Konfigurieren der Zertifikatregistrierung mit dem ACME-Protokoll auf einer sicheren Firewall

Inhalt

- Einleitung
- Voraussetzungen
  - Anforderungen
  - Verwendete Komponenten
  - Anforderungen und Einschränkungen
  - Überlegungen zur Herabstufung
- Hintergrundinformationen
- Konfigurieren
  - Konfiguration der Voraussetzungen
  - ACME-Anmeldung bei ASDM
  - ACME-Registrierung mit Secure Firewall ASA CLI
- Überprüfung
  - Installiertes Zertifikat in ASA anzeigen
  - Syslog-Ereignisse
- Fehlerbehebung
  - Befehle zur Fehlerbehebung
  - Fehlercode
  - Grund
  - Mögliche Ursache oder Beseitigung
- Zugehörige Informationen

Einleitung

In diesem Dokument wird das Verfahren zum Registrieren eines TLS-Zertifikats (Transport Layer Security) mithilfe des ACME-Protokolls (Automated Certificate Management Environment) auf der sicheren ASA-Firewall beschrieben.

Voraussetzungen

Anforderungen

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

- Cisco Secure Firewall Adaptative Security Appliance (ASA)
- Public Key Infrastructure (PKI)

Verwendete Komponenten

- Cisco ASAv, Version 9.23.1
- Cisco ASDM Version 7.23(1).
- CA-Server (Certificate Authority), der das ACME-Protokoll unterstützt

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.

Anforderungen und Einschränkungen

Die aktuellen Anforderungen und Einschränkungen für die ACME-Registrierung bei Secure Firewall ASA sind:

- Unterstützt auf ASA-Version 9.23.1 und ASDM 7.23.1
- Nicht unterstützt in mehreren Kontexten

- ACME unterstützt nicht die Erstellung von Platzhalterzertifikaten. Bei jeder Zertifikatanforderung muss ein genauer Domänenname angegeben werden.

- Jeder über ACME registrierte Trustpoint ist auf eine Schnittstelle beschränkt, d. h. bei ACME registrierte Zertifikate können nicht über mehrere Schnittstellen hinweg gemeinsam genutzt werden.

- Schlüsselpaare werden automatisch generiert und können nicht für Zertifikate freigegeben werden, die über ACME registriert sind. Jedes Zertifikat verwendet eine eindeutige Tastenkombination, wodurch die Sicherheit erhöht, die Wiederverwendung von Schlüsseln jedoch eingeschränkt wird.

Überlegungen zur Herabstufung

Nach dem Downgrade auf eine Version, die die ACME-Registrierung bei Secure Firewall ASA (9.22 und älter) nicht unterstützt:

- Alle ACME-bezogenen TrustPoint-Konfigurationen, die neu bei 9.23.x oder neuer sind, gehen verloren.
- Alle über ACME registrierten Zertifikate sind weiterhin zugänglich. Die Verknüpfung des privaten Schlüssels wird jedoch nach dem ersten Speichern und Neustart nach dem Downgrade aufgehoben.

Wenn eine Herabstufung erforderlich ist, führen Sie die nächste empfohlene Problemumgehung durch:

1. Stellen Sie vor dem Downgrade sicher, dass die ACME-Zertifikate im PKCS12-Format

exportiert werden.
2. Stellen Sie vor dem Downgrade sicher, dass die ACME-Vertrauenspunktkonfiguration entfernt wird.
3. Importieren Sie nach dem Downgrade das PKCS12-Zertifikat. Der daraus resultierende Vertrauenspunkt bleibt bis zum Ablauf des über ACME ausgestellten Zertifikats gültig.

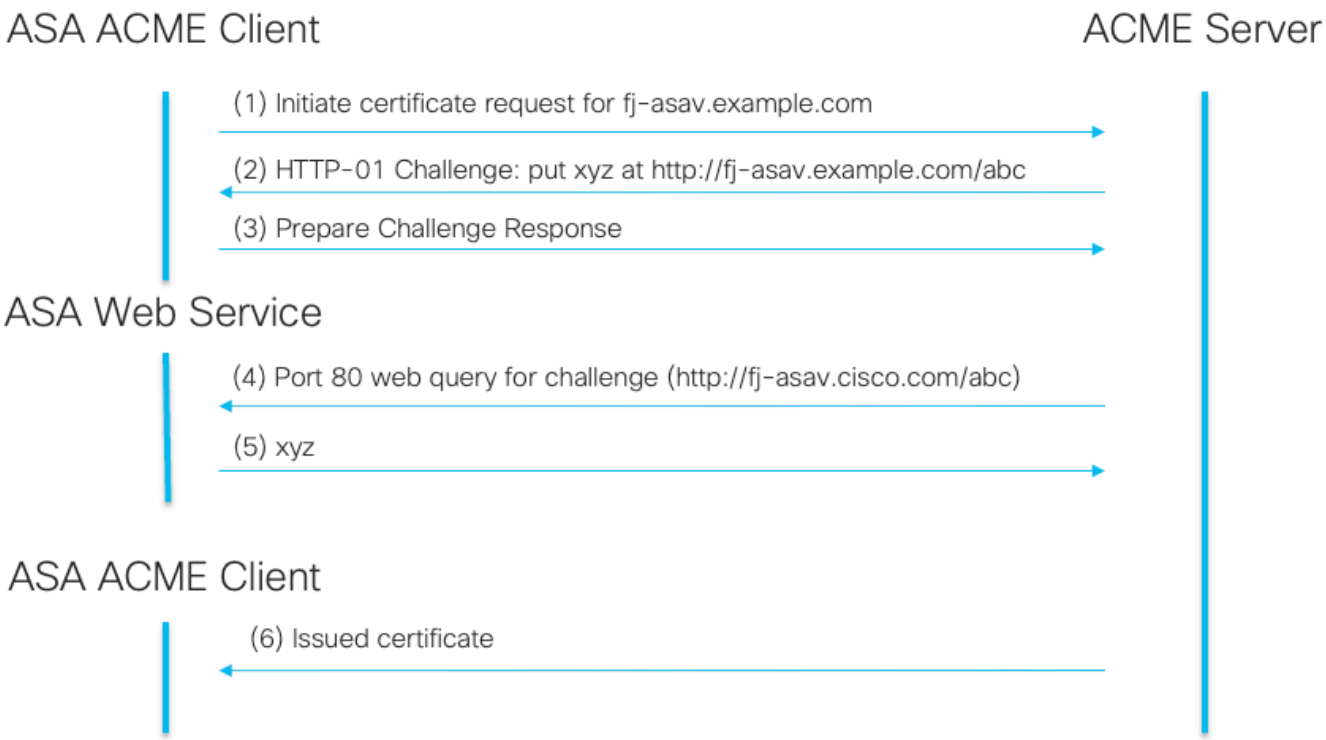
Hintergrundinformationen

Das ACME-Protokoll wurde entwickelt, um die Verwaltung von TLS-Zertifikaten für Netzwerkadministratoren zu optimieren. Mit ACME können Administratoren die Prozesse beim Erhalt und bei der Verlängerung von TLS-Zertifikaten automatisieren. Diese Automatisierung ist besonders nützlich, wenn Zertifizierungsstellen wie Let's Encrypt verwendet werden, die kostenlose, automatisierte und offene Zertifikate mit dem ACME-Protokoll anbieten.

ACME unterstützt die Ausstellung von DV-Zertifikaten (Domain Validation). Bei diesen Zertifikaten handelt es sich um eine Art digitales Zertifikat, das die Kontrolle des Zertifikatsinhabers über bestimmte Domänen bestätigt. Der Validierungsprozess für DV-Zertifikate wird in der Regel über einen HTTP-basierten Abfragemechanismus durchgeführt. Bei diesem Verfahren legt der Antragsteller eine bestimmte Datei auf seinem Webserver ab, die von der Zertifizierungsstelle (Certificate Authority, CA) überprüft wird, indem er auf die Datei über den HTTP-Server der Domäne zugreift. Der erfolgreiche Abschluss dieser Herausforderung zeigt der Zertifizierungsstelle, dass der Antragsteller die Kontrolle über die Domäne hat, sodass das DV-Zertifikat ausgestellt werden kann.

Die Registrierung erfolgt wie folgt:

1. Zertifikatanforderung initiieren: Der Client fordert ein Zertifikat vom ACME-Server an und gibt die Domäne(n) an, für die das Zertifikat erforderlich ist.
2. HTTP-01-Anforderung empfangen: Der ACME-Server stellt eine HTTP-01-Abfrage mit einem eindeutigen Token bereit, mit dem der Client die Domänenkontrolle überprüfen kann.
3. Vorbereitung auf die Challenge-Antwort:
    - Der Client erstellt eine Schlüsselautorisierung, indem er das Token des ACME-Servers mit seinem Kontoschlüssel kombiniert.
    - Der Client richtet seinen Webserver so ein, dass er diese Schlüsselautorisierung über einen bestimmten URL-Pfad bereitstellt.
4. ACME Server ruft Herausforderung ab: Der ACME-Server sendet eine HTTP GET-Anforderung an die angegebene URL, um die Schlüsselautorisierung abzurufen.
5. ACME Server verifiziert Besitz: Der Server überprüft, ob die abgerufene Schlüsselautorisierung mit dem erwarteten Wert übereinstimmt, um die Kontrolle des Clients über die Domäne zu bestätigen.
6. Ausstellungszertifikat: Nach erfolgreicher Validierung gibt der ACME-Server das SSL/TLS-Zertifikat an den Client aus.



ACME-Registrierung HTTP-01-Authentifizierungsablauf.

Die wichtigsten Vorteile des ACME-Protokolls für die Registrierung von TLS-Zertifikaten sind:

- ACME erleichtert die Beschaffung und Wartung von TLS-Domänenzertifikaten für die Secure Firewall ASA TLS-Schnittstellen. Durch diese Automatisierung werden manuelle Aufgaben erheblich reduziert und Zertifikate ohne ständige Überwachung auf dem neuesten Stand gehalten.
- Bei ACME-aktivierten Trustpoints werden Zertifikate automatisch erneuert, sobald sie ablaufen. Dadurch muss der Administrator weniger aufwändig agieren, die Sicherheit bleibt erhalten und ein unerwartetes Ablaufdatum des Zertifikats wird verhindert.

Konfigurieren

Konfiguration der Voraussetzungen

Bevor Sie den ACME-Registrierungsprozess einleiten, stellen Sie sicher, dass die folgenden Bedingungen erfüllt sind:

1. Auflösbarer Domänenname: Der Domänenname, für den Sie ein Zertifikat anfordern, muss vom ACME-Server auflösbar sein. Dadurch wird sichergestellt, dass der Server das Domäneneigentum überprüfen kann.
2. Sicherer Firewall-Zugriff auf ACME-Server: Die sichere Firewall muss über eine der Schnittstellen auf den ACME-Server zugreifen können. Dieser Zugriff muss nicht über die Schnittstelle erfolgen, für die das Zertifikat angefordert wird.
3. Verfügbarkeit von TCP-Port 80: TCP-Port 80 vom ACME CA-Server zu der Schnittstelle

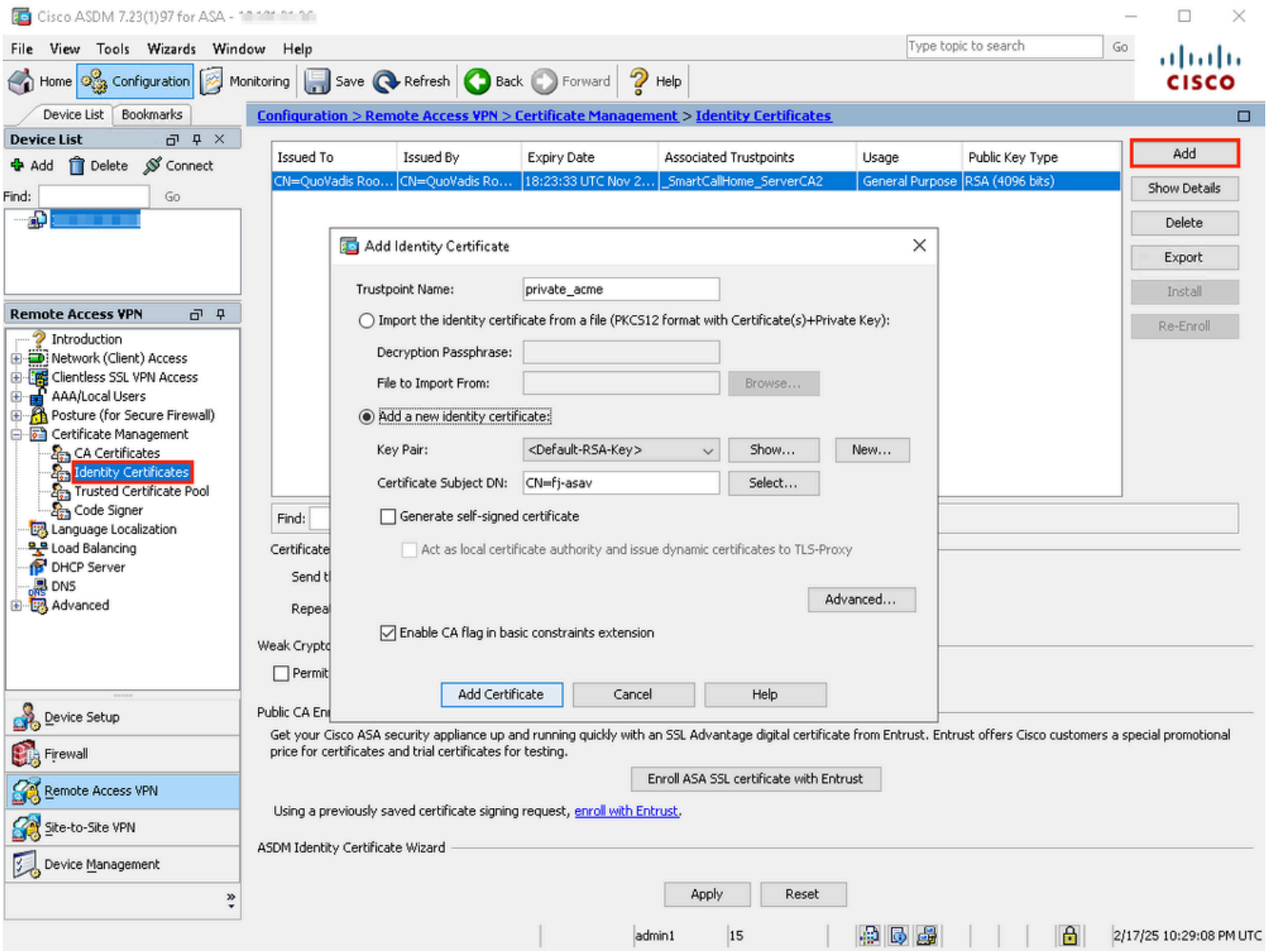
zulassen, die dem Domänennamen entspricht. Dies ist während des ACME-Austauschprozesses erforderlich, um die HTTP-01-Herausforderung abzuschließen.

Anmerkung: Während des Zeitraums, in dem Port 80 geöffnet ist, ist nur auf die ACME-Abfragedaten zugegriffen werden können.

ACME-Anmeldung bei ASDM

1. Hinzufügen eines neuen Identitätszertifikats

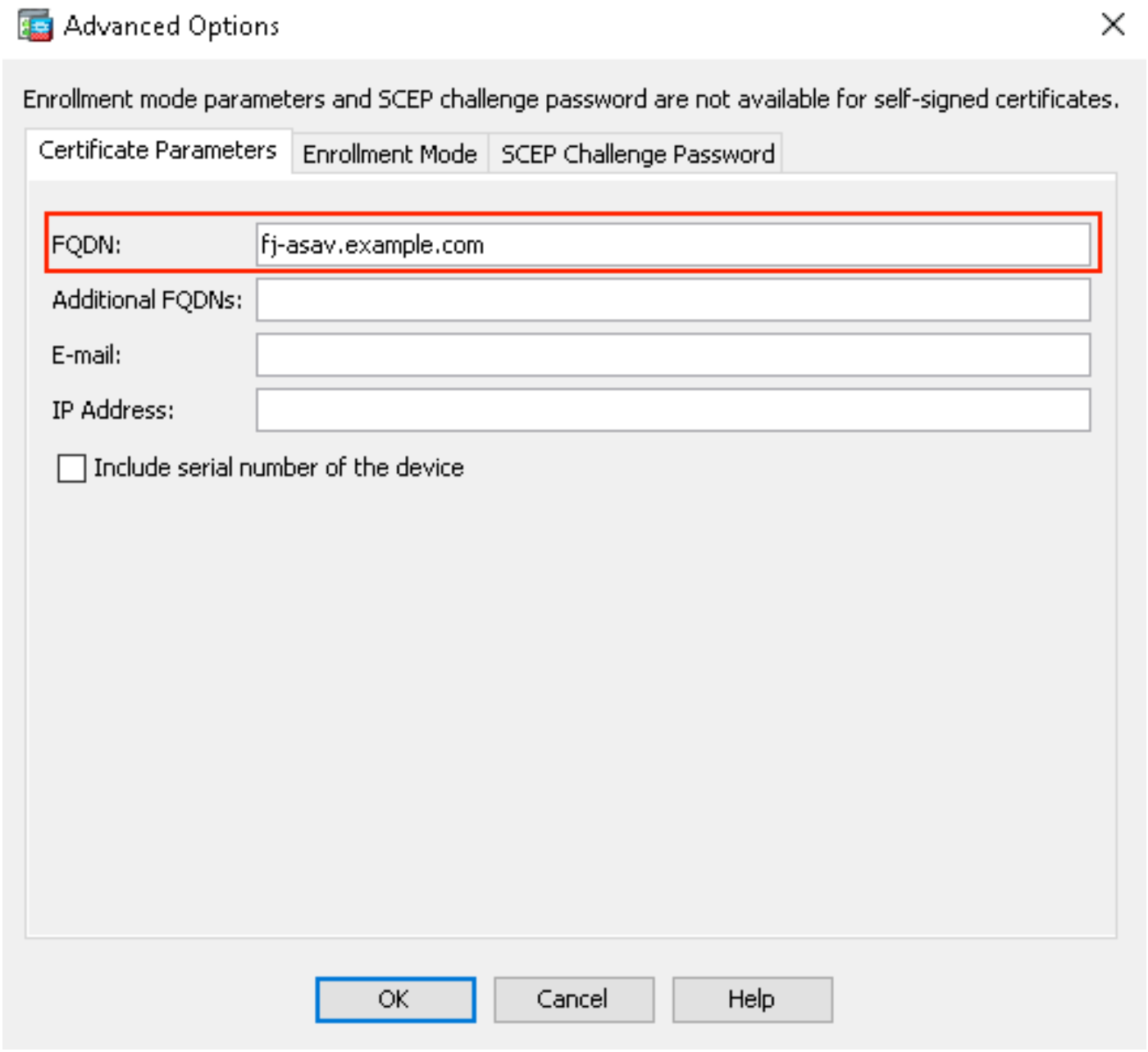
- Navigieren Sie zu Configuration > Remote Access VPN > Certificate Management > Identity Certificates.
- Klicken Sie auf die Schaltfläche Hinzufügen, und wählen Sie Neues Identitätszertifikat hinzufügen aus.



ASDM-Identitätszertifikat für die ACME-Registrierung.

2. Geben Sie den FQDN für das Identitätszertifikat an.

- Klicken Sie auf die Schaltfläche Erweitert.
- Geben Sie auf der Registerkarte Zertifikatparameter den FQDN an, über den das Zertifikat verfügen muss.

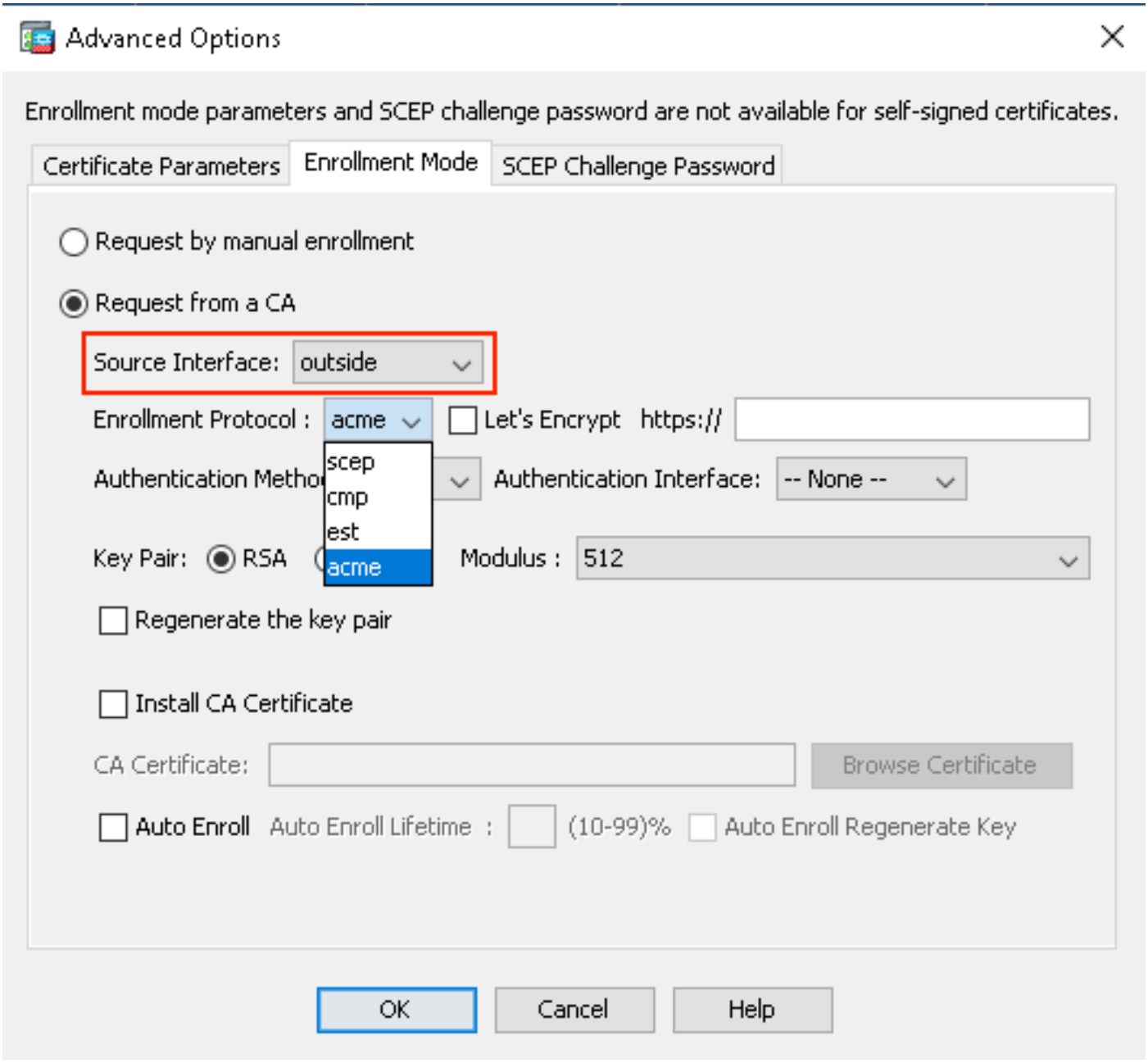


ASDM-FQDN für die ACME-Registrierung.

3. Wählen Sie ACME als Registrierungsprotokoll aus.

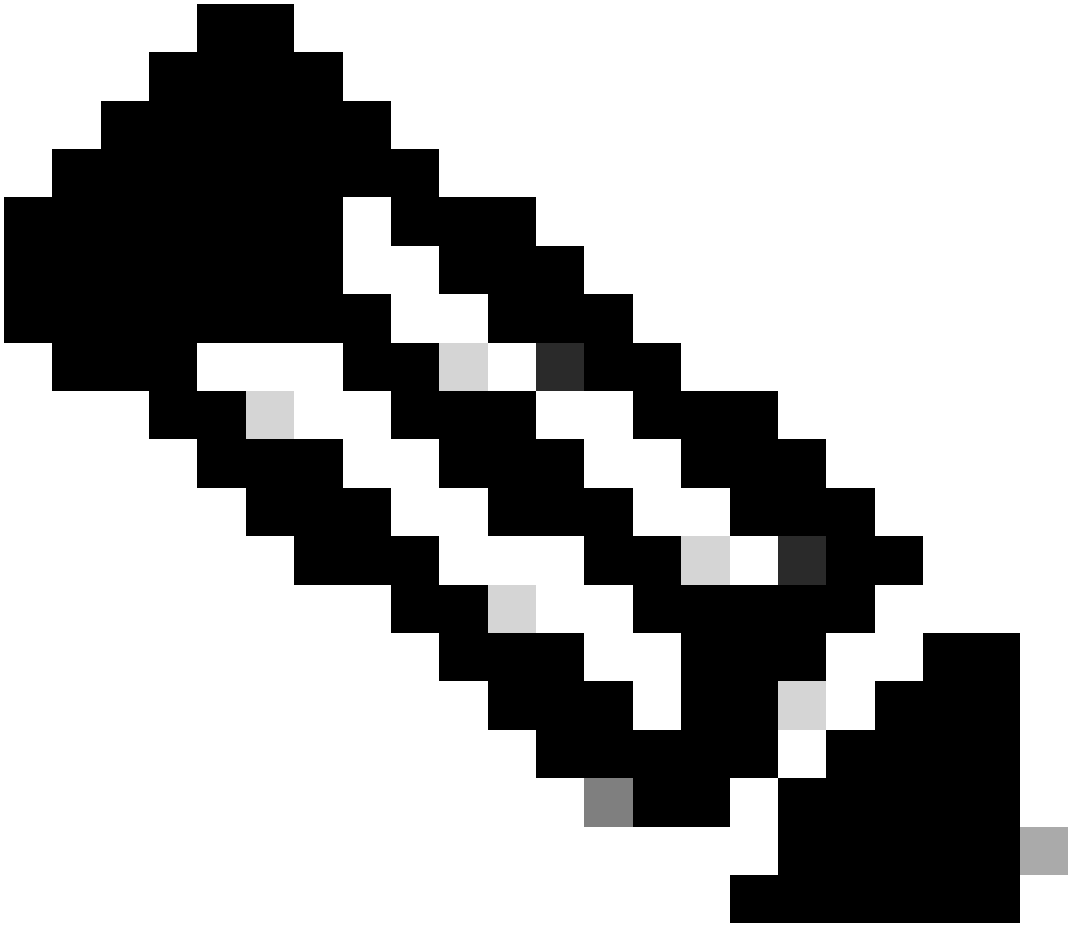
- Wählen Sie auf der Registerkarte Registrierungsmodus die Option Von CA anfordern aus.

- Geben Sie die Quellschnittstelle an, und wählen Sie acme als Registrierungsprotokoll aus.

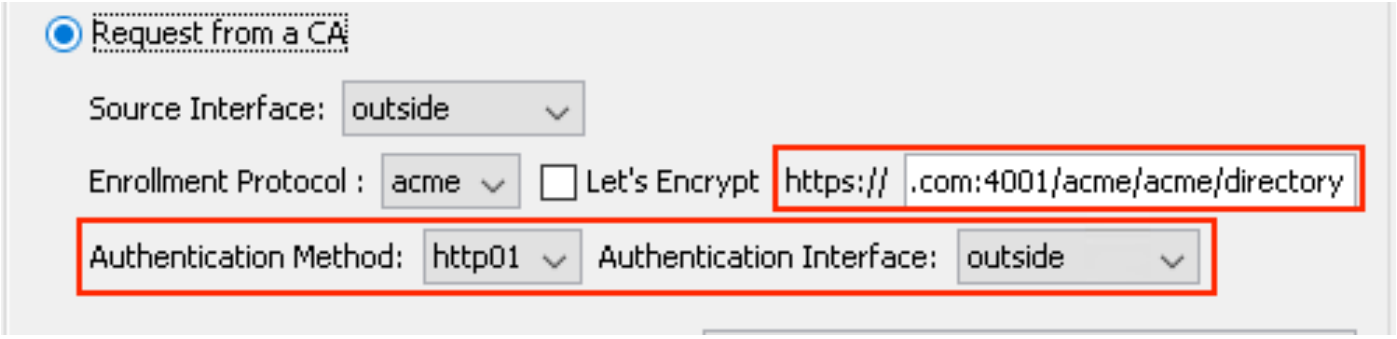


ACME Enrollment ASDM ACME-Protokoll. Selektion

4. Wählen Sie Let's Encrypt (Verschlüsseln) aus, damit Ihr Zertifikat von Let's Encrypt public CA signiert wird. Geben Sie andernfalls die URL der internen Zertifizierungsstelle an, die das ACME-Registrierungsprotokoll unterstützt. Geben Sie außerdem die Authentifizierungsschnittstelle an.



Anmerkung: Wenn das Kontrollkästchen Verschlüsseln aktiviert ist, wird die Server-URL automatisch eingetragen.



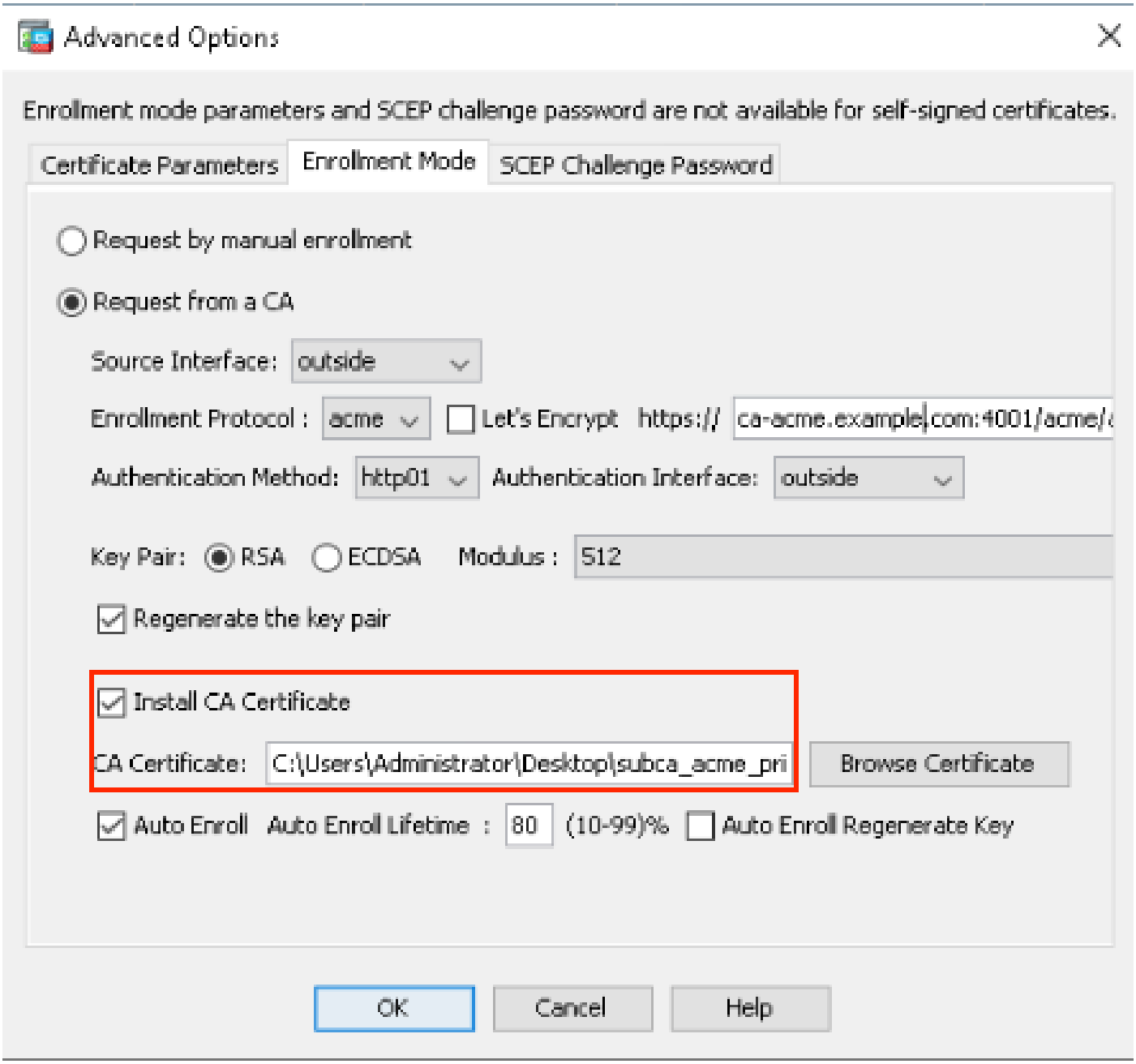
ASDM-Authentifizierungsmethode für die ACME-Registrierung.

5. CA-Zertifikat installieren

Wenn die Option Zertifizierungsstellenzertifikat installieren aktiviert ist, müssen Sie das Zertifikat der direkten Zertifizierungsstelle hochladen, die Ihr Zertifikat ausstellt.

Anmerkung: Wenn das Zertifizierungsstellenzertifikat bereits auf der sicheren Firewall vorhanden ist (entweder bei einer früheren Installation oder im Vertrauenspool), muss diese Option nicht aktiviert werden. Lassen Sie das Kontrollkästchen CA-Zertifikat installieren deaktiviert.

Anmerkung: Wenn Sie die Option Let's Encrypt (Verschlüsseln zulassen) auswählen, lassen Sie das Kontrollkästchen Install CA Certificate (Zertifizierungsstellenzertifikat installieren) deaktiviert, da die Stammzertifizierungsstellen für Let's Encrypt bereits im Vertrauenspool der sicheren Firewall enthalten sind.

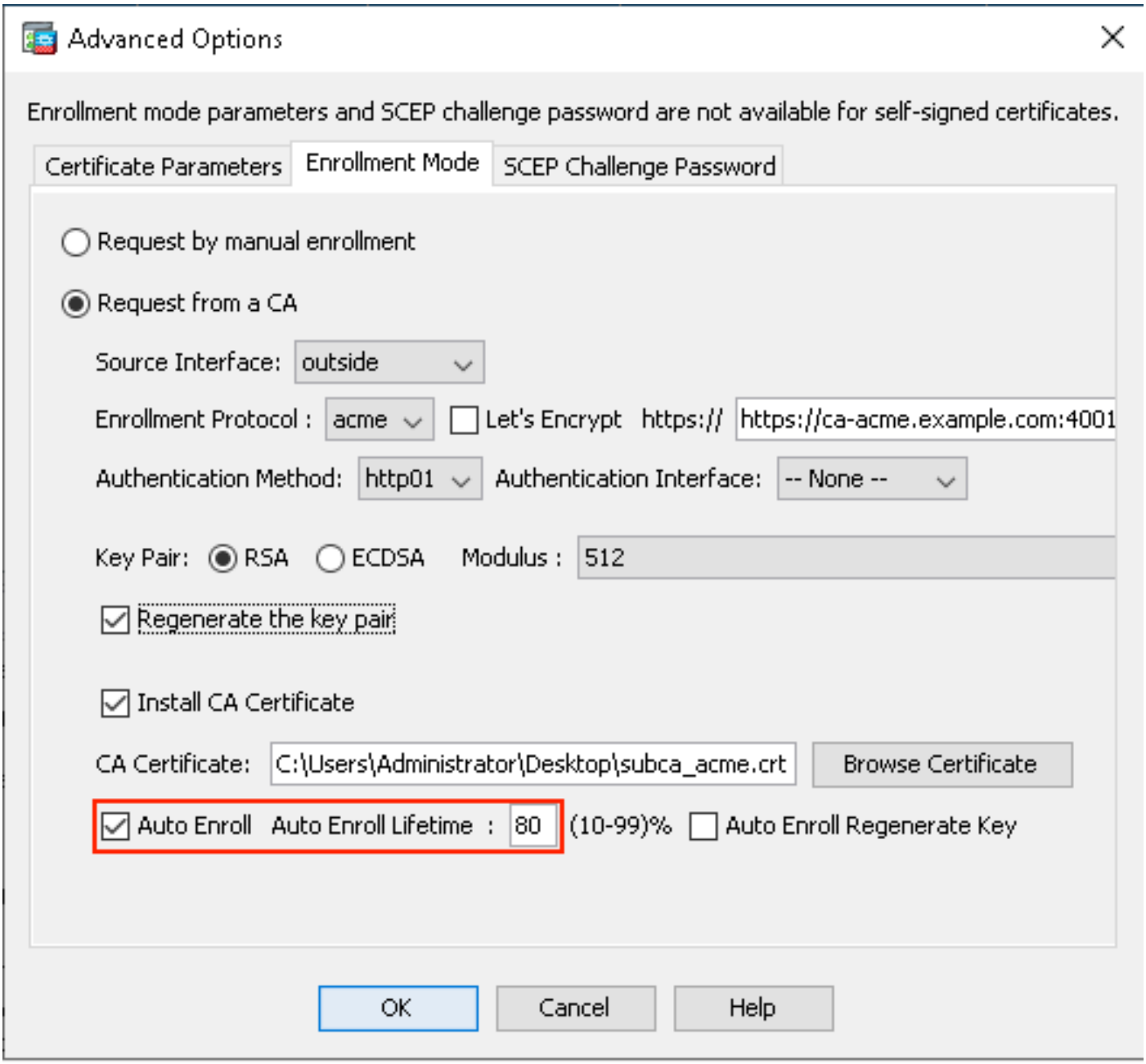


Installation der ACME-Registrierung für die ASDM-CA.

6. (Optional) Aktivieren Sie die automatische Registrierung für das Identitätszertifikat.

Aktivieren Sie das Kontrollkästchen Automatische Anmeldung, und geben Sie den Prozentsatz für die Lebensdauer der automatischen Anmeldung an.

Mit dieser Funktion wird sichergestellt, dass das Zertifikat vor Ablauf automatisch erneuert wird. Der Prozentsatz bestimmt, wie weit der Verlängerungsprozess vor Ablauf des Zertifikats beginnt. Wenn Sie beispielsweise einen Wert von 80 % festlegen, beginnt der Verlängerungsprozess, wenn das Zertifikat 80 % seiner Gültigkeitsdauer erreicht hat.



ACME-Registrierung ASDM Automatische Anmeldung.

7. Klicken Sie auf OK und speichern Sie die Konfiguration.

ACME-Registrierung mit Secure Firewall ASA CLI

1. Erstellen Sie einen neuen Vertrauenspunkt.

Erstellen Sie einen Vertrauenspunkt, und geben Sie acme als Registrierungsprotokoll an.

<#root>

```
asav(config)# crypto ca trustpoint private_acme
asav(config-ca-trustpoint)# enrollment protocol ?
```

```
crypto-ca-trustpoint mode commands/options:

acme Automatic Certificate Management Environment

  cmp Certificate Management Protocol Version 2
  est Enrollment over Secure Transport
  scep Simple Certificate Enrollment Protocol
```

2. Wählen Sie die HTTP-01-Authentifizierungsmethode aus, um die Domänenkontrolle zu überprüfen.

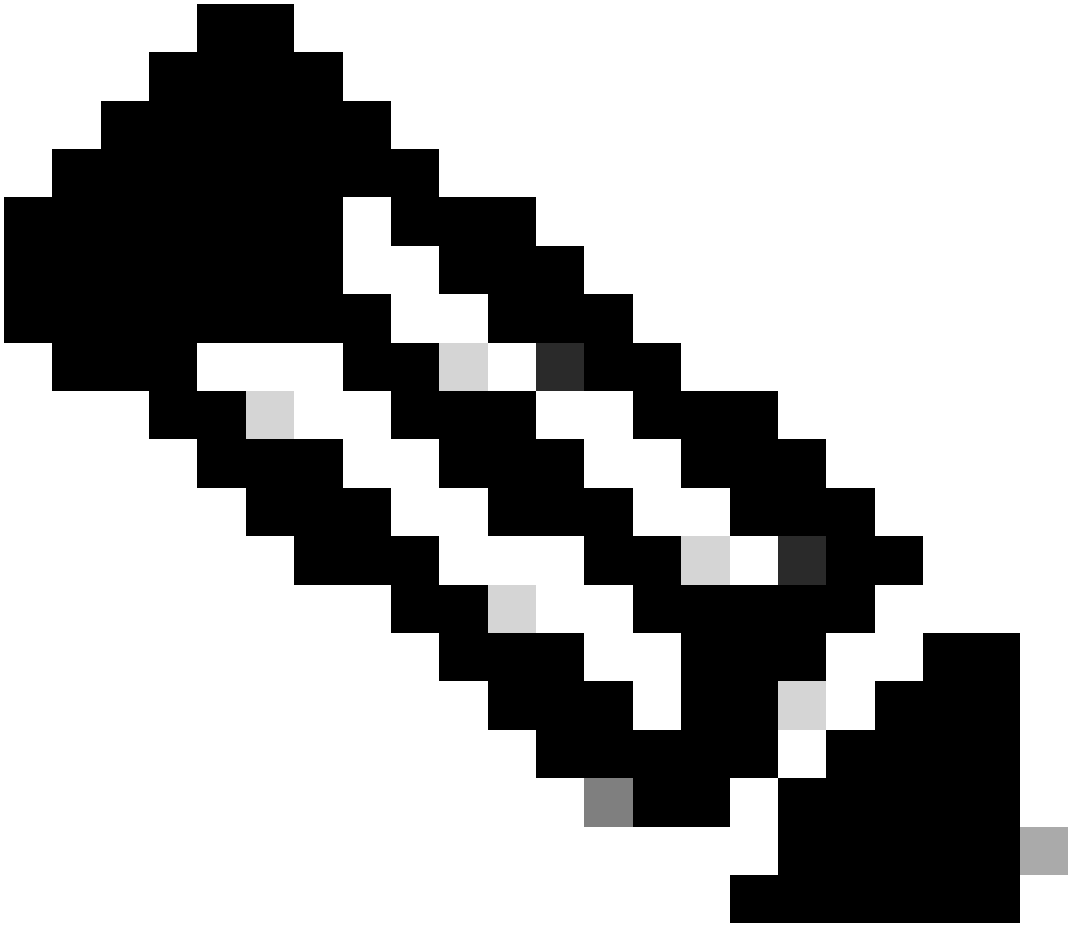
```
asav(config-ca-trustpoint)# enrollment protocol acme authentication ?

crypto-ca-trustpoint mode commands/options:
http01 Use the HTTP-01 method, which opens port 80 on the specified
interface
```

3. Wählen Sie Als ACME-CA verschlüsseln. Wenn Sie eine andere Zertifizierungsstelle verwenden, die das ACME-Protokoll unterstützt, geben Sie die entsprechende URL an.

```
asav(config-ca-trustpoint)# enrollment protocol acme url ?

crypto-ca-trustpoint mode commands/options:
LINE < 477 char URL
LetsEncrypt Use the Let's Encrypt CA
```



Anmerkung: Wenn das Schlüsselwort LetsEncrypt konfiguriert ist, wird die URL des Servers Let's Encrypt automatisch eingetragen.

4. Definieren Sie die RSA-Tastatur, den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) und den Antragstellernamen für das Zertifikat.

```
crypto ca trustpoint private_acme
 enrollment interface outside
 enrollment protocol acme authentication http01 outside
 enrollment protocol acme url https://ca-acme.example.com:4001/acme/acme/directory
 fqdn fj-asav.cisco.com
 subject-name CN=fj-asav.example.com
 keypair rsa modulus 4096
 auto-enroll 80 regenerate
 crl configure
```

5. Authentifizieren Sie den Vertrauenspunkt.

Anmerkung: Wenn die CA bereits auf der sicheren Firewall vorhanden ist oder Let's Encrypt verwendet wird, kann dieser Schritt übersprungen werden.

```
asav(config)# crypto ca authenticate private_acme
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----
MIIBwzCCAWqgAwIBAgIQedxaTDOJ1G6tLgAGti6tizAKBggqhkjOPQQDAjAsMRAw
DgYDVQQKEwdjYS1hY21lMRgwFgYDVQQDEw9jYS1hY21lIFJvb3QgQOEwHhcNMjQx
[truncated]
ADBEAiB7S4YZfnOK82K2yz5F5CzMe2t98LCpLRzoPJXMo7um1AIgH+K8EZMLstLN
AJQoplycJENo5D7kUmVrwUBBjREqv9I=
-----END CERTIFICATE-----
quit

INFO: Certificate has the following attributes:
Fingerprint: 40000000 40000000 40000000 40000000
Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.
```

6. Registrieren Sie das Zertifikat.

```
asav(config)# crypto ca enroll private_acme
% Start certificate enrollment ..
% The subject name in the certificate will be: CN=fj-asav.cisco.com

% The fully-qualified domain name in the certificate will be: fj-asav.example.com

% Include the device serial number in the subject name? [yes/no]: no

Request certificate from CA? [yes/no]: yes
```

Überprüfung

Installiertes Zertifikat in ASA anzeigen

Bestätigen Sie, dass das Zertifikat registriert ist, und überprüfen Sie das Verlängerungsdatum.

```
asav# show crypto ca certificates private_acme
```

```
CA Certificate
Status: Available
Certificate Serial Number: 79d000000000000000000008b
Certificate Usage: General Purpose
Public Key Type: ECDSA (256 bits)
Signature Algorithm: ecdsa-with-SHA256
Issuer Name:
CN=ca-acme Root CA
O=ca-acme
Subject Name:
CN=ca-acme Intermediate CA
O=ca-acme
Validity Date:
start date: 23:20:19 UTC Nov 26 2024
end date: 23:20:19 UTC Nov 24 2034
Storage: config
Associated Trustpoints: private_acme
Public Key Hashes:
SHA1 PublicKey hash: 8c8200000000000000000000000000000000000077
SHA1 PublicKeyInfo hash: 974c0000000000000000000000000000000009e1

Certificate
Status: Available
Certificate Serial Number: 666000000000000000000000000000be
Certificate Usage: General Purpose
Public Key Type: RSA (4096 bits)
Signature Algorithm: ecdsa-with-SHA256
Issuer Name:
CN=ca-acme Intermediate CA
O=ca-acme
Subject Name:
CN=fj-asav.example.com
Validity Date:
start date: 20:51:00 UTC Feb 14 2025
end date: 20:52:00 UTC Feb 15 2025
renew date: 16:03:48 UTC Feb 15 2025
Storage: immediate
Associated Trustpoints: private_acme
Public Key Hashes:
SHA1 PublicKey hash: e6e000000000000000000000000000000089a
SHA1 PublicKeyInfo hash: 5e300000000000000000000000000000009f
```

Syslog-Ereignisse

Die sichere Firewall enthält neue Syslogs zum Erfassen von Ereignissen im Zusammenhang mit der Zertifikatregistrierung mithilfe des ACME-Protokolls:

- 717067: Enthält Informationen zum Zeitpunkt des Beginns der ACME-Zertifikatregistrierung.

```
%ASA-5-717067: Starting ACME certificate enrollment for the trustpoint <private_acme> with CA <ca-acme.
```

- 717068: Informationen zum erfolgreichen Abschluss der ACME-Zertifikatregistrierung

```
%ASA-5-717068: ACME Certificate enrollment succeeded for trustpoint <private_acme> with CA <ca-acme.exa
```

- 717069: Informationen zum Fehlschlagen der ACME-Registrierung

```
%ASA-3-717069: ACME Certificate enrollment failed for trustpoint <private_acme>
```

- 717070: Stellt Informationen zur Verfügung, die sich auf das Tastenpaar für die Zertifikatregistrierung oder die Zertifikatverlängerung beziehen.

```
%ASA-5-717070: Keypair <Auto.private_acme> in the trustpoint <private_acme> is regenerated for <manual>
```

Fehlerbehebung

Wenn die Registrierung eines ACME-Zertifikats fehlschlägt, überlegen Sie sich die nächsten Schritte zur Identifizierung und Behebung des Problems:

- Überprüfen Sie die Verbindung zum Server: Bestätigen Sie, dass die sichere Firewall über eine Netzwerkverbindung zum ACME-Server verfügt. Stellen Sie sicher, dass keine Netzwerkprobleme auftreten oder die Kommunikation durch Firewall-Regeln blockiert wird.
- Stellen Sie sicher, dass der Domänenname der sicheren Firewall auflösbar ist: Stellen Sie sicher, dass der auf der sicheren Firewall konfigurierte Domänenname vom ACME-Server aufgelöst werden kann. Diese Verifizierung ist für den Server zur Validierung der Anfrage von entscheidender Bedeutung.
- Domäneninhaber bestätigen: Stellen Sie sicher, dass alle im Vertrauenspunkt angegebenen Domänennamen der sicheren Firewall gehören. Dadurch wird sichergestellt, dass der ACME-Server das Domäneneigentum überprüfen kann.

Befehle zur Fehlerbehebung

Sammeln Sie für weitere Informationen die Ausgabe der nächsten Debugbefehle:

- debug crypto ca acme <1-255>
- debug crypto ca <1-14>

Häufige ACME-Registrierungsfehler:

Fehlercode	Grund	Mögliche Ursache oder Beseitigung
7	Verbindung zum Server kann nicht hergestellt werden	Der Server ist erreichbar, aber der ACME-Dienst wird nicht ausgeführt.
28	Verbindung zum Server kann nicht hergestellt werden	Der Server ist nicht erreichbar. Prüfen Sie den grundlegenden Netzwerkzugriff auf den ACME-Server.
60	Serverzertifikat kann nicht überprüft werden	Stellen Sie sicher, dass die Stamm- oder Ausstellerzertifizierung in einem Vertrauenspunkt oder im Vertrauenspool vorhanden ist.
124	Zeitüberschreitung bei ACME-Verarbeitung	Stellen Sie sicher, dass alle angeforderten FQDNs in die für die HTTP-01-Authentifizierung konfigurierte Schnittstelle aufgelöst werden. Vergewissern Sie sich, dass die konfigurierte ACME-URL richtig ist.

Zugehörige Informationen

Weitere Unterstützung erhalten Sie beim TAC. Ein gültiger Supportvertrag ist erforderlich: [Weltweiter Kontakt zum Cisco Support.]
Sie können hier auch die Cisco VPN Community besuchen.

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.