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

Contenido

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

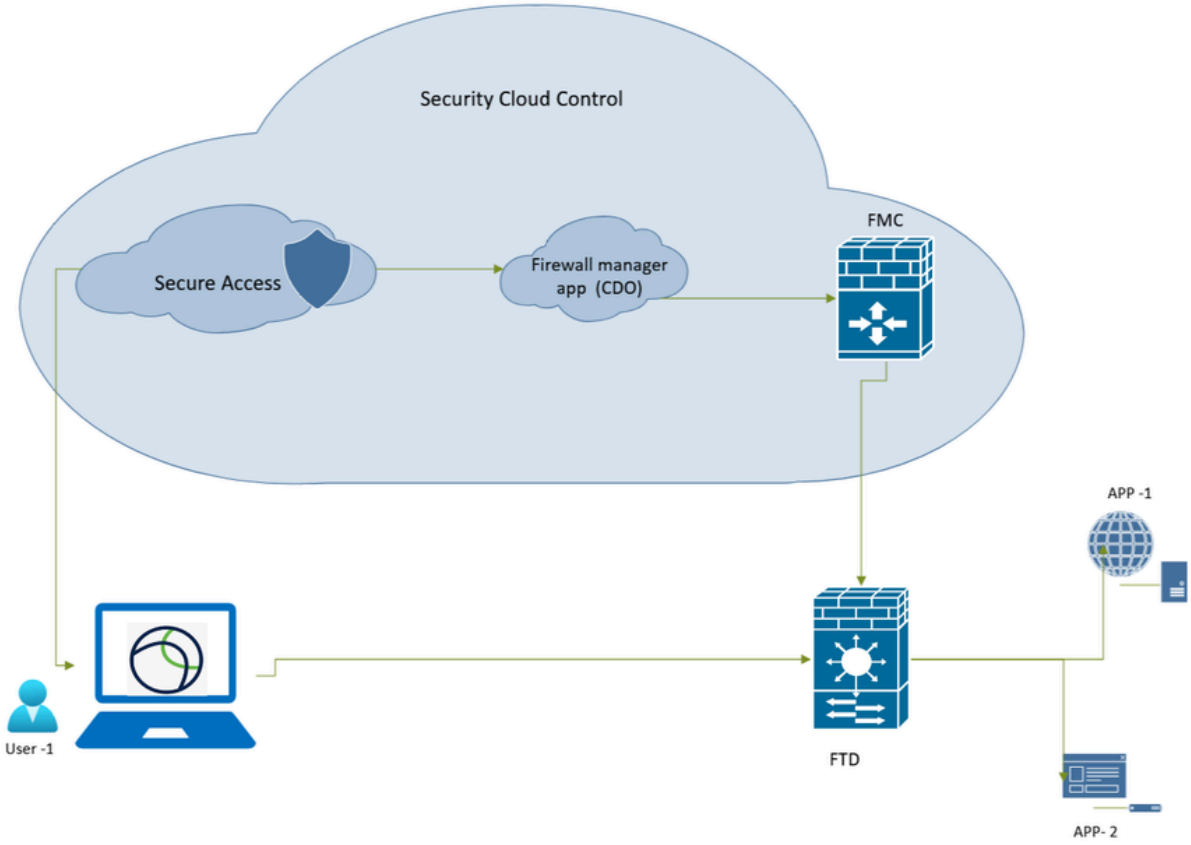
Componentes Utilizados

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.

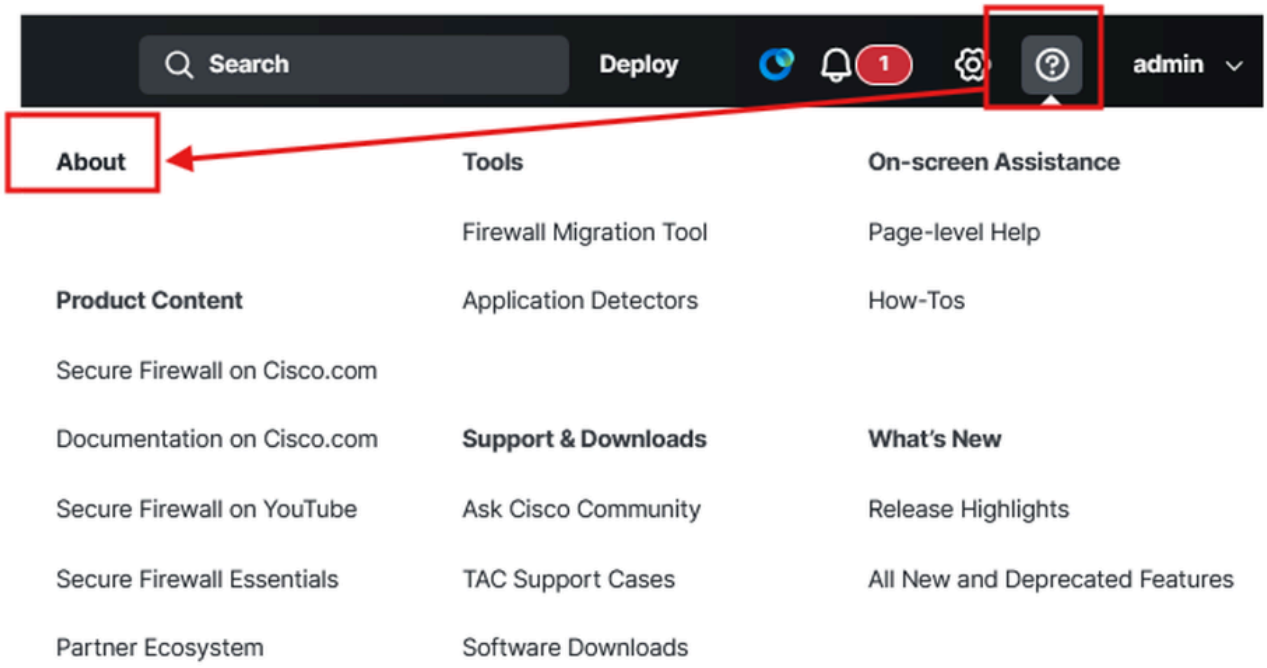
- No se admiten los FTD implementados como contenedores en series Firepower 4K y 9K
- Las sesiones ZTNA universales no admiten tramas jumbo

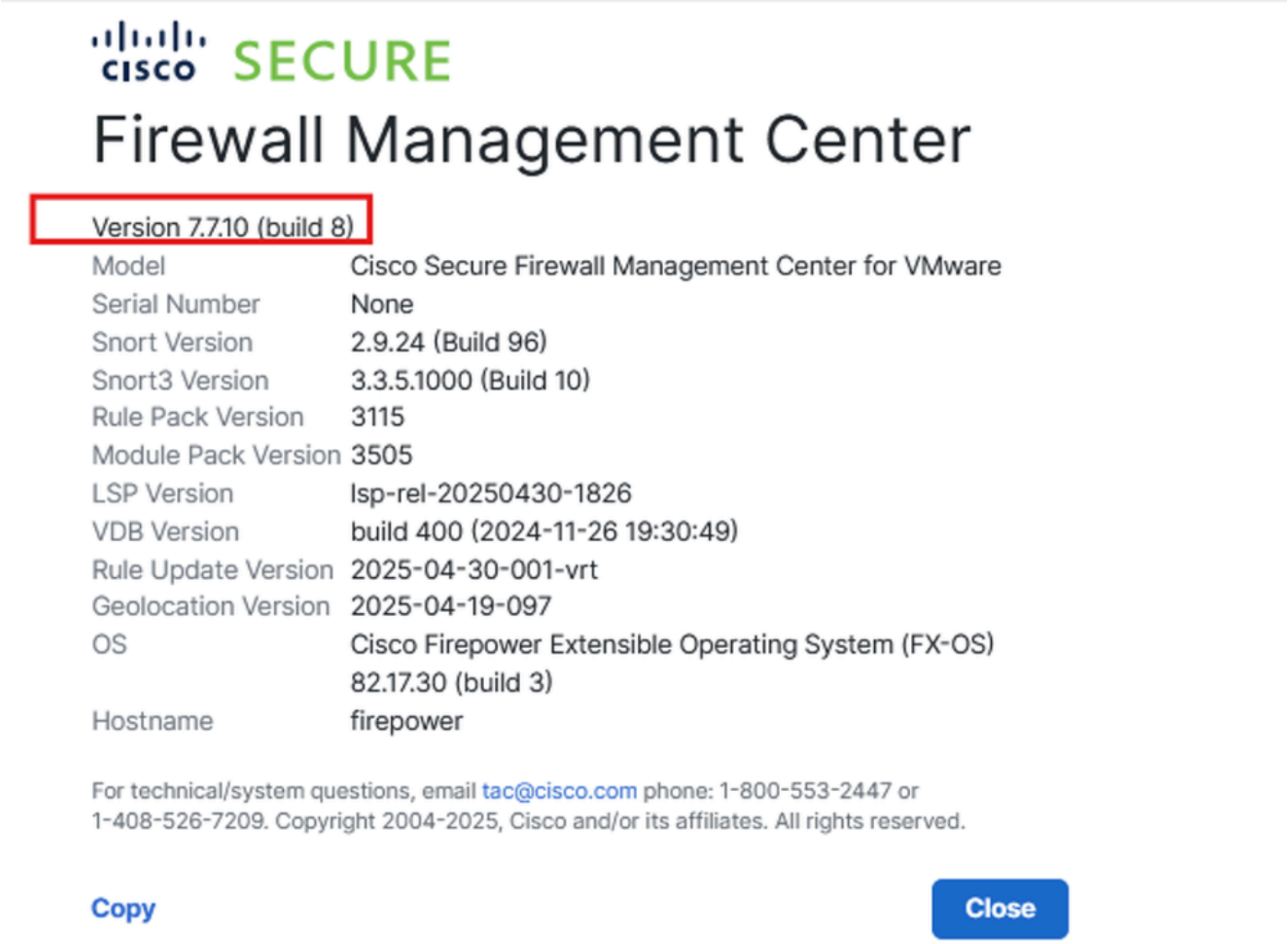
Configurar

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



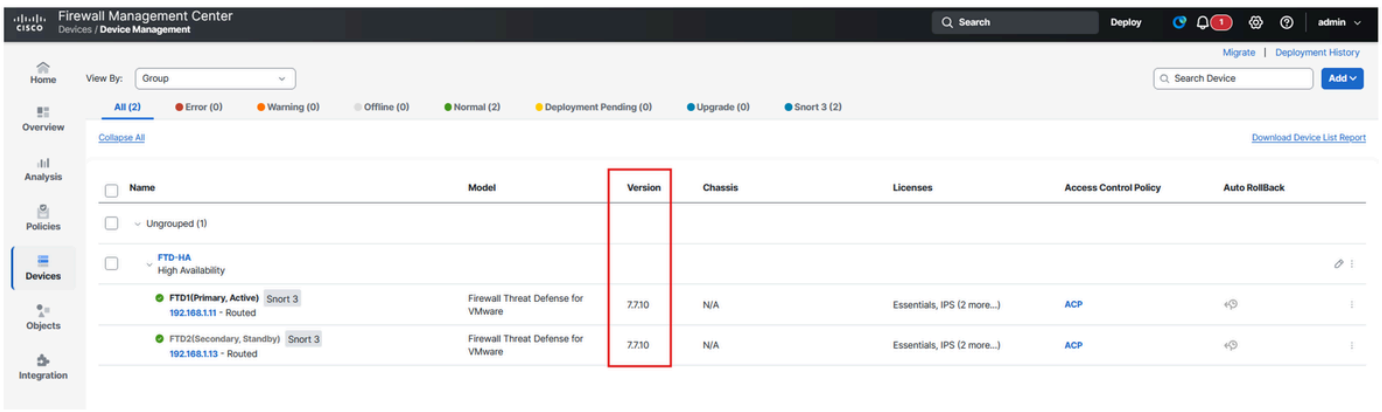


Secure Firewall Management Center - Versión de software

Comprobar versión de FTD

Vaya a FMC UI:

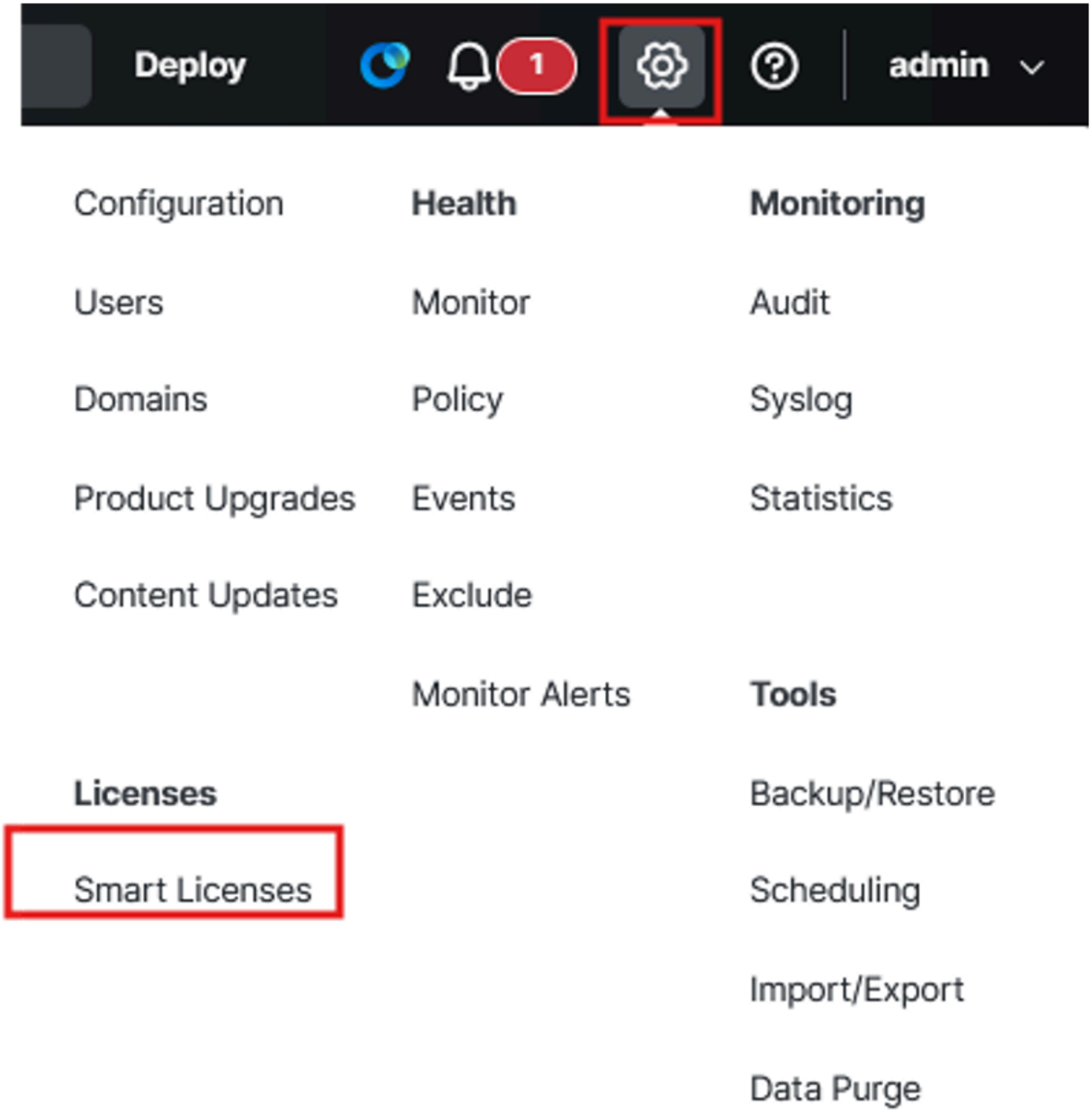
- Haga clic enDevices> Device Management

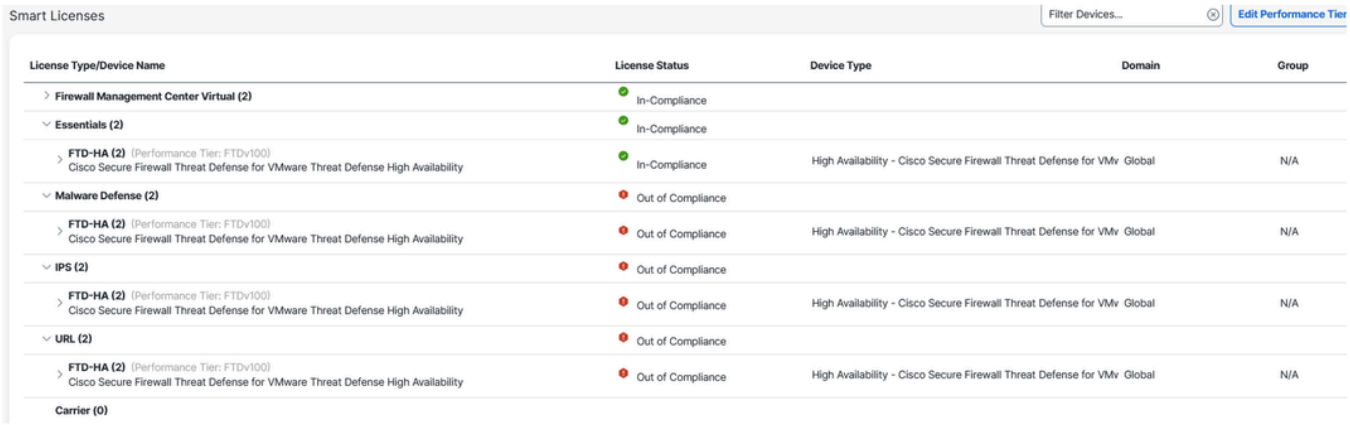


Secure Firewall Threat Defence - Versión de software

Verificar licencias FTD

- Haga clic en Setting Icon >Licenses> Smart Licenses





Firewall seguro Threat Defence - Licencias inteligentes

Compruebe los parámetros de la plataforma y el DNS configurado correctamente

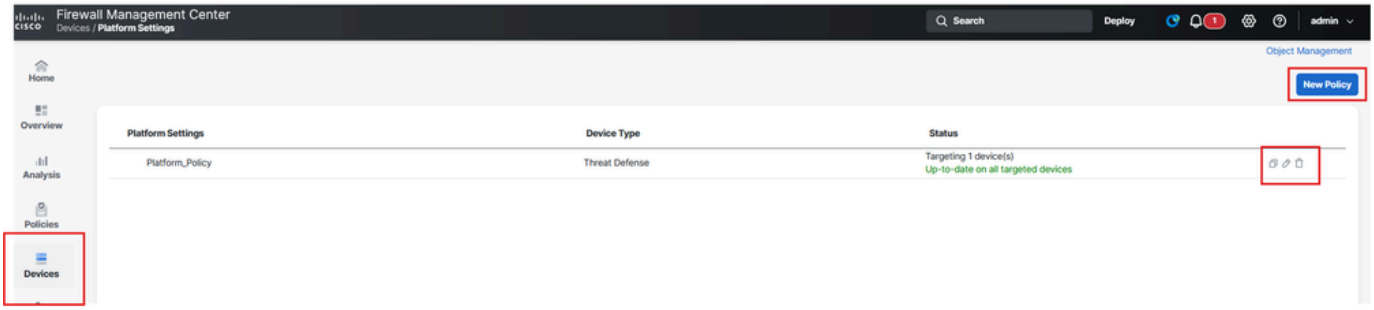
Registro en el FTD a través de CLI:

- Ejecute el comando para verificar si DNS está configurado:

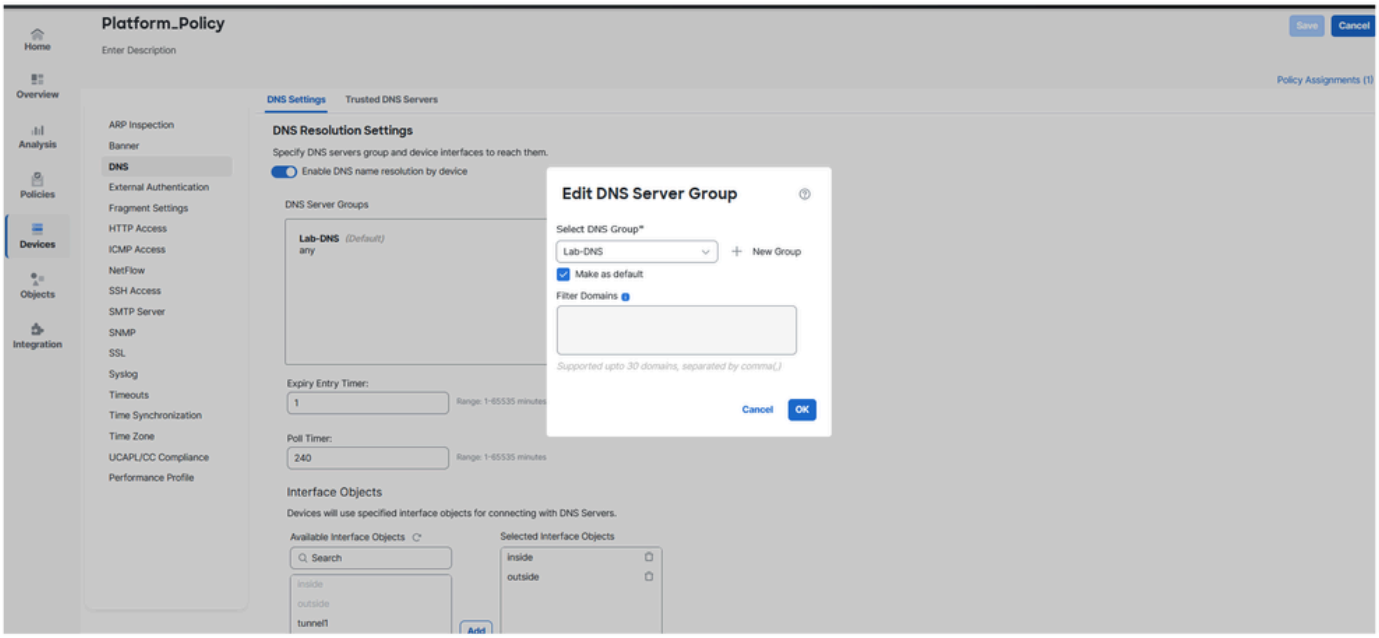
```
show run dns
```

En el CSP:

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



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).

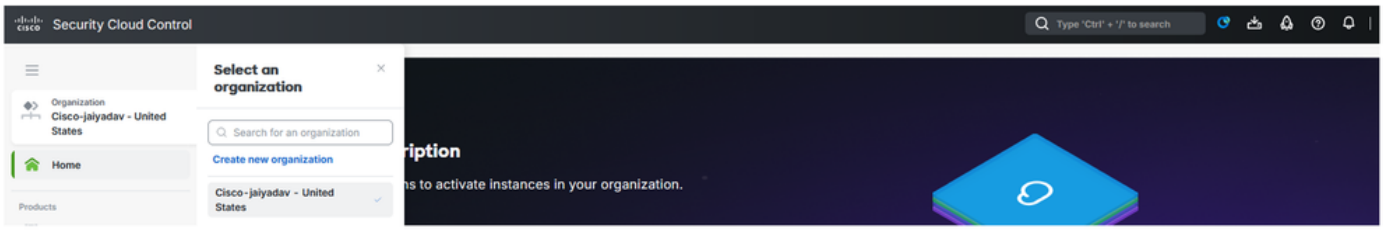
```
dns-group Lab-DNS
ftd1# ping ise.taclab.com
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.50, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
ftd1#
```

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.

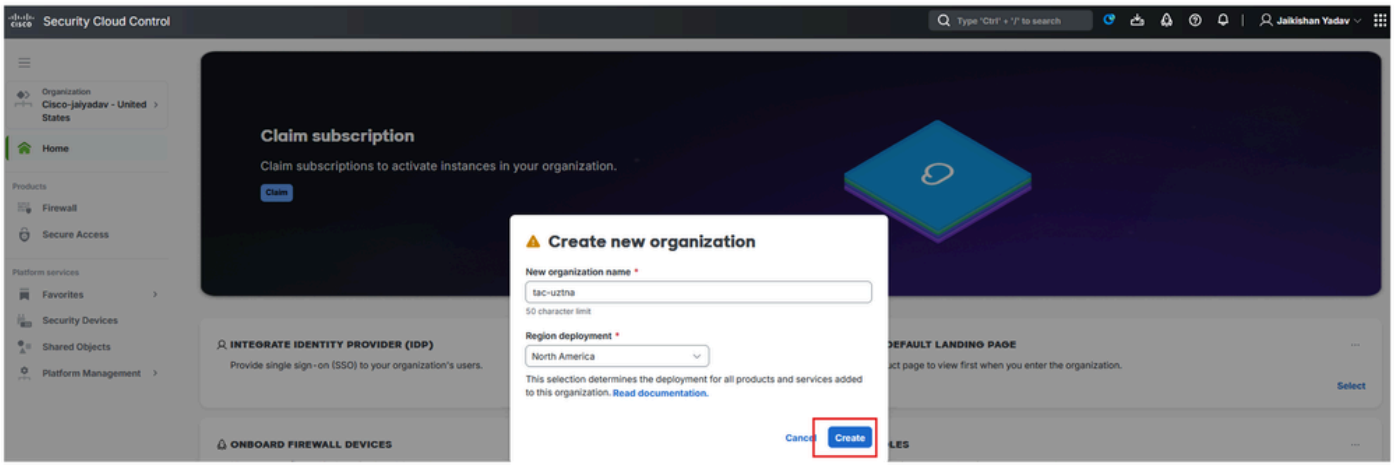
Vaya a Security Cloud Control:

- Haga clic enOrganization > Create new organization



Control seguro de la nube - Organización

- Haga clic en Create



Control seguro de la nube: creación de organizaciones

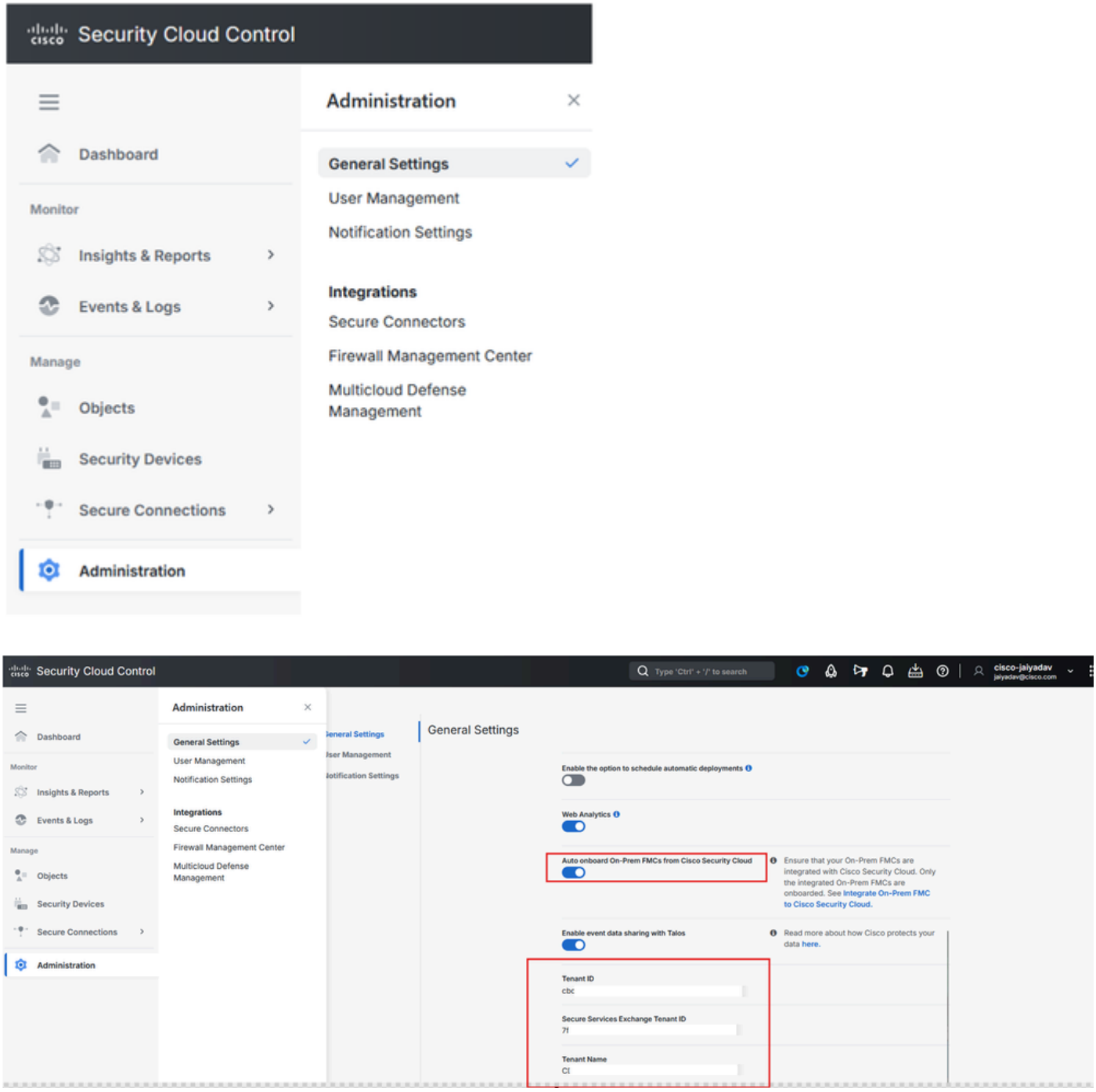
Una vez creado el arrendatario de SCC , recopile la información del arrendatario para habilitar la microaplicación Firewall y Secure Access y para habilitar ZUTNA.

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

Vaya a CDO/SCC:

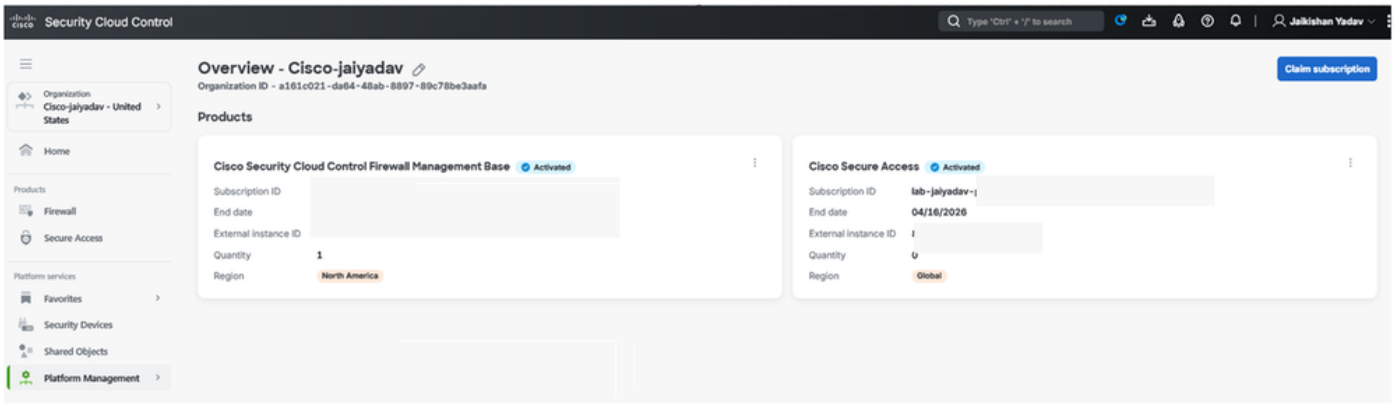
- Haga clic enAdministration> General Settings
- Asegúrese de que Auto onboard On-Prem FMCs from Cisco Security Cloud la opción está activada.

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



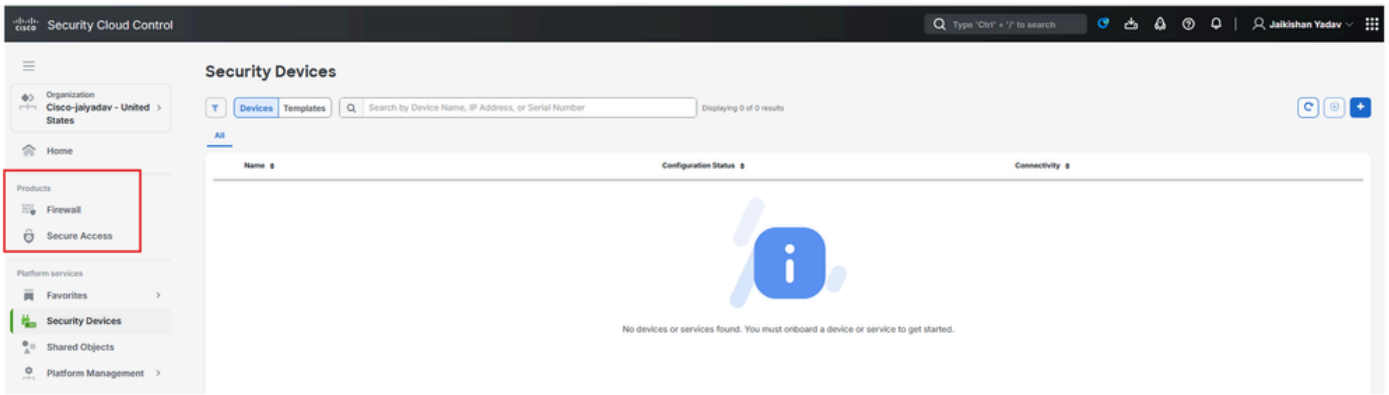
Secure Cloud Control - Detalles de la organización

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



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:



Control seguro de la nube: microaplicaciones

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

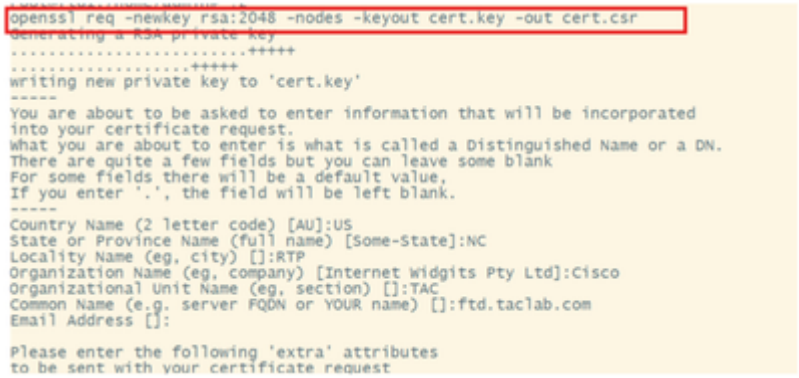
Nota: También puede utilizar certificados de FTD autofirmados Certificados de FTD (consulte la sección Generación de certificados de CA internos e internos autofirmados). El certificado debe estar en formato PKCS12 y debe estar presente en el almacén del equipo del usuario en la CA raíz de confianza.

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

- Navegar hasta FTD
- Ejecutar,expertcomando

- Generar CSR y clave mediante openssl
  - Comando OpenSSL:

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



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:

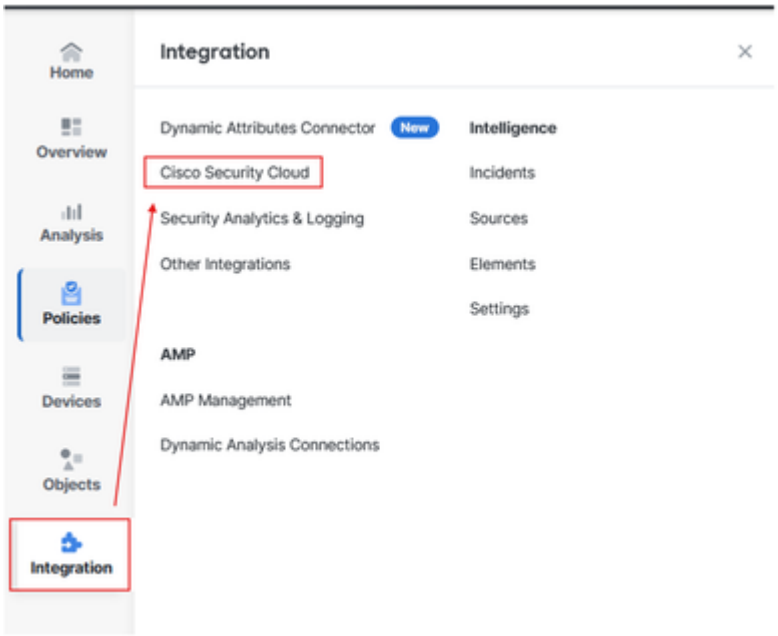
```
openssl pkcs12 -export -out ftdcert.p12 -in cert.crt -inkey cert.key
```

- Exporte el certificado mediante SCP u otra herramienta.

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

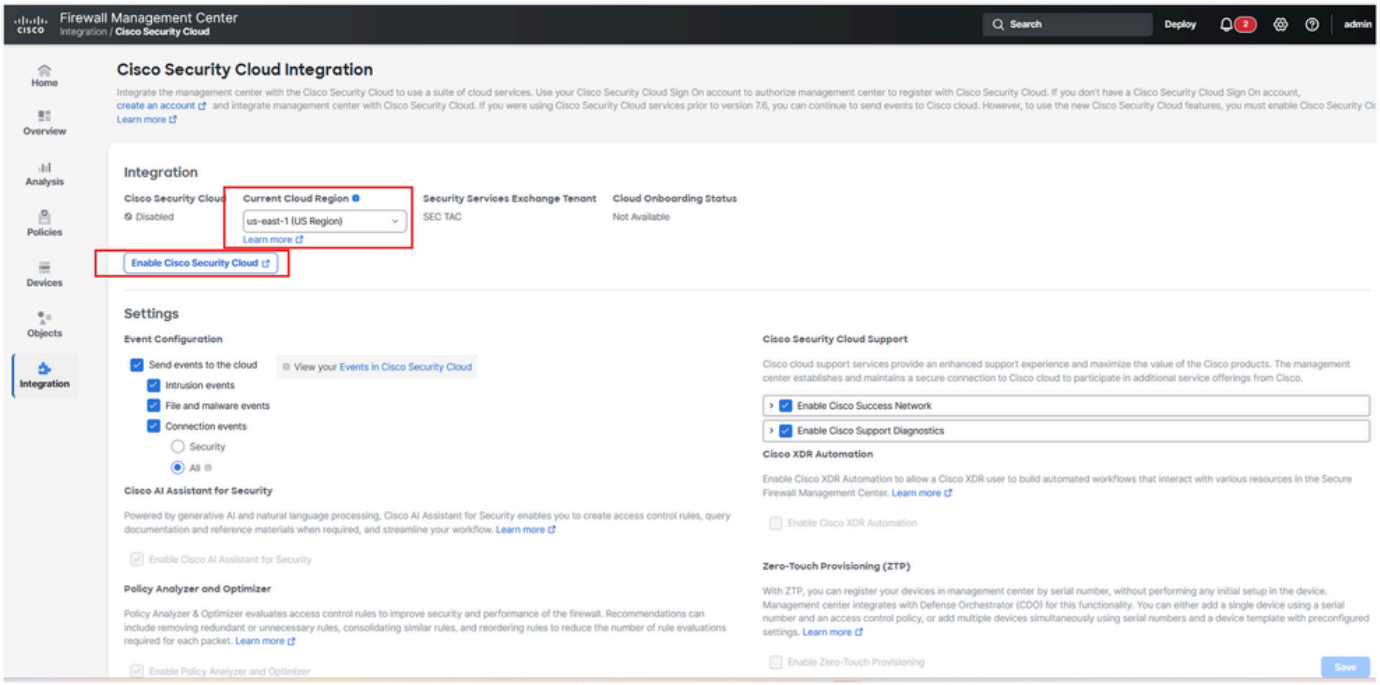
Acceda a FMC:

- Haga clic enIntegration> Cisco Security Cloud



Firewall Management Center e integración con SCC

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

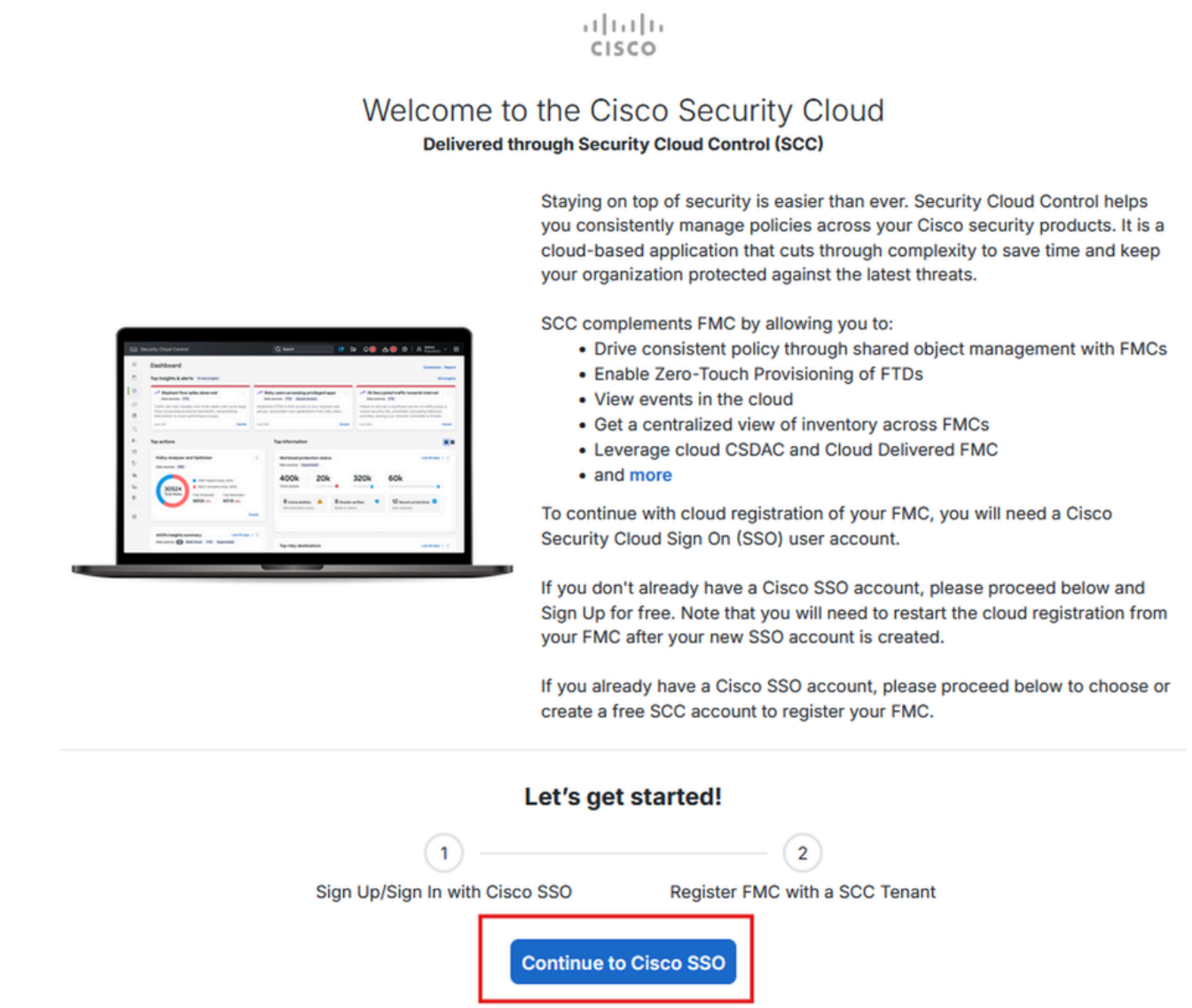


Integración de Firewall Management Center en SCC

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

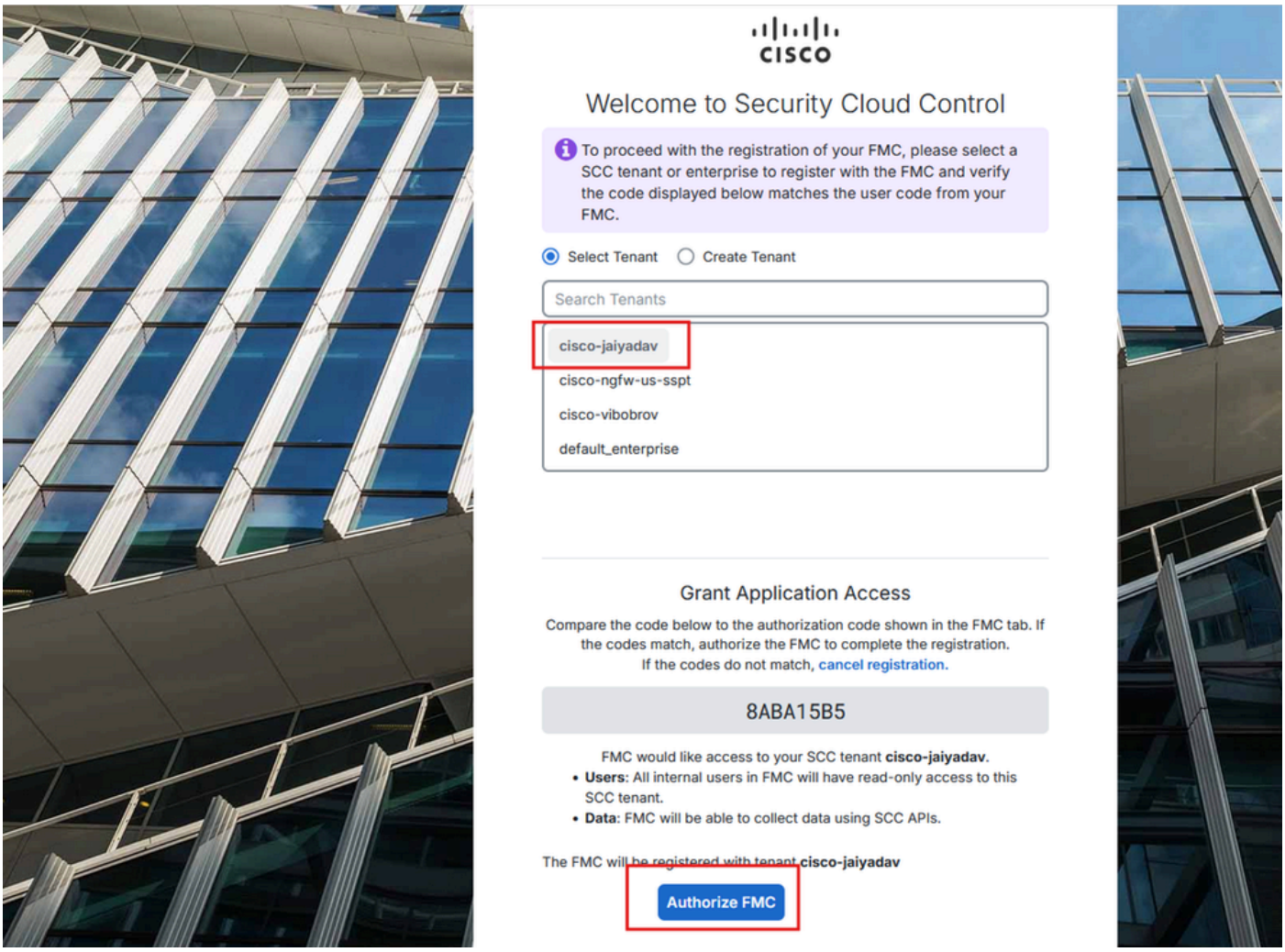
- Haga clic en Continue to Cisco SSO

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



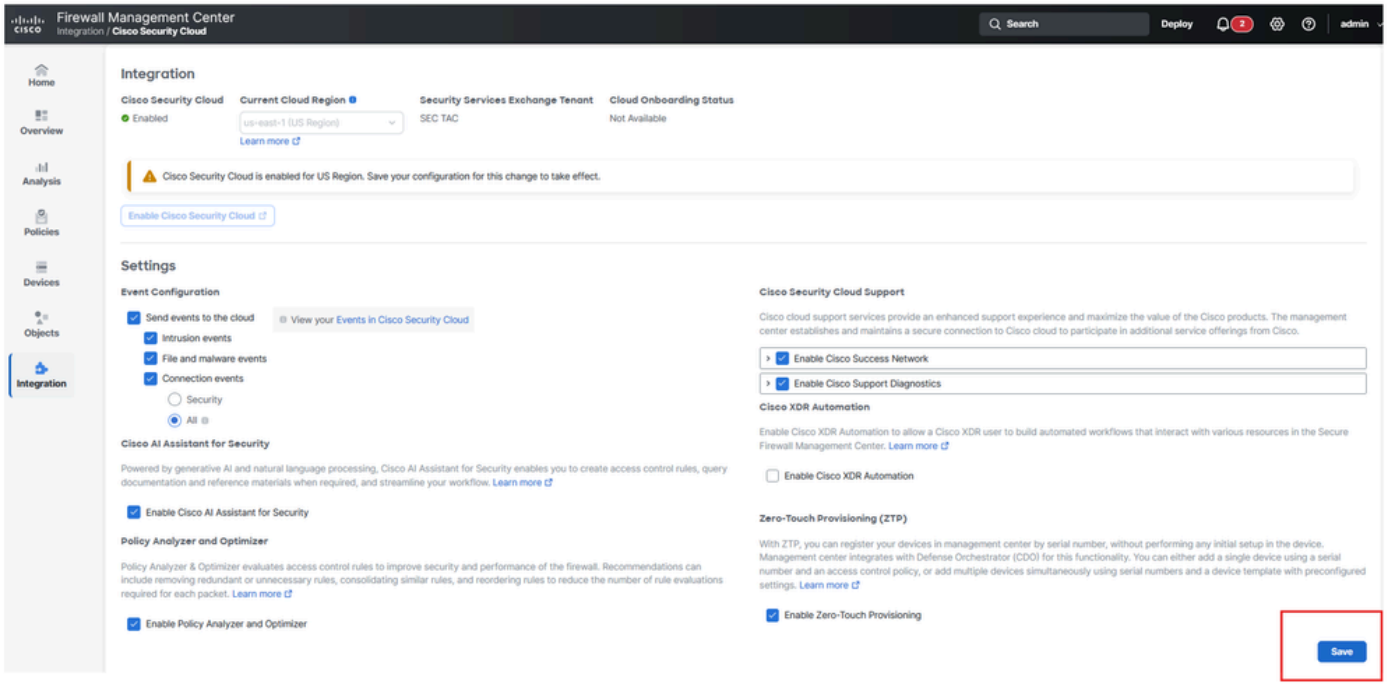
Integración de Firewall Management Center en SCC

- Elija su arrendatario de SCC y haga clic en Authorize FMC



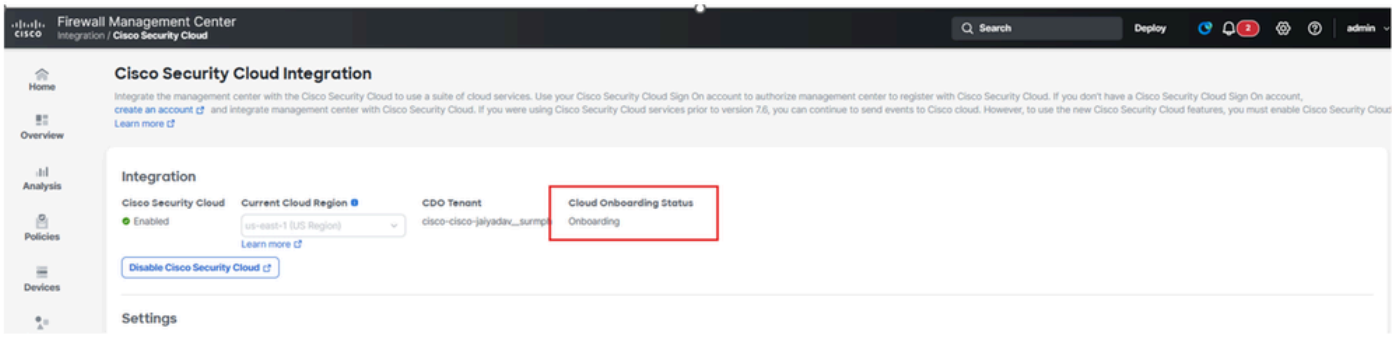
Integración de Firewall Management Center en SCC

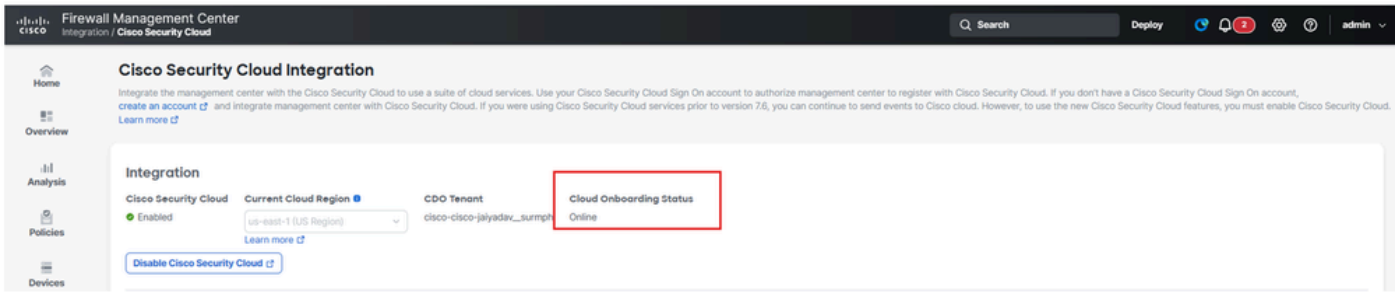
- Haga clic en Save



Integración de Firewall Management Center en SCC

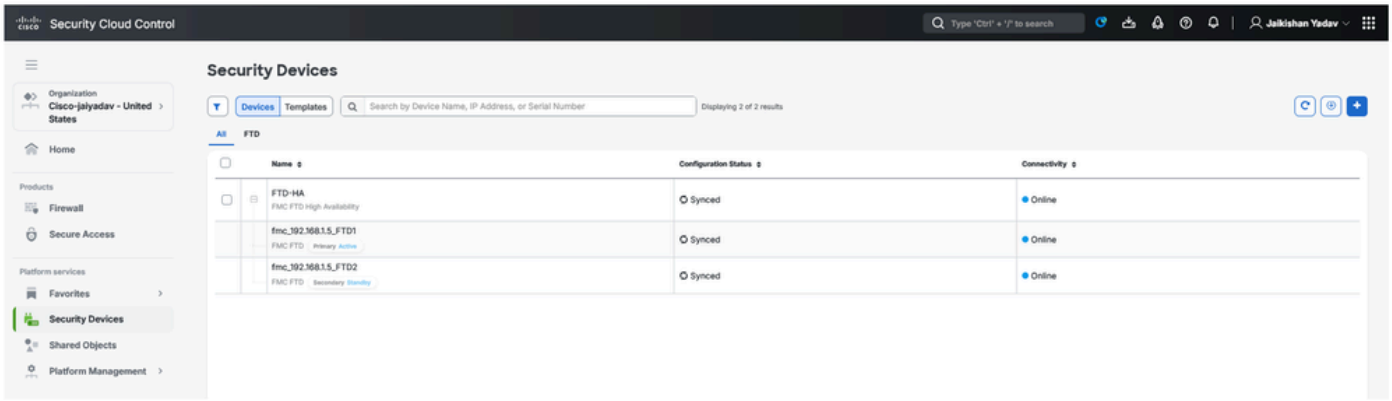
El estado de Cloud Onboarding Status debe cambiar de **Not Available** a Onboarding entonces Online.





Estado de onboarding de Firewall Management Center

- Vaya a SCC y compruebe el estado de FTD enPlatform Services> Security Devices

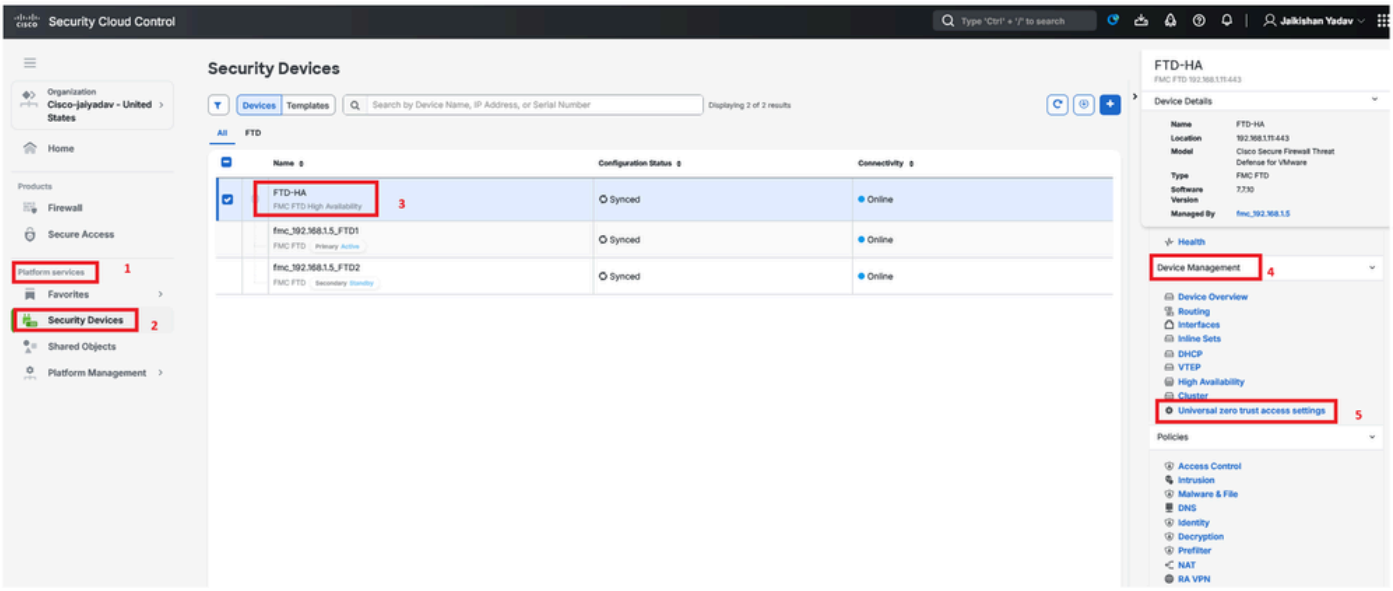


Estado de defensa frente a amenazas de firewall seguro en SCC

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

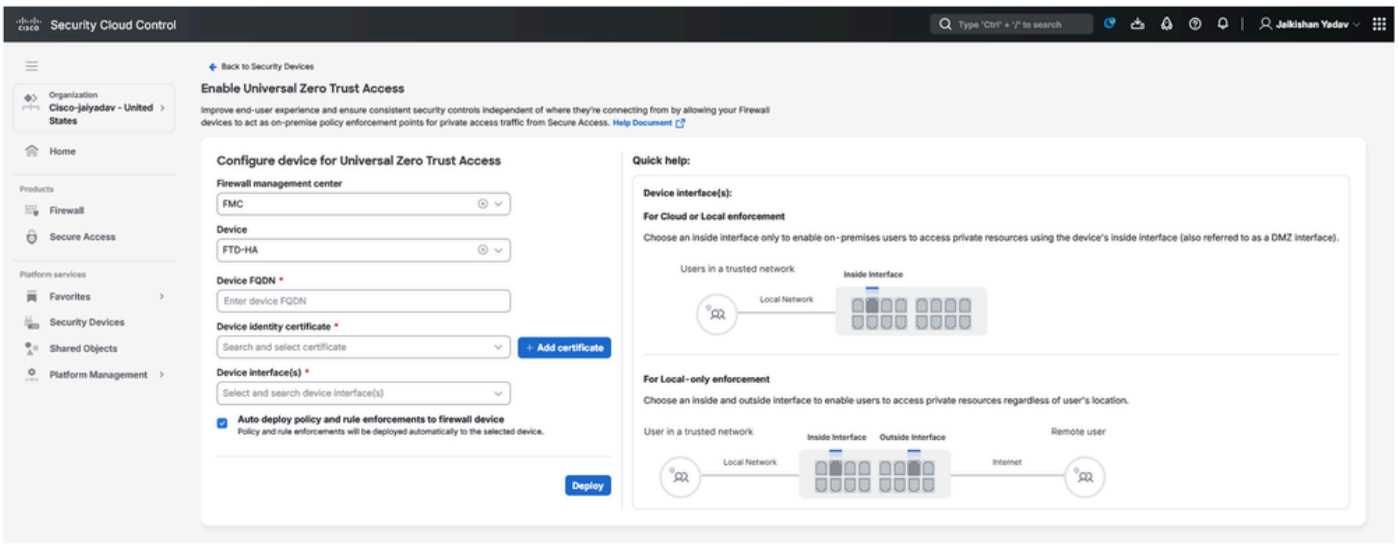
Vaya a SCC:

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

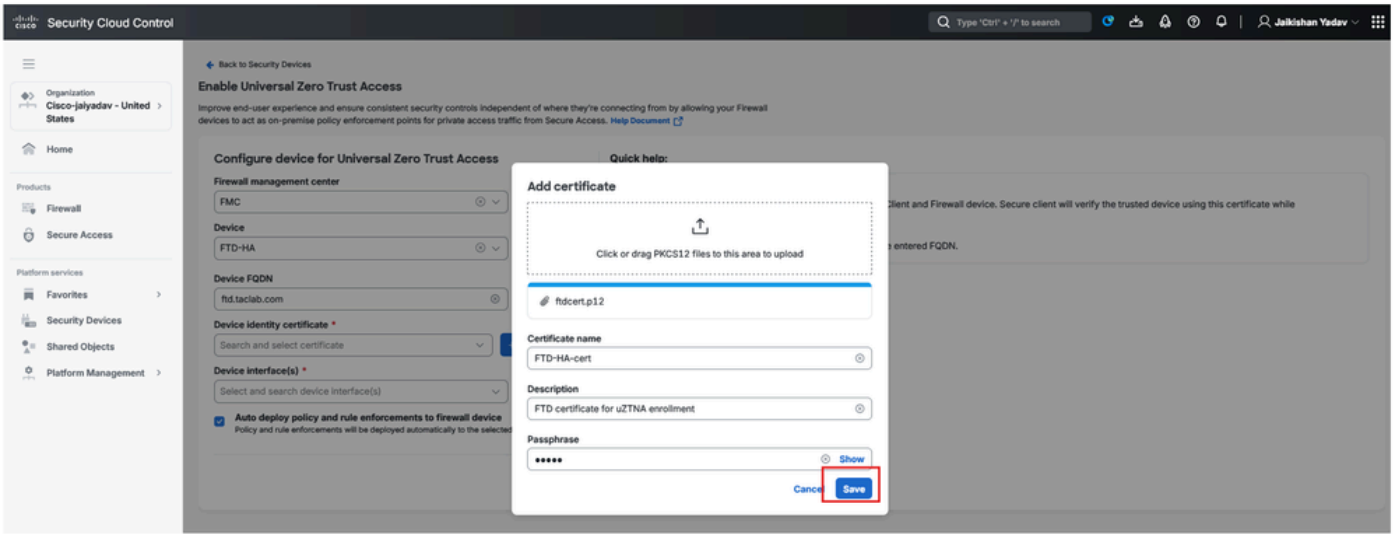


Protección frente a amenazas con firewall - Configuración ZTNA universal

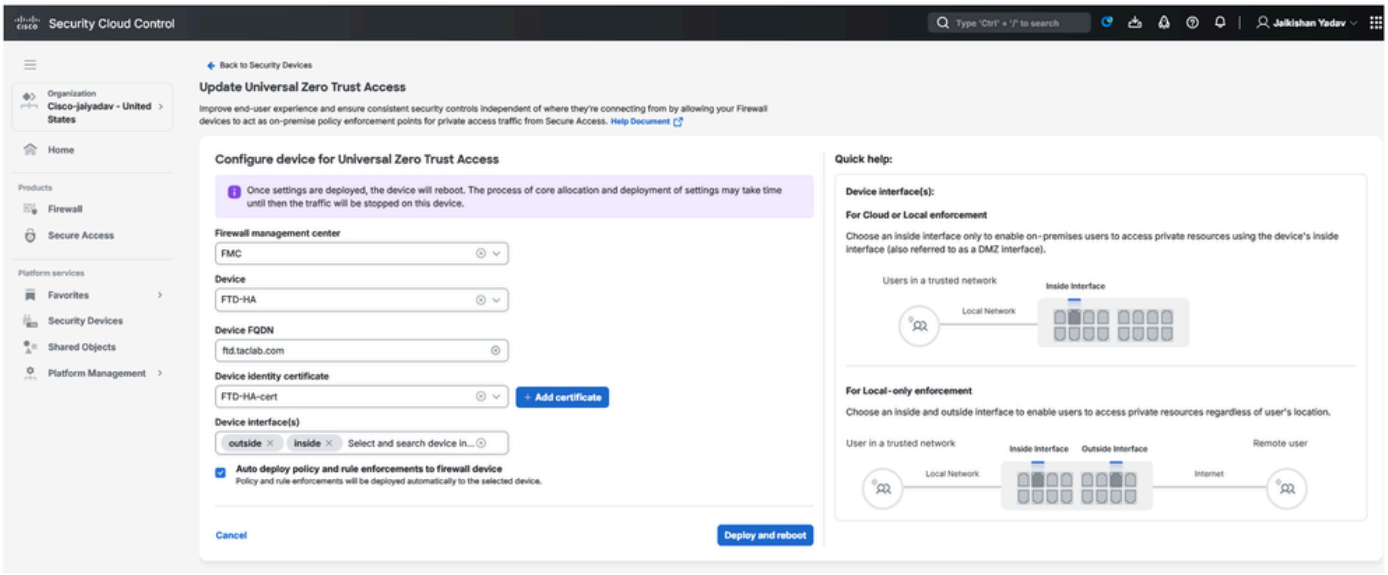
- Rellene la información y cargue el certificado de FTD generado en el paso Generar certificado firmado de CA de Defensa frente a amenazas de firewall (FTD)



Protección frente a amenazas con firewall - Configuración ZTNA universal



Protección frente a amenazas con firewall - Configuración ZTNA universal

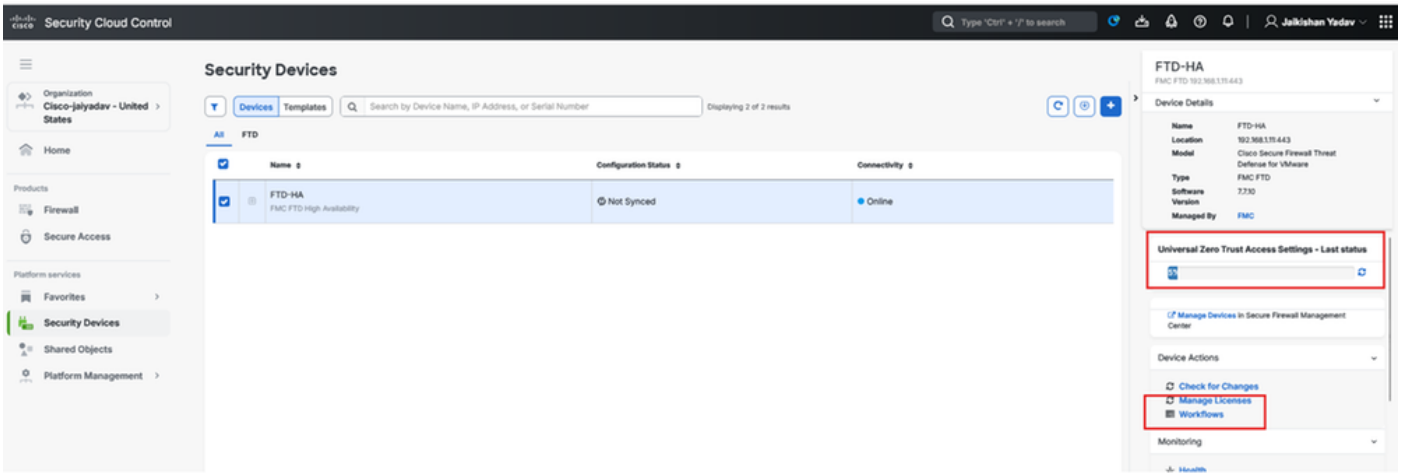


Protección frente a amenazas con firewall - Configuración ZTNA universal

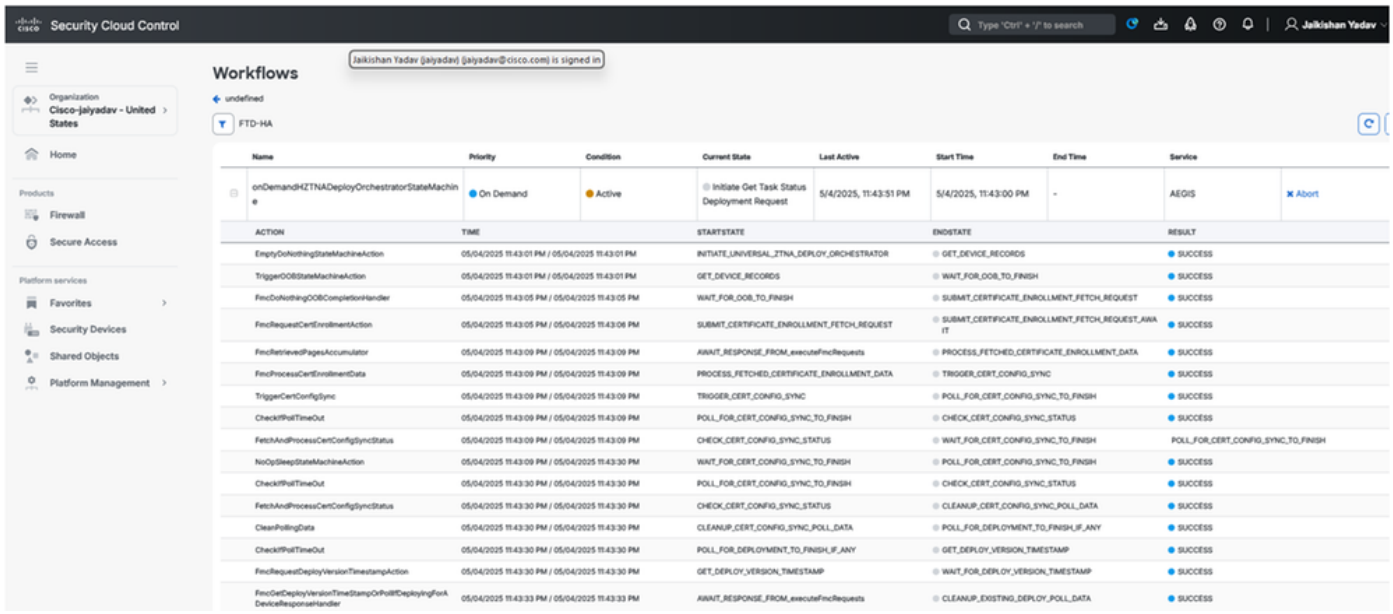
---

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

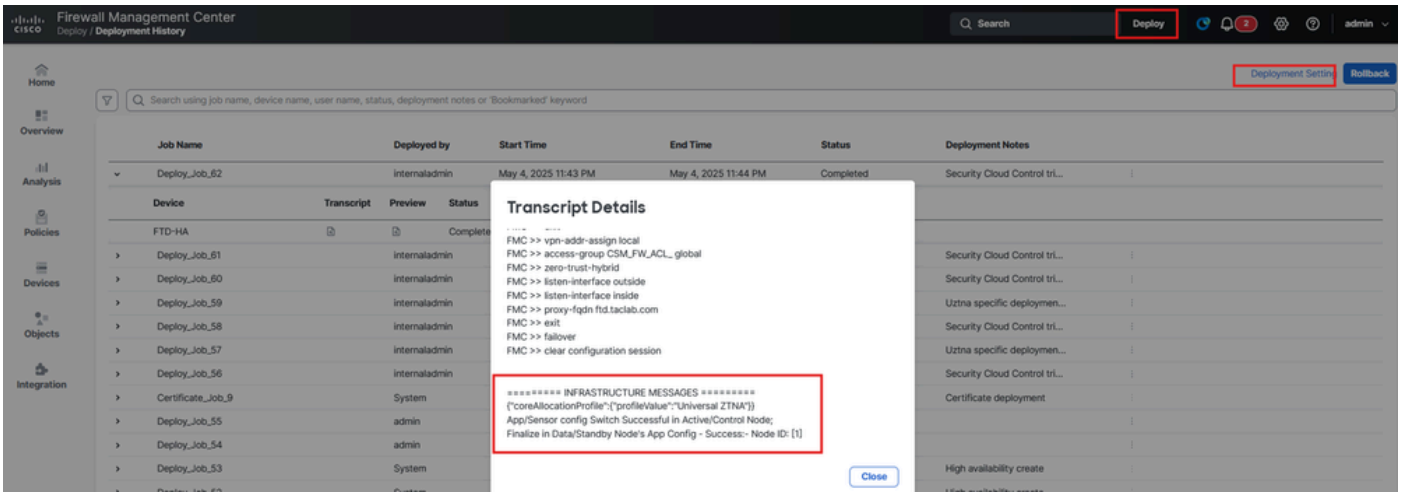


Secure Firewall Threat Defence - Estado de la configuración ZTNA universal



Flujo de trabajo de Security Cloud Control

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



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

Inscriba al cliente con ZUTNA

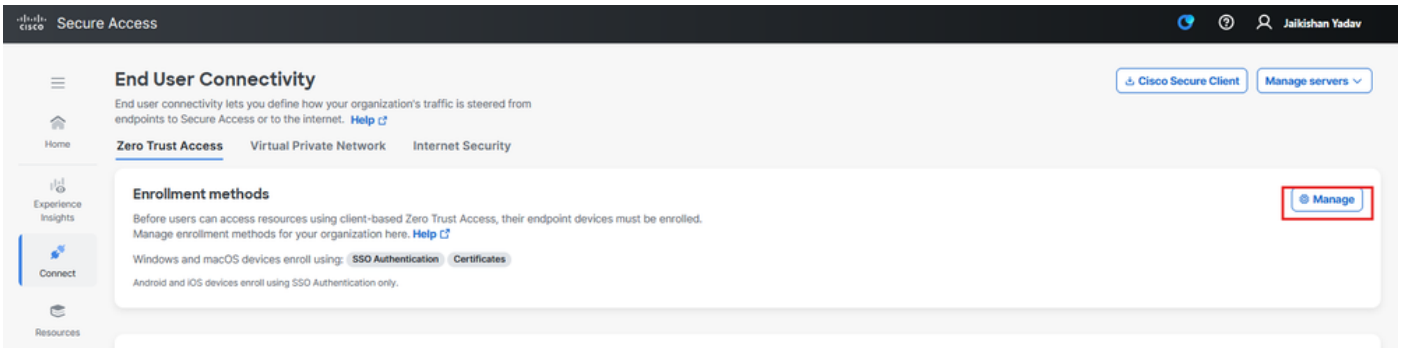
Configuración de Secure Access

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

---

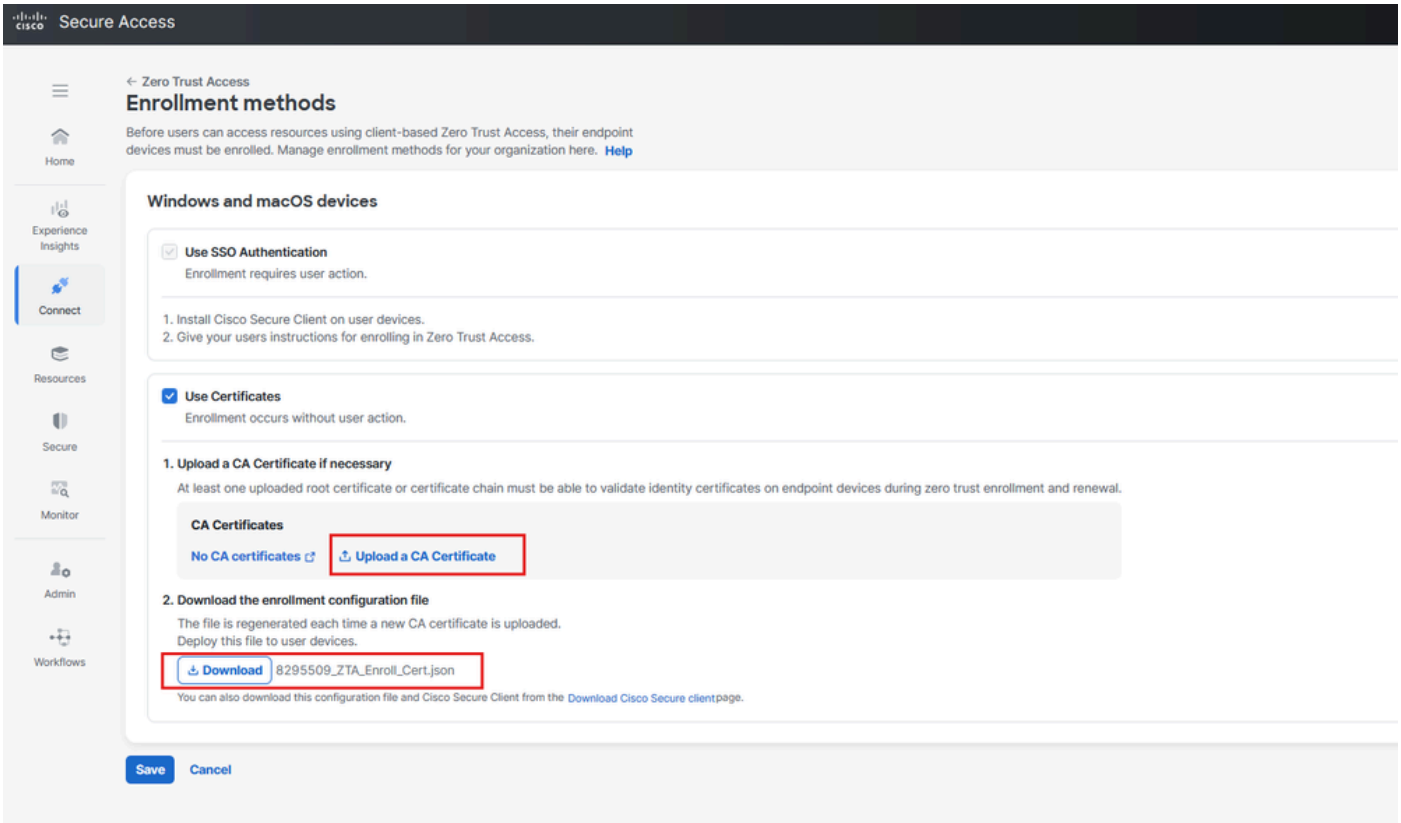
Vaya al Panel de Acceso Seguro:

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



Acceso seguro - Inscripción en certificados ZTA

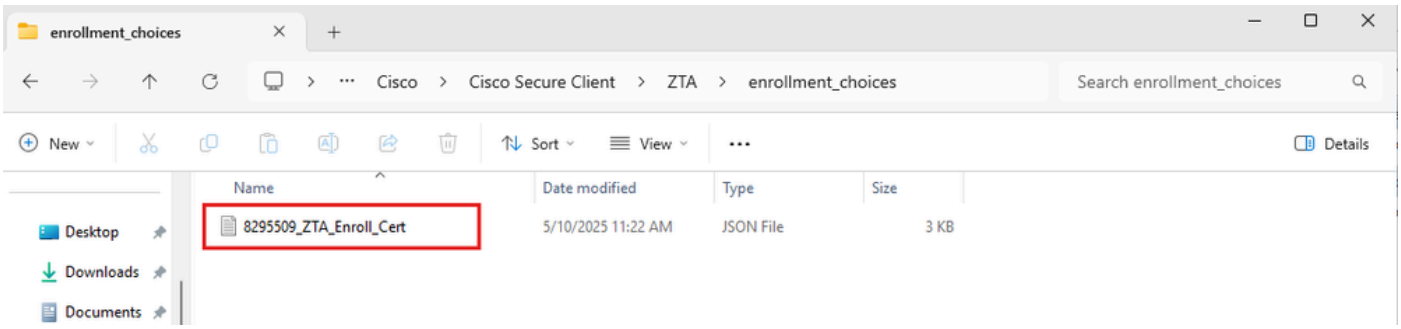
- Cargue el certificado de CA raíz y descargue el archivo de configuración de inscripción



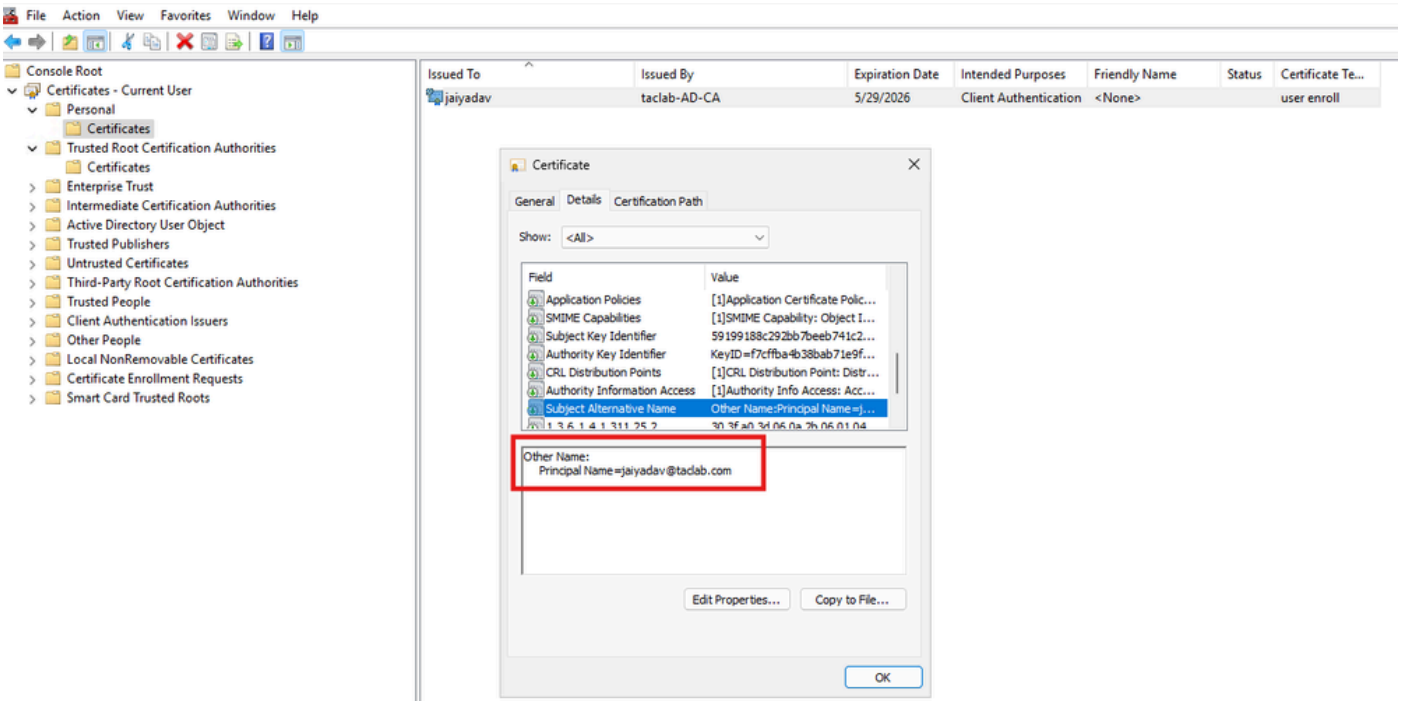
- Haga clic en Save

Configuración del Cliente

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

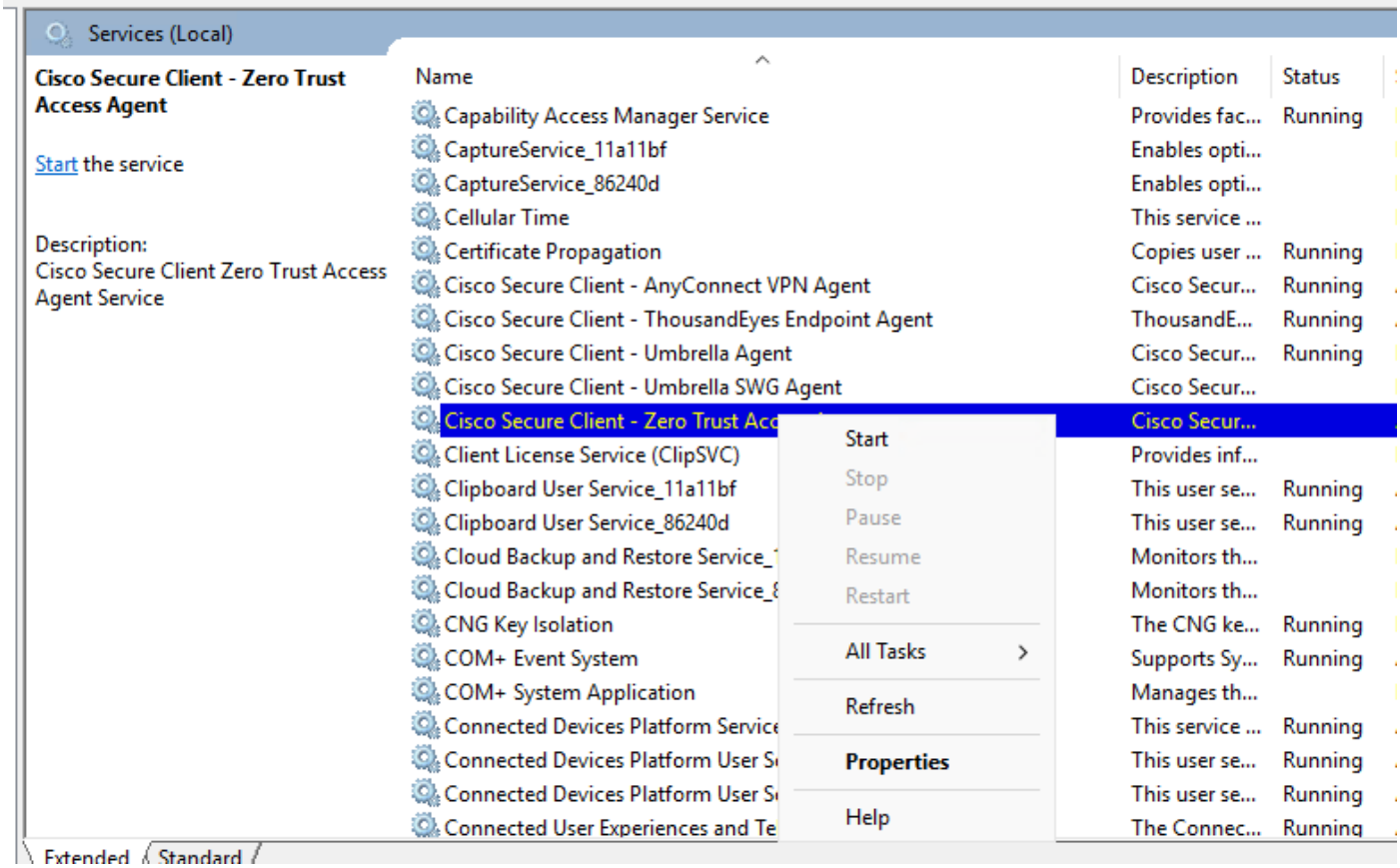


- Cree un certificado de cliente, que debe tener un UPN en un campo SAN



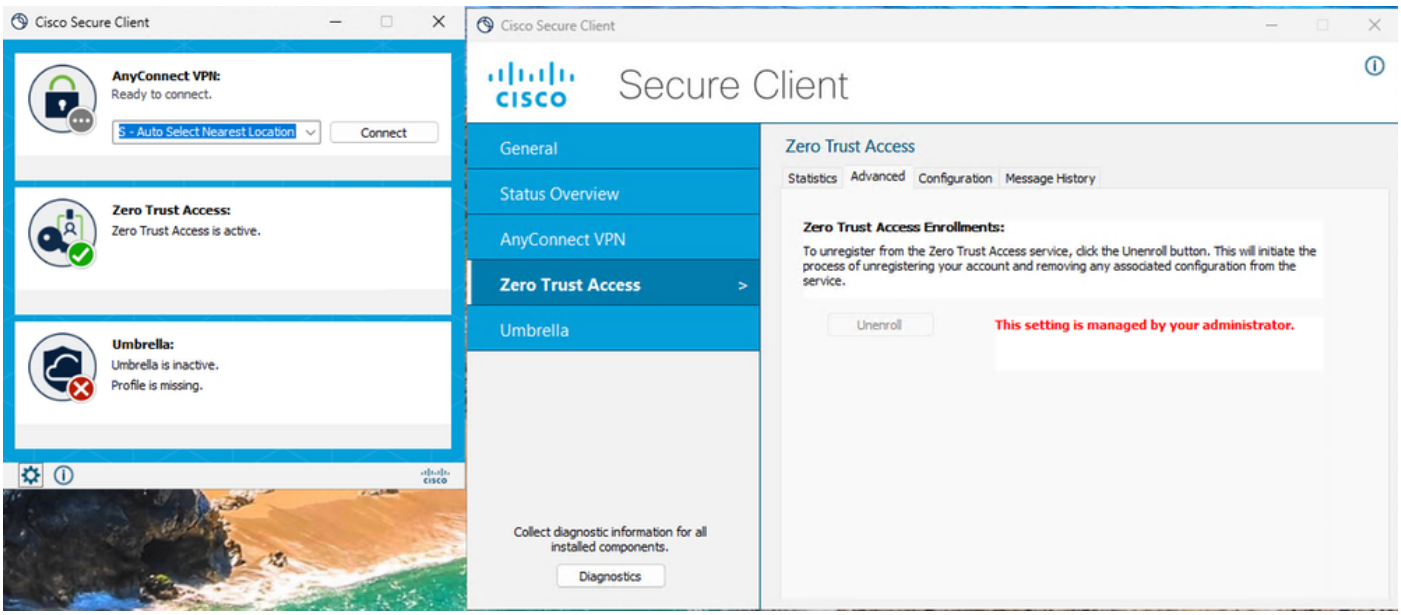
Instalación de certificados

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



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).