Catalyst 1200および1300スイッチの中間証明書および証明書チェーン

目的

この記事の目的は、ファームウェア4.1.3.36上のCatalyst 1200および1300スイッチの中間証明書の機能と証明書チェーンを確認し、それを設定する手順を説明することです。

該当するデバイス|ソフトウェアバージョン

- Catalyst 1200スイッチ| 4.1.3.36
- Catalyst 1300スイッチ| 4.1.3.36

はじめに

証明書はネットワークで使用され、セキュアなアクセスを提供します。証明書は、外部の認証局(CA)によって自己署名またはデジタル署名できます。 証明書チェーンのコンポーネントには、次のものがあります。

- ルートCA証明書:ルートCAまたはCA証明書は、証明書チェーンの階層の最上位にあり、自己署名されています。これは最終的なトラストアンカーであり、中間証明書の信頼性を確認するために使用されます。
- 中間証明書:中間証明書は、別の中間CAまたはルートCAである高レベルCAによって発行されます。場合によっては、証明書チェーンを形成する複数の中間証明書が存在することがあります。通常、中間CAはサーバ証明書の署名を行います。
- サーバ証明書:この証明書は、Webサイトなどの特定のサーバに対して発行されます。サーバの公開キーが含まれ、CAによって署名されます。CAは、ルートCAまたは中間CAです。

スイッチ（HTTPSサーバ）とブラウザ（HTTPSクライアント）間のSSL/TLSハンドシェイク中、スイッチは自身の署名付き証明書を提示します。ブラウザは、信頼できるストアにCA証明書を格納し、CAの公開キーを使用してサーバ証明書の署名を検証します。このプロセスにより、サーバのIDの信頼性が確立されます。検証が終わると、サーバとブラウザは暗号化パラメータの交換に進み、サーバとブラウザ間の転送中のデータの暗号化が有効になります。これにより、HTTPS経由でのデータ転送において、認証された安全な接続が保証されます。

サーバ証明書はルートCA証明書によって直接署名できますが、中間証明書を使用すると、署名プロセスを強化する階層構造が導入されます。中間証明書は、サーバ証明書とルートCA間の中間証明書として機能し、キーの侵害の分離によるセキュリティの向上、証明書管理の柔軟性、署名機関の委任機能などの利点を提供します。この階層型

アプローチにより、拡張性が向上し、証明書の更新プロセスが容易になり、失効をより詳細に制御できるようになります。基本的に、中間証明書を使用すると、セキュリティの強化、柔軟性、および証明書管理の合理化によって署名プロセスが強化されます。

Catalyst 1200および1300スイッチのファームウェア4.1.3.36では、中間証明書をインポートし、インストールされたサーバ証明書の証明書チェーンを表示できるようになりました。Catalystスイッチは、中間証明書およびHTTPSサーバ証明書チェーンに関する次の機能をサポートしています。

- 1つ以上の中間証明書のインストール。
- HTTPSクライアントとのTLSハンドシェイクに中間証明書を含める
- 中間証明書の表示
- デバイスのHTTPSサーバ証明書の証明書チェーンの表示

詳細については、お読みください！

目次

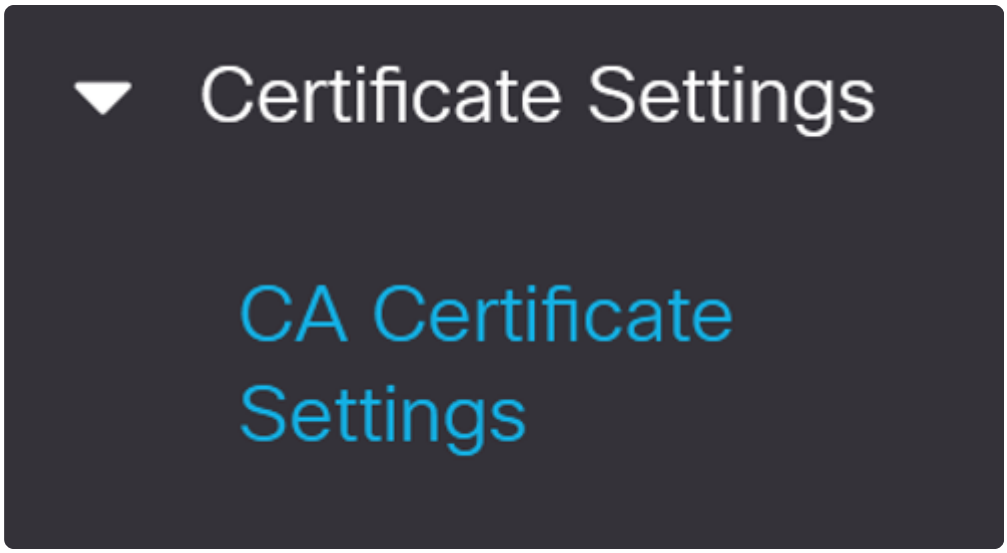
中間証明書のインポート

Catalyst 1200および1300スイッチのファームウェアバージョン4.1.3.36には、スイッチのWebユーザインターフェイスを使用して中間証明書をインポートするオプションがあります。

> **Note:**
> CAに基づいて、証明書ベンダーはルート証明書と中間証明書をバンドルとして提供し、サーバ証明書をサポートします。

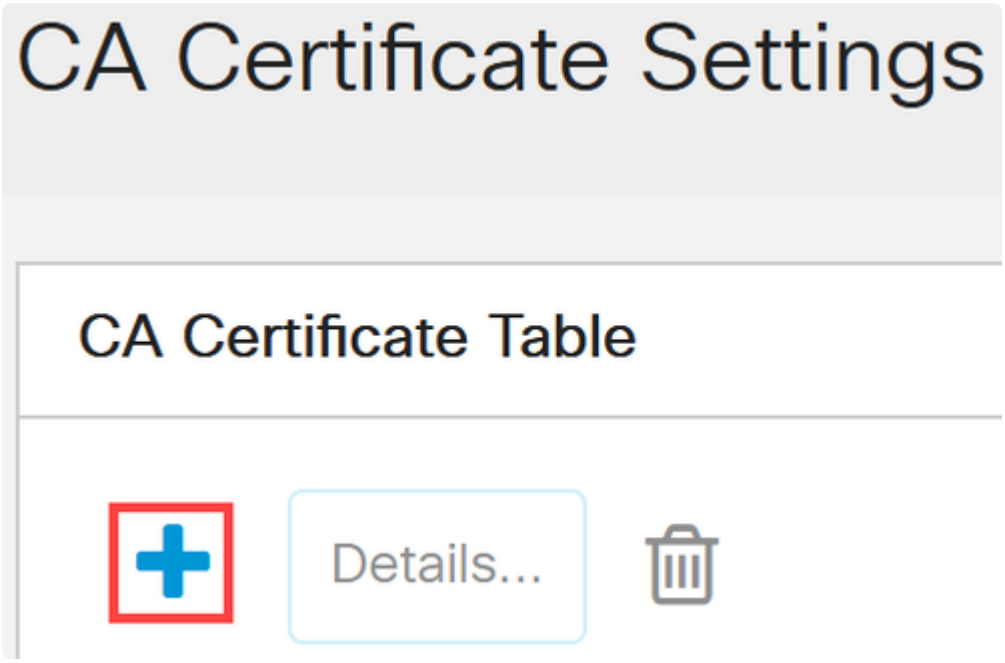
ステップ 1

Advancedビューの下で、ナビゲーションペインでSecurity > Certificate Settings > CA Certificate Settingsの順に移動します。



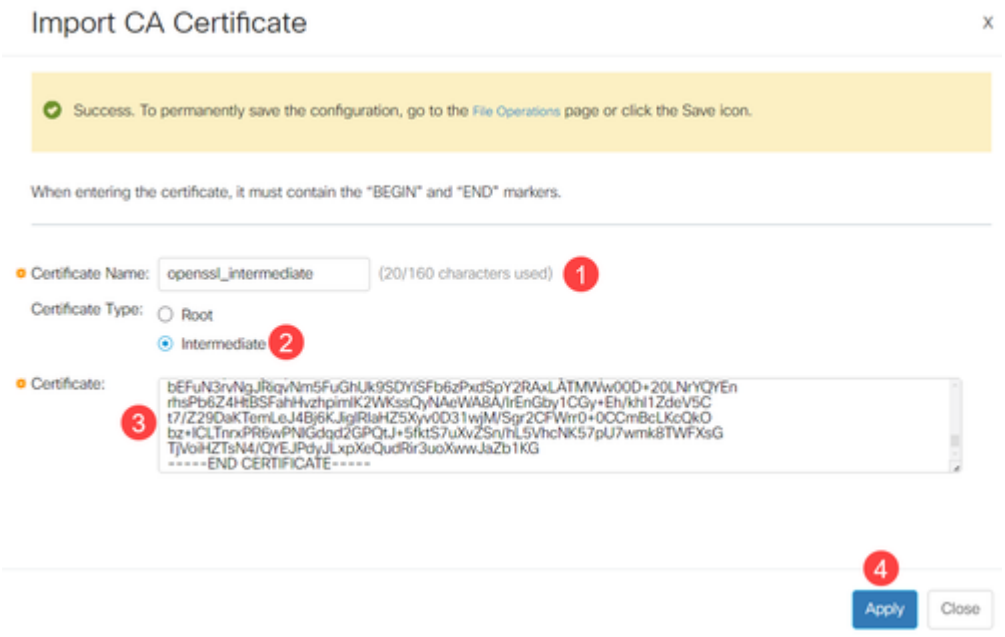
ステップ 2

証明書をインポートするには、プラス(+)アイコンをクリックします。



手順 3

証明書名を入力し、証明書のタイプとしてIntermediateを選択し、表示されたボックスに証明書を貼り付けます。次にApplyをクリックします。



成功の通知が画面の上部に表示されます。

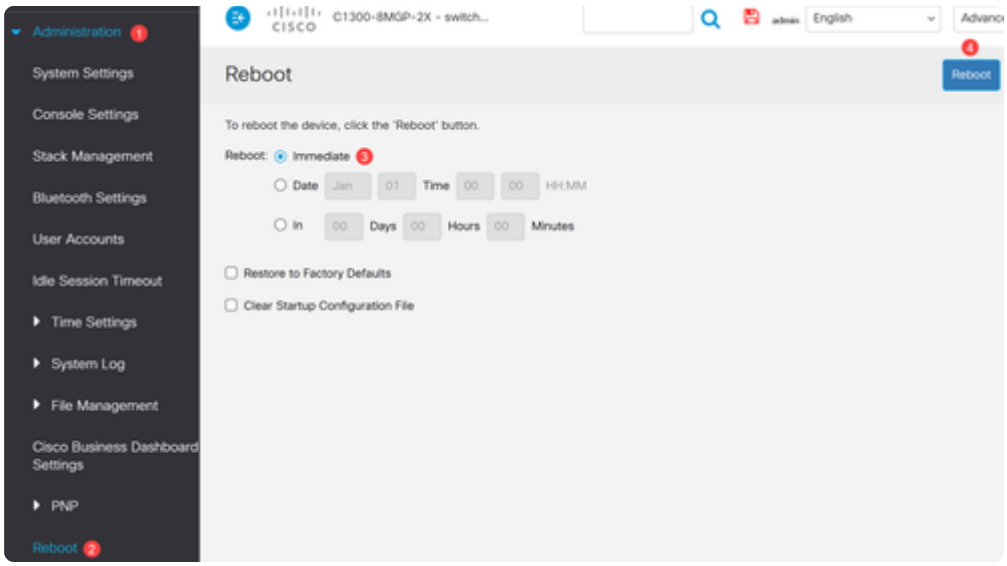
> **Note:**
> 証明書の種類がインストールされている証明書と一致しない場合は、エラーメッセージが表示されます。

ステップ 4

画面の上部にあるSaveアイコンをクリックします。

手順 5

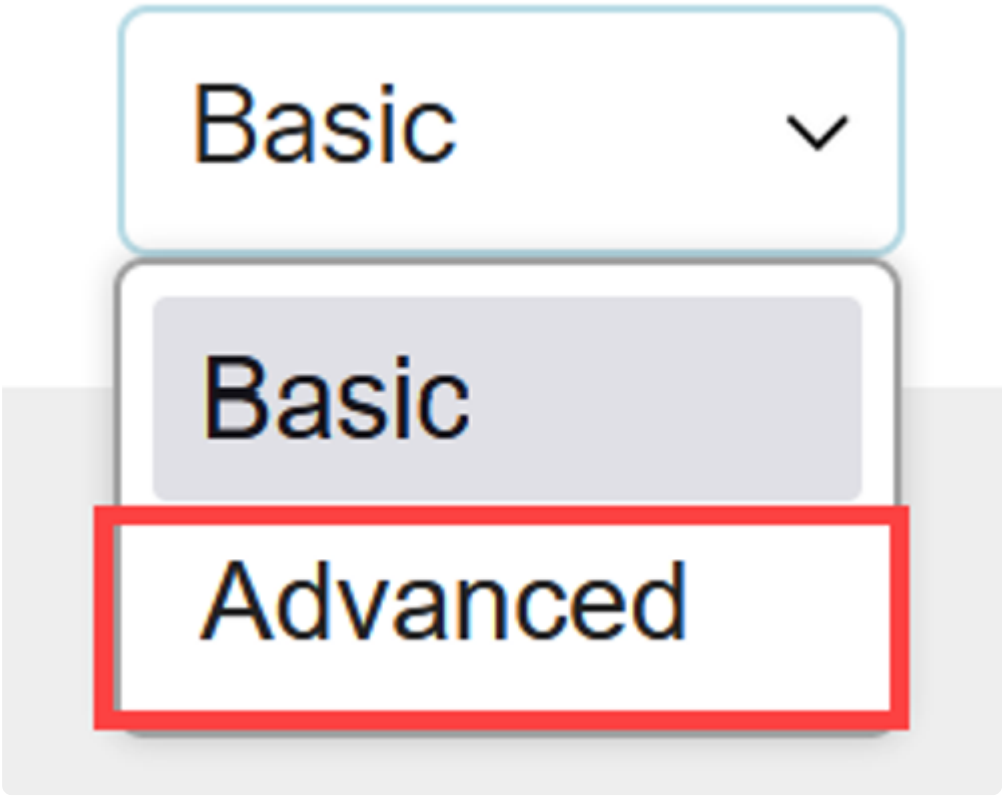
スイッチをリブートしてすべての変更を有効にします。リブートするには、Administration > Rebootメニューに移動し、Immediate rebootオプションが選択されていることを確認します。Rebootボタンをクリックします。



証明書チェーン

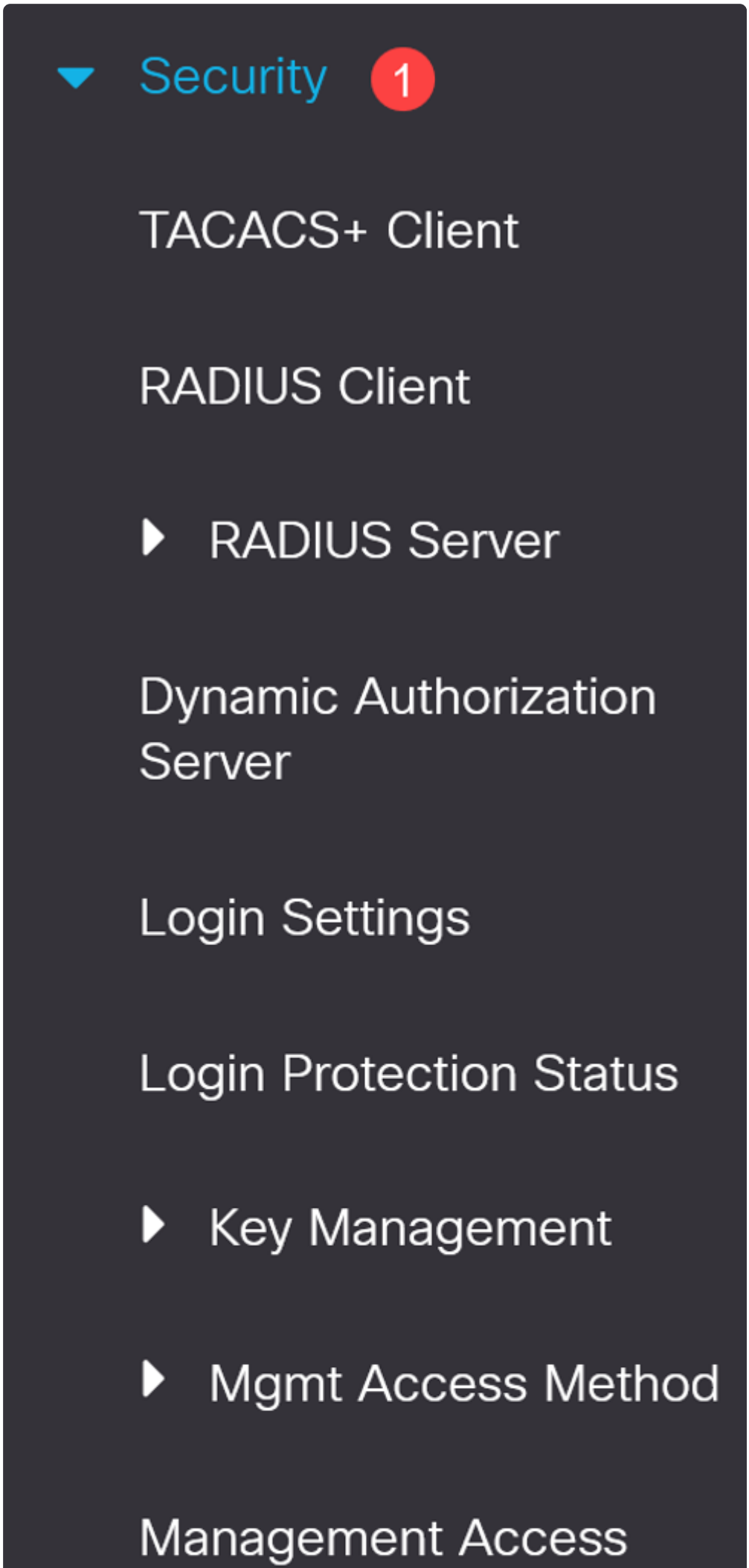
ステップ 1

Catalyst 1300スイッチにログインし、ユーザインターフェイスの右上隅にあるドロップダウンメニューからAdvancedビューに切り替えます。



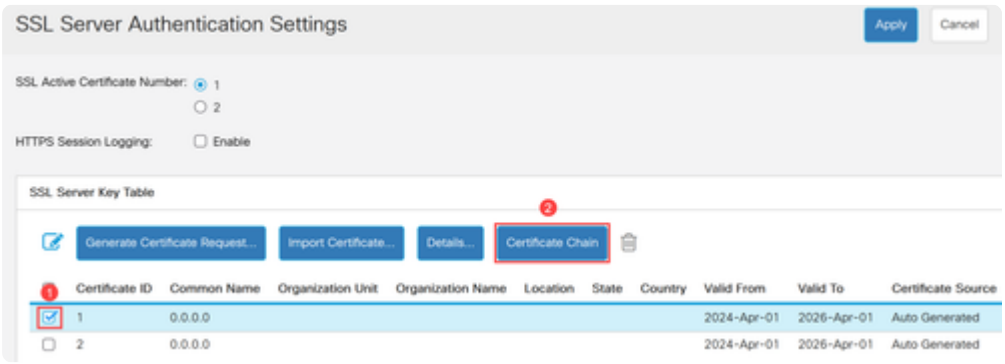
ステップ 2

ナビゲーションペインで、Security > SSL Server > SSL Server Authentication Settingsの順に選択します。

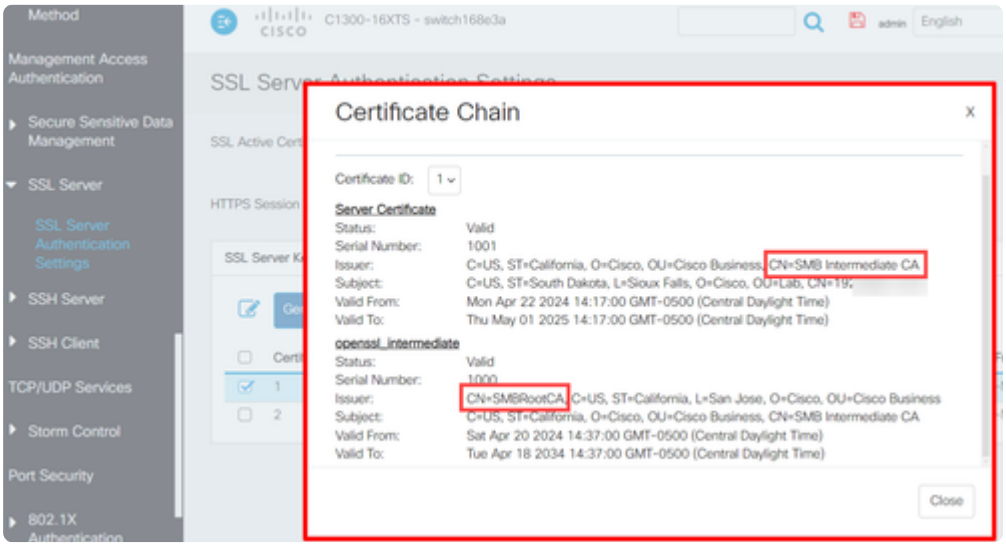

Security
1
TACACS+ Client
RADIUS Client
RADIUS Server
Dynamic Authorization Server
Login Settings
Login Protection Status
Key Management
Mgmt Access Method
Management Access

手順 3

テーブルから証明書を選択し、証明書チェーンボタンをクリックします。

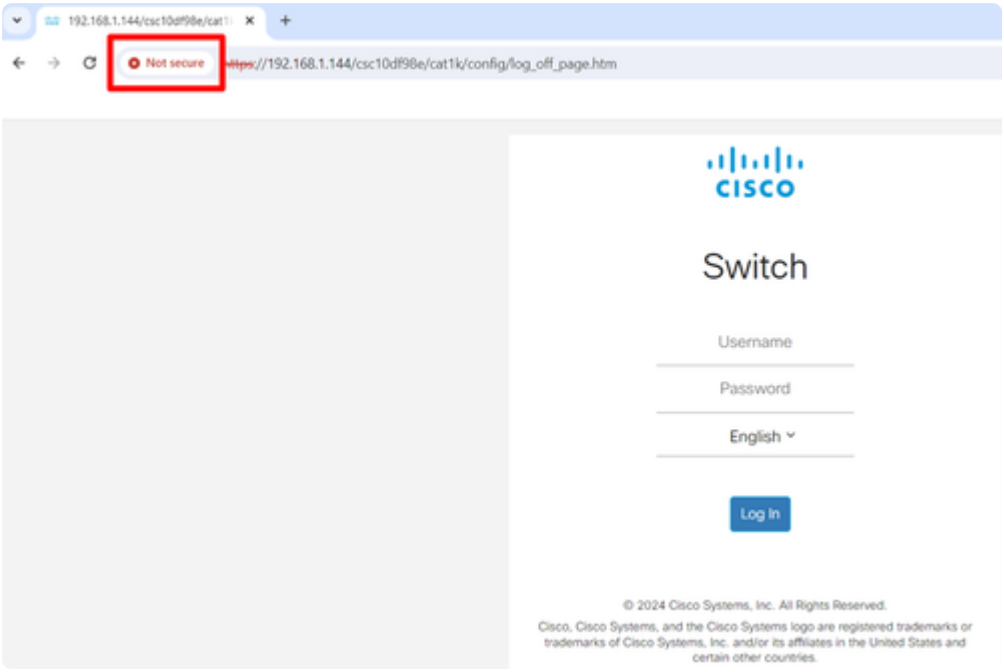


証明書チェーンの詳細を示すポップアップウィンドウが表示されます。この例では、サーバ証明書は「SMB Intermediate CA」という名前の中間CAによって署名されています。これは、サーバ証明書内の発行者の共通名(CN)で示されています。中間証明書の発行者はSMBRootCAです。

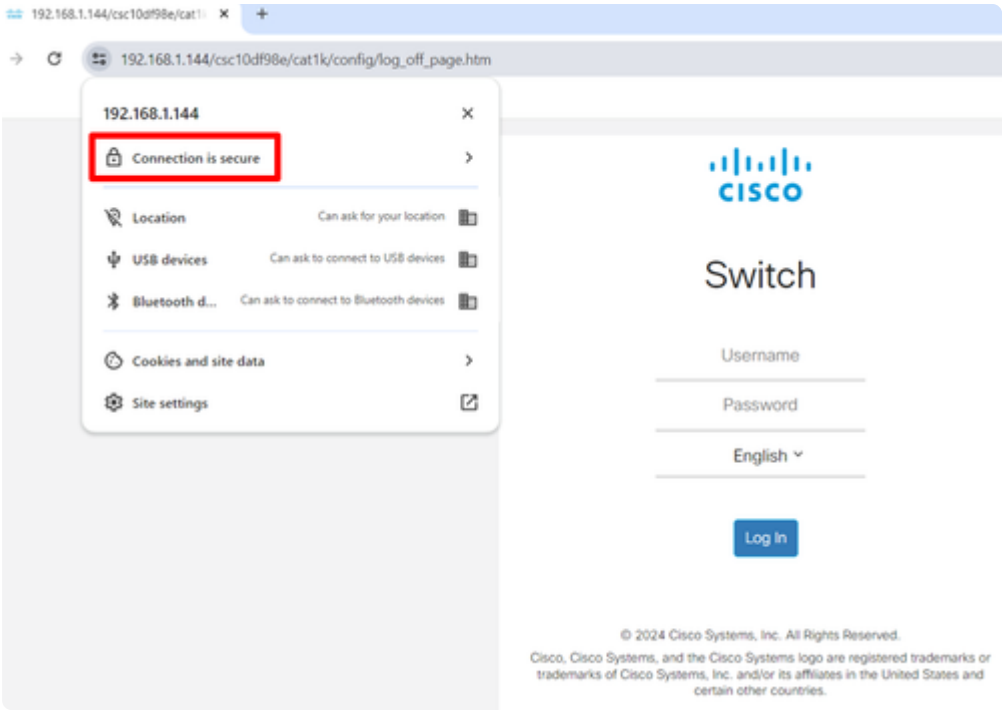


証明書チェーンの例

スイッチがデフォルトで自己署名証明書を使用する場合、これはクライアントシステム（この場合はWebブラウザ）で接続がセキュアでないというメッセージを表示することになります。



一方、証明書チェーンにルート証明書、中間証明書、サーバ証明書がインストールされている場合、ブラウザには接続がセキュアであると表示されます。



結論

行くぞ！以上で、中間証明書をアップロードする方法と、Catalyst 1200および1300ス

イッチの証明書チェーンを表示する方法について説明しました。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。