DO NOT REPRINT
© FORTINET

Zero Trust Access

Lab Guide

for FortiOS 7.2

Fortinet Training Institute

DO NOT REPRINT
© FORTINET

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

DO NOT REPRINT
© FORTINET

TABLE OF CONTENTS

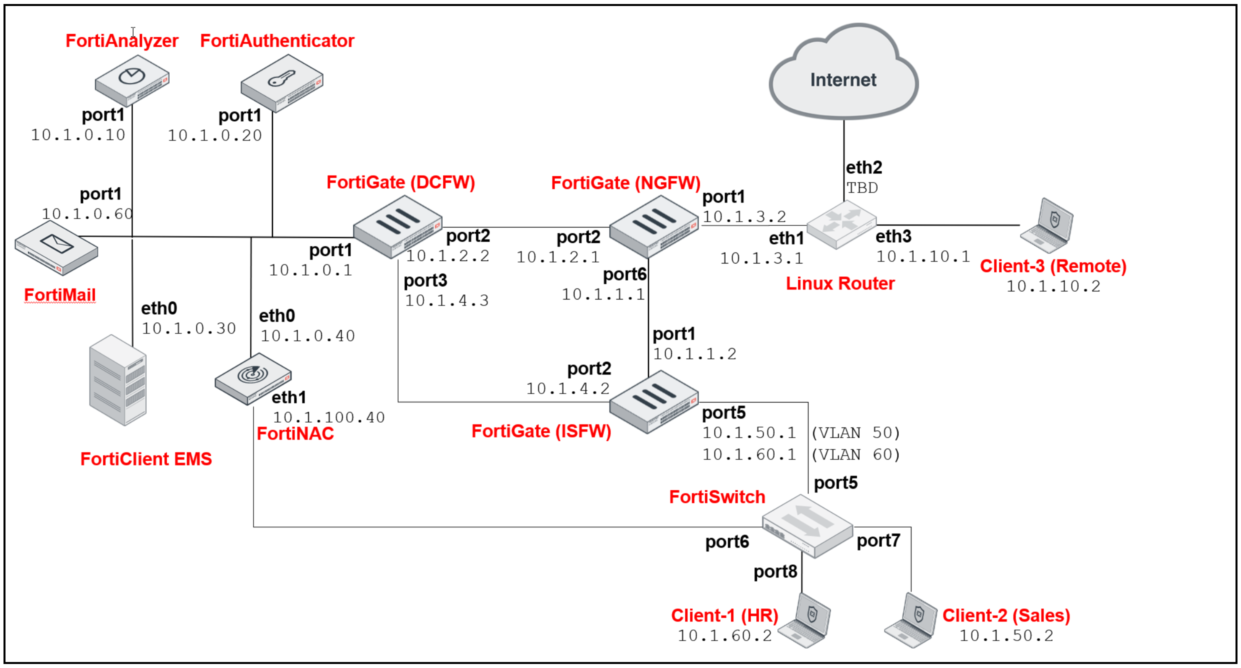
DO NOT REPRINT
© FORTINET

DO NOT REPRINT
© FORTINET

DO NOT REPRINT
© FORTINET

DO NOT REPRINT
© FORTINET

Network Topology



DO NOT REPRINT
© FORTINET

Lab 1: Legacy Architecture Challenges

In this lab, you will integrate FortiSwitch with ISFW-FortiGate and test scenarios to learn the shortcomings of traditional security architecture. Next, you will configure the network to achieve both macrosegmentation and microsegmentation. Finally, you will set up VPN access for remote endpoints to securely connect to the corporate infrastructure and understand the drawbacks of VPN technology with regard to zero trust.

Objectives

- Integrate FortiSwitch with FortiGate
- Achieve macrosegmentation and microsegmentation
- Enable remote access using VPN technology
- Understand the shortcomings of legacy security architecture

Time to Complete

Estimated: 60 minutes

DO NOT REPRINT
© FORTINET

Exercise 1: Integrating FortiSwitch

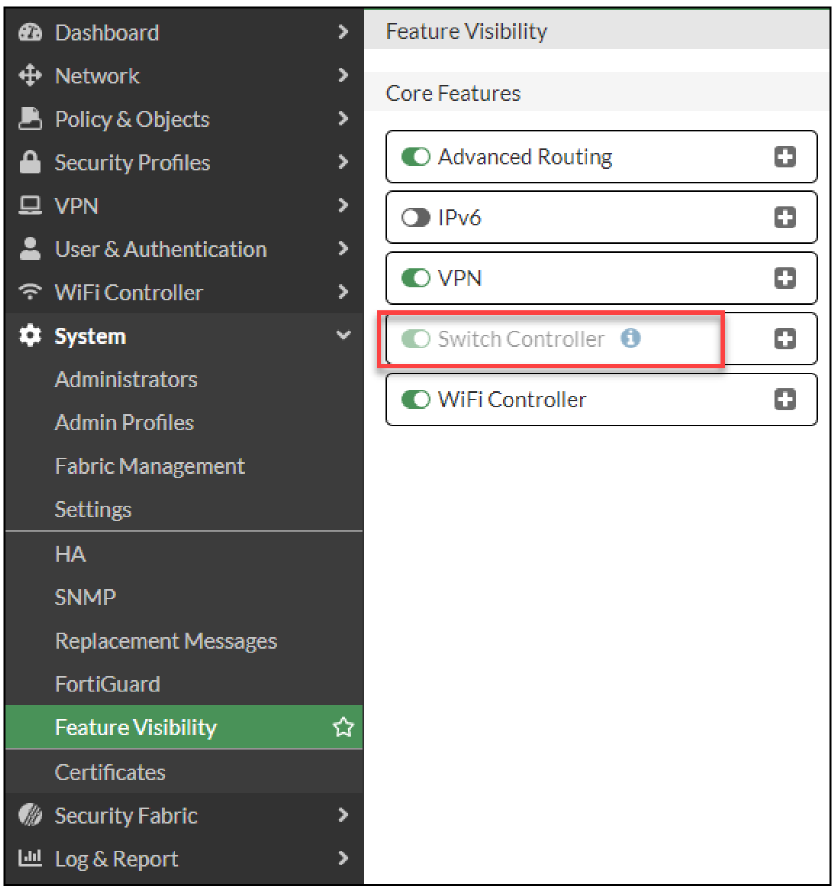
You will integrate FortiSwitch with FortiGate and configure a simulated flat network with a single subnet and unrestricted access to the data center and the internet.

Add FortiSwitch to ISFW FortiGate Management

You will enable FortiSwitch management of ISFW FortiGate by using the FortiLink protocol.

To add FortiSwitch to ISFW-FortiGate

1. Open an RDP connection to the FortiClient EMS VM, and then log in with the username `Administrator` and password `Password1!`.
2. Open Google Chrome, and then in **Bookmarks**, select the **ISFW** login page bookmark.
3. Log in to the ISFW FortiGate GUI with the username `admin` and password `password`.
4. Click **System** > **Feature Visibility**, and then enable **Switch Controller**.

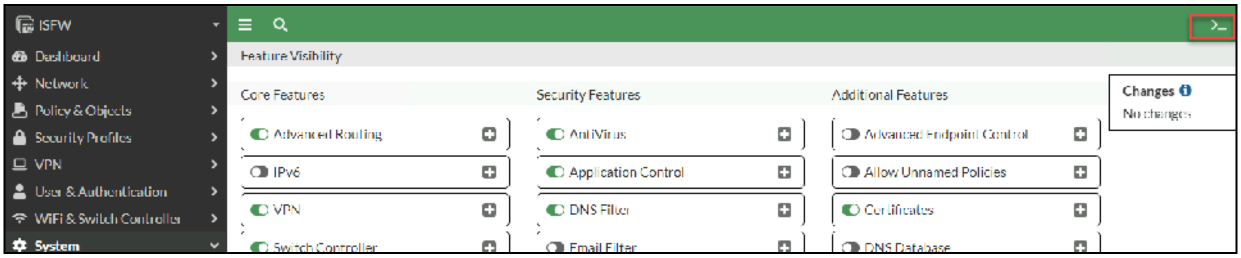


5. Click **Apply**.

DO NOT REPRINT
© FORTINET

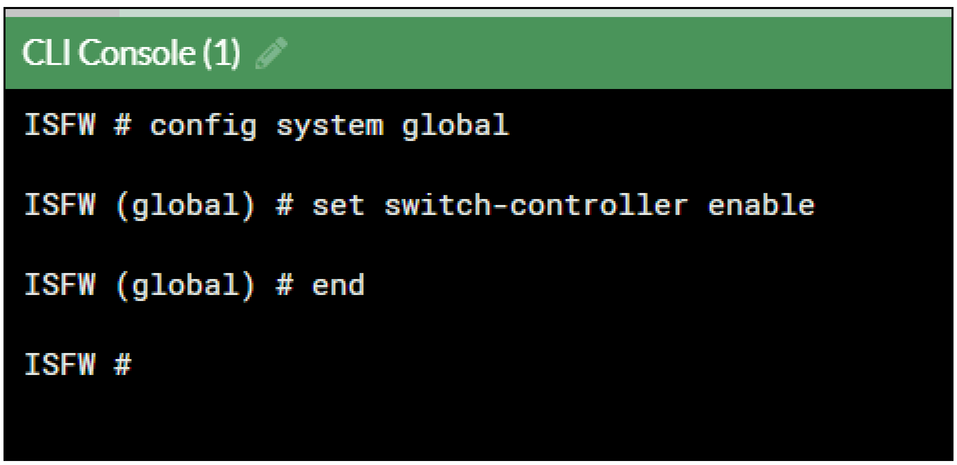
If the **Switch Controller** field and the **WiFi & Switch Controller** menu item are unavailable, you should enable the switch controller using the CLI. This is required only on FortiGate VMs; physical FortiGate devices have the switch controller enabled.

6. Click the **CLI console** icon to open the CLI console.



7. Enter the following commands to enable the switch controller:

```
config system global

set switch-controller enable

end
```

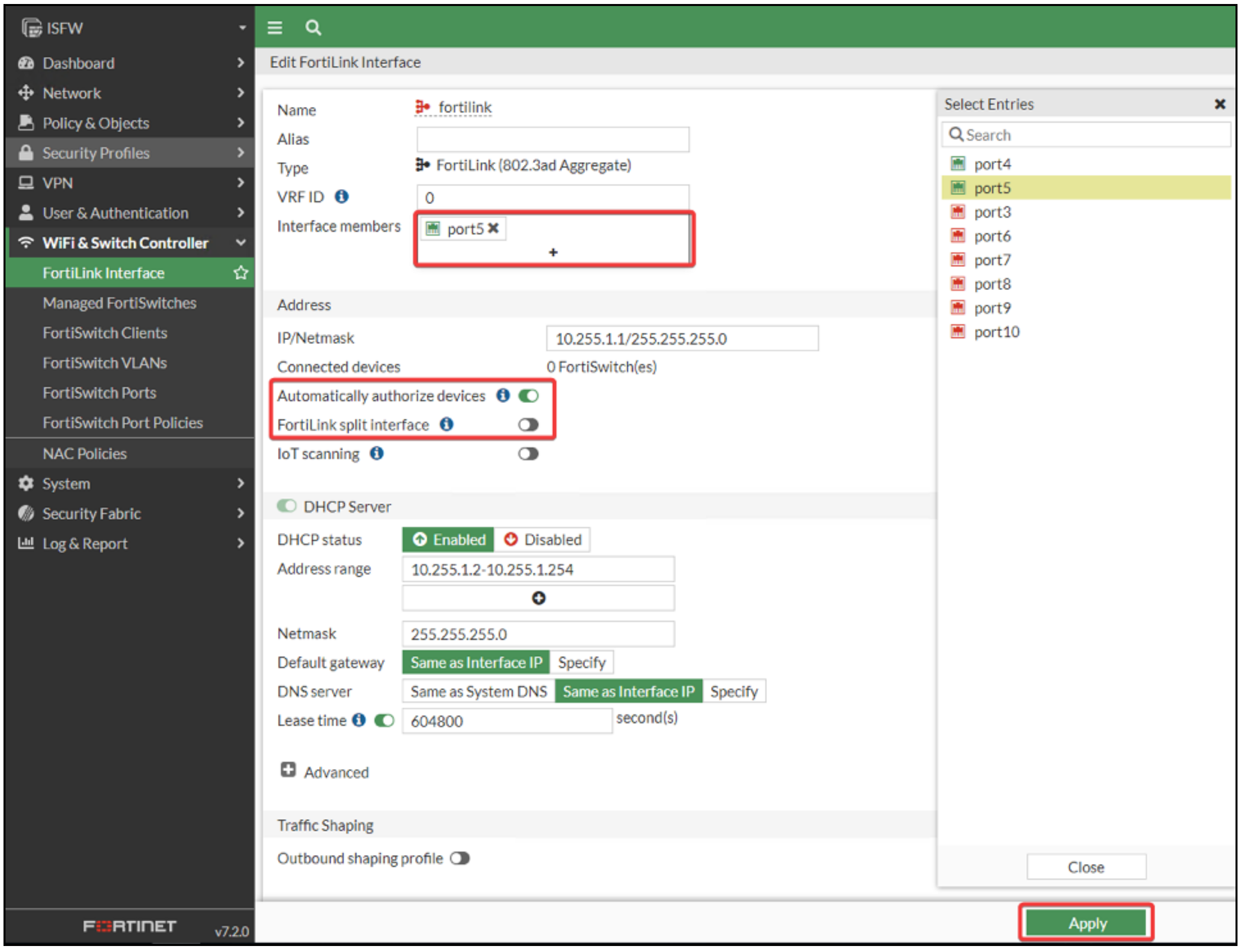


8. Close the CLI console.
9. Refresh the web page.

   The **WiFi & Switch Controller** menu item appears.

10. Click **WiFi & Switch Controller** > **FortiLink Interface**.
11. Select **port5**, and then add it to the **Interface members** field.
12. Verify that **Automatically authorize devices** is enabled, and that **FortiLink split interface** is disabled, and then click **Apply**.

DO NOT REPRINT
© FORTINET



13. Click **Managed FortiSwitches**.

    The FortiSwitch appears. Its state changes from **Offline** to **Connecting**, and then to **Online**.

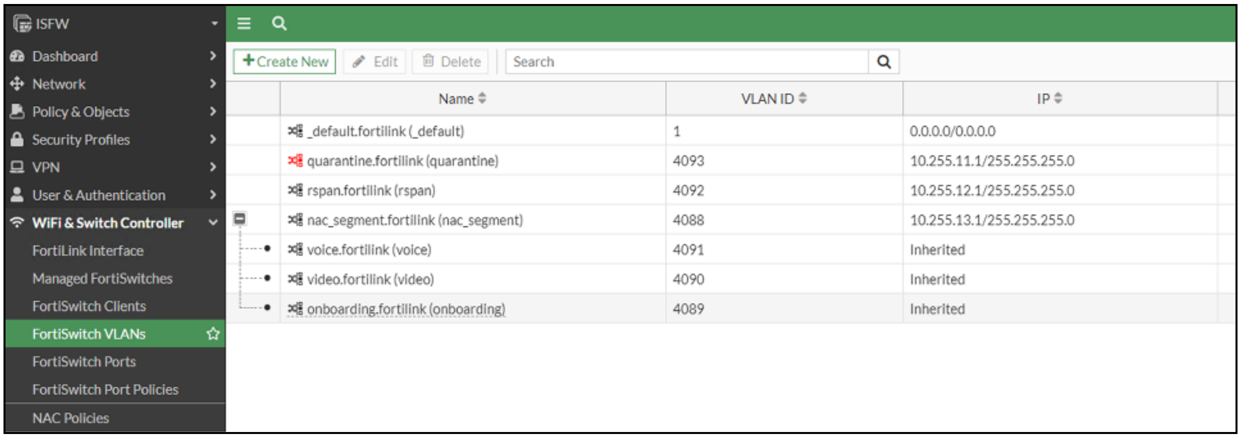
Configure the Default FortiLink VLAN

By default, FortiLink creates multiple VLANs for a managed FortiSwitch. You will now configure the default FortiLink VLAN.

To configure the default FortiLink VLAN

1. Continuing on the ISFW FortiGate GUI, click **WiFi & Switch Controller** > **FortiSwitch VLANs**.

DO NOT REPRINT
© FORTINET



The VLANs that appear are automatically generated when you integrate FortiSwitch with FortiGate and they do not reflect the VLANs you will use for integration with FortiNAC in a later exercise.

2. Edit the **_default.fortilink (_default)** interface and configure the following settings:

Field	Value
Role	LAN
IP/Netmask	10.1.99.1/24
Administrative Access	Ping

3. Click **OK**.
4. Click the **CLI console** icon to open the CLI console.
5. Enter the following command to run the script to enable the DHCP server and the IP address reservation for the interface **_default.fortilink (_default)**:

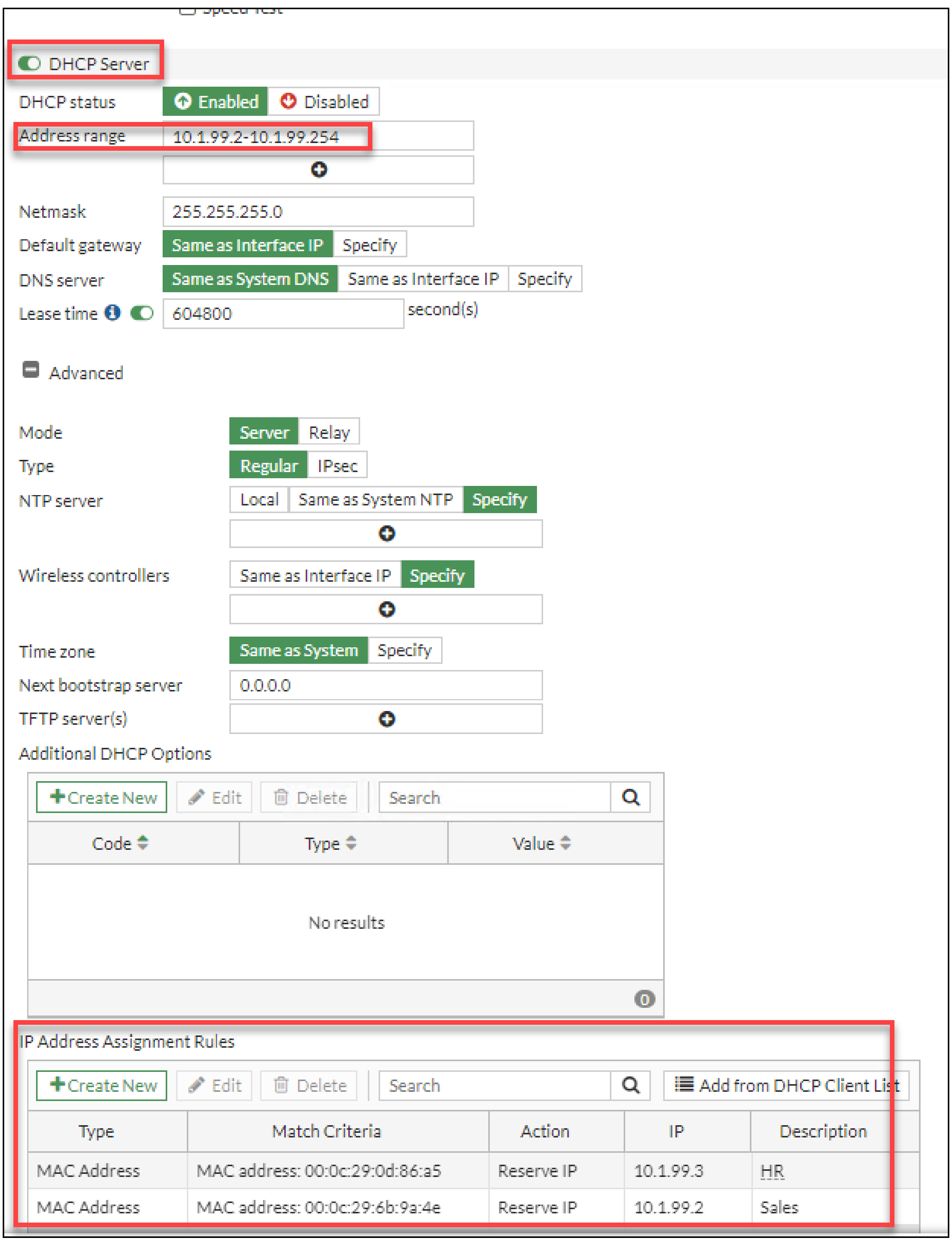
```
execute auto-script start dhcp_config
```

The `dhcp_config` autoscript enables a DHCP server for the interface **_default.fortilink (_default)**.The autoscript also reserves IP addresses for the HR VM and the Sales VM based on their MAC addresses. You can enter the following command on the ISFW FortiGate CLI to review the contents of the autoscript:

```
show system auto-script dhcp_config
```

6. Close the CLI console.
7. Click **WiFi & Switch Controller** > **FortiSwitch VLANS**, and then edit the **_default.fortilink (_default)** interface.
8. Verify that the **DHCP Server** is enabled and has an **Address range** specified.
9. Click **Advanced**, and then review the **IP Address Assignment Rules**.

DO NOT REPRINT
© FORTINET



10. Click **WiFi & Switch Controller** > **FortiSwitch Ports**, and then verify that all ports except **port5** have the **Native VLAN** set to **_default.fortilink (_default)**.

DO NOT REPRINT
© FORTINET

11. Click **Policy & Objects** > **Firewall Policy**.
12. Click **Create New**, and then configure the following settings:

Field	Value
Name	Allow_All
Incoming Interface	_default.fortilink (_default)
Outgoing Interface	port1, port2
Source	all
Destination	all
Schedule	always
Service	ALL
Action	Accept
NAT	Enable
Log Allowed Traffic	All Sessions

13. Click **OK**.

Test Connectivity

You will now test the connectivity to ensure that the firewall policy is allowing the traffic as intended.

To test the connectivity

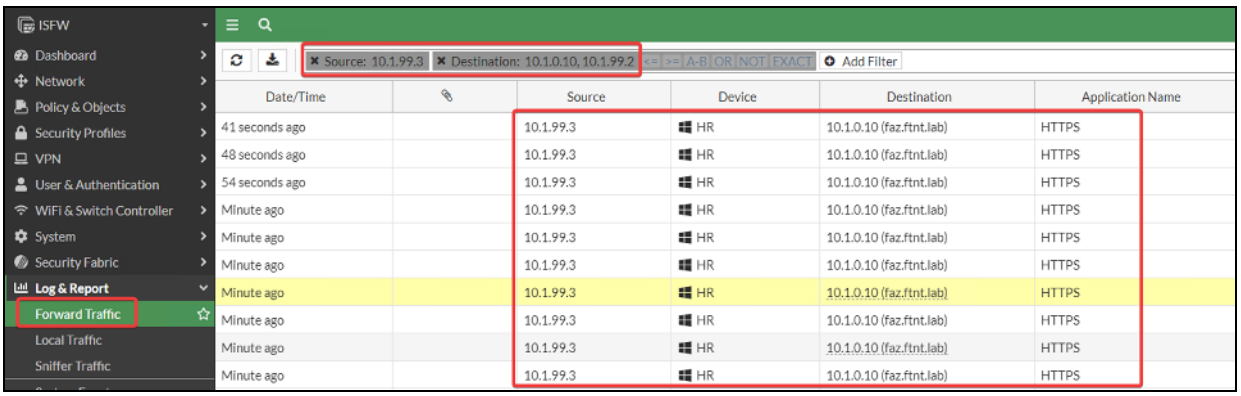
1. Open an RDP connection to the SALES VM, and then log in with the username `sales\student` and password `Password1!`.
2. Open a command prompt window, enter the following command to check IP access, and then note the IP address:
   ```
   ipconfig
   ```

> If the IP address is not in the `10.1.99.x` range, make sure you configured the switch as described in previous steps, and then enter the `ipconfig /release` and `ipconfig /renew` commands to obtain a new lease.

3. Enter the following command to test internet connectivity:
   ```
   ping 1.1.1.1
   ```
4. Enter the following command to ensure that you have connectivity to the data center and the EMS server:
   ```
   ping 10.1.0.30
   ```
5. Open an RDP connection to the HR VM, log in with the username `ftnt\hr` and password `Password1!`.
6. Repeat steps 2–4 for the HR VM.
7. Ping the SALES VM using the IP address that you noted in step 2, for example `ping 10.1.99.2`.

DO NOT REPRINT
© FORTINET

8. Return to the SALES VM, and ping the HR VM using the IP address that you noted.
9. Return to the HR VM, right-click on the **Windows** icon, and then click **Run**.
10. Type `mstsc`, and then click **OK** to open a Remote Desktop Connection.
11. Log in to `10.1.99.2` with the username `student`and password `Password1!`.
12. Click **Yes**.
13. Disconnect the RDP session.
14. Continuing on the HR VM, open Google Chrome, and then in **Bookmarks**, select the **FortiAnalyzer** login page bookmark.
15. Return to the ISFW FortiGate GUI on the FortiClient EMS VM, and click **Log & Report** > **Forward Traffic**, and then clear any existing search filters.
16. Add a filter for the **Source** using the IP address you noted for the HR VM, and then add a filter for the **Destination** using the IP address 10.1.0.10 (FortiAnalyzer) and the IP address you noted for the SALES VM, as shown in the following image:



Stop and think!

You see logs only for HTTPS access to FortiAnalyzer, but not for RDP access to the SALES VM. What is the reason for this?

Traffic flows within the same subnet never reach the firewall and are switched at the FortiSwitch level.

DO NOT REPRINT
© FORTINET

Exercise 2: Configuring Microsegmentation

In this exercise, you will configure microsegmentation with physical workloads.

Block traffic between endpoints in same VLAN

In this section, you will enable the **Block intra-VLAN traffic** field to block communication between devices connected to the same VLAN on a switch.

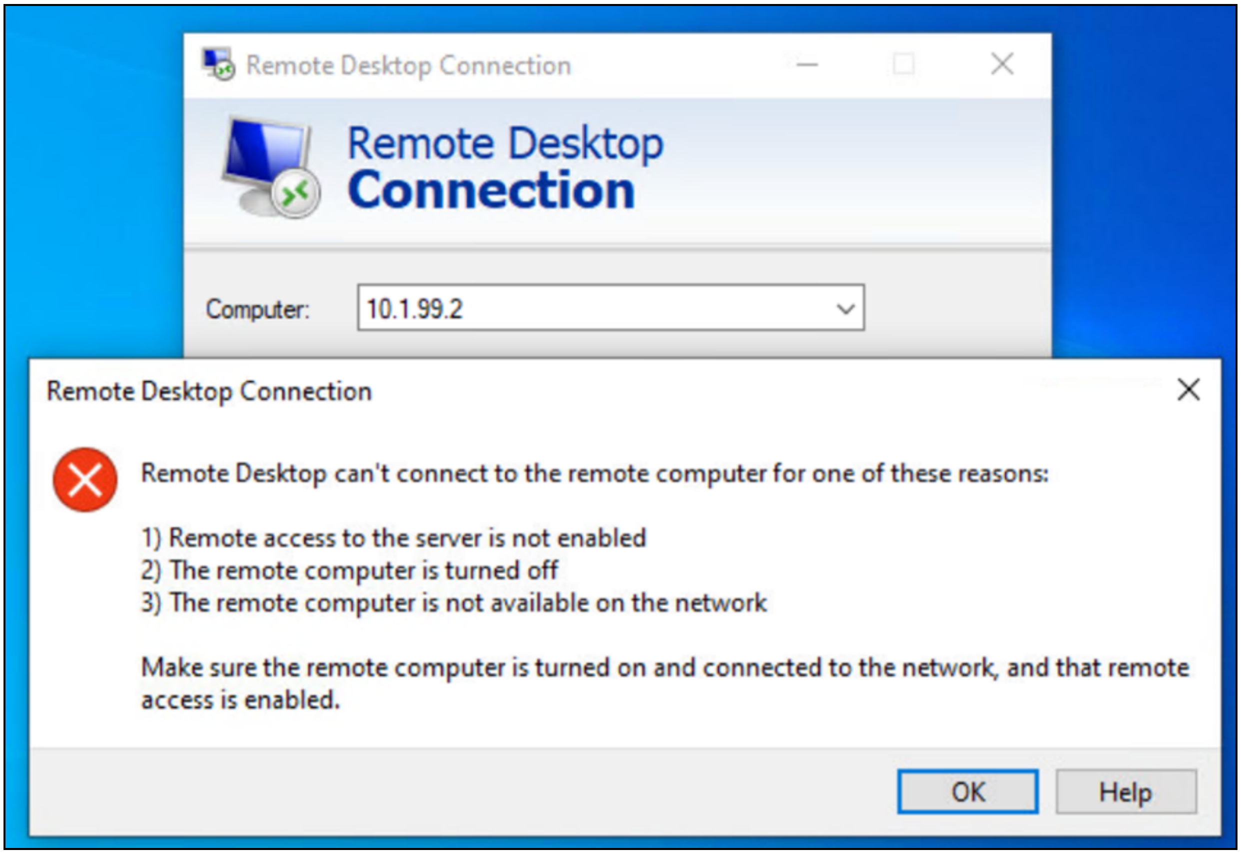
To block intraVLAN traffic

1. On the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **ISFW** login page bookmark.
2. Log in to the ISFW FortiGate GUI with the username `admin` and password `password`.
3. Click **WiFi & Switch Controller** > **FortiSwitch VLANs**.
4. Edit the **_default.fortilink (_default)** interface.
5. In the **Network** section, enable **Block intra-VLAN traffic**, and then click **OK**.
6. Return to the HR VM, open a command prompt window, and then enter the `ping` command using the IP address you noted in the previous exercise to verify connectivity to the SALES VM.

   The ping should fail.
7. Right-click on the **Windows** icon, and then click **Run**.
8. Type `mstsc`, and then click **OK** to open the Remote Desktop Connection application.
9. Type `10.1.99.2`, and then click **Connect**.

   The connection should fail and display the error shown in the following image:

DO NOT REPRINT
© FORTINET



Manage traffic between endpoints in the same VLAN

To allow intraVLAN traffic between specific endpoints, you will configure a firewall policy and proxy-arp for the endpoints. Next, you will restrict access to allow an RDP connection only between the SALES VM and the HR VM.

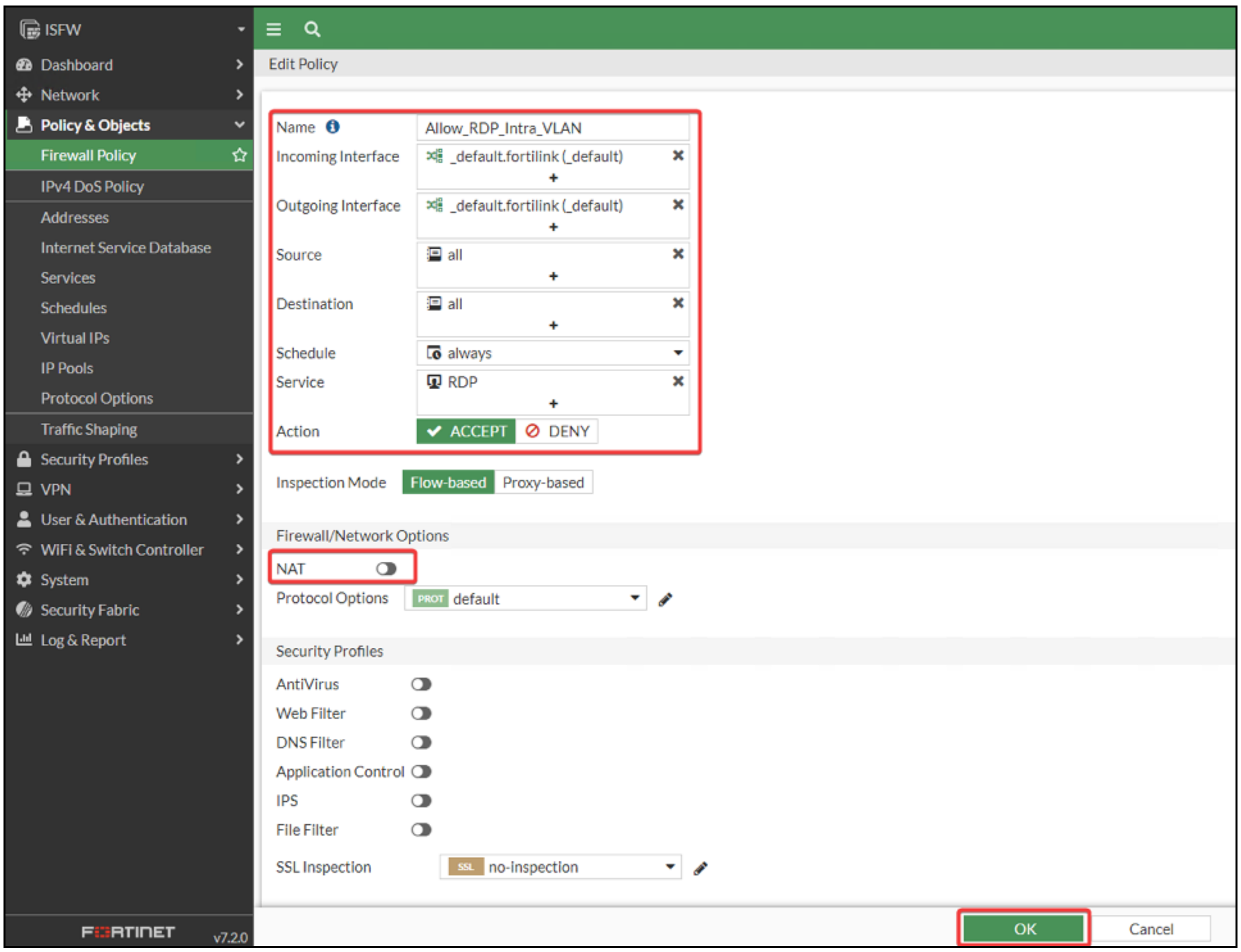
To manage traffic between endpoints

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

Field	Value
Name	Allow_RDP_Intra_VLAN
Incoming Interface	_default.fortilink (_default)
Outgoing Interface	_default.fortilink (_default)
Source	all
Destination	all

DO NOT REPRINT
© FORTINET

Field	Value
Schedule	always
Service	RDP
Action	ACCEPT
NAT	Disable
Log Allowed Traffic	All Sessions



3. Click **OK**.
4. On the ISFW FortiGate GUI, click **CLI Console**.
5. Enter the following commands to set up proxy arp for the subnet 10.1.99.x in the **_default Fortilink** interface as shown in the image below:

```
config system proxy-arp

edit 1

set interface _default

set ip 10.1.99.1
```

DO NOT REPRINT
© FORTINET


```
set end-ip 10.1.99.254
next
end
```

CLI Console (1)

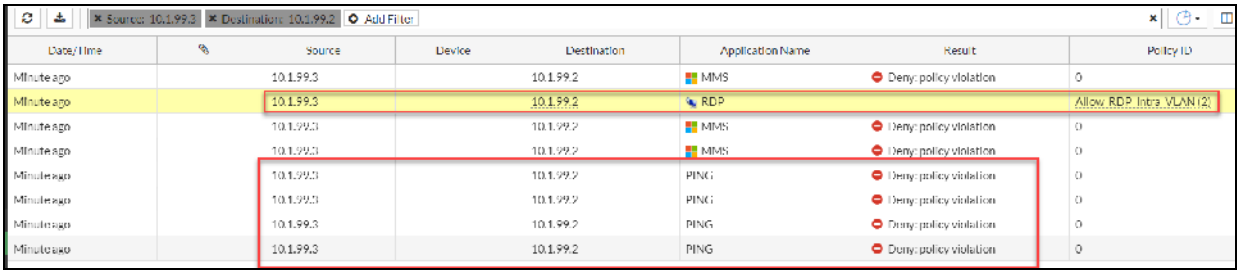
```
ISFW # config system proxy-arp

ISFW (proxy-arp) # edit 1
new entry '1' added

ISFW (1) # set interface _default

ISFW (1) # set ip 10.1.99.1

ISFW (1) # set end-ip 10.1.99.254

ISFW (1) # next

ISFW (proxy-arp) # end

ISFW #
```

6. Close the CLI console.
7. On the HR VM, open a command prompt window, and then enter the `ping` command to verify connectivity to the SALES VM, using the IP address you noted in the previous exercise.
   The pings should fail.
8. Right-click the **Windows** icon, and then click **Run**.
9. Type `mstsc`, and then click **OK** to open a Remote Desktop Connection.
10. Type `10.1.99.2`, and then click **Connect**.

If RDP fails the first time you try to connect, try again.

11. Log in with the username `student` and password `Password1!`.
12. Click **Yes**.
    You should now have RDP access to the SALES VM from the HR VM using the Remote Desktop Connection.
13. Disconnect from RDP.
14. Return to the ISFW FortiGate GUI, and then click **Log & Report** > **Forward Traffic**.
15. Add a filter for the **Source** using the IP address that you noted for the HR VM, and then add a filter for the **Destination** using the IP address that you noted for the SALES VM, as shown in the following image:

DO NOT REPRINT
© FORTINET


Source: 10.1.99.3 Destination: 10.1.99.2 Add Filter

Date/Time		Source	Device	Destination	Application Name	Result	Policy ID
Minute ago		10.1.99.3		10.1.99.2	MMS	Deny: policy violation	0
Minute ago		10.1.99.3		10.1.99.2	RDP		Allow_RDP_Intra_VLAN (2)
Minute ago		10.1.99.3		10.1.99.2	MMS	Deny: policy violation	0
Minute ago		10.1.99.3		10.1.99.2	MMS	Deny: policy violation	0
Minute ago		10.1.99.3		10.1.99.2	PING	Deny: policy violation	0
Minute ago		10.1.99.3		10.1.99.2	PING	Deny: policy violation	0
Minute ago		10.1.99.3		10.1.99.2	PING	Deny: policy violation	0
Minute ago		10.1.99.3		10.1.99.2	PING	Deny: policy violation	0

Investigate the logs and make note of the flows shown in the logs. FortiGate blocked PING traffic due to a policy violation. The **Allow_RDP_Intra_VLAN** policy you created allowed RDP access.

DO NOT REPRINT
© FORTINET

Exercise 3: Configuring Macrosegmentation

In this exercise, you will create two separate VLANs, one for the SALES VM and one for the HR VM. Next, you will restrict access between these VLANs and to the data center, providing macrosegmentation.

Create new VLAN segments for each department

You will create two new VLAN segments called HR and SALES and configure the Active Directory (AD) server in the data center as the DHCP and DNS server for these segments. We have preconfigured the AD server to act as the DHCP server for these VLANs and have configured DHCP reservations to assign specific IP addresses as shown in the lab topology.

To create VLAN segments

1. On the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **ISFW** login page bookmark.
2. Log in to the ISFW FortiGate GUI with the username `admin` and password `password`.
3. Click **WiFi & Switch Controller** > **FortiSwitch VLANs**.
4. Click **Create New**, and then configure the following settings:

Field	Value
Interface Name	SALES
VLAN ID	50
Role	LAN
IP/Netmask	10.1.50.1/24
Create address object matching subnet	Enabled
Administrative Access	Ping
DHCP Server	Enabled and click Advanced
Mode	Relay
DHCP Server IP	10.1.0.30, 10.1.0.40

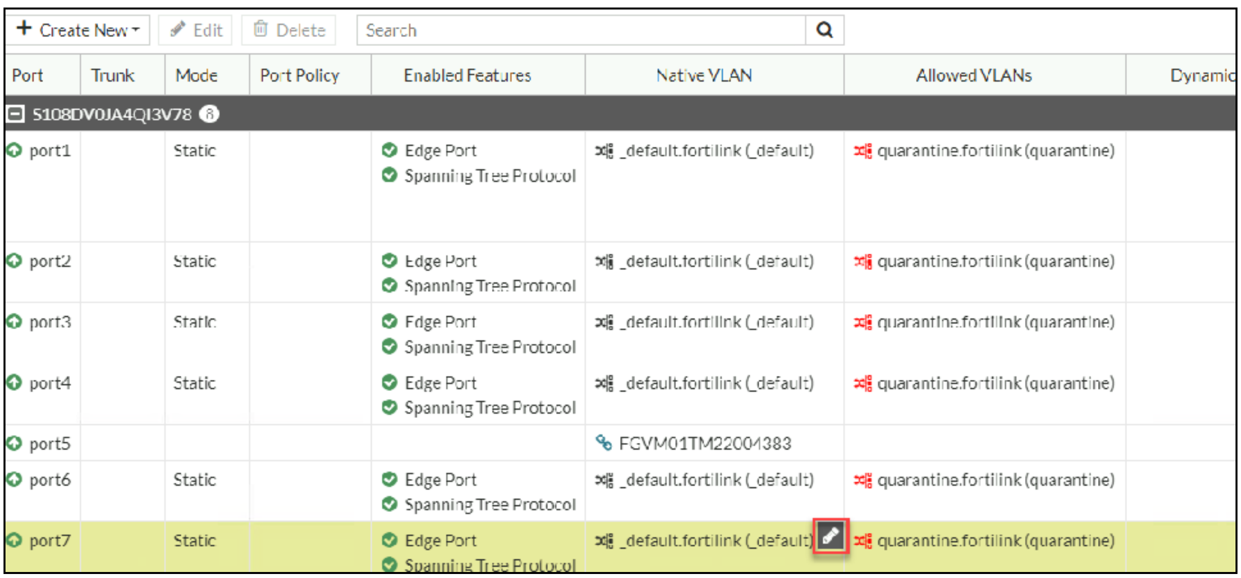
5. Click **OK**.
6. Click **Create New** to create another interface, and then configure the following settings:

Field	Value
Interface Name	HR

DO NOT REPRINT
© FORTINET

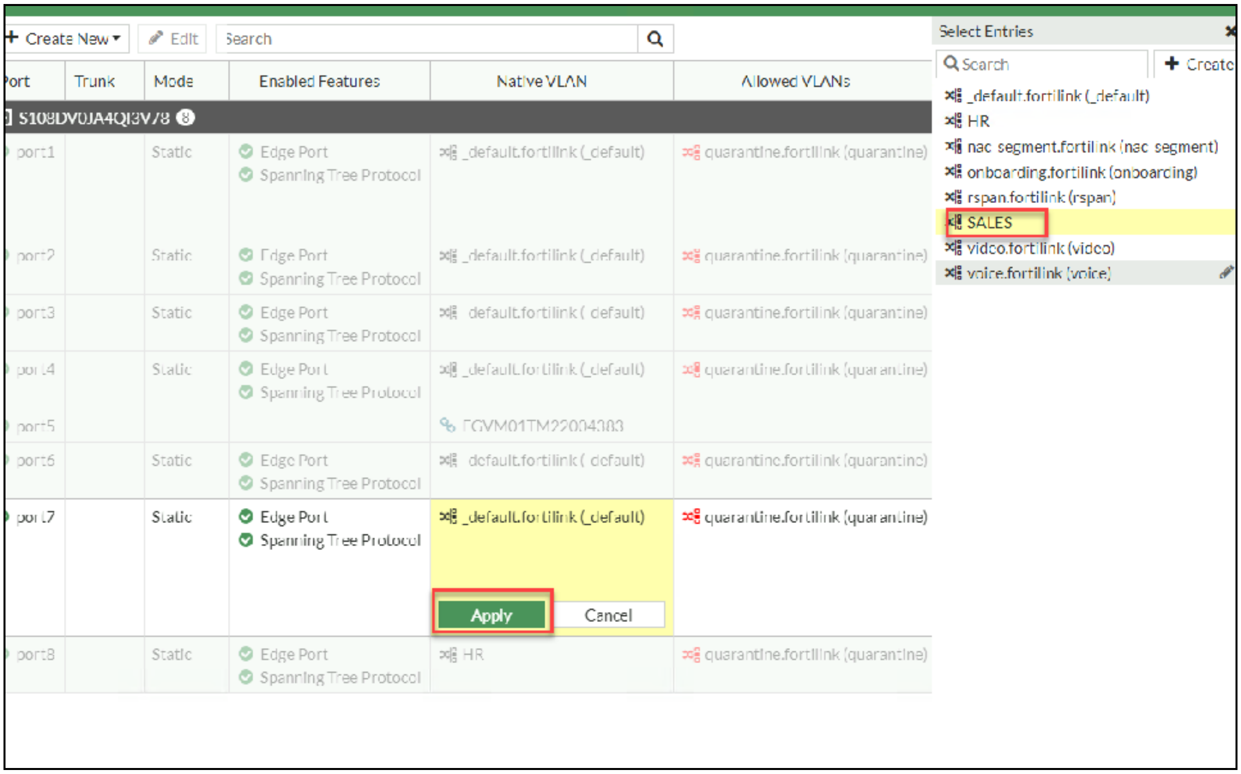
Field	Value
VLAN ID	60
Role	LAN
IP/Netmask	10.1.60.1/24
Create address object matching subnet	Enabled
Administrative Access	Ping
DHCP Server	Enabled and click Advanced
Mode	Relay
DHCP Server IP	10.1.0.30, 10.1.0.40

7. Click **OK**.
8. Click **WiFi & Switch Controller** > **FortiSwitch Ports**, and then set the native VLAN of port7 to **SALES**, and the native VLAN of port8 to **HR**.



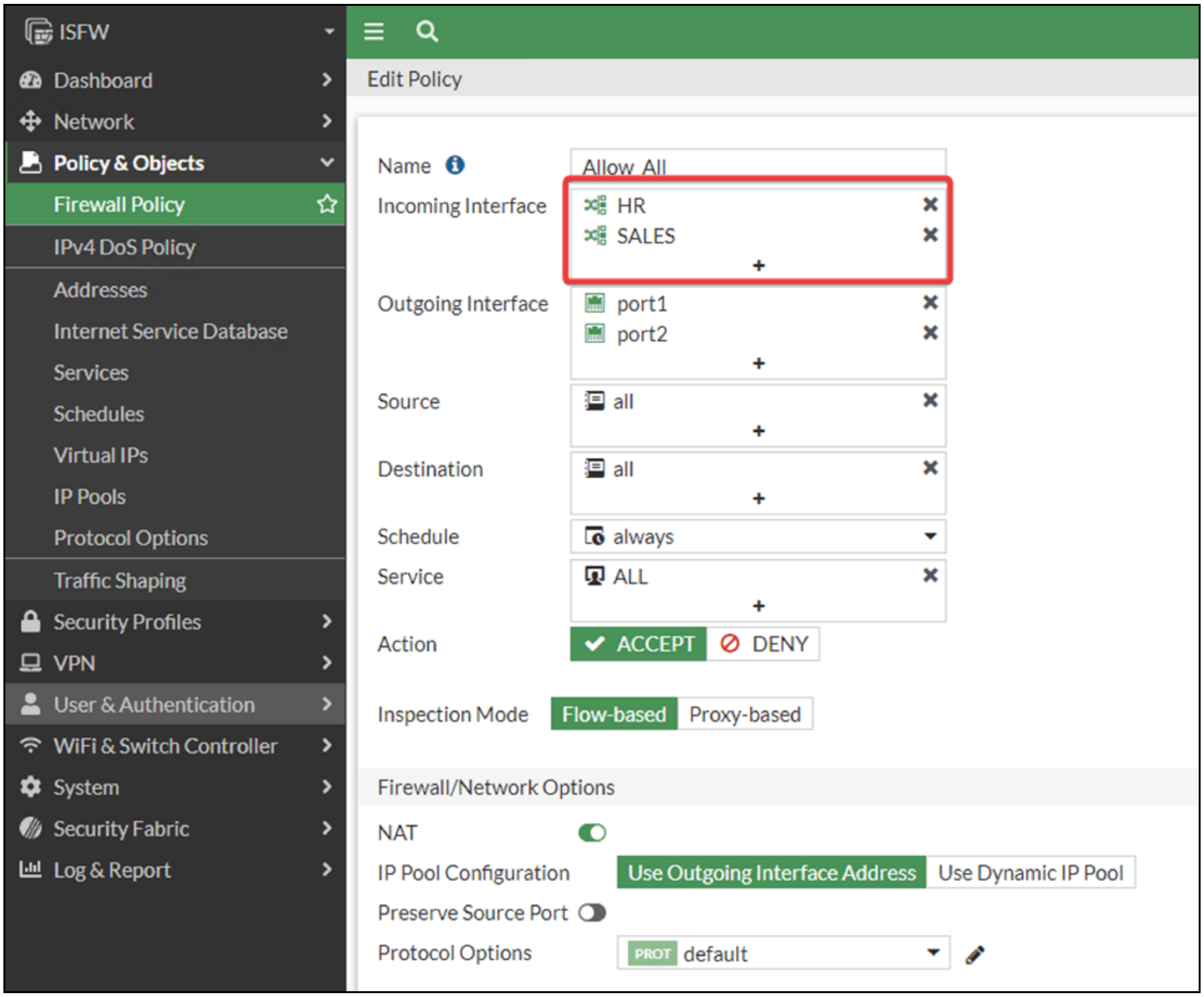
9. Click **Apply**.

DO NOT REPRINT
© FORTINET



10. Click **Policy & Objects** > **Firewall Policy**.
11. Edit the **Allow_All** policy to replace the **_default Fortilink** interface with the newly created VLAN interfaces **HR** and **SALES**. Leave all other options as is.

DO NOT REPRINT
© FORTINET



12. Click **OK** to save the changes.
13. On the HR VM, open a command prompt window, and then enter the following command:
    `ipconfig`

Does the IP address 10.1.60.2 appear? If not, enter the `ipconfig /release` and `ipconfig /renew` commands as Administrator to obtain an IP address from the newly assigned VLAN.

14. On the SALES VM, open a command prompt window, and then enter the following command:
    `ipconfig`

Does the IP address 10.1.50.2 appear? If not, enter the `ipconfig /release` and `ipconfig /renew` commands as Administrator to obtain an IP address from the newly assigned VLAN.

15. Return to the HR VM, and then enter the following command to test internet connectivity:
    `ping 1.1.1.1`
16. Enter the following command to test connectivity to the data center and the EMS server:

DO NOT REPRINT
© FORTINET


```
ping 10.1.0.30
```

17. Use the `ping` command to test connectivity to the IP addresses of FortiMail (10.1.0.60), FortiAuthenticator (10.1.0.20), FortiAnalyzer (10.1.0.10), and FortiNAC (10.1.0.40).
18. Enter the following command to test connectivity to the SALES VM:

    ```
    ping 10.1.50.2
    ```

    The ping connection should fail.
19. Continuing on the HR VM, right-click the **Windows** icon, and then click **Run**.
20. Type `mstsc`, and then click **OK** to open a Remote Desktop Connection.
21. Type `10.1.50.2`, and then click **Connect**.
    The RDP connection should fail.
22. On the SALES VM, open a command prompt window, and then use the `ping` command to test connectivity to the IP addresses of FortiMail (10.1.0.60), FortiAuthenticator (10.1.0.20), FortiAnalyzer (10.1.0.10), and FortiNAC (10.1.0.40).
23. Enter the following command to test connectivity to the HR VM:

    ```
    ping 10.1.60.2
    ```

    The ping should fail.
24. Continuing on the SALES VM, right-click the **Windows** icon, and then click **Run**.
25. Type `mstsc`, and then click **OK** to open a Remote Desktop Connection.
26. Type `10.1.60.2`, and then click **Connect**.
    The RDP connection should fail.

Stop and think!

Why we can no longer ping or RDP between the HR VM and the SALES VM?

Because there is no firewall policy allowing communication between the newly created VLANs.

27. On the ISFW FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
28. Delete the **Allow_RDP_Intra_VLAN** policy.
    You no longer require the intraVLAN traffic policy on the _default FortiLink interface.

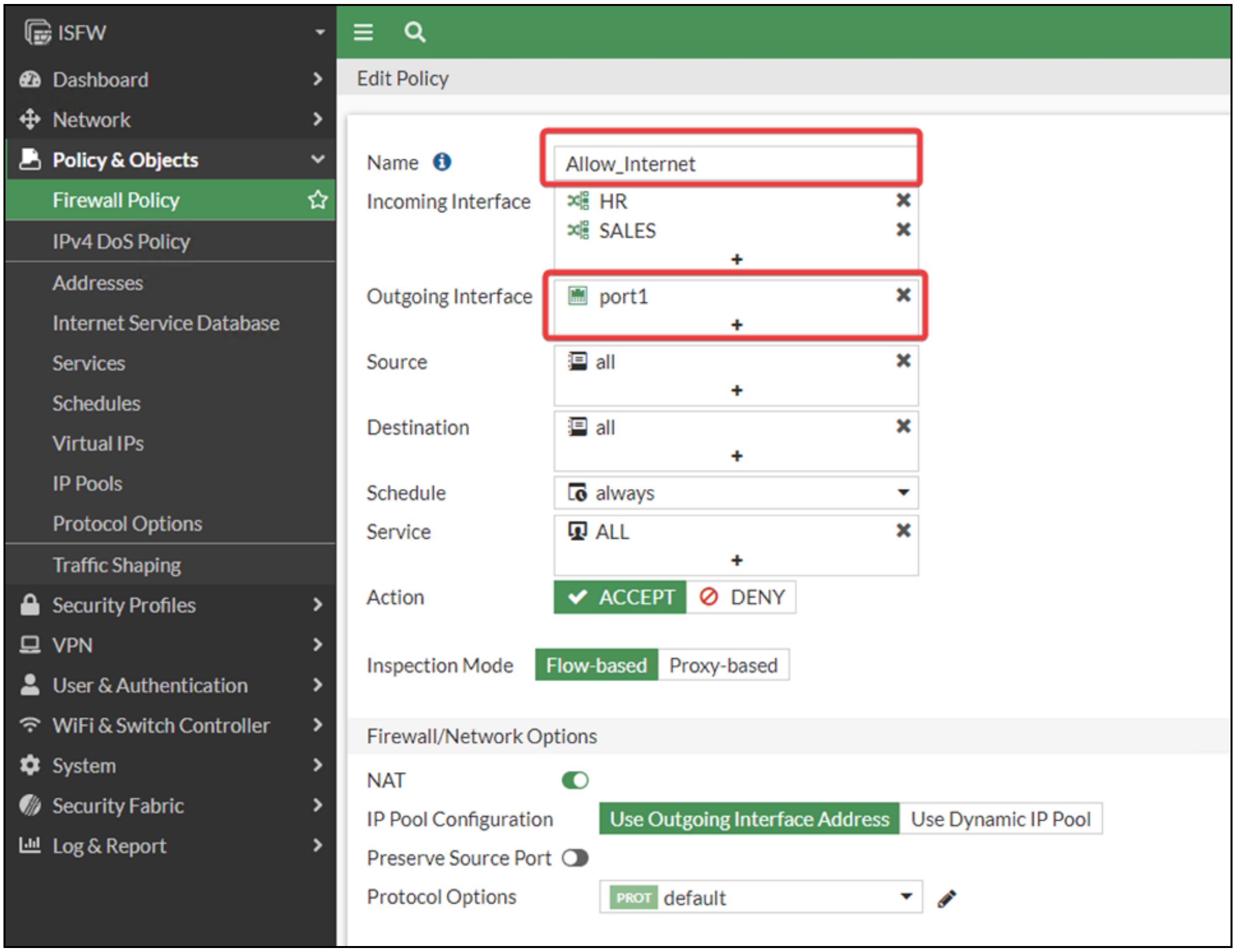
Restrict Access to the Data Center

You will create a firewall policy to restrict access to the data center. You will limit access to Active Directory, FortiClient EMS, FortiAuthenticator, and FortiMail.

To restrict access to the data center

1. Continuing on the ISFW FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. Edit the **Allow_All** policy to rename it to `Allow_Internet`, and then remove **port2** from the outgoing interface to remove DC access. Leave all other options as shown in the following image:

DO NOT REPRINT
© FORTINET

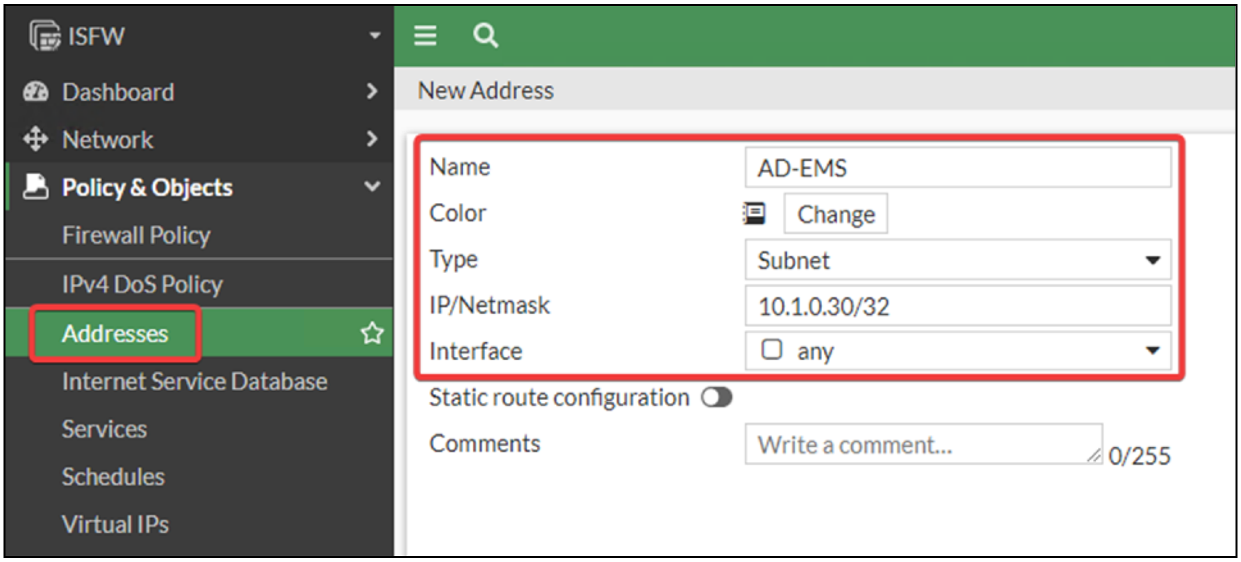


3. Click **OK**.
4. Click **Policy & Objects** > **Addresses**.
5. Click **Create New** > **Address**, and then configure the following settings:

Field	Value
Name	AD-EMS
Type	Subnet
IP/Netmask	10.1.0.30/32
Interface	any

6. Click **OK**.

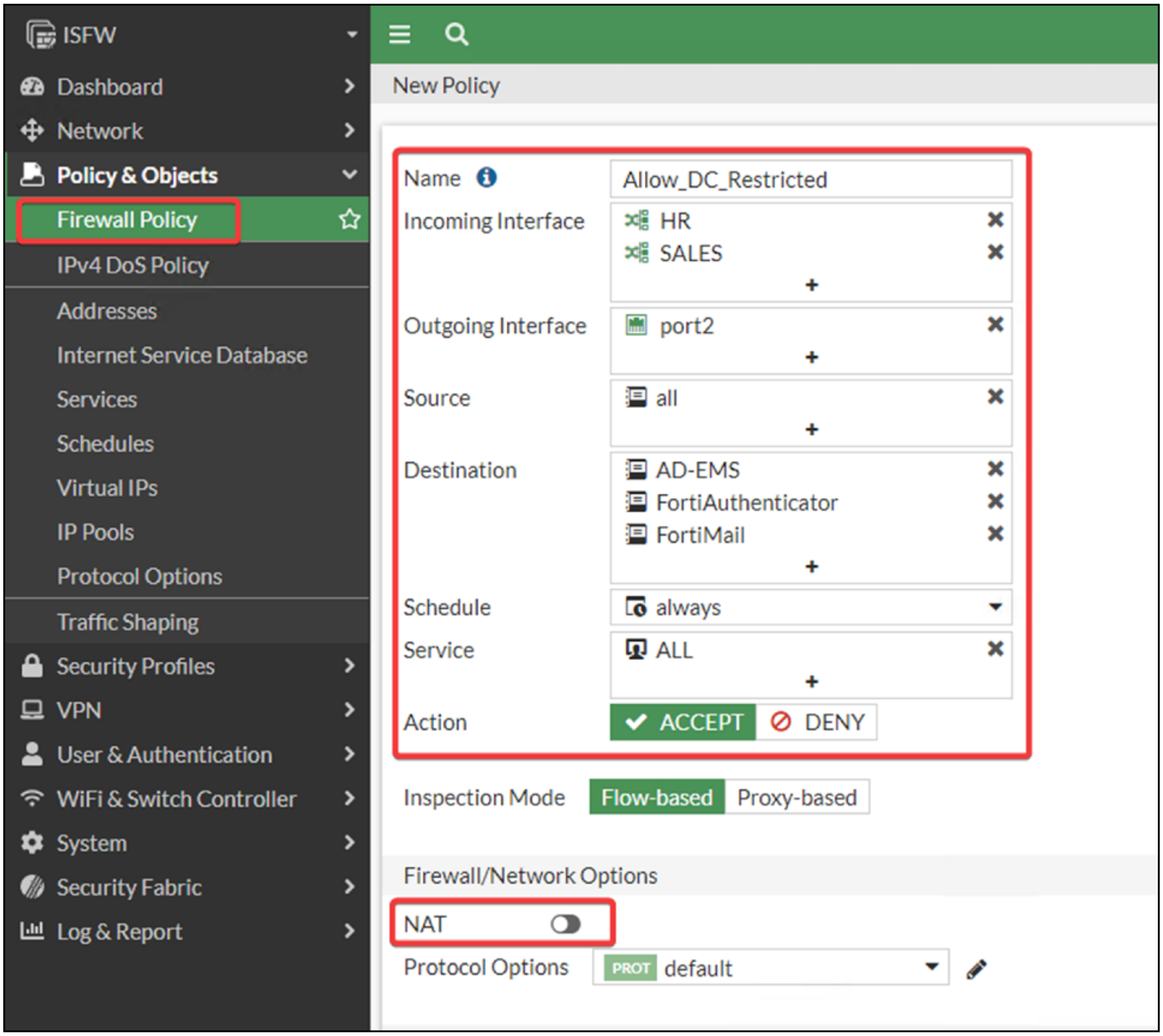
DO NOT REPRINT
© FORTINET



7. Repeat steps 4 and 5 to create address objects for FortiAuthenticator `10.1.0.20/32` and FortiMail `10.1.0.60/32`.
8. Click **Policy & Objects** > **Firewall Policy**.
9. Click **Create New**, and then configure the following settings to create a firewall policy to allow access to Active Directory/EMS, FortiAuthenticator, and FortiMail:

Field	Value
Name	Allow_DC_Restricted
Incoming Interface	HR, SALES
Outgoing Interface	port2
Source	all
Destination	AD-EMS, FortiAuthenticator, FortiMail
Schedule	always
Service	ALL
Action	ACCEPT
NAT	Disabled
Log Allowed Traffic	All Sessions

DO NOT REPRINT
© FORTINET



10. Click **OK**.
11. On both the SALES VM and the HR VM, enter the following commands to test connectivity to AD-EMS and FortiAuthenticator:

```
ping 10.1.0.30
```

```
ping 10.1.0.20
```

12. Visit `https://fml.ftnt.lab` to test connectivity to the FortiMail GUI.
13. Visit `10.1.0.10` to test connectivity to FortiAnalyzer and `10.1.0.40` to test connectivity to FortiNAC.

    You should not be able to access FortiAnalyzer or FortiNAC because the new firewall policy allows access only to AD-EMS, FortiAuthenticator, and FortiMail.

DO NOT REPRINT
© FORTINET

Exercise 4: Using a VPN for Remote Access

In this exercise, you will allow remote access to the SALES and HR subnets using SSL-VPN. Next, you will demonstrate some of the security risks and limitations of using VPN and zero trust access.

Set up a Remote Access VPN

You will create an SSL-VPN policy on NGFW to allow remote users to access the HR and SALES subnets via the ISFW firewall.

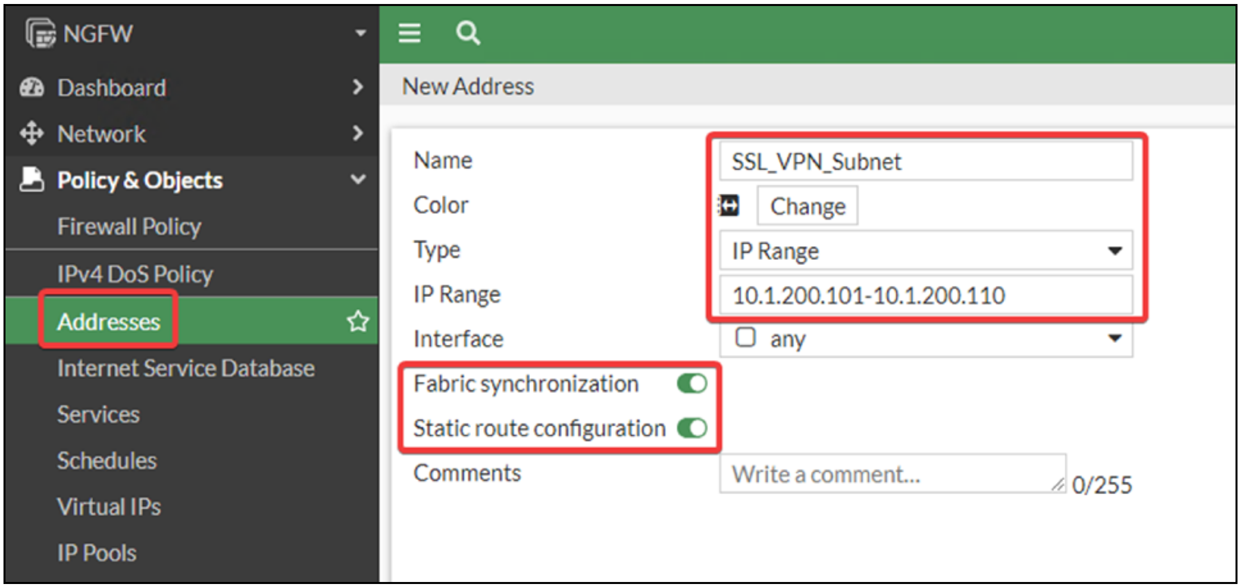
To create VLAN segments

1. On the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **NGFW** login page bookmark.
2. Log in with the username `admin` and password `password`.
3. Click **Policy & Objects** > **Addresses**.
4. Click **Create New** > **Address**, and then configure the following settings:

Field	Value
Name	SSL_VPN_Subnet
Type	IP Range
IP Range	10.1.200.101-10.1.200.110
Interface	any
Fabric synchronization	Enabled
Static route configuration	Enabled

5. Click **OK**.

DO NOT REPRINT
© FORTINET



6. Repeat the process to create an address object for an HR subnet with the following settings:

Field	Value
Name	HR_Subnet
IP/Netmask	10.1.60.0/24
Type	Subnet
Fabric synchronization	Enabled
Static route configuration	Enabled

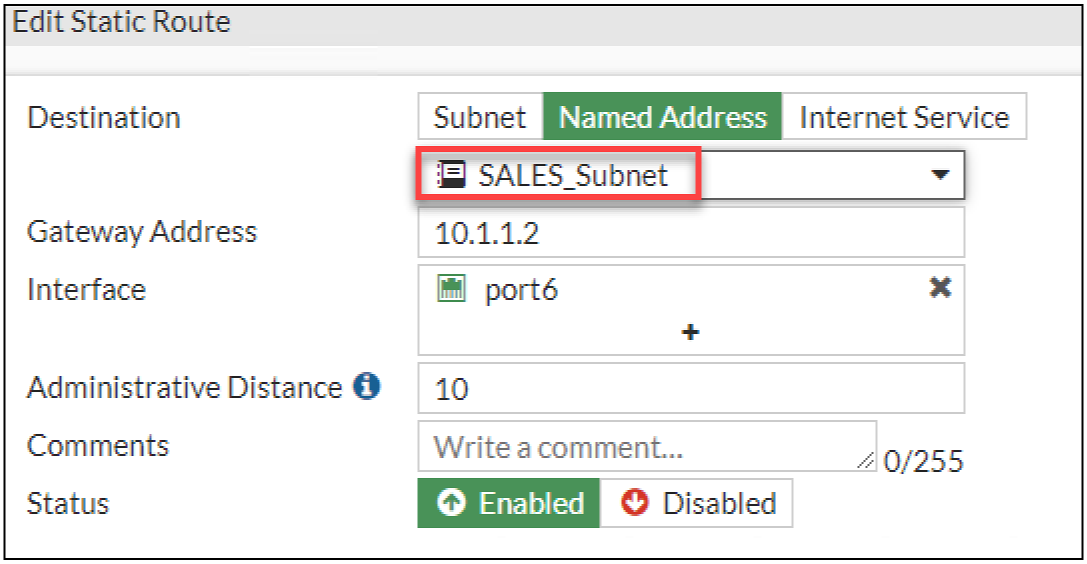
7. Repeat again to create an address object for a Sales subnet with the following settings:

Field	Value
Name	SALES_Subnet
IP/Netmask	10.1.50.0/24
Type	Subnet
Fabric synchronization	Enabled
Static route configuration	Enabled

8. Click **Network** > **Static Routes**.
9. Click **Create New**, and then configure the following settings:

DO NOT REPRINT
© FORTINET

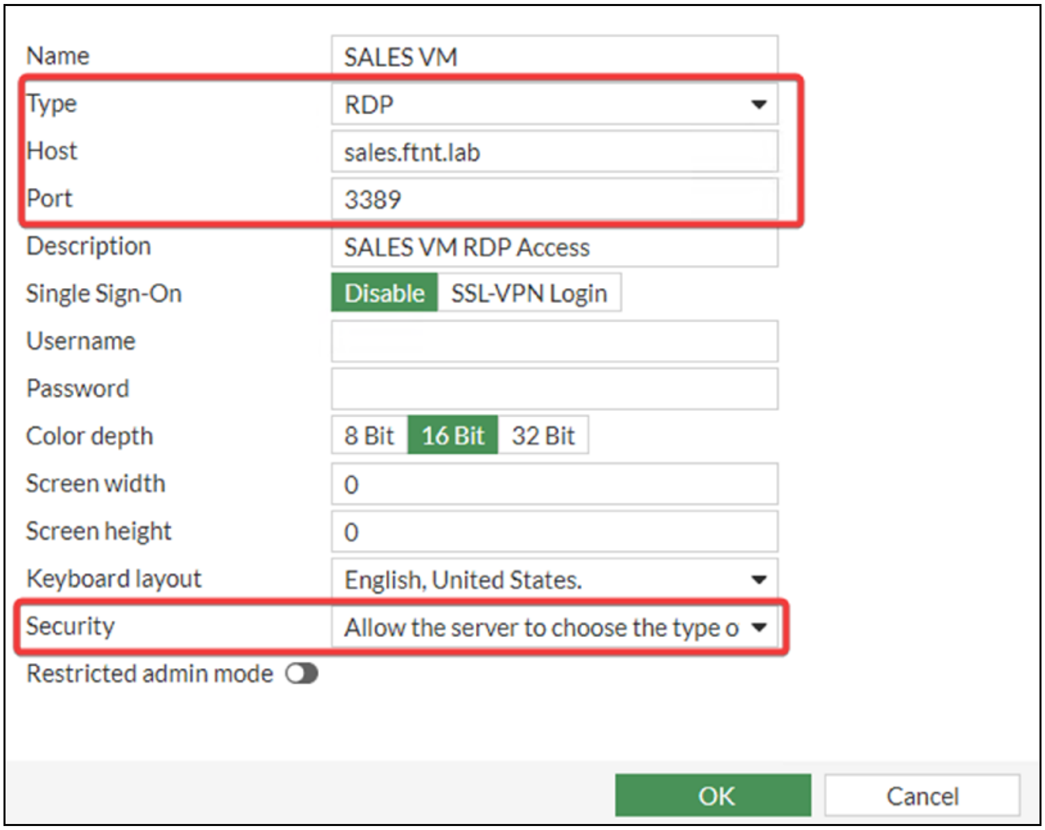
Field	Value
Destination	Named Address
Destination (drop-down list)	SALES_Subnet
Gateway Address	10.1.1.2
Interface	port6



10. Click **OK**.
11. Repeat the process to create a route for the HR subnet.
12. Click **VPN** > **SSL-VPN Portals**, and then edit the **full-access** portal.
13. Replace **Source IP Pools** with the **SSL_VPN_Subnet** address object.
14. Enable the following options: **Allow client to save password**, **Allow client to connect automatically**, and **Allow client to keep connections alive.**
15. Click **Create New** in the **Predefined Bookmarks** section, and then configure the following settings:

Field	Value
Name	SALES VM
Type	RDP
Host	sales.ftnt.lab
Port	3389
Security	Allow the server to choose the type of security

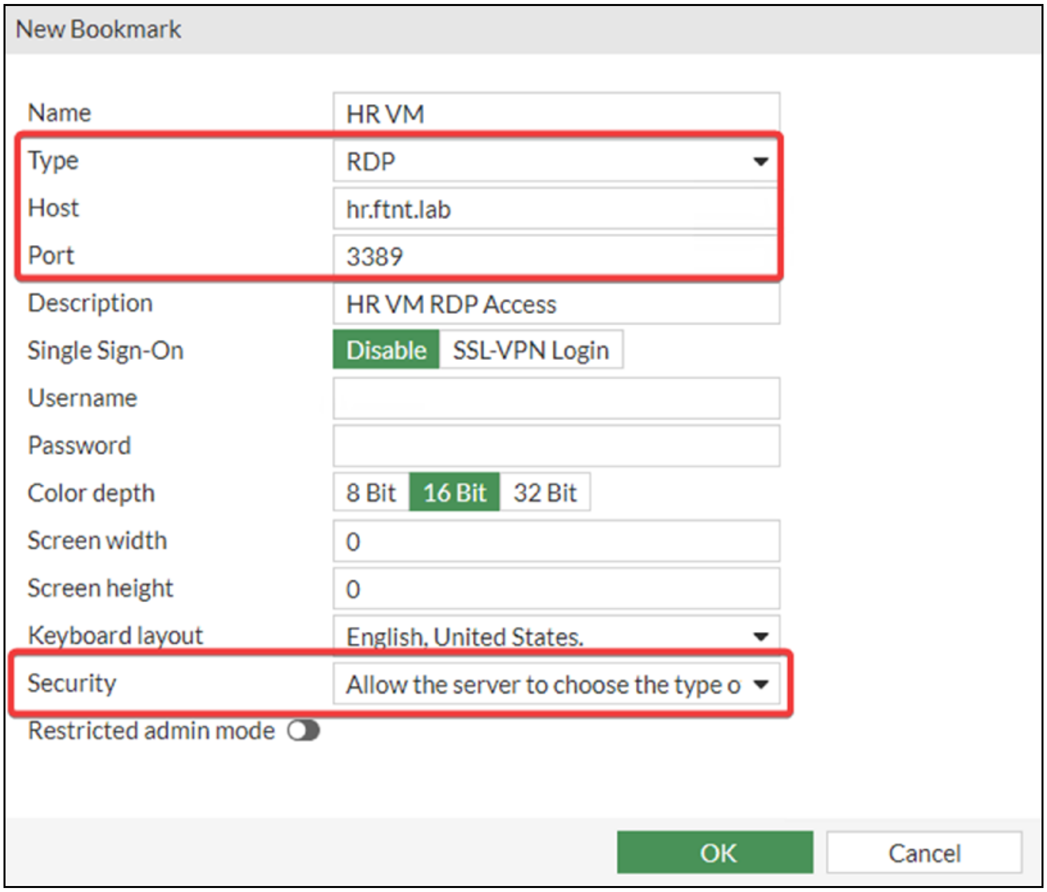
DO NOT REPRINT
© FORTINET



16. Click **OK**.
17. Click **Create New** in the **Predefined Bookmarks** section again, and then configure the following settings:

Field	Value
Name	HR VM
Type	RDP
Host	hr.ftnt.lab
Port	3389
Security	Allow the server to choose the type of security

DO NOT REPRINT
© FORTINET

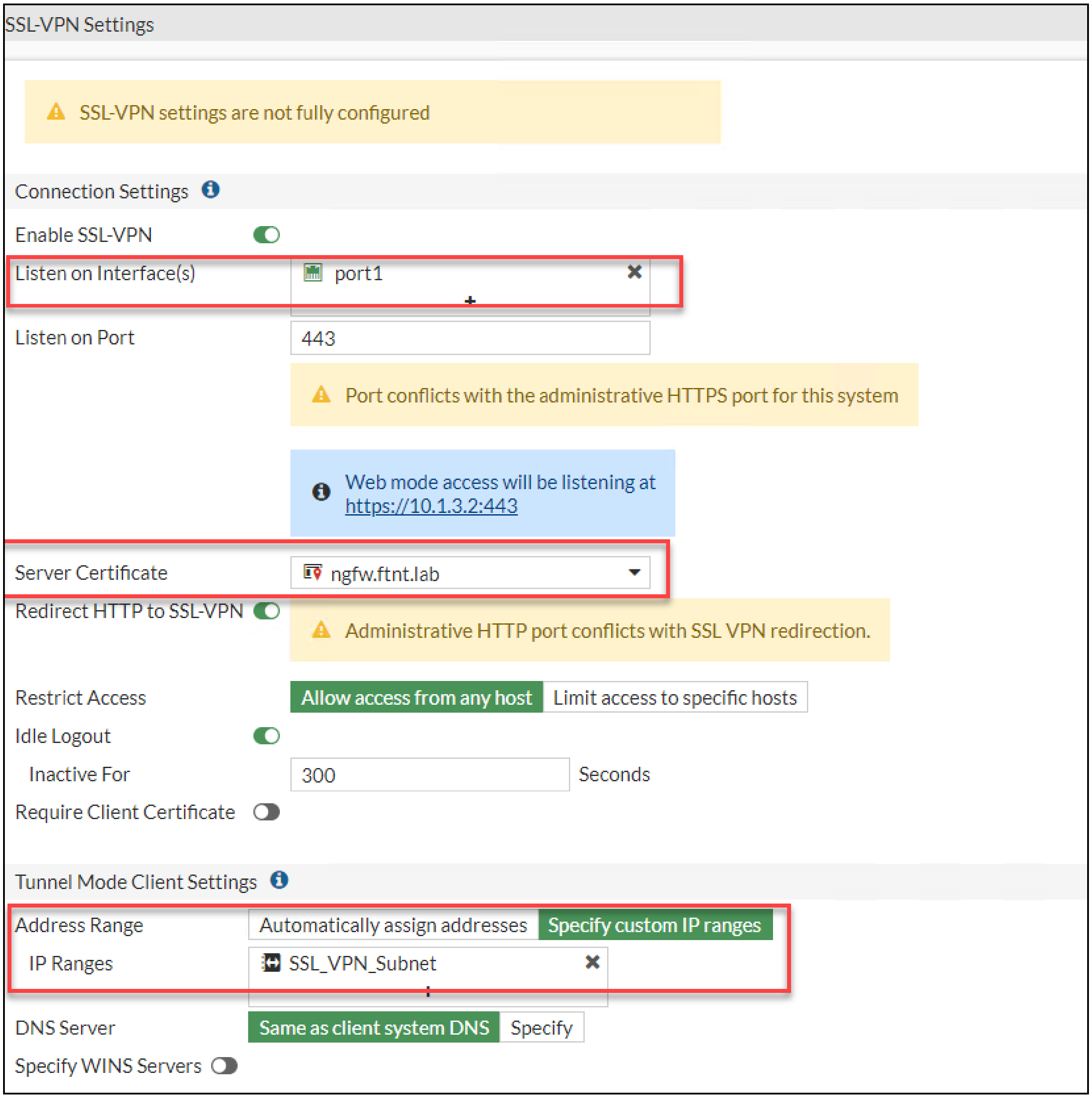


18. Click **OK**.
19. Click **OK** to save the changes.
20. Click **User & Authentication** > **User Groups**.
21. Click **Create New**.
22. In the **Name** field, type `SSL_VPN_Users`, and then click **+** for **Members**.
23. Click **Create** > **User**.
24. Select **Local User**, and then click **Next**.
25. In the **Username** field, type `remote`, in the **password** field, type `password`, and then click **Next**.
26. Leave **Two-Factor Authentication** disabled, and then click **Next**.
27. Verify that the **User Account Status** is **Enabled**, and then click **Submit**.
28. Select **remote**, and then click **OK**.
29. Click **VPN** > **SSL-VPN Settings**, and then configure the following settings:

Field	Value
Enable SSL-VPN	Enabled
Listen on Interface(s)	port1
Listen on Port	443

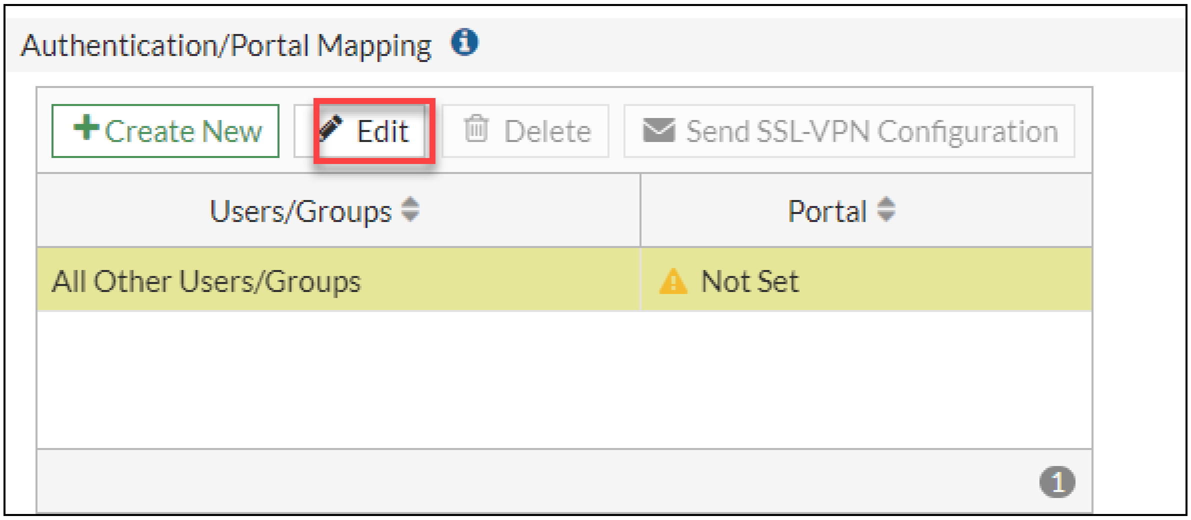
DO NOT REPRINT
© FORTINET

Field	Value
Server Certificate	ngfw.ftnt.lab
Redirect to HTTP to SSL-VPN	Enabled
Address Range	Specify custom IP ranges
IP Ranges	SSL_VPN_Subnet



30. In the **Authentication/Portal Mapping** section, edit **All Other Users/Groups**.

DO NOT REPRINT
© FORTINET



31. In the **Portal** field, select **full-access**.
32. Click **OK**.
33. Click **Apply**.
34. Click **Policy & Objects** > **Firewall Policy**.
35. Click **Create New**, and then configure the following settings:

Field	Value
Name	Remote_Access_VPN
Incoming Interface	SSL-VPN tunnel interface (ssl.root)
Outgoing Interface	port6
Source	Address: SSL_VPN_Subnet User: SSL_VPN_Users
Destination	HR_Subnet, SALES _Subnet
Schedule	Always
Service	ALL
Action	ACCEPT
NAT	Disabled
Log Allowed Traffic	All Sessions

36. Click **OK**.
37. Return to the ISFW FortiGate GUI, and then click **Policy & Objects** > **Addresses**.
38. Click **Create New** > **Address**, and then configure the following settings to create an address object for the egress interface:

    Use the IP address of the NGFW FortiGate firewall that SSL-VPN users will use in web access mode.

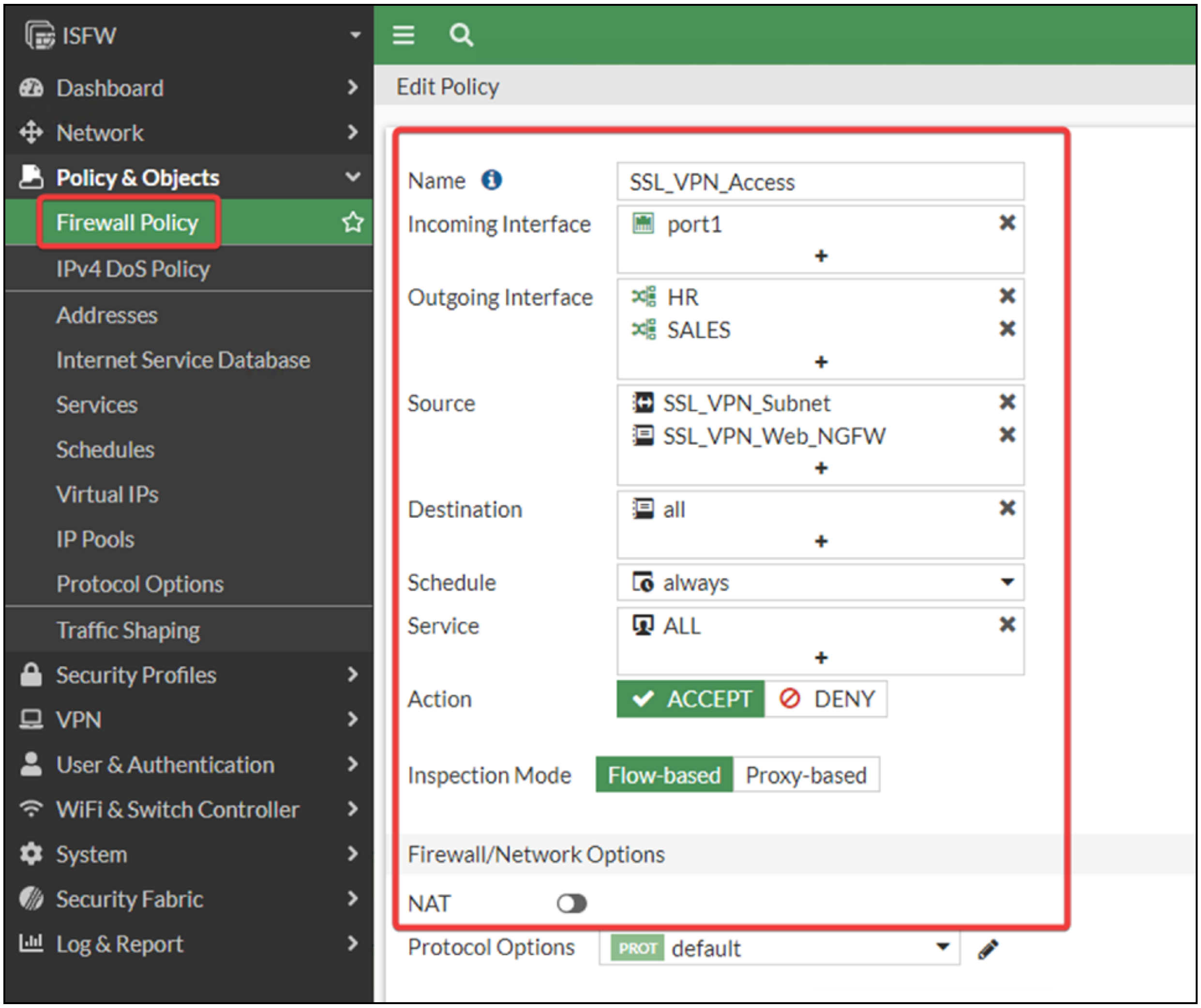
DO NOT REPRINT
© FORTINET

Field	Value
Name	SSL_VPN_Web_NGFW
Type	Subnet
IP Range	10.1.1.1 255.255.255.255
Interface	any

39. Click **OK**.
40. Click **Policy & Objects** > **Firewall Policy**.
41. Click **Create New**, and then configure the following settings:

Field	Value
Name	SSL_VPN_Access
Incoming Interface	port1
Outgoing Interface	HR, SALES
Source	SSL_VPN_Subnet SSL_VPN_Web_NGFW
Destination	All
Schedule	Always
Service	ALL
Action	ACCEPT
NAT	Disabled
Log Allowed Traffic	All Sessions

DO NOT REPRINT
© FORTINET



42. Click **OK**.

Examine the Security Limitations of VPNs

You will demonstrate how an attacker could potentially use a compromised endpoint with VPN access to laterally move within a corporate network and increase its privileges.

To demonstrate the security limitations of a VPN

1. Open an RDP connection to the remote VM, open Google Chrome, and then in **Bookmarks**, select the **SSL-VPN Webmode** login page bookmark.
2. Log in with the username `remote` and password `password`.

   You should see bookmarks for the SALES VM and the HR VM.
3. Click the **SALES VM** bookmark.
4. Log in with the username `student` and password `Password1!`.

DO NOT REPRINT
© FORTINET

5. Return to the **SSL-VPN Portal** tab in Google Chrome, and then in **Bookmarks**, select the **HR VM** bookmark.
6. Log in with the username `student` and password `Password1!`.

Stop and think!

How can a compromised endpoint move laterally and increase its privileges?

Although you were granted access only to HR VM, since you have RDP access to HR VM, you can access any endpoints the HR VM can access.

7. Continuing on the HR VM, right-click the **Windows** icon, and then click **Run**.
8. Type `mstsc`, and then click **OK** to open the Remote Desktop Connection.
9. Type `10.1.0.30` for the IP address of Active Directory, and then click **Connect**.
10. Log in with the username `FTNT\Administrator` and password `Password1!`.
11. Click **Yes**.
12. Open Google Chrome, and then in **Bookmarks**, select the **FortiAnalyzer** login page bookmark.
13. Repeat the previous step for the NGFW, ISFW, and DCFW login page bookmarks.

Stop and think!

Did you allow VPN access to data center resources?

Did the HR VM have access to FortiAnalyzer, ISFW, DCFW, and so on?

RDP hopping is a popular technique that attackers use to move laterally within a network and gradually increase their privileges to compromise the entire organization. Although this exercise simplifies the attack using known credentials, attackers use multiple tools to dump passwords, scan networks, and escalate privileges.

14. Disconnect the RDP session.
15. Close the HR VM and SALES VM sessions.
16. Log out of the SSL-VPN Web Mode page.

DO NOT REPRINT
© FORTINET

Lab 2: Zero Trust Components

In this lab, you will add certificate authentication to the existing SSL VPN configuration. Next, you will configure authentication for domain and non-domain users. You will also add FortiClient EMS to the Fortinet Security Fabric to extend the zero-trust infrastructure.

Objectives

- Enable two-factor authentication for SSL VPN with digital certificates
- Create a PKI user and install the CA-signed user certificate
- Configure FSSO authentication for domain computers
- Configure LDAP authentication for non-domain computers (BYOD)
- Add FortiClient EMS to the Security Fabric

Time to Complete

Estimated: 60 minutes

Prerequisites

Before you begin this lab, you must complete Lab 1 so that you can continue with the SSL VPN configuration.

DO NOT REPRINT
© FORTINET

Exercise 1: Configuring SSL VPN With Digital Certificates

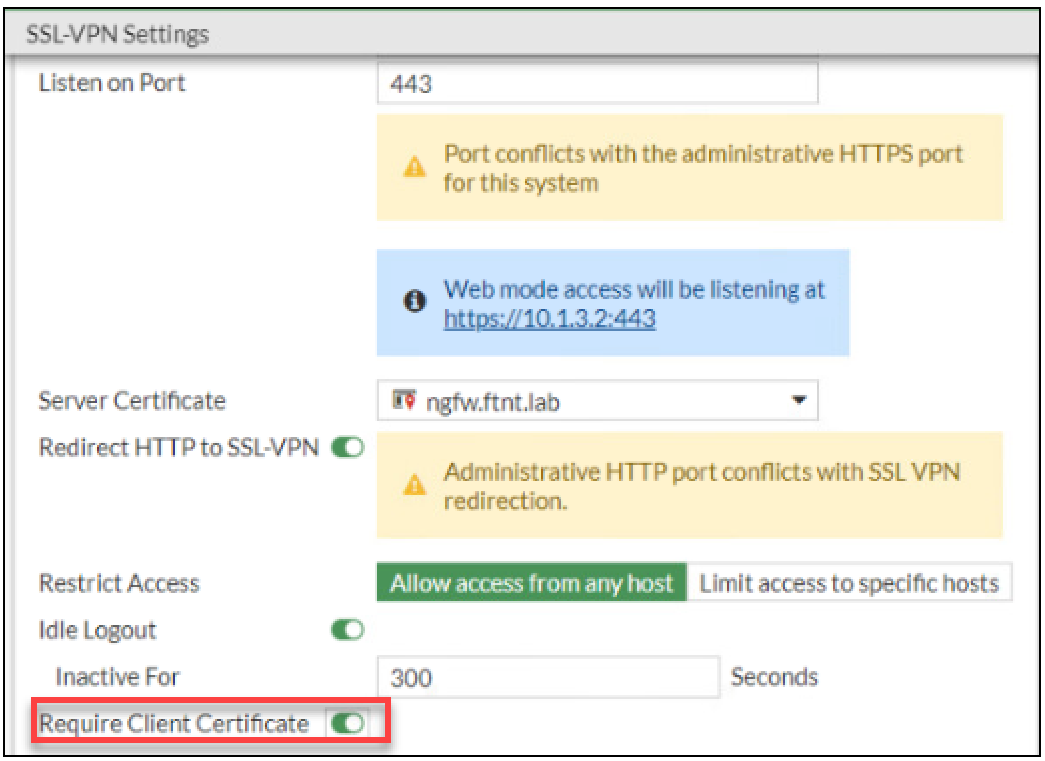
In this exercise, you will enable certificate-based authentication for SSL VPN.

Configure SSL VPN for Certificate-Based Authentication

You will enable certificate-based authentication for the SSL VPN client.

To configure SSL VPN for certificate-based authentication

1. On the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **NGFW** FortiGate login page bookmark.
2. Log in to the NGFW FortiGate GUI with the username `admin` and password `password`.
3. Click **VPN** > **SSL-VPN Settings**.
4. Enable **Require Client Certificate**.



5. Click **Apply**.
6. Open PuTTY, and then connect over SSH to the **NGFW**saved session.
7. Log in with the username `admin` and password `password`.
8. Enter the following commands to enable the real-time debug:

```
diag debug application sslvpn -1
diag debug enable
```

DO NOT REPRINT
© FORTINET

9. On the Remote VM, open Firefox, and then in **Bookmarks**, select the **SSL-VPN Webmode** login page bookmark.
10. In the **User Identification Request** window, click **OK**.
11. Log in with the username `remote` and password `password`.

    You should receive a permission denied error.

FortiClient is configured on the Remote VM and is connected to FortiClient EMS. FortiClient EMS has signed the client certificate and it is installed on the endpoint. When you try to connect to the SSL VPN in web mode, the browser tries to use the FortiClient EMS certificate, and it will fail because it is not a vaild SSL VPN certificate.

---

12. Return to the PuTTY session that was running the real-time debug, and then analyze its output.

    You should see some of the logs that appear in the following image:

```
NGFW # [796:root:50]allocSSLConn:303 sconn 0x7f9898af7b00 (0:root)
[796:root:50]SSL state:before SSL initialization (10.1.10.2)
[796:root:50]SSL state:before SSL initialization (10.1.10.2)
[796:root:50]no SNI received
[796:root:50]client cert requirement: yes
[796:root:50]SSL state:SSLv3/TLS read client hello (10.1.10.2)
[796:root:50]SSL state:SSLv3/TLS write server hello (10.1.10.2)
[796:root:50]SSL state:SSLv3/TLS write change cipher spec (10.1.10.2)
[796:root:50]SSL state:TLSv1.3 early data (10.1.10.2)
[796:root:50]SSL state:TLSv1.3 early data:system lib(10.1.10.2)
[796:root:50]SSL state:TLSv1.3 early data (10.1.10.2)
[796:root:50]no SNI received
[796:root:50]client cert requirement: yes
[796:root:50]SSL state:SSLv3/TLS read client hello (10.1.10.2)
[796:root:50]SSL state:SSLv3/TLS write server hello (10.1.10.2)
[796:root:50]SSL state:TLSv1.3 write encrypted extensions (10.1.10.2)
[796:root:50]SSL state:SSLv3/TLS write certificate request (10.1.10.2)
[796:root:50]SSL state:SSLv3/TLS write certificate (10.1.10.2)
[796:root:50]SSL state:TLSv1.3 write server certificate verify (10.1.10.2)
[796:root:50]SSL state:SSLv3/TLS write finished (10.1.10.2)
[796:root:50]SSL state:TLSv1.3 early data (10.1.10.2)
[796:root:50]SSL state:TLSv1.3 early data:system lib(10.1.10.2)
[796:root:50]SSL state:TLSv1.3 early data (10.1.10.2)
[796:root:50]SSL certificate verification: unable to get local issuer certificate
[796:root:0]Cert verification: can't find CA cert locally
```

13. Enter the following CLI command to disable the real-time debug, and then close the SSH connection:

```
diagnose debug disable
```

You have enabled **Require Client Certificate** for the SSL VPN connection, and the **remote** user configured in Lab 1 does not have a client certificate configured.

DO NOT REPRINT
© FORTINET

Exercise 2: Creating a PKI User and Installing the CA-Signed User Certificate

In this exercise, FortiAuthenticator is the certificate authority (CA) for your PKI infrastructure. You will create a local PKI user on FortiGate for SSL VPN, with two-factor authentication.

Create a PKI User

You will create a PKI user for certificate-based authentication. This user will be authorized to connect to the SSL VPN portal. Because the GUI does not display PKI users until you create the first PKI user, you will create the first PKI user on the CLI. You will also enable two-factor authentication, so that clients must present valid credentials in addition to presenting a valid signed certificate.

To create a PKI user

1. On the FortiClient EMS VM, open PuTTY, and then connect over SSH to the **NGFW** saved session.
2. Log in with the username `admin` and password `password`.
3. Enter the following commands to create the PKI user:

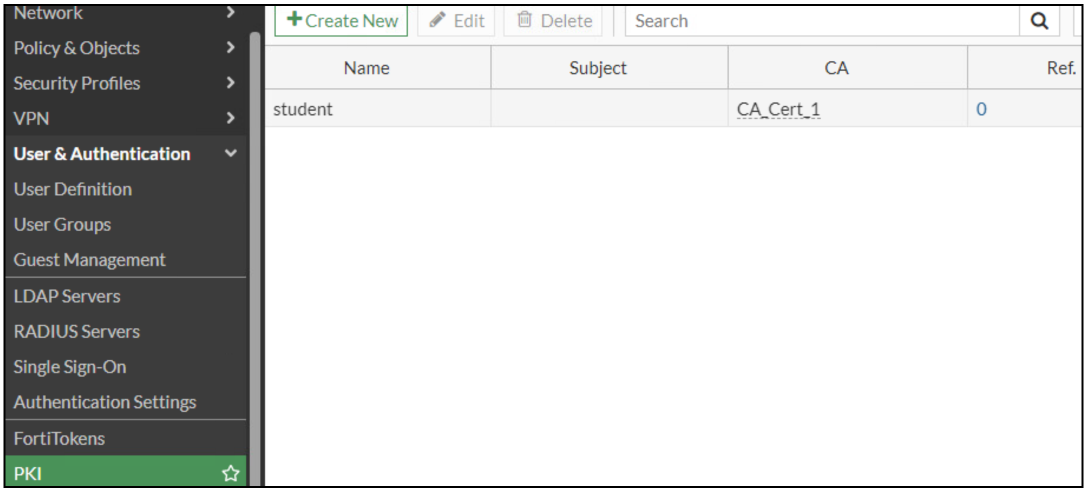
```
config user peer
   edit "student"
      set ca CA_Cert_1
      set cn student
      set two-factor enable
      set passwd password
   next
end
```

The FortiAuthenticator that you will use in this lab already has a CA. The CA certificate **CA_Cert_1** has already been imported into the FortiGate from FortiAuthenticator. The CN value is case sensitive and it should match the user certificate you create on FortiAuthenticator.

4. Refresh the NGFW FortiGate GUI page.
5. Click **User & Authentication** > **PKI**.

   After you create the first PKI user on the CLI, you can see the PKI users on the GUI.

DO NOT REPRINT
© FORTINET

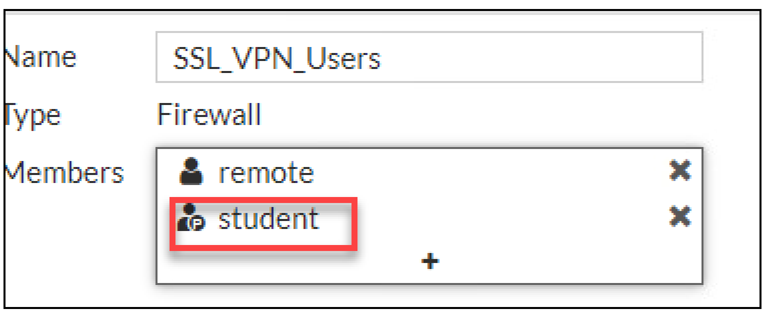


Add the PKI User to the Existing SSL VPN Group

You will add the new **student** PKI user to the **SSL_VPN_Users** user group for SSL VPN access.

To add the PKI user to the user group

1. Continuing on the NGFW FortiGate GUI, click **User & Authentication** > **User Groups**.
2. Edit the **SSL_VPN_Users** user group.
3. In the **Members** field, click **+**, and then select **student**.



4. Click **OK**.

Generate a CA-Signed User Certificate on FortiAuthenticator

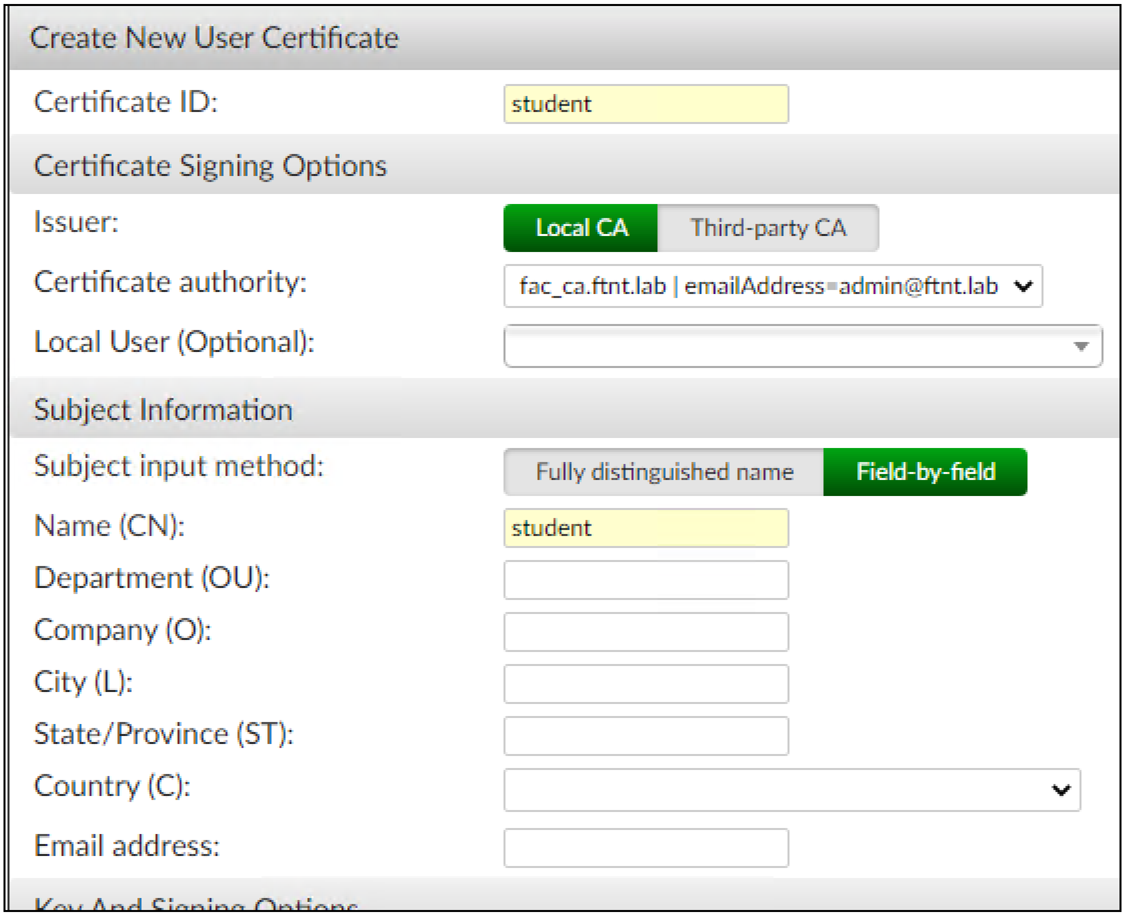
You will generate a user certificate that FortiAuthenticator signs, and then you will install it on the Remote VM. FortiAuthenticator is a CA that FortiGate trusts.

To generate a CA-signed user certificate

1. On the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **FortiAuthenticator** login page bookmark.
2. Log in to the FortiAuthenticator GUI with the username `admin` and password `password`.
3. Click **Certificate Management** > **End Entities** > **Users**.

DO NOT REPRINT
© FORTINET

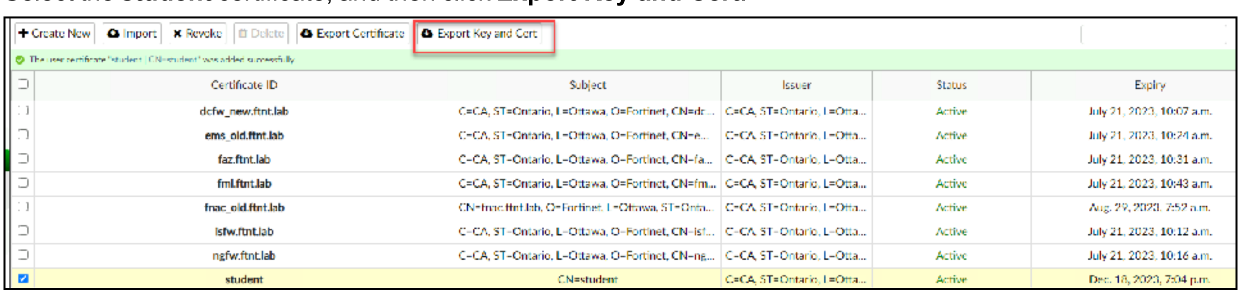
4. Click **Create New**.
5. In the **Certificate ID** field, type `student`.
6. In the **Name (CN)** field, type `student`.



7. Click **OK**.

To download the user certificate

1. Continuing on the FortiAuthenticator GUI, click **Certificate Management** > **End Entities** > **Users**.
2. Select the **student** certificate, and then click **Export Key and Cert**.



3. In the **Passphrase** field, type `fortinet`, and then in the **Confirm Passphrase** field, type `fortinet` again.
4. Click **OK**.
5. Click **Download PKCS#12 file**.
6. Click **Finish**.

DO NOT REPRINT
© FORTINET

To send the user certificate to the end user

1. Continuing on the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **FortiMail-Webmail** login page bookmark.
2. Log in with the username `student` and password `Password1!`.
3. Click the **Compose Mail** icon, and then compose a new email using the following information:

Field	Value
To	remote@ftnt.lab
Subject	User certificate
Message Body	User certificate

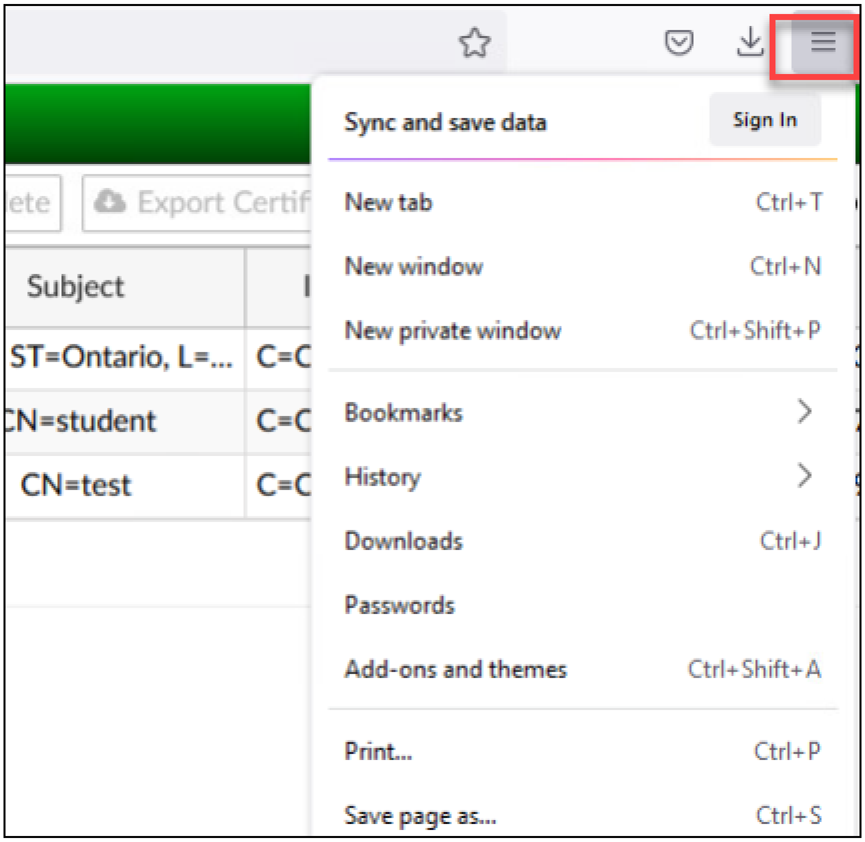
4. Click the attachment icon ( ).
5. Click **Downloads** > **student**, and then click **Open**.
6. Click **Send**.
7. Log out of FortiMail webmail.
8. On the Remote VM, open Firefox, and then in **Bookmarks**, select the **FortiMail-Webmail** login page bookmark.
9. Log in with the username `remote` and password `Password1!`.
10. Open the new email from **student@ftnt.lab**.
11. Click **student.p12**.

    This file should download to the **Downloads** directory.
12. Log out of FortiMail webmail.

To install the user certificate

1. Continuing on the Remote VM, click **Open** to open the Firefox settings.

DO NOT REPRINT
© FORTINET



2. Click **Settings**.
3. Click **Privacy & Security**.
4. Scroll down to the **Certificates** settings.
5. Click **View Certificates**.
6. Click the **Your Certificates** tab.
7. Click **Import**.
8. In the **Downloads** folder, select the `student.p12` file.
9. Click **Open**.
10. Type the password `fortinet`, and then click **Sign in**.
11. Click **OK**.
12. Restart Firefox.

Test Two-Factor Authentication With a Digital Certificate for the SSL VPN User

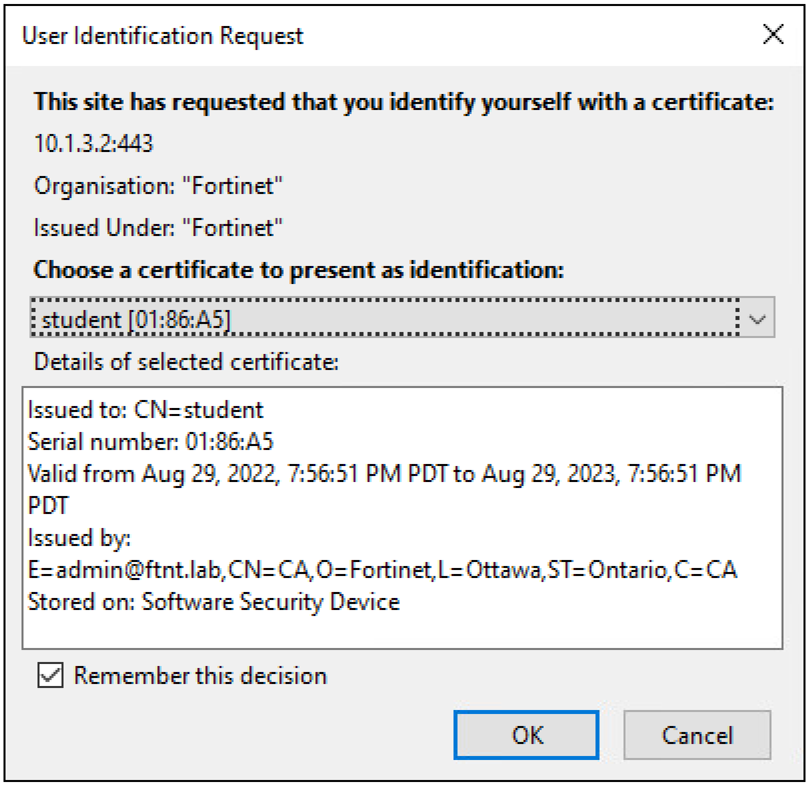
You will connect to the SSL VPN as the PKI user.

To test two-factor authentication for SSL VPN

1. On the FortiClient EMS VM, open PuTTY, and then connect over SSH to the NGFW saved session.
2. Log in with the username `admin` and password `password`.

DO NOT REPRINT
© FORTINET

3. Enter the following commands to enable the real-time debug:
```
diag debug application fnbamd -1
diag debug enable
```
4. On the Remote VM, open Firefox, and then in **Bookmarks**, select the **SSL-VPN Webmode** login page bookmark.
5. In the **User Identification Request** window, click **OK**.



If you do not see a certificate prompt window, open the **SSL-VPN Webmode** bookmark in a Firefox private window.

6. Log in with the username `student` and password `password`.

   This time, the user should authenticate successfully.

7. Return to the PuTTY session that was running the real-time debug, and then analyze its output.

   You should see some of the following logs indicating that the `student` peer user was able to authenticate successfully using the client certificate that was installed:

DO NOT REPRINT
© FORTINET


```
[287] fnbamd_chain_build-Self-sign detected.
[99] __cert_chg_st- 'Init' -> 'Validation'
[831] __cert_verify-req_id=1482481432
[832] __cert_verify-Chain is complete.
[457] fnbamd_cert_verify-Chain number:2
[471] fnbamd_cert_verify-Following cert chain depth 0
[533] fnbamd_cert_verify-Issuer found: CA_Cert_1 (SSL_DPI opt 1)
[471] fnbamd_cert_verify-Following cert chain depth 1
[675] fnbamd_cert_check_group_list-checking group with name 'SSL_VPN_Users'
[490] __check_add_peer-check 'remote'
[492] __check_add_peer-'remote' is not a peer user.
[490] __check_add_peer-check 'student'
[366] peer_subject_cn_check-Cert subject 'CN = student'
[294] __RDN_match-Checking 'CN' val 'student' -- match.
[404] peer_subject_cn_check-CN is good.
[497] __check_add_peer-'student' check ret:good
[612] __peer_user_clear_unmatched-Clear all user(s) other than 'student'
```

8. Enter the following CLI command to disable the real-time debug, and then close the SSH connection:

```
diagnose debug disable
```

DO NOT REPRINT
© FORTINET

Exercise 3: Configuring FSSO Authentication for Domain Computers

In this exercise, you will examine how to enable FSSO DC polling on FortiAuthenticator. You will also add FortiAuthenticator as an FSSO agent on FortiGate and configure relevant security policies for domain machines.

Create an FSSO Agent

You will add FortiAuthenticator as an FSSO agent on FortiGate.

To create an FSSO agent

1. On the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **ISFW** FortiGate login page bookmark.
2. Log in with the username `admin` and password `password`.
3. Click **Security Fabric** > **External Connectors**, and then click **Create New**.
4. In the **Endpoint/Identity** section, select **FSSO Agent On Windows AD**.
5. Configure the following settings:

Field	Value
Name	FAC-FSSO
Primary FSSO Agent IP/Name	fac.ftnt.lab
Password	fortinet

6. Keep the remaining settings, and then click **OK**.

Enable FortiGate SSO Authentication and DC Polling (Event Log Polling)

You will enable FortiGate FSSO authentication and DC polling on FortiAuthenticator.

To enable FortiGate SSO authentication and DC polling

1. On the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **FortiAuthenticator** login page bookmark.
2. Log in to the FortiAuthenticator GUI with the username `admin` and password `password`.
3. Click **Fortinet SSO Methods** > **SSO** > **General**.
4. In the **FortiGate** section, make sure that **Enable authentication** is enabled, and then in the **Secret key** field, type `fortinet`.
5. In the **Fortinet Single Sign-On (FSSO)** section, configure the following settings:

DO NOT REPRINT
© FORTINET

Field	Value
Enable Windows event log polling	Enable
Enable DNS lookup to get IP from workstation name	Enable
Directly use domain DNS suffix in lookup	Enable
Enable reverse DNS lookup to get workstation name from IP	Enable

6. Click **OK**.

Create a DC Account

You will create a DC account to poll the Active Directory event log to track user logins, and to poll the Windows Management Instrumentation (WMI) logs to track user logouts.

To create a DC account

1. Continuing on the FortiAuthenticator GUI, click **Fortinet SSO Methods** > **SSO** > **Windows Event Log Sources**, and then click **Create New**.
2. Configure the following settings:

Field	Value
NetBIOS name	FTNT
IP	10.1.0.30
Account	Administrator@ftnt.lab
Password	Password1!

3. Click **OK**.
   Ignore the warning prompt about DNS. DNS is already configured for this environment.
4. Click **Monitor** > **SSO** > **Windows Event Log Sources** to verify if the DC is connected.

Update Time	IP Address	Event Count	Event Processed	Last Event	Connected
e Aug 30 22:3...	10.1.0.30	4	4 (100.0%) (**See details**)	4776;Adminis...	✔

DO NOT REPRINT
© FORTINET

Create a FortiGate Filter

To provide FSSO only to specific groups on a remote LDAP server, you can filter the polling information so that it includes only those groups.

To create a FortiGate filter

1. Continuing on the FortiAuthenticator GUI, click **Fortinet SSO Methods** > **SSO** > **FortiGate Filtering**, and then click **Create New**.
2. Configure the following settings:

Field	Value
Name	ISFW
FortiGate name/IP	10.1.4.2

3. In the **Fortinet Single Sign-On (FSSO)** section, enable **Forward FSSO information for users from the following subset of users/groups/containers only**.
4. Click **Add Filtering Object**, and then configure the following settings:

Field	Value
Name	CN=HR-Group,CN=Users,DC=ftnt,DC=lab
Object Type	Group

5. Click **OK**.

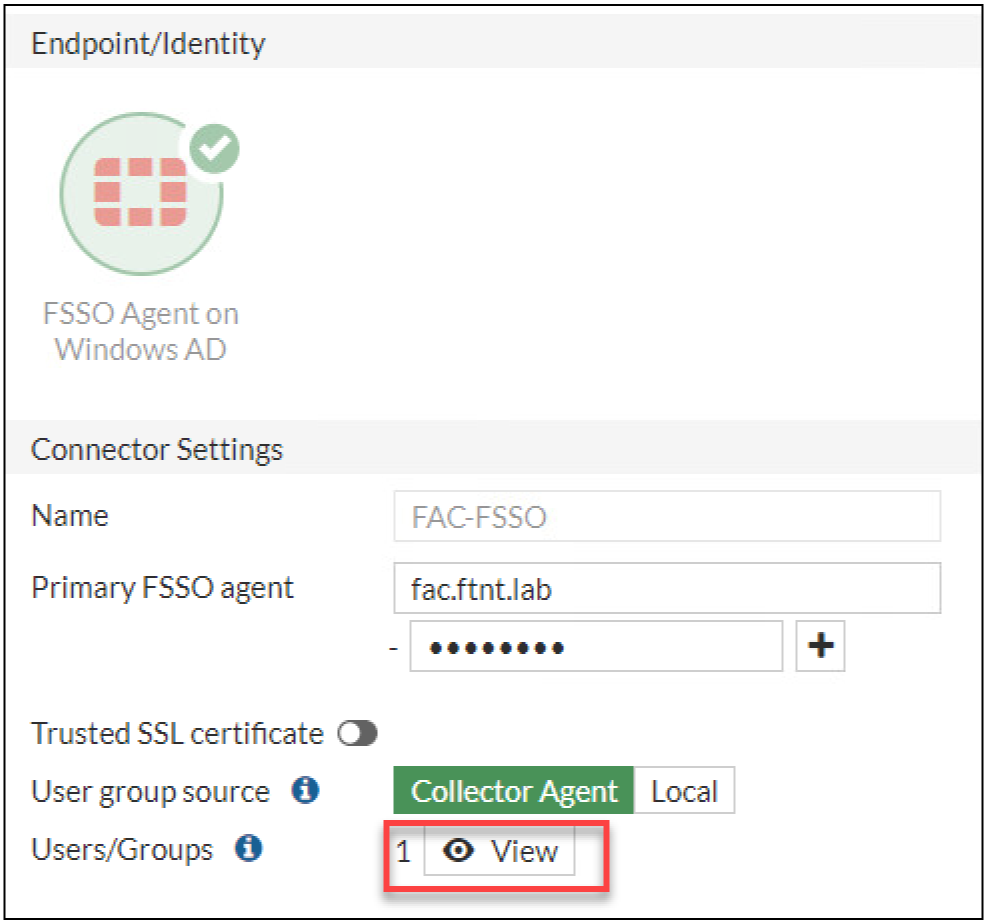
Add the FortiAuthenticator SSO Group to the FortiGate SSO Agent

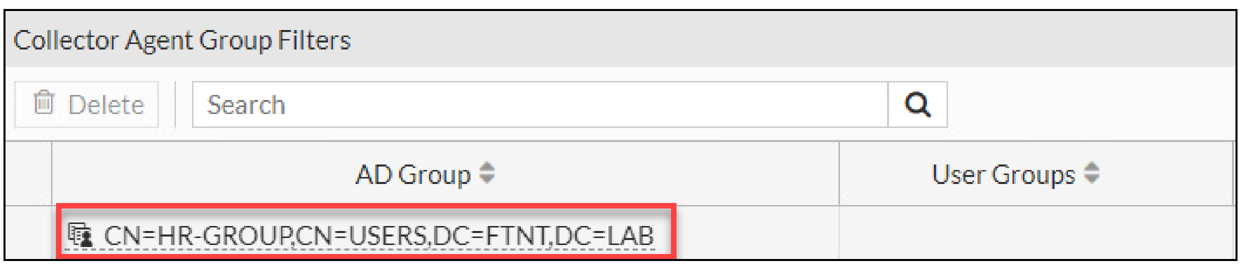
You will add the FortiAuthenticator SSO group to the FSSO agent, which you configured as an external connector on ISFW FortiGate at the beginning of this lab.

To add the AD user group to the FSSO agent

1. Return to the ISFW FortiGate GUI, click **Security Fabric** > **External Connectors**, and then edit **FAC-SSO**.
2. Click **Apply & Refresh**.
3. In the **Users/Groups** field, click **View** to confirm that the AD user group was imported.

DO NOT REPRINT
© FORTINET





Create an FSSO User Group

You will create an FSSO user group on FortiGate. This user group will be used for security policies, and traffic will be allowed based on FSSO group membership.

To create an FSSO user group

1. Continuing on the ISFW FortiGate GUI, click **User & Authentication** > **Users Groups**, and then click **Create New**.
2. Configure the following settings:

DO NOT REPRINT
© FORTINET

Field	Value
Name	HR-SSO
Type	Fortinet Single Sign-On (FSSO)
Members	CN=HR-Group,CN=Users,DC=ftnt,DC=lab

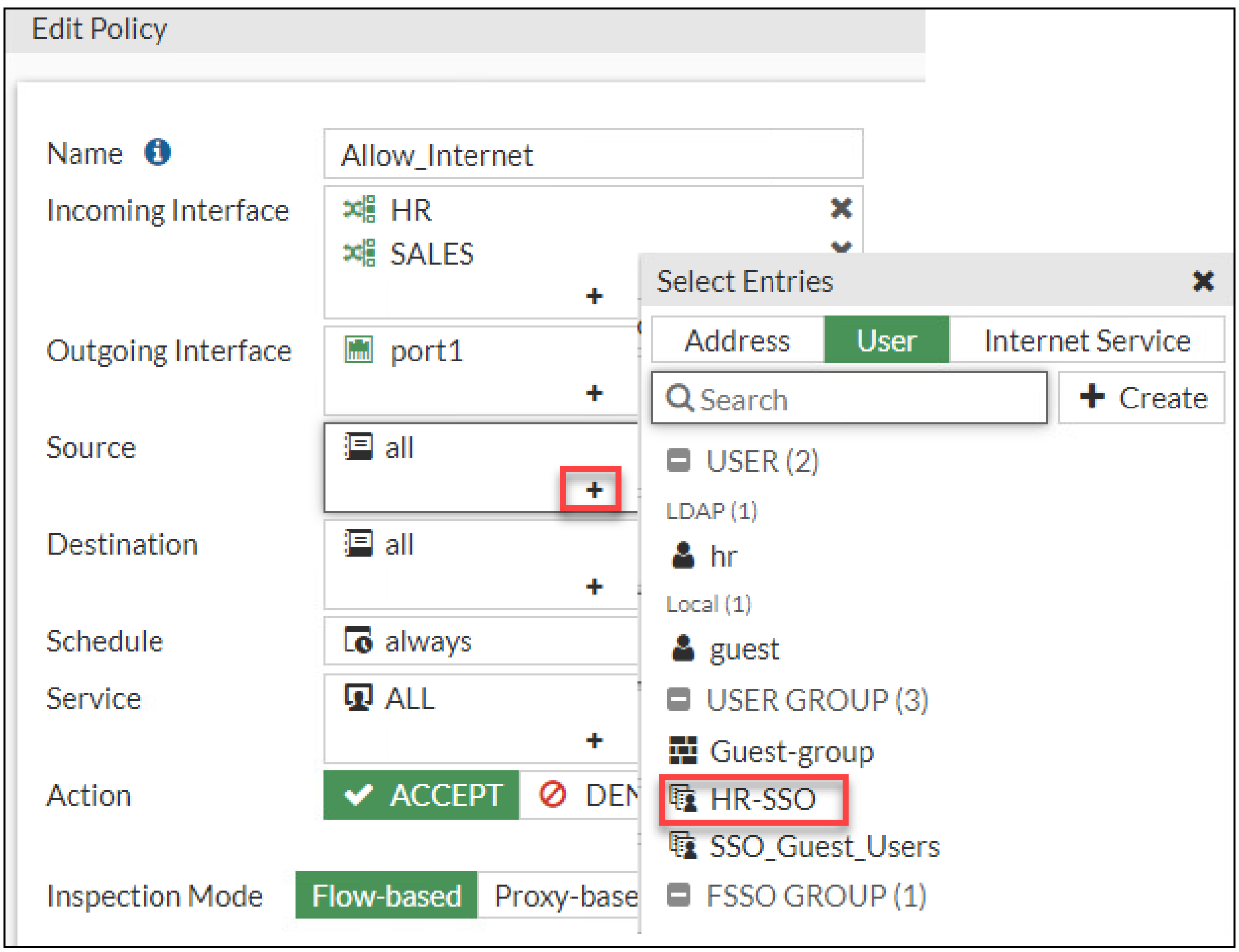
3. Click **OK**.

Configure an FSSO Firewall Policy

You will add the new FSSO user group to a firewall policy.

To add the FSSO user group to a firewall policy

1. Continuing on the ISFW FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. Edit the **Allow_Internet** policy.
3. In the **Source** field, click **+**, and then in the **Select Entries** window, select the **HR-SSO** user group.



4. Click **OK**.

DO NOT REPRINT
© FORTINET

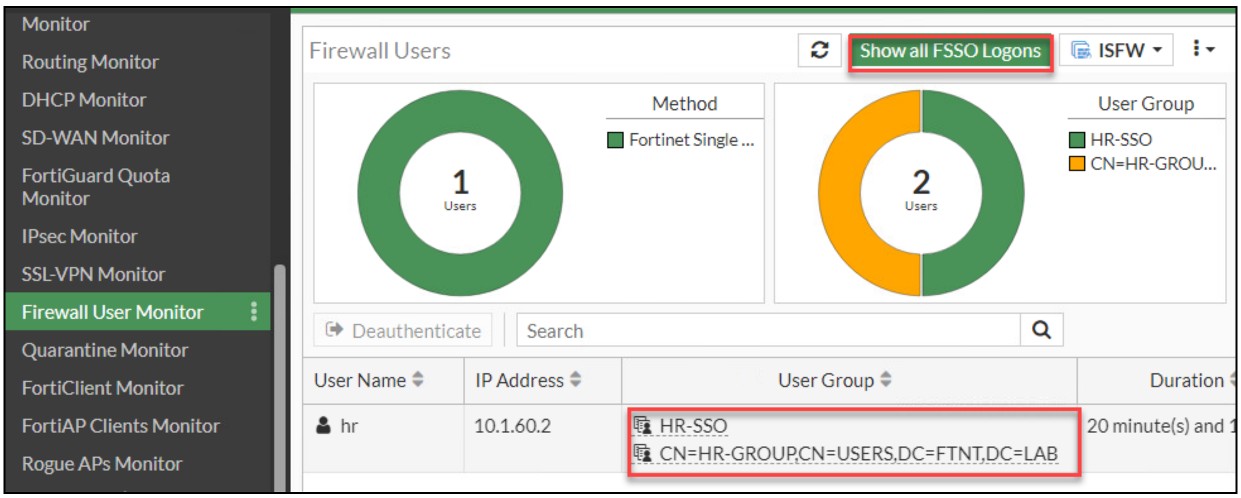
Test FSSO Authentication

You will access the internet with a user logged in to the domain and a non-domain machine.

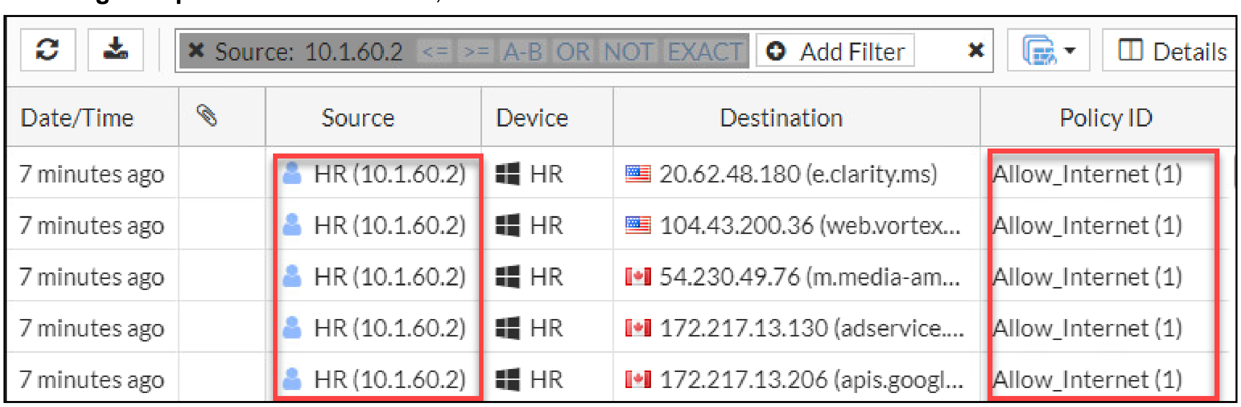
To test FSSO authentication

The **HR** user has already been added as member of the **CN=HR-Group,CN=Users,DC=ftnt,DC=lab** group in Active Directory.

1. On the HR VM, log in with the username `ftnt.lab\hr` and password `Password1!`.
2. Open a browser, and then access a few websites.
3. On the FortiClient EMS VM, return to the ISFW FortiGate GUI, and then click **Dashboard** > **Firewall User Monitor** > **Show all FSSO Logons**.



4. Click **Log & Report** > **Forward Traffic**, and then add a filter for **Source** as `10.1.60.2`.



The **HR** user logon event was recorded by FortiAuthenticator, and the AD group was forwarded to FortiGate. FortiGate matched the AD group with the **HR-SSO** local SSO group, and then allowed the traffic through the configured firewall policy.

DO NOT REPRINT
© FORTINET

5. On the Sales VM, log in with the username `student` and password `Password1!`.
6. Open a browser, and then access few websites.

   You will not be able to access any websites since the user did not log in to the domain.

7. On the FortiClient EMS VM, return to the ISFW FortiGate GUI, click **Log & Report** > **Forward Traffic**, remove the filters that you added in the previous steps, and then add a filter for **Source** as `10.1.50.2`.

Source	Device	Destination	Policy ID	Action
10.1.50.2	SALES.f...	151.101.131.5 (cnn.com)	0	Deny: policy violation
10.1.50.2	SALES.f...	151.101.131.5 (cnn.com)	0	Deny: policy violation
10.1.50.2	SALES.f...	35.244.181.201 (prod.balr...	0	Deny: policy violation
10.1.50.2	SALES.f...	34.107.221.82 (prod.detect...	0	Deny: policy violation
10.1.50.2	SALES.f...	54.255.157.103 (cricinfo.co...	0	Deny: policy violation
10.1.50.2	SALES.f...	35.244.181.201 (prod.balr...	0	Deny: policy violation

The **student** user logon was not recorded by FortiAuthenticator since it is not a user that logged in to the domain. There are no other firewall policies configured to provide internet access to non-domain users, and therefore the implicit deny policy rejected the traffic.

DO NOT REPRINT
© FORTINET

Exercise 4: Configuring LDAP Authentication for Non-Domain Computers (BYOD)

In this exercise, you will examine how to enable LDAP authentication on FortiGate to allow internet access for non-domain computers.

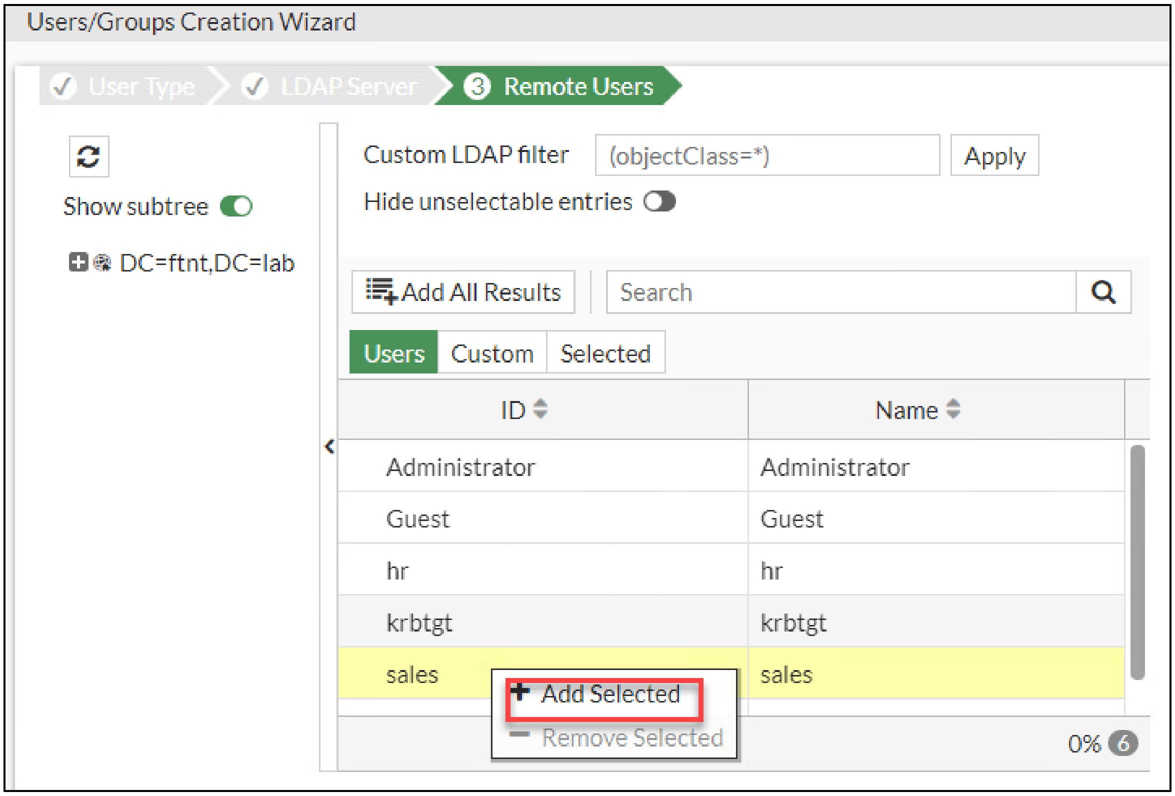
Create an LDAP User and User Group

You will create an LDAP user and user group on FortiGate. This user group will be used for security policies, and traffic will be allowed based on the LDAP group membership.

To create an LDAP user and user group

1. On the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **ISFW** FortiGate login page bookmark.
2. Log in with the username `admin` and password `password`.
3. Click **User & Authentication** > **Users Definition**.
4. Click **Create New**.
5. In the **User Type** field, select **Remote LDAP User**, and then click **Next**.
6. In the **LDAP Server** field, select **AD**, and then click **Next**.
7. Right-click **sales**, and then click **Add Selected**.

DO NOT REPRINT
© FORTINET



8. Click **Submit**.
9. Click **User & Authentication** > **Users Groups**, and then click **Create New**.
10. Configure the following settings:

Field	Value
Name	LDAP-Sales
Type	Firewall
Members	sales

11. Click **OK**.

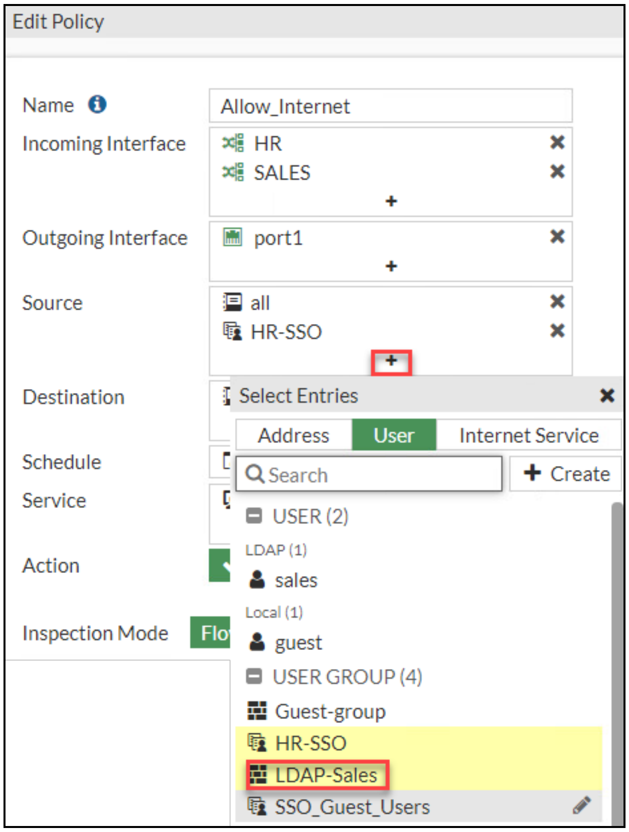
Configure Firewall LDAP Authentication

You will add the new LDAP user group to a firewall policy.

To add the LDAP user group to a firewall policy

1. Continuing on the ISFW FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. Edit the **Allow_Internet** policy.
3. In the **Source** field, click **+**, and then select the **LDAP-Sales** user group.

DO NOT REPRINT
© FORTINET



4. Click **OK**.

Test LDAP Authentication

You will use a non-domain-computer to access the internet using LDAP.

To test LDAP authentication

1. On the Sales VM, log in with the username `student` and password `Password1!`.
2. Open a browser, and then enter the following URL: `www.fortinet.com`.
3. At the authentication prompt, type the username `sales` and password `Password1!`, and then click **Continue**.

   The authentication should be successful and you should have access to the web page.

4. On the FortiClient EMS VM, return to the ISFW FortiGate GUI, and then click **Log & Report** > **Forward Traffic**.

   The logs show that internet traffic was allowed for the **sales** user.

DO NOT REPRINT
© FORTINET

Minute ago	sales (10.1.50.2)	SALES	13.107.4.52 (www.msftcon...	Allow_Internet (1)
Minute ago	sales (10.1.50.2)	SALES	34.107.221.82 (prod.detect...	Allow_Internet (1)
Minute ago	sales (10.1.50.2)	SALES	142.0.165.140	Allow_Internet (1)
Minute ago	sales (10.1.50.2)	SALES	138.199.57.151	Allow_Internet (1)
Minute ago	sales (10.1.50.2)	SALES	138.199.57.151	Allow_Internet (1)
Minute ago	sales (10.1.50.2)	SALES	54.74.240.166	Allow_Internet (1)

DO NOT REPRINT
© FORTINET

Exercise 5: Adding FortiClient EMS to the Security Fabric

In this exercise, you will add FortiClient EMS to the Security Fabric. You will use FortiClient EMS in a later lab to configure ZTNA tags and endpoint profiles.

Integrate FortiClient EMS With the Security Fabric

You will add FortiClient EMS to the Security Fabric.

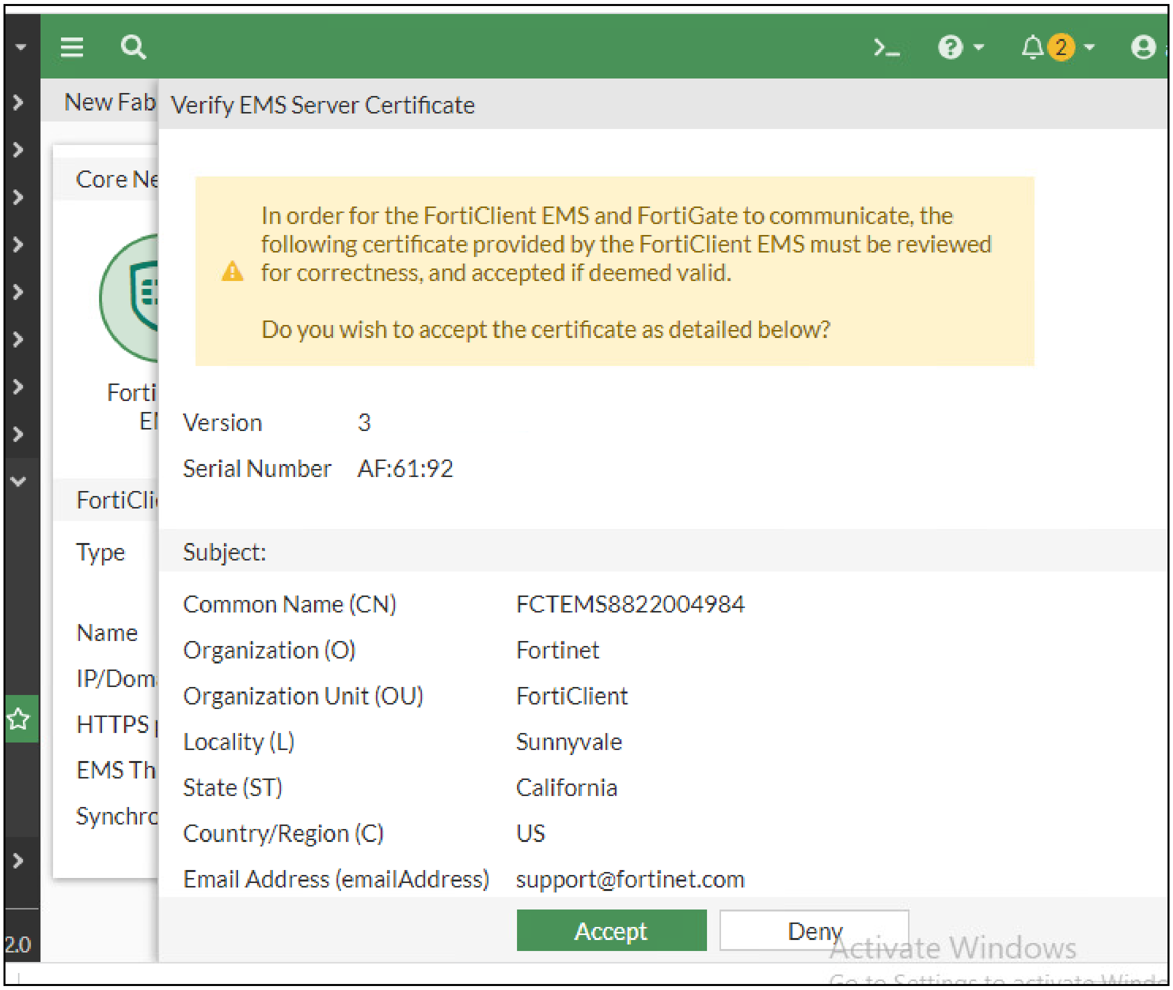
To integrate FortiClient EMS with FortiGate

1. On the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **NGFW** FortiGate login page bookmark.
2. Log in with the username `admin` and password `password`.
3. Click **Security Fabric** > **Fabric Connectors**.
4. In the list, select **FortiClient EMS**, and then click **Edit.**
5. In the **New Fabric Connector** window, configure the following settings:

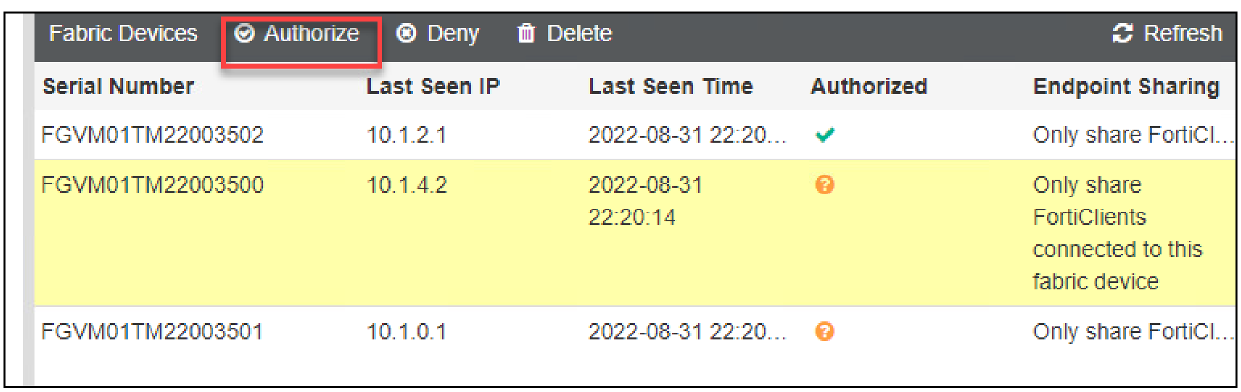
Field	Value
Name	EMS
IP/Domain Name	10.1.0.30

6. Click **OK**, and then click **Accept** to accept the certificate and save the settings.

DO NOT REPRINT
© FORTINET



7. Click **Close**.
8. In Google Chrome, open a new tab, and then in **Bookmarks**, select the **FortiClient EMS** login page bookmark.
9. Log in with the username `admin` and password `Password1!`.
10. Click **Administration** > **Fabric Devices**.
11. Select **FortiGate**, and then click **Authorize**.



12. Select the first FortiGate in the list, and then click **Edit**.
13. In the **FortiClient Endpoint Sharing** field, select **Share all FortiClients**.

DO NOT REPRINT
© FORTINET

14. Click **Save**.
15. Repeat steps 13–14 for the remaining two FortiGate devices.

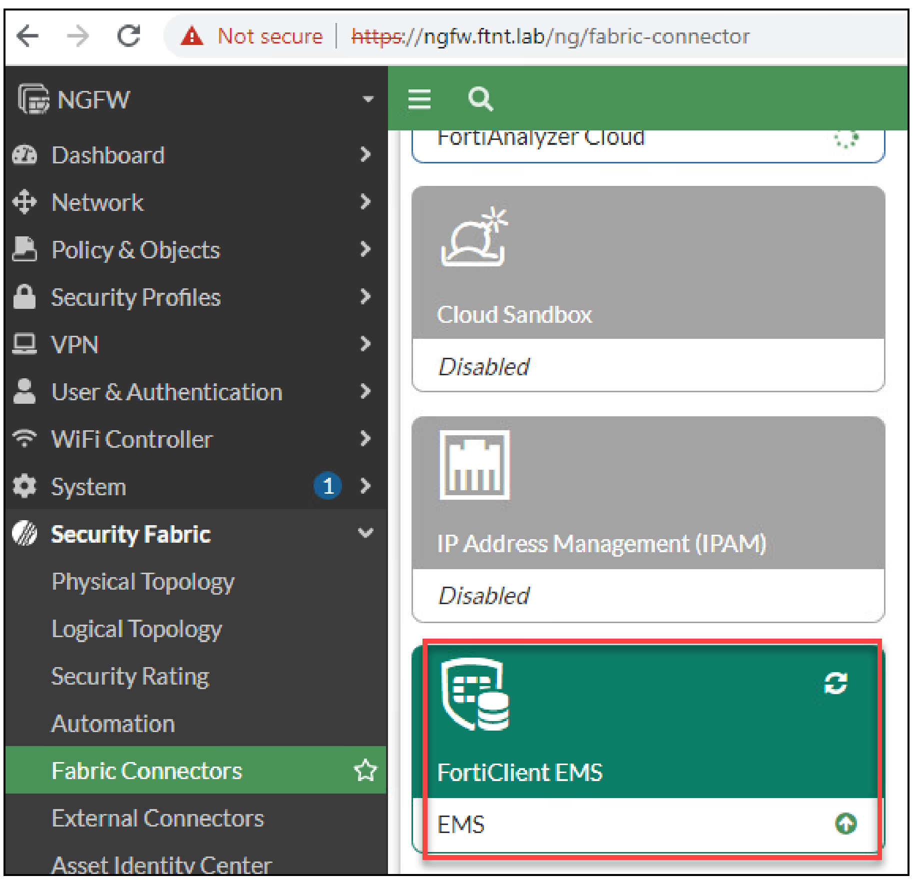
Fabric Devices

Serial Number	Last Seen IP	Last Seen Time	Authorized	Endpoint Sharing
FGVM01TM22004381	10.1.2.1	2022-12-18 19:48:13	✔	Share all FortiClients
FGVM01TM22004383	10.1.2.1	2022-12-18 19:48:32	✔	Share all FortiClients
FGVM01TM22004382	10.1.2.1	2022-12-18 19:47:46	✔	Share all FortiClients

The FortiGate devices have been already configured to participate in the Security Fabric. NGFW FortiGate is the Fabric root, and the EMS connector configuration has been synchronized to ISFW FortiGate and DCFW FortiGate.

16. Return to the NGFW FortiGate GUI, and then click **Security Fabric** > **Fabric Connectors**.
17. Scroll down to see the **FortiClient EMS** connector status.

    The status should display a green arrow.



18. Repeat steps 16–17 on the DCFW FortiGate and the ISFW FortiGate to confirm connectivity to the EMS server.

DO NOT REPRINT
© FORTINET

Lab 3: Network Access Security With FortiNAC

In this lab, you will work through various exercises to secure network access with FortiNAC. First, you will install SSL certificates for the FortiNAC GUI and captive portal for device onboarding. Next, you will add ISFW FortiGate and FortiSwitch to FortiNAC management.

Objectives

- Review the configuration wizard and license details
- Install SSL certificates for the FortiNAC GUI, portal, and agent communication
- Configure network modeling

Time to Complete

Estimated: 90 minutes

DO NOT REPRINT
© FORTINET

Exercise 1: Reviewing the Configuration Wizard and License Details

In this exercise, you will review the FortiNAC configuration wizard and license details.

Review the Configuration Wizard

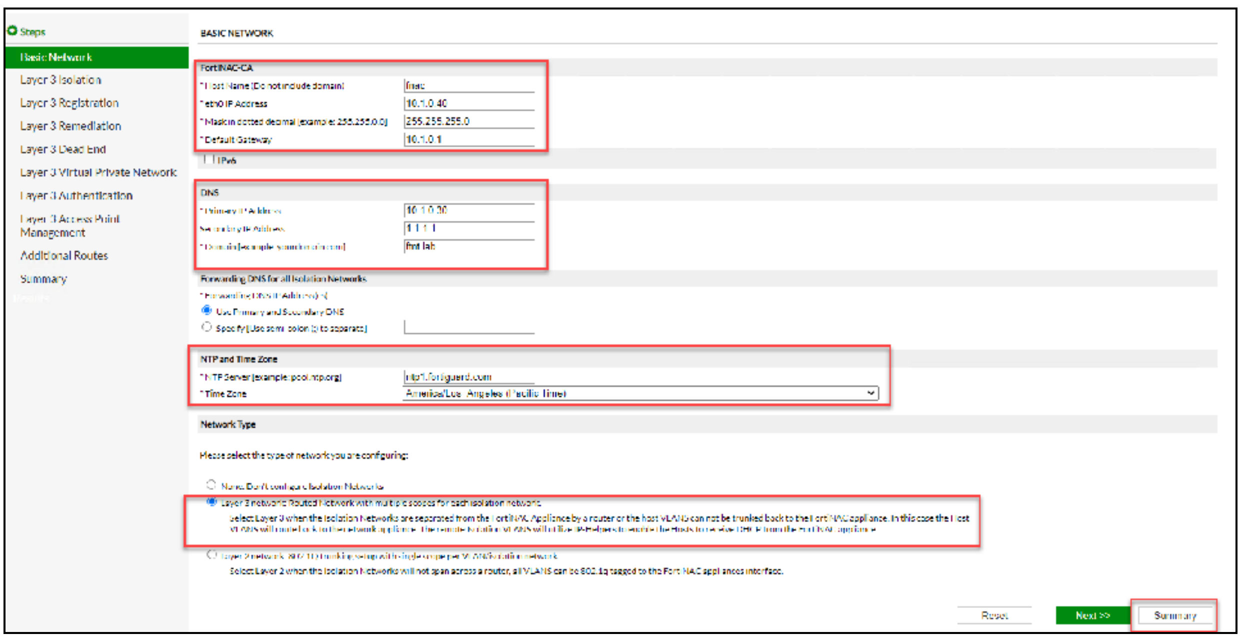
You will review the FortiNAC network configuration using the configuration wizard.

To review the configuration wizard

1. On the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **FortiNAC** login page bookmark.

   You may receive a certificate error. Click **Advanced** > **Proceed to fnac.ftnt.lab (unsafe)** to continue to login page.

2. Log in to the FortiNAC GUI with the username `admin` and password `Password1!`.
3. Click **System** > **Config Wizard**, review the settings, and then click **Summary**.



You can verify the host name, management IP address, gateway, DNS, NTP, and network type in use on the **Basic Network** page. DNS and NTP settings are critical for the correct operation of FortiNAC.

DO NOT REPRINT
© FORTINET

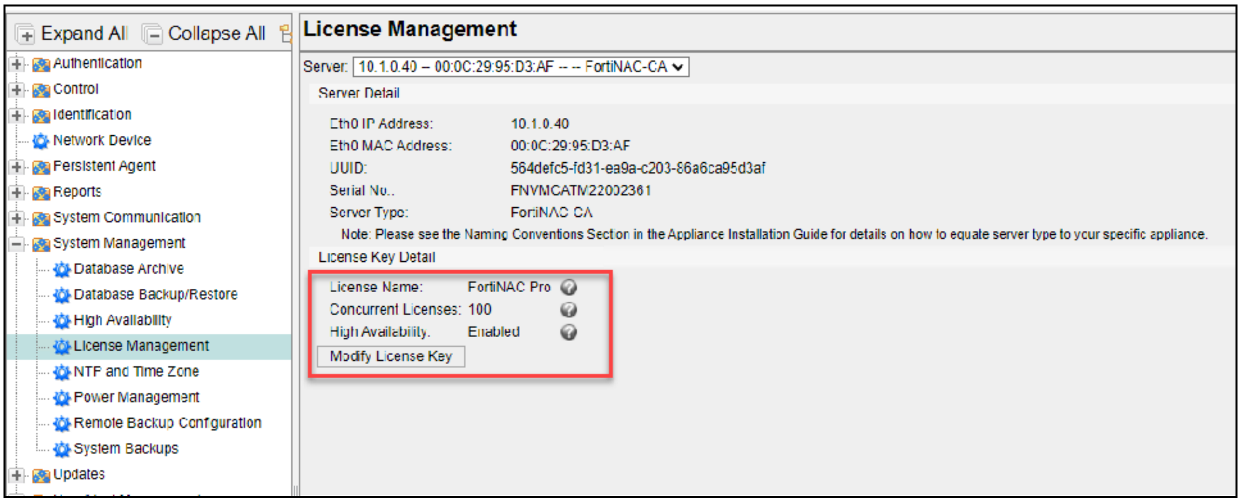
4. Review the **Summary** page for service interface details such as registration, remediation, and authentication interface IP and DHCP scopes assigned.

Review the License Information

You will review the FortiNAC license type and usage.

To review the FortiNAC license information

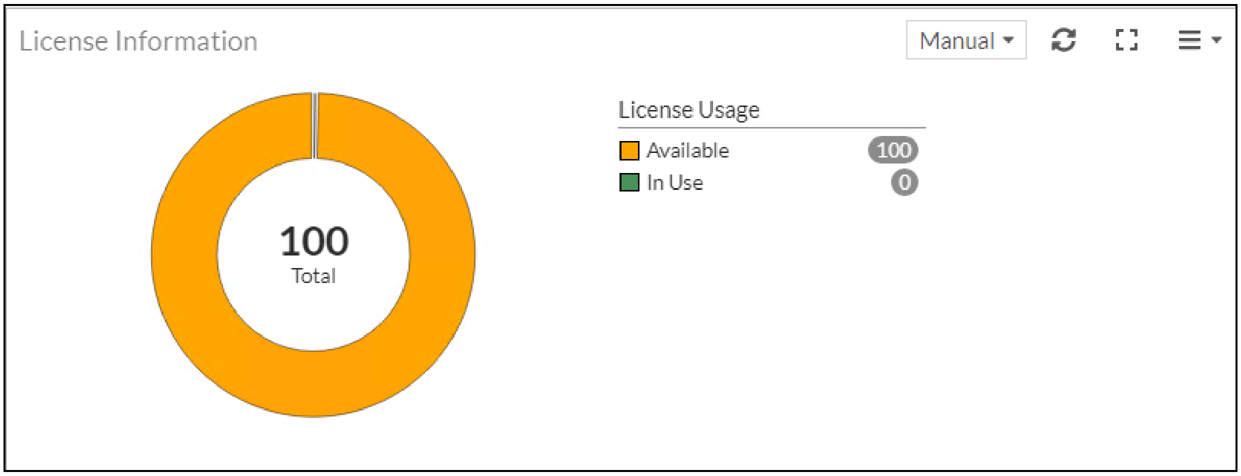
1. Continuing on the FortiNAC GUI, click **System** > **Settings**, expand **System Management**, and then click **License Management**.



A FortiNAC Pro license is recommended for comprehensive ZTA features.

2. Click **Dashboard** > **Main**, and then click **Add Widget** to add the **License Information** widget to the dashboard.
3. In the **System** section, select the **License Information** widget, select either **Table View** or **Pie Chart** for visualization, and then click **OK.**

DO NOT REPRINT
© FORTINET



The widget does not show the license type. To check your license variant, you must use the **Settings** menu.

DO NOT REPRINT
© FORTINET

Exercise 2: Managing Certificates

In this exercise, you will generate a certificate signing request (CSR) on FortiNAC, and then sign it using the FortiAuthenticator certificate authority (CA). You will also install the new certificate on the FortiNAC GUI, captive portal, and persistent agent.

Generate a CSR

You will generate a CSR on FortiNAC, and then sign the CSR using the FortiAuthenticator CA.

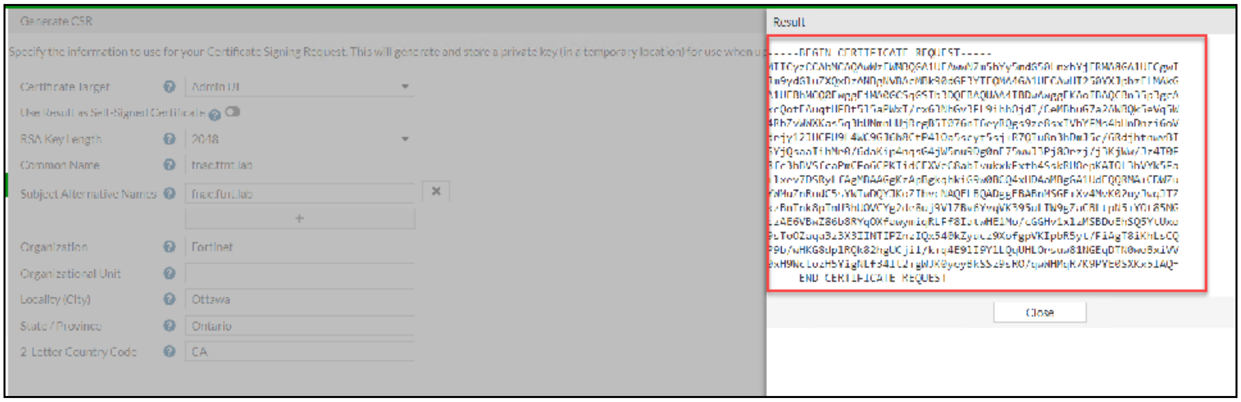
To generate a CSR

1. On the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **FortiNAC** login page bookmark.
2. Log in to the FortiNAC GUI with the username `admin` and password `Password1!`.
3. Click **System** > **Certificate Management**.
4. Click **Generate CSR**, configure the following settings, and then click **OK**:

Field	Value
Certificate Target	Admin UI
RSA Key Length	2048
Common Name	fnac.ftnt.lab
Subject Alternative Names	fnac.ftnt.lab
Organization	Fortinet
Locality (City)	Ottawa
State / Province	Ontario
2-Letter Country Code	CA

5. In the **Result** field, copy the text, paste it in a Notepad file, and then save the file as `fnac.ftnt.lab.csr`.

DO NOT REPRINT
© FORTINET



6. Click **Close**.
7. In Google Chrome, open a new tab, and then in **Bookmarks**, select the **FortiAuthenticator** login page bookmark.
8. Log in to the FortiAuthenticator GUI with the username `admin` and password `password`.
9. Click **Certificate Management** > **End Entities** > **Users**, and then click **Import**.
10. Configure the following settings, and then click **OK** to sign the certificate with these settings:

Field	Value
Type	CSR to Sign
Certificate ID	fnac.ftnt.lab
CSR file (.csr, .req)	Upload the file created in the previous step.
Add CRL Distribution Points extension	Enabled
Add OCSP Responder URL	Enabled
Advanced Options: Key Usages	Choose **Server Authentication** and **Client Authentication** under **Extended Key Usages**.

11. In the list, select **fnac.ftnt.lab**, and then click **Export Certificate**.

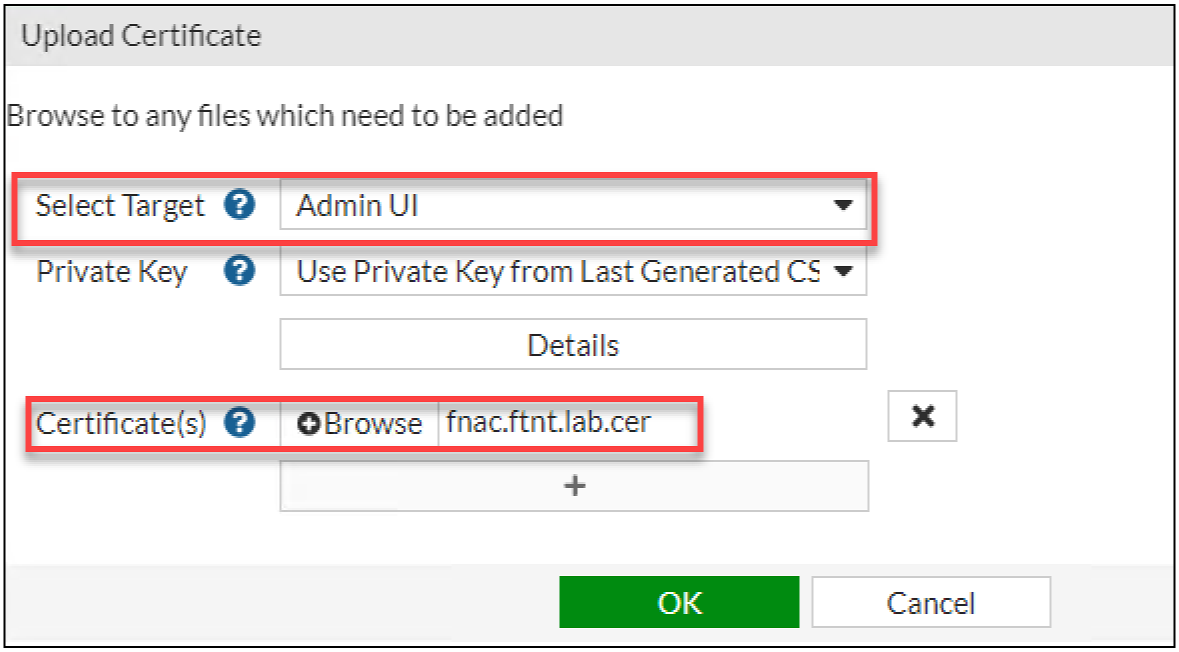
Install SSL Certificates for the FortiNAC GUI

You will install the new certificate for the FortiNAC GUI.

To install SSL certificates for the FortiNAC GUI

1. Return to the FortiNAC GUI, and then click **System** > **Certificate Management**.
2. Click **Upload Certificate**, and then in the **Select Target** field, select **Admin UI**.
3. In the **Certificate(s)** field, click **Browse**, upload the `fnac.ftnt.lab.cer` certificate that you downloaded in the previous task, and then click **OK**.

DO NOT REPRINT
© FORTINET

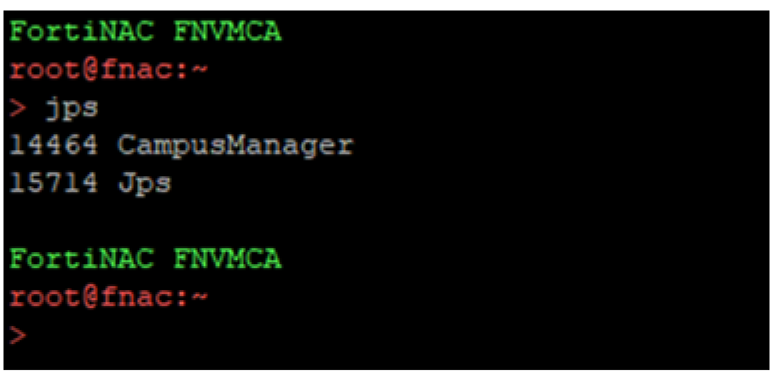


4. Click **Restart** to restart the service.

The FortiNAC GUI should now reload with the new certificate. If this is the case, you can skip to step 9. If not, you may need to restart the service manually on the CLI.

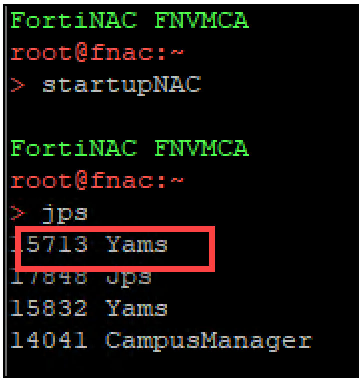
---

5. Open PuTTY, and then connect over SSH to the **FortiNAC**saved session.
6. Log in with the username `root` and password `Password1!`, and then enter `shutdownNAC` to stop all FortiNAC services.
7. Verify the services have stopped by entering the `jps` command and making sure the **Yams** process is not running, as shown in the following image:



8. Enter `startupNAC` to start all FortiNAC services.

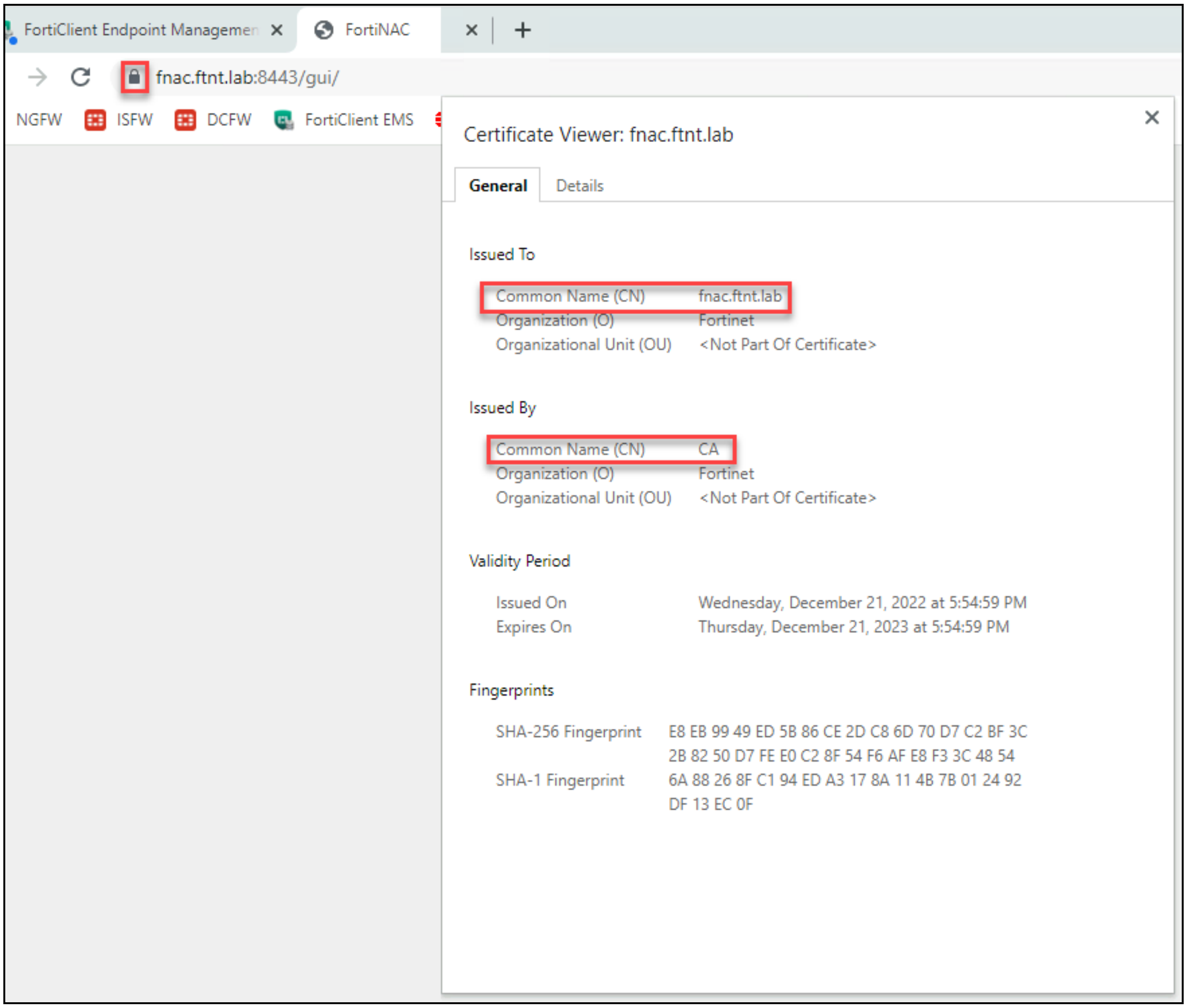
DO NOT REPRINT
© FORTINET



It may take up to 5 minutes for the services to start up. You can verify the services are running by entering the `jps` command and making sure the `Yams` process is running. You may still need to wait 1–2 minutes after the process starts before gaining access to the FortiNAC GUI.

9. Reload the FortiNAC GUI, and then log in with the username `admin` and password `Password1!`.
10. Verify that the certificate is valid and has been issued by the FortiAuthenticator CA.

DO NOT REPRINT
© FORTINET



11. Close the **Certificate Viewer**.

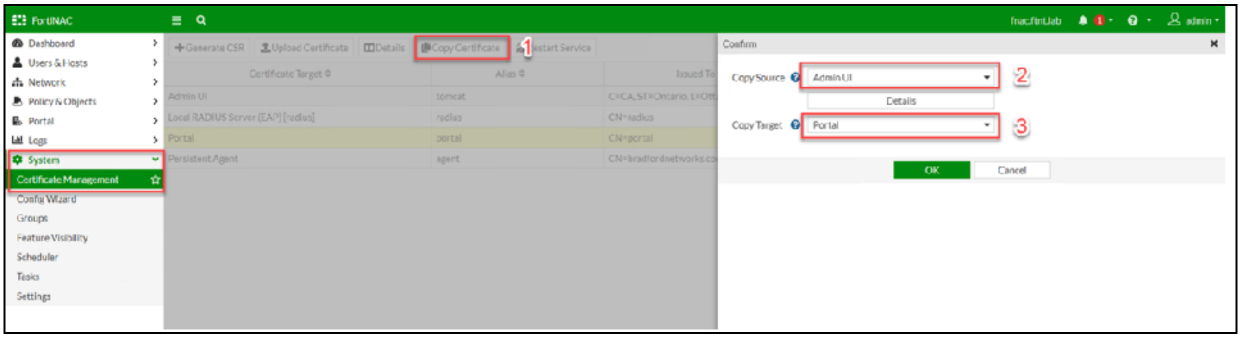
Install the SSL Certificate for the Captive Portal

You will install the new certificate for the FortiNAC captive portal.

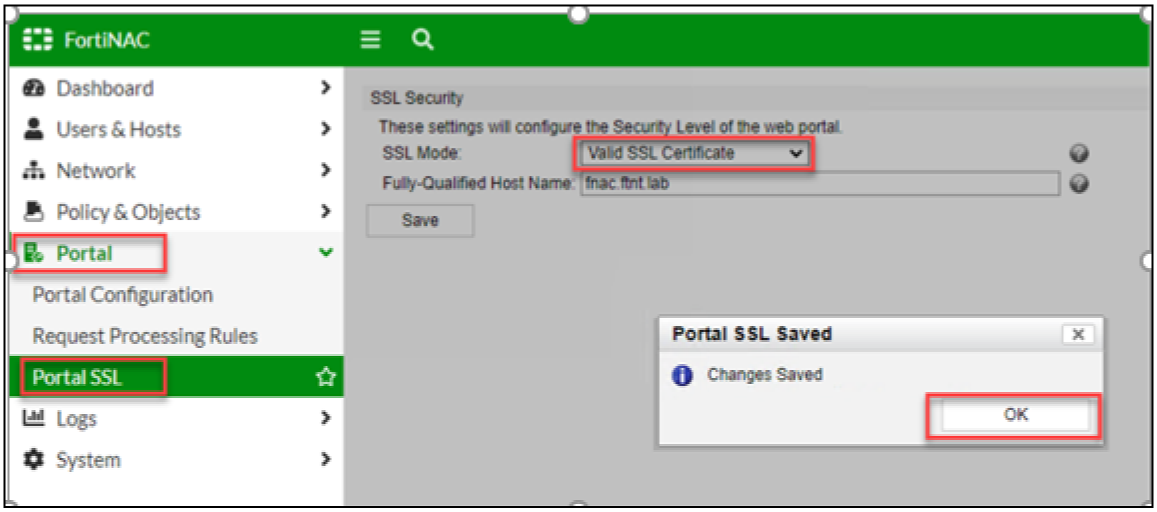
To install the SSL certificate for the FortiNAC captive portal

1. Continuing on the FortiNAC GUI, click **System** > **Certificate Management**, and then click **Portal**.
2. Click **Copy Certificate**, in the **Copy Source** field, select **Admin UI**, in the **Copy Target** field, select **Portal**, and then click **OK**.

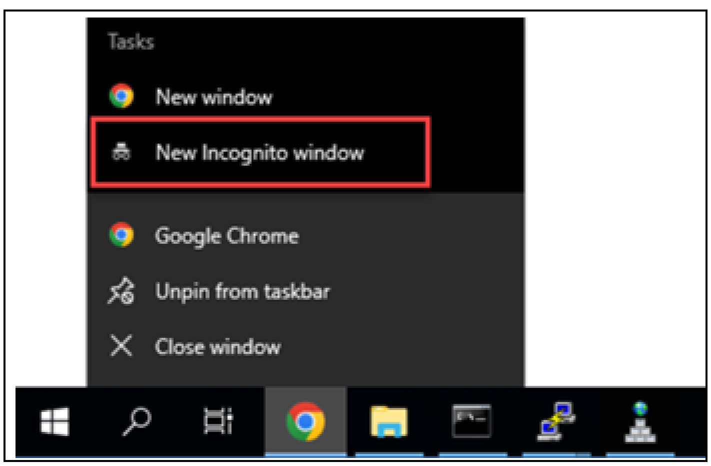
DO NOT REPRINT
© FORTINET



3. If you are asked to restart the service, click **Restart**.
4. Click **Portal** > **Portal SSL**, in the **SSL Mode** field, select **Valid SSL Certificate**, and then click **Save**.

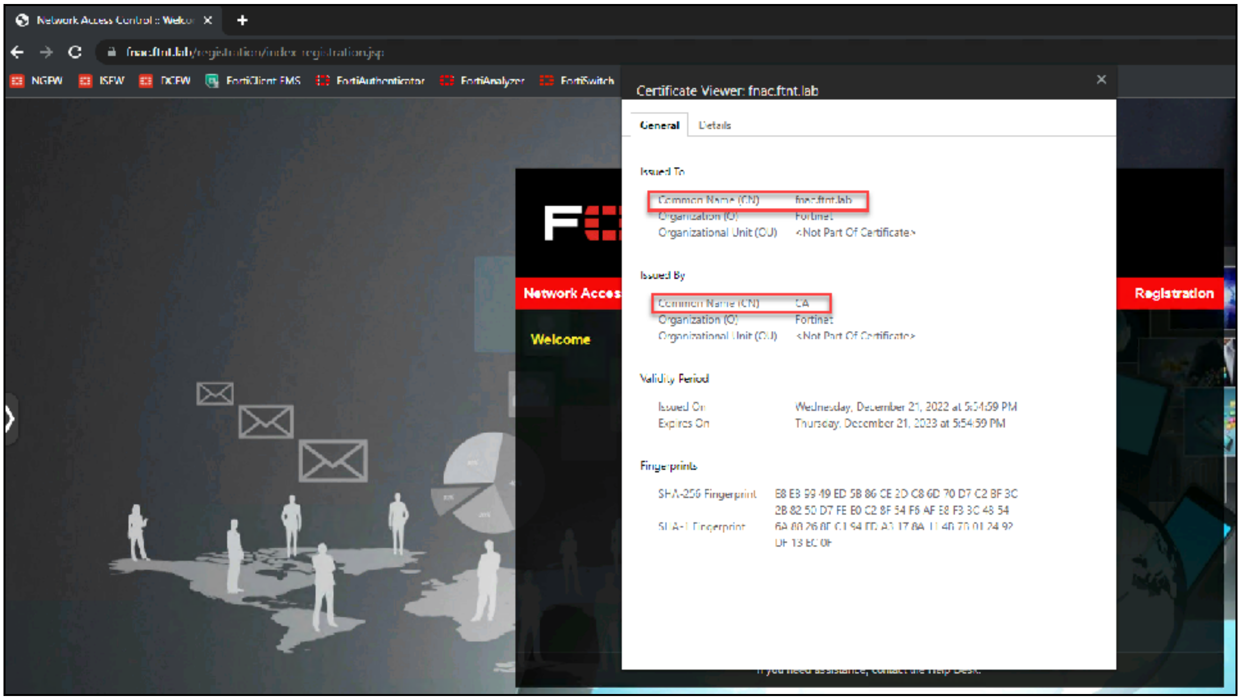


5. Click **OK**.
6. Open Google Chrome in a **New Incognito window**.



7. Navigate to `https://fnac.ftnt.lab/` to verify the portal certificate is updated with the FortiAuthenticator CA.

DO NOT REPRINT
© FORTINET



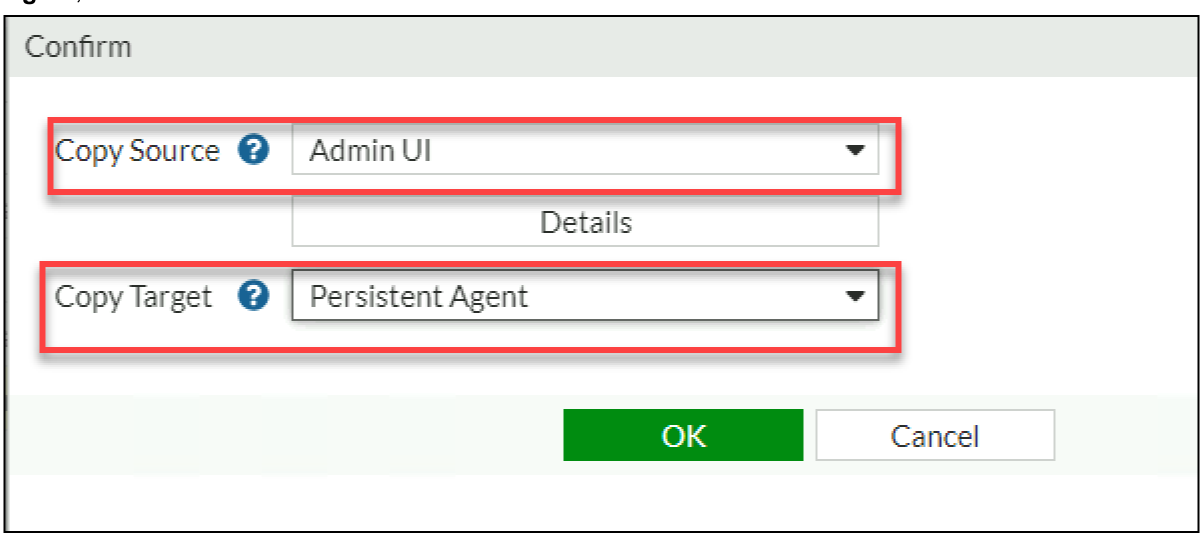
8. Close the incognito window.

Install the SSL Certificate for the Persistent Agent

You will install the new certificate for the FortiNAC persistent agent.

To install the SSL certificate for the FortiNAC persistent agent

1. Return to the FortiNAC GUI, click **System** > **Certificate Management**, and then click **Persistent Agent**.
2. Click **Copy Certificate**, in the **Copy Source** field, select **Admin UI**, in the **Copy Target** field, select **Persistent Agent**, and then click **OK**.

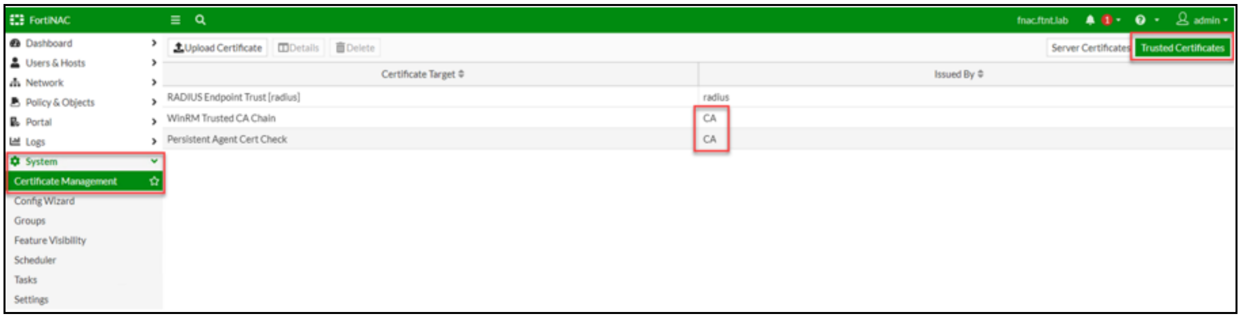


DO NOT REPRINT
© FORTINET

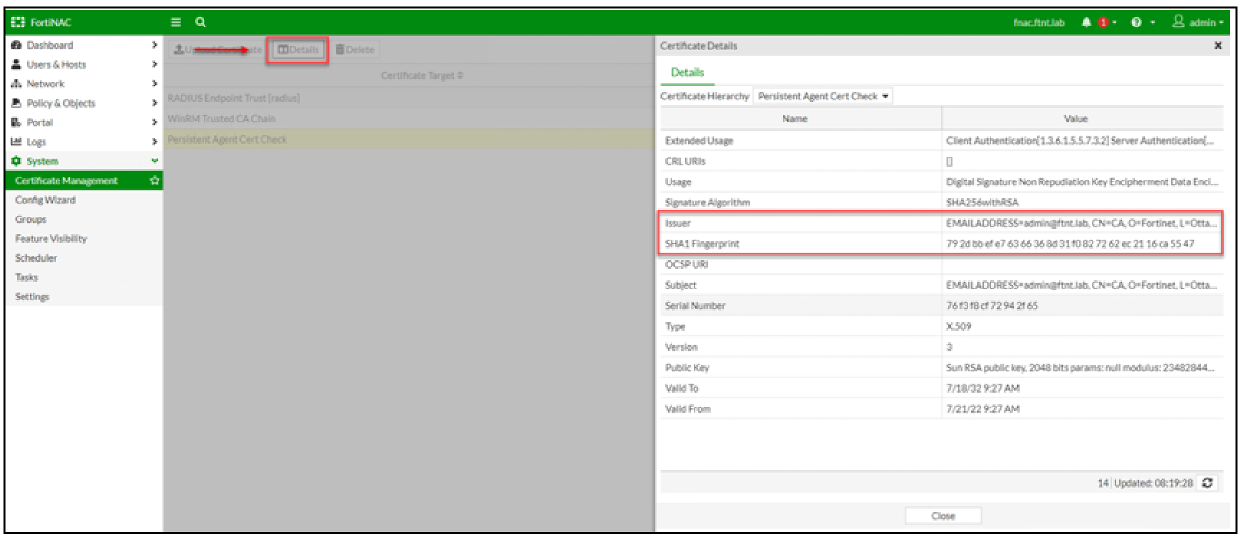
3. If you are asked to restart the service, click **Restart**.

   The FortiAuthenticator CA certificate has been preinstalled under **Trusted Certificates** for FortiNAC **Persistent Agent Cert Check** and **WinRM Trust CA Chain**.

4. Click **System** > **Certificate Management**, and then click **Trusted Certificates** to validate that the certificate was preinstalled.



5. Select **Persistent Agent Cert Check**, and then click **Details** to review the CA certificate.



You will validate the certificate in a later exercise.

DO NOT REPRINT
© FORTINET

Exercise 3: Configuring Network Modeling

In this exercise, you will create logical networks and add ISFW FortiGate to the FortiNAC inventory for management. You will also review captive VLANs that FortiGate will use to enable device onboarding and role-based access.

Create Logical Networks

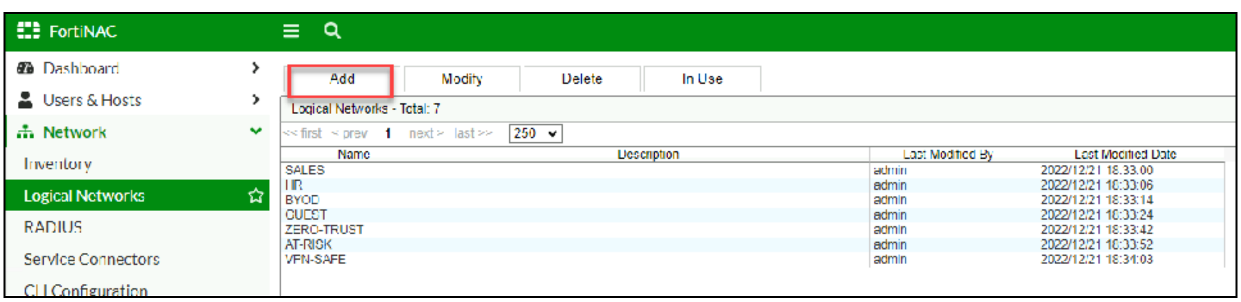
You will create logical networks on FortiNAC.

To create logical networks

1. On the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **FortiNAC** login page bookmark.
2. Log in to the FortiNAC GUI with the username `admin` and password `Password1!`.
3. Click **Network** > **Logical Networks**.

> If an **Initialize Network Access** message appears asking **Do you want to initialize Network Access policies to a pre-defined sample configuration?**, click **No**.

4. Click **Add**, and then create the following logical networks:
   - `SALES`
   - `HR`
   - `BYOD`
   - `GUEST`
   - `ZERO-TRUST`
   - `AT-RISK`
   - `VPN-SAFE`



Add FortiGate to the Inventory

You will add ISFW FortiGate to the FortiNAC inventory.

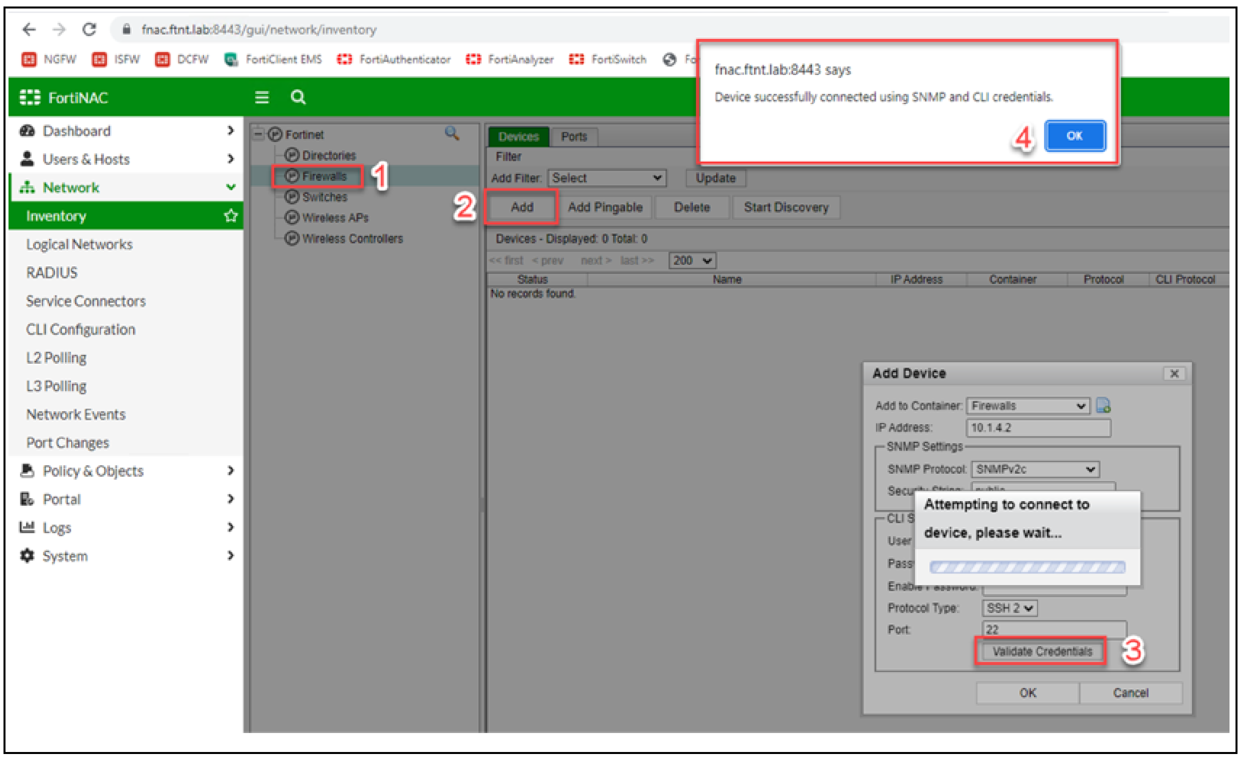
DO NOT REPRINT
© FORTINET

To add FortiGate to the FortiNAC inventory

1. Continuing on the FortiNAC GUI, click **Network** > **Inventory**, click **Firewalls**, and then click **Add** to add ISFW FortiGate with the following settings:

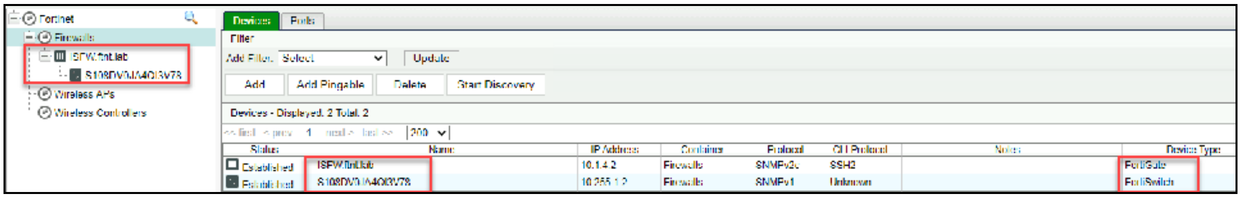
Field	Value
IP Address	10.1.4.2
SNMP Protocol	SNMPv2C
Security String	public
User Name	admin
Password	password
Enable Password	(Leave this field empty.)
Protocol Type	SSH 2
Port	22

2. Click **Validate Credentials**, ensure that you see a successful connection using SNMP and CLI credentials, and then click **OK**.



3. Click **OK** to add ISFW FortiGate to the inventory.
4. If the FortiGate does not appear on the **Inventory** page, refresh the browser page.

DO NOT REPRINT
© FORTINET

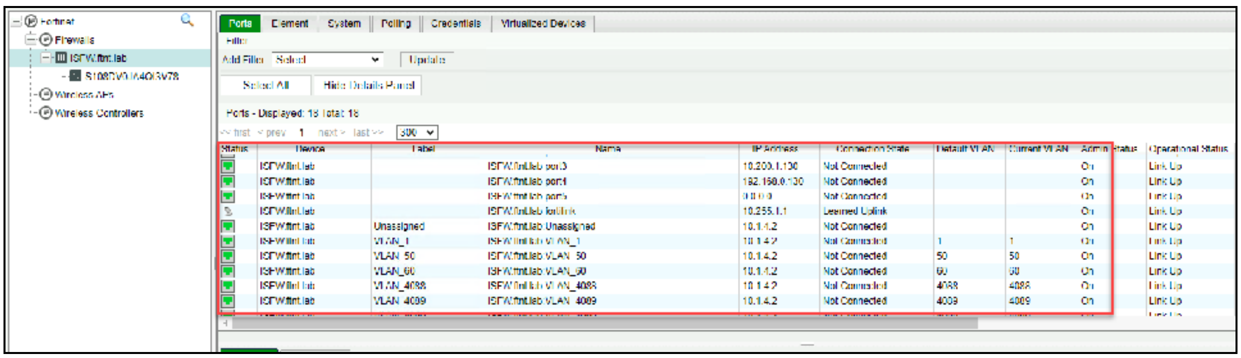


Stop and Think!

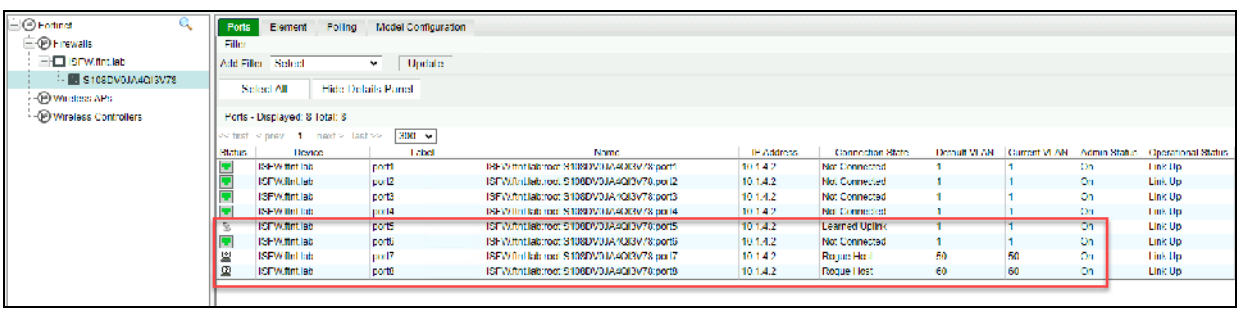
Do you know why FortiSwitch appears in the list even though it was FortiGate that you added to the inventory?

Is the FortiSwitch being managed as a standalone device or in FortiLink management mode?

5. Under **Firewalls**, click **ISFW.ftnt.lab**, and then review the interfaces shown in the following image:



6. Under **ISFW.ftnt.lab**, click **S108DV0JA4QI3V78**, and then review the interfaces shown in the following image:



DO NOT REPRINT
© FORTINET

Stop and Think!

You should now have visibility over devices connected to both FortiGate and FortiSwitch, but what do the icons shown in the image mean?

Discussion

Icons indicate whether an interface is an uplink, the types of devices that are connected (rogue versus registered), the state of the devices (safe versus at risk), and so on.

Hint

Ports 1–4 are not connected to any devices.

port5 is an uplink interface and is connected to FortiGate.

port6 is connected to the FortiNAC service interface.

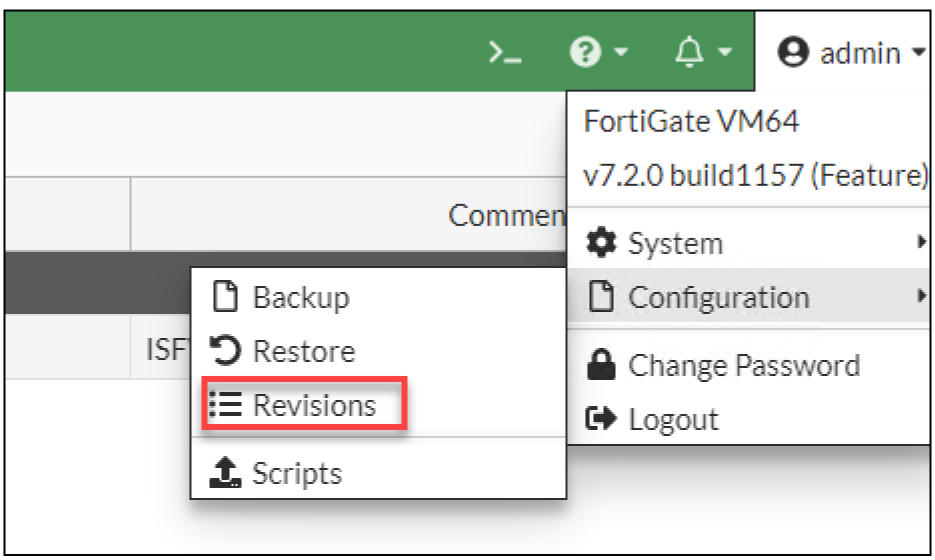
port7 and port8 indicate that rogue devices are connected.

Restore the FortiGate Configuration

Before you begin this task, you must restore configuration files to ISFW FortiGate, NGFW FortiGate, and DCFW FortiGate. VLANs, address objects, static routes, and firewall policies have been preconfigured for this exercise.

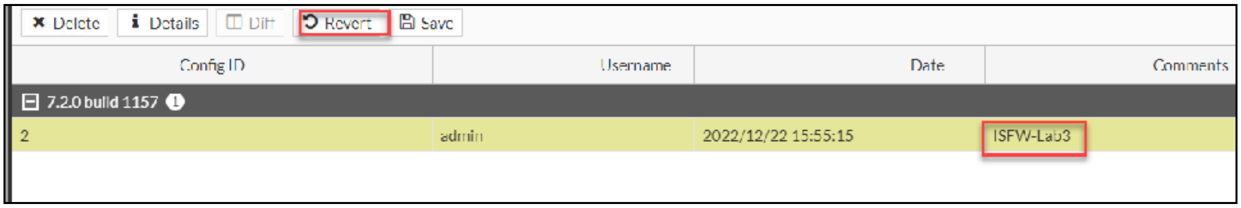
To restore the ISFW FortiGate configuration file

1. On the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **ISFW** FortiGate login page bookmark.
2. Log in with the username `admin` and password `password`.
3. In the upper-right corner, click **admin**, and then click **Configuration** > **Revisions**.



4. Click **+** to expand the list, select the configuration with the **ISFW-Lab3** comment, and then click **Revert**.

DO NOT REPRINT
© FORTINET



5. Click **OK** to reboot.

To restore the NGFW FortiGate configuration file

1. On the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **NGFW** FortiGate login page bookmark.
2. Log in with the username `admin` and password `password`.
3. In the upper-right corner, click **admin**, and then click **Configuration** > **Revisions**.
4. Click **+** to expand the list, select the configuration with the **NGFW-Lab3** comment, and then click **Revert**.
5. Click **OK** to reboot.

To restore the DCFW FortiGate configuration file

1. On the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **DCFW** FortiGate login page bookmark.
2. Log in with the username `admin` and password `password`.
3. In the upper-right corner, click **admin**, and then click **Configuration** > **Revisions**.
4. Click **+** to expand the list, select the configuration with the **DCFW-Lab3** comment, and then click **Revert**.
5. Click **OK** to reboot.

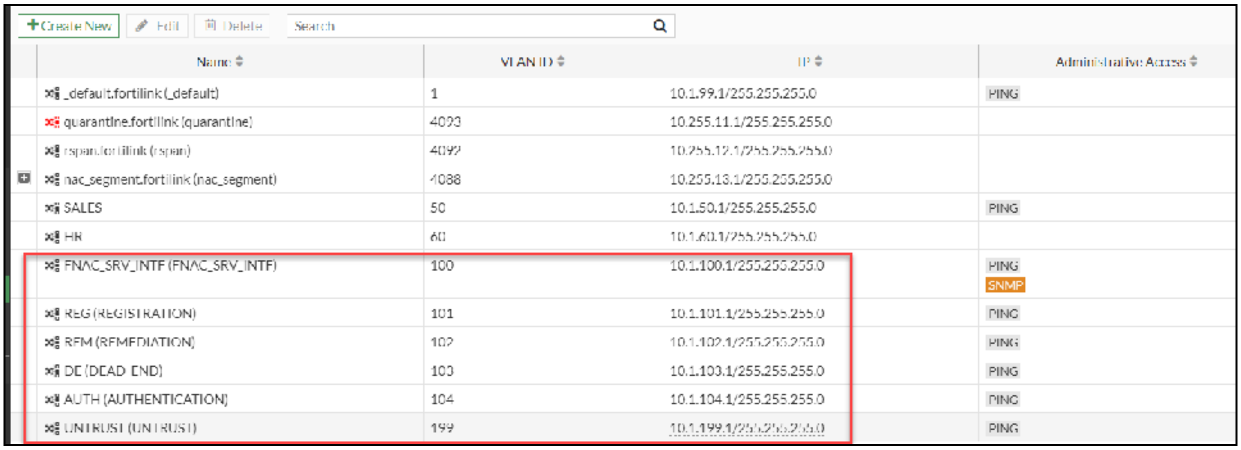
Review FortiNAC Service and Captive VLANs

You will review captive VLANs that FortiGate will use.

To review VLANs on FortiSwitch using the FortiGate switch controller

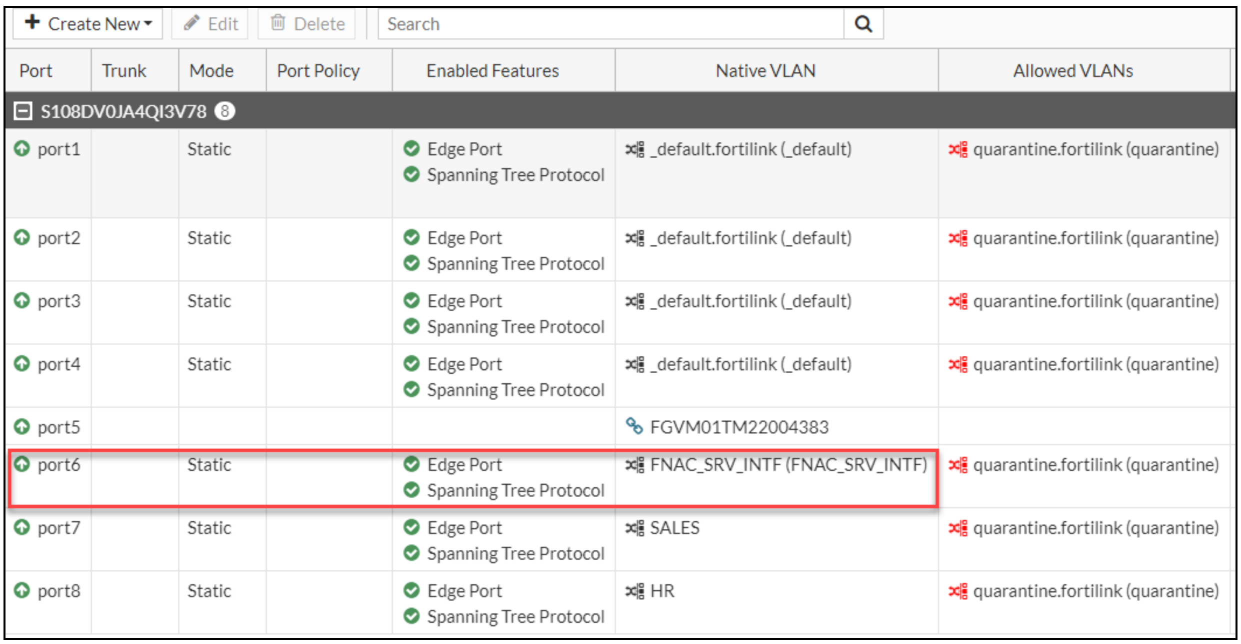
1. Return to the ISFW FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **WiFi & Switch Controller** > **FortiSwitch VLANs**, and then review the six new VLAN interfaces, VLAN IDs, and IP addresses.

DO NOT REPRINT
© FORTINET



Name	VLAN ID	IP	Administrative Access
_default.fortilink (_default)	1	10.1.99.1/255.255.255.0	PING
quarantine.fortilink (quarantine)	4093	10.255.11.1/255.255.255.0	
rspan.fortilink (rspan)	4092	10.255.12.1/255.255.255.0	
nac_segment.fortilink (nac_segment)	4088	10.255.13.1/255.255.255.0	
SALES	50	10.1.50.1/255.255.255.0	PING
HR	60	10.1.60.1/255.255.255.0	
FNAC_SRV_INTF (FNAC_SRV_INTF)	100	10.1.100.1/255.255.255.0	PING SNMP
REG (REGISTRATION)	101	10.1.101.1/255.255.255.0	PING
REM (REMEDIATION)	102	10.1.102.1/255.255.255.0	PING
DE (DEAD END)	103	10.1.103.1/255.255.255.0	PING
AUTH (AUTHENTICATION)	104	10.1.104.1/255.255.255.0	PING
UNTRUST (UNTRUST)	199	10.1.199.1/255.255.255.0	PING

3. Click **WiFi & Switch Controller** > **FortiSwitch Ports**, and then verify the native VLAN of **port6** is set to **FNAC_SRV_INTF**.



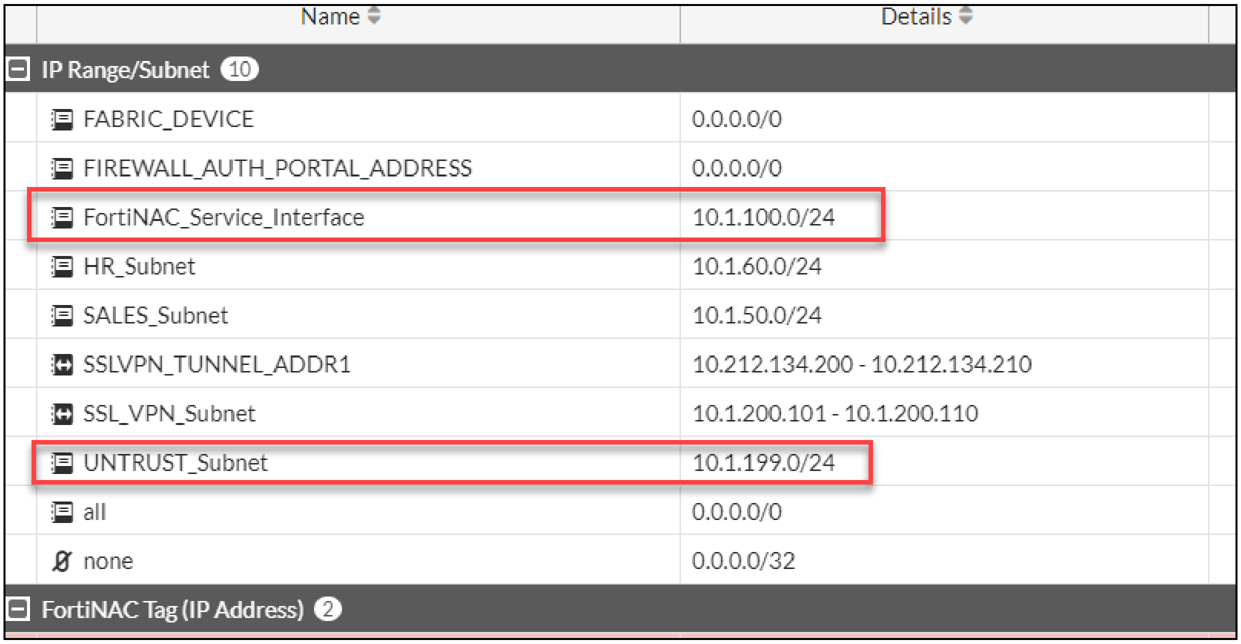
S108DV0JA4QI3V78 8

Port	Trunk	Mode	Port Policy	Enabled Features	Native VLAN	Allowed VLANs
port1		Static		Edge Port Spanning Tree Protocol	_default.fortilink (_default)	quarantine.fortilink (quarantine)
port2		Static		Edge Port Spanning Tree Protocol	_default.fortilink (_default)	quarantine.fortilink (quarantine)
port3		Static		Edge Port Spanning Tree Protocol	_default.fortilink (_default)	quarantine.fortilink (quarantine)
port4		Static		Edge Port Spanning Tree Protocol	_default.fortilink (_default)	quarantine.fortilink (quarantine)
port5					FGVM01TM22004383	
port6		Static		Edge Port Spanning Tree Protocol	FNAC_SRV_INTF (FNAC_SRV_INTF)	quarantine.fortilink (quarantine)
port7		Static		Edge Port Spanning Tree Protocol	SALES	quarantine.fortilink (quarantine)
port8		Static		Edge Port Spanning Tree Protocol	HR	quarantine.fortilink (quarantine)

You may need to wait a few minutes for the FortiSwitch to come back online.

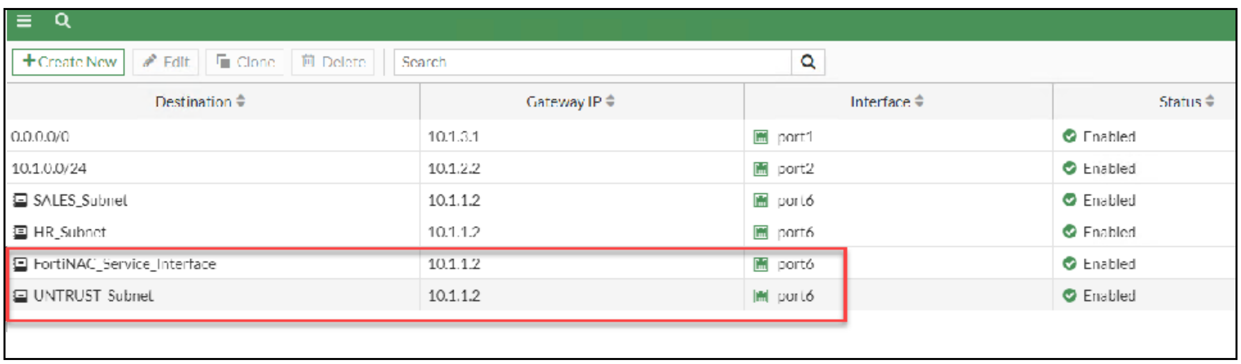
4. Return to the NGFW FortiGate GUI, and then log in with the username `admin` and password `password`.
5. Click **Policy & Objects** > **Addresses**, and then review the **FortiNAC_Service_Interface** and **UNTRUST_Subnet** address objects.

DO NOT REPRINT
© FORTINET



Name	Details
IP Range/Subnet 10	
FABRIC_DEVICE	0.0.0.0/0
FIREWALL_AUTH_PORTAL_ADDRESS	0.0.0.0/0
FortiNAC_Service_Interface	10.1.100.0/24
HR_Subnet	10.1.60.0/24
SALES_Subnet	10.1.50.0/24
SSLVPN_TUNNEL_ADDR1	10.212.134.200 - 10.212.134.210
SSL_VPN_Subnet	10.1.200.101 - 10.1.200.110
UNTRUST_Subnet	10.1.199.0/24
all	0.0.0.0/0
none	0.0.0.0/32
FortiNAC Tag (IP Address) 2	

6. Click **Network** > **Static Routes**, and then review the static route for the **FortiNAC_Service_Interface** and **UNTRUST_Subnet** destinations.



Destination	Gateway IP	Interface	Status
0.0.0.0/0	10.1.3.1	port1	Enabled
10.1.0.0/24	10.1.2.2	port2	Enabled
SALES_Subnet	10.1.1.2	port6	Enabled
HR_Subnet	10.1.1.2	port6	Enabled
FortiNAC_Service_Interface	10.1.1.2	port6	Enabled
UNTRUST_Subnet	10.1.1.2	port6	Enabled

7. Return to the DCFW FortiGate GUI, and then log in with the username `admin` and password `password`.
8. Click **Network** > **Static Routes**, and then review the static route for the **FortiNAC_Service_Interface** and **UNTRUST_Subnet** destinations.

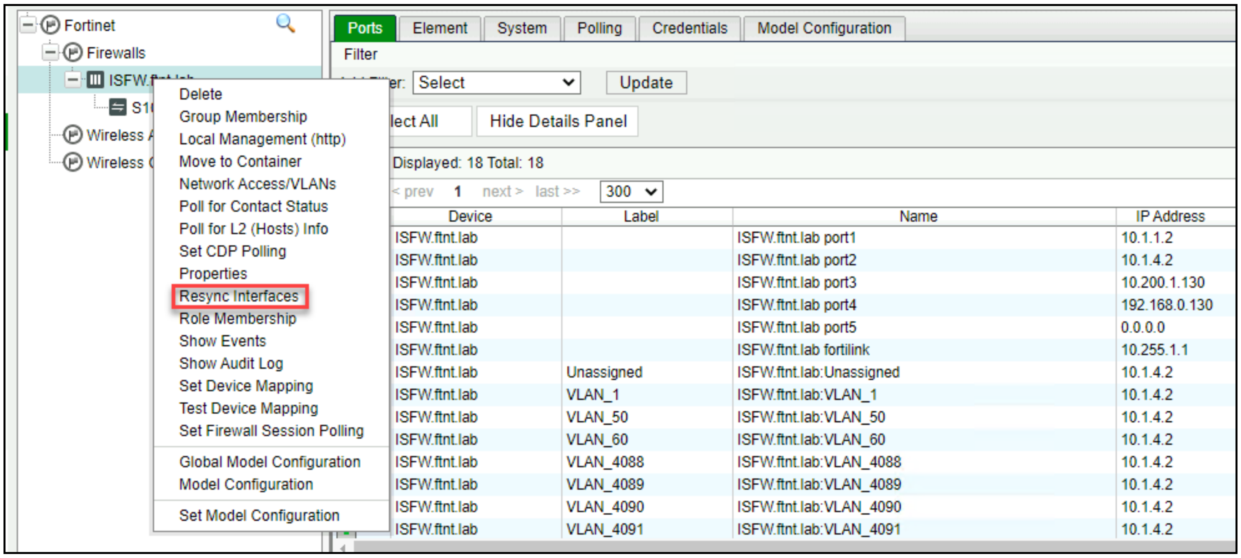
Configure FortiGate Device Modeling

You will configure device modeling on FortiNAC for FortiGate devices.

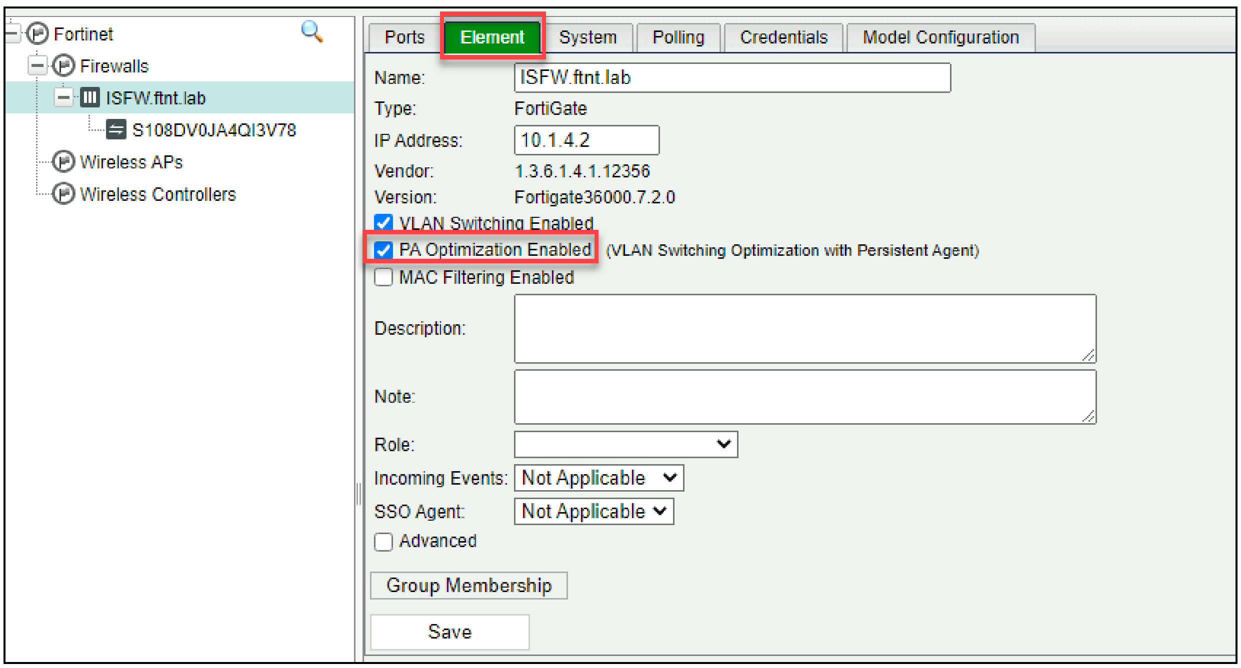
To configure device modeling on FortiNAC

1. On the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **FortiNAC** login page bookmark.
2. Log in to the FortiNAC GUI with the username `admin` and password `Password1!`.
3. Click **Network** > **Inventory**, expand the **Firewalls** section, right-click the **ISFW.ftnt.lab** firewall, and then click **Resync Interfaces** to update the inventory with new VLANs, as shown in the following image:

DO NOT REPRINT
© FORTINET

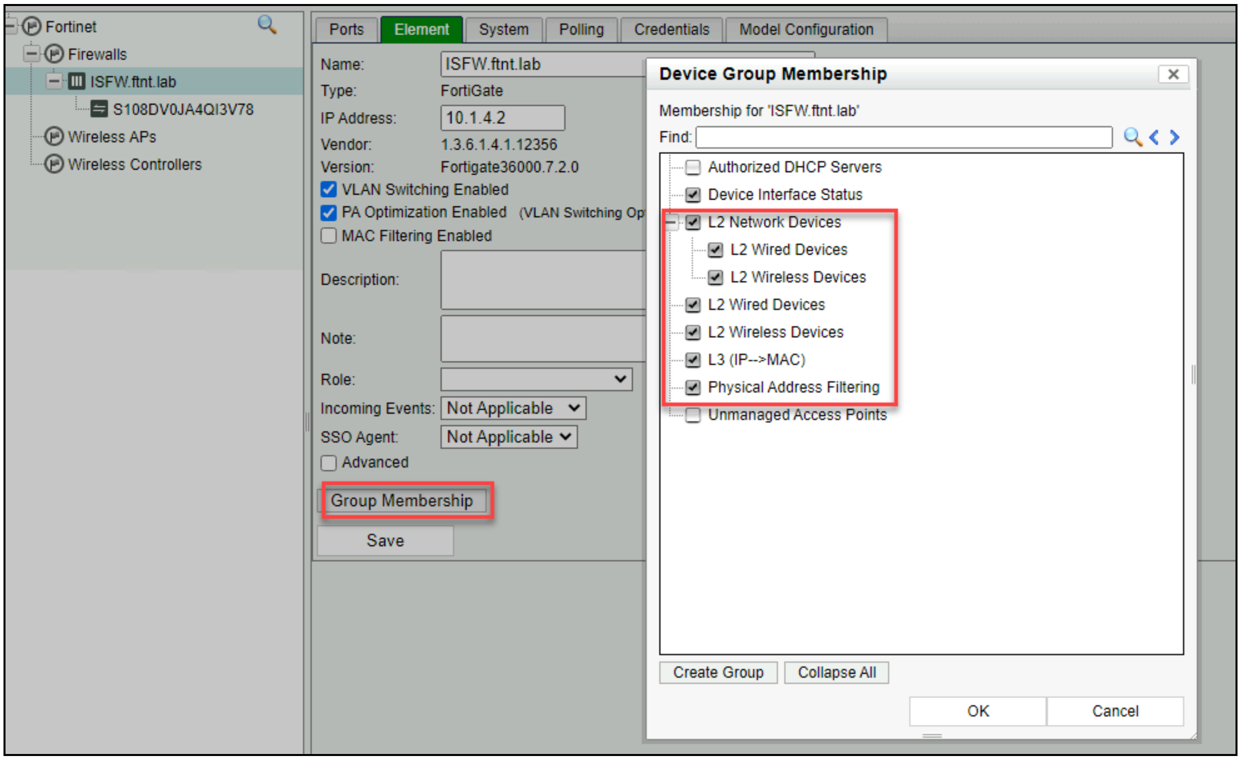


4. Click **Yes**.
5. Click the **Element** tab, and then select the **PA Optimization Enabled** checkbox.

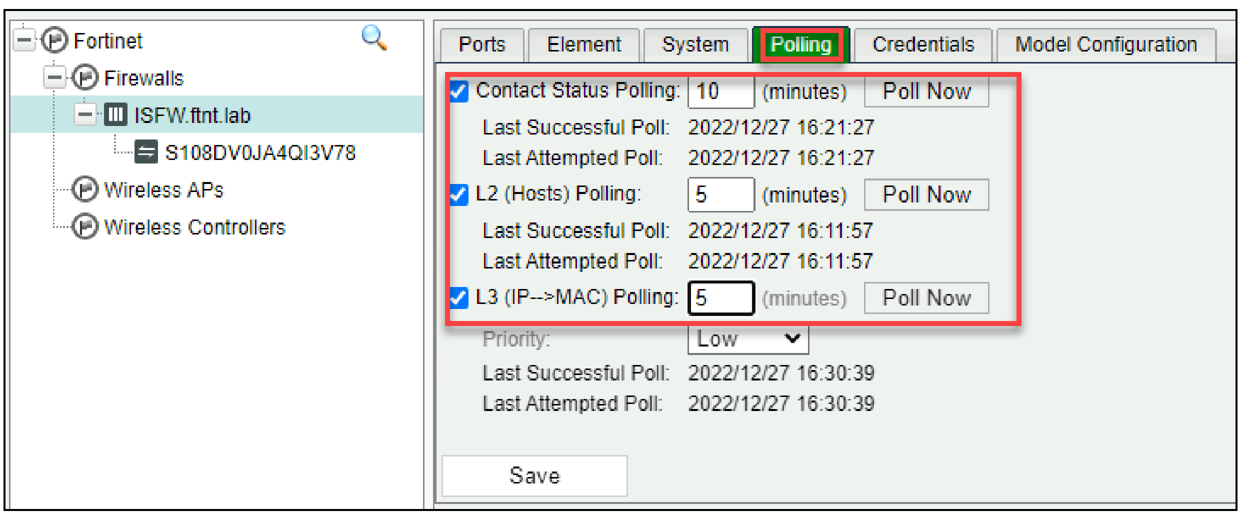


6. Click **Group Membership**, select the **Device Interface Status**, **L2 Network Devices**, **L2 Wired Devices**, **L2 Wireless Devices**, **L3 (IP --> MAC)**, and **Physical Address Filtering** checkboxes, and then click **OK**.

DO NOT REPRINT
© FORTINET



7. Click **OK**.
8. Click **Save**.
9. Click the **Polling** tab, and then change the **L2 (Hosts) Polling** and **L3 (IP-->MAC) Polling** fields to 5 **minutes**.



10. Click **Save**.
11. Click the **Virtualized Devices** tab, select the **root** VDOM, and then click **Model Configuration**.

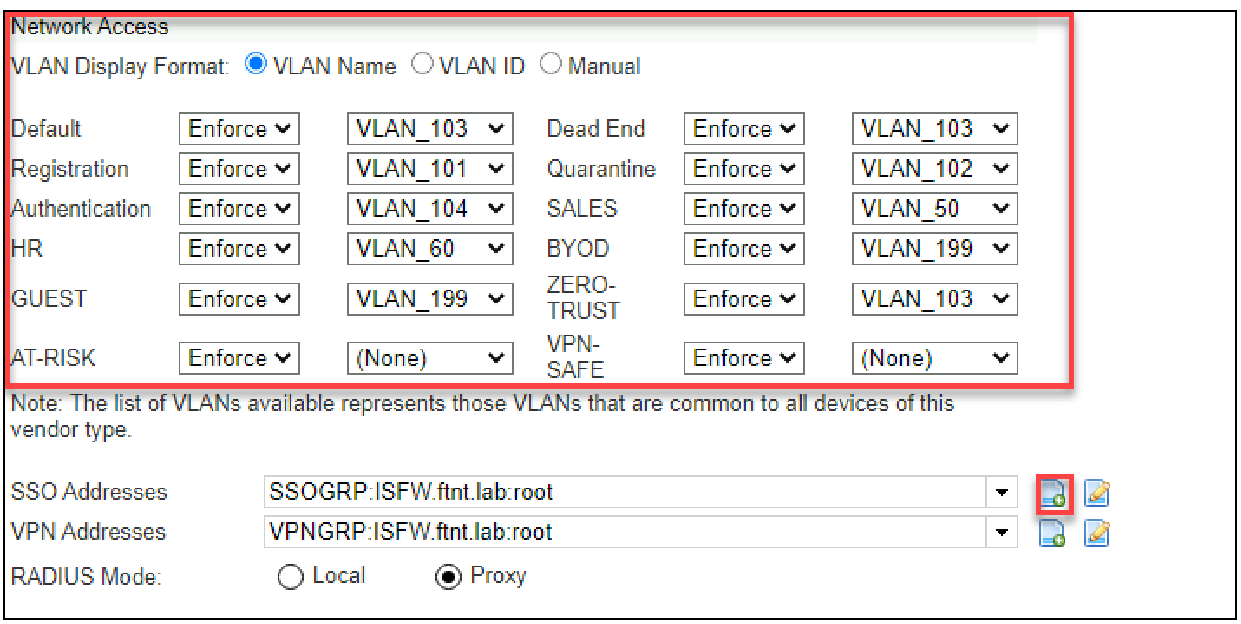
If you can't see the **Virtualized Devices** tab, in the left panel, right-click the **ISFW.ftnt.lab** device, select **Resync Interfaces** again, and then refresh the browser.

DO NOT REPRINT
© FORTINET

12. In the **Network Access** section, configure the following settings:

Network	Status	VLAN ID
Default	Enforce	VLAN_103
Dead End	Enforce	VLAN_103
Registration	Enforce	VLAN_101
Quarantine	Enforce	VLAN_102
Authentication	Enforce	VLAN_104
SALES	Enforce	VLAN_50
HR	Enforce	VLAN_60
BYOD	Enforce	VLAN_199
GUEST	Enforce	VLAN_199
ZERO-TRUST	Enforce	VLAN_103
AT-RISK	Enforce	None
VPN-SAFE	Enforce	None

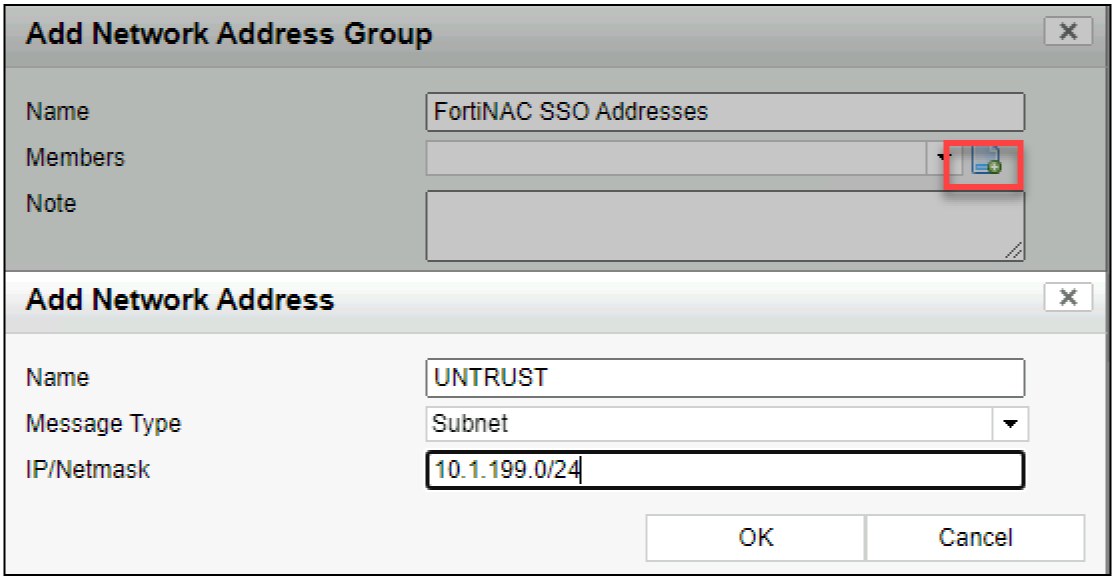
13. In the **SSO Addresses** field, click the **add** icon to add a new **Network Address Group**.



14. In the **Name** field, type `FortiNAC SSO Addresses`, and then click the **add** icon to configure a new **Network Address** with the following settings:

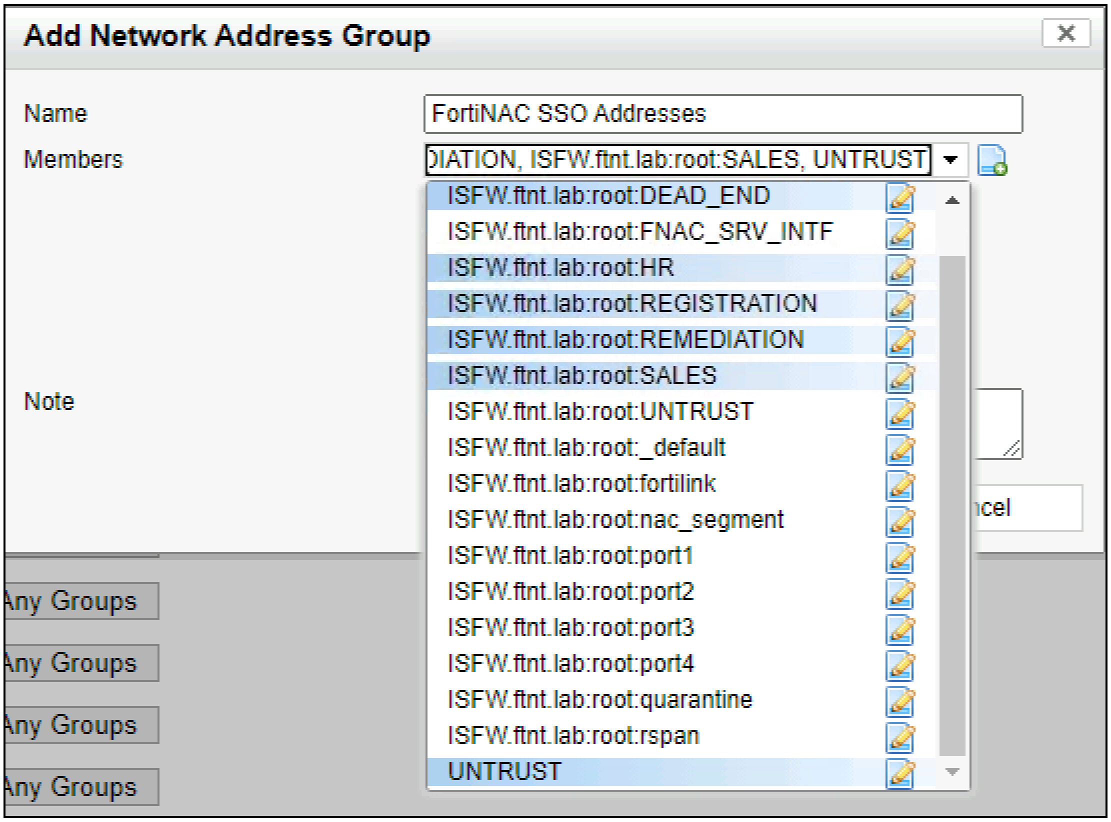
DO NOT REPRINT
© FORTINET

Field	Value
Name	UNTRUST
Message Type	Subnet
IP/Netmask	10.1.199.0/24



15. Click **OK**.
16. In the **Members** field, select **ISFW.ftnt.lab:root:HR**, **ISFW.ftnt.lab:root:SALES**, **ISFW.ftnt.lab:root:AUTHENTICATION**, **ISFW.ftnt.lab:root:DEAD_END**, **ISFW.ftnt.lab:root:REGISTRATION**, **ISFW.ftnt.lab:root:REMEDIATION**, and **UNTRUST**.

DO NOT REPRINT
© FORTINET

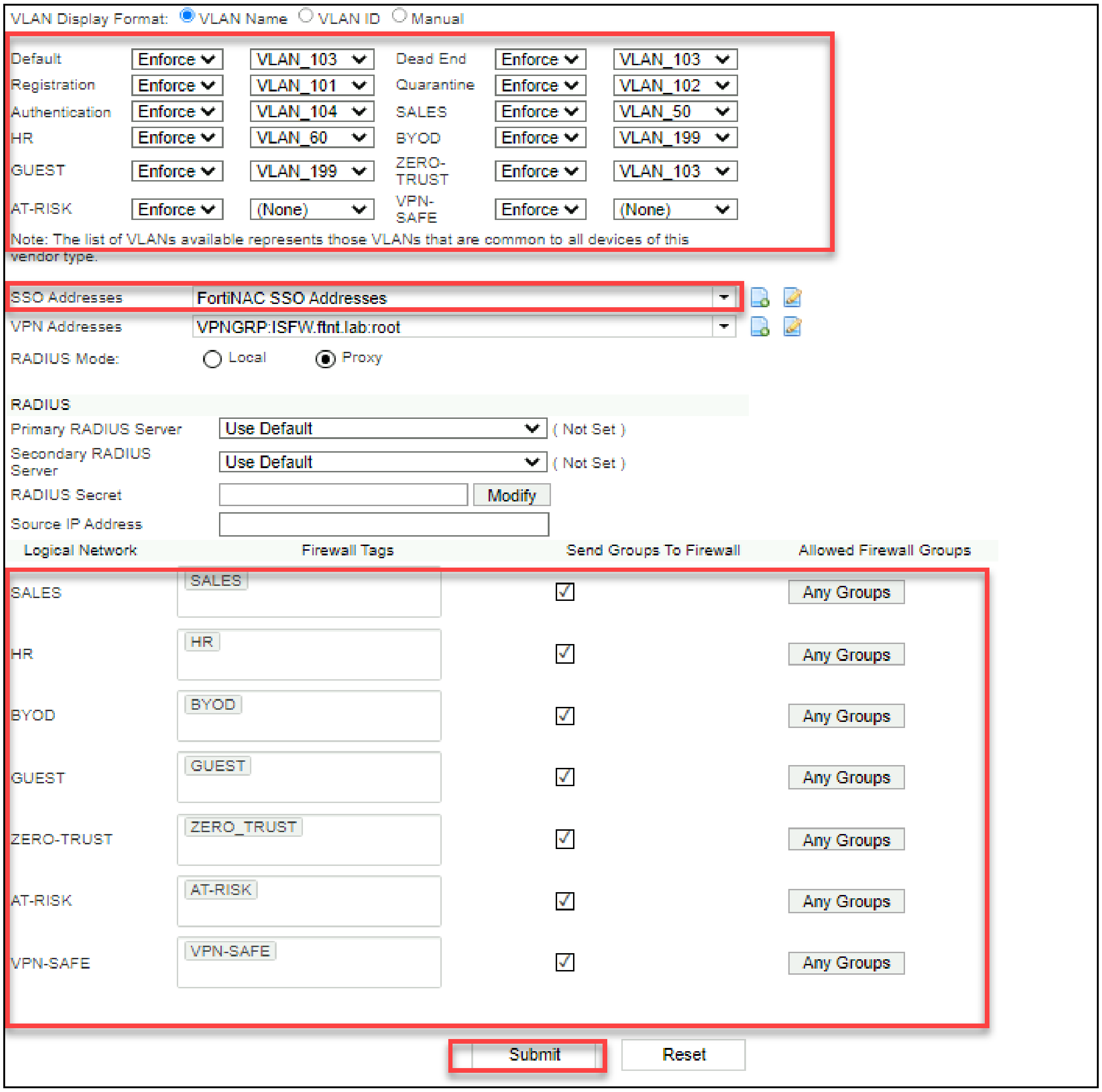


These are VLAN interfaces configured on ISFW FortiGate.

17. Click **OK**.
18. In the table at the bottom of the page, configure the following settings:

Logical Network	Firewall Tags	Send Groups To Firewall
SALES	SALES	Select the checkbox.
HR	HR	Select the checkbox.
BYOD	BYOD	Select the checkbox.
GUEST	GUEST	Select the checkbox.
ZERO-TRUST	ZERO-TRUST	Select the checkbox.
AT-RISK	AT_RISK	Select the checkbox.
VPN-SAFE	VPN-SAFE	Select the checkbox.

DO NOT REPRINT
© FORTINET



19. Ensure that the model configuration for the device looks like the image above, and then click **Submit** to save the settings.

DO NOT REPRINT
© FORTINET

Lab 3B: Network Access Security With FortiNAC

In this lab, you will integrate FortiNAC with Active Directory and the Fortinet Security Fabric, learn how to profile devices based on various factors, and then provide access based on device and user roles.

Objectives

- Integrate FortiNAC with Active Directory
- Add FortiNAC to the Security Fabric
- Configure device profiling and registration
- Configure dynamic policies with user roles

Time to Complete

Estimated: 90 minutes

DO NOT REPRINT
© FORTINET

Exercise 1: Integrating FortiNAC With ISFW FortiGate and Active Directory

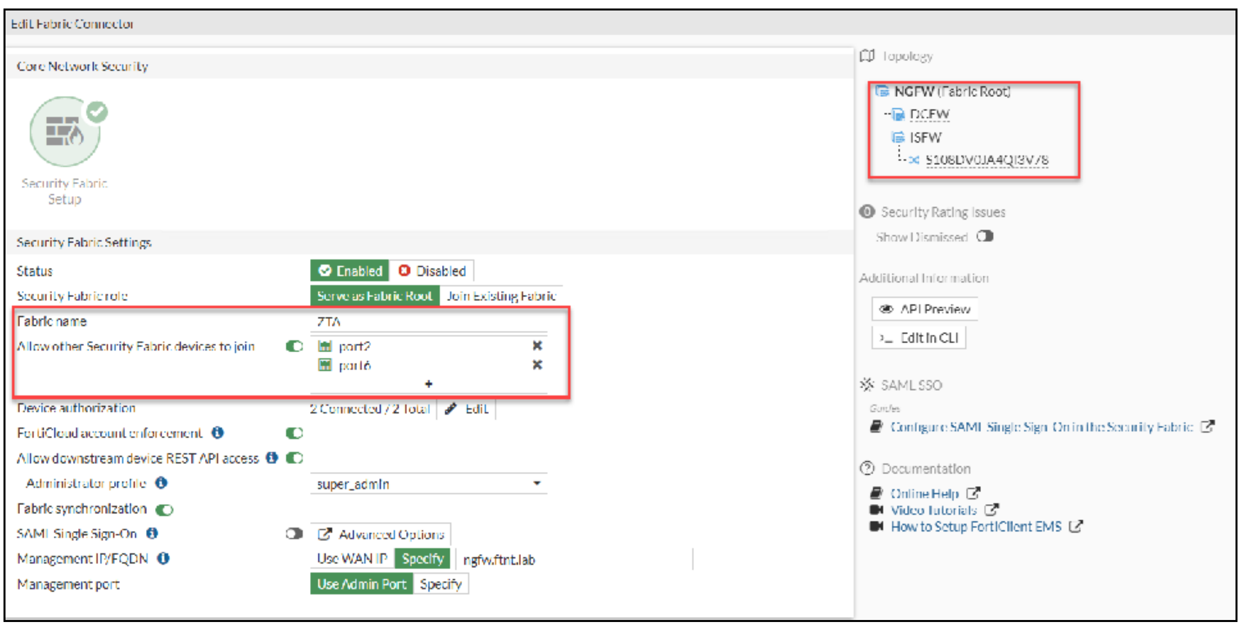
In this exercise, you will integrate FortiNAC with ISFW FortiGate using service connectors. You will also integrate FortiNAC with Active Directory.

Integrate With ISFW FortiGate Using Service Connectors

You will add ISFW FortiGate on FortiNAC using service connectors.

To add FortiGate using the FortiNAC service connector

1. On the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **NGFW** login page bookmark.
2. Log in with the username `admin` and password `password`.
3. Click **Security Fabric** > **Fabric Connectors**.
4. In the list, select **Security Fabric Setup (ZTA)**, and then click **Edit** to review the current **Security Fabric Settings** on the root FortiGate.

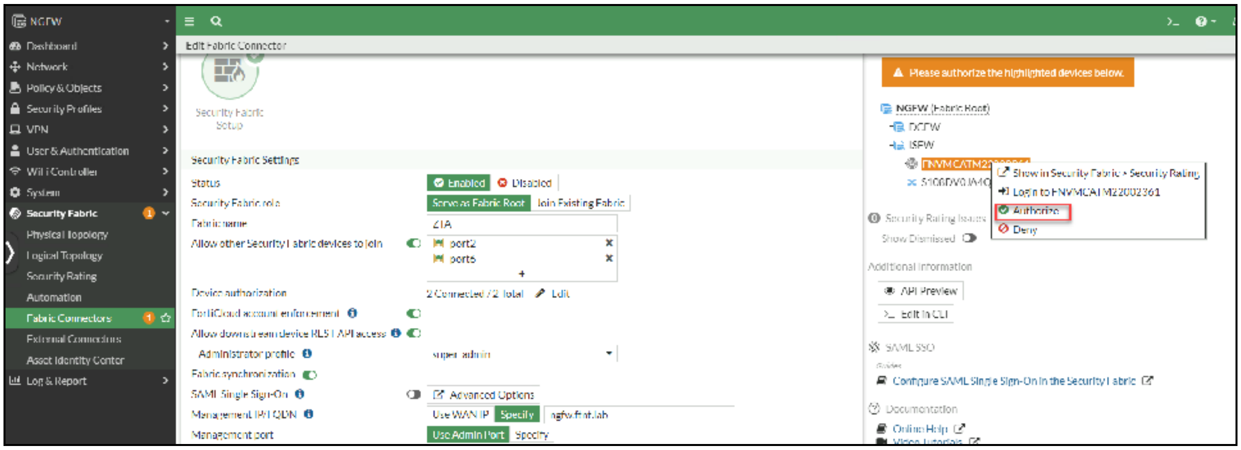


5. Open a new Google Chrome tab, and then in **Bookmarks**, select the **FortiNAC** login page bookmark.
6. Log in to the FortiNAC GUI with the username `admin` and password `Password1!`.
7. Click **Network** > **Service Connectors**, and then click **Create New**.
8. Click **Security Fabric Connection**, type the IP address `10.1.4.2`, and then click **OK**.

DO NOT REPRINT
© FORTINET

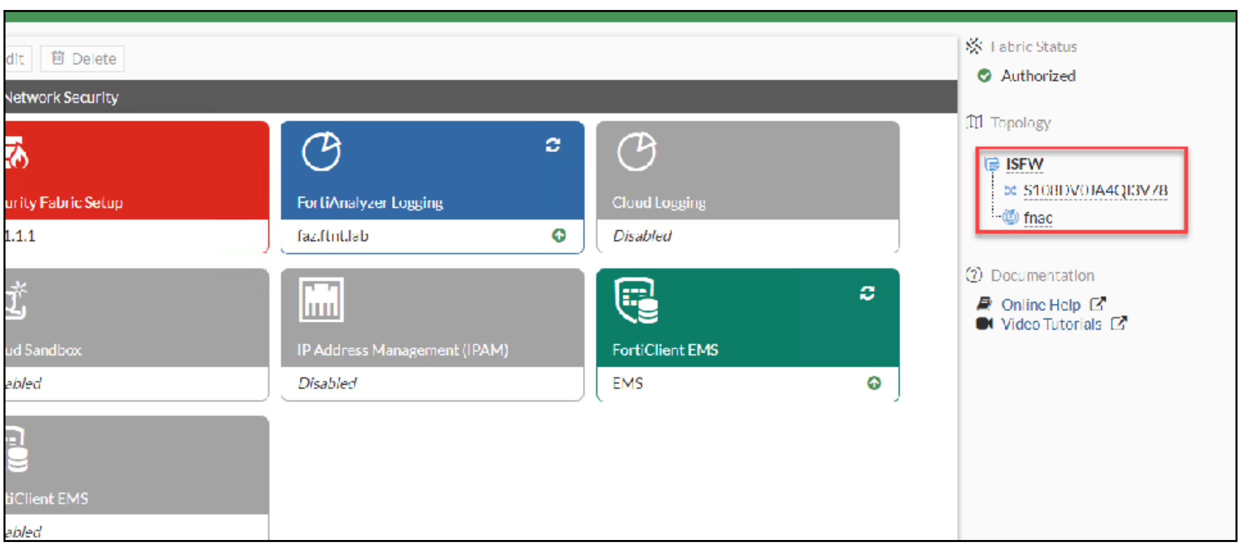
Although you enter the IP address for ISFW FortiGate, since NGFW FortiGate is the root device of the Security Fabric, the approval request appears on NGFW FortiGate instead of ISFW FortiGate.

9. Return to the NGFW GUI, click **Security Fabric** > **Fabric Connectors**, and then note the FortiNAC serial number that is displayed in the **Fabric Connectors** topology on the right.
10. Highlight the serial number, and then click **Authorize** to approve the FortiNAC service connector request.



This approves and adds the FortiNAC on both NGFW FortiGate and ISFW FortiGate.

11. Open a new Google Chrome tab, and then in **Bookmarks**, select the **ISFW** login page bookmark.
12. Log in with the username `admin` and password `password`.
13. Click **Security Fabric** > **Fabric Connectors**, and then under **ISFW**, hover over the FortiNAC icon to verify the connection status.



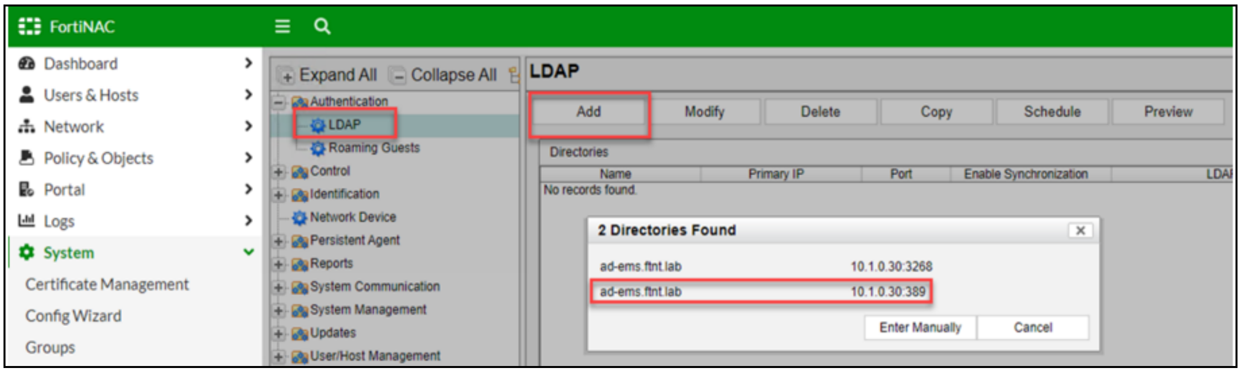
DO NOT REPRINT
© FORTINET

Integrate Active Directory With FortiNAC

You will integrate Active Directory with FortiNAC.

To integrate Active Directory with FortiNAC

1. Return to the FortiNAC GUI, click **System** > **Settings**, and then expand the **Authentication** section.
2. Click **LDAP**, and then click **Add**.
   You should see that the AD-EMS server was auto-discovered.

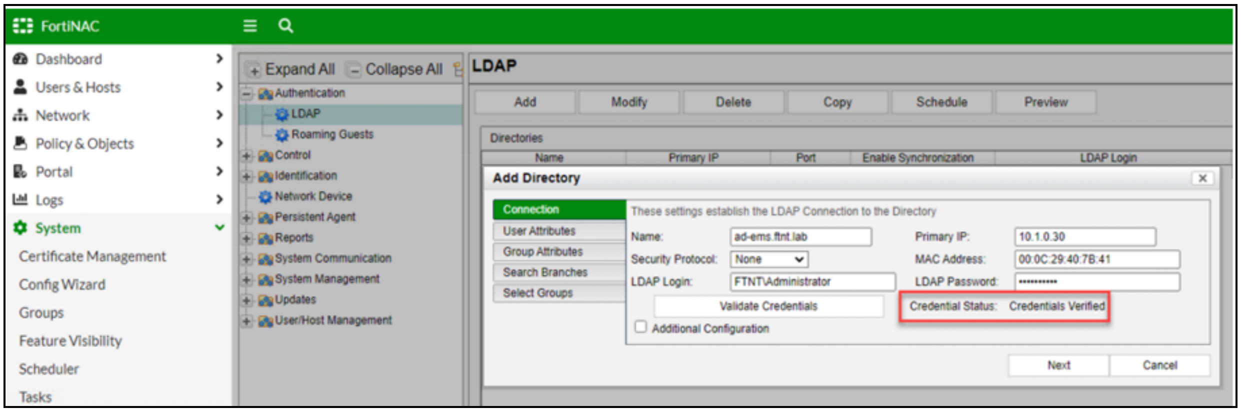


If you do not see the AD-EMS server as part of the auto-discovery process, you can still enter the same details manually.

3. Click the **ad-ems.ftnt.lab** server listening on **10.1.0.30:389** (the second option in the image above), configure the following settings, and then click **Validate Credentials**:

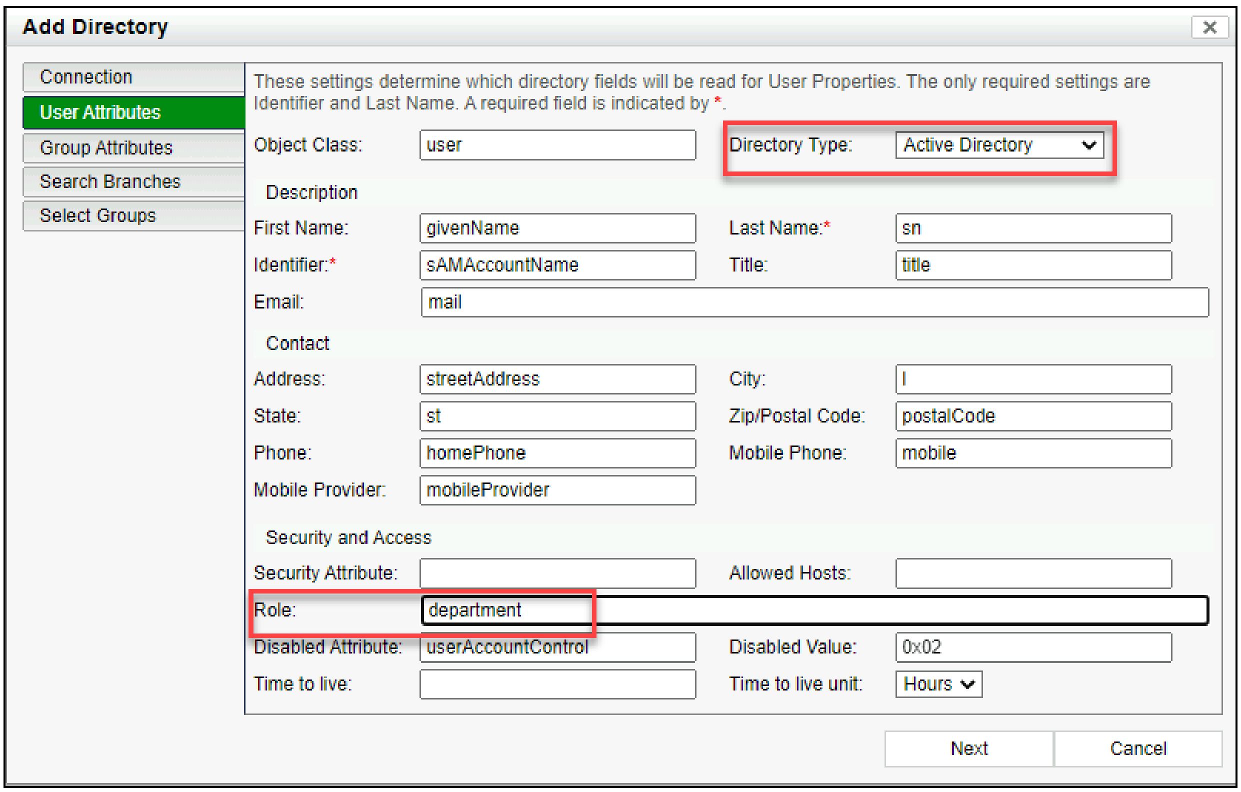
Field	Value
Name	ad-ems.ftnt.lab
Primary IP	10.1.0.30
Security Protocol	None
MAC Address	00:0C:29:40:7B:41
LDAP Login	FTNT\Administrator
LDAP Password	Password1!

DO NOT REPRINT
© FORTINET



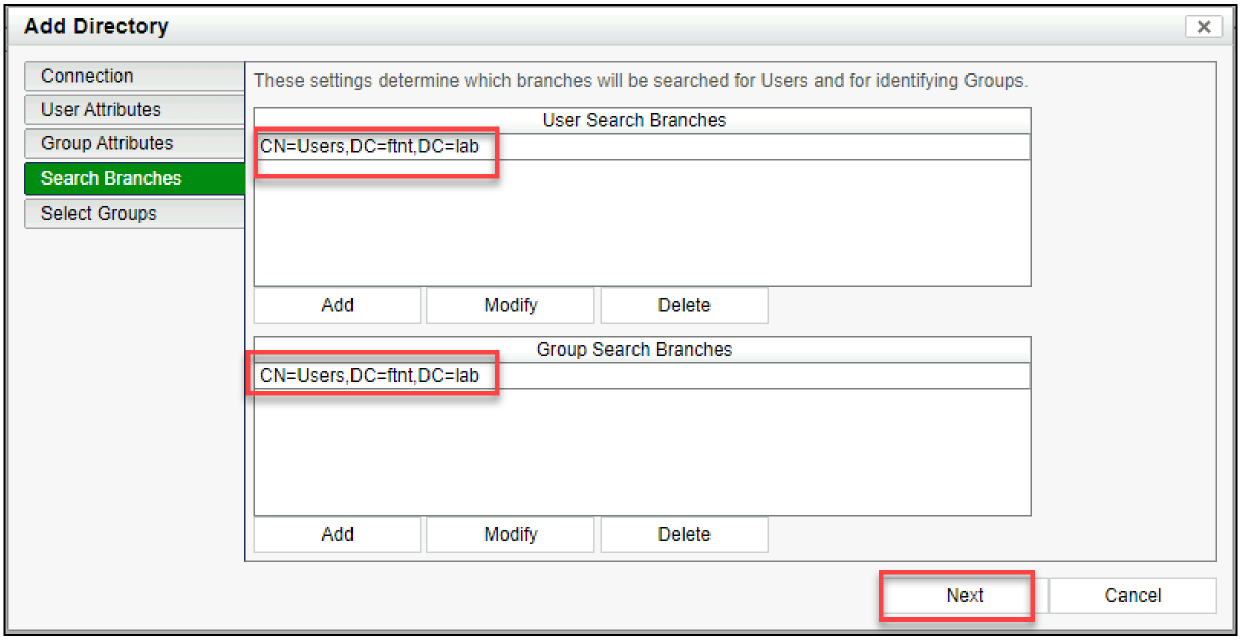
The **Credential Status** field should show **Credentials Verified.** If it does not, validate the settings, and then try again.

4. Click **Next.**
5. Ensure the **Directory Type** field is set to **Active Directory**, and then in the **Role** field, type `department`.



6. Leave all other options at the default settings, and then click **Next**.
7. Ensure the **Object Class** field is set to **group**, leave all other options at the default settings, and then click **Next**.
8. In the **User Search Branches** section, click **Add**, select **CN=Users,DC=ftnt,DC=lab**, and then click **OK**.
9. In the **Group Search Branches** section, click **Add**, select **CN=Users,DC=ftnt,DC=lab**, and then click **OK**.

DO NOT REPRINT
© FORTINET

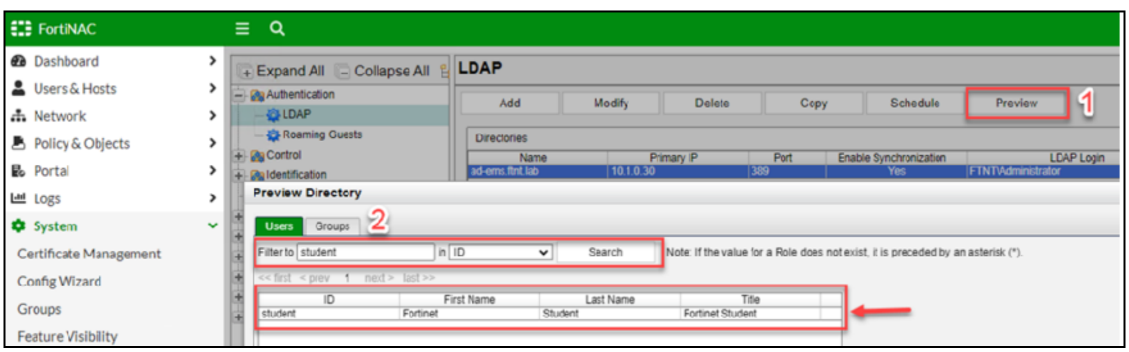


10. Click **Next**.
11. In the list of available groups to be imported, select the **Corporate** group, and then click **OK**.

Users from the directory are added to the FortiNAC database only when they connect to the network and register.

12. Click **Preview**, in the **Filter to** field, type `student`, in the **in** field, select **ID**, and then click **Search** to validate the LDAP connection.

    This should return a result.



13. Click **OK**.

DO NOT REPRINT
© FORTINET

Exercise 2: Configuring Device Profiling and Registration

In this exercise, you will create device profiling rules on FortiNAC for a domain connected PC. You will also configure firewall policies on ISFW FortiGate to allow traffic between FortiNAC and captive networks.

Configure Device Profiling for a Domain Connected PC

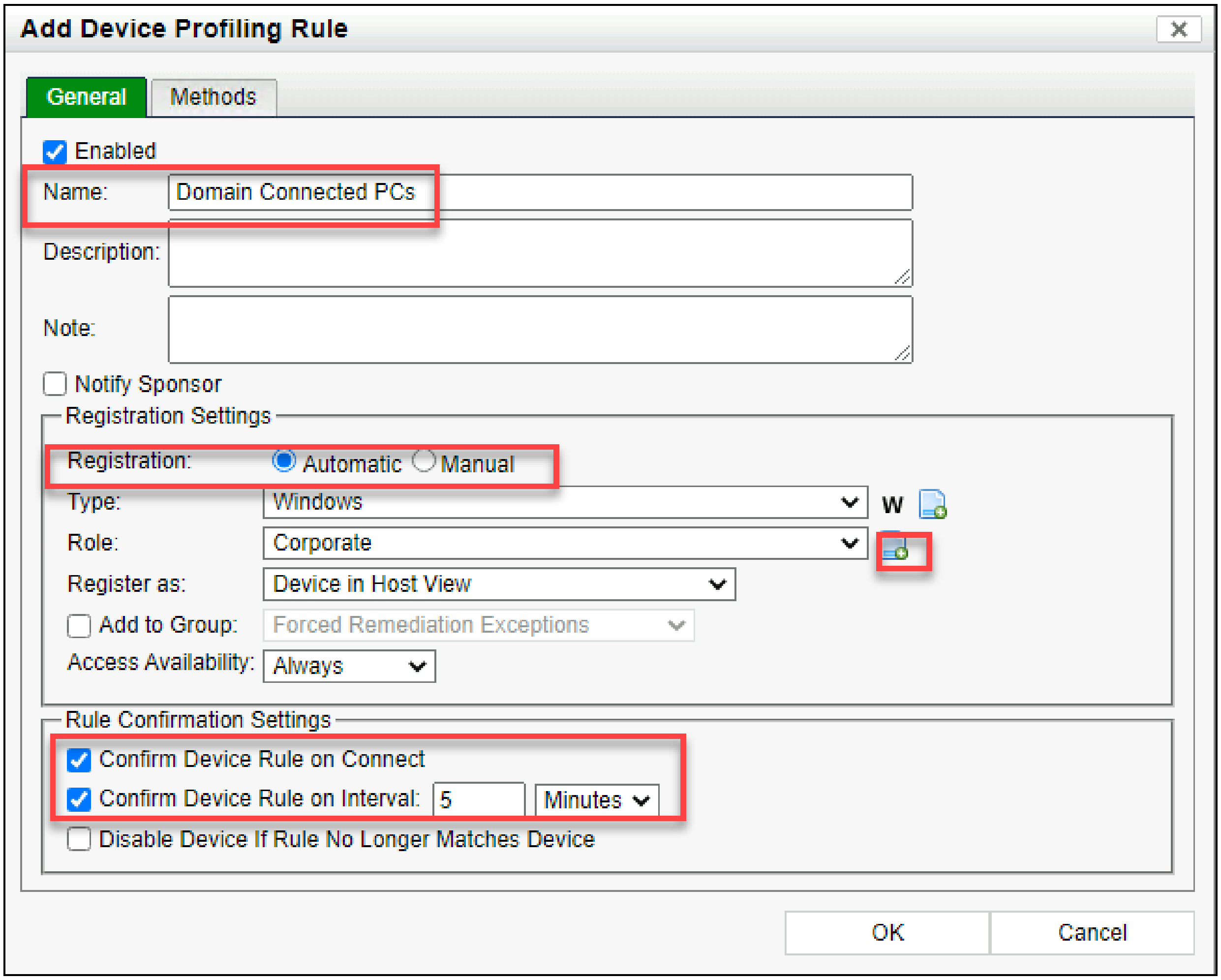
You will add and test device profiling rules on FortiNAC.

To add device profiling rules

1. On the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **FortiNAC** login page bookmark.
2. Log in to the FortiNAC GUI with the username `admin` and password `Password1!`.
3. Click **Users & Hosts** > **Device Profiling Rules**, click **Add**, and then on the **General** tab, configure the following settings to create a new device profiling rule:

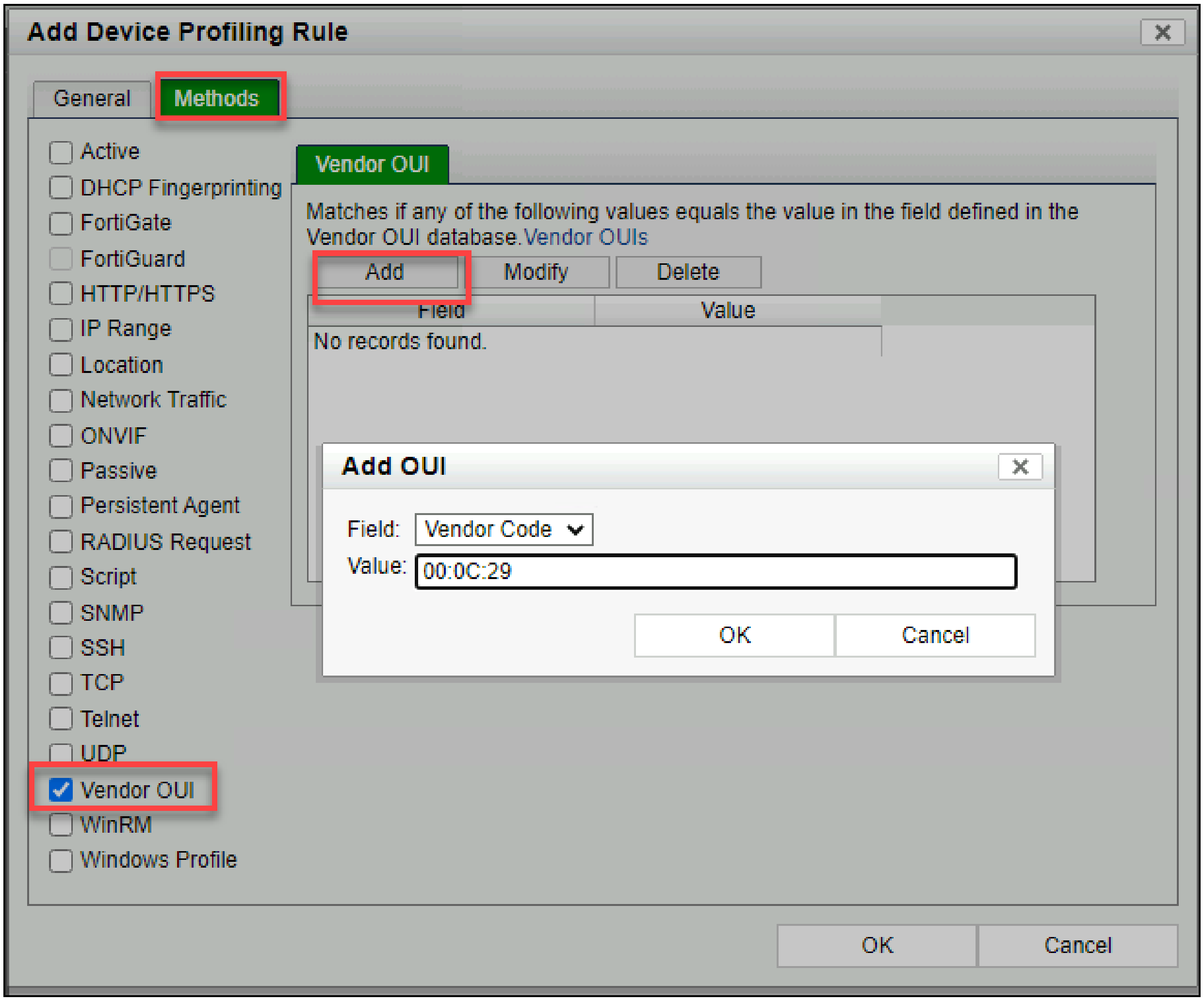
Field	Value
Enabled	Select the checkbox.
Name	Domain Connected PCs
Registration	Automatic
Type	Windows
Role	Add a new role called `Corporate`.
Register as	Device in Host View
Confirm Device Rule on Connect	Select the checkbox.
Confirm Device Rule on Interval	Select the checkbox, type `5`, and then select **Minutes**.

DO NOT REPRINT
© FORTINET



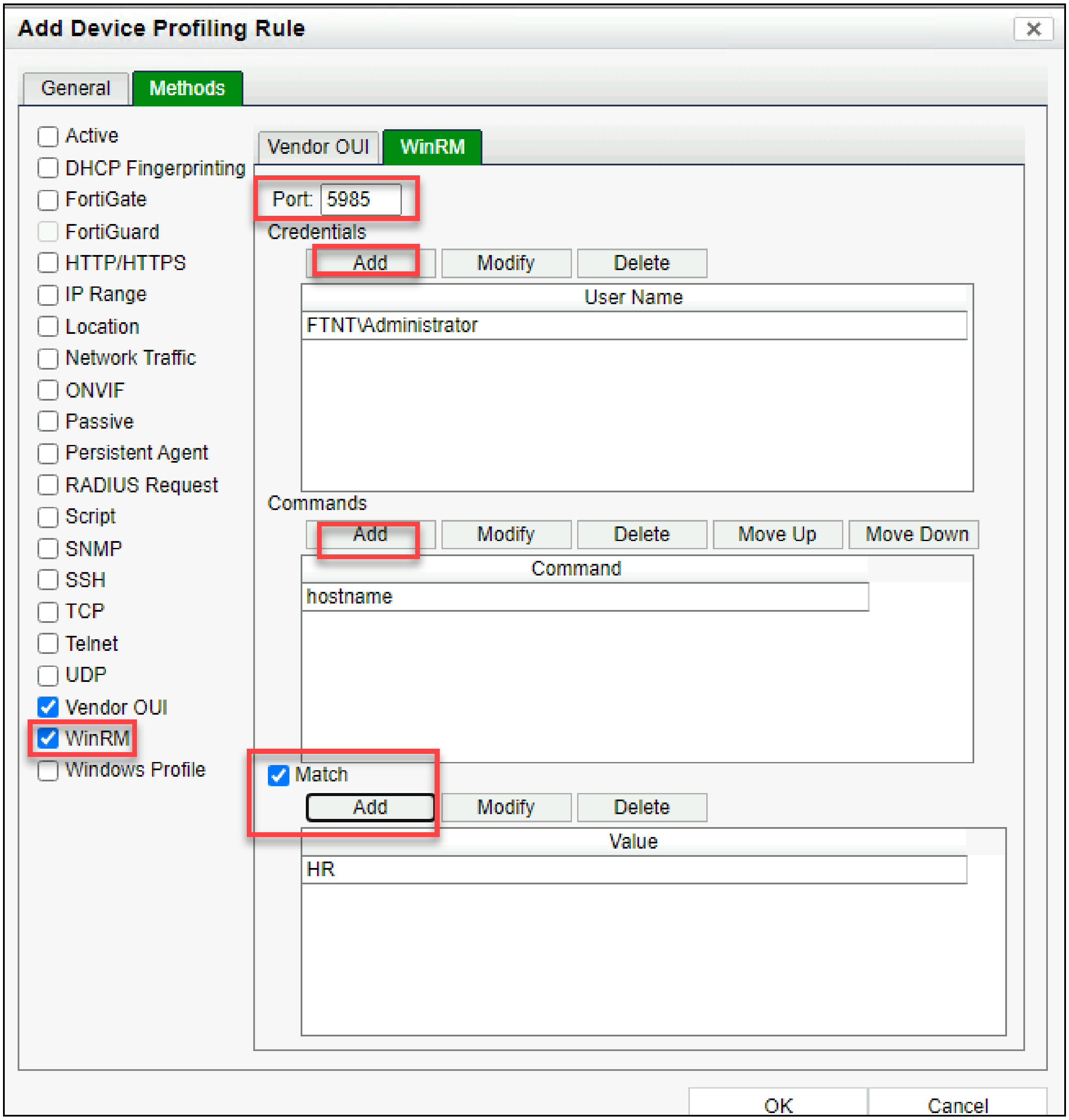
4. Click the **Methods** tab, select the **Vendor OUI** checkbox, and then click **Add**.
5. In the **Add OUI** window, in the **Field** field, select **Vendor Code**, in the **Value** field, type `00:0C:29`, and then click **OK**.

DO NOT REPRINT
© FORTINET



6. On the **Methods** tab, select the **WinRM** checkbox, and then change the **Port** field to `5985`.
7. In the **Credentials** section, click **Add**, in the **User Name** field, type `FTNT\Administrator`, in the **Password** field, type `Password1!`, and then click **OK**.
8. In the **Commands** section, click **Add**, in the **Command** field, type `hostname`, and then click **OK**.
9. Select the **Match** checkbox, click **Add**, in the **Value** field, type `HR`, and then click **OK**.

DO NOT REPRINT
© FORTINET

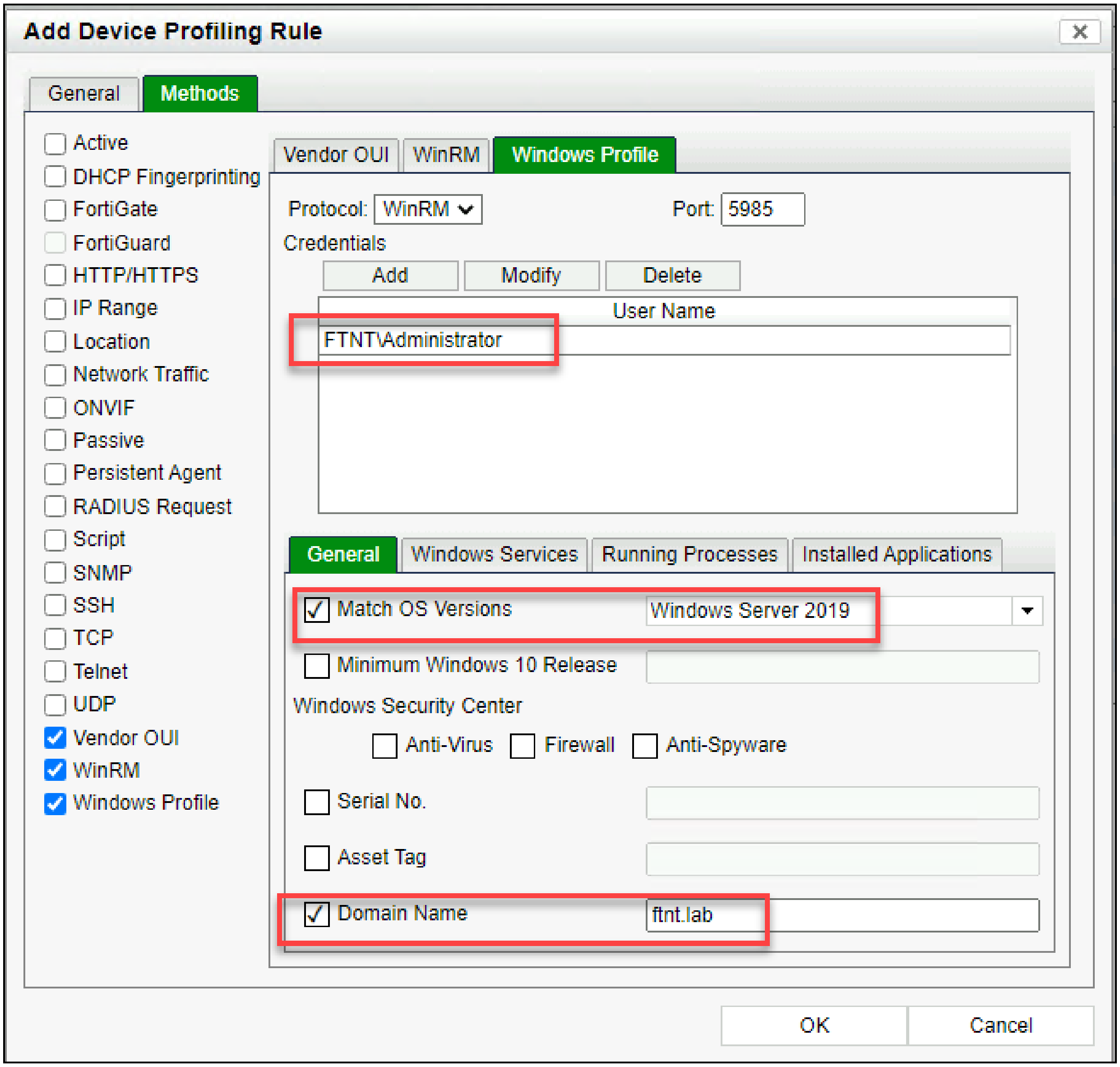


Values are case-sensitive and FortiNAC looks for an exact match. However, you can also combine values with wildcards where you need wider match criteria.

10. On the **Methods** tab, select the **Windows Profile** checkbox, ensure the **Protocol** field is set to **WinRM**, and then change the **Port** field to `5985`.
11. In the **Credentials** section, click **Add**, in the **User Name** field, type `FTNT\Administrator`, in the **Password** field, type `Password1!`, and then click **OK**.

DO NOT REPRINT
© FORTINET

12. On the **General** tab, in the **Match OS Versions** field, select **Windows Server 2019**, and then deselect **Windows 7**.
13. Select the **Domain Name** checkbox, and then type `ftnt.lab`.

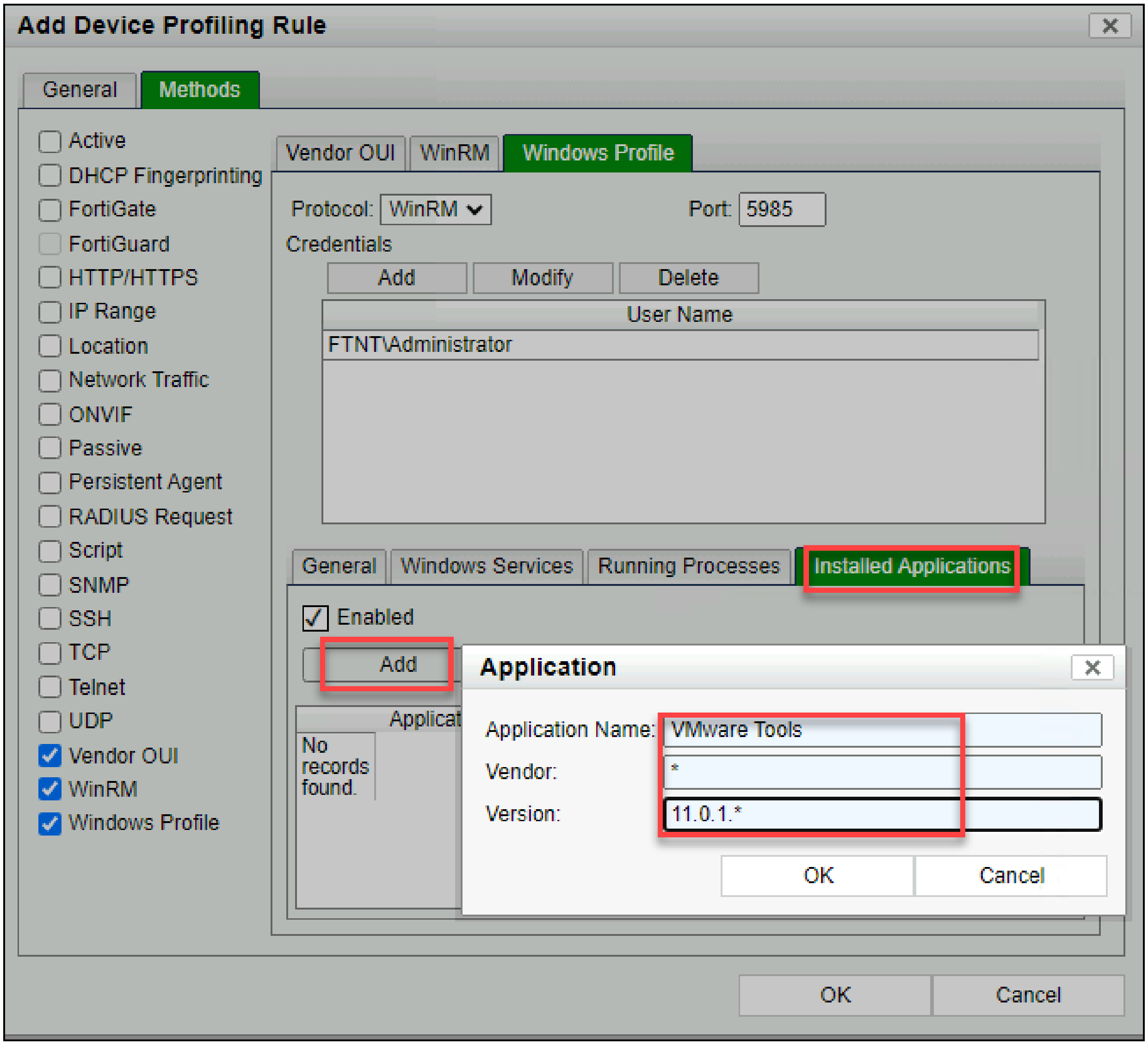


14. Click the **Windows Services** tab, and then clear the **Enabled** checkbox.
15. Click the **Running Processes** tab, in the **Process Name** section, click **Add**, type `vmtoolsd.exe`, and then click **OK**.
16. Click the **Installed Applications** tab, click **Add**, in the **Application** window, configure the following settings, and then click **OK**:

Field	Value
Application Name	VMware Tools
Vendor	*

DO NOT REPRINT
© FORTINET

Field	Value
Version	11.0.1.*

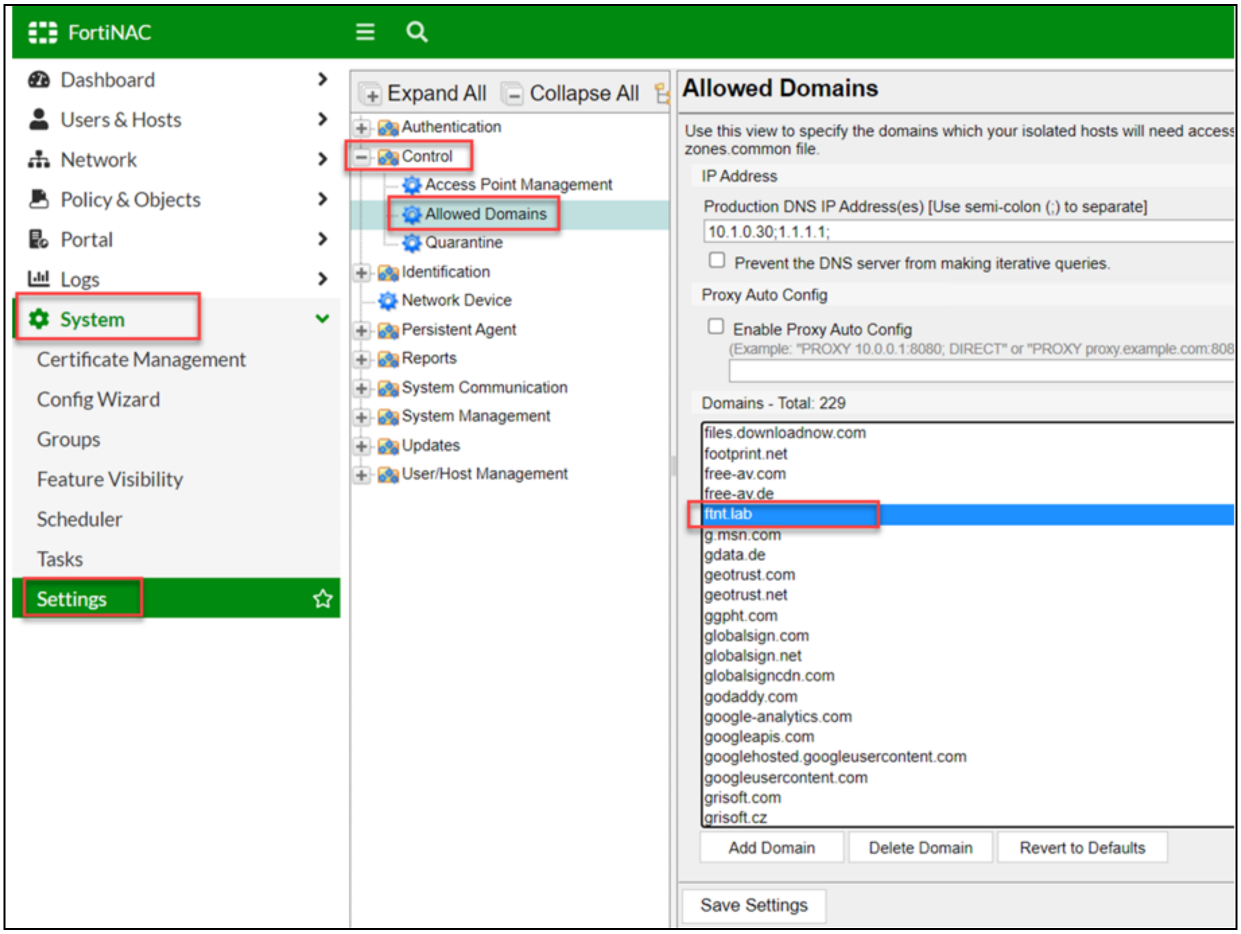


Values are not case-sensitive for Windows operating systems, but it is recommended to maintain the case.

17. Review some of the other profiling options available, and then click **OK**.
18. Select the **Domain Connected PCs** rule, click **Set Rank**, type `1` as the new rank, and then click **OK**.
19. Click **System** > **Settings**, expand **Control**, click **Allowed Domains**, and then ensure that the **ftnt.lab** internal domain is added.

DO NOT REPRINT
© FORTINET

If the **ftnt.lab** internal domain is not added, WinRM authentication will fail while the endpoint is in captive isolation networks.



Review FortiGate Policies for Captive Networks

You will review firewall policies on ISFW FortiGate to allow traffic between FortiNAC and captive networks.

To review firewall policies on ISFW FortiGate

1. On the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **ISFW** login page bookmark.
2. Log in to the ISFW GUI with the username `admin` and password `password`.
3. Click **Policy & Objects** > **Firewall Policy**, and then review the **Captive_Traffic** firewall policy.

   This policy allows traffic between FortiNAC and captive networks.

4. Review the **FortiNAC_To_Captive_Networks** firewall policy.

   This policy allows traffic from captive networks to FortiNAC.

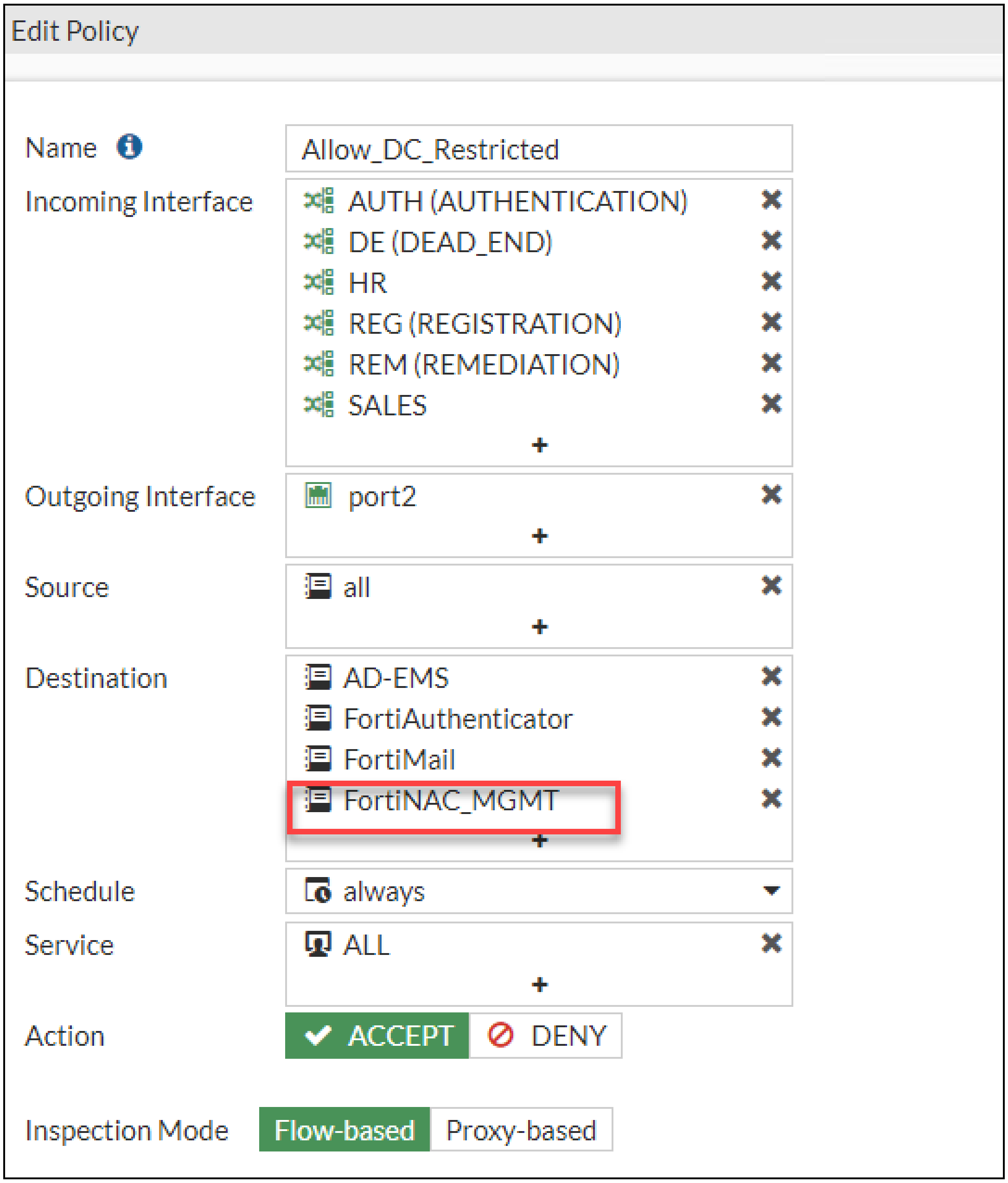
5. Review the **Allow_All_DC_To_ISFW_Segments** firewall policy.

   This policy allows traffic from data center subnets to captive networks.

6. Review the **Allow_DC_Restricted** firewall policy.

DO NOT REPRINT
© FORTINET

You will notice captive networks has been added to the source addresses and FortiNAC management is part of the destination addresses.



FortiNAC uses both the eth0 and eth1 interfaces for WinRM profiling. Allowing access to Active Directory from isolation networks is extremely important to validate the FortiNAC login while hosts are in isolation. You can lock down the access to specific ports, although we are allowing full access in our lab. FortiNAC management interface access is not required. It is being allowed DC access from ISFW subnets.

DO NOT REPRINT
© FORTINET

Test the Device Profiling Rule

You will test the device profiling rule you created earlier.

To test the device profiling rule

1. Restart the HR VM, and, log in with the username `hr\administrator` and password `Password1!`.

   Local windows user authentication is required to simulate a registered host state for a windows device on FortiNAC.

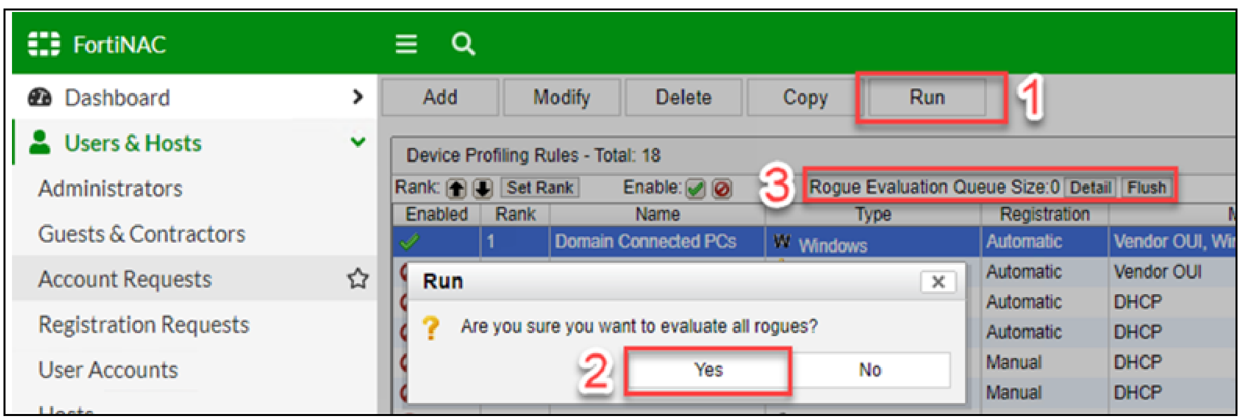
2. Return to the FortiNAC GUI, click **Users & Hosts** > **Adapters**, right-click the HR machine IP address **10.1.60.2**, and then select **Test Device Profiling Rule**.
3. Select **Domain Connected PCs**, and then click **OK**.

   FortiNAC communicates with the HR machine and gives you a result of **Rule Matches**. If you get a result of **Rule does not Match**, review your device profiling settings to ensure there are no configuration errors.

4. Click **OK**.
5. Repeat the test for the SALES VM, right-click the SALES machine IP address **10.1.50.2**, and then select **Test Device Profiling Rule**.
6. Select **Domain Connected PCs**, and then click **OK**.

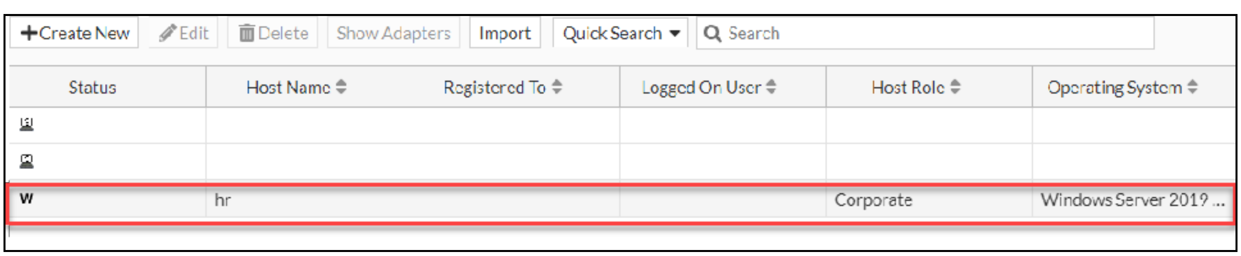
   FortiNAC communicates with the SALES machine and gives you a result of **Rule Does Not Match**. If you get a result of **Rule Matches**, review your device profiling settings to ensure there are no configuration errors.

7. Click **OK**.
8. Click **Users & Hosts** > **Device Profiling Rules**, and then click **Run** > **Yes** to begin evaluating all rogue devices.



   You can check details of rogue evaluation in the queue.

9. Click **OK**.
10. Click **Users & Hosts** > **Hosts**.



DO NOT REPRINT
© FORTINET

The **HR** device should now be registered and the **SALES** device still remains as a rogue device.

DO NOT REPRINT
© FORTINET

Exercise 3: Configuring Role-Based Access

In this exercise, you will create access policies for corporate, BYOD, and guest devices. You will also configure the self-registration portal. You will then test devices against each access policy.

Configure an Access Policy for Corporate Devices

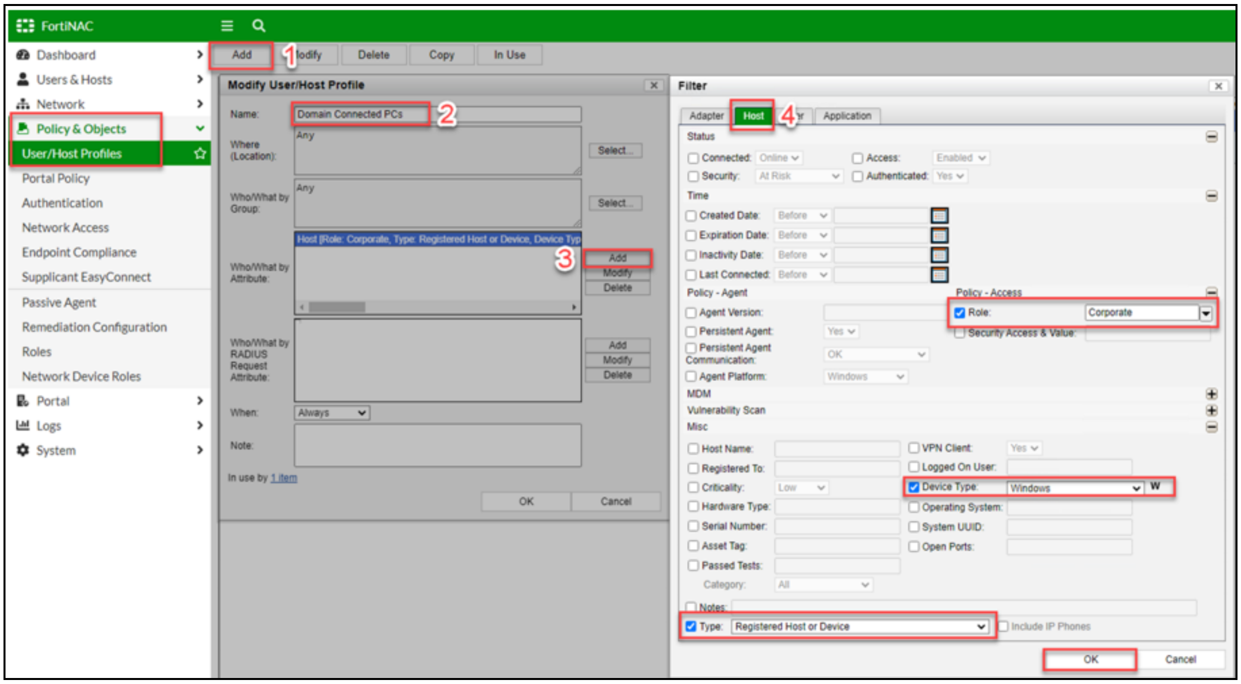
You will create an access policy for corporate devices.

To create an access policy for corporate devices

1. On the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **FortiNAC** login page bookmark.
2. Log in to the FortiNAC GUI with the username `admin` and password `Password1!`.
3. Click **Policy & Objects** > **User/Host Profiles**, and then click **Add** to create a new profile to identify corporate devices.
4. In the **Name** field, type `Domain Connected PCs`.
5. In the **Who/What by Attribute** field, click **Add**, click the **Host** tab, configure the following settings, and then click **OK**:

Host filter	Host filter values
Role	Select the checkbox, and then select **Corporate**.
Device Type	Select the checkbox, and then select **Windows**.
Type	Select the checkbox, and then select **Registered Host or Device**.

DO NOT REPRINT
© FORTINET



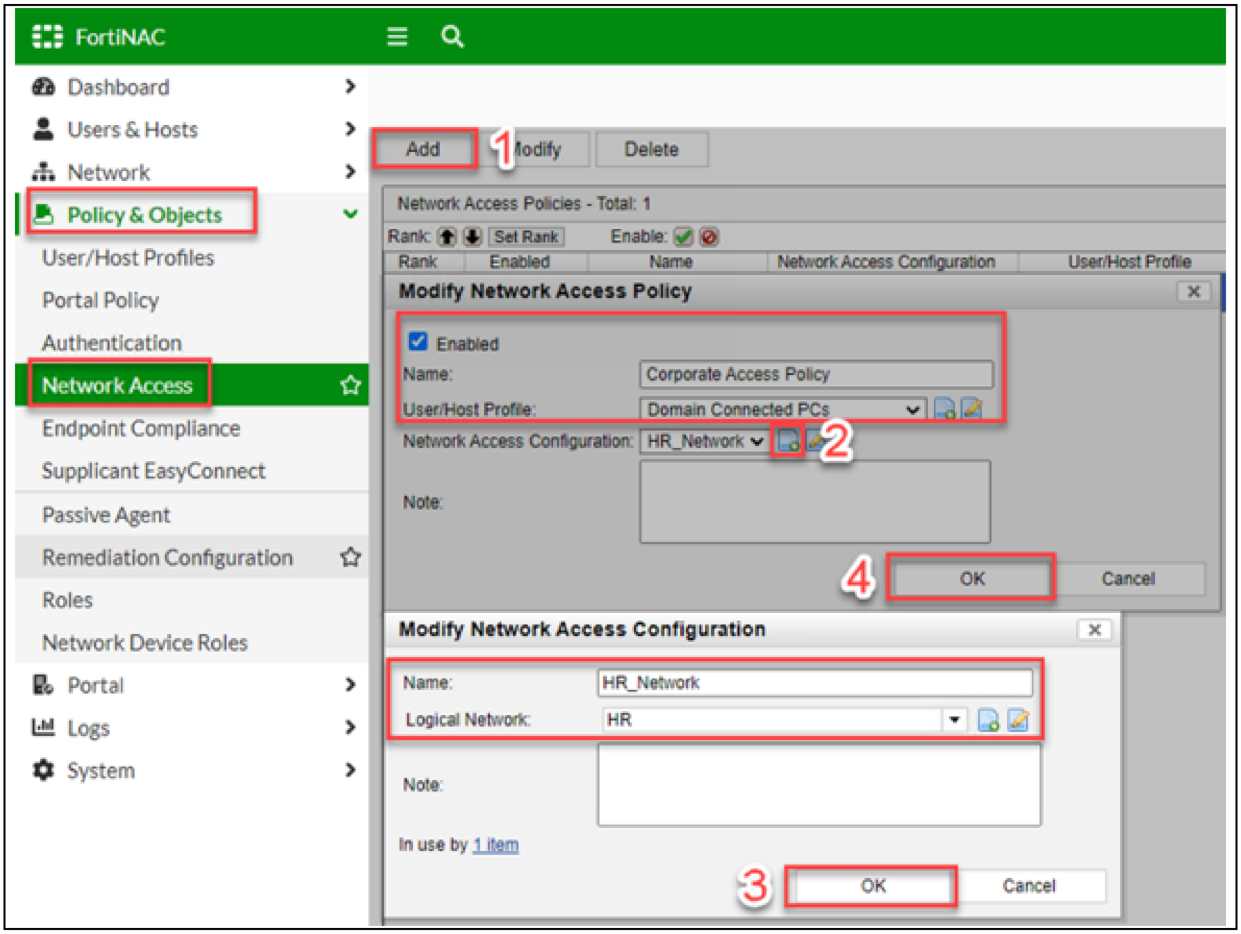
6. Click **OK**.
7. Click **Policy & Objects** > **Network Access**, click **Add**, and then configure the following settings to create a new network access policy:

Field	Value
Name	Corporate Access Policy
User/Host Profile	Domain Connected PCs

8. In the **Network Access Configuration** field, click the **Add** icon, configure the following settings, and then click **OK** to create a new network access configuration to allow access to the HR network:

Field	Value
Name	HR_Network
Logical Network	HR

DO NOT REPRINT
© FORTINET



9. Click **OK**.
10. Click **Policy & Objects** > **Authentication**, click **Add**, and then configure the following settings to create a new authentication policy:

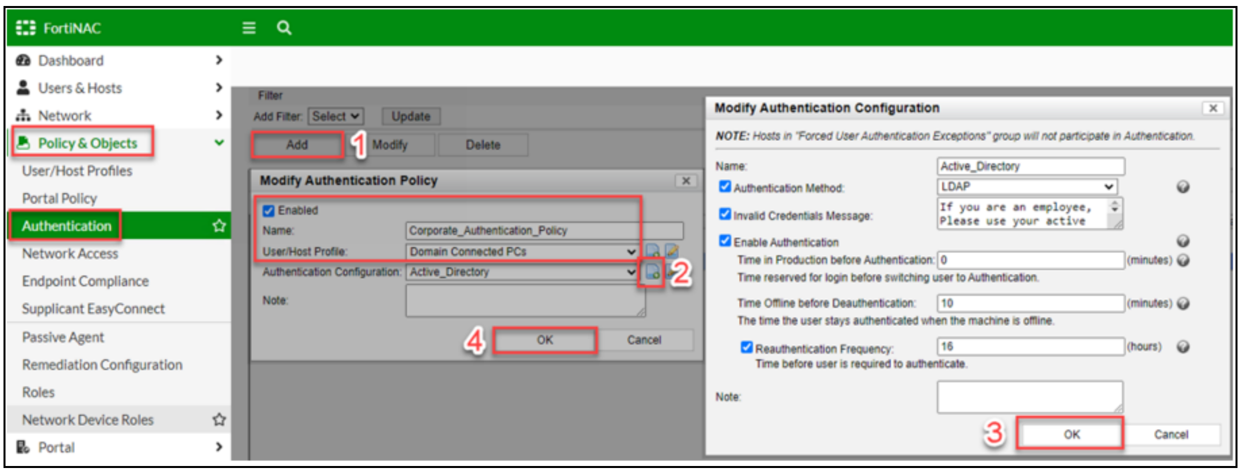
Field	Value
Enabled	Select the checkbox.
Name	Corporate_Authentication_Policy
User/Host Profile	Domain Connected PCs

11. In the **Authentication Configuration** field, click the **Add** icon, configure the following settings, and then click **OK** to create a new authentication configuration to authenticate corporate users:

Field	Value
Name	Active_Directory
Authentication Method	Select the checkbox, and then select **LDAP**.

DO NOT REPRINT
© FORTINET

Field	Value
Invalid Credentials Message	Select the checkbox, and then type `If you are an employee, please use your active directory credentials, or register as a guest user..`
Enable Authentication	Select the checkbox.
Time in Production before Authentication	0
Time Offline before Deauthentication	10
Reauthentication Frequency	Select the checkbox, and then type `16`.



12. Click **OK**.

Configure an Access Policy for BYOD Devices

You will create an access policy for BYOD devices.

To create an access policy for BYOD devices

1. Continuing on the FortiNAC GUI, click **Policy & Objects** > **Roles**, and then verify that the **BYOD** role is created.

If you do not see the BYOD role, click **Create New** to create a new role named `BYOD`, leave all other settings at the default values, and then click **OK**.

2. Click **Policy & Objects** > **User/Host Profiles**, and then click **Add** to create a new profile to identify BYOD devices.
3. In the **Name** field, type `BYOD Devices`.
4. In the **Who/What by Attribute** field, click **Add**, click the **Host** tab, configure the following settings, and then click **OK**:

DO NOT REPRINT
© FORTINET

Host filter	Host filter values
Role	Select the checkbox, and then select **BYOD**.
Device Type	Select the checkbox, and then select **Windows.**
Type	Select the checkbox, and then select **Registered Host or Device**.

5. Click **OK**.
6. Click **Policy & Objects** > **Network Access**, click **Add**, and then configure the following settings to create a new network access policy:

Field	Value
Name	BYOD Access Policy
User/Host Profile	BYOD Devices

7. In the **Network Access Configuration** field, click the **Add** icon, configure the following settings, and then click **OK** to create a new network access configuration to allow access to the BYOD network:

Field	Value
Name	BYOD_Network
Logical Network	BYOD

8. Click **OK**.
9. Click **Policy & Objects** > **Authentication**, click **Add**, and then configure the following settings to create a new authentication policy with the following values:

Field	Value
Enabled	Select the checkbox.
Name	BYOD_Authentication_Policy
User/Host Profile	BYOD Devices
Authentication Configuration	Active_Directory

10. Click **OK**.

Configure an Access Policy for Guest Devices

You will create an access policy for guest devices.

DO NOT REPRINT
© FORTINET

To create an access policy for guest devices

1. Continuing on the FortiNAC GUI, click **Policy & Objects** > **User/Host Profiles**, and then click **Add** to create a new profile to identify guest devices.
2. In the **Name** field, type `Self Registered Guest`.
3. In the **Who/What by Attribute** field, click **Add**, click the **Host** tab, configure the following settings, and then click **OK**:

Host filter	Host filter values
Role	Select the checkbox, and then select **GuestSelfRegistration**.
Device Type	Select the checkbox, and then select **Windows**.
Type	Select the checkbox, and then select **Registered Host or Device**.

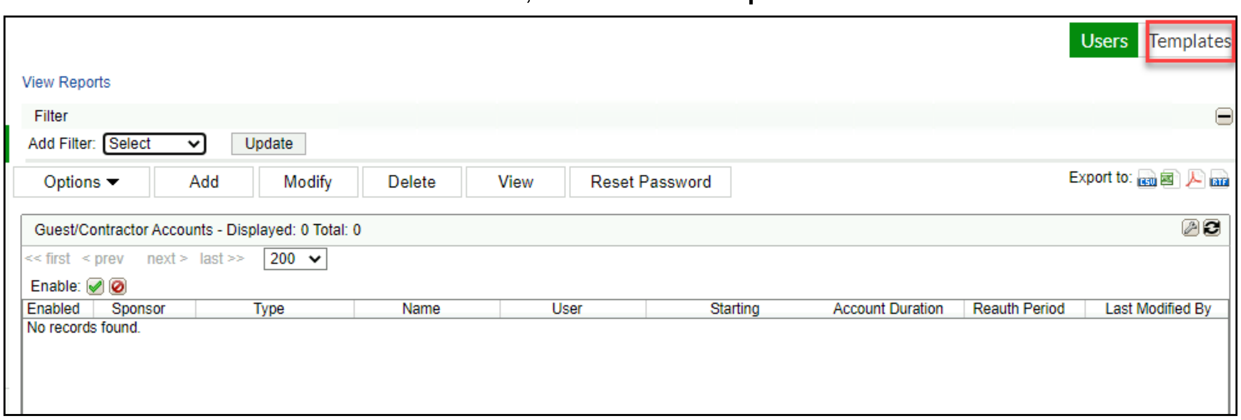
4. Click **OK**.
5. Click **Policy & Objects** > **Network Access**, click **Add**, and then configure the following settings to create a new network access policy:

Field	Value
Name	Guest Access Policy
User/Host Profile	Self Registered Guest

6. In the **Network Access Configuration** field, click the **Add** icon, configure the following settings, and then click **OK** to create a new network access configuration to allow access to the guest network:

Field	Value
Name	Guest_Network
Logical Network	GUEST

7. Click **OK**.
8. Click **Users & Hosts** > **Guests & Contractors**, and then click **Templates**.

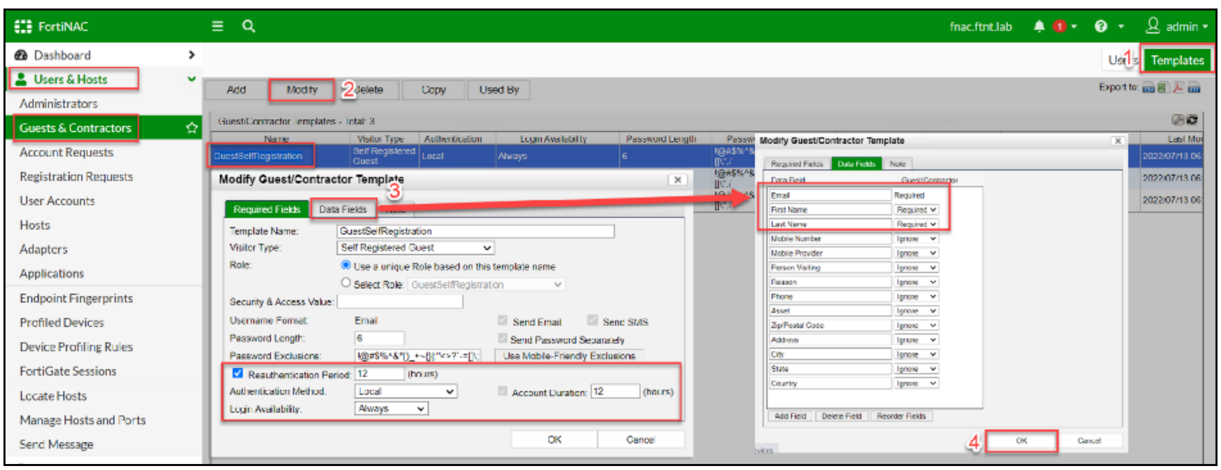


DO NOT REPRINT
© FORTINET

9. Select the **GuestSelfRegistration** template, click **Modify**, configure the following guest registration parameters, and then click **OK**:

Required Fields	Value
Template Name	GuestSelfRegistration
Visitor Type	Self Registered Guest
Password Length	6
Reauthentication Period	Select the checkbox, and then type `12`.
Account Duration	12

Data Fields	Value
Email	Required
First Name	Required
Last Name	Required
All other fields	Ignore



Configure the Self-Registration Portal

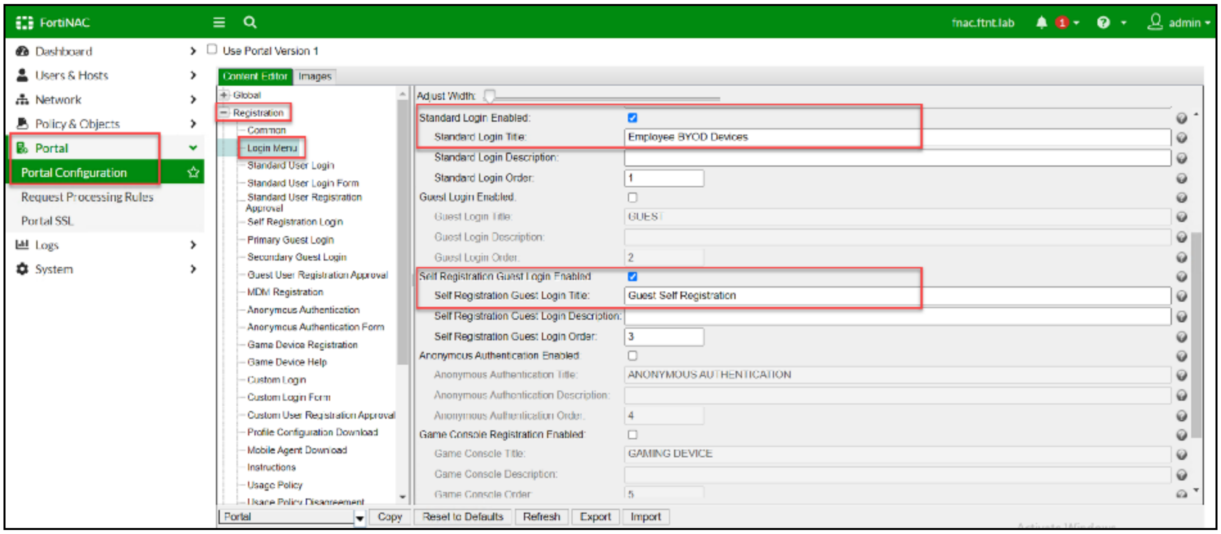
You will configure the FortiNAC self-registration portal.

To configure the self-registration portal

1. Continuing on the FortiNAC GUI, click **Portal** > **Portal Configuration**, expand **Global**, and then click **Settings**.
2. Ensure the **Standard User Login Type** field is set to **LDAP**, and then click **Apply**.

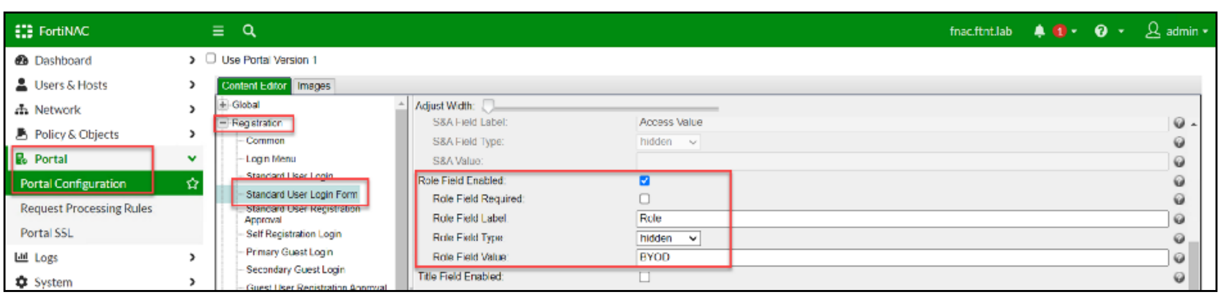
DO NOT REPRINT
© FORTINET

3. Expand **Registration**, click **Login Menu**, and then ensure that only the **Standard Login Enabled** and **Self Registration Guest Login Enabled** checkboxes are selected and the other registration checkboxes are cleared, as shown in the following image:



4. In the **Standard Login Title** field, change the value to `Employee BYOD Devices`.
5. Click **Apply**.
6. Expand **Registration**, click **Standard User Login Form**, scroll down, ensure the **Role Field Enabled** checkbox is selected, and then configure the following values:

Field	Value
Role Field Label	Role
Role Field Type	hidden
Role Field Value	BYOD



7. Expand **Registration**, click **Self Registration Login**, scroll down, and then review some of the default values to ensure that they match the following values:

Field	Value
Notify Sponsor of Guest Details	Clear the checkbox.

DO NOT REPRINT
© FORTINET

Field	Value
Required Sponsor Approval	None
Notify User via Portal Page	Select the checkbox.
Show Password in Portal Page Notification	Select the checkbox.
Notify User via Email	Clear the checkbox.
Notify User via SMS	Clear the checkbox.
Default Guest Template	GuestSelfRegistration

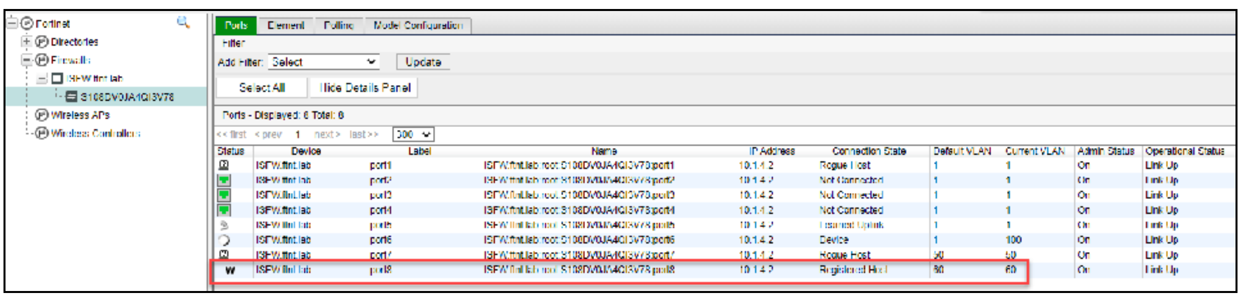
8. Click **Apply**.

Test Role-Based Access

You will test the different role-based access.

To test role-based access

1. Continuing on the FortiNAC GUI, click **Network** > **Inventory**, expand **Firewalls** > **ISFW.ftnt.lab**, and then click **S108DV0JA4QI3V78**.



You can see that the HR device is registered but not authenticated, while the SALES device is still showing as a rogue device.

Stop and Think!

Can you think why HR and SALES is given production corporate access even after you set up access and authentication policies to change their access?

Discussion

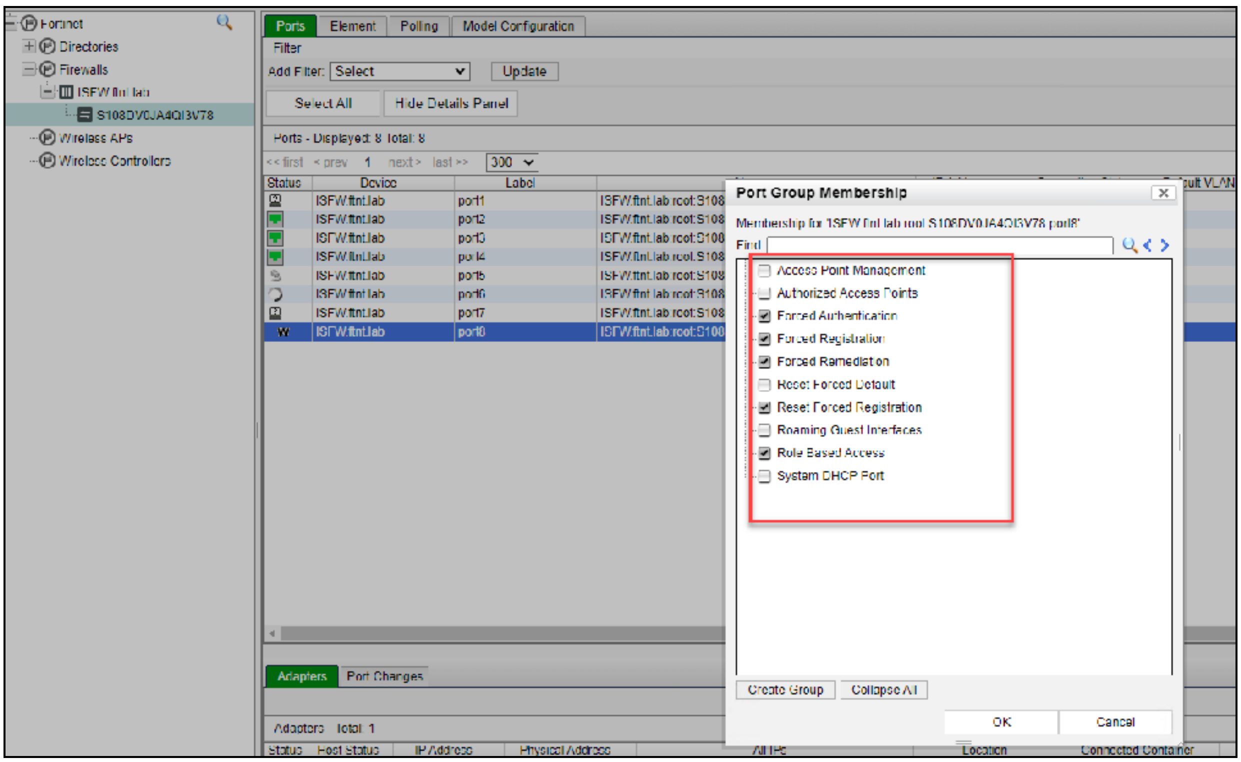
Is the policy enforced from configuration or do you need any additional configuration?

You must specify the ports where policy and authentication enforcement is required.

DO NOT REPRINT
© FORTINET

2. Right-click both **port7** and **port8**, click **Group Membership**, in the **Port Group Membership** window, select the checkboxes for the following groups, and then click **OK** to add the ports to the groups and enable enforcement on the ports:

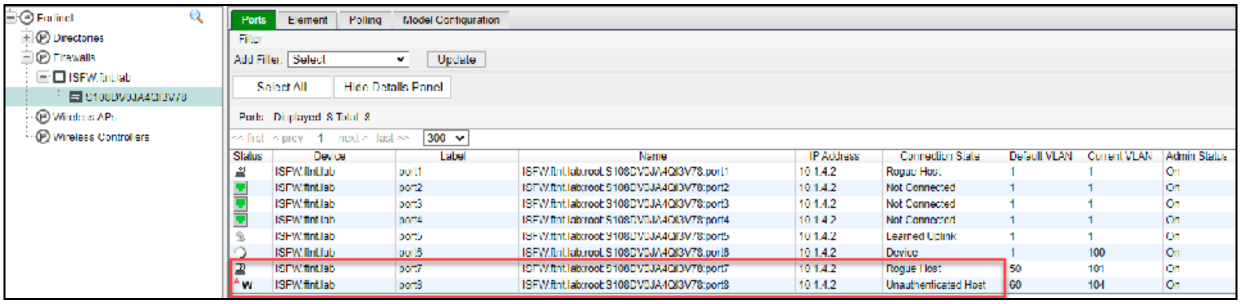
Group	Reason
Forced Authentication	Unauthenticated Hosts will be isolated until successful authentication
Forced Registration	Unregistered Rogue Hosts will be isolated until successful registration
Forced Remediation	Quarantined hosts are isolated until issues are remediated and passes scan
Reset Forced Registration	Ports return to Registration VLAN when hosts disconnect
Role Based Access	Access is provided to registered hosts based on Role and Network access policies



3. Refresh the page for 1–2 minutes to allow FortiNAC to start changing VLANs based on the state of the endpoints, as shown in the following image.

   You will notice that the HR machine is placed in the Authentication VLAN (104), because it is registered but not authenticated, and the SALES machine is placed in the Registration VLAN (101), because it is still a rogue device.

DO NOT REPRINT
© FORTINET



If the VLANs are not changed automatically within 2–3 minutes, right-click **ISFW.ftnt.lab**, and then click **Poll for L2 (Hosts) Info**.

4. On the HR VM, open a command prompt, and then enter the `ipconfig` command to check if the IP address has changed.

In the lab environment, we are using the FortiSwitch VM, which is not directly connected to the SALES or HR VMs. Therefore, when a VLAN change happens, the port up/down on FortiGate does not trigger a port up/down on the VM. As a workaround, we have configured a 1 minute DHCP lease on all production subnets to speed up IP changes. If it does not change automatically, you can run `ipconfig /release` and `ipconfig /renew` as Administrator on the VM to trigger the change immediately.

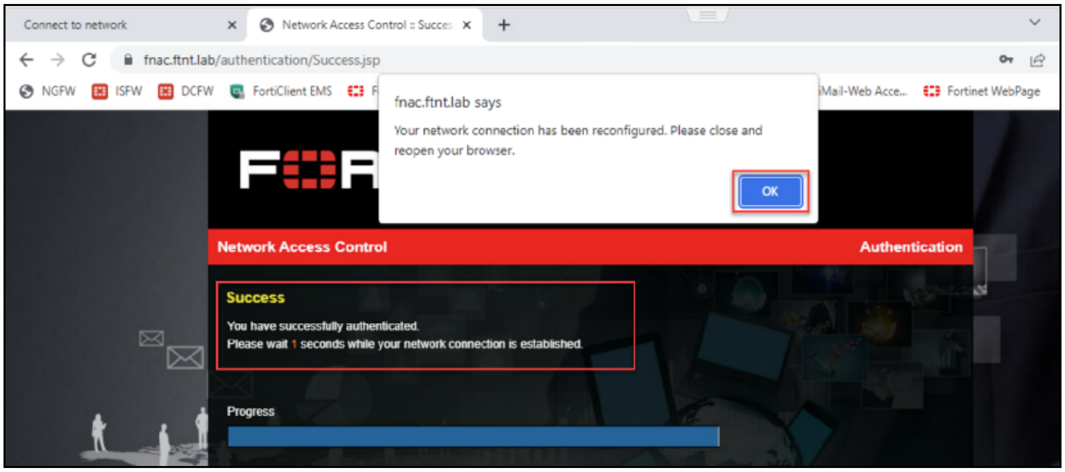
5. Open Google Chrome, and then navigate to `https://www.fortinet.com`.

   This should trigger a redirect to the Fortinet authentication page.

6. Click **USER**, log in with the username `hr` and password `Password1!`, and then click **Continue**.

   You should see a success message with a countdown, as well as a pop-up message, as shown in the following image:

DO NOT REPRINT
© FORTINET



7. Click **OK**, and then close the browser.
8. Open a command prompt, and then enter `ipconfig`.

   You should see an IP address of **10.1.60.2** from the HR subnet range.

9. Reopen Google Chrome, and then navigate to `https://www.fortinet.com`.

   You should now have access.

10. Navigate to the FortiAuthenticator URL at `https://fac.ftnt.lab` to access corporate resources.

    You should have access.

11. Repeat the steps for EMS and FortiMail.
12. Access the FortiAnalyzer URL at `https://faz.ftnt.lab`.

    You should not have access. Access was removed in an earlier lab from the HR subnet.

13. On the Sales VM, open a command prompt, and then enter the `ipconfig` command to check if the IP address has changed.

In the lab environment, we are using a FortiSwitch VM, which is not directly connected to the SALES or HR VMs. Therefore, when a VLAN change happens, the port up/down on FortiGate does not trigger a port up/down on the VM. As a workaround, we have configured a 1 minute DHCP lease on all production subnets to speed up IP changes. If it does not change automatically, you can run `ipconfig /release` and `ipconfig /renew` as Administrator on the VM to trigger the change immediately.

14. Open Google Chrome, and then navigate to `https://www.fortinet.com`.

    This should trigger a redirect to the Fortinet registration page.

DO NOT REPRINT
© FORTINET

15. Click **Employee BYOD Devices**, log in with the username `sales` and password `Password1!`, and then click **Continue**.

    You should see a success message with a countdown and you should be redirected to https://www.fortinet.com.

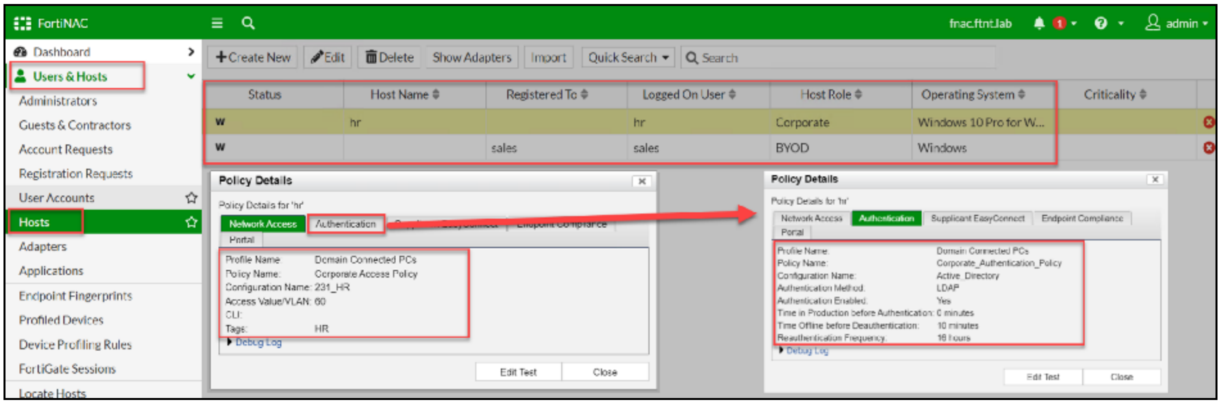
16. Open a command prompt, and then enter `ipconfig`.

    You should see an IP address of **10.1.199.2** from the UNTRUST subnet range.

17. Return to the FortiNAC GUI, and then click **Users & Hosts** > **Hosts**.

    You should now see that the **HR** device is enriched with user information.

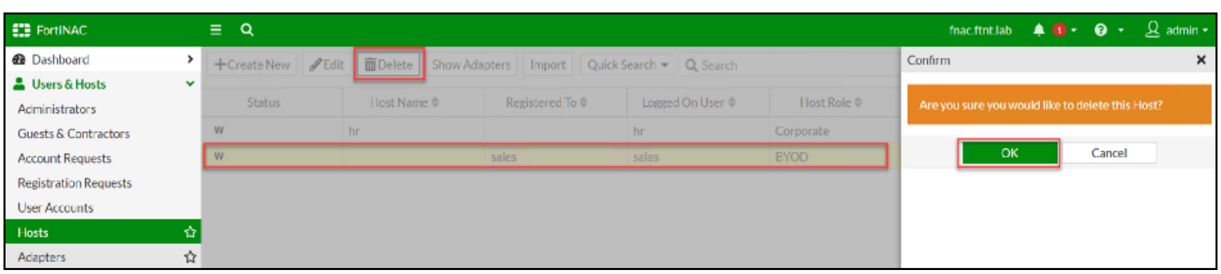
18. Right-click the host, and then select **Policy Details** to view the matched network access policy and the reason.



19. Click the **Authentication** tab to view the authentication method and the policy matched, and then click **Close**.

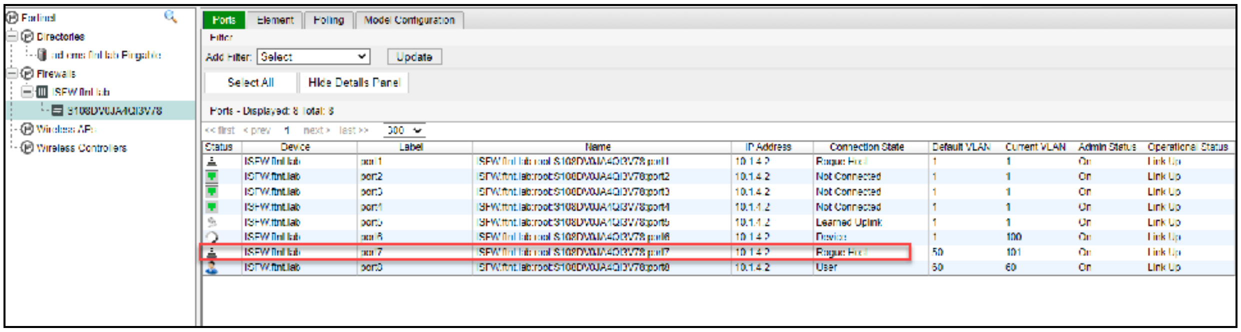
> **Stop and Think!**
>
> Why do you see the SALES machine registered to the **sales** user with a **BYOD** policy, but the HR machine is only showing **Logged On User**?
>
> **Discussion**
>
> How can you modify this behavior?
>
> Think about how you are registering the HR device and explore the options there.

20. Click the **SALES** host, click **Delete**, and then click **OK**.



21. Click **Network** > **Inventory**, expand **Firewall** > **ISFW.ftnt.lab**, and then click **S108DV0JA4QI3V78**.

DO NOT REPRINT
© FORTINET



You can see the HR device is registered and authenticated, while the SALES device is now a rogue device again.

If VLANs are not changed automatically within 2–3 minutes, right-click **ISFW.ftnt.lab**, and then click **Poll for L2 (Hosts) Info**.

22. On the Sales VM, open a command prompt, and then enter the `ipconfig` command to check if the IP address has changed.

In the lab environment, we are using the FortiSwitch VM, which is not directly connected to the SALES or HR VMs. Therefore, when a VLAN change happens, the port up/down on FortiGate does not trigger a port up/down on the VM. As a workaround, we have configured a 1 minute DHCP lease on all production subnets to speed up IP changes. If it does not change automatically, you can run `ipconfig /release` and `ipconfig /renew` as Administrator on the VM to trigger the change immediately.

23. Open Google Chrome, and then navigate to `https://www.fortinet.com`.

This should trigger a redirect to the Fortinet registration page.

24. Click **GUEST SELF REGISTRATION**, register for a guest account with the following settings, and then click **Request Access**:

Field	Value
Sponsor Email	admin@ftnt.lab

DO NOT REPRINT
© FORTINET

Field	Value
Email	<Enter your email.>
First Name	<Enter your first name.>
Last Name	<Enter your last name.>

It should register your account and autofill the username and password for your account. You can make a note of it, if needed. You can always register a new guest account.

25. Click **Login**.

    You should see a success message with a countdown and you should be redirected to https://www.fortinet.com.

26. Access corporate resources next by navigating to the FortiAuthenticator URL at `https://fac.ftnt.lab`.

    You should not have access.

27. Repeat the steps for EMS and FortiMail.
28. Open a command prompt, and then enter `ipconfig`.

    You should see an IP address of **10.1.199.2** from the UNTRUST subnet range.

29. Return to the FortiNAC GUI, click **Users & Hosts** > **Hosts**.

    You should now see the **Sales** device with the self-registered guest account information.

30. Right-click the host, and then select **Policy Details** to view the matched network access policy and reason.

DO NOT REPRINT
© FORTINET

Lab 4: Application Security Using ZTNA

In this lab, you will learn about the use of a zero trust network access (ZTNA) proxy for remote access to specific applications. You will configure the required ZTNA components. You will also review key ZTNA concepts.

Objectives

- Verify connectivity between FortiGate, FortiClient, and FortiClient EMS
- Configure on-fabric detection rules
- Enable ZTNA on FortiGate
- Configure EMS ZTNA tagging rules
- Configure a basic HTTPS access proxy with SSL certificate-based authentication
- Configure an HTTPS access proxy with basic local user authentication and ZTNA tags
- Configure a TCP forwarding access proxy for RDP and SSH
- Configure basic ZTNA IP/MAC filtering

Time to Complete

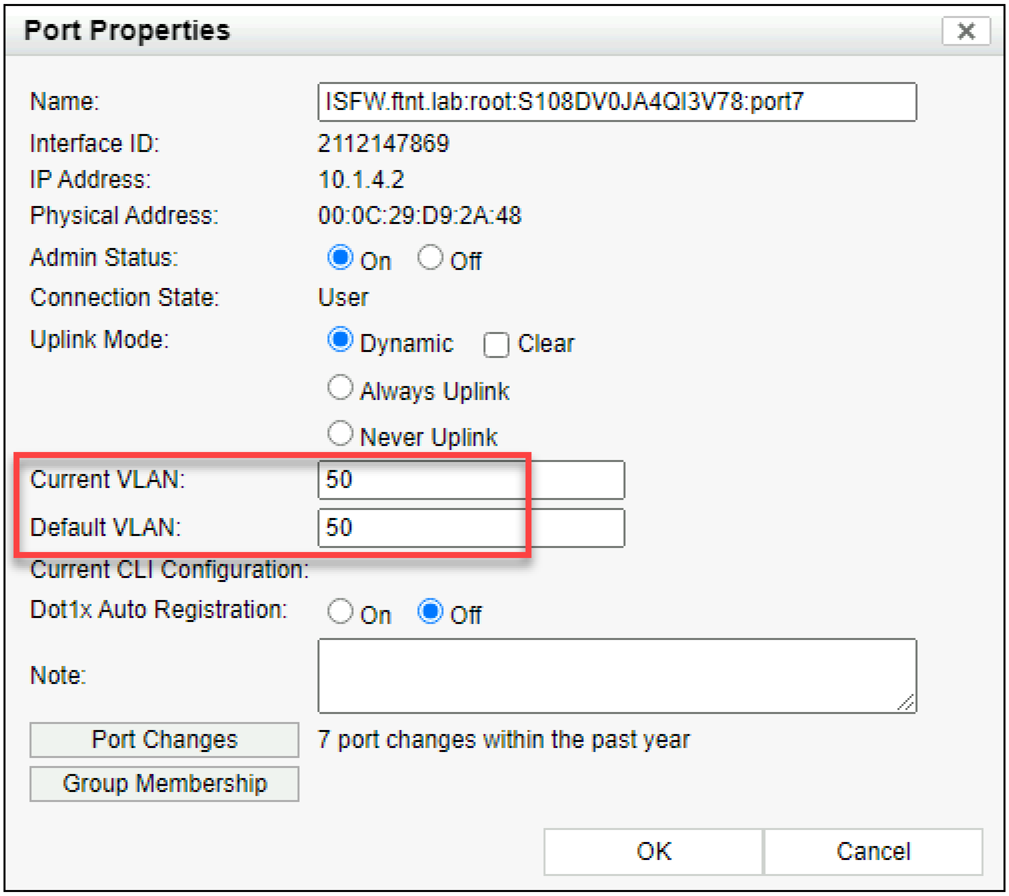
Estimated: 90 minutes

Prerequisites

Before you begin this lab, you must change the VLAN of the HR VM to VLAN 60 and the Sales VM to VLAN 50. You will also remove port enforcement for SALES VM.

1. Restart the HR VM, and, log in with the username `ftnt\hr` and password `Password1!`.
2. On the FortiNAC GUI, click **Network** > **Inventory**, expand **Firewalls** > **ISFW.ftnt.lab**, and then click **S108DV0JA4QI3V78**.
3. Right-click **port7**, and then click **Port Properties**.
4. In the **Current VLAN** field, change the value to `50`.

DO NOT REPRINT
© FORTINET



5. Click **Group Membership**.
6. In the **Port Group Membership** window, clear all the checkboxes.
7. Click **OK**.
8. Click **OK**.
9. Right-click **port8**, and then click **Port Properties**.
10. In the **Current VLAN** field, change the value to `60`.
11. Click **OK**.

DO NOT REPRINT
© FORTINET

Exercise 1: Configuring On-Fabric Rules on FortiClient EMS

In this exercise, you will verify the connection between FortiClient, FortiClient EMS, and FortiGate. You will also configure on-fabric rules on FortiClient EMS to determine the fabric status of the endpoint.

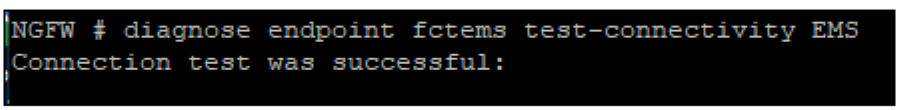
Verify the Connection Between FortiClient, FortiClient EMS, and FortiGate

You will verify that all of the devices have a stable connection, in order to exchange information required for on-fabric rules and ZTNA tagging to work properly.

To verify the connection between FortiGate and FortiClient EMS

1. On the FortiClient EMS VM, open PuTTY, and then connect over SSH to the **NGFW** saved session.
2. Log in with the username `admin` and password `password`.
3. Enter the following command to verify the status:

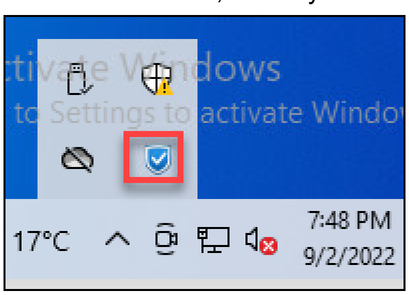
   `diagnose endpoint fctems test-connectivity EMS`

4. Repeat steps 1–3 on DCFW FortiGate and ISFW FortiGate to verify connectivity to the EMS server.

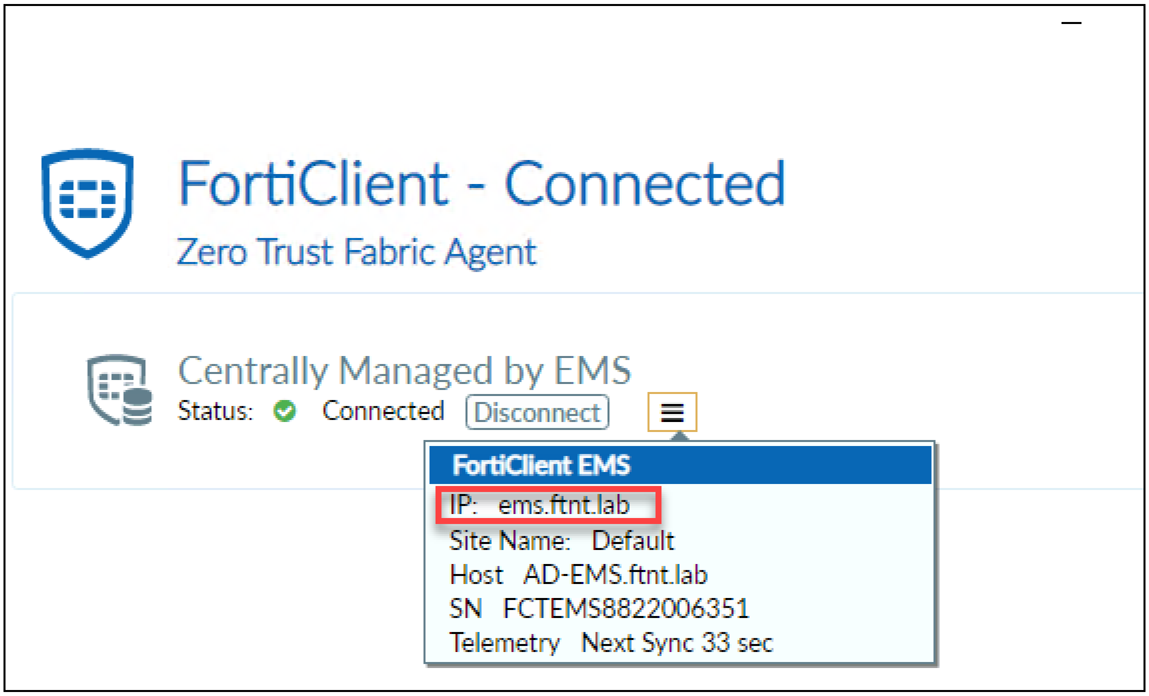
To verify the connection between FortiClient EMS and FortiClient

1. On the Remote VM, in the system tray, double-click the FortiClient icon.

2. In the **ZERO TRUST TELEMETRY** section, ensure the status of **Centrally Managed by EMS** is **Connected**. The IP address of the FortiClient EMS should be **ems.ftnt.lab**.

DO NOT REPRINT
© FORTINET



In this exercise, NGFW FortiGate is configured with a VIP and firewall policy that allows inbound connections so that the Remote-VM endpoint can connect to FortiClient EMS telemetry.

3. Open a command prompt, enter the `ipconfig` command, and then make a note of your default gateway.
4. Repeat steps 1-3 on the Sales VM and HR VM.

If the status of the **Centrally Managed by EMS** is **Not reachable**, you must reconnect the endpoint.

Remote VM:

1. In the **ZERO TRUST TELEMETRY** section, click **Disconnect**.
2. In the **Enter Server address or Invitation code** field, type `10.1.3.206` or `ems.ftnt.lab`, and then click **Connect** to reconnect the Remote VM to FortiClient EMS.
3. In the **Invalid certificate detected** window, click **Accept**.

Sales VM and HR VM:

1. In the **ZERO TRUST TELEMETRY** section, click **Disconnect**.
2. In the **Enter Server address or Invitation code** field, type `10.1.0.30` or `ems.ftnt.lab`, and then click **Connect** to reconnect the Sales VM and HR VM to FortiClient EMS.
3. In the **Invalid certificate detected** window, click **Accept**.

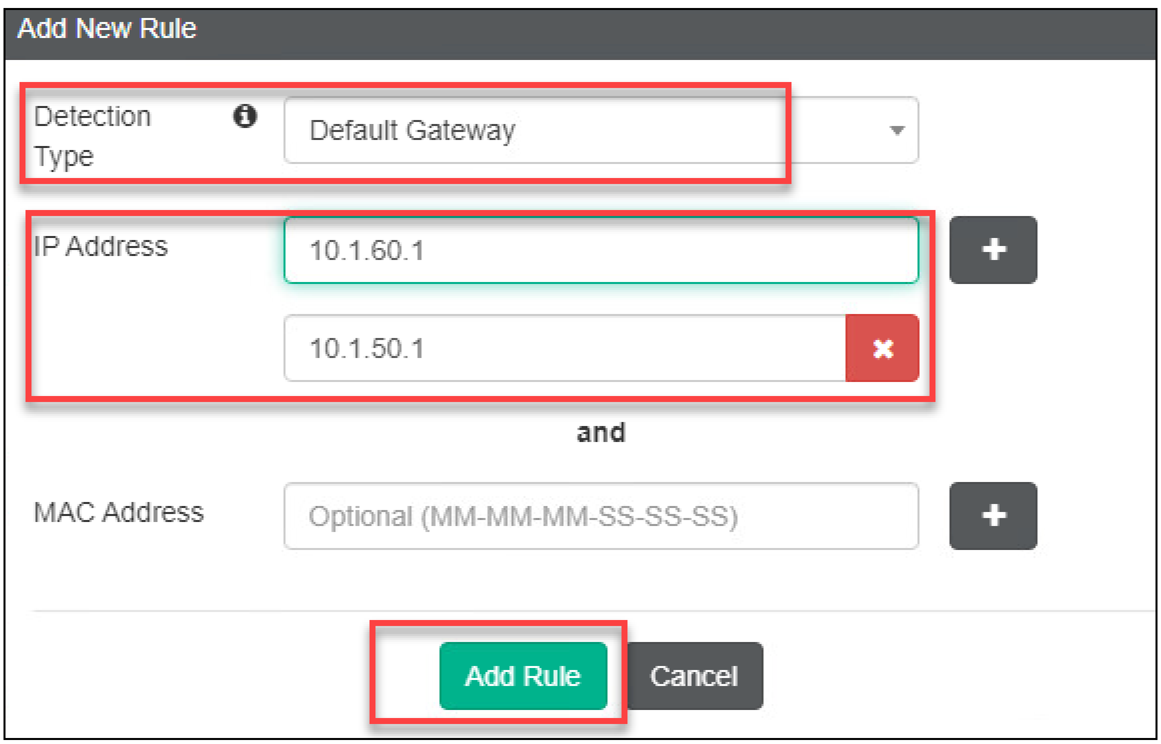
DO NOT REPRINT
© FORTINET

Configure On-Fabric Detection Rules

FortiClient EMS uses on-fabric detection rules to determine if a registered FortiClient endpoint is on-fabric or off-fabric. You will configure on-fabric detection rules.

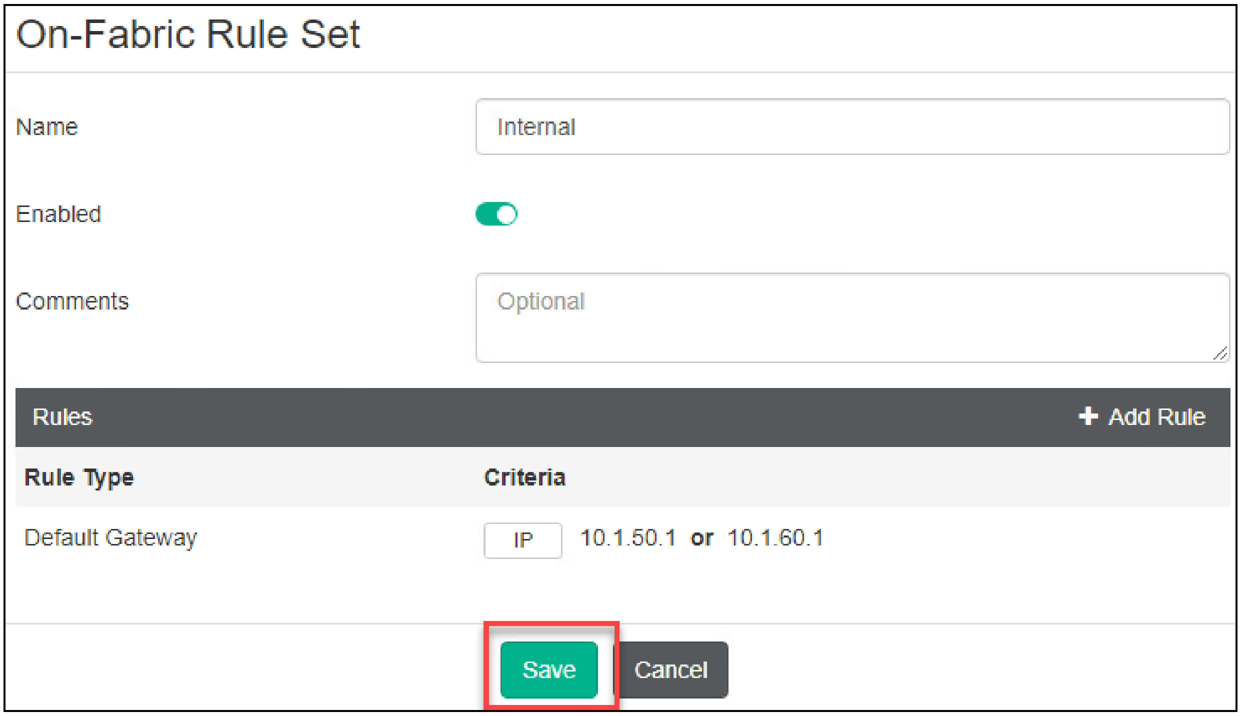
To configure on-fabric detection rules

1. On the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **FortiClient EMS** login page bookmark.
2. Log in with the username `admin` and password `Password1!`.
3. In the left menu, click **Endpoint Policy & Components** > **On-fabric Detection Rules**.
4. In the upper-right corner, click **Add**.
5. In the **Name** field, type `Internal`.
6. In the **Rules** section, click **Add Rule**.
7. In the **Detection Type** field, select **Default Gateway**.
8. In the **IP Address** field, type `10.1.50.1`.
9. Click + to add another IP address.
10. In the **IP Address** field, type `10.1.60.1`.
11. Click **Add Rule**.



12. Click **Save**.

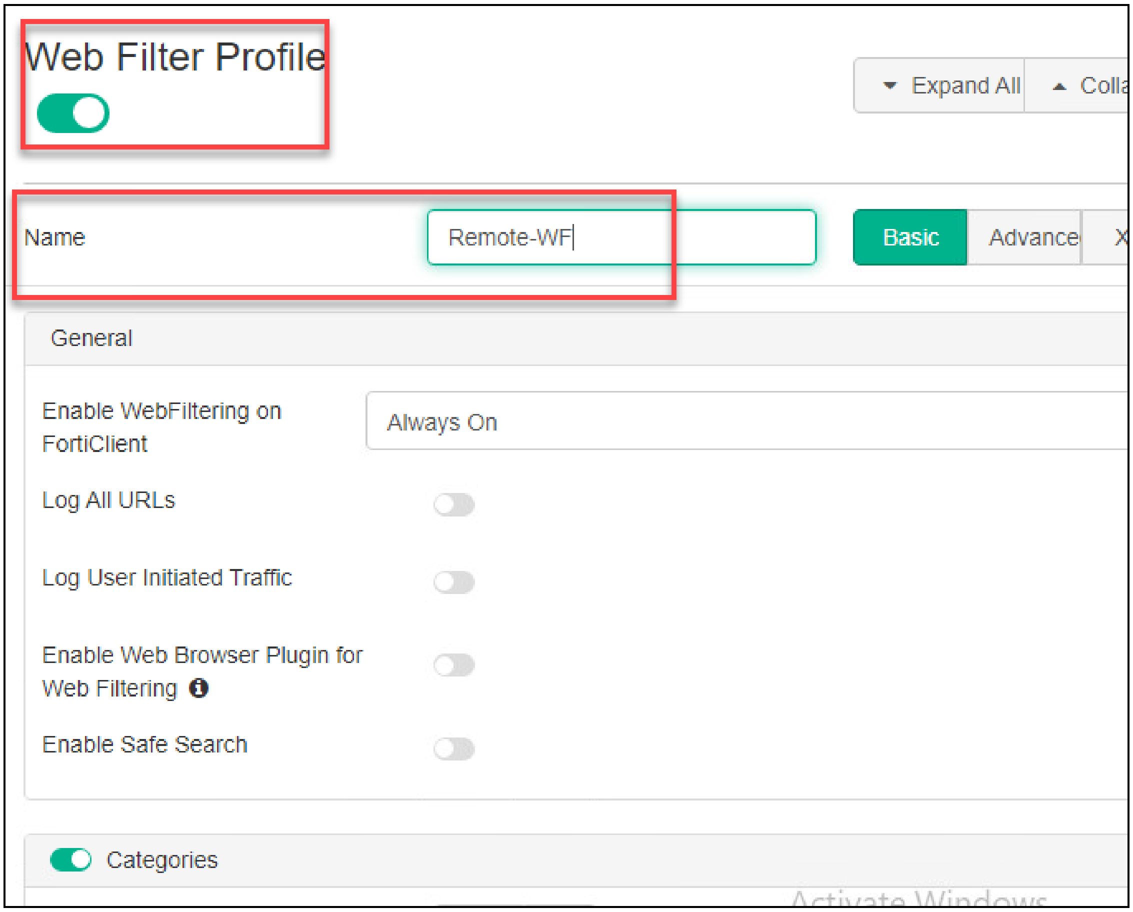
DO NOT REPRINT
© FORTINET



The default gateways specified in the on-fabric rules are IP addresses of VLANs configured on ISFW FortiGate in Lab 1. The Sales VM and HR VM use these gateways.

13. Click **Endpoint Profiles** > **Web Filter**.
14. In the upper-right corner, click **Add**.
15. In the **Name** field, type `Remote-WF`.
16. Enable **Web Filter Profile**.

DO NOT REPRINT
© FORTINET

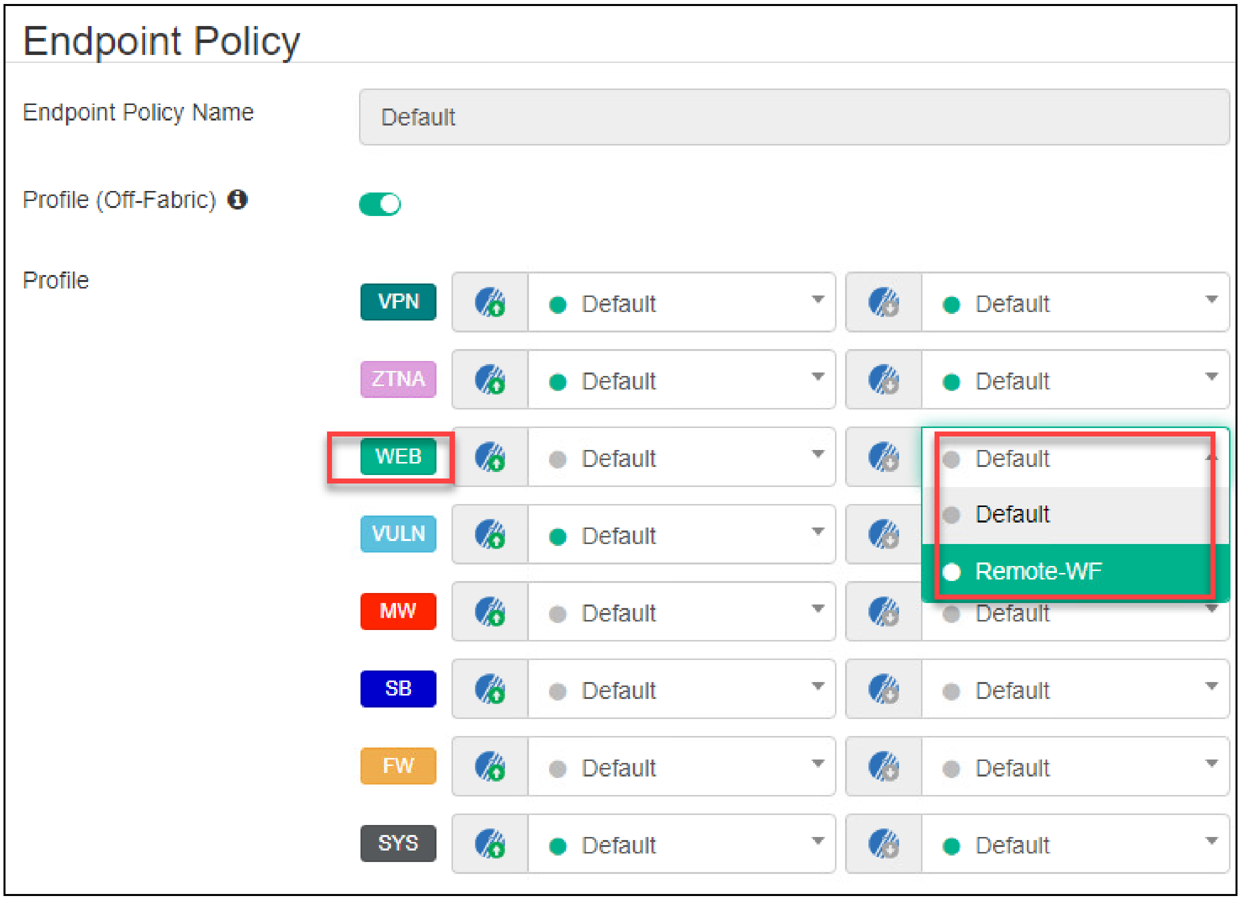


17. Click **Save**.
18. Click **Endpoint Policy & Components** > **Manage Policies**.
19. Select **Default** policy, and then click **Edit**.
20. Enable **Profile (Off-Fabric)**.

    You can see two profile columns. The one on the right is the **Off-Fabric** profile.

21. In the **Off-Fabric** profile, in the **WEB** field, select **Remote-WF**.

DO NOT REPRINT
© FORTINET



22. In the **On-Fabric Detection Rules** field, select **Internal**.
23. Click **Save**.

In this exercise, all endpoints registered to FortiClient EMS use the **Default** profile. When an endpoint matches the conditions specified in the on-fabric rule, it is classified as **On-Fabric**. Different endpoint profiles can be assigned based on the fabric status.

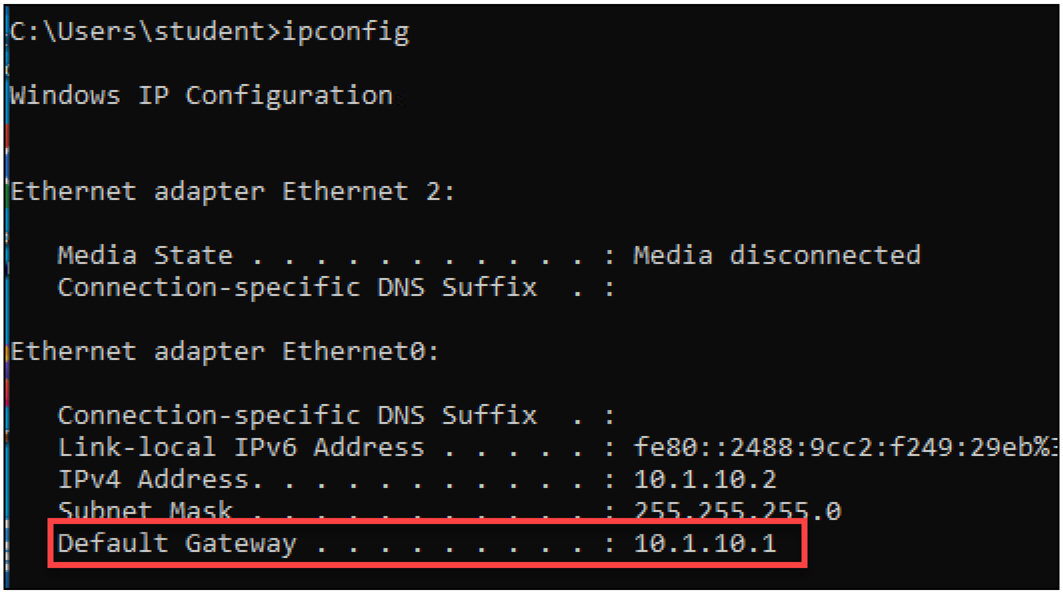
Verify On-Fabric Detection Rules

You will verify the on-fabric detection rules.

To verify on-fabric detection rules

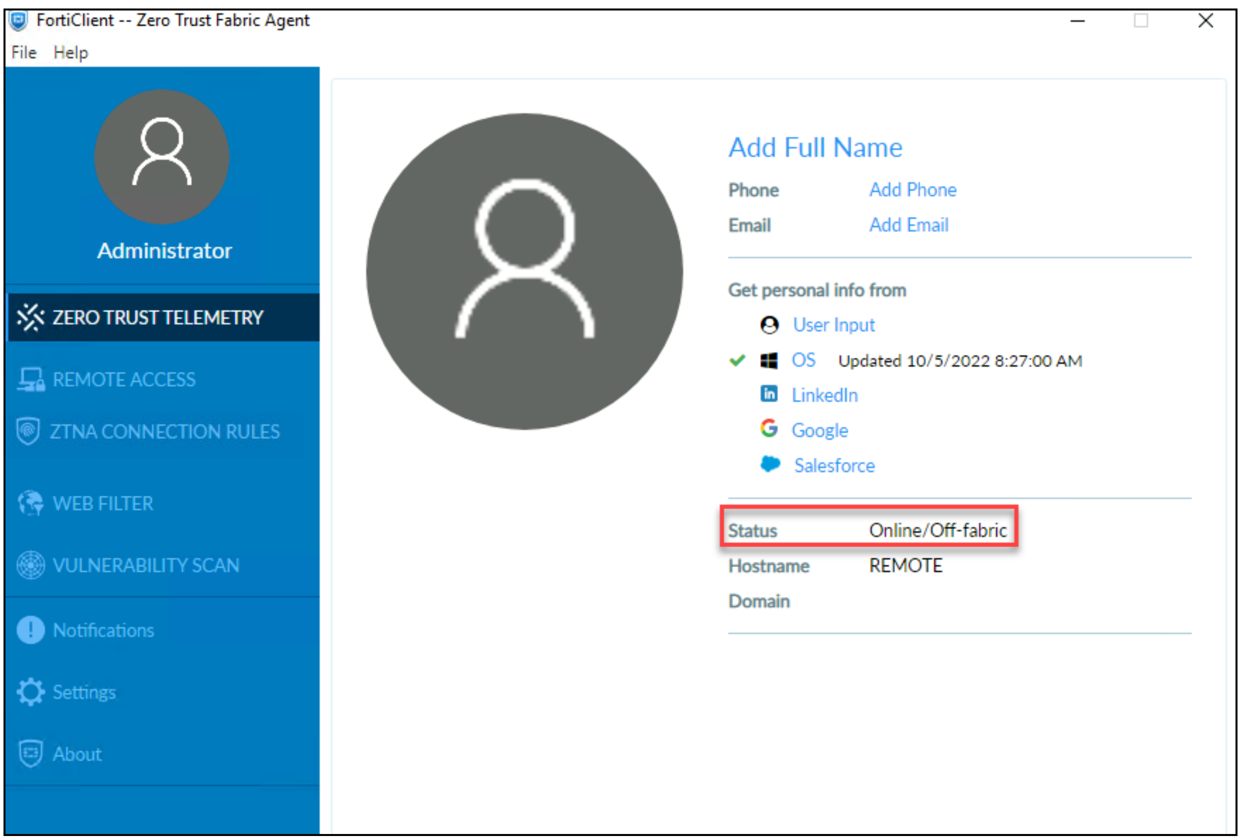
1. On the Remote VM, open a command prompt, enter the `ipconfig` command, and then make a note of your default gateway.

DO NOT REPRINT
© FORTINET



2. In the system tray, double-click the FortiClient icon.
3. Click the user avatar.

   The fabric status is **Off-fabric** and a web filter profile is also available.



DO NOT REPRINT
© FORTINET

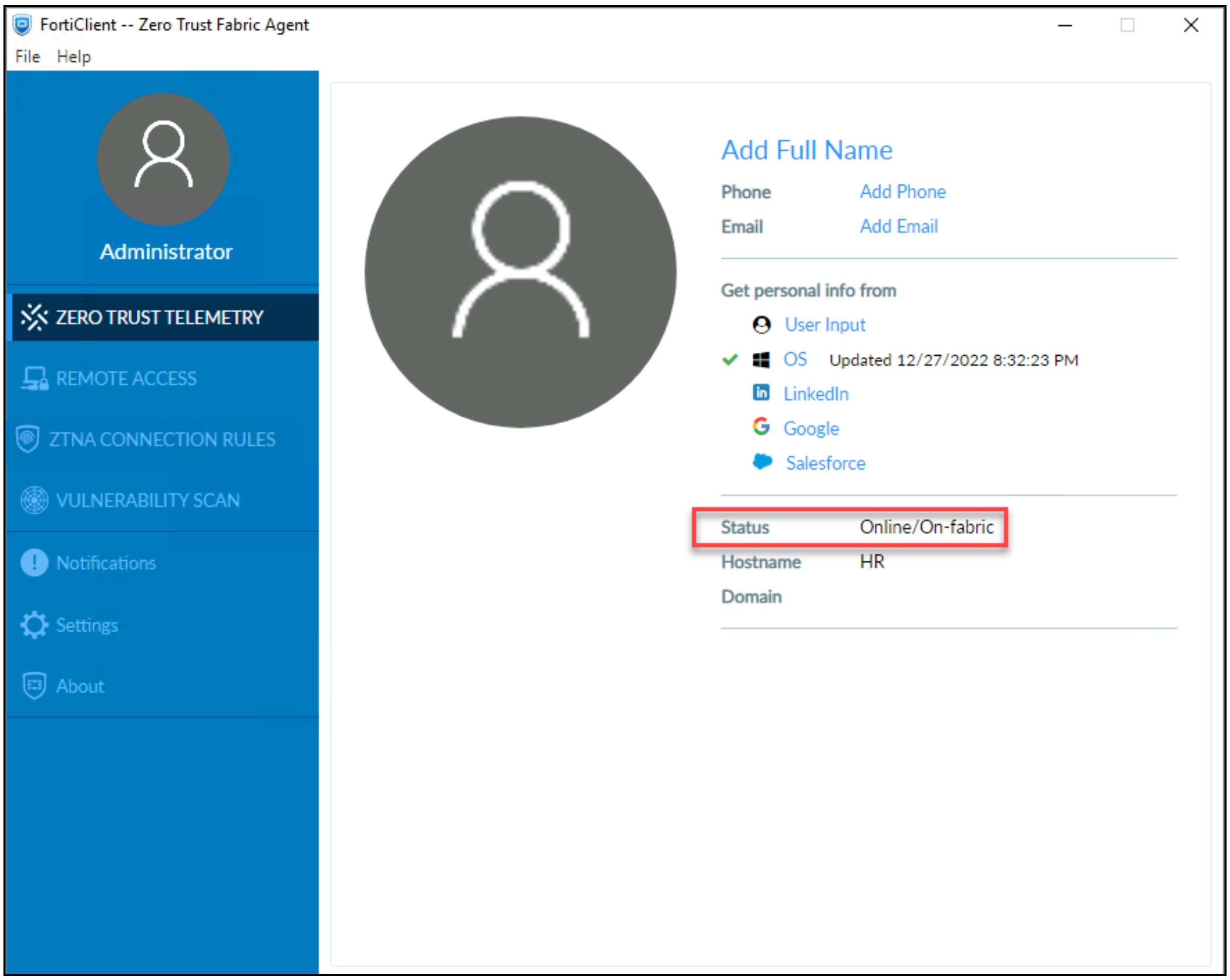
The default gateway on the Remote VM does not the match the IP addresses specified in the on-fabric rule. The endpoint was classified as off-fabric and the endpoint profile assigned has web filtering as part of it.

4. On the HR VM, open a command prompt, enter the `ipconfig` command, and then make a note of your default gateway.

   The gateway is **10.1.60.1** and matches the on-fabric rules previously configured.

5. In the system tray, double-click the FortiClient icon.
6. Click the user avatar.

   The fabric status is **On-fabric** and a web filter profile is not available.



The off-fabric and on-fabric endpoints have different endpoint profiles assigned based on their fabric status.

DO NOT REPRINT
© FORTINET

7. Return to the FortlClient EMS GUI, click **Endpoint Policy & Components** > **Manage Policies**.
8. Select **Default** policy, and then click **Edit**.
9. In the off-fabric profile, in the **WEB** field, select **Default**.
10. Click **Save**.

DO NOT REPRINT
© FORTINET

Exercise 2: Configuring ZTNA Tags, Tagging Rules, and Features

In this exercise, you will configure ZTNA tags and tagging rules, and then verify if the tags are synced on FortiClient and FortiGate. These tags will be used in the next exercises to authorize user traffic based on ZTNA tagging rules configured on FortiClient EMS.

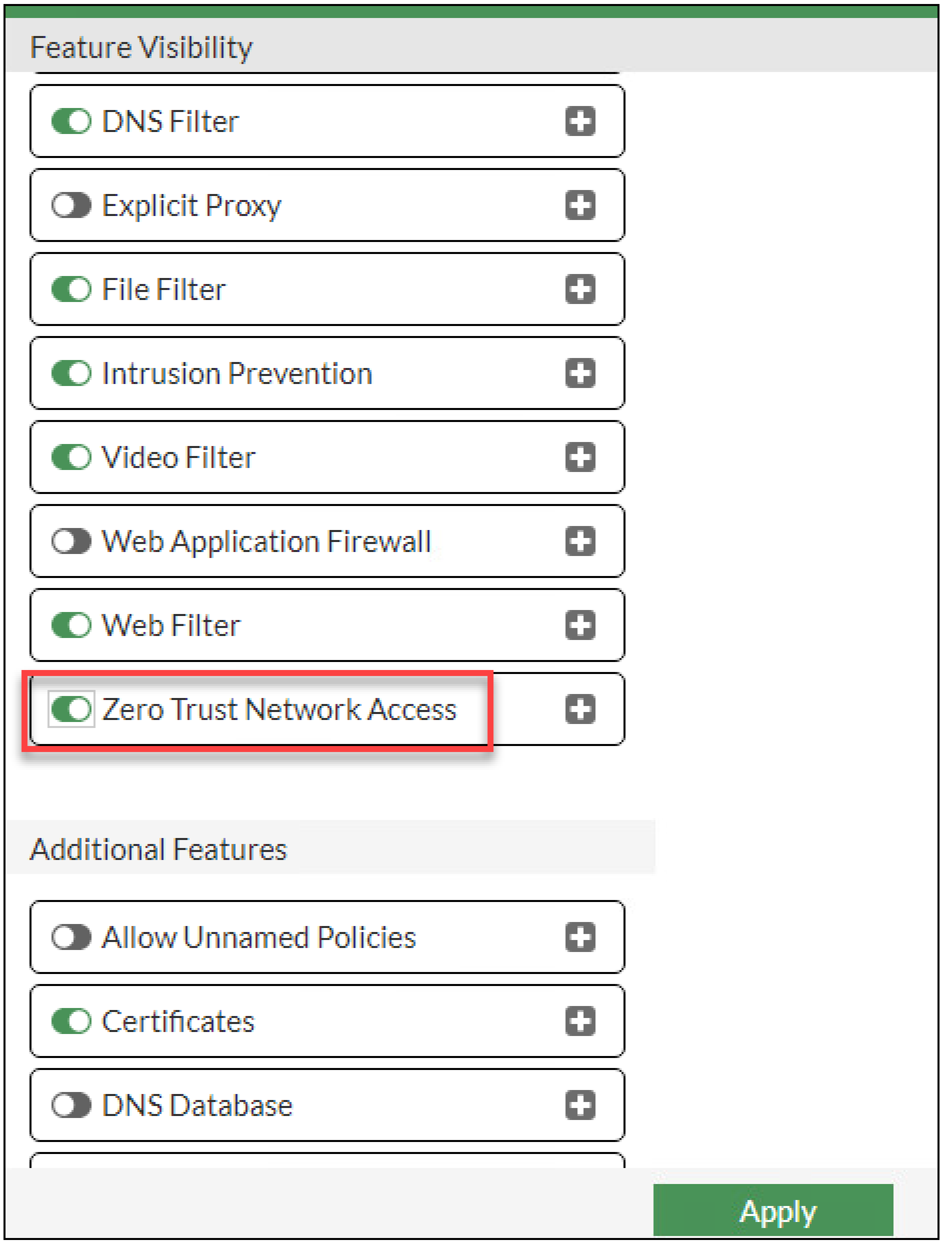
Enable ZTNA on the FortiGate GUI

You will enable ZTNA on FortiGate.

To enable ZTNA on FortiGate

1. On the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **NGFW** login page bookmark.
2. Log in to the NGFW GUI with the username `admin` and password `password`.
3. Click **System** > **Feature Visibility**.
4. Enable **Zero Trust Network Access**.

DO NOT REPRINT
© FORTINET



5. Click **Apply**.
6. Repeat steps 3–5 on the ISFW FortiGate GUI.

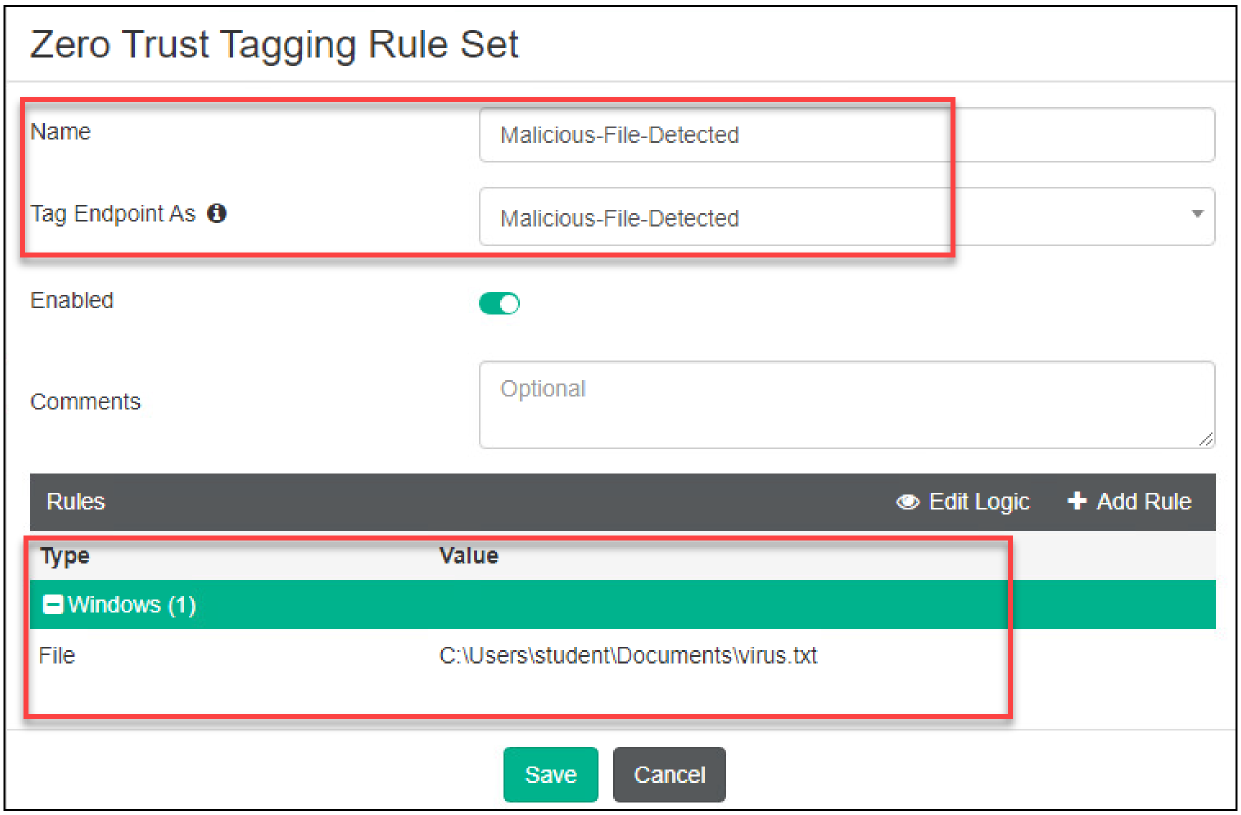
Configure FortiClient EMS ZTNA Tagging Rules

FortiClient EMS uses zero-trust tagging rules to tag endpoints based on the information that it has on each endpoint. The tags are shared with FortiGate, and are then used to assign authorization to user traffic. You will configure ZTNA tagging rules on the FortiClient EMS server.

DO NOT REPRINT
© FORTINET

To configure the FortiClient EMS ZTNA tagging rule for detecting a file

1. On the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **FortiClient EMS** login page bookmark.
2. Log in to the FortiClient EMS GUI with the username `admin` and password `Password1!`.
3. In the left menu, click **Zero Trust Tags** > **Zero Trust Tagging Rules**.
4. In the upper-right, click **Add**.
5. In the **Name** field, type `Malicious-File-Detected`.
6. In the **Tag Endpoint As** field, type `Malicious-File-Detected`, and then press `Enter`.
7. In the **Rules** section, click **Add Rule**, and then select **Windows OS**.
8. In the **Rule Type** field, select **File**.
9. In the **File** field, type `C:\Users\student\Documents\virus.txt`, and then click **Save**.

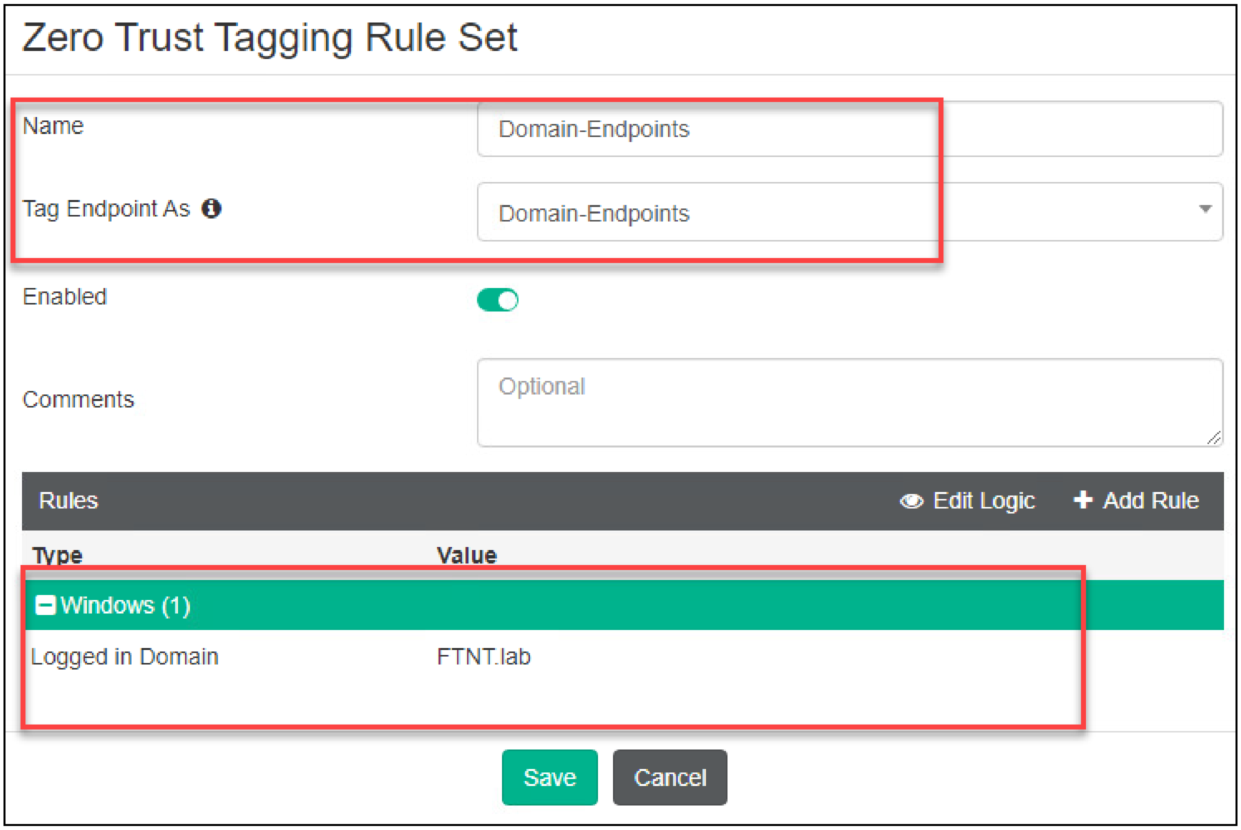


10. Click **Save** to save this zero-trust tagging rule.

To configure the FortiClient EMS ZTNA tagging rule for detecting endpoints logged into Active Directory Domain-FTNT.lab

1. Continuing on the FortiClient EMS GUI, click **Zero Trust Tags** > **Zero Trust Tagging Rules**.
2. In the upper-right, click **Add**.
3. In the **Name** field, type `Domain-Endpoints`.
4. In the **Tag Endpoint As** field, type `Domain-Endpoints`, and then press `Enter`.
5. In the **Rules** section, click **Add Rule**, and then select **Windows OS**.
6. In the **Rule Type** field, select **Logged in Domain**.
7. In the **Domain** field, type `FTNT.lab`, and then click **Save**.

DO NOT REPRINT
© FORTINET

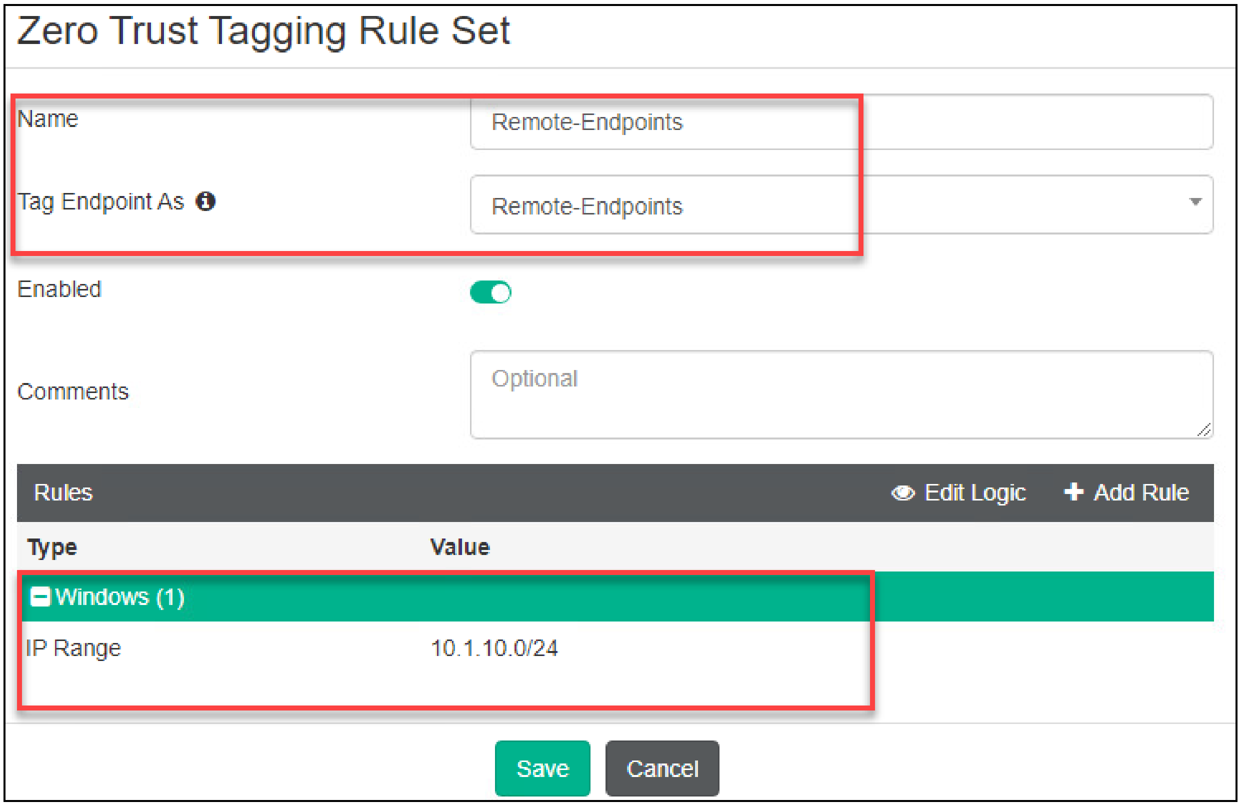


8. Click **Save** to save this zero-trust tagging rule.

To configure the FortiClient EMS ZTNA tagging rule for detecting remote endpoints

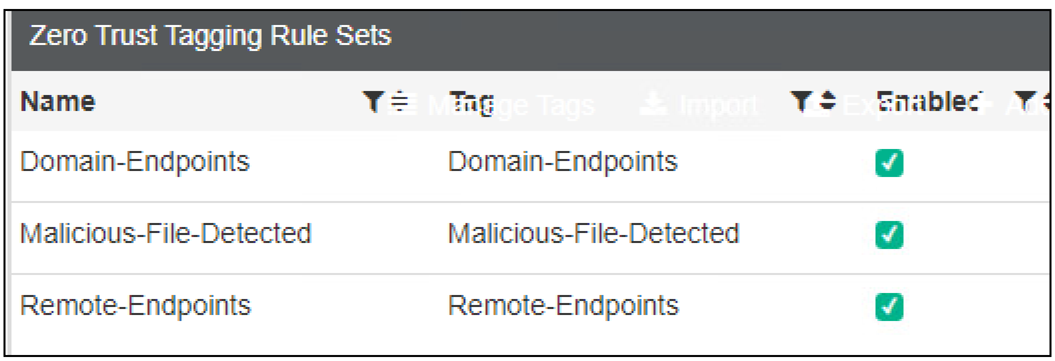
1. Continuing on the FortiClient EMS GUI, click **Zero Trust Tags** > **Zero Trust Tagging Rules**.
2. In the upper-right, click **Add**.
3. In the **Name** field, type `Remote-Endpoints`.
4. In the **Tag Endpoint As** field, type `Remote-Endpoints`, and then press `Enter`.
5. In the **Rules** section, click **Add Rule**, and then select **Windows OS**.
6. In the **Rule Type** field, select **IP Range**.
7. In the **IP range** field, type `10.1.10.0/24`, and then click **Save**.

DO NOT REPRINT
© FORTINET



8. Click **Save** to save this zero-trust tagging rule.

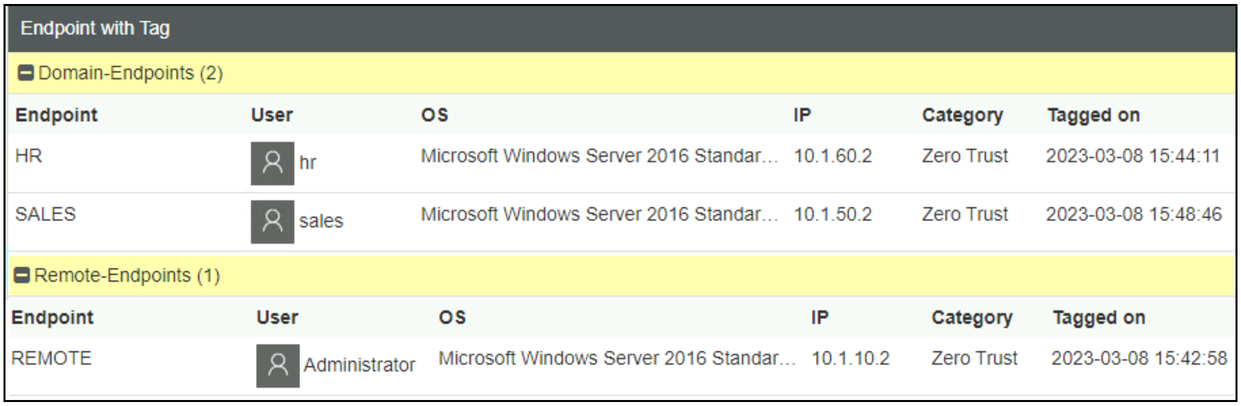
   Three rules appear in the **Zero Trust Tagging Rule Sets** section.



9. Click **Zero Trust Tags** > **Zero Trust Tag Monitor**.

   The REMOTE VM is tagged as **Remote-Endpoints** and the HR VM and SALES VM are tagged as **Domain-Endpoints**. If it does not appear immediately, use the **Refresh** button in the upper-right corner of the window.

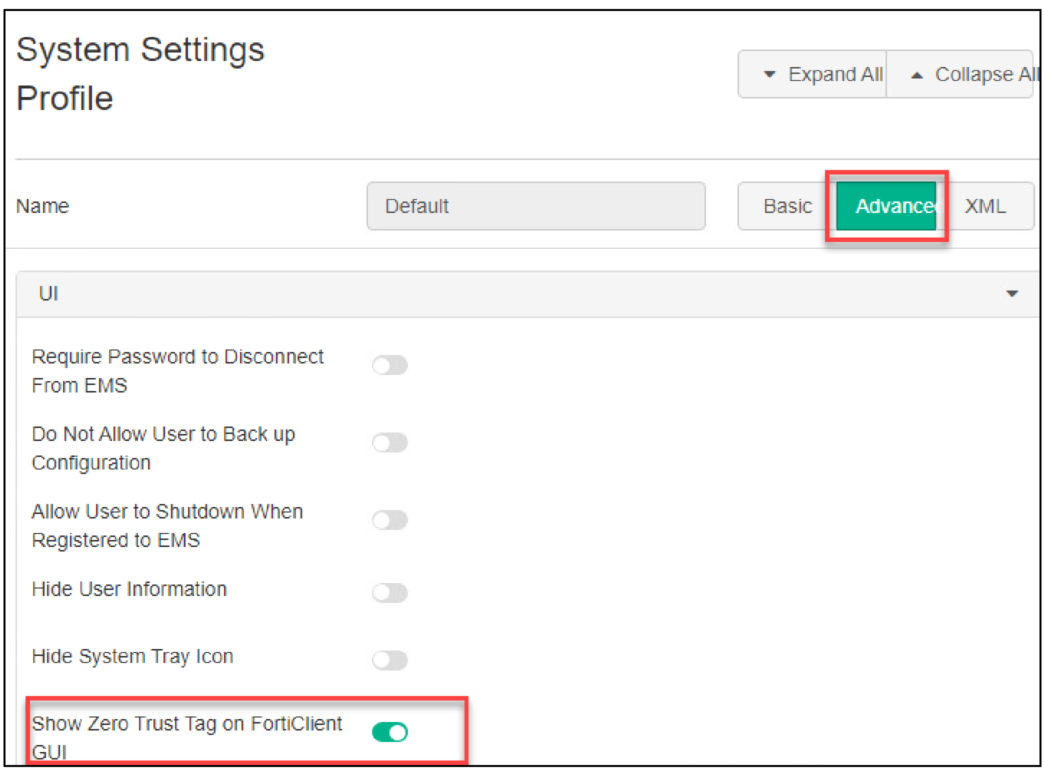
DO NOT REPRINT
© FORTINET



You will not see a tag for **Malicious-File-Detected** yet. You will create the file for detection in a later exercise.

To configure the ZTNA tag to display on FortiClient

1. Continuing on the FortiClient EMS GUI, click **Endpoint Profiles** > **System Settings**.
2. Select the **Default** profile, and then click **Edit**.
3. Click **Advanced**.
4. In the **UI** section, enable **Show Zero Trust Tag on FortiClient GUI**.

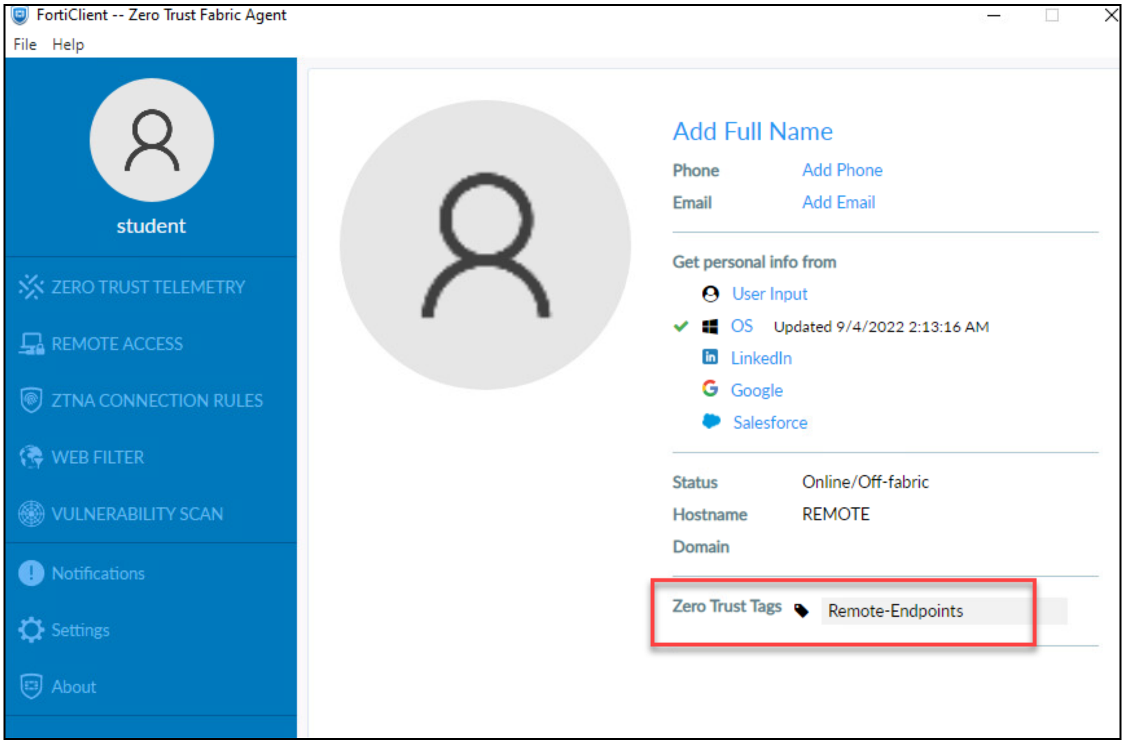


5. Click **Save** to apply the changes.

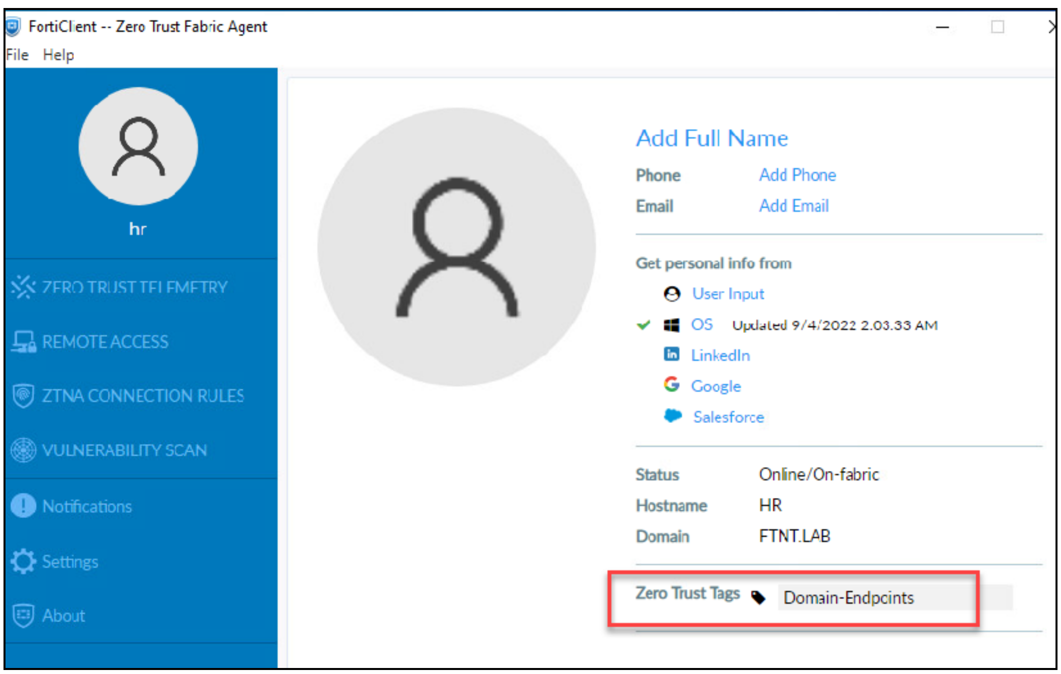
   The **Zero Trust Tags** field on FortiClient shows the currently detected tags.

6. On the Remote VM, open the FortiClient console, and then click the avatar to view the detected tags.

DO NOT REPRINT
© FORTINET



7. On the HR VM, open the FortiClient console, and then click the avatar to view the detected tags.



Verify That ZTNA Tags Are Synced

FortiOS receives only endpoint information and enforces compliance for directly connected endpoints. Directly connected endpoints are the ones that have FortiGate as the default gateway. This feature works for endpoints

DO NOT REPRINT
© FORTINET

that are connected to a VPN tunnel, as long as they can access FortiClient EMS and the FortiOS version is compatible with FortiClient EMS.

To verify ZTNA tags on ISFW FortiGate

1. Return to the FortiClient EMS VM, open PuTTY, and then connect over SSH to the ISFW saved session.
2. Log in with the username `admin` and password `password`.
3. Enter the following command to verify the status:

   `diagnose firewall dynamic list`

   The IP address of the `Domain-Endpoints` tag is displayed.

```
CMDB name: FCTEMS8822004984_Malicious-File-Detected
TAG name: Malicious-File-Detected
FCTEMS8822004984_Malicious-File-Detected: ID(25)
Total IP dynamic range blocks: 0.
Total IP dynamic addresses: 0.

CMDB name: FCTEMS8822004984_Domain-Endpoints
TAG name: Domain-Endpoints
FCTEMS8822004984_Domain-Endpoints: ID(80)
        ADDR(10.1.60.2)
Total IP dynamic range blocks: 1.
Total IP dynamic addresses: 0.

Total IP dynamic list entries: 12.
Total IP dynamic range blocks: 2.
```

To verify ZTNA tags on NGFW FortiGate

The Remote VM does not have a FortiGate as its default gateway. You will need to connect the SSL VPN to the NGFW FortiGate again for the zero-trust tags to sync.

1. On the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **NGFW** login page bookmark.
2. Log in with the username `admin` and password `password`.
3. Click **VPN** > **SSL-VPN Settings**.
4. Disable **Require Client Certificate**.
5. Click **Apply**.
6. On the Remote VM, in the system tray, double-click the FortiClient icon.
7. Click **REMOTE ACCESS**, and then click **Configure VPN**.
8. In the **Connection Name** field, type `NGFW SSLVPN`.
9. In the **Remote Gateway** field, type `10.1.3.2.`.
10. Click **Save**.
11. In the **Username** field, type `remote`.
12. In the **Password** field, type `password`.
13. Click **Connect**.

    If a FortiClient window appears, click **Yes** to continue.

DO NOT REPRINT
© FORTINET

14. Return to the FortiClient EMS VM, open PuTTY, and then connect over SSH to the NGFW saved session.
15. Log in with username `admin` and password `password`.
16. Enter the following command to verify the status:

    `diagnose firewall dynamic list`

```
FCTEMS8822004984_Domain-Endpoints: ID(80)
        ADDR(10.1.60.2)
Total IP dynamic range blocks: 1.
Total IP dynamic addresses: 0.

CMDB name: FCTEMS8822004984_Malicious-File-Detected
TAG name: Malicious-File-Detected
FCTEMS8822004984_Malicious-File-Detected: ID(25)
Total IP dynamic range blocks: 0.
Total IP dynamic addresses: 0.

CMDB name: FCTEMS8822004984_Remote-Endpoints
TAG name: Remote-Endpoints
FCTEMS8822004984_Remote-Endpoints: ID(66)
        ADDR(10.1.10.2)
        ADDR(10.1.200.101)
Total IP dynamic range blocks: 2.
Total IP dynamic addresses: 1.
```

17. Return to the Remote VM, and then in the system tray, double-click the FortiClient icon.
18. Click **REMOTE ACCESS**, and then click **Disconnect**.

DO NOT REPRINT
© FORTINET

Exercise 3: Configuring a Basic HTTPS Access Proxy With SSL Certificate-Based Authentication

In this exercise, you will configure a basic HTTPS access proxy with SSL certificate-based authentication. A client certificate is obtained when an endpoint registers with FortiClient EMS. FortiClient automatically submits a CSR request and FortiClient EMS signs and returns the client certificate. The endpoint information is synchronized between FortiGate and FortiClient EMS. You will also locate the certificate on the endpoint and match it on FortiClient EMS and FortiGate. Finally, you will see the behavior of the FortiGate `set client-cert` and `set empty-cert-action` options on the access-proxy object.

Configure a Basic HTTPS Access Proxy With Certificate-Based Authentication

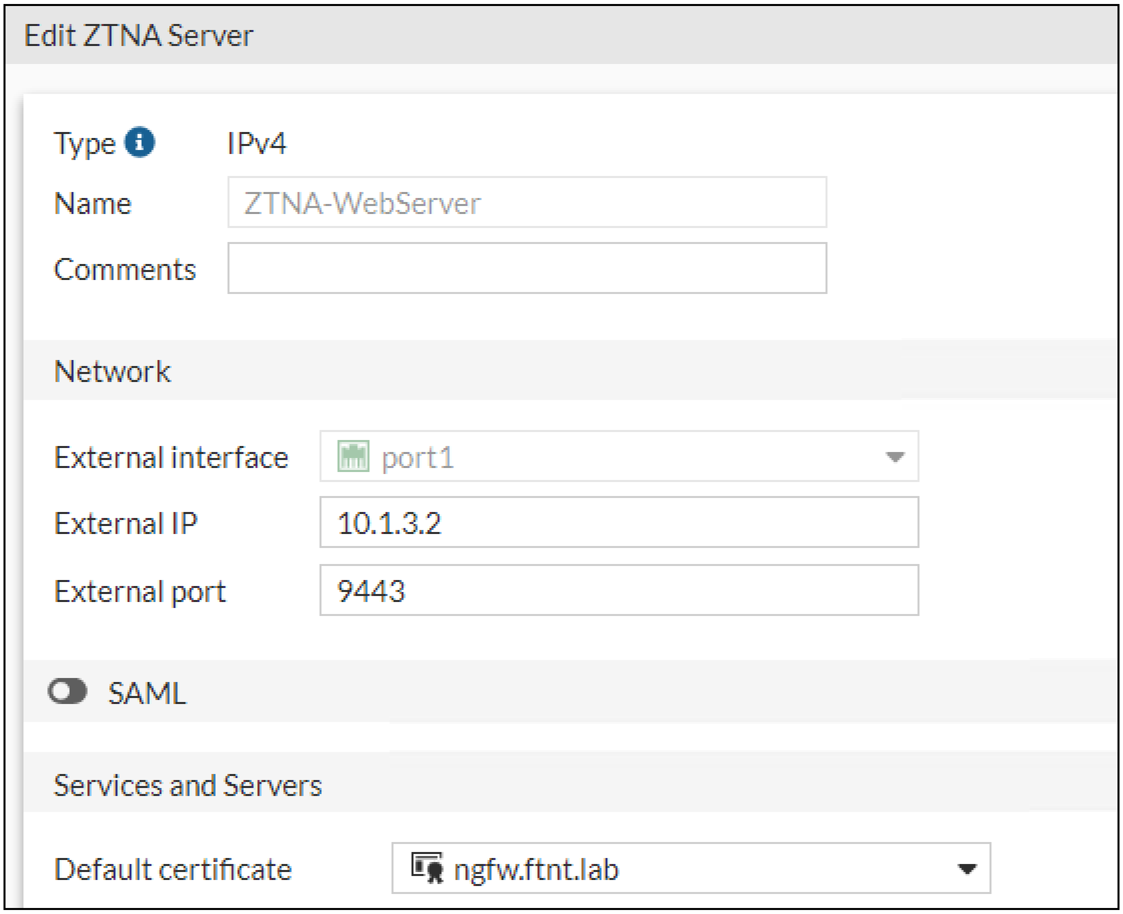
You will configure a basic HTTPS access proxy with certificate-based authentication. The HTTPS access proxy setup requires a ZTNA server, real server, and a ZTNA rule on FortiGate.

To configure the ZTNA server or HTTPS access proxy VIP

1. On the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **NGFW** login page bookmark.
2. Log in to the NGFW GUI with the username `admin` and password `password`.
3. Click **Policy & Objects** > **ZTNA**, and then click the **ZTNA Servers** tab.
4. Click **Create New**, and then configure the following settings to create a new server:

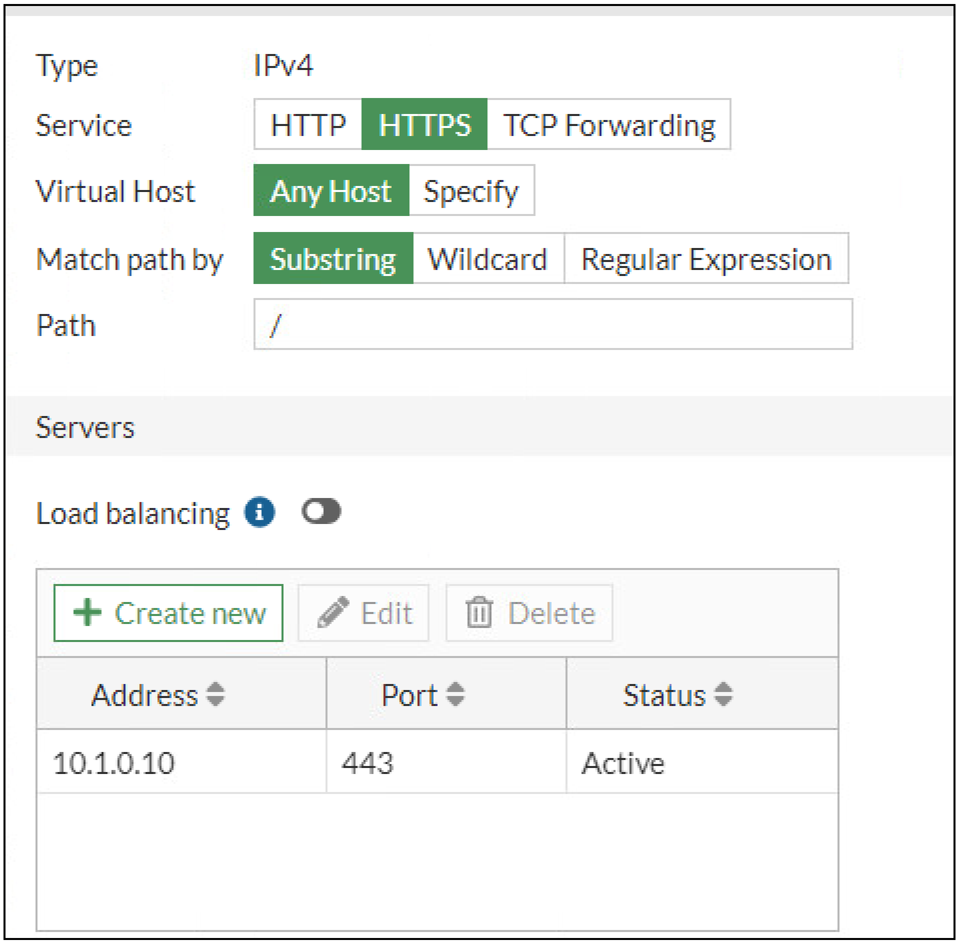
Field	Value
Name	ZTNA-WebServer
External interface	port1
External IP	10.1.3.2
External port	9443
Default certificate	ngfw.ftnt.lab

DO NOT REPRINT
© FORTINET



5. In the **Service/server mapping** section, click **Create New**.
6. In the **Service** field, select **HTTPS**.
7. In the **Virtual Host** field, select **Any Host**.
8. Leave the **Path** field at the default value of **/**.
9. In the **Servers** section, click **Create new** to create a new server mapping.
10. In the **IP** field, type `10.1.0.10`, in the **Port** field, type `443`, and then click **OK**.

DO NOT REPRINT
© FORTINET

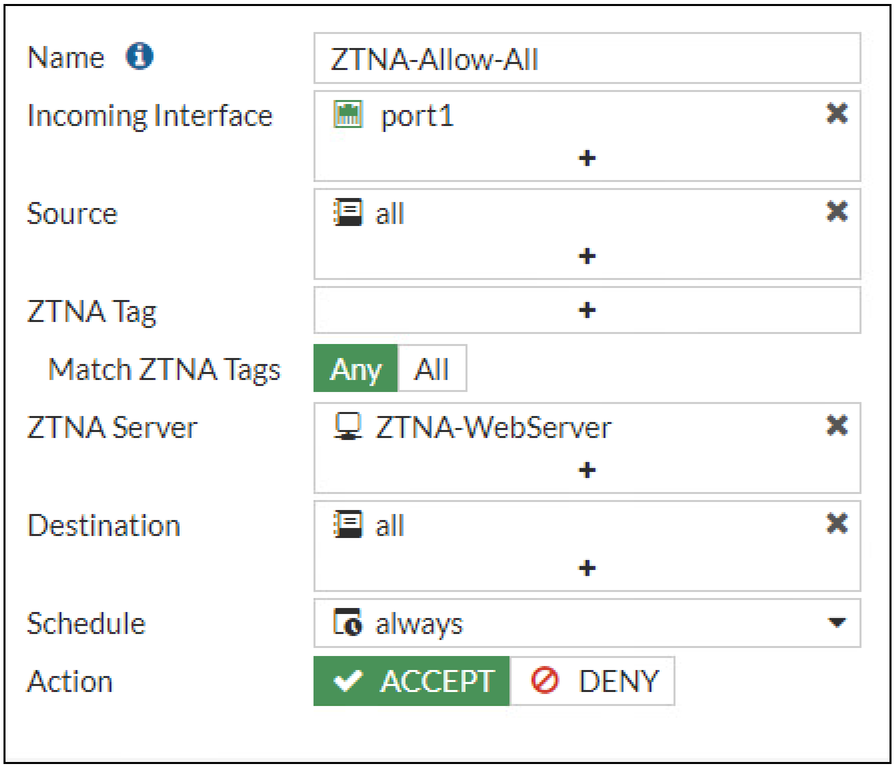


11. Click **OK** to save the **Service/server mapping** settings.
12. Click **OK** to complete the ZTNA server setup.

To configure the ZTNA rules

1. Continuing on the NGFW GUI, click **Policy & Objects** > **ZTNA**, and then click the **ZTNA Rules** tab.
2. Click **Create New** to create a new rule.
3. In the **Name** field, type `ZTNA-Allow-All`.
4. In the **Incoming Interface** field, select **port1**.
5. Leave the **Source** field set to **all**.
6. In the **ZTNA Server** field, select **ZTNA-Webserver**.
7. In the **Destination** field, select **all**.
8. In the **Action** field, select **ACCEPT**.
9. Ensure that **Enable this policy** is enabled.

DO NOT REPRINT
© FORTINET



10. Click **OK** to save the settings.

Test Remote Access to the HTTPS Access Proxy

Now that you configured FortiGate, you will test the HTTPS access proxy remote connection.

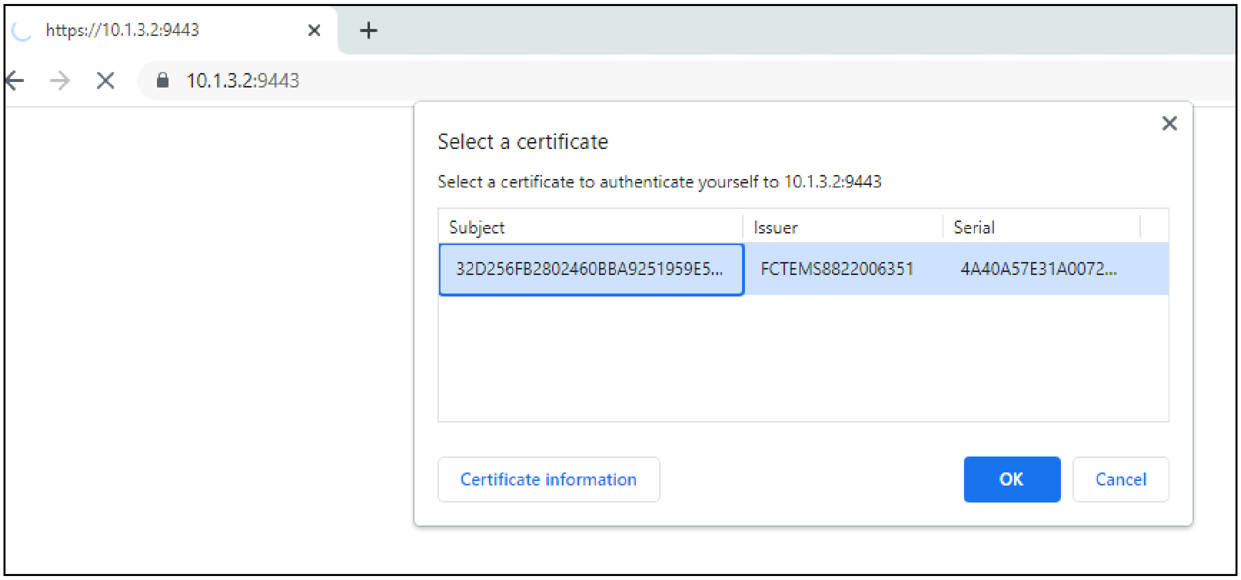
To test remote access to the HTTPS access proxy

1. On the Remote VM, open Google Chrome, and then in **Bookmarks**, select the **Webserver** bookmark.

   The browser prompts you for the client certificate to use.

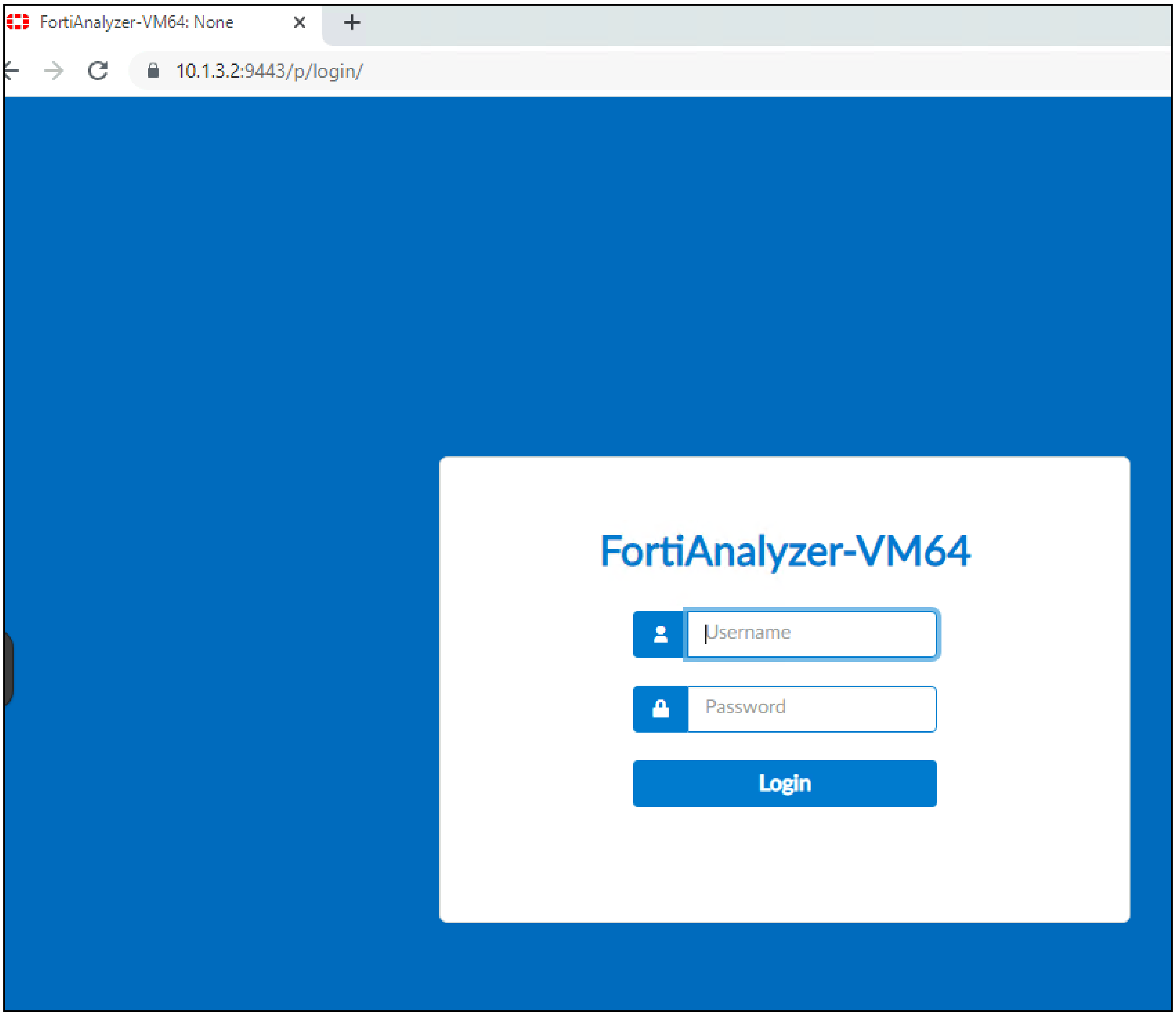
2. Select the first EMS signed certificate, and then click **OK**.

DO NOT REPRINT
© FORTINET



Access to the web server should be allowed. This lab uses the FortiAnalyzer login page to demonstrate the web page.

DO NOT REPRINT
© FORTINET

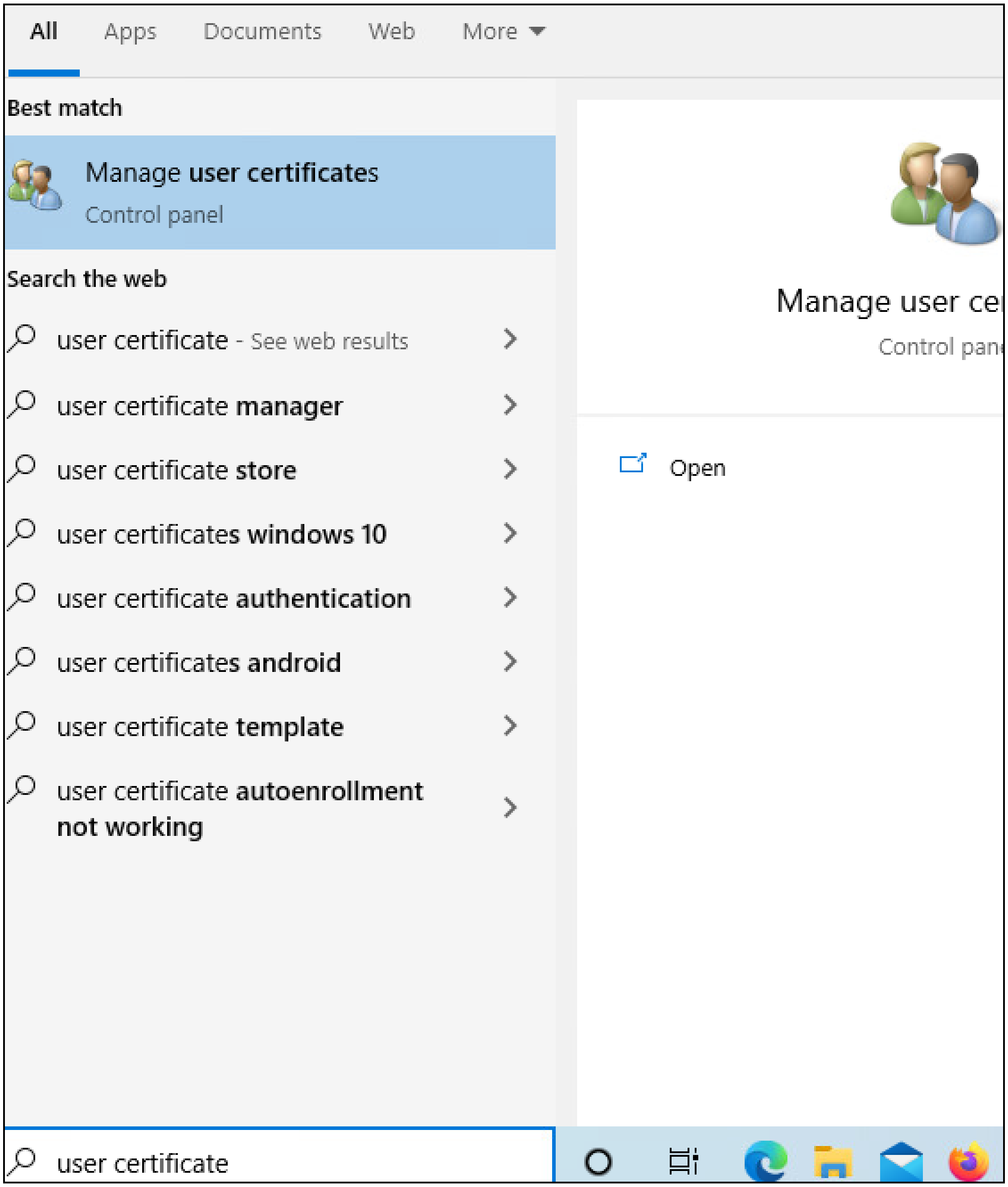


By default, client certificate authentication is enabled on the access proxy, so when the HTTPS request is received, the FortiGate WAD process challenges the client to identify itself with its certificate.

To locate the certificate on the endpoint and match it on FortiClient EMS and FortiGate

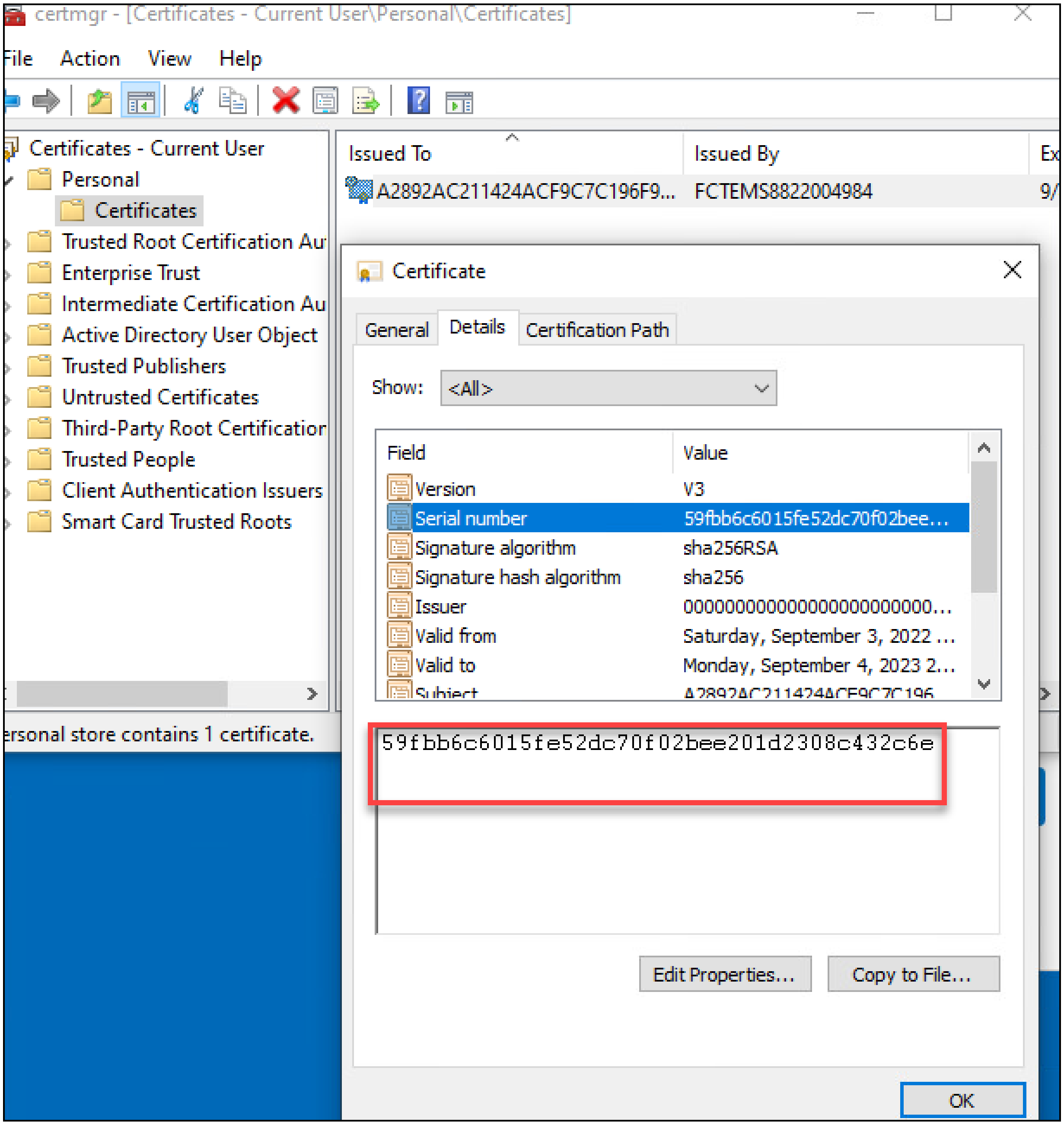
1. Continuing on the Remote VM, open a Windows search, and then search for `user certificate`.

DO NOT REPRINT
© FORTINET



2. In the user certificate store, open the **Personal** > **Certificates** folders.
3. Choose the `FCTEMS` issued certificate, and then double-click the certificate to view the properties.
4. Click the **Details** tab, and then find the **Serial number** of the certificate.

DO NOT REPRINT
© FORTINET



Your certificate might not match what is shown in this image.

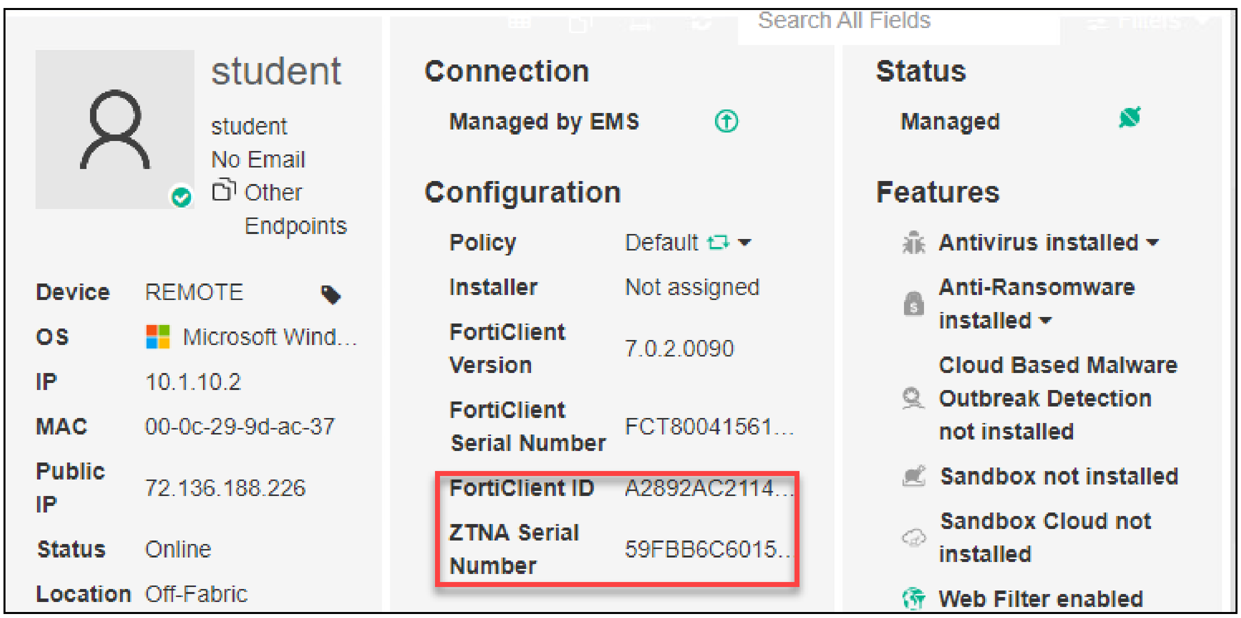
5. Return to the NGFW FortiGate, and then enter the following CLI command to view the endpoint serial number **SN**, **UID**, and other information:

```
diagnose endpoint record list
```

DO NOT REPRINT
© FORTINET


```
NGFW # diagnose endpoint record list
Record #1:
                IP Address = 10.1.10.2
                MAC Address = 00:0c:29:9d:ac:37
                MAC list = 00:0c:29:9d:ac:37;
                VDOM =  (-1)
                EMS serial number: FCTEMS8822004984
                Client cert SN: 59FBB6C6015FE52DC70F02BEE201D2308C432C6E
                Public IP address: 72.136.188.226
                Quarantined: no
                Online status: online
                Registration status: registered
                On-net status: off-net
                Gateway Interface:
                FortiClient version: 7.0.2
                AVDB version: 1.0
                FortiClient app signature version: 22.385
                FortiClient vulnerability scan engine version: 2.31
                FortiClient UID: A2892AC211424ACF9C7C196F9E84BCAA
                Host Name: REMOTE
                OS Type: WIN64
                OS Version: Microsoft Windows 10 , 64-bit  (build 19044) (version 2009)
                Host Description:
                Domain:
                Last Login User: student
```

6. Open a new Google Chrome tab, and then in **Bookmarks**, select the **FortiClient EMS** login page bookmark.
7. Log in to the FortiClient EMS with the username `admin` and password `Password1!`.
8. Click **Endpoints** > **All Endpoints**.
9. In the list, click **REMOTE**, and then in the **Configuration** section, check the **FortiClient ID** and **ZTNA Serial Number** fields to match the information.



DO NOT REPRINT
© FORTINET

Understand the Default Behavior of the set empty-cert-action Option

By default, client certificate authentication is enabled on the access proxy, and `empty-cert-action` is set to `block`. If a user clicks **Cancel** during the certificate challenge, one of the following actions occurs:

- If the `empty-cert-action` is set to `accept`, the client is allowed to continue with ZTNA proxy rule processing.
- If the `empty-cert-action` is set to `block`, the client is blocked from further ZTNA proxy rule processing (default behavior).

The `empty-cert-action` options can be configured from the CLI only.

To review the default FortiGate behavior of the empty certificate challenge

1. On the Remote VM, open Google Chrome, and then in **Bookmarks**, select the **Webserver** bookmark.

   The browser prompts you for the client certificate to use.

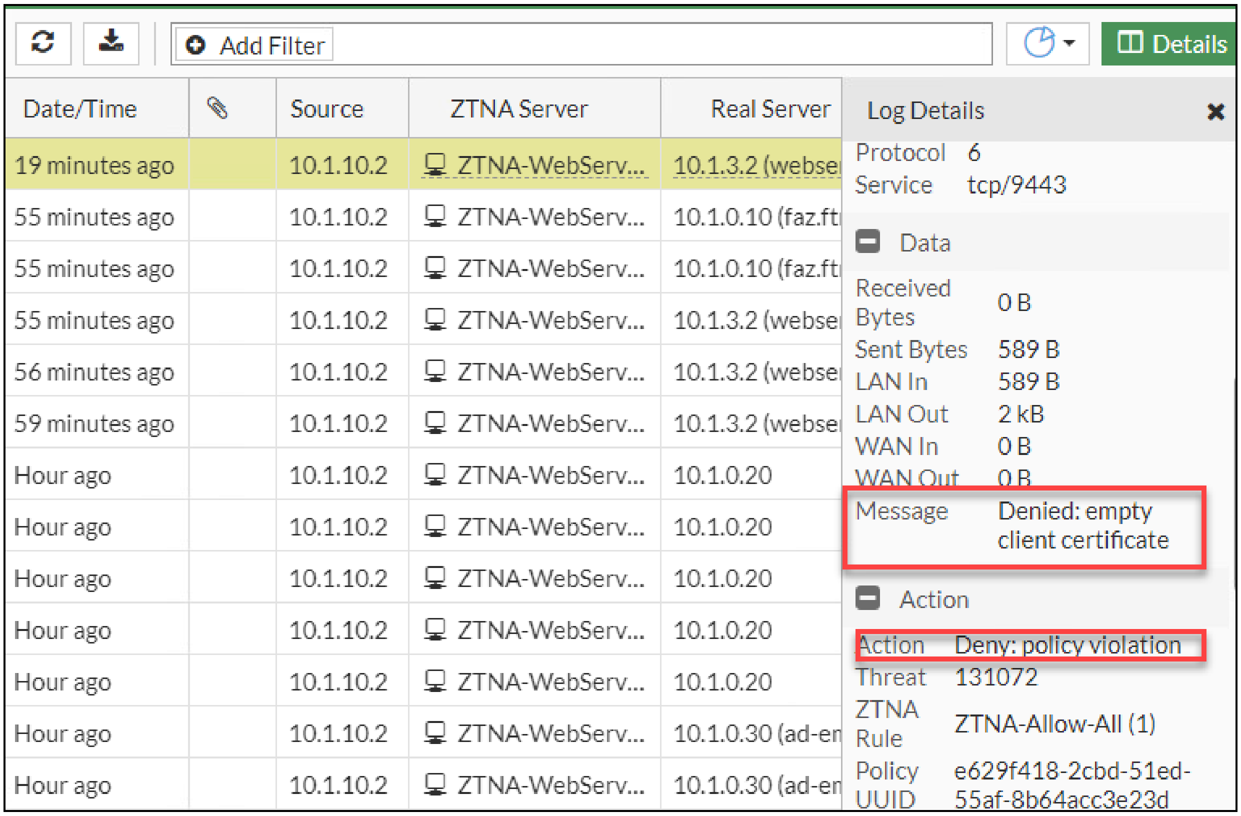
2. Click **Cancel**.

   FortiGate blocks access.

3. Return to the FortiClient EMS VM, and then on the NGFW GUI, click **Log & Report** > **ZTNA Traffic**.
4. Review the log with **Action Deny: policy violation**.

   The message shows **Denied: empty client certificate**.

DO NOT REPRINT
© FORTINET



DO NOT REPRINT
© FORTINET

Exercise 4: Configuring an HTTPS Access Proxy With Basic Local User Authentication and ZTNA Tags

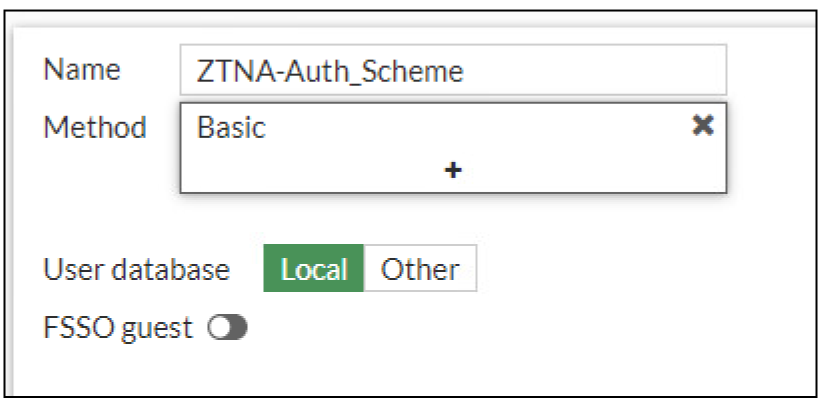
In this exercise, you will extend the solution to include performing user authentication with local users, and security posture checks with ZTNA tags.

Configure an HTTPS Access Proxy With Basic Local User Authentication and ZTNA Tags

You will configure an HTTPS access proxy with basic local user authentication and ZTNA tags. The HTTPS access proxy setup with local authentication and ZTNA tags requires an authentication scheme, authentication rule, and ZTNA tags configured on the ZTNA policies.

To configure an authentication scheme on FortiGate

1. On the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **NGFW** login page bookmark.
2. Log in to the NGFW GUI with the username `admin` and password `password`.
3. Click **Policy & Objects** > **Authentication Rules**, and then in the upper-right corner, select **Authentication Schemes**.
4. Click **Create New** > **Authentication Scheme**.
5. In the **Name** field, type `ZTNA-Auth-Scheme`.
6. In the **Method** field, select **Basic**.
7. Leave the **User database** field set to **Local**.



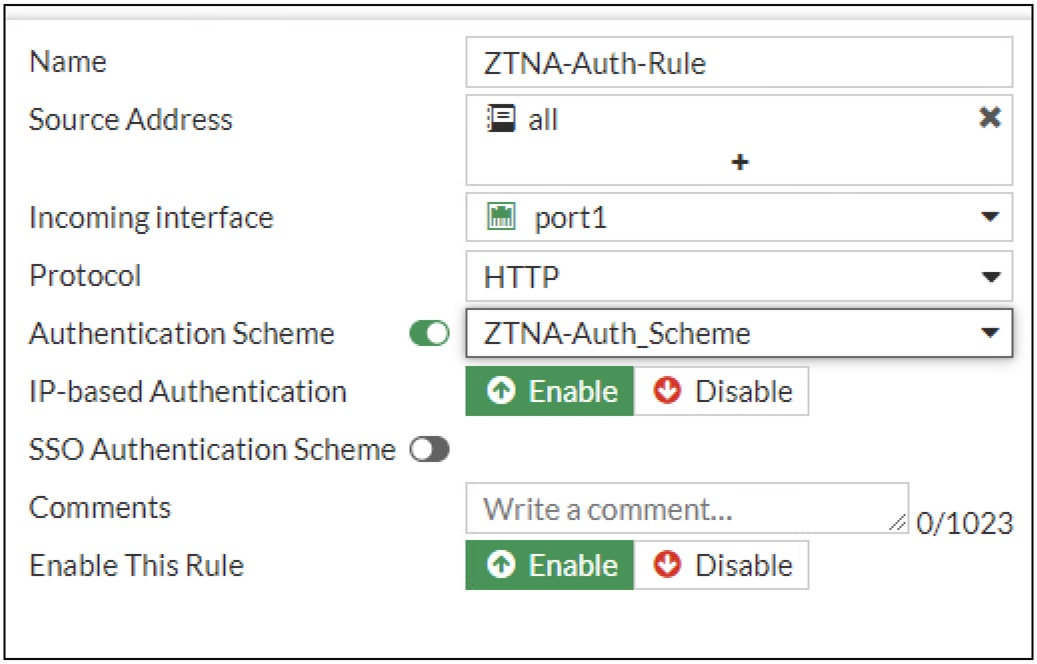
8. Click **OK** to save the settings.

To configure an authentication rule on FortiGate

1. Continuing on the **Authentication Rules** page, click **Create New** > **Authentication Rule**.
2. In the **Name** field, type `ZTNA-Auth-Rule`.
3. In the **Source Address** field, select **all**.

DO NOT REPRINT
© FORTINET

4. In the **Incoming interface** field, select **port1**.
5. Leave the **Protocol** field set to **HTTP**.
6. Enable **Authentication Scheme**, and then select **ZTNA-Auth_Scheme**.
7. Ensure that the **Enable This Rule** field is set to **Enable**.

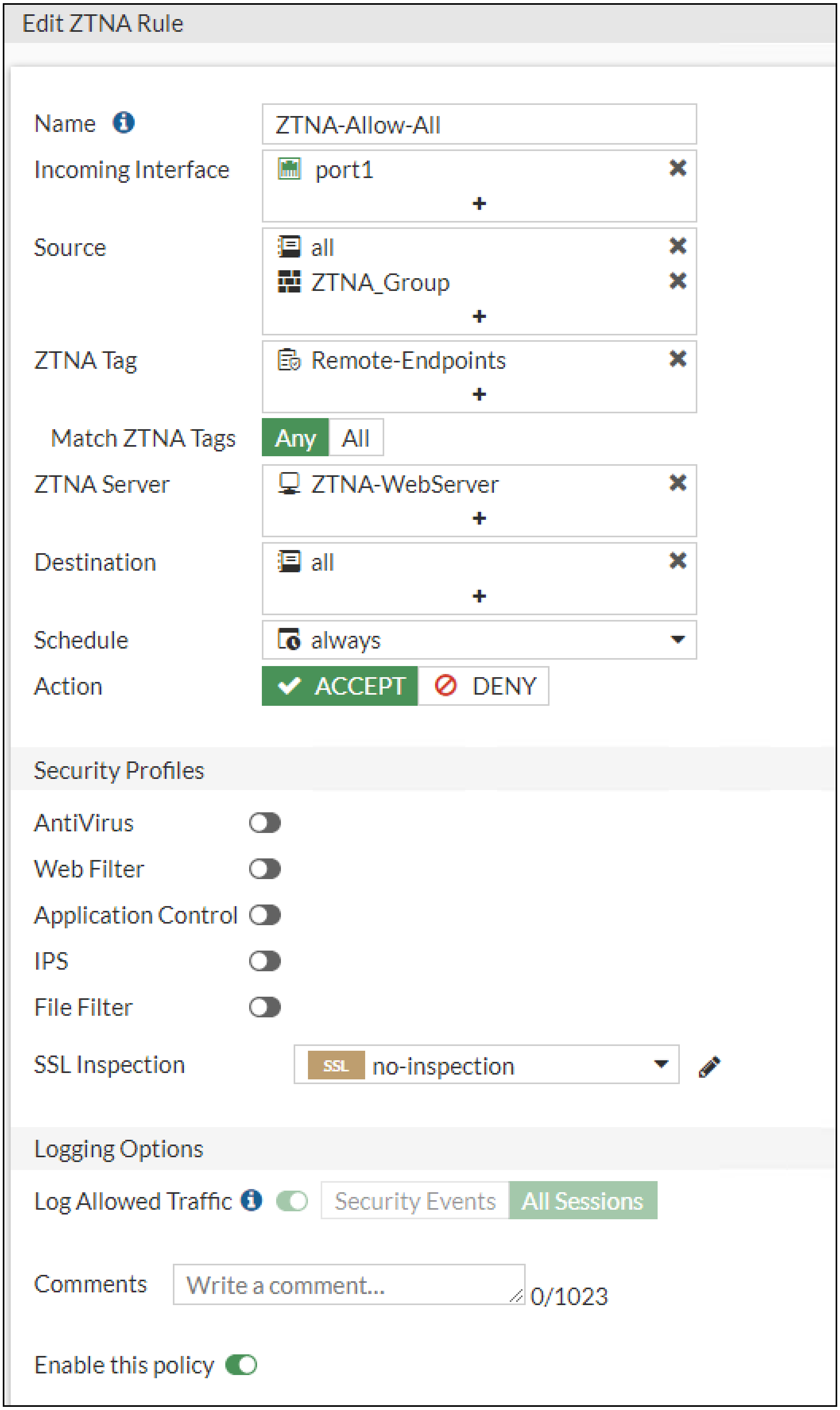


8. Click **OK** to save the rule.

To apply a user group and add a ZTNA tag on the ZTNA allow rule

1. Continuing on the NGFW FortiGate GUI, click **User & Authentication** > **User Groups**.
2. Edit the **ZTNA_Group** user group.
3. In the **Members** field, click **+**, and then select **remote**.
4. Click **OK**.
5. Click **Policy & Objects** > **ZTNA**.
6. Click **ZTNA Rules**, select **ZTNA-Allow-All**, and then click **Edit**.
7. In the **Source** field, click **+** to add a new entry.
8. Select **User**, and then select **ZTNA_Group**.
9. In the **ZTNA Tag** field, click **+**, and then select the **Remote-Endpoints** IP tag.

DO NOT REPRINT
© FORTINET



DO NOT REPRINT
© FORTINET

10. Click **OK** to apply the changes.

To create a deny rule for malicious file detection

1. Continuing on the NGFW GUI, click **Policy & Objects** > **ZTNA**, and then click the **ZTNA Rules** tab.
2. Click **Create New** to create a new rule.
3. In the **New ZTNA Rule** window, configure the following settings:

Field	Value
Name	ZTNA-Deny
Interface	port1
Source	Address: **all** User: **ZTNA_Group**
ZTNA Tag	Malicious-File-Detected
ZTNA Server	ZTNA-Webserver
Destination	all
Action	Deny
Enable this policy	<enable>

4. Click **OK** to save the new rule.
5. Move this rule above the **ZTNA-Allow-All** rule.

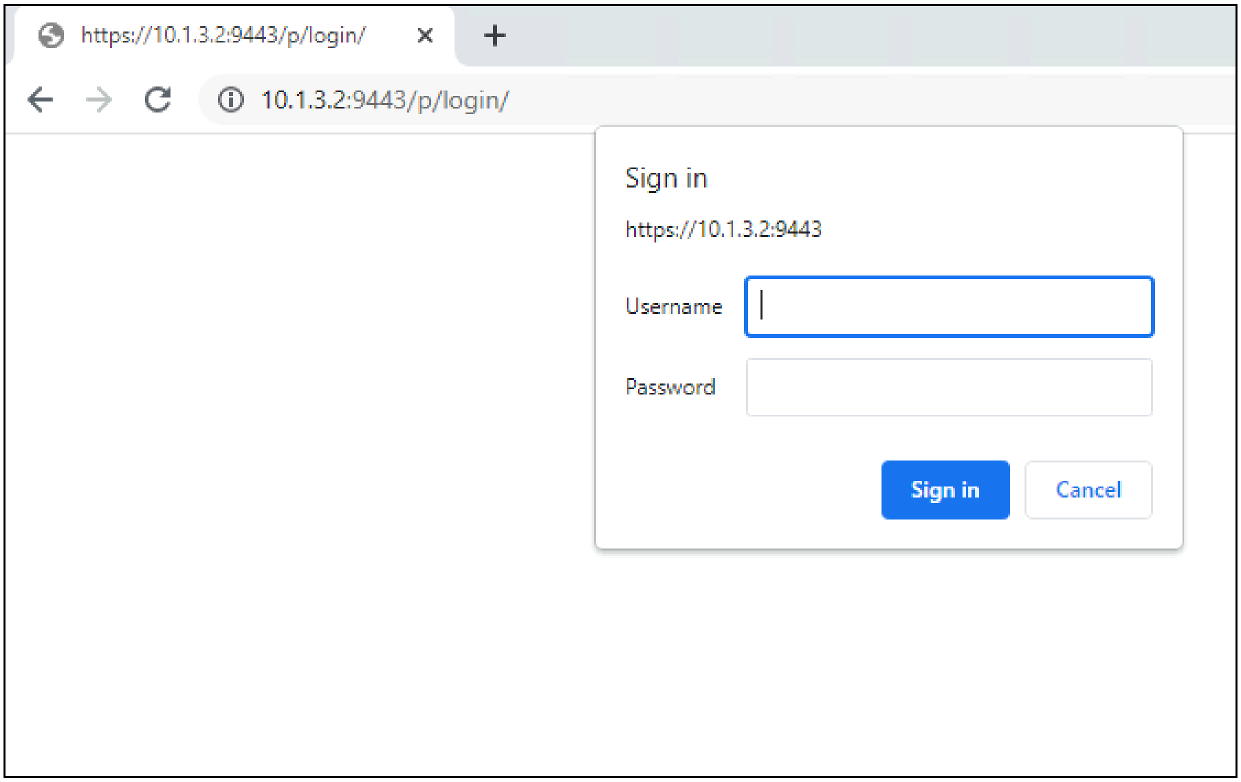
Test the Connection for Users

Now that you configured FortiGate, you will test the HTTPS access proxy remote connection.

To test the connection for authorized users

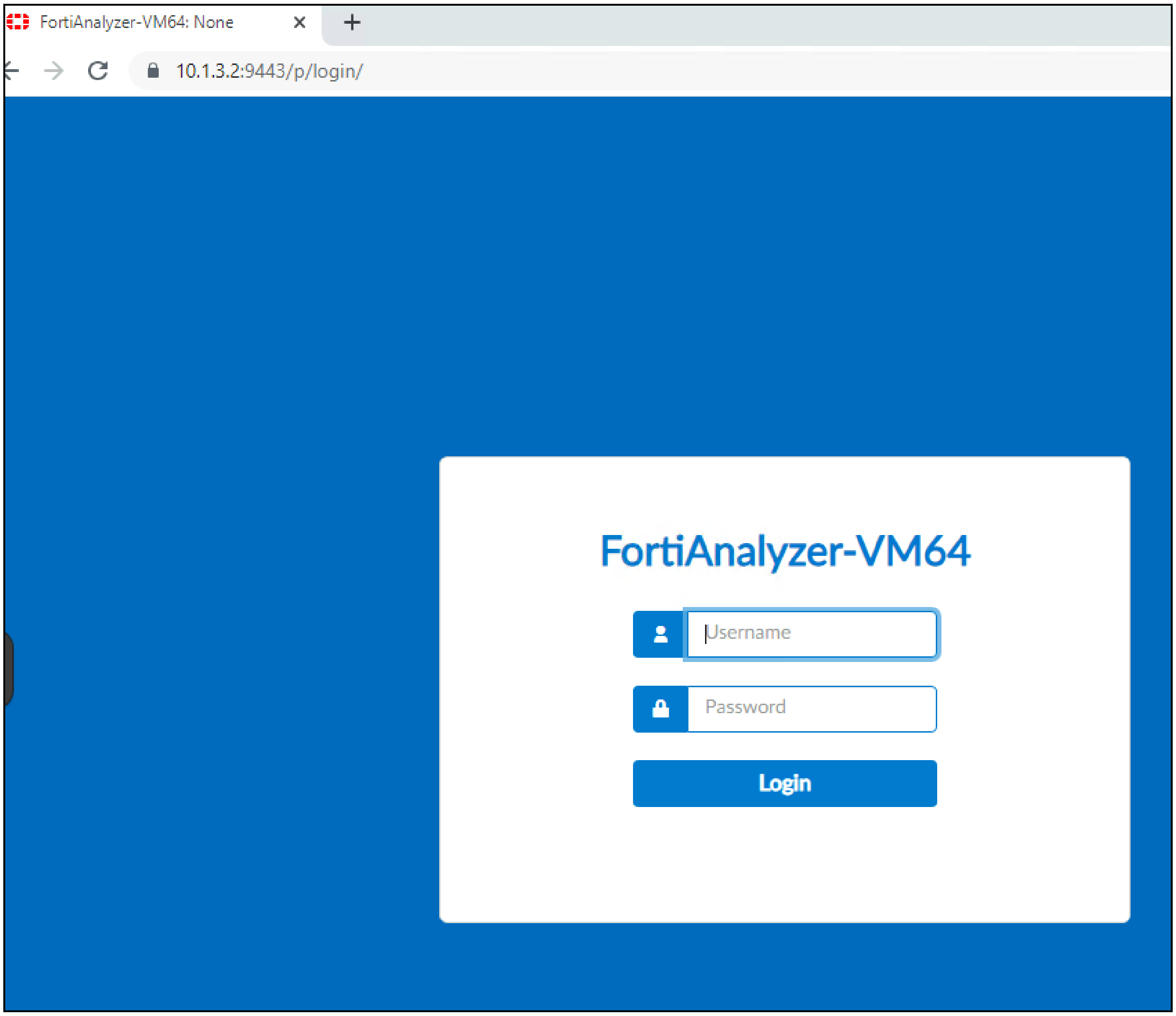
1. On the Remote VM, open Google Chrome, and then in **Bookmarks**, select the **Webserver** bookmark.
   The browser prompts you for the client certificate to use.
2. Select the EMS signed certificate, and then click **OK**.
3. When you are prompted to sign in, type the **Username** `remote` and **Password** `password`, and then click **Sign in** to access the page.

DO NOT REPRINT
© FORTINET

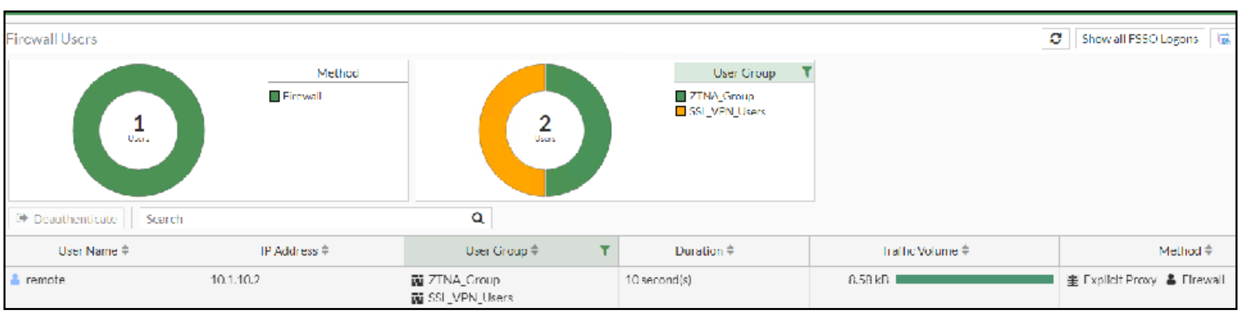


After successful authentication, you can access the web page.

DO NOT REPRINT
© FORTINET



4. Close the Google Chrome browser.
5. Return to the FortiClient-EMS VM, and then on the NGFW GUI, click **Dashboard** > **Firewall User Monitor**.



6. Select **remote**, and then click **Deauthenticate** to remove the user from FortiGate.

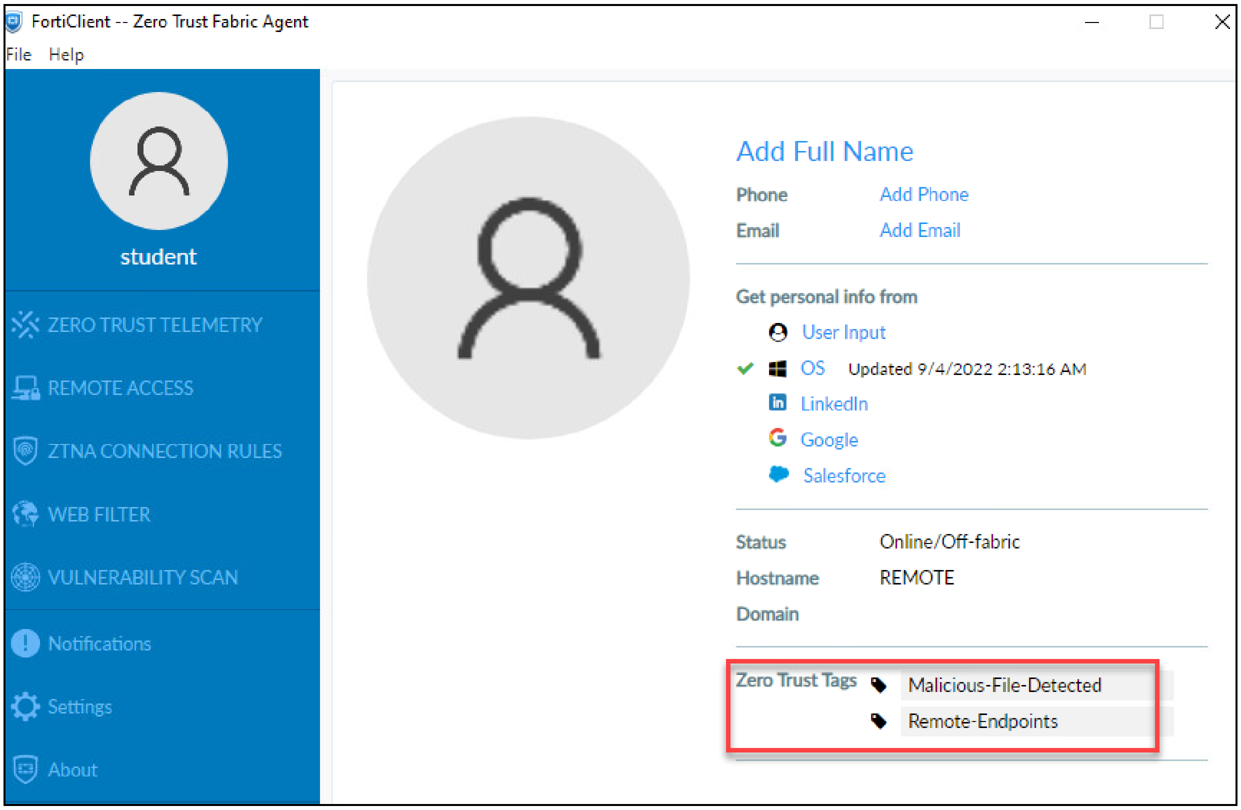
To detect a malicious file and tag an endpoint

1. Return to the Remote VM, open Notepad, and then create a file with dummy text.
2. Save the file in the **Documents** folder for the **student** user: `C:\Users\student\Documents\virus.txt`.

DO NOT REPRINT
© FORTINET

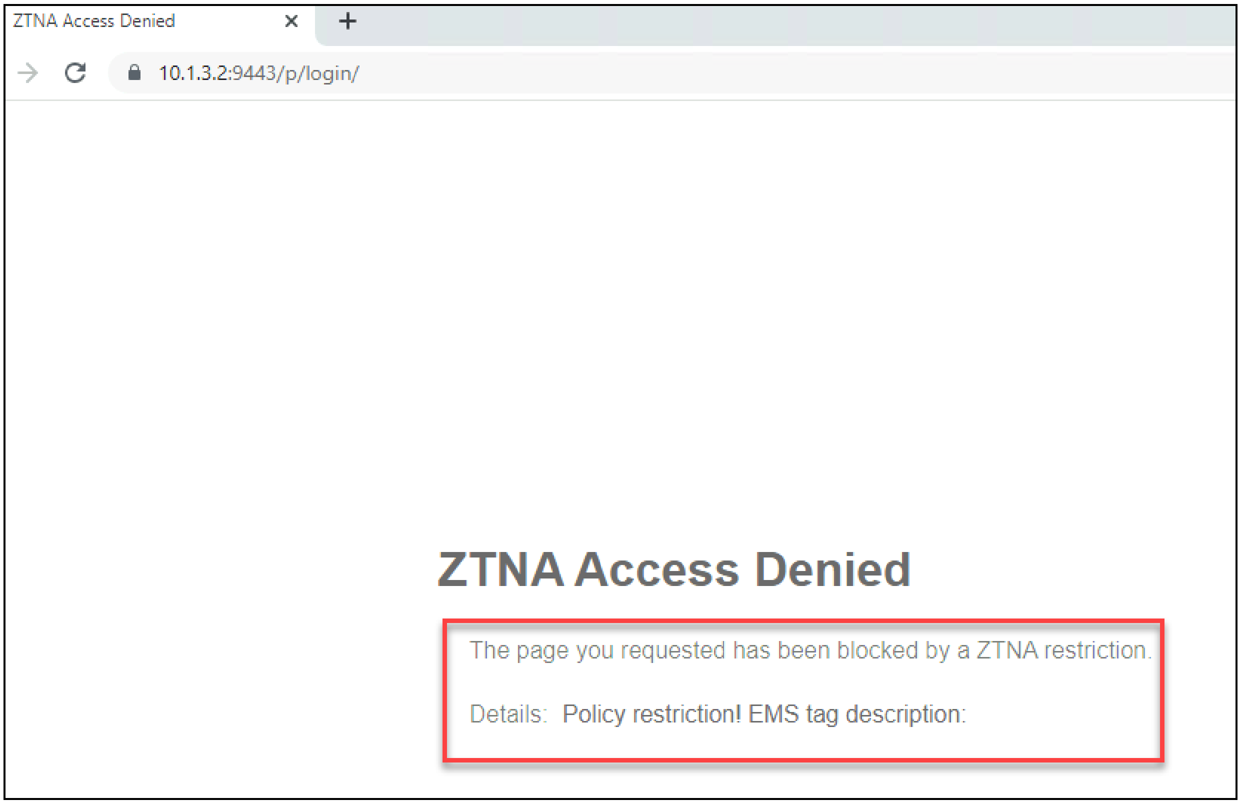
3. Open the FortiClient console, and then click the avatar to view the detected tags.

   It may take a minute to see the updated tags.



4. On the desktop, open Google Chrome, and then in **Bookmarks**, select the **Webserver** bookmark.
5. Select the EMS signed certificate, and then click **OK**.

DO NOT REPRINT
© FORTINET



Access is denied because the endpoint security posture has changed.

If access is still allowed, after the tags have been updated on FortiClient, restart the ZTNA process on NGFW FortiGate.

1. On the FortiClient EMS VM, open PuTTY, and then connect over SSH to the NGFW saved session.
2. Log in with the username `admin` and password `password`.
3. Enter the following command to restart the process:

```
diagnose test application fcnacd 99
```

---

6. On the Remote VM, delete the `C:\Users\student\Documents\virus.txt` file.

DO NOT REPRINT
© FORTINET

Exercise 5: Configuring a TCP Forwarding Access Proxy for RDP and SSH

In this exercise, you will configure TCP forwarding on FortiGate and the corresponding ZTNA connection rules on FortiClient to proxy the connections to the access proxy. A TCP forwarding access proxy is very similar to an HTTPS access proxy. A TCP forwarding access proxy works as a special type of HTTPS reverse proxy. TCP traffic is tunneled between the client and the access proxy over HTTPS, and forwarded to the protected resource over TCP using the original upper layer protocol.

Configure a TCP Access Proxy With ZTNA Tags

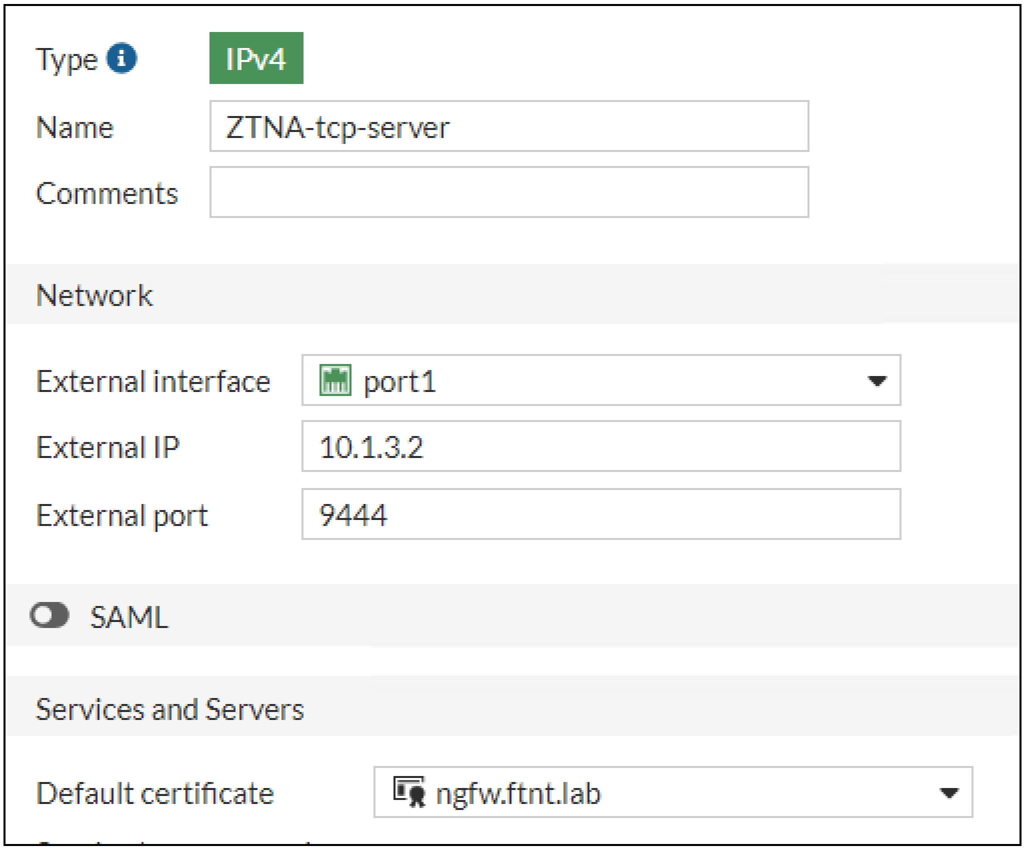
You will configure a TCP access proxy with ZTNA tags. The TCP access proxy setup requires a ZTNA server, real server, and ZTNA rule on FortiGate. You also require ZTNA connection rules on FortiClient.

To configure the ZTNA server for a TCP access proxy VIP for SSH to the FortiAnalyzer

1. On the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **NGFW** login page bookmark.
2. Log in to the NGFW GUI with the username `admin` and password `password`.
3. Click **Policy & Objects** > **ZTNA**, and then click the **ZTNA Servers** tab.
4. Click **Create New**, and then configure the following settings to create a new server:

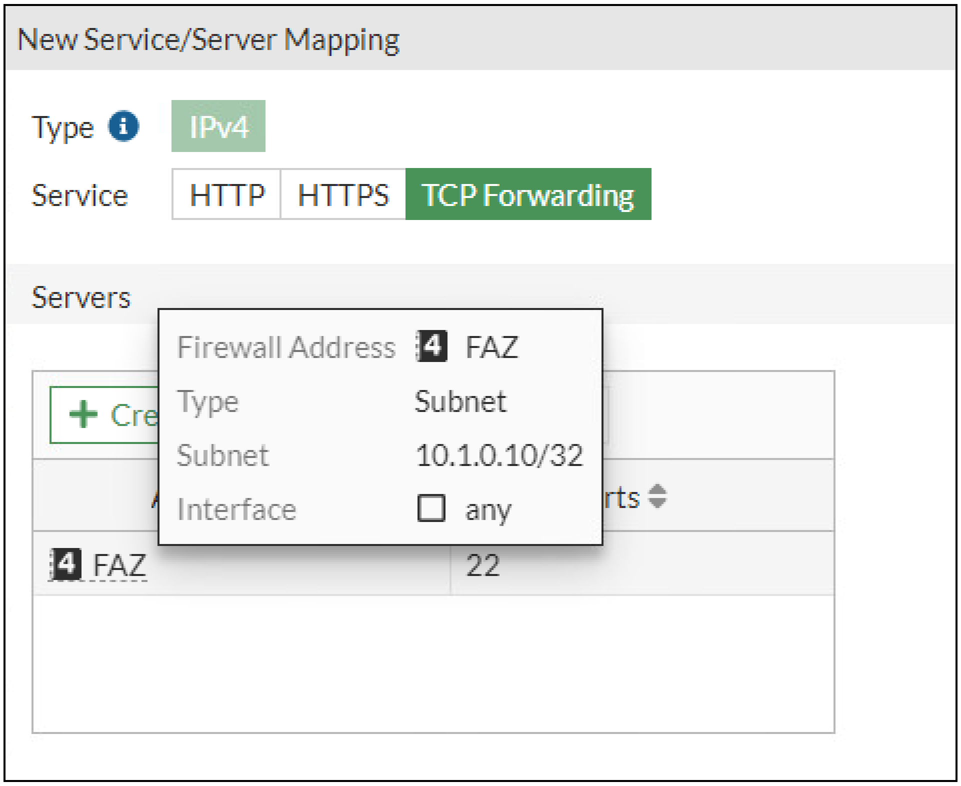
Field	Value
Name	ZTNA-tcp-server
External interface	port1
External IP	10.1.3.2
External port	9444
Default certificate	ngfw.ftnt.lab

DO NOT REPRINT
© FORTINET



5. In the **Service/server mapping** section, click **Create New**.
6. In the **Service** field, select **TCP Forwarding**.
7. In the **Servers** section, click **Create New** to create a new server mapping.
8. In the **Address** field, click **Create**, and then click **Firewall Address**.
9. In the **Name** field, type `FAZ`.
10. In the **IP/Netmask** field, type `10.1.0.10/32`.
11. Click **OK**.
12. Select **FAZ**.
13. In the **Ports** field, type `22`.
14. Click **OK**.

DO NOT REPRINT
© FORTINET

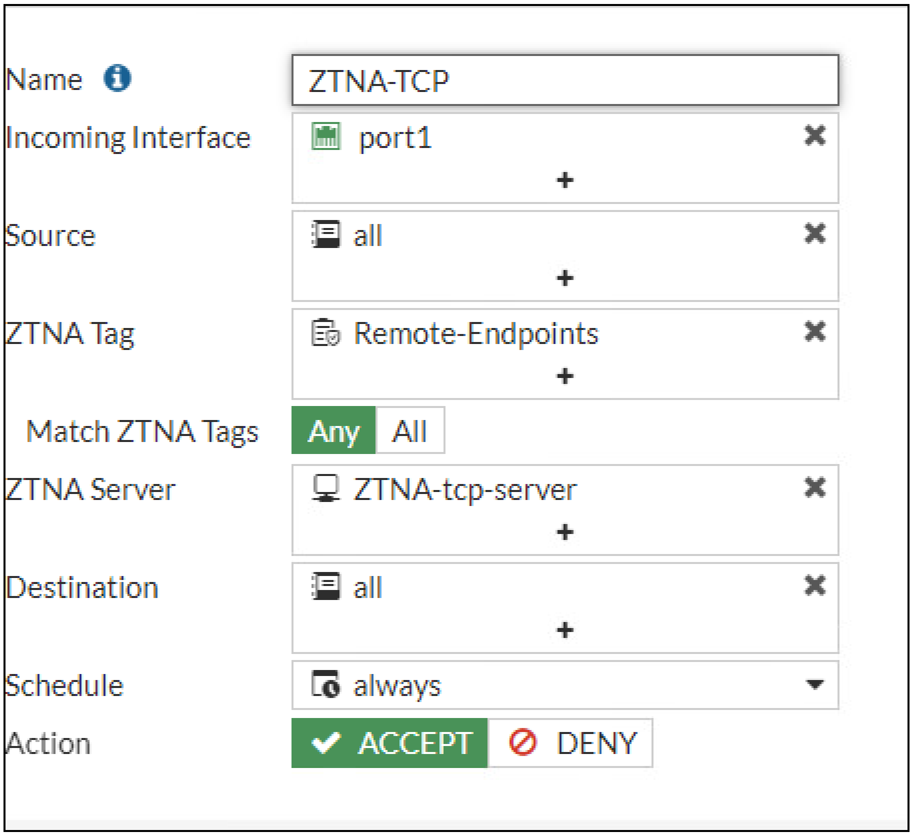


15. Click **OK**.
16. Click **OK** to complete the ZTNA server settings.

To configure the ZTNA rules

1. Continuing on the NGFW GUI, click **Policy & Objects** > **ZTNA**, and then click the **ZTNA Rules** tab.
2. Click **Create New** to create a new rule.
3. In the **Name** field, type `ZTNA-TCP`.
4. In the **Incoming Interface** field, click **+**, and then select **port1**.
5. Leave the **Source** field set to **all**.
6. In the **ZTNA Tag** field, click **+**, and then select the **Remote-Endpoints** IP tag.
7. In the **ZTNA Server** field, click **+**, and then select **ZTNA-tcp-server**.
8. In the **Destination** field, click **+**, and then select **all**.
9. In the **Action** field, select **ACCEPT**.
10. Ensure that **Enable this policy** is enabled.

DO NOT REPRINT
© FORTINET

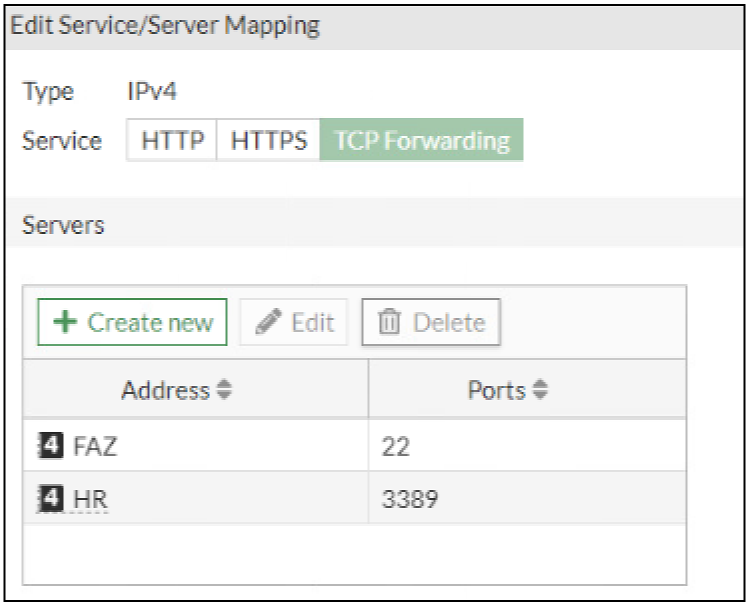


11. Click **OK** to apply the changes.

To configure the ZTNA server for a TCP access proxy VIP for RDP to the HR VM

1. Continuing on the NGFW GUI, click **Policy & Objects** > **ZTNA**, and then click the **ZTNA Servers** tab.
2. Double-click **ZTNA-tcp-server** to edit it.
3. In the **Service/server mapping** section, select **TCP Forwarding**, and then click **Edit**.
4. In the **Servers** section, click **Create new** to create a new server mapping.
5. In the **Address** field, click **Create**, and then click **Firewall Address**.
6. In the **Name** field, type `HR`.
7. In the **IP/Netmask** field, type `10.1.60.2/32`.
8. Click **OK**.
9. Select **HR**.
10. In the **Ports** field, type `3389`.
11. Click **OK**.

DO NOT REPRINT
© FORTINET



12. Click **OK**.
13. Click **OK** to complete the ZTNA server settings.

To configure the ZTNA destination rules on FortiClient

1. On the Remote VM, open the FortiClient console.
2. Click **ZTNA CONNECTION RULES**, and then click **Add Rule**.

3. In the **Rule Name** field, type `FAZ SSH`.
4. In the **Destination Host** field, type `10.1.0.10:22`.
5. In the **Proxy Gateway** field, type `10.1.3.2:9444`.

DO NOT REPRINT
© FORTINET

6. Click **Create**.
7. Click **Add Rule** again to add a new rule.
8. In the **Rule Name** field, type `HR RDP`.
9. In the **Destination Host** field, type `10.1.60.2:3389`.
10. In the **Proxy Gateway** field, type `10.1.3.2:9444`.
11. Click **Create**.

    Two rules should be listed in the ZTNA connection rules.

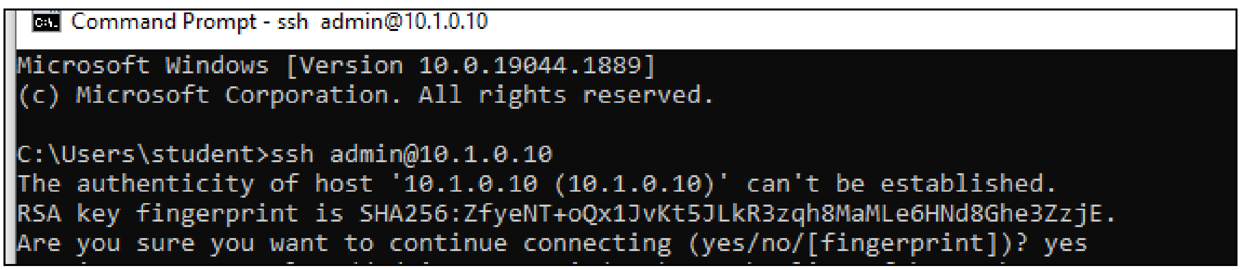
The ZTNA connection rules can also be configured on FortiClient EMS and pushed to FortiClient.

Test the Connection for Users

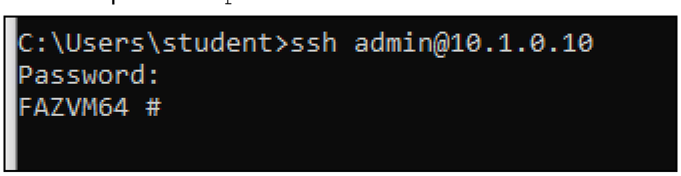
Now that you configured FortiGate and FortiClient, you will test the TCP proxy connection.

To test remote access to the TCP forwarding access proxy for SSH to FortiAnalyzer

1. Continuing on the Remote VM, open a command prompt.
2. Enter `ssh admin@10.1.0.10`.
3. If you are prompted to verify the RSA key fingerprint, type `yes` to continue connecting.



4. Enter the password `password`.



    You are connected to FortiAnalyzer using the SSH tcp-forwarding proxy.

5. Close the command prompt.

To test remote access to the TCP forwarding access proxy for RDP to the HR VM

1. Continuing on the Remote VM, in the lower-left corner, right-click the **Windows** icon, click **Run**, type `mstsc`, and then click **OK** to open the **Remote Desktop Connection** application.
2. In the **Computer** field, type `10.1.60.2`.

DO NOT REPRINT
© FORTINET

3. Log in with the username `ftnt.lab\hr` and password `Password1!`.
4. Click **Yes**.

   You are connected to the HR VM using the RDP tcp-forwarding proxy.

5. Disconnect the RDP session to the HR VM.

DO NOT REPRINT
© FORTINET

Exercise 6: Configuring Basic ZTNA IP/MAC Filtering

In this exercise, you will create and test a firewall policy using ZTNA IP/MAC filtering.

Configure a ZTNA IP/MAC Filtering Firewall Policy

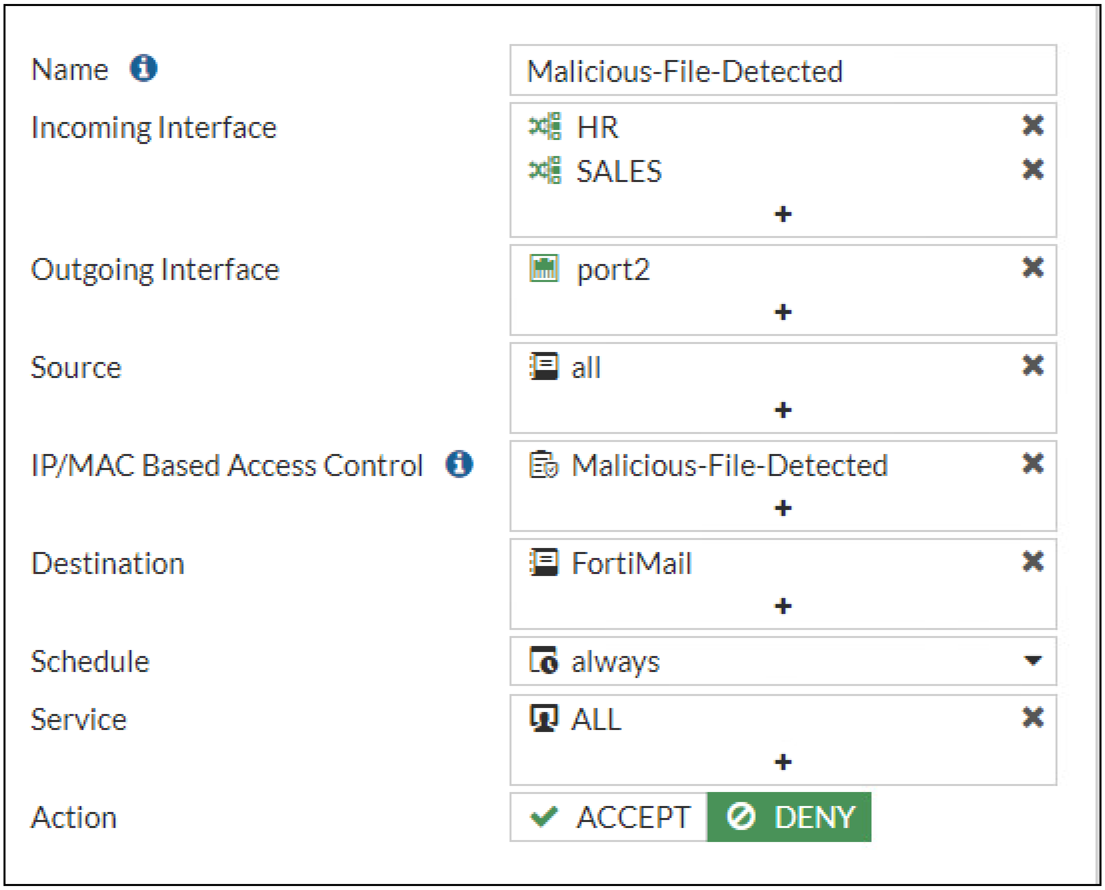
You will configure ZTNA IP/MAC filtering on FortiGate. ZTNA IP/MAC filtering is applied to regular firewall policies and used to provide access within the internal segment.

To create a new firewall policy with IP/ MAC filtering

1. On the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **ISFW** login page bookmark.
2. Log in to the ISFW GUI with the username `admin` and password `password`.
3. Click **Policy & Objects** > **Firewall Policy**, and then click **Create New** to create a new firewall policy.
4. In the **New Policy** window, configure the following settings:

Field	Value
Name	Malicious-File-Detected
Incoming Interface	HR Sales
Outgoing Interface	port2
Source	all
IP/MAC Based Access Control	Malicious-File-Detected
Destination	FortiMail
Service	ALL
Action	Deny

DO NOT REPRINT
© FORTINET



5. Click **OK** to add a new firewall policy.
6. Move the **Malicious-Filed-Detected** policy above the **Allow_DC_Restricted** policy.

Test Endpoint Access Using the IP/MAC Filtering Firewall Policy

You will test endpoint access control with a ZTNA tag.

To test endpoint access on the corporate network using the IP/MAC filtering ZTNA policy

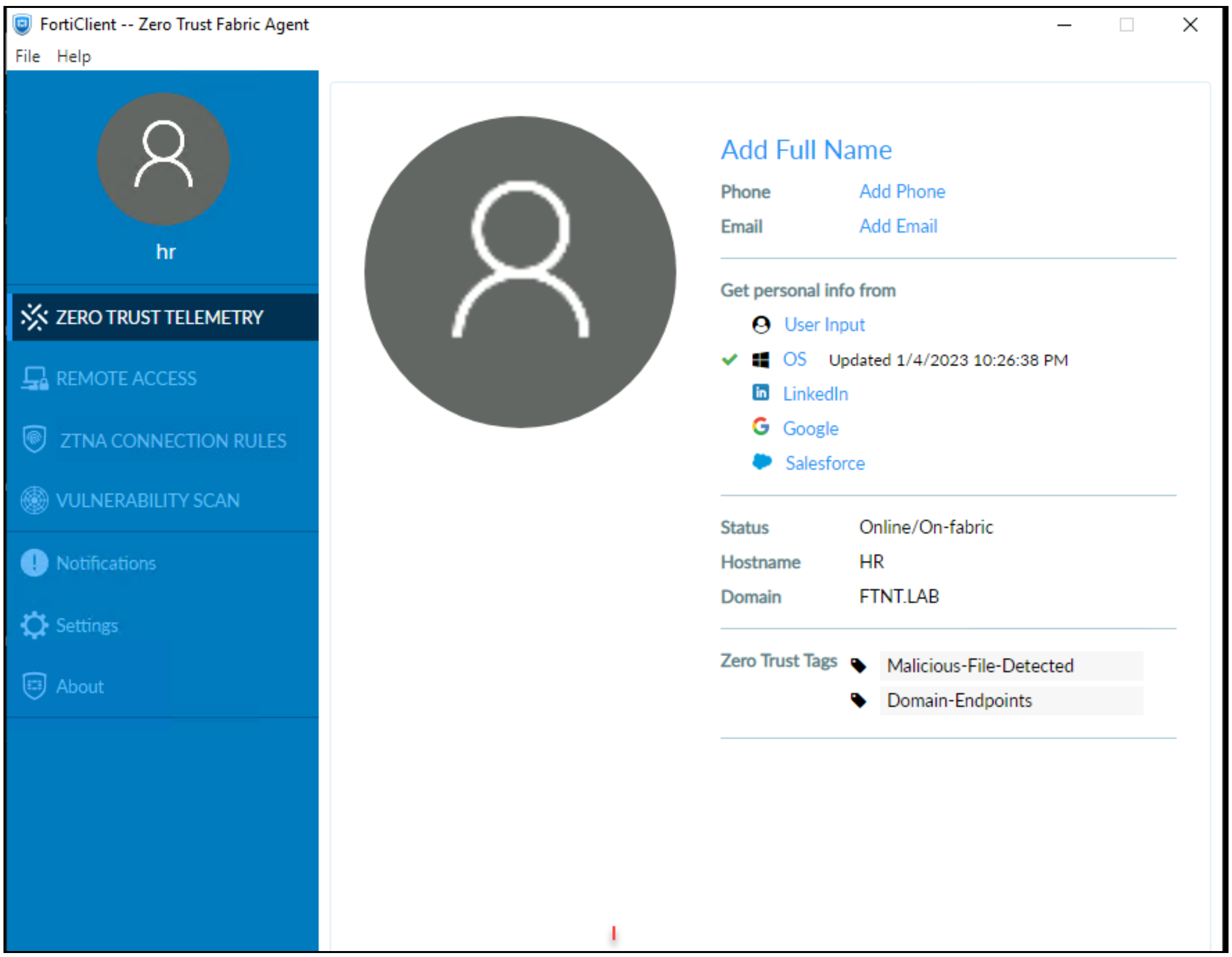
1. On HR VM, open a command prompt, and then enter `ping fml.ftnt.lab`.
   The ping should be allowed.

DO NOT REPRINT
© FORTINET


```
C:\Users\HR>ping fml.ftnt.lab

Pinging fml.ftnt.lab [10.1.0.60] with 32 bytes of data:
Reply from 10.1.0.60: bytes=32 time=2ms TTL=62
Reply from 10.1.0.60: bytes=32 time=2ms TTL=62
Reply from 10.1.0.60: bytes=32 time=2ms TTL=62
Reply from 10.1.0.60: bytes=32 time=2ms TTL=62

Ping statistics for 10.1.0.60:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

2. Open Notepad, and then create a file with dummy text.
3. Save the file in the **Documents** folder for the **student** user: `C:\Users\student\Documents\virus.txt`.
4. Click **Continue**on the permission access window.
5. Open the FortiClient console, and then click the avatar to view the detected tags.

   It may take a minute to see the updated tags.



6. Return to the command prompt, and then enter `ping fml.ftnt.lab`.

   This time, the ping should be stopped because the endpoint is detected with a malicious file detection tag.

DO NOT REPRINT
© FORTINET


```
C:\Users\HR>ping fml.ftnt.lab

Pinging fml.ftnt.lab [10.1.0.60] with 32 bytes of data:
Request timed out.
Request timed out.
```

If pings are still allowed, after the tags have been updated on FortiClient, restart the ZTNA process on ISFW FortiGate.

1. On the FortiClient EMS VM, open PuTTY, and then connect over SSH to the ISFW saved session.
2. Log in with the username `admin` and password `password`.
3. Enter the following command to restart the process:

```
diagnose test application fcnacd 99
```

7. On the HR VM, delete the `C:\Users\student\Documents\virus.txt` file.

DO NOT REPRINT
© FORTINET

Lab 5: Secure Access With Endpoint Posture and Compliance Checks

In this lab, you will configure and test endpoint compliance using FortiNAC. You will also use FortiClient EMS zero-trust tags for compliance checks to allow access to internal resources.

Objectives

- Create endpoint compliance configuration for different device types
- Test endpoint compliance for managed corporate devices
- Test endpoint compliance for guest and BYOD devices
- Integrate FortiNAC with FortiClient EMS and MDM with network access
- Configure FortiClient EMS ZTNA tagging rules to block access for remotely controlled machines
- Check compliance using FortiClient EMS zero-trust tags

Time to Complete

Estimated: 60 minutes

Prerequisites

Before you begin this lab, you must create a text file with the name `corporate.txt` on the HR VM. You will also enable port enforcement back for SALES VM.

1. On the HR VM, open Notepad as Administrator, and then create a file with dummy text.
2. Save the file in the `C:\Program Files\corporate.txt` directory.
3. On the FortiNAC GUI, click **Network** > **Inventory**, expand **Firewalls** > **ISFW.ftnt.lab**, and then click **S108DV0JA4QI3V78**.
4. Right-click **port7**, and then click **Port Properties**.
5. Click **Group Membership**.
6. In the **Port Group Membership** window, select the checkboxes for **Forced Authentication**,**Forced Registration**,**Forced Remediation**,**Reset Forced Registration**, and **Role Based Access**.
7. Click **OK**.
8. Click **OK**.

DO NOT REPRINT
© FORTINET

Exercise 1: Configuring Endpoint Compliance

In this exercise, you will configure endpoint compliance on FortiNAC for different device types.

Configure User and Host Profiles

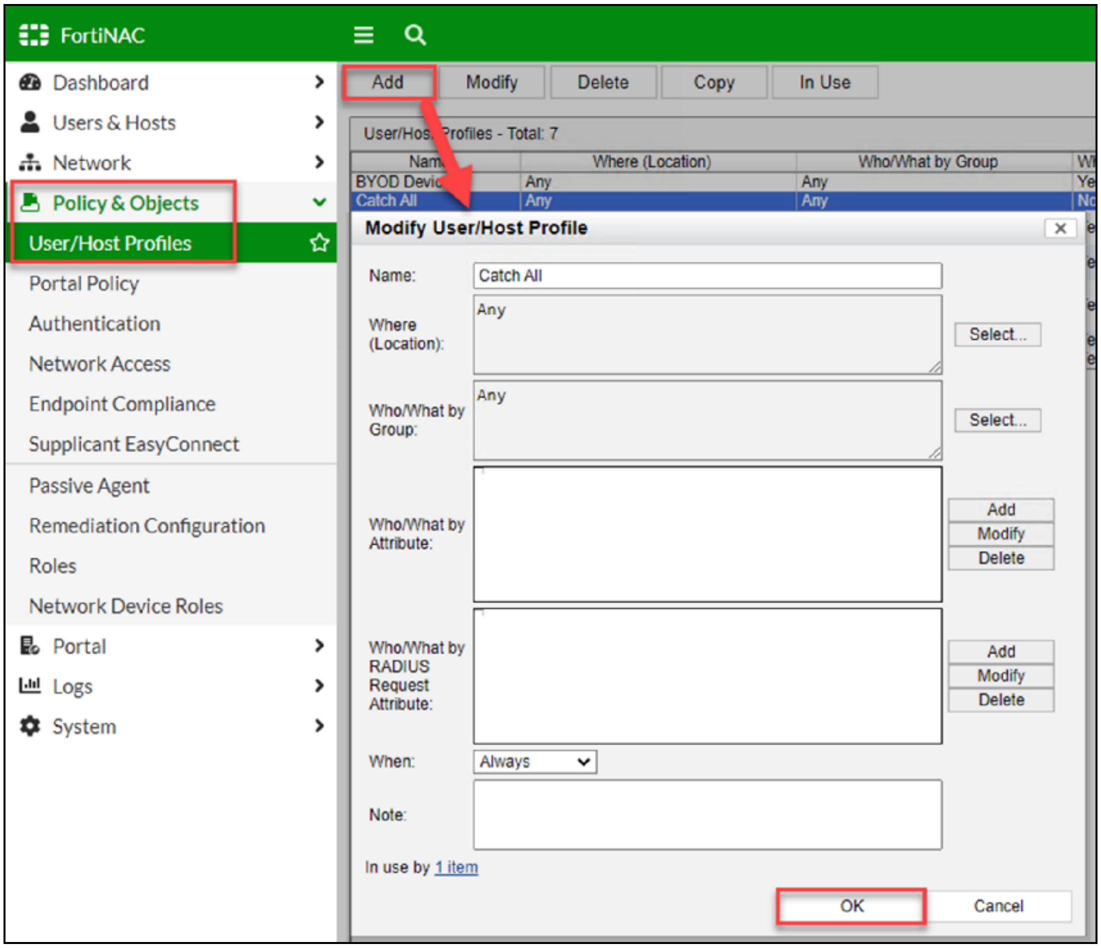
You will create user and host profiles that focus on the type of users identified on the registration page.

To configure user and host profiles

1. On the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **FortiNAC** login page bookmark.
2. Log in to the FortiNAC GUI with the username `admin` and password `Password1!`.
3. Click **Policy & Objects** > **User/Host Profiles**, click **Add**, configure the following settings, and then click **OK** to create a new profile to identify all devices:

Field	Value
Name	Catch All
Where (Location)	Any
Who/What by Group	Any
When	Always

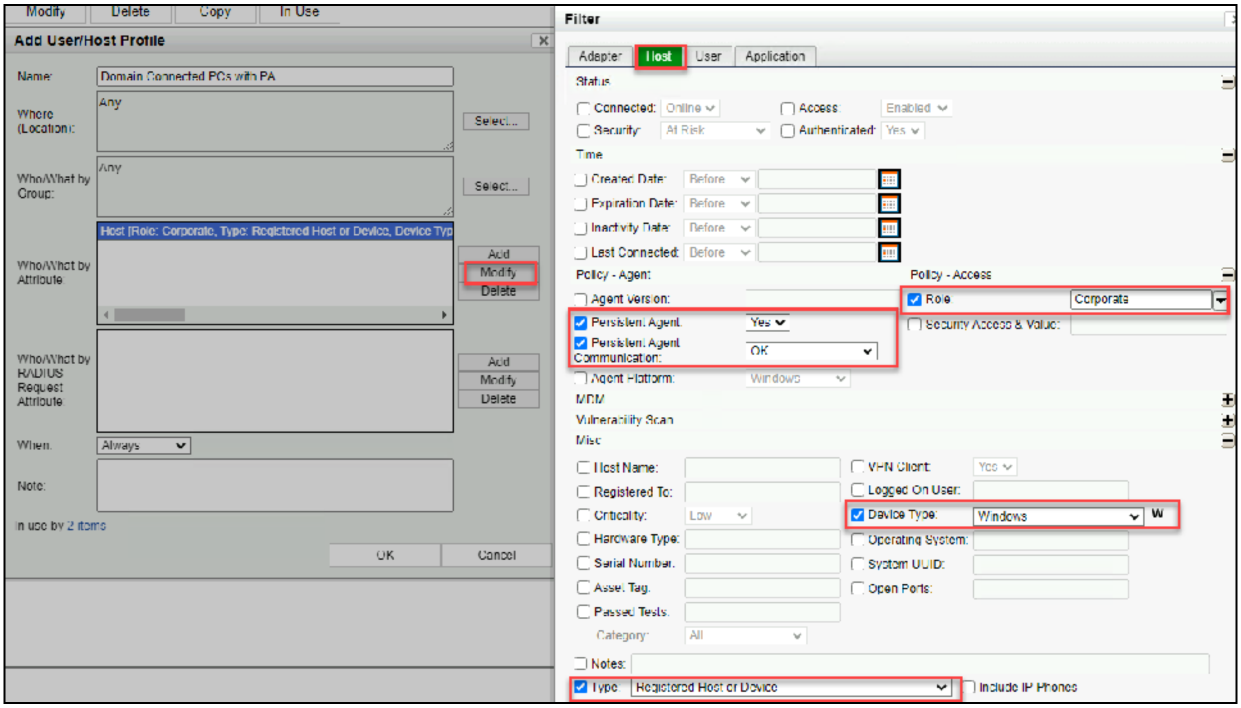
DO NOT REPRINT
© FORTINET



4. Click **Policy & Objects** > **User/Host Profiles**, select the **Domain Connected PCs** profile, and then click **Copy** to create a new profile named `Domain Connected PCs with PA` to identify corporate devices with a persistent agent.
5. In the **Who/What by Attribute** field, click **Modify**, click the **Host** tab, configure the following values, and then click **OK**:

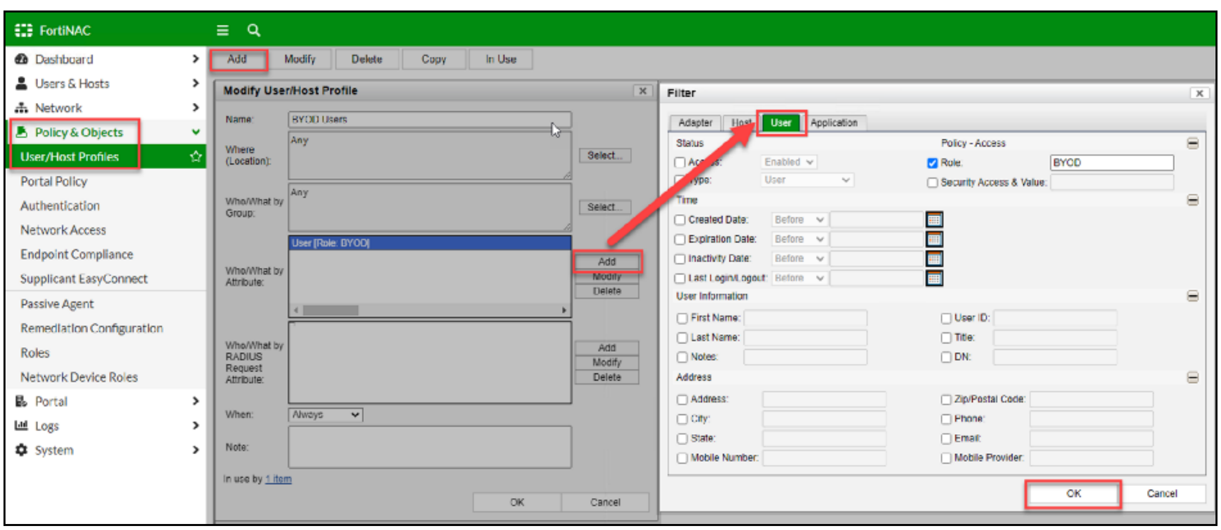
Field	Value
Role	Select the checkbox, and then select **Corporate**.
Persistent Agent	Select the checkbox, and then select **Yes**.
Persistent Agent Communication	Select the checkbox, and then select **OK**.
Device Type	Select the checkbox, and then select **Windows**.
Type	Select the checkbox, and then select **Registered Host or Device**.

DO NOT REPRINT
© FORTINET



6. Click **OK**.
7. Click **Policy & Objects** > **User/Host Profiles**, and then click **Add** to create a new profile named `BYOD Users` to identify BYOD users.
8. In the **Who/What by attribute** field, click **Add**, click the **User** tab to configure the following values, and then click **OK**:

Field	Value
Role	Select the checkbox, and then type `BYOD`.

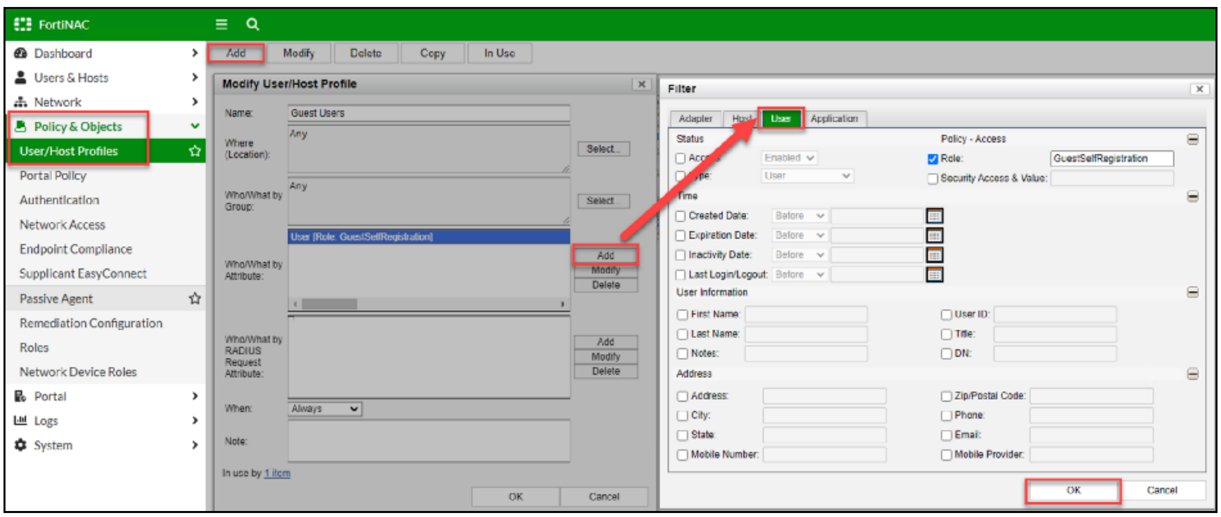


DO NOT REPRINT
© FORTINET

Compliance scans typically occur before registering the device. Therefore, you are creating new user/host profiles that focus on the type of users that are identified on the registration page. This allows you to create role-based compliance scans for rogue/unregistered devices.

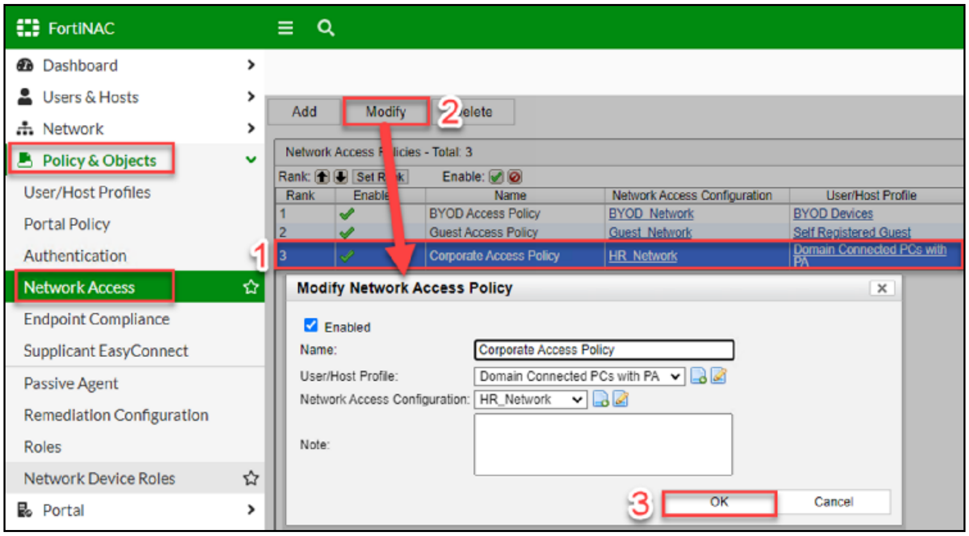
9. Click **OK**.
10. Click **Policy & Objects** > **User/Host Profiles**, and then click **Add** to create a new profile named `Guest Users` to identify guest users.
11. In the **Who/What by attribute** field, click **Add**, click the **User** tab to configure the following values, and then click **OK**:

Field	Value
Role	Select the checkbox, and then type `GuestSelfRegistration`.



12. Click **OK**.
13. Click **Policy & Objects** > **Network Access**, select the **Corporate Access Policy** profile, click **Modify**, change the **User/Host Profile** field to the new **Domain Connected PCs with PA** profile, as shown in the following image, and then click **OK**:

DO NOT REPRINT
© FORTINET

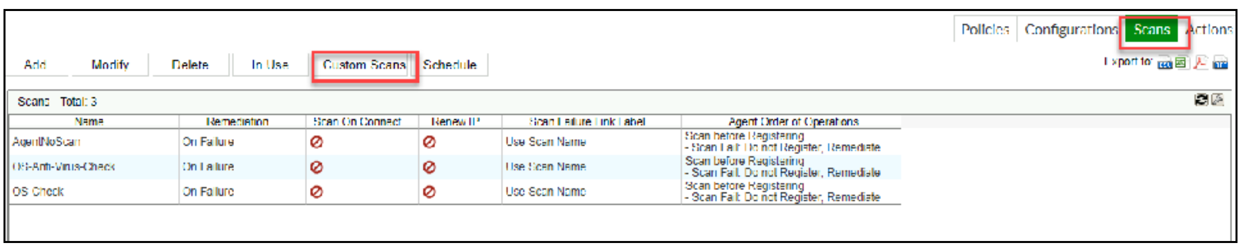


Configure Compliance Scans

You will configure compliance scans on FortiNAC.

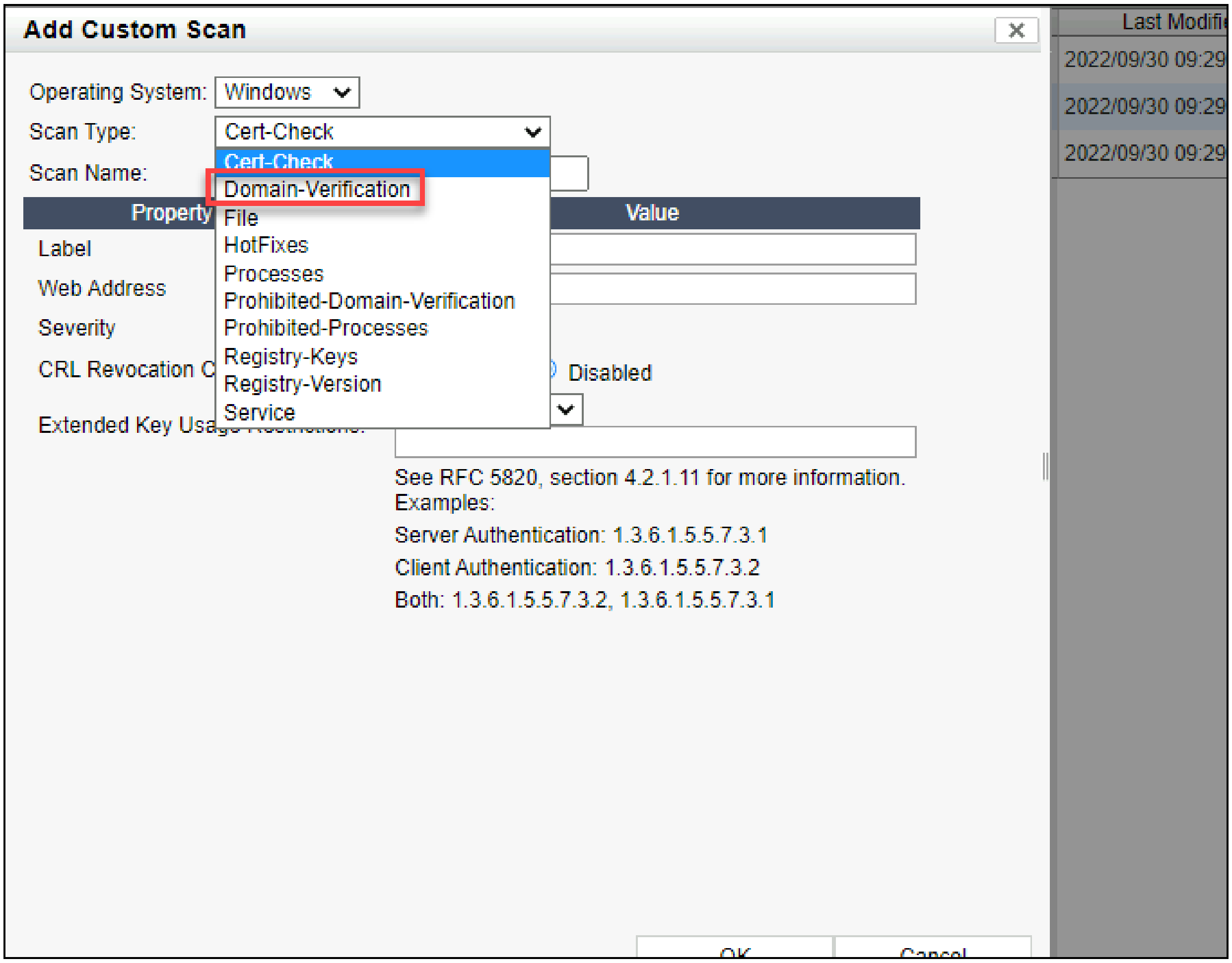
To configure compliance scans

1. Continuing on the FortiNAC GUI, click **Policy & Objects** > **Endpoint Compliance**, select **Scans**, and then click **Custom Scans**.



2. Click **Add**, and then in the **Scan Type** field, select **Domain-Verification.**

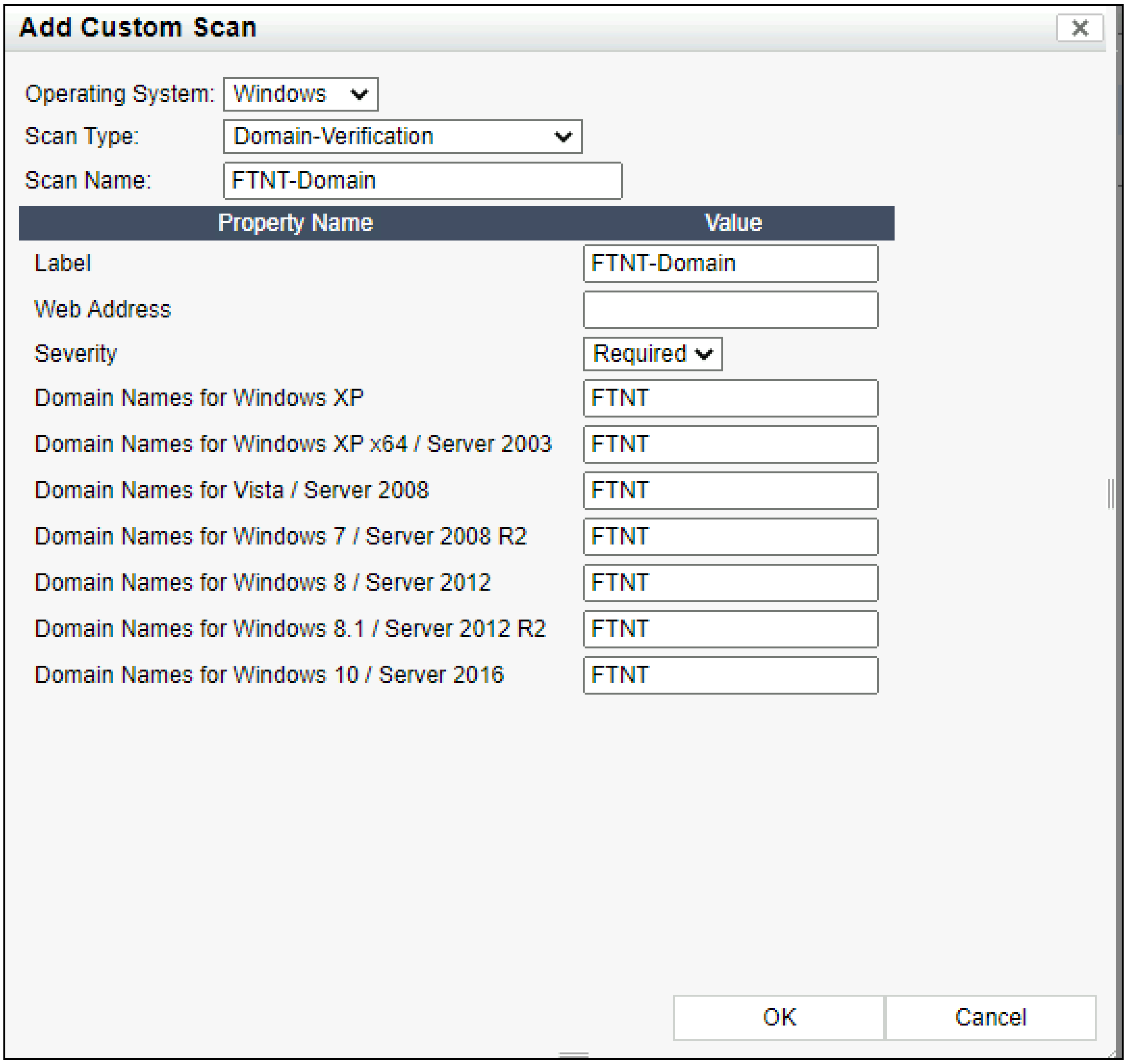
DO NOT REPRINT
© FORTINET



3. Configure the following settings, and then click **OK**:

Field	Value
Operating System	Windows
Scan Type	Domain-Verification
Scan Name	FTNT- Domain
Label	FTNT- Domain
Severity	Required
Domain Names for each OS	FTNT

DO NOT REPRINT
© FORTINET



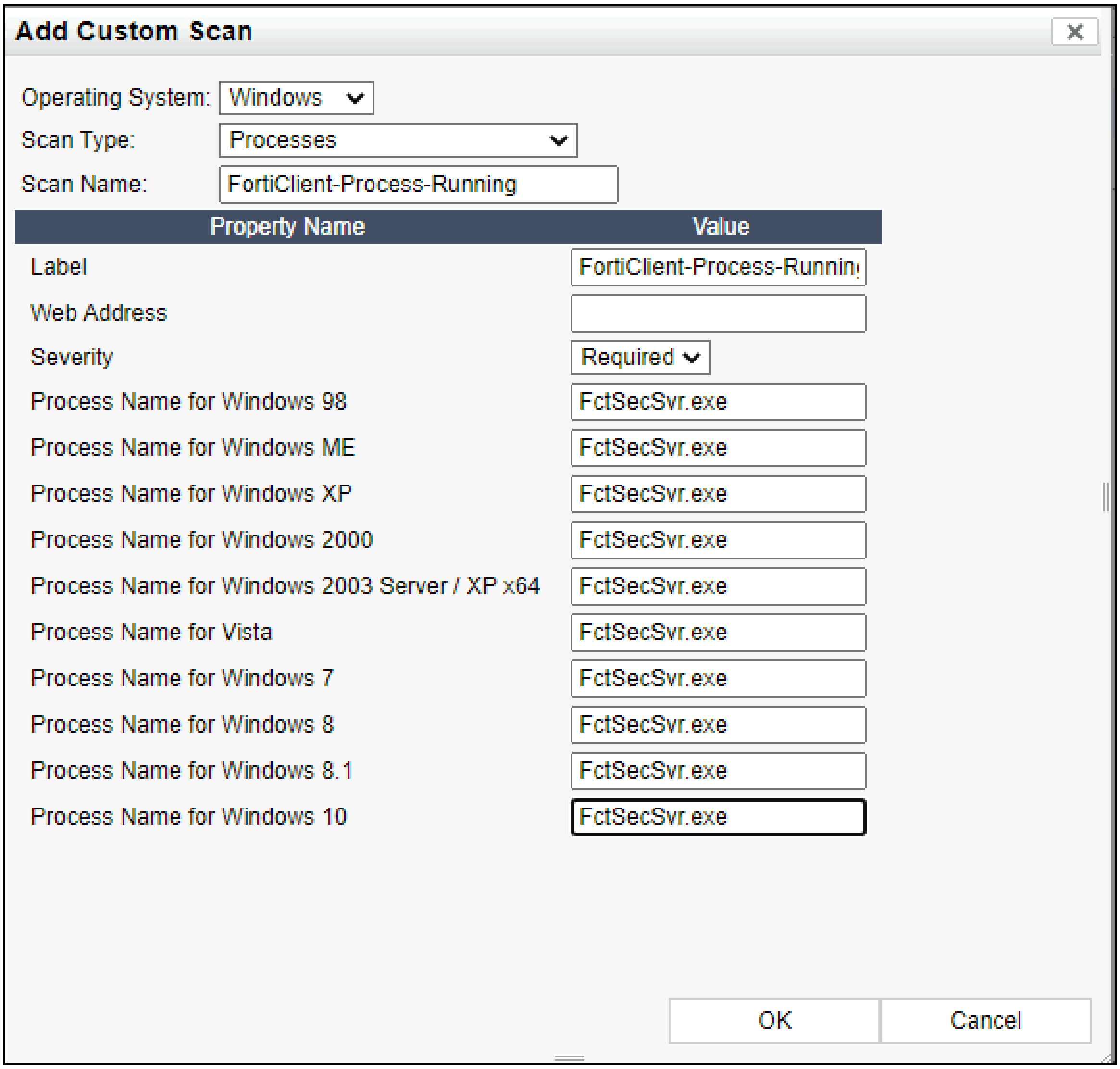
FortiNAC expects NETBIOS domain representation, not the actual domain name.

4. Click **Add**, and then in the **Scan Type** field, select **Processes**.
5. Configure the following settings, and then click **OK**:

Field	Value
Operating System	Windows
Scan Type	Processes
Scan Name	FortiClient-Process-Running

DO NOT REPRINT
© FORTINET

Field	Value
Label	FortiClient-Process-Running
Severity	Required
Domain Names for each OS	FctSecSvr.exe

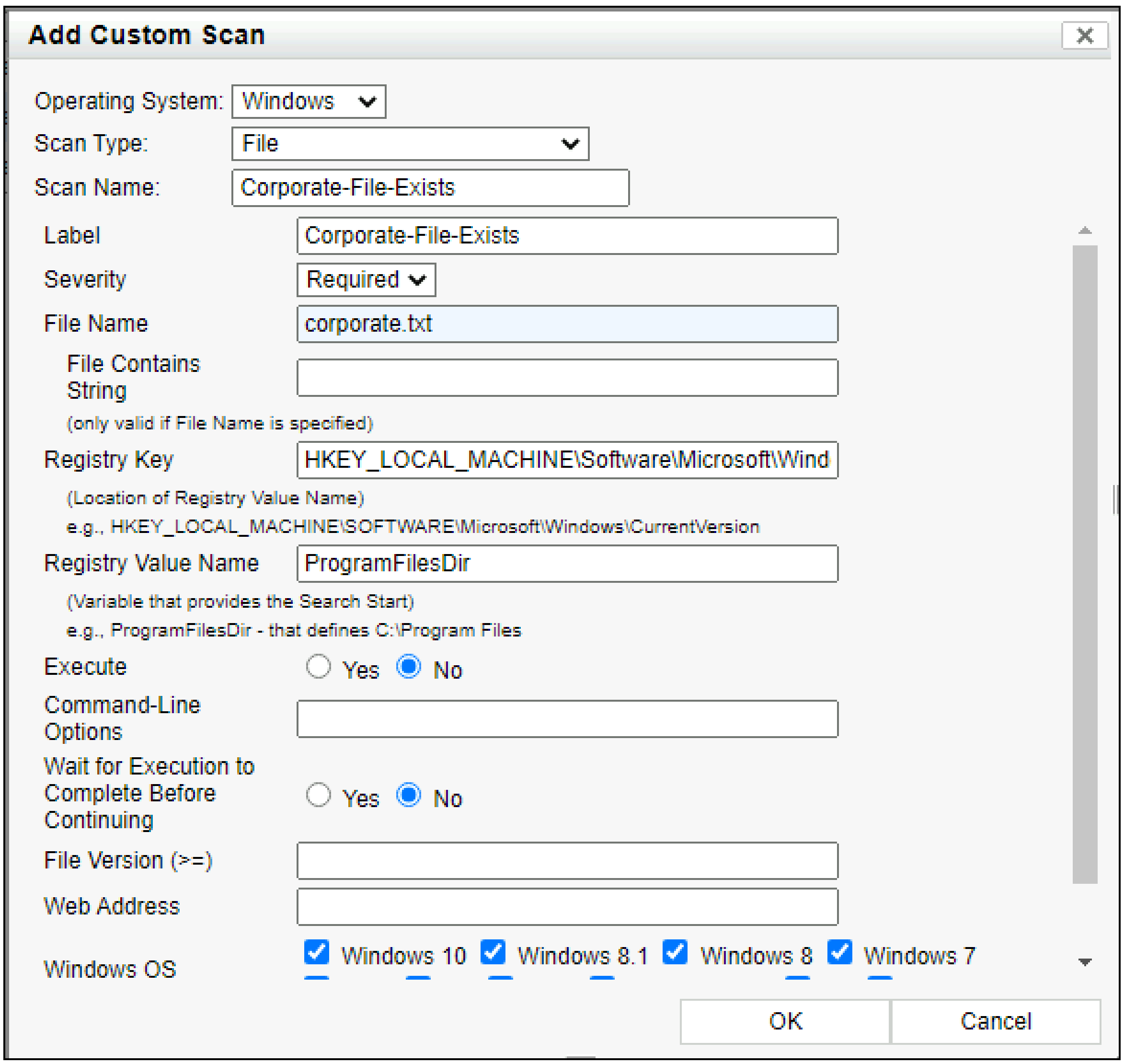


FortiNAC can verify the existence of AV software with the normal scan feature. However, you are using the custom scan to verify that the AV is active and running.

6. Click **Add**, and then in the **Scan Type** field, select **File**.
7. Configure the following settings, and then click **OK**:

DO NOT REPRINT
© FORTINET

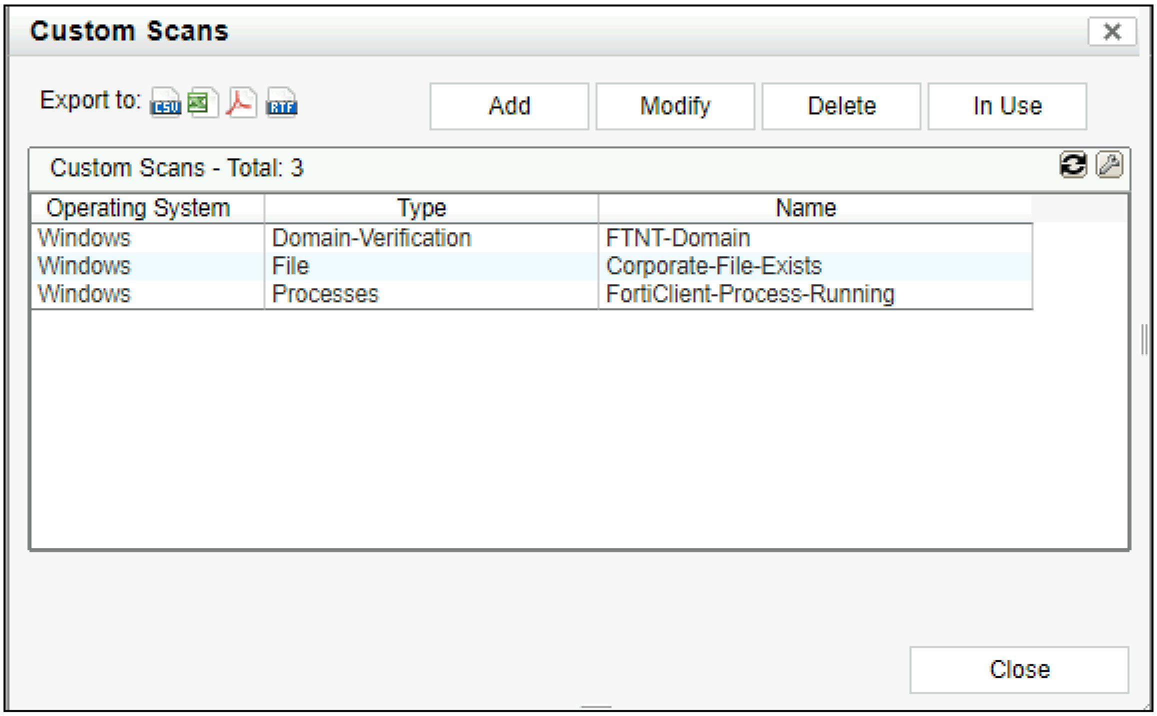
Field	Value
Operating System	Windows
Scan Type	File
Scan Name	Corporate-File-Exists
Label	Corporate-File-Exists
Severity	Required
File Name	corporate.txt
Registry Key	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion
Registry Value Name	ProgramFilesDir



DO NOT REPRINT
© FORTINET

FortiNAC looks for the file in the directory specified in the **Registry Value Name** field.

The three custom scans that you created should appear in the **Custom Scans** section, as shown in the following image:



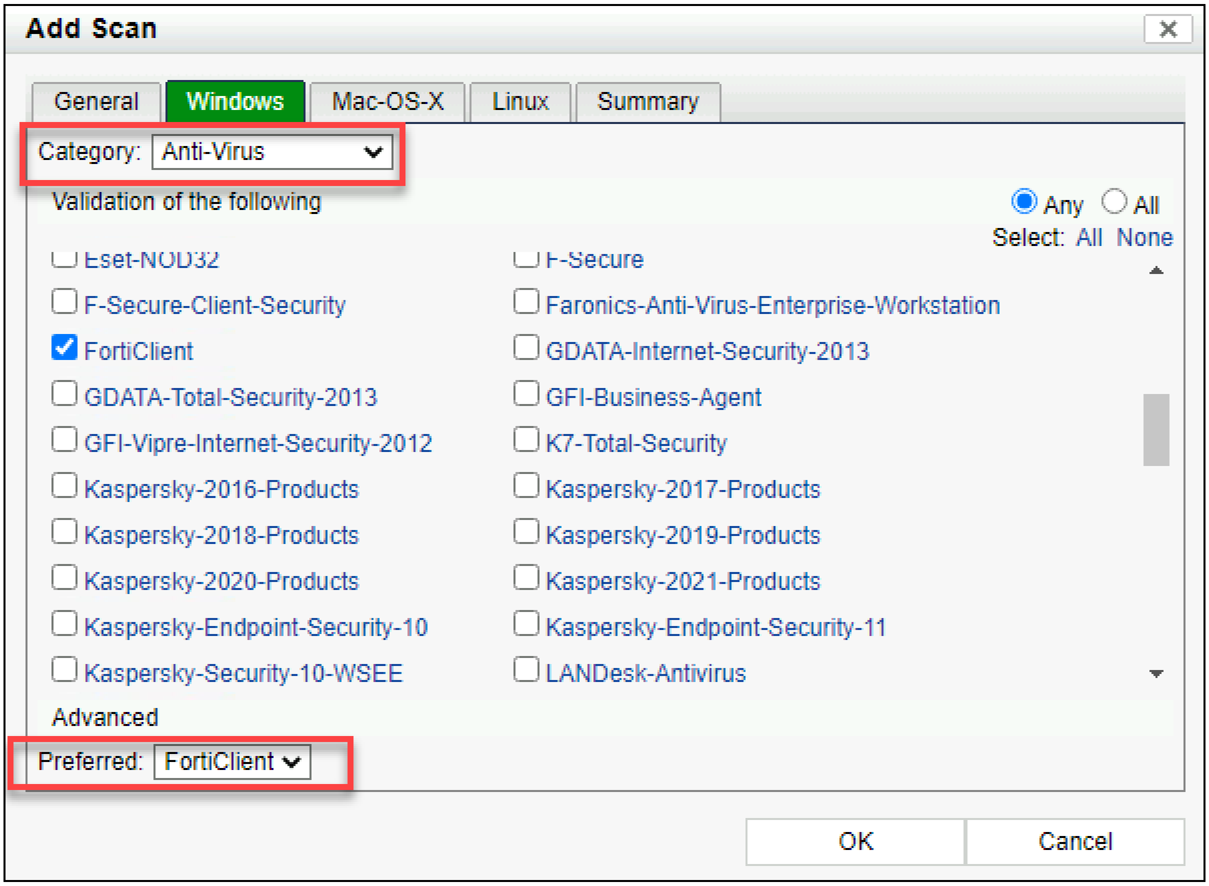
8. Click **Close**.
9. Click **Add**, and then configure the following settings to create a new scan:

Field	Value
Scan Name	Corporate-Scan
Scan On Connect (Persistent Agent Only)	Select the checkbox.

10. Click the **Windows** tab, in the **Category** field, select **Anti-Virus**, and then configure the following settings:

Field	Value
FortiClient	Select the checkbox.
Preferred	FortiClient

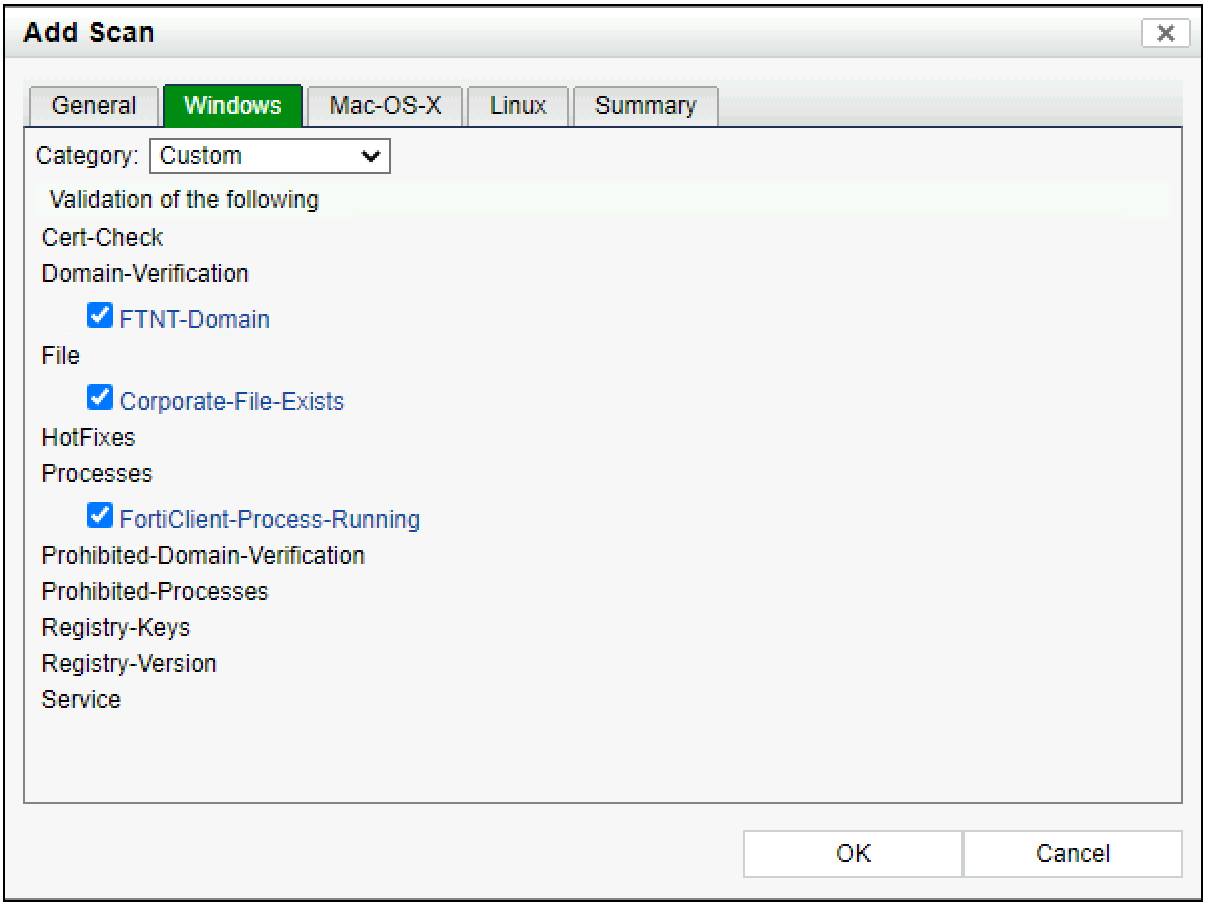
DO NOT REPRINT
© FORTINET



11. In the **Category** field, select **Custom**, and then configure the following settings:

Field	Value
FTNT-Domain	Select the checkbox.
Corporate-File-Exists	Select the checkbox.
FortiClient-Process-Running	Select the checkbox.

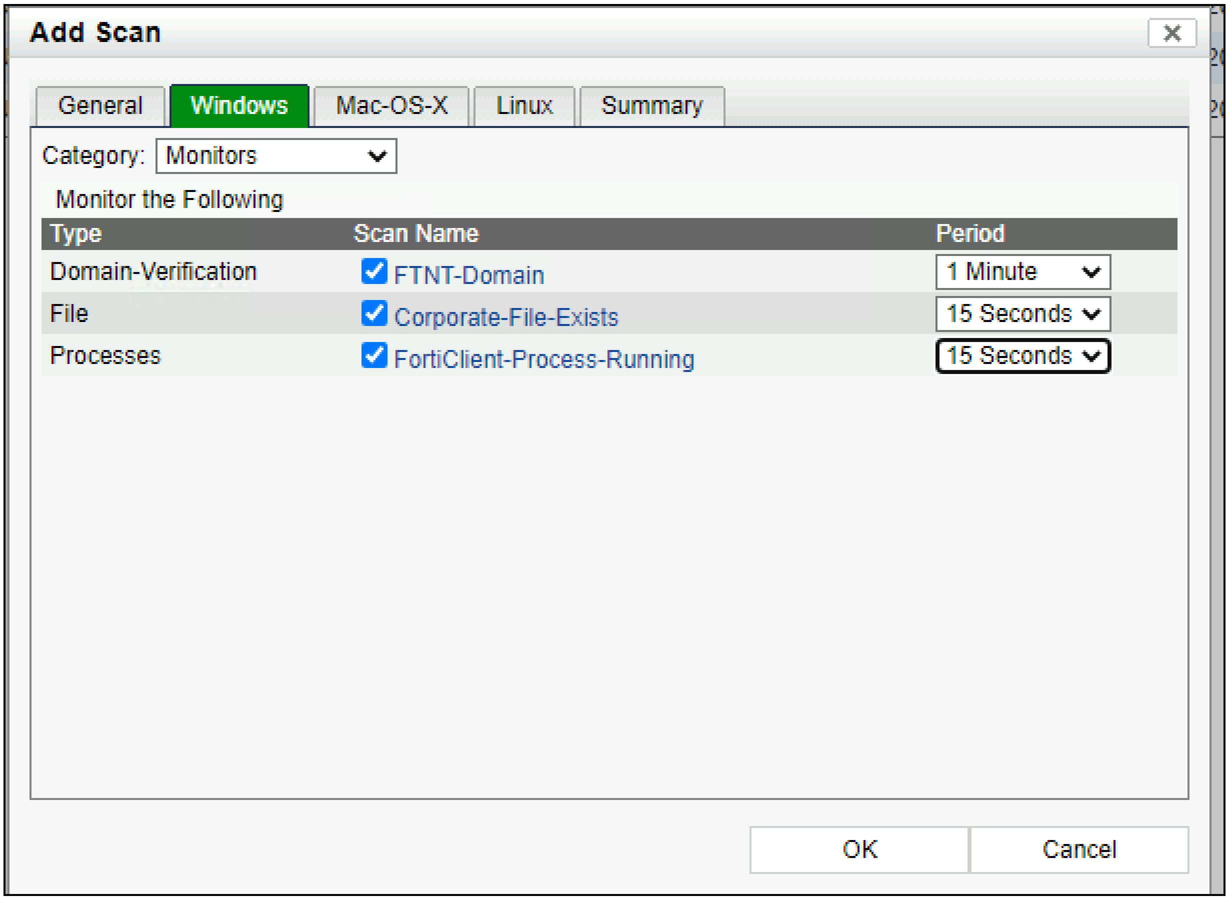
DO NOT REPRINT
© FORTINET



12. In the **Category** field, select **Monitors**, configure the following settings, and then click **OK**:

Field	Value
FTNT-Domain	Select the checkbox, and then in the **Period** column, select **1 Minute**.
Corporate-File-Exists	Select the checkbox, and then in the **Period** column, select **15 Seconds.**
FortiClient-Process-Running	Select the checkbox, and then in the **Period** column, select **15 Seconds.**

DO NOT REPRINT
© FORTINET

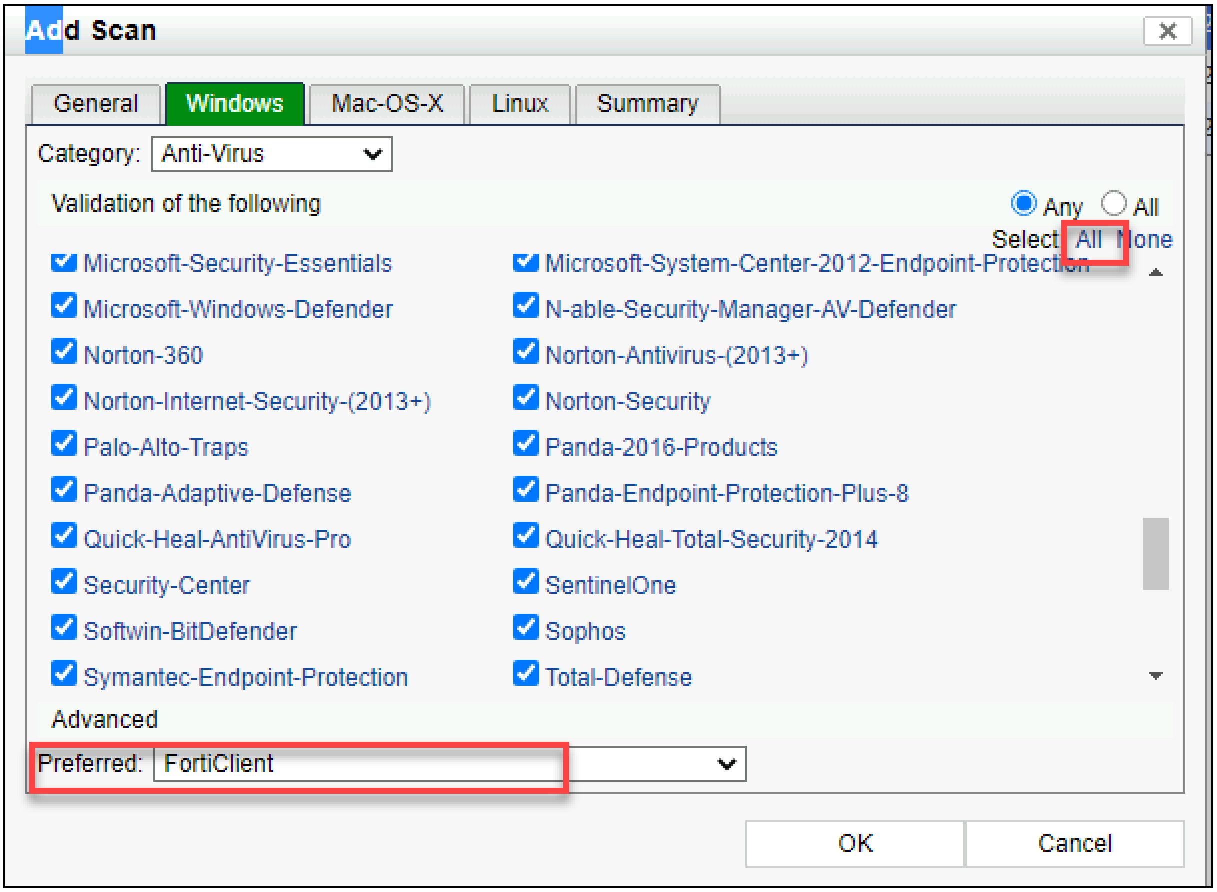


13. Click **Add**, and then configure the following settings to create a new scan:

Field	Value
Scan Name	BYOD-AV-Scan
Renew IP (Supported Dissolvable Agents Only)	Select the checkbox.

14. Click the **Windows** tab, in the **Category** field, select **Anti-Virus**, in the **Select** field, click **All** to check if any of the AV software is installed, in the **Preferred** field, select **FortiClient**, and then click **OK**.

DO NOT REPRINT
© FORTINET



15. Click **Add**, and then configure the following settings to create a new scan ,and then click **OK**:

Field	Value
Scan Name	Guest-Inv-Only-Scan
Renew IP (Supported Dissolvable Agents Only)	Select the checkbox.

16. Click **Add**, and then configure the following settings to create a new scan:

Field	Value
Scan Name	Catch-All-Device-Scan
Renew IP (Supported Dissolvable Agents Only)	Select the checkbox.

17. Click the **Windows** tab, in the **Category** field, select **Anti-Virus**, in the **Select** field, click **All** to check if any of the AV software is installed, in the **Preferred** field, select **FortiClient**, and then click **OK**.

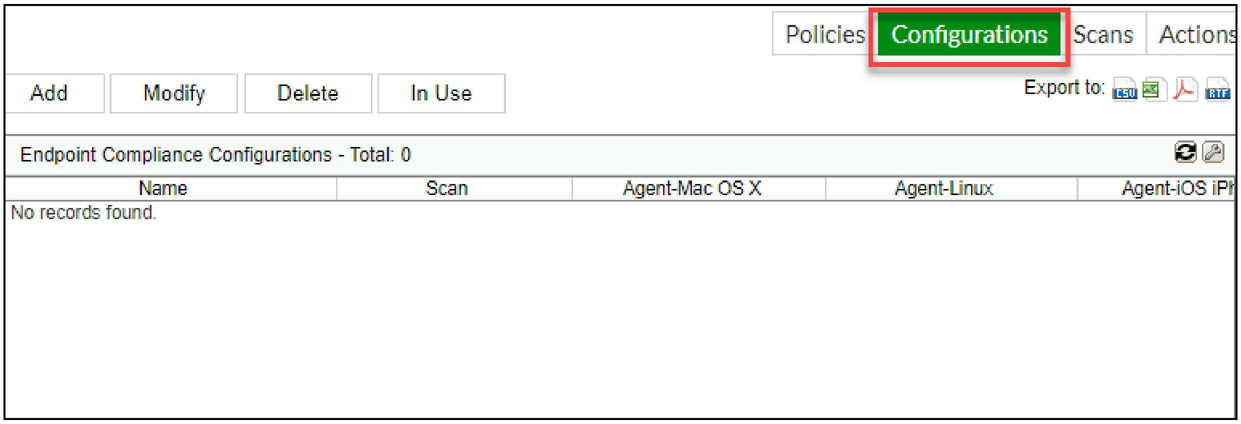
DO NOT REPRINT
© FORTINET

Configure Endpoint Compliance

You will configure endpoint compliance on FortiNAC.

To configure endpoint compliance

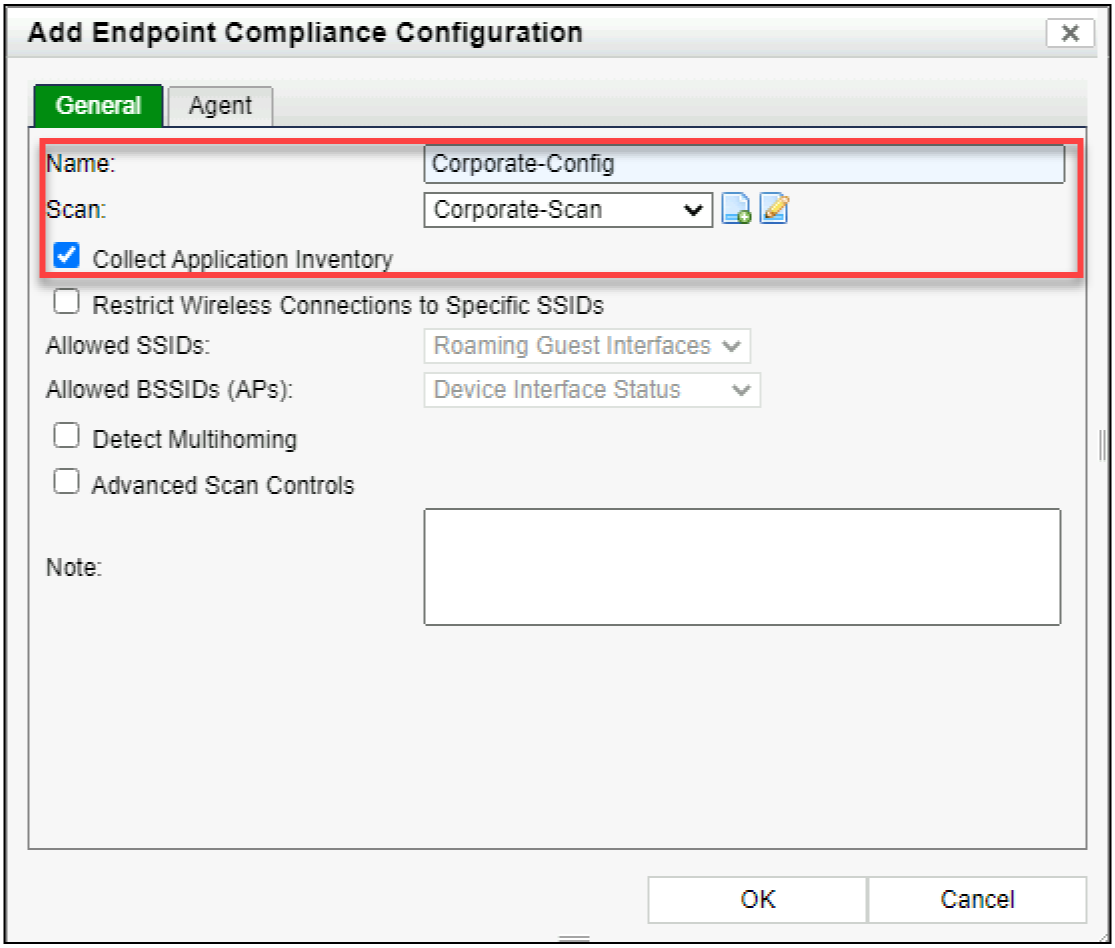
1. Continuing on the FortiNAC GUI, click **Policy & Objects** > **Endpoint Compliance**, and then select **Configurations**.



2. Click **Add**, and then configure the following settings to create a corporate compliance configuration (leave all other settings at the default values):

Field	Value
Name	Corporate-Config
Scan	Corporate-Scan
Collect Application Inventory	Select the checkbox.

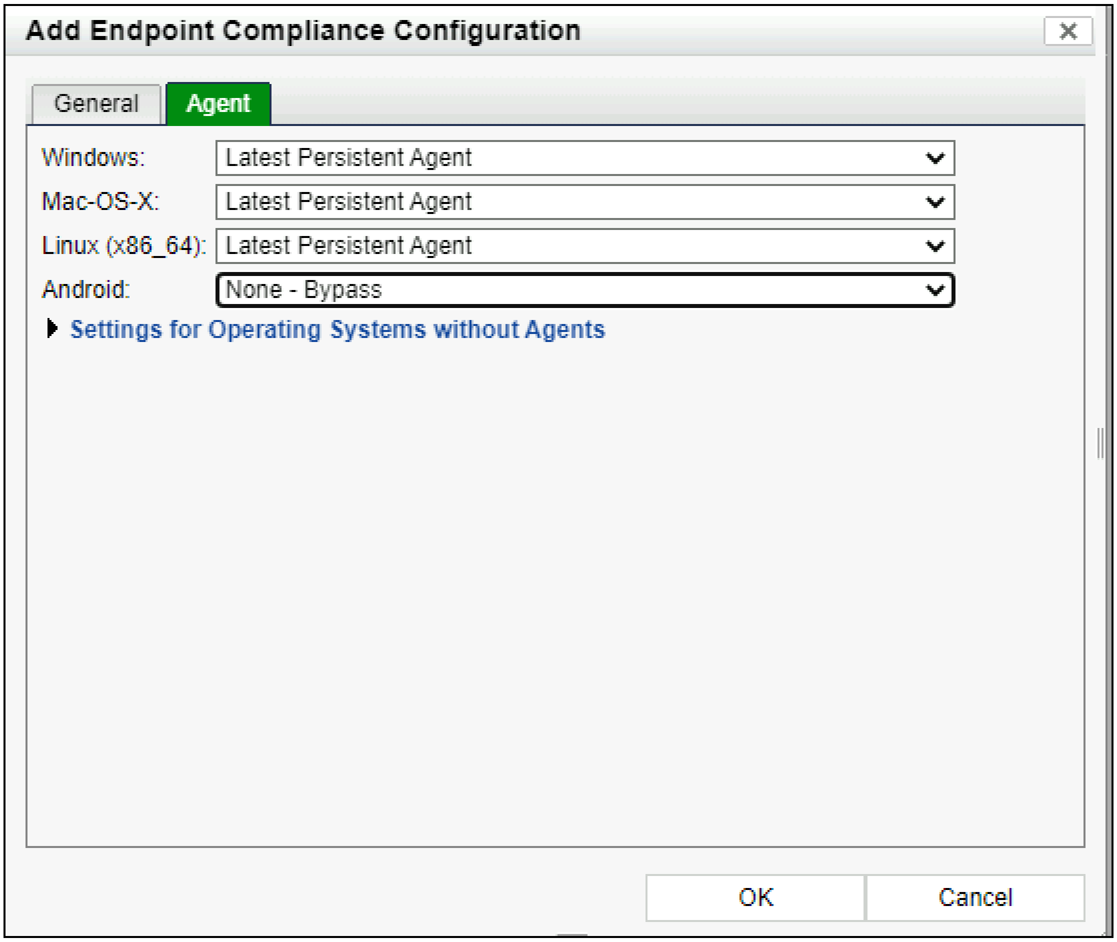
DO NOT REPRINT
© FORTINET



3. Click the **Agent** tab, configure the following values, and then click **OK**:

Field	Value
Windows	Latest Persistent Agent
Mac-OS-X	Latest Persistent Agent
Linux (x86_64)	Latest Persistent Agent
Android	None-Bypass

DO NOT REPRINT
© FORTINET



4. Click **Add**, and then configure the following settings to create a BYOD device compliance configuration (leave all other settings at the default values):

Field	Value
Name	BYOD-Config
Scan	BYOD-AV-Scan
Collect Application Inventory	Select the checkbox.

5. Click the **Agent** tab, configure the following settings, and then click **OK**:

Field	Value
Windows	Latest Dissolvable Agent
Mac-OS-X	Latest Dissolvable Agent
Linux (x86_64)	Latest Dissolvable Agent
Android	Latest Mobile Agent

DO NOT REPRINT
© FORTINET

6. Click **Add**, and then configure the following settings to create a guest compliance configuration (leave all other settings at the default values):

Field	Value
Name	Guest-DA-Inventory-Only
Scan	Guest-Inv-Only-Scan
Collect Application Inventory	Checked

7. Click the **Agent** tab, configure the following settings, and then click **OK**:

Field	Value
Windows	Latest Dissolvable Agent
Mac-OS-X	Latest Dissolvable Agent
Linux (x86_64)	Latest Dissolvable Agent
Android	Latest Mobile Agent

8. Click **Add**, and then configure the following settings to create a compliance configuration (leave all other settings at the default values):

Field	Value
Name	Catch-All-Config
Scan	Catch-All-Device-Scan
Collect Application Inventory	Select the checkbox.

9. Click the **Agent** tab, configure the following values, and then click **OK**:

Field	Value
Windows	Latest Dissolvable Agent
Mac-OS-X	Latest Dissolvable Agent
Linux (x86_64)	Latest Dissolvable Agent
Android	Latest Mobile Agent

Configure Endpoint Compliance Policies

You will configure endpoint compliance policies on FortiNAC.

DO NOT REPRINT
© FORTINET

To configure endpoint compliance policies

1. Continuing on the FortiNAC GUI, click **Policy & Objects** > **Endpoint Compliance**, and then click the **Policies** tab.
2. Click **Add**, configure the following settings to create a guest compliance policy, and then click **OK**:

Field	Value
Name	Guest-Compliance-DA
User/Host Profile	Guest Users
Endpoint Compliance Configuration	Guest-DA-Inventory-Only

3. Click **Add**, configure the following settings to create a BYOD compliance policy, and then click **OK**:

Field	Value
Name	BYOD-Compliance-DA
User/Host Profile	BYOD Users
Endpoint Compliance Configuration	BYOD-Config

4. Click **Add**, configure the following settings to create a corporate compliance policy, and then click **OK**:

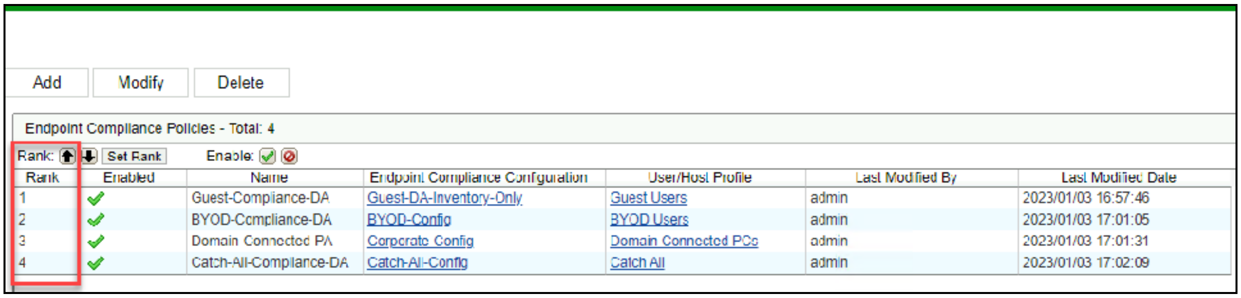
Field	Value
Name	Domain-Connected-PA
User/Host Profile	Domain Connected PCs
Endpoint Compliance Configuration	Corporate-Config

5. Click **Add**, configure the following settings to create a catch all compliance policy, and then click **OK**:

Field	Value
Name	Catch-All-Compliance-DA
User/Host Profile	Catch-All
Endpoint Compliance Configuration	Catch-All-Config

Policies should be ranked and appear as shown in the following image:

DO NOT REPRINT
© FORTINET



Rank	Enabled	Name	Endpoint Compliance Configuration	User/Host Profile	Last Modified By	Last Modified Date
1	✓	Guest-Compliance-DA	Guest-DA-Inventory-Only	Guest Users	admin	2023/01/03 16:57:46
2	✓	BYOD-Compliance-DA	BYOD-Config	BYOD Users	admin	2023/01/03 17:01:05
3	✓	Domain Connected PA	Corporate Config	Domain Connected PCs	admin	2023/01/03 17:01:31
4	✓	Catch-All-Compliance-DA	Catch-All-Config	Catch All	admin	2023/01/03 17:02:09

DO NOT REPRINT
© FORTINET

Exercise 2: Testing Endpoint Compliance for Managed Corporate Devices

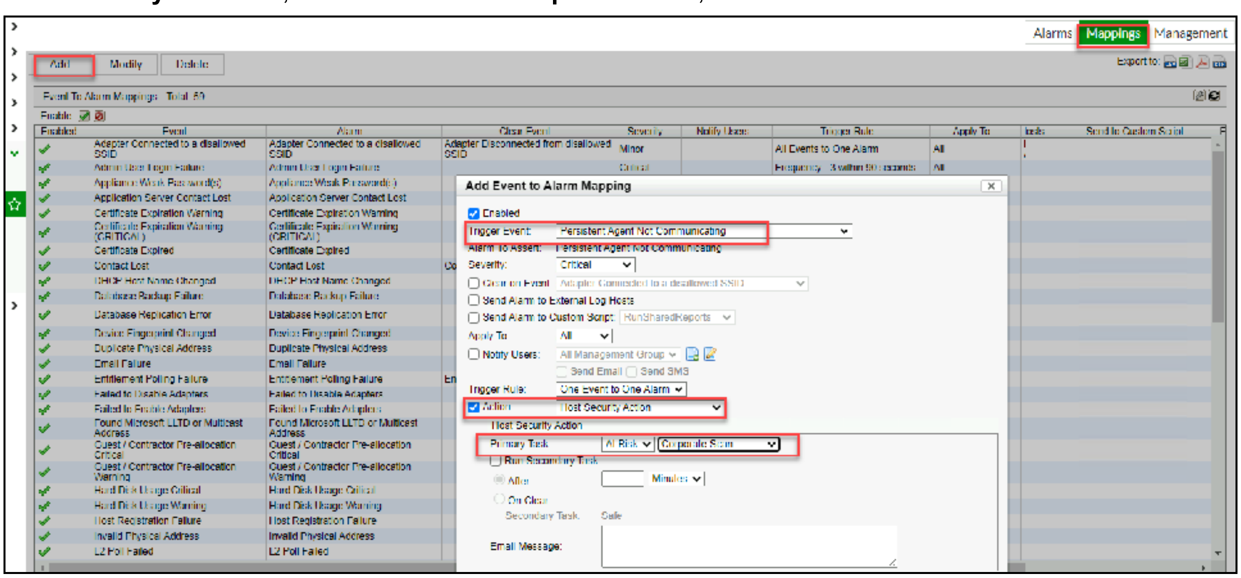
In this exercise, you will install a persistent agent on the HR VM and perform a compliance scan on the endpoint.

Install a Persistent Agent and Validate the Settings

You will install a FortiNAC persistent agent on the HR VM.

To install a persistent agent

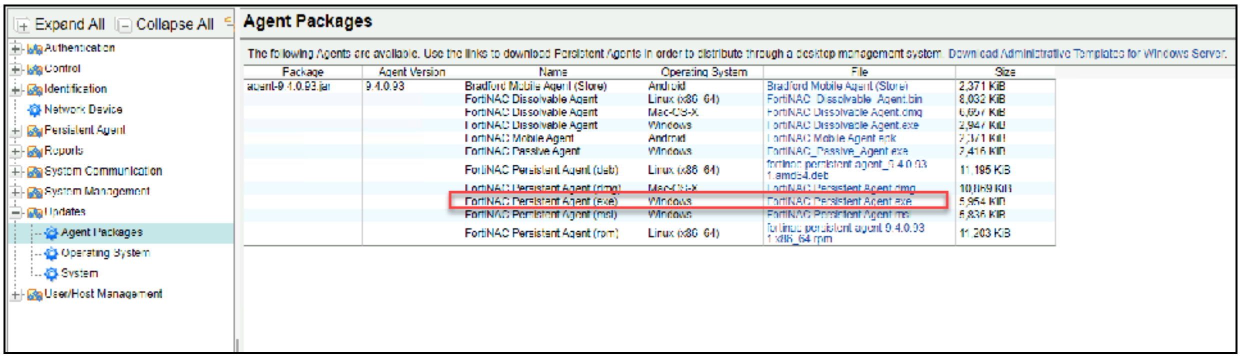
1. On the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **FortiNAC** login page bookmark.
2. Log in to the FortiNAC GUI with the username `admin` and password `Password1!`.
3. Click **System** > **Settings**.
4. Expand **Persistent Agent**, select **Credential Configuration**, and then ensure that the **Enable Registration** checkbox is not selected.
5. Click **Properties**, and in the **Primary Host Name** field type `fnac.ftnt.lab`.
6. Click **Save Settings**, and then Click **OK**.
7. Click **Status Notifications**, and then ensure that the **Provide a Log Off functionality from the tray icon for authenticated hosts** checkbox is not selected.
8. In the left menu, click **Logs** > **Events & Alarms**, click the **Mappings** tab, and then click **Add**.
9. In the **Trigger Event** field, select **Persistent Agent Not Communicating**, select the **Action** checkbox, and then select **Host Security Action**.
10. In the **Primary Task** field, select **At Risk** and **Corporate-Scan**, and then click **OK**.



DO NOT REPRINT
© FORTINET

You are using alarm mappings to handle malicious users who uninstall the persistent agent or tamper with service.

11. On the HR VM, open Google Chrome, and navigate to the FortiNAC GUI at `https://fnac.ftnt.lab:8443/`, and then log in with the username `admin` and password `Password1!`.
12. Click **System** > **Settings**, expand **Updates**, select **Agent Packages**, and then download the `FortiNAC Persistent Agent.exe` file.

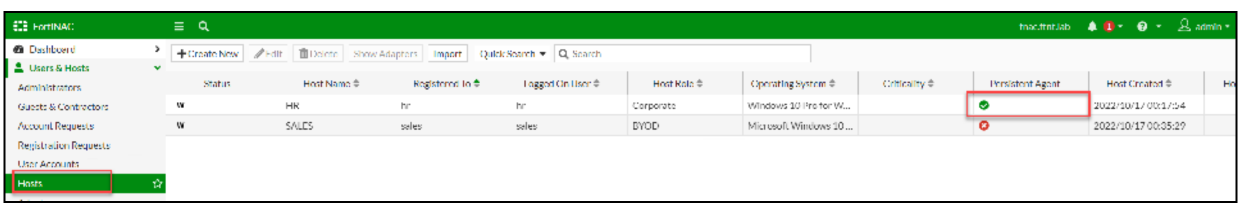


13. In the **Downloads** folder, double-click the file to install the persistent agent, and then follow the on-screen instructions.

    If you are prompted for administrator credentials on the HR VM, use the username `Administrator` and password `Password1!`.

14. Return to the FortiNAC GUI, and then confirm that you can now see persistent agent communication under **Users & Hosts** > **Hosts**.

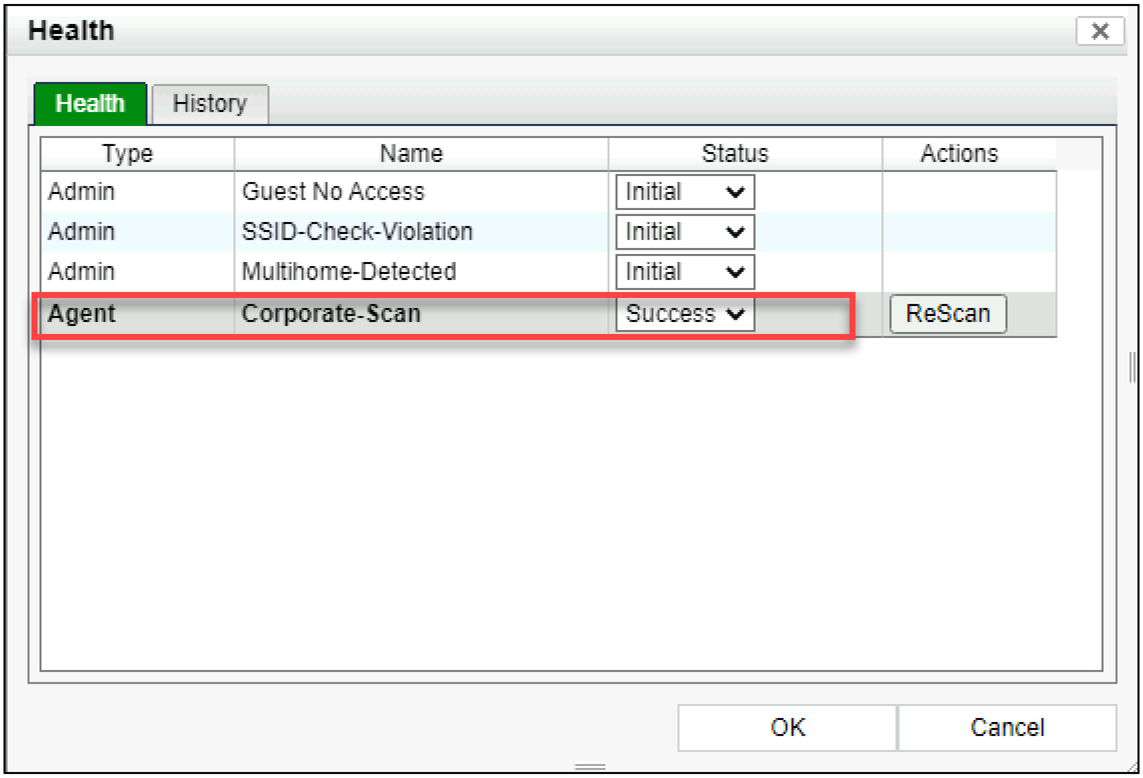
    You should see a green check mark in the **Persistent Agent** field for the HR VM.



15. Right-click the HR VM, select **Policy Details**, click the **Endpoint Compliance** tab, validate that the **Corporate-Scan** has been matched, and then click **Close**.
16. Right-click the HR VM, and then select **Host Health**.

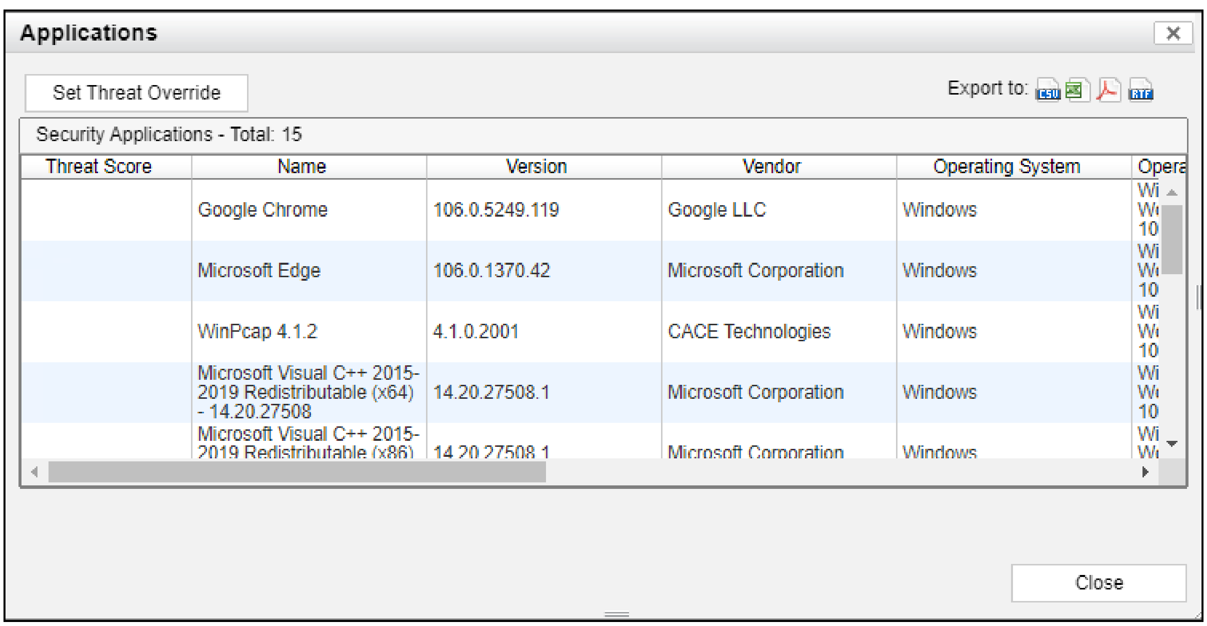
    You should now see the **Success** status for the **Corporate-Scan**.

DO NOT REPRINT
© FORTINET



17. Click the **History** tab, and then click the latest **Corporate-Scan** result to view more details about the scan results.
18. Right-click the HR VM, and then select **Host Applications**.

    You should see the list of applications installed on the HR VM.



DO NOT REPRINT
© FORTINET

Test a Persistent Agent

You will test compliance on an endpoint with a persistent agent installed.

To test a persistent agent

1. Continuing on the HR VM, open **File Explorer**, and then navigate to **C:\Program Files**.

   You should see a `corporate.txt` file in this directory.

2. Cut and paste, or move, the `corporate.txt` file to the **Desktop** folder.

> You should now see the FortiNAC icon marked **At Risk** in red in the Windows endpoint. Also, the FortiNAC GUI should now be inaccessible from the HR VM.

3. Return to the FortiNAC GUI on the FortiClient EMS VM, and then click **Users & Hosts** > **Hosts**.

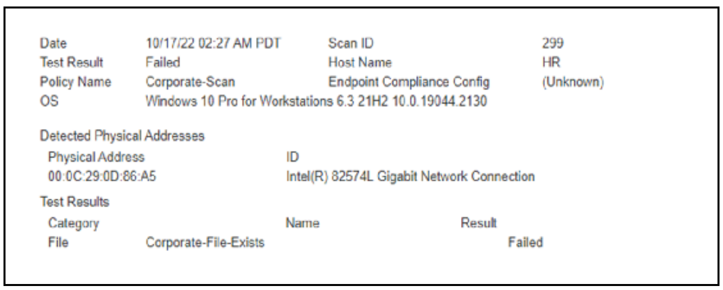
   You should now see a **+** icon over the HR VM.

4. Right-click the **HR** VM, and then select **Host Health**.

   You should see a **Failure** status under **Corporate-Scan**.

5. Click the **History** tab, and then click the latest **Corporate-Scan** result to view more details about the scan results.

   You should see that the **Corporate-File-Exists** monitor has **Failed**.



6. Click **Network** > **Inventory**, expand **Firewall** > **ISFW.ftnt.lab**, and then click **FSW**.

   You should see that **port8** on the HR VM is now assigned to **VLAN 102** which is the remediation VLAN.

7. Return to the HR VM, and then cut and paste, or move, the `corporate.txt` file from the **Desktop** folder back into the **C:\Program Files** directory.

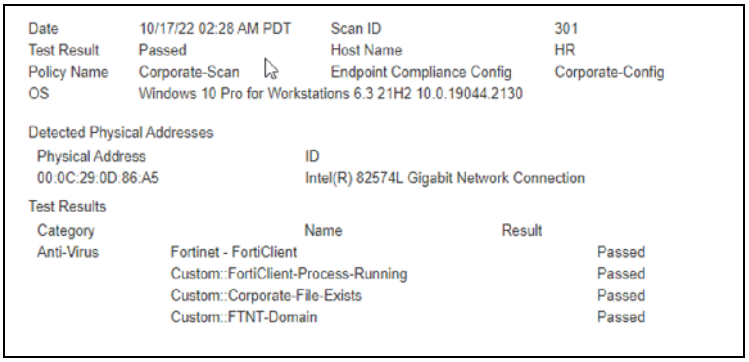
   If you are prompted for administrator credentials on the Windows VM, use the username `Administrator` and password `Password1!`.

> After few seconds, you should see a green check on the **Persistent Agent** icon and a status of **Normal**. You should also now be able to access the FortiNAC GUI from the HR VM.

8. Open Google Chrome, navigate to the FortiNAC GUI at `https://fnac.ftnt.lab:8443/`, and then log in with the username `admin` and password `Password1!` to validate access.
9. Click **Users & Hosts** > **Hosts**.
10. Right-click the HR VM, and then select **Host Health**.

DO NOT REPRINT
© FORTINET

You should now see the **Passed** status under **Corporate-Scan**.



Date	10/17/22 02:28 AM PDT	Scan ID	301
Test Result	Passed	Host Name	HR
Policy Name	Corporate-Scan	Endpoint Compliance Config	Corporate-Config
OS	Windows 10 Pro for Workstations 6.3 21H2 10.0.19044.2130		

Detected Physical Addresses

Physical Address	ID
00:0C:29:0D:86:A5	Intel(R) 82574L Gigabit Network Connection

Test Results

Category	Name	Result
Anti-Virus	Fortinet - FortiClient	Passed
	Custom::FortiClient-Process-Running	Passed
	Custom::Corporate-File-Exists	Passed
	Custom::FTNT-Domain	Passed

DO NOT REPRINT
© FORTINET

Exercise 3: Testing Endpoint Compliance for Guest and BYOD Devices

In this exercise, you will test compliance for guest and BYOD devices.

Test Guest Device Compliance

In this lab environment, since the devices are already onboarded to the network, there are a couple of ways to trigger a compliance scan. One way is to manually scan hosts from the **Hosts** section. However, you will simulate new rogue devices coming into the network, so you will start by deleting the SALES VM to let FortiNAC discover and reregister it and go through compliance scans.

To test guest device compliance

1. On the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **FortiNAC** login page bookmark.
2. Log in to the FortiNAC GUI with the username `admin` and password `Password1!`.
3. Click **Users & Hosts** > **Hosts**, click the **SALES** device, click **Delete** to delete the SALES VM from the FortiNAC inventory, and then click **OK**.
4. Click **Network** > **Inventory**, expand **Firewall** > **ISFW.ftnt.lab**, right-click **ISFW.ftnt.lab**, and then select **Poll for L2 (Hosts) Info**.

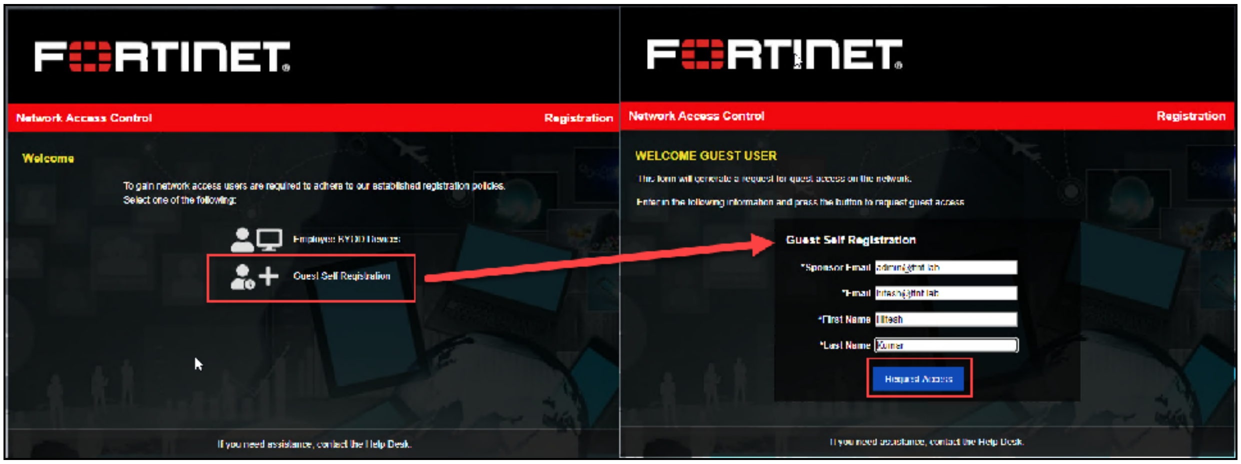
In a real-world scenario, FortiNAC automatically polls FortiSwitch and ISFW FortiGate for Layer 2 and Layer 3 information on connection. However, in this scenario, since we deleted the device manually, we can either force a poll or wait for the polling interval (5 minutes) for the SALES VM to be detected as a rogue device.

5. Click **Users & Hosts** > **Hosts**.
   You should now see a new rogue device.
6. Log in to the SALES VM with the username `sales` and password `Password1!`.
7. Open Google Chrome, and then try to navigate to the Fortinet website at `https://www.fortinet.com/`.
   You should be redirected to the FortiNAC registration page.
8. Select the **Guest Self Registration** option, type the values shown in the following table, and then click **Request Access**.

Field	Value
Sponsor Email	admin@ftnt.lab
Email	<type your email address>

DO NOT REPRINT
© FORTINET

Field	Value
First Name	<type your first name>
Last Name	<type your last name>



FortiNAC registers your user and provides your user credentials. You can make a note of it, if needed, but you can always reregister.

9. Click **Login**.

Nothing may happen on screen, but you should now see the FortiNAC dissolvable agent being downloaded. You can click **Instructions** to see the steps to run the dissolvable agent.

DO NOT REPRINT
© FORTINET

10. In the **Downloads** folder, run the `FortiNAC Dissolvable Agent.exe` file that you downloaded, and then if the SmartScreen window appears, click **Run**.
11. Click **Register** to begin the compliance scan, wait for the registration to complete, and then click **Finish**.
12. Open Google Chrome, and then try to navigate to the FortiNAC GUI at `https://fnac.ftnt.lab:8443/`.

    It should fail.
13. Try to navigate to `https://www.fortinet.com/`.

    It should work.
14. On the FortiClient EMS VM, return to the FortiNAC GUI, and then click **Users & Hosts** > **Hosts**.

    You should now see the SALES VM registered, with normal access.
15. Right-click the SALES VM, and then select **Host Health**.

    In the **Guest-Inv-Only-Scan** field, the status should be **Success**.
16. Click the **History** tab, and then click the latest **Guest-Inv-Only-Scan** result to view more details about the scan results.

    You may notice that you did not apply any compliance scans.
17. Click **OK**.
18. Right-click the SALES VM, and then select **Host Applications**.

    You should see the list of applications installed on the SALES VM.
19. Click **Close**.
20. Right-click the SALES VM, and then select **Policy Details**.

    You should see VLAN 199 assigned to the SALES VM, which should restrict access to the internet only.
21. Click **Network** > **Inventory**, select **Firewall** > **ISFW.ftnt.lab**, and then click **S108DV0JA4QI3V78**.

    You should see that **port7** on the SALES VM is now assigned to **VLAN 199**, which is the untrusted internet-only access VLAN.

Test BYOD Device Compliance

In this lab environment, you will reuse the SALES VM as the BYOD device, but since the device is already registered as a guest device, you will start by deleting the SALES VM to let FortiNAC discover and reregister it and go through compliance scans.

To test BYOD device compliance

1. Continuing on the FortiNAC GUI, click **Users & Hosts** > **Hosts**, click the SALES VM, click **Delete** to delete the SALES VM from the FortiNAC inventory, and then click **OK**.
2. Click **Network** > **Inventory**, expand **Firewall** > **ISFW.ftnt.lab**, right-click **ISFW.ftnt.lab**, and then select **Poll for L2 (Hosts) Info**.

In a real-world scenario, FortiNAC automatically polls FortiSwitch and ISFW FortiGate for Layer 2 and Layer 3 information on connection. However, in this scenario, since we deleted the device manually, we can either force a poll or wait for the polling interval (5 minutes) for the SALES VM to be detected again as a rogue device.

3. Click **Users & Hosts** > **Hosts**.

DO NOT REPRINT
© FORTINET

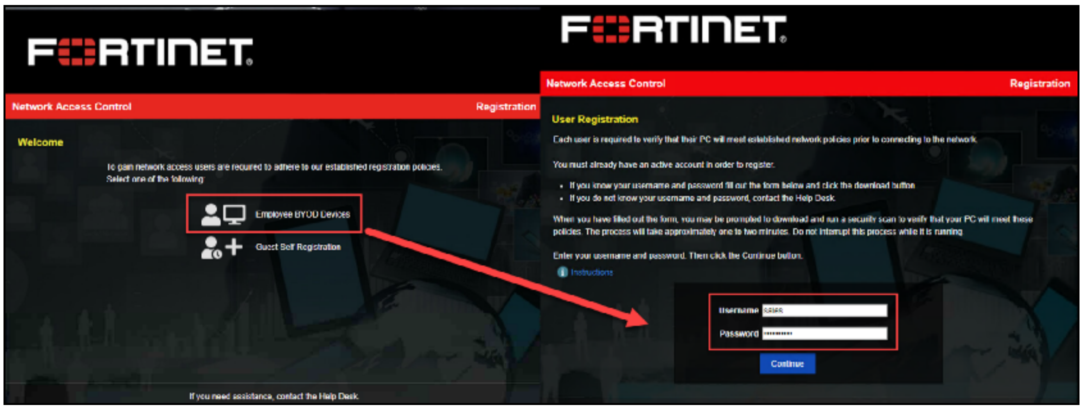
You should now see a new rogue device.

4. On the SALES VM, open Google Chrome, and then navigate to `https://www.fortinet.com/`.

   You should be redirected to the FortiNAC registration page.

5. Select the **Employee BYOD Devices** option, log in with the username `sales` and password `Password1!`, and then click **Continue**.

> You should now see the FortiNAC dissolvable agent being downloaded. You can click **Instructions** to see steps to run the dissolvable agent.



6. In the **Downloads** folder, run the `FortiNAC Dissolvable Agent.exe` file that you downloaded, and then if the SmartScreen window appears, click **Run**.
7. Click **Register** to begin the compliance scan, wait for the registration to complete, and then click **Finish**.
8. Open Google Chrome, and then navigate to the FortiNAC GUI at `https://fnac.ftnt.lab:8443/`.

   It should fail.

9. Navigate to `https://www.fortinet.com/`.

   It should work.

10. On the FortiClient EMS VM, return to the FortiNAC GUI, and then click **Users & Hosts** > **Hosts**.

    You should now see the SALES VM registered, with normal access.

11. Right-click the **SALES** device, and then select **Host Health**.

    In the **BYOD-AV-Scan** field, the status should be **Success**.

12. Click the **History** tab, and then click the latest **BYOD-AV-Scan** result to view more details about scan results.

    You can see FortiNAC matching FortiClient, Windows Defender, and/ or any other AV present according to the compliance scan.

DO NOT REPRINT
© FORTINET

Date	10/17/22 11:56 AM PDT	Scan ID	314
Test Result	Passed	Host Name	SALES
Policy Name	BYOD-AV-Scan	Endpoint Compliance Config	(Unknown)
OS	Windows 10 Pro for Workstations 6.3 21H2 10.0.19044.2130		

Detected Physical Addresses

Physical Address	ID
00:0C:29:6B:9A:4E	Intel(R) 82574L Gigabit Network Connection

Test Results

Category	Name	Result
Anti-Virus	Fortinet - FortiClient	Passed
Anti-Virus	Microsoft Windows Defender	Passed
Anti-Virus	Microsoft Windows Defender Engine Updates	Passed
Anti-Virus	Microsoft Windows Defender Signatures	Passed
Anti-Virus	Windows Defender Real-time Protection Check	Passed
Anti-Virus	Windows Defender 4.18.1909.6	Passed

13. Close the compliance history tab.
14. Click **OK**.
15. Right-click the SALES VM, and then select **Host Applications**.

    You should see the list of applications installed on the SALES VM.
16. Click **Close**.
17. Right-click the SALES VM, and then select **Policy Details**.

    You should see VLAN 199 assigned to the SALES VM, which should restrict access to the internet only.
18. Click **Network** > **Inventory**, expand **Firewall** > **ISFW.ftnt.lab**, and then click **S108DV0JA4QI3V78**.

    You should see that **port7** on the SALES VM is now assigned to **VLAN 199**, which is the untrusted internet-only access VLAN.

DO NOT REPRINT
© FORTINET

Exercise 4: Integrating MDM With Network Access

In this exercise, you will integrate FortiNAC with FortiClient EMS. You will also modify the user/host profile to use MDM compliance to work simultaneously with FortiClient EMS.

Integrate FortiNAC With FortiClient EMS

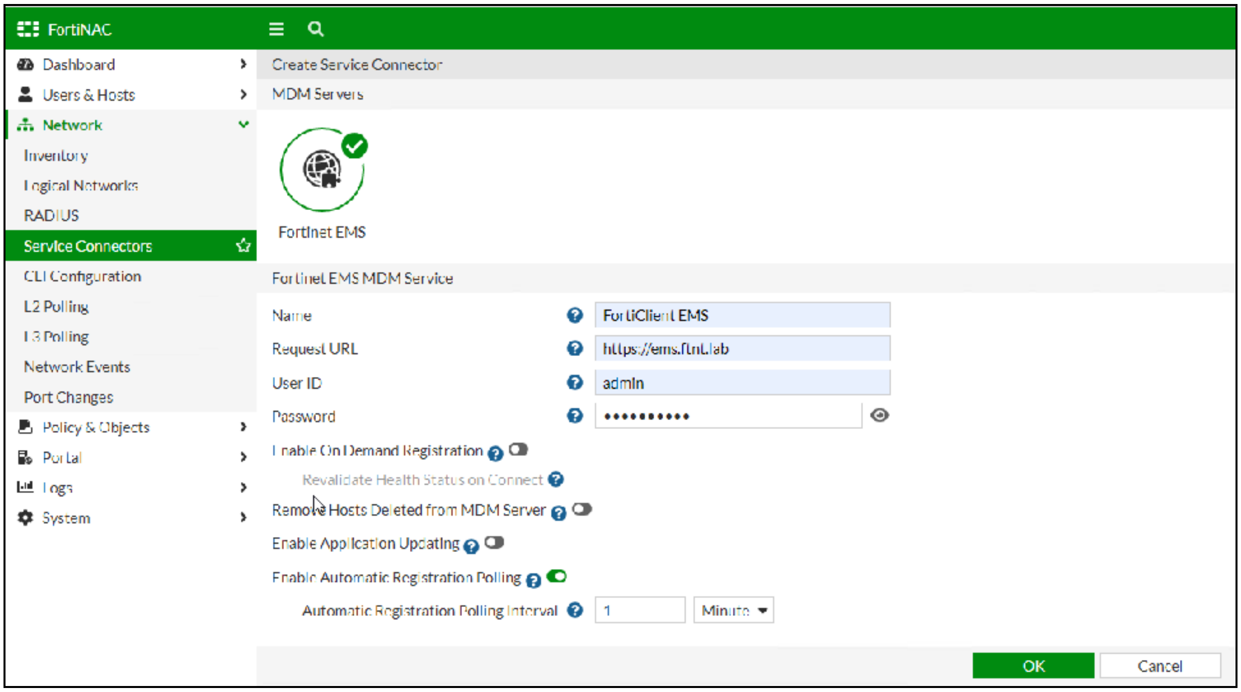
You will integrate FortiNAC with FortiClient EMS and poll endpoint data into FortiNAC.

To integrate FortiNAC with FortiClient EMS

1. On the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **FortiNAC** login page bookmark.
2. Log in to the FortiNAC GUI with the username `admin` and password `Password1!`.
3. Click **Network** > **Service Connectors**, click **Create New** > **Fortinet EMS**, configure the following settings, and then click **OK** to integrate FortiNAC with FortiClient EMS:

Field	Value
Name	FortiClient EMS
Request URL	https://ems.ftnt.lab
User ID	admin
Password	Password1!
Enable Automatic Registration Polling	Enabled
Automatic Registration Polling Interval	1 Minute

DO NOT REPRINT
© FORTINET



You should not set the timer too low in a production environment, because it could cause increased traffic between FortiNAC and the EMS server.

4. Right-click the **FortiClient EMS** service connector, and then click **Poll**.
5. Click **Users & Hosts** > **Hosts**.

   You should now see the **REMOTE** device registered but grayed out.

Stop and Think!

Why do we see the REMOTE machine registered to FortiNAC, even though FortiNAC does not manage the switch connected to the REMOTE VM?

Discussion

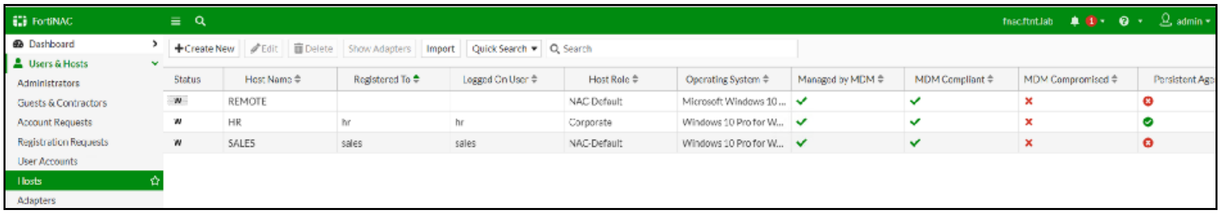
Explore the feature set of the Fortinet EMS service connector.

Do we import only the endpoint from FortiClient EMS, or do we import any other data?

6. Right-click the column name, add the **Manage by MDM**, **MDM Compliant**, and **MDM Compromised** columns if they are not already selected, and then click **Apply**.
7. Scroll right to find the MDM information.

   You should now see that all the devices found are being managed by MDM and all of the devices are marked as compliant.

DO NOT REPRINT
© FORTINET



Modify the User/Host Profile for MDM Compliance

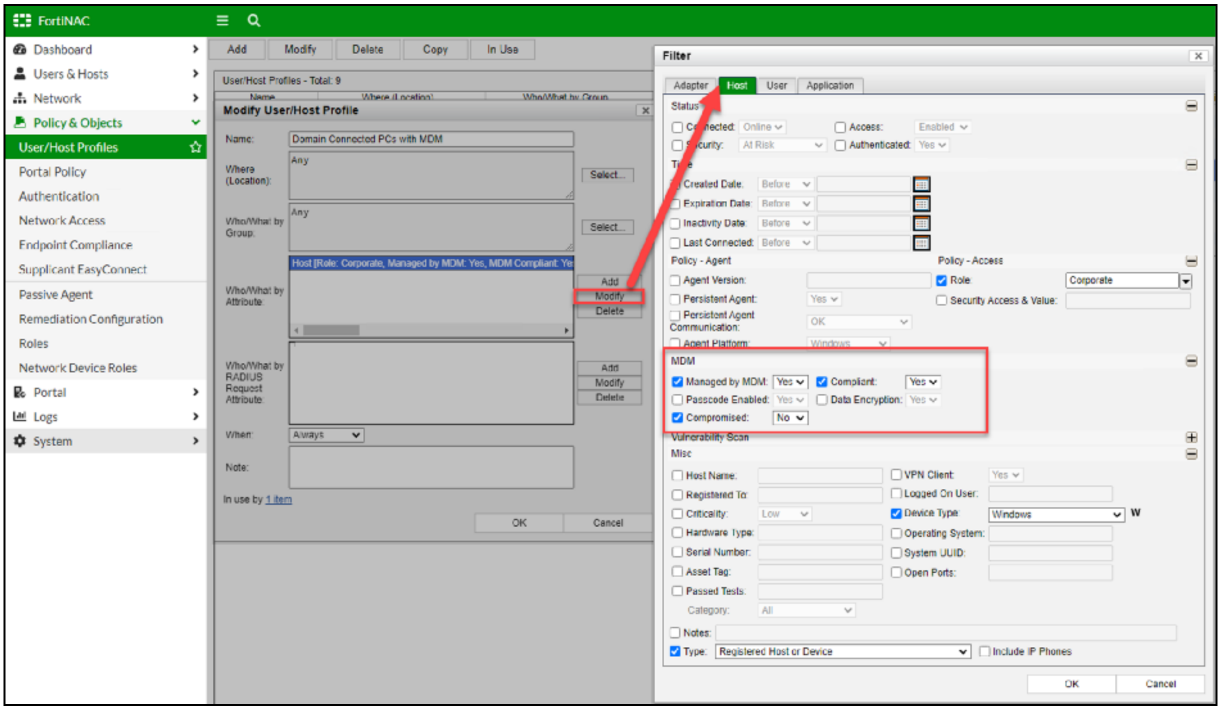
You will modify the user/host profile to use MDM compliance to work simultaneously with FortiClient EMS.

To modify the user/host profile for MDM compliance

1. Continuing on the FortiNAC GUI, click **Policy & Objects** > **User/Host Profiles**, select **Domain Connected PCs with PA**, and then click **Copy** to create a new profile named `Domain Connected PCs with MDM`.
2. In the **Who/What by Attribute** field, select an existing row, and then click **Modify**.
3. Click the **Host** tab, expand the **MDM** section, configure the following settings, and then click **OK** to look for MDM compliance:

Field	Value
Persistent Agent	Clear the checkbox.
Persistent Agent Communication	Clear the checkbox.
Managed by MDM	Select the checkbox, and then select **Yes**.
Compliant	Select the checkbox, and then select **Yes**.
Compromised	Select the checkbox, and then select **No**.

DO NOT REPRINT
© FORTINET



4. Click **OK**.
5. Click **Policy & Objects** > **Network Access**, select **Corporate Access Policy**, and then click **Modify**.
6. In the **User/Host Profile** field, change the value to **Domain Connected PCs with MDM**, and then click **OK**.
7. Click **Users & Hosts** > **Hosts**, right-click the **HR** device, and then select **Policy Details**.

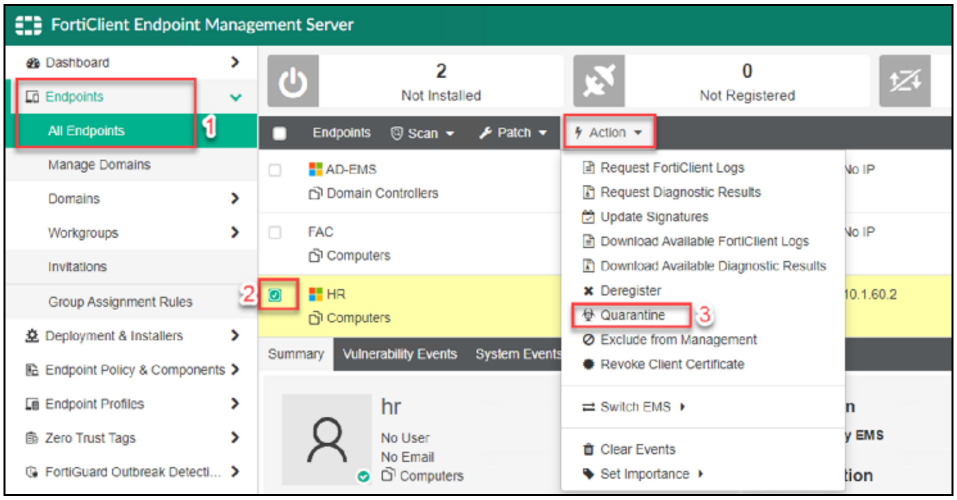
   You should see that it now matches the new MDM profile.

8. Click **Logs** > **Events & Alarms**, select the **Mappings** tab, and then click **Add**.
9. In the **Trigger Event** field, select **MDM Host Compliance Failed**, select the **Action** checkbox, and then select **Host Security Action**.
10. In the **Primary Task** field, select **At Risk** and **Corporate-Scan**, and then click **OK**.

You are using alarm mappings to mark the host as **At Risk** when MDM compliance fails. If you do not do this, you will not take any action on the host, but the host will no longer match any network access policy and will be dead-ended until an administrator takes action.

11. Open a new Google Chrome tab, and then in **Bookmarks**, select the **FortiClient EMS** login page bookmark.
12. Log in with the username `admin` and password `Password1!`.
13. Click **Endpoints** > **All Endpoints**, and then select the **HR** device.
14. Click **Action** > **Quarantine**.

DO NOT REPRINT
© FORTINET



15. Return to the FortiNAC GUI, click **Network** > **Service Connectors**, right-click **FortiClient EMS**, and then click **Poll**.

To save time, you are forcing the poll in the lab, but in a production environment, polling will be automated based on the time configured, and FortiNAC will take action accordingly.

16. Click **Users & Hosts** > **Hosts**.

    You should see a **+** icon on the **HR** device marking the host as **At Risk**.

17. Return to the FortiClient EMS GUI, click **Endpoints** > **All Endpoints**, and then select the **HR** device.
18. Click **Action** > **Unquarantine**.
19. Return to the FortiNAC GUI, click **Network** > **Service Connectors**, right-click **FortiClient EMS**, and then click **Poll**.
20. Click **Users & Hosts** > **Hosts**.

    You should see the **HR** device as **Normal**.

You may need to wait a few seconds for FortiNAC to change access VLANs and access to resume.

DO NOT REPRINT
© FORTINET

Exercise 5: Configuring FortiClient EMS ZTNA Tagging Rules to Block Remotely Controlled Machines

In this exercise, you will configure ZTNA tags to tag remotely controlled machines and block access to prevent the RDP hopping that was discussed in Lab 1.

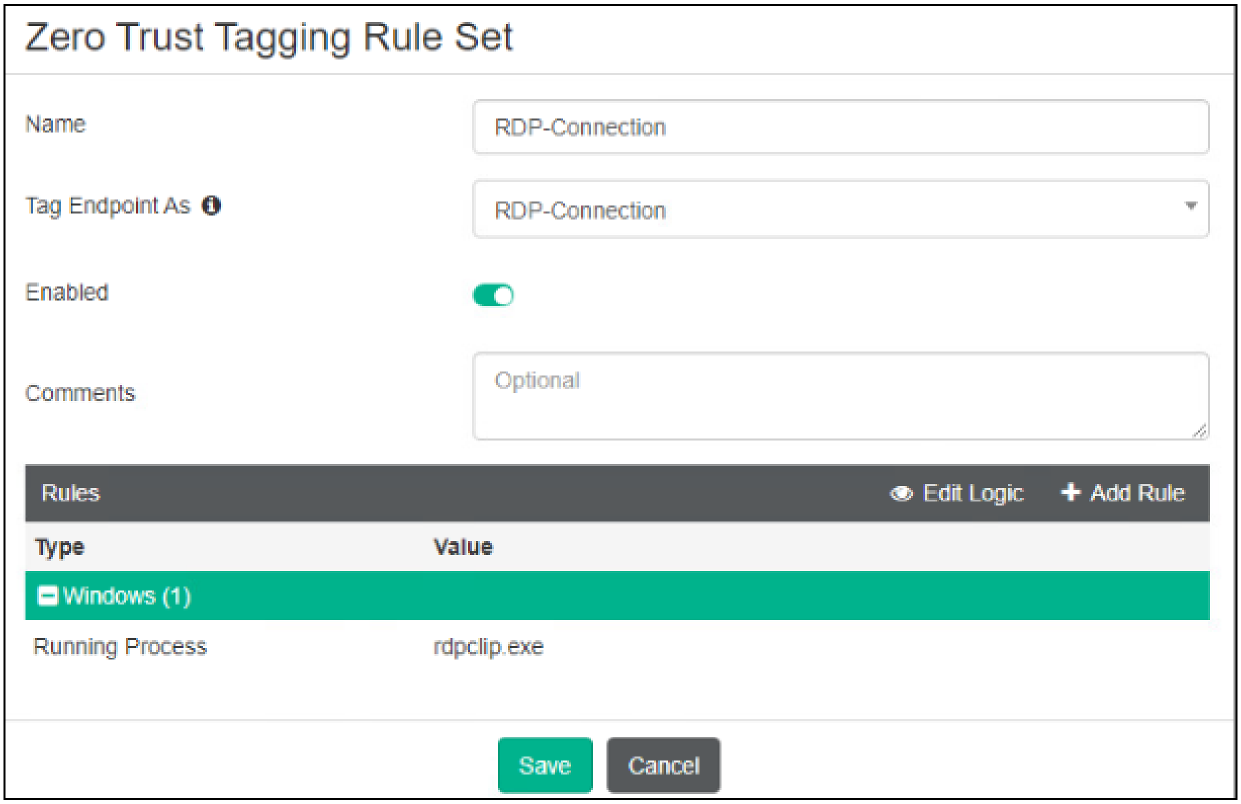
Configure the FortiClient EMS ZTNA Tagging Rule for Detecting an RDP Connection

You will create ZTNA tags on the FortiClient EMS to detect RDP connections.

To configure the FortiClient EMS ZTNA tagging rule

1. On the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **FortiClient EMS** login page bookmark.
2. Log in to the FortiClient EMS GUI with the username `admin` and password `Password1!`.
3. In the left menu, click **Zero Trust Tags** > **Zero Trust Tagging Rules**.
4. In the upper-right corner, click **Add**.
5. In the **Name** field, type `RDP-Connection`.
6. In the **Tag Endpoint As** field, type `RDP-Connection`, and then press `Enter`.
7. In the **Rules** section, click **Add Rule**, and then select **Windows OS**.
8. In the **Rule Type** field, select **Running Process**.
9. In the **Running Process** field, type `rdpclip.exe`, and then click **Save**.

DO NOT REPRINT
© FORTINET

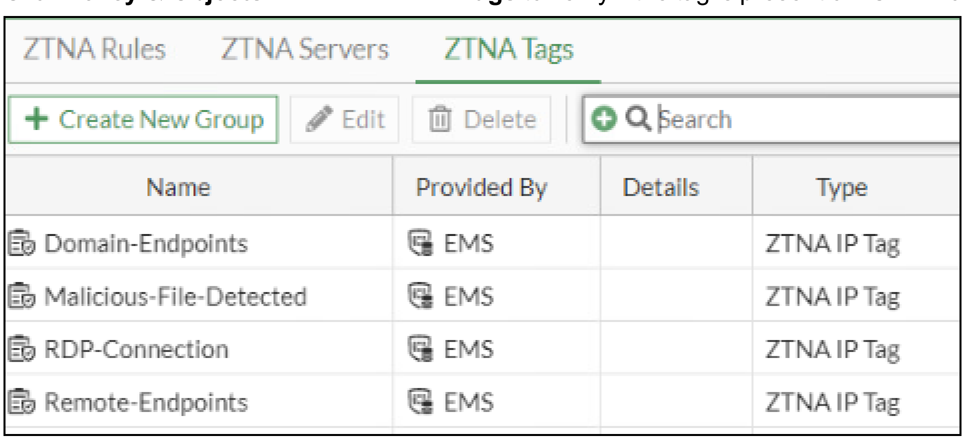


10. Click **Save** to save this zero-trust tagging rule.

`rdpclip.exe` is a Windows system process, started for each remote user when they connect to the remote desktop. This process is used for copy and paste functions between the local host and remote host.

To create a new firewall policy with IP and MAC address filtering and block RDP access

1. On the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **ISFW** login page bookmark.
2. Log in to the ISFW GUI with the username `admin` and password `password`.
3. Click **Policy & Objects** > **ZTNA** > **ZTNA Tags** to verify if the tag is present on ISFW FortiGate.



DO NOT REPRINT
© FORTINET

It may take a minute or two to see the updated tags. If the tag does not appear on ISFW FortiGate, restart the ZTNA process.

1. On the FortiClient EMS VM, open PuTTY, and then connect over SSH to the ISFW saved session.
2. Log in with the username `admin` and password `password`.
3. Enter the following command to restart the process:

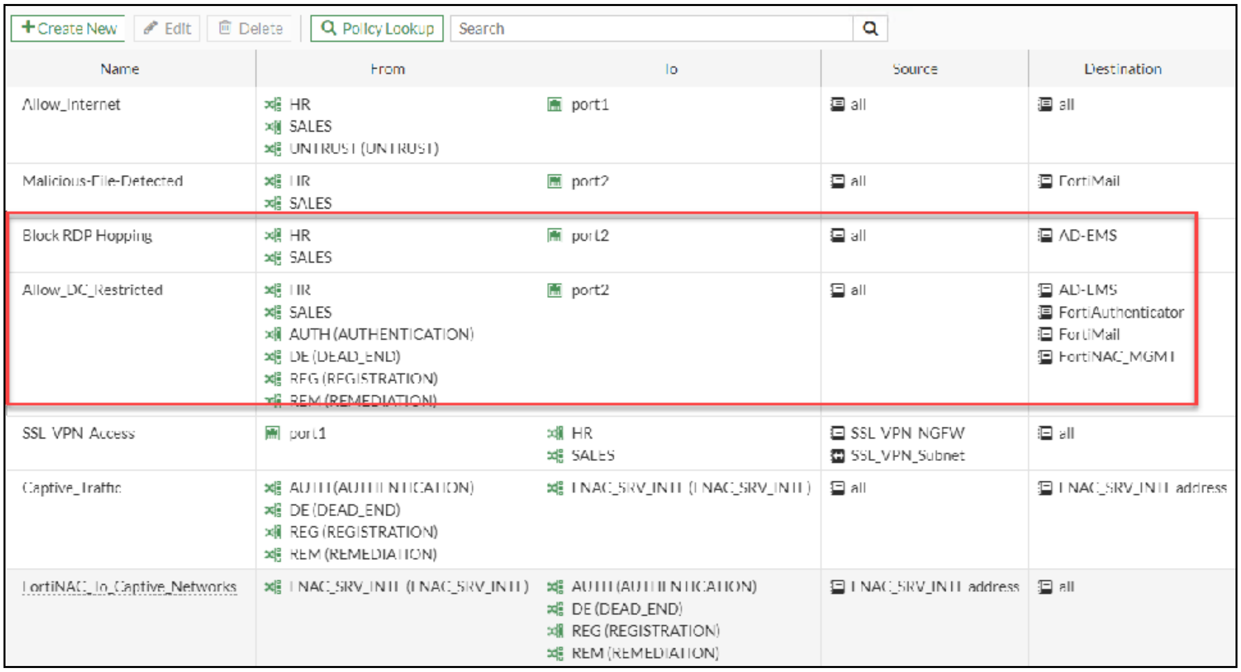
```
diagnose test application fcnacd 99
```

4. Click **Policy & Objects** > **Firewall Policy**, and then click **Create New** to create a new firewall policy.
5. In the **New Policy** window, configure the following settings:

Field	Value
Name	Block RDP Hopping
Incoming Interface	HR Sales
Outgoing Interface	port2
Source	all
IP/Mac Based Access Contro IP Tagl	RDP-Connection
Destination	AD-EMS
Service	RDP
Action	Deny

6. Click **OK** to add a new firewall policy.
7. Move the **Block RDP Hopping** policy above the **Allow_DC_Restricted** policy.

DO NOT REPRINT
© FORTINET



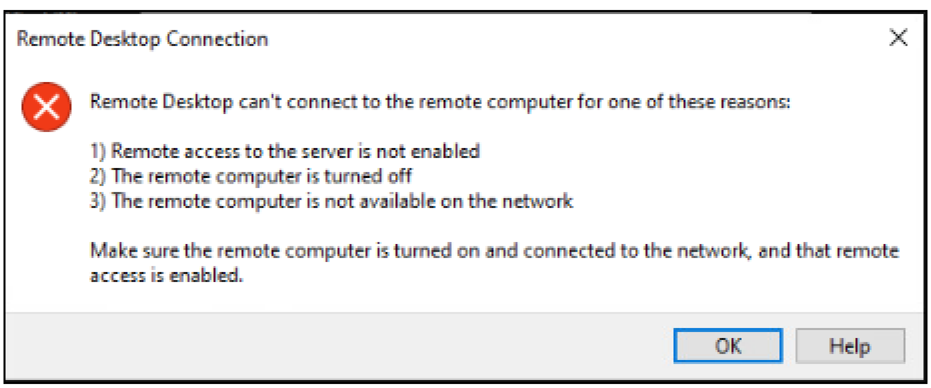
Name	From	To	Source	Destination
Allow_Internet	HR SALES UNTRUST (UNTRUST)	port1	all	all
Malicious-File-Detected	HR SALES	port2	all	FortiMail
Block RDP Hopping	HR SALES	port2	all	AD-EMS
Allow_DC_Restricted	HR SALES AUTH (AUTHENTICATION) DE (DEAD_END) REG (REGISTRATION) REM (REMEDIATION)	port2	all	AD-EMS FortiAuthenticator FortiMail FortiNAC_MGMT
SSL VPN Access	port1	HR SALES	SSL VPN NGFW SSL_VPN_Subnet	all
Captive_Traffic	AUTH (AUTHENTICATION) DE (DEAD_END) REG (REGISTRATION) REM (REMEDIATION)	FNAC_SRV_INT (FNAC_SRV_INT)	all	FNAC_SRV_INT address
FortiNAC_To_Captive_Networks	FNAC_SRV_INT (FNAC_SRV_INT)	AUTH (AUTHENTICATION) DE (DEAD_END) REG (REGISTRATION) REM (REMEDIATION)	FNAC_SRV_INT address	all

To test remote access to the EMS-AD server using RDP hopping

1. On the Remote VM, right-click the **Windows** icon, click **Run**, type `mstsc`, and then click **OK** to open the Remote Desktop Connection application.
2. In the **Computer** field, type `10.1.60.2`.
3. Log in with the username `ftnt.lab\hr` and password `Password1!`.

   You are connected to the HR VM using RDP.
4. On the HR VM, right-click the **Windows** icon, click **Run**, type `mstsc`, and then click **OK** to open the Remote Desktop Connection application.
5. In the **Computer** field, type `ems.ftnt.lab`.

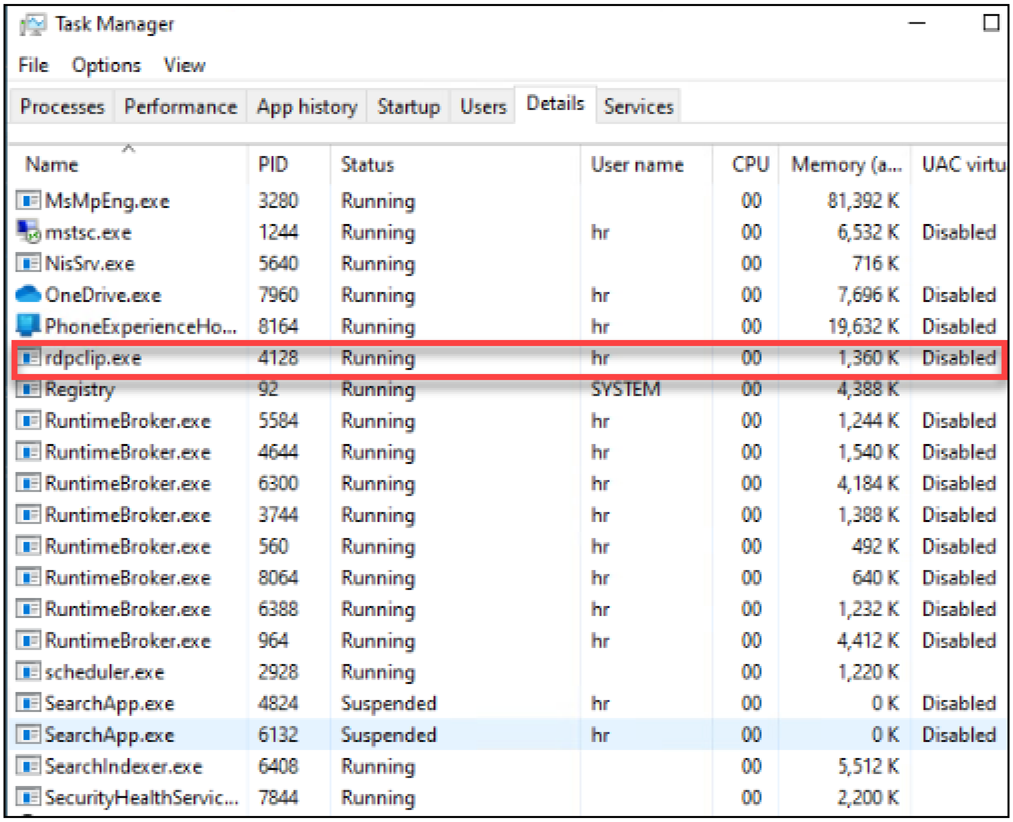
   The RDP connection to EMS-AD should fail.



6. Click **OK**.
7. Right-click the **Windows** icon, click **Run**, type `taskmgr`, and then click **OK** to open Task Manager.
8. Click the **Details** tab.

   There will be a process called `rdpclip.exe`.

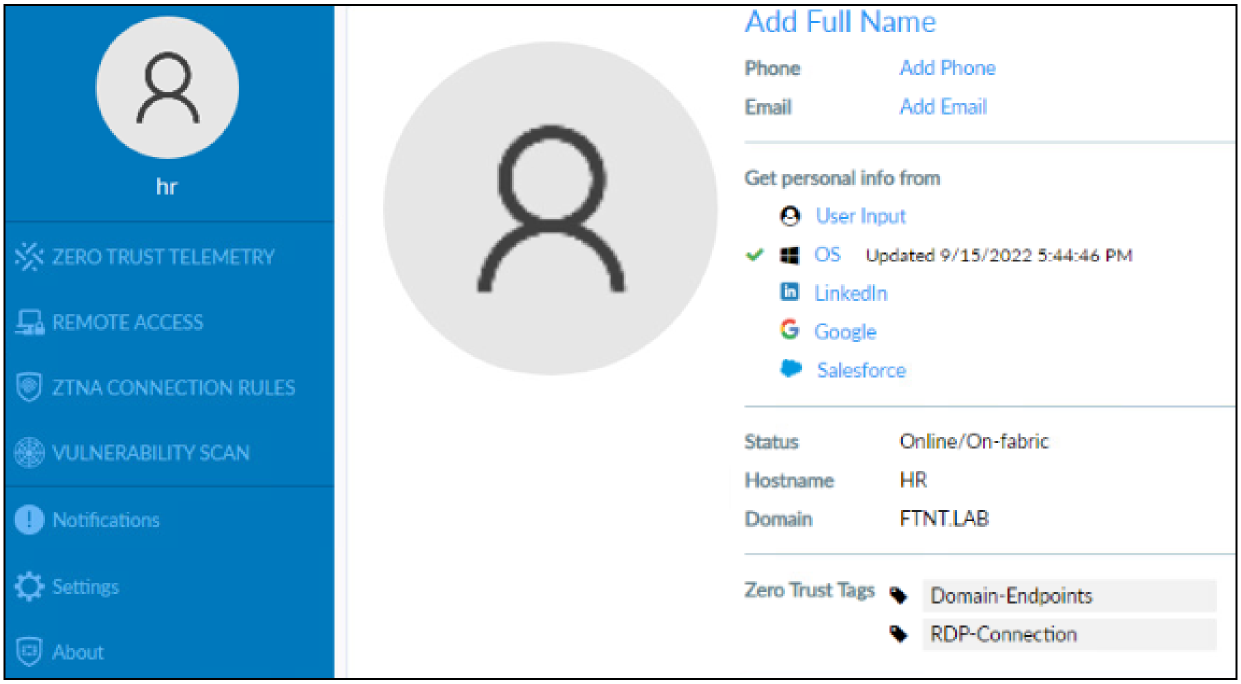
DO NOT REPRINT
© FORTINET



9. Close Task Manager.
10. On the system tray, double-click the **FortiClient** icon.
11. Click the user avatar.

    The endpoint is tagged as **RDP-Connection** because the `rdpclip.exe` process started when the remote VM established a remote desktop connection to the HR VM.

DO NOT REPRINT
© FORTINET



This scenario is simulated for a lab environment. In a production environment, different tags could be used depending on the organization's requirements.

12. Disconnect the RDP session to the HR VM.
13. Restart the HR VM.

DO NOT REPRINT
© FORTINET

Exercise 6: Checking Compliance Using FortiClient EMS Zero-Trust Tags

In this exercise, you will configure ZTNA tags for providing network access based on endpoint compliance checks.

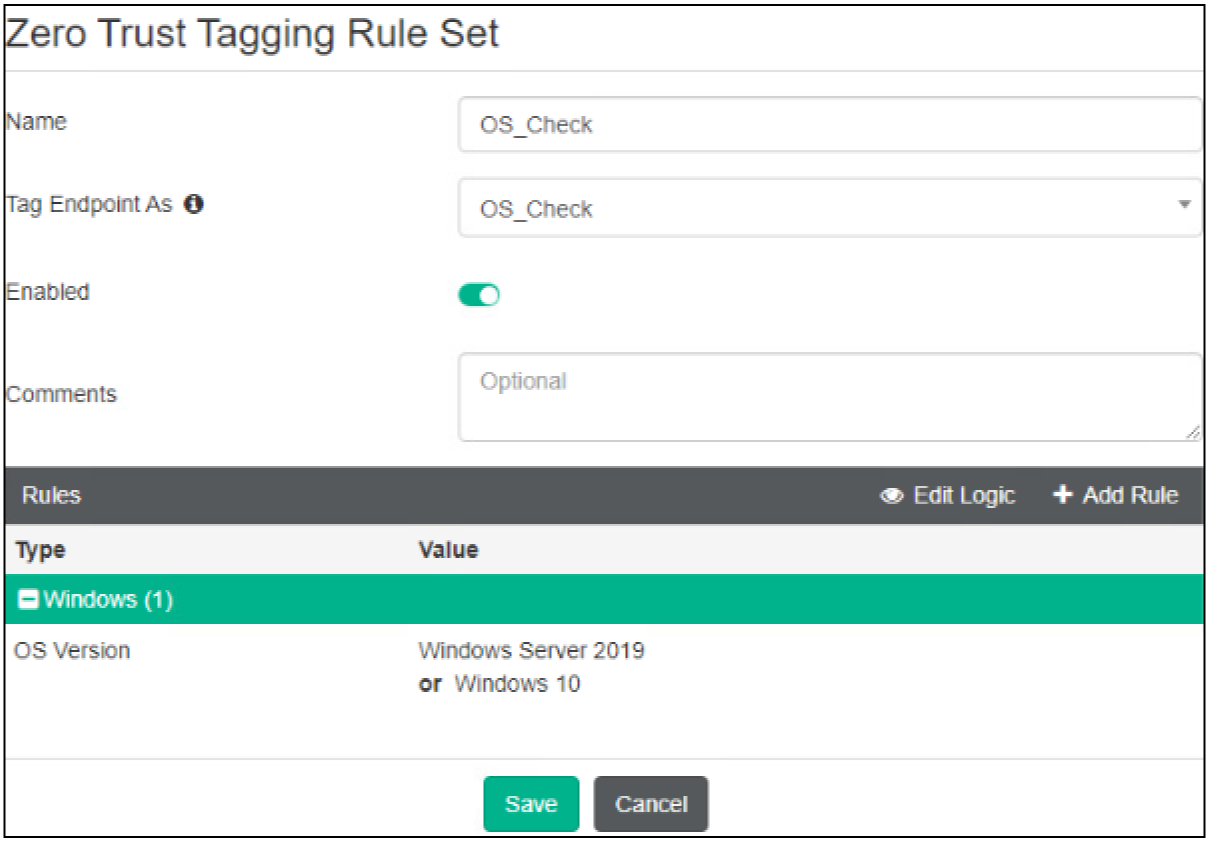
Configure the FortiClient EMS ZTNA Tagging Rule for OS Version and Antivirus Software Detection

You will create ZTNA tags to detect OS versions and if antivirus software is installed.

To configure the FortiClient EMS ZTNA tagging rule

1. On the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **FortiClient EMS** login page bookmark.
2. Log in to the EMS GUI with the username `admin` and password `Password1!`.
3. Click **Zero Trust Tags** > **Zero Trust Tagging Rules**.
4. Click **Add**.
5. In the **Name** field, type `OS-Check`.
6. In the **Tag Endpoint As** field, type `OS-Check`, and then press `Enter`.
7. In the **Rules** section, click **Add Rule**, and then select **Windows OS**.
8. In the **Rule Type** field, select **OS Version**.
9. In the **OS Version** drop-down list, select **Windows Server 2019**.
10. Click **+** to add another **OS Version**, select **Windows 10**, and then click **Save**.

DO NOT REPRINT
© FORTINET

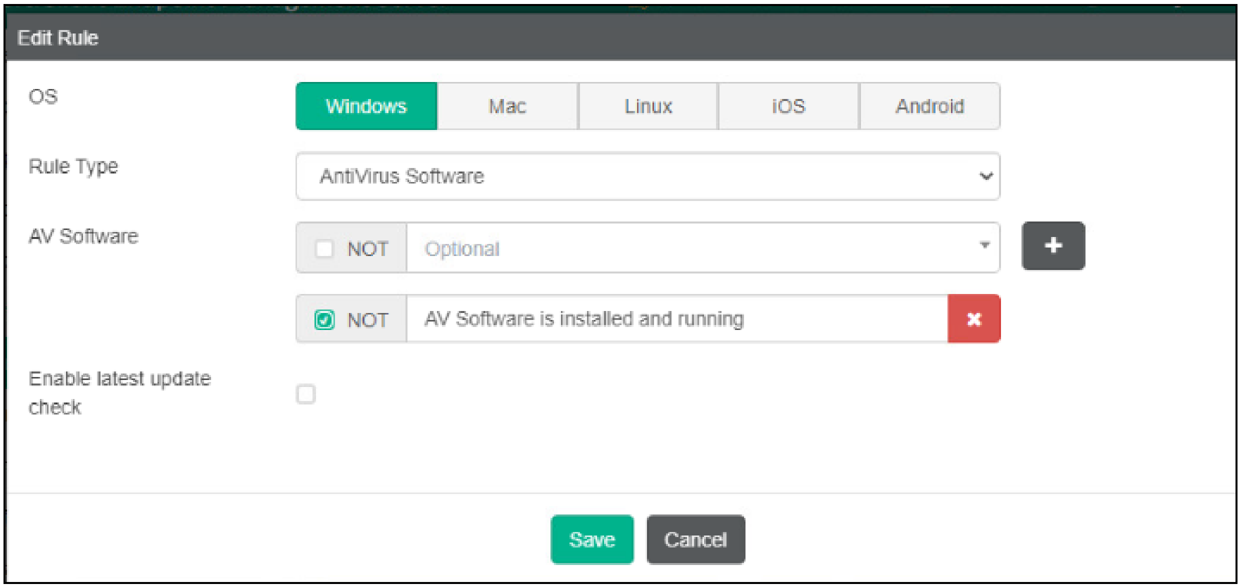


11. Click **Save** to save this zero-trust tagging rule.

To configure the FortiClient EMS ZTNA tagging rule for antivirus software detection

1. Continuing on the EMS GUI, click **Zero Trust Tags** > **Zero Trust Tagging Rules**.
2. Click **Add**.
3. In the **Name** field, type `AV`.
4. In the **Tag Endpoint As** field, type `AV`, and then press `Enter`.
5. In the **Rules** section, click **Add Rule**, and then select **Windows OS**.
6. In the **Rule Type** field, select **AntiVirus Software**.
7. In the **AV Software** field, select **AV Software is installed and running**, and then select the **NOT** checkbox.

DO NOT REPRINT
© FORTINET



8. Click **Save**.
9. Click **Save** to save this zero-trust tagging rule.

Configure Firewall Policies for Compliance Checks

You will configure firewall policies on NGFW FortiGate to allow or deny traffic based on compliance.

To configure firewall policies for compliance checks

1. On the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **NGFW** login page bookmark.
2. Log in with the username `admin` and password `password`.
3. Click **Policy & Objects** > **ZTNA**.
4. Edit the **ZTNA-Deny** policy.
5. In the **ZTNA Tag** field, click **+**, and then select **AV**.
6. Click **OK** to save policy changes.
7. Edit the **ZTNA-Allow-All** policy.
8. In the **ZTNA Tag** field, click **+**, and then select **OS-Check**.
9. Click **OK** to save the policy changes.

Test Access Based on Endpoint Compliance

You will control access to a web server based on endpoint compliance.

To test endpoint compliance

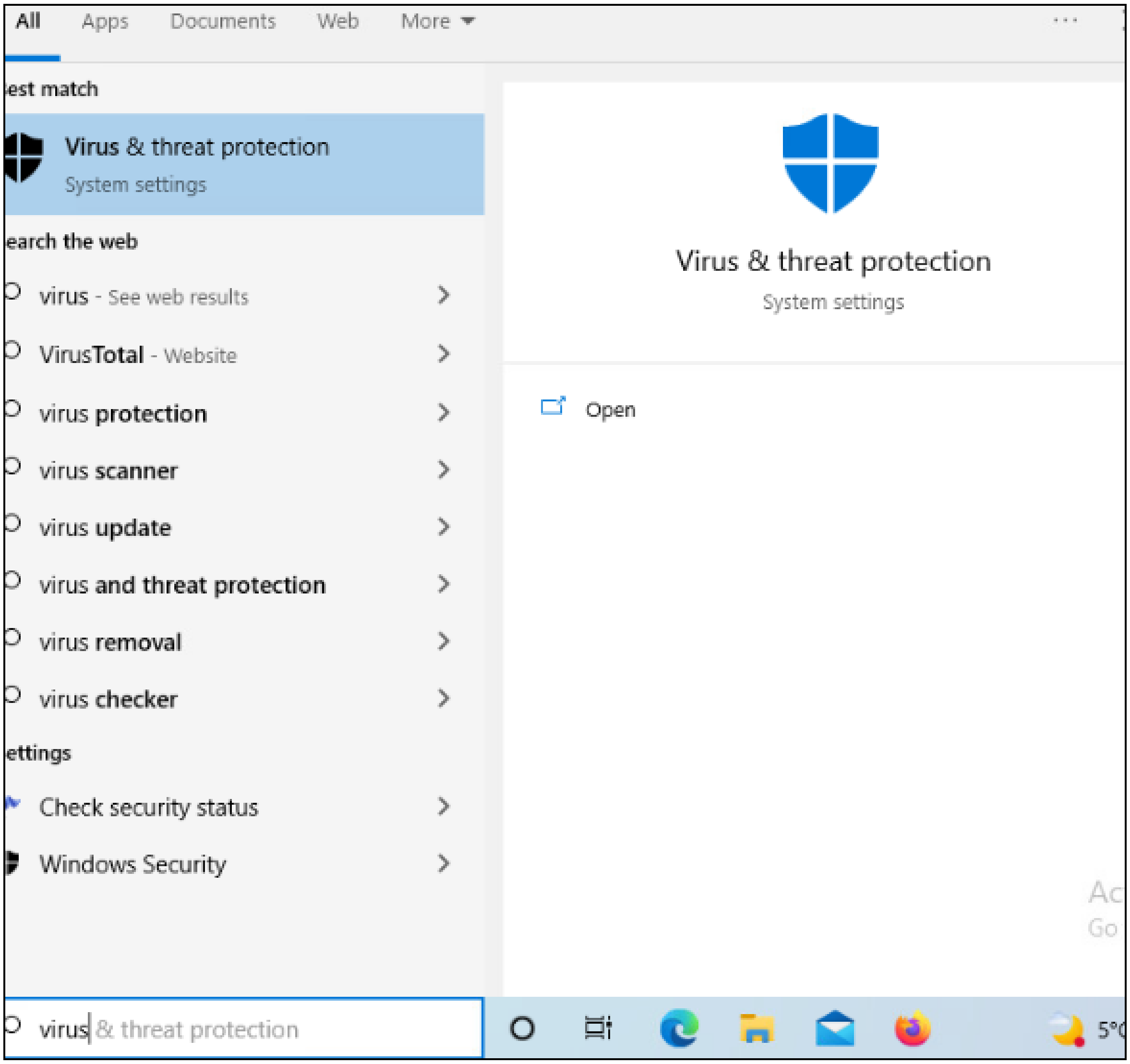
1. On the Remote VM, open Google Chrome, and then in **Bookmarks**, select the **Webserver** bookmark.
2. Choose the EMS signed certificate, and then click **OK**.

DO NOT REPRINT
© FORTINET

3. Log in with the username `remote` and password `password`.

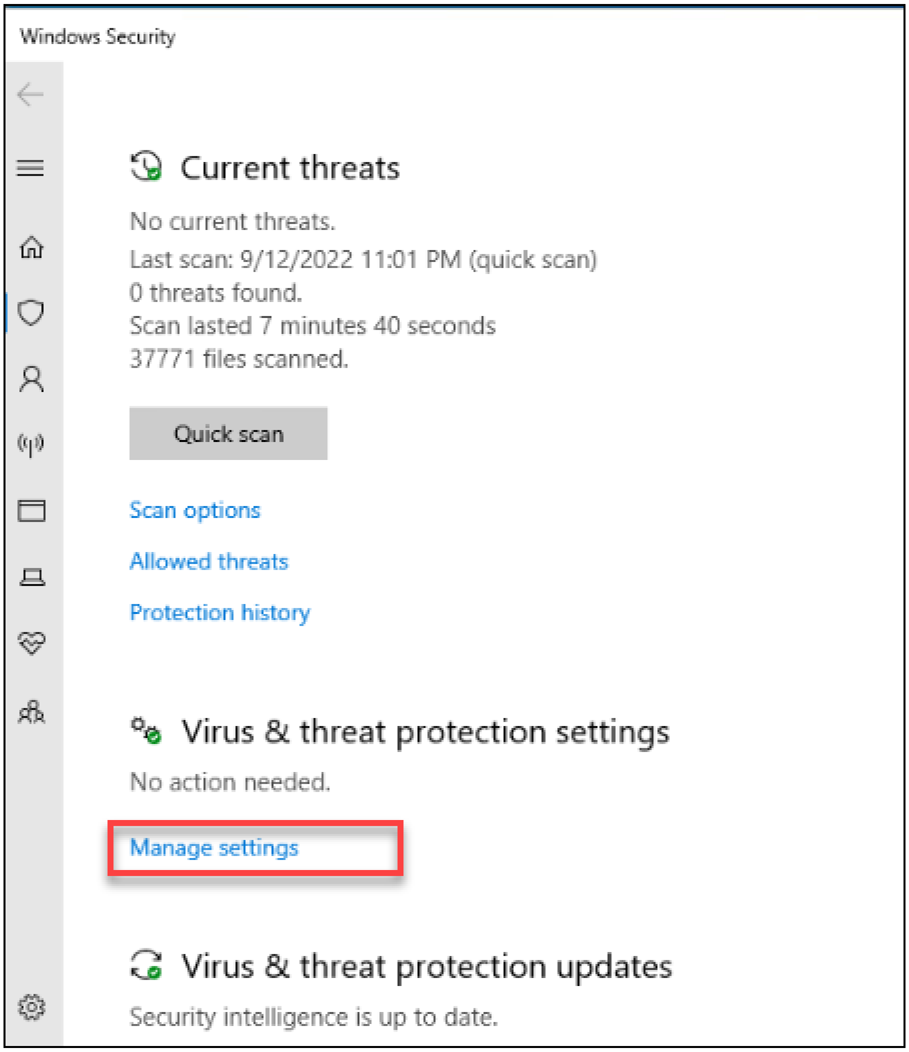
   After successful authentication, you can access the web page, since the endpoint matches the allowed OS versions.

4. Close Google Chrome.
5. Open a Windows search, and then search for **Virus & threat protection**.



6. In the **Windows Security** window, in the **Virus & threat protection settings** section, click **Manage settings**.

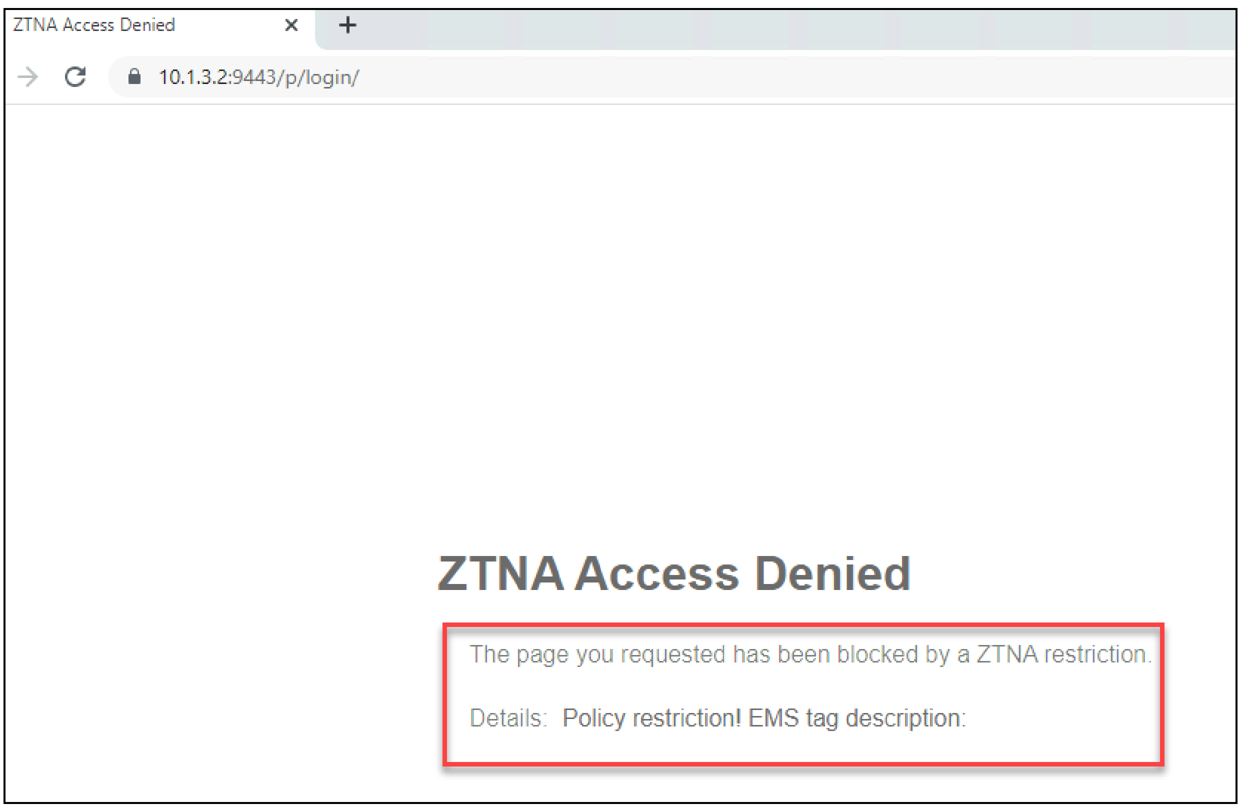
DO NOT REPRINT
© FORTINET



7. Turn off **Real-time protection**.
8. In the **User Account Control** window, click **Yes**.

DO NOT REPRINT
© FORTINET

9. Close the **Windows Security** window.
10. On the desktop, open the Google Chrome browser, in **Bookmarks**, select the **Webserver** bookmark.
11. Choose the EMS signed certificate, and then click **OK**.



Access is denied because the endpoint failed its compliance because it does not have antivirus software installed.

DO NOT REPRINT
© FORTINET

Lab 6: ZTA Enforcement and Incident Response

In this lab, you will configure different incident response solutions.

Objectives

- Configure SMTP endpoint alerts on FortiClient EMS
- Manually quarantine FortiClient endpoints
- Configure the EMS connector on FortiAnalyzer
- Configure automatic playbooks for endpoint quarantine
- Configure manual playbooks for endpoint unquarantine
- Configure security incident rules on FortiNAC and automated response

Time to Complete

Estimated: 45 minutes

DO NOT REPRINT
© FORTINET

Exercise 1: Manually Quarantine Off-Fabric FortiClient Endpoints

In this exercise, you will configure FortiClient EMS to send email alerts based on endpoint malicious activity. You will also manually quarantine an endpoint from the FortiClient EMS console.

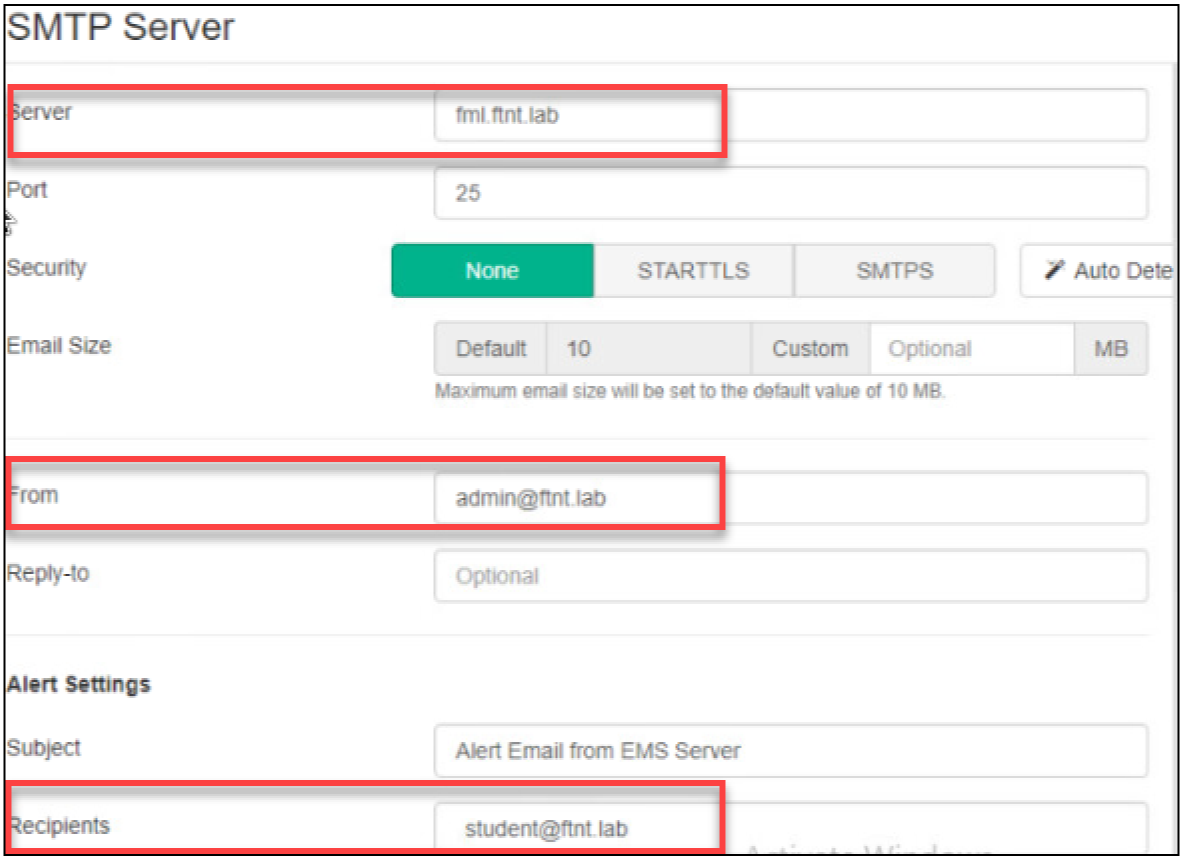
Configure an SMTP Server and Enable Endpoint Alerts on FortiClient EMS

You will configure an SMTP server on FortiClient EMS and enable endpoint alerts. You will also enable malware protection on the endpoint profile.

To configure an SMTP server

1. On the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **FortiClient EMS** login page bookmark.
2. Log in to the FortiClient EMS GUI with the username `admin` and password `Password1!`.
3. In the left menu, click **System Settings** > **SMTP Server**.
4. In the **Server** field, type `fml.ftnt.lab`.
5. In the **From** field, type `admin@ftnt.lab`.
6. In the **Recipients** field, type `student@ftnt.lab`.

DO NOT REPRINT
© FORTINET

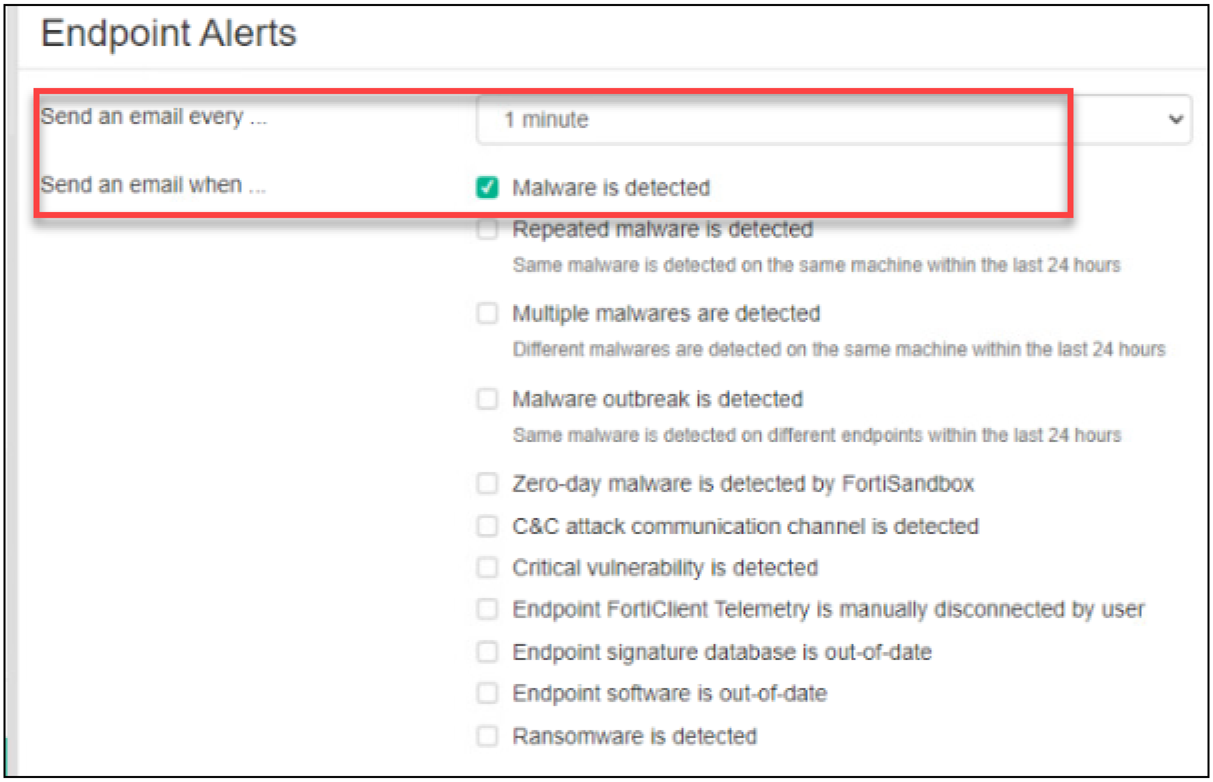


7. Click **Save**.
8. Click **Yes** to save the configuration.

To enable endpoint alerts

1. Continuing on the FortiClient EMS GUI, in the left menu, click **System Settings** > **Endpoint Alerts**.
2. In the **Send an email every** field, select **1 minute**.
3. In the **Send an email when** field, select the **Malware is detected** checkbox.

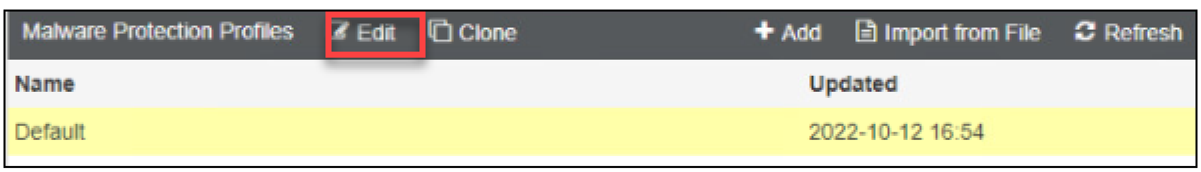
DO NOT REPRINT
© FORTINET



4. Click **Save**.

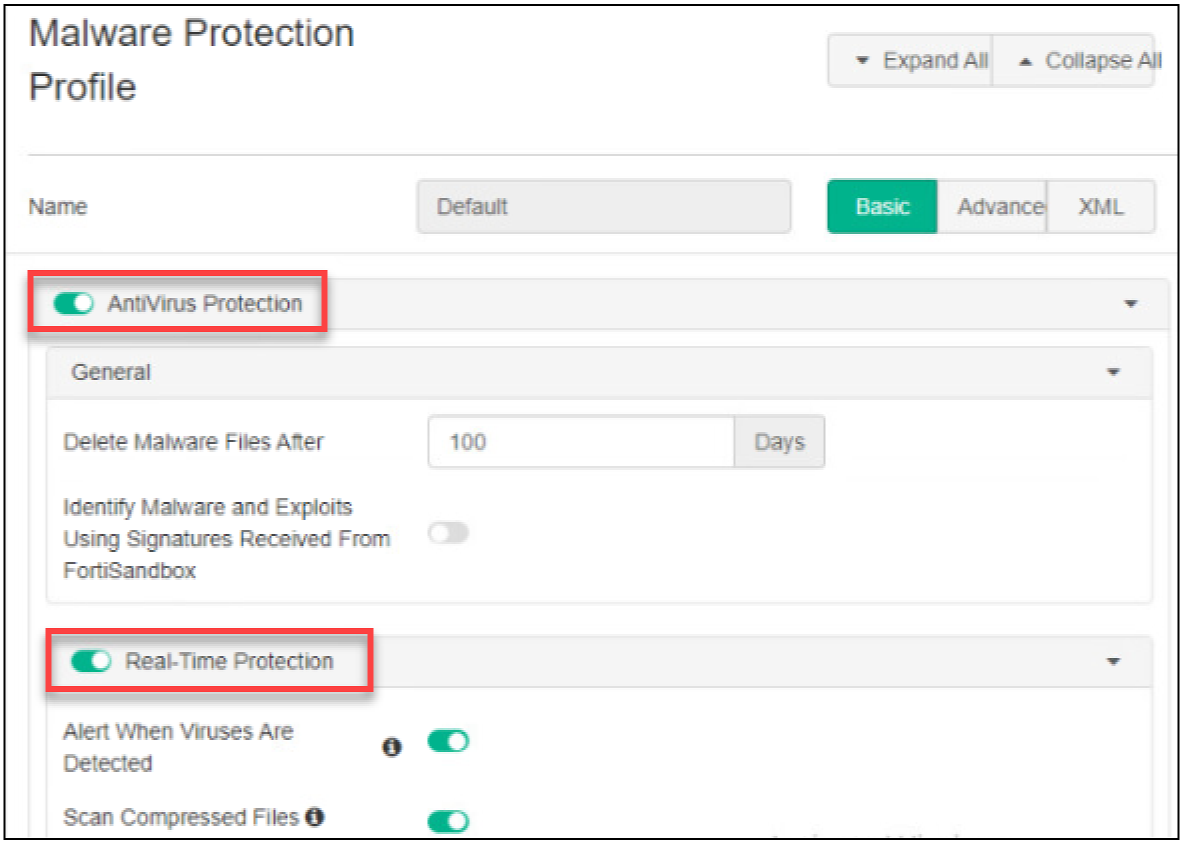
To enable malware protection

1. Continuing on the FortiClient EMS GUI, in the left menu, click **Endpoint Profiles** > **Malware Protection**.
2. Click the **Default** profile, and then click **Edit**.



3. Enable **AntiVirus Protection** to enable antivirus, and then confirm that **Real-Time Protection** is enabled.

DO NOT REPRINT
© FORTINET



4. Click **Save**.
   This enables malware protection on the default endpoint policy.

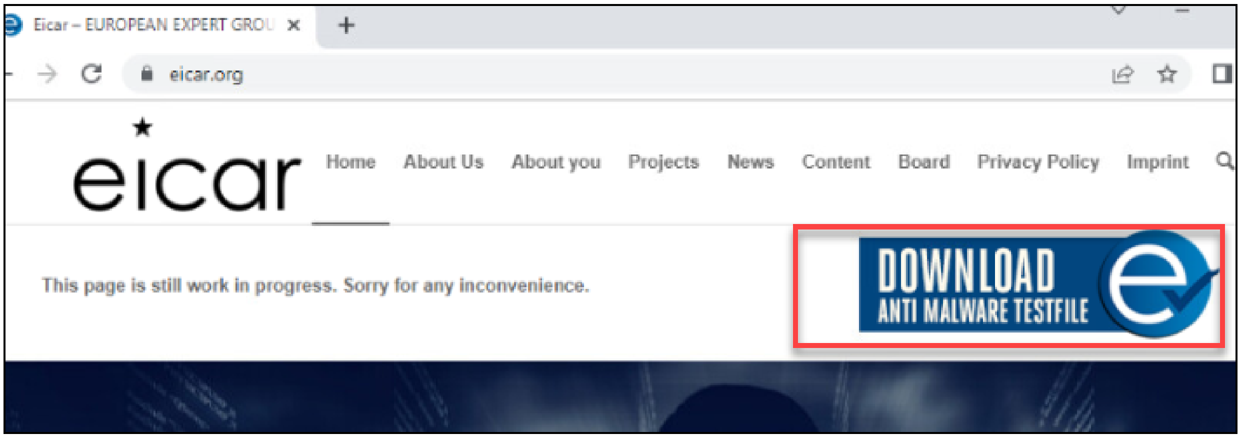
Test Email Alerts and Manually Quarantine an Endpoint on FortiClient EMS

You will test email alerts and manually quarantine an endpoint on FortiClient EMS.

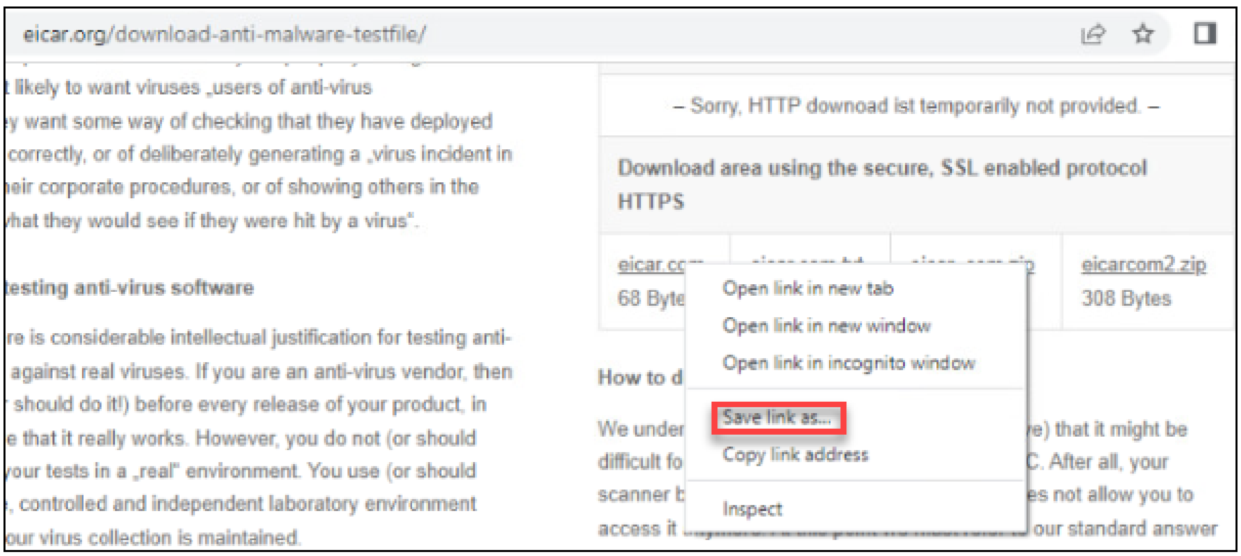
To test endpoint email alerts

1. On the Remote VM, log in with the username `student` and password `Password1!`.
2. Double-click the FortiClient icon, and then verify that the **MALWARE PROTECTION** section is available.
3. On the desktop, open Google Chrome, and then enter `http://eicar.org`.
4. Click **DOWNLOAD ANTI MALWARE TESTFILE**.

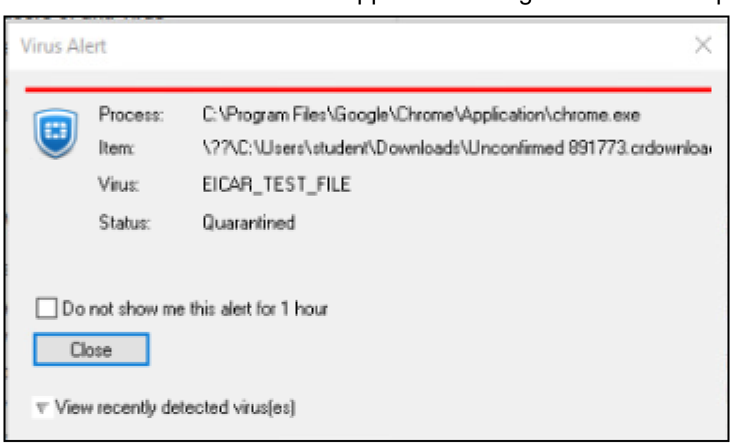
DO NOT REPRINT
© FORTINET



5. In the **Download area using the secure, SSL enabled protocol HTTPS** section, right-click **eicar.com**, and then select **Save link as**.



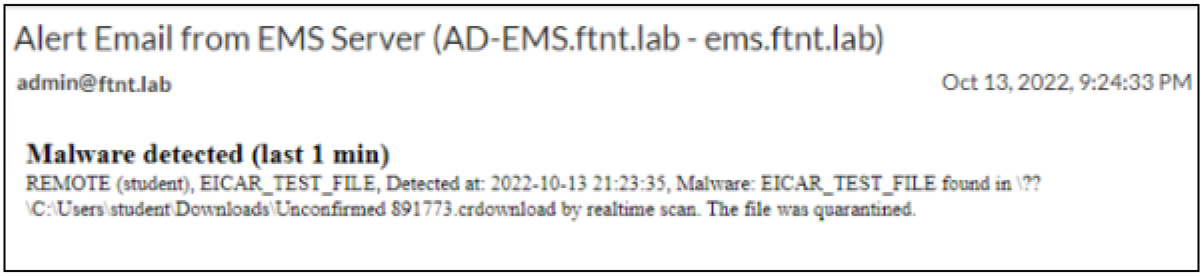
6. Click **Save** to save the file to your **Downloads** folder.
7. In the **Virus Alert** window that appears showing that FortiClient quarantined the file, click **Close**.



8. Return to the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **FortiMail-Webmail** login page bookmark.

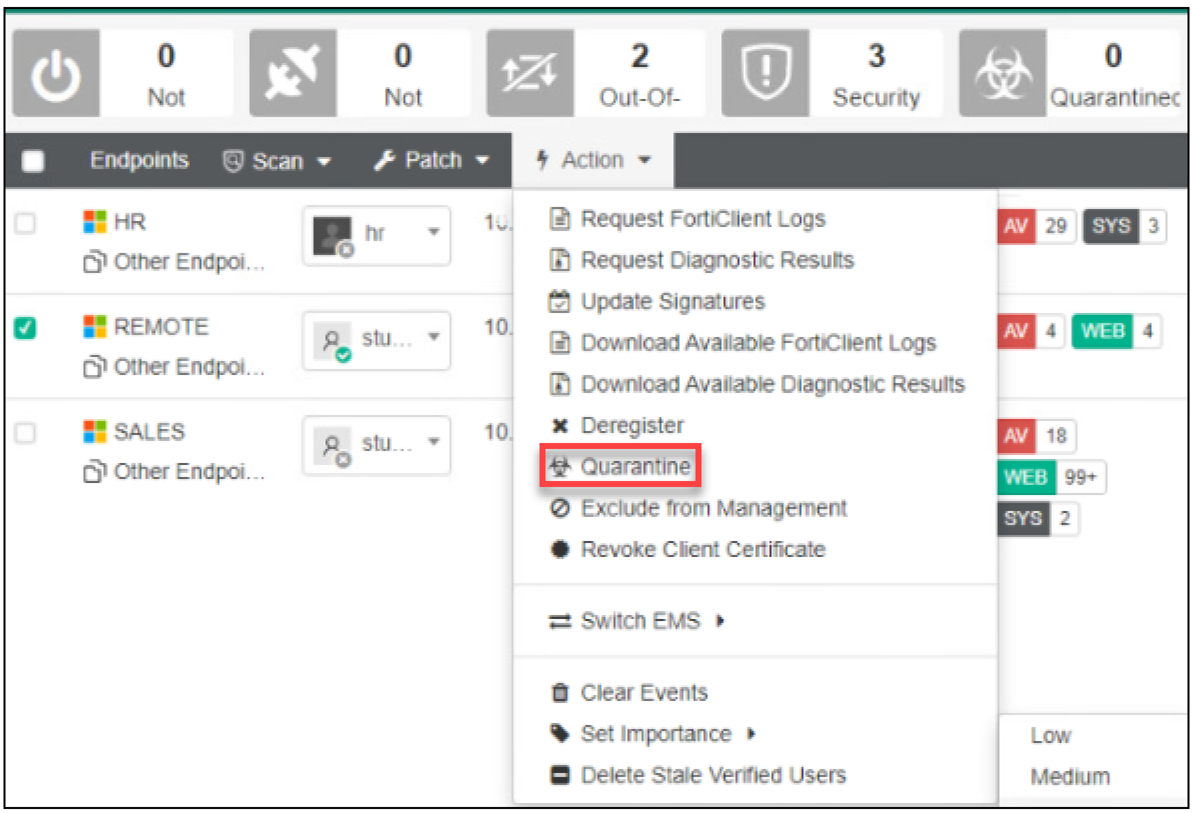
DO NOT REPRINT
© FORTINET

9. Log in with the username `student` and password `Password1!`.
10. Open the new email from `admin@ftnt.lab` to view the **Malware detected** alert email.



In a live environment, administrators can configure endpoint alerts on FortiClient EMS to get email notifications for any malicious activity on FortiClient endpoints, and then take action accordingly.

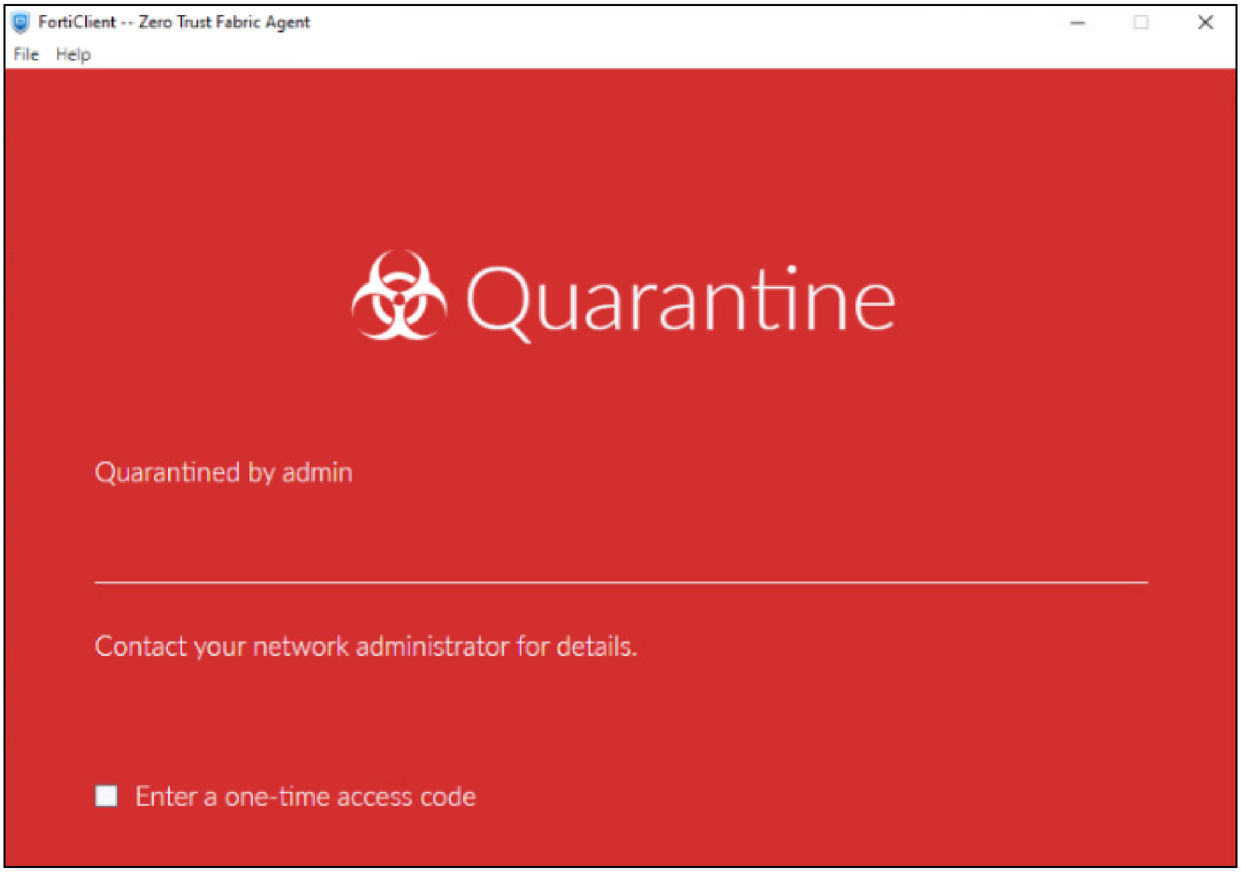
11. Return to the FortiClient EMS GUI, and then click **Endpoints** > **All Endpoints**.
12. In the right section, select the **REMOTE** checkbox, click **Action**, and then click **Quarantine** to block internet access to the malware detected endpoint.



13. Return to the REMOTE VM.

FortiClient shows the quarantine screen and blocks all communication, except to the EMS.

DO NOT REPRINT
© FORTINET



In a real case, you should thoroughly investigate the endpoint, including a virus scan, vulnerability patching, and so on before the endpoint can be unquarantined.

14. Return to the FortiClient EMS GUI, and then click **Endpoints** > **All Endpoints**.
15. In the right section, select the **REMOTE** checkbox, click **Action**, and then click **Unquarantine** to allow internet access.

DO NOT REPRINT
© FORTINET

Exercise 2: Configuring FortiAnalyzer Playbooks to Trigger Automatic Quarantine

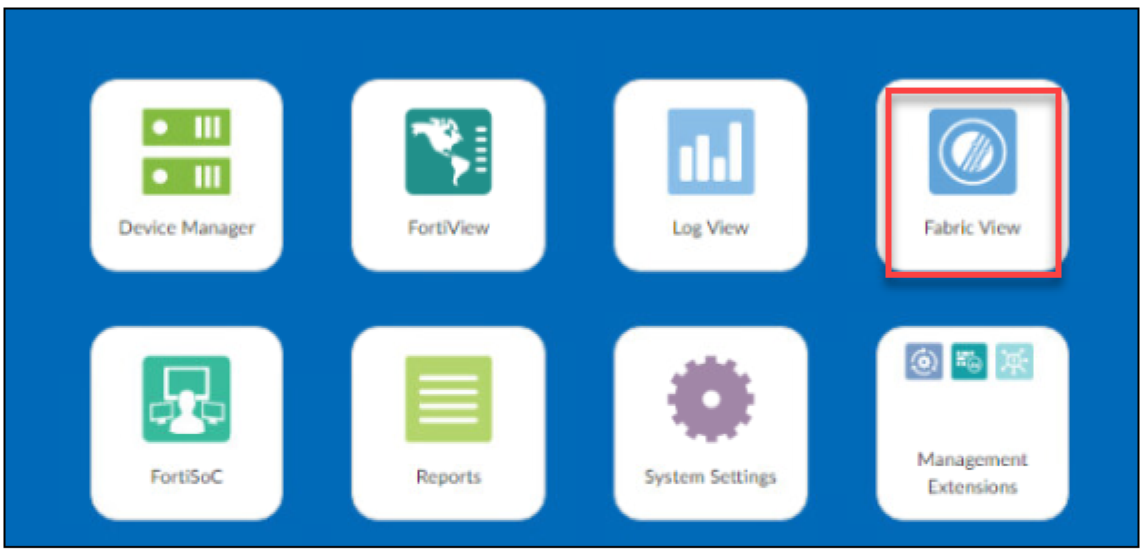
In this exercise, you will configure FortiAnalyzer playbooks to trigger automatic quarantine, based on indicators of compromise (IOC). You will also configure on-demand playbooks on FortiAnalyzer.

Enable the EMS Connector on FortiAnalyzer

You will enable the EMS connector on FortiAnalyzer.

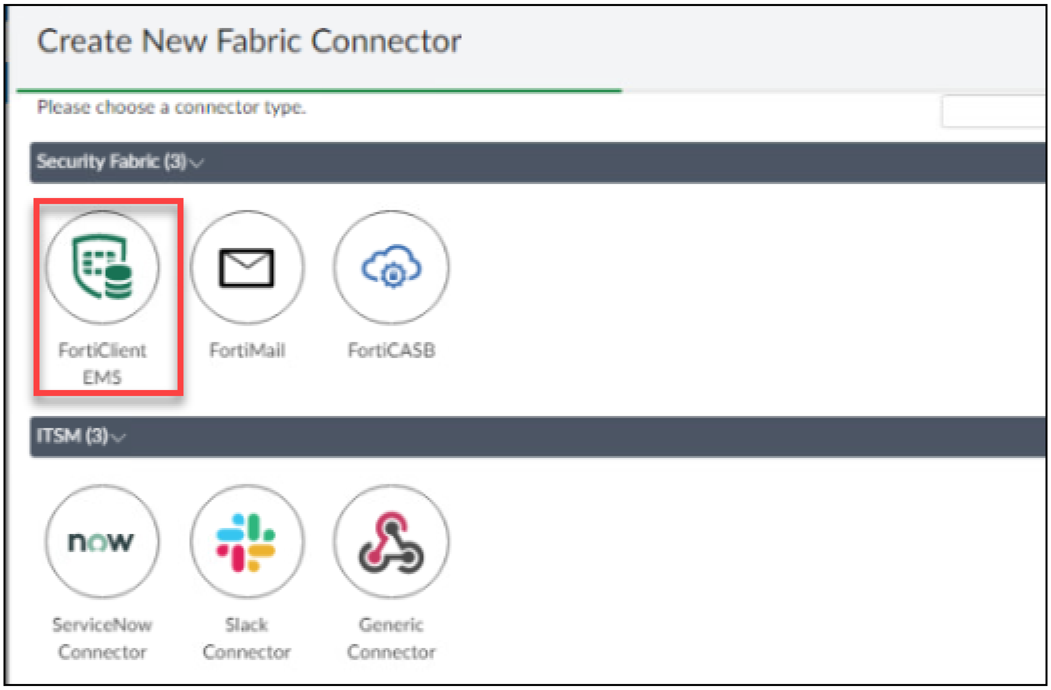
To enable the EMS connector on FortiAnalyzer

1. On the FortiClient EMS VM, open Google Chrome, and then in **Bookmarks**, select the **FortiAnalyzer** login page bookmark.
2. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
3. Click **Fabric View**.



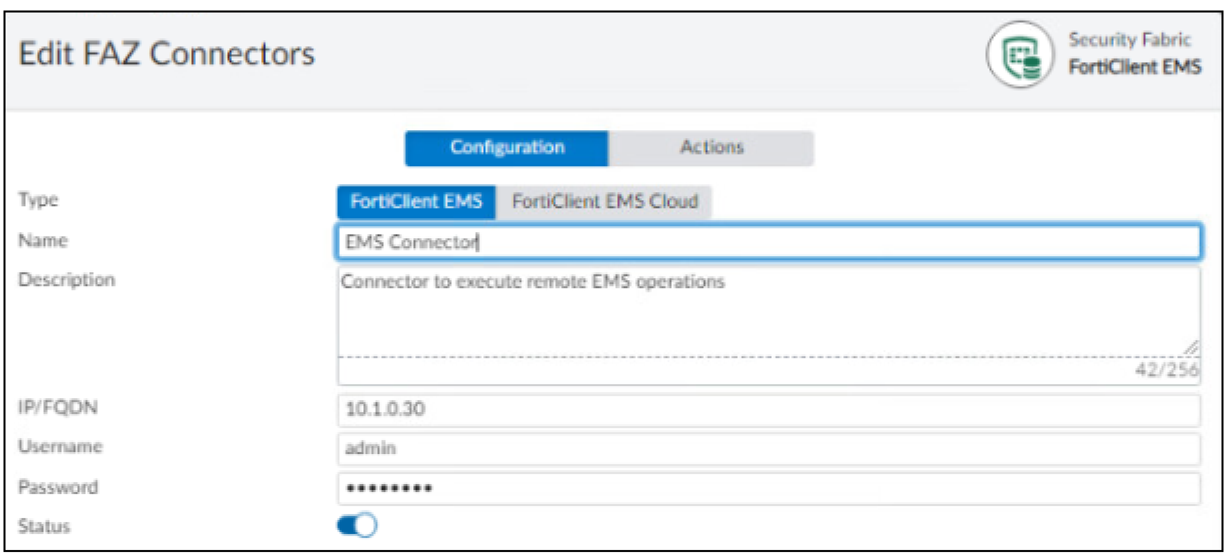
4. Click **Fabric** > **Connectors**, and then click **Create New**.
5. In the **Create New Fabric Connector** window, click **FortiClient EMS**.

DO NOT REPRINT
© FORTINET



6. In the **Create New Fabric Connector** window, configure the following settings:

Field	Value
IP/FQDN	10.1.0.30
Username	admin
Password	Password1!



7. Click **OK** to save the configuration.

DO NOT REPRINT
© FORTINET

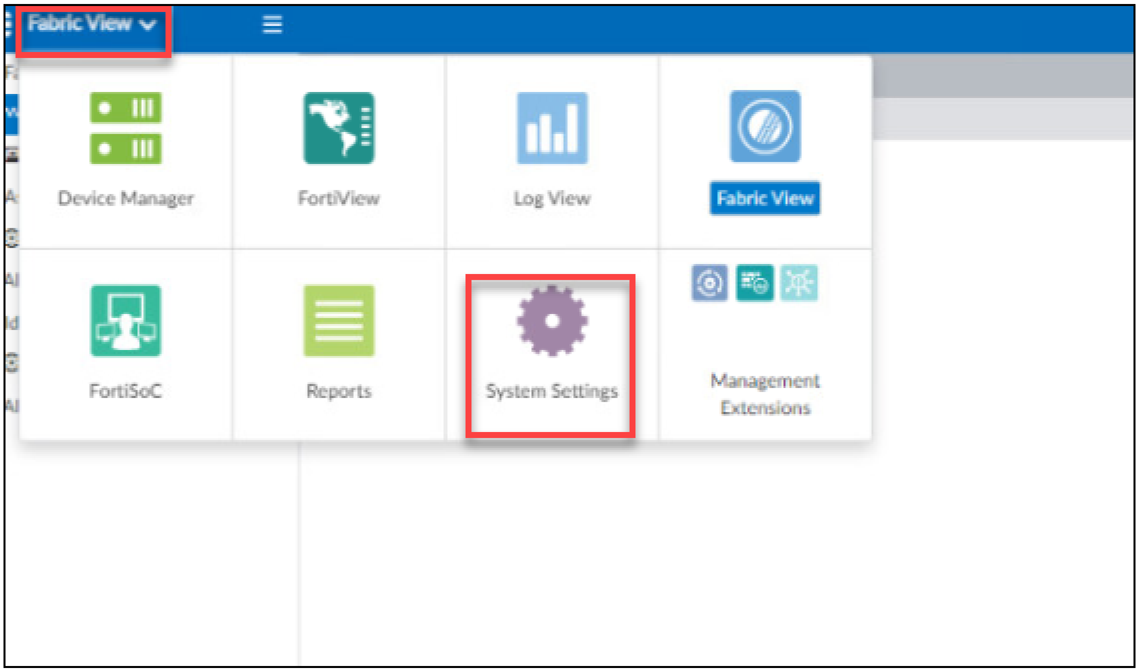
The configuration above gives the FortiAnalyzer API access to FortiClient EMS. FortiAnalyzer can send different actions to FortiClient EMS using playbooks to gather information and for quarantine management.

Configure Playbooks on FortiAnalyzer

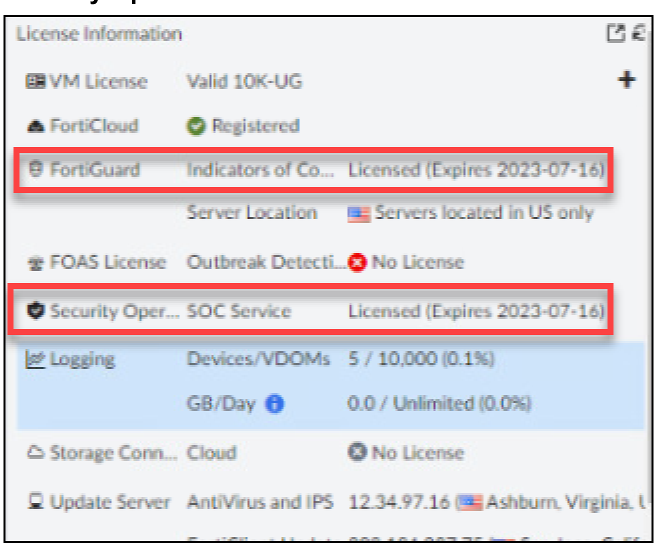
You will configure a playbook based on an event trigger and an on-demand playbook.

To configure a playbook to automatically trigger based on IOC

1. Continuing on the FortiAnalyzer GUI, in the upper-left corner, click **Fabric View**, and then click **System Settings**.



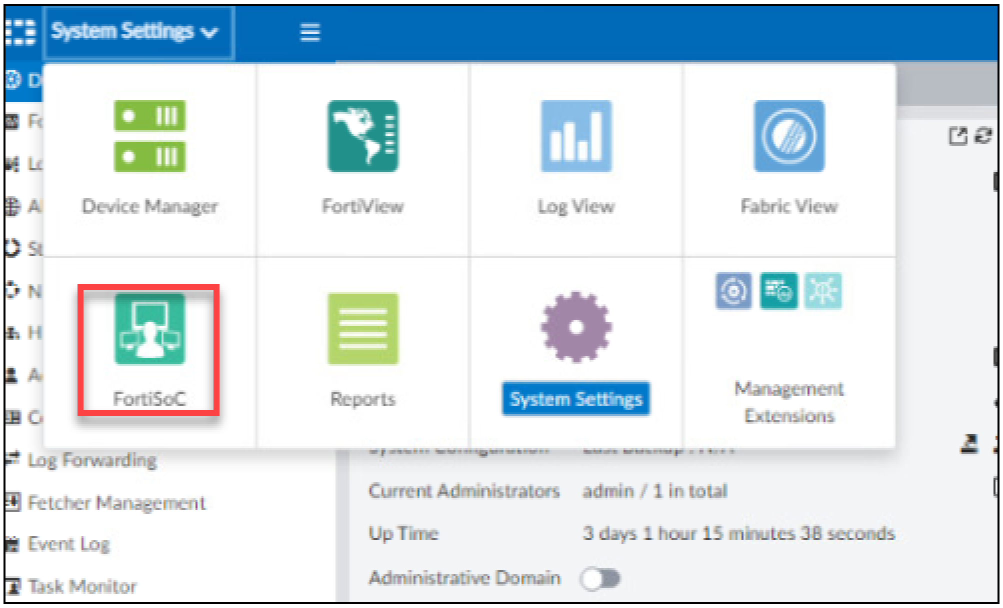
2. In the **License Information** widget, check the status of **FortiGuard Indicators of Compromise Service** and **Security Operation SOC Service**.



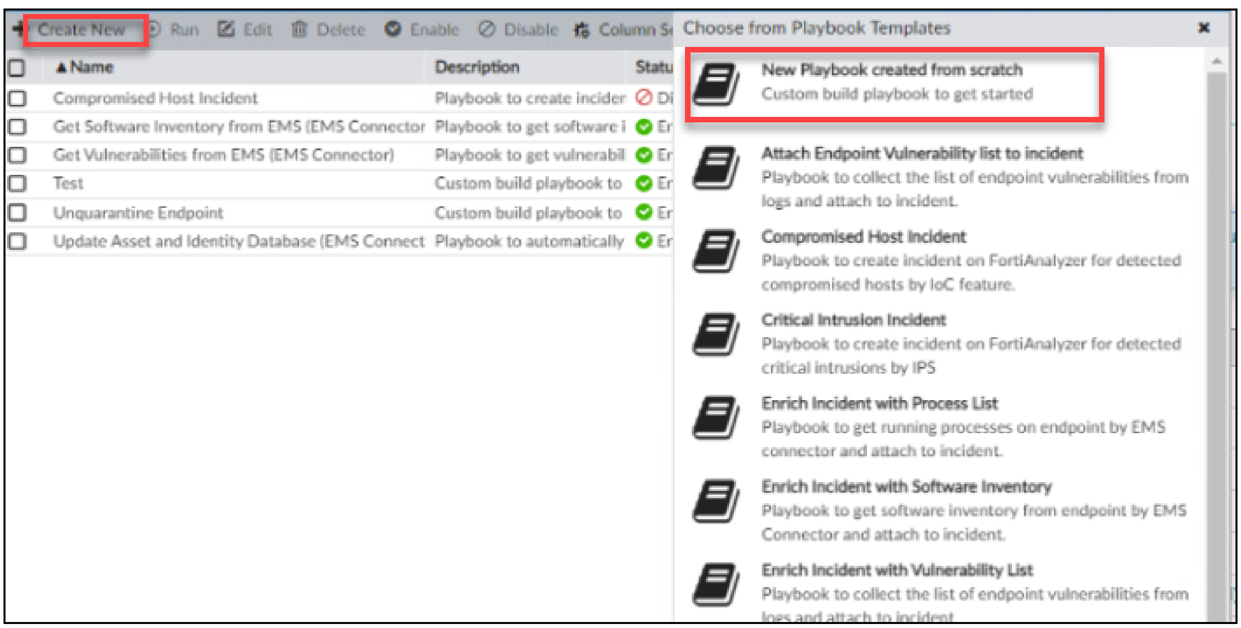
DO NOT REPRINT
© FORTINET

The SOC license allows you to configure and run playbooks on FortiAnalyzer.

3. In the upper-left corner, click **System Settings** > **FortiSoC**.

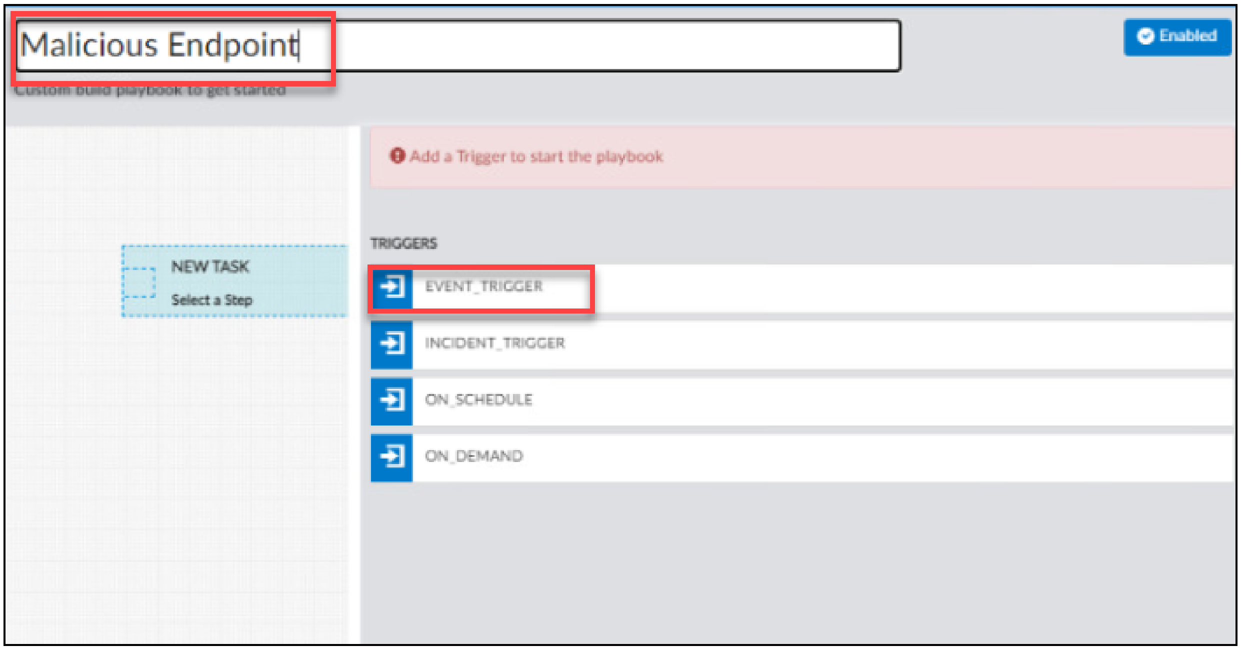


4. Click **Automation** > **Playbook**, and then click **Create New** to create a new playbook.
5. In the **Choose from Playbook Templates** window, select **New Playbook created from scratch**.



6. Name the playbook `Malicious Endpoint`, and then in the **TRIGGERS** section, select **EVENT_TRIGGER**.

DO NOT REPRINT
© FORTINET

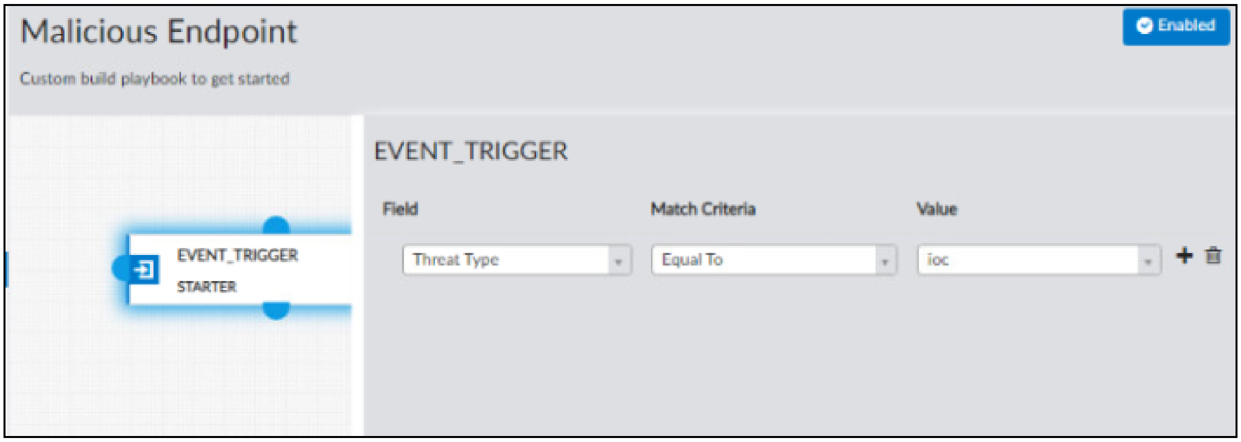


7. In the **EVENT_TRIGGER** window, click **+** to add a new trigger.

8. Configure the following settings:

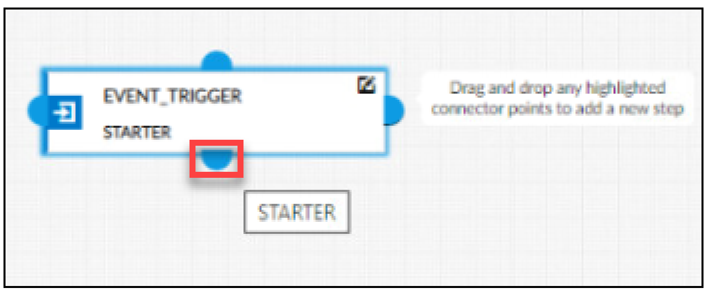
Field	Value
Field	Threat Type
Match Criteria	Equal To
Value	ioc

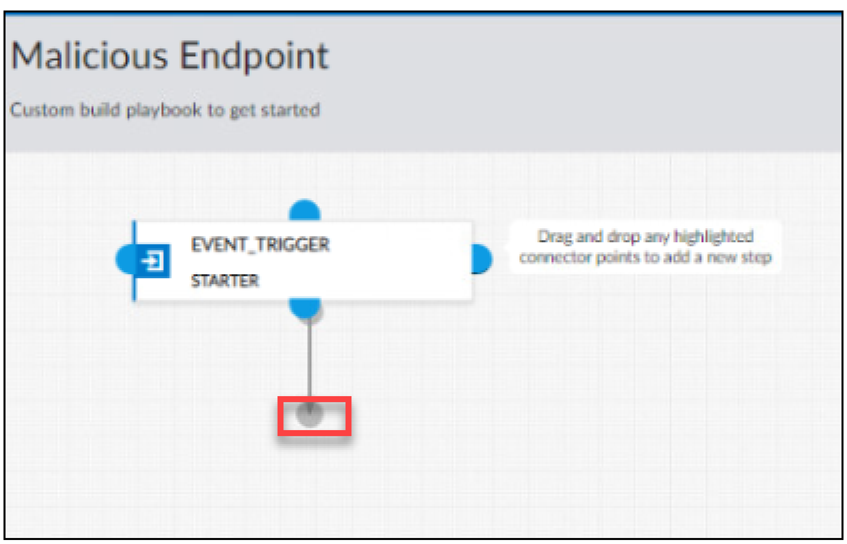
DO NOT REPRINT
© FORTINET



When FortiAnalyzer detects an IOC threat type event, this playbook automatically runs and executes the configured tasks.

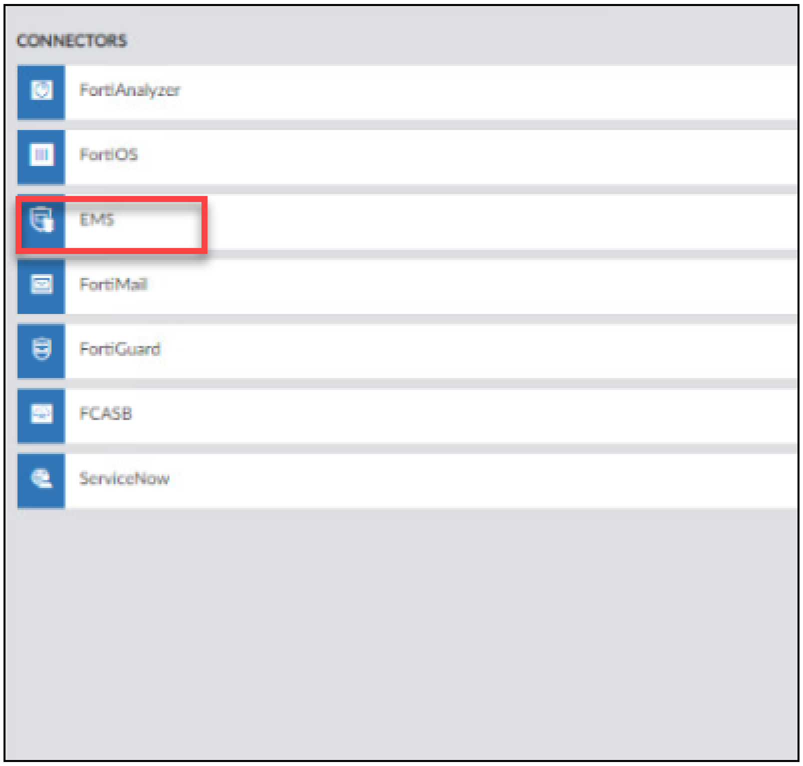
9. Click **OK** to save the trigger.
10. Drag and drop any highlighted connector points to add a new task.





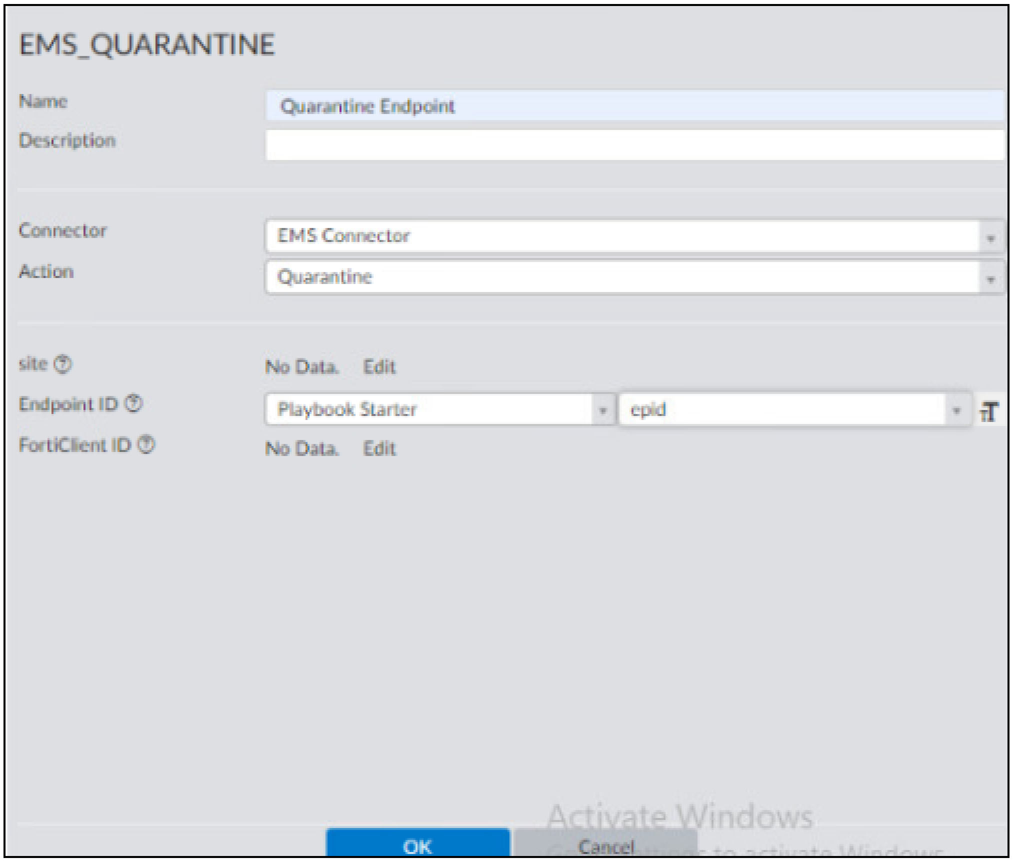
11. In the **CONNECTORS** window, select **EMS**.

DO NOT REPRINT
© FORTINET

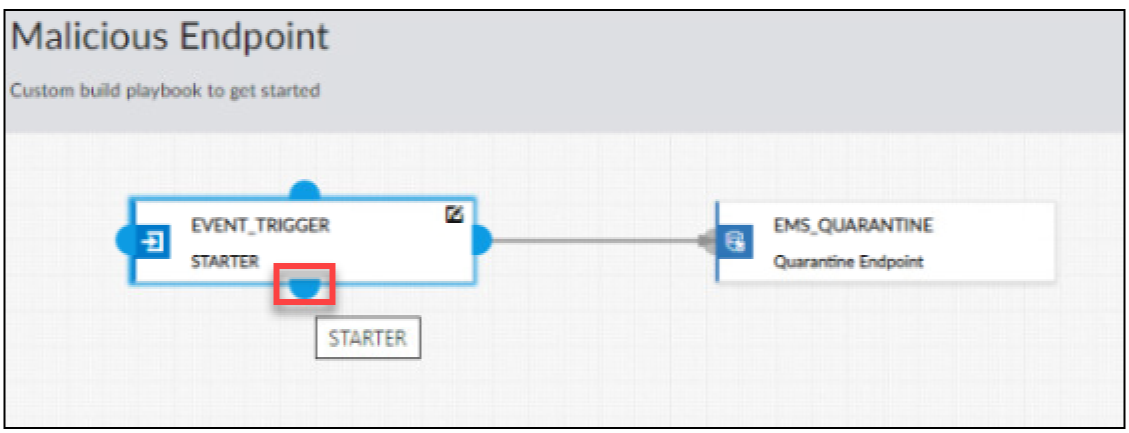


12. In the **Name** field, type `Quarantine Endpoint`.
13. In the **Action** field, select **Quarantine**.
14. In the **Endpoint ID** field, click **Edit**, and then select **epid** as the **Playbook Starter**.
15. Click **OK** to save the task.

DO NOT REPRINT
© FORTINET

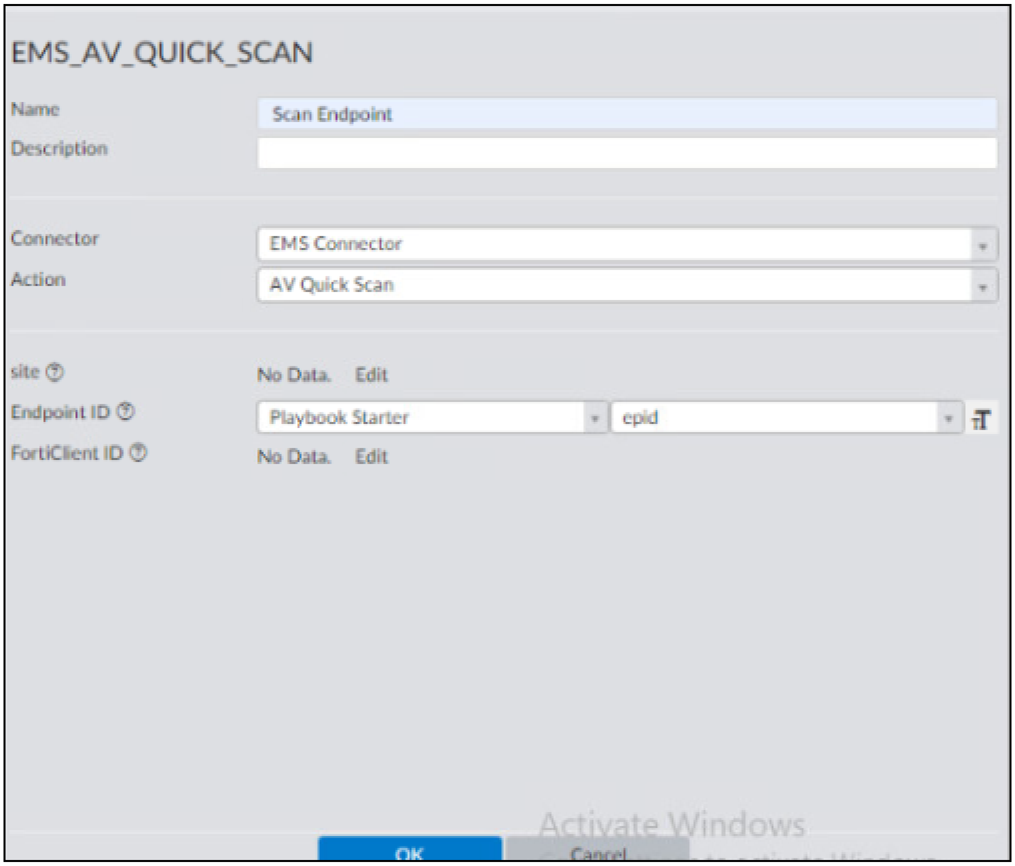


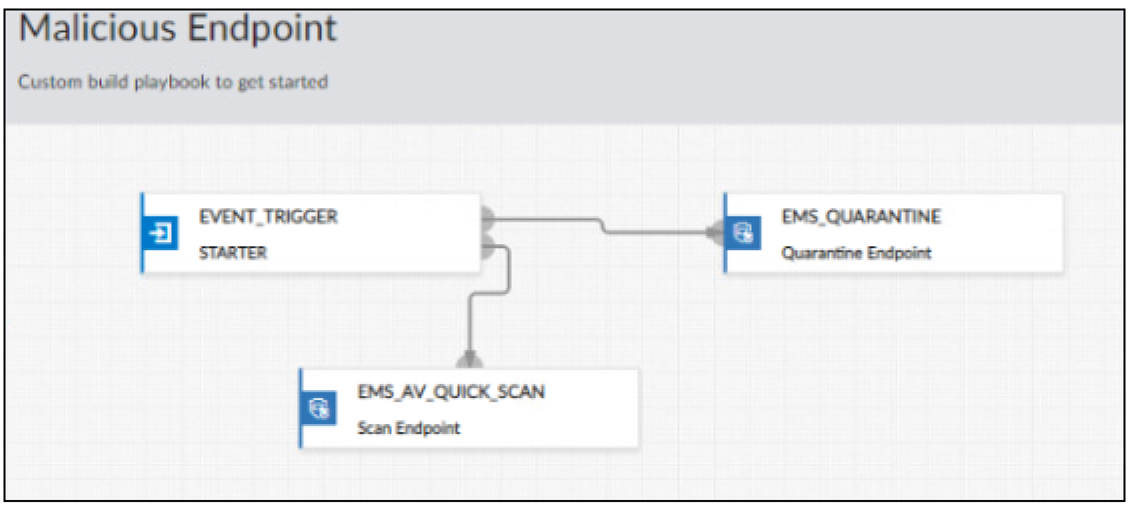
16. Drag and drop any highlighted connector on **EVENT_TRIGGER** to create a new task.



17. In the **CONNECTORS** window, select **EMS**.
18. In the **Name** field, type `Scan Endpoint`.
19. In the **Action** field, select **AV Quick SCAN**.
20. In the **Endpoint ID** field, click **Edit**, and then select **epid** as the **Playbook Starter**.
21. Click **OK** to save the task.

DO NOT REPRINT
© FORTINET



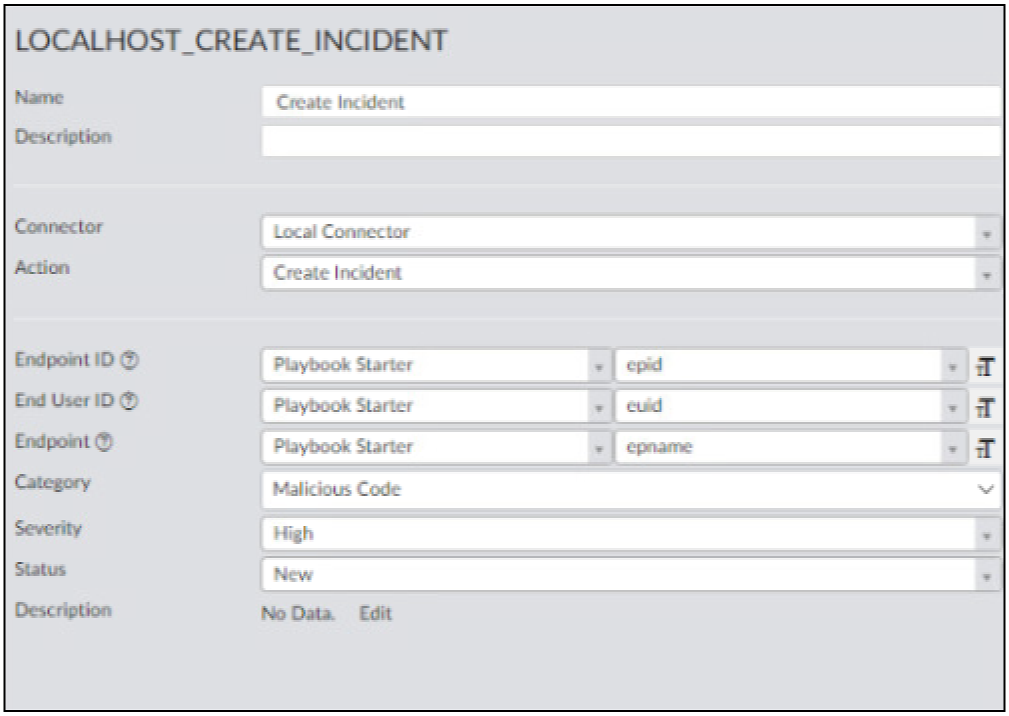


In this lab environment, we are using an AV quick scan instead of an AV full scan. The AV full scan takes a lot more time to complete.

22. Drag and drop any highlighted connector on **EVENT_TRIGGER** to create a new task.
23. In the **CONNECTORS** window, select **FortiAnalyzer**.
24. In the **Name** field, type `Create Incident`.

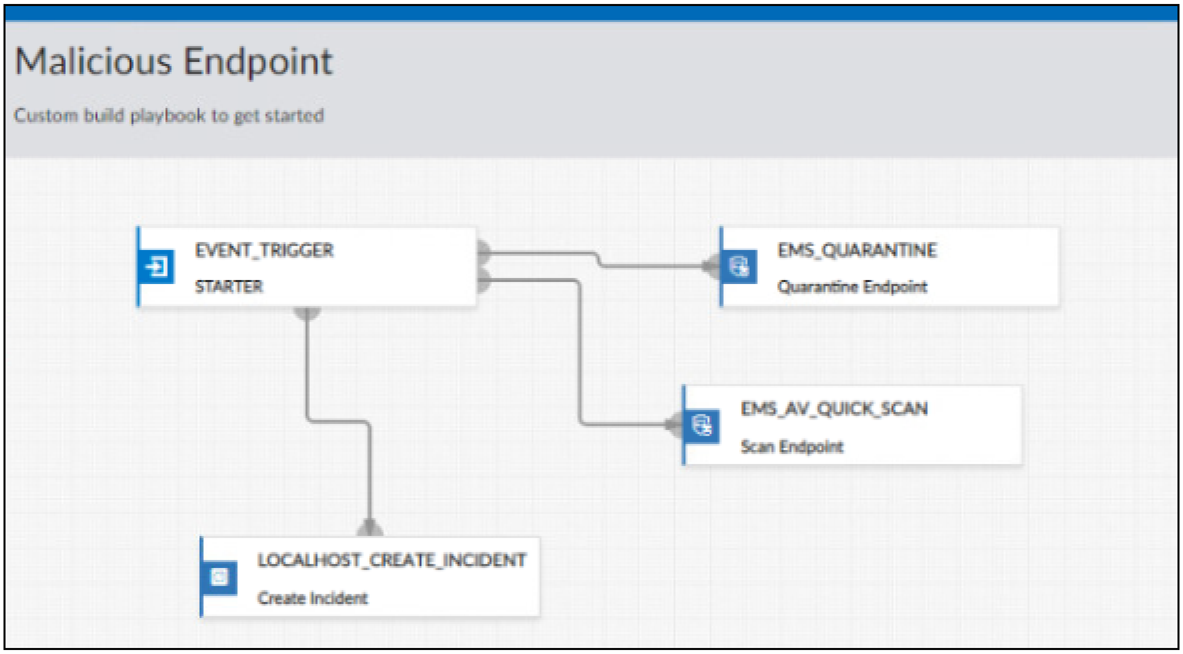
DO NOT REPRINT
© FORTINET

25. In the **Action** field, select **Create Incident**.
26. In the **Endpoint ID** field, click **Edit**, and then select **epid** as the **Playbook Starter**.
27. In the **End User ID** field, click **Edit**, and then select **euid** as the **Playbook Starter**.
28. In the **Endpoint** field, click **Edit**, and then select **epname** as the **Playbook Starter**.
29. In the **Category** field, click **Edit**, and then select **Malicious Code**.
30. In the **Severity** field, select **High**.
31. In the **Status** field, select **New**.
32. Click **OK** to save the task.



FortiAnalyzer creates an incident based on the logs it receives with the endpoint information.

DO NOT REPRINT
© FORTINET



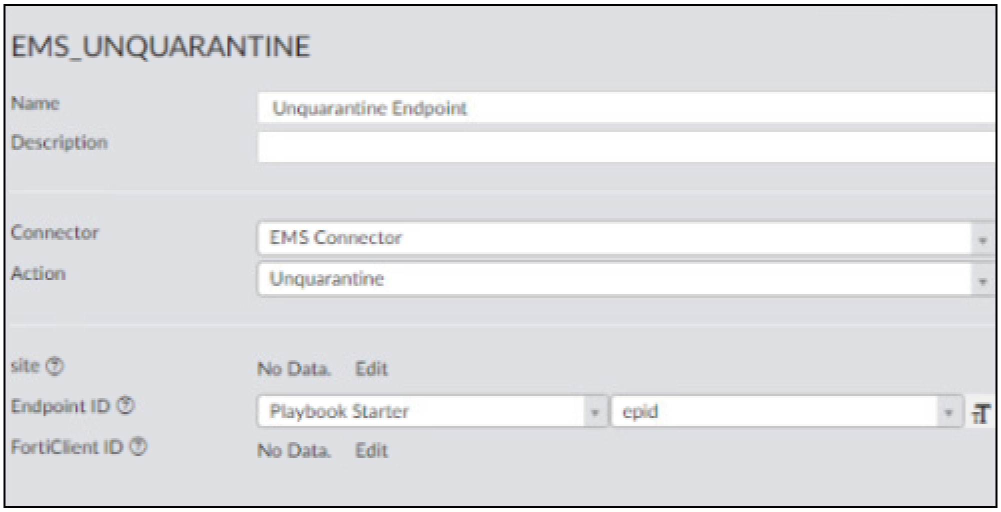
33. Click **Save Playbook** to save the playbook configuration.

    When FortiAnalyzer detects an IOC threat type event on an endpoint, this playbook automatically runs to quarantine the endpoint and runs a quick antivirus scan using an API. It also creates an incident on FortiAnalyzer.

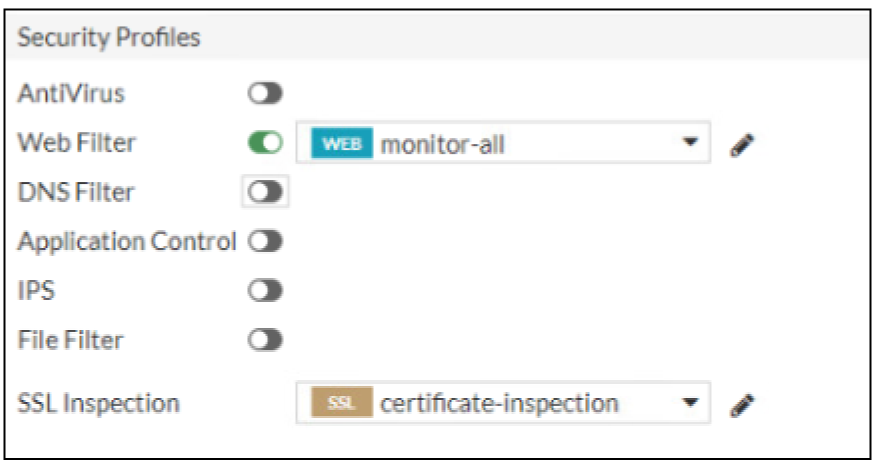
To configure a playbook with an on-demand trigger

1. Continuing on the FortiAnalyzer GUI, click **Create New** to create a new playbook.
2. In the **Choose from Playbook Templates** window, select **New Playbook created from scratch**.
3. Name the playbook `Unquarantine Endpoint`, and then in the **TRIGGERS** section, select **ON_DEMAND**.
4. Click **OK** to create an **ON_DEMAND** task.
5. Drag and drop any highlighted connector points to add a new task.
6. In the **CONNECTORS** window, select **EMS**.
7. In the **Name** field, type `Unquarantine Endpoint`.
8. In the **Action** field, select **Unquarantine**.
9. In the **Endpoint ID** field, click **Edit**, and then select **epid** as the **Playbook Starter**.
10. Click **OK** to save the task.

DO NOT REPRINT
© FORTINET



11. Click **Save Playbook** to save the playbook configuration.
12. Open a new tab in Google Chrome, and then in **Bookmarks**, select the **ISFW** login page bookmark.
13. Log in to the ISFW GUI with the username `admin` and password `password`.
14. Click **Policy & Objects** > **Firewall Policy**.
15. Edit the **Allow_Internet** policy.
16. Enable **Web Filter**, and then select **monitor-all**.
17. Enable **SSL Inspection**, and then select **certificate-inspection**.



18. Click **OK** to save the firewall configuration.

FortiAnalyzer uses web filter, traffic, and security logs from FortiGate to analyze traffic for IOC events.

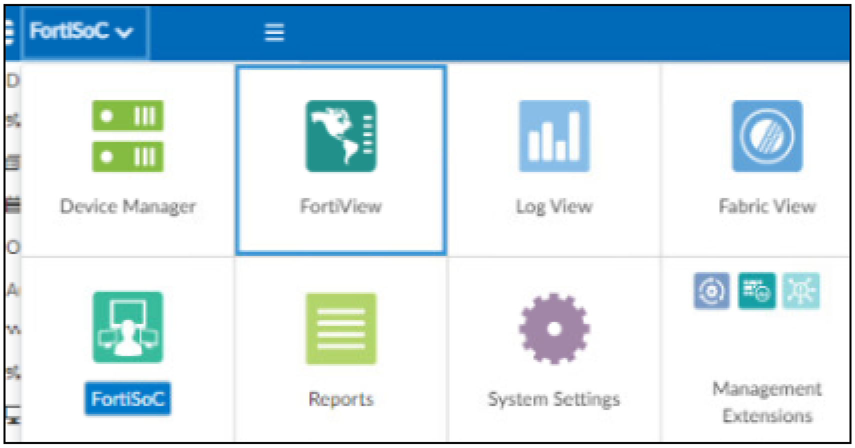
Test FortiAnalyzer Playbooks

You will test the playbooks you configured in the previous task.

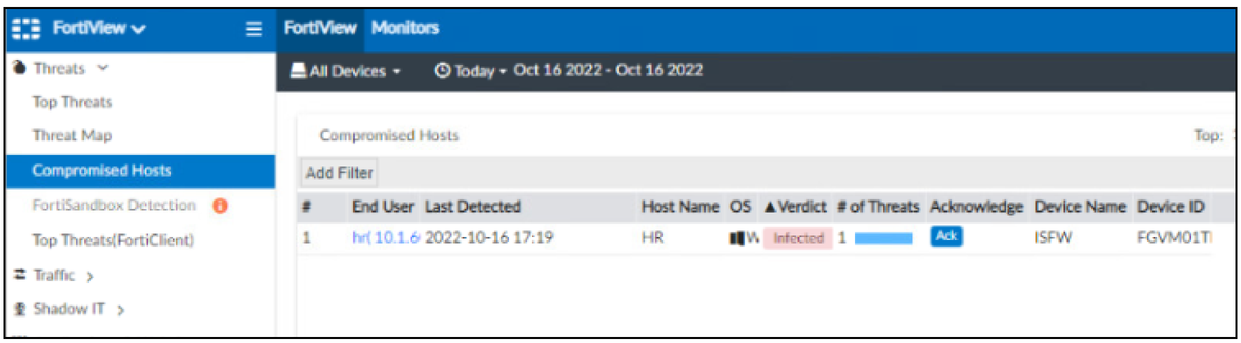
DO NOT REPRINT
© FORTINET

To test automatic and on-demand playbooks by IOC detection

1. On the HR VM, log in with the username `ftnt.lab\hr` and password `Password1!`, open Google Chrome, and then enter `http://voiceoverjobsonline.co.uk` to access the web page.
2. On the FortiClient EMS VM, return to the FortiAnalyzer GUI, in the upper-left corner, click **FortiSoC**, and then click **FortiView**.

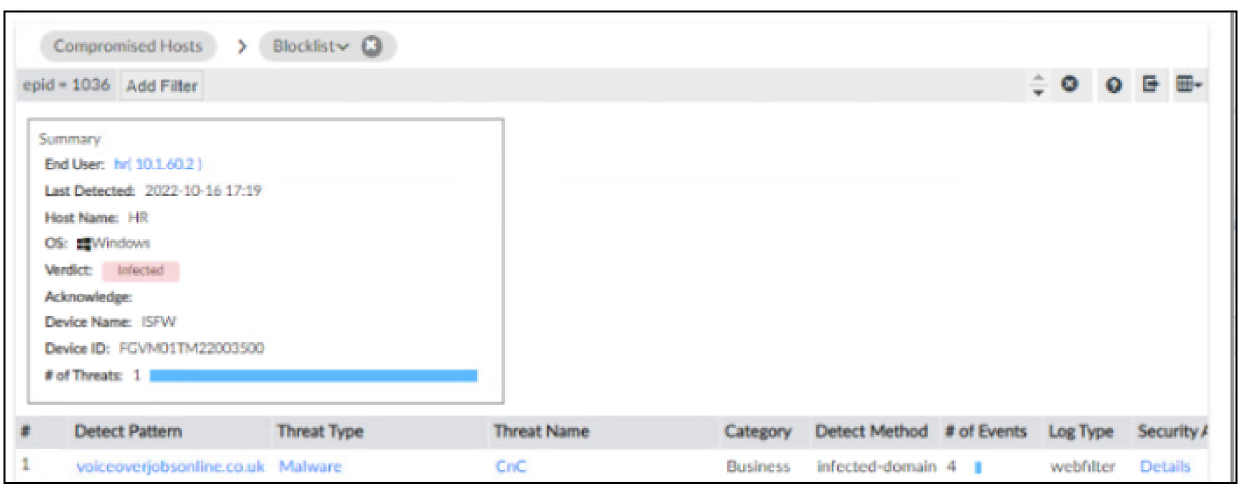


3. Click **Threats** > **Compromised Hosts**.



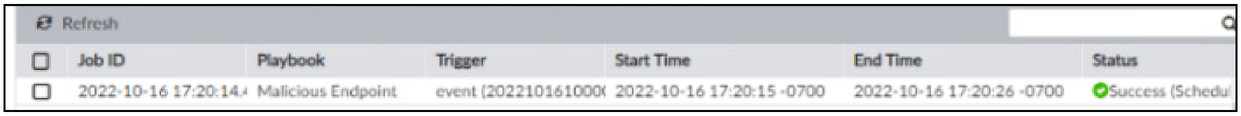
The endpoint appears in the window.

4. Double-click the host to see the details.



DO NOT REPRINT
© FORTINET

5. In the upper-left corner, click **FortiView**, and then click **FortiSoC**.
6. Click **Automation** > **Playbook Monitor**.

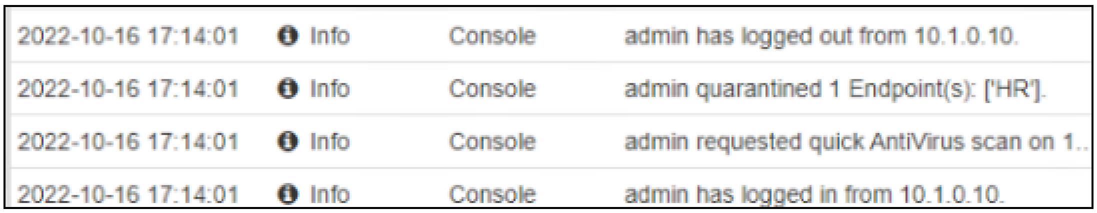


Job ID	Playbook	Trigger	Start Time	End Time	Status
2022-10-16 17:20:14.4	Malicious Endpoint	event (202210161000(	2022-10-16 17:20:15 -0700	2022-10-16 17:20:26 -0700	Success (Schedu

You can see that the **Malicious Endpoint** playbook triggered because of an event.

The **Malicious Endpoint** playbook you configured earlier has a task set to automatically run when an IOC event is detected.

7. Return to the FortiClient EMS GUI, and then log in with the username `admin` and password `Password1!`.
8. In the left menu, click **Administration** > **Log Viewer** to see the FortiAnalyzer API request.

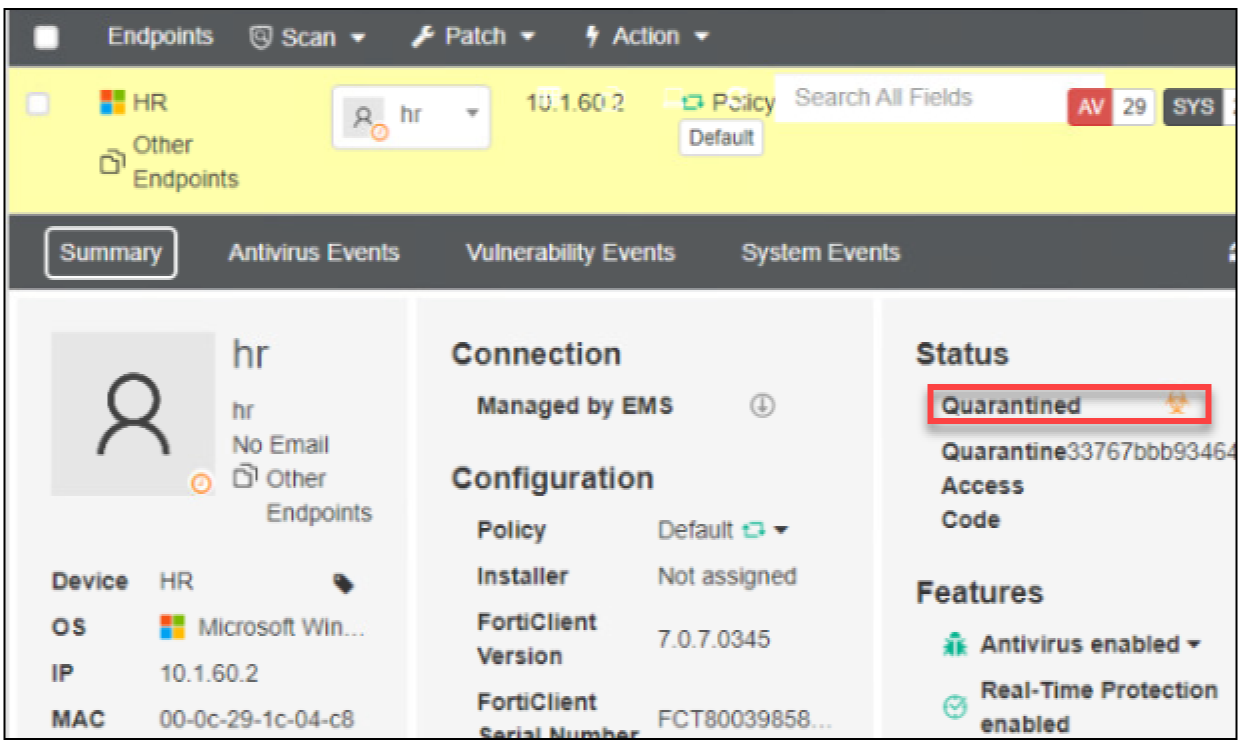


2022-10-16 17:14:01	Info	Console	admin has logged out from 10.1.0.10.
2022-10-16 17:14:01	Info	Console	admin quarantined 1 Endpoint(s): ['HR'].
2022-10-16 17:14:01	Info	Console	admin requested quick AntiVirus scan on 1...
2022-10-16 17:14:01	Info	Console	admin has logged in from 10.1.0.10.

The IP address of the FortiAnalyzer is **10.1.0.10** and it is performing the actions configured in the playbook.

9. In the left menu, click **Endpoints** > **All Endpoints**, and then click **HR**.

   The endpoint is **Quarantined**.

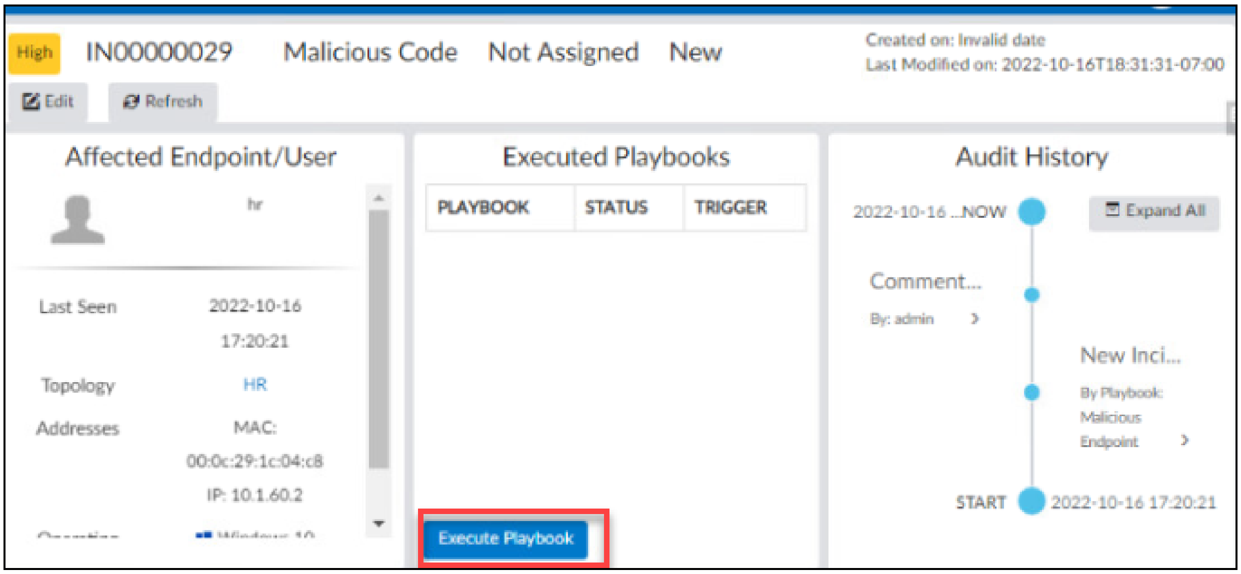


DO NOT REPRINT
© FORTINET

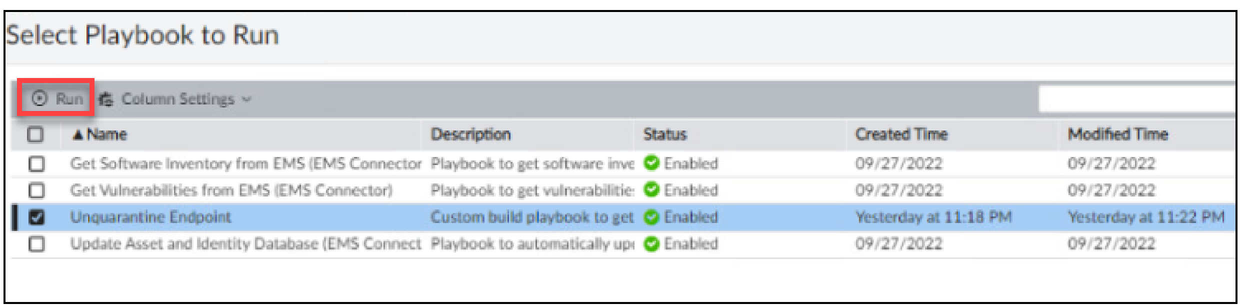
10. Return to the FortiAnalyzer GUI, and then click **FortiSoC** > **Incidents**.
11. Double-click the incident that has been created for the infected endpoint.

The SOC team can investigate the logs of the infected endpoint manually or configure the playbooks to attach the events to the playbook and take the necessary remediation actions.

12. In the **Execute Playbooks** section of the incident, click **Execute Playbook**.



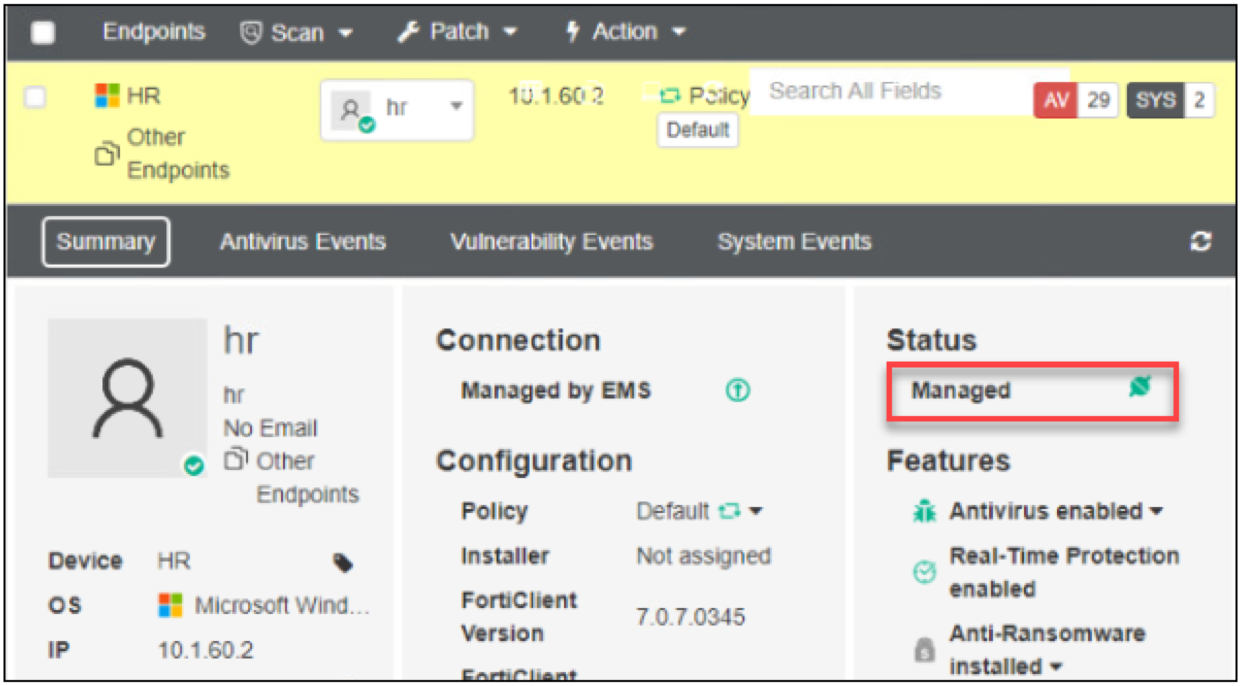
13. In the **Select Playbook to Run** window, select **Unquarantine Endpoint**, and then click **Run**.



14. In the **Manually Run Playbook** window, click **OK** to run the playbook.
15. Click **Close**.
16. Return to the FortiClient EMS GUI, click **Endpoints** > **All Endpoints**, and then click **HR**.

    The endpoint has changed from **Quarantined** to **Managed**.

DO NOT REPRINT
© FORTINET



DO NOT REPRINT
© FORTINET

Exercise 3: Configuring Automated Response With FortiNAC

In this exercise, you will create security incident rules to use the logs from FortiGate to trigger an automated response and disable offending hosts. You have already created a firewall policy with a web filter profile with logging enabled in the previous exercise—you will reuse the same policy in this exercise.

Configure Security Incident Rules

FortiGate was preconfigured to forward logs to FortiNAC. You will now create a parser to interpret those logs, and then create security incident rules to take automated actions on the offending hosts.

To configure security incident rules

1. On the FortiClient EMS VM, open PuTTY, and then connect over SSH to the **ISFW** saved session.
2. Log in with the username `admin` and password `password`.
3. Enter the following commands to configure the syslog filters:

```
config log syslogd filter
set forward-traffic enable
config free-style
edit 0
set category webfilter
set filter "(logid 0317013312)"
end
end
```

The above configuration will forward logs to syslog for particular events instead of collecting for the entire category. Log ID 0317013312 is for webfilter logs.

4. Open Google Chrome, and then in **Bookmarks**, select the **FortiNAC** login page bookmark.
5. Log in to the FortiNAC GUI with the username `admin` and password `Password1!`.
6. Click **System** > **Settings**, expand **System Communication** > **Security Event Parsers** , click **Add**, and then configure the following settings to create a parser to help FortiNAC understand logs that FortiGate sent:

Field	Value
Enabled	Select the checkbox.
Name	FortiGate

DO NOT REPRINT
© FORTINET

Field	Value
Vendor	Fortinet
Format	Tag/Value
Field Delimiter	<blank space>
Tag/Value Delimiter	=

7. In the **Data Fields** section, configure the following settings:

Data field	Data field drop-down	Value
Source IP Column/Tag	Entire Column/Tag	srcip
Destination IP Column/Tag	Entire Column/Tag	dstip
Type Column/Tag	Entire Column/Tag	type
Subtype Column/Tag	Entire Column/Tag	subtype
Threat ID Column/Tag	Entire Column/Tag	logid
Description Column/Tag	Entire Column/Tag	msg
Severity Column/Tag	Entire Column/Tag	level

8. Click the **Severity Mappings** section, click **Add**, configure the following settings, and then click **OK**:

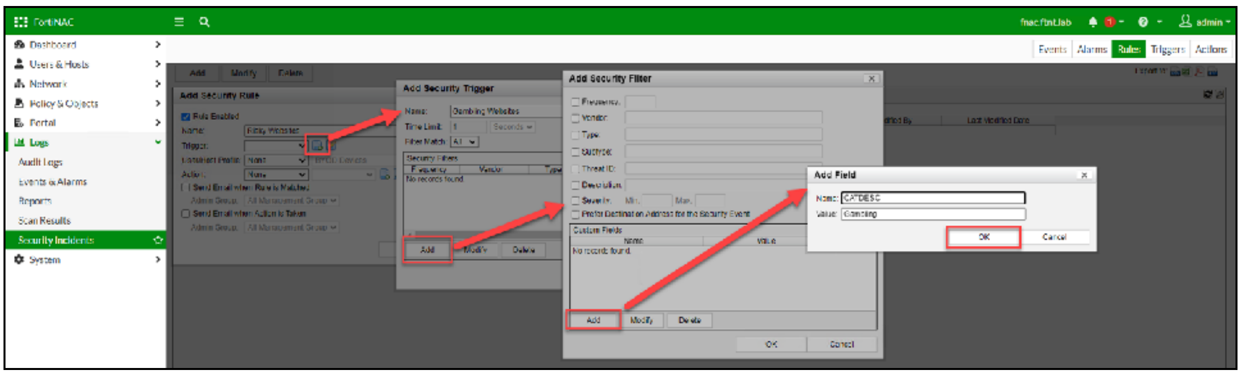
Source Value	Severity Value
critical	8
alert	7
emergency	10
warning	5
information	1
error	9
notice	3

9. Click **Network** > **Inventory**, expand **Firewall** > **ISFW.ftnt.lab**, click the **Element** tab, in the **Incoming Events** field, select **Security Events**, and then select the new **FortiGate** parser.
10. Click **Save**.
11. Click **Logs** > **Security Incidents**, and then on the right, click **Rules**.
12. Click **Add** to create a new security rule.
13. In the **Add Security Rule** window, in the **Name** field, type `Risky Websites`.
14. In the **Trigger** field, click the **Add** icon to create a new trigger.

DO NOT REPRINT
© FORTINET

15. In the **Add Security Trigger** window, in the **Name** field, type `Gambling Websites`.
16. In the **Security Filters** section, click **Add**.
17. In the **Add Security Filter** window, in the **Custom Fields** section, click **Add**.
18. In the **Add Field** window, configure the following settings to match gambling websites with the following values, and then click **OK** until you return to the **Add Security Rule** window:

Source Value	Severity Value
Name	CATDESC
Value	Gambling



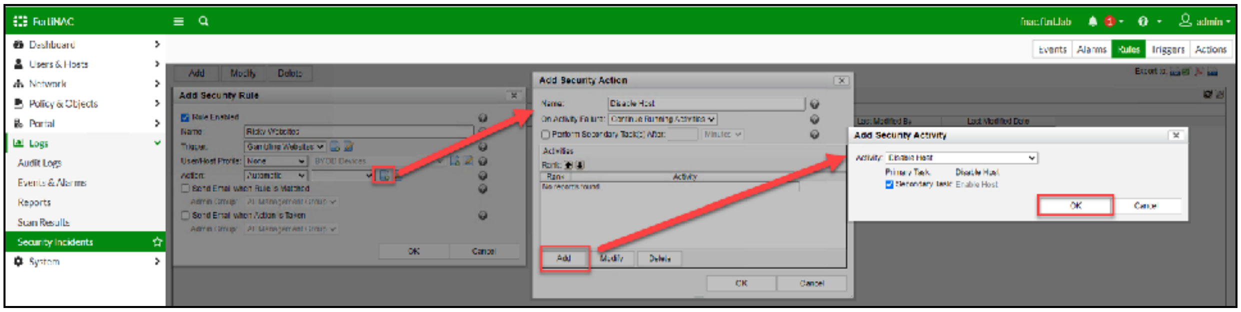
This lab uses gambling websites and the web filter profile as an example, but you should be able to take automated response actions for any category or UTM profile that would generate a log.

19. In the **Action** field, select **Automatic**, and then click the **Add** icon.
20. In the **Add Security Action** window, configure the following settings to create an action:

Source Value	Severity Value
Name	Disable Host
On Activity Failure	Continue Running Activities

21. In the **Activities** section, click **Add**.
22. In the **Add Security Activity** window, in the **Activity** field, select **Disable Host**, select the **Secondary Task** checkbox, click **OK** until you return to the **Add Security Rule** window, and then click **OK** again.

DO NOT REPRINT
© FORTINET

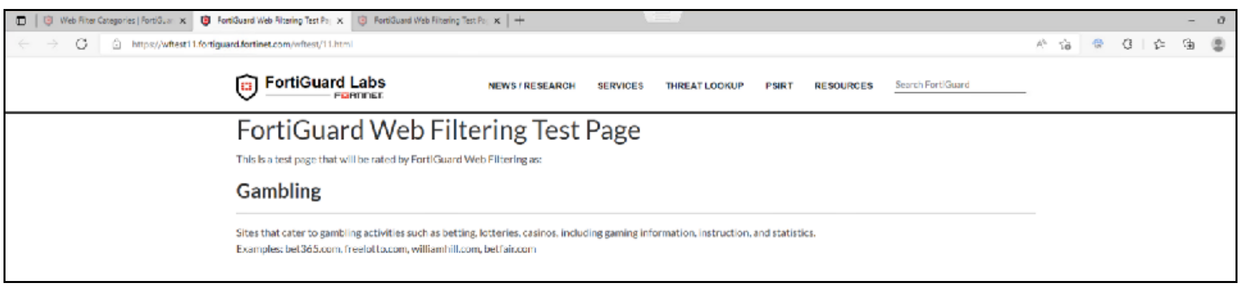


Test Automated Response

You will use the SALES VM to test the automated response of FortiNAC after navigating to a test site in the gambling category.

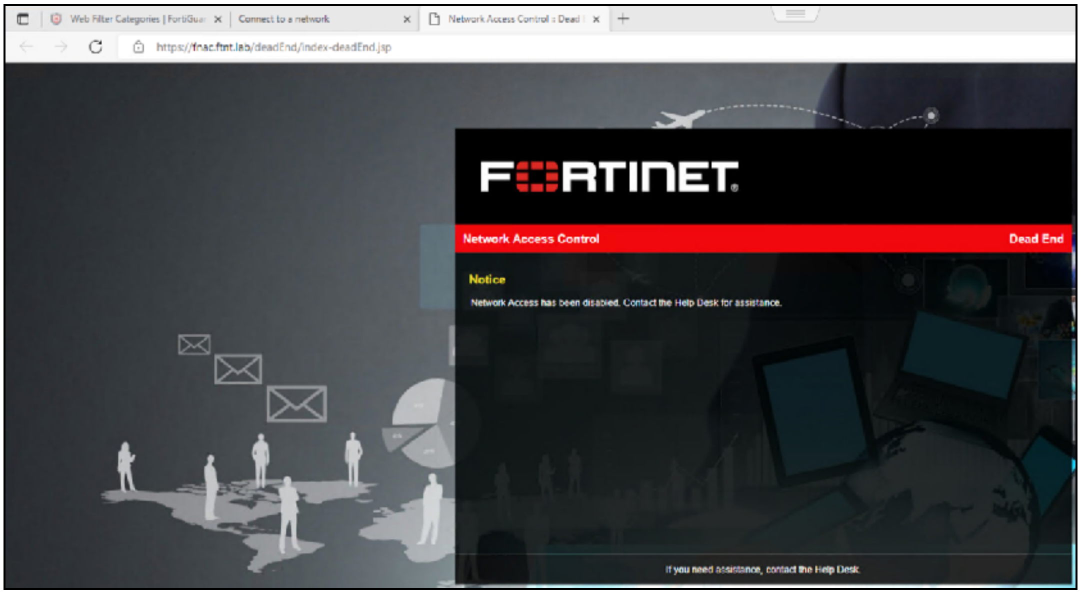
To test automated response

1. On the SALES VM, log in with the username `sales` and password `Password1!`.
2. Open Google Chrome, and then navigate to the Fortinet test website for the gambling category at `https://wftest11.fortiguard.fortinet.com/wftest/11.html` to reach the test site, as shown in the following image:



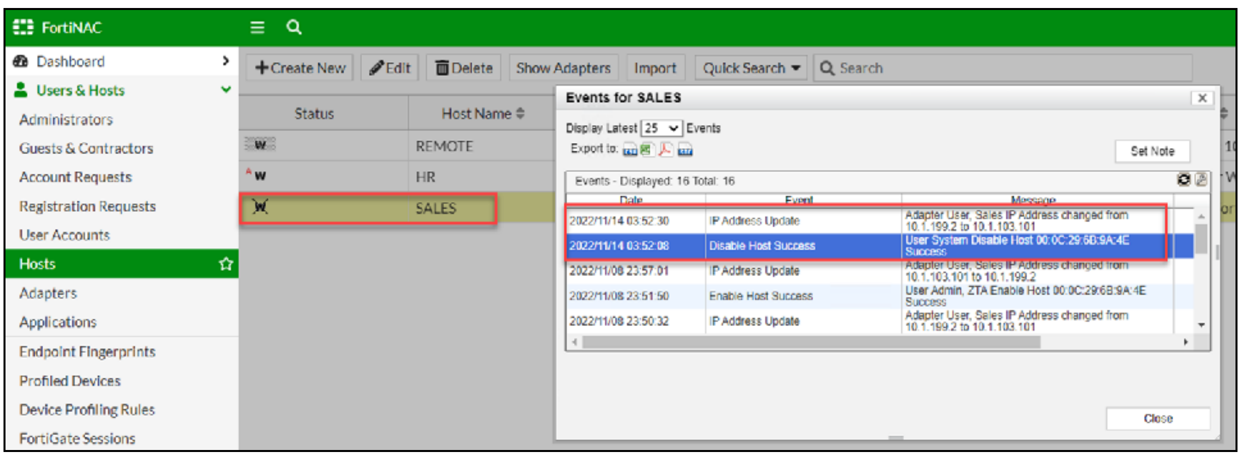
It may take 2–3 mins for FortiNAC to receive and process the logs from ISFW, and then disable the host. If you try to access any web page now, you should be redirected to a **Dead End** page, as shown in the following image:

DO NOT REPRINT
© FORTINET

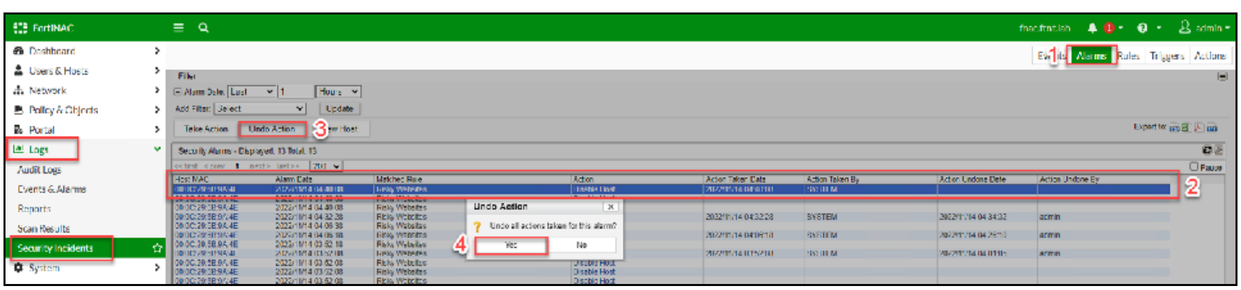


3. On the FortiClient EMS VM, return to the FortiNAC GUI, click **Users & Hosts** > **Hosts**, right-click the **SALES** host, and then select **Show Events** to validate those actions have been taken by FortiNAC.

   You should notice a **Dead End** icon and log associated with it.

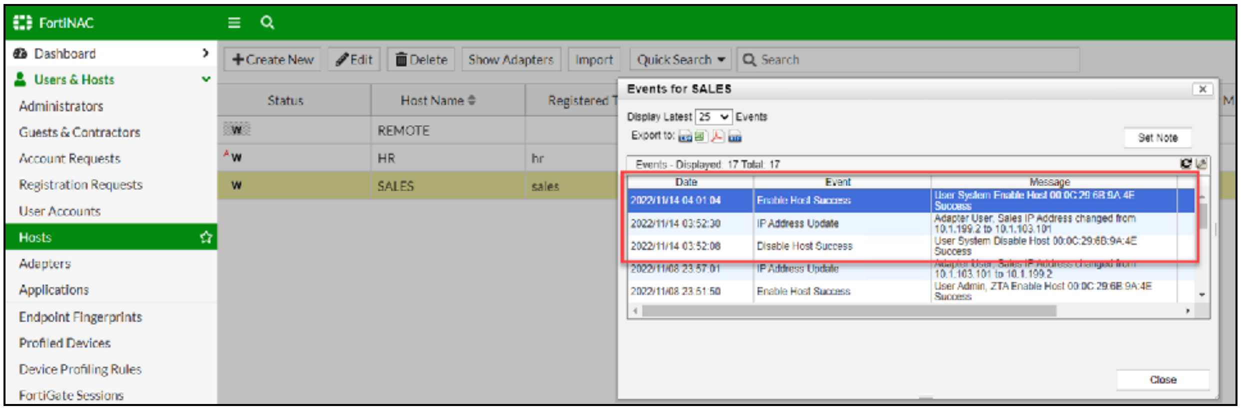


4. To revert the actions performed on the host, navigate to **Logs** > **Security Incidents**, click **Alarms**, select the previously generated alarm, and then click **Undo Action**.
5. Click **Yes** to continue.



6. Click **Users & Hosts** > **Hosts**, right-click the **SALES** host, and then select **Show Events** to validate that the access has been restored.

DO NOT REPRINT
© FORTINET



DO NOT REPRINT
© FORTINET

FORTINET

No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from Fortinet Inc., as stipulated by the United States Copyright Act of 1976.

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations,and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.