Certificats intermédiaires et chaîne de certificats dans les commutateurs Catalyst 1200 et 1300

Objectif

L'objectif de cet article est de passer en revue la fonctionnalité de certificat intermédiaire et la chaîne de certificats dans les commutateurs Catalyst 1200 et 1300 sur le microprogramme 4.1.3.36 et les étapes pour le configurer.

Périphériques pertinents | Version logicielle

- Commutateurs Catalyst 1200 |4.1.3.36
- Commutateurs Catalyst 1300 |4.1.3.36

Introduction

Les certificats sont utilisés dans un réseau pour fournir un accès sécurisé. Les certificats peuvent être auto-signés ou signés numériquement par une autorité de certification externe. Les composants d'une chaîne de certificats sont les suivants :

- Certificat CA racine : Le certificat de l'autorité de certification racine se trouve au sommet de la hiérarchie de la chaîne de certificats et il est auto-signé. Il s'agit de l'ancre de confiance ultime et elle est utilisée pour vérifier l'authenticité des certificats intermédiaires.
- Certificat(s) intermédiaire(s) : Un certificat intermédiaire est émis par une autorité de certification de niveau supérieur qui est soit une autre autorité de certification intermédiaire, soit une autorité de certification racine. Dans certains cas, plusieurs certificats intermédiaires peuvent former la chaîne de certificats. Normalement, l'autorité de certification intermédiaire est responsable de la signature des certificats du serveur.
- certificat du serveur: Ce certificat est émis pour un serveur spécifique, comme un site web par exemple. Il contient la clé publique du serveur et est signé par une autorité de certification. L'autorité de certification peut être une autorité de certification racine ou intermédiaire.

Lors de la connexion SSL/TLS entre le commutateur (serveur HTTPS) et un navigateur (client HTTPS), le commutateur présente son certificat signé. Le navigateur, ayant le certificat CA dans son magasin de confiance, utilise la clé publique de l'autorité de certification pour vérifier la signature sur le certificat du serveur. Ce processus établit l'authenticité de l'identité du serveur. Une fois la vérification effectuée, le serveur et le navigateur procèdent à l'échange de paramètres cryptographiques, ce qui permet le cryptage des données en transit entre eux, assurant ainsi une connexion sécurisée et authentifiée pour la transmission des données via HTTPS.

Bien que les certificats de serveur puissent être directement signés par le certificat d'autorité de certification racine, l'utilisation de certificats intermédiaires introduit une structure hiérarchique qui améliore le processus de signature. Les certificats intermédiaires servent d'intermédiaires entre le certificat du serveur et l'autorité de certification racine, offrant des avantages tels qu'une sécurité accrue grâce à l'isolation des compromissions de clés, une souplesse dans la gestion des certificats et la possibilité de déléguer le pouvoir de signature. Cette approche hiérarchique offre une meilleure évolutivité, facilite les processus de renouvellement des certificats et permet un contrôle plus granulaire de la révocation. En substance, l'utilisation de certificats intermédiaires enrichit le processus de signature en offrant une sécurité, une flexibilité et une gestion des certificats optimisées.

Dans le microprogramme 4.1.3.36 des commutateurs Catalyst 1200 et 1300, vous pouvez désormais importer des certificats intermédiaires et afficher la chaîne de certificats d'un certificat de serveur installé. Les commutateurs Catalyst prennent en charge les fonctionnalités suivantes relatives au certificat intermédiaire et à la chaîne de certificats du serveur HTTPS :

- Installation d'un ou plusieurs certificats intermédiaires.
- Inclusion des certificats intermédiaires dans la connexion TLS avec le client HTTPS
- Affichage des certificats intermédiaires
- Affichage de la chaîne de certificats des certificats du serveur HTTPS du périphérique

Continuez à lire pour en savoir plus !

Table des matières

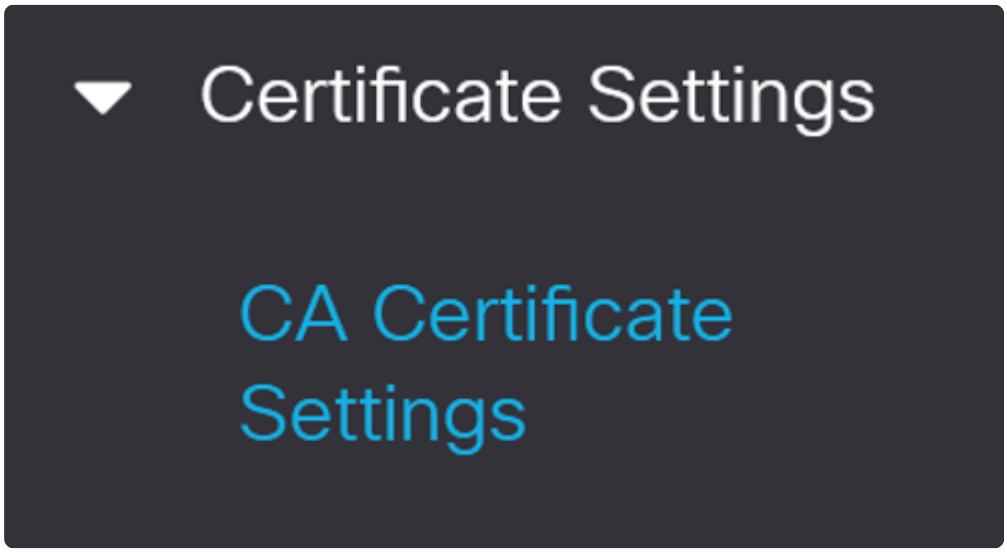
Importation d'un certificat intermédiaire

Dans la version 4.1.3.36 du microprogramme des commutateurs Catalyst 1200 et 1300, vous avez la possibilité d'importer des certificats intermédiaires à l'aide de l'interface utilisateur Web du commutateur.

> **Note:**
> Sur la base de l'autorité de certification, le fournisseur du certificat fournira le certificat racine et le certificat intermédiaire sous la forme d'un ensemble pour prendre en charge le certificat du serveur.

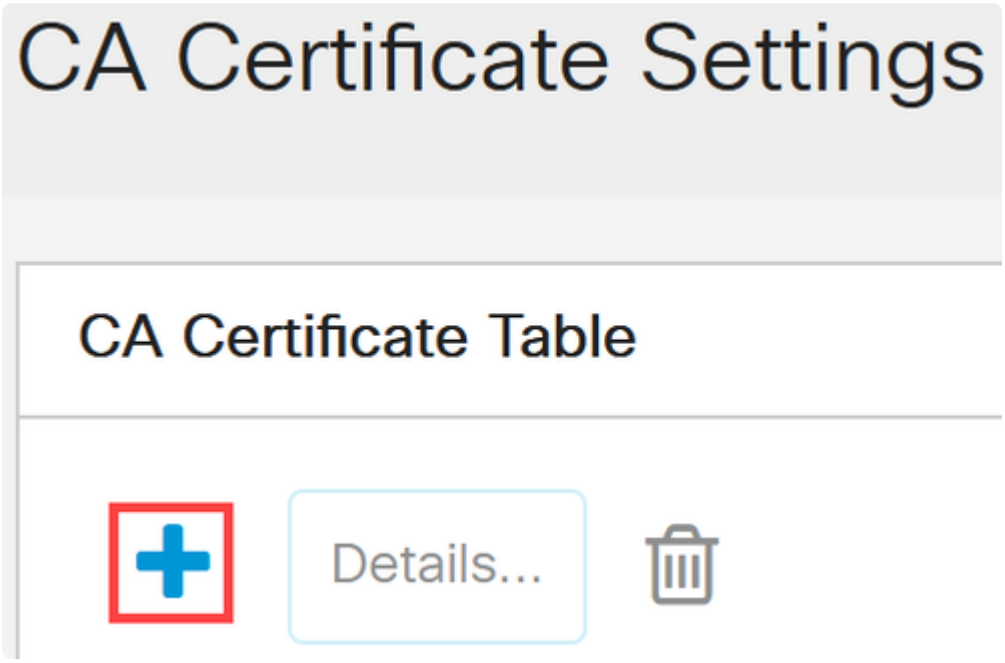
Étape 1

Sous l'affichage Avancé, accédez à Sécurité > Paramètres du certificat > Paramètres du certificat de l'autorité de certification dans le volet de navigation.



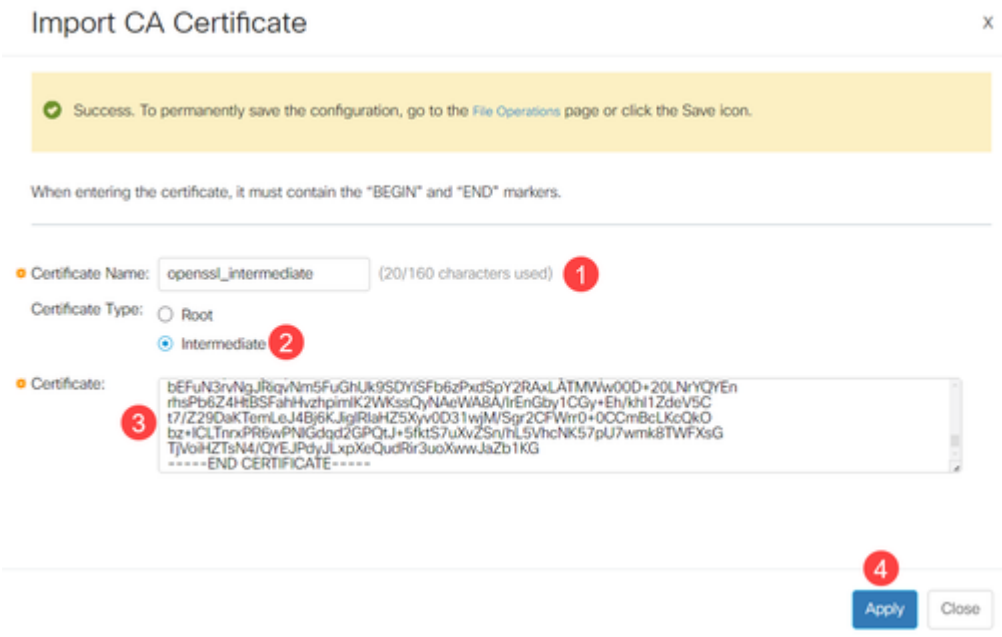
Étape 2

Cliquez sur l'icône plus pour importer un certificat.



Étape 3

Entrez le Nom du certificat, sélectionnez Intermédiaire comme type de certificat, collez le certificat dans la zone prévue à cet effet, puis cliquez sur Appliquer.



Une notification de réussite s'affiche en haut de l'écran.

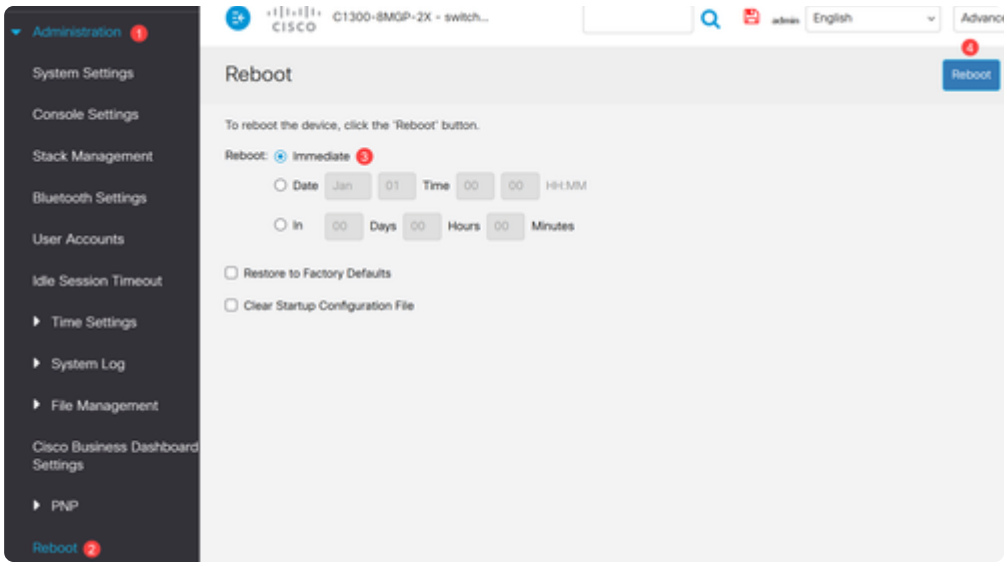
> **Note:**
> Un message d'erreur s'affiche si le type de certificat ne correspond pas au certificat en cours d'installation.

Étape 4

Cliquez sur l'icône Save en haut de l'écran.

Étape 5

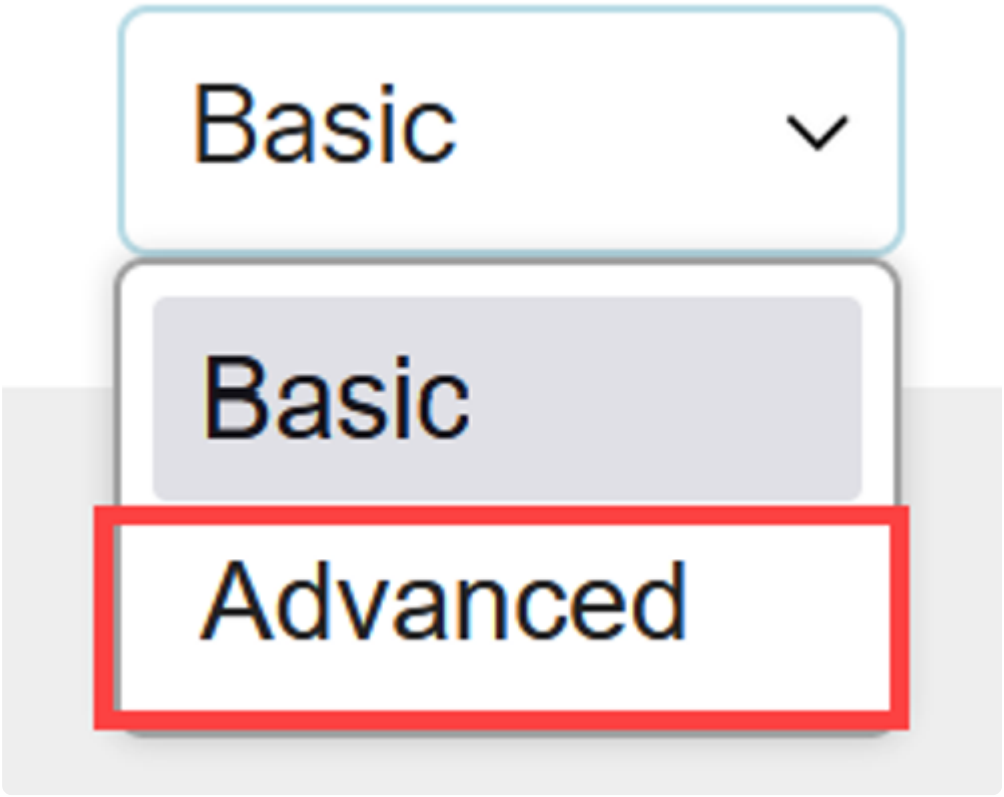
Redémarrez le commutateur pour que toutes les modifications prennent effet. Pour redémarrer, accédez au menu Administration > Reboot et assurez-vous que l'option Immediate reboot est sélectionnée. Cliquez sur le bouton Redémarrer.



Chaîne De Certificats

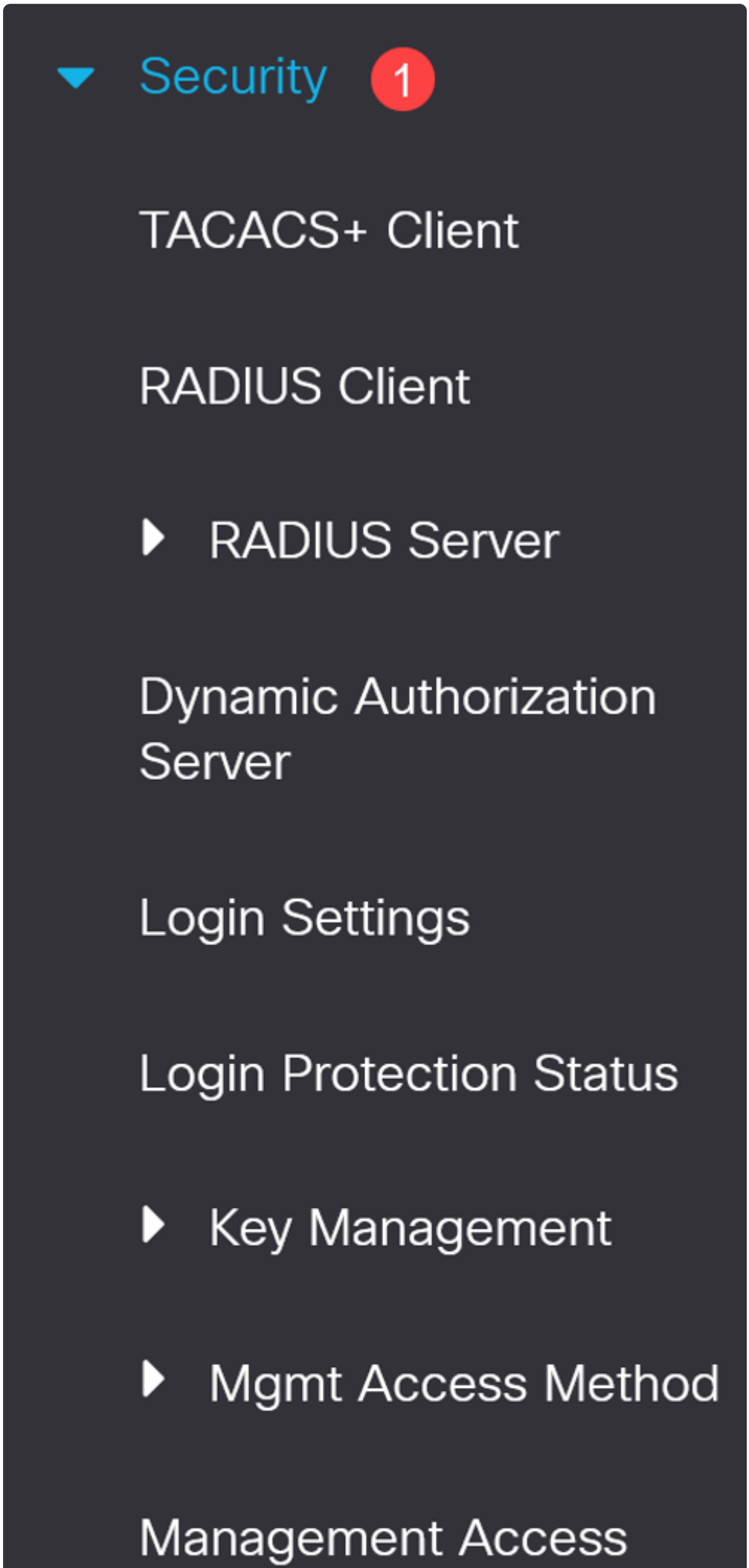
Étape 1

Connectez-vous au commutateur Catalyst 1300 et passez en mode Advanced à partir du menu déroulant dans l'angle supérieur droit de l'interface utilisateur.



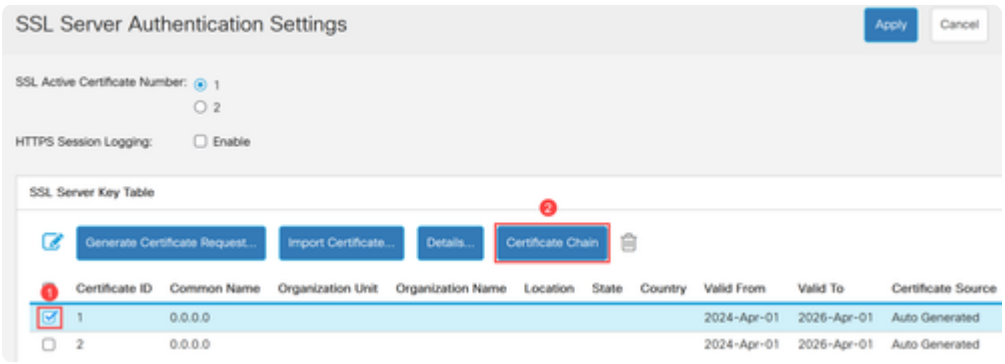
Étape 2

Accédez à Security > SSL Server > SSL Server Authentication Settings dans le volet de navigation.

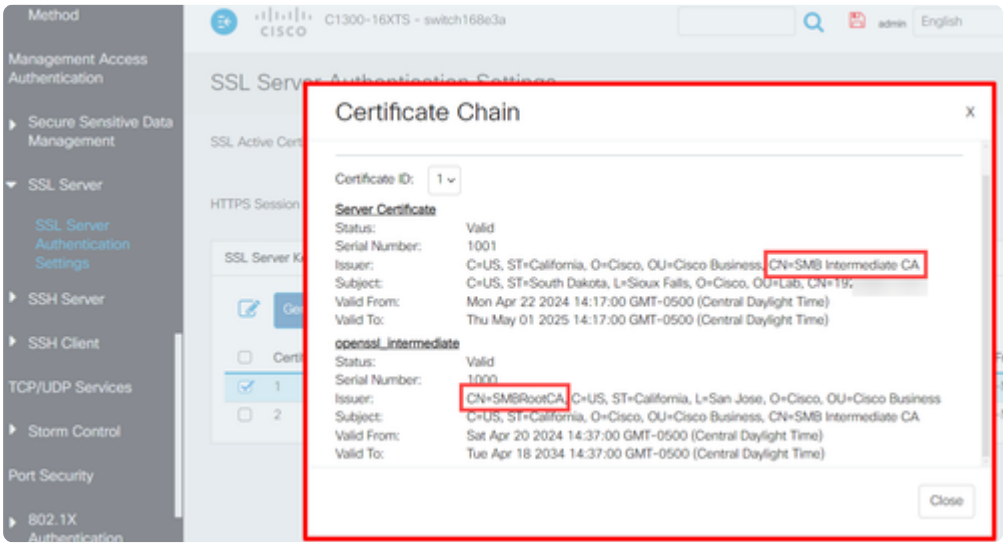

Security
1
TACACS+ Client
RADIUS Client
RADIUS Server
Dynamic Authorization Server
Login Settings
Login Protection Status
Key Management
Mgmt Access Method
Management Access

Étape 3

Sélectionnez le certificat dans le tableau, puis cliquez sur le bouton Certificate Chain.

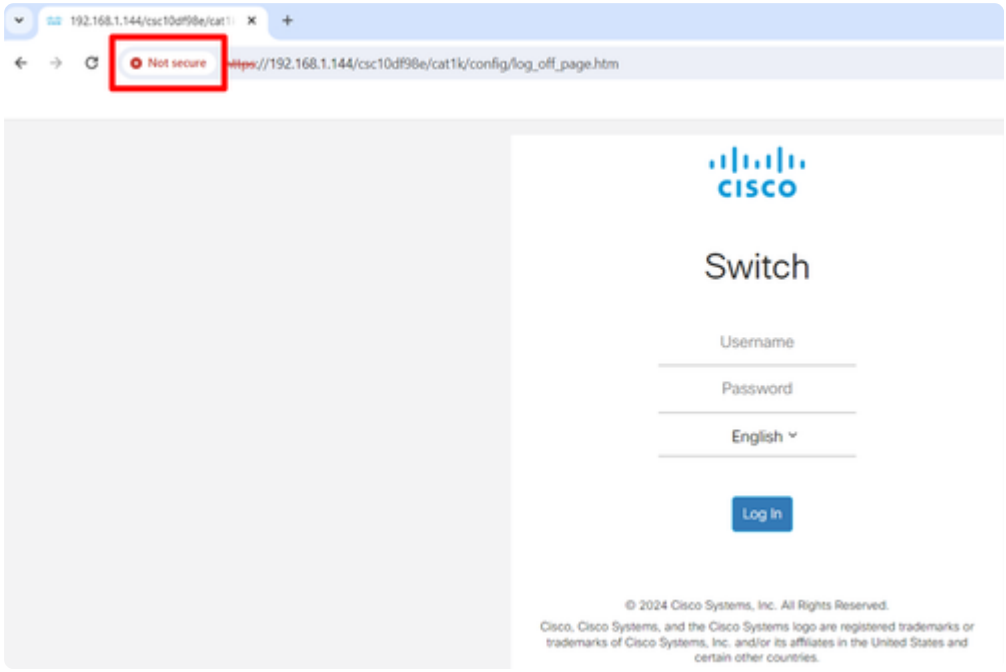


Une fenêtre contextuelle s'affiche avec les détails de la chaîne de certificats. Dans cet exemple, le certificat du serveur a été signé par une autorité de certification intermédiaire nommée « SMB Intermediate CA », comme indiqué par le nom commun (CN) de l'émetteur dans le certificat du serveur. L'émetteur du certificat intermédiaire est SMBRootCA.

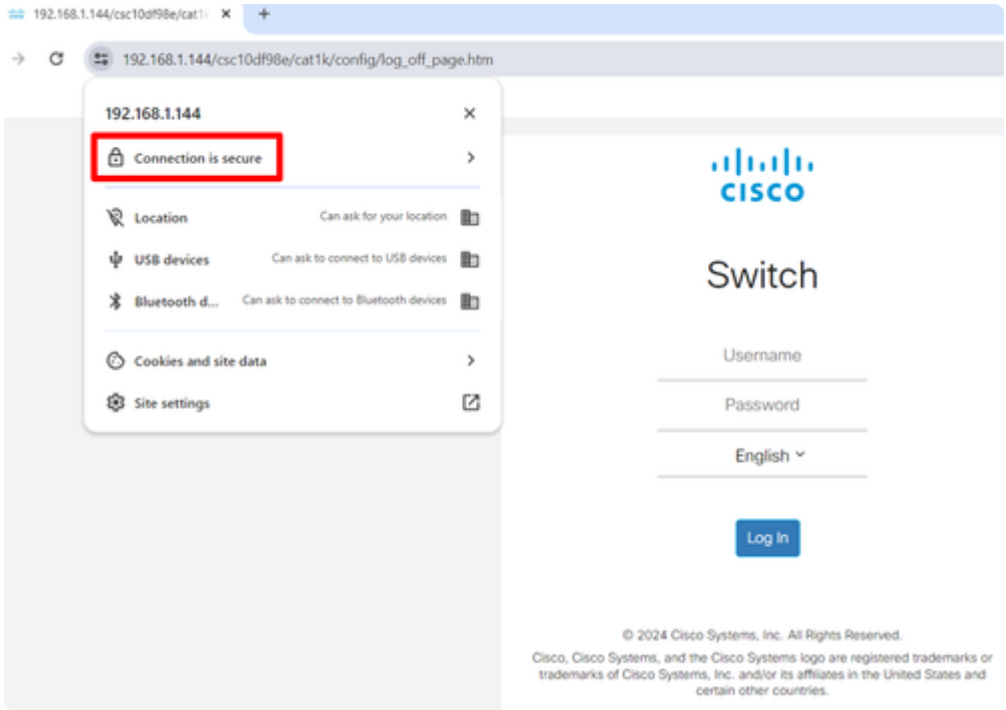


Exemple de chaîne de certificats

Lorsque les commutateurs utilisent un certificat auto-signé par défaut, cela se produit avec un système client, un navigateur Web dans ce cas, pour afficher un message indiquant que la connexion n'est pas sécurisée.



D'autre part, lorsque la chaîne de certificats est terminée avec un certificat racine, un certificat intermédiaire et un certificat de serveur installés, le navigateur affiche que la connexion est sécurisée.



Conclusion

Et voilà ! Allez ! Vous savez maintenant comment télécharger des certificats intermédiaires et afficher la chaîne de certificats dans les commutateurs Catalyst 1200 et 1300.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.