

# SCC上のオンプレミスマネージド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](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[ネットワーク図](#)

[Background情報](#)

[サポートされるデバイス](#)

[制限事項](#)

[設定](#)

[FMCバージョンの確認](#)

[FTDバージョンの確認](#)

[FTDライセンスの確認](#)

[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](#)

[CDOでのセキュリティクラウド制御テナントの作成](#)

[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](#)

[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](#)

[ファイアウォールの脅威に対する防護\(FTD\)CA署名付き証明書の生成](#)

[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](#)

[FTDのUniversal Zero Trust Network Access\(uZTNA\)設定の登録](#)

[uZTNAへのクライアントの登録](#)

[セキュアアクセスの設定](#)

[クライアントの設定](#)

[確認](#)

[関連情報](#)

---

## 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

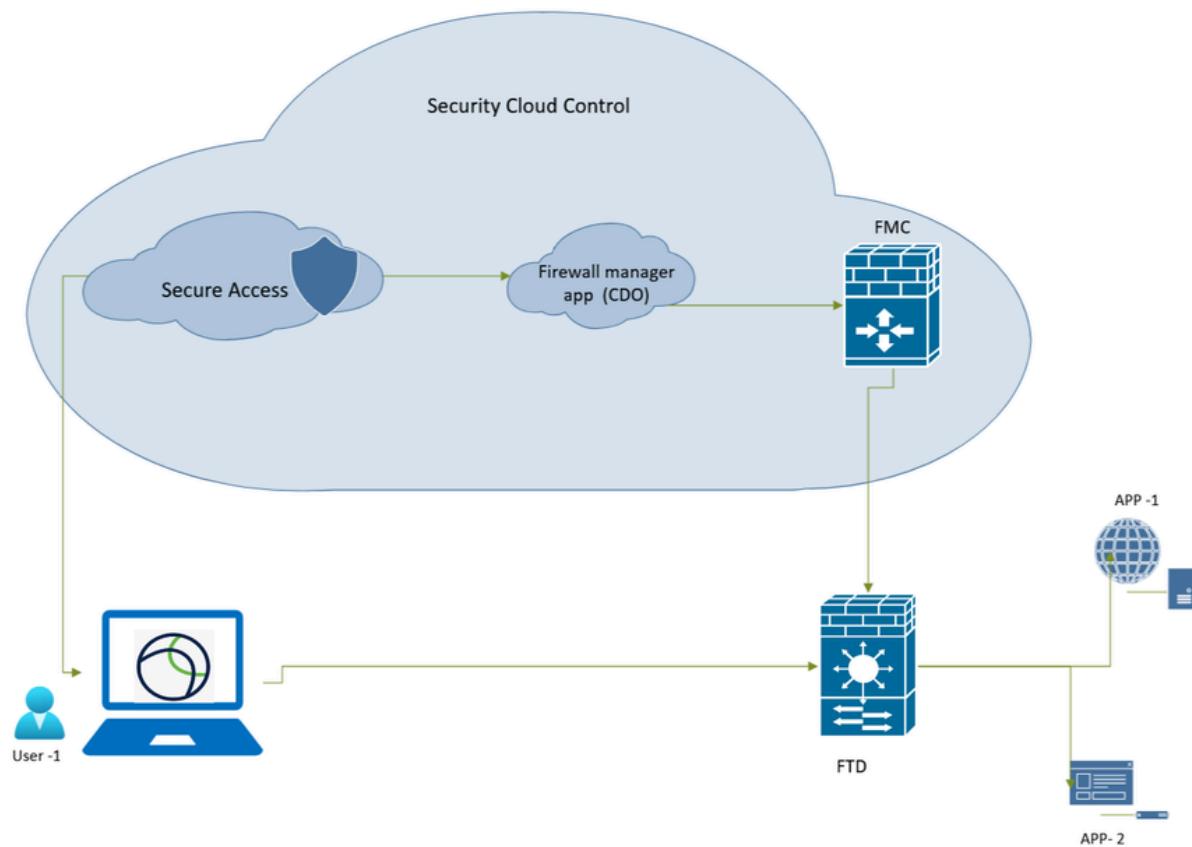
## 使用するコンポーネント

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

## Background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。

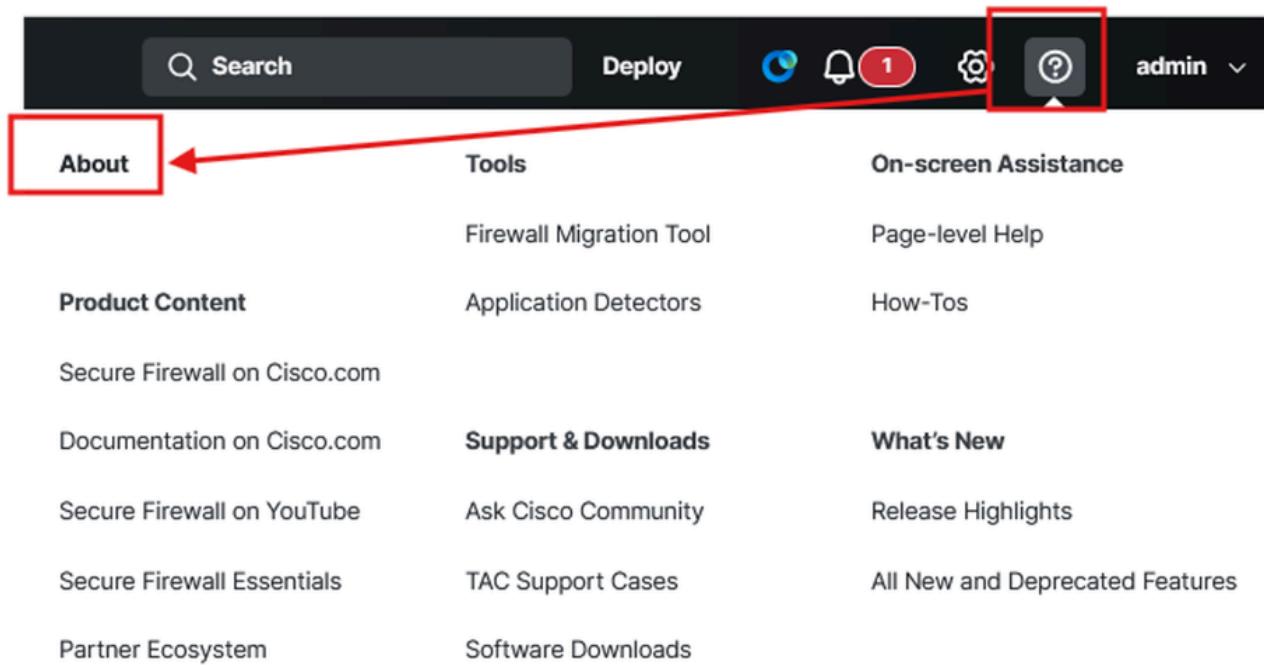
- 4Kおよび9K Firepowerシリーズでコンテナとして導入されるFTDはサポートされません
- ユニバーサルZTNAセッションはジャンボフレームをサポートしない

## 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。





# Firewall Management Center

Version 7.7.10 (build 8)

Model	Cisco Secure Firewall Management Center for VMware
Serial Number	None
Snort Version	2.9.24 (Build 96)
Snort3 Version	3.3.5.1000 (Build 10)
Rule Pack Version	3115
Module Pack Version	3505
LSP Version	Isp-rel-20250430-1826
VDB Version	build 400 (2024-11-26 19:30:49)
Rule Update Version	2025-04-30-001-vrt
Geolocation Version	2025-04-19-097
OS	Cisco Firepower Extensible Operating System (FX-OS) 82.17.30 (build 3)
Hostname	firepower

For technical/system questions, email [tac@cisco.com](mailto:tac@cisco.com) phone: 1-800-553-2447 or  
1-408-526-7209. Copyright 2004-2025, Cisco and/or its affiliates. All rights reserved.

[Copy](#)

[Close](#)

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。

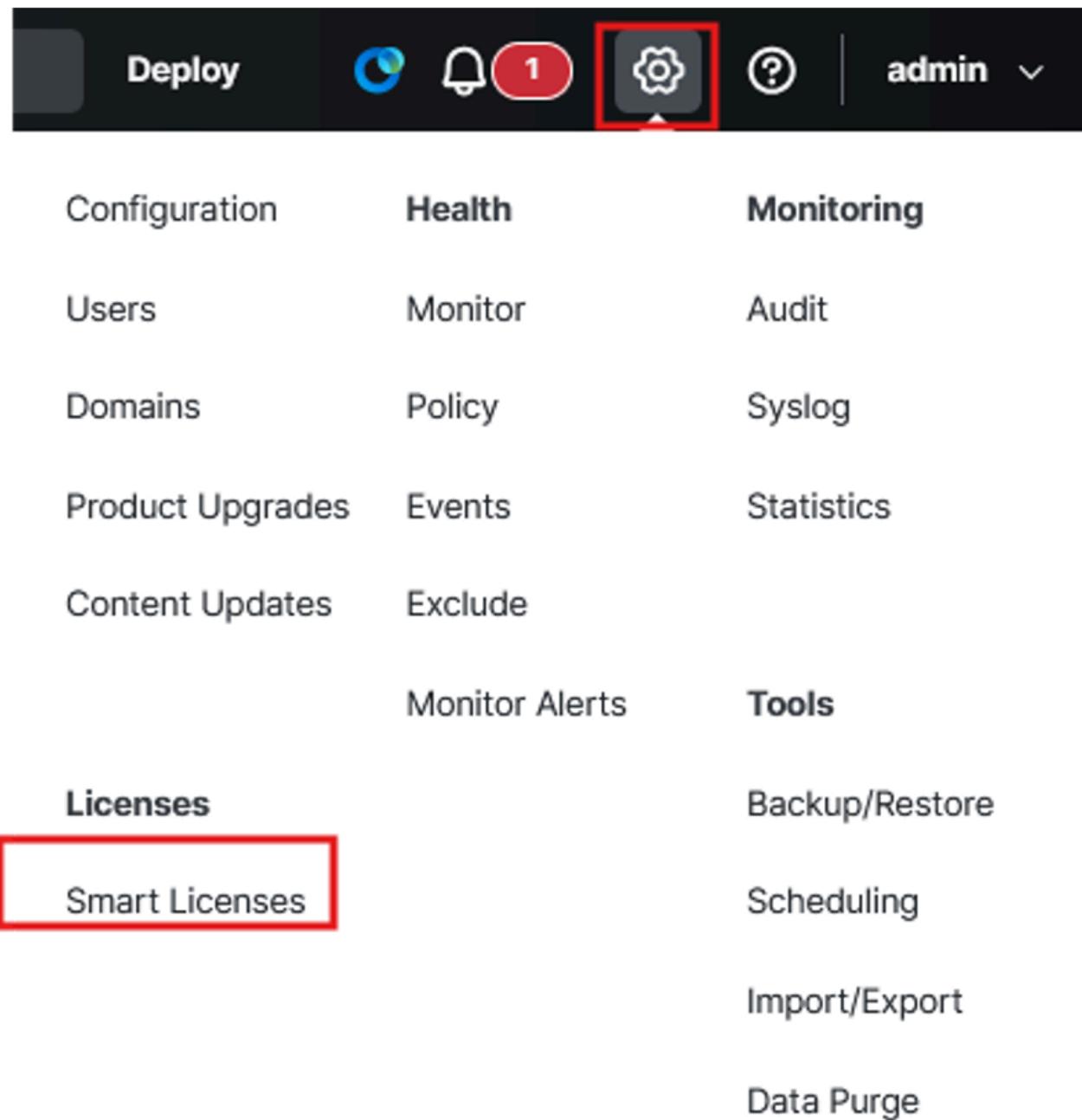
- Devices > Device Managementの順にクリックします。

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
FTD1(Primary, Active) 192.168.1.11 - Routed	Firewall Threat Defense for VMware	7.7.10	N/A	Essentials, IPS (2 more...)	ACP	
FTD2(Secondary, Standby) 192.168.1.13 - Routed	Firewall Threat Defense for VMware	7.7.10	N/A	Essentials, IPS (2 more...)	ACP	

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



The screenshot shows the FTD (Fortinet Threat Defense) interface. At the top, there is a navigation bar with the following items: Deploy, a blue gear icon, a bell icon with a red '1' notification, a gear icon (which is highlighted with a red box), a question mark icon, and the user 'admin'. Below the navigation bar is a main menu with three main categories: Configuration, Health, and Monitoring. Under Configuration, there are links for Users, Domains, Product Upgrades, and Content Updates. Under Health, there are links for Monitor, Policy, Events, and Exclude. Under Monitoring, there are links for Audit, Syslog, Statistics, and Monitor Alerts. Below the main menu, there is a section titled 'Tools' with links for Backup/Restore, Scheduling, Import/Export, and Data Purge. On the left side, there is a sidebar with a 'Licenses' section containing a link for 'Smart Licenses', which is also highlighted with a red box.

Configuration	Health	Monitoring
Users	Monitor	Audit
Domains	Policy	Syslog
Product Upgrades	Events	Statistics
Content Updates	Exclude	
	Monitor Alerts	<b>Tools</b>
<b>Licenses</b>		Backup/Restore
<b>Smart Licenses</b>		Scheduling
		Import/Export
		Data Purge

Smart Licenses		Filter Devices...	Edit Performance Tier	
License Type/Device Name	License Status	Device Type	Domain	Group
> Firewall Management Center Virtual (2)	● In-Compliance			
Essentials (2)	● In-Compliance			
FTD-HA (2) [Performance Tier: FTDv100] Cisco Secure Firewall Threat Defense for VMware Threat Defense High Availability	● In-Compliance	High Availability - Cisco Secure Firewall Threat Defense for VMv Global		N/A
Malware Defense (2)	● Out of Compliance			
FTD-HA (2) [Performance Tier: FTDv100] Cisco Secure Firewall Threat Defense for VMware Threat Defense High Availability	● Out of Compliance	High Availability - Cisco Secure Firewall Threat Defense for VMv Global		N/A
IPS (2)	● Out of Compliance			
FTD-HA (2) [Performance Tier: FTDv100] Cisco Secure Firewall Threat Defense for VMware Threat Defense High Availability	● Out of Compliance	High Availability - Cisco Secure Firewall Threat Defense for VMv Global		N/A
URL (2)	● Out of Compliance			
FTD-HA (2) [Performance Tier: FTDv100] Cisco Secure Firewall Threat Defense for VMware Threat Defense High Availability	● Out of Compliance	High Availability - Cisco Secure Firewall Threat Defense for VMv Global		N/A
Carrier (0)				

## 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）。

```
dns>group Lab-DNS
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



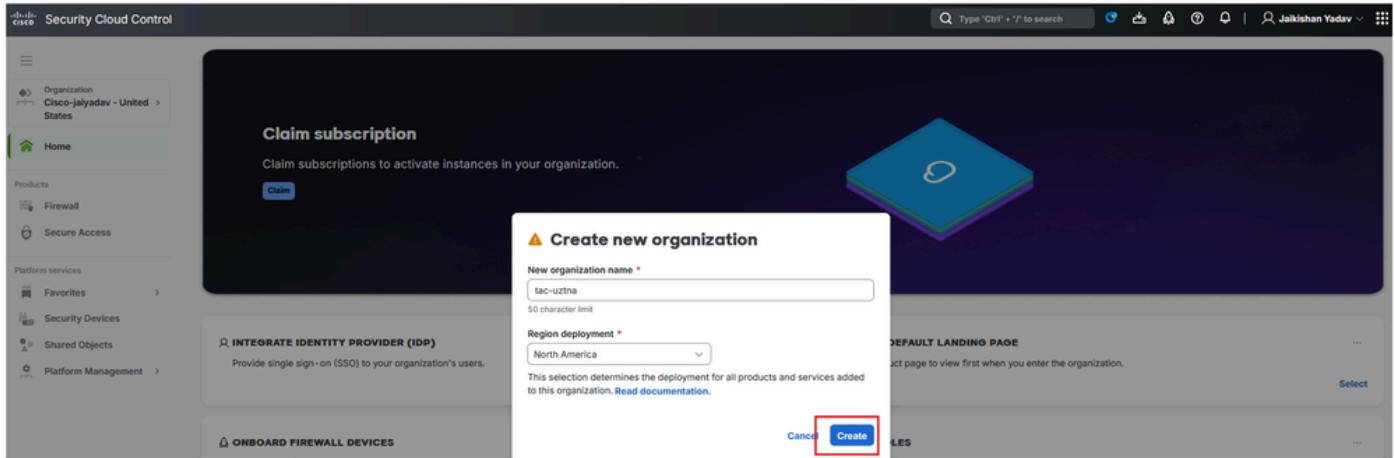
注：すでにSCCテナントが設定されている場合は、新しいテナントを作成する必要はありません。

### 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。

Security Cloud Control

Administration

General Settings

User Management

Notification Settings

Integrations

Secure Connectors

Firewall Management Center

Multicloud Defense Management

Objects

Security Devices

Secure Connections

Administration

Security Cloud Control

Administration

General Settings

User Management

Notification Settings

Integrations

Secure Connectors

Firewall Management Center

Multicloud Defense Management

Objects

Security Devices

Secure Connections

Administration

General Settings

Enable the option to schedule automatic deployments

Web Analytics

Auto onboard On-Prem FMCs from Cisco Security Cloud

Ensure that your On-Prem FMCs are integrated with Cisco Security Cloud. Only the integrated On-Prem FMCs are onboarded. See [Integrate On-Prem FMC to Cisco Security Cloud](#).

Enable event data sharing with Talos

Read more about how Cisco protects your data [here](#).

Tenant ID  
cbc

Secure Services Exchange Tenant ID  
71

Tenant Name  
CI

## 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ます、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
```

```
openssl req -newkey rsa:2048 -nodes -keyout cert.key -out cert.csr
Generating a RSA private key
-----+=====
-----+=====
writing new private key to 'cert.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:NC
Locality Name (eg, city) []:RTP
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco
Organizational Unit Name (eg, section) []:TAC
Common Name (e.g. server FQDN or YOUR name) []:ftd.taclab.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
```

## 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 :

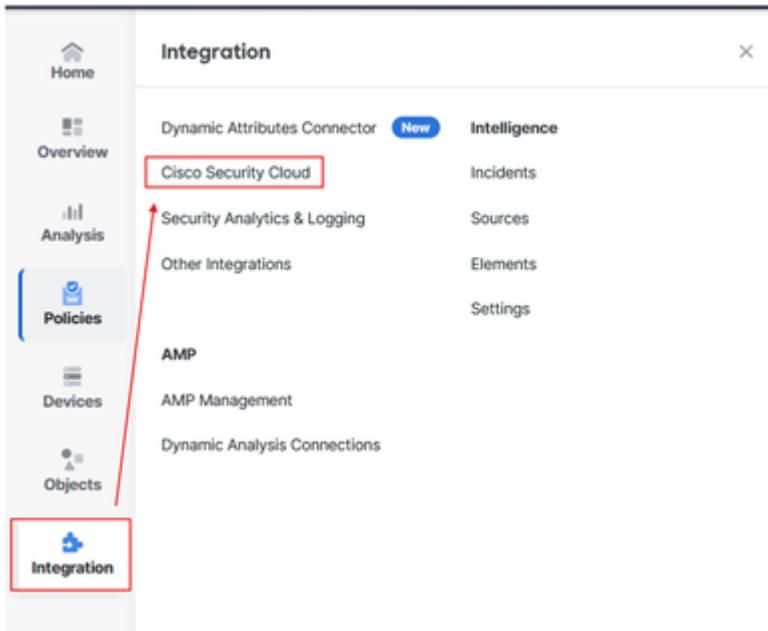
```
openssl pkcs12 -export -out ftdcert.p12 -in cert.crt -inkey cert.key
```

- 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

。



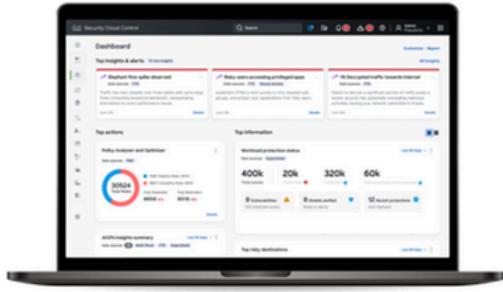
## Welcome to the Cisco Security Cloud

Delivered through Security Cloud Control (SCC)

Staying on top of security is easier than ever. Security Cloud Control helps you consistently manage policies across your Cisco security products. It is a cloud-based application that cuts through complexity to save time and keep your organization protected against the latest threats.

SCC complements FMC by allowing you to:

- Drive consistent policy through shared object management with FMCs
- Enable Zero-Touch Provisioning of FTDs
- View events in the cloud
- Get a centralized view of inventory across FMCs
- Leverage cloud CSDAC and Cloud Delivered FMC
- and more



To continue with cloud registration of your FMC, you will need a Cisco Security Cloud Sign On (SSO) user account.

If you don't already have a Cisco SSO account, please proceed below and Sign Up for free. Note that you will need to restart the cloud registration from your FMC after your new SSO account is created.

If you already have a Cisco SSO account, please proceed below to choose or create a free SCC account to register your FMC.

### Let's get started!

1

Sign Up/Sign In with Cisco SSO

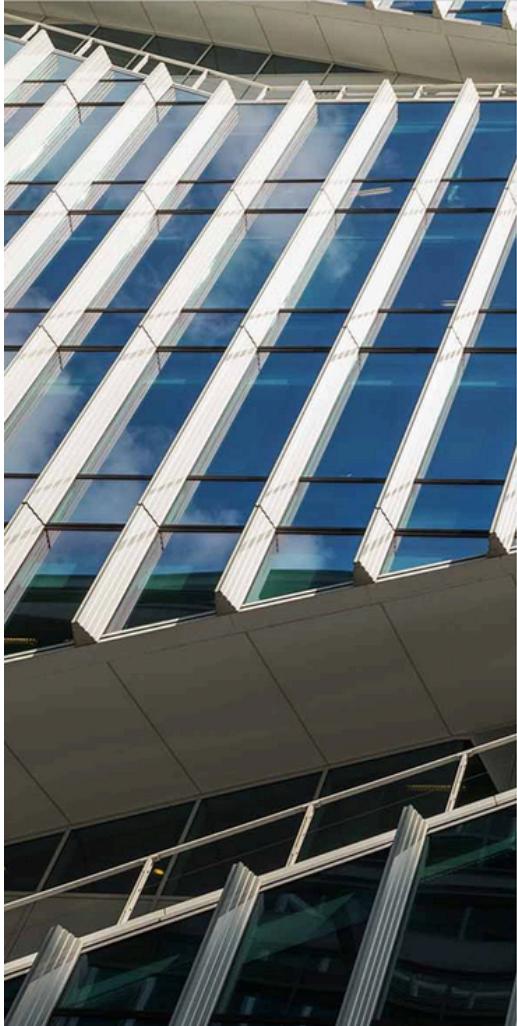
2

Register FMC with a SCC Tenant

[Continue to Cisco SSO](#)

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。



**Welcome to Security Cloud Control**

To proceed with the registration of your FMC, please select a SCC tenant or enterprise to register with the FMC and verify the code displayed below matches the user code from your FMC.

Select Tenant  Create Tenant

Search Tenants

cisco-jaiyadav  

cisco-ngfw-us-sspt

cisco-vibobrov

default\_enterprise

---

**Grant Application Access**

Compare the code below to the authorization code shown in the FMC tab. If the codes match, authorize the FMC to complete the registration. If the codes do not match, cancel registration.

8ABA15B5

FMC would like access to your SCC tenant **cisco-jaiyadav**.

- **Users:** All internal users in FMC will have read-only access to this SCC tenant.
- **Data:** FMC will be able to collect data using SCC APIs.

The FMC will be registered with tenant **cisco-jaiyadav**

**Authorize FMC**  

## 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。

**Firewall Management Center** Integration / Cisco Security Cloud

**Integration**

Cisco Security Cloud:  Enabled | Current Cloud Region: us-east-1 (US Region) | Security Services Exchange Tenant: SEC TAC | Cloud Onboarding Status: Not Available

**Settings**

**Event Configuration**

Send events to the cloud  View your Events in Cisco Security Cloud

Intrusion events

File and malware events

Connection events

Security

All

**Cisco AI Assistant for Security**

Powered by generative AI and natural language processing, Cisco AI Assistant for Security enables you to create access control rules, query documentation and reference materials when required, and streamline your workflow. [Learn more](#)

Enable Cisco AI Assistant for Security

**Policy Analyzer and Optimizer**

Policy Analyzer & Optimizer evaluates access control rules to improve security and performance of the firewall. Recommendations can include removing redundant or unnecessary rules, consolidating similar rules, and reordering rules to reduce the number of rule evaluations required for each packet. [Learn more](#)

Enable Policy Analyzer and Optimizer

**Cisco Security Cloud Support**

Cisco cloud support services provide an enhanced support experience and maximize the value of the Cisco products. The management center establishes and maintains a secure connection to Cisco cloud to participate in additional service offerings from Cisco.

Enable Cisco Success Network

Enable Cisco Support Diagnostics

**Cisco XDR Automation**

Enable Cisco XDR Automation to allow a Cisco XDR user to build automated workflows that interact with various resources in the Secure Firewall Management Center. [Learn more](#)

Enable Cisco XDR Automation

**Zero-Touch Provisioning (ZTP)**

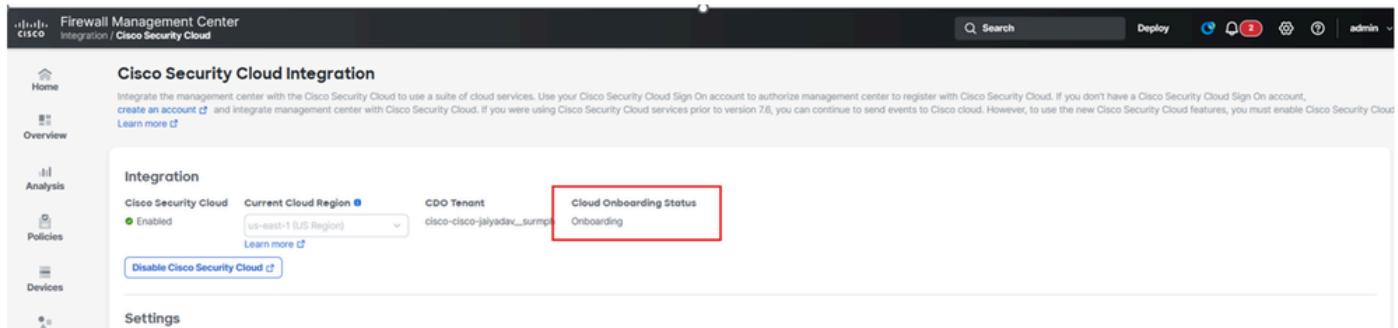
With ZTP, you can register your devices in management center by serial number, without performing any initial setup in the device. Management center integrates with Defense Orchestrator (DCO) for this functionality. You can either add a single device using a serial number and an access control policy, or add multiple devices simultaneously using serial numbers and a device template with preconfigured settings. [Learn more](#)

Enable Zero-Touch Provisioning

**Save**

## 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”に変わら必要があります。



Firewall Management Center - Integration / Cisco Security Cloud

### Cisco Security Cloud Integration

Integrate the management center with the Cisco Security Cloud to use a suite of cloud services. Use your Cisco Security Cloud Sign On account to authorize management center to register with Cisco Security Cloud. If you don't have a Cisco Security Cloud Sign On account, create an account and integrate management center with Cisco Security Cloud. If you were using Cisco Security Cloud services prior to version 7.6, you can continue to send events to Cisco cloud. However, to use the new Cisco Security Cloud features, you must enable Cisco Security Cloud.

Learn more [Cloud Onboarding Status](#)

**Integration**

Cisco Security Cloud: Enabled

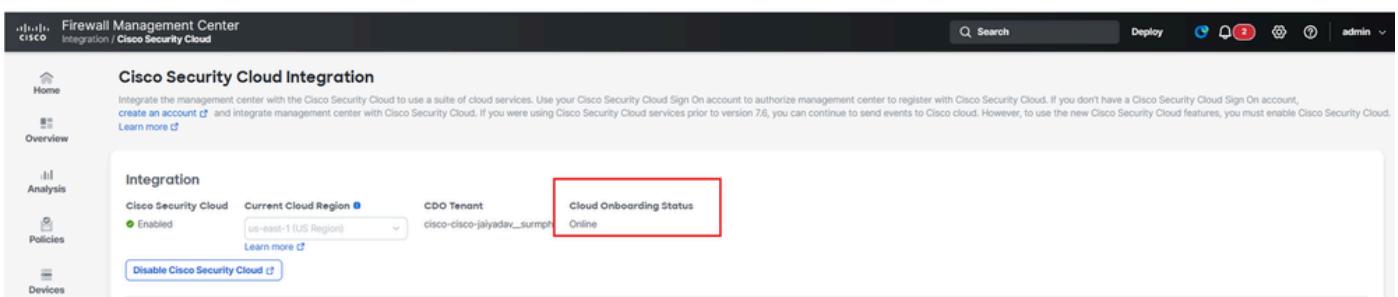
Current Cloud Region: us-east-1 (US Region)

CDO Tenant: cisco-cisco-jalyadav...surmpt

Cloud Onboarding Status: Onboarding

[Learn more](#) [Disable Cisco Security Cloud](#)

**Settings**



Firewall Management Center - Integration / Cisco Security Cloud

### Cisco Security Cloud Integration

Integrate the management center with the Cisco Security Cloud to use a suite of cloud services. Use your Cisco Security Cloud Sign On account to authorize management center to register with Cisco Security Cloud. If you don't have a Cisco Security Cloud Sign On account, create an account and integrate management center with Cisco Security Cloud. If you were using Cisco Security Cloud services prior to version 7.6, you can continue to send events to Cisco cloud. However, to use the new Cisco Security Cloud features, you must enable Cisco Security Cloud.

Learn more [Cloud Onboarding Status](#)

**Integration**

Cisco Security Cloud: Enabled

Current Cloud Region: us-east-1 (US Region)

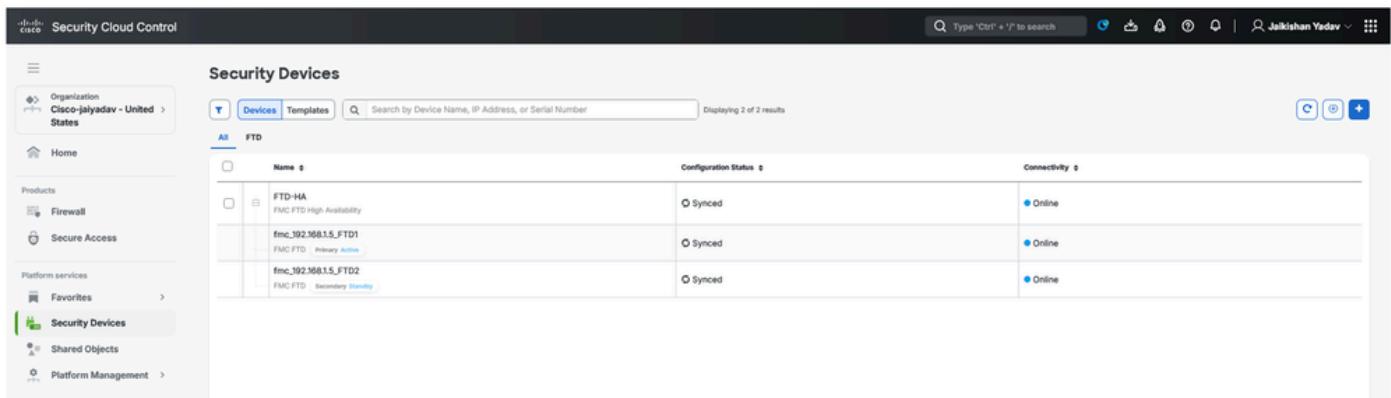
CDO Tenant: cisco-cisco-jalyadav...surmpt

Cloud Onboarding Status: Online

[Learn more](#) [Disable Cisco Security Cloud](#)

## 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



Security Cloud Control

### Security Devices

Organization: Cisco-jalyadav - United States

Products: Firewall, Secure Access

Platform services: Favorites, Security Devices, Shared Objects, Platform Management

Devices: Templates

Search: Search by Device Name, IP Address, or Serial Number

Displaying 2 of 2 results

Name	Configuration Status	Connectivity
FTD-HA FMC FTD: High Availability	Synced	Online
fmc_192.168.1.5_FT01 FMC FTD: Primary Active	Synced	Online
fmc_192.168.1.5_FT02 FMC FTD: Secondary Standby	Synced	Online

## 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。

Security Cloud Control

Organization: Cisco-Jalayadav - United States

Home

Products: Firewall, Secure Access, Platform services (1), Favorites (2), Security Devices (3)

Security Devices

Search: Search by Device Name, IP Address, or Serial Number

Displaying 2 of 2 results

Name	Configuration Status	Connectivity
FTD-HA (FMC FTD High Availability)	Synced	Online
fmc_192.168.1.5_FTD1 (FMC FTD Primary Active)	Synced	Online
fmc_192.168.1.5_FTD2 (FMC FTD Secondary Standby)	Synced	Online

FTD-HA (FMC FTD 192.168.1.5:443)

Device Details

- Name: FTD-HA
- Location: 192.168.1.5:443
- Model: Cisco Secure Firewall Threat Defense for VMware
- Type: FMC FTD
- Software Version: 7.7.10
- Managed By: fmc\_192.168.1.5

Health

Device Management (4)

- Device Overview
- Routing
- Interfaces
- Inline Sets
- DHCP
- VTEP
- High Availability
- Cluster
- Universal zero trust access settings** (5)

Policies

- Access Control
- Intrusion
- Malware & File
- DNS
- Identity
- Decryption
- Prefilter
- NAT
- RA VPN

## 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。

Security Cloud Control

Organization: Cisco-Jalayadav - United States

Home

Products: Firewall, Secure Access

Platform services: Favorites, Security Devices, Shared Objects, Platform Management

Enable Universal Zero Trust Access

Configure device for Universal Zero Trust Access

Firewall management center: FMC

Device: FTD-HA

Device FQDN: Enter device FQDN

Device identity certificate: Search and select certificate, Add certificate

Device Interface(s): Select and search device Interface(s)

Auto deploy policy and rule enforcements to firewall device

Deploy

Quick help:

Device interface(s): For Cloud or Local enforcement

Choose an inside interface only to enable on-premises users to access private resources using the device's inside interface (also referred to as a DMZ interface).

Users in a trusted network → Inside Interface

For Local-only enforcement

Choose an inside and outside interface to enable users to access private resources regardless of user's location.

User in a trusted network → Inside Interface → Outside Interface → Internet → Remote user

## 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ript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

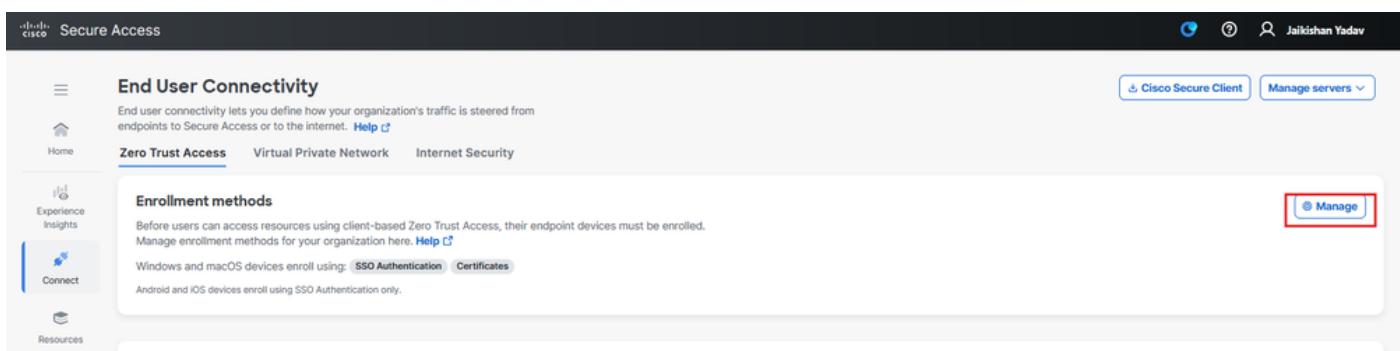
## セキュアアクセスの設定



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。

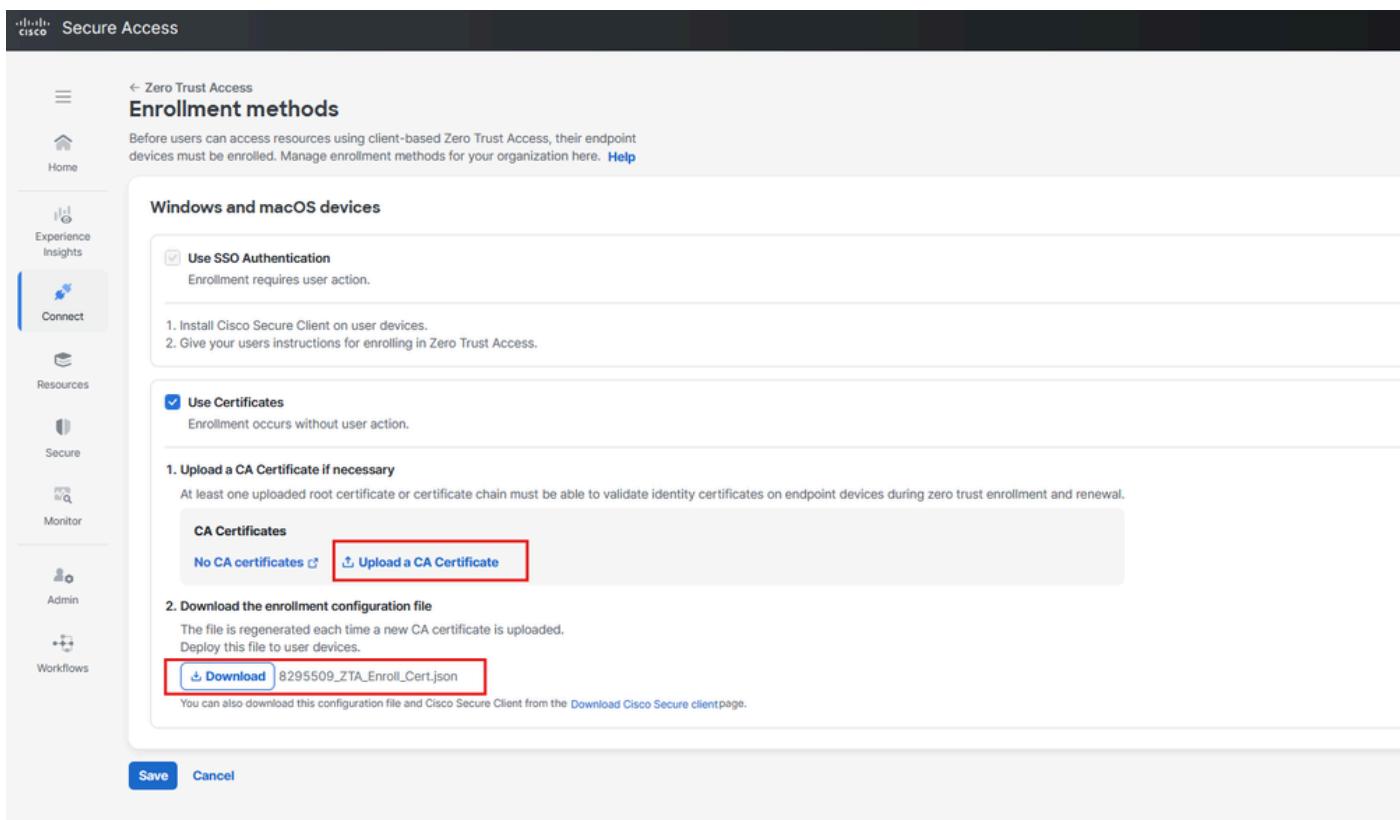
- Connect > End User Connectivity > Zero Trust Accessの順にクリックします
- Manageをクリックします。



The screenshot shows the Cisco Secure Access dashboard with the 'Zero Trust Access' tab selected. In the 'Enrollment methods' section, there is a 'Manage' button which is highlighted with a red box.

## 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



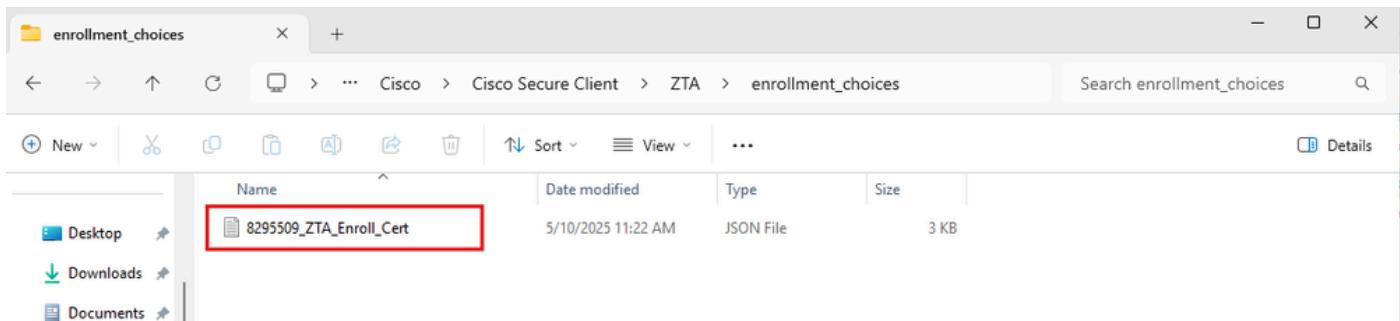
The screenshot shows the 'Enrollment methods' configuration page for Windows and macOS devices. It includes sections for 'Use SSO Authentication' and 'Use Certificates'. Under 'Use Certificates', there is a 'CA Certificates' section with a 'Upload a CA Certificate' button highlighted with a red box. Below this, there is a 'Download' button for the enrollment configuration file, also highlighted with a red box.

## セキュアアクセス - ZTA証明書の登録

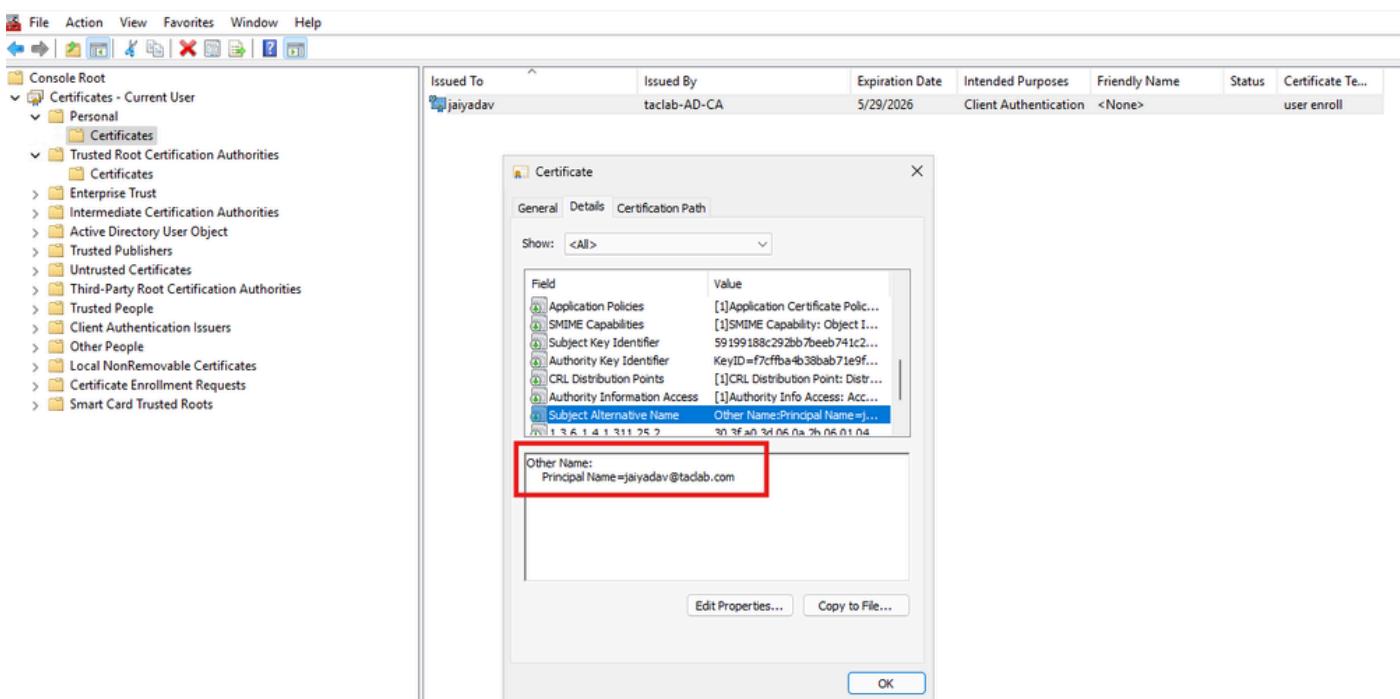
- [Save] をクリックします。

## 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

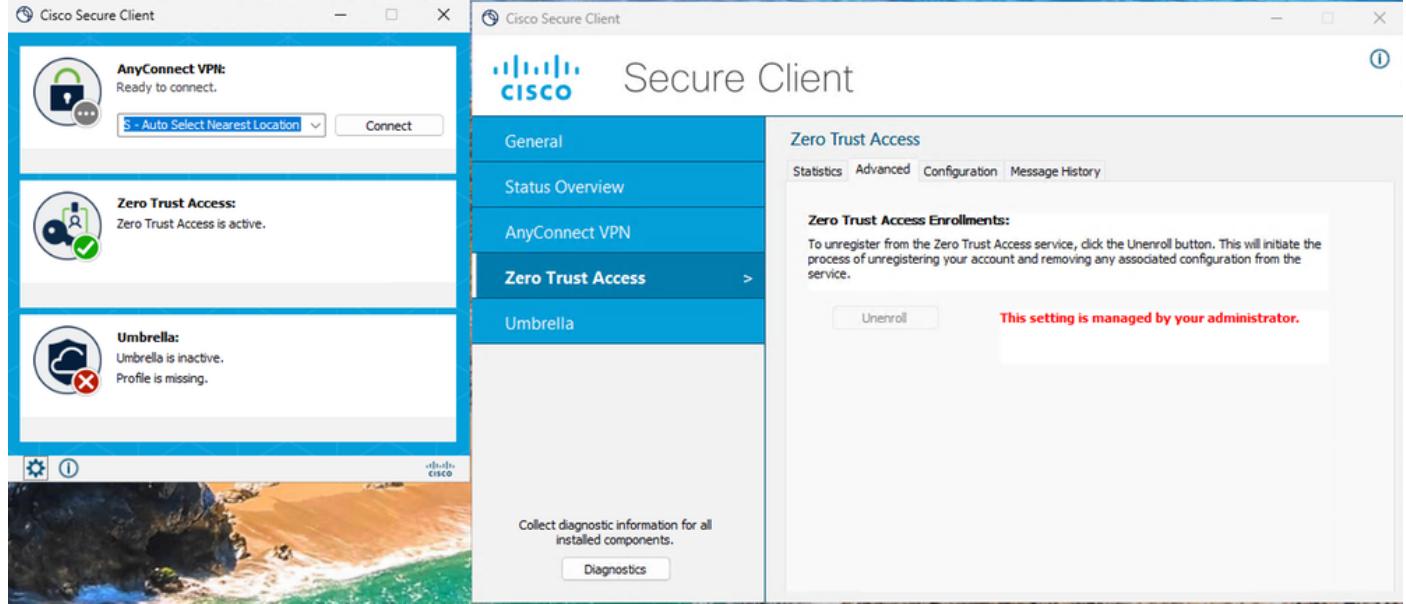
- Cisco Secure Client - Zero Trust Access Agentの開始/再起動

Services (Local)		
Name	Description	Status
<b>Cisco Secure Client - Zero Trust Access Agent</b>	Provides fac...	Running
<a href="#">Start the service</a>	Enables opti...	
<b>Description:</b> Cisco Secure Client Zero Trust Access Agent Service	Enables opti...	
<b>Cisco Secure Client - Zero Trust Access Agent</b>	This service ...	
<a href="#">Start</a>	Copies user ...	Running
<a href="#">Stop</a>	Cisco Secur...	Running
<a href="#">Pause</a>	ThousandE...	Running
<a href="#">Resume</a>	Cisco Secur...	Running
<a href="#">Restart</a>	Cisco Secur...	Running
<a href="#">All Tasks</a>	Cisco Secur...	
<a href="#">Refresh</a>	Provides inf...	
<a href="#">Properties</a>	This user se...	Running
<a href="#">Help</a>	Monitors th...	
	Monitors th...	
	The CNG ke...	Running
	Supports Sy...	Running
	Manages th...	
	This service ...	Running
	This user se...	Running
	This user se...	Running
	The Connec...	Running

Extended / Standard /

## 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。