Intermediate Certificates and Certificate Chain in Catalyst 1200 and 1300 Switches

Objective

The objective of this article is to go over the intermediate certificate feature and certificate chain in Catalyst 1200 and 1300 switches on firmware 4.1.3.36 and the steps to configure it.

Applicable Devices | Software Version

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

Introduction

Certificates are used in a network to provide secure access. Certificates can be self-signed or digitally signed by an external Certificate Authority (CA). The components of a certificate chain include:

- *Root CA Certificate*: The root CA, or CA certificate is at the top of the hierarchy for the certificate chain, and it is self-signed. It is the ultimate trust anchor and is used to verify the authenticity of intermediate certificates.
- *Intermediate Certificate(s)*: An intermediate certificate is issued by a higher-level CA that is either another intermediate CA or a root CA. In some cases, there can be multiple intermediate certificates forming the certificate chain. Normally, the intermediate CA is responsible for signing server certificates.
- *Server Certificate*: This certificate is issued for a specific server, like a website for example. It contains the public key of the server and is signed by a CA. The CA could be a root or intermediate CA.

During the SSL/TLS handshake between the switch (HTTPS server) and a browser (HTTPS client), the switch presents its signed certificate. The browser, having the CA certificate in its trusted store, uses the CA's public key to verify the signature on the server certificate. This process establishes authenticity of the server's identity. Once verified, the server and browser proceed to exchange cryptographic parameters, enabling the encryption of data in transit between them, ensuring a secure and authenticated connection for data transmission over HTTPS.

While server certificates can be directly signed by the root CA certificate, the use of intermediate certificates introduces a hierarchical structure that enhances the signing process. Intermediate certificates act as intermediaries between the server certificate and the root CA, offering benefits such as increased security through isolation of key compromises, flexibility in certificate management, and the ability to delegate signing authority. This hierarchical approach provides improved scalability, eases certificate renewal processes, and allows for more granular control over revocation. In essence, employing intermediate certificates enriches the signing

process by providing enhanced security, flexibility, and streamlined certificate management.

In firmware 4.1.3.36 of Catalyst 1200 and 1300 switches, you can now import intermediate certificates and view the certificate chain of an installed server certificate. The Catalyst switches support the following functionalities related to intermediate certificate and HTTPS server certificate chain:

- Installation of one or more intermediate certificates.
- Including the intermediate certificate(s) in the TLS handshake with the HTTPS client
- Display of intermediate certificates
- Display of the certificate chain of the device's HTTPS server certificates

Keep reading to find out more!

Table of Contents

Importing an Intermediate Certificate

In firmware version 4.1.3.36 of the Catalyst 1200 and 1300 switches, you have the option to import intermediate certificates using the web user interface of the switch.

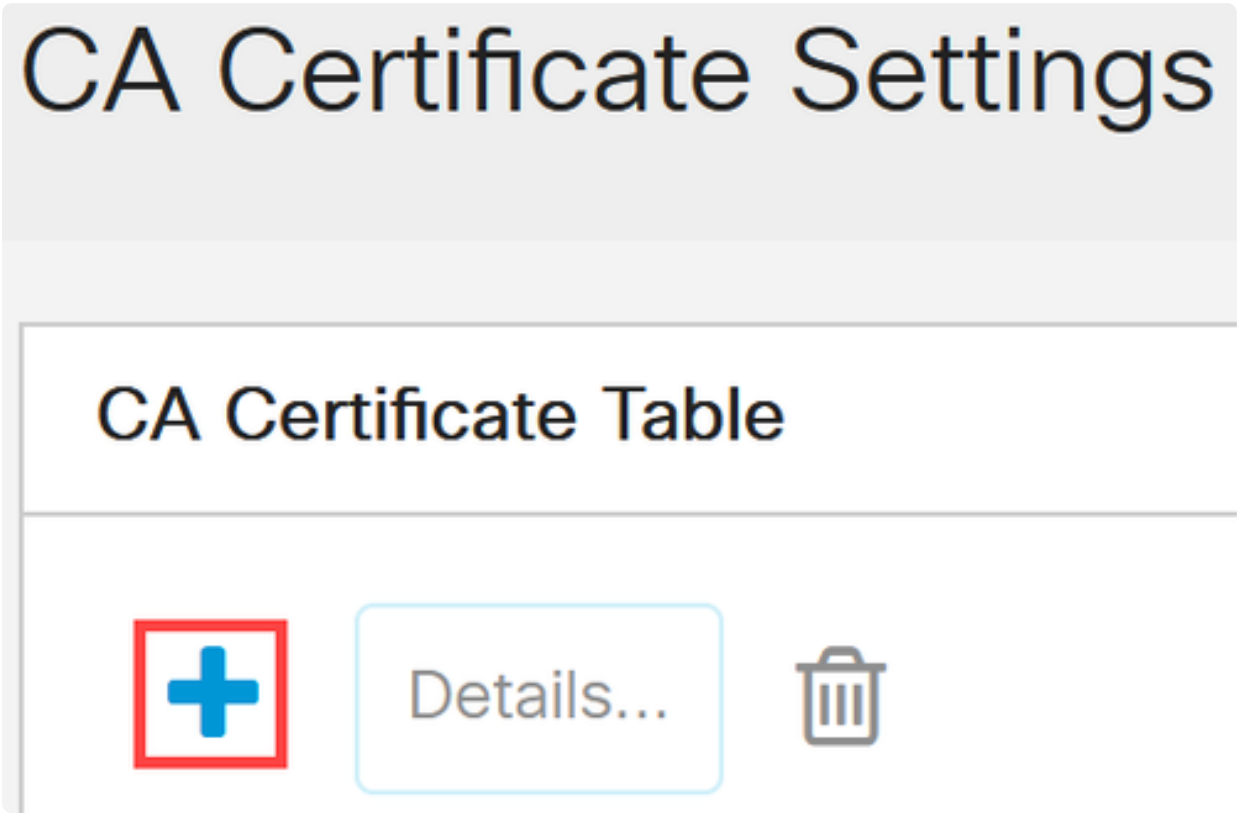
> **Note:**
> Based on the CA, the certificate vendor will provide the root certificate and intermediate certificate as a bundle to support the server certificate.

Step 1

Under **Advanced** view, navigate to **Security > Certificate Settings > CA Certificate Settings** in the navigation pane.

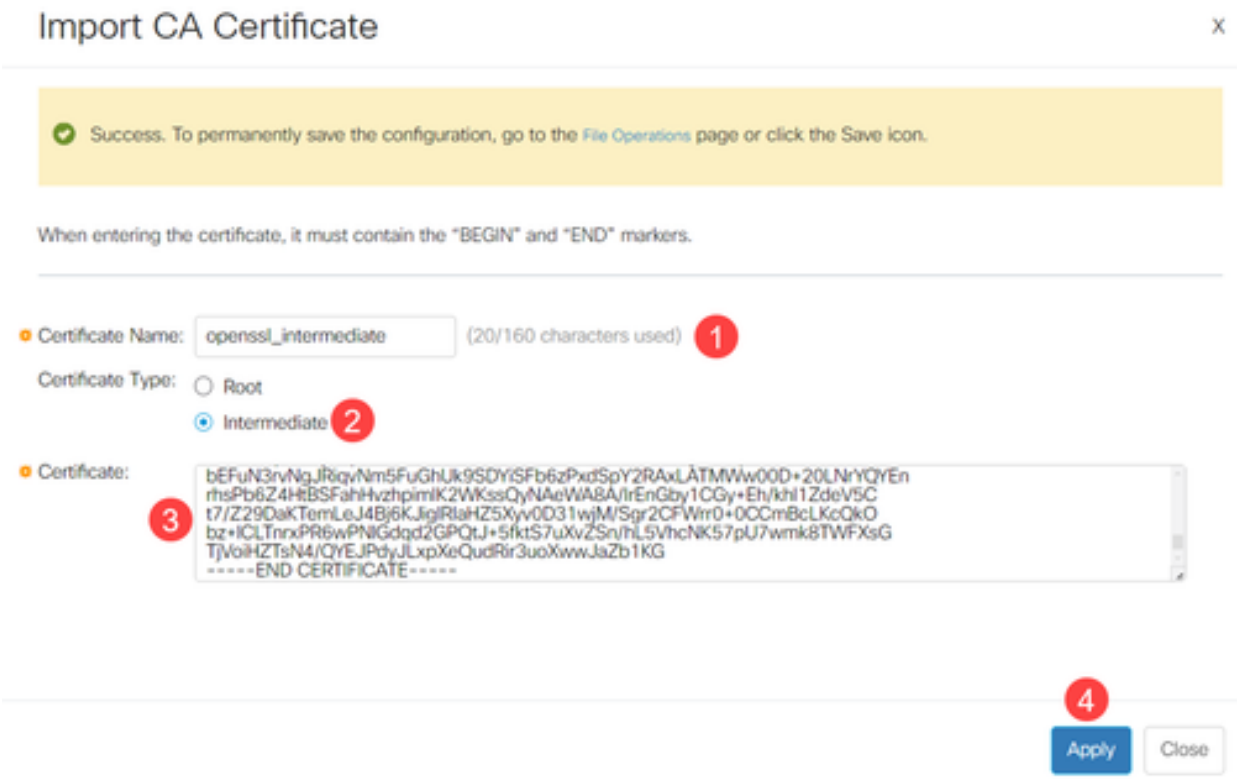
Step 2

Click on the **plus icon** to import a certificate.



Step 3

Enter the *Certificate Name*, select **Intermediate** as the certificate type, paste the certificate in the box provided, and then click **Apply**.



A success notification will appear at the top of the screen.

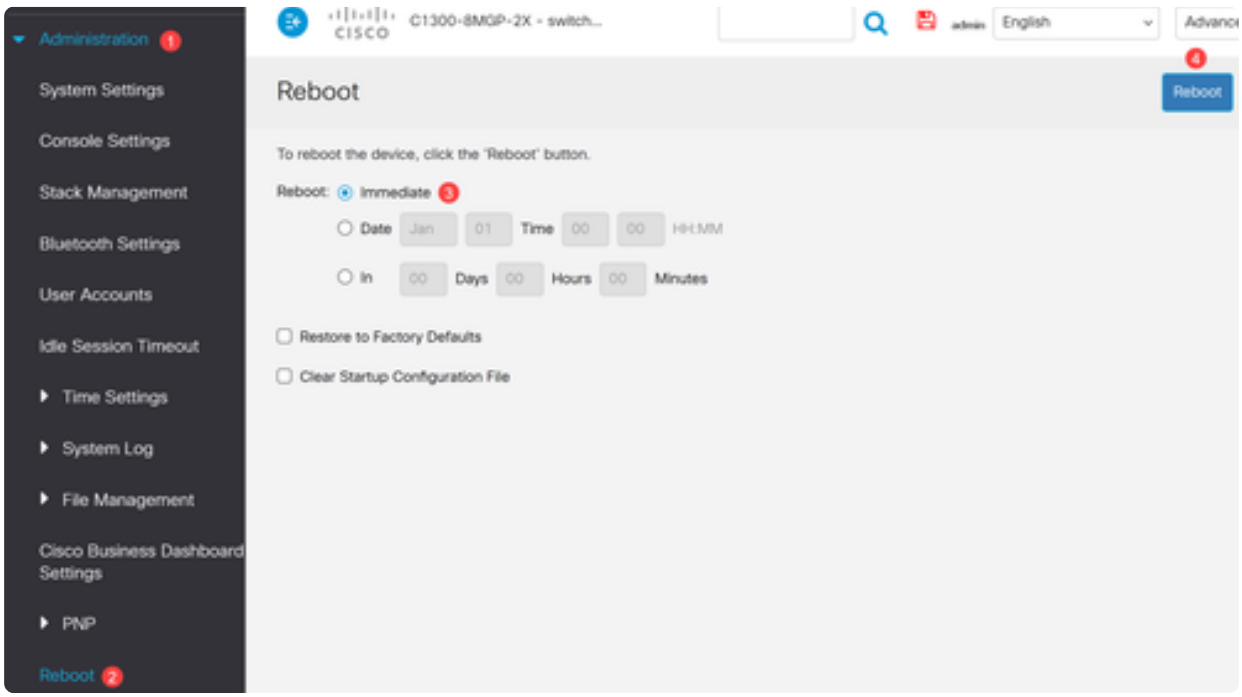
> **Note:**
> An error message will occur if the certificate type does not match the certificate that is being installed.

Step 4

Click the **Save** icon at the top of the screen.

Step 5

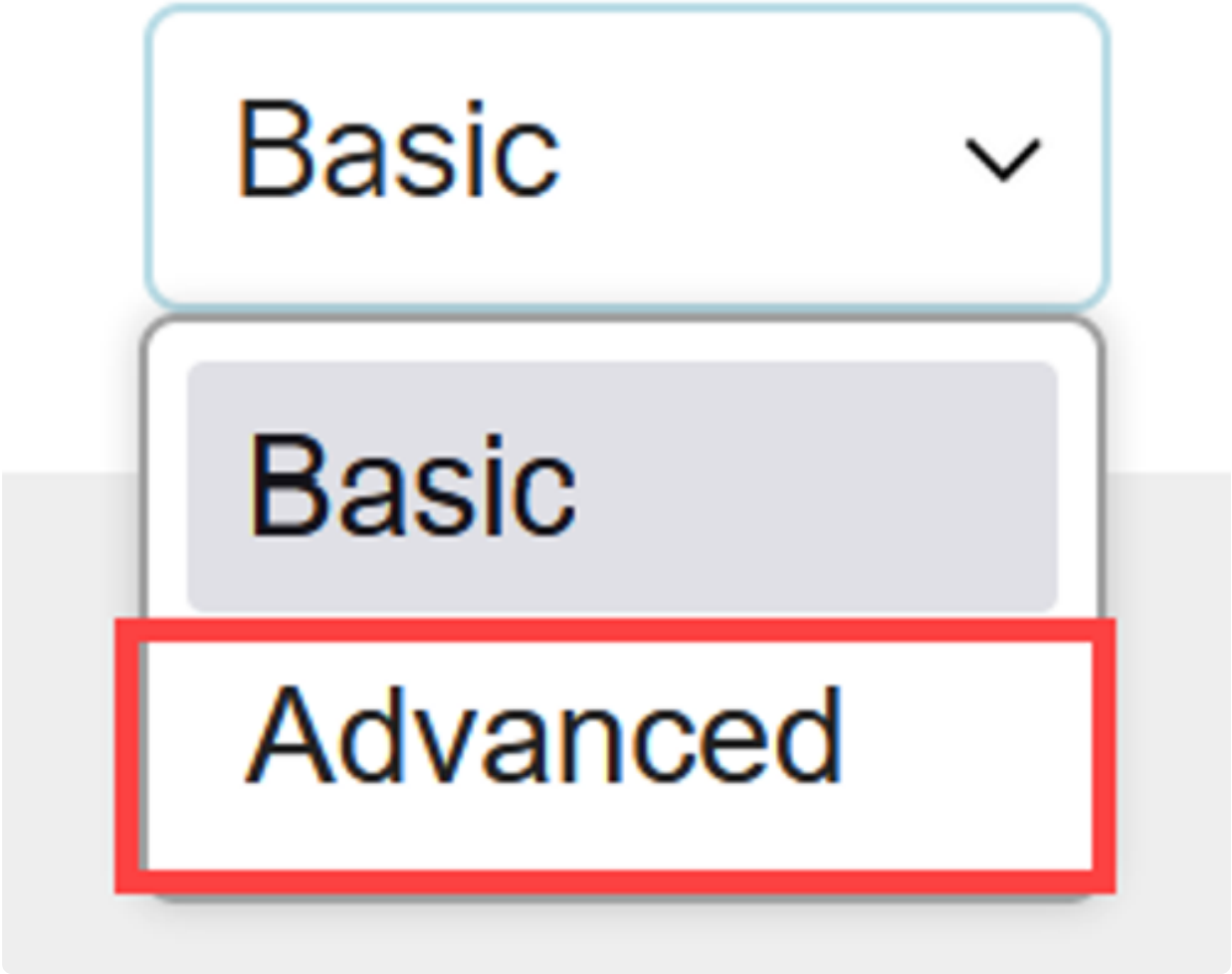
Reboot the switch for all the changes to take effect. To reboot, navigate to the **Administration > Reboot** menu and make sure the **Immediate** reboot option is selected. Click the Reboot button.



Certificate Chain

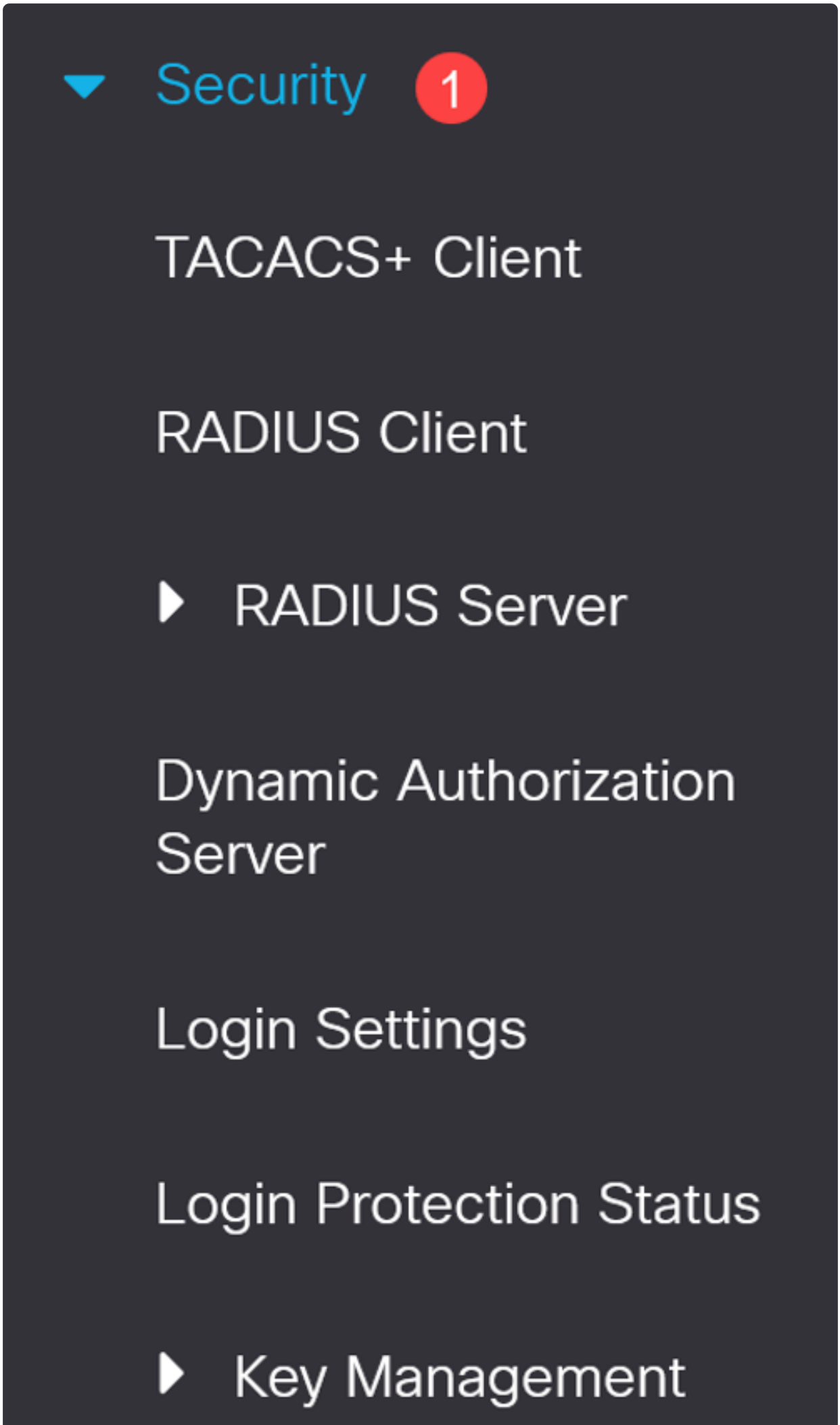
Step 1

Login to the Catalyst 1300 switch and switch to **Advanced** view from the drop-down menu at the top right-hand corner of the user interface.



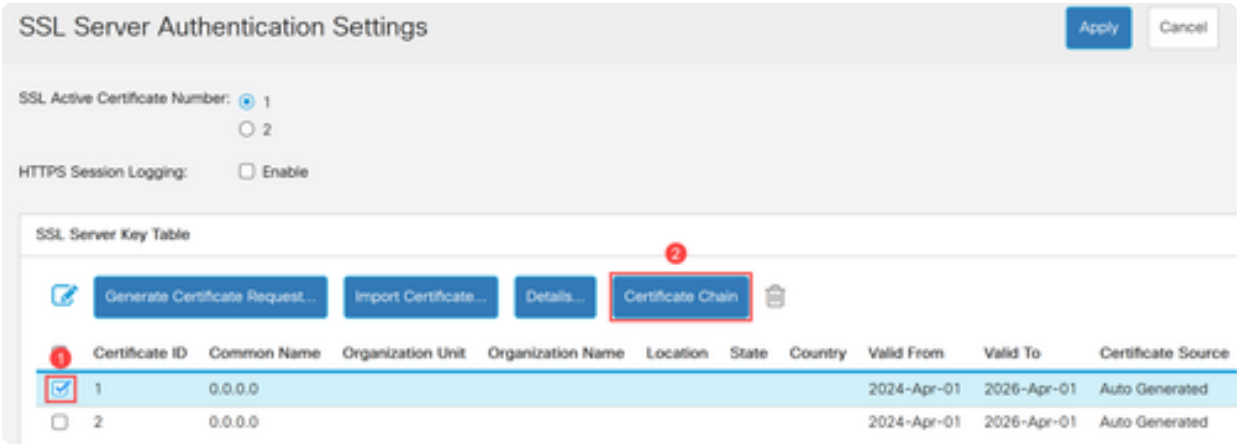
Step 2

Navigate to **Security > SSL Server > SSL Server Authentication Settings** in the navigation pane.

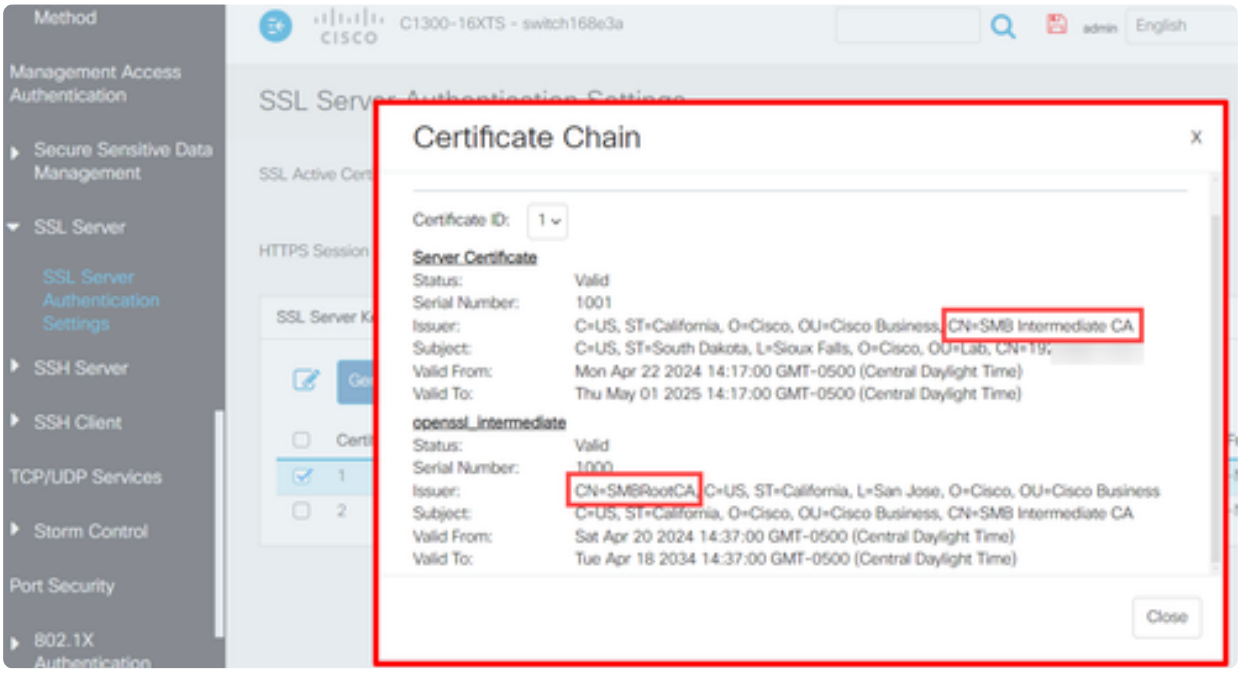

Security
1
TACACS+ Client
RADIUS Client
RADIUS Server
Dynamic Authorization Server
Login Settings
Login Protection Status
Key Management

Step 3

Select the certificate from the table and then click on **Certificate Chain** button.



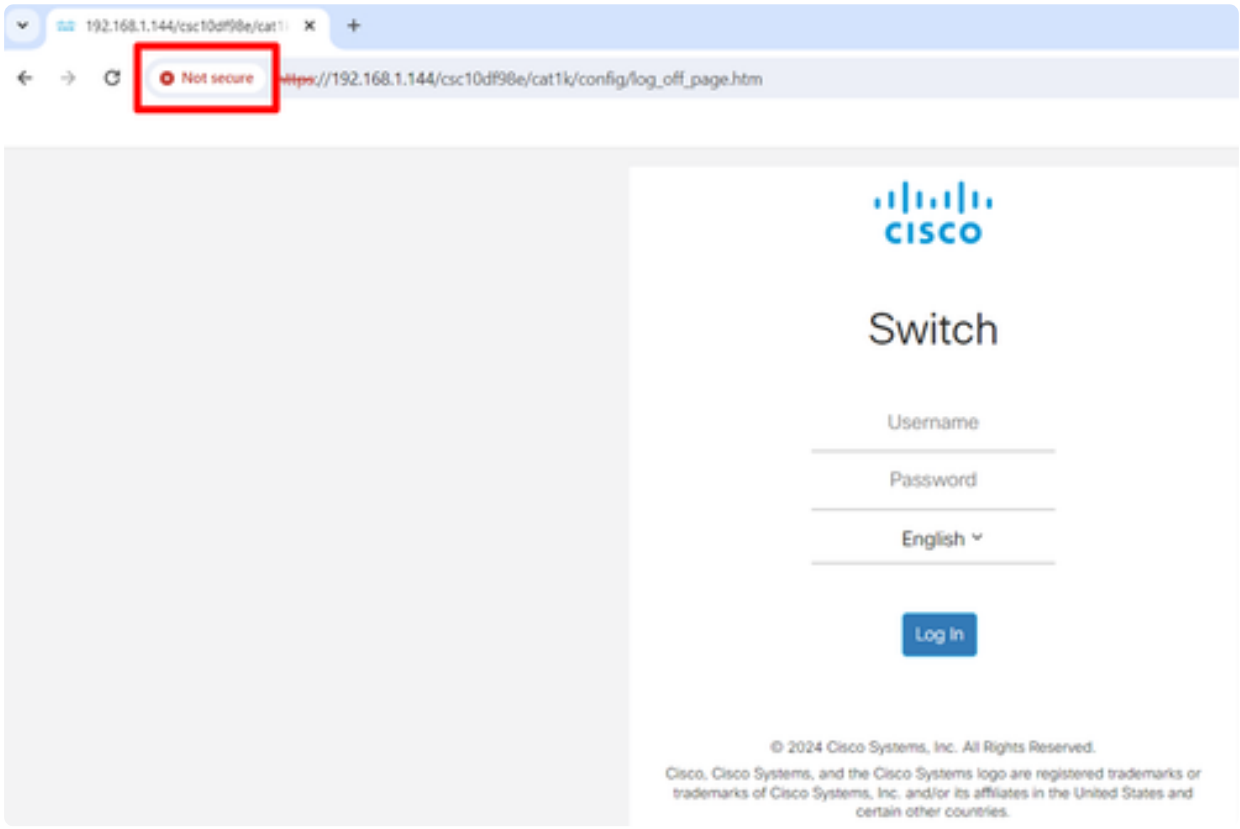
A pop-window will appear showing the details of the certificate chain. In this example, the server certificate was signed by an intermediate CA named "*SMB Intermediate CA*", as noted by the Common Name (CN) of the issuer in the server certificate. The issuer of the intermediate certificate is *SMBRootCA.*



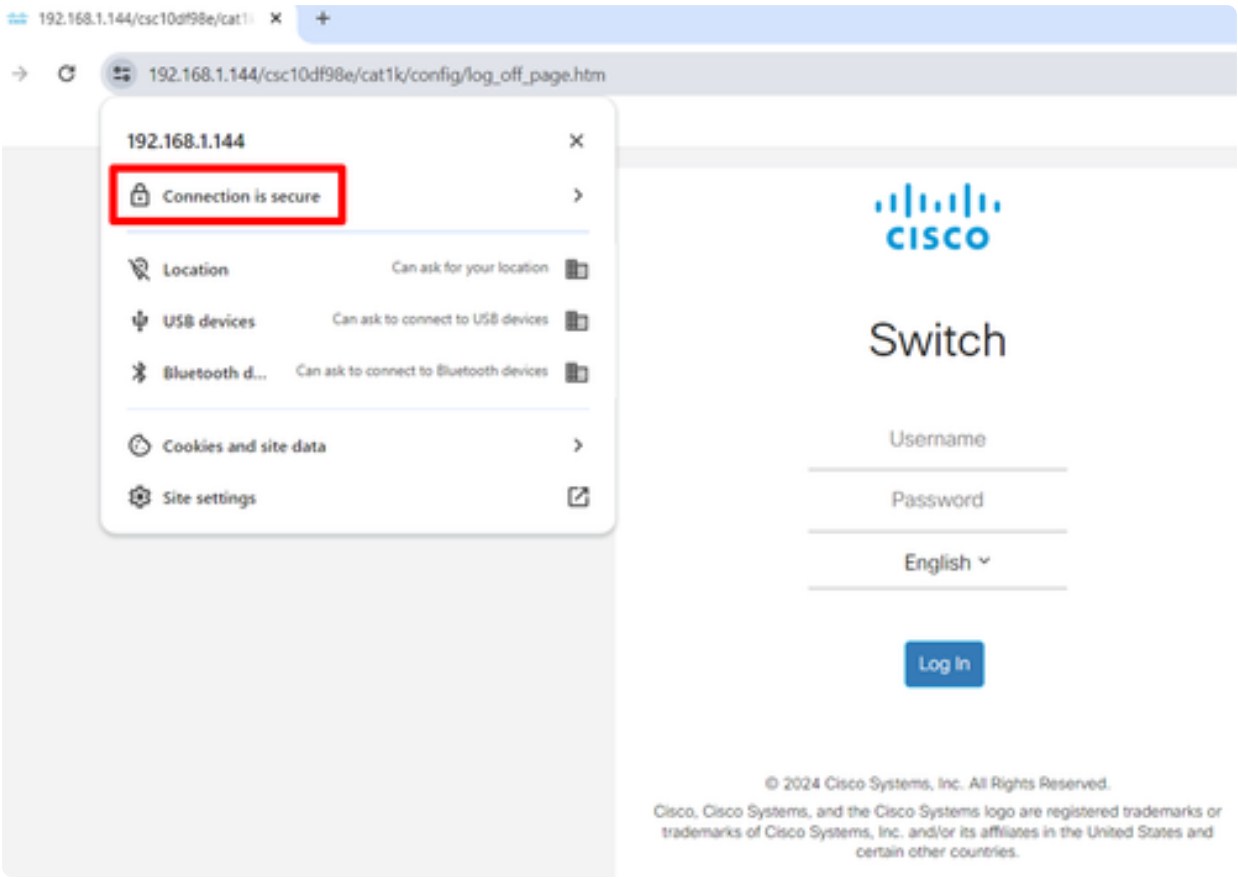
Certificate Chain Example

When switches use a self-signed certificate by default, this will result with a client system, a

web browser in this case, to display a message that the connection is *Not Secure*.



On the other hand, when the certificate chain is complete with a root certificate, intermediate certificate, and server certificate installed, the browser will display that the connection is *Secure*.



Conclusion

There you go! Now you know how to upload intermediate certificates and view the certificate chain in the Catalyst 1200 and 1300 switches.