Certificados Intermediários e Cadeia de Certificados nos Switches Catalyst 1200 e 1300

Objetivo

O objetivo deste artigo é rever o recurso de certificado intermediário e a cadeia de certificados nos switches Catalyst 1200 e 1300 no firmware 4.1.3.36 e as etapas para configurá-lo.

Dispositivos aplicáveis | Versão do software

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

Introdução

Os certificados são usados em uma rede para fornecer acesso seguro. Os certificados podem ser autoassinados ou assinados digitalmente por uma autoridade de certificação (CA) externa. Os componentes de uma cadeia de certificados incluem:

- Certificado CA raiz: O certificado raiz CA ou CA está no topo da hierarquia da cadeia de certificados e é autoassinado. É a âncora de confiança final e é usada para verificar a autenticidade de certificados intermediários.
- Certificado(s) intermediário(is): Um certificado intermediário é emitido por uma CA de nível superior que é outra CA intermediária ou uma CA raiz. Em alguns casos, pode haver vários certificados intermediários formando a cadeia de certificados. Normalmente, a CA intermediária é responsável pela assinatura dos certificados do servidor.
- Server Certificate: Esse certificado é emitido para um servidor específico, como um site da Web, por exemplo. Ele contém a chave pública do servidor e é assinado por uma CA. A CA pode ser uma CA raiz ou intermediária.

Durante o handshake SSL/TLS entre o switch (servidor HTTPS) e um navegador (cliente HTTPS), o switch apresenta seu certificado assinado. O navegador, com o certificado CA em seu armazenamento confiável, usa a chave pública da CA para verificar a assinatura no certificado do servidor. Esse processo estabelece a autenticidade da identidade do servidor. Uma vez verificados, o servidor e o navegador continuam a trocar parâmetros criptográficos, permitindo a criptografia de dados em trânsito entre eles, garantindo uma conexão segura e autenticada para a transmissão de dados por HTTPS.

Embora os certificados do servidor possam ser assinados diretamente pelo certificado

raiz da CA, o uso de certificados intermediários introduz uma estrutura hierárquica que aprimora o processo de assinatura. Os certificados intermediários atuam como intermediários entre o certificado do servidor e a CA raiz, oferecendo benefícios como maior segurança através do isolamento de comprometimentos de chave, flexibilidade no gerenciamento de certificados e a capacidade de delegar autoridade de assinatura. Essa abordagem hierárquica fornece melhor escalabilidade, facilita os processos de renovação de certificados e permite um controle mais granular sobre a revogação. Essencialmente, o emprego de certificados intermediários enriquece o processo de assinatura, fornecendo segurança avançada, flexibilidade e gerenciamento de certificados simplificado.

No firmware 4.1.3.36 dos switches Catalyst 1200 e 1300, agora você pode importar certificados intermediários e exibir a cadeia de certificados de um certificado de servidor instalado. Os switches Catalyst suportam as seguintes funcionalidades relacionadas ao certificado intermediário e à cadeia de certificados do servidor HTTPS:

- Instalação de um ou mais certificados intermédios.
- Incluindo o(s) certificado(s) intermediário(is) no handshake TLS com o cliente HTTPS
- Apresentação dos certificados intermédios
- Exibição da cadeia de certificados dos certificados do servidor HTTPS do dispositivo

Continue lendo para saber mais!

Table Of Contents

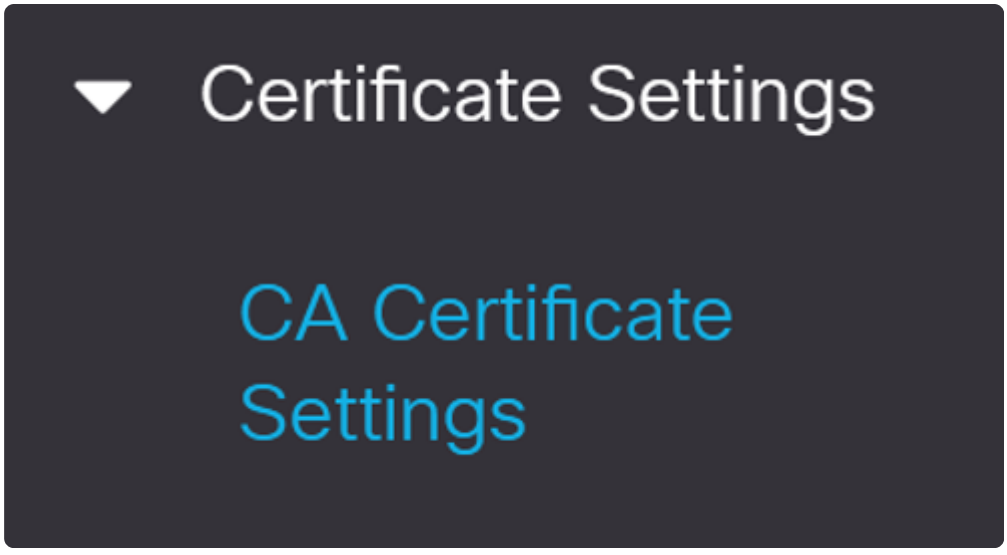
Importando um certificado intermediário

Na versão 4.1.3.36 do firmware dos switches Catalyst 1200 e 1300, você tem a opção de importar certificados intermediários usando a interface de usuário da Web do switch.

> **Note:**
> Com base na CA, o fornecedor do certificado fornecerá o certificado raiz e o certificado intermediário como um pacote para oferecer suporte ao certificado do servidor.

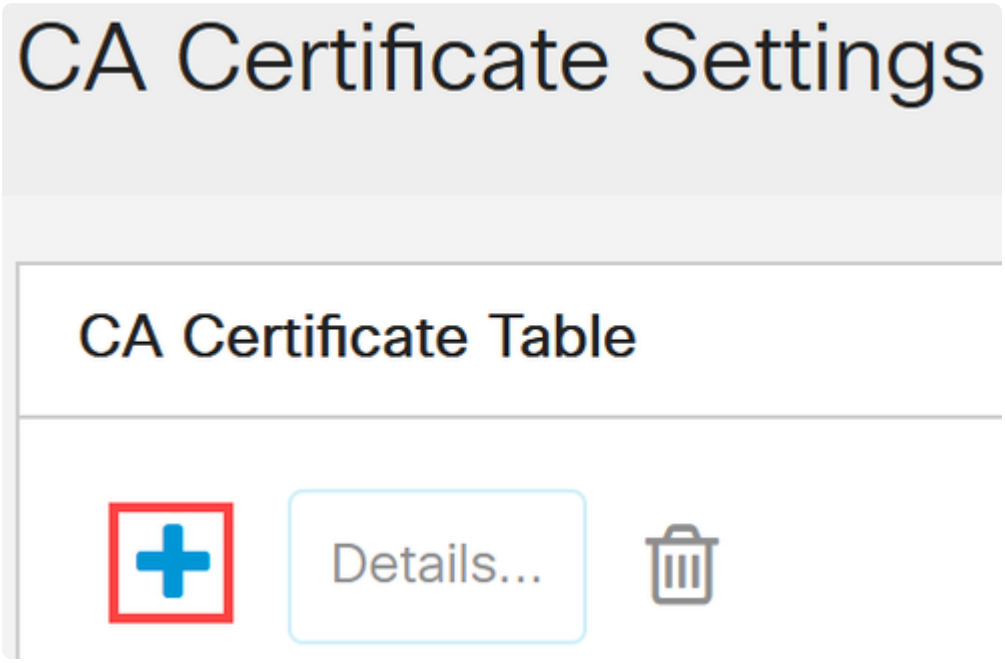
Passo 1

Na exibição Avançado, navegue para Segurança > Configurações de certificado > Configurações de certificado CA no painel de navegação.



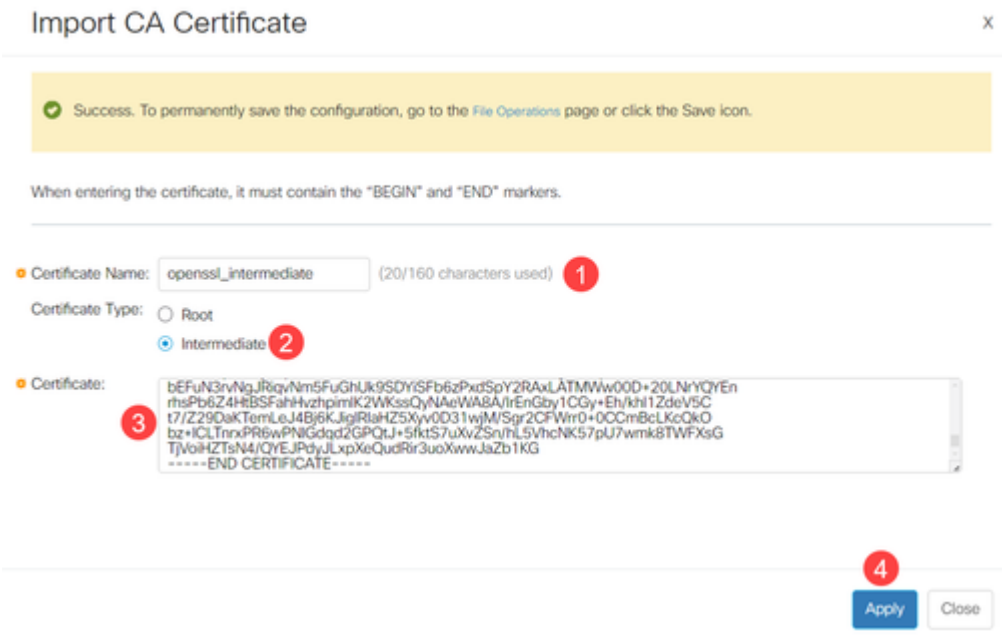
Passo 2

Clique no ícone de adição para importar um certificado.



Etapa 3

Insira o Nome do certificado, selecione Intermediário como o tipo de certificado, cole o certificado na caixa fornecida e clique em Aplicar.



Uma notificação de êxito será exibida na parte superior da tela.

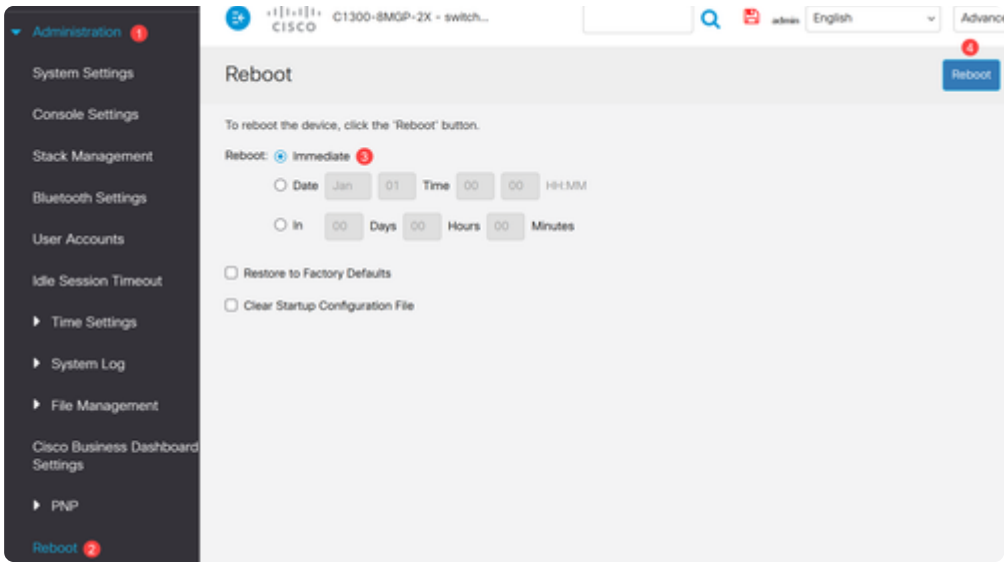
> **Note:**
> Uma mensagem de erro ocorrerá se o tipo de certificado não corresponder ao certificado que está sendo instalado.

Passo 4

Clique no ícone Save na parte superior da tela.

Etapa 5

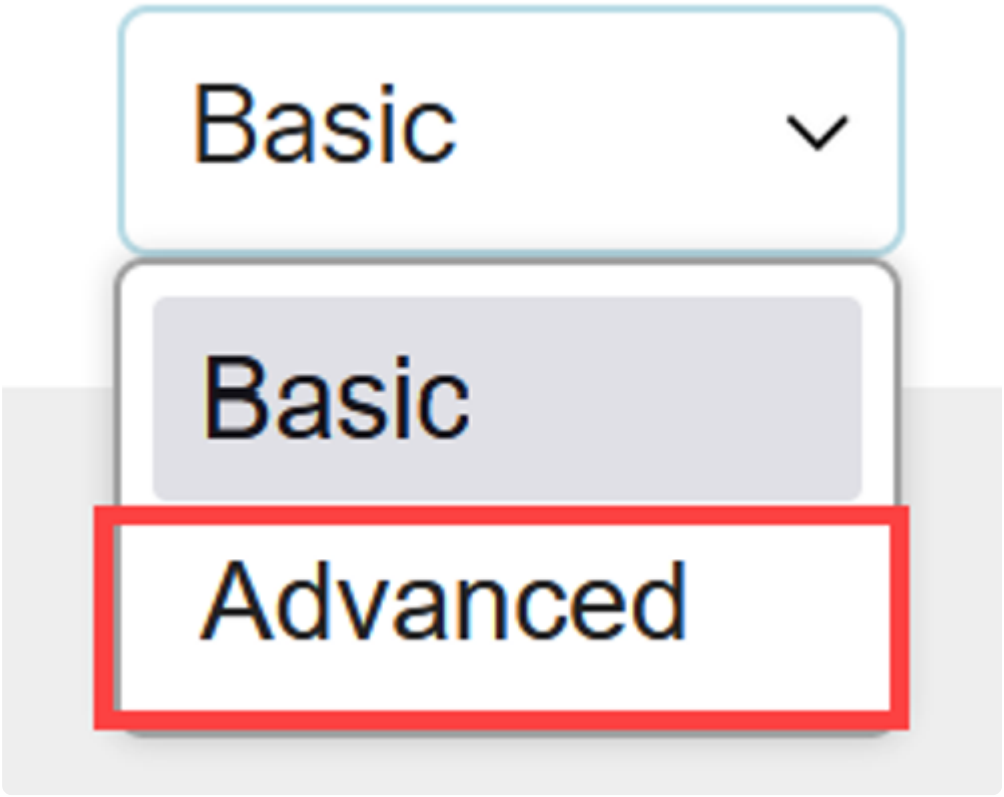
Reinicialize o switch para que todas as alterações tenham efeito. Para reinicializar, navegue até o menu Administração > Reinicialização e verifique se a opção de reinicialização Imediata está selecionada. Clique no botão Reinicializar.



Cadeia de Certificados

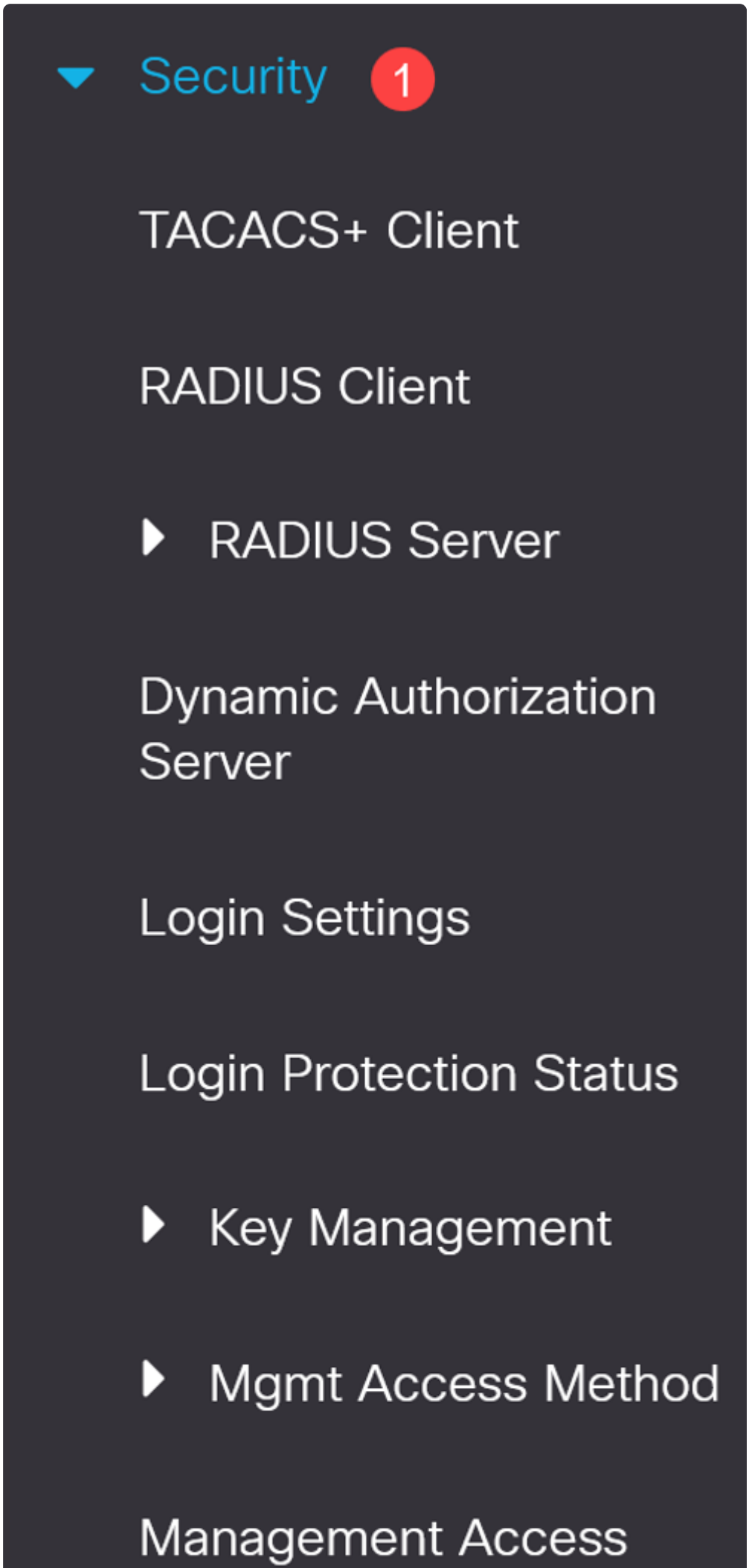
Passo 1

Faça login no switch Catalyst 1300 e alterne para a visualização Advanced no menu suspenso no canto superior direito da interface do usuário.



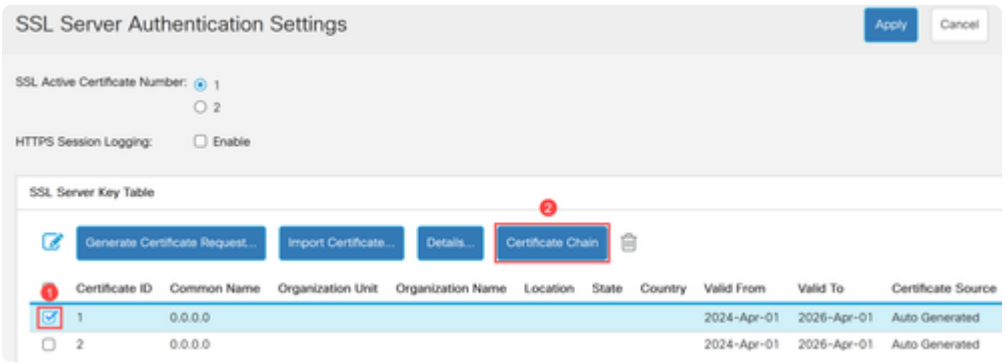
Passo 2

Navegue para Segurança > Servidor SSL > Configurações de autenticação de servidor SSL no painel de navegação.

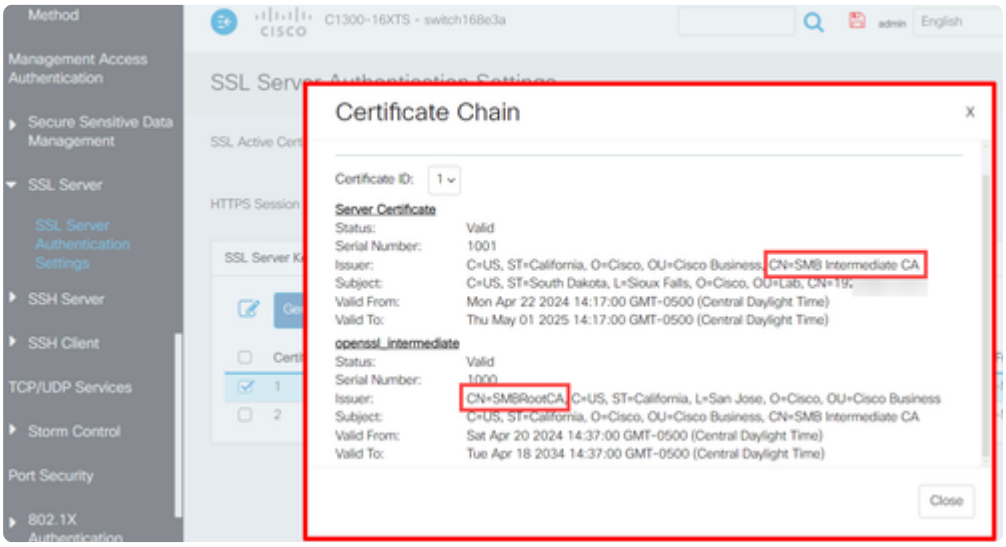

Security
1
TACACS+ Client
RADIUS Client
RADIUS Server
Dynamic Authorization Server
Login Settings
Login Protection Status
Key Management
Mgmt Access Method
Management Access

Etapa 3

Selecione o certificado na tabela e clique no botão Cadeia de Certificados.

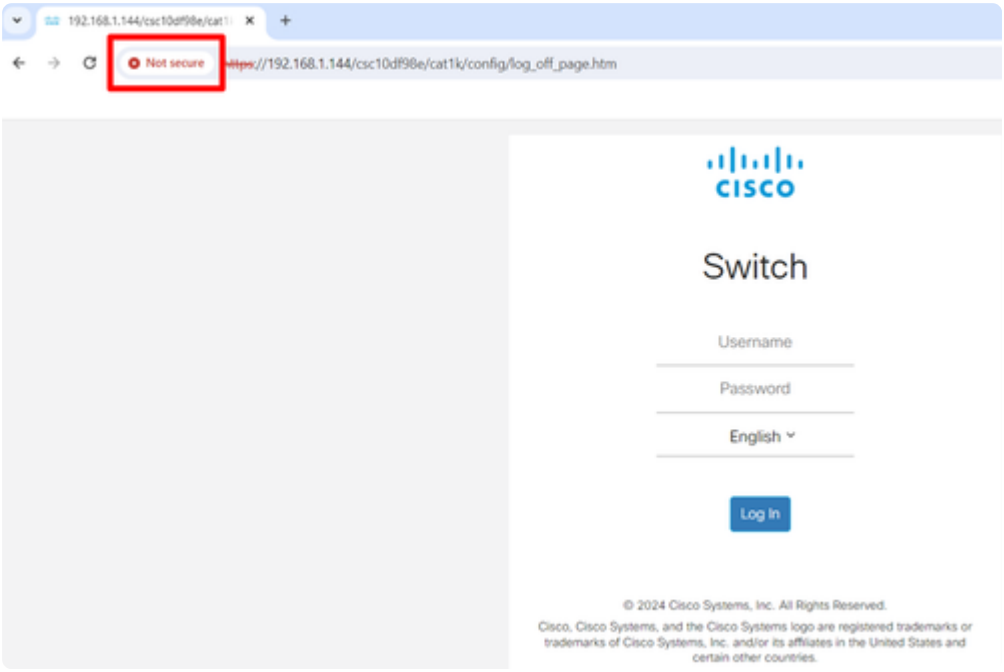


Uma janela pop-up será exibida mostrando os detalhes da cadeia de certificados. Neste exemplo, o certificado do servidor foi assinado por uma CA intermediária chamada "CA intermediária SMB", como observado pelo Nome comum (CN) do emissor no certificado do servidor. O emissor do certificado intermediário é SMBRootCA.

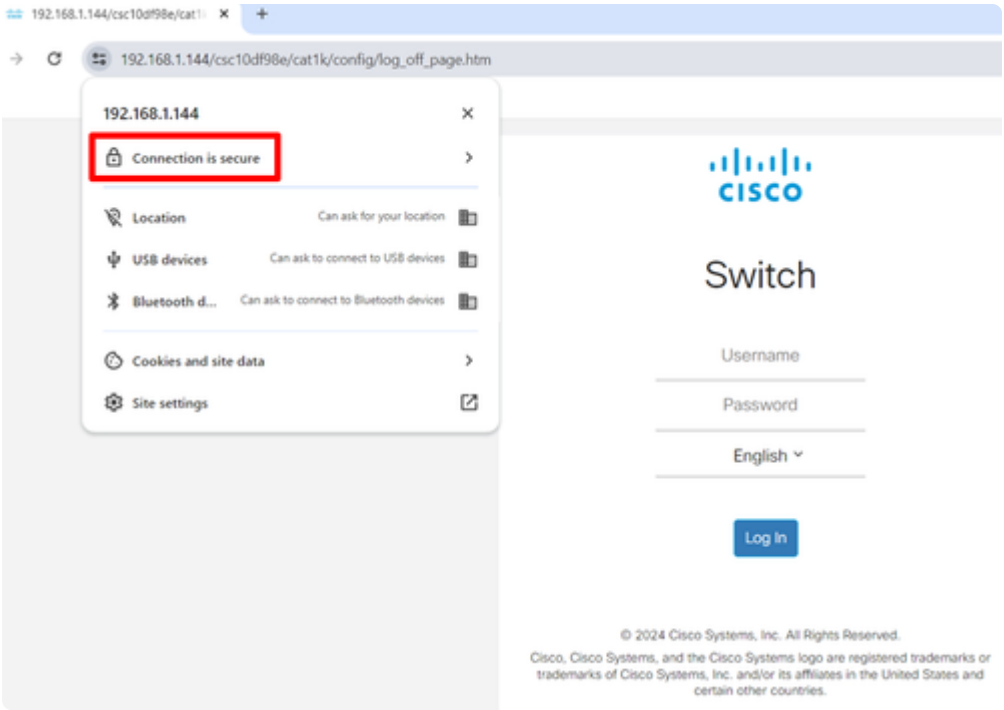


Exemplo de Cadeia de Certificados

Quando os switches usam um certificado autoassinado por padrão, isso resultará em um sistema cliente, um navegador da Web, nesse caso, para exibir uma mensagem de que a conexão é Não segura.



Por outro lado, quando a cadeia de certificados estiver completa com um certificado raiz, um certificado intermediário e um certificado de servidor instalados, o navegador exibirá que a conexão é Segura.



Conclusão

Pronto! Agora você sabe como carregar certificados intermediários e visualizar a cadeia de certificados nos switches Catalyst 1200 e 1300.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.