Installazione e rinnovo dei certificati su un'appliance ASA gestita da ASDM

Sommario

[Domande frequenti]

Introduzione

Questo documento descrive come richiedere, installare, considerare attendibili e rinnovare alcuni tipi di certificati su software Cisco ASA gestito con ASDM.

Prerequisiti

Requisiti

- Prima di iniziare, verificare che l'ora, la data e il fuso orario di Adaptive Security Appliance (ASA) siano corretti. Con l'autenticazione dei certificati, si consiglia di usare un server Network Time Protocol (NTP) per sincronizzare l'ora sull'appliance ASA. Consultare Informazioni correlate per riferimento.
- Per richiedere un certificato che utilizza la richiesta di firma del certificato (CSR), è necessario disporre dell'accesso a un'Autorità di certificazione (CA) interna o di terze parti attendibile. Esempi di fornitori di CA di terze parti includono, tra gli altri, Entrust, Geotrust, GoDaddy, Thawte e VeriSign.

Componenti usati

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

- ASAv 9.18.1
- Per la creazione di PKCS12, viene utilizzato OpenSSL.

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.

Premesse

I tipi di certificati a cui si riferisce il documento sono:

- certificati autofirmati
- certificati firmati da un'autorità di certificazione di terze parti o da una CA interna

SSL (Secure Sockets Layer), TLS (Transport Layer Security) e IKEv2 rfc7296 per i protocolli di autenticazione EAP richiedono che il server SSL/TLS/IKEv2 fornisca al client un certificato server per eseguire l'autenticazione del server. A tale scopo, è consigliabile utilizzare CA di terze parti attendibili per rilasciare certificati SSL all'appliance ASA.

Cisco sconsiglia di utilizzare un certificato autofirmato perché potrebbe essere impossibile

configurare inavvertitamente un browser per considerare attendibile un certificato rilasciato da un server non autorizzato. Vi è inoltre l'inconveniente per gli utenti di dover rispondere a un avviso di sicurezza quando si connette al gateway sicuro.

Richiedere e installare un nuovo certificato di identità con ASDM

È possibile richiedere un certificato a un'Autorità di certificazione (CA) e installarlo su un'appliance ASA in due modi:

- Utilizzare la richiesta di firma del certificato (CSR). Generare una coppia di chiavi, richiedere un certificato di identità a una CA con un CSR, installare il certificato di identità firmato ottenuto dalla CA.
- Utilizzare un file PKCS12 ottenuto da una CA o esportato da un dispositivo diverso. Il file PKCS12 contiene la coppia di chiavi, il certificato di identità e i certificati CA.

Richiedere e installare un nuovo certificato di identità con richiesta di firma del certificato (CSR)

Sul dispositivo viene creato un CSR che richiede un certificato di identità. Utilizzare una coppia di chiavi creata sul dispositivo.

Un CSR contiene:

- informazioni sulla richiesta di certificato - oggetto richiesto e altri attributi, chiave pubblica dalla coppia di chiavi,
- informazioni sull'algoritmo della firma,
- firma digitale delle informazioni della richiesta di certificato, firmata con la chiave privata dalla coppia di chiavi.

Il CSR viene passato all'Autorità di certificazione (CA), in modo che lo firmi, in un formato PKCS#10.

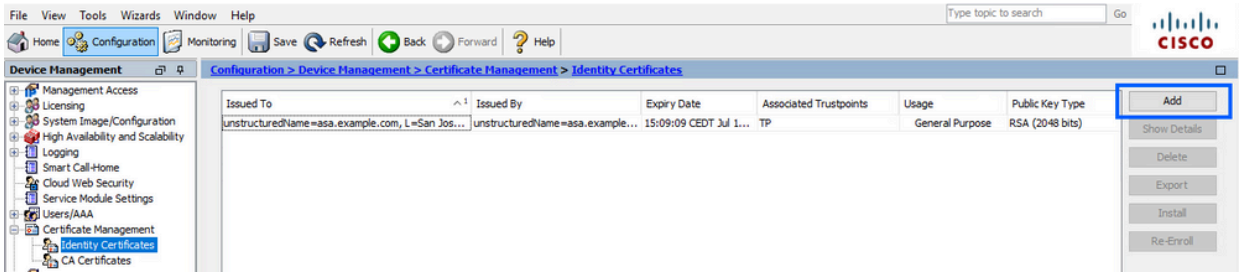
Il certificato firmato viene restituito dalla CA in un modulo PEM.

Nota: quando firma il CSR e crea un certificato di identità firmato, CA può modificare i parametri FQDN e Nome soggetto definiti nel Trustpoint.

Generare un CSR con ASDM

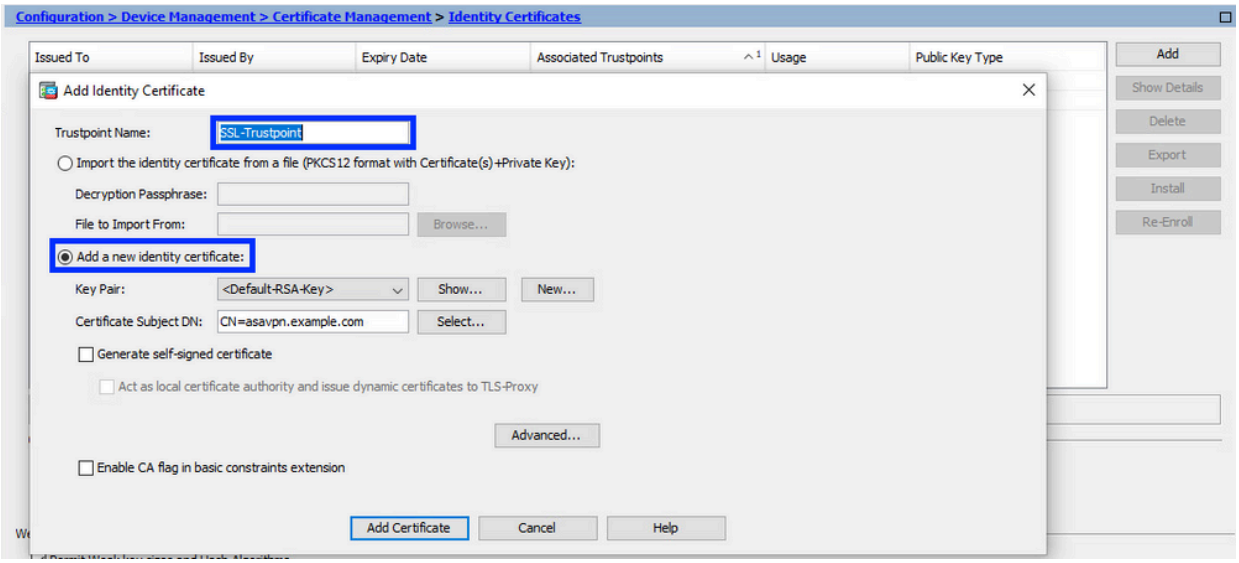
1. Creazione di un trust point con un nome specifico

    a. Passare a Configurazione > Gestione dispositivi > Gestione certificati > Certificati di identità.



b. Fare clic su Add.

c. Definire un nome di trust.



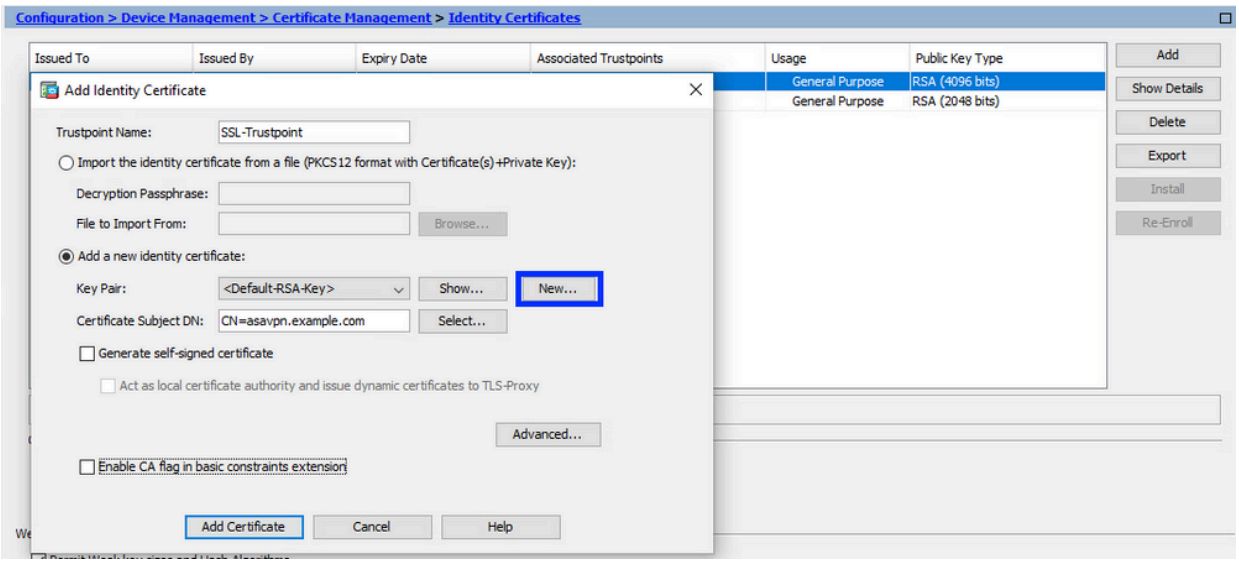
d. Fare clic sul pulsante di opzione Aggiungi nuovo certificato di identità.

2. (Facoltativo) Creare una nuova coppia di chiavi

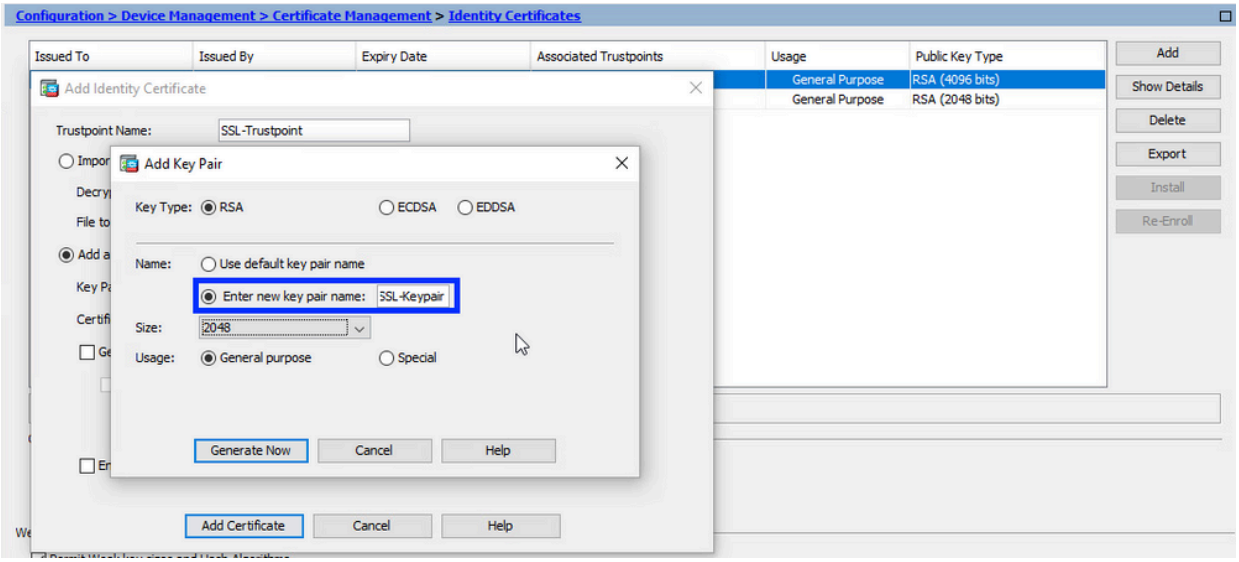
Nota: per impostazione predefinita, viene utilizzata la chiave RSA con il nome Default-RSA-Key e una dimensione di 2048; tuttavia, si consiglia di utilizzare una coppia di chiavi pubblica/privata univoca per ciascun certificato di identità.

---

a. Fare clic su Nuovo per generare una nuova coppia di chiavi.

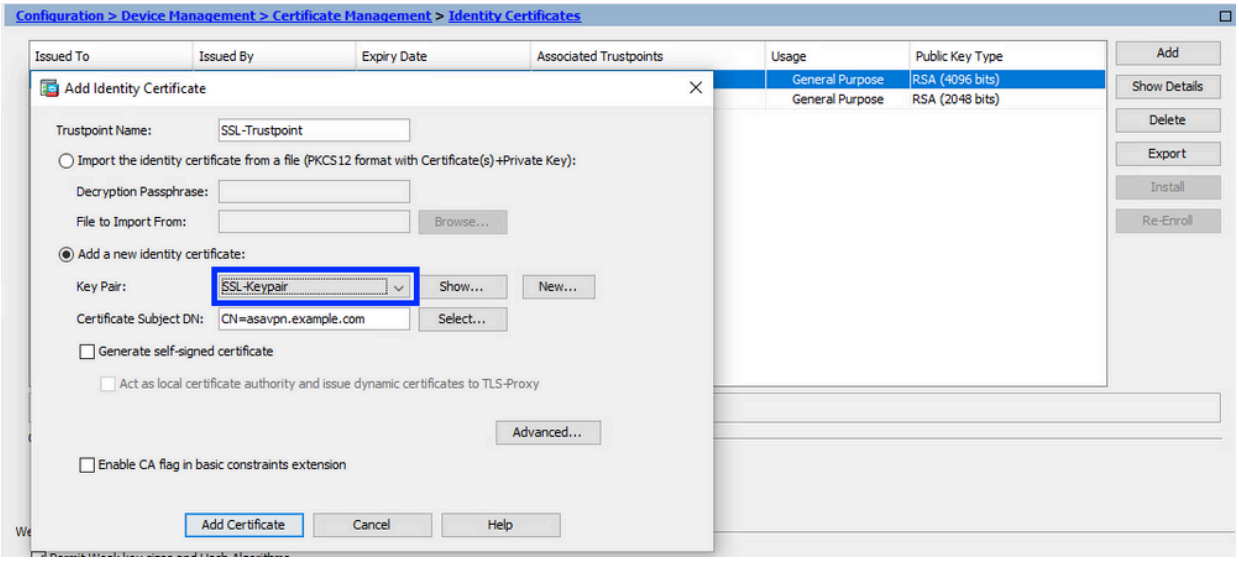


b. Scegliere l'opzione Immettere il nome della nuova coppia di chiavi e immettere un nome per la nuova coppia di chiavi.
c. Scegliere il tipo di chiave: RSA o ECDSA.
d. Scegliere le dimensioni della chiave; per RSA, scegliere Uso generico.
e. Fare clic su Genera ora. La coppia di chiavi è stata creata.



3. Scegliere il nome della coppia di chiavi

Scegliere la coppia di chiavi con cui firmare il CSR e da associare al nuovo certificato.

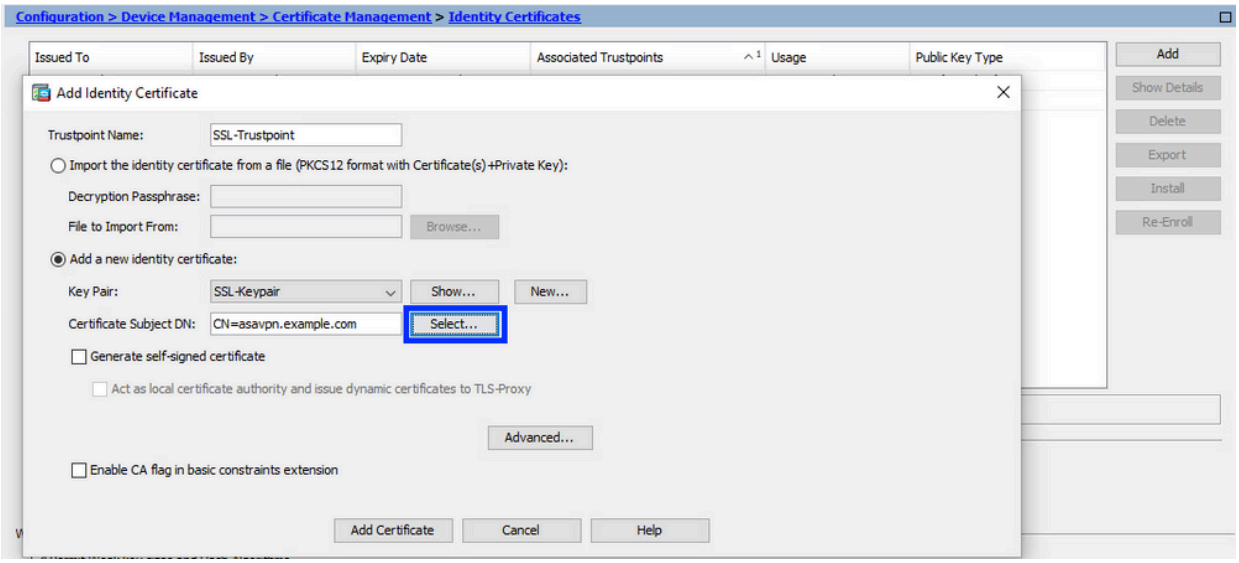


4. Configurare il soggetto del certificato e il nome di dominio completo (FQDN)

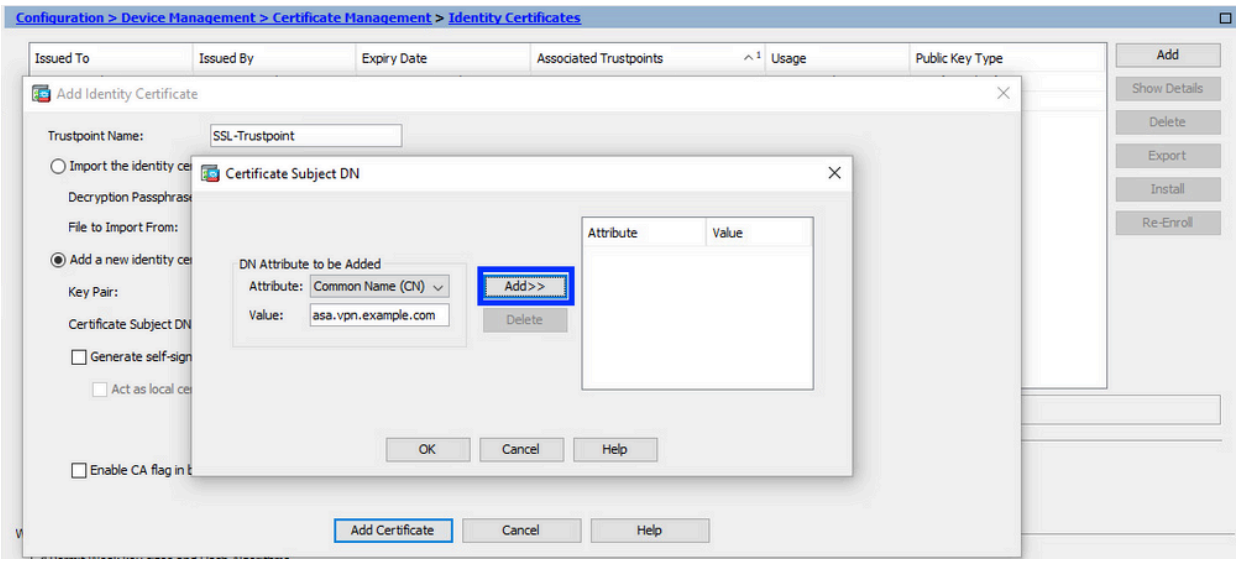
Attenzione: il parametro FQDN deve corrispondere all'FQDN o all'indirizzo IP dell'interfaccia ASA per cui viene utilizzato il certificato di identità. Questo parametro imposta l'estensione SAN (Subject Alternative Name) richiesta per il certificato di identità. L'estensione SAN viene utilizzata dal client SSL/TLS/IKEv2 per verificare se il certificato corrisponde all'FQDN a cui si connette.

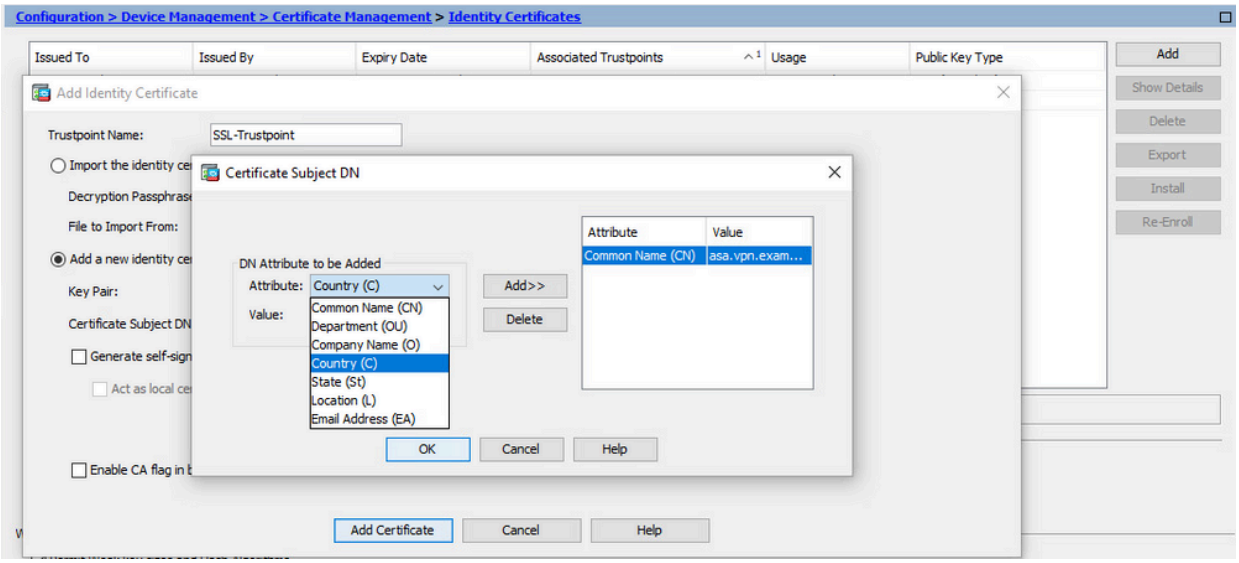
---

a. Fare clic su Seleziona.



b. Nella finestra DN soggetto certificato, configurare gli attributi del certificato - scegliere l'attributo dall'elenco a discesa, immettere il valore e fare clic su Aggiungi.



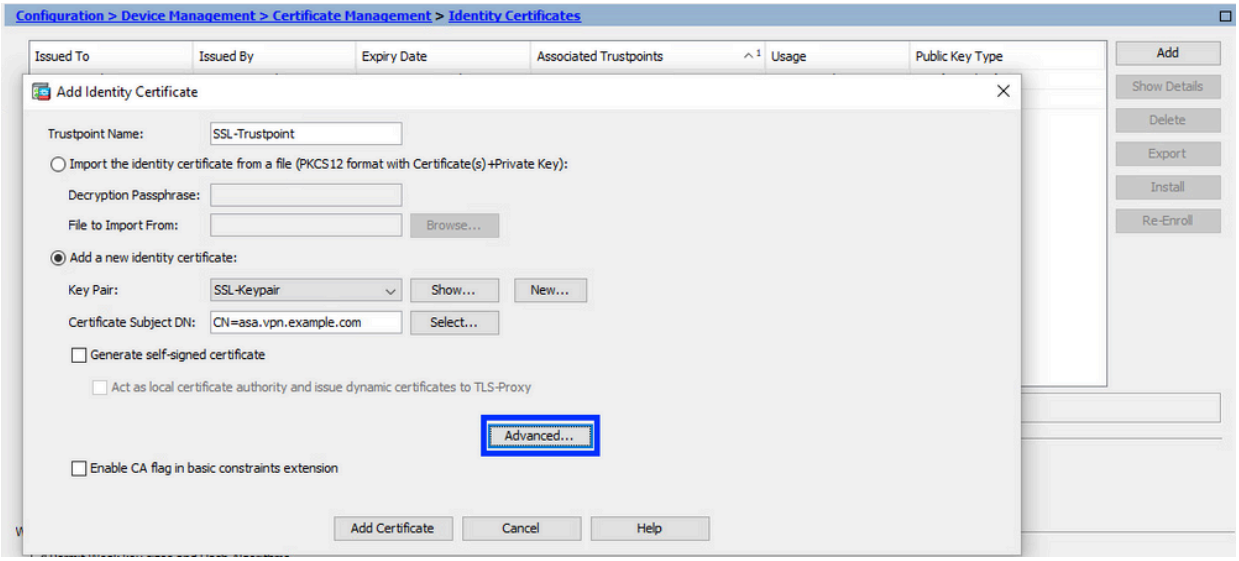


Attributo	Descrizione
CN	Il nome attraverso il quale è possibile accedere al firewall (in genere il nome di dominio completo, ad esempio vpn.example.com).
UO	Il nome del reparto all'interno dell'organizzazione
O	La ragione sociale legalmente registrata dell'azienda
C	Codice paese (codice a 2 lettere senza punteggiatura)
ST	Stato in cui si trova l'organizzazione.
L	Città in cui si trova l'organizzazione.
EA	Indirizzo email

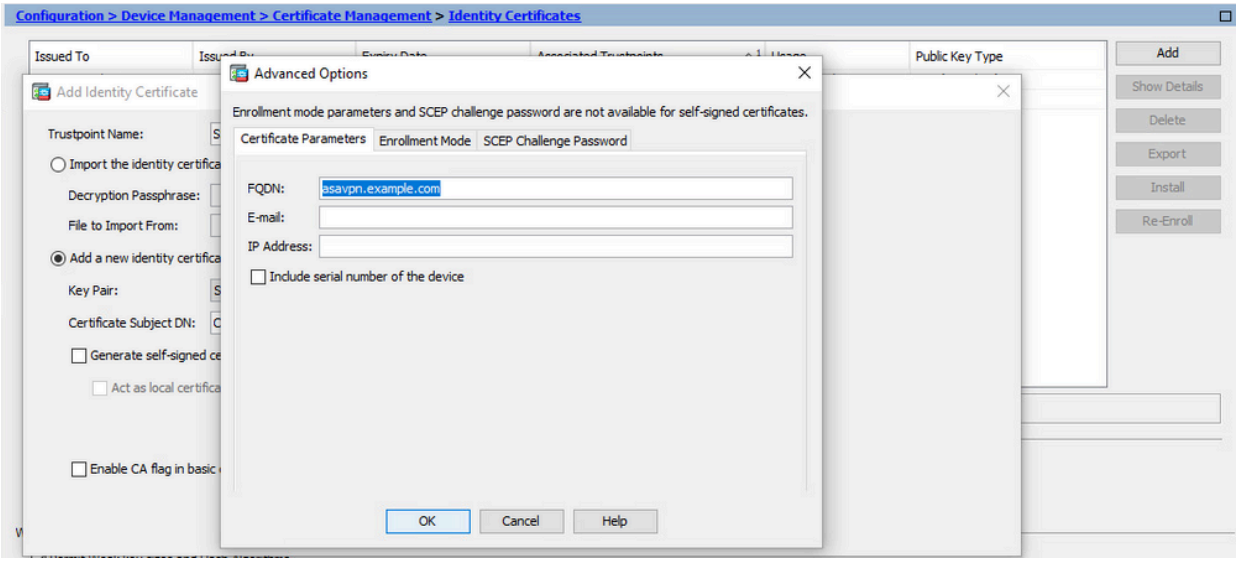
Nota: nessuno dei valori dei campi precedenti può superare il limite di 64 caratteri. Un valore più lungo può causare problemi con l'installazione del certificato di identità. Inoltre, non è necessario definire tutti gli attributi DN.

Dopo aver aggiunto tutti gli attributi, fare clic su OK.

c. Configurare l'FQDN del dispositivo - fare clic su Avanzate.

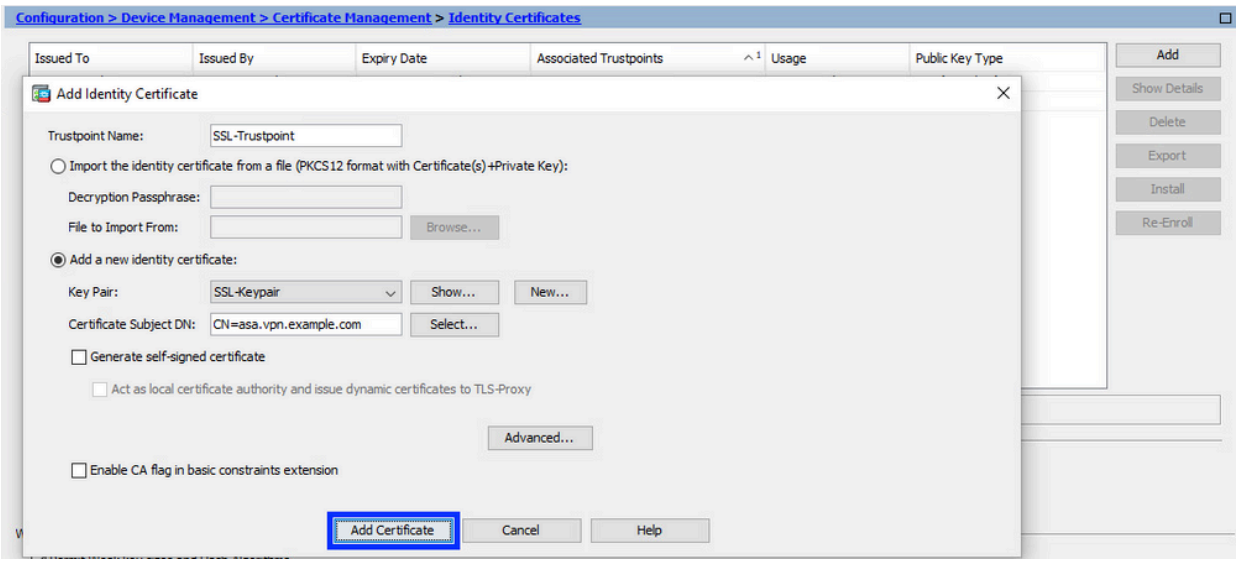


d. Nel campo FQDN immettere il nome di dominio completo tramite il quale il dispositivo è accessibile da Internet. Fare clic su OK.

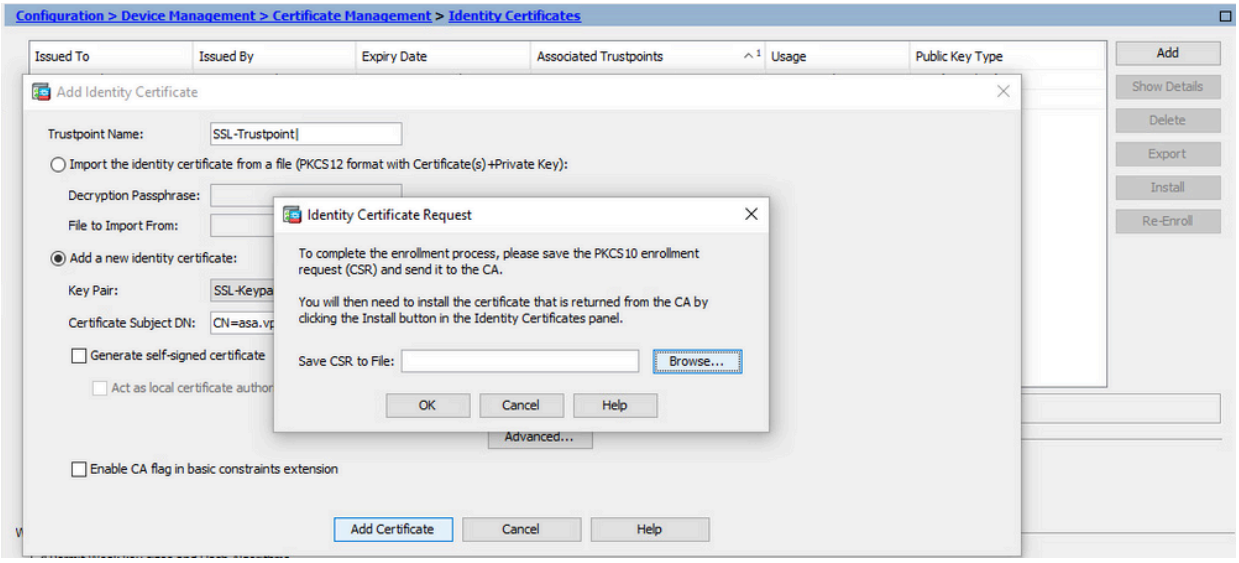


5. Generare e salvare il CSR

a. Fare clic su Aggiungi certificato.



b. Viene visualizzato un prompt per salvare il CSR in un file sul computer locale.

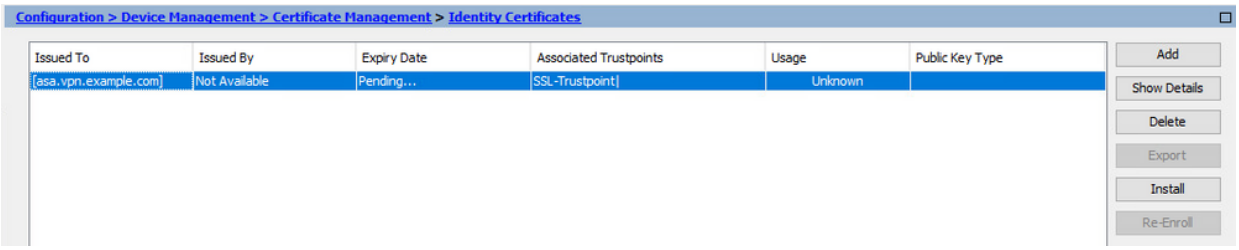


Fare clic su Sfoglia, scegliere il percorso in cui salvare il CSR e salvare il file con estensione txt.

Nota: quando il file viene salvato con estensione .txt, è possibile aprire e visualizzare la richiesta PKCS#10 con un editor di testo, ad esempio Blocco note.

---

c. A questo punto il nuovo trust point viene visualizzato in stato In sospeso.

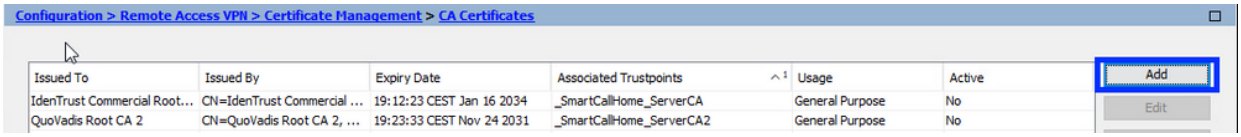


Installare il certificato di identità in formato PEM con ASDM

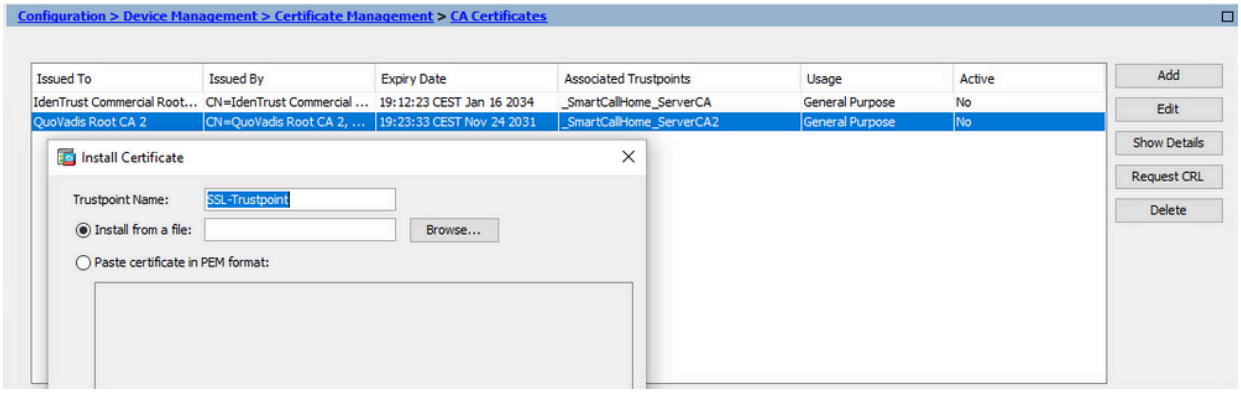
Nelle procedure di installazione si presuppone che l'autorità di certificazione abbia firmato il CSR e abbia fornito un certificato di identità con codifica PEM (.pem, .cer, .crt) e un bundle di certificati CA.

1. Installa certificato CA con firma CSR

   a. Passare a Configurazione > Gestione dispositivi > Gestione certificati > e scegliere Certificati CA. Fare clic su Add.



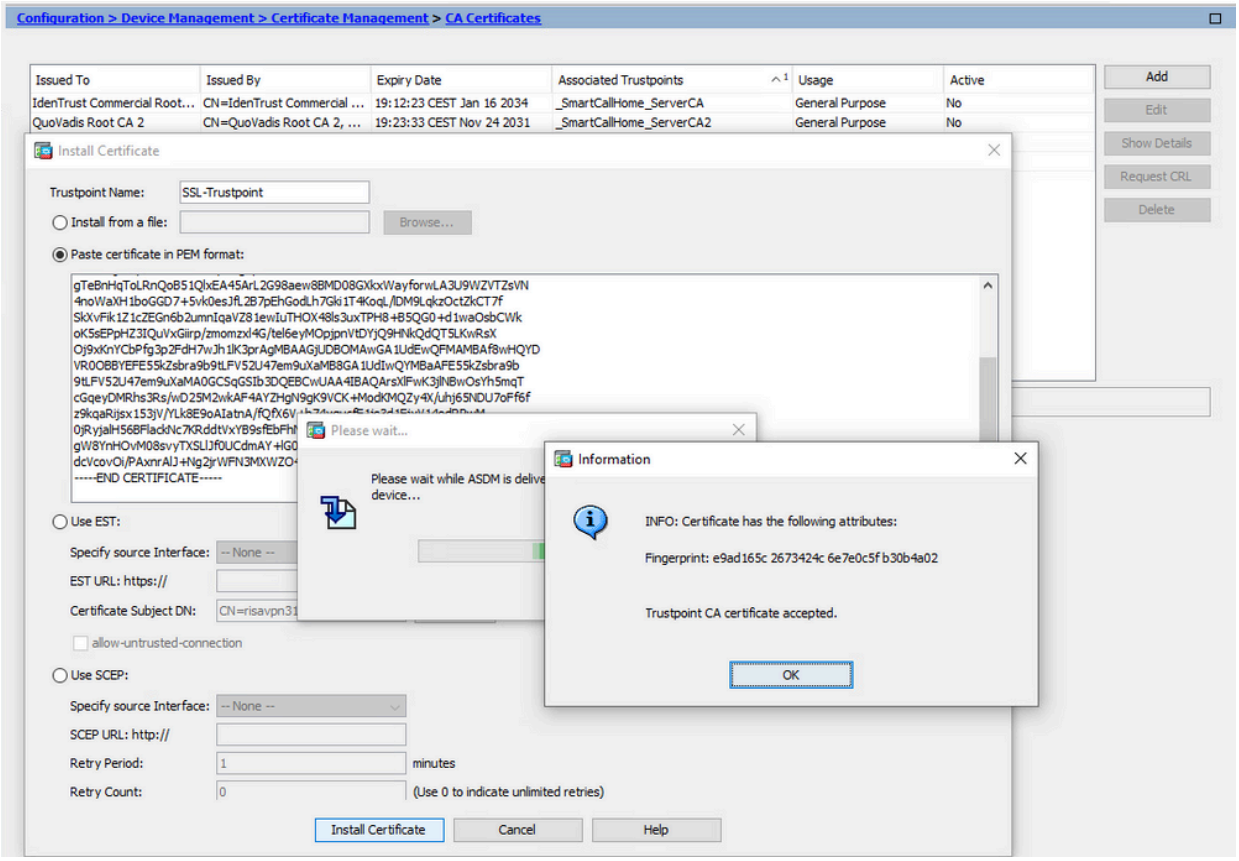
   b. Immettere il nome del Trustpoint e selezionare Installa da file, fare clic sul pulsante Sfoglia e selezionare il certificato intermedio. In alternativa, incollare il certificato CA con codifica PEM da un file di testo nel campo di testo.



Nota: installare il certificato CA che ha firmato il CSR e utilizzare lo stesso nome del trust point del certificato di identità. Gli altri certificati CA di livello superiore nella gerarchia PKI possono essere installati in punti di attendibilità separati.

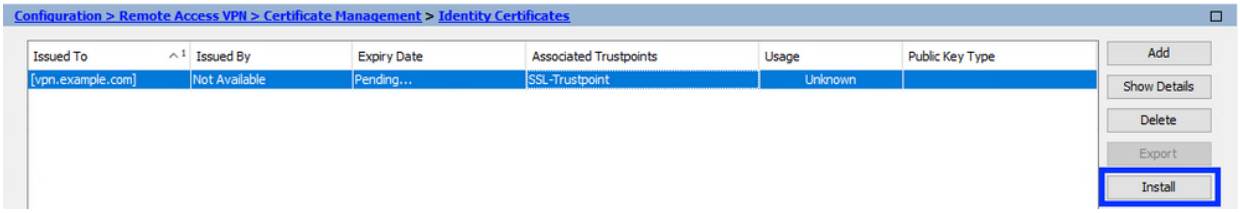
---

   c. Fare clic su Installa certificato.



2. Installa certificato di identità

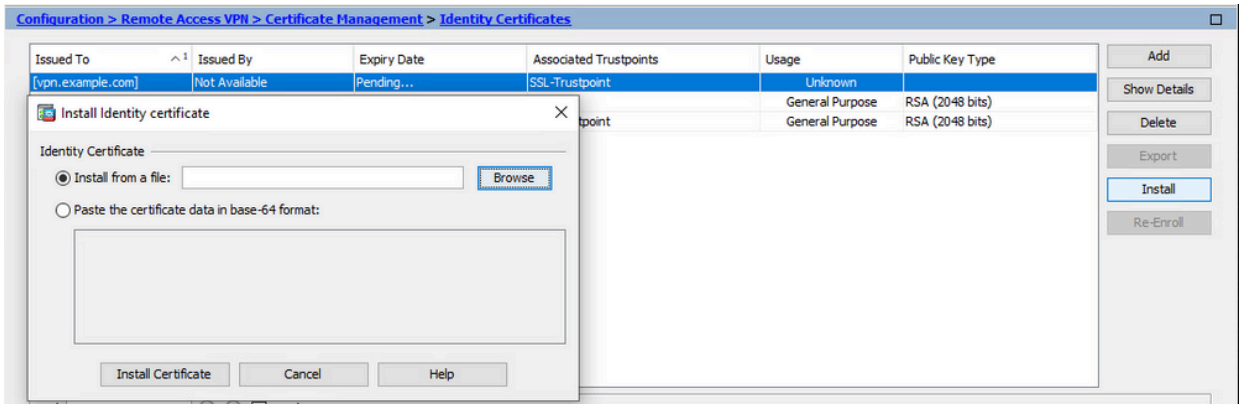
a. Scegliere il certificato di identità creato in precedenza durante la generazione di CSR. Fare clic su Install (Installa).



Nota: il campo Rilasciato da del certificato di identità può essere Non disponibile e il campo Data scadenza può essere impostato su In sospeso.

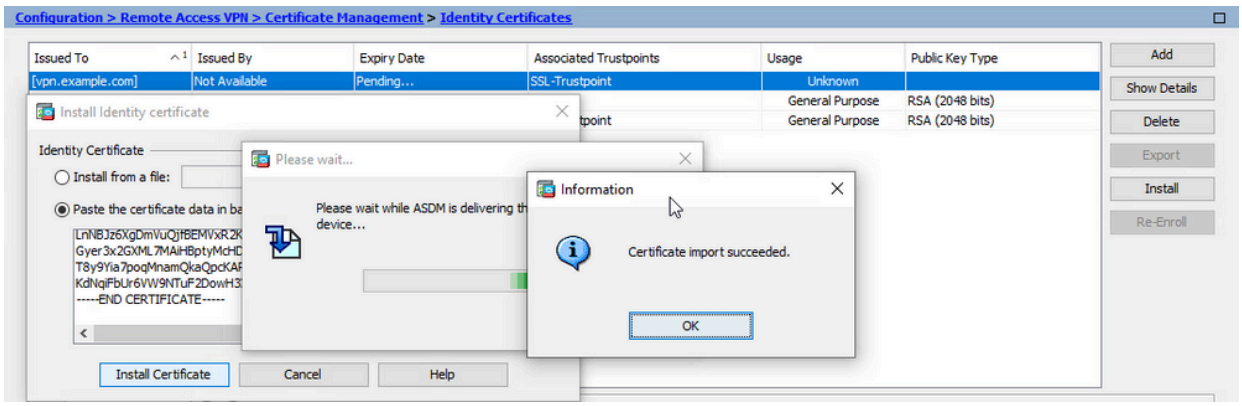
---

b. Scegliere un file contenente il certificato di identità con codifica PEM ricevuto dalla CA oppure aprire il certificato con codifica PEM in un editor di testo e copiare e incollare il certificato di identità fornito dalla CA nel campo di testo.



Nota: il certificato di identità può essere in formato .pem, .cer, .crt da installare.

c. Fare clic su Installa certificato.



3. Associare il nuovo certificato all'interfaccia con ASDM

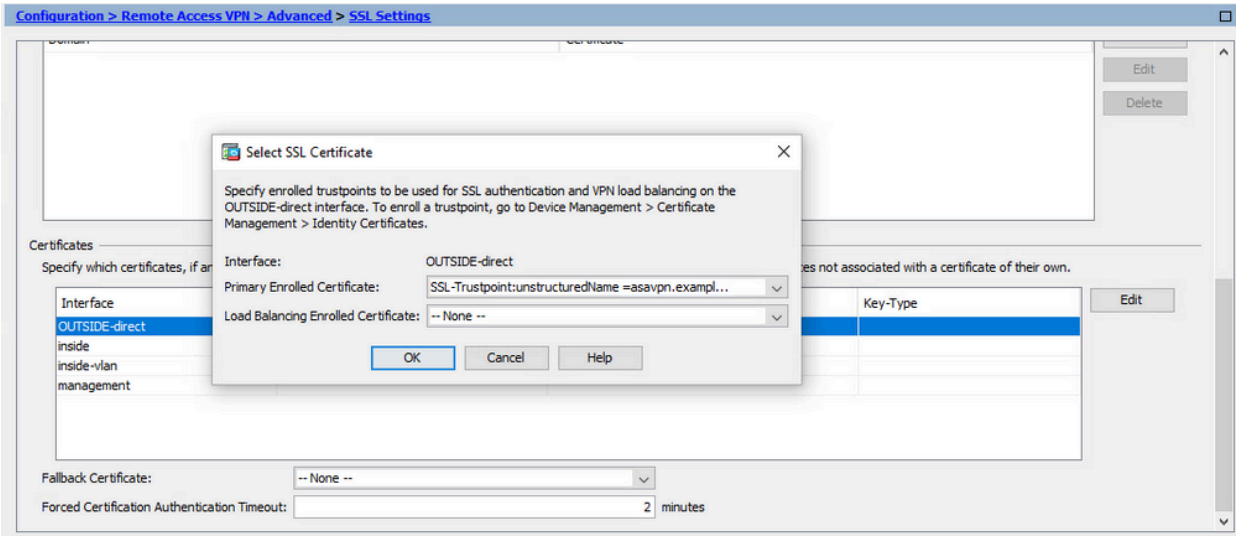
È necessario configurare l'ASA in modo che usi il nuovo certificato di identità per le sessioni WebVPN che terminano sull'interfaccia specificata.

a. Selezionare Configurazione > VPN ad accesso remoto > Avanzate > Impostazioni SSL.

b. In Certificati scegliere l'interfaccia utilizzata per terminare le sessioni WebVPN. nell'esempio viene usata l'interfaccia esterna.

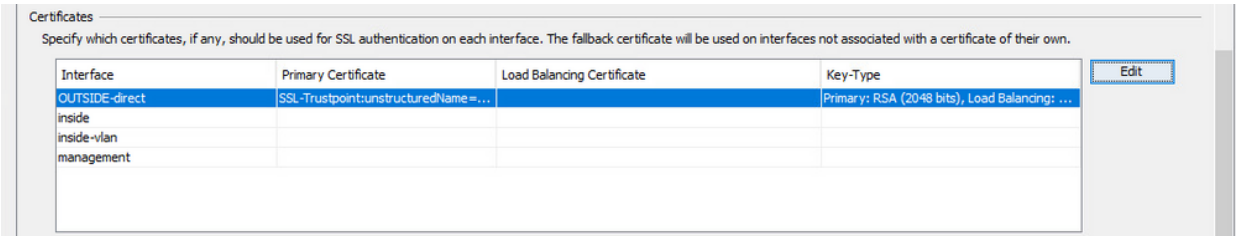
Fare clic su Modifica.

c. Nell'elenco a discesa Certificato scegliere il certificato appena installato.



d. Fare clic su OK.

e. Fare clic su Apply (Applica).



A questo punto il nuovo certificato di identità è in uso.

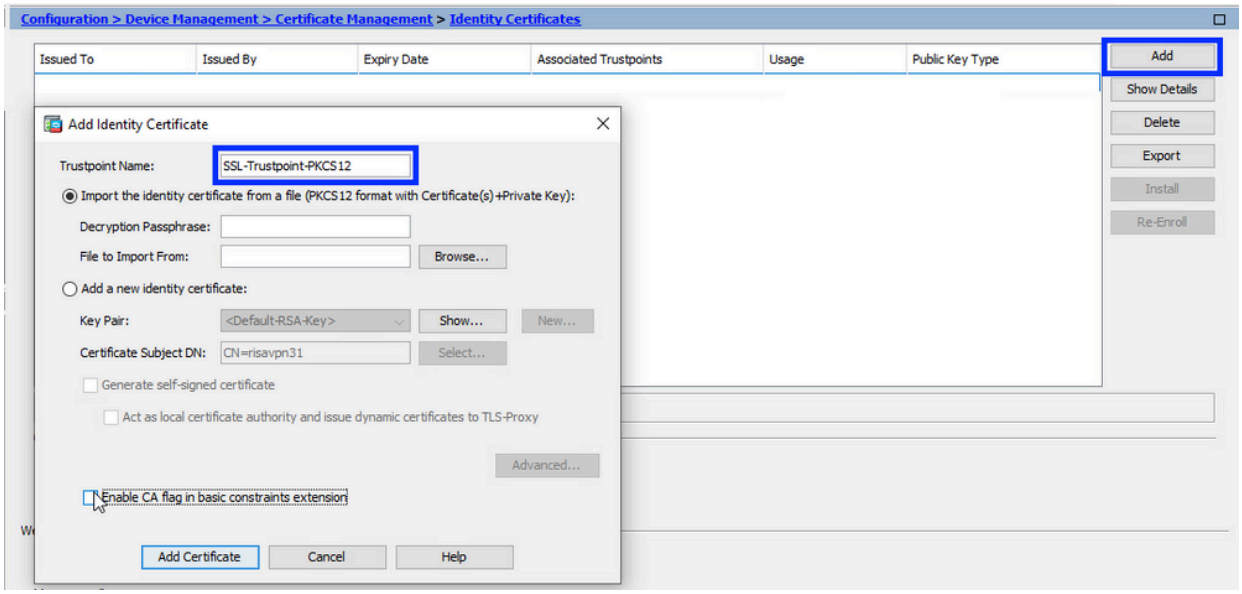
Installare un certificato di identità ricevuto nel formato PKCS12 con ASDM

Il file PKCS12 (formato .p12 o .pfx) contiene il certificato di identità, la coppia di chiavi e i certificati CA. Viene creata dalla CA, ad esempio in caso di certificato con caratteri jolly, o esportata da un dispositivo diverso. Si tratta di un file binario, che non può essere visualizzato con un editor di testo.

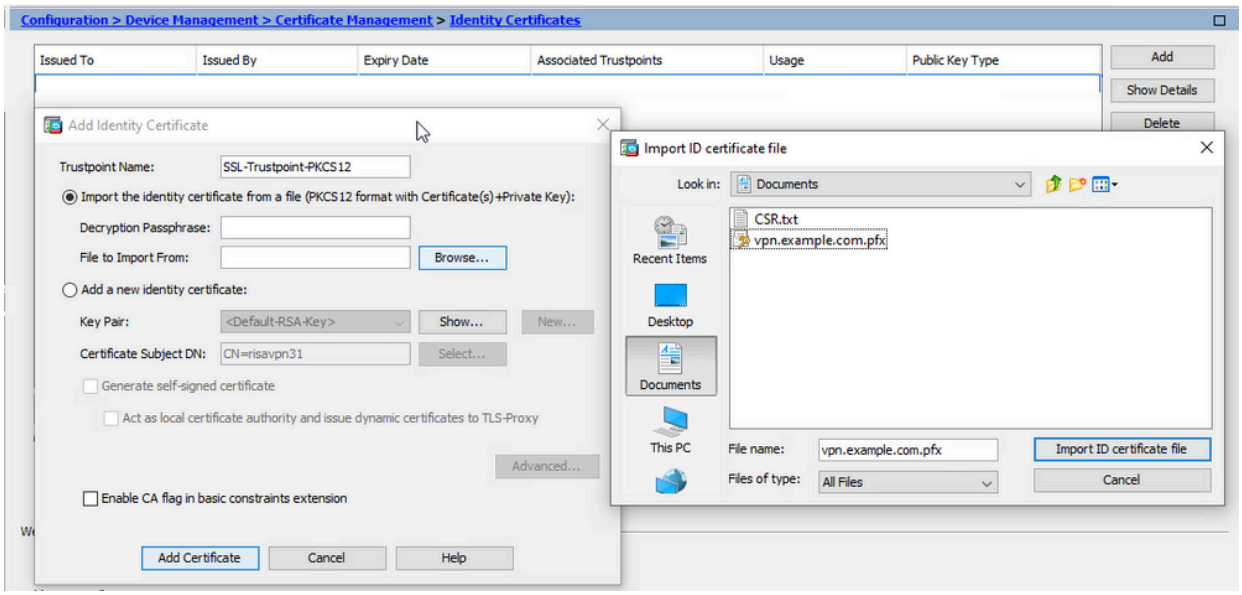
1. Installare i certificati di identità e CA da un file PKCS12

   Il certificato di identità, i certificati CA e la coppia di chiavi devono essere raggruppati in un unico file PKCS12.

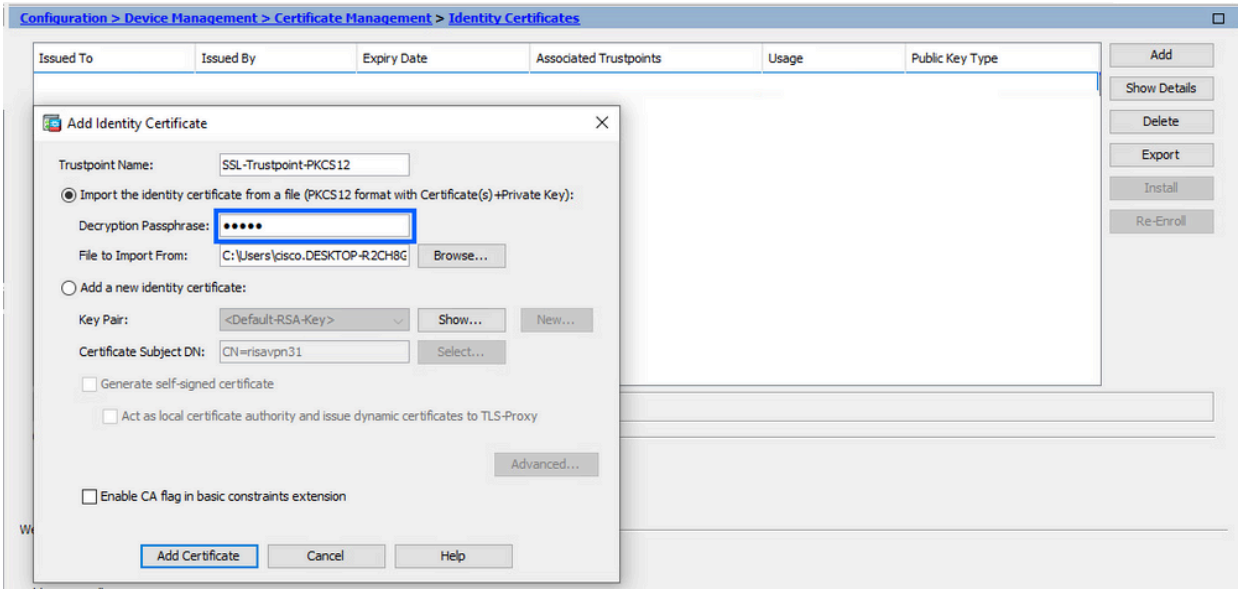
   a. Passare a Configurazione > Gestione dispositivi > Gestione certificati e scegliere Certificati di identità.
   b. Fare clic su Add.
   c. Specificare il nome di un Trustpoint.



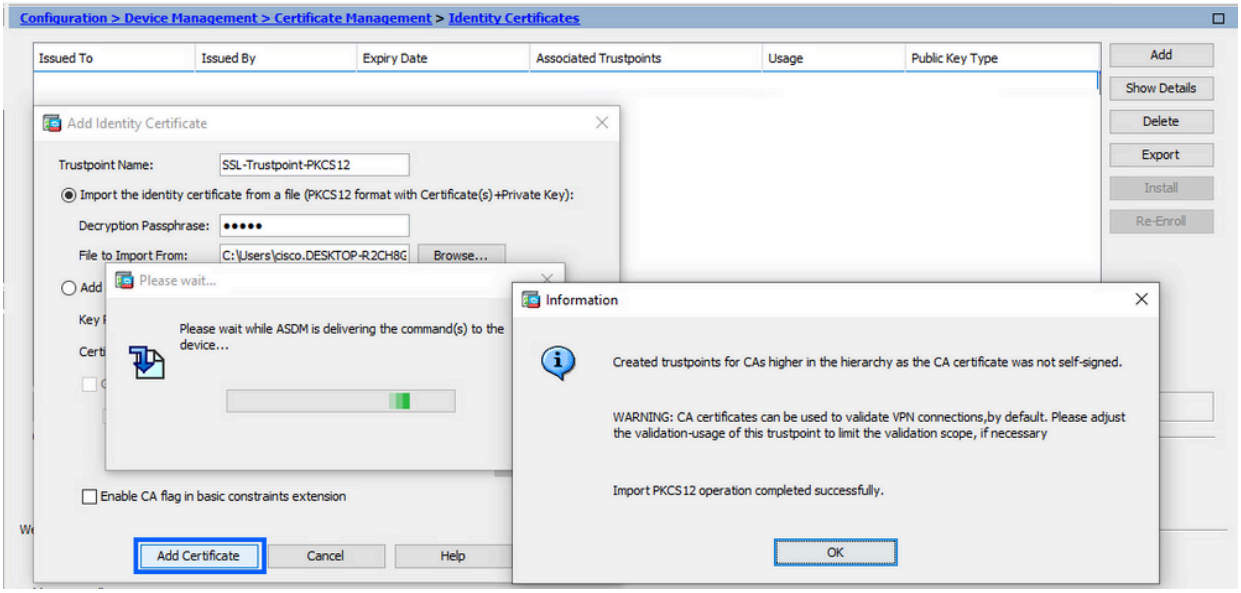
d. Fare clic sul pulsante di opzione Importa il certificato di identità da un file.



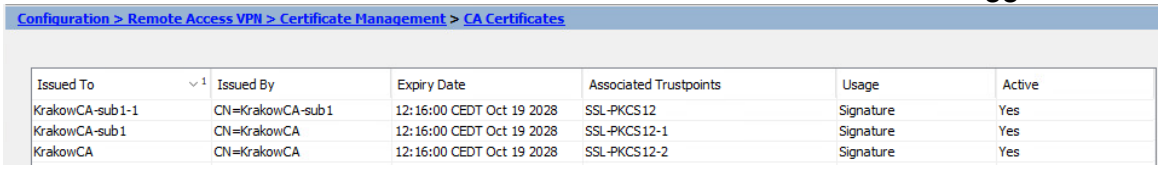
e. Immettere la passphrase utilizzata per creare il file PKCS12.



f. Fare clic su Aggiungi certificato.



Nota: quando si importa un PKCS12 con una catena di certificati CA, ASDM crea automaticamente i trust CA a monte con nomi con suffisso -number aggiunto.



Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active
KrakowCA-sub1-1	CN=KrakowCA-sub1	12:16:00 CEDT Oct 19 2028	SSL-PKCS12	Signature	Yes
KrakowCA-sub1	CN=KrakowCA	12:16:00 CEDT Oct 19 2028	SSL-PKCS12-1	Signature	Yes
KrakowCA	CN=KrakowCA	12:16:00 CEDT Oct 19 2028	SSL-PKCS12-2	Signature	Yes

2. Associare il nuovo certificato all'interfaccia con ASDM

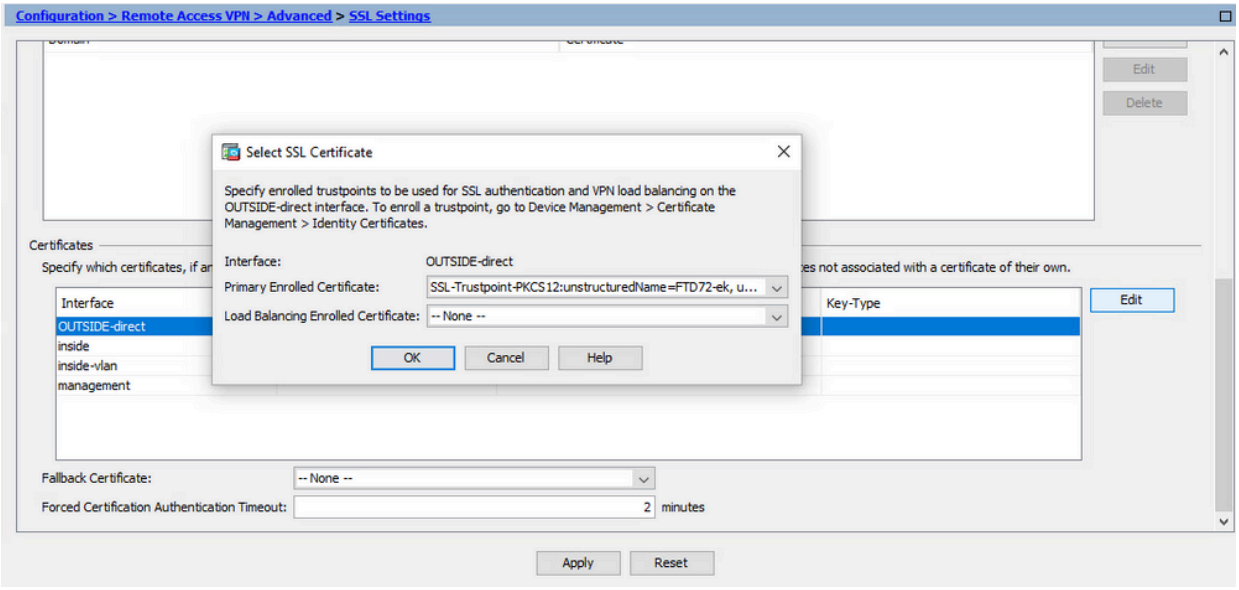
È necessario configurare l'ASA in modo che usi il nuovo certificato di identità per le sessioni WebVPN che terminano sull'interfaccia specificata.

a. Selezionare Configurazione > VPN ad accesso remoto > Avanzate > Impostazioni SSL.

b. In Certificati selezionare l'interfaccia utilizzata per terminare le sessioni WebVPN. nell'esempio viene usata l'interfaccia esterna.

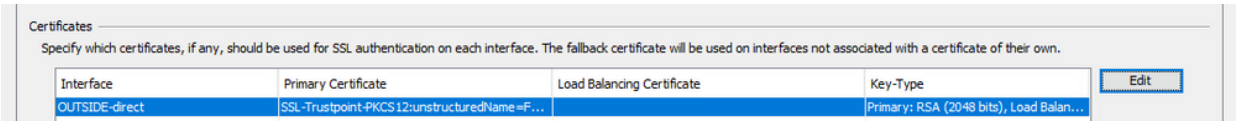
Fare clic su Modifica.

c. Nell'elenco a discesa Certificato scegliere il certificato appena installato.



d. Fare clic su OK.

e. Fare clic su Apply (Applica).



A questo punto il nuovo certificato di identità è in uso.

Rinnovo certificato

Rinnova un certificato registrato con Richiesta di firma del certificato (CSR) con ASDM

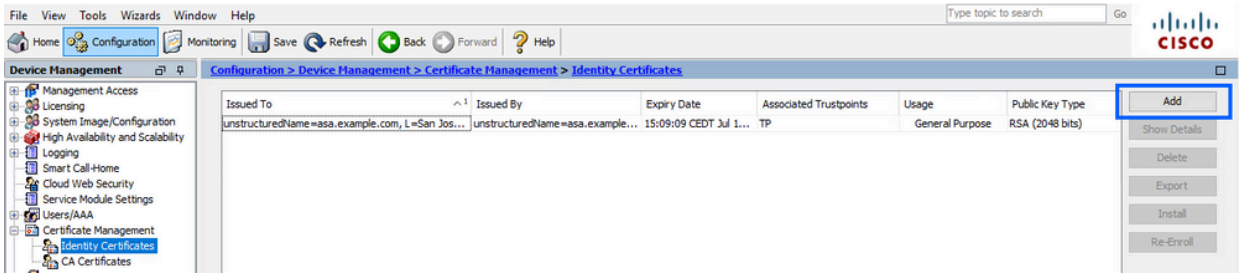
Il rinnovo del certificato del certificato registrato CSR richiede la creazione e la registrazione di un nuovo punto di attendibilità. Deve avere un nome diverso, ad esempio vecchio con suffisso anno di registrazione. Può utilizzare gli stessi parametri e la stessa coppia di chiavi del certificato precedente oppure diversi.

Generare un CSR con ASDM

1. Creare un nuovo trust point con un nome specifico.

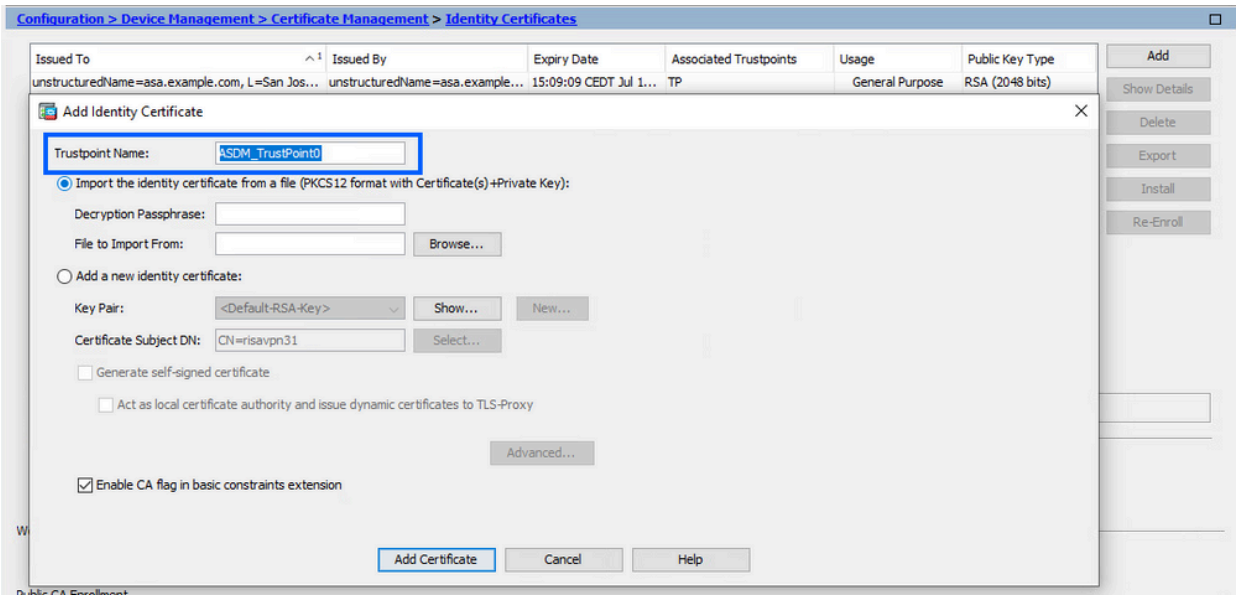
a. Passare a Configurazione > Gestione dispositivi > Gestione certificati > Certificati di

identità.



b. Fare clic su Add.

c. Definire un nome di trust.



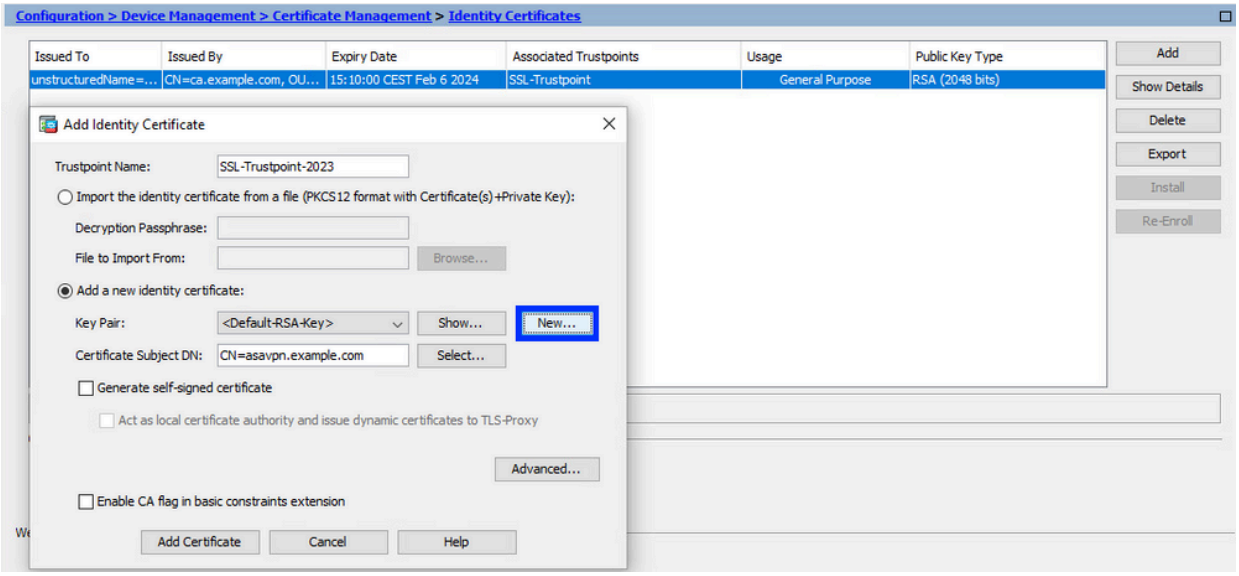
d. Fare clic sul pulsante di opzione Aggiungi nuovo certificato di identità.

2. (Facoltativo) Creare una nuova coppia di chiavi

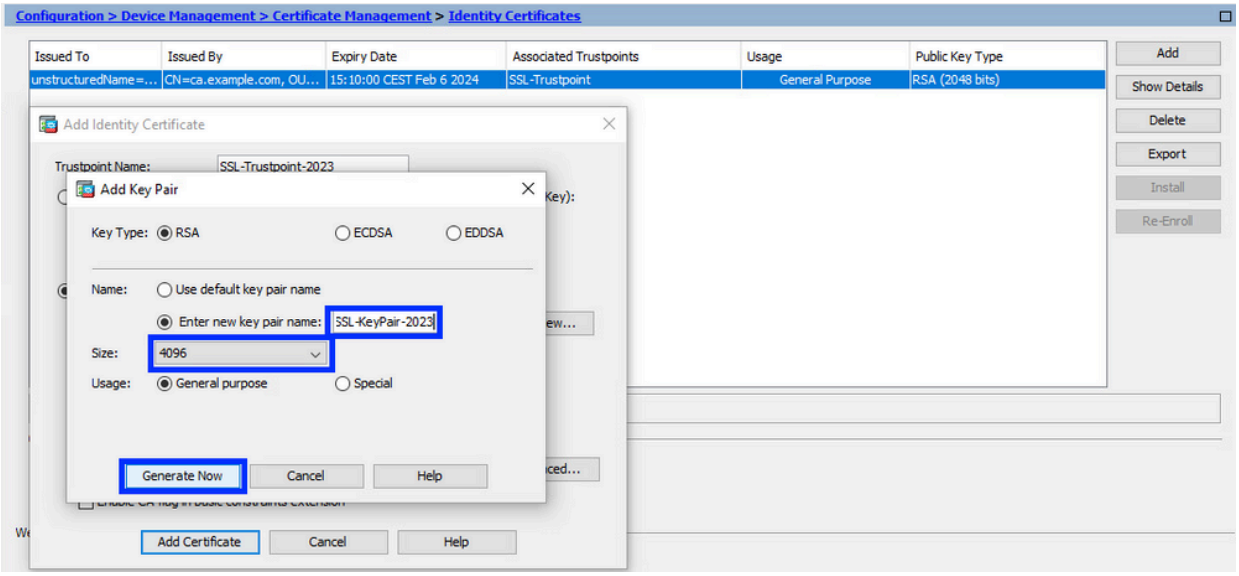
Nota: per impostazione predefinita, viene utilizzata la chiave RSA con il nome Default-RSA-Key e una dimensione di 2048; tuttavia, si consiglia di utilizzare una coppia di chiavi pubblica/privata univoca per ciascun certificato di identità.

---

a. Fare clic su Nuovo per generare una nuova coppia di chiavi.

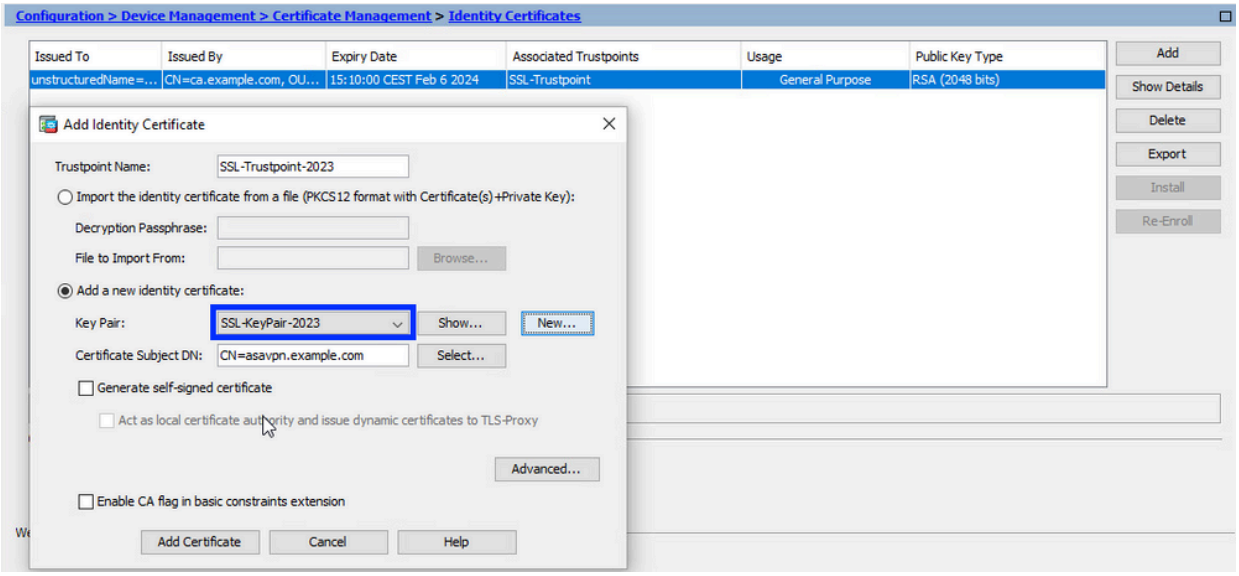


b. Scegliere l'opzione Immettere il nuovo nome della coppia di chiavi e immettere un nome per la nuova coppia di chiavi.
c. Scegliere il tipo di chiave: RSA o ECDSA.
d. Scegliere le dimensioni della chiave; per RSA, scegliere Uso generico.
e. Fare clic su Genera ora. La coppia di chiavi è stata creata.



3. Selezionare il nome della coppia di chiavi

Scegliere la coppia di chiavi con cui firmare il CSR e da associare al nuovo certificato.



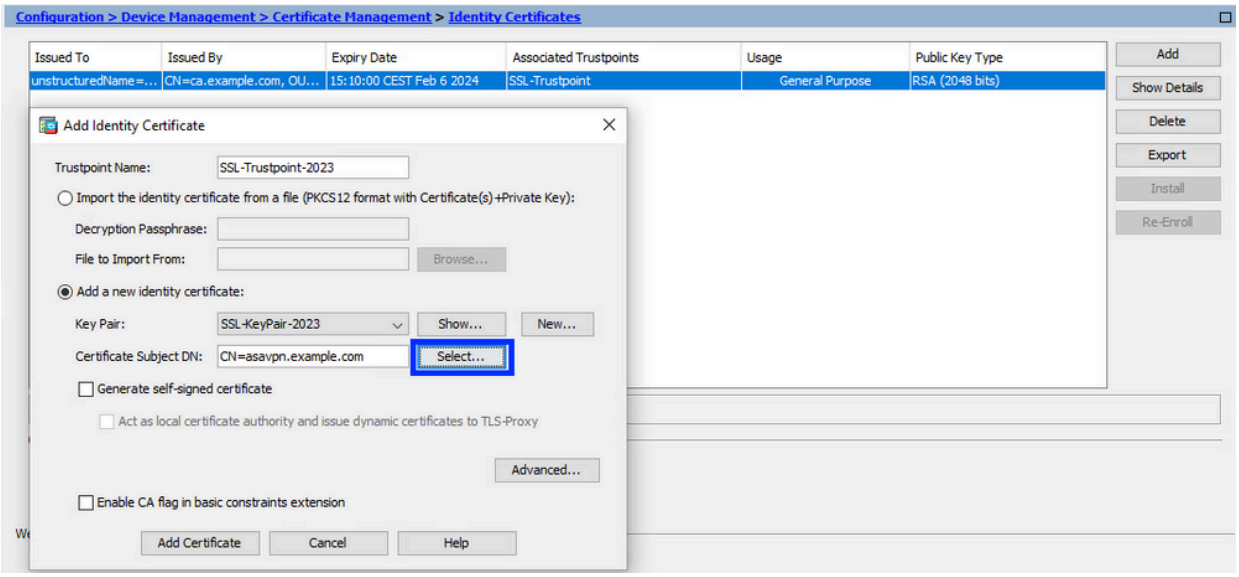
4. Configurare il soggetto del certificato e il nome di dominio completo (FQDN)

Attenzione: il parametro FQDN deve corrispondere all'FQDN o all'indirizzo IP dell'interfaccia ASA per cui viene utilizzato il certificato. Questo parametro imposta il nome alternativo del soggetto (SAN) per il certificato. Il campo SAN viene utilizzato dal client SSL/TLS/IKEv2 per verificare se il certificato corrisponde all'FQDN a cui si connette.

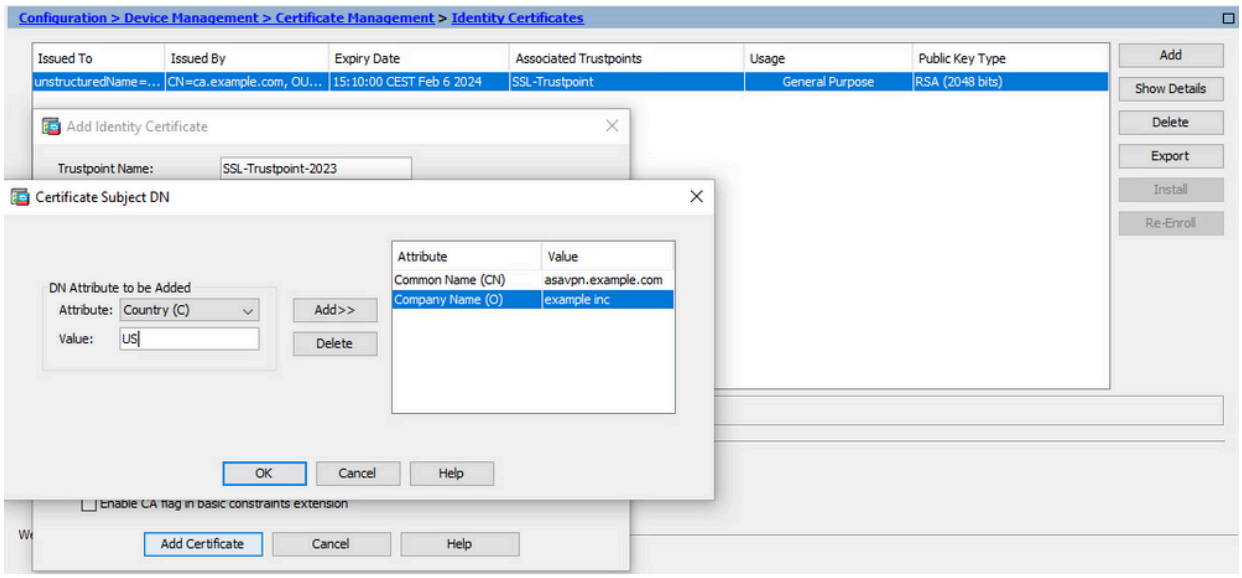
Nota: quando firma il CSR e crea un certificato di identità firmato, CA può modificare i parametri FQDN e Nome soggetto definiti nel trust point.

---

a. Fare clic su Seleziona.



b. Nella finestra DN soggetto certificato, configurare gli attributi del certificato - selezionare l'attributo dall'elenco a discesa, immettere il valore e fare clic su Aggiungi.

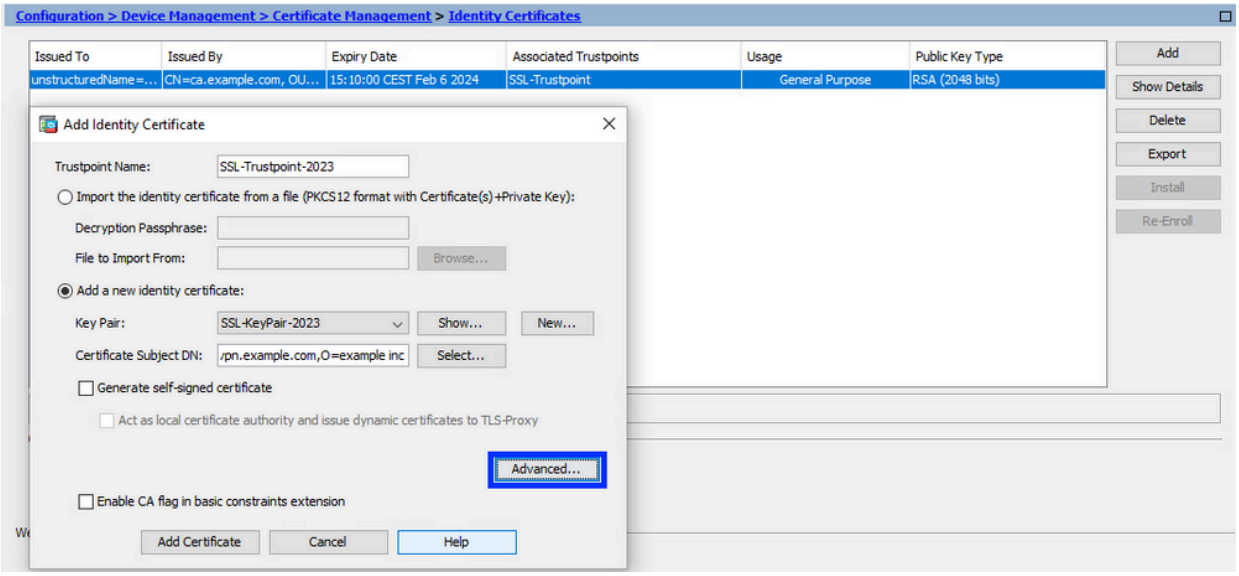


Attributo	Descrizione
CN	Il nome attraverso il quale è possibile accedere al firewall (in genere il nome di dominio completo, ad esempio vpn.example.com).
UO	Il nome del reparto all'interno dell'organizzazione
O	La ragione sociale legalmente registrata dell'azienda
C	Codice paese (codice a 2 lettere senza punteggiatura)
ST	Stato in cui si trova l'organizzazione.
L	Città in cui si trova l'organizzazione.
EA	Indirizzo email

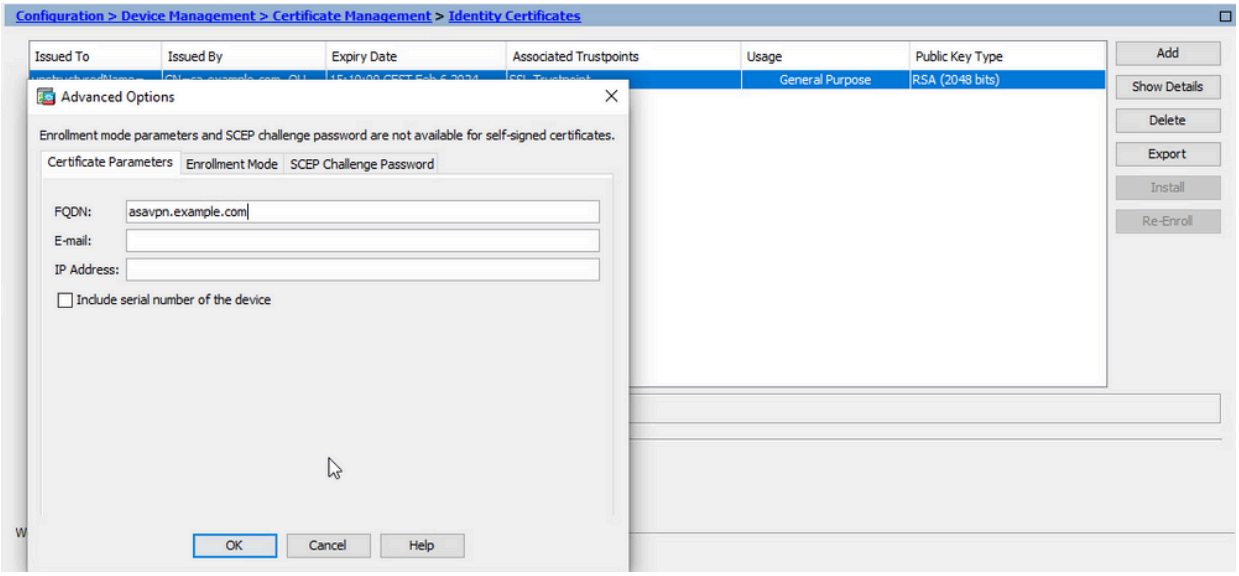
Nota: nessuno dei campi precedenti può superare il limite di 64 caratteri. Un valore più lungo può causare problemi con l'installazione del certificato di identità. Inoltre, non è necessario definire tutti gli attributi DN.

Dopo aver aggiunto tutti gli attributi, fare clic su OK.

c. Per configurare l'FQDN del dispositivo, fare clic su Avanzate.

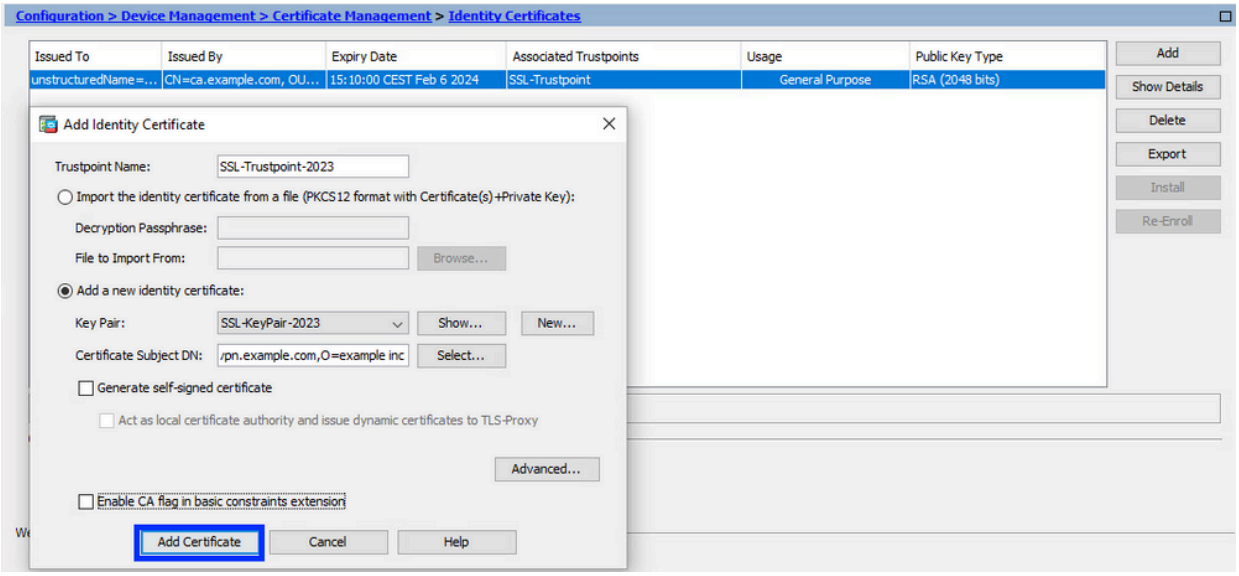


d. Nel campo FQDN immettere il nome di dominio completo tramite il quale il dispositivo è accessibile da Internet. Fare clic su OK.

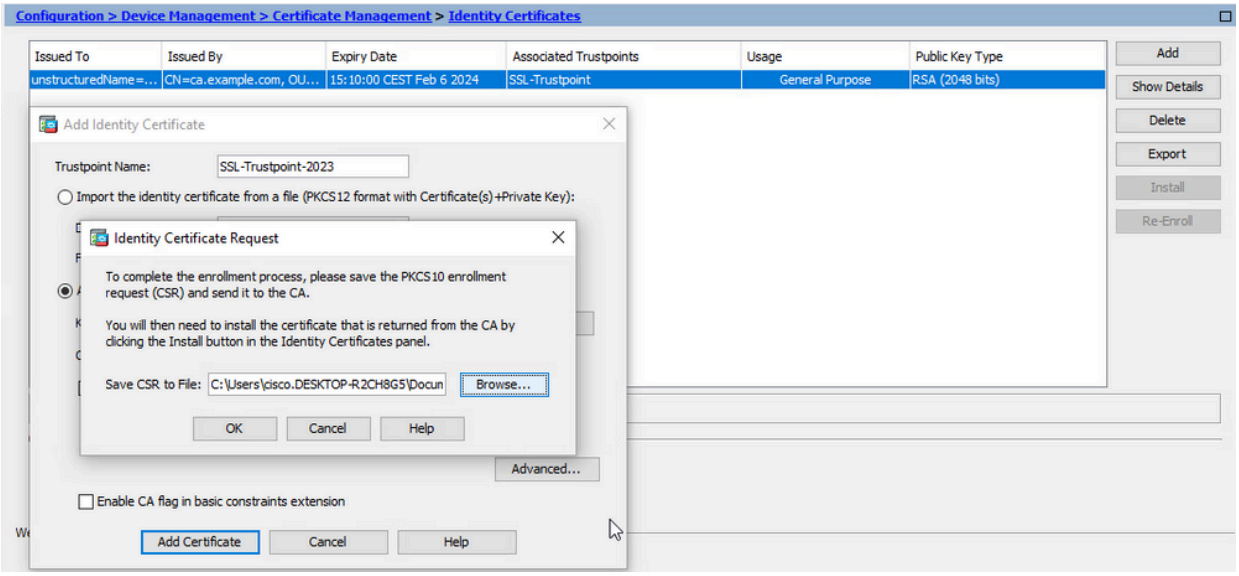


5. Generare e salvare il CSR

a. Fare clic su Aggiungi certificato.



b. Viene visualizzato un prompt per salvare il CSR in un file sul computer locale.

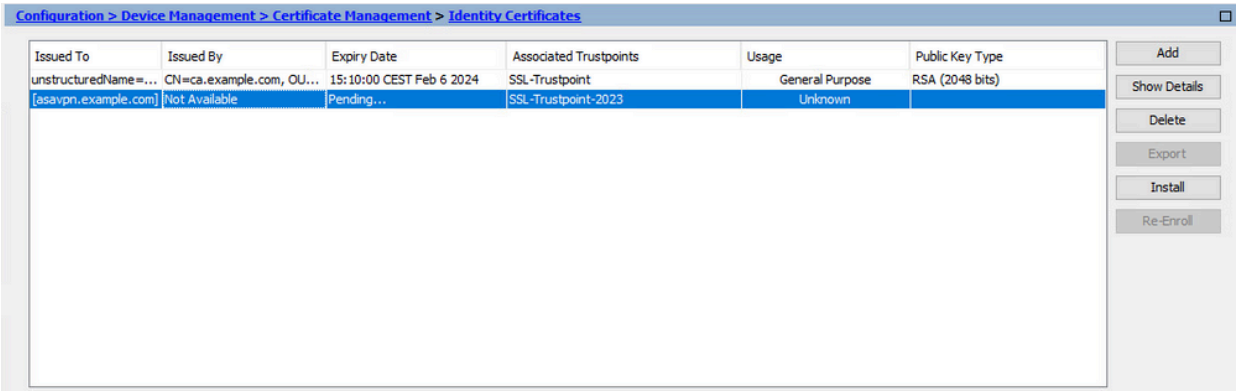


Scegliere Sfoglia. Scegliere un percorso in cui salvare il CSR e salvare il file con estensione .txt.

> Nota: quando il file viene salvato con estensione .txt, è possibile aprire e visualizzare la richiesta PKCS#10 con un editor di testo, ad esempio Blocco note.

---

c. A questo punto il nuovo trust point viene visualizzato in stato In sospeso.



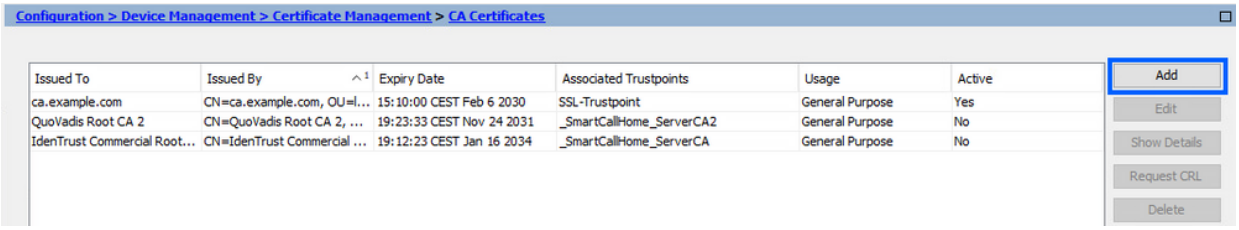
Installare il certificato di identità in formato PEM con ASDM

Nelle procedure di installazione si presuppone che l'autorità di certificazione abbia firmato il CSR e abbia fornito un nuovo certificato di identità e un bundle di certificati CA codificati PEM (.pem, .cer, .crt).

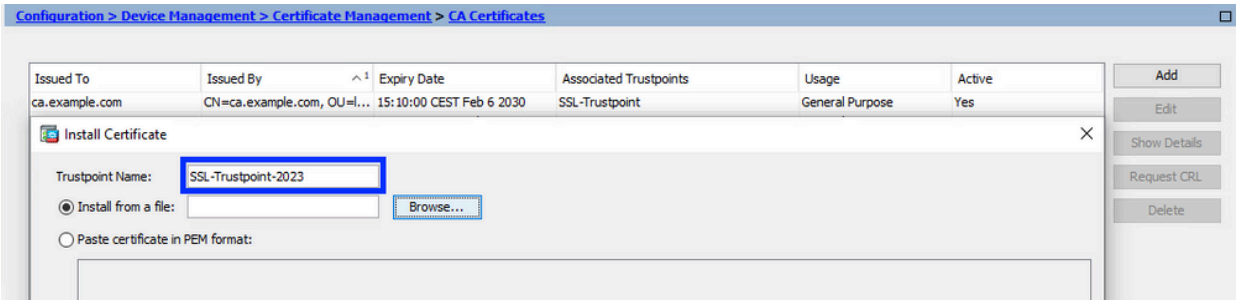
1. Installa certificato CA con firma CSR

   Il certificato CA che ha firmato il certificato di identità può essere installato nel punto di fiducia creato per il certificato di identità. Se il certificato di identità è firmato da un'autorità di certificazione intermedia, è possibile installare tale certificato nel punto di fiducia del certificato di identità. Tutti i certificati CA a monte nella gerarchia possono essere installati in punti di trust CA distinti.

   a. Passare a Configurazione > Gestione dispositivi >Gestione certificati > e scegliere Certificati CA. Fare clic su Add.



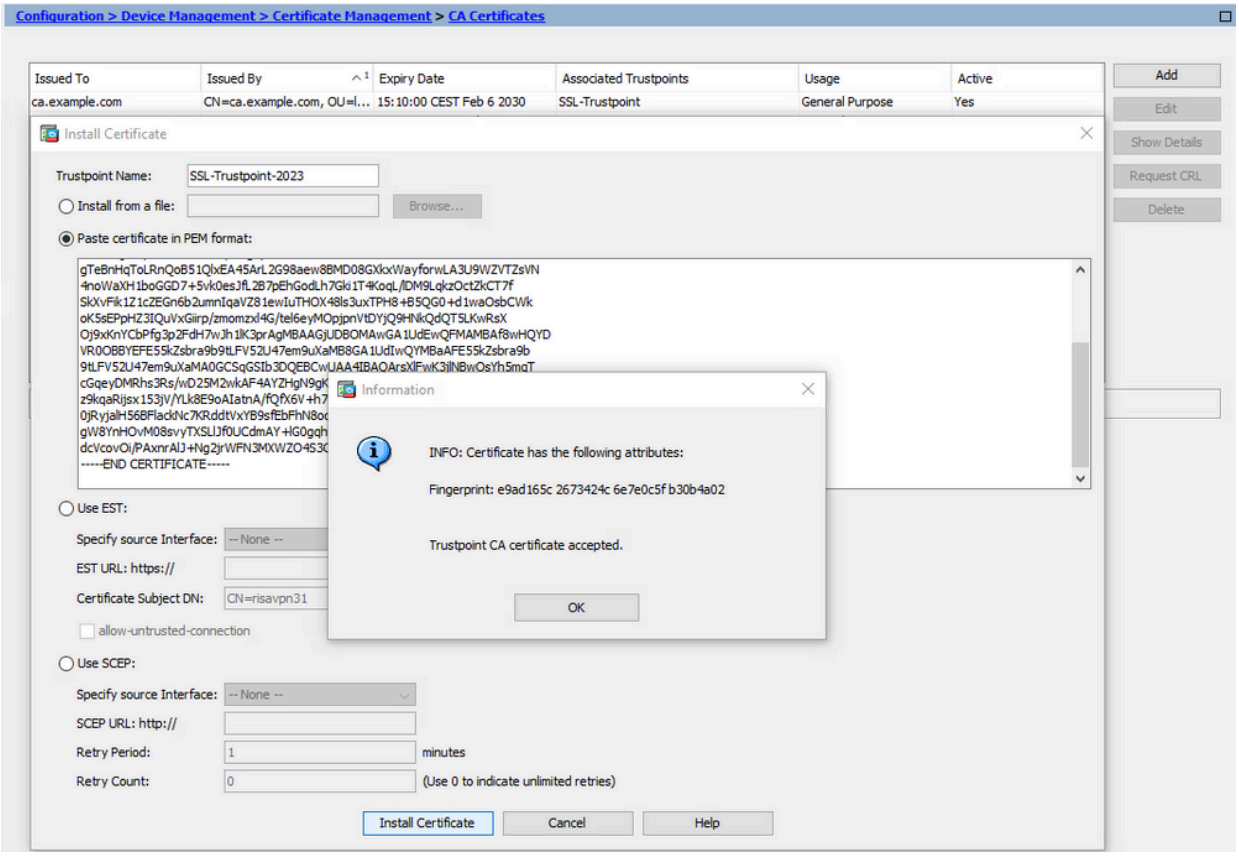
   b. Immettere il nome del Trustpoint e scegliere Installa da file, fare clic su Pulsante Sfoglia, quindi scegliere il certificato intermedio. In alternativa, incollare il certificato CA con codifica PEM da un file di testo nel campo di testo.



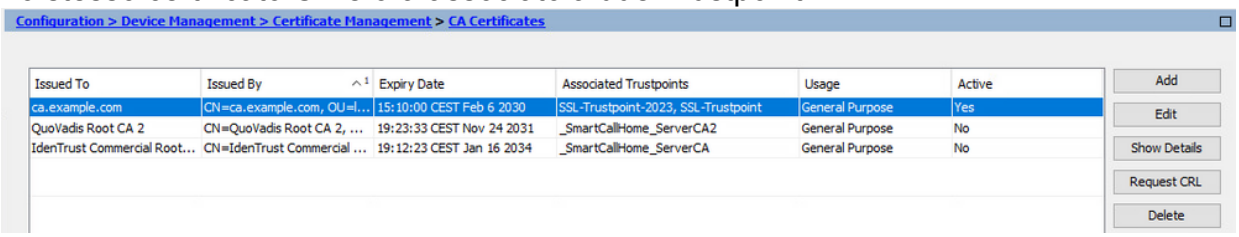
Nota: installare il certificato intermedio con lo stesso nome del trust point del

certificato di identità, se il certificato di identità è firmato da un certificato CA intermedio.

c. Fare clic su Installa certificato.

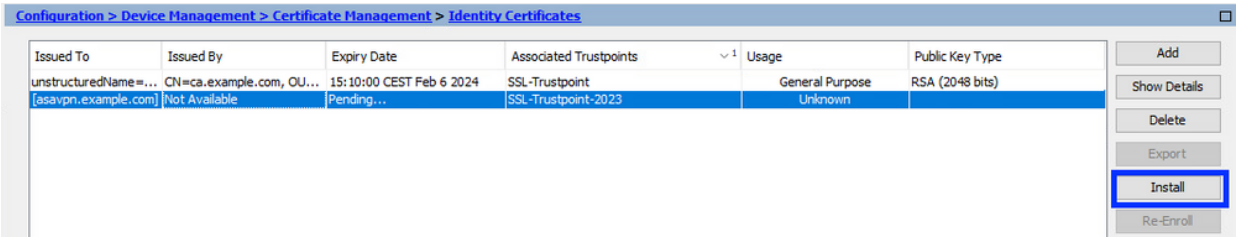


Nell'esempio il nuovo certificato è firmato con lo stesso certificato CA del precedente. Lo stesso certificato CA è ora associato a due Trustpoint.



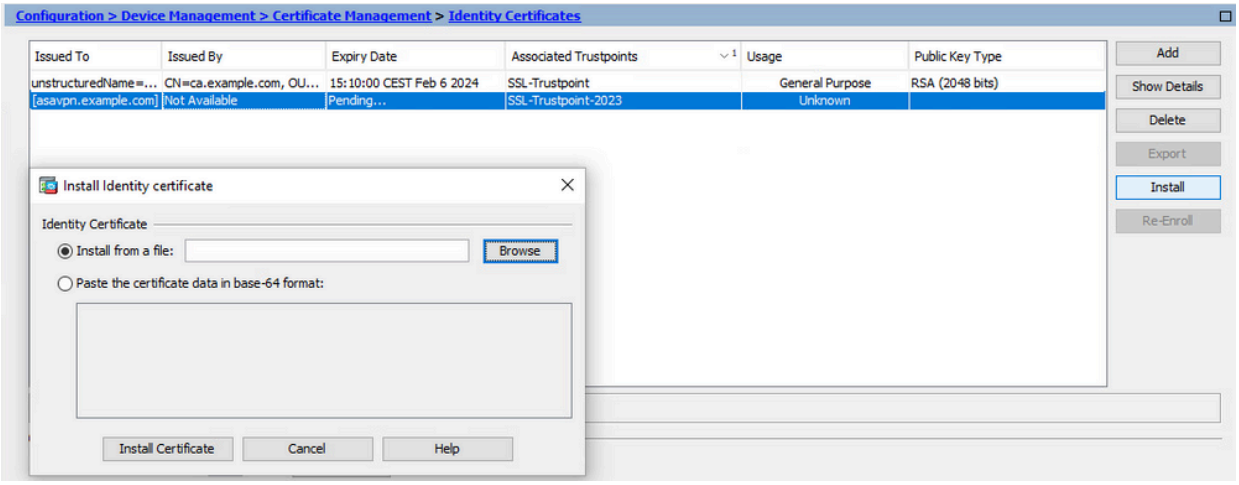
2. Installa certificato di identità

a. Scegliere il certificato di identità creato in precedenza con la generazione di CSR. Fare clic su Install (Installa).



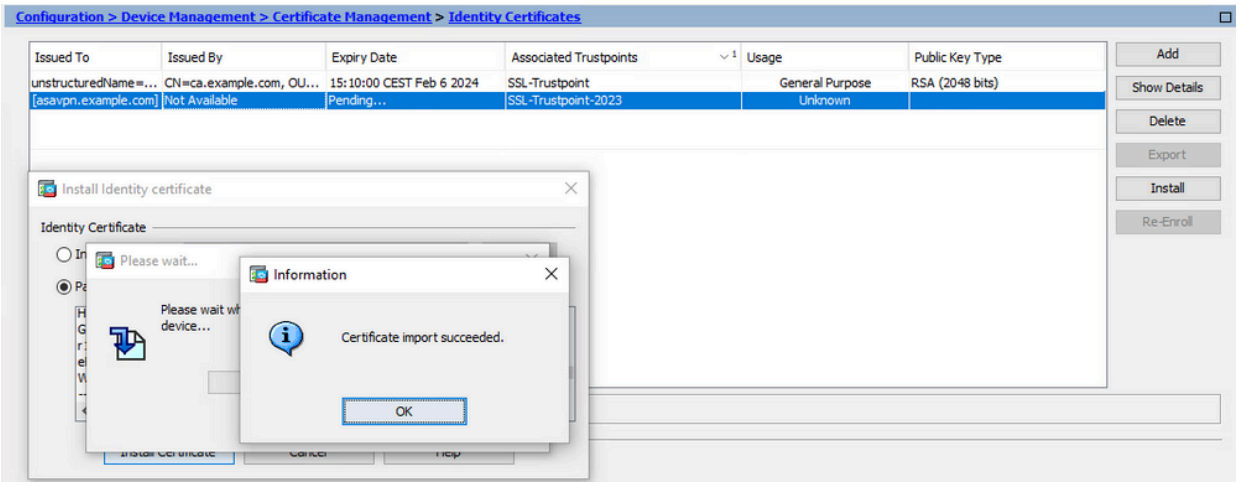
Nota: il campo Rilasciato da del certificato di identità può essere Non disponibile e il campo Data scadenza può essere impostato su In sospeso.

b. Scegliere un file contenente il certificato di identità con codifica PEM ricevuto dalla CA oppure aprire il certificato con codifica PEM in un editor di testo e copiare e incollare il certificato di identità fornito dalla CA nel campo di testo.

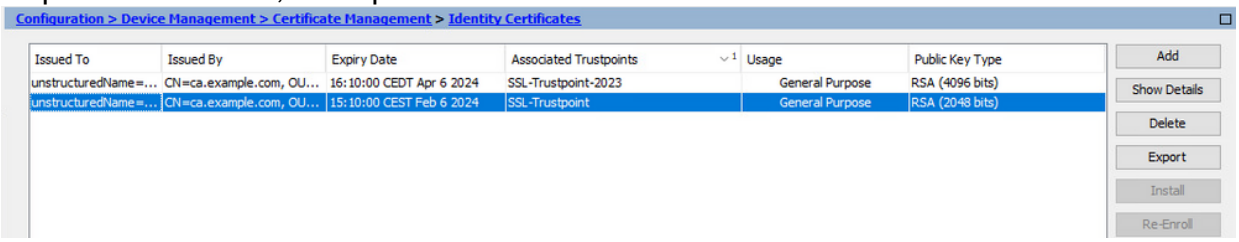


Nota: il certificato di identità può essere in formato .pem, .cer, .crt da installare.

c. Fare clic su Installa certificato.



Dopo l'installazione, sono presenti certificati di identità vecchi e nuovi.



3. Associare il nuovo certificato all'interfaccia con ASDM

È necessario configurare l'ASA in modo che usi il nuovo certificato di identità per le sessioni

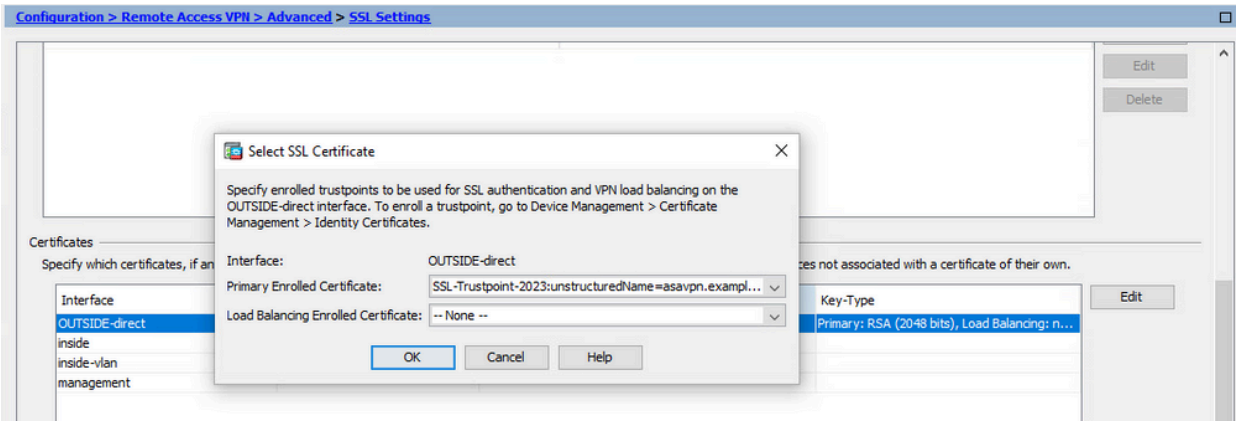
WebVPN che terminano sull'interfaccia specificata.

a. Selezionare Configurazione > VPN ad accesso remoto > Avanzate > Impostazioni SSL.

b. In Certificati scegliere l'interfaccia utilizzata per terminare le sessioni WebVPN. nell'esempio viene usata l'interfaccia esterna.

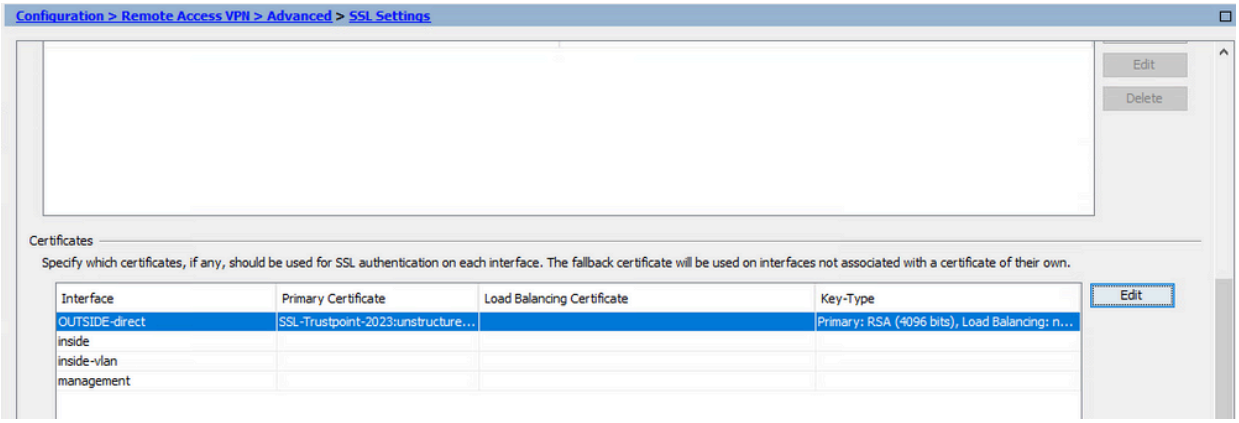
   Fare clic su Modifica.

c. Nell'elenco a discesa Certificato scegliere il certificato appena installato.



d. Fare clic su OK.

e. Fare clic su Apply (Applica). A questo punto il nuovo certificato di identità è in uso.



Rinnova un certificato registrato con un file PKCS12 con ASDM

Il rinnovo del certificato di un certificato registrato PKCS12 richiede la creazione e la registrazione di un nuovo trust point. Deve avere un nome diverso, ad esempio vecchio con suffisso anno di registrazione.

Il file PKCS12 (formato .p12 o .pfx) contiene il certificato di identità, la coppia di chiavi e i certificati CA. Viene creata dalla CA, ad esempio in caso di certificato con caratteri jolly, oppure esportata da un dispositivo diverso. Si tratta di un file binario e non può essere visualizzato con un editor di testo.

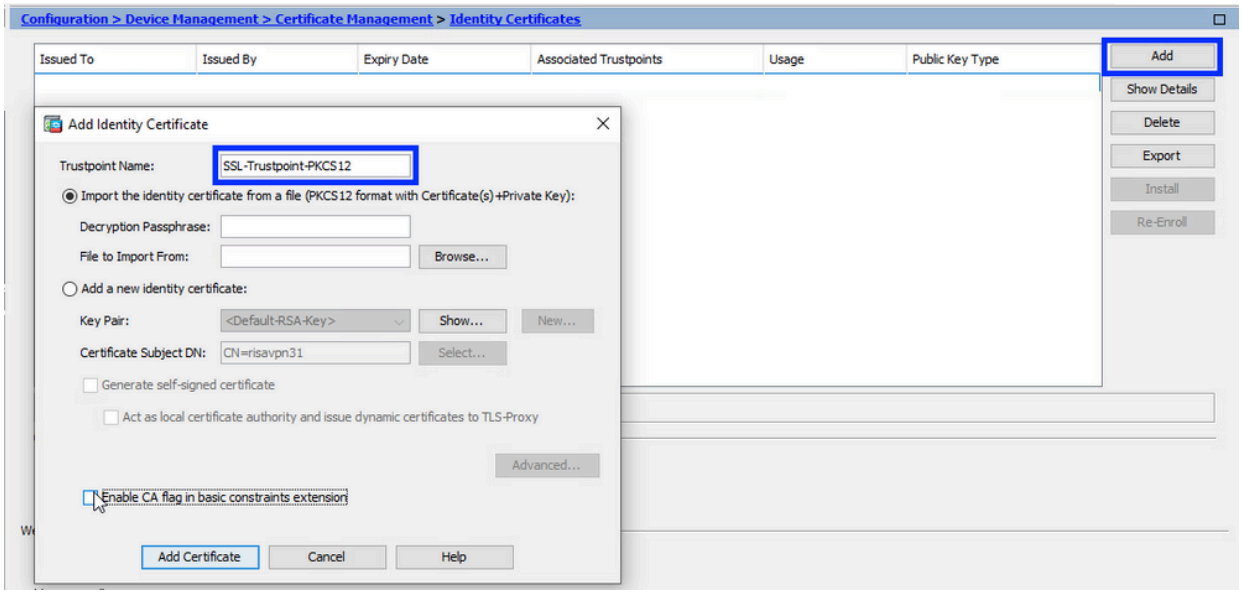
1. Installare il certificato di identità e i certificati CA rinnovati da un file PKCS12

Il certificato di identità, i certificati CA e la coppia di chiavi devono essere raggruppati in un unico file PKCS12.

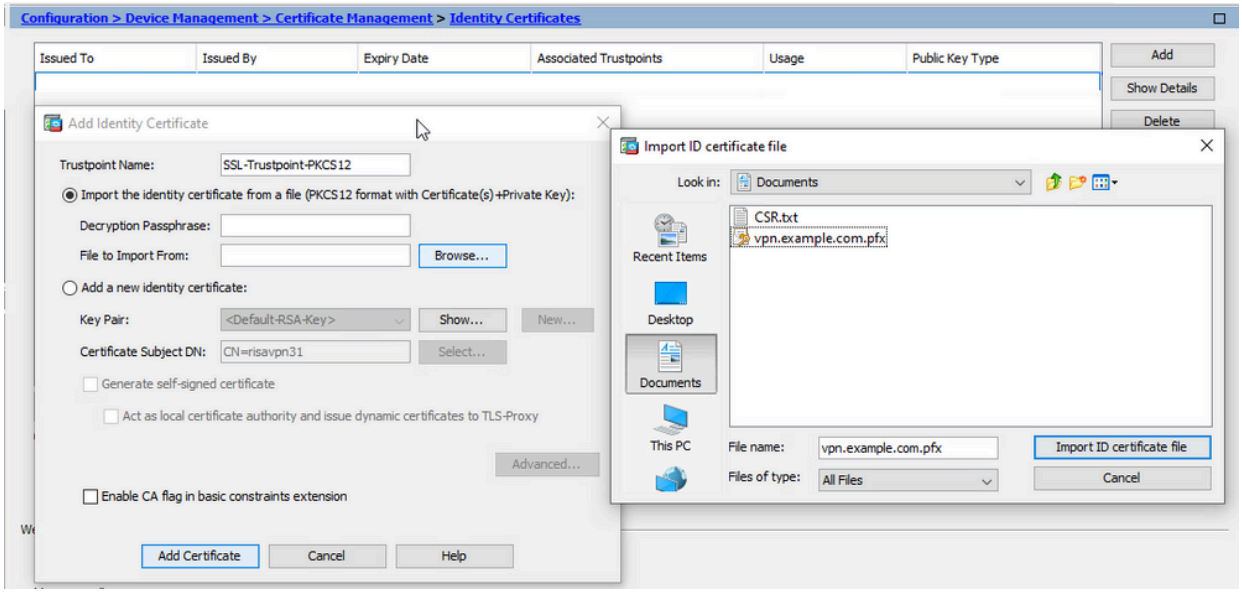
a. Passare a Configurazione > Gestione dispositivi > Gestione certificati e scegliere Certificati identità.

b. Fare clic su Add.

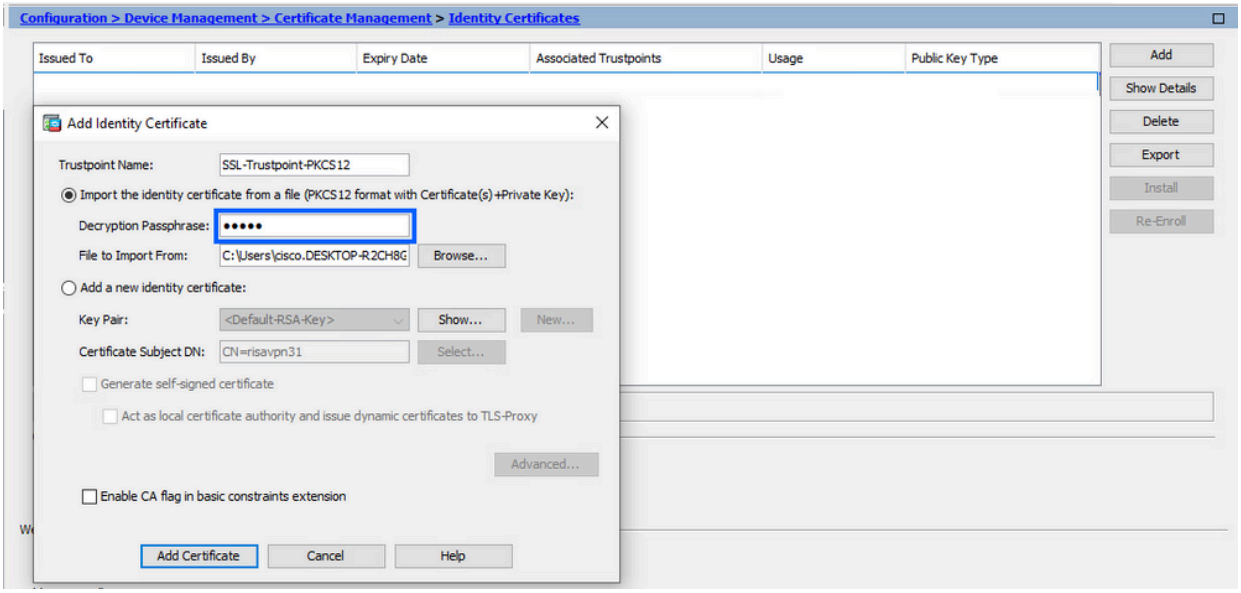
c. Specificare un nuovo nome per il punto di trust.



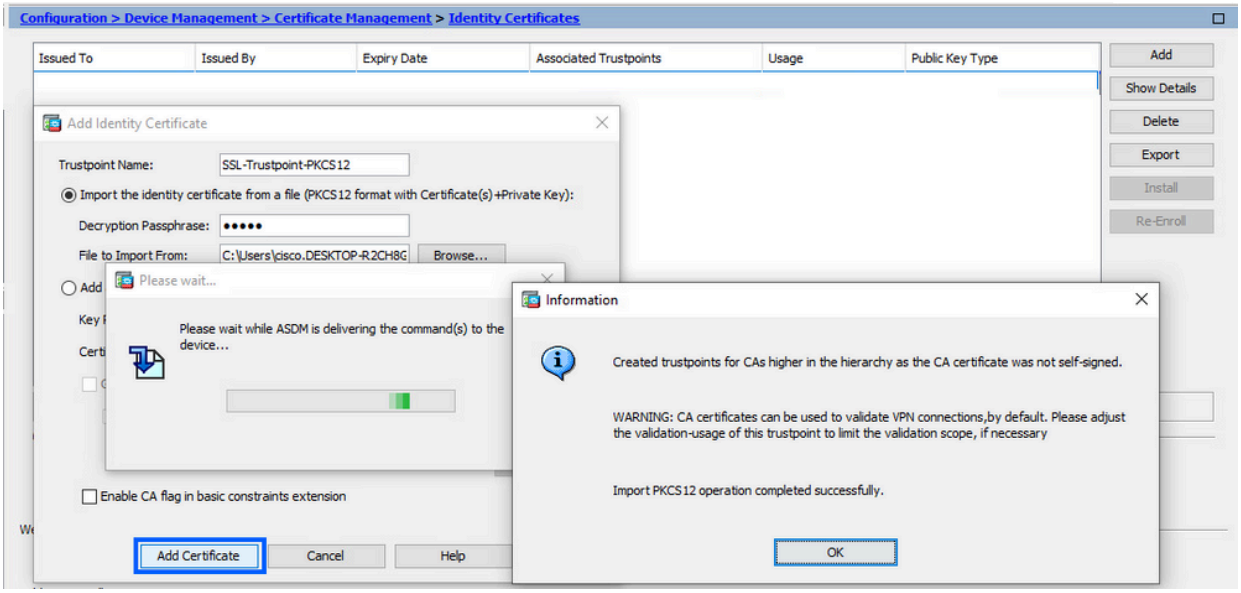
d. Fare clic sul pulsante di opzione Importa il certificato di identità da un file.



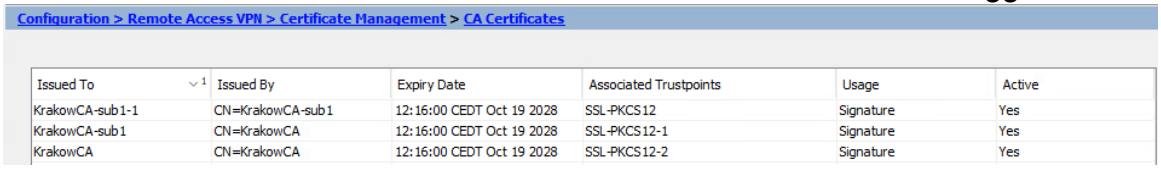
e. Immettere la passphrase utilizzata per creare il file PKCS12.



f. Fare clic su Aggiungi certificato.



Nota: quando si importa una catena di certificati PKCS12 con CA, ASDM crea automaticamente i trust CA a monte con nomi con suffisso -number aggiunto.



Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active
KrakowCA-sub1-1	CN=KrakowCA-sub1	12:16:00 CEDT Oct 19 2028	SSL-PKCS12	Signature	Yes
KrakowCA-sub1	CN=KrakowCA	12:16:00 CEDT Oct 19 2028	SSL-PKCS12-1	Signature	Yes
KrakowCA	CN=KrakowCA	12:16:00 CEDT Oct 19 2028	SSL-PKCS12-2	Signature	Yes

2. Associare il nuovo certificato all'interfaccia con ASDM

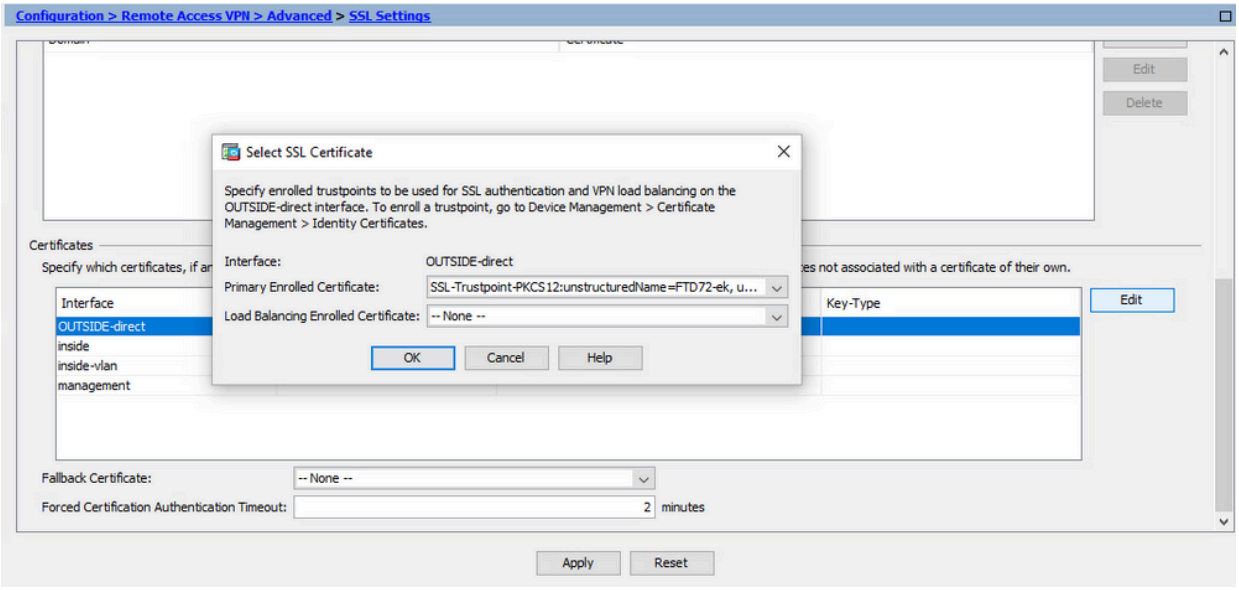
È necessario configurare l'ASA in modo che usi il nuovo certificato di identità per le sessioni WebVPN che terminano sull'interfaccia specificata.

a. Selezionare Configurazione > VPN ad accesso remoto > Avanzate > Impostazioni SSL.

b. In Certificati scegliere l'interfaccia utilizzata per terminare le sessioni WebVPN. nell'esempio viene usata l'interfaccia esterna.

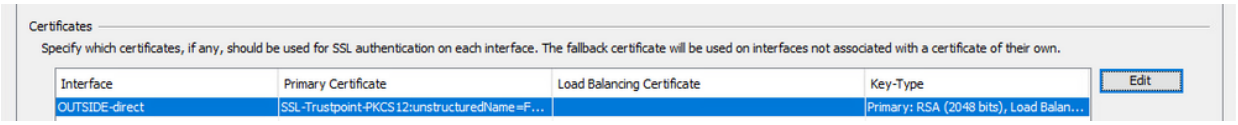
Fare clic su Modifica.

c. Nell'elenco a discesa Certificato scegliere il certificato appena installato.



d. Fare clic su OK.

e. Fare clic su Apply (Applica).



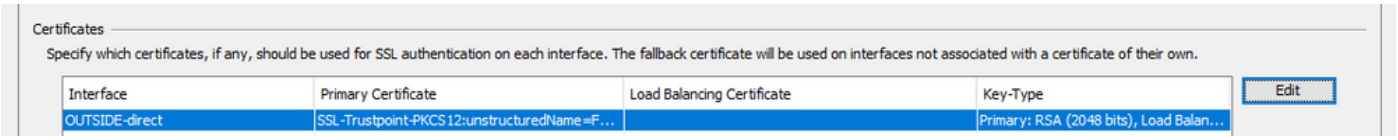
A questo punto il nuovo certificato di identità è in uso.

Verifica

Utilizzare questa procedura per verificare la corretta installazione del certificato del fornitore di terze parti e utilizzarlo per le connessioni VPN SSL.

Visualizza certificati installati tramite ASDM

1. Passare a Configurazione > VPN ad accesso remoto > Gestione certificati e scegliere Certificati di identità.
2. È possibile visualizzare il certificato di identità rilasciato dal fornitore di terze parti.



Risoluzione dei problemi

Questo comando debug deve essere raccolto nella CLI in caso di errore durante l'installazione di un certificato SSL.

- debug crypto ca 14

Domande frequenti

D. Che cos'è un PKCS12?
A.In crittografia, PKCS12 definisce un formato di file di archivio creato per archiviare molti oggetti di crittografia come un unico file. Viene in genere utilizzato per includere una chiave privata nel relativo certificato X.509 o per includere tutti i membri di una catena di attendibilità.

D. Che cos'è un CSR?
A. Nei sistemi con infrastruttura a chiave pubblica (PKI), una richiesta di firma del certificato (anche CSR o richiesta di certificazione) è un messaggio inviato da un richiedente a un'autorità di registrazione dell'infrastruttura a chiave pubblica per richiedere un certificato di identità digitale. In genere contiene la chiave pubblica per la quale è possibile rilasciare il certificato, le informazioni utilizzate per identificare il certificato firmato (ad esempio un nome di dominio in Oggetto) e la protezione dell'integrità (ad esempio, una firma digitale).

D. Dov'è la password di PKCS12?
A.Quando i certificati e le coppie di chiavi vengono esportati in un file PKCS12, la password viene specificata nel comando di esportazione. Per importare un file pkcs12, la password deve essere recapitata dal proprietario del server CA o dalla persona che ha esportato il PKCS12 da un altro dispositivo.

D.Qual è la differenza tra la radice e l'identità?
A.Nella crittografia e nella protezione del computer, un certificato radice è un certificato a chiave pubblica che identifica un'Autorità di certificazione (CA) radice. I certificati radice sono autofirmati (ed è possibile che un certificato abbia più percorsi di attendibilità, ad esempio se è stato rilasciato da una radice con firma incrociata) e costituiscono la base di un'infrastruttura a chiave pubblica (PKI) basata su X.509. Un certificato a chiave pubblica, noto anche come certificato digitale o certificato di identità, è un documento elettronico utilizzato per provare la proprietà di una chiave pubblica. Il certificato include informazioni sulla chiave, informazioni sull'identità del proprietario (denominato soggetto) e la firma digitale di un'entità che ha verificato il contenuto del certificato (denominata emittente). Se la firma è valida e il software che esamina il certificato considera attendibile l'emittente, può utilizzare tale chiave per comunicare in modo sicuro con il soggetto del certificato.

D.Ho installato il certificato. Perché non funziona?
R.Ciò può essere dovuto a diversi motivi, ad esempio:

1. Il certificato e il trust point sono configurati, ma non sono stati associati al processo che deve utilizzarli. Ad esempio, il trust point da utilizzare non è associato all'interfaccia esterna che

termina i client Anyconnect.

2. È installato un file PKCS12, ma vengono restituiti errori dovuti alla mancanza del certificato CA intermedio nel file PKCS12. I client in cui il certificato CA intermedio è considerato attendibile, ma il certificato CA radice non è considerato attendibile, non sono in grado di verificare l'intera catena di certificati e segnalare il certificato di identità del server come non attendibile.

3. Un certificato contenente attributi non corretti può causare errori di installazione o errori sul lato client. Alcuni attributi, ad esempio, potrebbero essere codificati utilizzando un formato non corretto. Un altro motivo è che nel certificato di identità manca il nome alternativo del soggetto (SAN) oppure il nome di dominio utilizzato per accedere al server non è presente come SAN.

D. L'installazione di un nuovo certificato richiede una finestra di manutenzione o causa tempi di inattività?
R. L'installazione di un nuovo certificato (identità o CA) non è intrusiva e non deve causare tempi di inattività o richiedere un intervento di manutenzione. L'abilitazione di un nuovo certificato da utilizzare per un servizio esistente è una modifica e potrebbe richiedere una finestra di richiesta di modifica o di manutenzione.

D. È possibile aggiungere o modificare un certificato per disconnettere gli utenti connessi?
A.No, gli utenti attualmente connessi rimangono connessi. Il certificato viene utilizzato al momento della connessione. Una volta riconnessi gli utenti, verrà utilizzato il nuovo certificato.

D.Come creare un CSR con un carattere jolly? O un nome alternativo del soggetto (SAN)?
R.Al momento, l'ASA/FTD non può creare un CSR con caratteri jolly; tuttavia, questa procedura può essere eseguita con OpenSSL. Per generare la chiave CSR e ID, è possibile eseguire i comandi seguenti:

```
openssl genrsa -out id.key 2048

openssl req -out id.csr -key id.key -new
```

Quando un trust point è configurato con l'attributo FQDN (Fully Qualified Domain Name), il CSR creato da ASA/FTD contiene la SAN con tale valore. La CA può aggiungere altri attributi SAN quando firma il CSR oppure è possibile creare il CSR con OpenSSL

Q. La sostituzione del certificato è immediata?

R. Il nuovo certificato di identità del server viene utilizzato solo per le nuove connessioni. Il nuovo certificato è pronto per essere utilizzato subito dopo la modifica, ma viene utilizzato con le nuove connessioni.

D.Come posso verificare se l'installazione ha funzionato?
A.Il comando CLI da verificare: show crypto ca cert <trustpointname>

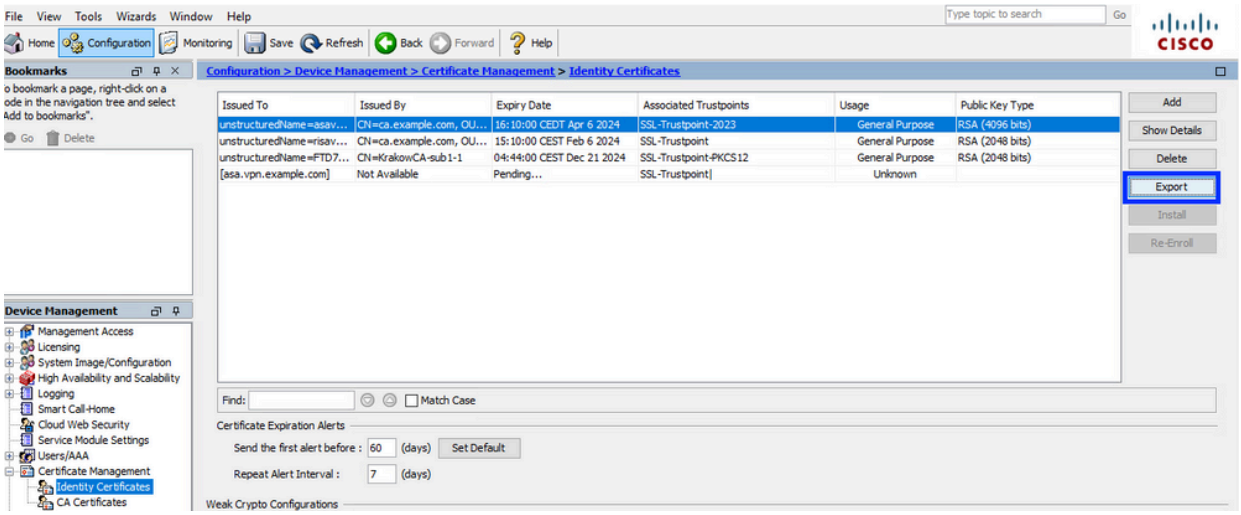
D.Come generare PKCS12 da un certificato di identità, un certificato CA e una chiave privata?
A. PKCS12 può essere creato con OpenSSL, con il comando:

```
openssl pkcs12 -export -out p12.pfx -inkey id.key -in id.crt -certfile ca.crt
```

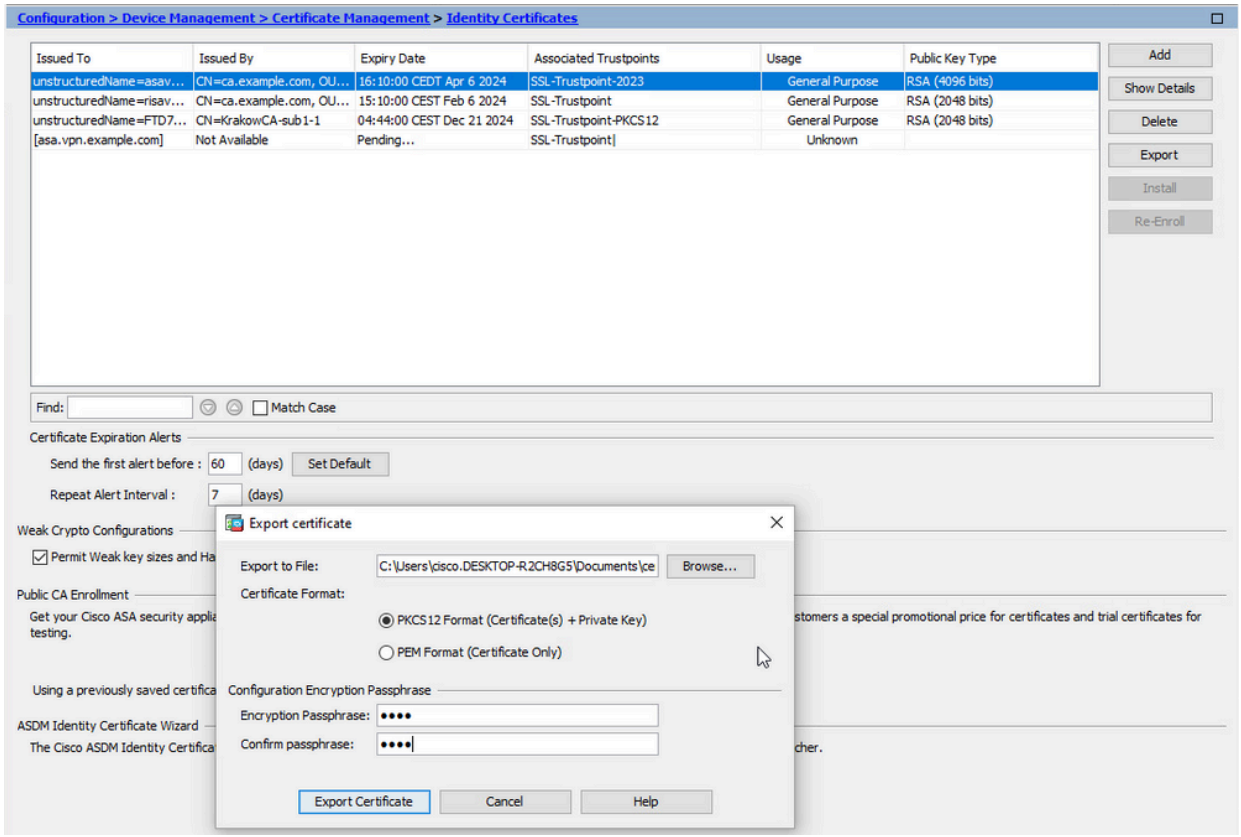
D. Come esportare un certificato per installarlo in una nuova appliance ASA?
R.

- Con CLI: utilizzare il comando crypto ca export <nometrust> pkcs12 <password>
- Con ASDM:

a. Passare a Configurazione > Gestione dispositivi > Gestione certificati > Certificati di identità e scegliere il certificato di identità. Fare clic su Esporta.



b. Scegliere dove esportare il file, specificare la password di esportazione e fare clic su Esporta certificato.



Il certificato esportato può trovarsi sul disco del computer. Prendere nota della

passphrase in un luogo sicuro, il file è inutile senza di essa.

D.Se vengono utilizzate chiavi ECDSA, il processo di generazione del certificato SSL è diverso?
A.L'unica differenza di configurazione è rappresentata dalla fase di generazione della coppia di chiavi, in cui è possibile generare una coppia di chiavi ECDSA anziché una coppia di chiavi RSA. Il resto dei gradini rimane lo stesso.

D.È sempre necessario generare una nuova coppia di chiavi?
A. Il passo di generazione della coppia di chiavi è facoltativo. È possibile utilizzare una coppia di chiavi esistente oppure, nel caso di PKCS12, tale coppia viene importata con il certificato. Vedere la sezione Selezionare il nome della coppia di chiavi per il rispettivo tipo di registrazione/ri-registrazione.

D.È sicuro generare una nuova coppia di chiavi per un nuovo certificato di identità?
A. Il processo è sicuro se si utilizza un nuovo nome di coppia di chiavi. In questo caso, le vecchie coppie di chiavi non vengono modificate.

D.È necessario generare nuovamente la chiave quando si sostituisce un firewall (come RMA)?
A.Il nuovo firewall non dispone per impostazione predefinita di una coppia di chiavi sul firewall precedente.
Il backup della configurazione corrente non contiene le coppie di chiavi.
Il backup completo eseguito con ASDM può contenere le coppie di chiavi.
È possibile esportare i certificati di identità da un'appliance ASA con ASDM o CLI prima che si verifichi un errore.
In caso di coppia di failover, i certificati e le coppie di chiavi vengono sincronizzati su un'unità in standby con il comando write standby. In caso di sostituzione di un nodo di coppia di failover, è sufficiente configurare il failover di base ed eseguire il push della configurazione sul nuovo dispositivo.
Se una coppia di chiavi viene persa con il dispositivo e non è disponibile alcun backup, è necessario firmare un nuovo certificato con la coppia di chiavi presente nel nuovo dispositivo.

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).