

CISCO  
SECURE

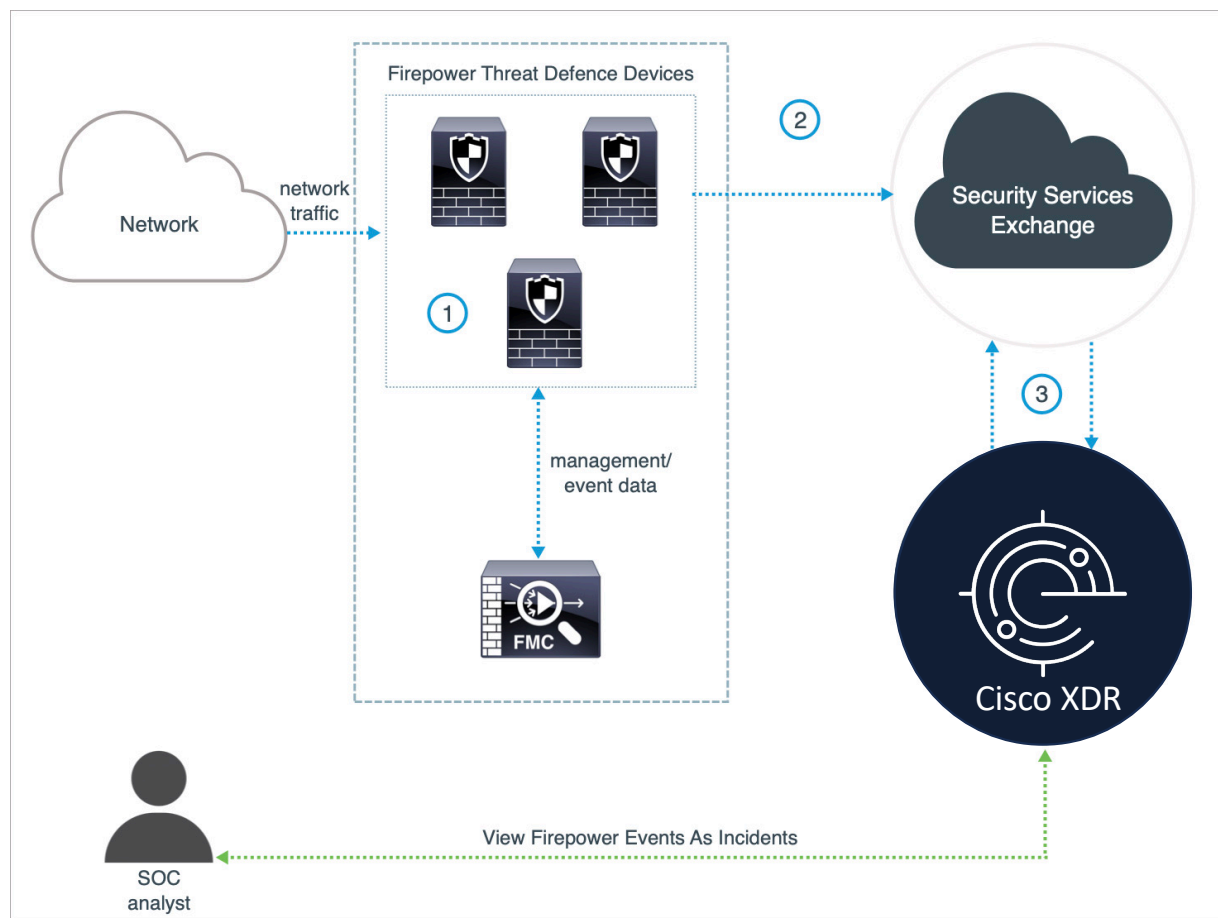
CISCO The bridge to possible

PSU VoD  
Cisco XDR  
製品統合ガイド  
Firewall Threat Defense 編

2024年3月  
シスコシステムズ合同会社 セキュリティ事業



# XDR – Firewall Threat Defense 構成と動作の仕組み



## 動作概要

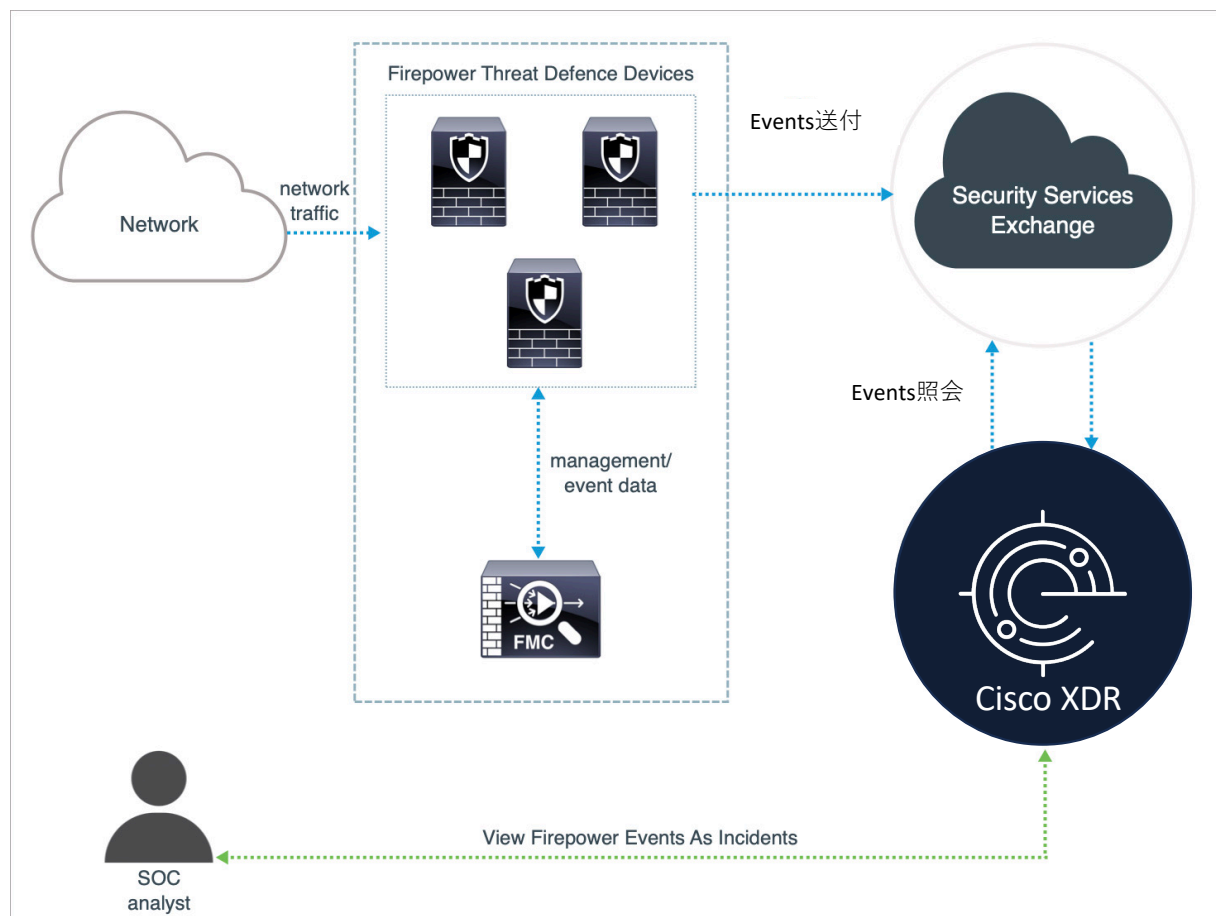
- 1) FMC で管理している FTD デバイスがイベントを生成
- 2) FTD デバイスが、サポートされているイベントを Security Service Exchange (SSX) に送信
- 3) XDR が検出情報を SSX に照会し、XDR にイベントやインシデントとして表示

# XDR – Firewall Threat Defense

## 本ガイドでの条件

- FMC 管理の FTD と XDR の連携方法を解説  
FDM 管理でも XDR との連携は可能だが本ガイドでは割愛
- FMC / FTD バージョン 7.2 以降で、FTD と XDR が直接連携する方法を解説  
Syslog 経由であればバージョン 6.3 から、直接連携であればバージョン 6.4 から FTD と XDR との連携は可能だが、バージョン 7.2 以降の直接連携が最もシンプルでわかりやすいので、本ガイドはその方法の解説に注力
- FMC でレジストしている Smart Account の Virtual Account に管理者権限が必要  
評価期間中の FMC / FTD (Smart License 未登録) では連携設定不可
- XDR と CDO のテナントが必要

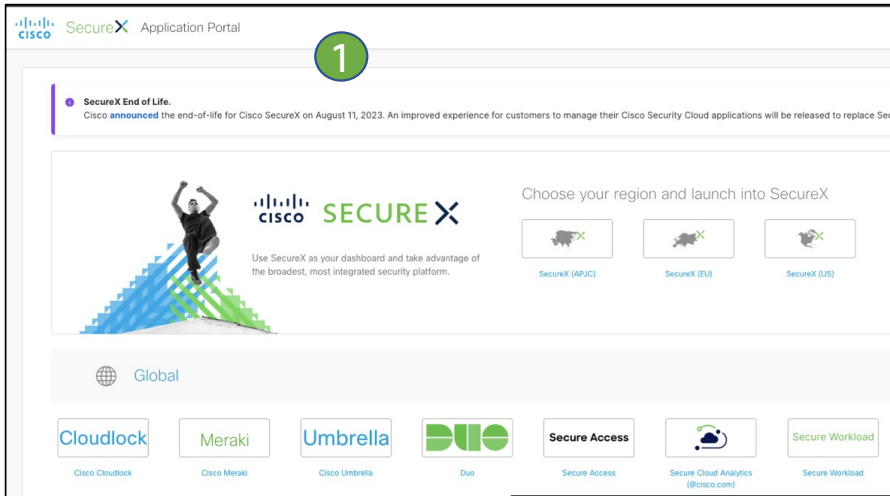
# XDR – Firewall Threat Defense 設定手順の流れ



## 設定手順

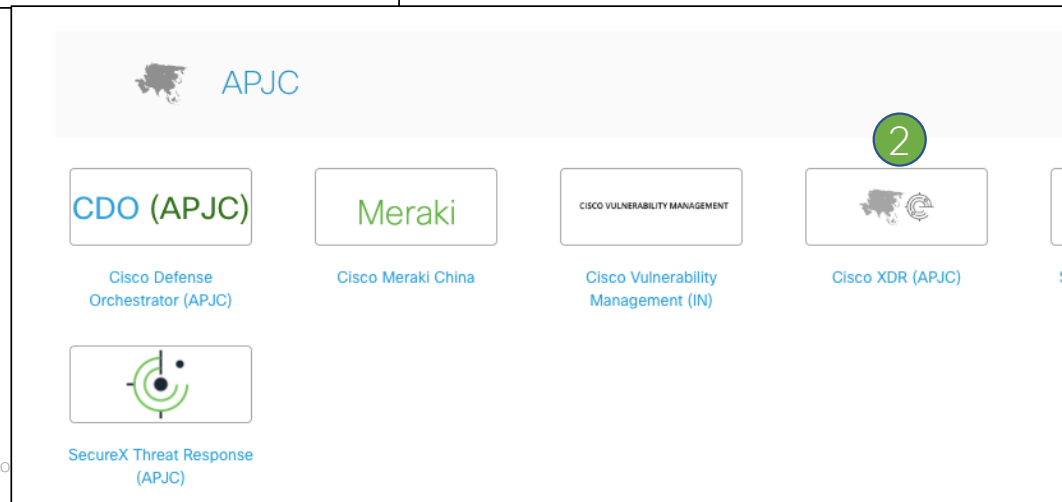
- 1) Security Services Exchange (SSX)にて Smart Account を紐付け
- 2) Firewall Management Center (FMC)にて XDR との連携設定
- 3) XDR 管理コンソールにて Secure Firewall (FTD) インテグレーションの確認
- 4) 動作確認

# 設定1) SSX で Smart Account の紐付け

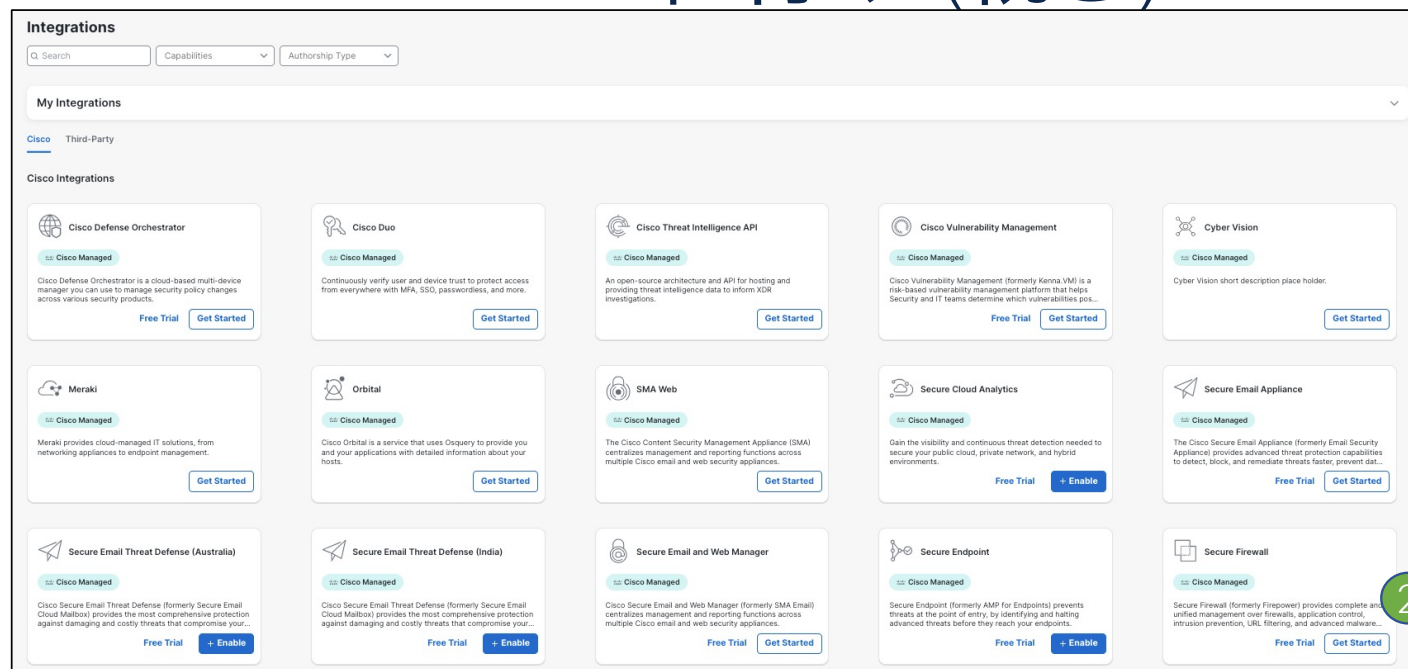
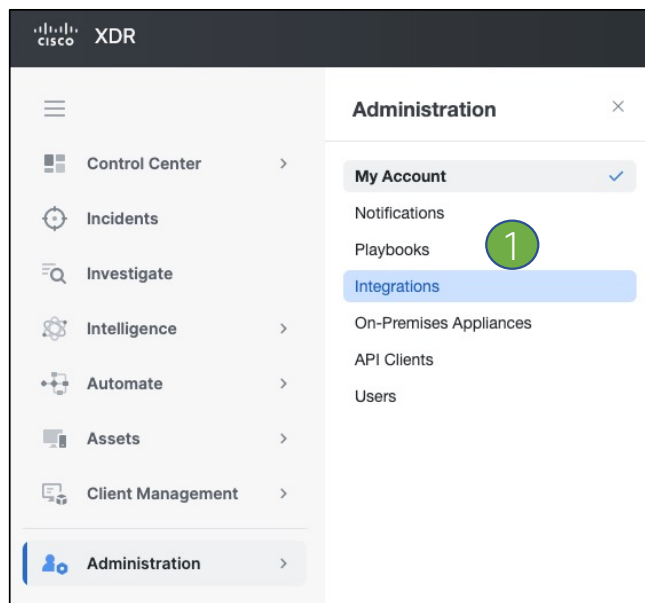


1 Cisco Security Cloud にログイン  
<https://sign-on.security.cisco.com>

2 使っているデータセンターの XDR をクリックして XDR 管理画面にログイン (本ガイドでは APJC)

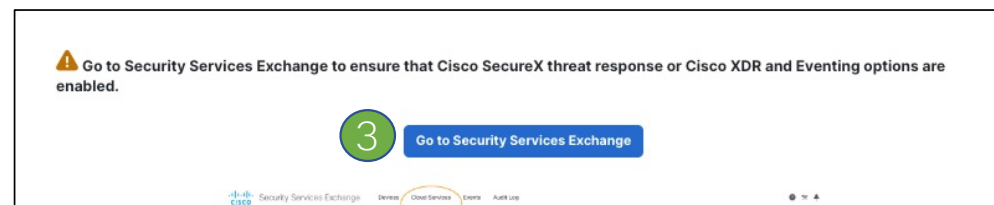


# 設定1) SSX で Smart Account の紐付け (続き)



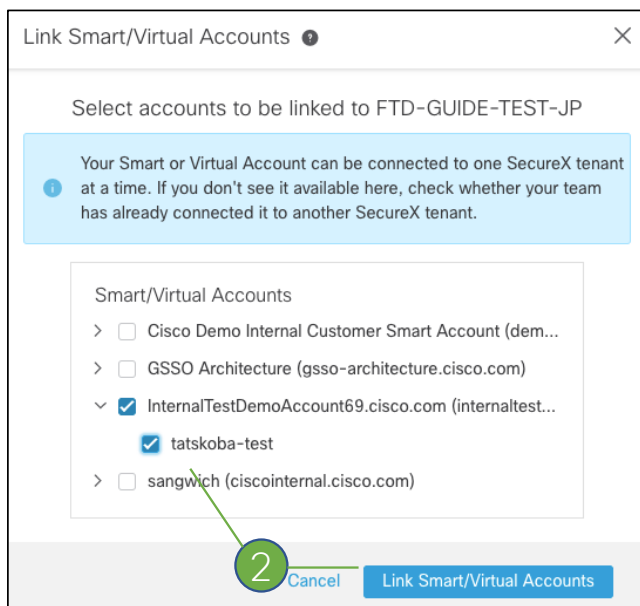
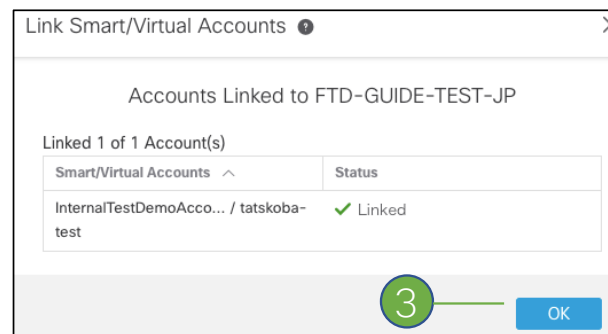
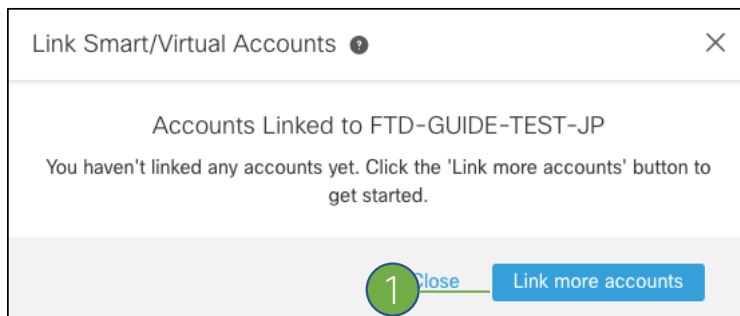
① XDR 画面左メニューより Administration → Integration をクリック

② Cisco Integrations から Secure Firewall の Get Started をクリック



③ Go to Security Service Exchange をクリック 6

# 設定1) SSX で Smart Account の紐付け (続き)



- 1 Link More accounts をクリック
- 2 FMC にてレジストしている Virtual Account (要管理者権限) を選択して Link Smart/Virtual Accounts をクリック
- 3 Smart/Virtual Account が SSX に紐付いたことを確認して OK をクリック

# 補足) SSX でのイベントプロモート

The screenshot shows the 'Settings' page with the 'Auto-Promote Events' tab selected. Under 'By Event Type', the following options are checked:

- Intrusion Events
  - Impact Red (Poor)
  - Talos IP Reputation ⓘ
  - All other lower impact events ⓘ
- Malware Events
- All Security Intelligence Events
  - DNS
  - IP Reputation
  - URL

At the bottom, there are expandable sections for 'By Custom IP Address (Intrusion Events Only)', 'By Intrusion Rule Category', and 'By Custom Security Intelligence Object'. 'Discard' and 'Save' buttons are visible at the bottom right.

The screenshot shows the 'Cloud Services' configuration page for 'FTD-GUIDE-TEST-JP'. Two settings are visible, both with toggle switches turned on:

- Cisco SecureX threat response or Cisco XDR**: Enabled. Description: Cisco SecureX threat response or Cisco XDR enablement allows you to utilize supported devices in the course of a cybersecurity investigation. It also allows this platform to send high fidelity security events and observations to Threat Response.
- Eventing**: Enabled. Description: Eventing allows you to collect and view events in the cloud.

本ガイドでは、Intrusion Event を全て SSX 経由で XDR で解析するため、SSX の Cloud Services → Eventing を有効にして Auto-Promote Events で Intrusion Events 全てを有効にしておくこと



# 設定2) FMC にて XDR 連携を設定

Firewall Management Center  
Integration / SecureX

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ 👤 admin | cisco SECURE

### SecureX Integration

#### SecureX Setup

This feature allows Secure Firewall Management Center to integrate with other SecureX services via SecureX ribbon. [Learn more](#)

1 Cloud Region  
This setting determines where events are sent to, if configured to send events to the cloud, as well as data generated by the Cisco Success Network and Cisco Support tools.  
Current Region:

#### Cisco Cloud Support

The Management Center establishes a secure connection to the Cisco Cloud so that it can participate in additional service offerings and maintain this secure connection at all times. You can turn off this connection and Cisco Support Diagnostics. Disabling these services will disconnect the Management Center from additional cloud service offerings.

Do you want to change the region?  
Changing your region without having either Smart Licensing or SecureX enabled will result in no change to region upon save.

Cancel Confirm

2 SecureX Enablement  
After completing this configuration, the SecureX ribbon will show up on each page. [Learn more](#)

Enable SecureX

3 Event Configuration

Send events to the cloud

- Intrusion events
- File and malware events
- Connection Events

Security (selected)  
All

4 Orchestration  
Enable SecureX orchestration to allow SecureX users to build automated workflows that interact with various resources in the Secure Firewall Management Center. [Learn more](#)

Enable SecureX Orchestration

Save

FMC の Integration → SecureX \* をクリック、SecureX Setup 画面の ① Cloud Region から XDR の Region (日本では通常は APCJ であり本ガイドも APJC を利用) を選択して Confirm をクリック

注) FMC での XDR 連携設定のメニューは、まだ SecureX という表記になっている

## 設定2) FMC にて XDR 連携を設定 (続き)

The screenshot shows the 'SecureX Integration' configuration page in the Firewall Management Center. The page is divided into four main sections:

- SecureX Setup:** This section allows integration with other SecureX services. It includes a 'Cloud Region' dropdown menu set to 'ap-northeast-1 (APJ Region)' and an 'Enable SecureX' button.
- Cisco Cloud Support:** This section establishes a secure connection to the Cisco Cloud. It includes two checkboxes: 'Enable Cisco Success Network' (checked) and 'Enable Cisco Support Diagnostics' (unchecked).
- Event Configuration:** This section allows sending events to the cloud. It includes a 'Send events to the cloud' checkbox (checked) and a 'View your Events In SecureX' link. A green circle '1' is placed around the 'View your Events In SecureX' link.
- Orchestration:** This section allows enabling SecureX orchestration. It includes an 'Enable SecureX Orchestration' checkbox (checked) and an 'Assigned Role' dropdown menu set to 'Access Admin'. A green circle '2' is placed around the 'Save' button.

① Event Configuration より XDR (SSX) に送りたいイベントを選択

② Save をクリックして設定を反映させる

## 設定2) FMC にて XDR 連携を設定 (続き)

Security Services Exchange **Devices** Cloud Services Events Audit Log Tatsuya Kobayashi

Devices for FTD-GUIDE-TEST-JP

Device Name / ID

0 Rows Selected

<input type="checkbox"/>	%	#	Name ^	Type	Version	Status	Cloud Connectivity	Description	Actions
<input type="checkbox"/>	>	1	cdo-cisco-tatskoba	Cisco Firewall Confi...	7.4.1	Registered	2024-03-29 03:46:48	10.200.23.27 cdo-cisco-tatskoba	
<input type="checkbox"/>	>	2	FMCTEST	Secure Firewall Man...	7.2.6	Registered	2024-03-29 04:02:58	192.168.254.67 FMCTEST	
<input type="checkbox"/>	>	3	FTDTEST	Cisco Firepower Thr...	7.2.6	Registered	2024-03-29 04:02:59	192.168.254.57 FTDTEST (FMC managed)	
<input type="checkbox"/>	>	4	Secure Event Connector - localhost.localdomain	Secure Event Conne...	2023120819...	Registered	2024-03-29 03:48:26	Secure Event Connector listening on TCP: 10125, UDP: 10025, N...	

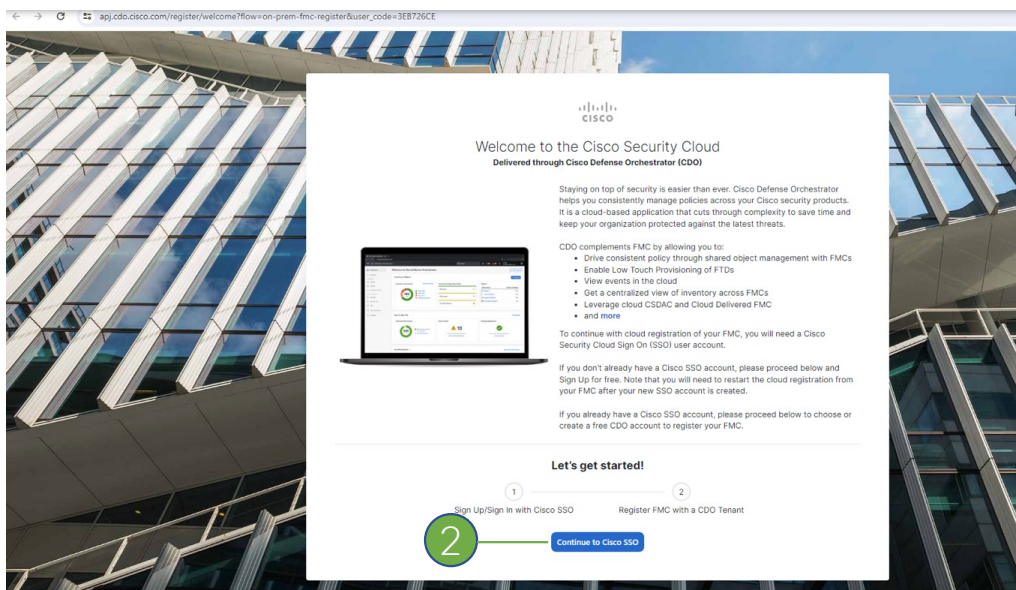
Page Size: 25 Total Entries: 4

FMC 側での Cloud Region 指定が終わると、SSX の Devices の画面に、FMC と FTD デバイスの一覧が表示される

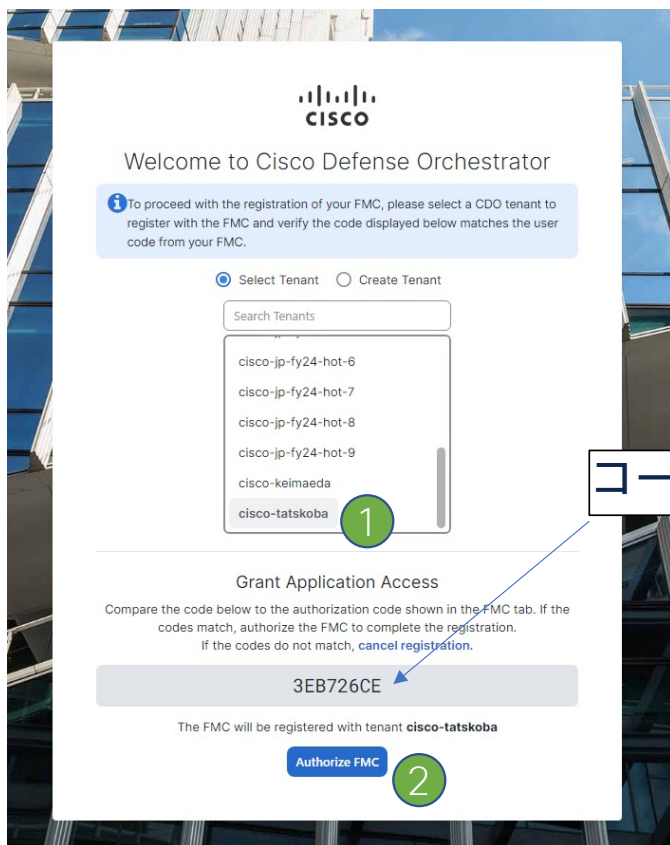
## 設定2) FMC にて XDR 連携を設定 (続き)



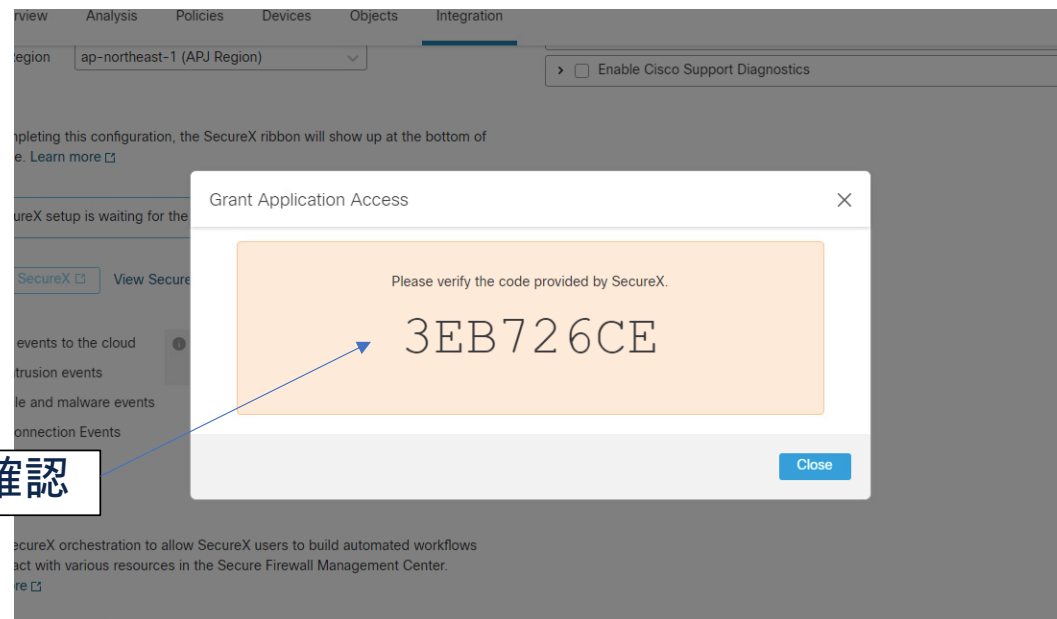
- 1 FMC に戻って ② SecureX Enablement にある Enable SecureX というボタンをクリック
- 2 ブラウザ内で新たなタブが起動、Continue to Cisco SSO をクリック、Cisco Security Cloud へのログインを行う



## 設定2) FMC にて XDR 連携を設定 (続き)



コードの合致を確認



- 1 Cisco Security Cloud にログイン後、利用する CDO のテナントが表示される (複数のテナントがあれば複数が表示されるので利用するテナントを選択)
- 2 画面下部に表示されたコードと、FMC の画面に表示されているコードが合っていることを確認して Authorize FMC をクリック

## 設定2) FMC にて XDR 連携を設定 (続き)

2 SecureX Enablement After completing this configuration, the SecureX ribbon will show up at the bottom of each page. [Learn more](#)

1 **▲ SecureX is enabled for APJ Region. You will need to save your configuration for this change to take effect.**

[Enable SecureX](#)

3 Event Configuration

- Send events to the cloud
- Intrusion events
- File and malware events
- Connection Events
  - Security
  - All

[View your Cisco Cloud configuration](#)  
[View your Events in SecureX](#)

4 Orchestration

Enable SecureX orchestration to allow SecureX users to build automated workflows that interact with various resources in the Secure Firewall Management Center. [Learn more](#)

Enable SecureX Orchestration

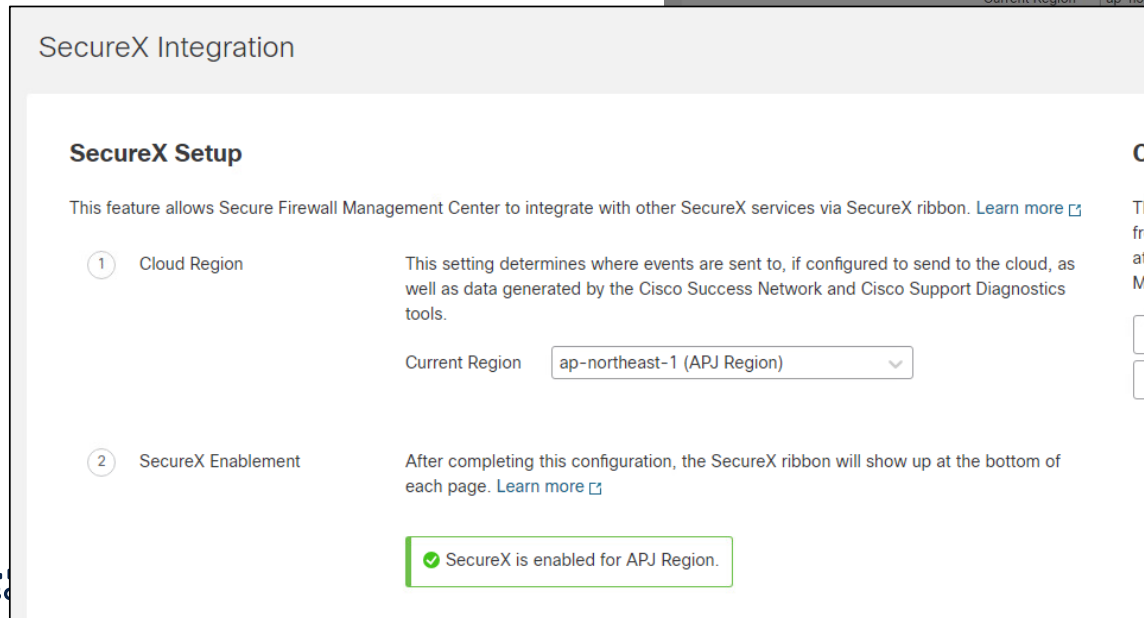
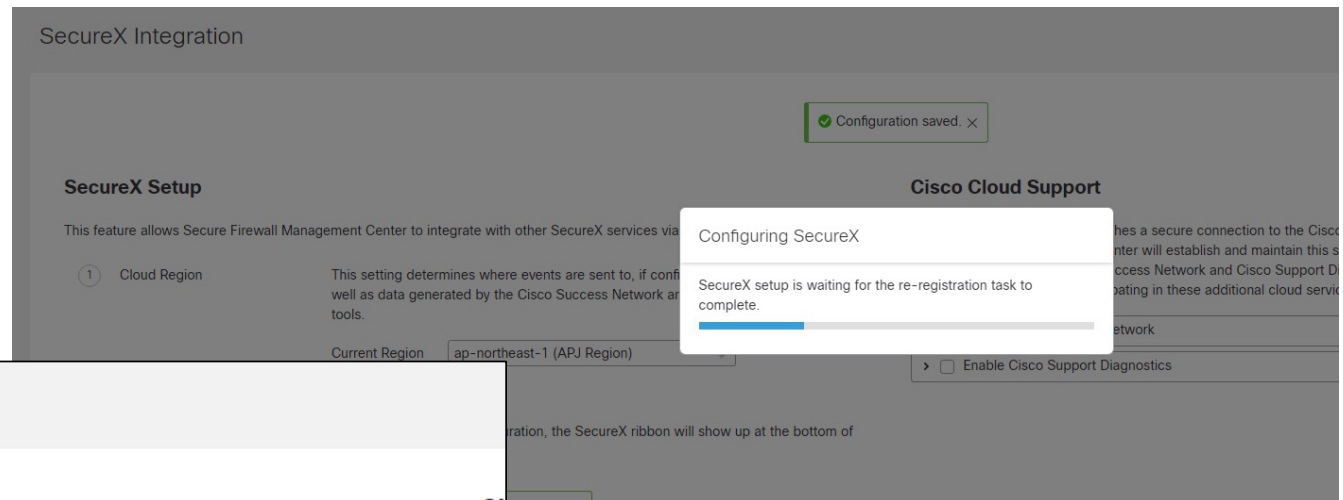
2 [Save](#)

① Authorized FMC が終わると Region で XDR (表示は SecureX) が Enable になった旨のメッセージが表示される

② Save をクリックして設定を保存

# 設定2) FMC にて XDR 連携を設定 (続き)

XDR へのレジストが終わり、  
XDR が有効になった旨のメッ  
セージ (表示は SecureX) が表示  
される



## 設定2) FMC にて XDR 連携を設定 (続き)

3 Event Configuration

- Send events to the cloud
  - Intrusion events
  - File and malware events
  - Connection Events
    - Security
    - All

4 Orchestration

Enable SecureX orchestration to allow SecureX users to build automated workflows that interact with various resources in the Secure Firewall Management Center. [Learn more](#)

Enable SecureX Orchestration

Save

Security Events を Cloud に送る設定になっていることを確認 (なっていない場合は再度設定して Save) し、Deploy を実施

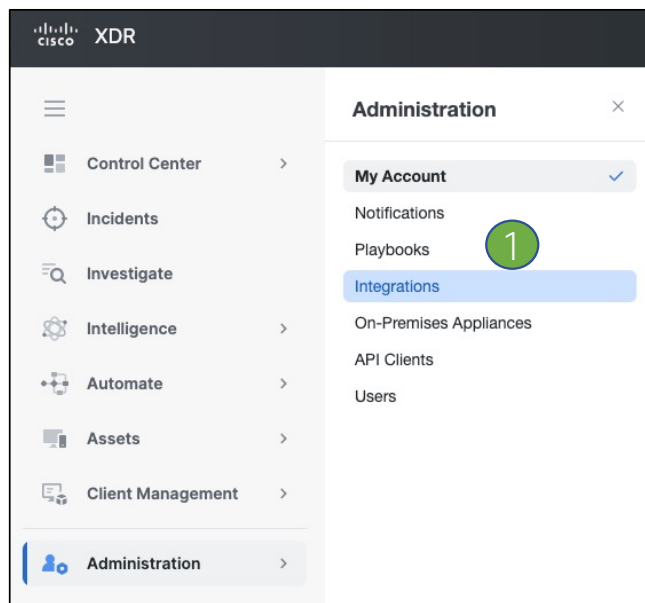
Deploy

Advanced Deploy Deploy

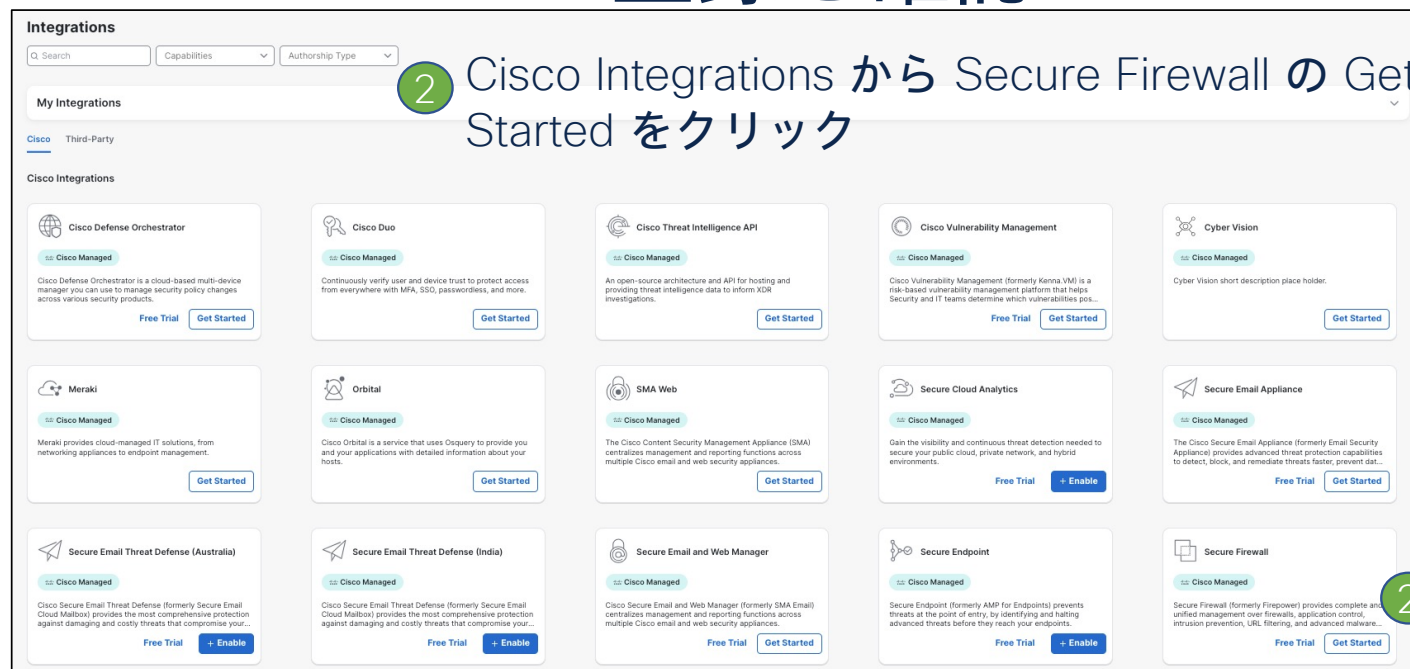
<input checked="" type="checkbox"/> FTDTEST	Ready for Deployment
---	----------------------



# 設定3) XDR にて FMC & FTD の登録を確認

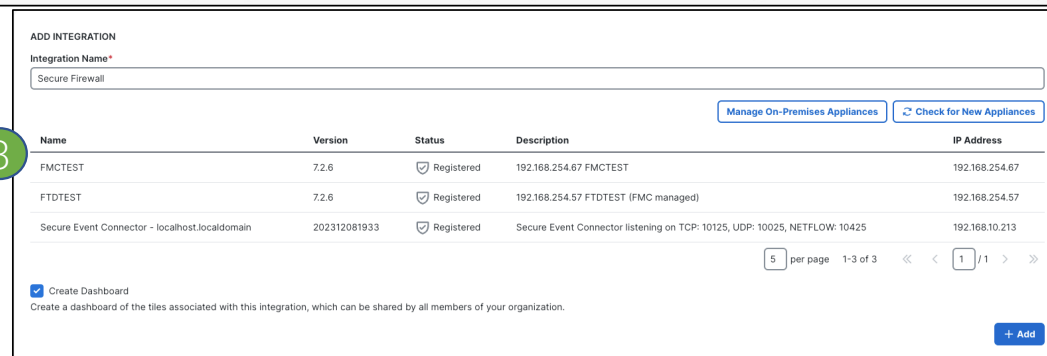


1 XDR 画面左メニューより Administration → Integration をクリック



2 Cisco Integrations から Secure Firewall の Get Started をクリック

3 FMC と FTD が登録されていることを確認



# 設定4) XDR にて FTD Dashboard を作成

The screenshot displays the Cisco XDR Control Center interface. On the left, a navigation menu is visible with 'Control Center' selected. The main area shows the 'Dashboards' section, which is currently empty, displaying a message: 'No data available for selected time period. Try choosing a larger time interval to see more data.' A 'Customize Dashboards' button is highlighted with a green circle '2'. The top right corner shows the user profile 'Tatsuya Kobayashi' and a 'Full screen' button. The bottom left corner shows the URL 'https://xdr.apic.security.cisco.com/control-center'.

① XDR 画面左メニューより Control Center → Dashboard をクリック

② Customize Dashboards をクリック

# 設定4) XDR にて FTD Dashboard を作成 (続き)

**Customize Dashboards** Refresh Tiles ×

**My Dashboards**

- Overview
- MyFTD-Dashboard

**Overview**  
Author: Cisco XDR  
The Overview dashboard provides a high-level summary of the incidents, including ATT&CK® tactics and techniques, an overview of unassigned incidents organized by sources, and a mean time summary of incidents within your organization by default and it is read-only.

**Shared dashboards** ⓘ  
No Dashboards

**Customize Dashboards** Refresh Tiles ×

**My Dashboards**

- Overview
- MyFTD-Dashboard

**Dashboard Name** 2  
MyFTD-Dashboard  
Dashboard name is required

Automation 0 selected Add All ▾

Private Intelligence 0 selected Add All ▾

Secure Client 0 selected Add All ▾

Secure Firewall 0 selected 2 Add All ▾

SecureX Global Threat Intelligence 0 selected Add All ▾

**Shared dashboards** ⓘ  
No Dashboards

Cancel Save

① + Create new dashboard をクリック

② 任意の Dashboard 名を追記し、  
Secure Firewall の Add All をクリック

## 設定4) XDR にて FTD Dashboard を作成 (続き)

**Customize Dashboards** Refresh Tiles ×

**My Dashboards**

- Overview
- MyFTD-Dashboard**

**Dashboard Name**  
MyFTD-Dashboard  
Dashboard name is required

Automation 0 selected Add All ▾

Private Intelligence 0 selected Add All ▾

Secure Client 0 selected Add All ▾

**Secure Firewall 9 selected** Remove All ▾

SecureX Global Threat Intelligence 0 selected Add All ▾

+ Create new dashboard

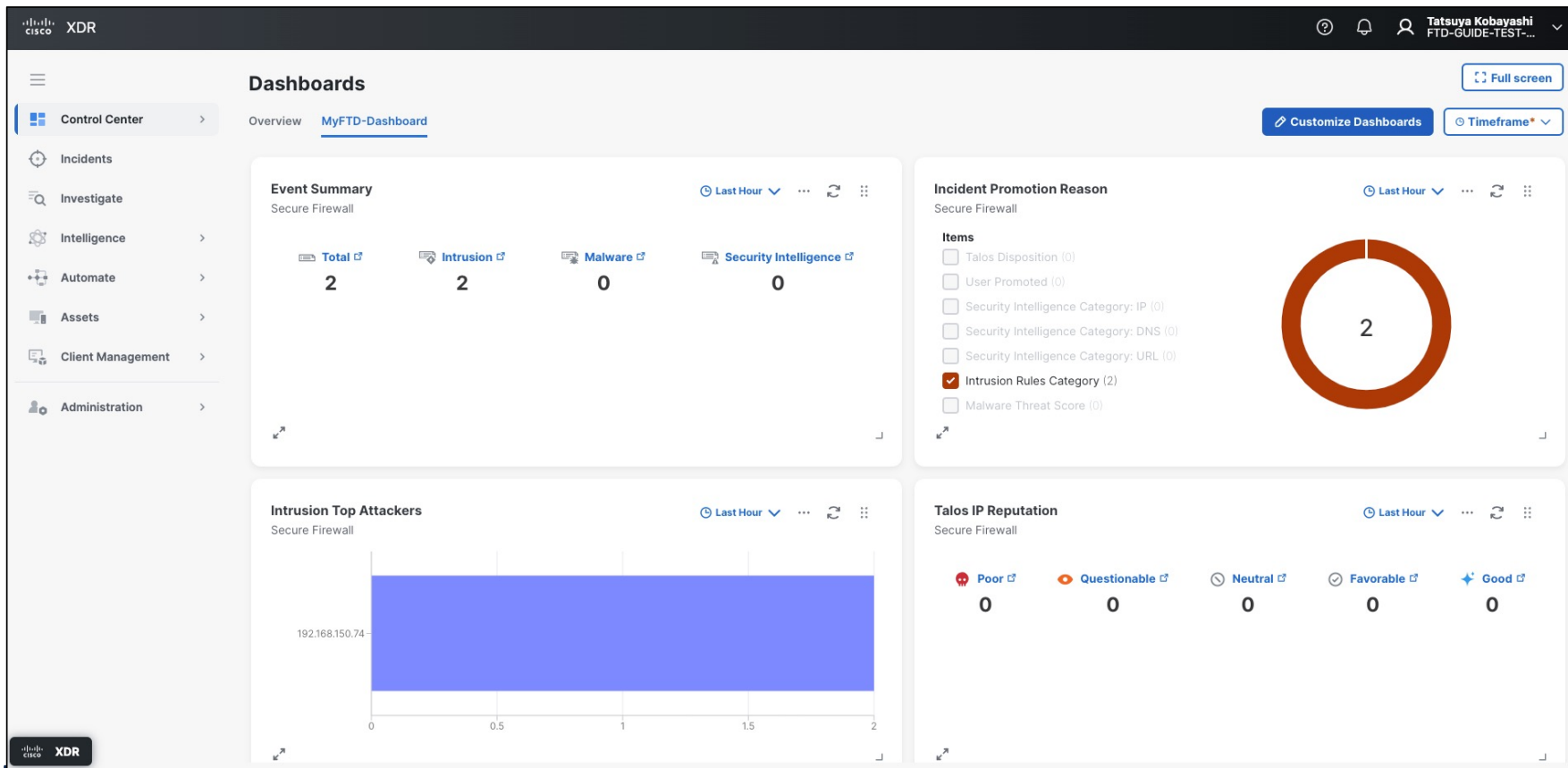
**Shared dashboards** ⓘ  
No Dashboards

Cancel Save

Secure Firewall で 9 selected (今後の Version によって数は変更有り) となったことを確認して Save をクリック

# 設定4) XDR にて FTD Dashboard を作成 (続き)

FTD の Dashboard が作成されたことを確認



# 設定5) 動作確認

The screenshot displays the Cisco Firewall Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The 'Analysis' tab is active, showing a search bar and a 'Refresh' button. Below the search bar, it indicates 'Showing 4 events (3 1)'. The main table lists events with columns for Time, Event Type, Action, Reason, Source IP, Destination IP, Source Port / ICMP Type, Destination Port / ICMP Code, Web Application, Access Control Rule, and Access Control Policy. One event is selected and expanded, showing detailed information:

- Event Type:** Intrusion
- Time:** 2024-03-29 17:17:24
- Priority:** medium
- Impact:** Impact 2
- Action:** Block
- Source IP:** 192.168.150.74
- Destination IP:** 192.168.10.72
- Source Port / ICMP Type:** 58425 / tcp
- Destination Port / ICMP Code:** 21 (ftp) / tcp
- Intrusion Message:** PROTOCOL-FTP CWD ~root attempt (1:336:17)
- Classification:** Potentially Bad Traffic
- Generator:** Standard Text Rule
- Application Protocol:** FTP
- Application Protocol Category:** remote file storage, network protocols/services
- Application Protocol Tag:** file sharing/transfer
- Client Application:** FTP client
- Application Risk:** Medium
- Business Relevance:** Medium
- Ingress Security Zone:** inzone
- Egress Security Zone:** outzone
- Domain:** Global
- Device:** FTDTTEST
- Ingress Interface:** inside
- Egress Interface:** outside
- Ingress Virtual Router:** Global
- Egress Virtual Router:** Global
- Intrusion Policy:** INTRUSION-1
- Access Control Policy:** ACP-1
- Access Control Rule:** CATCH-ALL
- Network Analysis Policy:** Balanced Security and Connectivity
- Source Host Criticality:** None
- Destination Host Criticality:** None

テスト用のイベントを発生させる。この例では、SID 336 の Intrusion Rule を Block に変更 (FTP サーバにログインして `cd ~root` を実施したら通信ブロック) し、実際にこの Rule にヒットするテスト通信を発生させている

# 設定5) 動作確認 (続き)

The screenshot displays the Cisco XDR interface. The main dashboard shows an 'Event Summary' for 'Secure Firewall' with a total of 3 events, all categorized as 'Intrusion'. The 'Incident Promotion Reason' section shows that all 3 incidents were promoted due to the 'Intrusion Rules Category'. The 'Intrusion Top Attackers' chart shows a single attacker IP, 192.168.150.74. An inset window shows the 'Event Stream for FTD-GUIDE-TEST-JP' with 3 rows of intrusion events.

Talos Disposition	Incident	Destination IP	Reporting Device ID	Event Time	Ingest Time	Message	Primary Device ID	Protocol	Source IP	Actions
Unknown	Promoting	192.168.10.72	2207c9e9-b10a-4bb3-a593-2945e3e...	2024-03-29 08:17:24 UTC	2024-03-29 08:17:28 UTC	PROTOCOL-F...		tcp	192.168.150.74	👁️ 🔄
Unknown	Yes	192.168.10.72	630f93d3-9dba-475c-b11e-0db0f17b...	2024-03-29 07:30:25 UTC	2024-03-29 07:30:29 UTC	PROTOCOL-F...		tcp	192.168.150.74	👁️ 🔄
Unknown	Yes	192.168.10.72	630f93d3-9dba-475c-b11e-0db0f17b...	2024-03-29 07:28:00 UTC	2024-03-29 07:28:03 UTC	PROTOCOL-F...		tcp	192.168.150.74	👁️ 🔄

数分後、XDR の Dashboard にて Intrusion Event がカウントアップしていることを確認

SSX のイベント画面でも同様に確認可能



SECURE