

Configurar la autenticación de certificados & Autenticación SAML DUO

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar pasos en DUO](#)

[Crear una directiva de protección de aplicaciones](#)

[Crear directiva de aplicación](#)

[Pasos de configuración para FMC](#)

[Implementación del certificado de identidad en el FTD](#)

[Implementación del certificado IDP en el FTD](#)

[Creación del Objeto SSO de SAML](#)

[Crear configuración de red privada virtual de acceso remoto \(RAVPN\)](#)

[Verificación](#)

[Troubleshoot](#)

[Problema 1: Error de autenticación de certificado.](#)

[problema 2: fallas SAML](#)

Introducción

Este documento describe un ejemplo de la implementación de la autenticación basada en certificados y la autenticación SAML dual.

Prerequisites

Las herramientas y dispositivos utilizados en la guía son:

- Cisco Firepower Threat Defence (FTD)
- Centro de administración Firepower (FMC)
- Autoridad de certificación interna (CA)
- Cuenta Premier de Cisco DUO
- Proxy de autenticación de Cisco DUO
- Cisco Secure Client (CSC)

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- VPN básica,
- SSL/TLS
- Infraestructura de clave pública
- Experiencia con FMC
- Cliente seguro de Cisco
- Código FTD 7.2.0 o superior
- Proxy de autenticación de Cisco DUO

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- FTD de Cisco (7.3.1)
- Cisco FMC (7.3.1)
- Cisco Secure Client (5.0.02075)
- Proxy de autenticación de Cisco DUO (6.0.1)
- Mac OS (13.4.1)
- Directorio activo

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.

Configurar pasos en DUO

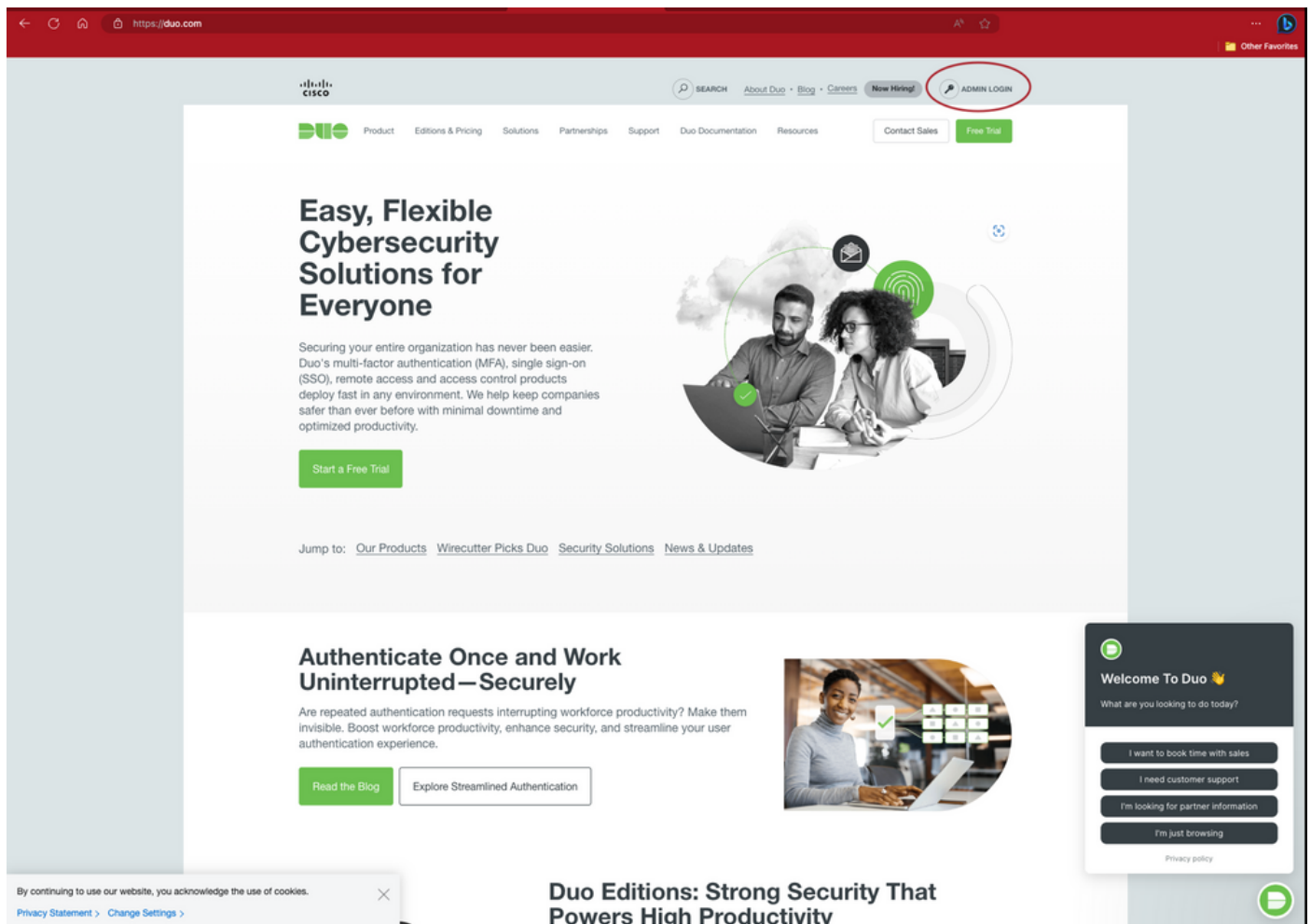
En esta sección se describen los pasos para configurar Cisco DUO Single Sign-on (SSO). Antes de comenzar, asegúrese de que el proxy de autenticación esté implementado.



Advertencia: Si no se ha implementado un proxy de autenticación, este link tiene la guía para esta tarea. [DUO Authentication Proxy Guide](#)

Crear una directiva de protección de aplicaciones

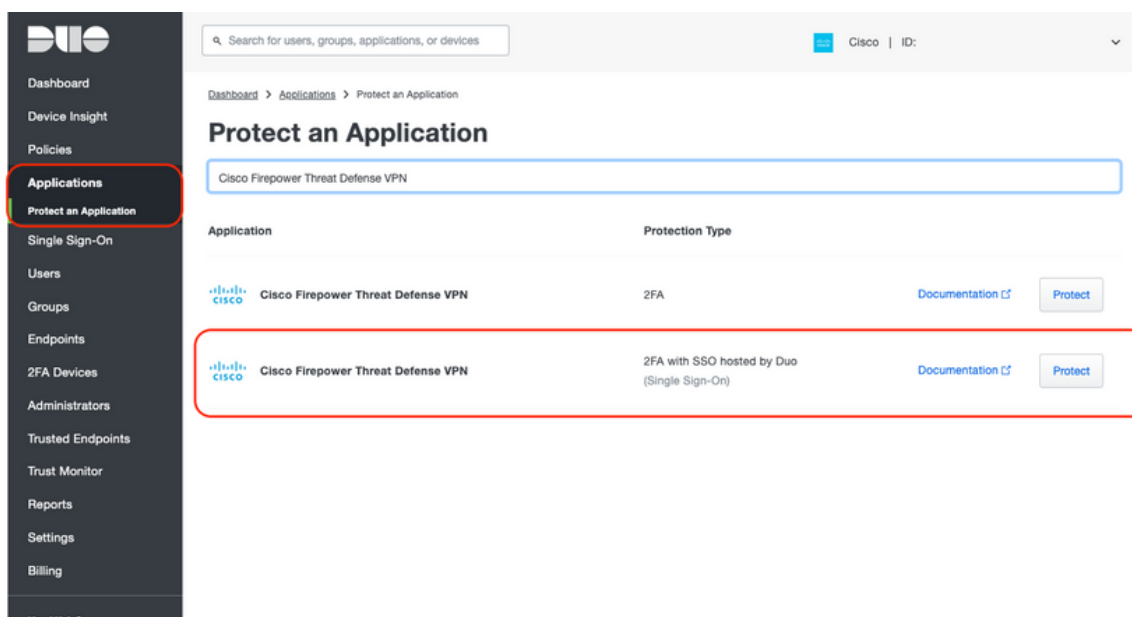
Paso 1. Inicie sesión en el panel de administración mediante este enlace [Cisco Duo](#)



Página de inicio de Cisco DUO

Paso 2. Navegue hasta Panel > Aplicaciones > Proteger una aplicación.

En la barra de búsqueda, introduzca "Cisco Firepower Threat Defence VPN" y seleccione "Proteger".



Proteger una captura de pantalla de aplicación

Seleccione la opción con el único tipo de protección "2FA con SSO alojado por Duo".

Paso 3: Copie esta información de URL en Metadatos.

- ID de entidad del proveedor de identidad
- URL DE SSO
- URL de desconexión

See the [Cisco ASA SSO documentation](#) to integrate Duo into your SAML-enabled service provider.

Metadata

Entity ID

Copy

Sign In URL

Copy

Sign Out URL

Copy

Ejemplo de información para copiar



Nota: Los enlaces se han omitido de la captura de pantalla.

Paso 4. Seleccione "Descargar certificado" para descargar el Certificado del Proveedor de Identidad en Descargas.

Paso 5. Rellene la información del proveedor de servicios

URL de Cisco Firepower Base: FQDN utilizado para alcanzar el FTD

Nombre Del Perfil De Conexión: El Nombre Del Grupo De Túnel

Crear directiva de aplicación

Paso 1: Para crear una política de aplicación en Política Seleccione "Aplicar una política a todos los usuarios" y, a continuación, seleccione "O, crear una nueva política" como se muestra en la imagen.

Policy

Policy defines when and how users will authenticate when accessing this application. Your global policy always applies, but you can override its rules with custom policies.

Group policies

Apply a policy to groups of users

Application policy

Apply a policy to all users

Ejemplo de creación de una directiva de aplicación

Apply a Policy



Policy

Select a Policy



[Or, create a new Policy](#)

Apply Policy

Ejemplo de creación de una directiva de aplicación

Paso 2. En Nombre de la política, ingrese el nombre deseado, seleccione "Política de autenticación" bajo Usuarios, y Select "Aplicar 2FA". A continuación, guárdelo con "Crear directiva".

Create a New Policy

Policy name

MFA

Users

New User policy

Authentication policy

User location

Devices

Trusted Endpoints

Device Health application

Remembered devices

Operating systems

Browsers

Plugins

Networks

Authorized networks

Anonymous networks

Authenticators

Risk-based factor selection

Authentication methods

Duo Mobile app

Tampered devices

Screen lock

Full-disk encryption

Mobile device biometrics

Authentication policy

Enforce 2FA

Require two-factor authentication or enrollment when applicable, unless there is a superseding policy configured.

Bypass 2FA

Skip two-factor authentication and enrollment, unless there is a superseding policy configured.

Deny access

Deny authentication to all users.

When enabled, this affects all users.

Choose another rule on the left to add to this policy.

Create Policy

Ejemplo de creación de una directiva de aplicación

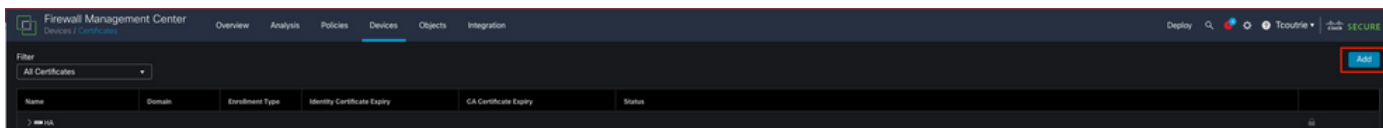
Paso 3. Aplique la política con "Aplicar Política" en la siguiente ventana. a continuación, desplácese hasta la parte inferior de la página y seleccione "Guardar" para finalizar las configuraciones DUO

Pasos de configuración para FMC

Implementación del certificado de identidad en el FTD

En esta sección se describe cómo configurar e implementar el certificado de identidad en el FTD necesario para la autenticación de certificados. Antes de comenzar, asegúrese de implementar todas las configuraciones.

Paso 1. Navegue hasta Dispositivos > Certificado y elija Agregar, como se muestra en la imagen.



Captura de pantalla de dispositivos/certificados

Paso 2: Elija el dispositivo FTD en el menú desplegable de dispositivos. Haga clic en el icono + para agregar un nuevo método de inscripción de certificados.

A screenshot of the 'Add New Certificate' dialog box in the FMC interface. The dialog has a title bar with a question mark icon. Below the title, there is a text instruction: 'Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.' Below this, there are two dropdown menus. The first is labeled 'Device*' and has 'HA' selected. The second is labeled 'Cert Enrollment*' and has 'Select a certificate enrollment object' selected. To the right of the second dropdown, there is a red box highlighting a '+' button. At the bottom right of the dialog, there are two buttons: 'Cancel' and 'Add'.

Captura de pantalla de Add New Certificate

Paso 3: Elija la opción que es el método preferido para obtener certificados en el entorno a través del "Tipo de inscripción", como se muestra en la imagen.

Add Cert Enrollment



Name*

FTD04-16

Description

Enrollment Type:

PKCS12 File



PKCS12 File*:

test.p12



[Browse PKCS12 File](#)

Passphrase:

.....



Validation Usage:



IPsec Client



SSL Client



SSL Server



Skip Check for CA flag in basic constraints of the CA Certificate



Allow Overrides

[Cancel](#)

[Save](#)

Captura de pantalla de la nueva página de inscripción de certificados



Consejo: Las opciones disponibles son: Certificado autofirmado: genere un nuevo certificado localmente, SCEP: utilice Simple Certificate Enrollment Protocol para obtener un certificado de una CA, Manual: instale manualmente el certificado de identidad y raíz, PKCS12: cargue el paquete de certificados cifrados con la raíz, la identidad y la clave

privada.

Implementación del certificado IDP en el FTD

En esta sección se describe la configuración y el despliegue del certificado de IDP en el FTD. Antes de comenzar, asegúrese de desplegar todas las configuraciones.

Paso 1: Navegue hasta Dispositivos > Certificado y elija Agregar."

Paso 2: Elija el dispositivo FTD en el menú desplegable de dispositivos. Haga clic en el icono + para agregar un nuevo método de inscripción de certificados.

Paso 3: Dentro de la ventana add Cert Enrollment, ingrese la información requerida como se muestra en la imagen, luego "Save" como se muestra en la imagen.

- Nombre: Nombre del objeto
- Tipo de inscripción: Manual
- Casilla de verificación activada: Solo CA
- Certificado de CA: Formato Pem del certificado

Add Cert Enrollment

Name*

duocert

Description

CA Information

Certificate Parameters

Key

Revocation

Enrollment Type

Manual

☒ CA Only
Check this option if you do not require an identity certificate to be created from this CA

CA Certificate:

OC957DUc7tc4
b79bVzOXuqz5ZpaJHqtXV8fLOH
eIPYblyYBwSstXB+k75VHs0Voz
AkeySJCWRQXF
ISSRGu8DpUIKzKu2zd55322+wd
fkyy/WMXUJWmSXKKnnHEsOqL
GCxmfd+5OsWlo
ICCMGa5gYgEv8EHF3Y++sFg=
-----END CERTIFICATE-----

Validation Usage:

☒ IPsec Client

☐ SSL Client

☒ SSL Server

☐ Skip Check for CA flag in basic constraints of the CA Certificate

☐ Allow Overrides

Cancel

Save

Ejemplo de creación de un objeto de inscripción de certificados



Precaución: Si es necesario, se puede utilizar "Omitir comprobación para el indicador de CA en las restricciones básicas del certificado de CA". Utilice esta opción con precaución.

Paso 4: Seleccione el objeto de inscripción de certificados recién creado en "Inscripción de

certificados*:" y, a continuación, seleccione "Agregar" como se muestra en la imagen.

Add New Certificate

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*:
HA

Cert Enrollment*:
duocert

Cert Enrollment Details:

Name: duocert
Enrollment Type: Manual (CA Only)
Enrollment URL: N/A

Cancel Add

Captura de pantalla del dispositivo y el objeto de inscripción de certificados agregados



Nota: Una vez agregado, el certificado implementa inmediatamente.

Creación del Objeto SSO de SAML

Esta sección describe los pasos para configurar el SSO de SAML a través de FMC. Antes de comenzar, asegúrese de implementar todas las configuraciones.

Paso 1. Navegue hasta Objetos > Servidor AAA > Servidor de Single Sign-on y seleccione "Agregar Servidor de Single Sign-on".

Firewall Management Center
Objects / Object Management

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ ? Tcourtrie | cisco SECURE

AAA Server
RADIUS Server Group
Single Sign-on Server
> Access List
> Address Pools
Application Filters
AS Path
bfd Template
Cipher Suite List
> Community List
DHCP IPv6 Pool
> Distinguished Name
DNS Server Group
> External Attributes
File List
> FlexConfig
Geolocation
Interface
Key Chain
Network
> PKI
Policy List
Port
> Prefix List
Route Map

Single Sign-on Server

[Add Single Sign-on Server](#) 🔍 Filter

Single Sign-on Server contains parameters for SAML based authentication. These Single Sign-on Servers are used to authenticate users logging in through Remote Access VPN connections.

Name	
AZ	 
DUO	 

Displaying 1 - 2 of 2 rows |< < Page 1 of 1 > >| 🔄

ejemplo de creación de un nuevo objeto SSO

Paso 2. Introduzca la información necesaria en "Crear una directiva de protección de aplicaciones"

". Para continuar una vez finalizado, seleccione "Guardar".

- Nombre*: Nombre del objeto
- ID de entidad del proveedor de identidad*: ID de entidad del paso 3
- URL DE SSO*: URL de inicio de sesión copiada del paso 3
- URL de cierre de sesión: URL de cierre de sesión copiada del paso 3
- URL base: Utilice el mismo FQDN que "URL de base de Cisco Firepower" en el paso 5
- Certificado del proveedor de identidad*: Certificado IDP implementado
- Certificado de proveedor de servicios: Certificado en la interfaz exterior del FTD

New Single Sign-on Server?

Name*

duosso

Identity Provider Entity ID*

SSO URL*

Logout URL

Base URL

https://vpn.ciscoexample.com

Identity Provider Certificate*

duocert

+

Service Provider Certificate

FTD04-16

+

Request Signature

--No Signature--

Request Timeout

Use the timeout set by the provide

seconds (1-7200)

☐ Enable IdP only accessible on Internal Network

☒ Request IdP re-authentication on Login

☐ Allow Overrides

Cancel

Save

Ejemplo de nuevo objeto SSO.



Nota: Los enlaces ID de entidad, URL de SSO y URL de desconexión se han omitido de

Crear configuración de red privada virtual de acceso remoto (RAVPN)

En esta sección se describen los pasos para configurar RAVPN mediante el asistente.

Paso 1. Navegue hasta Dispositivos > Acceso remoto y seleccione "Agregar."

Paso 2. En el asistente, ingrese el nombre del nuevo asistente de política RAVPN, seleccione SSL en Protocolos VPN: Agregue los dispositivos de destino, como se muestra en la imagen. Seleccione "Next" una vez completado.

The screenshot shows the 'Remote Access VPN Policy Wizard' with the 'Access & Certificate' step selected. The 'Targeted Devices and Protocols' section contains the following fields and options:

- Name:** A text field containing 'DLO'.
- Description:** An empty text field.
- VPN Protocols:** Radio buttons for 'SSL' (selected) and 'IPsec-IKEv2'.
- Targeted Devices:** Two columns. The 'Available Devices' column has a search bar and a list with 'HA' selected. The 'Selected Devices' column is empty.

On the right, the 'Before You Start' section lists prerequisites for the Authentication Server, Secure Client Package, and Device Interface. At the bottom right, there are 'Cancel', 'Back', and 'Next' buttons, with 'Next' highlighted in red.

Paso 1 del asistente de RAVPN

Paso 2. Para el perfil de conexión, establezca las opciones (que se muestra aquí): Seleccione "Next" una vez completado.

- Nombre del perfil de conexión: Utilice el nombre del grupo de túnel en el paso 5 de "Creación de una Política de Protección de Aplicación".

Autenticación, autorización y contabilidad (AAA):

- método de autenticación: Certificado de cliente y SAML
- Servidor de autenticación:* Seleccione el objeto SSO creado durante "Creación del objeto SSO SAML".

Asignación de dirección de cliente:

- Usar servidor AAA (rango o RADIUS solamente): Radius o LDAP
- Utilizar servidores DHCP: servidor DHCP

- Uso de Pools de Direcciones IP - Pool Local en el FTD

Firewall Management Center
Devices / VPN / Setup Wizard

Overview Analysis Policies **Devices** Objects Integration

Deploy Tcouterie **SECURE**

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 **Secure Client** 4 Access & Certificate 5 Summary

Connection Profile Name: **DUO**

This name is configured as a connection alias, it can be used to connect to the VPN gateway

Authentication, Authorization & Accounting (AAA):

Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method: **Client Certificate & SAML**

Authentication Server: **duosso**

SAML Login Experience: **VPN client embedded browser**

☐ Allow connection only if username from certificate and SAML are the same

☐ Use username from client certificate for authorization

Username From Certificate: ☐ Map specific field ☐ Use entire DN (Distinguished Name) as username

Primary Field: **DN (Distinguished Name) - Common Name**

Secondary Field: **DN (Distinguished Name) - Organization**

Authorization Server: **Realm or RADIUS**

Accounting Server: **RADIUS**

Client Address Assignment:

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

☐ Use AAA Server (Realm or RADIUS only)

☒ **Use DHCP Servers**

Use DHCP Servers: **Tcouterie-SRV**

☐ Use IP Address Pools

Group Policy:

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy: **DefaultPolicy**

[Edit Group Policy](#)

Cancel Back **Next**

Paso 2 del asistente de RAVPN



Consejo: Para este laboratorio, se utiliza un servidor DHCP.

Paso 3. Seleccione "+" para cargar una imagen de implementación web de Cisco Secure Client que se va a implementar. A continuación, seleccione la casilla de verificación de la imagen CSC que se va a implementar. Como se muestra en la imagen. Seleccione "Siguiente" una vez completado.

Firewall Management Center
Devices / VPN / Setup Wizard

Overview Analysis Policies **Devices** Objects Integration

Deploy Tcouterie **SECURE**

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 **Secure Client** 4 Access & Certificate 5 Summary

Remote User Secure Client Internet Outside VPN Device Inside Corporate Resources AAA

Secure Client image

The VPN gateway can automatically download the latest Secure Client package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download Secure Client packages from [Cisco Software Download Center](#).

Secure Client File Object Name	Secure Client Package Name	Operating System
☒ cisco-secure-client-macos-5.0.02075-web...	cisco-secure-client-macos-5.0.02075-web...	Mac OS
☒ cisco-secure-client-win-5.0.02075-web...	cisco-secure-client-win-5.0.02075-web...	Windows

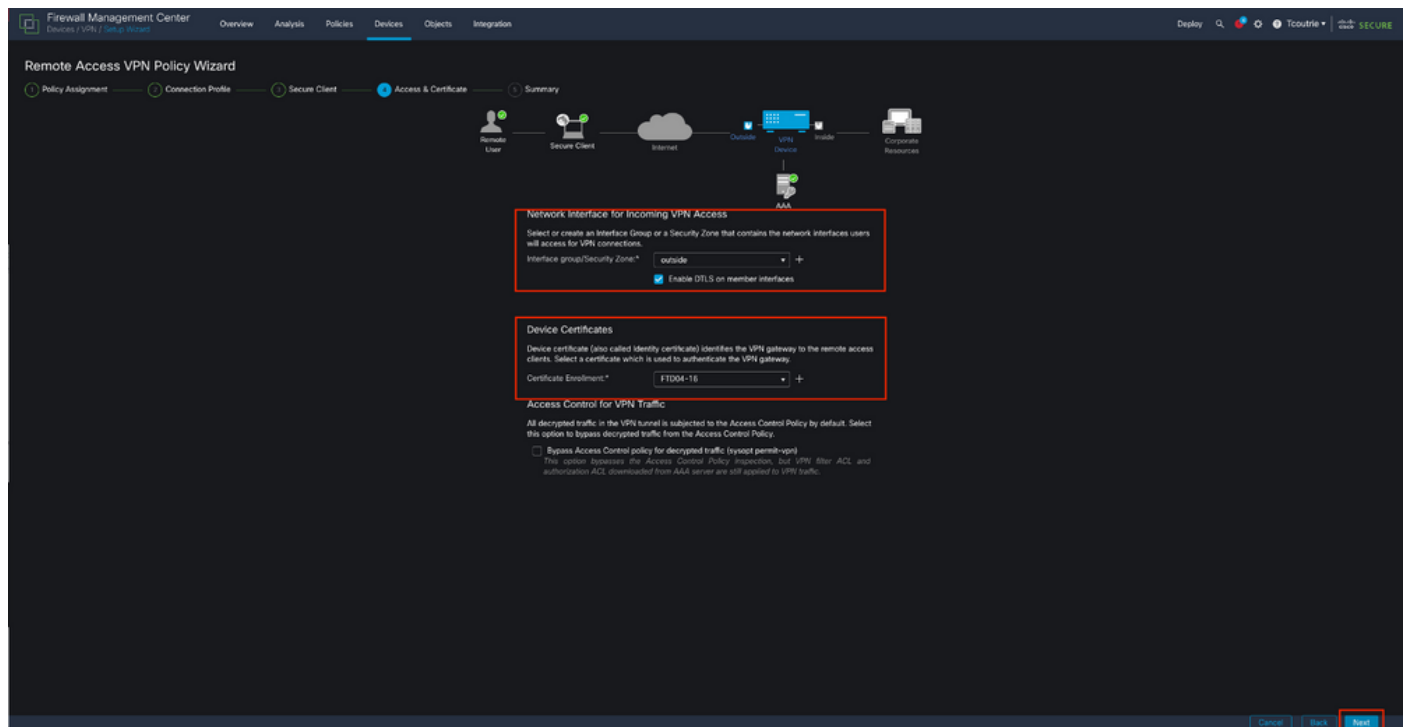
Cancel Back **Next**

Paso 3 Asistente de RAVPN

Paso 4. Establecer estos objetos (como se ve en la imagen): Seleccione "Next" una vez completado.

Grupo de interfaces/Zona de seguridad:* : Interfaz externa

"Inscripción de certificados:*": Certificado de identidad creado durante la sección "Implementación del certificado de identidad en el FTD" de esta guía



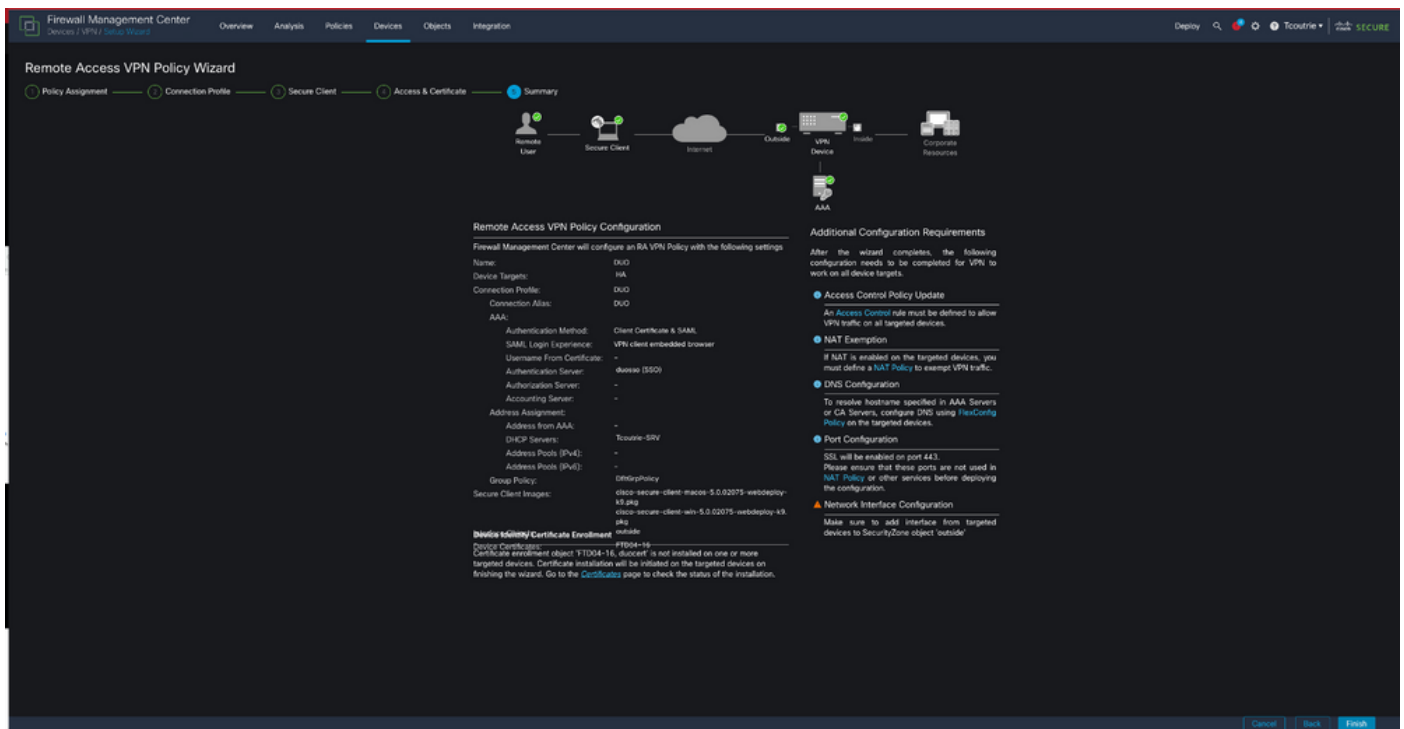
Paso 4 del asistente de RAVPN



Consejo: Si no se ha creado, agregue un nuevo objeto de inscripción de certificados seleccionando "+".

Paso 6. Resumen

Verifique toda la información. Si todo está correcto, continúe con "Finalizar".



página Resumen

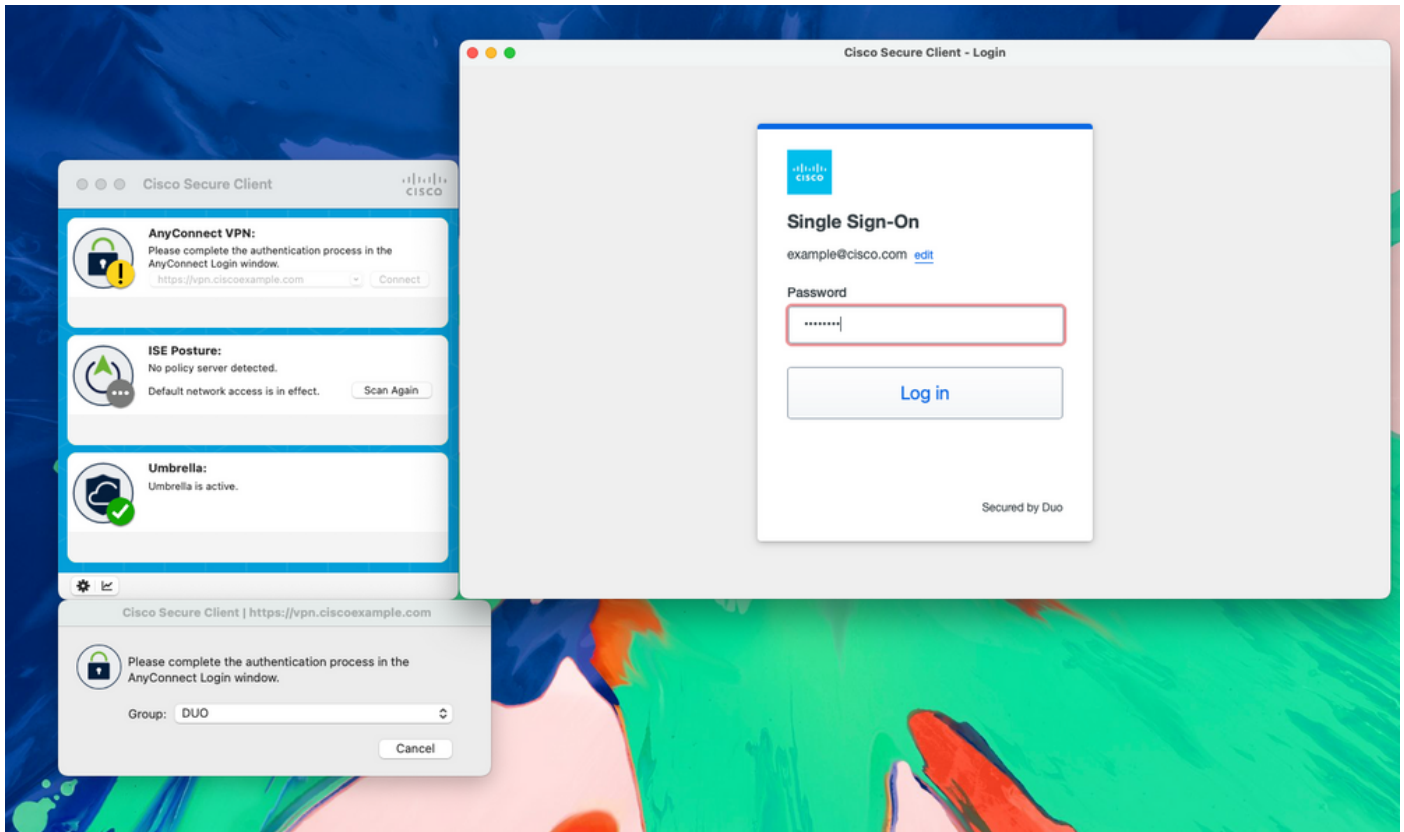
Paso 7. Implemente las configuraciones recién agregadas.

Verificación

En esta sección se describe la verificación de un intento de conexión correcto.

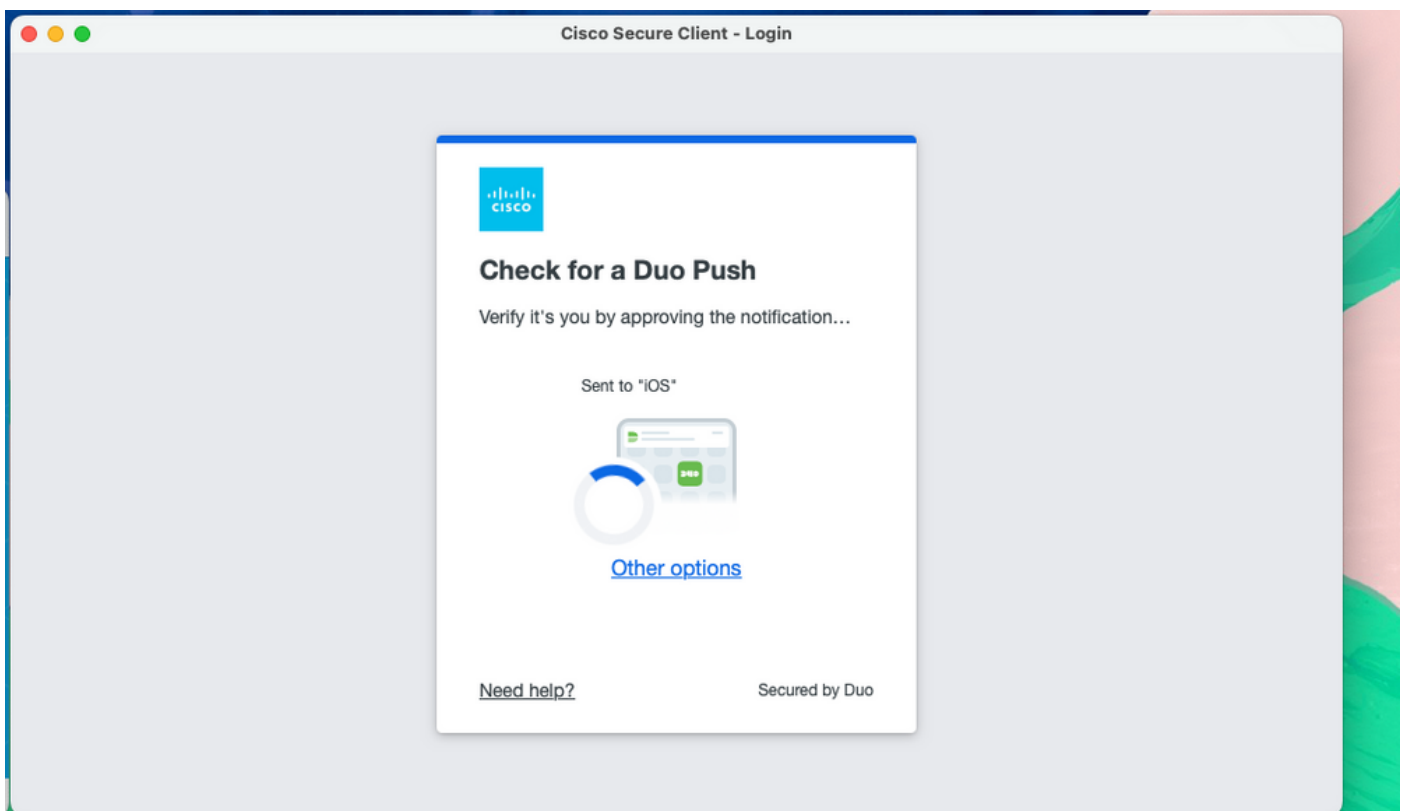
Abra Cisco Secure Client e introduzca el FQDN del FTD y conéctese.

Introduzca las credenciales en la página SSO.



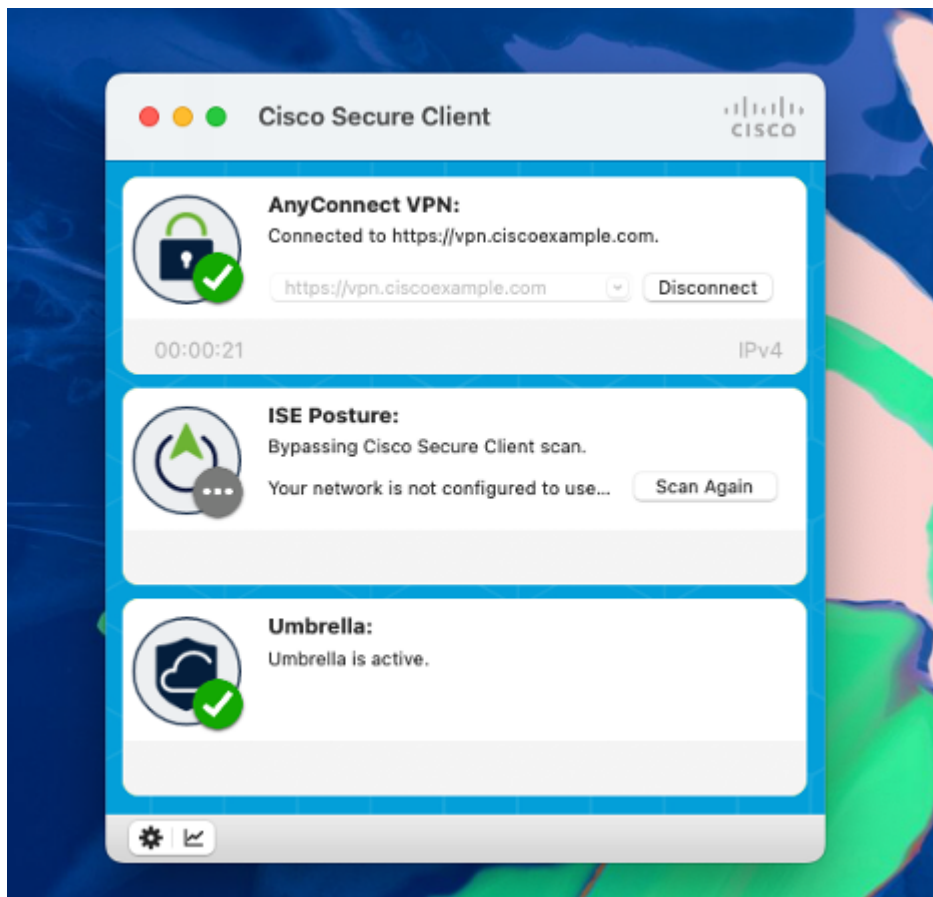
Página de SSO a través de Cisco Secure Client

Acepte la transferencia DUO al dispositivo registrado.



empuje DUO

Conexión correcta.



Conectado a FTD

Verifique la conexión en el FTD con el comando: `show vpn-sessiondb detail anyconnect`

```

tcoutrie-ftd2# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username      :                               Index      : 1916
Assigned IP   :                               Public IP   :
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-128  DTLS-Tunnel:
Hashing       : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA256  DTLS-Tunnel: (1)SH
Bytes Tx      : 390964                        Bytes Rx     : 124114
Pkts Tx       : 1216                          Pkts Rx      : 1223
Pkts Tx Drop  : 0                            Pkts Rx Drop : 0
Group Policy  :                               Tunnel Group :
Login Time    : 23:54:41 UTC Tue Jul 18 2023
Duration      : 0h:11m:28s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                          VLAN         : none
Audt Sess ID  : 0a7aa95d0077c00064b72641
Security Grp  : none                        Tunnel Zone  : 0

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
Tunnel ID     : 1916.1
Public IP     :
Encryption    : none                        Hashing       : none
TCP Src Port  : 53859                      TCP Dst Port  : 443
Auth Mode     : Certificate and SAML
Idle Time Out: 30 Minutes                  Idle TO Left  : 18 Minutes
Client OS     : mac-intel

```

Se ha omitido parte de la información del ejemplo de resultado

Troubleshoot

Estas son posibles cuestiones que surgen después de la aplicación.

Problema 1: Error de autenticación de certificado.

Asegúrese de que el certificado raíz esté instalado en el FTD;

utilice estas depuraciones:

debug crypto ca 14

debug aaa shim 128

debug aaa common 128

problema 2: fallas SAML

Estos debugs se pueden habilitar para resolver problemas:

debug aaa shim 128

debug aaa common 128

debug webvpn anyconnect 128

debug webvpn saml 255

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).