Konfigurieren des HTTPS-Zertifikats für die ACI APIC-GUI

Inhalt

Einleitung

Dieses Dokument beschreibt die Konfiguration von benutzerdefiniertem SSL und selbstsignierten SSL-Zertifikaten.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Digitale Signaturen und digitale Zertifikate
- Zertifikatausstellungsprozess durch die Zertifizierungsstelle (Certificate Authority, CA)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

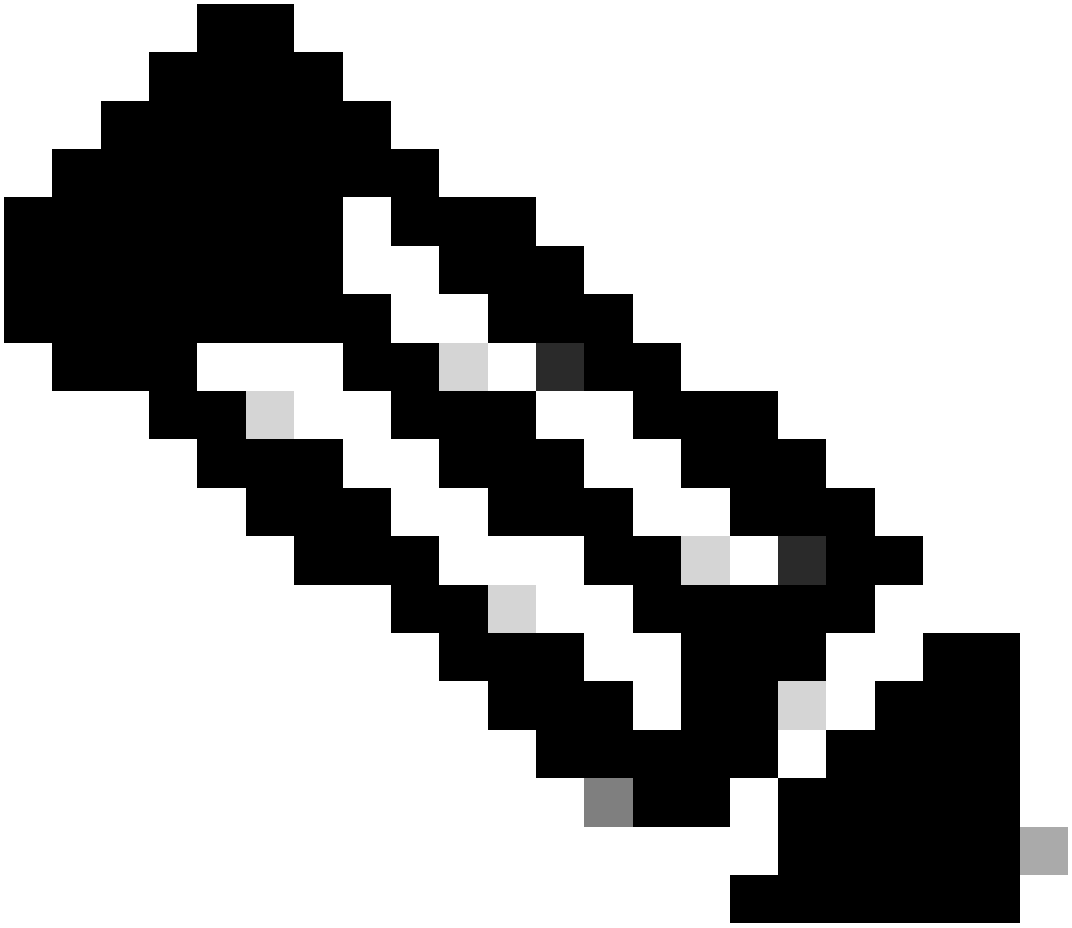
Nach der Initialisierung des Geräts verwendet es das selbstsignierte Zertifikat als SSL-Zertifikat für HTTPS. Das selbstsignierte Zertifikat ist 1000 Tage gültig.

Standardmäßig verlängert das Gerät automatisch ein neues selbstsigniertes Zertifikat und generiert es einen Monat vor Ablauf des selbstsignierten Zertifikats.

Konfigurationen

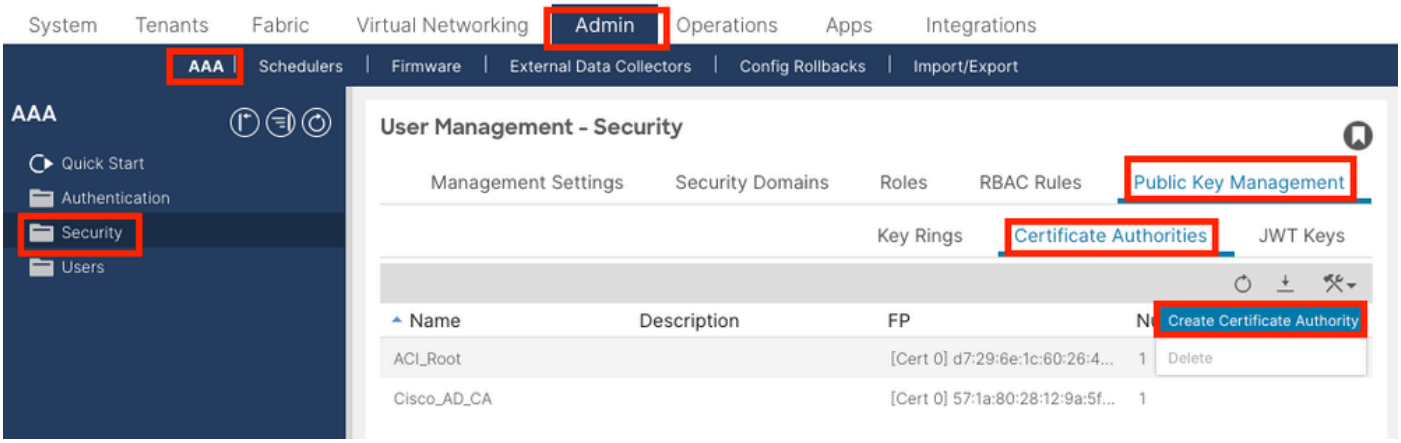
Das Gerät verwendet ein selbstsigniertes Zertifikat. Beim Zugriff auf die APIC-GUI weist der Browser darauf hin, dass das Zertifikat nicht vertrauenswürdig ist. Um dieses Problem zu beheben, wird in diesem Dokument eine vertrauenswürdige Zertifizierungsstelle zum Signieren des Zertifikats verwendet.

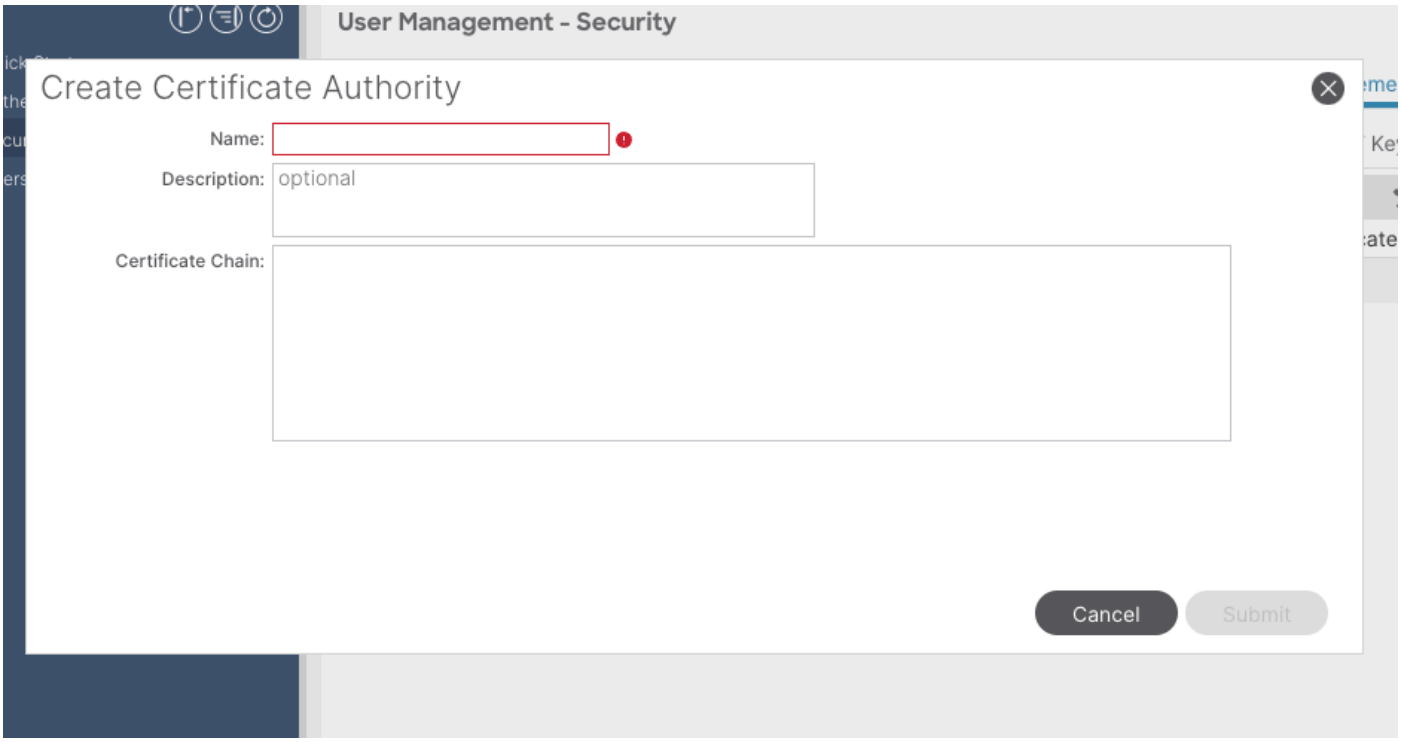
Schritt 1: Stammzertifikat oder Zwischenzertifikat der Zertifizierungsstelle importieren



Hinweis: Wenn Sie das Zertifikat der Zertifizierungsstelle für die direkte Signierung verwenden, können Sie das Zertifikat der Zertifizierungsstelle importieren. Wenn Sie jedoch ein Zwischenzertifikat zum Signieren verwenden, müssen Sie die gesamte Zertifikatkette importieren, d. h. das Stammzertifikat und die weniger vertrauenswürdigen Zwischenzertifikate.

Navigieren Sie in der Menüleiste zu Admin > AAA > Security > Public Key Management > Certificate Authorities.





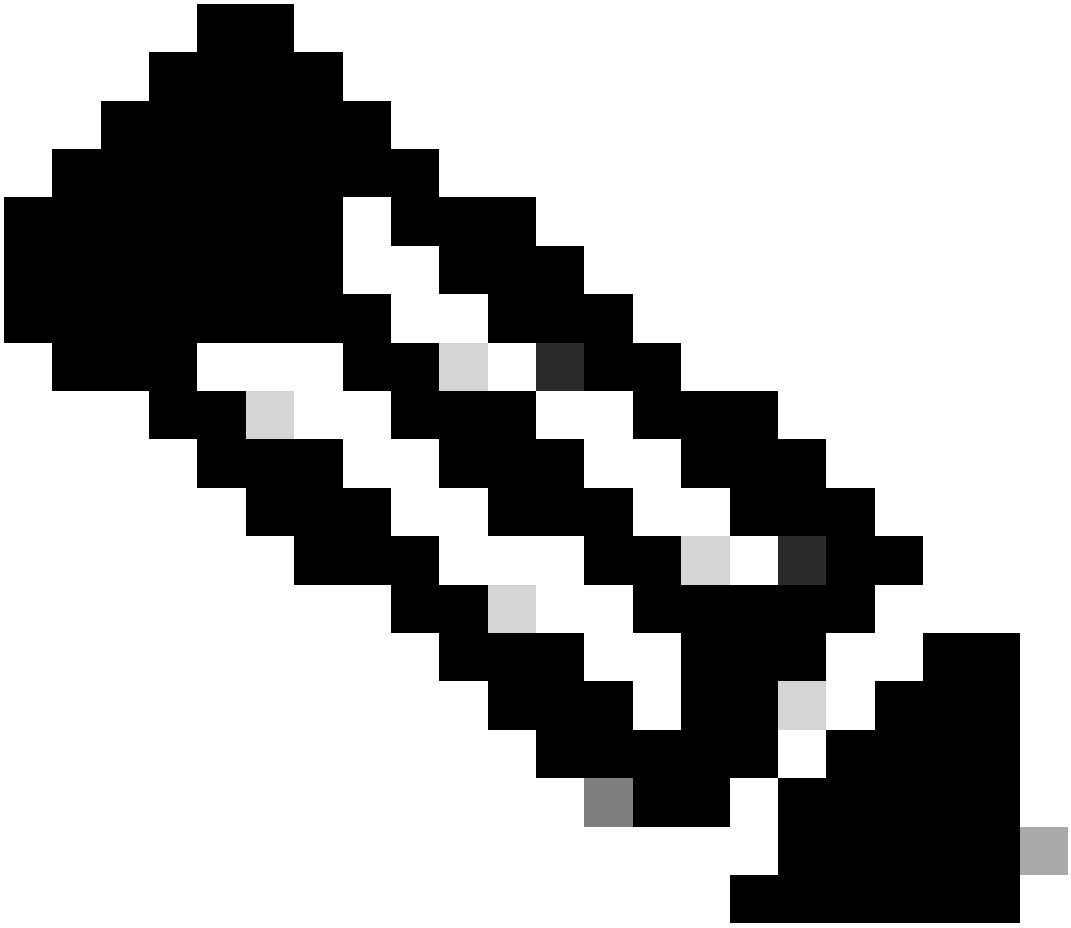
Name: **Erforderlich**.

Formulieren Sie den Inhalt gemäß Ihren Benennungsregeln. Es kann _ enthalten, darf jedoch keine englischen Sonderzeichen enthalten, wie z. B.:
, . ; ' " : | + * / = ` ~ ! @ # $ % ^ & ( ) und Leerzeichen.

Beschreibung: **Optional**.

Zertifizierungskette: **erforderlich**.

Füllen Sie das Zertifikat des vertrauenswürdigen Zertifizierungsstellen-Stammzertifikats und das Zwischenzertifikat der Zertifizierungsstelle aus.



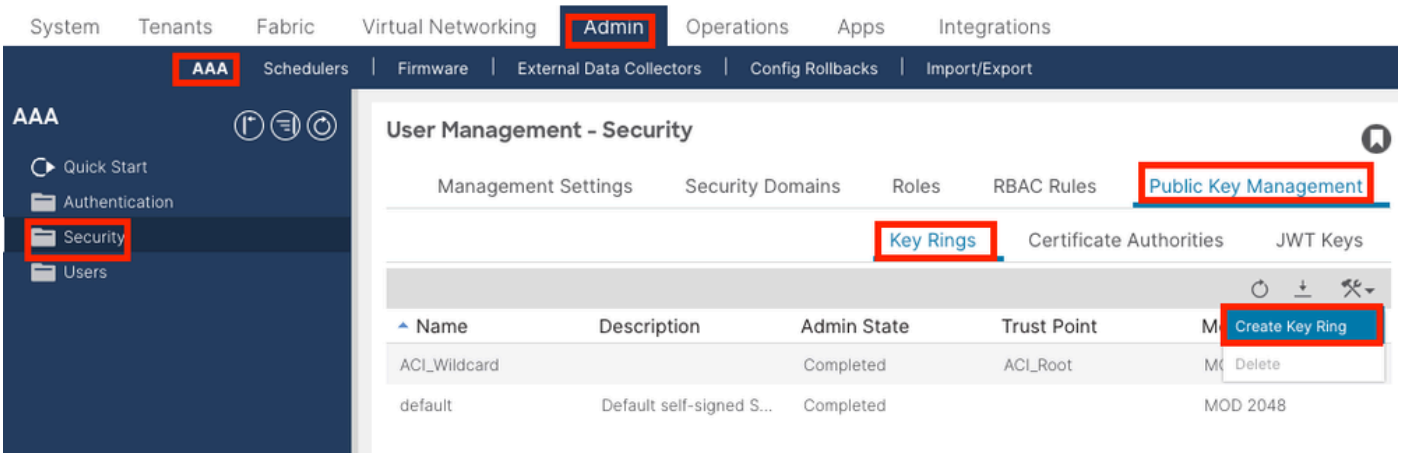
Hinweis: Jedes Zertifikat muss einem festen Format entsprechen.

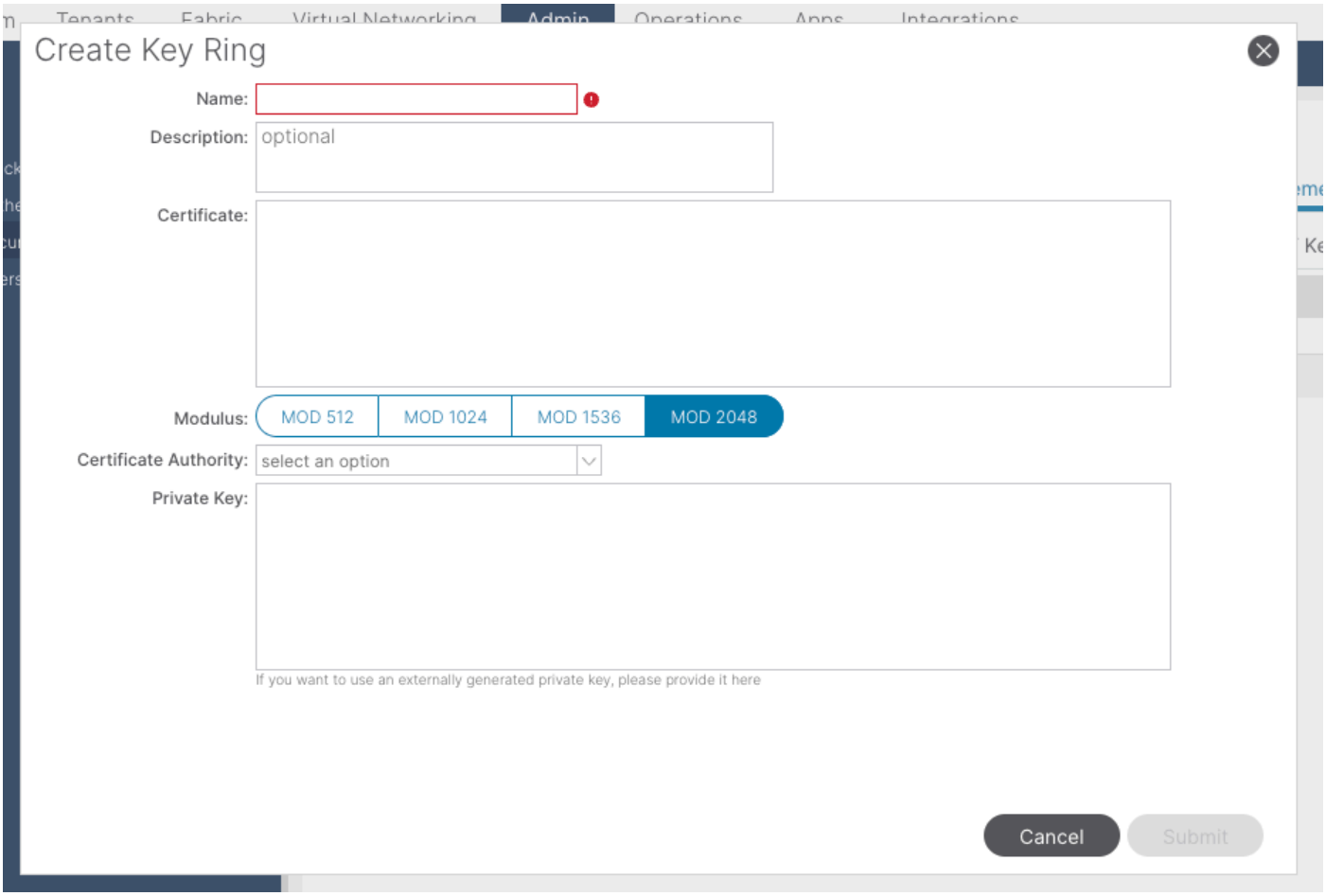
-----BEGIN CERTIFICATE----- INTER-CA-2 CERTIFICATE CONTENT HERE -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- INTER-CA-1 CERTIFICATE CONTENT HERE -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- ROOT-CA CERTIFICATE CONTENT HERE -----END CERTIFICATE-----

Klicken Sie auf die Schaltfläche "**Senden**".

Schritt 2: Keyring erstellen

Navigieren Sie in der Menüleiste zu Admin > AAA > Security > Public Key Management > Key Rings.





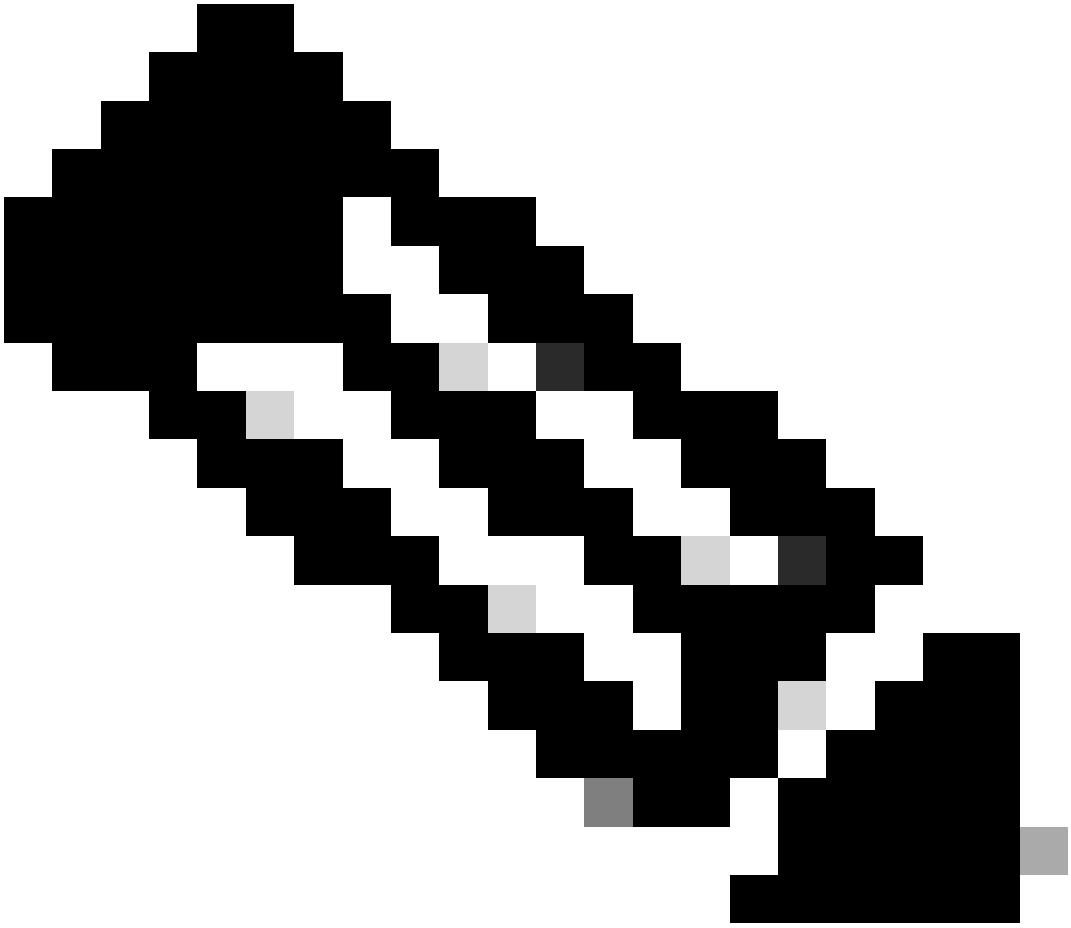
Name:**Erforderlich** (geben Sie einen Namen ein).

Zertifikat**: Fügen Sie** keine Inhalte hinzu, wenn Sie mithilfe des Cisco APIC über den Keyring eine CSR-Anfrage (Certificate Signing Request) erstellen. Alternativ können Sie den signierten Zertifikatsinhalt hinzufügen, wenn Sie bereits über einen Zertifikatsinhalt verfügen, der von der Zertifizierungsstelle aus den vorherigen Schritten signiert wurde, indem Sie einen privaten Schlüssel und einen CSR außerhalb des Cisco APIC generieren.

Modul: **Erforderlich** (Klicken Sie auf das Optionsfeld, um die gewünschte Stärke der Taste anzuzeigen).

Zertifizierungsstelle: **Erforderlich**. Wählen Sie aus der Dropdown-Liste die Zertifizierungsstelle aus, die Sie zuvor erstellt haben.

Privater Schlüssel: **Fügen Sie** keine Inhalte hinzu, wenn Sie mit dem Cisco APIC über den Keyring eine CSR-Anfrage erstellen. Sie können auch den privaten Schlüssel hinzufügen, der zum Generieren des CSR für das von Ihnen eingegebene signierte Zertifikat verwendet wird.

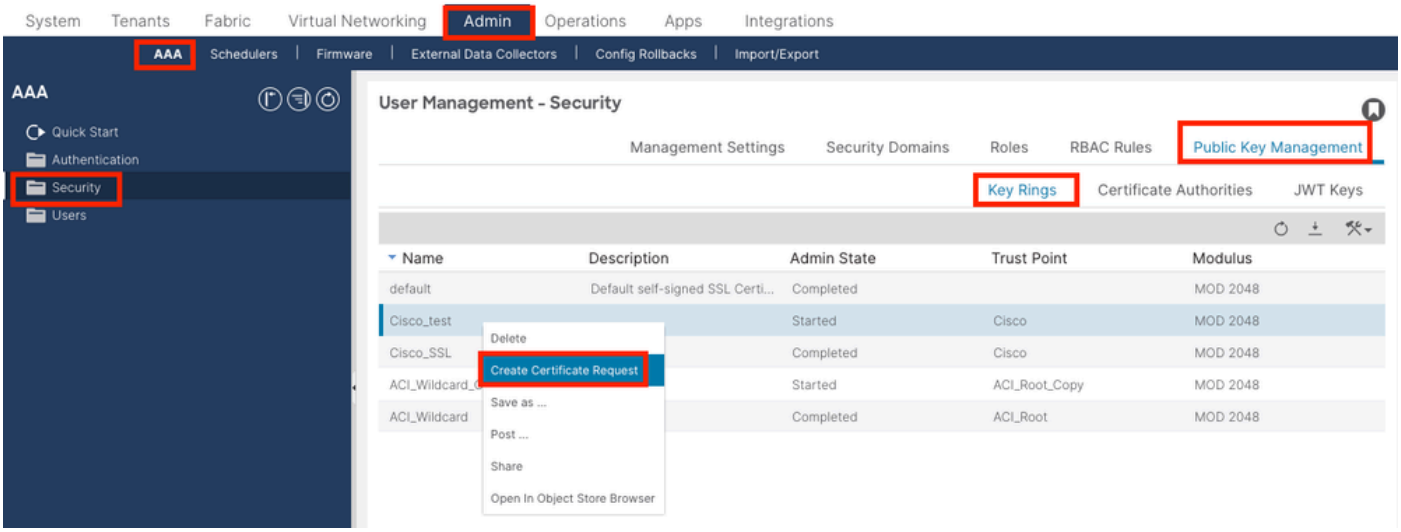


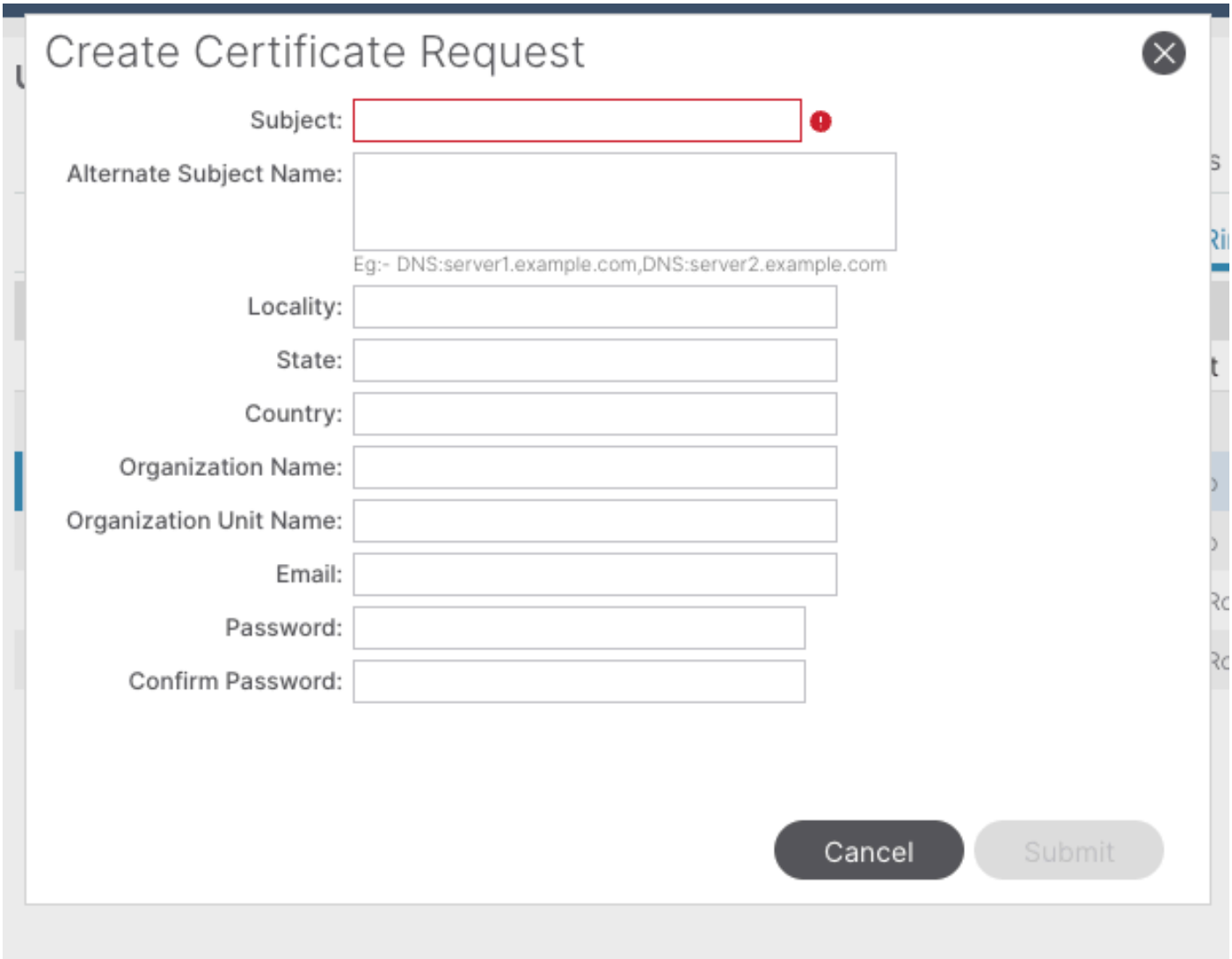
Hinweis: Wenn Sie den vom System generierten privaten Schlüssel und die CSR-Anfrage nicht verwenden und keinen benutzerdefinierten privaten Schlüssel und kein Zertifikat verwenden möchten, müssen Sie nur vier Felder ausfüllen: Name, Zertifikat, Zertifizierungsstelle und Privater Schlüssel. Nach dem Absenden müssen Sie nur den letzten Schritt, Schritt 5, durchführen.

Klicken Sie auf die Schaltfläche "**Senden**".

Schritt 3: Privaten Schlüssel und CSR generieren

Navigieren Sie in der Menüleiste zu Admin > AAA > Security > Public Key Management > Key Rings.



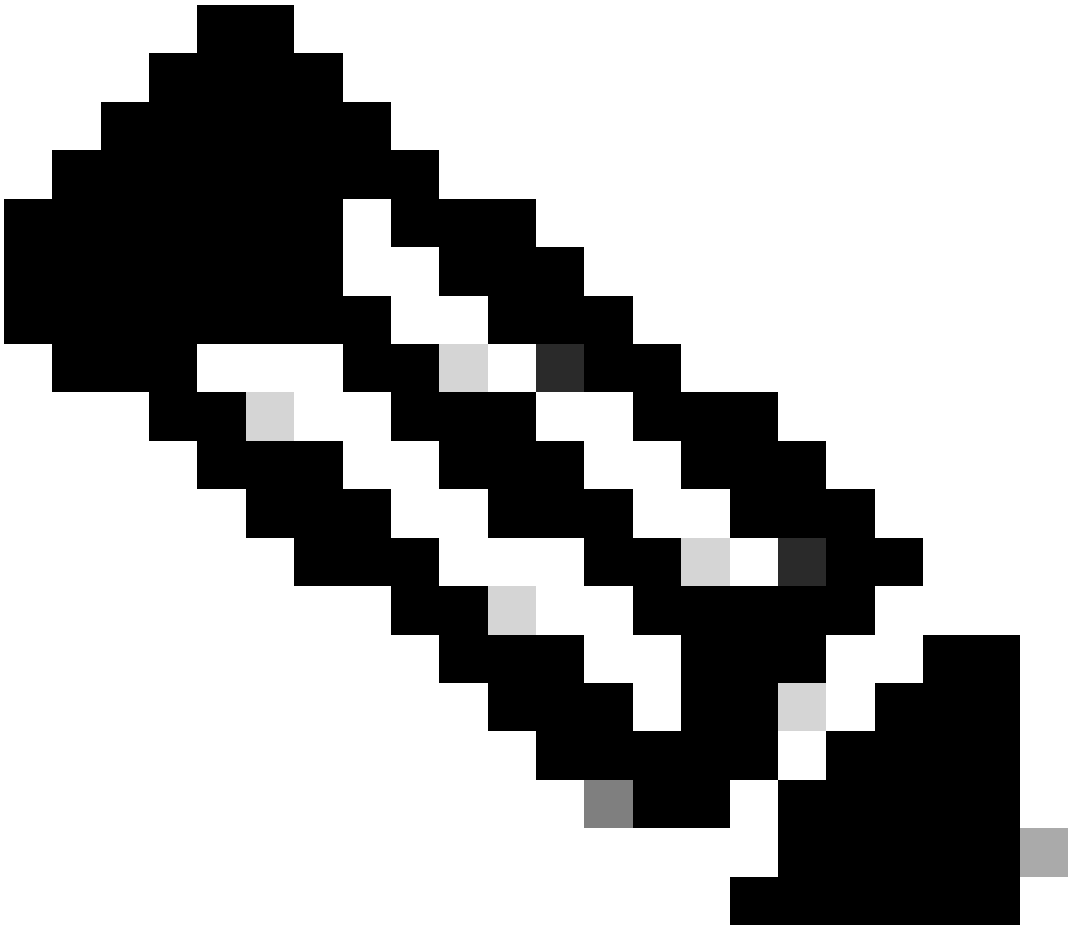


Betreff: **Erforderlich**. Geben Sie den allgemeinen Namen (CN) des CSR ein.

Sie können den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) der Cisco APICs mithilfe eines Platzhalters eingeben. In einem modernen Zertifikat wird jedoch generell empfohlen, einen identifizierbaren Namen des Zertifikats und den FQDN aller Cisco APICs im Feld Alternativer Antragstellername (auch als SAN bezeichnet - Alternativer Antragstellername) einzugeben, da viele moderne Browser erwarten den FQDN im SAN-Feld.

Alternativer Betreffname: **Pflichtfeld.** Geben Sie den FQDN aller Cisco APICs wie DNS:apic1.example.com,DNS:apic2.example.com,DNS:apic3.example.com oder DNS:*example.com ein.

Wenn Sie möchten, dass SAN mit einer IP-Adresse übereinstimmt, geben Sie die IP-Adressen der Cisco APICs in folgendem Format ein: IP:192.168.1.1.



Hinweis: In diesem Feld können Sie DNS-Namen (Domain Name Server), IPv4-Adressen oder eine Mischung aus beiden verwenden. IPv6-Adressen werden nicht unterstützt.

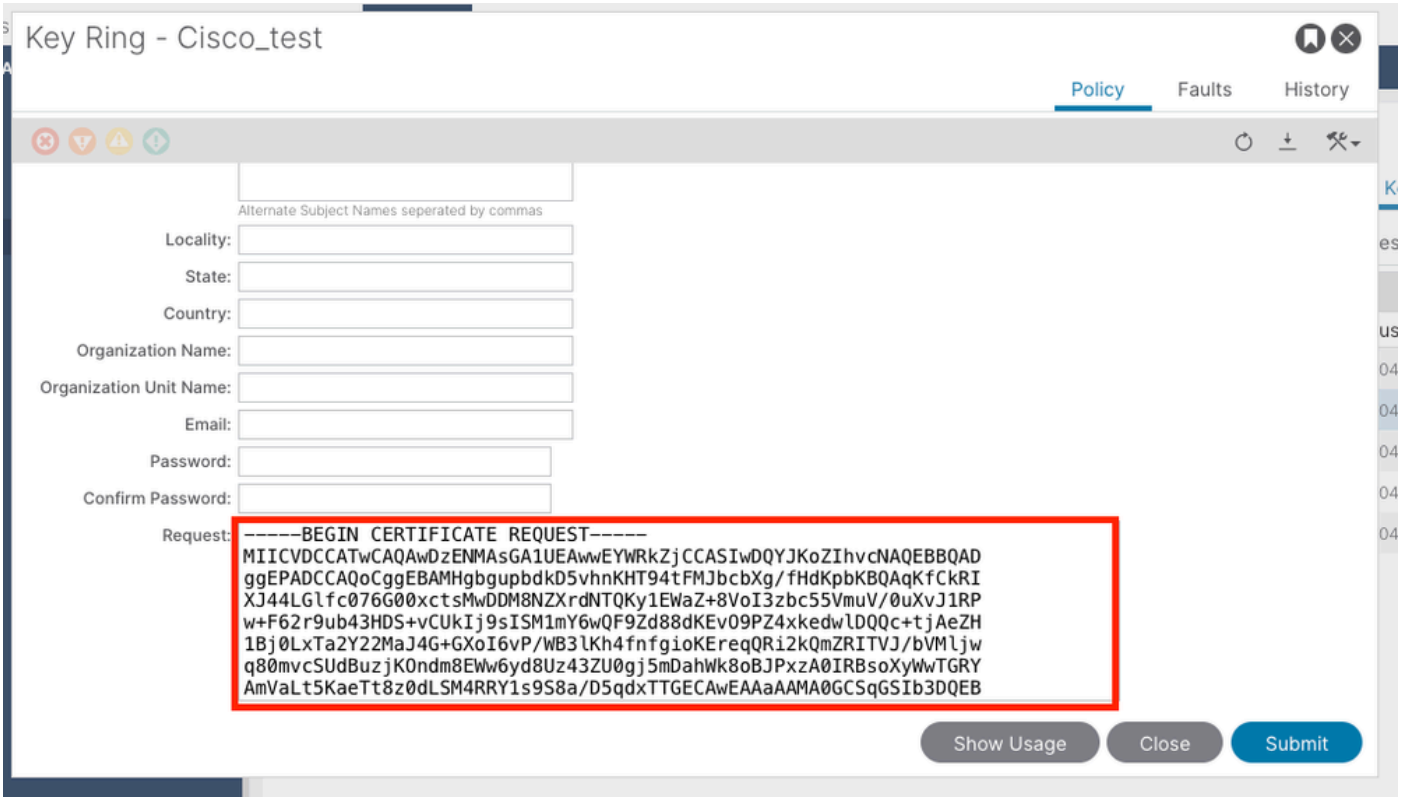
Füllen Sie die übrigen Felder entsprechend den Anforderungen der Zertifizierungsstelle aus, die Sie für die Ausstellung des Zertifikats beantragen.

Klicken Sie auf die Schaltfläche "**Senden**".

Schritt 4: Holen Sie sich den CSR, und senden Sie ihn an die Zertifizierungsstelle.

Navigieren Sie in der Menüleiste zu Admin > AAA > Security > Public Key Management > Key Rings.

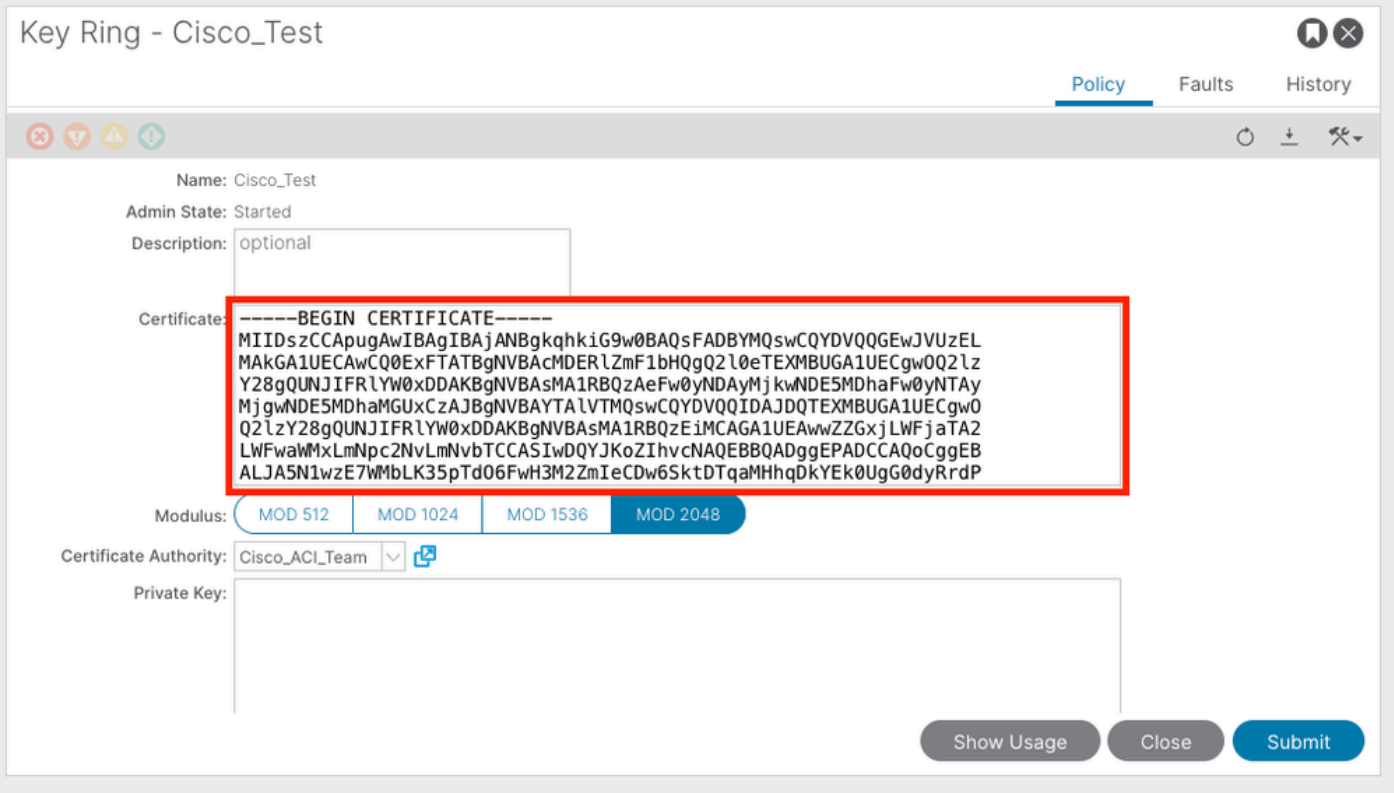
Doppelklicken Sie auf den Namen des **Keyrings** erstellen und suchen Sie die Option **Request**. Der Inhalt der Anforderung ist die CSR.

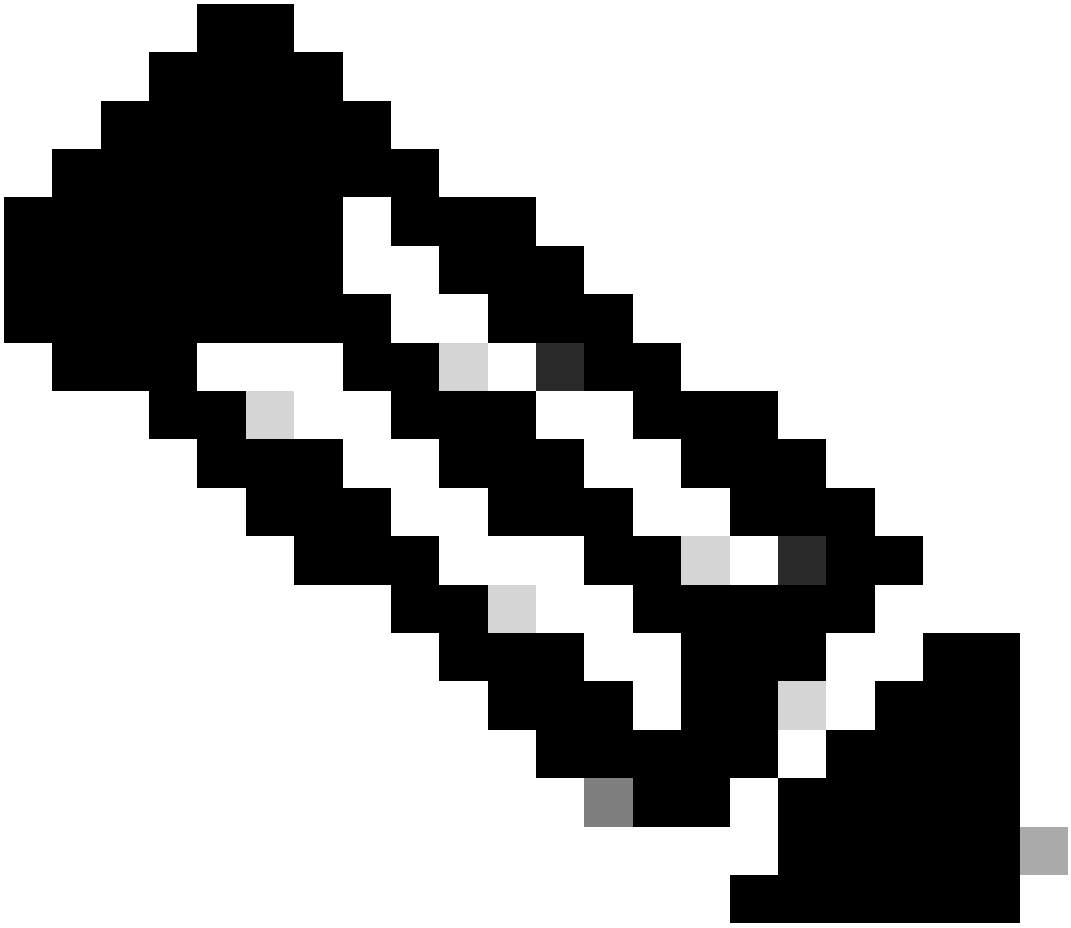


Kopieren Sie den gesamten Inhalt der Anforderung, und senden Sie ihn an Ihre Zertifizierungsstelle.

Die Zertifizierungsstelle verwendet ihren privaten Schlüssel, um die Signaturüberprüfung für Ihren CSR durchzuführen.

Nachdem das signierte Zertifikat von der Zertifizierungsstelle erhalten wurde, kopiert es das Zertifikat in das Zertifikat.


Key Ring - Cisco_Test
Policy
Faults
History
Name: Cisco_Test
Admin State: Started
Description: optional
Certificate:
-----BEGIN CERTIFICATE-----
MIIDszCCApugAwIBAgIBAjANBgkqhkiG9w0BAQsFADBYMQswCQYDVQQGEwJVUzEL
MAkGA1UECAwCQ0ExFTATBgNVBAcMDERlZmF1bHQgQ2l0eTEXMBUGA1UECgwOQ2lz
Y28gQUNJIFRlYW0xDDAKBgNVBAsMA1RBQzAeFw0yNDAyMjkwNDE5MDhaFw0yNTAy
MjgwNDE5MDhaMGUxCzAJBgNVBAYTAlVTMQswCQYDVQQIDAJDQTEXMBUGA1UECgwO
Q2lzY28gQUNJIFRlYW0xDDAKBgNVBAsMA1RBQzEiMCAGA1UEAwwZZGxjLWFjaTA2
LWFwaWMxLmNpc2NvLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
ALJA5N1wzE7WMbLK35pTdO6FwH3M2ZmIeCDw6SktDTqaMHhqDkYEk0UgG0dyRrdP
Modulus:
MOD 512
MOD 1024
MOD 1536
MOD 2048
Certificate Authority: Cisco_ACI_Team
Private Key:
Show Usage
Close
Submit



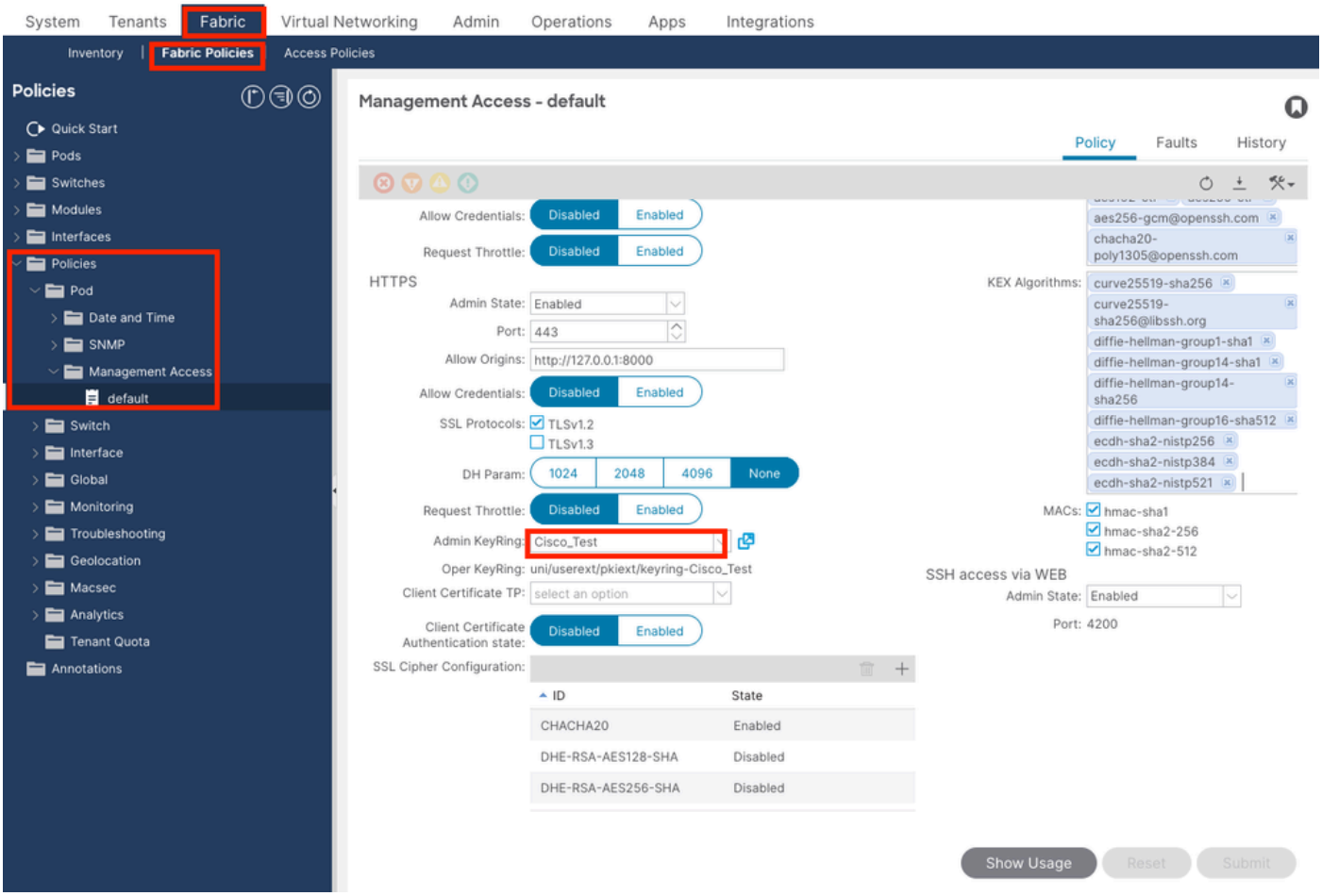
Hinweis: Jedes Zertifikat muss einem festen Format entsprechen.

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

Klicken Sie auf die Schaltfläche **"Senden**".

Schritt 5: Aktualisieren des Signaturzertifikats im Web

Navigieren Sie in der Menüleiste zu Fabric > Fabric Policies > Policies > Pod > Management Access > Default.



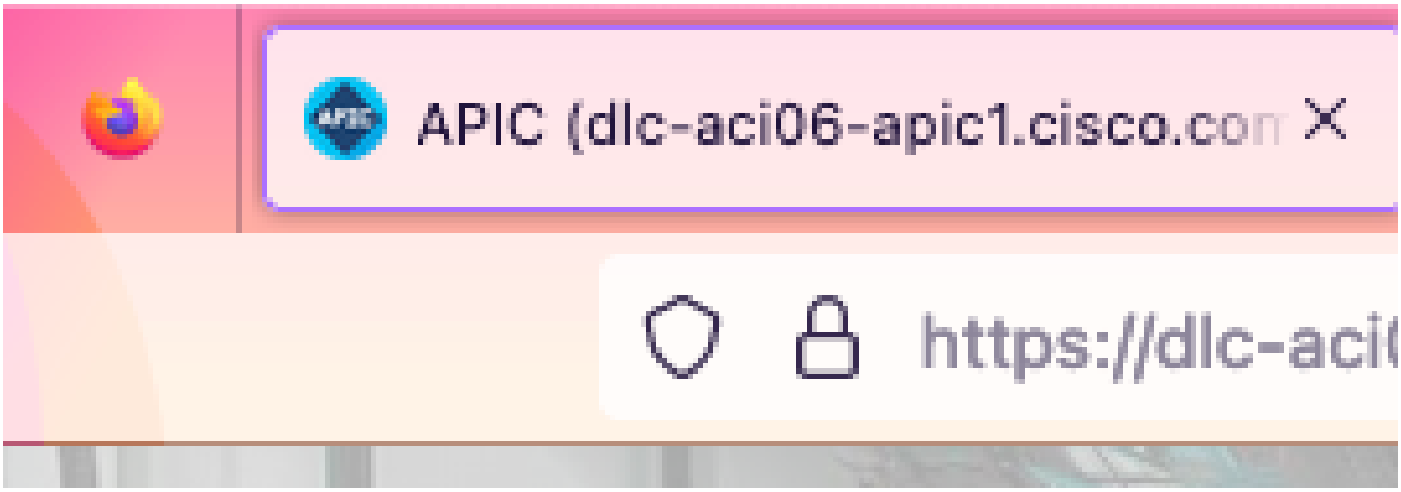
Wählen Sie in der Dropdown-Liste **Admin KeyRing** (Admin-Schlüsselring) den gewünschten Schlüsselring aus.

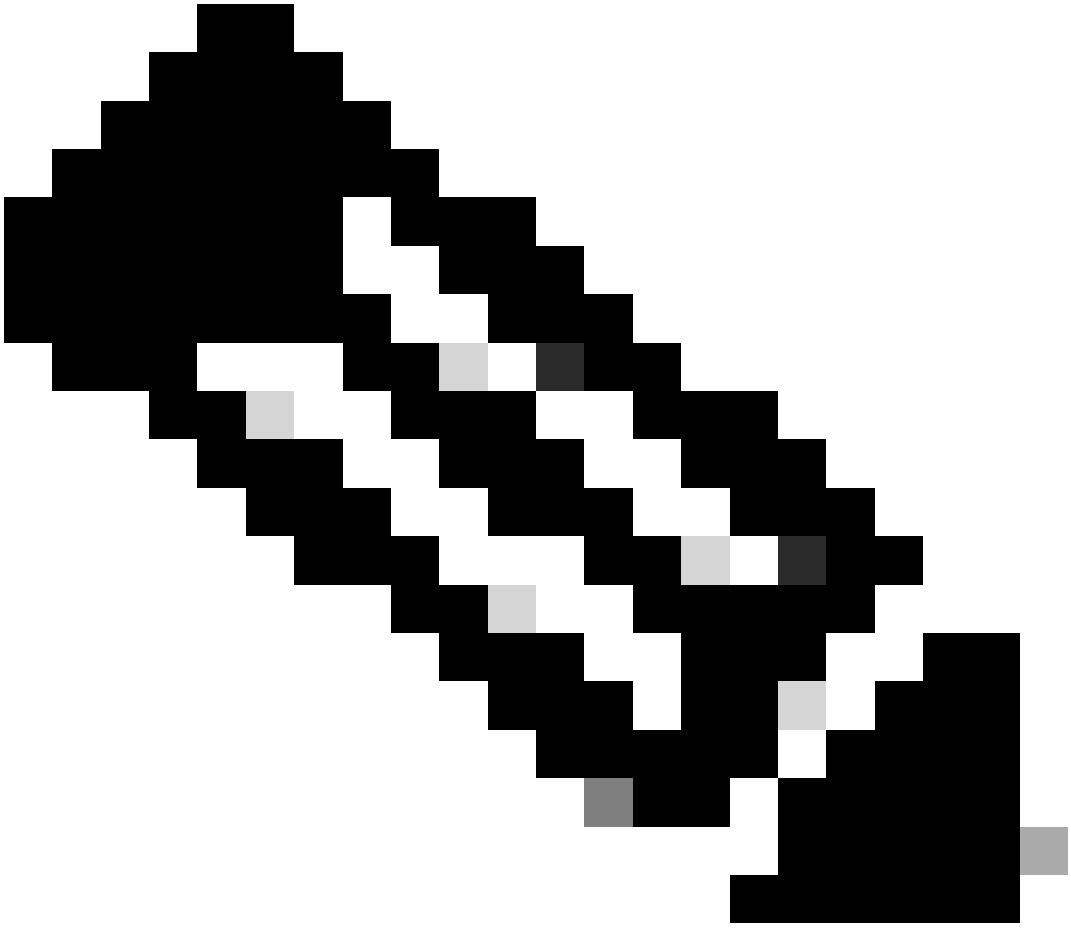
Klicken Sie auf die Schaltfläche "**Senden**".

Nachdem Sie auf die Schaltfläche zum Absenden geklickt haben, tritt aus Zertifikatgründen ein Fehler auf. Mit dem neuen Zertifikat aktualisieren.

Überprüfung

Nach dem Zugriff auf die APIC-GUI kommuniziert der APIC über das CA-signierte Zertifikat. Zeigen Sie die Zertifikatinformationen im Browser an, um sie zu überprüfen.



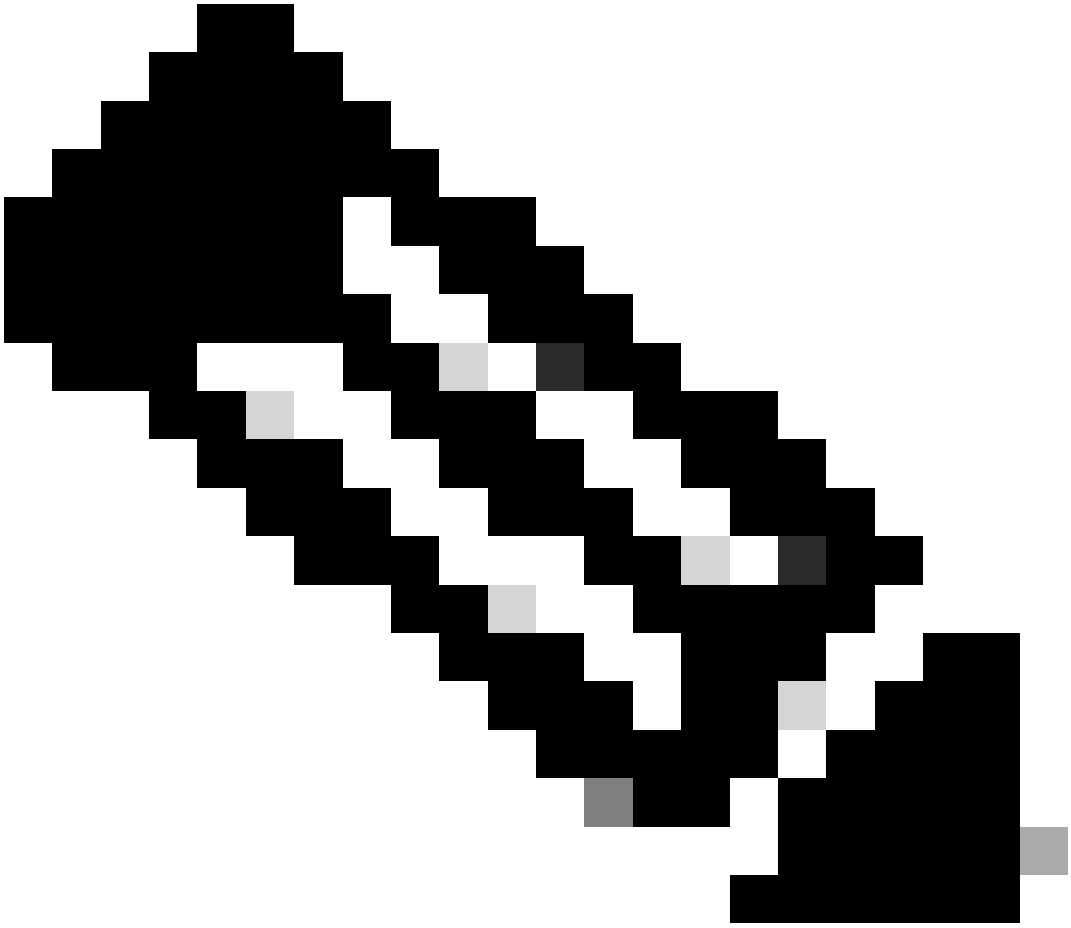


Hinweis: Die Methoden zum Anzeigen von HTTPS-Zertifikaten in verschiedenen Browsern sind nicht identisch. Spezifische Methoden finden Sie im Benutzerhandbuch Ihres Browsers.

Fehlerbehebung

Wenn der Browser weiterhin eine Meldung ausgibt, dass die APIC-GUI nicht vertrauenswürdig ist, prüfen Sie im Browser, ob das Zertifikat der GUI mit dem im Keyring übermittelten Zertifikat übereinstimmt.

Sie müssen dem **CA-Stammzertifikat** vertrauen, das das Zertifikat auf Ihrem Computer oder Browser ausgestellt hat.

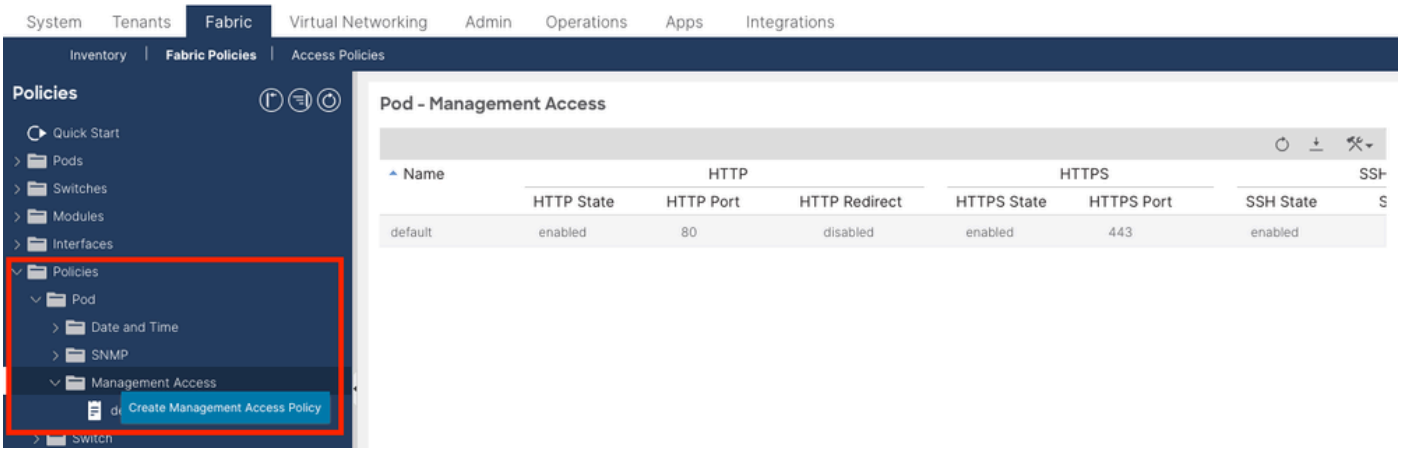


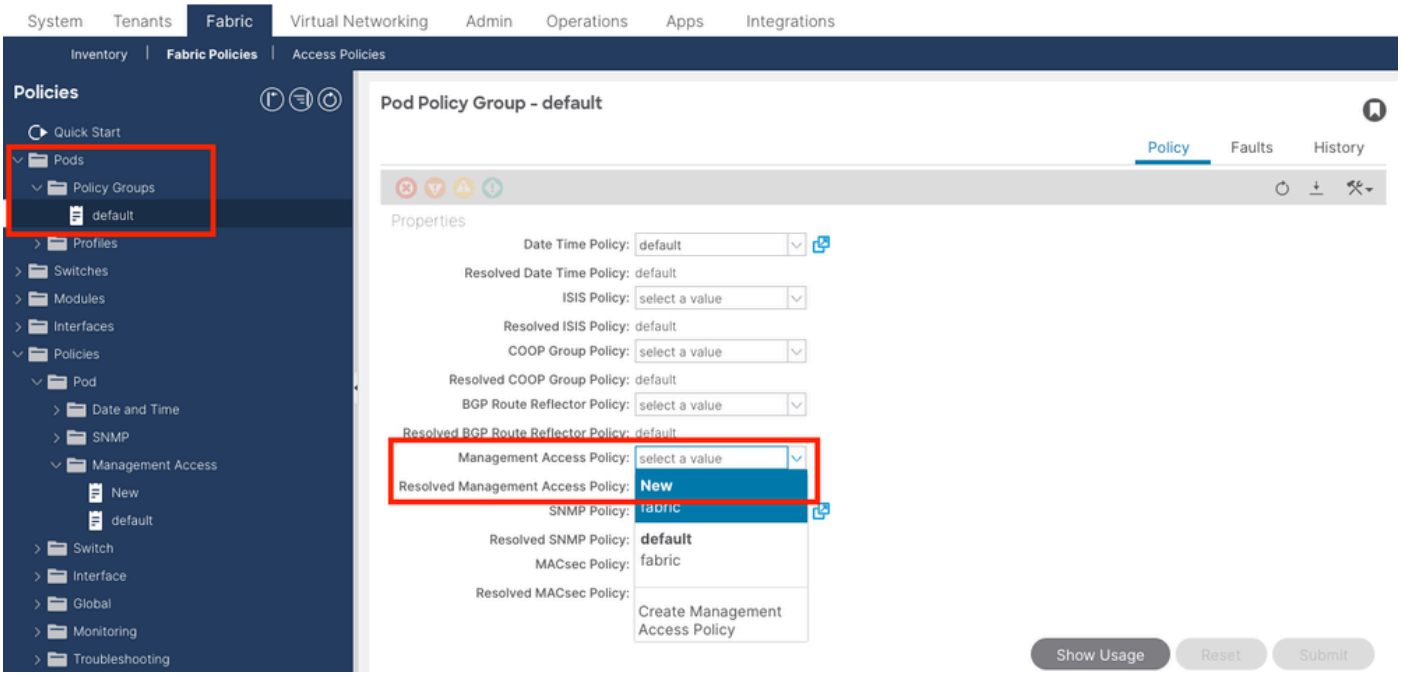
Hinweis: Der Google Chrome-Browser muss das **SAN** des Zertifikats überprüfen, um diesem Zertifikat zu vertrauen.

In APICs, die selbstsignierte Zertifikate verwenden, können in seltenen Fällen Warnungen vor Ablauf des Zertifikats auftreten.

Suchen Sie das Zertifikat in Keyring, verwenden Sie das Tool zum Analysieren des Zertifikats, um das Zertifikat zu analysieren, und vergleichen Sie es mit dem im Browser verwendeten Zertifikat.

Wenn das Zertifikat im Keyring erneuert wird, erstellen Sie eine neue Management-Zugriffsrichtlinie, und wenden Sie sie an.





Wenn das Zertifikat im Keyring nicht automatisch erneuert wird, wenden Sie sich an Cisco TAC, um weitere Unterstützung zu erhalten.

Zugehörige Informationen

- Cisco APIC Security Konfigurationsleitfaden, Version 5.2(x)
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.