

通過安全事件聯結器配置與安全雲控制的安全 FTD 事件整合

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[驗證](#)

[疑難排解](#)

簡介

本檔案介紹如何設定Cisco Secure FTD，以使用安全事件聯結器(SEC)將安全事件傳送到安全雲控制(SCC)。

必要條件

需求

思科建議您瞭解以下主題：

- 思科安全防火牆威脅防禦(FTD)
- Linux命令列介面(CLI)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科安全FTD 7.6
- Ubuntu伺服器版本24.04

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

步驟1.登入SCC雲門戶：



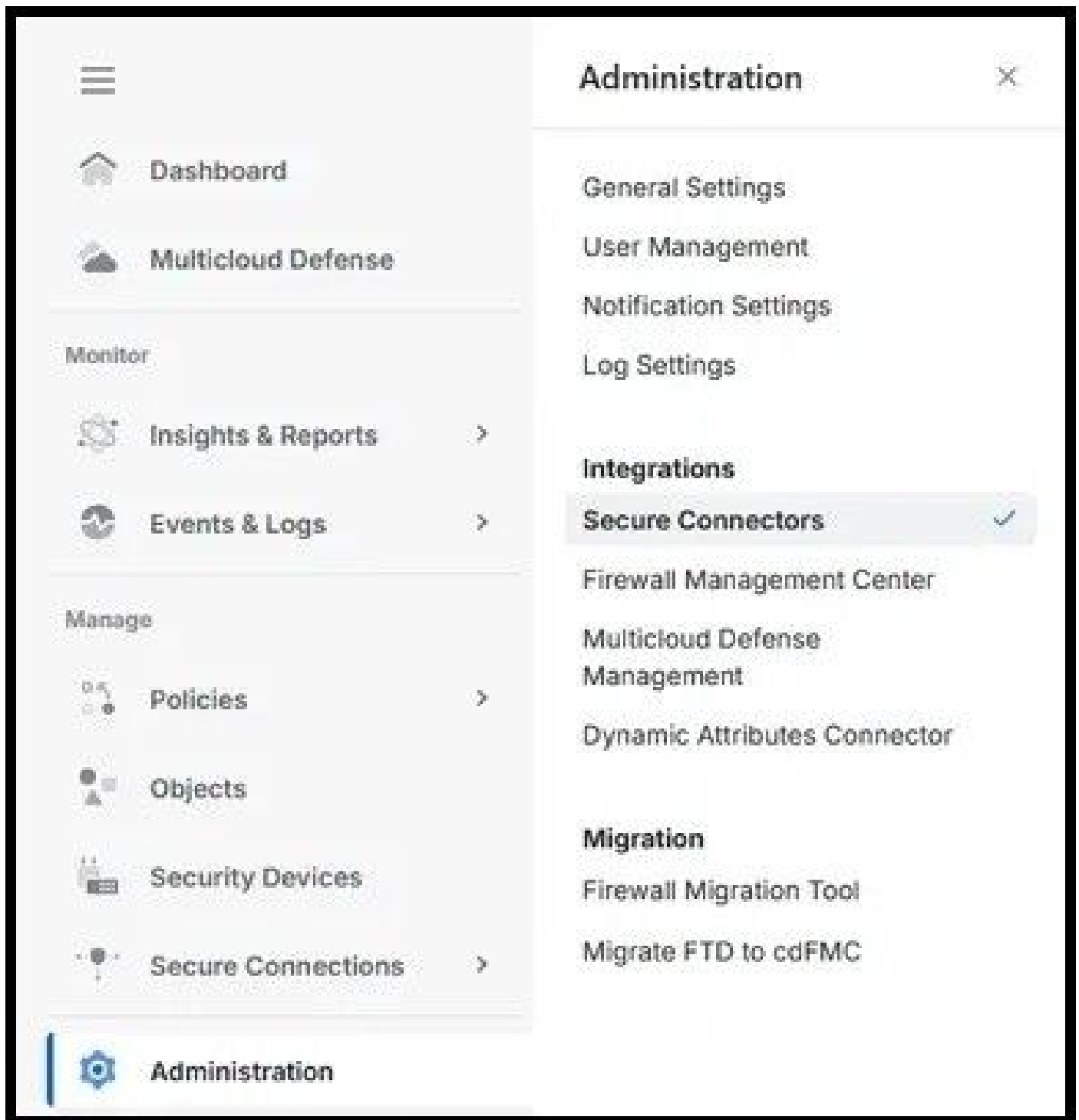
CONNECTING TO SECURITY CLOUD CONTROL (US)

Security Cloud Sign On

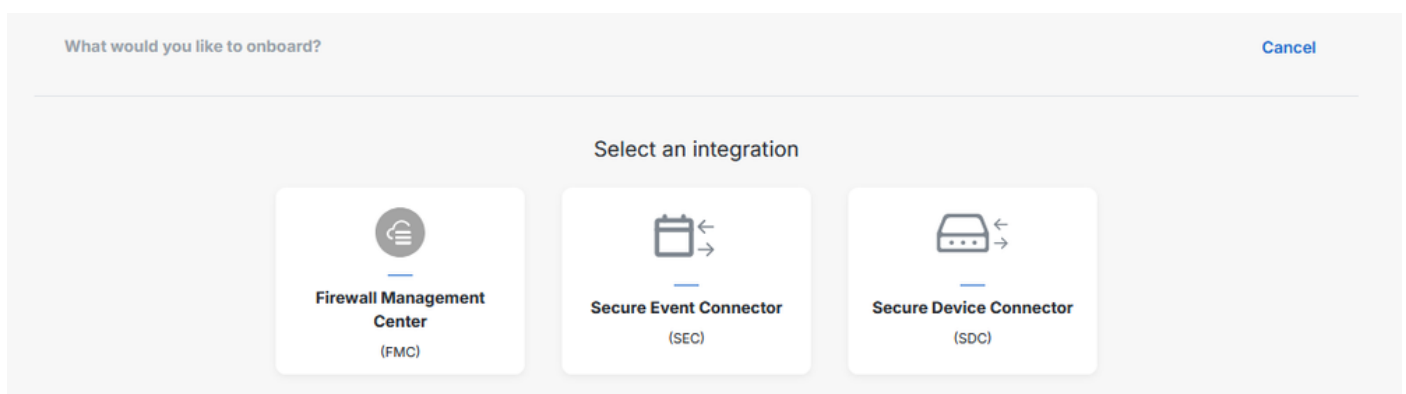
Email

Continue

步驟2.從左側選單中選擇Administration和Secure Connectors:



步驟3.在右上角，按一下plus 圖示以加入新的聯結器，然後選擇Secure Event Connector:



步驟4.根據在「使用我們的VM」、「使用您自己的VM」或「連線到現有的SDC或SEC VM」之間的所需選項，使用步驟安裝和引導聯結器：

Deploy an On-Premises Secure Event Connector

Using our VM

Using your own VM

To an Existing SDC or SEC VM

Step 1

Download the SCC Connector VM and follow the documentation to deploy and configure it.

Step 2

Once configured, follow these steps

1. Reconnect to the VM using SSH
2. Enter 'sudo su - sdc' command to switch to the sdc user
3. Copy the command below and enter it at the sdc prompt

 The SEC bootstrap data is valid until 00/05/2025, 12:19:27 PM

`sdc eventing bootstrap U1NFX0RFVkiDRV9JRD0iZTUyOTAyMDgt...`  Copy

Please review the [documentation](#) for more information.

OK

步驟5.成功執行引導時會出現類似消息：

```
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:~$
```

步驟6.在部署聯結器並引導後，埠資訊在SCC門戶中可見：

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

步驟7.在思科安全防火牆管理中心(FMC)上，導覽至Policies，然後導覽至Access Control。選擇與要登入的裝置對應的策略。

步驟8.選擇More，然後選擇Logging:

 **Firewall Management Center**
Policies / Access Control / Policy Editor

OverviewAnalysisPoliciesDevicesObjectsIntegrations

[Return to Access Control Policy Management](#)

FTD-Policy

Packets → ✓ Prefilter Rules → ○ Decryption → ✓ Security Intelligence → ✓ Identity → ✓ Access Control → ▼ More

▼

Q Type to search

	Name	Action	Source	
			Zones	Networks
☐				

Advanced Settings

HTTP Responses

Inheritance Settings

Logging

步驟9.啟用Send using specific syslog alert選項並新增新的Syslog警報。使用從SCC門戶中的

SEC聯結器獲取的Internet協定(IP)地址和埠資訊：

Create Syslog Alert Configuration

Name

SEC-Connector

Host

19.0.0.10

Port

10025

Facility

CONSOLE (ALERT)

Severity

ALERT

Tag

Cancel

Save

步驟10.返回訪問控制策略，修改單個規則以將事件傳送到Syslog伺服器：

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

步驟11.部署對FTD所做的變更，以便允許防火牆開始記錄事件。

驗證

若要確認變更是否成功執行以及事件日誌記錄是否正在發生，請導航到SCC門戶中的事件與日誌和事件日誌，並確認事件是否可見：

[Clear](#)Time Range **After 06/03/2025 11:40:01** 

Views

[View 1](#)

	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

疑難排解

在FTD上，使用與導航到SEC的流量相匹配的管理介面在裝置上執行封包擷取，以擷取系統日誌流量：

```
> 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 re

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 re

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

從SEC虛擬機器，確保虛擬機器具有Internet連線。執行命令sdc troubleshooting以生成疑難排解套件組合，該套件組合可用於檢查lar.log檔案以進行進一步診斷。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。