

DO NOT REPRINT
© FORTINET

Brave-Dumps.com



FortiClient EMS Administrator Lab Guide

FortiClient EMS 7.4

FORTINET
Training Institute

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

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>



3/14/2025

TABLE OF CONTENTS

Change Log	6
Network Topology	7
Lab 1: FortiClient EMS Installation	8
Exercise 1: Accessing the FortiClient EMS GUI	9
Access the FortiClient EMS GUI and Install the License.	9
Lab 2: System Administration	14
Exercise 1: Configuring FortiClient EMS System Settings	15
Configure Server Settings	15
Configure Log Settings	18
Configure Login Banner Settings	19
Exercise 2: Configuring SAML SSO for FortiClient EMS Administrator Login	21
Verify IdP Settings on FortiAuthenticator	21
Configure FortiClient EMS as an SP for Administrator SSO Login	21
Test SAML SSO Authentication for FortiClient EMS Login	25
Lab 3: FortiClient Deployment	28
Exercise 1: Creating a FortiClient Installer and an Invitation	31
Exercise 2: Installing FortiClient on Ubuntu Linux Endpoints	35
Exercise 3: Importing Endpoints to FortiClient EMS	37
Exercise 4: Installing FortiClient on AD Endpoints	40
Exercise 5: Registering FortiClient on FortiClient EMS Using an Invitation Code	43
Lab 4: Endpoint Policy Provisioning	45
Exercise 1: Creating an Endpoint Group, a Group Assignment Rule, and an Endpoint Policy	46
Create an Endpoint Group for a Linux Workgroup	46
Create a Group Assignment Rule for Linux Endpoints	48
Create and Assign an Endpoint Policy to a Workgroup	49
Exercise 2: Configuring On-Fabric Detection Rules	52
Configure On-Fabric Detection Rules	52
Verify On-Fabric Detection Rules	55
Lab 5: Endpoint Profiles	58
Exercise 1: Assigning an Endpoint Profile for Deployment	61

Enable the Security Features in the Endpoint Profile.....	61
Assign Endpoint Profiles to an Endpoint Policy.....	64
Exercise 2: Testing Antivirus Protection.....	66
Verify AntiVirus Protection Settings.....	66
Test the Antivirus Real-Time Configuration.....	67
Exercise 3: Performing Vulnerability Scans.....	69
Exercise 4: Testing the FortiGuard Web Filter.....	73
Verify FortiGuard Connectivity.....	73
Identify Web Filter Categories.....	73
Review a FortiGuard Category-Based Web Filter.....	75
Test the Web Filter.....	76
Lab 6: ZTNA.....	79
Lab 7: Zero Trust Network Access.....	80
Exercise 1: Adding FortiClient EMS to the Security Fabric.....	81
Exercise 2: Configuring Security Posture Tags, Tagging Rules, and Features.....	84
Verify the Connection Between FortiClient, FortiClient EMS, and FortiGate.....	84
Configure FortiClient EMS Security Posture Tagging Rules.....	86
Enable the ZTNA Feature and Verify That ZTNA Tags Are Synchronized.....	90
Exercise 3: Configuring an HTTPS Access Proxy With Certificate Authentication and Security Posture Tags.....	92
Configure a Basic HTTPS Access Proxy With Certificate-Based Authentication and Security Posture Tags.....	92
Test Remote Access to the HTTPS Access Proxy.....	96
Verify the Behavior When the Security Posture Changes on the Endpoint.....	101
Exercise 4: Configuring a TCP Forwarding Access Proxy for SSH.....	104
Configure a TCP Access Proxy for Private Applications.....	104
Test the Connection for Users.....	107
Exercise 5: Configuring ZTNA for SaaS Application Access.....	108
Configure a TCP Access Proxy for SaaS Applications.....	108
Test the Connection for Users.....	112
Lab 8: Security Incident Response.....	114
Exercise 1: Enabling the Security Fabric to Trigger Automatic Quarantine.....	115
Configure FortiClient Log Settings.....	115
Enable the Security Fabric on the FortiGate.....	116
Exercise 2: Configuring FortiAnalyzer Playbooks to Add Fabric Tags to FortiClient Endpoints.....	123
Enable the EMS Connector on FortiAnalyzer.....	123
Configure Playbooks on FortiAnalyzer.....	125
Run the FortiAnalyzer Playbook.....	128
Lab 9: Troubleshooting and Diagnostics.....	131
Exercise 1: Troubleshooting FortiClient Connectivity to FortiClient EMS.....	136

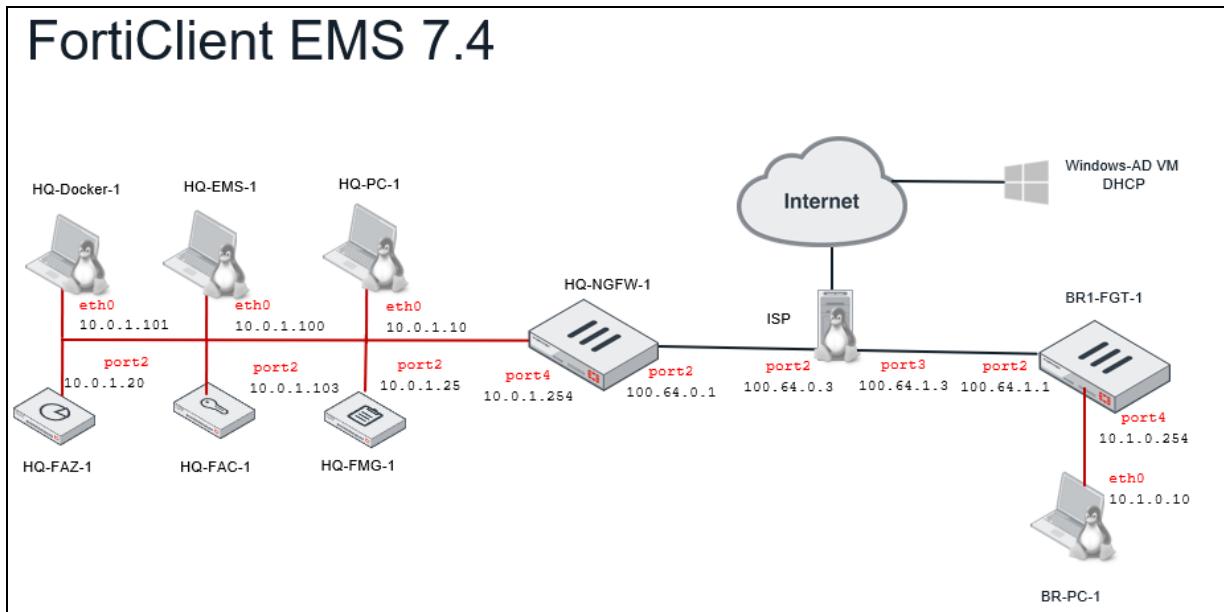
Review the FortiClient Telemetry Connectivity Status.....	136
Troubleshoot the FortiClient Telemetry Connectivity Issue.....	137
Exercise 2: Using the Password Recovery Tool to Reset the Built-In Administrator Password.....	142
Lab 10: FortiClient Cloud.....	145

Change Log

This table includes updates to the *FortiClient EMS 7.4 Lab Guide* dated 1/27/2025 to the updated document version dated 3/14/2025.

Change	Location
Added self-paced pre-requisites	"Prerequisites (Self-Paced Only)" on page 58
Added self-paced pre-requisites	"Prerequisites (Self-Paced Only)" on page 133

Network Topology



Lab 1: FortiClient EMS Installation

In this lab, you will create a FortiClient EMS administrator and apply the FortiClient EMS license.

Objectives

- Create FortiClient EMS administrator
- Apply a FortiClient EMS license

Time to Complete

Estimated: 20 minutes

Exercise 1: Accessing the FortiClient EMS GUI

In this exercise, you will access the FortiClient EMS GUI, create an administrator account, and then install the FortiClient EMS license.



In this environment, FortiClient EMS has already been installed with PostgreSQL in Docker.

Access the FortiClient EMS GUI and Install the License

You will access the FortiClient EMS GUI, create an administrator user and password, and install the license.

To access the FortiClient EMS GUI and create an administrator password

1. On the HQ-EMS-1 VM, open Google Chrome, and then enter <https://localhost> to access the FortiClient EMS GUI.
A certificate warning appears.
2. Accept the self-signed certificate to access the FortiClient EMS server.
3. In the username field, type `admin`, leave the password field empty, and then click **Sign in**.

FortiClient EMS prompts you to configure a new administrator and password.

The screenshot shows a dialog box titled "FortiClient Endpoint Management Server". It contains fields for "New Username" (admin), "New Password", and "Confirm Password". Below these fields are several validation messages and requirements:

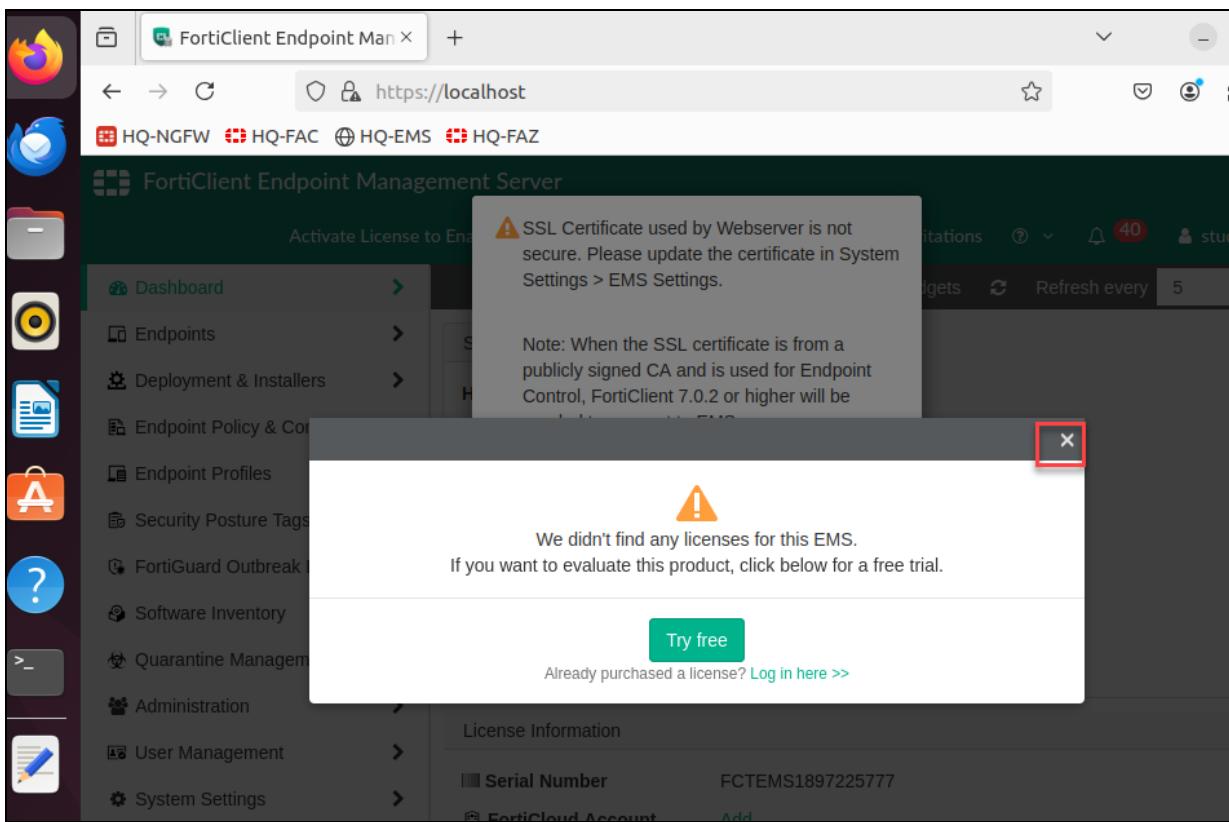
- For "New Username":
 - ✓ Different from default admin username
 - ✗ At least 5 characters long
- For "New Password" and "Confirm Password":
 - Your password must be
 - ✗ At least 8 characters long
 - And has 3 out of the 4 following:
 - ✗ At least one uppercase letter (A-Z)
 - ✗ At least one lowercase letter (a-z)
 - ✗ At least one number (0-9)
 - ✗ At least one symbol (e.g. ! \$#%)

At the bottom are "Submit" and "Cancel" buttons.

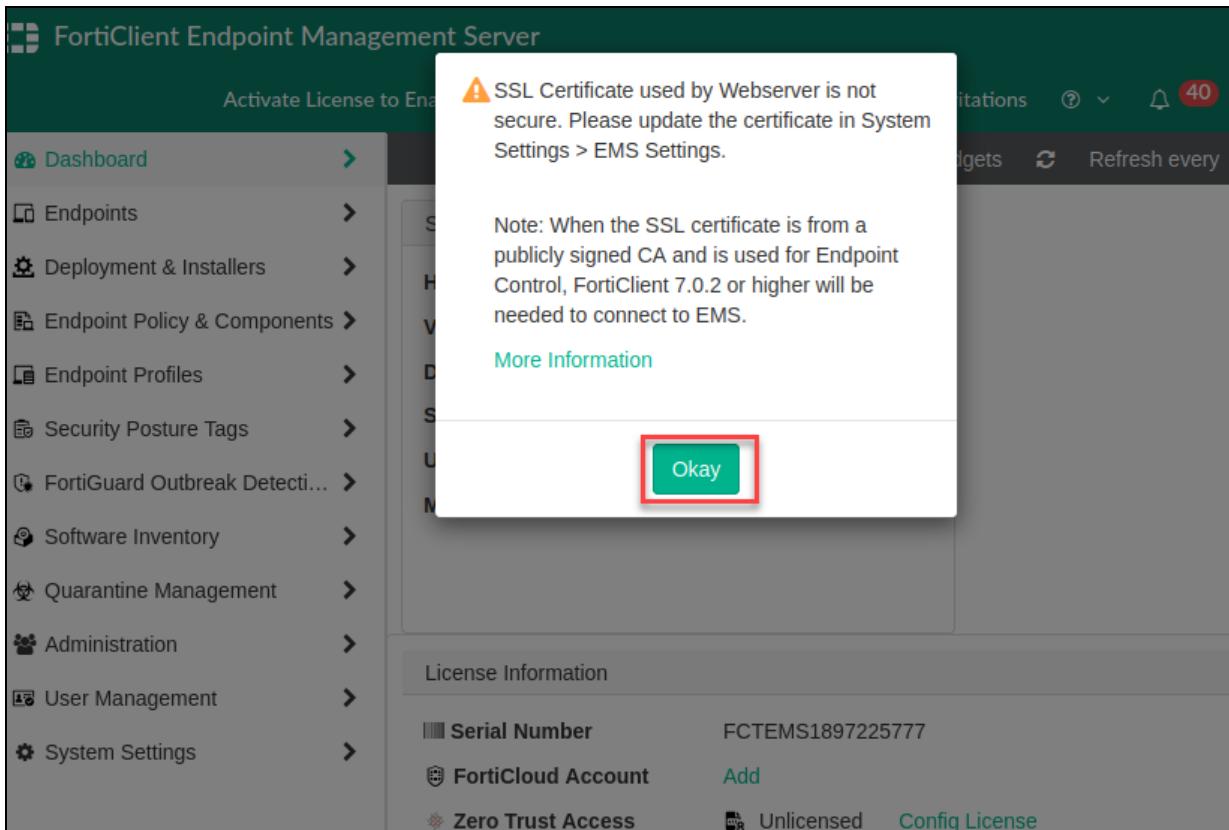
4. In the **New Username** field, type `student1`.
5. In the **New Password** and **Confirm Password** fields, type `Password1!` to meet the password requirements, and then click **Submit** to save the password.

To install the FortiClient EMS license

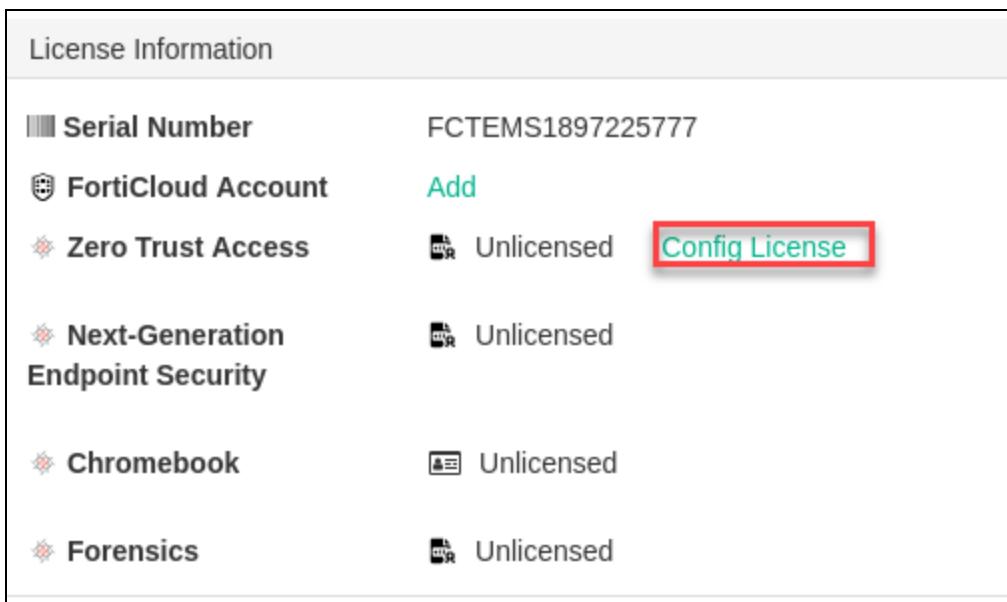
1. Log in to the FortiClient EMS GUI with the following credentials:
 - Username: `student1`
 - Password: `Password1!`
2. Click **X** to close the EMS license warning window.



- Click **Okay** to close the SSL certificate warning window.



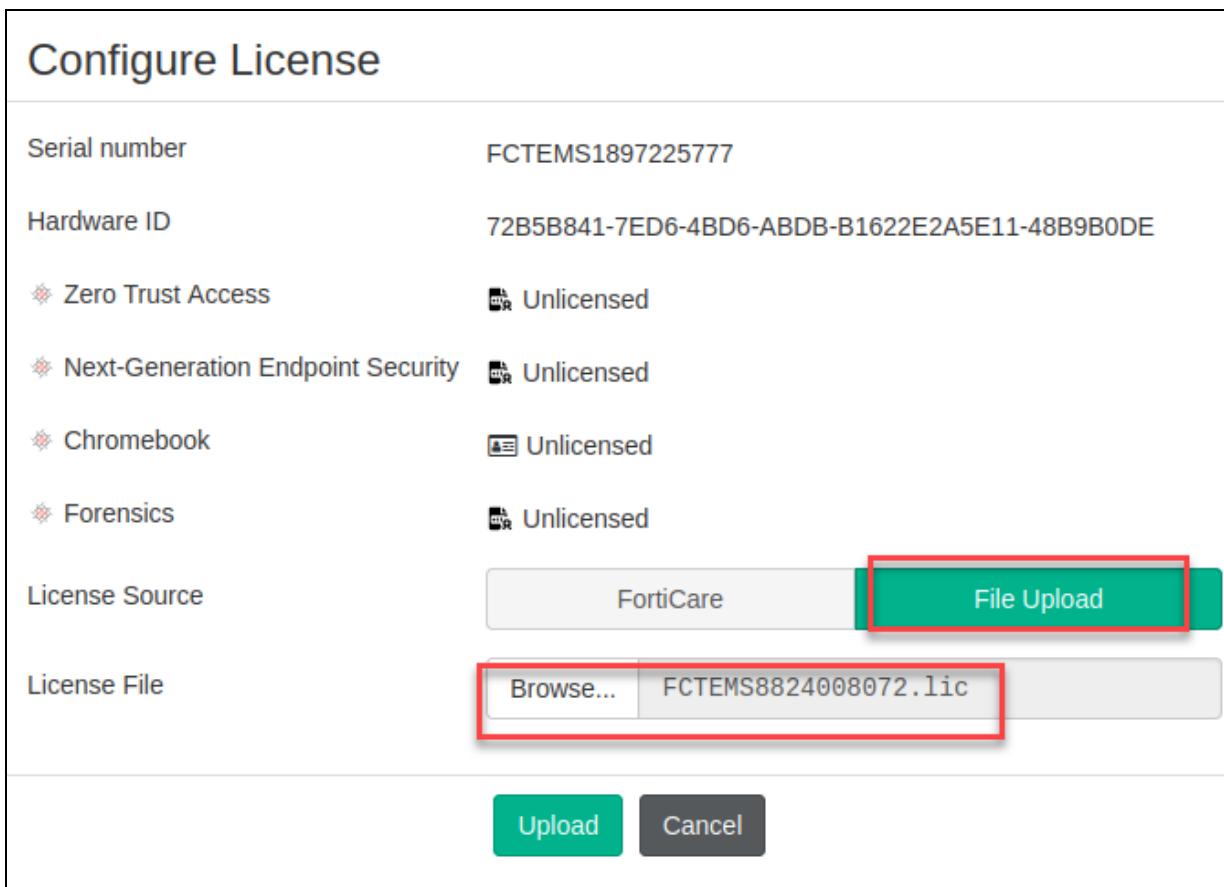
4. In the **Dashboard > Status > License Information** widget, click **Config License**.



The screenshot shows a table with the following data:

License Information		
Serial Number	FCTEMS1897225777	
FortiCloud Account	Add	
Zero Trust Access	Unlicensed	Config License
Next-Generation Endpoint Security	Unlicensed	
Chromebook	Unlicensed	
Forensics	Unlicensed	

5. In the **License Source** field, select **File Upload**, click **Browse**, navigate to the **Desktop > Resources** folder, and then select the license file.



The screenshot shows the **Configure License** page with the following fields:

Configure License		
Serial number	FCTEMS1897225777	
Hardware ID	72B5B841-7ED6-4BD6-ABDB-B1622E2A5E11-48B9B0DE	
Zero Trust Access	Unlicensed	
Next-Generation Endpoint Security	Unlicensed	
Chromebook	Unlicensed	
Forensics	Unlicensed	
License Source	FortiCare	File Upload
License File	Browse...	FCTEMS8824008072.lic
Upload Cancel		

6. Click **Upload** to activate the new license.
7. Refresh the FortiClient EMS GUI page.
A certificate warning appears.
8. Accept the self-signed certificate to access the FortiClient EMS server.
9. Click **Okay** to close the SSL certificate warning window.
10. On the FortiClient EMS GUI, click **Dashboard > Status** to see the license information.

License Information

Module	Status	Expiration Date	Usage
Serial Number	FCTEMS8824008072		
FortiCloud Account	Add		
Zero Trust Access	Included		
Next-Generation Endpoint Security	Licensed	2025-09-16	0 used of 25
Chromebook	Unlicensed		
Forensics	Unlicensed		

Lab 2: System Administration

In this lab, you will examine the configuration of the FortiClient EMS system settings.

Objectives

- Configure system settings
- Enable SSO authentication for FortiClient EMS administrator login

Time to Complete

Estimated: 35 minutes

Exercise 1: Configuring FortiClient EMS System Settings

In this exercise, you will configure the following FortiClient EMS system settings:

- Server settings
- Log settings
- Login banner settings

Configure Server Settings

On the **EMS Settings** page, you can configure settings, such as the host name and FQDN. You will configure the FQDN to access the FortiClient EMS server, using the configured FQDN. You will also upload the SSL certificate for web server access and endpoint control.

To configure the FQDN on FortiClient EMS

1. On the HQ-EMS-1 VM, open Google Chrome, and then log in to the FortiClient EMS GUI with the following credentials:
 - Username: student1
 - Password: Password1 !
2. Click **Okay** to close the SSL certificate warning window.
3. Click **System Settings > EMS Settings**.
4. In the **Shared Settings** section, in the **Listen on IP** field, ensure that the value is **10.0.1.100**.
5. In the **Use FQDN** field, select the checkbox, and then type `ems.training.lab`.

EMS Settings

Shared Settings

Hostname: hq-ems-1

Listen on IP: 10.0.1.100

Use FQDN: ems.training.lab

Remote HTTPS access:

HTTPS port: 443

Pre-defined hostname: *,10.0.1.100,192.168.0.100

Custom hostname: Optional

6. In the **EMS Settings** section, in the **FortiClient download URL** field, ensure that the value is **10.0.1.100**.
7. Click **Save** to apply the changes.
8. Click **Yes** to restart the server.
9. Restart Chrome, enter `https://ems.training.lab`, and then accept the self-signed certificate to access the FortiClient EMS server.
10. Log in with the following credentials:
 - **Username:** student1
 - **Password:** Password1!
11. Click **Okay** to close the SSL certificate warning window.



The HQ-EMS-1 VM host file has been modified to make `ems.training.lab` accessible.

To upload the SSL certificate

1. Continuing on the FortiClient EMS GUI, click **System Settings > EMS Server Certificates**.
2. Click **Add**, and then in the **Add Certificate** window, select **Upload PKCS12**.
3. In the **Certificate** field, click **Browse**, on the desktop, click **Resources**, and then select the `ems_admin.p12` certificate.
4. In the **Certificate Password** field, type `fortinet`.

Add Certificate

Type: Automated

Upload PKCS12

Upload PEM

Certificate: Browse... ems_admin.p12

Certificate Password:

Upload Cancel

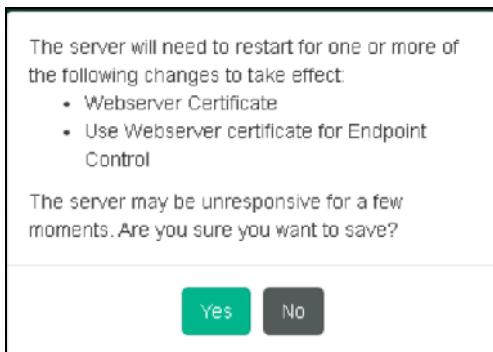
- Click **Upload**.

On the **EMS Server Certificates** page, the value in the **Type** column for the certificate should be **Uploaded**.

EMS Server Certificates						+ Add	Refresh
<input type="checkbox"/>	Name	Type	Expiry Date	Assigned To			
<input type="checkbox"/>	server.crt	Default	Valid 2035-11-19 05:...				
<input type="checkbox"/>	FCTEMS8824008072...	FortiCare	Valid 2056-05-26 10...				
<input type="checkbox"/>	FCTEMS8824008072...	FortiCare	Valid 2038-01-18 11:...	Webserver	...		
<input type="checkbox"/>	ems_admin.p12	Uploaded	Valid 2030-10-04 03...				

To select the newly uploaded certificate for web server and endpoint control

- Continuing on the FortiClient EMS GUI, click **System Settings > EMS Settings**.
- In the **Shared Settings** section, in the **Webserver Certificate** field, select **ems_admin.p12**.
- Select the **Use Webserver certificate for Endpoint Control** checkbox.
- Click **Save**, and then in the window warning you about a server restart, click **Yes**.



- Click **Okay**.
- Refresh the FortiClient EMS GUI page.

Configure Log Settings

On the **Log Settings** page, you can configure the log level, and the number of days that you want to keep logs, events, and alerts before they are cleared. You will change the **Log level** setting.

To configure log settings

1. On the FortiClient EMS GUI, click **System Settings > Log Settings**.



You may need to log out and log in again to load the **Log Settings** page.

2. In the **Log level** field, ensure that the value is **Info**.

The screenshot shows the FortiClient Endpoint Management Server interface. The left sidebar has a tree view with nodes like 'Endpoint Policy & Components', 'Endpoint Profiles', 'Zero Trust Tags', 'FortiGuard Outbreak Detect...', 'Software Inventory', 'Quarantine Management', 'Administration', 'User Management', 'System Settings' (which is expanded to show 'EMS Settings' and 'Log Settings'), and 'Log Settings' (which is selected and highlighted in green). The main content area is titled 'Log Settings'. It contains a 'Log level' dropdown set to 'Info', which is highlighted with a red box. Below it are three sections for clearing logs: 'Automatically clear logs older than' (30 days), 'Automatically clear alerts older than' (30 days), and 'Automatically clear events older than' (30 days). Each section has a 'Clear all now' button. At the bottom, there are three buttons for 'Send system log messages externally': 'Disabled' (highlighted in green), 'FortiAnalyzer', and 'SysLog'. A 'Save' button is at the bottom right.

3. Click **Administration > Log Viewer** to view the logs.

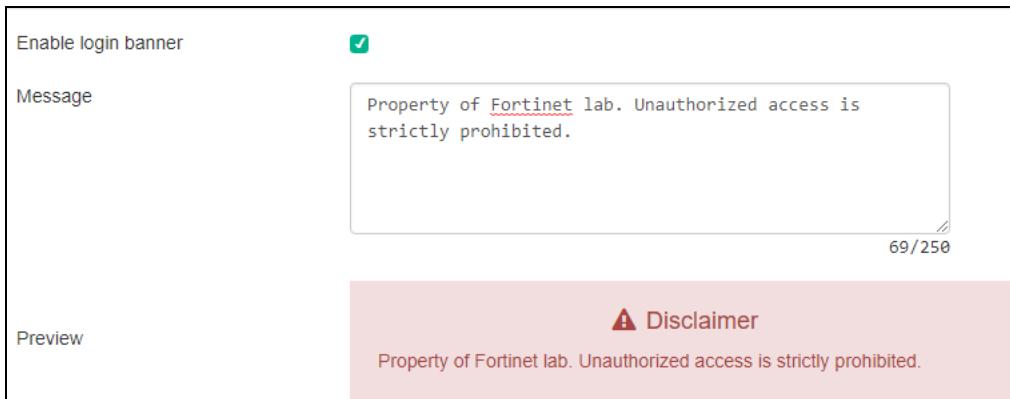
Date	Level	Source	Message	Occurrences
2024-10-14 01:2...	⚠ Warning	Console	Session has expired or does not exist.	1 time sinc...
2024-10-14 01:2...	ℹ Info	Console	student1 changed Server Settings.	1 time sinc...
2024-10-14 01:2...	ℹ Info	Console	student1 uploaded a certificate: ems_...	1 time sinc...
2024-10-14 01:1...	ℹ Info	Console	student1 has logged in from 10.0.1.100.	1 time sinc...
2024-10-14 01:1...	⚠ Warning	Console	Session has expired or does not exist.	2 times sinc...
2024-10-14 01:1...	ℹ Info	Console	student1 changed Server Settings.	1 time sinc...
2024-10-14 01:0...	⚠ Warning	Console	Session has expired or does not exist.	4 times sinc...
2024-10-14 01:0...	ℹ Info	Console	student1 uploaded License with serial...	1 time sinc...
2024-10-14 01:0...	ℹ Info	Console	student1 has logged in from ::1.	1 time sinc...
2024-10-14 01:0...	ℹ Info	EMS Service	Tags cleared for all endpoints	6 times sinc...
2024-10-14 01:0...	ℹ Info	Console	admin changed password	1 time sinc...

Configure Login Banner Settings

On the **EMS Settings** page, you will configure a disclaimer message that appears before a user logs in to FortiClient EMS.

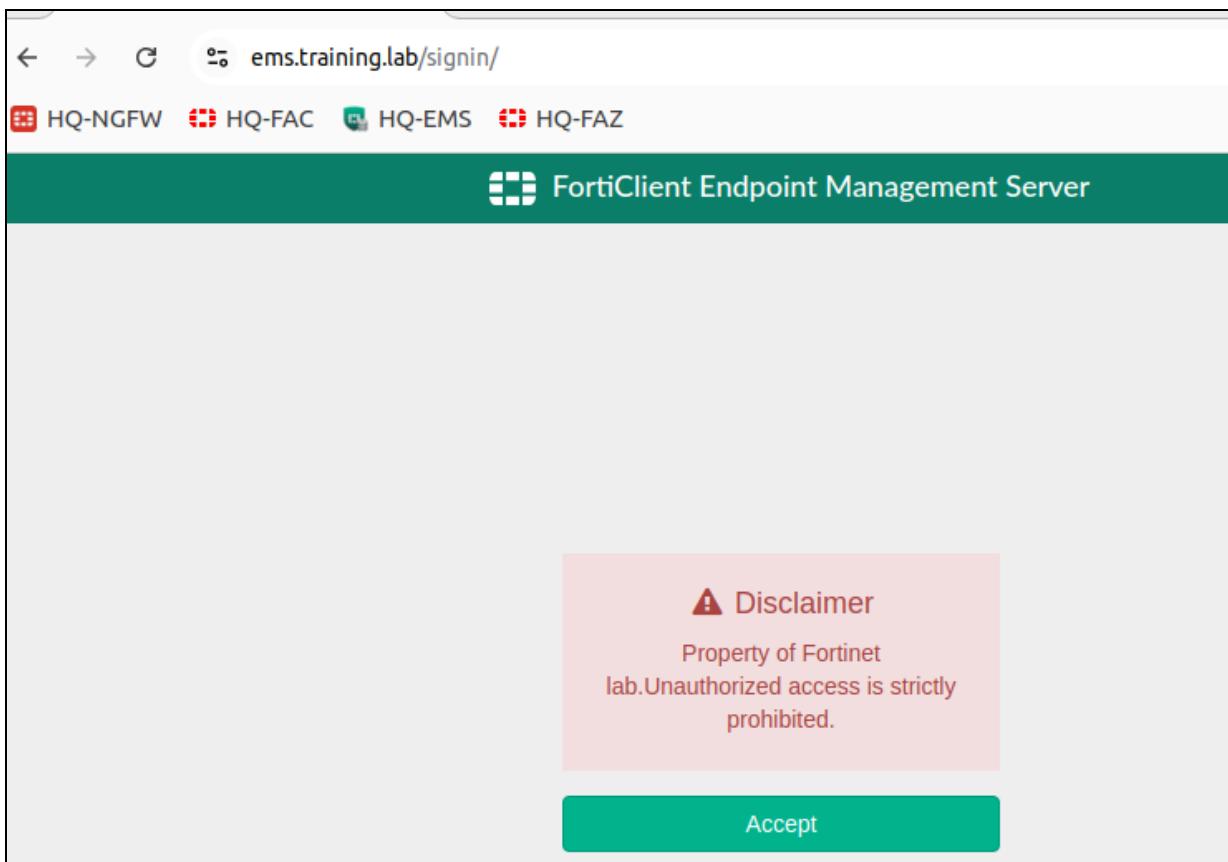
To configure login banner settings

1. Continuing on the FortiClient EMS GUI, click **System Settings > EMS Settings**.
2. Select the **Enable login banner** checkbox, and then in the **Message** field, type the following message:
Property of Fortinet lab. Unauthorized access is strictly prohibited.



3. Click **Save** to apply the changes.
4. Log out of the FortiClient EMS GUI as **student1**.

A **Disclaimer** appears.



5. Click **Accept** to go to the login page.

Exercise 2: Configuring SAML SSO for FortiClient EMS Administrator Login

In this exercise, you will configure FortiAuthenticator as an IdP server, with FortiClient EMS as an SP.

Verify IdP Settings on FortiAuthenticator

You will verify FortiAuthenticator IdP settings.

To verify FortiAuthenticator IdP settings

1. On the HQ-EMS-1 VM, open Chrome, and then in **Bookmarks**, select the **HQ-FAC** login page bookmark.
2. Log in to the FortiAuthenticator GUI with the following credentials:
 - Username: admin
 - Password: Fortinet1!
3. Click **Authentication > SAML IdP > General**.
4. In the **Server address** field, ensure that the value is **10.0.1.103**.
5. In the **Realms** section, in the **Realm** column of the table, ensure that **local | Local users** is selected.
6. In the **Default IdP certificate** field, ensure that the value is **fac [C=CA, ST=Ontario, L=Ottawa, O=Fortinet, OU=Training, CN=fac]**.

The screenshot shows the 'SAML Identity Provider portal' configuration page. Key settings include:

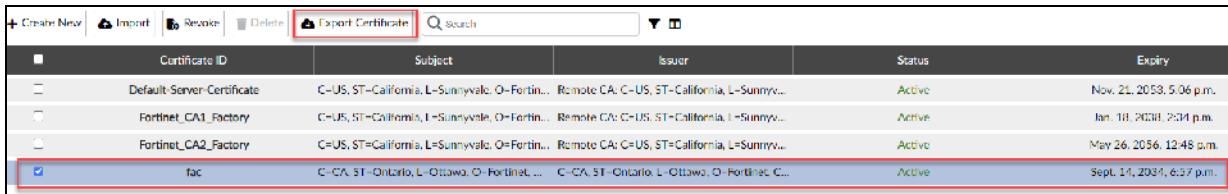
- Server address:** 10.0.1.103
- IdP-Initiated login URL:** https://10.0.1.103/saml-idp/portal/
- Username input format:** username@realm
- Captcha:** Disabled
- Realms:** A table with one row, 'local | Local users' selected in the 'Realm' column.
- Default IdP certificate:** fac [C=CA, ST=Ontario, L=Ottawa, O=Fortinet, OU=Training, CN=fac]
- Login session timeout:** 400 minutes
- Default signing algorithm:** http://www.w3.org/2001/04/xmldsig-more#rsa256

Configure FortiClient EMS as an SP for Administrator SSO Login

You will download an IdP certificate from FortiAuthenticator and import it into FortiClient EMS. You will also configure FortiClient EMS as an SP for administrator SSO login and securely identify the IdP.

To download an IdP server certificate from FortiAuthenticator

1. Continuing on the FortiAuthenticator GUI, click **Certificate Management > End Entities > Local Services**.
2. Select the checkbox for the **fac** certificate, and then click **Export Certificate**.

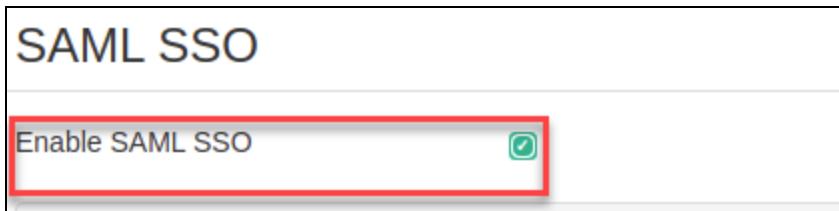


+ Create New	Import	Revoke	Delete	Export Certificate	Search	▼	□
Certificate ID	Subject	Issuer	Status	Expiry			
Default_Server-Certificate	C=US, ST=California, L=Sunnyvale, O=Fortin...	Remote CA: C=US, ST=California, L=Sunnyv...	Active	Nov. 21, 2058, 5:06 p.m.			
Fortinet_CA1_Factory	C=US, ST=California, L=Sunnyvale, O=Fortin...	Remote CA: C=US, ST=California, L=Sunnyv...	Active	Jan. 18, 2038, 2:04 p.m.			
Fortinet_CA2_Factory	C=US, ST=California, L=Sunnyvale, O=Fortin...	Remote CA: C=US, ST=California, L=Sunnyv...	Active	May 26, 2056, 12:48 p.m.			
<input checked="" type="checkbox"/> fac	C=CA, ST=Ontario, L=Ottawa, O=Fortinet, C...	C=CA, ST=Ontario, L=Ottawa, O=Fortinet, C...	Active	Sept. 14, 2034, 6:57 p.m.			

The certificate is exported to the **Downloads** folder.

To configure FortiClient EMS As an SP

1. Log in to the FortiClient EMS GUI with the following credentials:
 - Username: **student1**
 - Password: **Password1!**
2. Click **Administration > SAML SSO**.
3. On the **SAML SSO** page, select the **Enable SAML SSO** checkbox.



SAML SSO

Enable SAML SSO

4. Return to the FortiAuthenticator GUI, and then click **Authentication > SAML IdP > Service Providers**.
5. Select the **EMS-Login** SP name, click **Edit**, and then leave the page open.
6. Return to the FortiClient EMS GUI, and then in the **Service Provider Settings** section, in the **SP Address** field, type **10.0.1.100**.
7. In the **SP Entity ID** field, copy the value, and then on the FortiAuthenticator GUI, in the **SP Metadata** section, paste it in the **SP entity ID** field.
8. Return to the FortiClient EMS GUI, in the **SP ACS (login) URL** field, copy the value, and then on the FortiAuthenticator GUI, paste it in the **SP ACS (login) URL** field.

SAML SSO

Enable SAML SSO

Assertion Attributes

Username Claim

⚠ Please configure the SAML IdP to have the username attribute matching the claim here. This matching attribute will be used as the admin user username on EMS.

Service Provider Settings

SP Address

SP Entity ID

SP ACS (login) URL

Edit SAML Service Provider

SP name:

Server certificate:

IdP signing algorithm:

Support IdP-initiated assertion response

Participate in single logout

IdP Metadata

Select an identifier to display IdP info:

SP Metadata

SP entity ID:

SP ACS (login) URL:

- Click **Save**.
- Select the **EMS-Login** SP name, click **Edit**, and then in the **IdP Metadata** section, select **emslogin**.

Edit SAML Service Provider

SP name: EMS-Login

Server certificate: Use default setting in SAML IdP General page

IdP signing algorithm: Use default signing algorithm in SAML IdP General page

Support IdP-initiated assertion response

Participate in single logout

IdP Metadata

Choose SAML service provider using these identifiers

INFO: Please select emslogin +

SP Metadata: Please select emslogin

11. In the **IdP entity id** field, copy the value, and then on the FortiClient GUI EMS, paste it in the **IdP Entity ID** field.
12. Return to the FortiAuthenticator GUI, in the **IdP single sign-on URL** field, copy the value, and then on the FortiClient EMS GUI, paste it in the **IdP single sign-on URL** field.

Edit SAML Service Provider

SP name: EMS-Login

Server certificate: Use default setting in SAML IdP General page

IdP signing algorithm: Use default signing algorithm in SAML IdP General page

Support IdP-initiated assertion response

Participate in single logout

IdP Metadata

Select an identifier to display IdP info: emslogin emslogin +

IdP entity id: http://10.0.1.103/saml-idp/emslogin/metadata/ [copy]

IdP single sign-on URL: https://10.0.1.103/saml-idp/emslogin/login/ [copy]

IdP single logout URL: https://10.0.1.103/saml-idp/emslogin/logout/ [copy]

[download] IdP metadata

Identity Provider Settings

IdP Entity ID	http://10.0.1.103/saml-idp/emslogin/metadata/
IdP single sign-on URL	https://10.0.1.103/saml-idp/emslogin/login/
IdP Certificate	No certificate imported

13. In the **IdP Certificate** field, click  to upload the FortiAuthenticator IdP certificate.
14. In the **Certificate** field, click **Browse**, click **Downloads**, and then select the `fac.cer` certificate.
15. Click **Test**.

Identity Provider Settings

IdP Entity ID	http://10.0.1.103/saml-idp/emslogin/metadata/
IdP single sign-on URL	https://10.0.1.103/saml-idp/emslogin/login/
IdP Certificate	No certificate imported
Certificate	<input type="button" value="Browse..."/> <code>fac.cer</code>  

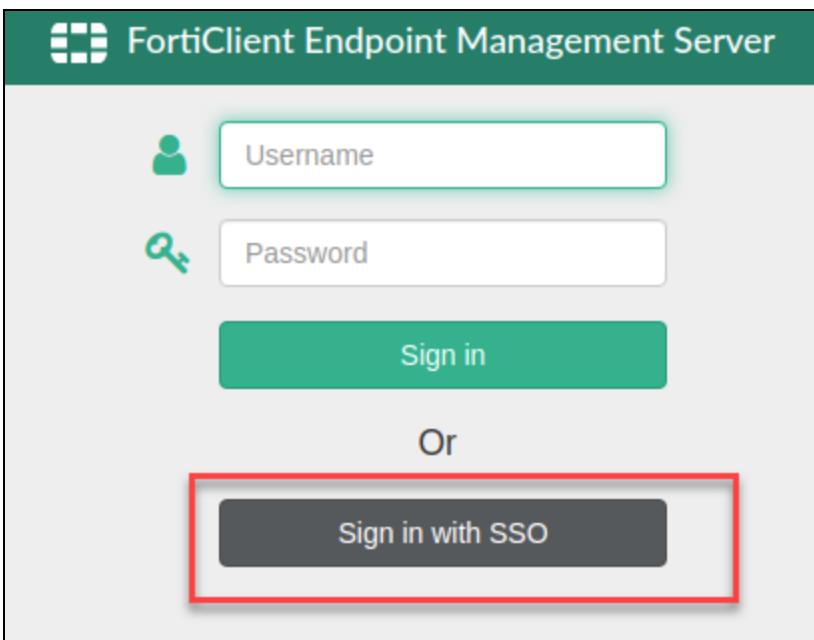
16. Click **Save**.

Test SAML SSO Authentication for FortiClient EMS Login

You will test the SSO SAML server integration on FortiClient EMS. You will log in to FortiClient EMS using an SSO SAML account.

To test SAML SSO authentication for FortiClient EMS login

1. Open a Chrome incognito window, and then in **Bookmarks**, select the **HQ-EMS** login page bookmark.
2. Click **Accept**.
3. Click **Sign in with SSO**.



4. In the **Username** field, type `student2`, and then click **Next**.
5. In the **Password** field, type `Password2!`, and then click **Login**.



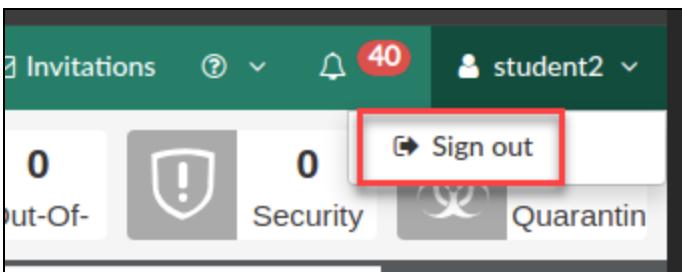
The **student2** user is already configured on FortiAuthenticator as a local user.

The **student2** user is assigned a restricted administrator role, which has no permissions enabled.



IdP administrators will have a restricted administrator role, and that cannot be changed through the SAML attributes on FortiClient EMS.

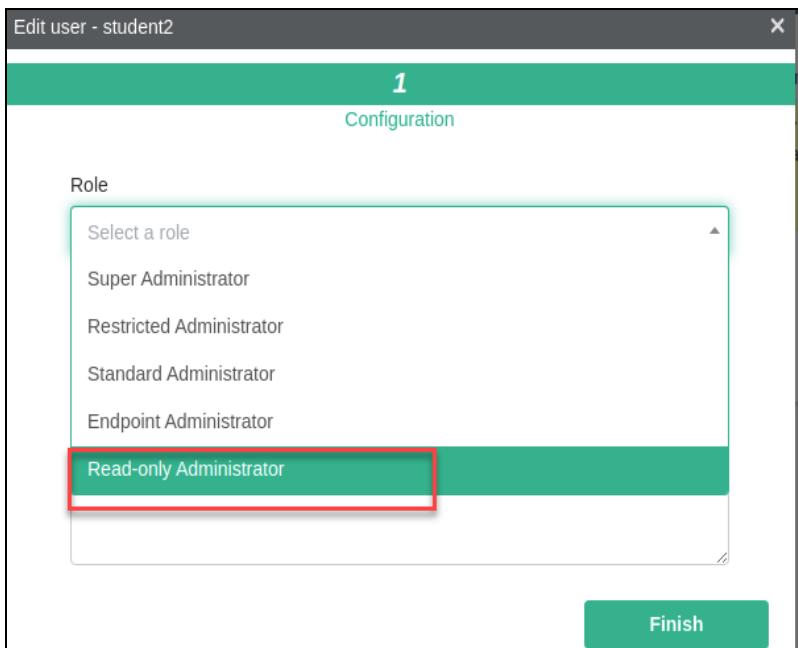
6. In the upper-right corner, click the **student2** icon, and then select **Sign out**.



7. Return to the FortiClient EMS session in the main Chrome browser, and then click **Administration > Admin Users**.

There is an entry with the **student2** name and **Restricted administrator** role.

8. Select **student2**, and then click **Edit**.
9. In the **Role** field, select **Read-only Administrator** to change the role.



10. Click **Finish**.
11. Return to the Chrome incognito window, and then click **Accept**.
12. Click **Sign in with SSO**.
13. Click **System Settings > EMS Server Certificates**.
The **Add** option is not available because this is a read-only profile.
14. Close Chrome.

Lab 3: FortiClient Deployment

In this lab, you will learn about the deployment of FortiClient on endpoints.

Objectives

- Create a FortiClient installer
- Create an invitation code
- Install FortiClient on a Linux endpoint
- Import endpoints to FortiClient EMS from Windows AD
- Install FortiClient on AD endpoints
- Register FortiClient on FortiClient EMS using an invitation code

Time to Complete

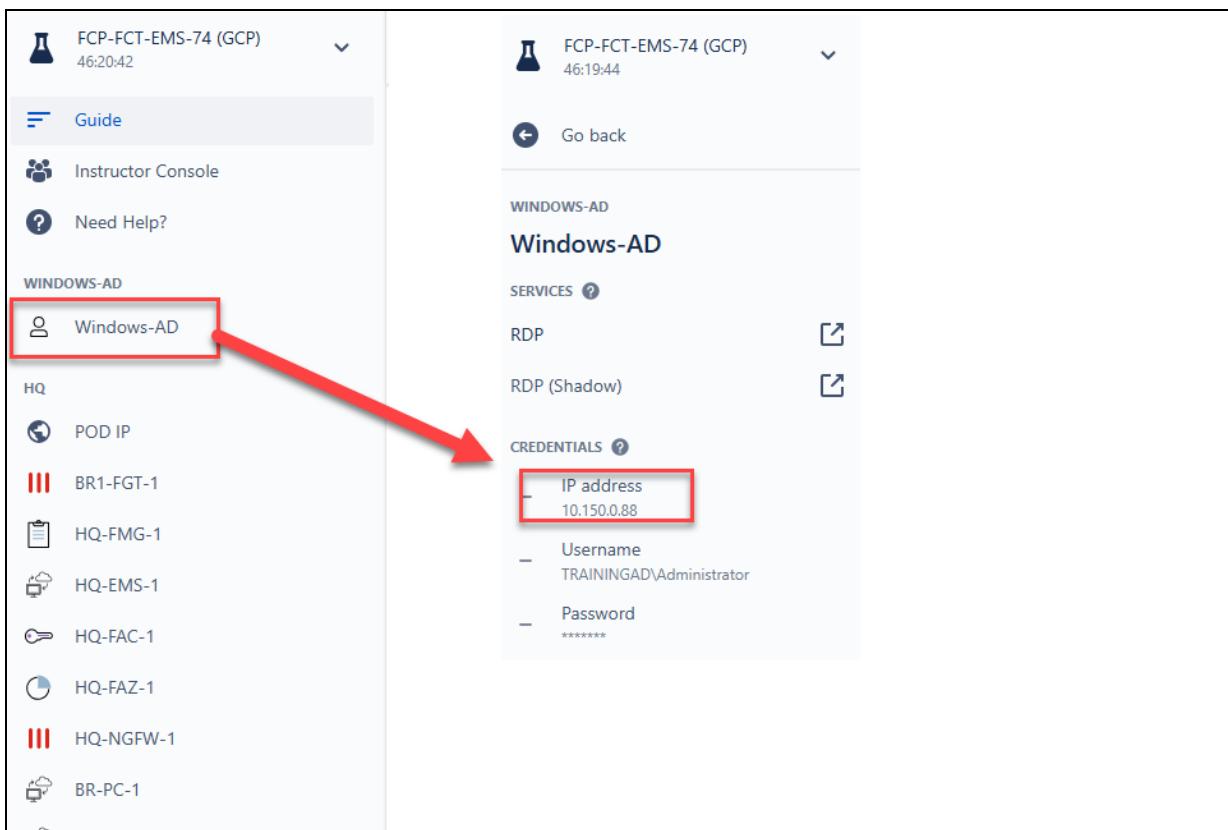
Estimated: 40 minutes

Prerequisites

Before you begin this lab, you must identify the IP address of the Windows-AD VM.

To identify the IP address of the Windows-AD VM

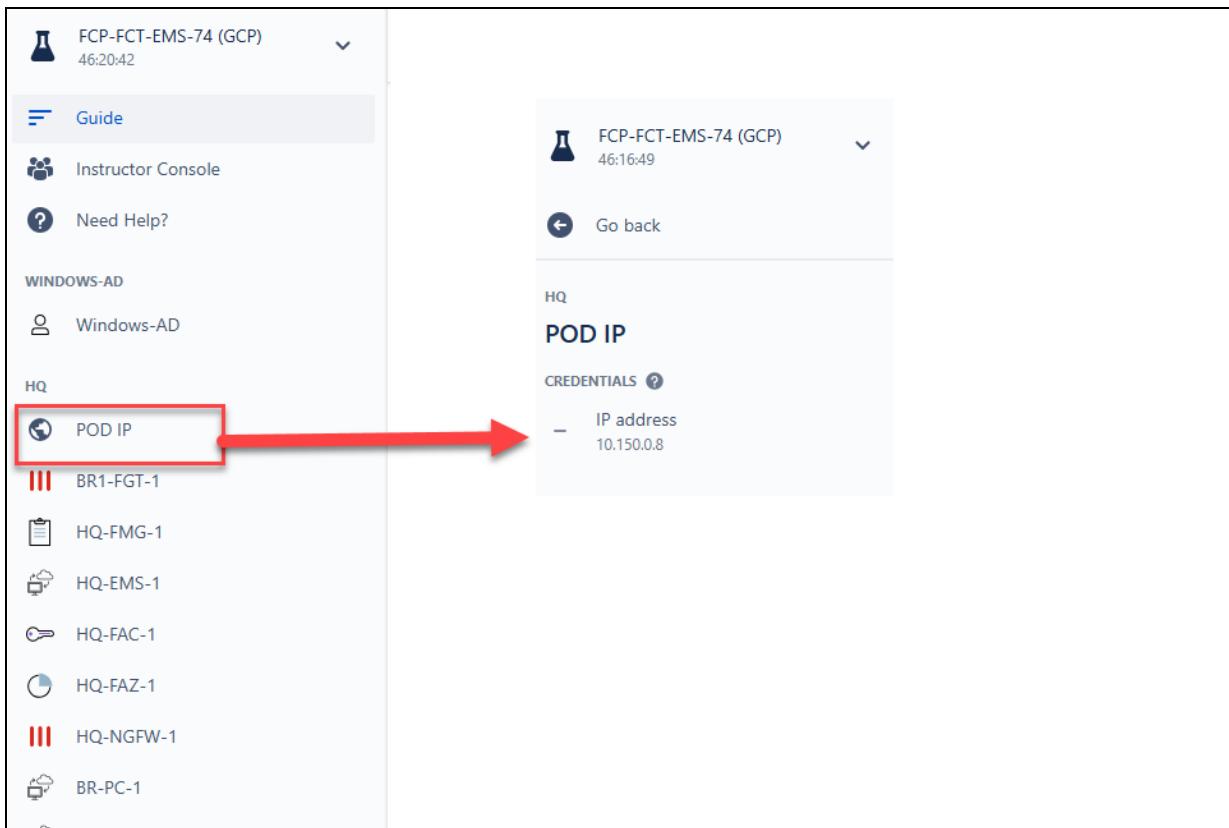
1. On the Fortinet Training Institute side bar, click **Windows-AD**.
2. In the **CREDENTIALS** section, under **IP address**, locate and make a note of the IP address.
You will use this address where the lab asks for <Windows-AD IP address>.



Before you begin this lab, you must identify the IP address of the FortiClient EMS.

To identify the IP address of the FortiClient EMS

1. On the Fortinet Training Institute side bar, click **POD IP**.
2. In the **CREDENTIALS** section, under **IP address**, locate and make a note of the IP address.
You will use this address where the lab asks for <FortiClient EMS IP address>.

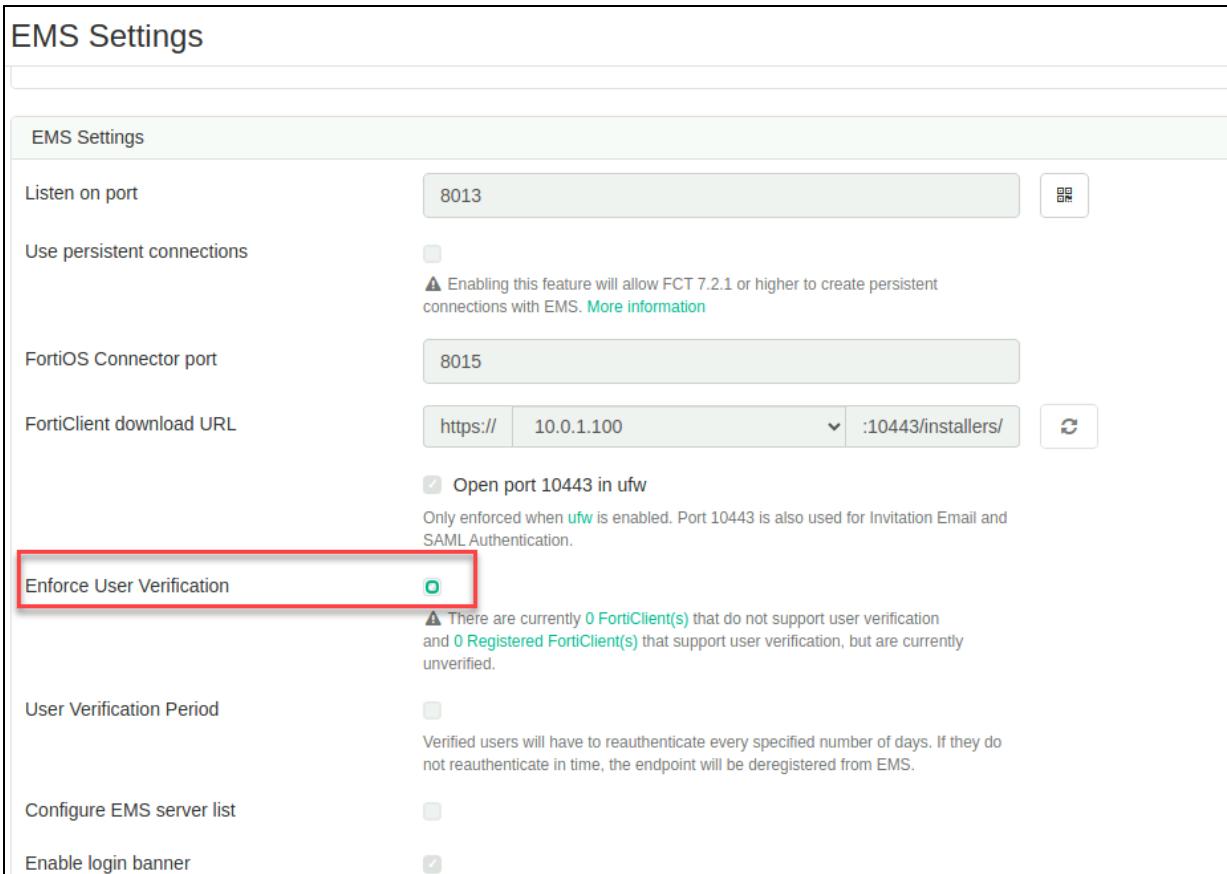


Exercise 1: Creating a FortiClient Installer and an Invitation

In this exercise, you will create an installer for deploying FortiClient on endpoints and an invitation code.

To create an installer

1. On the HQ-EMS-1 VM, log in to the FortiClient EMS GUI.
2. Click **System Settings > EMS Settings**, clear the **Enforce User Verification** checkbox, and then click **Save**.



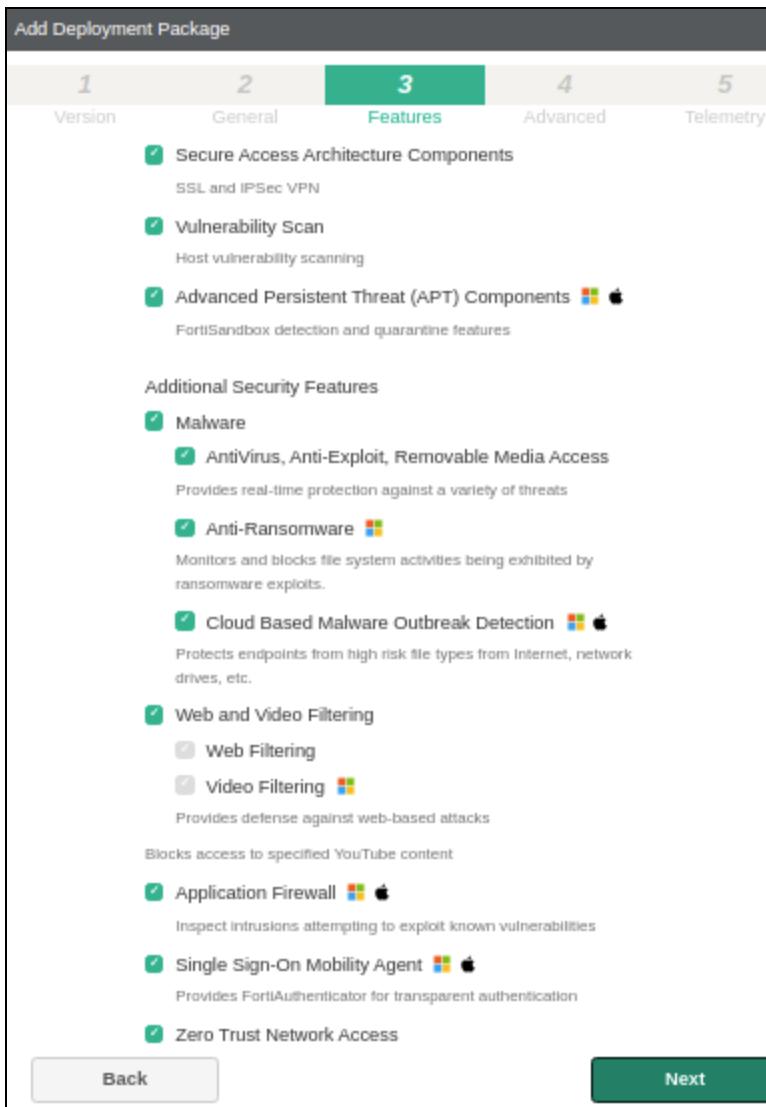
The screenshot shows the 'EMS Settings' page. The 'Enforce User Verification' checkbox is highlighted with a red box. The checkbox is currently unchecked. A tooltip message indicates that there are 0 FortiClient(s) that do not support user verification and 0 Registered FortiClient(s) that support user verification but are currently unverified.



In a real-world environment, you should enable the **Enforce User Verification** setting for an additional layer of security. In this lab environment, you are disabling it so FortiClient can connect without an invitation code.

3. Click **Deployment & Installers > FortiClient Installer**, and then click **Add** to open a new window.
4. On the **Version** tab, keep the default settings for **Installer Type** and **Release**, in the **Patch** field, select **7.4.0**, and then click **Next**.
5. On the **General** tab, in the **Name** field, type `fctinstaller`, and then click **Next**.
6. On the **Features** tab, in the **Basic Security Features** section, ensure that the **Secure Access Architecture Components**, **Vulnerability Scan**, and **Advanced Persistent Threat (APT) Components** checkboxes are selected.

7. In the **Additional Security Features** section, ensure that the **Malware, Web and Video Filtering, Application Firewall, Single Sign-On Mobility Agent, and Zero Trust Network Access** checkboxes are selected.



8. Click **Next**.

9. On the **Advanced** tab, in the **Invalid Certificate Action** field, select **Deny**, and then keep the default values for the other settings.

Add Deployment Package

1 Version 2 General 3 Features 4 Advanced 5 Telemetry

Shortcuts

Enable desktop shortcut
 Enable start menu shortcut

Installer Files

Include MSI installer files 

Installer ID

Enable Installer ID

Endpoint Profile

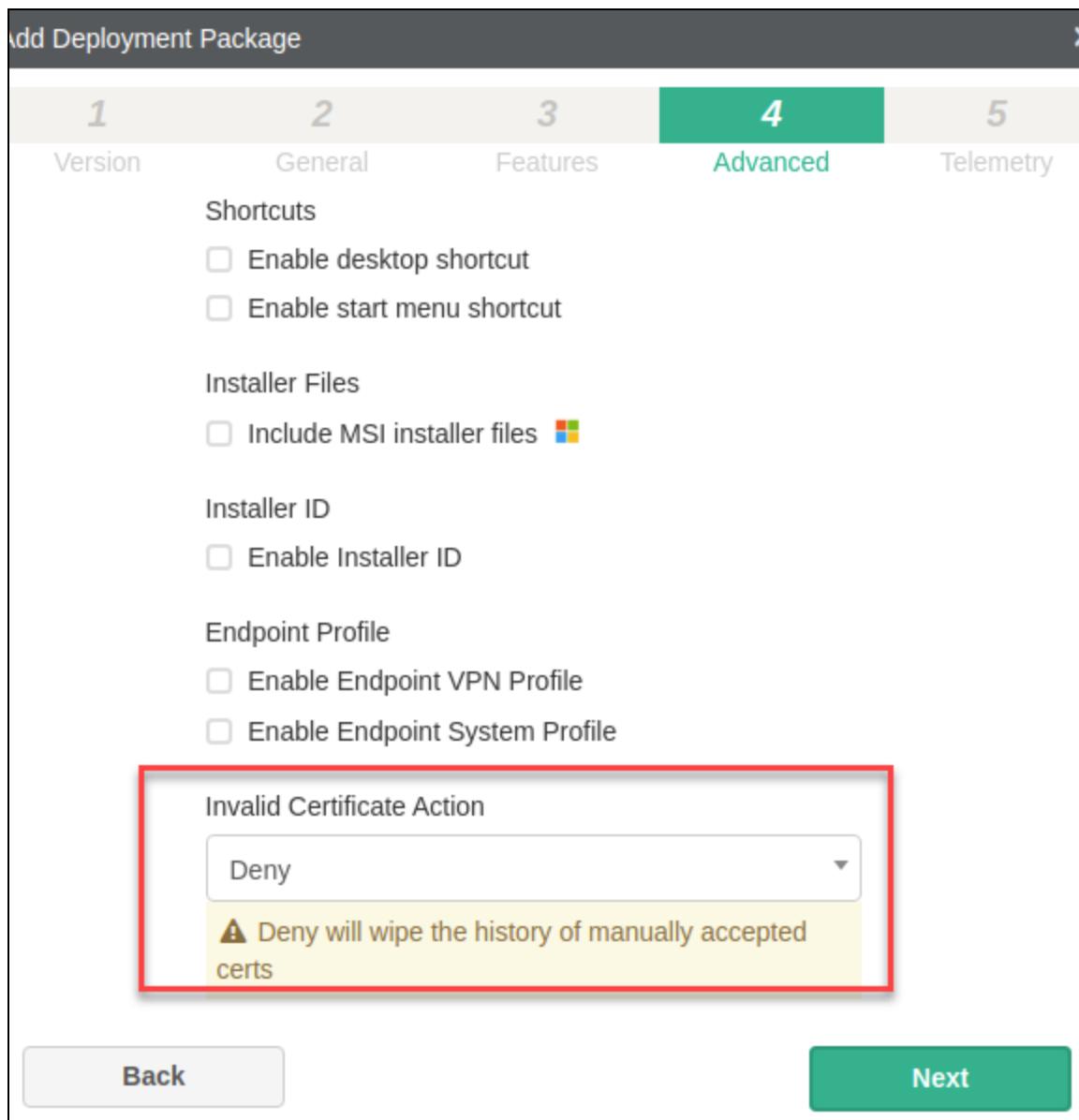
Enable Endpoint VPN Profile
 Enable Endpoint System Profile

Invalid Certificate Action

Deny

⚠ Deny will wipe the history of manually accepted certs

Back Next



10. Click **Next**.
11. On the **Telemetry** tab, notice that it shows that FortiClient will be managed by <EMS host name and FQDN address>.
12. Click **Finish** to add the deployment package to FortiClient EMS.



It takes a few minutes for the FortiClient installer to be created because the cloud controller service generates FortiClient installers for Windows, macOS, and Linux operating systems.

To create an invitation

1. Continuing on the FortiClient EMS GUI, click **User Management > Invitations**, and then click **Add** to open a new window.

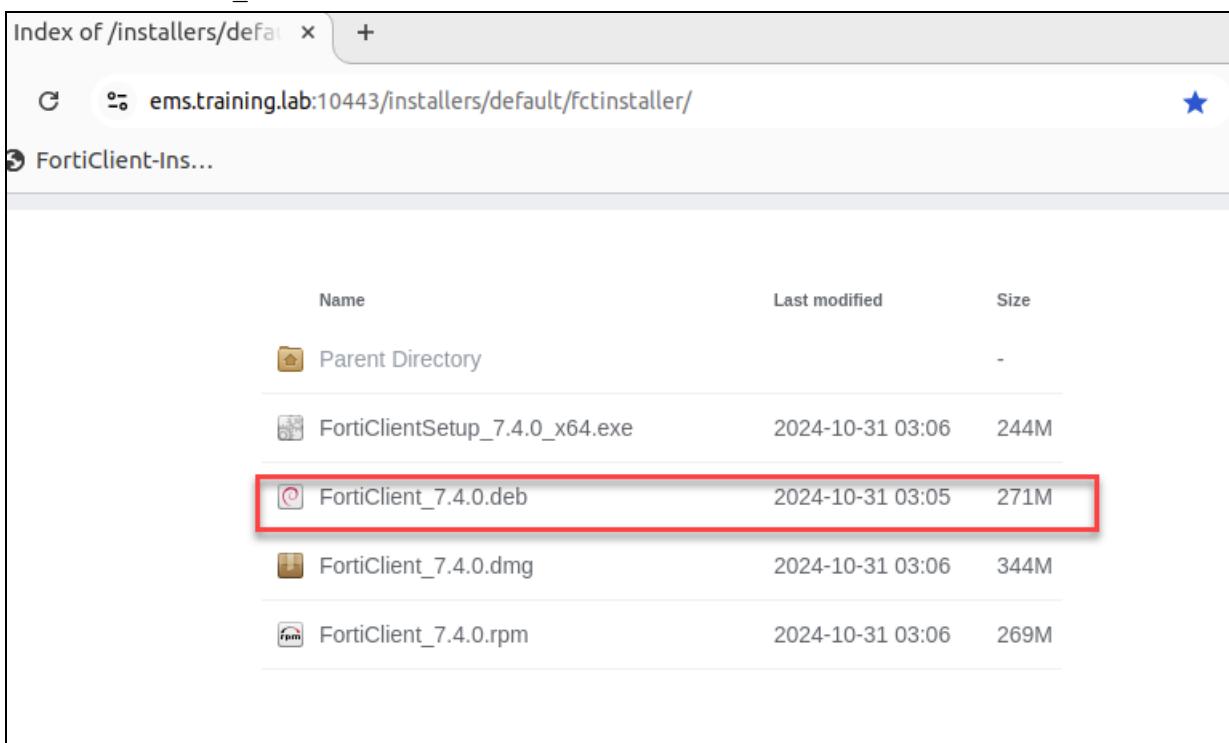
2. In the **Name** field, type `FortiClient_Invitation`.
3. In the **EMS Listen Address** field, select `ems.training.lab:8013`.
4. Click **Save** to save the invitation.

Exercise 2: Installing FortiClient on Ubuntu Linux Endpoints

In this exercise, you will use the installer link to download the installation file and install FortiClient on the HQ-PC-1 VM.

To install FortiClient

1. On the HQ-PC-1 VM, open Google Chrome.
2. On the bookmarks bar, click **FortiClient-Installer** to access the FortiClient installer download page.
3. Click `FortiClient_7.4.0.deb` to download the file.



The screenshot shows a file download list in a browser window. The URL in the address bar is `ems.training.lab:10443/installers/default/fctinstaller/`. The list includes:

Name	Last modified	Size
Parent Directory		-
FortiClientSetup_7.4.0_x64.exe	2024-10-31 03:06	244M
FortiClient_7.4.0.deb	2024-10-31 03:05	271M
FortiClient_7.4.0.dmg	2024-10-31 03:06	344M
FortiClient_7.4.0.rpm	2024-10-31 03:06	269M

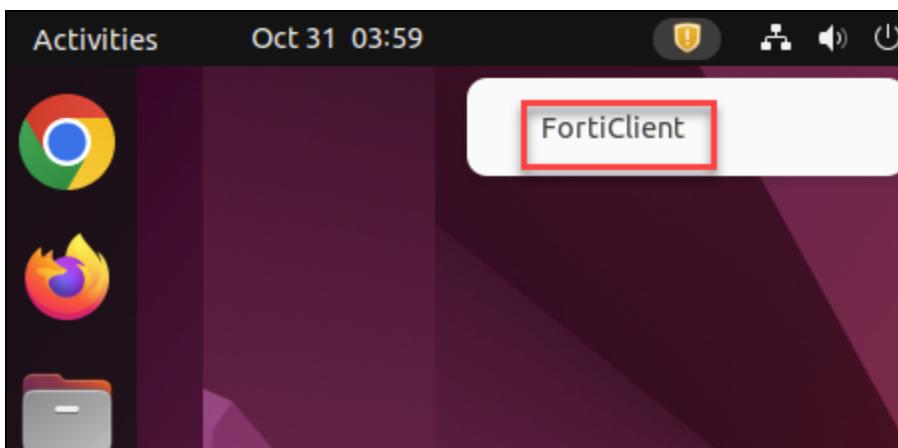
4. Once the download completes, close the browser.
5. Click the **Terminal** icon to open the terminal window.
6. Enter the following command:
`sudo apt-get install /home/admin/Downloads/FortiClient_7.4.0.deb -y`
7. Enter the following sudo password:
`Fortinet1!`



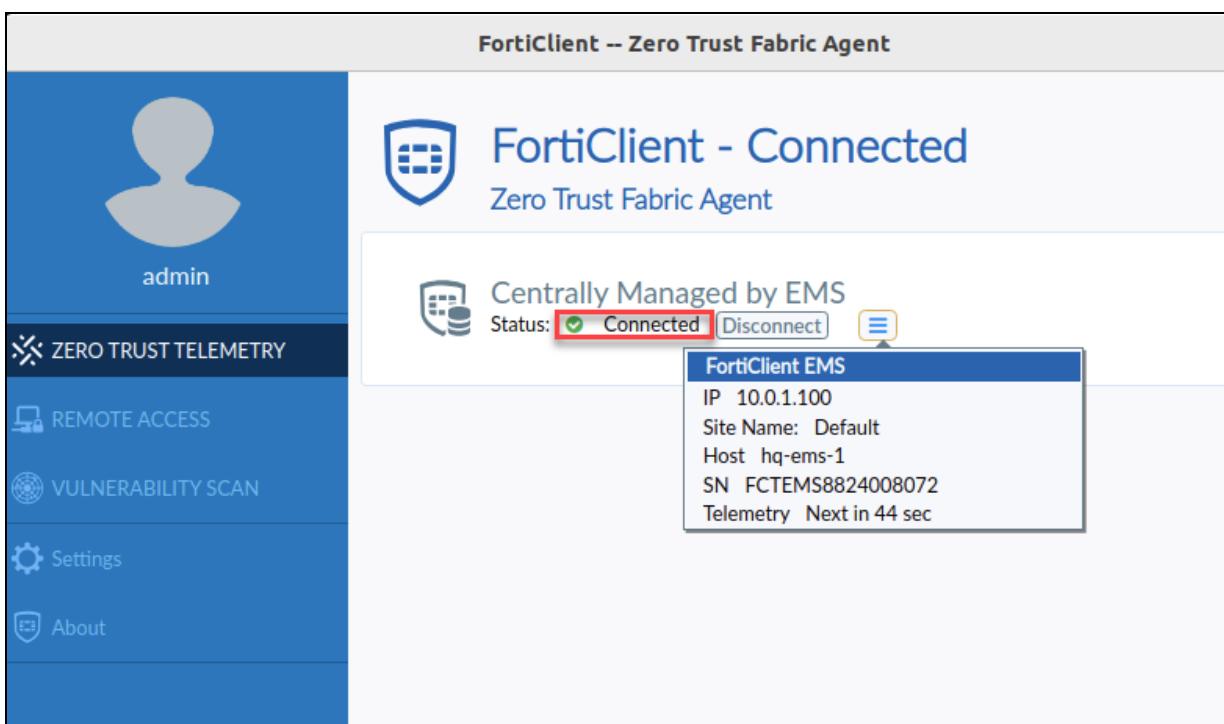
This command installs FortiClient on the Ubuntu Linux endpoint.

A permission denied error message appears at the end of the installation—you can ignore this error message.

8. Click the FortiClient icon, and then click **FortiClient** to open the FortiClient console.



FortiClient is autoregistered to FortiClient EMS.



In this lab environment, you use FortiAuthenticator as the local CA server and the root certificate is preinstalled on the Ubuntu VMs.

Exercise 3: Importing Endpoints to FortiClient EMS

In this exercise, you will manually import endpoints from an AD server into the FortiClient EMS server. You will import and synchronize information about computer accounts with an LDAP or LDAPS service. You will also add endpoints by identifying the endpoints that are part of an AD domain server.

To add an authentication server on FortiClient EMS

1. On the HQ-EMS-1 VM, log in to the FortiClient EMS GUI.
2. Click **Administration > Authentication Servers**, click **Add > ADDS** to open the **Authentication Server** window, and then configure the following settings:

Field	Value
IP address/Hostname	<Windows-AD IP address> This is the IP address of the Windows-AD VM. For more information, see the prerequisites at the beginning of this lab.
Port	389
Username	ADadmin
Password	Fortinet1!
LDAPS connection	Disable this setting. In a real-world environment, you should use secure LDAP (LDAPS) instead of LDAP. LDAPS allows for the encryption of LDAP data in transit when a directory bind is being established, which protects against credential theft.

3. Click **Test** to check the connectivity.

Success

Authentication Server

Active Directory

IP address/Hostname: 172.16.9.56

Port: 389

Username: ADadmin

Password: ######

LDAPS connection:

- Click **Save** to save the authentication server.

To add endpoints using an AD domain server

- Continuing on the FortiClient EMS GUI, click **Endpoints > Manage Domains**, and then click **Add > ADDS** to open the **Domain Import** window.
- In the **Authentication Server** field, select **trainingAD.training.lab**.
This populates the domain user and computer groups.
- In the **Select Base DN** section, select the **trainingAD.training.lab** checkbox to add all the groups.

Selected Base DN	
Status	Path
Recently Added	trainingAD.training.lab

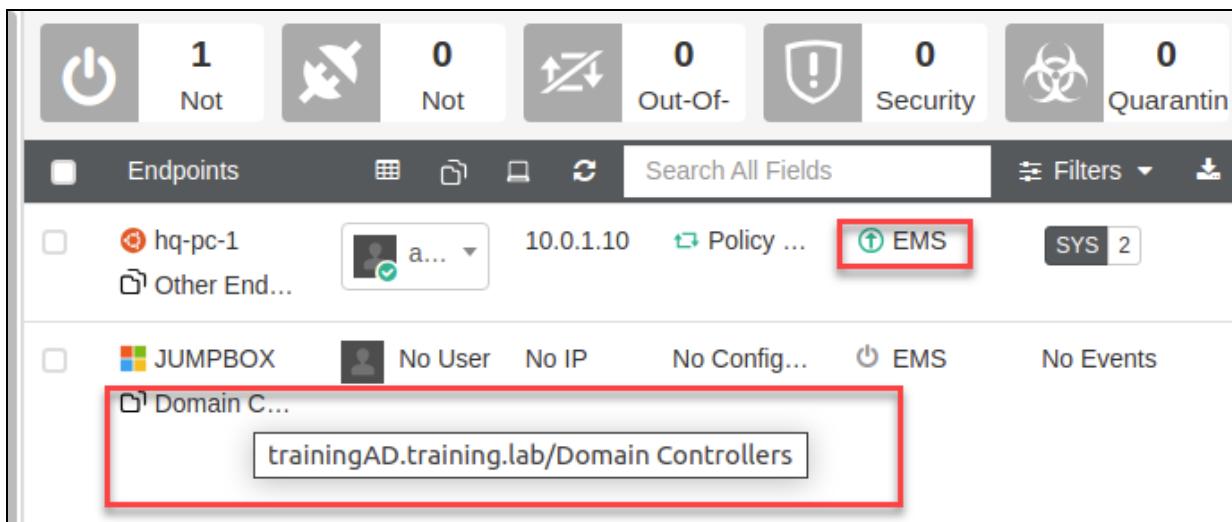
- Click **Save** to import all the endpoints and users.



You can add the entire domain or an organizational unit (OU) from the domain. After you import endpoints from an AD server, you can edit the endpoints. These changes are not synchronized with the AD server.

- Click **Endpoints > All Endpoints**.

There are two endpoints. The **hq-pc-1** Linux endpoint is managed by FortiClient EMS, which was configured earlier in this lab. The **JUMPBOX** Windows endpoint was imported into FortiClient EMS through AD integration and belongs to the **trainingAD.training.lab/Domain Controllers** OU.



The screenshot shows the FortiClient EMS interface with the following data:

Endpoint Type	Status	IP Address	Policy	EMS	Events
Endpoint	Not	10.0.1.10	Policy ...	<input checked="" type="button"/> EMS	SYS 2
Endpoint	Not				
Jumpbox	No User	No IP	No Config...	EMS	No Events
Domain Controller	trainingAD.training.lab/Domain Controllers				

Annotations: A red box highlights the 'EMS' button for the first endpoint. A larger red box highlights the 'Domain Controller' entry, which is expanded to show its details.

Exercise 4: Installing FortiClient on AD Endpoints

In this exercise, you will install FortiClient on the AD endpoint that was added from the AD domain server. FortiClient EMS no longer supports initial FortiClient installations to AD domain-joined endpoints. You will install FortiClient using the installation file that is provided.

To install FortiClient

1. On the Windows-AD VM, on the desktop, open the **Resources** folder.
2. Double-click the **FortiClient.msi** file.
3. In the **FortiClient Setup** window, select the checkbox to accept the license agreement, and then click **Next** to start the installation.



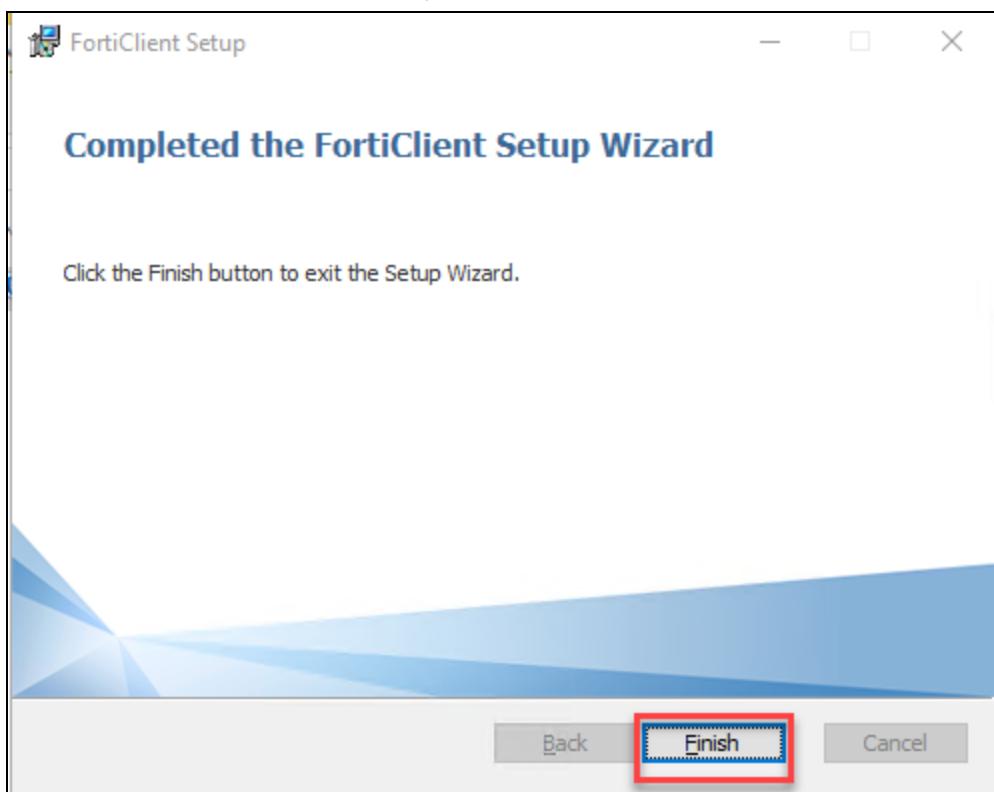
4. In the **Choose Setup Type** window, ensure that the **Secure Remote Access**, **Vulnerability Scan**, **Advanced Persistent Threat (APT) Components**, **Sandbox detection**, **Cloud Scan**, and **ZTNA** checkboxes are selected.
5. Click **Next** to continue.
6. In the **Additional Security Features** window, select **Antivirus**, **Web Filtering**, and **Anti-Ransomware** checkboxes.
7. Click **Next** to continue.

By default, the FortiClient files are installed in the following location: **C:\Program Files\Fortinet\FortiClient**.

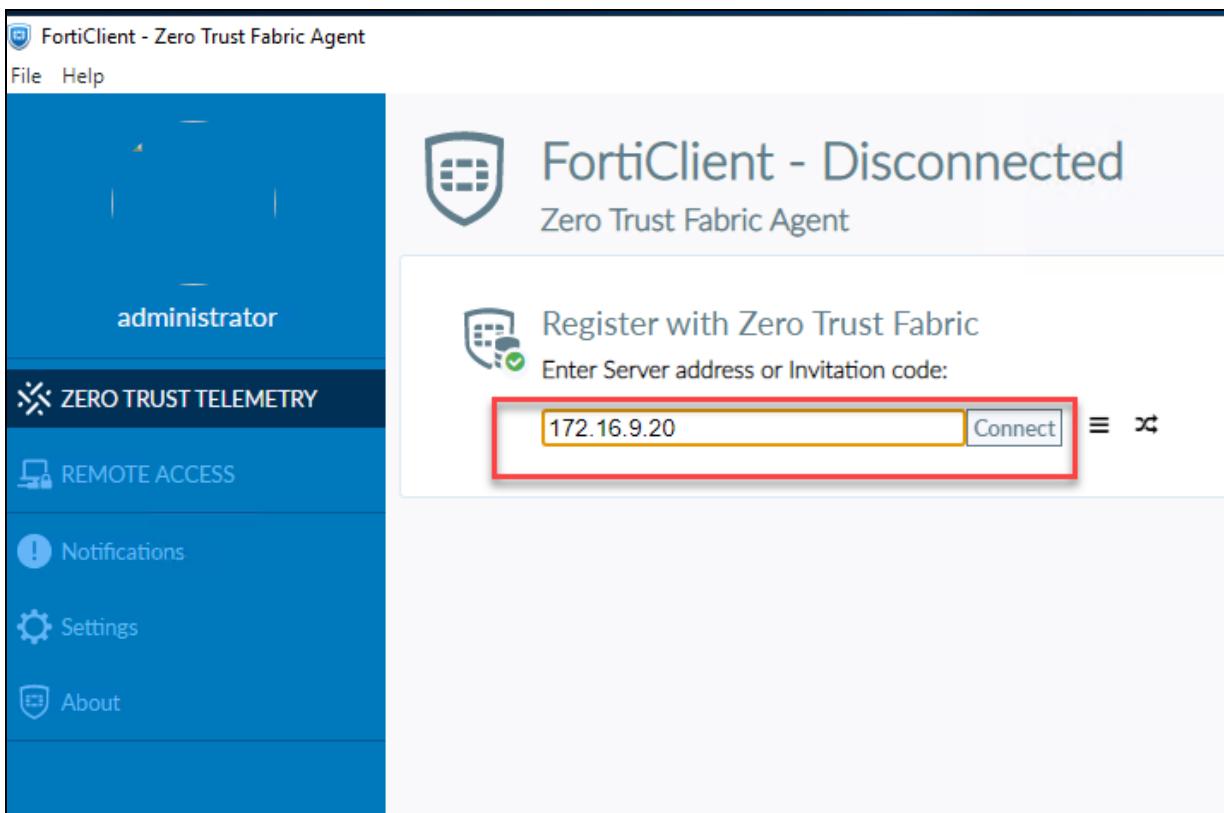
8. Click **Next** to continue.
9. Click **Install** to continue.

The setup wizard installs FortiClient on the Windows-AD VM.

10. After the FortiClient installation is complete, click **Finish**.



11. Open the FortiClient console.
12. In the **Enter Server address or Invitation code** field, type the <FortiClient EMS IP address> (located in the lab prerequisites).



13. Click **Connect**.

14. In the **Invalid certificate detected** window, click **Accept**.



In a real-world environment, the certificate that the FortiClient EMS uses will be signed with an FQDN or a static IP address. The certificates should be imported into the endpoint to avoid the certificate trust errors. In this lab environment, a dynamic IP address is used instead of an FQDN or a static IP address, which is causing the certificate trust error.

FortiClient is registered to FortiClient EMS using the IP address of FortiClient EMS.



In a real-world environment, the FortiClient EMS administrator has the following options to distribute the FortiClient installer:

- Download the preconfigured installer with the included invitation code, and install FortiClient on endpoints using third-party tools such as Intune or MDM.
- Send an email that contains the FortiClient installer and invitation code.
- Download the unconfigured installer with no invitation code, install FortiClient manually or using third-party tools, and provide the invitation code.

Exercise 5: Registering FortiClient on FortiClient EMS Using an Invitation Code

You will register a Linux endpoint on FortiClient EMS using an invitation code.

To copy the invitation code

1. On the BR-PC-1 VM, open Chrome.
2. On the bookmarks bar, click **HQ-EMS-1** to access the FortiClient EMS GUI.
3. Click **Accept**.
4. Log in to the FortiClient EMS GUI with the following credentials:
 - Username: student1
 - Password: Password1 !
5. Click **User Management > Invitations**.
6. In the **FortiClient Invitation**, click **Edit**.
7. In the **Code** field, click the icon to copy the code.

Edit Invitation

Name	FortiClient Invitation	
Code	_VjE6ZW1zLnRyYWluaW5nLmxhYjo4MDEzOmRIZmF1bHQ6MzRjYTI4YTctNjY4Zi00M2Q1LWJhNjItNmRInzQ2MzM2MDA2	
EMS Listen Address	ems.training.lab:8013	
Type	Individual	Bulk
Send Email Notifications	<input type="checkbox"/> <small>⚠ To enable this feature, please configure SMTP Settings at System Settings -> SMTP Server.</small>	
Include FortiClient Installer	fctinstaller	<input type="button" value="Delete"/> <input type="button" value="Add"/>

To register FortiClient

1. Continuing on the BR-PC-1 VM, open the FortiClient console.
2. In the **Enter Server address or Invitation code** section, paste the code you copied in the previous procedure.
3. Click **Connect**.

FortiClient is registered to FortiClient EMS using the invitation code of FortiClient EMS.

4. Return to the FortiClient EMS GUI, and then click **Endpoints > All Endpoints**.

You can see that there are three endpoints registered and managed by FortiClient EMS.

5. Close Chrome.

Lab 4: Endpoint Policy Provisioning

In this lab, you will learn about provisioning FortiClient endpoint policies on FortiClient endpoints.

Objectives

- Create an endpoint group and assign it to endpoints using group assignment rules
- Create an endpoint policy and assign it to a workgroup
- Configure on-fabric detection rules

Time to Complete

Estimated: 20 minutes

Exercise 1: Creating an Endpoint Group, a Group Assignment Rule, and an Endpoint Policy

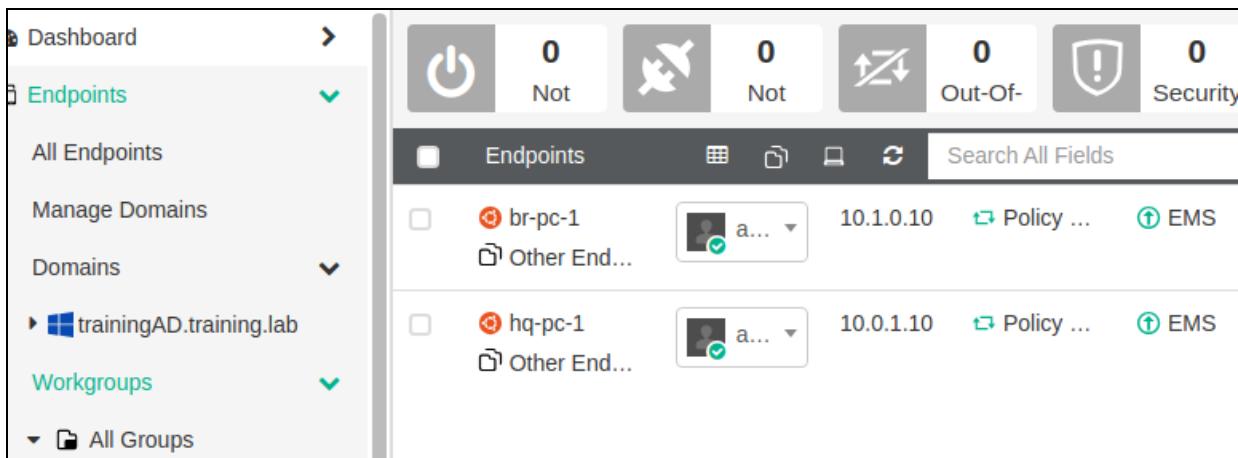
In this exercise, you will create an endpoint group and a group assignment rule, and assign the new endpoint workgroup to an endpoint policy.

Create an Endpoint Group for a Linux Workgroup

You will create an endpoint group for Linux workgroup endpoints on FortiClient EMS.

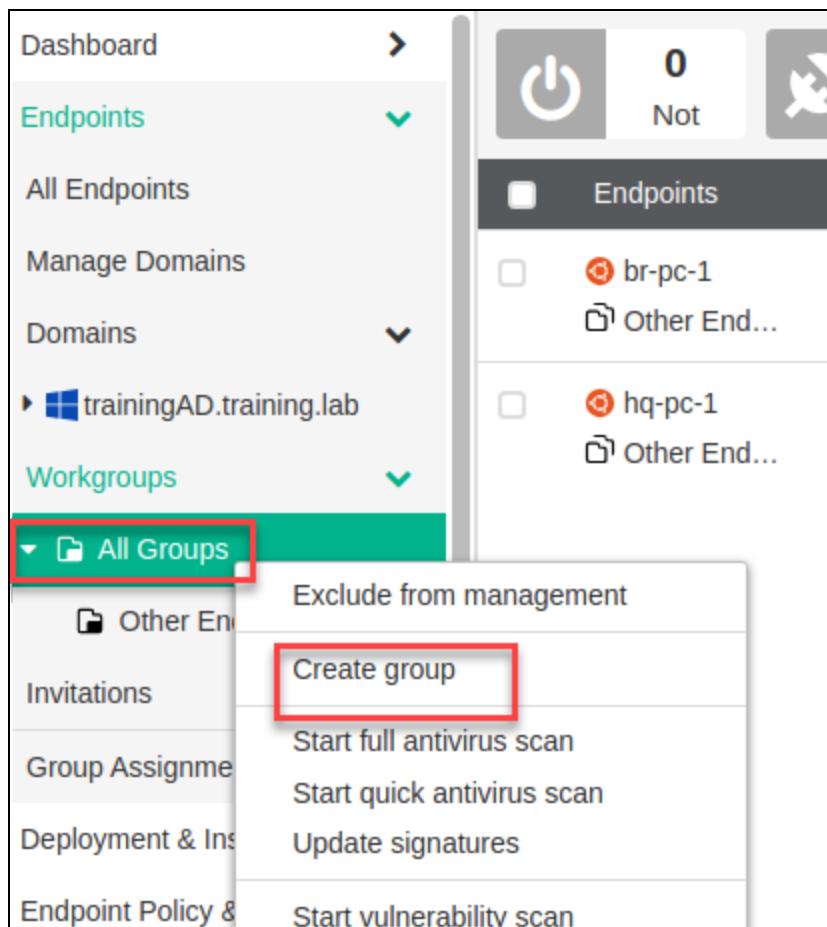
To create a group for a Linux workgroup

1. On the HQ-EMS-1 VM, log in to the FortiClient EMS GUI.
2. Click **Endpoints > Workgroups**.
By default, all the non-AD workgroup endpoints are in the **Other Endpoints** group.
3. Click **All Groups > Other Endpoints** to view the registered endpoints.

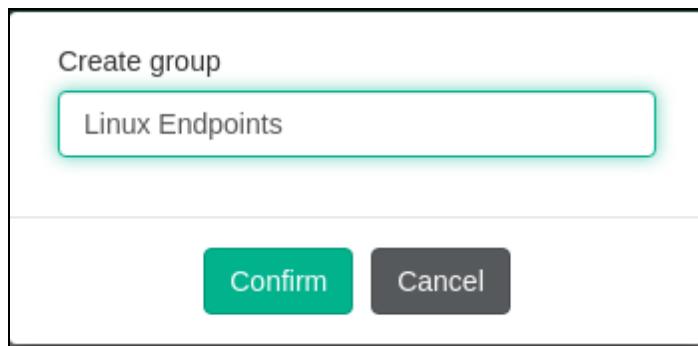


The screenshot shows the FortiClient EMS interface. On the left, a sidebar menu is open with the following options: Dashboard, Endpoints (selected), All Endpoints, Manage Domains, Domains, trainingAD.training.lab, Workgroups (selected), and All Groups. The main panel displays a list of endpoints. At the top of the list, there are four status indicators: 0 Not, 0 Not, 0 Out-Of-, and 0 Security. Below these are buttons for Endpoints, a search bar, and a 'Search All Fields' button. The endpoint list shows two entries: 'br-pc-1' and 'hq-pc-1', both of which are assigned to the 'Other Endpoints' group, as indicated by the checkmark in the dropdown menu next to their names.

4. In the **Workgroups** drop-down list, right-click **All Groups**, and then click **Create group**.



5. In the **Create group** field, type `Linux Endpoints`.



6. Click **Confirm** to create the group.



Create a Group Assignment Rule for Linux Endpoints

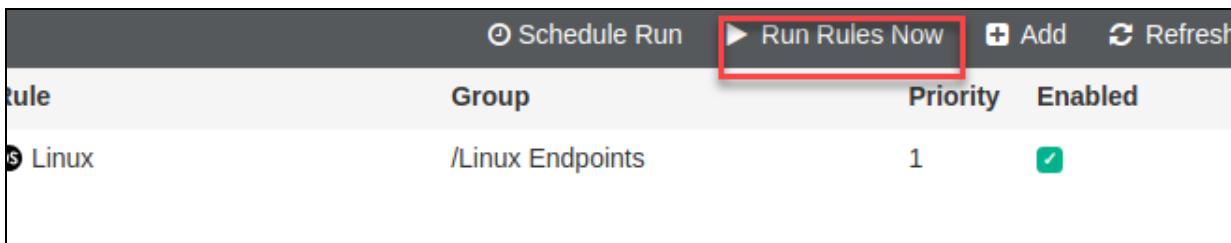
FortiClient EMS can use group assignment rules to automatically place endpoints into custom groups, based on the installer ID, IP address, OS, or AD group of the endpoints. You will create a group assignment rule based on an OS.

To create a group assignment rule

1. On the FortiClient EMS GUI, click **Endpoints > Group Assignment Rules**.
2. In the section on the right, click **Add** to create a new rule.
3. In the **Group Assignment Rule** window, configure the following settings:

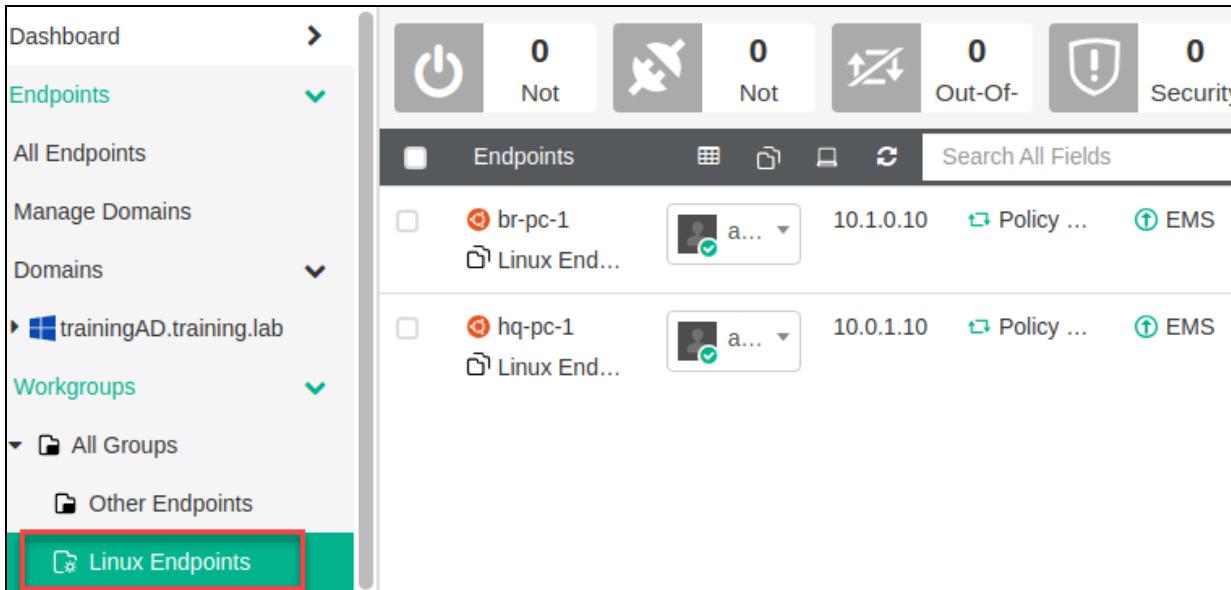
Field	Value
Type	OS
OS	Linux (L must be uppercase or this configuration will not work.)
Group	Linux Endpoints
Enable Rule	Enabled

4. Click **Save** to add a new group assignment rule.
5. In the section on the right, click **Run Rules Now** to add Linux endpoints to the new group.



Rule	Group	Priority	Enabled
Linux	/Linux Endpoints	1	<input checked="" type="checkbox"/>

br-pc-1 and hq-pc-1 are moved to the **Linux Endpoints** workgroup.



The screenshot shows the FortiClient EMS interface. On the left, a sidebar menu includes 'Dashboard', 'Endpoints' (selected), 'All Endpoints', 'Manage Domains', 'Domains' (selected), 'Workgroups' (selected), 'All Groups', 'Other Endpoints', and 'Linux Endpoints' (highlighted with a red box). The main panel displays a summary of endpoint status (0 Not, 0 Not, 0 Out-Of-Sync, 0 Security) and a list of endpoints: 'br-pc-1' (Linux Endpoint, 10.1.0.10) and 'hq-pc-1' (Linux Endpoint, 10.0.1.10). A 'Search All Fields' bar is at the top of the main panel.



FortiClient EMS automatically places endpoints that do not apply to a group assignment rule into the **Other Endpoints** group.

Create and Assign an Endpoint Policy to a Workgroup

FortiClient EMS endpoint management can assign endpoint policies to endpoint device groups of Windows, macOS, and Linux endpoints.

To create an endpoint policy

1. Continuing on the FortiClient EMS GUI, click **Endpoint Policy & Components > Manage Policies**.
2. Click **Add**.
3. In the **Endpoint Policy Name** field, type `Linux Policy`.
4. In the **Endpoint Groups** field, click **Add > Workgroups**.

Endpoint Policy

Endpoint Policy Name

Endpoint Groups Filter Endpoint Groups

Path / group	Domain	Workgroups
No Groups Assigned		

Total: 0

Users

5. Click **Skip**.

Tutorial On How To Assign Workgroups

Workgroups

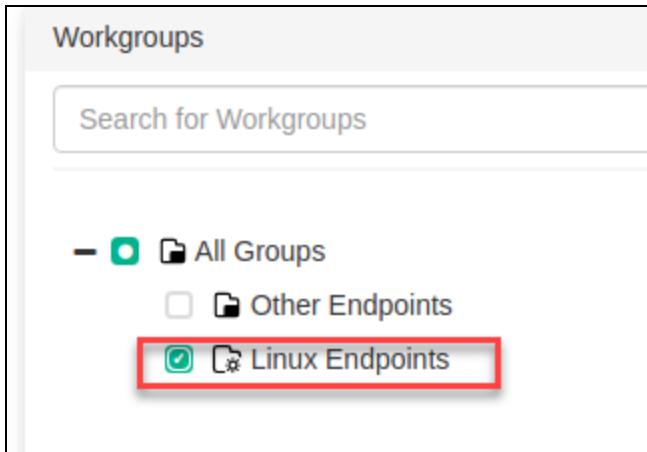
All Groups

Changes to selected Workgroups		<input type="button" value="Revert Changes"/>
Status	Path	
<input checked="" type="checkbox"/> Will be Added	All Groups	

To assign entire Workgroup, the user needs to select the parent Workgroup. All Workgroups will be assigned.

Skip

6. Select the **Linux Endpoints** checkbox, and then click **Save**.



7. Click **Save**.

The **Linux Endpoints** workgroup is managed by the **Linux Policy** endpoint policy, while the Windows AD endpoint is still managed by the **Default** endpoint policy.

Name	Assigned Gro...	Endpoint ...	Profile ...	Off-Fabri...	Policy C...	St...
Linux Policy	<input type="checkbox"/> All Groups/Li...	2	<input type="checkbox"/> VPN <input type="checkbox"/> ZTNA <input type="checkbox"/> WF <input type="checkbox"/> VF <input type="checkbox"/> VULN <input type="checkbox"/> MW <input type="checkbox"/> SB <input type="checkbox"/> FW <input type="checkbox"/> SYS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Enabled	
Default	<input type="checkbox"/> 1		<input type="checkbox"/> VPN <input type="checkbox"/> ZTNA <input type="checkbox"/> WF <input type="checkbox"/> VF <input type="checkbox"/> VULN <input type="checkbox"/> MW <input type="checkbox"/> SB	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Enabled	



FortiClient EMS automatically manages endpoints using the **Default** policy if they are not assigned to specific endpoint policies.

Exercise 2: Configuring On-Fabric Detection Rules

In this exercise, you will configure on-fabric rules on FortiClient EMS to determine the fabric status of the endpoint.

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 HQ-EMS-1 VM, log in to the FortiClient EMS GUI.
2. Click **Endpoint Policy & Components > On-fabric Detection Rules**.
3. Click **Add**.
4. In the **Name** field, type **On-Premises**.
5. In the **Rules** section, click **Add Rule**.
6. In the **Detection Type** field, select **Default Gateway**.
7. In the **IP Address** field, type **10.0.1.254**.
8. Click **Add Rule**.

On-Fabric Rule Set

Name	On-Premises
Enabled	<input checked="" type="checkbox"/>
Comments	Optional
Rules	
Rule Type	Criteria
Default Gateway	<input type="text"/> IP 10.0.1.254
Save Cancel	

9. Click **Save**.



The default gateway you specified in the on-fabric rule is the IP address of the HQ-NGFW FortiGate. The HQ-PC-1 VM uses this gateway.

10. Click **Endpoint Profiles > Remote Access**.
11. Click **Add**.
12. In the **Name** field, type **NO-VPN**.
13. Disable **Remote Access Profile**.

Remote Access Profile

Name

General

Allow Personal VPN

Show VPN before Logon

14. Click **Save**.
15. Click **Endpoint Policy & Components > Manage Policies**.
16. Select the **Linux Policy** policy, and then click **Edit**.
17. Enable **Profile (Off-Fabric)**.

There are two profile columns. The one on the right is the **Off-Fabric** profile.

18. In the **On-Fabric** profile, in the **VPN** field, select **NO-VPN**.

Endpoint Policy

Endpoint Policy Name	Linux Policy						
Endpoint Groups	<input type="button"/> Filter Endpoint Groups <input type="button"/> Delete <input type="button"/> Edit						
	<input type="checkbox"/> Path / group Domain Type						
	<input type="checkbox"/> Linux Endpoints <input type="checkbox"/> Workgroups						
	Showing: 1 Total: 1						
Users	Optional						
Profile (Off-Fabric) <input type="button"/>	<input checked="" type="checkbox"/>						
Profile	<table border="1"><tr><td colspan="2">On-Fabric</td><td>Off-Fabric</td></tr><tr><td>VPN <input type="button"/></td><td><input type="button"/> <input type="radio"/> NO-VPN <input type="button"/></td><td><input type="button"/> <input type="radio"/> Default <input type="button"/></td></tr></table>	On-Fabric		Off-Fabric	VPN <input type="button"/>	<input type="button"/> <input type="radio"/> NO-VPN <input type="button"/>	<input type="button"/> <input type="radio"/> Default <input type="button"/>
On-Fabric		Off-Fabric					
VPN <input type="button"/>	<input type="button"/> <input type="radio"/> NO-VPN <input type="button"/>	<input type="button"/> <input type="radio"/> Default <input type="button"/>					

19. In the **On-Fabric Detection Rules** field, select **On-Premises**.

Endpoint Policy

SB <input type="button"/> <input type="radio"/> Default <input type="button"/> <input type="radio"/> Default <input type="button"/>	FW <input type="button"/> <input type="radio"/> Default <input type="button"/> <input type="radio"/> Default <input type="button"/>	SYS <input type="button"/> <input type="radio"/> Default <input type="button"/> <input type="radio"/> Default <input type="button"/>
Download Profile XML <input type="button"/> Profile XML <input type="button"/> Off-Fabric Profile XML		
On-Fabric Detection Rules <input type="button"/> <input checked="" type="radio"/> On-Premises <input type="button"/> <input type="button"/> <input type="button"/>		
Comments <input type="button"/> Optional <input type="button"/> Optional		
Priority <input type="button"/> 1 <input type="button"/> Edit		

20. Click **Save**.



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 HQ-PC-1 VM, open a terminal window, enter the `ip route show` command, and then make a note of your default gateway.

```
admin@hq-pc-1:~$ ip route show
default via 10.0.1.254 dev ens3 proto static metric 100
10.0.1.0/24 dev ens3 proto kernel scope link src 10.0.1.10 metric 100
169.254.0.0/16 dev ens3 scope link metric 1000
192.168.0.0/24 dev ens4 proto kernel scope link src 192.168.0.10 metric 101
admin@hq-pc-1:~$
```

2. Open the FortiClient console, and then click the user avatar.

The fabric status is **On-fabric** and a remote access profile is not available.

The screenshot shows the FortiClient console interface. On the left, a sidebar menu includes 'ZERO TRUST TELEMETRY', 'VULNERABILITY SCAN', 'Settings', and 'About'. The main area displays a user profile for 'admin'. The profile picture is a placeholder (grey silhouette). To the right, there is a 'Get personal info from' section with 'User Input' and 'OS' (selected). The 'OS' section shows 'Updated 11/18/2024 11:25:45 PM'. Below this, a table shows endpoint details:

Status	Online/On-fabric
Hostname	hq-pc-1
Domain	



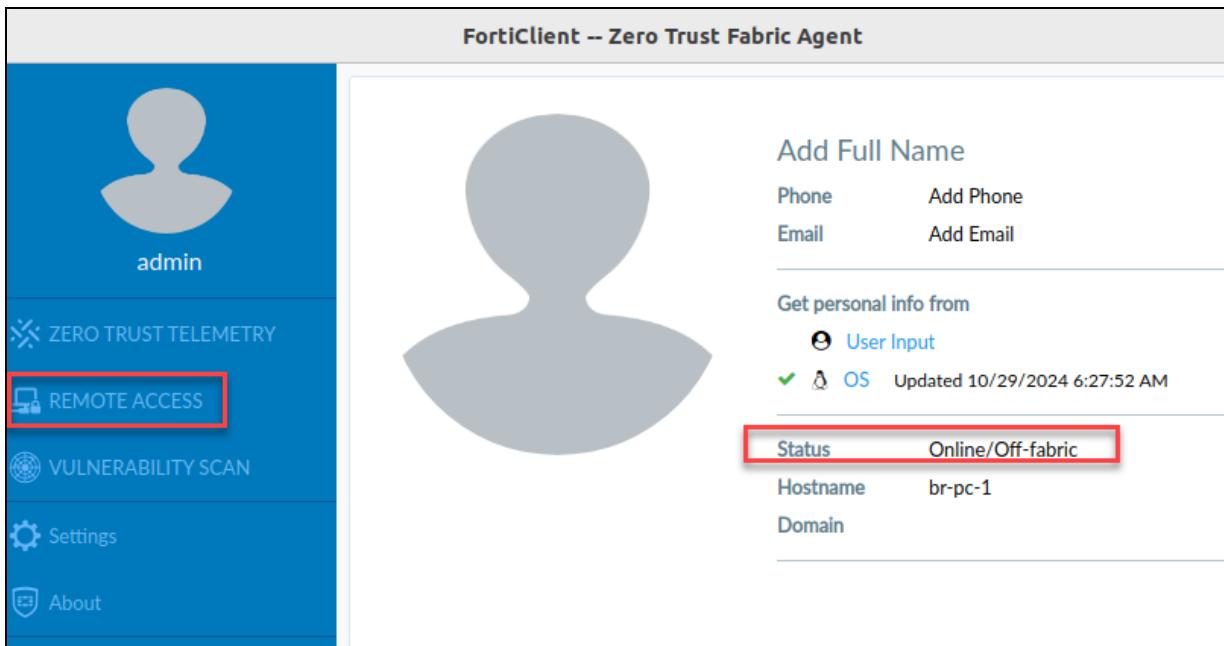
The default gateway on the HQ-PC-1 VM matches the IP address specified in the on-fabric rule. The endpoint was classified as on-fabric and the endpoint policy removed the remote access profile.

3. On the BR-PC-1 VM, open a terminal window, enter the `ip route show` command, and then make a note of your default gateway.

The gateway is **10.1.0.254** and does not match the on-fabric rules that have been configured.

4. Open the FortiClient console, and then click the user avatar.

The fabric status is **Off-fabric** and a remote access profile is also available.

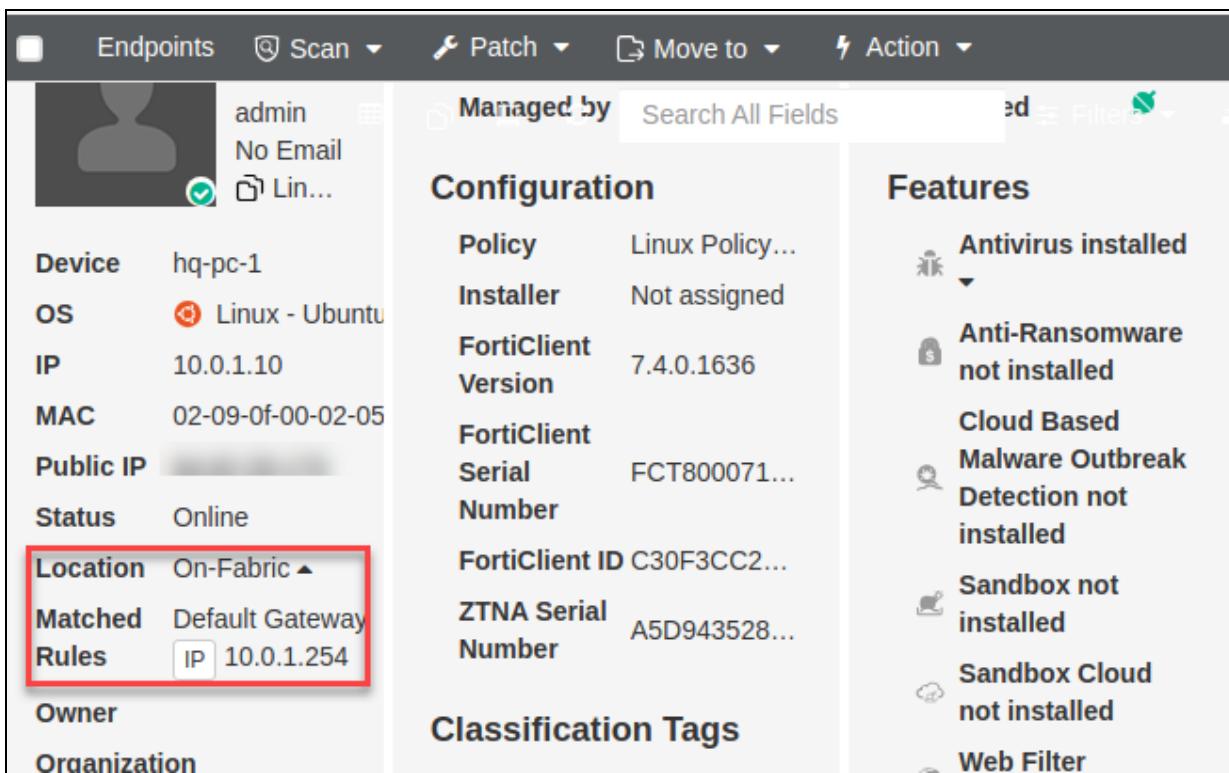


The off-fabric and on-fabric endpoints have different endpoint profiles assigned based on their fabric status.

5. Return to the FortiClient EMS GUI, and then click **Endpoints > All Endpoints**.

6. Click **hq-pc-1**.

The **Location** of the endpoint is classified as **On-Fabric** and matches the rule you configured earlier for on-fabric detection.



Endpoints Scan Patch Move to Action

Managed by Search All Fields

Configuration

Device	hq-pc-1	Policy	Linux Policy...
OS	Linux - Ubuntu	Installer	Not assigned
IP	10.0.1.10	FortiClient Version	7.4.0.1636
MAC	02-09-0f-00-02-05	FortiClient Serial	FCT800071...
Public IP	[REDACTED]	Number	
Status	Online	FortiClient ID	C30F3CC2...
Location	On-Fabric	ZTNA Serial Number	A5D943528...
Matched Rules	Default Gateway		
Owner			
Organization			

Features

- Antivirus installed
- Anti-Ransomware not installed
- Cloud Based Malware Outbreak Detection not installed
- Sandbox not installed
- Sandbox Cloud not installed
- Web Filter

Classification Tags

Lab 5: Endpoint Profiles

In this lab, you will learn about endpoint profiles and provision them on FortiClient endpoints using FortiClient EMS.

Objectives

- Enable the web filter, vulnerability scan, and antivirus features
- Create a policy to assign a new endpoint profile to an endpoint policy
- Test the security features on FortiClient endpoints

Time to Complete

Estimated: 35 minutes

Prerequisites (Self-Paced Only)

Before you begin this lab, you must identify the IP address of the FortiClient EMS, Windows-AD VM, and install FortiClient on Windows endpoint.



Do not perform these steps if you are taking an instructor-led class. These steps are required only if you are performing the self-paced labs.

To identify the IP address of the FortiClient EMS

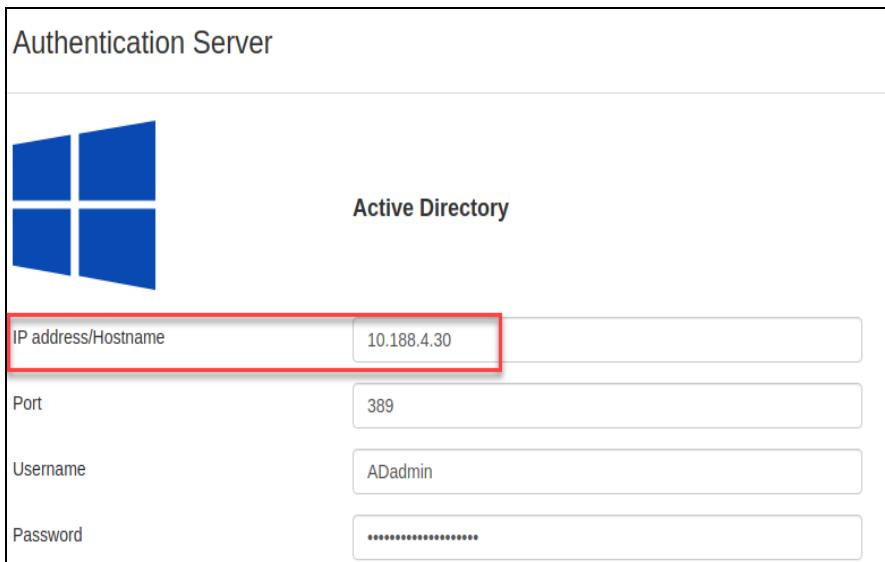
1. On the Fortinet Training Institute side bar, click **POD IP**.
2. In the **CREDENTIALS** section, under **IP address**, locate and make a note of the IP address.
You will use this address where the lab asks for <FortiClient EMS IP address>.

To identify the IP address of the Windows-AD VM

1. On the Fortinet Training Institute side bar, click **Windows-AD**.
2. In the **CREDENTIALS** section, under **IP address**, locate and make a note of the IP address.
You will use this address where the lab asks for <Windows-AD IP address>.

To update the IP address of the Windows-AD VM

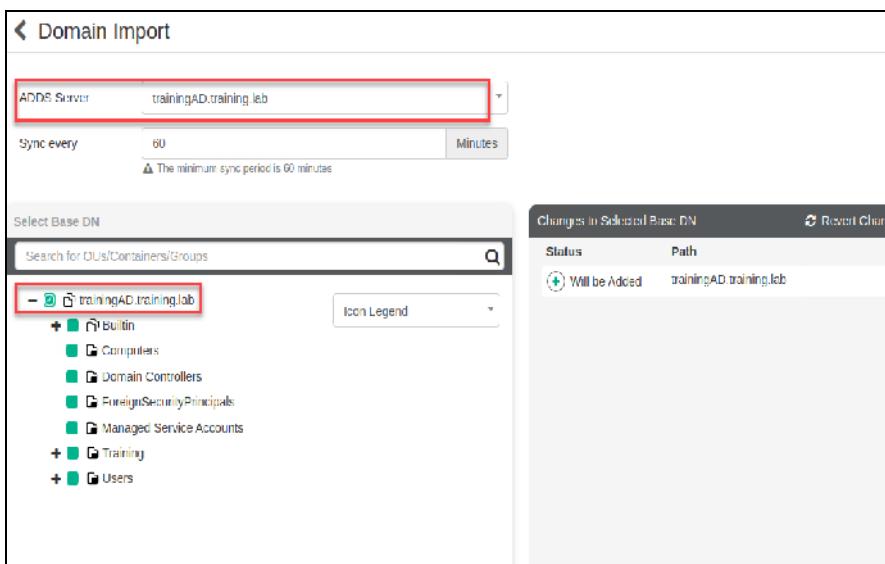
1. On the HQ-EMS-1 VM, log in to the FortiClient EMS GUI.
2. Click **Administration > Authentication Servers**, and edit the existing **Active Directory** entry.
3. Update the **IP address/Hostname** field to match the Windows-AD VM IP address.



4. Click **Test** to check the connectivity.
5. Click **Save** to save the authentication server.

To update the Domain Windows-AD VM

1. Continuing on the FortiClient EMS GUI, click **Endpoints > Manage Domains**, and delete the existing entry.
2. Click **Yes**.
3. Click **Add > ADDS** to open the **Domain Import** window.
4. In the **ADDS Server** field, select **trainingAD.training.lab**.
5. In the **Select Base DN** section, select the **trainingAD.training.lab** checkbox to add all the groups.



6. Click **Save** to import all the endpoints and users.

Install FortiClient on AD Endpoint

1. On the Windows-AD VM, on the desktop, open the **Resources** folder.
2. Double-click the **FortiClient.msi** file.
3. In the **FortiClient Setup** window, select the checkbox to accept the license agreement, and then click **Next** to start the installation.
4. In the **Choose Setup Type** window, ensure that the **Secure Remote Access, Vulnerability Scan, Advanced Persistent Threat (APT) Components, Sandbox detection, Cloud Scan**, and **ZTNA** checkboxes are selected.
5. Click **Next** to continue.
6. In the **Additional Security Features** window, select **Antivirus, Web Filtering**, and **Anti-Ransomware** checkboxes.
7. Click **Next** to continue.
8. Click **Next** to continue.
9. Click **Install** to continue.
10. After the FortiClient installation is complete, click **Finish**.
11. Open the FortiClient console.
12. In the **Enter Server address or Invitation code** field, type the <FortiClient EMS IP address>.
13. Click **Connect**.
14. In the **Invalid certificate detected** window, click **Accept**.

Exercise 1: Assigning an Endpoint Profile for Deployment

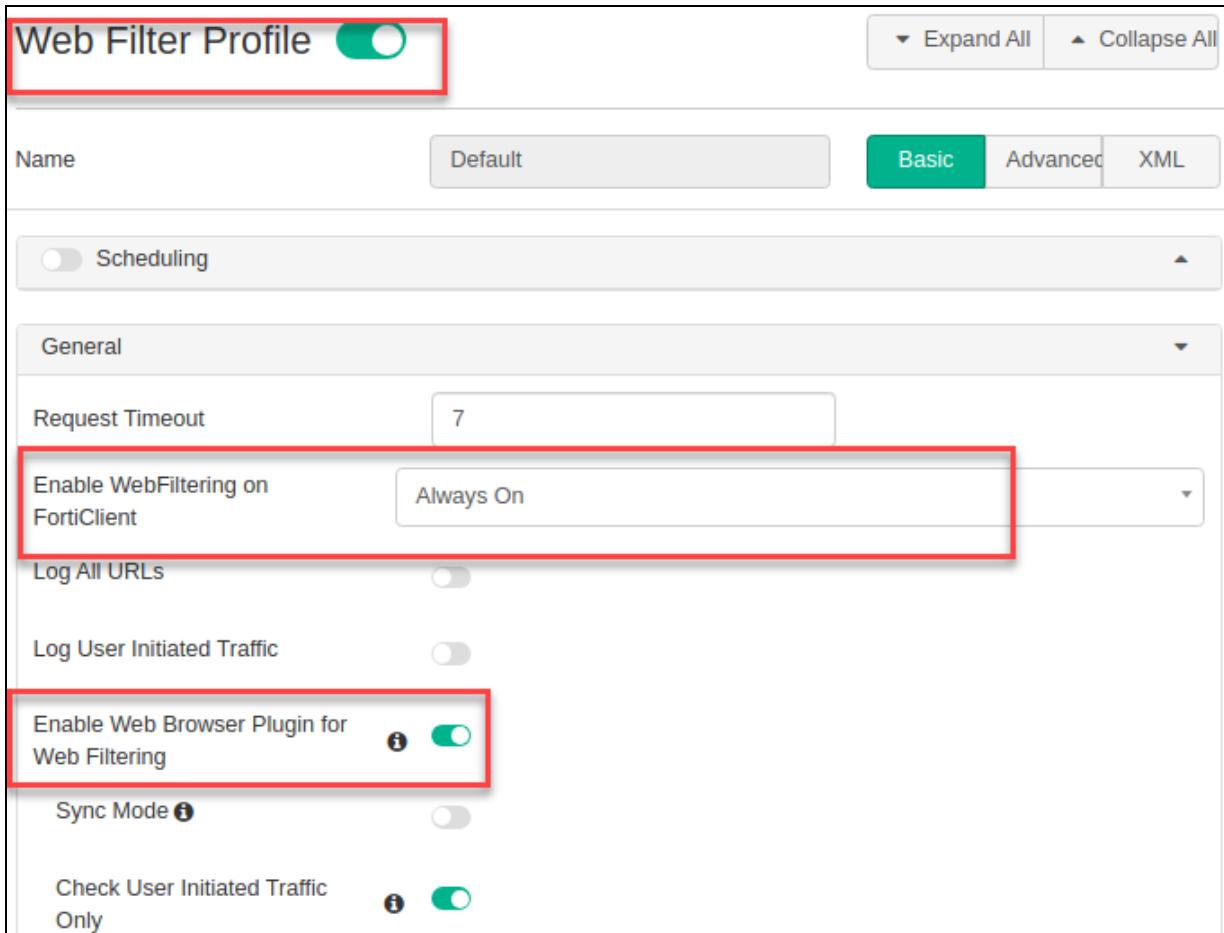
In this exercise, you will configure security profiles in the endpoint profile. After you complete provisioning, FortiClient EMS pushes the configuration to FortiClient endpoints.

Enable the Security Features in the Endpoint Profile

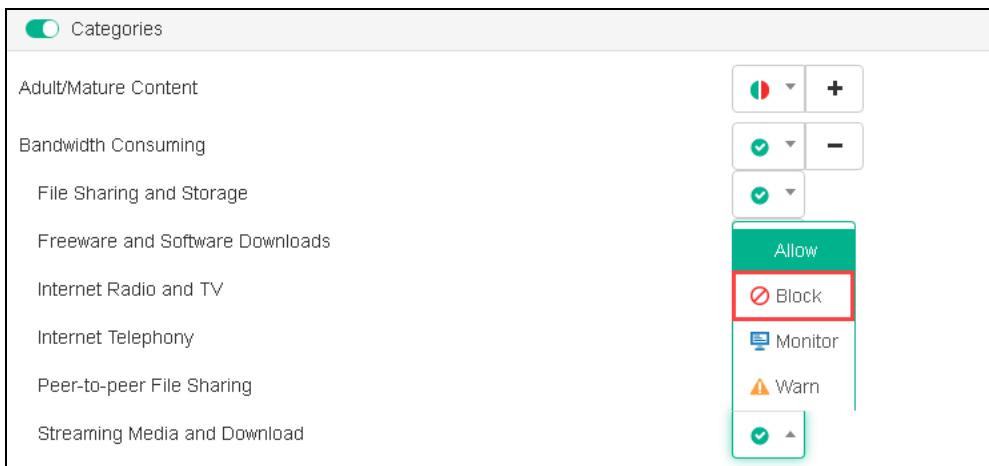
You can enable and disable security features, such as web filter, malware (antivirus), and vulnerability scan, in endpoint profiles.

To enable the web filter feature in the endpoint profile

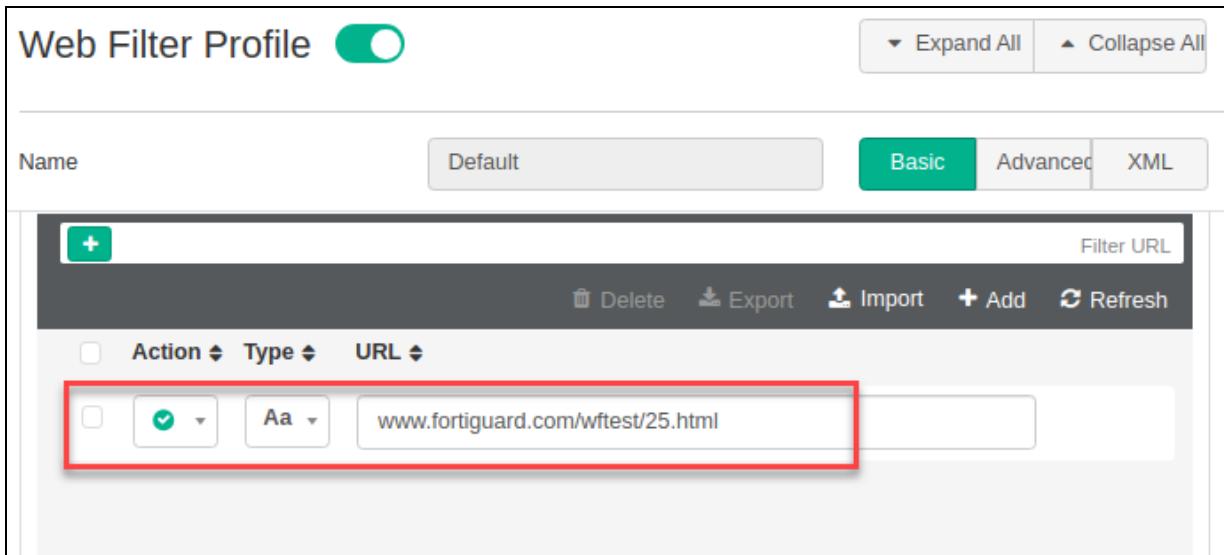
1. On the FortiClient EMS GUI, click **Endpoint Profiles > Web Filter**, select **Default**, and then click **Edit**.
2. On the **Web Filter Profile** page, enable **Web Filter Profile**, and then ensure that the value in the **Enable WebFiltering on FortiClient** field is **Always On**.
3. Enable **Enable Web Browser Plugin for Web Filtering**.



4. In the **Categories** section, in the **Bandwidth Consuming** field, click **+** to expand the list.
5. In the **Streaming Media and Download** field, select **Block**.



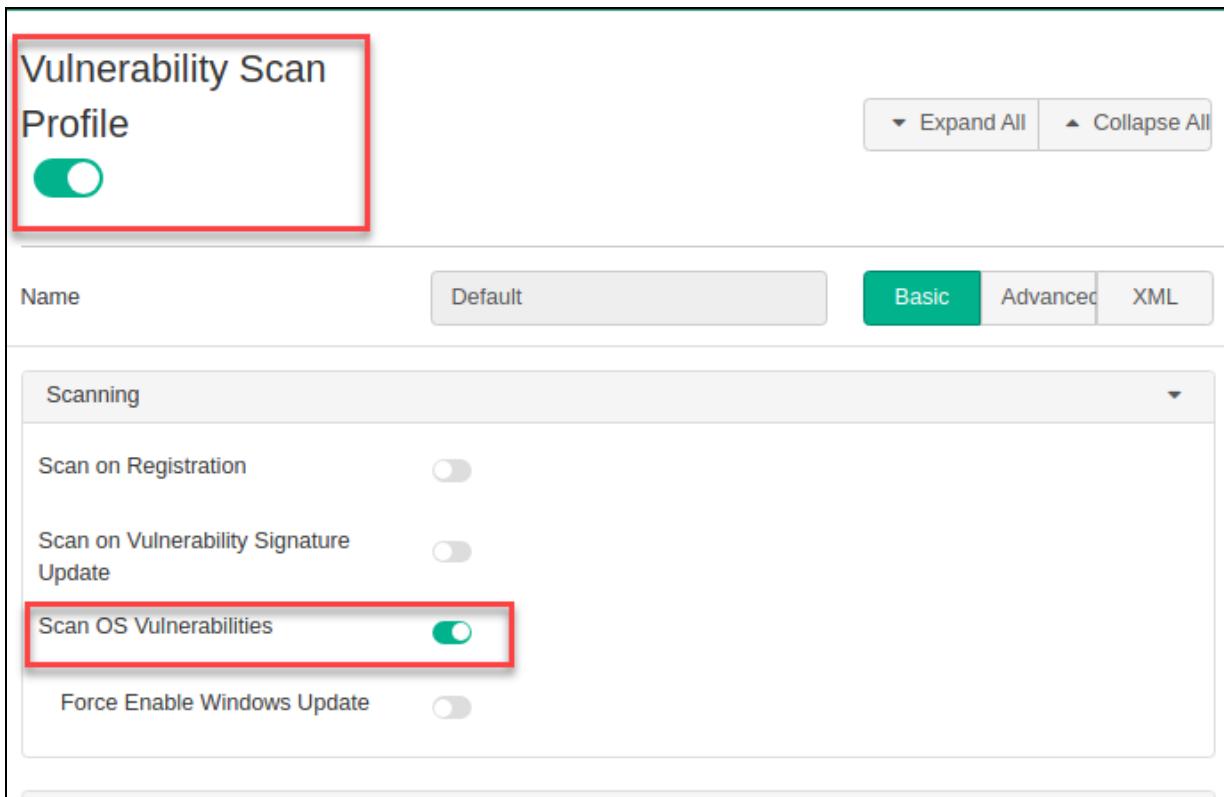
6. In the **Exclusion List** section, click **Add**, change the action to **Allow**, type www.fortiguard.com/wftest/25.html, and then leave the other settings at the default values.



7. Click **Save** to apply the web filter profile.

To verify the vulnerability scan configuration in the endpoint profile

1. Continuing on the **Endpoint Profiles** page, click **Vulnerability Scan**.
2. Click **Default**, and then click **Edit**.
3. On the **Vulnerability Scan Profile** page, ensure **Vulnerability Scan Profile** is enabled, and then in the **Scanning** section, ensure **Scan OS Vulnerabilities** is enabled.



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

To enable the antivirus feature in the endpoint profile

1. Continuing on the **Endpoint Profiles** page, click **Malware Protection**.
2. Click **Default**, and then click **Edit**.
3. Enable **AntiVirus Protection**, ensure that **Real-Time Protection** is enabled, and then leave all other settings at the default values.

Malware Protection Profile

Name: Default Basic Advanced XML

AntiVirus Protection

General

Delete Malware Files After: 100 Days

Identify Malware and Exploits Using Signatures Received From FortiSandbox:

Real-Time Protection

Alert When Viruses Are Detected:

If another AntiVirus product has already been installed: Disable FortiClient Real-Time Protection

Scan Compressed Files:

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



In this exercise, you are using the **Default** profile for the security profiles. In a production environment, you can create custom profiles and assign them to endpoint groups or domains.

Assign Endpoint Profiles to an Endpoint Policy

After you enable the endpoint profiles, you must assign the endpoint profiles to an endpoint policy. When you create this endpoint policy, the profile settings are automatically pushed to the endpoints in the domain or workgroup.

To assign endpoint profiles to an endpoint policy

1. Click **Endpoint Policy & Components > Manage Policies**, click **Linux Policy**, and then click **Edit**.
2. Ensure that the **Default** profiles are applied and enabled for **WF**, **VULN**, and **MW**.

Profile	On-Fabric	Off-Fabric
VPN	 NO-VPN	 Default
ZTNA	 Default	 Default
WF	 Default	 Default
VF	 Default	 Default
VULN	 Default	 Default
MW	 Default	 Default
SB	 Default	 Default
FW	 Default	 Default
SYS	 Default	 Default

3. Click **Save** to apply the changes.
4. Repeat steps 2-3 for the **Default** endpoint policy.

Exercise 2: Testing Antivirus Protection

In this exercise, you will test the FortiClient malware protection features that you configured in the first exercise. You will test antivirus protection to understand how FortiClient performs real-time protection.

Verify AntiVirus Protection Settings

You will verify antivirus settings on FortiClient, which you configured in the FortiClient EMS endpoint profile, and it was then pushed to FortiClient.

To view and verify current FortiClient antivirus protection settings

1. On the Windows-AD VM, open the FortiClient console, click **MALWARE PROTECTION**, and then in the **AntiVirus Protection** section, ensure that the value in the **Realtime Protection** field is **ON**.

 **AntiVirus Protection**

Realtime-protection against file cased malware & attack communication channels

Realtime Protection:	ON
AntiExploit shielded applications:	9
AntiExploit blocked exploit attempts:	0
Dynamic Threat Detection:	OFF
Virus Threats Detected:	0
Scan Schedule	Scan on the 1st day of each month at 19:30



If an antivirus scan is already in progress, stop the scan, and then click **X** to close the scan window.

2. Click the settings icon , and then verify that the **Scan files as they are downloaded or copied to my system** checkbox is selected.

— **AntiVirus Protection**

— **Settings**

Scan files as they are downloaded or copied to my system

Antimalware Scan Interface (AMSI)

Dynamic threat detection using threat intelligence data

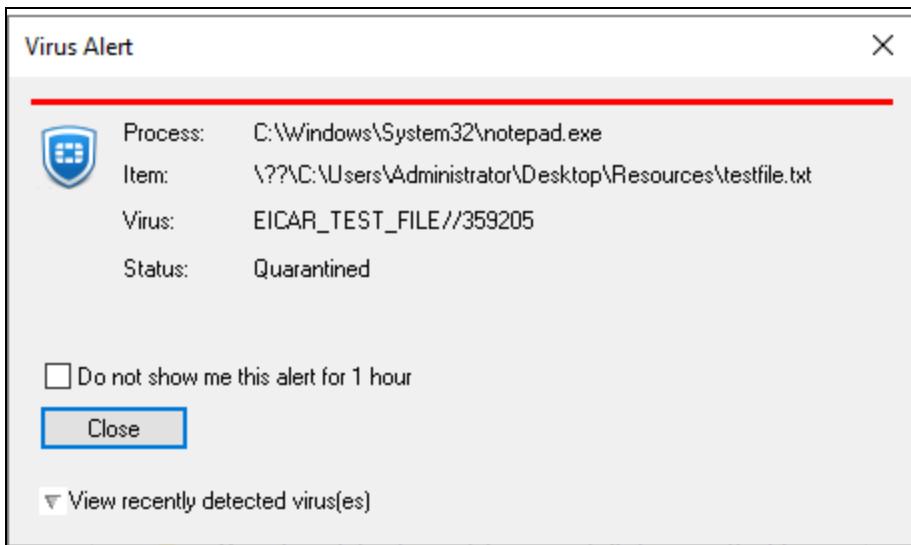
Test the Antivirus Real-Time Configuration

You will open a file that contains the EICAR virus hash on your Windows-AD VM. The EICAR test file is an industry-standard virus that is used to test antivirus detection without causing damage.

To test the antivirus configuration

1. On the Windows-AD VM, on the desktop, open the **Resources** folder.
2. Double-click the `testfile.txt` file.

The file is quarantined because it contains the EICAR virus hash.



3. Click **Close**.

4. Click **OK**.

Why did the file fail to open?

Stop and think!

Because the file is quarantined, a FortiClient EMS administrator must add it to the allowlist and restore it to view the content.

5. Return to the FortiClient EMS GUI, and then click **Quarantine Management > Files**.

It takes a few minutes for quarantined file to be displayed on FortiClient EMS.

Host	File	Size	Threat	Source	Status	Summary
JUMFDOX C:\Domain Controllers	testfile.txt D607D2070CF13092D6531E2C354D00FBA67C69C757...	72.0 B	EICAR_TEST_FILE	Realtime Scan	Quarantined 2021-12-11 03:10:10	1 instance 1 host affected

The FortiClient EMS administrator can review the quarantined file. If the file is safe, the FortiClient EMS administrator can add the file to the allowlist and restore the quarantined files. This releases the files from

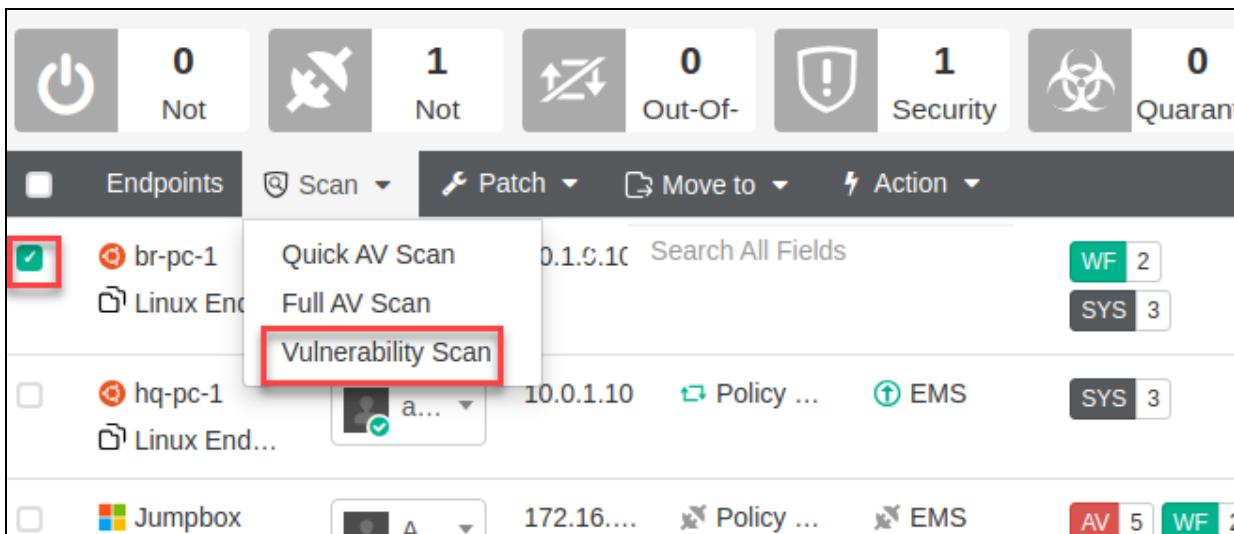
quarantine and makes them accessible on the endpoint with the next telemetry communication between FortiClient EMS and FortiClient.

Exercise 3: Performing Vulnerability Scans

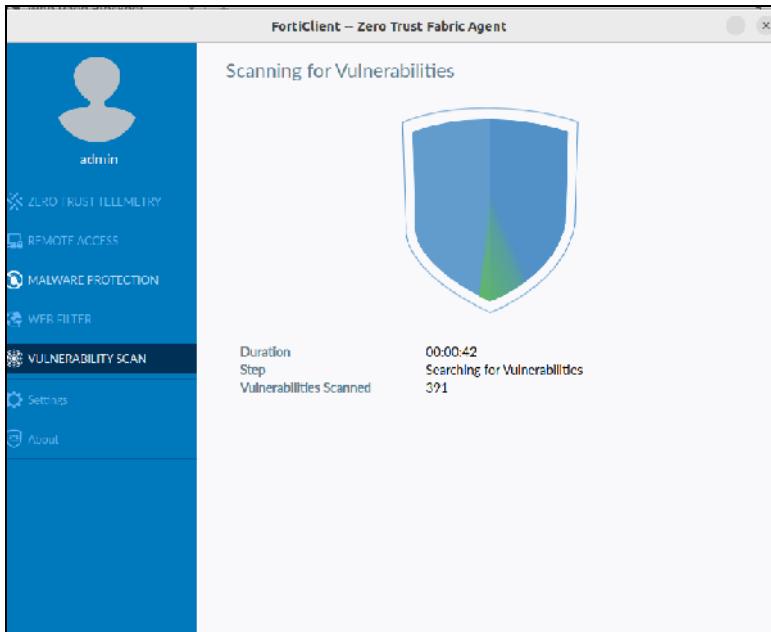
In this exercise, you will learn how a vulnerability scan helps detect and patch application vulnerabilities that can be exploited by known and unknown threats. You will run a vulnerability scan from FortiClient EMS to a registered FortiClient endpoint. You already enabled the vulnerability endpoint profile in the first exercise, and it was then pushed to FortiClient.

To run a vulnerability scan from FortiClient EMS

1. On the FortiClient EMS GUI, click **Endpoints > All Endpoints**, and then select the **br-pc-1** checkbox.
2. Click **Scan**, and then select **Vulnerability Scan** to perform a vulnerability scan on the selected endpoint.



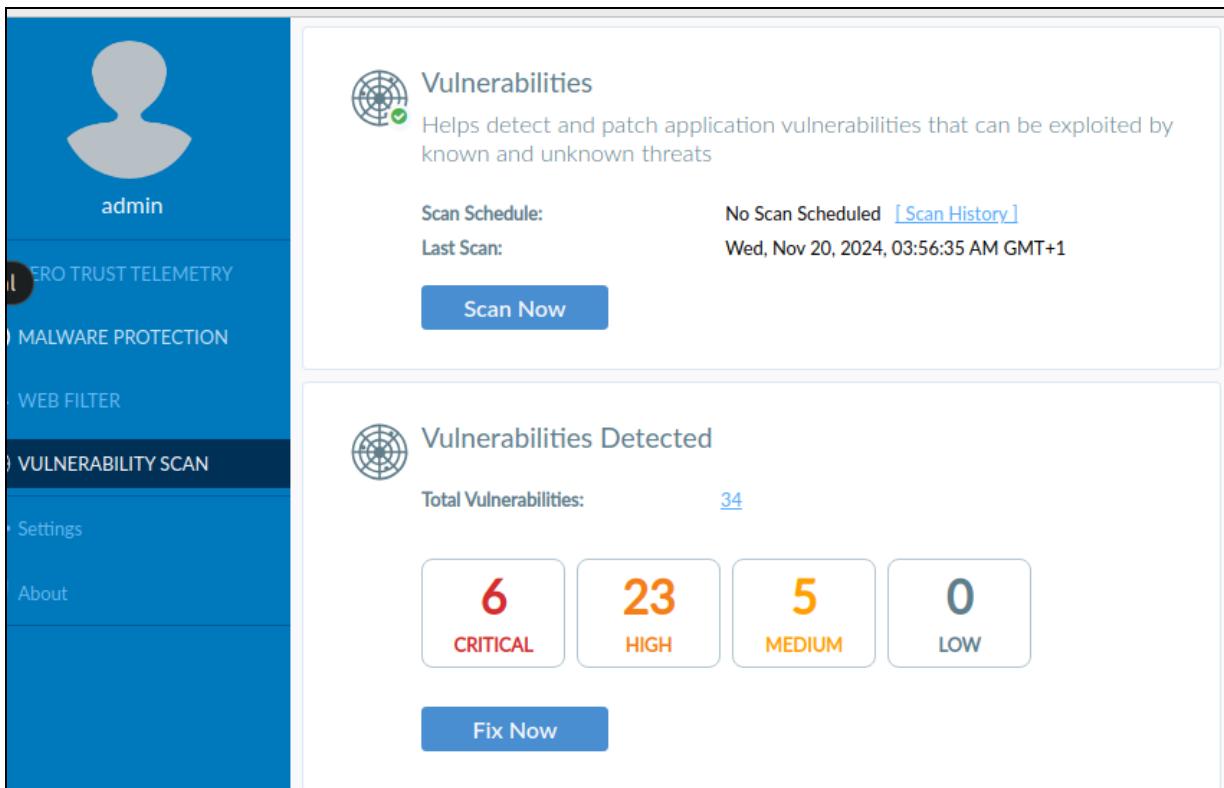
3. On the BR-PC-1 VM, open the FortiClient console, and then click **VULNERABILITY SCAN** to view the scan progress.
It will take a few minutes for the vulnerability scan to complete.



To review the vulnerability scan results

1. After the scan is finished, close the scan window.

Vulnerability information appears on the FortiClient console, similar to the following example:

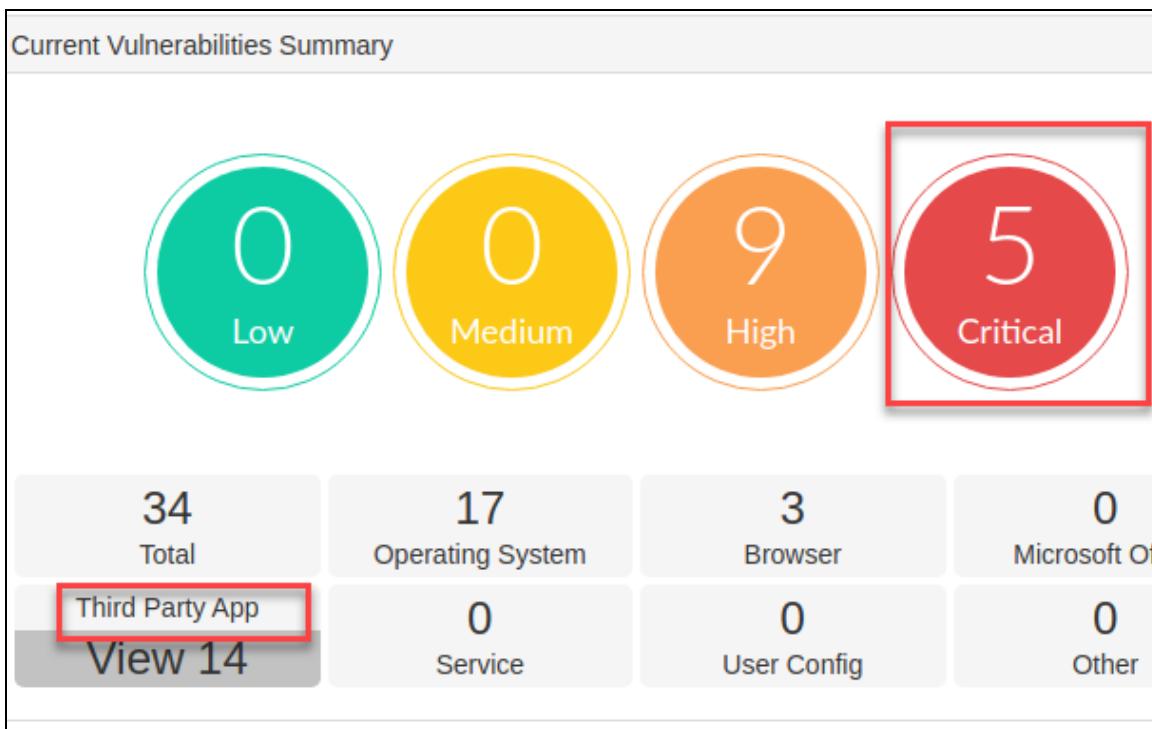


2. To review the vulnerability details, click **CRITICAL**, and then expand **3rd Party App**.

3rd Party App (1)			
APPLICATIONS	SEVERITY	RECOMMENDED ACTION	
thunderbird 1:102.15.0+build1-Oubuntu0.22.04.1 (5)	Critical	Auto-Patch	
VULNERABILITY NAME			
Security Vulnerabilities fixed in thunderbird USN-6405-1	Critical	≡	
Security Vulnerabilities fixed in thunderbird USN-6468-1	Critical	≡	
Security Vulnerabilities fixed in Ubuntu thunderbird USN-6903-1	Critical	≡	
Security Vulnerabilities fixed in Ubuntu thunderbird USN-6995-1	Critical	≡	
Ubuntu thunderbird CVE-2024-9680 Vulnerability	Critical	≡	

In this case, FortiClient can install the software patch because the recommended action is **Auto-Patch**.

3. Close all the windows.
4. Return to the FortiClient EMS GUI, and then click **Dashboard > Vulnerability Scan**.
5. In the **Current Vulnerabilities Summary** widget, click **Third Party App**, and then click **Critical** to view the critical vulnerabilities on the affected endpoint.



In this case, the FortiClient EMS administrator has the option to patch the endpoint for these specific vulnerabilities.

Security Vulnerabilities fixed in thunderbird USN-...	77285	CVE-2023-57...	1	<button>Patch</button>
Security Vulnerabilities fixed in Ubuntu thunderbi...	80548	CVE-2024-66...	1	<button>Patch</button>
Security Vulnerabilities fixed in Ubuntu thunderbi...	81065	CVE-2024-75...	1	<button>Patch</button>
Ubuntu thunderbird CVE-2024-9680 Vulnerability	81681	CVE-2024-9680	1	<button>Patch</button>

6. In the **Affected Endpoints** column, for any vulnerability, click the number.

Critical Severity Application Vulnerabilities					
Vulnerability Name	Send Message	FortiClient	CVE...	Affecte...	Patch...
Security Vulnerabilities fixed in thun...	76686	CVE-202...	1	<button>Patch</button>	
Security Vulnerabilities fixed in thun...	77285	CVE-202...	1	<button>Patch</button>	
Security Vulnerabilities fixed in Ubu...	80548	CVE-202...	1	<button>Patch</button>	
Security Vulnerabilities fixed in Ubu...	81065	CVE-202...	1	<button>Patch</button>	
Ubuntu thunderbird CVE-2024-968...	81681	CVE-202...	1	<button>Patch</button>	

The FortiClient EMS administrator can view which endpoints are impacted by vulnerabilities.



In a production environment, you should install the patches for affected applications.

Exercise 4: Testing the FortiGuard Web Filter

In this exercise, you will test the configuration (web filter profile) that you defined in a previous exercise. First, you will examine the FortiClient web filter, based on FortiGuard categories, by making sure that FortiClient can contact the FortiGuard servers. Next, you will review a category-based web filter security profile on FortiClient and inspect the web traffic.

Verify FortiGuard Connectivity

You will verify connectivity to FortiGuard Distribution Servers (FDS) from the FortiClient host VM. FDS is required because it handles URL categorization. FortiClient takes action to allow or block websites based on category.

To verify FortiGuard connectivity

1. On the BR-PC-1 VM, open the CLI, and then enter the following command:

```
ping -c 4 fgd1.fortigate.com
```

If FortiClient can contact FortiGuard, you should see the following output:

```
admin@br-pc-1:~$ ping -c 4 fgd1.fortigate.com
PING guard.fortinet.net (173.243.138.91) 56(84) bytes of data.
64 bytes from 173.243.138.91 (173.243.138.91): icmp_seq=1 ttl=55 time=63.5 ms
64 bytes from 173.243.138.91 (173.243.138.91): icmp_seq=2 ttl=55 time=60.9 ms
64 bytes from 173.243.138.91 (173.243.138.91): icmp_seq=3 ttl=55 time=60.6 ms
64 bytes from 173.243.138.91 (173.243.138.91): icmp_seq=4 ttl=55 time=63.8 ms

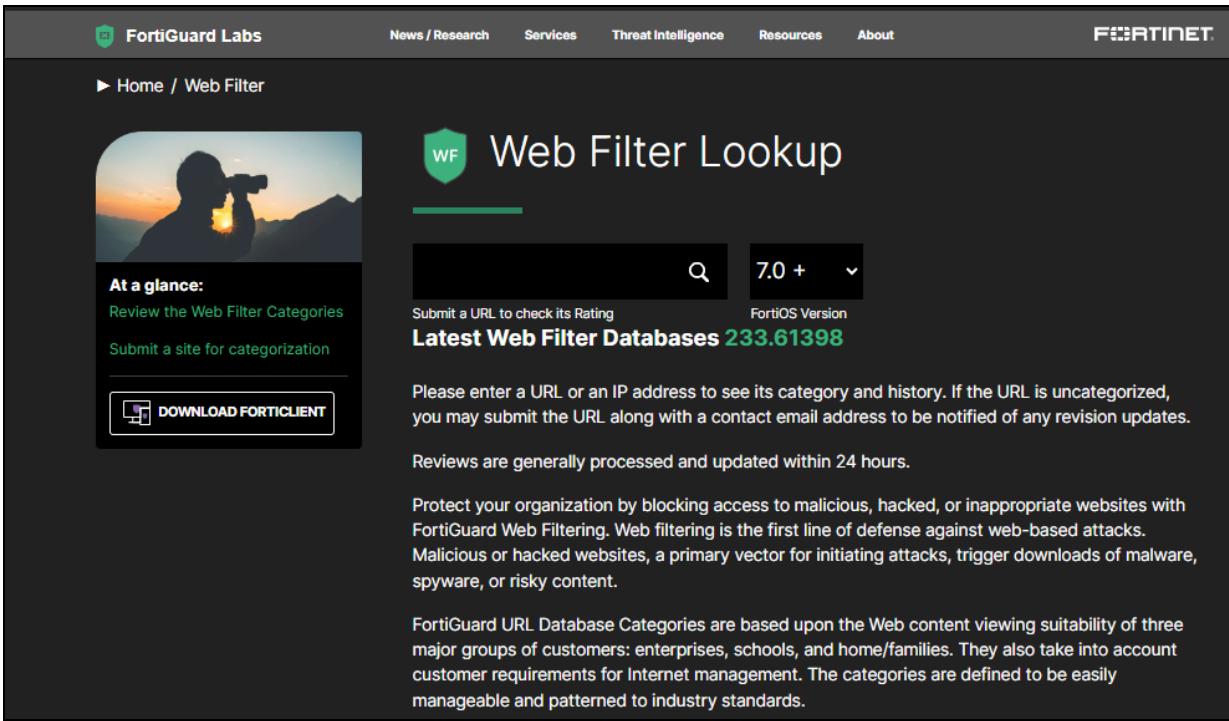
--- guard.fortinet.net ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 60.564/62.201/63.775/1.458 ms
```

Identify Web Filter Categories

To understand how websites are categorized on FortiGuard, you must first identify how the FortiGuard service categorizes specific websites.

To identify web filter categories

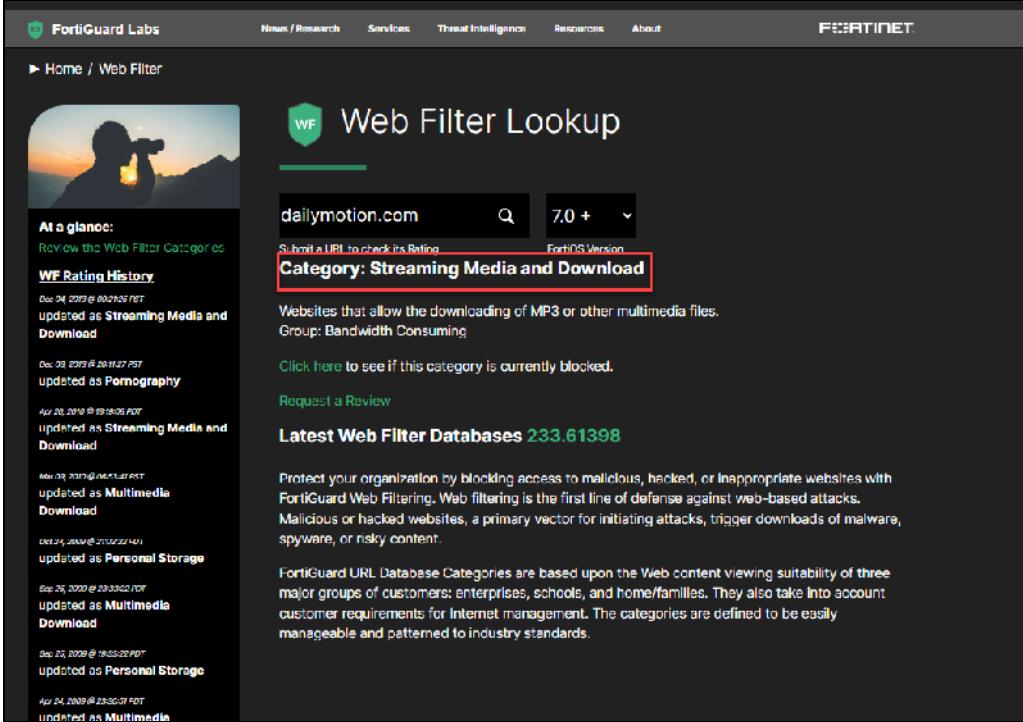
1. Continuing on the BR-PC-1 VM, open a new browser tab, and then visit <https://www.fortiguard.com/webfilter>.



The screenshot shows the homepage of the FortiGuard Labs Web Filter Lookup tool. At the top, there's a navigation bar with links for News / Research, Services, Threat Intelligence, Resources, and About. The main content area features a large image of a person looking through binoculars at a sunset. Below the image, there's a section titled "At a glance:" with links to "Review the Web Filter Categories" and "Submit a site for categorization". A "DOWNLOAD FORTICLIENT" button is also present. To the right, there's a "Web Filter Lookup" section with a search bar containing "7.0 +". Below the search bar, it says "Submit a URL to check its Rating" and "FortiOS Version". A bold text "Latest Web Filter Databases 233.61398" is displayed. The main text area explains the purpose of the tool: "Please enter a URL or an IP address to see its category and history. If the URL is uncategorized, you may submit the URL along with a contact email address to be notified of any revision updates." It also mentions that reviews are processed within 24 hours and that FortiGuard Web Filtering is a defense against web-based attacks.

2. Use the **Web Filter Lookup** tool to search for the following URL:

www.dailymotion.com



The screenshot shows the results for the URL "dailymotion.com" in the FortiGuard Web Filter Lookup tool. The "Category" is highlighted in a red box as "Streaming Media and Download". Below this, it says "Websites that allow the downloading of MP3 or other multimedia files. Group: Bandwidth Consuming". There are links to "Click here to see if this category is currently blocked." and "Request a Review". A "Latest Web Filter Databases 233.61398" link is also present. The bottom section of the page contains a summary of the tool's purpose and how it categorizes websites.

Dailymotion is listed in the **Streaming Media and Download** category.

3. Use the **Web Filter Lookup** tool again to find the web filter categories for the following website:

www.fortiguard.com/wftest/25.html

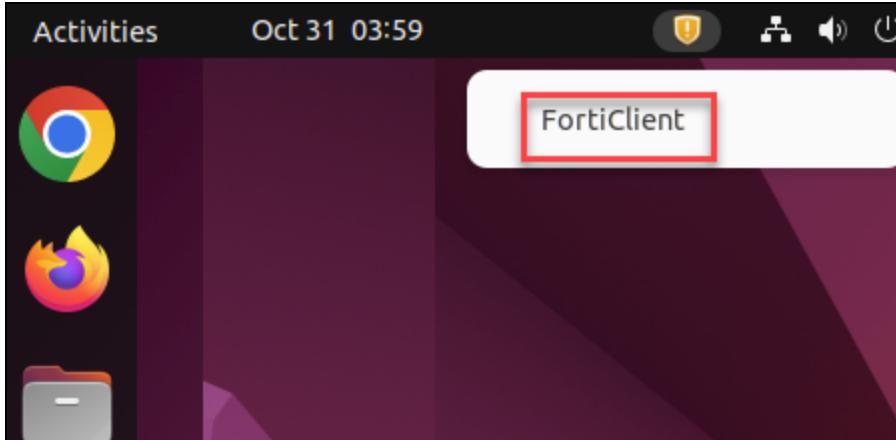
You will test your web filter using these websites.

Review a FortiGuard Category-Based Web Filter

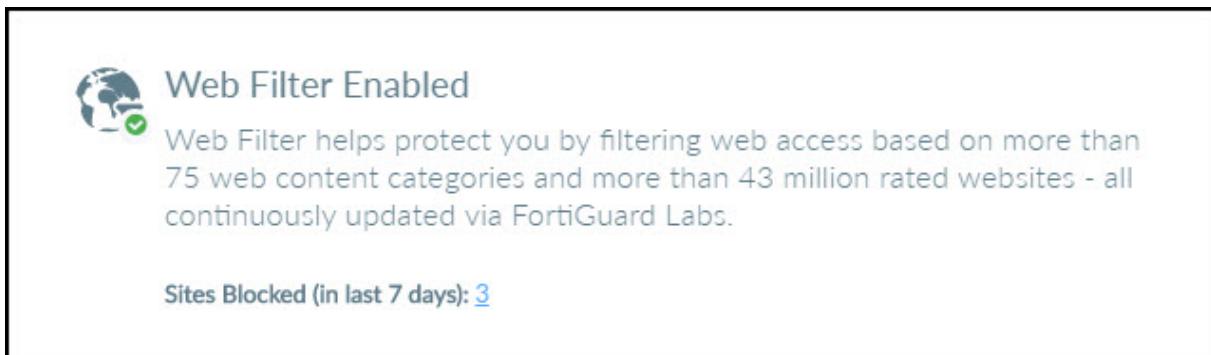
You will review the web filter profile and configuration of the FortiGuard category-based filter. These are the web filter settings that you configured in a previous exercise on endpoint profiles, which EMS then pushed to the endpoints.

To review the web filter profile

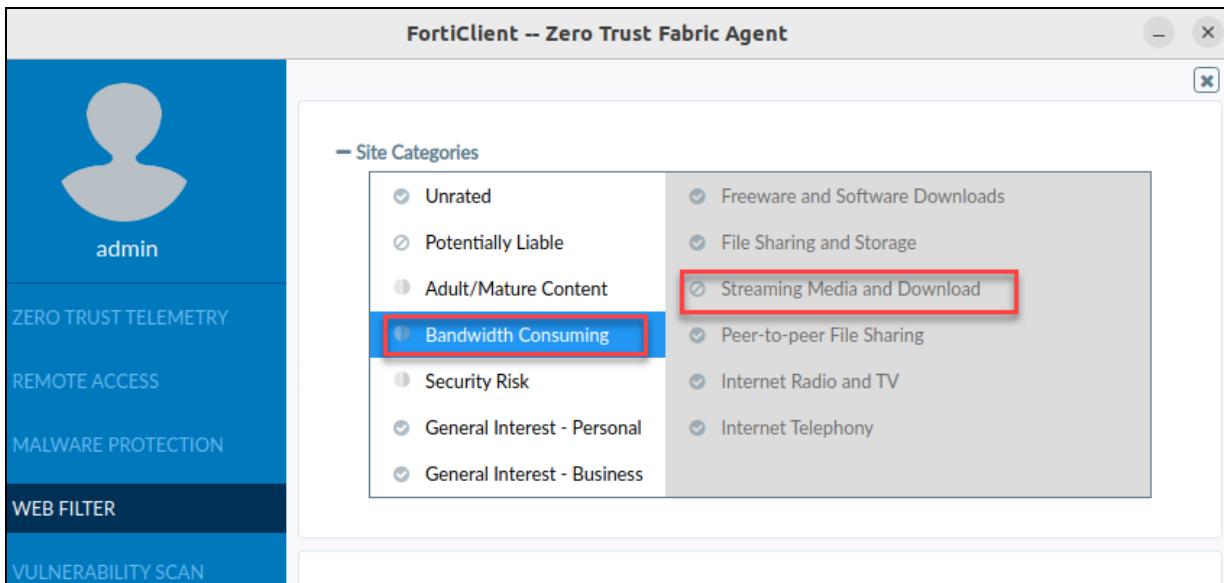
1. On the BR-PC-1 VM, click the FortiClient icon, and then click **FortiClient** to open the FortiClient GUI.



2. Click **WEB FILTER**, and then verify that **FortiGuard category based filter** is enabled.



3. In the upper-right corner, click the settings icon .
4. Click **Bandwidth Consuming** to expand it and view the subcategories.



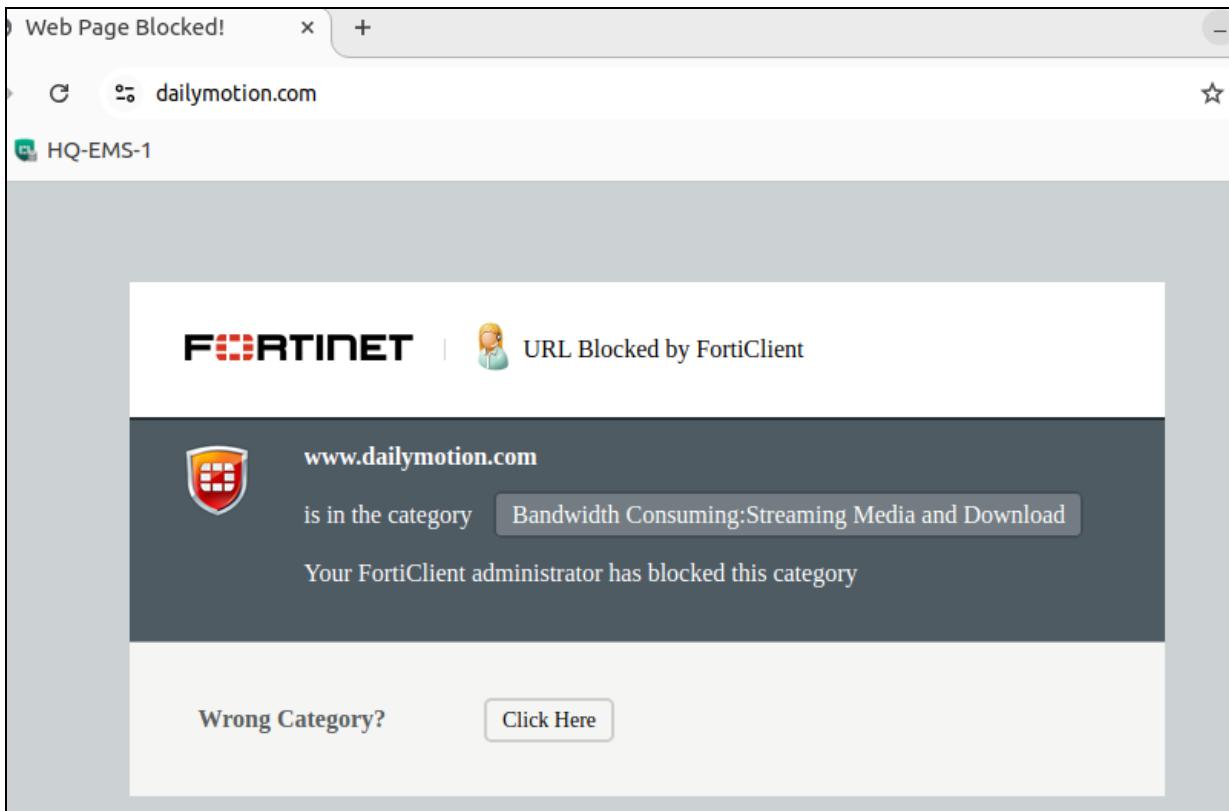
5. Verify that **Streaming Media and Download** is set to **Block**.

Test the Web Filter

You will test the web filter security profile for the configured category. You will also verify that the www.fortiguard.com/wftest/25.html URL is included in the exclusion list and test the web exclusion list.

To test the web filter

1. Continuing on the BR-PC-1 VM, open a new browser tab, and then visit www.dailymotion.com. A blocked page message is displayed because of the predefined action for this website category.



To verify a URL is included in the exclusion list

1. On the BR-PC-1 VM, open the FortiClient console, and then select **WEBFILTER**.
2. In the upper-right corner, click the settings icon .
3. Expand **Exclusion List**.

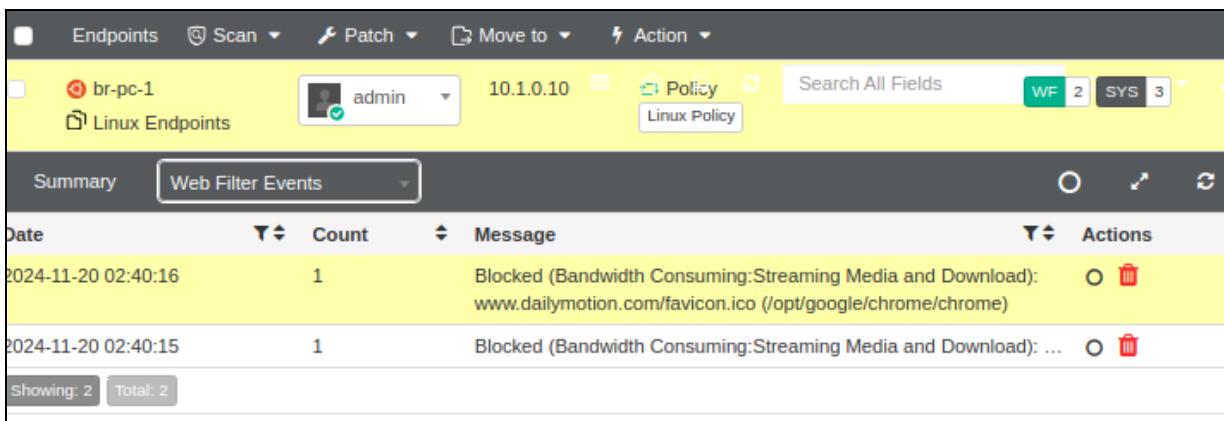
Exclusion List		
PERMISSION	TYPE	URL
<input checked="" type="checkbox"/>	URL	www.fortiguard.com/wftest/25.html

To test the web exclusion list

1. Continuing on the BR-PC-1 VM, open a new browser tab, and then try to access the website www.fortiguard.com/wftest/25.html.
This website is allowed because it matches an exclusion list to bypass the FortiGuard block category.

To review the web filter profile events for the category-based filter

1. Return to the FortiClient EMS GUI, click **Endpoints > All Endpoints**, and then click **br-pc-1**.
2. Click **Web Filter Events**.



Date	Count	Message	Actions
2024-11-20 02:40:16	1	Blocked (Bandwidth Consuming:Streaming Media and Download): www.dailymotion.com/favicon.ico (/opt/google/chrome/chrome)	<input type="radio"/> <input type="checkbox"/>
2024-11-20 02:40:15	1	Blocked (Bandwidth Consuming:Streaming Media and Download): ...	<input type="radio"/> <input type="checkbox"/>

According to the events, www.dailymotion.com was blocked because the URL belonged to a denied category—**Bandwidth Consuming: Streaming Media and Download**.

Lab 6: ZTNA

There is no lab associated with Lesson 6 at this time. You will configure ZTNA after Lesson 7.

Lab 7: Zero Trust Network Access

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 configuration on FortiClient EMS, FortiGate, and FortiClient.

Objectives

- Add FortiClient EMS to the Security Fabric
- Verify the FortiGate and FortiClient EMS connection
- Configure security posture tagging rules
- Enable the ZTNA feature on FortiGate and verify security posture tags
- Configure a basic HTTPS access proxy with SSL certificate-based authentication
- Configure a TCP forwarding access proxy SSH
- Configure ZTNA for SaaS application access

Time to Complete

Estimated: 60 minutes

Exercise 1: Adding FortiClient EMS to the Security Fabric

In this exercise, you will add FortiClient EMS to the Security Fabric.

To integrate FortiClient EMS with FortiGate

1. On the HQ-EMS-1 VM, open Google Chrome, and then in **Bookmarks**, select the **HQ-NGFW** login page bookmark.
2. Log in to the FortiGate GUI with the following credentials:
 - Username: admin
 - Password: Fortinet1!
3. Click **Security Fabric > Fabric Connectors**.
4. In the list, select **FortiClient EMS**, and then click **Edit**.
5. In the **FortiClient EMS Settings** window, select **EMS 1**, click **Enabled**, and then configure the following settings:

Field	Value
Name	EMSServer
IP/Domain name	10.0.1.100

FortiClient EMS Settings

Settings Info

EMS 1 - EMSServer

Status	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Type	<input checked="" type="radio"/> FortiClient EMS <input type="radio"/> FortiClient EMS Cloud
Name	EMSServer
IP/Domain name	10.0.1.100
HTTPS port	443
EMS threat feed <small>(i)</small>	<input checked="" type="checkbox"/>

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

Verify EMS Server Certificate

In order for the FortiClient EMS and FortiGate to communicate, the following certificate provided by the FortiClient EMS must be reviewed for correctness, and accepted if deemed valid.

⚠ Do you wish to accept the certificate as detailed below?

Version 3

Serial Number 0C:AB:4A:44:BB:E5:D2:E3

Subject:

Common Name (CN) EMS

Organization (O) Fortinet

Organization Unit (OU) Training

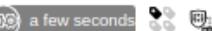
Locality (L) Ottawa

State (ST) Ontario

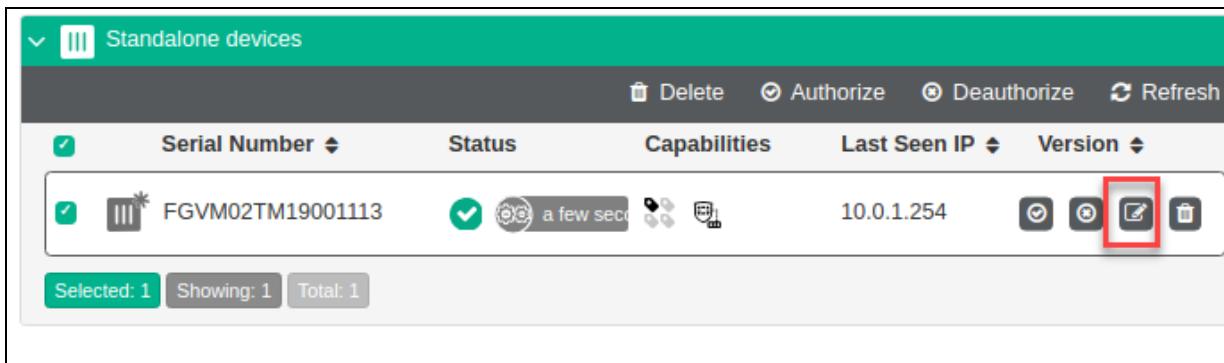
Country/Region (C) CA

Accept **Deny**

7. Click **Close** to close the **FortiClient EMS Status** warning window.
8. On the FortiClient EMS GUI, click **Administration > Fabric Devices**.
9. Select the checkbox for the FortiGate, and then click **Authorize**.

Standalone devices					
<input checked="" type="checkbox"/>	Serial Number	Status	Capabilities	Last Seen IP	Version
<input checked="" type="checkbox"/>	FGVM02TM19001113	 a few seconds		10.0.1.254	
Selected: 1 Showing: 1 Total: 1					

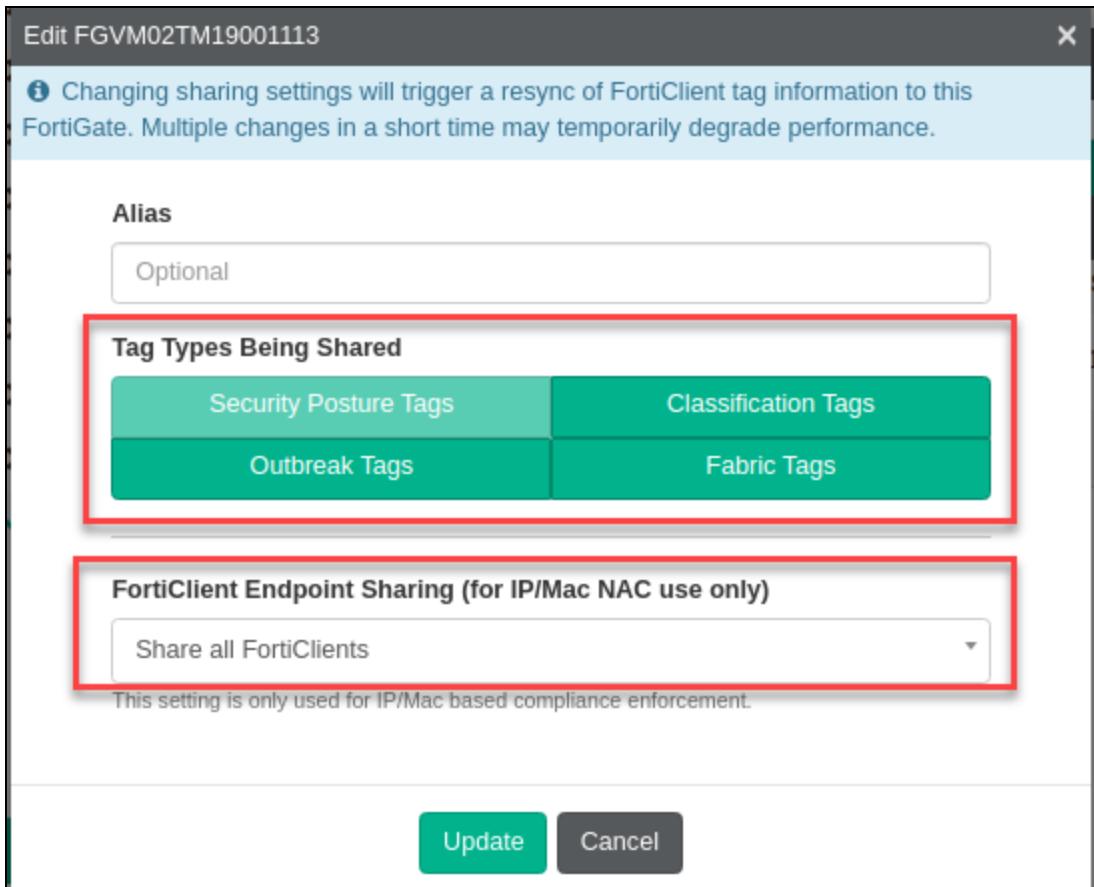
10. Select the checkbox for the FortiGate again, and then click the edit icon .



The screenshot shows a table of standalone devices. A single device is selected, and the edit icon (pencil icon) in the toolbar is highlighted with a red box.

Serial Number	Status	Capabilities	Last Seen IP	Version
FGVM02TM19001113	a few seconds	File, Print, Scan, Firewall, NAT, SSL, IPSec, FortiClient	10.0.1.254	7.4.0

11. In the **Tag Types Being Shared** field, select all tag types.
12. In the **FortiClient Endpoint Sharing (for IP/Mac NAC user only)** field, select **Share all FortiClients**.
13. Click **Update** to apply the changes.



The dialog box contains the following fields:

- Alias:** Optional (text input field)
- Tag Types Being Shared:** A grid of four buttons:
 - Security Posture Tags
 - Classification Tags
 - Outbreak Tags
 - Fabric Tags
- FortiClient Endpoint Sharing (for IP/Mac NAC use only):** A dropdown menu set to "Share all FortiClients".

This setting is only used for IP/Mac based compliance enforcement.
- Buttons:** Update (green) and Cancel (grey)

Exercise 2: Configuring Security Posture Tags, Tagging Rules, and Features

In this exercise, you will verify the connection between FortiClient, FortiClient EMS, and FortiGate. You will also configure security posture tags and tagging rules, and then verify if the tags are synchronized on FortiClient and FortiGate. These tags will be used in the next exercises to authorize user traffic based on security posture tagging rules configured on FortiClient EMS.

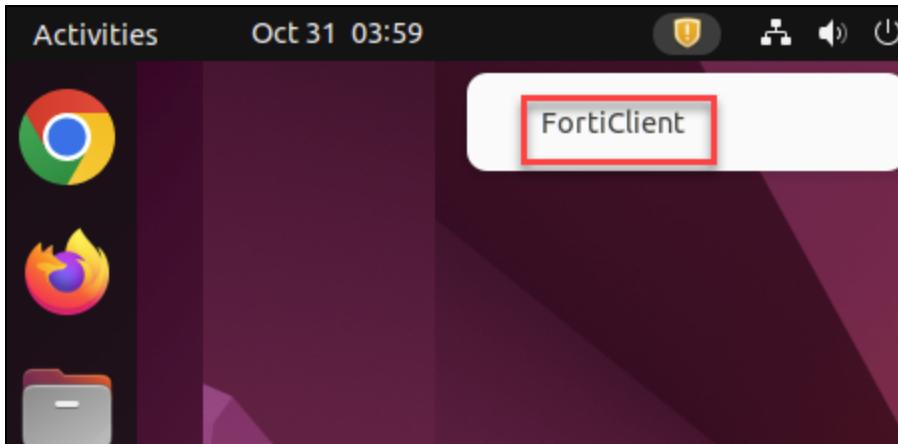
Verify the Connection Between FortiClient, FortiClient EMS, and FortiGate

Establishing device identity and device trust between FortiClient, FortiClient EMS, and FortiGate is integral to ZTNA setup. All of these devices must have a stable connection in order to exchange the information required for ZTNA tagging to work correctly.

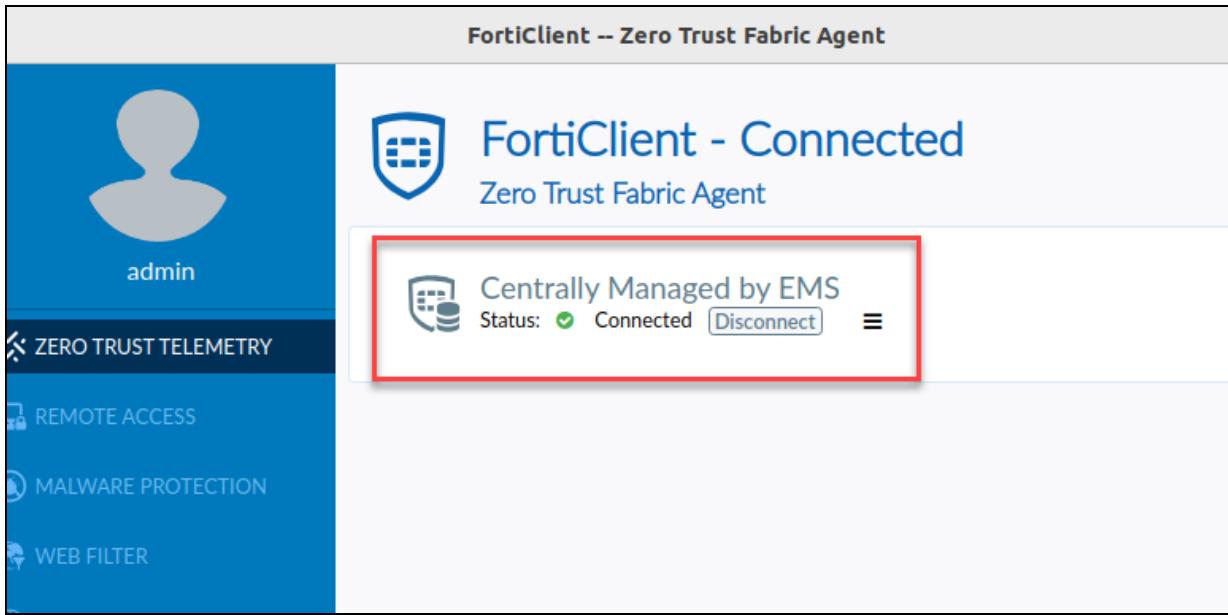
You will verify the status of telemetry connections on the FortiClient console and FortiGate Fabric connector.

To verify the FortiClient to FortiClient EMS connection

1. On the BR-PC-1 VM, click the FortiClient icon, and then click **FortiClient** to open the FortiClient GUI.

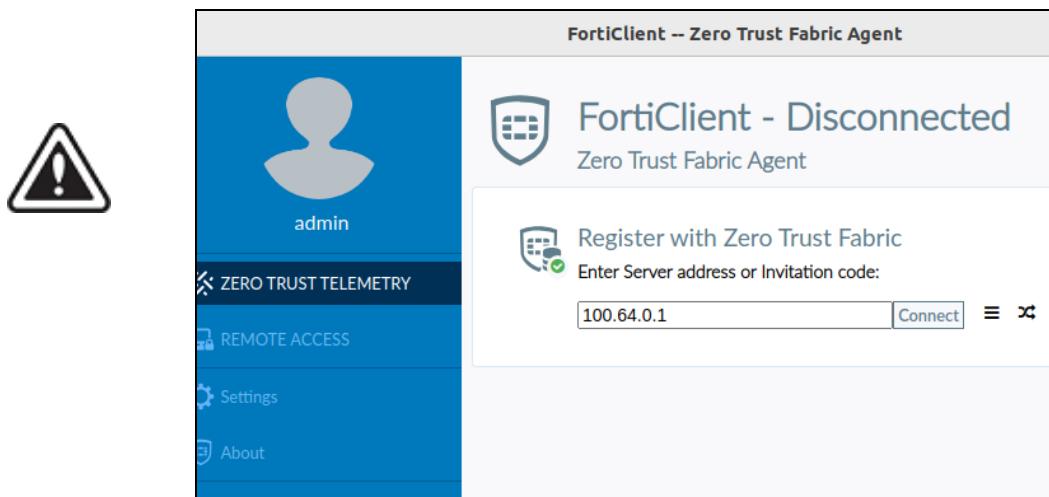


2. In the **ZERO TRUST TELEMETRY** section, ensure that the status of **Centrally Managed by EMS** is **Connected**.



If the status is **Not reachable**, you must reconnect the endpoint.

1. In the **ZERO TRUST TELEMETRY** section, click **Disconnect**.
2. In the **Enter Server address or Invitation code** field, type **100.64.0.1**, and then click **Connect** to reconnect the BR-PC-1 VM to FortiClient EMS.



To verify FortiClient EMS as the Fabric Connector

1. On the HQ-EMS-1 VM, open Chrome, and then log in to the HQ-NGFW FortiGate GUI.
2. Click **Security Fabric > Fabric Connectors**.
3. In the **FortiClient EMS** section, in the **EMSServer** field, see the connector status.

The up arrow should be green.

Core Network Security Connectors

 Security Fabric Setup

Role Standalone

LAN Edge Devices

Device Type	Device Count	Status
FortiGate	1	All authorized & registered
FortiAP	0	None configured
FortiSwitch	0	None configured
FortiExtender	0	None configured

 Logging & Analytics

FortiAnalyzer  Disabled

Cloud Logging  Disabled

 FortiClient EMS

EMSServer  Connected

IP address 10.0.1.100

You can also verify the status by entering the following command on the FortiGate CLI:



diagnose endpoint fctems test-connectivity <fctems ID>

```
HQ-NGFW-1 # diagnose endpoint fctems test-connectivity 1
Connection test was successful.
```

Configure FortiClient EMS Security Posture Tagging Rules

FortiClient EMS uses security posture tagging rules to tag endpoints based on the information that it has on each endpoint. The tags are shared with FortiGate, which then uses them to assign authorization to user traffic.

You will configure security posture tagging rules on the FortiClient EMS server.

To configure the FortiClient EMS security posture tagging rule for compliant endpoints

1. On the FortiClient EMS GUI, click **Security Posture Tags > Security Posture Tagging Rules**.
2. Click **Add**.
3. In the **Name** field, type **Compliant**.
4. In the **Tag Endpoint As** field, type **Compliant**, and then press **Enter**.
5. In the **Rules** section, click **Add Rule**, and then in the **OS** field, select **Linux**.
6. In the **Rule Type** field, select **FortiClient Version**.
7. In the **FortiClient Version** field, type **7.4.0**, and then click **Save**.
8. Click **Add Rule** again to create a second rule.
9. In the **OS** field, select **Linux**.
10. In the **Rule Type** field, select **AntiVirus Software**.
11. In the **AV Software** field, select **AntiVirus Software is installed and running**, and then click **Save**.

Security Posture Tagging Rule Set

Name	Compliant
Tag Endpoint As	Compliant
Enabled	<input checked="" type="checkbox"/>
Comments	Optional
Rules	
Type	Value
Linux (2)	
FortiClient Version	= 7.4.0
AntiVirus Software	AV Software is installed and running

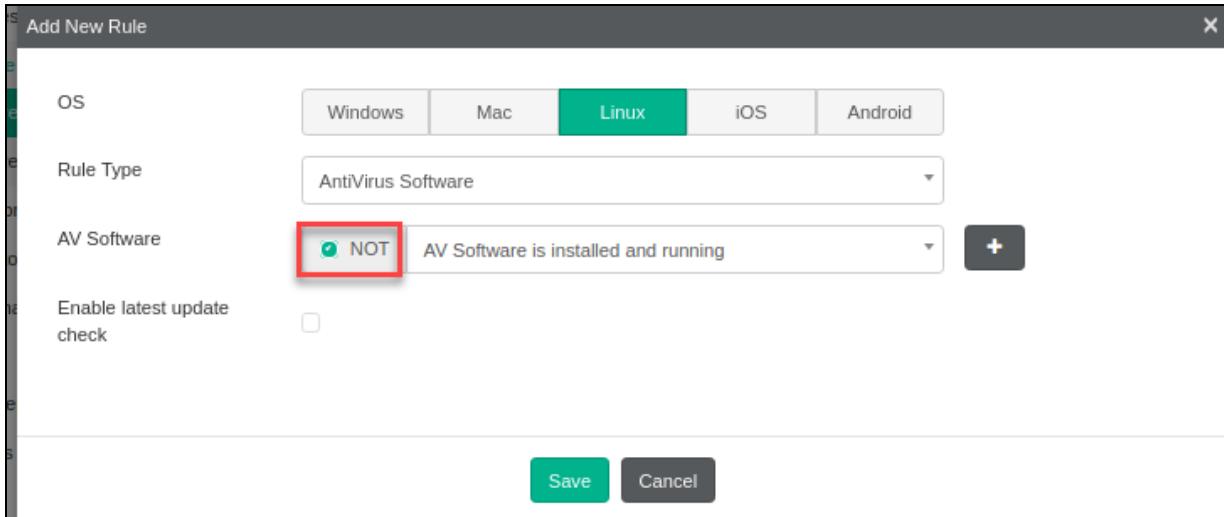
Save Cancel

12. Click **Save** to save this security posture tagging rule set.

To configure the FortiClient EMS security posture tagging rule for detecting non-compliant endpoints

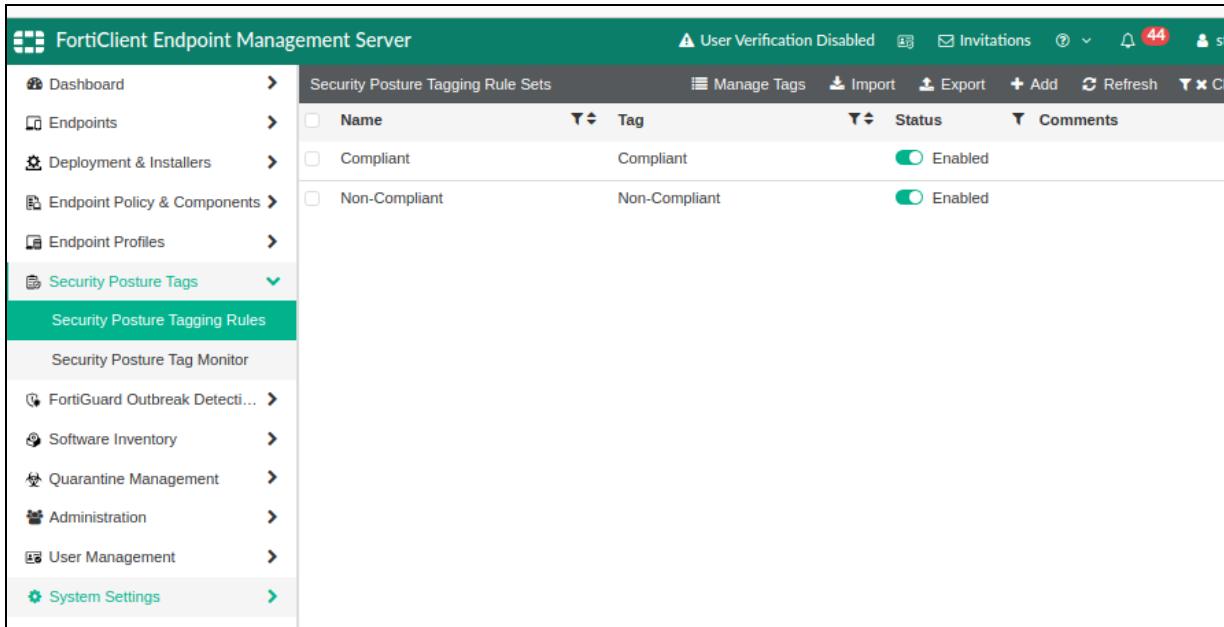
1. Click **Security Posture Tags > Security Posture Tagging Rules**.
2. Click **Add**.
3. In the **Name** field, type **Non-Compliant**.
4. In the **Tag Endpoint As** field, type **Non-Compliant**, and then press **Enter**.
5. Click **Add Rule** to create a rule.

6. In the **OS** field, select **Linux**.
7. In the **Rule Type** field, select **AntiVirus Software**.
8. In the **AV Software** field, select **AntiVirus Software is installed and running**, and then select the **NOT** checkbox.



9. Click **Save**.
10. Click **Save** to save this security posture tagging rule.

Both rules appear in the **Security Posture Tagging Rule Sets** section.



Name	Tag	Status
Compliant	Compliant	Enabled
Non-Compliant	Non-Compliant	Enabled

11. Click **Security Posture Tags > Security Posture Tag Monitor**.

br-pc-1 and **hq-pc-1** are tagged as **Compliant**. If this does not appear immediately, in the upper-right corner, click **Refresh**.

Endpoint with Tag					
Compliant (2)					
Endpoint	User	OS	IP	Category	Tagged on
br-pc-1	 admin	Linux - Ubuntu 22.0...	10.1.0.10	Security Posture	2024-11-21 02:34:06
hq-pc-1	 admin	Linux - Ubuntu 22.0...	10.0.1.10	Security Posture	2024-11-21 02:20:18

To configure the security posture tag to display on FortiClient

1. Continuing on the FortiClient EMS GUI, click **Endpoint Profiles > System Settings**.
2. Select the **Default** profile, click **Edit**, and then click **Advanced**.
3. On the **System Settings Profile** page, in the **UI** section, enable **Show Security Posture Tag on FortiClient GUI**.

System Settings Profile

Advanced (highlighted with a red box)

UI

Require Password to Disconnect From EMS

Do Not Allow User to Back up Configuration

Allow User to Shutdown When Registered to EMS

Hide User Information

Hide System Tray Icon

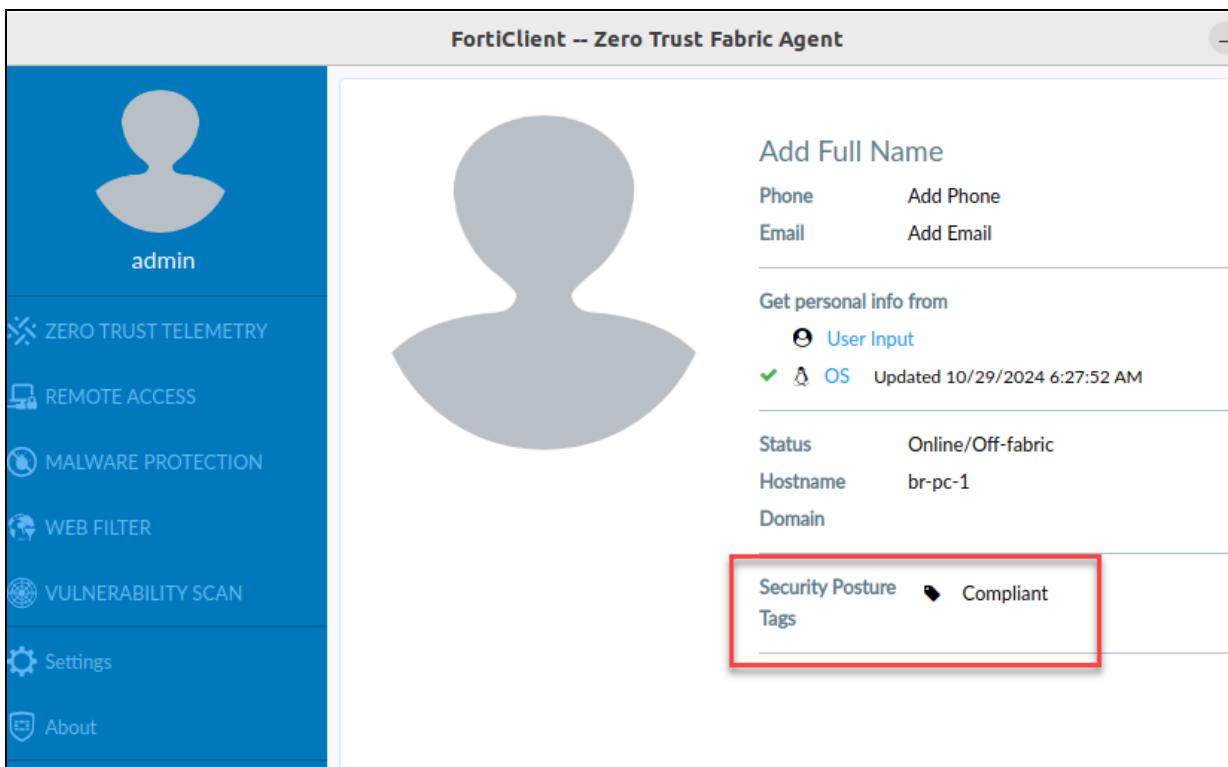
Show Security Posture Tag on FortiClient GUI (highlighted with a red box)

Language 

Default Tab

4. Click **Save** to apply the changes.
5. On the BR-PC-1 VM, on the FortiClient GUI, click the user avatar.

The **Security Posture Tags** field shows the currently detected tags.



FortiClient -- Zero Trust Fabric Agent

admin

ZERO TRUST TELEMETRY

REMOTE ACCESS

MALWARE PROTECTION

WEB FILTER

VULNERABILITY SCAN

Settings

About

Add Full Name

Phone Add Phone

Email Add Email

Get personal info from

User Input

OS Updated 10/29/2024 6:27:52 AM

Status Online/Off-fabric

Hostname br-pc-1

Domain

Security Posture Tags

Compliant

You may need to wait until the next FortiClient synchronization cycle with FortiClient EMS before the tags appear on the FortiClient console.

Enable the ZTNA Feature and Verify That ZTNA Tags Are Synchronized

You will enable the ZTNA feature on FortiGate, and then verify that the tags are synchronized between FortiClient EMS and FortiGate.

To enable the ZTNA feature and verify that ZTNA tags are synchronized on FortiGate

1. Return to the FortiGate GUI, click **System > Feature Visibility**, enable **Zero Trust Network Access**, and then click **Apply**.
2. Click **Policy & Objects > ZTNA**, and then click the **Security Posture Tag** tab.
3. Expand **Security Posture IP Tag**.
Security posture tags should be displayed.
4. Hover over the **Compliant** tag, and then click **View resolved addresses** to see the IP addresses of the endpoints.

The screenshot shows the 'Security Posture Tag' configuration page. A context menu is open over a tag named 'EMSServer'. The menu items are: 'View matched endpoints' (1) and 'View resolved addresses' (2). The 'View resolved addresses' item is highlighted with a red box.

ZTNA Server	Security Posture Tag	Security Posture Tag Group
<input type="button" value="Search"/> Name Security Posture CLASS IP: Low COMP IP: Google Chrome	IP TAG Compliant Provided By: EMSServer Type: IP Category: Security Posture References: 0	
	<input type="button" value="View matched endpoints 1"/>	<input type="button" value="View resolved addresses 2"/>

Exercise 3: Configuring an HTTPS Access Proxy With Certificate Authentication and Security Posture Tags

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 configure ZTNA policies to apply security posture checks using security posture tags.

Configure a Basic HTTPS Access Proxy With Certificate-Based Authentication and Security Posture Tags

You will create a ZTNA server, real server, and ZTNA rule on FortiGate, which are all required by the HTTPS access proxy setup.

To configure the ZTNA server or HTTPS access proxy VIP

1. On the HQ-EMS-1 VM, open Chrome, and then in **Bookmarks**, select the **HQ-NGFW** login page bookmark.
2. Log in to the FortiGate GUI with the following credentials:
 - Username: admin
 - Password: Fortinet1!
3. Click **Policy & Objects > ZTNA**, and then click the **ZTNA Server** tab.
4. Click **Create New** to create a new server, and then configure the following settings:

Field	Value
Name	ZTNA-Server
Interface	Select port2 .
IP address	100.64.0.1
Port	9443
Default certificate	Select FGT .

New ZTNA Server

Type **IPv4**

Name **ZTNA-Server**

Comments

Connect On

Interface **port2**

IP address **100.64.0.1**

Port **9443**

SAML

Services and Servers

Default certificate **FGT**

Service/server mapping

5. In the **Service/server mapping** section, click **Create New**.
6. In the **Service** field, ensure that **HTTPS** is selected.
7. In the **Virtual Host** field, ensure that **Any Host** is selected.
8. In the **Match path by** field, ensure that **Substring** is selected.
9. Leave the **Path** field at the default value of **/**.
10. In the **Server** section, in the **IP address** field, type **10.0.1.20**, in the **Port** field, type **443**, and then click **OK**.

New Service/Server Mapping

Type **IPv4**

Service **HTTPS**

Virtual Host **Any Host**

Match path by **Substring**

Path **/**

Server

Address type **IP**

IP address **10.0.1.20**

Port **443**

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

To configure a ZTNA policy

1. Click **Policy & Objects > Firewall Policy**.
2. Click **Create New** to create a new rule.
3. In the **Name** field, type **ZTNA-Access**.
4. In the **Schedule** field, ensure that **always** is selected.
5. In the **Action** field, select **ACCEPT**.
6. In the **Type** field, select **ZTNA**.
7. In the **Incoming interface** field, select **port2**.
8. In the **Source** field, select **all**.
9. In the **Security posture tag** field, select **All of**, and then add **IP TAG Compliant**.
10. In the **ZTNA server** field, select **ZTNA-Server**.
11. In the **Logging Options** section, ensure that the **Log Allowed Traffic** field is set to **All Sessions**.
12. Ensure that **Enable this policy** is enabled.

The screenshot shows the 'Firewall Policy' configuration window. The policy is named 'ZTNA-Access' and is set to 'ACCEPT' with a 'Standard' type. It is applied to 'port2' and always. The 'Source & Destination' section shows 'all' as the source and 'ZTNA-Server' as the destination. The 'Security posture tag' section is configured to 'All of' 'Compliant' (IP TAG). The 'ZTNA server' section lists 'ZTNA-Server'.

Field	Value
Name	ZTNA-Access
Schedule	always
Action	✓ ACCEPT
Type	Standard
Incoming interface	port2
Source	all
User/group	
Security posture tag	All of Compliant (IP TAG)
ZTNA server	ZTNA-Server

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

To create a deny policy for compliance failure

1. Click **Policy & Objects > Firewall Policy**, and then click **Create New**.
2. In the **Create New Policy** window, configure the following settings:

Field	Value
Name	ZTNA-Compliance-Failure
Schedule	always
Action	DENY
Type	ZTNA
Incoming interface	port2
Source	all

Field	Value
Security posture tag	All of IP TAG Non-Compliant
ZTNA server	ZTNA-Server
Log violation traffic	Enabled
Enable this policy	Enabled

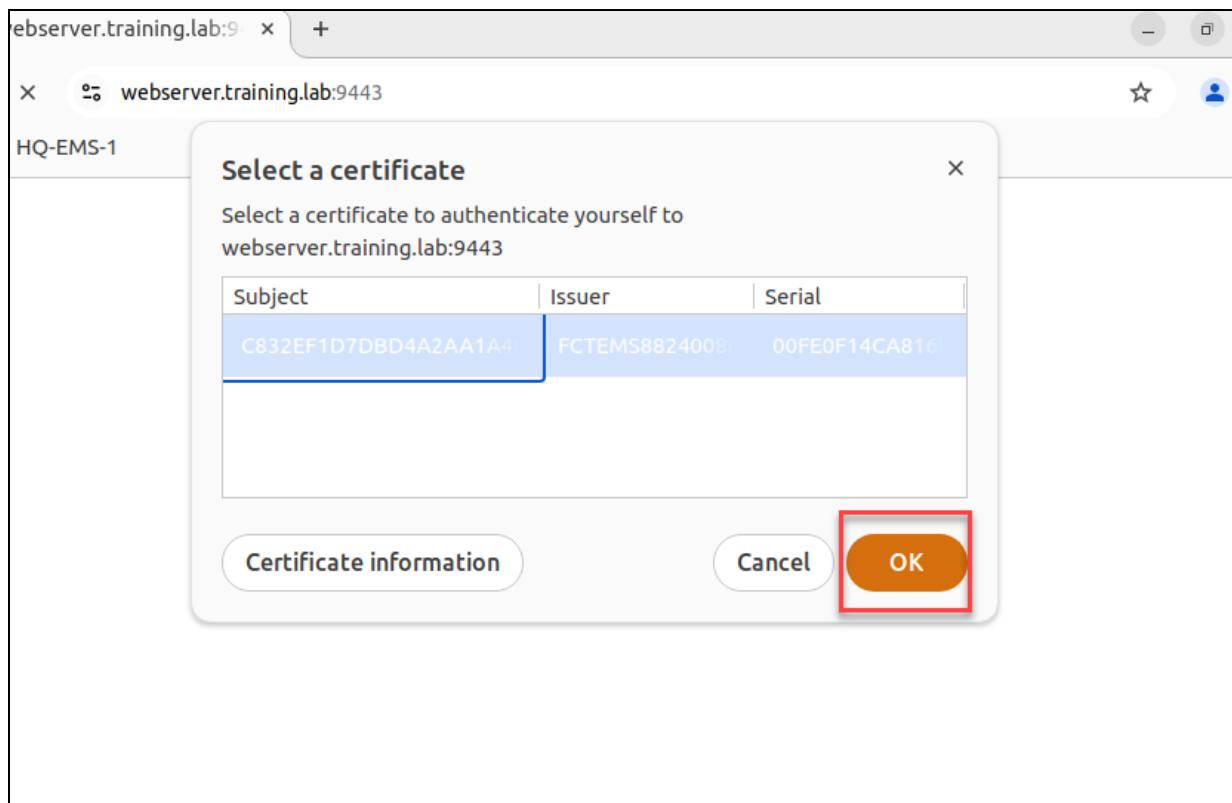
3. Click **OK** to save the new rule.
4. Move this policy above the **ZTNA-Access** policy.

Test Remote Access to the HTTPS Access Proxy

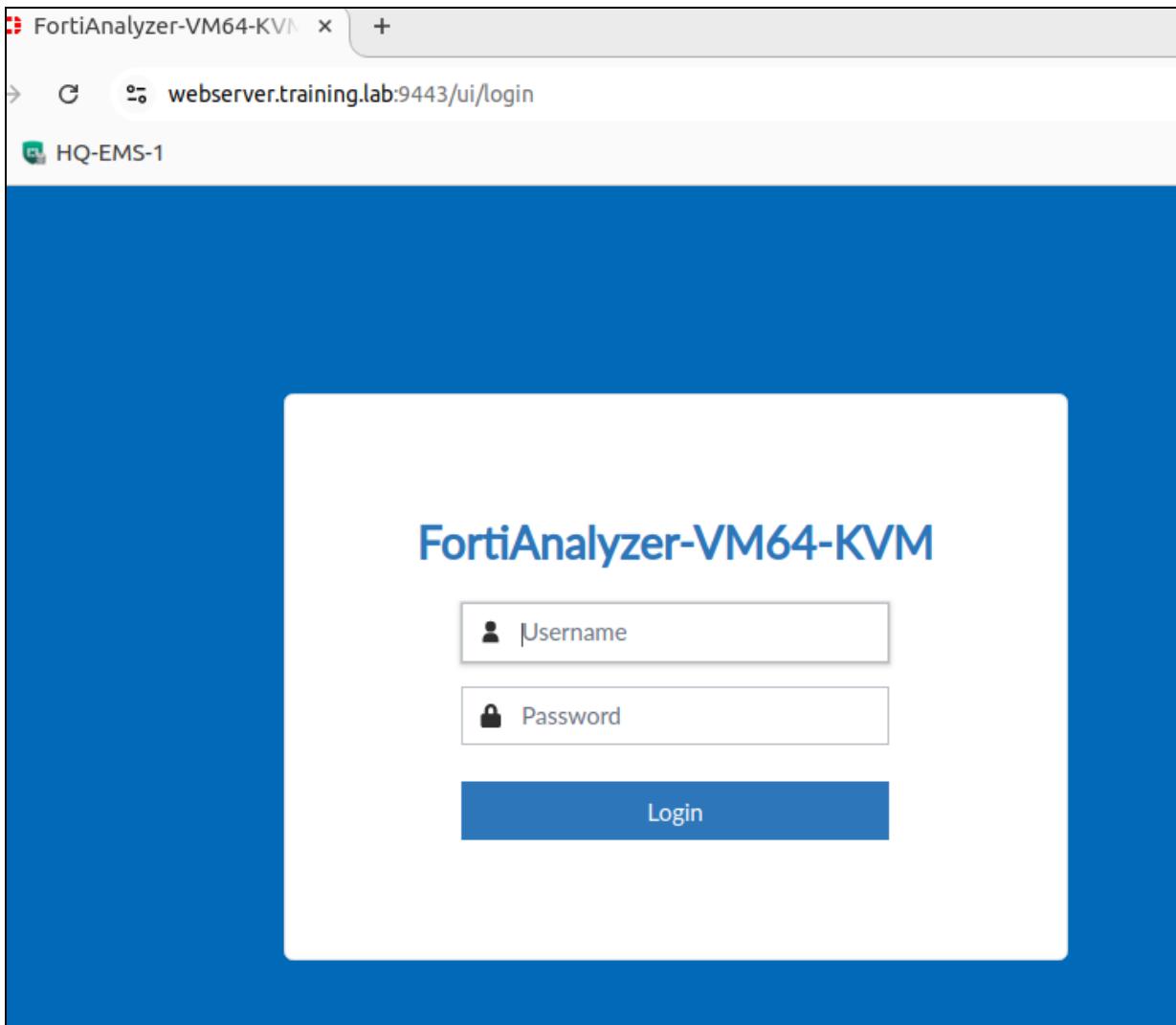
You will test the HTTPS access proxy connection for authorized users.

To test the connection for authorized users

1. On the BR-PC-1 VM, open a terminal window.
2. Enter `ping -c 4 webserver.training.lab`, and then verify that it resolves to `100.64.0.1`.
3. Open Chrome, and then enter `webserver.training.lab:9443`.
The browser prompts you for the client certificate to use.
4. Select the EMS signed certificate, and then click **OK**.



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



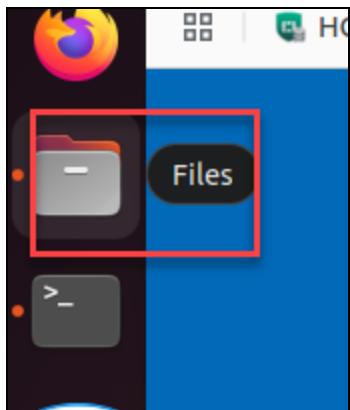
5. Close Chrome.



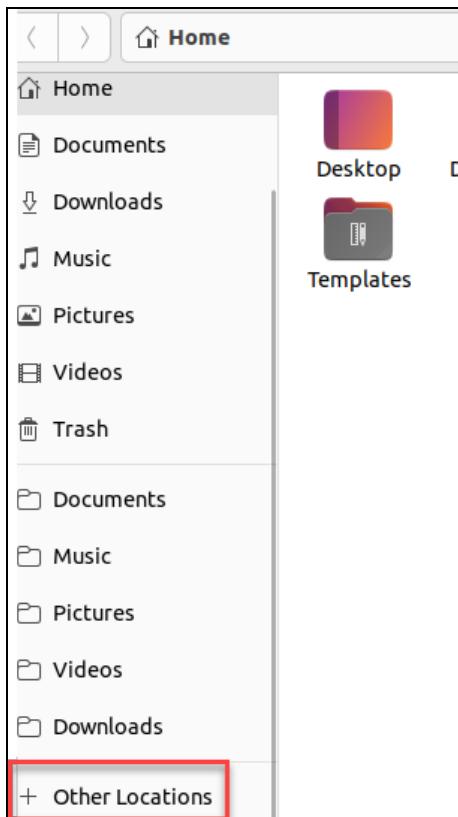
By default, client certificate authentication is enabled on the access proxy, so when the HTTPS request is received, the FortiGate WAD process challenges the client to identify itself with its certificate.

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

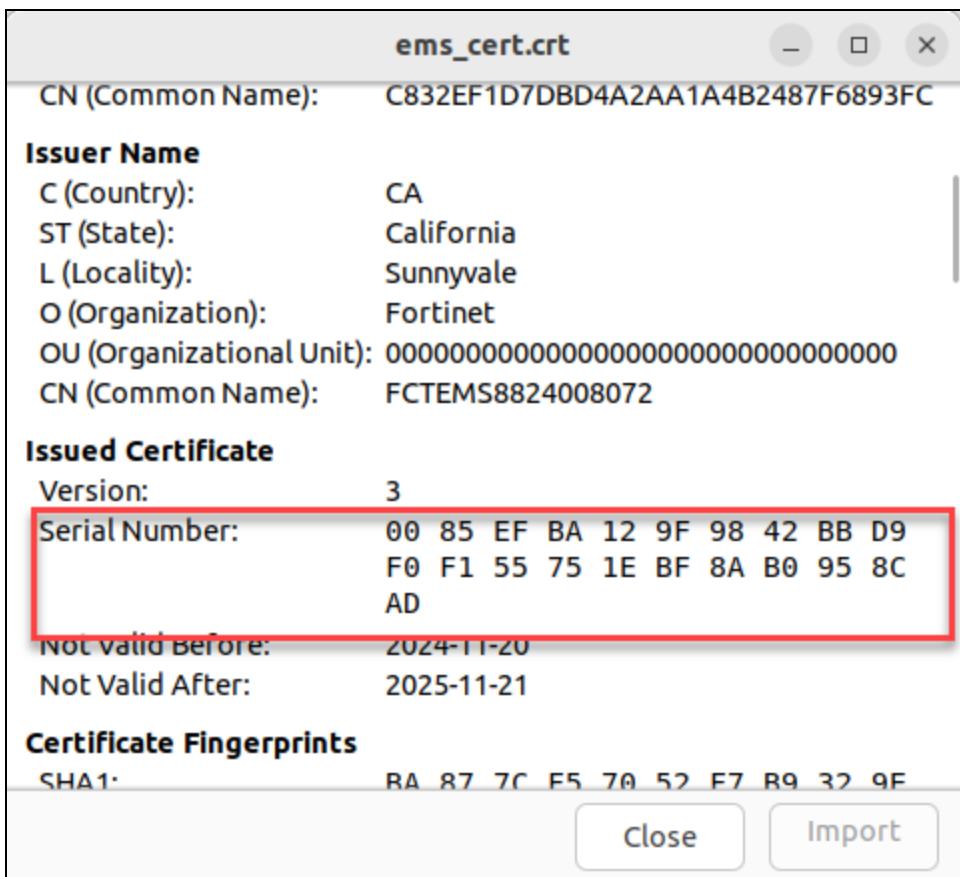
1. Continuing on the BR-PC-1 VM, click the **Files** icon.



2. Click **Other Locations**.



3. Double-click **Computer > opt > forticlient**.
4. Double-click **ems_cert.crt** to view the certificate.
5. Click **Details**, and then find the serial number of the certificate.



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

6. Return to the FortiClient EMS GUI, and then click **Endpoints > All Endpoints**.
7. In the list, click **br-pc-1**, and then in the **Configuration** section, check the **FortiClient ID** and **ZTNA Serial Number** fields to match the information.

Classification Tags	
ZTNA Serial Number	85EFBA129F9...
	85EFBA129F9842BBD9F0F155751EBF8AB0958CAD
Classification Tags	

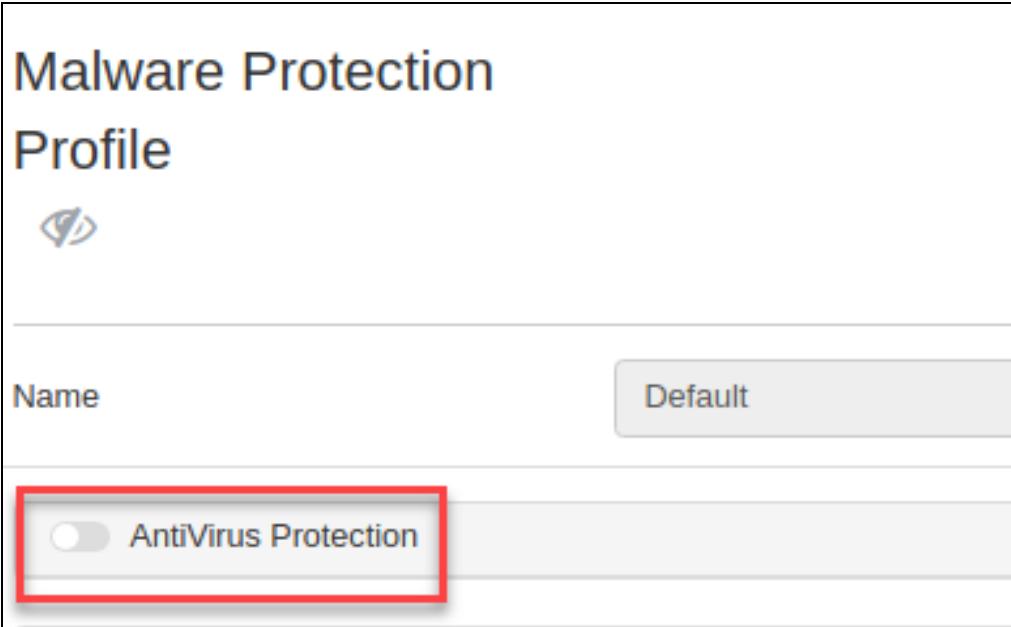
Your FortiClient ID and certificate serial number might not match what is shown in this example.

Verify the Behavior When the Security Posture Changes on the Endpoint

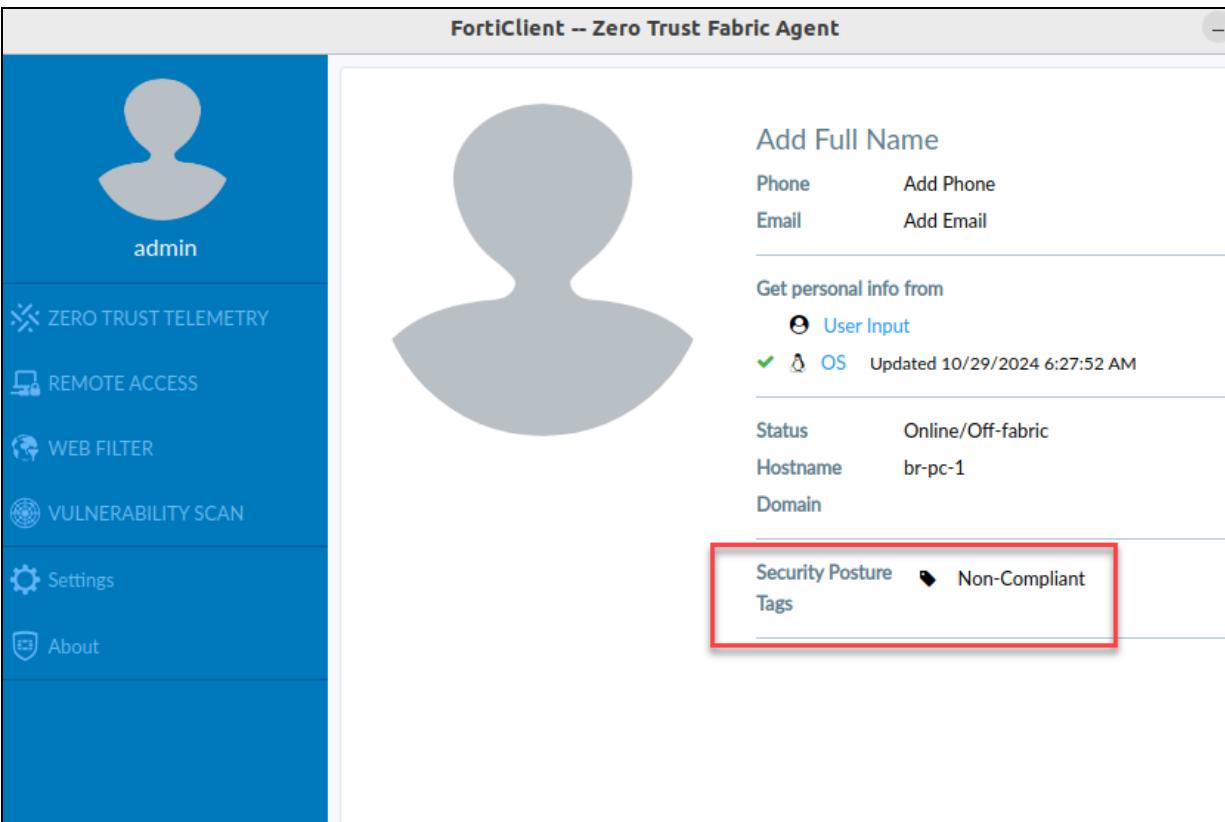
You will test a scenario where the endpoint security posture changes because no antivirus software is installed on the endpoint. You will disable malware protection in the endpoint profile to trigger security posture tag detection, which you configured in a previous exercise.

To disable antivirus and tag an endpoint

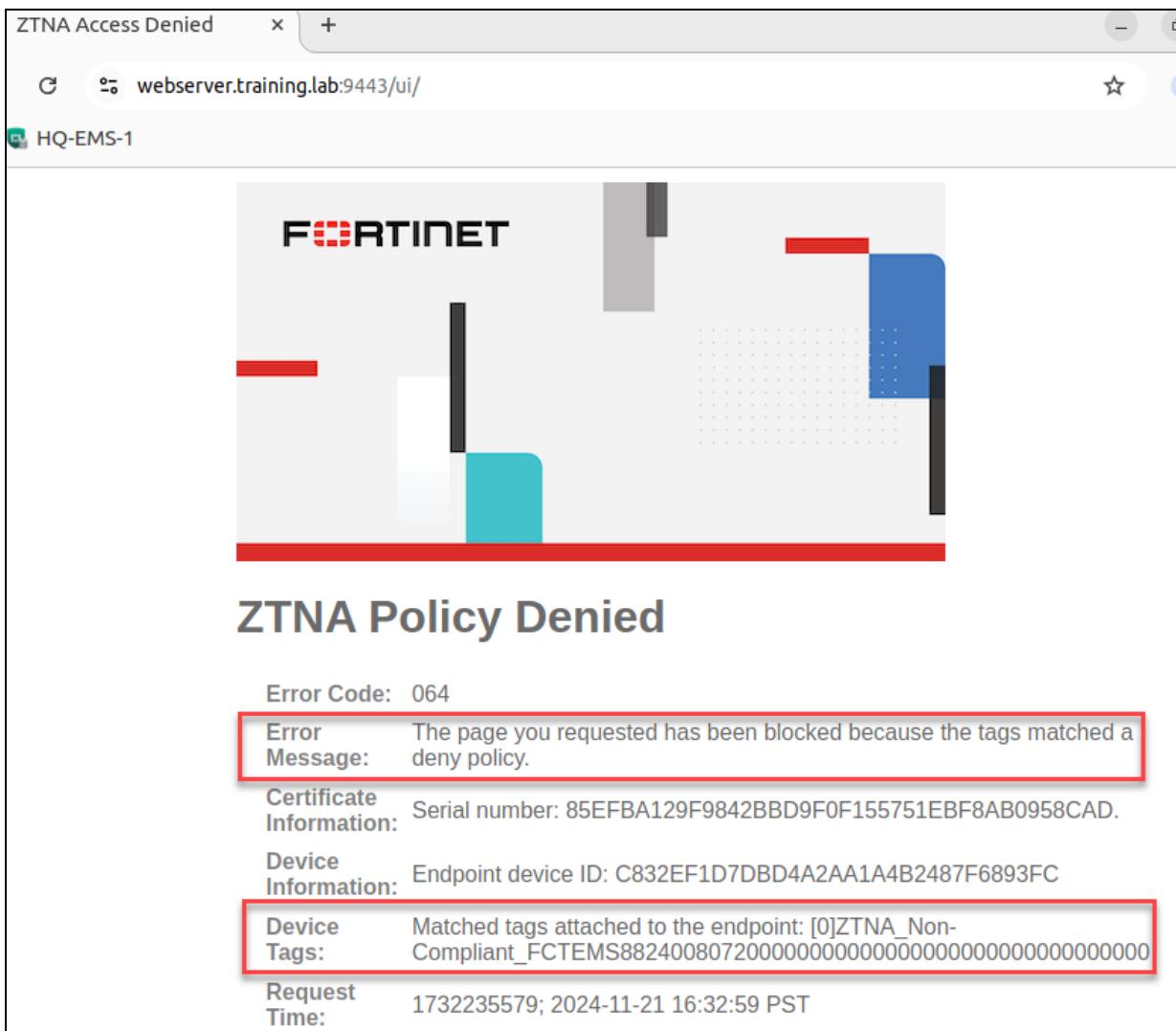
1. On the FortiClient EMS GUI, click **Endpoint Profiles > Malware Protection**.
2. Click **Default**, and then click **Edit**.
3. Disable **AntiVirus Protection**.



4. Click **Save**.
5. On the BR-PC-1 VM, open the FortiClient console, and then click the avatar to view the detected tags. It may take a minute for the updated tags to appear.



6. On the desktop, open Chrome, and then enter `webserver.training.lab:9443` to access the web server.
7. Select the EMS signed certificate, and then click **OK**.



8. Return to the FortiClient EMS GUI, and then click **Endpoint Profiles > Malware Protection**.
9. Click **Default**, and then click **Edit**.
10. Enable **AntiVirus Protection**.
11. Click **Save**.

Exercise 4: Configuring a TCP Forwarding Access Proxy for SSH

In this exercise, you will configure TCP forwarding on FortiGate and the corresponding ZTNA destination 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 for Private Applications

The TCP access proxy setup requires a ZTNA server, real server, and ZTNA rule on FortiGate. You also require ZTNA destinations on FortiClient.

To add a new server mapping to an existing ZTNA server for a TCP access proxy

1. On the HQ-EMS-1 VM, open Chrome, and then in **Bookmarks**, select the **HQ-NGFW** login page bookmark.
2. Log in to the FortiGate GUI with the following credentials:
 - Username: admin
 - Password: Fortinet1!
3. Click **Policy & Objects > ZTNA**, and then click the **ZTNA Server** tab.
4. Click **ZTNA-Server**, and then click **Edit**.
5. In the **Service/server mapping** section, click **Create New**.
6. In the **Service** field, select **TCP Forwarding**.
7. In the **Servers** section, in the **Address** field, click **+**, and then click **Address**.
8. In the **Name** field, type **FortiAnalyzer**.
9. In the **IP/Netmask** field, type **10.0.1.20/32**.
10. Click **OK**.
11. Click **OK** to select the new entry.
12. In the **Ports** field, type **22**.
13. Click **OK**.

Edit ZTNA Server

Type **IPv4**

Name **ZTNA-Server**

Comments

Connect On

Interface **port2**

IP address **100.64.0.1**

Port **9443**

SAML

Services and Servers

Default certificate **FGT**

Service/server mapping

+ Create new	Edit	Delete
<input type="checkbox"/> Service	<input type="checkbox"/> URL	<input type="checkbox"/> Server
<input type="checkbox"/> HTTPS	/	10.0.1.20:443
<input type="checkbox"/> TCP Forwarding	/tcp	FortiAnalyzer:22

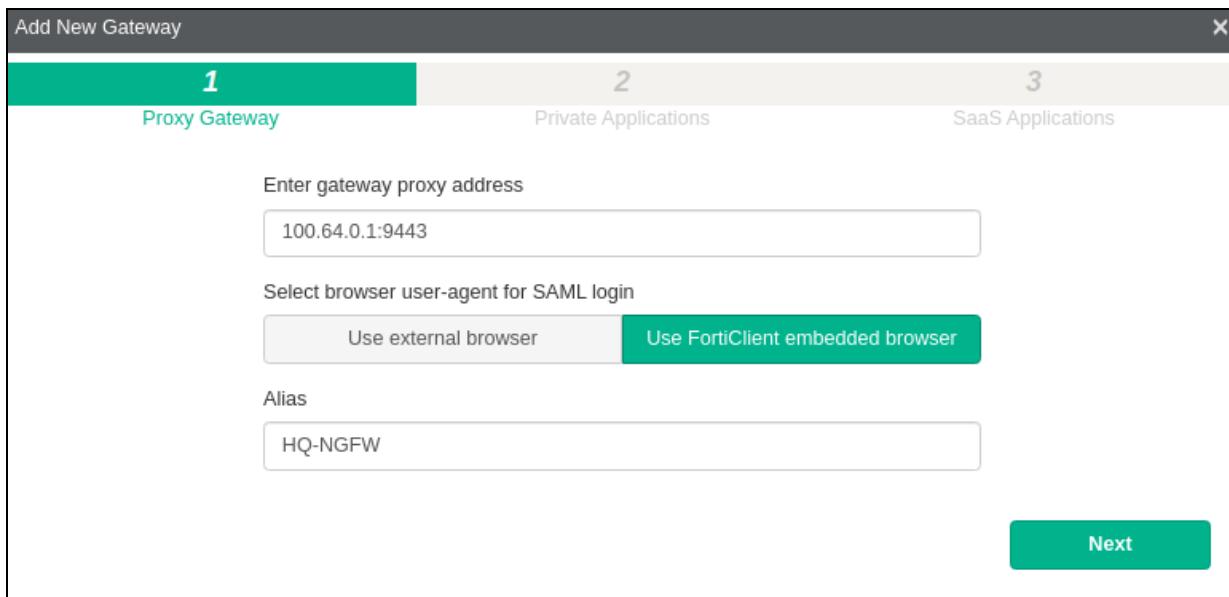
14. Click OK.

You already configured the ZTNA policy in the previous exercise, with security posture tags for the same ZTNA server.

To configure the ZTNA destinations on FortiClient

1. On the FortiClient EMS GUI, click **Endpoint Profiles > ZTNA Destinations**, select **Default**, and then click **Edit**.
2. Click the  icon to enable visibility of the feature on FortiClient.

3. In the **Destinations** section, click **Add**.
4. In the **Enter gateway proxy address** field, type **100.64.0.1:9443**.
5. In the **Alias** field, type **HQ-NGFW**.



Add New Gateway

1 Proxy Gateway 2 Private Applications 3 SaaS Applications

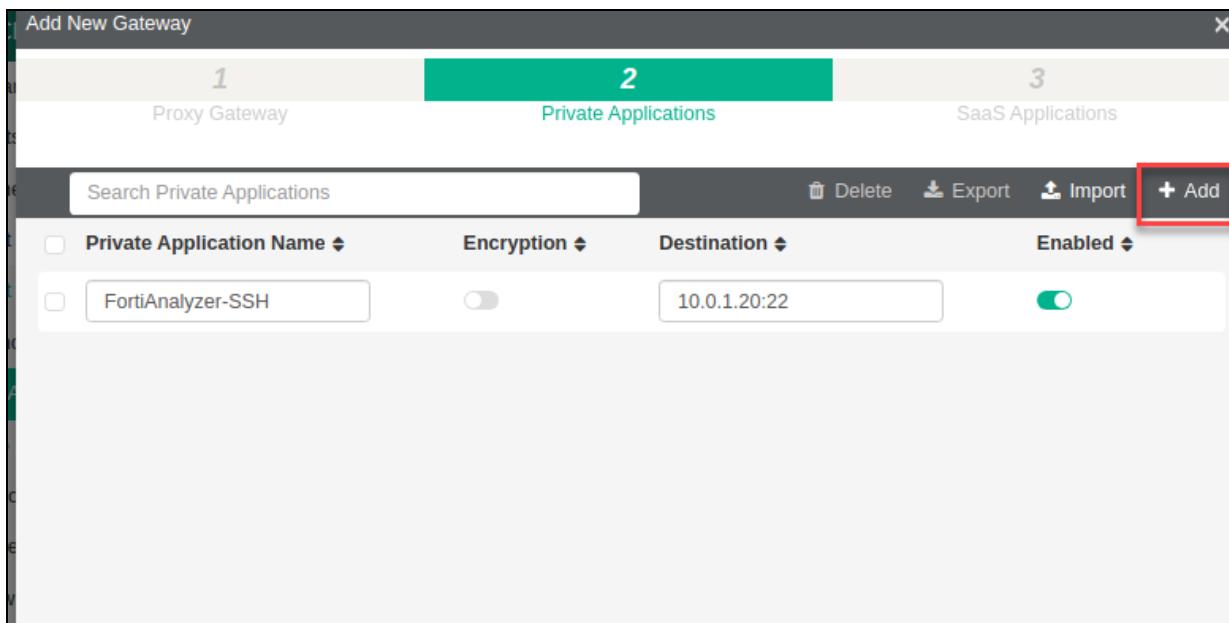
Enter gateway proxy address
100.64.0.1:9443

Select browser user-agent for SAML login
Use external browser Use FortiClient embedded browser

Alias
HQ-NGFW

Next

6. Click **Next**.
7. In the **Private Applications** window, click **Add**.
8. In the **Private Application Name** field, type **FortiAnalyzer-SSH**.
9. In the **Destination** field, type **10.0.1.20:22**.



Add New Gateway

1 Proxy Gateway 2 Private Applications 3 SaaS Applications

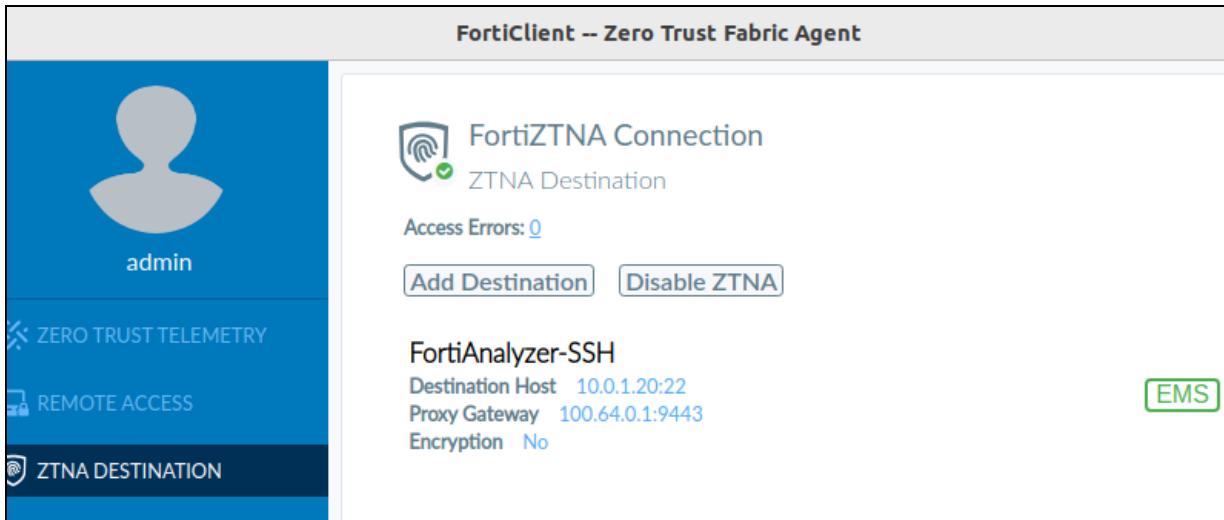
Search Private Applications Delete Export Import + Add

Private Application Name	Encryption	Destination	Enabled
FortiAnalyzer-SSH	Off	10.0.1.20:22	On

10. Click **Next**.
11. Click **Finish**.
12. Click **Save**.

To verify the ZTNA destinations on FortiClient

1. On the BR-PC-1 VM, open the FortiClient console, and then click **ZTNA DESTINATION**.
It may take a minute for the ZTNA destinations to appear.



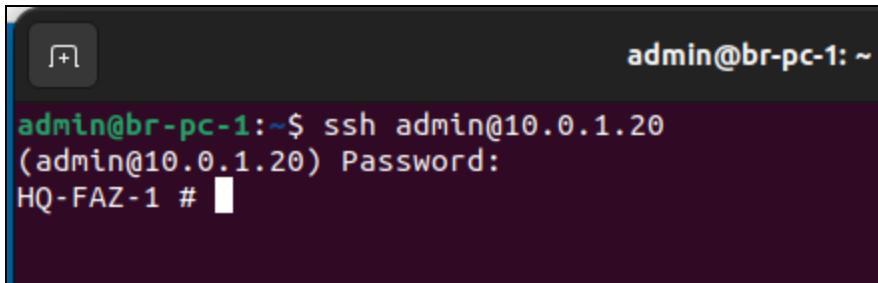
Test the Connection for Users

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 BR-PC-1 VM, open a terminal window.
2. Enter `ssh admin@10.0.1.20`.
3. If you are prompted to verify the RSA key fingerprint, type `yes` to continue connecting.
4. Enter the following password:

Fortinet1!



```
admin@br-pc-1:~$ ssh admin@10.0.1.20
(admin@10.0.1.20) Password:
HQ-FAZ-1 #
```

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

5. Close the terminal window.

Exercise 5: Configuring ZTNA for SaaS Application Access

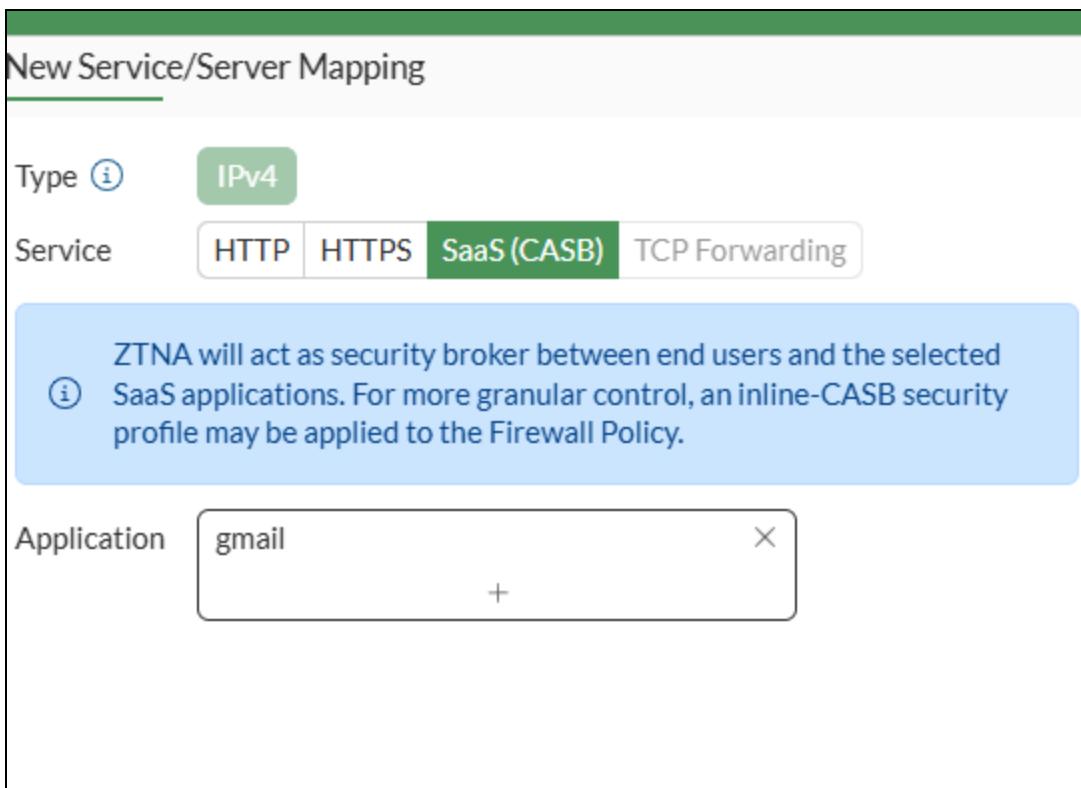
In this exercise, you will configure FortiGate as a ZTNA application gateway. You can configure a ZTNA application gateway to provide access control to software-as-a-service (SaaS) traffic. A FortiGate ZTNA TCP forwarding access proxy configuration specifies SaaS application destinations using application names that are defined in the FortiGuard Inline CASB Database (ICDB).

Configure a TCP Access Proxy for SaaS Applications

The TCP access proxy setup requires a ZTNA server, real server, and ZTNA policy on FortiGate. You also require ZTNA destinations on FortiClient.

To add a new server mapping to an existing ZTNA server for SaaS applications

1. On the HQ-EMS-1 VM, open Chrome, and then in **Bookmarks**, select the **HQ-NGFW** login page bookmark.
2. Log in to the FortiGate GUI with the following credentials:
 - Username: admin
 - Password: Fortinet1!
3. Click **Policy & Objects > ZTNA**, and then click the **ZTNA Server** tab.
4. Click **ZTNA-Server**, and then click **Edit**.
5. In the **Service/server mapping** section, click **Create New**.
6. In the **Service** field, select **SaaS (CASB)**.
7. In the **Application** field, click **+**, and then click **gmail**.



8. Click **OK**.

edit ZTNA Server

Type **IPv4**

Name **ZTNA-Server**

Comments

Connect On

Interface **port2**

IP address **100.64.0.1**

Port **9443**

SAML

Services and Servers

Default certificate **FGT** X +

Service/server mapping

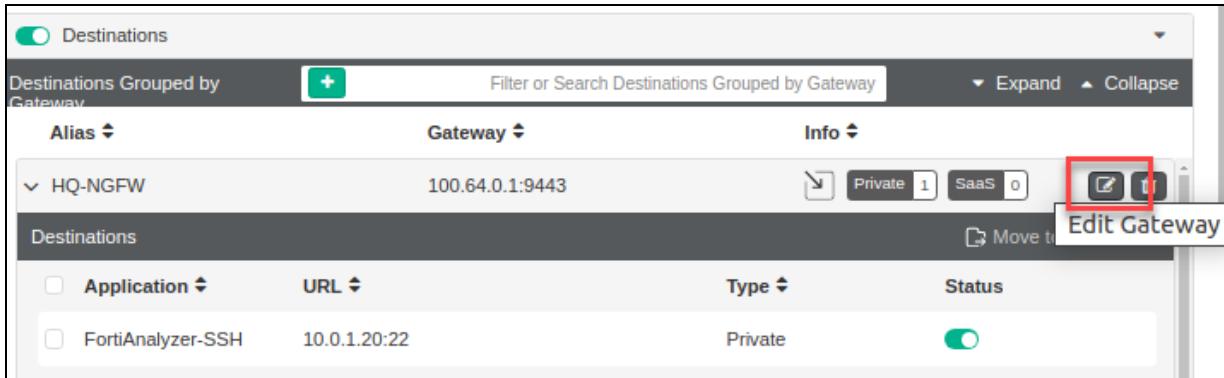
+ Create new	Edit	Delete
<input type="checkbox"/> Service	URL	Server
<input type="checkbox"/> HTTPS	/	10.0.1.20:443
<input type="checkbox"/> TCP Forwarding	/tcp	FortiAnalyzer:22
<input type="checkbox"/> SaaS	/saas	gmail

9. Click **OK**.

You already configured the ZTNA policy in the first exercise, with security posture tags for the same ZTNA server.

To configure the ZTNA destinations on FortiClient

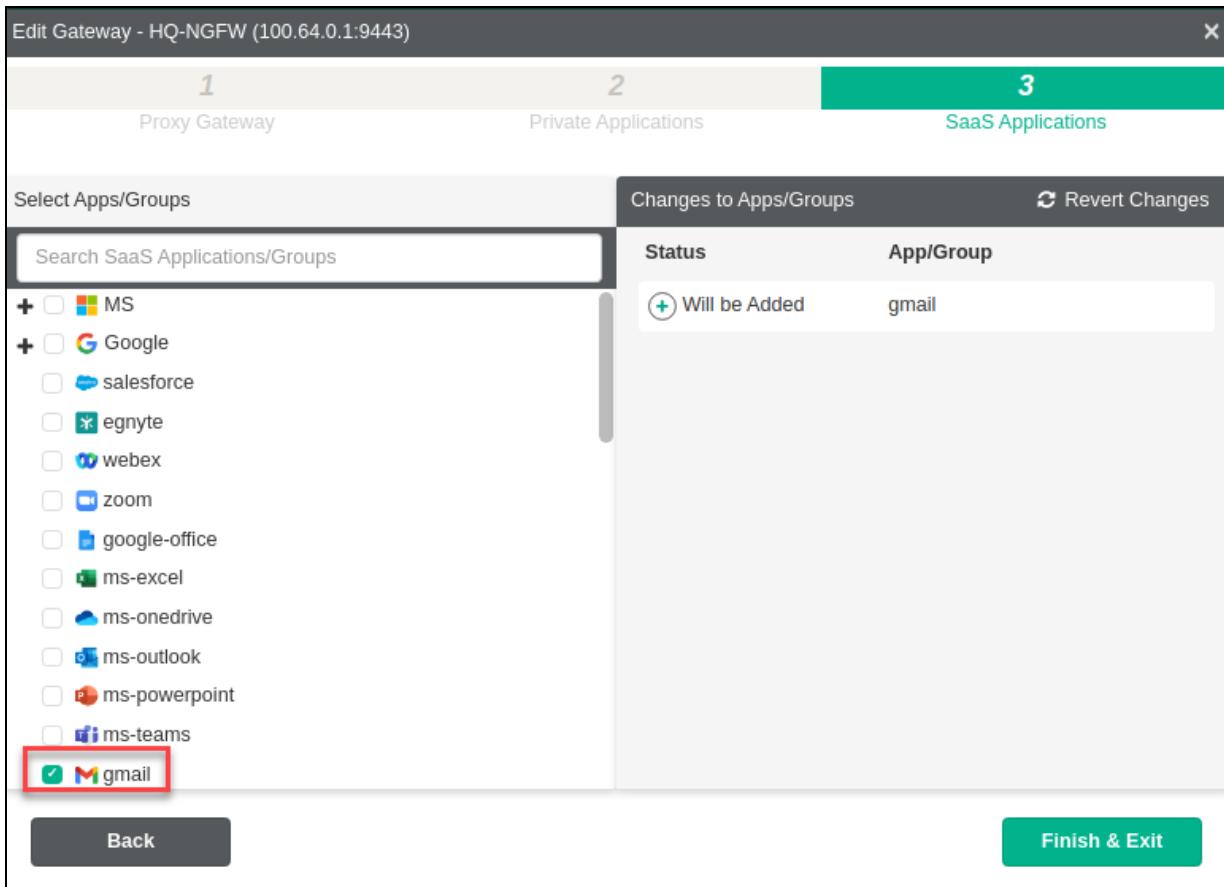
1. On the FortiClient EMS GUI, click **Endpoint Profiles** > **ZTNA Destinations**, select **Default**, and then click **Edit**.
2. In the **Destinations** section, click the edit icon  to edit the HQ-NGFW gateway.



The screenshot shows the 'Destinations' configuration screen. The 'HQ-NGFW' gateway is selected. The 'Edit' icon (a pencil icon inside a box) is highlighted with a red box. The table below lists destinations, with 'FortiAnalyzer-SSH' selected.

Alias	Gateway	Info	
HQ-NGFW	100.64.0.1:9443	Private 1 SaaS 0	
Destinations		Move to	
Application	URL	Type	Status
FortiAnalyzer-SSH	10.0.1.20:22	Private	On

3. Click **Next**.
4. Click **Next**.
5. In the **Select Apps/Groups** section, select the **gmail** checkbox.



The screenshot shows the 'Edit Gateway' dialog for the HQ-NGFW gateway. The 'SaaS Applications' tab is selected. The 'Changes to Apps/Groups' table shows a single entry: 'Will be Added' for 'gmail'. The 'Select Apps/Groups' list on the left shows a list of SaaS applications, with 'gmail' checked and highlighted with a red box.

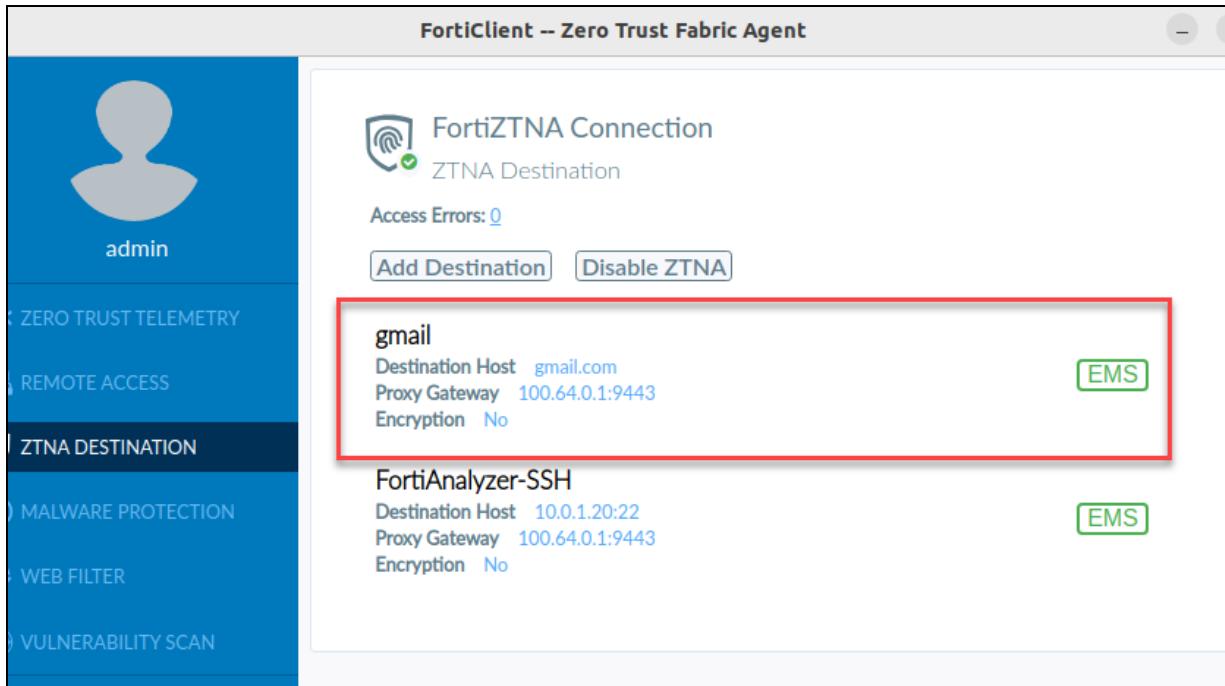
Status	App/Group
Will be Added	gmail

6. Click **Finish & Exit**.
7. Click **Save**.

To verify the ZTNA destinations on FortiClient

1. On the BR-PC-1 VM, open the FortiClient console, and then click **ZTNA DESTINATION**.

It may take a minute for the ZTNA destinations to appear.



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 BR-PC-1 VM, open Chrome.
2. Enter `gmail.com` to access Gmail.
3. Return to the HQ-NGFW GUI, and then click **Log & Report > ZTNA Traffic**.
4. Review the logs with **SaaS name= gmail**.

Date/Time	source	ZTNA Server	Real Server	Service	Result	ZTNA Rule
2024/11/21 16:44:22	100.64.1.1	[ZTNA-Server]	142.250.190.97	1111PS	✓ Accept (2.16 kB / 9.26 kB)	4
2024/11/21 16:44:22	100.64.1.1	[ZTNA-Server]	142.250.191.131	1111PS	✓ Accept (2.14 kB / 4.2 kB)	4
2024/11/21 16:44:22	100.64.1.1	[ZTNA-Server]	142.250.190.97	1111PS	✓ Accept (2.16 kB / 9.26 kB)	4
2024/11/21 16:44:20	100.64.1.1	[ZTNA-Server]	142.250.191.131	1111PS	✓ Accept (2.14 kB / 4.2 kB)	4
2024/11/21 16:44:20	100.64.1.1	[ZTNA-Server]	142.250.191.131	1111PS	✓ Accept (2.14 kB / 4.2 kB)	4
2024/11/21 16:44:18	100.64.1.1	[ZTNA-Server]	142.250.190.97	1111PS	✓ Accept (2.16 kB / 9.26 kB)	4
2024/11/21 16:44:18	100.64.1.1	[ZTNA-Server]	142.250.190.97	1111PS	✓ Accept (2.16 kB / 9.26 kB)	4
2024/11/21 16:44:16	100.64.1.1	[ZTNA-Server]	142.250.190.97	1111PS	✓ Accept (2.16 kB / 9.26 kB)	4
2024/11/21 16:44:14	100.64.1.1	[ZTNA-Server]	142.250.190.93	1111PS	✓ Accept (2.14 kB / 4.2 kB)	4
2024/11/21 16:44:08	100.64.1.1	[ZTNA-Server]	172.21.7.1.100	1111PS	✓ Accept (2.11 kB / 4.1 kB)	4
2024/11/21 16:44:07	100.64.1.1	[ZTNA-Server]	172.21.7.1.100	1111PS	✓ Accept (2.14 kB / 4.16 kB)	4

The logs indicate that Gmail is connected using the TCP-forwarding proxy that is configured on FortiGate.



In a production environment, you can configure the FortiGate ZTNA application gateway to act as an inline cloud access security broker (CASB) by providing access control to SaaS traffic using ZTNA access control rules and an inline CASB profile. A CASB is located between users and their cloud service to enforce security policies as they access cloud-based resources.

5. Return to the FortiClient EMS GUI, and then click **Endpoint Profiles > ZTNA Destinations**.
6. Click **Default**, and then click **Edit**.
7. Disable **ZTNA Destination Profile**.
8. Click **Save**.

Lab 8: Security Incident Response

In this lab, you will configure different incident response solutions.

Objectives

- Upload FortiClient logs to FortiAnalyzer
- Promote a FortiGate to serve as the root device in the Fortinet Security Fabric
- Configure automation stitches on FortiGate
- Quarantine a FortiClient endpoint using an automation stitch
- Configure FortiAnalyzer playbooks to tag FortiClient endpoints

Time to Complete

Estimated: 45 minutes

Exercise 1: Enabling the Security Fabric to Trigger Automatic Quarantine

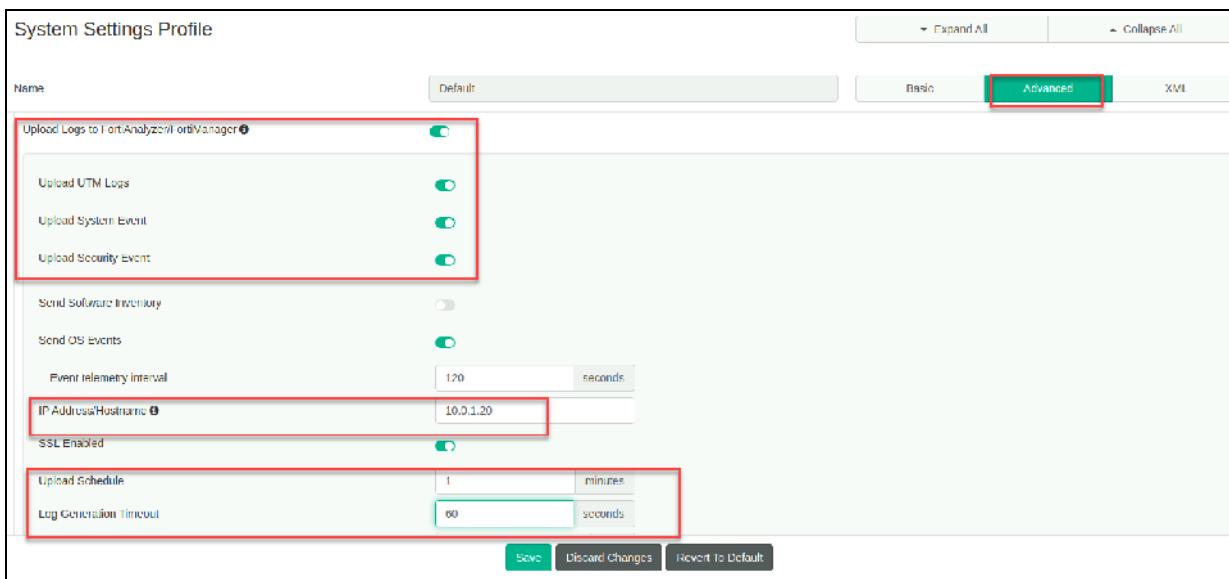
In this exercise, you will enable the Fortinet Security Fabric to trigger automatic quarantine, based on indicators of compromise (IOC) on FortiAnalyzer.

Configure FortiClient Log Settings

To identify compromised hosts, FortiClient must send logs to FortiAnalyzer. You will configure FortiClient log settings.

To configure FortiClient log settings

1. On the HQ-EMS-1 VM, log in to the FortiClient EMS GUI.
2. Click **Endpoint Profiles > System Settings**, select **Default**, and then click **Edit**.
3. Click **Advanced**.
4. In the **Log** section, enable **Upload Logs to FortiAnalyzer/FortiManager**, **Upload UTM Logs**, **Upload System Event**, and **Upload Security Event**.
5. In the **IP Address/Hostname** field, type **10.0.1.20**.
6. In the **Upload Schedule** field, type **1 minute**.
7. In the **Log Generation Timeout** field, type **60 seconds**.



System Settings Profile

Advanced

Upload Logs to FortiAnalyzer/FortiManager

Upload UTM Logs

Upload System Event

Upload Security Event

Send Software Inventory

Send OS Events

Event Telemetry Interval: 120 seconds

IP Address/Hostname: 10.0.1.20

SSL Enabled

Upload Schedule: 1 minutes

Log Generation Timeout: 60 seconds

Save Discard Changes Revert To Default

8. Click **Save**.

Enable the Security Fabric on the FortiGate

You will configure the Security Fabric and enable telemetry on the FortiGate internal interface.

To configure the Security Fabric and enable telemetry on the FortiGate

1. Continuing on the HQ-EMS-1 VM, open a new Chrome tab, and then in **Bookmarks**, select the **HQ-NGFW** login page bookmark.
2. Log in to the FortiGate GUI with the following credentials:
 - Username: admin
 - Password: Fortinet1!
3. On the FortiGate GUI, click **Security Fabric > Fabric Connectors**.
4. Select **Security Fabric Setup**, and then click **Edit**.
5. In the **Security Fabric Settings** section, in the **Security Fabric role** field, click **Serve as Fabric Root**.
A new window opens.
6. In the **FortiAnalyzer Settings** section, in the **Status** field, select **Enabled**, and then configure the following settings:

Field	Value
IP address	10.0.1.20
Upload option	Real Time

7. Click **OK**.
8. When the **Verify FortiAnalyzer Serial Number** warning appears, click **Accept**.
9. Configure the following settings:

Field	Value
Allow other Security Fabric devices to join	port4
Fabric name	Training
Management port	Use Admin Port

Your configuration should look like the following example:

Security Fabric Settings

Security Fabric role	<input type="radio"/> Standalone <input checked="" type="radio"/> Serve as Fabric Root <input type="radio"/> Join Existing Fabric
Allow other Security Fabric devices to join	<input checked="" type="radio"/> port4 <input type="button" value="X"/> <input data-bbox="1019 369 1052 411" type="button" value="+"/>
Fabric name	Training
Device authorization	None <input type="button" value="Edit"/>
FortiCloud account enforcement <small>(i)</small>	<input checked="" type="radio"/>
Allow downstream device REST API access <small>(i)</small>	<input type="radio"/>
Fabric global object	<input checked="" type="radio"/>
Management IP/FQDN <small>(i)</small>	<input type="radio"/> Use WAN IP <input checked="" type="radio"/> Specify
Management port	<input type="radio"/> Use Admin Port <input checked="" type="radio"/> Specify
SAML SSO Settings	
SAML Single Sign-On <small>(i)</small> <input type="radio"/> <input type="checkbox"/> Advanced Options	

10. Click **OK**.
11. Continuing on the HQ-EMS-1 VM, open a new Chrome tab, and then in **Bookmarks**, select the **HQ-FAZ** login page bookmark.
12. Log in to the FortiAnalyzer GUI with the following credentials:
 - **Username:** admin
 - **Password:** Fortinet1!
13. Click the **root** ADOM.
14. Click **Device Manager > Unauthorized Devices**.
15. Select the checkbox beside **Device Name**, click **Authorize**, and then click **OK** to complete the authorization.

Search...		<input checked="" type="checkbox"/> Authorize	<input type="button" value="Hide"/>	<input type="button" value="Delete"/>	<input type="button" value="Edit"/>	Search...
		<input checked="" type="checkbox"/>	Device Name	Platform	Serial	<input type="button" value=""/>
All Logging Devices	(0)	<input checked="" type="checkbox"/>				
Unauthorized Devices	(2)	<input checked="" type="checkbox"/>	FCTEMS8824008072	FortiClient-EMS	FCTEMS	<input type="button" value=""/>
		<input checked="" type="checkbox"/>	HQ-NGFW-1	FortiGate-VM64...	FGVM02	<input type="button" value=""/>

16. Click **Close**.
17. Return to the HQ-NGFW-1 GUI, click **Security Fabric > Fabric Connectors**.
18. Click **Logging & Analytics**, and then click **Edit**.

In the **FortiAnalyzer** section, the value in the **Connection status** field is **Connected**.

Logging Settings

Settings Info

FortiAnalyzer Cloud Logging

Status Enabled Disabled

Server 10.0.1.20

Connection status Connected Refresh

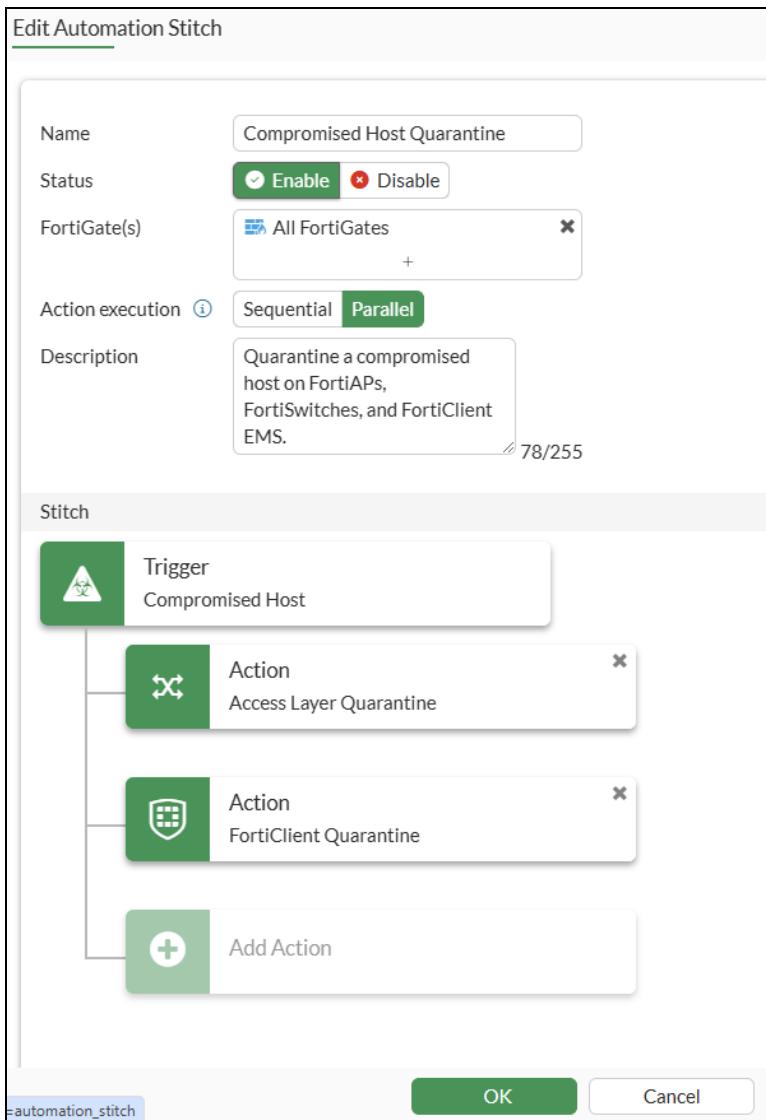
Upload option Real Time Every Minute Every 5 Minutes

Allow access to FortiGate REST API

Verify FortiAnalyzer certificate FAZ-VMTM24012176

To enable Security Fabric automation and create a new stitch

1. Continuing on the FortiGate GUI, click **Security Fabric** > **Automation**.
2. Select the predefined default stitch **Compromised Host Quarantine**, and then click **Edit**.
3. In the **Edit Automation Stitch** window, in the **Status** field, select **Enable**, and then leave the other settings at the default values.



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

The stitch, trigger, and action are enabled for a compromised host.

To configure firewall policies on FortiGate

1. Continuing on the HQ-NGFW-1 FortiGate GUI, click **Policy & Objects > Firewall Policy**.
2. Select the **Internet Traffic** policy, and then click **Edit**.
3. In the **Security Profiles** section, enable **Web filter**, and then select **monitor-all**.
4. In the **SSL inspection** field, select **certificate-inspection**.

Edit Policy

Settings Info

Firewall/Network Options

NAT

IP pool configuration Use Outgoing Interface Address Use Dynamic IP Pool

Preserve source port

Protocol options PROT default

Security Profiles

AntiVirus

Web filter WEB monitor-all

DNS filter

Application control

IPS

File filter

SSL inspection SSL certificate-inspection



FortiAnalyzer uses web filter, traffic, and security logs from FortiGate to analyze traffic for IOC events.

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

To verify that the FortiAnalyzer license includes the IOC service

1. Return to the FortiAnalyzer GUI, click **Dashboards > Status**, and then in the **License Information** widget, in the **FortiGuard** section, check the status of the **Indicators of Compromise Service** license.

License Information

VM License	Valid 10K-UG
FortiCare Support	<input checked="" type="checkbox"/> Registered (FortiCloud Account: courseware@fortinet.com)

FortiGuard

Indicators of Com...	<input checked="" type="checkbox"/> Licensed (Expires 2025-09-01)
Outbreak Detecti...	<input checked="" type="checkbox"/> Licensed (Expires 2025-09-01)
Security Automati...	<input checked="" type="checkbox"/> Licensed (Expires 2025-09-01)
Industrial Security...	<input checked="" type="checkbox"/> Licensed (Expires 2025-09-01)
Security Rating U...	<input checked="" type="checkbox"/> Licensed (Expires 2025-09-01)
Storage Connecto...	<input type="checkbox"/> Not Licensed

To test the automatic quarantine that IOC detection triggered

1. On the HQ-PC-1 VM, open Chrome, and then enter the URL www.google.com
2. Open a new browser tab, and then enter <http://195.22.28.198>.

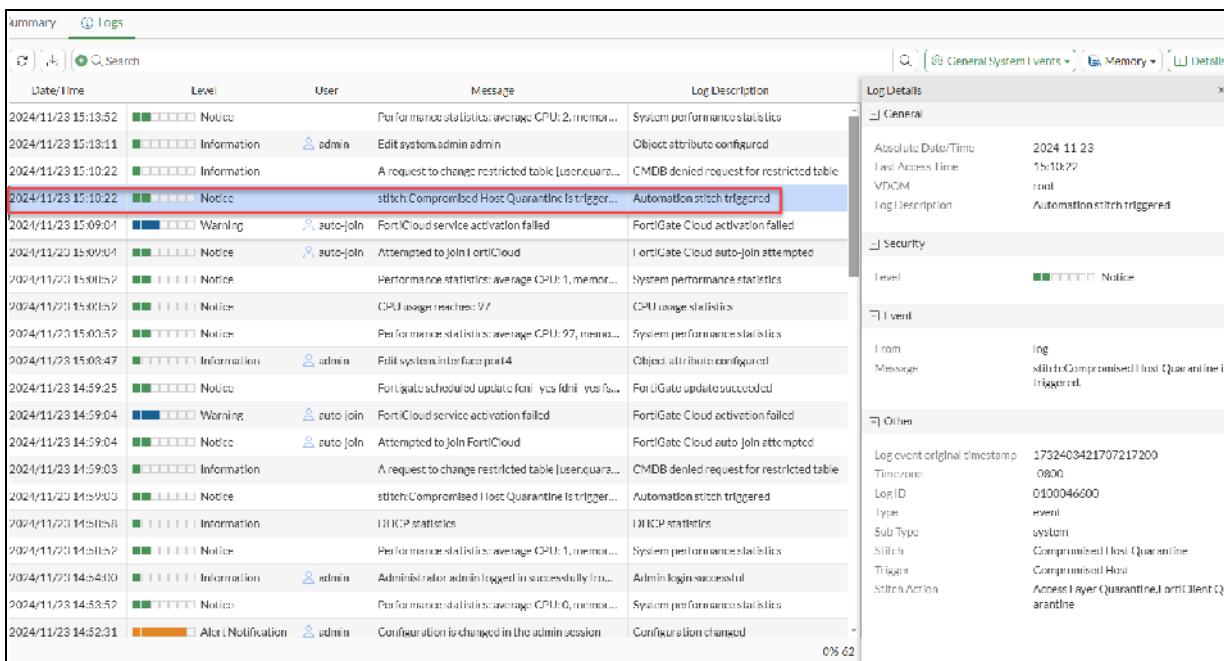
The connection to the website will time out, and when FortiClient is quarantined, you may not be able to access the HQ-PC-1 VM using RDP.

3. Return to the FortiAnalyzer GUI, and then click **FortiView > Threats > Indicator of Compromise**.

The compromised endpoint appears in the window after a couple of minutes.

Indicator of Compromise 1										
Source (User/IP) 1	Last Detected 1	Host Name 1	Log Types	Security Actions	Verdict 1	# of Threats 1	Acknowledge	Device Name	Device ID 1	Actions
10.0.1.10	2024-11-23 14:59	hq-pc-1	Traffic	Timeout	Infected	1	ACK	HQ-NGFW-1	FGVM02TM19001113	1

4. Return to the HQ-NGFW-1 GUI, click **Log & Report > System Events > General System Events** to view the logs.



The screenshot shows the FortiGate Log Viewer interface. The main pane displays a table of log entries with columns: Date/Time, Level, User, Message, and Log Description. A specific log entry from 2024/11/23 15:10:22 is highlighted with a red box and a tooltip: "stitch Compromised Host Quarantine Is triggered". The right pane, titled "Log Details", provides a detailed view of this specific log entry, including fields like Absolute Date/Time, Log Access Time, VDOM, Log Description, and a detailed breakdown of the log message.

5. Return to the FortiClient EMS GUI, and then click **Administration > Log Viewer** to see the quarantine logs.

Date	Level	Source	Message	Occurrences
2024-11-24 00:20:49	Info	Console	Certificate user: FGVM02TM19001113 FGT authoriz...	1 time since 20...
2024-11-24 00:19:41	Info	Console	student1 requested logs from 1 Endpoint(s): hq-...	1 time since 20...
2024-11-24 00:13:28	Info	Console	Certificate user: FGVM02TM19001113 FGT authoriz...	1 time since 20...
2024-11-24 00:10:21	Info	Console	The endpoint hq-pc-1 will eventually be quarantined by FortiGate HQ-NGFW-1 (0.0.0.0).	1 time since 2024-11-24 00:10:21
2024-11-24 00:07:17	Info	Console	student1 requested diagnostics from 1 Endpoint(s): h...	1 time since 20...
2024-11-24 00:06:55	Info	Console	student1 unquarantined 1 Endpoint(s): ['hq-pc-1'].	1 time since 20...
2024-11-24 00:06:08	Info	Console	Certificate user: FGVM02TM19001113 FGT authoriz...	1 time since 20...

Exercise 2: Configuring FortiAnalyzer Playbooks to Add Fabric Tags to FortiClient Endpoints

In this exercise, you will configure playbooks on FortiAnalyzer to tag FortiClient endpoints.

Enable the EMS Connector on FortiAnalyzer

You will enable the EMS connector on FortiAnalyzer.

To enable the EMS connector on FortiAnalyzer

1. On the HQ-EMS-1 VM, log in to the FortiAnalyzer GUI.
2. Click **Dashboards > Status**, and then in the **License Information** widget, in the **FortiGuard** section, check the status of the **Security Automation** license.
3. Click **Incidents & Events > Automation**, and then click **Active Connectors**.
4. Click **FortiClient EMS Connector**, and then click **Edit**.
A new window opens.
5. In the **FortiClient EMS** section, configure the following settings:

Field	Value
IP /FQDN	10.0.1.100
User Name	student1
Password	Password1!

Edit FortiClient EMS - FortiClient EMS Connector

Configuration Action

Connector Settings

Type	FortiClient EMS	FortiClient EMS Cloud
Name	FortiClient EMS Connector	
Description	FortiClient EMS Connector	
25/256		

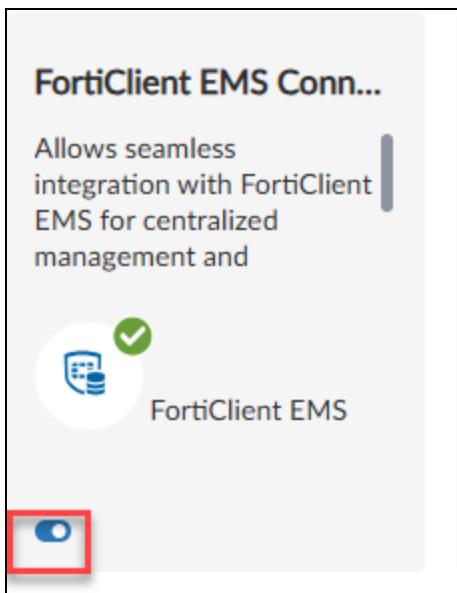
FortiClient EMS

IP/FQDN	10.0.1.100
User Name	student1
Password	*****

6. Click **OK** to save the configuration.

This configuration 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.

7. Enable the connector.



It takes a few minutes for the connector to establish the connection with FortiClient EMS.

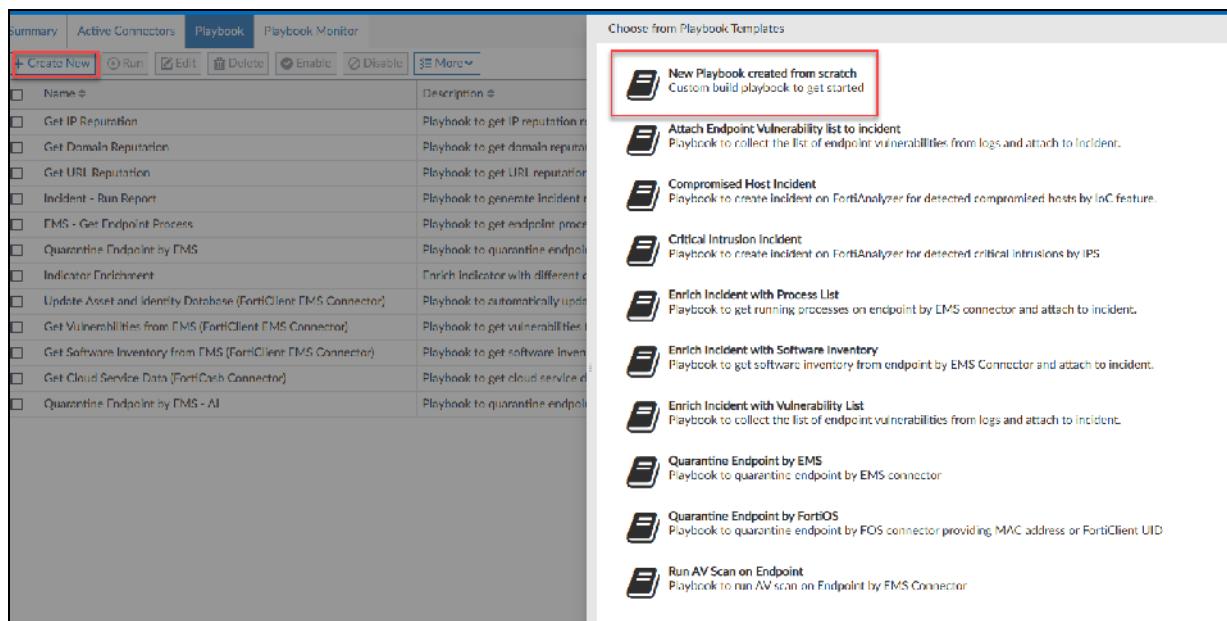
8. Refresh the FortiAnalyzer page to see the green check mark status.

Configure Playbooks on FortiAnalyzer

You will configure an on-demand playbook.

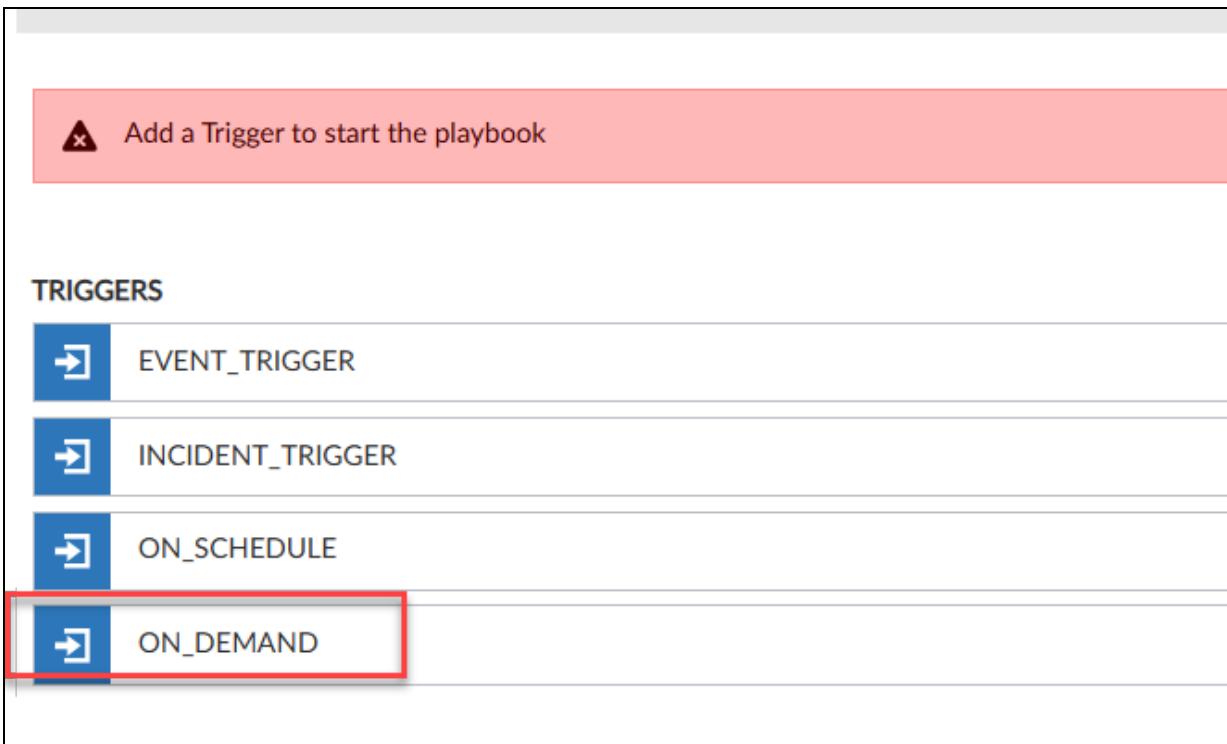
To configure a playbook with an on-demand trigger

1. Continuing on the FortiAnalyzer GUI, click **Incidents & Events > Automation**, and then click **Playbook**.
2. Click **Create New** to create a new playbook.
3. In the **Choose from Playbook Templates** window, select **New Playbook created from scratch**.

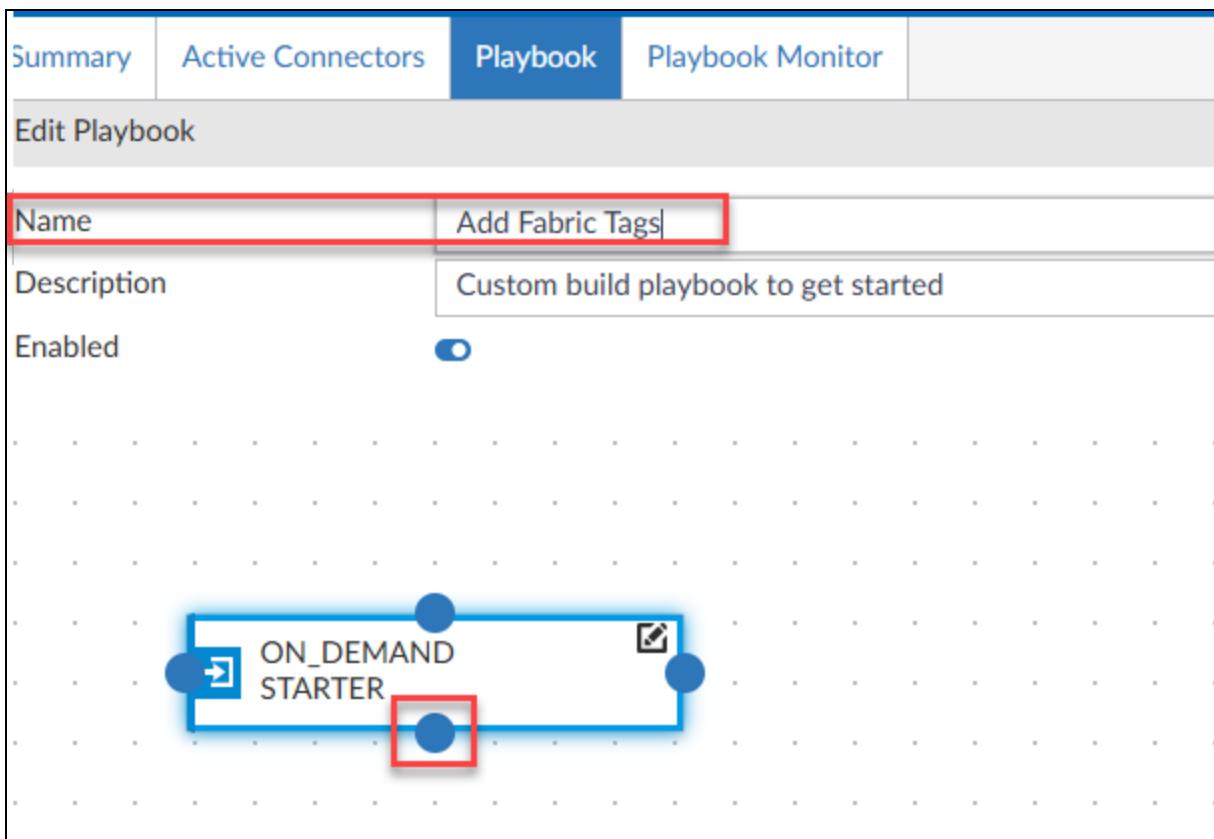


A new window opens.

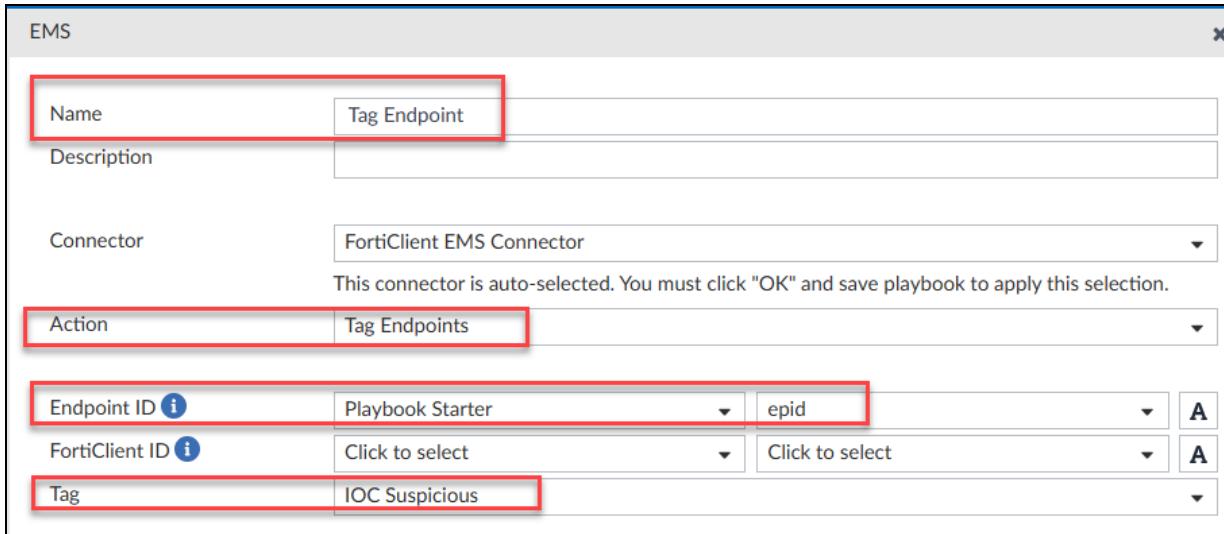
4. In the **TRIGGERS** section, select **ON_DEMAND**.



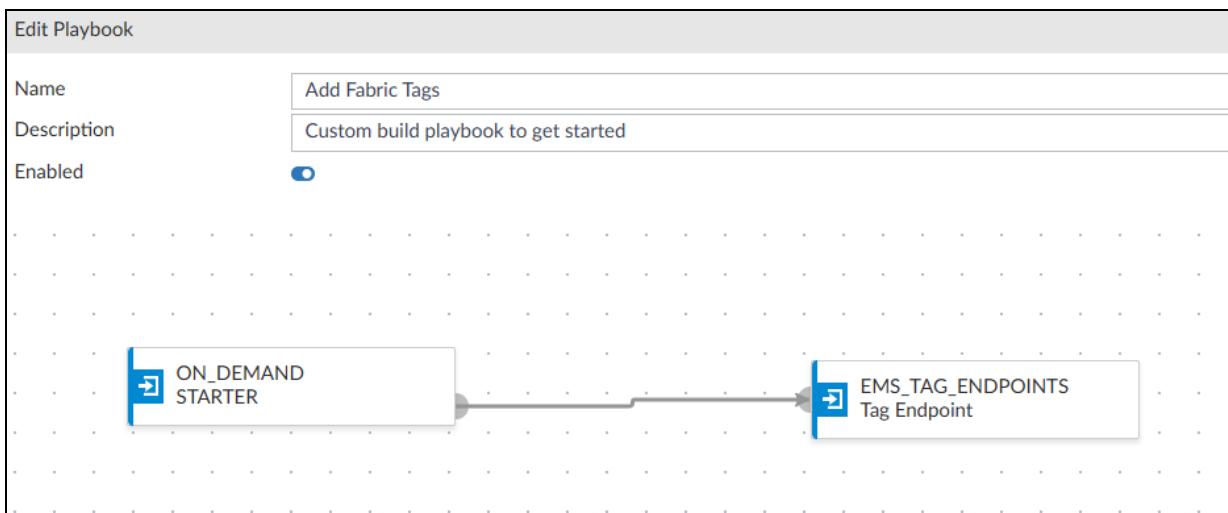
5. Click **Save**.
6. In the **Name** field, type Add Fabric Tags.
7. Drag and drop any highlighted connector points to add a new task.



8. In the **CONNECTORS** window, select **EMS**.
9. In the **Name** field, type **Tag Endpoint**.
10. In the **Action** field, select **Tag Endpoints**.
11. In the **Endpoint ID** field, select **Playbook Starter** and **epid**.
12. In the **Tag** field, select **IOC Suspicious**.



13. Click **OK** to save the task.



- Click **Save Playbook** to save the playbook configuration.

Run the FortiAnalyzer Playbook

You will run the playbook you configured in the previous task.

To run the on-demand playbook

- Continuing on the FortiAnalyzer GUI, click **Incidents & Events > Automation**, and then click **Playbook**.
- Select the **Add Fabric Tags** checkbox, and then click **Run**.

The screenshot shows the 'Playbook' list interface. The 'Run' button is highlighted with a red box. The 'Add Fabric Tags' playbook is selected and highlighted with a blue box. The table lists various playbooks with their descriptions and status.

	Name	Description	Status
<input type="checkbox"/>	Get IP Reputation	Playbook to get IP reputation report through VirusTotal connector	Enabled
<input type="checkbox"/>	Get Domain Reputation	Playbook to get domain reputation report through VirusTotal connector	Enabled
<input type="checkbox"/>	Get URL Reputation	Playbook to get URL reputation report through VirusTotal connector	Enabled
<input type="checkbox"/>	Incident - Run Report	Playbook to generate incident report	Enabled
<input type="checkbox"/>	EMS_Gct Endpoint Process	Playbook to get endpoint process	Enabled
<input checked="" type="checkbox"/>	Add Fabric Tags	Custom build playbook to get started	Enabled
<input type="checkbox"/>	Quarantine Endpoint by EMS	Playbook to quarantine endpoint by EMS connector	Enabled

- In the **Endpoint** field, select **hq-pc-1**.

The screenshot shows the 'Manually Run Playbook Add Fabric Tags' dialog box. The 'Endpoint' field is set to 'hq-pc-1 (1034)'. The 'OK' and 'Cancel' buttons are visible at the bottom.

4. Click **OK**.

It takes a couple of minutes for the playbook to execute.

5. Click **Incidents & Events > Automation**, and then click **Playbook Monitor**.

Summary	Active Connectors	Playbook	Playbook Monitor	Search...
Job ID: 2024-11-24 18:12:46:438-08	Playbook: Add Fabric Tags	Trigger: user/admin	Start Time: 2024-11-24 18:12:49 0800	End Time: 2024-11-24 18:13:00 0800

You can see that the **Add Fabric Tags** playbook ran successfully.

6. Continuing on the HQ-EMS-1 VM, log in to the FortiClient EMS GUI.

7. Click **Administration > Log Viewer** to see the FortiAnalyzer API request.

Date	Level	Source	Message	Occurrences
2024-11-25 03:17:58	Info	Console	student1 has logged in from 10.0.1.100.	1 time since 20...
2024-11-25 03:15:30	Info	Console	Certificate user: FGVM02TM19001113 FGT authoriz...	1 time since 20...
2024-11-25 03:12:55	Info	Console	student1 has logged out from 10.0.1.20.	1 time since 20...
2024-11-25 03:12:55	Info	Console	FAZ tagged hq-pc-1 as [IOC Suspicious].	1 time since 2024-11-25 03:12:55
2024-11-25 03:12:55	Info	Console	student1 has logged in from 10.0.1.20.	1 time since 20...

The IP address of the FortiAnalyzer is **10.0.1.20** and it is performing the actions configured in the playbook.

8. Click **Endpoints > All Endpoints**, and then click **hq-pc-1**.

The endpoint is tagged as **IOC Suspicious**. The **Classification Tags-Fabric** value can also be shared with fabric FortiGate devices and can be applied to firewall policies to restrict access.

Summary	Antivirus Events	Web Filter Events	Vulnerability Events	PUA Events	System Events	⋮								
<div> <p>admin admin No Email Linux Endpoints</p> <p>Device: hq-pc-1 OS: Linux - Ubuntu 22.0... IP: 10.0.1.10 MAC: 02-09-0f-00-02-05 Public IP: Status: Online Location: On-Fabric Owner: Organization: Group Tag: Security: all_registered_clients Posture: Compliant Tags: Network: ens3 Status: </p> </div>	<p>Connection Managed by EMS </p> <p>Configuration</p> <table> <tbody> <tr> <td>Policy</td> <td>Linux Policy </td> </tr> <tr> <td>Installer</td> <td>Not assigned</td> </tr> <tr> <td>FortiClient Version</td> <td>7.4.0.1636</td> </tr> <tr> <td>FortiClient Serial Number</td> <td>FCT8002553990302</td> </tr> <tr> <td>FortiClient ID</td> <td>F575ACDBF9F54E...</td> </tr> <tr> <td>ZTNA Serial Number</td> <td>Disabled</td> </tr> </tbody> </table> <p>Classification Tags</p> <p> Low + Add</p> <p>Classification Tags - Fabric</p> <p> IOC Suspicious </p>	Policy	Linux Policy	Installer	Not assigned	FortiClient Version	7.4.0.1636	FortiClient Serial Number	FCT8002553990302	FortiClient ID	F575ACDBF9F54E...	ZTNA Serial Number	Disabled	<p>Status</p> <p>Quarantined Quarantine: b72f4d6146584315 Access Code: </p> <p>Features</p> <ul style="list-style-type: none"> Antivirus enabled Real-Time Protection enabled Anti-Ransomware not installed Cloud Based Malware Outbreak Detection not installed Sandbox not installed Sandbox Cloud not installed Web Filter enabled Application Firewall not installed Remote Access installed Vulnerability Scan enabled SSOMA not installed
Policy	Linux Policy													
Installer	Not assigned													
FortiClient Version	7.4.0.1636													
FortiClient Serial Number	FCT8002553990302													
FortiClient ID	F575ACDBF9F54E...													
ZTNA Serial Number	Disabled													



The SOC team and the FortiClient EMS administrator can investigate the logs of the infected endpoint manually or configure the playbooks to attach the events to the playbook, and then take the necessary remediation actions.

9. Click **Endpoints > All Endpoints**, select **hq-pc-1**, click **Action**, and then click **Unquarantine** to allow internet access to the endpoint.

The screenshot shows the FortiClient EMS interface. At the top, there are summary statistics: 0 Not Installed, 0 Not Registered, 1 Out-Of-Sync, and 2 Security Risk. Below this is a navigation bar with 'Endpoints', 'Scan', 'Patch', and 'Move to' buttons. The main list displays three endpoints: 'br-pc-1' (Linux Endpoints, admin, 10.1.0.10), 'hq-pc-1' (Linux Endpoints, admin, 10.0.1.10, selected), and 'Jumpbox' (Domain Controllers, Adminis..., 172.16.9.50). A context menu is open for 'hq-pc-1', showing options like 'Request FortiClient Logs', 'Unquarantine' (which is highlighted with a red box), 'Exclude from Management', 'Revoke Client Certificate', 'Switch EMS', 'Clear Events', 'Set Importance', 'Delete Stale Verified Users', and 'Send Message'. On the right side of the interface, there are status indicators for Workflows (WF 2), System (SYS 4), and Vulnerabilities (VUL 3).

10. Return to the HQ-PC-1 VM.
11. Close Chrome.
12. Try to ping FortiGate, the FortiClient EMS server, and google.com.
Your traffic should now be allowed.

Lab 9: Troubleshooting and Diagnostics

In this lab, you will troubleshoot connectivity issues from FortiClient to FortiClient EMS. You will also learn how to reset the local built-in administrator password on FortiClient EMS.

Objectives

- Determine why FortiClient cannot establish a telemetry connection with FortiClient EMS
- Reset the FortiClient EMS local built-in administrator password

Time to Complete

Estimated: 25 minutes

Prerequisites

Before you begin this lab, you must identify the FortiClient EMS IP address.

To identify the FortiClient EMS IP address

1. On the Fortinet Training Institute side bar, click **POD IP**.
2. In the **CREDENTIALS** section, under **IP address**, locate and make a note of the IP address.
You will use this address where the lab asks for <FortiClient EMS IP>.
Before you begin this lab, you must run a script to break the communication from the FortiClient to the FortiClient EMS.
3. On the Windows-AD VM desktop, open the **Resources** folder, and then double-click the `firewallon.bat` script.

Prerequisites (Self-Paced Only)

Before you begin this lab, you must identify the IP address of the FortiClient EMS, Windows-AD VM, and install FortiClient on Windows endpoint.



Do not perform these steps if you are taking an instructor-led class. These steps are required only if you are performing the self-paced labs.

To identify the IP address of the FortiClient EMS

1. On the Fortinet Training Institute side bar, click **POD IP**.
2. In the **CREDENTIALS** section, under **IP address**, locate and make a note of the IP address.
You will use this address where the lab asks for <FortiClient EMS IP address>.

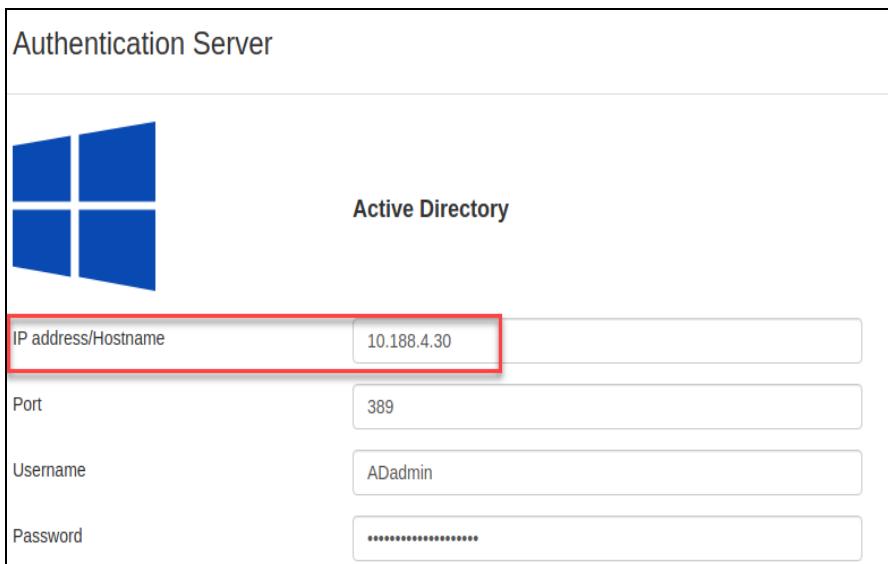
To identify the IP address of the Windows-AD VM

1. On the Fortinet Training Institute side bar, click **Windows-AD**.
2. In the **CREDENTIALS** section, under **IP address**, locate and make a note of the IP address.

You will use this address where the lab asks for <Windows-AD IP address>.

To update the IP address of the Windows-AD VM

1. On the HQ-EMS-1 VM, log in to the FortiClient EMS GUI.
2. Click **Administration > Authentication Servers**, and edit the existing **Active Directory** entry.
3. Update the **IP address/Hostname** field to match the Windows-AD VM IP address.



The screenshot shows the 'Authentication Server' configuration for 'Active Directory'. It includes a Windows logo icon, fields for 'IP address/Hostname' (10.188.4.30), 'Port' (389), 'Username' (ADadmin), and 'Password' (redacted). The 'IP address/Hostname' field is highlighted with a red border.

4. Click **Test** to check the connectivity.
5. Click **Save** to save the authentication server.

To update the Domain Windows-AD VM

1. Continuing on the FortiClient EMS GUI, click **Endpoints > Manage Domains**, and delete the existing entry.
2. Click **Yes**.
3. Click **Add > ADDS** to open the **Domain Import** window.
4. In the **ADDS Server** field, select **trainingAD.training.lab**.
5. In the **Select Base DN** section, select the **trainingAD.training.lab** checkbox to add all the groups.

6. Click **Save** to import all the endpoints and users.

Install FortiClient on AD Endpoint

1. On the Windows-AD VM, on the desktop, open the **Resources** folder.
2. Double-click the **FortiClient.msi** file.
3. In the **FortiClient Setup** window, select the checkbox to accept the license agreement, and then click **Next** to start the installation.
4. In the **Choose Setup Type** window, ensure that the **Secure Remote Access, Vulnerability Scan, Advanced Persistent Threat (APT) Components, Sandbox detection, Cloud Scan, and ZTNA** checkboxes are selected.
5. Click **Next** to continue.
6. In the **Additional Security Features** window, select **Antivirus, Web Filtering, and Anti-Ransomware** checkboxes.
7. Click **Next** to continue.
8. Click **Next** to continue.
9. Click **Install** to continue.
10. After the FortiClient installation is complete, click **Finish**.
11. Open the FortiClient console.
12. In the **Enter Server address or Invitation code** field, type the <FortiClient EMS IP address>.
13. Click **Connect**.
14. In the **Invalid certificate detected** window, click **Accept**.

Prerequisites (Self-Paced Only)

Before you begin this lab, you must identify the IP address of the FortiClient EMS, Windows-AD VM, and install FortiClient on Windows endpoint.



Do not perform these steps if you are taking an instructor-led class. These steps are required only if you are performing the self-paced labs.

To identify the IP address of the FortiClient EMS

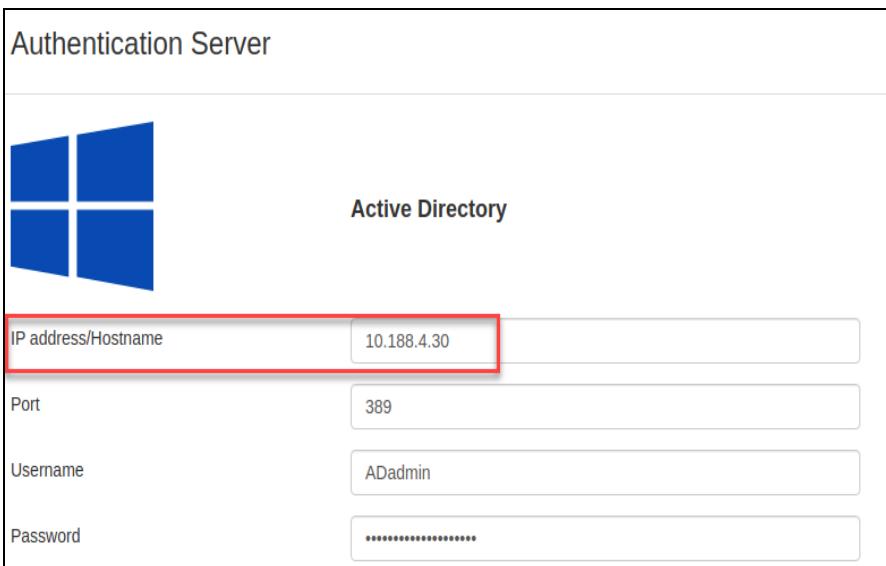
1. On the Fortinet Training Institute side bar, click **POD IP**.
2. In the **CREDENTIALS** section, under **IP address**, locate and make a note of the IP address.
You will use this address where the lab asks for <FortiClient EMS IP address>.

To identify the IP address of the Windows-AD VM

1. On the Fortinet Training Institute side bar, click **Windows-AD**.
2. In the **CREDENTIALS** section, under **IP address**, locate and make a note of the IP address.
You will use this address where the lab asks for <Windows-AD IP address>.

To update the IP address of the Windows-AD VM

1. On the HQ-EMS-1 VM, log in to the FortiClient EMS GUI.
2. Click **Administration > Authentication Servers**, and edit the existing **Active Directory** entry.
3. Update the **IP address/Hostname** field to match the Windows-AD VM IP address.



Authentication Server	
Active Directory	
IP address/Hostname	10.188.4.30
Port	389
Username	ADadmin
Password	*****

4. Click **Test** to check the connectivity.
5. Click **Save** to save the authentication server.

To update the Domain Windows-AD VM

1. Continuing on the FortiClient EMS GUI, click **Endpoints > Manage Domains**, and delete the existing entry.
2. Click **Yes**.
3. Click **Add > ADDS** to open the **Domain Import** window.
4. In the **ADDS Server** field, select **trainingAD.training.lab**.
5. In the **Select Base DN** section, select the **trainingAD.training.lab** checkbox to add all the groups.

6. Click **Save** to import all the endpoints and users.

Install FortiClient on AD Endpoint

1. On the Windows-AD VM, on the desktop, open the **Resources** folder.
2. Double-click the **FortiClient.msi** file.
3. In the **FortiClient Setup** window, select the checkbox to accept the license agreement, and then click **Next** to start the installation.
4. In the **Choose Setup Type** window, ensure that the **Secure Remote Access, Vulnerability Scan, Advanced Persistent Threat (APT) Components, Sandbox detection, Cloud Scan, and ZTNA** checkboxes are selected.
5. Click **Next** to continue.
6. In the **Additional Security Features** window, select **Antivirus, Web Filtering, and Anti-Ransomware** checkboxes.
7. Click **Next** to continue.
8. Click **Next** to continue.
9. Click **Install** to continue.
10. After the FortiClient installation is complete, click **Finish**.
11. Open the FortiClient console.
12. In the **Enter Server address or Invitation code** field, type the <FortiClient EMS IP address>.
13. Click **Connect**.
14. In the **Invalid certificate detected** window, click **Accept**.

Exercise 1: Troubleshooting FortiClient Connectivity to FortiClient EMS

In this exercise, you will troubleshoot a telemetry connectivity issue between FortiClient and FortiClient EMS.



The steps in this exercise only work if you executed the script as instructed in the *Prerequisites* section of this lab.

Review the FortiClient Telemetry Connectivity Status

You will review the FortiClient telemetry status on FortiClient EMS.

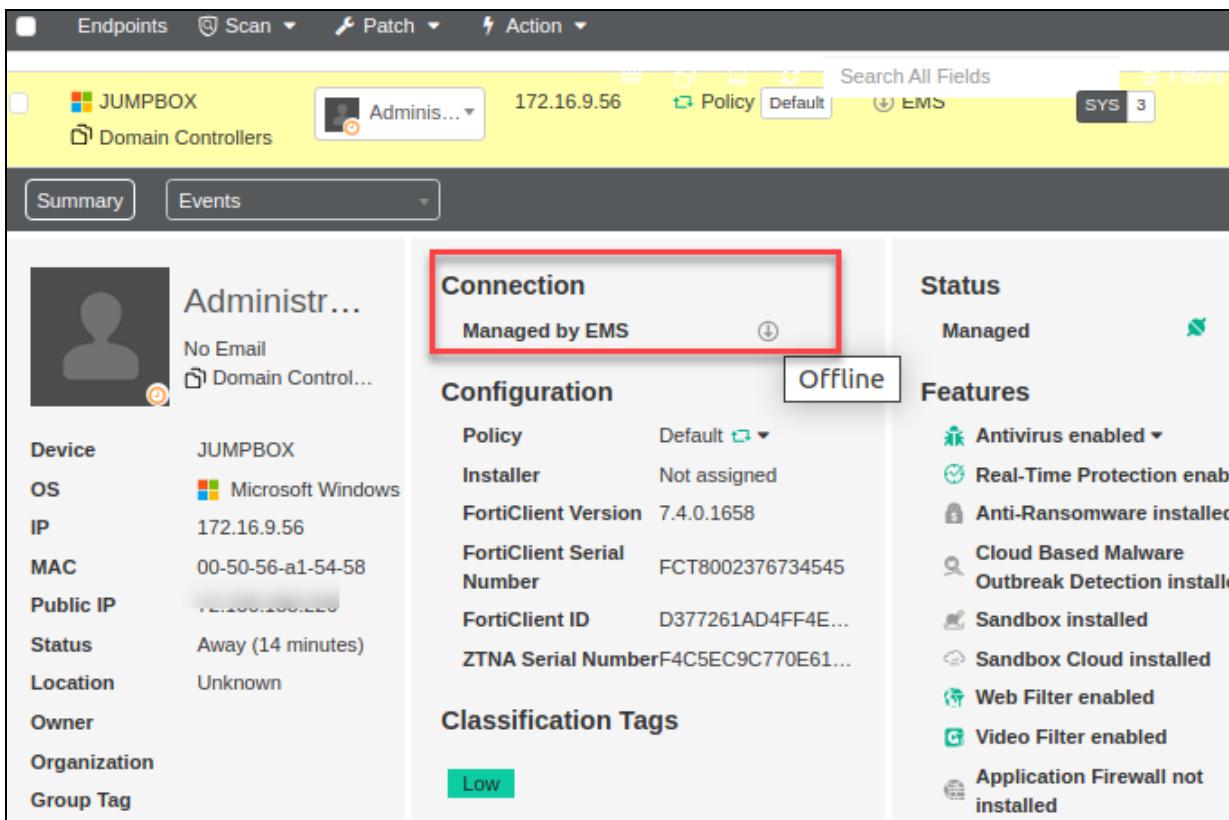
To review the FortiClient telemetry connectivity status

1. On the HQ-EMS-1 VM, log in to the FortiClient EMS GUI.
2. Click **Endpoints > All Endpoints**, and then click **JUMPBOX**.



It will take a few minutes for the endpoint to be marked as offline. The default keep-alive interval is 60 seconds and it takes 5 missed keep-alives for an endpoint to be marked as offline.

In the **Connection** section, the value in the **Managed by EMS** field is **Offline**.



The screenshot shows the FortiClient EMS interface. At the top, there are tabs for 'Endpoints', 'Scan', 'Patch', and 'Action'. Below the tabs, a search bar and a 'Filters' button are present. The main area displays a list of devices. The first device is 'JUMPBOX', which is a 'Domain Controllers' type. The device details are as follows:

Administr...	Managed by EMS	Status
No Email	Offline	Managed
Domain Control...		
Device: JUMPBOX	Policy: Default	Features: Antivirus enabled, Real-Time Protection enabled, Anti-Ransomware installed, Cloud Based Malware Outbreak Detection installed, Sandbox installed, Sandbox Cloud installed, Web Filter enabled, Video Filter enabled, Application Firewall not installed
OS: Microsoft Windows	Installer: Not assigned	
IP: 172.16.9.56	FortiClient Version: 7.4.0.1658	
MAC: 00-50-56-a1-54-58	FortiClient Serial Number: FCT8002376734545	
Public IP: 172.16.9.56	FortiClient ID: D377261AD4FF4E...	
Status: Away (14 minutes)	ZTNA Serial Number: F4C5EC9C770E61...	
Location: Unknown		
Owner:	Classification Tags: Low	
Organization:		
Group Tag:		



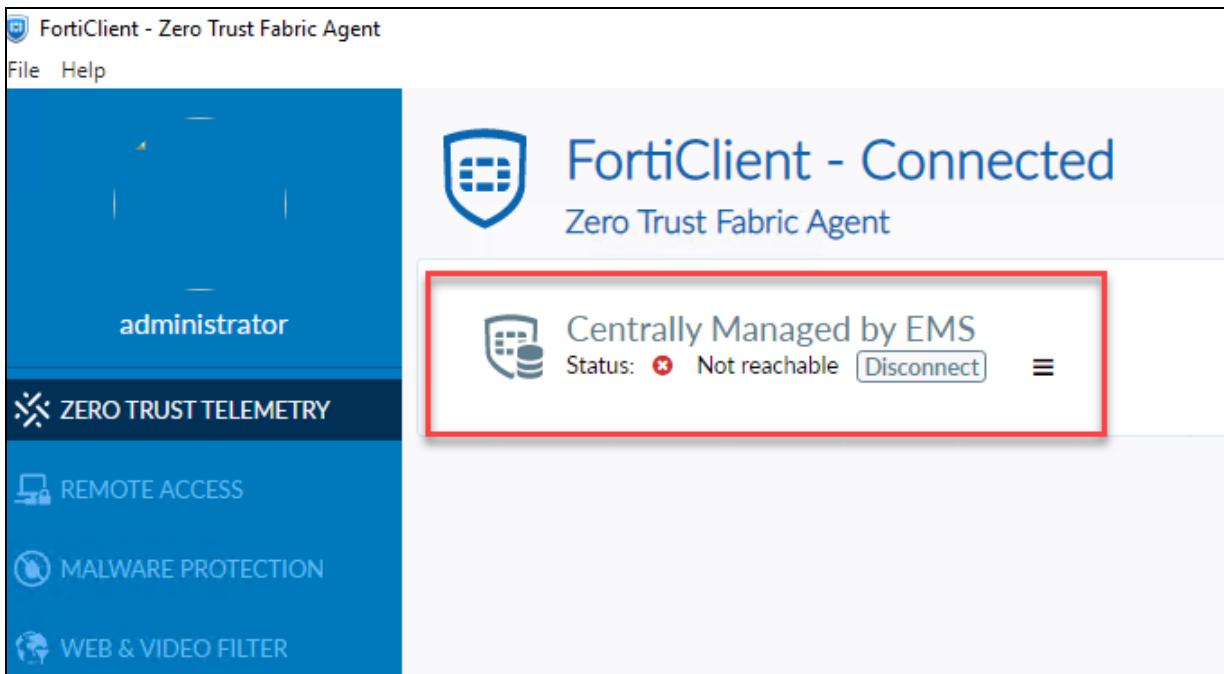
A status of **Offline** means that FortiClient cannot establish a telemetry connection to FortiClient EMS.

Troubleshoot the FortiClient Telemetry Connectivity Issue

You will troubleshoot the FortiClient telemetry connectivity issue on the Windows FortiClient endpoint.

To troubleshoot the Windows-AD VM

1. On the Windows-AD VM, open the FortiClient console, in the **ZERO TRUST TELEMETRY** section, ensure that the status of **Centrally Managed by EMS** is **Not reachable**.



2. Open the command prompt, and then ping the <FortiClient EMS IP>. You made a note of this IP address when you completed the lab prerequisites.
3. If you can ping the server, enter `telnet <FortiClient EMS IP> 8013` to test the telemetry connection to the FortiClient EMS.

```
C:\Users\Administrator>ping 172.16.9.20

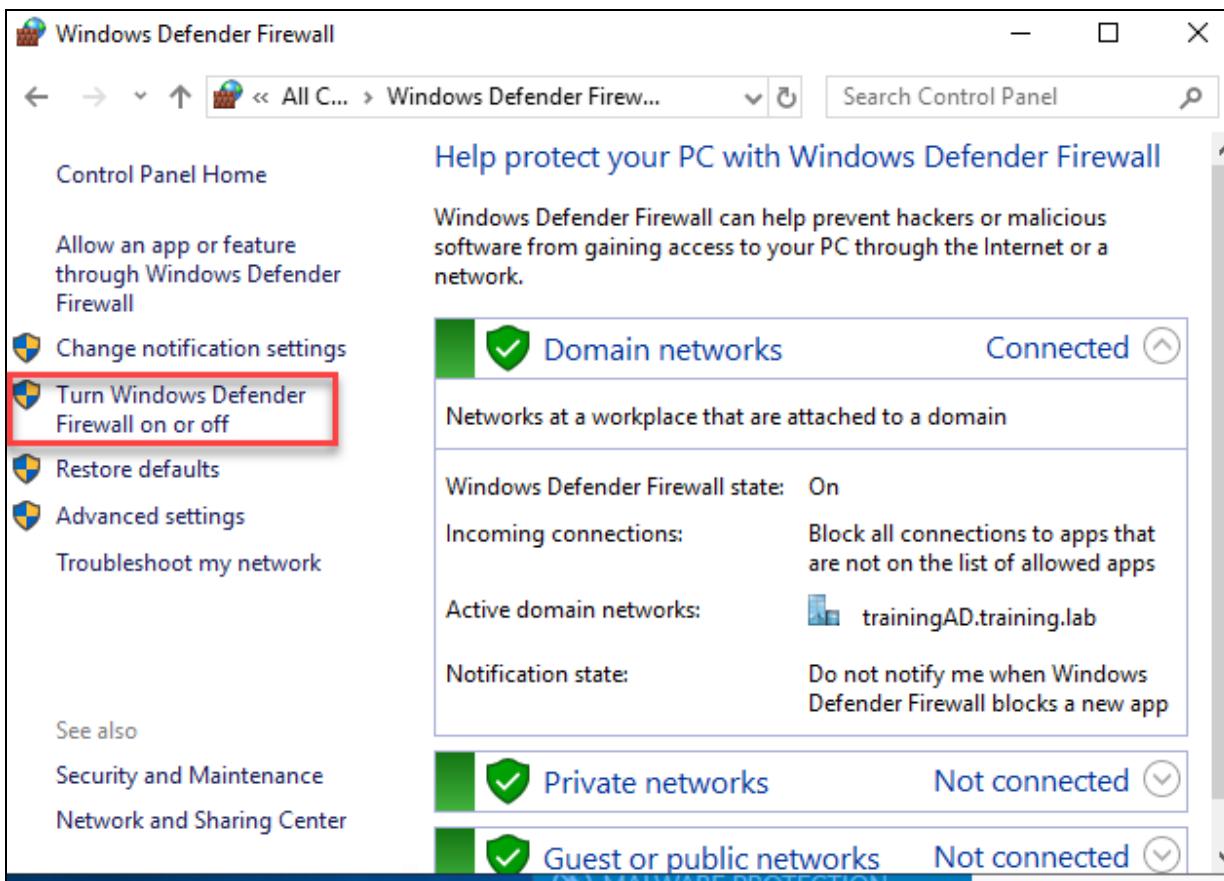
Pinging 172.16.9.20 with 32 bytes of data:
Reply from 172.16.9.20: bytes=32 time<1ms TTL=64

Ping statistics for 172.16.9.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>telnet 172.16.9.20 8013
Connecting To 172.16.9.20...Could not open connection to the host, on port 8013: Connect failed
```

The connection fails because Windows Firewall is active.

4. Click **Start > Control Panel**, click **System and Security**, and then click **Windows Defender Firewall**.
5. Click **Turn Windows Defender Firewall on or off**.



6. For each type of network, select **Turn off Windows Defender Firewall**.

Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Domain network settings

 Turn on Windows Defender Firewall

Block all incoming connections, including those in the list of allowed apps

Notify me when Windows Defender Firewall blocks a new app

 Turn off Windows Defender Firewall (not recommended)

Private network settings

 Turn on Windows Defender Firewall

Block all incoming connections, including those in the list of allowed apps

Notify me when Windows Defender Firewall blocks a new app

 Turn off Windows Defender Firewall (not recommended)

Public network settings

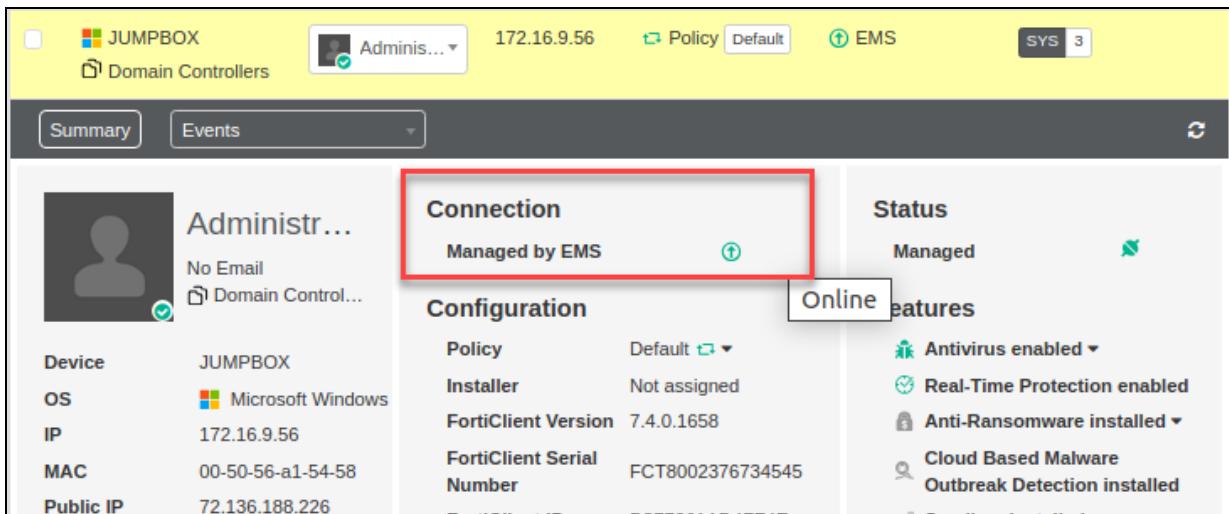
 Turn on Windows Defender Firewall

Block all incoming connections, including those in the list of allowed apps

Notify me when Windows Defender Firewall blocks a new app

 Turn off Windows Defender Firewall (not recommended)

7. Click **OK** to save the settings.
8. Return to the command prompt, and then enter `telnet <FortiClient EMS IP> 8013` to test connectivity. There should be an empty command prompt window. This means the connection was successful.
9. Return to the FortiClient console, and then in the **ZERO TRUST TELEMETRY** section, ensure that the status of **Centrally Managed by EMS** is **Connected**.
It may take a minute to see the updated status.
10. Return to the FortiClient EMS GUI, click **Endpoints > All Endpoints**, and then click **JUMPBOX**.
In the **Connection** section, the value in the **Managed by EMS** field is **Online**.



The screenshot shows the FortiClient EMS interface. At the top, there is a navigation bar with a 'JUMPBOX' icon, the IP address '172.16.9.56', a 'Policy' dropdown set to 'Default', an 'EMS' icon, and a 'SYS 3' button. Below the navigation bar, there are tabs for 'Summary' and 'Events'. The main content area displays a device profile for 'JUMPBOX'. The profile includes a user icon, the name 'Administr...', and a note 'No Email'. Below this, there is a list of device details: Device (JUMPBOX), OS (Microsoft Windows), IP (172.16.9.56), MAC (00-50-56-a1-54-58), and Public IP (72.136.188.226). To the right of the device details, there are three sections: 'Connection' (highlighted with a red box), 'Configuration', and 'Status'. The 'Connection' section shows 'Managed by EMS'. The 'Configuration' section shows 'Policy' (Default), 'Installer' (Not assigned), 'FortiClient Version' (7.4.0.1658), and 'FortiClient Serial Number' (FCT8002376734545). The 'Status' section shows 'Managed' and indicates the device is 'Online'. Below the status, there is a list of features: Antivirus enabled, Real-Time Protection enabled, Anti-Ransomware installed, Cloud Based Malware, and Outbreak Detection installed.

Device	JUMPBOX
OS	Microsoft Windows
IP	172.16.9.56
MAC	00-50-56-a1-54-58
Public IP	72.136.188.226

Connection	
Managed by EMS	

Configuration	
Policy	Default
Installer	Not assigned
FortiClient Version	7.4.0.1658
FortiClient Serial Number	FCT8002376734545

Status	
Managed	Online

Features	
Antivirus enabled	✓
Real-Time Protection enabled	✓
Anti-Ransomware installed	✓
Cloud Based Malware	
Outbreak Detection installed	

Exercise 2: Using the Password Recovery Tool to Reset the Built-In Administrator Password

In this exercise, you will reset the password for the FortiClient EMS built-in administrator using the password recovery tool. You will run the password recovery tool on the HQ-EMS-1 VM to generate a temporary password for the built-in administrator.



You must have execute permissions to run the password recovery tool.

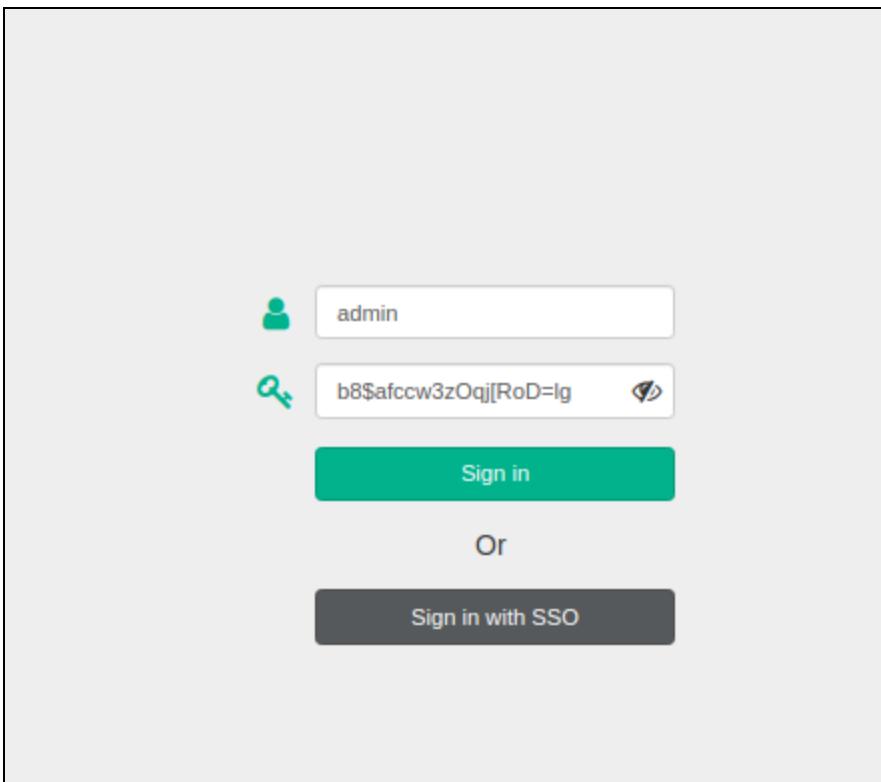
To run the password recovery tool

1. On the HQ-EMS-1 VM, click the **Terminal** icon to open the terminal window.
2. Enter `sudo -i`, and then if prompted, enter the following password:
Fortinet1!
3. Enter the following command:
`cd /opt/forticlientems/bin/`
4. Enter the following command:
`./PasswordRecovery`
5. Enter `yes`.
6. In the `Temporary password` field, copy the value.

```
root@hq-ems-1:/opt/forticlientems/bin# ./PasswordRecovery
Resetting "admin"s password
Please type 'yes' if you are sure to proceed: yes
Username has been reset to 'admin' and password has been updated.

Temporary password:
b8$afccw3z0qj[RoD=lg
```

7. Open a Chrome window, and then in **Bookmarks**, select the **HQ-EMS** login page bookmark.
8. Click **Accept**.
9. In the username field, type `admin`, in the password field, paste the temporary password, and then click **Sign in**.



FortiClient EMS prompts you to configure a new administrator and password.

10. In the **New Username** field, type `student1`.
11. In the **New Password** and **Confirm Password** fields, type `Password2!` to meet the password requirements, and then click **Submit** to save the password.

FortiClient Endpoint Management Server

This password is temporary. Please update your password.

	admin
	b8\$afccw3zOqj[RoD=lg
	student1

Different from default admin username
 At least 5 characters long

Your password must be
 At least 8 characters long

And has 3 out of the 4 following:
 At least one uppercase letter (A-Z)
 At least one lowercase letter (a-z)
 At least one number (0-9)
 At least one symbol (e.g. !\$#%)

Submit

Cancel

Lab 10: FortiClient Cloud

There is no lab associated with Lesson 10 at this time.

**DO NOT REPRINT
© FORTINET**

Brave-Dumps.com



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© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

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