Genera e aggiungi i certificati necessari per l'installazione di Secure Endpoint Private Cloud 3.x e versioni successive

Sommario

Introduzione

In questo documento viene descritto il processo di generazione dei certificati da caricare con ogni nuova installazione di Secure Console Private Cloud o di rinnovo dei Servizi certificati installati.

Prerequisiti

Requisiti

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

hardware:

- Windows Server 2008
- CentOS 7/8
- Secure Console Virtual Private Cloud 3.0.2 (In Avanti)
- OpenSSL 1.1.1

Componenti usati

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Windows Server 2008 (in avanti)
- Installazione Secure Console Private Cloud
- Infrastruttura a chiave pubblica
- OpenSSL
- CLI Linux

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

Con l'introduzione di Secure Console Private Cloud 3.X, i nomi host e le coppie certificato/chiave sono necessari per tutti i seguenti servizi:

- Portale di amministrazione
- Autenticazione (novità in Private Cloud 3.X)
- Console protetta
- Server di disposizione
- Server di disposizione - Protocollo esteso
- Servizio di aggiornamento della disposizione
- Firepower Management Center

In questo documento viene illustrato come generare e caricare rapidamente i certificati richiesti. È possibile modificare ogni parametro, incluso l'algoritmo di hashing, le dimensioni della chiave e altri, in base ai criteri dell'organizzazione e il meccanismo di generazione dei certificati potrebbe non corrispondere a quanto descritto in questa sezione.

> **Avviso**: la procedura indicata di seguito può variare in base alla configurazione del server CA. È previsto che il provisioning del server CA prescelto sia già stato eseguito e che la configurazione dello stesso sia stata completata. La nota tecnica seguente descrive solo un esempio di generazione dei certificati e Cisco TAC non è coinvolto nella risoluzione dei problemi relativi alla generazione dei certificati e/o ai problemi dei server CA di alcun tipo.

Creazione certificato

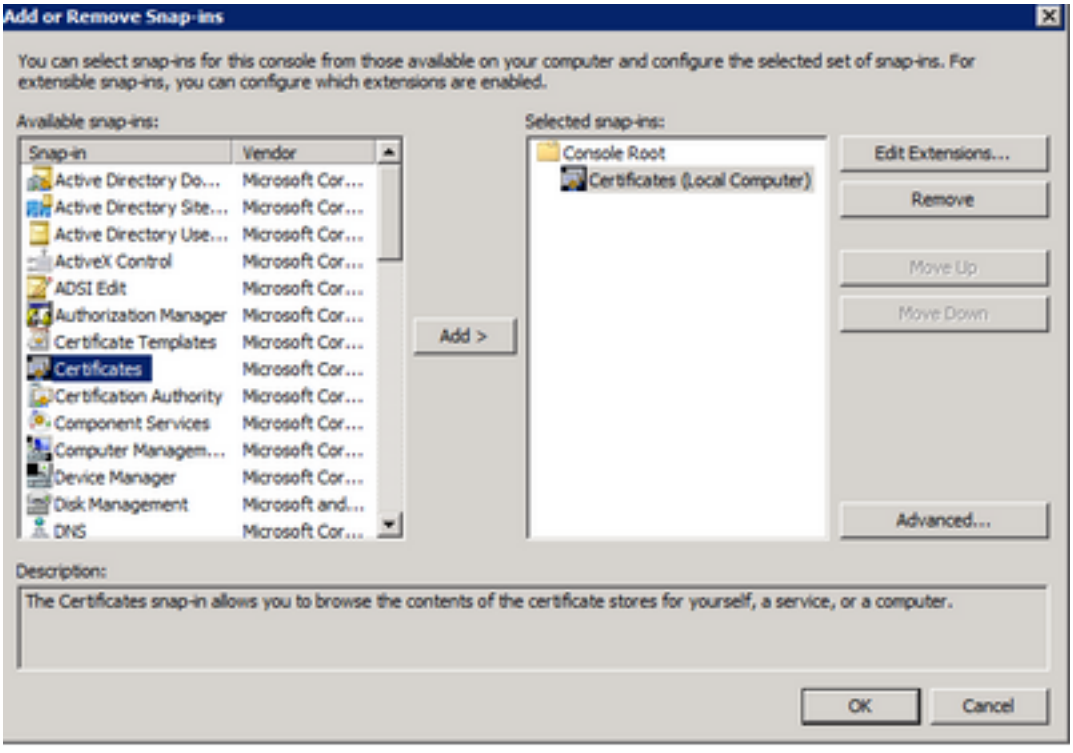
Genera certificati sul server di Windows

Verificare che i ruoli seguenti siano installati e configurati nel server Windows.

- Servizi certificati Active Directory
- Autorità di certificazione
- Registrazione Web Autorità di certificazione
- Risponditore online
- Servizio Web di registrazione certificati
- Servizio Web di informazioni sulle registrazioni di certificati
- Servizi di dominio Active Directory
- Server DNS
- Server Web (IIS)

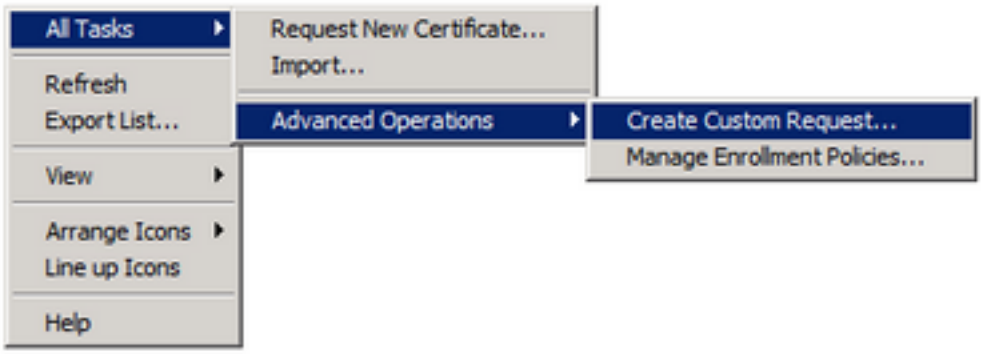
Genera una richiesta di firma del certificato (CSR)

Passaggio 1. Passare alla console MMC e aggiungere lo snap-in Certificati per l'account computer, come illustrato nell'immagine.

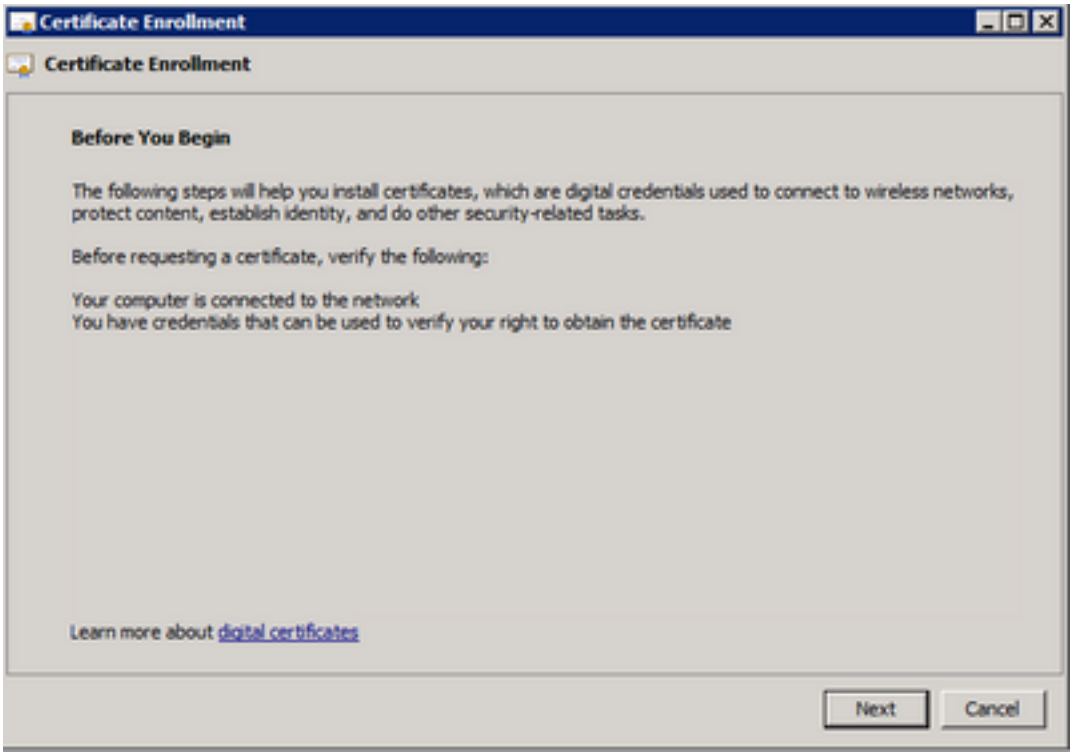


Passaggio 2. Espandere **Certificati (Computer locale) > Personale > Certificati**.

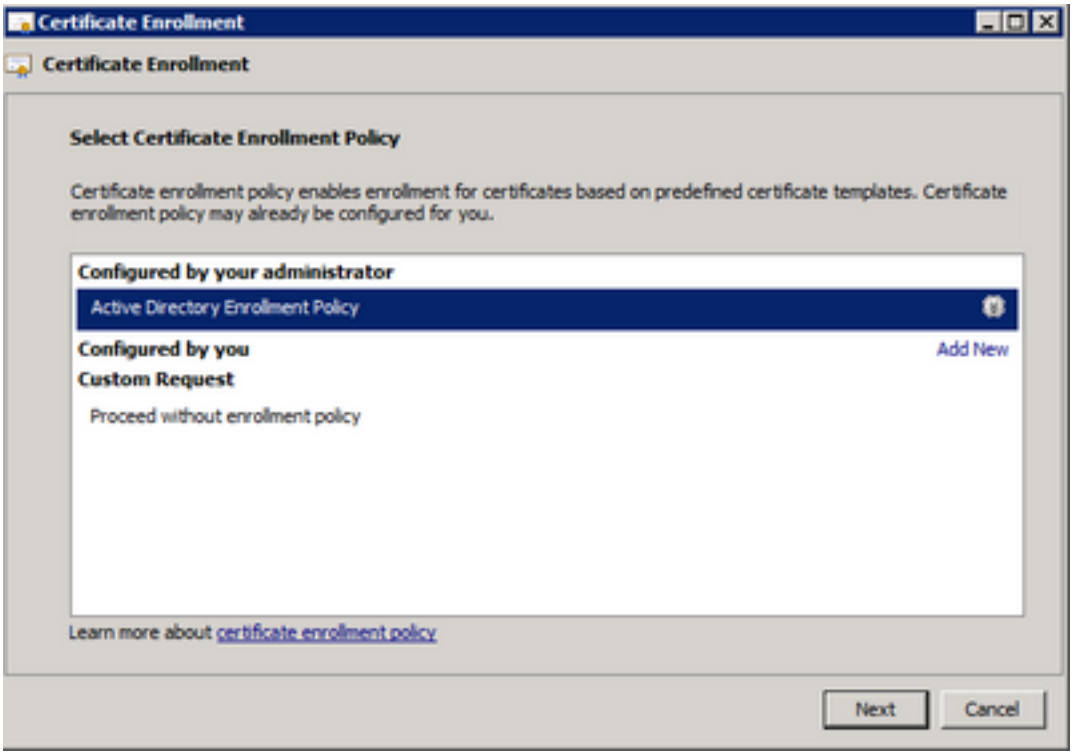
Passaggio 3. Fare clic con il pulsante destro del mouse sullo spazio vuoto e selezionare **All Tasks > Advanced Operations > Create Custom Request.**



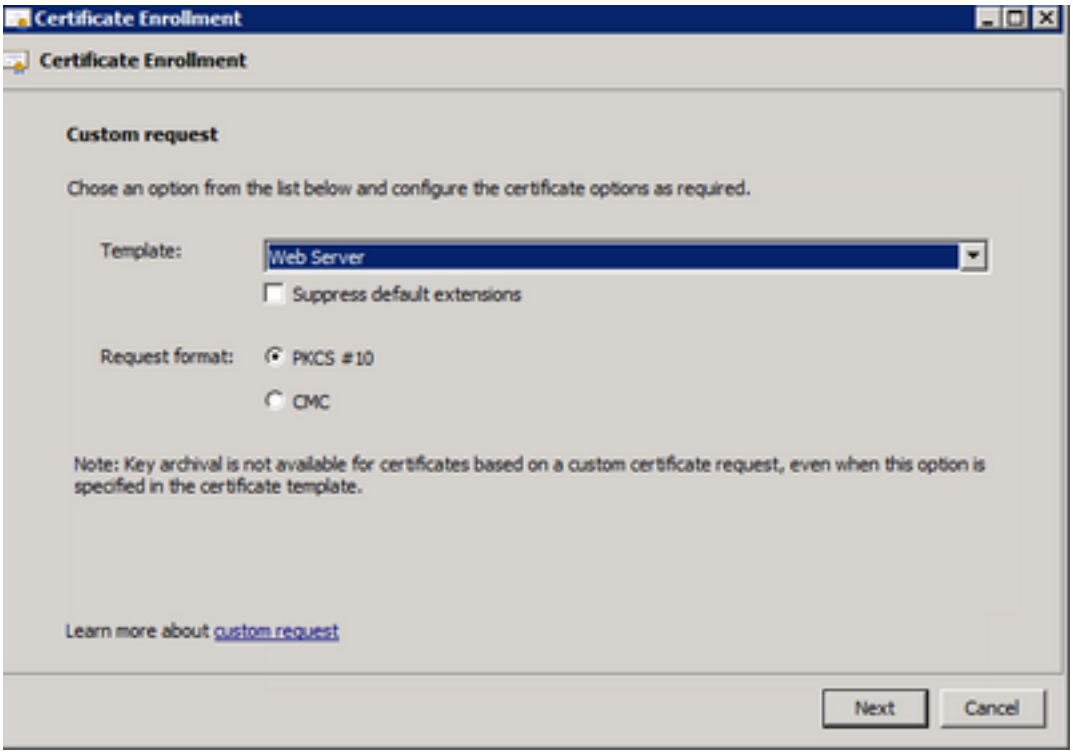
Passaggio 4. Selezionare **Successivo** nella finestra Iscrizione.



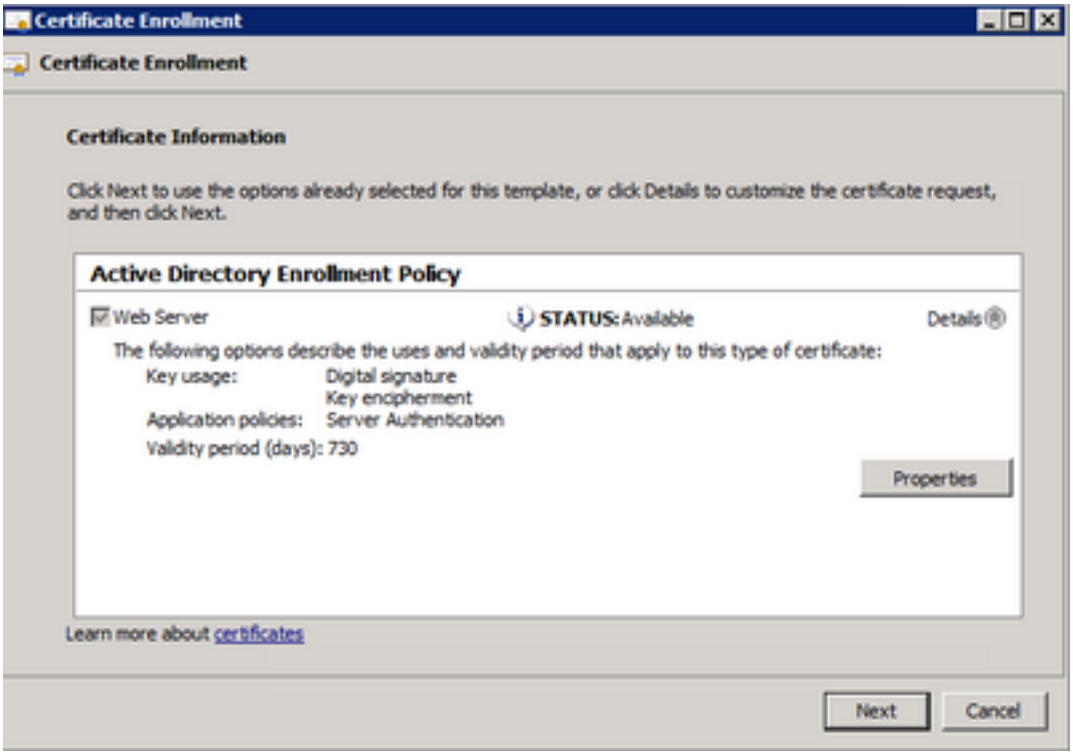
Passaggio 5. Selezionare il criterio di registrazione dei certificati e scegliere **Avanti**.



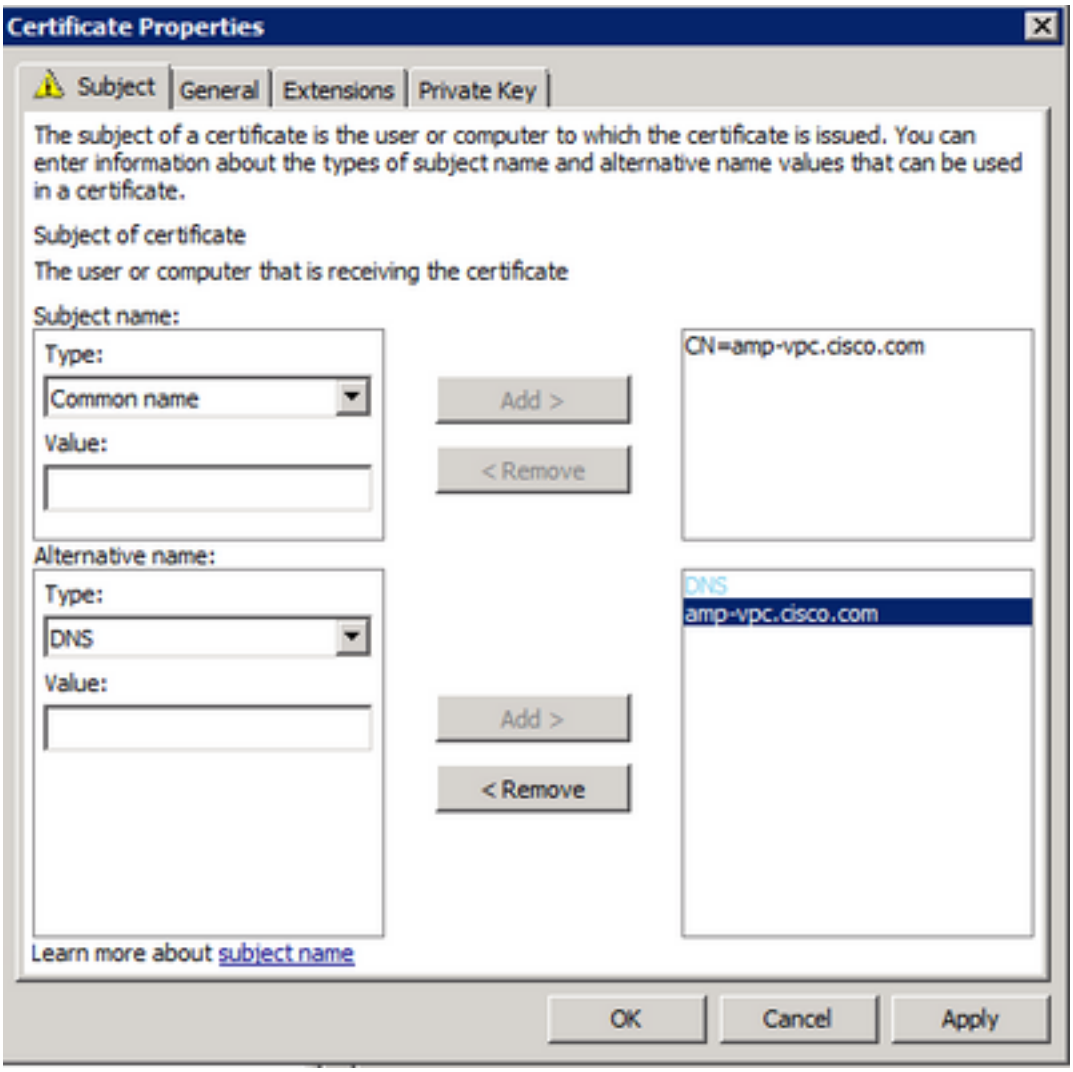
Passaggio 6. Scegliere il modello come **server Web** e selezionare **Avanti**.



Passaggio 7. Se il modello "Server Web" è stato configurato correttamente ed è disponibile per la registrazione, verrà visualizzato lo stato Disponibile. Selezionare **Dettagli** per espandere Proprietà.

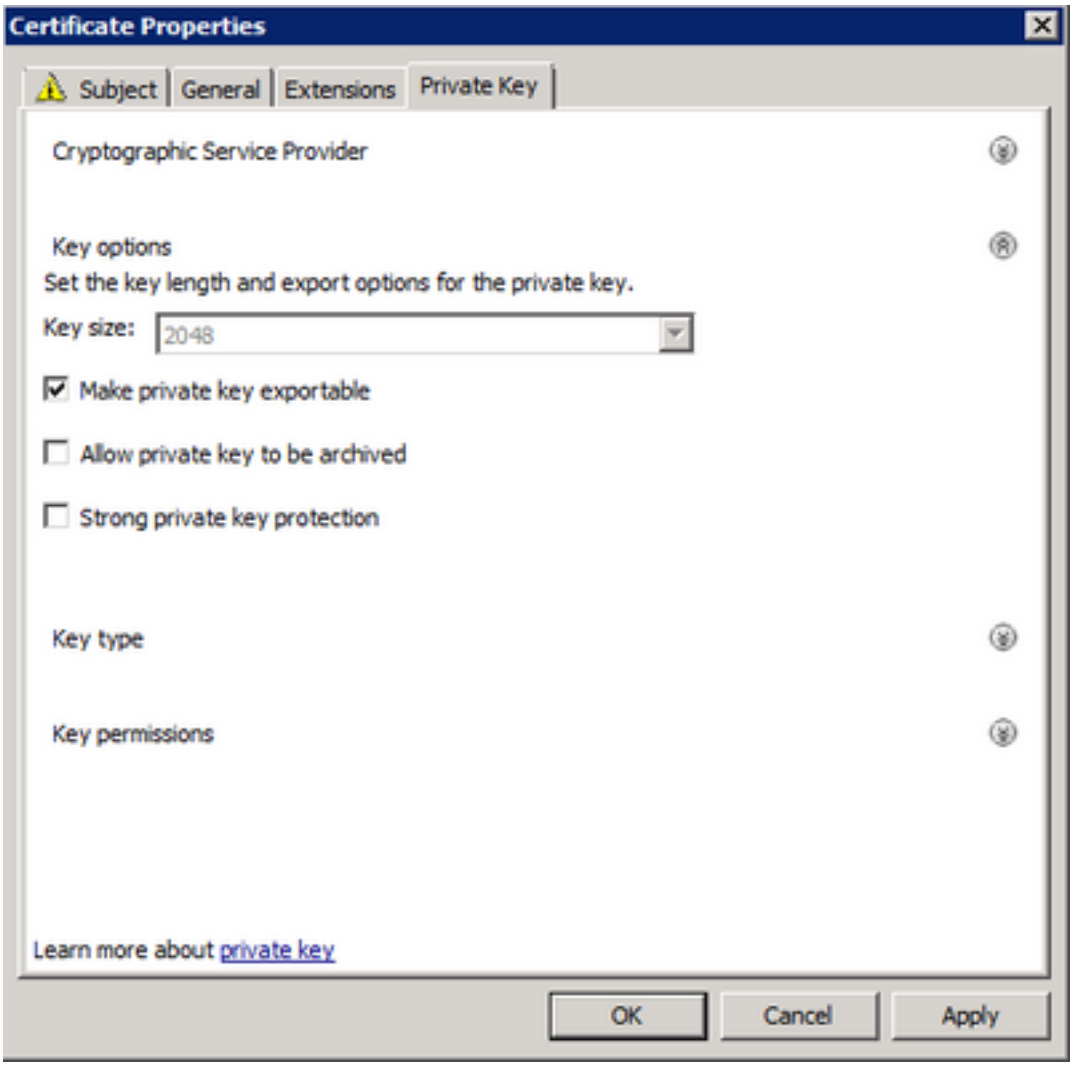


Passaggio 8. Aggiungere almeno gli attributi CN e DNS. Gli altri attributi possono essere aggiunti in base ai requisiti di sicurezza.



Passaggio 9. Facoltativamente, assegnare un Nome descrittivo nella scheda **Generale**.

Passaggio 10. Fare clic sulla scheda **Private Key** e verificare che sia attivata l'opzione **Make private key exportable** nella sezione **Key Options**.

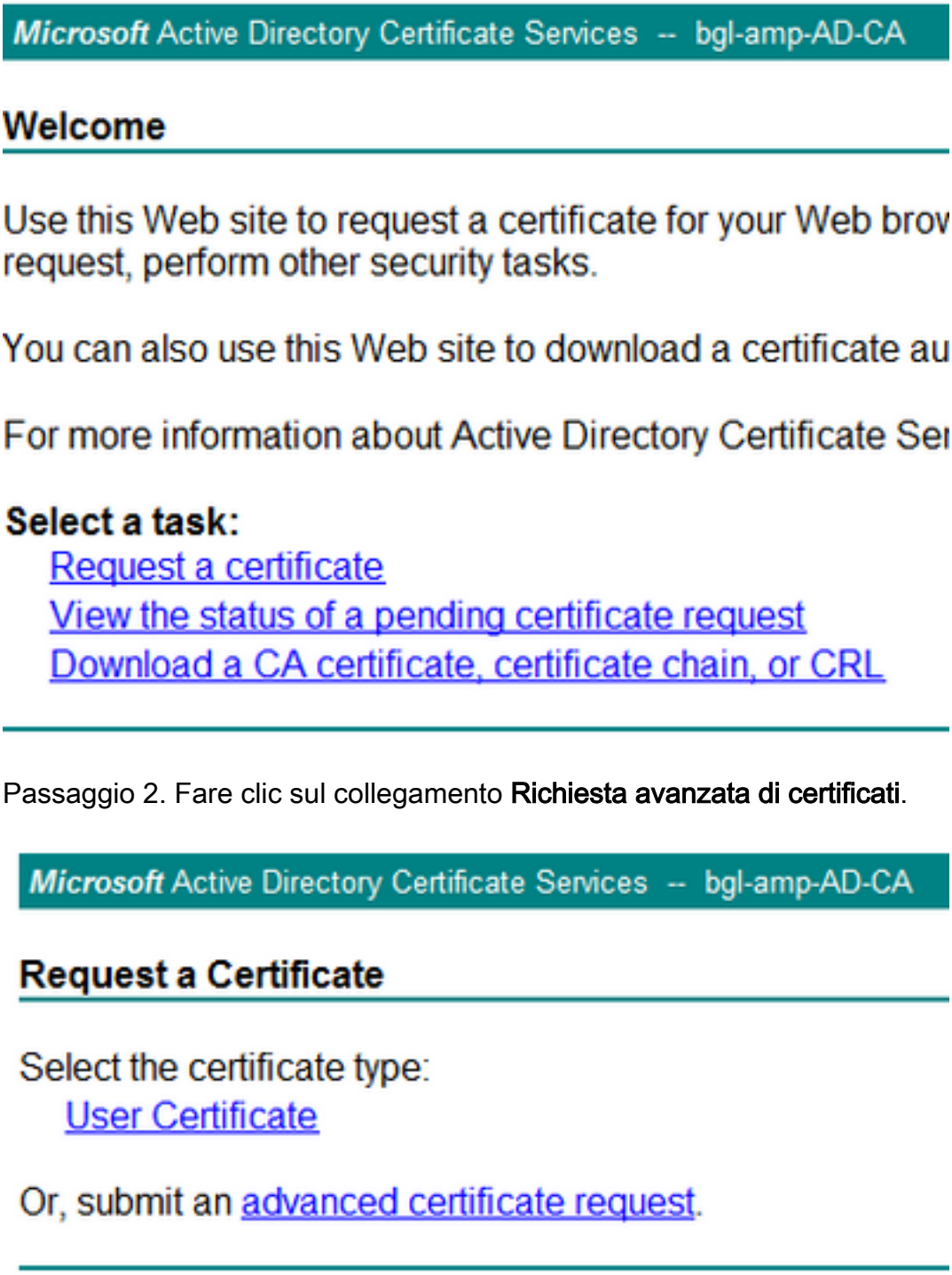


Passaggio 11. Infine, selezionare **OK**. Verrà visualizzata la finestra di dialogo Registrazione certificato in cui è possibile selezionare **Avanti**.

Passaggio 12. Individuare il percorso in cui salvare il file con estensione req inviato al server CA per la firma.

Invio del CSR alla CA e generazione del certificato

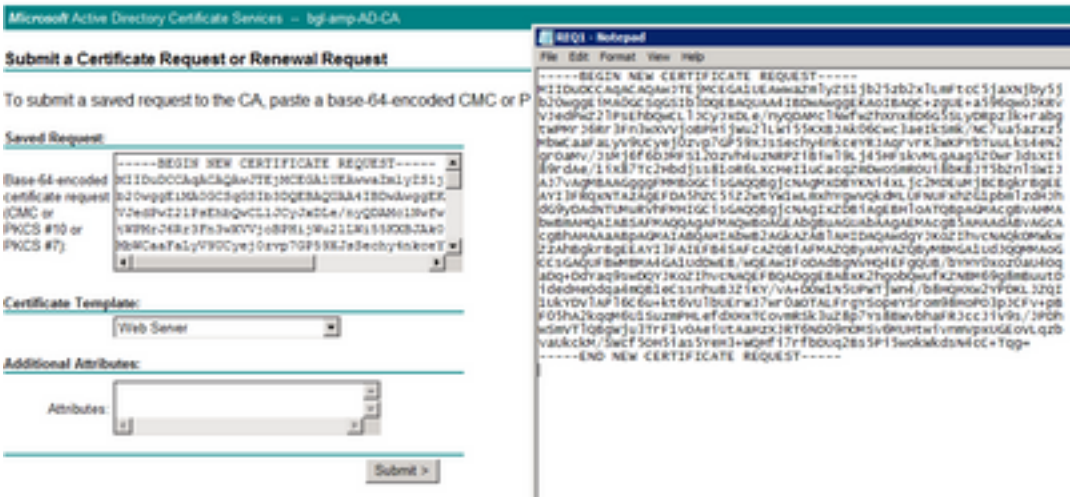
Passaggio 1. Passare alla pagina Web di Servizi certificati MS AD come indicato di seguito e selezionare **Richiedi certificato**.



Passaggio 2. Fare clic sul collegamento **Richiesta avanzata di certificati**.

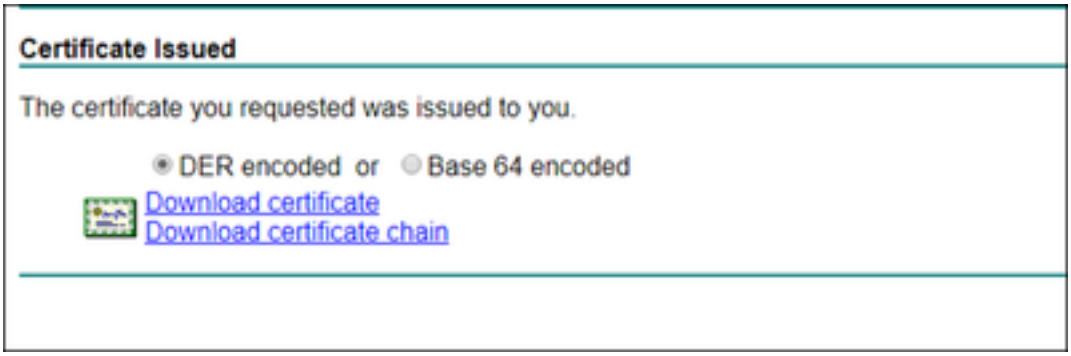
Passaggio 3. Selezionare **Invia una richiesta di certificato utilizzando un file CMC o PKCS #10 con codifica Base 64 oppure inviare una richiesta di rinnovo utilizzando un file PKCS #7 con codifica Base 64**.

Passaggio 4. Aprire il contenuto del file .req (CSR) salvato in precedenza tramite il Blocco note. Copiare il contenuto e incollarlo qui. Verificare che il modello di certificato sia selezionato come **server Web**



Passaggio 5. Infine, selezionare **Invia**.

Passaggio 6. A questo punto, è necessario essere in grado di **scaricare** il certificato, come mostrato nell'immagine.



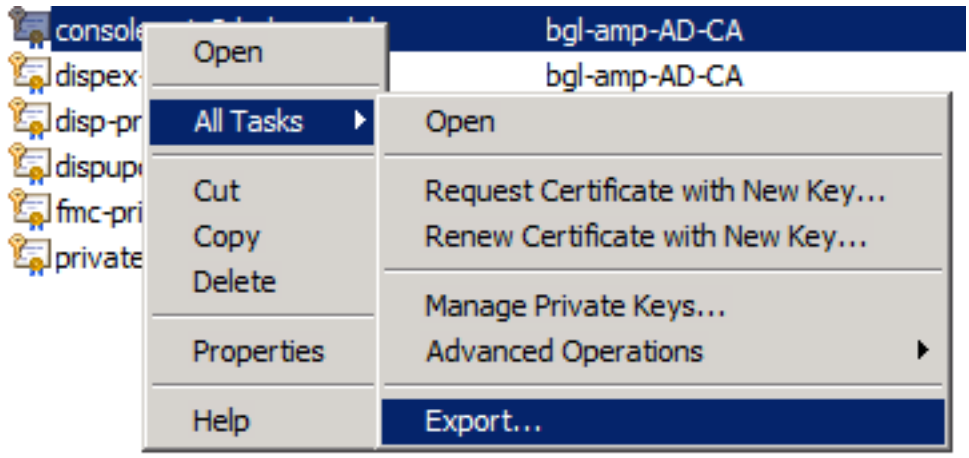
Esportazione della chiave privata e conversione in formato PEM

Passaggio 1. Installare il certificato nell'archivio certificati aprendo il file con estensione cer e selezionando **Installa certificato**.

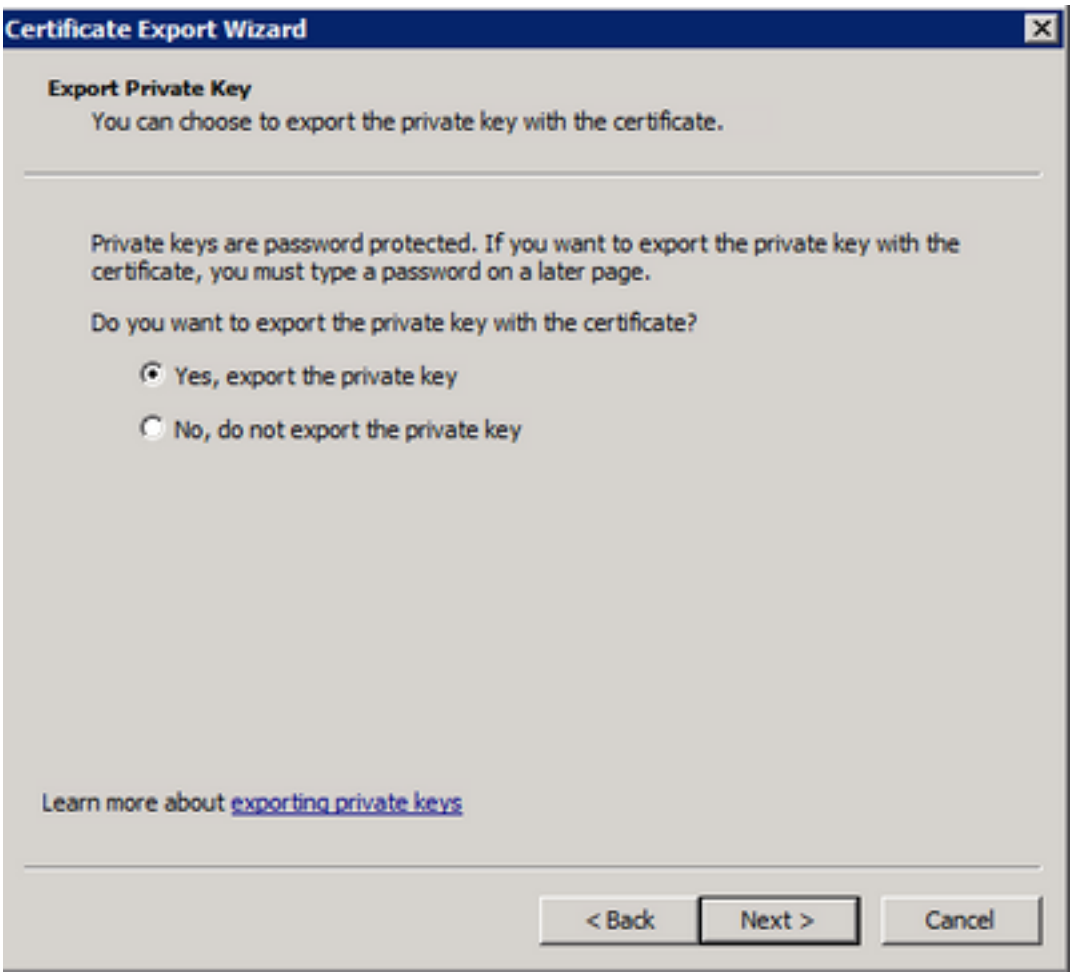
Passaggio 2. Passare allo snap-in di MMC selezionato in precedenza.

Passaggio 3. Passare all'archivio in cui è stato installato il certificato.

Passaggio 4. Fare clic con il pulsante destro del mouse sul certificato corretto, selezionare **Tutte le attività > Esporta**.



Passaggio 5. Nell'Esportazione guidata certificati confermare l'esportazione della chiave privata, come illustrato nell'immagine.



Passaggio 6. Immettere una password e selezionare **Avanti** per salvare la chiave privata sul disco.

Passaggio 7. In questo modo la chiave privata viene salvata in formato PFX, tuttavia è necessario convertirla in formato PEM per utilizzarla con Secure Endpoint Private Cloud.

Passaggio 8. Installare le librerie OpenSSL.

Passaggio 9. Aprire una finestra del prompt dei comandi e passare alla directory in cui è stato installato OpenSSL.

Passaggio 10. Eseguire il comando seguente per estrarre la chiave privata e salvarla in un nuovo file: (Se il file PFX non si trova nello stesso percorso in cui è memorizzata la libreria OpenSSL, è necessario specificare il percorso esatto insieme al nome del file)

```
openssl pkcs12 -in yourpfxfile.pfx -nocerts -out privatekey.pem -nodes
```

Passaggio 11. Eseguire il comando seguente per estrarre anche il certificato pubblico e salvarlo in un nuovo file:

```
openssl pkcs12 -in yourpfxfile.pfx -nokeys -out publiccert.pem -nodes
```

Genera certificato su server Linux (controllo SSL rigoroso DISABILITATO)

> **Nota**: Strict TLS Check verifica che il certificato soddisfi i requisiti TLS di Apple. Per ulteriori informazioni, consultare la Guida dell'amministratore.

Verificare che nel server Linux che si sta tentando di generare i certificati richiesti siano installate le librerie OpenSSL 1.1.1. Verificare se questa e la procedura riportata di seguito possono variare rispetto alla distribuzione Linux in esecuzione. Questa parte è stata documentata, come avviene su un server CentOS 8.4.

Genera RootCA autofirmata

Passaggio 1. Generare la chiave privata per il certificato CA radice.

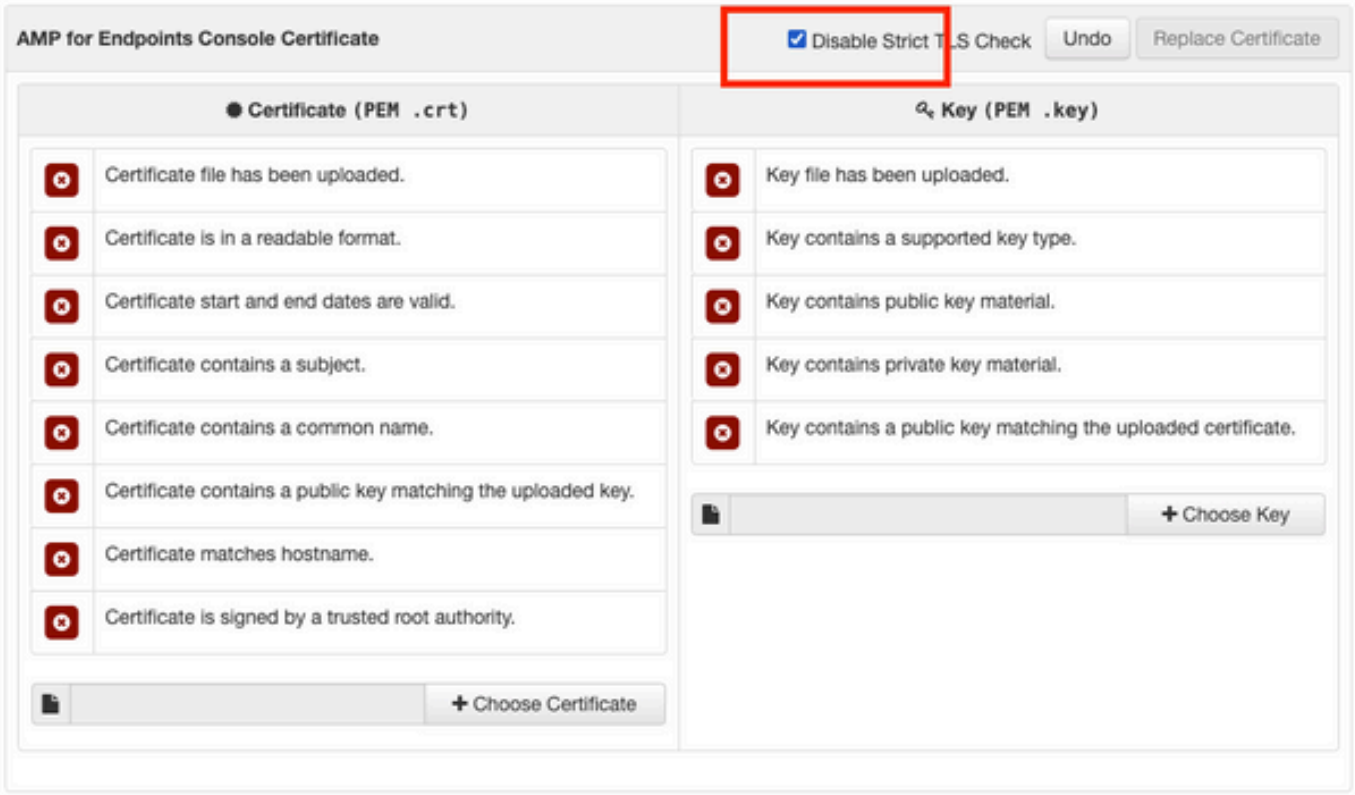
```
openssl genrsa -out
```

Passaggio 2. Generare il certificato CA.

```
openssl req \
-subj '/CN=
-addext "extendedKeyUsage = serverAuth, clientAuth" \
-outform pem -out
-key
-days "1000"
```

Genera un certificato per ogni servizio

Creare il certificato per l'autenticazione, la console, l'eliminazione, l'eliminazione estesa, il server di aggiornamento, il servizio Firepower Management Center (FMC) in base alla voce relativa al nome DNS. È necessario ripetere il processo di generazione del certificato seguente per ogni servizio (autenticazione, console e così via).



Genera chiave privata

```
openssl genrsa -out
```

Sostituire <YourServiceName.key> con il nuovo nome del file KEY da creare come Auth-Cert.key

Genera CSR

```
openssl req -new \
-subj '/CN=
-key
```

Sostituire il <YourServiceName.key> con il file KEY del certificato corrente o nuovo, ad esempio Auth-Cert.key

Sostituire <YourServiceName.csr> con il nome del file CSR da creare, ad esempio Auth-Cert.crt

Genera certificato

```
openssl x509 -req \
-in
-CAkey
-days 397 -sha256
```

Sostituire <YourServiceName.csr> con il CSR del certificato effettivo o nuovo, ad esempio Auth-Cert.csr

Sostituire <YourRootCAName.pem> con il nome file PEM effettivo (o nuovo) come RootCAName.pem

Sostituire <YourServiceName.key> con il file KEY del certificato corrente o nuovo, ad esempio Auth-Cert.key

Sostituire <YourServiceName.crt> con il nome del file da creare, ad esempio Auth-Cert.crt

Genera certificato su server Linux (controllo SSL rigoroso ABILITATO)

> **Nota**: Strict TLS Check verifica che il certificato soddisfi i requisiti TLS di Apple. Per ulteriori informazioni, consultare la Guida dell'amministratore.

Genera RootCA autofirmata

Passaggio 1. Generare la chiave privata per il certificato CA radice.

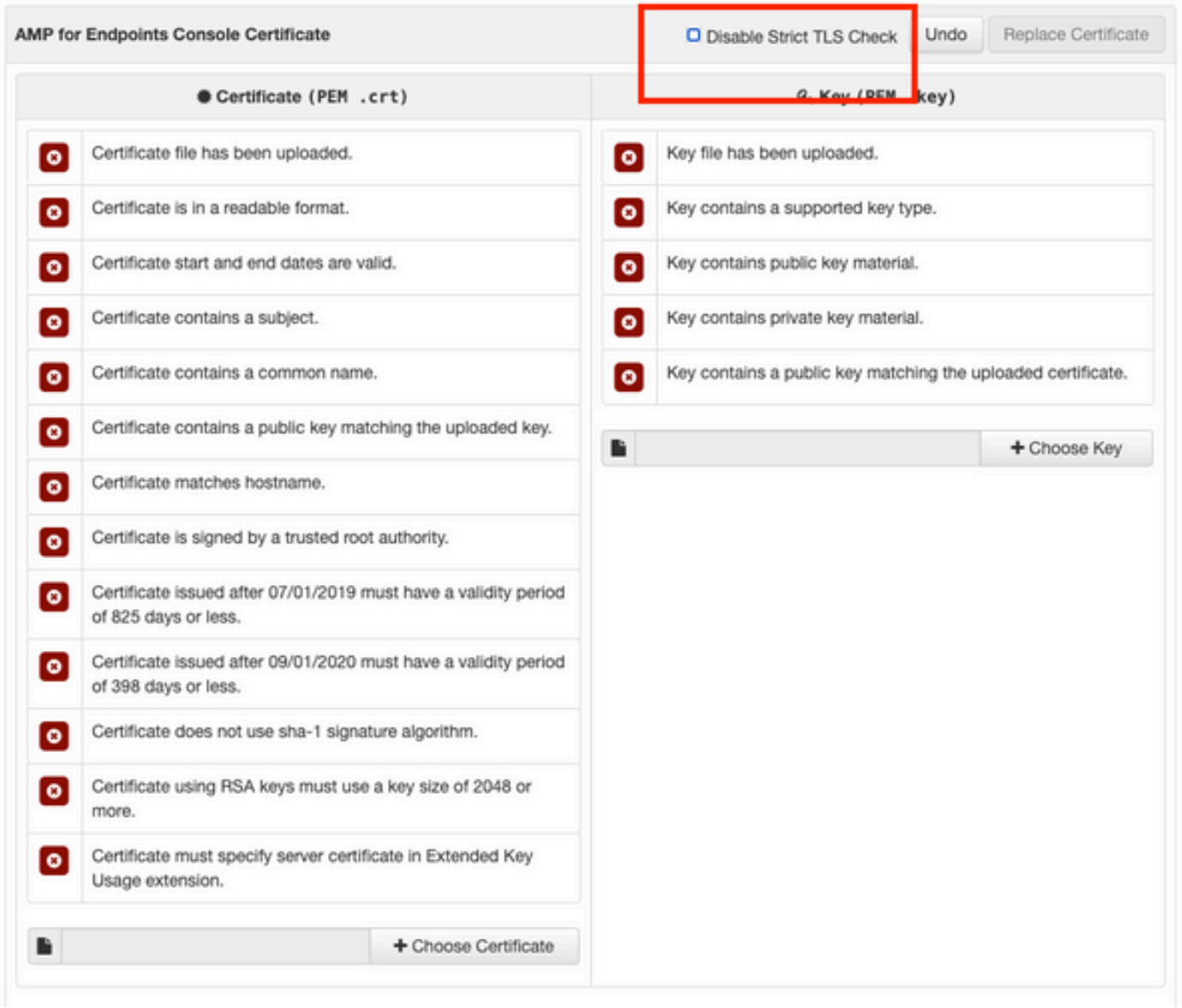
```
openssl genrsa -out
```

Passaggio 2. Generare il certificato CA.

```
openssl req \
-subj '/CN=
-outform pem -out
-key
-days "1000"
```

Genera un certificato per ogni servizio

Creare il certificato per l'autenticazione, la console, l'eliminazione, l'eliminazione estesa, il server di aggiornamento, il servizio Firepower Management Center (FMC) in base alla voce relativa al nome DNS. È necessario ripetere il processo di generazione del certificato seguente per ogni servizio (autenticazione, console e così via).



Creare un file di configurazione delle estensioni e salvarlo (extensions.cnf)

```
[v3_ca]
basicConstraints = CA:FALSE
keyUsage = critical, digitalSignature, keyEncipherment
extendedKeyUsage = critical, serverAuth, clientAuth
```

Genera chiave privata

```
openssl genrsa -out
```

Sostituire <YourServiceName.key> con un nuovo nome file KEY da creare come Auth-Cert.key

Genera CSR

```
openssl req -new \
-key
-subj '/CN=
-out
```

Sostituire il <YourServiceName.key> con la chiave del certificato corrente o nuova, ad esempio

Auth-Cert.key

Sostituire <YourServiceName.csr> con il CSR del certificato corrente o nuovo, ad esempio Auth-Cert.csr

Genera certificato

```
openssl x509 -req -in
-CA
-CAcreateserial -out
-extensions v3_ca -extfile extensions.cnf \
-days 397 -sha256
```

Sostituire <YourServiceName.csr> con il CSR del certificato corrente o nuovo, ad esempio Auth-Cert.csr

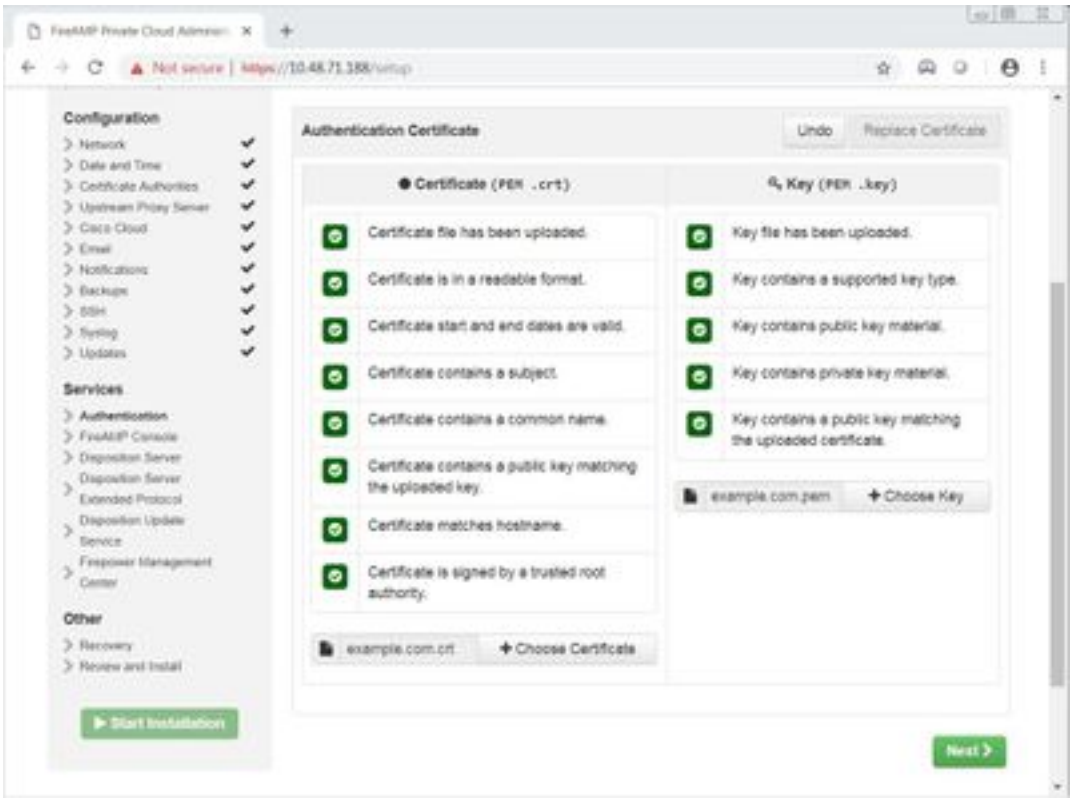
Sostituire <YourRootCAName.pem> con il nome file PEM corrente (o nuovo) come RootCAName.pem

Sostituire <YourServiceName.key> con il file KEY del certificato corrente o nuovo, ad esempio Auth-Cert.key

Sostituire <YourServiceName.crt> con il nome del file da creare, ad esempio Auth-Cert.crt

Aggiunta dei certificati al cloud privato della console protetta

Passaggio 1. Una volta generati i certificati utilizzando uno dei metodi descritti in precedenza, caricare il certificato corrispondente per ogni servizio. Se sono stati generati correttamente, tutti i segni di spunta sono attivati come mostrato nell'immagine qui.



Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

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).