

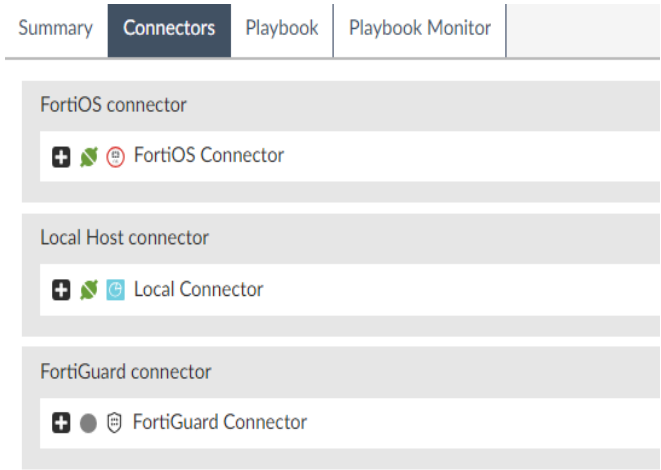
Exercise 1: Configuring Connectors

In this exercise, you will configure the EMS connector on FortiAnalyzer to receive endpoint inventory updates and perform quarantine and unquarantine actions on endpoints using FortiClient EMS.

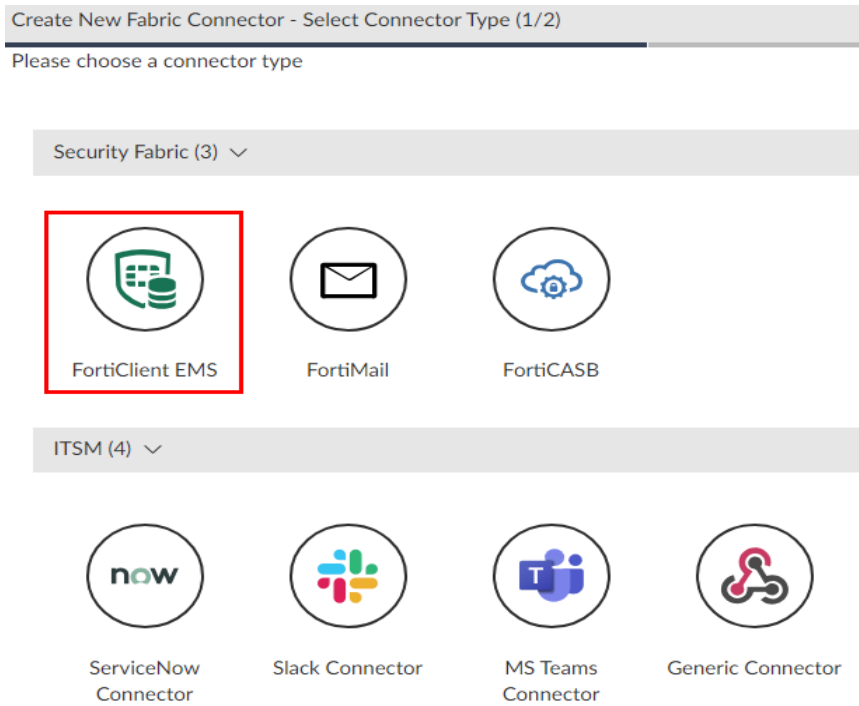
To configure the EMS connector

1. On the bastion host, in Chrome, log in to the FAZ-SiteB GUI (10.200.4.238) with the following credentials:
 - Username: admin
 - Password: Fortinet1!
2. Click **Fabric View > Automation > Connectors**.

Notice that the FortiClient EMS connector is not listed.



3. Click **Fabric View > Fabric Connectors**.
4. Click **Create New**.
5. In the **Create New Fabric Connector - Select Connector Type (1/2)** window, select **FortiClient EMS**.



6. On the **Configuration** tab, configure the following settings:

Field	Value
Type	FortiClient EMS

Field	Value
Name	EMS Connector
IP/FQDN	10.200.3.1
User Name	admin
Password	Fortinet1!
Status	Enabled

Create New Fabric Connector - FortiClient EMS (2/2)

Configuration

Action

Connector Settings

Type

FortiClient EMS

FortiClient EMS Cloud

Name

EMS Connector

Description

Connector to execute remote EMS operations

42/256

FortiClient EMS

IP/FQDN

10.200.3.1

User Name

admin

Password

Fortinet1!

ⓧ 🔒

Status

Notice that when you configure the FortiClient EMS connector, FortiAnalyzer automatically creates three playbooks.

The following playbooks will be created for the connector:

- Update Asset and Identity Database
- Get Vulnerabilities from EMS
- Get Software Inventory from EMS

Back

OK

Cancel

- Click the **Action** tab.
- Review all the actions that you can perform using the FortiClient EMS connector from FortiAnalyzer.

Configuration


Action


Search...				
Status ▾	Name ▾	Description ▾	Filters/Parameters ▾	⚙
Enabled	GET_ENDPOINTS	retrieve list of endpoints and all of th...	filter.ip: filter.group:	
Enabled	QUARANTINE	quarantines endpoints	id: cmd:	
Enabled	UNQUARANTINE	unquarantines endpoints	id: cmd:	
Enabled	GET_SOFTWARE_INVENTORY	retrieve list of software and apps inst...	id: cmd:	
Enabled	VULN_SCAN	run vulnerability scan on endpoints	id: cmd: vuln_scan	
Enabled	AV_QUICK_SCAN	run quick av scan on endpoints	id: cmd: av_quick_scan	
Enabled	AV_FULL_SCAN	run full av scan on endpoints	id: cmd: av_full_scan	
				0% 10


- Click **OK**.

Your configuration should match the following example:


+ Create New

 Edit


 Delete

 Clone

Security Fabric (1)



FortiClient EMS



EMS Connector

LAB-4 > Configuring Connectors