Tussenliggende certificaten en certificaatketen in katalysator 1200 en 1300 Switches

Doel

Het doel van dit artikel is om de tussenliggende certificaatfunctie en certificaatketen in Catalyst 1200 en 1300 switches op firmware 4.1.3.36 en de stappen om deze te configureren te doornemen.

Toepasselijke apparaten | Softwareversie

- Katalysator 1200 Switches | 4.1.3.36
- Katalysator 1300 Switches | 4.1.3.36

Inleiding

Certificaten worden gebruikt in een netwerk om veilige toegang te bieden. Certificaten kunnen zelf ondertekend of digitaal ondertekend worden door een externe Certificaat Autoriteit (CA). Onderdelen van een certificaatketen zijn:

- Root CA-certificaat: Het root CA- of CA-certificaat staat bovenaan de hiërarchie voor de certificaatketen en is zelf ondertekend. Het is het ultieme vertrouwensanker en wordt gebruikt om de authenticiteit van tussenliggende certificaten te verifiëren.
- Intermediair(e) certificaat(en): een intermediair certificaat wordt afgegeven door een CA van een hoger niveau die een andere intermediaire CA of een root-CA is. In sommige gevallen kunnen er meerdere tussenliggende certificaten zijn die de certificaatketen vormen. Normaal gesproken is de intermediaire CA verantwoordelijk voor het ondertekenen van servercertificaten.
- Servercertificaat: Dit certificaat wordt afgegeven voor een specifieke server, zoals bijvoorbeeld een website. Het bevat de publieke sleutel van de server en is ondertekend door een CA. De CA kan een root of intermediaire CA zijn.

Tijdens de SSL/TLS-handshake tussen de switch (HTTPS-server) en een browser (HTTPS-client) presenteert de switch zijn ondertekende certificaat. De browser, die het CA-certificaat in zijn vertrouwde archief heeft, gebruikt de openbare sleutel van de CA om de handtekening op het servercertificaat te verifiëren. Dit proces zorgt voor de authenticiteit van de identiteit van de server. Na verificatie gaan de server en de browser over tot het uitwisselen van cryptografische parameters, waardoor de codering van gegevens in transit tussen hen mogelijk wordt, waardoor een veilige en geverifieerde verbinding voor gegevensoverdracht via HTTPS wordt gewaarborgd.

Servercertificaten kunnen rechtstreeks worden ondertekend door het root CA-

certificaat, maar het gebruik van tussenliggende certificaten introduceert een hiërarchische structuur die het ondertekeningsproces verbetert. Tussenliggende certificaten fungeren als tussenpersonen tussen het servercertificaat en de basiscertificeringsinstantie en bieden voordelen zoals verhoogde beveiliging door essentiële compromissen te isoleren, flexibiliteit in certificaatbeheer en de mogelijkheid om ondertekeningsautoriteit te delegeren. Deze hiërarchische aanpak biedt verbeterde schaalbaarheid, vereenvoudigt de processen voor het vernieuwen van certificaten en biedt meer gedetailleerde controle over intrekking. In wezen verrijkt het gebruik van tussenliggende certificaten het ondertekeningsproces door verbeterde beveiliging, flexibiliteit en gestroomlijnd certificaatbeheer te bieden.

In firmware 4.1.3.36 van Catalyst 1200 en 1300 switches kunt u nu tussenliggende certificaten importeren en de certificaatketen van een servercertificaat bekijken. De Catalyst-switches ondersteunen de volgende functies met betrekking tot intermediaire certificaatketen en HTTPS-servercertificaatketen:

- Installatie van een of meer tussenliggende certificaten.
- Inclusief tussencertificaat(en) in de TLS-handshake met de HTTPS-client
- Weergave van tussentijdse certificaten
- Weergave van de certificaatketen van de HTTPS-servercertificaten van het apparaat

Blijf lezen om meer te weten te komen!

Inhoud

- Een tussentijds certificaat importeren
- certificaatketen
- Voorbeeld certificaatketen

Een tussentijds certificaat importeren

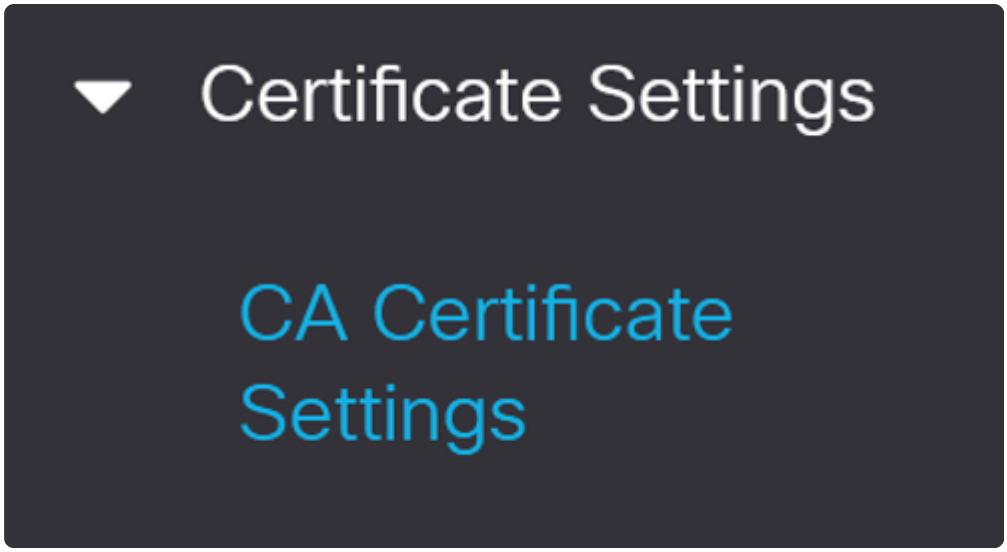
In firmwareversie 4.1.3.36 van de Catalyst 1200 en 1300 switches kunt u tussenliggende certificaten importeren via de webgebruikersinterface van de switch.

> **Note:**
> Op basis van de CA levert de certificaatverkoper het basiscertificaat en het tussenliggende certificaat als bundel ter ondersteuning van het servercertificaat.

Stap 1

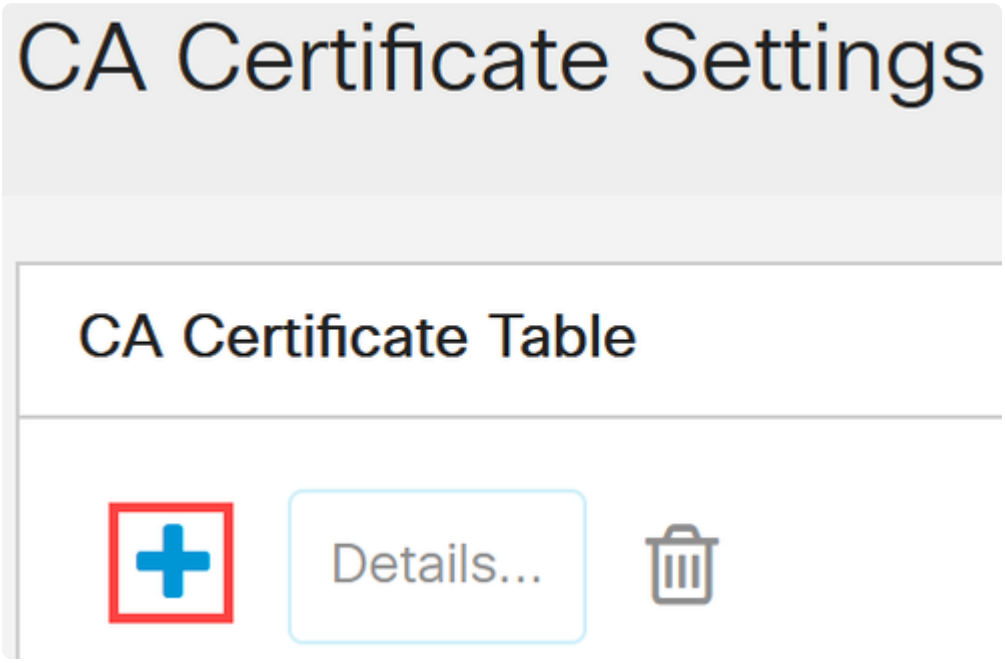
Navigeer onder Geavanceerd naar Beveiliging > Certificaatinstellingen > CA-

certificaatinstellingen in het navigatiedeelvenster.



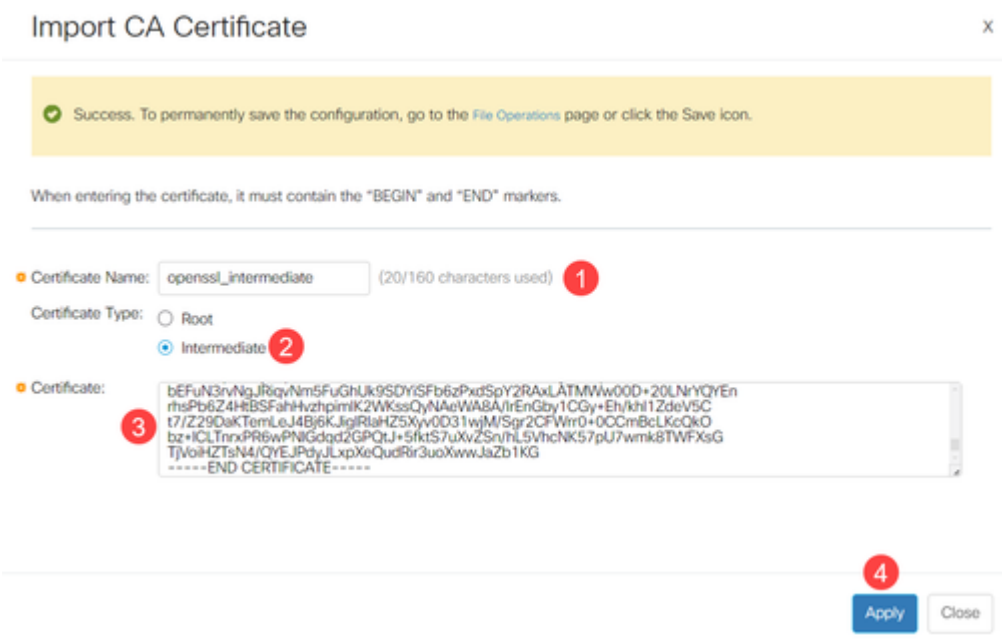
Stap 2

Klik op het plusteken om een certificaat te importeren.



Stap 3

Voer de certificaatnaam in, selecteer Intermediate als het certificaattype, plak het certificaat in het opgegeven vak en klik vervolgens op Toepassen.



Een succesmelding verschijnt bovenaan het scherm.

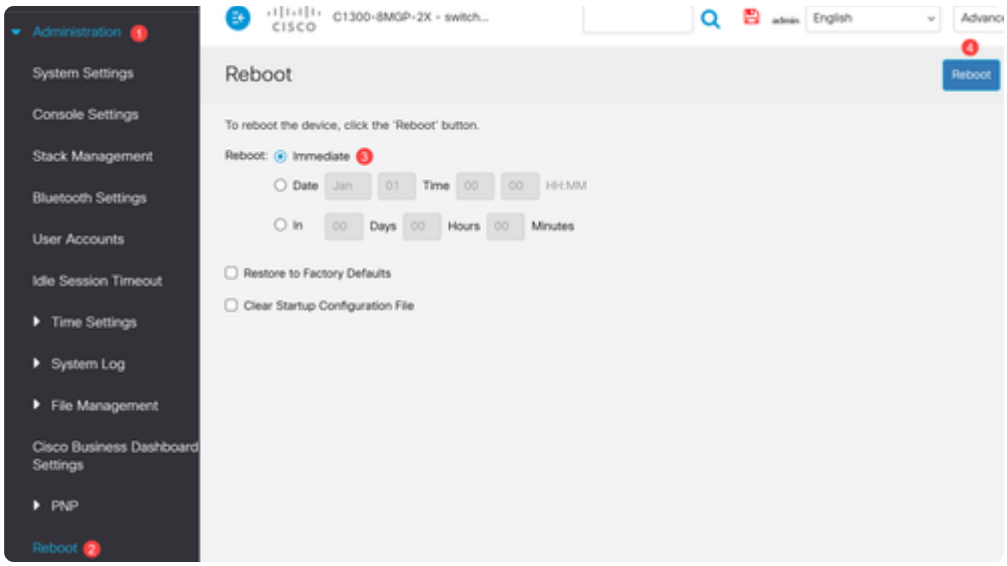
> **Note:**
> Er wordt een foutbericht weergegeven als het certificaattype niet overeenkomt met het certificaat dat wordt geïnstalleerd.

Stap 4

Klik op het pictogram Opslaan boven aan het scherm.

Stap 5

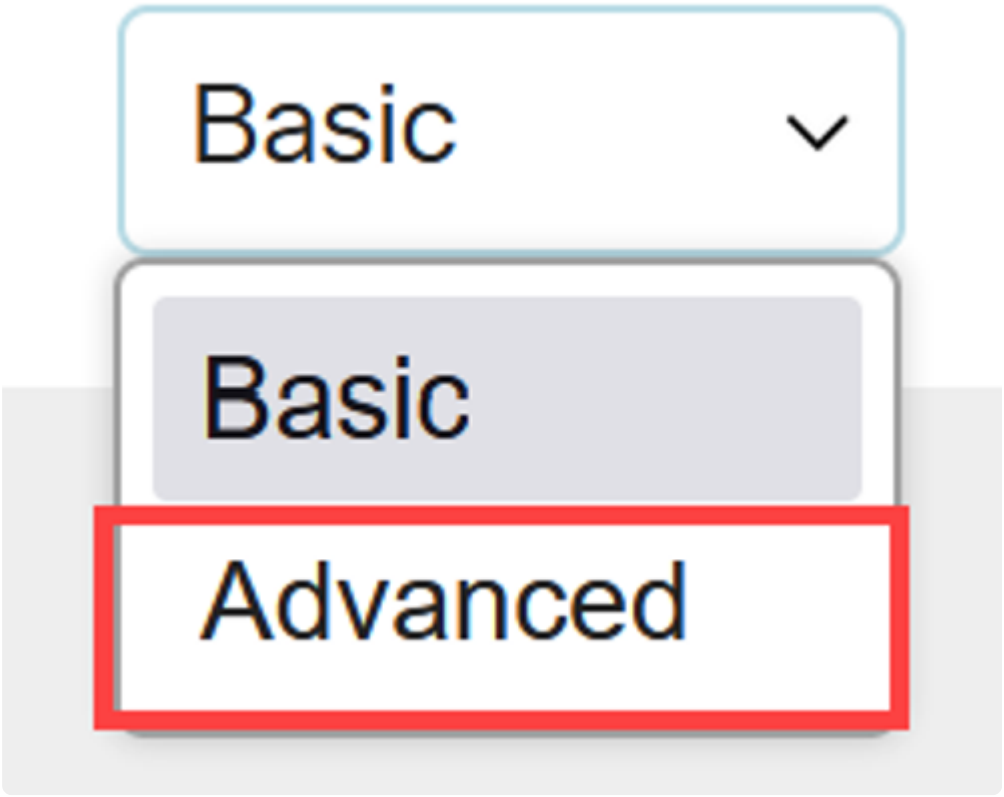
Start de switch opnieuw op zodat alle wijzigingen van kracht worden. Als u opnieuw wilt opstarten, gaat u naar het menu Beheer > Opnieuw opstarten en controleert u of de optie Direct opnieuw opstarten is geselecteerd. Klik op de knop Opnieuw opstarten.



certificaatketen

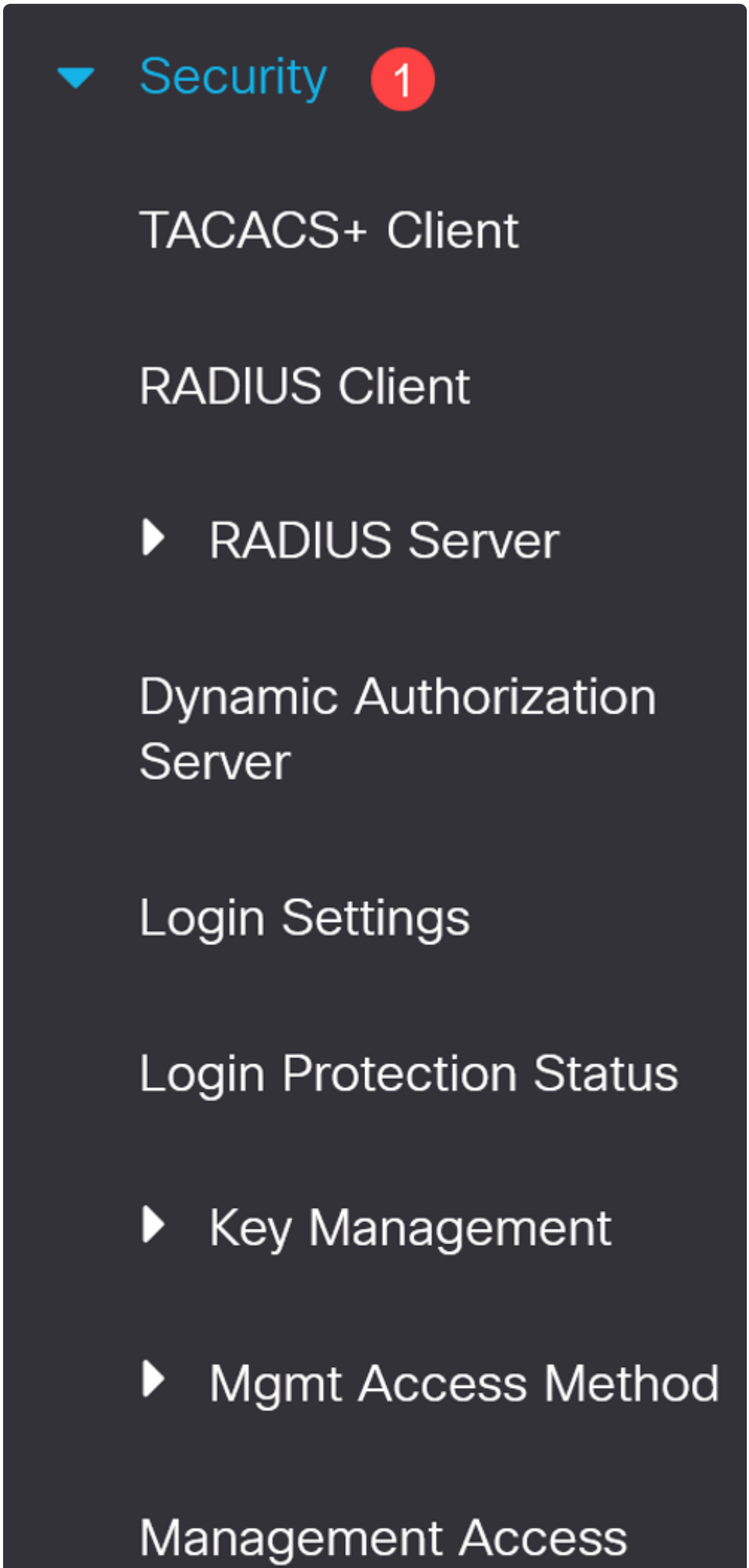
Stap 1

Meld u aan bij de switch Catalyst 1300 en switch bij de weergave Geavanceerd in het vervolgkeuzemenu rechtsboven in de gebruikersinterface.



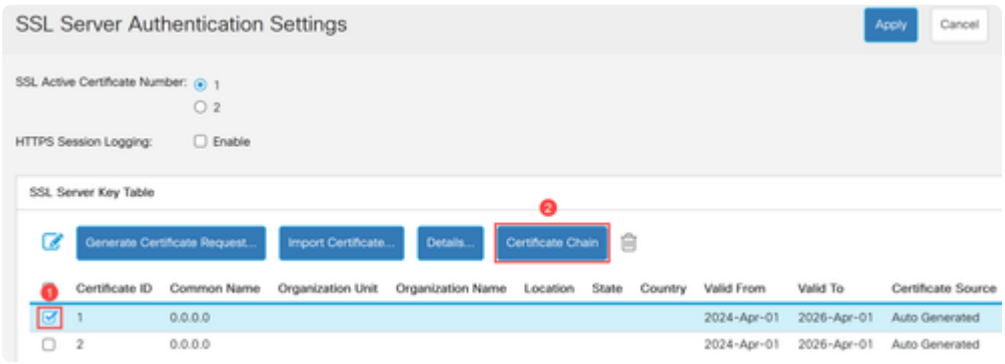
Stap 2

Navigeer naar Beveiliging > SSL-server > Verificatie-instellingen voor SSL-server in het navigatiedeelvenster.

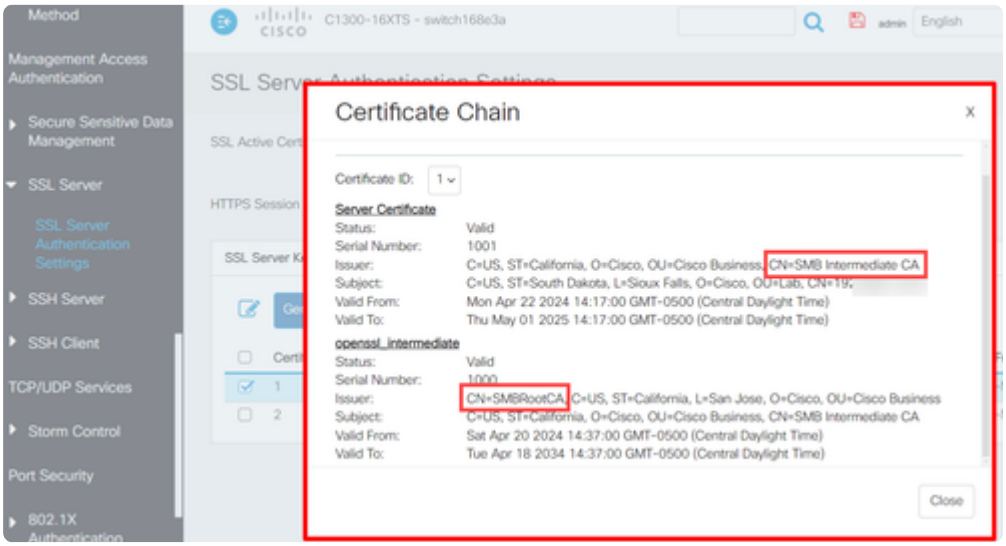

Security
1
TACACS+ Client
RADIUS Client
RADIUS Server
Dynamic Authorization Server
Login Settings
Login Protection Status
Key Management
Mgmt Access Method
Management Access

Stap 3

Selecteer het certificaat in de tabel en klik vervolgens op de knop Certificaatketen.

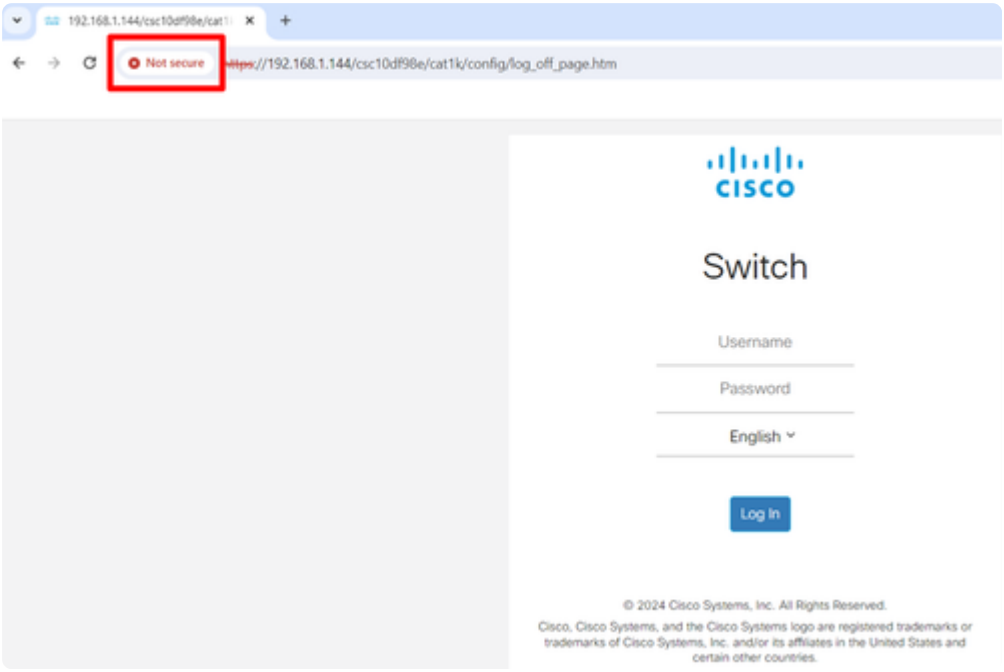


Er verschijnt een pop-upvenster met de details van de certificaatketen. In dit voorbeeld is het servercertificaat ondertekend door een tussenliggende CA met de naam "SMB Intermediate CA", zoals aangegeven door de Common Name (CN) van de uitgever in het servercertificaat. De uitgever van het intermediair certificaat is SMBRootCA.

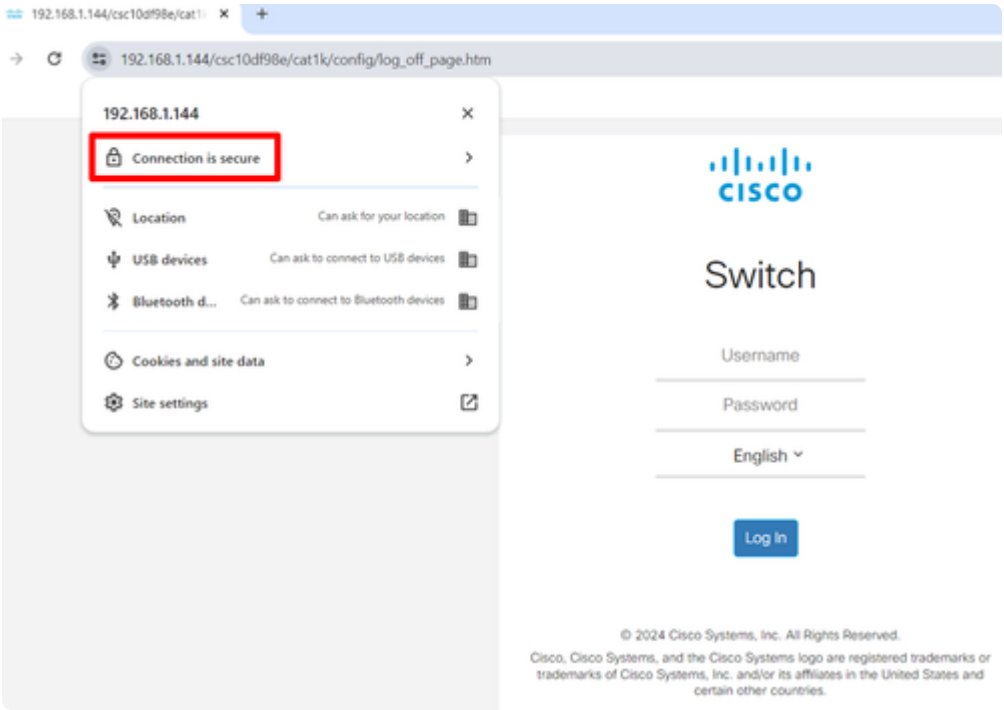


Voorbeeld certificaatketen

Wanneer switches standaard een zelf ondertekend certificaat gebruiken, resulteert dit in een clientsysteem, in dit geval een webbrowser, om een bericht weer te geven dat de verbinding niet beveiligd is.



Aan de andere kant, wanneer de certificaatketen is voltooid met een root-certificaat, tussenliggend certificaat en servercertificaat geïnstalleerd, geeft de browser aan dat de verbinding beveiligd is.



Conclusie

Daar ga je! Nu weet je hoe je tussencertificaten kunt uploaden en de certificaatketen in de Catalyst 1200 en 1300 switches kunt bekijken.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.