

Configuración del acceso seguro para ZTNA universal con FMC gestionado in situ en SCC

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Diagrama de la red](#)

[Información general](#)

[Dispositivos compatibles](#)

[Limitaciones](#)

[Configurar](#)

[Comprobar la versión de FMC](#)

[Comprobar versión de FTD](#)

[Verificar licencias FTD](#)

[Compruebe los parámetros de la plataforma y el DNS configurado correctamente](#)

[Crear un arrendatario de control de seguridad en la nube en CDO](#)

[Asegúrese de que se ha configurado la configuración general de Firewall de SCC](#)

[Verifique su integración de base de gestión de firewall de control de seguridad y arrendatario de acceso seguro](#)

[Generar certificado firmado de CA de Firewall Threat Defence \(FTD\)](#)

[Centro de gestión de firewall en las instalaciones para control de la seguridad en la nube](#)

[Inscriba la configuración de Acceso a red de confianza cero universal \(uZTNA\) en FTD](#)

[Inscriba al cliente con ZUTNA](#)

[Configuración de Secure Access](#)

[Configuración del Cliente](#)

[Verificación](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar el ZTNA universal con Secure Access y FTD virtual administrado por un FMC virtual en las instalaciones.

Prerequisites

- Es necesario implementar Firewall Management Center (FMC) y Firewall Threat Defence (FTD) mediante la versión 7.7.10 o superior del software.
- Firewall Threat Defence (FTD) debe estar gestionado por Firewall Management Center (FMC)

- Firewall Threat Defence (FTD) debe contar con una licencia de cifrado (el cifrado avanzado debe activarse con la función de exportación activada), se necesitan licencias de IPS y de amenazas para los controles de seguridad
- La configuración básica de Firewall Threat Defence (FTD) debe realizarse desde el centro de gestión de firewall (FMC), como la interfaz, el routing, etc.
- La configuración de DNS debe aplicarse en el dispositivo desde FMC para resolver el FQDN de la aplicación
- La versión de Cisco Secure Client debe ser 5.1.10 o superior
- El control de seguridad en la nube se proporciona a los clientes con el firewall y las microaplicaciones de acceso seguro, y los indicadores de funciones de UZTNA habilitados

Requirements

- Todos los Secure Firewall Management Center (FMC), incluidos los dispositivos cdFMC y Firewall Threat Defence (FTD), deben ejecutar la versión de software 7.7.10 o posterior.
- Firewall Threat Defence (FTD) debe estar gestionado por Firewall Management Center; no se admite el administrador local Firewall Defense Manager (FDM)
- Todos los dispositivos de defensa frente a amenazas de firewall (FTD) deben configurarse para el modo enrutado; no se admite el modo transparente.
- No se admiten dispositivos agrupados.
- Compatibilidad con dispositivos de alta disponibilidad (HA); se muestran como una entidad.
- Secure Client versión 5.1.10 o posterior

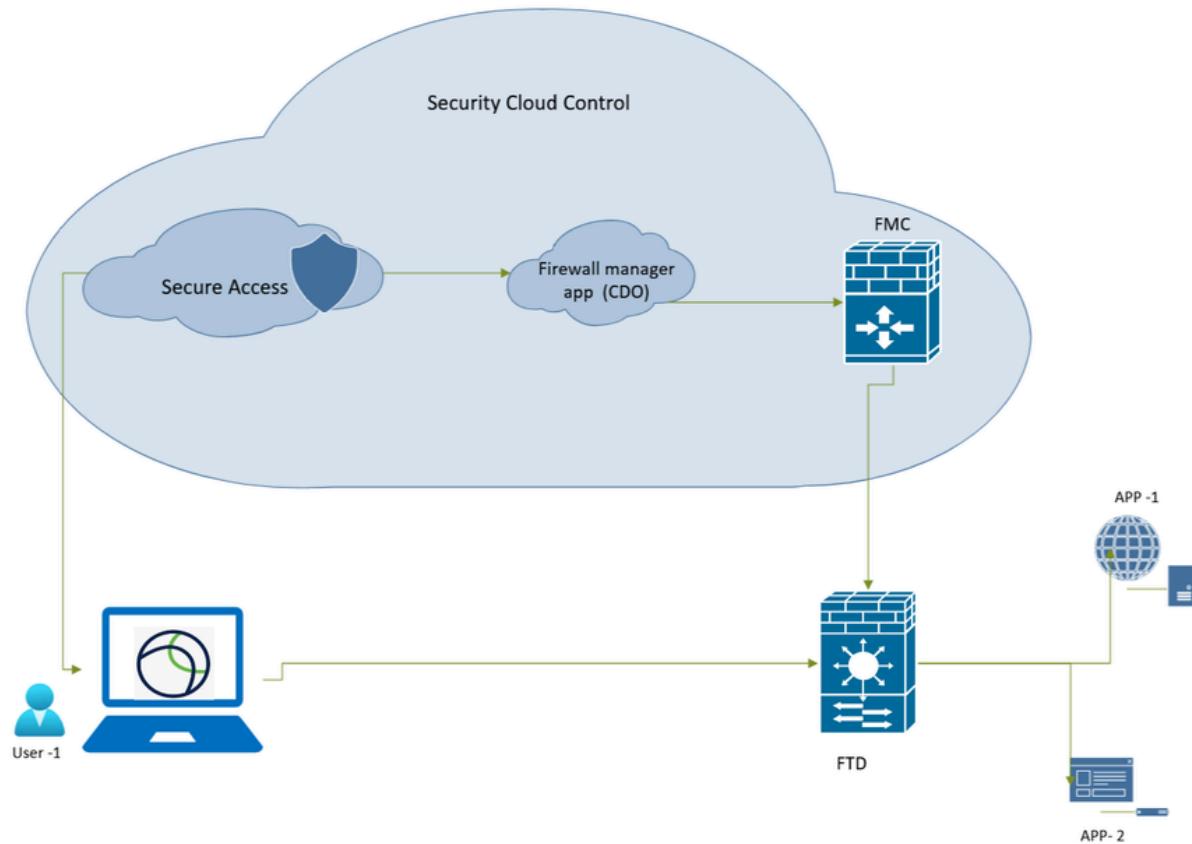
Componentes Utilizados

La información de este documento se basa en

- Control de seguridad en la nube (SCC)
- Secure Firewall Management Center (FMC) versión 7.7.10
- Secure Firewall Threat Defence (FTD) virtual -100 versión 7.7.10
- Secure Client para Windows versión 5.1.10
- Acceso seguro

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Diagrama de la red



Acceso seguro - Topología de red

Información general

Dispositivos compatibles

Modelos compatibles de Secure Firewall Threat Defence:

- FPR 1150
- FPR 3105, 3110, 3120, 3130 y 3140
- FPR4115,4125,4145,4112
- FPR4215,4225,4245
- Firewall Threat Defence (FTD) virtual con un mínimo de 16 núcleos de CPU

Limitaciones

- Uso compartido de objetos
- No se admite IPv6.
- Sólo se soporta el VRF global.
- Las políticas ZTNA universales no se aplican en el tráfico de túnel de sitio a sitio a un dispositivo .
- No se admiten dispositivos agrupados.

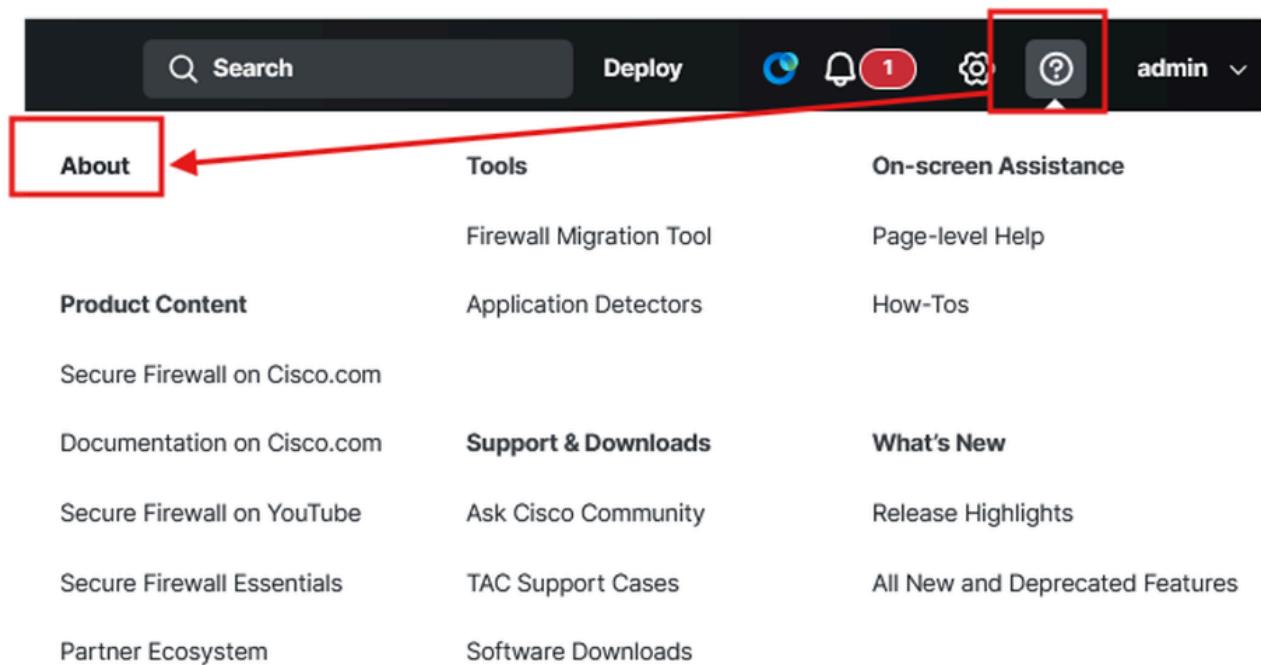
- No se admiten los FTD implementados como contenedores en series Firepower 4K y 9K
- Las sesiones ZTNA universales no admiten tramas jumbo

Configurar

Comprobar la versión de FMC

Verifique que Firewall Management Center y Firewall FTD se ejecuten en la versión de software compatible para ZTNA universal (puede ser 7.7.10 o superior):

- Haga clic en ?(esquina superior derecha) y haga clic en 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	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 - Versión de software

Comprobar versión de FTD

Vaya a FMC UI:

- Haga clic en **Devices > Device Management**

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
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 Defence - Versión de software

Verificar licencias FTD

- Haga clic en 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)					

Firewall seguro Threat Defence - Licencias inteligentes

Compruebe los parámetros de la plataforma y el DNS configurado correctamente

Registro en el FTD a través de CLI:

- Ejecute el comando para verificar si DNS está configurado:

```
show run dns
```

En el CSP:

- Haga clic en Devices > Platform Settings , edite o cree una nueva política

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

Firewall seguro Threat Defence - Política de plataforma

Protección frente a amenazas de firewall - Configuración de DNS

Verifique a través de la CLI de FTD que puede hacer ping a la dirección IP y FQDN de los recursos privados (si desea acceder a PR mediante su 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#
```

Crear un arrendatario de control de seguridad en la nube en CDO



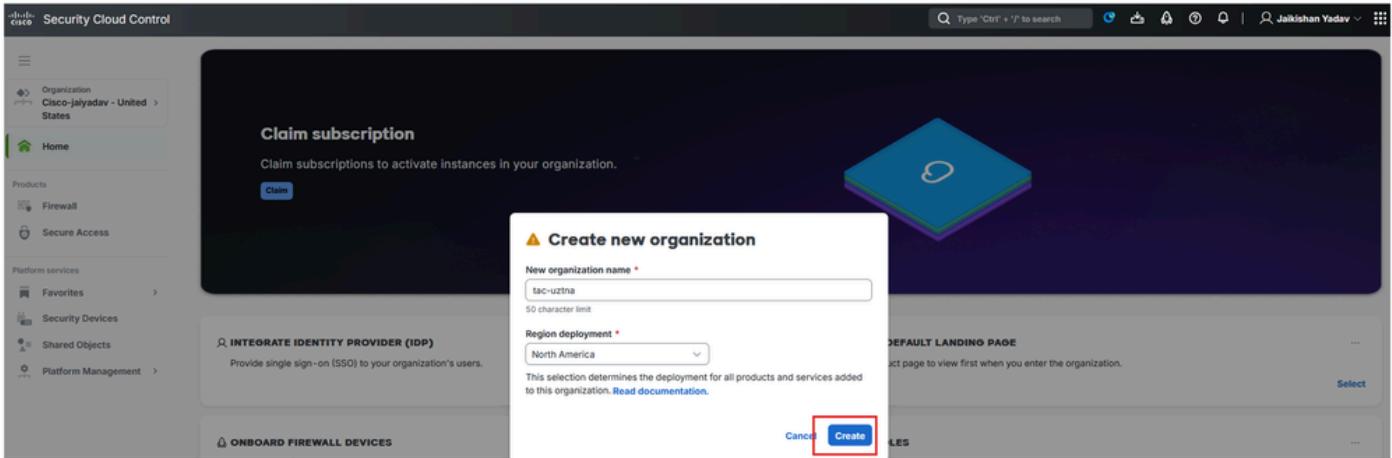
Nota: Si ya tiene configurado un arrendatario de SCC, no es necesario crear un nuevo arrendatario.

Vaya a [Security Cloud Control](#):

- Haga clic en Organization > Create new organization

Control seguro de la nube - Organización

- Haga clic en Create



Control seguro de la nube: creación de organizaciones

Una vez creado el arrendatario de SCC , recopile la información del arrendatario para habilitar la microaplicación Firewall y Secure Access y para habilitar ZUTNA.

Asegúrese de que se ha configurado la configuración general de Firewall de SCC

Vaya a [CDO/SCC](#):

- Haga clic en Administration > General Settings
- Asegúrese de que Auto onboard On-Prem FMCs from Cisco Security Cloud la opción está activada.



Nota: El usuario que intenta acceder a Secure Access MicroApp debe tener Secure Access funciones de administrador y Security Cloud Control administrador.

Security Cloud Control

The screenshot shows the Cisco Security Cloud Control interface. The left sidebar includes sections for Dashboard, Monitor, Insights & Reports, Events & Logs, Manage, Objects, Security Devices, Secure Connections, and Administration. The Administration section is currently selected. The main content area is titled "Administration" and contains a "General Settings" tab (selected) and other tabs for User Management and Notification Settings. Below these tabs is a "Integrations" section with options for Secure Connectors, Firewall Management Center, Multicloud Defense, and Management.

The screenshot shows the "General Settings" page within the Cisco Security Cloud Control Administration interface. The "Auto onboard On-Prem FMCs from Cisco Security Cloud" toggle switch is highlighted with a red box. Below it, the "Enable event data sharing with Talos" toggle switch is also highlighted with a red box. A callout box provides instructions for integrating On-Prem FMCs. At the bottom, three input fields are highlighted with a red box: "Tenant ID" (containing "cbc"), "Secure Services Exchange Tenant ID" (containing "?"), and "Tenant Name" (containing "CI").

Secure Cloud Control - Detalles de la organización

Verifique su integración de base de gestión de firewall de control de seguridad y arrendatario de acceso seguro

Overview - Cisco-jaiyadav

Organization ID - a161c021-d864-48ab-8897-89c78be3aafa

Products

Cisco Security Cloud Control Firewall Management Base Activated

Subscription ID lab-jaiyadav-1

End date 04/16/2026

External instance ID 1

Quantity 1

Region North America

Cisco Secure Access Activated

Subscription ID lab-jaiyadav-1

End date 04/16/2026

External instance ID 1

Quantity 1

Region Global

Secure Cloud Control: activación de acceso seguro

Una vez que complete el paso [Crear un arrendatario de control de la nube de seguridad en CDO](#) y [Crear un arrendatario de control de la nube de seguridad en CDO](#), podrá ver las microaplicaciones de firewall y acceso seguro en el panel de SCC:

Security Devices

Devices Templates Search by Device Name, IP Address, or Serial Number Displaying 0 of 0 results

Name Configuration Status Connectivity

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

Control seguro de la nube: microaplicaciones

Generar certificado firmado de CA de Firewall Threat Defence (FTD)



Nota: También puede utilizar certificados de FTD autofirmados [Certificados de FTD](#) (consulte la sección Generación de certificados de CA internos e internos autofirmados). El certificado debe estar en formato PKCS12 y debe estar presente en el almacén del equipo del usuario en la CA raíz de confianza.

Para generar un certificado firmado por CA utilizando FTD en la función build openssl:

- Navegar hasta FTD
- Ejecutar `expert` comando
- Generar CSR y clave mediante openssl
 - Comando OpenSSL:

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

```
openssl req -newkey rsa:2048 -nodes -keyout cert.key -out cert.csr
Generating a RSA private key
-----+=====
-----+=====
writing new private key to 'cert.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:NC
Locality Name (eg, city) []:RTP
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco
Organizational Unit Name (eg, section) []:TAC
Common Name (e.g. server FQDN or YOUR name) []:ftd.taclab.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
```

Solicitud de firma de certificado

- Copie el CSR y obtenga un certificado firmado por la CA
- Utilice el certificado y la clave firmados por la CA de FTD y convierta el certificado al formato PKCS12
 - Comando OpenSSL:

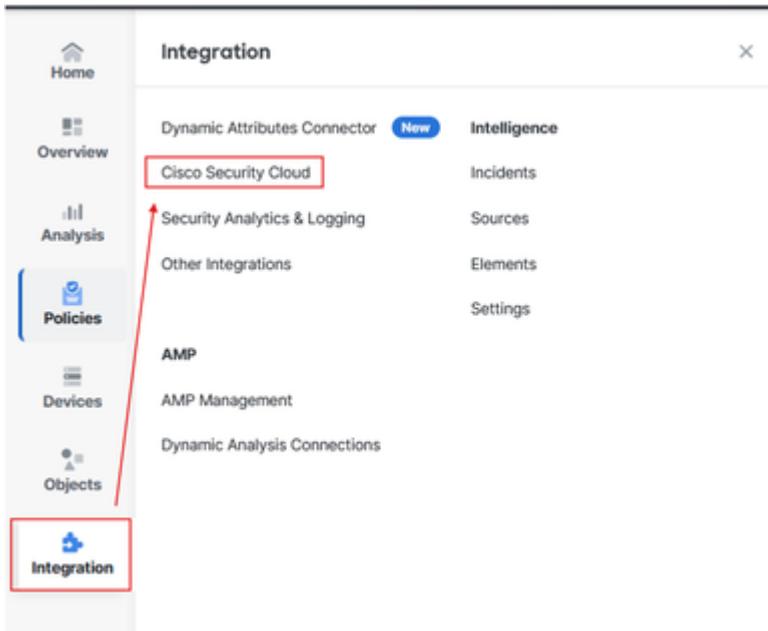
```
openssl pkcs12 -export -out ftdcert.p12 -in cert.crt -inkey cert.key
```

- Exporte el certificado mediante SCP u otra herramienta.

Centro de gestión de firewall en las instalaciones para control de la seguridad en la nube

Acceda a FMC:

- Haga clic en Integration > Cisco Security Cloud



Firewall Management Center e integración con SCC

- Seleccione la región de la nube y haga clic en Enable Cisco Security Cloud

Integración de Firewall Management Center en SCC

Se abrirá una nueva pestaña del navegador, en la nueva pestaña:

- Haga clic en Continue to Cisco SSO



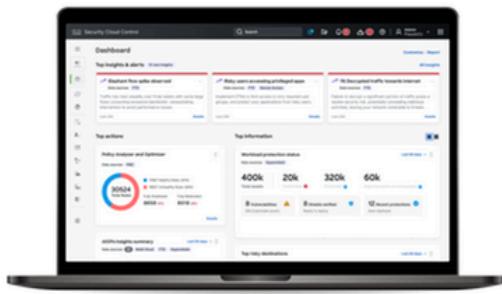
Nota: Asegúrese de que está desconectado de SCC y de que no tiene ninguna otra pestaña abierta.



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](#)

Integración de Firewall Management Center en SCC

- Elija su arrendatario de SCC y haga clic en 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

Integración de Firewall Management Center en SCC

- Haga clic en 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 | Learn more

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

Integración de Firewall Management Center en SCC

El estado de Cloud Onboarding Status debe cambiar de Not Available a Onboarding entonces Online.

The screenshot shows the Cisco Security Cloud Integration page. The 'Cloud Onboarding Status' field is highlighted with a red box and contains the value 'Onboarding'. Other fields visible include 'Cisco Security Cloud' (Enabled), 'Current Cloud Region' (us-east-1 (US Region)), and 'CDO Tenant' (cisco-cisco-jalyadav...surmp).

The screenshot shows the Cisco Security Cloud Integration page. The 'Cloud Onboarding Status' field is highlighted with a red box and contains the value 'Online'. Other fields visible include 'Cisco Security Cloud' (Enabled), 'Current Cloud Region' (us-east-1 (US Region)), and 'CDO Tenant' (cisco-cisco-jalyadav...surmp).

Estado de onboardin de Firewall Management Center

- Vaya a [SCC](#) y compruebe el estado de FTD en Platform Services > Security Devices

The screenshot shows the Security Devices page in Security Cloud Control. It lists three FTD devices: 'FTD-HA' (Synced, Online), 'fmc_192.168.1.5_FT01' (Synced, Online), and 'fmc_192.168.1.5_FT02' (Synced, Online). The left sidebar shows the navigation path: Organization > Cisco-Jalyadav - United > States > Home > Products > Firewall > Secure Access > Platform services > Favorites > Security Devices.

Estado de defensa frente a amenazas de firewall seguro en SCC

Inscriba la configuración de Acceso a red de confianza cero universal (uZTNA) en FTD

Vaya a SCC:

- Haga clic en Platform Services > Security Devices > FTD > Device Management > Universal Zero Trust Network Access

Screenshot of the Cisco Security Cloud Control interface showing the 'Security Devices' section. The left sidebar shows navigation paths: Home, Products (Firewall, Secure Access, Platform services, Security Devices), and Favorites. The main area displays a table of devices with columns: Name, Configuration Status, and Connectivity. A device named 'FTD-HA' is selected, highlighted with a red box. To the right, detailed information is shown for 'FTD-HA' under 'Device Details' and 'Health'. Under 'Device Management', a sub-section 'Universal zero trust access settings' is highlighted with a red box. A legend at the bottom right indicates that red boxes highlight specific steps: 1, 2, 3, 4, and 5.

Protección frente a amenazas con firewall - Configuración ZTNA universal

- Rellene la información y cargue el certificado de FTD generado en el paso [Generar certificado firmado de CA de Defensa frente a amenazas de firewall \(FTD\)](#)

Screenshot of the 'Enable Universal Zero Trust Access' configuration page. The left sidebar shows the same navigation as the previous screenshot. The main form is titled 'Configure device for Universal Zero Trust Access' and includes fields for Firewall management center (FMC), Device (FTD-HA), Device FQDN, Device identity certificate, and Device Interface(s). A checkbox for 'Auto deploy policy and rule enforcements to firewall device' is checked. On the right, there is 'Quick help' with two diagrams: 'For Cloud or Local enforcement' and 'For Local-only enforcement'. The 'For Cloud or Local enforcement' diagram shows a user in a trusted network connected to an 'Inside Interface' of a device, which then connects to the Internet. The 'For Local-only enforcement' diagram shows a user in a trusted network connected to both an 'Inside Interface' and an 'Outside Interface' of the device, with the Internet connected to the outside interface. A legend at the bottom right indicates that red boxes highlight specific steps: 1, 2, 3, 4, and 5.

Protección frente a amenazas con firewall - Configuración ZTNA universal

Protección frente a amenazas con firewall - Configuración ZTNA universal

Protección frente a amenazas con firewall - Configuración ZTNA universal



Nota: Al activar ZUTNA en FTD HA , se implementarán los cambios y se reiniciarán ambas unidades de defensa frente a amenazas de firewall (FTD) al mismo tiempo. Asegúrese de programar una ventana de mantenimiento adecuada.

- Haga clic en Workflow para comprobar los registros

Security Devices

Name	Configuration Status	Connectivity
FTD-HA	Not Synced	Online

Device Details

FTD-HA
FMC FTD High Availability

Universal Zero Trust Access Settings - Last status

Check for Changes
Manage Licenses
Workflows

Secure Firewall Threat Defence - Estado de la configuración ZTNA universal

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
ACTION	TIME		STARTSTATE	ENDSTATE			RESULT
EmptyOnNothingStateMachineAction	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
FmcOnboardingOOBCompletionHandler	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_WAIT			SUCCESS
FmcReceivedPagesAccumulator	05/04/2025 11:43:09 PM / 05/04/2025 11:43:09 PM		AWAIT_RESPONSE_FROM_EXECUTE_INCHIEQUESTS	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
CheckPollTimeOut	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 11:43:30 PM / 05/04/2025 11:43:30 PM		WAIT_FOR_CERT_CONFIG_SYNC_TO_FINISH	POLL_FOR_CERT_CONFIG_SYNC_TO_FINISH			SUCCESS
CheckPollTimeOut	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
CheckPollTimeOut	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_EXECUTE_INCHIEQUESTS	CLEANUP_EXISTING_DEPLOY_POLL_DATA			SUCCESS

Flujo de trabajo de Security Cloud Control

En Detalles de transcripción puede ver Policy Deployment Status y ver cambios en FMC.

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 trl...
Transcript Details					
FMC >> vpn-addr-assign local					Security Cloud Control trl...
FMC >> access-group CSM_FW_ACL_global					Security Cloud Control trl...
FMC >> zero-trust-hybrid					Uztna specific deploymen...
FMC >> listen-interface outside					Security Cloud Control trl...
FMC >> listen-interface inside					Uztna specific deploymen...
FMC >> proxy-fqdn ftd.taclab.com					Security Cloud Control trl...
FMC >> exit					Certificate deployment
FMC >> failover					
FMC >> clear configuration session					
***** INFRASTRUCTURE MESSAGES *****					High availability create
({"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]					

Centro de gestión de firewall seguro: estado de implementación de políticas

Inscriba al cliente con ZUTNA

Configuración de Secure Access



Nota: Puede utilizar SSO o una inscripción ZTA basada en certificados. A continuación, se indican los pasos para la inscripción ZTA basada en certificados

Vaya al [Panel de Acceso Seguro](#):

- Haga clic en Connect > End User Connectivity > Zero Trust Access
- Haga clic en Manage

The screenshot shows the Cisco Secure Access dashboard. On the left, there's a sidebar with icons for Experience Insights, Home, Connect (which is selected), and Resources. The main content area has a title 'End User Connectivity' and a sub-section 'Zero Trust Access'. Below this, under 'Enrollment methods', it says 'Before users can access resources using client-based Zero Trust Access, their endpoint devices must be enrolled.' There are two tabs: 'SSO Authentication' (selected) and 'Certificates'. A red box highlights the 'Manage' button at the top right of the enrollment section.

Acceso seguro - Inscripción en certificados ZTA

- Cargue el certificado de CA raíz y descargue el archivo de configuración de inscripción

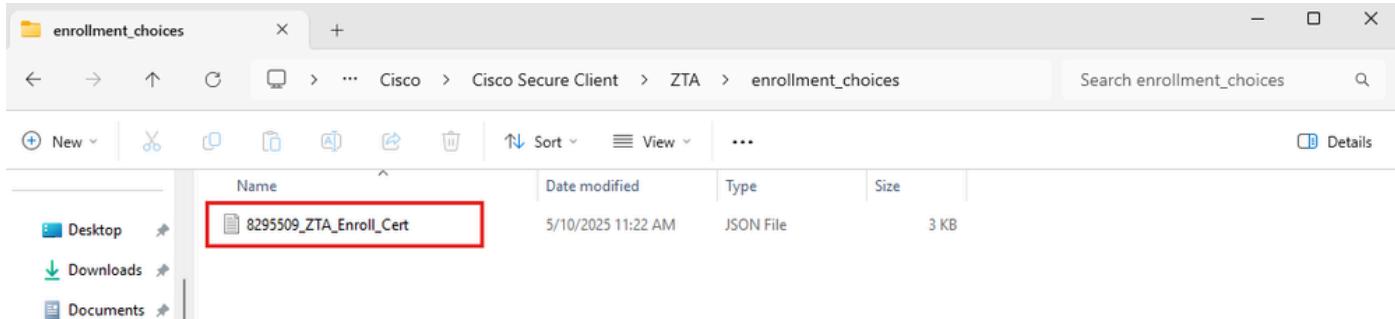
The screenshot shows the 'Windows and macOS devices' configuration page under the 'Enrollment methods' section. It includes sections for 'Use SSO Authentication' (checkbox checked, note: Enrollment requires user action) and 'Use Certificates' (checkbox checked, note: Enrollment occurs without user action). There are two main steps: 1. 'Upload a CA Certificate if necessary' (button 'Upload a CA Certificate' highlighted with a red box) and 2. 'Download the enrollment configuration file' (button 'Download' highlighted with a red box). A note at the bottom says 'You can also download this configuration file and Cisco Secure Client from the Download Cisco Secure client page.'

Acceso seguro - Inscripción en certificados ZTA

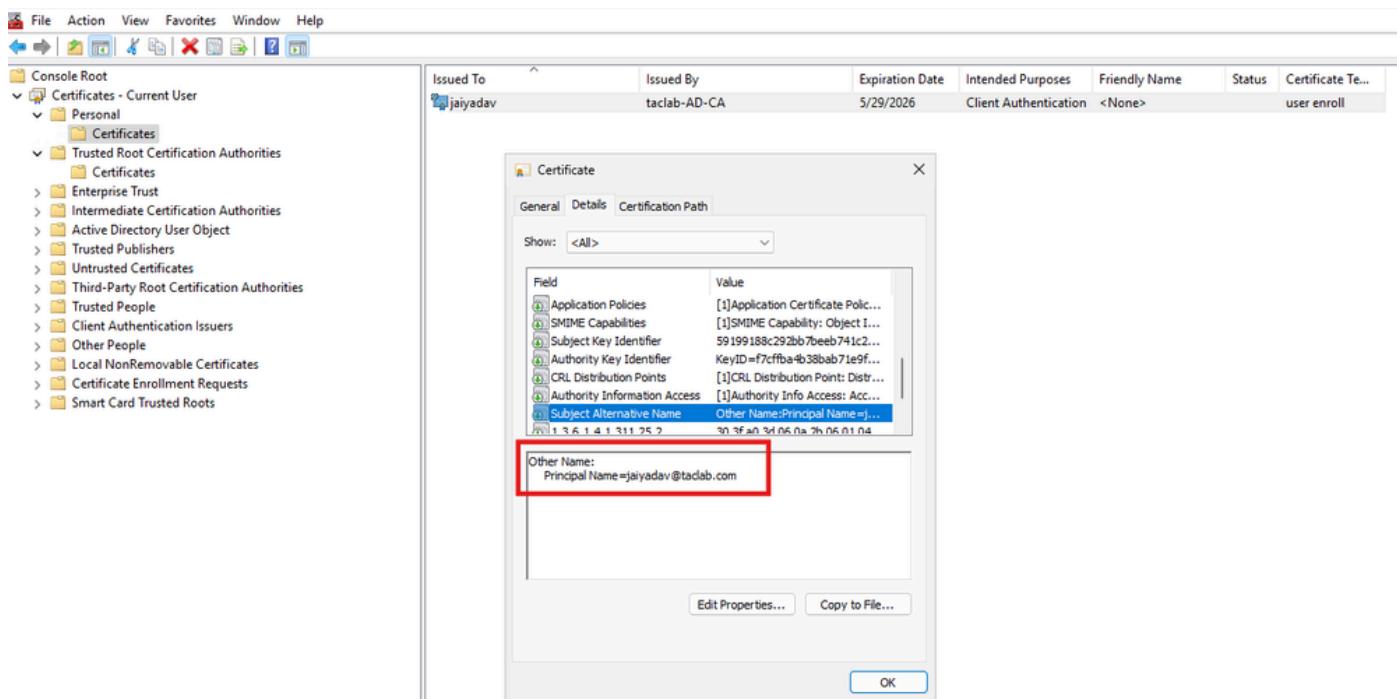
- Haga clic en Save

Configuración del Cliente

Copie el archivo de configuración de inscripción en C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollment_choices



- Cree un certificado de cliente, que debe tener un UPN en un campo SAN



Instalación de certificados

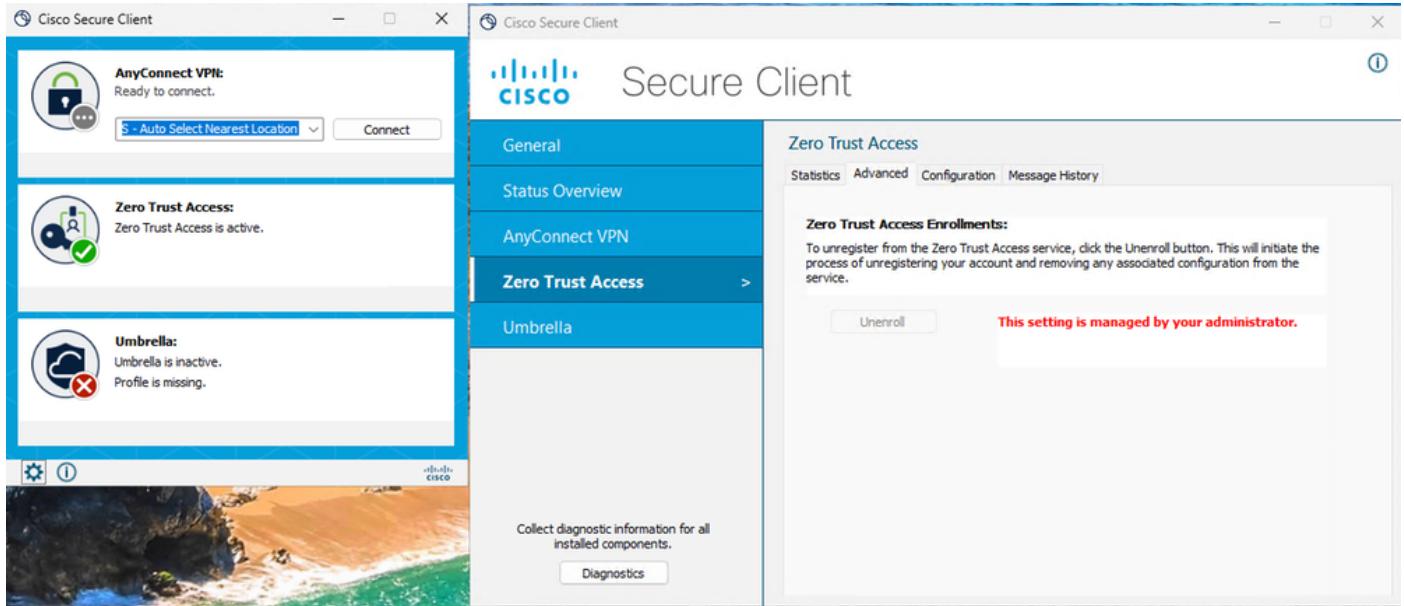
- Iniciar/ Reiniciar Cisco Secure Client - Zero Trust Access Agent

Services (Local)		
Name	Description	Status
Cisco Secure Client - Zero Trust Access Agent	Provides fac... Enables opti... Enables opti... This service ... Copies user ... Cisco Secur... ThousandE... Cisco Secur... Cisco Secur...	Running
Start the service		
Description: Cisco Secure Client Zero Trust Access Agent Service		
Cisco Secure Client - Zero Trust Access Agent	Cisco Secure... Provides inf... This user se... This user se... Monitors th... Monitors th... The CNG ke... Supports Sy... Manages th... This service ... This user se... This user se... This user se... The Connec...	Running
	Start	
	Stop	
	Pause	
	Resume	
	Restart	
	All Tasks >	
	Refresh	
	Properties	
	Help	

Extended / Standard /

Servicios de Windows

- Verifique el estado del módulo ZTA



Acceso seguro - Estado de inscripción del certificado ZTA

Verificación

Utilice el siguiente comando para verificar la configuración de ZUTNA en Firewall Threat Defence (FTD):

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

Información Relacionada

- [Soporte técnico y descargas de Cisco](#)
- [Centro de ayuda de Cisco Secure Access](#)
- [Guía de diseño de Cisco SASE](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).