

Configurare il certificato HTTPS della GUI ACI APIC

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Configurazioni](#)

[Passaggio 1. Importare il certificato radice o il certificato intermedio dell'autorità CA](#)

[Passaggio 2. Creazione dell'anello della chiave](#)

[Passaggio 3. Generazione della chiave privata e di CSR](#)

[Passaggio 4. Ottenere il CSR e inviarlo all'organizzazione CA](#)

[Passaggio 5. Aggiornare il certificato di firma sul Web](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

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.

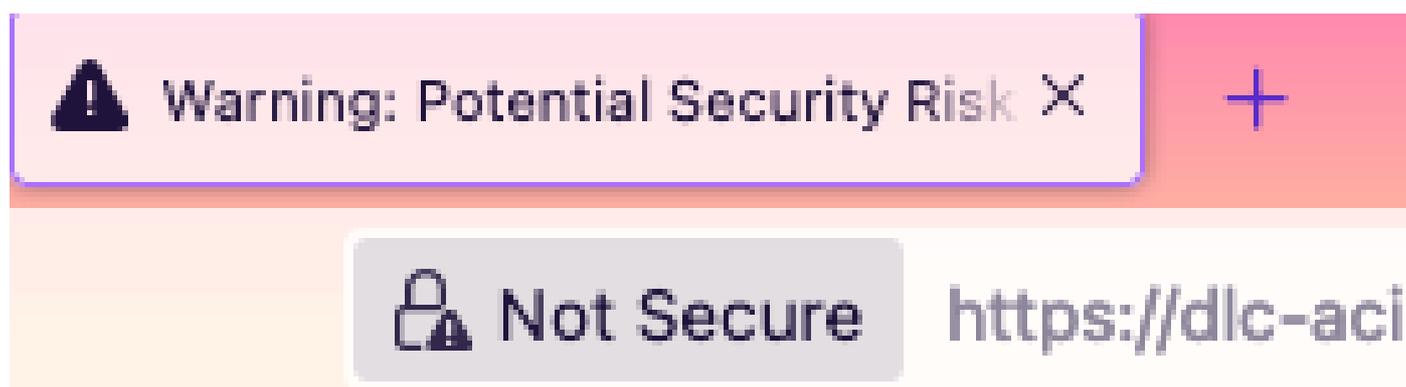
Configurazione

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

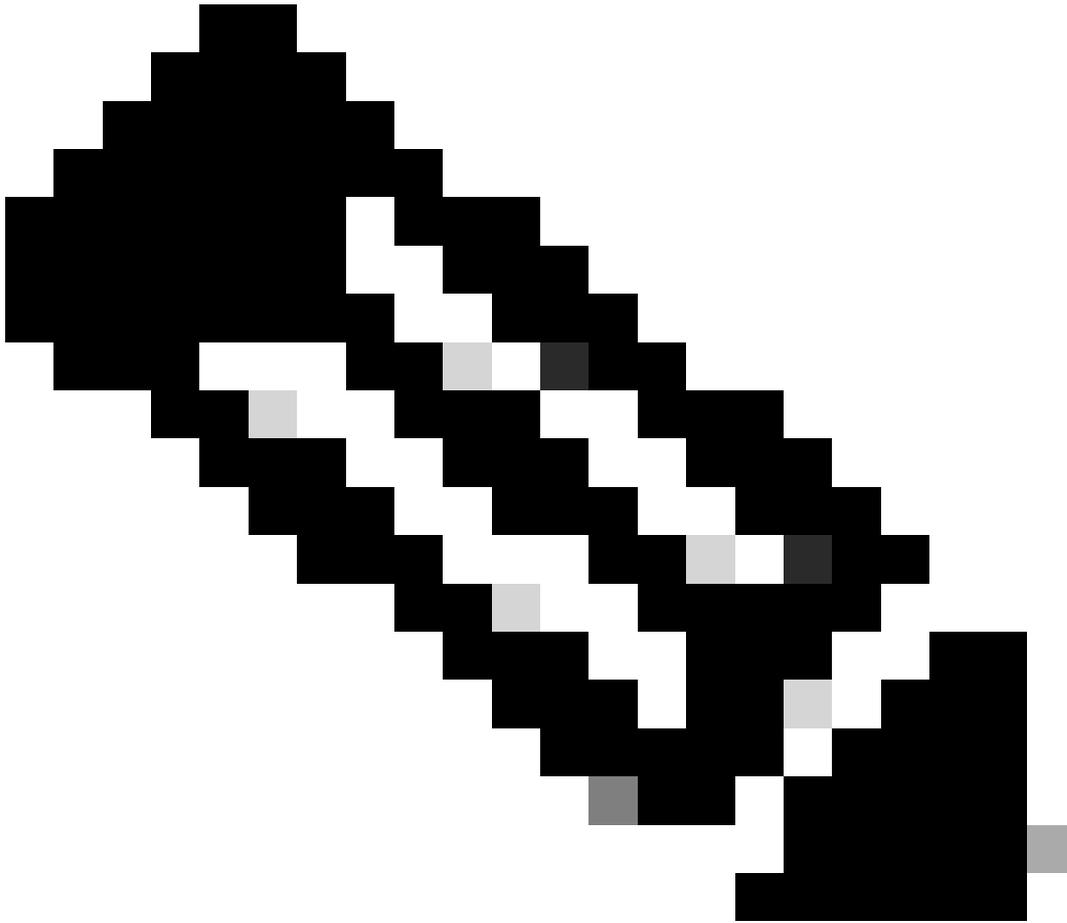
Per impostazione predefinita, il dispositivo rinnova e genera automaticamente un nuovo certificato autofirmato un mese prima della scadenza del certificato stesso.

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 a Admin > AAA > Security > Public Key Management > Certificate Authorities.

The screenshot displays the Cisco ICM web interface. The top navigation bar includes 'System', 'Tenants', 'Fabric', 'Virtual Networking', 'Admin', 'Operations', 'Apps', and 'Integrations'. The 'Admin' menu is expanded, showing 'AAA', 'Schedulers', 'Firmware', 'External Data Collectors', 'Config Rollbacks', and 'Import/Export'. The 'AAA' menu is further expanded to show 'Quick Start', 'Authentication', 'Security', and 'Users'. The 'Security' menu item is highlighted with a red box. The main content area is titled 'User Management - Security' and contains several sub-menus: 'Management Settings', 'Security Domains', 'Roles', 'RBAC Rules', 'Public Key Management', 'Key Rings', 'Certificate Authorities', and 'JWT Keys'. The 'Public Key Management' and 'Certificate Authorities' sub-menus are highlighted with red boxes. Below these sub-menus is a table with columns for 'Name', 'Description', 'FP', and 'N'. The table contains two entries: 'ACI_Root' and 'Cisco_AD_CA'. A 'Create Certificate Authority' button is highlighted with a red box, and a 'Delete' button is visible next to the 'ACI_Root' entry.

Name	Description	FP	N
ACI_Root		[Cert 0] d7:29:6e:1c:60:26:4...	1
Cisco_AD_CA		[Cert 0] 57:1a:80:28:12:9a:5f...	1

The screenshot shows a web application window titled "User Management - Security". A modal dialog box titled "Create Certificate Authority" is open. The dialog has a close button in the top right corner. It contains three input fields: "Name:" (with a red border and a red error icon), "Description:" (with the text "optional" inside), and "Certificate Chain:". At the bottom right of the dialog are two buttons: "Cancel" and "Submit".

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 a **Admin > AAA > Security > Public Key Management > Key Rings**.

System Tenants Fabric Virtual Networking **Admin** Operations Apps Integrations

AAA Schedulers Firmware External Data Collectors Config Rollbacks Import/Export

AAA

- Quick Start
- Authentication
- Security**
- Users

User Management - Security

Management Settings Security Domains Roles RBAC Rules **Public Key Management**

Key Rings Certificate Authorities JWT Keys

Name	Description	Admin State	Trust Point	M	
ACL_Wildcard		Completed	ACL_Root	M	Delete
default	Default self-signed S...	Completed			MOD 2048

Create Key Ring

Create Key Ring

Name:

Description: optional

Certificate:

Modulus: MOD 512 MOD 1024 MOD 1536 **MOD 2048**

Certificate Authority: select an option

Private Key:

If you want to use an externally generated private key, please provide it here

Cancel Submit

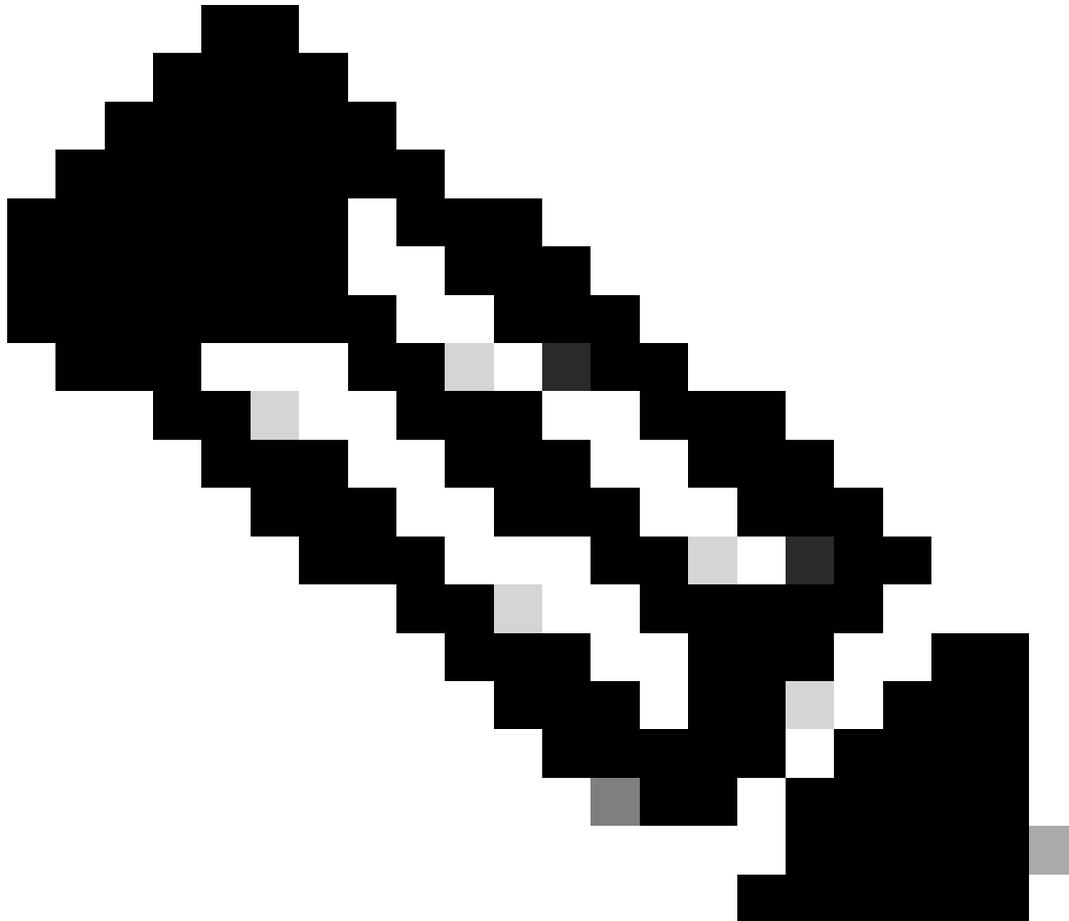
Nome: obbligatorio (immettere un nome).

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.

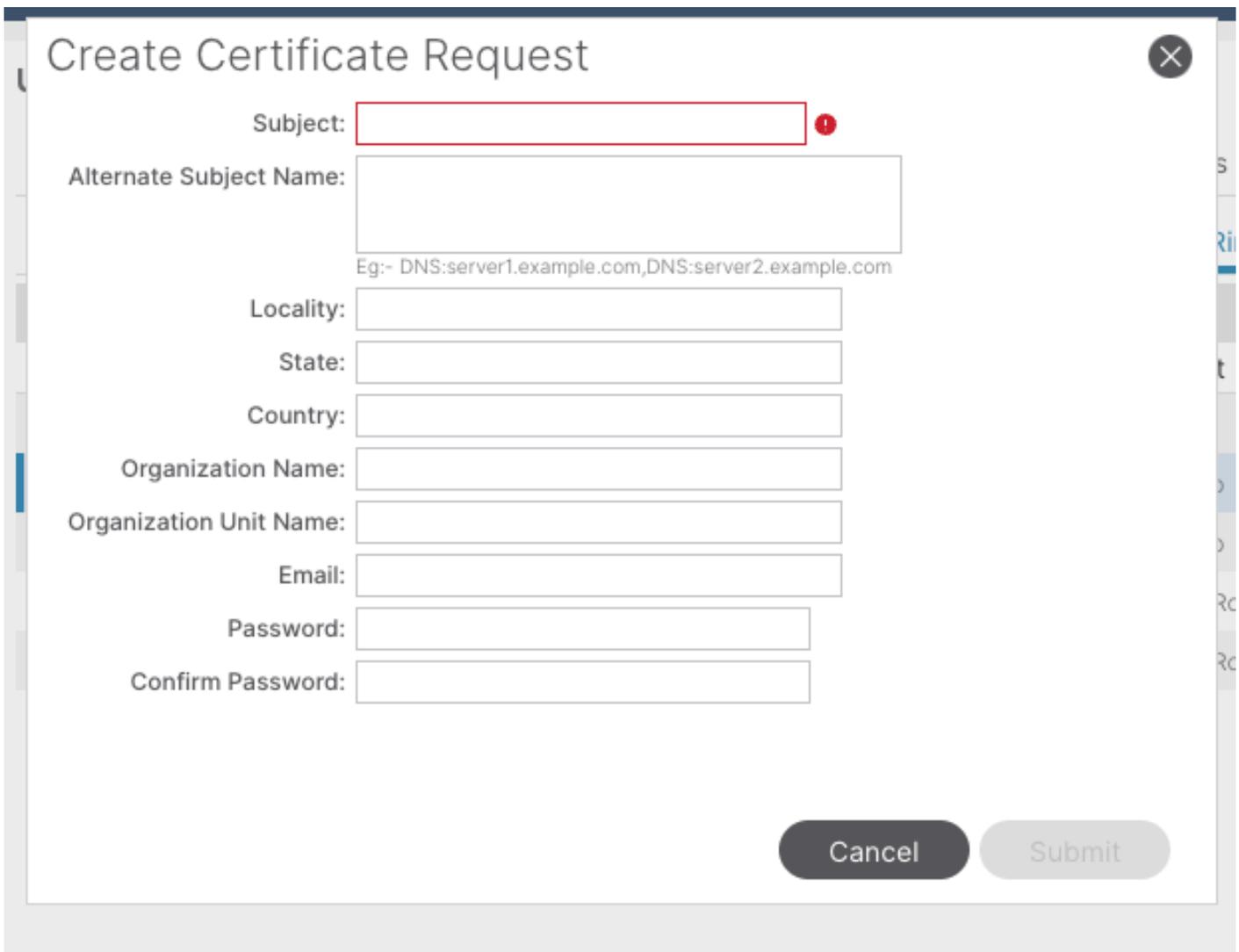
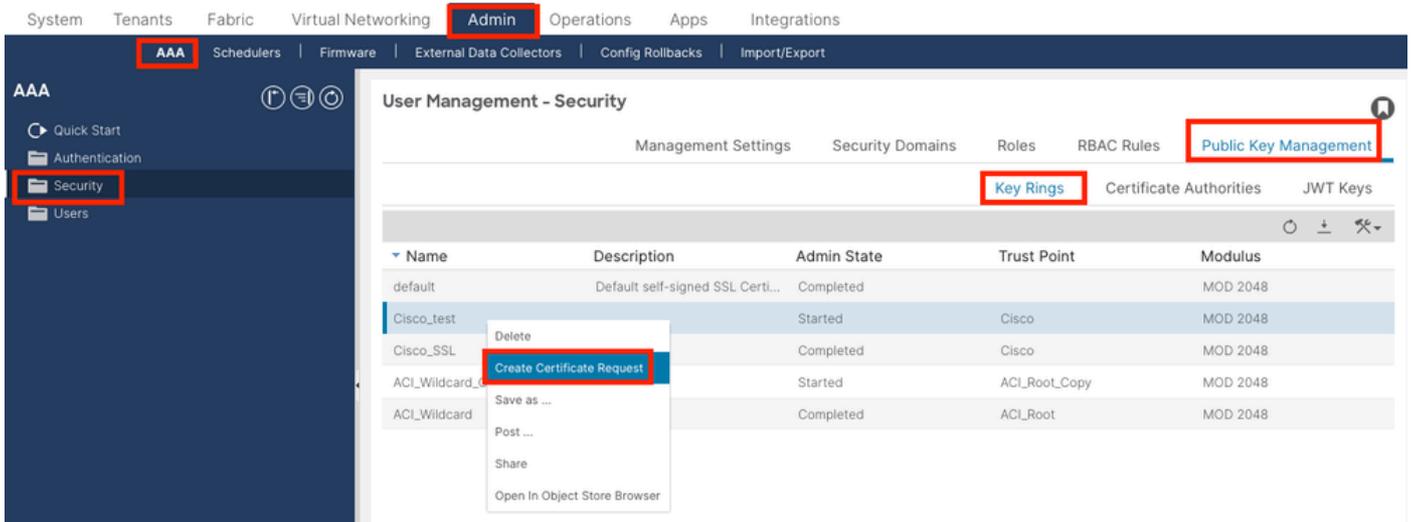


Nota: Se non si desidera utilizzare la chiave privata e il CSR generati dal sistema e utilizzare una chiave privata e un certificato personalizzati, è necessario specificare solo quattro elementi: Nome, Certificato, Autorità di certificazione e Chiave privata. Dopo l'invio è necessario eseguire solo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

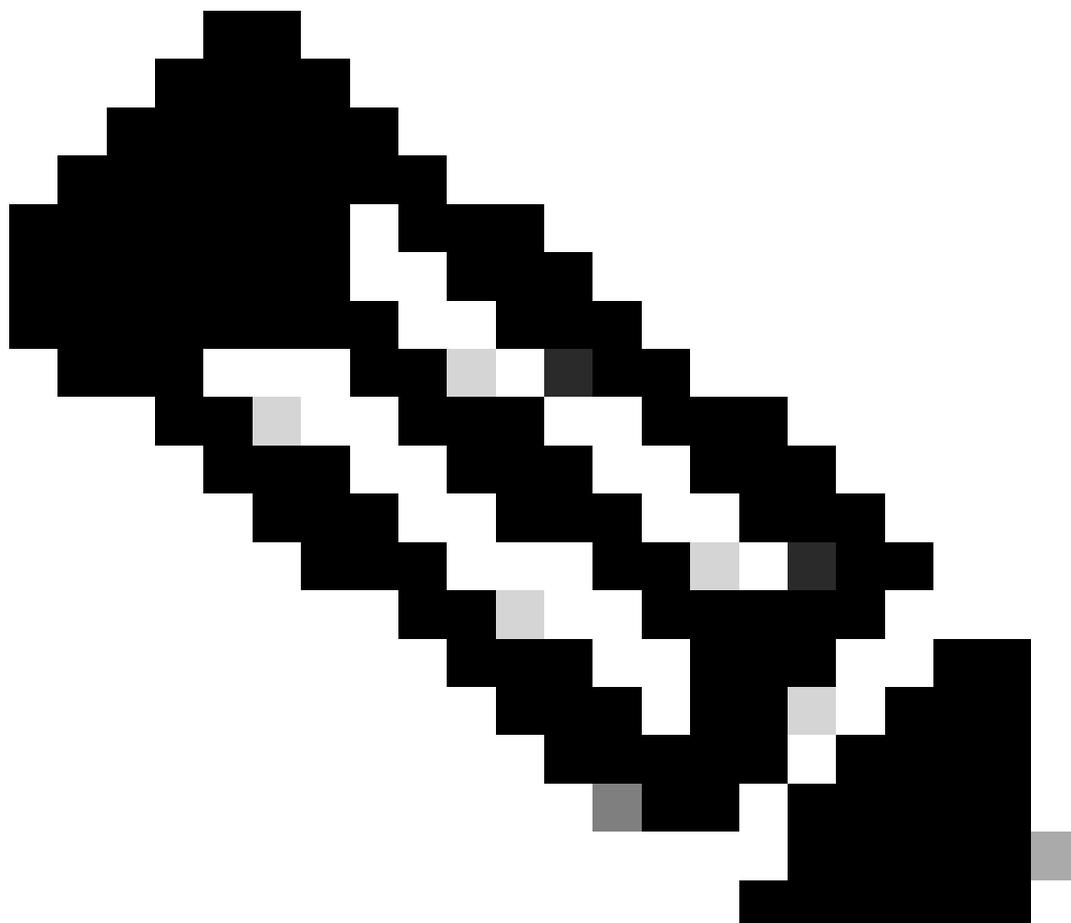


Oggetto: obbligatorio. Immettere il nome comune (CN) del CSR.

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 esempio `DNS:apic1.example.com,DNS:apic2.example.com,DNS:apic3.example.comODNS:*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.

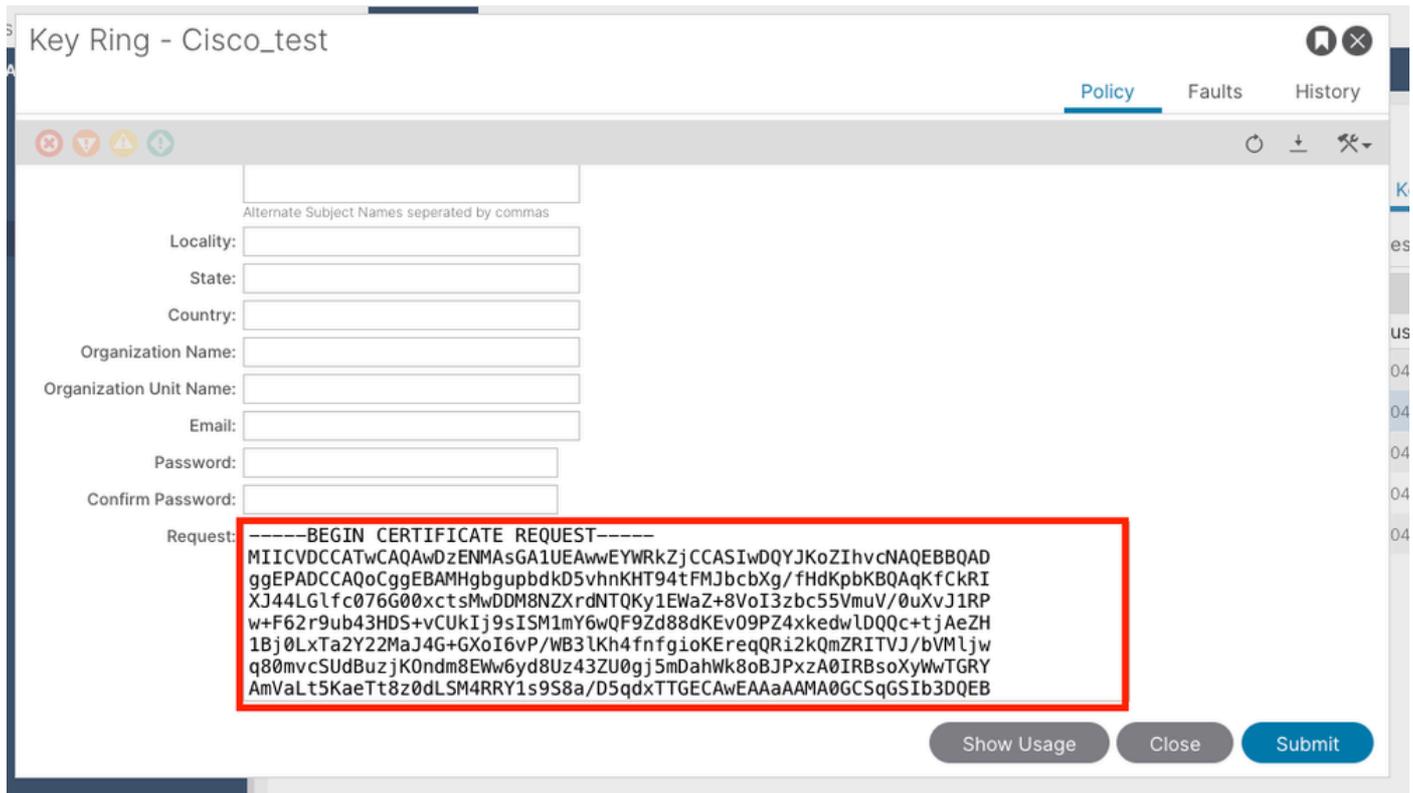
Compilare i campi rimanenti in base ai requisiti dell'organizzazione CA che si sta richiedendo per il rilascio del certificato.

Fare clic sul pulsante Invia.

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

Sulla barra dei menu, passare a `Admin > 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.



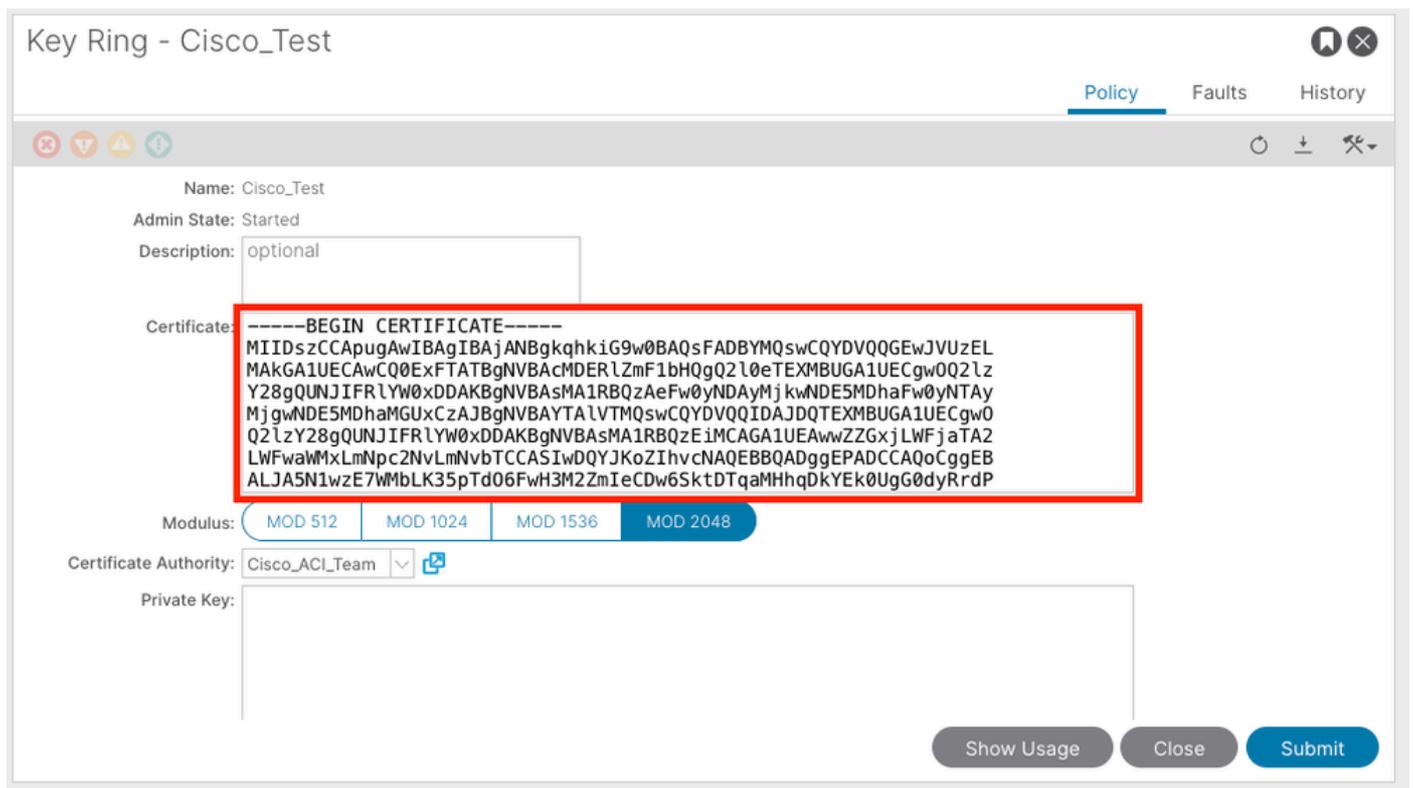
The screenshot shows the 'Key Ring - Cisco_test' configuration page. The 'Request' field is highlighted with a red box and contains the following text:

```
-----BEGIN CERTIFICATE REQUEST-----
MIICVDCCATwCAQAwDzENMAsgA1UEAwEYWRkZjCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAMHgbgubpdKd5vhnKHT94tFMJbcbXg/fHdKpbKBQAqKfCkRI
XJ44LGLfc076G00xctsmwDDM8NZXRdNTQKy1EwaZ+8VoI3zbc55VmuV/0uXvJ1RP
w+F62r9ub43HDS+vCUkIj9sISM1mY6wQF9Zd88dKEv09PZ4xkedwLDQqc+tjAeZH
1Bj0LxTa2Y22MaJ4G+GxoI6vP/WB3lKh4fnfgioKreqQRi2kQmZRITVJ/bVMljw
q80mvcSUDbuzjK0ndm8EwW6yd8Uz43ZU0gj5mDahWk8oBJPxA0IRBsoXyWtGRY
AmValt5KaeTt8z0dLSM4RRY1s9S8a/D5qdxTTGECAwEAaAAMA0GCSqSqsGSIb3DQEB
```

Copiare tutto il contenuto della richiesta e inviarlo alla CA.

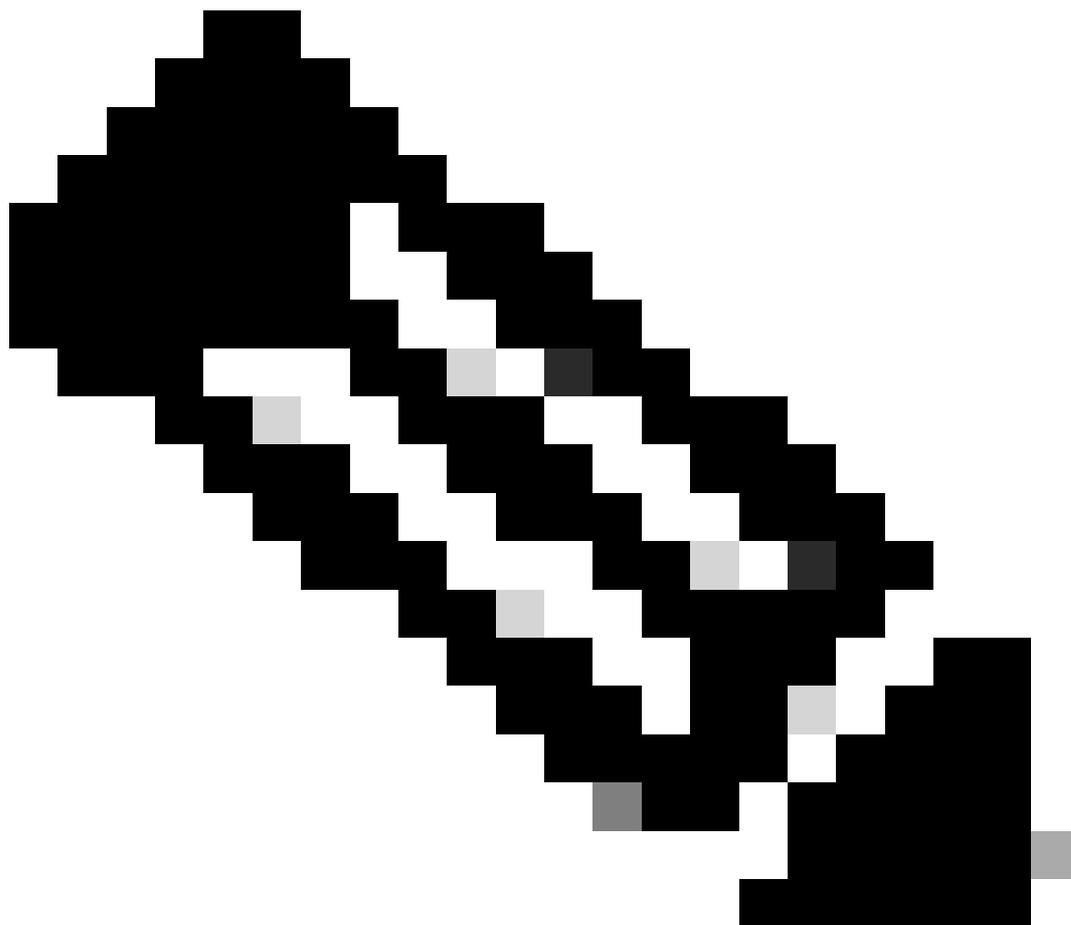
La CA utilizza la propria chiave privata per eseguire la verifica della firma sul CSR.

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



The screenshot shows the 'Key Ring - Cisco_Test' configuration page. The 'Certificate' field is highlighted with a red box and contains the following text:

```
-----BEGIN CERTIFICATE-----
MIIDSzCCApugAwIBAgIBAgjANBgqhkiG9w0BAQsFADBhYMQswCQYDVQQGEwJVUzEL
MAKGA1UECAwCQ0EwFATBgNVBAcMDERlZmF1bH0gQ2l0eTEwMDUyMDEwMDUyMDEw
Y28gQUNJIFRlYW0xMDEwMDUyMDEwMDUyMDEwMDUyMDEwMDUyMDEwMDUyMDEw
MjgwNDE5MDhaMGUxMDEwMDUyMDEwMDUyMDEwMDUyMDEwMDUyMDEwMDUyMDEw
Q2lZMDE5MDhaMGUxMDEwMDUyMDEwMDUyMDEwMDUyMDEwMDUyMDEwMDUyMDEw
LWFwawMxLmNpc2NvLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
ALJA5N1wzE7WmbLK35pTd06FwH3M2ZmIeCDw6SktDTqaMHhQdKYEK0UgGdyRdP
```



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 a [Fabric > Fabric Policies > Policies > Pod > Management Access > Default](#).

System Tenants **Fabric** Virtual Networking Admin Operations Apps Integrations

Inventory **Fabric Policies** Access Policies

Policies

- Quick Start
- Pods
- Switches
- Modules
- Interfaces
- Policies**
 - Pod
 - Date and Time
 - SNMP
 - Management Access
 - default**
 - Switch
 - Interface
 - Global
 - Monitoring
 - Troubleshooting
 - Geolocation
 - Macsec
 - Analytics
 - Tenant Quota
 - Annotations

Management Access - default

Policy Faults History

Allow Credentials: Disabled Enabled

Request Throttle: Disabled Enabled

HTTPS

Admin State: Enabled

Port: 443

Allow Origins: http://127.0.0.1:8000

Allow Credentials: Disabled Enabled

SSL Protocols: TLSv1.2 TLSv1.3

DH Param: 1024 2048 4096 None

Request Throttle: Disabled Enabled

Admin KeyRing: **Cisco_Test**

Oper KeyRing: uni/userext/pkiext/keyring-Cisco_Test

Client Certificate TP: select an option

Client Certificate Authentication state: Disabled Enabled

SSH access via WEB

Admin State: Enabled

Port: 4200

MACS: hmac-sha1 hmac-sha2-256 hmac-sha2-512

KEX Algorithms: aes256-gcm@openssh.com, chacha20-poly1305@openssh.com, curve25519-sha256, curve25519-sha256@libssh.org, diffie-hellman-group1-sha1, diffie-hellman-group14-sha1, diffie-hellman-group14-sha256, diffie-hellman-group16-sha512, ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521

SSL Cipher Configuration:

ID	State
CHACHA20	Enabled
DHE-RSA-AES128-SHA	Disabled
DHE-RSA-AES256-SHA	Disabled

Show Usage Reset Submit

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

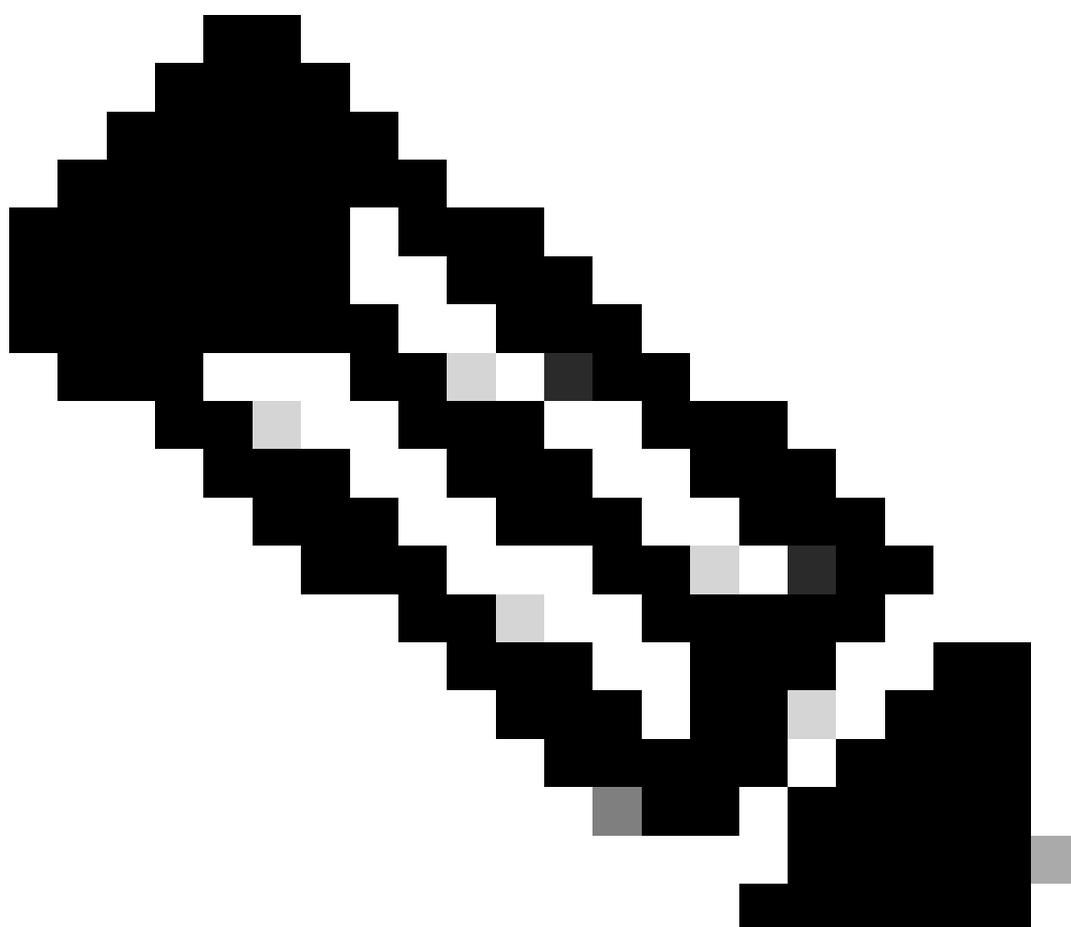
Dopo aver effettuato l'accesso all'interfaccia utente grafica di APIC, l'APIC utilizza il certificato firmato dall'autorità di certificazione per comunicare. Visualizzare le informazioni sul certificato nel browser per verificarle.



APIC (dlc-aci06-apic1.cisco.com) X



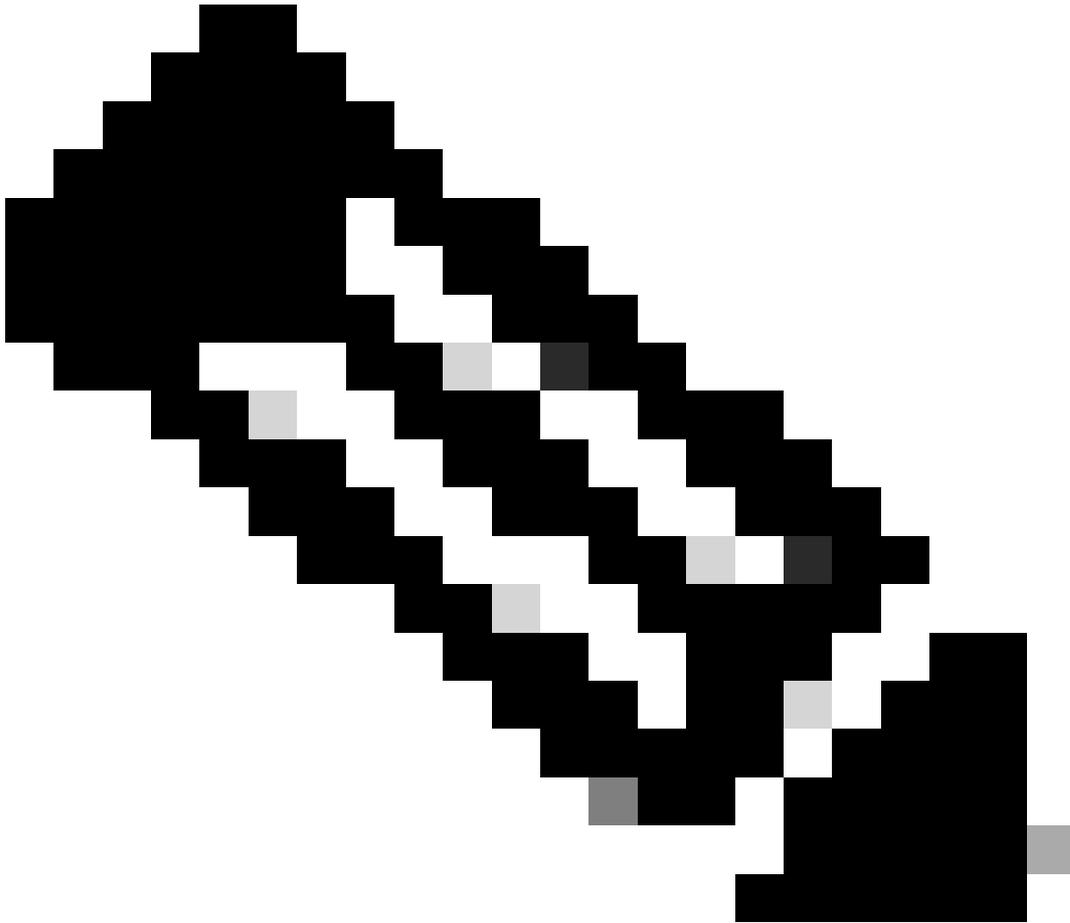
https://dlc-aci06-apic1.cisco.com



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.

Name	HTTP			HTTPS		SSH
	HTTP State	HTTP Port	HTTP Redirect	HTTPS State	HTTPS Port	SSH State
default	enabled	80	disabled	enabled	443	enabled

Properties

- Date Time Policy: default
- Resolved Date Time Policy: default
- ISIS Policy: select a value
- Resolved ISIS Policy: default
- COOP Group Policy: select a value
- Resolved COOP Group Policy: default
- BGP Route Reflector Policy: select a value
- Resolved BGP Route Reflector Policy: default
- Management Access Policy: select a value**
- Resolved Management Access Policy: **New**
- SNMP Policy: 1AD1C
- Resolved SNMP Policy: default
- MACsec Policy: fabric
- Resolved MACsec Policy: fabric

Create Management Access Policy

Show Usage Reset Submit

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).