Configurar acesso seguro para ZTNA universal com FMC gerenciado no local em SCC

Contents

Introdução

Pré-requisitos

- Requisitos
- Componentes Utilizados
- Diagrama de Rede

Informações de suporte

- Dispositivos suportados
- Limitações

Configurar

- Verificar a versão do FMC
- Verificar Versão do FTD
- Verificar licenças de FTD
- Verifique as configurações da plataforma e o DNS configurado corretamente
- Criar um locatário do Security Cloud Control no CDO
- Verifique se as configurações gerais do firewall SCC estão definidas
- Verificar a integração da base de gerenciamento de firewall de controle de segurança e locatário de acesso seguro
- Gerar certificado assinado de CA de FTD (Firewall Threat Defense, Defesa contra Ameaças)
- Centro de gerenciamento de firewall local integrado para controle de segurança na nuvem
- Registrar as configurações do Universal Zero Trust Network Access (ZTNA) no FTD
- Inscreva o cliente na ZTNA
  - Configuração de acesso seguro
  - Configuração do Cliente

Verificar

Informações Relacionadas

Introdução

Este documento descreve como configurar o Universal ZTNA com Secure Access e o FTD virtual gerenciado por um FMC virtual no local.

Pré-requisitos

- O Firewall Management Center (FMC) e o Firewall Threat Defense (FTD) precisam ser implantados usando a versão de software 7.7.10 ou posterior.
- O Firewall Threat Defense (FTD) deve ser gerenciado pelo Firewall Management Center (FMC)

- O Firewall Threat Defense (FTD) deve ser licenciado com criptografia (a criptografia forte deve ser habilitada com o recurso de exportação habilitado), IPS e licenças de ameaças necessárias para controles de segurança
- A configuração básica do Firewall Threat Defense (FTD) deve ser executada no Firewall Management Center (FMC), como interface, roteamento, etc.
- A configuração DNS precisa ser aplicada no dispositivo do FMC para resolver o FQDN do aplicativo
- A versão do Cisco Secure Client precisa ser 5.1.10 ou superior
- O controle da nuvem de segurança é fornecido aos clientes com os sinalizadores de recursos Firewall e Secure Access Micro Apps e UZTNA habilitados

Requisitos

- Todos os dispositivos Secure Firewall Management Center (FMC), incluindo cdFMC e Firewall Threat Defense (FTD), devem executar a versão de software 7.7.10 ou posterior.
- O Firewall Threat Defense (FTD) deve ser gerenciado pelo Firewall Management Center; Gerenciador local O Firewall Defense Manager (FDM) não é suportado
- Todos os dispositivos de Firewall Threat Defense (FTD) devem ser configurados para o modo roteado; não há suporte para o modo transparente.
- Não há suporte para dispositivos em cluster.
- Dispositivos de alta disponibilidade (HA) são suportados; eles são exibidos como uma entidade.
- Secure Client versão 5.1.10 ou posterior

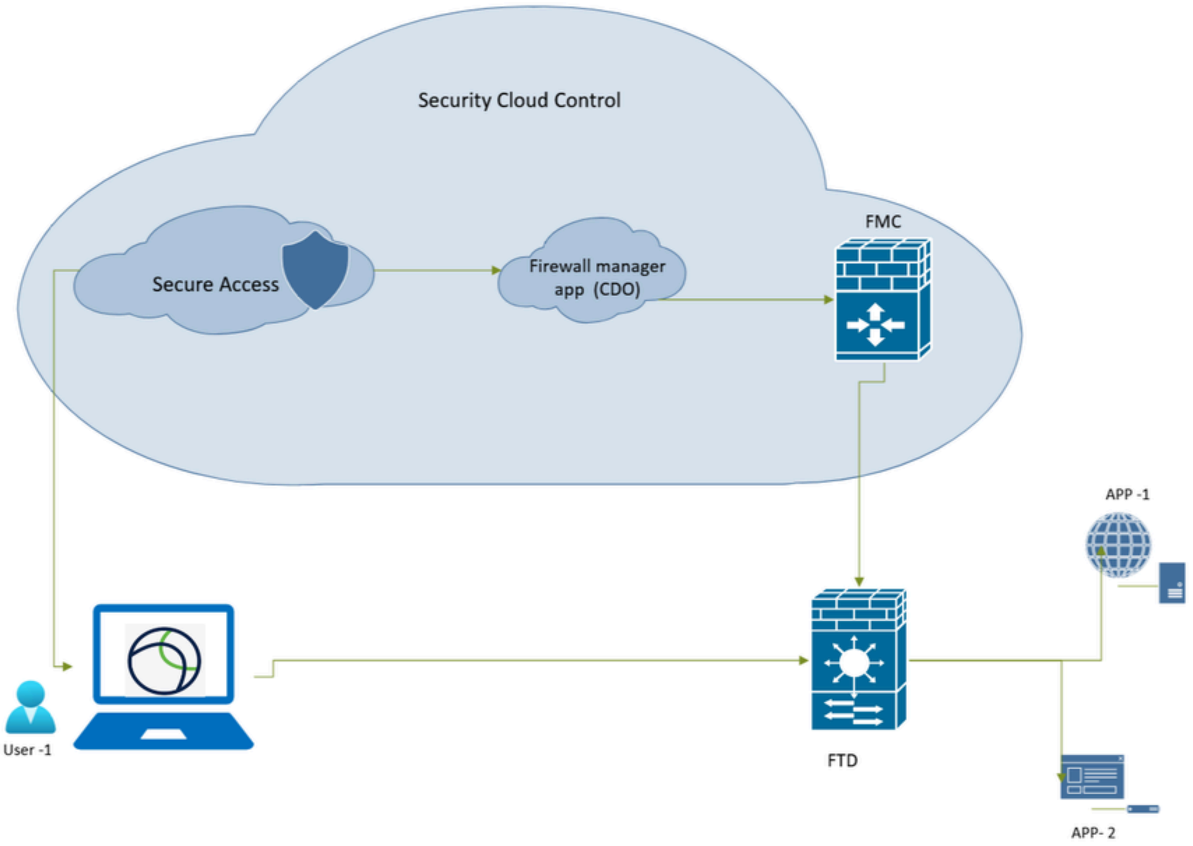
Componentes Utilizados

As informações neste documento são baseadas em

- Controle de nuvem de segurança (SCC)
- Secure Firewall Management Center (FMC) versão 7.7.10
- Secure Firewall Threat Defense (FTD) virtual -100 versão 7.7.10
- Secure Client para Windows versão 5.1.10
- Acesso seguro

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Diagrama de Rede



Acesso seguro - Topologia de rede

Informações de suporte

Dispositivos suportados

Modelos compatíveis com Secure Firewall Threat Defense:

- FPR 1150
- FPR 3105, 3110,3120,3130,3140
- FPR4115,4125,4145,4112
- FPR4215,4225,4245
- Firewall Threat Defense (FTD) virtual com no mínimo 16 núcleos de CPU

Limitações

- Compartilhamento de objetos
- IPv6 sem suporte.
- Somente o VRF global é compatível.
- As políticas ZTNA universais não são aplicadas no tráfego de túnel de site a site para um dispositivo .
- Não há suporte para dispositivos em cluster.

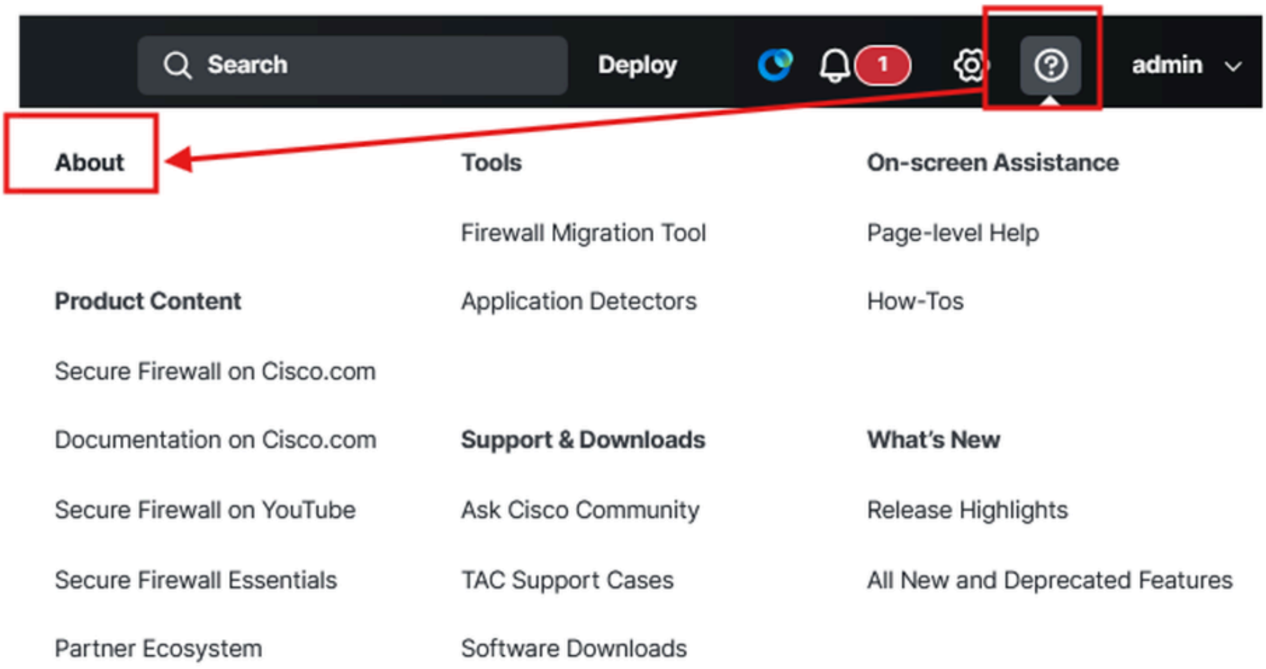
- FTDs implantados como contêineres nas séries 4K e 9K do firepower não são suportados
- As sessões ZTNA universais não suportam quadros jumbo

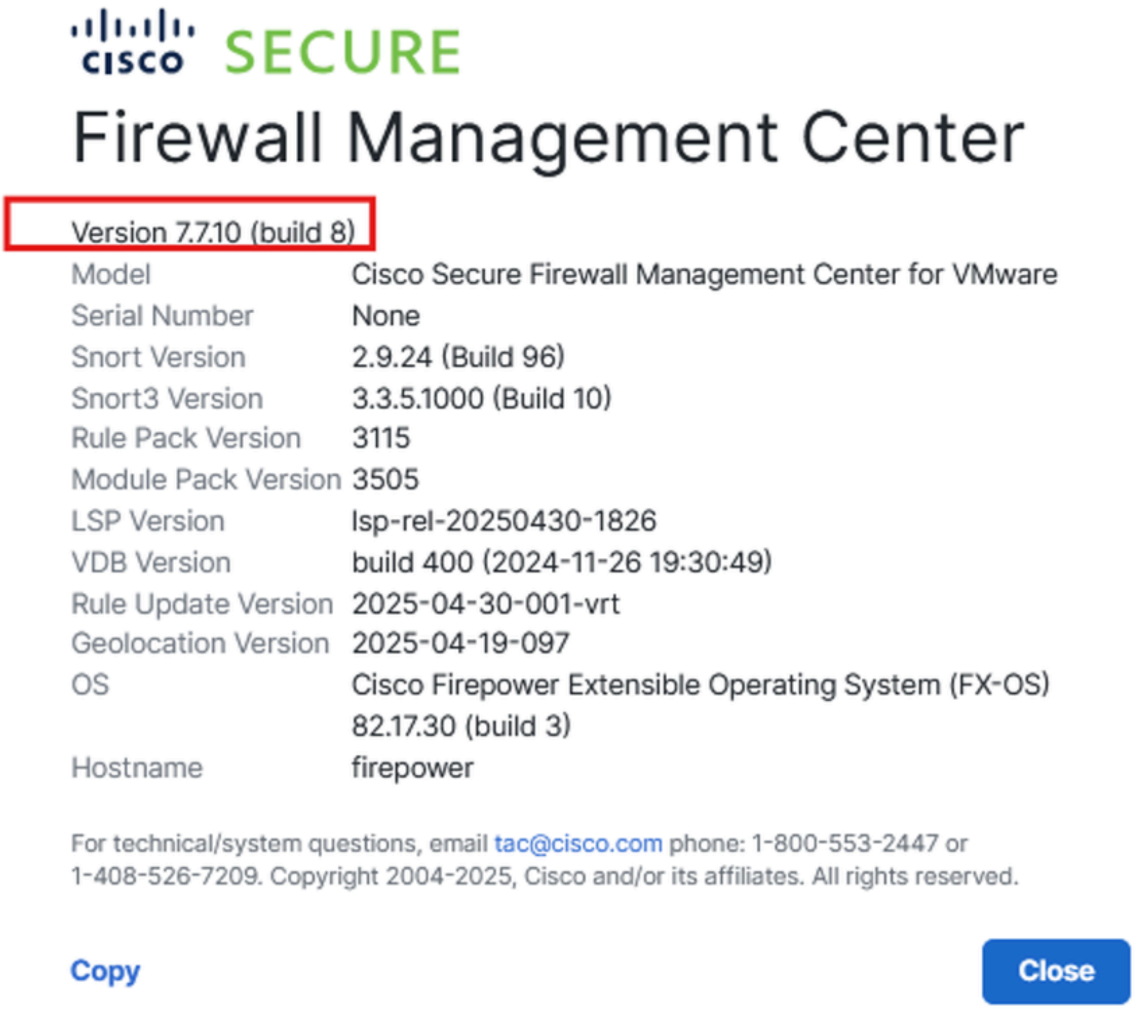
Configurar

Verificar a versão do FMC

Verifique se o Firewall Management Center e o Firewall FTD estão sendo executados na versão de software suportada para ZTNA universal (pode ser 7.7.10 ou superior):

- Clique em ?(canto superior direito) e clique em 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

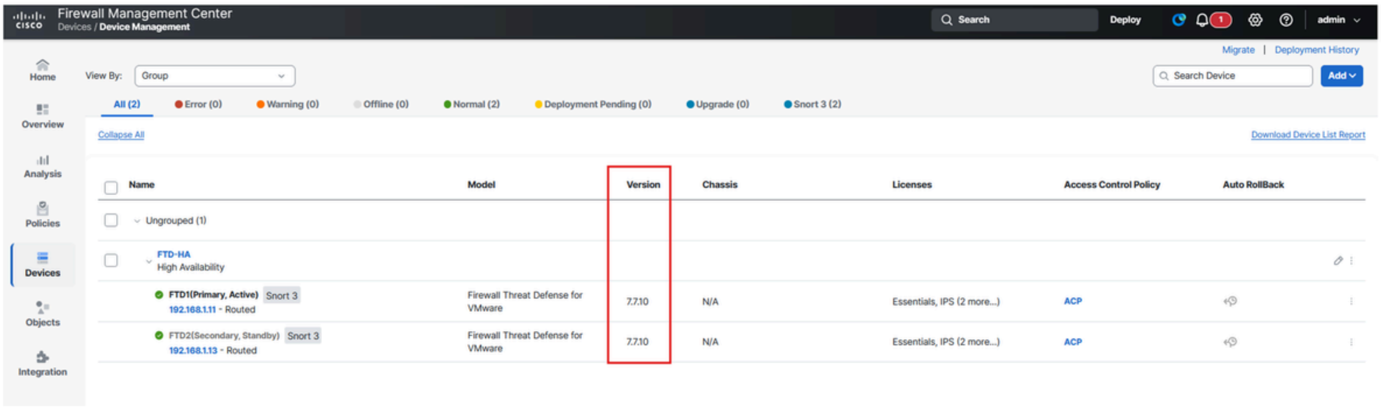
For technical/system questions, email tac@cisco.com phone: 1-800-553-2447 or 1-408-526-7209. Copyright 2004-2025, Cisco and/or its affiliates. All rights reserved.

Secure Firewall Management Center - Versão do software

Verificar Versão do FTD

Navegue até a interface do usuário do FMC:

- Clique emDevices> Device Management

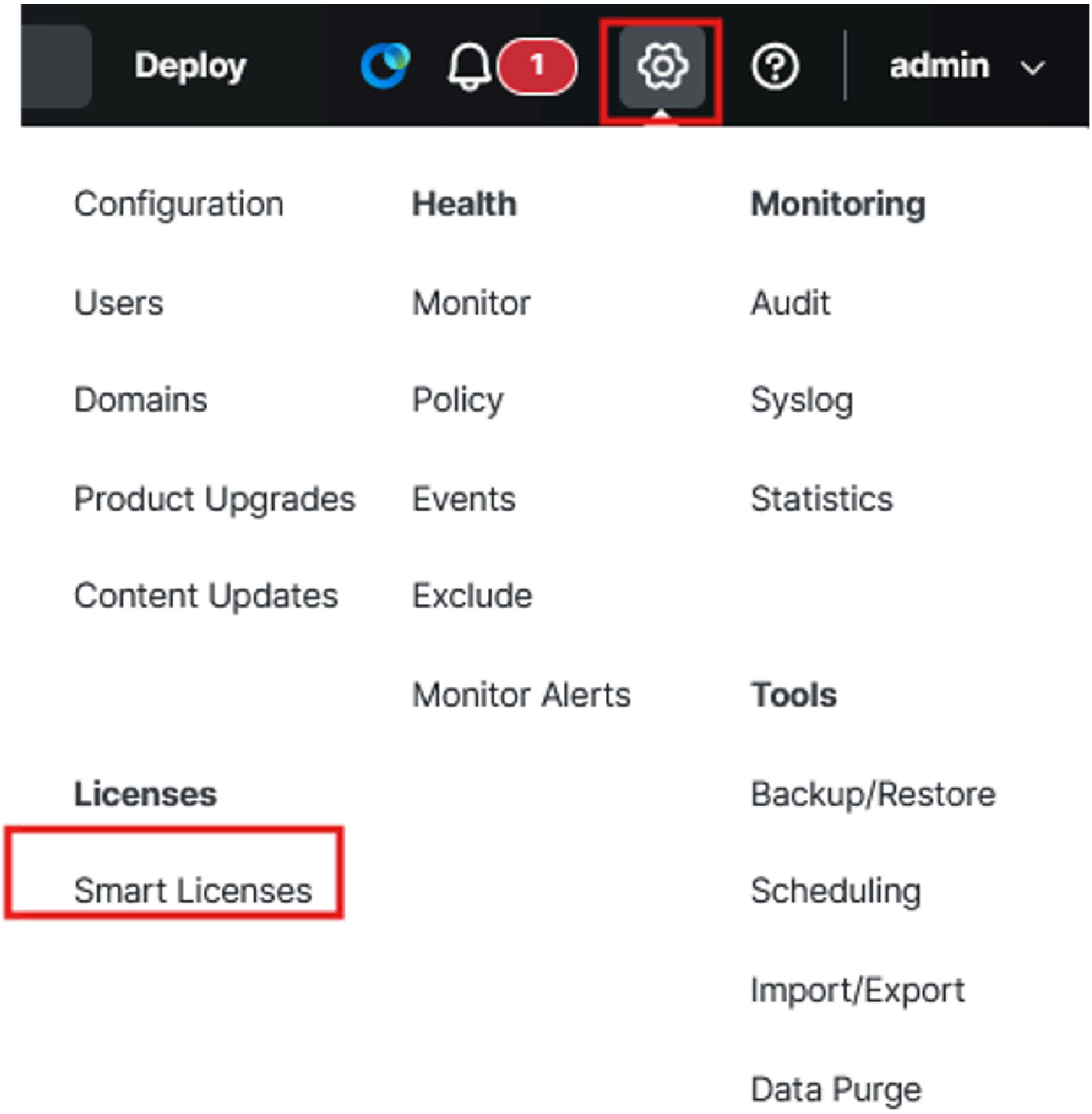


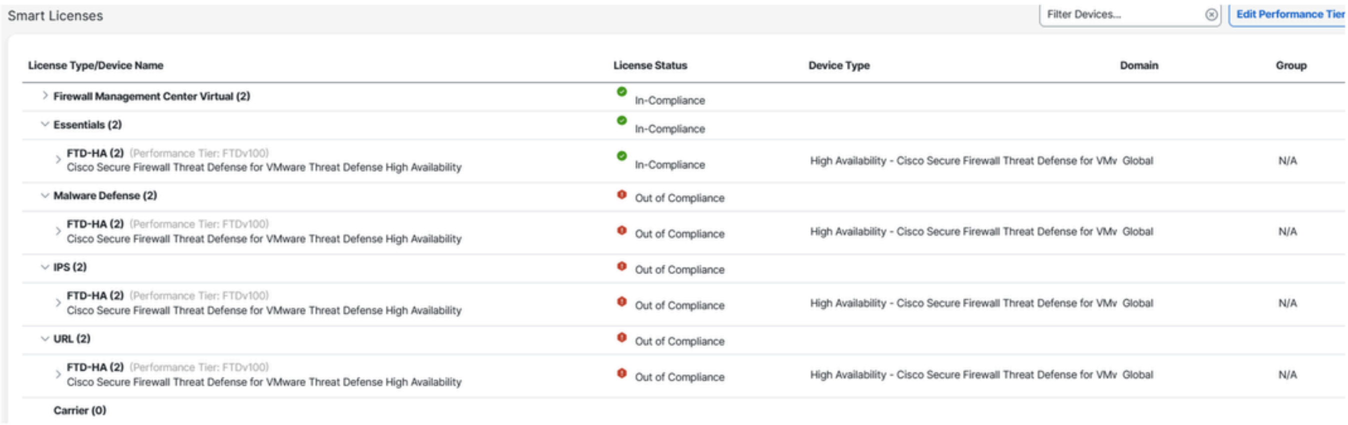
□ Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
□ Ungrouped (1)						
□ FTD-HA High Availability						
FTD1(Primary, Active) Snort 3 192.168.1.11 - Routed	Firewall Threat Defense for VMware	7.7.10	N/A	Essentials, IPS (2 more...)	ACP	
FTD2(Secondary, Standby) Snort 3 192.168.1.13 - Routed	Firewall Threat Defense for VMware	7.7.10	N/A	Essentials, IPS (2 more...)	ACP	

Secure Firewall Threat Defense - Versão do software

Verificar licenças de FTD

- Clique em Setting Icon >Licenses> Smart Licenses





Smart Licenses

License Type/Device Name	License Status	Device Type	Domain	Group
Firewall Management Center Virtual (2)	In-Compliance			
Essentials (2)	In-Compliance			
FTD-HA (2) (Performance Tier: FTDv100) Cisco Secure Firewall Threat Defense for VMware Threat Defense High Availability	In-Compliance	High Availability - Cisco Secure Firewall Threat Defense for VMv	Global	N/A
Malware Defense (2)	Out of Compliance			
FTD-HA (2) (Performance Tier: FTDv100) Cisco Secure Firewall Threat Defense for VMware Threat Defense High Availability	Out of Compliance	High Availability - Cisco Secure Firewall Threat Defense for VMv	Global	N/A
IPS (2)	Out of Compliance			
FTD-HA (2) (Performance Tier: FTDv100) Cisco Secure Firewall Threat Defense for VMware Threat Defense High Availability	Out of Compliance	High Availability - Cisco Secure Firewall Threat Defense for VMv	Global	N/A
URL (2)	Out of Compliance			
FTD-HA (2) (Performance Tier: FTDv100) Cisco Secure Firewall Threat Defense for VMware Threat Defense High Availability	Out of Compliance	High Availability - Cisco Secure Firewall Threat Defense for VMv	Global	N/A
Carrier (0)				

Secure Firewall Threat Defense - Smart Licenses

Verifique as configurações da plataforma e o DNS configurado corretamente

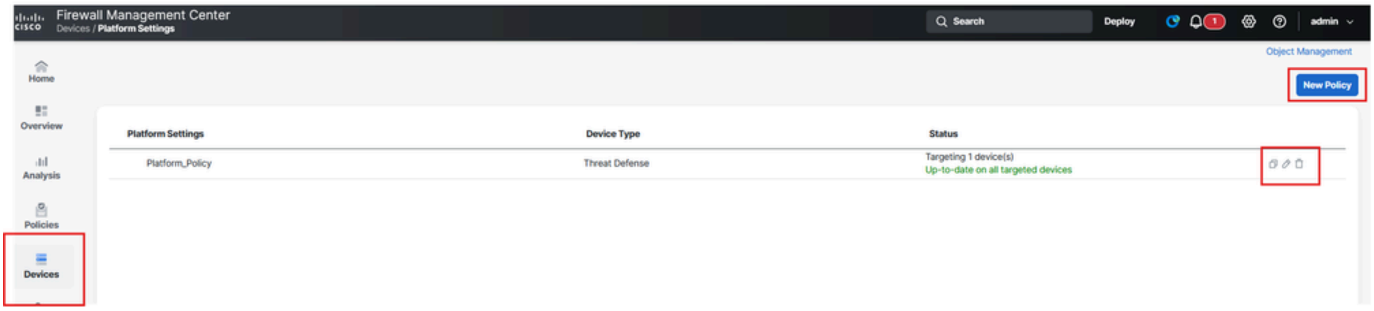
Fazendo login no FTD via CLI:

- Execute o comando para verificar se o DNS está configurado:

```
show run dns
```

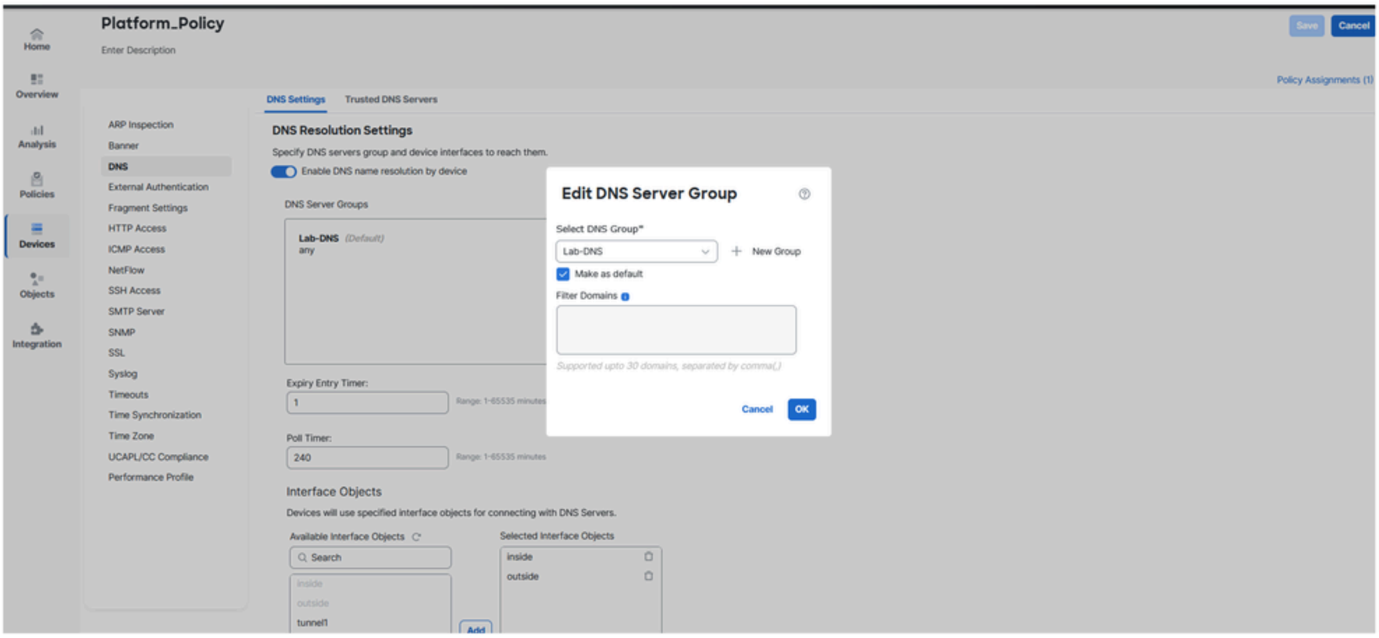
No CVP:

- Clique emDevices> Platform Settings , edite ou crie uma nova política



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

Secure Firewall Threat Defense - Política de plataforma



Platform_Policy

Enter Description

DNS Resolution Settings

Specify DNS servers group and device interfaces to reach them.

Enable DNS name resolution by device

DNS Server Groups

Lab-DNS (Default)
any

Expiry Entry Timer: 1 Range: 1-65535 minutes

Poll Timer: 240 Range: 1-65535 minutes

Interface Objects

Devices will use specified interface objects for connecting with DNS Servers.

Available Interface Objects: inside, outside, tunnel1

Selected Interface Objects: inside, outside

Edit DNS Server Group

Select DNS Group*: Lab-DNS

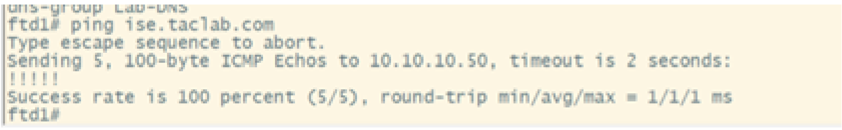
☑ Make as default

Filter Domains

Supported upto 30 domains, separated by comma(,)

Secure Firewall Threat Defense - Configuração do DNS

Verifique via FTD cli se você pode fazer ping no endereço IP e no FQDN dos recursos privados (se quiser acessar o PR usando seu FQDN).



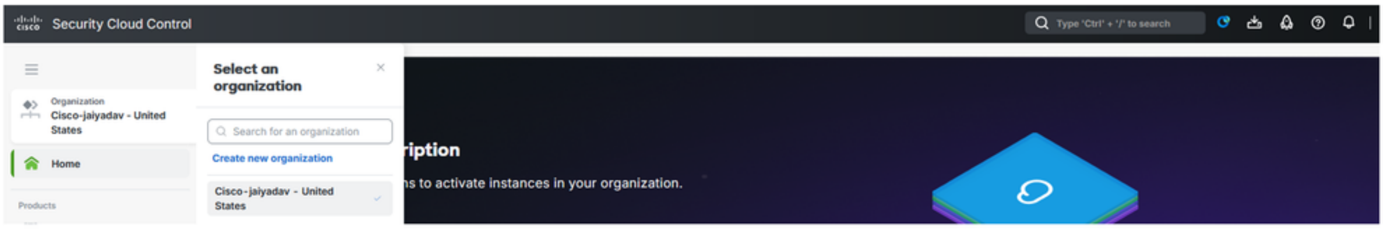
```
dns-group Lab-DNS
ftd1# ping ise.taclab.com
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.50, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
ftd1#
```

Criar um locatário do Security Cloud Control no CDO

Note: Se você já tiver um espaço SCC configurado, não será necessário criar um novo espaço.

Navegue até Security Cloud Control:

- Clique emOrganization > Create new organization

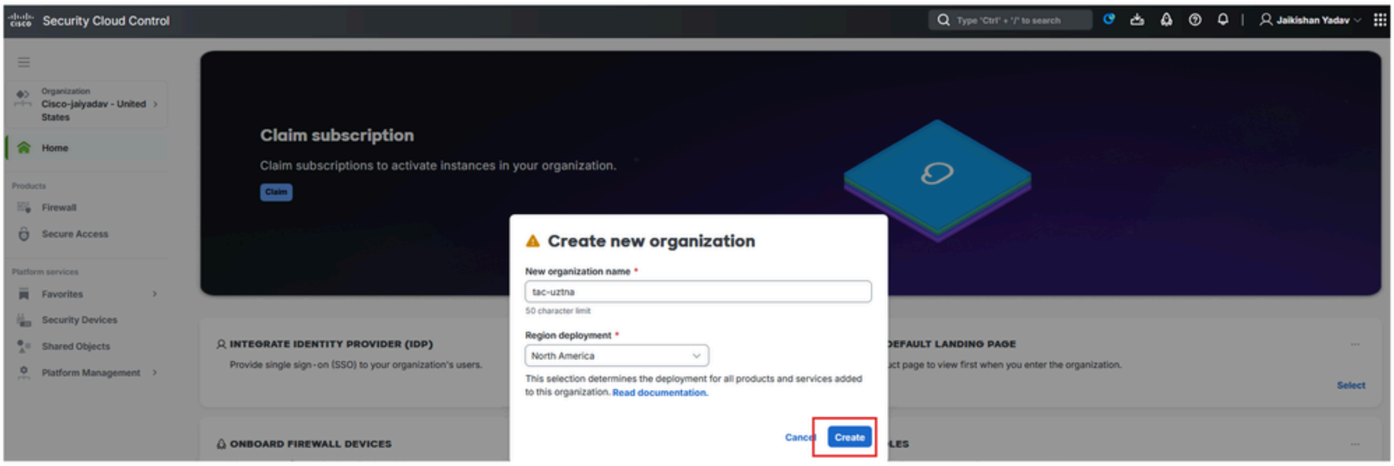

Security Cloud Control
Type 'Ctrl' + '/' to search
Home
Products
Select an organization
Search for an organization
Create new organization
ription
s to activate instances in your organization.

Organization: Cisco-jaiyadav - United States

Cisco-jaiyadav - United States

Controle de nuvem seguro - Organização

- Clique em Create



Claim subscription

Claim subscriptions to activate instances in your organization.

Provide single sign-on (SSO) to your organization's users.

...ct page to view first when you enter the organization.

Create new organization

New organization name *: tac-uztna

50 character limit

Region deployment *: North America

This selection determines the deployment for all products and services added to this organization. Read documentation.

Controle de nuvem seguro - Criação de organização

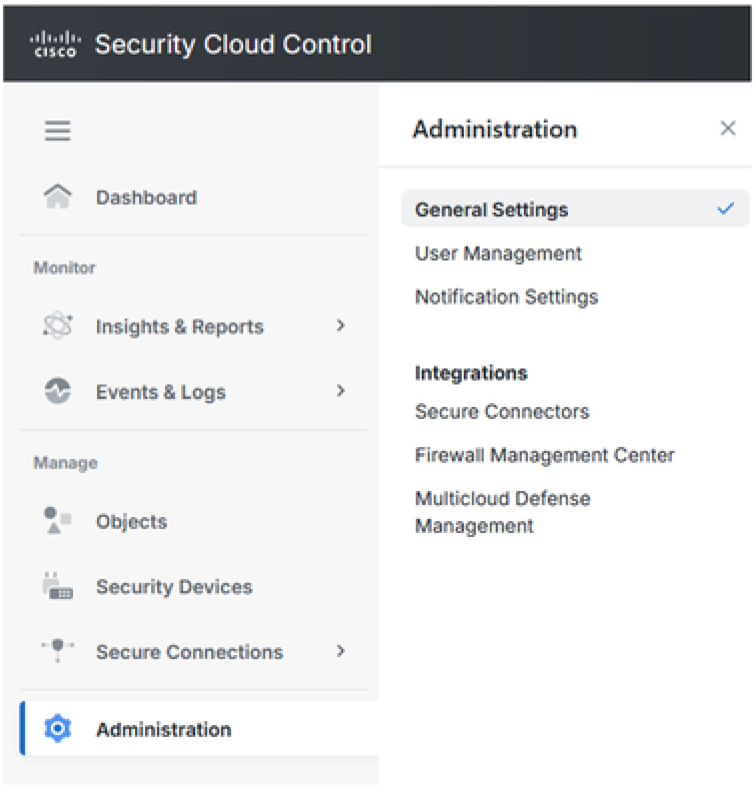
Depois que o espaço SCC for criado , reúna as informações do espaço para habilitar o firewall e o microaplicativo Secure Access e habilitar a ZTNA.

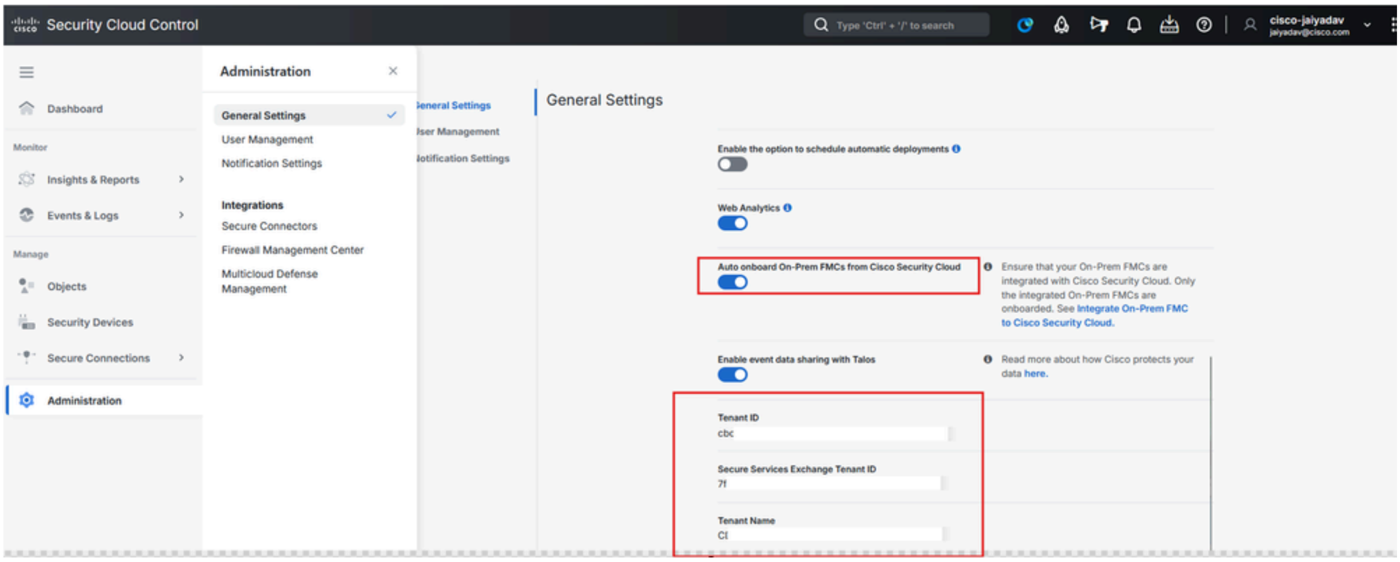
Verifique se as configurações gerais do firewall SCC estão definidas

Navegue até CDO/SCC:

- Clique emAdministration> General Settings
- Verifique se Auto onboard On-Prem FMCs from Cisco Security Cloud a opção está habilitada.

Note: O usuário que está tentando acessar o Secure Access MicroApp deve terSecure Accessfunções de administrador e Security Cloud Control .





General Settings

Enable the option to schedule automatic deployments ○

Web Analytics ●

Auto onboard On-Prem FMCs from Cisco Security Cloud ●

Ensure that your On-Prem FMCs are integrated with Cisco Security Cloud. Only the integrated On-Prem FMCs are onboarded. See Integrate On-Prem FMC to Cisco Security Cloud.

Enable event data sharing with Talos ●

Read more about how Cisco protects your data here.

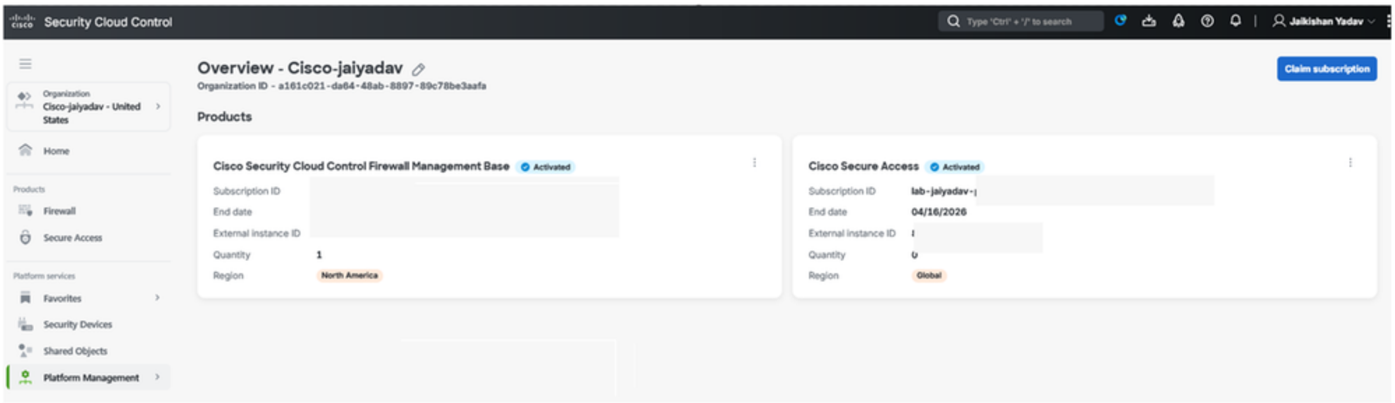
Tenant ID
cbc [redacted]

Secure Services Exchange Tenant ID
7f [redacted]

Tenant Name
Cl [redacted]

Controle de nuvem seguro - Detalhes da empresa

Verificar a integração da base de gerenciamento de firewall de controle de segurança e locatário de acesso seguro



Overview - Cisco-jaiyadav
Organization ID - a161c021-da64-48ab-8897-89c78be3aafa

Products

Cisco Security Cloud Control Firewall Management Base

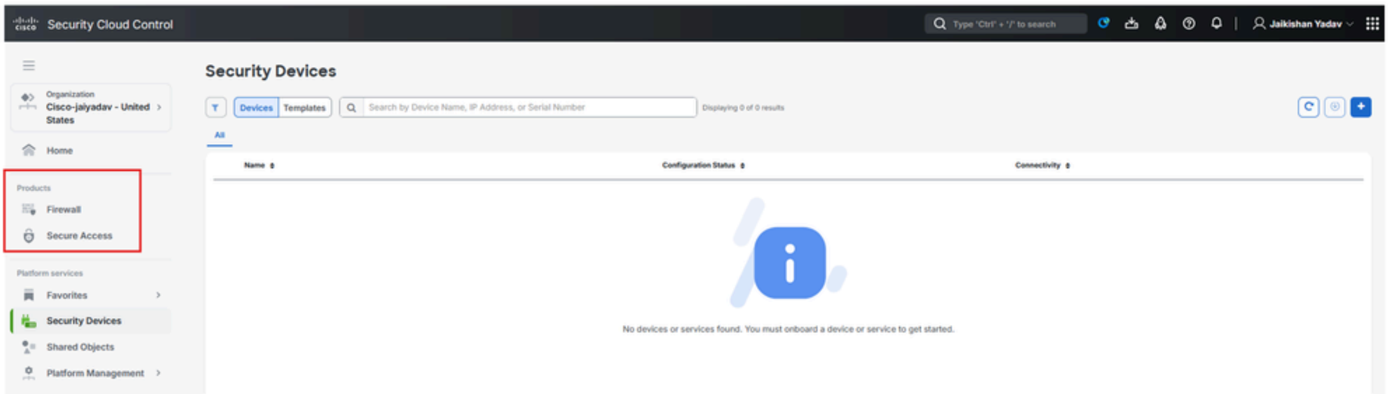
Subscription ID [redacted]
End date
External instance ID
Quantity 1
Region North America

Cisco Secure Access

Subscription ID lab-jaiyadav-[redacted]
End date 04/16/2026
External instance ID [redacted]
Quantity 0
Region Global

Controle de nuvem seguro - Ativação de acesso seguro

Depois de concluir a etapa [Criar um locatário do Security Cloud Control no CDO]() e [Criar um locatário do Security Cloud Control no CDO](), você poderá ver os microaplicativos Firewall e Secure Access no painel do SCC:



Security Devices

Displaying 0 of 0 results

No devices or services found. You must onboard a device or service to get started.

Controle de nuvem seguro - Microaplicativos

Gerar certificado assinado de CA de FTD (Firewall Threat Defense, Defesa contra Ameaças)

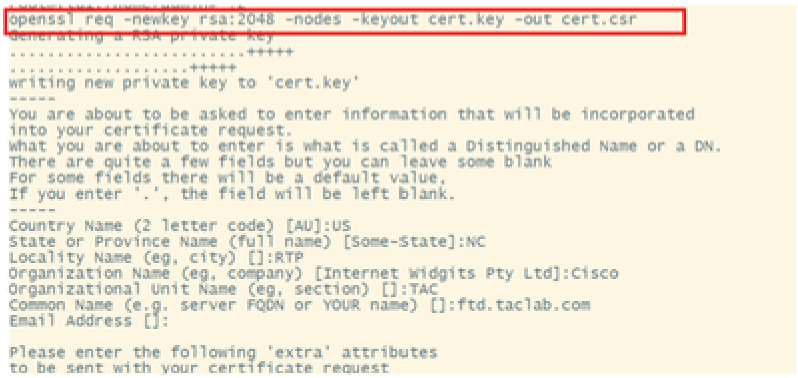
> Note: Você também pode usar certificados FTD autoassinados [Certificados FTD]() (consulte a seção Geração de Certificados CA Internos e Internos AutoAssinados). O certificado deve estar no formato PKCS12 e deve estar presente no armazenamento do computador do usuário sob a CA raiz confiável.

Para gerar um certificado assinado por CA usando FTD no recurso build openssl:

- Navegar para FTD
- Executar`expert`comando

- Gerar CSR e chave usando openssl
  - Comando do 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
```

Solicitação de assinatura de certificado

- Copiar o CSR e obter um certificado assinado pela CA
- Usar certificado e chave assinados por CA FTD e converter certificado no formato PKCS12
  - Comando do OpenSSL:

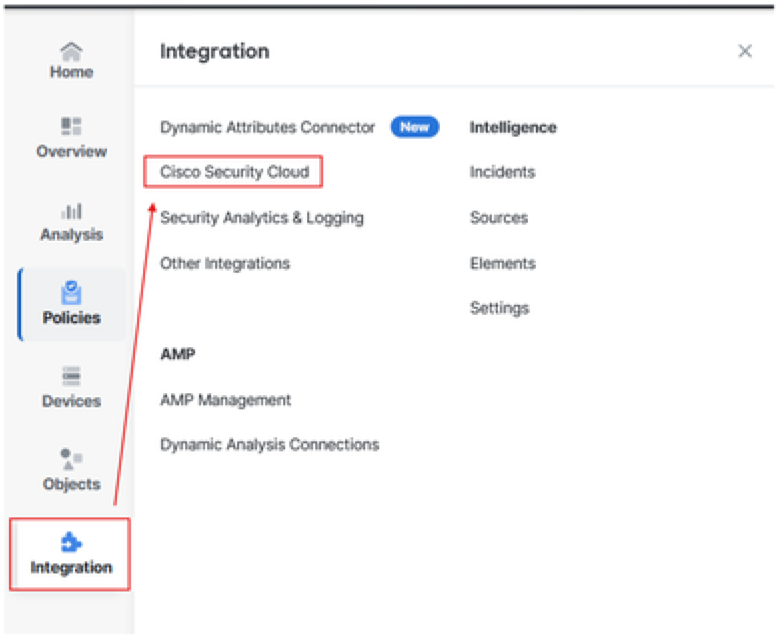
```
openssl pkcs12 -export -out ftdcert.p12 -in cert.crt -inkey cert.key
```

- Exporte o certificado usando SCP ou outra ferramenta.

Centro de gerenciamento de firewall local integrado para controle de segurança na nuvem

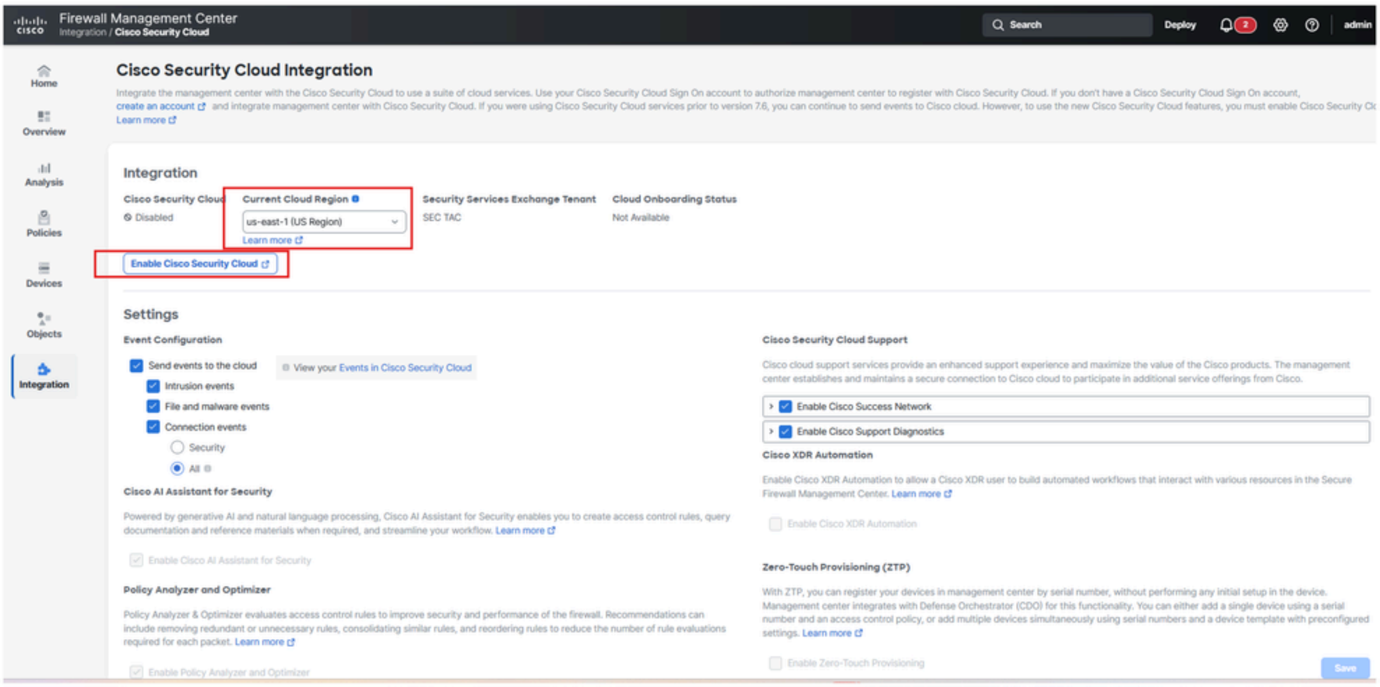
Navegue até o FMC:

- Clique emIntegration> Cisco Security Cloud



Centro de gerenciamento de firewall e integração SCC

- Escolha a região da nuvem e clique em Enable Cisco Security Cloud



Cisco Security Cloud Integration

Integrate the management center with the Cisco Security Cloud to use a suite of cloud services. Use your Cisco Security Cloud Sign On account to authorize management center to register with Cisco Security Cloud. If you don't have a Cisco Security Cloud Sign On account, create an account and integrate management center with Cisco Security Cloud. If you were using Cisco Security Cloud services prior to version 7.6, you can continue to send events to Cisco cloud. However, to use the new Cisco Security Cloud features, you must enable Cisco Security Cl
Learn more

Integration

Cisco Security Cloud	Current Cloud Region	Security Services Exchange Tenant	Cloud Onboarding Status
Disabled	us-east-1 (US Region)	SEC TAC	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

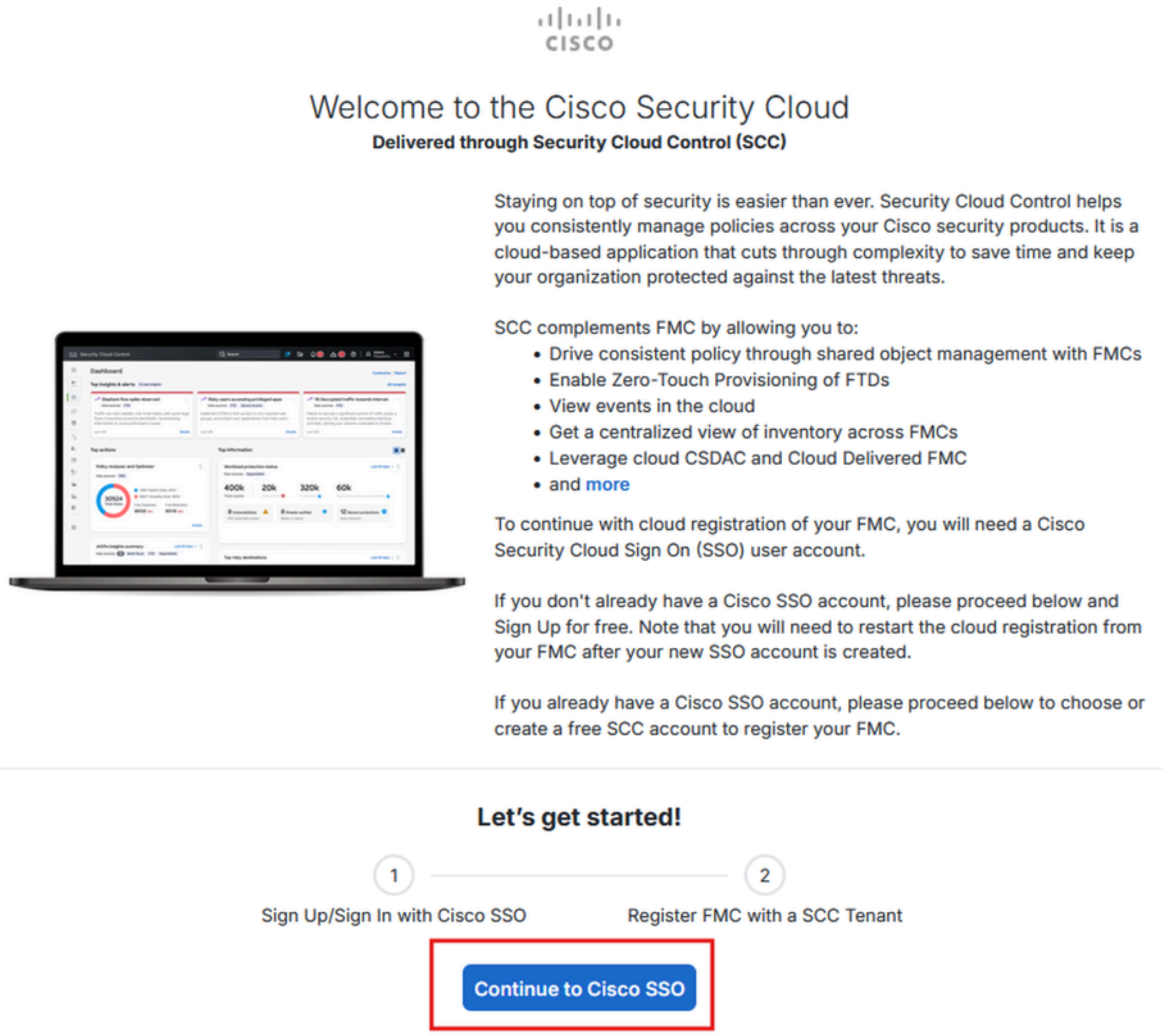
Save

Integração do Centro de gerenciamento de firewall ao SCC

Ele abrirá uma nova guia do navegador, na nova guia:

- Clique em Continue to Cisco SSO

Note: Certifique-se de que você está desconectado do SCC e não tem nenhuma outra guia aberta.



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.

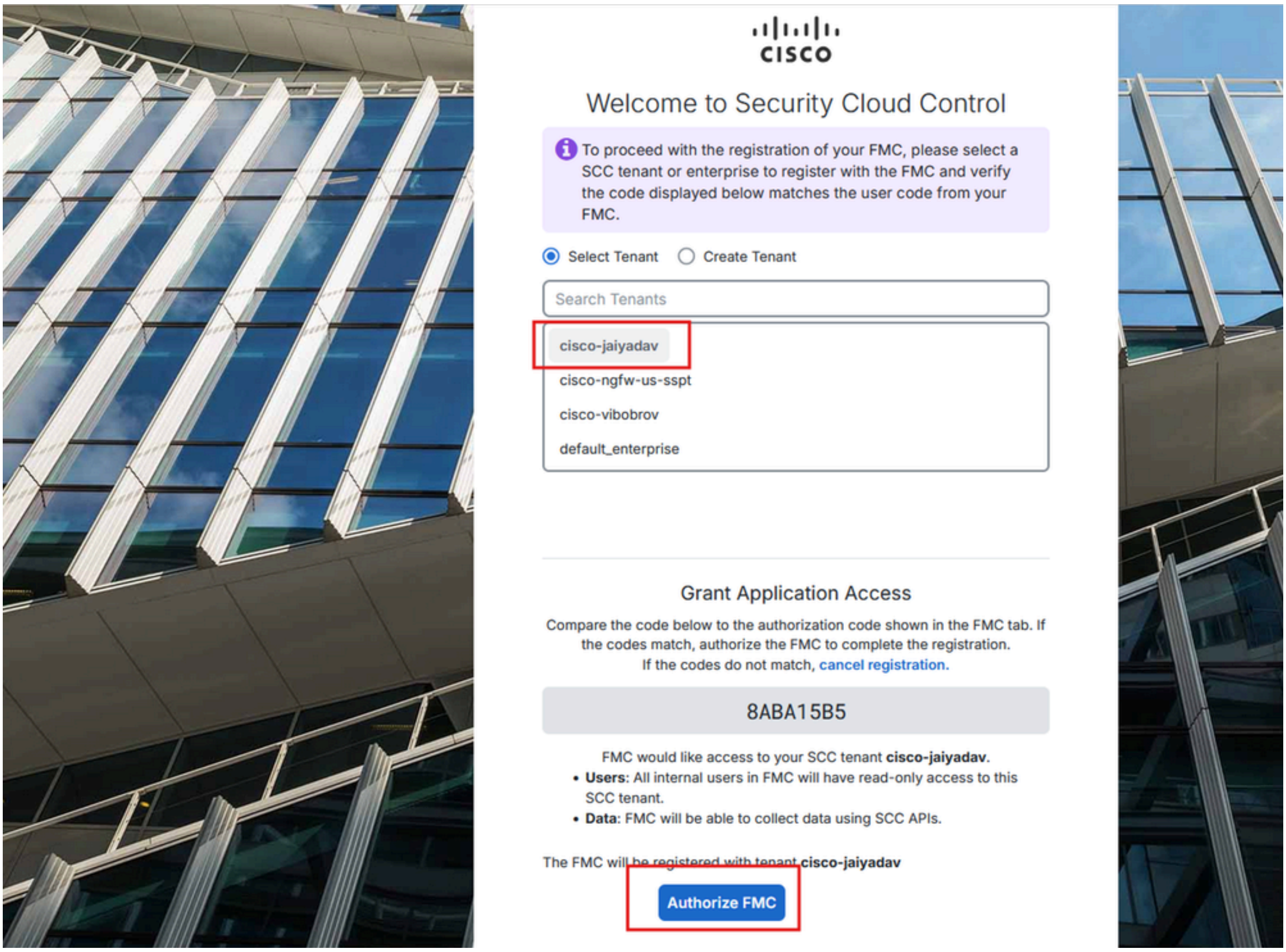
Let's get started!

1 Sign Up/Sign In with Cisco SSO

2 Register FMC with a SCC Tenant

Integração do Centro de gerenciamento de firewall ao SCC

- Escolha seu locatário SCC e clique em 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

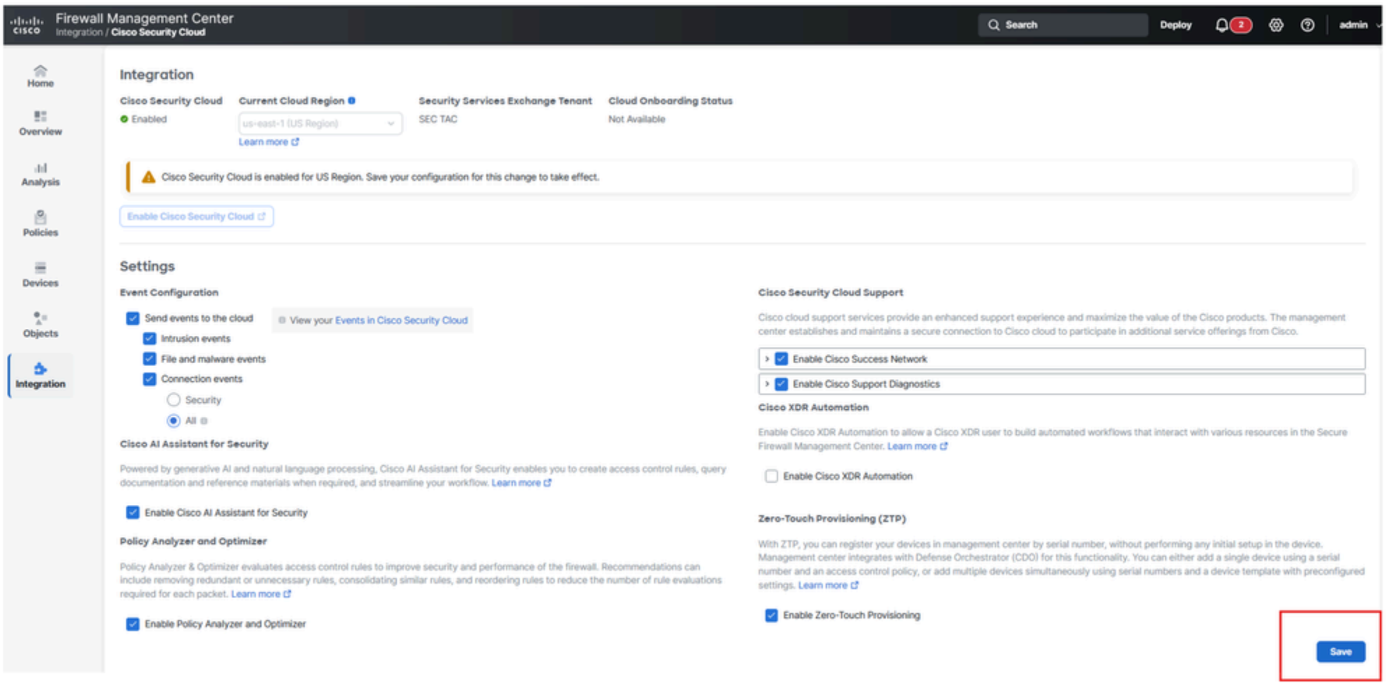
FMC would like access to your SCC tenant **cisco-jaiyadav**.

- **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**

Integração do Centro de gerenciamento de firewall ao SCC

- Clique em Save



cisco
Firewall Management Center
Integration / Cisco Security Cloud
Search
Deploy
2
admin
Home
Overview
Analysis
Policies
Devices
Objects
Integration

Integration

Cisco Security Cloud	Current Cloud Region	Security Services Exchange Tenant	Cloud Onboarding Status
Enabled	us-east-1 (US Region) Learn more	SEC TAC	Not Available

Cisco Security Cloud is enabled for US Region. Save your configuration for this change to take effect.

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

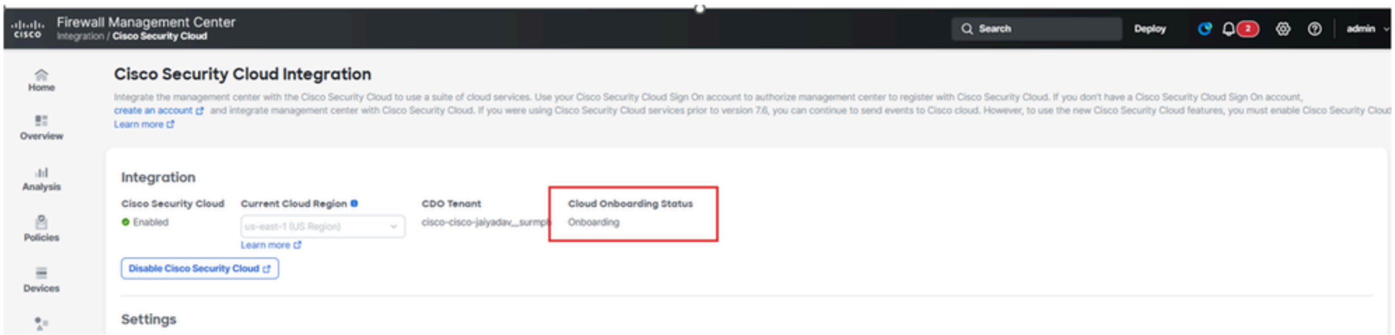
Zero-Touch Provisioning (ZTP)

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

Integração do Centro de gerenciamento de firewall ao SCC

O status de Cloud Onboarding Status deve mudar de **Not Available** para Onboarding e, em seguida, Online.



Firewall Management Center
Integration / Cisco Security Cloud
Search
Deploy
admin
Home
Overview
Analysis
Policies
Devices

Cisco Security Cloud Integration

Integrate the management center with the Cisco Security Cloud to use a suite of cloud services. Use your Cisco Security Cloud Sign On account to authorize management center to register with Cisco Security Cloud. If you don't have a Cisco Security Cloud Sign On account, create an account and integrate management center with Cisco Security Cloud. If you were using Cisco Security Cloud services prior to version 7.6, you can continue to send events to Cisco cloud. However, to use the new Cisco Security Cloud features, you must enable Cisco Security Cloud

Learn more

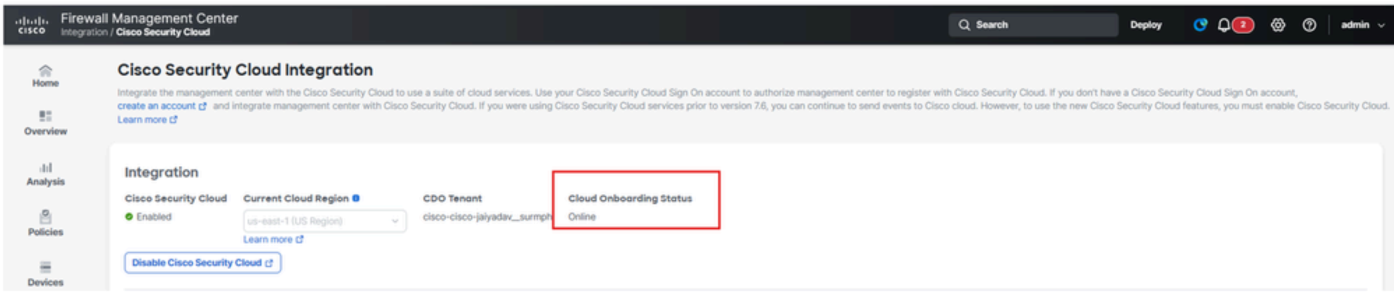
Integration

Cisco Security Cloud	Current Cloud Region	CDO Tenant	Cloud Onboarding Status
Enabled	us-east-1 (US Region)	cisco-cisco-jaiyadav__surmpl	Onboarding

Learn more

Disable Cisco Security Cloud

Settings



Firewall Management Center
Integration / Cisco Security Cloud
Search
Deploy
admin
Home
Overview
Analysis
Policies
Devices

Cisco Security Cloud Integration

Integrate the management center with the Cisco Security Cloud to use a suite of cloud services. Use your Cisco Security Cloud Sign On account to authorize management center to register with Cisco Security Cloud. If you don't have a Cisco Security Cloud Sign On account, create an account and integrate management center with Cisco Security Cloud. If you were using Cisco Security Cloud services prior to version 7.6, you can continue to send events to Cisco cloud. However, to use the new Cisco Security Cloud features, you must enable Cisco Security Cloud.

Learn more

Integration

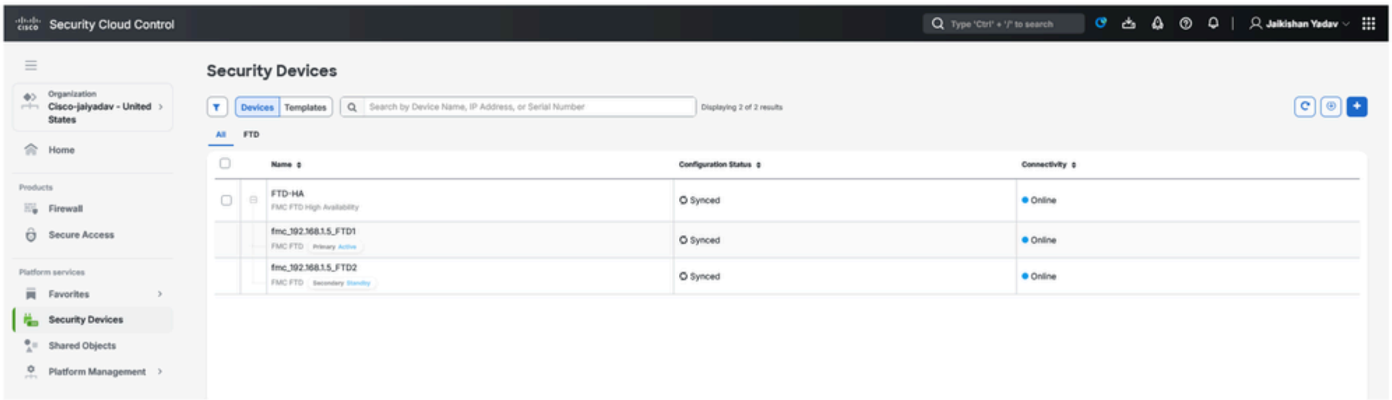
Cisco Security Cloud	Current Cloud Region	CDO Tenant	Cloud Onboarding Status
Enabled	us-east-1 (US Region)	cisco-cisco-jaiyadav__surmpl	Online

Learn more

Disable Cisco Security Cloud

Status de Integração do Centro de Gerenciamento de Firewall

- Navegue até [SCC](SCC) e verifique o status do FTD emPlatform Services> Security Devices



Security Devices

Search by Device Name, IP Address, or Serial Number

Displaying 2 of 2 results

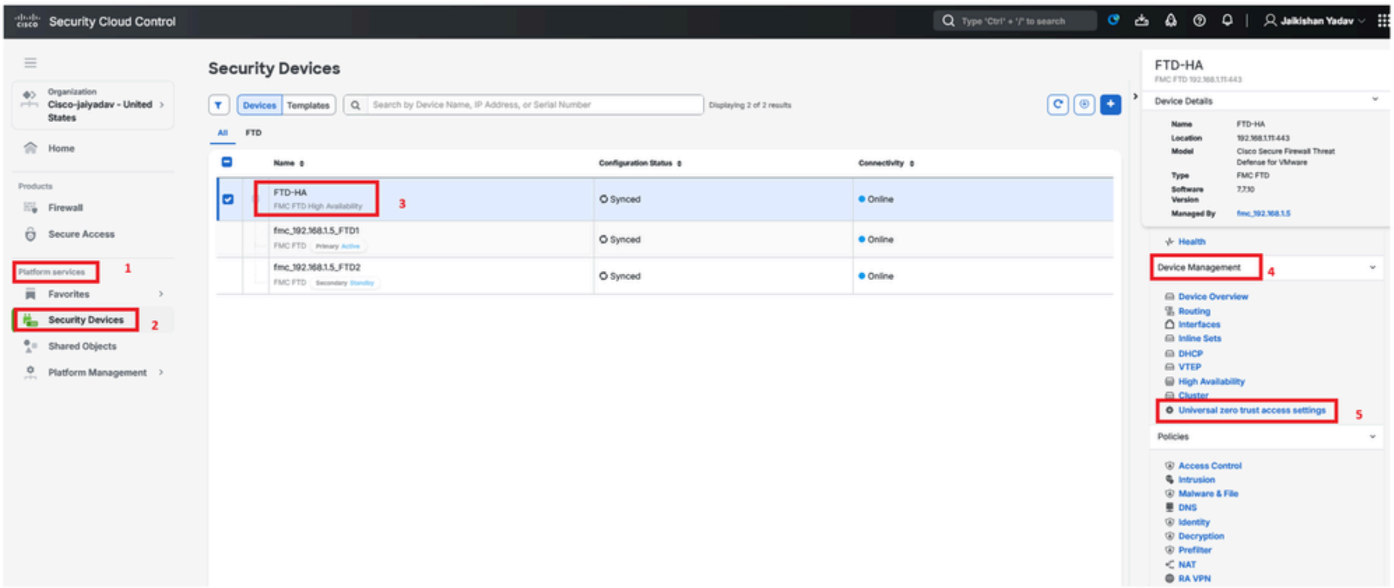
Name	Configuration Status	Connectivity
FTD-HA FMC FTD High Availability	Synced	Online
fmc_192.168.1.5_FTD1 FMC FTD Primary Active	Synced	Online
fmc_192.168.1.5_FTD2 FMC FTD Secondary Standby	Synced	Online

Status da defesa contra ameaças do firewall seguro no SCC

Registrar as configurações do Universal Zero Trust Network Access (ZTNA) no FTD

Navegue até SCC:

- Clique em Platform Services > **Security Devices** > **FTD** > **Device Management** > Universal Zero Trust Network Access



	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

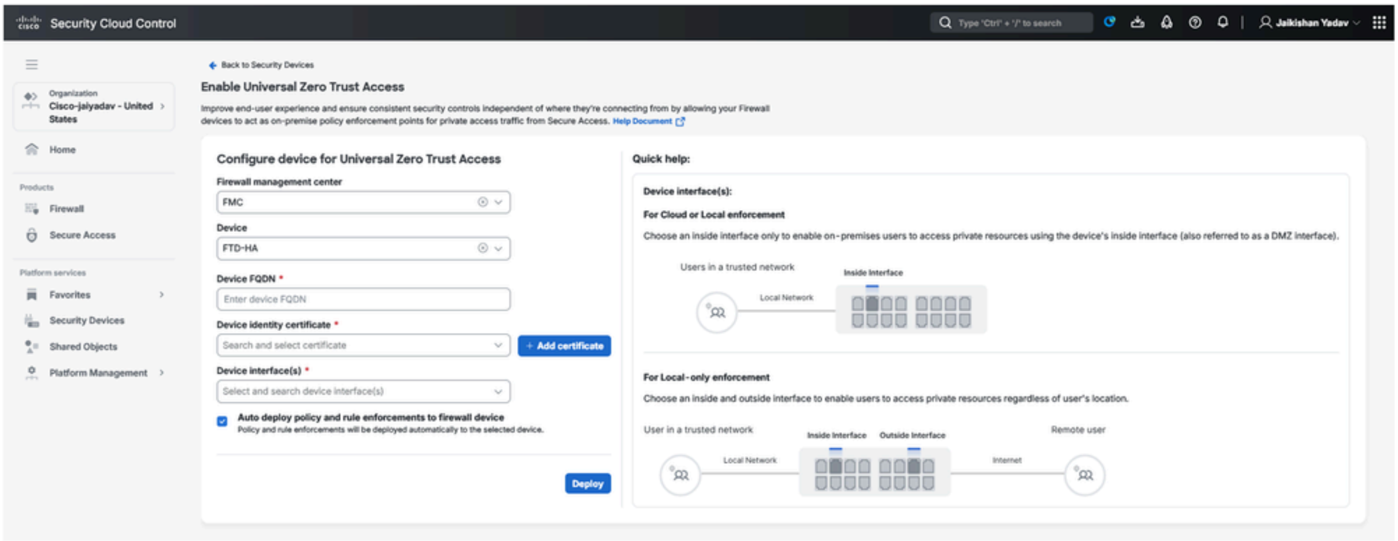
FTD-HA
FMC FTD 192.168.1.11:443

Device Details

Name	FTD-HA
Location	192.168.1.11:443
Model	Cisco Secure Firewall Threat Defense for VMware
Type	FMC FTD
Software Version	7.7.10
Managed By	fmc_192.168.1.5

Secure Firewall Threat Defense - Configuração universal do ZTNA

- Preencha as informações e carregue o certificado FTD gerado na etapa Gerar um certificado assinado CA FTD (Firewall Threat Defense)



Enable Universal Zero Trust Access

Improve end-user experience and ensure consistent security controls independent of where they're connecting from by allowing your Firewall devices to act as on-premise policy enforcement points for private access traffic from Secure Access. Help Document

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

Device interface(s) *: Select and search device interface(s)

☑ Auto deploy policy and rule enforcements to firewall device
Policy and rule enforcements will be deployed automatically to the selected device.

Quick help:

Device interface(s):

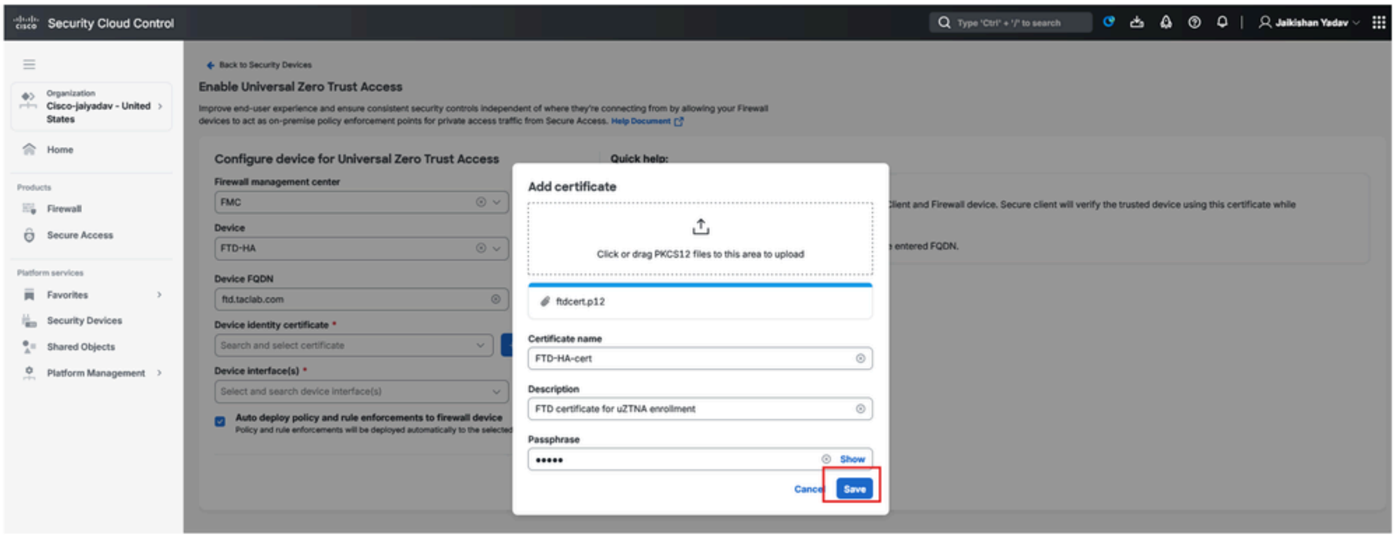
For Cloud or Local enforcement

Choose an inside interface only to enable on-premises users to access private resources using the device's inside interface (also referred to as a DMZ interface).

For Local-only enforcement

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

Secure Firewall Threat Defense - Configuração universal do ZTNA



Security Cloud Control

Organization
Cisco-jaiyadav - United States

Back to Security Devices

Enable Universal Zero Trust Access

Improve end-user experience and ensure consistent security controls independent of where they're connecting from by allowing your Firewall devices to act as on-premise policy enforcement points for private access traffic from Secure Access. Help Document

Configure device for Universal Zero Trust Access

Firewall management center: FMC

Device: FTD-HA

Device FQDN: ftd.taclab.com

Device identity certificate *: Search and select certificate

Device interface(s) *: Select and search device interface(s)

☑ Auto deploy policy and rule enforcements to firewall device
Policy and rule enforcements will be deployed automatically to the selected

Quick help:

Client and Firewall device. Secure client will verify the trusted device using this certificate while

entered FQDN.

Add certificate

Click or drag PKCS12 files to this area to upload

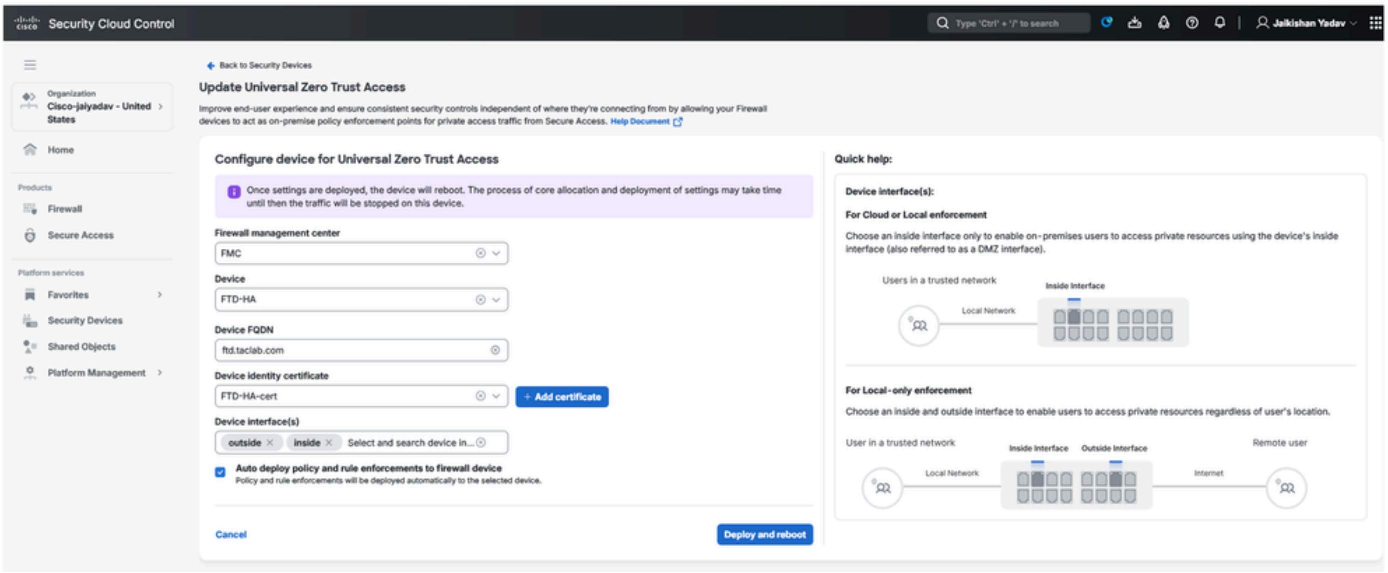
ftdcert.p12

Certificate name: FTD-HA-cert

Description: FTD certificate for uZTNA enrollment

Passphrase: ●●●●● Show

Secure Firewall Threat Defense - Configuração universal do ZTNA



Security Cloud Control

Organization
Cisco-jaiyadav - United States

Back to Security Devices

Update Universal Zero Trust Access

Improve end-user experience and ensure consistent security controls independent of where they're connecting from by allowing your Firewall devices to act as on-premise policy enforcement points for private access traffic from Secure Access. Help Document

Configure device for Universal Zero Trust Access

Once settings are deployed, the device will reboot. The process of core allocation and deployment of settings may take time until then the traffic will be stopped on this device.

Firewall management center: FMC

Device: FTD-HA

Device FQDN: ftd.taclab.com

Device identity certificate: FTD-HA-cert

Device interface(s): outside × inside × Select and search device in...

☑ Auto deploy policy and rule enforcements to firewall device
Policy and rule enforcements will be deployed automatically to the selected device.

Quick help:

Device interface(s):

For Cloud or Local enforcement

Choose an inside interface only to enable on-premises users to access private resources using the device's inside interface (also referred to as a DMZ interface).

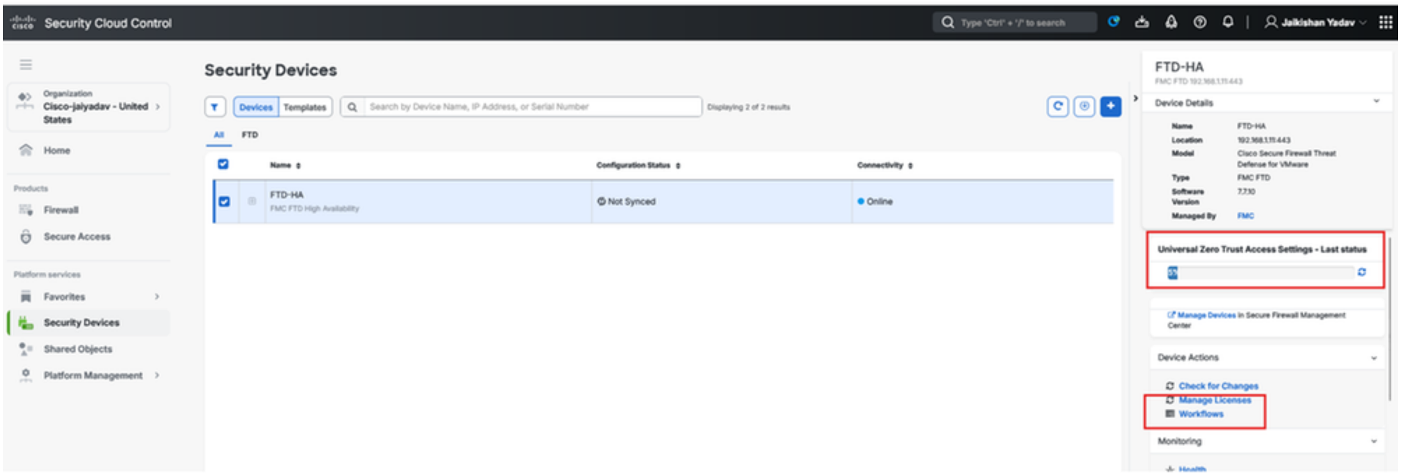
For Local-only enforcement

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

Secure Firewall Threat Defense - Configuração universal do ZTNA

Note: Quando você habilita o ZTNA no FTD HA , ele implementa as alterações e reinicializa as unidades de Firewall Threat Defense (FTD) ao mesmo tempo. Certifique-se de agendar uma janela de manutenção apropriada.

- Clique em Workflow para verificar os logs



Security Devices

Name	Configuration Status	Connectivity
FTD-HA FMC FTD High Availability	Not Synced	● Online

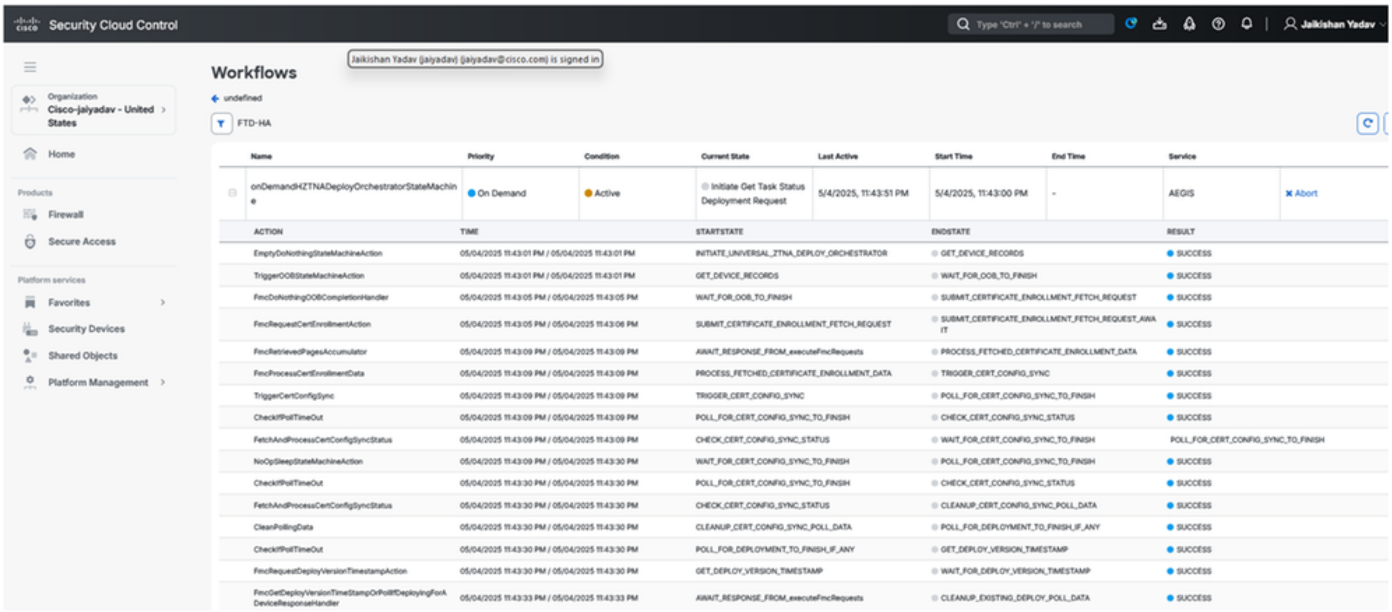
FTD-HA
FMC FTD 192.168.1.11:443

Device Details

Name	FTD-HA
Location	192.168.1.11:443
Model	Cisco Secure Firewall Threat Defense for VMware
Type	FMC FTD
Software Version	7.7.10
Managed By	FMC

Universal Zero Trust Access Settings - Last status

Secure Firewall Threat Defense - Status da configuração universal do ZTNA



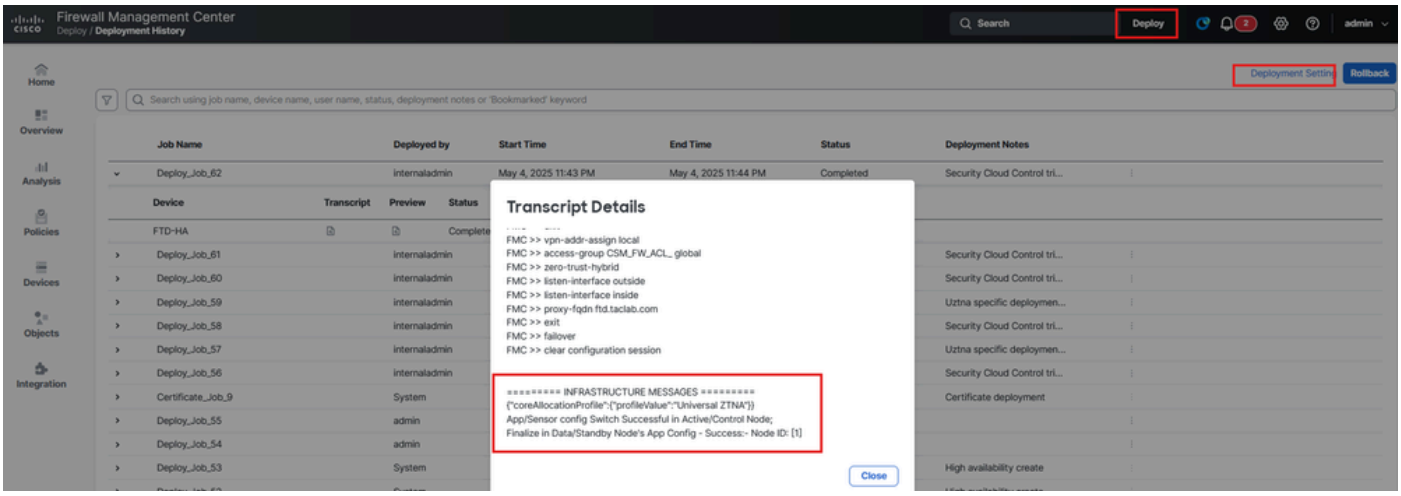
Workflows

Name	Priority	Condition	Current State	Last Active	Start Time	End Time	Service	
onDemandHZTNADeployOrchestratorStateMachine	● On Demand	● Active	Initiate Get Task Status Deployment Request	5/4/2025, 11:43:51 PM	5/4/2025, 11:43:00 PM	-	AEGIS	✖ Abort

ACTION	TIME	STARTSTATE	ENDSTATE	RESULT
EmptyDoNothingStateMachineAction	05/04/2025 11:43:01 PM / 05/04/2025 11:43:01 PM	INITIATE_UNIVERSAL_ZTNA_DEPLOY_ORCHESTRATOR	GET_DEVICE_RECORDS	● SUCCESS
TriggerOOBStateMachineAction	05/04/2025 11:43:01 PM / 05/04/2025 11:43:01 PM	GET_DEVICE_RECORDS	WAIT_FOR_OOB_TO_FINISH	● SUCCESS
FmcDoNothingOOBCompletionHandler	05/04/2025 11:43:05 PM / 05/04/2025 11:43:05 PM	WAIT_FOR_OOB_TO_FINISH	SUBMIT_CERTIFICATE_ENROLLMENT_FETCH_REQUEST	● SUCCESS
FmcRequestCertEnrollmentAction	05/04/2025 11:43:05 PM / 05/04/2025 11:43:06 PM	SUBMIT_CERTIFICATE_ENROLLMENT_FETCH_REQUEST	SUBMIT_CERTIFICATE_ENROLLMENT_FETCH_REQUEST_AWAIT	● SUCCESS
FmcRetrievedPagesAccumulator	05/04/2025 11:43:09 PM / 05/04/2025 11:43:09 PM	AWAIT_RESPONSE_FROM_executeFmcRequests	PROCESS_FETCHED_CERTIFICATE_ENROLLMENT_DATA	● SUCCESS
FmcProcessCertEnrollmentData	05/04/2025 11:43:09 PM / 05/04/2025 11:43:09 PM	PROCESS_FETCHED_CERTIFICATE_ENROLLMENT_DATA	TRIGGER_CERT_CONFIG_SYNC	● SUCCESS
TriggerCertConfigSync	05/04/2025 11:43:09 PM / 05/04/2025 11:43:09 PM	TRIGGER_CERT_CONFIG_SYNC	POLL_FOR_CERT_CONFIG_SYNC_TO_FINISH	● SUCCESS
CheckIfPollTimeOut	05/04/2025 11:43:09 PM / 05/04/2025 11:43:09 PM	POLL_FOR_CERT_CONFIG_SYNC_TO_FINISH	CHECK_CERT_CONFIG_SYNC_STATUS	● SUCCESS
FetchAndProcessCertConfigSyncStatus	05/04/2025 11:43:09 PM / 05/04/2025 11:43:09 PM	CHECK_CERT_CONFIG_SYNC_STATUS	WAIT_FOR_CERT_CONFIG_SYNC_TO_FINISH	POLL_FOR_CERT_CONFIG_SYNC_TO_FINISH
NoOpSleepStateMachineAction	05/04/2025 11:43:09 PM / 05/04/2025 11:43:30 PM	WAIT_FOR_CERT_CONFIG_SYNC_TO_FINISH	POLL_FOR_CERT_CONFIG_SYNC_TO_FINISH	● SUCCESS
CheckIfPollTimeOut	05/04/2025 11:43:30 PM / 05/04/2025 11:43:30 PM	POLL_FOR_CERT_CONFIG_SYNC_TO_FINISH	CHECK_CERT_CONFIG_SYNC_STATUS	● SUCCESS
FetchAndProcessCertConfigSyncStatus	05/04/2025 11:43:30 PM / 05/04/2025 11:43:30 PM	CHECK_CERT_CONFIG_SYNC_STATUS	CLEANUP_CERT_CONFIG_SYNC_POLL_DATA	● SUCCESS
CleanPollingData	05/04/2025 11:43:30 PM / 05/04/2025 11:43:30 PM	CLEANUP_CERT_CONFIG_SYNC_POLL_DATA	POLL_FOR_DEPLOYMENT_TO_FINISH_IF_ANY	● SUCCESS
CheckIfPollTimeOut	05/04/2025 11:43:30 PM / 05/04/2025 11:43:30 PM	POLL_FOR_DEPLOYMENT_TO_FINISH_IF_ANY	GET_DEPLOY_VERSION_TIMESTAMP	● SUCCESS
FmcRequestDeployVersionTimestampAction	05/04/2025 11:43:30 PM / 05/04/2025 11:43:30 PM	GET_DEPLOY_VERSION_TIMESTAMP	WAIT_FOR_DEPLOY_VERSION_TIMESTAMP	● SUCCESS
FmcGetDeployVersionTimeStampOrPollIfDeployingForADeviceResponseHandler	05/04/2025 11:43:33 PM / 05/04/2025 11:43:33 PM	AWAIT_RESPONSE_FROM_executeFmcRequests	CLEANUP_EXISTING_DEPLOY_POLL_DATA	● SUCCESS

Fluxo de trabalho de controle de nuvem de segurança

Em Detalhes da transcrição, você pode ver Policy Deployment Status e alterações em FMC.


Firewall Management Center
Deploy / Deployment History
Search
Deploy
admin
Home
Overview
Analysis
Policies
Devices
Objects
Integration
Deployment Setting
Rollback
Search using job name, device name, user name, status, deployment notes or 'Bookmarked' keyword
Close

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

Device	Transcript	Preview	Status
FTD-HA			Complete

Transcript Details

```
FMC >> vpn-addr-assign local
FMC >> access-group CSM_FW_ACL_ global
FMC >> zero-trust-hybrid
FMC >> listen-interface outside
FMC >> listen-interface inside
FMC >> proxy-fqdn ftd.taclab.com
FMC >> exit
FMC >> failover
FMC >> clear configuration session

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

Secure Firewall Management Center - Status de implantação da política

Inscreva o cliente na ZTNA

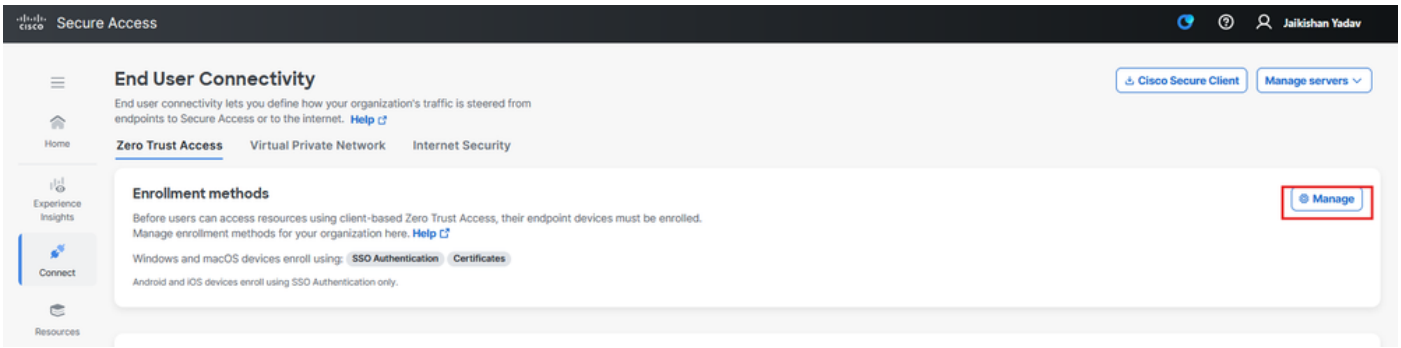
Configuração de acesso seguro

Note: Você pode usar o SSO ou um Certificado com base no registro ZTA. A seguir, estão as etapas para o registro ZTA baseado em certificado

---

Navegue até Secure Access Dashboard:

- Clique em **Connect** > **End User Connectivity** > Zero Trust Access
- Clique em Manage



End User Connectivity

End user connectivity lets you define how your organization's traffic is steered from endpoints to Secure Access or to the internet. Help

Enrollment methods

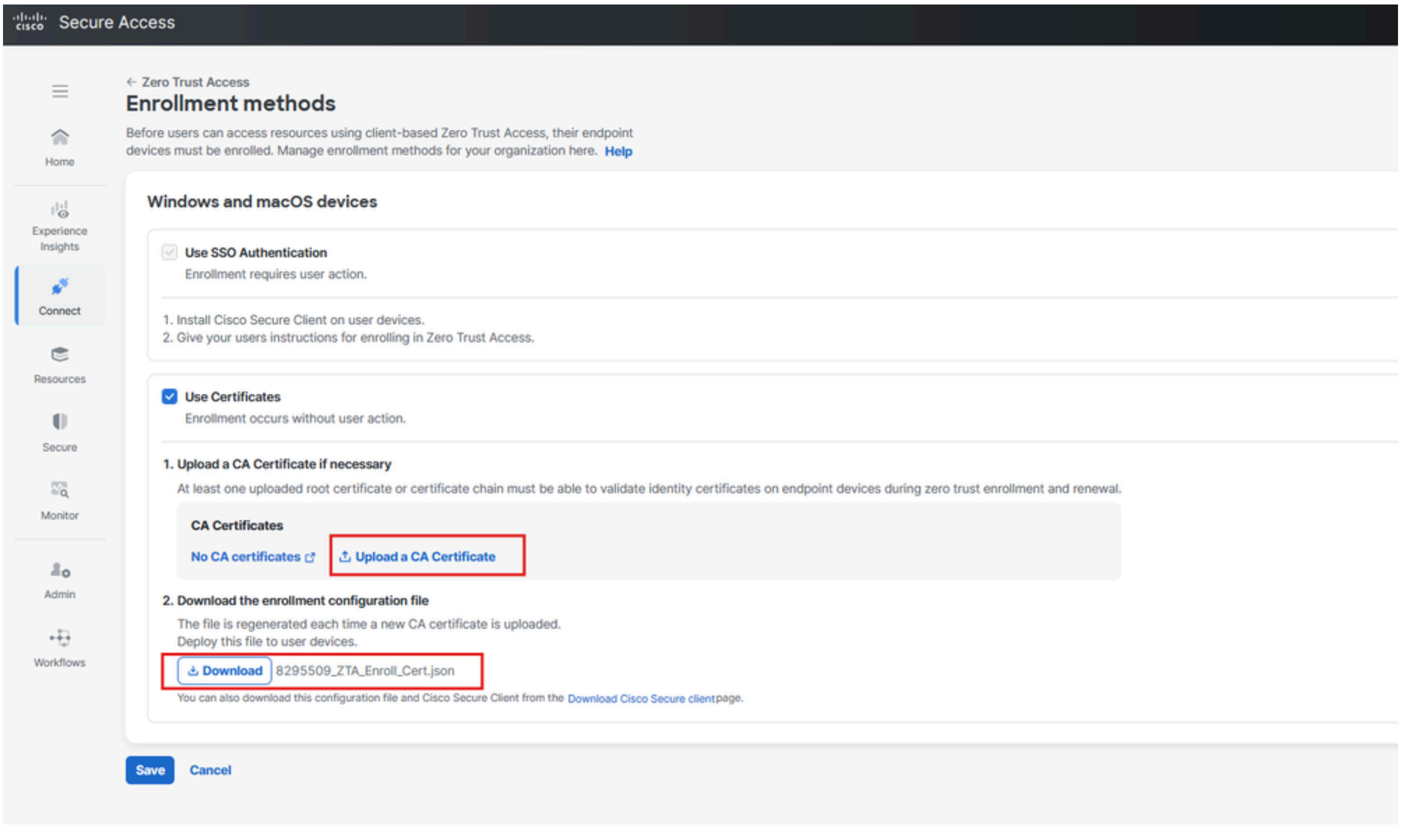
Before users can access resources using client-based Zero Trust Access, their endpoint devices must be enrolled. Manage enrollment methods for your organization here. Help

Windows and macOS devices enroll using: SSO Authentication Certificates

Android and iOS devices enroll using SSO Authentication only.

Acesso seguro - Inscrição de certificado ZTA

- Carregar o certificado da autoridade de certificação raiz e baixar o arquivo de configuração de registro



← 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 clientpage.

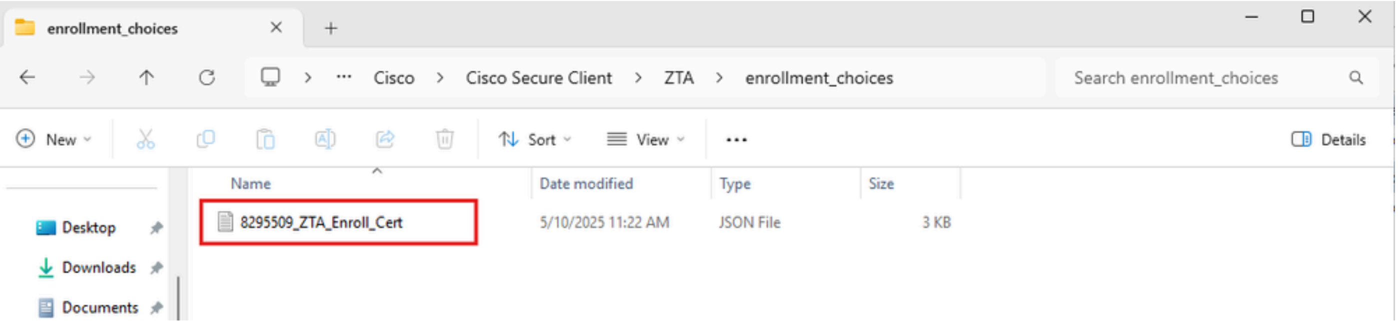
Save Cancel

Acesso seguro - Inscrição de certificado ZTA

- Clique em Save

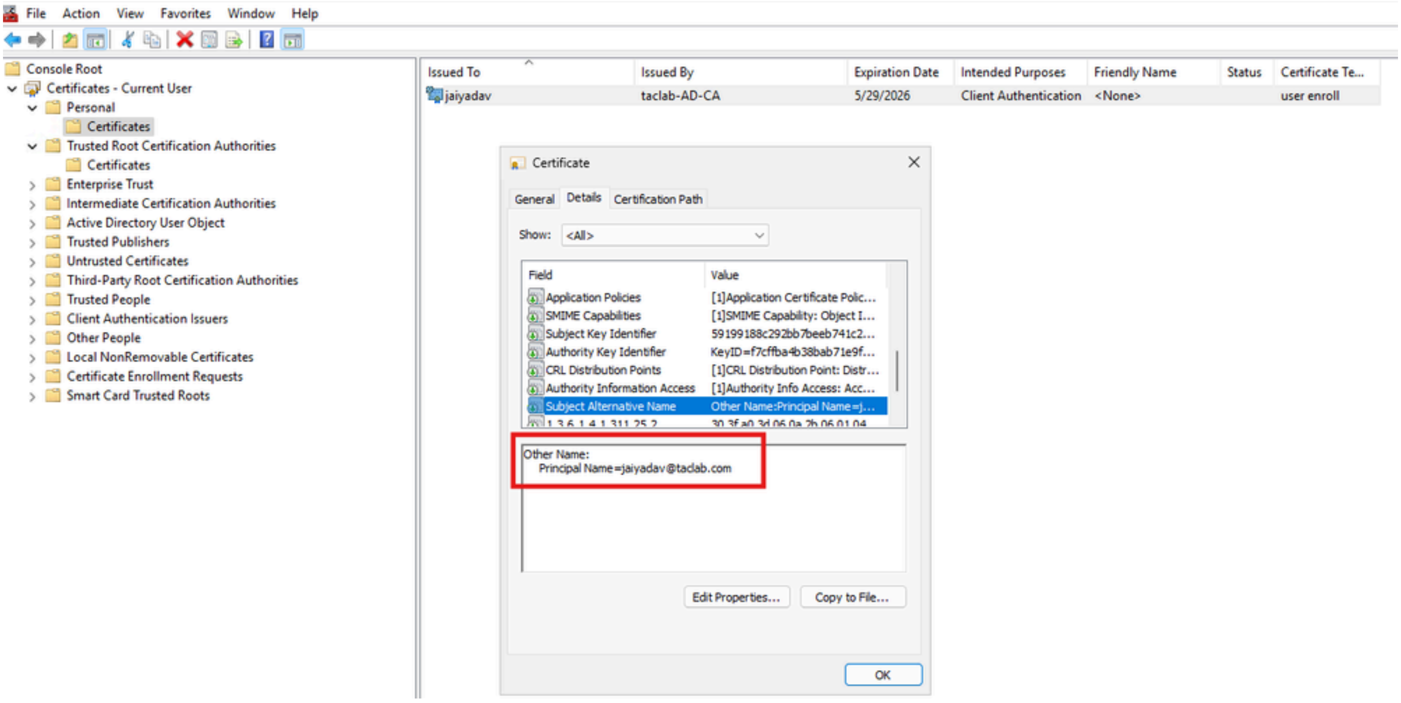
Configuração do Cliente

Copie o arquivo de configuração de registro para C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollment_choices


enrollment_choices
Cisco > Cisco Secure Client > ZTA > enrollment_choices
Search enrollment_choices
New
Sort
View
Details
Desktop
Downloads
Documents

Name	Date modified	Type	Size
8295509_ZTA_Enroll_Cert	5/10/2025 11:22 AM	JSON File	3 KB

- Criar um certificado de cliente, que deve ter UPN no SAN arquivado



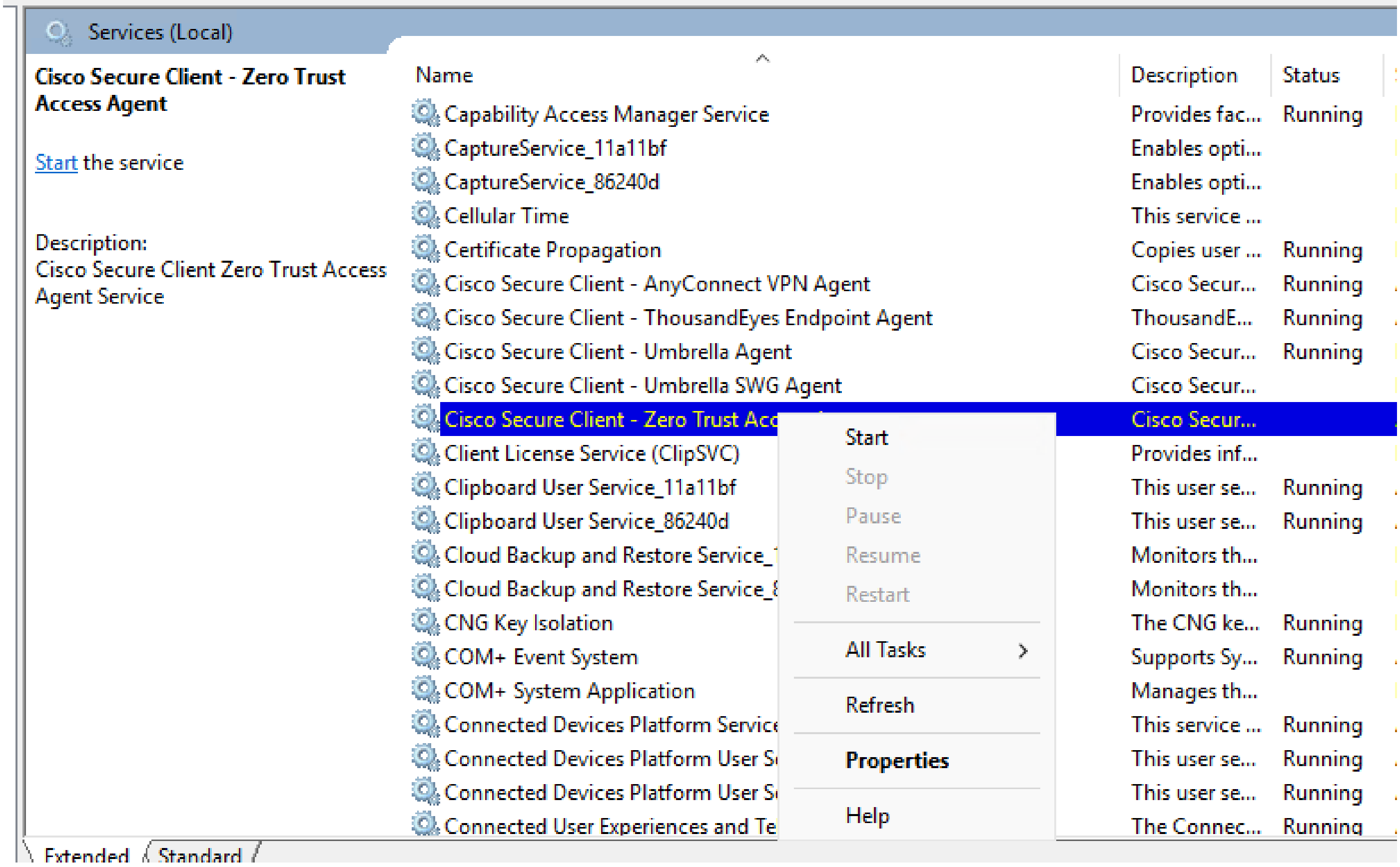
Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Te...
jaiyadav	taclab-AD-CA	5/29/2026	Client Authentication	<None>		user enroll

Field	Value
Application Policies	[1]Application Certificate Polic...
SMIME Capabilities	[1]SMIME Capability: Object I...
Subject Key Identifier	59199188c292bb7beeb741c2...
Authority Key Identifier	KeyID=f7cffba4b38bab71e9f...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Subject Alternative Name	Other Name:Principal Name=j...
1.3.6.1.4.1.311.25.2	30 3f a0 3d 06 0a 2b 06 01 04

Other Name:
Principal Name=jaiyadav@taclab.com

Instalação do certificado

- Iniciar/ Reiniciar Cisco Secure Client - Zero Trust Access Agent



Cisco Secure Client - Zero Trust Access Agent

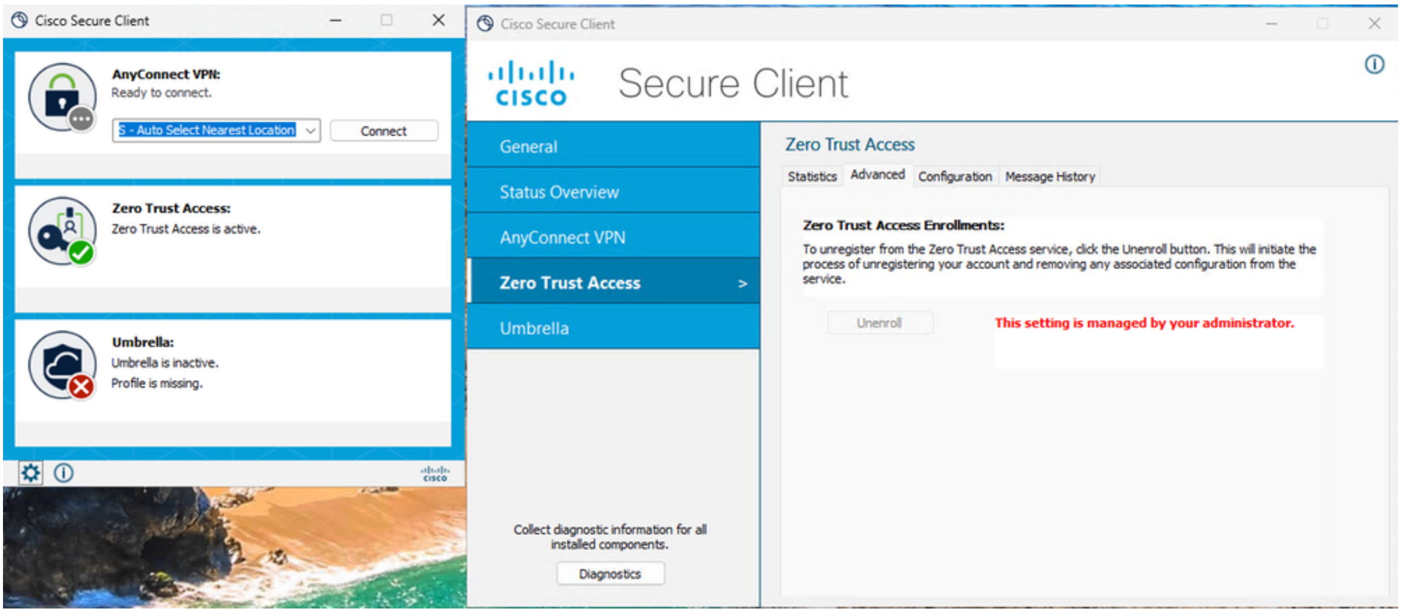
Start the service

Description:
Cisco Secure Client Zero Trust Access Agent Service

Name	Description	Status
Capability Access Manager Service	Provides fac...	Running
CaptureService_11a11bf	Enables opti...	
CaptureService_86240d	Enables opti...	
Cellular Time	This service ...	
Certificate Propagation	Copies user ...	Running
Cisco Secure Client - AnyConnect VPN Agent	Cisco Secur...	Running
Cisco Secure Client - ThousandEyes Endpoint Agent	ThousandE...	Running
Cisco Secure Client - Umbrella Agent	Cisco Secur...	Running
Cisco Secure Client - Umbrella SWG Agent	Cisco Secur...	
Cisco Secure Client - Zero Trust Acc	Cisco Secur...	
Client License Service (ClipSVC)	Provides inf...	
Clipboard User Service_11a11bf	This user se...	Running
Clipboard User Service_86240d	This user se...	Running
Cloud Backup and Restore Service_	Monitors th...	
Cloud Backup and Restore Service_8	Monitors th...	
CNG Key Isolation	The CNG ke...	Running
COM+ Event System	Supports Sy...	Running
COM+ System Application	Manages th...	
Connected Devices Platform Service	This service ...	Running
Connected Devices Platform User S	This user se...	Running
Connected Devices Platform User S	This user se...	Running
Connected User Experiences and Te	The Connec...	Running

Serviços do Windows

- Verifique o status do módulo ZTA



AnyConnect VPN:
Ready to connect.
S - Auto Select Nearest Location

Zero Trust Access:
Zero Trust Access is active.

Umbrella:
Umbrella is inactive.
Profile is missing.

Zero Trust Access

Zero Trust Access Enrollments:

To unregister from the Zero Trust Access service, click the Unenroll button. This will initiate the process of unregistering your account and removing any associated configuration from the service.

This setting is managed by your administrator.

Collect diagnostic information for all installed components.

Acesso seguro - Status de inscrição de certificado ZTA

Verificar

Use o próximo comando para verificar a configuração da ZTNA no Firewall Threat Defense (FTD):

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

Informações Relacionadas

- Suporte técnico e downloads da Cisco
- Central de ajuda do Cisco Secure Access
- Guia de design do Cisco SASE