Configuración de SSL Secure Client con autenticación local en FTD

Contenido

Introducción

Este documento describe cómo configurar Cisco Secure Client (incluye Anyconnect) con autenticación local en Cisco FTD administrado por Cisco FMC.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración de SSL Secure Client mediante Firepower Management Center (FMC)
- Configuración de objetos FirePOWER mediante FMC
- Certificados SSL en Firepower

Componentes Utilizados

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

- Cisco Firepower Threat Defense (FTD) versión 7.0.0 (Compilación 94)
- Cisco FMC versión 7.0.0 (Compilación 94)
- Cisco Secure Mobility Client 4.10.01075

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.

Antecedentes

En este ejemplo, se utiliza Secure Sockets Layer (SSL) para crear una red privada virtual (VPN) entre FTD y un cliente Windows 10.

A partir de la versión 7.0.0, el FTD gestionado por FMC admite la autenticación local para Cisco Secure Clients. Esto se puede definir como el método de autenticación principal o como reserva en caso de que el método principal falle. En este ejemplo, la autenticación local se configura como la autenticación primaria.

Antes de esta versión de software, la autenticación local de Cisco Secure Client en FTD solo estaba disponible en Cisco Firepower Device Manager (FDM).

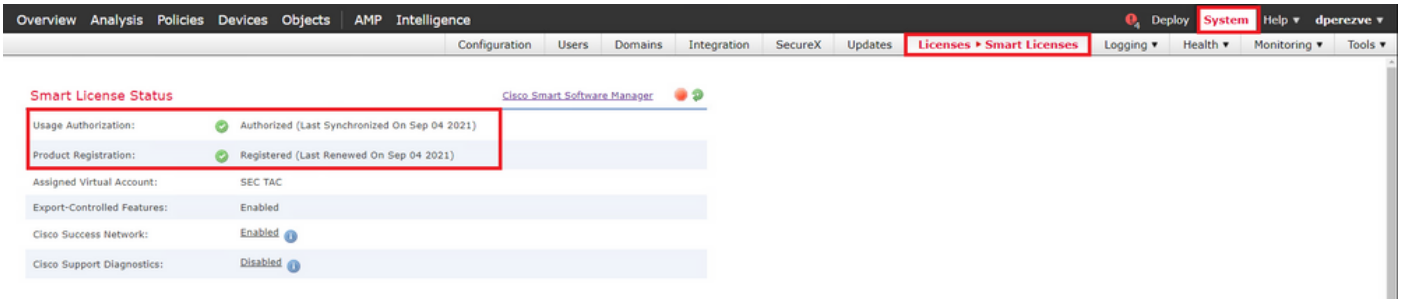
Configurar

Configuraciones

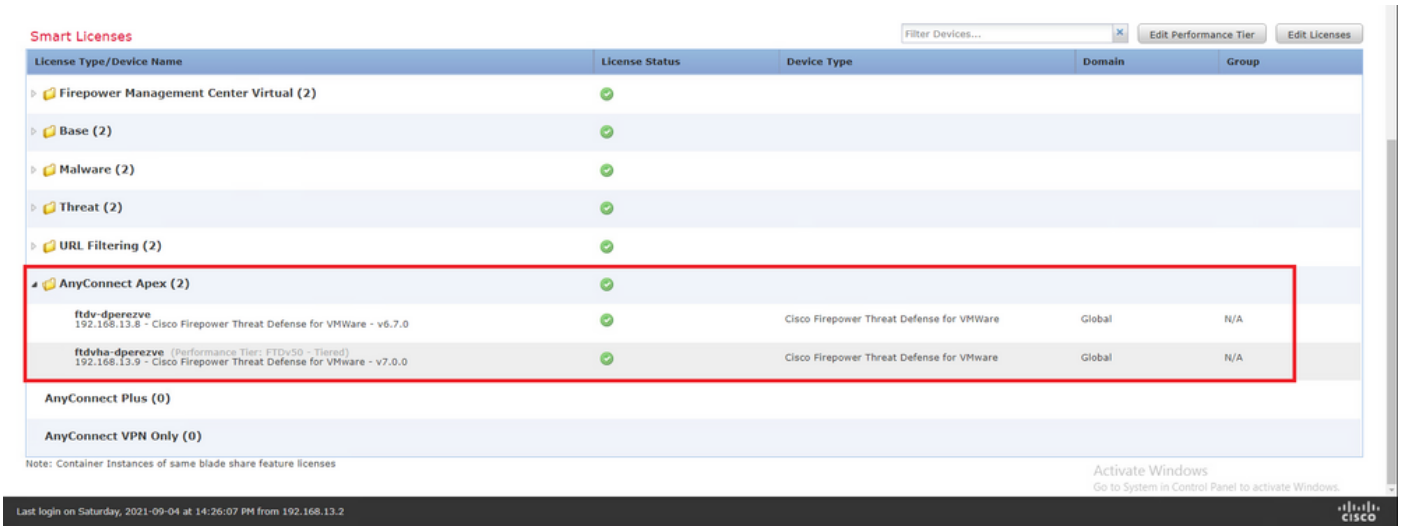
Paso 1. Verificar licencia

Antes de configurar Cisco Secure Client, el FMC debe estar registrado y ser compatible con Smart Licensing Portal. No puede implementar Cisco Secure Client si FTD no tiene una licencia válida Plus, Apex o VPN Only.

Navegue hasta System > Licenses > Smart Licenses para validar que FMC está registrado y cumple con el portal de licencias inteligentes.



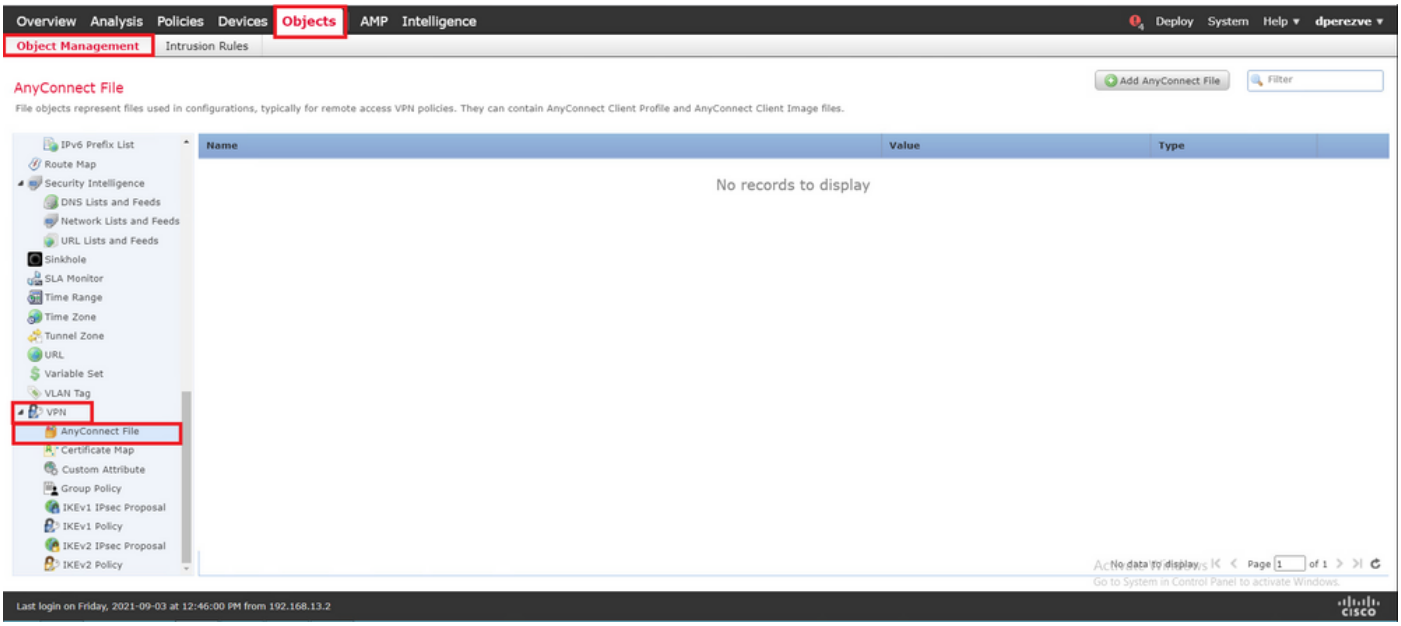
Desplácese hacia abajo en la misma página, en la parte inferior del gráfico Licencias inteligentes puede ver los diferentes tipos de licencias de Cisco Secure Client (AnyConnect) disponibles y los dispositivos suscritos a cada una. Validar que el FTD en cuestión está registrado en cualquiera de estas categorías.



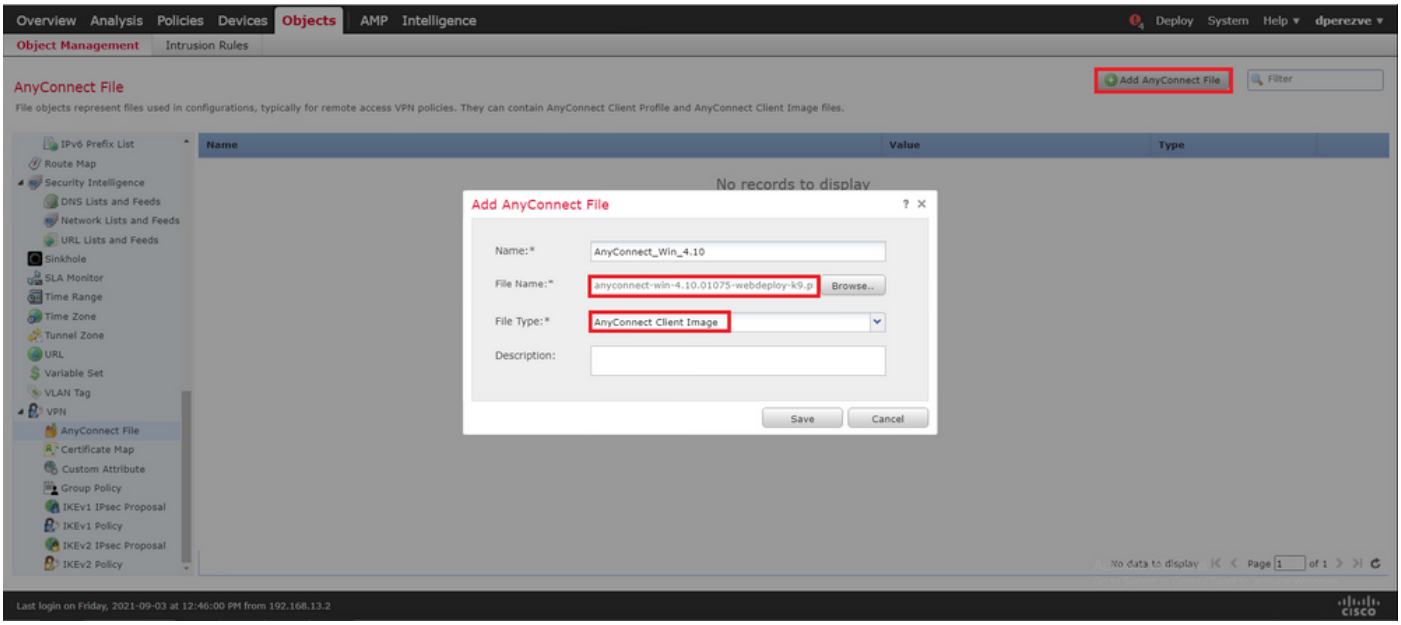
Paso 2. Cargar paquete de Cisco Secure Client en FMC

Descargue el paquete de implementación de cabecera de Cisco Secure Client (AnyConnect) para Windows de cisco.com.

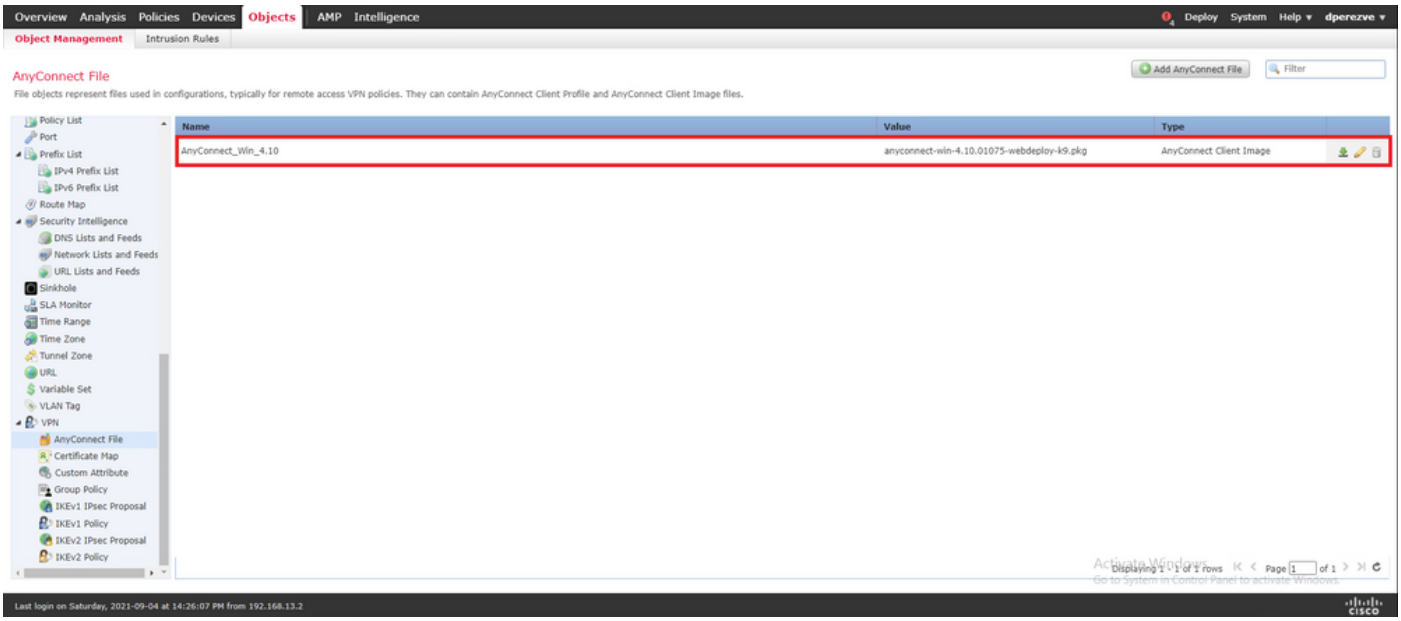
Para cargar la imagen de Cisco Secure Client, navegue hasta Objetos > Administración de objetos y elija Cisco Secure Client File bajo la categoría VPN en la tabla de contenido.



Elija el botón Add AnyConnect File. En la ventana Add AnyConnect Secure Client File, asigne un nombre para el objeto, luego elija Browse.. para elegir el paquete Cisco Secure Client y finalmente elija AnyConnect Client Image como el tipo de archivo en el menú desplegable.



Haga clic en el botón Guardar. El objeto debe agregarse a la lista de objetos.



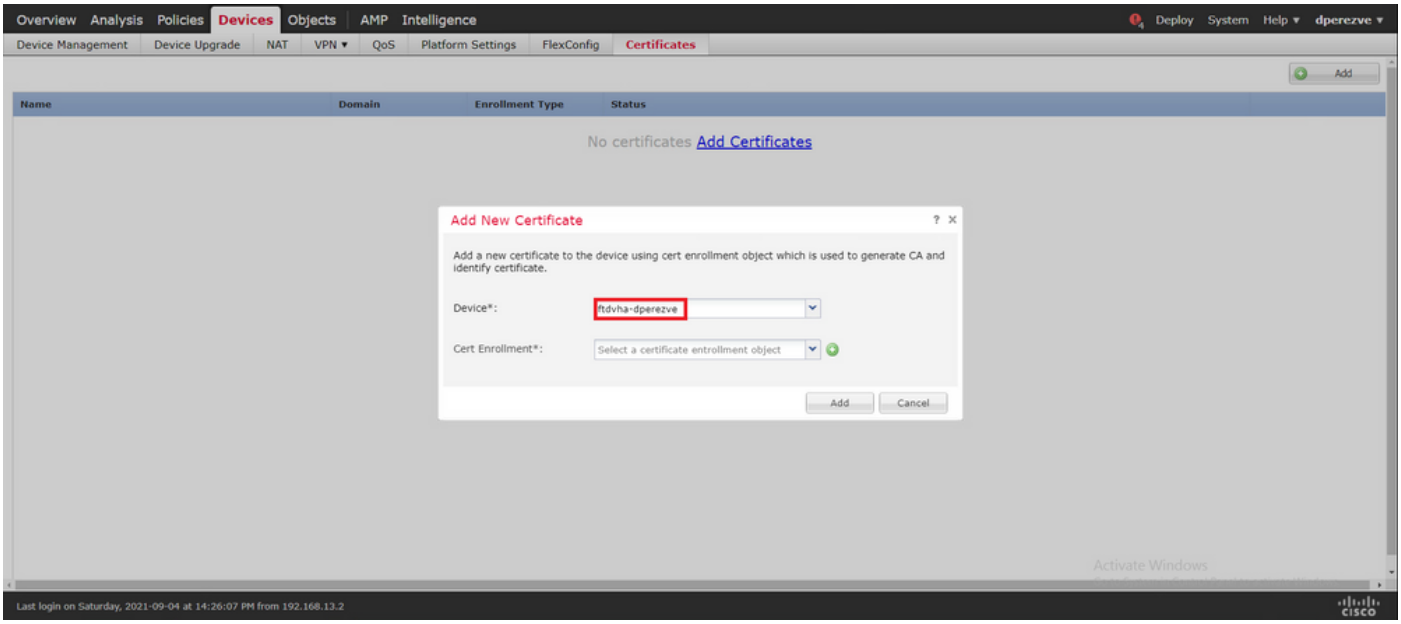
Paso 3. Generar certificado de firma automática

SSL Cisco Secure Client (AnyConnect) requiere un certificado válido para utilizarse en el intercambio de señales SSL entre el centro distribuidor de VPN y el cliente.

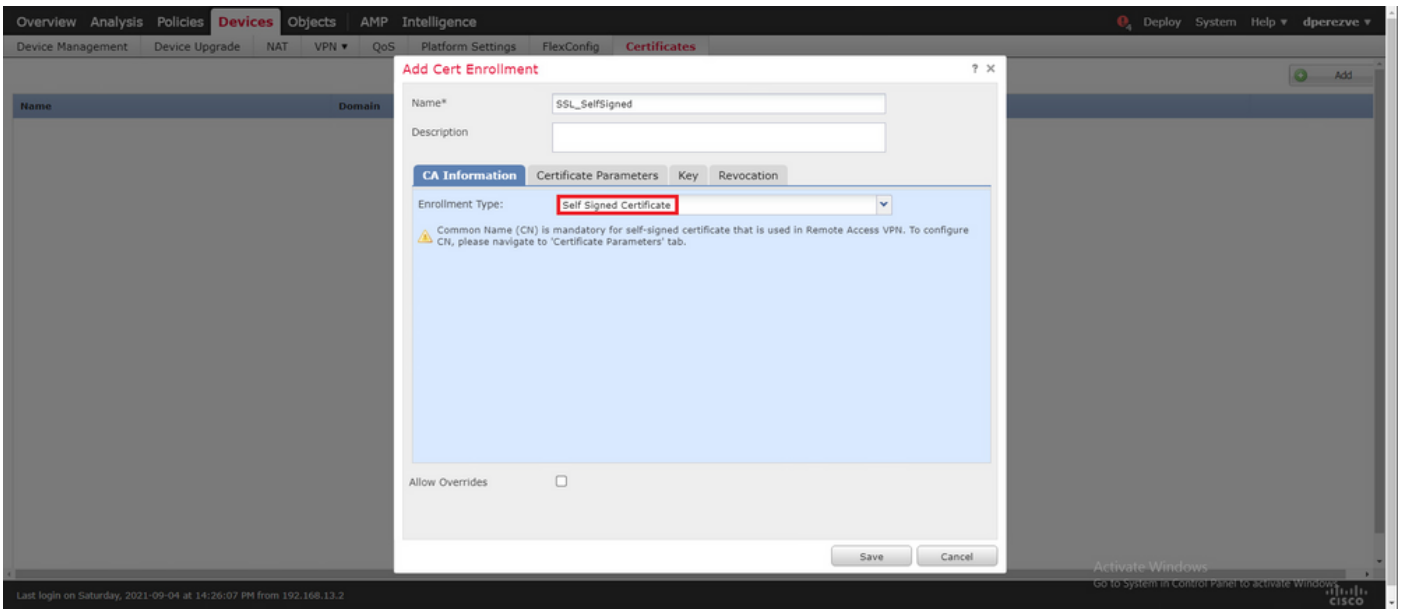
Nota: En este ejemplo, se genera un certificado autofirmado con este fin. Sin embargo, además de los certificados autofirmados, también es posible cargar un certificado firmado por una autoridad de certificación (CA) interna o una CA conocida.

Para crear el certificado autofirmado, navegue hasta Dispositivos > Certificados.

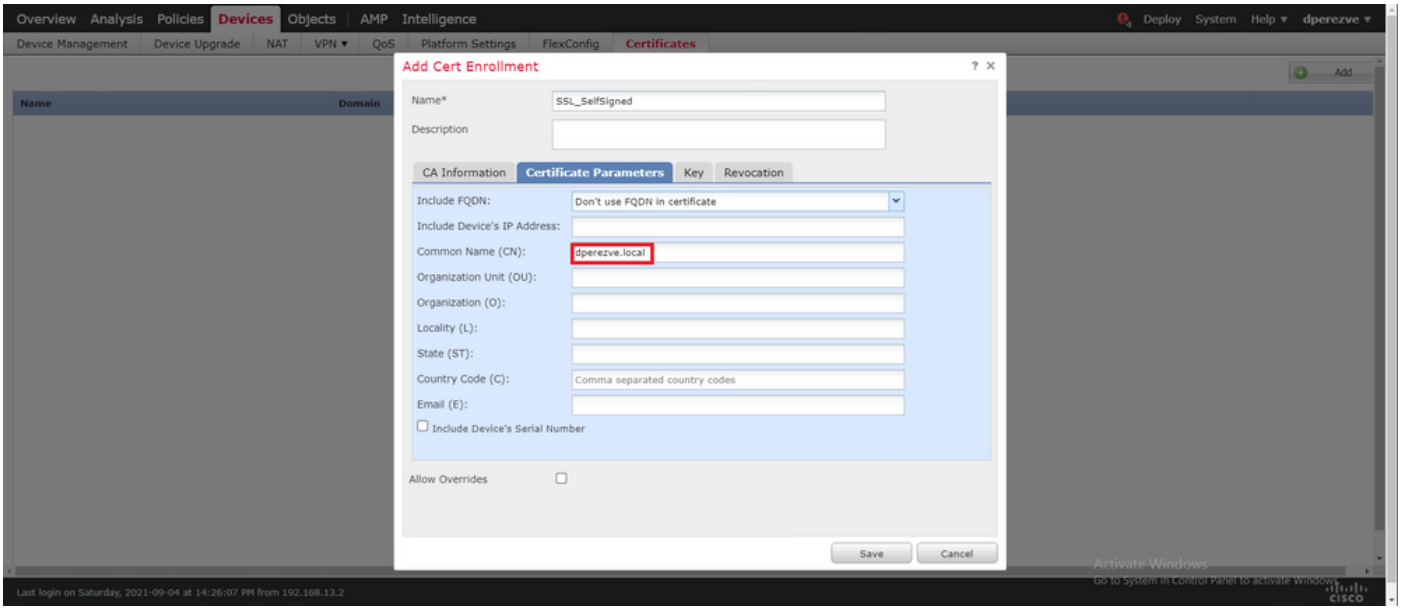
Elija el botón Add. A continuación, seleccione el FTD que desee en el menú desplegable Device de la ventana Add New Certificate.



Elija el botón Add Cert Enrollment (verde + símbolo) para crear un nuevo objeto de inscripción. Ahora, en la ventana Add Cert Enrollment, asigne un nombre para el objeto y elija Self Signed Certificate en el menú desplegable Enrollment Type.



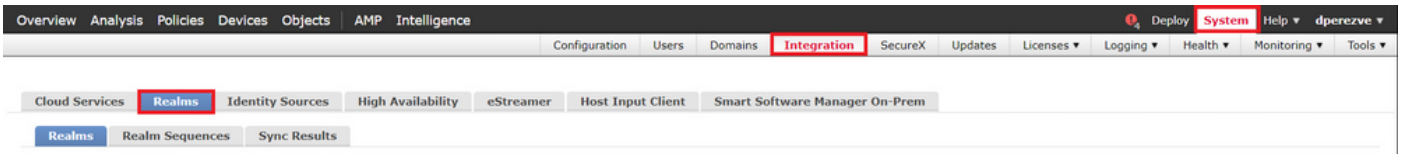
Por último, en el caso de los certificados autofirmados, es obligatorio disponer de un nombre común (NC). Navegue hasta la pestaña Parámetros de Certificado para definir un CN.



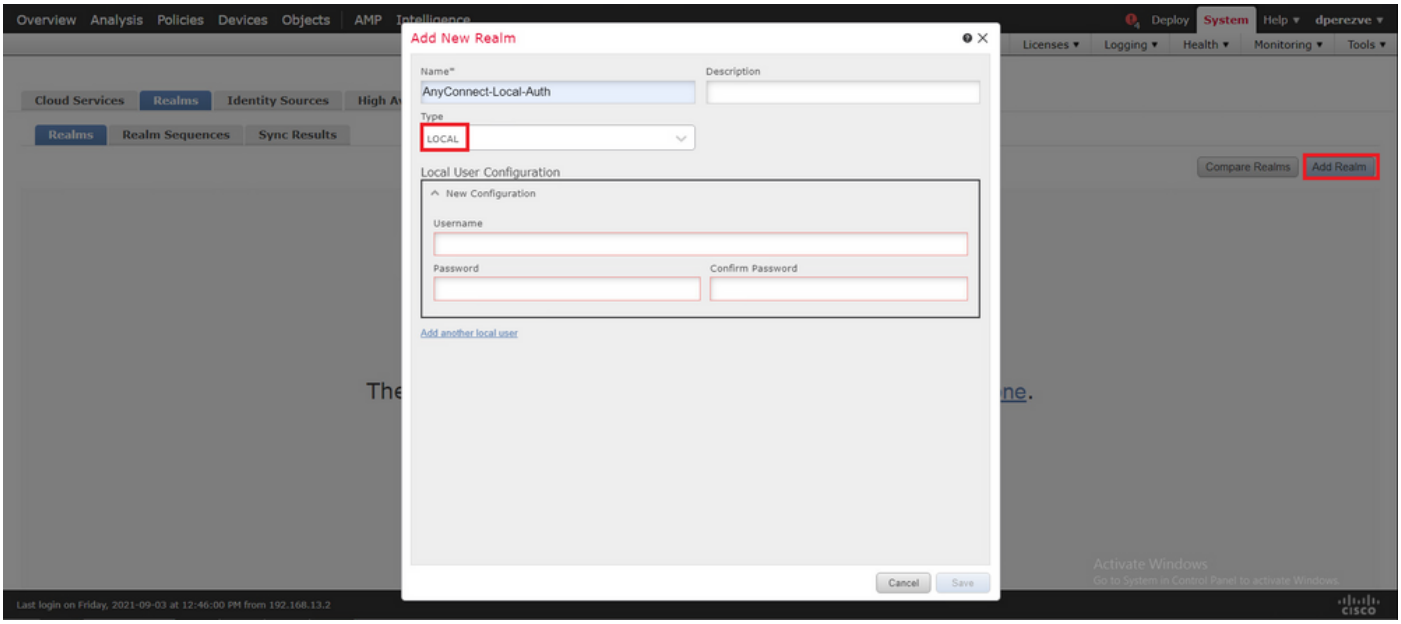
Elija los botones Guardar y Agregar. Después de un par de segundos, el nuevo certificado debe agregarse a la lista de certificados.

Paso 4. Crear rango local en FMC

La base de datos de usuarios locales y las respectivas contraseñas se almacenan en un rango local. Para crear el rango local, navegue hasta System > Integration > Realms.

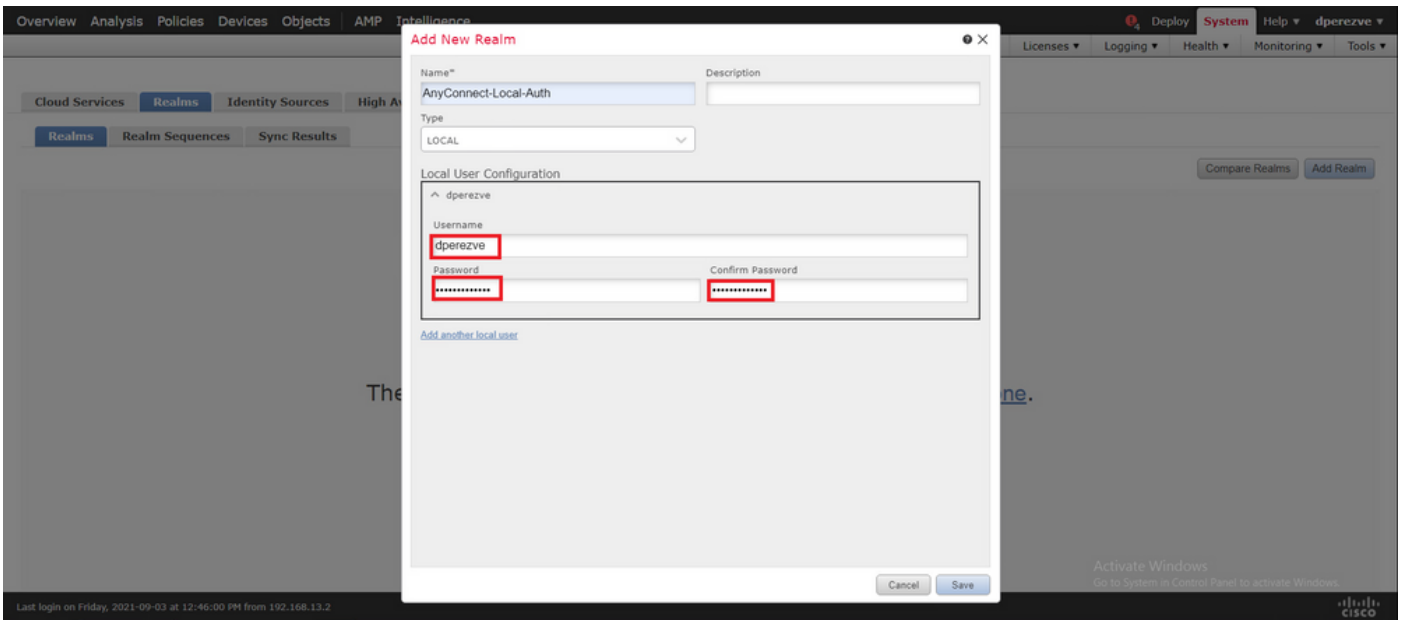


Elija el botón Add Realm. En la ventana Add New Realm, asigne un nombre y elija la opción LOCAL en el menú desplegable Type.

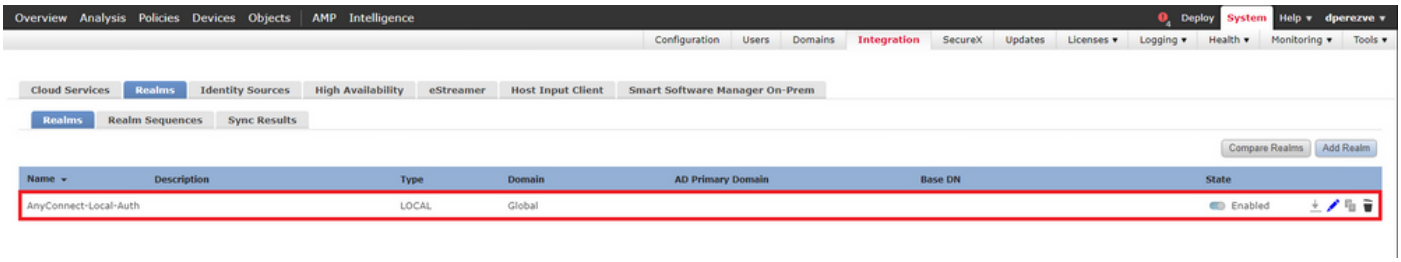


Las cuentas de usuario y las contraseñas se crean en la sección Configuración de usuario local.

Nota: Las contraseñas deben tener al menos una letra mayúscula, una minúscula, un número y un carácter especial.

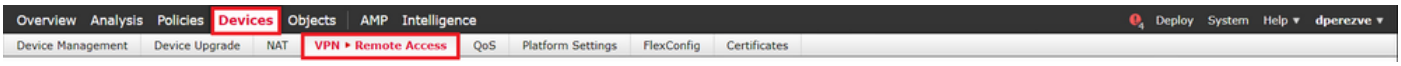


Los cambios guardados y el nuevo rango deben agregarse a la lista de rangos existentes.

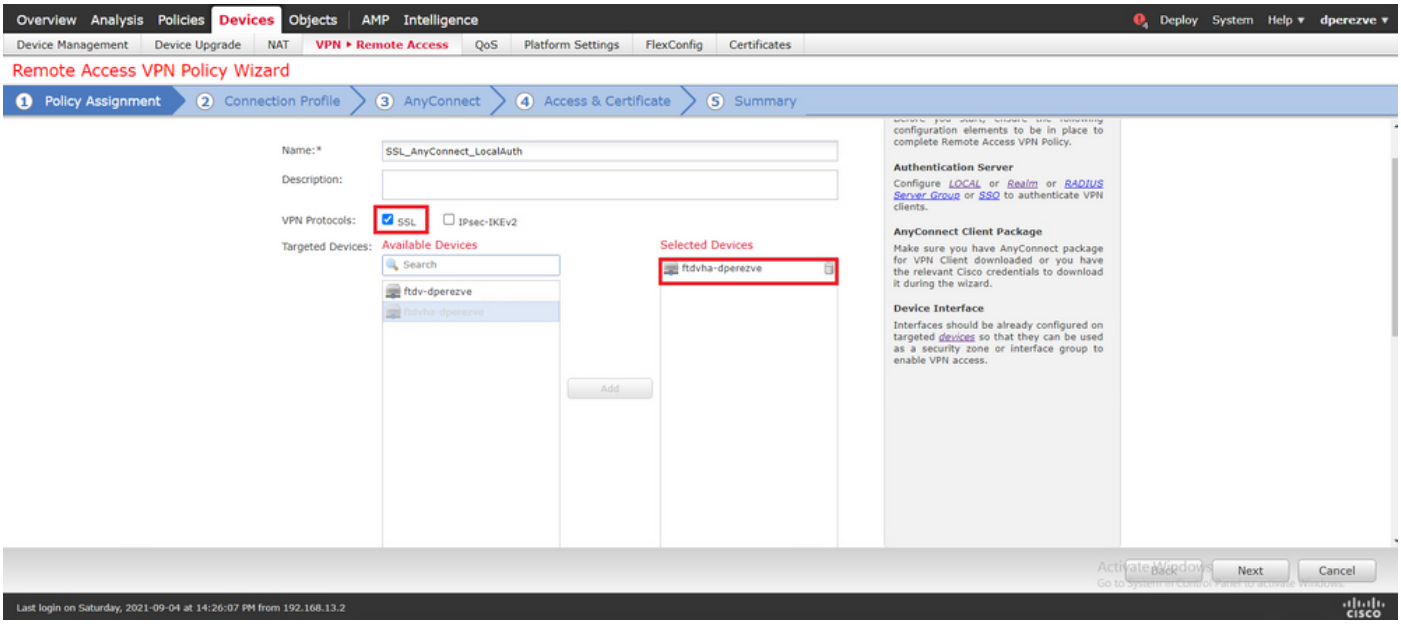


Paso 5. Configuración de Cisco Secure Client SSL

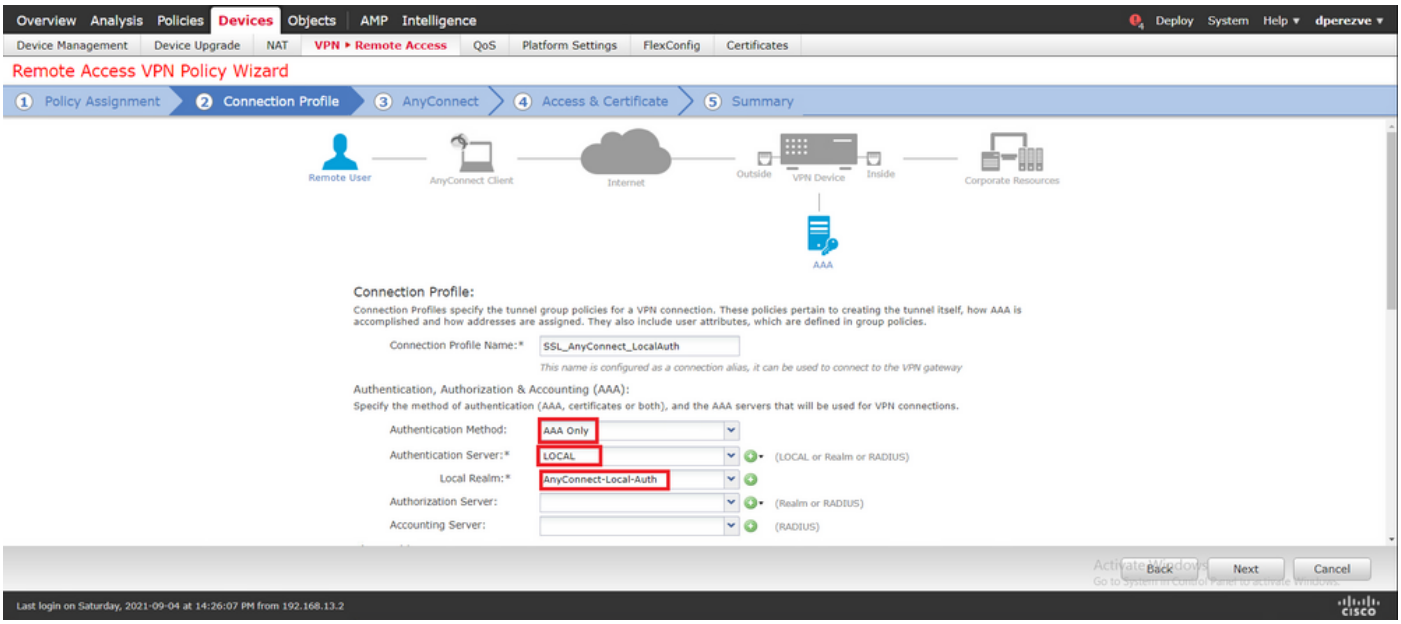
Para configurar SSL Cisco Secure Client, navegue hasta Devices > VPN > Remote Access.



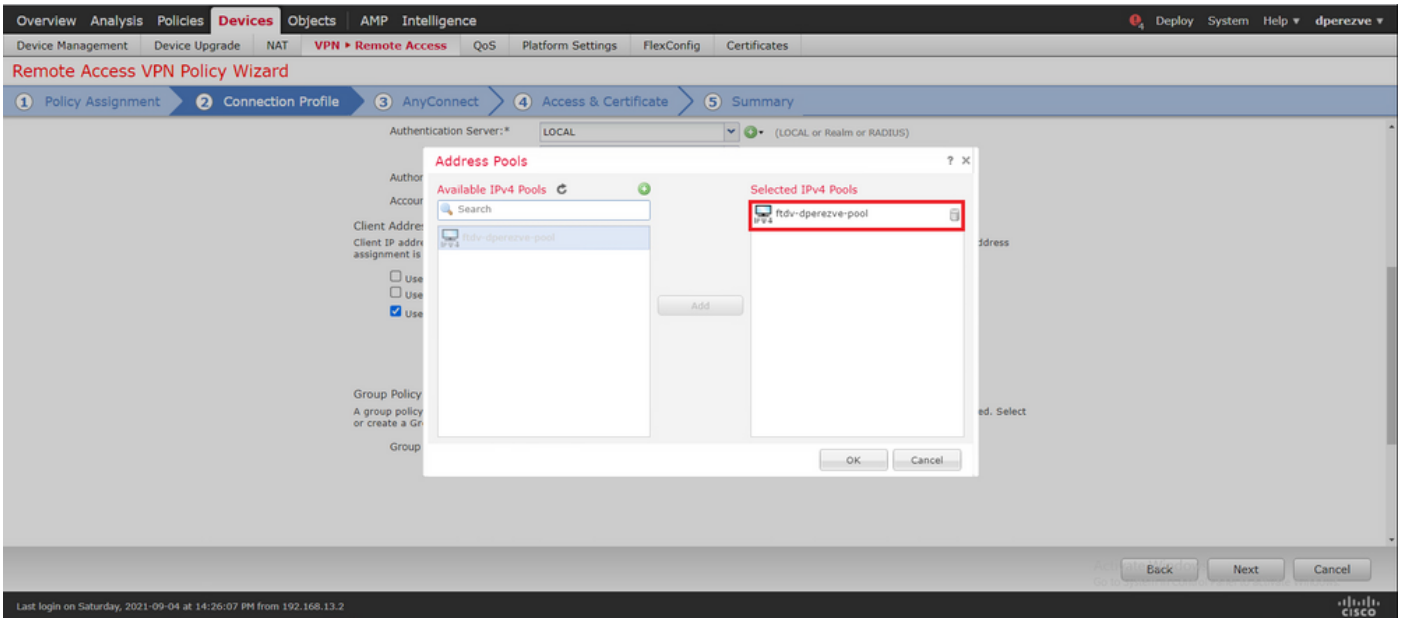
Elija el botón Add para crear una nueva política VPN. Defina un nombre para el perfil de conexión, seleccione la casilla SSL y elija el FTD que desee como dispositivo de destino. Todo debe configurarse en la sección Asignación de políticas del Asistente para políticas VPN de acceso remoto.



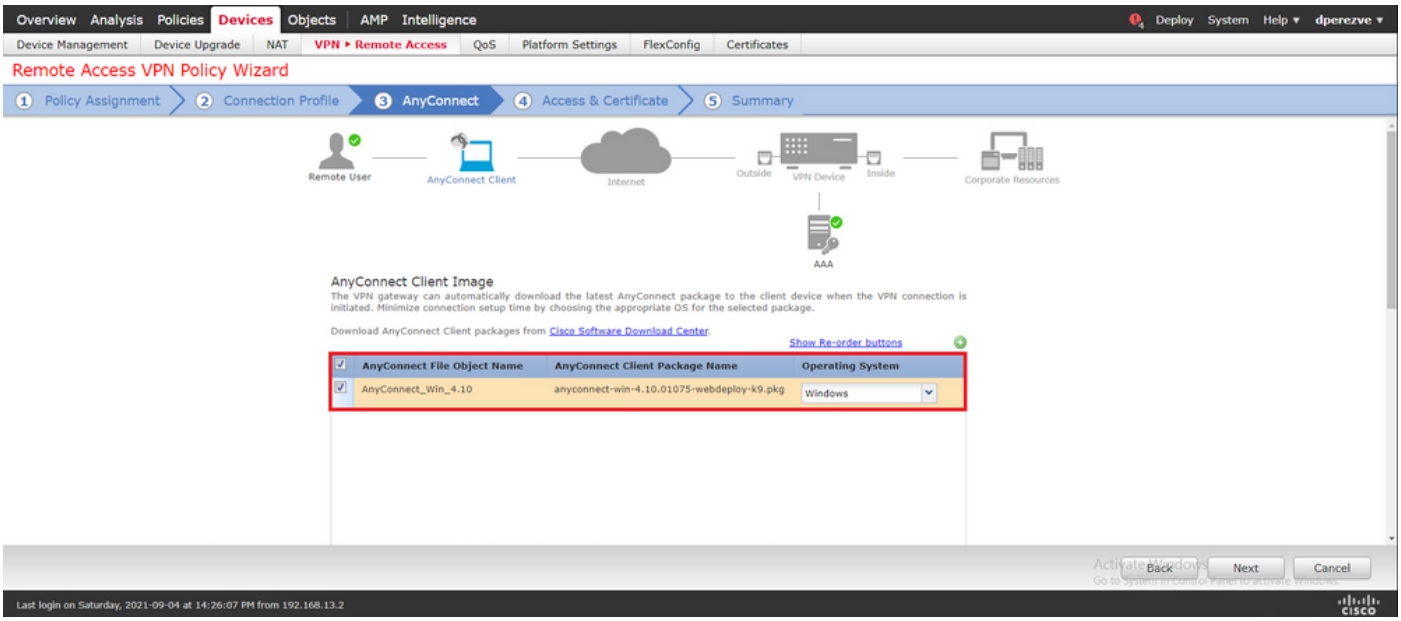
Elija Next para pasar a la configuración del perfil de conexión. Defina un nombre para el perfil de conexión y elija AAA Only como método de autenticación. Luego, en el menú desplegable Authentication Server, elija LOCAL y, finalmente, elija el rango local creado en el Paso 4 del menú desplegable Local Realm.



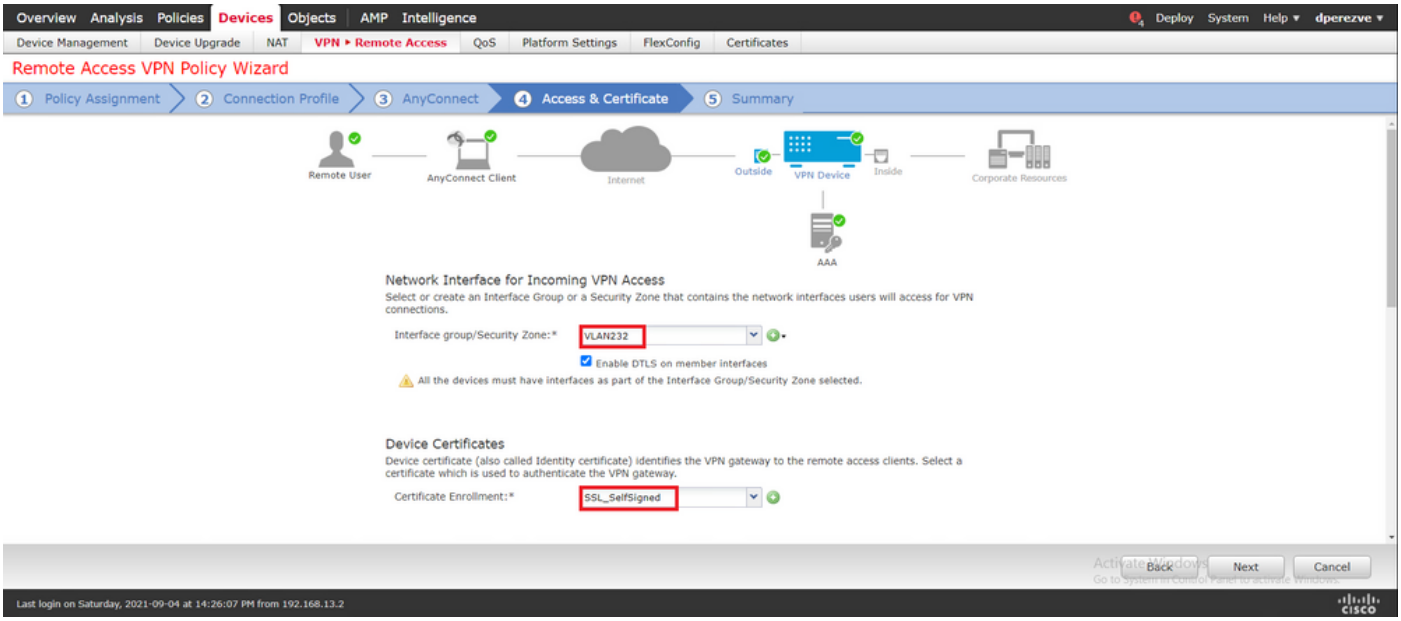
Desplácese hacia abajo en la misma página, luego elija el icono de lápiz en la sección Pool de Direcciones IPv4 para definir el pool IP utilizado por Cisco Secure Clients.



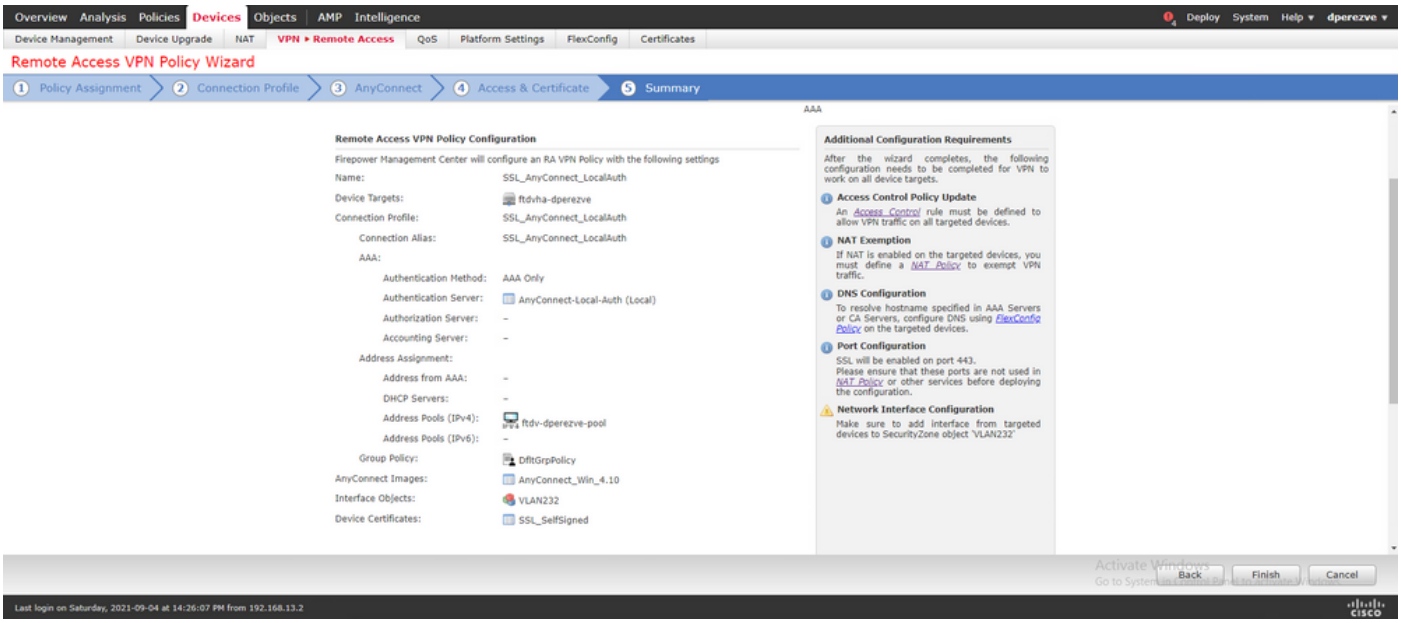
Elija Next para pasar a la sección AnyConnect. Ahora, elija la imagen de Cisco Secure Client cargada en el paso 2.



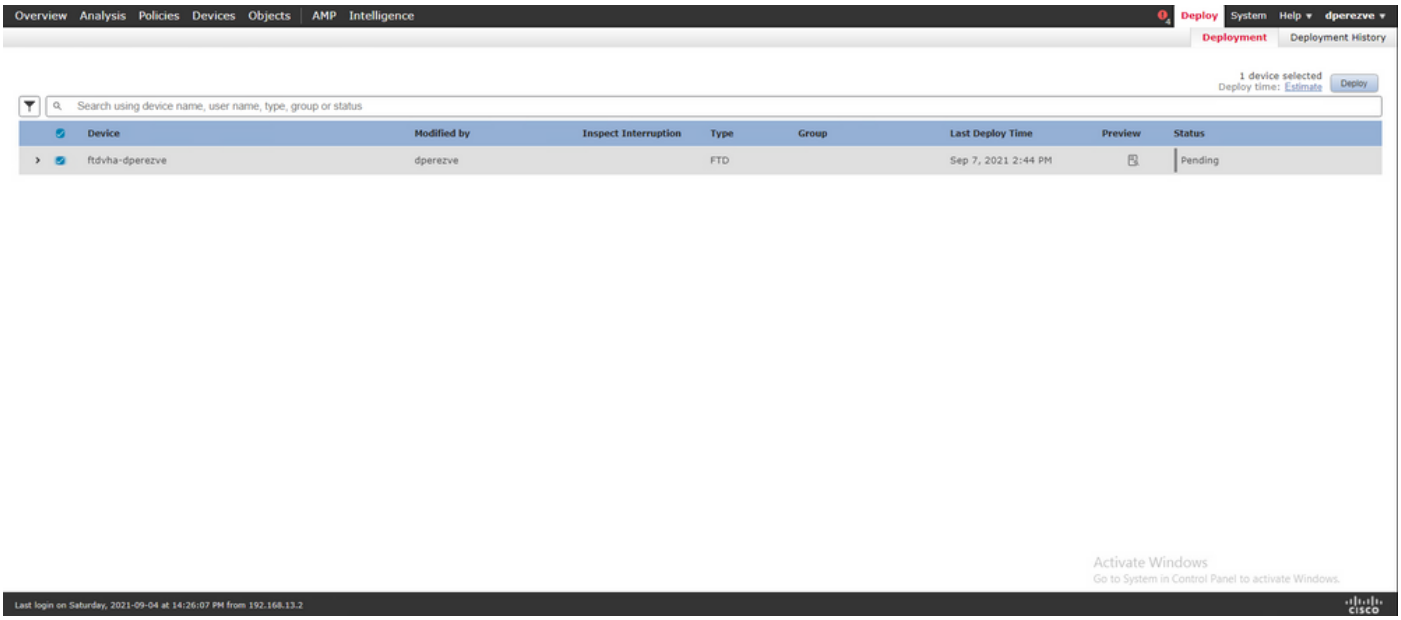
Elija Next para pasar a la sección Access & Certificate. En el menú desplegable Grupo de interfaces/Zona de seguridad, elija la interfaz en la que debe activarse Cisco Secure Client (AnyConnect). A continuación, en el menú desplegable Certificate Enrollment, elija el certificado creado en el paso 3.



Finalmente, elija Next para ver un resumen de la configuración de Cisco Secure Client.

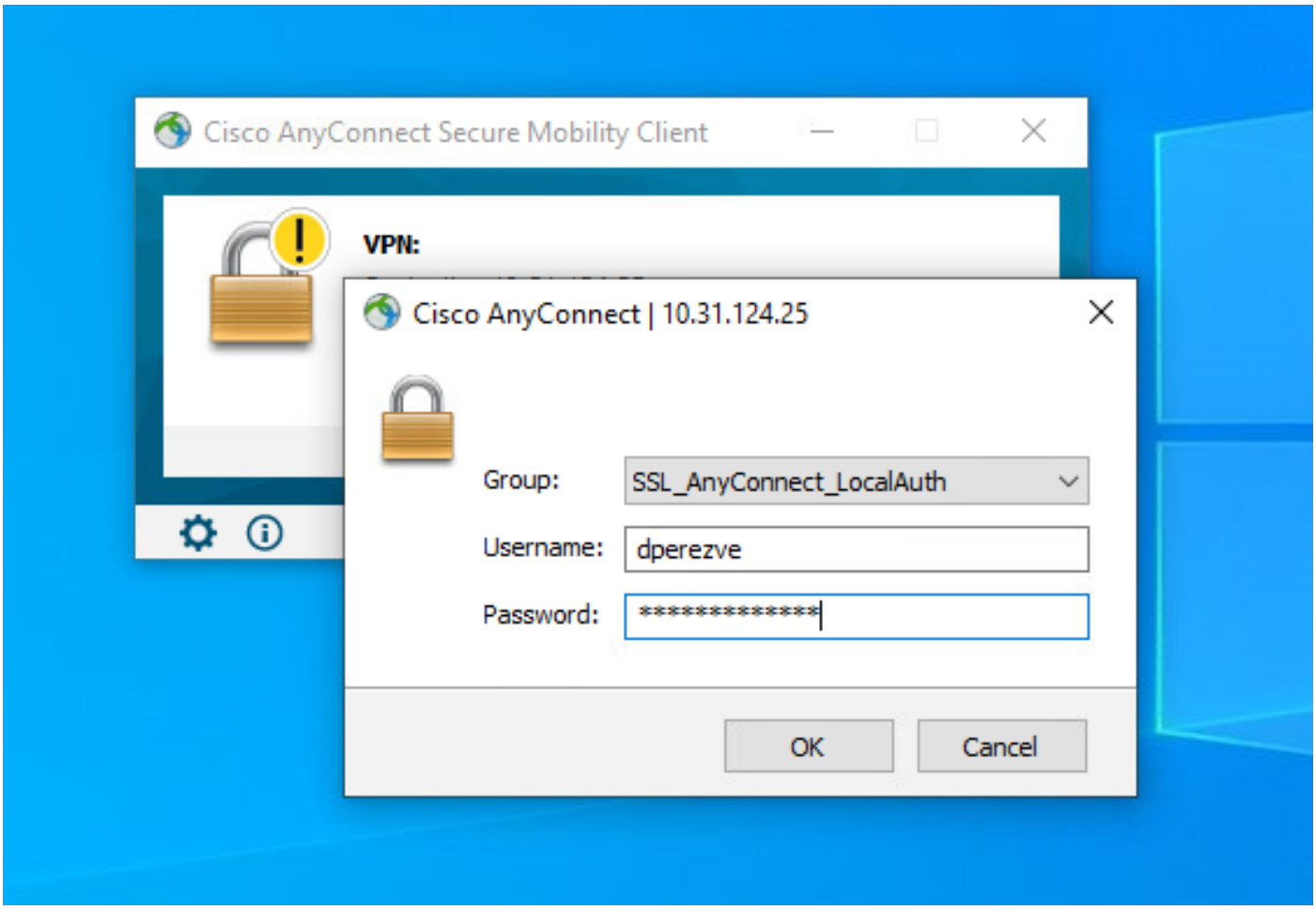


Si todas las configuraciones son correctas, elija Finalizar e implemente los cambios en FTD.

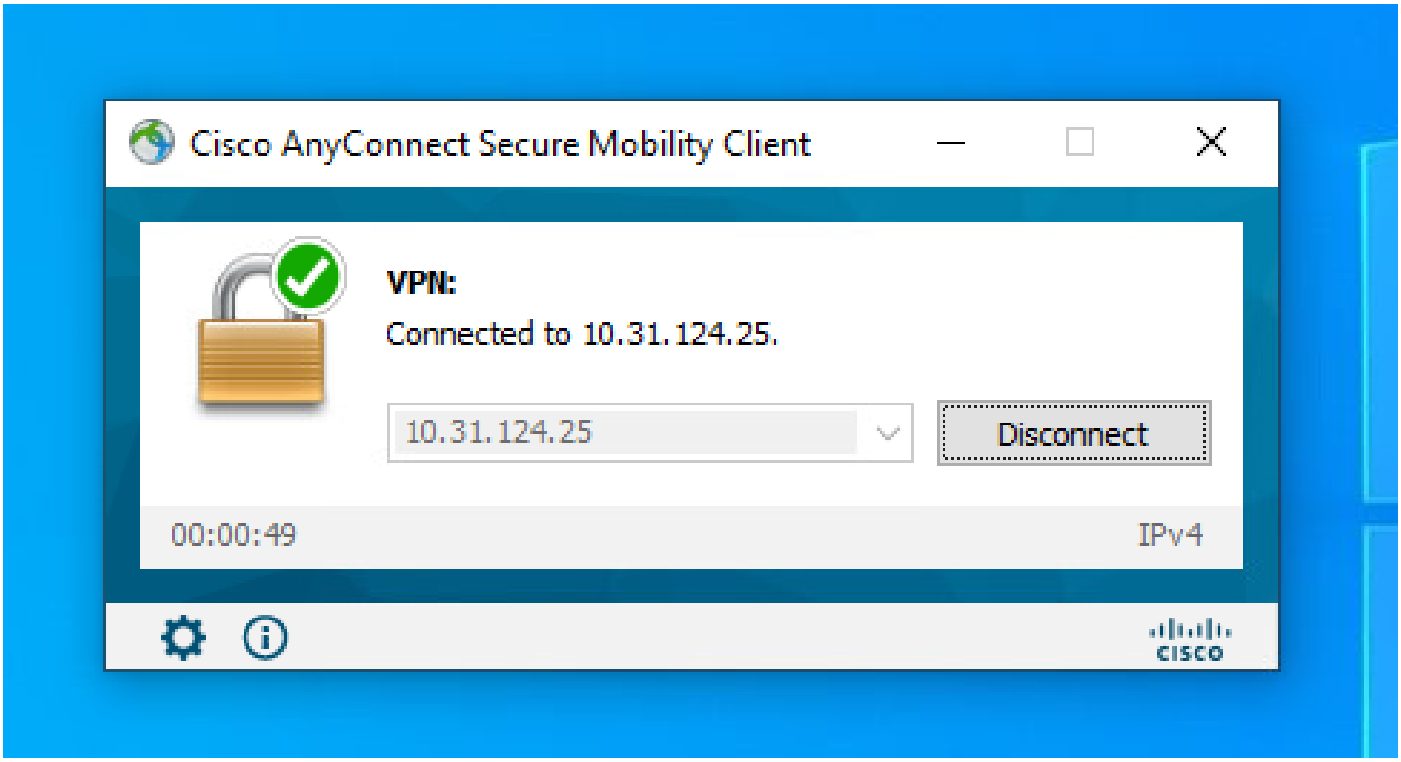


Verificación

Una vez que la implementación se haya realizado correctamente, inicie una conexión de Cisco AnyConnect Secure Mobility Client desde el cliente Windows al FTD. El nombre de usuario y la contraseña utilizados en la solicitud de autenticación deben ser los mismos que los creados en el paso 4.



Una vez que el FTD apruebe las credenciales, la aplicación Cisco AnyConnect Secure Mobility Client debe mostrar el estado de conexión.



Desde FTD puede ejecutar el comando show vpn-sessiondb anyconnect para mostrar las

sesiones de Cisco Secure Client actualmente activas en el Firewall.

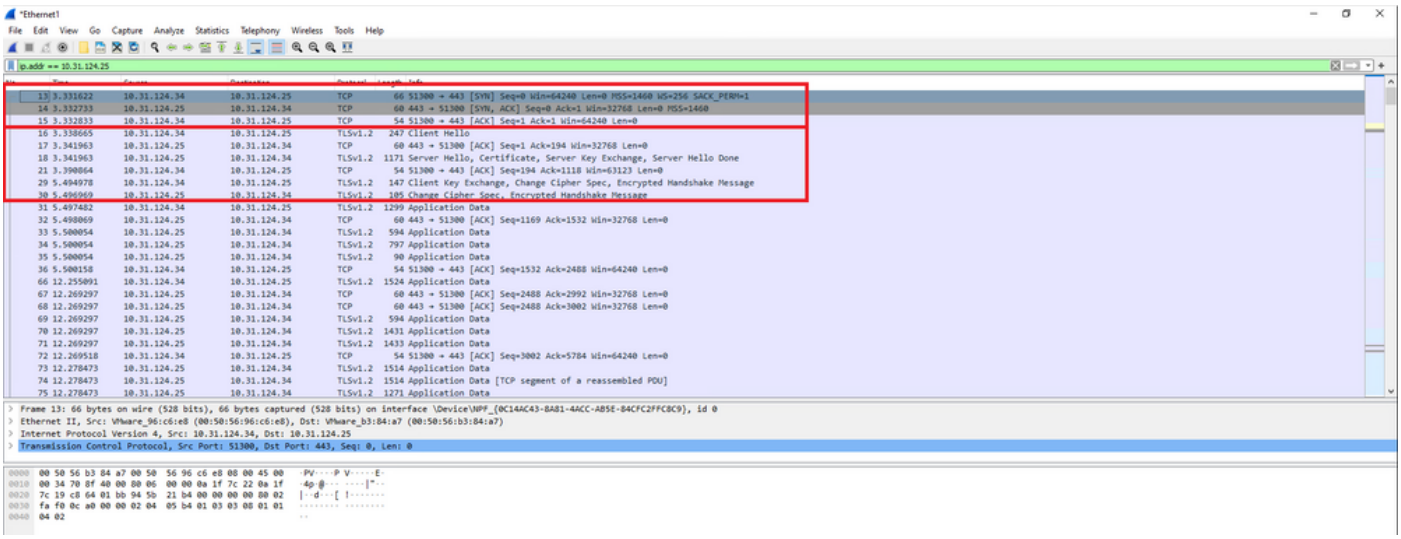
```
firepower# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : dperezve               Index        : 8
Assigned IP  : 172.16.13.1            Public IP    : 10.31.124.34
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES-GCM-256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA384
Bytes Tx     : 15756                  Bytes Rx     : 14606
Group Policy : DfltGrpPolicy
Tunnel Group : SSL_AnyConnect_LocalAuth
Login Time   : 21:42:33 UTC Tue Sep 7 2021
Duration     : 0h:00m:30s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 00000000000080006137dcc9
Security Grp : none                   Tunnel Zone  : 0
```

Troubleshoot

Ejecute el comando debug webvpn anyconnect 255 en FTD para ver el flujo de conexión SSL en FTD.

```
firepower# debug webvpn anyconnect 255
```

Además de las depuraciones de Cisco Secure Client, también se puede observar el flujo de conexión con las capturas de paquetes TCP. Este es un ejemplo de una conexión exitosa, se completa un intercambio regular de tres señales entre el cliente Windows y FTD, seguido por un intercambio de señales SSL usado para acordar cifrados.



Después de los saludos de protocolo, el FTD debe validar las credenciales con la información almacenada en el rango local.

Recopile el paquete DART y póngase en contacto con el TAC de Cisco para obtener más información.

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).

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).

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).