

Exercise 7: Quarantining the Compromised Host

In this exercise, you will quarantine the compromised Windows client VM that was used to gain initial access to the network.


Quarantine the Compromised Host

You will configure playbooks to use FortiClient EMS to get endpoint information about the host, and use that information to quarantine the compromised host by running a second playbook.

To configure a playbook to quarantine an infected endpoint


1. Log in to the FAZ-SiteB GUI (10.200.4.238) with the following credentials:
- Username: admin
 - Password: Fortinet1!
2. Click **Fabric View**.
3. Click **Automation**.
4. Click the **Playbook** tab.
5. Click **Create New**.
6. Select **Quarantine Endpoint by EMS**.

Choose from Playbook Templates




Enrich Incident with Process List

Playbook to get running processes on endpoint by EMS connector and attach to incident.




Enrich Incident with Software Inventory

Playbook to get software inventory from endpoint by EMS Connector and attach to incident.




Enrich Incident with Vulnerability List

Playbook to collect the list of endpoint vulnerabilities from logs and attach to incident.



Quarantine Endpoint by EMS

Playbook to quarantine endpoint by EMS connector



Quarantine Endpoint by FortiOS

Playbook to quarantine endpoint by FOS connector providing MAC address or FortiClient UID

The playbook is automatically created with the required steps.

Edit Playbook

Name


Quarantine Endpoint by EMS - 2024-02-19 13:30:17


Description


Playbook to quarantine endpoint by EMS connector


Enabled

☒

 ON_DEMAND STARTER

 QUARANTINE Quarantine Endpoint

 ATTACH_DATA_TO_INCIDENT Attach Status


7. In the **Name** field, type Quarantine Endpoint by EMS.
8. Hover over the **Quarantine Endpoint** step, and then click the  icon to edit it.
9. Configure the following settings:

Field	Value
Name	Quarantine Endpoint

Field	Value
Description	Step to specify which endpoint to quarantine
Connector	EMS Connector
Action	Quarantine
site	Playbook Starter site
Endpoint ID	Playbook Starter epid
FortiClient ID	Playbook Starter fctuid

Quarantine Endpoint ✕

Name	Quarantine Endpoint		
Description	Step to specify which endpoint to quarantine		
Connector	<div>EMS Connector</div> <div>This connector is auto-selected. You must click "OK" and save playbook to apply this selection.</div>		
Action	Quarantine		
site ⓘ	Playbook Starter	site	A
Endpoint ID ⓘ	Playbook Starter	epid	A
FortiClient ID ⓘ	Playbook Starter	fctuid	A

- Click **OK**.
- Hover over the **Attach Status** step, and then click the  icon to edit it.
- Confirm that the **Attach Status** step configuration matches the following image:


Attach Status ✕

Name	Attach Status		
Description	Attach action status to incident		
Connector	Local Connector		
Action	Attach Data to Incident		
Incident ID ⓘ	Playbook Starter	incid	A
Attachment ⓘ	Quarantine Endpoint (ems_quarantine_endpoint)	status	A

- Click **OK**.
- Click **Save Playbook**.


To configure and run a playbook to retrieve asset information

- Continuing on the FAZ-SiteB GUI, click **Fabric View > Automation > Playbook**.
- Select the checkbox for the **Update Asset and Identity Database** playbook.

Summary	Connectors	Playbook	Playbook Monitor
<div> <div>+ Create New</div> <div>⌂ Run</div> <div>✎ Edit</div> <div>🗑 Delete</div> <div>✔ Enable</div> <div>⛔ Disable</div> <div>☰ More ▾</div> </div>			
	Name ⇅	Description ⇅	Status ⇅
<input type="checkbox"/>	Spear_Phishing_Attachment_Playbook	Custom build playbook to get started	✔ Enabled
<input checked="" type="checkbox"/>	Update Asset and Identity Database (EMS Connector)	Playbook to automatically update FortiAnalyzer Asset and Identity database with...	✔ Enabled
<input type="checkbox"/>	Get Vulnerabilities from EMS (EMS Connector)	Playbook to get vulnerabilities from EMS	✔ Enabled
<input type="checkbox"/>	Get Software Inventory from EMS (EMS Connector)	Playbook to get software inventory from EMS	✔ Enabled
<input type="checkbox"/>	SMTP Enumeration Incident_Playbook	Custom build playbook to get started	✔ Enabled
<input type="checkbox"/>	New Playbook created from scratch - 2024-02-19 12:40:17	Custom build playbook to get started	✔ Enabled

- Click **Run**.
- Click **OK**.

A confirmation that the playbook started should appear.


Started playbook Update Asset and Identity Database (EMS Connector)


- Click **Playbook Monitor**.
- Confirm that the playbook ran successfully.

Summary	Connectors	Playbook	Playbook Monitor
<div> <div>↻ Refresh</div> <div>🗑 Delete</div> </div>			
<input type="checkbox"/>	Job ID ⇅	Playbook ⇅	Trigger ⇅
<input type="checkbox"/>	2024-07-25 13:56:24-07	Update Asset and Identity Database (EMS Connector)	user(admin)

- Click **Fabric View > Asset Identity Center**.
- Click the **Asset Identity List** tab.

The **Asset Identity List** tab provides a list of all the assets that are currently connected in the Security Fabric and all third-party devices that are sending logs to FortiAnalyzer directly.

By running the **Update Asset and Identity Database** playbook, FortiAnalyzer used the FortiClient EMS connector to retrieve a list of all the FortiClient endpoints that the FortiClient EMS is provisioning and managing.



In the previous exercises, you noted that the WIN-CLIENT VM is being targeted during the persistence and evasion part of the attack. You will quarantine this compromised host.

- Make a note of the **FortiClient UUID** of the **WIN-CLIENT** VM.

Summary

Asset Identity List

Asset List

OT View

Last N Days

N = 60

2024-05-26 13:59:39 - 2024-07-25 13:59:39

Custom View

Reload

More

Asset

Iden

Endpoint Name	Tags	User	MAC Address	IP Address	FortiClient UUID
WIN-AD	<div><div></div>all_registered_clients</div>	<div><div></div>Administrator</div> <div><div></div>bob</div>	00:0c:29:ba:2f:d1	10.200.3.1	32624B6F96834BE09A02F41A2C536430
WIN-CLIENT	<div><div></div>all_registered_clients</div>	<div><div></div>student</div> <div><div></div>bob</div>	00:0c:29:eb:74:13	10.200.3.219	66BE205CCA864B23B55E40C61350DE99

To quarantine the infected host

- Continuing on the FAZ-SiteB GUI, click **Fabric View > Automation > Playbook**.
- Select the checkbox for **Quarantine Endpoint by EMS**.
- Click **Run**.

Summary		Connectors		Playbook		Playbook Monitor							
<div>+ Create New</div>		<div>⏮ Run</div>		<div>✎ Edit</div>		<div>🗑 Delete</div>		<div>✔ Enable</div>		<div>⏮ Disable</div>		<div>☰ More ▾</div>	
<div><input type="checkbox"/></div>		Name ▴▾				Description ▴▾				Status ▴▾			
<div><input type="checkbox"/></div>		Get Software Inventory from EMS (EMS Connector)				Playbook to get software inventory from EMS				<div>✔ Enabled</div>			
<div><input type="checkbox"/></div>		Get Vulnerabilities from EMS (EMS Connector)				Playbook to get vulnerabilities from EMS				<div>✔ Enabled</div>			
<div><input checked="" type="checkbox"/></div>		Quarantine Endpoint by EMS				Playbook to quarantine endpoint by EMS connector				<div>✔ Enabled</div>			

The **Manually Run Playbook Quarantine Endpoint by EMS** window opens.

4. Configure the following settings:

Field	Value
Endpoint	WIN-CLIENT (1034)
site	default
fctuid	66BE205CCA864B23B55E40C61350DE99 IN00000002
incid	(Your incident ID may differ. Type the incident number that the Spear_Phishing_Attachment_Playbook created).

Manually Run Playbook Quarantine Endpoint by EMS

Endpoint

WIN-CLIENT (1034)

site

default

fctuid

66BE205CCA864B23B55E40C61350DE99

incid

IN00000002

- 5. Click **OK**.
- 6. Click **Playbook Monitor**.
- 7. Click the **Quarantine Endpoint by EMS** playbook.
- 8. Confirm that both tasks ran successfully.

Playbook Tasks					
🔄 Refresh	📄 View Raw Log	Search...			
<input type="checkbox"/>	Task ID ↕	Task ↕	Start Time ↕	End Time ↕	Status ↕
<input type="checkbox"/>	faz_attach_action_status_to_incident	Attach Status	2024-07-25 17:06:30-0700	2024-07-25 17:06:30-0700	success
<input type="checkbox"/>	ems_quarantine_endpoint	Quarantine Endpoint	2024-07-25 17:06:27-0700	2024-07-25 17:06:29-0700	success

9. Close the **Playbook Tasks** window.

Confirm Endpoint Quarantine

You will confirm that the Windows-Client VM is quarantined.

To confirm endpoint quarantine

- 1. On the bastion host, on the desktop, double-click the Windows-Client RDP shortcut (**Windows-Client.rdp**).

The connection attempt will fail.

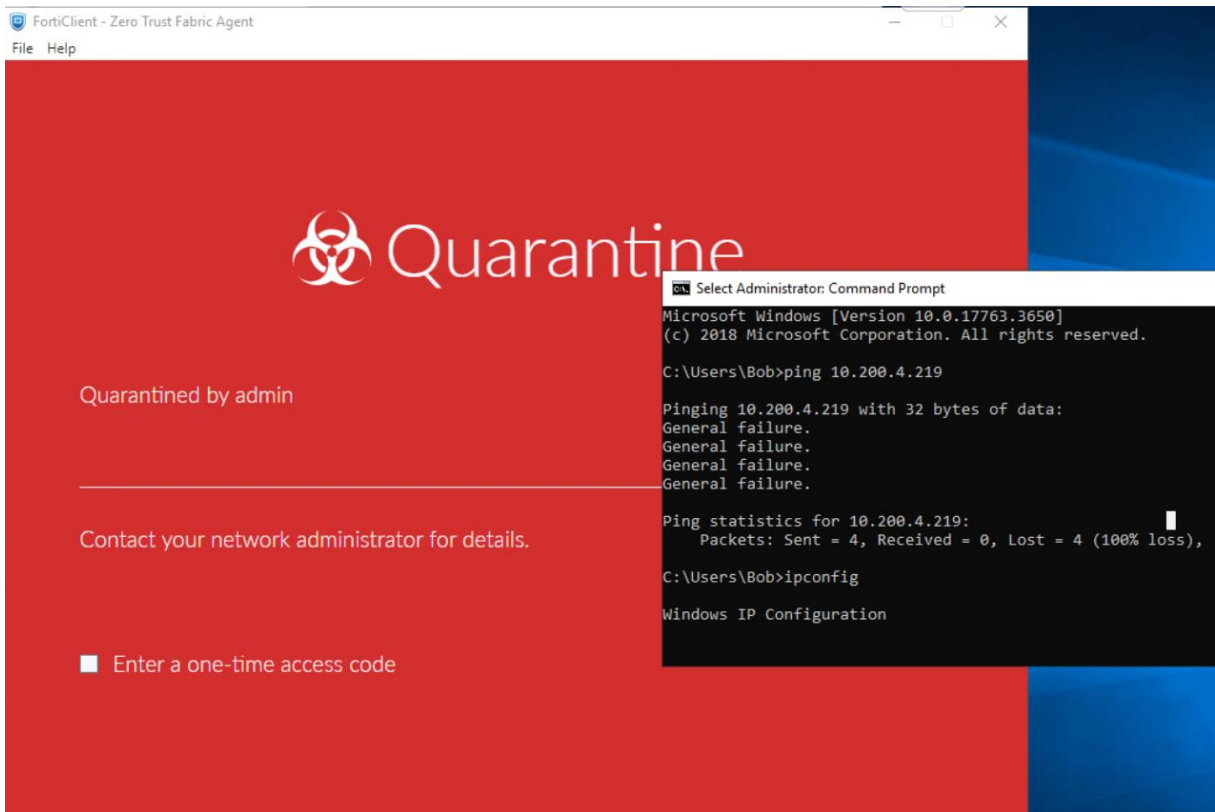
Stop and think!

Why is the RDP connection failing?

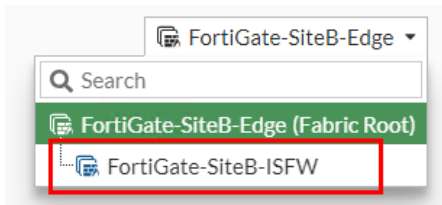
FortiClient EMS has locked down the compromised client, which prevents it from accessing the network.

Using an ESXi console connection, you can see the quarantined status of the client VM. The steps are not shown. The image below is for demonstrating what you would see *if* you logged in to the console.

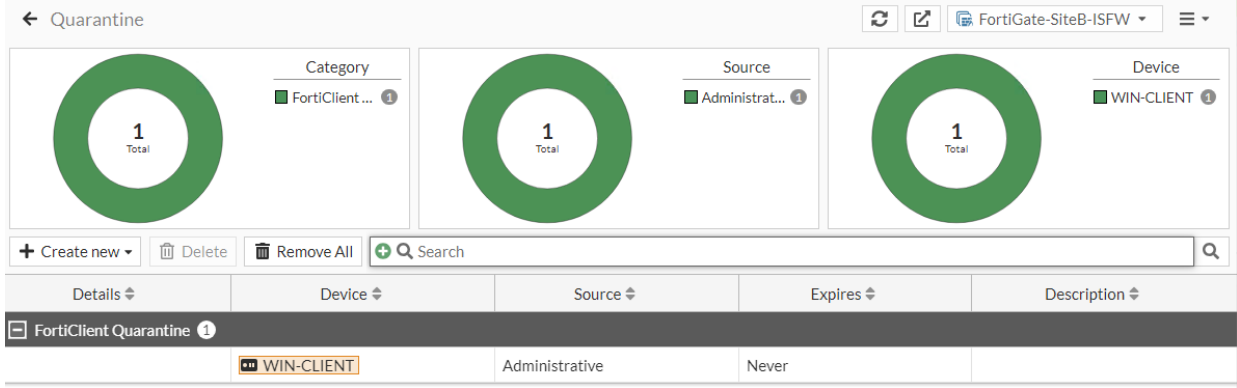
You do *not* need to log in to the console. Proceed to the next step.




2. Return to the bastion host, and then in Chrome, log in to the FortiGate-SiteB-Edge (10.200.4.249) GUI with the following credentials:
 - Username: admin
 - Password: Fortinet1!
3. Click **Dashboard**.
4. Click **Assets & Identities**.
5. In the **FortiGate-SiteB-Edge** drop-down list, select **FortiGate-SiteB-ISFW**.



6. Click the **Quarantine** widget.
7. Notice the quarantined host and the user that performed this action.



Now that the host has been quarantined, the adversary Group ABC cannot perform any further actions on the infected host, such as lateral movement across the network to infect or compromise a critical server.

 Performing remediation actions on the infected host is beyond the scope of this lab. Once you have cleaned the infected host and deleted the malware from it, you can release the host from quarantine using FortiAnalyzer.

Release the VM From Quarantine

You will run a second playbook on FAZ-SiteB to release the host from quarantine.

To configure the playbook to release the host from quarantine

- 1. Return to the FAZ-SiteB GUI, and then click **Fabric View > Automation > Playbook**.
- 2. Click **Create New**.
- 3. In the **Choose from Playbook Templates** section, select **Unquarantine Endpoint EMS**.
- 4. In the **Name** field, type Unquarantine Endpoint by EMS.
- 5. Edit the **Unquarantine Endpoint** step.
- 6. Configure the following settings:

Field	Value
Name	Unquarantine Endpoint
Connector	EMS Connector
Action	Unquarantine
site	Playbook Starter site
Endpoint ID	Playbook Starter epid
FortiClient ID	Playbook Starter fctuid

Unquarantine Endpoint

Name

Unquarantine Endpoint

Description

Connector

EMS Connector

This connector is auto-selected. You must click "OK" and save playbook to apply this selection.

Action

Unquarantine

site

Playbook Starter

site

A

Endpoint ID

Playbook Starter

epid

A

FortiClient ID

Playbook Starter

fctuid

A

- 7. Click **OK**.

Edit Playbook

Name

Unquarantine Endpoint by EMS

Description

Playbook to unquarantine endpoint by EMS connector

Enabled

ON_DEMAND STARTER

UNQUARANTINE Unquarantine Endpoint

ATTACH_DATA_TO_INCIDENT Attach Status

Save Playbook

Cancel

8. Click **Save Playbook**.
9. Select **Unquarantine Endpoint by EMS** playbook.
10. Click **Run**.

The **Manually Run Playbook Unquarantine Endpoint by EMS** window opens.

11. Configure the settings:

Field	Value
Endpoint	WIN-CLIENT (1034)
fctuid	66BE205CCA864B23B55E40C61350DE99
site	default
incid	IN00000002
	(Your incident ID may differ. Type the incident number that the Spear_Phishing_Attachment_Playbook created).

Manually Run Playbook Unquarantine Endpoint by EMS

Endpoint

WIN-CLIENT (1034)

fctuid

66BE205CCA864B23B55E40C61350DE99

site

default

incid

IN00000002

12. Click **OK**.
13. Click **Playbook Monitor**.
14. Click **Unquarantine Endpoint by EMS**.
15. Confirm that the playbook tasks ran successfully.

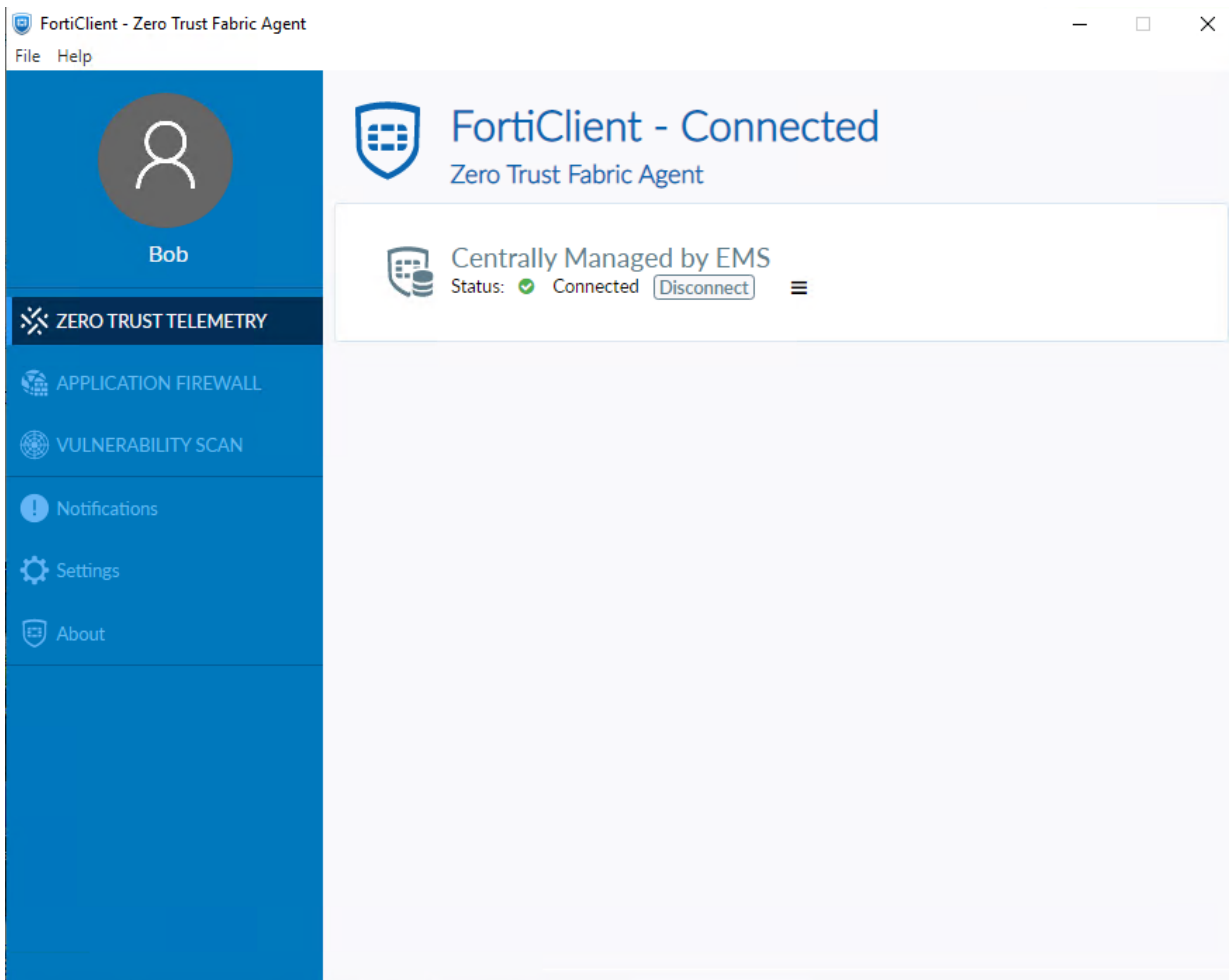
Refresh		View Raw Log		Search...	
<input type="checkbox"/>	Task ID	Task	Start Time	End Time	Status
<input type="checkbox"/>	ems_unquarantine_endpoint	Attach Status	2024-07-25 17:38:15-0700	2024-07-25 17:38:15-0700	success
<input type="checkbox"/>	unquarantine_endpoint	Unquarantine Endpoint	2024-07-25 17:38:11-0700	2024-07-25 17:38:13-0700	success

16. Close the **Playbook Tasks** window.

To confirm that the host was released from quarantine

1. On the bastion host, on the desktop, double-click the Windows-Client RDP shortcut (**Windows-Client.rdp**).
2. Log in with the following credentials:
 - Username: bob
 - Password: Passw0rd
3. Open the FortiClient console, and then verify that the host is released from quarantine.

You should see that the FortiClient console has returned to its original state and is not red (quarantine).



LAB-CHALLENGE > Quarantining the Compromised Host