

Configuration de l'accès sécurisé pour Universal ZTNA avec FMC géré sur site sur SCC

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Diagramme du réseau](#)

[Informations générales](#)

[Périphériques pris en charge](#)

[Limites](#)

[Configurer](#)

[Vérifier la version FMC](#)

[Vérifier la version FTD](#)

[Vérifier les licences FTD](#)

[Vérifier les paramètres de la plate-forme et le DNS correctement configuré](#)

[Créer un locataire de contrôle cloud de sécurité sur CDO](#)

[Vérifiez que les paramètres généraux du pare-feu SCC sont configurés](#)

[Vérifier l'intégration de la base de gestion du pare-feu Secure Access Tenant and Security Control](#)

[Générer un certificat signé par l'autorité de certification Firewall Threat Defense \(FTD\)](#)

[Centre de gestion des pare-feu sur site pour le contrôle du cloud de sécurité](#)

[Inscription des paramètres d'accès réseau sans confiance universel \(uZTNA\) sur FTD](#)

[Inscrire le client avec ZuTNA](#)

[Configuration d'accès sécurisé](#)

[Configuration du client](#)

[Vérifier](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer Universal ZTNA avec Secure Access et FTD virtuel géré par un FMC virtuel On-Prem.

Conditions préalables

- Firewall Management Center (FMC) et Firewall Threat Defense (FTD) doivent être déployés à l'aide de la version 7.7.10 ou ultérieure du logiciel.
- La défense contre les menaces de pare-feu (FTD) doit être gérée par le centre de gestion des pare-feu (FMC)

- La licence FTD (Firewall Threat Defense) doit être fournie avec crypto (le cryptage fort doit être activé avec la fonction d'exportation activée), les licences IPS et Threat requises pour les contrôles de sécurité
- La configuration de base sur Firewall Threat Defense (FTD) doit être effectuée à partir du centre de gestion des pare-feu (FMC), par exemple l'interface, le routage, etc.
- La configuration DNS doit être appliquée sur le périphérique à partir des FMC pour résoudre le FQDN de l'application
- La version de Cisco Secure Client doit être 5.1.10 ou supérieure
- Le contrôle du cloud de sécurité est mis à la disposition des clients avec les options Firewall et Secure Access Micro Apps et UZTNA

Exigences

- Tous les périphériques Secure Firewall Management Center (FMC), y compris cdFMC et Firewall Threat Defense (FTD), doivent exécuter la version 7.7.10 ou ultérieure du logiciel.
- Firewall Threat Defense (FTD) doit être géré par Firewall Management Center ; Gestionnaire local Firewall Defense Manager (FDM) non pris en charge
- Tous les périphériques Firewall Threat Defense (FTD) doivent être configurés pour le mode routé ; le mode transparent n'est pas pris en charge.
- Les périphériques en cluster ne sont pas pris en charge.
- Les périphériques haute disponibilité (HA) sont pris en charge ; ils s'affichent comme une seule entité.
- Client sécurisé version 5.1.10 ou ultérieure

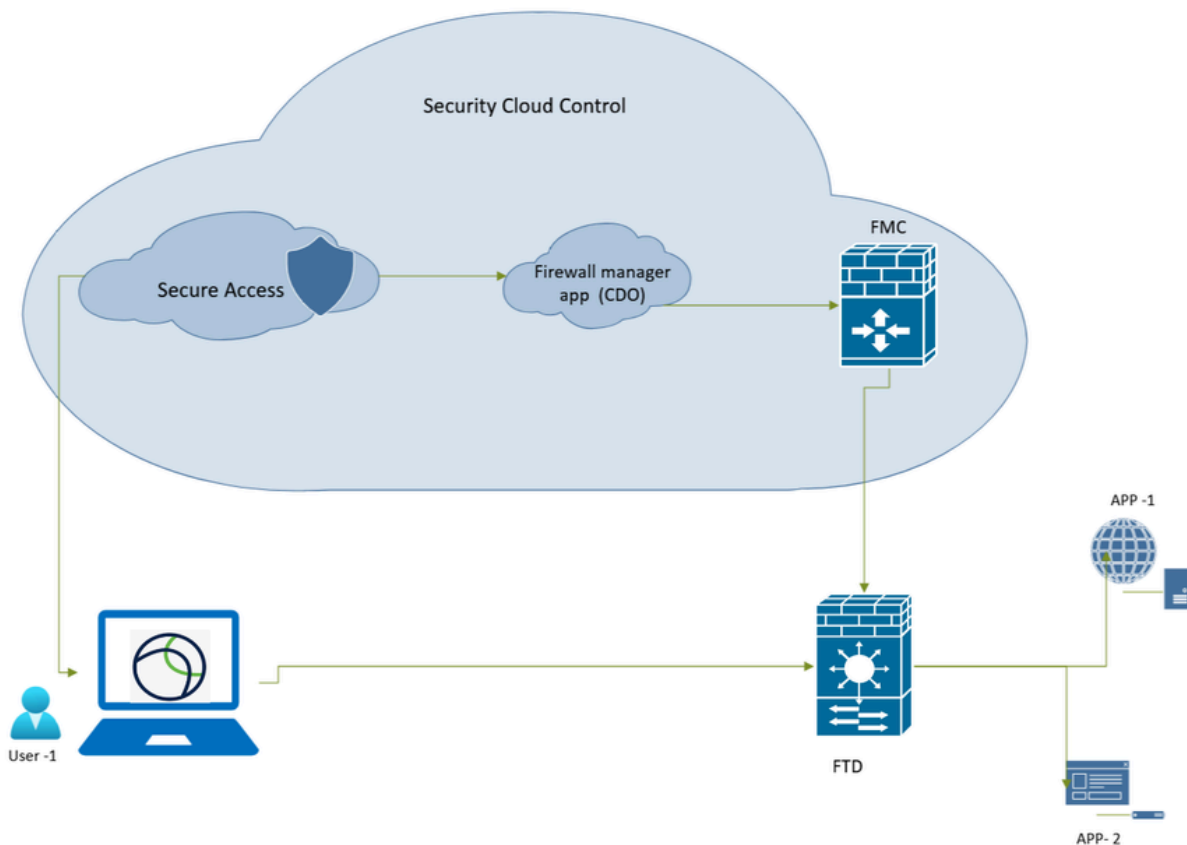
Composants utilisés

Les informations contenues dans ce document sont basées sur

- Contrôle du cloud de sécurité (SCC)
- Secure Firewall Management Center (FMC) version 7.7.10
- Secure Firewall Threat Defense (FTD) virtuel -100 version 7.7.10
- Client sécurisé pour Windows version 5.1.10
- Accès sécurisé

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Diagramme du réseau



Accès sécurisé - Topologie du réseau

Informations générales

Périphériques pris en charge

Modèles de défense contre les menaces par pare-feu :

- FPR 1150
- FPR 3105, 3110,3120,3130,3140
- FPR4115,4125,4145,4112
- FPR4215,4225,4245
- Protection contre les menaces de pare-feu (FTD) virtuelle avec un minimum de 16 coeurs de processeur

Limites

- Partage d'objets
- IPv6 n'est pas pris en charge.
- Seul le VRF global est pris en charge.
- Les politiques ZTNA universelles ne sont pas appliquées au trafic de tunnel de site à site vers un périphérique .

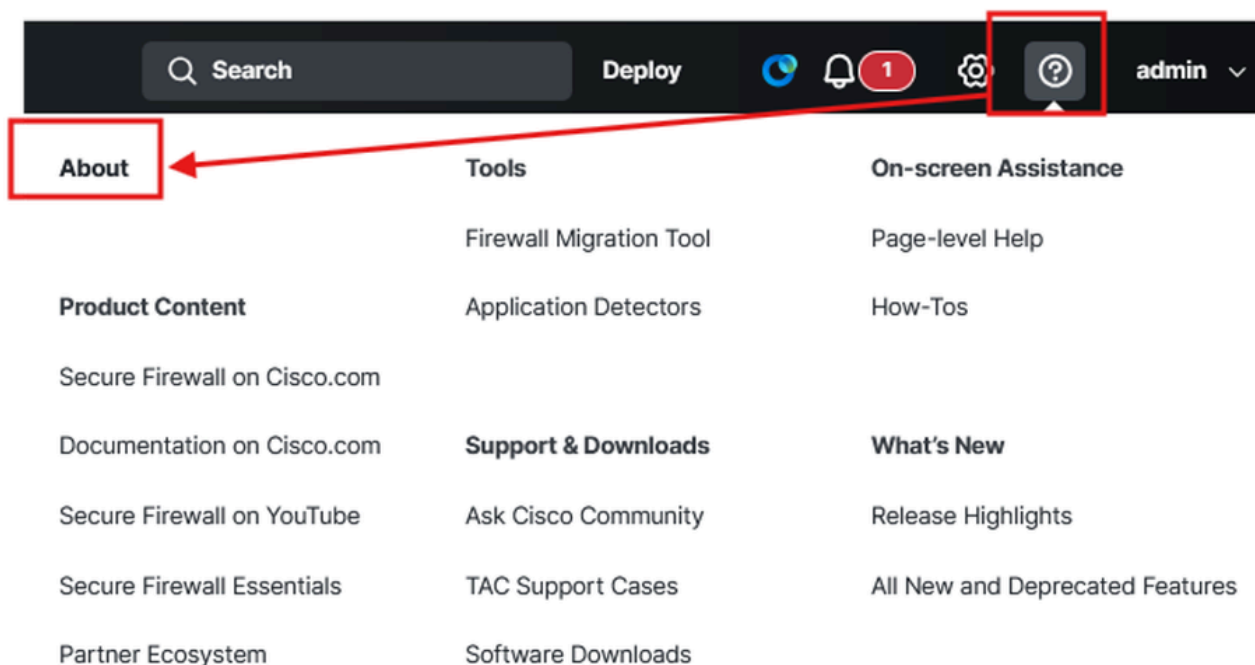
- Les périphériques en cluster ne sont pas pris en charge.
- Les FTD déployés en tant que conteneurs sur les gammes Firepower 4K et 9K ne sont pas pris en charge
- Les sessions ZTNA universelles ne prennent pas en charge les trames jumbo

Configurer

Vérifier la version FMC

Vérifiez que Firewall Management Center et Firewall FTD s'exécutent sur la version logicielle prise en charge pour le ZTNA universel (version 7.7.10 ou ultérieure) :

- Cliquez sur ? (coin supérieur droit) et cliquez sur [About](#)



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	lsp-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 phone: 1-800-553-2447 or 1-408-526-7209. Copyright 2004-2025, Cisco and/or its affiliates. All rights reserved.

Copy

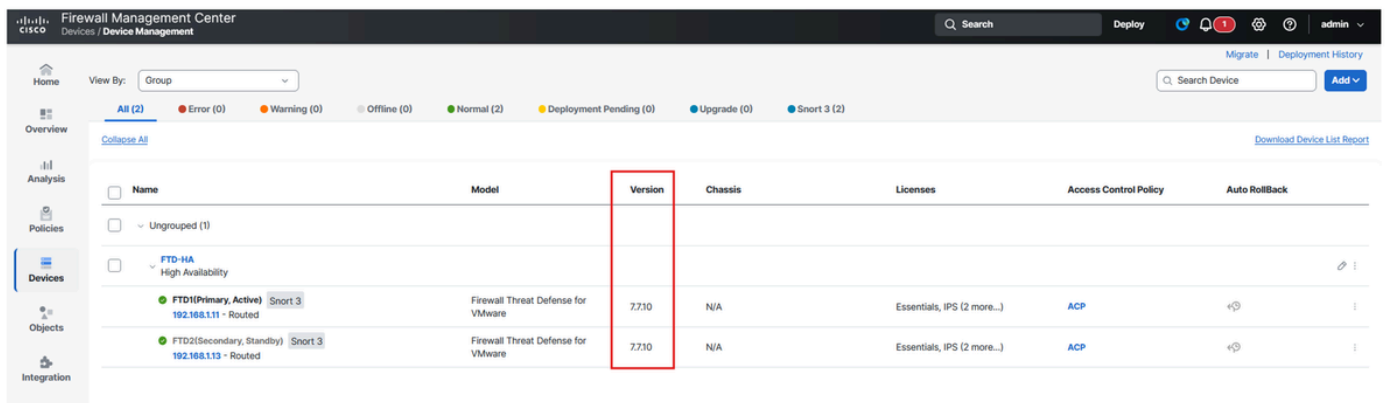
Close

Secure Firewall Management Center - Version du logiciel

Vérifier la version FTD

Accédez à l'interface utilisateur FMC :

- Cliquez sur **Devices** > Device Management



Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
Ungrouped (1)						
FTD-HA High Availability						
FTD1(Primary, Active) 192.168.1.11 - Routed Snort 3	Firewall Threat Defense for VMware	7.7.10	N/A	Essentials, IPS (2 more...)	ACP	+
FTD2(Secondary, Standby) 192.168.1.13 - Routed Snort 3	Firewall Threat Defense for VMware	7.7.10	N/A	Essentials, IPS (2 more...)	ACP	+

Protection pare-feu sécurisée contre les menaces - Version logicielle

Vérifier les licences FTD

- Cliquez sur Setting Icon > Licenses> Smart Licenses



Configuration

Users

Domains

Product Upgrades

Content Updates

Licenses

Smart Licenses

Health

Monitor

Policy

Events

Exclude

Monitor Alerts

Monitoring

Audit

Syslog

Statistics

Tools

Backup/Restore

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)						

Protection pare-feu sécurisée contre les menaces - Licences Smart

Vérifier les paramètres de la plate-forme et le DNS correctement configuré

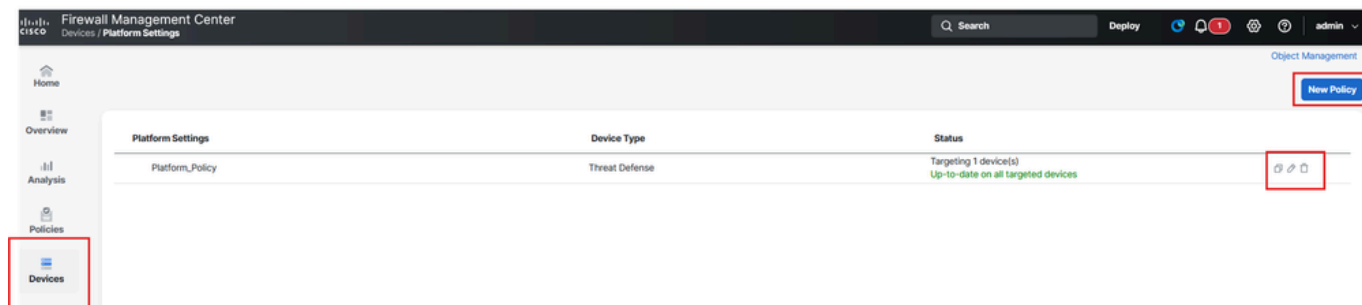
Connexion au FTD via CLI :

- Exécutez la commande pour vérifier si DNS est configuré :

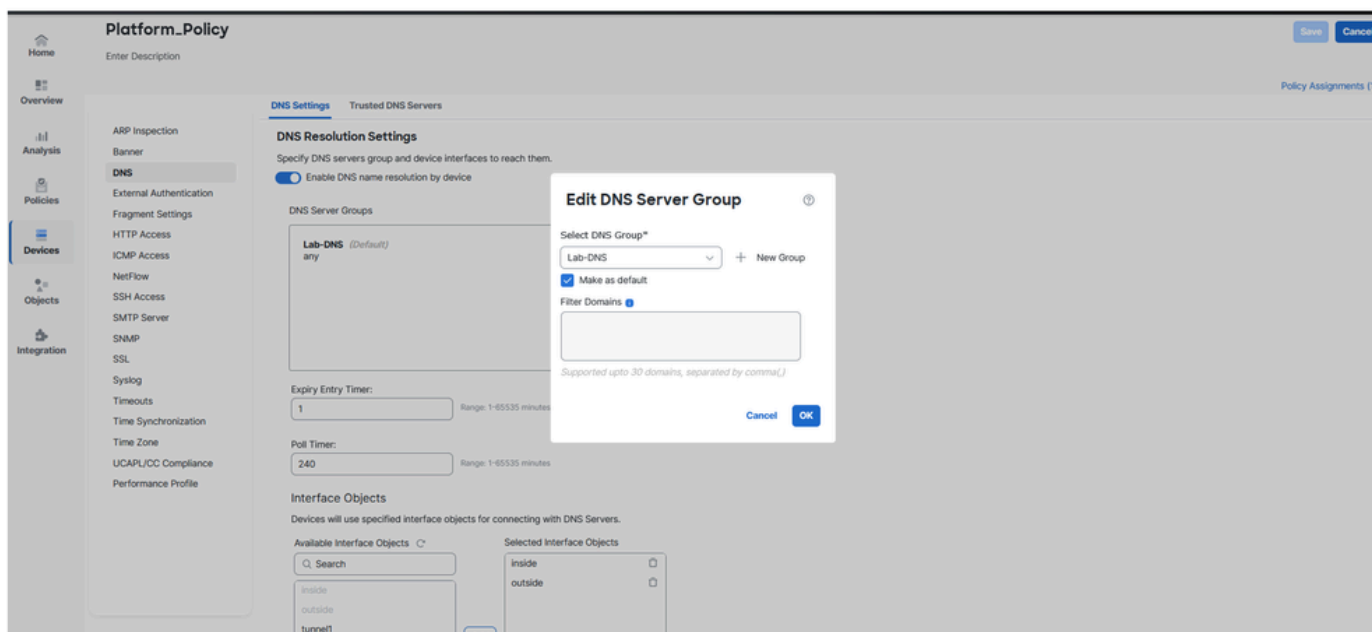
```
show run dns
```

Dans le FMC :

- Cliquez sur **Devices** > Platform Settings , modifiez ou créez une nouvelle stratégie



Protection pare-feu sécurisée - Politique de plate-forme



Protection pare-feu sécurisée contre les menaces - Configuration DNS

Vérifiez via l'interface de ligne de commande FTD que vous pouvez envoyer une requête ping à l'adresse IP et au nom de domaine complet des ressources privées (si vous voulez accéder à PR en utilisant son nom de domaine complet).

```
dns-group Lab-DNS
ftd1# ping ise.tac1ab.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#
```

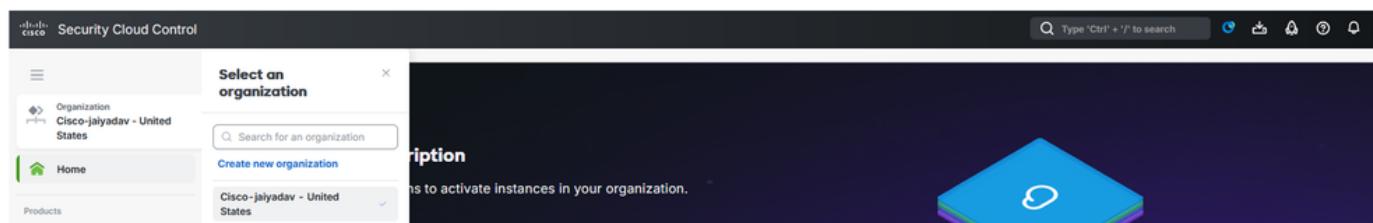
Créer un locataire de contrôle cloud de sécurité sur CDO



Remarque : Si un service partagé SCC est déjà configuré, vous n'avez pas besoin d'en créer un nouveau.

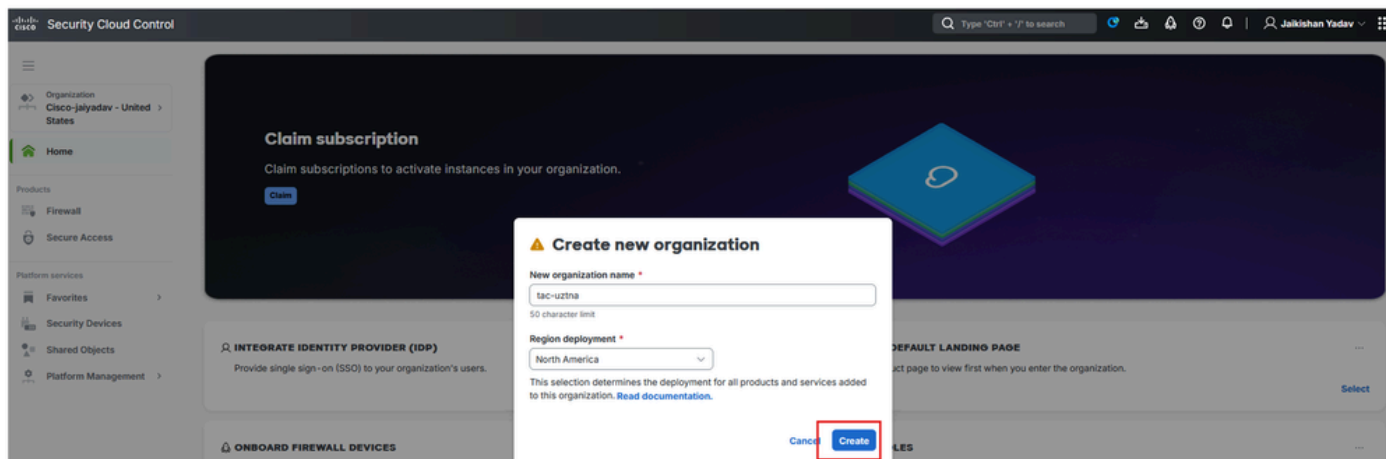
Accédez à [Security Cloud Control](#) :

- Cliquez sur **Organization** > **Create new organization**



Contrôle cloud sécurisé - Entreprise

- Cliquez sur **Create**



Contrôle cloud sécurisé - Création d'entreprise

Une fois le locataire SCC créé, collectez les informations sur le locataire pour activer la microapplication Firewall and Secure Access et pour activer Zutna.

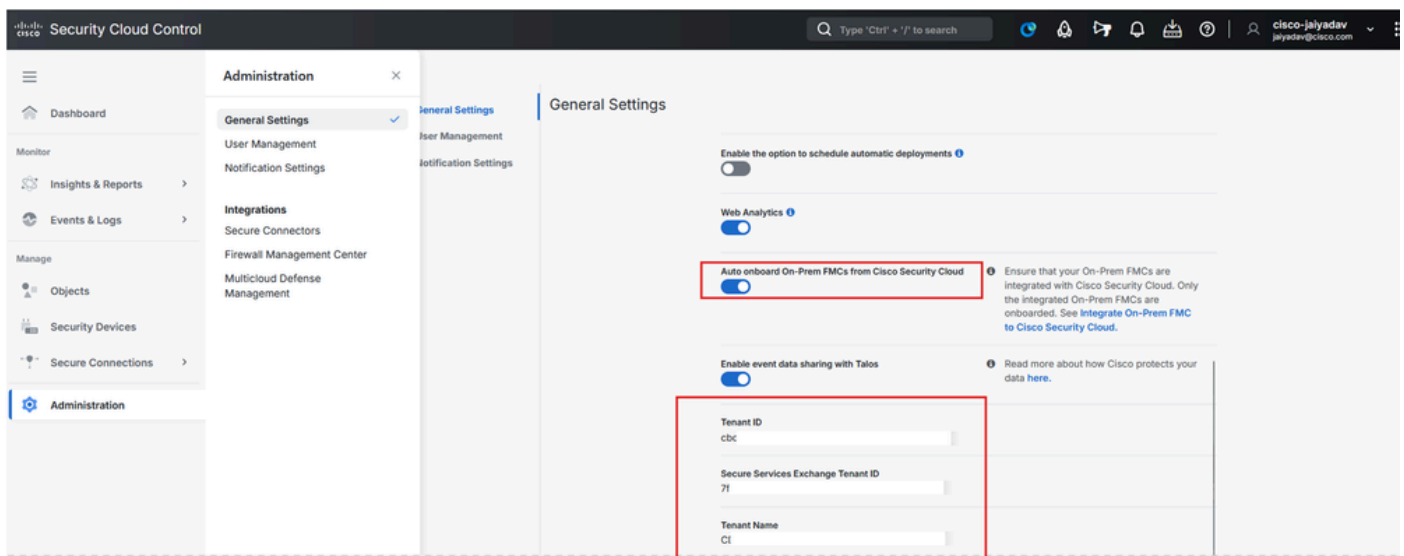
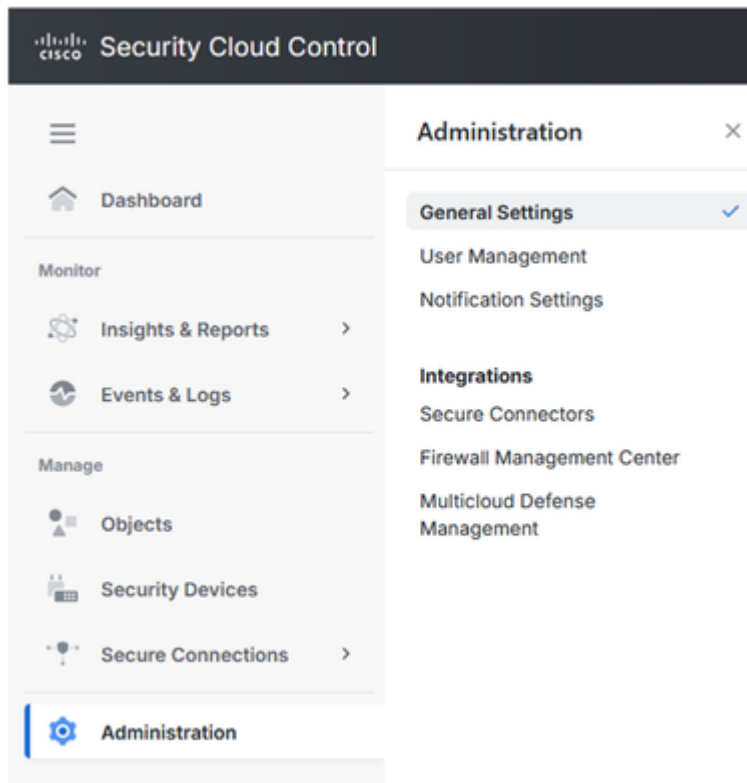
Vérifiez que les paramètres généraux du pare-feu SCC sont configurés

Accédez à [CDO/SCC](#) :

- Cliquez sur **Administration** > **General Settings**
- Assurez-vous que cette **Auto onboard On-Prem FMCs from Cisco Security Cloud** option est activée.

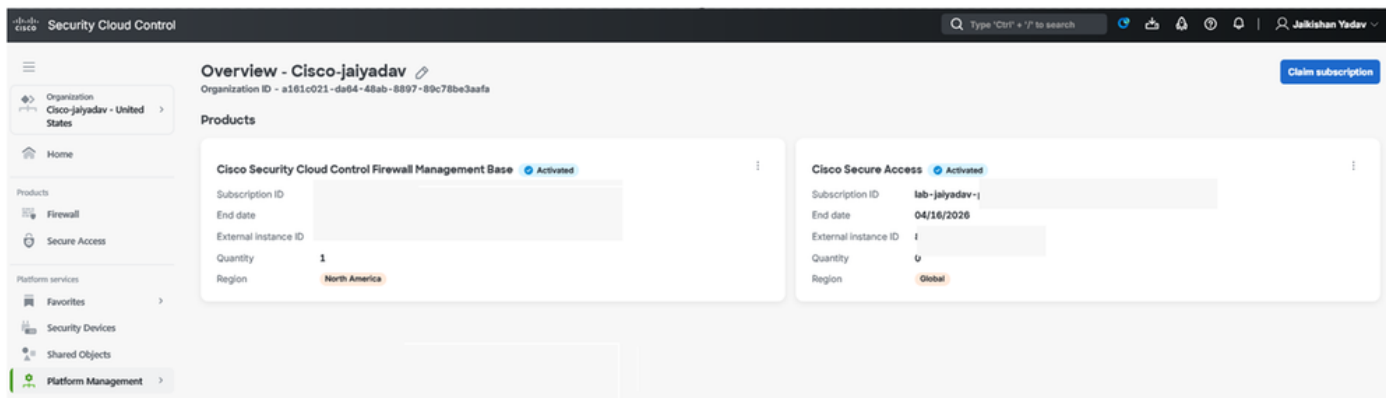


Remarque : L'utilisateur qui tente d'accéder à Secure Access MicroApp doit avoir des rôles **administrateur Security Cloud Control** et **administrateur**.



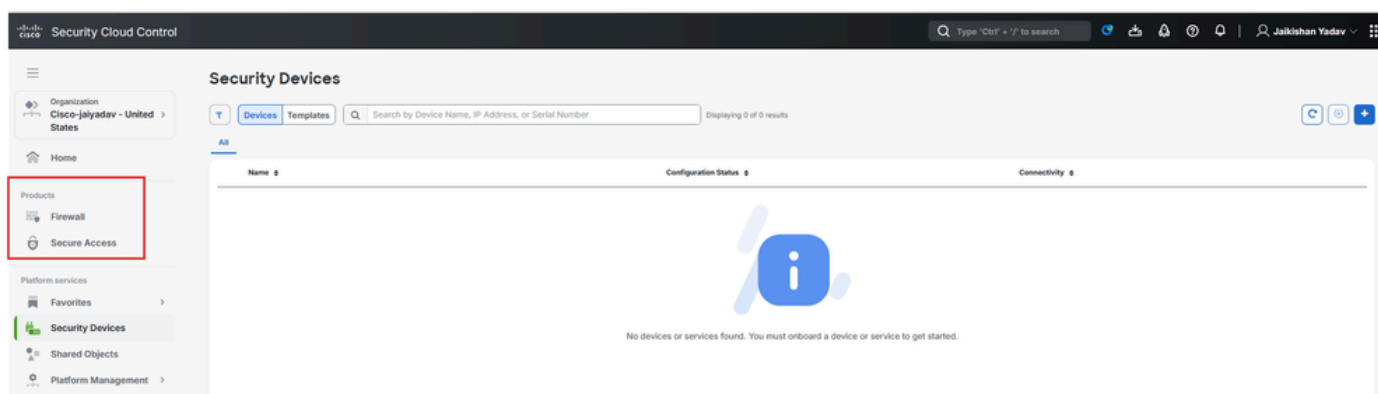
Contrôle cloud sécurisé - Détails de l'entreprise

Vérifier l'intégration de la base de gestion du pare-feu Secure Access Tenant and Security Control



Contrôle du cloud sécurisé - Activation de l'accès sécurisé

Une fois que vous avez terminé l'étape [Create a Security Cloud Control Tenant sur CDO](#) et [Create a Security Cloud Control Tenant sur CDO](#) alors vous pouvez voir les micro-applications de pare-feu et d'accès sécurisé sur le tableau de bord SCC :



Contrôle cloud sécurisé - Micro applications

Générer un certificat signé par l'autorité de certification Firewall Threat Defense (FTD)



Remarque : Vous pouvez également utiliser des certificats [FTD](#) auto-signés FTD (reportez-vous à la section Génération de certificats CA internes et internes auto-signés). Le certificat doit être au format PKCS12 et doit être présent dans le magasin de la machine utilisateur sous l'autorité de certification racine approuvée.

Afin de générer un certificat signé par l'autorité de certification en utilisant FTD dans la fonctionnalité openssl de build :

- Accédez à FTD
- Exécuter la `expertcommande`
- Générer une CSR et une clé avec openssl
 - Commande OpenSSL :

```
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
```

Demande de signature de certificat

- Copier le CSR et obtenir un certificat CA signé
- Utiliser le certificat et la clé signés par l'autorité de certification FTD et convertir le certificat au format PKCS12
 - Commande OpenSSL :

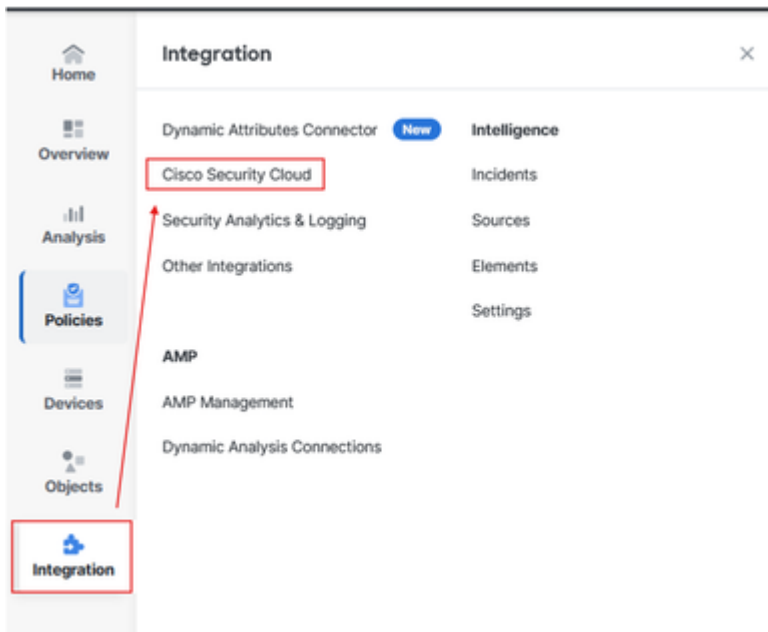
```
openssl pkcs12 -export -out ftdcert.p12 -in cert.crt -inkey cert.key
```

- Exportez le certificat à l'aide de SCP ou d'un autre outil.

Centre de gestion des pare-feu sur site pour le contrôle du cloud de sécurité

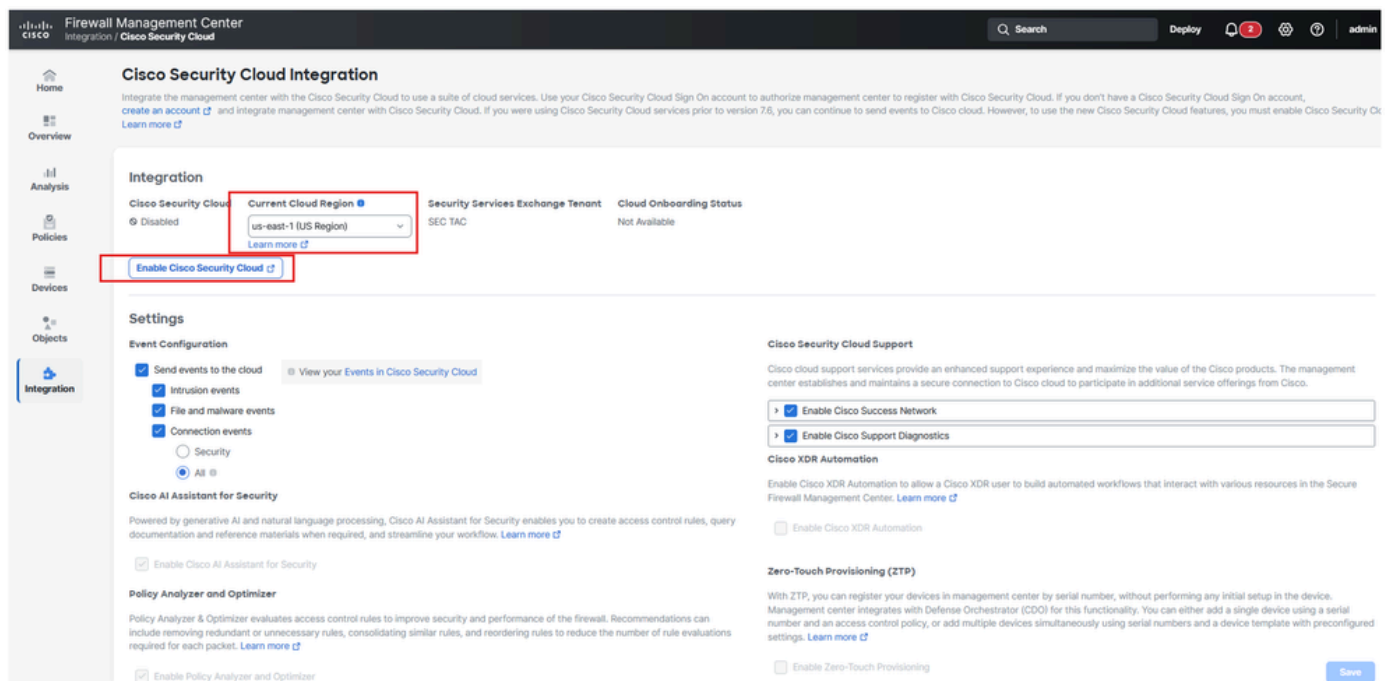
Accédez à FMC :

- Cliquez sur **Integration** > Cisco Security Cloud



Intégration de Firewall Management Center et SCC

- Sélectionnez la région Cloud, puis cliquez sur [Enable Cisco Security Cloud](#)



Intégration de Firewall Management Center à SCC

Il ouvrira un nouvel onglet de navigateur, sur le nouvel onglet :

- Cliquez sur [Continue to Cisco SSO](#)



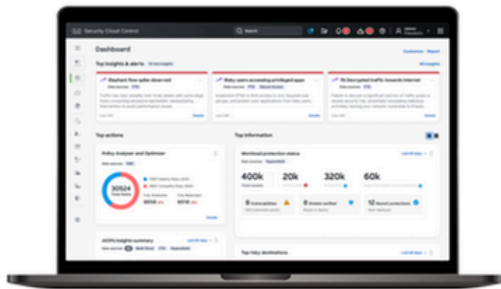
Remarque : Assurez-vous que vous vous déconnectez de SCC et qu'aucun autre onglet n'est ouvert.



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

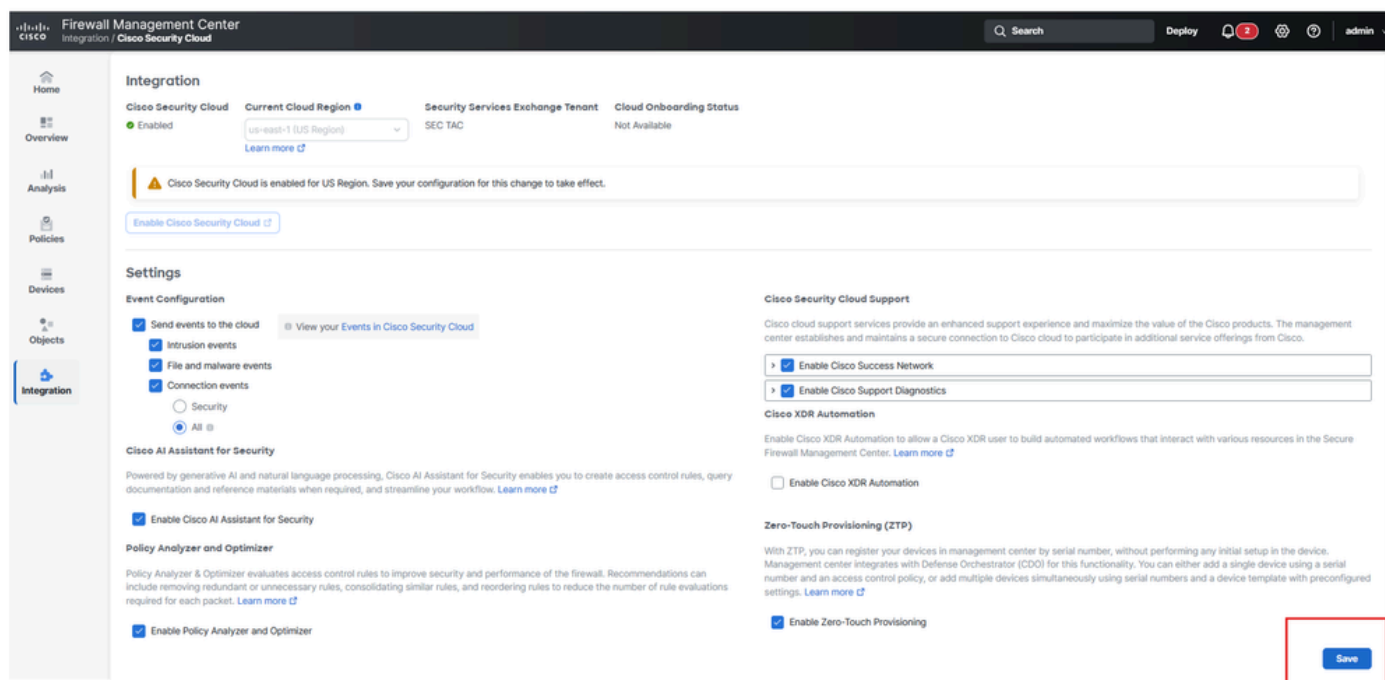
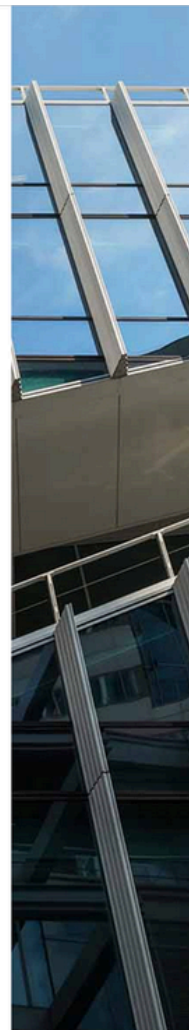
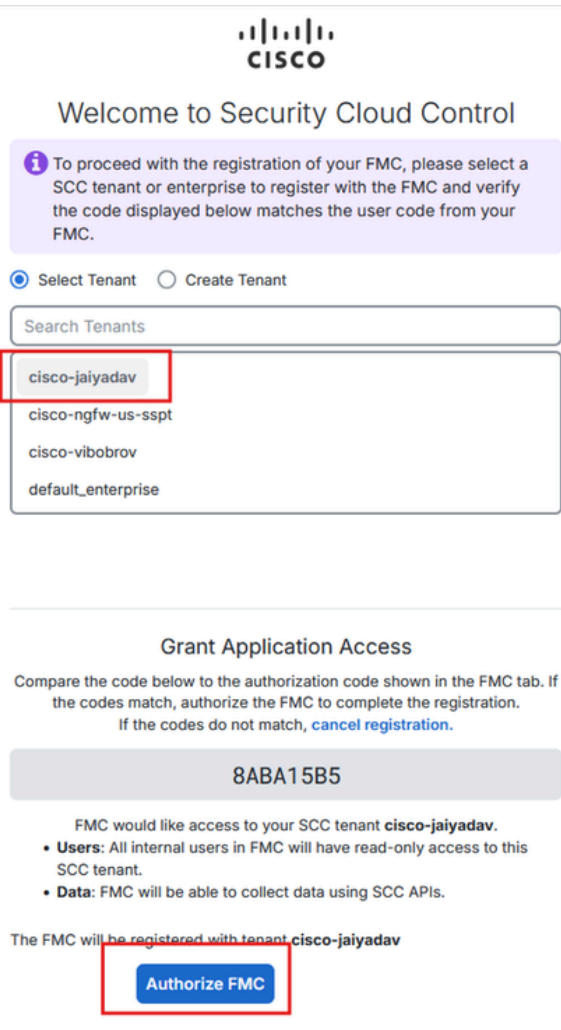
2

Register FMC with a SCC Tenant

[Continue to Cisco SSO](#)

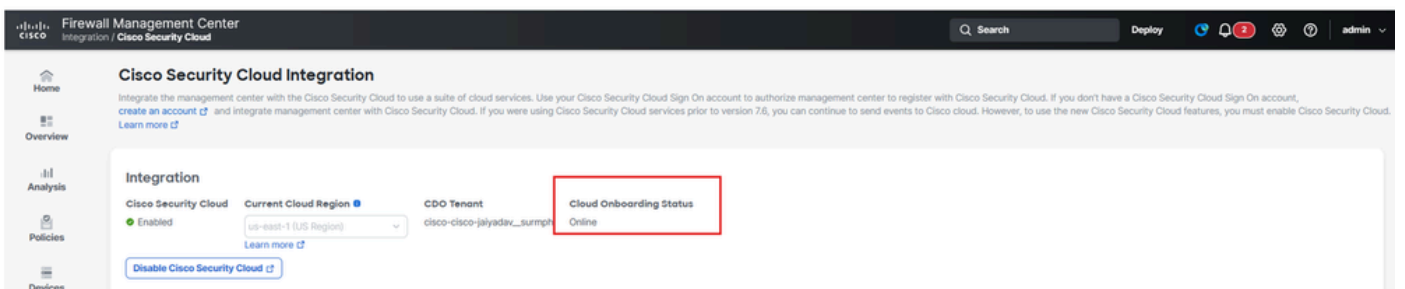
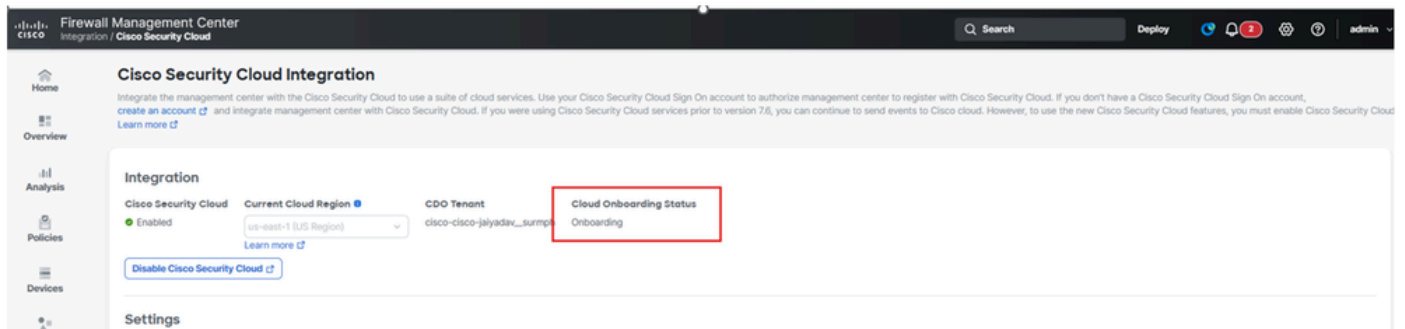
Intégration de Firewall Management Center à SCC

- Choisissez votre client SCC et cliquez sur [Authorize FMC](#)



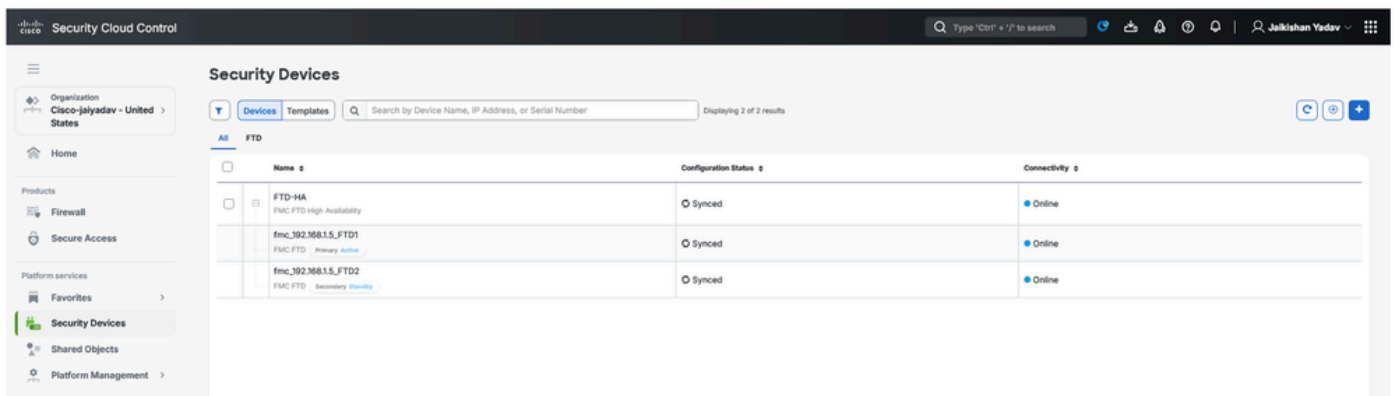
Intégration de Firewall Management Center à SCC

L'état de Cloud Onboarding Status doit passer de Not Available à Onboarding , puis Online.



État d'intégration de Firewall Management Center

- Accédez à [SCC](#) et vérifiez l'état FTD sous Platform Services > Security Devices



Statut de défense contre les menaces du pare-feu sécurisé sur SCC

Inscription des paramètres d'accès réseau sans confiance universel (uZTNA) sur FTD

Accédez à SCC :

- Cliquez sur Platform Services > Security Devices > FTD > Device Management > Universal Zero Trust Network Access

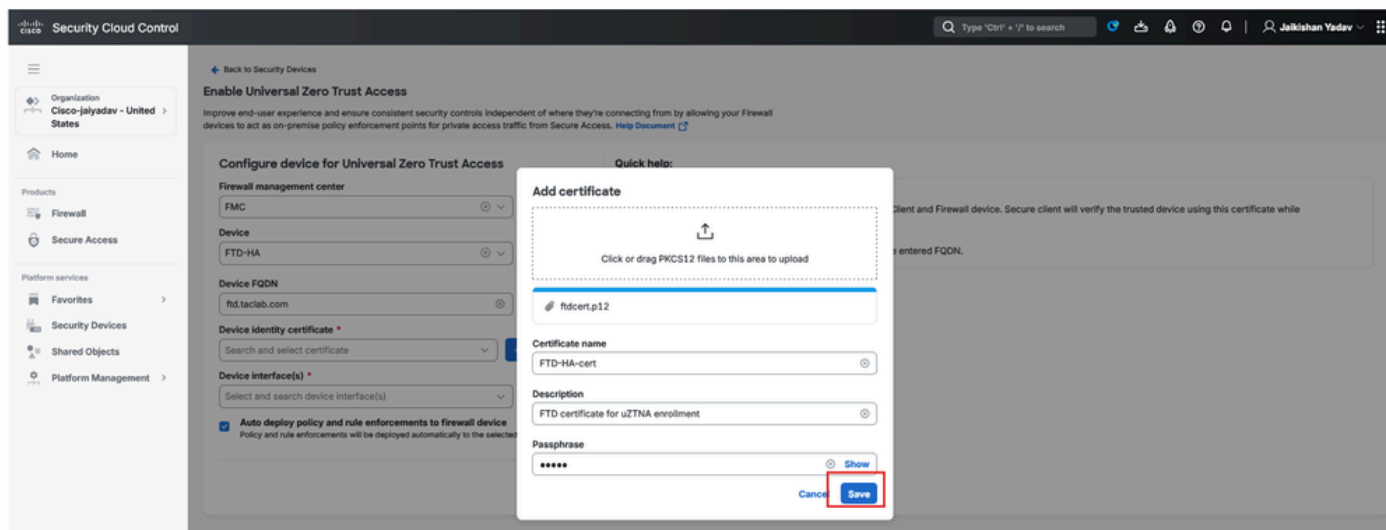
The screenshot shows the Cisco Security Cloud Control interface. On the left, the navigation menu includes 'Platform services' (1) and 'Security Devices' (2). The main area displays a table of security devices under the 'FTD' filter. The first device, 'FTD-HA' (3), is highlighted. On the right, the 'Device Details' panel for 'FTD-HA' is shown, with 'Device Management' (4) and 'Universal zero trust access settings' (5) highlighted.

Protection pare-feu sécurisée contre les menaces - Configuration ZTNA universelle

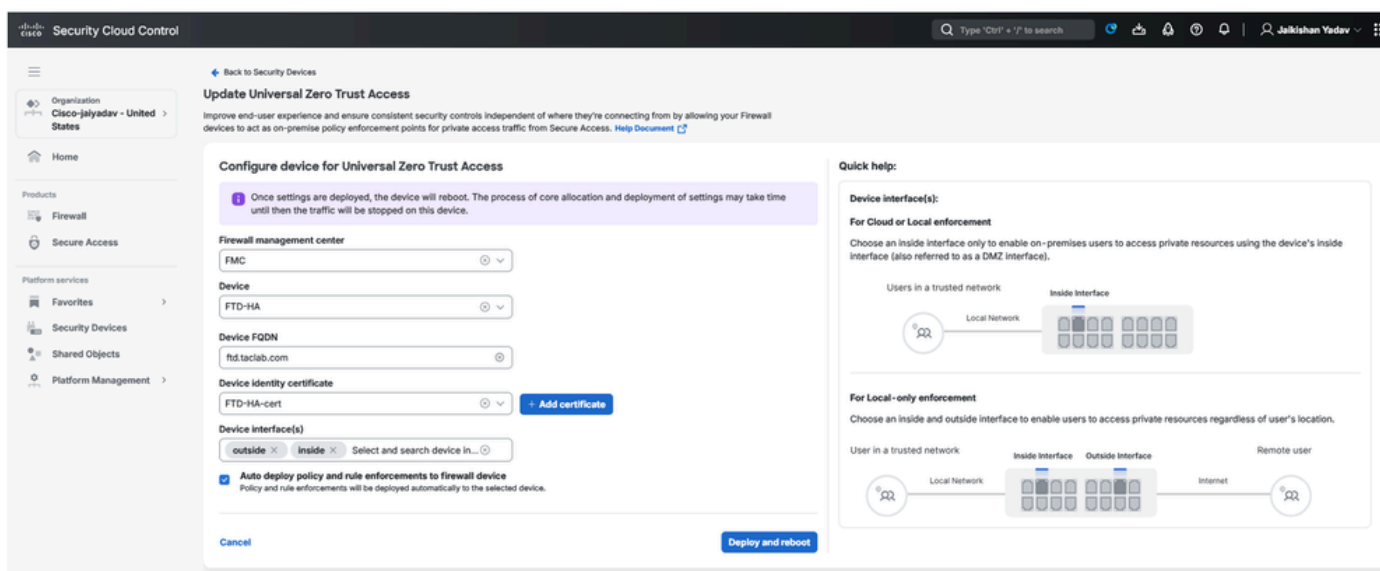
- Remplissez les informations et téléchargez le certificat FTD généré à l'étape [Générer un certificat signé par l'autorité de certification Firewall Threat Defense \(FTD\)](#)

The screenshot shows the 'Enable Universal Zero Trust Access' configuration page. The 'Configure device for Universal Zero Trust Access' section includes the following fields: 'Firewall management center' (FMC), 'Device' (FTD-HA), 'Device FQDN' (Enter device FQDN), 'Device identity certificate' (Search and select certificate), and 'Device interface(s)' (Select and search device interface(s)). There is an 'Add certificate' button and a 'Deploy' button. The 'Quick help' section provides diagrams for 'For Cloud or Local enforcement' and 'For Local-only enforcement'.

Protection pare-feu sécurisée contre les menaces - Configuration ZTNA universelle



Protection pare-feu sécurisée contre les menaces - Configuration ZTNA universelle

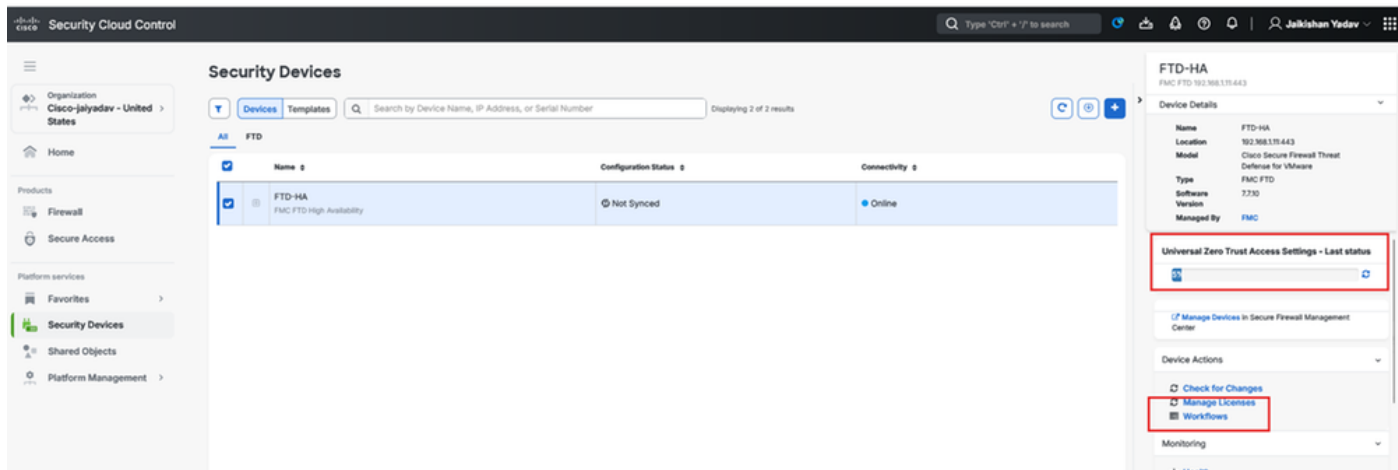


Protection pare-feu sécurisée contre les menaces - Configuration ZTNA universelle

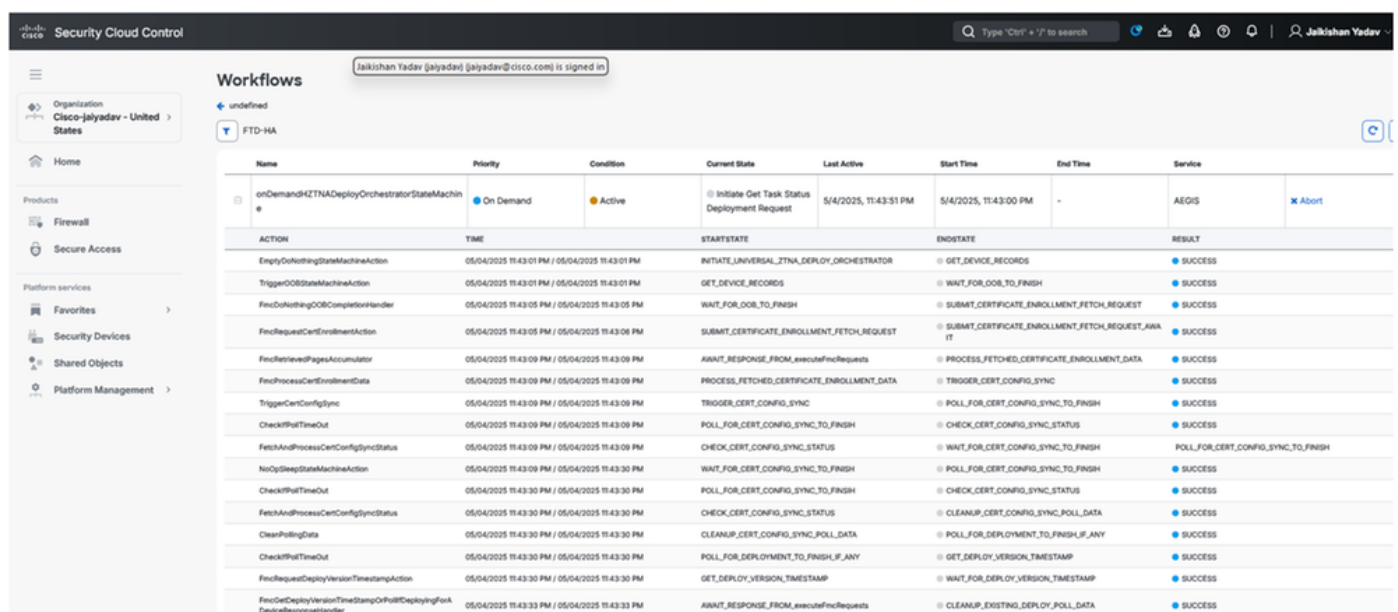


Remarque : Lorsque vous activez Zuta sur FTD HA , il déploie les modifications et redémarre simultanément les deux unités Firewall Threat Defense (FTD). Veillez à planifier une fenêtre de maintenance appropriée.

- Cliquez sur **Workflow** pour vérifier les journaux

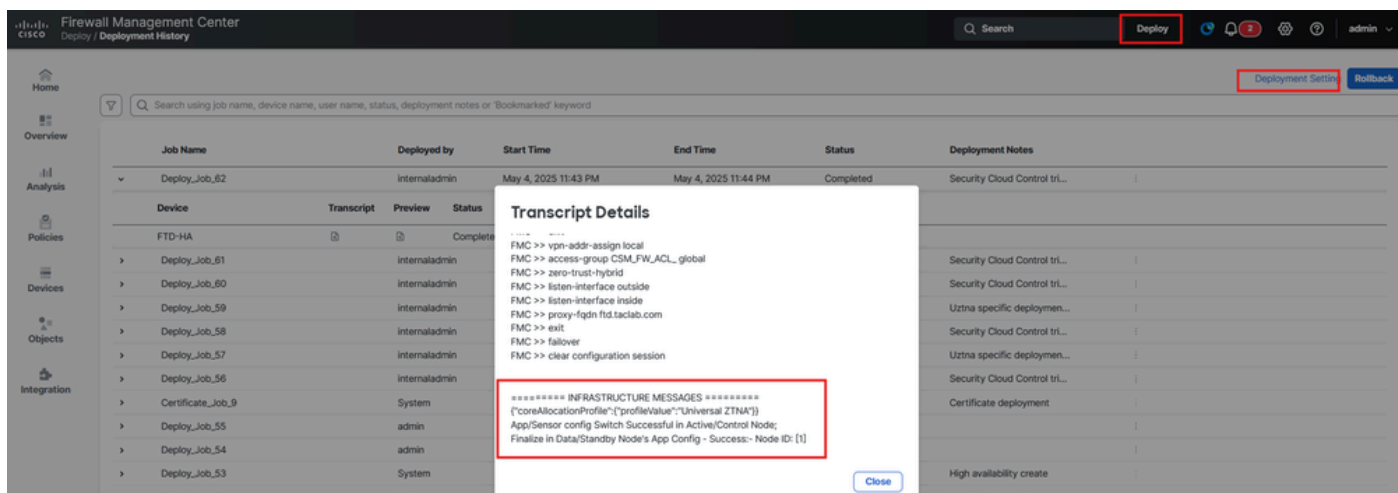


Protection pare-feu sécurisée contre les menaces : état de configuration ZTNA universel



Flux de travail de contrôle cloud de sécurité

Sous Détails de la transcription, vous pouvez voir Policy Deployment Status et modifier FMC.



Secure Firewall Management Center - État du déploiement des politiques

Inscrire le client avec ZuTNA

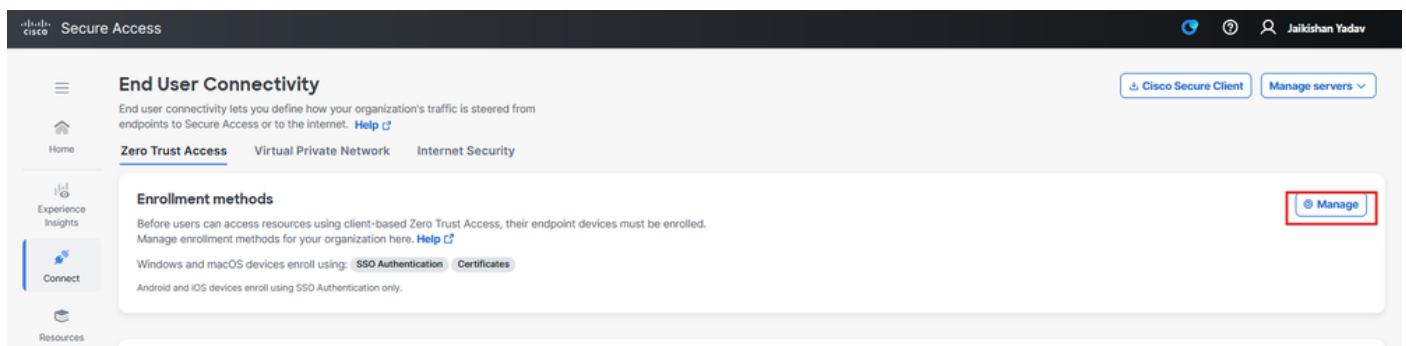
Configuration d'accès sécurisé



Remarque : Vous pouvez utiliser SSO ou une inscription ZTA basée sur un certificat. Les étapes suivantes décrivent l'inscription ZTA basée sur un certificat

Accédez à [Secure Access Dashboard](#) :

- Cliquez sur **Connect** > **End User Connectivity** > Zero Trust Access
- Cliquez sur **Manage**



Accès sécurisé - Inscription au certificat ZTA

- Télécharger le certificat d'autorité de certification racine et télécharger le fichier de configuration d'inscription

Secure Access

Zero Trust Access

Enrollment methods

Before users can access resources using client-based Zero Trust Access, their endpoint devices must be enrolled. Manage enrollment methods for your organization here. [Help](#)

Windows and macOS devices

☒ **Use SSO Authentication**
Enrollment requires user action.

1. Install Cisco Secure Client on user devices.
2. Give your users instructions for enrolling in Zero Trust Access.

☒ **Use Certificates**
Enrollment occurs without user action.

1. Upload a CA Certificate if necessary
At least one uploaded root certificate or certificate chain must be able to validate identity certificates on endpoint devices during zero trust enrollment and renewal.

CA Certificates

[No CA certificates](#) [Upload a CA Certificate](#)

2. Download the enrollment configuration file
The file is regenerated each time a new CA certificate is uploaded.
Deploy this file to user devices.

[Download](#) 8295509_ZTA_Enroll_Cert.json

You can also download this configuration file and Cisco Secure Client from the [Download Cisco Secure client](#) page.

[Save](#) [Cancel](#)

Accès sécurisé - Inscription au certificat ZTA

- Cliquez sur **Save**

Configuration du client

Copier le fichier de configuration d'inscription dans C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollment_choices

enrollment_choices

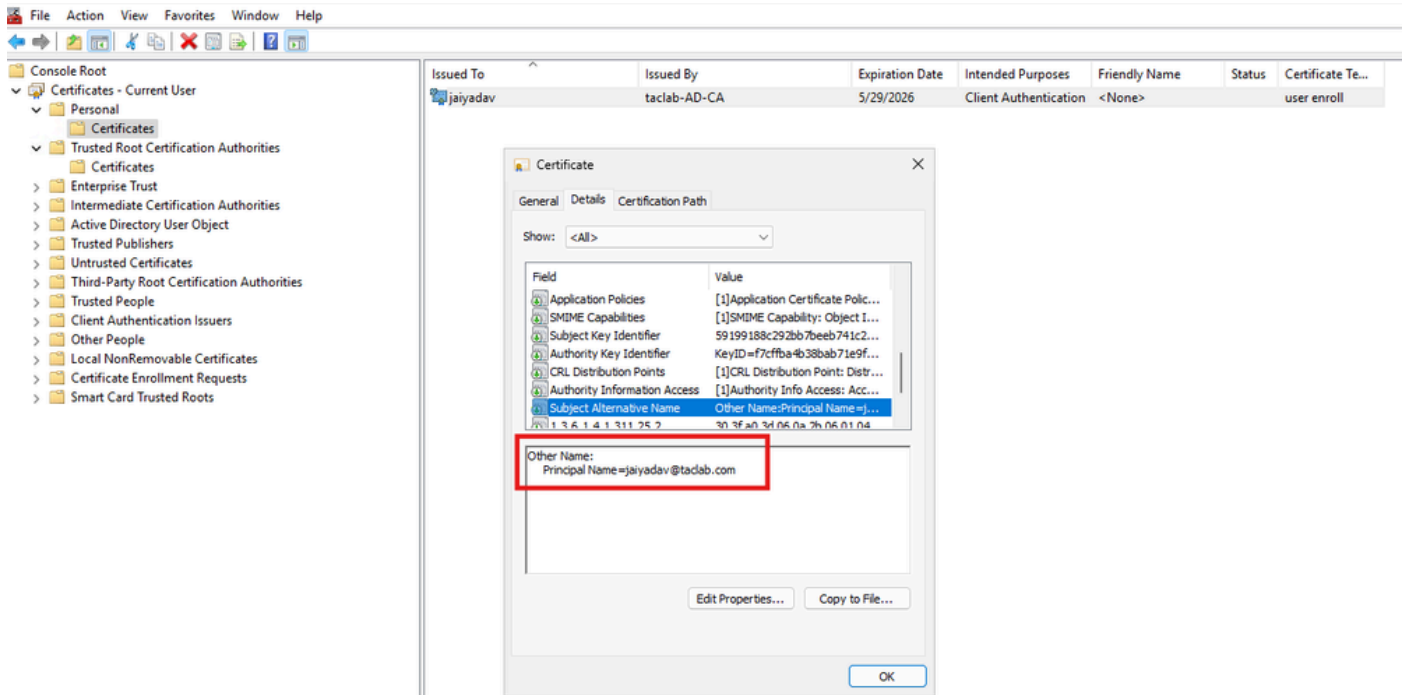
Cisco > Cisco Secure Client > ZTA > enrollment_choices

Search enrollment_choices

New | Cut | Copy | Paste | Delete | Sort | View | Details

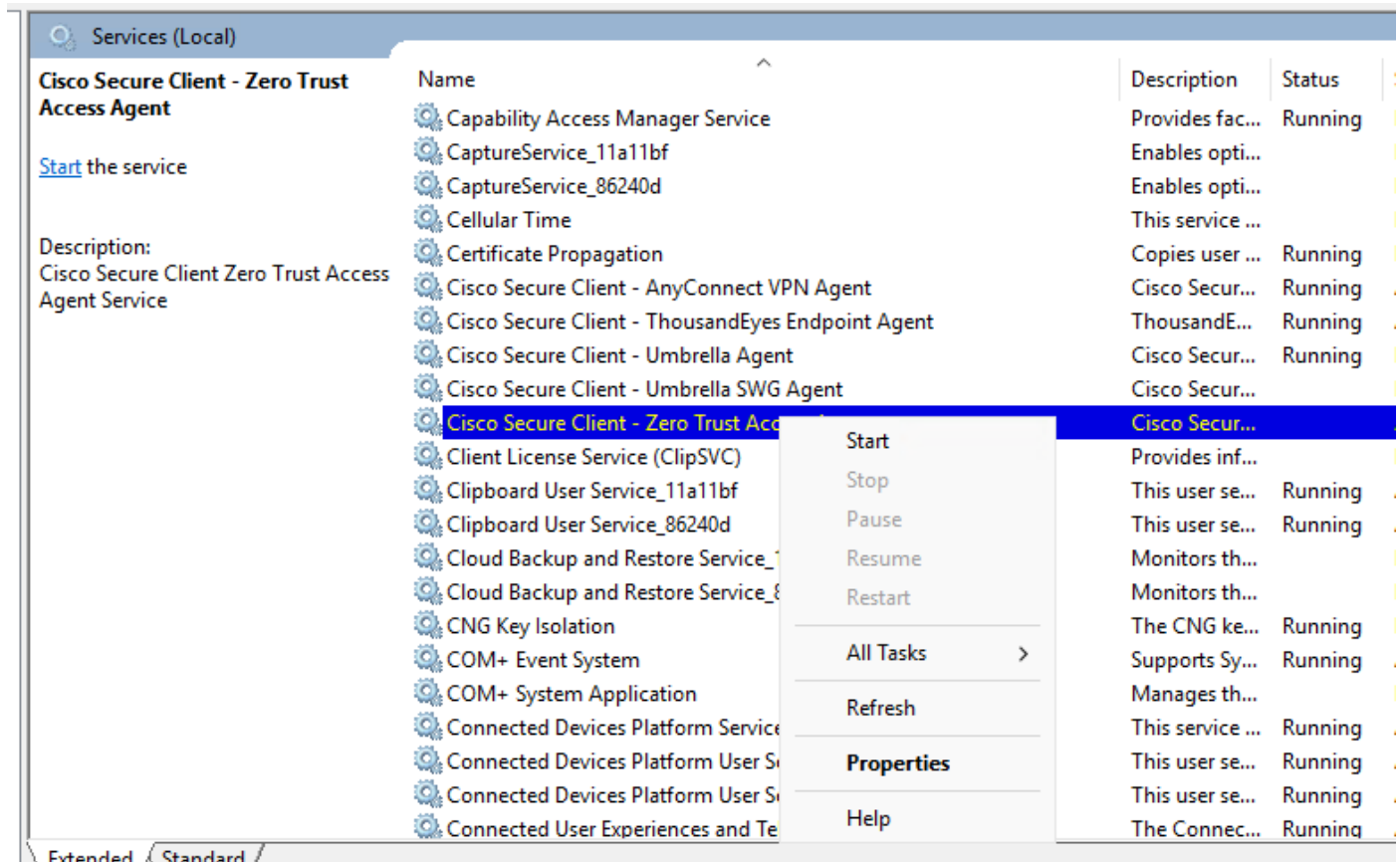
Name	Date modified	Type	Size
8295509_ZTA_Enroll_Cert	5/10/2025 11:22 AM	JSON File	3 KB

- Créer un certificat client, qui doit avoir un champ UPN dans SAN



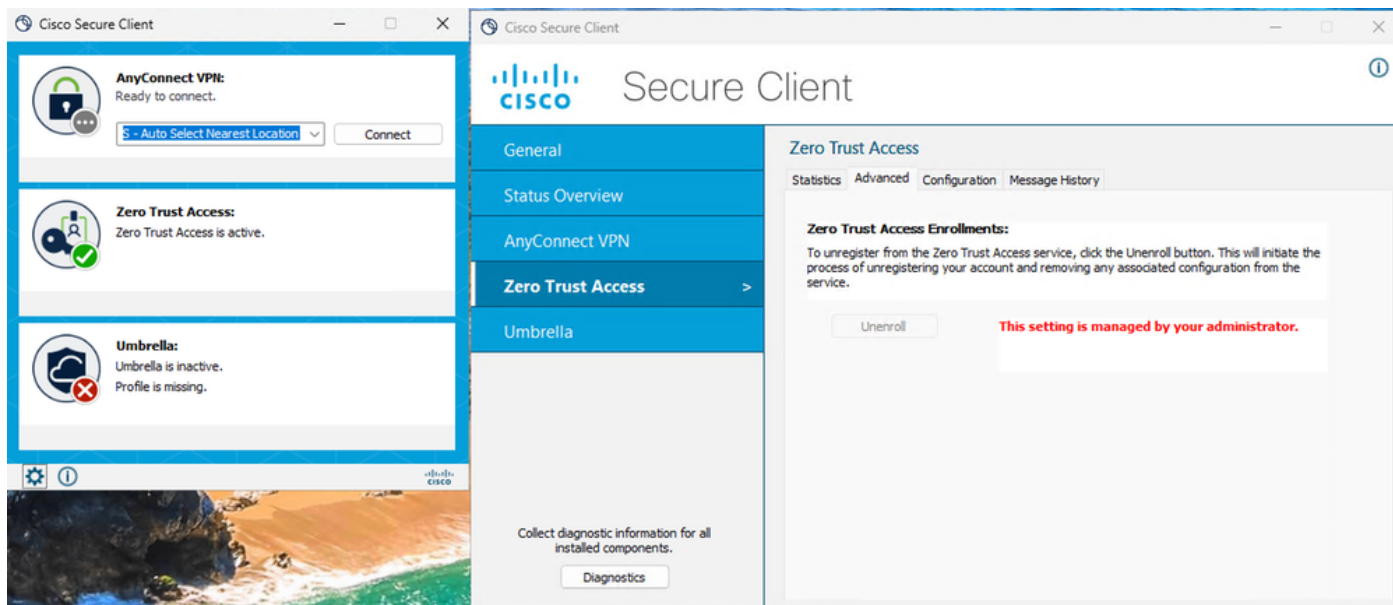
Installation du certificat

- Démarrer/ Redémarrer Cisco Secure Client - Zero Trust Access Agent



Services Windows

- Vérification de l'état du module ZTA



Accès sécurisé - Statut d'inscription de certificat ZTA

Vérifier

Utilisez la commande suivante pour vérifier la configuration ZUNTA sur Firewall Threat Defense (FTD) :

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

Informations connexes

- [Assistance technique de Cisco et téléchargements](#)
- [Centre d'aide Cisco Secure Access](#)
- [Guide de conception Cisco SASE](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.