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

Table des matières

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

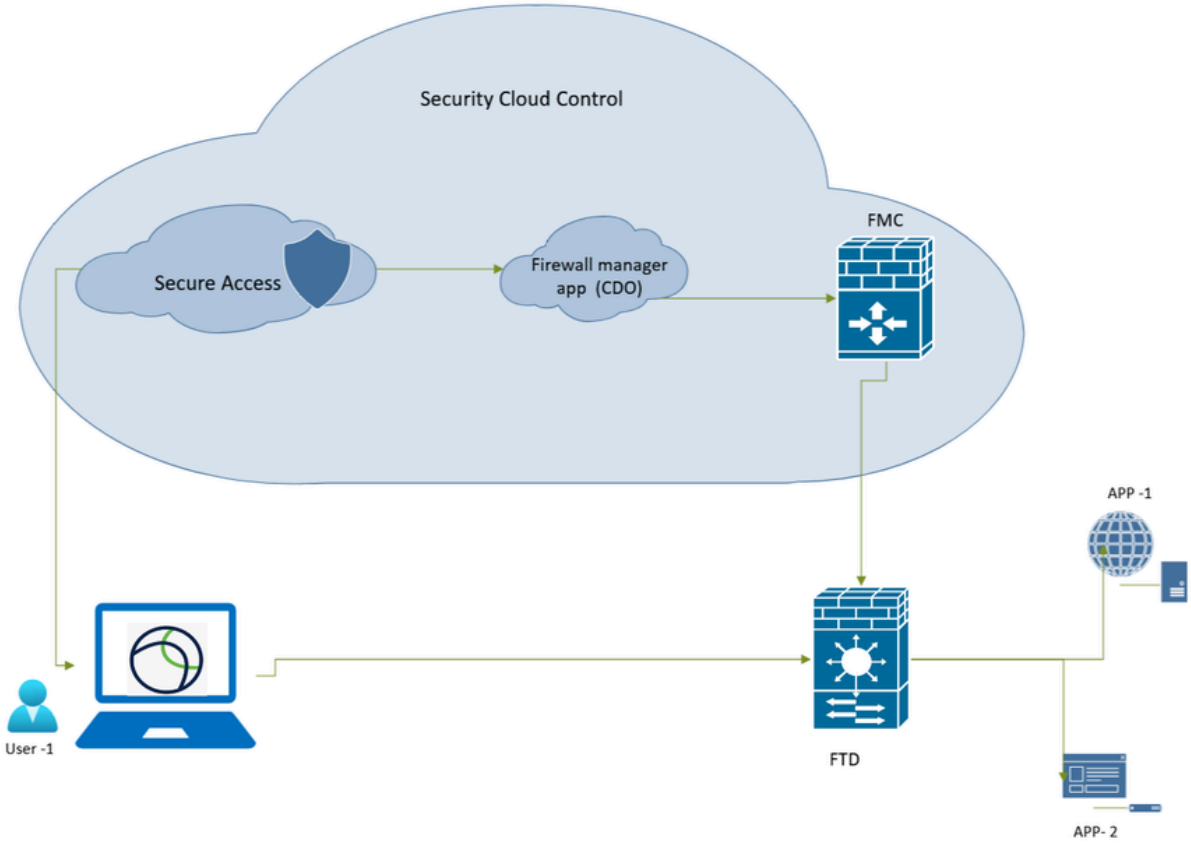
Composants utilisés

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

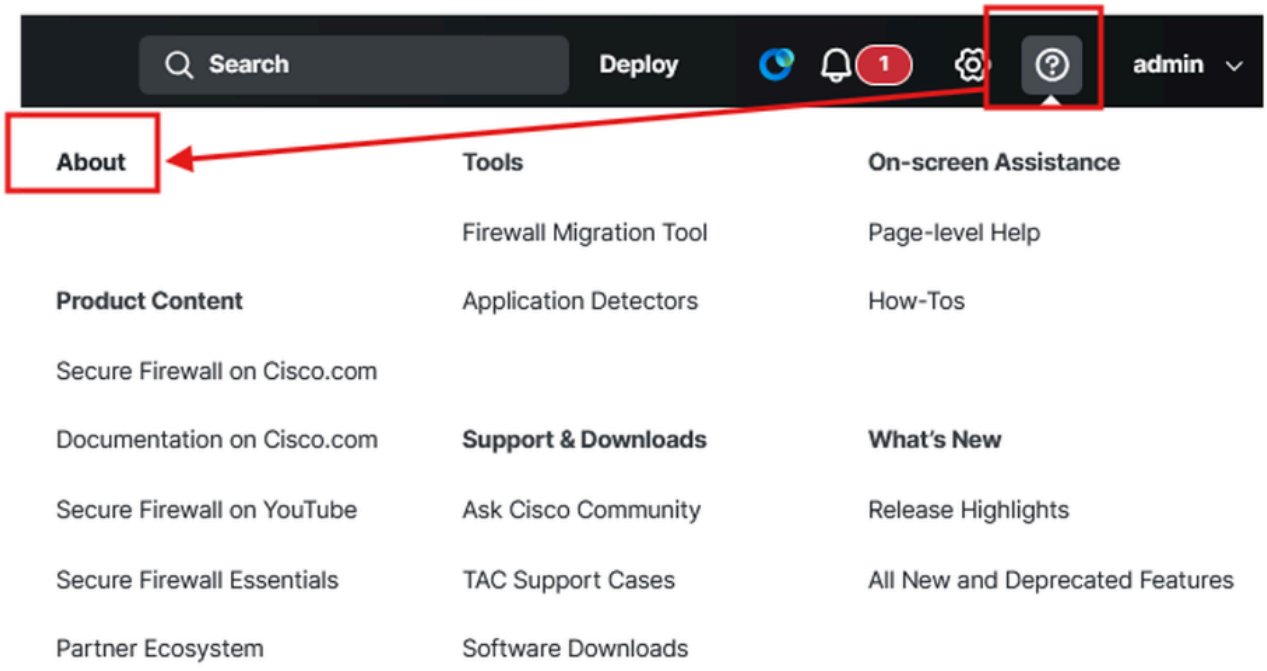
- Les sessions ZTNA universelles ne prennent pas en charge les trames jumbo

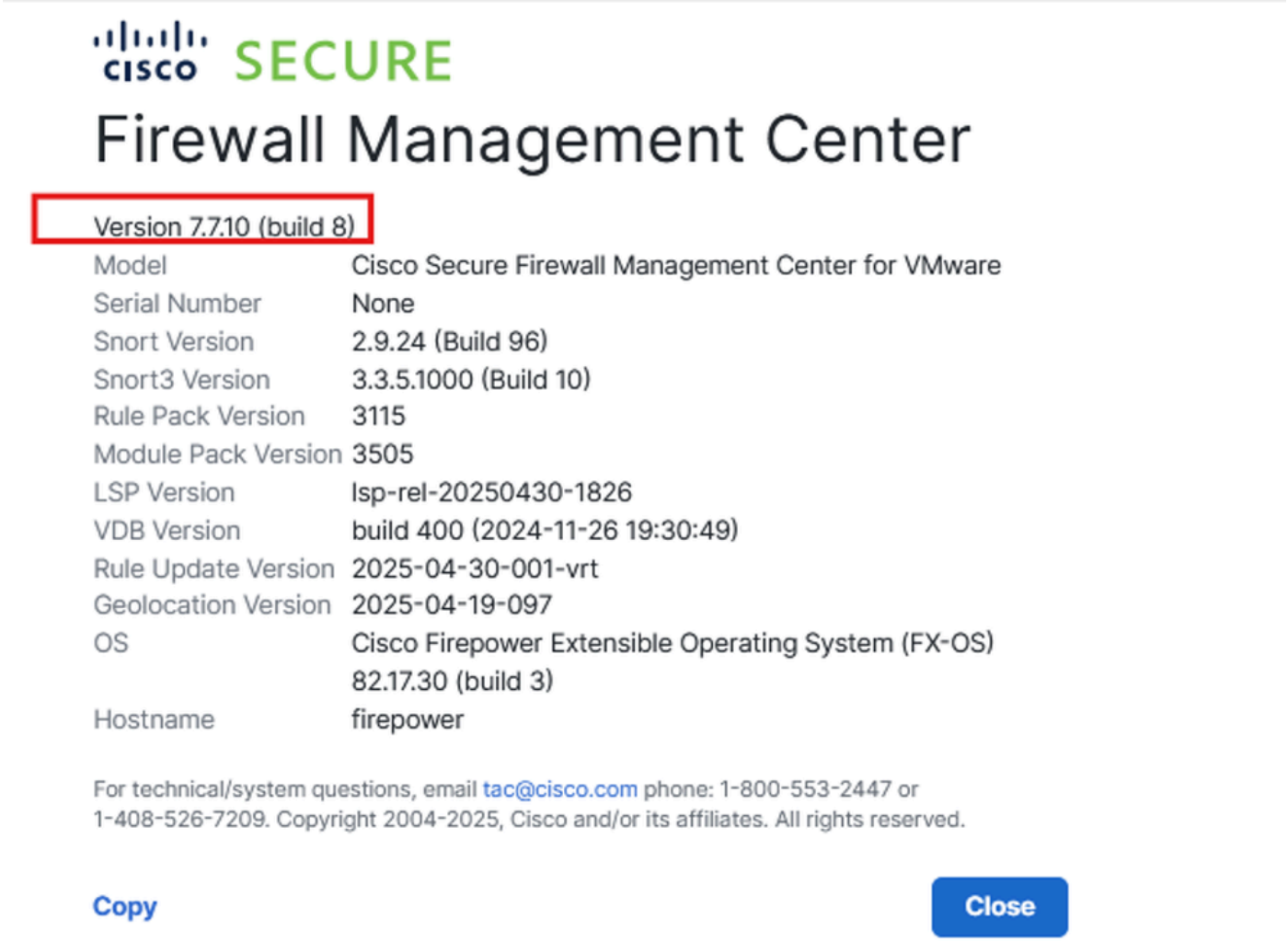
Configurer

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



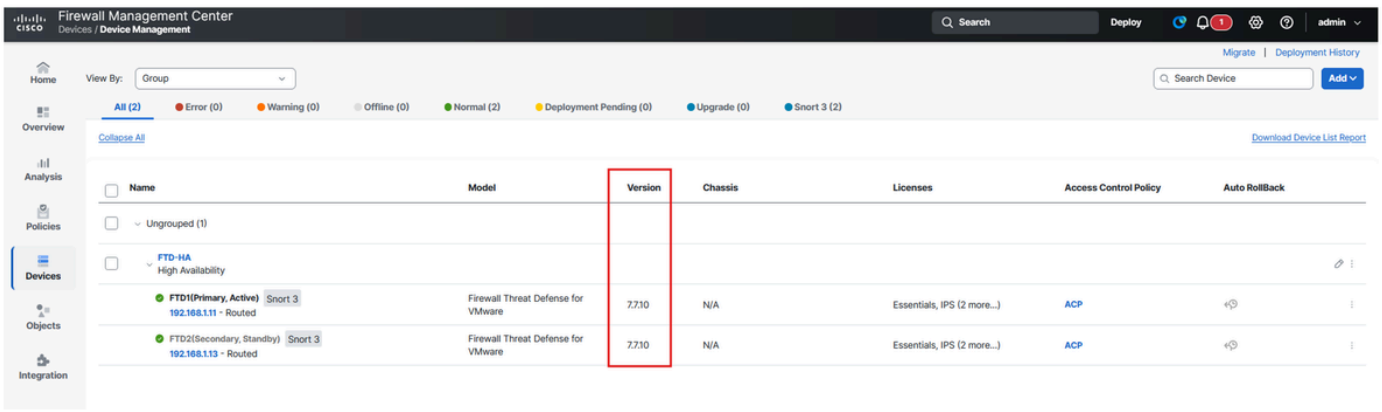


Secure Firewall Management Center - Version du logiciel

Vérifier la version FTD

Accédez à l'interface utilisateur FMC :

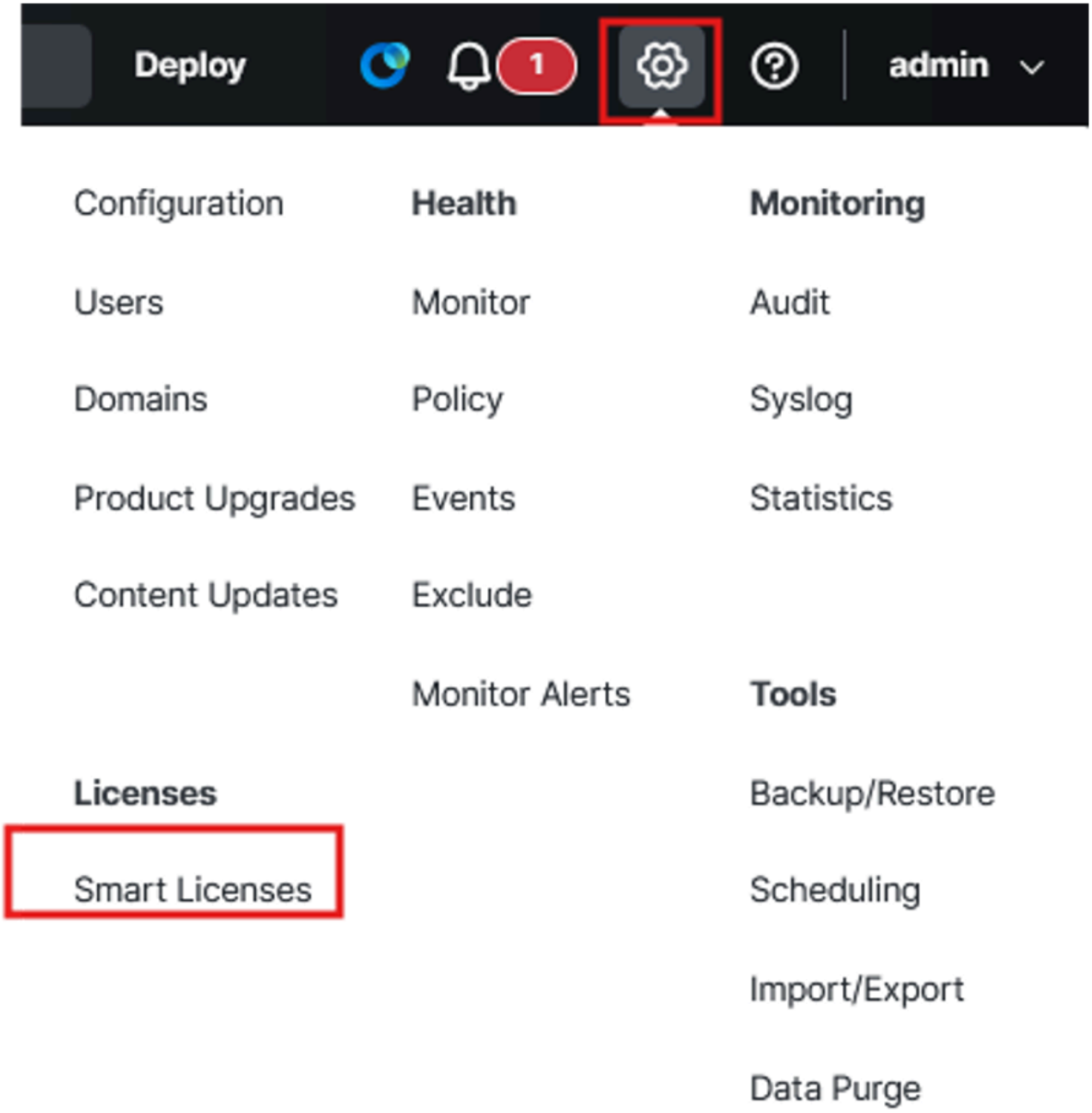
- Cliquez surDevices> Device Management

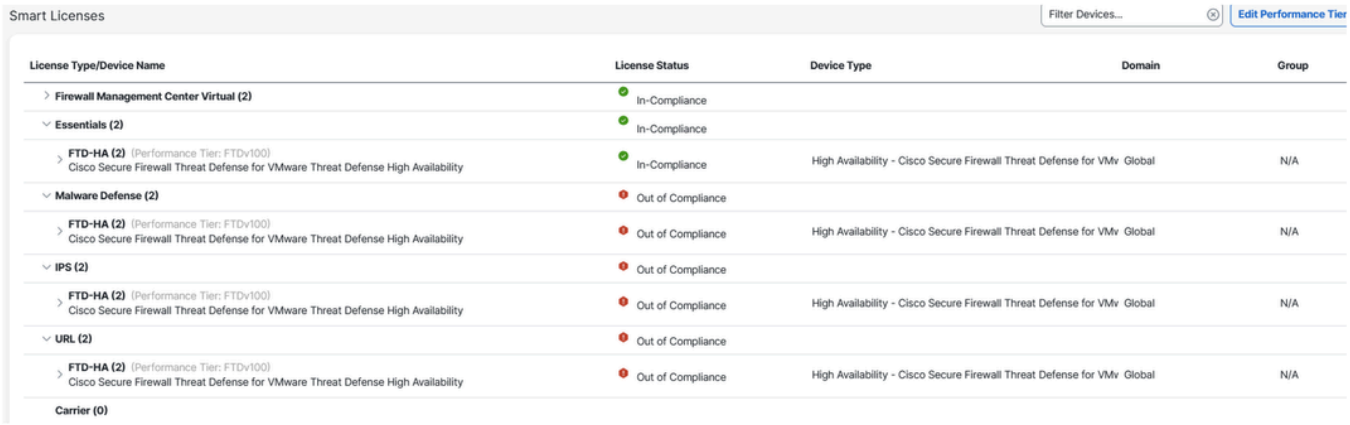


Protection pare-feu sécurisée contre les menaces - Version logicielle

Vérifier les licences FTD

- Cliquez sur Setting Icon > Licenses> Smart Licenses





Protection pare-feu sécurisée contre les menaces - Licences Smart

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

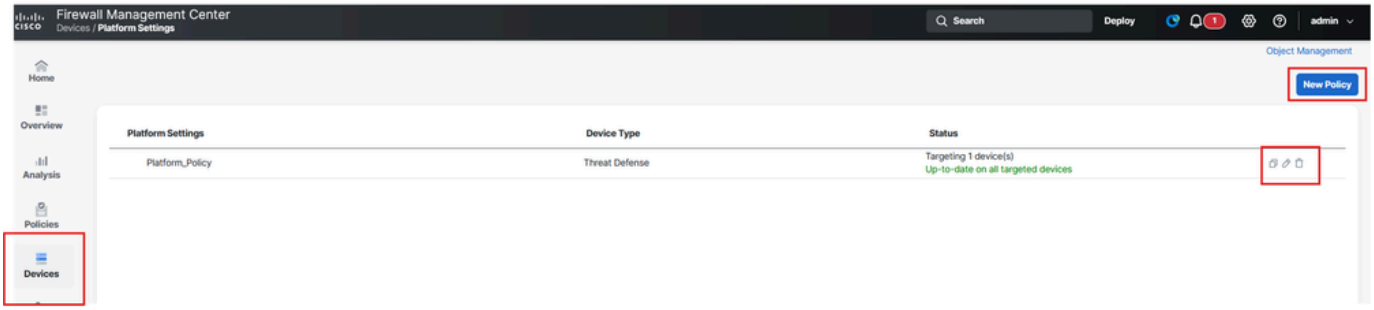
Connexion au FTD via CLI :

- Exécutez la commande pour vérifier si DNS est configuré :

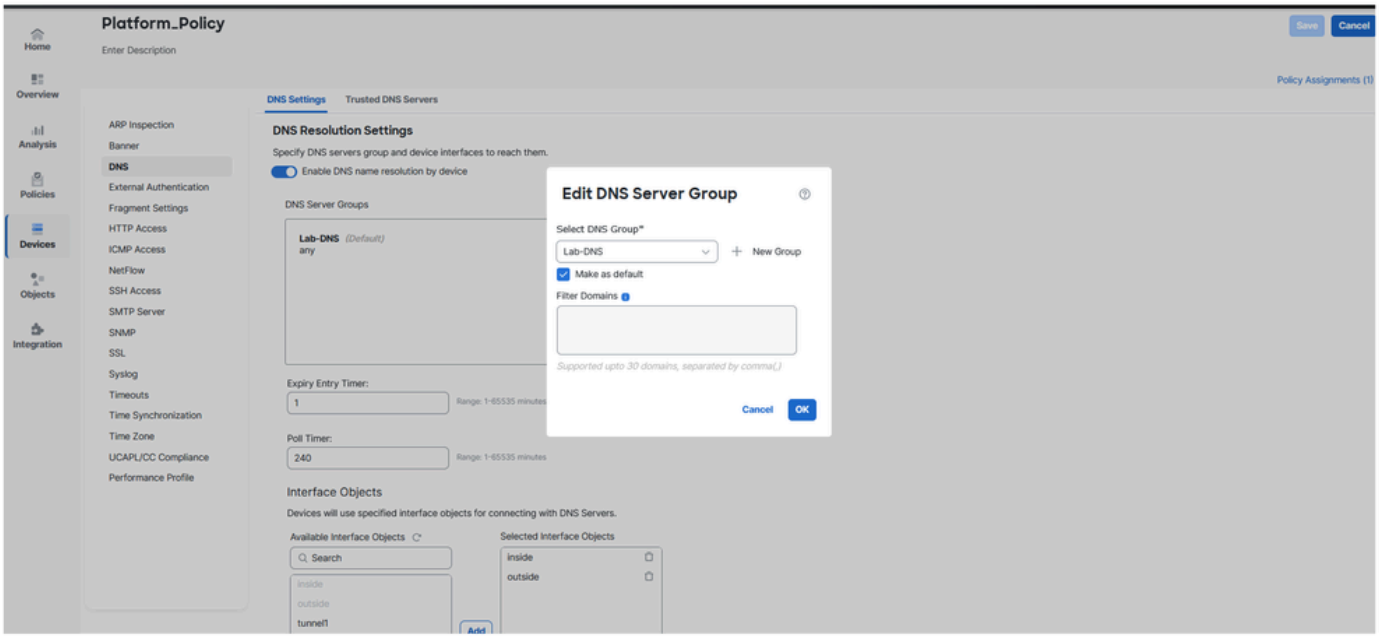
```
show run dns
```

Dans le FMC :

- Cliquez surDevices> 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).

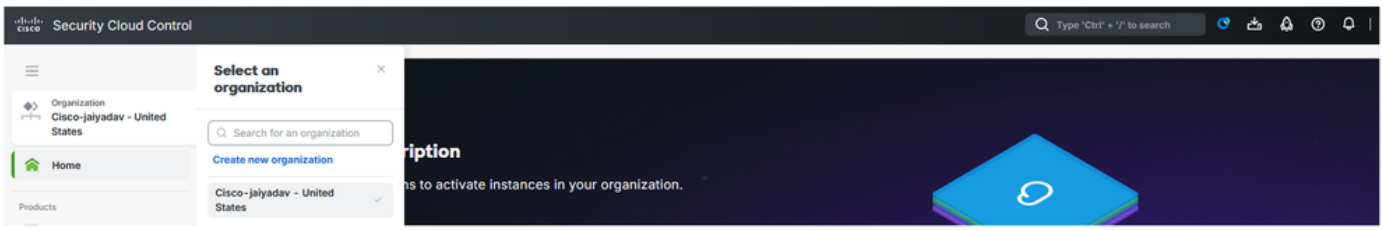
```
dns-group Lab-DNS
ftd1# ping ise.taclab.com
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.50, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
ftd1#
```

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.

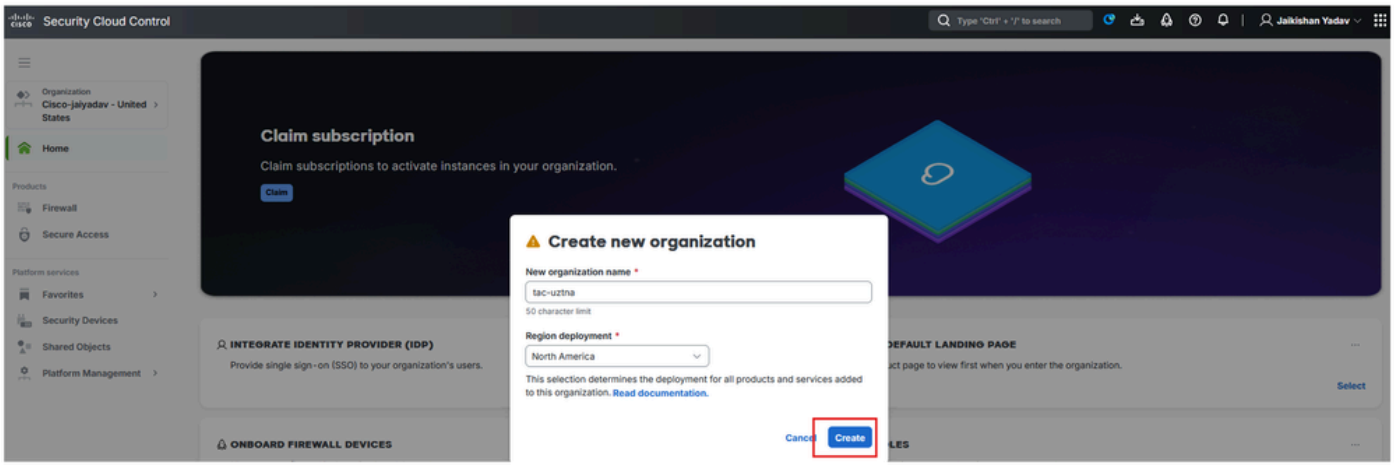
Accédez à Security Cloud Control :

- Cliquez surOrganization > Create new organization



Contrôle cloud sécurisé - Entreprise

- Cliquez sur Create



Contrôle cloud sécurisé - Création d'entreprise

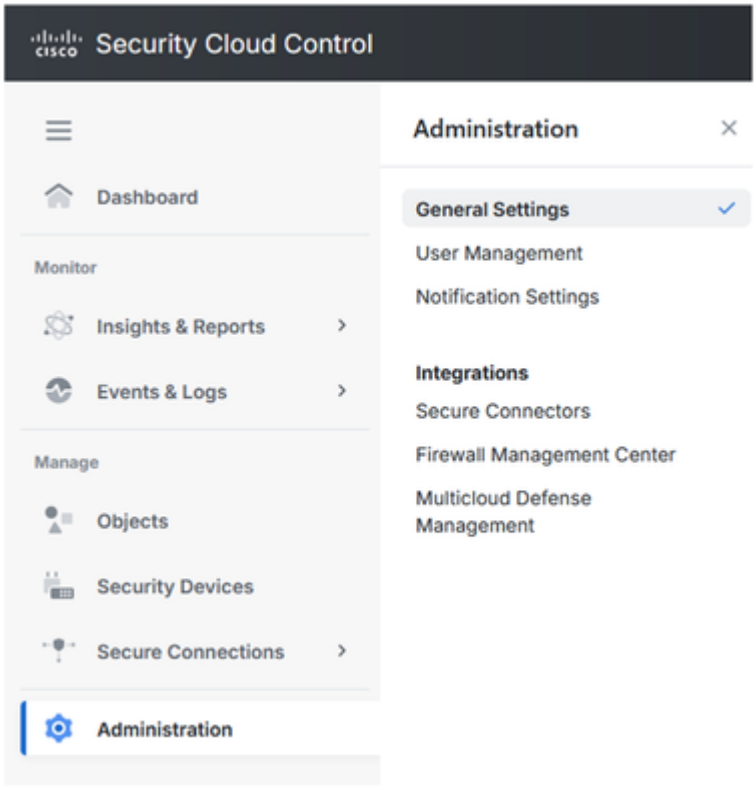
Une fois le locataire SCC créé, collectez les informations sur le locataire pour activer la microapplication Firewall and Secure Access et pour activer Zutna.

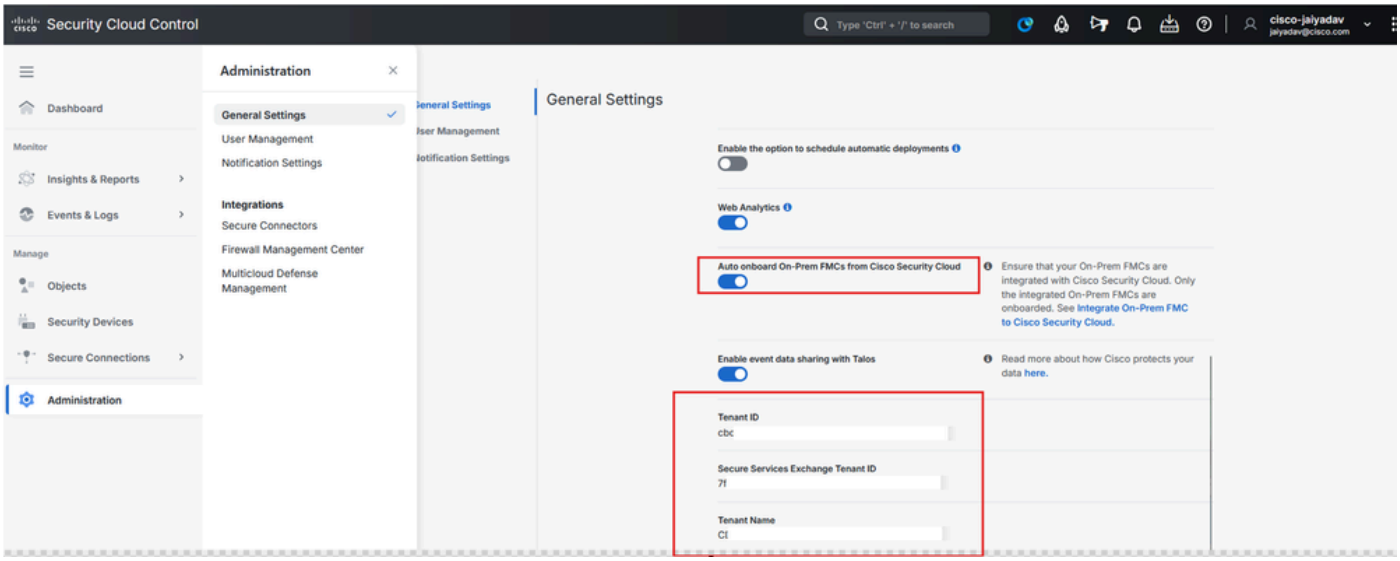
Vérifiez que les paramètres généraux du pare-feu SCC sont configurés

Accédez à CDO/SCC :

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

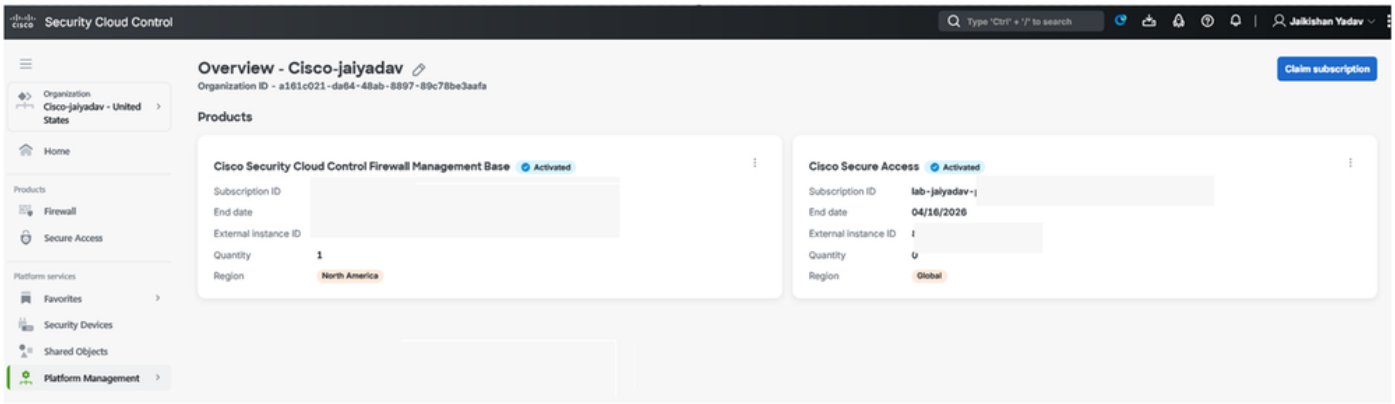
Remarque : L'utilisateur qui tente d'accéder à Secure Access MicroApp doit avoir desSecure Accessrôles administrateur Security Cloud Control et administrateur.





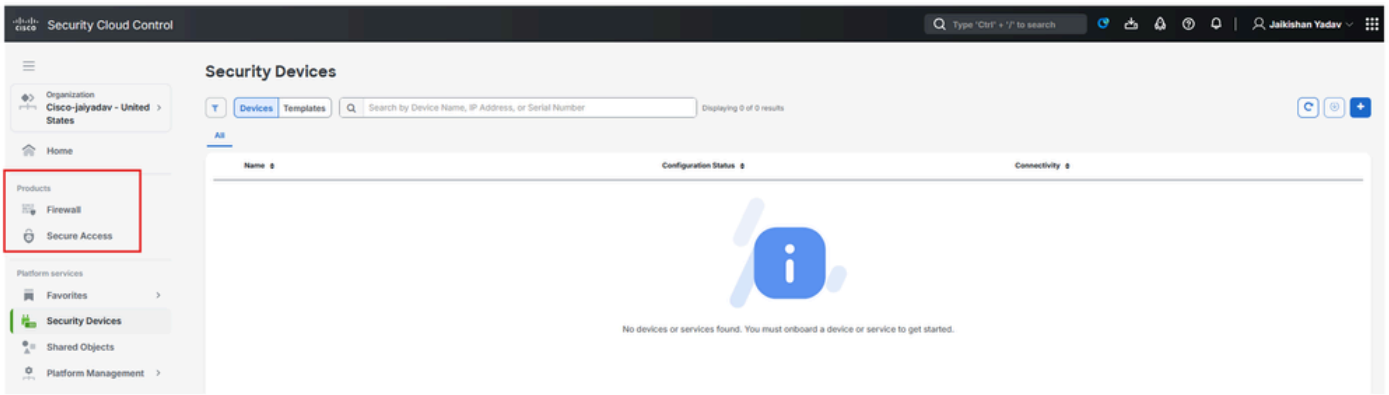
Contrôle cloud sécurisé - Détails de l'entreprise

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)

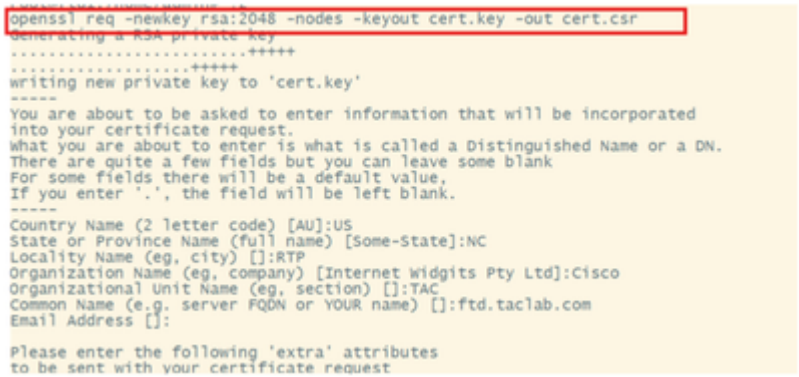
Remarque : Vous pouvez également utiliser des certificats FTD auto-signés FTD (reportez-vous à la section Génération de certificats CA internes et internes auto-signés). Le certificat doit être au format PKCS12 et doit être présent dans le magasin de la machine utilisateur sous l'autorité de certification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

- Générer une CSR et une clé avec openssl
  - Commande OpenSSL :

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



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 :

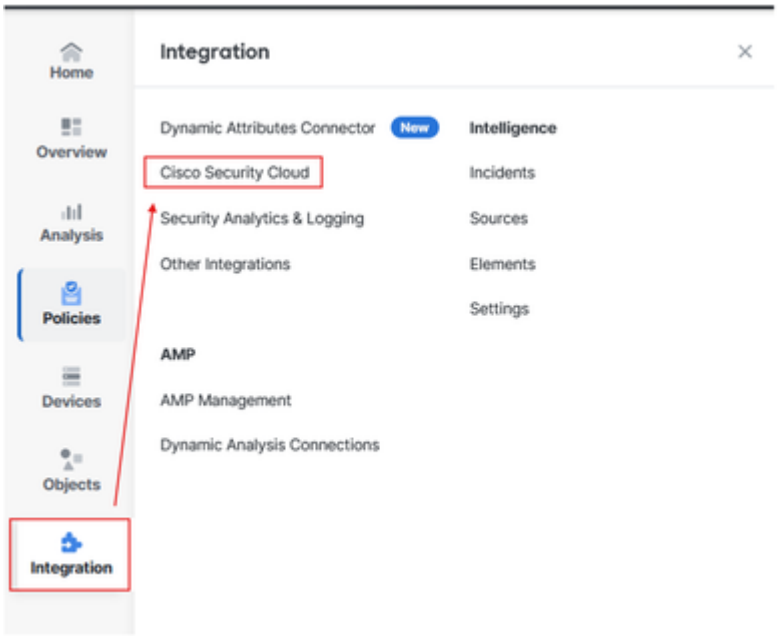
```
openssl pkcs12 -export -out ftdcert.p12 -in cert.crt -inkey cert.key
```

- 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

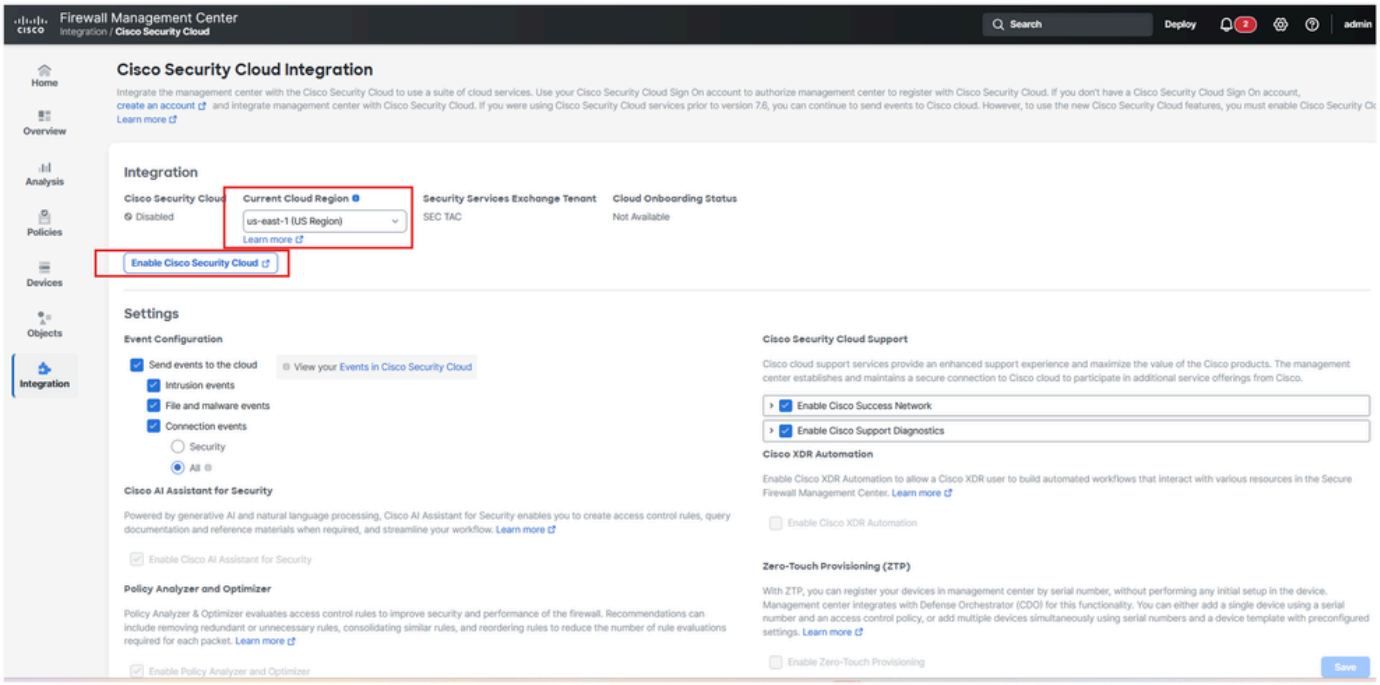
Accédez à FMC :

- Cliquez surIntegration> Cisco Security Cloud



Intégration de Firewall Management Center et SCC

- Sélectionnez la région Cloud, puis cliquez sur Enable Cisco Security Cloud

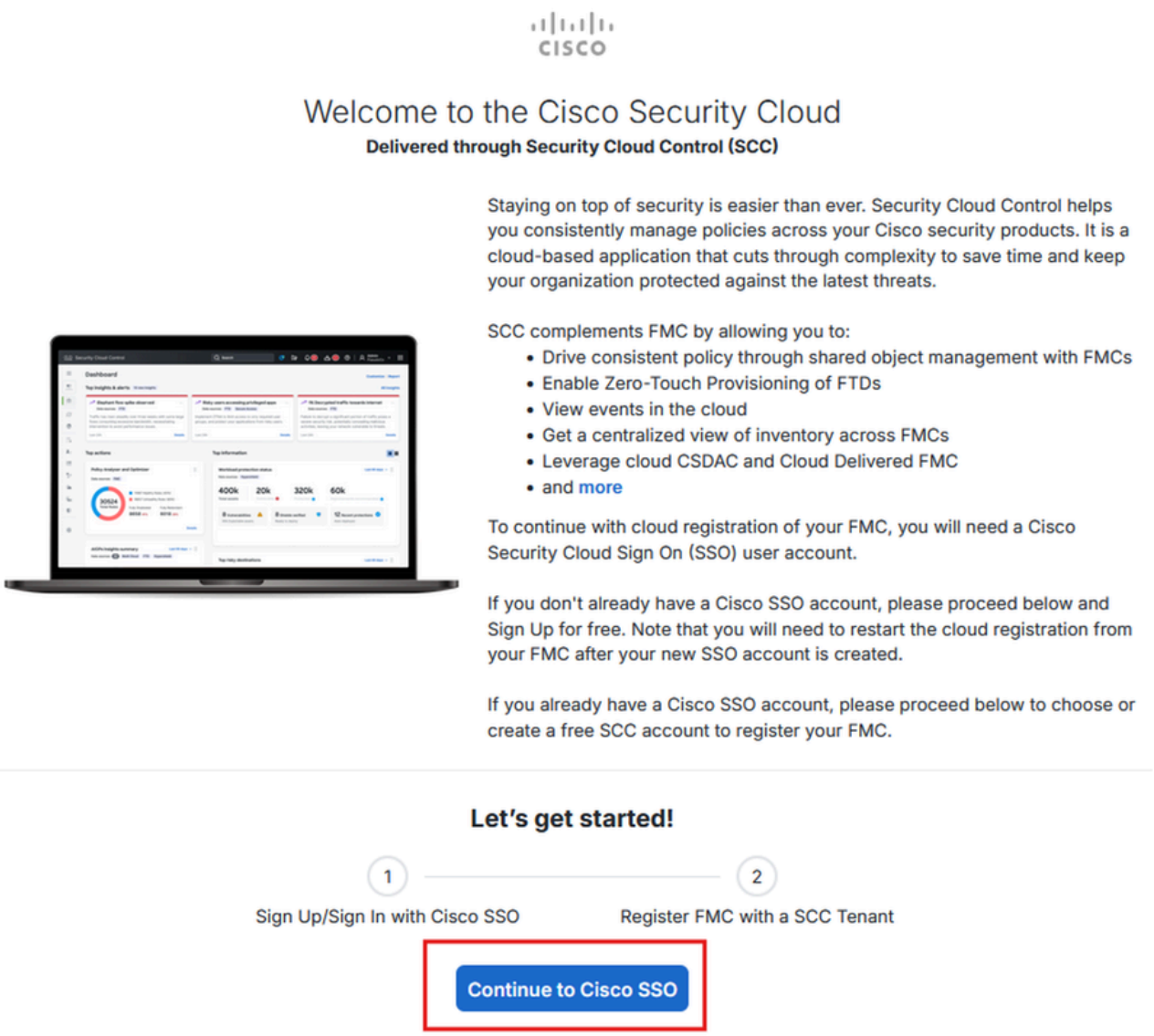


Intégration de Firewall Management Center à SCC

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

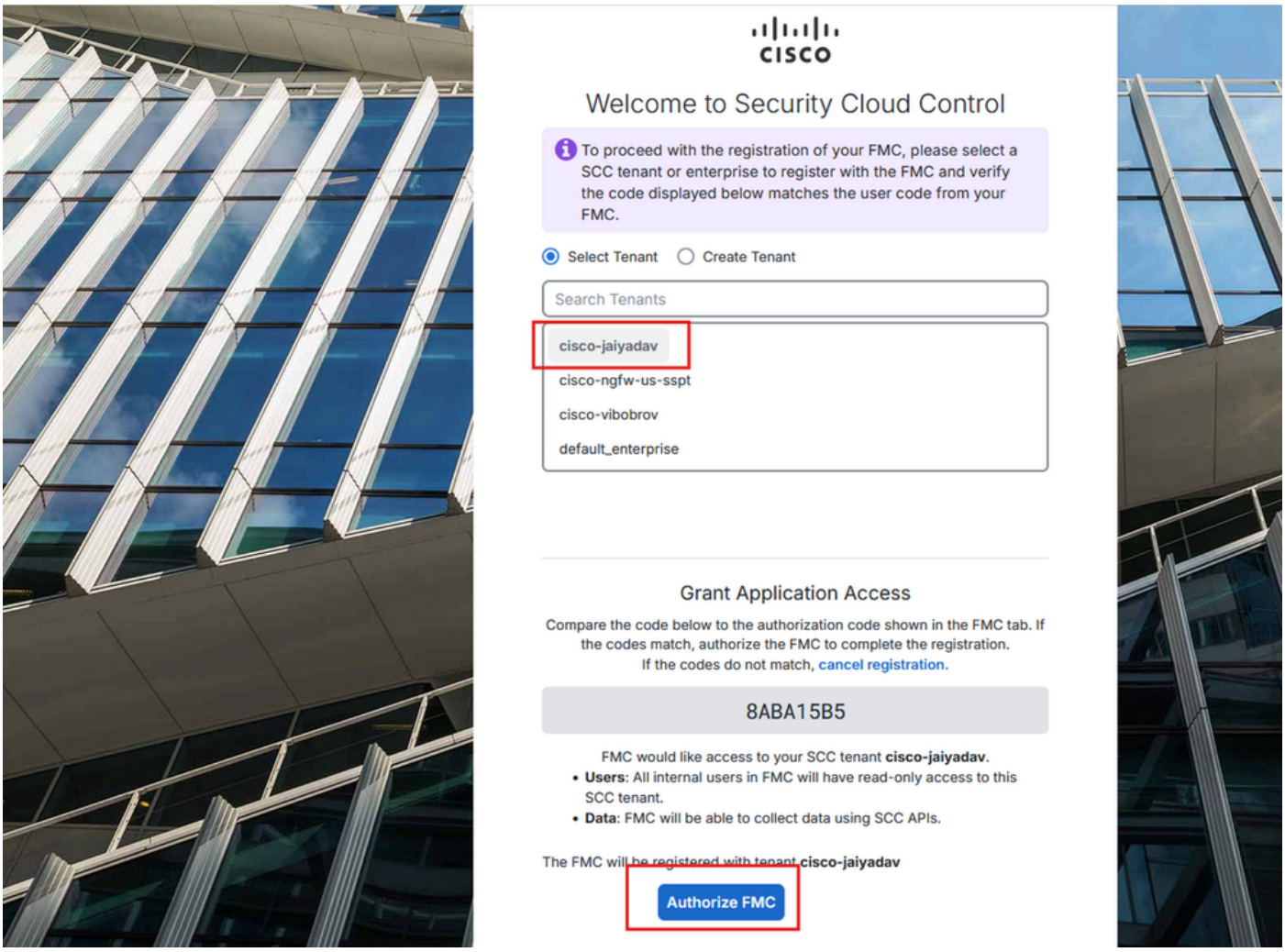
- Cliquez sur Continue to Cisco SSO

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



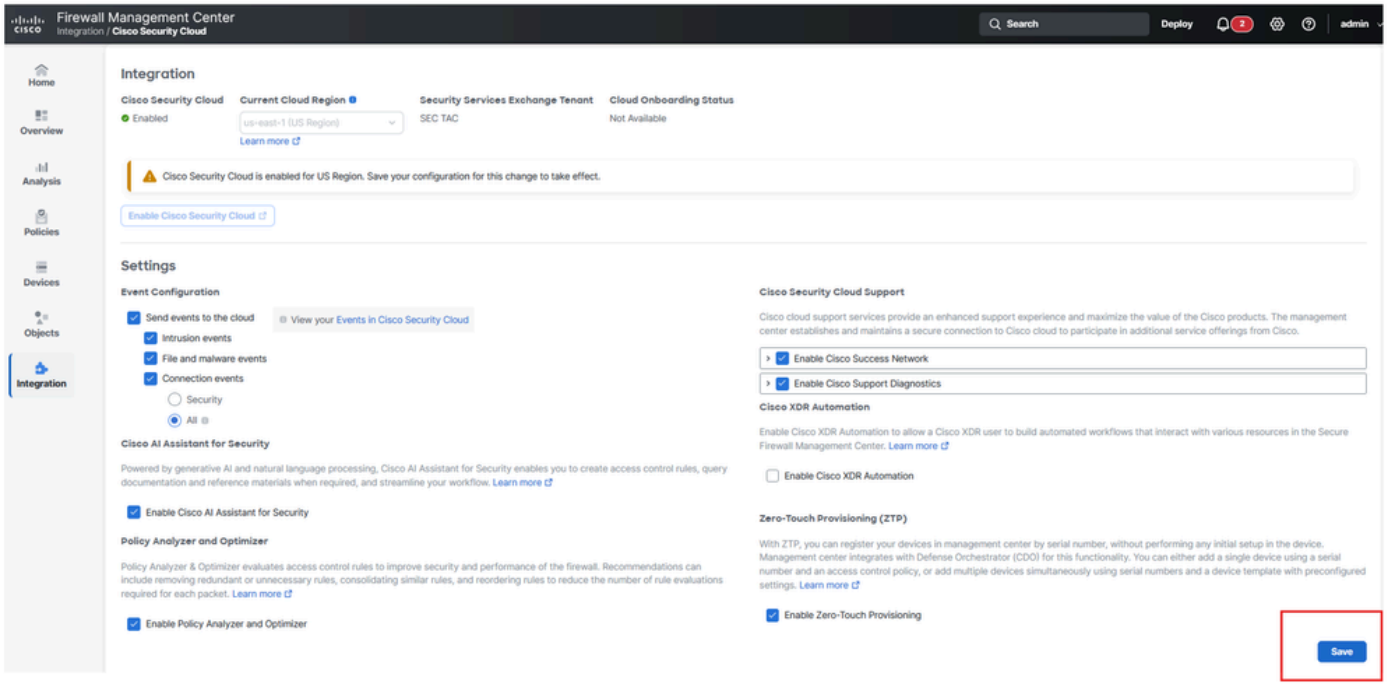
Intégration de Firewall Management Center à SCC

- Choisissez votre client SCC et cliquez sur Authorize FMC



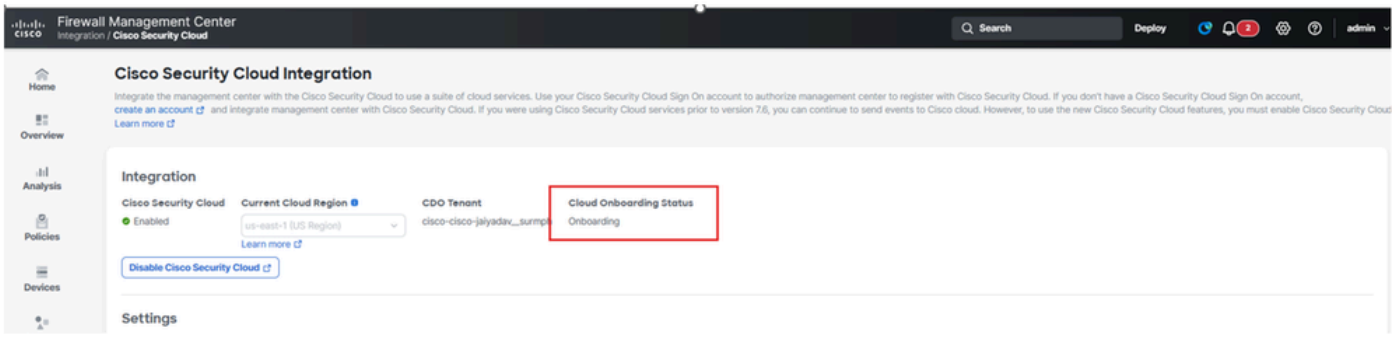
Intégration de Firewall Management Center à SCC

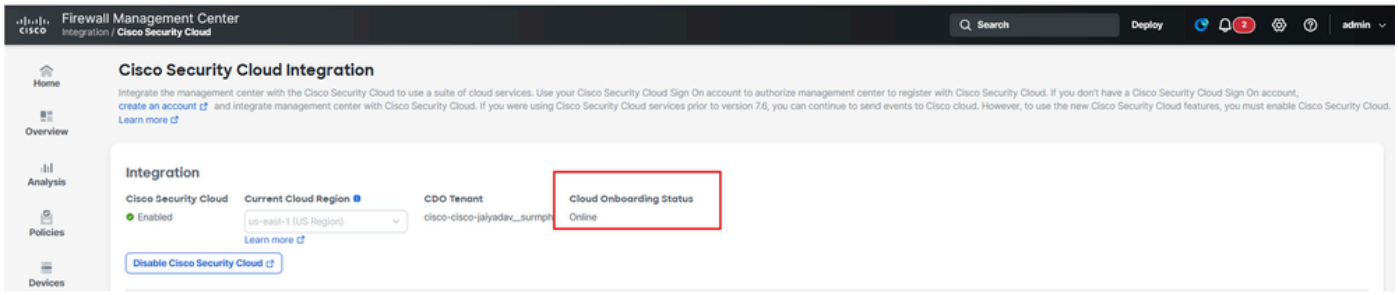
- Cliquez sur Save



Intégration de Firewall Management Center à SCC

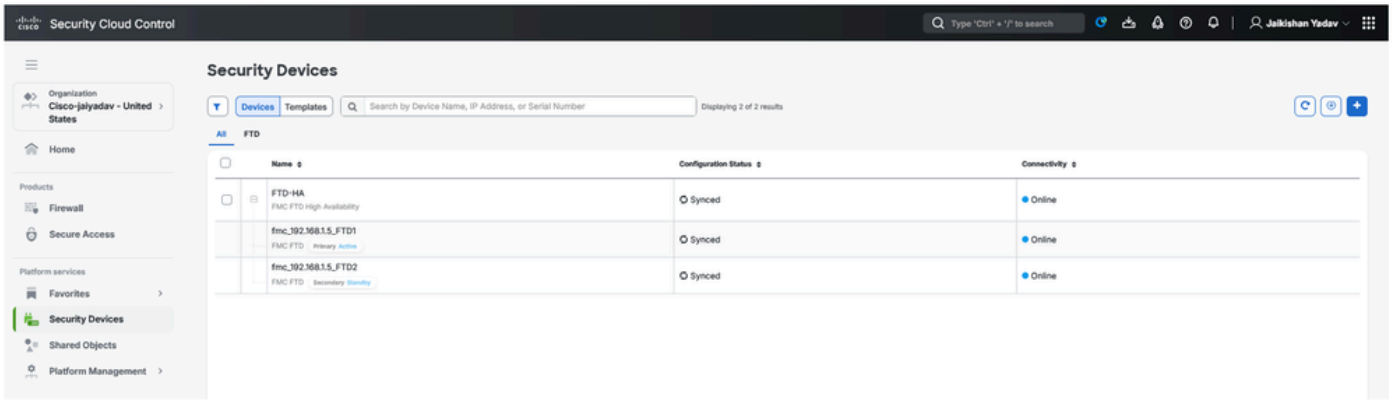
L'état de Cloud Onboarding Status doit passer de **Not Available** à Onboarding , puis Online.





État d'intégration de Firewall Management Center

- Accédez à SCC et vérifiez l'état FTD sousPlatform Services> Security Devices

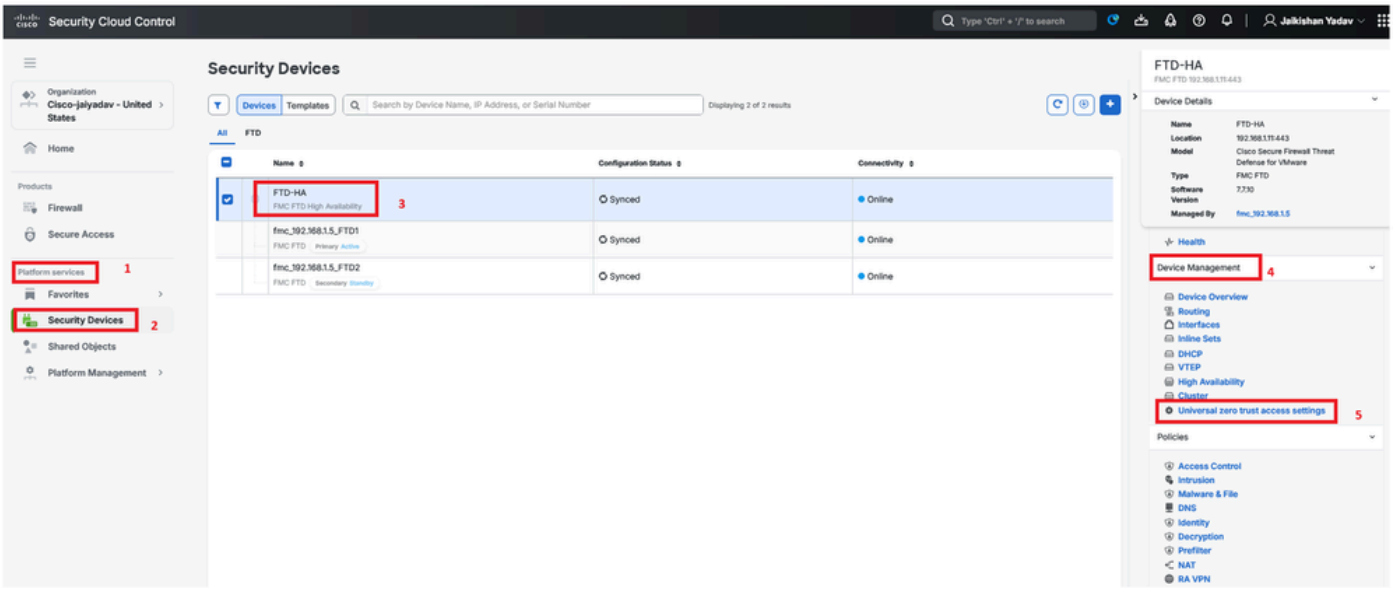


Statut de défense contre les menaces du pare-feu sécurisé sur SCC

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

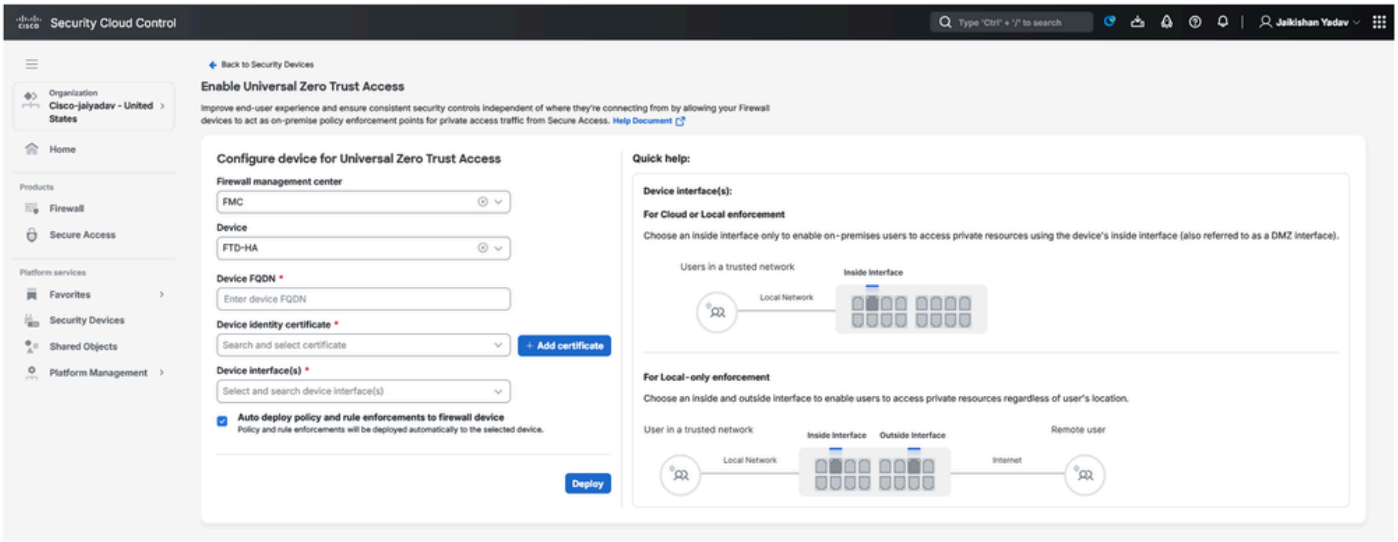
Accédez à SCC :

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

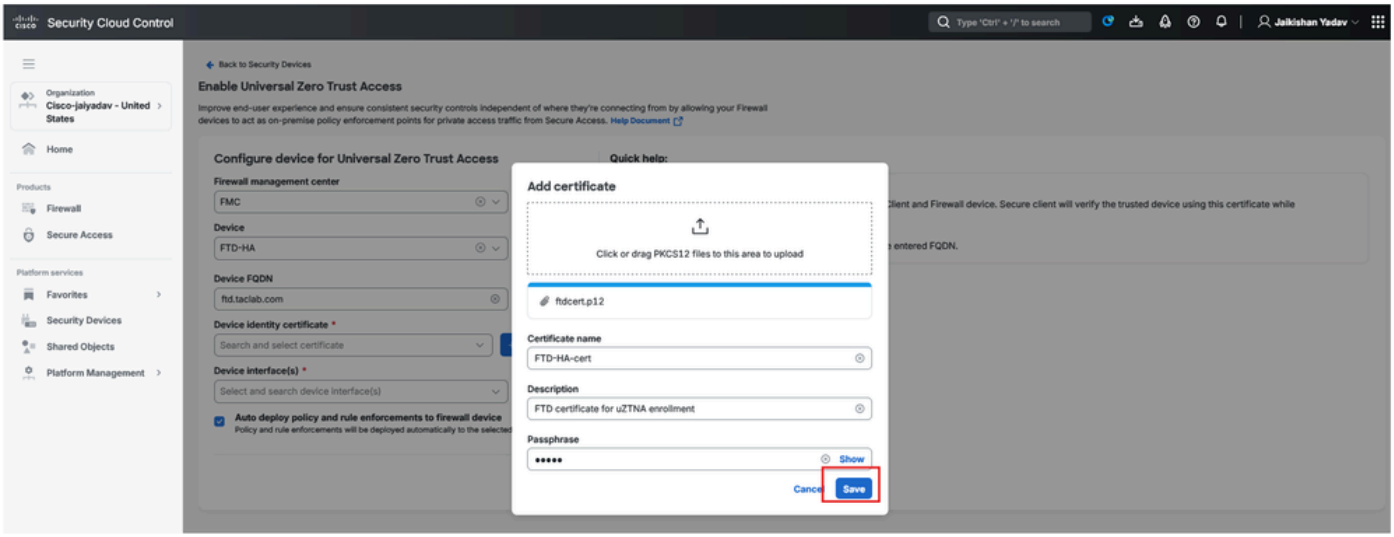


Protection pare-feu sécurisée contre les menaces - Configuration ZTNA universelle

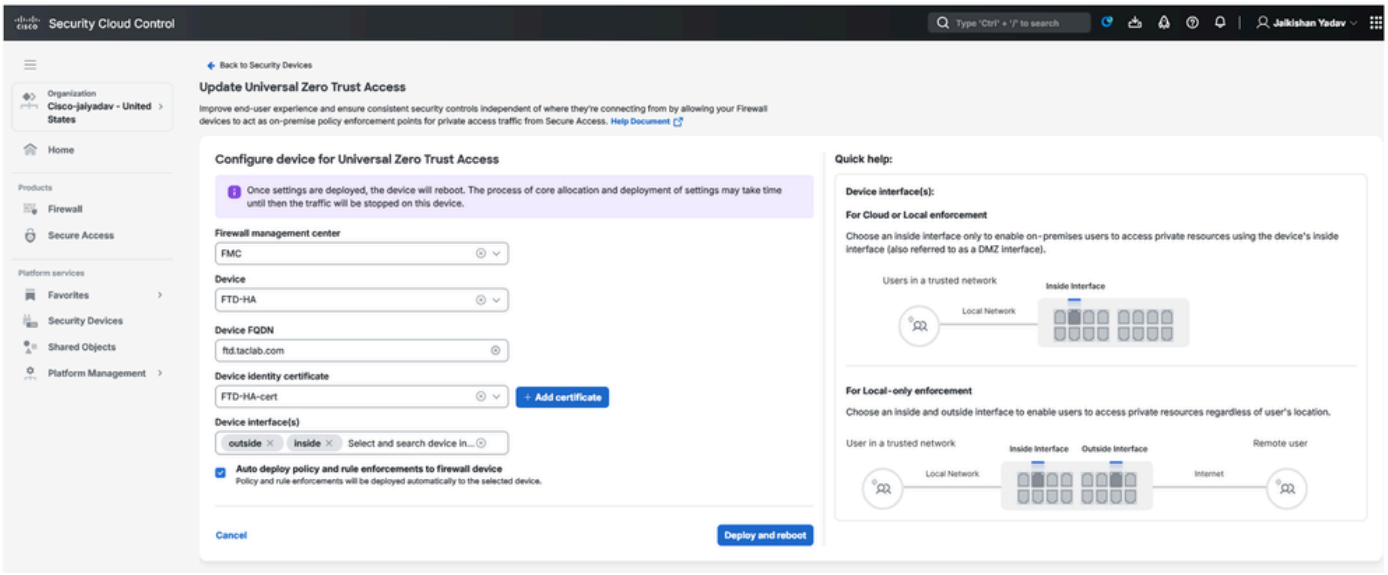
- Remplissez les informations et téléchargez le certificat FTD généré à l'étape [Générer un certificat signé par l'autorité de certification Firewall Threat Defense (FTD)]



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



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

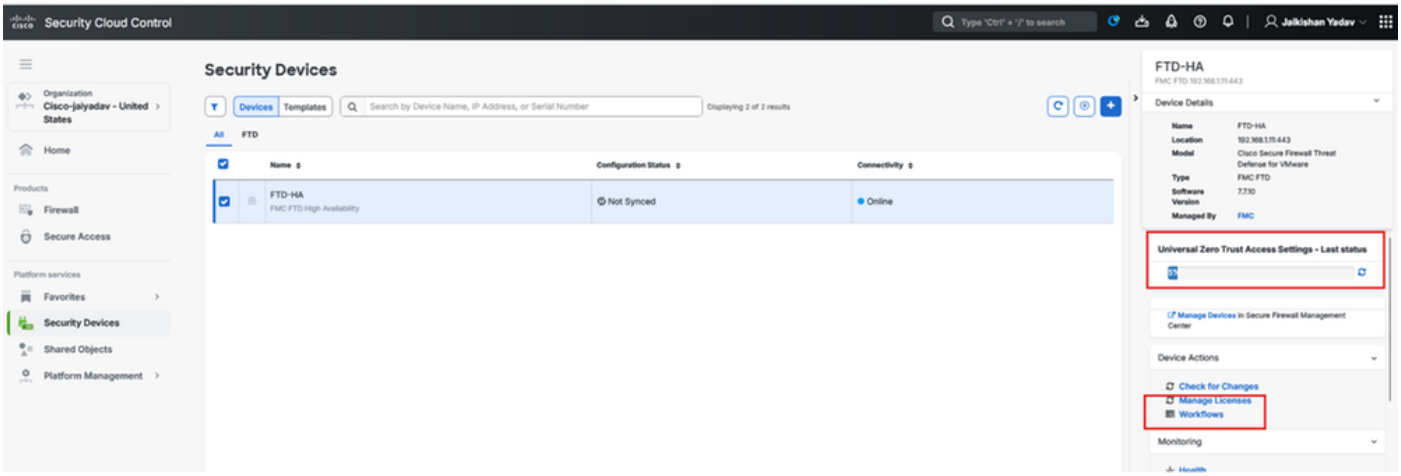


Protection pare-feu sécurisée contre les menaces - Configuration ZTNA universelle

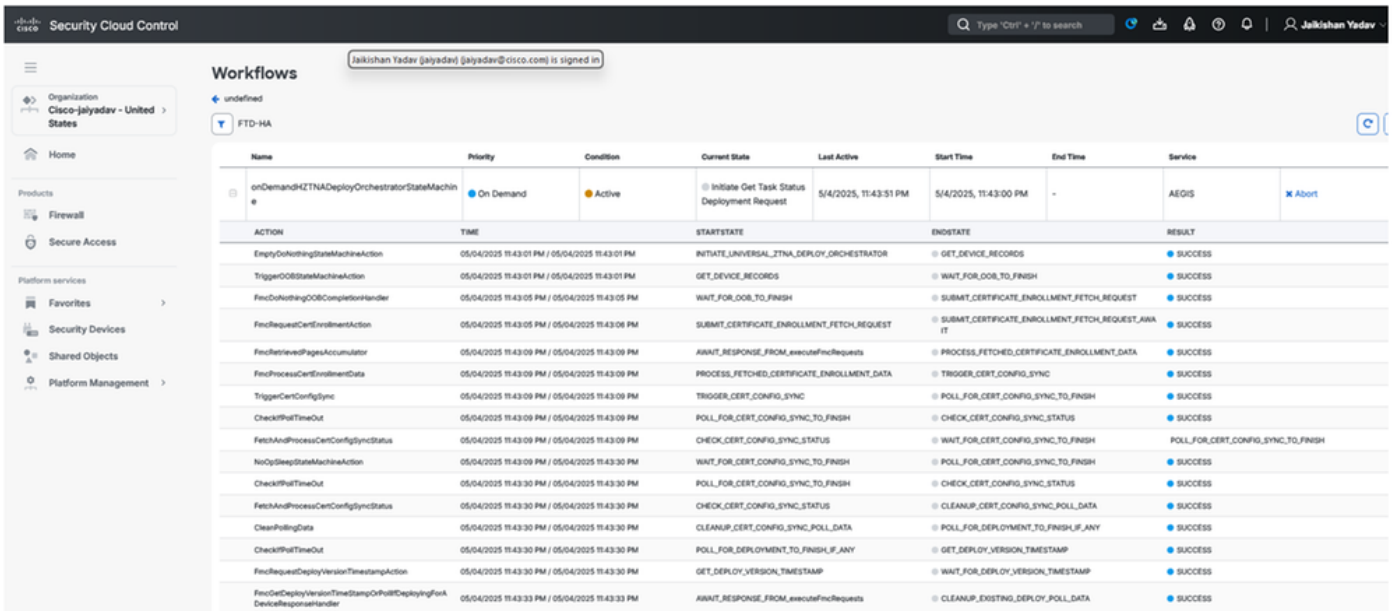
---

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

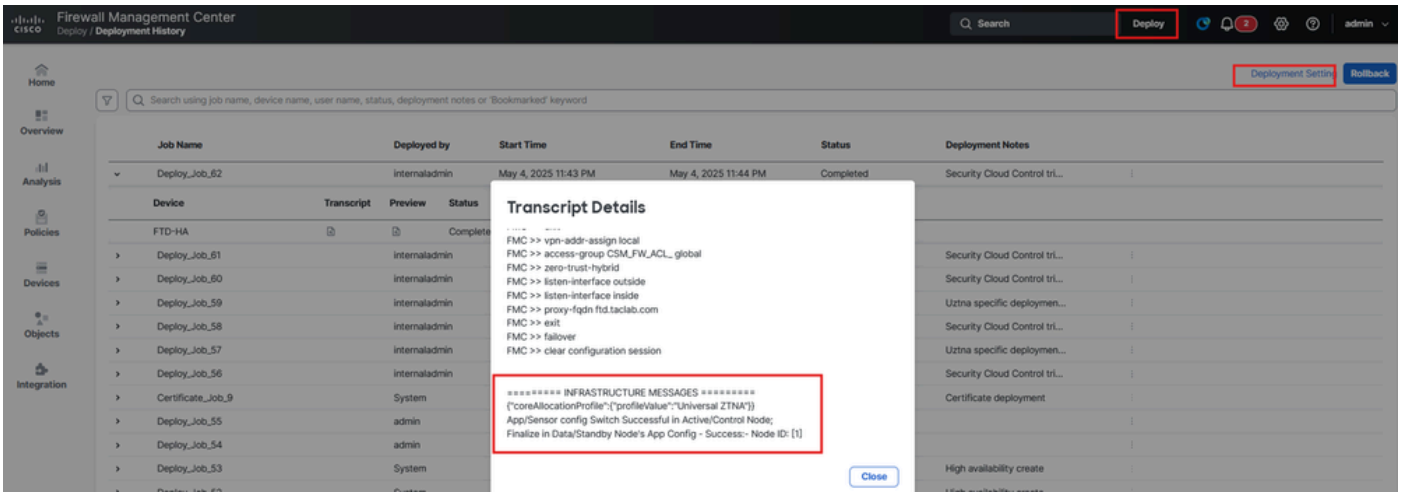


Protection pare-feu sécurisée contre les menaces : état de configuration ZTNA universel



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

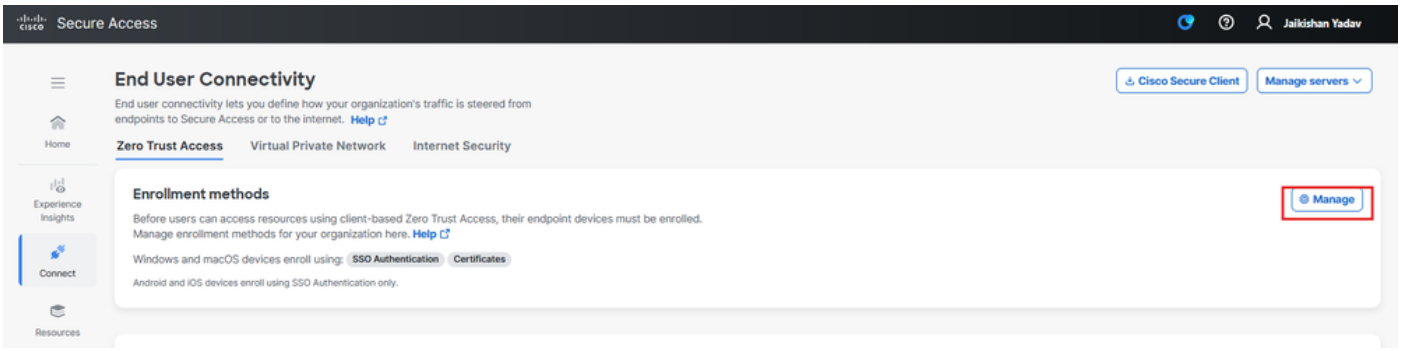
Configuration d'accès sécurisé

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

---

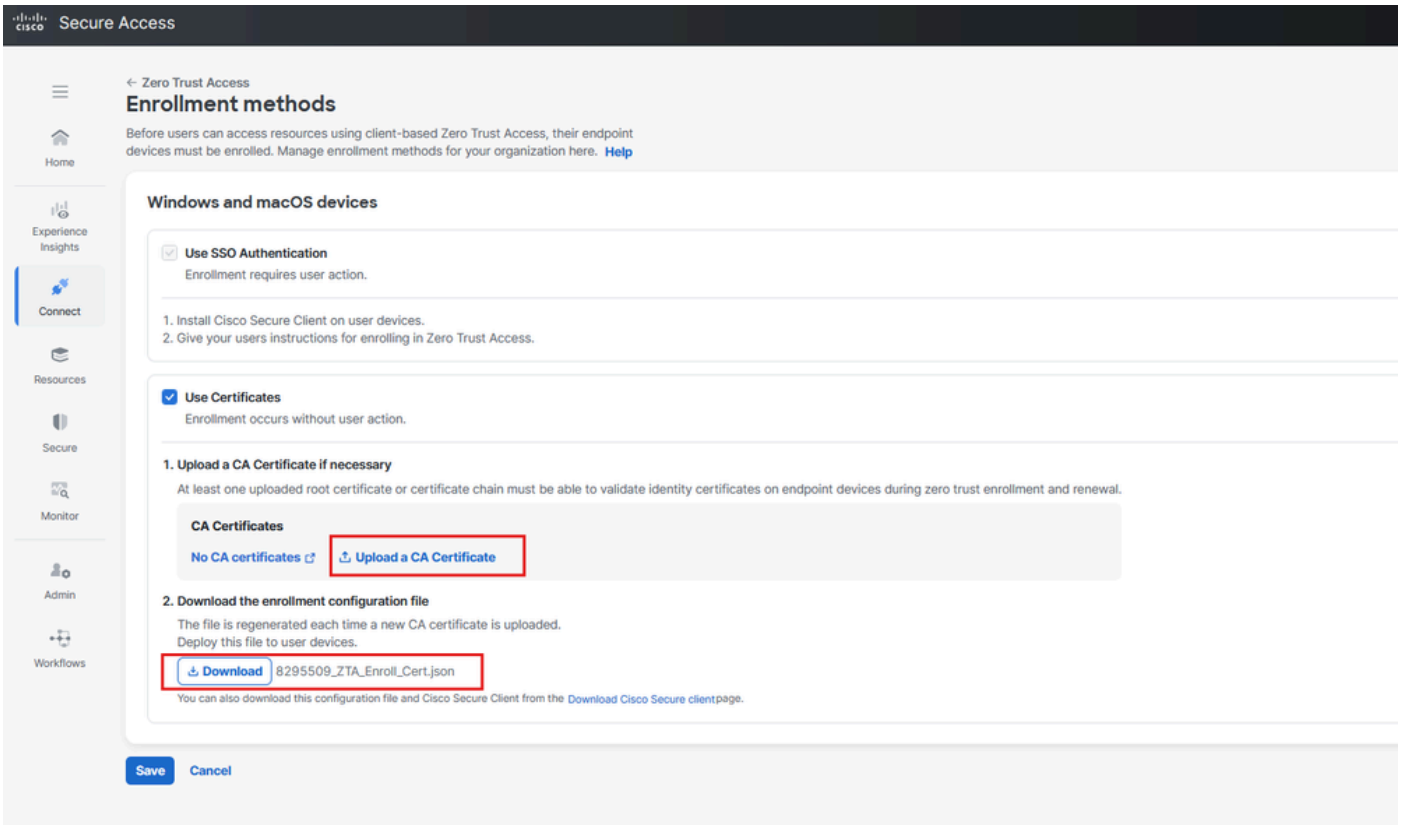
Accédez à Secure Access Dashboard :

- 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

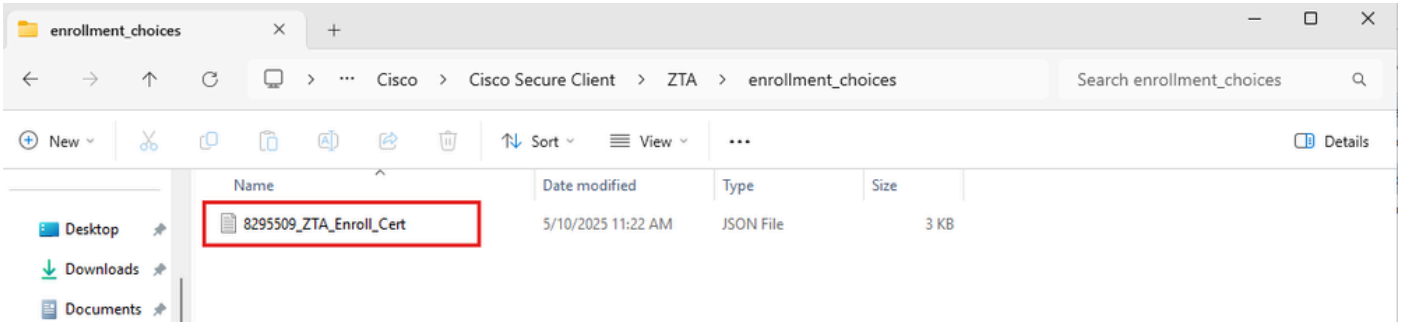


Accès sécurisé - Inscription au certificat ZTA

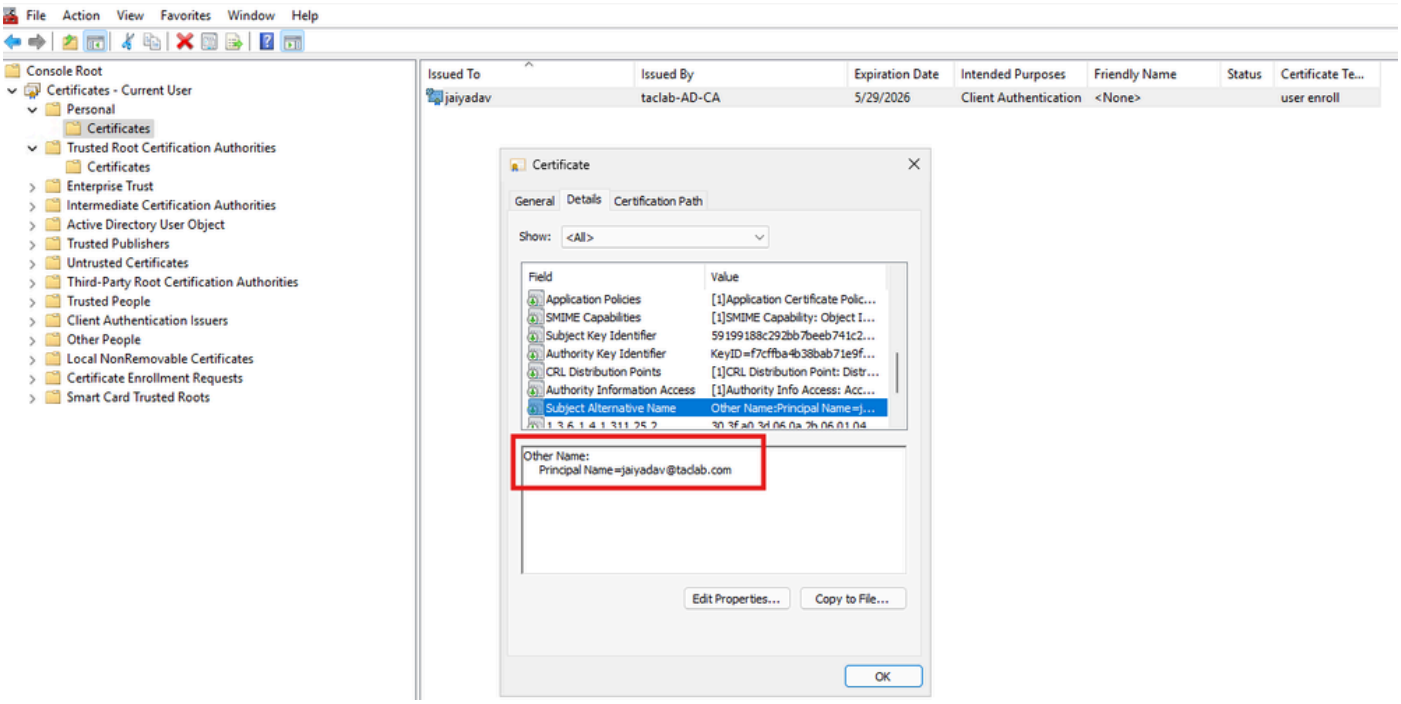
- Cliquez sur Save

Configuration du client

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

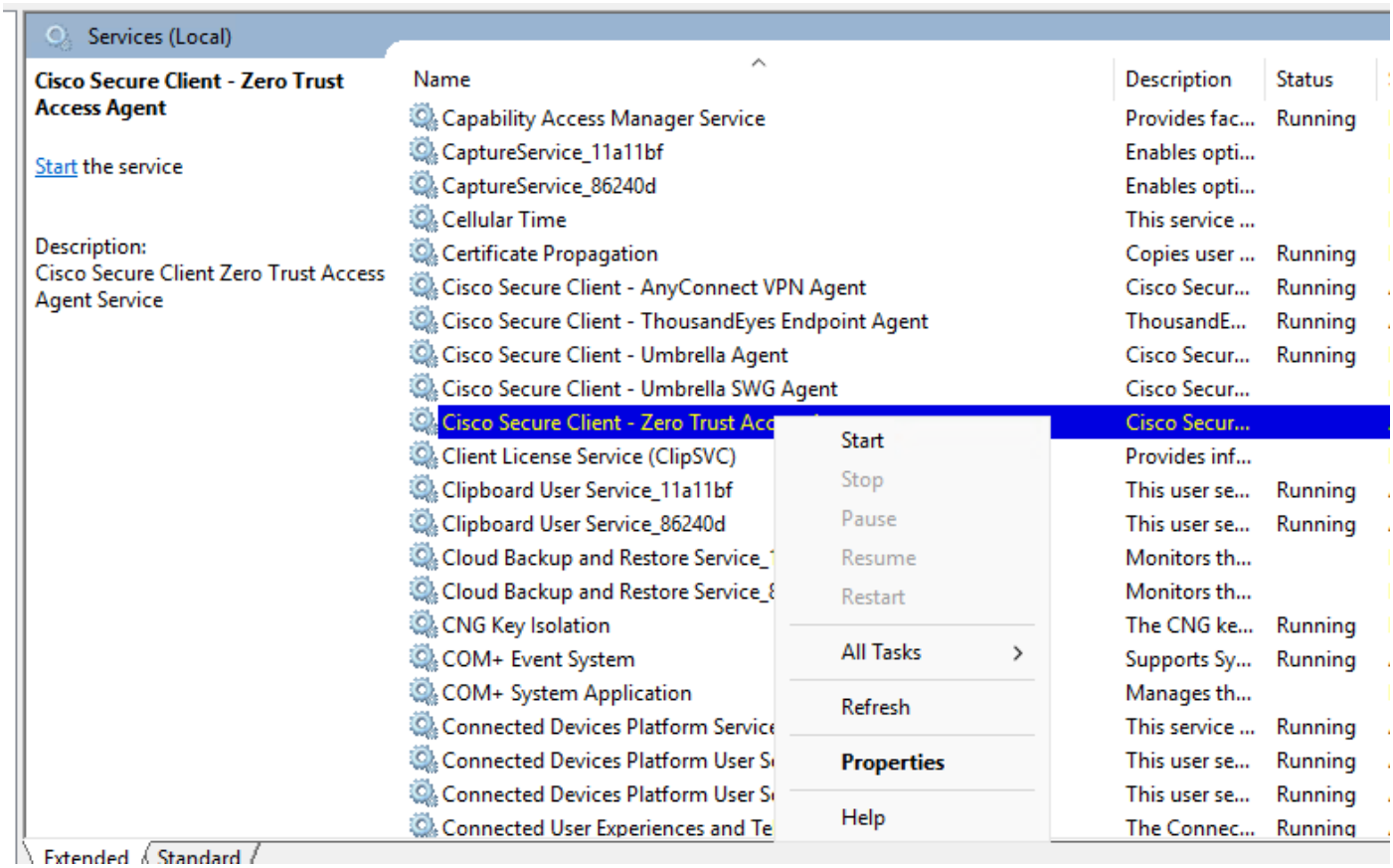


- Créer un certificat client, qui doit avoir un champ UPN dans SAN



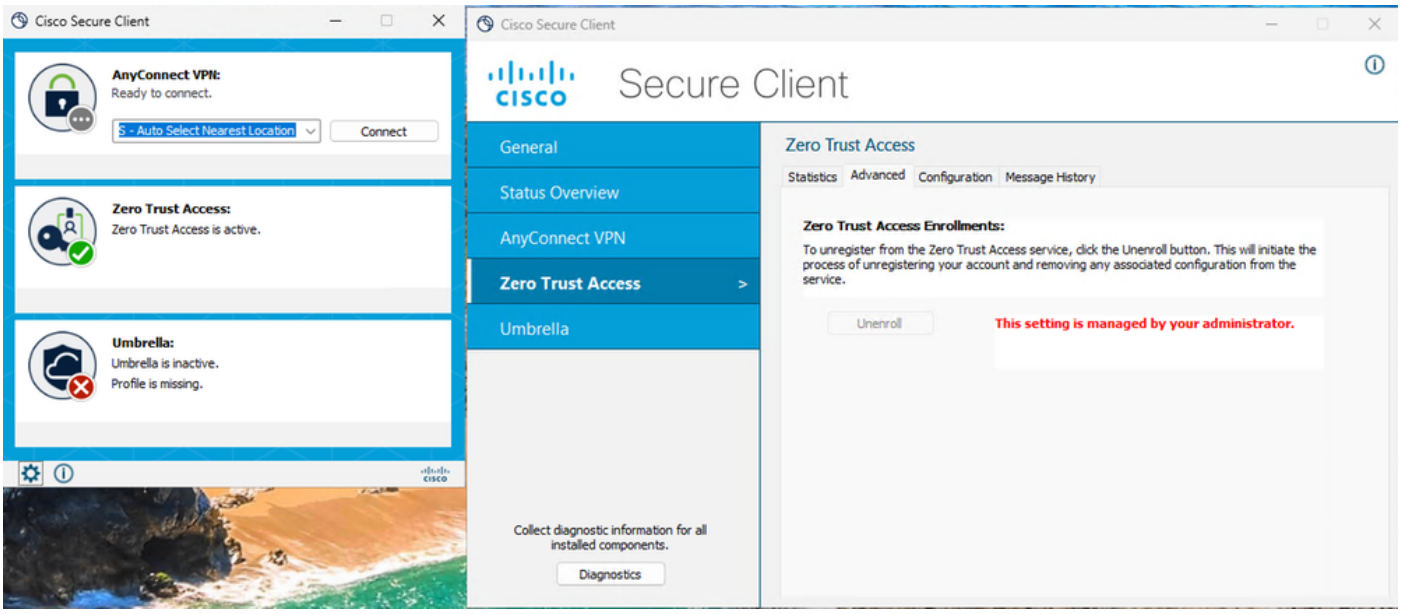
Installation du certificat

- 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.