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

Sommario

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

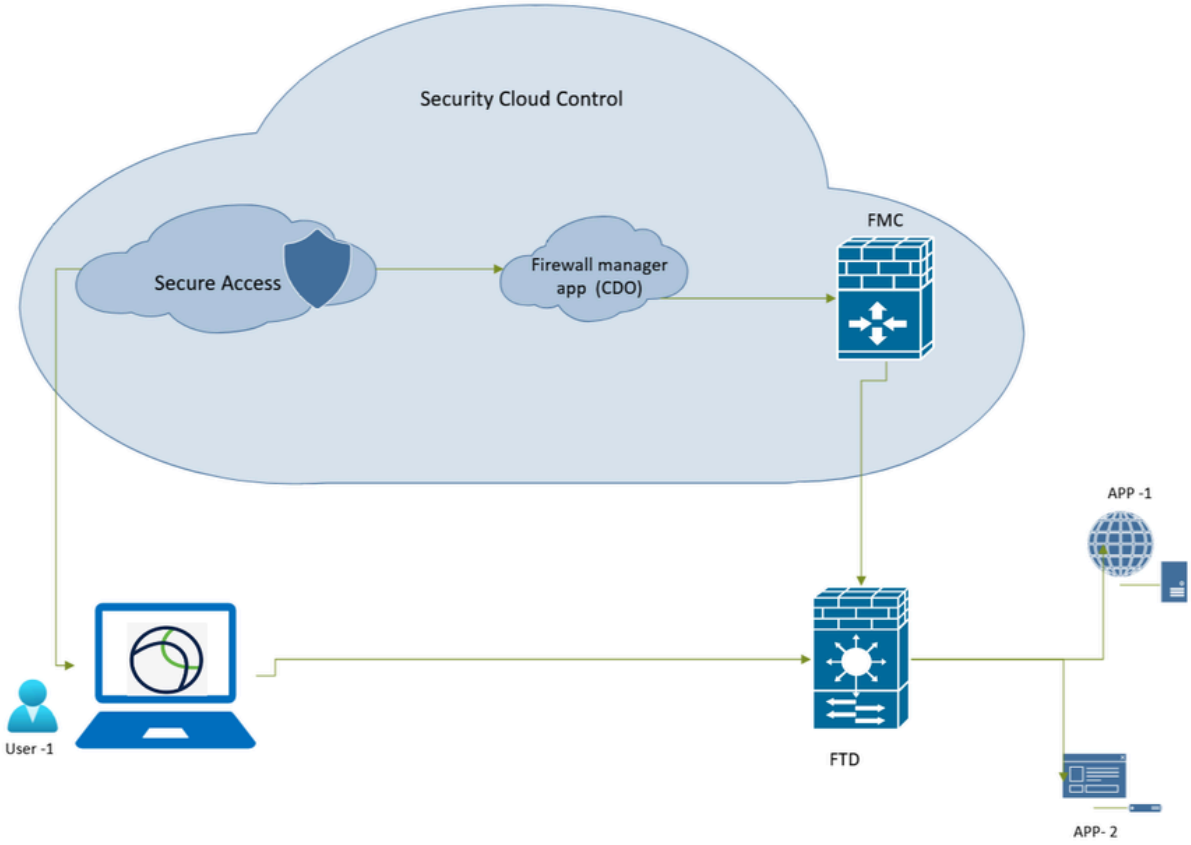
Componenti usati

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.

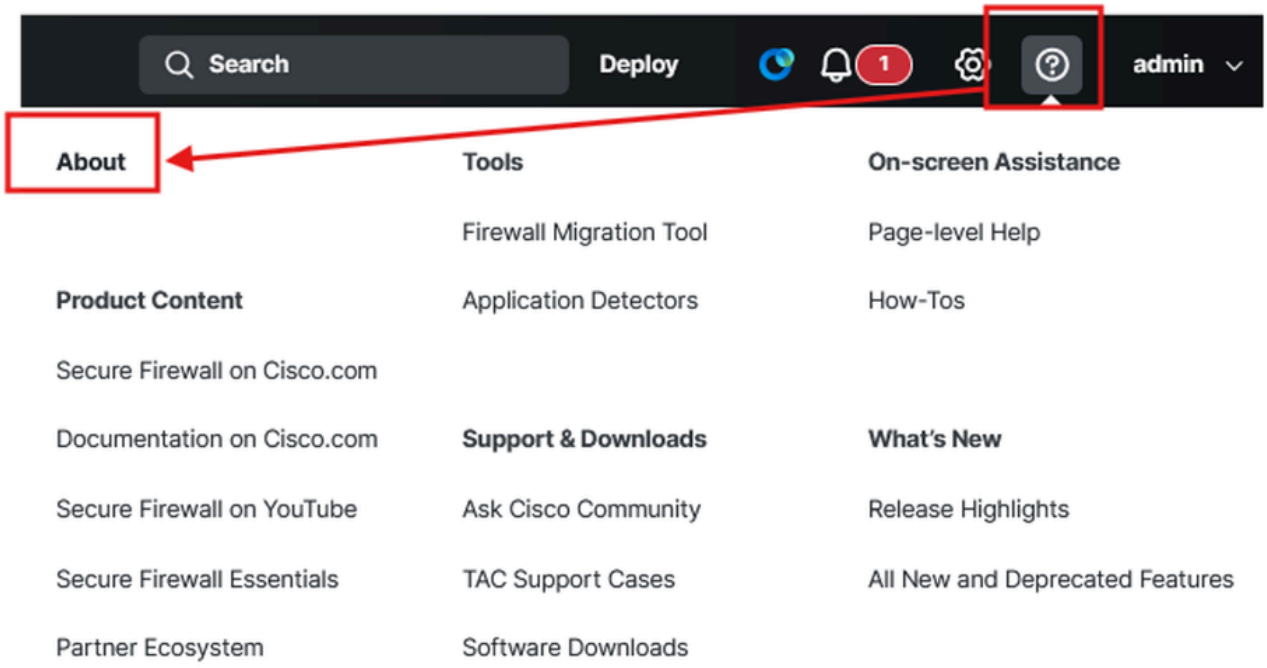
- Gli FTD distribuiti come contenitori sulle serie firepower 4K e 9K non sono supportati
- Le sessioni universali ZTNA non supportano i frame jumbo

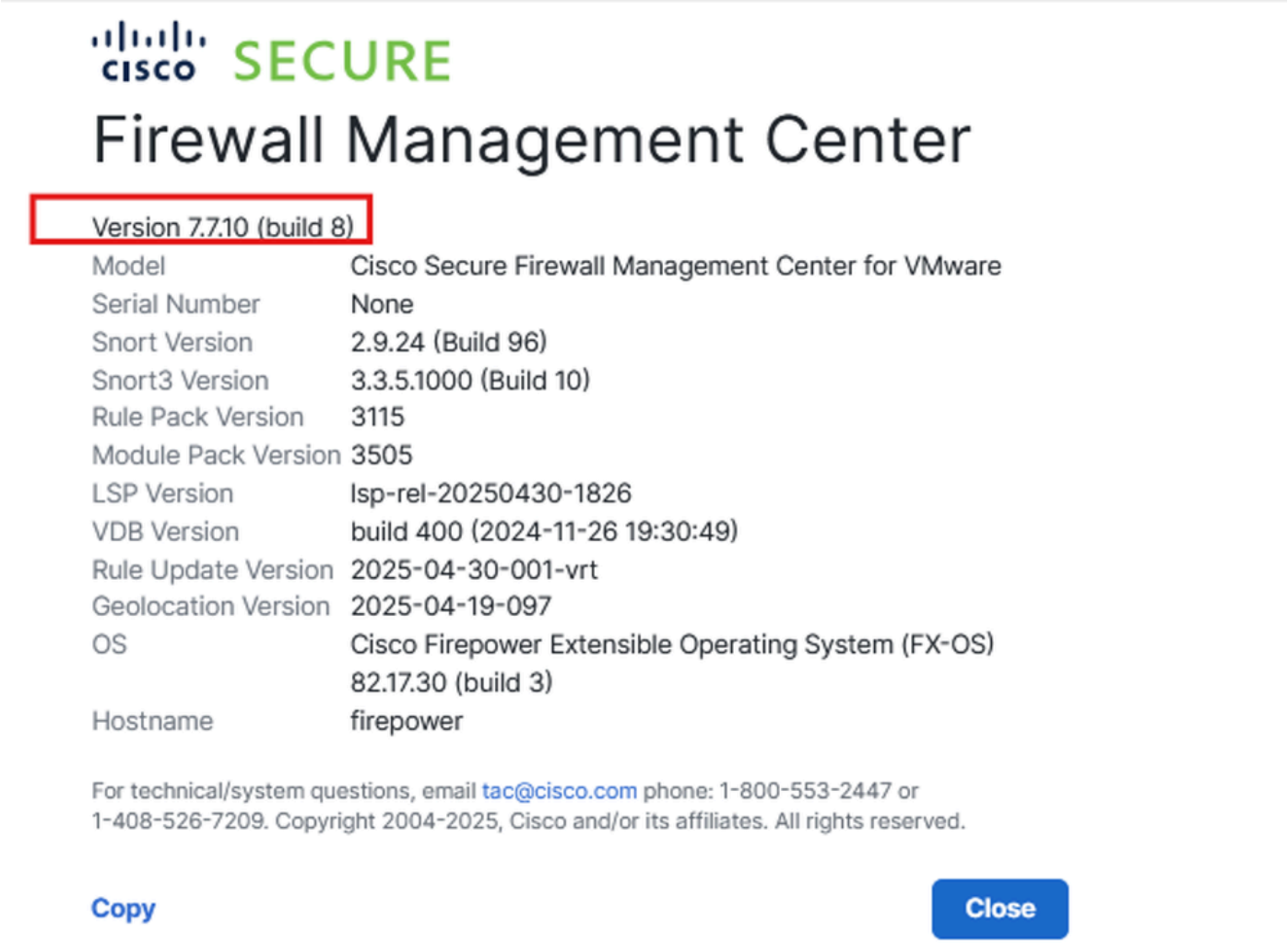
Configurazione

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



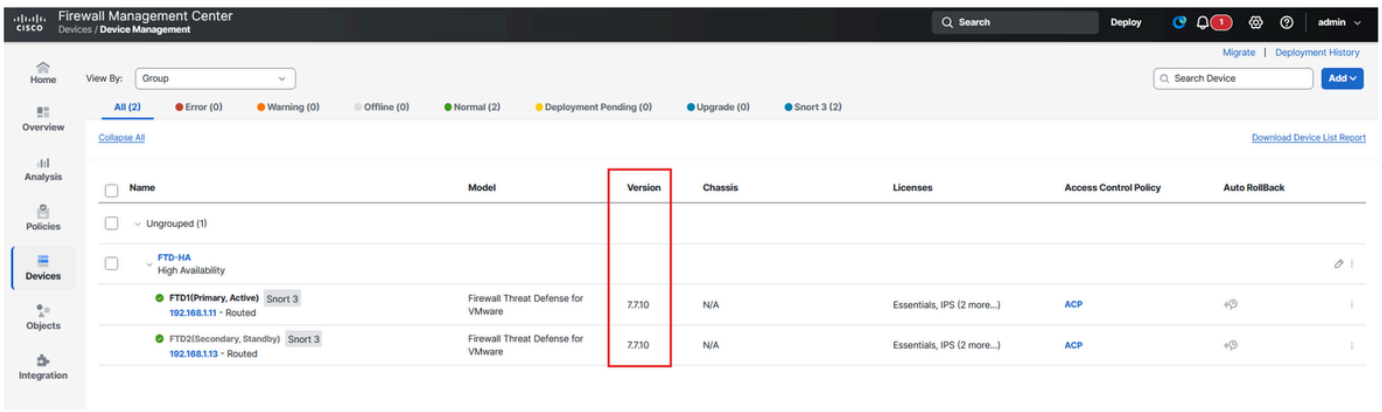


Secure Firewall Management Center - Versione software

Verifica versione FTD

Passare all'interfaccia utente di FMC:

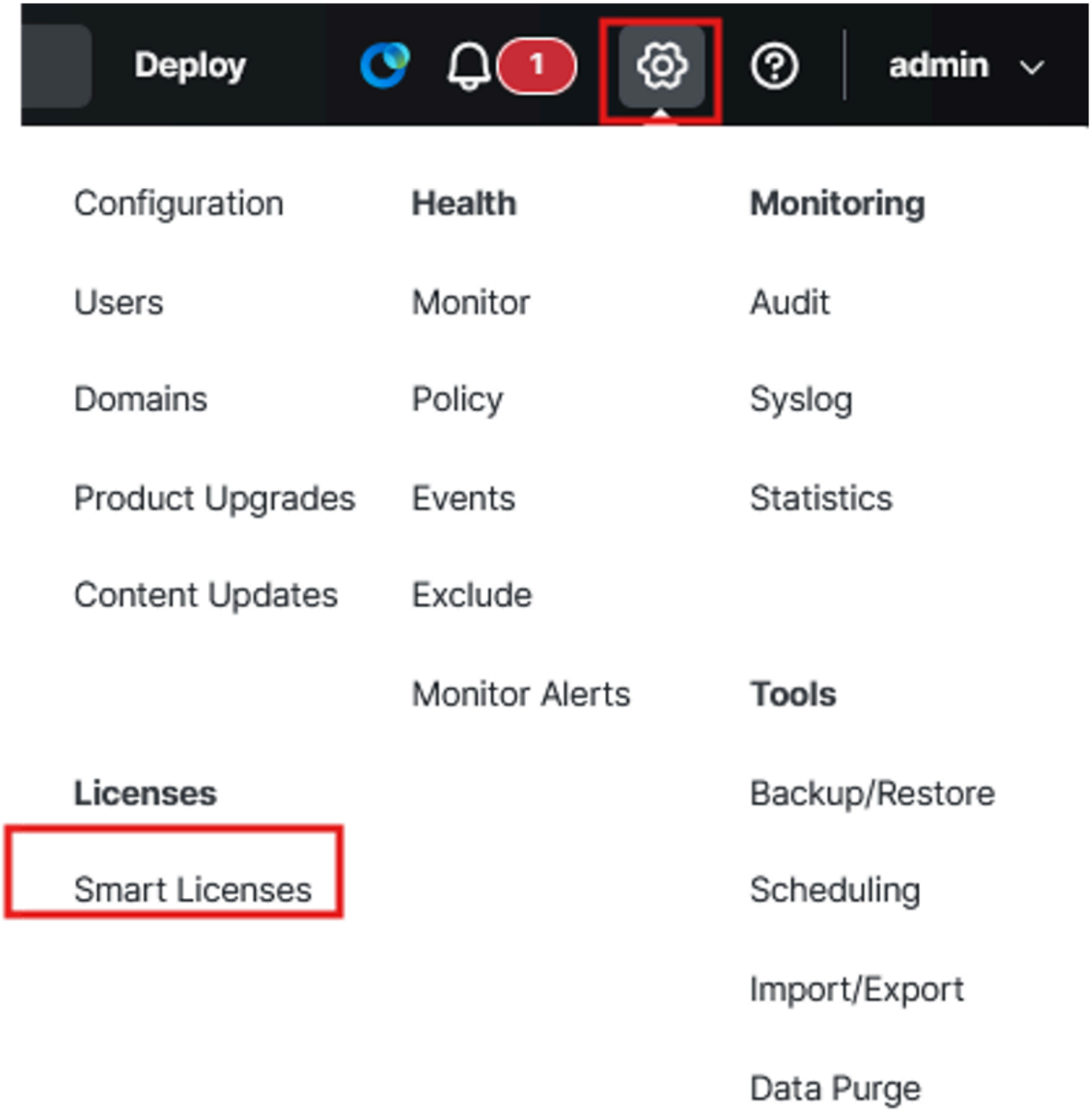
- Fai clic suDevices> Device Management

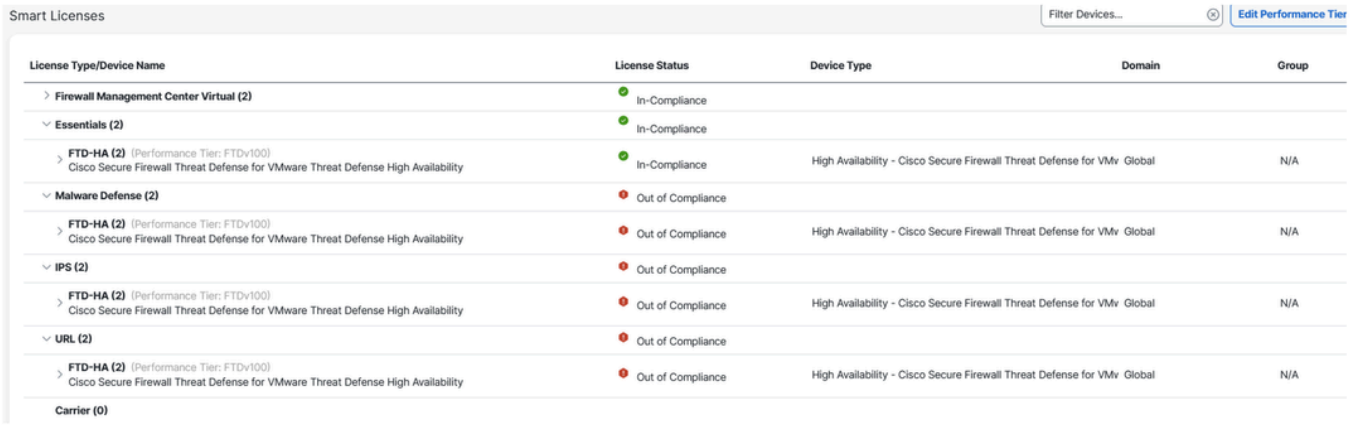


Secure Firewall Threat Defense - Versione software

Verifica licenze FTD

- Fare clic su Setting Icon > Licenses> Smart Licenses





Secure Firewall Threat Defense - Licenze Smart

Verificare le impostazioni della piattaforma e il DNS configurato correttamente

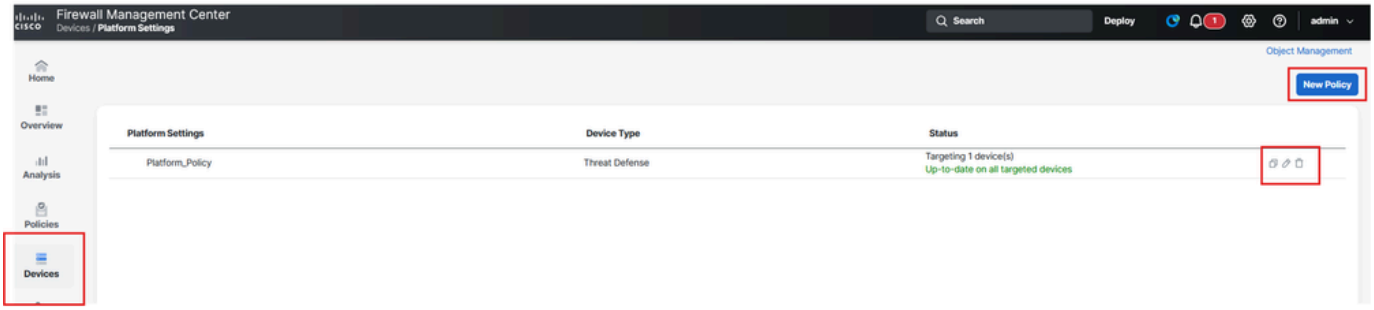
Accesso all'FTD tramite CLI:

- Eseguire il comando per verificare se DNS è configurato:

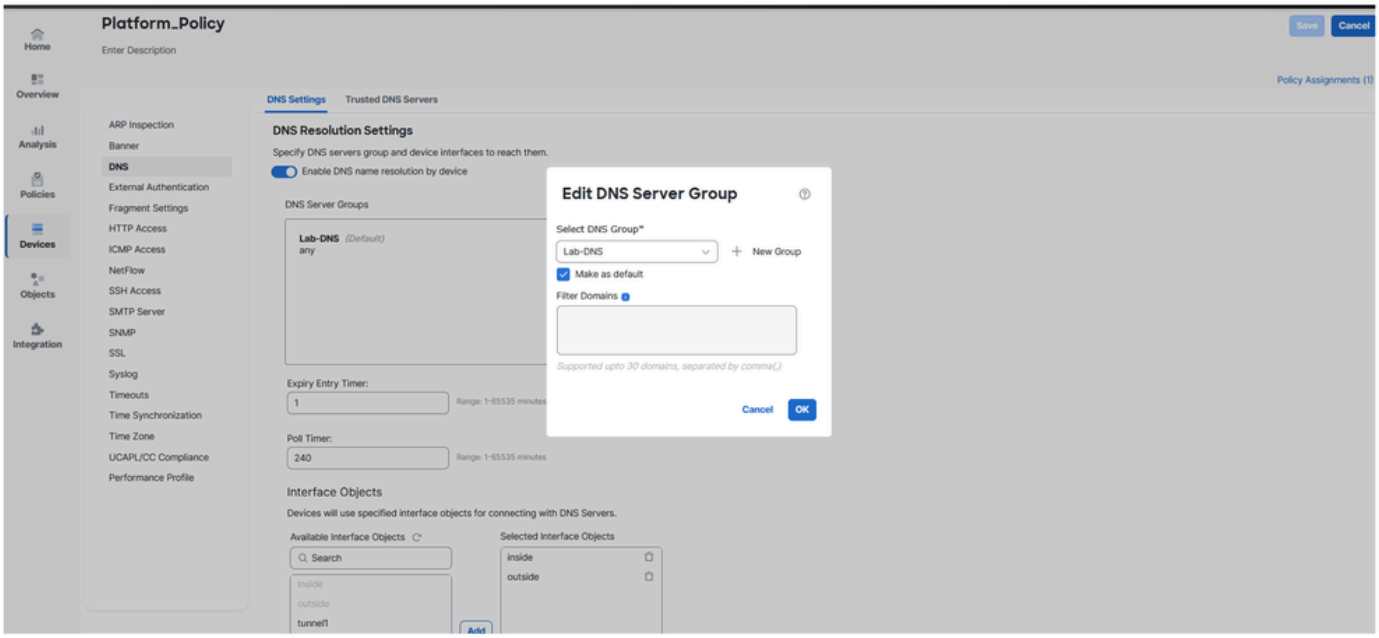
```
show run dns
```

Nel CCP:

- Fai clic suDevices>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).

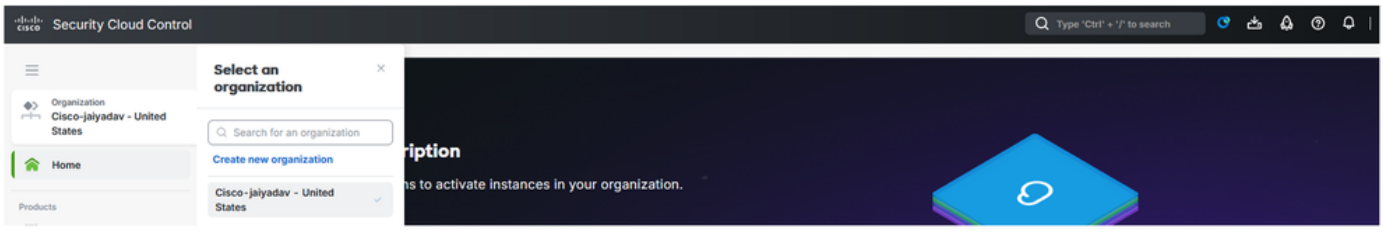
```
dns-group Lab-DNS
ftd1# ping ise.taclab.com
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.50, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
ftd1#
```

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.

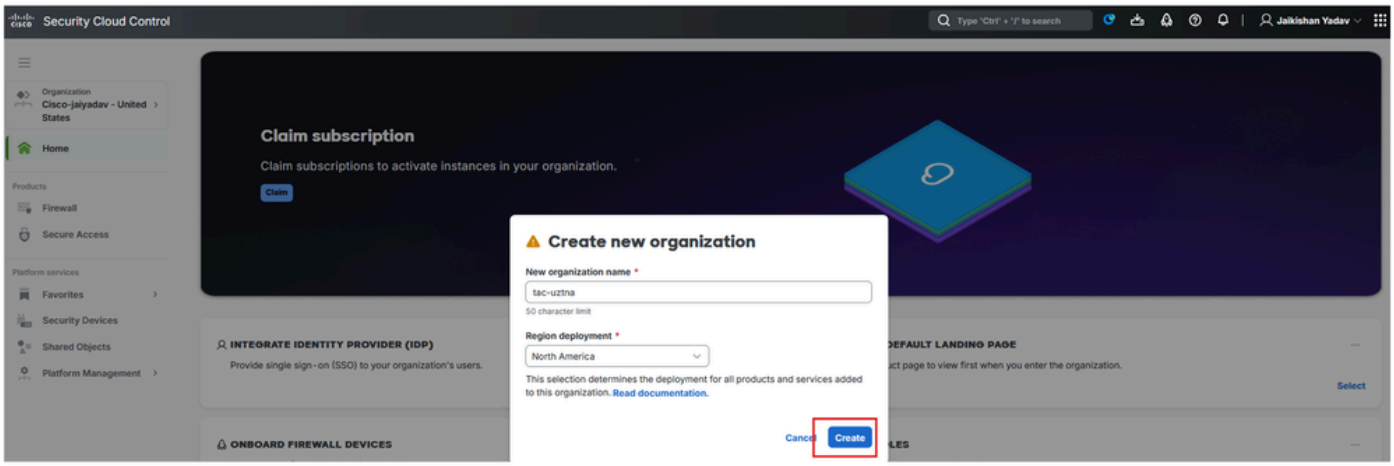
Passare a Security Cloud Control:

- Fare clic suOrganization > Create new organization



Secure Cloud Control - Organizzazione

- Fare clic su Create



Secure Cloud Control - Creazione di organizzazioni

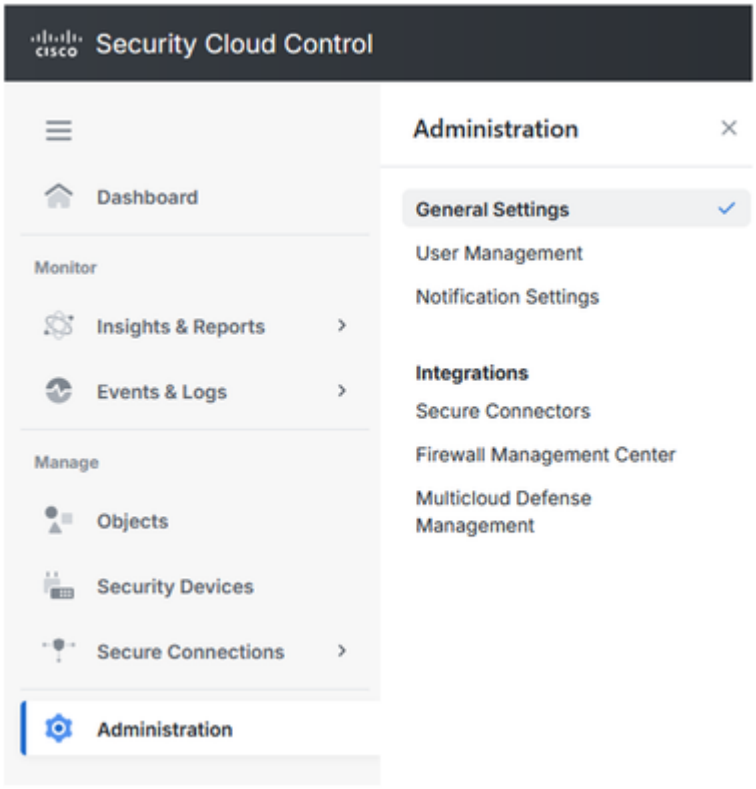
Una volta creato il tenant SCC, raccogliere le informazioni sul tenant per abilitare la microapp Firewall e accesso sicuro e per abilitare uZTNA.

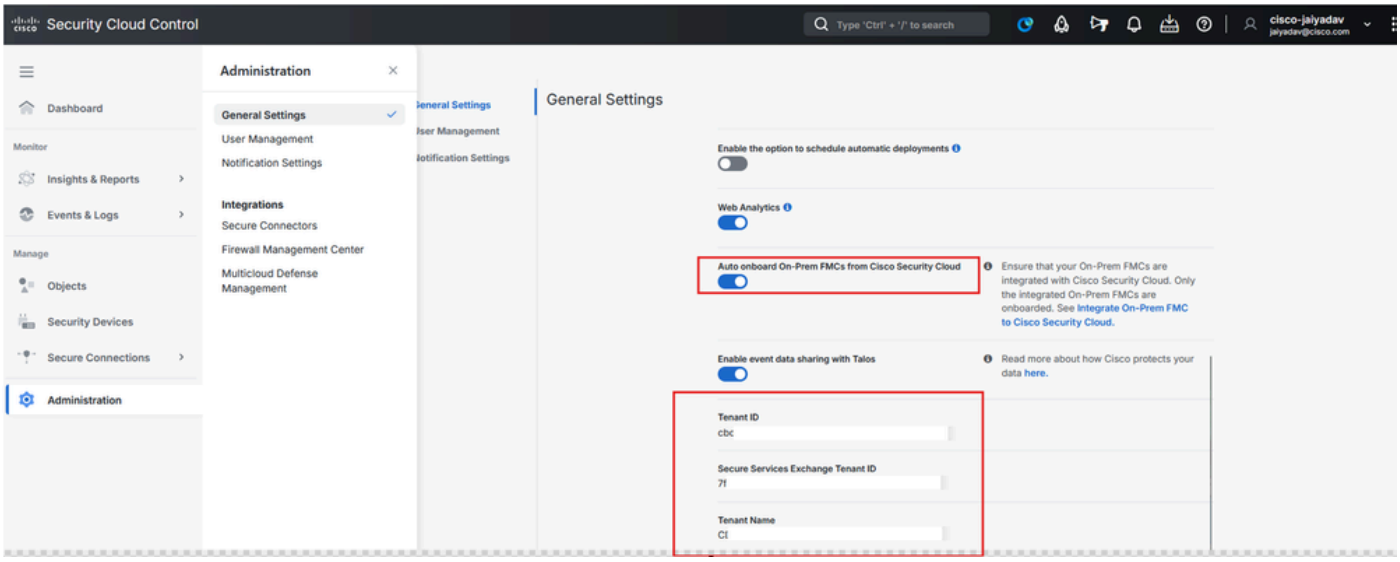
Verificare che le impostazioni generali di SCC Firewall siano configurate

Passare a CDO/SCC:

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

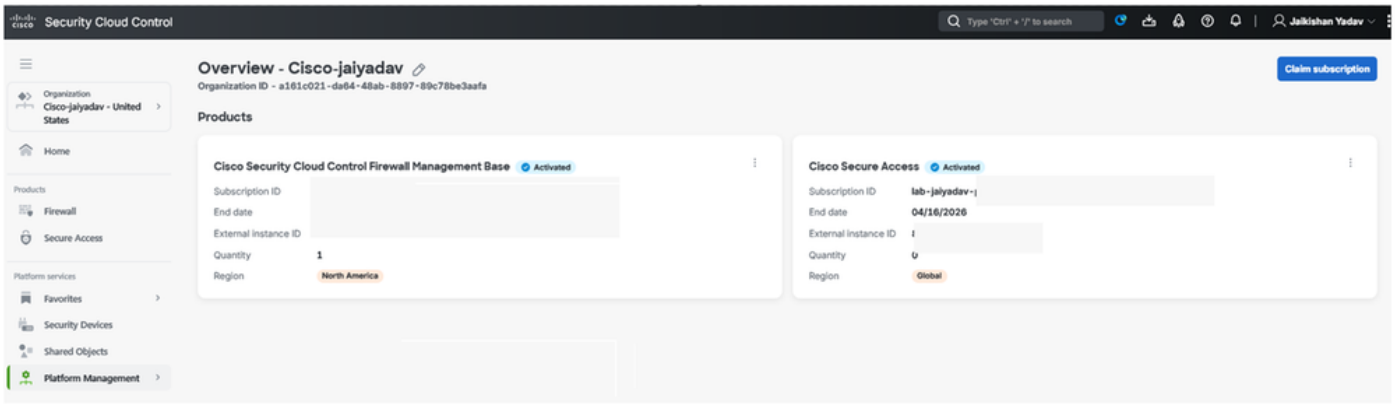
Nota: L'utente che tenta di accedere a Secure Access MicroApp deve disporre di ruoli di amministratoreSecure Accesse Security Cloud Control.





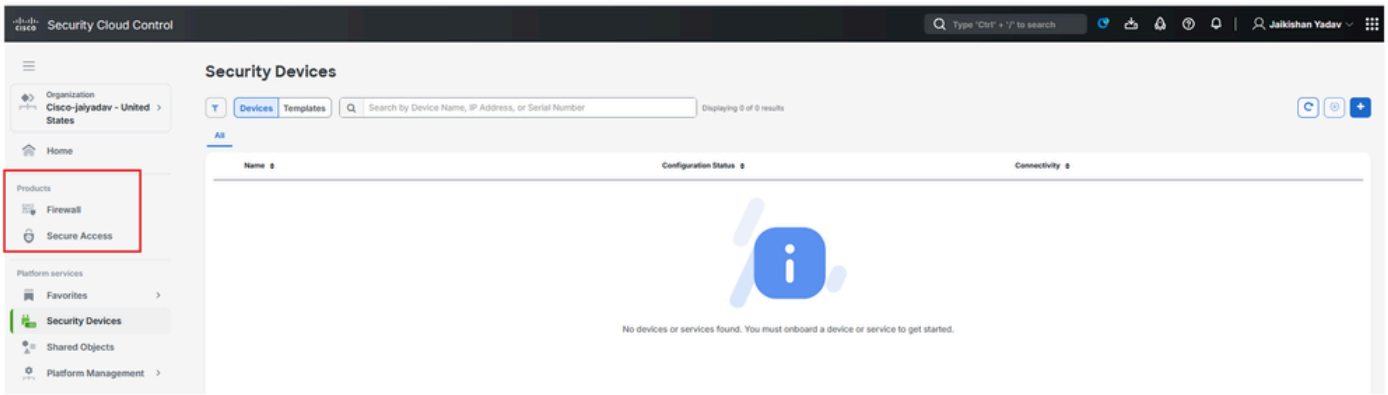
Secure Cloud Control - Dettagli organizzazione

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,expertcomando

- 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:

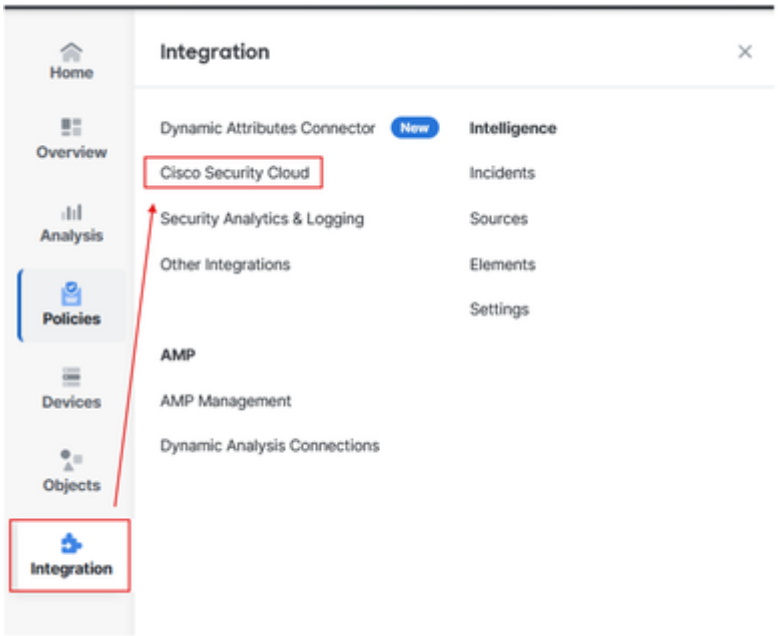
```
openssl pkcs12 -export -out ftdcert.p12 -in cert.crt -inkey cert.key
```

- Esportare il certificato utilizzando SCP o un altro strumento.

Centro gestione firewall locale integrato per Security Cloud Control

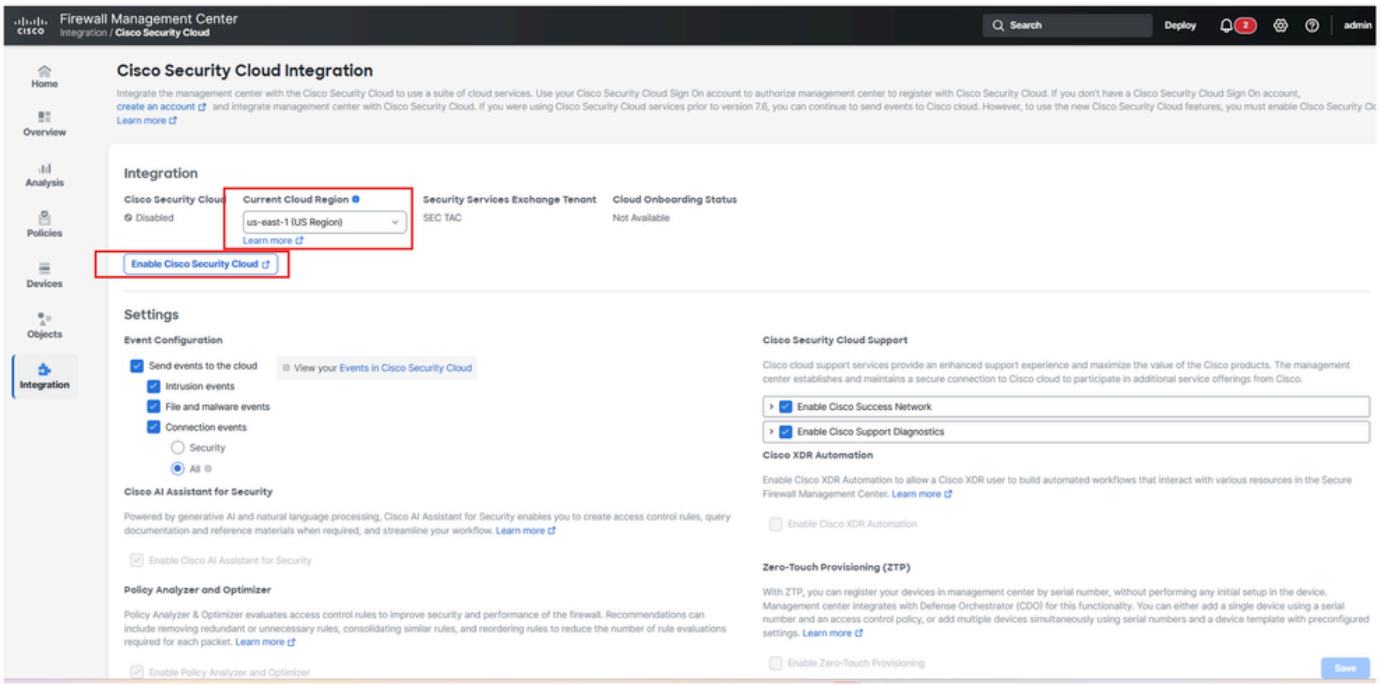
Passare al CCP:

- Fai clic suIntegration> Cisco Security Cloud



Integrazione di Centro gestione firewall e SCC

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

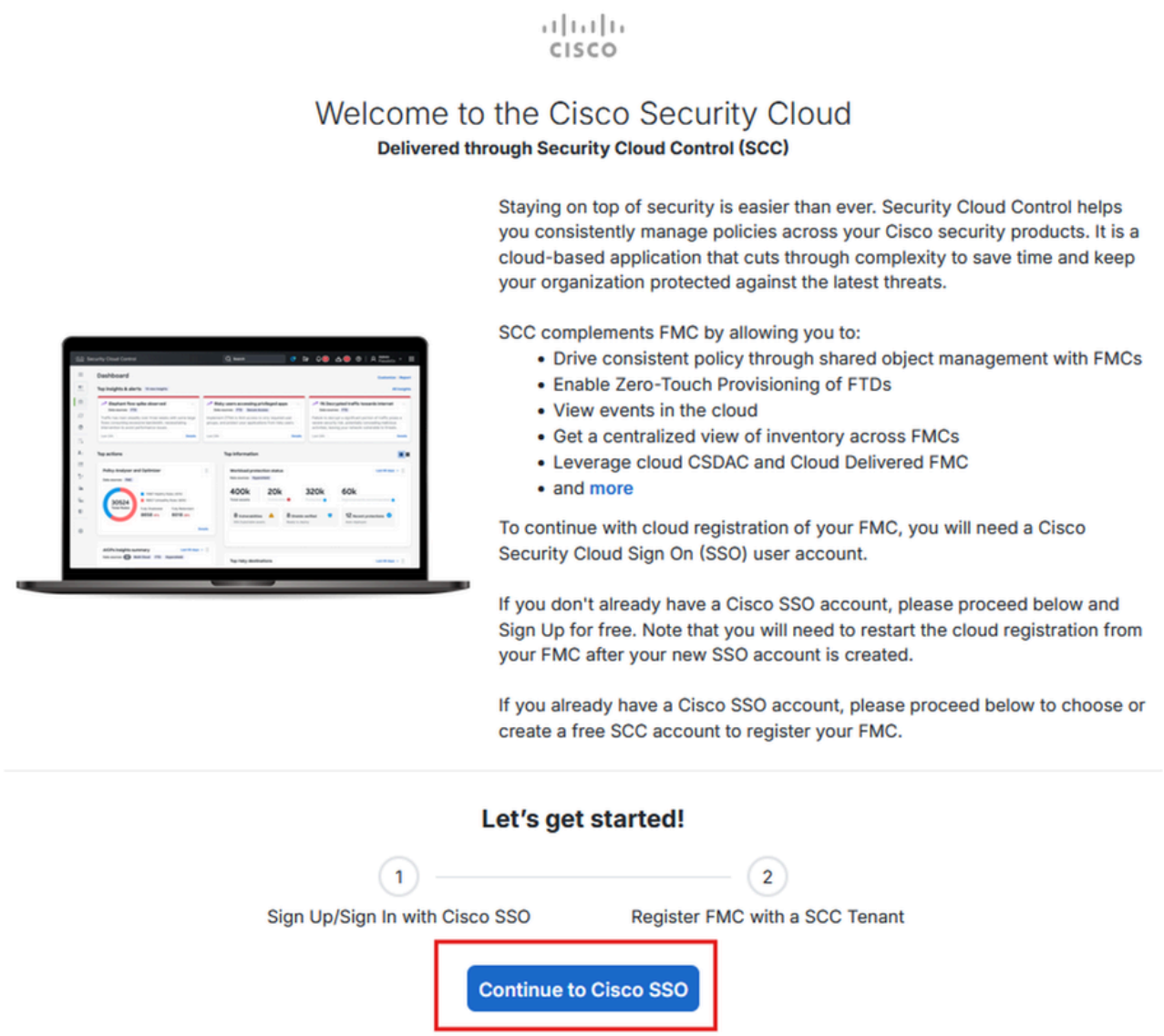


Onboarding di Firewall Management Center in SCC

Verrà aperta una nuova scheda del browser nella nuova scheda:

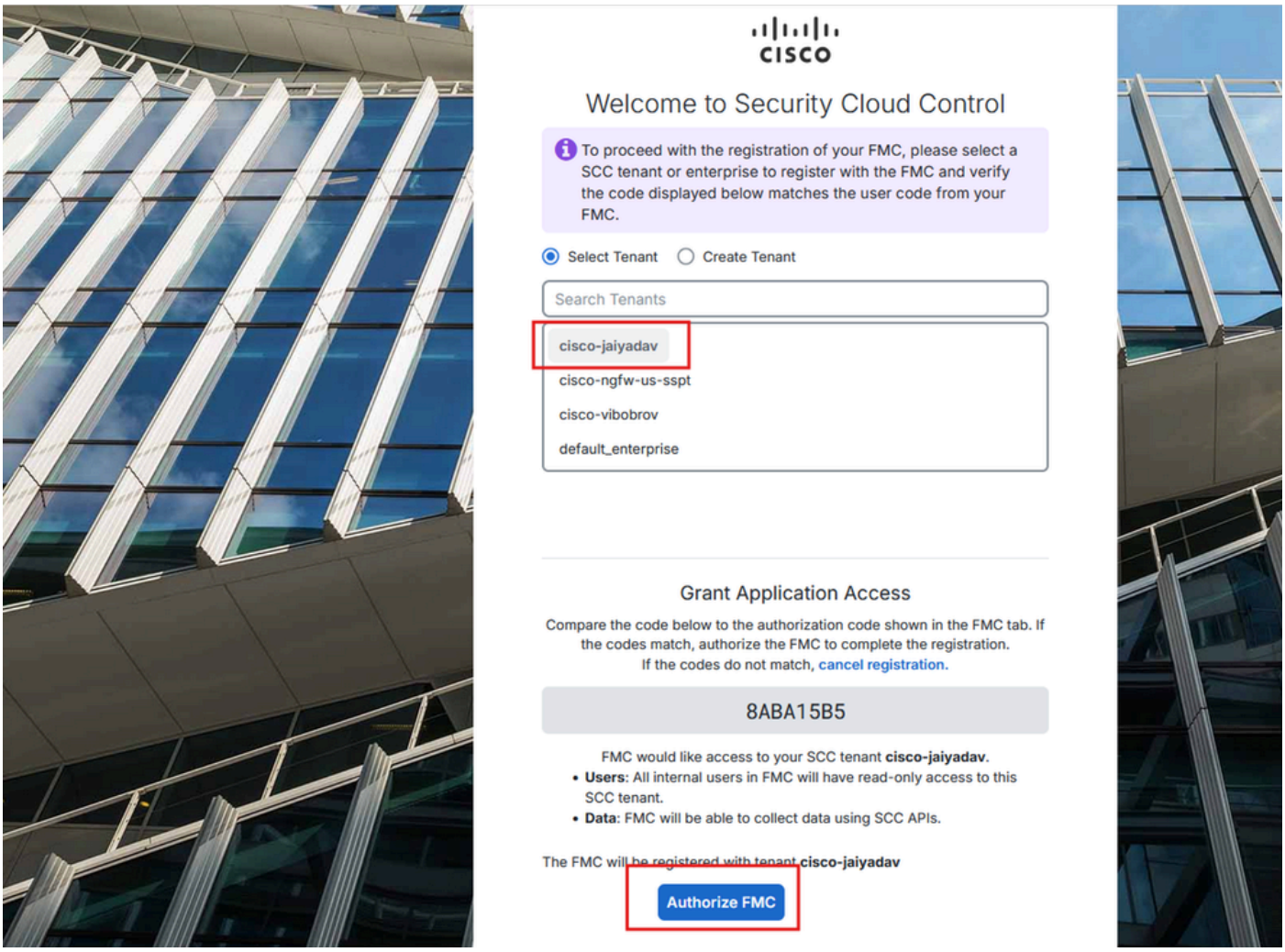
- Fare clic su Continue to Cisco SSO

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



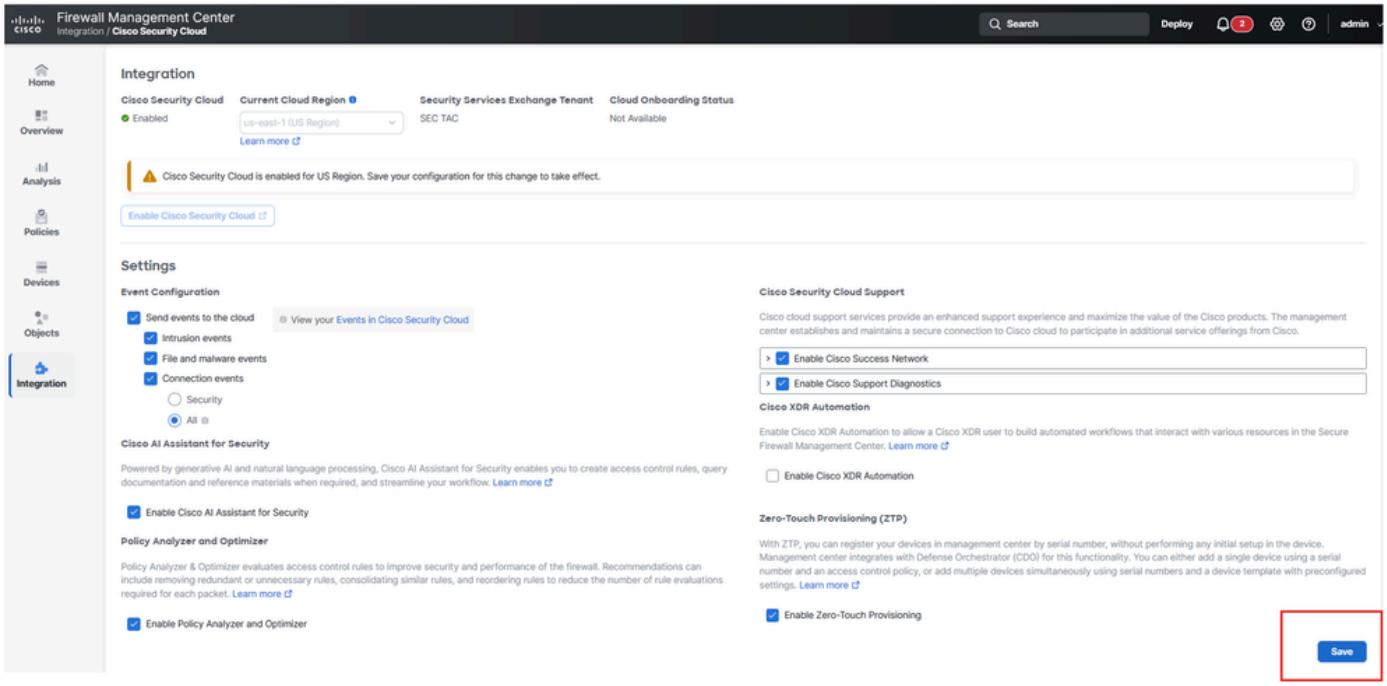
Onboarding di Firewall Management Center in SCC

- Scegliere il tenant SCC e fare clic su Authorize FMC



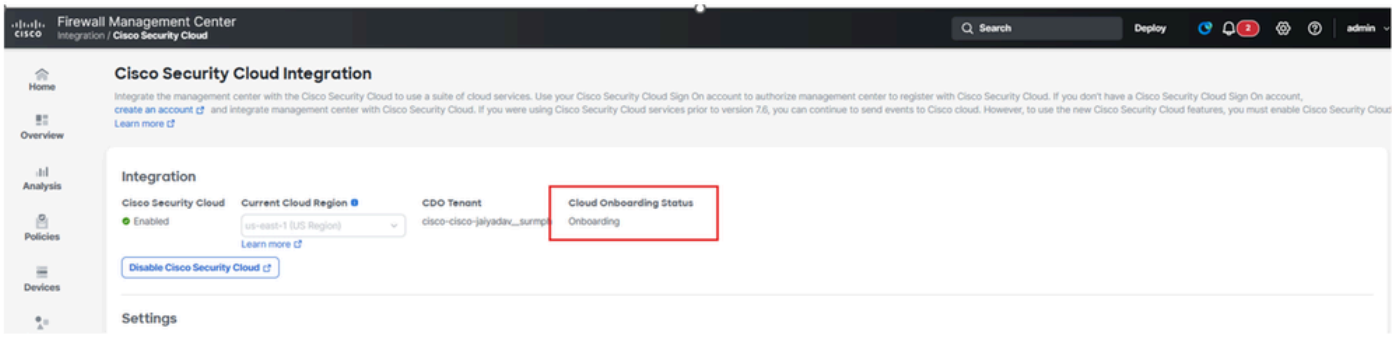
Onboarding di Firewall Management Center in SCC

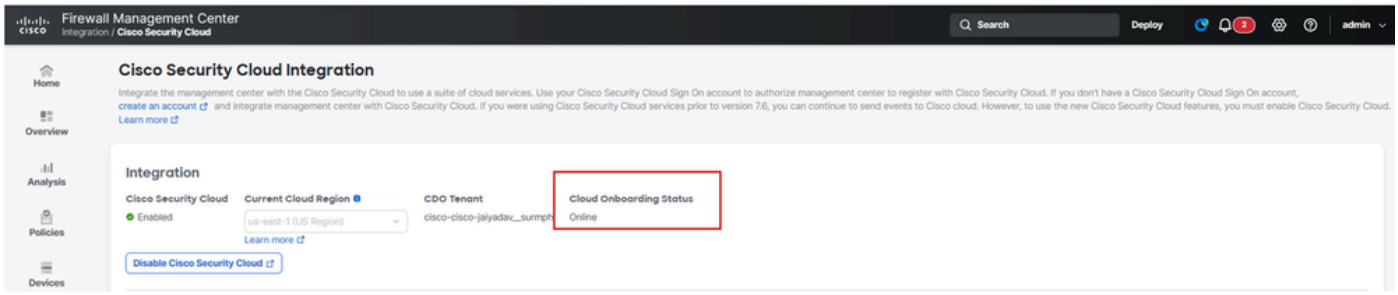
- Fare clic su Save



Onboarding di Firewall Management Center in SCC

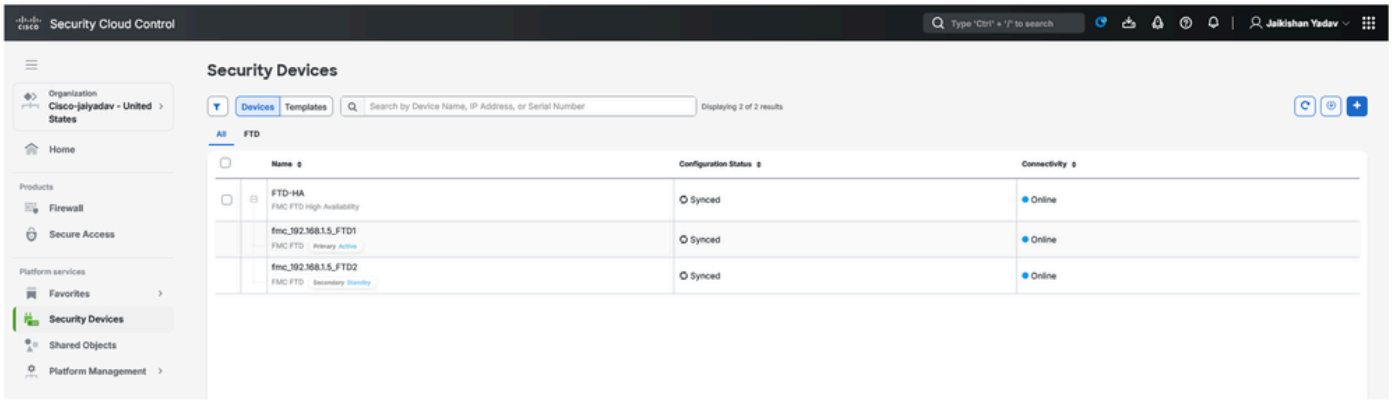
Lo stato di deve Cloud Onboarding Status essere modificato da **Not Available** a Onboarding Online.





Stato di caricamento di Centro gestione firewall

- Passare a SCC e controllare lo stato FTD inPlatform Services> Security Devices

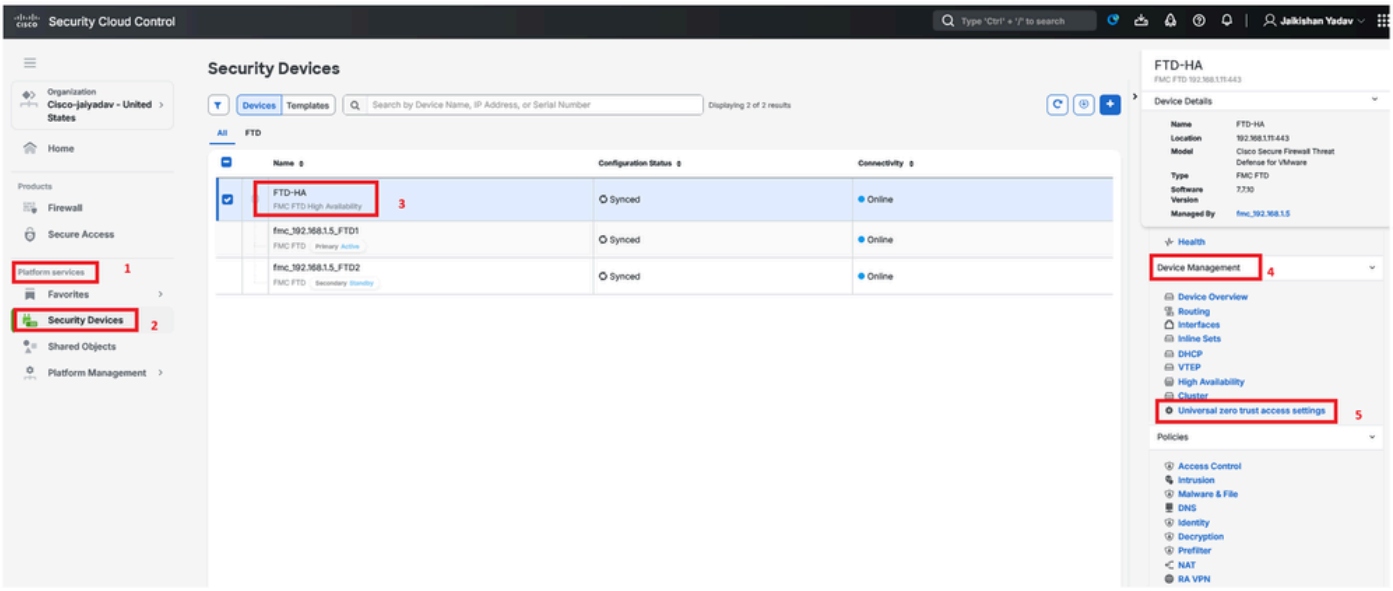


Stato di difesa dalle minacce del firewall sicuro su SCC

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

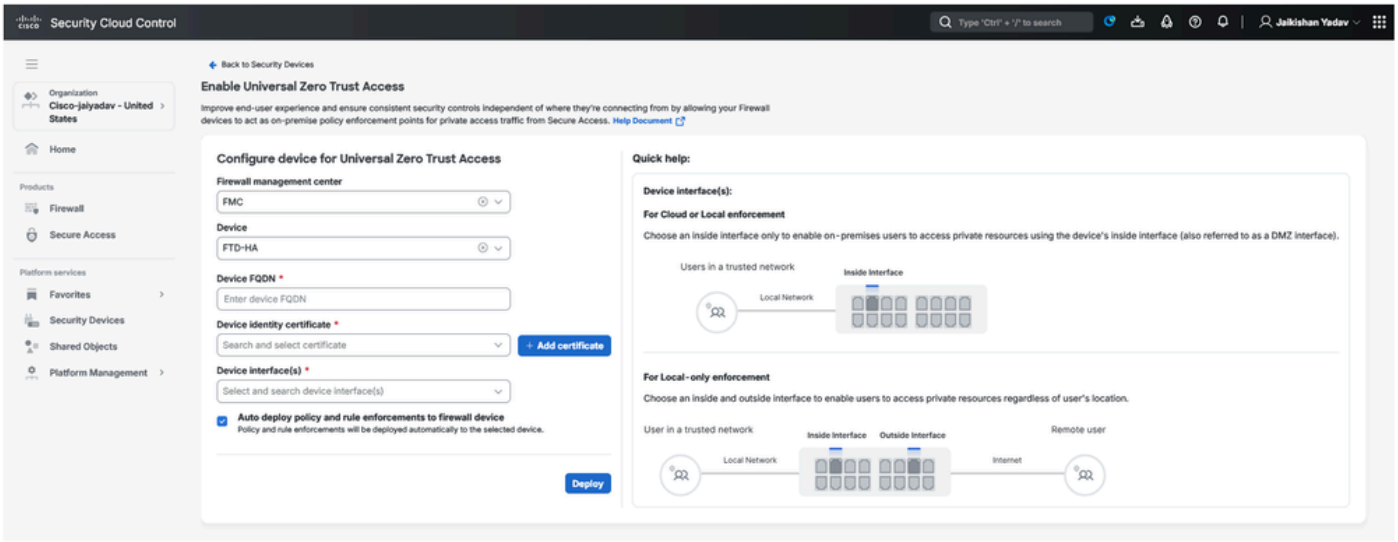
Passare a SCC:

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

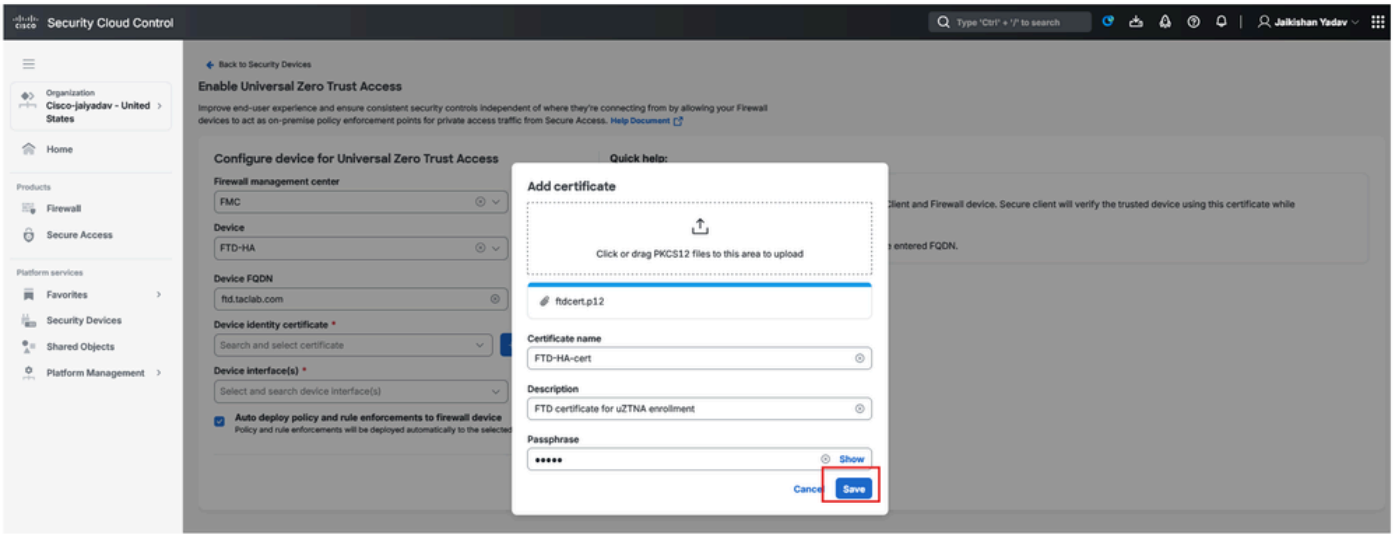


Secure Firewall Threat Defense - Configurazione ZTNA universale

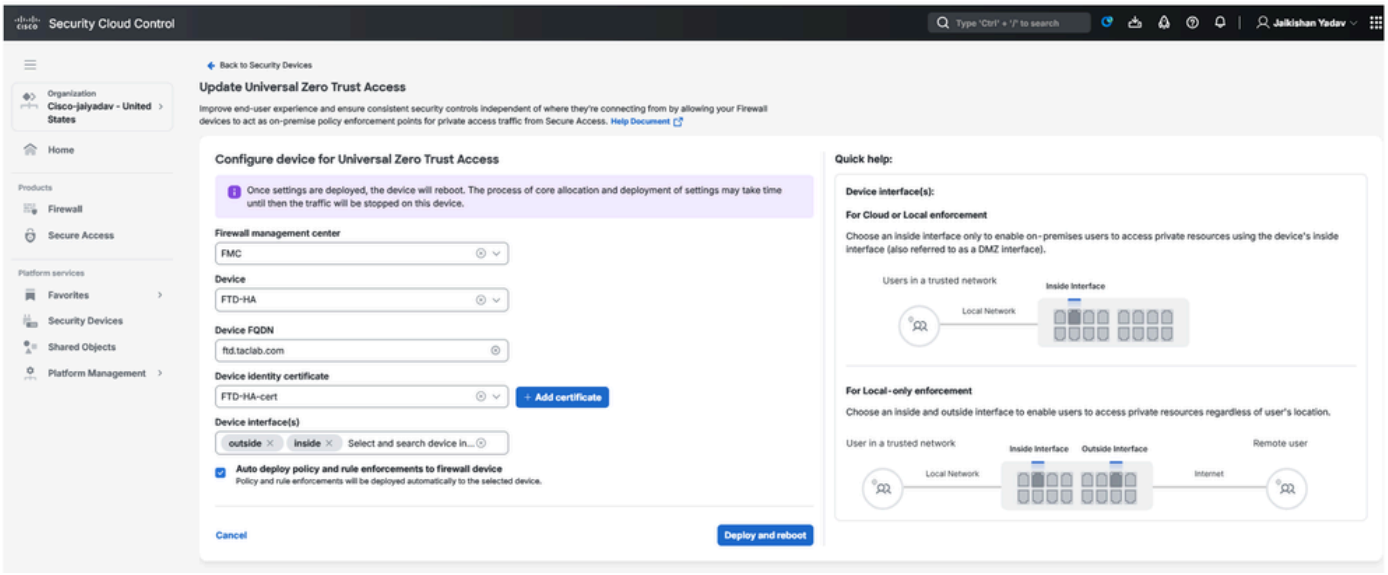
- Compilare le informazioni e caricare il certificato FTD generato nella fase [Generate Firewall Threat Defense (FTD) CA signed certificate]



Secure Firewall Threat Defense - Configurazione ZTNA universale



Secure Firewall Threat Defense - Configurazione ZTNA universale

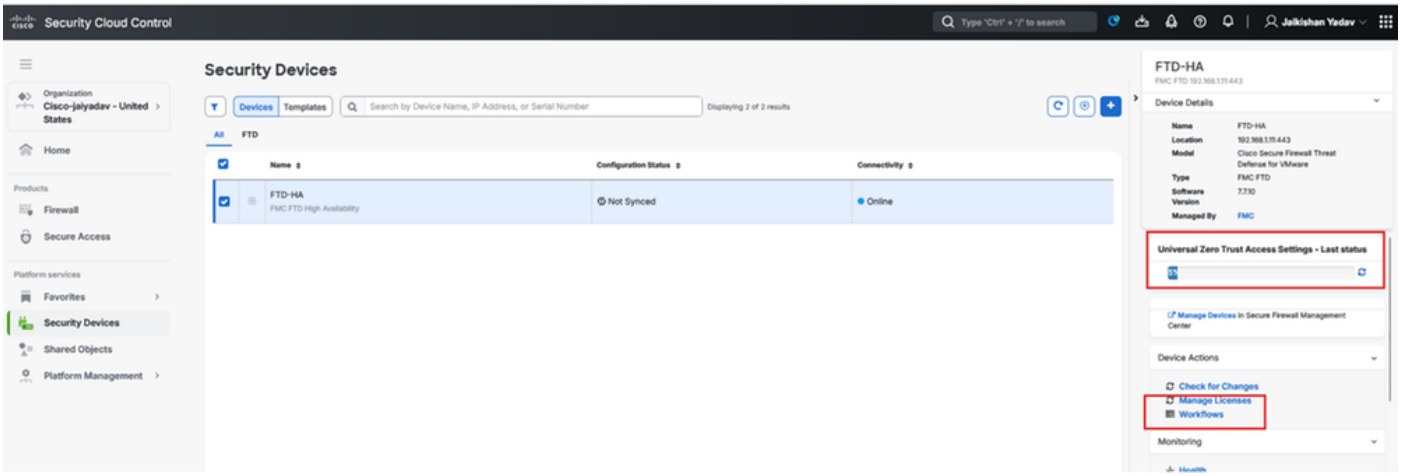


Secure Firewall Threat Defense - Configurazione ZTNA universale

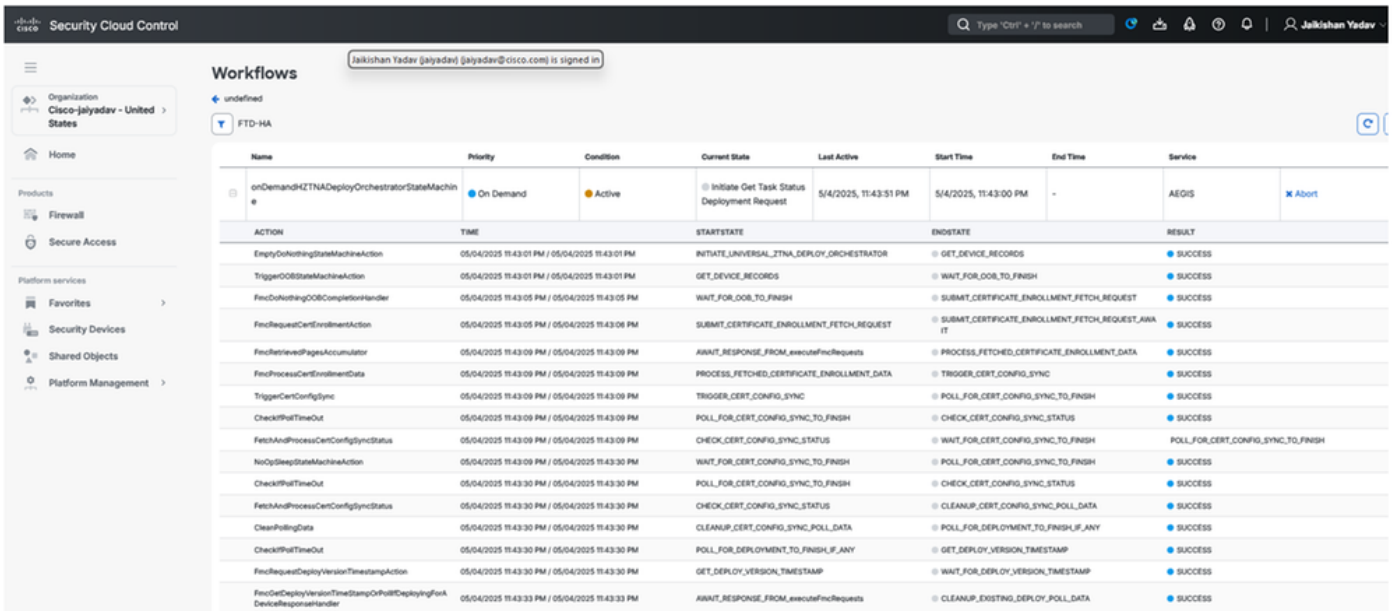
---

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

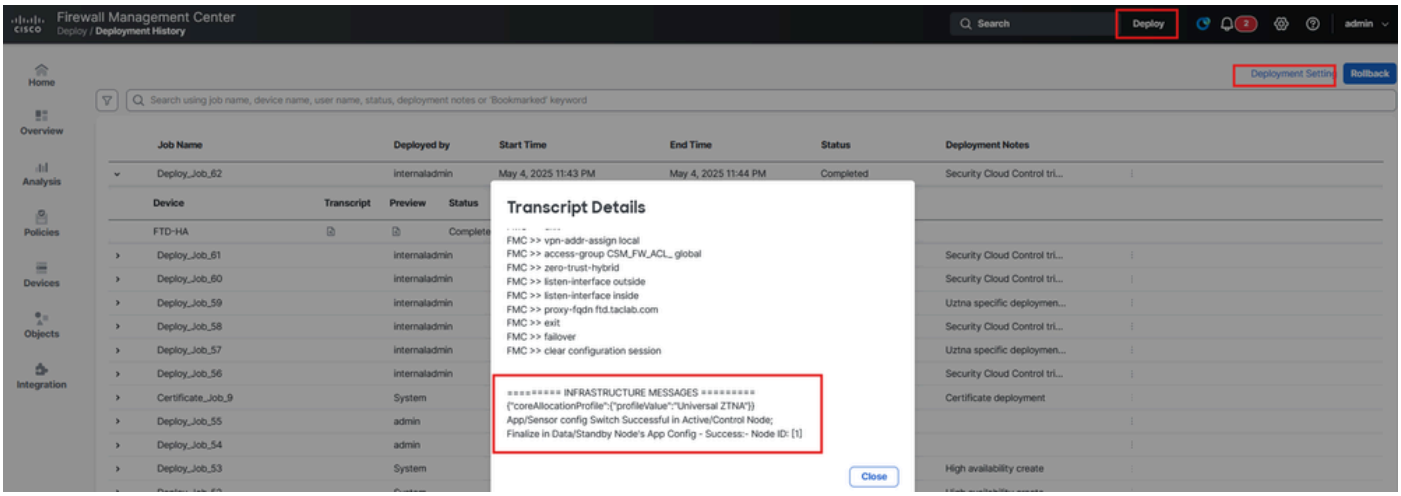


Secure Firewall Threat Defense - Stato configurazione ZTNA universale



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

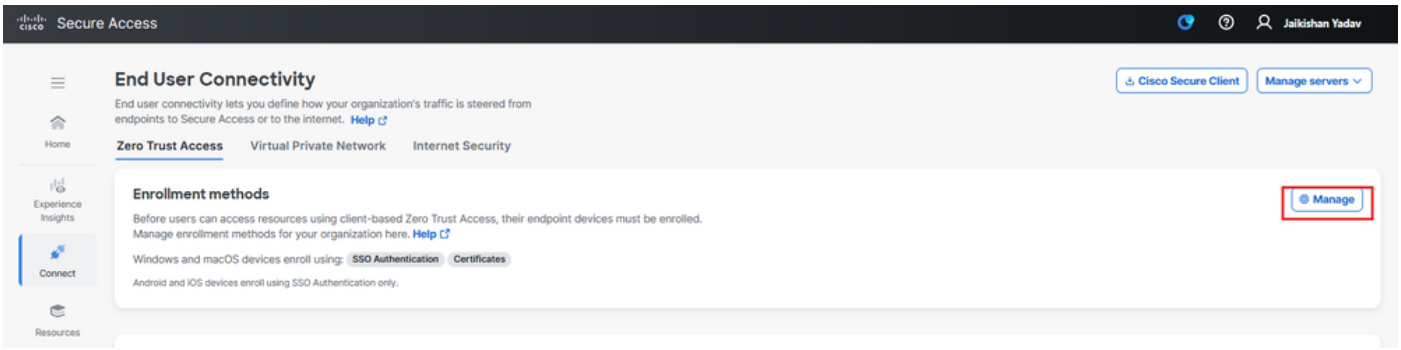
Configurazione accesso sicuro

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

---

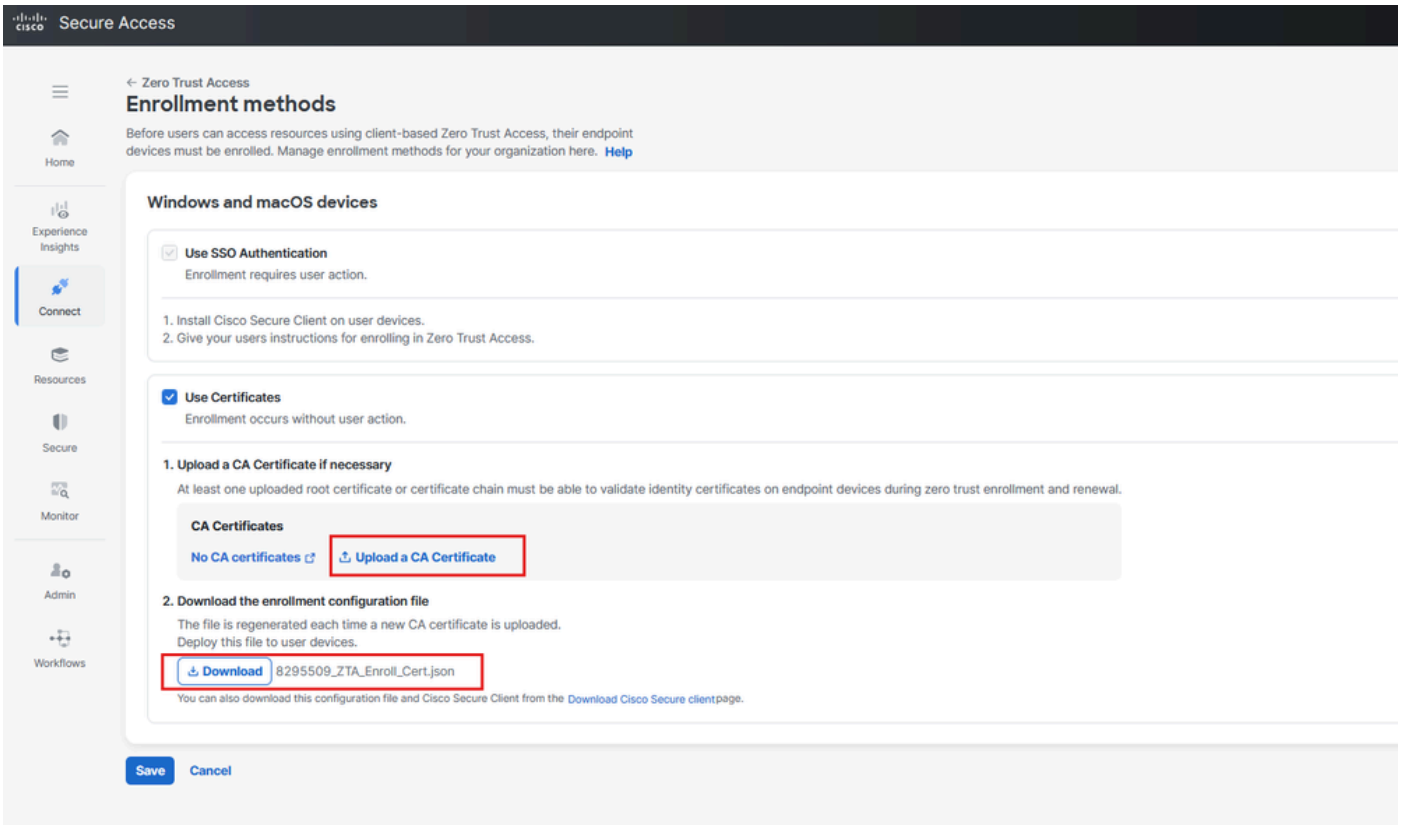
Passare a Dashboard accesso protetto:

- 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

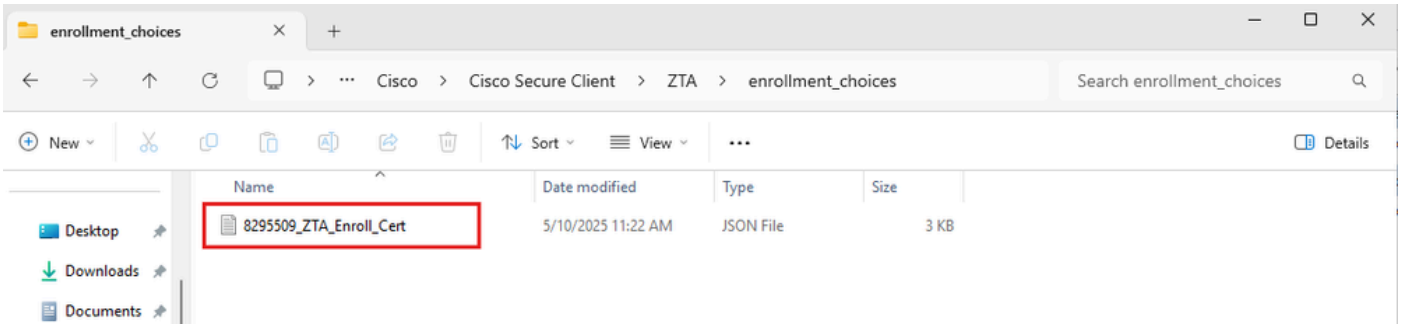


Accesso sicuro - Registrazione certificato ZTA

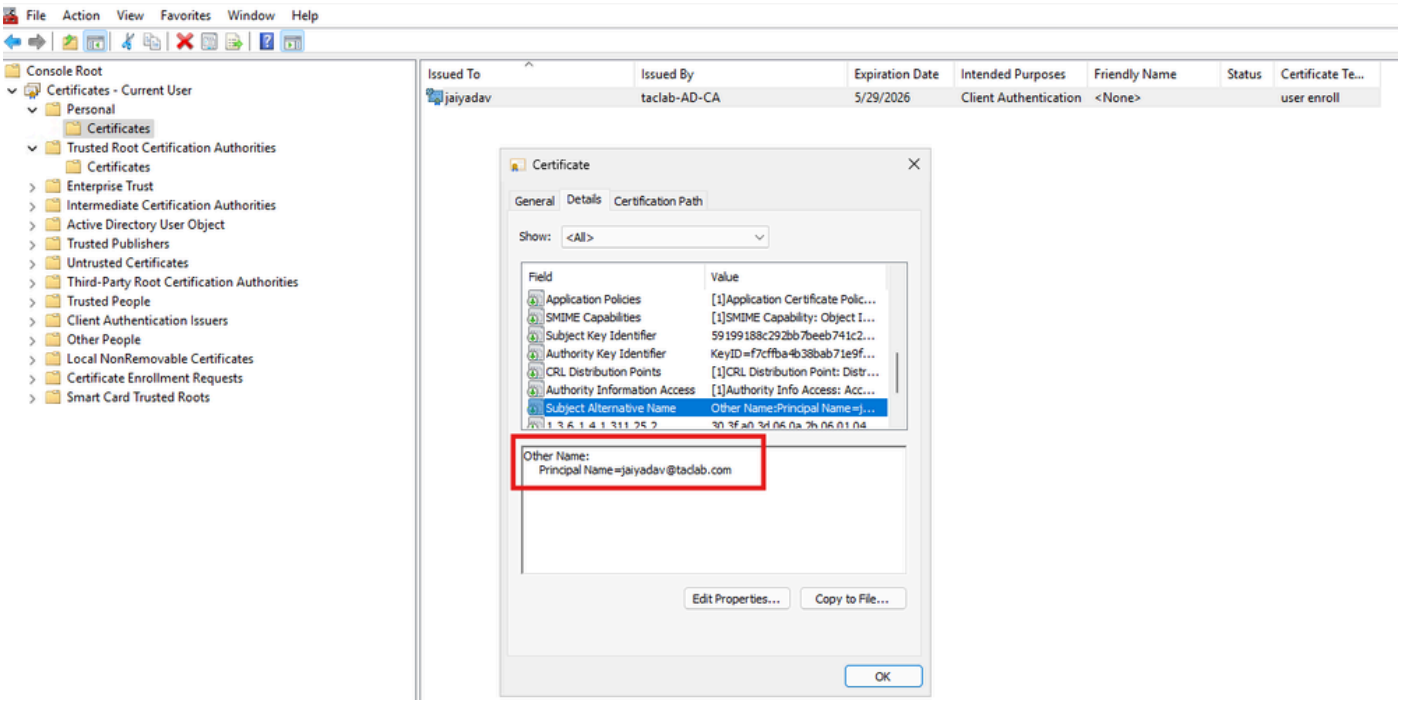
- Fare clic su Save

Configurazione client

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

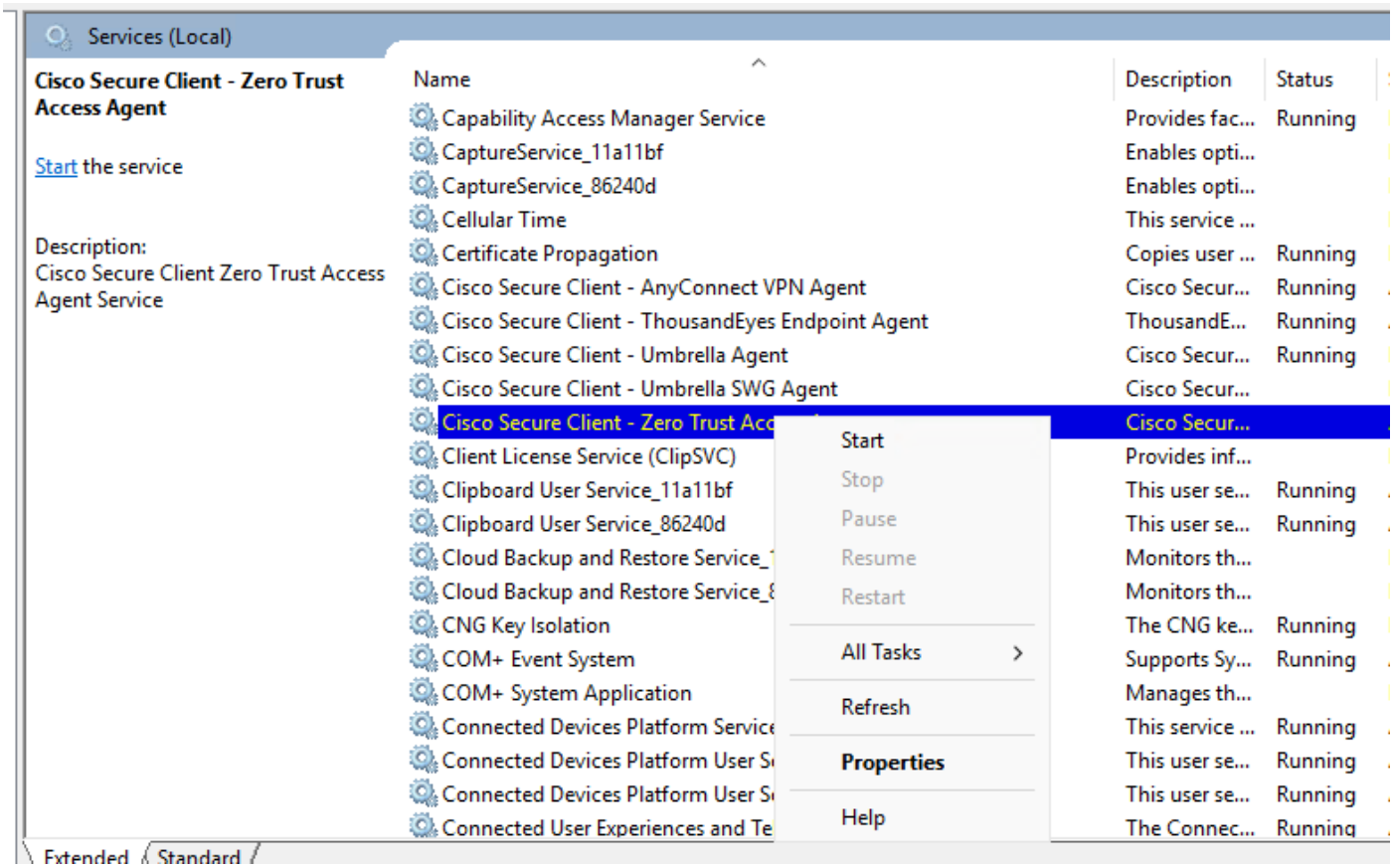


- Creare un certificato client, che deve avere un UPN nel campo SAN



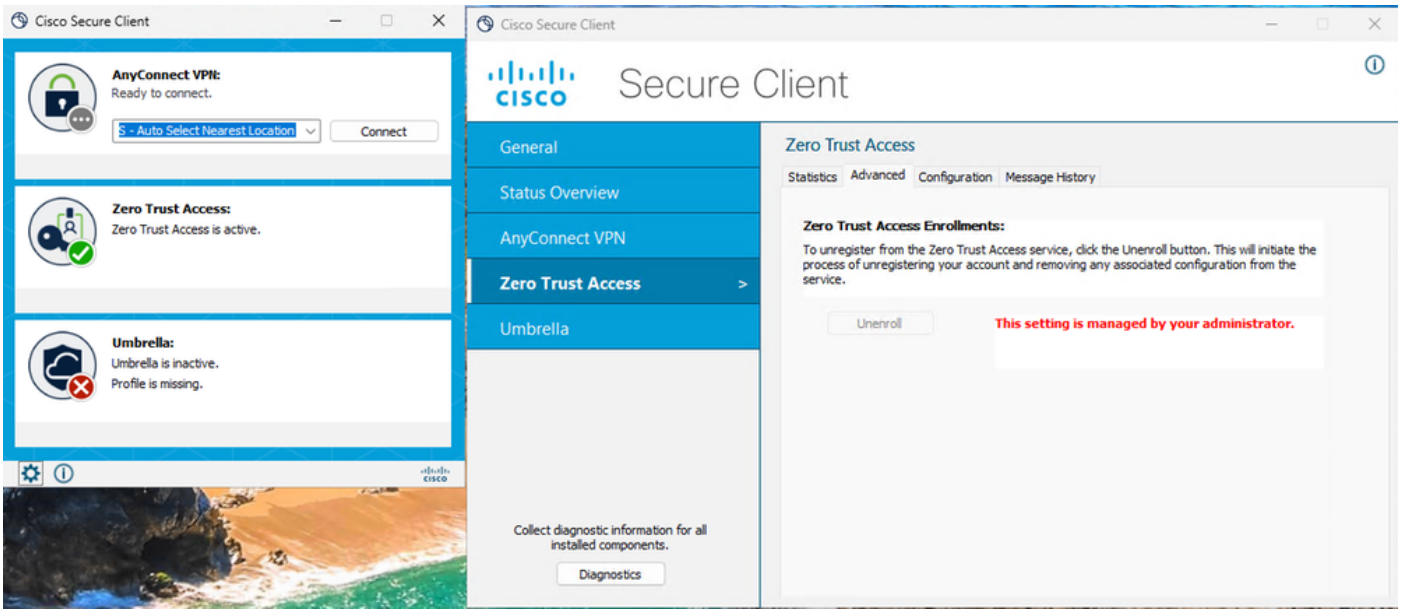
Installazione certificato

- 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).