Zwischenzertifikate und Zertifikatskette in Catalyst Switches der Serien 1200 und 1300

Ziel

Ziel dieses Artikels ist es, die Funktionen und die Zertifikatskette für Zwischenzertifikate in Catalyst 1200 und 1300 Switches mit der Firmware 4.1.3.36 und die Schritte zu deren Konfiguration zu durchlaufen.

Unterstützte Geräte | Software-Version

- Catalyst Switches der Serie 1200 | 4.1.3.36
- Catalyst Switches der Serie 1300 | 4.1.3.36

Einleitung

Zertifikate werden in einem Netzwerk verwendet, um einen sicheren Zugriff bereitzustellen. Zertifikate können selbstsigniert oder von einer externen Zertifizierungsstelle digital signiert werden. Zu den Komponenten einer Zertifikatskette gehören:

- Zertifikat der Stammzertifizierungsstelle: Die Stammzertifizierungsstelle oder das Zertifikat der Zertifizierungsstelle befindet sich an der Spitze der Hierarchie der Zertifikatskette und ist selbstsigniert. Es ist der ultimative Vertrauensanker und wird verwendet, um die Authentizität von Zwischenzertifikaten zu überprüfen.
- Zwischenzertifikat(e): Ein Zwischenzertifikat wird von einer Zertifizierungsstelle höherer Ebene ausgestellt, die entweder eine andere Zwischenzertifikatstelle oder eine Stammzertifizierungsstelle ist. In einigen Fällen können mehrere Zwischenzertifikate die Zertifikatskette bilden. Normalerweise ist die zwischengeschaltete Zertifizierungsstelle für das Signieren von Serverzertifikaten zuständig.
- Serverzertifikat: Dieses Zertifikat wird für einen bestimmten Server ausgestellt, wie z.B. eine Website. Er enthält den öffentlichen Schlüssel des Servers und wird von einer Zertifizierungsstelle signiert. Die CA kann eine Stamm- oder Zwischen-CA sein.

Beim SSL/TLS-Handshake zwischen dem Switch (HTTPS-Server) und einem Browser (HTTPS-Client) präsentiert der Switch sein signiertes Zertifikat. Der Browser, der das Zertifizierungsstellenzertifikat in seinem vertrauenswürdigen Speicher hat, verwendet den öffentlichen Schlüssel der Zertifizierungsstelle, um die Signatur auf dem Serverzertifikat zu überprüfen. Bei diesem Prozess wird die Authentizität der Serveridentität festgestellt. Nach der Überprüfung tauschen der Server und der Browser kryptografische Parameter aus. Dadurch wird die Verschlüsselung der Daten bei der Übertragung zwischen den Servern ermöglicht und eine sichere und

authentifizierte Verbindung für die Datenübertragung über HTTPS sichergestellt.

Während Serverzertifikate direkt vom Stammzertifikat der Zertifizierungsstelle signiert werden können, führt die Verwendung von Zwischenzertifikaten zu einer hierarchischen Struktur, die den Signierungsprozess verbessert. Zwischenzertifikate fungieren als Vermittler zwischen dem Serverzertifikat und der Stammzertifizierungsstelle und bieten Vorteile wie erhöhte Sicherheit durch die Isolierung wichtiger Kompromittierungen, Flexibilität bei der Zertifikatsverwaltung und die Möglichkeit, die Signaturberechtigung zu delegieren. Dieser hierarchische Ansatz bietet eine verbesserte Skalierbarkeit, vereinfacht die Zertifikatverlängerungsprozesse und ermöglicht eine präzisere Kontrolle über den Widerruf. Im Wesentlichen bereichert die Verwendung von Zwischenzertifikaten den Signierungsprozess durch mehr Sicherheit, Flexibilität und ein optimiertes Zertifikatsmanagement.

In der Firmware-Version 4.1.3.36 der Catalyst 1200- und 1300-Switches können Sie jetzt Zwischenzertifikate importieren und die Zertifikatskette eines installierten Serverzertifikats anzeigen. Die Catalyst Switches unterstützen die folgenden Funktionen für Zwischenzertifikate und HTTPS-Server-Zertifikatsketten:

- Installation eines oder mehrerer Zwischenzertifikate.
- Einschließlich der Zwischenzertifikate im TLS-Handshake mit dem HTTPS-Client
- Anzeige von Zwischenzertifikaten
- Anzeige der Zertifikatskette der HTTPS-Serverzertifikate des Geräts

Lesen Sie weiter, um mehr zu erfahren!

Inhalt

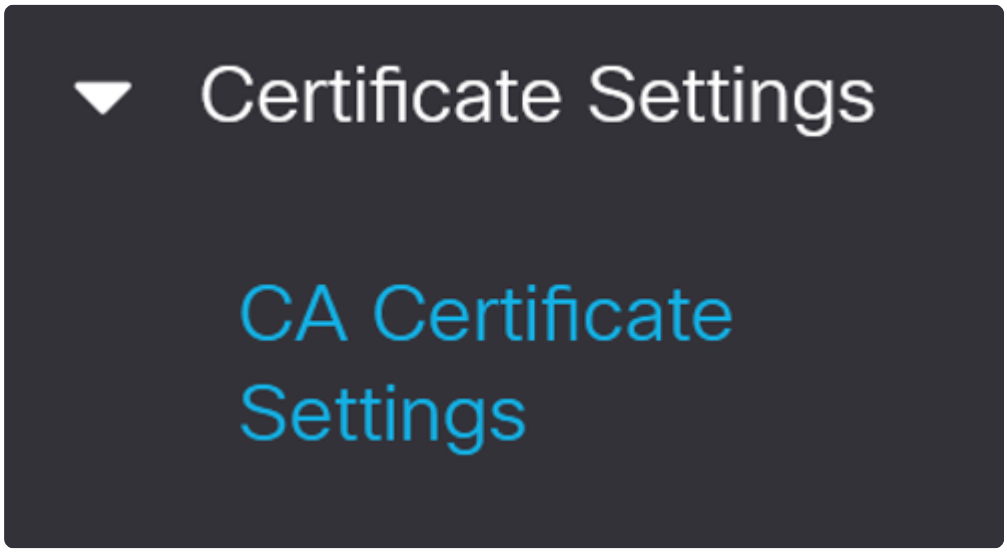
Importieren eines Zwischenzertifikats

In der Firmware-Version 4.1.3.36 der Catalyst 1200- und 1300-Switches können Sie Zwischenzertifikate über die Web-Benutzeroberfläche des Switches importieren.

> **Note:**
> Auf Basis der Zertifizierungsstelle stellt der Zertifikatanbieter das Stammzertifikat und das Zwischenzertifikat als Paket zur Verfügung, um das Serverzertifikat zu unterstützen.

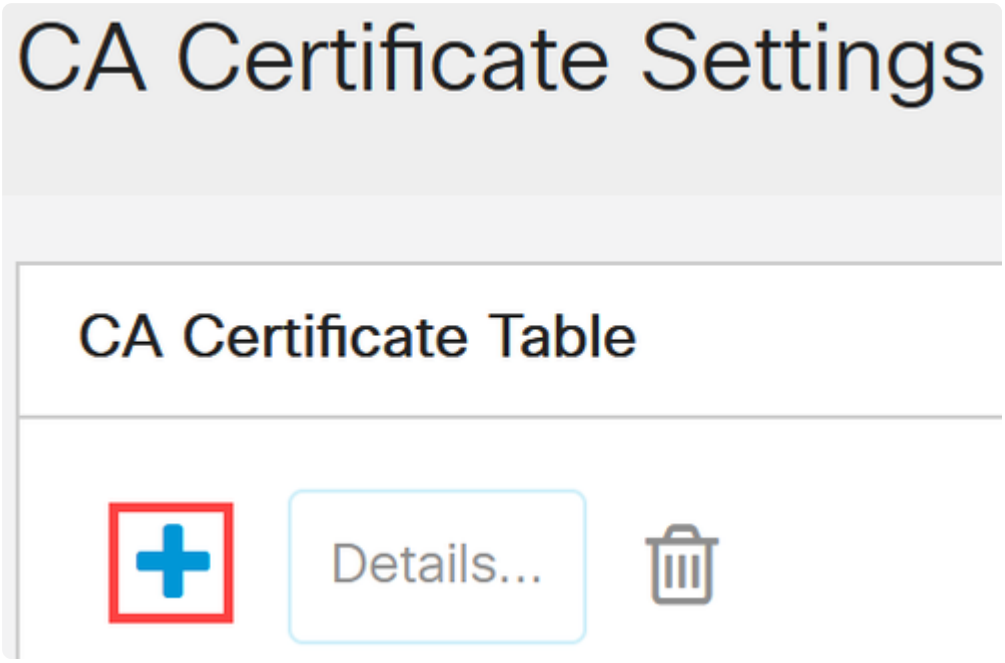
Schritt 1

Navigieren Sie in der erweiterten Ansicht im Navigationsbereich zu Sicherheit > Zertifikateinstellungen > Zertifikatseinstellungen der Zertifizierungsstelle.



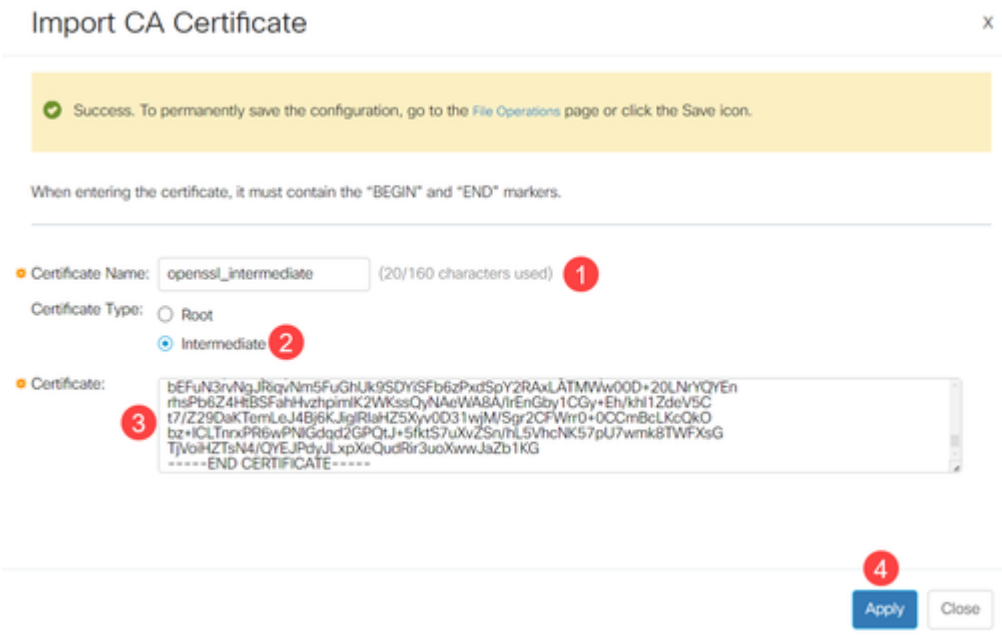
Schritt 2

Klicken Sie auf das Pluszeichen, um ein Zertifikat zu importieren.



Schritt 3

Geben Sie den Zertifikatsnamen ein, wählen Sie als Zertifikattyp Intermediate aus, fügen Sie das Zertifikat in das bereitgestellte Feld ein, und klicken Sie dann auf Apply.



Oben im Bildschirm wird eine Erfolgsmeldung angezeigt.

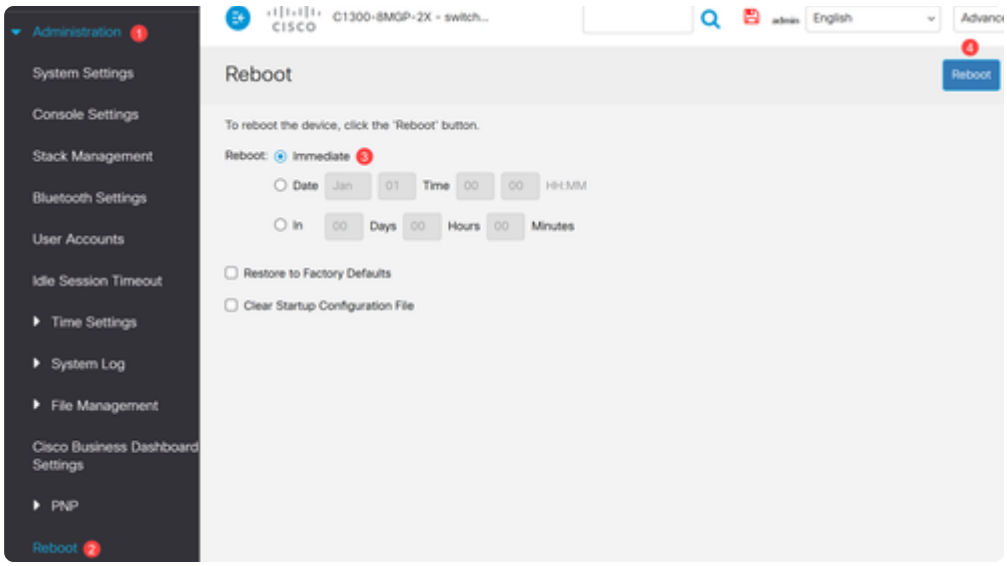
> **Note:**
> Wenn der Zertifikatstyp nicht mit dem installierten Zertifikat übereinstimmt, wird eine Fehlermeldung angezeigt.

Schritt 4

Klicken Sie oben im Bildschirm auf das Symbol Speichern.

Schritt 5

Starten Sie den Switch neu, damit alle Änderungen wirksam werden. Um einen Neustart durchzuführen, navigieren Sie zum Menü Administration > Reboot (Verwaltung > Neustart), und stellen Sie sicher, dass die Option Immediate reboot (Sofortiger Neustart) ausgewählt ist. Klicken Sie auf die Schaltfläche Neustart.

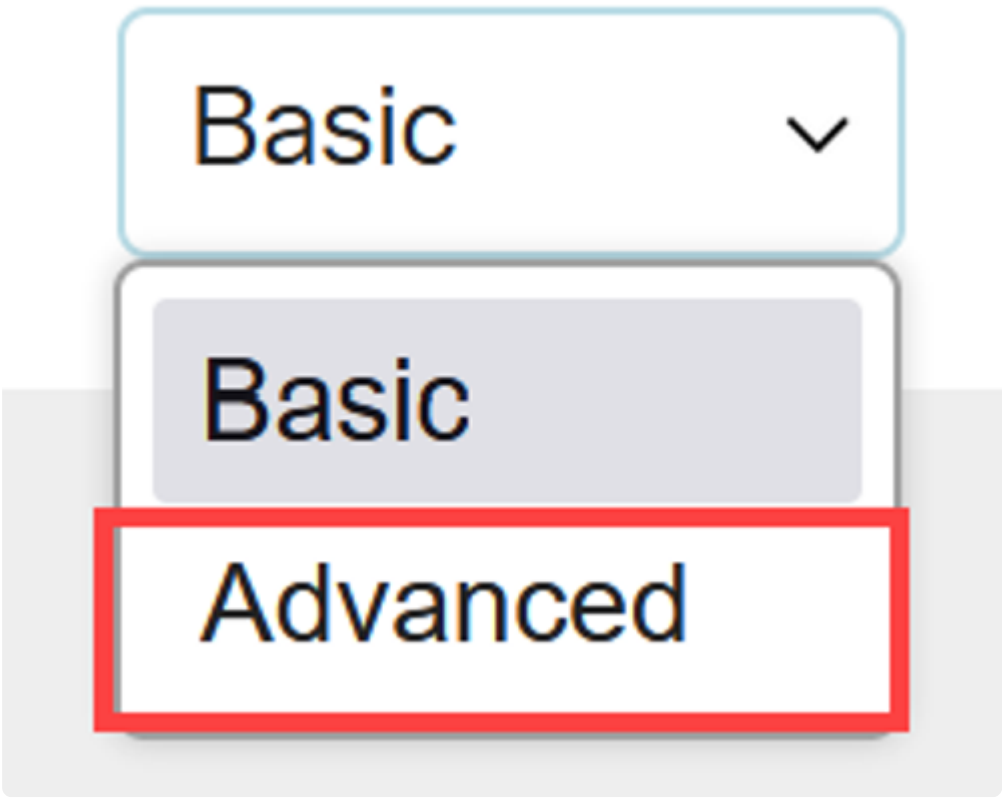


Zertifikatkette

Schritt 1

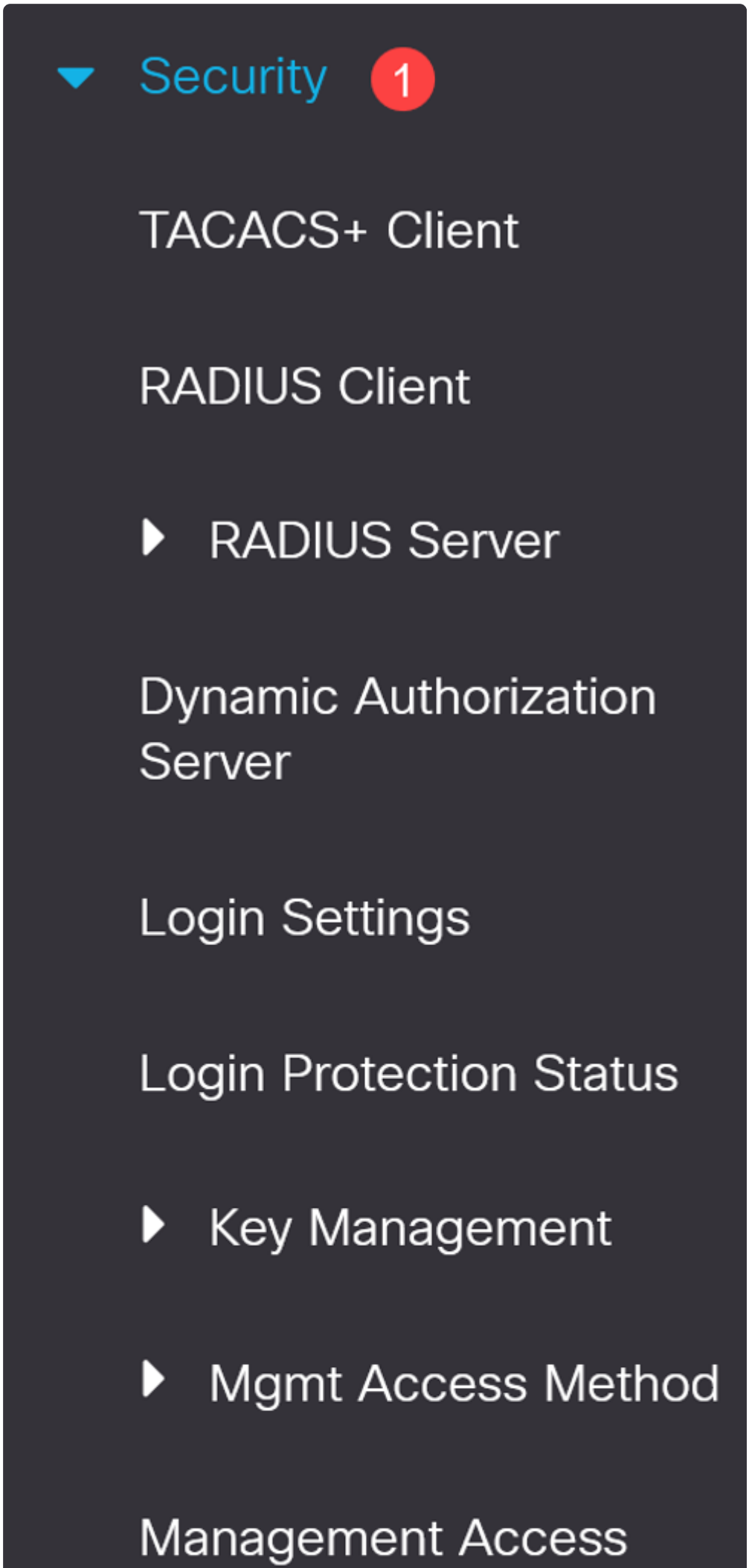
Melden Sie sich beim Catalyst 1300 Switch an, und wechseln Sie vom Dropdown-

Menü oben rechts auf der Benutzeroberfläche zur erweiterten Ansicht.



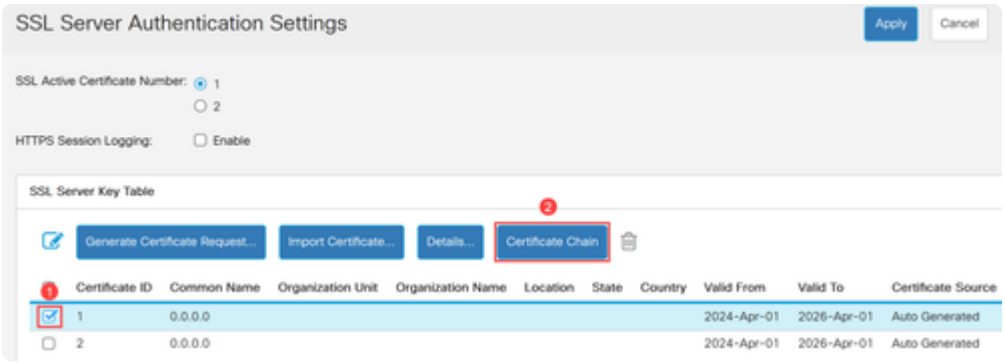
Schritt 2

Navigieren Sie im Navigationsbereich zu Security > SSL Server > SSL Server Authentication Settings (Sicherheit > SSL-Server > SSL-Serverauthentifizierungseinstellungen).

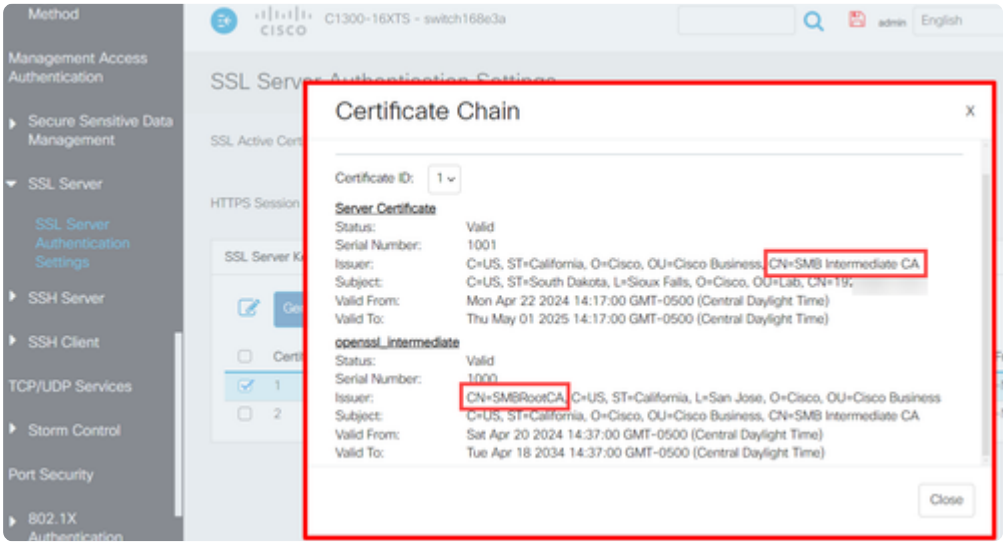

Security
1
TACACS+ Client
RADIUS Client
RADIUS Server
Dynamic Authorization Server
Login Settings
Login Protection Status
Key Management
Mgmt Access Method
Management Access

Schritt 3

Wählen Sie das Zertifikat aus der Tabelle aus, und klicken Sie dann auf die Schaltfläche Zertifikatskette.

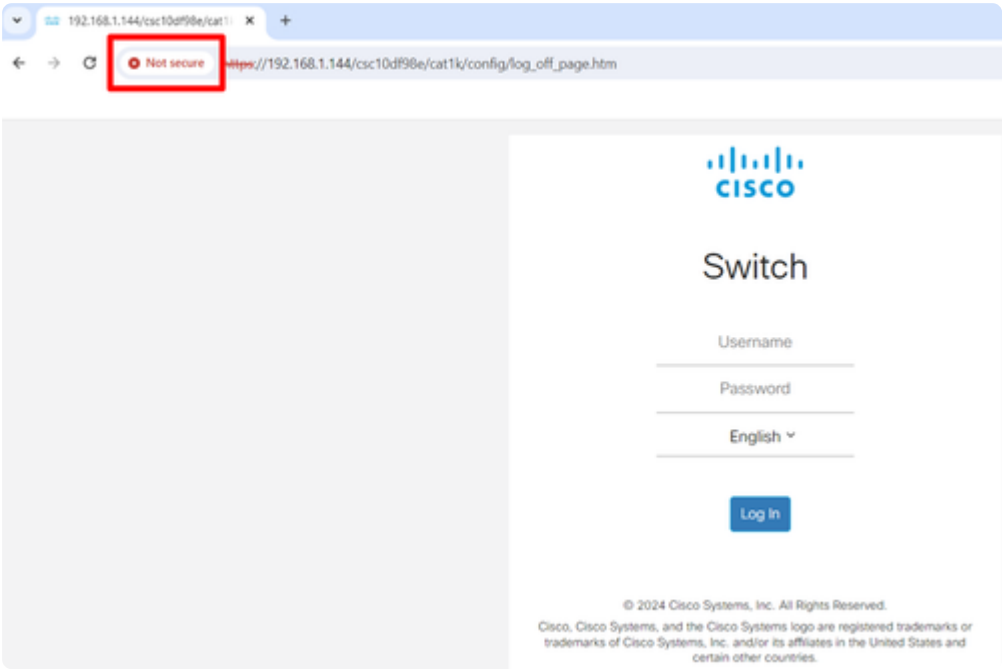


Ein Popup-Fenster mit den Details der Zertifikatskette wird angezeigt. In diesem Beispiel wurde das Serverzertifikat von einer zwischengeschalteten Zertifizierungsstelle mit dem Namen "SMB Intermediate CA" signiert, wie im Common Name (CN) des Ausstellers im Serverzertifikat angegeben. Der Aussteller des Zwischenzertifikats ist SMBRootCA.

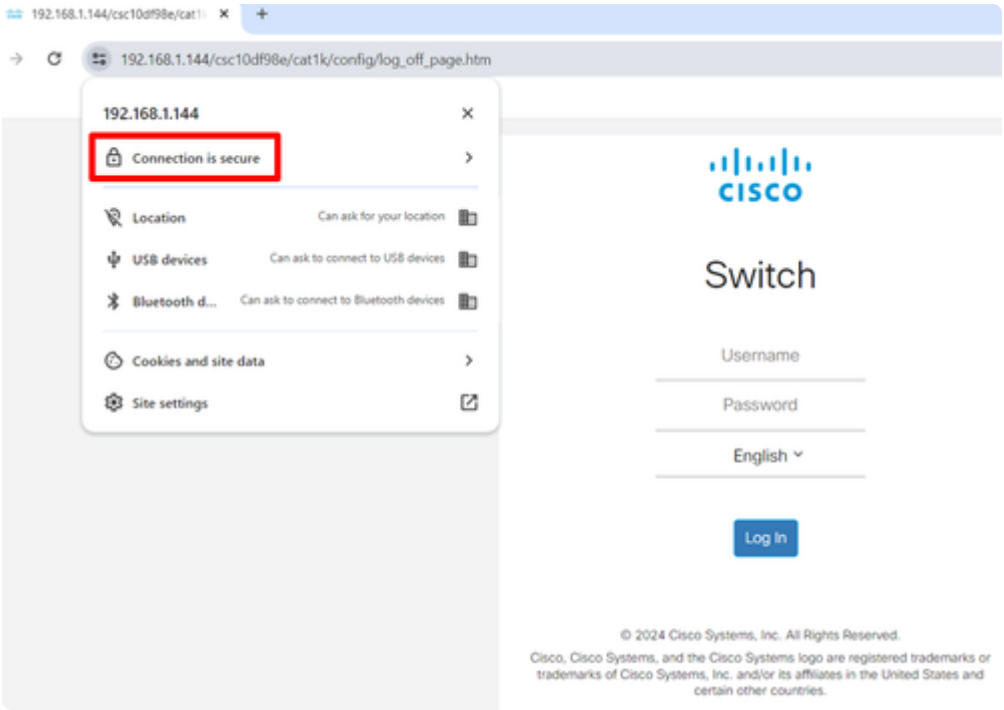


Beispiel für eine Zertifikatkette

Wenn Switches standardmäßig ein selbstsigniertes Zertifikat verwenden, zeigt ein Client-System, in diesem Fall ein Webbrowser, die Meldung an, dass die Verbindung nicht sicher ist.



Wenn die Zertifikatskette jedoch mit einem Stammzertifikat, einem Zwischenzertifikat und einem installierten Serverzertifikat abgeschlossen ist, zeigt der Browser an, dass die Verbindung sicher ist.



Schlussfolgerung

Da haben Sie es! Jetzt wissen Sie, wie Sie Zwischenzertifikate hochladen und die Zertifikatskette in den Catalyst Switches der Serien 1200 und 1300 anzeigen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.