Certificati intermedi e catena di certificati sugli switch Catalyst 1200 e 1300

Obiettivo

L'obiettivo di questo articolo è esaminare la funzionalità e la catena di certificati intermedia negli switch Catalyst 1200 e 1300 sul firmware 4.1.3.36 e i passaggi per configurarlo.

Dispositivi interessati | Versione software

- Catalyst 1200 Switch |4.1.3.36
- Catalyst 1300 Switch |4.1.3.36

Introduzione

I certificati vengono utilizzati in una rete per fornire un accesso sicuro. I certificati possono essere autofirmati o firmati digitalmente da un'Autorità di certificazione (CA) esterna. I componenti di una catena di certificati includono:

- Certificato CA radice: La CA radice, o certificato CA, si trova nella parte superiore della gerarchia per la catena di certificati ed è autofirmato. Si tratta del trust anchor finale e viene utilizzato per verificare l'autenticità dei certificati intermedi.
- Certificati intermedi: Un certificato intermedio viene emesso da una CA di livello superiore, che può essere un'altra CA intermedia o una CA radice. In alcuni casi possono esistere più certificati intermedi che formano la catena di certificati. In genere, la CA intermedia è responsabile della firma dei certificati del server.
- Certificato server: Questo certificato viene rilasciato per un server specifico, ad esempio un sito Web. Contiene la chiave pubblica del server ed è firmato da una CA. La CA può essere una CA radice o intermedia.

Durante l'handshake SSL/TLS tra lo switch (server HTTPS) e un browser (client HTTPS), lo switch presenta il proprio certificato firmato. Il browser, che dispone del certificato CA nell'archivio attendibile, utilizza la chiave pubblica della CA per verificare la firma sul certificato del server. Questo processo stabilisce l'autenticità dell'identità del server. Una volta verificato, il server e il browser procedono allo scambio dei parametri di crittografia, abilitando la crittografia dei dati in transito tra di essi, garantendo una connessione sicura e autenticata per la trasmissione dei dati tramite HTTPS.

Mentre i certificati server possono essere firmati direttamente dal certificato CA radice,

l'utilizzo dei certificati intermedi introduce una struttura gerarchica che migliora il processo di firma. I certificati intermedi fungono da intermediari tra il certificato del server e la CA radice, offrendo vantaggi quali una maggiore sicurezza tramite l'isolamento dei compromessi chiave, flessibilità nella gestione dei certificati e la possibilità di delegare l'autorità di firma. Questo approccio gerarchico offre una maggiore scalabilità, semplifica i processi di rinnovo dei certificati e consente un controllo più granulare sulle revoche. In sostanza, l'utilizzo di certificati intermedi arricchisce il processo di firma fornendo maggiore sicurezza, flessibilità e gestione semplificata dei certificati.

Nel firmware 4.1.3.36 degli switch Catalyst 1200 e 1300, è ora possibile importare certificati intermedi e visualizzare la catena di certificati di un certificato server installato. Gli switch Catalyst supportano le seguenti funzionalità relative ai certificati intermedi e alla catena di certificati del server HTTPS:

- Installazione di uno o più certificati intermedi.
- Inclusione dei certificati intermedi nell'handshake TLS con il client HTTPS
- Visualizzazione dei certificati intermedi
- Visualizzazione della catena di certificati dei certificati server HTTPS del dispositivo

Continua a leggere per saperne di più!

Sommario

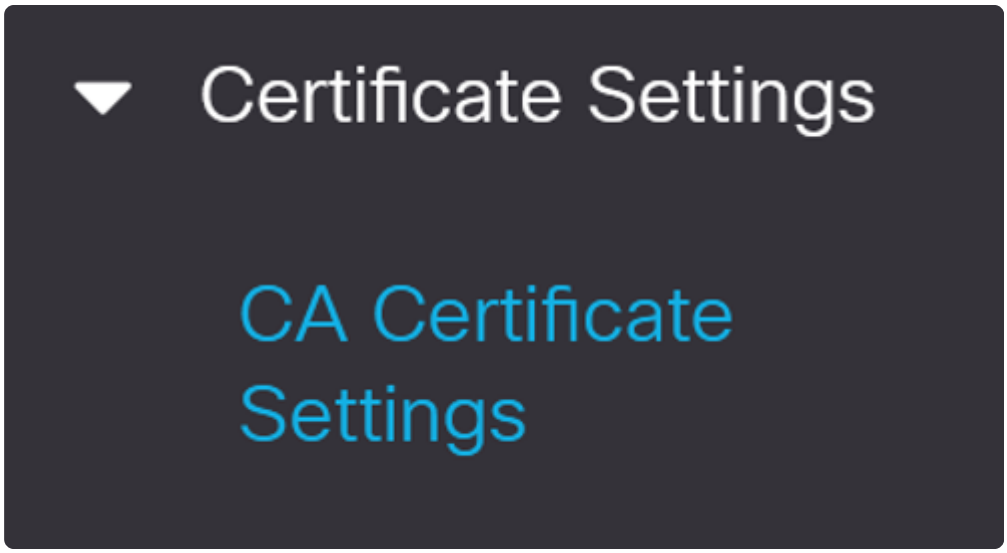
Importazione di un certificato intermedio

Nel firmware versione 4.1.3.36 degli switch Catalyst 1200 e 1300, è possibile importare i certificati intermedi usando l'interfaccia utente Web dello switch.

> **Note:**
> In base alla CA, il fornitore del certificato fornirà il certificato radice e il certificato intermedio come bundle per il supporto del certificato del server.

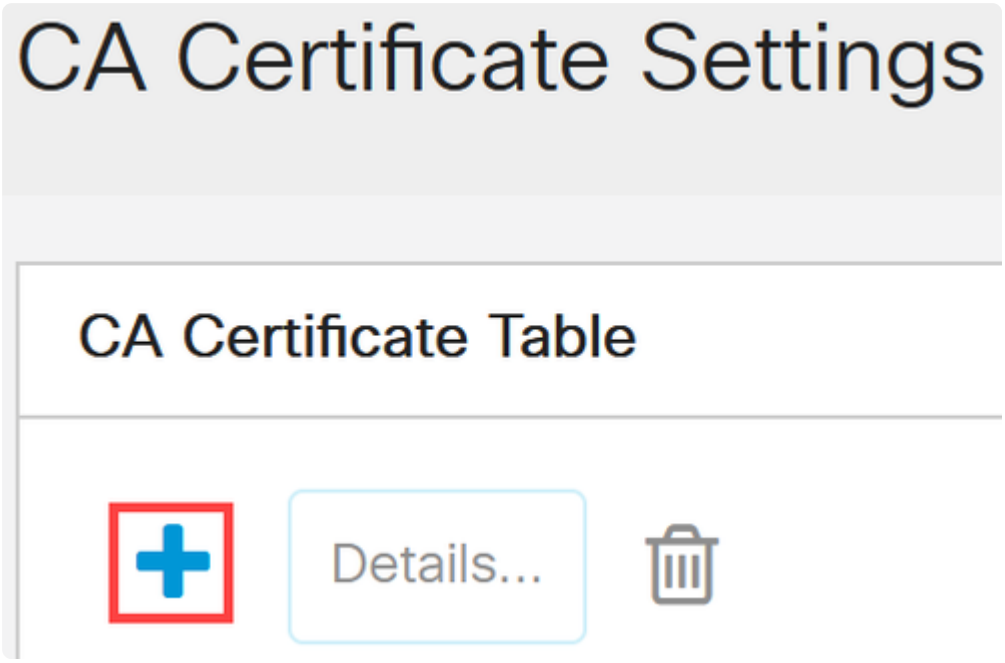
Passaggio 1

In visualizzazione Avanzata, passare a Protezione > Impostazioni certificato > Impostazioni certificato CA nel riquadro di navigazione.



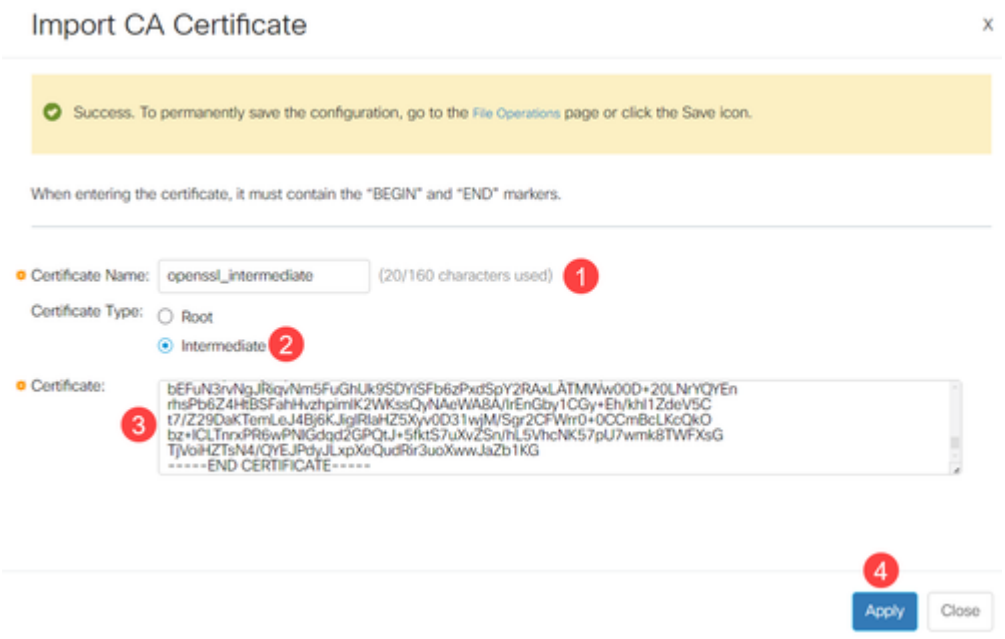
Passaggio 2

Fare clic sull'icona più per importare un certificato.



Passaggio 3

Immettere il Nome certificato, selezionare Intermedio come tipo di certificato, incollare il certificato nella casella apposita e quindi fare clic su Applica.



Nella parte superiore dello schermo verrà visualizzata una notifica di operazione riuscita.

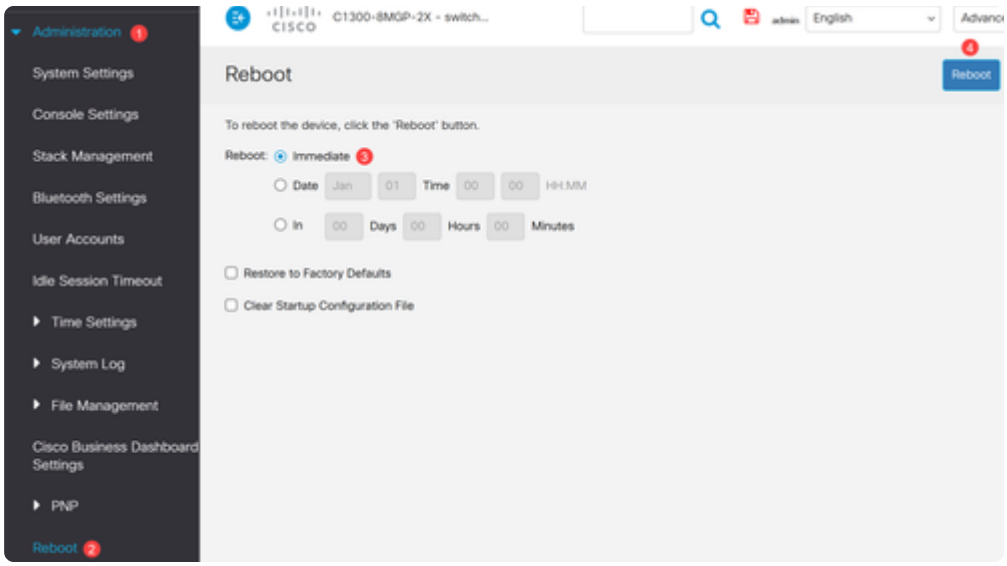
> **Note:**
> Se il tipo di certificato non corrisponde al certificato da installare, verrà visualizzato un messaggio di errore.

Passaggio 4

Fare clic sull'icona Save (Salva) nella parte superiore dello schermo.

Passaggio 5

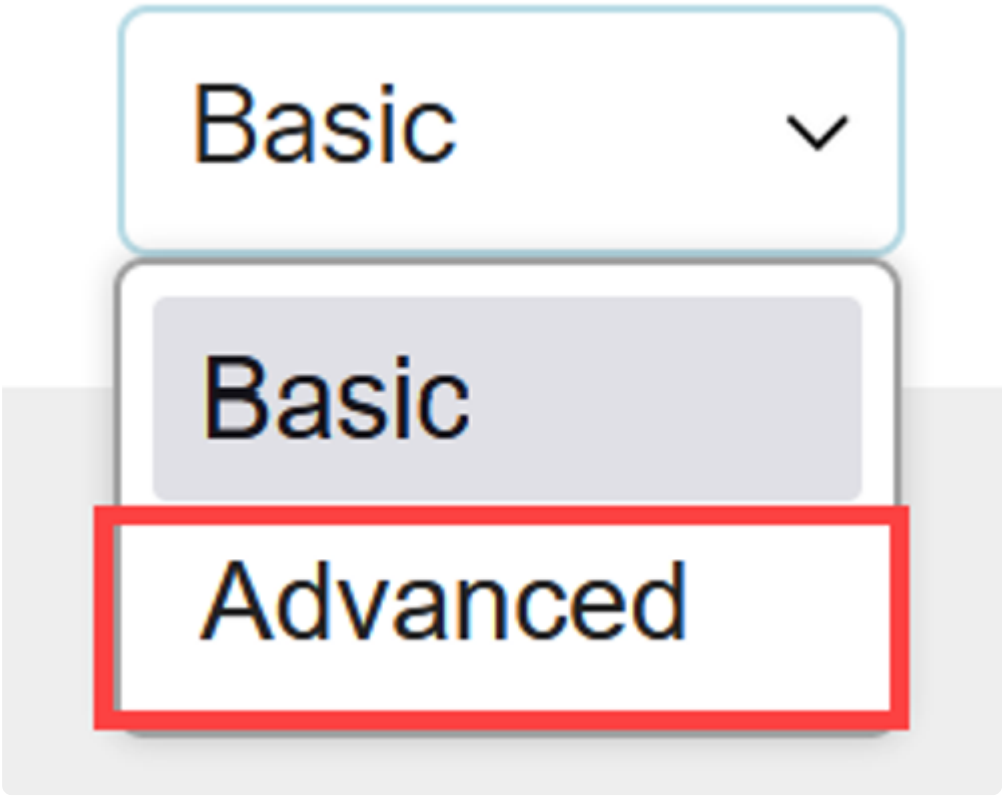
Riavviare lo switch per rendere effettive tutte le modifiche. Per riavviare, selezionare il menu Amministrazione > Riavvia e assicurarsi che l'opzione Immediate reboot sia selezionata. Fare clic sul pulsante Riavvia.



Catena di certificati

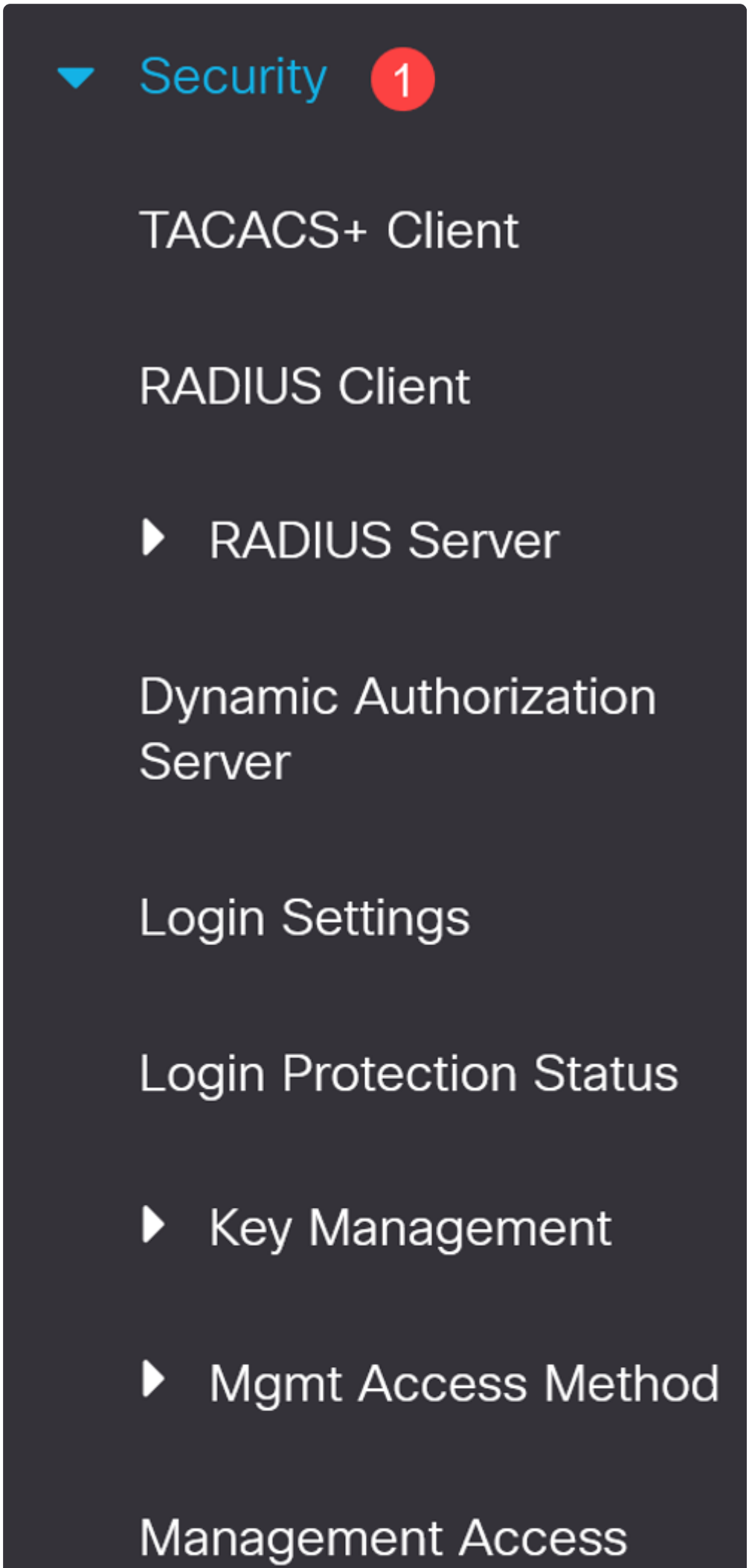
Passaggio 1

Accedere allo switch Catalyst 1300 e passare alla visualizzazione avanzata dal menu a discesa nell'angolo in alto a destra dell'interfaccia utente.



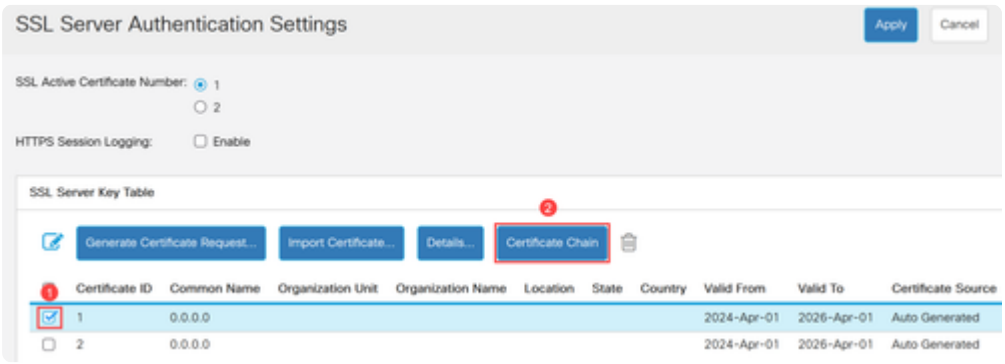
Passaggio 2

Nel riquadro di navigazione, selezionare Sicurezza > Server SSL > Impostazioni autenticazione server SSL.

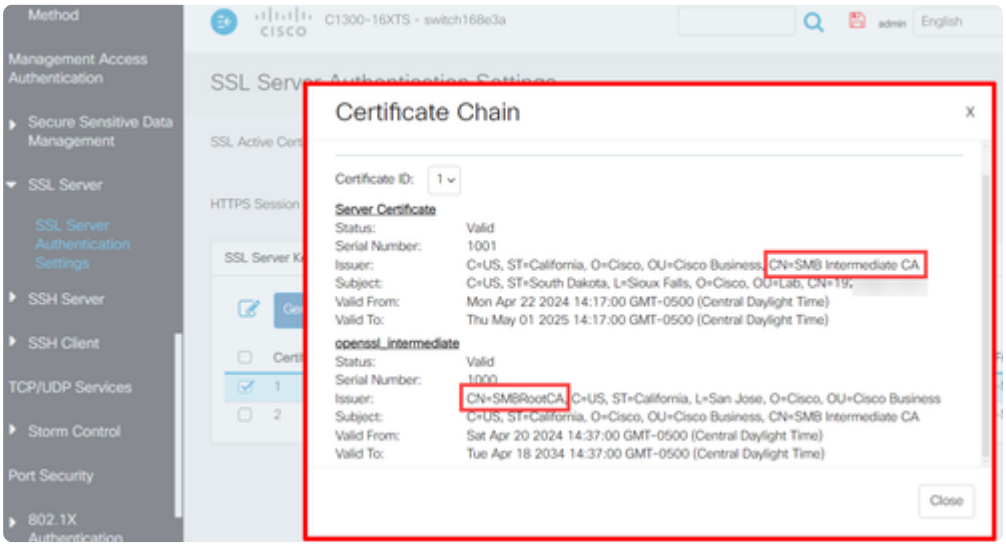

Security
1
TACACS+ Client
RADIUS Client
RADIUS Server
Dynamic Authorization Server
Login Settings
Login Protection Status
Key Management
Mgmt Access Method
Management Access

Passaggio 3

Selezionare il certificato dalla tabella, quindi fare clic sul pulsante Catena di certificati.

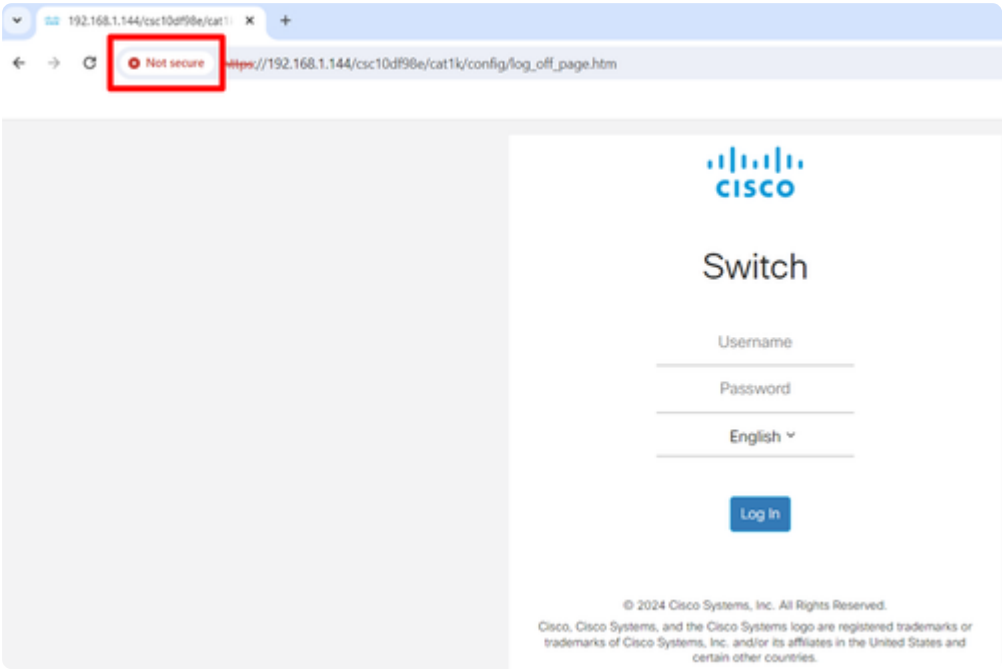


Verrà visualizzata una finestra popup con i dettagli della catena di certificati. In questo esempio, il certificato server è stato firmato da una CA intermedia denominata "SMB Intermediate CA", come indicato dal nome comune (CN) dell'autorità emittente nel certificato server. L'autorità emittente del certificato intermedio è SMBRootCA.

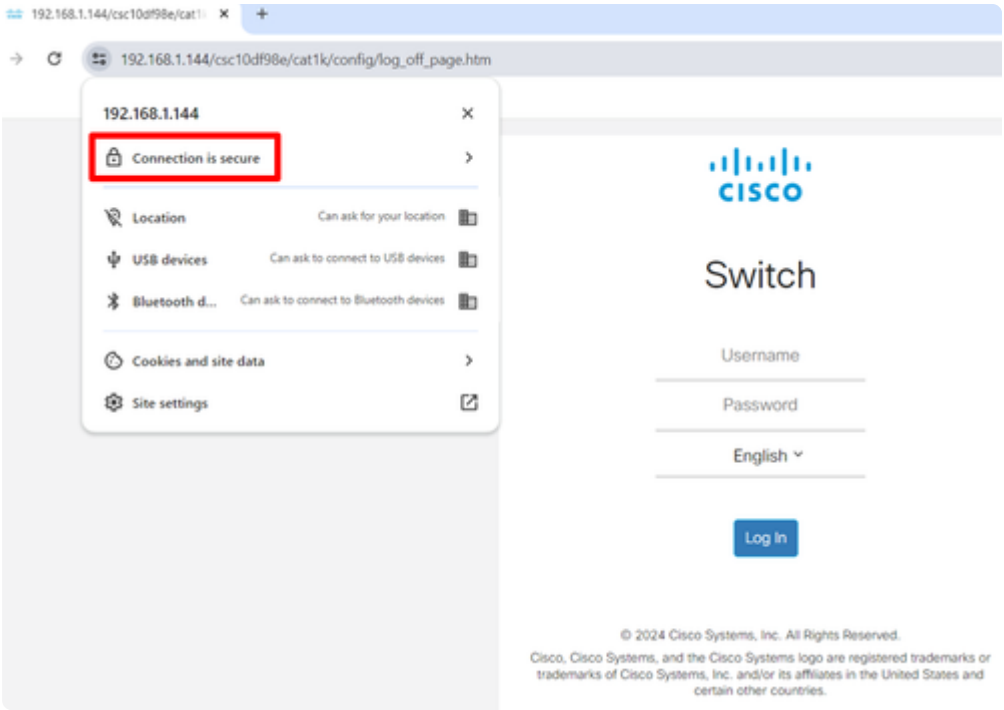


Esempio di catena di certificati

Se per impostazione predefinita gli switch utilizzano un certificato autofirmato, il sistema client, in questo caso un browser Web, visualizzerà un messaggio che indica che la connessione non è protetta.



Quando invece la catena di certificati è completata con un certificato radice, un certificato intermedio e un certificato server installati, nel browser verrà visualizzato che la connessione è protetta.



Conclusioni

Ecco qua! A questo punto è possibile caricare i certificati intermedi e visualizzare la catena di certificati sugli switch Catalyst 1200 e 1300.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).