

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

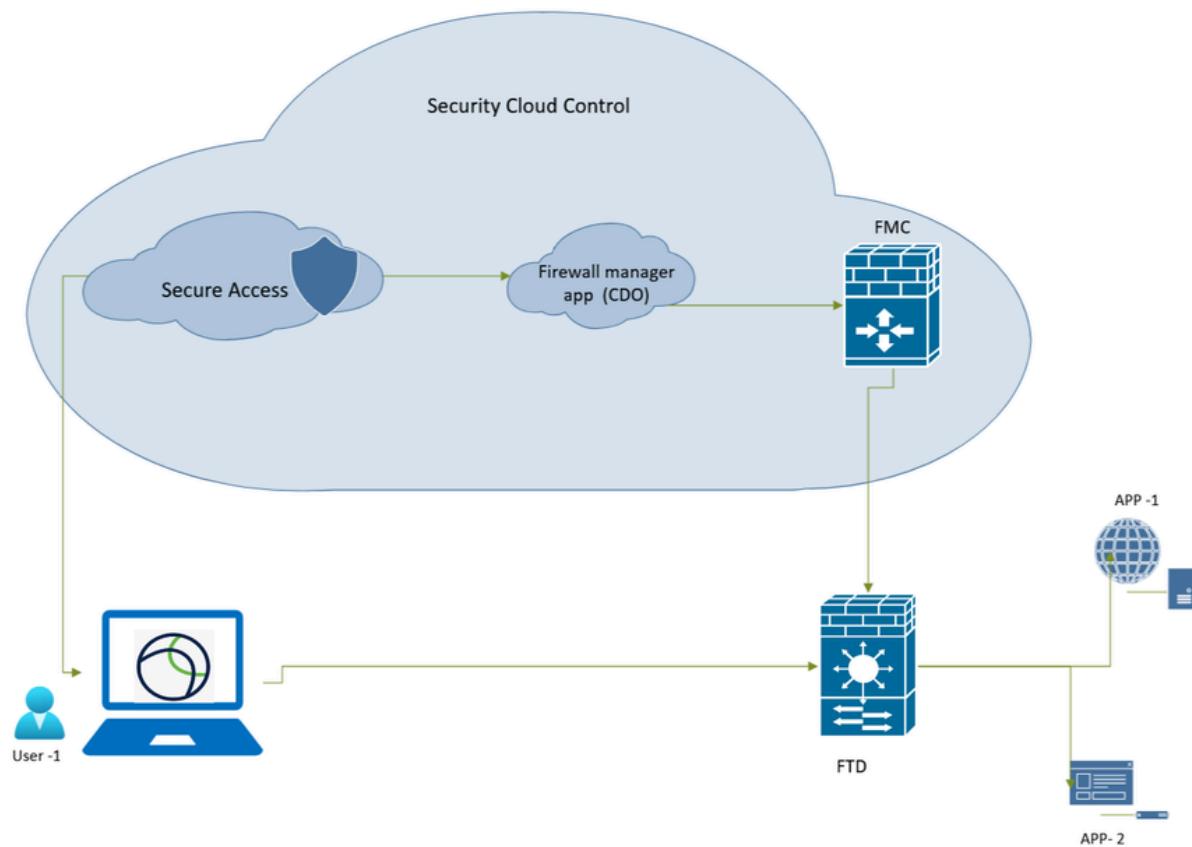
Composants utilisés

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 .

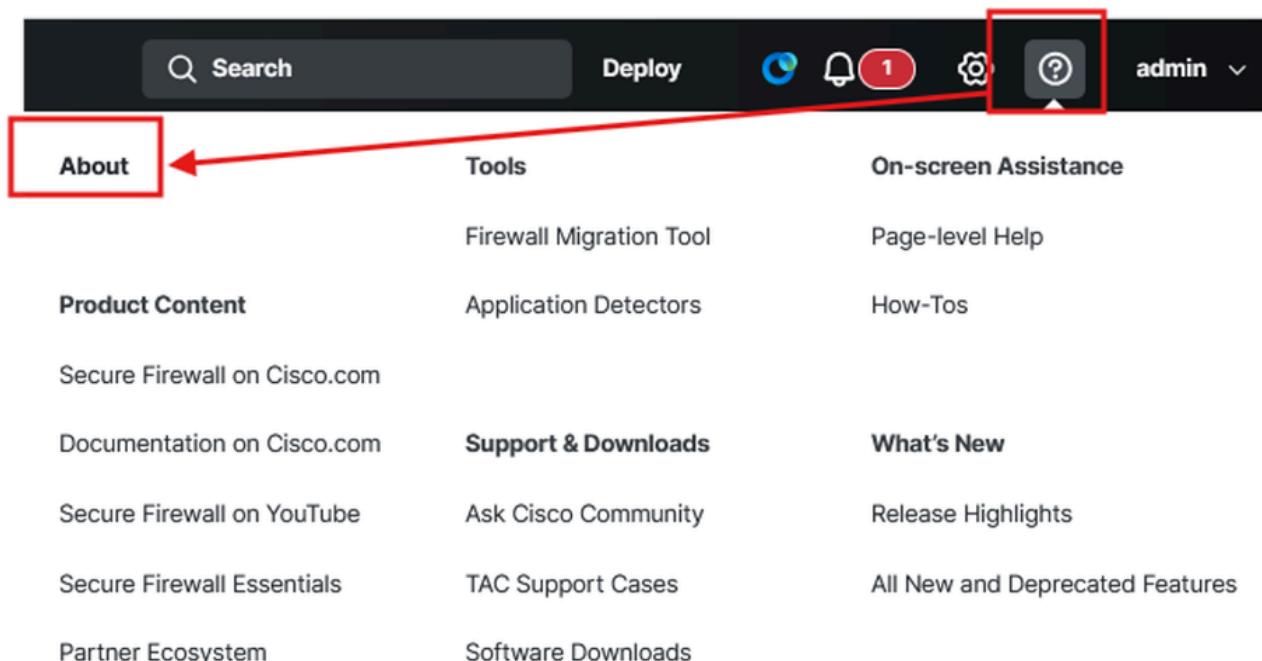
- Les périphériques en cluster ne sont pas pris en charge.
- Les FTD déployés en tant que conteneurs sur les gammes Firepower 4K et 9K ne sont pas pris en charge
- Les sessions ZTNA universelles ne prennent pas en charge les trames jumbo

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	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 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
FTD1(Primary, Active) Snort 3 192.168.1.11 - Routed	Firewall Threat Defense for VMware	7.7.10	N/A	Essentials, IPS (2 more...)	ACP	
FTD2(Secondary, Standby) Snort 3 192.168.1.13 - Routed	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

Health

Monitoring

Users

Monitor

Audit

Domains

Policy

Syslog

Product Upgrades

Events

Statistics

Content Updates

Exclude

Monitor Alerts

Tools

Licenses

Backup/Restore

Smart Licenses

Scheduling

Import/Export

Data Purge

Smart Licenses				
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

Platform Settings	Device Type	Status
Platform,Policy	Threat Defense	Targeting 1 device(s) Up-to-date on all targeted devices

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



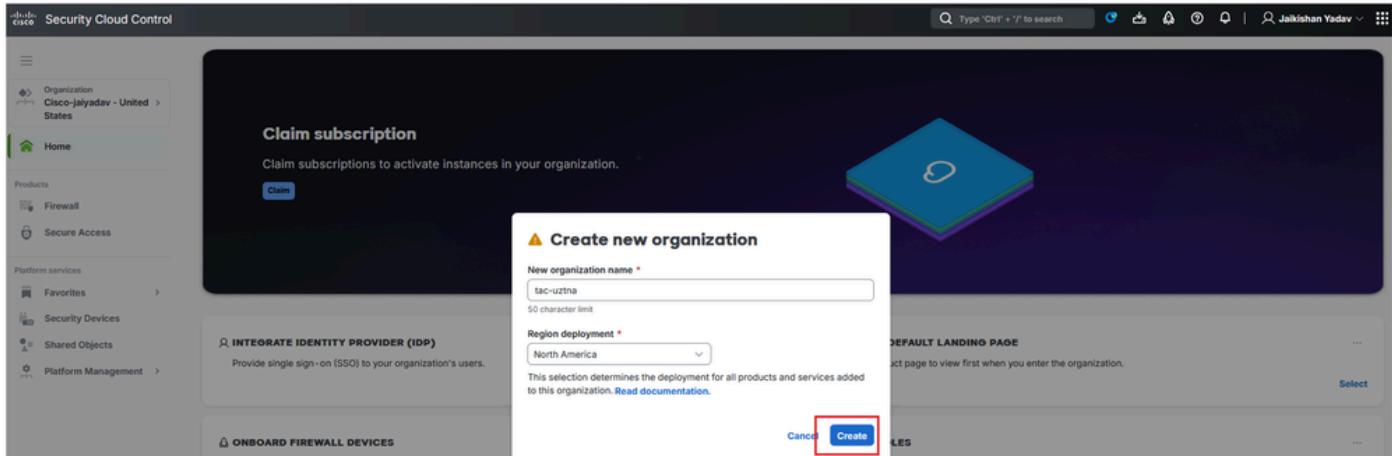
Remarque : Si un service partagé SCC est déjà configuré, vous n'avez pas besoin d'en créer un nouveau.

Accédez à [Security Cloud Control](#) :

- Cliquez 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 **Secure Access** rôles administrateur Security Cloud Control et administrateur.

Security Cloud Control

Administration

- General Settings
- User Management
- Notification Settings

Integrations

- Secure Connectors
- Firewall Management Center
- Multicloud Defense Management

Security Cloud Control

General Settings

- Enable the option to schedule automatic deployments
- Web Analytics
- Auto onboard On-Prem FMCs from Cisco Security Cloud
- Enable event data sharing with Talos

General Settings

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](#).

Tenant ID
cbc

Secure Services Exchange Tenant ID
71

Tenant Name
CI

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 `expert` commande
- 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 :

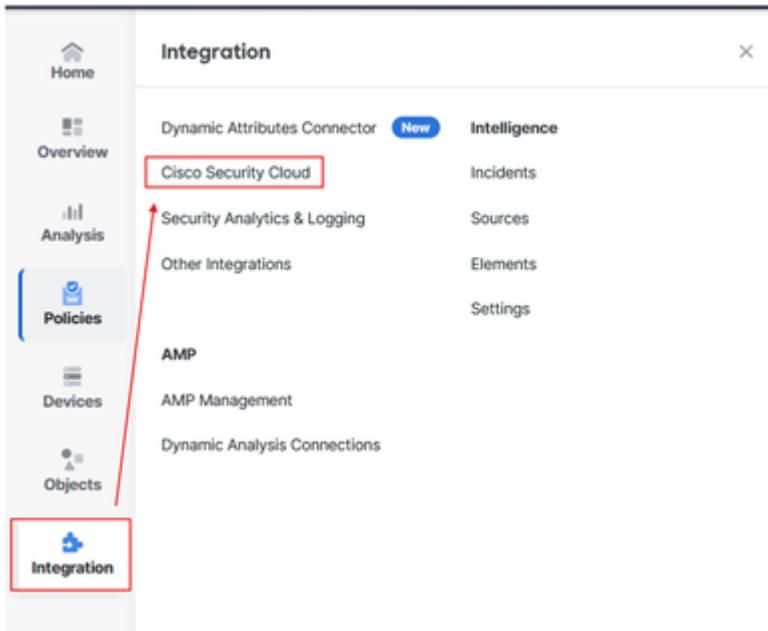
```
openssl pkcs12 -export -out ftdcert.p12 -in cert.crt -inkey cert.key
```

- 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.



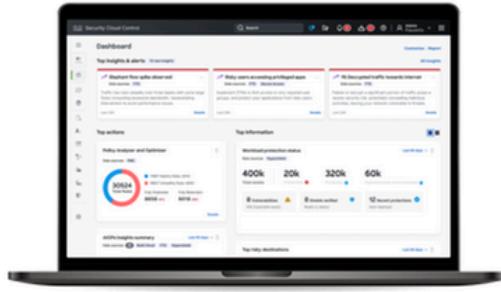
Welcome to the Cisco Security Cloud

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



CISCO

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

Intégration de Firewall Management Center à SCC

- Cliquez sur Save

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 | Learn more

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)

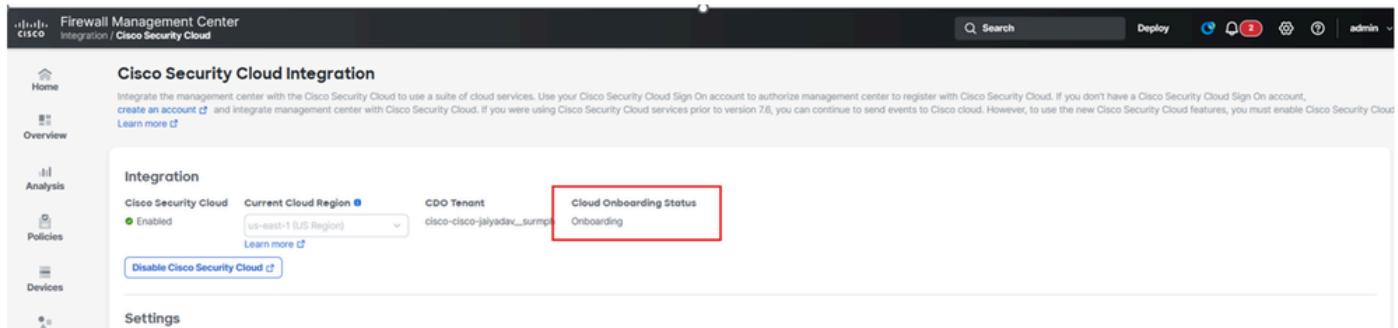
With ZTP, you can register your devices in management center by serial number, without performing any initial setup in the device. Management center integrates with Defense Orchestrator (DCO) for this functionality. You can either add a single device using a serial number and an access control policy,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

Enable Zero-Touch Provisioning

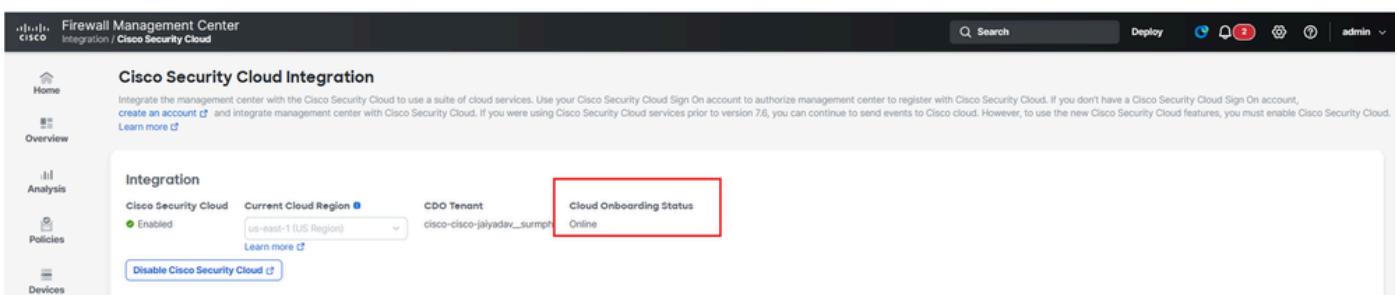
Save

Intégration de Firewall Management Center à SCC

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



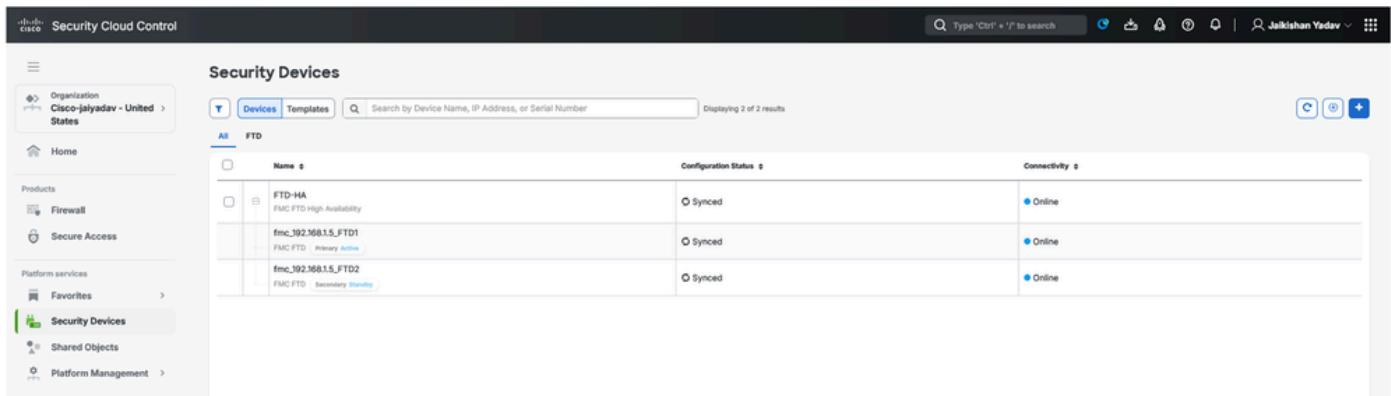
The screenshot shows the 'Cisco Security Cloud Integration' page. The 'Cloud Onboarding Status' field is highlighted with a red box and contains the text 'Onboarding'.



The screenshot shows the 'Cisco Security Cloud Integration' page. The 'Cloud Onboarding Status' field is highlighted with a red box and contains the text 'Online'.

État d'intégration de Firewall Management Center

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



The screenshot shows the 'Security Devices' list in the 'Security Devices' section of the Security Cloud Control interface. The table displays three FTD devices:

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

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](#)

Security Cloud Control

Organization: Cisco-jalyadav - United States

Home

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

Security Devices

Devices, Templates, 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

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 \(FTD\)](#)

Security Cloud Control

Organization: Cisco-jalyadav - 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).

For Local-only enforcement

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

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

Security Devices

Name	Configuration Status	Connectivity
FTD-HA	Not Synced	Online

FTD-HA
FMC FTD High Availability

Device Details

Universal Zero Trust Access Settings - Last status

Device Actions

- Check for Changes
- Manage Licenses
- Workflows

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

Name	Priority	Condition	Current State	Last Active	Start Time	End Time	Service
onDemandZTNADeployOrchestratorStateMachine	On Demand	Active	Initiate Get Task Status Deployment Request	5/4/2025, 11:43:51 PM	5/4/2025, 11:43:00 PM	-	AEGIS
ACTION	TIME	STARTSTATE	ENDSTATE	RESULT			
EmptyOnNothingStateMachineAction	05/04/2025 11:43:01 PM / 05/04/2025 11:43:01 PM	INITIATE_UNIVERSAL_ZTNA_DEPLOY_ORCHESTRATOR	GET_DEVICE_RECORDS	SUCCESS			
TriggerCertMachineAction	05/04/2025 11:43:01 PM / 05/04/2025 11:43:01 PM	GET_DEVICE_RECORDS	WAIT_FOR_OOB_TO_FINISH	SUCCESS			
FmcOnNothingOobCompletionHandler	05/04/2025 11:43:05 PM / 05/04/2025 11:43:05 PM	WAIT_FOR_OOB_TO_FINISH	SUBMIT_CERTIFICATE_ENROLLMENT_FETCH_REQUEST	SUCCESS			
FmcRequestCertEnrollmentAction	05/04/2025 11:43:05 PM / 05/04/2025 11:43:06 PM	SUBMIT_CERTIFICATE_ENROLLMENT_FETCH_REQUEST	SUBMIT_CERTIFICATE_ENROLLMENT_FETCH_REQUEST_WAIT	SUCCESS			
FmcRetrieveDpssAccumulator	05/04/2025 11:43:09 PM / 05/04/2025 11:43:09 PM	AWAIT_RESPONSE_FROM_EXECUTE_INCHIEQUESTS	PROCESS_FETCHED_CERTIFICATE_ENROLLMENT_DATA	SUCCESS			
FmcProcessCertEnrollmentData	05/04/2025 11:43:09 PM / 05/04/2025 11:43:09 PM	PROCESS_FETCHED_CERTIFICATE_ENROLLMENT_DATA	TRIGGER_CERT_CONFIG_SYNC	SUCCESS			
TriggerCertConfigSync	05/04/2025 11:43:09 PM / 05/04/2025 11:43:09 PM	TRIGGER_CERT_CONFIG_SYNC	POLL_FOR_CERT_CONFIG_SYNC_TO_FINISH	SUCCESS			
CheckPollTimeOut	05/04/2025 11:43:09 PM / 05/04/2025 11:43:09 PM	POLL_FOR_CERT_CONFIG_SYNC_TO_FINISH	CHECK_CERT_CONFIG_SYNC_STATUS	SUCCESS			
FetchAndProcessCertConfigSyncStatus	05/04/2025 11:43:09 PM / 05/04/2025 11:43:09 PM	CHECK_CERT_CONFIG_SYNC_STATUS	WAIT_FOR_CERT_CONFIG_SYNC_TO_FINISH	POLL_FOR_CERT_CONFIG_SYNC_TO_FINISH			
NoOpSleepMachineAction	05/04/2025 11:43:09 PM / 05/04/2025 11:43:30 PM	WAIT_FOR_CERT_CONFIG_SYNC_TO_FINISH	POLL_FOR_CERT_CONFIG_SYNC_TO_FINISH	SUCCESS			
CheckPollTimeOut	05/04/2025 11:43:30 PM / 05/04/2025 11:43:30 PM	POLL_FOR_CERT_CONFIG_SYNC_TO_FINISH	CHECK_CERT_CONFIG_SYNC_STATUS	SUCCESS			
FetchAndProcessCertConfigSyncStatus	05/04/2025 11:43:30 PM / 05/04/2025 11:43:30 PM	CHECK_CERT_CONFIG_SYNC_STATUS	CLEANUP_CERT_CONFIG_SYNC_POLL_DATA	SUCCESS			
CleanPollingData	05/04/2025 11:43:30 PM / 05/04/2025 11:43:30 PM	CLEANUP_CERT_CONFIG_SYNC_POLL_DATA	POLL_FOR_DEPLOYMENT_TO_FINISH_IF_ANY	SUCCESS			
CheckPollTimeOut	05/04/2025 11:43:30 PM / 05/04/2025 11:43:30 PM	POLL_FOR_DEPLOYMENT_TO_FINISH_IF_ANY	GET_DEPLOY_VERSION_TIMESTAMP	SUCCESS			
FmcRequestDeployVersionTimestampAction	05/04/2025 11:43:30 PM / 05/04/2025 11:43:30 PM	GET_DEPLOY_VERSION_TIMESTAMP	WAIT_FOR_DEPLOY_VERSION_TIMESTAMP	SUCCESS			
FmcGetDeployVersionTimestampOrPollIfDeployingForADeviceResponseHandler	05/04/2025 11:43:33 PM / 05/04/2025 11:43:33 PM	AWAIT_RESPONSE_FROM_EXECUTE_INCHIEQUESTS	CLEANUP_EXISTING_DEPLOY_POLL_DATA	SUCCESS			

Flux de travail de contrôle cloud de sécurité

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

Job Name	Deployed by	Start Time	End Time	Status	Deployment Notes
Deploy_Job_62	internaladmin	May 4, 2025 11:43:44 PM	May 4, 2025 11:44:00 PM	Completed	Security Cloud Control tri...
FTD-HA	Transcript	Complete			
Deploy_Job_61	internaladmin				Security Cloud Control tri...
Deploy_Job_60	internaladmin				Security Cloud Control tri...
Deploy_Job_59	internaladmin				Uztna specific deploymen...
Deploy_Job_58	internaladmin				Security Cloud Control tri...
Deploy_Job_57	internaladmin				Uztna specific deploymen...
Deploy_Job_56	internaladmin				Security Cloud Control tri...
Certificate_Job_9	System				Certificate deployment
Deploy_Job_55	admin				
Deploy_Job_54	admin				
Deploy_Job_53	System				High availability create

Transcript Details

```
=====
INFRASTRUCTURE MESSAGES =====
("coreAllocationProfile","profileValue":"Universal ZTNA")
App/Sensor config Switch Successful in Active/Control Node;
Finalize in Data/Standby Node's App Config - Success- Node ID: [1]
```

Secure Firewall Management Center - État du déploiement des politiques

Inscrire le client avec ZuTNA

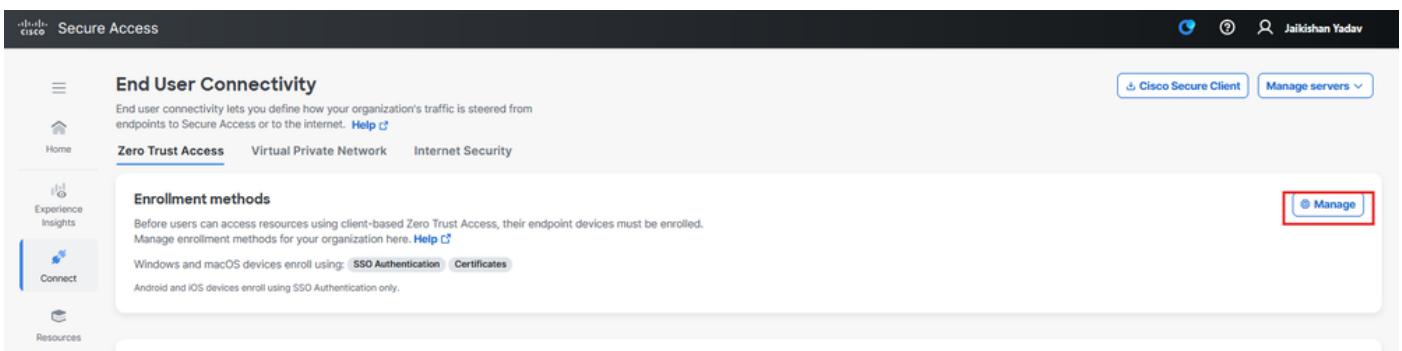
Configuration d'accès sécurisé



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



The screenshot shows the Cisco Secure Access dashboard with the 'End User Connectivity' section selected. Under 'Zero Trust Access', the 'Enrollment methods' section is visible. A red box highlights the 'Manage' button in the top right corner of this section. The dashboard also includes a navigation bar with 'Cisco Secure Client' and 'Manage servers' buttons.

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](#)

 Home

 Experience Insights

 Connect

 Resources

 Secure

 Monitor

 Admin

 Workflows

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 

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.

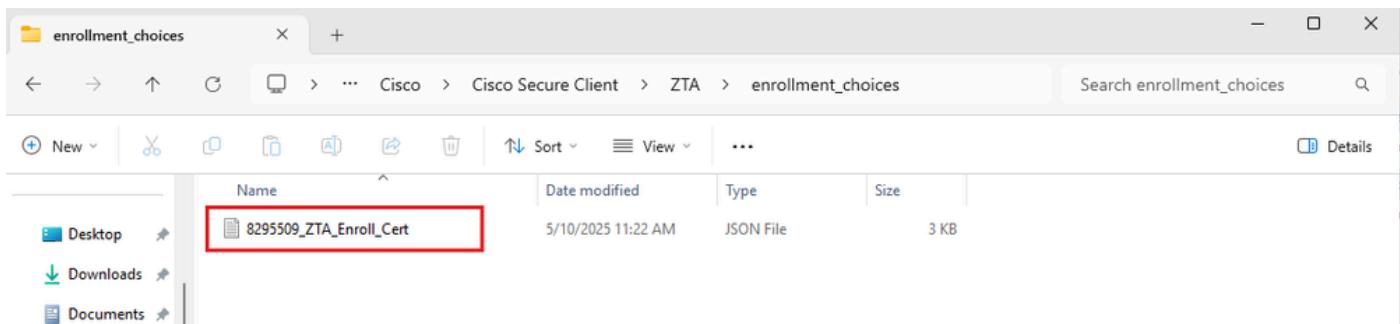
[Save](#) [Cancel](#)

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



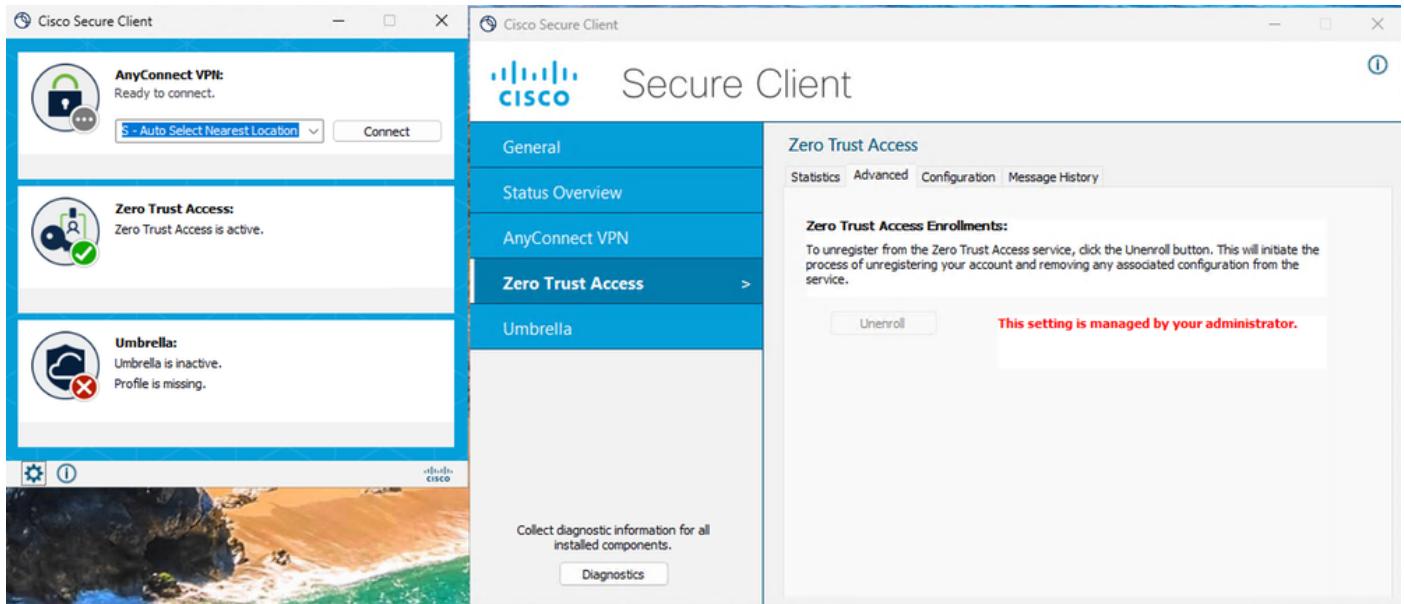
- Créer un certificat client, qui doit avoir un champ UPN dans SAN

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.