

DO NOT REPRINT

© FORTINET



FortiClient EMS Lab Guide

for FortiClient EMS 7.0

Fortinet Training

<https://training.fortinet.com>

Fortinet Document Library

<https://docs.fortinet.com>

Fortinet Knowledge Base

<https://kb.fortinet.com>

Fortinet Fuse User Community

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

Fortinet Forums

<https://forum.fortinet.com>

Fortinet Support

<https://support.fortinet.com>

FortiGuard Labs

<https://www.fortiguards.com>

Fortinet Network Security Expert Program (NSE)

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

Fortinet | Pearson VUE

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

Feedback

Email: askcourseware@fortinet.com



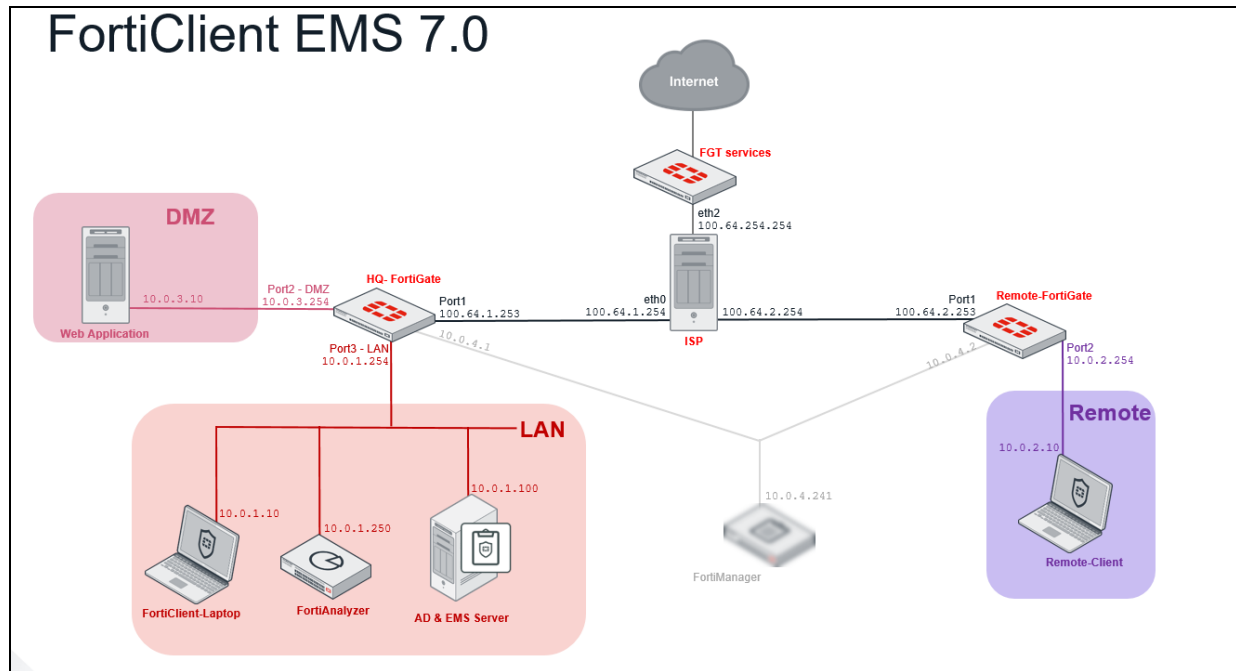
9/21/2021

TABLE OF CONTENTS

Network Topology	5
Lab 1: Introduction	6
Lab 2: FortiClient EMS and FortiClient Installation	7
Exercise 1: Installing FortiClient EMS	8
Install FortiClient EMS Using an Installation File	8
Access the FortiClient EMS GUI and Install the License	10
Exercise 2: Installing FortiClient	13
Install FortiClient Using a Custom Installer File From FortiClient EMS	13
Lab 3: FortiClient EMS Configuration	17
Exercise 1: Accessing the GUI and Creating a FortiClient EMS Administrator	18
Access the FortiClient EMS GUI	18
Create a New FortiClient EMS Administrator	20
Exercise 2: Configuring FortiClient EMS System Settings	22
Configure Server Settings	22
Configure Log Settings	23
Configure Login Banner Settings	23
Exercise 3: Creating an Endpoint Group and a Group Assignment Rule, and Running Scans	25
Create an Endpoint Group for a Windows Workgroup	25
Create a Group Assignment Rule for Windows Endpoints	26
Run Antivirus and Vulnerability Scans on a Registered Endpoint	27
Exercise 4: Enabling the Security Fabric to Trigger Automatic Quarantine	32
Verify FortiClient Log Settings	32
Enable the Security Fabric on the Root FortiGate	33
Lab 4: FortiClient Deployment Using FortiClient EMS	44
Exercise 1: Creating an Installer for Deployment	45
Create a FortiClient Installer for Deployment	45
Exercise 2: Adding Endpoints to FortiClient EMS	48
Add Endpoints Using an AD Domain Server	48
Exercise 3: Creating a Deployment Package to Install FortiClient	50
Create a Deployment Package to Install FortiClient	50
Lab 5: FortiClient Provisioning Using FortiClient EMS	52
Exercise 1: Creating and Assigning an Endpoint Profile for Deployment	53

Create an Endpoint Profile on FortiClient EMS.....	53
Create a Profile to Deploy FortiClient.....	53
Enable the Web Filter Feature in the Endpoint Profile.....	53
Provision a VPN in the Endpoint Profile.....	56
Create an Endpoint Policy to Assign the Endpoint Profile.....	57
Exercise 2: Testing the FortiGuard Web Filter.....	60
Verify FortiGuard Connectivity.....	60
Identify Web Filter Categories.....	60
Review a FortiGuard Category-Based Web Filter.....	63
Test the Web Filter.....	65
Verify a Web Filter Exclusion List.....	66
Test the Web Exclusion List.....	67
Exercise 3: Understanding Antivirus Protection and Vulnerability Scans.....	68
Verify AntiVirus Protection Settings.....	68
Test the Antivirus Real-Time Configuration.....	69
Run an On-Demand Vulnerability Scan.....	70
Lab 6: Zero Trust Network Access.....	72
Exercise 1: Configuring ZTNA Tags, Tagging Rules, and Features.....	74
Verify the Connection Between FortiClient, FortiClient EMS, and FortiGate.....	74
Configure FortiClient EMS ZTNA Tagging Rules.....	76
Enable the ZTNA Feature and Verify That ZTNA Tags Are Synced.....	80
Exercise 2: Configuring a Basic HTTPS Access Proxy With SSL Certificate-Based Authentication.....	81
Configure a Basic HTTPS Access Proxy With Certificate-Based Authentication.....	81
Test Remote Access to the HTTPS Access Proxy.....	85
Understand the Behavior of the set empty-cert-action Option.....	89
Exercise 3: Configuring an HTTPS Access Proxy With User Authentication and ZTNA Tags.....	91
Configure an Authentication Rule.....	92
Apply the User Group and ZTNA Tag to a ZTNA Rule.....	93
Test Remote Access to the HTTPS Access Proxy With User Authentication.....	94
Verify the Behavior When the Security Posture Changes on the Endpoint.....	97
Exercise 4: Configuring and Testing Compliance Rules to Create Dynamic Groups and Policies.....	99
Create a Firewall Policy.....	99
Test Endpoint Access Using the IP/MAC Filtering ZTNA Firewall Policy.....	100
Lab 7: Diagnostics and Troubleshooting.....	104
Exercise 1: Running Diagnostic Tools.....	105
Run the FortiClient Diagnostic Tool.....	105
Run the FortiClient EMS Diagnostic Tool.....	108

Network Topology



Lab 1: Introduction

There is no lab associated with Lesson 1.

Lab 2: FortiClient EMS and FortiClient Installation

In this lab, you will examine FortiClient EMS and FortiClient installation.

Objectives

- Install FortiClient EMS on a Windows AD server
- Apply a FortiClient EMS license
- Install FortiClient on a Windows endpoint

Time to Complete

Estimated: 25 minutes

Prerequisites

Before beginning this lab, you must make sure that the installer file from the EMS deployment package is available on the desktop of the FortiClient-Laptop VM, in the **Resources** folder.

Exercise 1: Installing FortiClient EMS

In this exercise, you will install FortiClient EMS on the AD server.



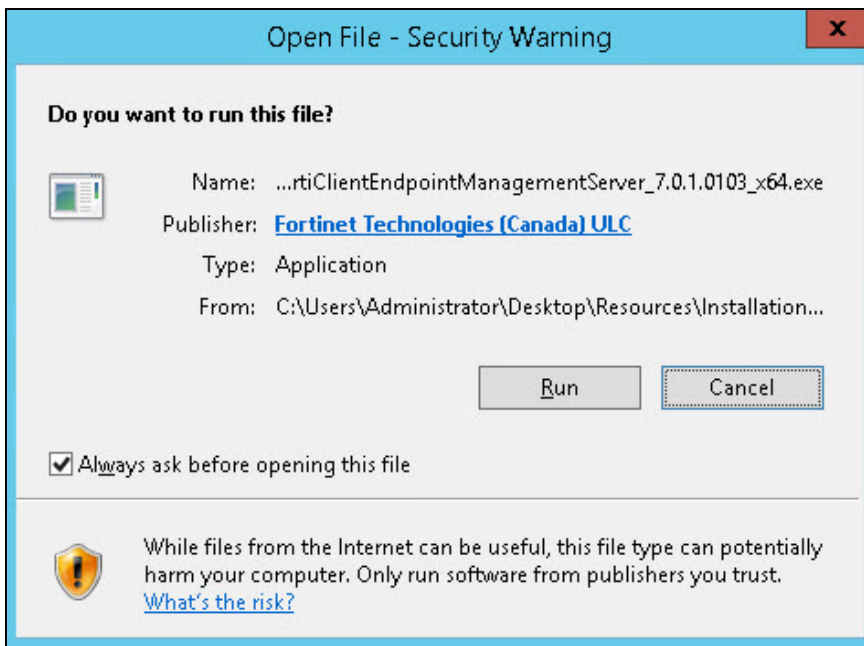
For this exercise, we have provided a FortiClient EMS installation file and license. In a real environment, you should *not* install FortiClient EMS on a Windows server that is hosting AD or any other services.

Install FortiClient EMS Using an Installation File

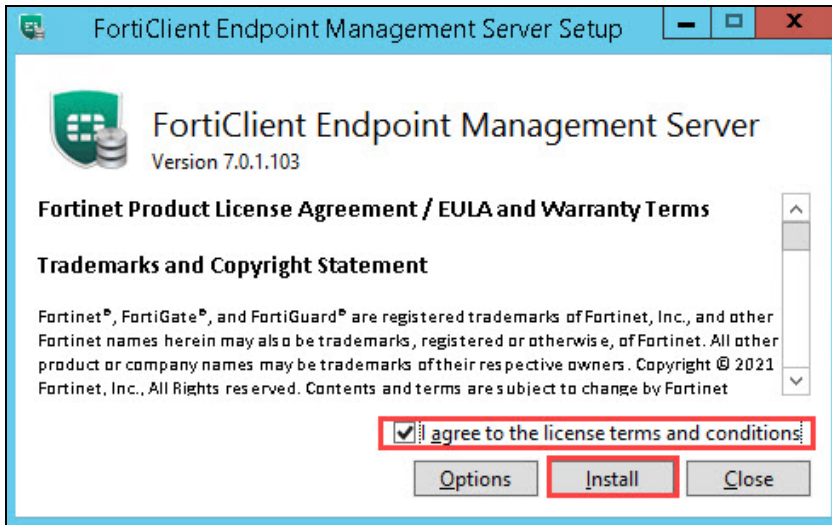
You will install FortiClient EMS using an installer file.

To install FortiClient EMS using an installer file

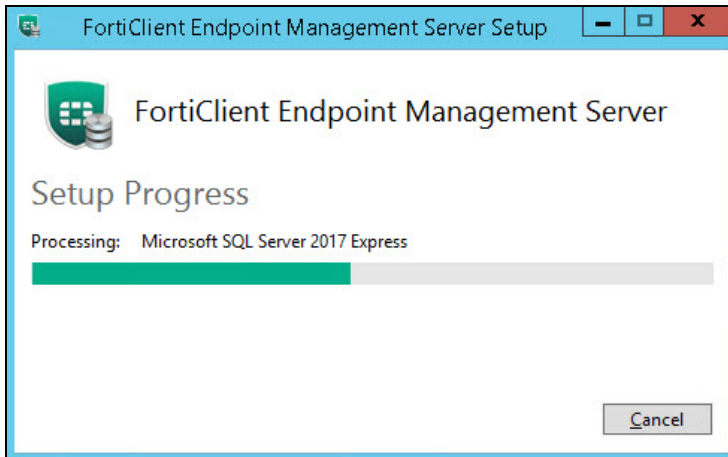
1. On the AD Server VM, on the desktop, click **Resources > Installation Files**.
2. Open the `FortiClientEndpointManagementServer_7.0.1.0103_x64.exe` file to launch the installation window.
3. Click **Run**.



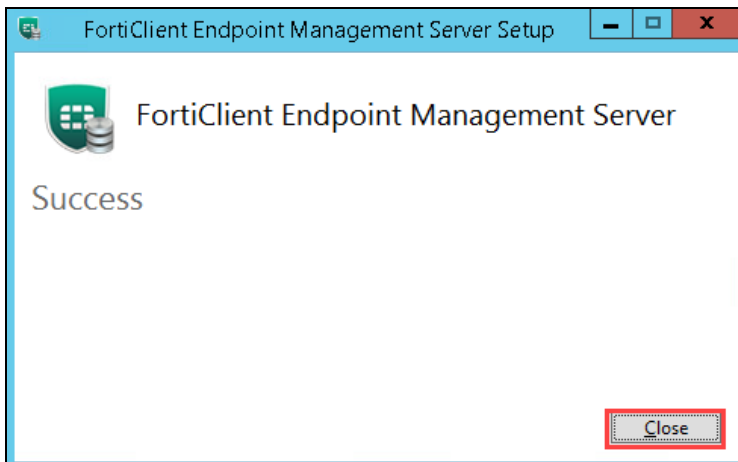
4. Accept the license agreement, and then click **Install** to start the installation.



The setup wizard installs FortiClient on the host machine. By default, the FortiClient EMS files are installed in the **C:\Program Files\Fortinet\FortiClient** folder.



5. After the FortiClient EMS installation is complete, click **Close**.



Access the FortiClient EMS GUI and Install the License

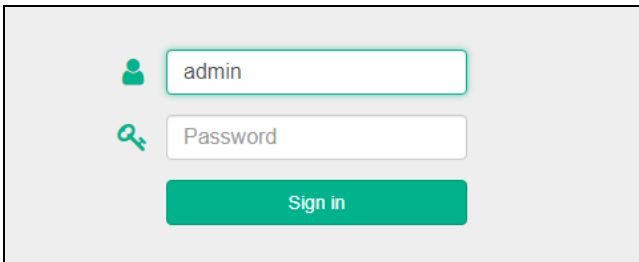
You will access the FortiClient EMS GUI, create an administrator password, and install the license.

To access the FortiClient EMS GUI and create an administrator password

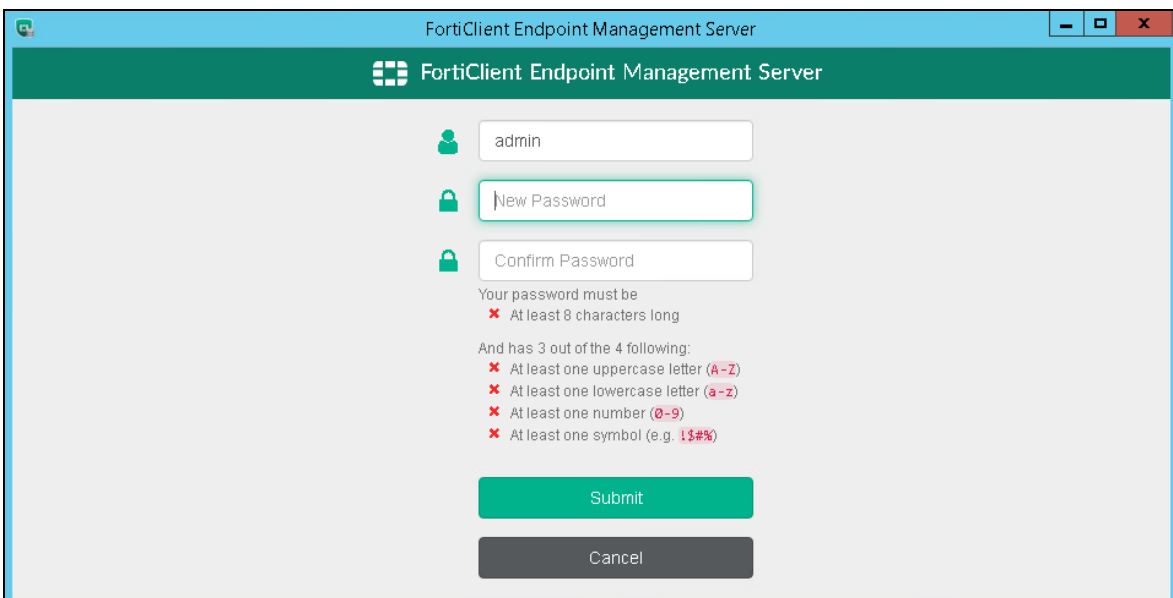
1. On the AD Server VM, click the FortiClient EMS icon on the desktop to launch the application.



2. Click **Sign in**, and then log in to the FortiClient EMS GUI with the username `admin` and no password.



FortiClient EMS prompts you to configure an administrator password.

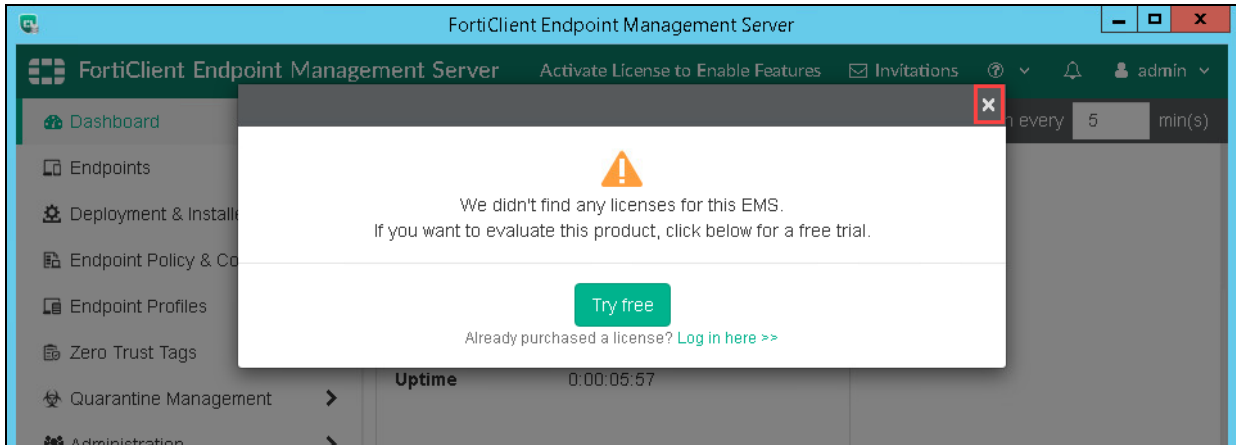


3. Type `Password123` in the **New Password** and **Confirm Password** fields to meet the password requirement, and then click **Submit** to save the password.

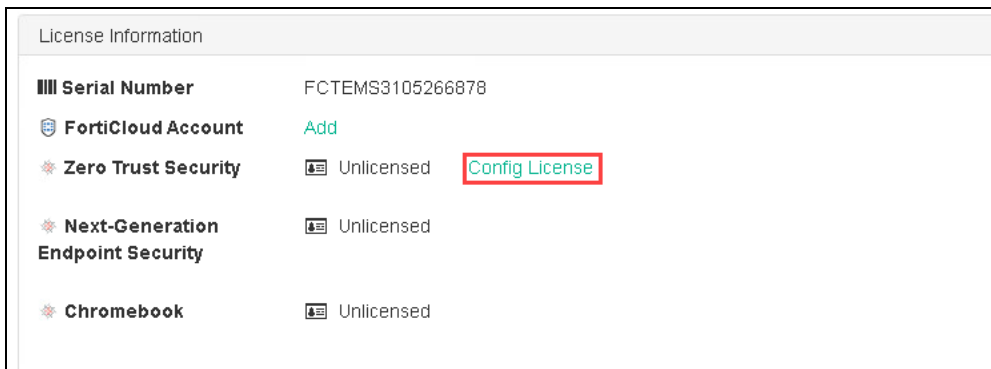
To install the FortiClient EMS license

1. Log in to the FortiClient EMS GUI with the username `admin` and password `Password123`.

A warning for the EMS license appears.



2. Click **X** to close the window.
3. On the **Dashboard > License Information** widget, click **Config License**.



4. In the **License Source** field, click **File Upload**, and then click **Browse** to select the license file in the **Desktop > Resources > Installation Files** folder.

Configure License

Serial number	FCTEMS3105266878
Hardware ID	736D7A92-51E6-4B14-89E7-607EBCED87EE-E7C20B63
Zero Trust Security	Unlicensed
Next-Generation Endpoint Security	Unlicensed
Chromebook	Unlicensed
License Source	FortiCare File Upload
License File	Browse... FCTEMS0000101875.l1c

Upload

Cancel

5. Click **Upload** to activate the new license.

✓ License updated successfully.

Configure License

Serial number	FCTEMS0000101875
Hardware ID	736D7A92-51E6-4B14-89E7-607EBCED87EE-E7C20B63
Zero Trust Security	Included
Next-Generation Endpoint Security	Licensed 2022-10-23

0 used of 25

6. On the FortiClient EMS GUI, click **Dashboard > Status** to see the license information.

Exercise 2: Installing FortiClient

In this exercise, you will install FortiClient on the FortiClient-Laptop VM.



From version 6.2.0 or later, FortiClient must be used with FortiClient EMS. FortiClient must connect to FortiClient EMS to activate its license and become provisioned by the endpoint profile that the administrator configured in FortiClient EMS. For this exercise, we have provided a deployment package file from FortiClient EMS. You cannot use FortiClient features until FortiClient is connected to FortiClient EMS and licensed.

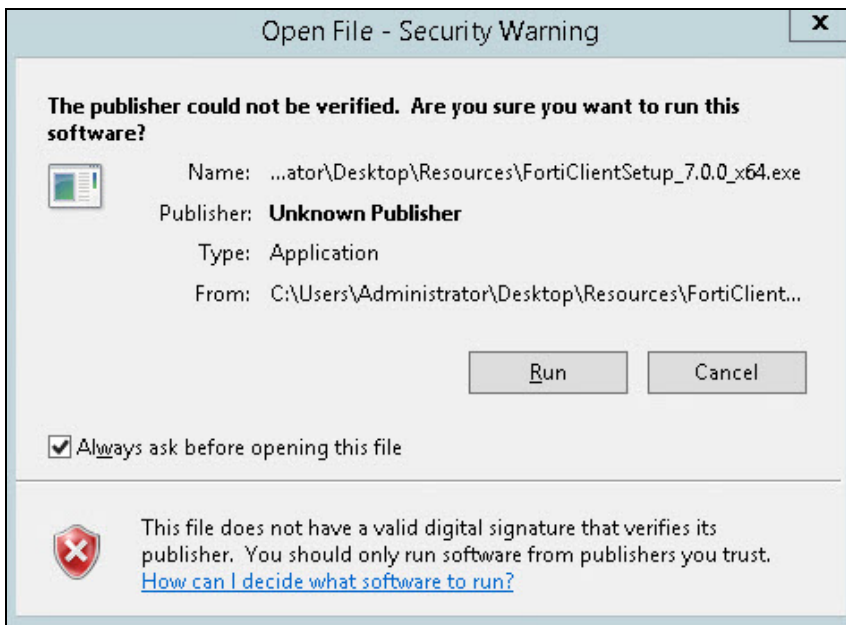
After installation, FortiClient will be managed by FortiClient EMS, and all security profiles have been configured to perform lab tasks.

Install FortiClient Using a Custom Installer File From FortiClient EMS

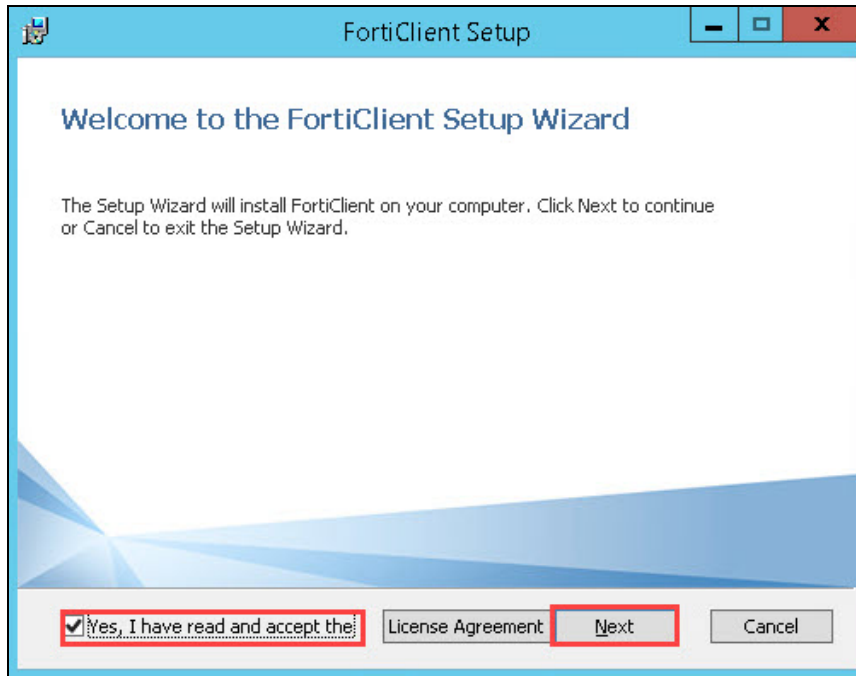
You will install FortiClient using an installer file from FortiClient EMS.

To install FortiClient using the installer file from FortiClient EMS

1. On the FortiClient-Laptop VM, on the desktop, open the **Resources** folder.
2. Run the `FortiClientSetup_7.0.0_x64.exe` file to start the FortiClient installation.

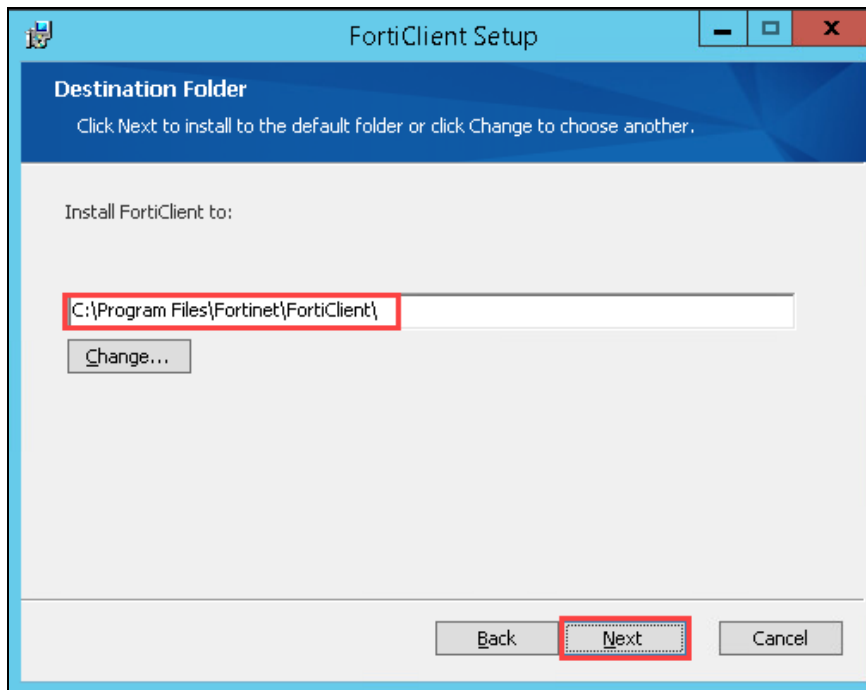


3. Accept the license agreement, and then click **Next** to start the installation.

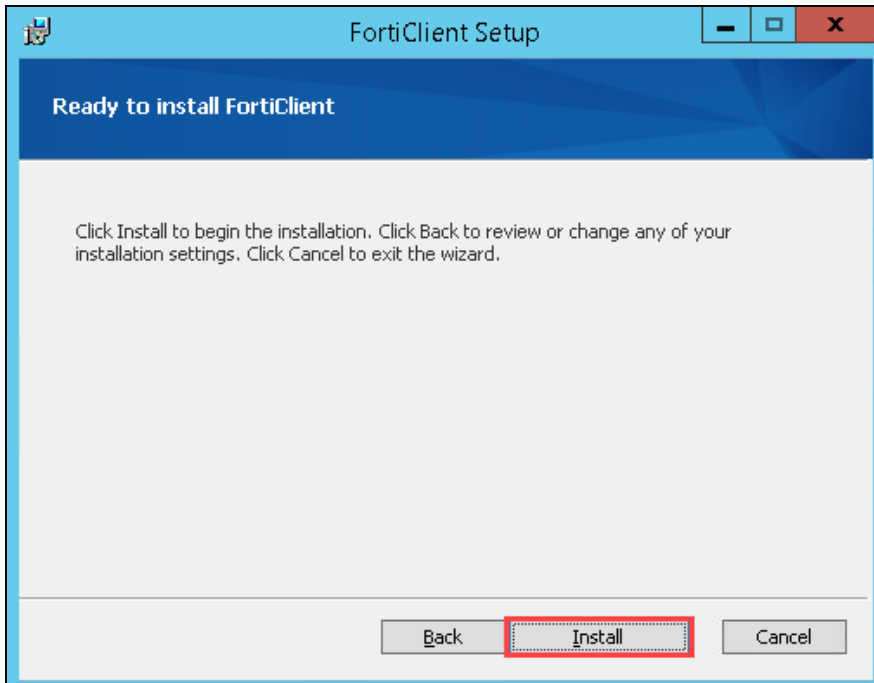


By default, the FortiClient files are installed in the **C:\Program Files\Fortinet\FortiClient** folder.

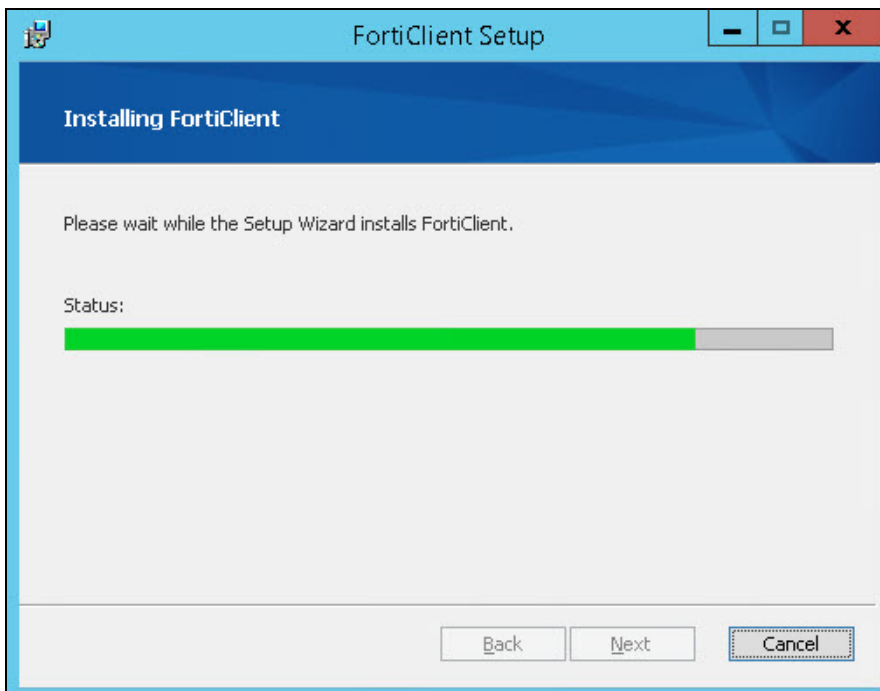
4. Click **Next** to continue.



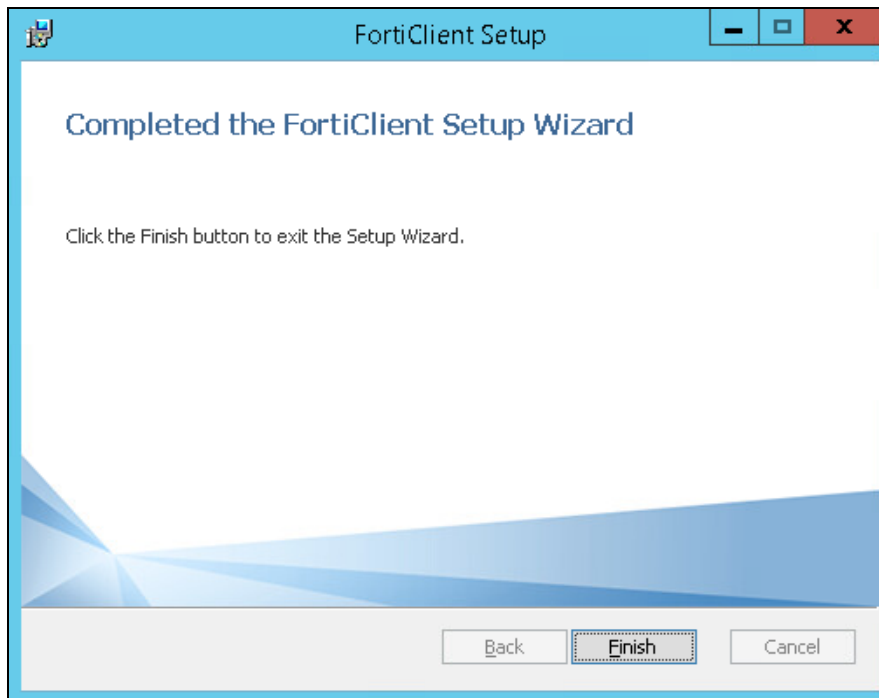
5. Click **Install**.



The setup wizard installs FortiClient on the host machine.



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



FortiClient downloads all the signature databases to get up-to-date. It may take some time before the download completes and FortiClient is available for you to configure other options. However, you can continue with the lab steps as the download process runs in the background.

7. On the FortiClient-Laptop VM, in the system tray, right-click the FortiClient icon.
8. Click **Open FortiClient Console** to open the FortiClient GUI.



Allow some time for FortiClient to get all of its configuration from FortiClient EMS.

Lab 3: FortiClient EMS Configuration

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

Objectives

- Access the FortiClient EMS GUI
- Explore the dashboard and view system information
- Create an administrator
- Configure system settings
- Create an endpoint group
- Run a vulnerability scan on an endpoint

Time to Complete

Estimated: 65 minutes

Prerequisites

Before beginning this lab, you must finish the previous lab.

Exercise 1: Accessing the GUI and Creating a FortiClient EMS Administrator

In this exercise, you will access the FortiClient EMS GUI, and then create a new administrator account.

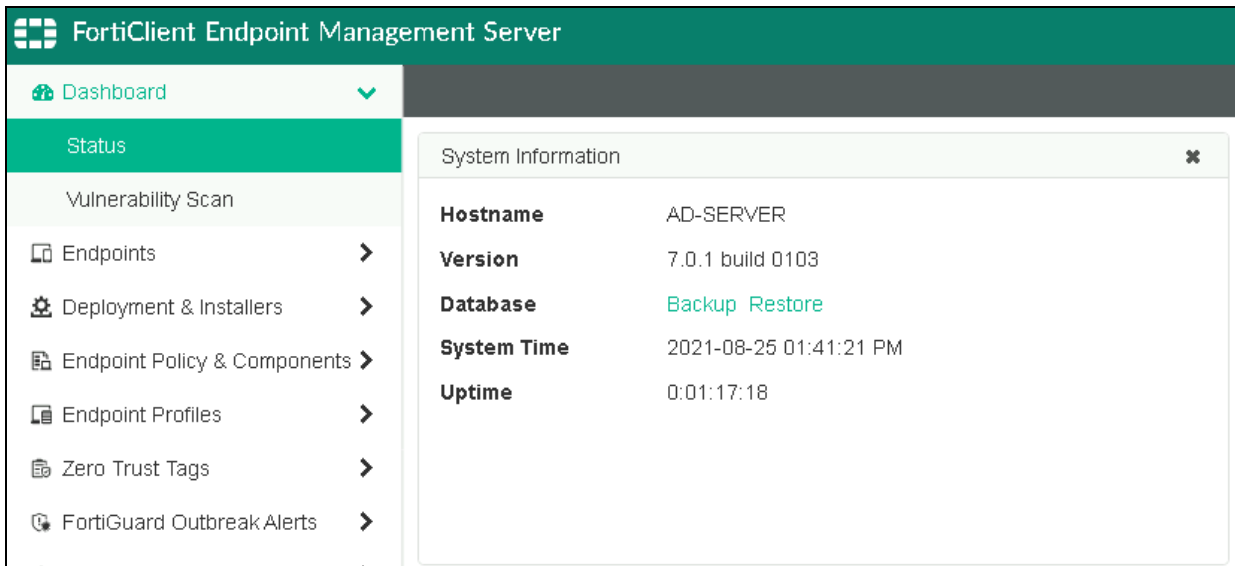
Access the FortiClient EMS GUI

You will access the FortiClient EMS GUI, by either launching the application or using a browser.

To access the FortiClient EMS GUI by launching the application

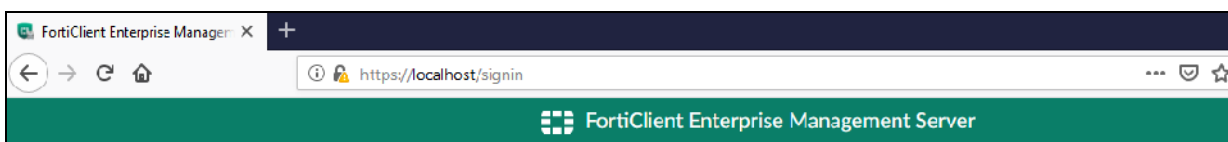
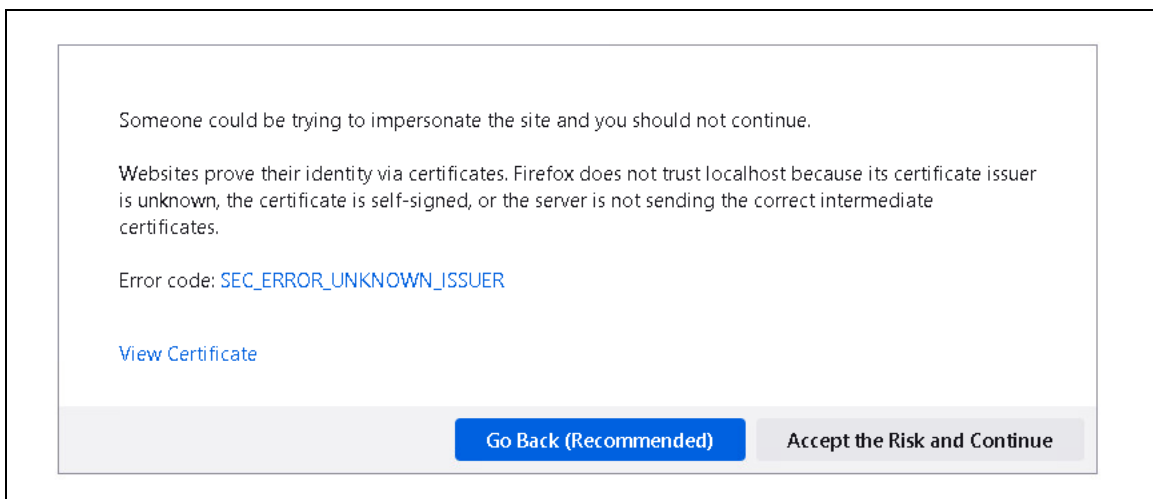
1. On the AD Server VM, click the FortiClient EMS icon to launch the application.
2. Log in to the FortiClient EMS GUI with the username `admin` and password `Password123`.
3. Locate the **System Information** widget, and then write down the software version that appears in the **Version** field.

You should see the following details:

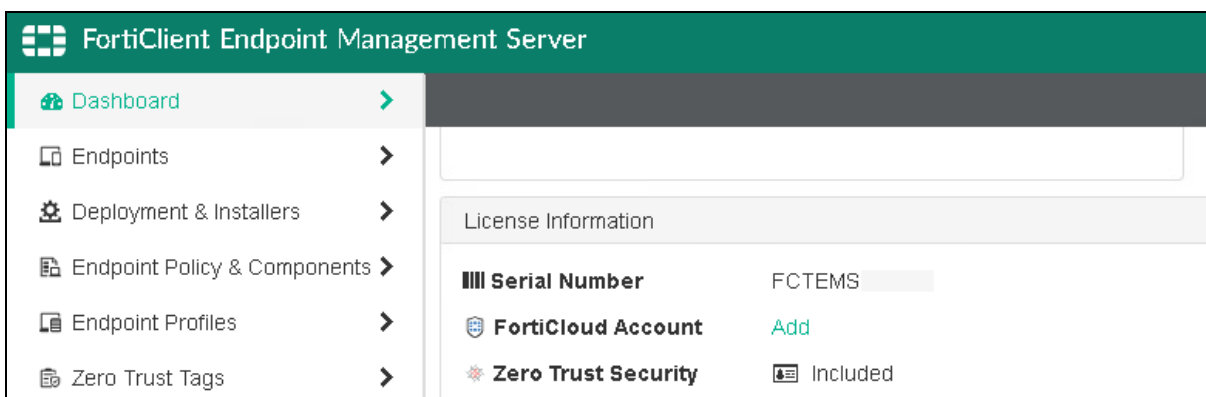


To access the FortiClient EMS GUI using a browser

1. Continuing on the AD Server VM, on the desktop, open Firefox.
2. In the address bar, type `https://localhost` to access the FortiClient EMS GUI.
3. Click **Advanced** > **Accept the Risk and Continue** to accept the self-signed certificate.



4. Log in to the FortiClient EMS GUI with the username `admin` and password `Password123`.
5. Click **Dashboard > Status** to confirm the FortiClient EMS serial number.
6. Locate the **License Information** widget, and then write down the serial number that appears in the **Serial Number** field.



You can also access the FortiClient EMS GUI using the server host name `https://<server_name>`.

Tip: You can get the `<server_name>` by running `ipconfig /all` on the server. The **Host Name** appears under Windows IP Configuration. If you cannot access the FortiClient EMS remotely, make sure that you can ping `<server_name>`, by adding it to the DNS entry or the Windows host file.

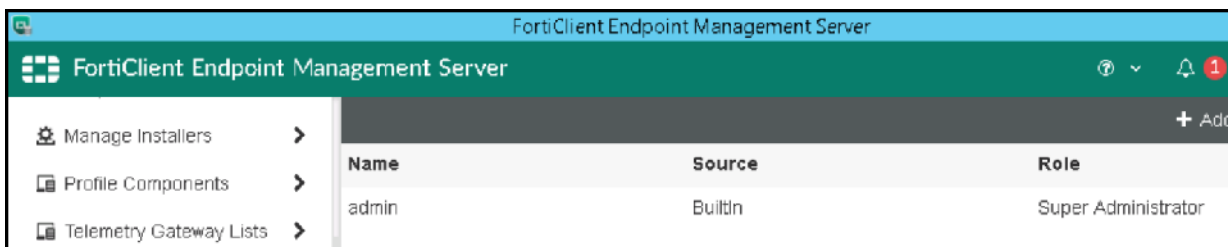
7. Navigate to **Endpoint Policy & Components**, and then you will see **CA Certificates**. Here, you can upload and manage certificates that can be used for EMS HTTPS access.

Create a New FortiClient EMS Administrator

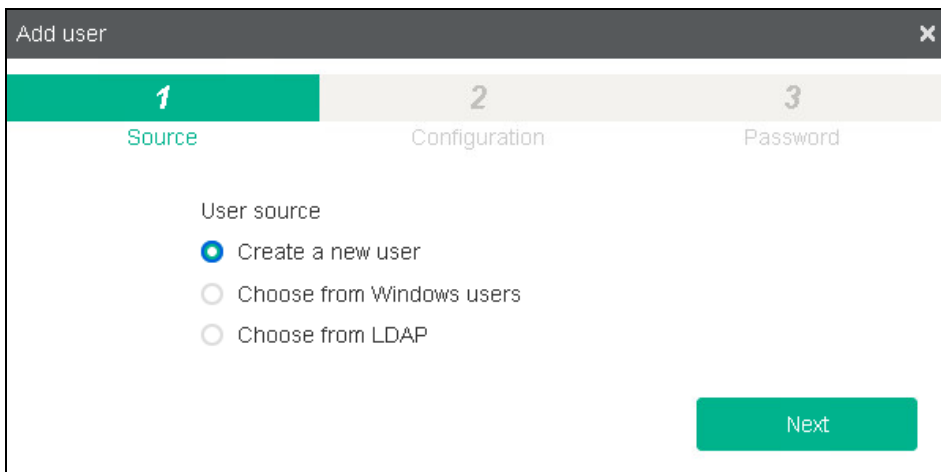
To log in to FortiClient EMS, you require a user administrator account. You will create both a super administrator and a limited access account.

To create a new FortiClient EMS administrator account

1. On the pane on the left side of the screen, click **Administration > Administrators**.
You will see an entry with the name **admin**, source **Builtin**, and role **Super Administrator**.
2. Click **Add** to create a Windows based user administrator account.
A new window opens.



3. In the **Add user** window, in the **User source** section, select **Create a new user**, and then click **Next**.



4. In the configuration window, configure the following settings:

Field	Value
User	EPadmin
Role	Endpoint Administrator

5. Click **Next**.
6. In the **Password** and **Confirm Password** fields, type `Fortinet123`.

Add user

1 Source 2 Configuration 3 Password

Password

Confirm Password

Your password must be

- ✓ At least 8 characters long

And has 3 out of the 4 following:

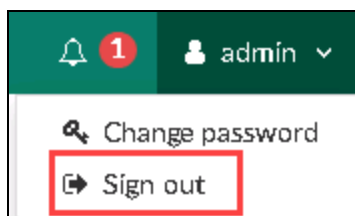
- ✓ At least one uppercase letter (A-Z)
- ✓ At least one lowercase letter (a-z)
- ✓ At least one number (0-9)
- At least one symbol (e.g. !\$#%)

Back Finish

7. Click **Finish** to create a new administrator account.

Name	Source	Role
admin	Builtin	Super Administrator
EMSadmin	Windows	Endpoint Administrator

8. Click the **admin** icon on the right side of the EMS GUI, and then select **Sign out**.



9. Log back in with the username `EPadmin` and password `Fortinet123`.
Under **Endpoint Profiles**, you will see **View Profiles** instead of **Manage Profiles**.

Stop and think!

When you log in with the username `EPadmin`, why do you see only **View Profiles** under **Endpoint Profiles**?

This user account has limited permissions and is not allowed to access endpoint profile management. The **Endpoint Administrator** role that this user account is assigned to allows only read-only permissions to the **Settings Permissions** category. This is the category that allows access to **Endpoint Profiles**.

Exercise 2: Configuring FortiClient EMS System Settings

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

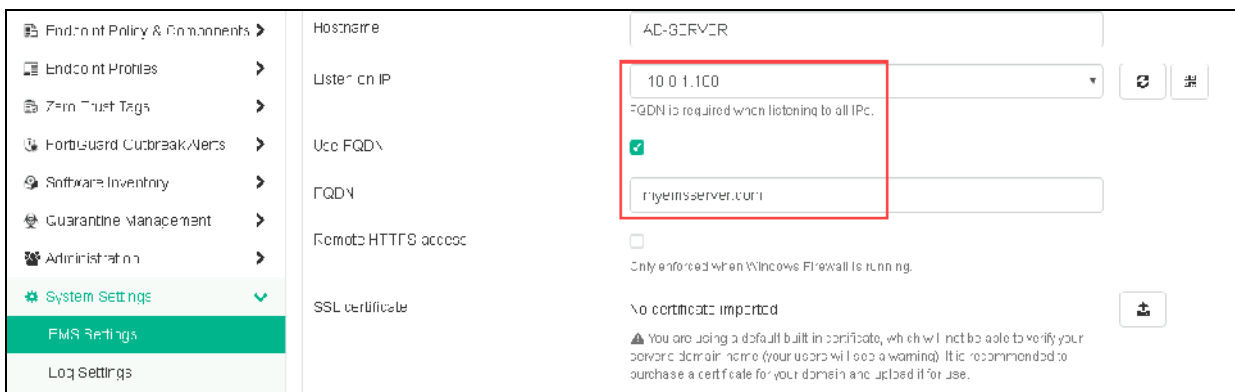
- Server settings
- Log settings
- Login banner settings

Configure Server Settings

In **EMS Settings**, you can configure settings, such as the host name, the FQDN, and remote access. You will configure the FQDN to access the FortiClient EMS server, using the configured FQDN.

To configure the FQDN on FortiClient EMS

1. On the AD Server VM, log in to the FortiClient EMS GUI with the username `admin` and password `Password123`.
2. Click **System Settings > EMS Settings**.
3. In the **Shared Settings** section, in the **Listen on IP** field, select **10.0.1.100**, select the **Use FQDN** checkbox, and then in the **FQDN** field, type `myemsserver.com`.
4. Select the **Remote HTTPS access** checkbox to enable remote access.



The screenshot shows the FortiClient EMS GUI with the following settings:

- Host name:** AD-SERVER
- Listen on IP:** 10.0.1.100 (highlighted with a red box)
- Use FQDN:** ☒ (highlighted with a red box)
- FQDN:** myemsserver.com (highlighted with a red box)
- Remote HTTPS access:** ☒
- SSL certificate:** No certificate imported

5. Click **Save** to apply the changes.
6. On the FortiClient-Laptop, open Firefox, type the URL `https://myemsserver.com`, and then accept the self-signed certificate to access the FortiClient EMS server.



The FortiClient-Laptop host file has been modified to make `myemsserver.com` accessible.

Configure Log Settings

In **Log Settings**, 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**.
2. In the **Log level** field, verify that **Info** is selected.

FortiClient Endpoint Management Server

- Dashboard
- Endpoints
- Deployment & Installers
- Endpoint Policy & Components
- Endpoint Profiles
- Zero Trust Log
- FortiGuard Outbreak Alerts
- Software Inventory
- Quarantine Management
- Administration
- System Settings**
 - EMS Settings
 - Log Settings**

Log Settings

Log cycle: Info

Automatically clear logs older than	30	days	Clear all now
Automatically clear alerts older than	70	days	Clear all now
Automatically clear events older than	70	days	Clear all now

Save

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

Date	T	Level	T	Source	T	Message	T	Occurrences
2022-09-03 13:38:17		Info		Concise		admin has logged in from 172.17.0.1	11	11 times 2022-09-03 13:38:23
2022-09-03 13:38:07		Info		Concise		admin has logged out from 172.17.0.1	11	11 times 2022-09-03 13:38:23
2022-09-03 13:32:20		Info		Jdstate Service		Get server AV/allowlist signature info (sig count=0, version=1.00300)	11	11 times 2022-09-03 13:32:22
2022-09-03 13:30:00		Info		Concise		admin changed: logs Settings	11	11 times 2022-09-03 13:30:02
2022-09-03 13:10:40		Info		Jdstate Service		Monitor service status	11	11 times 2022-09-03 13:10:42
2022-09-03 13:17:50		Info		Concise		admin has logged in from 172.17.0.1	11	11 times 2022-09-03 13:17:52
2022-09-03 13:16:54		Warning		Concise		See similar request in cloud console	11	11 times 2022-09-03 13:16:56
2022-09-03 13:16:54		Warning		Concise		See similar request in cloud console	11	11 times 2022-09-03 13:16:56
2022-09-03 13:16:18		Info		jdopkgd Service		Created: /usr/libexec/ld/ld-linux.so.2	11	11 times 2022-09-03 13:16:20
2022-09-03 13:16:34		Info		Jdstate Service		Get server AV/allowlist signature info (sig count=0, version=1.00300)	11	11 times 2022-09-03 13:16:36
2022-09-03 13:16:26		Info		Concise		admin changed: Service Settings	11	11 times 2022-09-03 13:16:28
2022-09-03 13:16:24		Info		EvS Service		Service stopped	11	11 times 2022-09-03 13:16:26
2022-09-03 13:18:00		Info		EvS Service		Tags cleared for endpoint: FortiClient-Lab-1	11	11 times 2022-09-03 13:18:02
2022-09-03 13:12:36		Info		FortiClient-Lab-1		FortiClient-Lab-1 registered	11	11 times 2022-09-03 13:12:38

Configure Login Banner Settings

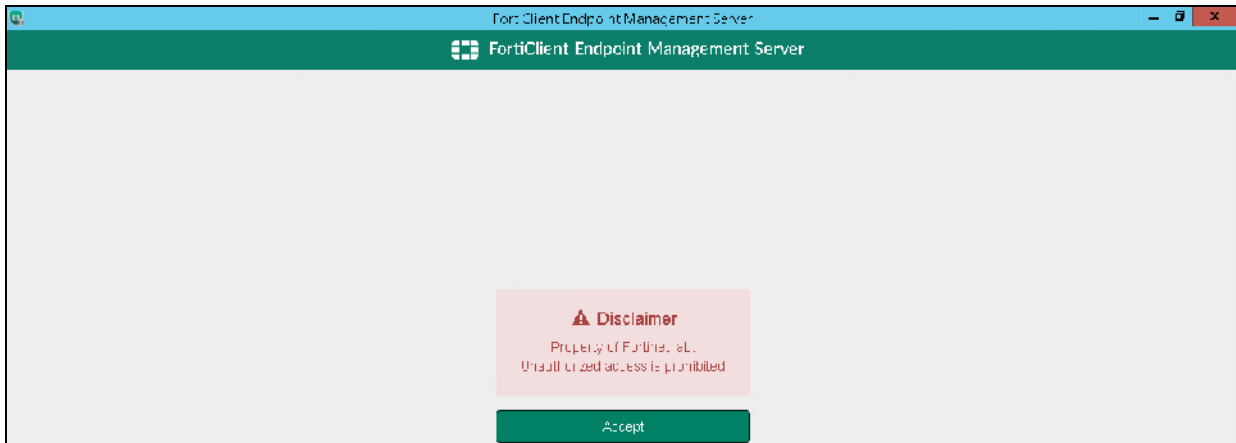
In **EMS Settings**, you will configure a disclaimer message that appears before a user logs in to FortiClient EMS.

To configure login banner settings

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

The screenshot shows the 'Configure Login Banner' settings in the FortiClient EMS GUI. The 'Enable login banner' checkbox is checked. The 'Message' field contains the text: 'Property of Fortinet lab. Unauthorized access is strictly prohibited.' The character count '69/250' is displayed at the bottom right of the message field. Below the message field is a 'Preview' section showing a red box with a warning icon and the text 'Disclaimer' followed by 'Property of Fortinet lab. Unauthorized access is strictly prohibited.'

3. Click **Save** to apply the changes.
4. Log out as **admin** from the FortiClient EMS GUI, and then close the application.
5. Open the FortiClient EMS GUI.
A **Disclaimer** appears.



6. Click **Accept** to go to the login screen.

Exercise 3: Creating an Endpoint Group and a Group Assignment Rule, and Running Scans

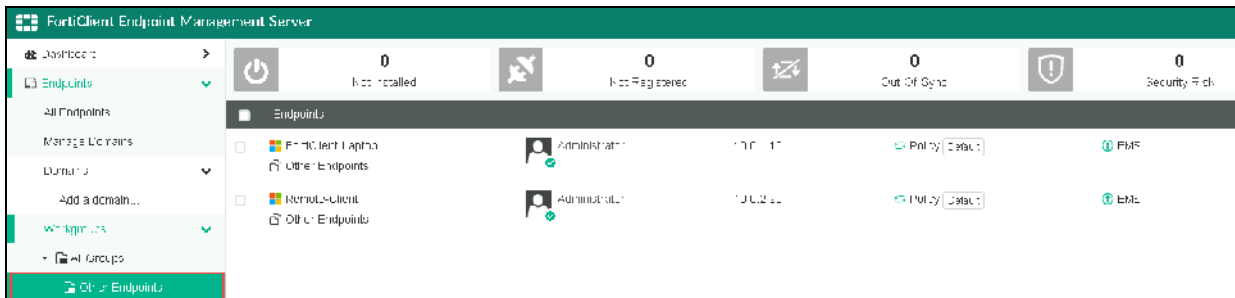
In this exercise, you will create an endpoint group and a group assignment rule, and run antivirus and vulnerability scans on endpoints. Endpoint management enables FortiClient EMS to perform various actions and run scans.

Create an Endpoint Group for a Windows Workgroup

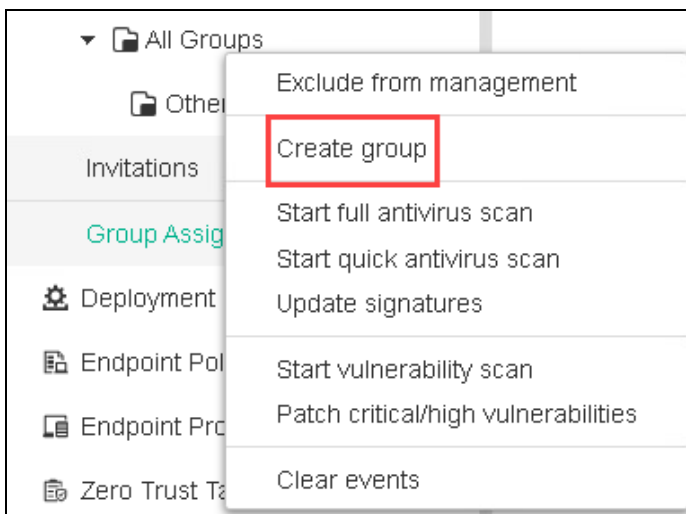
You will create individual groups for Windows workgroup endpoints on FortiClient EMS.

To create a group for a Windows workgroup

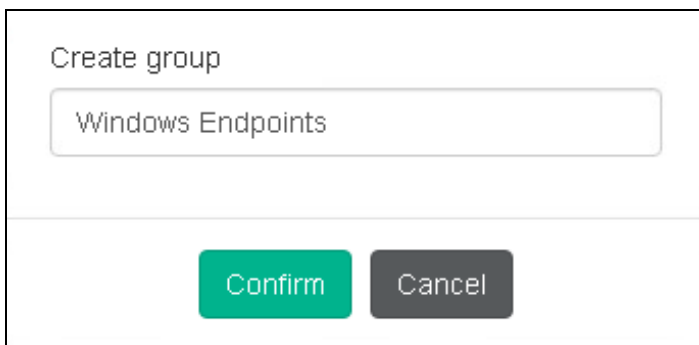
1. On the AD Server VM, open the FortiClient EMS GUI, and then click **Endpoints > Workgroups**.
By default, all the workgroup endpoints are in the **Other Endpoints** group.
2. Click **All Groups > Other Endpoints** to view the registered endpoints.



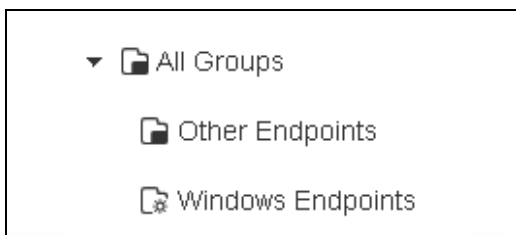
3. In the **Workgroups** drop-down list, right-click **All Groups**, and then click **Create group**.



4. In the **Create group** field, type `Windows Endpoints`.



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



Create a Group Assignment Rule for Windows Endpoints

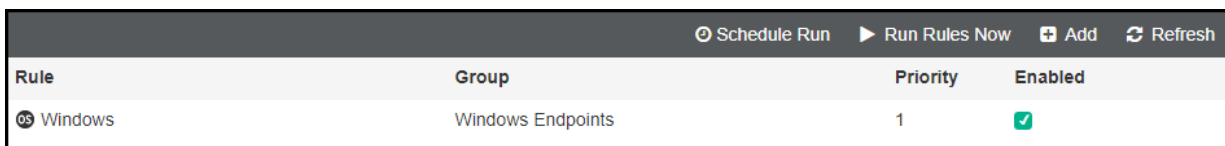
FortiClient EMS can use group assignment rules to automatically place endpoints into custom groups, based on the installer ID, IP address, OS, or AD group of the endpoints. You will create a group assignment rule based on OS.

To create a group assignment rule

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

Field	Value
Type	OS
OS	Windows (<i>W</i> must be uppercase or this will not work)
Group	Windows Endpoints
Enable Rule	(Enabled)

4. Click **Save** to add a new group assignment rule.



Schedule Run Run Rules Now Add Refresh			
Rule	Group	Priority	Enabled
Windows	Windows Endpoints	1	☒

5. On the pane on the right, click **Run Rules Now** to add Windows endpoints to the new group.



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

Run Antivirus and Vulnerability Scans on a Registered Endpoint

FortiClient EMS endpoint management can run scans on managed clients. Before you can run an AV scan, you must change the endpoint profile on FortiClient EMS.



To run scans, FortiClient, which is installed on the FortiClient-Laptop VM, must connect to FortiClient EMS. Click **ZERO TRUST TELEMETRY**, ensure that the FortiClient status is **Connected**, and then click the menu icon beside the **Disconnect** button, and ensure that it shows a FortiClient EMS IP address of 10.0.1.100.

To enable antivirus protection for the default endpoint profile

1. On the AD Server VM, open the FortiClient EMS GUI, and then click **Endpoint Profiles > Manage Profiles**.
2. Select the **Default** profile, and then click **Edit**.
3. On the **Malware** tab, enable **AntiVirus Protection**, and then leave the other settings at their default values.

The screenshot shows the FortiClient EMS Malware Protection settings for the Default profile. The 'AntiVirus Protection' toggle is turned on and highlighted with a red box. Below it, the 'General' section contains several settings: 'Block Known Communication Channels Used by Attackers' is off, 'Block Access to Malicious Websites' is on, 'Security Risk' is set to 'Low', 'Use the Exclusion List Defined in the Web Filter Profile' is on, 'Delete Malware Files After' is set to '100 Days', 'Real-Time Protection' is on, 'Action On Virus Discovery' is set to 'Quarantine Infected Files', and 'Alert When Viruses Are Detected' is on. The 'Save' button at the bottom is highlighted with a red box.

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

After the **Default** profile is synced, on the FortiClient-Laptop VM, **MALWARE PROTECTION** appears on the FortiClient GUI.

Stop and think!

Why wasn't **MALWARE PROTECTION** available on FortiClient?

The **Default** endpoint profile doesn't have the malware protection feature enabled by default. To enable AV, click the **AntiVirus Protection** button.

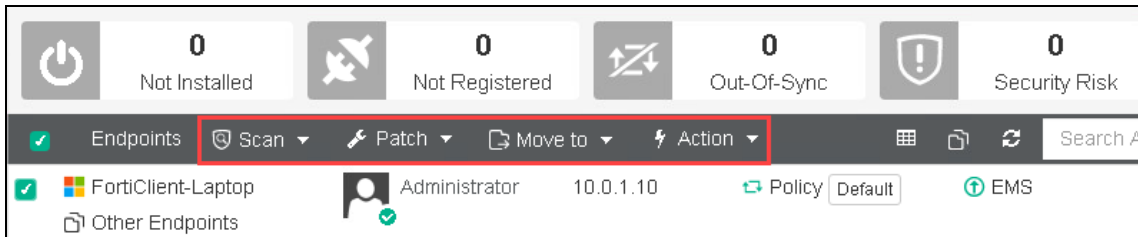
To run antivirus and vulnerability scans on a registered endpoint

1. On the AD Server VM, continuing on the FortiClient EMS, on the pane on the left, click **Endpoints > All Endpoints**.

You will see the registered client.

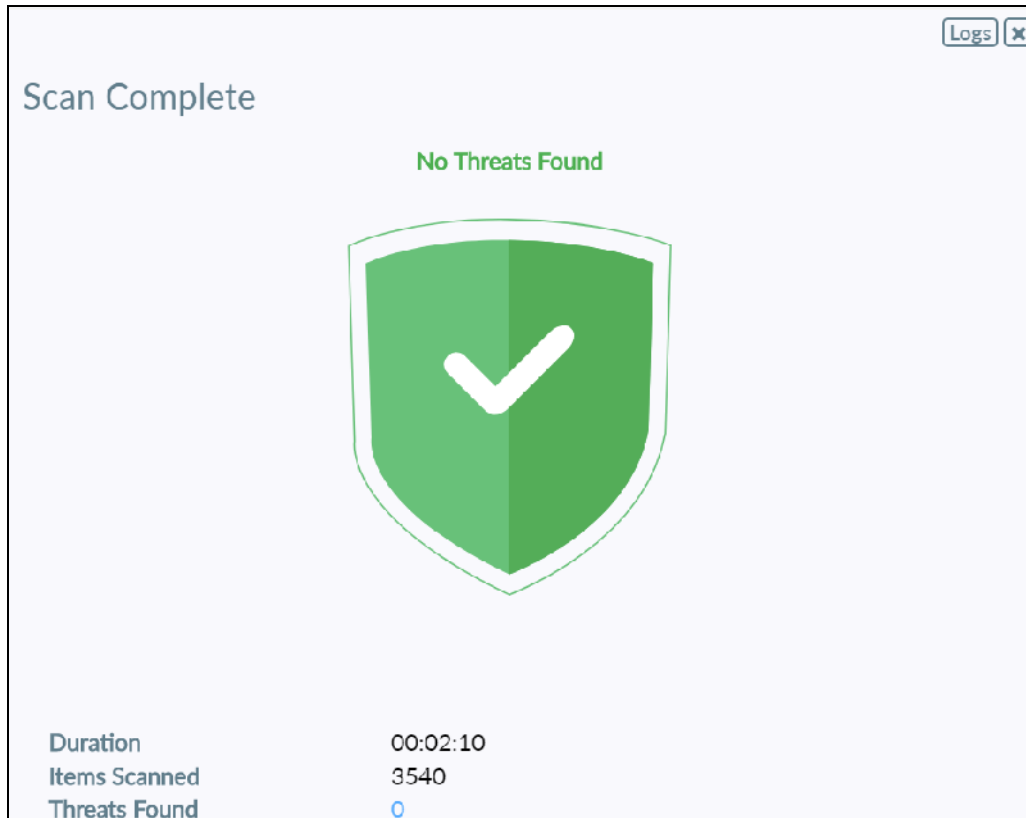
2. Beside the registered client, select the checkbox to highlight the registered client.

The following options appear: **Scan**, **Patch**, **Move to**, and **Action**.



3. Click **Scan**, and then click **Quick AV Scan**.

The scan starts after the endpoint sends the next keepalive packet.



- Click **X** to close **Scan Complete** and **FortiClient Scan Progress** windows.
- Continuing on the FortiClient EMS GUI, click **Scan > Vulnerability Scan** to perform a vulnerability scan.

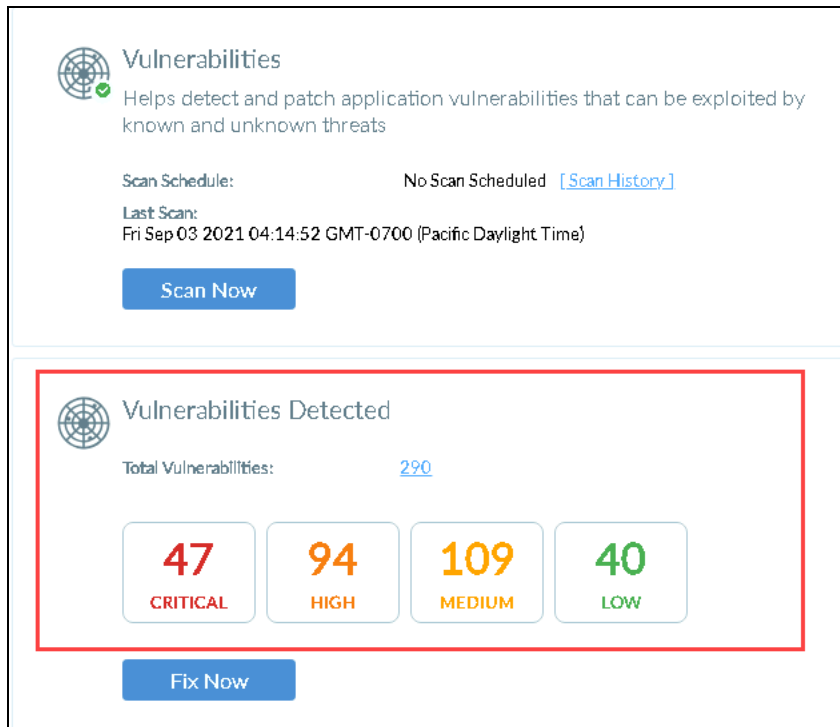


The scan starts, and it will finish after the endpoint resyncs or sends the next keepalive packet.



- Click **X** to close the scan window after the scan is finished.

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



- Click the **CRITICAL** vulnerability level box to see the details.

Install Selected

- OS (2)			
☐	OS	SEVERITY	RECOMMENDED ACTION
☐	> Windows 7,Windows Server 2008 R2,Windows 8.1,Windows Server 2012,Windows Server 2012 R2,Windows RT 8.1,Windows 10 (1)	Critical	Auto-Patch
☐	> Windows Server 2012 (3)	Critical	Auto-Patch
- Browser (0)			
☐	BROWSER	SEVERITY	RECOMMENDED ACTION
+ MS Office (0)			
- 3rd Party App (4)			
☐	APPLICATIONS	SEVERITY	RECOMMENDED ACTION
☐	> Adobe Reader X 10.0.0.396 (1)	Critical	Manual Install
☐	> Wireshark 2.4.2.0 (1)	Critical	Manual Install
☐	> Java JRE 8.0.910.14 (37)	Critical	Auto-Patch
☐	> Java JRE 8.0.1510.12 (4)	Critical	Auto-Patch

You can also click > to see more details about the applications.

Exercise 4: 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.

Verify FortiClient Log Settings

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

To verify FortiClient log settings

1. On the AD Server VM, log in to the FortiClient EMS application.
2. Click **Endpoint Profiles** > **Manage Profiles**, select **Default**, and then click **Edit**.
3. On the **System Settings** tab, in the **Log** section, ensure that **Upload Logs to FortiAnalyzer/FortiManager**, **Upload UTM Logs**, **Upload System Event**, and **Upload Security Event** are enabled.
4. Set **IP Address/Hostname** to 10.0.1.250, **Upload Schedule** to 1 minute, and **Log Generation Timeout** to 60 seconds.

Malware | Sandbox | Web Filter | Firewall | VPN | Vulnerability Scan | System Settings

☒ Client-Based Logging When On-Fabric ⓘ

☒ Upload Logs to FortiAnalyzer/FortiManager ⓘ

☒ Upload UTM Logs

☒ Upload System Event

☒ Upload Security Event

☐ Upload Vulnerability Logs ⓘ

☐ Upload Event Logs

☐ Send Software Inventory

☒ Send OS Events

Event telemetry interval: 120 seconds

IP Address/Hostname: 10.0.1.250 ⓘ

☒ SSL Enabled

Upload Schedule: 1 minutes

Log Generation Timeout: 60 seconds

Log Retention: 90 days



If you are using a browser to access FortiClient EMS, you must enable **Advanced** view settings on the FortiClient EMS **Endpoint Profiles** page.

5. Click **Save** to finish.

Enable the Security Fabric on the Root 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 root FortiGate

1. On the AD Server VM, open Firefox, type the FortiGate IP address 10.0.1.254, and log in with the username `admin` and password `password`.
2. On the FortiGate GUI, click **Security Fabric > Fabric Connectors**.
3. Select **Security Fabric Setup**, and then click **Edit**.
4. In the **Security Fabric Settings** section, click **Enabled**.

Security Fabric Settings

Status

✔ Enabled

✖ Disabled

5. Click **Serve as Fabric Root**.
A new window opens.
6. In the **FortiAnalyzer Settings** section, configure the following settings:

Field	Value
IP address	10.0.1.250
Upload option	Real Time

7. Click **Test Connectivity**.

FortiAnalyzer Settings

Status

✔ Enabled

✖ Disabled

IP address

10.0.1.250

Test Connectivity

Upload option ⓘ

Real Time

Every Minute

Every 5 Minutes

Allow access to FortiGate REST API ☒



A warning appears indicating that HQ-FortiGate isn't yet authorized on FortiAnalyzer. This authorization is configured on FortiAnalyzer in a later step.

8. Click **OK**.
9. When the **Verify FortiAnalyzer Serial Number** warning appears, click **Accept**.
10. When the FortiAnalyzer status warning appears, click **Close** because you will configure this in a later step.
11. Configure the following settings:

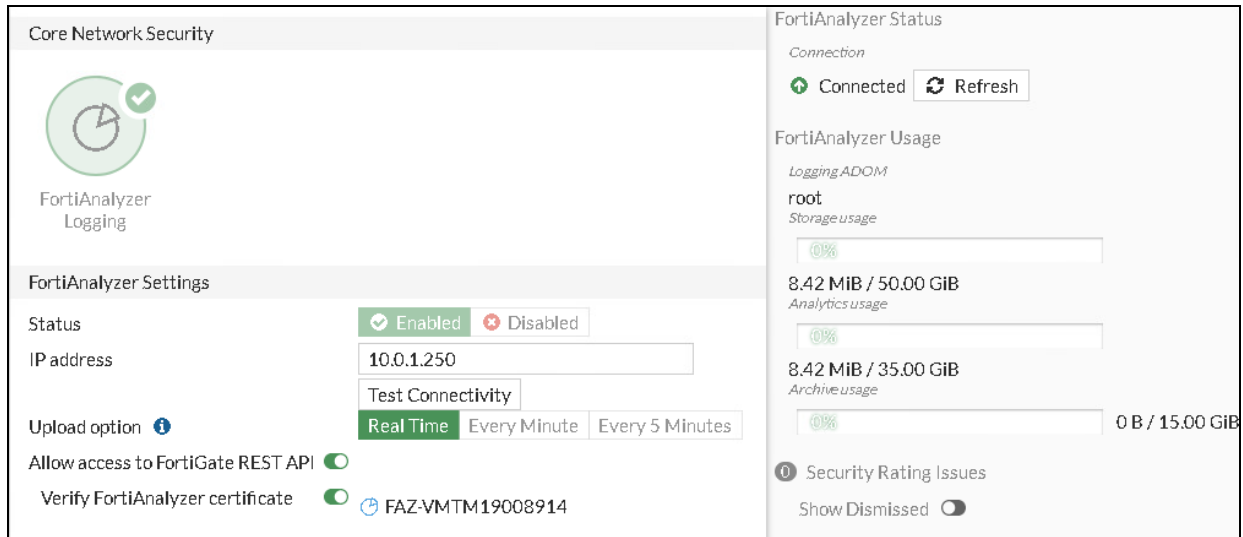
Field	Value
Fabric name	fortinet
Allow other Security Fabric devices to join	enable port3
Management port	Use Admin Port

Your configuration should look like the following example:

12. Click **OK**.
13. Click **OK** to confirm.
14. Open Firefox, type `https://10.0.1.250`, and then log in with the username `admin` and password `password` to authorize FortiGate on FortiAnalyzer.
15. Click **X** to close the FortiAnalyzer setup window.
16. In **Device Manager**, in the upper-right, click **Unauthorized Devices**.

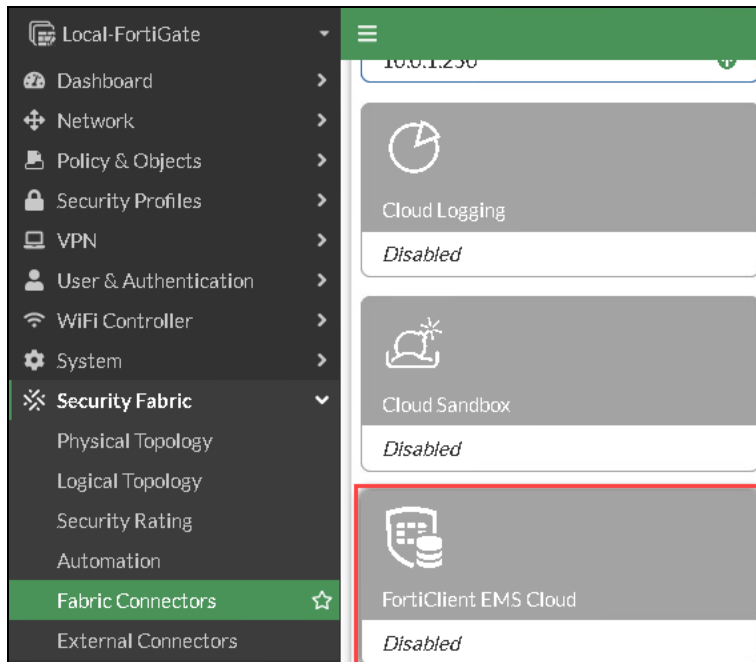
17. Select the **HQ-FortiGate** device, click **Authorize**, and then click **OK** to complete the authorization.
18. On the HQ-FortiGate GUI, click **Security Fabric > Fabric Connectors**.
19. Click **FortiAnalyzer Logging**, and then click **Edit**.

In the **FortiAnalyzer Status** section, the **Connection** status is **Connected**.



To enable the FortiClient EMS Connector

1. Continuing on the FortiGate GUI, click **Security Fabric > Fabric Connectors**.
2. In the list, select **FortiClient EMS Cloud**, and then at the top, click **Edit**.



3. In the **New Fabric Connector** window, select **FortiClient EMS**, and then configure the following settings:

Field	Value
Name	EMSServer
IP/Domain name	10.0.1.100

New Fabric Connector

Core Network Security

 FortiClient EMS

FortiClient EMS Settings

Type: **FortiClient EMS** FortiClient EMS Cloud

Name: EMSServer

IP/Domain name: 10.0.1.100

HTTPS port: 443

EMS Threat Feed  ☒

Synchronize firewall addresses  ☒

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

New Fabric Connector

Core Network Security

 FortiClient EMS

FortiClient EMS Settings

Type: **FortiClient EMS** FortiClient EMS Cloud

Name: EMSServer

IP/Domain name: 10.0.1.100

HTTPS port: 443

EMS Threat Feed  ☒

Synchronize firewall addresses  ☒

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

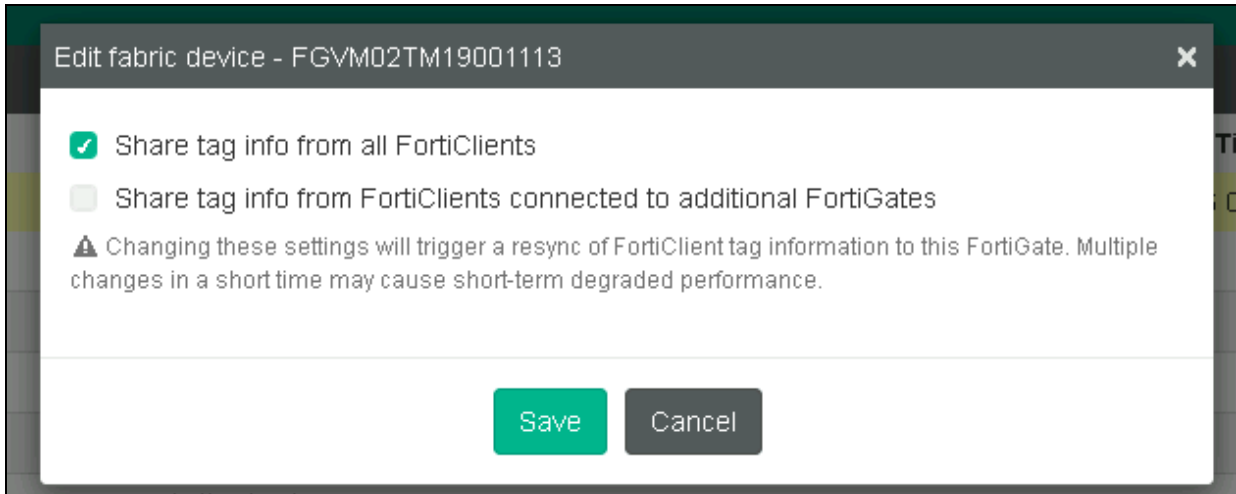
Serial Number: 63:00:15

Subject:

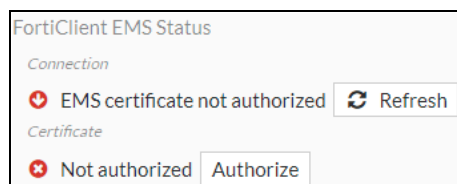
Common Name (CN)	FCTEM50000101875
Organization (O)	Fortinet
Organization Unit (OU)	FortiClient
Locality (L)	Sunnyvale
State (ST)	California
Country/Region (C)	US

Accept **Deny**

- On the FortiClient EMS GUI, click **Administration > Fabric Devices**.
- On the right side, select FortiGate, and then click **Authorize**.
- On the AD Server desktop, click PuTTY, double-click **HQ-FortiGate**, and then log in with the username `admin` and password `password`.
- Run the `execute fctems verify EMSServer` CLI command.
- On the FortiClient EMS GUI, on the **Administration > Fabric Devices** page, select FortiGate again, and then click **Edit**.
- In the edit window, select the **Share tag info from all FortiClients** checkbox, and then click **Save** to apply the changes.



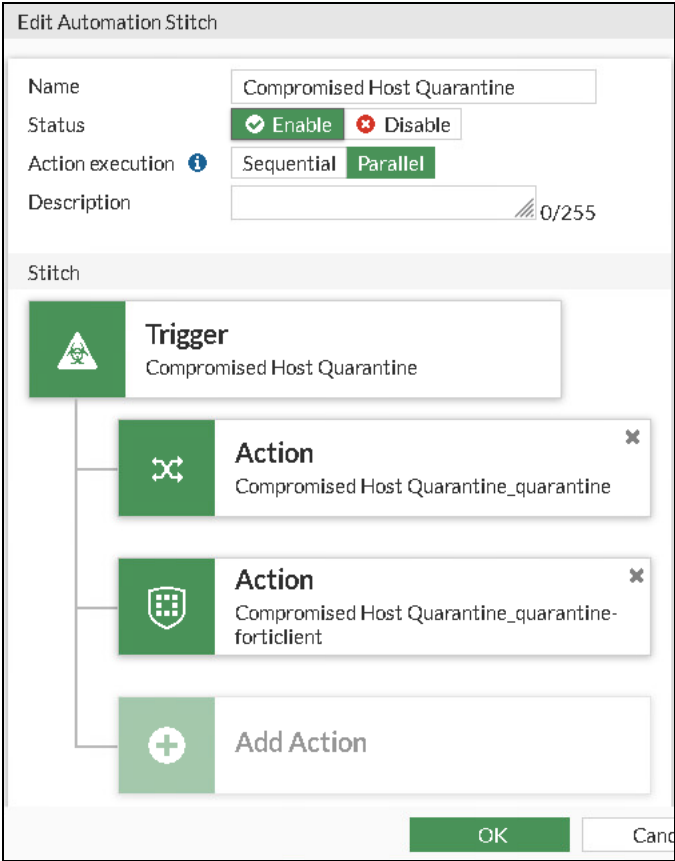
For this lab, the FortiClient EMS certificate is already trusted by FortiGate. When you configure a new connection, you must install the FortiClient EMS CA certificate on FortiGate before you authorize. Otherwise, you will see the following status:



For more information, see *FortiOS 7.0.1 Administration Guide*.

To enable Security Fabric automation and create a new stitch

- Continuing on the FortiGate GUI, click **Security Fabric > Automation**.
- Select the predefined default stitch **Compromised Host Quarantine**, and then click **Edit**.
- In the automation stitch window, select **Enable**, leave other settings as default, and then click **OK** to save the settings.



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

To configure firewall policies on FortiGate

- 1. Continuing on the HQ-FortiGate GUI, click **Policy & Objects > Firewall Policy**.
- 2. Click **Create New**, and then configure the following policy settings to allow traffic to pass from **LAN(port3)** to **port1**:

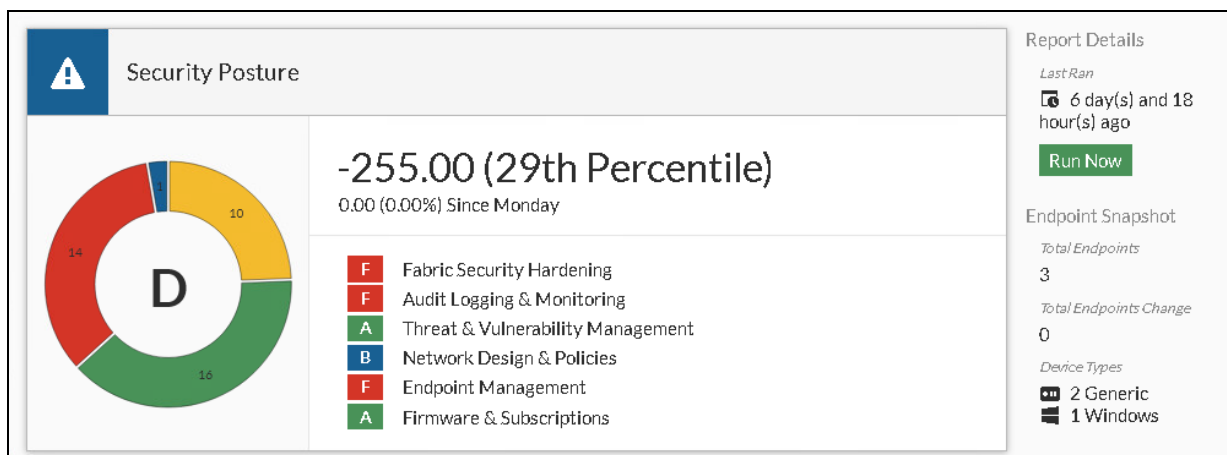
Field	Value
Name	IOC_Policy
Incoming Interface	LAN(port3)
Outgoing Interface	port1
Source	FortiClient-Laptop
Destination	all
Schedule	always
Service	ALL

Field	Value
Action	ACCEPT
Inspection Mode	Proxy-based
NAT	<enable>
IP Pool Configuration	Use Outgoing Interface Address
Web Filter	monitor-all
SSL/SSH Inspection	certificate-inspection
Log Allowed Traffic	All Sessions (greyed out)

3. Click **OK**.
4. Drag and drop the **IOC_Policy** policy above the **Full_Access** policy.

To run a security rating on FortiGate

1. Continuing on the HQ-FortiGate GUI, click **Security Fabric > Security Rating**.
2. On the **Security Posture** page, click **Run Now** to update the ranking.



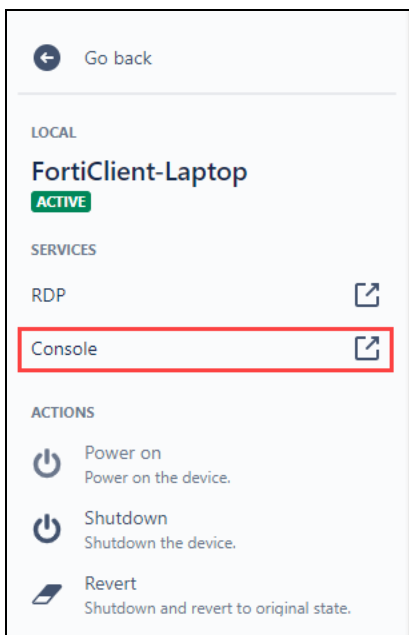
To verify the FortiAnalyzer license includes the IOC service

1. On the AD Server VM, open a browser, and then type the 10.0.1.250 IP address.
2. On the login page, enter the username `admin` and password `password`.
3. Click **System Settings**, and then in the **License Information** widget, check the status of the **FortiGuard Indicators of Compromise Service** license.

License Information			
VM License	Type	Valid	
FortiCloud	Registered		
FortiGuard	Indicators of C...	Licensed (Expires 2021-10-31)	
		Servers located in US only	
Security	SOC Service		
Operations			
Logging	Devices/VDOMs	2 of 10,000 (0	
	GB/Day	0.0 of 1 (0.0%	
	VM Storage	50.00 GB of 5	
Storage	Cloud	No License	
Connector			
Service			
Update	AntiVirus and I...	208.184.237.66 (San Jose, Calif...	
Server	FortiClient Up...	208.184.237.75 (San Jose, Calif...	

To test automatic quarantine triggered by IOC detection

1. In the lab menu, on the FortiClient-Laptop VM, click **Console** access method under **Services** to access FortiClient-Laptop using console.



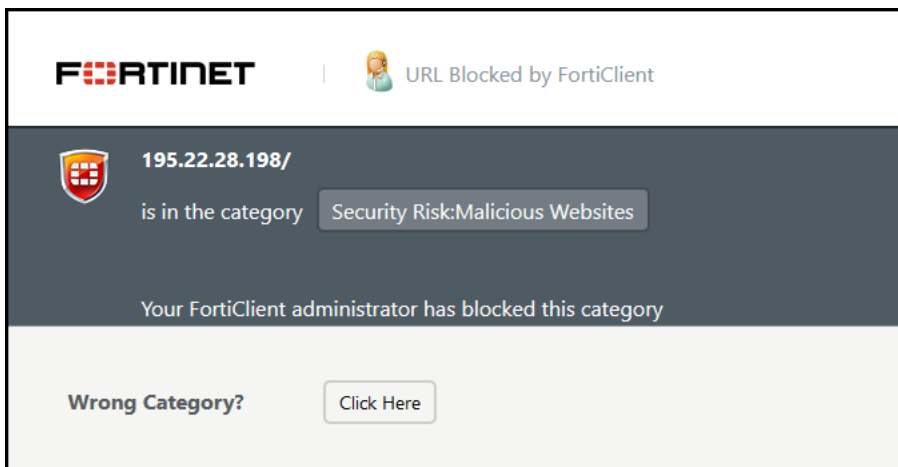
Reason for using console access is that when FortiClient is quarantined, you may not be able to access FortiClient-Laptop using RDP.



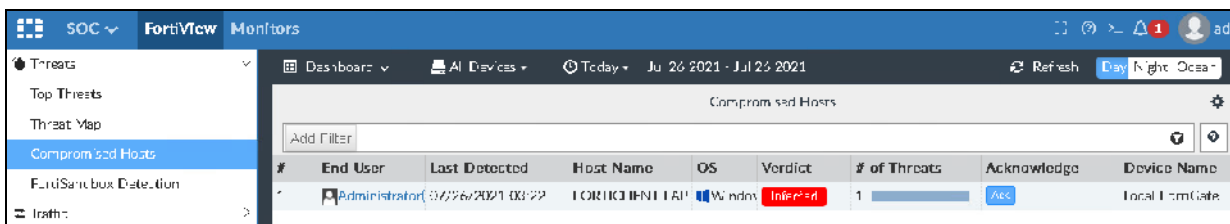
If lab menu shows any other VM, then use the **Go back** option in the lab menu to return to the lists of VMs and then select **FortiClient-Laptop** from the list.

2. Click the **Ctrl+Alt+Delete** button on the upper-right corner, so you can enter a password.
3. Enter the password `password` to log in to Windows using the console connection.
4. On the FortiClient-Laptop VM, open Firefox, and then type the URL `www.google.com`.
5. Open a new browser tab, and then type `http://195.22.28.198`.

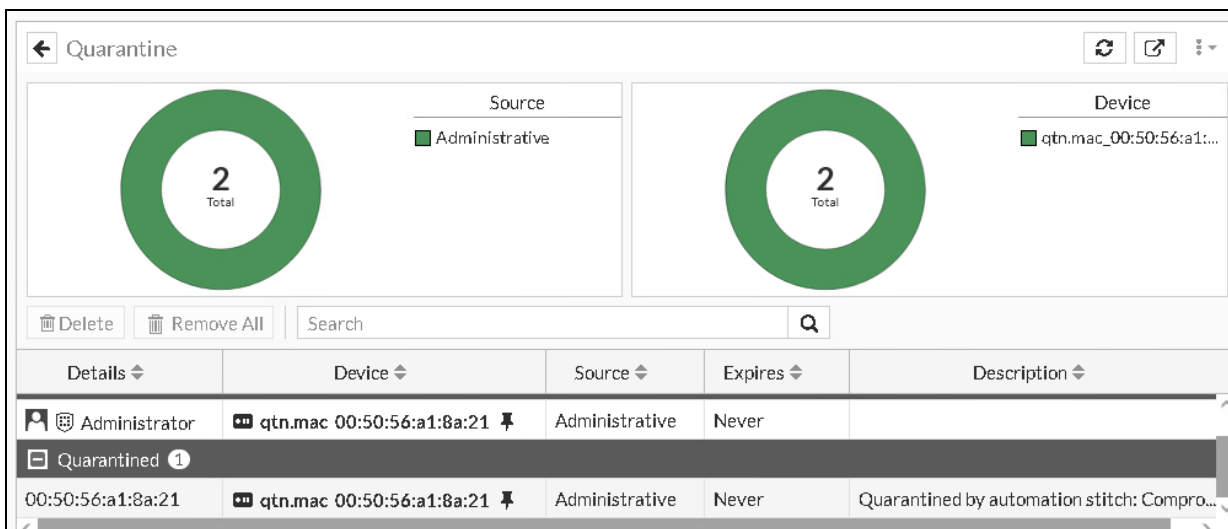
This IP address is blocked by the FortiClient malicious websites category.



6. Continuing on the AD Server VM, on the FortiAnalyzer GUI, click **SOC > FortiView > Compromised Hosts**. The endpoint appears in the window.
7. Double-click the host to see details.

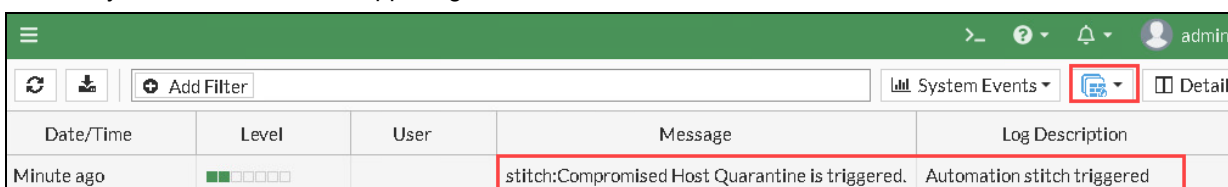


8. Continuing on the FortiClient-Laptop VM, log in to the FortiGate GUI.
9. Click **Dashboard > Users & Devices**, and then scroll down and click the **Quarantine** widget to view it. You will see that the endpoint has been quarantined.

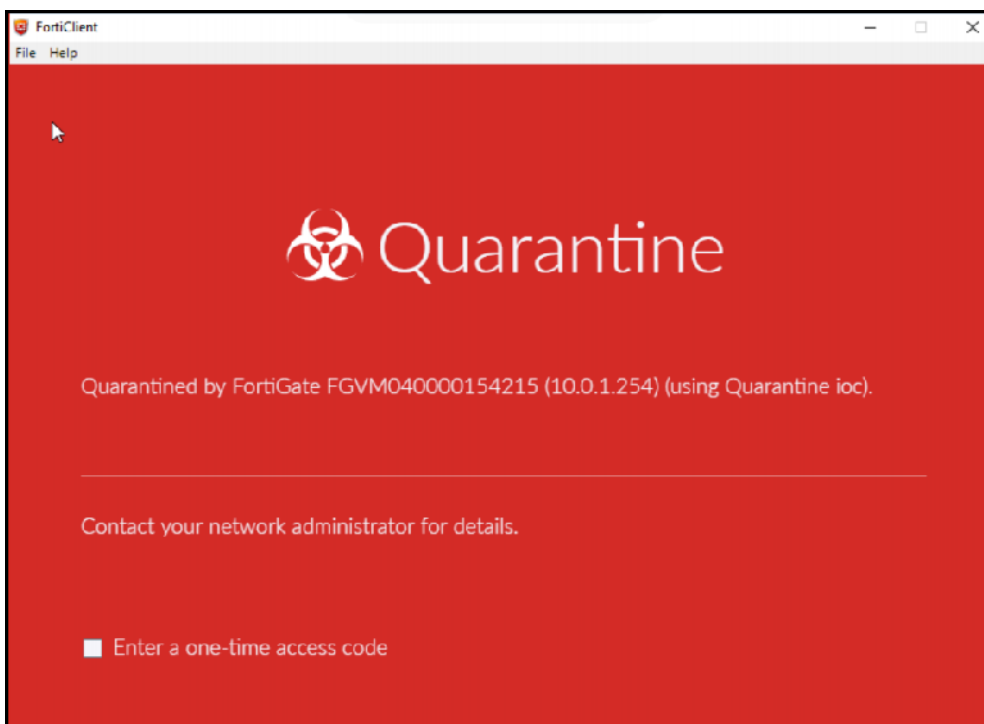


The result on your FortiGate may not match the lab example above.

10. Click **Log & Report > Events > System Events** to view the logs. You may need to change log source from FortiAnalyzer to local disk in the upper-right corner.



11. FortiClient will show the quarantine screen. FortiClient is blocking all communication, except to the EMS.

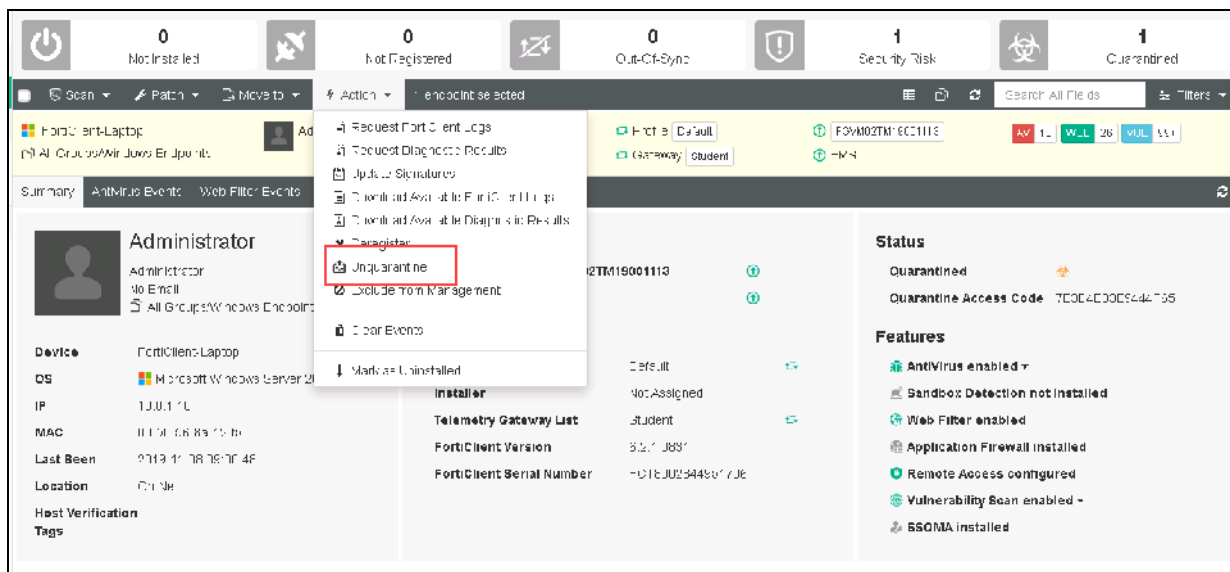


The endpoint is blocked at the client network device level.



To remove the client from the compromised hosts list, on the FortiAnalyzer GUI, click **SOC > FortiView**. To clear the host, click **Threats > Compromised Hosts**, click **ACK** to acknowledge the host, and then write some text. This will also clear the host from FortiGate.

12. On the AD Server VM, log in to the FortiClient EMS GUI, and then select **Endpoints > All Endpoints**.
13. In the right pane, select FortiClient-Laptop, click **Action**, and then click **Unquarantine** to allow internet access to the endpoint.



14. Return to the FortiClient-Laptop VM.
15. Try to ping FortiGate, the EMS server, and google.com.
Your traffic should now be allowed.

Lab 4: FortiClient Deployment Using FortiClient EMS

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

Objectives

- Create a FortiClient installer
- Add endpoints to FortiClient EMS from Windows AD
- Create and manage a deployment package

Time to Complete

Estimated: 20 minutes

Prerequisites

Before beginning this lab, you must finish the previous lab.

Exercise 1: Creating an Installer for Deployment

In this exercise, you will create an installer for endpoint deployment.

Create a FortiClient Installer for Deployment

You will create an installer for deploying FortiClient on endpoints.

To create an installer

1. On the AD Server VM, log in to the FortiClient EMS GUI.
2. In the pane on the left, click **Deployment & Installers > FortiClient Installer**, and then click **+Add** to open a new window.
3. In the **Version** tab, keep the default settings for **Installer Type** and **Release**, in the **Patch** field, select 7.0.1, and then click **Next**.

Add Deployment Package

1 Version 2 General 3 Features 4 Advanced 5 Telemetry

Installer Type

☒ Choose an official release

☐ Choose a custom installer

Release

7.0

Patch

7.0.1

☐ Keep updated to the latest patch

Next

4. In the **General** tab, in the **Name** field, type `FortiClient-Version-7.0`, and then click **Next**.
5. In the **Features** tab, under **Basic Security Features**, select the **Secure Access Architecture Components** and **Vulnerability Scan** checkboxes, and then under **Additional Security Features**, select the **Malware, Web Filtering**, and **Application Firewall** checkboxes.

The screenshot shows the 'Add Deployment Package' dialog box with the 'Features' tab selected. The dialog has five tabs: 1 Version, 2 General, 3 Features, 4 Advanced, and 5 Telemetry. The 'Features' tab is active, showing a list of security features with checkboxes. The 'Next' button is highlighted in green.

Add Deployment Package

1 Version 2 General **3 Features** 4 Advanced 5 Telemetry

Basic Security Features

- ☒ Zero Trust Telemetry
Fabric Telemetry
- ☒ Secure Access Architecture Components
SSL and IPSec VPN
- ☒ Vulnerability Scan
Host vulnerability scanning
- ☐ Advanced Persistent Threat (APT) Components
FortiSandbox detection and quarantine features

Additional Security Features

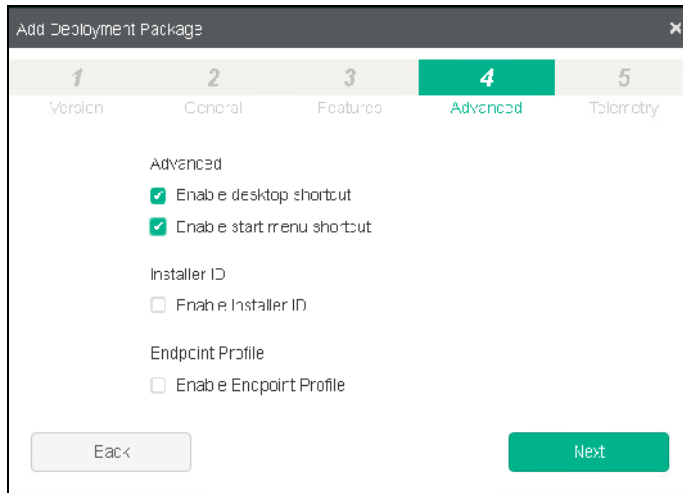
- ☒ Malware
 - ☒ AntiVirus, Anti-Exploit, Removable Media Access
Provides real-time protection against a variety of threats
 - ☒ Anti-Ransomware 
Monitors and blocks file system activities being exhibited by ransomware exploits.
 - ☒ Cloud Based Malware Outbreak Detection
Protects endpoints from high risk file types from Internet, network drives, etc.
- ☒ Web Filtering
Provides defense against web-based attacks
- ☒ Application Firewall
Inspect intrusions attempting to exploit known vulnerabilities
- ☐ Single Sign-On Mobility Agent
Provides FortiAuthenticator for transparent authentication

*  Windows-only features

Back Next

6. Click **Next**.

7. In the **Advanced** tab, select the **Enable desktop shortcut** and **Enable start menu shortcut** checkboxes, and then keep the default values for the other settings.



8. Click **Next**.
9. In the **Telemetry** tab, notice that it shows that FortiClient will be managed by *<EMS hostname and FQDN address>*.
10. Click **Finish** to add the deployment package to FortiClient EMS.
The installer appears on the **Deployment & Installers > FortiClient Installer** pane.



FortiClient EMS automatically connects to the FortiGuard Distribution Network (FDN) to provide access to the FortiClient installers, which you can use with FortiClient EMS deployment packages. If a connection to FDN is not available, or you want a custom installer, you must manually download a FortiClient installer, and then upload it to add it to FortiClient EMS.

Exercise 2: Adding Endpoints to FortiClient EMS

In this exercise, you will add AD endpoints to the EMS server.

Add Endpoints Using an AD Domain Server

You will manually import endpoints from an AD 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 endpoints using an AD domain server

1. On the AD Server VM, log in to the FortiClient EMS GUI.
2. In the pane on the left, click **Endpoints > Manage Domains**, and then click **+Add** to open the **Domain** window.
3. In the **IP address/Hostname** field, type `10.0.1.100`, and then keep the default values for **Port** and **Distinguished name**.
4. In the **Bind type** section, select **Regular**, and then configure the following settings:

Field	Value
Username	ADadmin
Password	password

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

The screenshot shows the 'Domain' configuration window in FortiClient EMS. At the top, a green bar indicates 'Success'. Below this, the 'Domain' title is followed by a list of configuration fields: 'IP address/Hostname' (10.0.1.100), 'Port' (389), 'Distinguished name' (Optional), 'Bind type' (with 'Simple', 'Anonymous', and 'Regular' buttons, where 'Regular' is selected), 'Username' (ADadmin), and 'Password' (masked with dots and an eye icon).

6. Perform one of the following tasks:
 - If the test is successful, select **Save** to save the new domain.
 - If the test is not successful, correct the information, and then test the settings again.

Domain	
IP address/Hostname	10.0.1.100
Port	389
Distinguished name	DC=trainingAD,DC=training,DC=lab



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 back to the AD server.

Exercise 3: Creating a Deployment Package to Install FortiClient

In this exercise, you will create a deployment package to install FortiClient on AD endpoints.

Create a Deployment Package to Install FortiClient

You must add a FortiClient installer to the FortiClient EMS deployment package to install FortiClient. You will select the installer that you created in exercise 1.

To create a profile to deploy FortiClient

1. On the FortiClient EMS GUI, click **Deployment & Installers > Manage Deployment**.
2. Click **+Add** to open a new profile window.
3. In the **Name** field, type **AD-Deployment**.
4. In the **Endpoint Groups** field, click **Edit**, and then select **trainingAD.training.lab**.
5. Ensure that the **Action** field is set to **Install**.
6. In the **Deployment Package** field, select **FortiClient-Version-7.0**.

Deployment

Name

AD-Deployment

Endpoint Groups

trainingAD.training.lab

Edit

Action

Install

Uninstall

Deployment Package

FortiClient-Version-7.0

Name	FortiClient-Version-7.0
Versions	Windows 7.0.0, Mac 7.0.0
Auto Update	Disabled
Managed by EMS	0.0.0.0:8013
Auto Registration	Enabled
Desktop Shortcut	Enabled
Start Menu Shortcut	Enabled

7. Enable **Start at a Scheduled Time**, and then specify the installation start time, which should be five minutes from the current time.
8. Disable **Reboot when no users are logged in**, and then keep the default values for all other settings.
9. In the **Username** field, type `Administrator`, and then in the **Password** field, type `password`.
10. Enable **Enable the Deployment**.
11. Click **Save**.

The deployment package appears on the **Deployment & Installers > Manage Deployment** page.

FortiClient Endpoint Management Server

Invitations

admin

Dashboard

Endpoints

Deployment & Installers

Manage Deployment

FortiClient installer

Deployments

Name

Assigned Groups

Deployment Package

Scheduled Upgrade Time

Priority

Enabled

AL-Deployment

trainingAD.training lab

FortiClient-Vers on-7.0

12.23



This deployment installs FortiClient on the AD Server VM. After this exercise, wait until FortiClient installs, updates signatures, and then connects to the EMS server.

Lab 5: FortiClient Provisioning Using FortiClient EMS

In this lab, you will learn about using FortiClient EMS to provision FortiClient on endpoints.

Objectives

- Create an endpoint profile
- Enable the web filter and antivirus features
- Configure a VPN tunnel
- Create a policy to assign a new endpoint profile to an AD domain or workgroup endpoints

Time to Complete

Estimated: 35 minutes

Prerequisites

Before beginning this lab, you must finish the previous lab.

Exercise 1: Creating and Assigning an Endpoint Profile for Deployment

In this exercise, you will create an endpoint profile and assign the profile to endpoints. You will also configure a security profile and provision a VPN. After you complete provisioning, the configuration is pushed to FortiClient endpoints by FortiClient EMS.

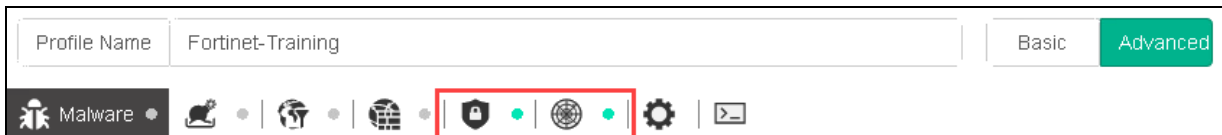
Create an Endpoint Profile on FortiClient EMS

To push the configuration to FortiClient endpoints, you must create an endpoint profile. The endpoint profile has profile references that enable and disable FortiClient features and deployment.

To create an endpoint profile on FortiClient EMS

1. On the FortiClient EMS GUI, click **Endpoint Profiles > Manage Profiles**.
2. Click **Add** to open a new profile window.
3. In the **Profile Name** field, type `Fortinet-Training`.
4. Click **VPN** and **Vulnerability Scan**.

These settings are enabled by default.



5. Click **Save** to save the endpoint profile.

Create a Profile to Deploy FortiClient

You must add a FortiClient installer to the FortiClient EMS before you can select an endpoint profile. You will select the installer that you created in *Lab 4—Exercise 1*.

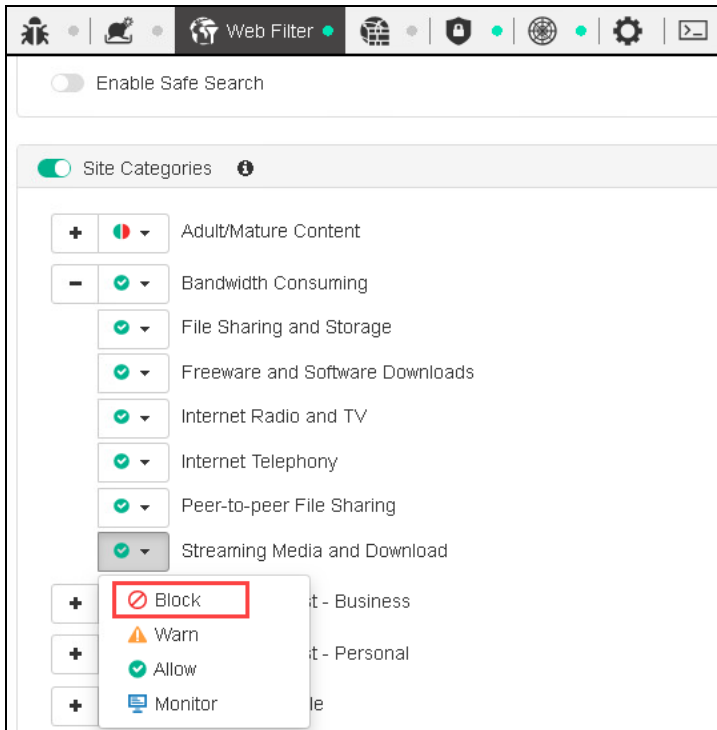
Enable the Web Filter Feature in the Endpoint Profile

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

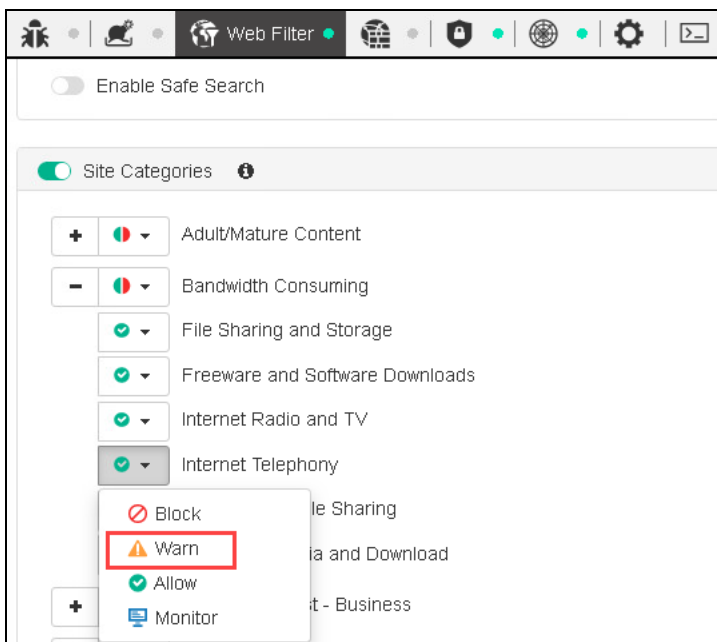
To enable the web filter feature in the endpoint profile

1. Continuing on the FortiClient EMS GUI, click **Endpoint Profiles > Manage Profiles**, select **Fortinet-Training**, and then click **Edit**.

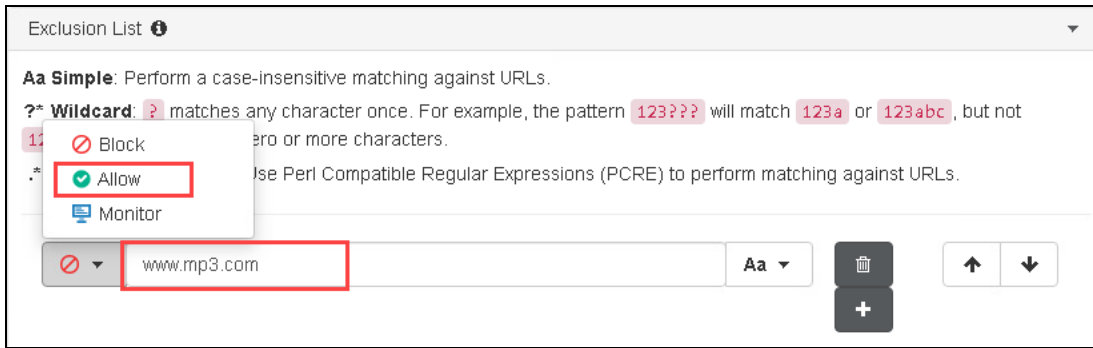
2. On the **Web Filter** tab, in the **General** section, enable **Web Filter**, and then keep **Enable WebFiltering on FortiClient** set to **Always On**.
3. In the **Site Categories** section, beside **Bandwidth Consuming**, click **+** to expand the list.
4. In the list, beside **Streaming Media and Download**, select **Block**.



5. In the list, beside **Internet Telephony**, select **Warn**.



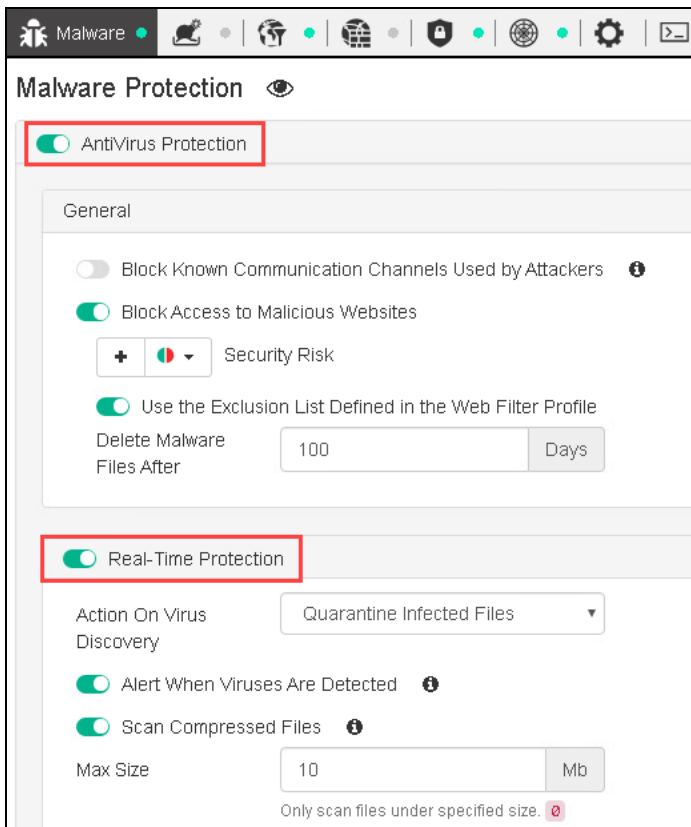
6. In the **Exclusion List** section, change the action to **Allow**, type `www.mp3.com`, and then leave the other settings at the default values.



7. Click **Save**.

To enable the antivirus feature in the endpoint profile

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



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

Provision a VPN in the Endpoint Profile

You will provision the VPN settings. The VPN profile is applied to FortiClient when the profile installs on the endpoint.

To provision a VPN in the endpoint profile

1. On the **VPN** tab, enable **VPN**, and then disable all options except **Minimize FortiClient Console on Connect** in the **General** section.
2. On the **SSL VPN** tab, configure the following settings:

The screenshot shows the 'SSL VPN' configuration tab. It includes a toggle for 'SSL VPN' which is turned on. Below it, there is a 'DNS Cache Service Control' section with a dropdown menu set to 'Disable dnscache serv'. At the bottom, there is a 'Prefer SSL VPN DNS' toggle which is also turned on.

3. On the **VPN Tunnels** tab, click **Add Tunnel**, keep the VPN type set to **Manual** (default selection), and then click **Next**.
4. In the next window, configure the following settings:

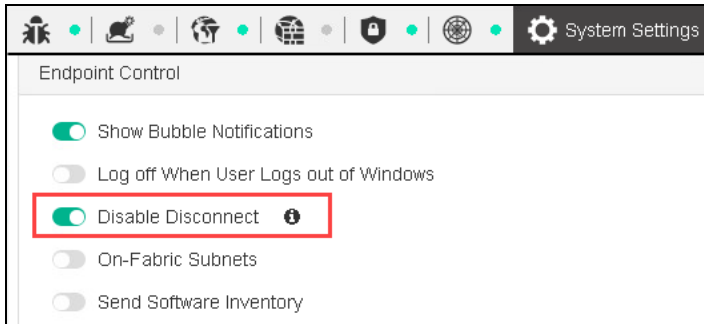
Field	Value
Name	Student-SSL VPN
Type	SSL VPN
Remote Gateway	10.0.1.254
Port	10443
Prompt for Username	(Enable)

The screenshot shows the 'Creating VPN Tunnel' dialog box. It has a 'Basic Settings' tab selected. The 'Split Tunnel' section is expanded, showing 'Application Based' selected. The 'Advanced Settings' section is also expanded, showing 'On Connect Script' and 'On Disconnect Script'. The 'Name' field is set to 'STUDENT SSL VPN'. The 'Type' is set to 'SSL VPN'. The 'Remote Gateway' is set to '10.0.1.254'. The 'Port' is set to '10443'. The 'Require Certificate' toggle is turned off, and the 'Prompt for Username' toggle is turned on. At the bottom, there are 'Add Tunnel' and 'Cancel' buttons.

5. Click **Add Tunnel** to save the VPN profile.
6. Click **Save**.

To disable disconnect from the EMS

1. Click the **System Settings** tab.
2. In the **Endpoint Control** section, enable **Disable Disconnect**.



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

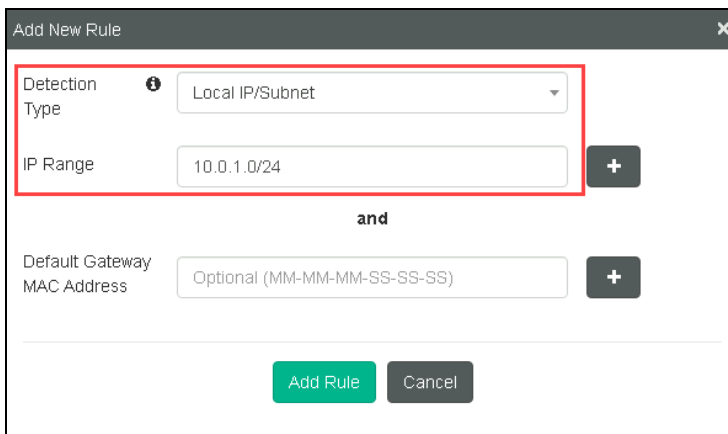
Create an Endpoint Policy to Assign the Endpoint Profile

After creating the profile, you must create an endpoint policy to assign the profile to domains or workgroups. When you create an endpoint policy to assign the profile to domains or workgroups, the profile settings are automatically pushed to the endpoints in the domain or workgroup.

If you do not assign a profile to a specific domain or workgroup, the default profile is automatically applied to the domain or workgroup.

To create an endpoint policy

1. On the FortiClient EMS GUI, click **Endpoint Policy & Components > On-fabric Detection Rules > Add**.
2. In the **On-Fabric Rule Set** window, in the **Name** field, type **On-Fabric**.
3. In the **Rule** section, click **Add Rule**.
4. In the **Add New Rule** window, select **Detection Type** as **Local IP/Subnet** and type **10.0.1.0/24** in the **IP Range** field.



5. Click **Add Rule**, and then click **Save** to add the on-fabric detection rule.

On-Fabric Rule Set

Name

On-Fabric

Enabled

☒

Comments

Optional

Rules

+ Add Rule

Rule Type	Criteria
Local IP/Subnet	☐ IF 10.0.0.0/24

6. On the **Endpoint Policy & Components** menu, select **Manage Policies > Add**.
7. In the **Endpoint Policy** window, in the **Endpoint Policy Name** field, type **Training**.
8. In the **Endpoint Groups** field, click **Edit**, select **trainingAD.training.lab** and **All Groups**, and then click **Save**.
9. In the **Profile** field, select **Fortinet-Training** in the profiles list.
10. In the **Profile (Off-Fabric)** field, select **Default** in the profiles list.
- This profile applies when the endpoint is off-fabric. You cannot select the same endpoint profile for the on-fabric and off-fabric status.
11. In the **On-Fabric Detection Rules** field, select **On-Fabric** in the drop-down list.
12. Ensure that **Enable the Policy** is enabled.
13. Keep the other settings at the default values, and then click **Save** to add the endpoint policy.

The endpoint policy should have the following settings:

Endpoint Policy

Endpoint Policy Name

Training

Endpoint Groups

All Groups... trainingAD.training.lab...

Edit

Users

Optional

Profile

Fortinet-Training

Profile (Off-Fabric)

Default

On-Fabric Detection Rules

☒ On-Fabric

Comments

Optional

Enable the Policy

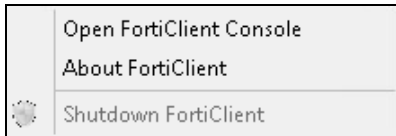
☒

Save

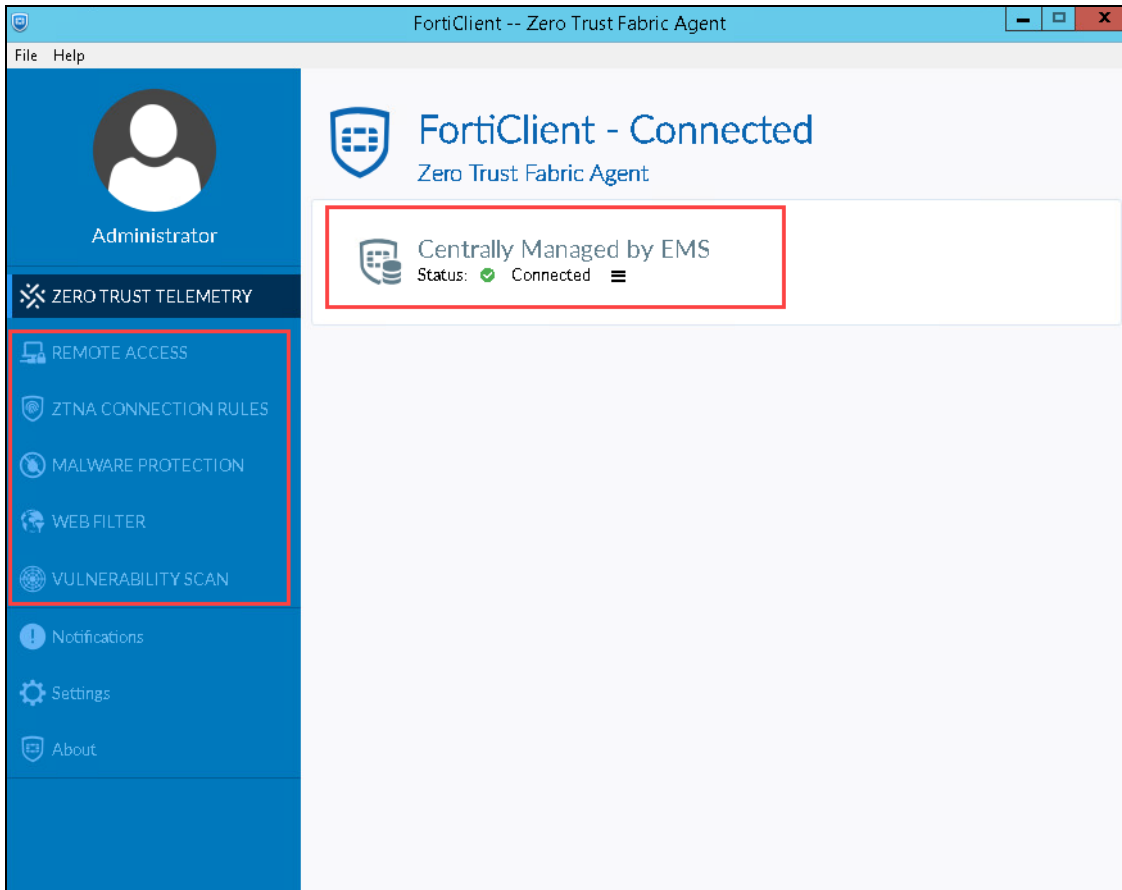
Cancel

The endpoint profile is assigned to the endpoint policy. After FortiClient is deployed on the endpoints and the endpoints are connected to FortiClient EMS, you can update the endpoints by editing the associated profiles.

14. On the FortiClient-Laptop VM, in the system tray, right-click the FortiClient icon.
15. Click **Open FortiClient Console** to show the VPN profile.



16. Verify that FortiClient is connected to EMS and all configurations are enabled on the endpoint.



Exercise 2: Testing the FortiGuard Web Filter

In this exercise, you will test the configuration (WF profile) that you defined in the previous exercise. You will examine the FortiClient web filter, based on FortiGuard categories, by making sure that FortiClient can contact the FortiGuard servers.

Then, you will review a category-based web filter security profile on FortiClient and inspect the HTTP traffic.

Finally, you will test different actions taken by FortiClient, according to website categories that you configured in the previous exercise.

Verify FortiGuard Connectivity

You will verify connectivity to FortiGuard Distribution Servers (FDS) from the FortiClient host machine. 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 FortiClient-Laptop VM, open the CLI, and then ping `fgd1.fortigate.com`.
If FortiClient can contact FortiGuard, you should see the following output:

```
C:\Users\Administrator>ping fgd1.fortigate.com

Pinging guard.fortinet.net [173.243.138.194] with 32 bytes of data:
Reply from 173.243.138.194: bytes=32 time=58ms TTL=48
Reply from 173.243.138.194: bytes=32 time=55ms TTL=48
Reply from 173.243.138.194: bytes=32 time=55ms TTL=48
Reply from 173.243.138.194: bytes=32 time=55ms TTL=48

Ping statistics for 173.243.138.194:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 55ms, Maximum = 58ms, Average = 55ms
```

Identify Web Filter Categories

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

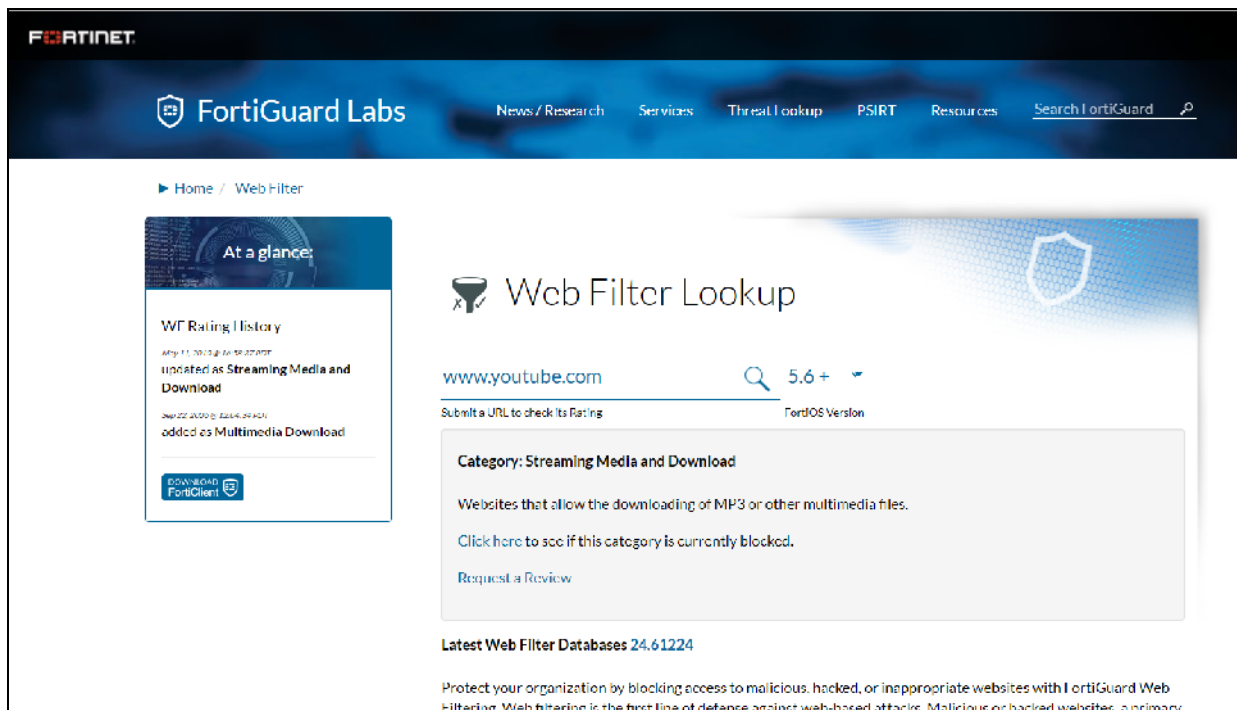
To identify web filter categories

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



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

www.youtube.com



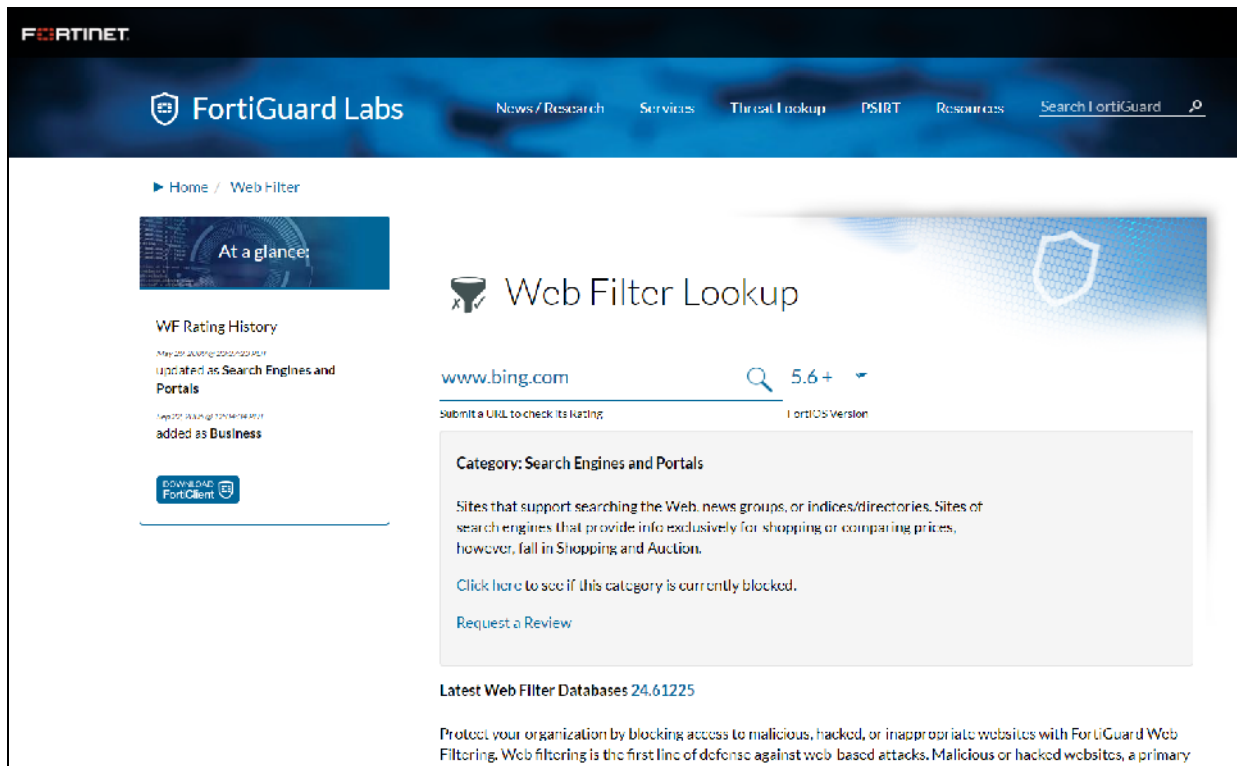
YouTube is listed in the **Streaming Media and Download** category.

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

- www.viber.com
- www.ask.com
- www.bing.com

The screenshot shows the FortiGuard Labs Web Filter Lookup interface. The page title is "Web Filter Lookup". The URL entered is "www.viber.com". The rating is "5.6+". The category is "Internet Telephony". The description states: "Websites that enable telephone communications over the Internet." There is a link to "Click here to see if this category is currently blocked." and a link to "Request a Review". The latest web filter databases are listed as 24.61223. A "Download FortiClient" button is visible in the bottom left corner.

The screenshot shows the FortiGuard Labs Web Filter Lookup interface. The page title is "Web Filter Lookup". The URL entered is "www.ask.com". The rating is "5.6+". The category is "Search Engines and Portals". The description states: "Sites that support searching the Web, news groups, or indices/directories. Sites of search engines that provide info exclusively for shopping or comparing prices, however, fall in Shopping and Auction." There is a link to "Click here to see if this category is currently blocked." and a link to "Request a Review". The latest web filter databases are listed as 24.61224. A "Download FortiClient" button is visible in the bottom left corner.



You will also test your web filter using these websites.

The following table shows the category assigned to each URL, as well as the action to take, which is configured on FortiClient based on your web filter settings:

Website	Category	Action
www.dailymotion.com	Streaming Media and Download	Block
www.viber.com	Internet Telephony	Warning
www.bing.com	Search Engines and Portals	Allow
www.mp3.com	Streaming Media and Download	Block

Review a FortiGuard Category-Based Web Filter

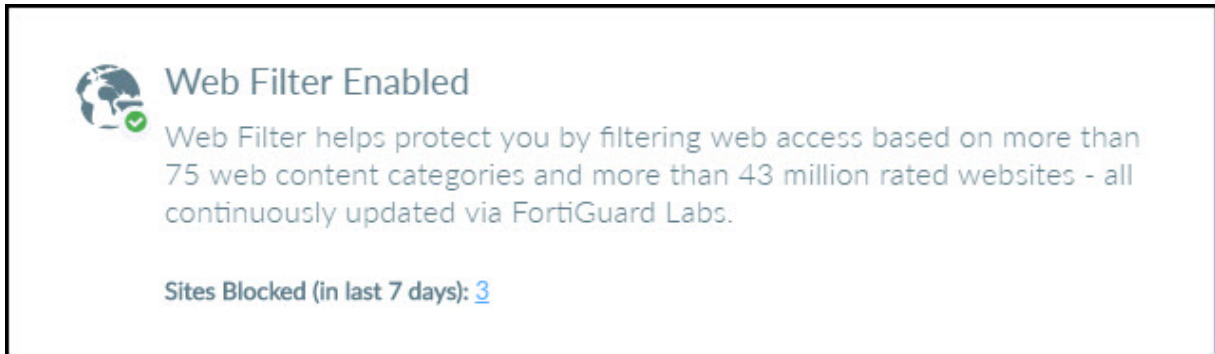
You will review the web filter profile and configuration of the FortiGuard category-based filter. These are the web filter settings that you configured in the previous exercise on endpoint profiles, which were then pushed by EMS.

To review the web filter profile

1. On the FortiClient-Laptop VM, in the system tray, right-click the FortiClient icon.
2. Click **Open FortiClient Console** to open the FortiClient GUI.



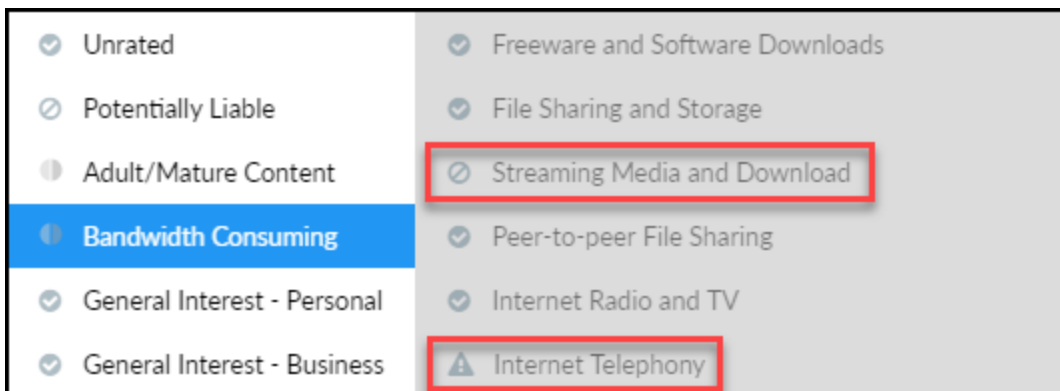
- Verify that **FortiGuard category based filter** is enabled.



- On the **Web Filter** tab, in the upper-right corner, click the settings icon .
- Review the configured actions for the following categories:

Category	Action
Potentially Liable	Block
Adult/Mature Content	Allow: Sports Hunting and War Games, Sex Education, and Lingerie and Swimsuit Block: all other subcategories Tip: Expand or click Adult/Mature Content to view the subcategories.
General Interest - Personal	Allow
General Interest - Business	Allow
Unrated	Allow

- Click **Bandwidth Consuming** to expand it and view the subcategories.



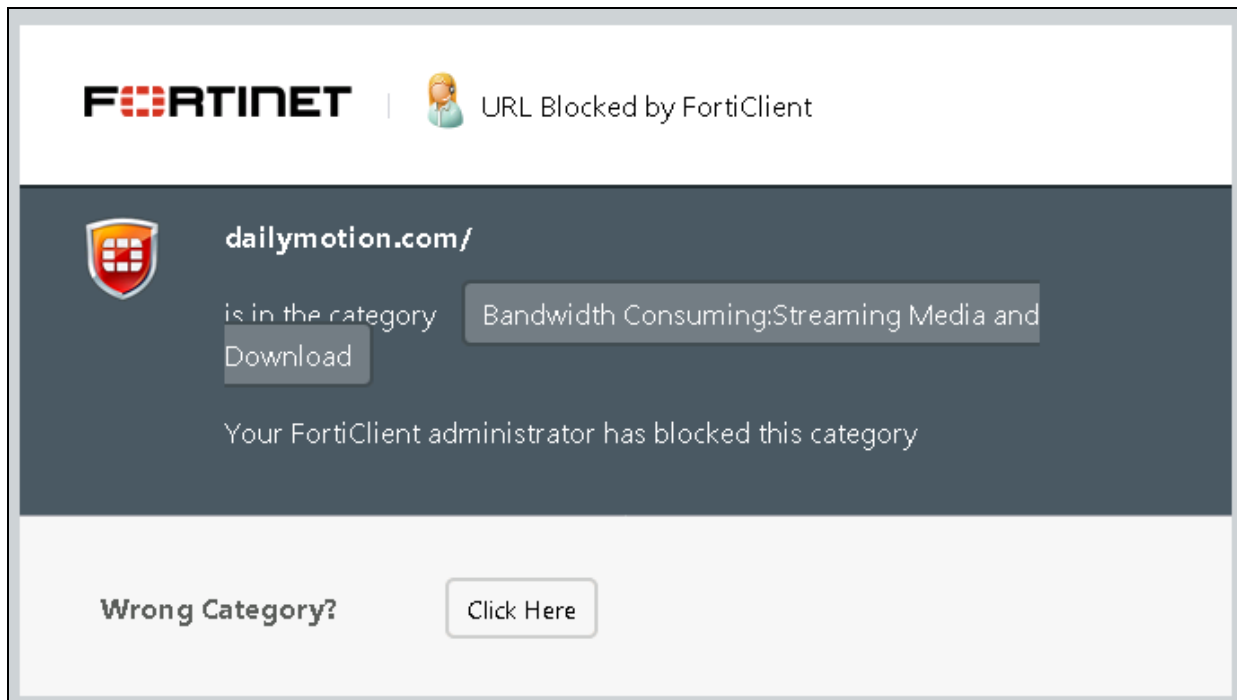
7. Verify that **Streaming Media and Download** is set to **Block**, and **Internet Telephony** is set to **Warn**.

Test the Web Filter

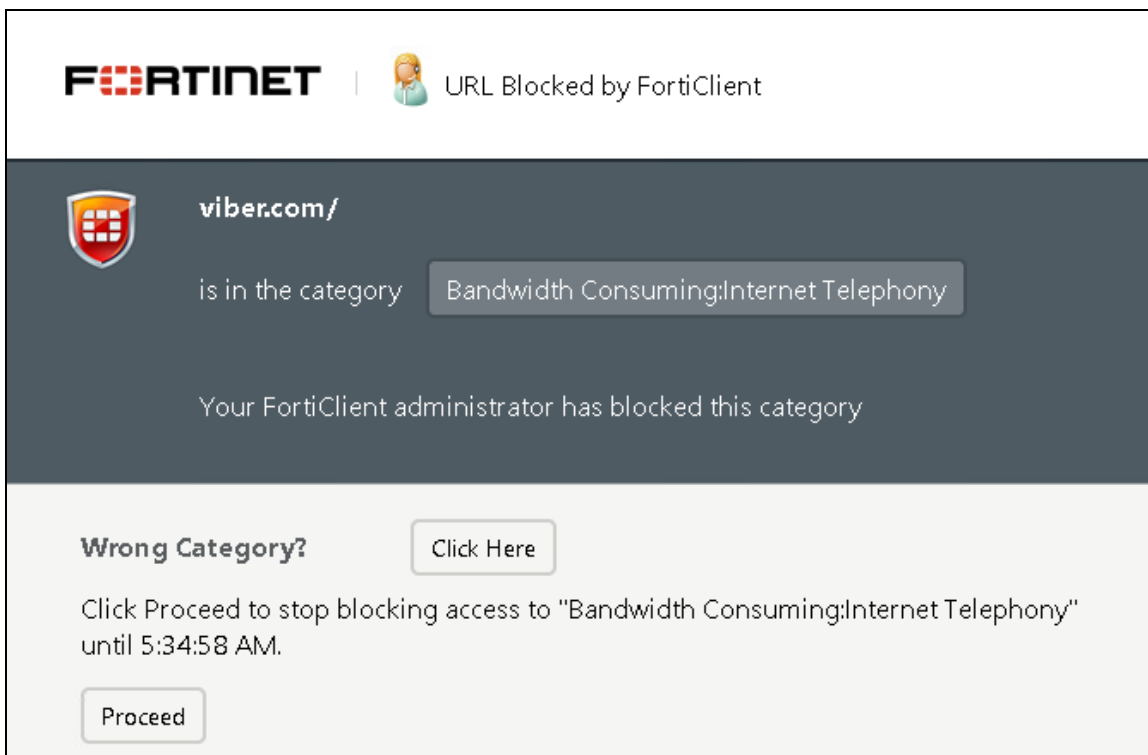
For the purposes of this lab, you will test the web filter security profile that is configured for each category.

To test the web filter

1. Continuing on the FortiClient-Laptop VM, open a new browser tab, and then visit `www.dailymotion.com`. The system displays a warning according to the predefined action for this website category.



2. Open a new browser tab, and then visit `www.viber.com`. The system displays a warning according to the predefined action for this website category.



3. Click **Proceed** to accept the warning and access the website.
4. Open a new browser tab, and then visit `www.bing.com`.
This website appears because it belongs to the **Search Engines and Portals** category, which is set to **Allow**.

Verify a Web Filter Exclusion List

You will verify that the URL `www.mp3.com` is included in the exclusion list.

To verify a URL is included in the exclusion list

1. On the FortiClient-Laptop VM, open the FortiClient console, and then select **WEB FILTER**.
2. On the **Web Filter** tab, in the upper-right corner, click the settings icon .
3. Click the + sign to expand **Exclusion List**.



Test the Web Exclusion List

You will test the web exclusion list you reviewed in the previous procedure.

To test the web exclusion list

1. Continuing on the FortiClient-Laptop VM, open a new browser tab, and then try to access the website `www.mp3.com`.

The website is allowed and it matches an exclusion list to bypass the FortiGuard block category. If you try to access `www.dailymotion.com` again, FortiGuard will block it.

Exercise 3: Understanding Antivirus Protection and Vulnerability Scans

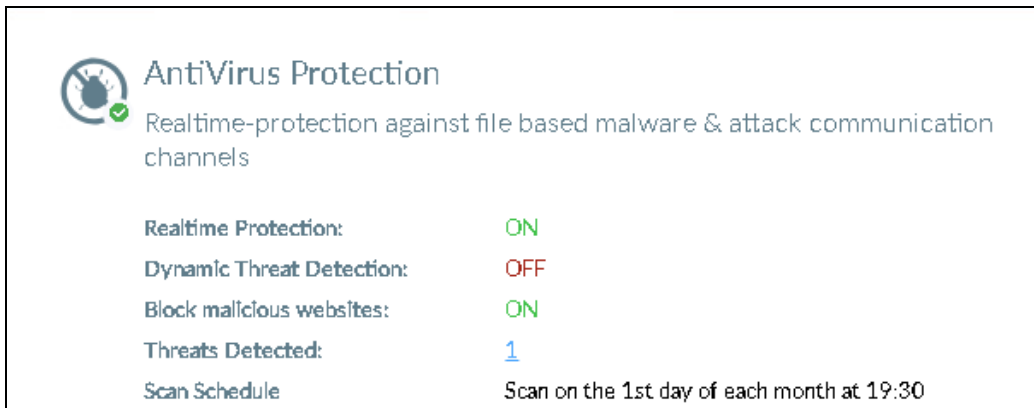
In this exercise, you will test the FortiClient malware protection features that you configured in *Exercise 1*. You will test antivirus protection to understand how FortiClient performs real-time protection. You will also learn how a vulnerability scan helps detect and patch application vulnerabilities that can be exploited by known and unknown threats.

Verify AntiVirus Protection Settings

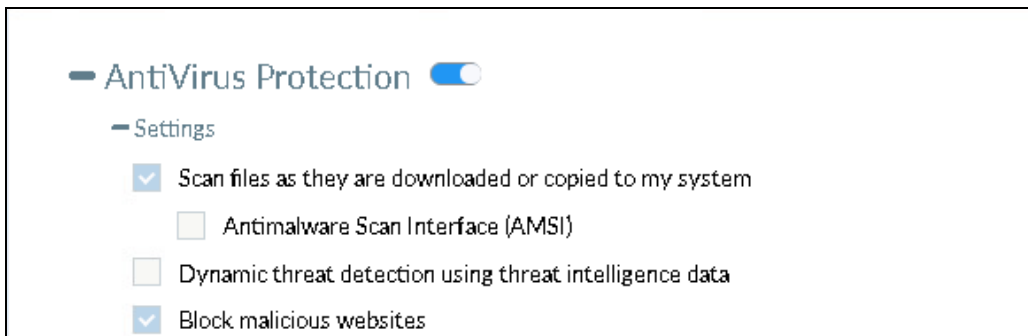
You will verify antivirus settings on FortiClient, which you configured in the EMS endpoint profile, and were then pushed to FortiClient.

To view and verify current FortiClient antiVirus protection settings

1. In the pane on the left side of the window, click **Malware Protection**, and then verify that real-time protection is enabled.



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



Test the Antivirus Real-Time Configuration

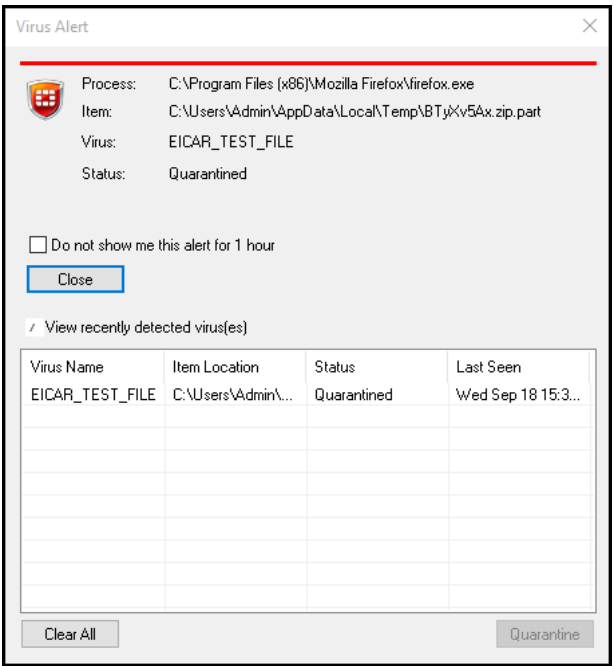
You will download the EICAR test file to your FortiClient-Laptop VM. The EICAR test file is an industry-standard virus that is used to test antivirus detection without causing damage.

To test the antivirus configuration

- Continuing on the FortiClient-Laptop VM, open a new browser tab, and then visit the following website:
`www.eicar.org`
- On the EICAR website, in the upper-right corner of the page, click **DOWNLOAD ANTI MALWARE TESTFILE**.
- On the left side of the page, click the **Download** link.
- In the **Download area using the secure, SSL enabled protocol HTTPS** section, download the sample file named `ecar_com.zip`.

Download area using the standard protocol HTTP			
– Sorry, HTTP download ist temporarily not provided. –			
Download area using the secure, SSL enabled protocol HTTPS			
ecar.com 68 Bytes	ecar.com.txt 68 Bytes	ecar_com.zip 184 Bytes	ecarcom2.zip 308 Bytes

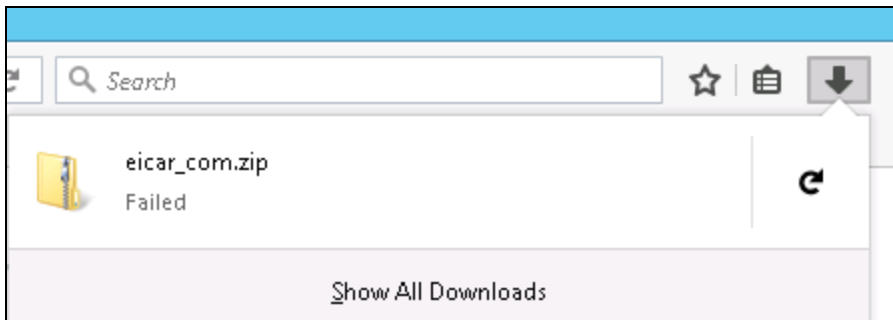
FortiClient should quarantine the download attempt and insert a replacement message similar to the following example:



FortiClient shows the HTTP/HTTPS virus message when it blocks or quarantines infected files.

5. Click **Close** to close the alert window.
6. In the download window, click **OK** to save the file.
7. Change the download location to **Desktop**, and then click **Save**.

You should see that the file you downloaded on the desktop shows the download error in the Firefox downloads dialog.



Why did the download fail?

Stop and think!

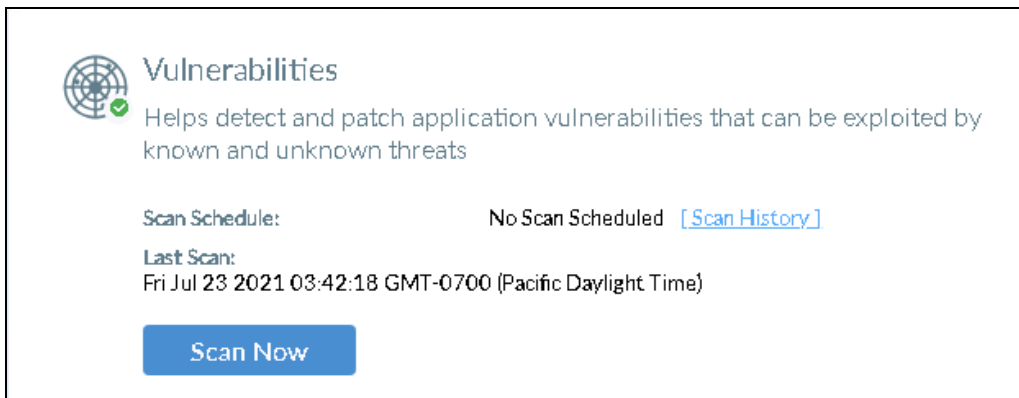
Because the file is quarantined, an EMS administrator must add it to the allowlist it and restore it to view the content.

Run an On-Demand Vulnerability Scan

You will test an on-demand vulnerability scan that you configured on the EMS endpoint profile in the first exercise, which was then pushed to FortiClient. Vulnerability scans help detect and patch application vulnerabilities that can be exploited.

To run an on-demand vulnerability scan

1. Continuing on the FortiClient console, in the pane on the left side of the window, select **Vulnerability Scan** to view the tab.
2. On the **Vulnerabilities** tab, click **Scan Now** to start an on-demand scan.



- 3. After the scan is finished, you will see the scan results under **Vulnerabilities Detected**.
- 4. To review the vulnerability details, click **CRITICAL**, and then expand **3rd Party App**.

3rd Party App (1)			
APPLICATIONS		SEVERITY	RECOMMENDED ACTION
☐	Adobe Reader X 10.0.0.396 (1) C:\Program Files (x86)\Adobe\Reader 10.0\Reader\AcroRd32.exe	Critical	Manual Install
VULNERABILITY NAME		SEVERITY	DETAILS
WARNING: Adobe Reader X is no longer supported by the vendor		Critical	≡

In this case, FortiClient cannot automatically install the software patch because the recommended action is **Manual Install**. You can manually download and install the latest version of vulnerable software to fix the vulnerability.

- 5. Close all open windows.



In the real environment, you should install the patch on affected applications.

Lab 6: 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 components, from the FortiClient EMS, to FortiGate and FortiClient. You will also review key ZTNA concepts.

Objectives

- Verify the FortiGate and FortiClient EMS connection
- Configure EMS ZTNA tagging rules
- Enable the ZTNA feature on FortiGate and verify ZTNA tags
- Configure a basic HTTPS access proxy with SSL certificate-based authentication
- Configure an HTTPS access proxy with basic user authentication and ZTNA tags
- Configure basic ZTNA IP/MAC filtering

Time to Complete

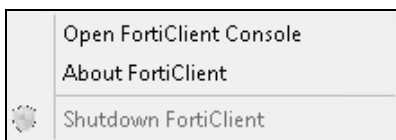
Estimated: 55 minutes

Prerequisites

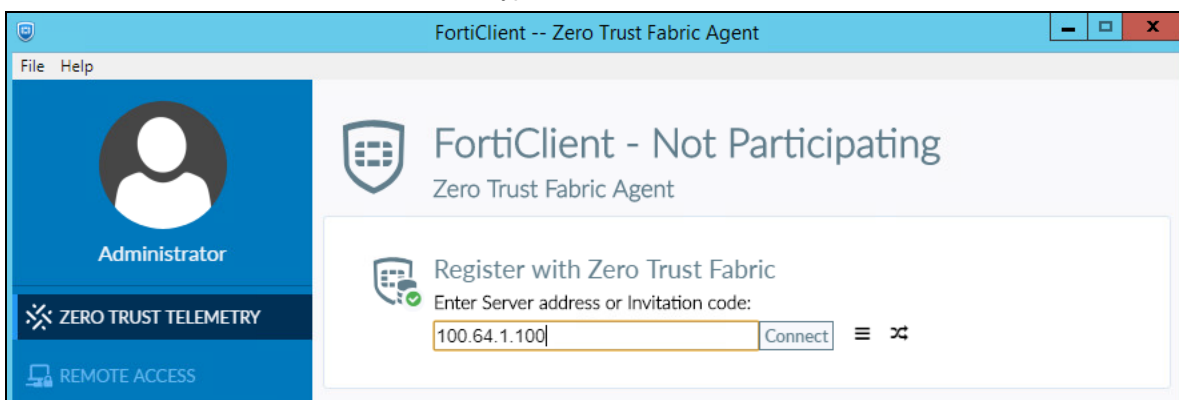
Before you start this lab, you must connect the Remote-Client endpoint to FortiClient EMS. FortiClient is already installed on the endpoint and must establish a connection to FortiClient EMS.

To connect a remote endpoint to FortiClient EMS

1. On the Remote-Client VM, in the system tray, right-click the FortiClient icon.
2. Click **Open FortiClient Console** to open the FortiClient GUI.

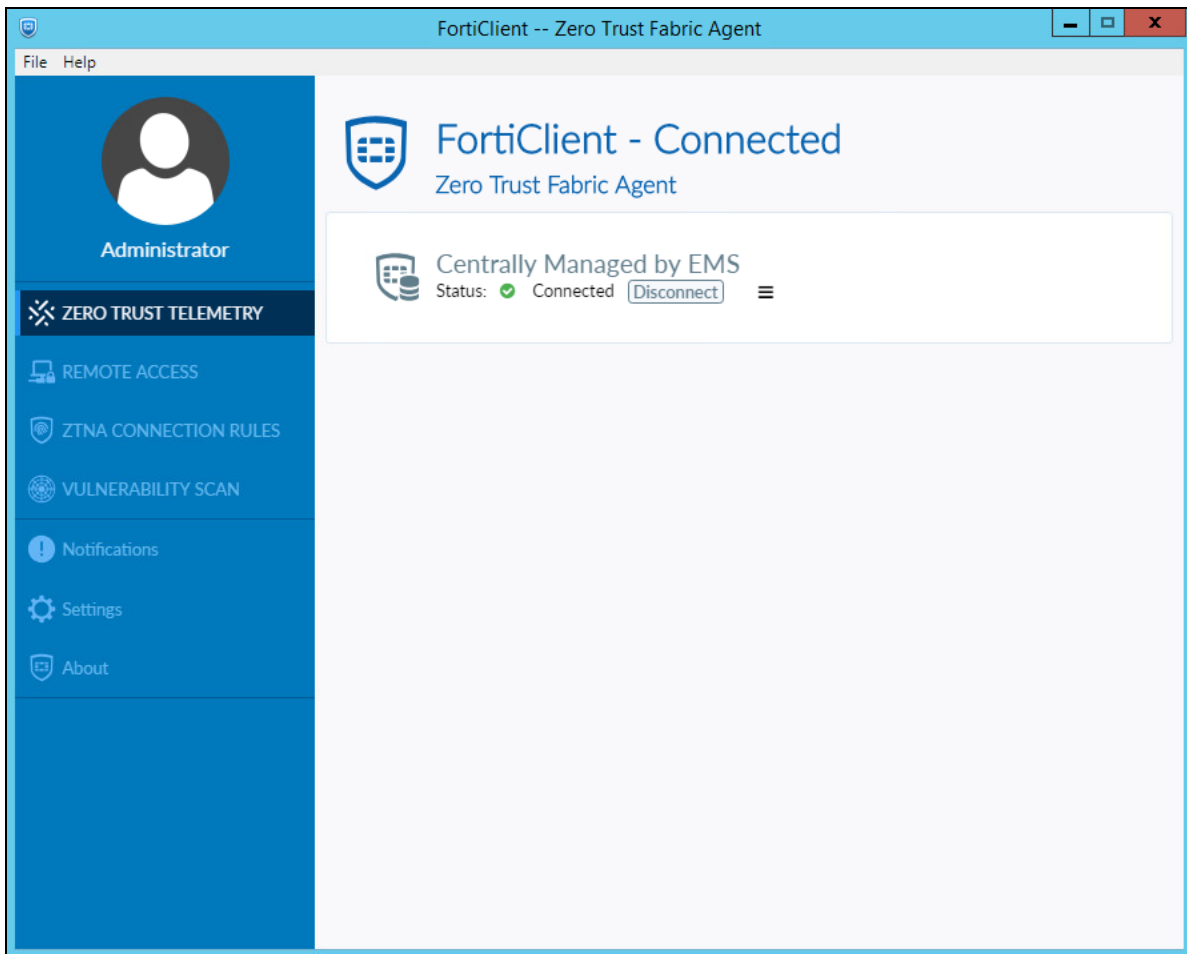


3. In the **ZERO TRUST TELEMETRY** section, type the IP address 100.64.1.100.



4. Click **Connect**.

After a few minutes, the status changes to connect, and FortiClient has all the configuration pushed by FortiClient EMS.



Exercise 1: Configuring ZTNA Tags, Tagging Rules, and Features

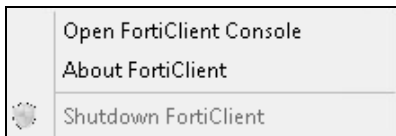
In this exercise, you will verify the connection between FortiClient, FortiClient EMS, and FortiGate. You will also configure ZTNA tags and tagging rules, and then verify if the tags are synced on FortiClient and FortiGate. These tags will be used in the next exercises to authorize user traffic based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

Verify the Connection Between FortiClient, FortiClient EMS, and FortiGate

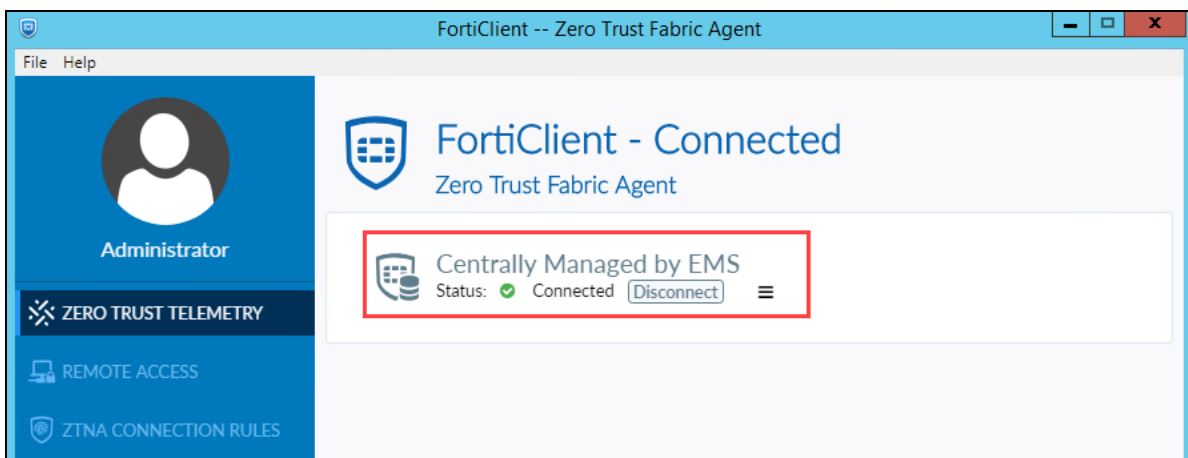
Establishing device identity and device trust between FortiClient, FortiClient EMS, and FortiGate is integral to ZTNA setup. All of these devices must have a stable connection in order to exchange information required for ZTNA tagging to work properly.

To verify the FortiClient to FortiClient EMS connection

1. On the Remote-Client VM, in the system tray, right-click the FortiClient icon.
2. Click **Open FortiClient Console** to open the FortiClient GUI.

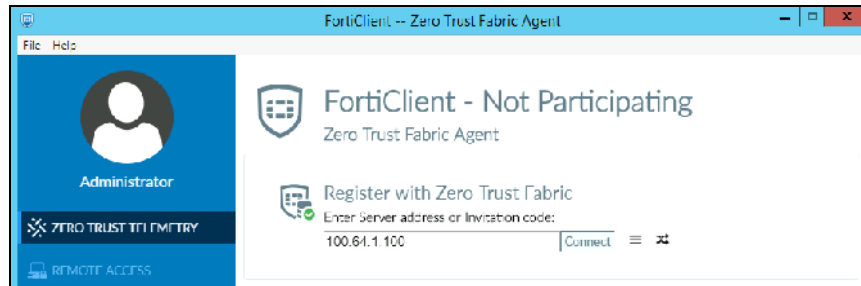


3. In the **ZERO TRUST TELEMETRY** section, ensure that the status of **Centrally Managed by EMS** is **Connected**.



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

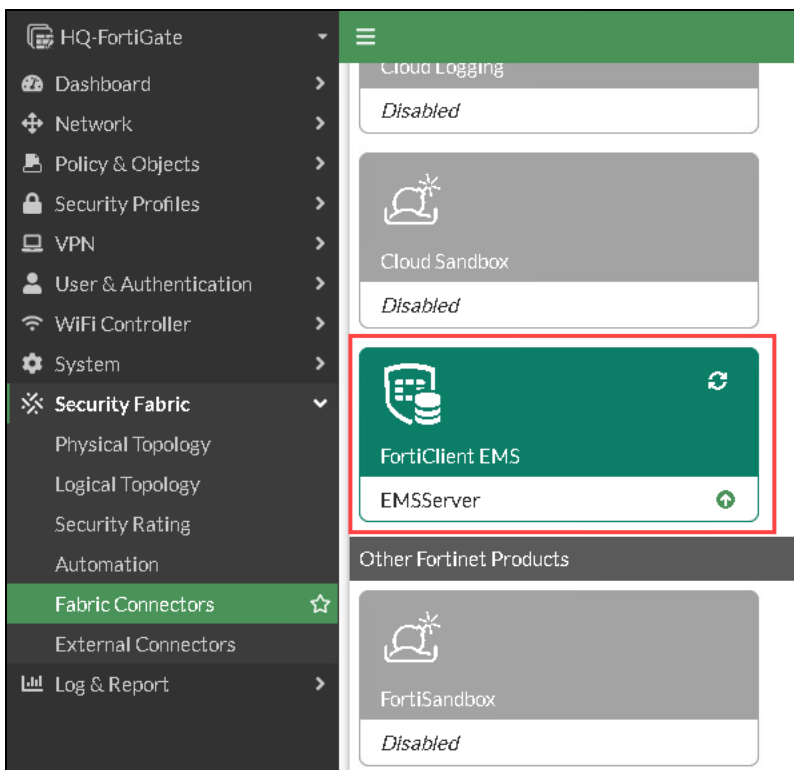
1. In the **ZERO TRUST TELEMETRY** section, click **Disconnect**.
2. In the **Enter Server address or Invitation code** field, type `100.64.1.100`, and then click **Connect** to reconnect the Remote-Client VM to FortiClient EMS.



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

To verify FortiClient EMS as the Fabric connector

1. On the AD Server VM, open Firefox, type the FortiGate IP address `10.0.1.254`, and then log in with the username `admin` and password `password`.
2. On the FortiGate GUI, click **Security Fabric > Fabric Connectors**.
3. On the right side, scroll down to see the **FortiClient EMS** connector status.
The status arrow should be a green up arrow.



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

```
diagnose endpoint fctems test-connectivity <EMS name>
```

```
HQ-FortiGate # diagnose endpoint fctems test-connectivity EMSServer
Connection test was successful:
```

Configure FortiClient EMS ZTNA Tagging Rules

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

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

1. On the AD Server VM, click the FortiClient EMS icon to launch the application.
2. Log in to the FortiClient EMS GUI with the username `admin` and password `Password123`.
3. In the left menu, click **Zero Trust Tags > Zero Trust Tagging Rules**.
4. In the upper-right, click **Add**.
5. In the **Name** field, type `Malicious-File-Detected`.
6. In the **Tag Endpoint As** field, type `Malicious-File-Detected`, and then press **Enter**.
7. In the **Rules** section, click **Add Rule**, and then select **Windows OS**.
8. In the **Rule Type** field, select **File**.

9. In the **File** field, type `C:\virus.txt`, and then click **Save**.
10. Click **Save** to save this zero-trust tagging rule.

Zero Trust Tagging Rule Set

Name

Malicious-File-Detected

Tag Endpoint As ⓘ

Malicious-File-Detected

Enabled

☒

Comments

Optional

Rules

+ Add Rule

Type	Value
Windows (1)	
File	C:\virus.txt

Save

Cancel

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

1. Continuing on **Zero Trust Tags > Zero Trust Tagging Rules**.
2. In the upper-right, click **Add**.
3. In the **Name** field, type `Remote-Endpoints`.
4. In the **Tag Endpoint As** field, type `Remote-Endpoints`, and then press `Enter`.
5. In the **Rules** section, click **Add Rule**, and then select **Windows OS**.
6. In the **Rule Type** field, select **IP Range**.
7. In the **IP Range** field, type `10.0.2.0/24`, and then click **Save**.
8. Click **Save** to save this zero-trust tagging rule.

Zero Trust Tagging Rule Set

Name

Remote-Endpoints

Tag Endpoint As ⓘ

Remote-Endpoints

Enabled

☒

Comments

Optional

Rules

+ Add Rule

Type	Value
Windows (1)	
IP Range	10.0.2.0/24

Save

Cancel

Both rules appear under **Zero Trust Tagging Rules**.

FortiClient Endpoint Management Server		Invitations ⓘ ⚙️ 🔔 admin ⌵				
Zero Trust Tagging Rule Sets		Import Signatures Manage Tags + Add Refresh Clear Filters				
		Name	Tag	Enabled	Comments	
		Malicious File Detected	Malicious File Detected	✔️		
		Remote-Endpoints	Remote-Endpoints	✔️		

9. Click **Zero Trust Tags > Zero Trust Tag Monitor**.
Remote-Client is tagged as **Remote-Endpoints**. If it does not appear immediately, use the **Refresh** button in the upper-right corner of the window.

Endpoint with Tag

Refresh

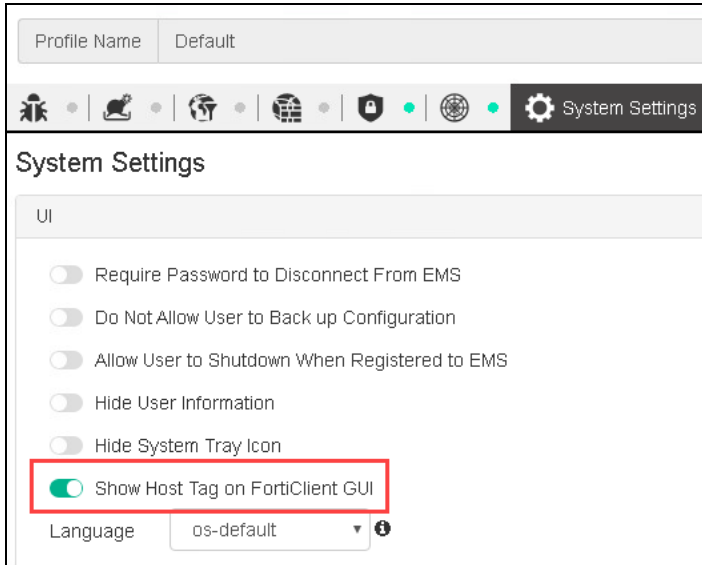
Low (3)

Remote-Endpoints (1)

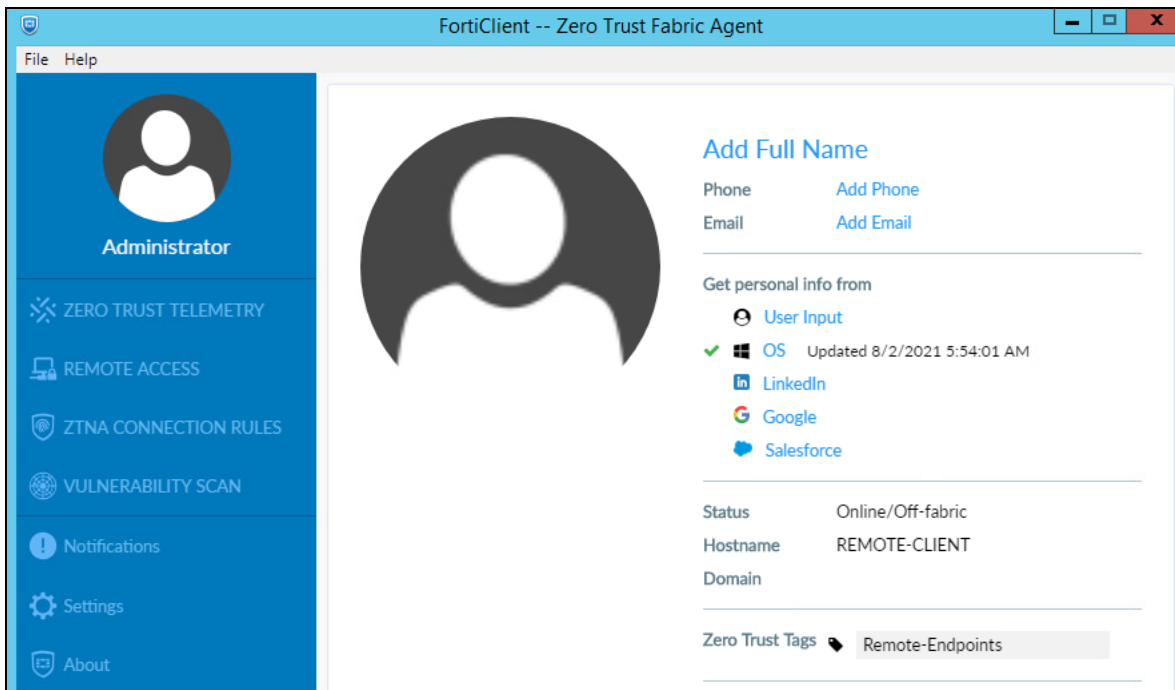
Endpoint	User	OS	IP	Tagged on
Remote-Client	 Administrator	Microsoft Windows Ser...	10.0.2.20	2021-08-10 07:17:38

To configure the ZTNA tag to display on FortiClient

1. Continuing on the FortiClient EMS GUI, click **Endpoint Profiles > Manage Profiles**.
2. Select the **Default** profile, and then click **Edit**.
3. On the **System Settings** tab, under **UI**, enable **Show Host Tag on FortiClient GUI**.



4. Click **Save** to apply the changes.
5. Repeat steps 1–4 for the **Fortinet-Training** endpoint profile.
6. On the Remote-Client VM, on the FortiClient GUI, click the user avatar.
The **Zero Trust Tags** field shows the currently detected tags.

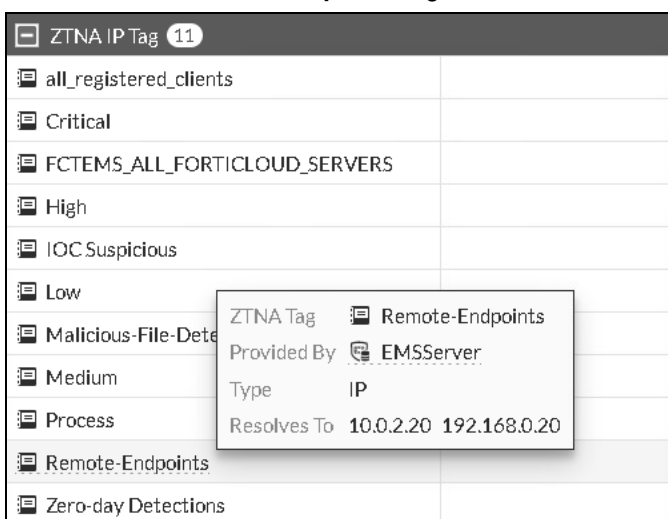


Enable the ZTNA Feature and Verify That ZTNA Tags Are Synced

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

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

1. On the AD server VM, on the FortiGate GUI, click **System > Feature Visibility**, and then enable **Zero Trust Network Access**.
2. Click **Policy & Objects > ZTNA**, and then on the right side, click the **ZTNA Tags** tab.
ZTNA tags should be displayed on the page.
3. Hover over the **Remote-Endpoints** tag to see the IP address of the endpoint.



Exercise 2: Configuring a Basic HTTPS Access Proxy With SSL Certificate-Based Authentication

In this exercise, you will configure a basic HTTPS proxy access with SSL certificate-based authentication. A client certificate is obtained when an endpoint registers with FortiClient EMS. FortiClient automatically submits a CSR request and FortiClient EMS signs and returns the client certificate. The endpoint information is synchronized between FortiGate and FortiClient EMS.

You will also locate the certificate on the endpoint and match it on FortiClient EMS and FortiGate. Finally, you will see the behavior of the FortiGate `set client-cert` and `set empty-cert-action` options on the access-proxy object.

Configure a Basic HTTPS Access Proxy With Certificate-Based Authentication

The HTTPS access proxy setup requires a ZTNA server, real server, ZTNA rule, and firewall policy on FortiGate.

To configure the ZTNA server or HTTPS access proxy VIP

1. On the HQ-FortiGate GUI, click **Policy & Objects** > **ZTNA**, and then click the **ZTNA Servers** tab.
2. Click **Create New** to create a new server, and then configure the following settings:

Field	Value
Name	ZTNA-webserver
External interface	Select port1 .
External IP	100.64.1.10
External port	9443
Default certificate	Select Fortinet_SSL .

Name

Comments

Network

Service **HTTPS**

External interface

External IP

External port

Services and Servers

Default certificate

Service/server mapping

[+ Create New](#) [Edit](#) [Delete](#)

Service	URL
HTTPS	/

- 3. In the **Service/server mapping** section, click **Create New**.
- 4. In the **Virtual Host** field, select **Any Host**.
- 5. Leave the **Path** field at the default value of **/**.
- 6. In the **Servers** section, click **Create New** to create a new server mapping.
- 7. In the **IP** field, type **10.0.3.10**, in the **Port** field, type **443**, and then click **OK**.

Service **HTTPS**

Virtual Host **Any Host** [Specify](#)

Match path by **Substring** [Wildcard](#) [Regular Expression](#)

Path

Servers

[+ Create New](#) [Edit](#) [Delete](#)

IP	Port	Status
10.0.3.10	443	Active

- 8. Click **OK** to save the **Service/server mapping** settings.
- 9. Click **OK** to complete the ZTNA server setup.

To configure ZTNA rules

- 1. Continuing on **Policy & Objects > ZTNA**, click the **ZTNA Rules** tab.
- 2. Click **Create New** to create a new rule.

- 3. In the **Name** field, type `ZTNA-Allow-All`.
- 4. Leave the **Source** field set to `all`.
- 5. In the **ZTNA Server** field, select `ZTNA-webserver`.
- 6. In the **Action** field, select **ACCEPT**.
- 7. In the **Logging Options** section, ensure that the **Log Allowed Traffic** field is set to **All Sessions**.
- 8. Ensure that **Enable this policy** is enabled.

New ZTNA Rule

Name ⓘ

ZTNA-Allow-All

Source

all

+

×

ZTNA Tag

+

ZTNA Server

ZTNA-webserver

▼

Action

✓ ACCEPT

⊘ DENY

Security Profiles

AntiVirus

⊘

Web Filter

⊘

Video Filter

⊘

Application Control

⊘

IPS

⊘

File Filter

⊘

SSL Inspection

SSL

no-inspection

▼

✎

Logging Options

Log Allowed Traffic ⓘ

⊘ Security Events

⊙ All Sessions

Comments

Write a comment...

0/1023

Enable this policy

⊙

- 9. Click **OK** to save the settings.

To configure a firewall policy on FortiGate for full ZTNA

- 1. Continuing on the HQ-FortiGate GUI, click **Policy & Objects > Firewall Policy**.
- 2. Click **Create New** to add a new firewall policy.
- 3. Configure the following settings:

Field	Value
Name	ZTNA-WAN
ZTNA	Enable ZTNA , and then select Full ZTNA .

FortiClient EMS 7.0 Lab Guide
Fortinet Technologies Inc.

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

83

Field	Value
Incoming Interface	port1
Source	all
ZTNA Server	ZTNA-webserver
Schedule	always
Service	ALL
Action	ACCEPT
NAT	<disable>
Log Allowed Traffic	<enable>
Enable this policy	<enable>

New Policy

Name ⓘ

ZTNA-WAN

ZTNA ⓘ

☒ Full ZTNA

☐ IP/MAC filtering

Incoming Interface ⓘ

port1

Source ⓘ

all

+

×

ZTNA Server ⓘ

ZTNA-webserver

+

×

Schedule ⓘ

always

Service ⓘ

ALL

+

×

Action ⓘ

☒ ACCEPT

☐ DENY

Firewall / Network Options

NAT ⓘ

☐

Logging Options

Log Allowed Traffic ⓘ

☒

Comments ⓘ

Write a comment...

0/1023

Enable this policy ⓘ

☒

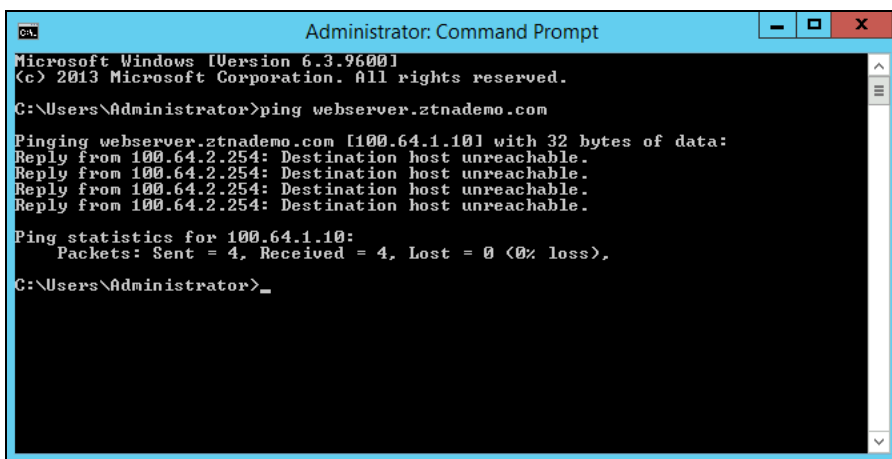
4. Click **OK** to save the settings.

Test Remote Access to the HTTPS Access Proxy

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

To test remote access to the HTTPS access proxy

1. On the Remote-Client VM, open the command prompt from the task bar.
2. Enter `ping webserver.ztnademo.com`, and then verify it resolves to `100.64.1.10`.



```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping webserver.ztnademo.com

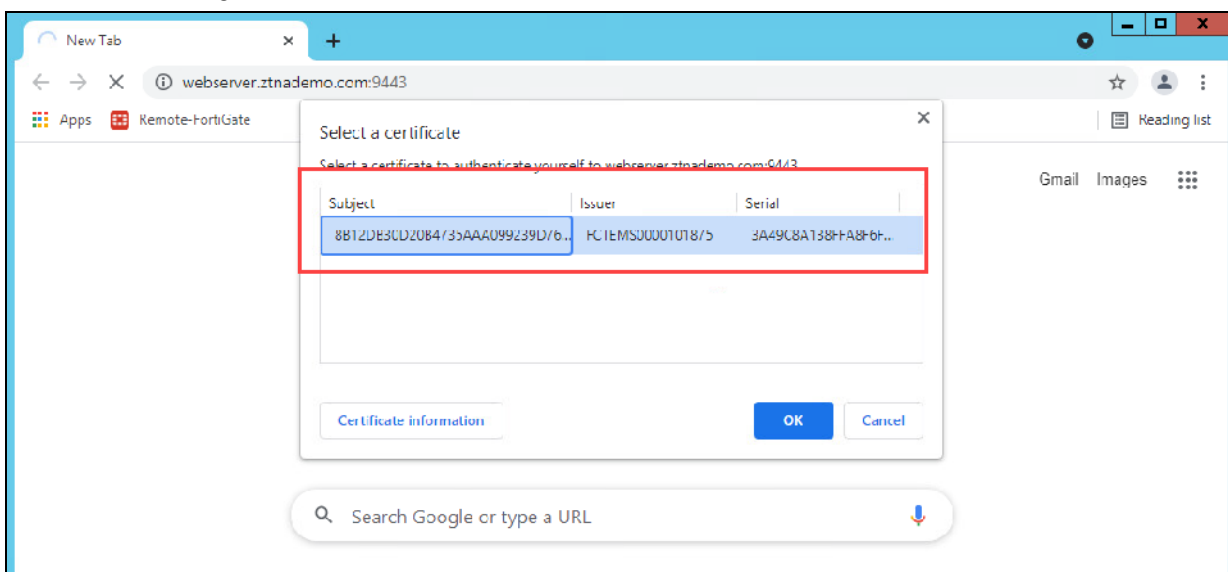
Pinging webserver.ztnademo.com [100.64.1.10] with 32 bytes of data:
Reply from 100.64.2.254: Destination host unreachable.
Reply from 100.64.2.254: Destination host unreachable.
Reply from 100.64.2.254: Destination host unreachable.
Reply from 100.64.2.254: Destination host unreachable.

Ping statistics for 100.64.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

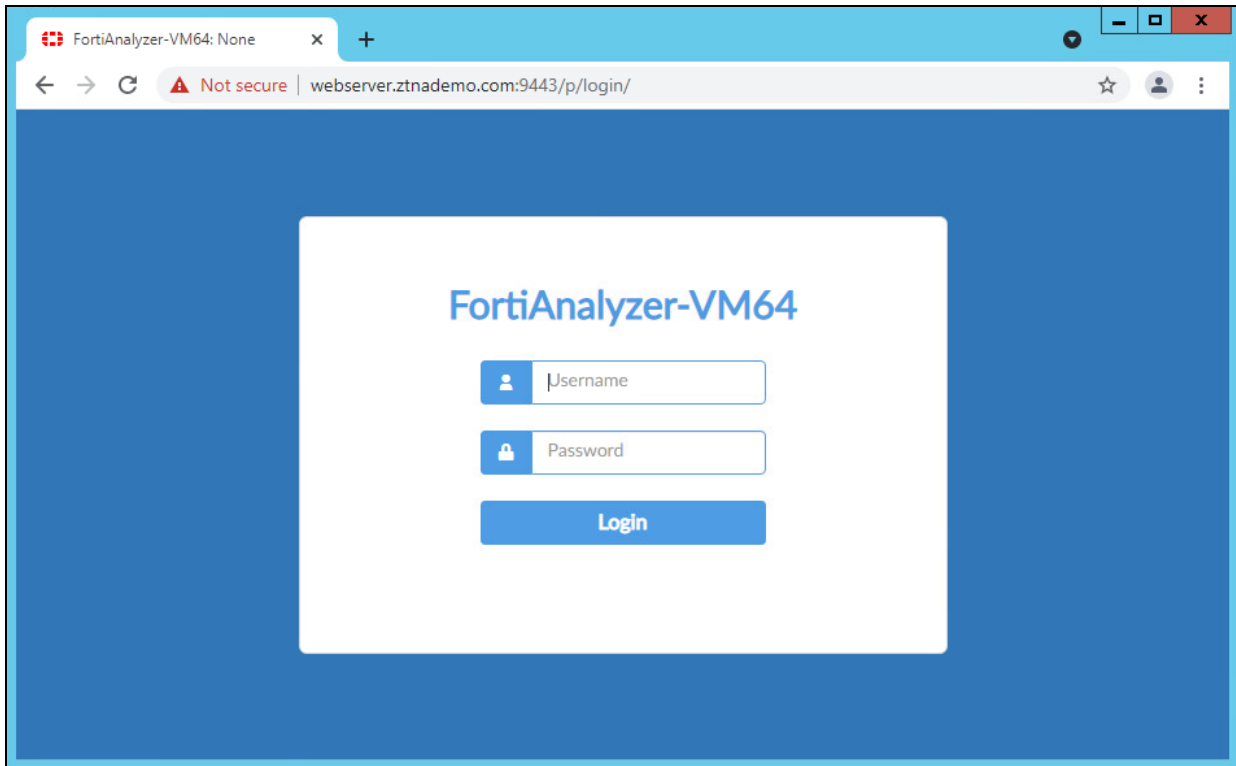
C:\Users\Administrator>
```

The actual ping will not be successful—you just want to be sure that the DNS resolves.

3. Close the command prompt window.
4. Open the Chrome browser from the desktop, and then type `https://webserver.ztnademo.com:9443`. The browser prompts you for the client certificate to use.
5. Choose the EMS signed certificate, and then click **OK**.



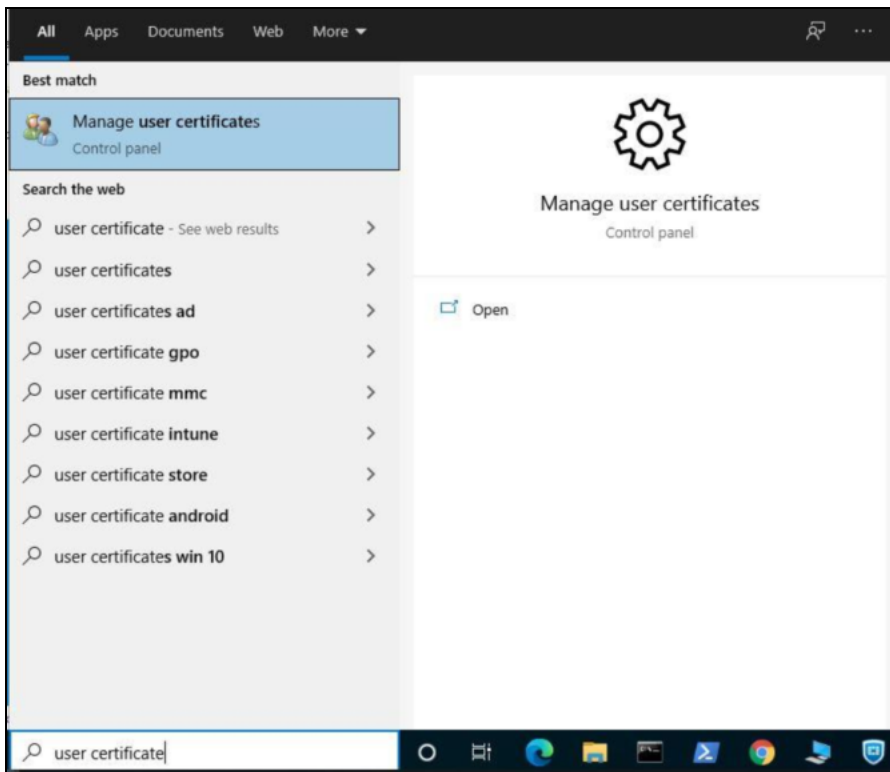
Access to the web server should be allowed. We're using the FortiAnalyzer login page to demonstrate the web page.



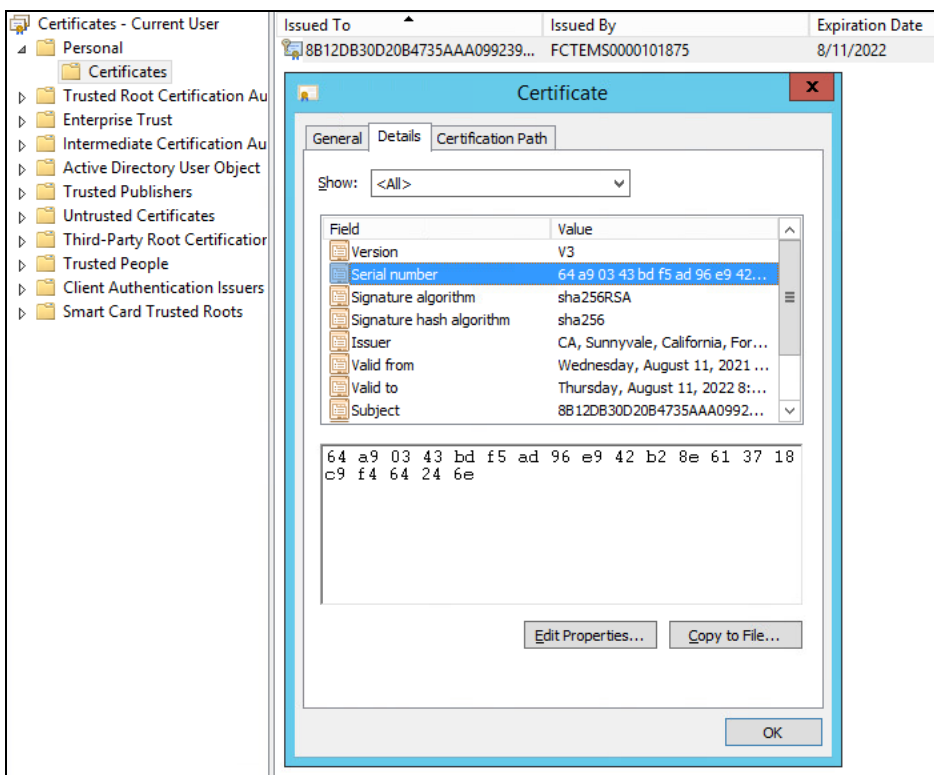
By default, client certificate authentication is enabled on the access proxy, so when the HTTPS request is received, the FortiGate WAD process challenges the client to identify itself with its certificate.

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

1. Continuing on the Remote-Client VM, open a Windows search, and then look for user certificates.



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



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

- On the desktop, open PuTTY, and then double-click **HQ-FortiGate** from the saved session to open FortiGate CLI access.
- Enter the username `admin` and password `password` to log in, and then enter the following CLI command to view the endpoint serial number (**SN**) and other information:

`diagnose endpoint record list`

```
Record #3:
    IP Address = 10.0.2.20
    MAC Address = 00:50:56:a1:06:87
    MAC list = 00:50:56:a1:06:87;00:50:56:a1:1e:1a;
    VDOM = (-1)
    EMS serial number: FCTEMS0000101875
    Client cert SN: 64A90343BDF5AD96E942B28E613718C9F464246E
    Public IP address: 206.47.132.124
    Quarantined: no
    Online status: online
    Registration status: registered
    On-net status: off-net
    Gateway Interface:
    FortiClient version: 7.0.0
    AVDB version: 88.289
    FortiClient app signature version: 18.139
    FortiClient vulnerability scan engine version: 2.31
    FortiClient UID: 8B12DB30D20B4735AAA099239D76B99C
    Host Name: Remote-Client
    OS Type: WIN64
    OS Version: Microsoft Windows Server 2012 R2 Standard Edition, 6
4-bit (build 9600)
    Host Description:
    Domain:
    Last Login User: Administrator
```

- On the AD server tab, open the FortiClient EMS GUI, and then click **Endpoints > All Endpoints**.
- In the list, click **Remote-Client**, and then in the **Configuration** section, check the **FortiClient ID** and **ZTNA Serial Number** fields to match the information.

The screenshot displays the FortiClient EMS GUI. At the top, there's a table of endpoints. The 'Remote-Client' endpoint is highlighted in yellow. Below the table, the 'Configuration' section for the 'Remote-Client' is shown. The 'FortiClient ID' and 'ZTNA Serial Number' fields are highlighted with red boxes, matching the values from the CLI output. The 'Status' section on the right shows various features installed, including Antivirus, Anti-Ransomware, Cloud Based Malware Outbreak Detection, Sandbox, and Web Filter.

Endpoint	User	IP Address	Policy	Deployment	EMS	WEB	VUL	SYS
AD-Server	Administrator	10.0.1.100	Training	✓	EMS	14		
FortiClient-Laptop	Administrator	10.0.1.10	Training	✓	EMS	99+		
Remote-Client	Administrator	10.0.2.20	Training	✓	EMS	2	99+	3

Configuration Details for Remote-Client:

- Policy:** Training
- Profile:** Fortinet-Training
- Off-Fabric Profile:** Default
- Installer:** Not assigned
- FortiClient Version:** 7.0.0.0029
- FortiClient Serial Number:** FCT8000906335614
- FortiClient ID:** 8B12DB30D20B4735AAA...
- ZTNA Serial Number:** 64A90343BDF5AD96E942...

Status: Managed

Features: Antivirus installed, Anti-Ransomware installed, Cloud Based Malware Outbreak Detection installed, Sandbox installed, Sandbox Cloud installed, Web Filter enabled (hidden), Application Firewall installed, Remote Access configured, Vulnerability Scan enabled, SSOMA installed.

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

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

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. FortiGate also has a configuration to accept or block an empty client certificate.



If a user clicks cancel during the certificate challenge, one of the following actions occurs:

1. If the `empty-cert-action` is `accept`, the client is allowed to continue with ZTNA proxy rule processing.
2. If the `empty-cert-action` is `block`, the client is blocked from further ZTNA proxy rule processing.

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

To configure FortiGate to block empty certificate challenges

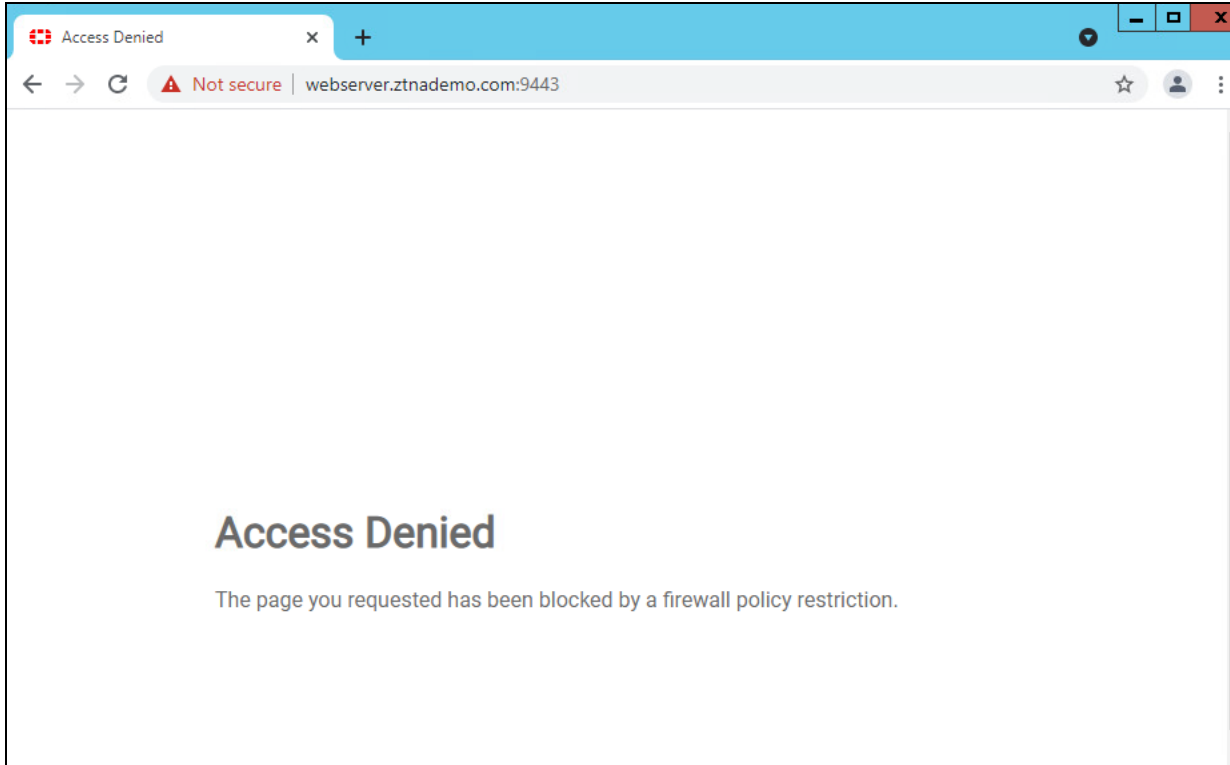
1. On the PuTTY session, enter the following CLI commands:

```
config firewall access-proxy
edit ZTNA-webserver
set empty-cert-action block
end
```



By default, in 7.0.1, `empty-cert-action` is set to `block`. In 7.0.0, it was set to `accept`.

2. Close the PuTTY session.
3. On the desktop, open the Chrome browser, and then type `https://webserver.ztnademo.com:9443`. The browser prompts you for the client certificate to use.
4. Click **Cancel**.
FortiGate blocks access.

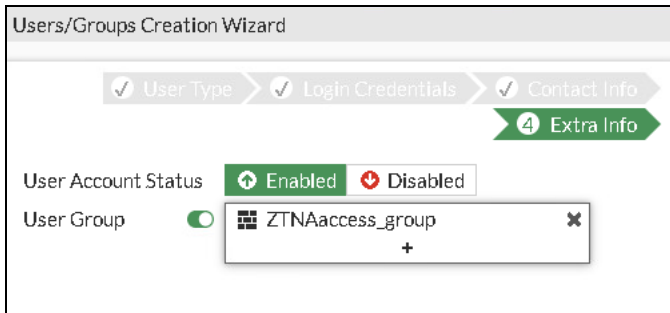


Exercise 3: Configuring an HTTPS Access Proxy With User Authentication and ZTNA Tags

In this exercise, you will extend the solution to include user authentication with local users and security posture checks with ZTNA tags. You will configure local user authentication and ZTNA rules to apply security posture checks using ZTNA tags.

To configure a local user on FortiGate

1. On the AD Server VM, open a browser to log in to the HQ-FortiGate IP address 10.0.1.254 with the username `admin` and password `password`.
2. In the left menu, click **User & Authentication > User Definition**.
3. Click **Create New** to create a new user.
4. In the wizard, select **Local User**, and then click **Next**.
5. In the **Username** field, type `ZTNAuser`, in the **Password** field, type `fortinet`, and then click **Next**.
6. Leave **Two-factor Authentication** disabled, and then click **Next**.
7. Ensure that the **User Account Status** field is set to **Enabled**.
8. Enable **User Group**, and then select **ZTNAaccess_group**.



9. Click **Submit** to save the user.



You can also use LDAP, RADIUS, and TACACS+ users for authentication.

To configure an authentication scheme on FortiGate

1. Continuing on the HQ-FortiGate GUI, click **System > Feature Visibility**, and then enable **Explicit Proxy** to make the **Authentication Rules** page visible.
2. Click **Apply**.
3. Click **Policy & Objects > Authentication Rules**, and then in the top-right, select **Authentication Schemes**.
4. Click **Create New > Authentication Scheme**.
5. In the **Name** field, type `ZTNA-Auth-scheme`.

6. In the **Method** field, select **Basic**.
7. Leave the **User database** field set to **Local**.

Name: ZTNA-Auth-scheme

Method: Basic

User database: Local Other

FSSO guest: ☐

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

Configure an Authentication Rule

An authentication rule specifies which proxy sources and destinations require authentication and which authentication scheme to apply. You will use active authentication through the basic HTTP prompt and apply it to all sources.

To configure an authentication rule on FortiGate

1. Continuing on the **Authentication Rules** page, click **Create New > Authentication Rules**.
2. In the **Name** field, type **ZTNA-Auth-Rule**.
3. In the **Source Address** field, select **all**.
4. Leave the **Protocol** field set to **HTTP**.
5. Enable **Authentication Scheme**, and then select **ZTNA-Auth-scheme**.
6. Ensure that the **Enable This Rule** field is set to **Enable**.

Name: ZTNA-Auth-Rule

Source Address: all

Protocol: HTTP

Authentication Scheme: ☒ ZTNA-Auth-scheme

IP-based Authentication: ☒ Enable ☐ Disable

SSO Authentication Scheme: ☐

Comments: Write a comment... 0/1023

Enable This Rule: ☒ Enable ☐ Disable

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

Apply the User Group and ZTNA Tag to a ZTNA Rule

You must apply a user or user group to one or more ZTNA rules that you want to use to control user access. The authenticated user from the authentication scheme and rule must match the user or user group in the ZTNA rule.

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

1. Continuing on the HQ-FortiGate GUI, click **Policy & Objects > ZTNA**.
2. Click **ZTNA Rules**, select **ZTNA-Allow-All**, and then click **Edit**.
3. In the **Source** field, click **+** to add a new entry.
4. In the window, select **User**, and then choose **ZTNAaccess_group**.
5. In the **ZTNA Tag** field, click **+**, and then add the **Remote-Endpoints** IP tag.

Edit ZTNA Rule

Name

ZTNA-Allow-All

Source

all

ZTNAaccess_group

+

ZTNA Tag

Remote-Endpoints

+

ZTNA Server

ZTNA-webserver

Action

ACCEPT

DENY

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

To create a deny rule for malicious file detection

1. Click **ZTNA > ZTNA Rules**, and then click **Create New**.
2. In the **New ZTNA Rule** window, configure the following settings:

Field	Value
Name	ZTNA-Deny-Malicious
Source	Address: all User: ZTNAaccess_group
ZTNA Tag	Malicious-File-Detected
ZTNA Server	ZTNA-webserver
Action	Deny
Enable this policy	<enable>

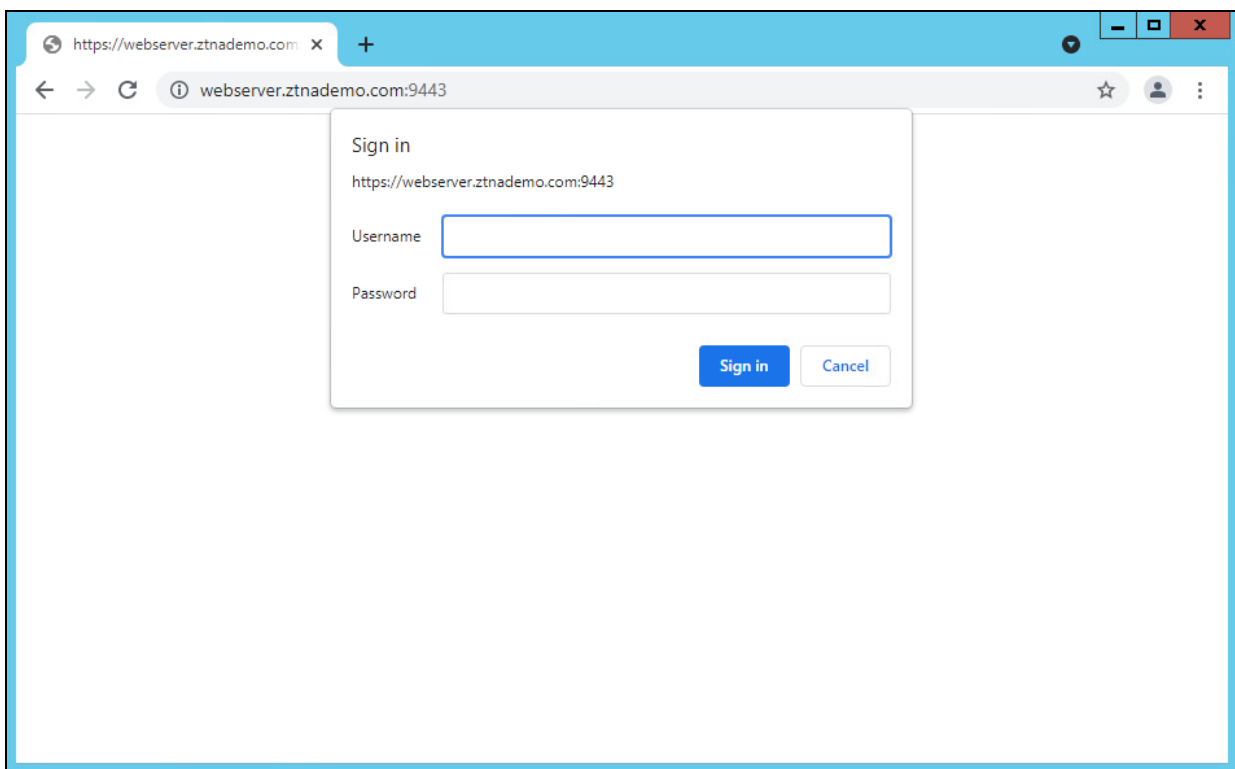
3. Click **OK** to save the new rule.
4. Move this rule above the **ZTNA-Allow-All** rule.

Test Remote Access to the HTTPS Access Proxy With User Authentication

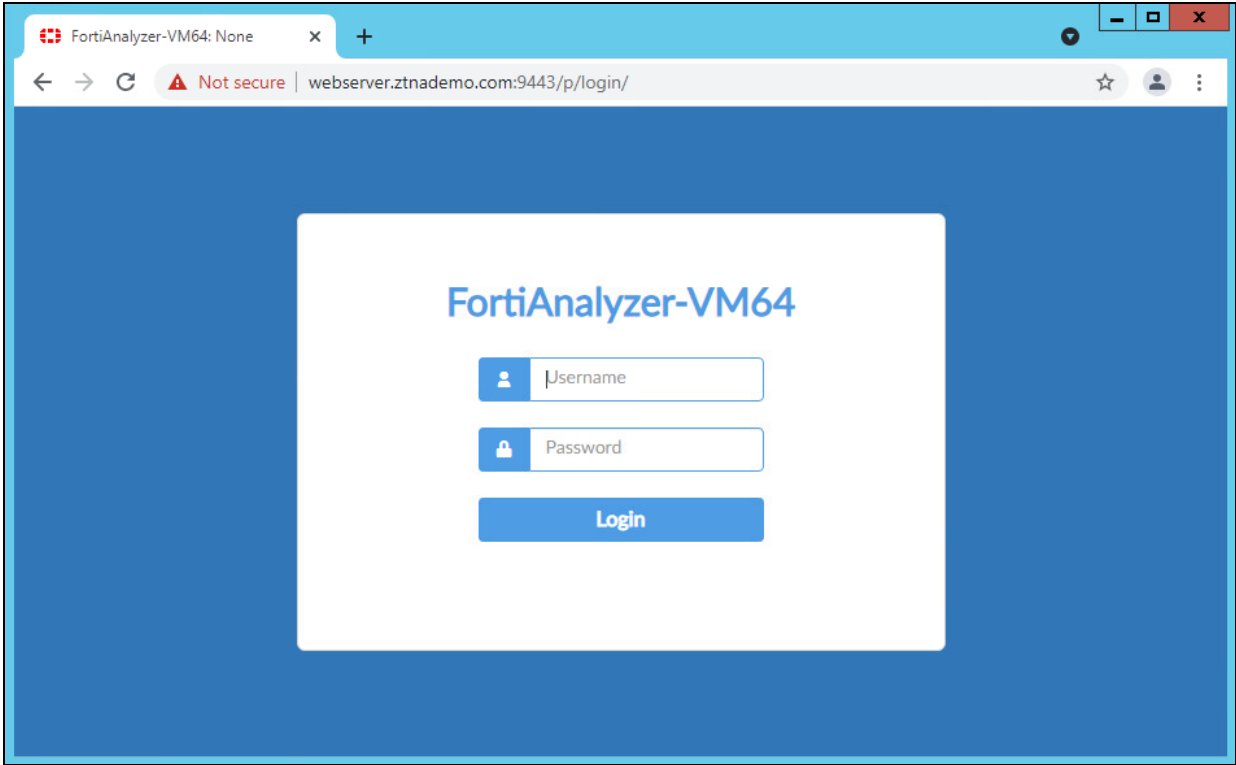
You will test the HTTPS access proxy connection for authorized and unauthorized users.

To test the connection for authorized users

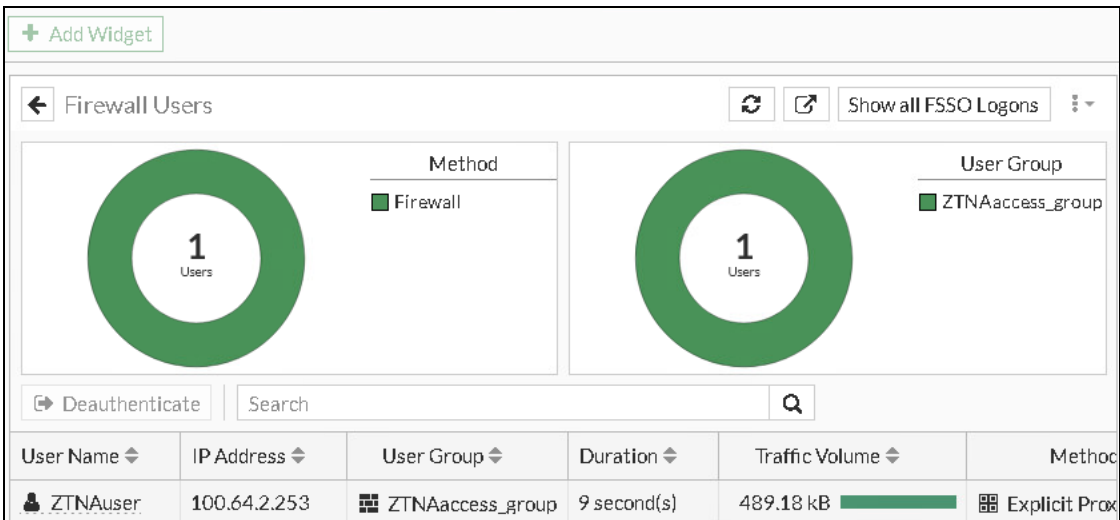
1. On the Remote-Client VM, open the Chrome browser from the desktop, and then type `https://webserver.ztnademo.com:9443`.
The browser prompts you for the client certificate to use.
2. Choose the EMS signed certificate, and then click **OK**.
3. When prompted for sign-in, type the **Username** `ZTNAuser` and **Password** `fortinet`, and then click **Sign in** to access the page.



After successful authentication, you can access the web page.



4. Close the browser.
5. On the AD Server VM, on the FortiGate GUI, click **Dashboard > Users & Devices**.
6. Open the **Firewall Users** widget to see the authenticated user.

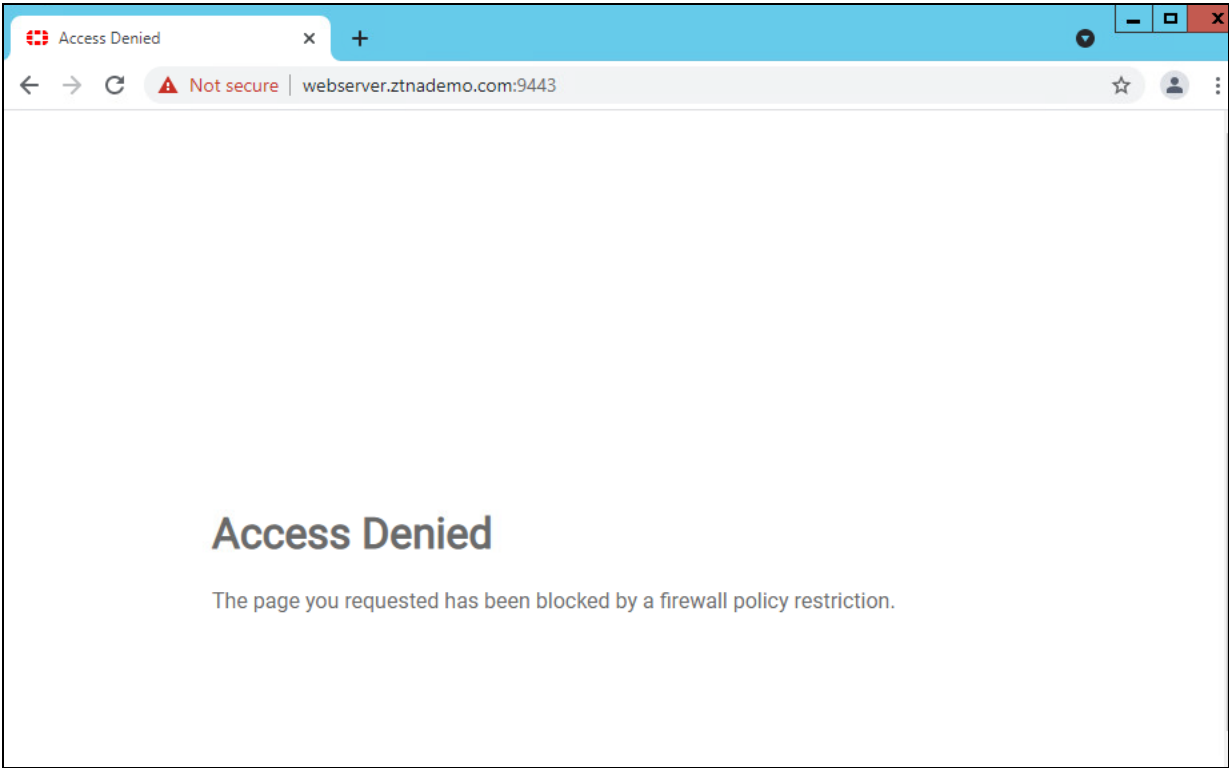


7. Select **ZTNAuser**, and then click **Deauthenticate** to remove the user from FortiGate.

To test the connection for unauthorized users

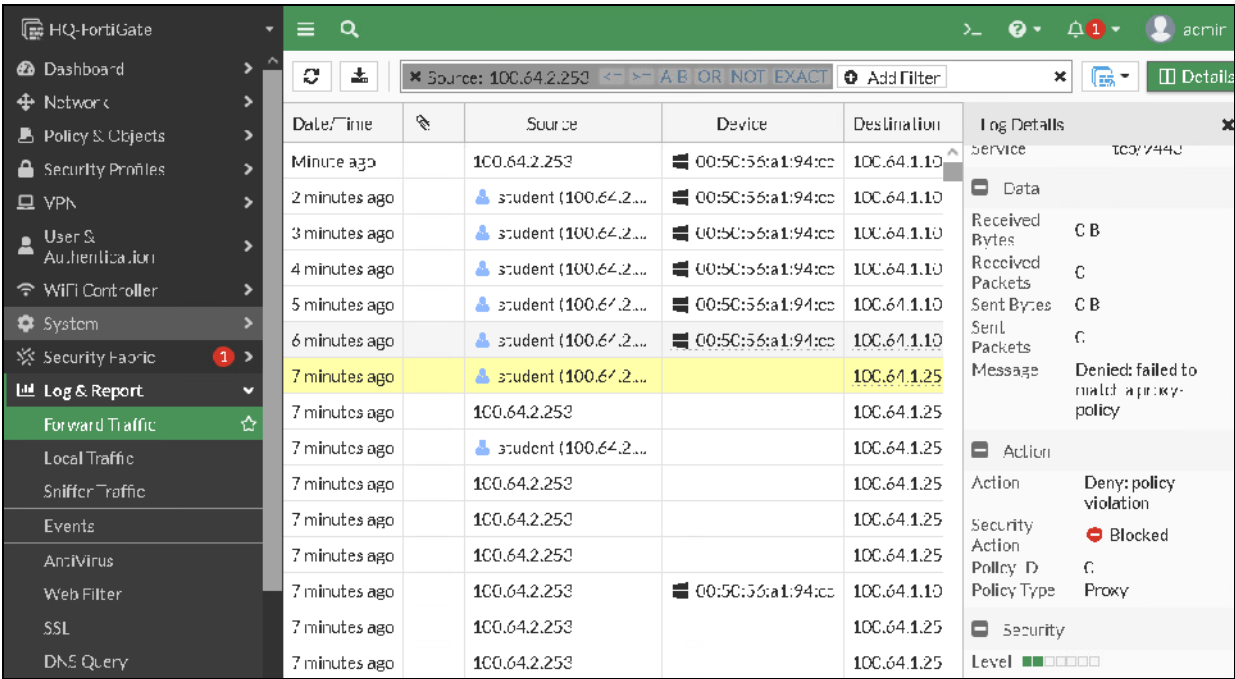
1. Repeat the previous steps to access `https://webserver.ztnademo.com:9443`.
The browser prompts you for the client certificate to use.

- 2. Choose the EMS signed certificate, and then click **OK**.
- 3. When prompted for sign-in, type the **Username** `student` and **Password** `fortinet`, and then click **Sign in** to access the page.



Access is denied because the user is not authorized to access the resource.

- 4. On the HQ-FortiGate GUI, click **Log & Report > Forward Traffic** to check the deny logs for the **student** user.



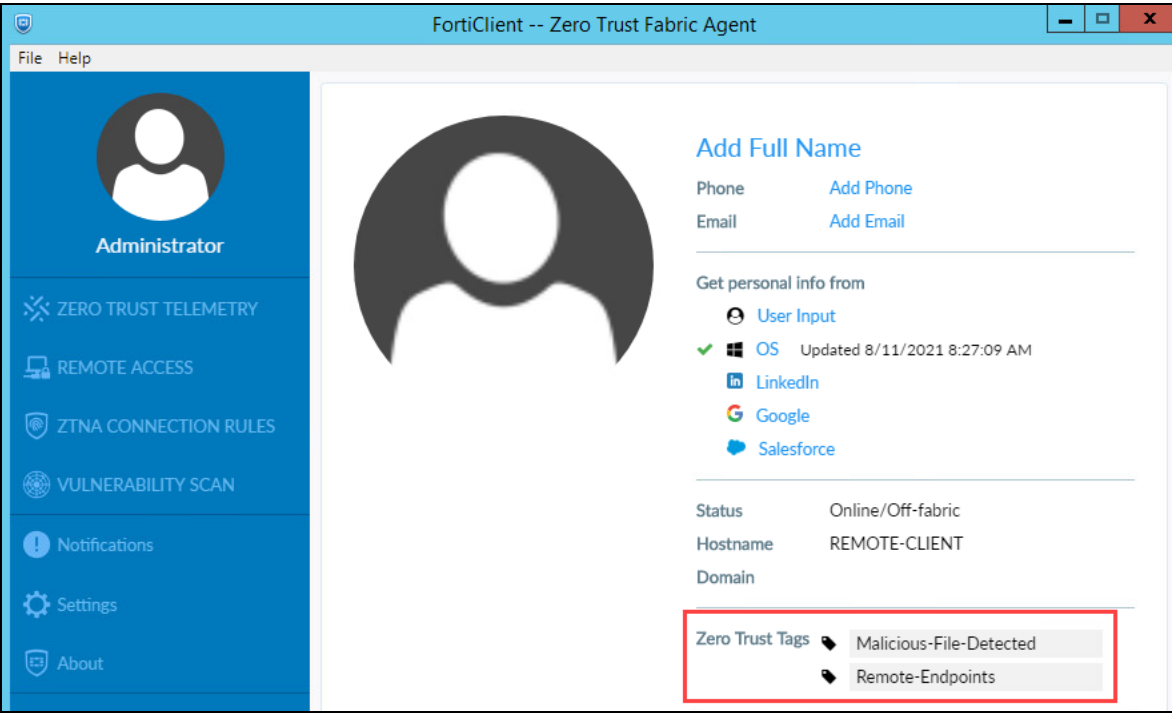
You may need to filter the **Source** IP address to 100.64.2.253 to see the related logs.

Verify the Behavior When the Security Posture Changes on the Endpoint

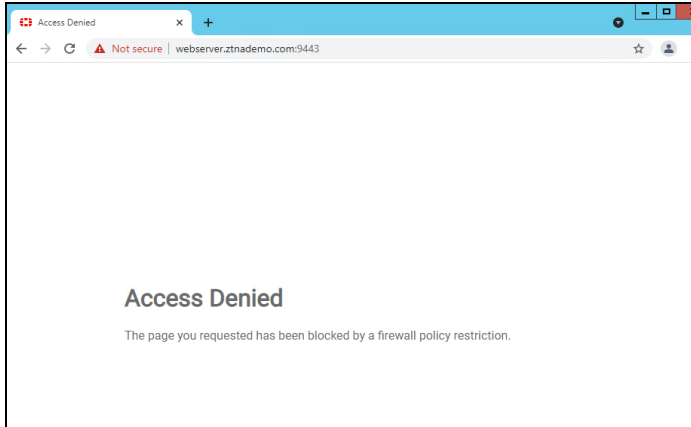
You will test a scenario where the endpoint security posture changed because of a malicious file. You will create a test virus file to trigger the ZTNA tag detection that you created in the previous exercise.

To detect a malicious file and tag an endpoint

1. On the Remote-Client VM, open Notepad, and then create a file with dummy text.
 2. On the C: drive, save the file as `virus`.
 3. Open the FortiClient console, and then click the avatar to view the detected tags.
- It may take a minute to see the updated tags.



4. On the desktop, open the Chrome browser, and then type `https://webserver.ztnademo.com:9443` to access the web page.



Access is denied because the endpoint security posture has changed.

5. On the C: drive, delete the file `virus`.
6. On the AD Server VM, on the FortiGate GUI, click **Dashboard > Users & Devices**.
7. Open the **Firewall Users** widget to see the authenticated user.
8. On the FortiGate GUI, select **student**, and then click **Deauthenticate** to remove the user from FortiGate.

Exercise 4: Configuring and Testing Compliance Rules to Create Dynamic Groups and Policies

In this exercise, you will create and test a firewall policy using ZTNA IP/MAC filtering. You will use an existing ZTNA tag to block endpoint access when a malicious file exists on the endpoint. ZTNA IP/MAC filtering mode enhances security when endpoints are physically on the corporate network, whereas full ZTNA mode focuses on access for remote users.

Create a Firewall Policy

To enforce compliance for local endpoints, you can select a ZTNA IP/MAC filtering option and apply a ZTNA tag to a firewall policy.

To create a new firewall policy to apply a ZTNA tag

1. On the HQ-FortiGate GUI, click **Policy & Objects > Firewall Policy**, and then click **Create New** to create a new firewall policy.
2. In the **New Policy** window, configure the following settings:

Field	Value
Name	Block-Malicious
ZTNA	Enable this option, and then select IP/MAC filtering .
ZTNA Tag	Malicious-File-Detected
Incoming Interface	port3
Outgoing Interface	port1
Source	all
Destination	all
Schedule	always
Service	ALL
Action	DENY
Enable this policy	<enable>

3. Click **OK** to add a new firewall policy.

Name: Block-Malicious

ZTNA: ☒ Full ZTNA **IP/MAC filtering**

ZTNA Tag: Malicious-File-Detected

Incoming Interface: LAN (port3)

Outgoing Interface: port1

Source: all

Destination: all

Schedule: always

Service: ALL

Action: ☒ ACCEPT ☒ DENY

☒ Log Violation Traffic

Comments: Write a comment... 0/1023

Enable this policy: ☒

OK

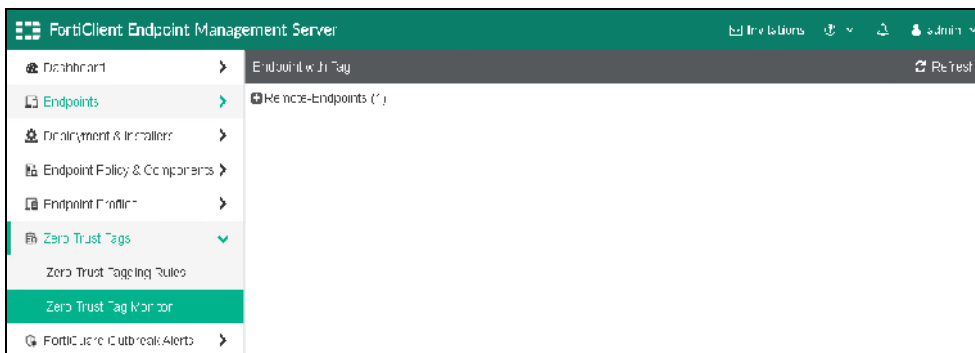
4. Move the **Block-Malicious** policy above the **IOC_Policy** policy at the top.

Test Endpoint Access Using the IP/MAC Filtering ZTNA Firewall Policy

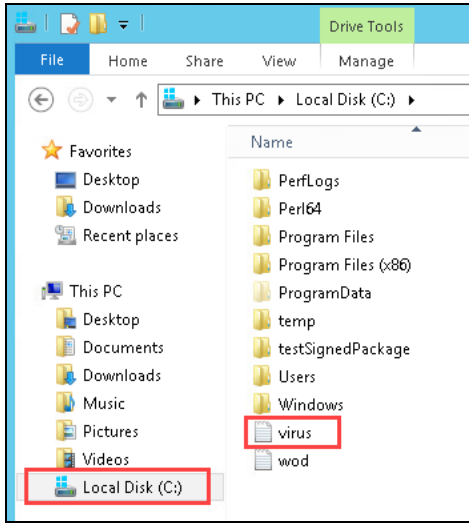
You will test endpoint access control with a ZTNA tag.

To test endpoint access using the IP/MAC filtering ZTNA firewall policy

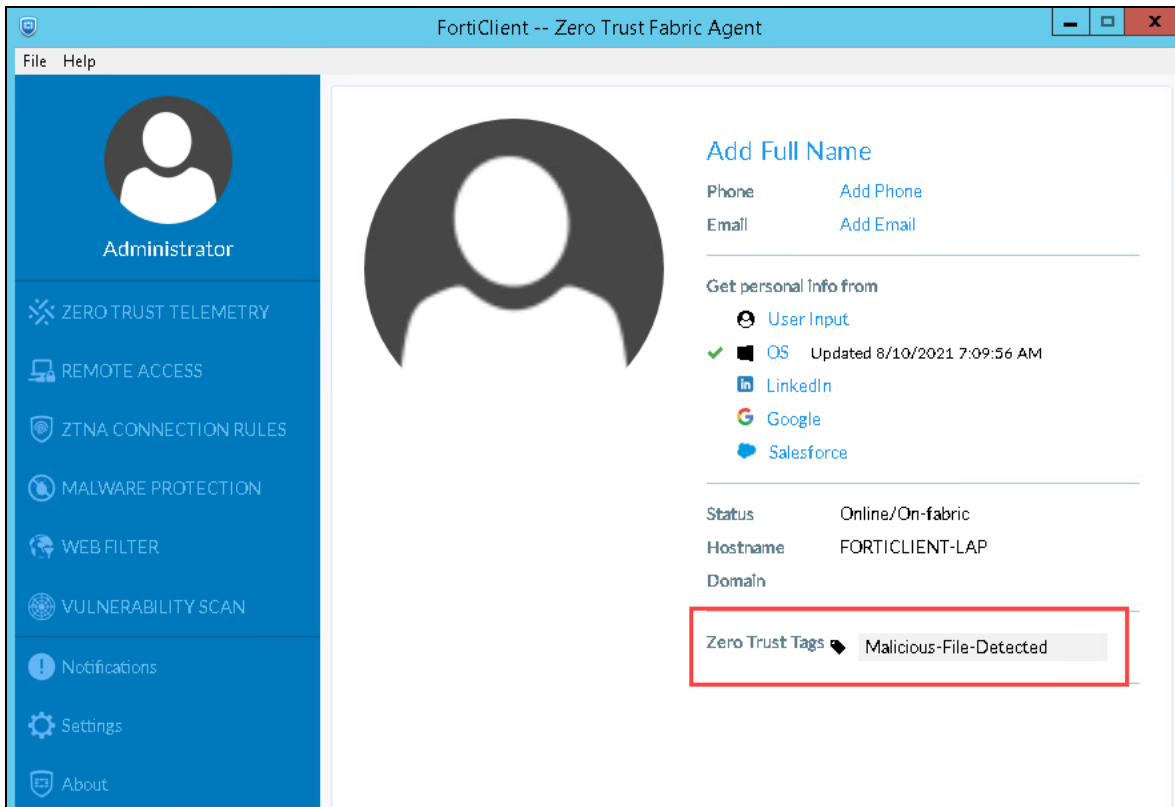
1. On the FortiClient-Laptop VM, ping IP 8.8.8.8 -t continuously to check connectivity to the internet. It must be allowed.
2. On the FortiClient EMS GUI, click **Zero Trust Tags > Zero Trust Tag Monitor**. There should not be any endpoints with the **Malicious-File-Detected** tag.



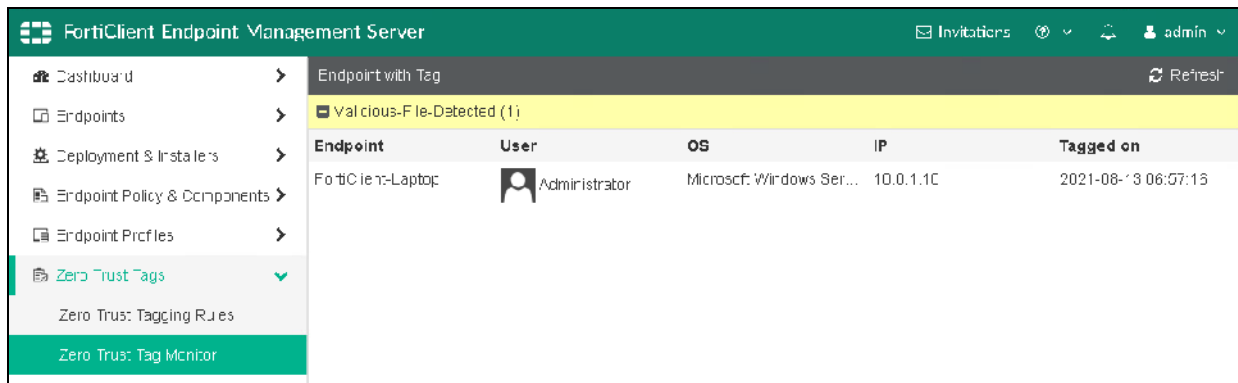
- On the FortiClient-Laptop VM, open Notepad, and then create a file with dummy text.
- On the C: drive, save the file as virus.



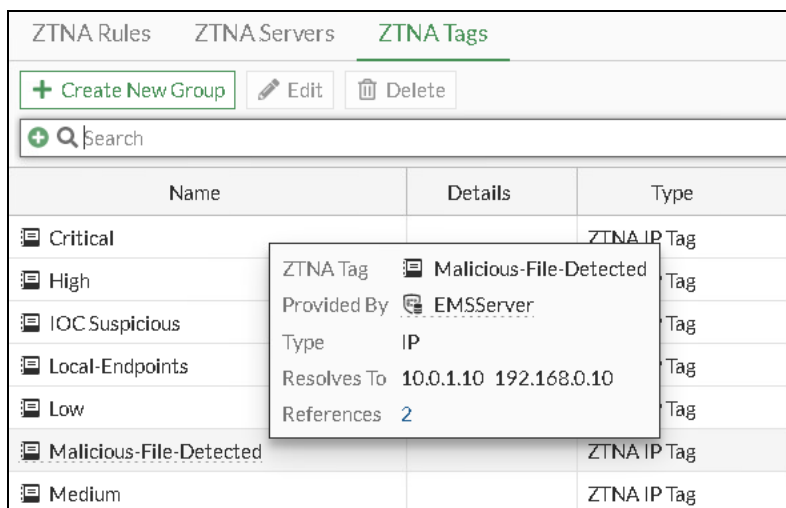
- Open the FortiClient console, and then click the avatar to view the detected tag. It may take a minute to see the updated tag.



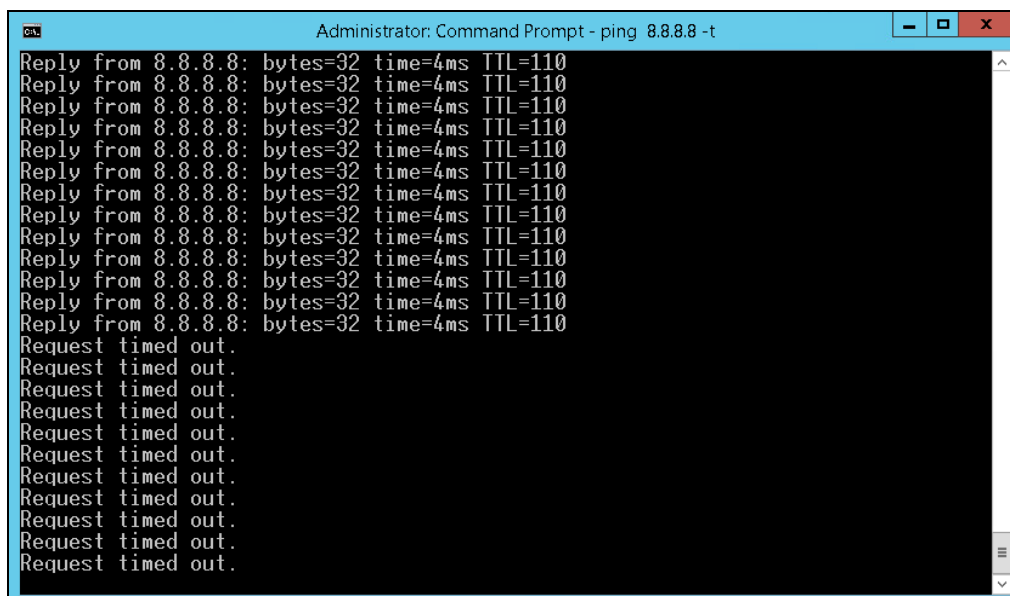
- On the FortiClient EMS GUI, click **Zero Trust Tags > Zero Trust Tag Monitor**. An endpoint appears on the **Malicious-File-Detected** tag.



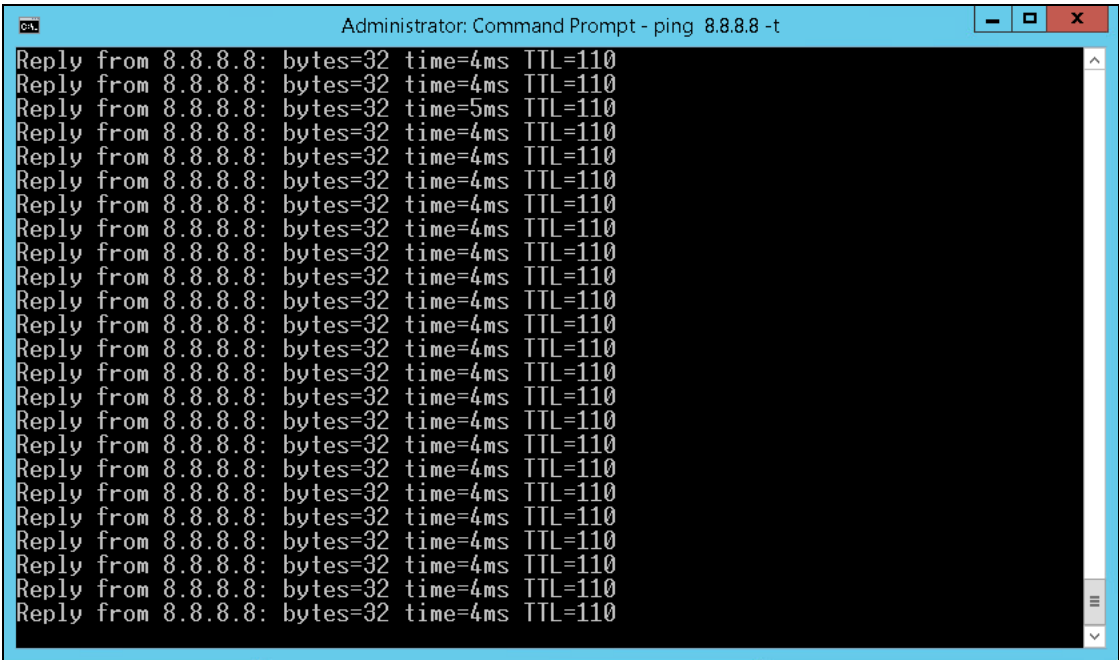
- On the HQ-FortiGate GUI, click **Policy & Objects > ZTNA**.
- Click **ZTNA Tags**, and then hover over the **Malicious-File-Detected** tag to see the endpoint details.



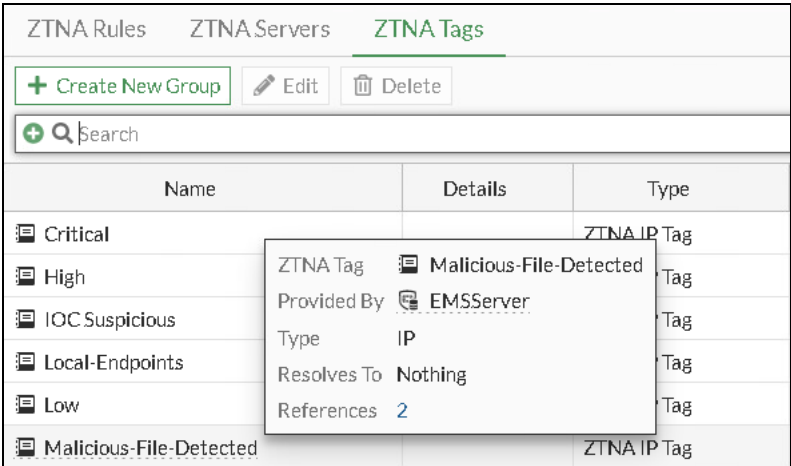
The endpoint IP address is shown. The ping should have stopped because the endpoint is tagged with a malicious file detection tag.



9. On the FortiClient-Laptop VM, on the C: drive, delete the virus file.
After some time, a ping should start.



10. On the AD Server VM, on the FortiClient EMS GUI, click **Zero Trust Tags > Zero Trust Tag Monitor**. There is no **Malicious-File-Detected** tag.
11. On the FortiGate GUI, click **Policy & Objects > ZTNA**.
12. Click **ZTNA Tags**, and then hover over the **Malicious-File-Detected** tag.
There is no IP address.



Lab 7: Diagnostics and Troubleshooting

In this lab, you will examine the files that are created by running the diagnostic tools of FortiClient and FortiClient EMS.

Objectives

- Run FortiClient and FortiClient EMS diagnostic tools

Time to Complete

Estimated: 20 minutes

Prerequisites

Before beginning this lab, you must finish the previous lab.

Exercise 1: Running Diagnostic Tools

In this exercise, you will run FortiClient and FortiClient EMS diagnostic tools on the FortiClient-Laptop VM and AD Server VM.

Run the FortiClient Diagnostic Tool

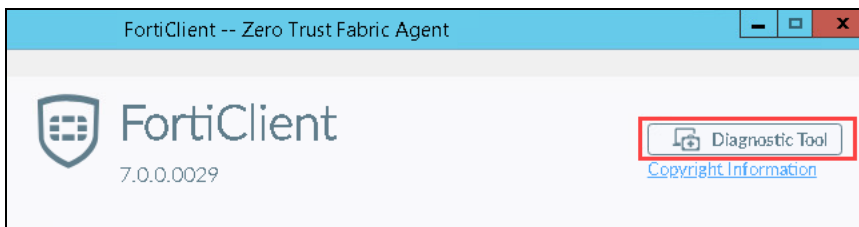
You will run the diagnostic tool on FortiClient endpoints to gather system information.



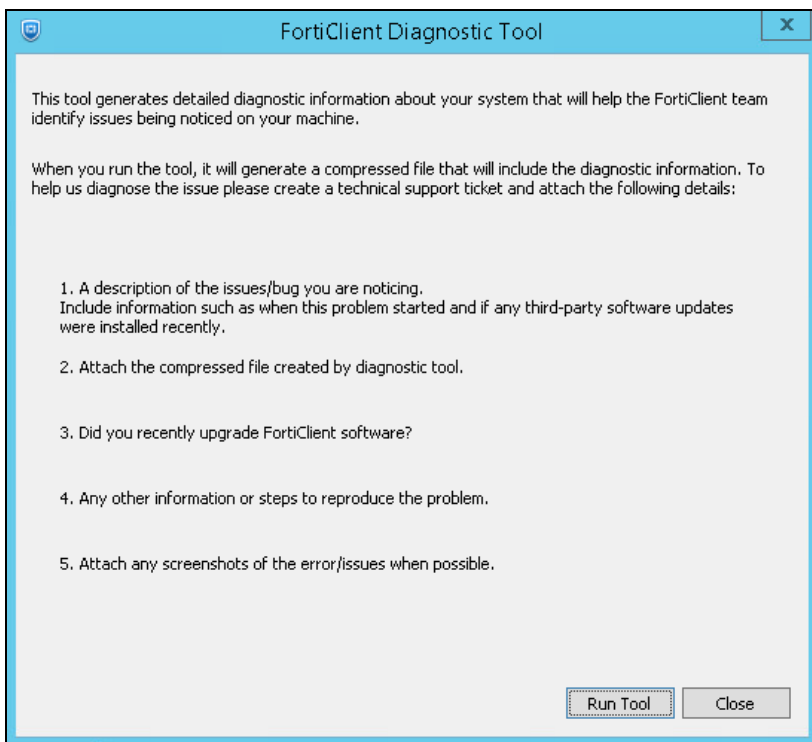
Before you run the diagnostic tool, you must change the FortiClient log level to **Debug**. On the FortiClient EMS GUI, click **Endpoint Profiles > Fortinet-Training**, click **Edit** on the **System Settings** tab, and then under **Log**, change the log level to **Debug**.

To run the FortiClient diagnostic tool from the FortiClient console

1. On the FortiClient-Laptop VM, open the FortiClient console.
2. Click **About**, and then click **Diagnostic Tool** to open the tool window.



3. In the **Diagnostic Tool** window, click **Run Diagnostic Tool**.
4. On the console, click **Run Tool**.



A command line window opens and the diagnostic tool runs tasks to collect system data.

```
task started: system information
task finished: system information
task started: Windows update log
task finished: Windows update log
task started: Windows mini dump files
task finished: Windows mini dump files
task started: product installation
task finished: product installation
task started: export logs
task finished: export logs
task started: FortiClient configuration
task finished: FortiClient configuration
task started: export registry values: Local Machine
task finished: export registry values: Local Machine
task started: export registry values: Current User
task finished: export registry values: Current User
task started: export registry values: Registered Class
task finished: export registry values: Registered Class
task started: list all installed softwares
task finished: list all installed softwares
task started: copy setupapi log file(s)
task finished: copy setupapi log file(s)
task started: collect FortiClient installation log file(s)
task finished: collect FortiClient installation log file(s)
task started: ipconfig
task finished: ipconfig
task started: routing table
task finished: routing table
task started: run ipsec tunnels
```

5. Press any key to continue the VPN diagnostics.

After all tasks are completed, the tool opens the

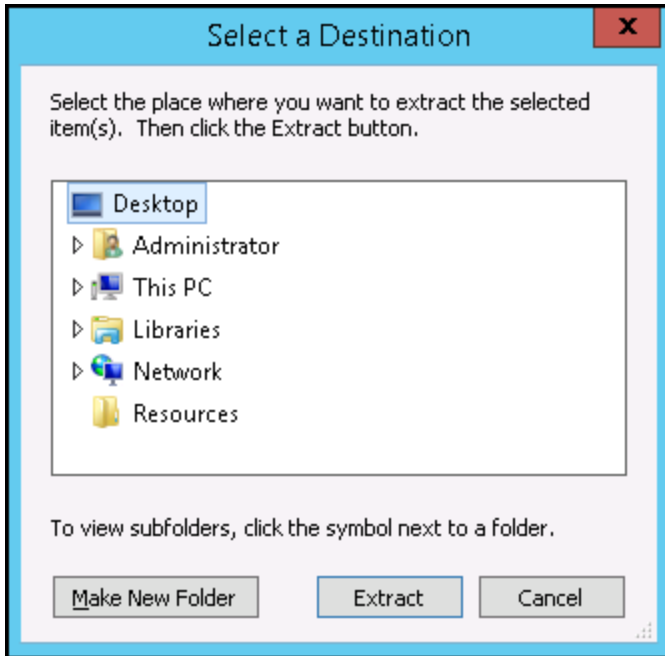
C:\Users\Administrator\AppData\Local\Temp\1\Diagnostic_Result link to show the Diagnostic_Result.zip file.

6. Click **Close** to close the diagnostic tool.
7. Extract the Diagnostic_Result.zip file, and then search for the SystemInfo.txt and ipconfig.txt files.



If Windows cannot extract or unzip the folder, you may need to use 7-Zip software to unzip a file. 7-Zip is installed on the VM.

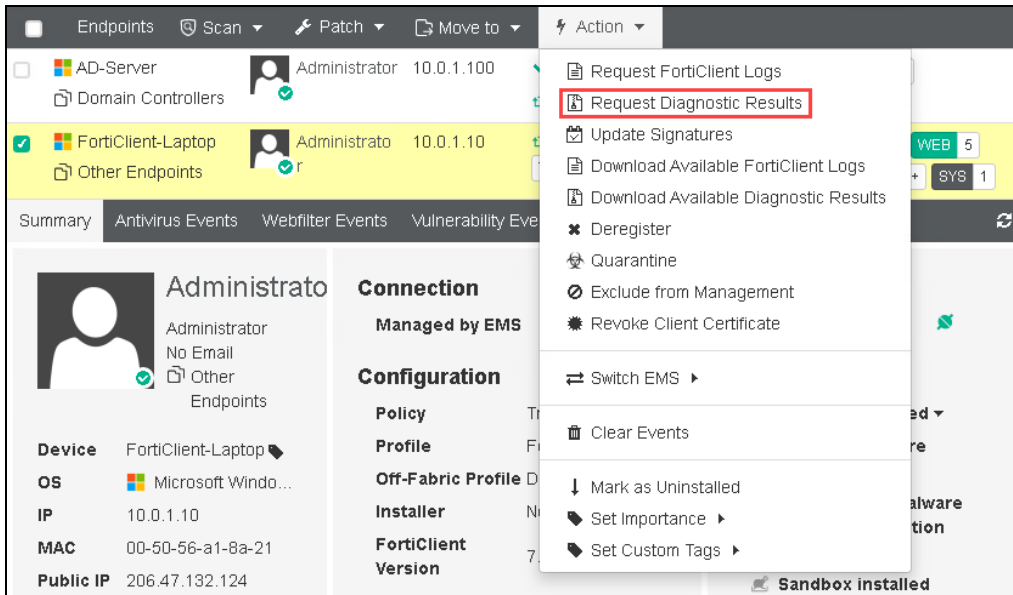
8. To review the file content, click these files. When you click a file, a window opens and extracts the file to a destination. Select **Desktop** for the destination.



Log files are compressed, so to read them, you must extract the files.

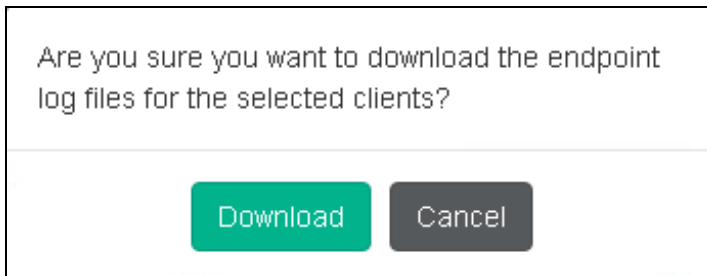
To run the FortiClient diagnostic tool from FortiClient EMS

1. On the AD-Server VM, log in to the FortiClient EMS GUI.
2. Click **Endpoints > All Endpoints**, and then select endpoint IP 10.0.1.10.
3. Click **Action**, and then select **Request Diagnostic Results** to run the tool on the selected endpoint.



The tool starts to run in the background. The file should be available after three keepalive cycles. The default is 60 seconds for each cycle.

- Continuing on the FortiClient EMS GUI, click **Action**, and then select **Download Available Diagnostics Results** to download the results file.



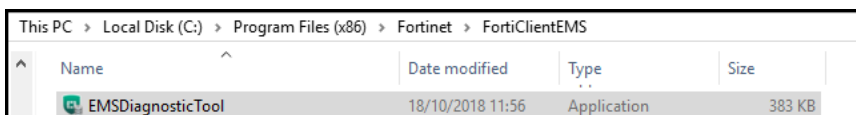
- Click **Save** again to download the file to the FortiClient EMS server download folder.

Run the FortiClient EMS Diagnostic Tool

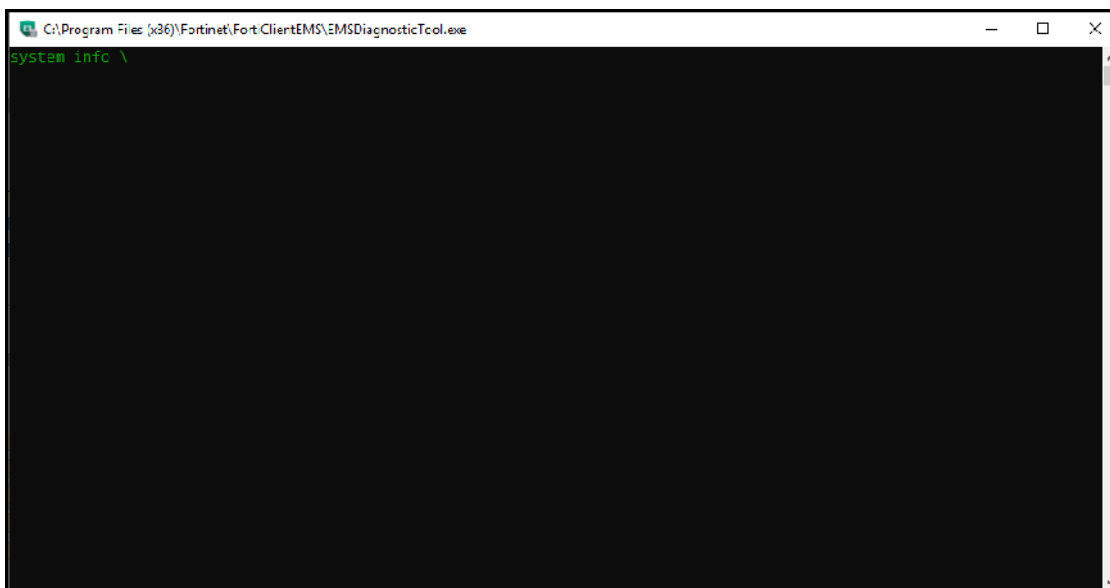
You will run the FortiClient EMS diagnostic tool on the AD server to gather information. Before you run the tool, you must change the FortiClient EMS log level to **DEBUG**.

To run the FortiClient EMS diagnostic tool

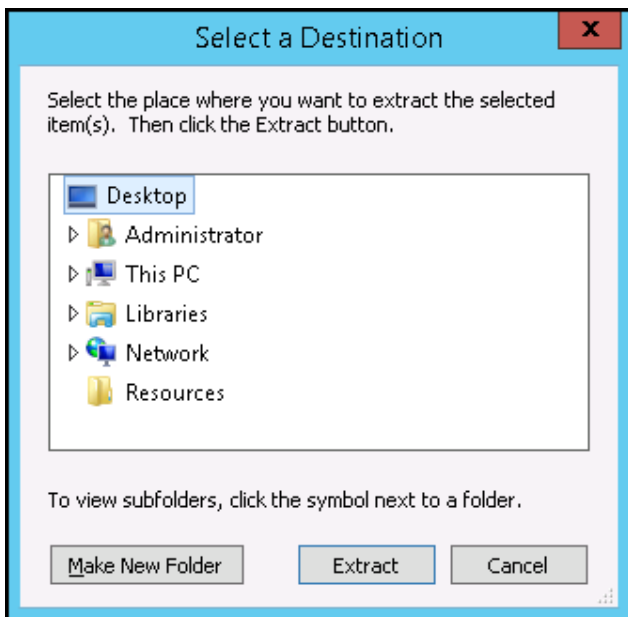
- On the AD server, go to the FortiClient EMS installation folder at the following location: C:\Program Files (x86)\Fortinet\FortiClientEMS.
- Search for the EMSDiagnosticTool file, and then double-click the file to run the tool.



A command line window opens and the diagnostic tool runs tasks to collect system data.



3. After all tasks are completed, the tool opens the `C:\Users\Administrator\AppData\Local\Temp\1` link to show the `forticlientems_diagnostic.zip` file.
4. Extract or unzip the `forticlientems_7.0.1.0103_diagnostic_<xxxxxxx-xxx-xxxx-xxxx-xxxxxxxx-xxxxxxx>.zip` file, and then search for the `SystemInfo.txt`, `events`, and `debug_xx-xx-xxxx` files.
5. To review the file content, click these files. When you click a file, a window opens and extracts the file to a destination. Select **Desktop** for the destination.



Log files are compressed, so to read them, you must extract the files.

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© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

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