

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

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Netzwerkdiagramm](#)

[Informationen zu Haltestellen](#)

[Unterstützte Geräte](#)

[Einschränkungen](#)

[Konfigurieren](#)

[FMC-Version überprüfen](#)

[FTD-Version überprüfen](#)

[FTD-Lizenzen überprüfen](#)

[Überprüfen Sie die Plattformvoreinstellungen und den ordnungsgemäß konfigurierten DNS.](#)

[Erstellen eines Security Cloud Control-Tenants für CDO](#)

[Konfigurieren der allgemeinen SCC-Firewall-Einstellungen](#)

[Überprüfung der Integration von Secure Access Tenant und Security Control Firewall Management Base](#)

[Signiertes Zertifikat der Firewall Threat Defense \(FTD\)-Zertifizierungsstelle generieren](#)

[Integriertes Firewall Management Center zur Sicherheit Cloud-Kontrolle](#)

[Registrieren der ZTNA-Einstellungen \(Universal Zero Trust Network Access\) für FTD](#)

[Registrieren Sie den Kunden mit uZTNA](#)

[Konfiguration des sicheren Zugriffs](#)

[Client-Konfiguration](#)

[Überprüfung](#)

[Zugehörige Informationen](#)

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 aktiver 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 aktiver 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

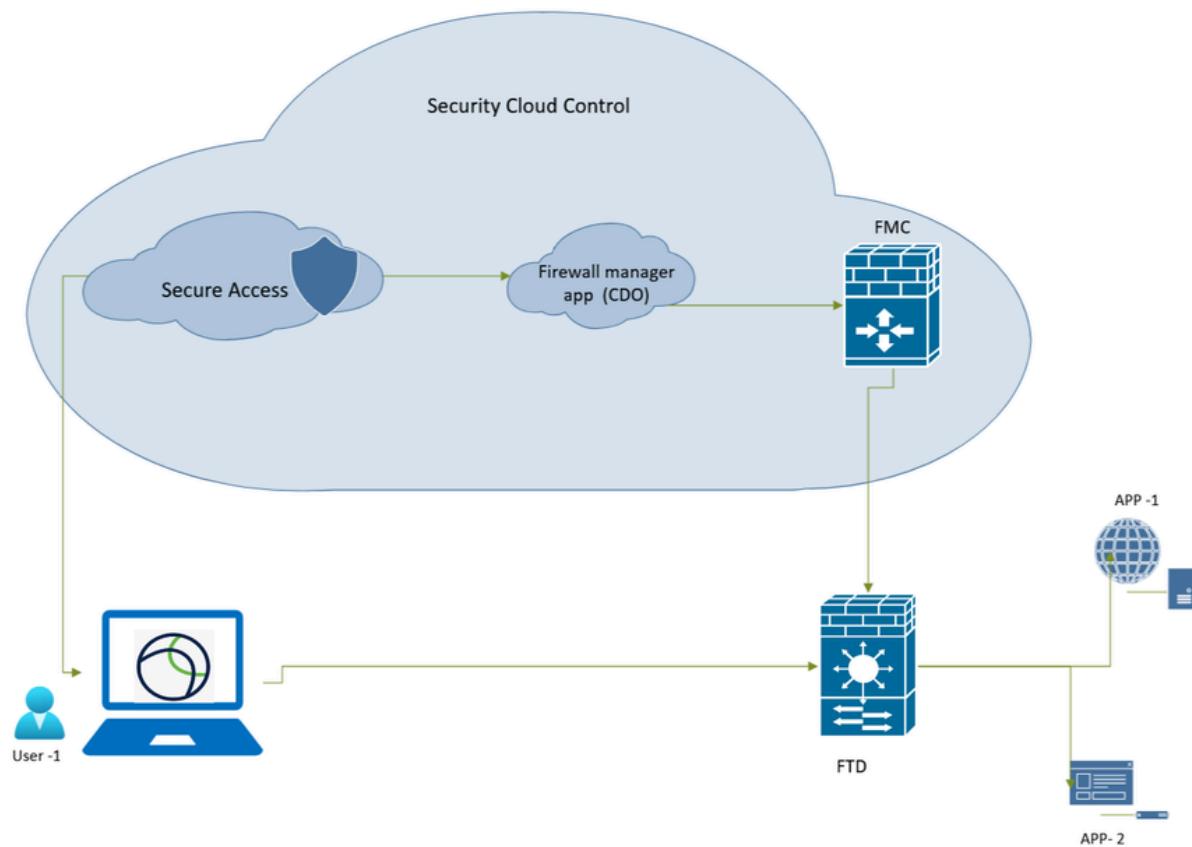
Verwendete Komponenten

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

The screenshot shows the FMC interface with the 'About' menu highlighted. The 'About' button is located in the top right corner of the main menu bar. The 'About' menu is expanded, showing options like 'Product Content', 'Support & Downloads', and 'What's New'.

About		
Product Content	Support & Downloads	What's New
Secure Firewall on Cisco.com	Ask Cisco Community	Release Highlights
Documentation on Cisco.com	TAC Support Cases	All New and Deprecated Features
Secure Firewall on YouTube	Software Downloads	
Secure Firewall Essentials		
Partner Ecosystem		



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 - Softwareversion

FTD-Version überprüfen

Navigieren Sie zur FMC-Benutzeroberfläche:

- Auf [Devices](#) > Device Management

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
FTD1(Primary, Active) 192.168.1.11 - Routed	Firewall Threat Defense for VMware	7.7.10	N/A	Essentials, IPS (2 more...)	ACP	
FTD2(Secondary, Standby) 192.168.1.13 - Routed	Firewall Threat Defense for VMware	7.7.10	N/A	Essentials, IPS (2 more...)	ACP	

Sichere Firewall-Abwehr - Softwareversion

FTD-Lizenzen überprüfen

- Klicken Sie auf 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

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)					

Sichere Firewall-Bedrohungsbewehr - Smart Licenses

Überprüfen Sie die Plattformmeinstellungen 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 auf **Devices > Platform Settings**, bearbeiten oder erstellen Sie eine neue Richtlinie.

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

Sichere Firewall-Bedrohungsbewehr - Plattformrichtlinie

Sichere Firewall-Bedrohungsbewehr - 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



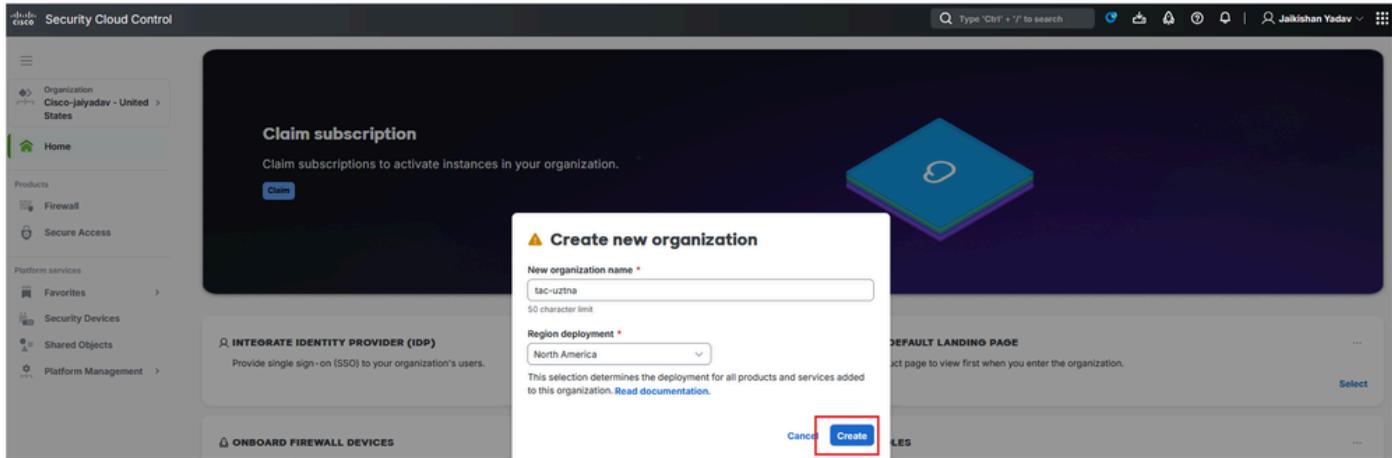
Anmerkung: Wenn Sie bereits über einen SCC-Tenant verfügen, müssen Sie keinen neuen Tenant erstellen.

Navigieren Sie zu [Security Cloud Control](#):

- Klicken Sie auf [Organization > 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](#):

- Auf Administration > 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 über Secure Access eine Rolle und eine Rolle für den Security Cloud Control Administrator verfügen.

Security Cloud Control

Administration

General Settings

User Management

Notification Settings

Integrations

Secure Connectors

Firewall Management Center

Multicloud Defense Management

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

Tenant ID: cfc

Secure Services Exchange Tenant ID: 71

Tenant Name: C1

Administration

General Settings

User Management

Notification Settings

Integrations

Secure Connectors

Firewall Management Center

Multicloud Defense Management

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

Tenant ID: cfc

Secure Services Exchange Tenant ID: 71

Tenant Name: C1

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

```
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
```

Zertifikatsignierungsanforderung

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

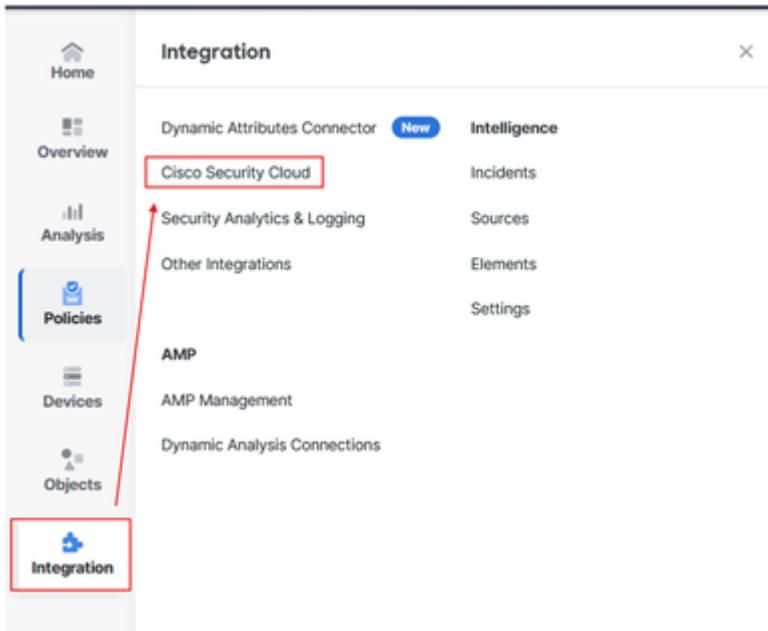
```
openssl pkcs12 -export -out ftdcert.p12 -in cert.crt -inkey cert.key
```

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

Integriertes Firewall Management Center zur Sicherheit Cloud-Kontrolle

Navigation zum FMC:

- Auf **Integration > 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



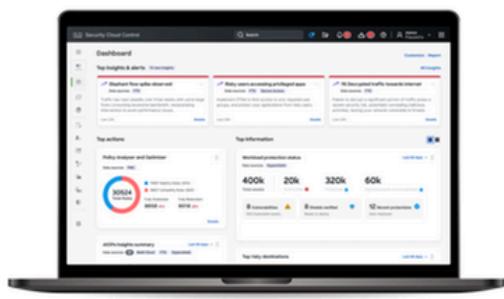
Anmerkung: Stellen Sie sicher, dass Sie sich von SCC abmelden und keine anderen Registerkarten geöffnet haben.



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](#)

Integration von Firewall Management Center in SCC

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



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

Integration von Firewall Management Center in SCC

- Klicken Sie 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

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)

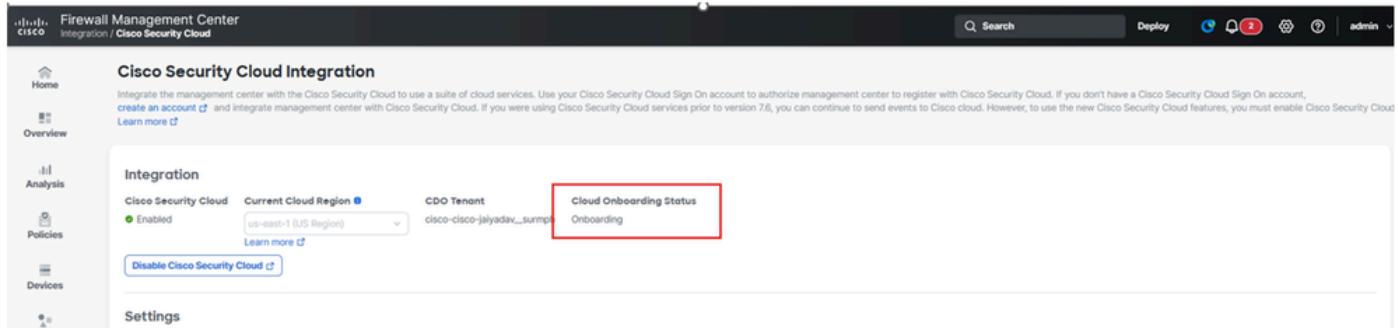
With ZTP, you can register your devices in management center by serial number, without performing any initial setup in the device. Management center integrates with Defense Orchestrator (DCO) for this functionality. You can either add a single device using a serial number and an access control policy,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

Enable Zero-Touch Provisioning

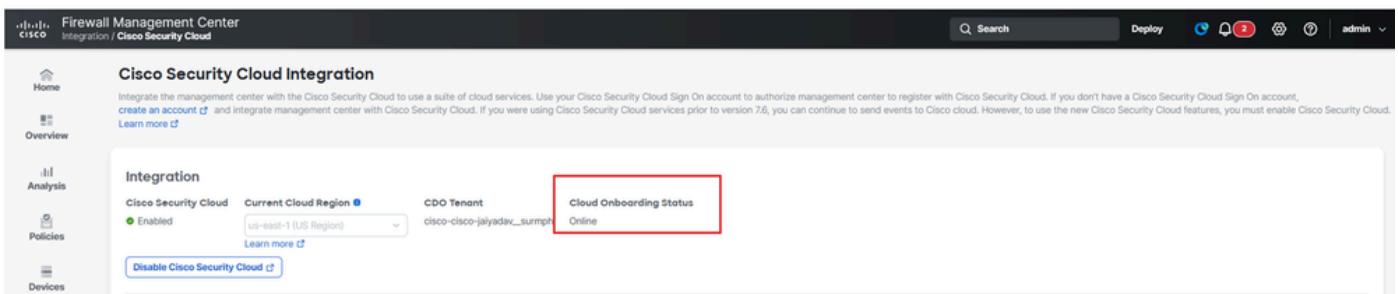
Save

Integration von Firewall Management Center in SCC

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



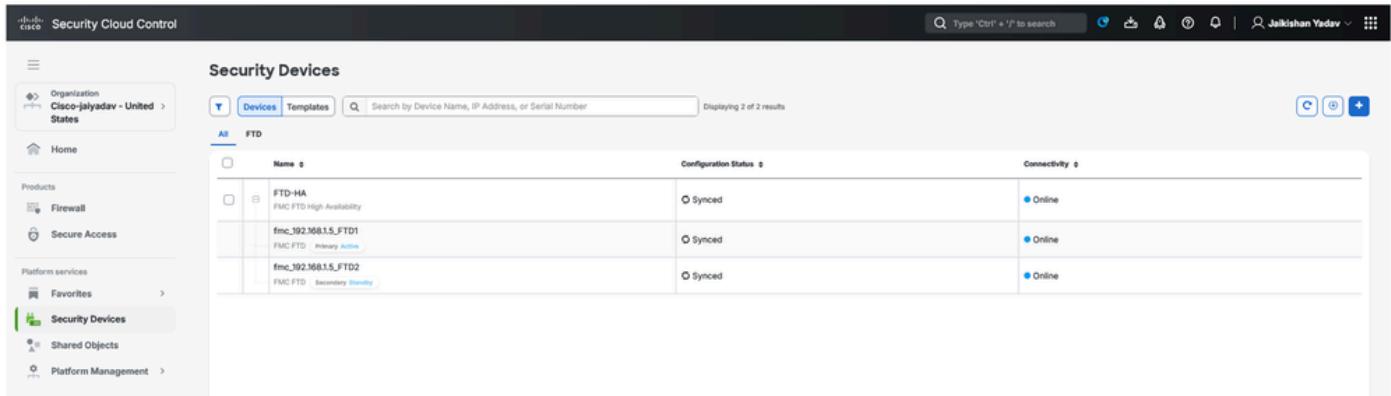
The screenshot shows the 'Cisco Security Cloud Integration' page in the Firewall Management Center. The 'Cloud Onboarding Status' field is highlighted with a red box and shows the value 'Onboarding'.



The screenshot shows the 'Cisco Security Cloud Integration' page in the Firewall Management Center. The 'Cloud Onboarding Status' field is highlighted with a red box and shows the value 'Online'.

Firewall Management Center - Onboarding-Status

- Navigieren Sie zu [SCC](#), und prüfen Sie den FTD-Status unter [Platform Services > Security Devices](#)



The screenshot shows the 'Security Devices' list in the Security Cloud Control interface. The table displays three FTD devices: 'FTD-HA' (Synced, Online), 'fmc_192.168.1.5_FT01' (Synced, Online), and 'fmc_192.168.1.5_FT02' (Synced, Online).

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

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](#)

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

Sichere Firewall-Bedrohungsbewehr - 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.

Security Cloud Control

Organization: Cisco-jalyadav - United States

Home

Products: Firewall, Secure Access

Platform services: Favorites, Security Devices, Shared Objects, Platform Management

Back to Security Devices

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).

Users in a trusted network → Inside Interface

For Local-only enforcement

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

User in a trusted network → Inside Interface → Outside Interface → Internet → Remote user

Sichere Firewall-Bedrohungsbewehr - Universelle ZTNA-Konfiguration

Sichere Firewall-Bedrohungsbewehr - Universelle ZTNA-Konfiguration

Sichere Firewall-Bedrohungsbewehr - 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-Bedrohungsbewehr - 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

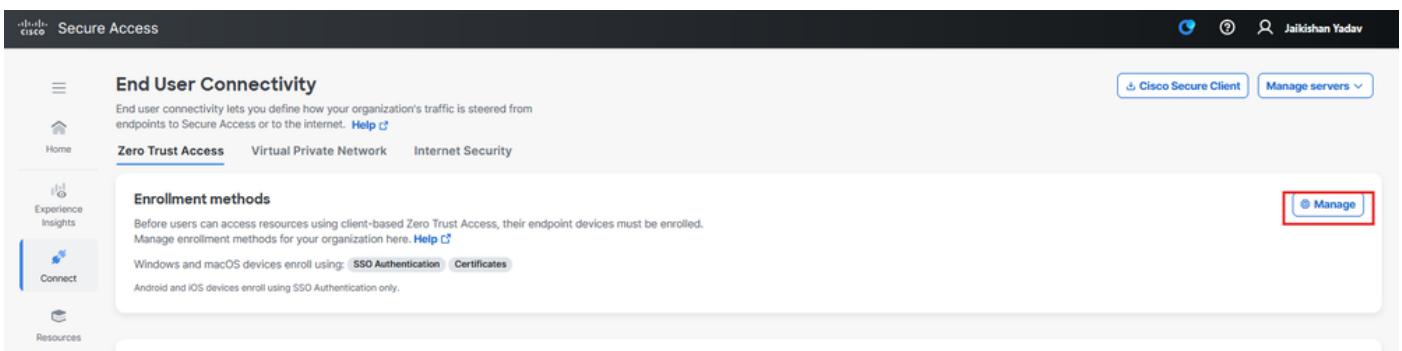
Konfiguration des sicheren Zugriffs



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**



The screenshot shows the Cisco Secure Access interface. The top navigation bar includes the Cisco logo, a search bar, and user information (Jaikishan Yadav). Below the navigation is a sidebar with icons for Experience Insights, Home, Connect (which is selected and highlighted in blue), and Resources. The main content area is titled 'End User Connectivity' and describes how it lets you define traffic steering from endpoints to Secure Access or the internet. It shows tabs for Zero Trust Access (selected), Virtual Private Network, and Internet Security. A sub-section titled 'Enrollment methods' explains that users can access resources using client-based Zero Trust Access, requiring endpoint devices to be enrolled. It provides links for SSO Authentication and Certificates, and notes that Android and iOS devices enroll using SSO Authentication only. A red box highlights the 'Manage' button in the top right corner of this section.

Sicherer Zugriff - Registrierung von ZTA-Zertifikaten

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

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](#)

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 [Upload a CA Certificate](#)

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.

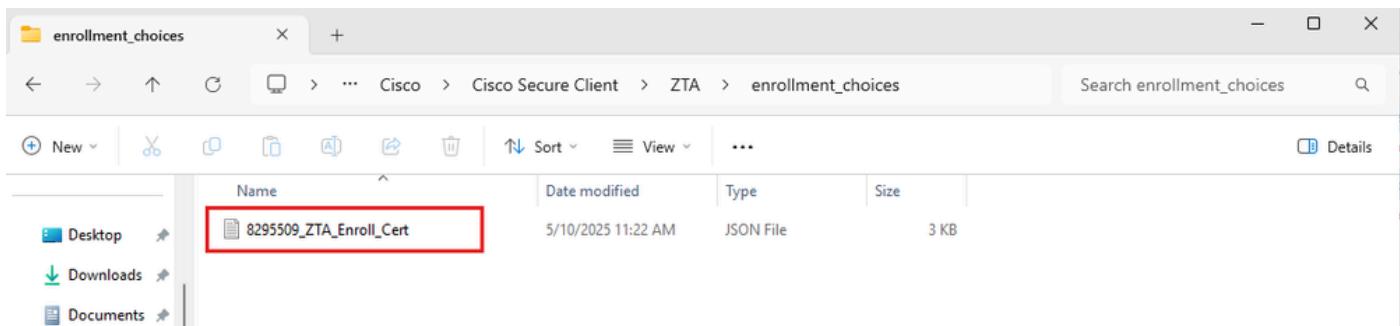
[Save](#) [Cancel](#)

Sicherer Zugriff - Registrierung von ZTA-Zertifikaten

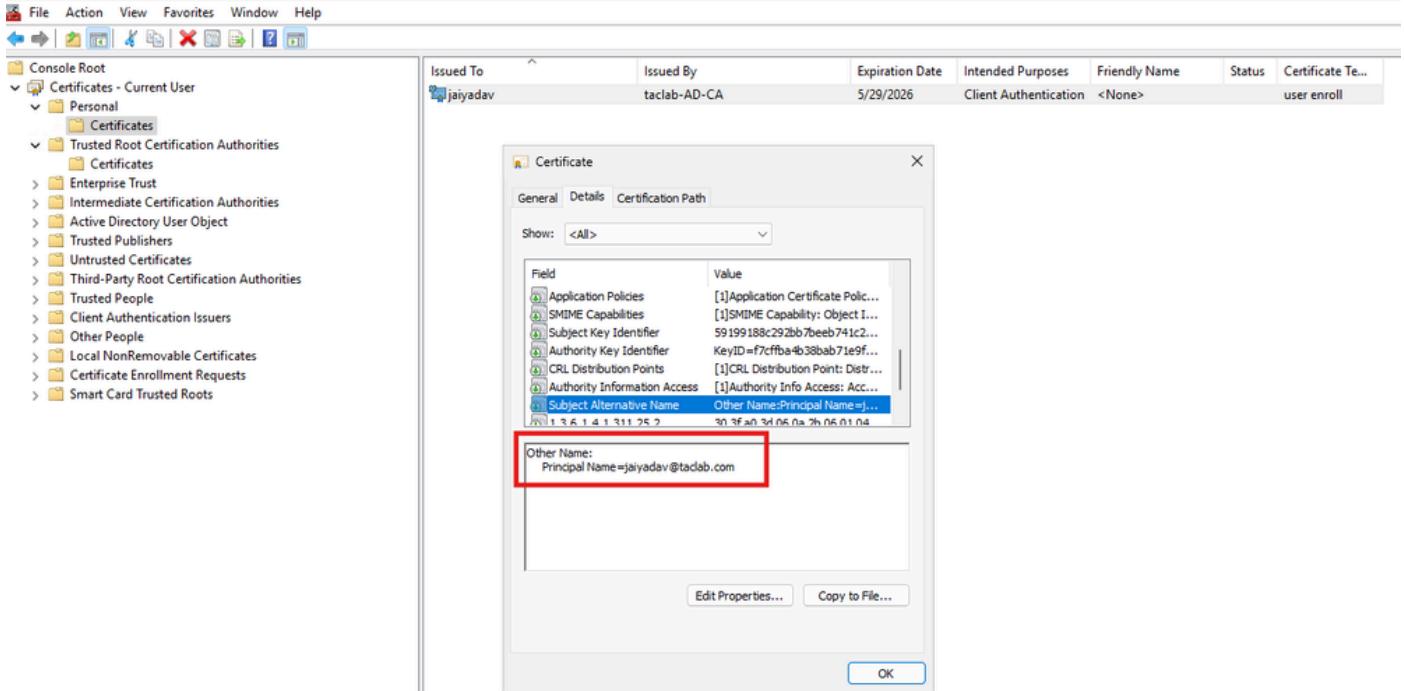
- Klicken Sie Save

Client-Konfiguration

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

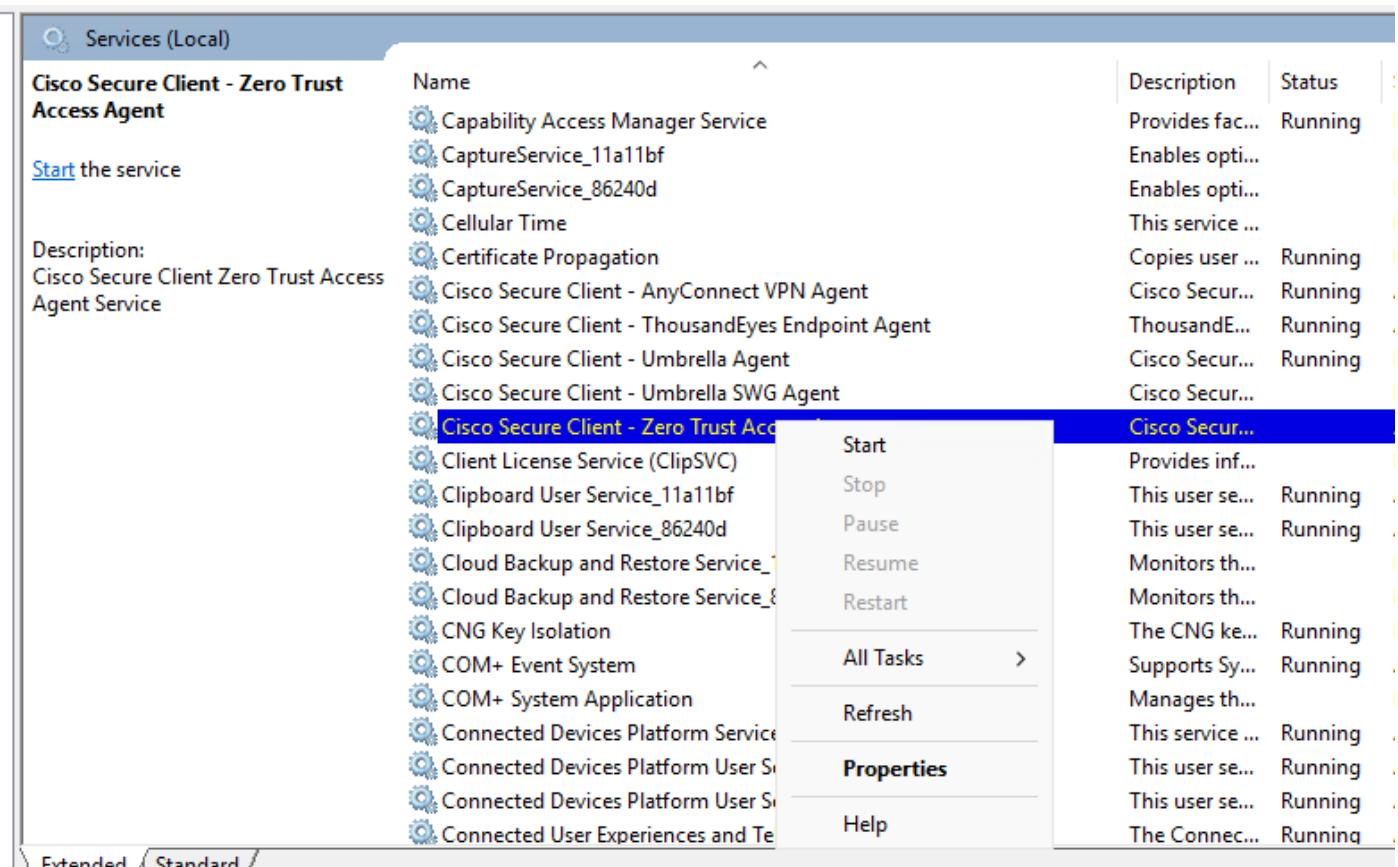


- Erstellen Sie ein Client-Zertifikat, für das UPN im SAN-Feld erforderlich ist.



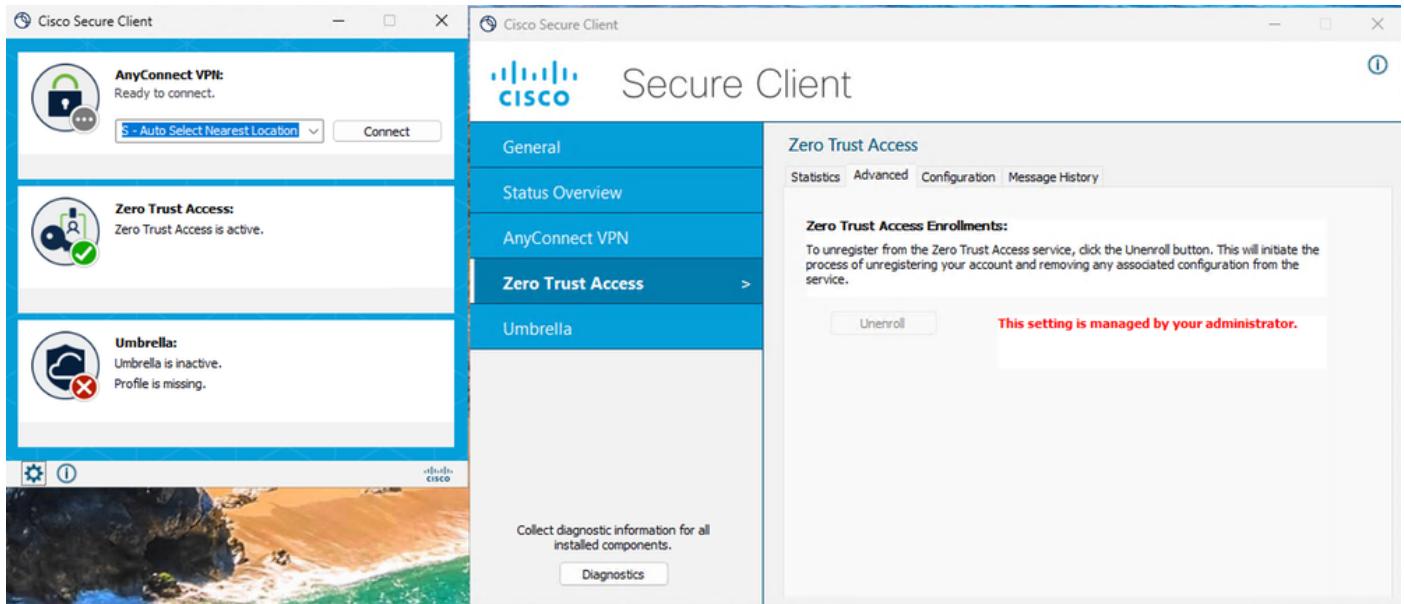
Installation des Zertifikats

- 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.