Configurazione della registrazione dei certificati con il protocollo ACME su Secure Firewall

Sommario

Introduzione

In questo documento viene descritto il processo di registrazione di un certificato TLS (Transport Layer Security) tramite il protocollo ACME (Automated Certificate Management Environment) su ASA Secure Firewall.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

- Cisco ASAv versione 9.23.1.
- Cisco ASDM versione 7.23(1).
- Server CA (Certification Authority) che supporta il protocollo ACME.

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.

Requisiti e limitazioni

Gli attuali requisiti e limitazioni per la registrazione ACME su Secure Firewall ASA sono:

- Supportato su ASA versione 9.23.1 e ASDM 7.23.1 e successive
- Non supportato in più contesti
- ACME non supporta la creazione di certificati jolly. Ogni richiesta di certificato deve specificare un nome di dominio esatto.
- Ogni trust point registrato tramite ACME è limitato a una singola interfaccia, il che significa che i certificati registrati con ACME non possono essere condivisi tra più interfacce.
- Le coppie di chiavi vengono generate automaticamente e non possono essere condivise per i certificati registrati tramite ACME. Ogni certificato utilizza una coppia di chiavi univoca, migliorando la protezione ma limitando il riutilizzo delle chiavi.

Considerazioni sul downgrade

Al momento del downgrade a una versione che non supporta la registrazione ACME su Secure Firewall ASA (9.22 e versioni precedenti):

- Tutte le configurazioni di trust point relative ad ACME nuove rispetto alla versione 9.23.x o successive vengono perse
- Tutti i certificati registrati tramite ACME rimangono accessibili, ma la chiave privata viene dissociata dopo il primo salvataggio e riavvio successivo al downgrade

Se è necessario un downgrade, eseguire la procedura di soluzione consigliata seguente:

1. Prima di effettuare il downgrade, accertarsi di esportare i certificati ACME in formato PKCS12.
2. Prima di effettuare il downgrade, accertarsi di rimuovere la configurazione del trust point ACME.
3. Dopo il downgrade, importare il certificato PKCS12. Il trust point risultante è ancora valido fino alla scadenza del certificato rilasciato tramite ACME.

Premesse

Il protocollo ACME è progettato per semplificare la gestione dei certificati TLS per gli amministratori di rete. Grazie all'utilizzo di ACME, gli amministratori possono automatizzare i processi necessari per ottenere e rinnovare i certificati TLS. Questa automazione è particolarmente utile quando si utilizzano autorità di certificazione (CA) come Let's Encrypt, che offrono certificati gratuiti, automatizzati e aperti utilizzando il protocollo ACME.

ACME supporta il rilascio di certificati DV (Domain Validation). Questi certificati sono un tipo di certificato digitale che conferma il controllo del detentore del certificato sui domini specificati. Il processo di convalida dei certificati DV viene in genere eseguito tramite un meccanismo di verifica basato su HTTP. In questo meccanismo, il richiedente inserisce un file specifico sul proprio server Web, che l'Autorità di certificazione (CA) verifica accedendo al file tramite il server HTTP del dominio. Il completamento di questa verifica dimostra alla CA che il richiedente ha il controllo sul dominio, consentendo il rilascio del certificato DV.

Per completare l'iscrizione, procedere come segue:

1. Avvia richiesta certificato: Il client richiede un certificato dal server ACME e specifica il dominio o i domini per i quali il certificato è richiesto.
2. Receive HTTP-01 Challenge: Il server ACME fornisce una richiesta HTTP-01 con un token univoco che il client può utilizzare per dimostrare il controllo del dominio.
3. Preparazione risposta di verifica:
    - Il client crea un'autorizzazione della chiave combinando il token del server ACME con la relativa chiave account.
    - Il client configura il proprio server Web per gestire questa autorizzazione chiave in un percorso URL specifico.
4. Il server ACME recupera la sfida: Il server ACME invia una richiesta HTTP GET all'URL specificato per recuperare l'autorizzazione della chiave.
5. Il server ACME verifica la proprietà: Il server verifica se l'autorizzazione della chiave recuperata corrisponde al valore previsto per confermare il controllo del client sul dominio.
6. Rilascia certificato: Dopo la convalida, il server ACME rilascia il certificato SSL/TLS al client.

Flusso di autenticazione HTTP-01 della registrazione ACME.

I vantaggi più rilevanti dell'utilizzo del protocollo ACME per la registrazione dei certificati TLS sono:

- ACME semplifica l'acquisizione e la manutenzione dei certificati di dominio TLS per le interfacce ASA TLS Secure Firewall. Questa automazione consente di ridurre in modo significativo le attività manuali e di mantenere aggiornati i certificati senza controllo costante.
- Con i trust point abilitati ACME, i certificati vengono rinnovati automaticamente in prossimità della scadenza. Questa funzionalità riduce la necessità di intervento amministrativo, garantendo una protezione ininterrotta e impedendo la scadenza imprevista dei certificati.

Configurazione

Configurazione prerequisiti

Prima di avviare il processo di registrazione ACME, verificare che siano soddisfatte le seguenti condizioni:

1. Nome dominio risolvibile: Il nome di dominio per il quale si richiede un certificato deve essere risolvibile dal server ACME. In questo modo il server può verificare la proprietà del dominio.
2. Accesso sicuro del firewall al server ACME: Il firewall protetto deve essere in grado di accedere al server ACME tramite una delle relative interfacce. Non è necessario che l'accesso venga eseguito tramite l'interfaccia per cui è richiesto il certificato.
3. Disponibilità porta TCP 80: Consentire alla porta TCP 80 dal server ACME CA di accedere all'interfaccia corrispondente al nome di dominio. Questa operazione è necessaria durante il

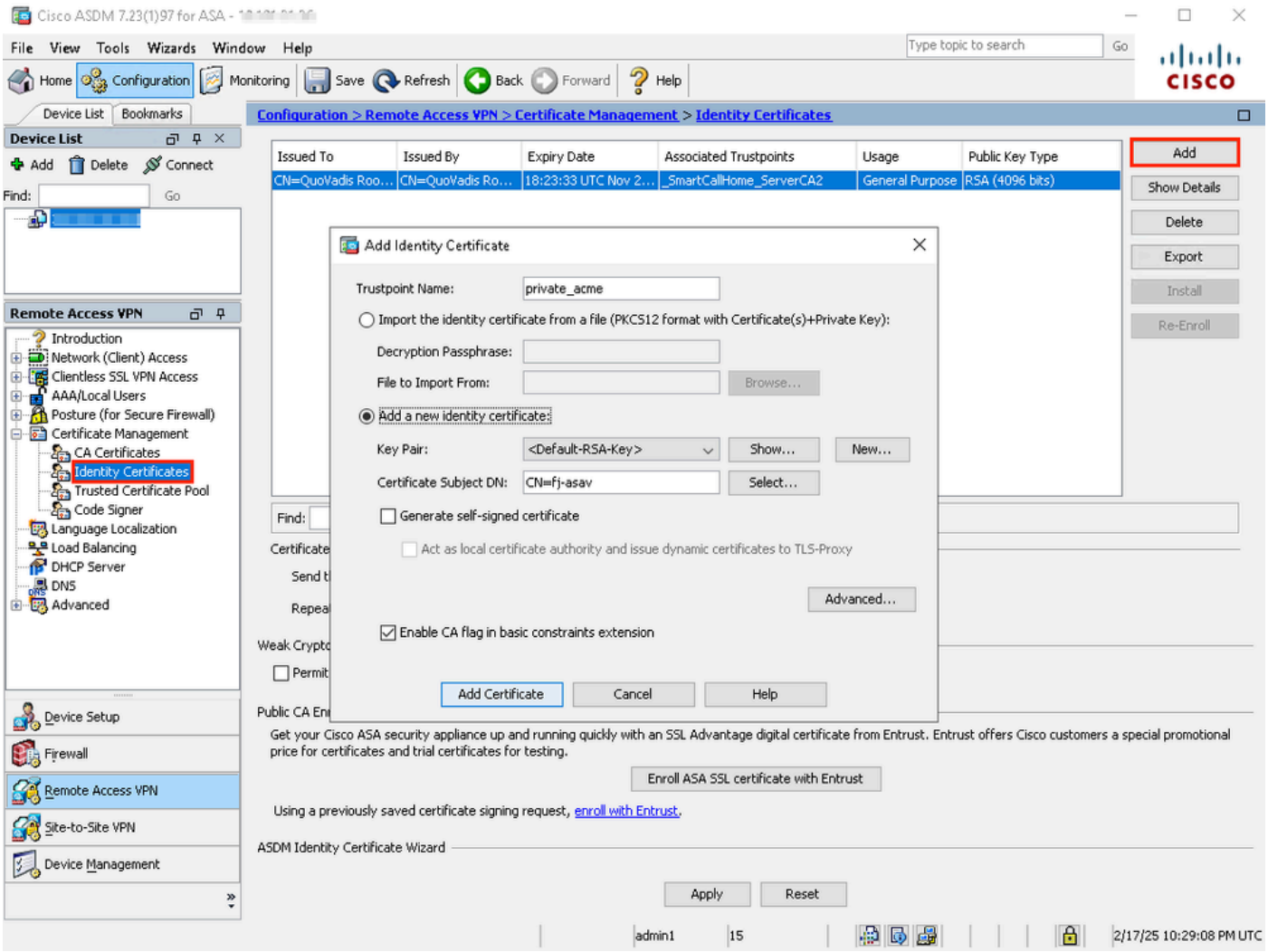
processo di scambio ACME per completare la richiesta HTTP-01.

Nota: Durante il periodo in cui la porta 80 è aperta, sono accessibili solo i dati di richiesta ACME.

Iscrizione ACME con ASDM

1. Aggiungere un nuovo certificato di identità.

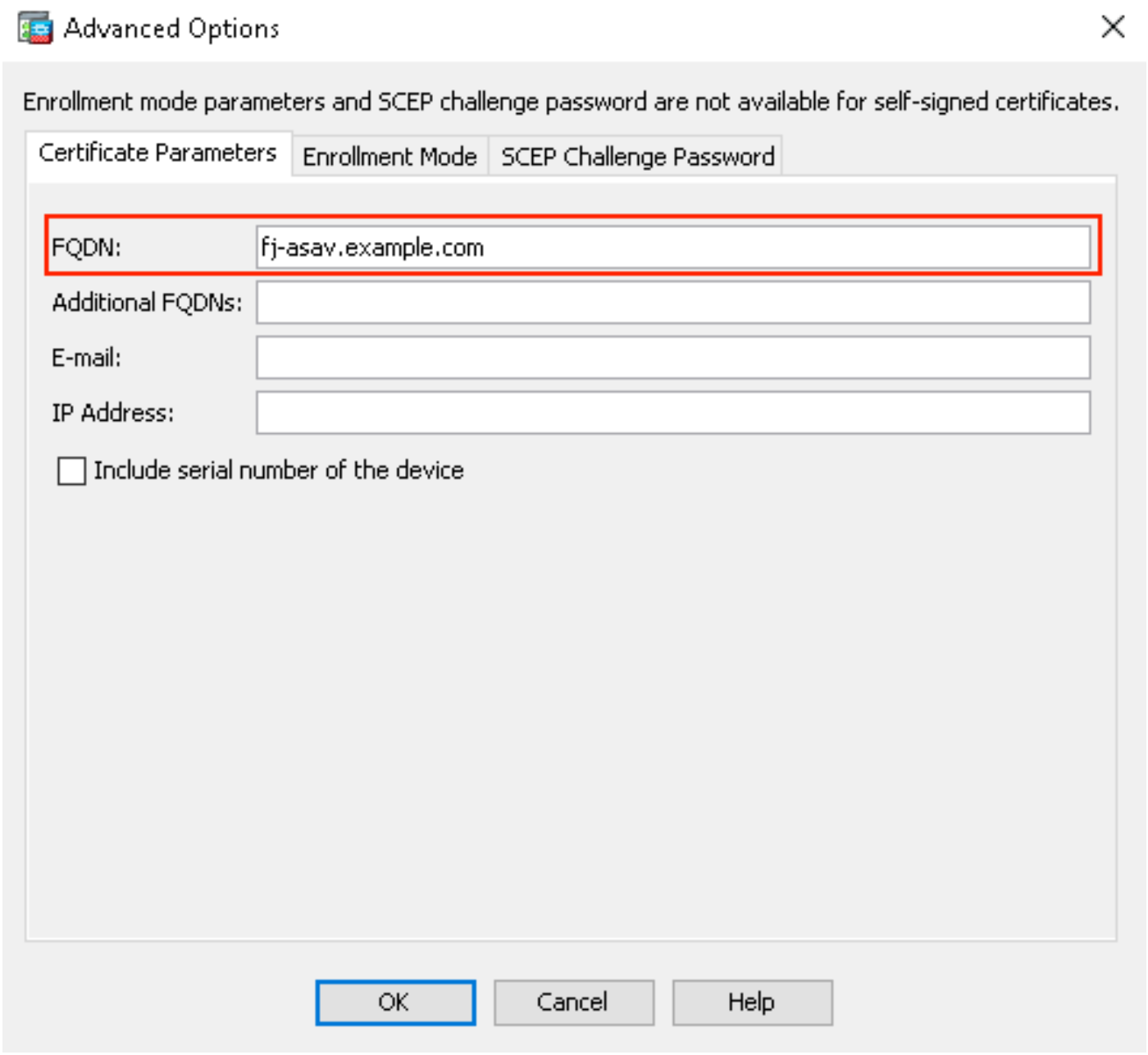
- Passare a Configurazione > VPN ad accesso remoto > Gestione certificati > Certificati di identità.
- Fare clic sul pulsante Aggiungi e selezionare Aggiungi nuovo certificato di identità.



Certificato di identità ASDM di registrazione ACME.

2. Specificare il nome di dominio completo (FQDN) per il certificato di identità.

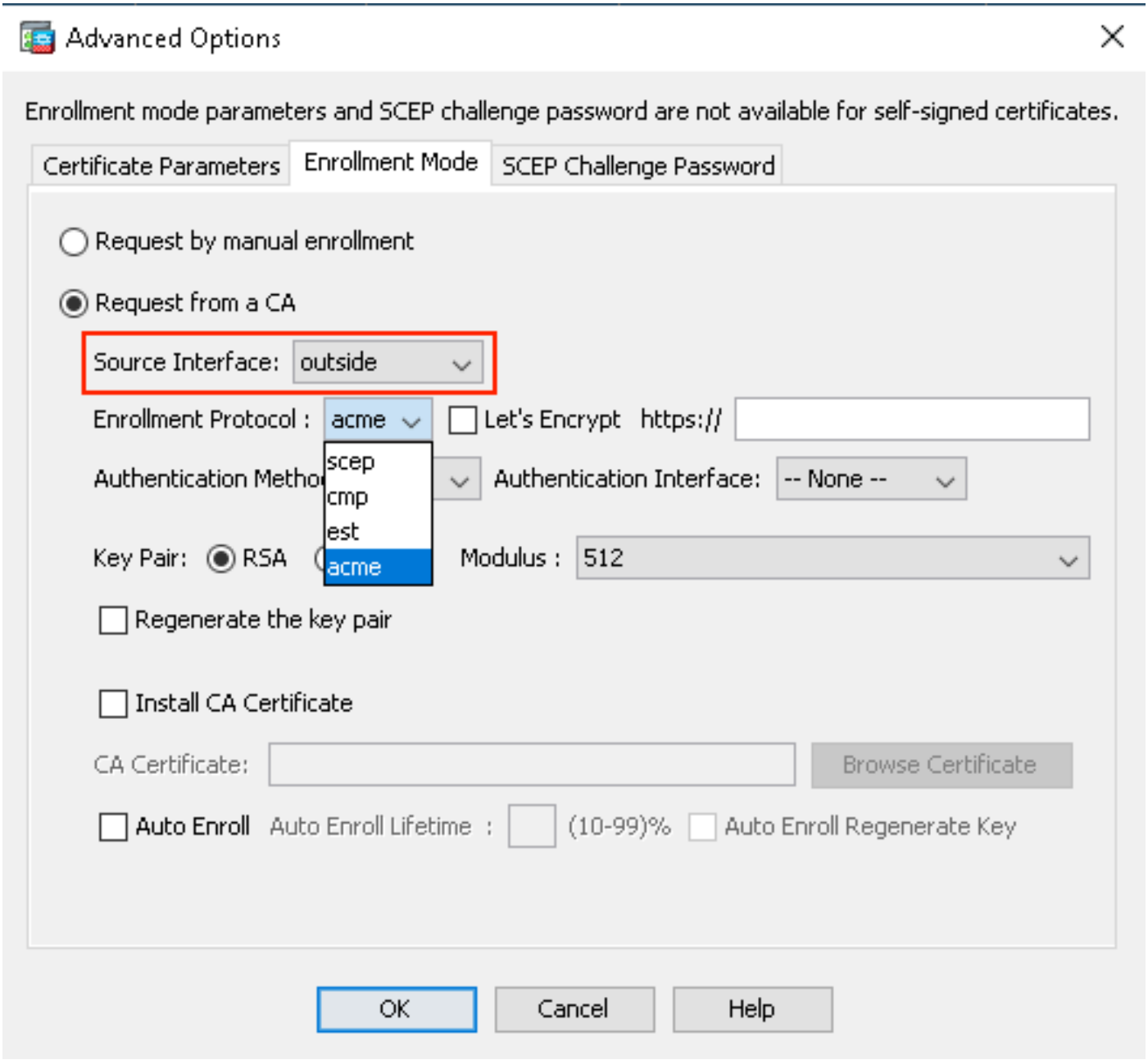
- Fare clic sul pulsante Avanzate.
- Nella scheda Parametri certificato, specificare il nome di dominio completo (FQDN) che deve avere il certificato.



FQDN di ASDM per l'iscrizione ACME.

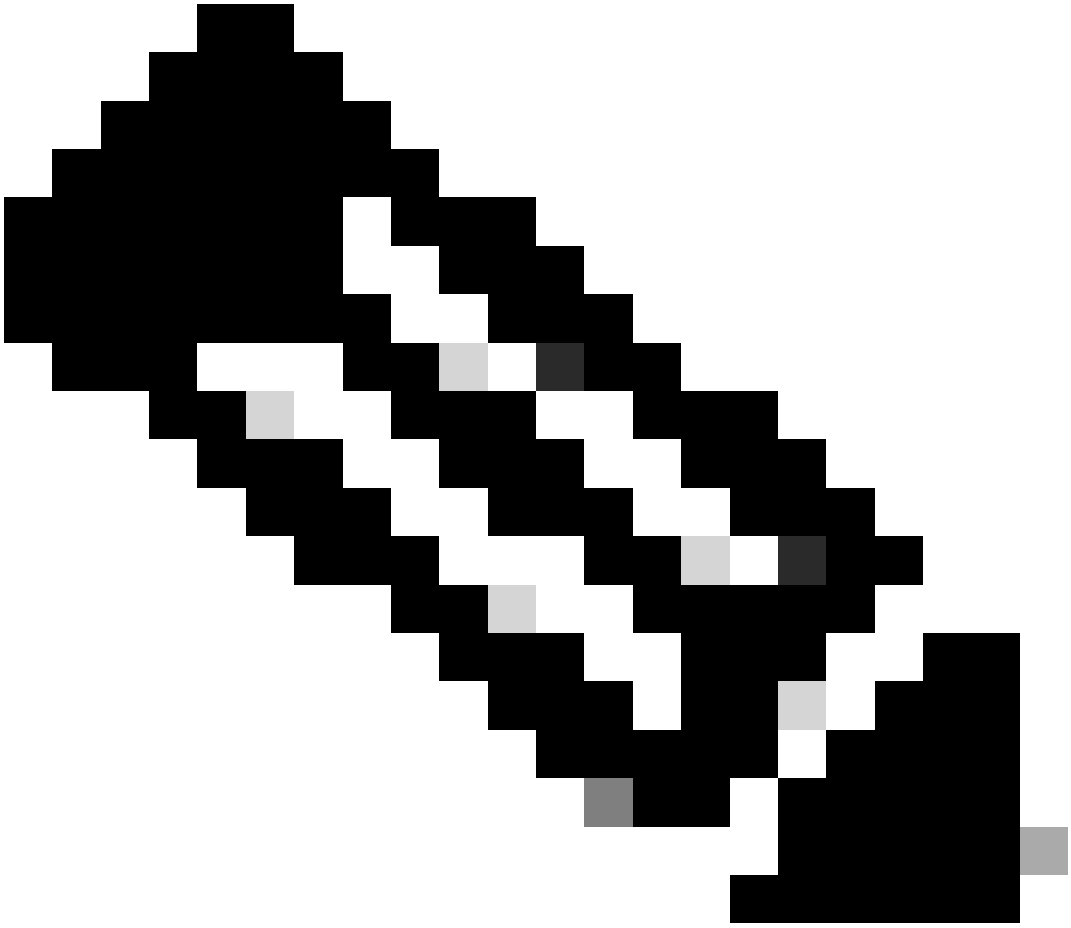
3. Selezionare ACME come protocollo di iscrizione.

- Nella scheda Modalità di registrazione selezionare l'opzione Richiesta da CA.
- Specificare l'interfaccia di origine e selezionare acme come protocollo di registrazione.

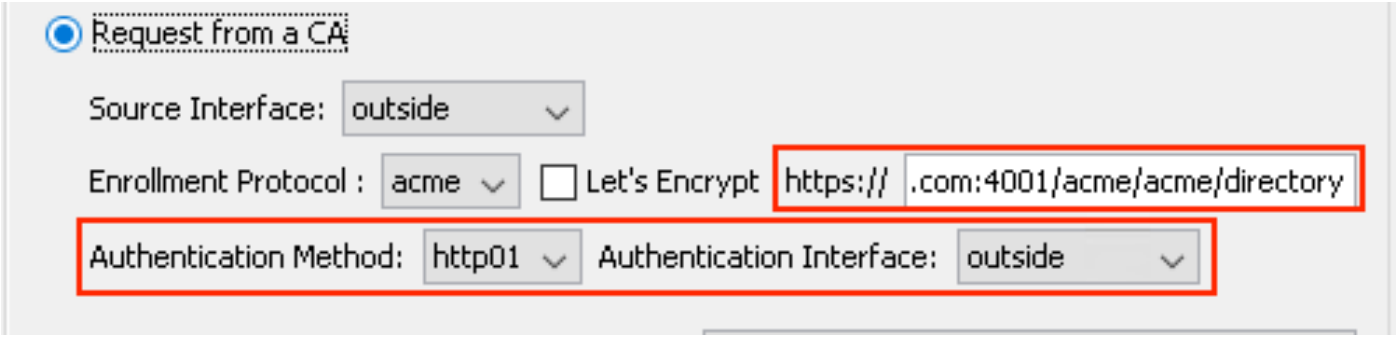


Protocollo acme ASDM di registrazione ACME. selezione

4. Selezionare Crittografa per il certificato che deve essere firmato da Crittografa CA pubblica. In caso contrario, specificare l'URL della CA interna che supporta il protocollo di registrazione ACME. Specificare inoltre l'interfaccia di autenticazione.



Nota: Quando la casella di controllo Crittografia è selezionata, l'URL del server viene popolato automaticamente.



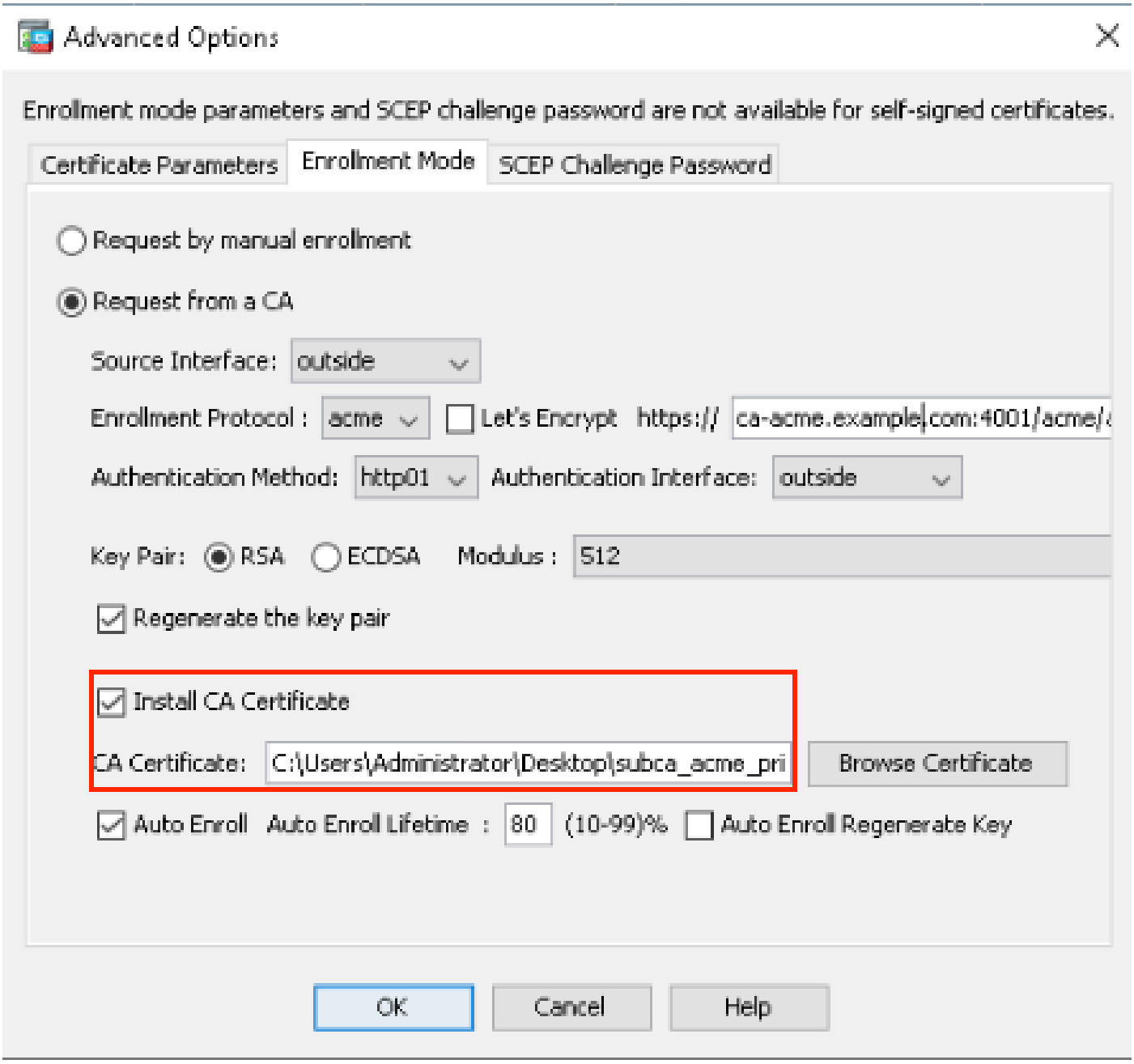
Metodo di autenticazione ASDM di registrazione ACME.

5. Installare il certificato CA.

Se l'opzione Installa certificato CA è selezionata, è necessario caricare il certificato della CA che rilascia immediatamente il certificato.

Nota: Se il certificato CA esiste già nel firewall protetto, da un'installazione precedente o all'interno del trust pool, non è necessario selezionare questa opzione. Lasciare deselezionata la casella di controllo Installa certificato CA.

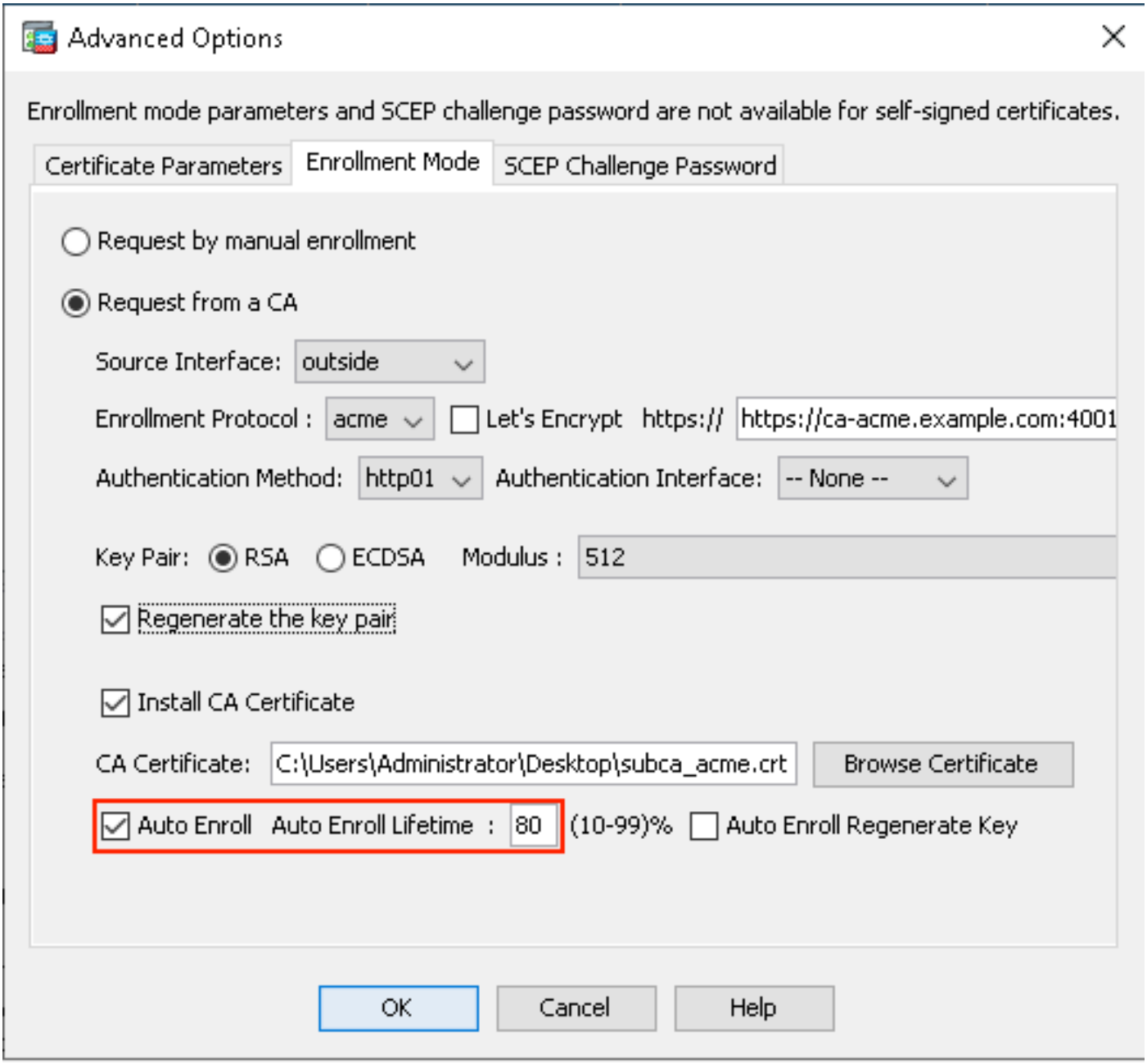
Nota: Quando si seleziona l'opzione Crittografia, lasciare deselezionata la casella di controllo Installa certificato CA, in quanto i certificati CA radice per Crittografia sono già inclusi nel pool di trust di Secure Firewall.



6. (Facoltativo) Abilitare la registrazione automatica per il certificato di identità.

Selezionare la casella di controllo Registrazione automatica e specificare la percentuale per la durata della registrazione automatica.

Questa funzionalità garantisce che il certificato venga rinnovato automaticamente prima della scadenza. La percentuale determina quanto tempo prima della scadenza del certificato inizia il processo di rinnovo. Se ad esempio è impostato su 80%, il processo di rinnovo inizia quando il certificato raggiunge l'80% del periodo di validità.



Iscrizione ACME Registrazione automatica ASDM.

7. Fare clic su OK e salvare la configurazione.

Registrazione ACME con Secure Firewall ASA CLI

1. Creare un nuovo trust point.

Creare un trust point e specificare acme come protocollo di registrazione.

<#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. Selezionare il metodo HTTP-01 per l'autenticazione per verificare il controllo del dominio.

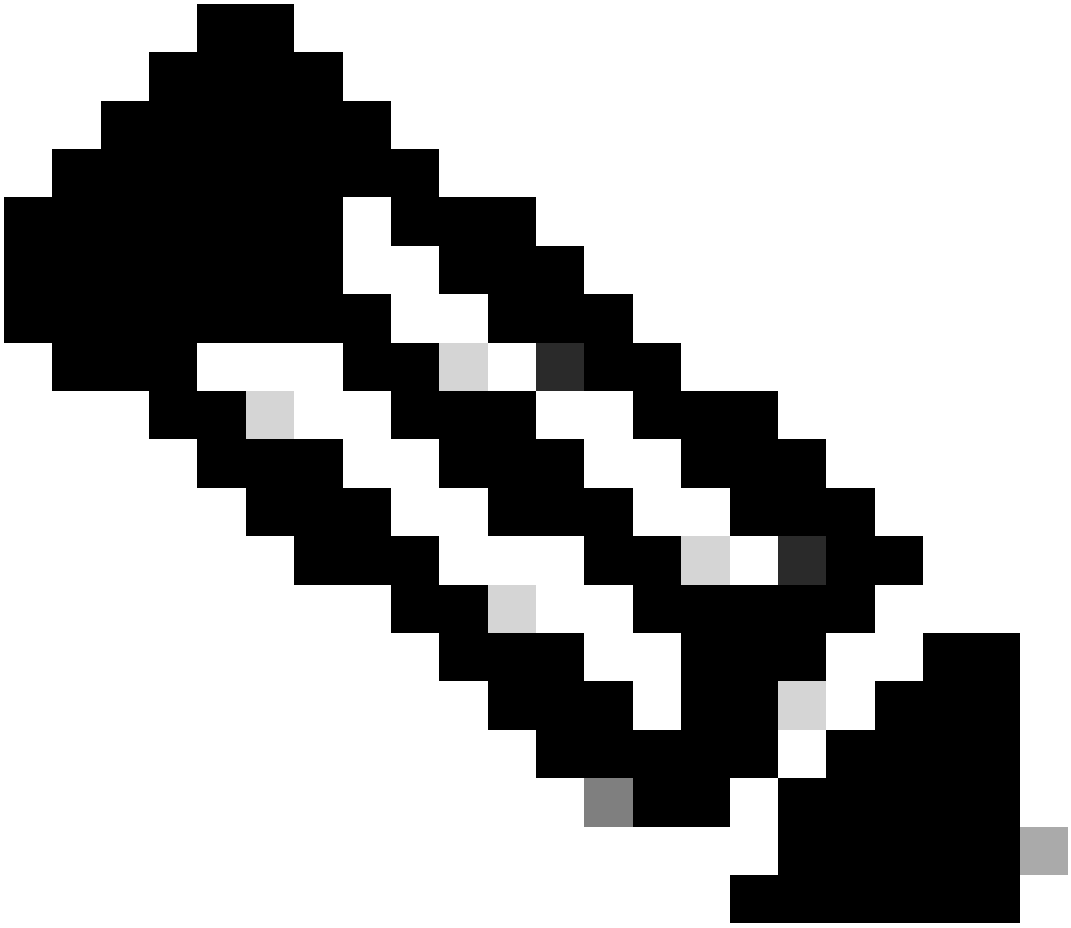
```
asav(config-ca-trustpoint)# enrollment protocol acme authentication ?

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

3. Selezionare Let's Encrypt come CA ACME. Se si utilizza un'altra CA che supporta il protocollo ACME, fornire l'URL appropriato.

```
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
```



Nota: Quando la parola chiave LetsEncrypt è configurata, l'URL del server Let's Encrypt viene popolato automaticamente.

4. Definire la coppia di chiavi RSA, il nome di dominio completo (FQDN) e il nome del soggetto per il certificato.

```
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. Autenticare il trust point.

Nota: Se la CA esiste già nel firewall protetto o quando si utilizza Crittografia, è possibile ignorare questo passaggio.

```
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. Registrare il certificato.

```
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
```

Verifica

Visualizza certificato installato in ASA

Confermare che il certificato è registrato e verificare la data di rinnovo.

```
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: e6e000000000000000000000000000000000089a
SHA1 PublicKeyInfo hash: 5e300000000000000000000000000000000009f
```

Eventi Syslog

Nel firewall protetto sono presenti nuovi syslog per acquisire gli eventi relativi alla registrazione dei certificati tramite il protocollo ACME:

- 717067: Fornisce informazioni sull'avvio della registrazione dei certificati ACME

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

- 717068: Fornisce informazioni sull'esito della registrazione del certificato ACME

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

- 717069: Fornisce informazioni su quando l'iscrizione ACME non riesce

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

- 717070: Fornisce informazioni relative alla coppia di chiavi per la registrazione o il rinnovo del certificato

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

Risoluzione dei problemi

Se la registrazione di un certificato ACME non riesce, considerare i passaggi successivi per identificare e risolvere il problema:

- Verificare la connettività al server: Verificare che il firewall protetto disponga della connettività di rete al server ACME. Verificare che non vi siano problemi di rete o che le regole del firewall blocchino la comunicazione.
- Verificare che il nome di dominio del firewall sicuro sia risolvibile: Verificare che il nome di dominio configurato sul firewall protetto sia risolvibile dal server ACME. Questa verifica è fondamentale per la convalida della richiesta da parte del server.
- Conferma proprietà dominio: Verificare che tutti i nomi di dominio specificati nel trust point appartengano al firewall protetto. In questo modo il server ACME può convalidare la proprietà del dominio.

Comandi per la risoluzione dei problemi

Per ulteriori informazioni, catturare l'output dei comandi di debug successivi:

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

Errori comuni di registrazione ACME:

Codice di errore	Motivo	Possibile causa o risoluzione
7	Impossibile connettersi al server	Il server è raggiungibile ma il servizio ACME non è in esecuzione.
28	Impossibile connettersi al server	Server non raggiungibile. Controllare l'accesso di base alla rete al server ACME.
60	Impossibile convalidare il certificato del server	Verificare che la CA radice o emittente sia presente in un trust point o nel trustpool.
124	Timeout elaborazione ACME	Verificare che tutti gli FQDN richiesti vengano risolti nell'interfaccia configurata per l'autenticazione HTTP-01. Verificare che l'URL ACME configurato sia corretto.

Informazioni correlate

Per ulteriore assistenza, contattare TAC. È necessario un contratto di supporto valido: Contatti del supporto Cisco internazionali.
Qui è possibile anche visitare la Cisco VPN Community.

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).