Konfigurieren von sicherem Zugriff für universelles ZTNA mit vor Ort verwaltetem FMC auf SCC

Inhalt

Einleitung

Dieses Dokument beschreibt die Konfiguration von ZTNA mit sicherem Zugriff und virtuellem FTD, das von einem virtuellen FMC vor Ort verwaltet wird.

Voraussetzungen

- Firewall Management Center (FMC) und Firewall Threat Defense (FTD) müssen mit der Softwareversion 7.7.10 oder höher bereitgestellt werden.

- Firewall Threat Defense (FTD) muss von Firewall Management Center (FMC) verwaltet werden.
- Firewall Threat Defense (FTD) muss mit Verschlüsselung (starke Verschlüsselung muss bei aktivierter Exportfunktion aktiviert sein), IPS- und Threat-Lizenzen für Sicherheitskontrollen lizenziert werden
- Die Basiskonfiguration der Firewall Threat Defense (FTD) muss über das Firewall Management Center (FMC) erfolgen, z. B. Schnittstelle, Routing usw.
- Die DNS-Konfiguration muss auf das Gerät von FMCs angewendet werden, um den FQDN der App aufzulösen.
- Version 5.1.10 oder höher für Cisco Secure Client erforderlich
- Sicherheit Cloud-Kontrolle wird Kunden mit aktivierter Firewall und sicheren Zugriffs-Mikroanwendungen und UZTNA-Funktionsmarkierungen bereitgestellt

Anforderungen

- Auf allen Secure Firewall Management Center (FMC)-Geräten, einschließlich cdFMC- und Firewall Threat Defense (FTD)-Geräten, muss die Softwareversion 7.7.10 oder höher ausgeführt werden.
- Firewall Threat Defense (FTD) muss von Firewall Management Center verwaltet werden. Lokaler Manager Firewall Defense Manager (FDM) wird nicht unterstützt
- Alle FTD-Geräte (Firewall Threat Defense) müssen für den Routing-Modus konfiguriert sein. Der transparente Modus wird nicht unterstützt.
- Cluster-Geräte werden nicht unterstützt.
- Hochverfügbarkeitsgeräte werden unterstützt. werden sie als eine Einheit angezeigt.
- Secure Client Version 5.1.10 oder höher

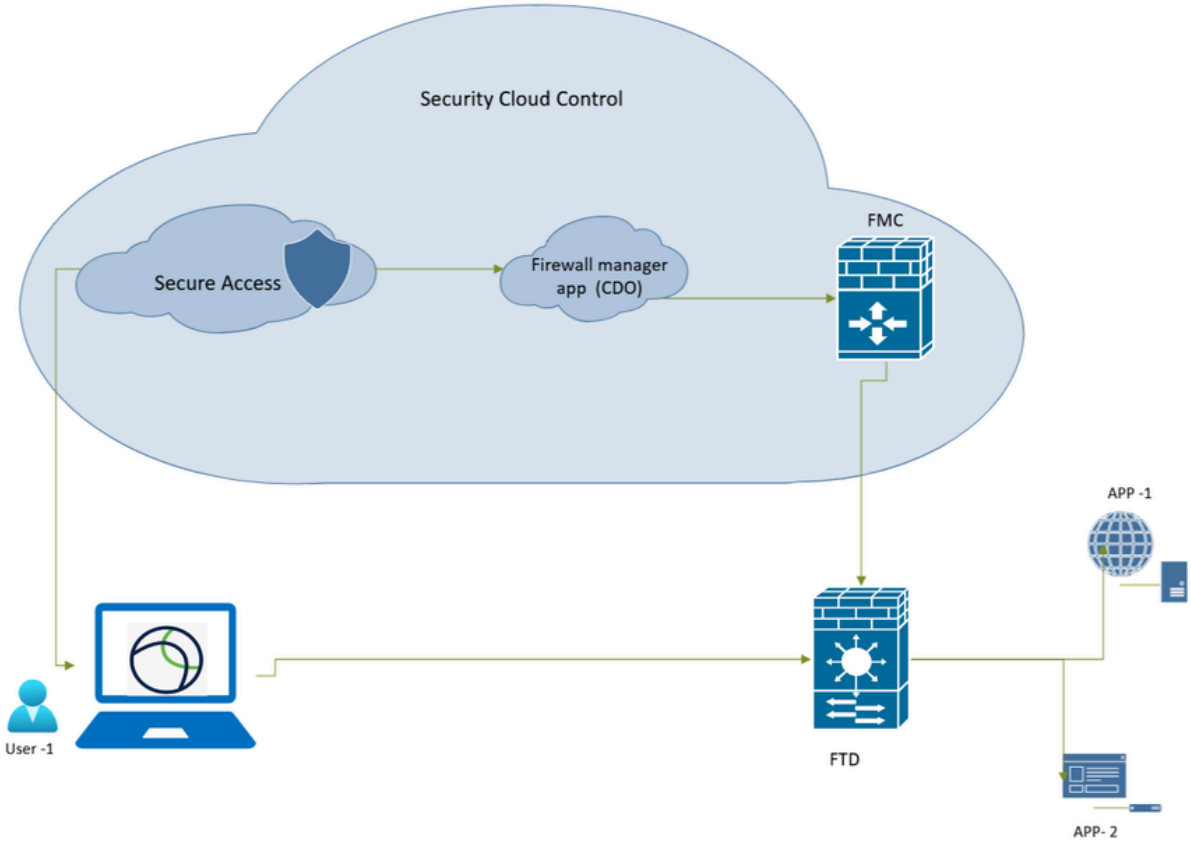
Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf

- Security Cloud Control (SCC)
- Secure Firewall Management Center (FMC) Version 7.7.10
- Secure Firewall Threat Defense (FTD) virtual -100 Version 7.7.10
- Secure Client für Windows Version 5.1.10
- Sicherer Zugriff

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Netzwerkdiagramm



Sicherer Zugriff - Netzwerktopologie

Informationen zu Haltestellen

Unterstützte Geräte

Unterstützte Modelle für sicheren Schutz vor Bedrohungen durch Firewalls:

- PR 1150
- FPR 3105 3110 3120 3130 3140
- FPR4115,4125,4145,4112
- FPR4215,4225,4245
- Firewall Threat Defense (FTD) virtuell mit mindestens 16 CPU-Kernen

Einschränkungen

- Objektfreigabe
- IPv6 wird nicht unterstützt.
- Nur globale VRF-Instanzen werden unterstützt.
- Universelle ZTNA-Richtlinien werden für den standortübergreifenden Tunnelverkehr zu einem Gerät nicht durchgesetzt.
- Cluster-Geräte werden nicht unterstützt.

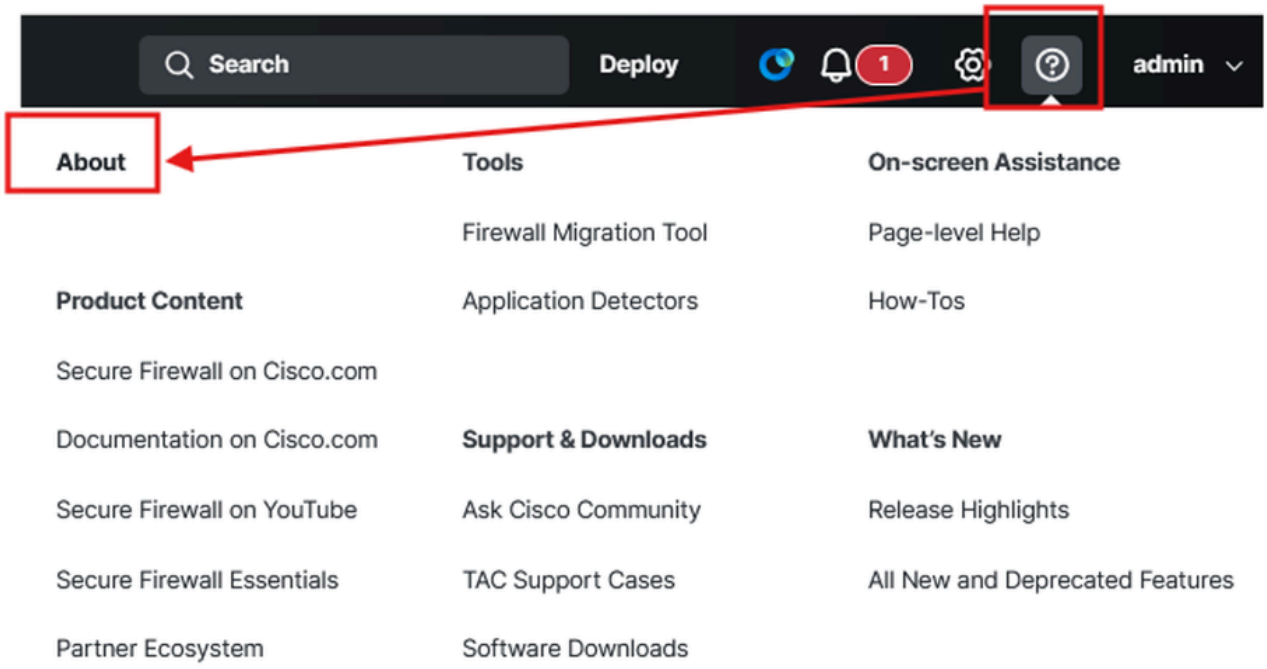
- FTDs, die als Container auf Firepower-Serien der Serien 4000 und 9000 bereitgestellt werden, werden nicht unterstützt
- Universelle ZTNA-Sitzungen unterstützen keine Jumbo Frames.

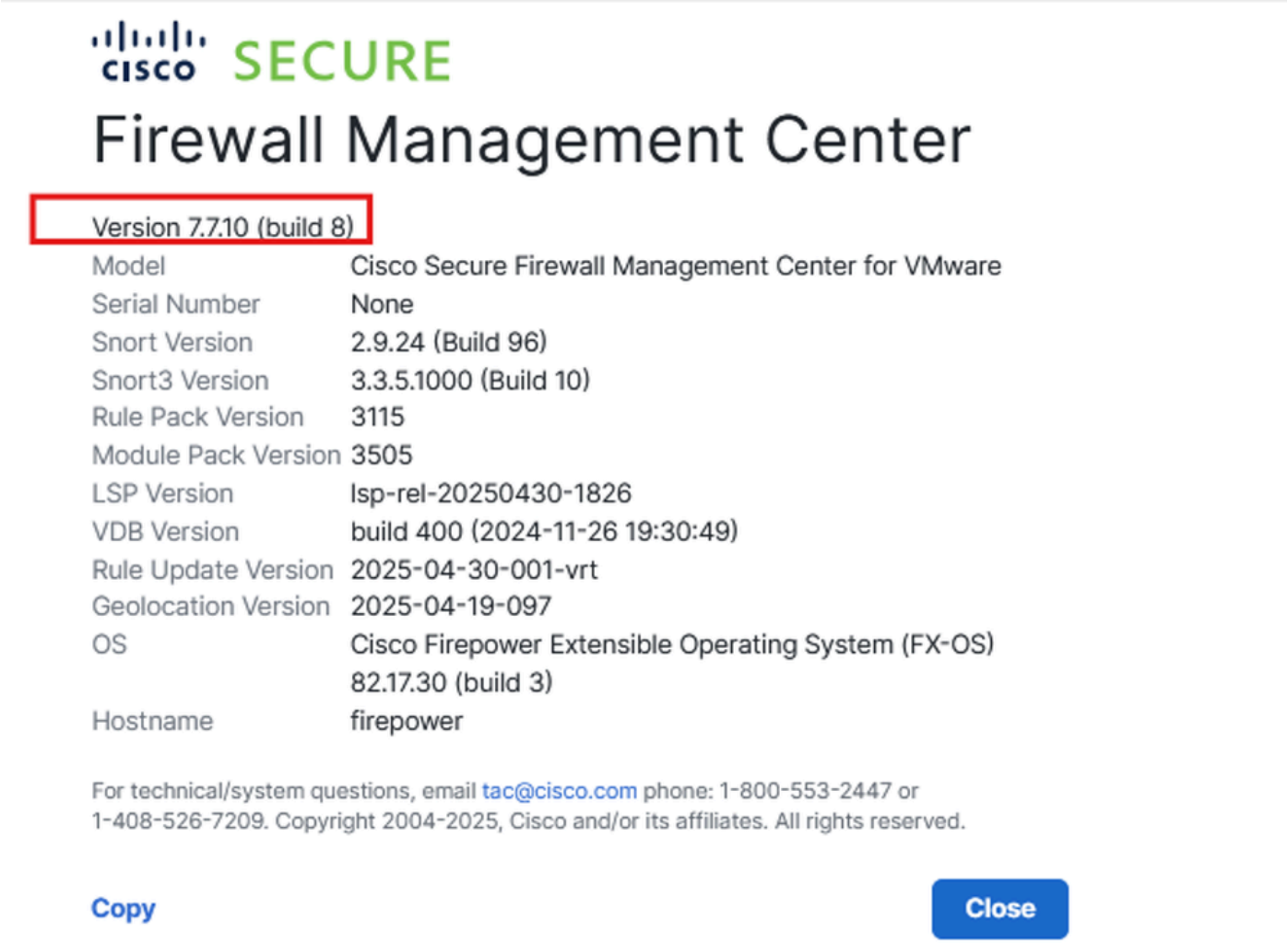
Konfigurieren

FMC-Version überprüfen

Überprüfen Sie, ob Firewall Management Center und Firewall FTD auf der unterstützten Softwareversion für Universal ZTNA (kann 7.7.10 oder höher sein) ausgeführt werden:

- Klicke auf ?(rechte obere Ecke) und klicke auf About



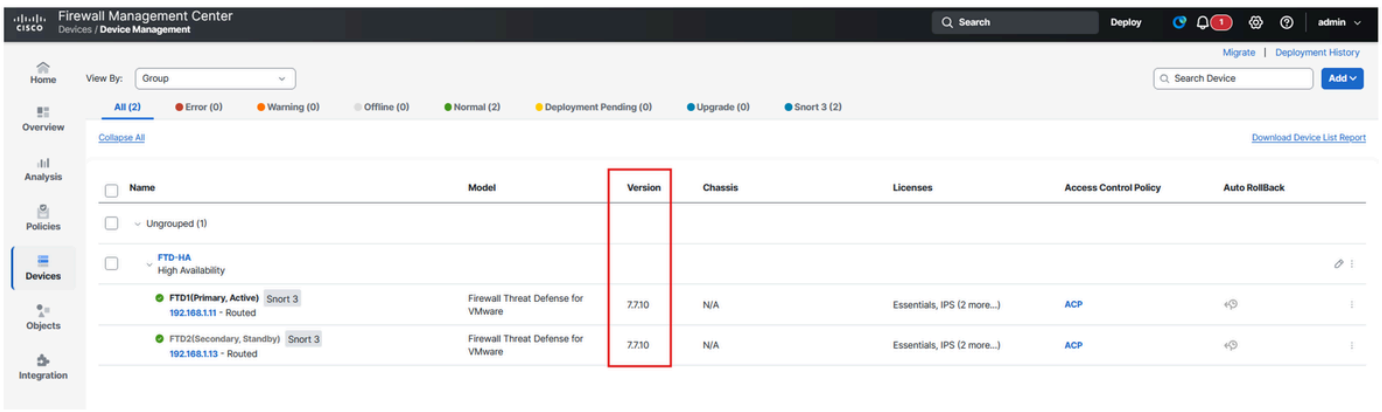


Secure Firewall Management Center - Softwareversion

FTD-Version überprüfen

Navigieren Sie zur FMC-Benutzeroberfläche:

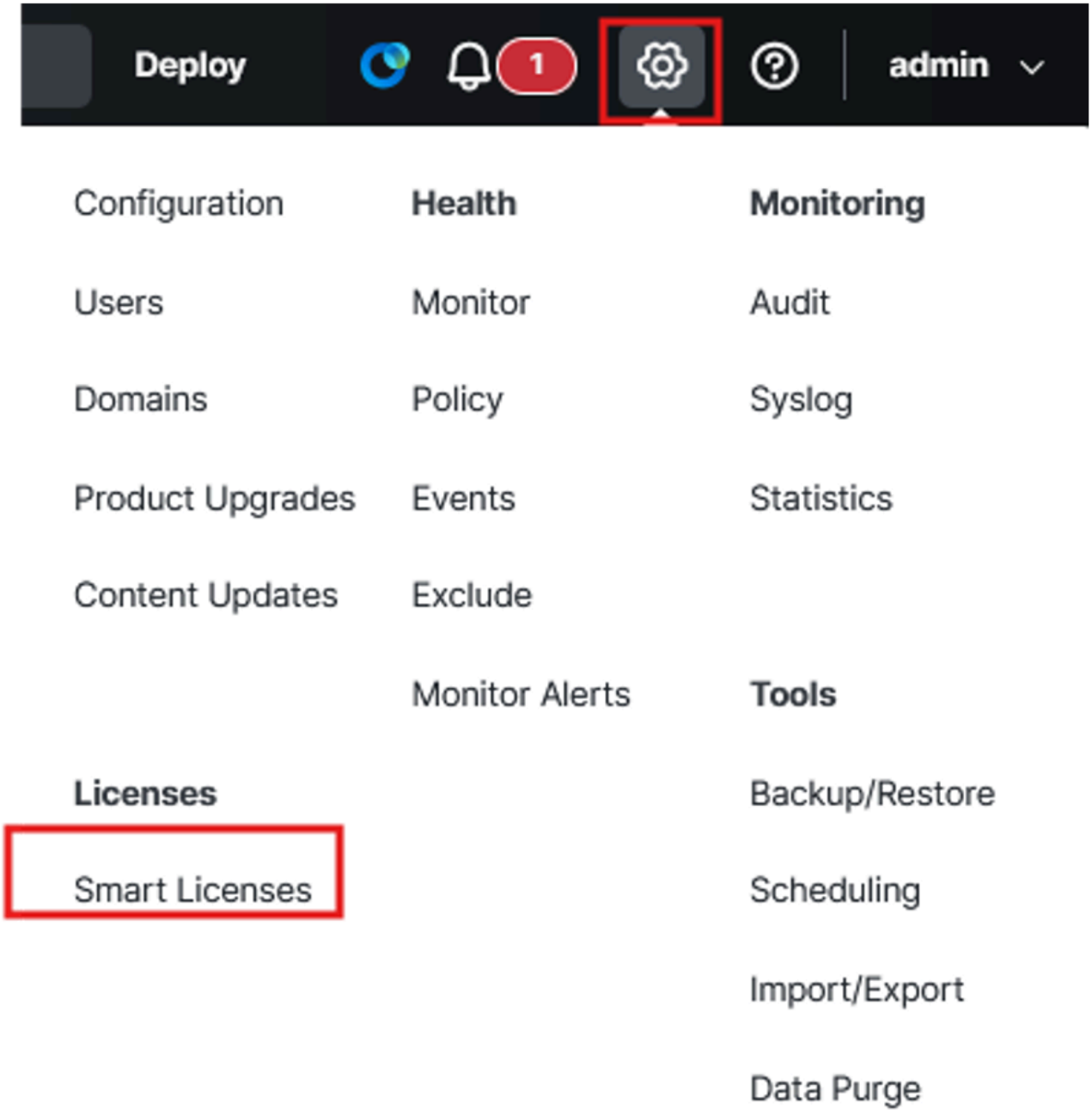
- AufDevices> Device Management

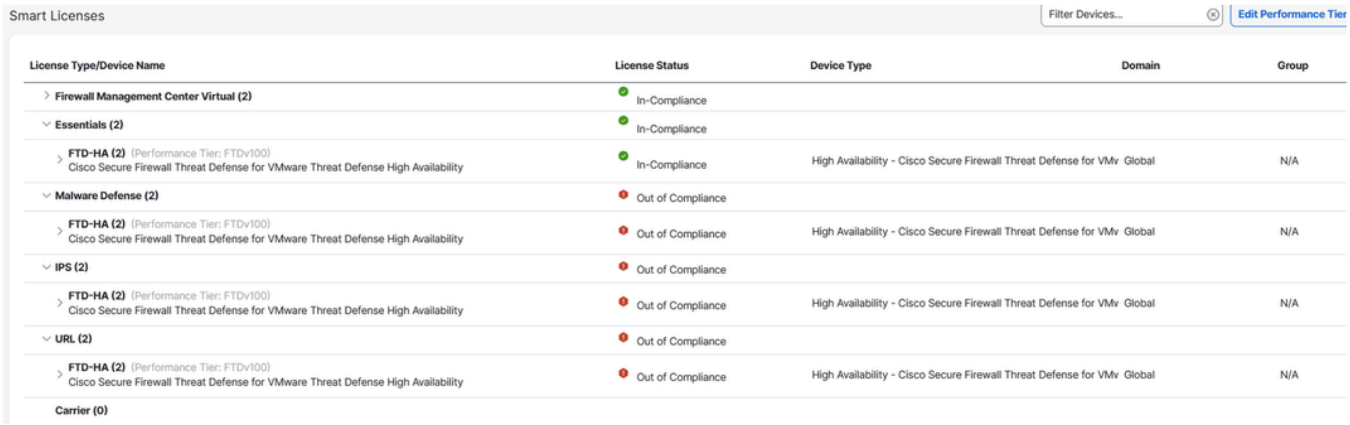


Sichere Firewall-Abwehr - Softwareversion

FTD-Lizenzen überprüfen

- Klicken Sie auf Setting Icon > Licenses> Smart Licenses





Sichere Firewall-Bedrohungsabwehr - Smart Licenses

Überprüfen Sie die Plattformeinstellungen und den ordnungsgemäß konfigurierten DNS.

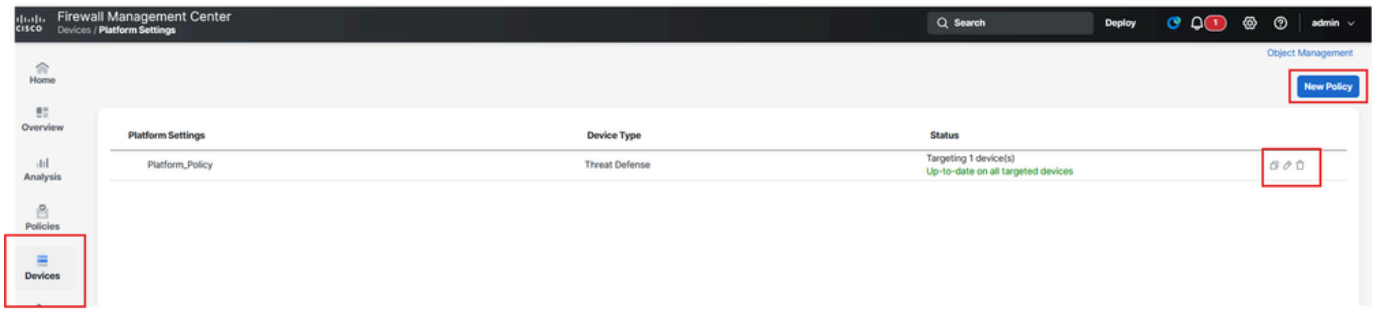
Anmeldung beim FTD über CLI:

- Führen Sie den Befehl aus, um zu überprüfen, ob DNS konfiguriert ist:

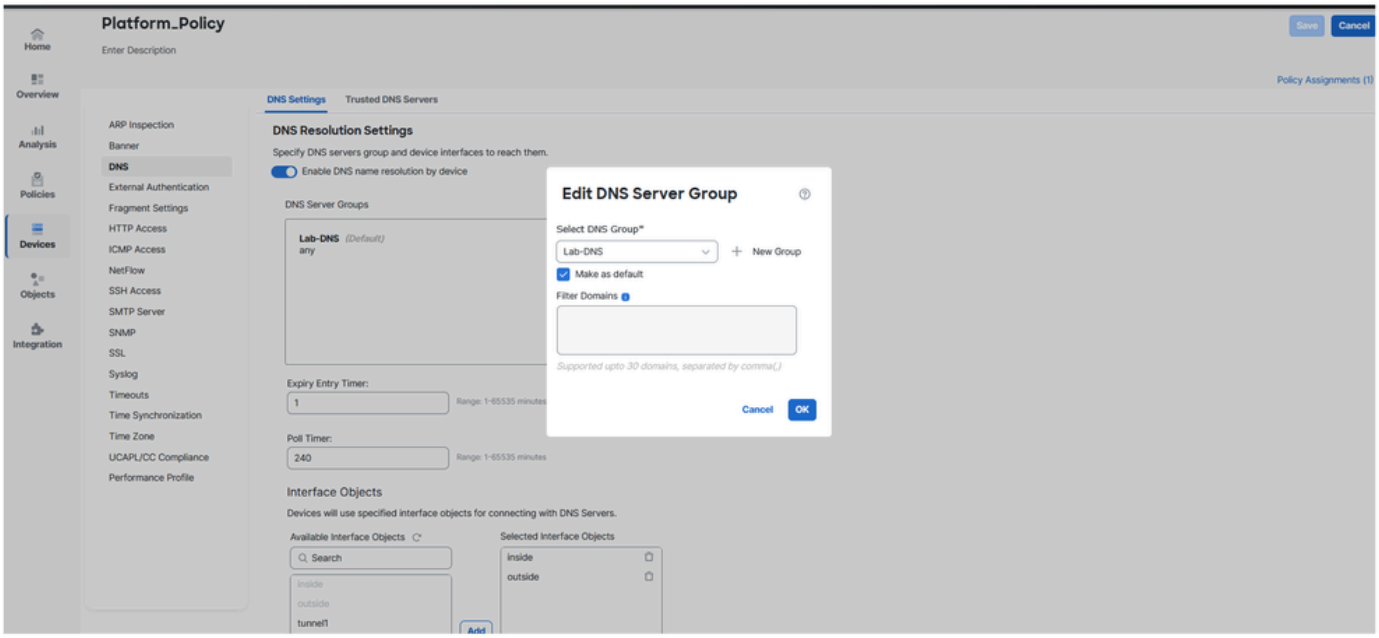
```
show run dns
```

Im FÜZ:

- Klicken Sie aufDevices> Platform Settings , bearbeiten oder erstellen Sie eine neue Richtlinie.



Sichere Firewall-Bedrohungsabwehr - Plattformrichtlinie



Sichere Firewall-Bedrohungsabwehr - DNS-Konfiguration

Überprüfen Sie mithilfe der FTD-CLI, dass Sie einen Ping an die IP-Adresse und den FQDN der privaten Ressourcen senden können (wenn Sie über den FQDN auf PR zugreifen möchten).

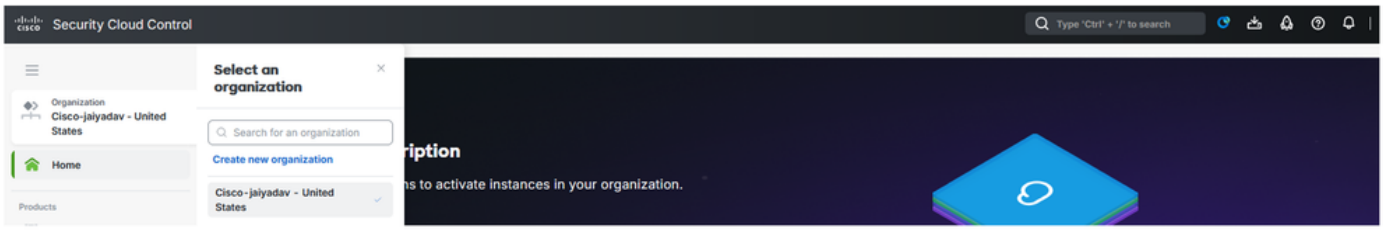
```
dns-group Lab-DNS
ftd1# ping ise.taclab.com
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.50, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
ftd1#
```

Erstellen eines Security Cloud Control-Tenants für CDO

Anmerkung: Wenn Sie bereits über einen SCC-Tenant verfügen, müssen Sie keinen neuen Tenant erstellen.

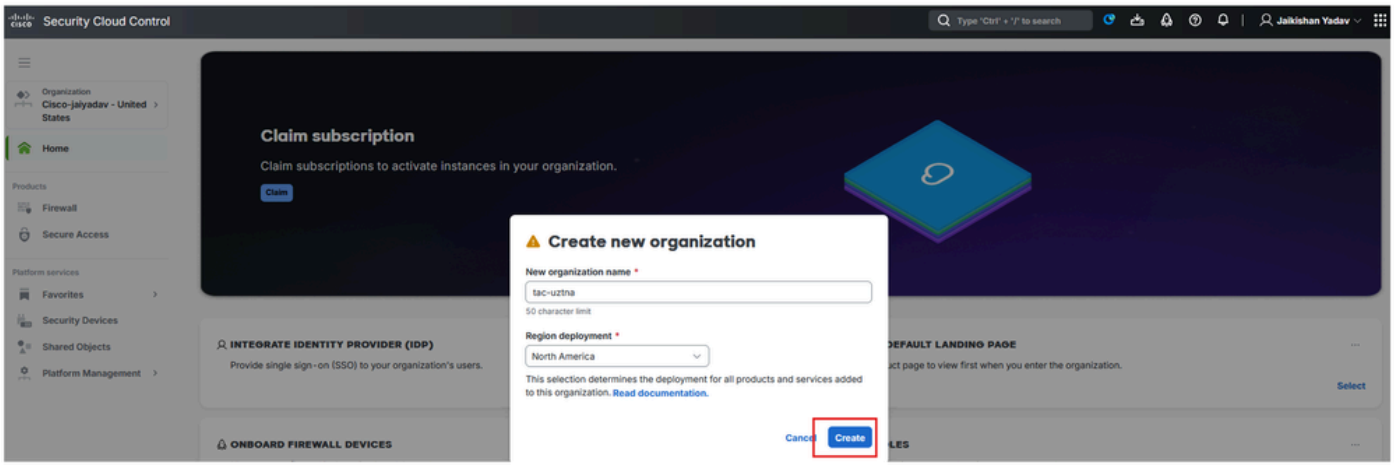
Navigieren Sie zu Security Cloud Control:

- Klicken Sie aufOrganization > Create new organization



Sichere Cloud-Kontrolle - Organisation

- Klicken Sie Create



Sichere Cloud-Kontrolle - Erstellung von Organisationen

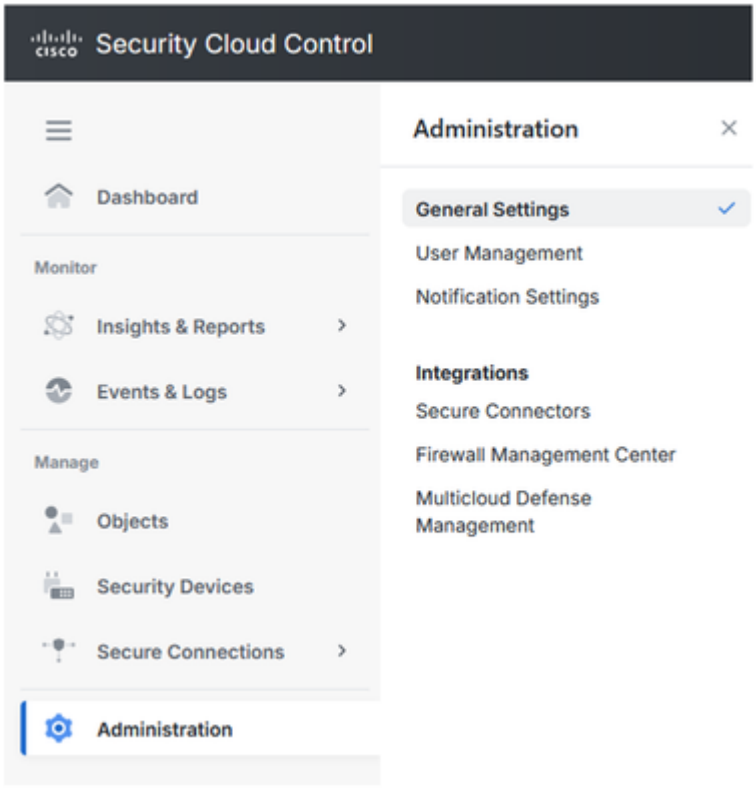
Nachdem der SCC-Tenant erstellt wurde, sammeln Sie die Tenant-Informationen, um die Firewall und die Secure Access-Mikroanwendung zu aktivieren und uZTNA zu aktivieren.

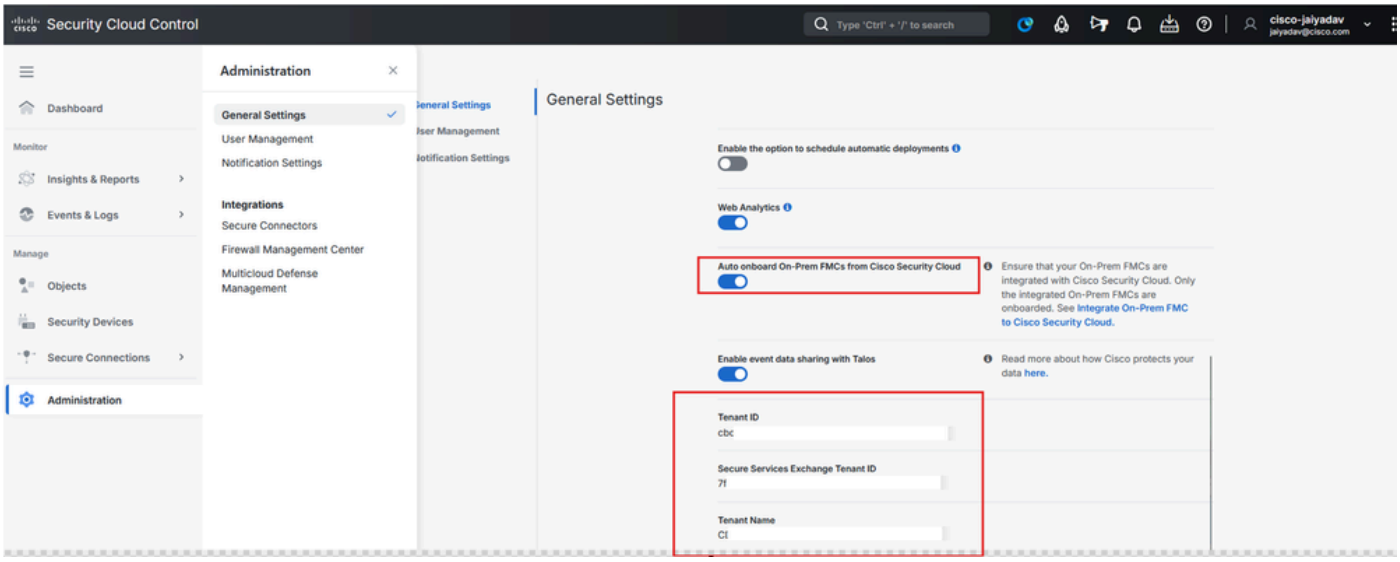
Konfigurieren der allgemeinen SCC-Firewall-Einstellungen

Navigieren Sie zu CDO/SCC:

- AufAdministration> General Settings
- Stellen Sie sicher, dass Auto onboard On-Prem FMCs from Cisco Security Cloud Option aktiviert ist.

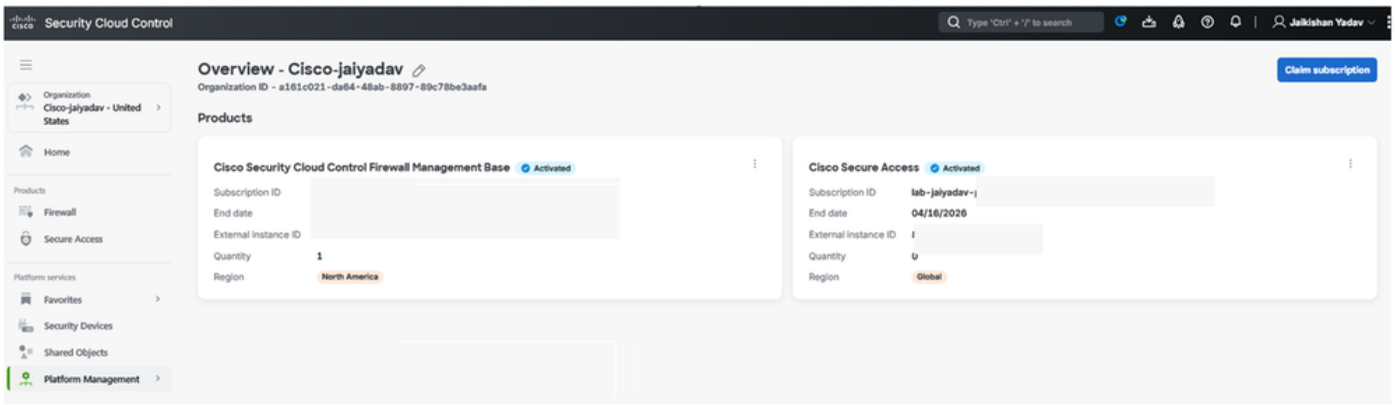
Anmerkung: Der Benutzer, der versucht, auf die Secure Access MicroApp zuzugreifen, muss überSecure Accesseine Rolle und eine Rolle für den Security Cloud Control Administrator verfügen.





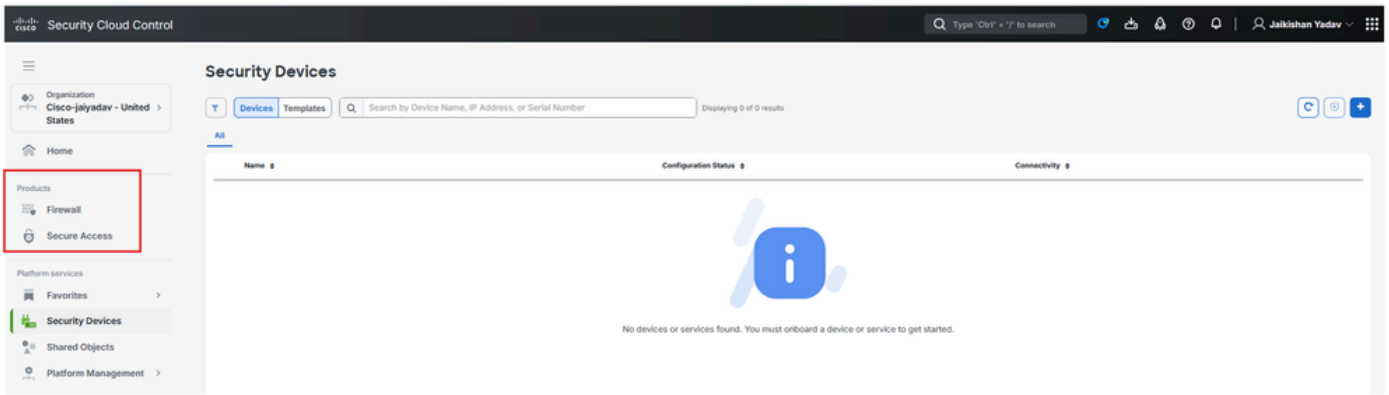
Sichere Cloud-Kontrolle - Organisationsdetails

Überprüfung der Integration von Secure Access Tenant und Security Control Firewall Management Base



Sichere Cloud-Kontrolle - Aktivierung des sicheren Zugriffs

Wenn Sie Schritt Erstellen eines Security Cloud Control Tenant auf CDO und Erstellen eines Security Cloud Control Tenant auf CDO abgeschlossen haben, können Sie die Mikroanwendungen für Firewall und sicheren Zugriff auf dem SCC-Dashboard anzeigen:



Sichere Cloud-Kontrolle - Mikroanwendungen

Signiertes Zertifikat der Firewall Threat Defense (FTD)-Zertifizierungsstelle generieren

---

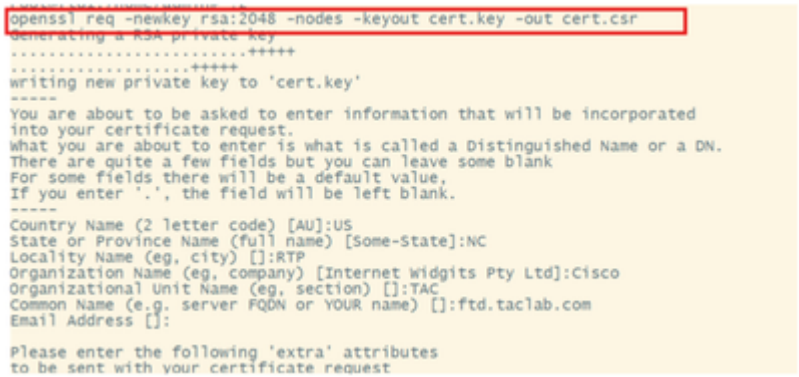
Anmerkung: Sie können auch selbstsignierte FTD-Zertifikate FTD-Zertifikate verwenden (siehe Abschnitt Generating Self-Signed Internal and Internal CA Certificates). Das Zertifikat muss im PKCS12-Format vorliegen und im Benutzercomputerspeicher unter der vertrauenswürdigen Stammzertifizierungsstelle vorhanden sein.

Um ein CA-signiertes Zertifikat mit FTD in der Build Open SSL-Funktion zu generieren, gehen Sie wie folgt vor:

- Zu FTD navigieren
- Befehlexpertausführen

- CSR und Schlüssel mit openssl generieren
    - OpenSSL-Befehl:

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



Zertifikatsignierungsanforderung

- CSR kopieren und ein CA-signiertes Zertifikat erhalten
- FTD CA-signiertes Zertifikat und Schlüssel verwenden und Zertifikat in PKCS12-Format konvertieren
    - OpenSSL-Befehl:

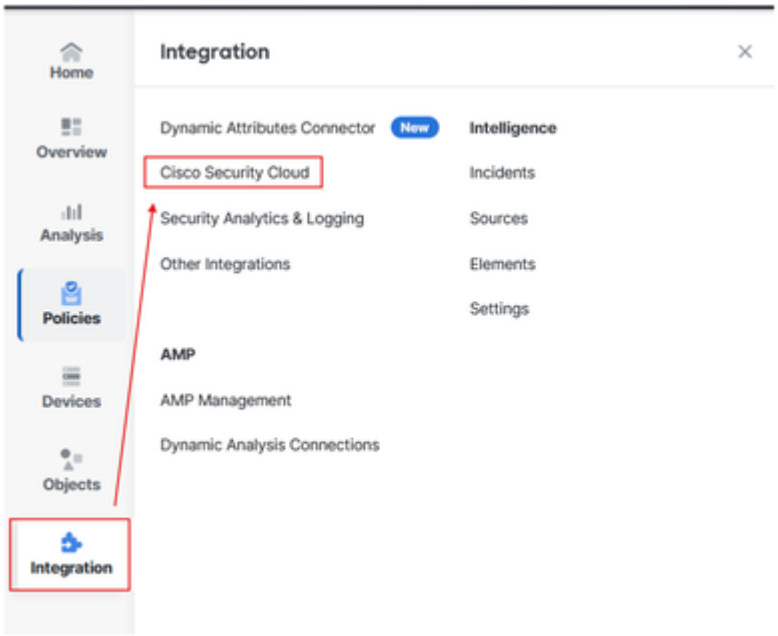
```
openssl pkcs12 -export -out ftdcert.p12 -in cert.crt -inkey cert.key
```

- Exportieren Sie das Zertifikat mithilfe der SCP oder eines anderen Tools.

Integriertes Firewall Management Center zur Sicherheit Cloud-Kontrolle

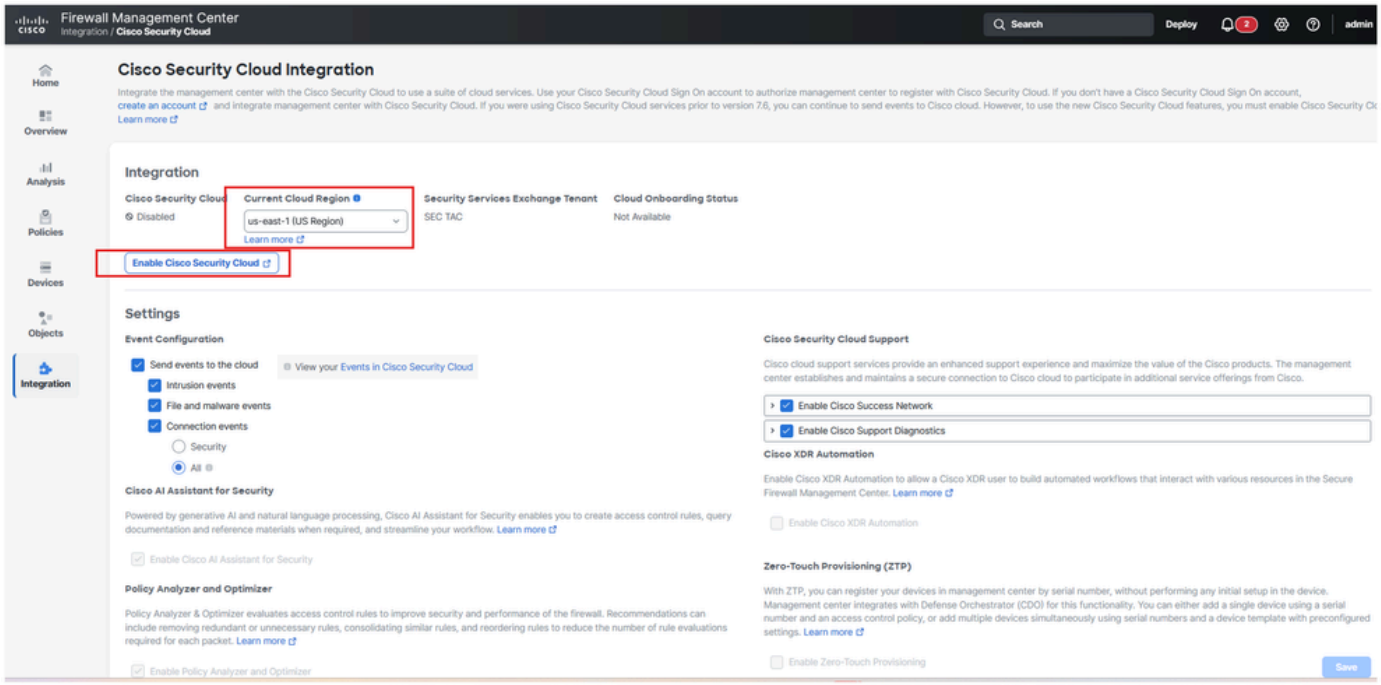
Navigation zum FMC:

- AufIntegration> Cisco Security Cloud



Integration von Firewall Management Center und SCC

- Wählen Sie die Cloud-Region aus, und klicken Sie dann auf Enable Cisco Security Cloud

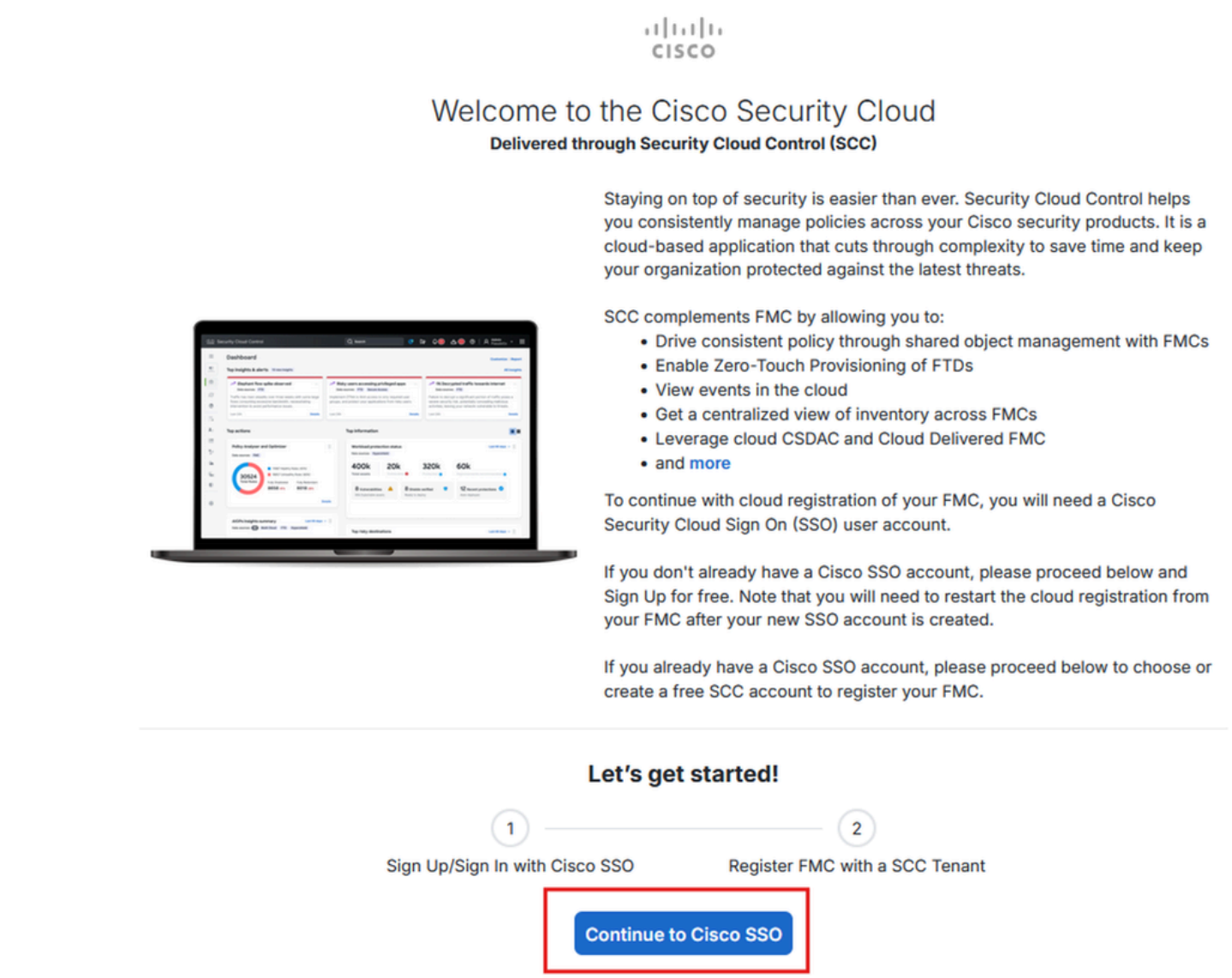


Integration von Firewall Management Center in SCC

Es öffnet sich eine neue Browser-Registerkarte, auf der neuen Registerkarte:

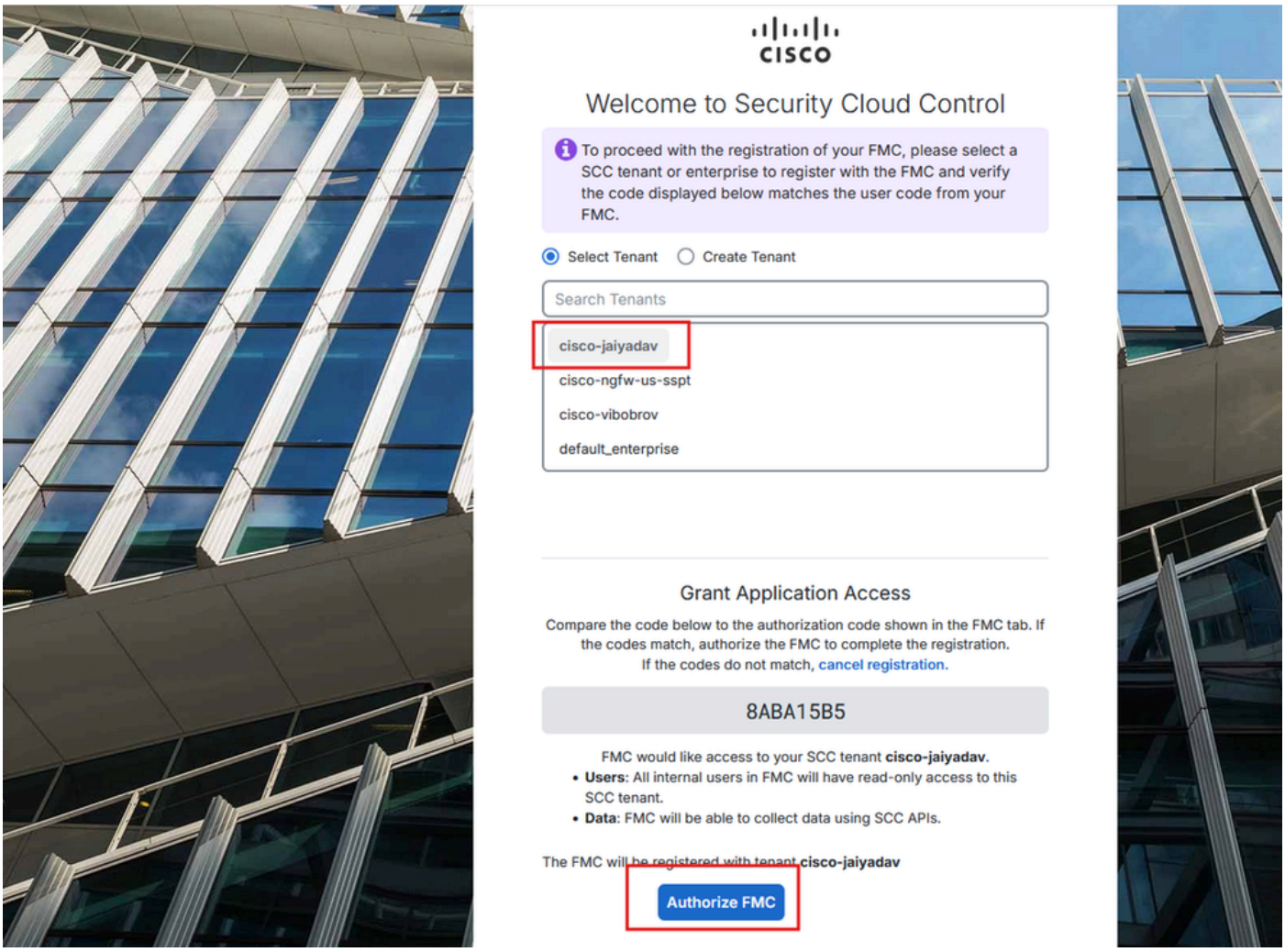
- Klicken Sie Continue to Cisco SSO

Anmerkung: Stellen Sie sicher, dass Sie sich von SCC abmelden und keine anderen Registerkarten geöffnet haben.



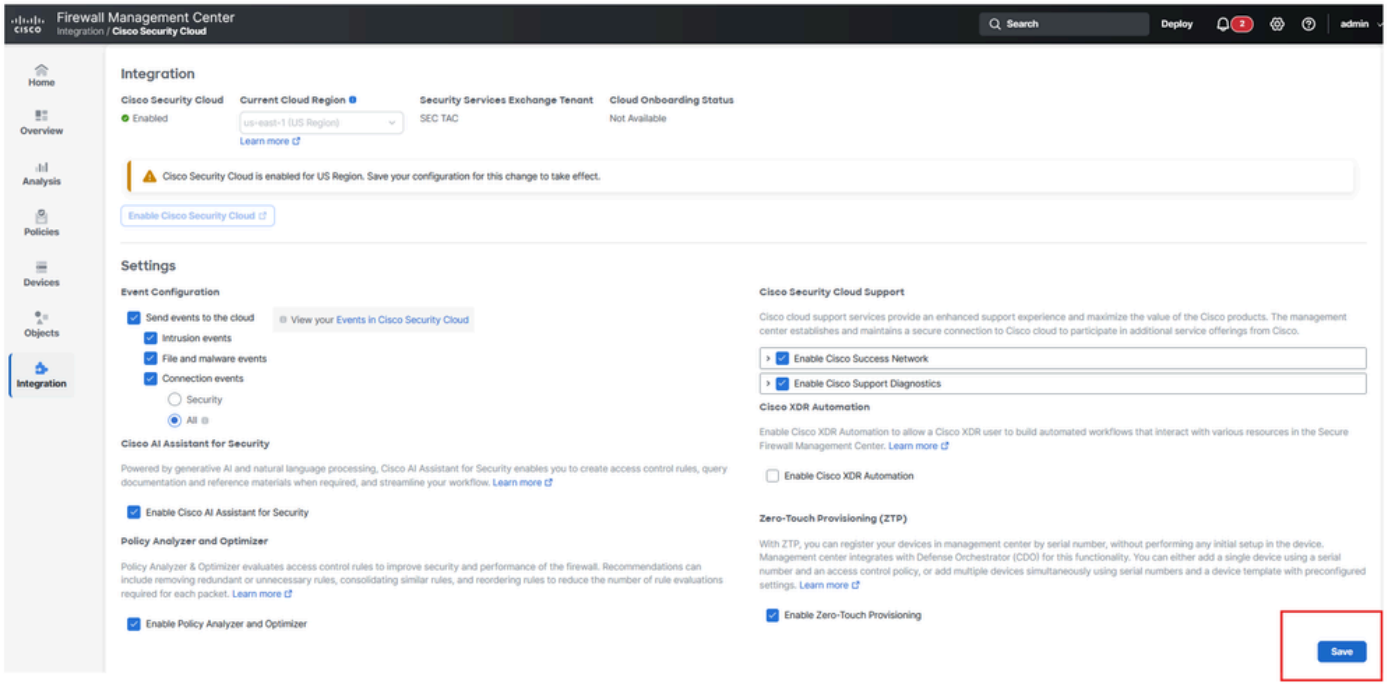
Integration von Firewall Management Center in SCC

- Wählen Sie Ihren SCC-Tenant aus und klicken Sie auf Authorize FMC



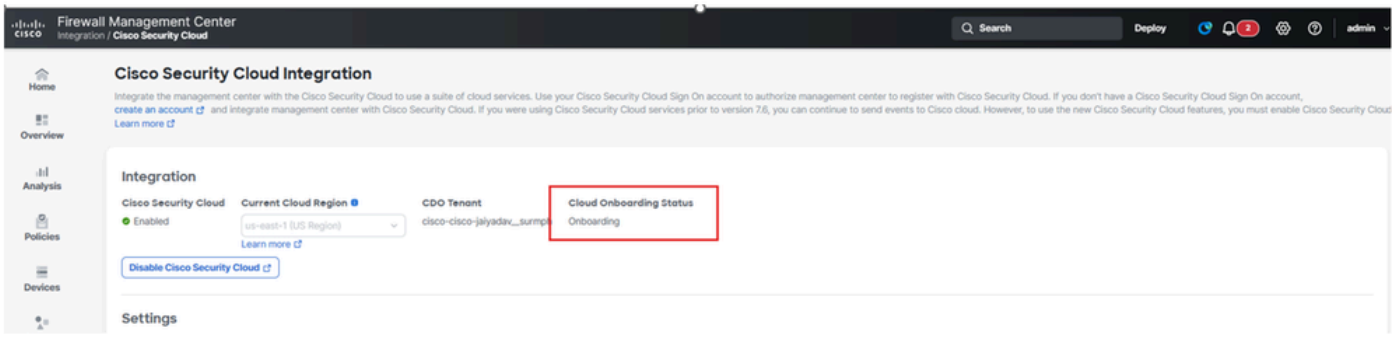
Integration von Firewall Management Center in SCC

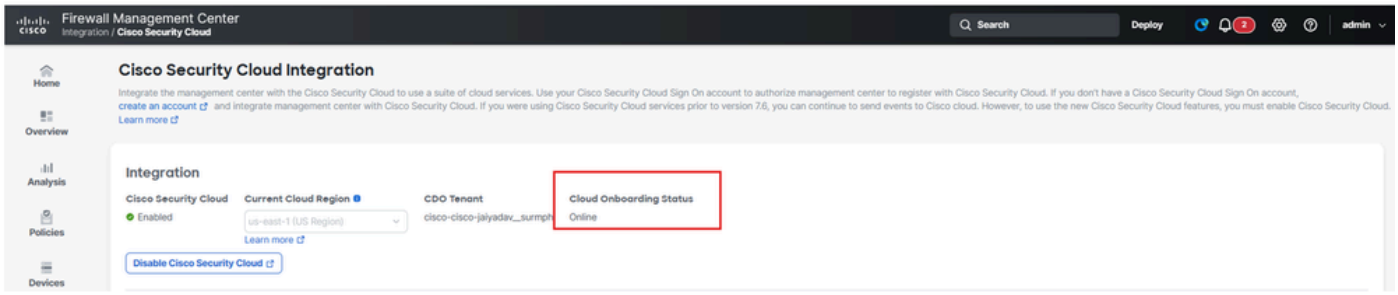
- Klicken Sie Save



Integration von Firewall Management Center in SCC

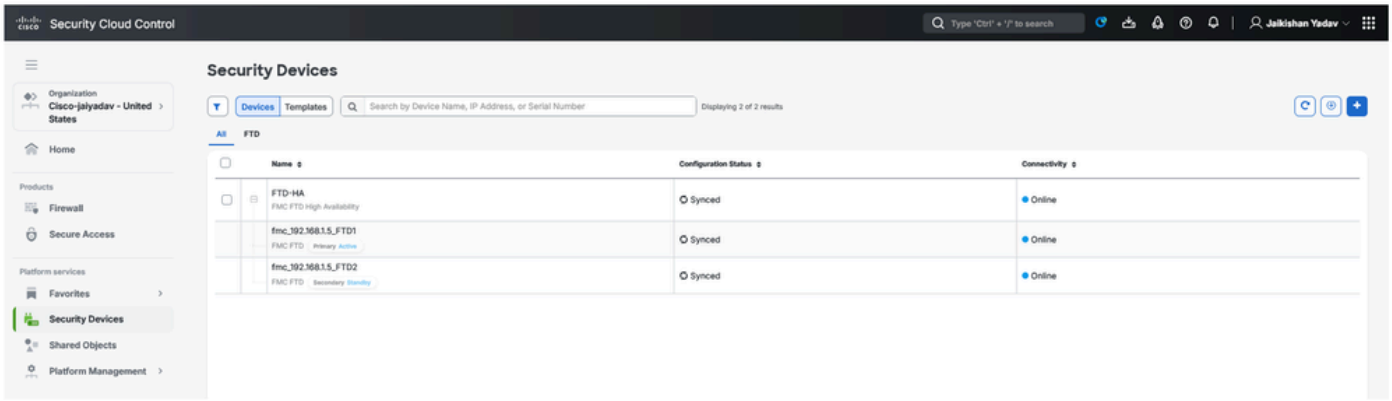
Der Status von Cloud Onboarding Status muss sich von **Not Available** auf Onboarding ändern Online.





Firewall Management Center - Onboarding-Status

- Navigieren Sie zu SCC, und prüfen Sie den FTD-Status unterPlatform Services> Security Devices

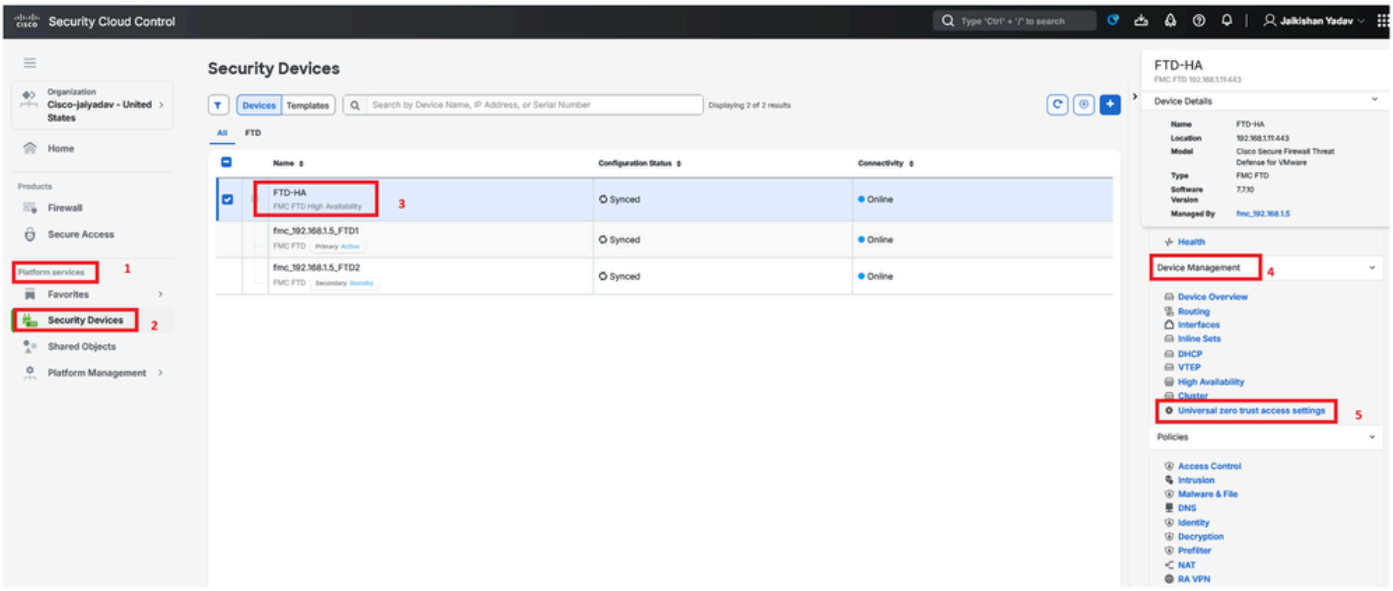


Schutz vor Bedrohungen durch sichere Firewall auf SCC

Registrieren der ZTNA-Einstellungen (Universal Zero Trust Network Access) für FTD

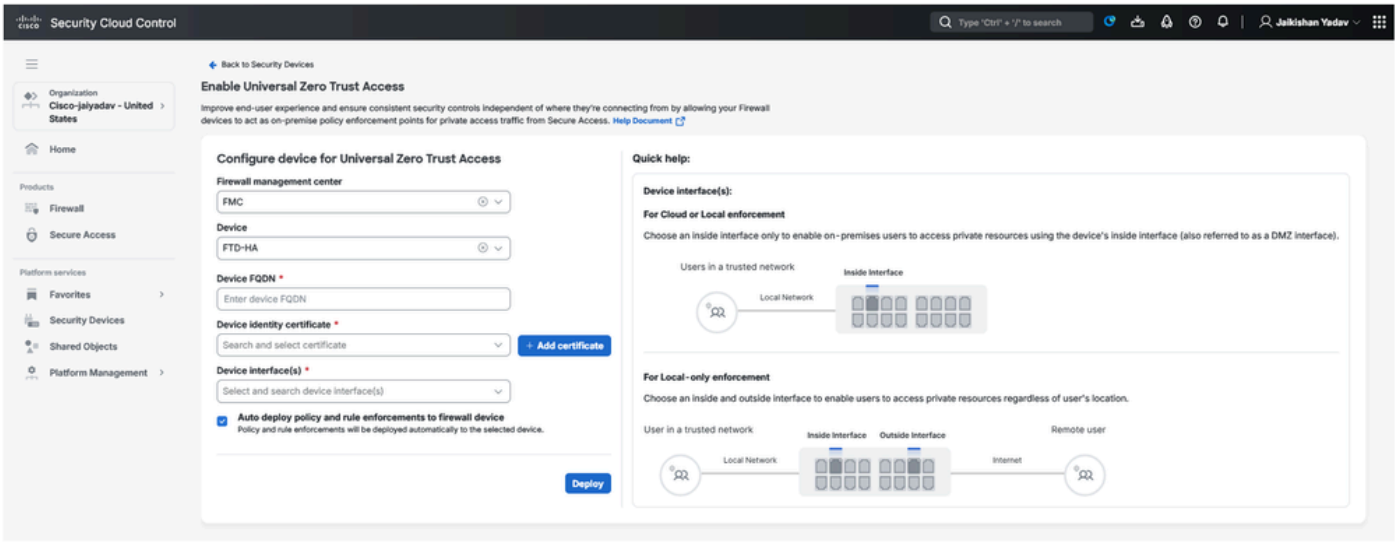
Navigieren Sie zu SCC:

- Klicken Sie auf Platform Services > **Security Devices** > **FTD** > **Device Management** > Universal Zero Trust Network Access

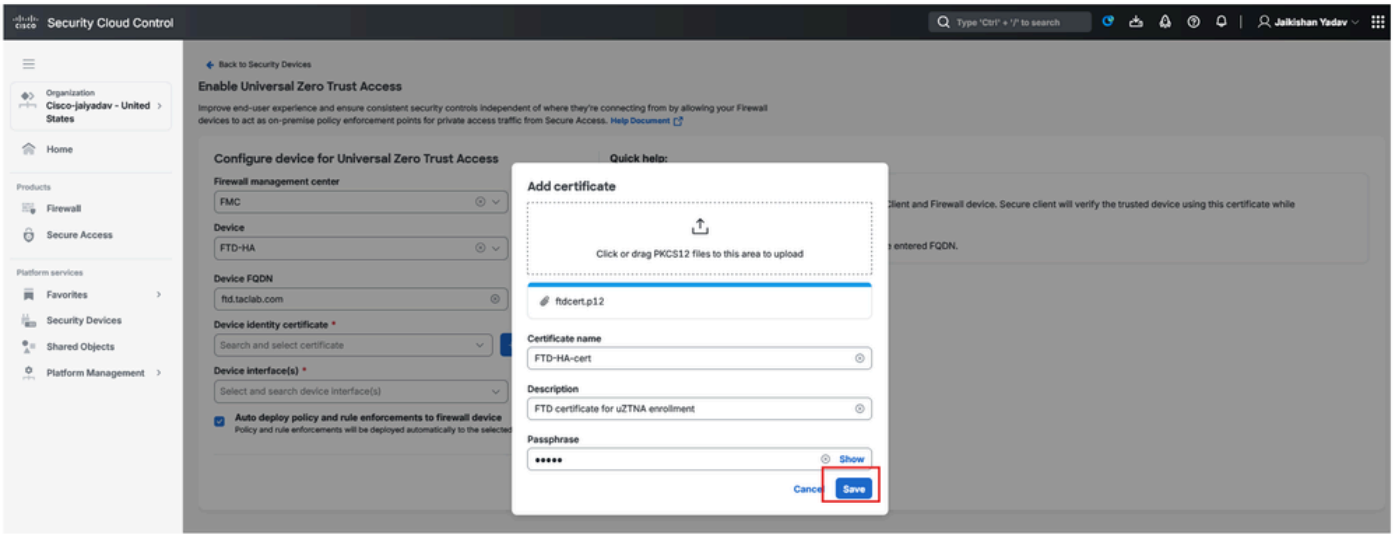


Sichere Firewall-Bedrohungsabwehr - Universelle ZTNA-Konfiguration

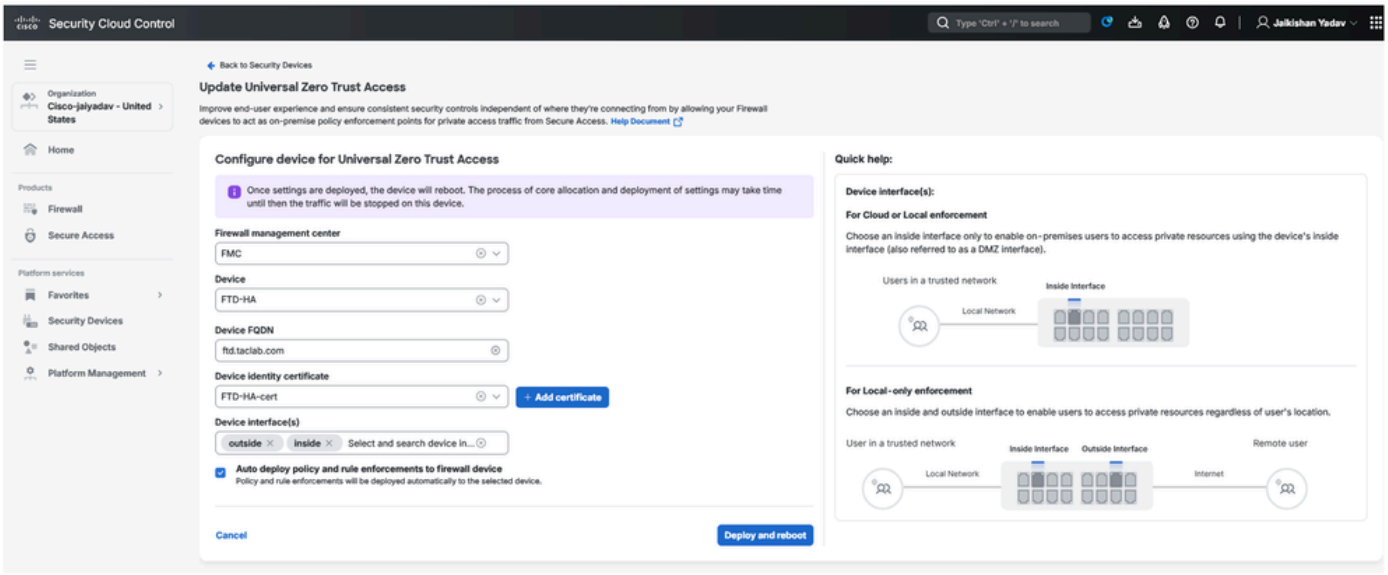
- Füllen Sie die Informationen aus, und laden Sie das FTD-Zertifikat hoch, das im Schritt Generate Firewall Threat Defense (FTD) CA-signiertes Zertifikat generiert wurde.



Sichere Firewall-Bedrohungsabwehr - Universelle ZTNA-Konfiguration



Sichere Firewall-Bedrohungsabwehr - Universelle ZTNA-Konfiguration

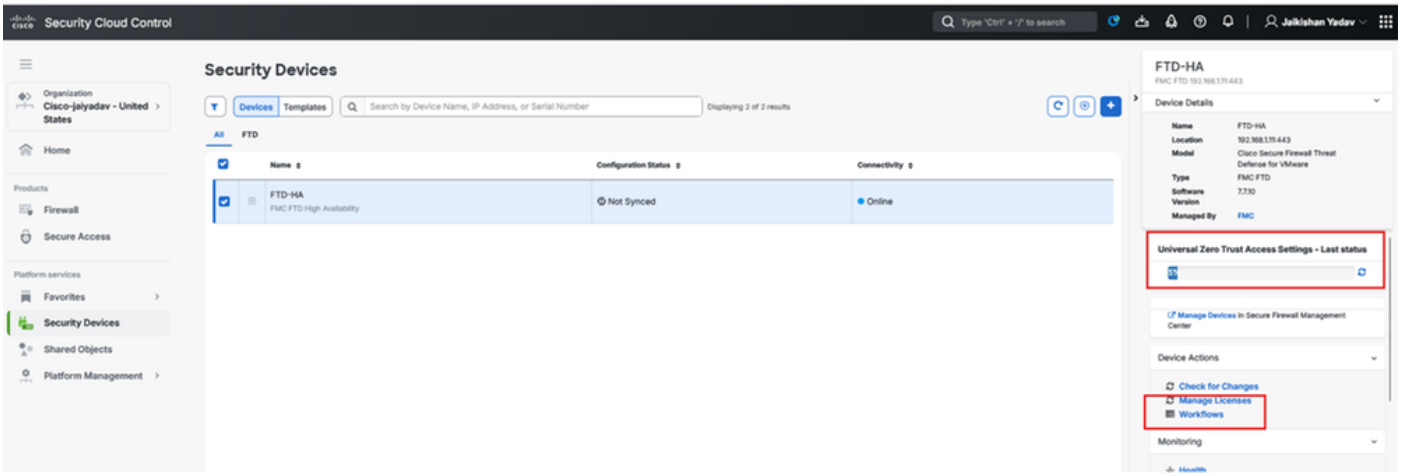


Sichere Firewall-Bedrohungsabwehr - Universelle ZTNA-Konfiguration

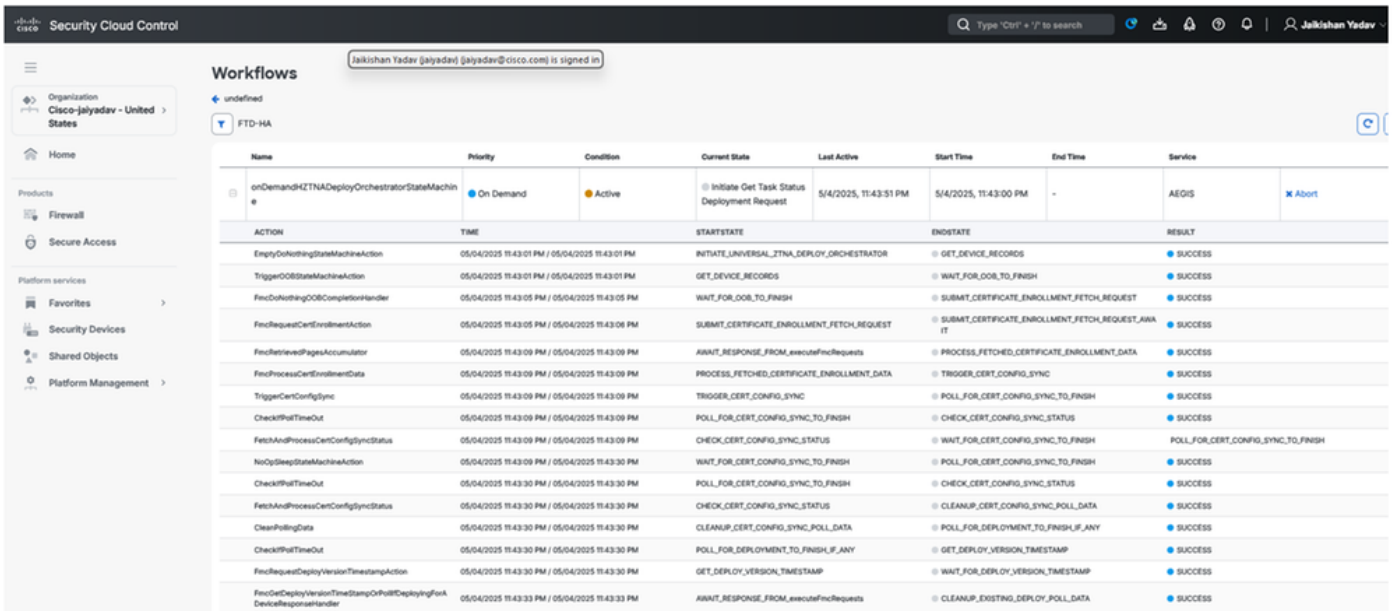
---

Anmerkung: Wenn Sie uZTNA auf FTD HA aktivieren, werden die Änderungen bereitgestellt und beide FTD-Einheiten (Firewall Threat Defense) gleichzeitig neu gestartet. Stellen Sie sicher, dass Sie ein ordnungsgemäßes Wartungsfenster planen.

- Klicken Sie auf Workflow , um die Protokolle zu überprüfen.

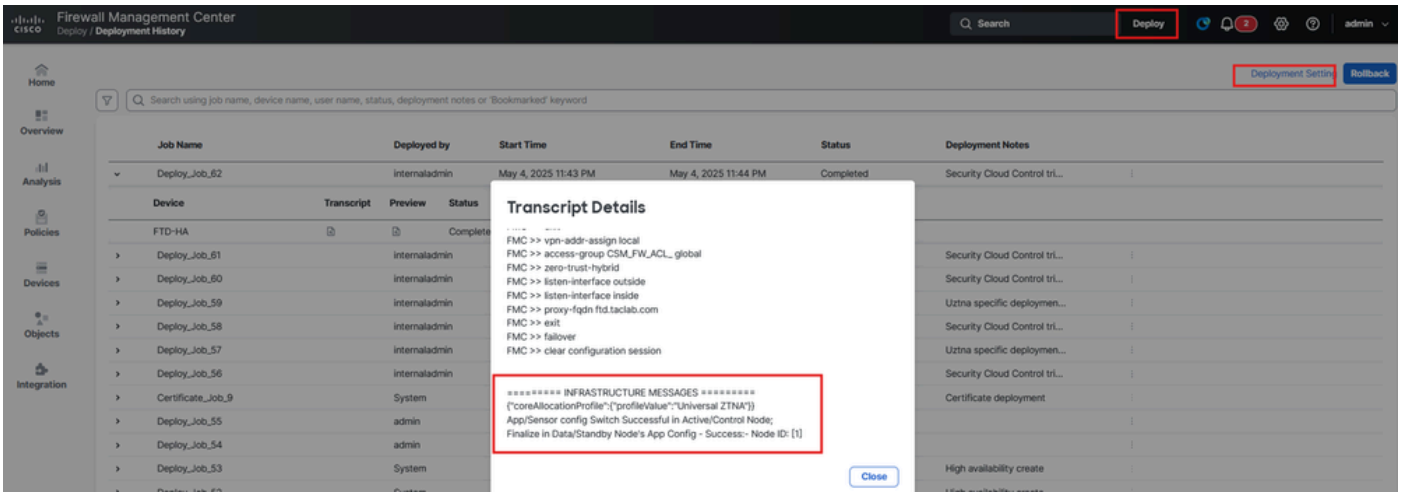


Sichere Firewall-Bedrohungsabwehr - Allgemeiner ZTNA-Konfigurationsstatus



Sicherheits-Cloud-Steuerungs-Workflow

Unter Transkriptdetails können Sie Änderungen sehen Policy Deployment Status am FMC.



Secure Firewall Management Center - Status der Richtlinienbereitstellung

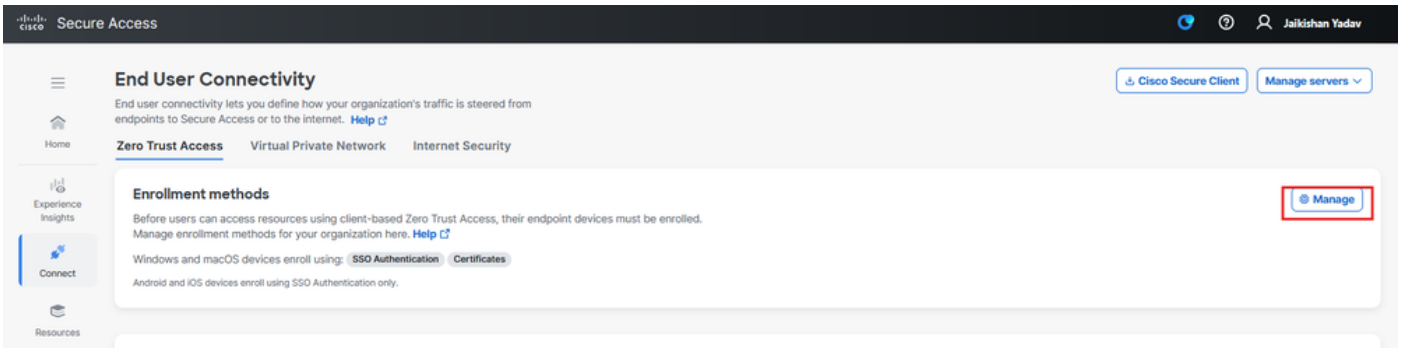
Registrieren Sie den Kunden mit uZTNA

Konfiguration des sicheren Zugriffs

Anmerkung: Sie können SSO oder eine zertifikatbasierte ZTA-Registrierung verwenden. Im nächsten Schritt erfolgt die zertifizierungsbasierte ZTA-Registrierung.

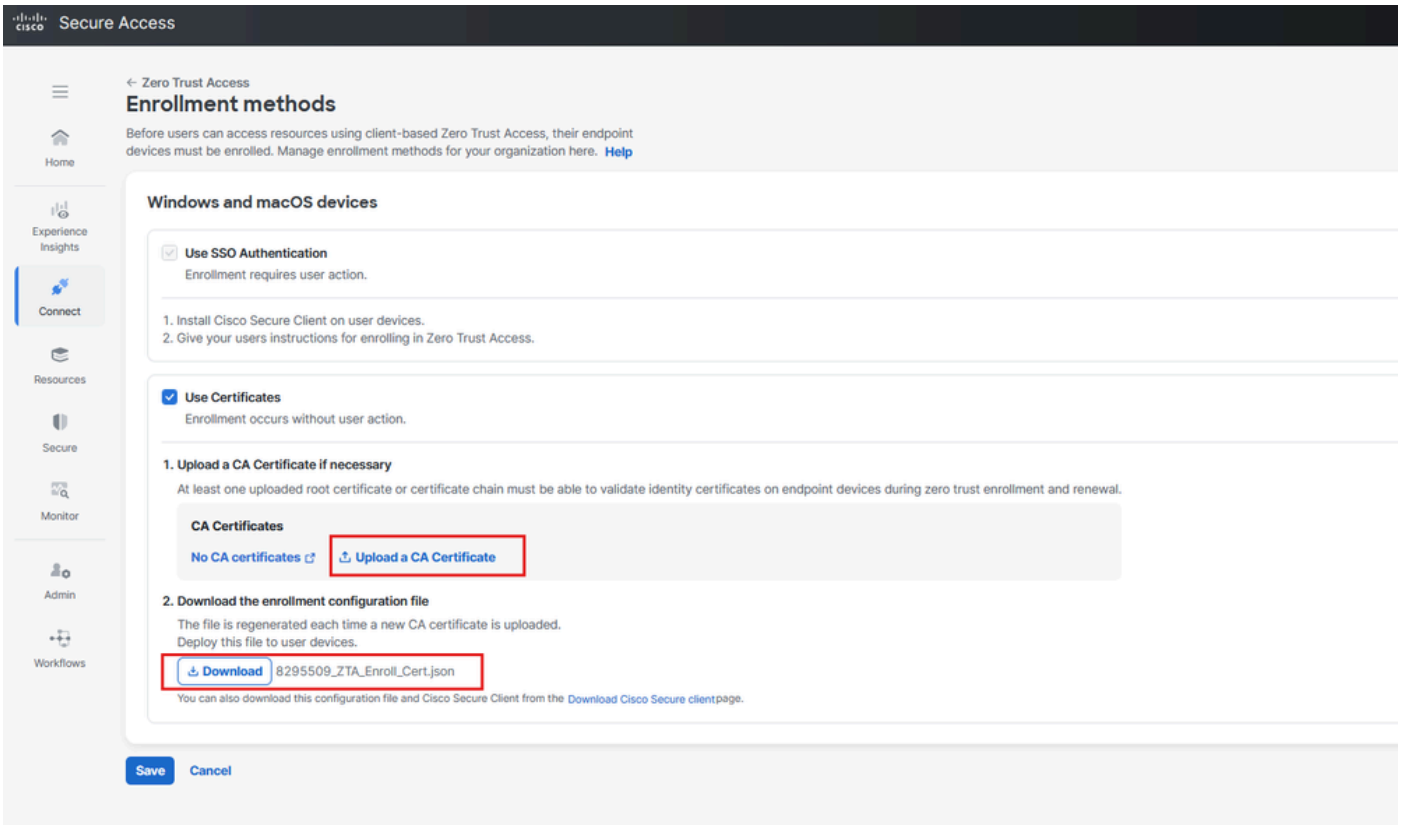
Navigieren Sie zum Dashboard für sicheren Zugriff:

- Klicken Sie auf **Connect** > **End User Connectivity** > Zero Trust Access
- Klicken Sie Manage



Sicherer Zugriff - Registrierung von ZTA-Zertifikaten

- Laden Sie das Zertifikat der Stammzertifizierungsstelle hoch, und laden Sie die Konfigurationsdatei für die Registrierung herunter.

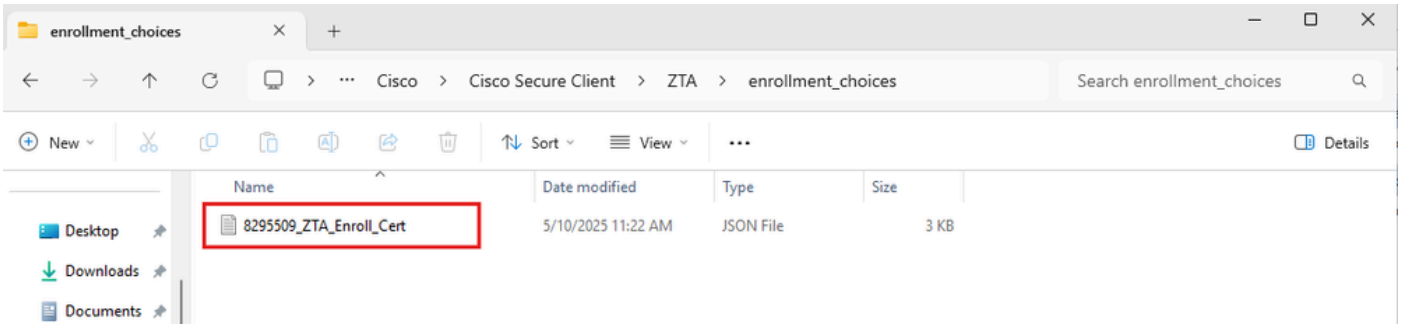


Sicherer Zugriff - Registrierung von ZTA-Zertifikaten

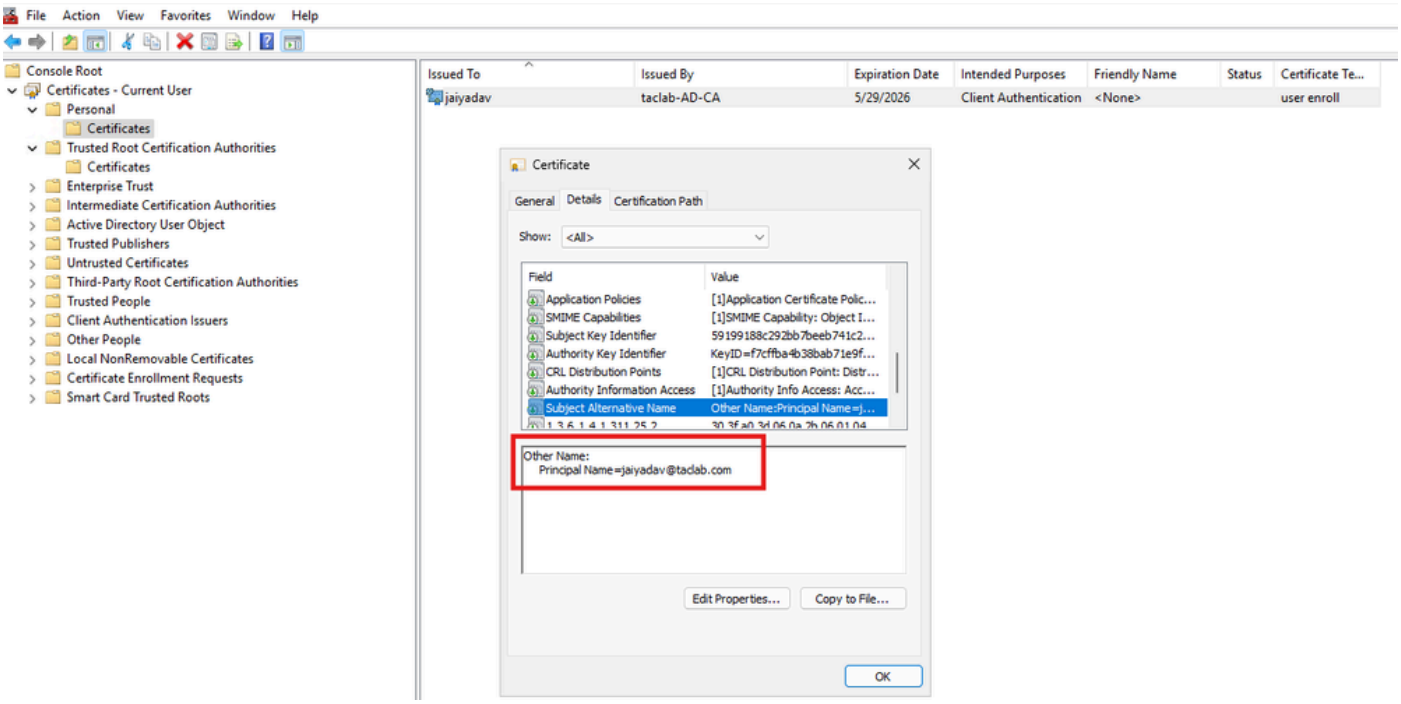
- Klicken Sie Save

Client-Konfiguration

Kopieren Sie die Registrierungskonfigurationsdatei nach C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollment_choices

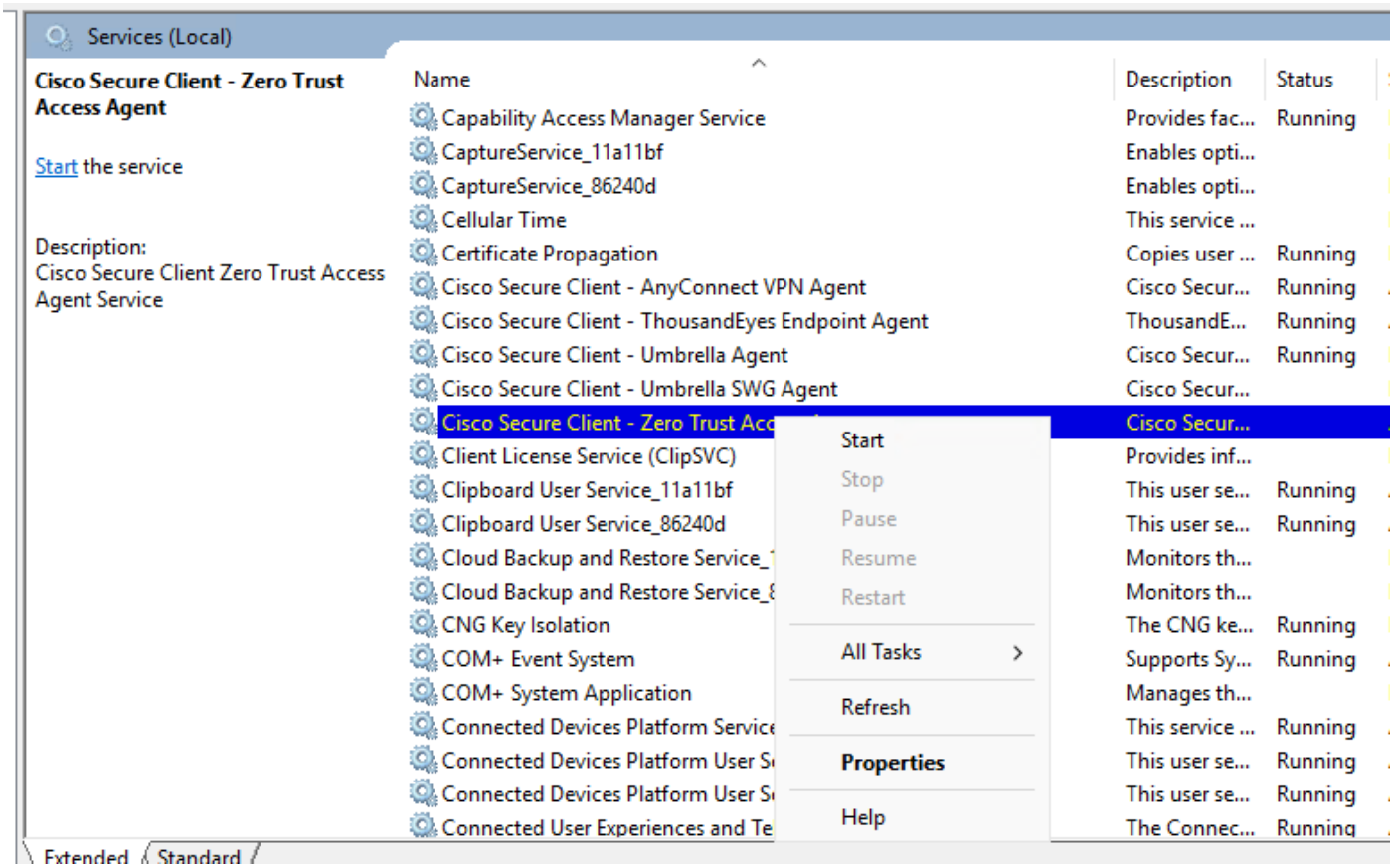


- Erstellen Sie ein Client-Zertifikat, für das UPN im SAN-Feld erforderlich ist.



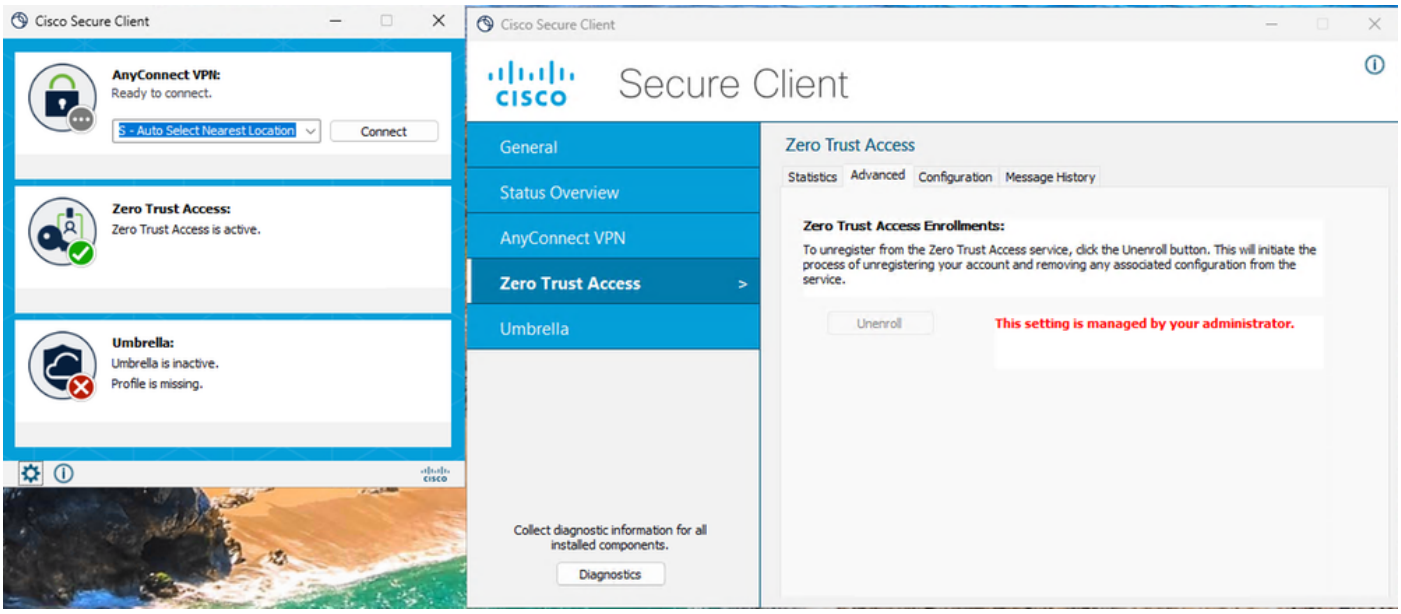
Installation des Zertifikats

- Starten/Neu starten Cisco Secure Client - Zero Trust Access Agent



Windows-Dienste

- Überprüfen des ZTA-Modulstatus



Sicherer Zugriff - Registrierungsstatus für ZTA-Zertifikate

Überprüfung

Verwenden Sie den nächsten Befehl, um die uZTNA-Konfiguration auf Firewall Threat Defense (FTD) zu überprüfen:

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

Zugehörige Informationen

- Technischer Support und Downloads von Cisco
- Cisco Secure Access-Hilfecenter
- Cisco SASE Designleitfaden

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.