

Configurazione dell'accesso sicuro per Universal ZTNA con FMC gestito in locale su SCC

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Esempio di rete](#)

[Informazioni sulle parentesi](#)

[Dispositivi supportati](#)

[Limitazioni](#)

[Configurazione](#)

[Verifica versione FMC](#)

[Verifica versione FTD](#)

[Verifica licenze FTD](#)

[Verificare le impostazioni della piattaforma e il DNS configurato correttamente](#)

[Crea un tenant di controllo del cloud di sicurezza su CDO](#)

[Verificare che le impostazioni generali di SCC Firewall siano configurate](#)

[Verificare l'integrazione di Secure Access Tenant e Security Control Firewall Management Base](#)

[Genera certificato firmato CA Firewall Threat Defense \(FTD\)](#)

[Centro gestione firewall locale integrato per Security Cloud Control](#)

[Registra impostazioni Universal Zero Trust Network Access \(uZTNA\) su FTD](#)

[Registrare il client con uZTNA](#)

[Configurazione accesso sicuro](#)

[Configurazione client](#)

[Verifica](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare Universal ZTNA con Secure Access e FTD virtuale gestiti da un FMC virtuale locale.

Prerequisiti

- È necessario installare Firewall Management Center (FMC) e Firewall Threat Defense (FTD) utilizzando la versione software 7.7.10 o successiva.
- Firewall Threat Defense (FTD) deve essere gestito dal Centro gestione firewall
- Firewall Threat Defense (FTD) deve essere concesso in licenza con crittografia (la

crittografia avanzata deve essere abilitata con la funzionalità di esportazione abilitata), licenze IPS e Threat necessarie per i controlli di sicurezza

- La configurazione di base di Firewall Threat Defense (FTD) deve essere eseguita da Firewall Management Center (FMC), ad esempio interfaccia, routing e così via.
- Per risolvere il nome di dominio completo dell'app, è necessario applicare la configurazione DNS nel dispositivo dal FMC
- La versione di Cisco Secure Client deve essere 5.1.10 o successiva
- Il controllo del cloud di sicurezza è fornito ai clienti con i flag delle microapplicazioni firewall e Secure Access e delle funzionalità UZTNA abilitati

Requisiti

- Tutti i dispositivi Secure Firewall Management Center (FMC), inclusi cdFMC e Firewall Threat Defense (FTD), devono eseguire il software versione 7.7.10 o successive.
- Firewall Threat Defense (FTD) deve essere gestito da Firewall Management Center; local manager Firewall Defense Manager (FDM) non è supportato
- Tutti i dispositivi Firewall Threat Defense (FTD) devono essere configurati per la modalità routing; modalità trasparente non supportata.
- I dispositivi del cluster non sono supportati.
- sono supportati dispositivi ad alta disponibilità (HA); vengono visualizzati come un'unica entità.
- Secure Client versione 5.1.10 o successive

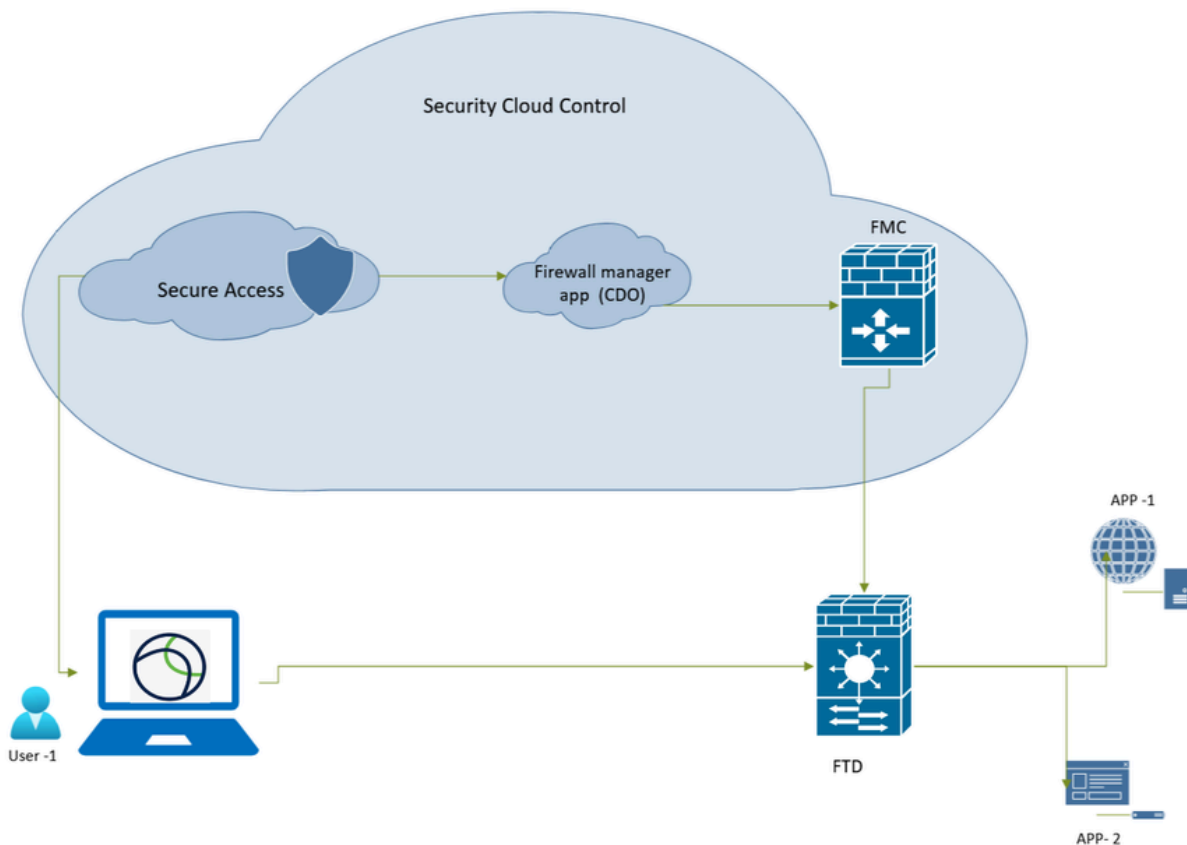
Componenti usati

Le informazioni di questo documento si basano

- Security Cloud Control (SCC)
- Secure Firewall Management Center (FMC) versione 7.7.10
- Virtual Secure Firewall Threat Defense (FTD) -100 versione 7.7.10
- Secure Client per Windows versione 5.1.10
- Accesso sicuro

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Esempio di rete



Accesso sicuro - Topologia di rete

Informazioni sulle parentesi

Dispositivi supportati

Modelli supportati di difesa dalle minacce Secure Firewall:

- FPR 1150
- FPR 3105, 3110,3120,3130,3140
- FPR4115,4125,4145,4112
- FPR4215,4225,4245
- Virtuale Firewall Threat Defense (FTD) con almeno 16 core CPU

Limitazioni

- Condivisione oggetti
- IPv6 non supportato.
- È supportata solo la VRF globale.
- I criteri ZTNA universali non vengono applicati al traffico del tunnel da sito a sito verso un dispositivo.
- I dispositivi del cluster non sono supportati.

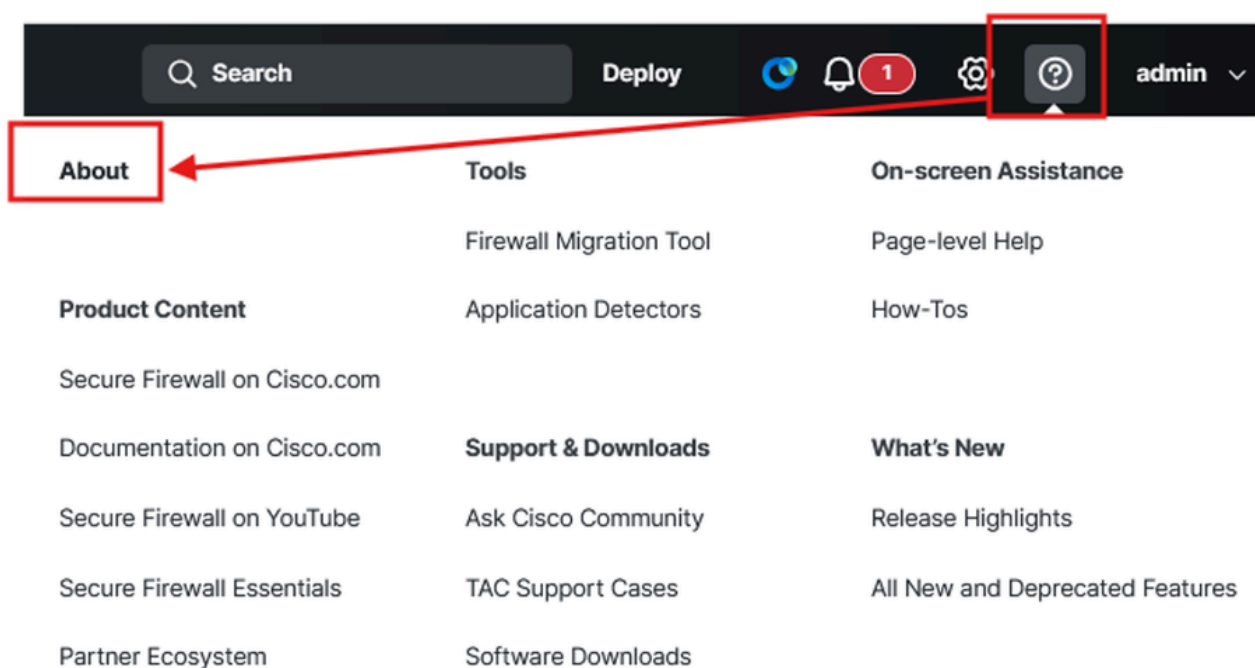
- Gli FTD distribuiti come contenitori sulle serie firepower 4K e 9K non sono supportati
- Le sessioni universali ZTNA non supportano i frame jumbo

Configurazione

Verifica versione FMC

Verificare che Firewall Management Center e Firewall FTD siano in esecuzione sulla versione software supportata per ZTNA universale (può essere 7.7.10 o superiore):

- Fare clic su ? (angolo superiore destro) e fare clic su [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

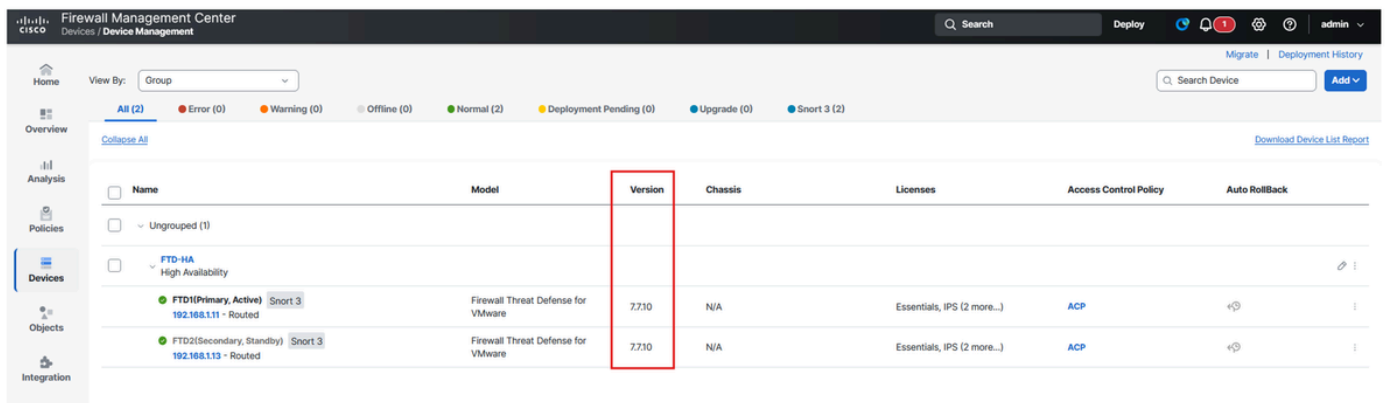
Close

Secure Firewall Management Center - Versione software

Verifica versione FTD

Passare all'interfaccia utente di FMC:

- Fai clic su **Devices** > Device Management



Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
Ungrouped (1)						
FTD-1A 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	+

Secure Firewall Threat Defense - Versione software

Verifica licenze FTD

- Fare clic su 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)						

Secure Firewall Threat Defense - Licenze Smart

Verificare le impostazioni della piattaforma e il DNS configurato correttamente

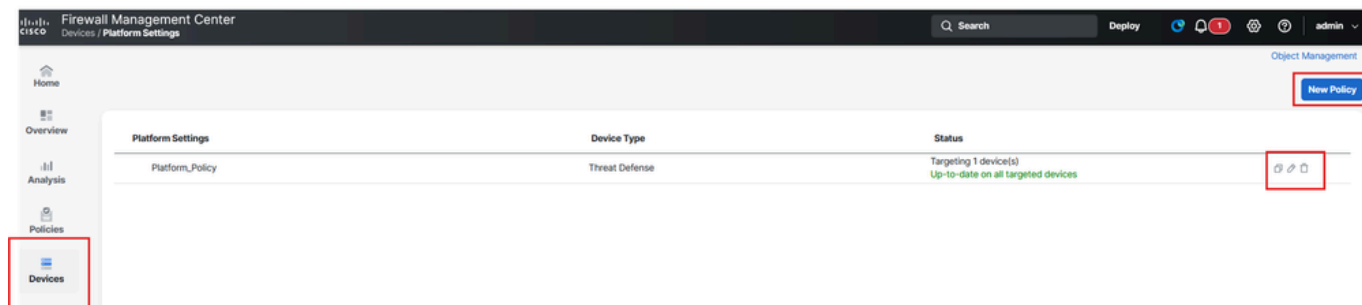
Accesso all'FTD tramite CLI:

- Eseguire il comando per verificare se DNS è configurato:

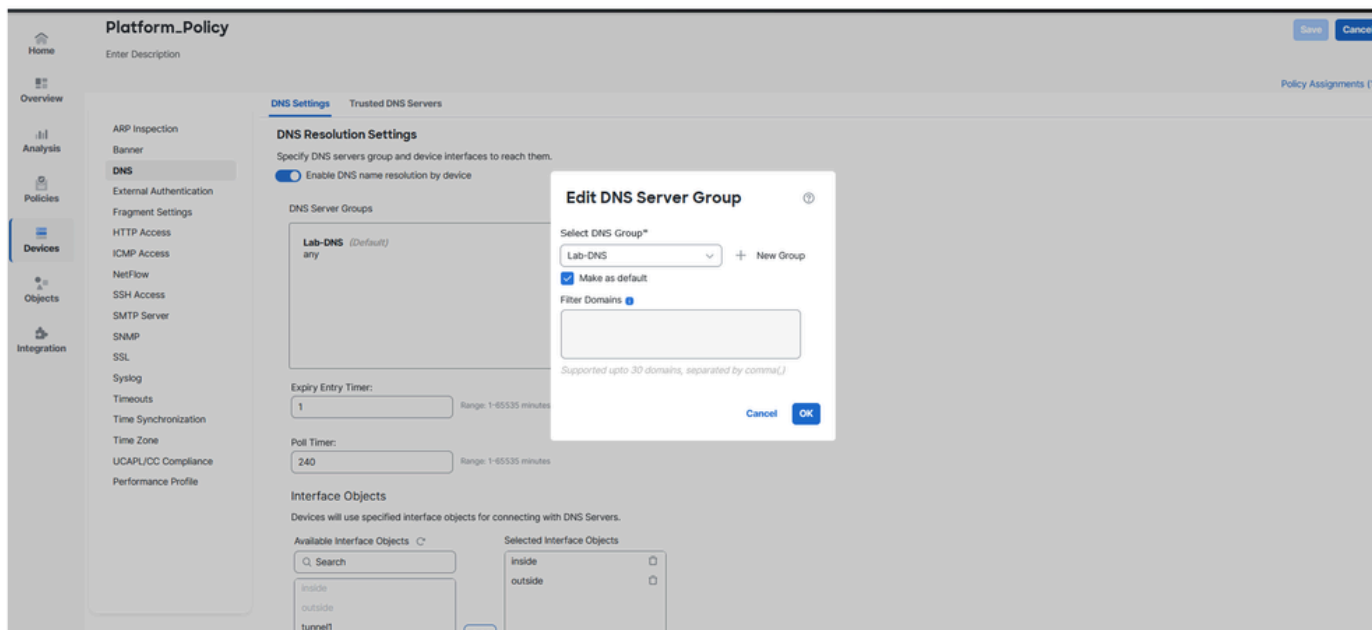
```
show run dns
```

Nel CCP:

- Fai clic su **Devices > Platform Settings**, modifica o crea un nuovo criterio



Protezione da minacce firewall - Criteri piattaforma



Protezione da minacce del firewall - Configurazione DNS

Verificare tramite CLI FTD che sia possibile eseguire il ping dell'indirizzo IP e del nome FQDN delle risorse private (se si desidera accedere a PR utilizzando il relativo nome FQDN).

```

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#
  
```

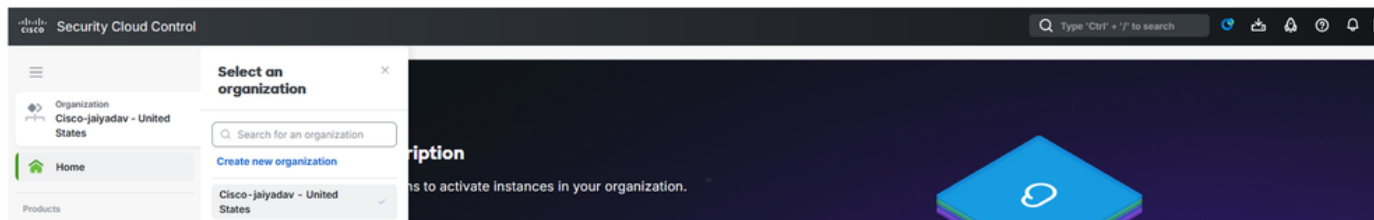
Crea un tenant di controllo del cloud di sicurezza su CDO



Nota: Se è già stato configurato un tenant SCC, non è necessario creare un nuovo tenant.

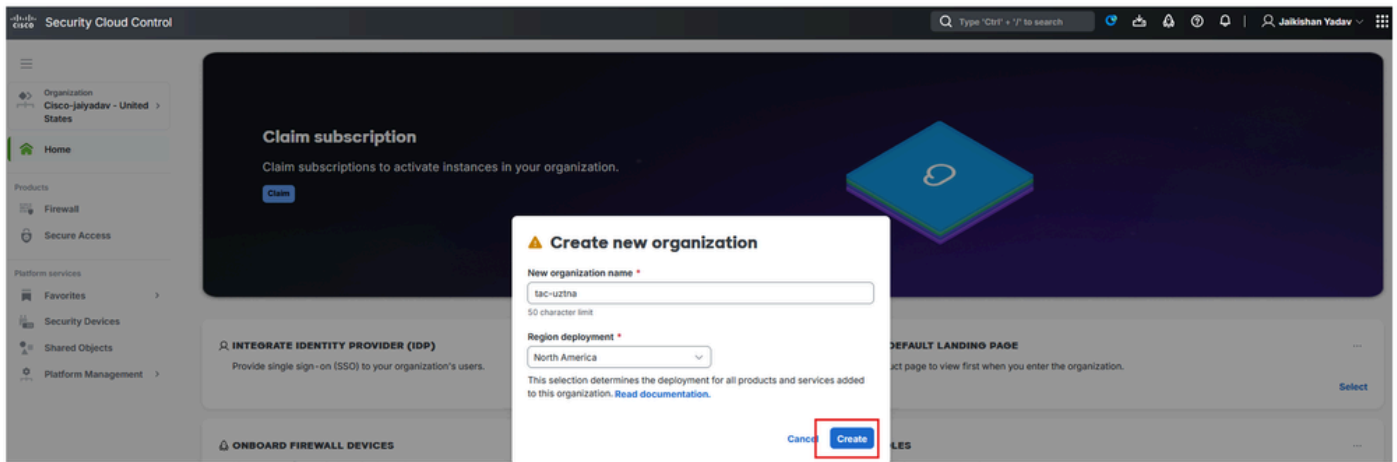
Passare a [Security Cloud Control](#):

- Fare clic su Organization > Create new organization



Secure Cloud Control - Organizzazione

- Fare clic su Create



Secure Cloud Control - Creazione di organizzazioni

Una volta creato il tenant SCC, raccogliere le informazioni sul tenant per abilitare la microapp Firewall e accesso sicuro e per abilitare uZTNA.

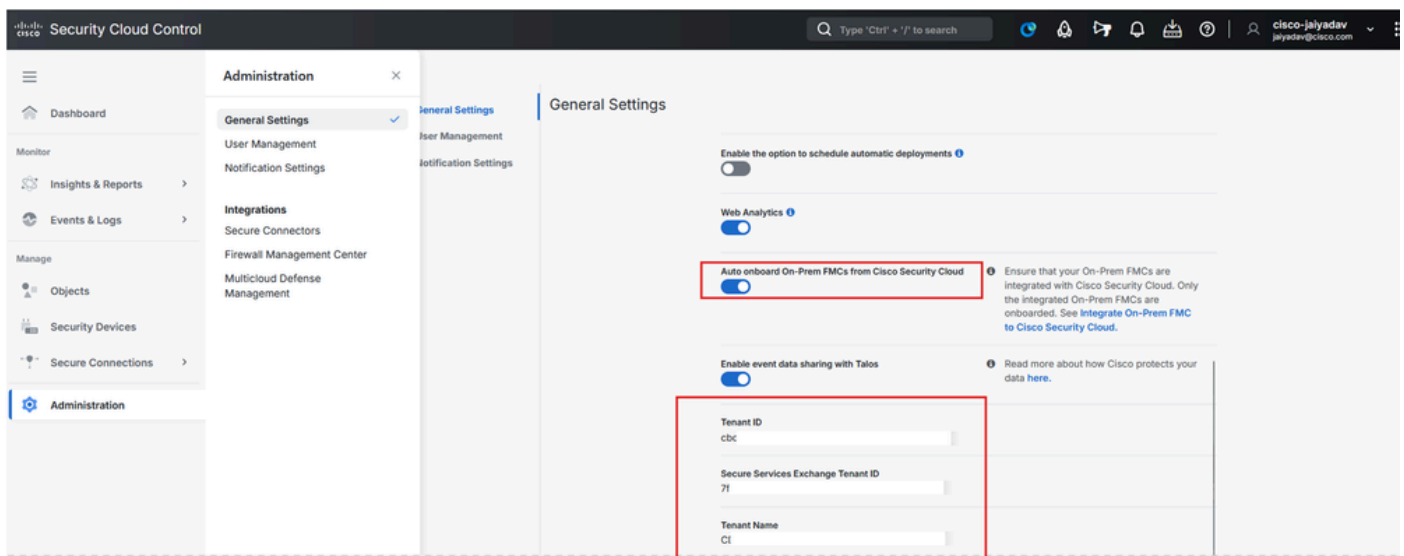
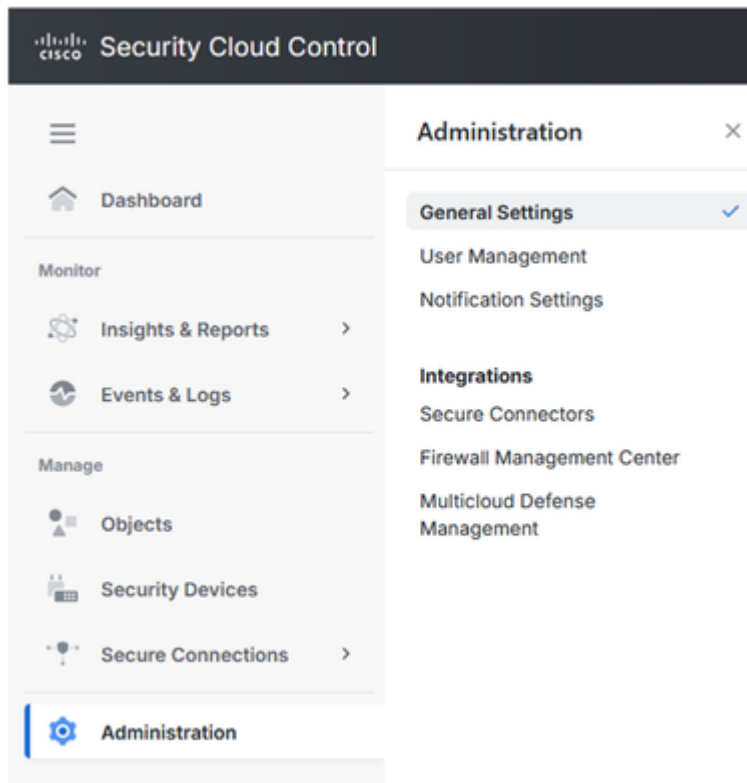
Verificare che le impostazioni generali di SCC Firewall siano configurate

Passare a [CDO/SCC](#):

- Fai clic su **Administration** > **General Settings**
- Assicurarsi che l'opzione sia **Auto onboard On-Prem FMCs from Cisco Security Cloud** **attivata**.

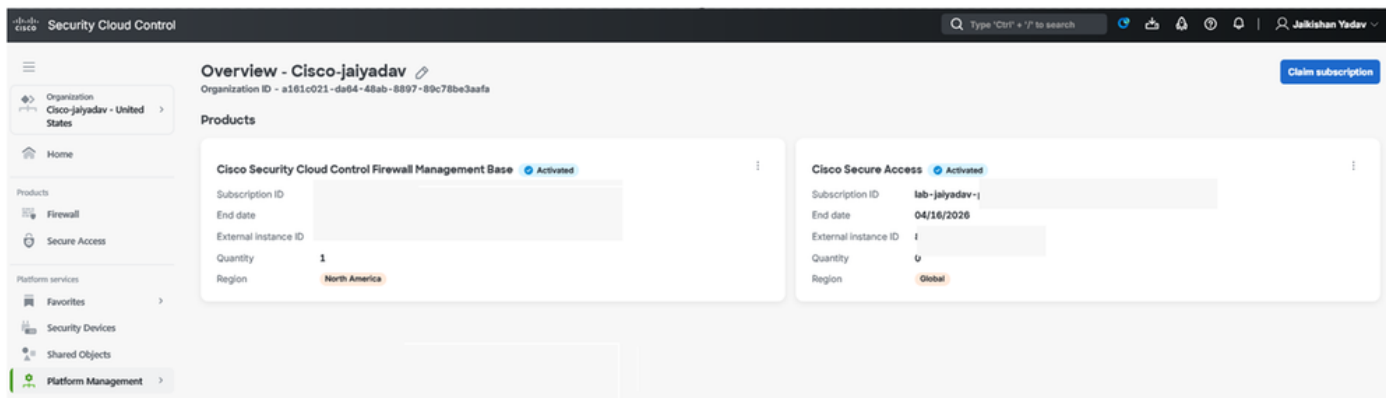


Nota: L'utente che tenta di accedere a Secure Access MicroApp deve disporre di ruoli di amministratore Secure Access e Security Cloud Control.



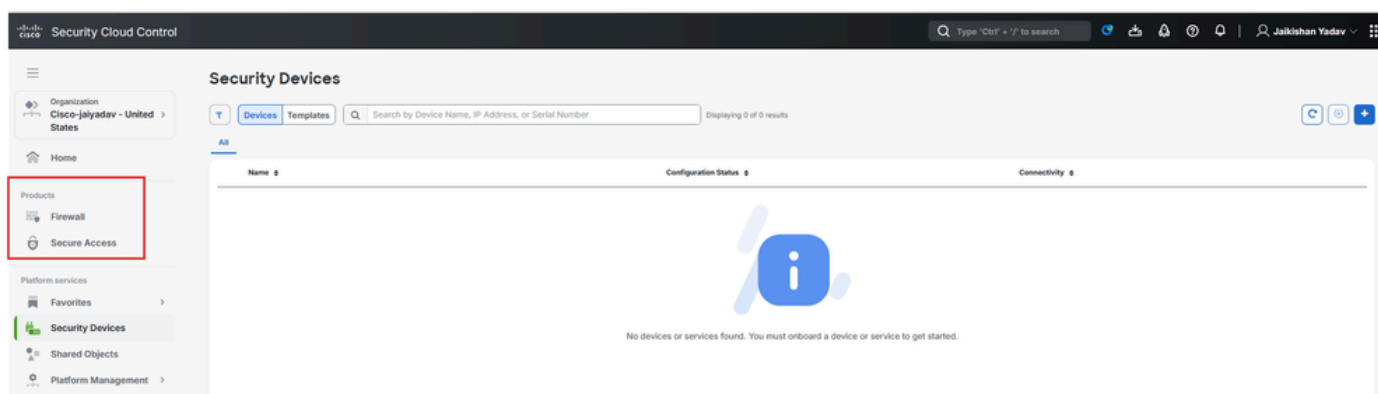
Secure Cloud Control - Dettagli organizzazione

Verificare l'integrazione di Secure Access Tenant e Security Control Firewall Management Base



Secure Cloud Control - Attivazione accesso sicuro

Una volta completato il passaggio [Creazione di un tenant di controllo del cloud di sicurezza su CDO](#) e [Creazione di un tenant di controllo del cloud di sicurezza su CDO](#), è possibile visualizzare le micro app di firewall e accesso sicuro sul dashboard SCC:



Controllo Secure Cloud - Micro App

Genera certificato firmato CA Firewall Threat Defense (FTD)



Nota: È inoltre possibile utilizzare i [certificati FTD](#) autofirmati FTD (fare riferimento alla sezione Generazione di certificati CA interni e autofirmati). Il certificato deve essere in formato PKCS12 e deve essere presente nell'archivio del computer dell'utente in una CA radice attendibile.

Per generare un certificato firmato da un'autorità di certificazione utilizzando FTD nella funzione build openssl:

- Passa a FTD
- Esegui, `expert` comando
- Genera CSR e chiave tramite openssl
 - Comando 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
```

Richiesta di firma del certificato

- Copiare il CSR e ottenere un certificato firmato dall'autorità di certificazione
- Usa chiave e certificato firmati CA FTD e converti il certificato nel formato PKCS12
 - Comando OpenSSL:

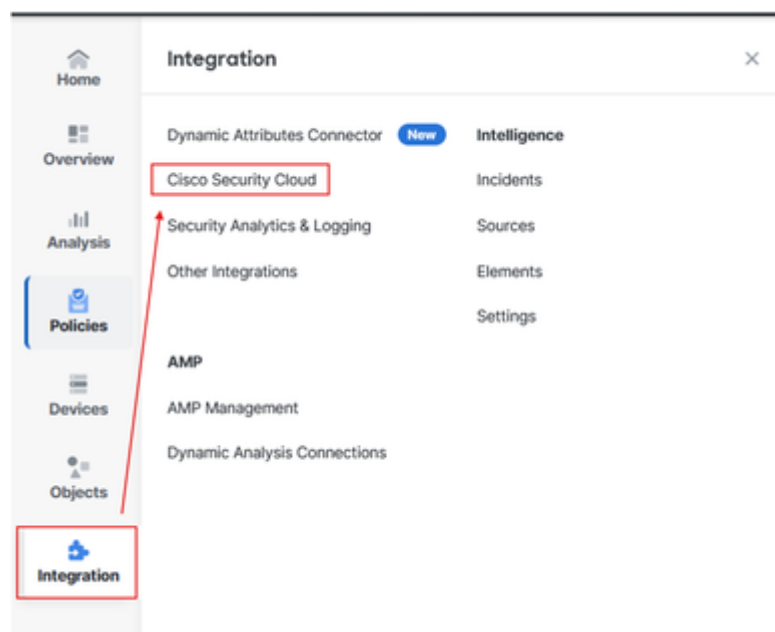
```
openssl pkcs12 -export -out ftdcert.p12 -in cert.crt -inkey cert.key
```

- Esportare il certificato utilizzando SCP o un altro strumento.

Centro gestione firewall locale integrato per Security Cloud Control

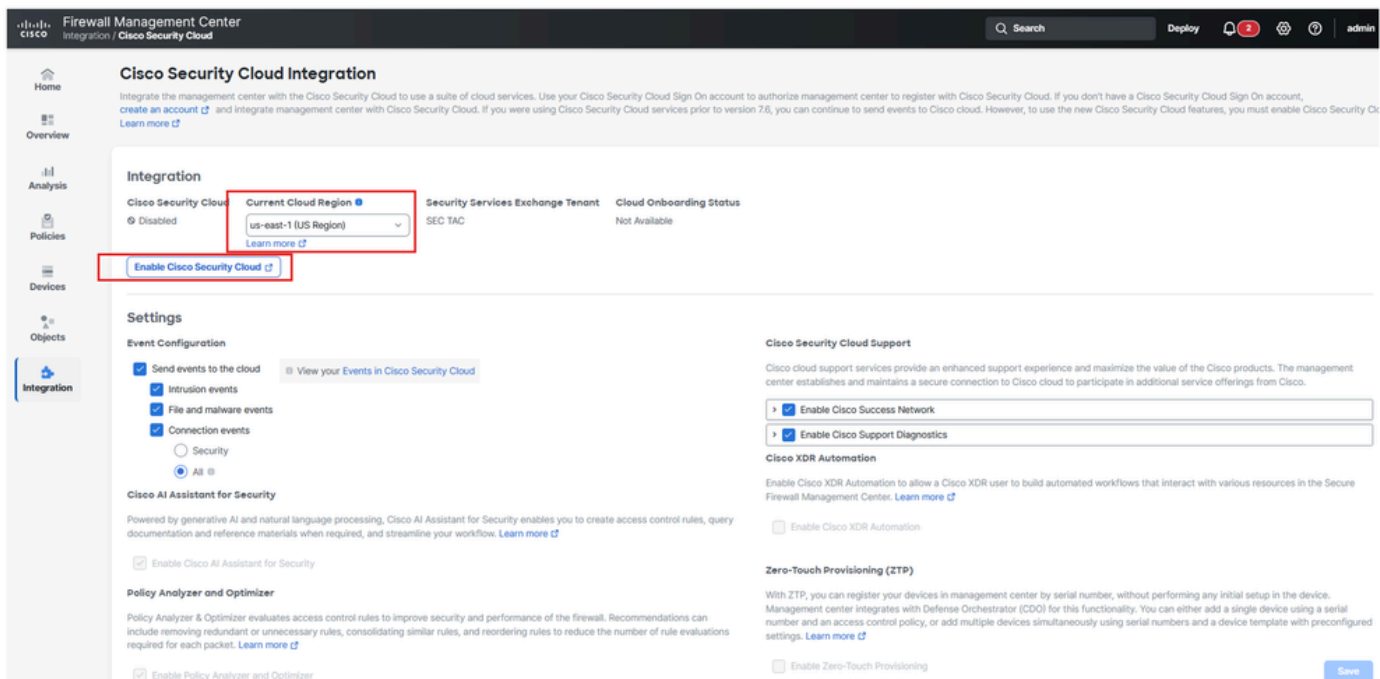
Passare al CCP:

- Fai clic su **Integration** > Cisco Security Cloud



Integrazione di Centro gestione firewall e SCC

- Scegliere l'area cloud, quindi fare clic su **Enable Cisco Security Cloud**



The screenshot displays the Cisco Firewall Management Center (FMC) interface, specifically the 'Cisco Security Cloud Integration' page. The page is divided into several sections:

- Integration:** This section contains the 'Current Cloud Region' dropdown menu, which is currently set to 'us-east-1 (US Region)'. Below this, there is a button labeled 'Enable Cisco Security Cloud'.
- Settings:** This section includes 'Event Configuration' and 'Cisco AI Assistant for Security'.
- Cisco Security Cloud Support:** This section contains checkboxes for 'Enable Cisco Success Network' and 'Enable Cisco Support Diagnostics'.
- Cisco XDR Automation:** This section includes a checkbox for 'Enable Cisco XDR Automation'.
- Zero-Touch Provisioning (ZTP):** This section includes a checkbox for 'Enable Zero-Touch Provisioning'.

Onboarding di Firewall Management Center in SCC

Verrà aperta una nuova scheda del browser nella nuova scheda:

- Fare clic su **Continue to Cisco SSO**



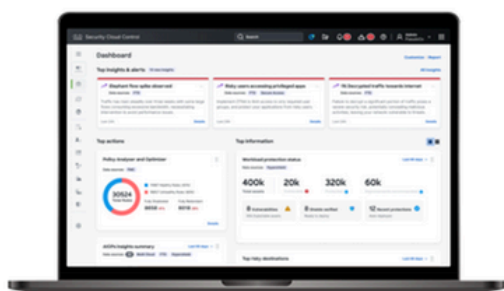
Nota: Accertarsi di essere disconnessi da SCC e di non avere altre schede aperte.



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](#)

Onboarding di Firewall Management Center in SCC

- Scegliere il tenant SCC e fare clic su [Authorize FMC](#)



Welcome to Security Cloud Control

i 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

- 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

Onboarding di Firewall Management Center in SCC

- Fare clic su Save


Firewall Management Center
 Integration / Cisco Security Cloud

Deploy
2
admin

Home

Overview

Analysis

Policies

Devices

Objects

Integration

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

Enable Cisco Security Cloud

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)

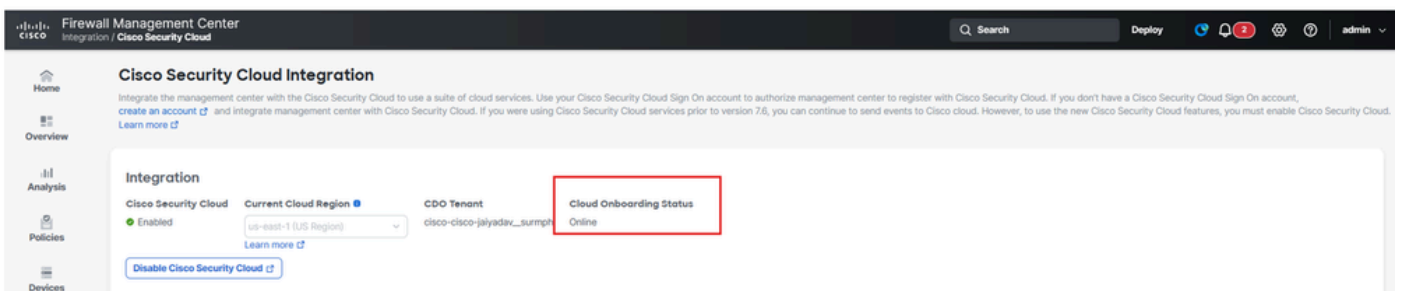
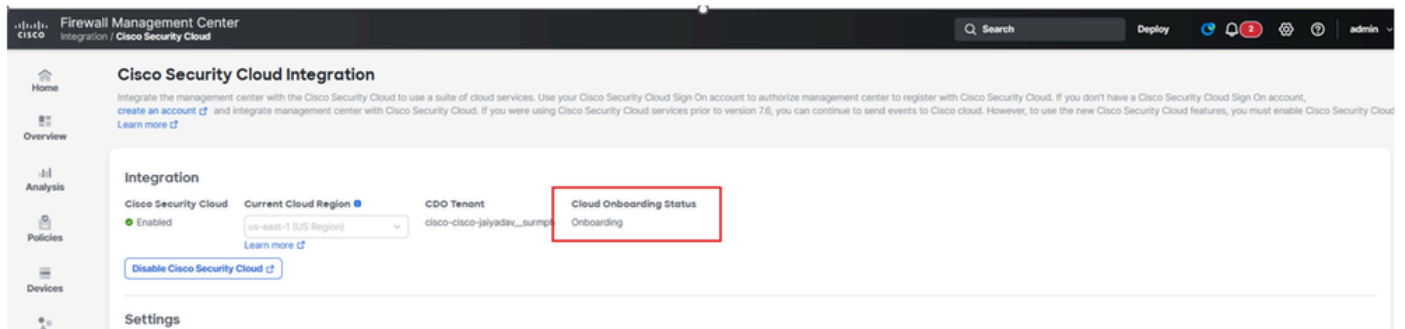
With ZTP, you can register your devices in management center by serial number, without performing any initial setup in the device. Management center integrates with Defense Orchestrator (CDO) for this functionality. You can either add a single device using a serial number and an access control policy,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

☒ Enable Zero-Touch Provisioning

Save

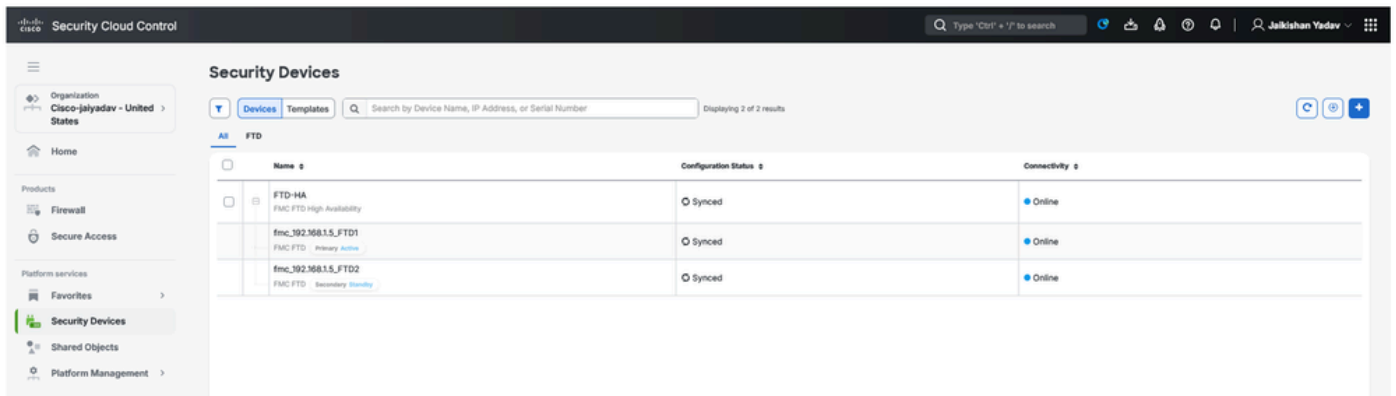
Onboarding di Firewall Management Center in SCC

Lo stato di deve Cloud Onboarding Status essere modificato da **Not Available** a **Onboarding** Online.



Stato di caricamento di Centro gestione firewall

- Passare a [SCC](#) e controllare lo stato FTD in Platform Services > Security Devices



Stato di difesa dalle minacce del firewall sicuro su SCC

Registra impostazioni Universal Zero Trust Network Access (uZTNA) su FTD

Passare a SCC:

- Fare clic su Platform Services > Security Devices > FTD > Device Management > Universal Zero Trust Network Access

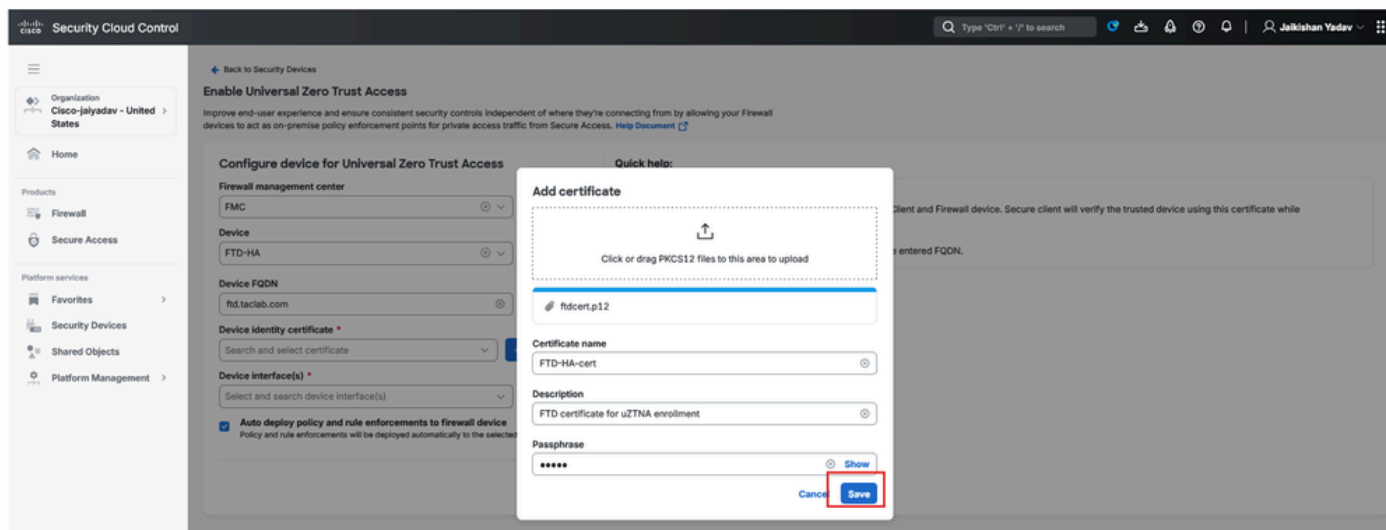
The screenshot shows the Cisco Security Cloud Control interface. On the left, the navigation menu includes 'Platform services' (1) and 'Security Devices' (2). The main area displays a table of 'Security Devices' with columns for Name, Configuration Status, and Connectivity. The first device, 'FTD-HA',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

Secure Firewall Threat Defense - Configurazione ZTNA universale

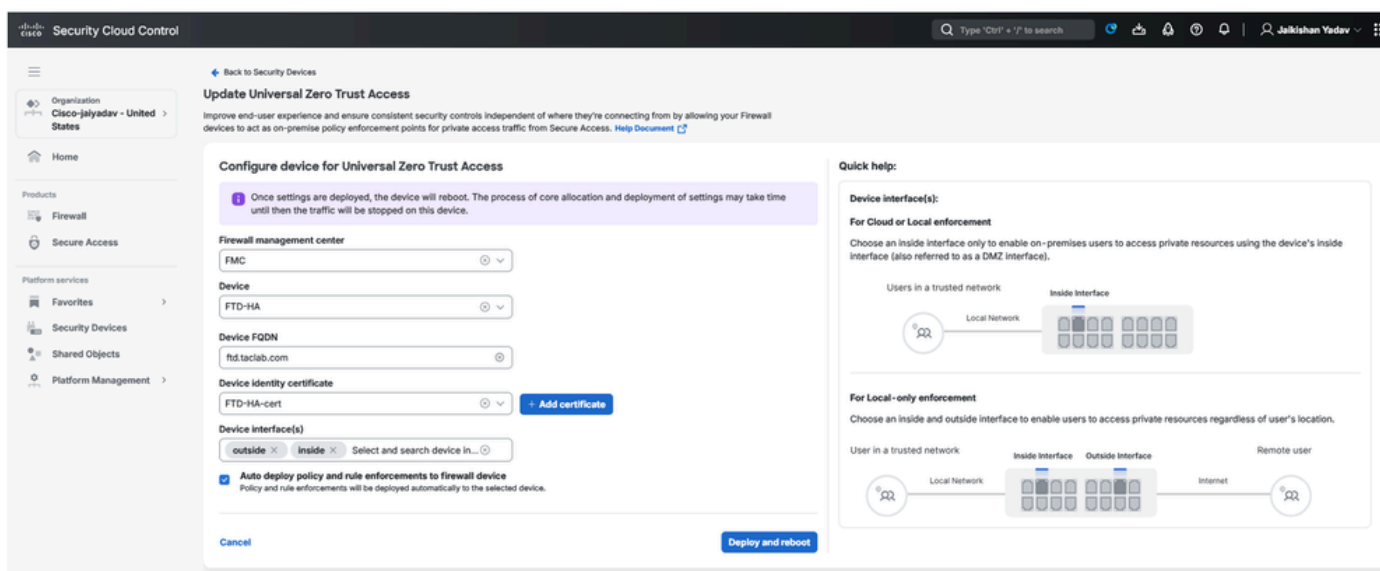
- Compilare le informazioni e caricare il certificato FTD generato nella fase [Generate Firewall Threat Defense \(FTD\) CA signed certificate](#)

The screenshot shows the 'Enable Universal Zero Trust Access' configuration page. The 'Configure device for Universal Zero Trust Access' section includes fields for 'Firewall management center' (FMC), 'Device' (FTD-HA), 'Device FQDN', 'Device identity certificate', and 'Device interface(s)'. There is an 'Add certificate' button and a checkbox for 'Auto deploy policy and rule enforcements to firewall device'. The 'Quick help' section provides diagrams for 'For Cloud or Local enforcement' and 'For Local-only enforcement'.

Secure Firewall Threat Defense - Configurazione ZTNA universale



Secure Firewall Threat Defense - Configurazione ZTNA universale

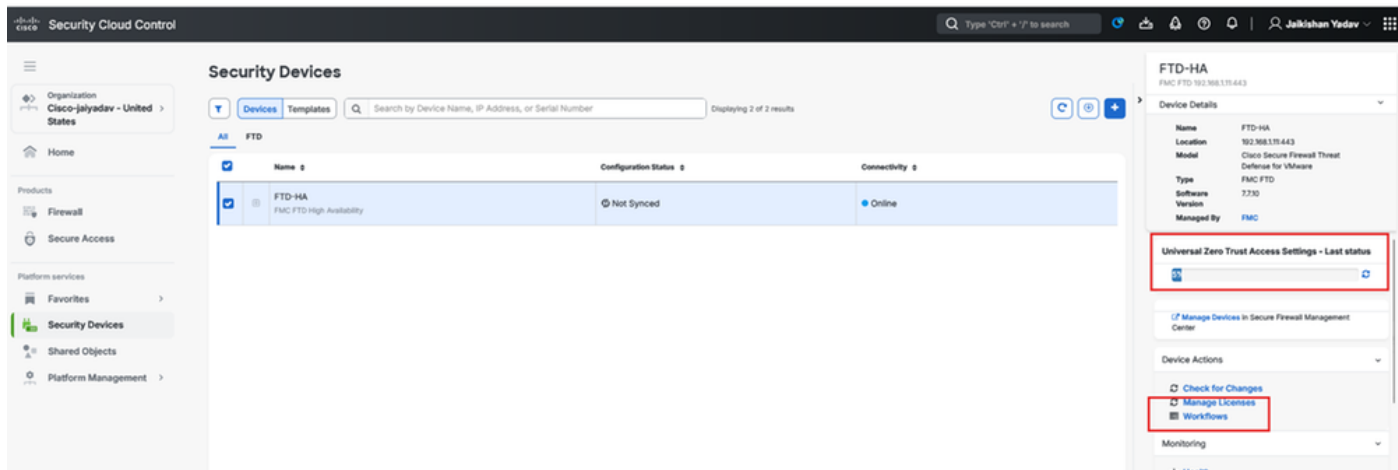


Secure Firewall Threat Defense - Configurazione ZTNA universale

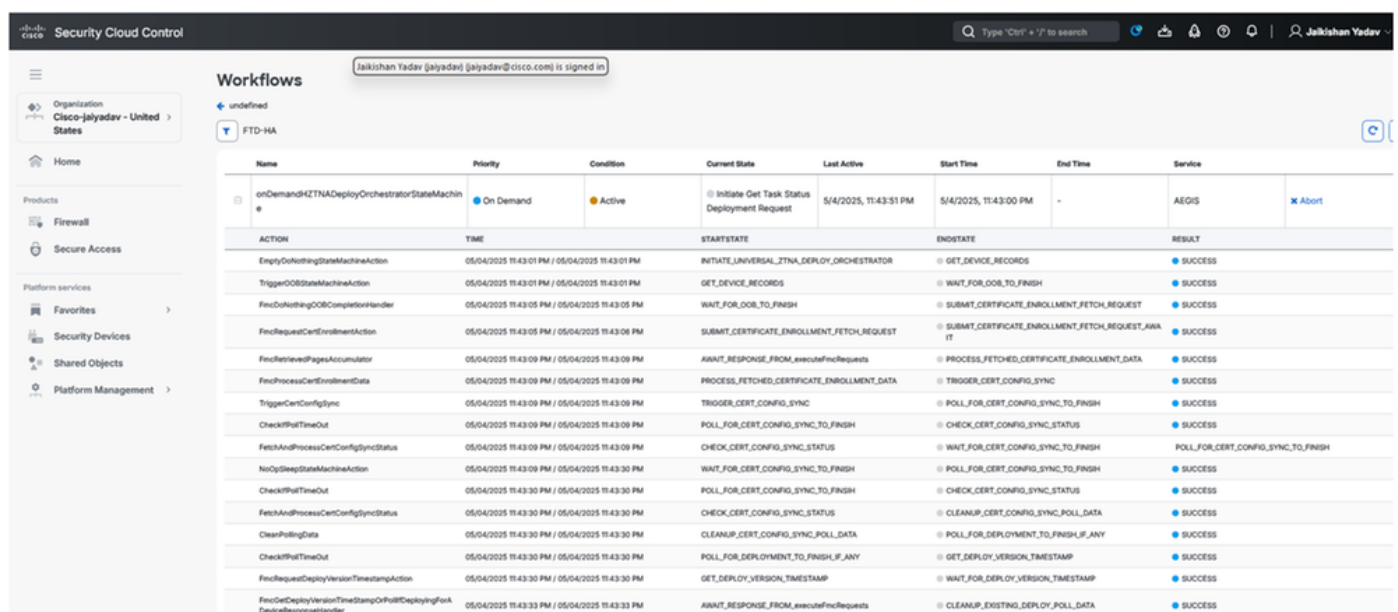


Nota: Quando si abilita uZTNA su FTD HA, le modifiche vengono distribuite e le unità Firewall Threat Defense (FTD) vengono riavviate contemporaneamente. Assicurarsi di pianificare una finestra di manutenzione adeguata.

- Fare clic su Workflow per controllare i registri

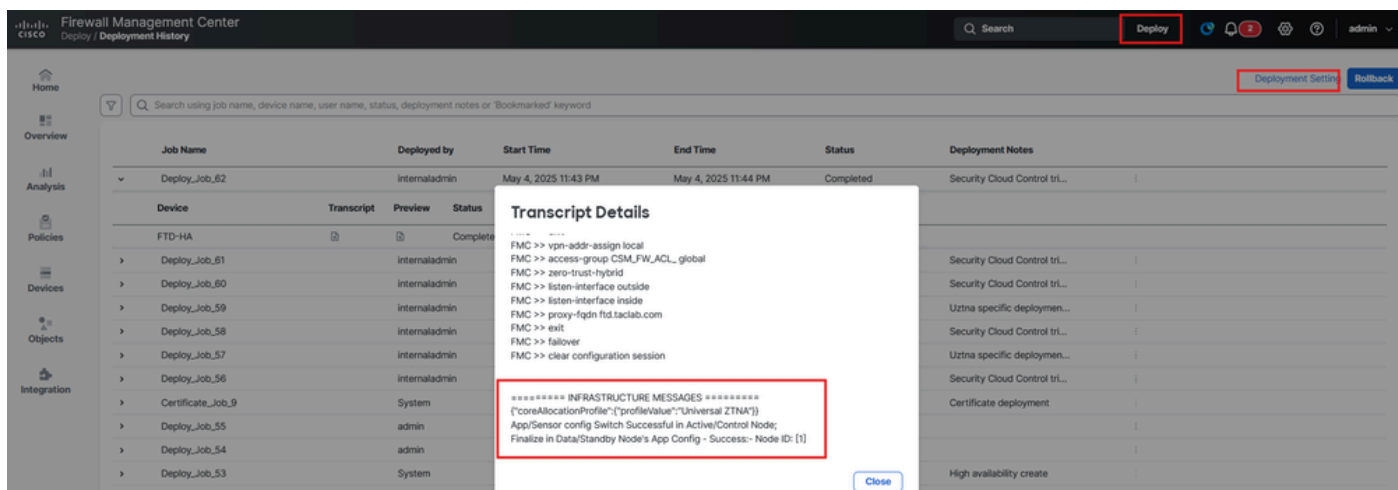


Secure Firewall Threat Defense - Stato configurazione ZTNA universale



Flusso di lavoro di controllo del cloud di sicurezza

In Dettagli trascrizione è possibile visualizzare Policy Deployment Status e modificare FMC.



Centro gestione firewall protetto - Stato distribuzione criteri

Registrare il client con uZTNA

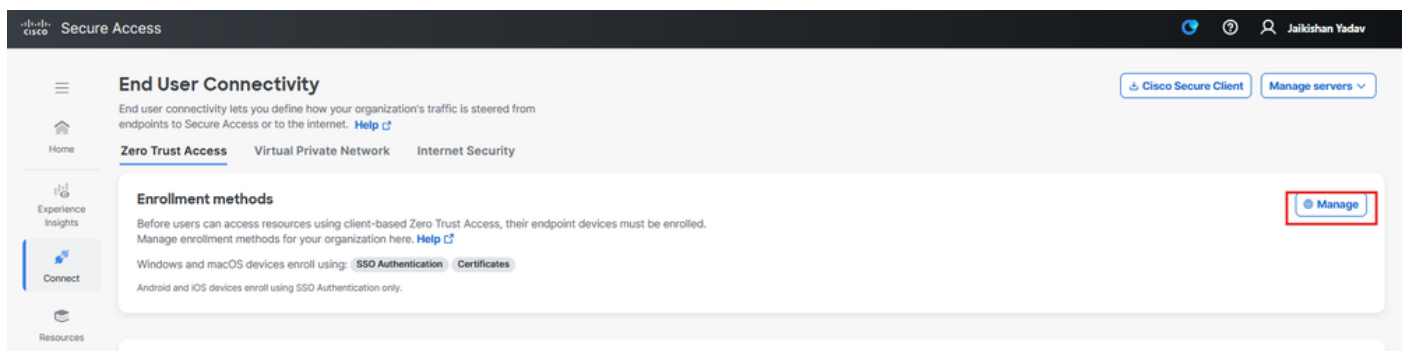
Configurazione accesso sicuro



Nota: È possibile utilizzare la registrazione SSO o una registrazione ZTA basata su certificato. Di seguito sono riportati i passaggi per la registrazione ZTA basata su certificati

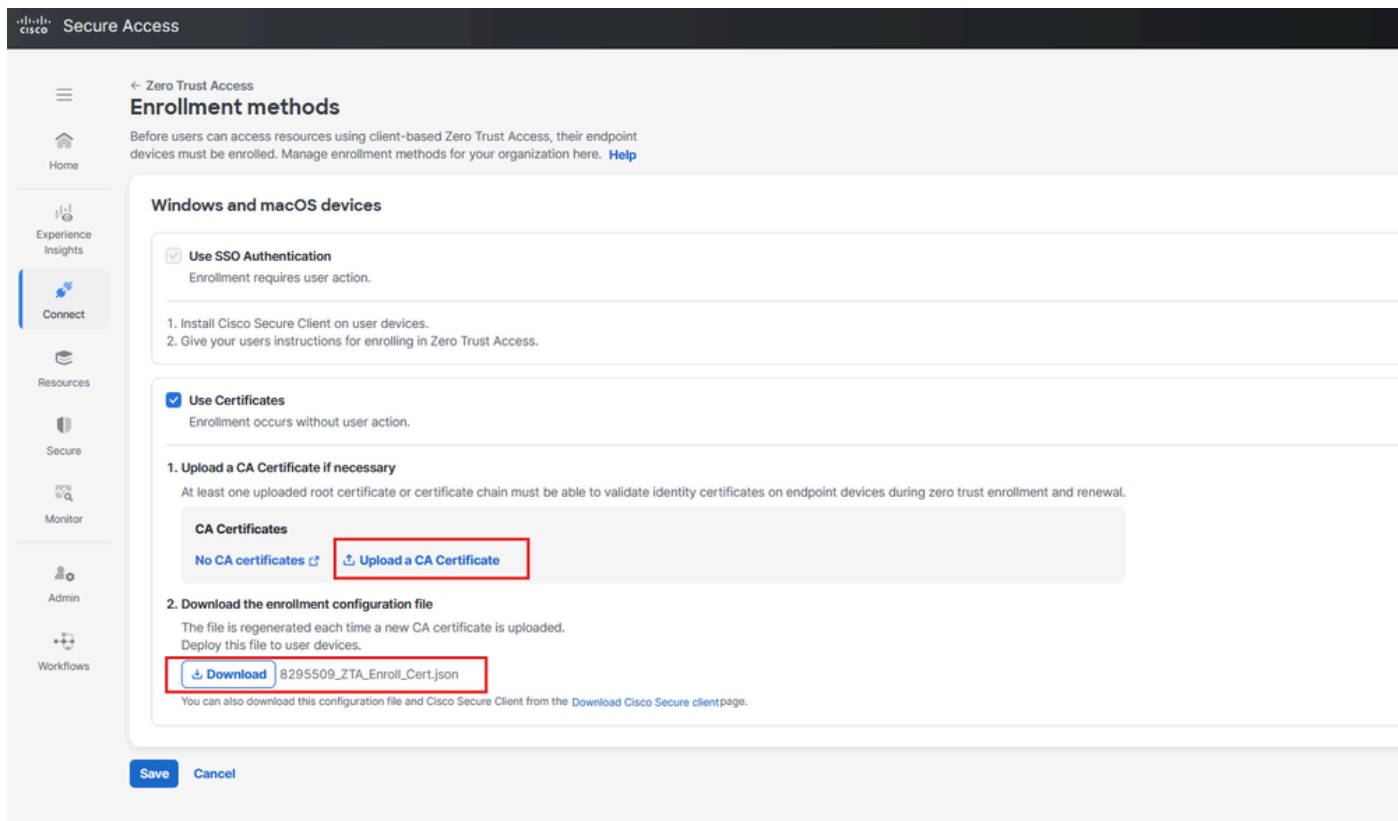
Passare a [Dashboard accesso protetto](#):

- Fare clic su **Connect > End User Connectivity > Zero Trust Access**
- Fare clic su **Manage**



Accesso sicuro - Registrazione certificato ZTA

- Carica il certificato CA radice e scarica il file di configurazione della registrazione

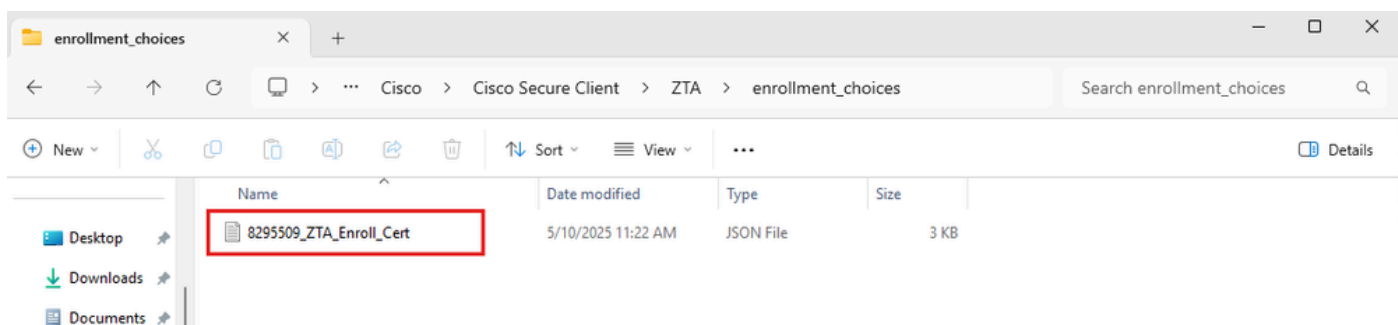


Accesso sicuro - Registrazione certificato ZTA

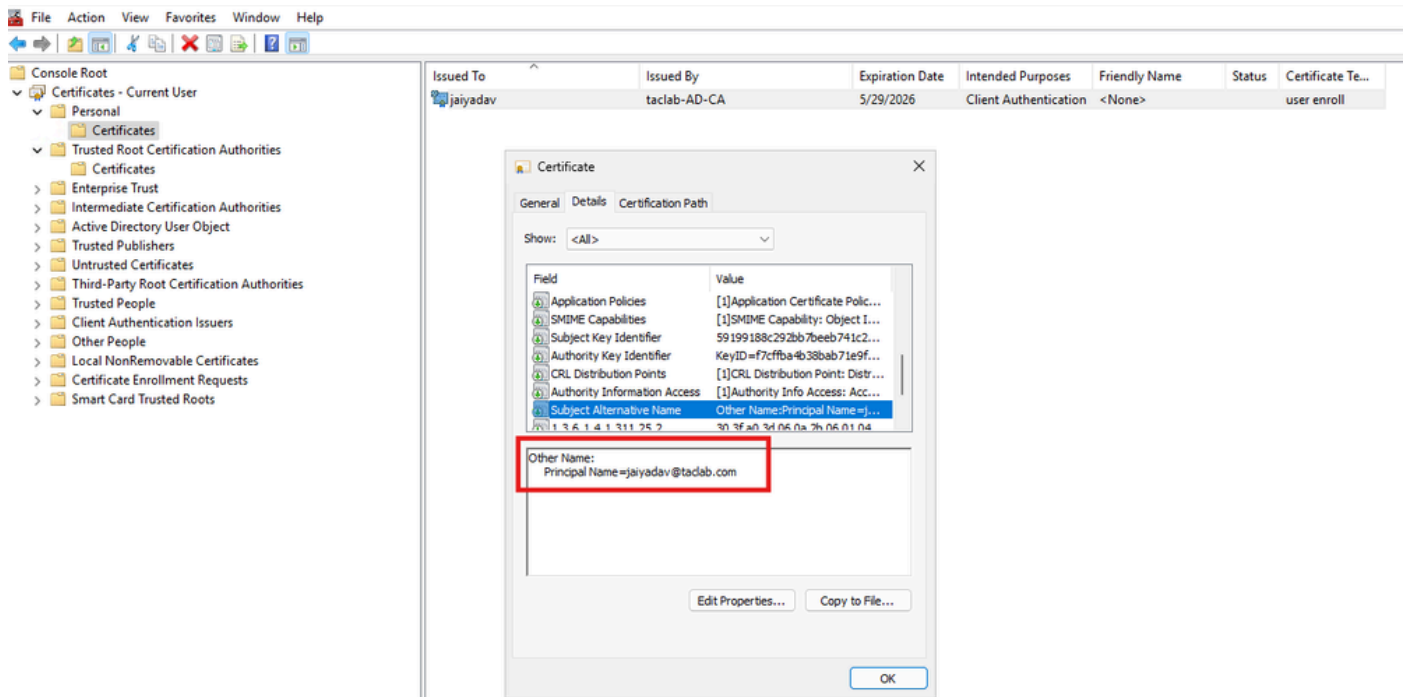
- Fare clic su [Save](#)

Configurazione client

Copiare il file di configurazione della registrazione in C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollment_choices

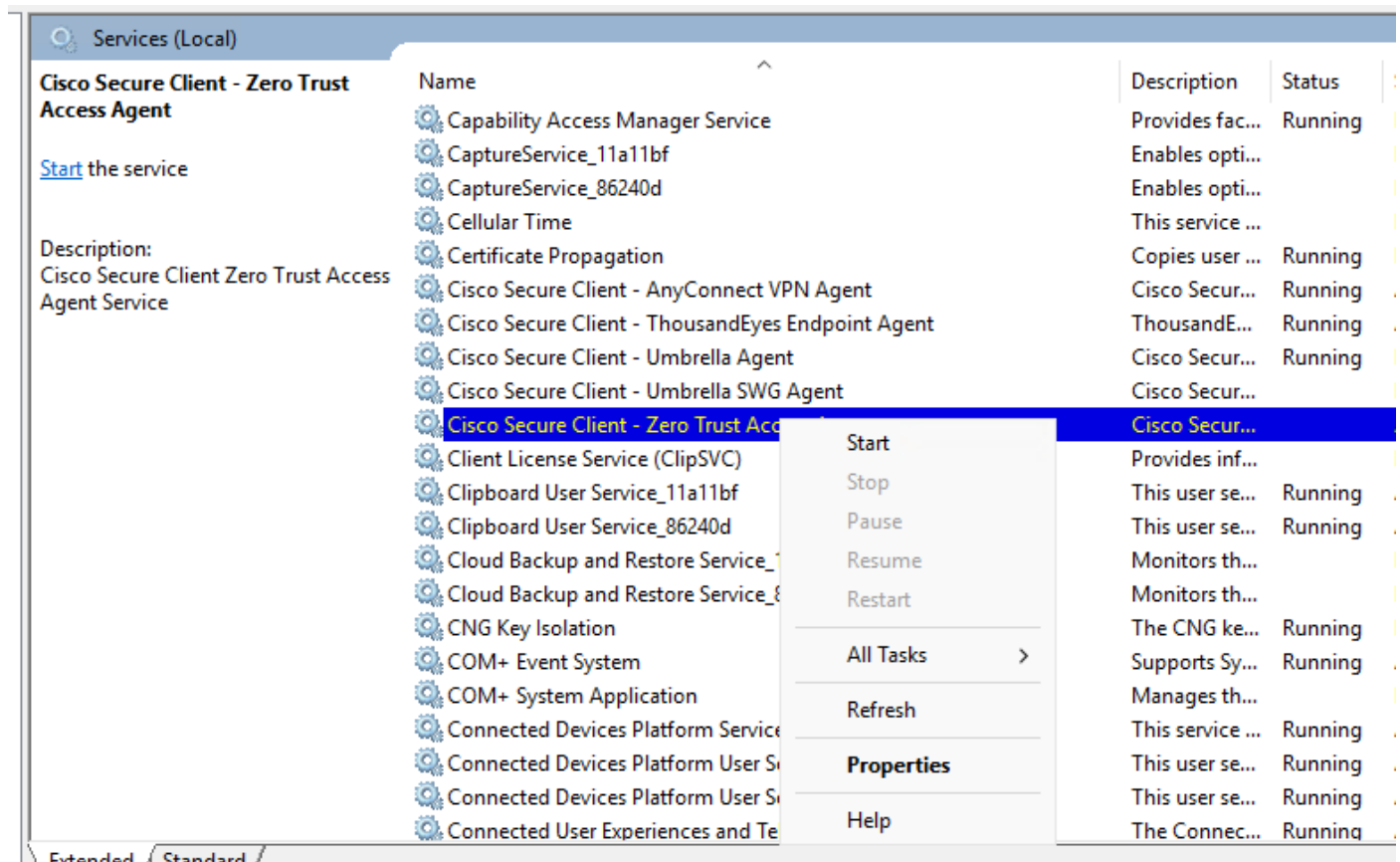


- Creare un certificato client, che deve avere un UPN nel campo SAN



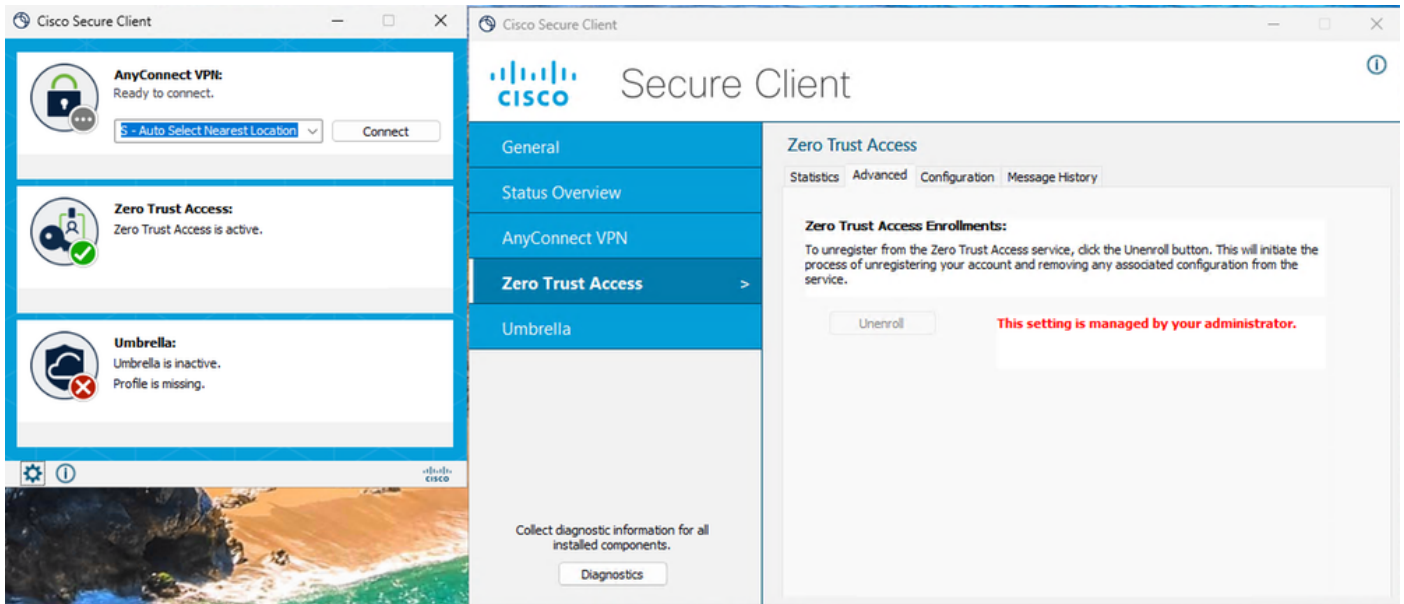
Installazione certificato

- **Avvia/Riavvia** Cisco Secure Client - Zero Trust Access Agent



Servizi Windows

- Verificare lo stato del modulo ZTA



Accesso sicuro - Stato registrazione certificato ZTA

Verifica

Utilizzare il comando successivo per verificare la configurazione uZTNA su Firewall Threat Defense (FTD):

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

Informazioni correlate

- [Supporto tecnico Cisco e download](#)
- [Cisco Secure Access Help Center](#)
- [Guida alla progettazione di Cisco BASE](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).