FORTINET
Training Institute

FORTINET
CERTIFIED
SOLUTION
SPECIALIST
Security
Operations

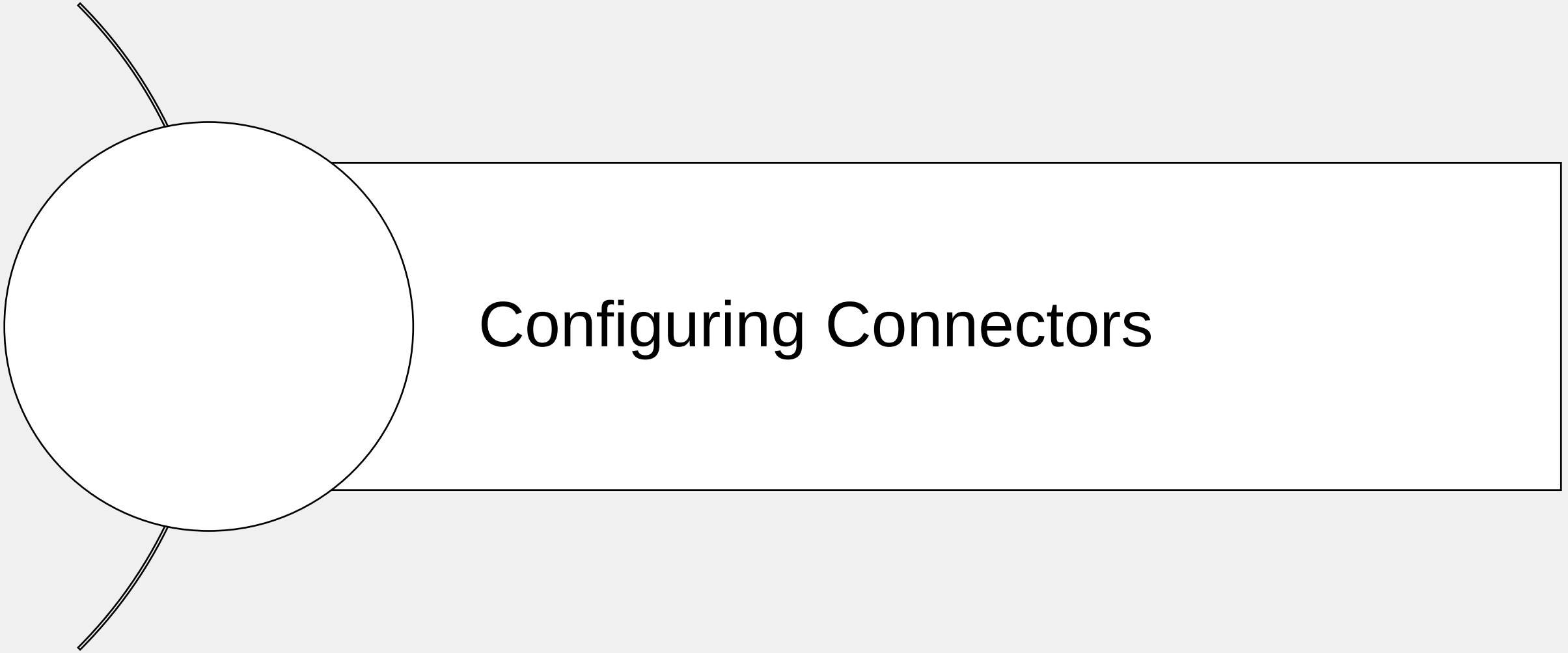
Security Operations Analyst

SOC Automation

FortiAnalyzer 7.4

Last Modified: 21 January 2025

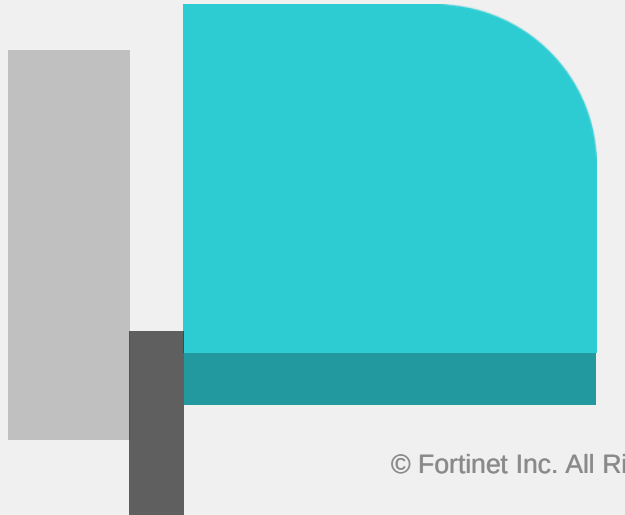
Lesson Overview



Configuring Connectors

Objectives

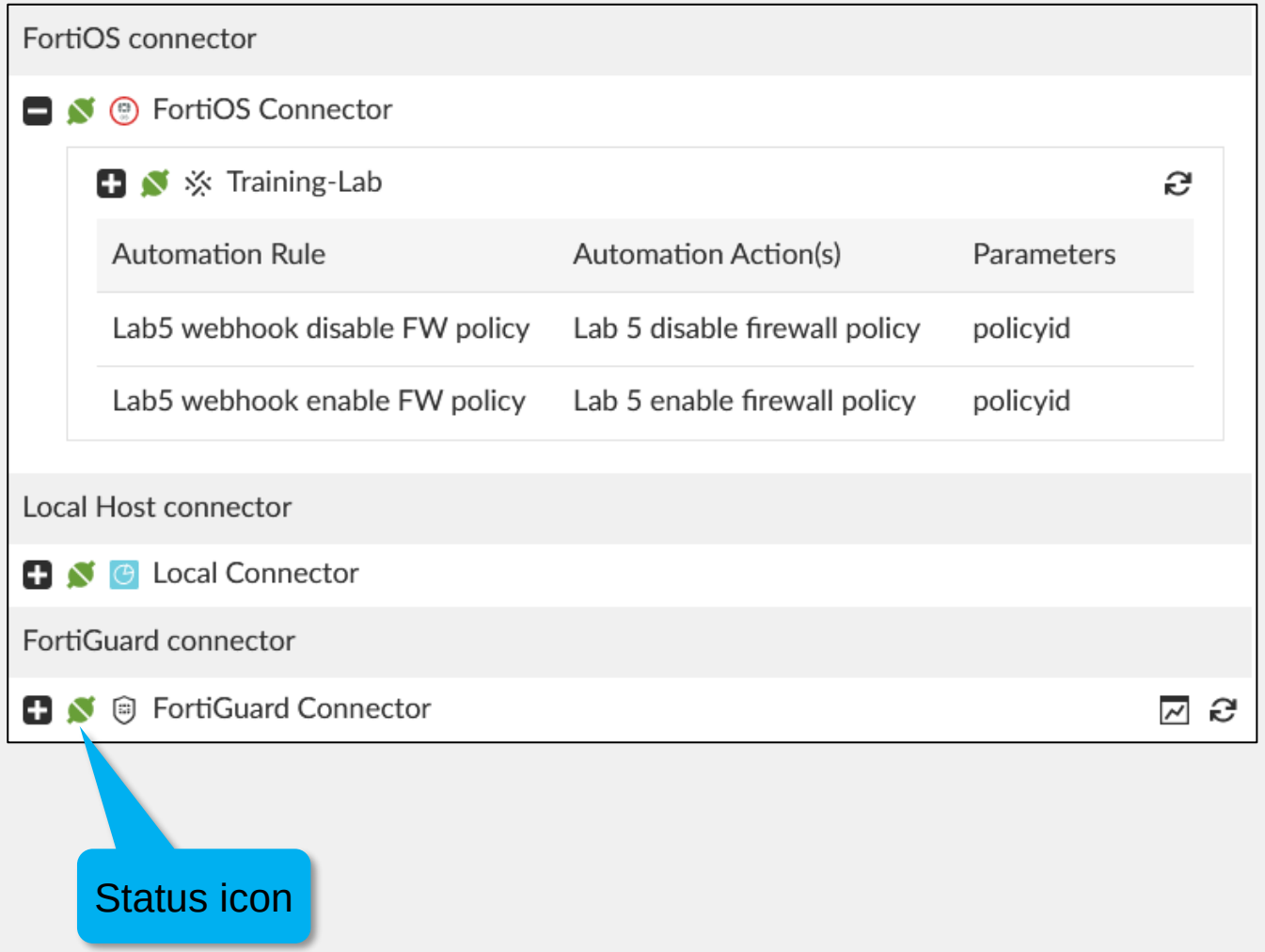
- Describe connector types
- Configure connector actions



Connectors

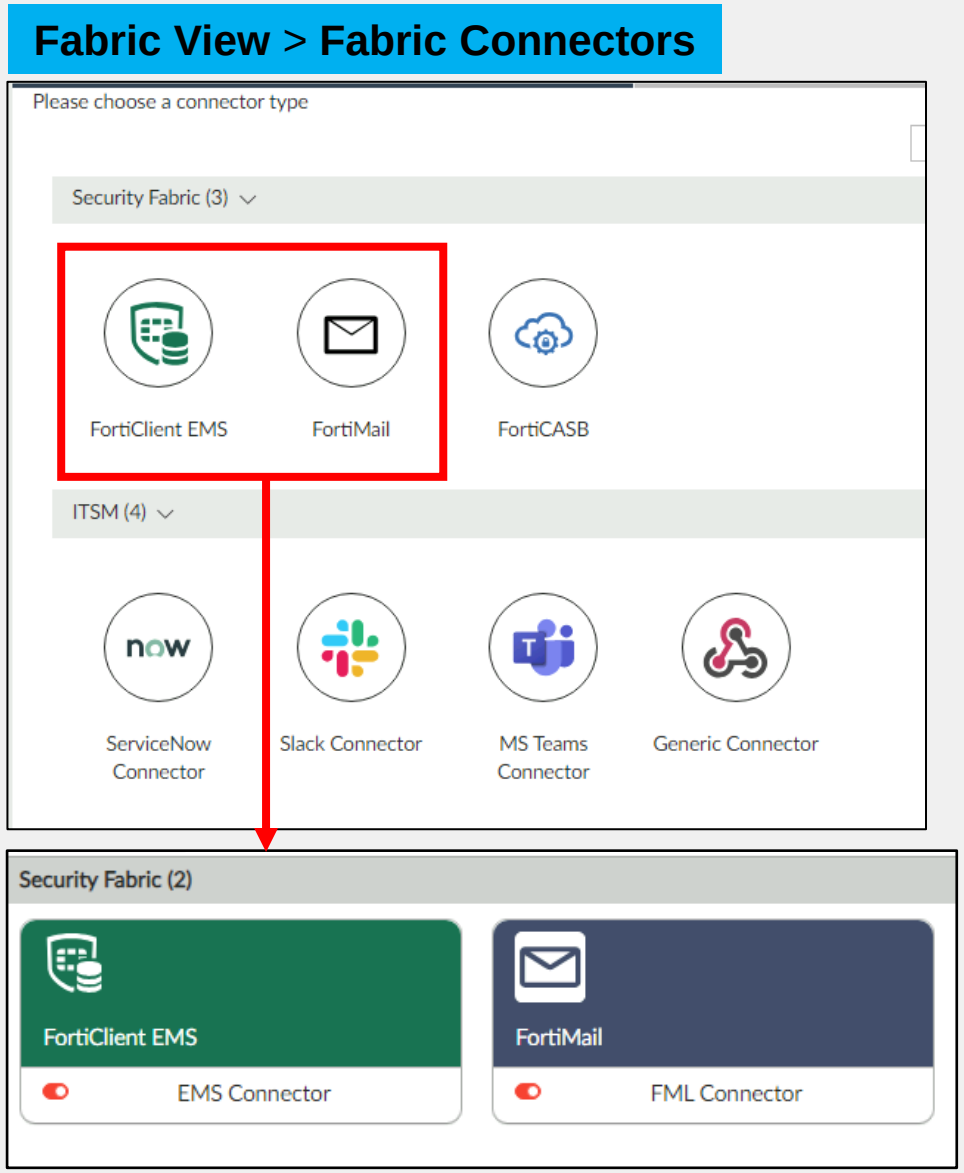
- Allow playbooks to interact with devices in the Security Fabric and other standalone devices
- Determine which actions can be performed by playbook tasks
- The local connector does not need any additional configuration
  - All other connector types must be configured
- The connector status icon is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

Fabric View > Automation > Connectors



Connector Types

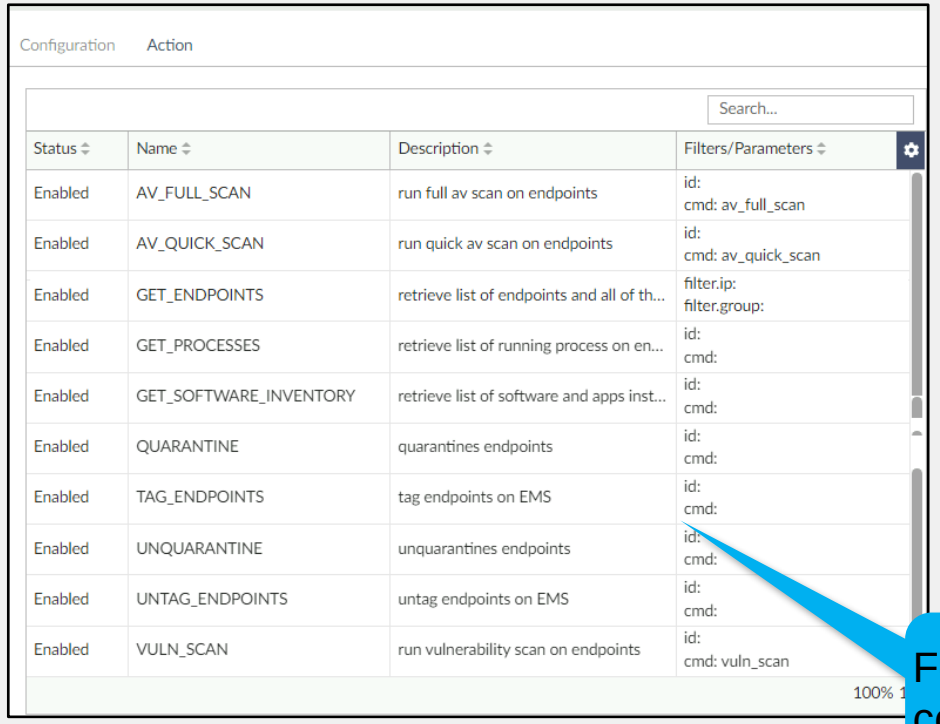
- Two types of connectors
  - Security Fabric
  - ITSM
- Security Fabric connectors:
  - FortiClient EMS
  - FortiMail
  - FortiCASB
- ITSM connectors:
  - Service Now
  - Slack
  - MS Teams
  - Generic: Support additional third-party ticketing platforms



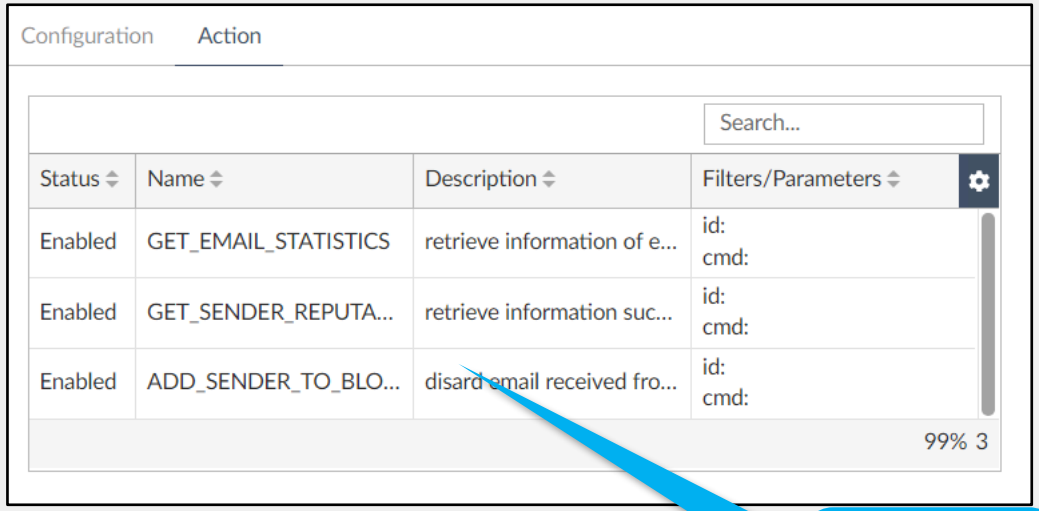
Connector Actions

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

Fabric View > Fabric Connectors



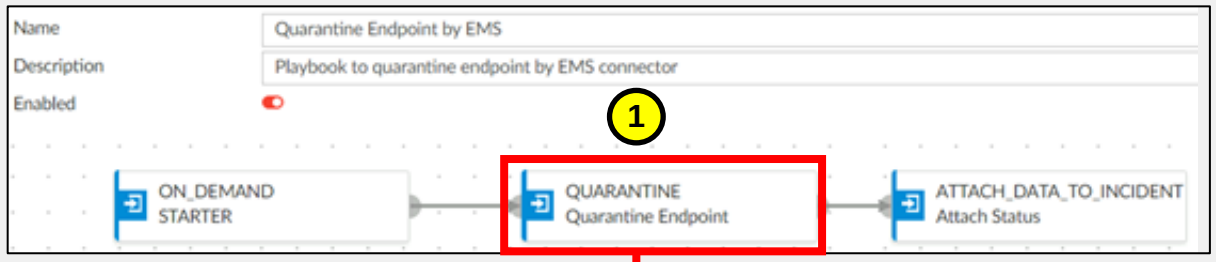
FortiClient EMS connector actions

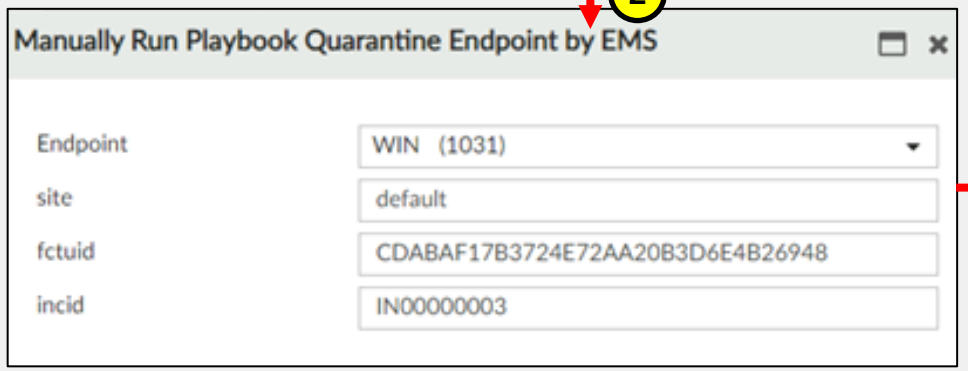


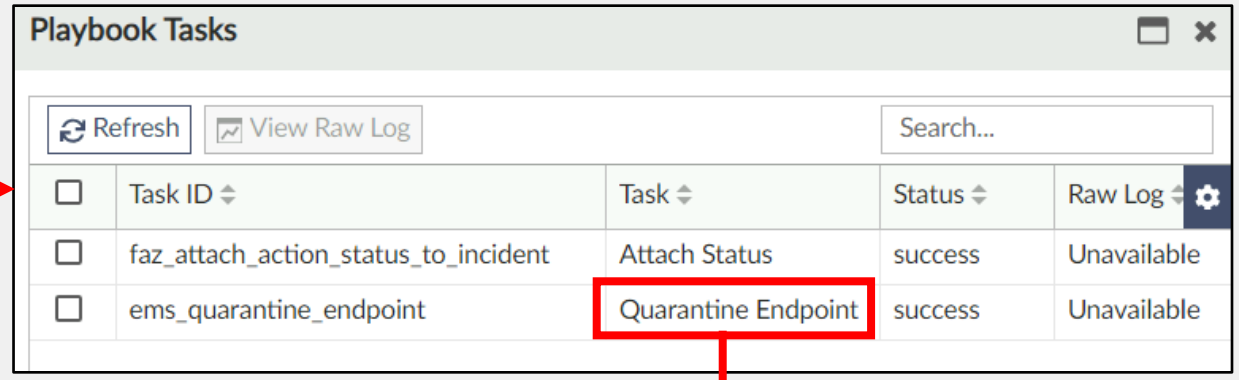
FortiMail connector actions

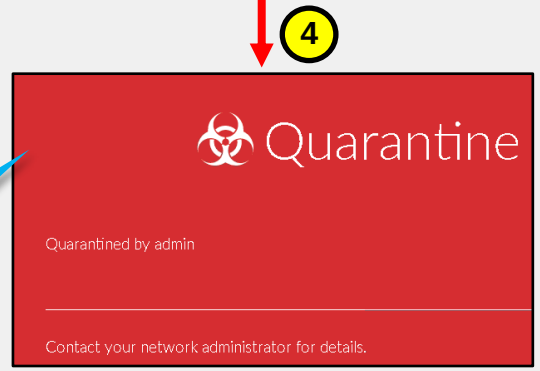
Use Case

Fabric View > Automation > Playbooks









Infected host is quarantined

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/Succ

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