Certificados intermedios y cadena de certificados en switches Catalyst 1200 y 1300

Objetivo

El objetivo de este artículo es revisar la función de certificado intermedio y la cadena de certificados en los switches Catalyst 1200 y 1300 en el firmware 4.1.3.36 y los pasos para configurarlo.

Dispositivos aplicables | Versión de software

- Switches Catalyst 1200 |4.1.3.36
- Switches Catalyst 1300 |4.1.3.36

Introducción

Los certificados se utilizan en una red para proporcionar un acceso seguro. Los certificados pueden ser autofirmados o firmados digitalmente por una autoridad de certificación (CA) externa. Los componentes de una cadena de certificados incluyen:

- Certificado de CA raíz: La CA raíz o certificado de CA se encuentra en la parte superior de la jerarquía de la cadena de certificados y está autofirmado. Es el ancla de confianza definitiva y se utiliza para verificar la autenticidad de los certificados intermedios.
- Certificado(s) intermedio(s): Una CA de nivel superior que sea otra CA intermedia o una CA raíz emite un certificado intermedio. En algunos casos, puede haber varios certificados intermedios formando la cadena de certificados. Normalmente, la CA intermedia es responsable de firmar los certificados de servidor.
- Certificado de servidor: Este certificado se emite para un servidor específico, como un sitio web por ejemplo. Contiene la clave pública del servidor y está firmada por una CA. La CA puede ser una CA raíz o intermedia.

Durante el intercambio de señales SSL/TLS entre el switch (servidor HTTPS) y un navegador (cliente HTTPS), el switch presenta su certificado firmado. El explorador, que tiene el certificado de la CA en su almacén de confianza, utiliza la clave pública de la CA para comprobar la firma en el certificado del servidor. Este proceso establece la autenticidad de la identidad del servidor. Una vez verificados, el servidor y el navegador proceden a intercambiar parámetros criptográficos, lo que permite el cifrado de los datos en tránsito entre ellos y garantiza una conexión segura y autenticada para la transmisión de datos a través de HTTPS.

Aunque los certificados de servidor pueden estar firmados directamente por el

certificado de CA raíz, el uso de certificados intermedios introduce una estructura jerárquica que mejora el proceso de firma. Los certificados intermedios actúan como intermediarios entre el certificado de servidor y la CA raíz, lo que ofrece ventajas como una mayor seguridad mediante el aislamiento de los riesgos clave, la flexibilidad en la administración de certificados y la capacidad de delegar la autoridad de firma. Este enfoque jerárquico proporciona una escalabilidad mejorada, facilita los procesos de renovación de certificados y permite un control más granular de la revocación. Básicamente, el uso de certificados intermedios enriquece el proceso de firma al proporcionar una seguridad mejorada, flexibilidad y una administración de certificados simplificada.

En el firmware 4.1.3.36 de los switches Catalyst 1200 y 1300, ahora puede importar certificados intermedios y ver la cadena de certificados de un certificado de servidor instalado. Los switches Catalyst admiten las siguientes funcionalidades relacionadas con el certificado intermedio y la cadena de certificados del servidor HTTPS:

- Instalación de uno o más certificados intermedios.
- Incluidos los certificados intermedios en el intercambio de señales TLS con el cliente HTTPS
- Visualización de certificados intermedios
- Visualización de la cadena de certificados de los certificados de servidor HTTPS del dispositivo

Siga leyendo para obtener más información.

Table Of Contents

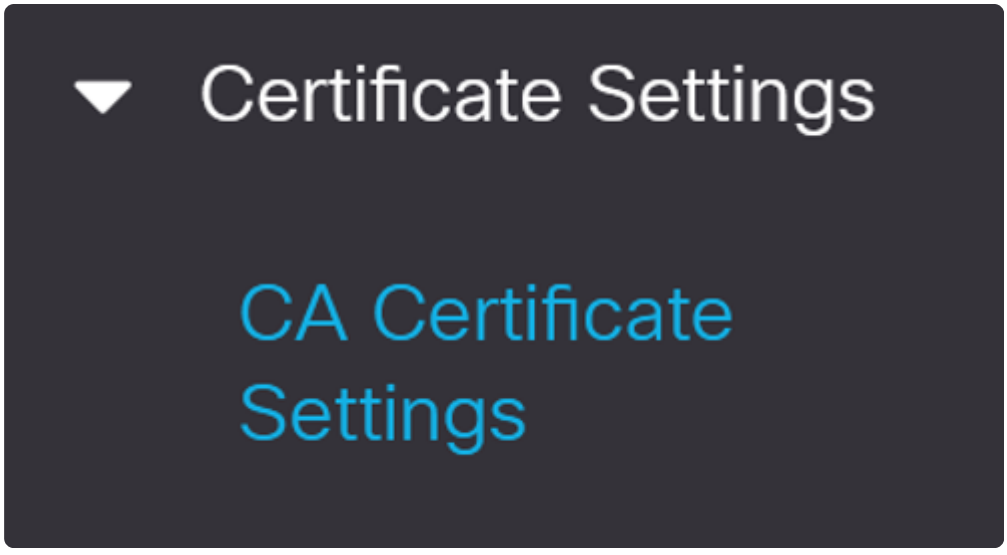
Importación de un Certificado Intermedio

En la versión de firmware 4.1.3.36 de los switches Catalyst 1200 y 1300, tiene la opción de importar certificados intermedios mediante la interfaz de usuario web del switch.

> **Note:**
> En función de la CA, el proveedor de certificados proporcionará el certificado raíz y el certificado intermedio como un paquete para admitir el certificado del servidor.

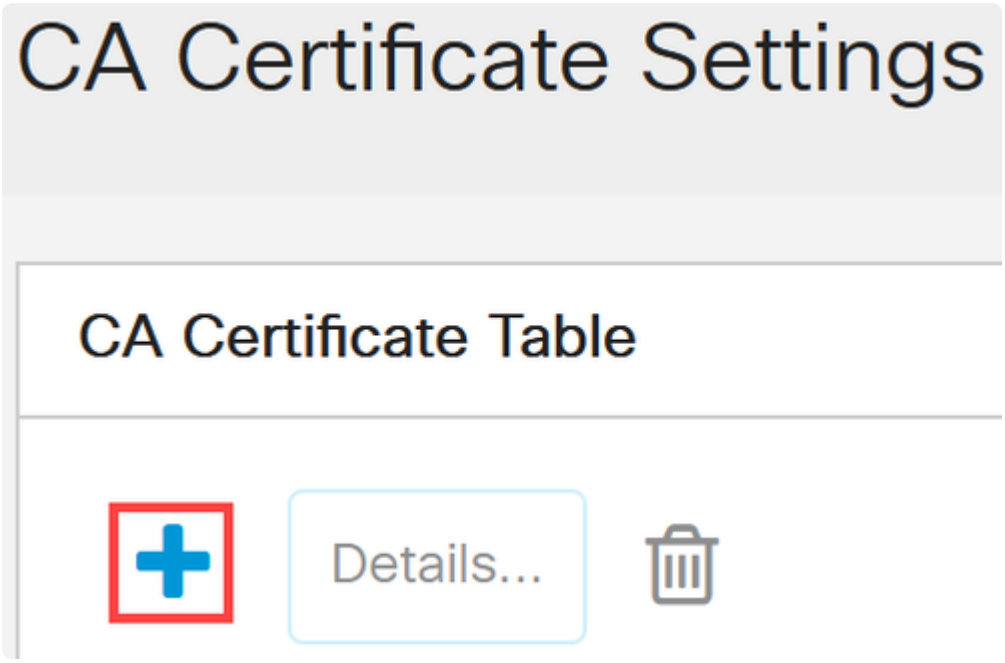
Paso 1

En la vista Avanzada, navegue hasta Seguridad > Configuración de certificado > Configuración de certificado de CA en el panel de navegación.



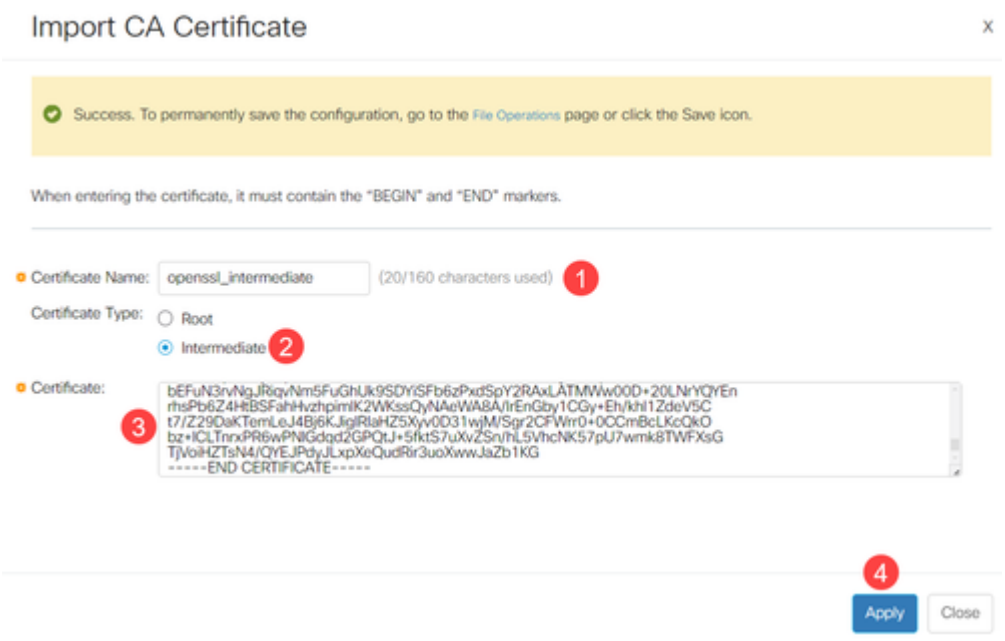
Paso 2

Haga clic en el icono más para importar un certificado.



Paso 3

Ingrese el Nombre del certificado, seleccione Intermedio como el tipo de certificado, pegue el certificado en el cuadro proporcionado y luego haga clic en Aplicar.



En la parte superior de la pantalla aparecerá una notificación de confirmación.

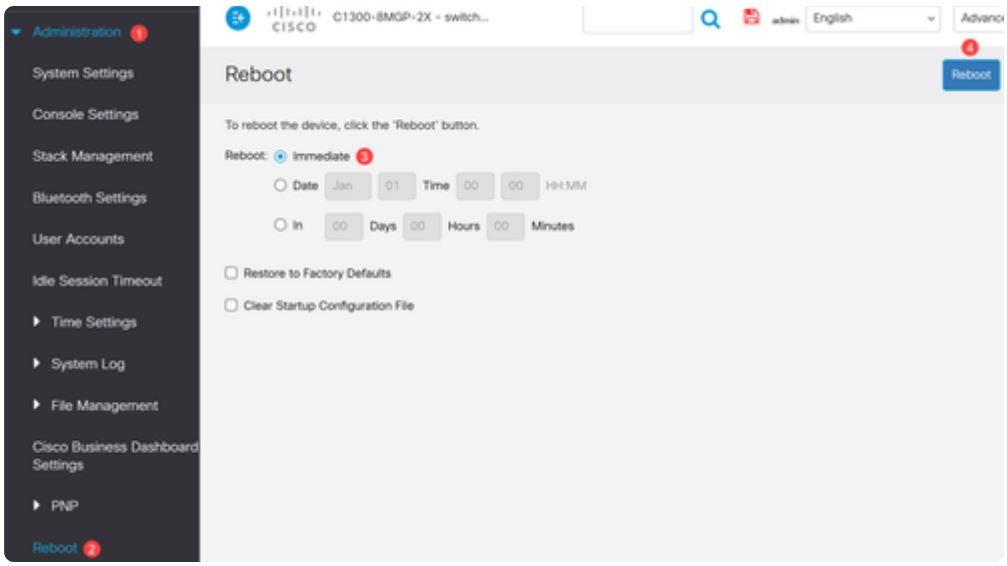
> **Note:**
> Se producirá un mensaje de error si el tipo de certificado no coincide con el certificado que se está instalando.

Paso 4

Haga clic en el icono Save en la parte superior de la pantalla.

Paso 5

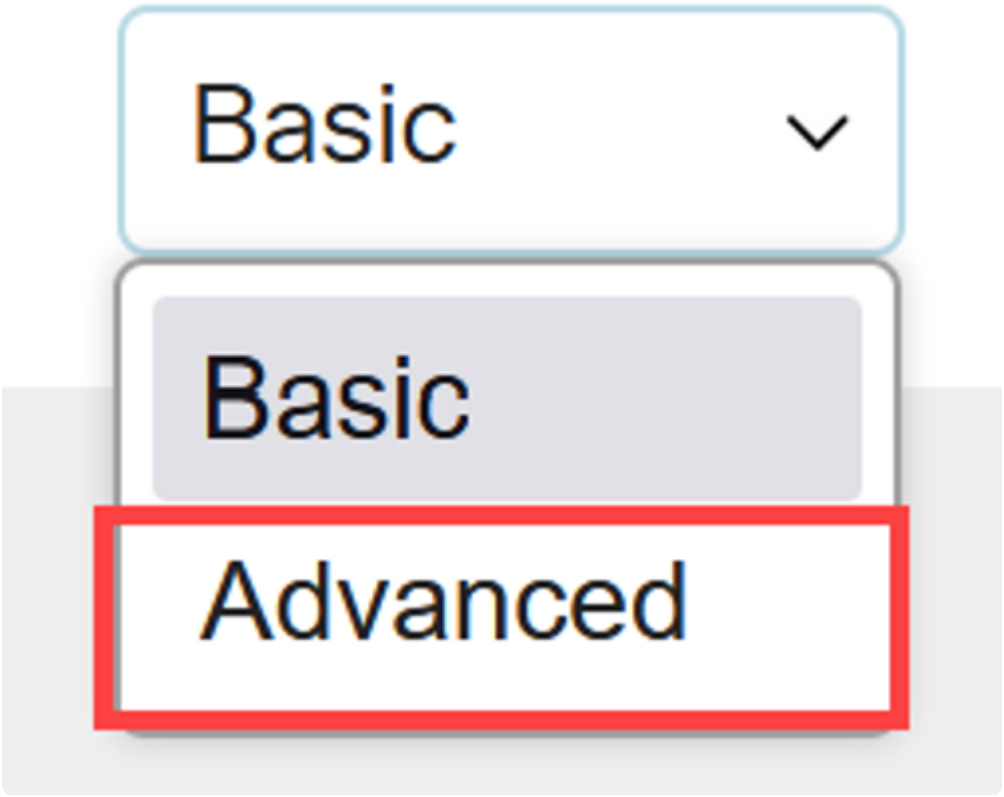
Reinicie el switch para que todos los cambios surtan efecto. Para reiniciar, navegue hasta el menú Administration > Reboot y asegúrese de que la opción Immediate reboot esté seleccionada. Haga clic en el botón Reiniciar.



Cadena de certificados

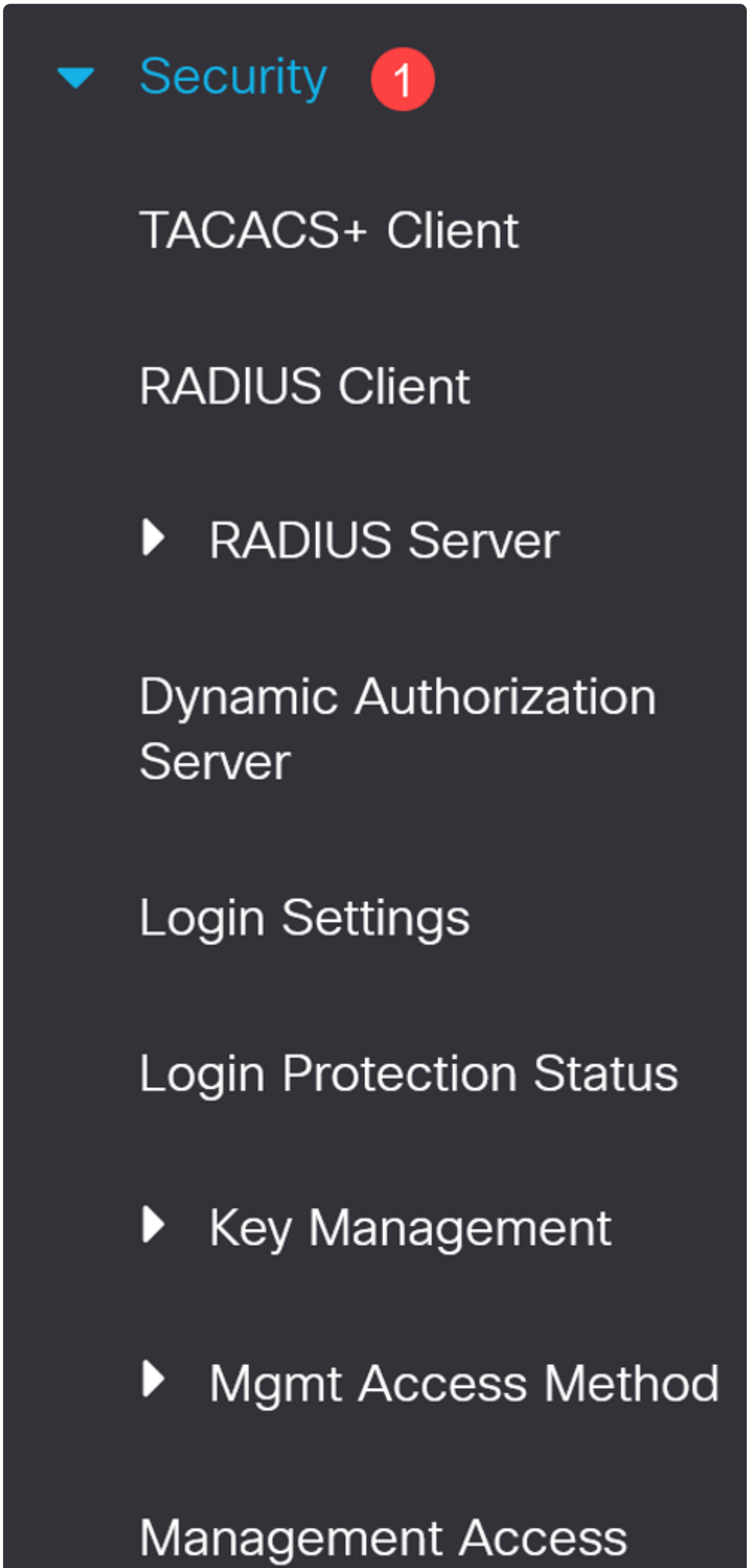
Paso 1

Inicie sesión en el switch Catalyst 1300 y cambie a la vista Avanzada desde el menú desplegable en la esquina superior derecha de la interfaz de usuario.



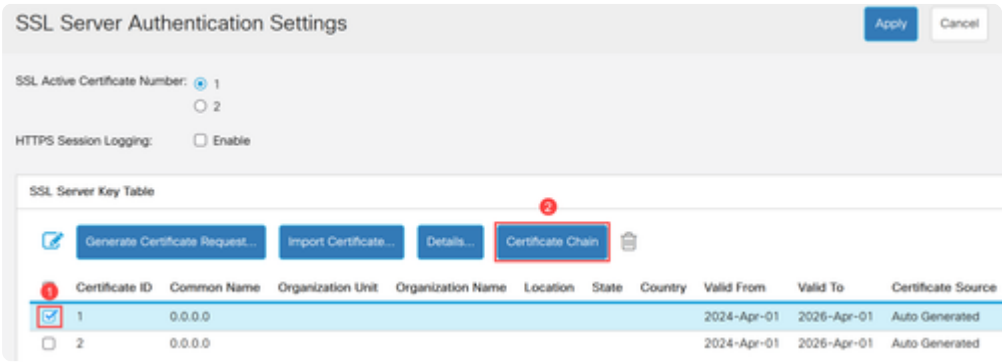
Paso 2

Navegue hasta Seguridad > Servidor SSL > Configuración de autenticación del servidor SSL en el panel de navegación.

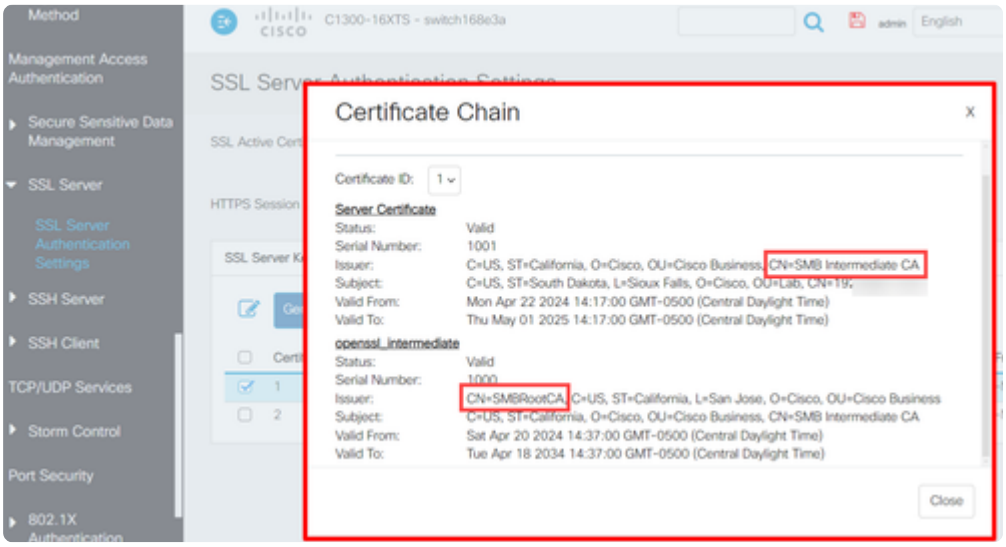

Security
1
TACACS+ Client
RADIUS Client
RADIUS Server
Dynamic Authorization Server
Login Settings
Login Protection Status
Key Management
Mgmt Access Method
Management Access

Paso 3

Seleccione el certificado de la tabla y, a continuación, haga clic en el botón Cadena de certificado.

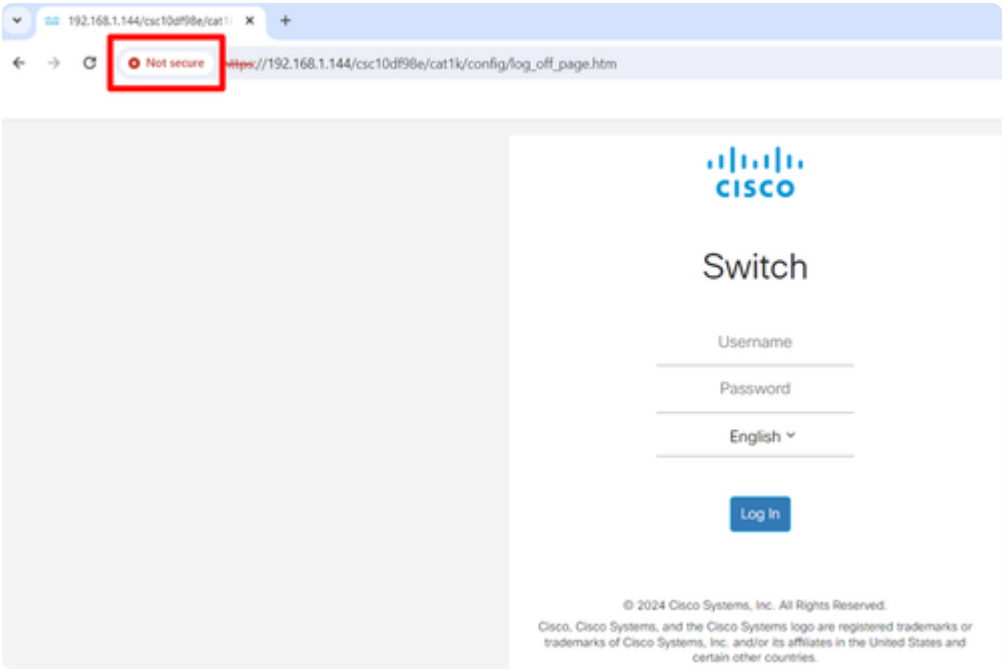


Aparecerá una ventana emergente con los detalles de la cadena de certificados. En este ejemplo, el certificado de servidor estaba firmado por una CA intermedia denominada "SMB Intermediate CA", como indica el nombre común (CN) del emisor en el certificado de servidor. El emisor del certificado intermedio es SMBRootCA.

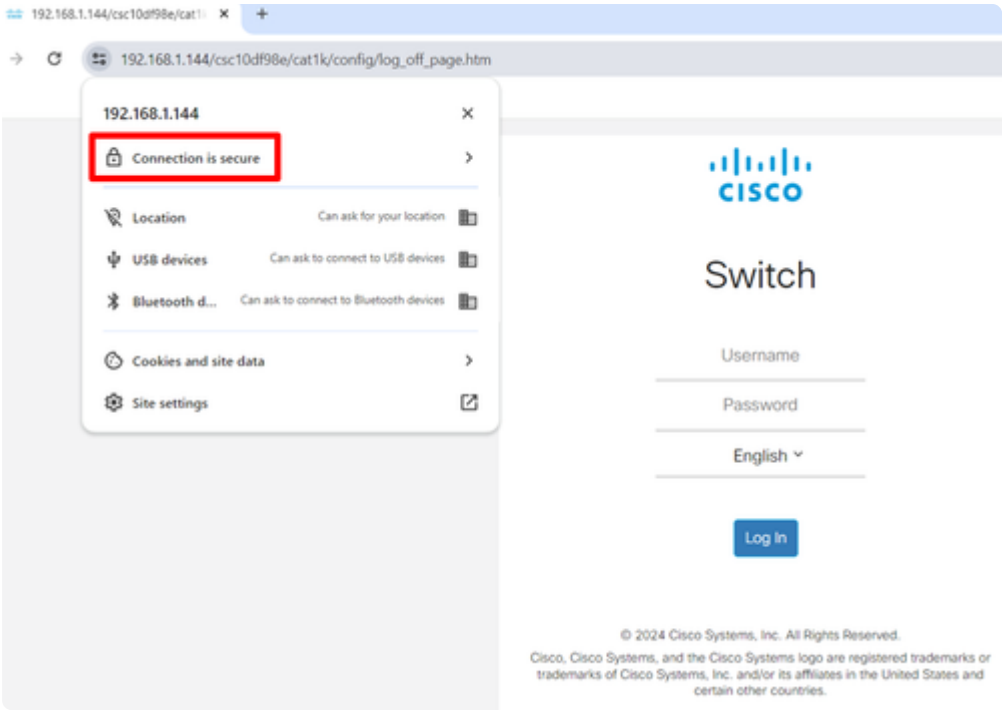


Ejemplo de Cadena de Certificados

Cuando los switches utilizan un certificado autofirmado de forma predeterminada, esto resultará en un sistema cliente, un navegador web en este caso, para mostrar un mensaje de que la conexión es No segura.



Por otro lado, cuando la cadena de certificados se completa con un certificado raíz, un certificado intermedio y un certificado de servidor instalados, el navegador mostrará que la conexión es segura.



Conclusión

¡Ahí tienes! Ahora sabe cómo cargar certificados intermedios y ver la cadena de certificados en los switches Catalyst 1200 y 1300.

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).