Configurare il certificato HTTPS della GUI ACI APIC

Sommario

Introduzione

In questo documento viene descritta la configurazione dei certificati SSL personalizzati e SSL autofirmati.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Firme digitali e certificati digitali
- Processo di rilascio del certificato da parte dell'organizzazione CA

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Application Policy Infrastructure Controller (APIC)
- Browser
- ACI in esecuzione 5.2 (8e)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

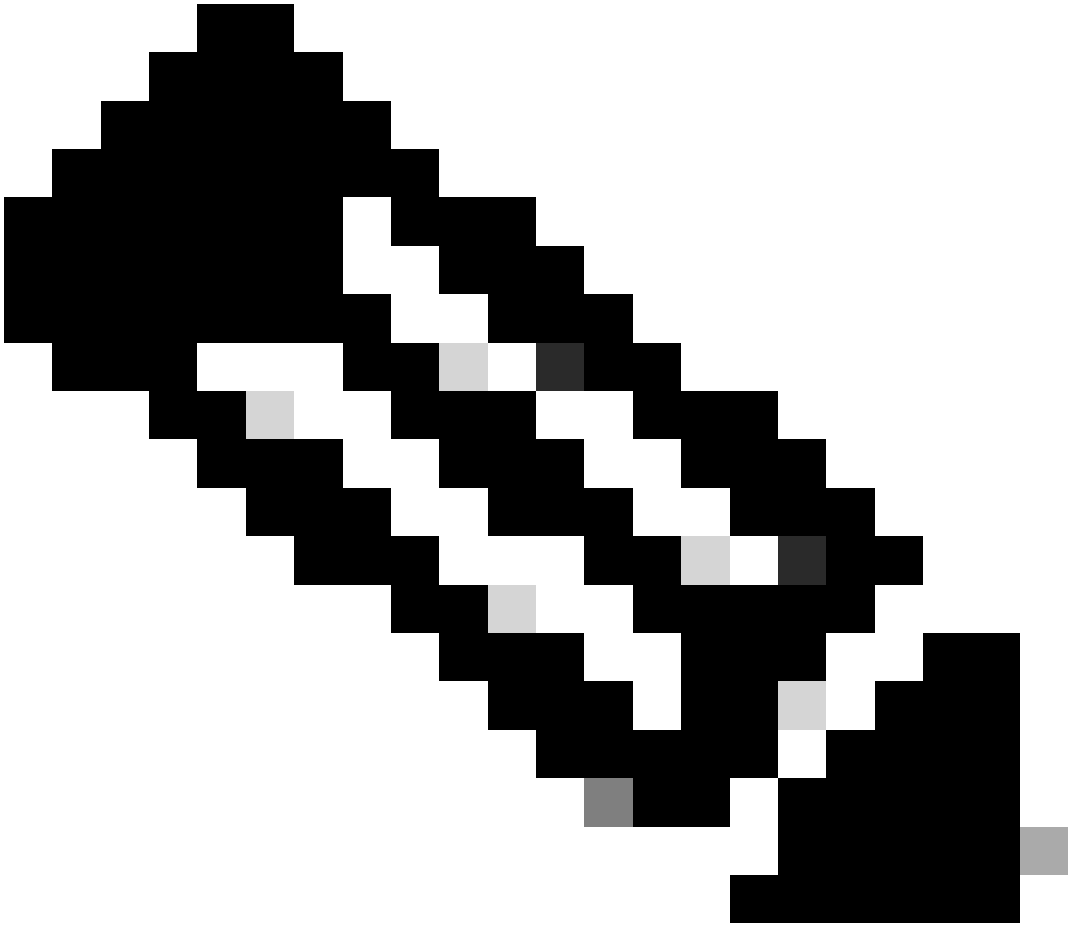
Dopo l'inizializzazione, il dispositivo utilizza il certificato autofirmato come certificato SSL per HTTPS. Il certificato autofirmato è valido per 1000 giorni.

Per impostazione predefinita, il dispositivo rinnova e genera automaticamente un nuovo certificato autofirmato un mese prima della scadenza del certificato stesso.

Configurazioni

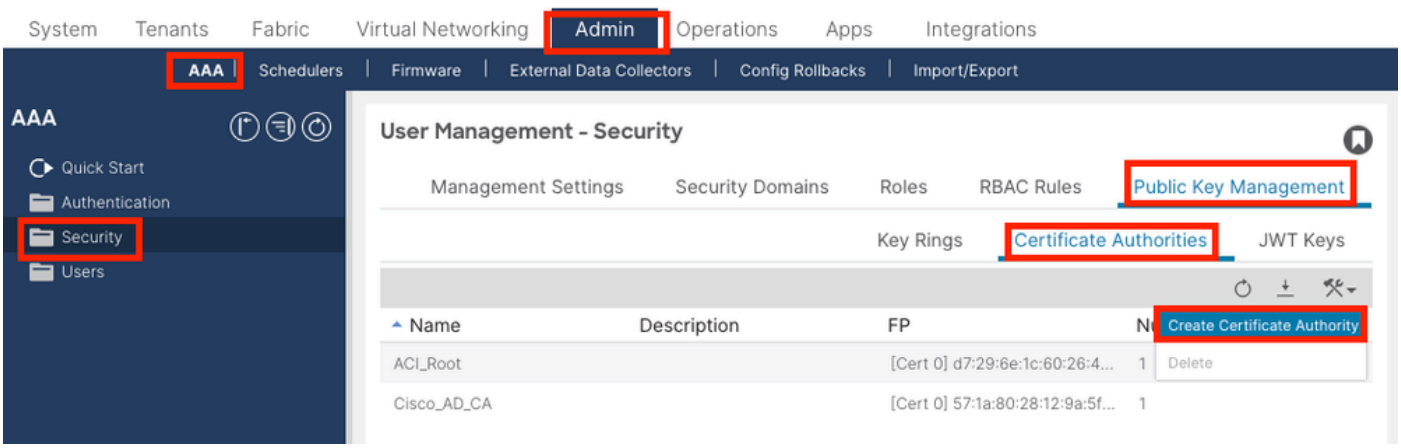
Il dispositivo utilizza un certificato autofirmato. Quando si accede alla GUI di APIC, il browser chiede che il certificato non sia attendibile. Per risolvere il problema, nel documento viene utilizzata un'autorità CA attendibile per firmare il certificato.

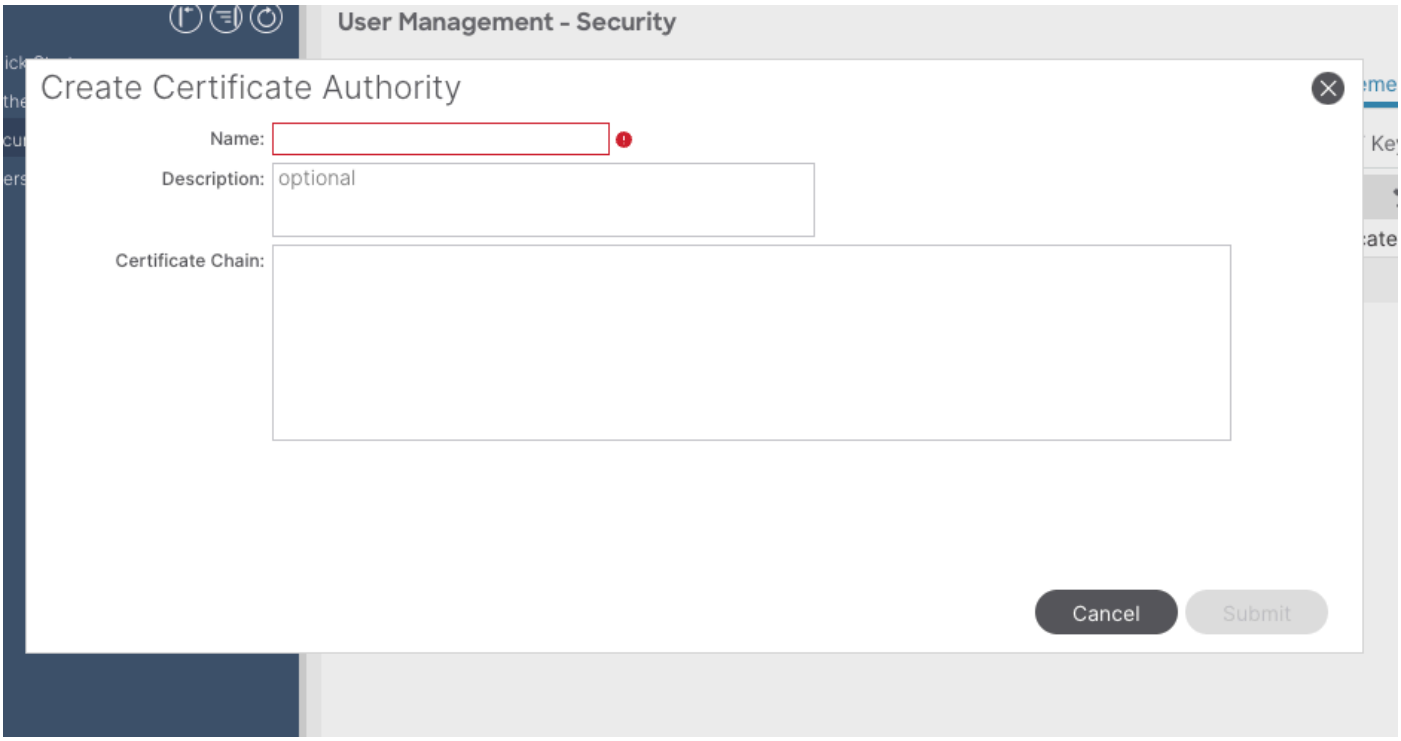
Passaggio 1. Importazione del certificato radice o intermedio dell'autorità CA



Nota: Se si utilizza il certificato radice CA per la firma diretta, è sufficiente importare il certificato radice CA. Se invece si utilizza un certificato intermedio per la firma, è necessario importare l'intera catena di certificati, ovvero: il certificato radice e i certificati intermedi meno attendibili.

Sulla barra dei menu, passare aAdmin > AAA > Security > Public Key Management > Certificate Authorities.





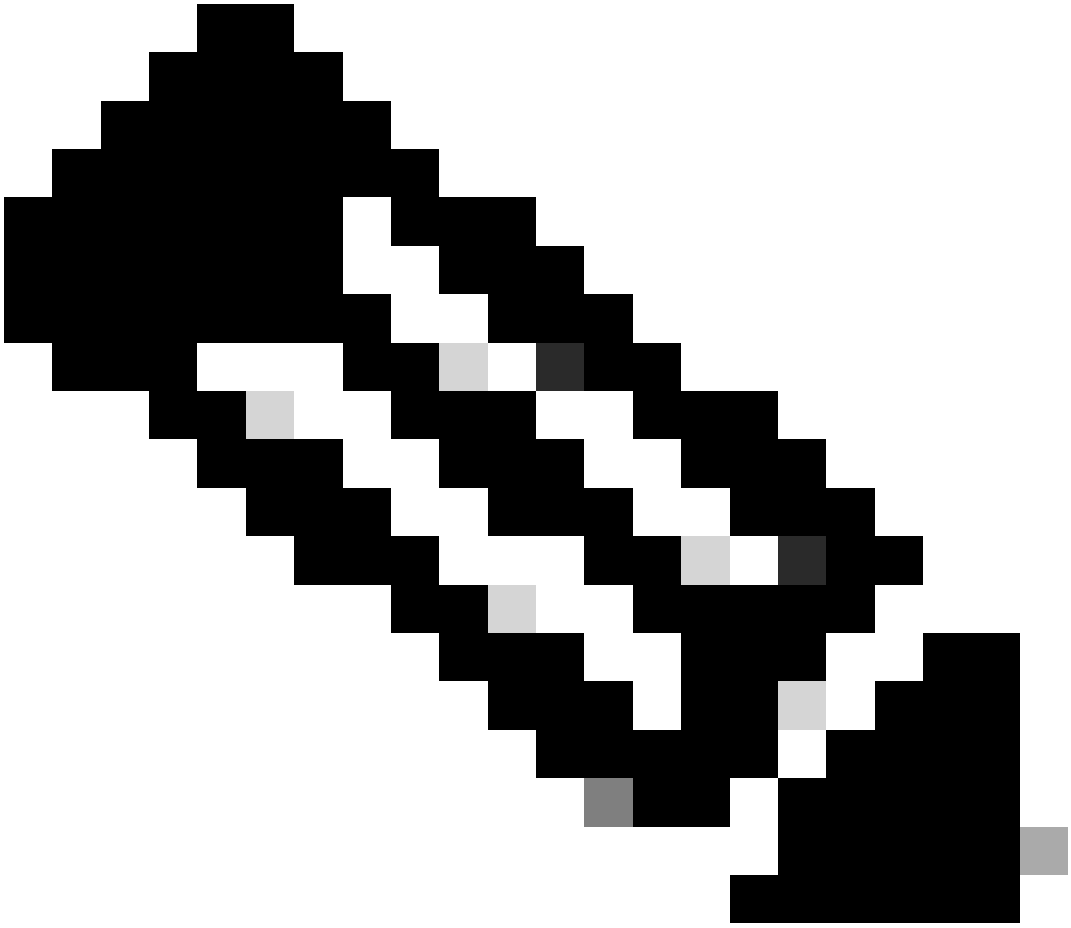
Nome: obbligatorio.

Formulare il contenuto in base alle regole di denominazione. Può contenere_, ma non caratteri inglesi speciali, ad esempio:
, . ; ' " : | + * / = ` ~ ! @ # $ % ^ & ( ) e spazi.

Descrizione: facoltativa.

Catena di certificazione: obbligatorio.

Immettere il certificato radice CA attendibile e il certificato intermedio CA.



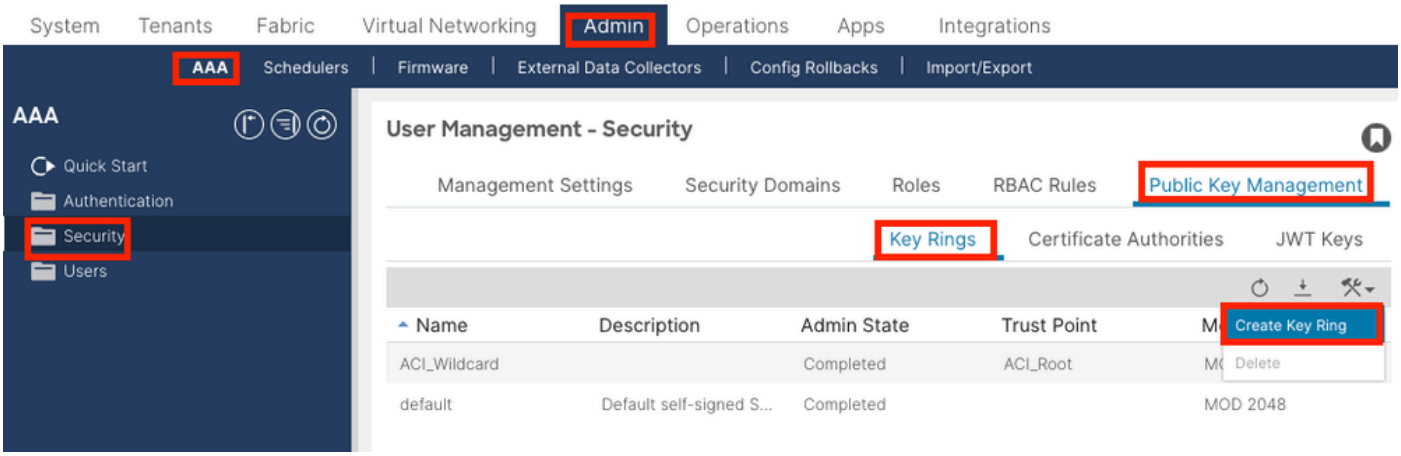
Nota: Ogni certificato deve essere conforme a un formato fisso.

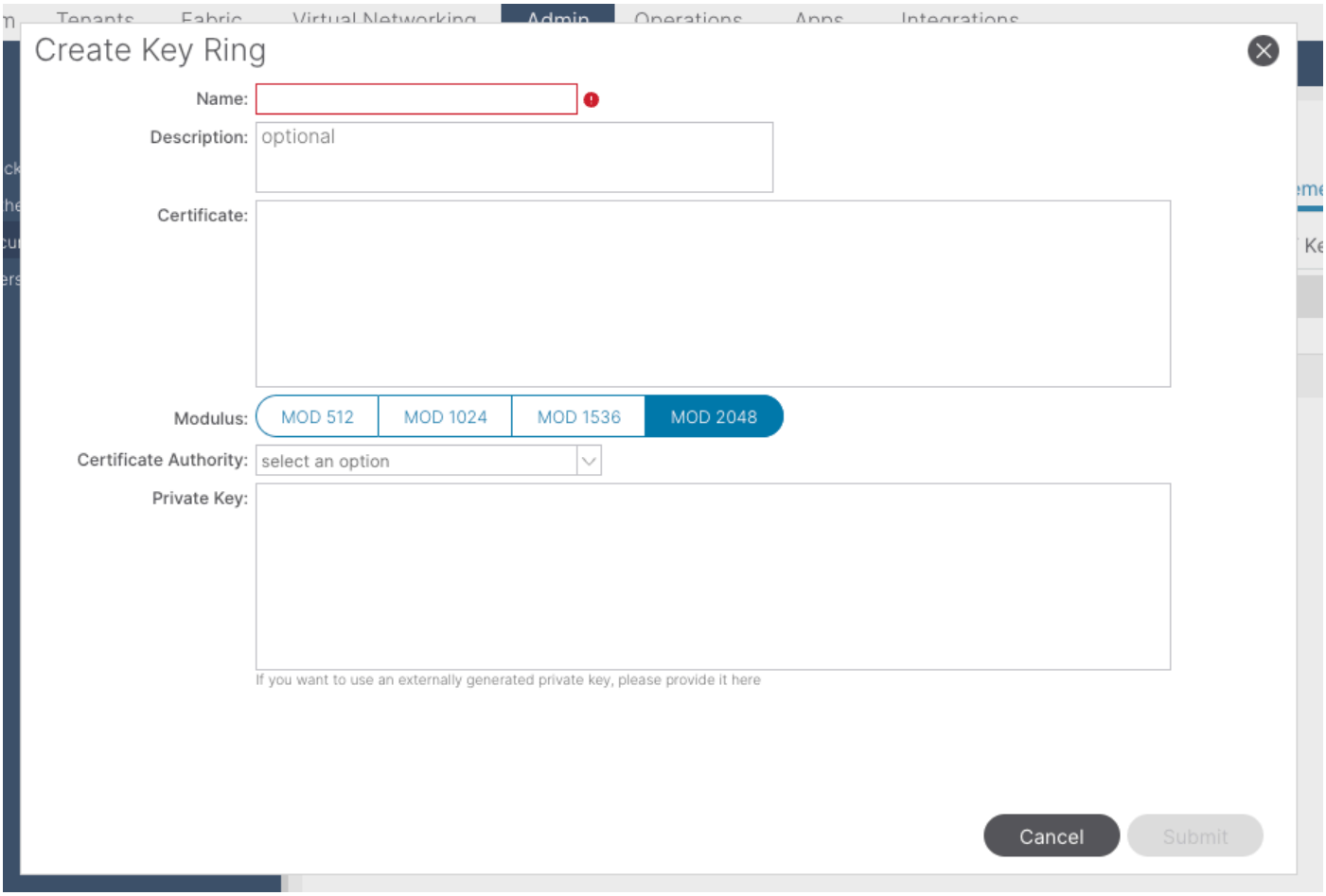
-----BEGIN CERTIFICATE----- INTER-CA-2 CERTIFICATE CONTENT HERE -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- INTER-CA-1 CERTIFICATE CONTENT HERE -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- ROOT-CA CERTIFICATE CONTENT HERE -----END CERTIFICATE-----

Fare clic sul pulsante Invia.

Passaggio 2. Creazione dell'anello della chiave

Sulla barra dei menu, passare aAdmin > AAA > Security > Public Key Management > Key Rings.





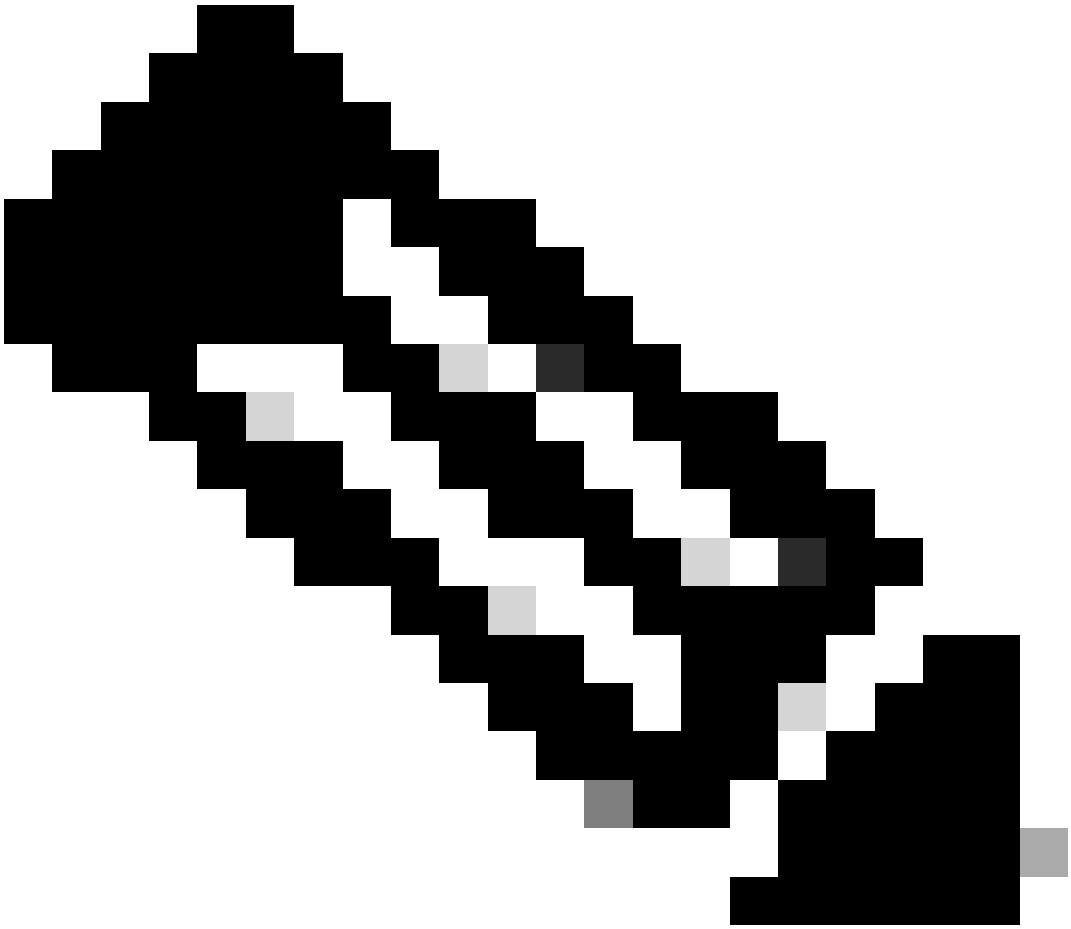
Nome:obbligatorio (immettere un nome).

Certificato:non aggiungere alcun contenuto se si genera una richiesta di firma del certificato (CSR) utilizzando Cisco APIC tramite l'anello della chiave. In alternativa, aggiungere il contenuto del certificato firmato, se ne esiste già uno firmato dalla CA nei passaggi precedenti, generando una chiave privata e un CSR all'esterno di Cisco APIC.

Modulo: obbligatorio (fare clic sul pulsante di opzione per impostare la forza desiderata della chiave).

Autorità di certificazione: obbligatorio. Dall'elenco a discesa, scegliere l'Autorità di certificazione creata in precedenza.

Chiave privata:non aggiungere alcun contenuto se si genera un CSR utilizzando l'apic di Cisco tramite l'anello della chiave. In alternativa, aggiungere la chiave privata utilizzata per generare il CSR per il certificato firmato immesso.

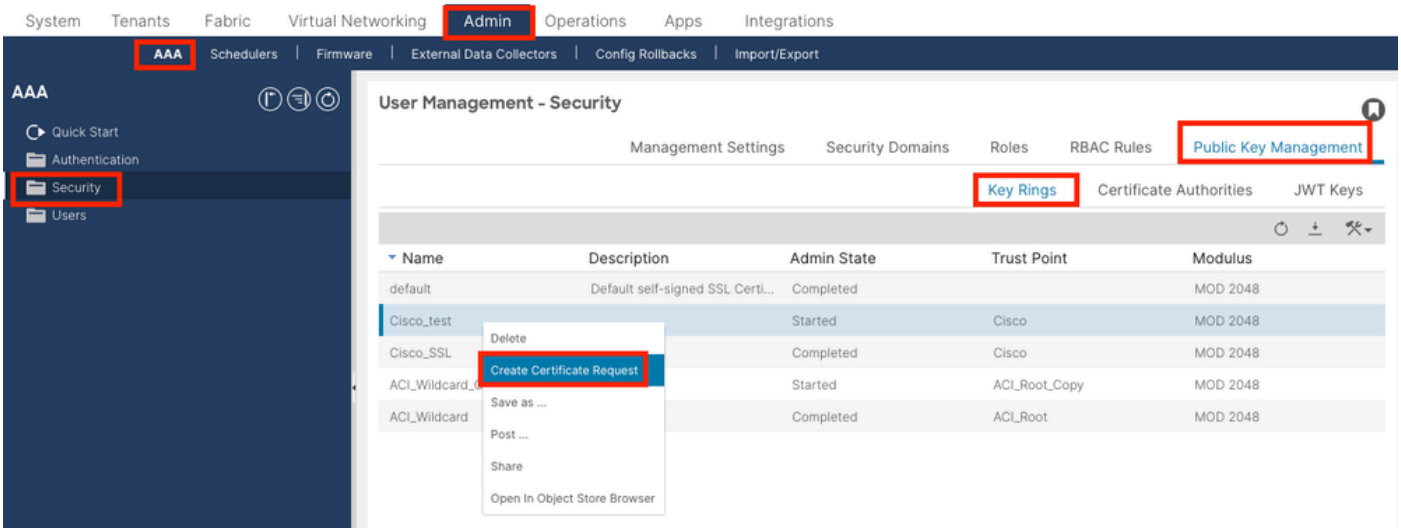


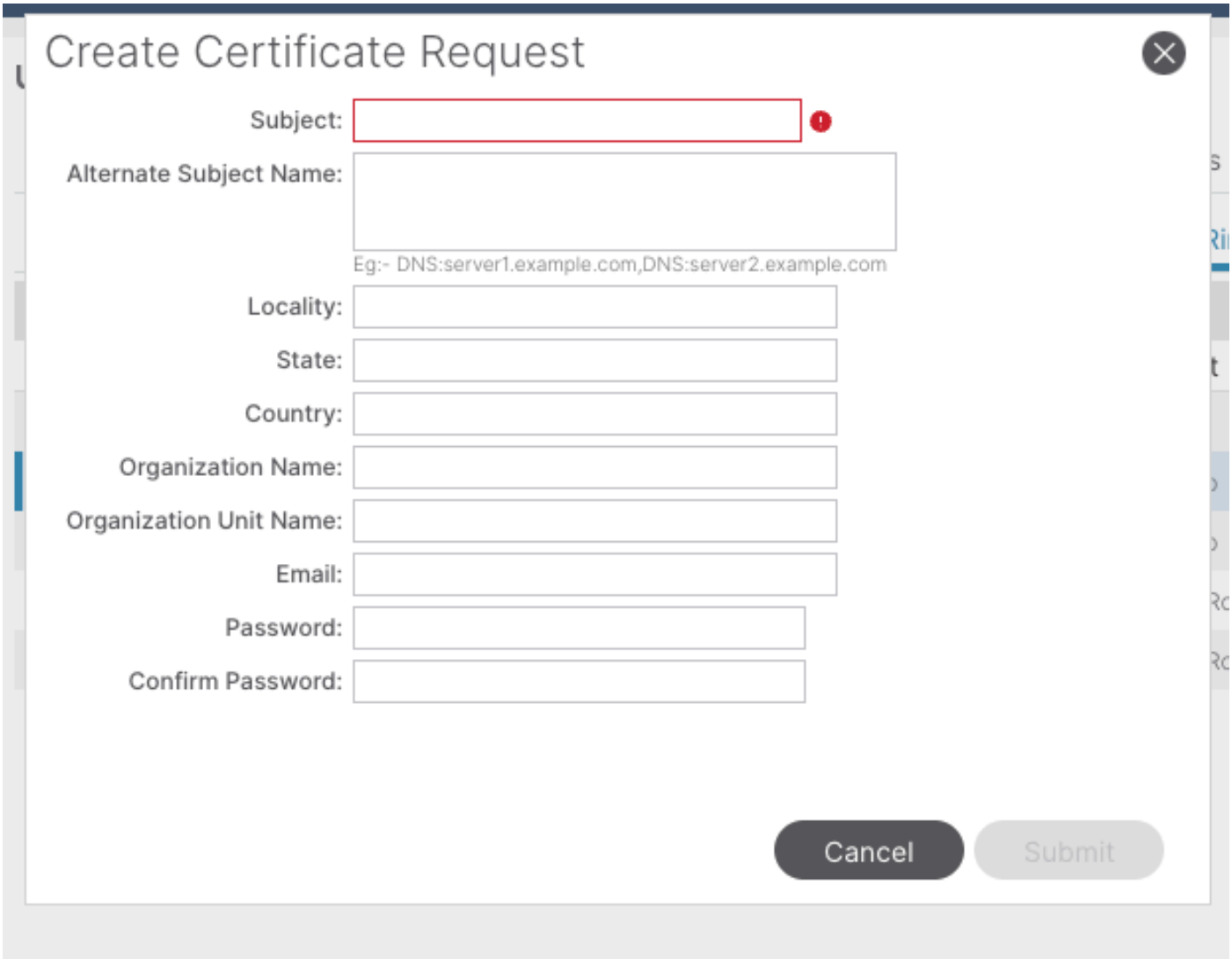
> Nota: Se non si desidera utilizzare la chiave privata e il CSR generati dal sistema e utilizzare una chiave privata e un certificato personalizzati, è necessario specificare solo quattro elementi: Nome, Certificato, Autorità di certificazione e Chiave privata. Dopo l'invio è necessario eseguire solo l'ultimo passaggio, il passaggio 5.

Fare clic sul pulsante Invia.

Passaggio 3. Generazione della chiave privata e di CSR

Sulla barra dei menu, passare a Admin > AAA > Security > Public Key Management > Key Rings.



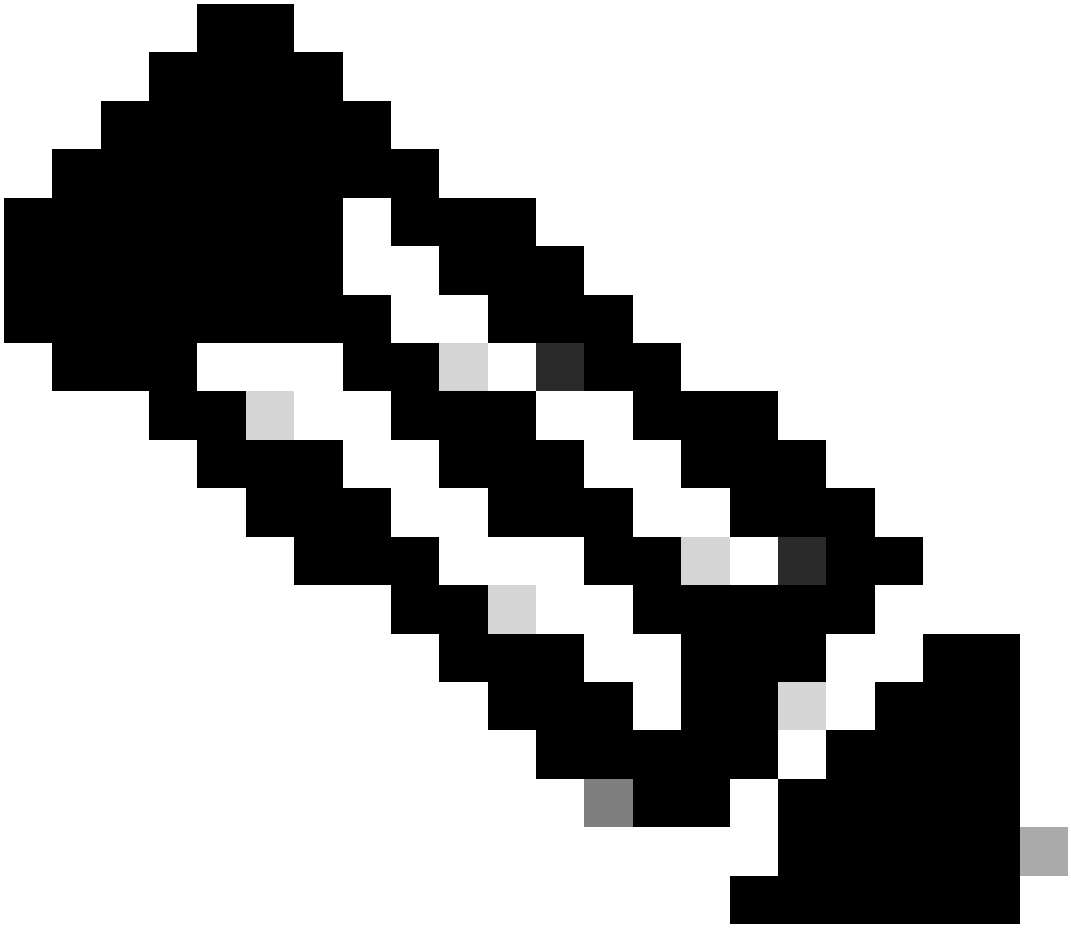


Oggetto: obbligatorio. Immettere il nome comune (CN) del CSR.

È possibile immettere il nome di dominio completo (FQDN) degli APIC Cisco utilizzando un carattere jolly, ma in un certificato moderno è in genere consigliabile immettere un nome identificabile del certificato e il nome di dominio completo di tutti gli APIC Cisco nel campo Nome soggetto alternativo (noto anche come SAN- Nome alternativo soggetto) perché molti browser moderni si aspettano il nome di dominio completo nel campo SAN.

Nome soggetto alternativo: obbligatorio. Immettere il nome di dominio completo (FQDN) di tutti gli APIC Cisco, ad esempioDNS:apic1.example.com,DNS:apic2.example.com,DNS:apic3.example.com**O**DNS:*example.com.

In alternativa, se si desidera che la rete SAN corrisponda a un indirizzo IP, immettere gli indirizzi IP degli ACL Cisco nel formato: IP:192.168.1.1.



> Nota: In questo campo è possibile utilizzare nomi DNS (Domain Name Server), indirizzi IPv4 o una combinazione di entrambi. Gli indirizzi IPv6 non sono supportati.

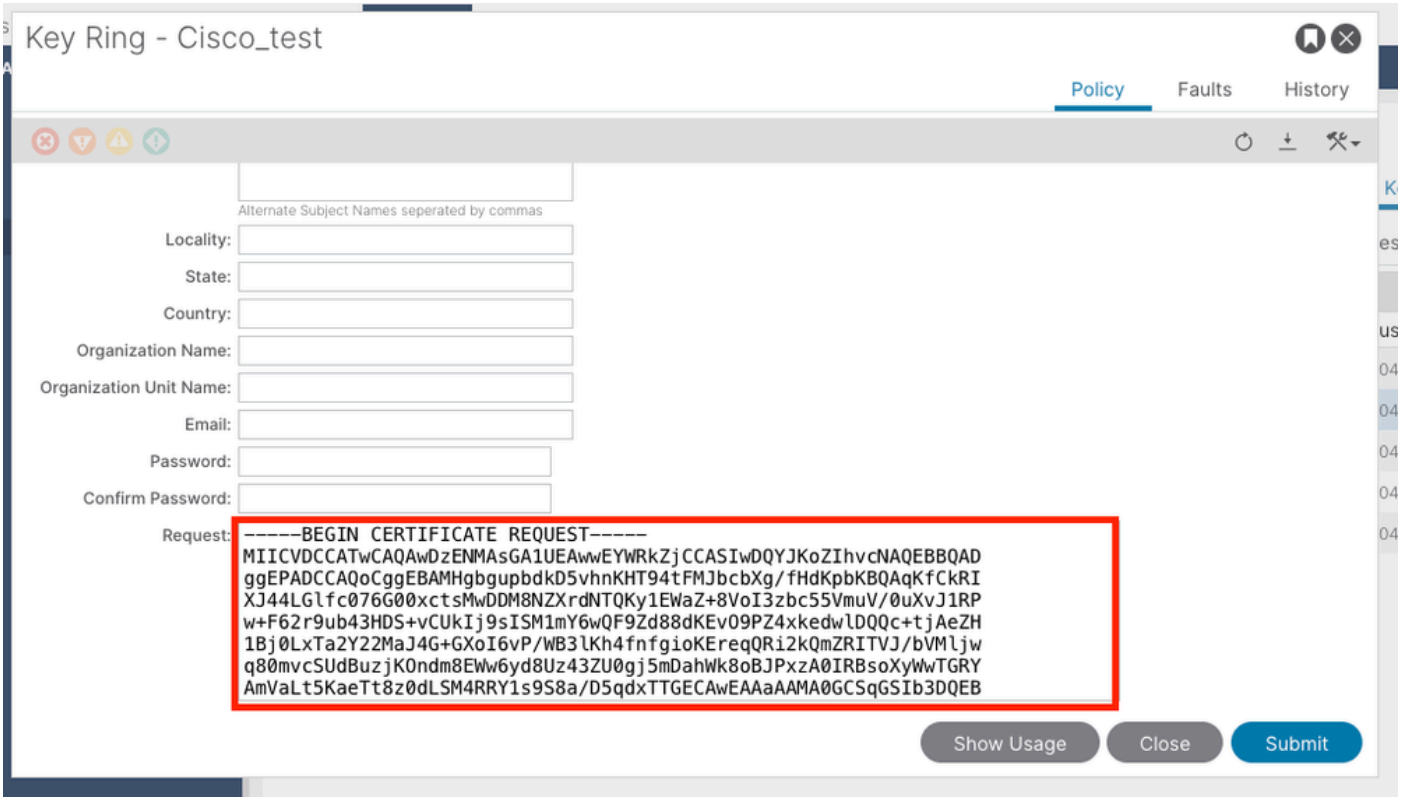
Compilare i campi rimanenti in base ai requisiti dell'organizzazione CA che si sta richiedendo per il rilascio del certificato.

Fare clic sul pulsante Invia.

Passaggio 4. Ottenere il CSR e inviarlo all'organizzazione CA

Sulla barra dei menu, passare aAdmin > AAA > Security > Public Key Management > Key Rings.

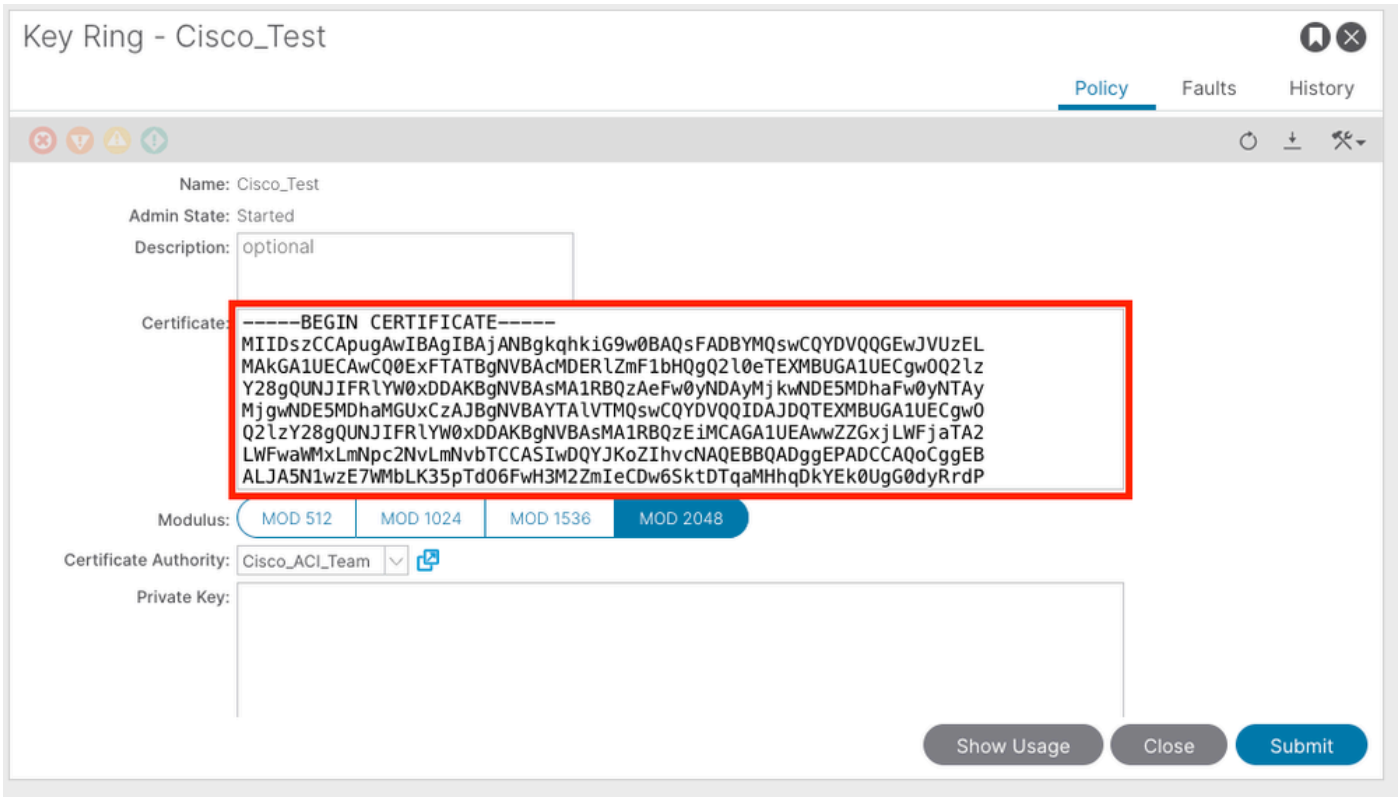
Fare doppio clic sul nome dell'anello chiave creato e individuare l'opzione Richiesta. Il contenuto della richiesta è il CSR.

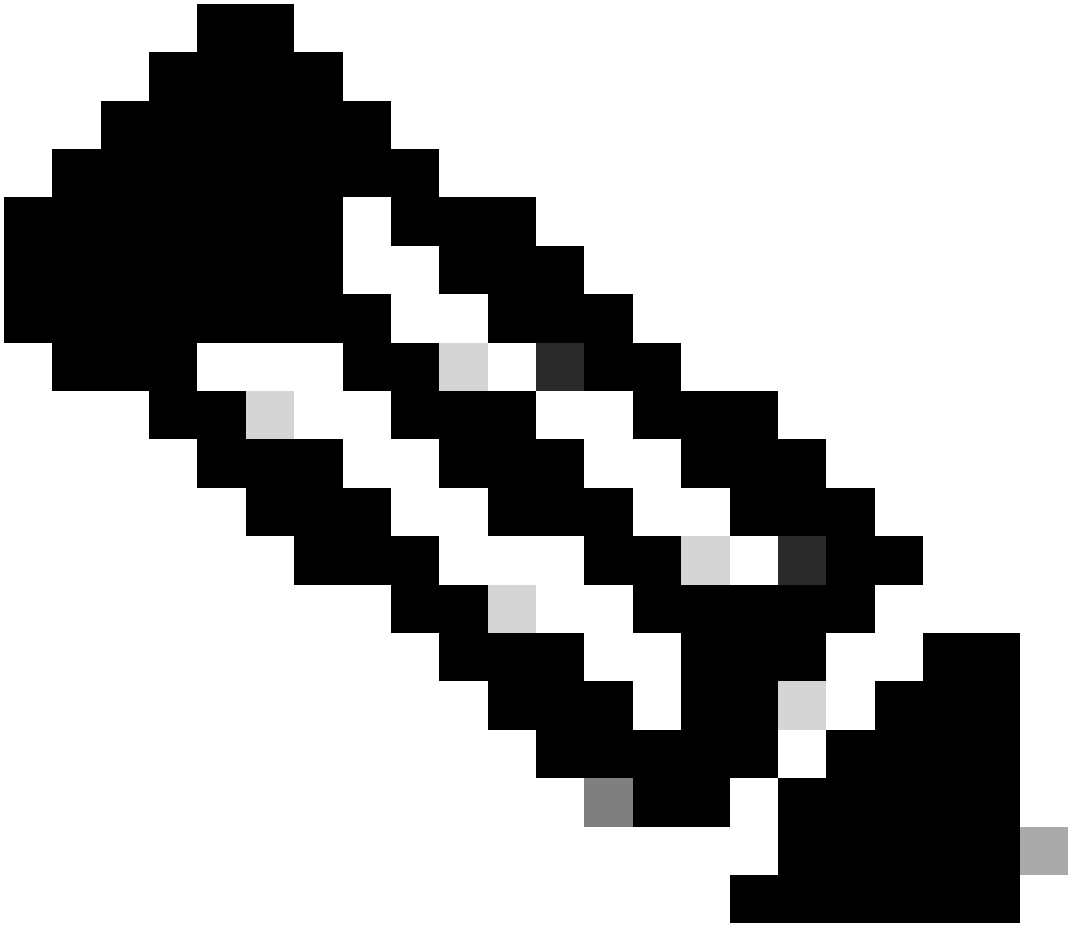


Copiare tutto il contenuto della richiesta e inviarlo alla CA.

La CA utilizza la propria chiave privata per eseguire la verifica della firma sul CSR.

Dopo aver ottenuto il certificato firmato dalla CA, il certificato viene copiato nel certificato.





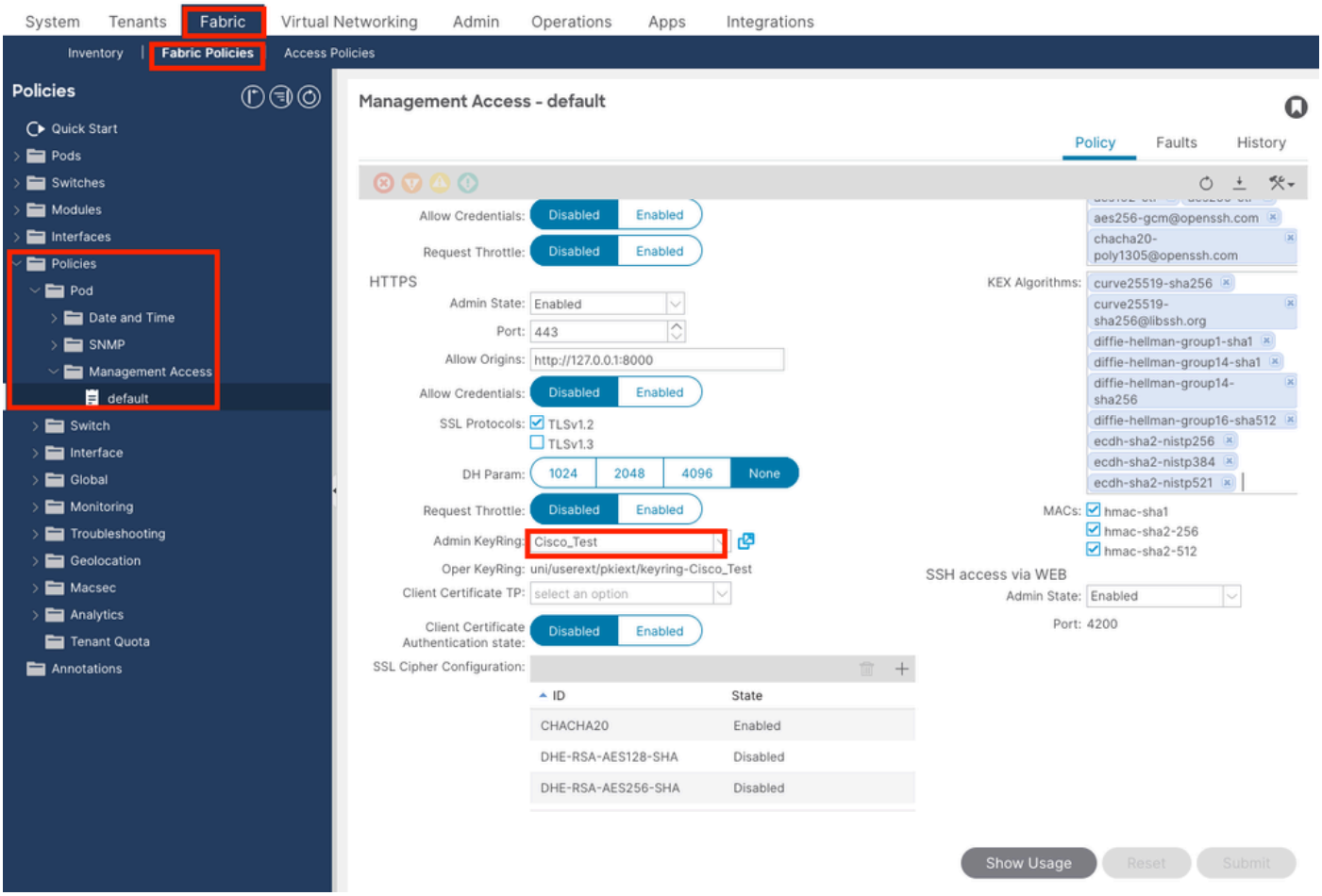
Nota: Ogni certificato deve essere conforme a un formato fisso.

-----BEGIN CERTIFICATE----- CERTIFICATE CONTENT HERE -----END CERTIFICATE-----

Fare clic sul pulsante Invia.

Passaggio 5. Aggiornare il certificato di firma sul Web

Sulla barra dei menu, passare aFabric > Fabric Policies > Policies > Pod > Management Access > Default.



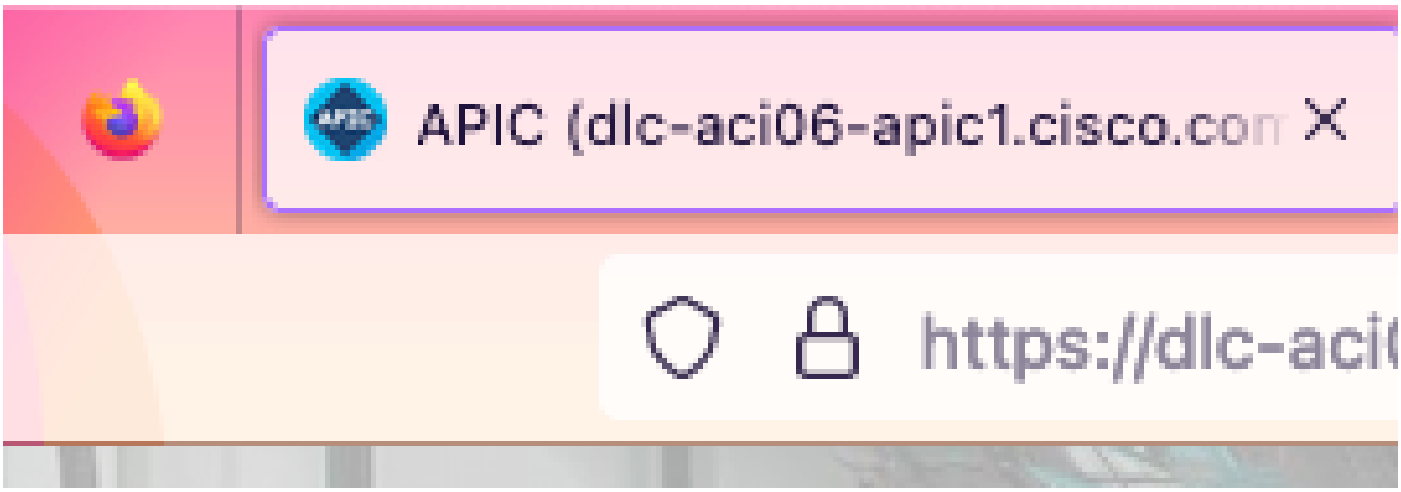
nell'elenco a discesa Admin KeyRing, scegliere il KeyRing desiderato.

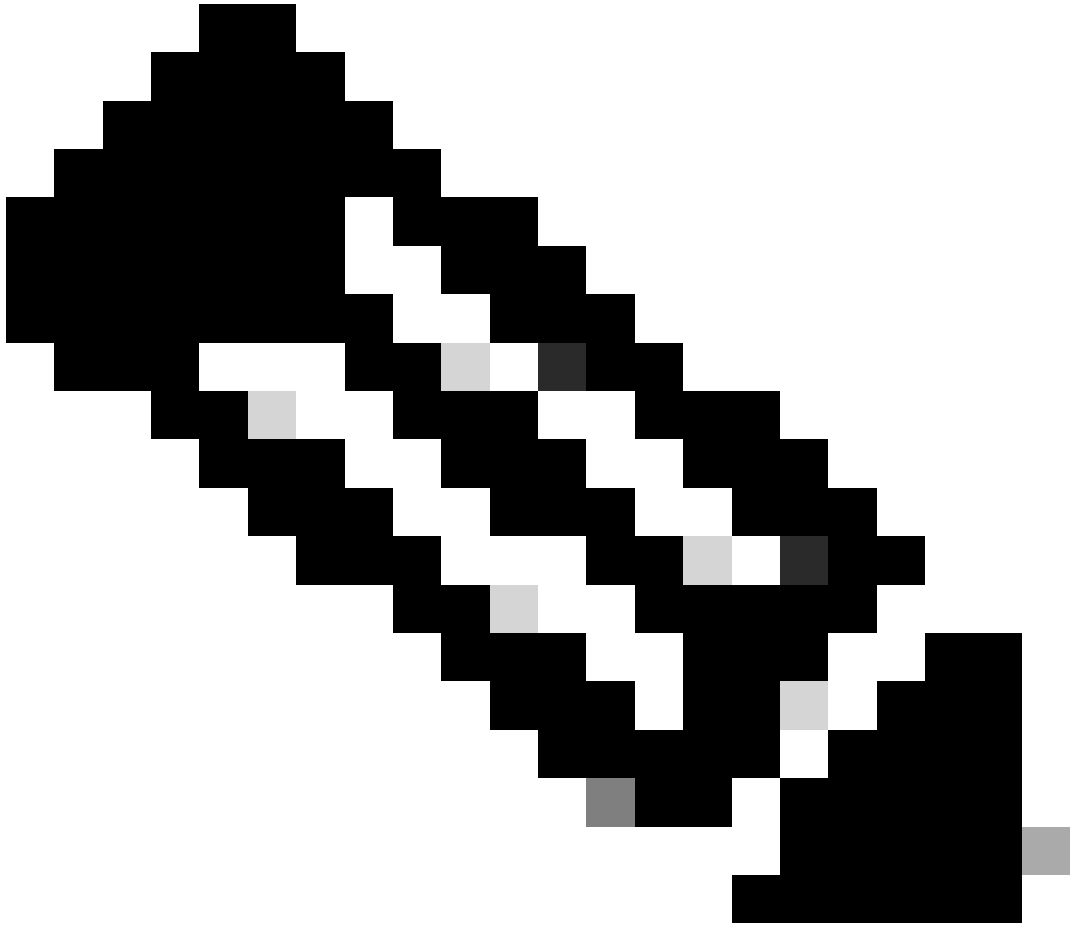
Fare clic sul pulsante Invia.

Dopo aver fatto clic su Invia, si verificherà un errore dovuto a motivi del certificato. Aggiornare con il nuovo certificato.

Verifica

Dopo aver effettuato l'accesso all'interfaccia utente grafica di APIC, l'APIC utilizza il certificato firmato dall'autorità di certificazione per comunicare. Visualizzare le informazioni sul certificato nel browser per verificarle.

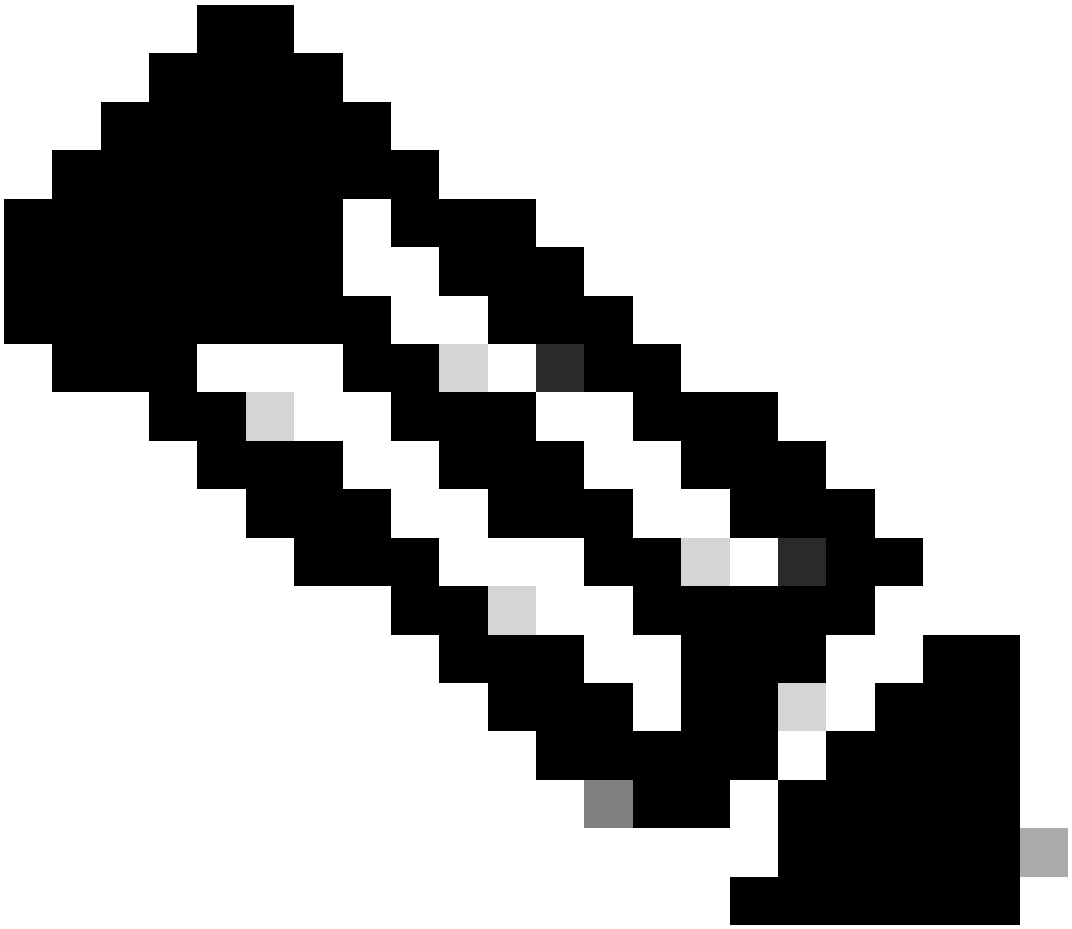




Nota: I metodi di visualizzazione dei certificati HTTPS in browser diversi non sono esattamente gli stessi. Per informazioni su metodi specifici, consultare la guida dell'utente del browser.

Risoluzione dei problemi

Se il browser continua a richiedere che l'interfaccia grafica APIC non è attendibile, verificare nel browser se il certificato dell'interfaccia utente grafica è coerente con quello inviato nel Keyring. È necessario considerare attendibile il certificato radice CA che ha emesso il certificato nel computer o nel browser.



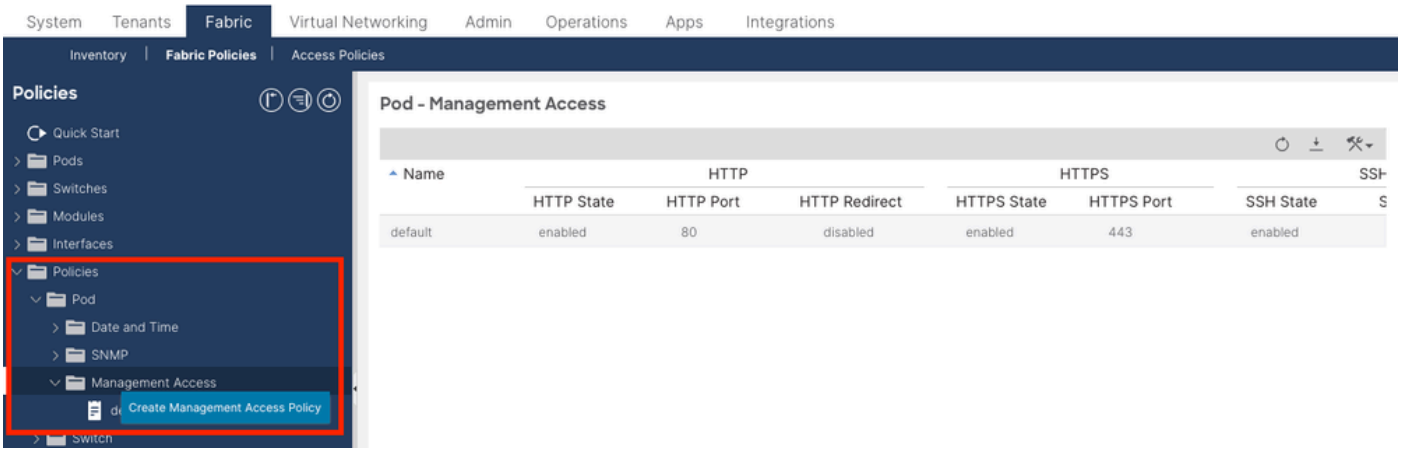
> Nota: Il browser Google Chrome deve verificare la SAN del certificato per poter considerare attendibile questo certificato.

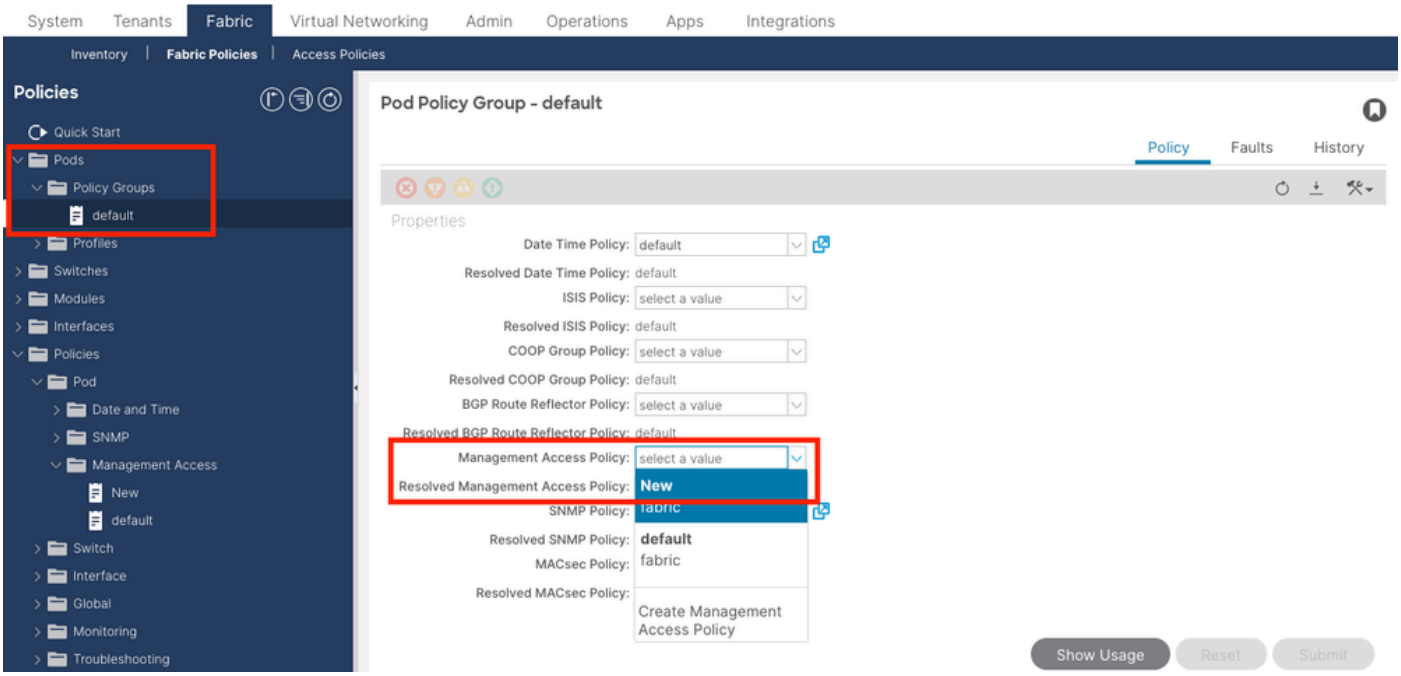
Negli APIC che utilizzano certificati autofirmati, in rari casi possono essere visualizzati avvisi di scadenza dei certificati.

Individuare il certificato in Gruppo di chiavi, utilizzare lo strumento di analisi dei certificati per analizzare il certificato e confrontarlo con il certificato utilizzato nel browser.

Se il certificato nel keyring viene rinnovato, creare un nuovo criterio di accesso alla gestione e

applicarlo.





Se il certificato in Keyring non viene rinnovato automaticamente, contattare Cisco TAC per ulteriore assistenza.

Informazioni correlate

- Guida alla configurazione della sicurezza di Cisco APIC, versione 5.2(x)
- Supporto tecnico Cisco e download

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).