

Defense OrchestratorへのオンボードFDM

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[コンフィギュレーション](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

はじめに

このドキュメントでは、登録キーを使用して、Firepower Device Manager(FDM)によって管理されるデバイスをCisco Defense Orchestrator(CDO)にオンボーディングする方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Firepower Device Manager (FDM)
- Cisco Defense Orchestrator(CDO)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- バージョン7.4.1を実行しているFirepowerデバイスマネージャー(FDM)Azure

互換性のあるバージョンと製品の包括的なリストについては、『[Secure Firewall Threat Defense Compatibility Guide](#)』を参照してください。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

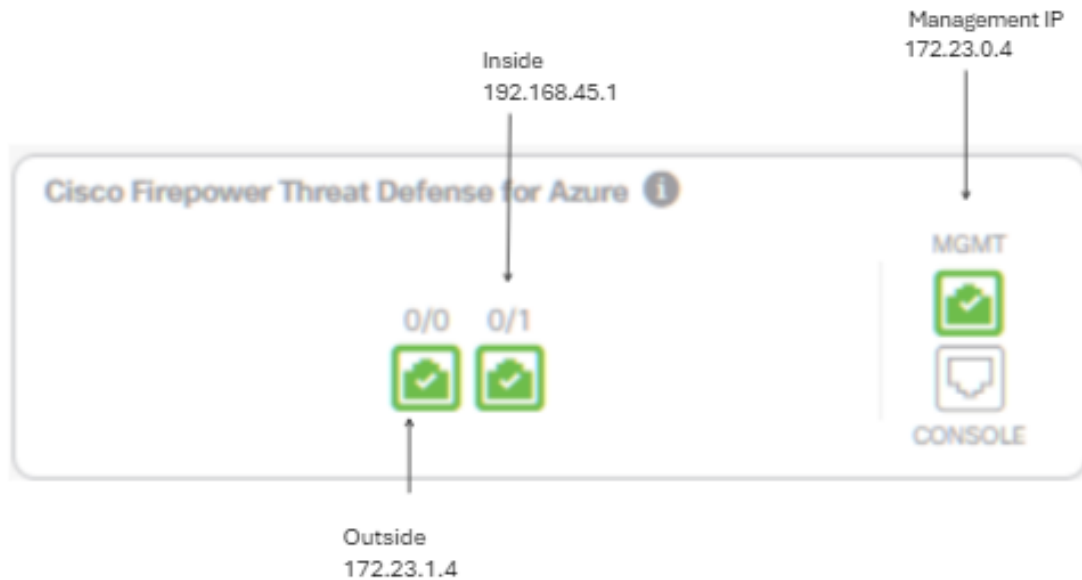
登録キーを使用してCisco Defense Orchestrator(CDO)へのFDM管理対象デバイスのオンボーディングプロセスを開始する前に、次の前提条件を満たしていることを確認してください：

1. 互換性のあるバージョン：デバイスでバージョン6.6以降が実行されている必要があります。
2. ネットワーク要件:[Cisco Defense Orchestratorを管理対象デバイスに接続する](#)
3. 管理ソフトウェア：デバイスはSecure Firewall Device Manager(FDM)で管理する必要があります。
4. ライセンス：デバイスは90日間評価ライセンスまたはスマートライセンスを使用できます。
5. 既存の登録：デバイスがシスコクラウドサービスにまだ登録されていないことを確認して、オンボーディングプロセス中の競合を回避します。
6. 保留中の変更：デバイスに保留中の変更がないことを確認します。
7. DNS構成: FDM管理対象デバイスでDNS設定を正しく構成する必要があります。
8. タイムサービス：デバイス上のタイムサービスを正確に設定して、ネットワークタイムプロトコルと確実に同期させることができます。
9. FDMサポートのアクティブ化の要件。ファイアウォールデバイスマネージャ(FDM)のサポートとその機能は、要求に応じて排他的に許可されます。テナントでFDMサポートが有効になっていないユーザは、FDM管理対象デバイスに対して設定を管理または展開できません。このプラットフォームをアクティブにするには、ユーザーがFDMサポートを有効にする[リクエストをサポート・チームに送信](#)する必要があります。

設定

ネットワーク図

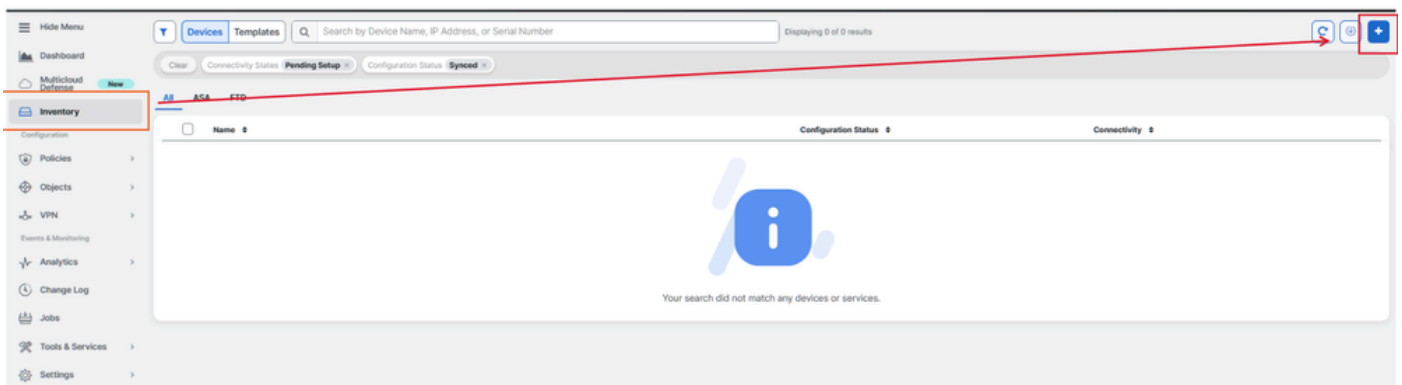
この記事では、管理インターフェイスを介して制御されるFDM(Firepower Device Manager)デバイスに焦点を当てています。このインターフェイスは、デバイスをCisco Defense Orchestrator(CDO)に登録するために不可欠なインターネットアクセスを備えています。



コンフィギュレーション

ステップ 1 : [Cisco Defense Orchestrator](#)(CDO)にログインします。

ステップ 2 : Inventoryペインに移動し、青色のプラス(+)ボタンを選択してデバイスをオンボーディングします。



ステップ 3 : FTDオプションを選択します。

What would you like to onboard?

Select a Device or Service Type

No Secure Device Connector found to communicate with some types of devices. [Set up a Secure Device Connector](#)


| | | |
|---|--|---|
| ASA Adaptive Security Appliance (8.4+) | Multiple ASAs Adaptive Security Appliance (8.4+) | FTD Cisco Secure Firewall Threat Defense |
| Meraki Meraki Security Appliance | Integrations Enable basic CDO functionality for integrations | VPC AWS VPC Amazon Virtual Private Cloud |
| Duo Admin Duo Admin Panel | Umbrella Umbrella Organization View Umbrella Organization Policies from CDO | Import Import configuration for offline management |

ステップ4オンボードFTDデバイスのセクションに進み、登録プロセスを開始します。脅威対策デバイスのオンボーディングに使用できる方法に注意することが重要です。

- シリアル番号別：この方式は、サポートされているソフトウェアバージョンを使用する Firepower 1000、Firepower 2100、セキュアファイアウォール3100シリーズなどの物理デバイスに適用されます。シャーシまたはPCAのシリアル番号とインターネットへのネットワーク接続が必要になります。
- 登録キーによる：これは、デバイスのIPアドレスに変更があった場合でもCDOとの接続を維持するのに役立つため、オンボーディングに適した方法です。特に、DHCP経由でIPアドレスを受信するデバイスに適しています。
- クレデンシャルの使用：ネットワーク内のデバイス設定に合わせて、デバイスのクレデンシャルと、外部、内部、または管理インターフェイスのIPアドレスを入力する方法もあります。

このプロセスでは、FDMオプションを選択してからUse Registration Keyオプションを選択し、デバイスIPアドレスの潜在的な変更に関係なく、CDOへの一貫した接続を確保します。


Follow the steps below Cancel



Firewall Threat Defense
Management Mode:


FTD ⓘ FDM ⓘ
(Recommended)

Important: This method of onboarding allows for local co-management of the firewall via FDM. To manage your device with cloud-delivered Firewall Management System, click the FTD button instead. [Learn more](#)




Use Registration Key

Onboard a device using a registration key generated from CDO and applied on the device using Firepower Device Manager.



Use Serial Number

Use this method for low-touch provisioning or for onboarding configured devices using their serial number.
(FTD 6.7+, 1000, 2100 and 3100 series only)




Use Credentials (Basic)

Onboard a device using its IP address, or host name, and a username and password.

ステップ 5 : Device Nameフィールドに目的のデバイス名を入力し、Policy Assignmentを指定します。また、デバイスに関連付ける必要があるサブスクリプションライセンスも選択します。


Follow the steps below Cancel



Firewall Threat Defense
Management Mode:


FTD ⓘ FDM ⓘ
(Recommended)

Important: This method of onboarding allows for local co-management of the firewall via FDM. To manage your device with cloud-delivered Firewall Management System, click the FTD button instead. [Learn more](#)




Use Registration Key

Onboard a device using a registration key generated from CDO and applied on the device using Firepower Device Manager.



Use Serial Number

Use this method for low-touch provisioning or for onboarding configured devices using their serial number.
(FTD 6.7+, 1000, 2100 and 3100 series only)



Use Credentials (Basic)

Onboard a device using its IP address, or host name, and a username and password.

1 Device Name

Device Name

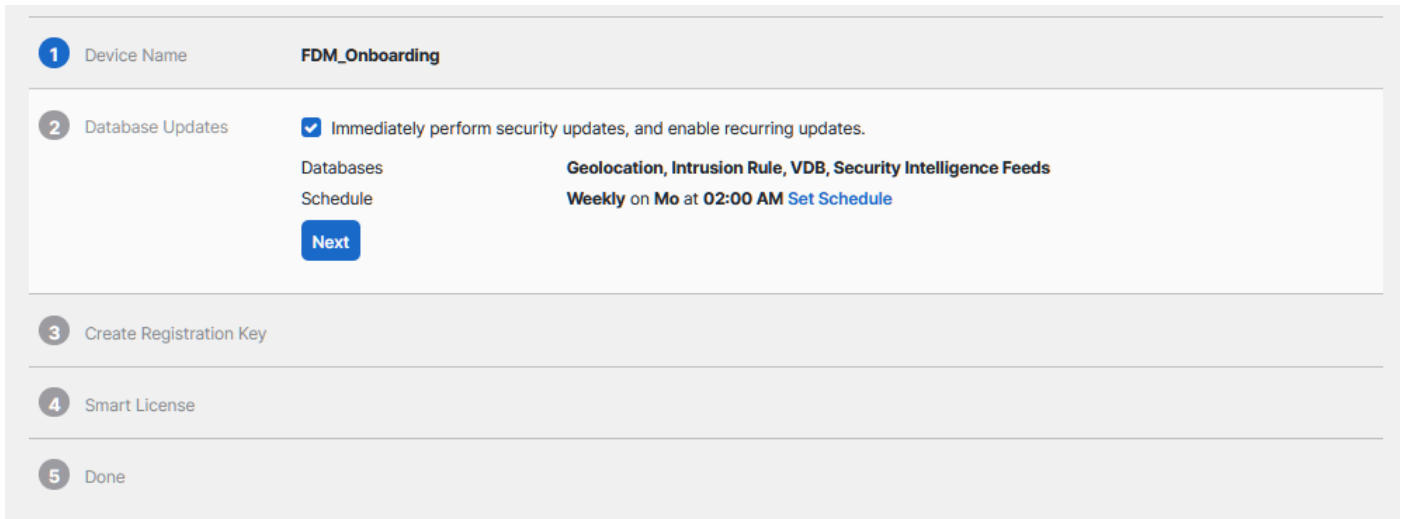
Next

Important: If you already have a SecureX or Cisco Threat Response (CTR) account, you will need to merge your CDO tenant and SecureX/CTR account in order for your devices to be registered with SecureX. You can do so through the SecureX portal. See [Merge Your CDO and SecureX Accounts](#) for instructions.

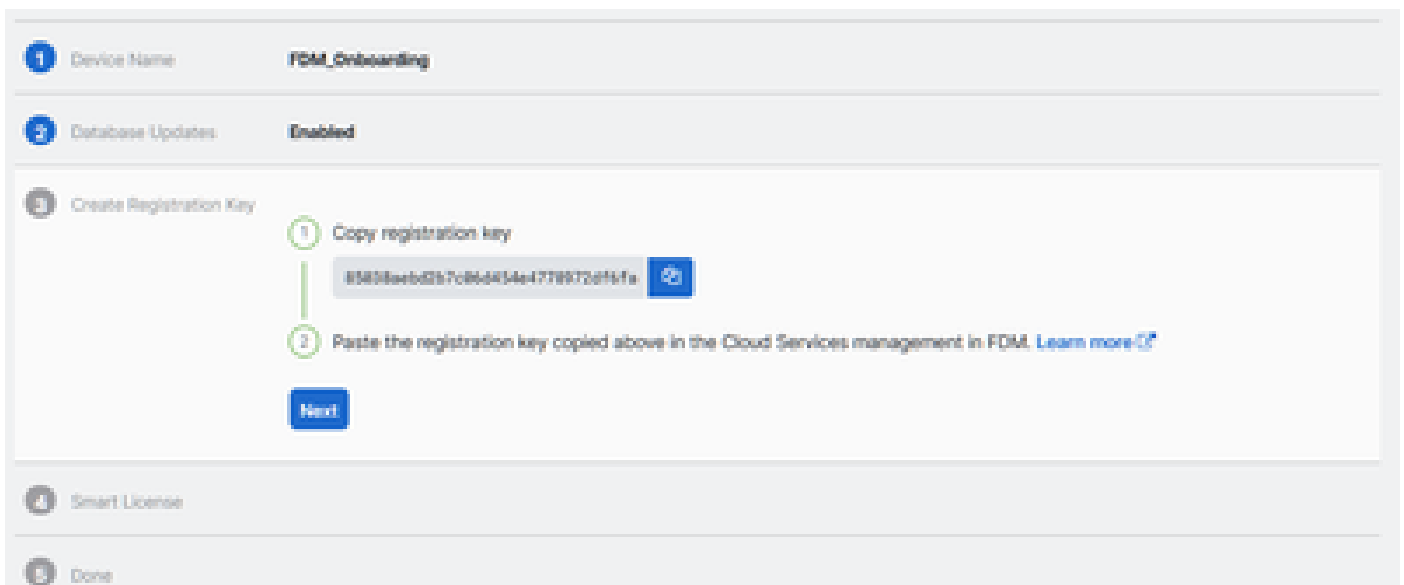
Until your accounts are merged, you will not be able to see your device's events in SecureX or benefit from other SecureX features.

2 Database Updates

手順 6 : Database Updatesセクションは、セキュリティ更新を即時に実行し、定期的な更新を設定するようにデフォルトで設定されています。この設定を変更しても、Secure Firewallデバイスマネージャで確立された既存の更新スケジュールは変更されません。



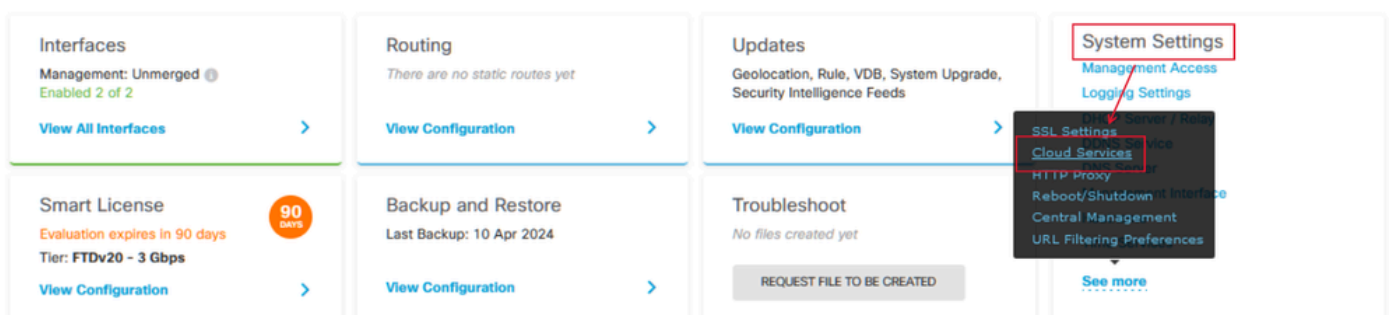
手順 7： CLI Registration Keyセクションでは、CDOが登録キーを自動生成します。完了前にオンボーディングインターフェイスを終了すると、インベントリ内のデバイスのプレースホルダが作成されます。登録キーは、この場所から後で必要に応じて取得できます。



ステップ 8： [コピー]アイコンを使用して、生成された登録キーをコピーします。

ステップ 9： CDOへのオンボーディングに使用するSecure Firewall Device Manager(SDM)デバイスにアクセスします。

ステップ 10： System SettingsメニューからCloud Servicesを選択します。




ステップ 11 テナントの地理的位置に合わせて、正しいシスコクラウドのリージョンをリージョンのドロップダウンで指定します。

- defenseorchestrator.comについては、USを選択します。
- defenseorchestrator.euについては、EUを選択します。
- apj.cdo.cisco.comの場合は、APJを選択します。

Device Summary

Cloud Services

 **Not Registered**

You can register the device with the Cisco cloud to use additional cloud-based services. If you want to use Cisco Defense Orchestrator (CDO) for management or want to remain in evaluation mode, then register with the cloud using your CDO or other security account registration key. You can alternatively auto-enroll with CDO or a Secure Firewall Management Center using the device serial number. If you want to use Secure Firewall device manager for management and are ready to license the device, then configure Smart Licensing, which automatically registers the device with the Cisco cloud. After you register with the cloud, you can enable or disable features as needed.

Enrollment Type

Security/CDO Account

Smart Licensing

Region

US Region

Registration Key

85038aebd2b7c06d454e4778972df6fa

Service Enrollment


Cisco Defense Orchestrator

Cisco Defense Orchestrator is a cloud-based management tool used for managing network devices. Select this option if you want to register the device in your Cisco Defense Orchestrator account.

Enable Cisco Defense Orchestrator

Cisco Success Network

Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network.

Check out the [Sample Data](#) that will be sent to Cisco. [See more](#) 

Enroll Cisco Success Network

REGISTER

[Need help?](#) 

ステップ 12 [登録の種類]セクションで、セキュリティアカウントを選択します。

Device Summary

Cloud Services



Not Registered

You can register the device with the Cisco cloud to use additional cloud-based services. If you want to use Cisco Defense Orchestrator (CDO) for management or want to remain in evaluation mode, then register with the cloud using your CDO or other security account registration key. You can alternatively auto-enroll with CDO or a Secure Firewall Management Center using the device serial number. If you want to use Secure Firewall device manager for management and are ready to license the device, then configure Smart Licensing, which automatically registers the device with the Cisco cloud. After you register with the cloud, you can enable or disable features as needed.

Enrollment Type

Security/CDO Account

Smart Licensing

Region

US Region

Registration Key

85038aebd2b7c06d454e4778972df6a

Service Enrollment

Cisco Defense Orchestrator

Cisco Defense Orchestrator is a cloud-based management tool used for managing network devices. Select this option if you want to register the device in your Cisco Defense Orchestrator account.

Enable Cisco Defense Orchestrator

Cisco Success Network

Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network.

Check out the [Sample Data](#) that will be sent to Cisco. [See more](#) ▾

Enroll Cisco Success Network


REGISTER

Need help?

ステップ 13 Registration Keyフィールドに登録キーを貼り付けます。

Device Summary

Cloud Services

 Not Registered

You can register the device with the Cisco cloud to use additional cloud-based services. If you want to use Cisco Defense Orchestrator (CDO) for management or want to remain in evaluation mode, then register with the cloud using your CDO or other security account registration key. You can alternatively auto-enroll with CDO or a Secure Firewall Management Center using the device serial number. If you want to use Secure Firewall device manager for management and are ready to license the device, then configure Smart Licensing, which automatically registers the device with the Cisco cloud. After you register with the cloud, you can enable or disable features as needed.

Enrollment Type

Security/CDO Account

Smart Licensing

Region

US Region

Registration Key

85038aebd2b7c06d454e4778972d96fa

Service Enrollment

Cisco Defense Orchestrator

Cisco Defense Orchestrator is a cloud-based management tool used for managing network devices. Select this option if you want to register the device in your Cisco Defense Orchestrator account.

Enable Cisco Defense Orchestrator

Cisco Success Network

Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network.

Check out the [Sample Data](#) that will be sent to Cisco. [See more](#) ▼

Enroll Cisco Success Network

REGISTER

Need help? 

ステップ 14 : バージョン6.7以降のデバイスでは、Cisco Defense Orchestratorがサービス登録セクションで有効になっていることを確認します。

Device Summary

Cloud Services



Not Registered

You can register the device with the Cisco cloud to use additional cloud-based services. If you want to use Cisco Defense Orchestrator (CDO) for management or want to remain in evaluation mode, then register with the cloud using your CDO or other security account registration key. You can alternatively auto-enroll with CDO or a Secure Firewall Management Center using the device serial number. If you want to use Secure Firewall device manager for management and are ready to license the device, then configure Smart Licensing, which automatically registers the device with the Cisco cloud. After you register with the cloud, you can enable or disable features as needed.

Enrollment Type

Security/CDO Account

Smart Licensing

Region

US Region

Registration Key

65038aebd2b7c06d454e4778973df6fa



Service Enrollment

Cisco Defense Orchestrator

Cisco Defense Orchestrator is a cloud-based management tool used for managing network devices. Select this option if you want to register the device in your Cisco Defense Orchestrator account.

Enable Cisco Defense Orchestrator

Cisco Success Network

Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network.

Check out the [Sample Data](#) that will be sent to Cisco. [See more](#) ▾

Enroll Cisco Success Network

REGISTER

Need help? [?](#)

ステップ15: (オプション) Cisco Success Network Enrollmentの詳細を確認します。参加しない場合は、Enroll Cisco Success Networkチェックボックスの選択を解除します。

ステップ 16 : Registerを選択し、シスコによる情報開示を受け入れます。Secure Firewall Device Manager(SDM)は、登録をCDOに送信します。

Device Summary
Cloud Services

Not Registered

You can register the device with the Cisco cloud to use additional cloud-based services. If you want to use Cisco Defense Orchestrator (CDO) for management or want to remain in evaluation mode, then register with the cloud using your CDO or other security account registration key. You can alternatively auto-enroll with CDO or a Secure Firewall Management Center using the device serial number. If you want to use Secure Firewall device manager for management and are ready to license the device, then configure Smart Licensing, which automatically registers the device with the Cisco cloud. After you register with the cloud, you can enable or disable features as needed.

Enrollment Type
Security/CDO Account Smart Licensing

Region
US Region

Registration Key
85038aebd2b7c06d454e4778972d6fa

Service Enrollment

Cisco Defense Orchestrator
Cisco Defense Orchestrator is a cloud-based man devices. Select this option if you want to register if account.
 Enable Cisco Defense Orchestrator

Cisco Success Network
Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network.
Check out the [Sample Data](#) that will be sent to Cisco. [See more](#) ▼
 Enroll Cisco Success Network

REGISTER Need help?

Cisco Disclosure
Your device establishes a secure connection to the Cisco Cloud so that your device can participate in additional service offerings from Cisco such as technical support services, cloud management and monitoring services. Your device will establish and maintain this secure connection at all times. You can turn off this connection at any time by disabling Cisco Success Network, Cisco SecureX threat response and Cisco Defense Orchestrator. Disabling all will disconnect the device from the cloud.
Disconnection of Cisco Success Network, Cisco SecureX threat response and Cisco Defense Orchestrator will not impact the receipt of Updates or operation of the Smart Licensing capabilities; such functions will continue to operate normally.

DECLINE ACCEPT

ステップ 17 : CDOに戻り、登録キー作成領域でNextを選択します。

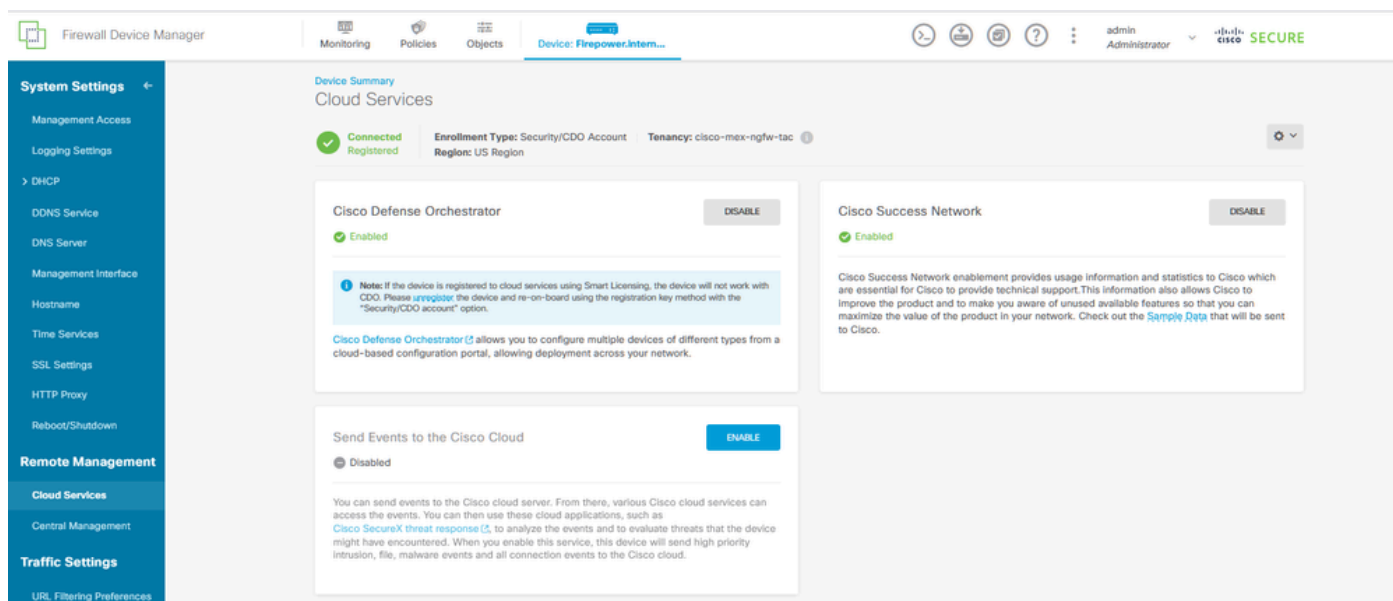
ステップ18: (オプション) デバイス用のライセンスを特定して選択し、 Nextを選択して続行します。

ステップ 19 : CDOインベントリのデバイスステータスが、UnprovisionedからLocating、Syncing、最後にSyncedに移行していることを確認します。

確認

ここでは、設定が正常に機能しているかどうかを確認します。

CDOポータルに移動し、デバイスステータスを確認します。OnlineとSyncedが表示されています。また、ステータスの確認はFDM GUIを介して実行できます。System > Cloud Servicesの順に選択し、Cisco Defense OrchestratorとCisco Success Networkの接続ステータスを確認します。インターフェイスにConnectedステータスが表示され、サービスとの統合が正常に完了したことが確認されます。



トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

- クラウドサービスFQDNエラーの解決

クラウドサービスFQDNを解決できないためにデバイス登録が失敗した場合は、ネットワーク接続またはDNS設定を確認し、デバイスのオンボーディングを再試行します。

- 無効な登録キーエラー

ファイアウォールデバイスマネージャに無効な登録キーが入力されたことが原因でデバイスの登録が完了しない場合は、Cisco Defense Orchestratorから正しい登録キーのコピーに進み、登録プロセスを再試行します。デバイスがすでにスマートライセンスを取得している場合は、ファイアウォールデバイスマネージャで登録キーを入力する前に、スマートライセンスを削除します。

- ライセンス不足の問題

デバイスの接続ステータスが「ライセンス不足」を示している場合は、次の手順を実行します。

1. Cisco Smart Software Managerではデバイスに新しいライセンスを適用するために期間が必要になる場合があるため、デバイスがライセンスを取得するまで少し時間をおきます。
2. デバイスのステータスが変更されない場合は、CDOポータルを更新するために、サインアウトしてから再度サインインし、ライセンスサーバーとデバイス間のネットワーク通信の問題を解決してください。
3. ポータルを更新してもデバイスのステータスが更新されない場合は、次の操作を実行します。
 - [Cisco Smart Software Manager](#)から新しい登録キーを生成してコピーします。手順については、『[Generate Smart Licensing](#)』ビデオを参照してください。
 - CDOナビゲーションバーでInventoryページを選択します。
 - Insufficient License状態でリストされたデバイスを選択します。
 - デバイスの詳細ペインで、Insufficient Licensesアラートの下にあるManage Licensesをクリックします。[ライセンスを管理]ウィンドウが表示されます。
 - Activateフィールドに新しい登録キーをペーストして、Register Deviceを選択します。

新しい登録キーが正常に適用されると、デバイスの接続状態は「Online」に変わります。

登録キーに別の方法を使用してFirepower Device Manager(FDM)を登録する際の包括的なガイドランスについては、『[FDM管理対象デバイスのトラブルシューティング](#)』リンクで提供される詳細なドキュメントを参照してください。

このリソースでは、FDMをCisco Defense Orchestrator(CDO)に正常にオンボーディングするために使用できるさまざまな登録技術の手順とトラブルシューティングのヒントを示します。

関連情報

- [FDM管理対象デバイスのトラブルシューティング](#)
- [Cisco Defense OrchestratorでのFDMデバイスの管理](#)
- [シスコのテクニカルサポートとダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。