

Configure Secure FTD Event Integration with Security Cloud Control via Secure Event Connector

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Verify](#)

[Troubleshoot](#)

Introduction

This document describes how to configure the Cisco Secure FTD to send security events to the Security Cloud Control (SCC) using the Secure Event Connector (SEC).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Secure Firewall Threat Defense (FTD)
- Linux Command Line Interface (CLI)

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Secure FTD 7.6
- Ubuntu Server version 24.04

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Step 1. Login to the SCC cloud portal:



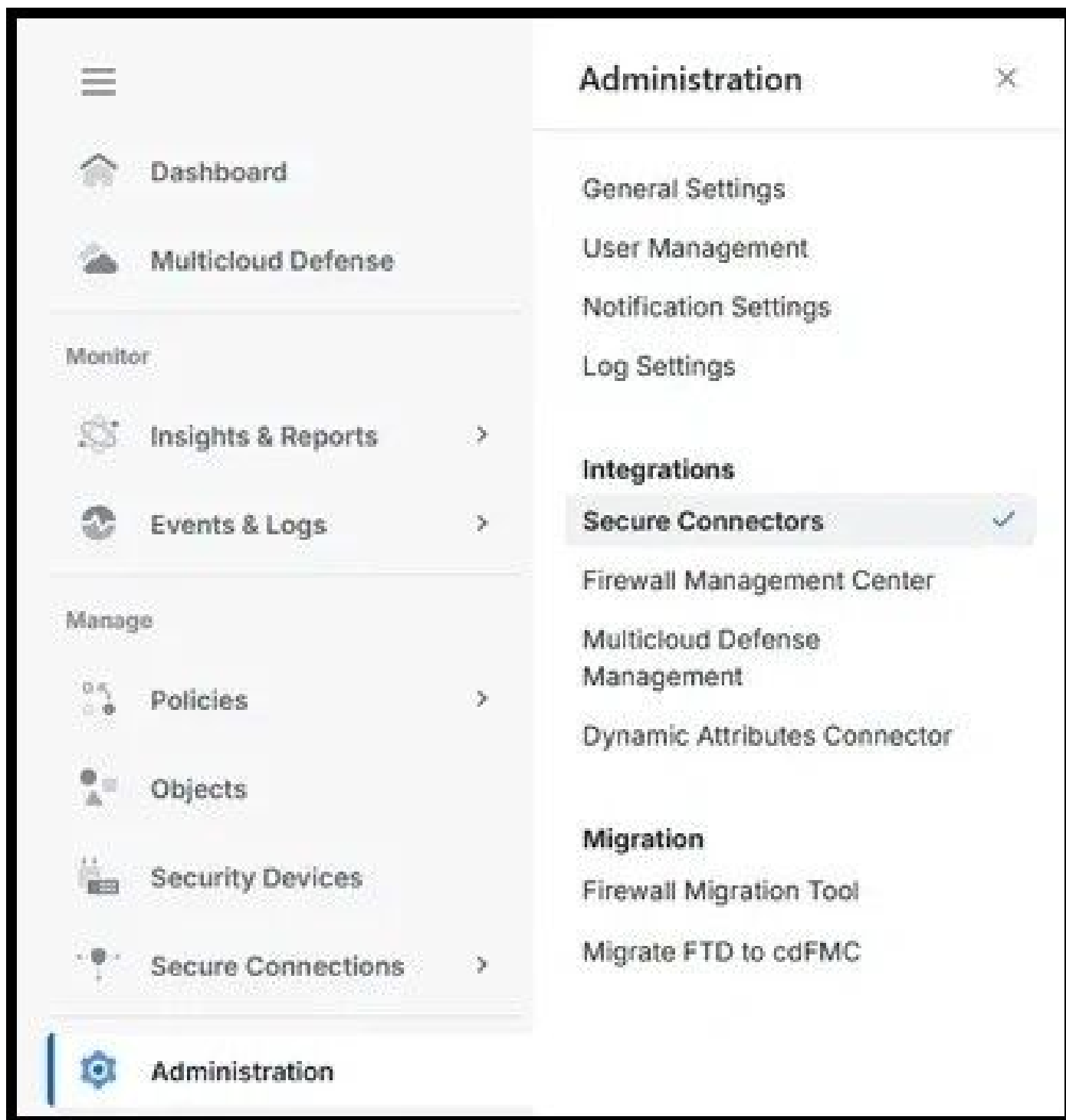
CONNECTING TO SECURITY CLOUD CONTROL (US)

Security Cloud Sign On

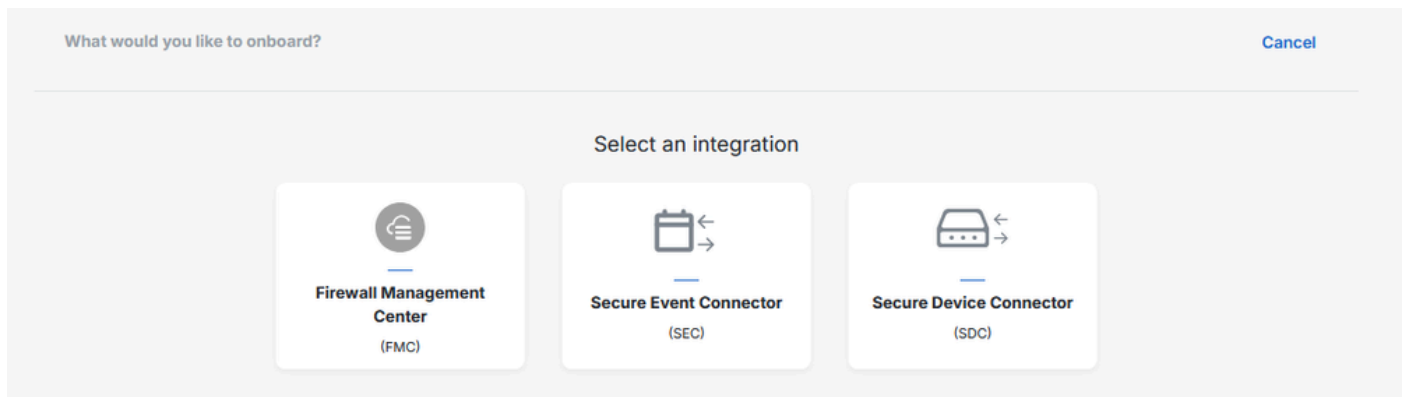
Email

Continue

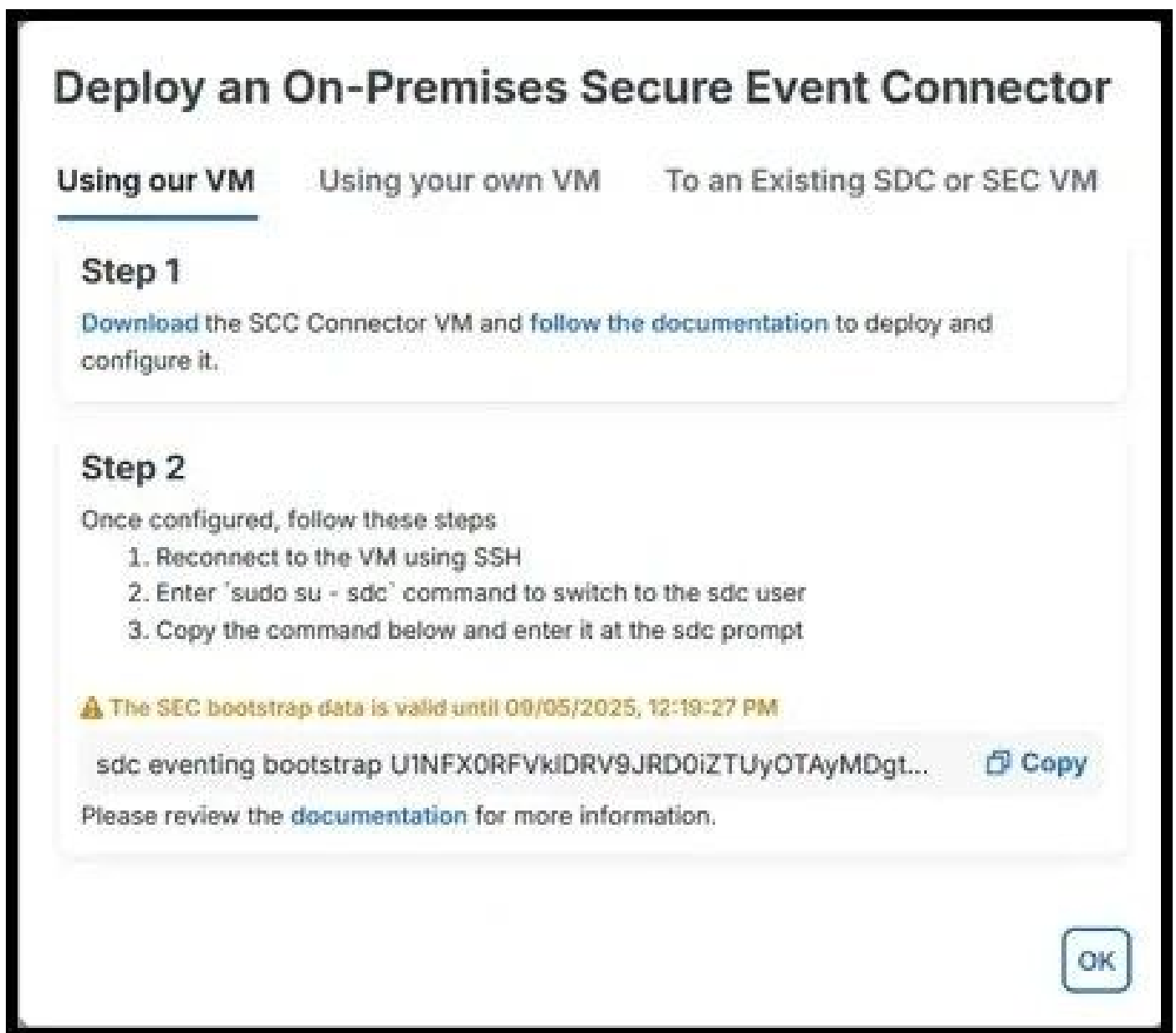
Step 2. From the left hand side menu, choose **Administration** and **Secure Connectors**:



Step 3. On the top right hand side, click the **plus icon** in order to onboard a new connector and choose **Secure Event Connector**:



Step 4. Use the steps to install and bootstrap the connector depending on the desired option between 'Using our VM', 'Using your own VM' or 'To an Existing SDC or SEC VM':



Step 5. A similar message is seen when the bootstrap is performed successfully:

```
2025-06-09 05:41:56 [INFO] Bootstrap package processed successfully
2025-06-09 05:41:56 [INFO] Default AWS Region is us-west-2
2025-06-09 05:42:00 [INFO] Scanning for next available TCP port starting with 10125
2025-06-09 05:42:00 [INFO] TCP port found and set to 10125
2025-06-09 05:42:00 [INFO] Scanning for next available UDP port starting with 10025
2025-06-09 05:42:00 [INFO] UDP port found and set to 10025
2025-06-09 05:42:00 [INFO] Scanning for next available Netflow port starting with 10425
2025-06-09 05:42:00 [INFO] Netflow port found and set to 10425

WARNING! Your credentials are stored unencrypted in '/var/lib/sdc/.docker/config.json'.
Configure a credential helper to remove this warning. See
https://docs.docker.com/go/credential-store/

5a99d0351c1ae91cd790dcf18ee1d0594d37fcfaf5a1725473eed042342a567
2025-06-09 05:42:06 [INFO] The SEC is up and running - You should be all set to go
2025-06-09 05:42:08 [INFO] Your SEC has been successfully bootstrapped! Please verify that everything is working within
the SCC UI, and thank you for being a customer
sdc@lcorream-sdc:~$
```

Step 6. Once the connector is deployed and bootstrapped, port information is visible in the SCC portal:


CDO_cisco-lcorream-cdo-us_swz1we-SEC_a3889708-0844-4110-a1e8-641bf17374a6

Details

| | |
|--------------|--------------------------------------|
| ID | a3889708-0844-4110-a1e8-641bf17374a6 |
| Tenant ID | 77cbf34d-91e0-4b2a-a7a8-2597430ce7ce |
| Version | 202407211709 |
| IP Address | 19.0.0.10 |
| TCP Port | 10125 |
| UDP Port | 10025 |
| NetFlow Port | 10425 |

Step 7. On the Cisco Secure Firewall Management Center (FMC), navigate to **Policies** and then to **Access Control**. Choose the policy corresponding to the device(s) being onboarded.

Step 8. Choose **More** and then **Logging**:



Firewall Management Center
Policies / Access Control / Policy Editor

Overview

Analysis


Policies








Devices


Objects

Integrations

[Return to Access Control Policy Management](#)

FTD-Policy 

 Packets →  Prefilter Rules →  Decryption →  Security Intelligence →  Identity →  Access Control →  More



| <input type="checkbox"/> | Name | Action | Source | |
|--------------------------|------|--------|--------|----------|
| | | | Zones | Networks |
| | | | | |

Advanced Settings

HTTP Responses

Inheritance Settings

Logging

Step 9. Enable the **Send using specific syslog alert** option and add a new **Syslog Alert**. Use the Internet Protocol (IP) address and port information obtained from the SEC connector in the SCC portal:

Create Syslog Alert Configuration



Name

SEC-Connector

Host

19.0.0.10

Port

10025

Facility

CONSOLE (ALERT)



Severity

ALERT



Tag

Cancel

Save

Step 10. Back in the Access Control Policy, modify the individual rules in order to send the events to the Syslog server:

Logging settings for Rule 12: PC-to-Internet

☒ Log at beginning of connection

☒ Log at end of connection

☒ Log Files

 File Policy

FTDv-Malware/File



Send Connection Events to:

☒ Firewall Management Center

☒ Syslog server

(Using default syslog configuration in Access Control Logging)

[> Show overrides](#)

Discard

Confirm

Step 11. Deploy the changes made to the FTD in order to allow the firewall to start logging the events.

Verify

In order to verify that the changes were executed successfully and that event logging is taking place, navigate to **Events & Logs** and **Event Logging** in the SCC portal and confirm that events are visible:

| <div> <div>Clear</div> <div>Time Range After 06/03/2025 11:40:01 </div> </div> | | | |
|---|-----------------------|-------------|------------|
| <div> <div> Views</div> <div><u>View 1</u></div> </div> | | | |
| | Date/Time | Device Type | Event Type |
| | Jun 5, 2025, 11:49:17 | FTD | Connection |
| | Jun 5, 2025, 11:49:18 | FTD | Connection |
| | Jun 5, 2025, 11:49:46 | FTD | Connection |
| | Jun 5, 2025, 11:49:46 | FTD | Connection |
| | Jun 5, 2025, 11:49:59 | FTD | Connection |
| | Jun 5, 2025, 11:50:02 | FTD | Connection |
| | Jun 5, 2025, 11:50:10 | FTD | Connection |
| | Jun 5, 2025, 11:50:47 | FTD | Connection |
| | Jun 5, 2025, 11:51:08 | FTD | Connection |
| | Jun 5, 2025, 11:51:15 | FTD | Connection |
| | Jun 5, 2025, 11:51:23 | FTD | Connection |
| | Jun 5, 2025, 11:51:38 | FTD | Connection |
| | Jun 5, 2025, 11:51:40 | FTD | Connection |

Troubleshoot

On FTD, run a packet capture on the device using the management interface matching the traffic navigating to the SEC in order to capture the syslog traffic:

```
> capture-traffic
```

Please choose domain to capture traffic from:

0 - eth0

1 - Global

Selection? 0

Warning: Blanket capture may cause high CPU usage and reduced throughput, use selective filtering to reduce capture size.
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options: host 19.0.0.10 port 10025
Starting traffic capture, press ctrl + c to exit (Maximum 1,000,000 packets will be captured)
HS_PACKET_BUFFER_SIZE is set to 4.
tcpdump: can't parse filter expression: syntax error
Exiting.

> capture-traffic

Please choose domain to capture traffic from:

- 0 - eth0
- 1 - Global

Selection? 0

Warning: Blanket capture may cause high CPU usage and reduced throughput, use selective filtering to reduce capture size.
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options: host 19.0.0.10 and port 10025
Starting traffic capture, press ctrl + c to exit (Maximum 1,000,000 packets will be captured)
HS_PACKET_BUFFER_SIZE is set to 4.
10:43:00.191655 IP firepower.56533 > 19.0.0.10.10025: UDP, length 876
10:43:01.195318 IP firepower.56533 > 19.0.0.10.10025: UDP, length 1192
10:43:03.206738 IP firepower.56533 > 19.0.0.10.10025: UDP, length 809
10:43:08.242948 IP firepower.56533 > 19.0.0.10.10025: UDP, length 1170

From the SEC virtual machine, ensure that the virtual machine has internet connectivity. Run the command **sdc troubleshoot**, in order to generate a troubleshooting bundle which can be used to check the **lar.log** file for further diagnosis.