

Security Operations Analyst

SOC Automation

Lesson Overview



Configuring Connectors



Configuring Connectors



Objectives

- Describe connector types
- Configure connector actions

Connectors

- Allow playbooks to interact with devices in the Security Fabric and other standalone devices
- Determine which actions can be performed by playbook tasks
- The local connector does not need any additional configuration
 - All other connector types must be configured
- The connector status icon is colour coded:
 - **Green**: connection successful
 - **Black**: connection unknown
 - **Red**: connection down

Fabric View > Automation > Connectors

FortiOS connector

FortiOS Connector

Training-Lab

Automation Rule	Automation Action(s)	Parameters
Lab5 webhook disable FW policy	Lab 5 disable firewall policy	policyid
Lab5 webhook enable FW policy	Lab 5 enable firewall policy	policyid

Local Host connector

Local Connector

FortiGuard connector

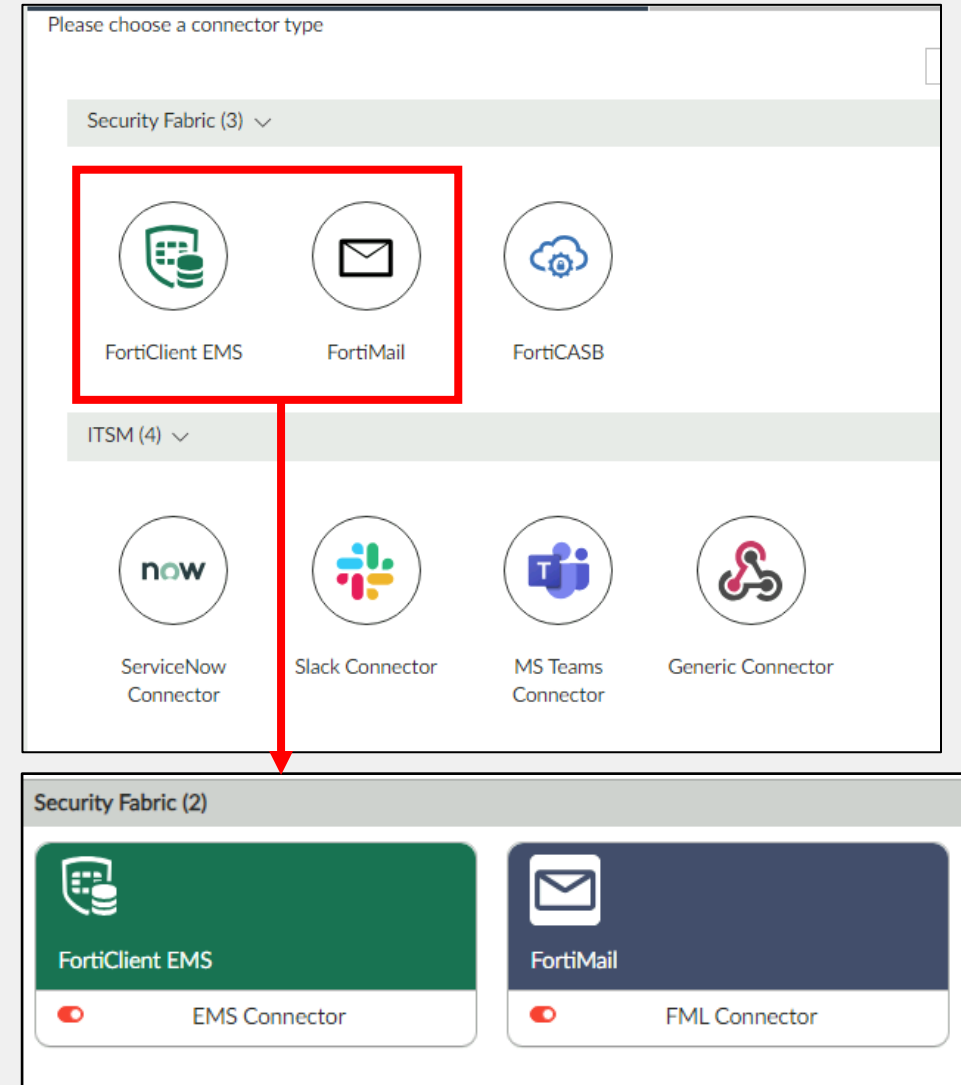
FortiGuard Connector

Status icon

Connector Types

- Two types of connectors
 - Security Fabric
 - ITSM
- Security Fabric connectors:
 - FortiClient EMS
 - FortiMail
 - FortiCASB
- ITSM connectors:
 - Service Now
 - Slack
 - MS Teams
 - Generic: Support additional third-party ticketing platforms

Fabric View > Fabric Connectors



Connector Actions

- Connector actions are automated
- Each connector has its own set of actions
- Connector actions are predefined

Fabric View > Fabric Connectors

Configuration			
Action			
Search...			
Status ▾	Name ▾	Description ▾	Filters/Parameters ▾ ⚙
Enabled	AV_FULL_SCAN	run full av scan on endpoints	id: cmd: av_full_scan
Enabled	AV_QUICK_SCAN	run quick av scan on endpoints	id: cmd: av_quick_scan
Enabled	GET_ENDPOINTS	retrieve list of endpoints and all of th...	filter.ip: filter.group:
Enabled	GET_PROCESSES	retrieve list of running process on en...	id: cmd:
Enabled	GET_SOFTWARE_INVENTORY	retrieve list of software and apps inst...	id: cmd:
Enabled	QUARANTINE	quarantines endpoints	id: cmd:
Enabled	TAG_ENDPOINTS	tag endpoints on EMS	id: cmd:
Enabled	UNQUARANTINE	unquarantines endpoints	id: cmd:
Enabled	UNTAG_ENDPOINTS	untag endpoints on EMS	id: cmd:
Enabled	VULN_SCAN	run vulnerability scan on endpoints	id: cmd: vuln_scan
100% 1			

FortiClient EMS
connector actions

Configuration			
Action			
Search...			
Status ▾	Name ▾	Description ▾	Filters/Parameters ▾ ⚙
Enabled	GET_EMAIL_STATISTICS	retrieve information of e...	id: cmd:
Enabled	GET_SENDER_REPUTA...	retrieve information suc...	id: cmd:
Enabled	ADD_SENDER_TO_BLO...	disard email received fro...	id: cmd:
99% 3			

FortiMail
connector
actions

Use Case

Fabric View > Automation > Playbooks

Name

Quarantine Endpoint by EMS

Description

Playbook to quarantine endpoint by EMS connector

Enabled

ON_DEMAND STARTER

1

QUARANTINE
Quarantine Endpoint

ATTACH_DATA_TO_INCIDENT
Attach Status

Manually Run Playbook Quarantine Endpoint by EMS

Endpoint

WIN (1031)

site

default

fctuid

CDABAF17B3724E72AA20B3D6E4B26948

incid

IN00000003

Playbook Tasks

Refresh

View Raw Log

Search...

<input type="checkbox"/>	Task ID	Task	Status	Raw Log
<input type="checkbox"/>	faz_attach_action_status_to_incident	Attach Status	success	Unavailable
<input type="checkbox"/>	ems_quarantine_endpoint	Quarantine Endpoint	success	Unavailable

Infected host is quarantined

Quarantine

Quarantined by admin

Contact your network administrator for details.

Fabric View > Automation > Playbook Monitor

Job ID	Playbook	Trigger	Start Time	End Time	Status
2024-03-13 19:07:07-07	Quarantine Endpoint by EMS	user(admin)	2024-03-13 19:07:11-0700	2024-03-13 19:24:11-0700	✔ success(Scheduled:0/Running:0/Succes

Knowledge Check

1. Which connector requires additional configuration?

- ✓ A. FortiOS connector
- B. Local connector

2. Which connector type allows integration with third-party ticketing applications?

- A. Security Fabric
- ✓ B. ITSM

Review

- ✓ Configure connector actions