.

10. Right-click the **Fortinet Training** container, and then select **Add Container**.
    The **Add Container** window opens.
11. Configure the following settings:

Field	Value
Name	Nashua Facility
Note	Nashua infrastructure devices

12. Click **OK**.
13. Right-click the **Nashua Facility** container, and then select **Add Device**.
    The **Add Device** window opens.
14. Configure the following settings:

Field	Value
IP Address	10.0.1.27
Security String	public

There are no CLI settings.

15. Keep the values for the remaining settings, and then click **OK**.
16. Right-click the **Fortinet Training** container, and then select **Add Container**.
    The **Add Container** window opens.
17. Configure the following settings:

Field	Value
Name	Manchester Facility
Note	Manchester facility infrastructure devices

18. Click **OK**.
19. Right-click the **Manchester Facility** container, and then select **Add Device**.
    The **Add Device** window opens.
20. Configure the following settings:

Field	Value
IP Address	10.0.1.30
Security String	public

21. Keep the values for the remaining settings, and then click **OK**.
22. Right-click the **Data Center** container, and then select **Add Device**.
    The **Add Device** window opens.
23. Configure the following settings:

Field	Value
IP Address	10.0.1.15
Security String	public
User Name	admin
Password	password

FortiNAC names modeled devices using the sysName object read from the MIB during modeling. Notice that this last switch is named **Engineering-Switch**.

24. Click **OK**.

To discover the FortiGate

1. Right-click the **Fortinet Training** container, and then select **Add Container**.
   The **Add Container** window appears.
2. Configure the following settings:

Field	Value
Name	Security Devices
Note	Our security devices

3. Click **OK**.
4. Right-click the new container, and then select **Add Device**.
   The **Add Device** window opens.
5. Configure the following settings:

Field	Value
Add to Container	Security Devices

Field	Value
IP Address	10.0.1.254
SNMP Protocol	SNMPv1
Security String	private
User Name	admin
Password	password
Enable Password	(Leave this field empty.)
Protocol	SSH2

6. Click **OK**.
   FortiGate-Edge appears in the container.
7. Expand the **Security Devices** container, and then select the **FortiGate-Edge** device.
8. Click the **Virtualized Devices** tab, right-click the **root** virtualized device, and then select **Model Configuration**.
9. In the **RADIUS Mode** field, select **Local**.
10. In the **RADIUS** section, click **Change**, and then in the **RADIUS Secret** field, type `password`.
11. In the **RADIUS** section, verify that the **Source IP Address** field is set to `10.0.1.254`.
12. Click **OK**.

Configure Layer 3 Polling

You will configure FortiNAC to gather Layer 3 information (IP address) from FortiGate to enhance endpoint visibility.

To configure Layer 3 polling

1. Click **Network** > **L3 Polling**, and then in the **Display** field, select **All Devices**.

2. In the list of network devices, select **FortiGate-Edge**, and then at the top of the page, click **Set Polling**.
   The **Set Polling** window opens.
3. Select the **Enable Polling** checkbox, in the **Interval** field, select **5 Minutes**, in the **Priority** field, select **Low**, and then click **OK**.

Exercise 2: Creating and Populating Groups

In this exercise, you will create and modify several groups using methods that will help you achieve the site deployment objectives.

Create and Populate Port Groups

You can use port groups to organize physical ports into logical groups, to meet the requirements of a deployment strategy.

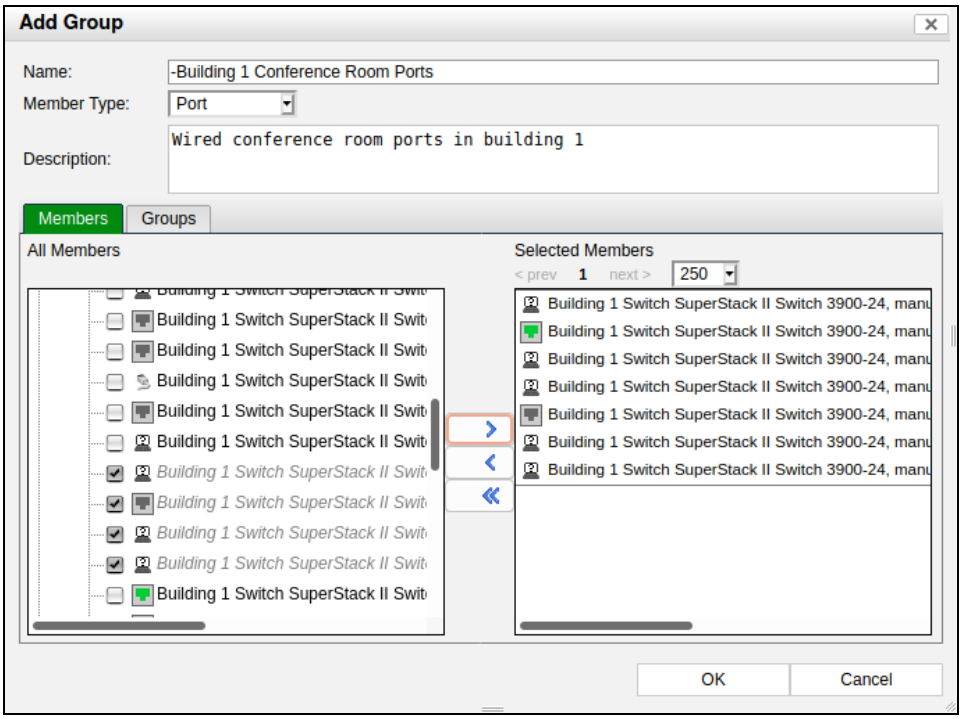
You will create eight port groups to organize different sets of ports.

To create and populate port groups

1. Log in to the FortiNAC-Primary GUI with the username `admin` and password `password`.
2. Click **System** > **Groups**, and then click **Add**.
   The first group that you add is used to identify the physical wired ports in the conference room in building 1.
3. In the **Add Group** window, configure the following settings:

Field	Value
Name	-Building 1 Conference Room Ports (Add – in front of the names, so they are sorted to the top of the list.)
Member Type	Port
Description	Wired conference room ports in building 1

4. On the **Members** tab, in the topology tree, locate and expand **Building 1 Switch**.
   Expand the pop-up window to make the port numbers visible.
5. In the **All Members** field, select ports 2–4 and ports 16–19, and then click the arrow to move them to the **Selected Members** field.



There are no settings for the **Groups** tab at this time.

6. Click **OK**.
7. Following the same steps, configure the following settings to build a second port group:

Field	Value
Name	-Building 1 Ports (Add – in front of the names, so they are sorted to the top of the list.)
Member Type	Port
Description	All wired ports in building 1

8. On the **Members** tab, in the **All Members** field, select the **Building 1** container, and then click the arrow to move the ports to the **Selected Members** field.
9. Click **OK**.
10. Following the same steps, configure the following settings to build another port group:

Field	Value
Name	-Nashua Facility Ports (Add – in front of the names, so they are sorted to the top of the list.)
Member Type	Port
Description	All wired ports in the Nashua facility

11. On the **Members** tab, add all of the ports from the switch that you modeled in the **Nashua** container.
12. Click **OK**.
13. Following the same steps, configure the following settings to build another port group:

Field	Value
Name	-Nashua Facility Conference Room Ports (Add – in front of the names, so they are sorted to the top of the list.)
Member Type	Port
Description	All conference room ports in the Nashua facility

14. On the **Members** tab, add ports 7–9 and 18–21 from the switch that you modeled in the **Nashua Facility** container.
15. Click **OK**.
16. Following the same steps, configure the following settings to build another port group:

Field	Value
Name	-Manchester Facility Ports (Add – in front of the names, so they are sorted to the top of the list.)
Member Type	Port
Description	All wired ports in the Manchester facility

17. On the **Members** tab, add all of the ports from the switch that you modeled in the **Manchester** container.
18. Click **OK**.
19. Following the same steps, configure the following settings to build another port group:

Field	Value
Name	-Building 3 Wired Ports (Add – in front of the names so they are sorted to the top of the list.)
Member Type	Port
Description	Access ports in building 3

20. On the **Members** tab, add ports 2–8 from the switch modeled in the **Building 3** container.
21. Click **OK**.
22. Following the same steps, configure the following settings to build another port group:

Field	Value
Name	-Building 4 Wired Ports (Add – in front of the names, so they are sorted to the top of the list.)
Member Type	Port
Description	Access ports in building 4

23. On the **Members** tab, add ports 2–8 from the switch modeled in the **Building 4** container.
24. Click **OK**.
25. Following the same steps, configure the following settings to build another port group:

Field	Value
Name	-Engineering Ports (Add – in front of the names, so they are sorted to the top of the list.)
Member Type	Port
Description	Access ports used by engineering

26. On the **Members** tab, add ports 2–8 from the **EngineeringSwitch** switch that you modeled in the **Data Center** container.
27. Click **OK**.

Create and Populate Port Groups With SSIDs

When you add SSIDs to port groups, you can use them to identify the point of connection in the same way that you use physical ports.

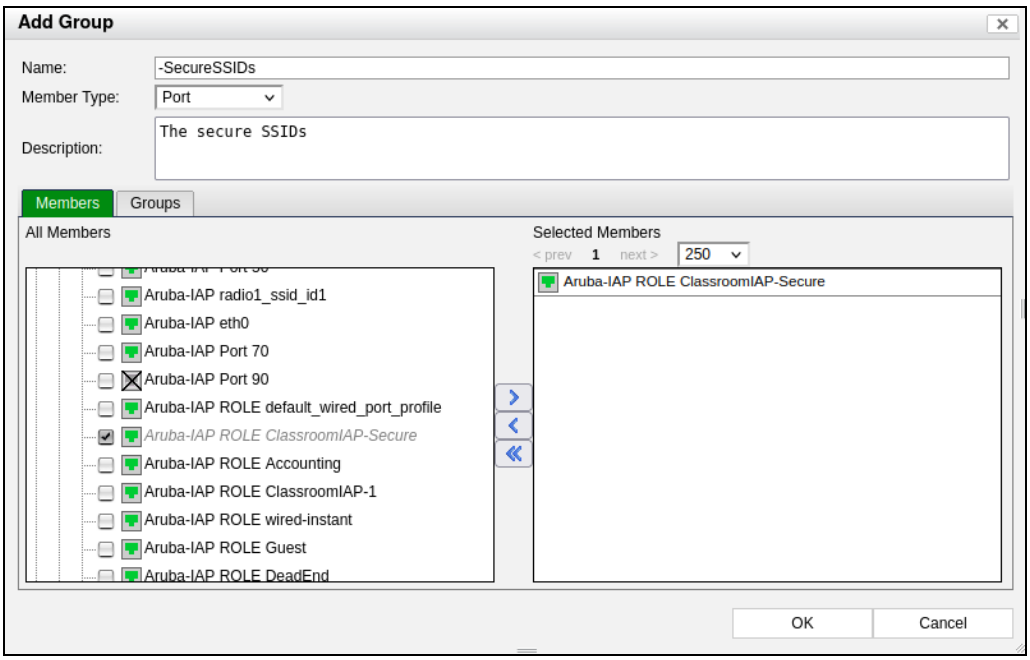
You will create two additional port groups and add SSIDs to them.

To create and populate port groups with SSIDs

1. Following the same steps as in the previous procedure, create two groups.
   The first group will be used to identify Fortinet Secure SSIDs.
2. In the **Add Group** window, configure the following settings:

Field	Value
Name	-SecureSSIDs (Add – in front of the names, so they are sorted to the top of the list.)
Member Type	Port
Description	The secure SSIDs

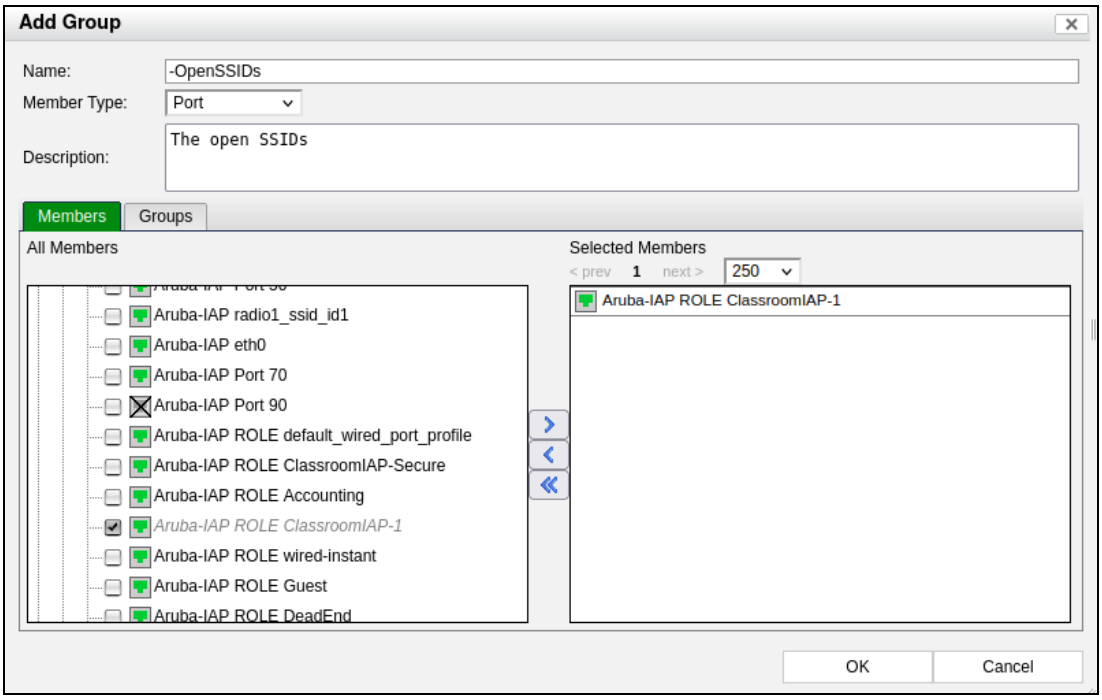
3. In the **All Members** field, expand the **Wireless APs** container.
4. Locate and expand **Aruba-IAP**.
5. Select the **Aruba-IAP ROLE ClassroomIAP-Secure** SSID, and then click the arrow to move it to the **Selected Members** field.



6. Click **OK**.
7. Create another group, using the following settings:

Field	Value
Name	-OpenSSIDs (Add – in front of the names, so they are sorted to the top of the list.)
Member Type	Port
Description	The open SSIDs

8. In the **All Members** field, expand the **Wireless APs** container.
9. Locate and expand the **Aruba-IAP** controller.
10. Select the **Aruba-IAP ROLE ClassroomIAP-1** SSID, and then click the arrow to move it to the **Selected Members** field.



11. Click **OK**.

Create Host Groups

You can use host groups to organize endpoints for management.

You will create a host group that you will use in the next lab to automatically organize endpoints.

To create a host group

1. Click **System** > **Groups**, and then click **Add**.
   The **Add Group** window opens.
2. Configure the following settings:

Field	Value
Name	-Card Readers (Add – in front of the names, so they are sorted to the top of the list.)
Member Type	Host
Days Valid	(Leave this field empty.)
Days Inactive	(Leave this field empty.)
Description	All card readers at Fortinet

Do not select any members for this group (no card readers are identified yet). You will use this group when you begin identifying the hosts on the network.

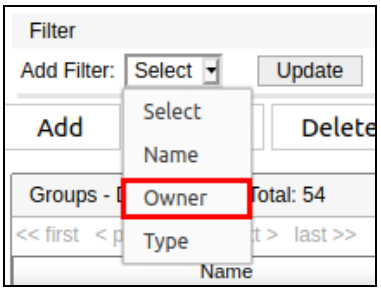
3. Click **OK**.

Set Aging Host Records

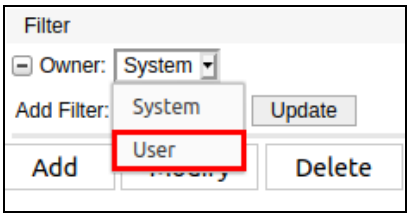
You can set aging values for host records. These values define how long a host remains in the database before it is deleted. This is an automated method to keep the database efficient. Setting aging at the group level overrides global aging settings.

To age hosts by group

1. In the **Filter** section, in the **Add Filter** field, select **Owner**.



2. In the **Owner** field, select **User**, and then click **Update**.



The list of user-owned groups that appears should include **Accounting**, **Engineering**, and **IT Services**. These groups are imported from Active Directory. Fortinet employees are members of these groups. Use the `Ctrl` key and your mouse to select only these three groups.

3. Right-click one of the selected **Host** groups, and then select **Set Aging**.
4. In the **Set Aging** window, leave the **Days Valid** field empty, and then in the **Days Inactive** field, type `90`.
5. Click **OK**.

   The **Days Inactive** columns should reflect the change.

Aging settings will be discussed in detail in an upcoming lesson. Setting the **Days Inactive** value to `90` deletes members of the group from the database if they have not been online for 90 consecutive days.

Lab 3: Identification and Classification of Rogue Devices Using Device Profiling Rules

In this lab, you will modify the FortiNAC database of vendor OUIs and leverage these changes when you configure device profiling rules.

Objectives

- Make changes to the FortiNAC vendor OUI database
- Create device profiling rules to automate the identification and classification of devices

Time to Complete

Estimated: 30 minutes

Exercise 1: Updating Vendor OUI Tables

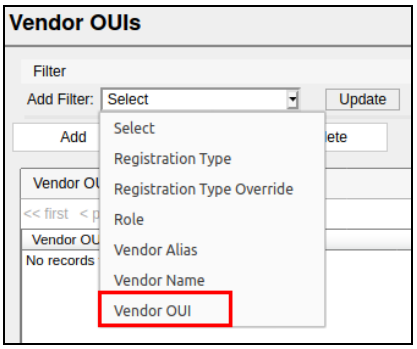
In this exercise, you will modify entries in the vendor OUI tables and leverage the powerful capabilities of the device profiling tool.

Update Vendor OUI Aliases for Card Readers

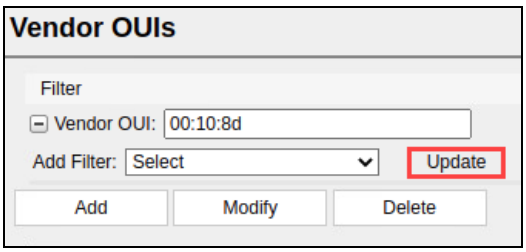
The vendor OUI tables allow FortiNAC to identify invalid OUIs if they attempt to access the network. You can also modify the tables so that you can use them in device profiling rules.

To update vendor OUI aliases for card readers

1. Log in to the FortiNAC-Primary GUI with the username `admin` and password `password`.
2. Click **Network** > **Settings**, open the **Identification** folder, and then select **Vendor OUIs**.
3. In the **Add Filter** field, select **Vendor OUI**.



4. In the **Vendor OUI** field, type `00:10:8d`, and then click **Update**.



One vendor OUI is displayed.

5. Double-click the entry or select it, and then click **Modify**.
The **Modify Vendor OUI** window opens.
6. In the **Vendor Alias** field, type `Card Readers`, and then click **OK**.
7. Repeat steps 4–6 using the vendor OUI `00:01:e6` to identify another type of card reader.

Update Vendor OUI Aliases for IP Phones

You will update vendor OUI aliases for all of the IP phones.

To update vendor OUI aliases for IP phones

1. In the **Vendor OUI** field, type `00:06:5B`, and then click **Update**.
2. Double-click the entry or select it, and then click **Modify**.
   The **Modify Vendor OUI** window opens.
3. In the **Vendor Alias** field, type `IP Phones`, and then click **OK**.
4. Repeat steps 1–3 using the vendor OUI `00:03:E3` to identify another type of IP phone.

Update Vendor OUI Aliases for Cameras

You will update the vendor OUI aliases for all of the cameras.

To update vendor OUI aliases for cameras

1. In the **Vendor OUI** field, type `00:0D:56`, and then click **Update**.
2. Double-click the entry or select it, and then click **Modify**.
   The **Modify Vendor OUI** window opens.
3. In the **Vendor Alias** field, type `Cameras`, and then click **OK**.
4. Repeat steps 1–3 using the vendor OUI `00:50:56` to identify another type of camera.

Exercise 2: Creating Device Profiling Rules

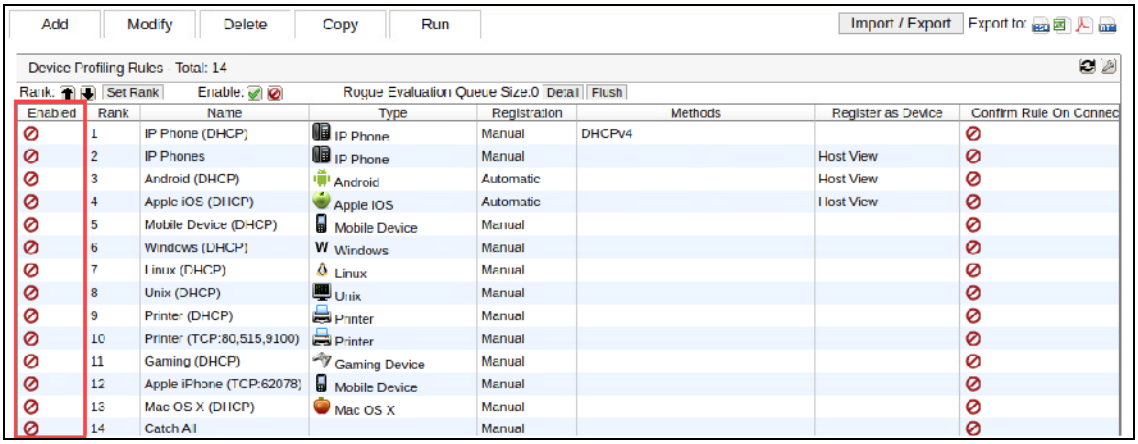
In this exercise, you will create several device profiling rules to identify and classify some of the many types of devices connected to the lab environment. Next, you will evaluate all of the unknown devices against these rules and view the results. Finally, you will create a backup copy of the FortiNAC database to prevent data loss.

Create a Device Profiling Rule for IP Phones

You will create a device profiling rule for IP phones, and then set a rule rank.

To create a device profiling rule for IP phones

1. Log in to the FortiNAC-Primary GUI with the username `admin` and password `password`.
2. Click **Users & Hosts** > **Device Profiling Rules**, and then make sure that all of the existing rules are disabled.



3. Click **Add**.
4. In the **Add Device Profiling Rule** window, configure the following settings:

Field	Value
Enabled	(Select this option.)
Name	Our IP Phones
Description	Identifies all connected IP phones
Note	(Leave this field empty.)
Notify Sponsor	(Ensure this checkbox is not selected.)
Registration	Automatic
Type	IP Phone

Field	Value
Role	NAC-Default
Register as	Device in Host View
Add to Group	(Ensure this checkbox is not selected.)
Access Availability	Always

5. Ensure that none of the **Rule Confirmation Settings** are selected.
6. Click the **Methods** tab.
7. Select the **Vendor OUI** method, and then in the **Vendor OUI** tab, click **Add**.
   The **Add OUI** window opens.
8. In the **Field** field, select **Vendor Alias**.
9. In the **Value** field, type `IP Phones`, and then click **OK**.
10. Click **OK**.
    The new device profiling rule appears in the rules list as the only enabled rule.
11. Select the rule, and then click **Set Rank** to set its rank to **1**.

Create a Device Profiling Rule for Card Readers

You will create a device profiling rule for card readers, and then set a rule rank.

To create a device profiling rule for card readers

1. Click **Users & Hosts** > **Device Profiling Rules**, and then click **Add**.
2. In the **Add Device Profiling Rule** window, configure the following settings:

Field	Value
Enabled	(Select this option.)
Name	Card Readers
Description	Identifies card readers
Note	(Leave this field empty.)
Notify Sponsor	(Ensure this checkbox is not selected.)
Registration	Automatic
Type	Card Reader
Role	NAC-Default
Register as	Device in Host View

Field	Value
Add to Group	-Card Readers
Access Availability	Always

3. Ensure that none of the **Rule Confirmation Settings** are selected.
4. Click the **Methods** tab.
5. Select the **Vendor OUI** method, and then in the **Vendor OUI** tab, click **Add**.
   The **Add OUI** window opens.
6. In the **Field** field, select **Vendor Alias**.
7. In the **Value** field, type `Card Readers`, and then click **OK**.
8. Click **OK**.
9. Select the rule, and then click **Set Rank** to set its rank to **2**.

Create Device Profiling Rules for Cameras in the Manchester and Nashua Facilities

You will create device profiling rules for cameras at two locations, and then set rule rankings.

To create a device profiling rule for cameras in the Manchester facility

1. Click **Users & Hosts** > **Device Profiling Rules**, and then click **Add**.
2. In the **Add Device Profiling Rule** window, configure the following settings:

Field	Value
Enabled	(Select this option.)
Name	Cameras in Manchester
Description	Identifies cameras in the Manchester facility
Note	(Leave this field empty.)
Notify Sponsor	(Ensure this checkbox is not selected.)
Registration	Automatic
Type	Camera
Role	NAC-Default
Register as	Device in Host View
Access Availability	Always

3. Ensure that none of the **Rule Confirmation Settings** are selected.
4. Click the **Methods** tab.

5. Select the **Location** method, and then click **Add**.
6. Select the port group named **-Manchester Facility Ports**, and then click **OK**.
7. Select the **Vendor OUI** method, and then in the **Vendor OUI** tab, click **Add**.
   The **Add OUI** window opens.
8. In the **Field** field, select **Vendor Alias**.
9. In the **Value** field, type `Cameras`, and then click **OK**.
10. Click **OK**.
11. Select the rule, and then click **Set Rank** to set its rank to **3**.

To create a device profiling rule for cameras in the Nashua facility

1. Click **Users & Hosts** > **Device Profiling Rules**, and then click **Add**.
2. In the **Add Device Profiling Rule** window, configure the following settings:

Field	Value
Enabled	(Select this option.)
Name	Cameras in Nashua
Description	Identifies cameras in the Nashua facility
Note	(Leave this field empty.)
Notify Sponsor	(Ensure this checkbox is not selected.)
Registration	Automatic
Type	Camera
Role	NAC-Default
Register as	Device in Host View
Access Availability	Always

3. Ensure that none of the **Rule Confirmation Settings** are selected.
4. Click the **Methods** tab.
5. Select the **Location** method, and then click **Add**.
6. Select the port group named **-Nashua Facility Ports**, and then click **OK**.
7. Select the **Vendor OUI** method, and in the **Vendor OUI** tab, click **Add**.
   The **Add OUI** window opens.
8. In the **Field** field, select **Vendor Alias**.
9. In the **Value** field, type `Cameras`, and then click **OK**.
10. In the **Add Device Profiling Rule** window, click **OK**.
11. Select the rule, and then click **Set Rank** to set its rank to **4**.

Create a Device Profiling Rule for Environmental Units

You will create a device profiling rule for environmental units, and then set a rule rank.

To create a device profiling rule for environmental units

1. Click **Users & Hosts** > **Device Profiling Rules**, and then click **Add**.
2. In the **Add Device Profiling Rule** window, configure the following settings:

Field	Value
Enabled	(Select this option.)
Name	Environmental Control Units
Description	Identifies Mitsubishi ECUs
Note	(Leave this field empty.)
Notify Sponsor	(Ensure this checkbox is not selected.)
Registration	Automatic
Type	Environmental Control
Role	NAC-Default
Register as	Device in Host View
Access Availability	Always
Confirm Device Rule on Connect	(Select this option.)

3. Ensure that the remaining **Rule Confirmation Settings** are not selected.
4. Click the **Methods** tab.
5. Select the **Vendor OUI** method, and then click **Add**.
6. Configure the following settings:

Field	Value
Field	Vendor Code
Value	02:09:0F

7. Click **OK**.
8. Select the **SNMP** method, and then configure the following settings:

Field	Value
OID	1.3.6.1.2.1.1.2.0

Field	Value
Port	161
SNMP V1 Security String	public

9. Select the **Match** checkbox, and then click **Add**.
10. In the **Add Value** field, type `1.3.6.1.4.1.673.5685`, and then click **OK**.
11. Select the **TCP** method, and then type the following two ports (separated by a comma): `6005,8090`.
12. Click **OK**.
13. Select the rule, and then click **Set Rank** to set its rank to **5**.

Create a Device Profiling Rule for Healthcare Devices

You will create a device profiling rule for blood pressure monitors, and then set a rule rank.

To create a device profiling rule for healthcare devices

1. Click **Users & Hosts** > **Device Profiling Rules**, and then click **Add**.
2. In the **Add Device Profiling Rules** window, configure the following settings:

Field	Value
Enabled	(Select this option.)
Name	Healthcare Device
Description	Network connected blood pressure monitors
Note	(Leave this field empty.)
Notify Sponsor	(Ensure this checkbox is not selected.)
Registration	Automatic
Type	Health Care Device
Role	NAC-Default
Register as	Device in Host View
Access Availability	Always
Confirm Device Rule on Connect	(Select this option.)

3. Ensure that the remaining **Rule Confirmation Settings** are not selected.
4. Click the **Methods** tab.
5. Select the **Vendor OUI** method, and then click **Add**.
6. Configure the following settings:

Field	Value
Field	Vendor Code
Value	02:09:0F

7. Click **OK**.
8. Select the **SSH** method.
9. In the **Credentials** section, click **Add**, and then configure the following settings:

Field	Value
Name	admin
Password	password

10. Click **OK**.
11. In the **Commands** section, click **Add**, and then configure the following settings:

Field	Value
Type	Expect
Command	.*?@BPMonitor:

12. Click **OK**.
13. Select the **Match** checkbox, and then click **Add**.
14. In the **Add Value** field, type `BPMonitor`, and then click **OK**.
15. Select the **TCP** method, and in the **Port** field, type `8080`.
16. In the **Add Device Profiling Rule** window, click **OK**.
17. Select the rule, and then click **Set Rank** to set its rank to **6**.

Profile Existing Rogues, Evaluate New Rogues, and View Results

You will evaluate all existing rogues against all enabled device profiling rules.

To profile existing rogues, evaluate new rogues, and view results

1. In the **Device Profiling Rules** window, click **Run**.
   A window opens asking if you are sure you want to evaluate all rogues.
2. Click **Yes**, and then click **OK**.
   FortiNAC evaluates all rogues that currently exist in its database.
3. Click **Users & Hosts** > **Profiled Devices**, and then in the **Filter** section, click **Update**.
   FortiNAC should have identified many of the devices on the network.

Create a Backup of the FortiNAC Database

You will back up the FortiNAC database.

To create a backup of the FortiNAC database

1. Click **System** > **Settings**, and then expand the **System Management** folder.
2. Click **Database Backup/Restore**.
3. In the **Schedule Database Backup** section, click **Run Now**.
   A new entry appears in the **Database Restore** field with the current date and timestamp.

Lab 4: Visibility Views, Event Management, and Logging

In this lab, you will use the **Hosts** page to gather inventory information about network devices. Then, you will configure an upstream log receiver and the necessary events to meet logging requirements.

Objectives

- Create filters on the **Hosts** page
- Troubleshoot host connectivity issues
- Configure upstream logging for events

Time to Complete

Estimated: 20 minutes

Exercise 1: Creating Filters on the Hosts Page

In this exercise, you will create custom and quick filters on the **Hosts** page.

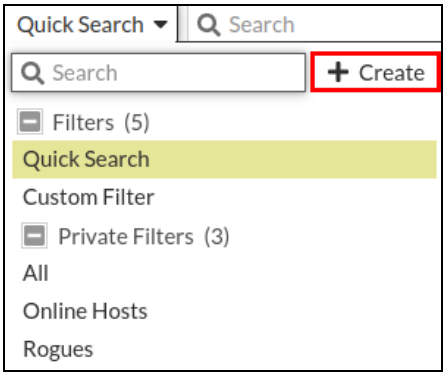
Create a Filter on the Hosts Page

Custom filters allow you to locate user, host, and adapter records.

You will use custom filters to create and export a list of cameras that belong to a specific vendor and are connected to the network.

To create a filter on the Hosts page

1. Log in to the FortiNAC-Primary GUI with the username `admin` and password `password`.
2. Click **Users & Hosts** > **Hosts**, in the **Quick Search** drop-down list, click **Create**.



The **New Filter** window opens.

3. In the **Filter Name** field, type `Camera by OUI`, select **Private**, and then click **OK**.
4. On the **Adapter** tab, select the **Physical Address** checkbox, and then type `00:50:56*`.
5. Click the **Host** tab.
6. In the **Misc** section, select **Device Type**, and then select **Camera**.
7. Click **OK**.
   The **Hosts** page should update and display only cameras that have the designated vendor OUI.

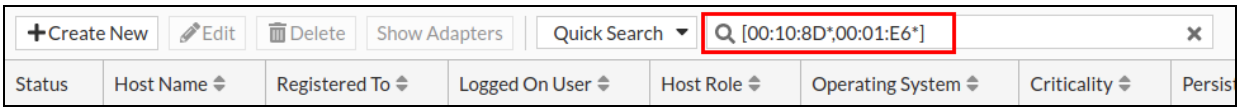
Use a Quick Filter

Quick filters allow you to create quick and simple filters that focus on the most common filter criteria.

You will create a quick filter to display and export card readers that are connected to the network.

To use a quick filter

1. In the **Custom Filter** drop-down list, select **Quick Search**.
2. In the search field, type `[00:10:8D*,00:01:E6*]`, and then press `Enter`.



The **Hosts** page should update and display all of the card readers.

You can use brackets in the **Quick Search** field to search for multiple criteria. This example shows all devices that have either vendor OUI.

Exercise 2: Troubleshooting a Host Connectivity Issue

In this exercise, you will troubleshoot a card reader that is not being profiled. The card reader is from a different vendor than other card readers used in the environment. You will determine if the card reader is in the database and why FortiNAC is not profiling it. After determining why it is not being profiled, you will manually classify the card reader.

Determine if the Host Is in the Database

You will use the FortiNAC CLI and FortiNAC GUI to validate that FortiNAC detected the card reader on the network.

To determine if the host is in the database

1. Log in to the FortiNAC-Primary CLI with the username `root` and password `password`.
2. Enter the following command to determine if the card reader was added to the database:

   ```
   Client -mac *B1:FD:97
   ```

   The following image shows sample output:

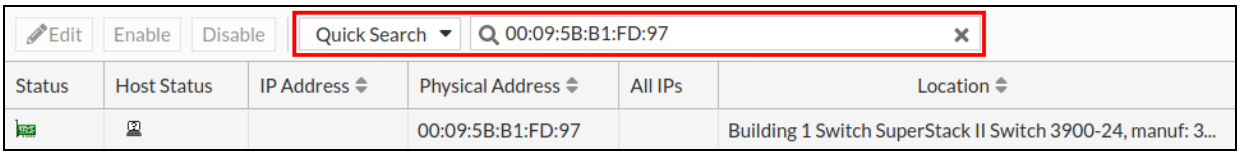
```
> Client -mac *B1:FD:97
Found 1 matches for client

NETGEAR
        DBID = 63
        MAC = 00:09:5B:B1:FD:97
        IP = null
        Medium = null
        Description = null
        Status = Connected
        State = Initial
        Type = RogueDynamicClient
        Ident = null
        UserID = null
        ParentID = 1642
        Role = null
        Security Access Value = null
        OS = null
        Location = Building 1 Switch SuperStack II Switch 3900-24
```

   The device was found in the database, but it is not classified (`Type = RogueDynamicClient`).

Note that the systems being used in the lab environment are FortiNAC systems running on CentOS. The lesson presented NAC-OS CLI commands that will not work on CentOS systems.

3. Log in to the FortiNAC-Primary GUI with the username `admin` and password `password`.
4. Click **Users & Hosts** > **Adapters**.
5. In the **Quick Search** field, type the MAC address, and then press `Enter`.



The search results show that a rogue host exists in the database with that MAC address.

Test the Host Against the Card Readers Profiling Rule

You will test the host against the **Card Readers** device profiling rule to validate that it does not match.

To test the host against the Card Readers profiling rule

1. Continuing on the **Adapters** page, right-click the adapter, and then select **Test Device Profiling Rule**.
2. In the **Test Device Profiling Rule** window, in the **Select a Device Profiling Rule to test** field, select **Card Readers**, and then click **OK**.
   The **Test Device Profiling Rule** window displays a **Rule Does Not Match** result.

> **Stop and think!**
>
> Why would this card reader not match the existing device profiling rule?
>
> This card reader is from a vendor that was not included in the device profiling rule.

3. Click **OK** to close the results window.

Classify the Device as a Card Reader Manually

You will manually classify the device as a card reader.

To classify the device as a card reader manually

1. Continuing on the **Adapters** page, right-click the adapter, and then select **Register as Device**.
2. In the **Register As Device** window, configure the following settings:

Field	Value
Manage in	Device in Host View
Device Type	Card Reader
Role	NAC-Default

3. Click **OK**.
   The **Host Status** icon changes from a rogue icon to a card reader icon.
4. Return to the CLI, and then enter the `Client -mac *B1:FD:97` command again.
   The `Type` field should now be set to `DynamicClient`.

```
root@fortinac-primary:~
> Client -mac *B1:FD:97
Found 1 matches for client

NETGEAR
        DBID = 9
        MAC = 00:09:5B:B1:FD:97
        IP = null
        Medium = null
        Description = null
        Status = Connected
        State = Initial
        Type = DynamicClient
        Ident = null
        UserID = null
        ParentID = 1642
        Role = NAC-Default
        Security Access Value = null
        OS = null
        Location = Building 1 Switch SuperStack II Switch 3900-24, manuf:
```

Note that the systems being used in the lab environment are FortiNAC systems running on CentOS. The lesson presented NAC-OS CLI commands that will not work on CentOS systems.

Exercise 3: Configuring Upstream Logging for FortiNAC Events

In this exercise, you will configure an upstream log host, and then designate an event to send upstream to that host when the event occurs.

Configure an Upstream Log Receiver and Events for Upstream Logging

By configuring an upstream log receiver, FortiNAC event and alarm information can be passed to an external system for logging.

You will create an upstream log receiver, and then configure events for upstream logging.

To configure an upstream log receiver

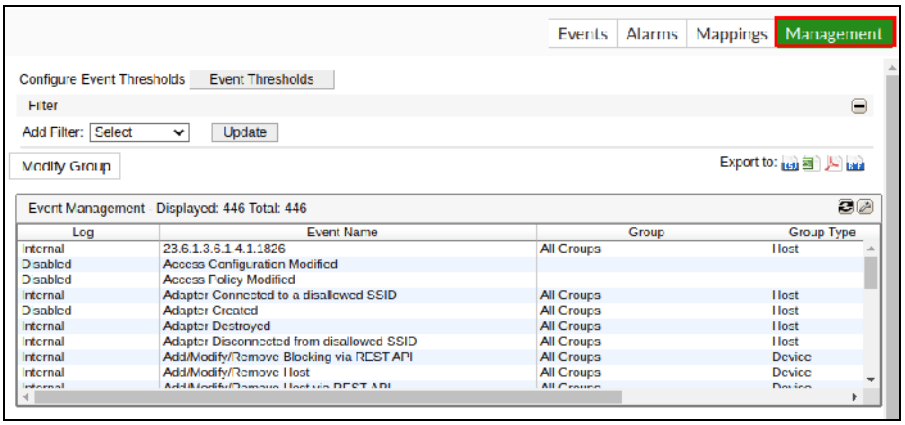
1. Log in to the FortiNAC-Primary GUI with the username `admin` and password `password`.
2. Click **System** > **Settings** > **System Communication** > **Log Receivers**.
3. Click **Add**.
4. In the **Add Log Host** window, configure the following settings:

Field	Value
Type	FortiAnalyzer
IP Address	10.0.1.25
Port	514

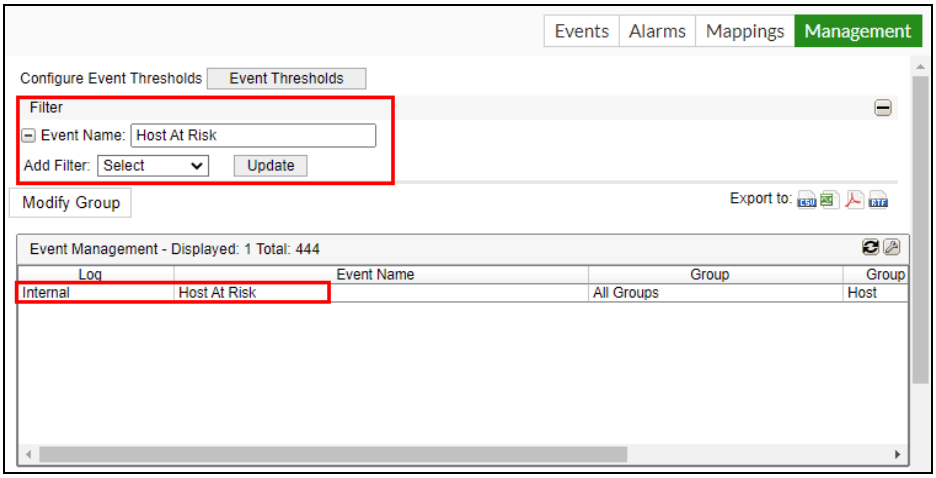
5. Click **OK**.

To configure events for upstream logging

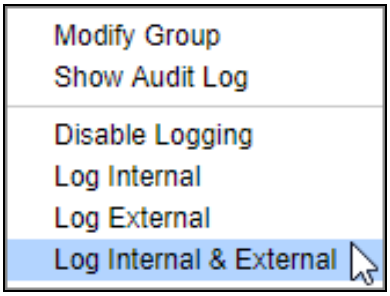
1. Click **Logs** > **Events & Alarms**, and then select **Management**.



2. In the **Add Filter** drop-down list, select **Event Name**, type `Host At Risk`, and then click **Update**.



3. Right-click the event, and then select **Log Internal & External**.



4. Repeat step 3 for the **Disable Host Success** event.

Create a Backup of the FortiNAC Database

You will back up the FortiNAC database.

To create a backup of the FortiNAC database

1. Click **System** > **Settings**, and then expand the **System Management** folder.
2. Select **Database Backup/Restore**.
3. In the **Schedule Database Backup** section, click **Run Now**.
   A new entry appears in the **Database Restore** field with the current date and timestamp.

Lab 5: Logical Networks and Security Fabric Integration

In this lab, you will integrate FortiNAC with FortiGate. First, you will configure both devices to dynamically apply firewall policies to endpoints, based on tags and group memberships that are assigned using FortiNAC security policies. Then, you will configure logical networks to simplify network access policy management.

Objectives

- Define logical networks
- Configure Security Fabric integration between FortiNAC and FortiGate
- Define firewall tags

Time to Complete

Estimated: 30 minutes

Exercise 1: Configuring Logical Networks and Creating a Firewall Tag

In this exercise, you will define logical networks that FortiNAC network access policies will use. Logical networks create an abstraction layer between a value and any number of access configurations. This provides flexibility when enforcing access control, and greatly reduces the number of access control policies.

Create Logical Networks for Card Readers, Cameras, and Contractors

You will create and define logical networks for card readers, cameras, and contractors.

To create logical networks

1. Log in to the FortiNAC-Primary GUI with the username `admin` and password `password`.
2. Click **Network** > **Logical Networks**, click **Create New**, and then configure the following settings to create a new logical network:

Field	Value
Name	Card Readers
Description	Used to provision badge readers

3. Click **OK**.
   The **Card Readers** logical network now appears in the list.
4. Click **Create New**, and then configure the following settings to create another logical network:

Field	Value
Name	Cameras
Description	Used to provision cameras

5. Click **OK**.
   There should be two entries on the **Logical Networks** page.
6. Click **Create New**, and then configure the following settings to create a third logical network:

Field	Value
Name	Contractors
Description	Used to provision contractors

7. Click **OK**.

There should be three entries on the **Logical Networks** page.

8. Click **Create New**, and then configure the following settings to create a fourth logical network:

Field	Value
Name	No Access
Description	Used to deny network access

9. Click **OK**.
   There should be four entries on the **Logical Networks** page.

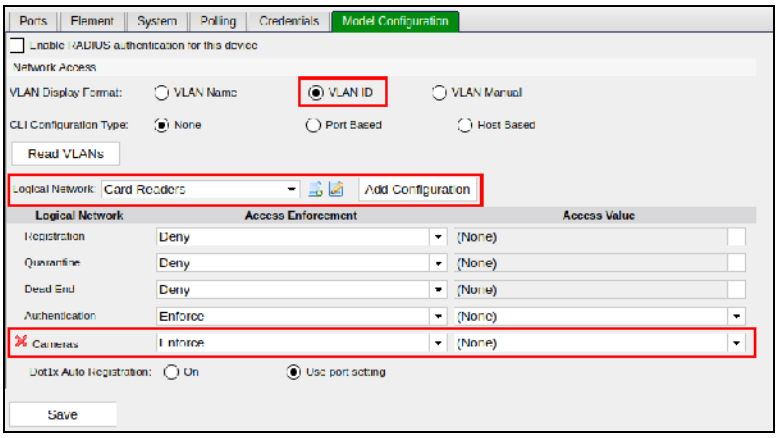
Define Logical Networks for Card Readers, Cameras, and Contractors by VLAN ID and VLAN Name

After logical networks are configured, they appear in the model configuration of each infrastructure device in the topology view. They can be defined by VLAN name or VLAN ID.

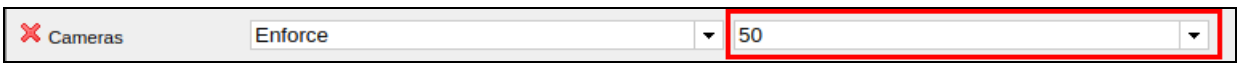
You will define what each logical network means, on multiple devices, using VLAN IDs.

To define logical networks by VLAN ID

1. Continuing on the FortiNAC-Primary GUI, click **Network** > **Inventory**, in the topology tree, expand the **Building 3** branch, and then click **Switch-3**.
2. On the right, click the **Model Configuration** tab.
3. In the **Network Access** section, in the **VLAN Display Format** field, select **VLAN ID**.
4. In the **Logical Network** field, select **Cameras**, and then click **Add Configuration**.
   The **Cameras** logical network appears in the definable **Logical Network** list.

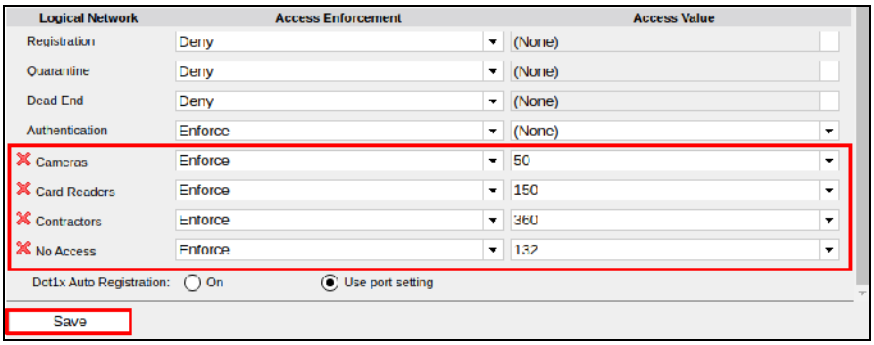


5. In the **Cameras** row, in the **Access Value** column, select **50**.



6. Perform the same steps to add and define the following logical networks:

Logical Network	Access Value
Card Readers	150
Contractors	360
No Access	132



7. Click **Save**.
8. In the topology tree, expand the **Building 4** branch, and then click **Switch-4**.
9. Click the **Model Configuration** tab.
10. In the **Network Access** section, in the **VLAN Display Format** row, select **VLAN ID**.
11. In the **Logical Network** field, select **Cameras**, and then click **Add Configuration**.
    The **Cameras** logical network appears in the definable **Logical Network** list.
12. In the **Cameras** row, in the **Access Value** column, select **25**.
13. Perform the same steps to add and define the following logical networks:

Logical Network	Access Value
Card Readers	60
Contractors	460
No Access	142

14. Click **Save**.

To define logical networks by VLAN name

1. In the topology tree, expand the **Data Center** branch, and then click **Engineering-Switch**.
2. Click the **Model Configuration** tab.
3. In the **Network Access** section, in the **VLAN Display Format** row, select **VLAN Name**.
4. In the **Logical Network** field, select **Cameras**, and then click **Add Configuration**.
   The **Cameras** logical network appears in the definable **Logical Network** list.
5. In the **Cameras** row, in the **Access Value** column, select **Cameras**.
6. Perform the same steps to add and define the following logical networks:

Logical Network	Access Value
Card Readers	CardReaders
Contractors	Contractors
No Access	Eng-DeadEnd

7. Click **Save**.

These logical network names can be configured differently on each infrastructure device. This is an extremely useful feature if, for example, cameras use different VLANs at different locations.

Create a Firewall Tag for Contractors

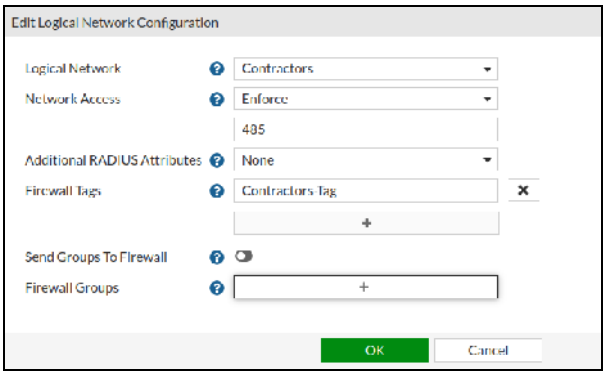
You will create a firewall tag that will be applied to all contractors. This firewall tag will ultimately define group membership on FortiGate and result in the enforcement of firewall policies.

To create a firewall tag

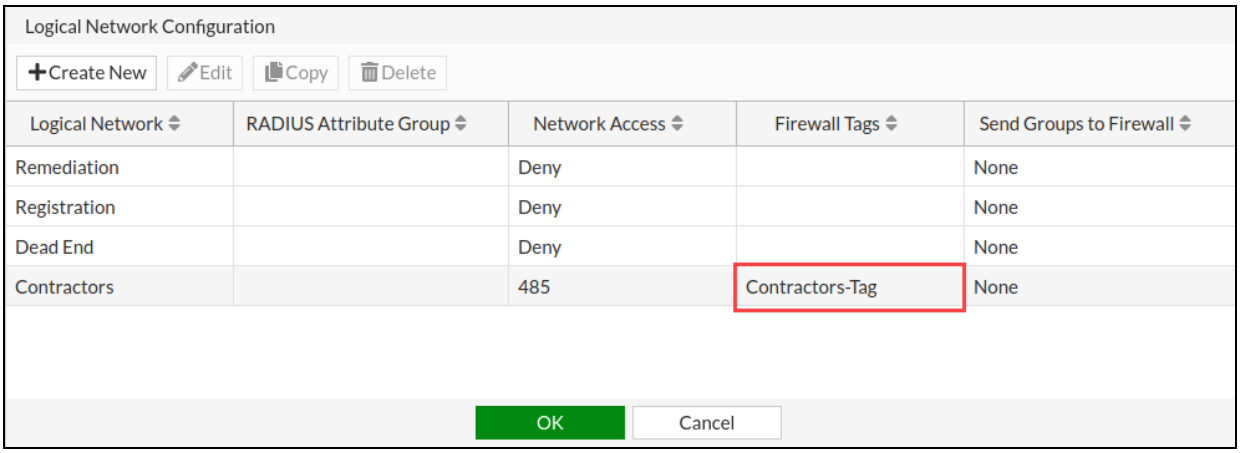
1. Continuing on the FortiNAC-Primary GUI, click **Network** > **Inventory**, in the topology tree, expand the **Security Devices** container, and then click **FortiGate-Edge**.
2. On the right, click the **Virtualized Devices** tab, right-click the **root** virtualized device, and then click **Model Configuration**.
3. In the **Logical Network Configuration** section, click **Create New**, and then configure the following settings.

Field	Value
Logical Network	Contractors
Network Access	Enforce 485
Additional RADIUS Attributes	None
Firewall Tags	Contractors-Tag

4. Leave all other settings at the default values, and then click **OK**.



5. Click **OK**.



6. Click **OK**.

You can create firewall tags directly on the configuration page of the FortiGate virtualized device model, as you did here, or you can create them on the **Firewall Tags** page that is located at **System** > **Settings**, in the **System Communication** folder.

The firewall tag is applied by a security policy, as a result of a template that is applied to contractor accounts. This is covered in a future lab.

Exercise 2: Integrating FortiNAC Into the Security Fabric

In this exercise, you will configure the FortiNAC service connector settings to prepare for Fortinet Security Fabric integration with FortiGate. Integrating FortiNAC into the Security Fabric allows it to pass endpoint group and tag information to FortiGate, which can then be used to dynamically populate FortiGate groups.

Configure the FortiNAC Service Connector for Security Fabric Integration

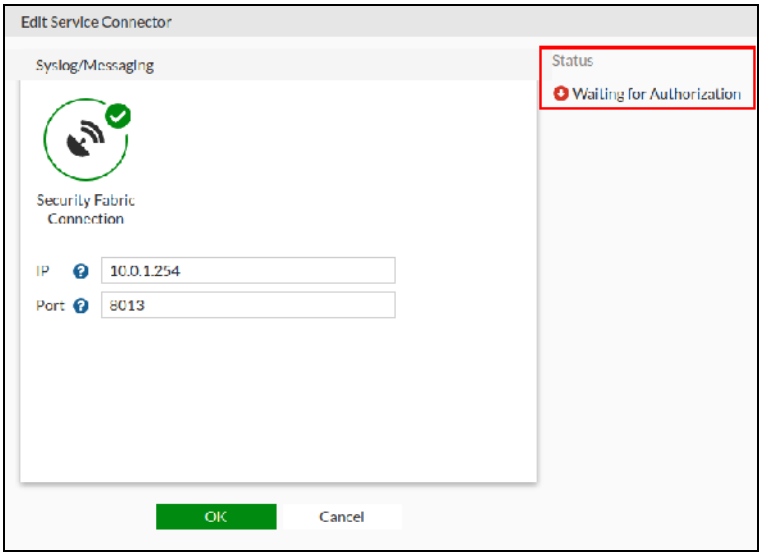
You will configure the settings that allow FortiNAC to be added as a Security Fabric connector.

To configure the FortiNAC service connector for Security Fabric integration

1. Log in to the FortiNAC-Primary GUI with the username `admin` and password `password`.
2. Click **Network** > **Service Connectors**.
3. Click **Create New**.
4. In the **Syslog/Messaging** section, click **Security Fabric Connection**.
5. In the **Create Service Connector** window, configure the following settings:

Field	Value
IP	10.0.1.254
Port	8013

6. Click **OK**.
7. Double-click the **Security Fabric Connection** connector to view the settings.
   The **Status** is **Waiting for Authorization**.



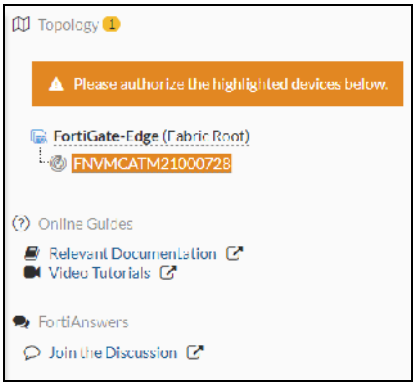
8. Click **OK** to close the **Edit Service Connector** window.

Authorize the FortiNAC to Join the Security Fabric

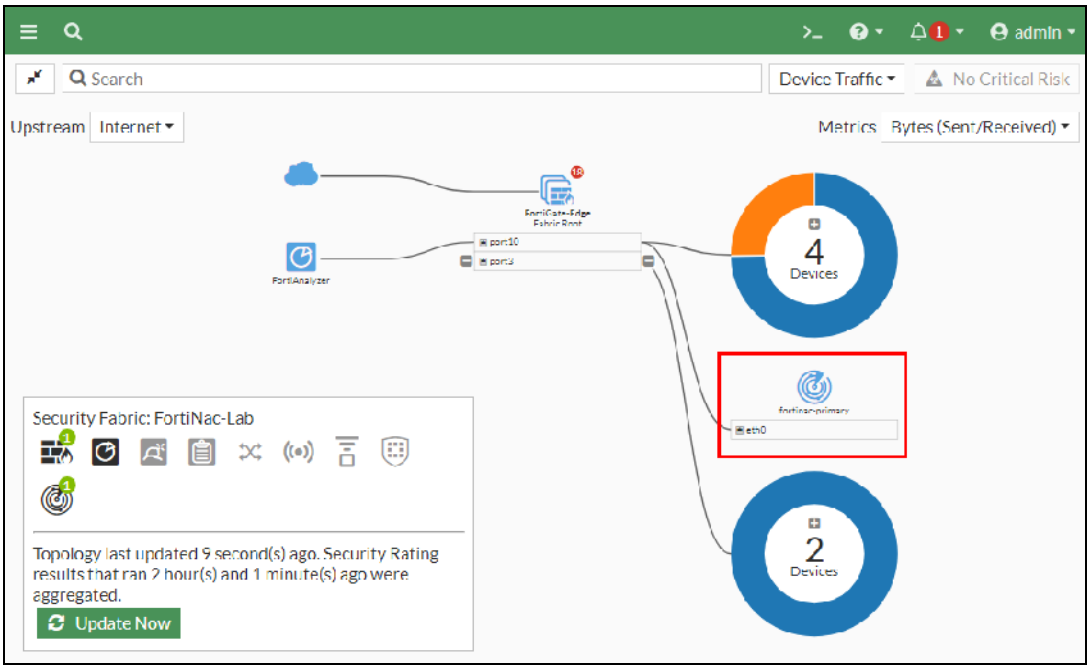
You will log in to the Security Fabric root FortiGate and authorize the FortiNAC to join the Security Fabric.

To authorize the FortiNAC to join the Security Fabric

1. Log in to the FortiGate-Edge GUI with the username `admin` and password `password`.
2. Click **Security Fabric** > **Fabric Connectors**.
   On the right, you can see the FortiNAC waiting to be authorized to join the Security Fabric.



3. Click **FNVMCATM21000728**, and then click **Authorize**.
4. Click **Security Fabric** > **Logical Topology**, and then verify the FortiNAC appears as part of the **Security Fabric**.



5. Log out of the FortiGate-Edge GUI.

Lab 6: Portal Configuration and Access Control Enforcement

In this lab, you will customize your captive portal pages for unknown host registration and verify the page appearance. Then, you will enable registration enforcement for unknown hosts by placing all your access ports in the **Forced Registration** group. You will enable enforcement on the wireless network, using the model configuration pages for your wireless devices.

Objectives

- Customize the captive portal pages
- Prepare devices for endpoint isolation
- Enforce access control

Time to Complete

Estimated: 25 minutes

Exercise 1: Customizing the Captive Portal Pages

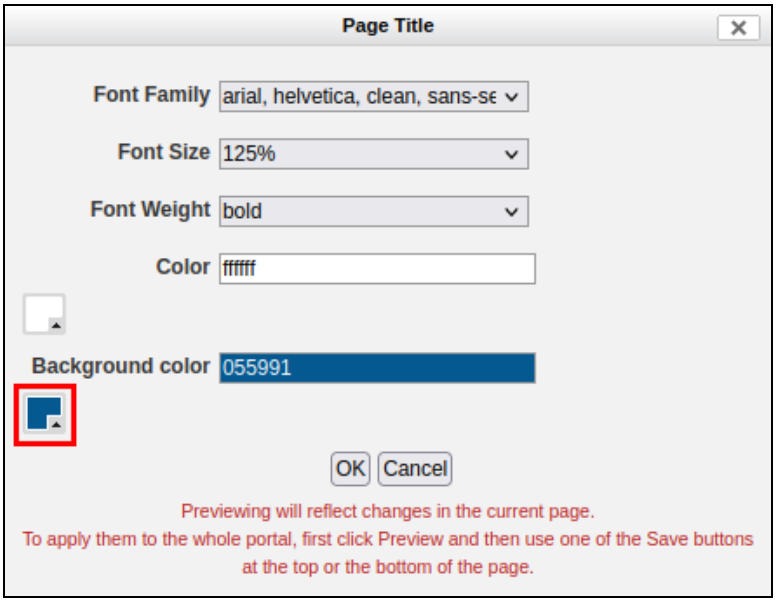
In this exercise, you will customize the registration captive portal page for your registration network.

Customize the Default Portal Page for the Registration Context

The captive portal pages are the web pages that end users are directed to when they have been isolated because of their host state. You will customize the default portal page.

To customize the captive portal pages

1. Log in to the FortiNAC-Primary GUI with the username `admin` and password `password`.
2. Click **Portal** > **Portal Configuration**.
3. On the **Content Editor** tab, expand **Global**, and then select **Styles**.
4. Click the blue banner labeled **the network** on the left and **Registration** on the right.
   The **Page Title** window opens.
5. Below the **Background color** field, click the box to open the color picker.



6. Select a color for your page, and then click **OK**.
7. In the **Page Title** window, click **OK**.
8. On the **Content Editor** tab, expand **Registration**, and then select **Common**.
9. In the **Context Title** field, type `Fortinet Training Registration Page` to change the title.
10. Under **Registration**, select **Login Menu**.
11. In the **Window Title** field, type `Welcome to Fortinet Training`.
12. Scroll down, and then clear the **Game Console Registration Enabled** and **Custom Registration Enabled** checkboxes.

13. In the **Guest Login Title** field, type `Contractor Registration<hr>`.
14. Change the **Guest Login Description** field to `<a href="GuestLoginGCS.jsp">Contractors who have a temporary account.</a>`.
15. Click **Apply**.
16. Log in to the workstation, open Firefox, and then click the **Contractor Registration** bookmark to verify the changes.

    The registration page shows the changes you made on the **Portal Configuration** page.
17. Close the browser, and then log out of the workstation.

Exercise 2: Preparing Devices for Endpoint Isolation

In this exercise, you will configure the infrastructure device models to enable access control enforcement.

Configure the Network Device Model Settings for State-Based Enforcement

State-based enforcement is the process of automatically isolating endpoints based on their assigned state in the FortiNAC database. You will configure several of the devices in the network inventory to enforce state-based isolation of end points.

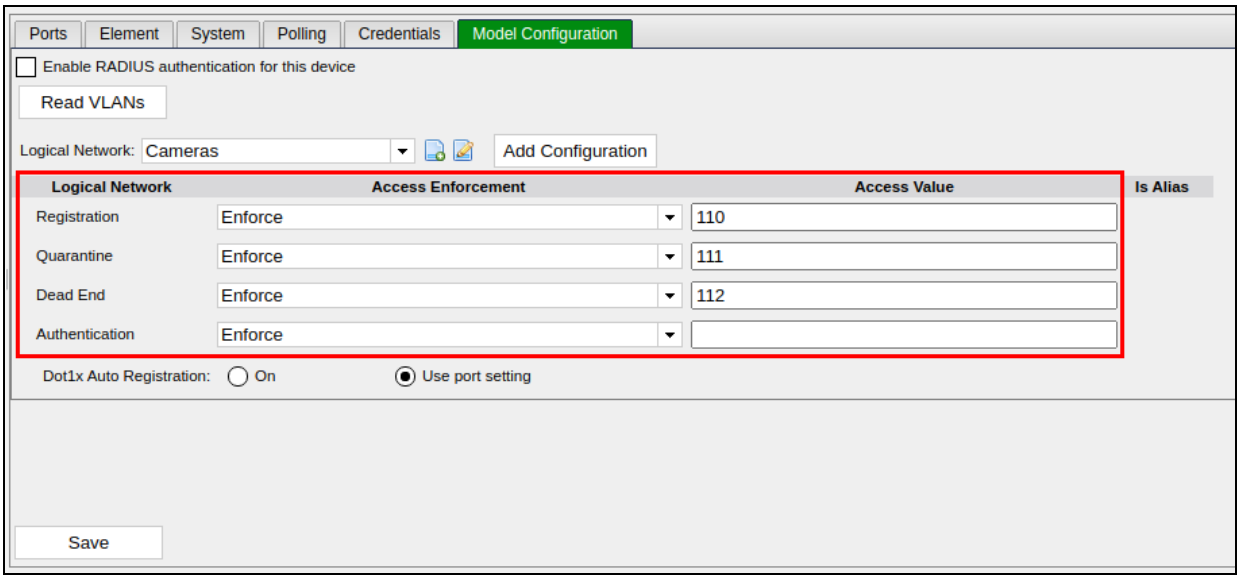
To configure wired device models for access control enforcement using VLAN IDs

1. Log in to the FortiNAC-Primary GUI with the username `admin` and password `password`.
2. Click **Network** > **Inventory**.
3. In the topology tree, expand **Building 1**.
4. Select **Building 1 Switch**, and then click the **Model Configuration** tab.

You can access the model configuration settings on the **Model Configuration** tab, or by right-clicking the device, and then selecting **Model Configuration**.

5. In the **Logical Network** column, in the **Registration** row, in the **Access Enforcement** column drop-down list, select **Enforce**, and then in the **Access Value** field, type `110`.
6. Perform the same steps to configure the following settings:

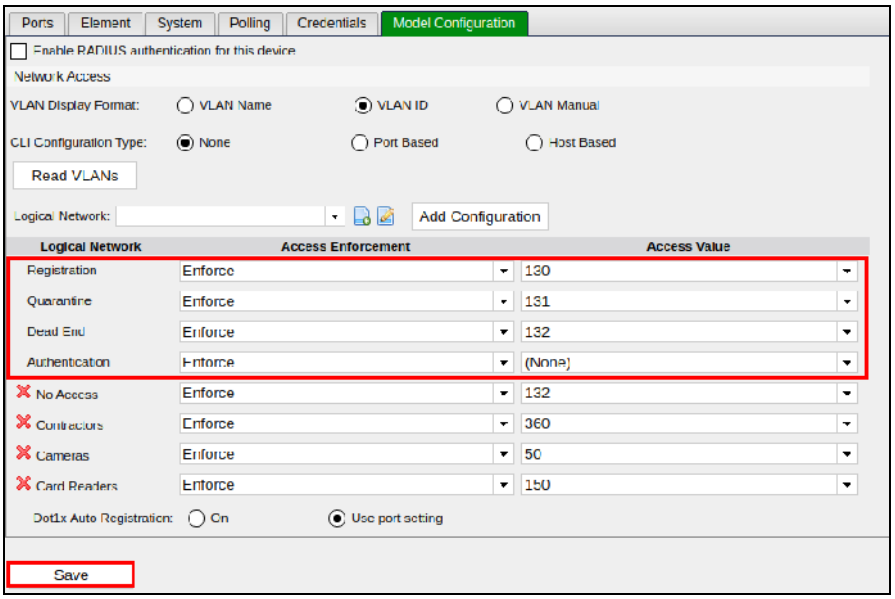
Logical Network	Access Enforcement	Access Value
Quarantine	Enforce	111
Dead End	Enforce	112
Authentication	Enforce	Leave blank



7. Click **Save**.
8. In the topology tree, expand **Building 3**.
9. Select **Switch-3**, and then click the **Model Configuration** tab.
10. In the **Logical Network** column, in the **Registration** row, in the **Access Enforcement** column drop-down list, select **Enforce**, and then in the **Access Value** drop-down list, select **130**.
11. Perform the same steps to configure the following settings:

Logical Network	Access Enforcement	Access Value
Quarantine	Enforce	131
Dead End	Enforce	132
Authentication	Enforce	(None)

12. Click **Save**.



To configure wired device models for access control enforcement using VLAN names

1. In the topology tree, expand **Building 4**.
2. Select **Switch-4**, and then click the **Model Configuration** tab.
3. In the **Network Access** section, in the **VLAN Display Format** row, select **VLAN Name**.
4. In the **Logical Network** column, in the **Registration** row, in the **Access Enforcement** column drop-down list, select **Enforce**, and then in the **Access Value** drop-down list, select **Bldg4-Reg**.
5. Perform the same steps to configure the following settings:

Logical Network	Access Enforcement	Access Value
Quarantine	Enforce	Bldg4-Quar
Dead End	Enforce	Bldg4-DeadEnd
Authentication	Enforce	(None)

6. Click **Save**.
7. In the topology tree, expand **Data Center**.
8. Select **Engineering-Switch**, and then click the **Model Configuration** tab.
9. In the **Network Access** section, in the **VLAN Display Format** row, select **VLAN Name**.
10. In the **Logical Network** column, in the **Registration** row, in the **Access Enforcement** column drop-down list, select **Enforce**, and then in the **Access Value** drop-down list, select **Eng-Reg**.
11. Perform the same steps to configure the following settings:

Logical Network	Access Enforcement	Access Value
Quarantine	Enforce	Eng-Quar
Dead End	Enforce	Eng-DeadEnd
Authentication	Enforce	(None)

12. Click **Save**.

To configure wireless device models for access control enforcement

1. Expand **Wireless APs**, select **Aruba-IAP**, and then click the **Model Configuration** tab.
2. In the **Logical Network** column, in the **Default Wireless** row, in the **Access Value** column drop-down list, select **Production**.
3. In the **Logical Network** column, in the **Registration Wireless** row, in the **Access Enforcement** column drop-down list, select **Enforce**, and then in the **Access Value** drop-down list, select **Registration**.
4. Perform the same steps to configure the following settings:

Logical Network	Access Enforcement	Access Value
Quarantine Wireless	Enforce	Remediation
Dead End Wireless	Enforce	DeadEnd
Authentication Wireless	Bypass	(None)
Roaming Guest	Bypass	(None)

5. Click **Save**.

The access values selected for the Aruba-IAP are Aruba roles that were defined on the AP or controller and learned by FortiNAC.

Exercise 3: Enforcing Access Control

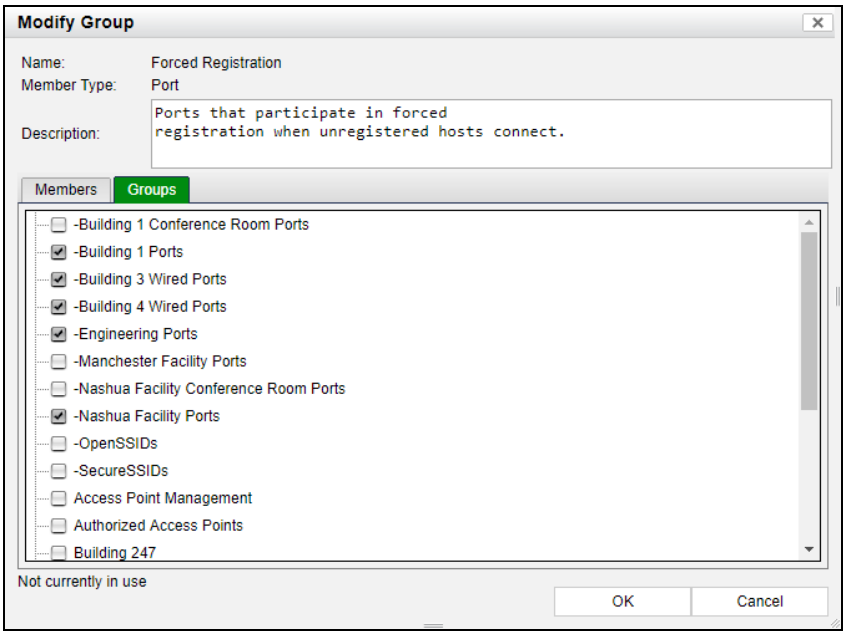
In this exercise, you will turn on the enforcement of access control, which prevents unknown devices from gaining access to the production network in specific locations.

Configure FortiNAC to Enforce State-Based Access Control

Access control is the automated isolation of connecting endpoints, based on the assigned state of each endpoint. You will enable enforcement on physical ports by adding them to enforcement groups.

To enforce access control on rogue hosts in specific locations

1. Log in to the FortiNAC-Primary GUI with the username `admin` and password `password`.
2. Click **System** > **Groups**.
3. Double-click the **Forced Registration** group.
4. In the **Modify Group** window, click the **Groups** tab.
5. Select **-Building 1 Ports**, **-Nashua Facility Ports**, **-Building 3 Wired Ports**, **-Building 4 Wired Ports**, and **-Engineering Ports**.



6. Click **OK**.
   There should now be a **+** to the left of the **Forced Registration** group.
7. Click **+** to expand the group, and then verify that the port groups you added are displayed.
8. Double-click the **Role Based Access** group.
9. In the **Modify Group** window, click the **Groups** tab.
10. Select **-Building 1 Ports** and **-Nashua Facility Ports**.
11. Click **OK**.

The **Forced Registration** group enforces access control on connected hosts that have a system-assigned state or a status of rogue. The **Role Based Access** group enforces network access policies on connected hosts.

To enforce access control on at-risk hosts in specific locations

1. Click **System** > **Groups**.
2. Double-click the **Forced Remediation** group.
3. In the **Modify Group** window, click the **Groups** tab.
4. Select **-Building 1 Ports**, **-Nashua Facility Ports**, **-Building 3 Wired Ports**, and **-Building 4 Wired Ports**.
5. Click **OK**.
   There should now be a **+** to the left of the **Forced Remediation** group.
6. Expand the group, and then verify that the port groups you added are displayed.

Create a Backup of the FortiNAC Database (Optional)

You will back up the FortiNAC database.

To back up the FortiNAC database

1. Click **System** > **Settings**, and then expand the **System Management** folder.
2. Select **Database Backup/Restore**.
3. In the **Schedule Database Backup** section, click **Run Now**.
   A new entry appears in the **Database Restore** field with the current date and timestamp.

Lab 7: Security Policies for Network Access Control and Endpoint Compliance

In this lab, you will create user/host profiles to identify some of the different types of devices (card readers and cameras) and contractor hosts in your lab environment. You will then use these profiles to create network access policies for correct provisioning, and an endpoint compliance policy for host posture checking of contractor systems.

Network access policies are used to automate the network provisioning of endpoints.

Objectives

- Create user/host profiles and network access policies for card readers and cameras
- Create user/host profiles and network access policies for contractors
- Create an endpoint compliance policy for contractors

Time to Complete

Estimated: 30 minutes

Prerequisites

Before you begin this lab, you must complete the previous labs.

Exercise 1: Creating User/Host Profiles and Network Access Policies for Card Readers and Cameras

In this exercise, you will create network access policies for the dynamic provisioning of the connected card readers and cameras, based on the logical networks defined in the model configurations of each device. This is a fundamental part of classification and control capabilities.

Create User/Host Profiles That Identify Card Readers and Cameras

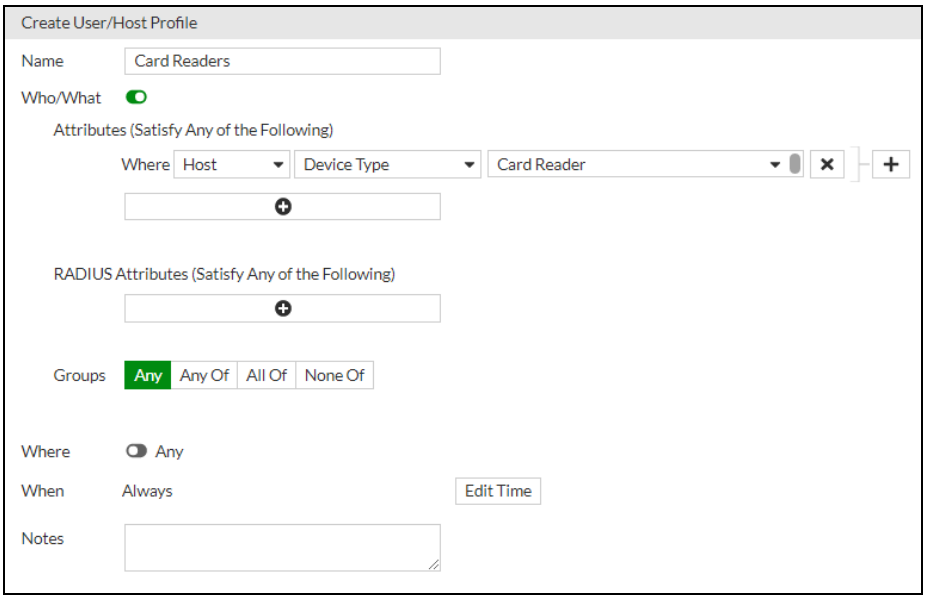
You will create user/host profiles that identify card readers and cameras that are connected to the network.

To create a user/host profile for card readers

1. Log in to the FortiNAC-Primary GUI with the username `admin` and password `password`.
2. Click **Policy & Objects** > **User/Host Profiles**, and then click **Create New**.
3. In the **Create User/Host Profile** window, configure the following settings:

Field	Value
Name	Card Readers
Who/What	Enabled
Attributes	1. Click **+** to add an attribute criteria. 2. In the first drop-down list, select **Host**. 3. In the second drop-down list, in the **Miscellaneous** section, select **Device Type**. 4. In the third drop-down list, select **Card Reader**.
Where	Disabled
When	Always

4. Click **OK**.
   You now have a profile that will match any card reader that connects to the network.



To create a user/host profile for cameras

1. Continuing on the FortiNAC-Primary GUI, click **Policy & Objects** > **User/Host Profiles**, and then click **Create New**.
2. In the **Create User/Host Profile** window, configure the following settings:

Field	Value
Name	Cameras
Who/What	Enabled
Attributes	1. Click **+** to add an attribute criteria. 2. In the first drop-down list, select **Host**. 3. In the second drop-down list, in the **Miscellaneous** section, select **Device Type**. 4. In the third drop-down list, select **Camera**.
Where	Disabled
When	Always

3. Click **OK**.
   You now have a profile that will match any camera.

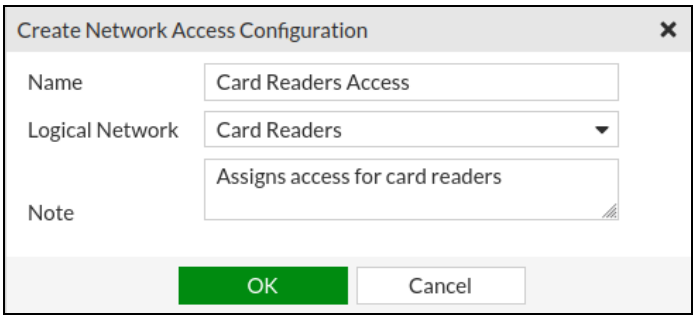
To create a network access policy for card readers

1. Continuing on the FortiNAC-Primary GUI, click **Policy & Objects** > **Network Access**, and then click **Create New**.
2. In the **Create Network Access Policy** window, configure the following settings:

Field	Value
Name	Card Readers Access Policy
Configuration	Select **Create** in the drop-down list.

3. In the **Create Network Access Configuration** window, configure the following settings:

Field	Value
Name	Card Reader Access
Logical Network	Card Readers
Note	Assigns access for card readers



4. Click **OK**.
5. In the **Configuration** field, select **Card Readers Access**.
6. In the **User/Host Profile** field, select **Card Readers**.
7. Click **OK**.
   There is now one network access policy listed.

To create a network access policy for cameras

1. Continuing on the FortiNAC-Primary GUI, click **Policy & Objects** > **Network Access**, and then **Create New**.
2. In the **Create Network Access Policy** window, configure the following settings:

Field	Value
Name	Camera Access Policy
Configuration	Create

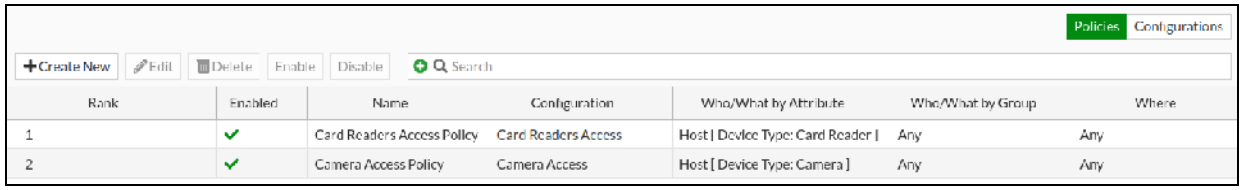
3. In the **Create Network Access Configuration** window, configure the following settings:

Field	Value
Name	Camera Access

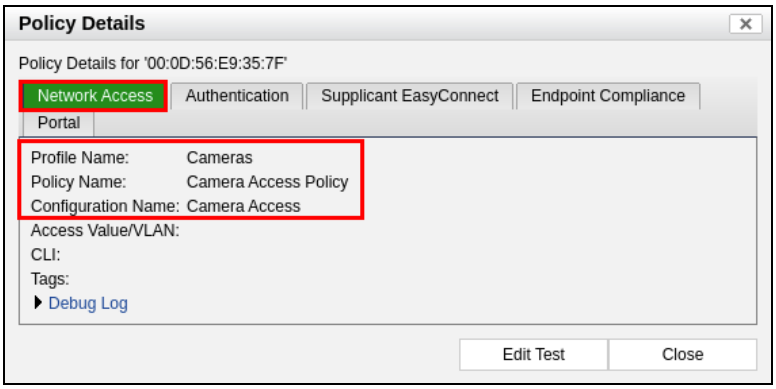
Field	Value
Logical Network	Cameras
Note	Assigns access for cameras

4. Click **OK**.
5. In the **Configuration** field, select **Camera Access**.
6. In the **User/Host Profile** field, select **Cameras**.
7. Click **OK**.

   There are now two network access policies listed.



8. Click **Users & Host** > **Hosts**.
9. Create a private filter to display all card readers or cameras.
10. Right-click individual devices, select **Policy Details**, and then in the **Policy Details** window, verify that the card reader or camera policies are being assigned.



11. Close the **Policy Details** window.

Exercise 2: Creating User/Host Profiles and Network Access Policies for Contractors

In this exercise, you will create user/host profiles that will identify contractors when they are connected to the network. You will then create network access policies for the dynamic provisioning of the contractors.

Create User/Host Profiles That Identify Contractors

You will create the necessary network access policies for the autoprovisioning of contractors.

To create a user/host profile to identify contractors with nonsecure connections

1. Log in to the FortiNAC-Primary GUI with the username `admin` and password `password`.
2. Click **Policy & Objects** > **User/Host Profiles**, and then click **Create New**.
3. In the **Create User/Host Profile** window, configure the following settings:

Field	Value
Name	Contractors - No Access
Who/What	Enabled
Attributes	1. Click **+** to add a criteria. 2. In the first drop-down list, select **Host**. 3. In the second drop-down list, in the **Policy Access** section, select **Role**. 4. In the third drop-down list, select **Contractor**.
Where	Enabled
Locations	1. Click **+** to add locations. 2. In the **Select Entries** pane, select **-Building 1 Conference Room Ports**, **-Nashua Facility Conference Room Ports**, and **-OpenSSIDs**. 3. Click **Close** to close the panel.
When	Always

4. Click **OK**.
   You now have a user/host profile that identifies contractors connected to conference room ports and nonsecure SSIDs.

To create a user/profile to identify contractors with secure connections

1. Continuing on the FortiNAC-Primary GUI, click **Policy & Objects** > **User/Host Profiles**, and then click **Create New**.
2. In the **Create User/Host Profile** window, configure the following settings:

Field	Value
Name	Contractors
Who/What	Enabled
Attributes	1. Click **+** to add a criteria. 2. In the first drop-down list, select **Host**. 3. In the second drop-down list, in the **Policy Access** section, select **Role**. 4. In the third drop-down list, select **Contractor**.
When	Always

3. Click **OK**.
   You now have a user/host profile that identifies all contractors.

To create network access policies to block contractor access

The ranking of policies is very important. The first matched policy is applied to the user or host. In this exercise, you will rank the restrictive policies (no access) higher than the production access policies.

1. Continuing on the FortiNAC-Primary GUI, click **Policy & Objects** > **Network Access**, and then click **Create New**.
2. In the **Create Network Access Policy** window, configure the following settings:

Field	Value
Name	No Contractor Access
Configuration	Create

3. In the **Create Network Access Configuration** window, configure the following settings:

Field	Value
Name	Restricted Access
Logical Network	No Access
Note	Denies network access

4. Click **OK**.
5. In the **Configuration** field, select **Restricted Access**.
6. In the **User/Host Profile** field, select **Contractors - No Access**.
7. Click **OK**.
   There are now three network access policies listed.

To create network access policies to allow contractor access

1. Continuing on the FortiNAC-Primary GUI, click **Policy & Objects** > **Network Access**, and then click **Create New**.
2. In the **Create Network Access Policy** window, configure the following settings:

Field	Value
Name	Contractor Production Access
Configuration	Create

3. In the **Create Network Access Configuration** window, configure the following settings:

Field	Value
Name	Contractor Access
Logical Network	Contractors
Note	Assigns access for contractors

4. Click **OK**.
5. In the **Configuration** field, select **Contractor Access**.
6. In the **User/Host Profile** field, select **Contractors**.
7. Click **OK**.
   There are now four network access policies listed.

Note that you are leveraging the ranking so that any contractor connected to a forbidden location will match policy three (because of the **Where** criteria). All other contractors will match policy four.

To create an endpoint compliance policy for contractors

1. Continuing on the FortiNAC-Primary GUI, click **Policy & Objects** > **Endpoint Compliance**.
2. Make sure the **Policies** tab is selected, and then click **Create New**.
3. In the **Create Endpoint Compliance Policy** window, configure the following settings:

Field	Value
Name	Fortinet Contractor Compliance Policy
Configuration	Create

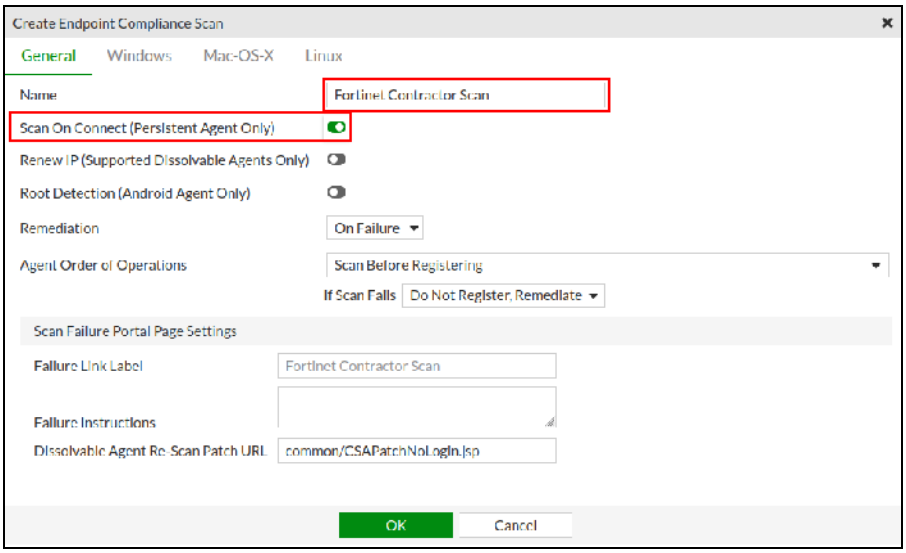
4. Configure the following settings:

Field	Value
Name	Contractor Compliance Configuration
Scan	Create

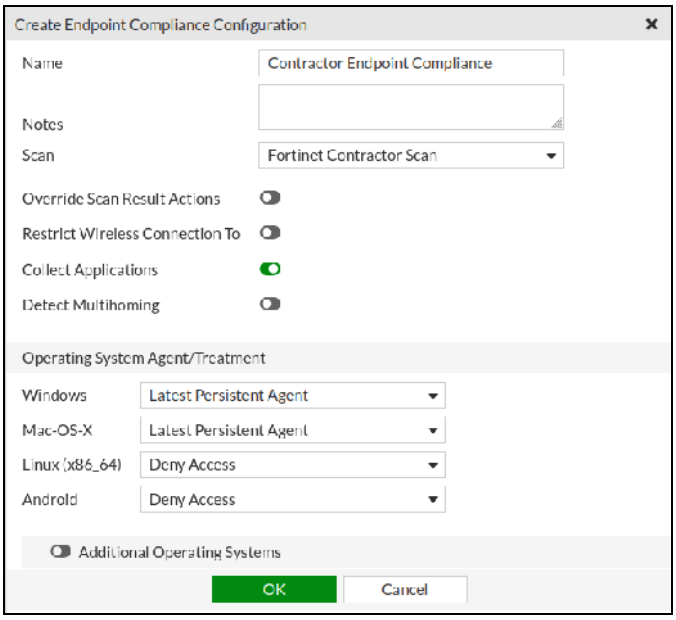
5. Configure the following settings:

Field	Value
Name	Fortinet Contractor Scan
Scan On Connect	Enable the option

6. On the **General** tab, leave the rest of the scan settings at the default values.



7. Click the **Windows** tab.
8. Click the **Antivirus** tab, click **+**, and then select **FortiClient**.
9. Click **Close** to close the antivirus list window.
10. Click the **Operating System** tab, click **+**, and then select the following:
    - **Windows 10**
    - **Windows-10-x64**
11. Click **Close** to close the operating systems list window.
12. Click the **Mac-OS-X** tab.
13. Click the **Antivirus** tab, click **+**, and then select **FortiClient**.
14. Click **Close** to close the antivirus list window.
15. Click the **Operating System** tab, click **+**, and then select the following:
    - **12-Monterey**
    - **13-Ventura**
16. Click **Close** to close the operating systems list window.
17. Click **OK**.
18. In the **Scan** field, select **Fortinet Contractor Scan**.
19. Enable **Collect Applications**.
20. In the **Operating System Agent/Treatment** section, in both the **Windows** and **Mac-OS-X** fields, select **Latest Persistent Agent**.
21. In both the **Linux** and **Android** fields, select **Deny Access**.
22. Click **OK**.



23. In the **Configuration** field, select **Contractor Endpoint Compliance**.
24. In the **User/Host Profile** field, select **Contractors**.
25. Click **OK**.
    There is now one network access policy listed.

Create a Backup of the FortiNAC Database (Optional)

You will back up the FortiNAC database.

To back up the FortiNAC database

1. On the FortiNAC-Primary GUI, click **System** > **Settings**.
2. Expand the **System Management** folder, and then select **Database Backup/Restore**.
3. In the **Database Backup/Restore** section, click **Run Now**.
   A new entry appears in the **Database Restore** field with the current date and timestamp.

Lab 8: Guest and Contractor Services Configuration

In this lab, you will create a contractor template to define the capabilities of your contractors. Next, you will create an administrative profile and administrative user to act as your guest/contractor manager. Next, acting as the guest/contractor manager, you will create a contractor account. Next, you will register the Linux machine in the lab to the contractor. Finally, you will create a firewall policy leveraging FortiNAC tags.

Objectives

- Create a contractor template, administrative profile, and administrative user for contractor management
- Create and test a contractor account
- Create a firewall policy using FortiNAC tags

Time to Complete

Estimated: 30 minutes

Prerequisites

Before you begin this lab, you must complete the previous labs.

Exercise 1: Creating a Contractor Template

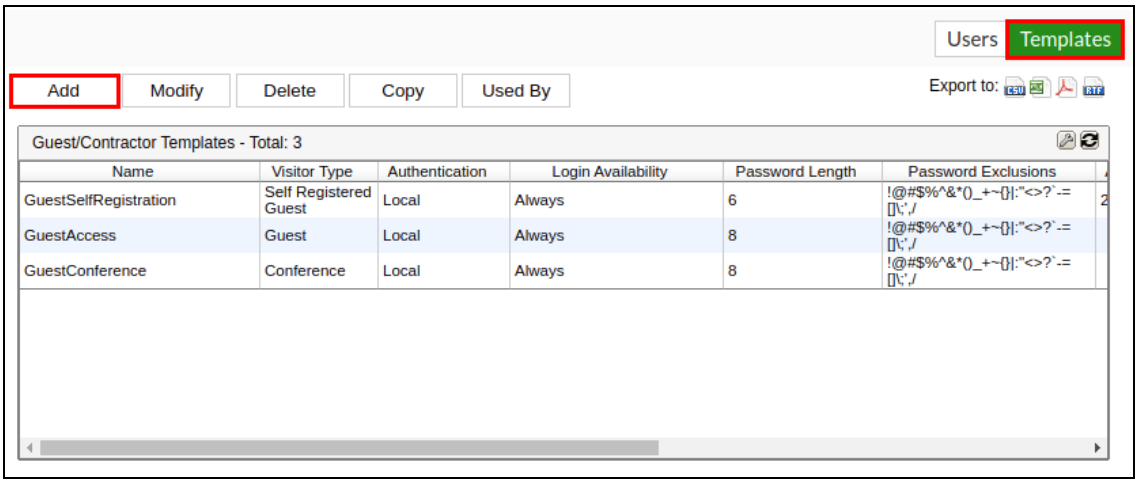
In this exercise, you will create a contractor template that defines the attributes of all accounts that are built from this template. You will then create an administrator profile that will grant an administrative user the ability to create and manage contractor accounts.

Create a Contractor Template and an Administrative Sponsor

Guest and contractor templates define the characteristics of the accounts that are created from them. You can create administrative sponsors for the delegation of contractor management.

To create a guest/contractor template

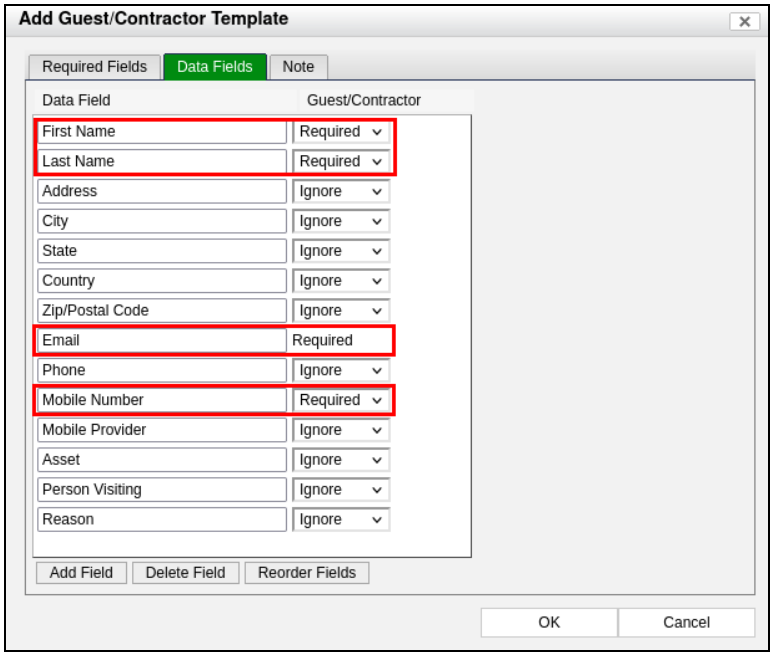
1. Log in to the FortiNAC-Primary GUI with the username `admin` and password `password`.
2. Click **Users & Hosts** > **Guests & Contractors**.
3. Select **Templates**, and then click **Add**.



4. In the **Add Guest/Contractor Template** window, configure the following settings:

Field	Value
Template Name	Fortinet Contractor
Visitor Type	Contractor
Role	Click **Select Role**, and then select **Contractor**.
Password Length	5
Account Duration	Select the checkbox, and then type `744`.

5. Leave the remaining settings at the default values, and then click the **Data Fields** tab.
6. On the **Data Fields** tab, leave the **First Name**, **Last Name**, **Email**, and **Mobile Number** fields set to **Required**, and then set all other fields to **Ignore**.



7. Click **OK**.

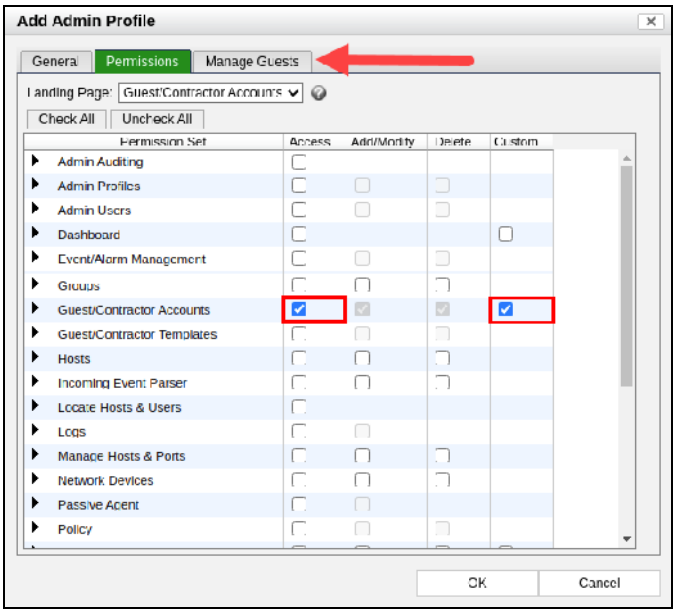
To create an administrative profile for guest and contractor management

1. Continuing on the FortiNAC-Primary GUI, click **Users & Hosts** > **Administrators**, and then select **Profiles**.
2. Click **Add** to create a new administrative profile.
3. Configure the following settings:

Field	Value
Name	Guest and Contractor Manager
Login Availability	Always
Log Out After	20
Manage Hosts and Ports	All
Note	Profile for management of contractor accounts

4. Select the **Associated users do not expire** checkbox, and then leave all other settings at the default values.
5. Click the **Permissions** tab.
6. In the row for the **Guest/Contractor Accounts** permissions set, select the checkboxes in the **Access** and **Custom** columns.

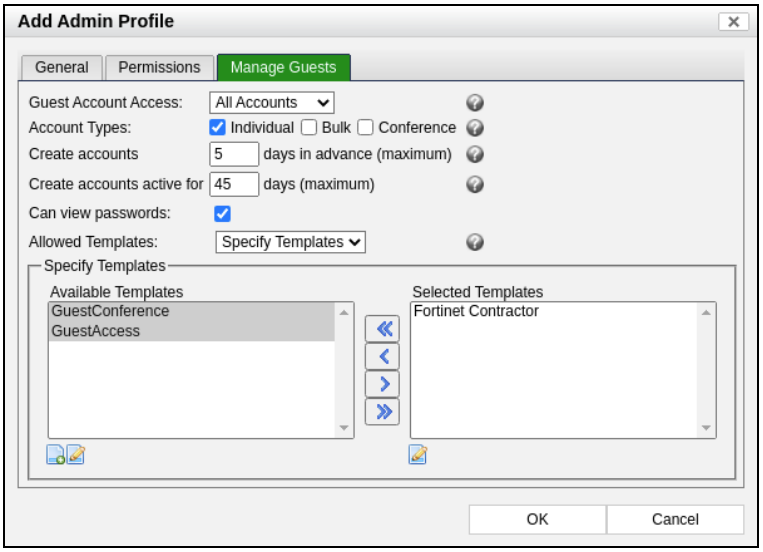
   When you select the checkbox in the **Custom** column, a new **Manage Guests** tab appears.



7. Click the **Manage Guests** tab.
8. Configure the following settings:

Field	Value
Guest Account Access	All Accounts
Account Types	Individual
Create accounts	5
Create accounts active for	45
Allowed Templates	Specify Templates

9. In the **Selected Templates** field, remove all templates except **Fortinet Contractor**.



10. Click **OK**.

To create an administrative user for guest and contractor management

1. Continuing on the FortiNAC-Primary GUI, click **Users & Hosts** > **Administrators**.
2. Select **Users**, and then click **Add** to create a new administrator.
3. In the **User ID** field, type `Larry`, and then click **OK**.
4. In the **Add User** window, configure the following settings:

Field	Value
Authentication Type	Local
Admin Profile	Guest and Contractor Manager
Password	password
Last Name	Smith

5. Click **OK**.

Exercise 2: Creating and Testing a Contractor Account

In this exercise, you will create a contractor account using the template from the previous exercise. You will then register the workstation system as a contractor machine.

Create and Validate a Contractor Account

Contractor accounts are used to grant the required access to a contractor.

You will create a contractor template and an administrative sponsor to manage the contractors. You will then access the system as the sponsor, to create and validate the account.

To create a Fortinet contractor

1. Log out of the FortiNAC-Primary GUI, and then close the browser.
2. Log back in to the FortiNAC-Primary GUI with the username `Larry` and password `password`.
3. Accept the **End User License Agreement**, and then click **OK**.
4. Click **Users & Hosts** > **Guests & Contractors**.
5. Click **Add** to create a new contractor account, and then configure the following settings:

Field	Value
Template	Fortinet Contractor
Email	joe.contractor@fortinet.com
Password	(Note the auto-generated password to use later.)
Account Start Date	(Set the date to today.)
Account End Date	(Set the date to one week from now.)
First Name	Joe
Last Name	Contractor
Mobile Phone	555-0152

Notice that the only available option in the **Template** field is **Fortinet Contractor**. This is because it is the only template that you made available in Larry's administrative profile.

6. Click **OK**.
   The **View Accounts** window opens.
7. Click **Close**.

To register a host as a Fortinet contractor and verify the policy

1. Log in to the workstation GUI with the username `student` and password `password`.
2. Open Firefox.
3. In the **Bookmarks** menu, click **Hacker Site**.
   The website should load correctly.
4. In the **Bookmarks** menu, click **Contractor Registration**.
5. On the **Registration** page, select the **Contractor Registration** login option.
6. Use the credentials from the contractor account you created, and register your lab system.

Create an IPv4 Policy That Uses Dynamic Group Memberships and a Test Policy

You will configure a policy that relies partly on membership in the dynamic address group, which FortiNAC updates dynamically, based on a security policy.

To create an IPv4 policy on FortiGate

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

Field	Value
Name	Contractor Internet Access
Incoming Interface	port3
Outgoing Interface	port1
Source	FNVMCATM21000728_Contractor-Tag (in the **Address** tab)
Destination	all
Schedule	always
Service	ALL
Action	ACCEPT
Inspection-Mode	Proxy-based
NAT	(Enable this option.)
AntiVirus	Enable this option, and then select **Eicar Virus**.
Web Filter	Enable this option, and then select **Contractor Web Filter**.
SSL Inspection	deep-inspection

Field	Value
Log Allowed Traffic	Enable this option, and then select **Security Events**.
Enable this policy	(Enable this option.)

4. Keep the default values for all other settings, and then click **OK** to save the changes.
5. In the **Name** column, drag and drop the **Contractor Internet Access** policy under the **Generate Security Alert** policy to rank it as second for this interface pair.
6. Log out of the FortiGate GUI.

This policy was created here to demonstrate how the **Contractors** group, whose membership is determined by the FortiNAC firewall tag, can be associated with an IPv4 policy. You will see the results of this policy in a future lab.

To test the contractor policy

1. Log in to the workstation GUI with the username `student` and password `password`.
2. Open Firefox.
3. In the **Bookmarks** menu, click **Hacker Site**.
   You should receive a **Web Page Blocked!** message.

The web page is blocked by the FortiGate IPv4 policy that you created in previous steps. The endpoint is now a member of the **Contractors-Tags** address group on FortiGate because of the firewall tag and network access policy configured on FortiNAC.

Create a Backup of the FortiNAC Database (Optional)

You will back up the FortiNAC database.

To back up the FortiNAC database

1. On the FortiNAC-Primary GUI, click **System** > **Settings**.
2. Expand the **System Management** folder, and then select **Database Backup/Restore**.
3. In the **Database Backup/Restore** section, click **Run Now**.
   A new entry appears in the **Database Restore** field with the current date and timestamp.

Lab 9: FortiNAC Integrations

In this lab, you will perform the necessary configurations to integrate a security device capable of issuing SNMP traps with FortiNAC. Then, you will model the device as a pingable device, so that FortiNAC will accept the traps from the device. Next, you will perform the same procedures for a security device that issues syslog messages. Finally, you will set up help desk notifications that will be sent when the alarm is triggered.

Objectives

- Configure an integration with a device that issues SNMP traps
- Configure an integration with a device that issues syslog messages
- Configure notifications for alarms
- Configure FortiNAC to process FortiGate syslog messages
- Create security rules for automated threat response
- Create a custom security event parser
- Validate integrations

Time to Complete

Estimated: 60 minutes

Prerequisites

Before you begin this lab, you must complete the previous labs.

Exercise 1: Creating an Integration Using SNMP Trap Input

In this exercise, you will create an integration with a third-party device, using SNMP traps as input sent to FortiNAC.

Create a Third-Party Integration Using SNMP Traps

Integration with third-party systems allows for the creation of events, alarms, and the automated execution of actions.

You will create a custom trap configuration for a security device, and then add a device to the inventory.

To create an integration with devices using SNMP traps

1. Log in to the FortiNAC-Primary GUI with the username `admin` and password `password`.
2. Click **System** > **Settings** > **System Communication**, and then select **Trap MIB Files**.
3. At the top of the page, click **Add MIB**, and then configure the following settings:

Field	Value
MIB File Name	TrainingTrap
Label	Content Violation Event
Specific Type	23
Enterprise OID	1.3.6.1.4.1.1826
IP Address OID	1.3.6.1.4.1.1826.1.0.0.5
MAC Address OID	(Leave this field empty.)
User ID OID	(Leave this field empty.)
Alarm Cause	Possible Violation of Web Content Rules
Event Format (Java Message API)	Event caused by device with IP: {5}

4. Click **OK**.
5. Click **Network** > **Inventory**.
6. Right-click **Security Devices**, and then select **Add Pingable Device**.
7. On the **Element** tab, configure the following settings:

Field	Value
Add to Container	Security Devices
Name	Guardian IPS
IP Address	10.10.5.75
Physical Address	00:50:8B:EE:0E:7A
Device Type	IPS/IDS
Incoming Events	Not Applicable
SSO Agent	Not Applicable
Role	NAC-Default
Description	Guardian is an inline security device
Note	John Doe manages this device

8. Click the **Details** tab, and then configure the following settings:

Field	Value
Machine Name	Guardian
Department	IT Security
Owner	John Doe

9. Leave all other fields empty, and then click **OK**.

Exercise 2: Creating an Integration Using syslog Input

In this exercise, you will create an integration with a third-party device, using syslog messages as input sent to FortiNAC.

Create a Third-Party Integration Using Incoming syslog Information

Integration with third-party systems allows for the creation of events, alarms, and the automated execution of actions.

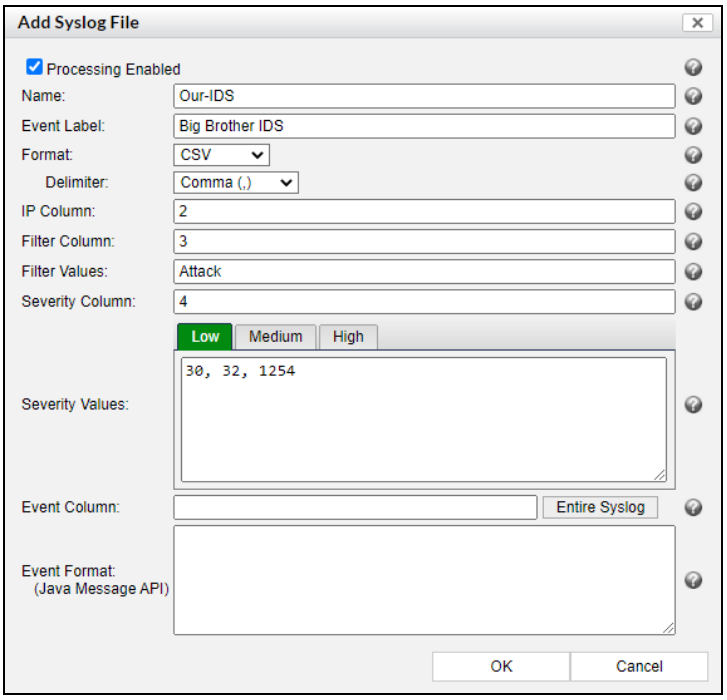
You will integrate with a security device by creating a custom syslog parser for that device, and then test the integration by validating event and alarm creation.

To create an integration using syslog messages as input

1. Log in to the FortiNAC-Primary GUI with the username `admin` and password `password`.
2. Click **System** > **Settings** > **System Communication** > **Syslog Files**.
3. Click **Add**, and then configure the following settings:

Field	Value
Processing Enabled	(Select the checkbox.)
Name	Our-IDS
Event Label	Big Brother IDS
Format	CSV Delimiter: Comma (,)
IP Column	2
Filter Column	3
Filter Values	Attack
Severity Column	4
Low Severity Values	30, 32, 1254
Medium Severity Values	40, 46
High Severity Values	50, 62

4. Click **OK**.



5. Click **Network** > **Inventory**, right-click **Security Devices**, and then click **Add Pingable Device**.
6. On the **Element** tab, configure the following settings:

Field	Value
Add to Container	Security Devices
Name	Big Brother IDS
IP Address	10.10.4.55
Physical Address	00:50:56:B8:45:28
Device Type	IPS/IDS
Incoming Events	Syslog In the drop-down list, click **Big Brother IDS**.
SSO Agent	Not Applicable
Role	NAC-Default
Description	Big Brother is an inline security device
Note	John Doe manages this device

7. On the **Details** tab, configure the following settings:

Field	Value
Machine Name	Big Brother
Department	IT Security
Owner	John Doe

8. Leave all other fields empty, and then click **OK**.

Exercise 3: Creating an Administrative Group for Alarm Notification

In this exercise, you will configure an alarm to automatically notify an administrative user group when that alarm is generated.

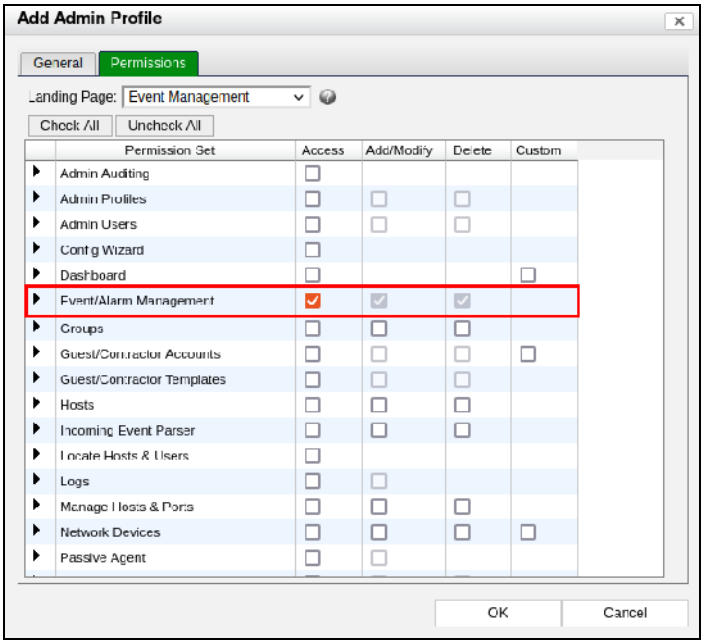
Create an Administrative Group for the Automated Notification of Alarms

Alarm information can be automatically passed to members of administrative groups, in the form of email or SMS messages.

You will create an administrative group to represent the help desk users. Then, you will use this group for notifications when the alarm is generated.

To create a help desk user and group

1. Log in to the FortiNAC-Primary GUI with the username `admin` and password `password`.
2. Click **Users & Hosts** > **Administrators**, and then click the **Profiles** tab.
3. Click **Add** to create a new admin profile.
4. In the **Name** field, type `Helpdesk Level 1`.
5. On the **General** tab, keep the default values for all settings.
6. On the **Permissions** tab, select the **Access** checkbox for the **Event/Alarm Management** permission set.
7. Click **OK**.



8. Click the **Users** tab, and then click **Add** to create a new administrative user.
9. In the **User ID** field, type `dgray`, and then click **OK**.
   The **Add User** window opens.
10. In the **Add User** window, configure the following settings:

Field	Value
Admin Profile	Helpdesk Level 1
Password	password
Last Name	Gray
Email	dgray@fortinet.com

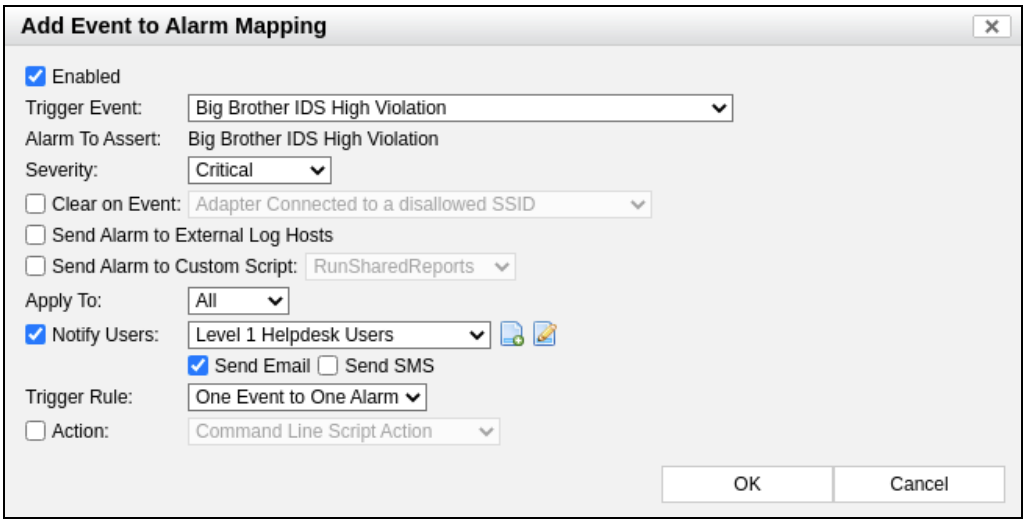
11. Click **OK**.
12. Click **System** > **Groups**.
13. Click **Add** to create a new group.
14. In the **Name** field, type `Level 1 Helpdesk Users`.
15. In the **Member Type** field, select **Administrator**.
16. Move **Gray, (dgray)** to the **Selected Members** list.
17. Click **OK**.

To configure an alarm notification

1. Click **Logs** > **Events & Alarms**, and then click the **Mappings** tab.
2. Click **Add** to create a new mapping, and then configure the following settings:

Field	Value
Trigger Event	Select **Big Brother IDS High Violation**.
Severity	Critical
Notify Users	Select the checkbox, and then select **Level 1 Helpdesk Users**.
Send Email	(Select the checkbox.)

3. Leave all other settings at the default values, and then click **OK**.



The new mapping is highlighted on the page. Note that **Level 1 Helpdesk Users** is in the **Notify Users** column.

Exercise 4: Configuring FortiNAC to Process FortiGate syslog Messages for Automated Response

In this exercise, you will configure FortiNAC to parse syslog input from FortiGate.

Configure FortiNAC to Process FortiGate syslog Messages

To process syslog messages from FortiGate, FortiNAC must be configured to use the appropriate syslog message parser. You will define the syslog message parser that FortiNAC uses when it processes syslog messages that FortiGate sends.

To configure FortiNAC to process FortiGate syslog messages

1. Log in to the FortiNAC-Primary GUI with the username `admin` and password `password`.
2. Click **Network** > **Inventory**, and then expand **Security Devices**.
3. Select **FortiGate-Edge**, and then click the **Element** tab.
4. To the right of **Incoming Events**, select **Security Events**.
   A new drop-down menu appears.
5. Select **FortiOS5**.
   This configures how FortiNAC parses incoming security event (syslog) messages from this device (FortiGate-Edge).
6. Click **Save**.

The selected parser is named **FortiOS5**, but it will parse the current FortiOS security events because the format has not changed.

Exercise 5: Creating Security Rules for Automated Threat Response

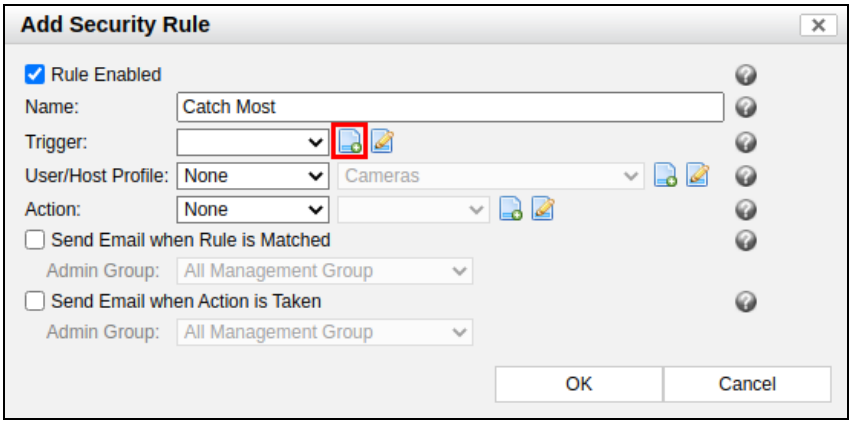
In this exercise, you will examine how to create security rules that will trigger based on input from external security devices. These security rules are the key to automated responses and threat mitigation.

Create Security Rules

You will build a series of security rules, beginning with a very general rule (a catch most rule) and then more detailed rules, using security events generated from the initial rule.

To create a security rule

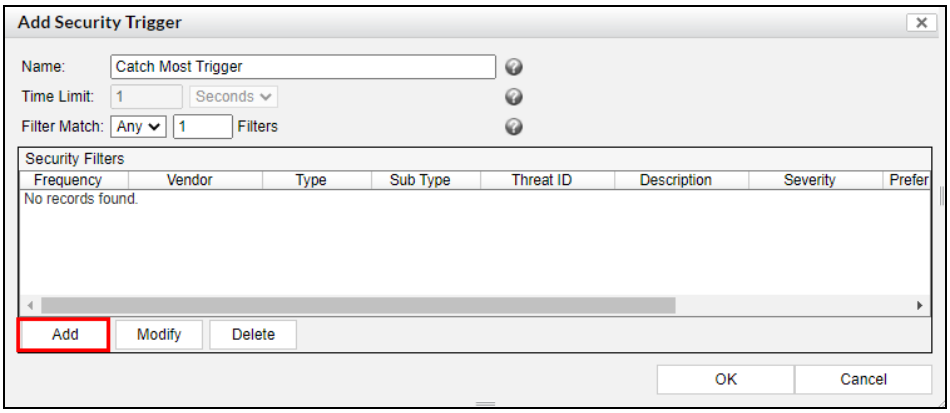
1. Log in to the FortiNAC-Primary GUI with the username `admin` and password `password`.
2. Click **Logs** > **Security Incidents**.
3. Click the **Rules** tab.
4. Click **Add** to create a new security rule.
5. Make sure the **Rule Enabled** checkbox is selected.
6. In the **Name** field, type `Catch Most`.
7. Click the **Add Security Trigger** icon to create a new security trigger.



8. In the **Add Security Trigger** window, configure the following settings:

Field	Value
Name	Catch Most Trigger
Time Limit	1
Filter Match	Any 1

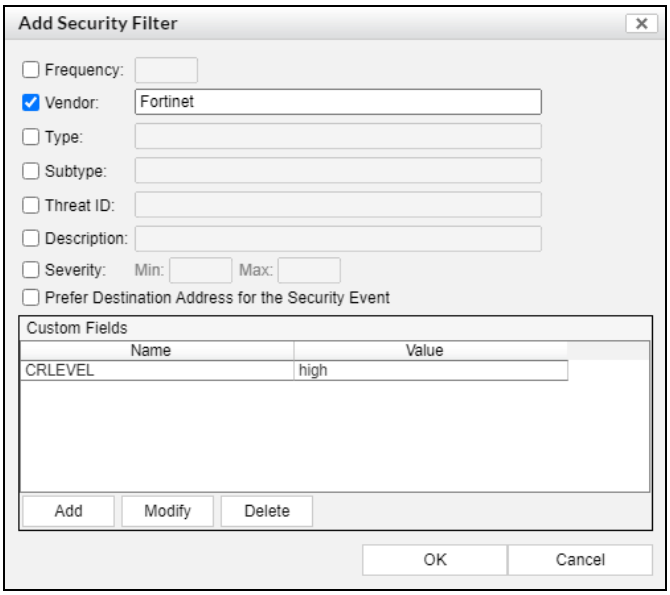
9. In the **Security Filters** section, click **Add** to create a new security filter.



10. Select **Vendor**, and then type `Fortinet`.
11. In the **Custom Fields** section, click **Add**, and then configure the following settings:

Field	Value
Name	CRLEVEL
Value	high

12. Click **OK**.



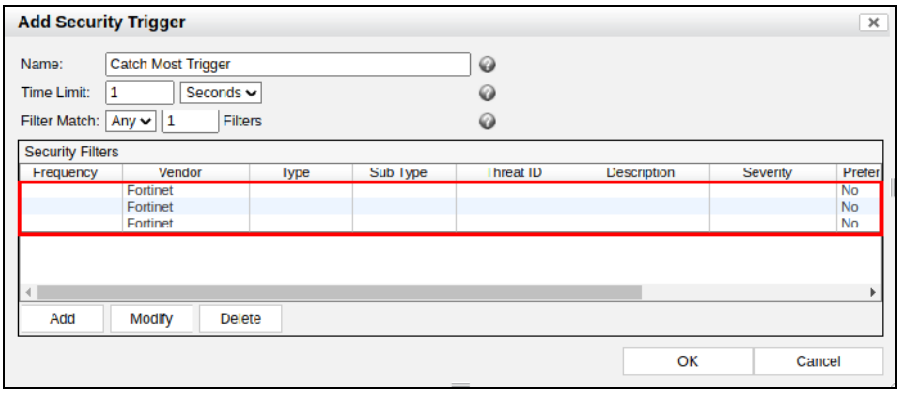
13. In the **Add Security Filter** window, click **OK**.
    The security trigger now has one security filter.
14. Click **Add** to create a second security filter.
15. Select **Vendor**, and then type `Fortinet`.
16. In the **Custom Fields** section, click **Add**, and then configure the following settings:

Field	Value
Name	CRLEVEL
Value	critical

17. In the **Add Field** window, click **OK**.
18. In the **Add Security Filter** window, click **OK**.
19. Click **Add** to create a third security filter.
20. Select **Vendor**, and then type `Fortinet`.
21. In the **Custom Fields** section, click **Add**, and then configure the following settings:

Field	Value
Name	LEVEL
Value	warning

22. In the **Add Field** window, click **OK**.
23. In the **Add Security Filter** window, click **OK**.
24. In the **Add Security Trigger** window, click **OK**.



25. In the **Add Security Rule** window, leave the **User/Host Profile** set to **None**.
26. In the **Action** field, select **Automatic**.
27. Click the **Add Security Action** icon to create a new security action, and then configure the following settings:

Field	Value
Name	Log to SIEM
On Activity Failure	Continue Running Activities

28. Ensure that the **Perform Secondary Task(s)** checkbox is cleared.
29. In the **Activities** section, click **Add** to add a new activity.
30. In the **Activity** field, select **Send Alarm to External Log Hosts**, and then click **OK**.
31. In both the **Add Security Action** and **Add Security Rule** windows, click **OK**.
    You now have one security rule named **Catch Most**.

32. On the workstation client machine, open Firefox.
33. Click the **News** bookmark.
    You should receive a **Web Page Blocked** message.
34. Click the **AV Test** bookmark.
    You should receive a **High Security Alert!** message.
35. Click the **SecurityRisk** bookmark, let it try to load for a couple of seconds, and then click **X** to stop trying to load the page.
36. Return to the FortiNAC-Primary GUI.

Configure a Denied Category Web Filter Rule

You will create a security rule from a security event that the initial **Catch Most** security rule generated.

To build a security rule from an existing security event

1. Click **Logs** > **Security Incidents**, and then click the **Events** tab.
2. In the **Filter** section, click **Update**.
   Security events should populate the view.
3. Right-click the event with **Alert Type = utm** and **Subtype = webfilter**.
4. Click **View Details**, and then scroll through the **Event Details** to see all the information that the alert that FortiGate sent contains.
5. Leave the **Event Details** window open, right-click the same event again, and then this time, select **Create Event Rule**.
6. In the **Create Event Rule** window, in the **Available Fields** section, select the following fields, and then click **>** to move them to the **Selected Fields** section:
   - **Alert Type**
   - **Subtype**
   - **PROFILE**
   - **MSG**
   - **CATDESC**
7. Click **OK**.
   The **Add Security Trigger** window opens with a security filter already created based on the fields that you selected.
8. In the **Add Security Trigger** window, configure the following settings:

Field	Value
Name	Denied Category Trigger
Time Limit	1
Filter Match	Any 1

9. Click **OK**.

The **Add Security Rule** window appears.

10. Configure the security rule with the following settings:

Field	Value
Name	Denied Category Web Filter Matched by Contractor

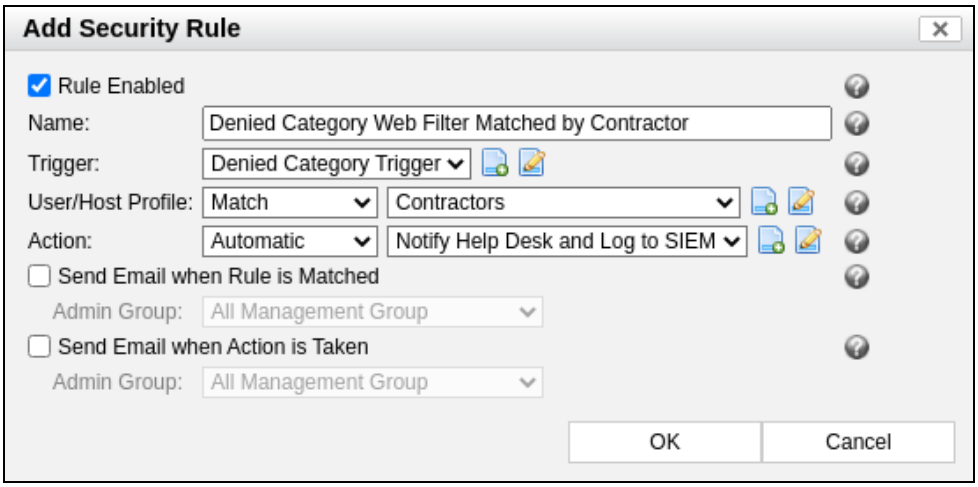
11. In the **User/Host Profile** field, select **Match**, and then in the second drop-down list, select **Contractors**.
12. In the **Action** field, select **Automatic**.
13. Click the **Add Security Action** icon to add a new security action, and then configure the following settings:

Field	Value
Name	Notify Help Desk and Log to SIEM
On Activity Failure	Continue Running Activities

14. Do not select the **Perform Secondary Task(s)** checkbox.
15. In the **Activities** section of the **Add Security Action** window, click **Add** to add a new activity.
16. In the **Activity** field, select **Send Alarm to External Log Host**, and then click **OK**.
17. Click **Add** a second time, and then in the **Activity** field, select **Email Group Action**.
18. Configure the following **Security Activity** settings:

Field	Value
Group	HelpDesk
Message	A contractor has attempted to access a denied website. Details were sent to SIEM.

19. In the **Add Security Activity** window, click **OK**.
20. In the **Add Security Action** window, click **OK**.
21. Ensure that the **Send Email when Rule is Matched** and **Send Email when Action is Taken** checkboxes are cleared.
22. Click **OK**.



23. Close the **Event Details** window.
24. Click the **Rules** tab.

    You will see two security rules listed: **Catch Most** and **Denied Category Web Filter Matched by Contractor**.

Configure a Virus Infected File (EICAR Test File) Rule

You will create a third security rule from a security event that the initial **Catch Most** security rule generated.

To build a security rule from an existing security event

1. Click the **Events** tab.
2. Right-click the event with **Alert Type** = **utm** and **Subtype** = **virus**.
3. Select **View Details**, and then scroll through **Event Details** to see all the information that the alert that FortiGate sent contains.
4. Leave the **Event Details** window open, and then right-click the same event again.
5. Select **Create Event Rule**.
6. In the **Create Event Rule** window, in the **Available Fields** section, select the following fields, and then click **>** to move them to the **Selected Fields** section:
   - **Alert Type**
   - **Subtype**
   - **PROFILE**
   - **DTYPE**
7. Click **OK**.

   The **Add Security Trigger** window opens with a security filter already created based on the fields that you selected.
8. In the **Name** field, type `Virus Infected File`.
9. Leave the **Time Limit** and **Filter Match** as they are, and then click **OK**.
10. Configure the following settings:

Field	Value
Name	Virus Infected File Detected-Contractor

11. In the **User/Host Profile** field, select **Match**, and then in the second drop-down list, select **Contractors**.
12. In the **Action** field, select **Automatic**.
13. Click the **Add Security Action** icon, and then configure a new security action with the following settings:

Field	Value
Name	Notify Help Desk, SOC, and Log to SIEM
On Activity Failure	Continue Running Activities

14. Ensure that the **Perform Secondary Task(s)** checkbox is cleared.
15. In the **Activities** section, click **Add**, and then in the **Activity** field, select **Send Alarm to External Log Hosts**.
16. Click **OK**.
17. Click **Add**, in the **Activity** field, select **Email Group Action**, and then configure the following settings:

Field	Value
Group	SOC
Message	A contractor has attempted to download a file containing a virus. Details have been sent to SIEM.

18. Click **OK**.
19. Click **Add**, in the **Activity** field, select **Email Group Action**, and then configure the following settings:

Field	Value
Group	HelpDesk
Message	A contractor has attempted to download a file containing a virus. Details have been sent to the SOC and SIEM.

20. In the **Add Security Action** window, click **OK**.
21. Ensure that the **Send Email when Rule is Matched** and **Send Email when Action is Taken** checkboxes are cleared.
22. Click **OK**.
23. Close the **Event Details** window.
24. Click the **Rules** tab.

    You should see three security rules listed: **Catch Most**, **Denied Category Web Filter Matched by Contractor**, and **Virus Infected File Detected-Contractor**.

Configure a General Security Risk Rule

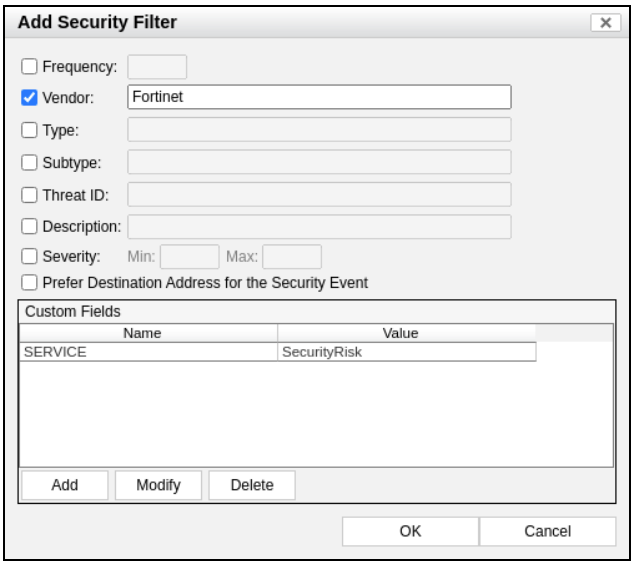
You will build a security rule, that is more specific than the **Catch Most** rule, without using an existing security event.

To manually build a security rule without an existing security event

1. Click **Logs** > **Security Incidents**, and then click the **Rules** tab.
2. Click **Add** to create a new security rule.
3. Ensure that the **Rule Enabled** checkbox is selected, and then name the new security rule `General Security Risk`.
4. To the right of the **Trigger** field, click the **Add Security Trigger** icon to create a new security trigger.
5. Name the security trigger `General Security Risk Trigger`.
6. Leave the **Time Limit** set to **1 second** and the **Filter Match** set to **All**.
7. In the **Security Filters** section, click **Add** to add a new security filter.
8. Select **Vendor**, and then type `Fortinet`.
9. In the **Custom Fields** section, click **Add**, and then configure the following settings:

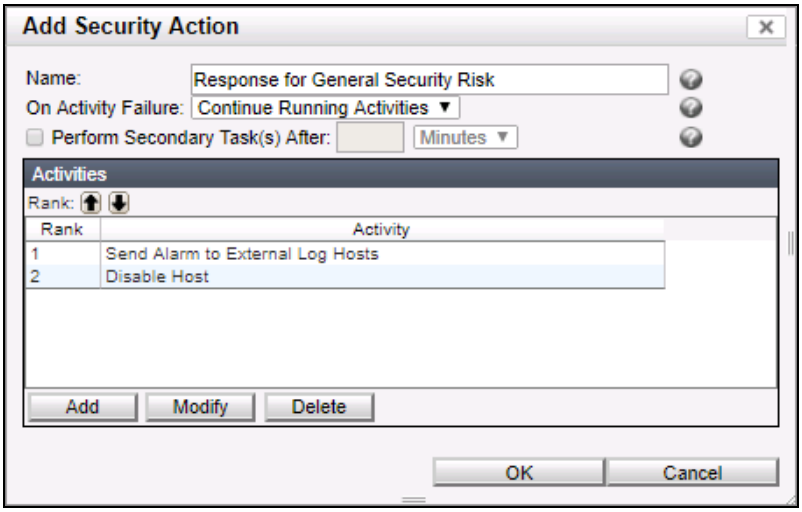
Field	Value
Name	SERVICE
Value	SecurityRisk

10. Click **OK**.

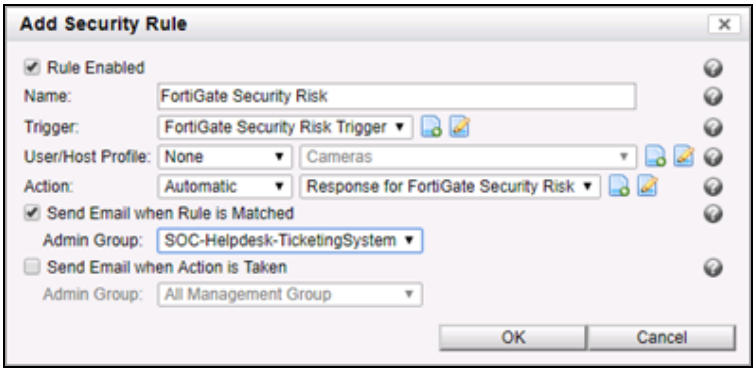


11. In the **Add Security Filter** window, click **OK**.
12. In the **Add Security Trigger** window, click **OK**.
13. Leave the **User/Host Profile** field set to **None**, and then set the **Action** field to **Automatic**.
14. Click the **Add Security Action** icon to create a new action.
15. Name the new security action `Response for General Security Risk`.

16. Leave the **On Activity Failure** field set to **Continue Running Activities** and the **Perform Secondary Task(s) After** checkbox cleared.
17. In the **Activities** section, click **Add** to add a new activity.
18. In the **Activity** field, select **Send Alarm to External Log Hosts**, and then click **OK**.
19. Click **Add** to add a second activity, and then select **Disable Host**.
20. Leave the **Secondary Task** checkbox cleared, and then click **OK**.



21. In the **Add Security Action** window, click **OK**.
22. Select the **Send Email when Rule is Matched** checkbox.
23. In the **Admin Group** field, select **SOC-Helpdesk-TicketingSystem** (this is an administratively created group of administrative users who will be notified).
24. Click **OK**.



Exercise 6: Creating a Custom Security Event Parser

In this exercise, you will create a security event parser for integration with third-party devices that do not have an out-of-the-box parser.

Create a Customized Security Event Parser

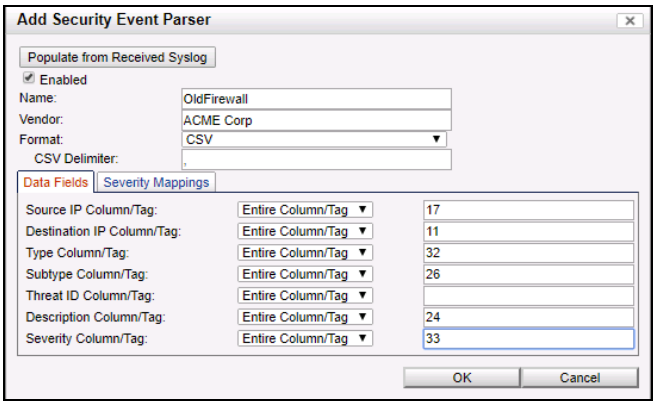
Customized security event parsers allow for integration with nearly any type of security device.

You will integrate with a new type of security device, generate security events and alarms, and see the execution of an automated work flow.

To use the event parsers tool to integrate with a firewall

1. Log in to the FortiNAC-Primary GUI with the username `admin` and password `password`.
2. Click **System** > **Settings**.
3. Open the **System Communication** folder, and then select **Security Event Parsers**.
4. Click **Add** to create a new event parser.
5. In the **Add Security Event Parser** window, configure the following settings:

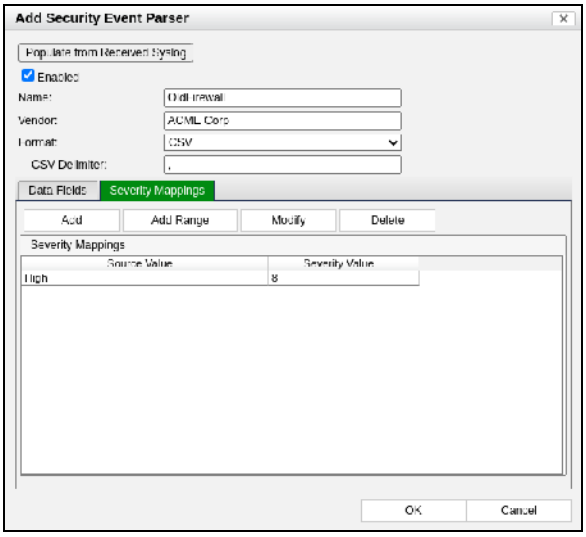
Field	Value
Enabled	(Select the checkbox.)
Name	OldFirewall
Vendor	ACME Corp
Format	CSV In the **CSV Delimiter** field, type , (a comma).
Source IP Column/Tag	17
Destination IP Column/Tag	11
Type Column/Tag	32
Subtype Column/Tag	26
Threat ID Column/Tag	(Leave this field empty.)
Description Column/Tag	24
Severity Column/Tag	33



6. Click the **Severity Mappings** tab.
7. Click **Add**, and then configure the following settings:

Field	Value
Source Value	High
Severity Value	8

8. Click **OK**.



9. Click **OK** to complete the creation of the new syslog event parser.

To model and integrate with the old firewall in the topology view

1. Click **Network** > **Inventory**.
2. Right-click **Security Devices**, and then select **Add Pingable Device**.
3. In the **Add Pingable Device** window, configure the following settings:

Field	Value
Add to Container	Security Devices
Name	OldFirewall
IP Address	100.64.1.1
Physical Address	00:50:56:b8:25:3f
Device Type	Firewall
Incoming Events	Security Events OldFirewall

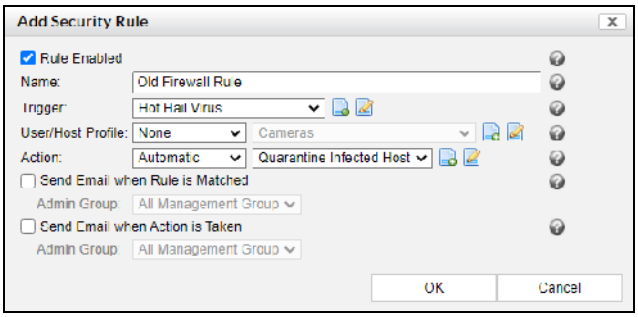
4. Leave all other settings at the default values, and then click **OK**.

To create a security rule for the old firewall

1. Click **Logs** > **Security Incidents**, and then click the **Rules** tab.
2. Click **Add** to create a new security rule.
   The **Add Security Rule** window opens.
3. Ensure that the **Rule Enabled** checkbox is selected.
4. In the **Name** field, type `Old Firewall Rule`.
5. Click **Add Security Trigger** to create a new trigger for this rule.
   The **Add Security Trigger** window opens.
6. Configure the following settings:

Field	Value
Name	Hot Hail Virus
Time Limit	1 Seconds
Filter Match	All

7. In the **Security Filter** section, click **Add**, and then configure the following settings:
   a. Select **Vendor**, and then type `ACME Corp`.
   b. Select **Type**, and then type `Alert`.
   c. Select **Subtype**, and then type `Virus`.
   d. Select **Description**, and then type `FlashGordon-HotHail-Virus Detected`.
   e. Select **Severity**, in the **Min** field, type `7`, and then in the **Max** field, type `9`.
   f. Click **OK**.
8. In the **Add Security Trigger** window, click **OK**.
9. In the **Action** field, select **Automatic**, and then click the **Add Security Action** icon to create a new security action.
10. In the **Name** field, type `Quarantine Infected Host`.
11. In the **Activities** section, click **Add**.
    The **Add Security Activity** window opens.
    a. In the **Activity** field, select **Mark Host At Risk**.
    b. In the **Primary Task** field, select **Quarantine Host**.
    c. Click **OK**.



12. Click **OK** to complete the security rule creation.

Rank the Security Rules

Security rules are processed in the order they are ranked. You will rank the security rules.

To rank the security rules

1. Select each rule individually, and then use the **Rank** arrows or the **Set Rank** button to rank the security rules in the following order:

a. Virus Infected File Detected-Contractor

b. Denied Category Web Filter Matched by Contractor

c. General Security Risk

d. Old Firewall Rule

e. Catch Most

Exercise 7: Validating Security Rules

In this exercise, you will validate that the security rules are triggered by input from FortiGate.

Validate Security Events, Alarms, and Actions

You will validate the security rules are generating security events, alarms, and actions.

To validate security events, alarms, and actions

1. Log in to the FortiNAC-Primary GUI with the username `admin` and password `password`.
2. Click **Logs** > **Security Incidents**, and then click the **Events** tab.
3. At the top of the page, configure the filter to show events generated in the last **5** minutes.
4. Click **Update**.
   There should be no—or very few—events.
5. On the workstation client machine, open Firefox.
6. Click the **News** bookmark.
   You should receive a **Web Page Blocked** message.
7. Click the **AV Test** bookmark.
   You should receive a **High Security Alert!** message.
8. Click the **SecurityRisk** bookmark, let it try to load for a couple of seconds, and then click **X** to stop trying to load the page.
9. Return to the FortiNAC-Primary GUI, click **Logs** > **Security Incidents**, select the **Events** tab, and then view the entries.
   There should be several entries.
10. Click the **Alarms** tab.
    There are security alarms listed in the view.
11. Locate, and then select the **General Security Risk** security alarm that has an **Action Taken Date** listed.
12. At the bottom of the page, view the entry in the **Events** tab, and then select the **Actions Taken** tab to validate that the configured actions were taken.
13. Return to the workstation client machine.
14. Click the **News** bookmark.
15. Return to the FortiNAC-Primary GUI, click **Logs** > **Security Incidents**, select the **Events** tab, and then view the entries.
    There should be several entries.
16. Click **Logs** > **Security Incidents**, and then select the **Alarms** tab.
    The **Security Alarms** window opens, and security alarms should be listed on the page for the **Denied Category Web Filter Matched by Contractor** rule.
17. Return to the workstation machine.
18. Click the **AV test** bookmark.

19. Return to the FortiNAC-Primary GUI, click **Logs** > **Security Incidents**, select the **Events** tab, and then view the entries.

    There should be several entries.

20. Click the **Alarms** tab.

    The **Security Alarms** window opens, and security alarms should be listed in the view for the **Virus Infected File Detected-Contractor** rule.

21. Click **Users & Hosts** > **Hosts**.
22. In the **Search** field, type `*00:02:02` (the last six digits of the MAC address noted in the security event), and then press `Enter`.

    The host record should be displayed, and the **Status** column should have an **X** through it, indicating that the host was disabled.

Lab 10: FortiNAC High Availability and Control Manager

In this lab, you will configure and test high availability (HA) by adding a secondary FortiNAC, and then forcing a failover. Next, you will integrate FortiNAC Manager and the FortiNAC system you have been working with throughout the labs. The integration will allow you to explore the capabilities of FortiNAC Manager.

Objectives

- Configure and test HA
- Model and manage FortiNAC with FortiNAC Manager

Time to Complete

Estimated: 40 minutes

Exercise 1: Configuring FortiNAC for HA

In this exercise, you will pair two FortiNAC devices to work in a fault tolerant HA pair. The primary FortiNAC will continuously sync database and configuration information with the designated secondary FortiNAC. The secondary FortiNAC will remain in a standby state. Next, using both the FortiNAC CLI and FortiNAC GUI, you will validate that the two devices are communicating.

Configure FortiNAC for HA

You will configure FortiNAC for HA.

To configure FortiNAC for HA

1. Log in to the jump box, and then launch the browser.
2. Use the bookmark to log in to the FortiNAC-Primary GUI with the username `admin` and password `password`.
3. Click **System** > **Settings** > **System Management**, and then select **High Availability**.
4. Select the **Use Shared IP Address** checkbox, and then in the **FortiNAC Server** section, configure the following settings:

Field	Value
Shared IP Address	10.0.1.118
Shared Subnet Mask(bits)	24
Shared Host Name	FortiNAC-HA

5. In the **FortiNAC Server Configuration** section, in the **Primary Appliance** section, configure the following settings:

Field	Value
IP Address	10.0.1.110
Gateway IP Address	10.0.1.254
CLI/SSH root Password [User:root]	password

6. After you type and confirm the password, click **OK**.
7. In the **FortiNAC Server Configuration** section, in the **Secondary Appliance** section, configure the following settings:

Field	Value
IP Address	10.0.1.115

Field	Value
Host Name	FortiNAC-Secondary
Gateway IP Address	10.0.1.254
CLI/SSH root Password [User: root]	password

8. After you type and confirm the password, click **OK**.

The gateway address defined on the **High Availability** page is not a gateway for routing traffic—this is defined in the configuration wizard. The gateway defined here is used only to test network connectivity if the primary and secondary devices lose connectivity.

9. Click **Save Settings**.
   A window appears with the following text: **Applying Settings. This could take a few minutes. Please wait**. It may take several minutes for the window to disappear.

   Another window appears and gives you the option to restart the FortiNAC servers.
10. Click **Yes** to restart the services, and then click **OK**.
11. Wait 4–5 minutes for the reboot and system startup to complete before beginning the next exercise.

Exercise 2: Validating the HA Status and Successful Failover

In this exercise, you will validate that the HA configuration is working correctly and that the primary and secondary FortiNAC servers are communicating successfully. Next, you will perform a failover test to validate a successful transition from the primary server to the secondary server. Finally, you will perform a transfer of control from the secondary server back to the primary server, and then ensure that the devices resume normal HA operation.

Validate the HA Status on the GUI

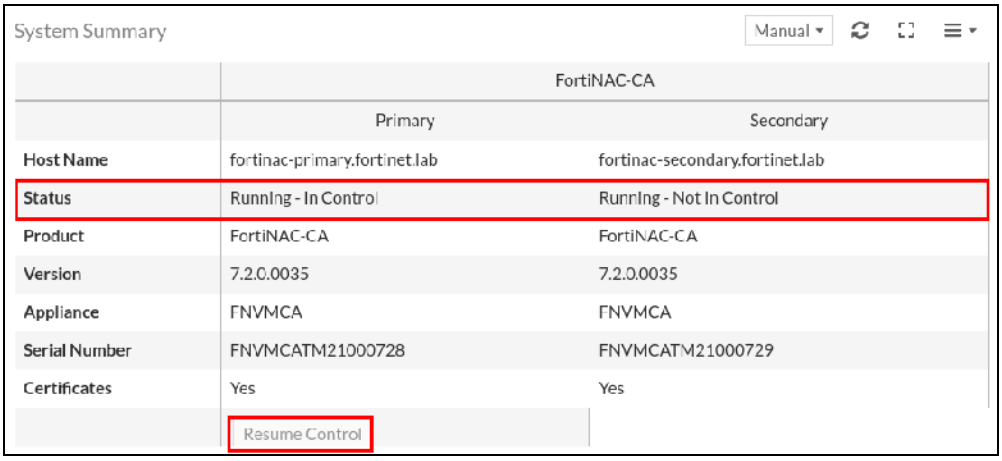
Using the GUI dashboard, you will validate that the primary and secondary FortiNAC servers are communicating correctly.

To validate the HA status on the GUI

1. From the jump box, log in to the FortiNAC-HA GUI with the username `admin` and password `password`.

Once FortiNAC is running in HA using a shared IP address, you can access the GUI only by using the shared IP address. For the rest of this exercise, you should use the FortiNAC-HA browser bookmark to access the GUI.

2. In the **Dashboard** > **Main** view, examine the **System Summary** section.
   The **Status** field in the **Primary** column shows **Running - In Control** and in the **Secondary** column shows **Running - Not in Control**. At the bottom of the **Primary** column, **Resume Control** is unavailable.

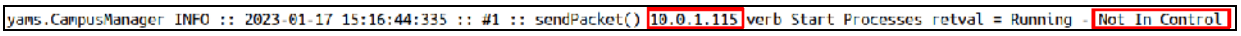


Validate the HA Status on the CLI

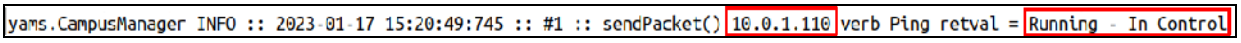
You will validate HA communication on the CLI using the log output of the primary and secondary servers.

To validate the HA status on the CLI

1. Use PuTTY to log in to the FortiNAC-Primary CLI with the username `root` and password `password`.
2. Enter the following commands:
   ```
   logs
   ```
   ```
   tf output.processManager
   ```
3. Monitor the log file for a few minutes.
   You should see a log entry that ends with `sendPacket() 10.0.1.115 verb Ping retval = Running - Not In Control` repeating approximately every 30 seconds. This indicates that the secondary server (10.0.1.115) is running, but is not in control.



4. Use PuTTY to log in to the FortiNAC-Secondary CLI with the username `root` and password `password`.
5. Enter the following commands:
   ```
   logs
   ```
   ```
   tf output.processManager
   ```
6. Monitor the log file for a few minutes.
   You should see a log entry that ends with `sendPacket() 10.0.1.110 verb Ping retval = Running - In Control` repeating approximately every 30 seconds. This indicates that the primary server (10.0.1.110) is running and in control.



7. Press `Ctrl+C` to stop the log file output.

Force an HA Failover, Validate It, and Recover

The final step in HA validation is to force a failover from the primary FortiNAC server to the secondary FortiNAC server. You will force the failover, validate its success, and then return control to the primary FortiNAC server.

To force an HA failover, validate it, and recover

1. On the FortiNAC-Primary CLI, enter the following command:
   ```
   shutdownNAC -kill
   ```
   This command shuts the FortiNAC processes down completely, which simulates a system failure.
2. On the FortiNAC-Secondary CLI, enter the following commands:
   - `logs`
   - `tf output.processManager`

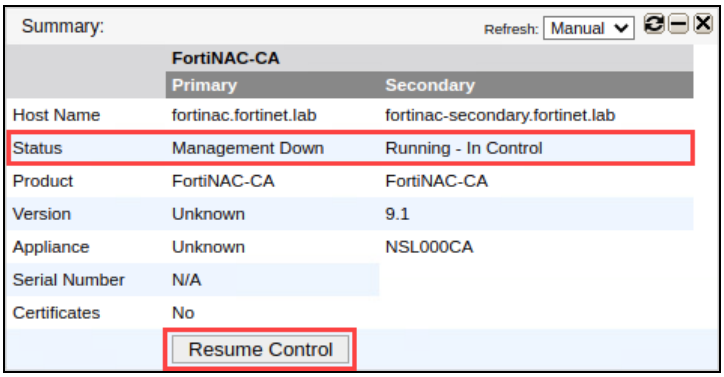
3. Monitor the log output for `**** Failed to talk to primary **** PingRetryCnt = X pingRetries = 3`.

   `PingRetryCnt` is the current retry and `pingRetries` is the total number of retries that FortiNAC will attempt. Soon after the final retry, the failover to FortiNAC-Secondary begins. The failover takes about 5 minutes to complete.

For the purpose of speeding up the lab, the number of retries is set to 3, instead of the default of 5.

4. Log in to the FortiNAC-HA GUI with the username `admin` and password `password`.
5. Click **Dashboard** > **Main**, and then examine the **System Summary** section to validate that the failover completed successfully.

   The primary server should have a status of **Management Down** and the secondary server should have a status of **Running - In Control**. The **Resume Control** button at the bottom of the **Primary** column should now be available.



6. Click **Resume Control** to restore control to the primary FortiNAC server and return FortiNAC-Secondary to the role of standby server.
7. Click **OK**.

   The restore process may take 4–5 minutes.

8. Log back in to the FortiNAC-HA GUI, and then confirm that **Resume Control** is unavailable.

Exercise 3: Managing FortiNAC With FortiNAC Manager

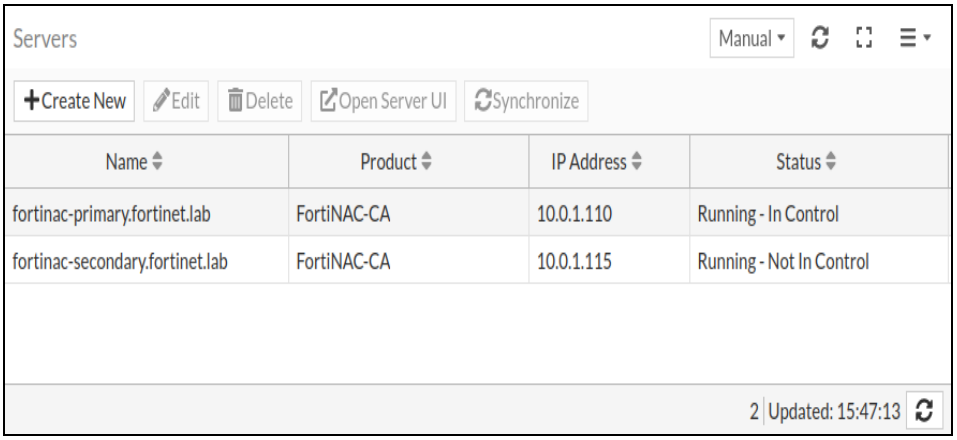
In a distributed environment with more than one FortiNAC, FortiNAC Manager provides the ability to manage administrative configurations and network-wide visibility from a single interface. In this lab, you will model FortiNAC in FortiNAC Manager and demonstrate its capabilities.

Add a FortiNAC to FortiNAC Manager

You will model FortiNAC in FortiNAC Manager and examine the management capabilities.

To add a FortiNAC to FortiNAC Manager

1. Log in to the jump box with the username `admin` and password `password`.
2. Launch the browser, and then click the **FortiNAC-Manager** bookmark.
3. Log in to the FortiNAC Manager GUI with the username `admin` and password `password`.
4. Click **Dashboard** > **Main**, and then in the **Servers** section, click **Create New**.
5. In the **IP Address** field, type `10.0.1.118`, and then click **OK**.
6. Wait a few moments, and then refresh the **Servers** section.
   The FortiNAC HA pair appears in the list of servers.



If the columns are not populated after you add the server, refresh the **Servers** section.

Manage Device Classification and Global Provisioning

You will create a global device profiling rule that organizes profiled devices by adding them to a global group. The group is used to assign a network access policy. You will then synchronize the configurations with the FortiNAC

HA pair.

To create a global device group

1. Continuing on the FortiNAC Manager GUI, click **System** > **Groups**.
2. Click **Add**, and then configure the following settings:

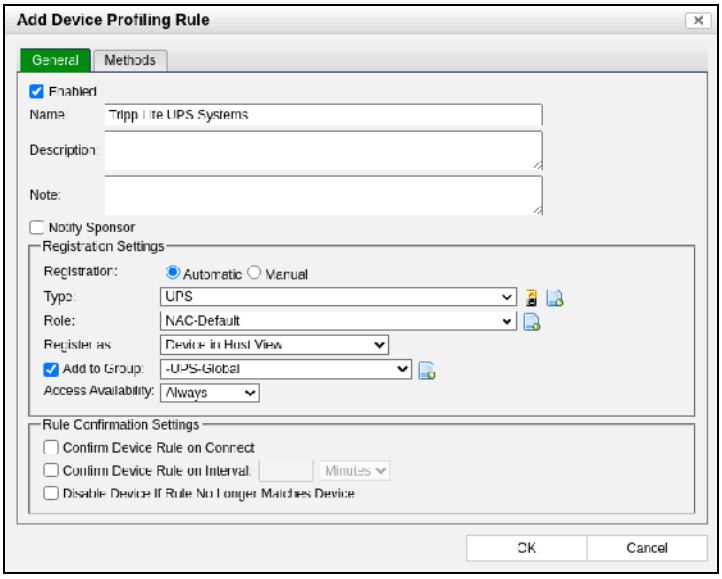
Field	Value
Name	-UPS-Global
Member Type	Host
Description	Global group for UPS systems

3. Click **OK**.

To create a global device profiling rule

1. Continuing on the FortiNAC Manager GUI, click **Hosts** > **Device Profiling Rules**.
2. Click **Add**, and then configure the following settings:

Field	Value
Enabled	(Select the checkbox.)
Name	Tripp Lite UPS Systems
Registration	**Automatic**
Type	**UPS**
Register as	**Device in Host View**
Add to Group	Select the checkbox, and then select **-UPS-Global**.



3. Click the **Methods** tab, and then select the **Vendor OUI** method.
4. Click **Add**, and then in the **Add OUI** window, configure the following settings:

Field	Value
Field	Vendor Name
Value	Tripp Lite

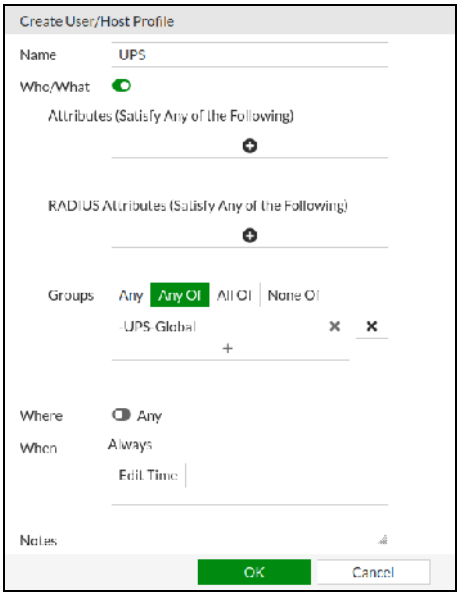
5. Click **OK**.
6. In the **Add Device Profiling Rule** window, click **OK**.

To create a global logical network and network access policy

1. Continuing on the FortiNAC Manager GUI, click **Network** > **Logical Networks**.
2. Click **Create New**, and then in the **Create Logical Network** window, in the **Name** field, type `Network Monitoring`.
3. Click **OK**.
4. Click **Policy & Objects** > **User/Host Profiles**.
5. Click **Create New**, and then in the **Create User/Host Profile** window, configure the following settings:

Field	Value
Name	UPS
Who/What	(Enable this setting.)
Groups	1. Select **Any Of**. 2. Click **+**, and then select **-UPS-Global**. 3. Close the **Select Entries** panel.

6. In the **Create User/Host Profile** window, click **OK**.



7. Click **Policy & Objects** > **Network Access**.
8. Click the **Configurations** tab, and then click **Create New**.
9. In the **Create Network Access Configuration** window, configure the following settings:

Field	Value
Name	Provision to Monitor
Logical Network	Network Monitoring

10. Click **OK**.
11. Click the **Policies** tab, and then click **Create New**.
12. In the **Create Network Access Policy** window, configure the following settings:

Field	Value
Name	UPS Access Policy
Configuration	Provision to Monitor
User/Host Profile	UPS

13. Click **OK**.
14. Click **Dashboard** > **Main**.
15. In the **Server** section, select **fortinac-primary.fortinet.lab**, and then click **Synchronize**.

Only one FortiNAC HA pair exists in the lab environment. Typically, FortiNAC Manager manages two or more pairs, and the synchronization process updates each pair with the global configurations.

16. In the **Servers** section, select **fortinac-primary.fortinet.lab**, and then click **Open Server UI**.
17. On the new tab, accept any security warnings to load the FortiNAC-Primary GUI.
18. Verify that the GUI loads correctly, and then close the tab.
19. Log out of FortiNAC Manager.

To validate the global configurations

1. Log in to the FortiNAC-HA GUI with the username `admin` and password `password`.
2. Click **System** > **Groups**.
3. Verify that the **-UPS-Global** group was added to the list of groups.
4. Click **Policy & Objects** > **Network Access**.
5. Verify that **UPS Access Policy** appears in the list of access policies.
6. Click **Users & Hosts** > **Device Profiling Rules**.
7. Verify that **Tripp Lite UPS Systems** appears in the list of device profiling rules.
8. Click **Run** to evaluate existing rogue devices.

The **Run** option evaluates all rogue devices currently in the FortiNAC database. FortiNAC automatically evaluates any new rogue devices that connect to it.

9. Click **Users & Hosts** > **Hosts**.
10. In the search field type `00:06:67*`, and then press `Enter`.
11. Right-click one of the UPS devices, and then select **Policy Details**.
    The UPS now has the **UPS Access Policy** assigned to it.
12. Click **Close**.

You must still define the logical networks in the model configuration views of the local FortiNAC devices.

Examine the Global Visibility Views

You will examine the different visibility views that provide consolidation in distributed FortiNAC environments.

To examine the global visibility views

1. Log in to the FortiNAC Manager GUI with the username `admin` and password `password`.
2. Click **Users** > **User Accounts**.
3. In the upper-right corner, click the refresh button.
   Note that the users were synchronized from FortiNAC. In a distributed environment with more than one FortiNAC, you can use the **Servers** drop-down list to limit the search results to a specific server.
4. Click **Hosts** > **Hosts**.
5. Examine the hosts that were synchronized from the FortiNAC.
   Note that the **Server** column identifies the FortiNAC that most recently managed the host.
6. Click **Hosts** > **Adapters**.
7. Examine the adapter list.

Tips and Tricks

This section provides several helpful tools, commands, and log files to assist with troubleshooting different aspects of the FortiNAC product.

Log Files

To access log files, log in to the FortiNAC using the CLI.

- Type `diagnose tail -f <output file>` at the prompt and press `enter`
- The Master Loader log file is: `output.master`
- The Nessus Loader log file is: `output.nessus`
- The DHCP service log file is: `dhcpd.log`

L2 Poll

The following commands performs an L2 poll on the specified device.

```
execute enter-shell
UpdateClients -ip 11.17.104.2
```

L3 Poll

The following commands performs an L3 poll on the specified device.

```
execute enter-shell
ReadArpCache -ip 11.17.104.2
```

Portal

Enter the following as a URL to view a specific portal when there is more than one portal.

```
http://<FortiNAC IP Address>/registration/?portalName=<name>
```

Captive Portal

Host is not being moved to the captive VLAN:

- Verify that FortiNAC has the correct configuration for device control (CLI and Read/Write SNMP security strings) within the Model Configuration.

- Verify that the Network Access Value is correctly set in the Model Configuration.
- Verify that the device is configured correctly.

If a host is in the captive VLAN but not being presented the captive portal:

- Verify the host is in the captive VLAN
- Verify the host does not have static IP or DNS entries
- Ping sites that are not in the zones.common (approved) list. All sites should resolve to the FortiNAC captive interface.
- Ping sites that are in the zones.common (approved) list. Sites should resolve correctly.

Device Profiler

Device profiling rules can be viewed using the following commands:

- `diagnose dump-dpc-rules display-by-id <rule ID>`
- `diagnose dump-dpc-rules display-by-name <rule name>`