SCC上のオンプレミマネージドFMCを使用したUniversal ZTNAのセキュアアクセスの設定

内容

はじめに

このドキュメントでは、セキュアなアクセスと、オンプレミス仮想FMCによって管理される仮想FTDを使用してユニバーサルZTNAを設定する方法について説明します。

前提条件

- 7.7.10以降のソフトウェアバージョンを使用して、Firewall Management Center(FMC)とFirewall Threat Defense(FTD)を導入する必要があります。
- ファイアウォール脅威対策(FTD)は、ファイアウォール管理センター(FMC)で管理する必要

があります
- ファイアウォール脅威対策(FTD)は、暗号化（エクスポート機能を有効にして強力な暗号化を有効にする必要があります）、セキュリティ制御に必要なIPSおよび脅威ライセンスとともにライセンスを取得する必要があります
- ファイアウォール脅威対策(FTD)の基本設定は、インターフェイスやルーティングなどのFirewall Management Center(FMC)から実行する必要があります。
- アプリケーションのFQDNを解決するには、FMCのデバイスにDNS設定を適用する必要があります
- Cisco Secure Clientのバージョンは5.1.10以降である必要があります。
- セキュリティクラウド制御は、ファイアウォールおよびセキュアアクセスマイクロアプリケーションとUZTNA機能フラグが有効になっている顧客にプロビジョニングされます。

要件

- cdFMCおよびFirewall Threat Defense(FTD)デバイスを含むすべてのSecure Firewall Management Center(FMC)で、ソフトウェアバージョン7.7.10以降が稼働している必要があります。
- ファイアウォール脅威対策(FTD)は、ファイアウォール管理センターで管理する必要があります。ローカルマネージャのファイアウォール防御マネージャ(FDM)はサポートされていません
- すべてのファイアウォール脅威対策(FTD)デバイスは、ルーテッドモードに設定する必要があります。トランスペアレントモードはサポートされていません。
- クラスタ化されたデバイスはサポートされていません。
- ハイアベイラビリティ(HA)デバイスがサポートされ、1つのエンティティとして表示されます。
- Secure Clientバージョン5.1.10以降

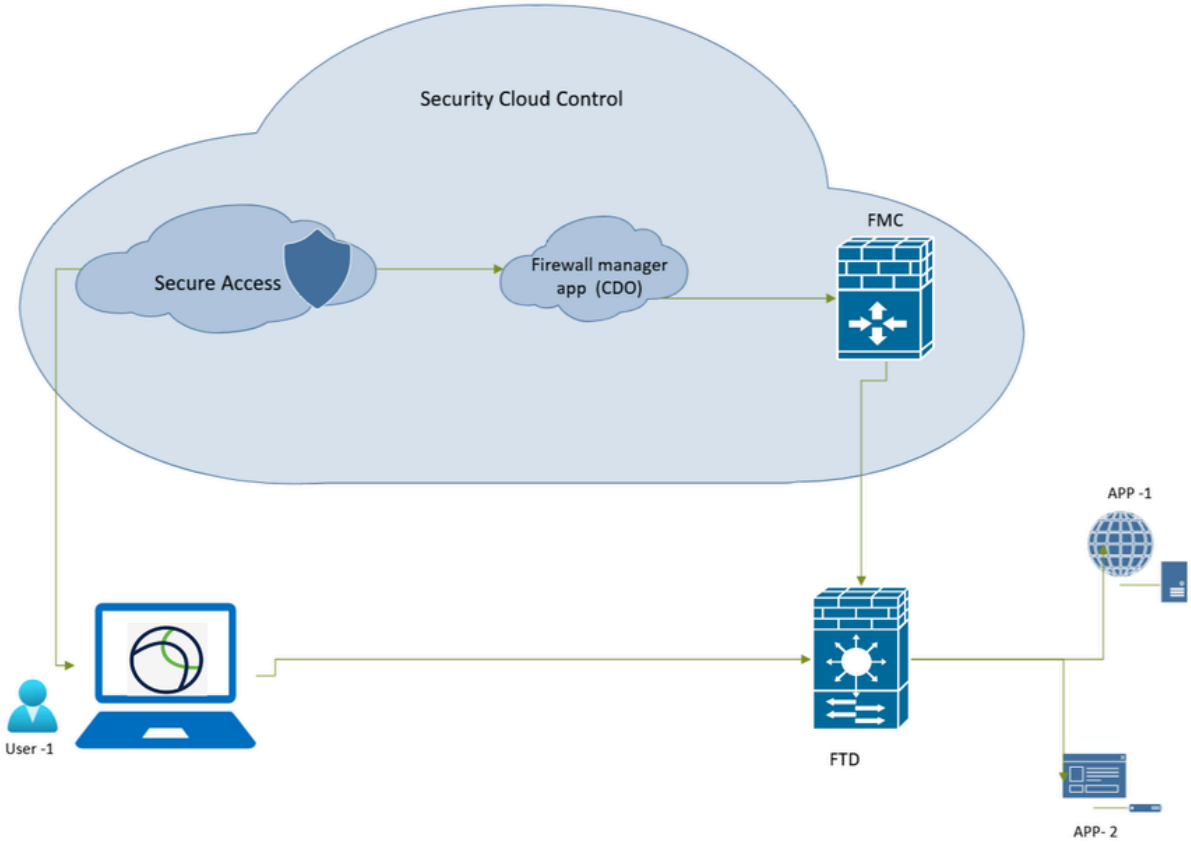
使用するコンポーネント

このドキュメントの情報は、次に基づくものです。

- セキュリティクラウド制御(SCC)
- Secure Firewall Management Center(FMC)バージョン7.7.10
- セキュアファイアウォール脅威対策(FTD)仮想–100バージョン7.7.10
- Secure Client for Windowsバージョン5.1.10
- セキュアなアクセス

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。

ネットワーク図



セキュアアクセス – ネットワークトポロジ

Brackground情報

サポートされるデバイス

サポートされるセキュアファイアウォール脅威対策モデル：

- FPR 1150
- FPR 3105、3110,3120,3130,3140
- FPR4115,4125,4145,4112
- FPR4215,4225,4245
- ファイアウォール脅威対策(FTD)仮想（CPUコア数16以上）

制限事項

- オブジェクト共有
- IPv6はサポートされていません。
- グローバルVRFだけがサポートされます。
- ユニバーサルZTNAポリシーは、デバイスへのサイト間トンネルトラフィックには適用されません。
- クラスタ化されたデバイスはサポートされていません。

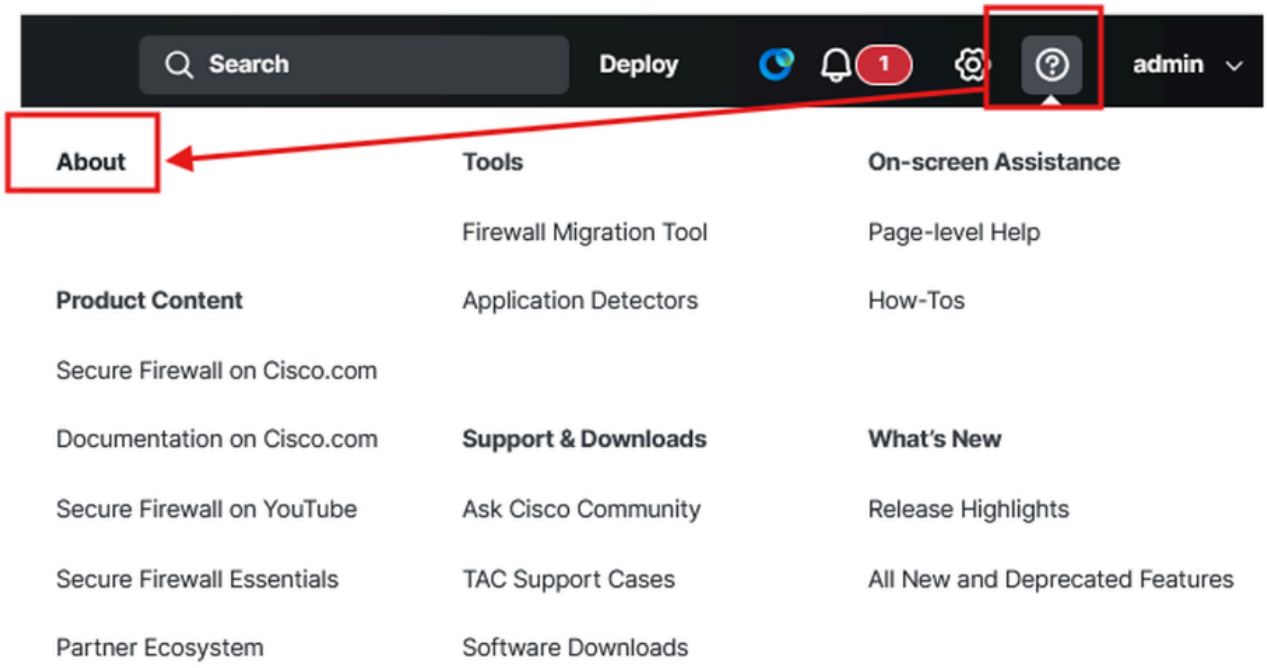
- 4Kおよび9K Firepowerシリーズでコンテナとして導入されるFTDはサポートされません
- ユニバーサルZTNAセッションはジャンボフレームをサポートしない

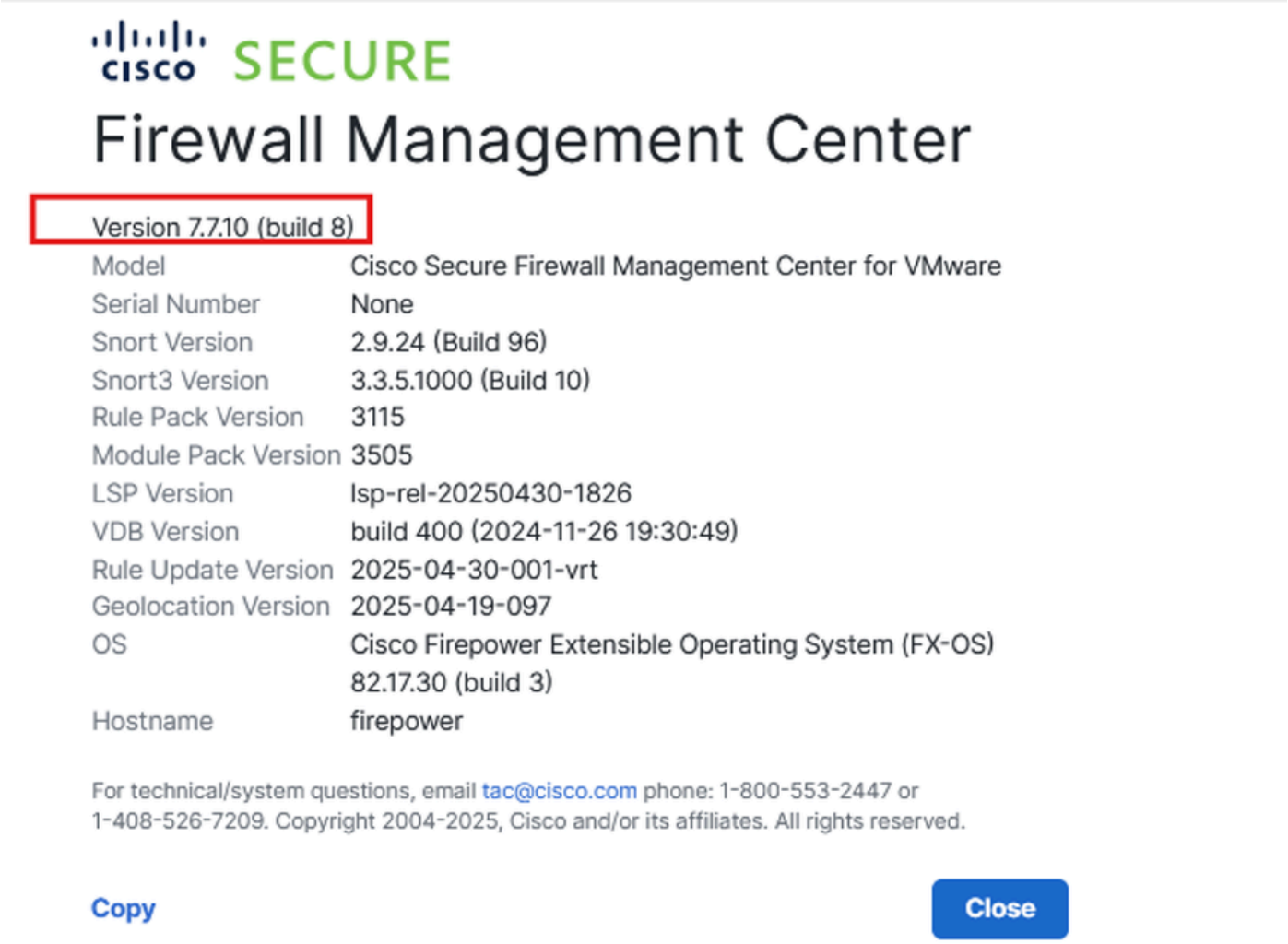
設定

FMCバージョンの確認

ユニバーサルZTNA（7.7.10以上）でサポートされているソフトウェアバージョンで実行されているファイアウォール管理センター(FMC)およびファイアウォールFTDを確認します。

- 右上の?をクリックして、Aboutをクリックします。



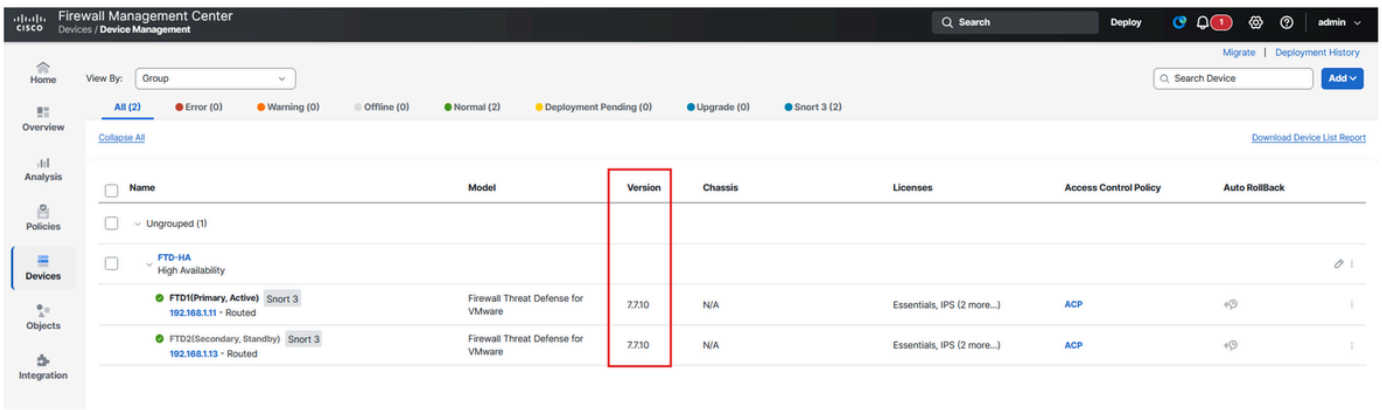


Secure Firewall Management Center – ソフトウェアバージョン

FTDバージョンの確認

FMC UIに移動します。

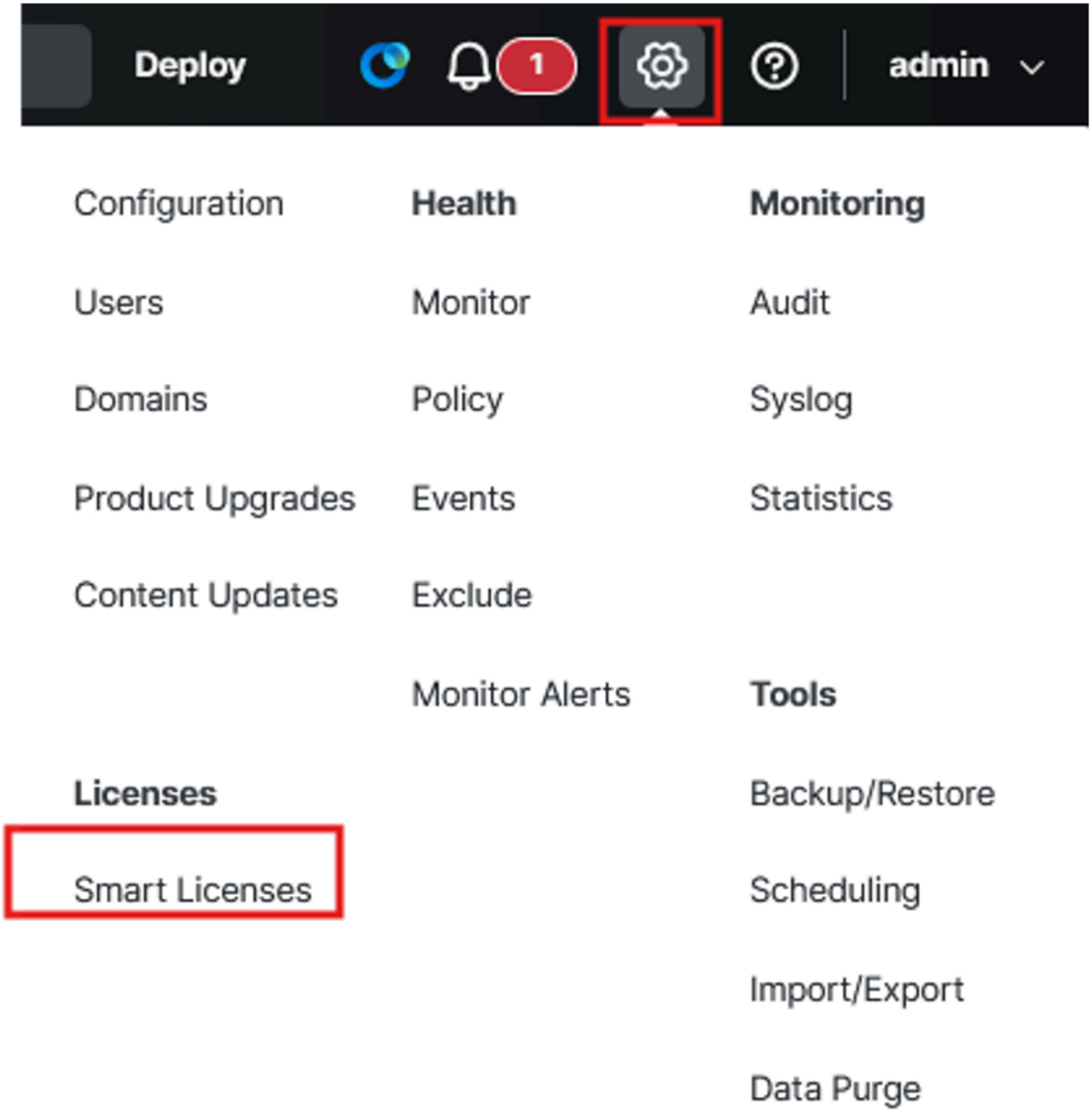
- Devices > Device Managementの順にクリックします。

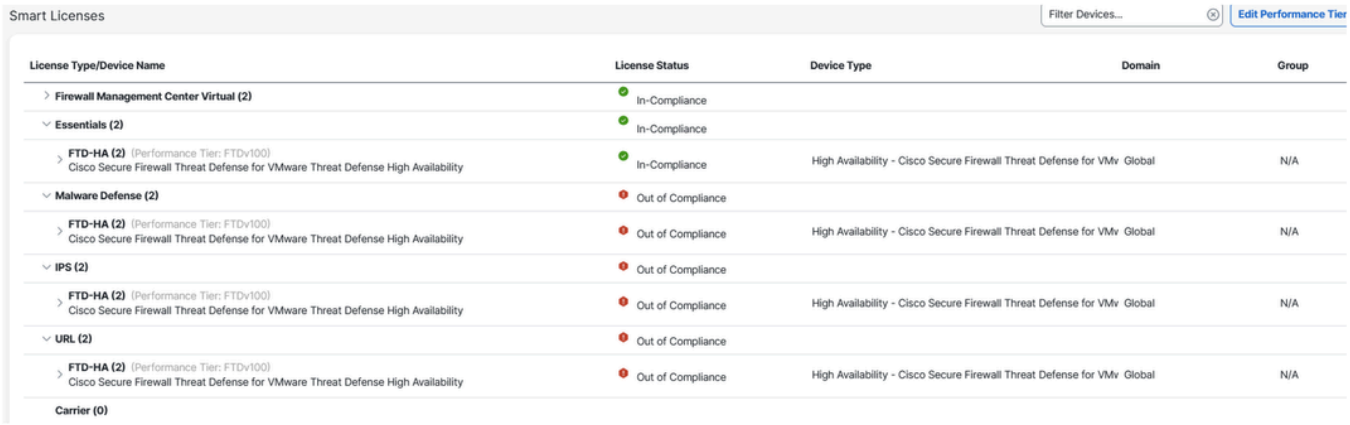


セキュアファイアウォール脅威対策 – ソフトウェアバージョン

FTDライセンスの確認

- Setting Icon > Licenses > Smart Licensesの順にクリックします





セキュアファイアウォール脅威対策 – スマートライセンス

プラットフォーム設定とDNSが正しく設定されていることを確認する

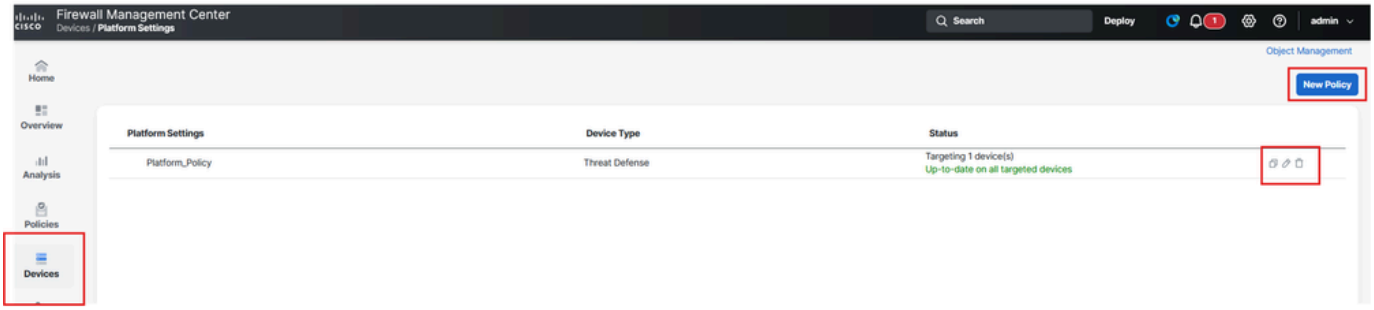
CLI経由でFTDにログインします。

- DNSが設定されているかどうかを確認するには、次のコマンドを実行します。

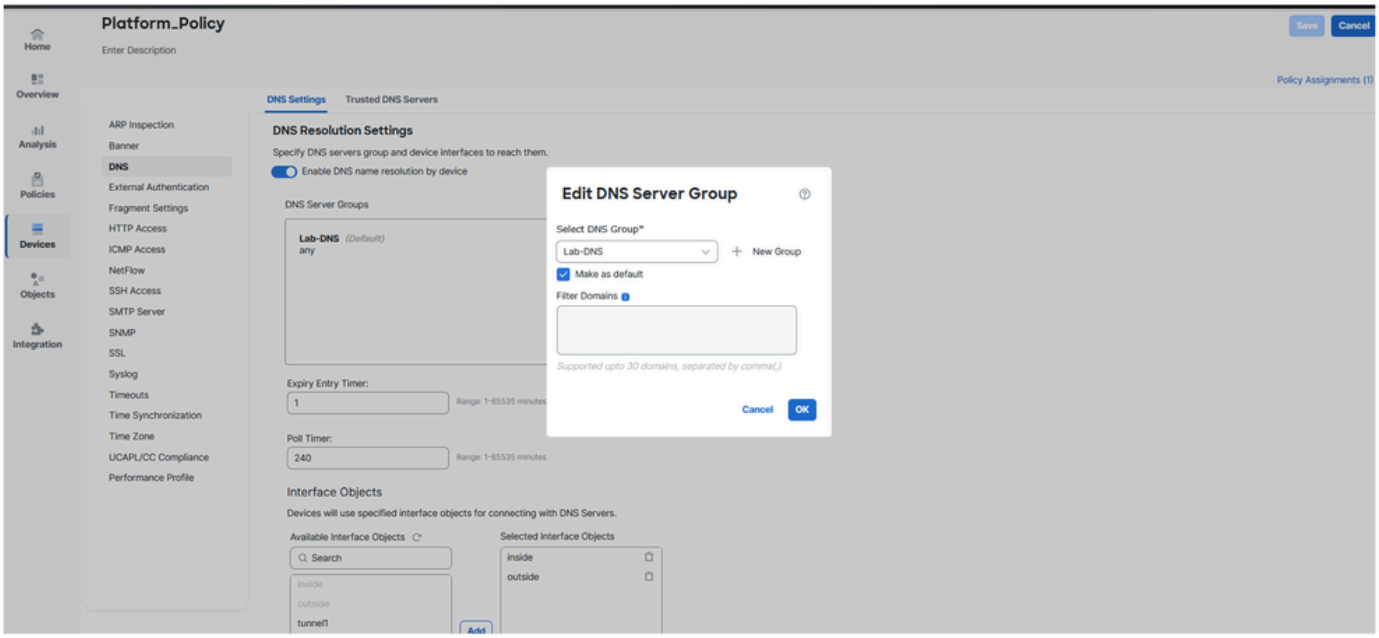
```
show run dns
```

FMCで、次の操作を行います。

- Devices > Platform Settingsの順にクリックし、ポリシーを編集または作成します



セキュアファイアウォール脅威対策 – プラットフォームポリシー



セキュアファイアウォール脅威対策 – DNS設定

FTD cliを使用して、プライベートリソースのIPアドレスとFQDNにpingできることを確認します（FQDNを使用してPRにアクセスする場合）。

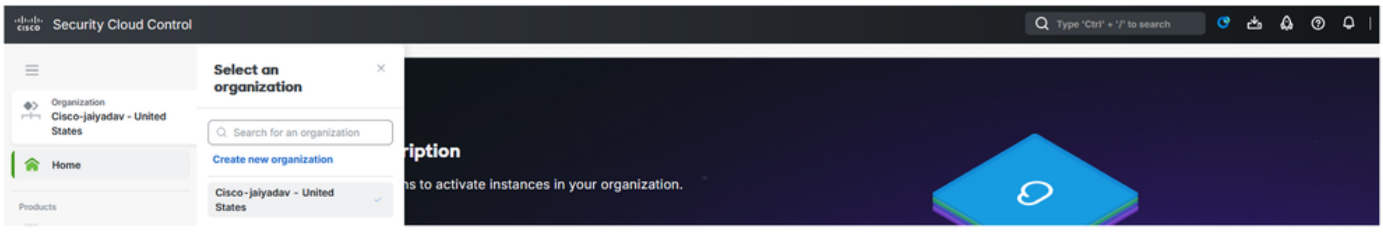
```
ftd1# ping ise.taclab.com
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.50, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
ftd1#
```

CDOでのセキュリティクラウド制御テナントの作成

注：すでにSCCテナントが設定されている場合は、新しいテナントを作成する必要はありません。

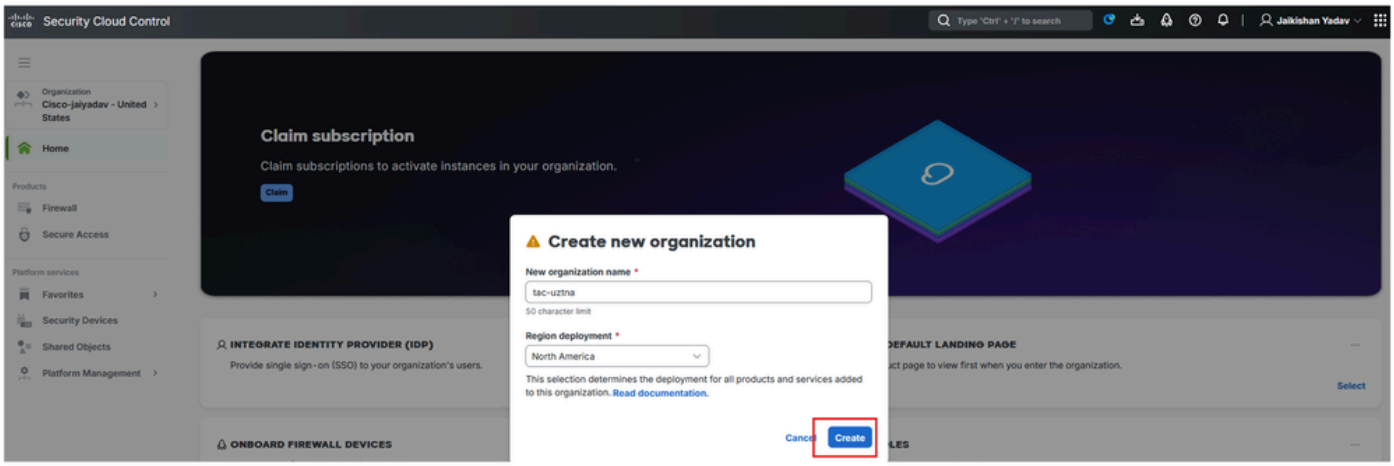
Security Cloud Control:

- onOrganization > Create new organizationの順にクリックします



セキュアなクラウド制御：組織

- Createをクリックします。



セキュアなクラウド制御 – 組織の作成

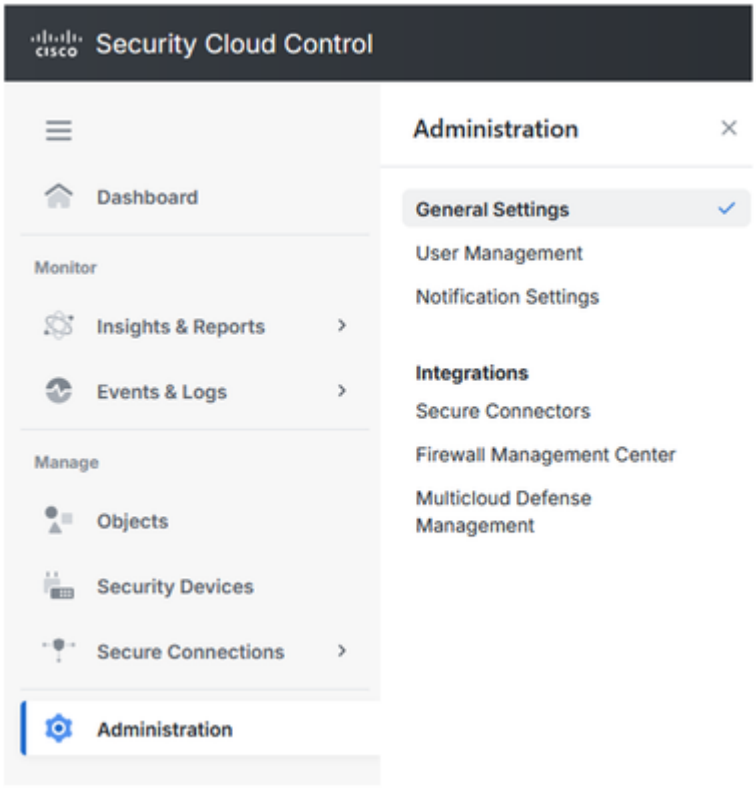
SCCテナントが作成されたら（図1を参照）、テナント情報を収集して、ファイアウォールとセキュアアクセスのマイクロアプリを有効にし、uZTNAを有効にします。

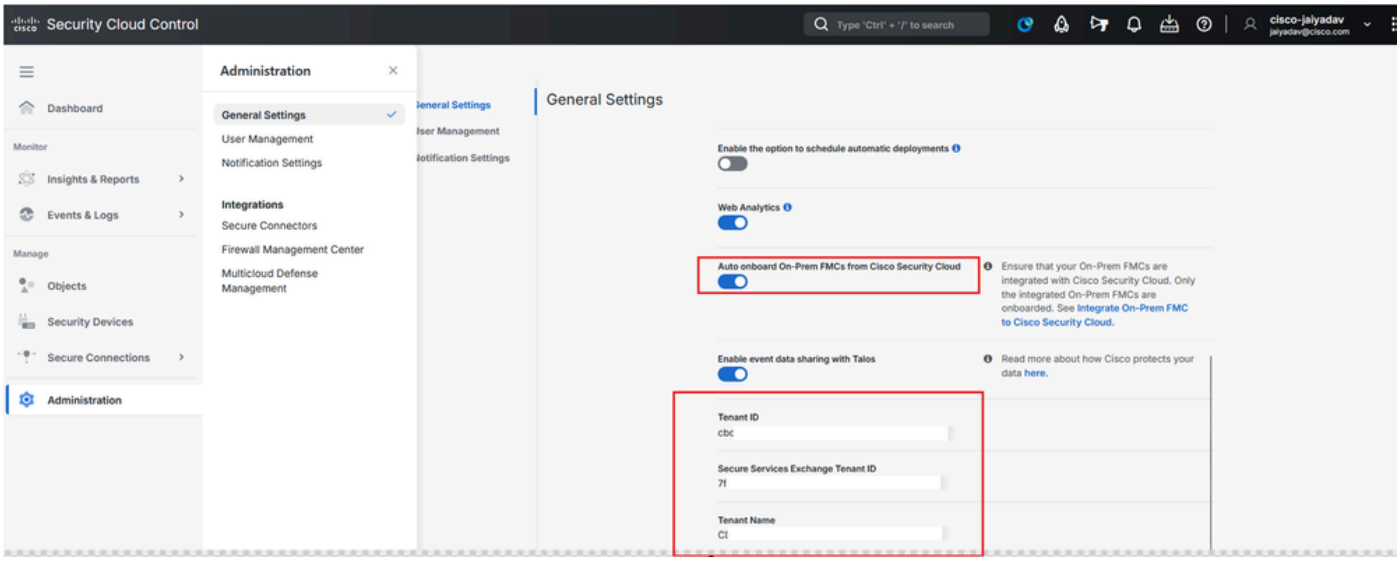
SCCファイアウォールの一般設定が設定されていることを確認する

CDO/SCCに移動します。

- Administration > General Settingsをクリックします。
- Auto Onboard On-Prem FMCs from Cisco Security Cloudオプションが有効になっていることを確認します。

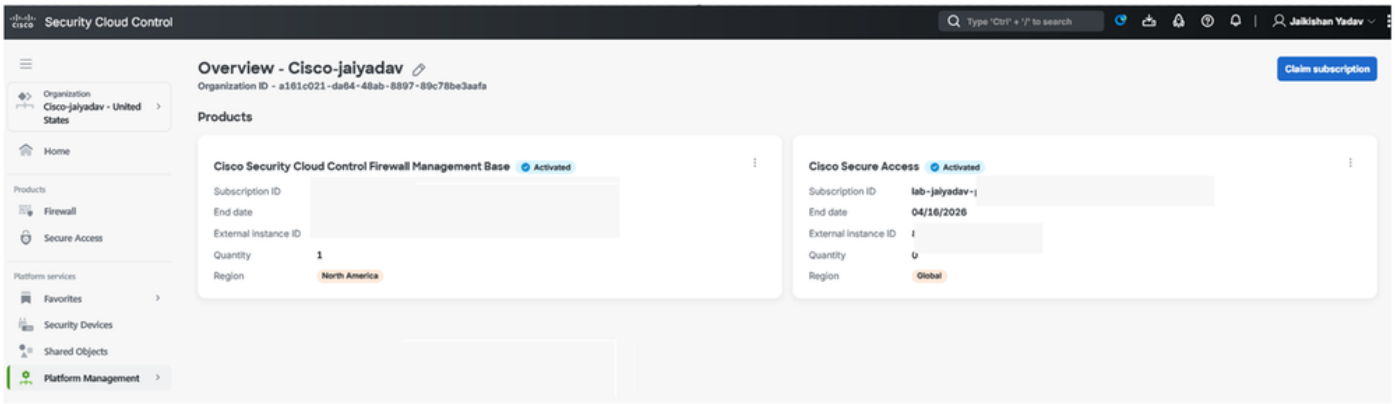
注:Secure Access MicroAppにアクセスするユーザは、 セキュアなアクセス および Security Cloud Controlの管理者ロール。





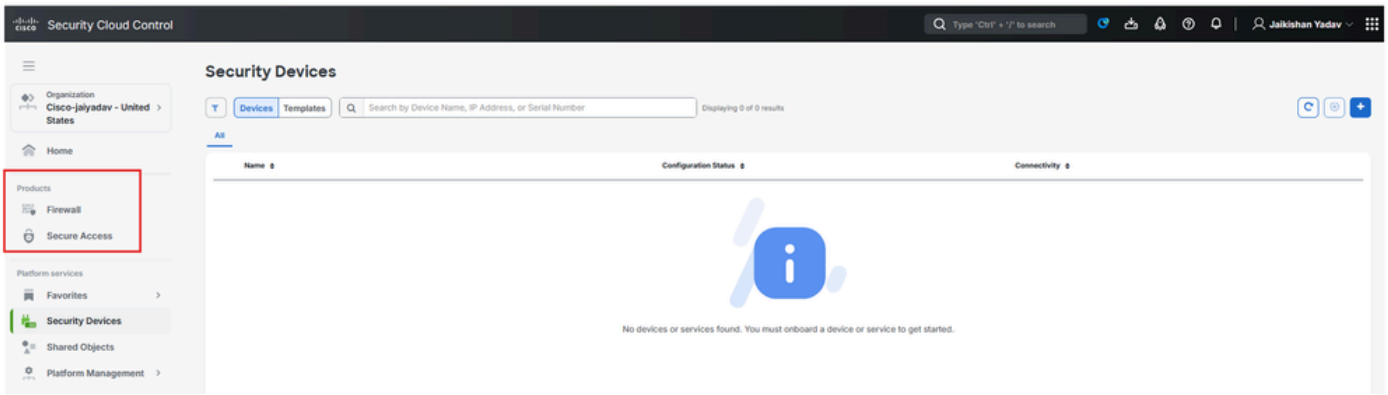
Secure Cloud Control – 組織の詳細

セキュアアクセステナントとセキュリティコントロールファイアウォール管理ベースの統合の確認



Secure Cloud Control – セキュアアクセスアクティベーション

CDOでSecurity Cloud Control Tenantを作成し、CDOでSecurity Cloud Control Tenantを作成するステップを完了すると、SCCダッシュボードにファイアウォールとSecure Accessのマイクロアプリケーションを表示できるようになります。



セキュアなクラウド制御 – マイクロアプリケーション

ファイアウォールの脅威に対する防御(FTD)CA署名付き証明書の生成

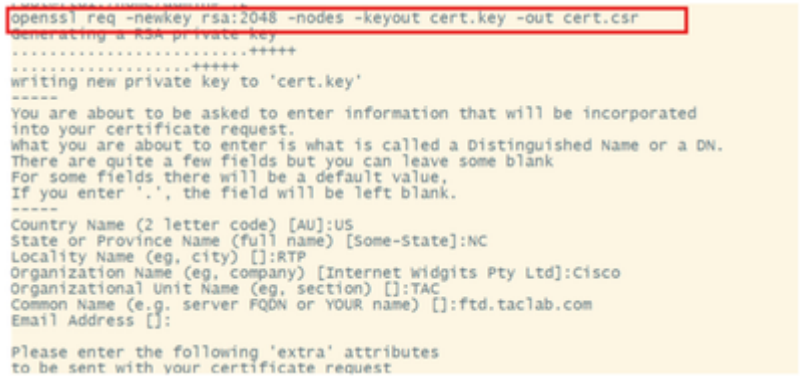
注：FTD自己署名証明書FTD証明書を使用することもできます（「自己署名証明書を使用した内部CA証明書および内部CA証明書の生成」の項を参照）。 証明書はPKCS12形式である必要があり、信頼されたルートCAの下のユーザマシンストアに存在する必要があります。

ビルドopenssl機能でFTDを使用してCA署名付き証明書を生成するには、次の手順を実行します。

- FTDに移動します。
- expert コマンドを実行します

- opensslを使用したCSRとキーの生成
  - OpenSSLコマンド：

```
openssl req -newkey rsa:2048 -nodes -keyout cert.key -out cert.csr
```



証明書署名要求

- CSRをコピーし、CA署名付き証明書を取得する
- FTDのCA署名付き証明書とキーを使用し、証明書をPKCS12形式に変換する
    - OpenSSLコマンド：

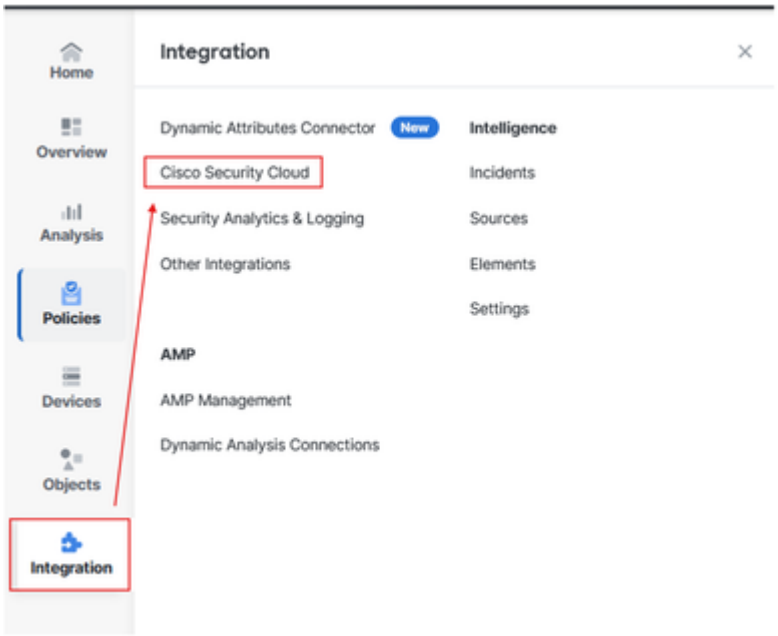
```
openssl pkcs12 -export -out ftdcert.p12 -in cert.crt -inkey cert.key
```

- SCPまたはその他のツールを使用して証明書をエクスポートします。

オンプレミスのファイアウォール管理センターをセキュリティクラウドコントロールにオンボード

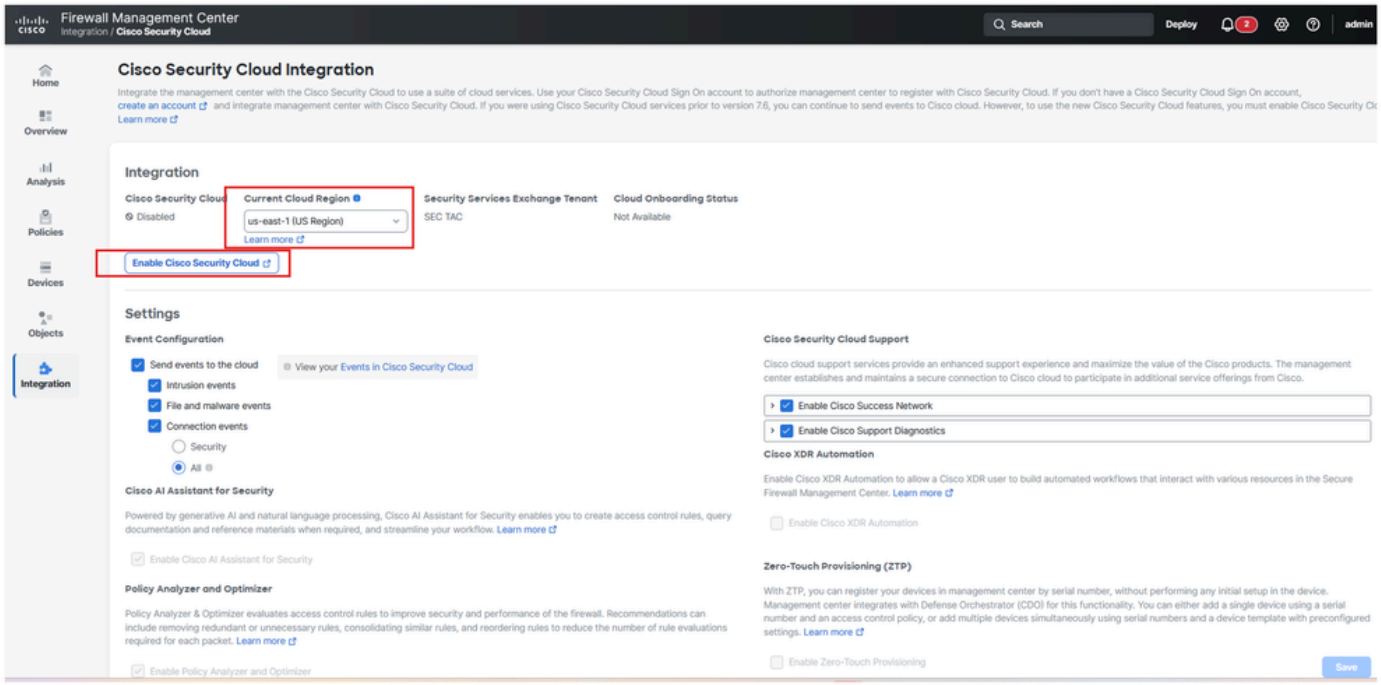
FMCに移動します。

- Integration > Cisco Security Cloudの順にクリックします。



ファイアウォール管理センターとSCCの統合

- クラウドリージョンを選択し、Enable Cisco Security Cloudをクリックします。

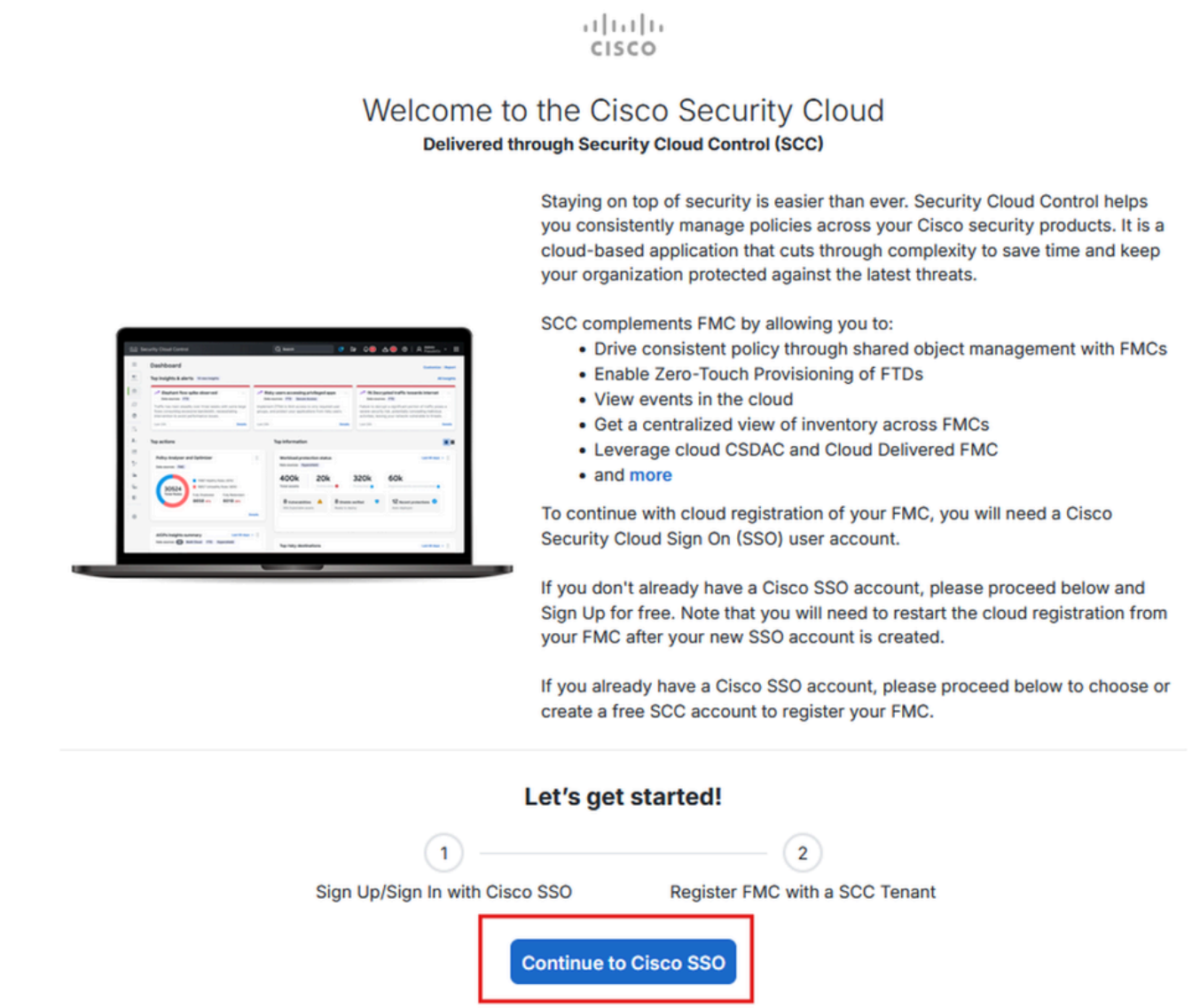


ファイアウォール管理センターのSCCへのオンボーディング

新しいブラウザタブが新しいタブで開きます。

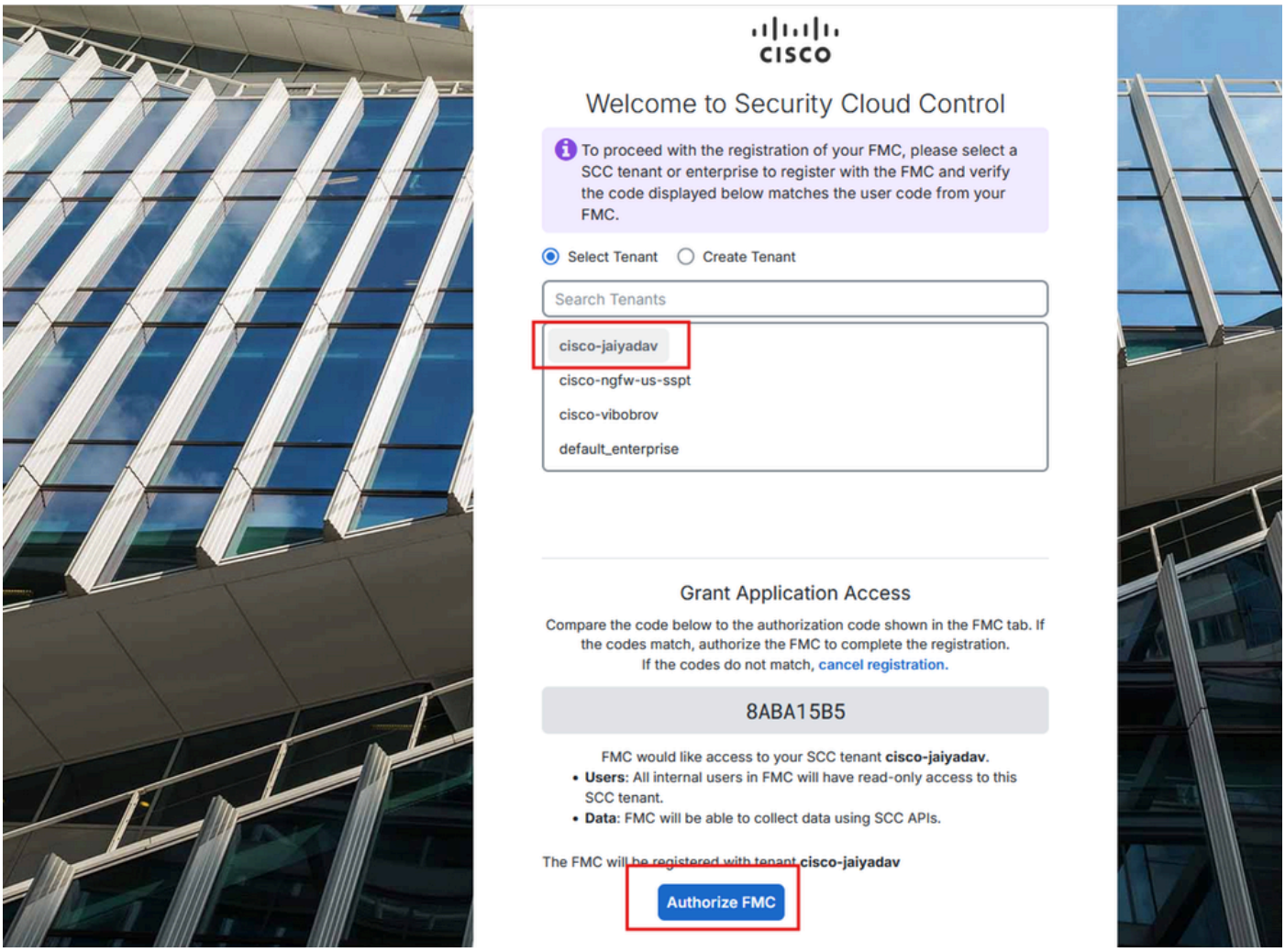
- Continue to Cisco SSOをクリックします。

注:SCCからログアウトしていること、および他のタブが開いていないことを確認します。



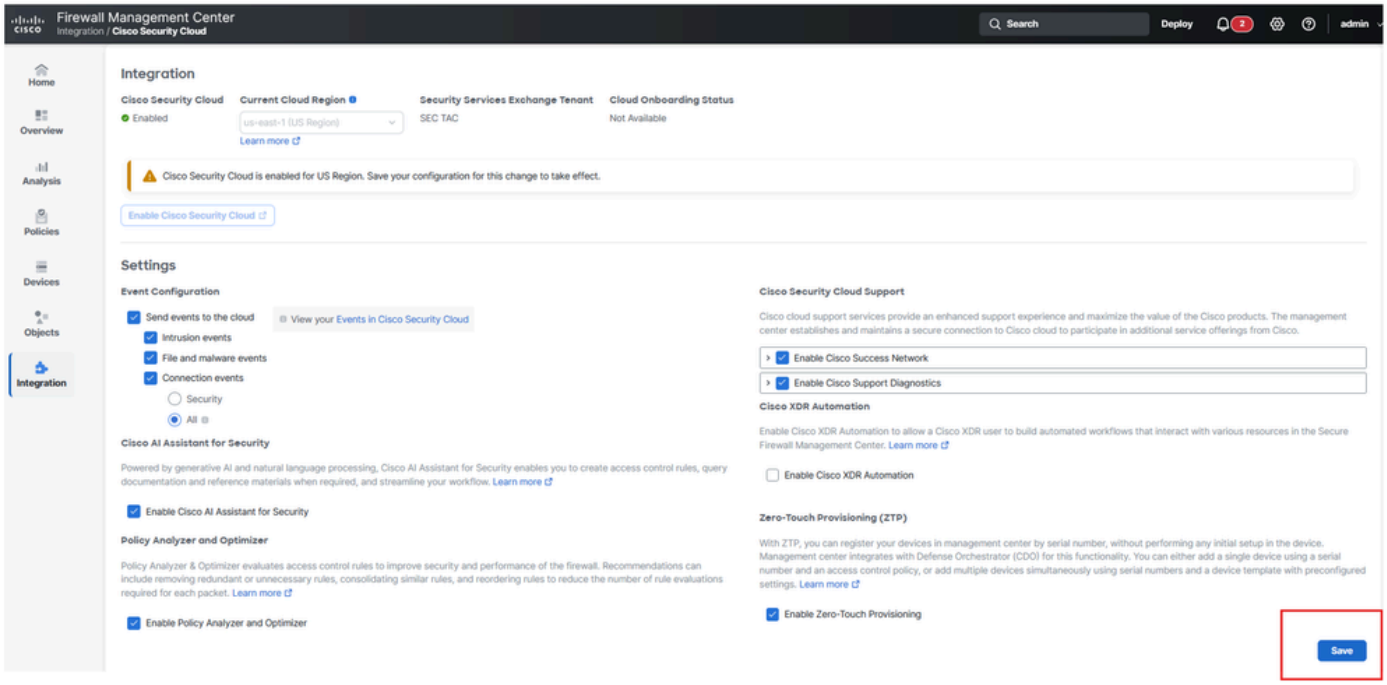
ファイアウォール管理センターのSCCへのオンボーディング

- SCCテナントを選択し、Authorize FMCをクリックします。



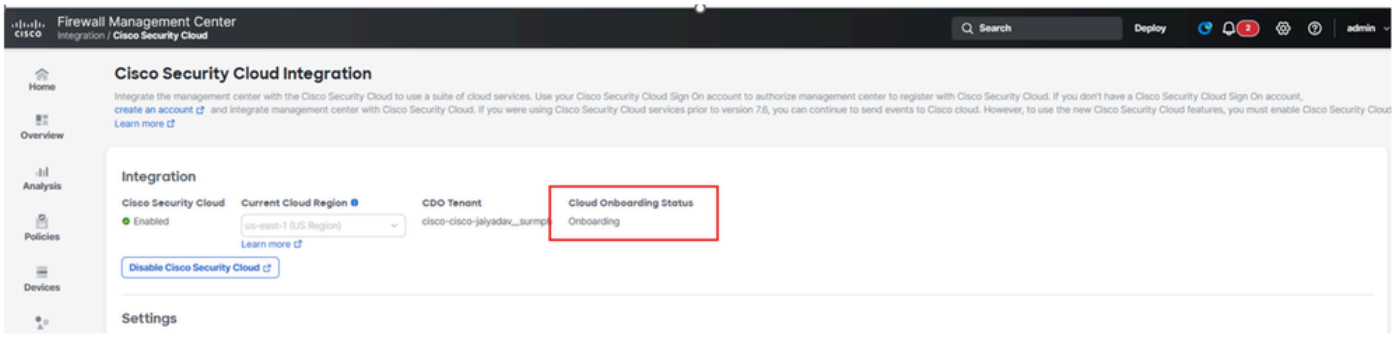
ファイアウォール管理センターのSCCへのオンボーディング

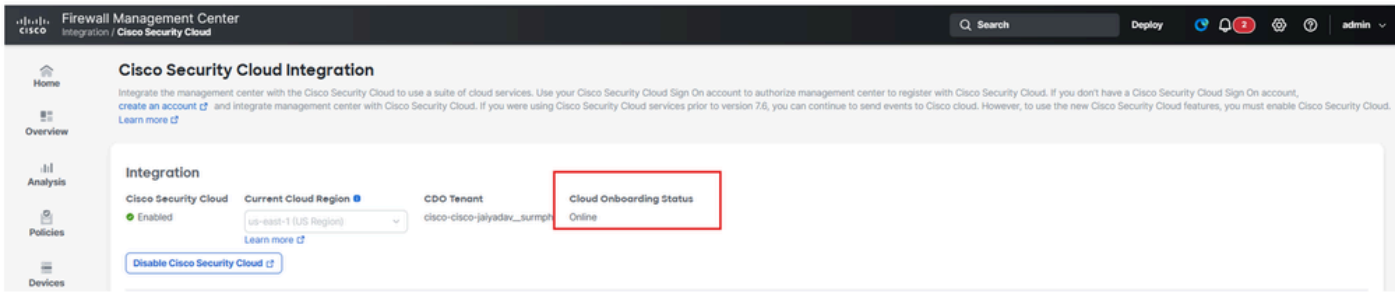
- [Save] をクリックします。



ファイアウォール管理センターのSCCへのオンボーディング

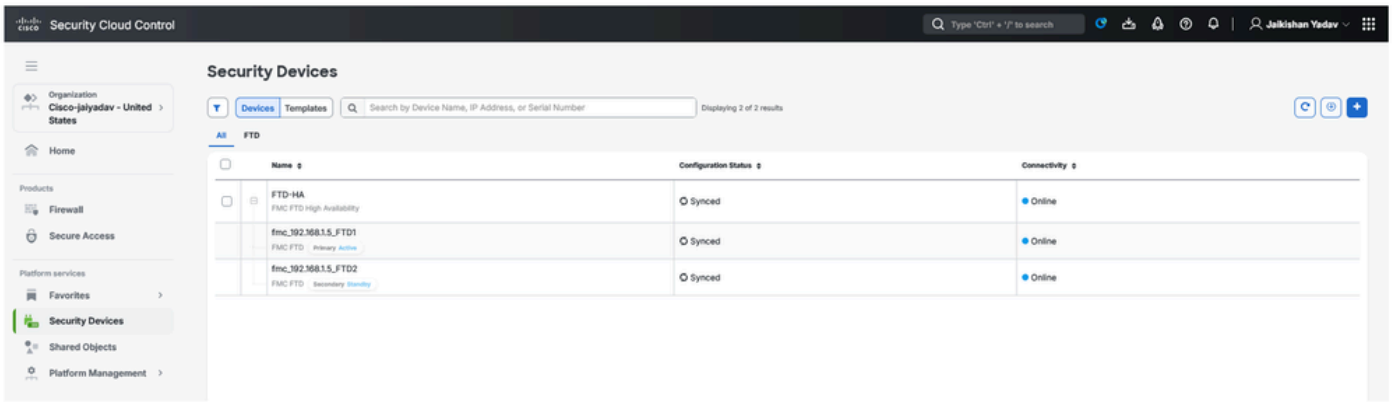
Cloud Onboarding Statusのステータスが Not Available から Onboarding、 Online に変わる必要があります。





ファイアウォール管理センターのオンボーディングステータス

- SCCに移動し、Platform Services > Security DevicesでFTDのステータスを確認します

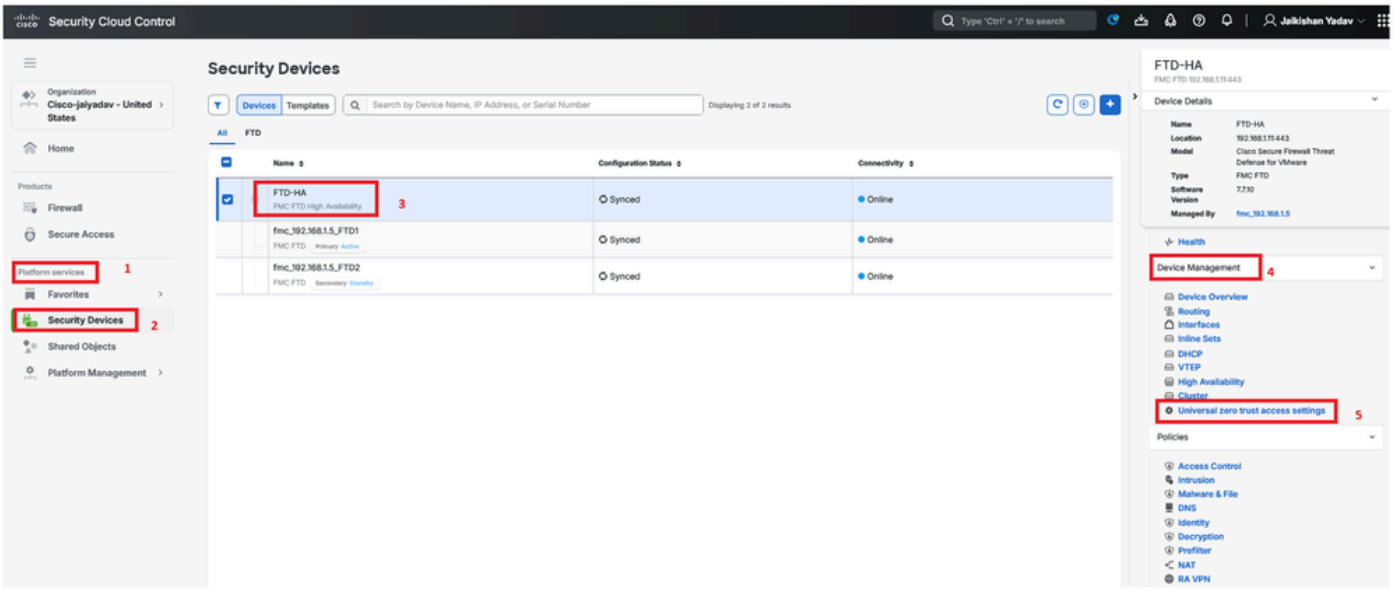


SCCでのセキュアファイアウォール脅威防御のステータス

FTDのUniversal Zero Trust Network Access(uZTNA)設定の登録

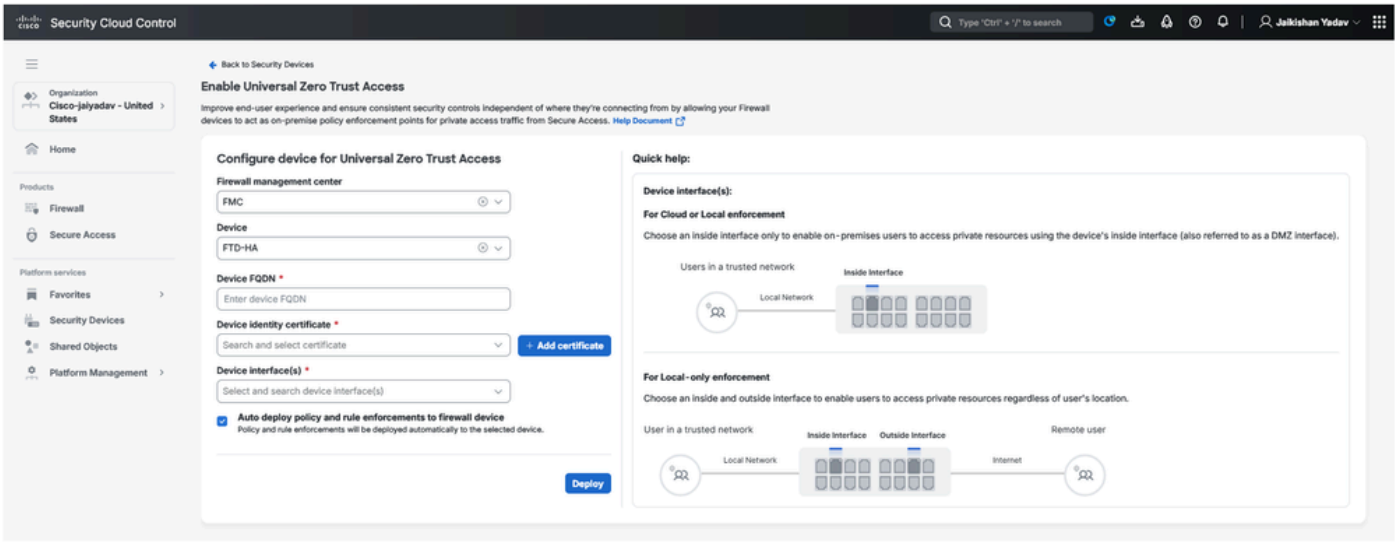
SCCに移動します。

- Platform Services > Security Devices > FTD > Device Management > Universal Zero Trust Network Accessの順にクリックします。

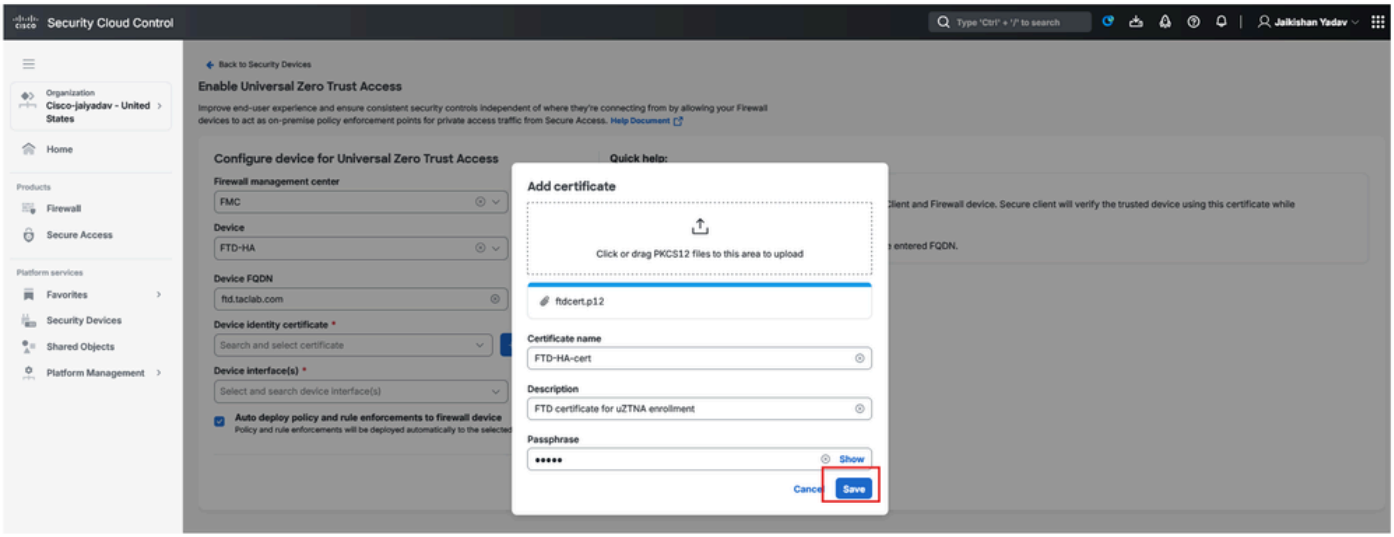


セキュアファイアウォール脅威対策 – ユニバーサルZTNA設定

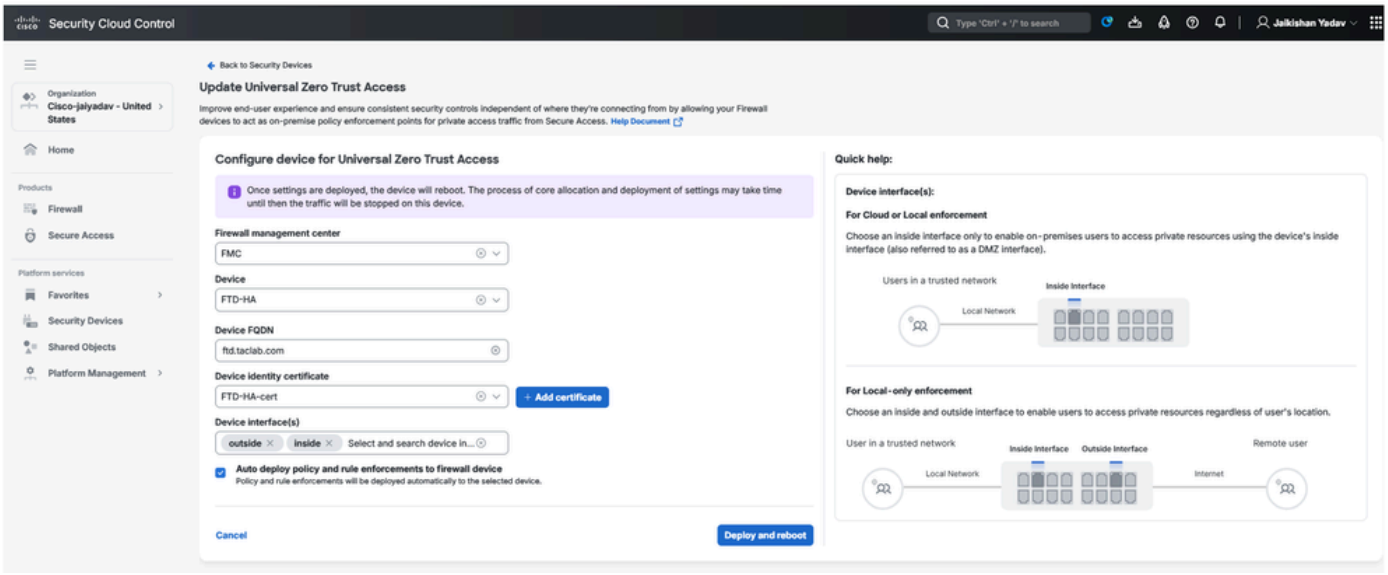
- 情報を入力し、手順「ファイアウォールの脅威に対する防御(FTD)CA署名付き証明書の生成」で生成されたFTD証明書をアップロードします。



セキュアファイアウォール脅威対策 – ユニバーサルZTNA設定



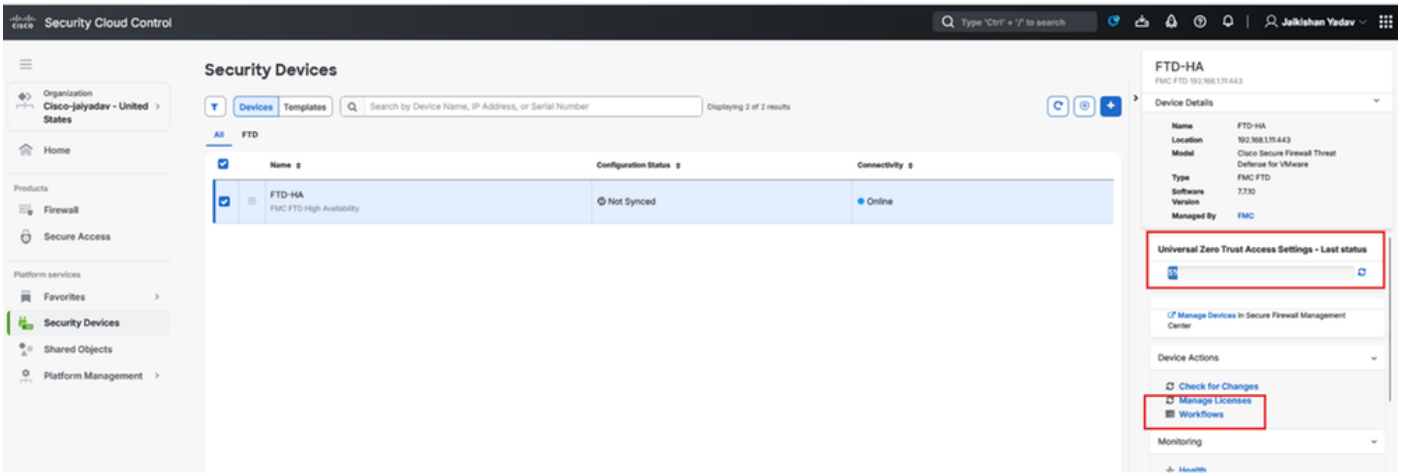
セキュアファイアウォール脅威対策 – ユニバーサルZTNA設定



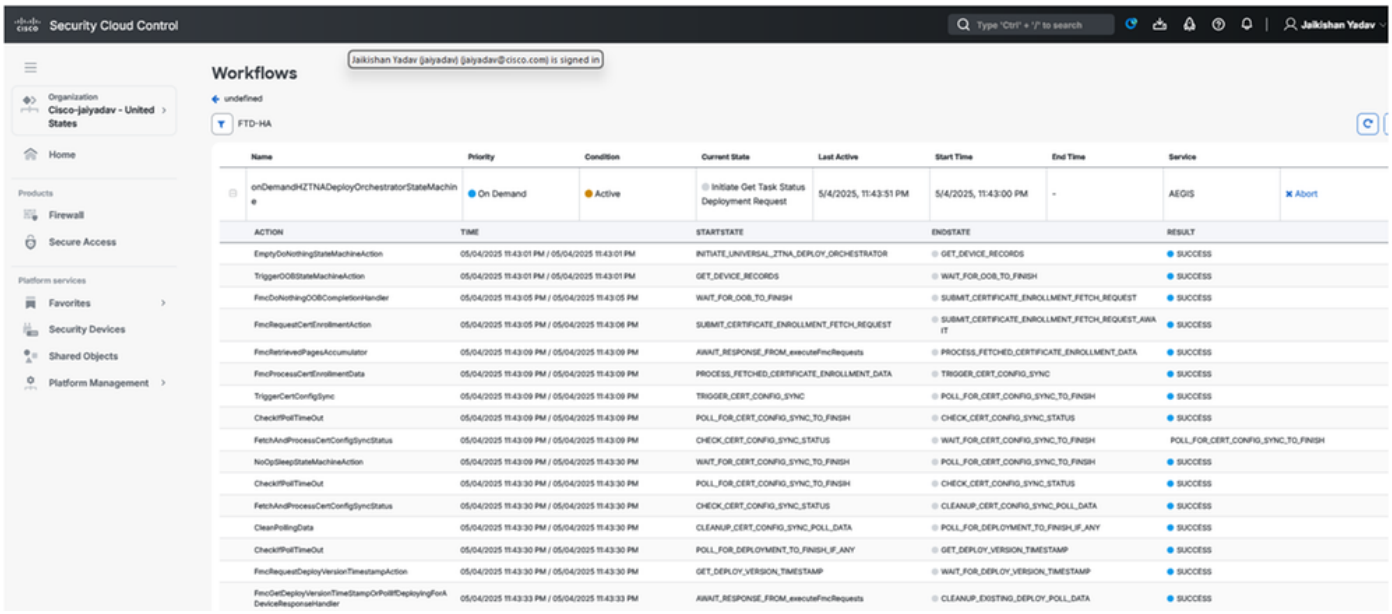
セキュアファイアウォール脅威対策 – ユニバーサルZTNA設定

注:FTD HAでuZTNAを有効にすると、変更が導入され、両方のファイアウォール脅威対策(FTD)ユニットが同時にリブートされます。適切なメンテナンスウィンドウを必ずスケジュールしてください。

- Workflowをクリックして、ログを確認します

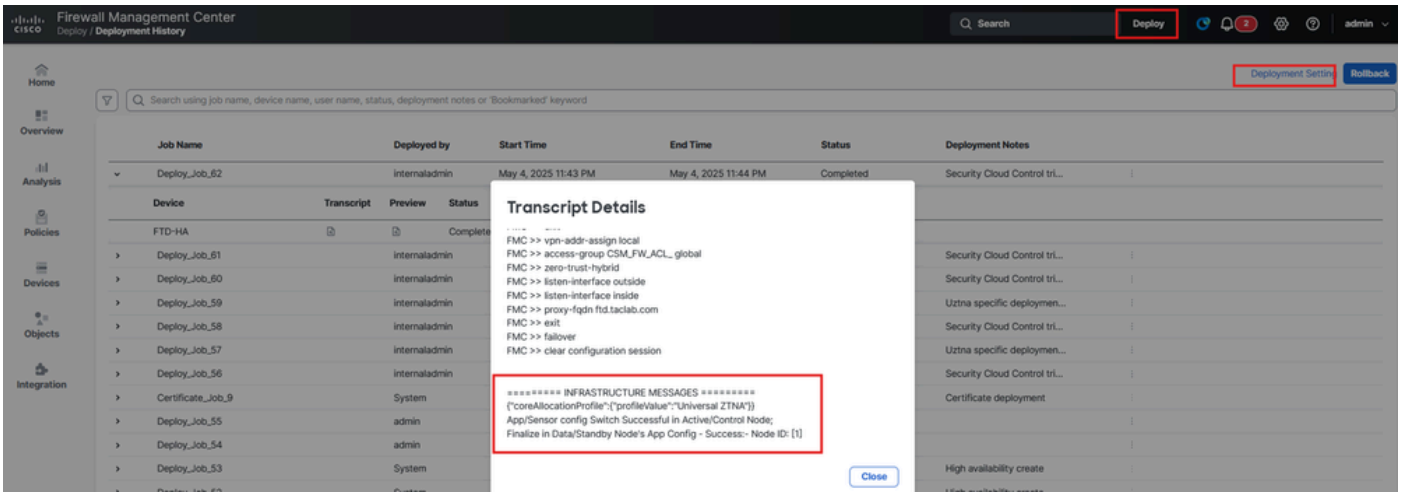


セキュアファイアウォール脅威対策：ユニバーサルZTNA設定ステータス



セキュリティクラウド制御のワークフロー

トランスクリプトの詳細で、ポリシー導入ステータスとFMCでの変更を確認できます。



Secure Firewall Management Center – ポリシー展開の状態

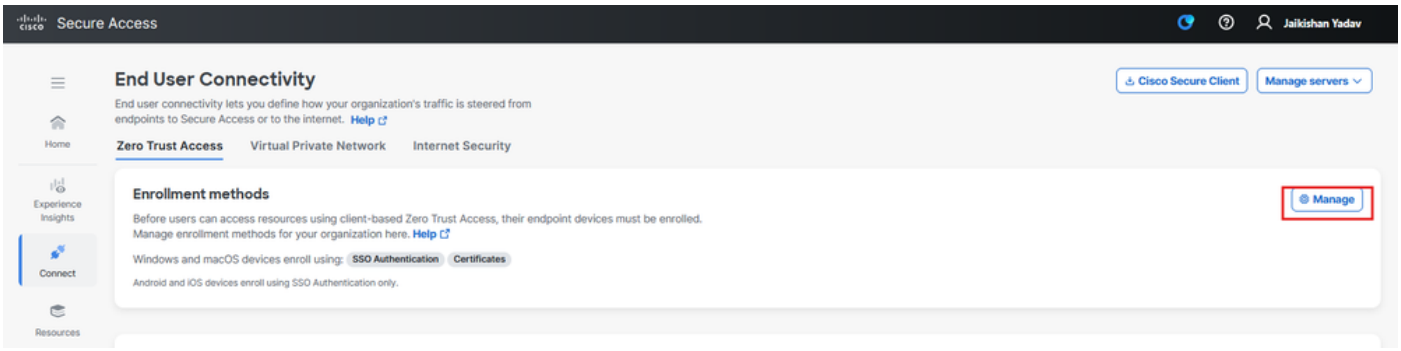
uZTNAへのクライアントの登録

セキュアアクセスの設定

注:SSOまたは証明書ベースのZTA登録を使用できます。次は、証明書ベースのZTA登録の手順です

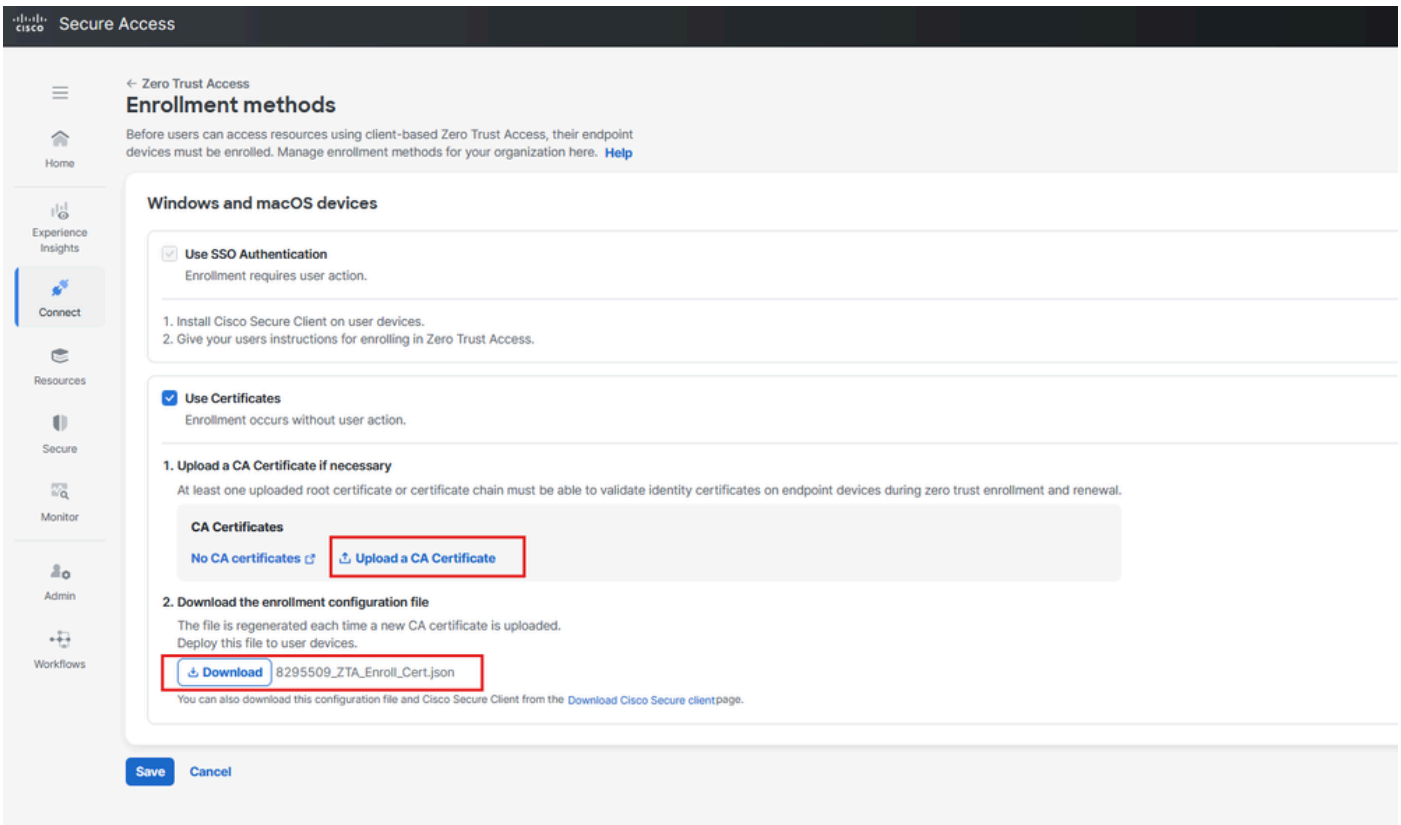
Secure Access Dashboardに移動します。

- **Connect** > **End User Connectivity** > **Zero Trust Access**の順にクリックします
- Manageをクリックします。



セキュアアクセス – ZTA証明書の登録

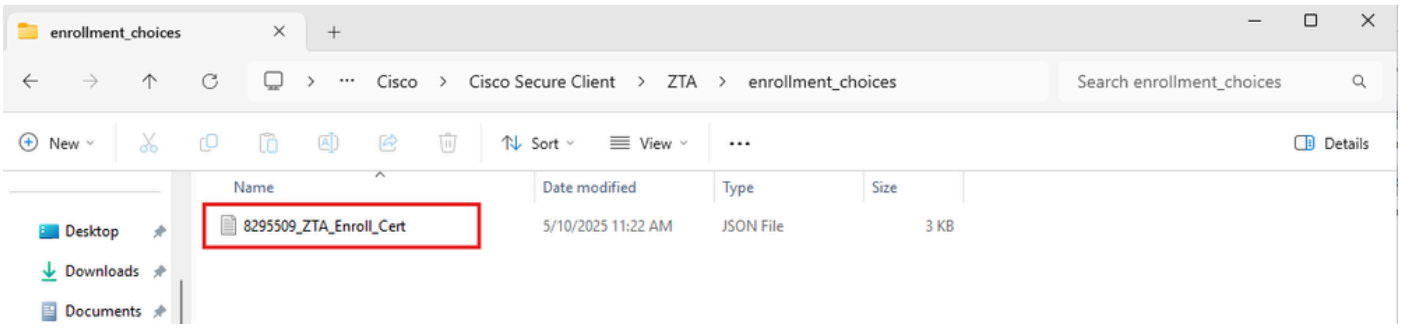
- ルートCA証明書をアップロードし、登録設定ファイルをダウンロードする



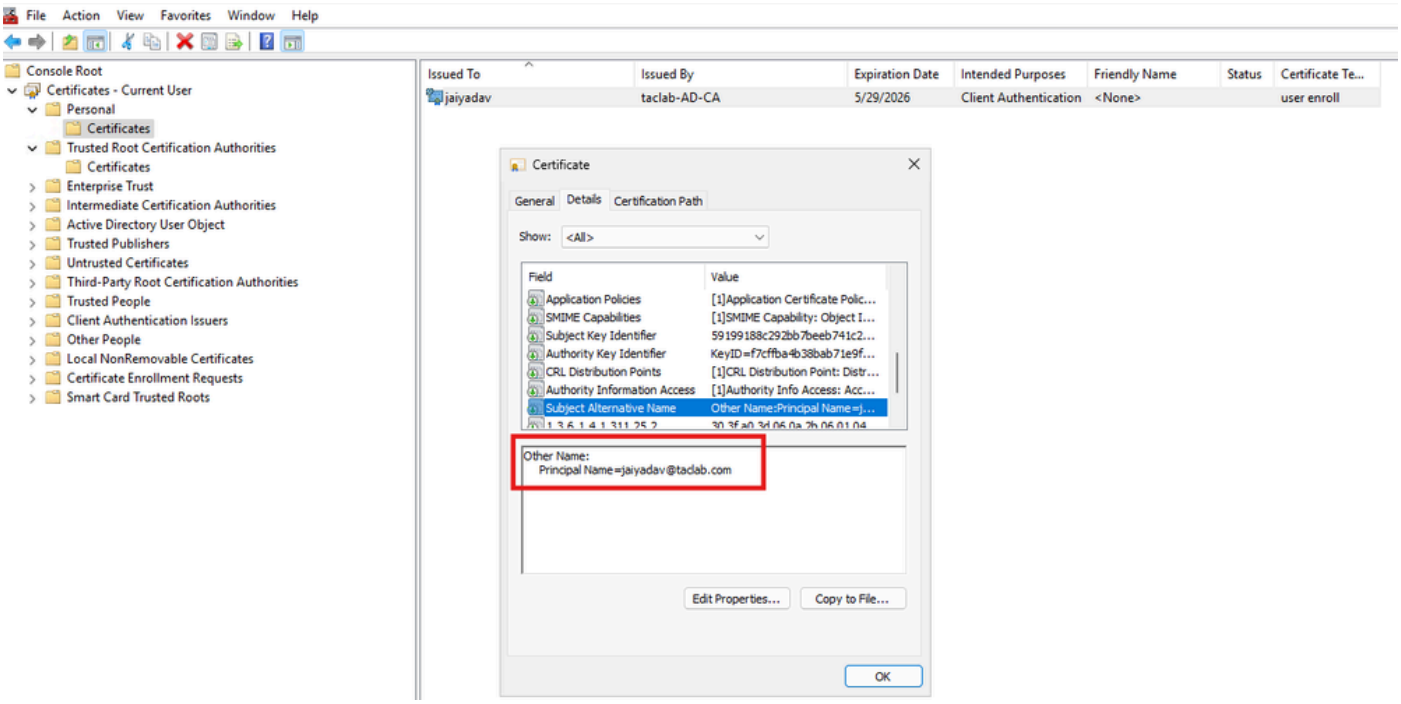
- [Save] をクリックします。

クライアントの設定

登録設定ファイルをC:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollment_choicesにコピーします。

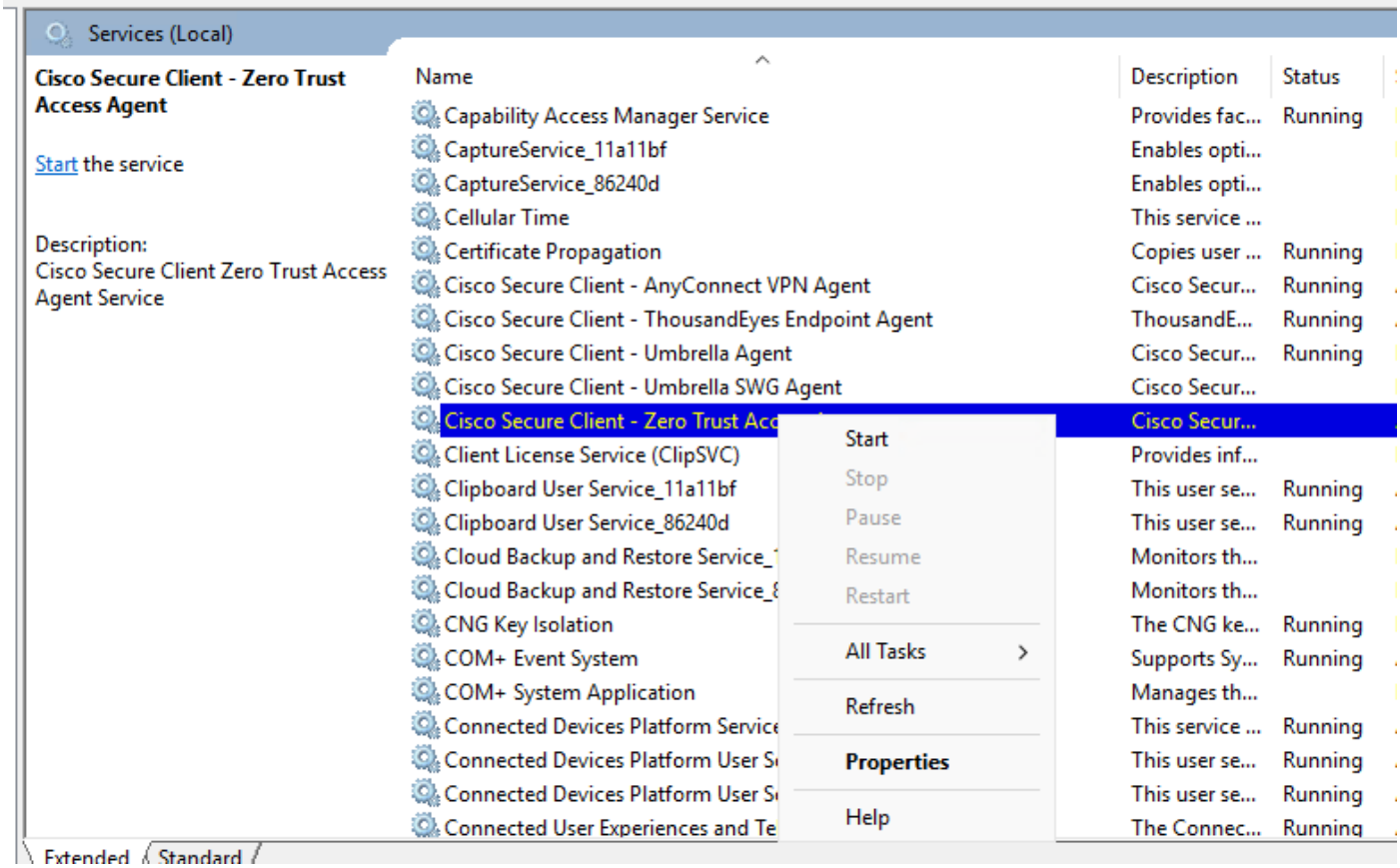


- クライアント証明書を作成します。この証明書にはSAN内のUPNが必要です。



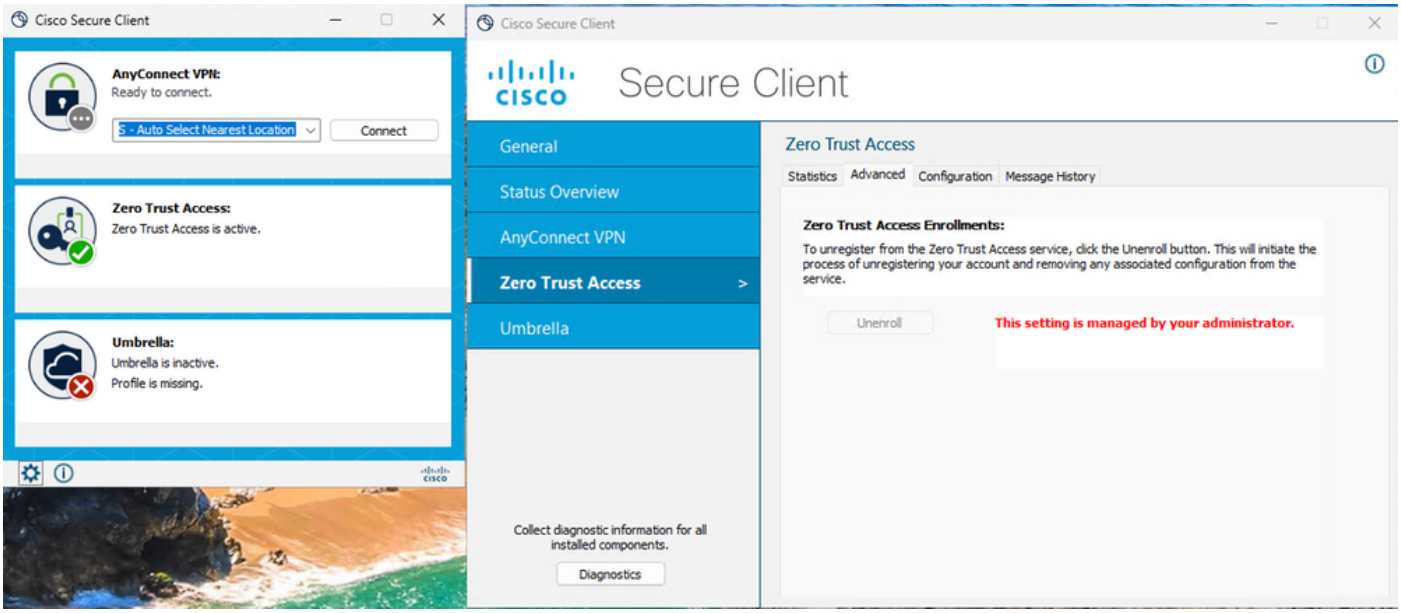
証明書のインストール

- Cisco Secure Client - Zero Trust Access Agentの開始/再起動



Windowsサービス

- ZTAモジュールのステータスを確認します



セキュアアクセス – ZTA証明書登録ステータス

確認

次のコマンドを使用して、ファイアウォール脅威対策(FTD)のuZTNA設定を確認します。

```
show allocate-core profile
show running-config universal-zero-trust
```

関連情報

- シスコのテクニカルサポートとダウンロード
- Cisco Secure Accessヘルプセンター
- Cisco SASE設計ガイド

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。