

# Installa e rinnova certificati su FTD Gestito da FMC

## Sommario

- [Introduzione](#)
- [Prerequisiti](#)
- [Requisiti](#)
- [Componenti usati](#)
- [Introduzione](#)
- [Configurazione](#)
- [Installazione certificato](#)
- [Iscrizione autofirmata](#)
- [Iscrizione manuale](#)
- [Iscrizione PKCS12](#)
- [Rinnovo certificato](#)
- [Rinnovo certificato autofirmato](#)
- [Rinnovo manuale dei certificati](#)
- [Rinnovo PKCS12](#)
- [Creazione di PKCS12 con OpenSSL](#)
- [Verifica](#)
- [Visualizza certificati installati in FMC](#)
- [Visualizza certificati installati nella CLI](#)
- [Risoluzione dei problemi](#)
- [Comandi debug](#)
- [Problemi comuni](#)

## Introduzione

In questo documento viene descritto come installare, considerare attendibili e rinnovare certificati in un FTD gestito da FMC.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- La registrazione manuale dei certificati richiede l'accesso a una CA di terze parti attendibile.
- Esempi di fornitori di CA di terze parti includono, tra gli altri, Entrust, Geotrust, GoDaddy, Thawte e VeriSign.
- Verificare che l'FTD abbia l'ora, la data e il fuso orario corretti. Con l'autenticazione dei certificati, si consiglia di utilizzare un server NTP (Network Time Protocol) per sincronizzare l'ora sull'FTD.

### Componenti usati

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

- FMCv in esecuzione 6.5

- FTDv in esecuzione 6.5
- 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.

## Introduzione

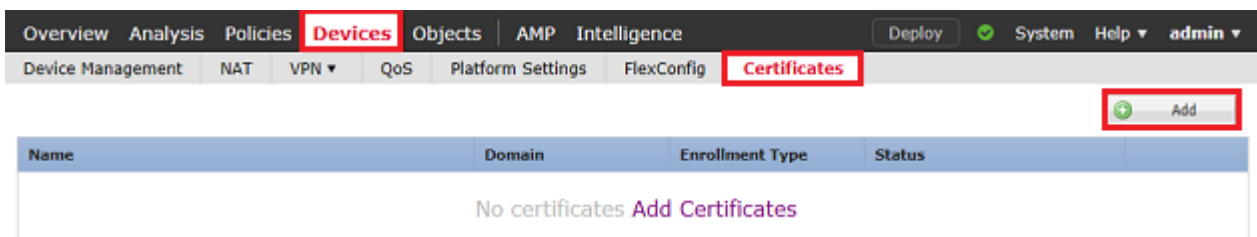
In questo documento viene descritto come installare, considerare attendibili e rinnovare certificati autofirmati e certificati firmati da un'Autorità di certificazione (CA) di terze parti o da una CA interna su un Firepower Threat Defense (FTD) gestito da Firepower Management Center (FMC).

## Configurazione

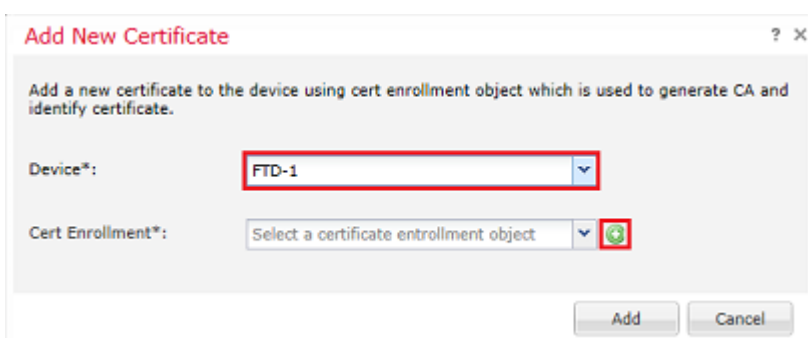
### Installazione certificato

#### Iscrizione autofirmata

1. Passare a **Dispositivi** > **Certificati**, quindi fare clic su **Aggiungi** come mostrato nell'immagine.



2. Selezionare il dispositivo e il certificato viene aggiunto nel menu a discesa **Device\***. Quindi fate clic sul simbolo verde + come mostrato nell'immagine.



3. Specificare un **nome** per il trust point e nella scheda **Informazioni CA** selezionare Tipo di registrazione: **Certificato autofirmato** come mostrato nell'immagine.

**Add Cert Enrollment** ? X

Name\*

Description

**CA Information** Certificate Parameters Key Revocation

Enrollment Type:

⚠ Common Name (CN) is mandatory for self-signed certificate that is used in Remote Access VPN. To configure CN, please navigate to 'Certificate Parameters' tab.

Allow Overrides

Save Cancel

4. Nella scheda **Parametri certificato**, inserire un nome comune per il certificato. Deve corrispondere all'FQDN o all'indirizzo IP del servizio per il quale viene utilizzato il certificato, come mostrato nell'immagine.

**Add Cert Enrollment** ? X

Name\*

Description

**CA Information** **Certificate Parameters** Key Revocation

Include FQDN:

Include Device's IP Address:

Common Name (CN):

Organization Unit (OU):

Organization (O):

Locality (L):

State (ST):

Country Code (C):

Email (E):

Include Device's Serial Number

Allow Overrides

Save Cancel

5. (Facoltativo) Nella scheda **Chiave** è possibile specificare il tipo, il nome e le dimensioni della chiave privata utilizzata per il certificato. Per impostazione predefinita, la chiave utilizza una chiave RSA con il nome **<Default-RSA-Key>** e una dimensione di 2048; tuttavia, si consiglia di utilizzare un nome univoco per ciascun certificato, in modo che non utilizzi la stessa coppia di chiavi pubblica/privata mostrata

nell'immagine.

**Add Cert Enrollment** ? X

Name\*

Description

CA Information Certificate Parameters **Key** Revocation

Key Type:  RSA  ECDSA

Key Name:\*

Key Size:

**Advanced Settings**

Ignore IPsec Key Usage  
Do not validate values in the Key Usage and extended Key Usage extensions of IPsec remote client certificates.

Allow Overrides

Save Cancel

6. Al termine, fare clic su **Save** (Salva), quindi su **Add** (Aggiungi), come mostrato nell'immagine.

**Add New Certificate** ? X

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device\*:

Cert Enrollment\*:

Cert Enrollment Details:

Name: FTD-1-Self-Signed

Enrollment Type: Self-Signed

SCEP URL: NA

**Add** Cancel

7. Una volta completato, il certificato autofirmato viene visualizzato nell'immagine.

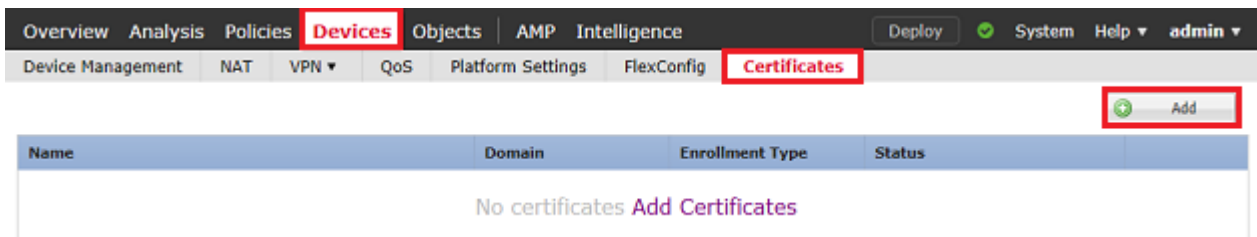
Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT VPN QoS Platform Settings FlexConfig **Certificates**

Name	Domain	Enrollment Type	Status
FTD-1			
FTD-1-Self-Signed	Global	Self-Signed	CA ID

## Iscrizione manuale

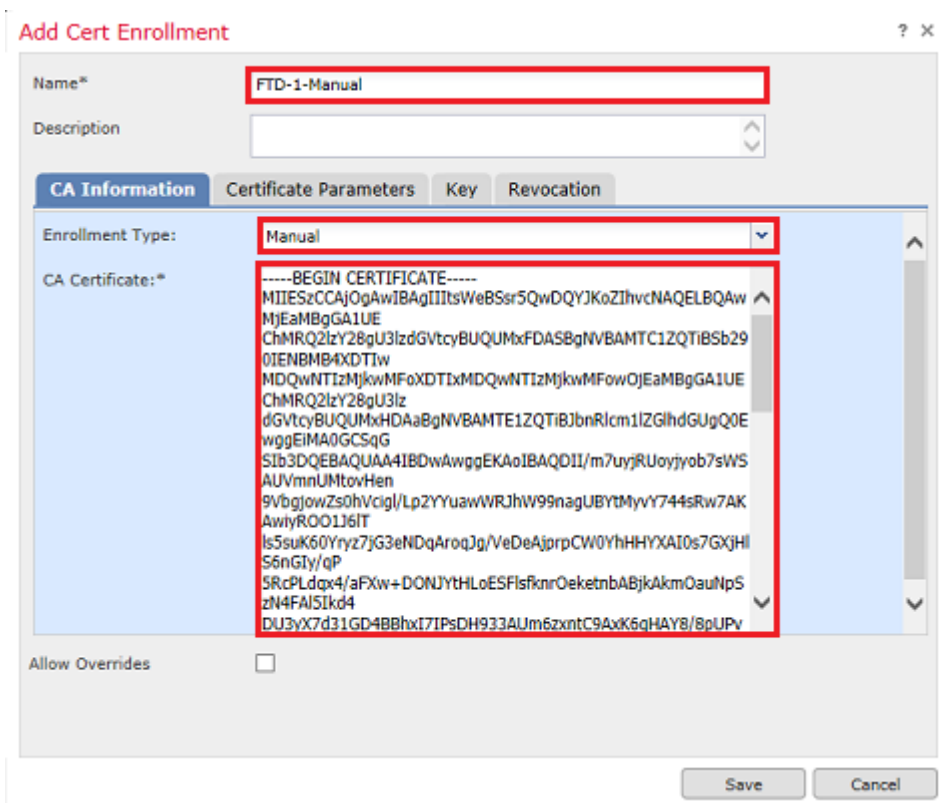
1. Passare a **Dispositivi** > **Certificati**, quindi fare clic su **Aggiungi** come mostrato nell'immagine.



2. Selezionare il dispositivo a cui viene aggiunto il certificato nell'elenco a discesa **Device\***, quindi fare clic sul simbolo verde + come mostrato nell'immagine.



3. Specificare un **Nome** per il trust point e nella scheda **Informazioni CA** selezionare Tipo di iscrizione: **Manuale**. Immettere il certificato in formato pem della CA utilizzata per firmare il certificato di identità. Se il certificato non è al momento disponibile o non è noto, aggiungere qualsiasi certificato CA come segnaposto e, dopo il rilascio del certificato di identità, ripetere questo passaggio per aggiungere la CA emittente effettiva, come mostrato nell'immagine.



4. Nella scheda **Parametri certificato**, inserire un nome comune per il certificato. Deve corrispondere all'FQDN o all'indirizzo IP del servizio per il quale viene utilizzato il certificato, come mostrato nell'immagine.

## Add Cert Enrollment

? X

Name\*

Description

CA Information **Certificate Parameters** Key Revocation

Include FQDN:

Include Device's IP Address:

Common Name (CN):

Organization Unit (OU):

Organization (O):

Locality (L):

State (ST):

Country Code (C):

Email (E):

Include Device's Serial Number

Allow Overrides

Save Cancel

5. (Facoltativo) Nella scheda **Chiave** è possibile specificare facoltativamente il tipo, il nome e le dimensioni della chiave privata utilizzata per il certificato. Per impostazione predefinita, la chiave utilizza una chiave RSA con il nome **<Default-RSA-Key>** e una dimensione di 2048; tuttavia, si consiglia di utilizzare un nome univoco per ciascun certificato in modo che non utilizzi la stessa coppia di chiavi pubblica/privata mostrata nell'immagine.

## Add Cert Enrollment

? X

Name\*

Description

CA Information Certificate Parameters **Key** Revocation

Key Type:  RSA  ECDSA

Key Name:\*

Key Size:

**Advanced Settings**

Ignore IPsec Key Usage  
Do not validate values in the Key Usage and extended Key Usage extensions of IPsec remote client certificates.

Allow Overrides

Save Cancel

6. (Facoltativo) Nella scheda **Revoca**, la revoca dell'elenco di revoche di certificati (CRL) o del protocollo di stato del certificato in linea (OCSP) è selezionata e può essere configurata. Per impostazione predefinita,

nessuno dei due è selezionato come mostrato nell'immagine.

**Add Cert Enrollment** ? X

Name\*

Description

CA Information Certificate Parameters Key **Revocation**

Enable Certificate Revocation Lists (CRL)

Use CRL distribution point from the certificate

User static URL configured

CRL Server URLs:\*

Enable Online Certificate Status Protocol (OCSP)

OCSP Server URL:

Consider the certificate valid if revocation information can not be reached

Allow Overrides

Save Cancel

7. Al termine, fare clic su **Save** (Salva), quindi su **Add** (Aggiungi), come mostrato nell'immagine.

**Add New Certificate** ? X

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device\*:

Cert Enrollment\*:

**Cert Enrollment Details:**

Name: FTD-1-Manual

Enrollment Type: Manual

SCEP URL: NA

Add Cancel

8. Dopo l'elaborazione della richiesta, in FMC viene visualizzata l'opzione per l'aggiunta di un certificato di identità. Fare clic sul pulsante **ID** come mostrato nell'immagine.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT VPN QoS Platform Settings FlexConfig **Certificates**

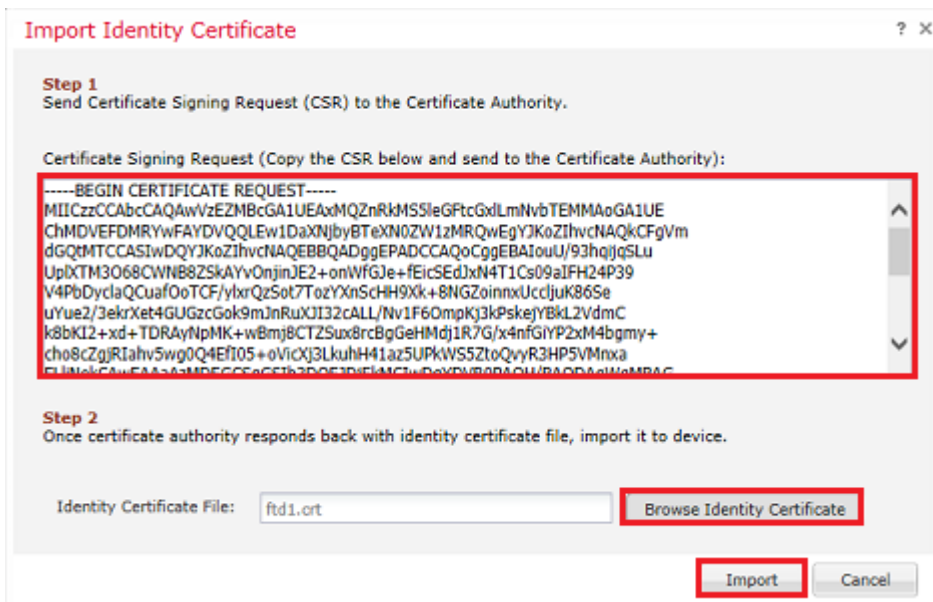
+ Add

Name	Domain	Enrollment Type	Status
FTD-1			
FTD-1-Manual	Global	Manual	CA ID Identity certificate import required

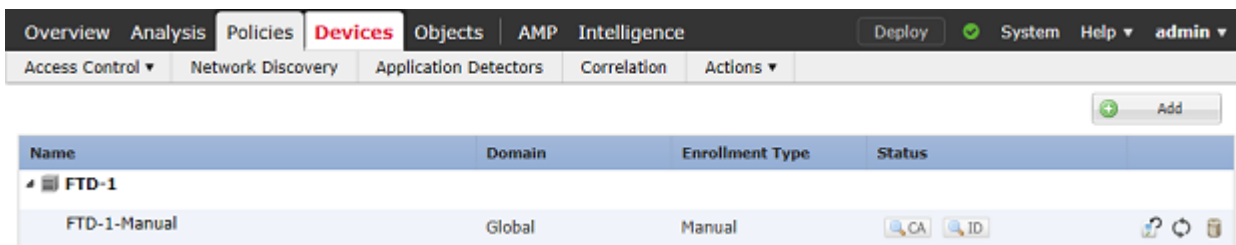
9. Viene visualizzata una finestra che informa che è stato generato un CSR. Fare clic su **Yes** (Sì) come illustrato nell'immagine.



10. Successivamente, viene generato un CSR che può essere copiato e inviato a una CA. Una volta firmato il CSR, viene fornito un certificato di identità. Individuare il certificato di identità fornito e selezionarlo, quindi fare clic su **Importa** come mostrato nell'immagine.

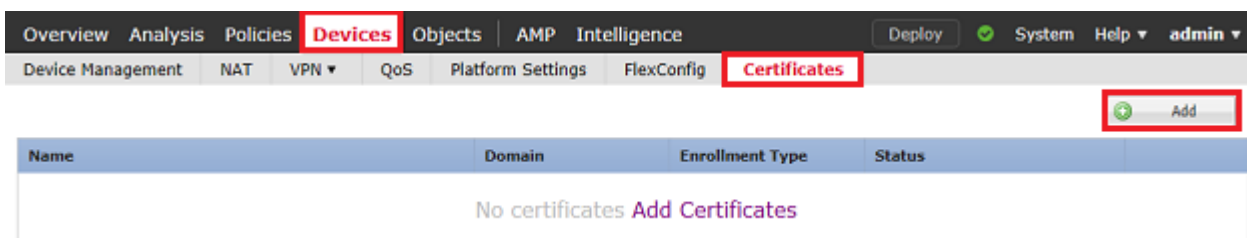


11. Una volta completato, il certificato manuale viene visualizzato come nell'immagine.



## Iscrizione PKCS12

1. Per installare un file PKCS12 ricevuto o creato, passare a **Dispositivi > Certificati**, quindi fare clic su **Aggiungi** come mostrato nell'immagine.



2. Selezionare il dispositivo a cui viene aggiunto il certificato nell'elenco a discesa **Device\***, quindi fare clic sul simbolo verde + come mostrato nell'immagine.



**Add New Certificate** ? X

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device\*: FTD-1

Cert Enrollment\*: Select a certificate enrollment object

Add Cancel

3. Specificare un **nome** per il trust point e nella scheda **Informazioni CA** selezionare Tipo di registrazione: **file PKCS12**. Individuare il file PKCS12 creato e selezionarlo. Immettere il passcode utilizzato per la creazione del PKCS12, come illustrato nell'immagine.

**Add Cert Enrollment** ? X

Name\*: FTD-1-PKCS12

Description

**CA Information** Certificate Parameters Key Revocation

Enrollment Type: PKCS12 File

PKCS12 File\*: PKCS12File.pfx Browse PKCS12 File

Passphrase: .....

Allow Overrides

Save Cancel

4. (Facoltativo) Le schede **Parametri certificato** e **Chiave** sono disattivate in quanto sono già state create con PKCS12. È tuttavia possibile modificare la scheda **Revoca** per abilitare il controllo delle revoche di CRL e/o OCSP. Per impostazione predefinita, nessuno dei due controlli è selezionato come mostrato nell'immagine.

**Add Cert Enrollment** ? x

Name\*

Description

CA Information Certificate Parameters Key **Revocation**

Enable Certificate Revocation Lists (CRL)

Use CRL distribution point from the certificate

User static URL configured

CRL Server URLs\*

Enable Online Certificate Status Protocol (OCSP)

OCSP Server URL:

Consider the certificate valid if revocation information can not be reached

Allow Overrides

Save Cancel

5. Al termine, fare clic su **Save** (Salva), quindi su **Add** (Aggiungi) in questa finestra, come mostrato nell'immagine.

**Add New Certificate** ? x

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device\*:

Cert Enrollment\*:

Cert Enrollment Details:

Name: FTD-1-PKCS12

Enrollment Type: PKCS12 file

SCEP URL: NA

Add Cancel

6. Al termine, il certificato PKCS12 viene visualizzato come illustrato nell'immagine.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

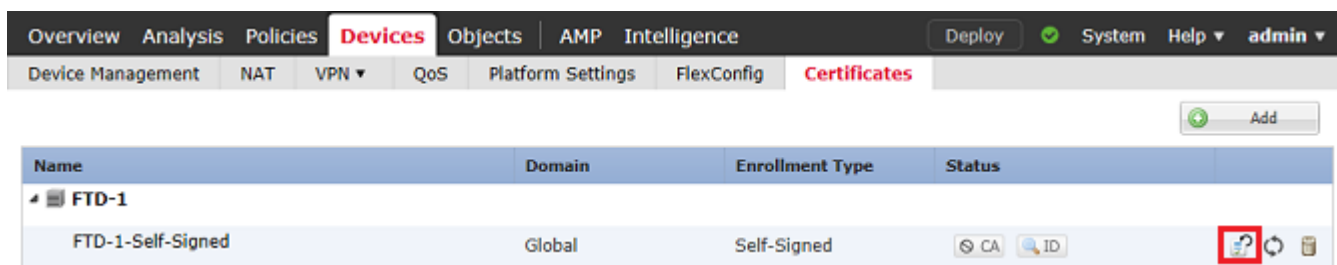
Device Management NAT VPN QoS Platform Settings FlexConfig **Certificates**

Name	Domain	Enrollment Type	Status
FTD-1			
FTD-1-PKCS12	Global	PKCS12 file	CA ID

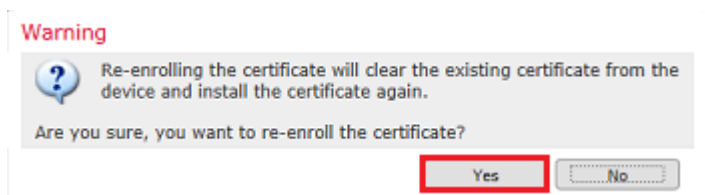
## Rinnovo certificato

## Rinnovo certificato autofirmato

1. Scegliere il pulsante Registra nuovamente certificato come illustrato nell'immagine.



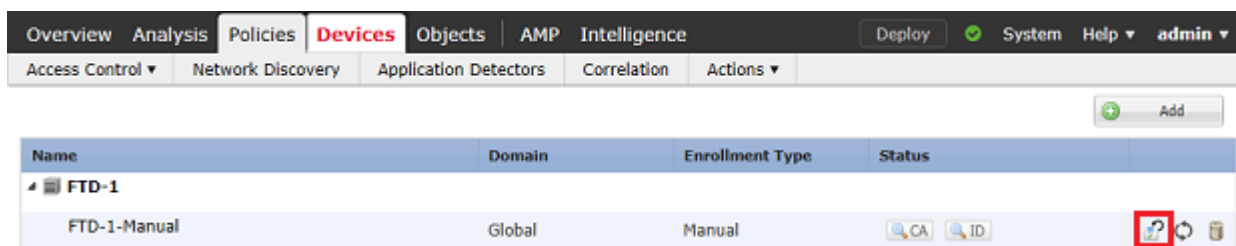
2. Viene visualizzata una finestra in cui viene richiesto di rimuovere e sostituire il certificato autofirmato. Fare clic su **Yes** (Sì) come illustrato nell'immagine.



3. Viene eseguito il push di un documento autofirmato rinnovato nell'FTD. È possibile verificare questa condizione facendo clic sul pulsante ID e selezionando l'opzione Valid time (Ora valida).

## Rinnovo manuale dei certificati

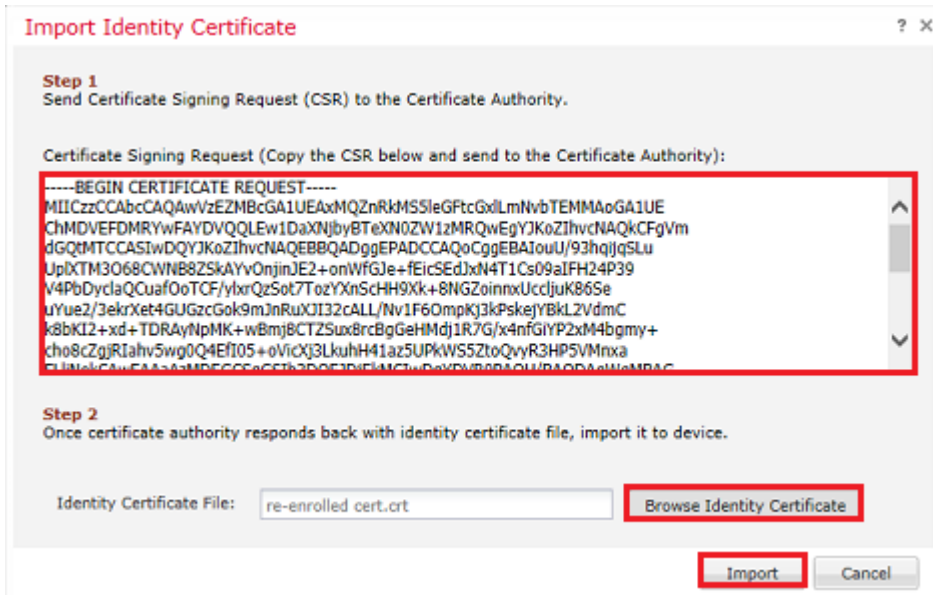
1. Scegliere il pulsante Registra nuovamente certificato come illustrato nell'immagine.



2. Viene visualizzata una finestra in cui viene richiesto di generare una richiesta di firma del certificato. Fare clic su **Yes** (Sì) come illustrato nell'immagine.



3. In questa finestra viene generato un CSR che può essere copiato e inviato alla stessa CA che ha firmato il certificato di identità in precedenza. Una volta firmato il CSR, viene fornito il certificato di identità rinnovato. Individuare il certificato di identità fornito e selezionarlo, quindi fare clic su **Importa** come mostrato nell'immagine.



4. Un certificato manuale rinnovato viene inviato all'FTD. È possibile verificare questa condizione facendo clic sul pulsante ID e selezionando l'opzione Valid time (Ora valida).

## Rinnovo PKCS12

Se si fa clic sul pulsante Registra di nuovo certificato, il certificato non viene rinnovato. Per rinnovare un PKCS12, è necessario creare e caricare un nuovo file PKCS12 utilizzando i metodi menzionati in precedenza.

## Creazione di PKCS12 con OpenSSL

1. Con l'utilizzo di OpenSSL o di un'applicazione simile, generare una chiave privata e una richiesta di firma del certificato (CSR). Nell'esempio vengono mostrate una chiave RSA a 2048 bit denominata **private.key** e una CSR denominata **ftd1.csr** creata in OpenSSL:

```
openssl req -new -newkey rsa:2048 -nodes -keyout private.key -out ftd1.csr
Generating a 2048 bit RSA private key
.....+++
.....+++
written to a new private key to 'private.key'
-----
You are about to be asked to enter information that is incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there is be a default value,
If you enter '.', the field is left blank.
-----
Country Name (2 letter code) [AU]:.
State or Province Name (full name) [Some-State]:.
Locality Name (eg, city) []:.
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco Systems
Organizational Unit Name (eg, section) []:TAC
Common Name (e.g. server FQDN or YOUR name) []:ftd1.example.com
Email Address []:.
```

Please enter these 'extra' attributes

to be sent with your certificate request  
A challenge password []:  
An optional company name []:

2. Copiare il CSR generato e inviarlo a una CA. Una volta firmato il CSR, viene fornito un certificato di identità. In genere vengono forniti anche i certificati CA. Per creare un PKCS12, eseguire uno dei seguenti comandi in OpenSSL:

Per includere solo il certificato CA rilasciato all'interno di PKCS12, utilizzare questo comando:

```
openssl pkcs12 -export -out ftd.pfx -in ftd.crt -inkey private.key -certfile ca.crt  
Enter Export Password: *****  
Verifying - Enter Export Password: *****
```

- **ftd.pfx** è il nome del file pkcs12 (in formato der) esportato da openssl.
- **ftd.crt** è il nome del certificato di identità firmato rilasciato dalla CA in formato pem.
- **private.key** è la coppia di chiavi creata nel passaggio 1.
- **ca.crt** è il certificato dell'autorità di certificazione emittente in formato pem.

Se il certificato fa parte di una catena con una CA radice e una o più CA intermedie, è possibile utilizzare questo comando per aggiungere la catena completa in PKCS12:

```
openssl pkcs12 -export -out ftd.pfx -in ftd.crt -inkey private.key -chain -CAfile cachain.pem  
Enter Export Password: *****  
Verifying - Enter Export Password: *****
```

- **ftd.pfx** è il nome del file pkcs12 (in formato der) esportato da OpenSSL.
- **ftd.crt** è il nome del certificato di identità firmato rilasciato dalla CA in formato pem.
- **private.key** è la coppia di chiavi creata nel passaggio 1.
- **cachain.pem** è un file che contiene i certificati CA nella catena che inizia con la CA intermedia emittente e termina con la CA radice in formato pem.

Se viene restituito un file PKCS7 (.p7b, .p7c), questi comandi possono essere utilizzati anche per creare PKCS12. Se il p7b è in formato der, assicurarsi di aggiungere **-informar der** agli argomenti, altrimenti non includerlo:

```
openssl pkcs7 -in ftd.p7b -inform der -print_certs -out ftdpem.crt
```

```
openssl pkcs12 -export -in ftdpem.crt -inkey private.key -out ftd.pfx  
Enter Export Password: *****  
Verifying - Enter Export Password: *****
```

- **ftd.p7b** è il PKCS7 restituito dalla CA contenente il certificato di identità firmato e la catena di CA.
- **ftdpem.crt** è il file p7b convertito.
- **ftd.pfx** è il nome del file pkcs12 (in formato der) esportato da OpenSSL.

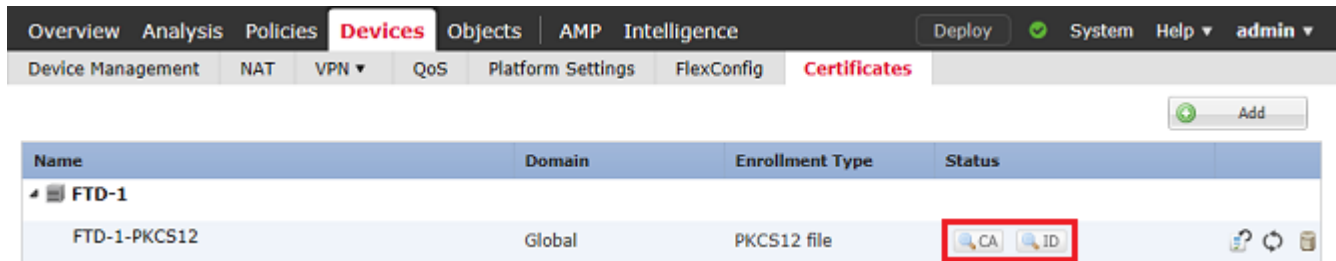
- **private.key** è la coppia di chiavi creata nel passaggio 1.

## Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

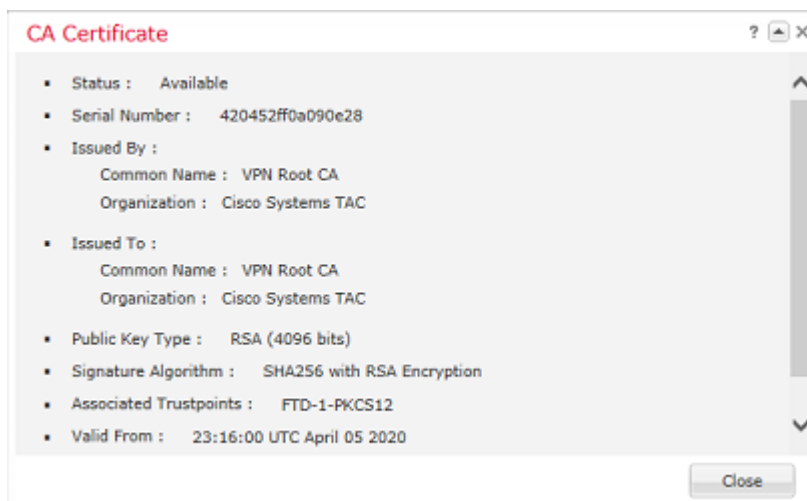
### Visualizza certificati installati in FMC

In FMC, selezionare **Dispositivi > Certificati**. Per il trust point appropriato, fare clic sulla **CA** o sull'**ID** per visualizzare ulteriori dettagli sul certificato, come mostrato nell'immagine.

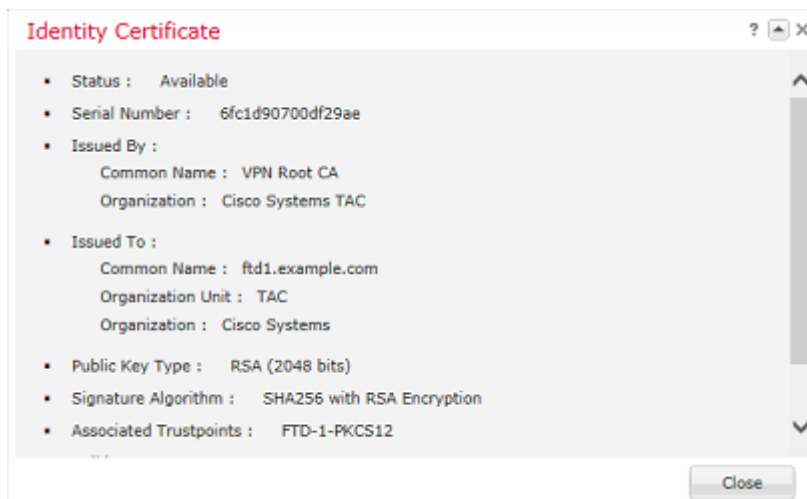


Name	Domain	Enrollment Type	Status
FTD-1			
FTD-1-PKCS12	Global	PKCS12 file	CA ID

Verificare il certificato CA come mostrato nell'immagine.



Verificare il certificato di identità come mostrato nell'immagine.



## Visualizza certificati installati nella CLI

SSH sull'FTD e immettere il comando **show crypto ca certificate**.

```
> show crypto ca certificates
Certificate
  Status: Available
  Certificate Serial Number: 6fc1d90700df29ae
  Certificate Usage: General Purpose
  Public Key Type: RSA (2048 bits)
  Signature Algorithm: SHA256 with RSA Encryption
  Issuer Name:
    cn=VPN Root CA
    o=Cisco Systems TAC
  Subject Name:
    cn=ftd1.example.com
    ou=TAC
    o=Cisco Systems
  Validity Date:
    start date: 15:47:00 UTC Apr 8 2020
    end   date: 15:47:00 UTC Apr 8 2021
  Storage: config
  Associated Trustpoints: FTD-1-PKCS12
```

```
CA Certificate
  Status: Available
  Certificate Serial Number: 420452ff0a090e28
  Certificate Usage: General Purpose
  Public Key Type: RSA (4096 bits)
  Signature Algorithm: SHA256 with RSA Encryption
  Issuer Name:
    cn=VPN Root CA
    o=Cisco Systems TAC
  Subject Name:
    cn=VPN Root CA
    o=Cisco Systems TAC
  Validity Date:
    start date: 23:16:00 UTC Apr 5 2020
    end   date: 23:16:00 UTC Apr 5 2030
  Storage: config
  Associated Trustpoints: FTD-1-PKCS12
```

## Risoluzione dei problemi

In questa sezione vengono fornite informazioni utili per risolvere i problemi di configurazione.

### Comandi debug

I debug possono essere eseguiti dalla CLI di diagnostica dopo la connessione dell'FTD tramite SSH in caso di errore nell'installazione di un certificato SSL:

#### **debug crypto ca 14**

Nelle versioni precedenti di FTD, questi debug sono disponibili e consigliati per la risoluzione dei problemi:

**debug crypto ca 255**

**debug crypto ca message 255**

**debug crypto ca transaction 255**

## **Problemi comuni**

Dopo l'importazione del certificato di identità emesso, visualizzare comunque il messaggio "Importazione certificato di identità obbligatoria".

Ciò può verificarsi a causa di due problemi distinti:

### 1. Il certificato CA emittente non è stato aggiunto durante la registrazione manuale

Quando il certificato di identità viene importato, viene confrontato con il certificato CA aggiunto nella scheda Informazioni CA alla registrazione manuale. A volte gli amministratori di rete non dispongono del certificato CA per la CA utilizzata per firmare il certificato di identità. In questo caso, è necessario aggiungere un certificato CA segnaposto quando si esegue la registrazione manuale. Una volta rilasciato il certificato di identità e fornito il certificato CA, è possibile eseguire una nuova registrazione manuale con il certificato CA corretto. Quando si esegue di nuovo la procedura guidata di registrazione manuale, assicurarsi di specificare per la coppia di chiavi lo stesso nome e le stesse dimensioni della registrazione manuale originale. Al termine, invece di inoltrare nuovamente il CSR alla CA, è possibile importare il certificato di identità rilasciato in precedenza nel trust point appena creato con il certificato CA corretto.

Per verificare se lo stesso certificato CA è stato applicato durante la registrazione manuale, fare clic sul pulsante CA come specificato nella sezione Verifica oppure controllare l'output di **show crypto ca certificates**. Campi quali Rilasciato a e Numero di serie possono essere confrontati con i campi nel certificato CA fornito dall'autorità di certificazione.

### 2. La coppia di chiavi nel trust point creato è diversa da quella utilizzata quando viene creato il CSR per il certificato rilasciato.

Con la registrazione manuale, quando vengono generati la coppia di chiavi e il CSR, la chiave pubblica viene aggiunta al CSR in modo che possa essere inclusa nel certificato di identità rilasciato. Se per qualche motivo la coppia di chiavi sull'FTD viene modificata o il certificato di identità rilasciato include una chiave pubblica diversa, l'FTD non installa il certificato di identità rilasciato. Per verificare se questa condizione si è verificata, sono disponibili due test diversi:

In OpenSSL, è possibile eseguire questi comandi per confrontare la chiave pubblica nel CSR con la chiave pubblica nel certificato emesso:

```
openssl req -noout -modulus -in ftd.csr
```

```
Modulus=8A2E53FF7786A8A3A922EE5299574CCDCEEBC096341F194A4018BCE9E38A7244DBEA2759F1897BE7C489C484749C4DE1  
0FDFD5783DB0F27256900AE69F3A84C217FCA5C6B4334A8B7B4E8CD85E749C1C7F5793EF0D199A229E7C5471C963B8AF3A49EB98  
81941B3706A24F6626746E5C9237D9C00B2FF36FD45E8E9A92A3DE43EC91E8D80642F655D98293C6CA236FB177E4C3440C8DA4C2  
C7CADC06019E1CC763D51EC6FF1E277C68983F6C4CE1B826CBE721A3C7198234486A1BF9C20D10E047C8D39FA85627178F72E4BA  
B966DA10BF24771CFE55327C5A14B96235E9
```

```
openssl x509 -noout -modulus -in id.crt
```

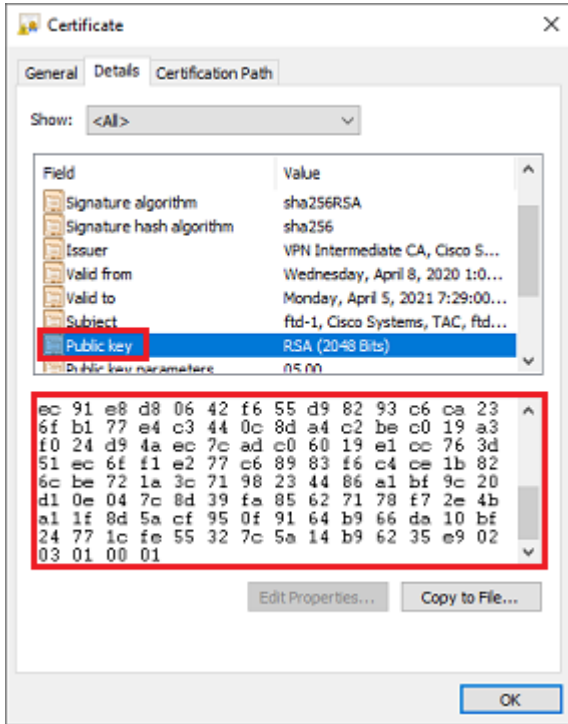
```
Modulus=8A2E53FF7786A8A3A922EE5299574CCDCEEBC096341F194A4018BCE9E38A7244DBEA2759F1897BE7C489C484749C4DE1  
0FDFD5783DB0F27256900AE69F3A84C217FCA5C6B4334A8B7B4E8CD85E749C1C7F5793EF0D199A229E7C5471C963B8AF3A49EB98  
81941B3706A24F6626746E5C9237D9C00B2FF36FD45E8E9A92A3DE43EC91E8D80642F655D98293C6CA236FB177E4C3440C8DA4C2  
C7CADC06019E1CC763D51EC6FF1E277C68983F6C4CE1B826CBE721A3C7198234486A1BF9C20D10E047C8D39FA85627178F72E4BA  
B966DA10BF24771CFE55327C5A14B96235E9
```



- **ftd.csr** è il CSR copiato da FMC al momento dell'iscrizione manuale.
- **id.crt** è il certificato di identità firmato dalla CA.

In alternativa, il valore della chiave pubblica sull'FTD può anche essere confrontato con la chiave pubblica all'interno del certificato di identità rilasciato. Si noti che i primi caratteri del certificato non corrispondono a quelli nell'output FTD a causa della spaziatura interna:

Certificato di identità rilasciato aperto nel PC Windows:



Output chiave pubblica estratto dal certificato di identità:

```
3082010a02820101008a2e53ff7786a8a3a922ee5299574ccdceebc096341f194a4018bce9e38a7244dbea2759f1897be7c489c4
f6e0dfd5783db0f27256900ae69f3a84c217fca5c6b4334a8b7b4e8cd85e749c1c7f5793ef0d199a229e7c5471c963b8af3a49e
1b3706a24f6626746e5c9237d9c00b2ff36fd45e8e9a92a3de43ec91e8d80642f655d98293c6ca236fb177e4c3440c8da4c2bec0
e1cc763d51ec6ff1e277c68983f6c4ce1b826cbe721a3c7198234486a1bf9c20d10e047c8d39fa85627178f72e4ba11f8d5acf95
55327c5a14b96235e90203010001
```

**Mostra l'output della chiave crittografica mypubkey rsa** dal FTD. Al momento dell'iscrizione manuale, per creare il CSR è stata utilizzata la **<Default-RSA-Key>**. La sezione in grassetto corrisponde all'output della chiave pubblica estratto dal certificato di identità.

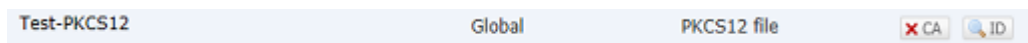
```
> show crypto key mypubkey rsa
Key pair was generated at: 16:58:44 UTC Jan 25 2019
Key name: <Default-RSA-Key>
Usage: General Purpose Key
Modulus Size (bits): 2048
Storage: config
Key Data:
```

```
30820122 300d0609 2a864886 f70d0101 01050003 82010f00 3082010a 02820101
```

```
008a2e53 ff7786a8 a3a922ee 5299574c cdceebc0 96341f19 4a4018bc e9e38a72
44dbea27 59f1897b e7c489c4 84749c4d e13d42b3 4f5a2051 f6e0dfd 5783db0f
27256900 ae69f3a8 4c217fca 5c6b4334 a8b7b4e8 cd85e749 c1c7f579 3ef0d199
a229e7c5 471c963b 8af3a49e b98b9edb fdde92b5 deb78194 1b3706a2 4f662674
6e5c9237 d9c00b2f f36fd45e 8e9a92a3 de43ec91 e8d80642 f655d982 93c6ca23
6fb177e4 c3440c8d a4c2bec0 19a3f024 d94aec7c adc06019 e1cc763d 51ec6ff1
e277c689 83f6c4ce 1b826cbe 721a3c71 98234486 a1bf9c20 d10e047c 8d39fa85
627178f7 2e4ba11f 8d5acf95 0f9164b9 66da10bf 24771cfe 55327c5a 14b96235
e9020301 0001
```

## X rossa accanto a CA in FMC

Questa situazione può verificarsi con la registrazione PKCS12 perché il certificato CA non è incluso nel pacchetto PKCS12.



Per risolvere il problema, è necessario aggiungere il certificato CA a PKCS12.

Utilizzare questi comandi per estrarre il certificato di identità e la chiave privata. La password utilizzata al momento della creazione di PKCS12 e la chiave privata protetta sono necessarie:

```
openssl pkcs12 -info -in test.p12
Enter Import Password: [pkcs12 pass phrase here]
MAC Iteration 1
MAC verified OK
PKCS7 Encrypted data: pbeWithSHA1And40BitRC2-CBC, Iteration 2048
Certificate bag
Bag Attributes
    friendlyName: Test
    localKeyID: 76 8F D1 75 F0 69 FA E6 2F CF D3 A6 83 48 01 C4 63 F4 9B F2
subject=/CN=ftd1.example.com
issuer=/O=Cisco Systems TAC/CN=VPN Intermediate CA
-----BEGIN CERTIFICATE-----
MIIC+TCCAeGgAwIBAgIIAUIM3+3IMhIwDQYJKoZIhvcNAQELBQAwOjEaMBGGA1UE
ChMRQ2lzY28gU3lzdGVtcyBUQUxHDAaBgNVBAMTE1ZQTiBjb3R1cm1lZGlhdGUg
Q0EwHhcNMjAwNDA0MTY1ODAwWhcNMjEwNDA1MjMyOTAwWjAbMRkwFwYDVQQDExBm
dGQxLmV4Y29tY29tY29tY29tY29tY29tY29tY29tY29tY29tY29tY29tY29tY29t
043eLVP18K0jnyfHCBZuFUyRXTTB28Z1ouIJ5yyrDzCN781GFrb/wCczRx/jW4n
pF9q2z7FHr5bQCI4oSUSX40UQfr0/u0K5riI1uZumpUx1Vp1zVkyuqDd/i1r0+0j
PyS7BmyGfV7aebYWznr8R9ebDsnC2U3nKjP5RaE/wNdVGTS/180HlrIjMpcFMXps
LwxdxiEz0hCMnDm9RC+7uWZQdlwZ9oNANCBQC0px/Zikj9Dz7ORhbbzBTeUNKD3p
sN3VqdDPvGZHFGLPCnhKYyZ79+6p+CHC8X8BFjuTJYoo1l6uGgiB4Jz2Y9ZeFSQz
Q11IH3v+xKMJnv6IkZLuvwIDAQABoyIwIDAeBg1ghkgBhvCAQ0EERYPeGNhIGN1
cnRpZmljYXRlMA0GCsqGSIb3DQEBcUAA4IBAQCv/MgshWxXtpwmmMF/6KqEj8nB
SljbfzLzNuPV/LLMSnxMLDo6+LB8tizNR+ao9dGATRY54taRI27W+gLneCbQAux
9amxXuhpxP5E0hkn+tsYS9eriAKpHuS1Y/2uwN92fHIbh3HEXP01HBjueI8PH3ZK
4lrPKA9oIQPUW/uueHEF+xCbG4xCLi5H0GeHX+FTigGNqazaX5GM4RBUa4bk8jks
Ig53twvop71wE53COTH0EkSRCsVcW5mdJsd9BUZHjguhpw8Giv7Z36qWv18I/Owf
RhLhtsgenc25udglvv9Sy5xK53a5Ieg8biRpWL9tIjgUgjxYZwtyVeHi32S7
-----END CERTIFICATE-----
PKCS7 Data
Shrouded Keybag: pbeWithSHA1And3-KeyTripleDES-CBC, Iteration 2048
Bag Attributes
    friendlyName: Test
    localKeyID: 76 8F D1 75 F0 69 FA E6 2F CF D3 A6 83 48 01 C4 63 F4 9B F2
Key Attributes: <No Attributes>
```

```
Enter PEM pass phrase: [private-key pass phrase here]
Verifying - Enter PEM pass phrase: [private-key pass phrase here]
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFDjBABGkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQIILKyWXk8cgTMCaggA
MBQGcCqGSIb3DQMHBAGm0qRXh/dcwSCBmIF7BpgJNIPhdU5Zorn1jm3pmsI/XkJ
MRHc1Reel0ziSLCZ05Tr84JFQxNpbThXLhsHC9WhpPy5sNXIvXS7Gu+U10/V1NSA
rWlX6SPftAYiFq5QXyEutSHdZZwQIQpj97seu3Px0agvI0bW1Lo8or5lSydnMjp
Ptv50Ko95BSHwWycqkTAia4ZKxytyIc/mIu5m72Luc0FmoRB05JZu1avWXjbCAA+
k2ebkb1FT0YRQT1Z4tZHSqX1LFPZe170NZEUG7rIcWAk1Yw7XNUPh0n6FHL/ieIZ
IhvIfj+1gQKeovHkSKuwzb24Zx0exkhafPsgp0PMAPxBnQ/Cxh7Dq2dh1FD8P15E
Gnh8r3l903AlkPMBkMdx0qlpzo2naIy2KGrUnOSHajVwclR9dTPWIDyjd95YoeS
IUE7Ma00pjJc02FNbWyxRrYt+4hp3aJt0ZW83FHiS1B5UIzGrBMAgKJc2Hb2RTV
9gxZGve1cRcolLeJRYoK9+PeZ7t17xzLSg5wad4R/ZPKUwTBUaShn0wHzridF8Zn
F06XvBDSyuxVSpkxwAd1Twxq62tUnLIkyRXo2CSz8z8W29UXmF04o3G67n28//LJ
Ku8wj1jjeqlvFgXSQiWLADNhiY772RNwzCMeobfxG1BprF9DPT8yvyBdQviUIuFpJ
nNs5FYbLTV9ygZ1S9xwQpTcqEu+y4F5BJuYlMhqcZ+VpFA4nM0YHhZ5M3sceRSR4
1L+a3BPJJsh1TIJQg0TIxDaveCfpDcpS+ydUgS6YWY8xw17v0+1f7y5z1t4TkZrt
ItBHHA6yDzR0Cn0/ZH3y88a/asDcukw6bsRaY5iT8nAWgTQVed3xXj+EgeRs25HB
dIBBX5gTvqN7qDanhkaPUcEawj1/38M0pAYULei3e1fKKrhwaYsBFaV/BeUMWuNW
BmKprkKKQv/JdWnoJ149KcS4bfa3GHG9XXnyvbg8HxopcYFMTEjao+wLZH9aggKe
Y0jyoHFN6ccBBC7vn7u12tmX0M5RcnPLmaDaBFDSBBFS8Y8VkeHn3P0q7+sEQ26d
vL807WdgLH/wKqovoJRyxwzz+TryRq9cd5BNyyLaABESa1sWRhk81C2P+B+Jdg9w
d6RsvJ2dt3pd1/+pUR3CdC0b8qRZ0oL03+onUIUoEsCCNdp0x8Yj/mvc6ReXt0KB
2qVmhVMYseiUlR0AQGt7XMe1UuiJ+dRnqcFAfbdGeOp+6epm1TK1BJL2mAlQWx5l
73Qo4M7rR7laeq/dqob3o1PhcoMLa5z/Lo5vDe7S+LZMuAWjRkSfso0KQOY3kAP1
eZ2Eh2go4eJ7hHf5VFqBLl8Ci3rd3E0ijRkNm3fAQmFJlaFmooBM3Y2Ba+U8cMTH
lgjSFk11FAWpfxw9aSEECNCvEMm1Ghm6/tJDLV1jyTqwajHnWIZCc+P2AXgn1LzG
HVVfxs0c8FGUJJPQHatXYd7worWCxszaufJ99E4PaoZnAOYUFw2jaZEwo0NBPbD1
AjQ8aciuosv0FKpp/jXDI78/aYAEk662tPsfGmxvAWB+UMFarA9ZTiihK3x/tDPy
GZ6ByGWJYp/0tNNmJRCFhcAyy83EztzHK9h+8LatFA6WrJ4j3dhceUPzrPXjMffNN
0Yg=
-----END ENCRYPTED PRIVATE KEY-----
```

Una volta completato, il certificato di identità e la chiave privata possono essere inseriti in file separati e il certificato CA può essere importato in un nuovo file PKCS12 seguendo i passaggi indicati al punto 2 della **creazione di PKCS12 con OpenSSL**.

## 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).