Implementazione di certificati CA firmati in una soluzione CCE

Sommario

Introduzione

In questo documento viene descritto come implementare i certificati firmati da un'Autorità di certificazione (CA) nella soluzione Cisco Contact Center Enterprise (CCE).

Contributo di Anuj Bhatia, Robert Rogier e Ramiro Amaya, Cisco TAC Engineers.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Unified Contact Center Enterprise (UCCE) release 12.5(1)
- Package Contact Center Enterprise release 12.5(1)
- Customer Voice Portal (CVP) versione 12.5 (1)
- Cisco Virtualized Voice Browser (VB)
- Cisco CVP Operations and Administration Console (OAMP)
- Cisco Unified Intelligence Center (CUIC)
- Cisco Unified Communications Manager (CUCM)

Componenti usati

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

- PCCE 12.5(1)
- CVP 12.5(1)
- Cisco VB 12.5
- Finesse 12.5
- CUIC 12.5
- Windows 2016

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

I certificati vengono utilizzati per garantire la sicurezza delle comunicazioni con l'autenticazione tra client e server.

Gli utenti possono acquistare certificati da una CA o utilizzare certificati autofirmati.

I certificati autofirmati (come indica il nome) sono firmati dalla stessa entità di cui certificano l'identità, anziché da un'autorità di certificazione. I certificati autofirmati non sono considerati sicuri come i certificati CA, ma vengono utilizzati per impostazione predefinita in molte applicazioni.

Nella soluzione Package Contact Center Enterprise (PCCE) versione 12.x, tutti i componenti della soluzione sono controllati da Single Pane of Glass (SPOG), che è ospitato nel server AW (Admin Workstation) principale.

A causa di Security Management Compliance (SRC) nella versione PCCE 12.5(1), tutte le comunicazioni tra SPOG e gli altri componenti della soluzione avvengono tramite il protocollo HTTP protetto. In UCCE 12.5 la comunicazione tra i componenti viene effettuata anche tramite il protocollo HTTP protetto.

In questo documento vengono illustrati in dettaglio i passaggi necessari per implementare i certificati firmati dall'autorità di certificazione in una soluzione CCE per la comunicazione HTTP

protetta. Per qualsiasi altra considerazione sulla sicurezza UCCE, fare riferimento alle linee guida sulla sicurezza UCCE. Per qualunque comunicazione aggiuntiva protetta da CVP diversa da HTTP protetta, consultare le linee guida sulla sicurezza nella guida alla configurazione di CVP: Linee guida per la sicurezza di CVP.

Procedura

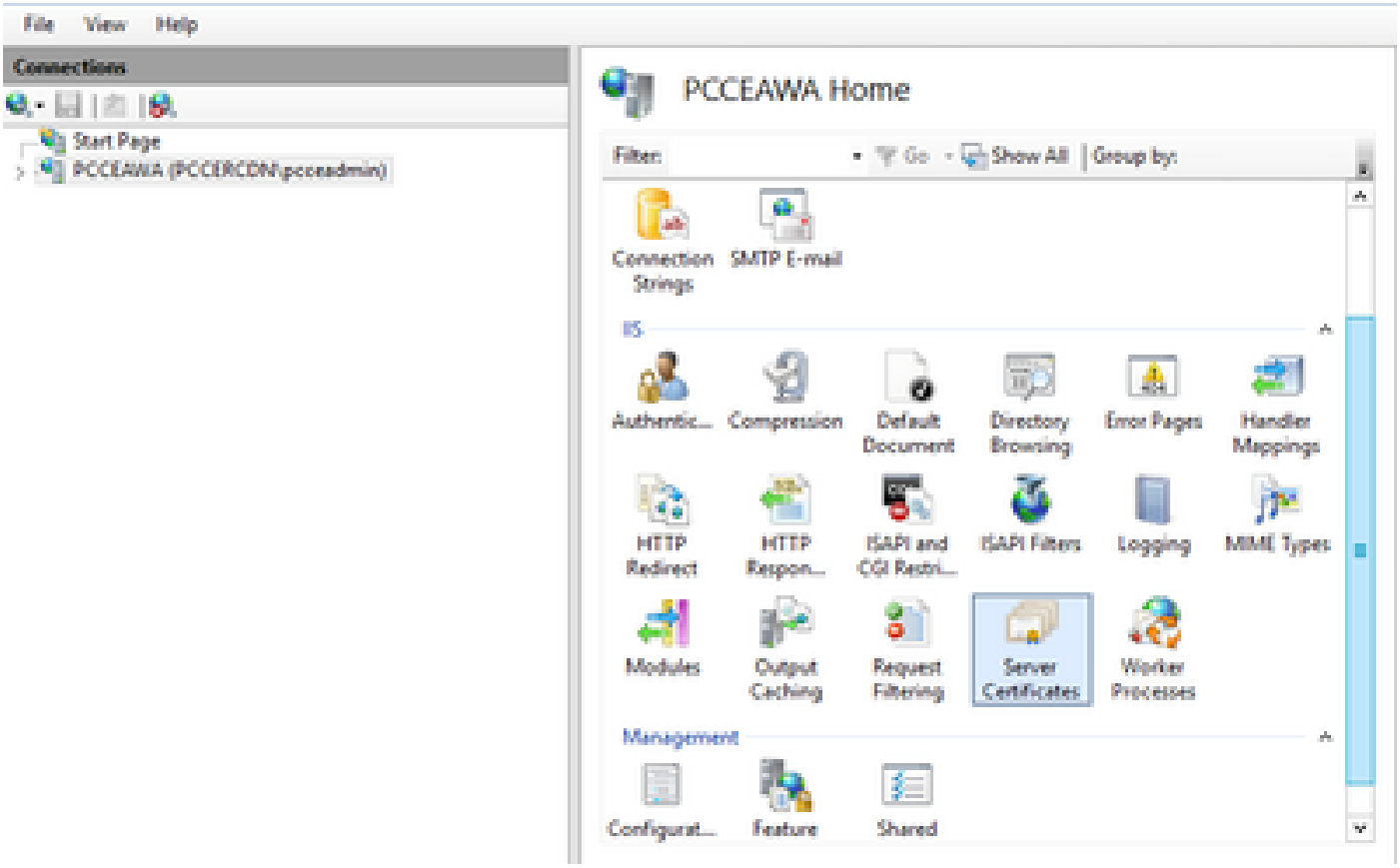
Server CCE basati su Windows

1. Generare CSR

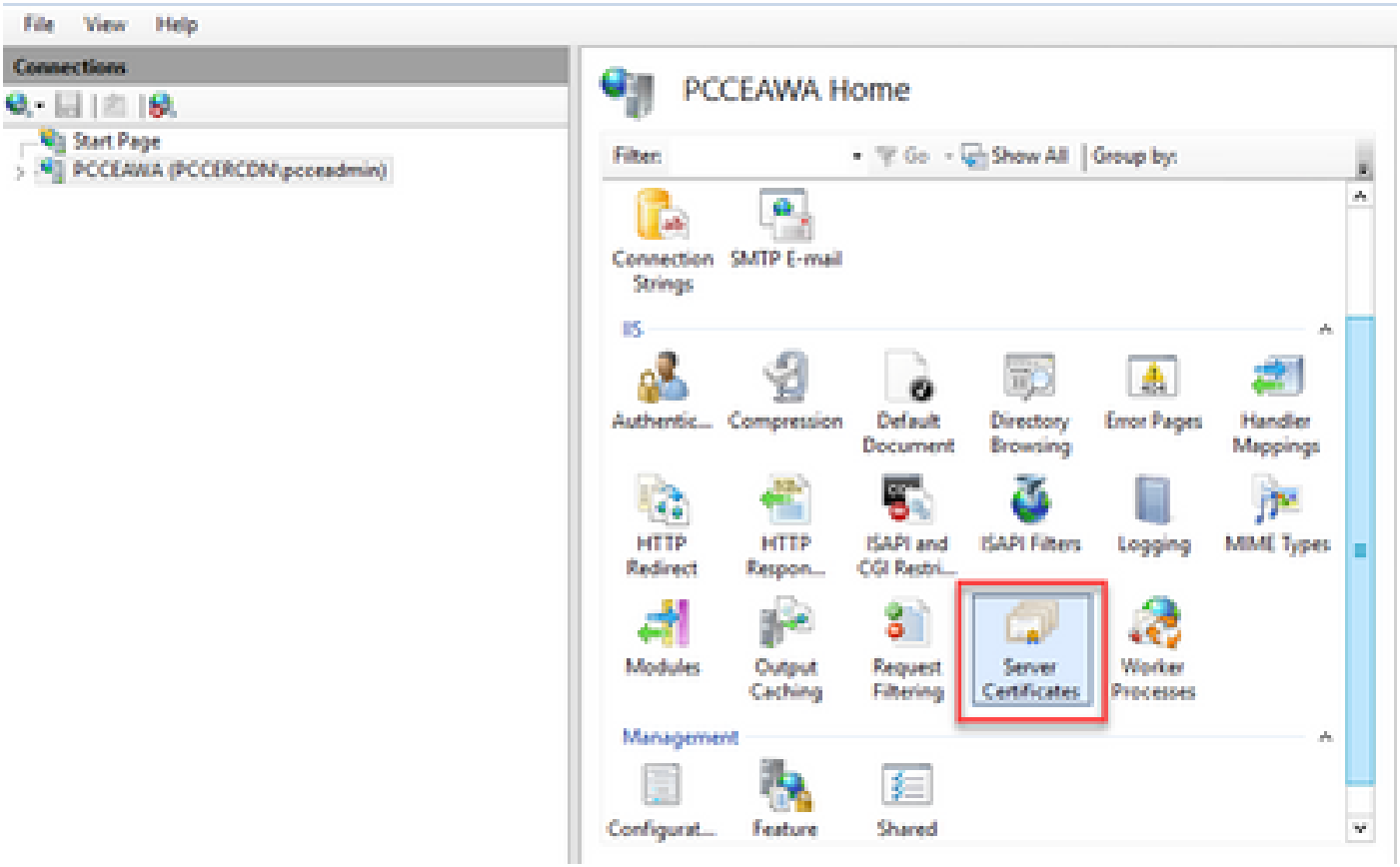
In questa procedura viene illustrato come generare una richiesta di firma di certificato (CSR) da Gestione Internet Information Services (IIS).

Passaggio 1. Accedere a Windows e scegliere Pannello di controllo > Strumenti di amministrazione > Gestione Internet Information Services (IIS).

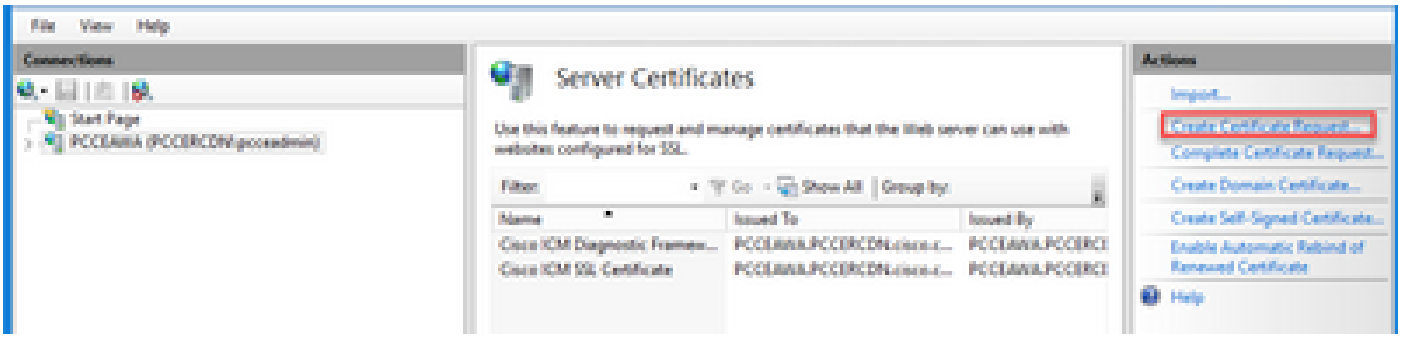
Passaggio 2. Nel riquadro Connessioni fare clic sul nome del server. Viene visualizzato il riquadro Home del server.



Passaggio 3. Nell'area IIS fare doppio clic su Certificati server.

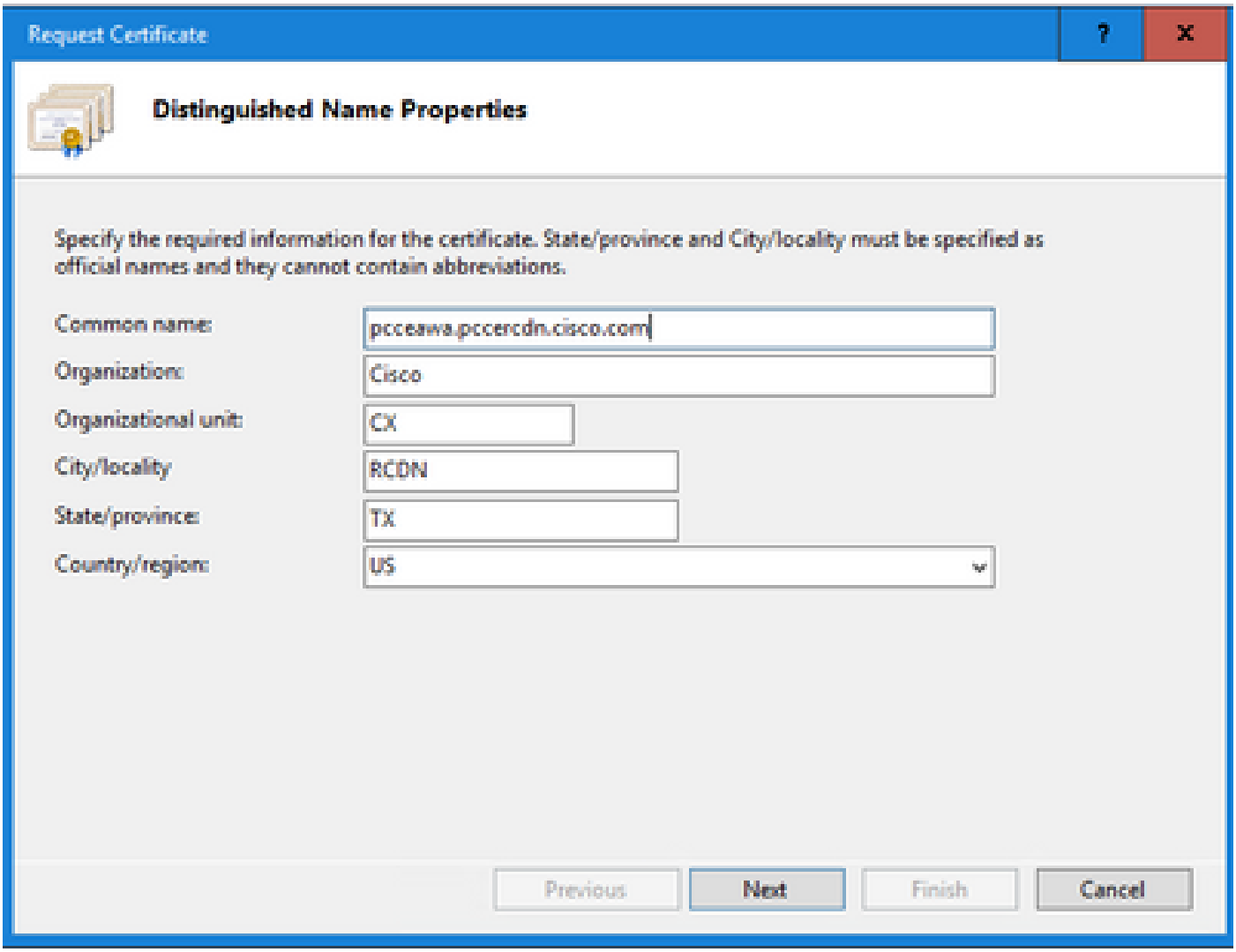


Passaggio 4. Nel riquadro Azioni fare clic su Crea richiesta certificato.



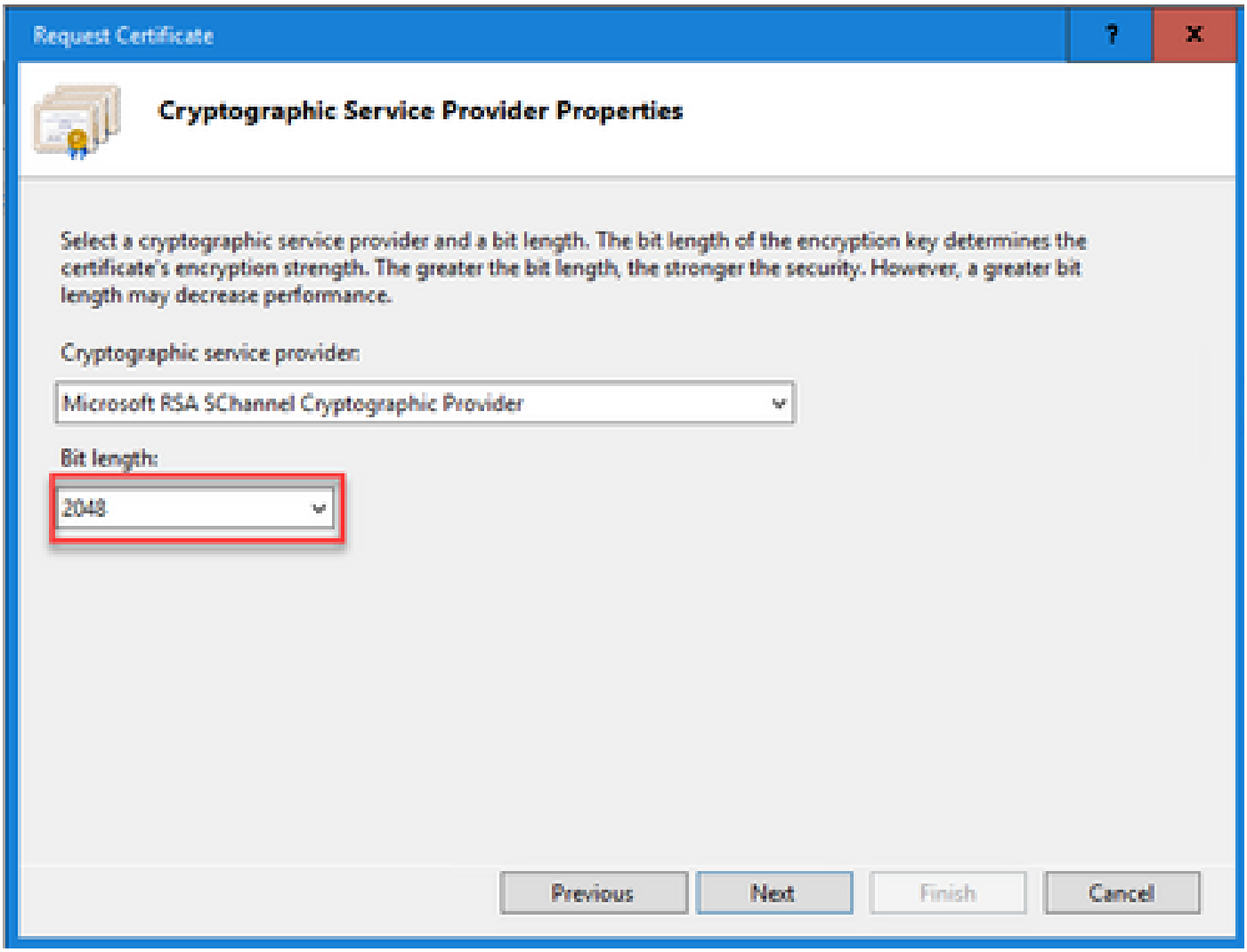
Passaggio 5. Nella finestra di dialogo Richiedi certificato eseguire le operazioni seguenti:

Specificare le informazioni richieste nei campi visualizzati e fare clic su Avanti.

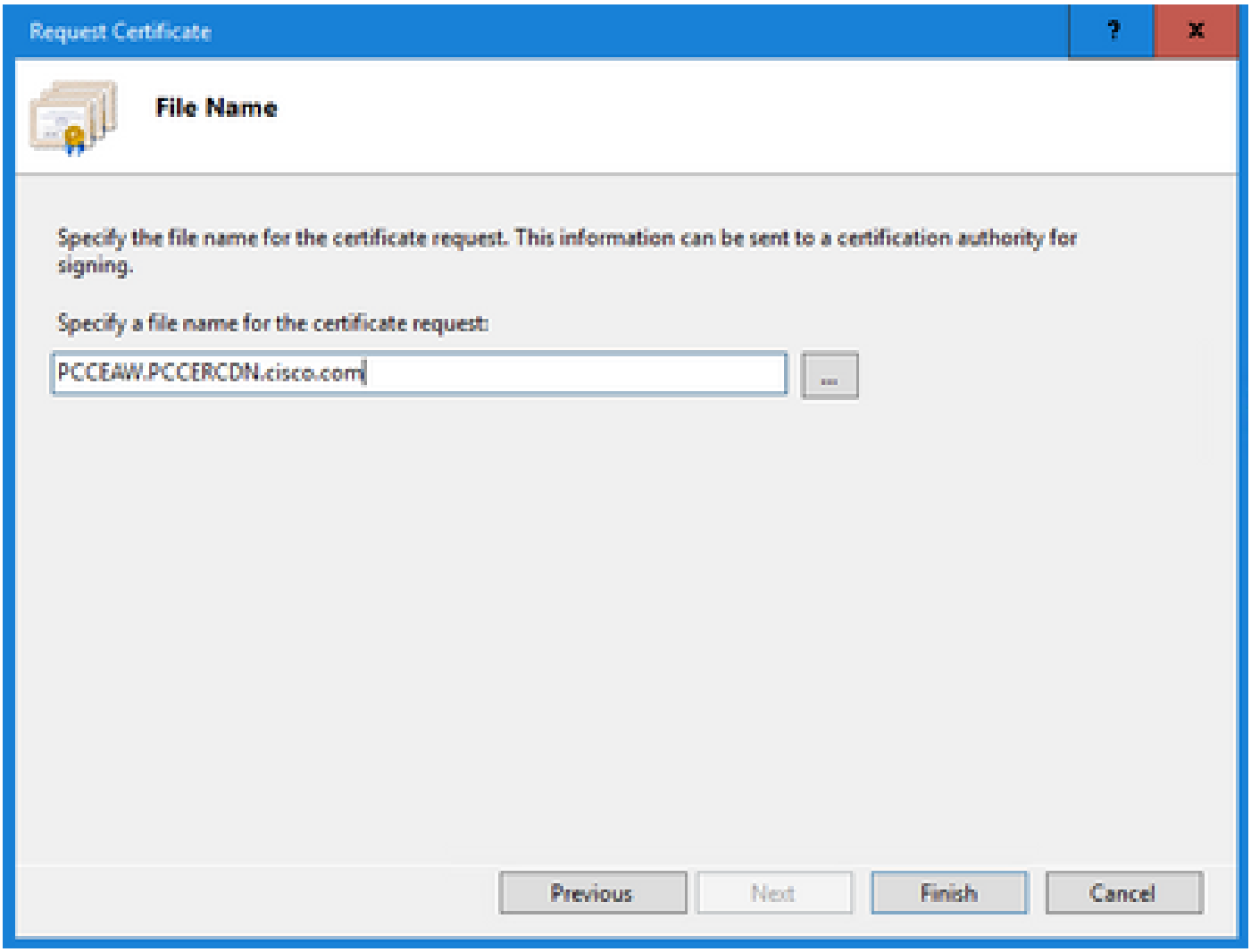


Lasciare invariata l'impostazione predefinita nell'elenco a discesa Provider del servizio di crittografia.

Dall'elenco a discesa Lunghezza bit selezionare 2048.



Passaggio 6. Specificare un nome file per la richiesta di certificato e fare clic su Fine.



2. Ottenere i certificati firmati dalla CA

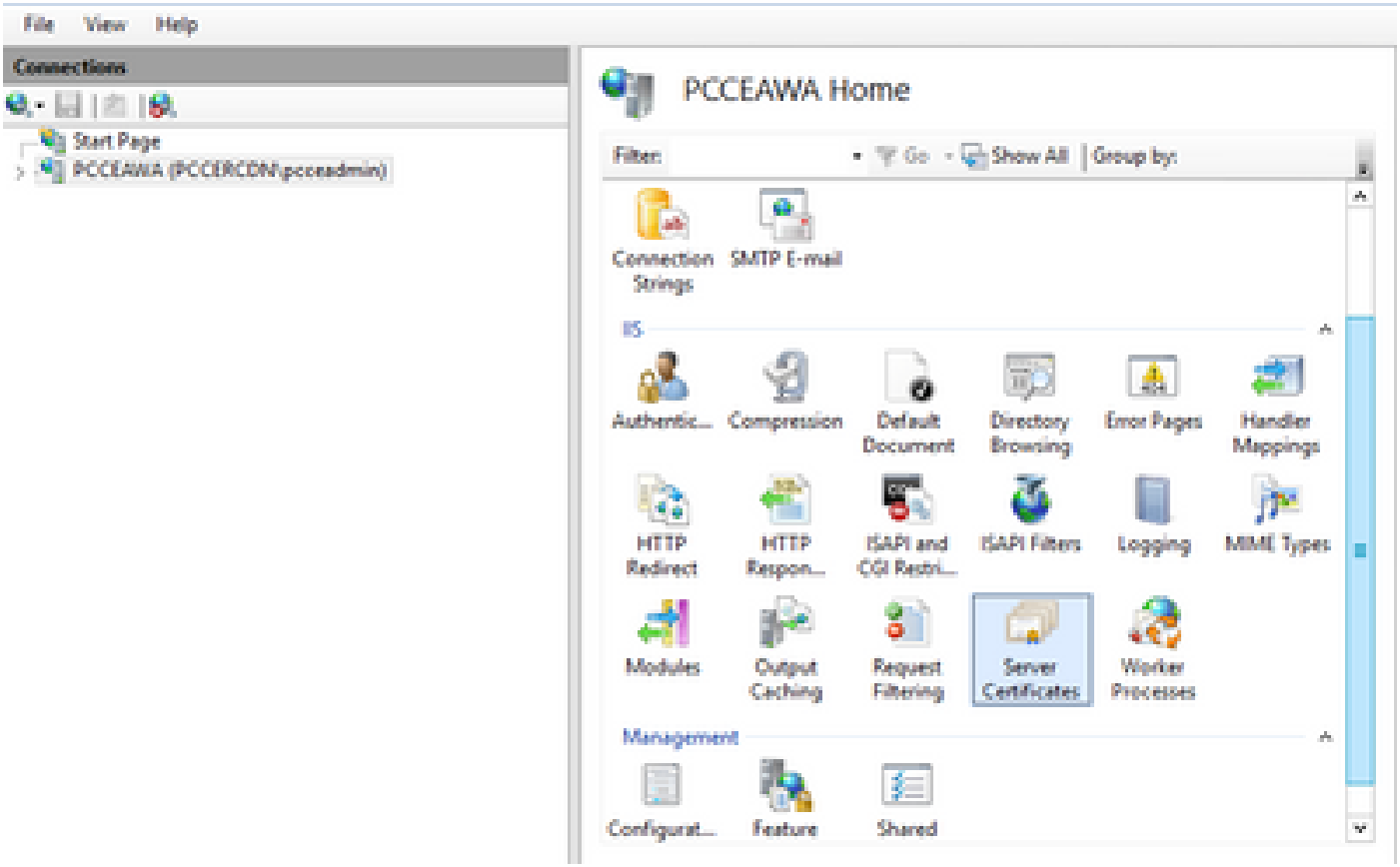
Passaggio 1. Firmare il certificato su una CA.

Nota: verificare che il modello di certificato utilizzato dalla CA includa l'autenticazione client e server.

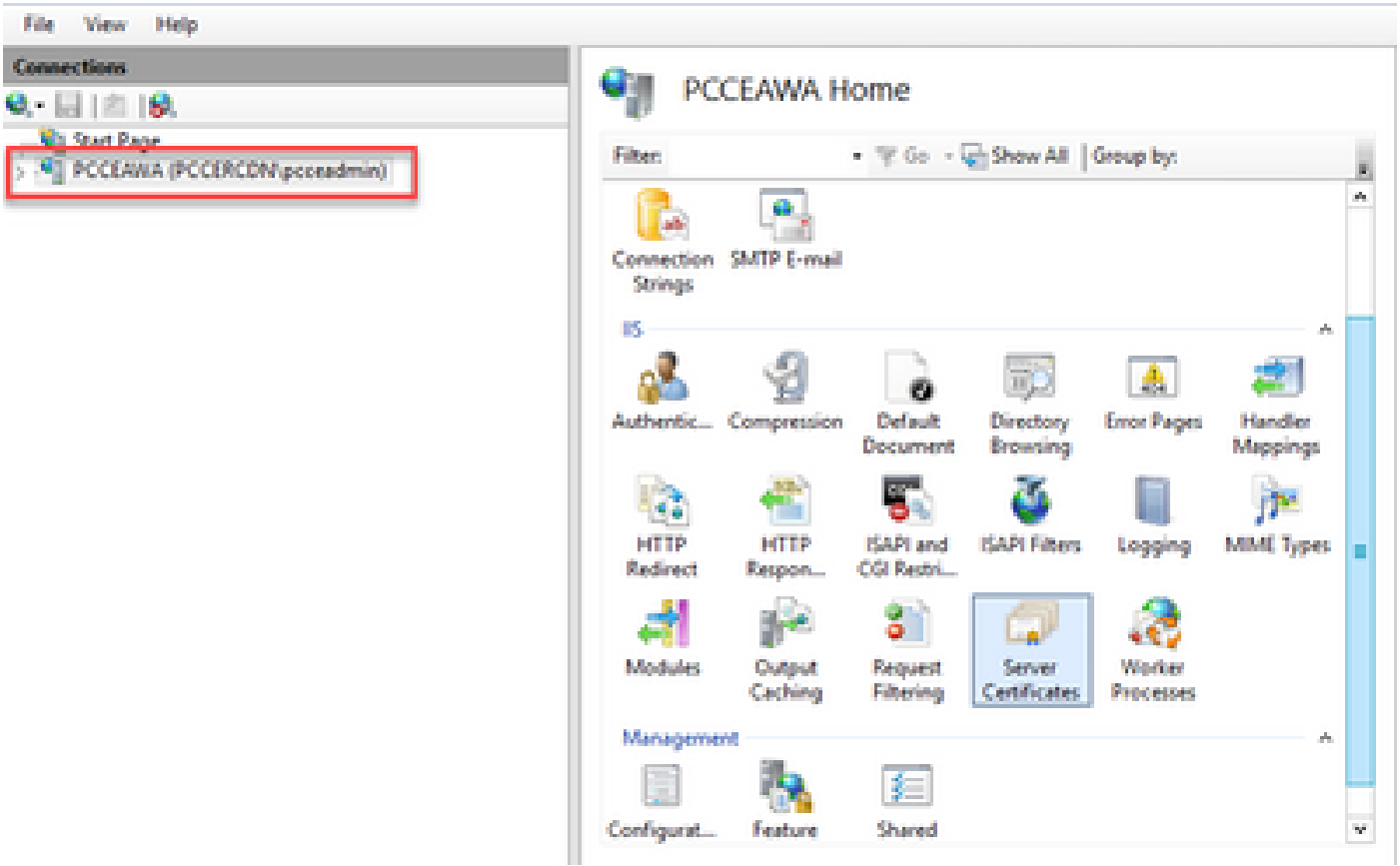
Passaggio 2. Ottenere i certificati CA firmati dall'autorità di certificazione (radice, applicazione e intermedio, se presenti).

3. Caricare i certificati firmati dalla CA

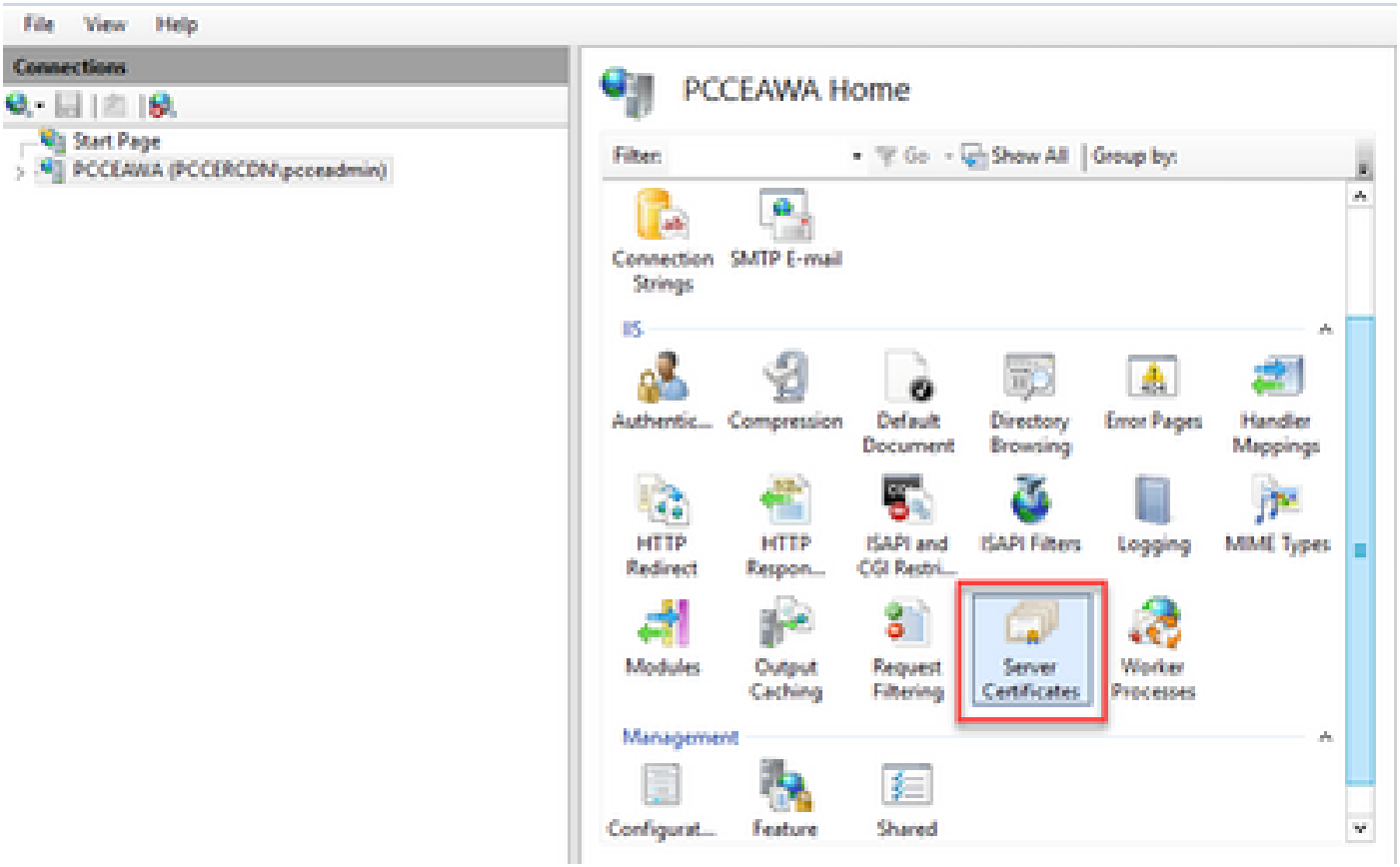
Passaggio 1. Accedere a Windows e scegliere Pannello di controllo > Strumenti di amministrazione > Gestione Internet Information Services (IIS).



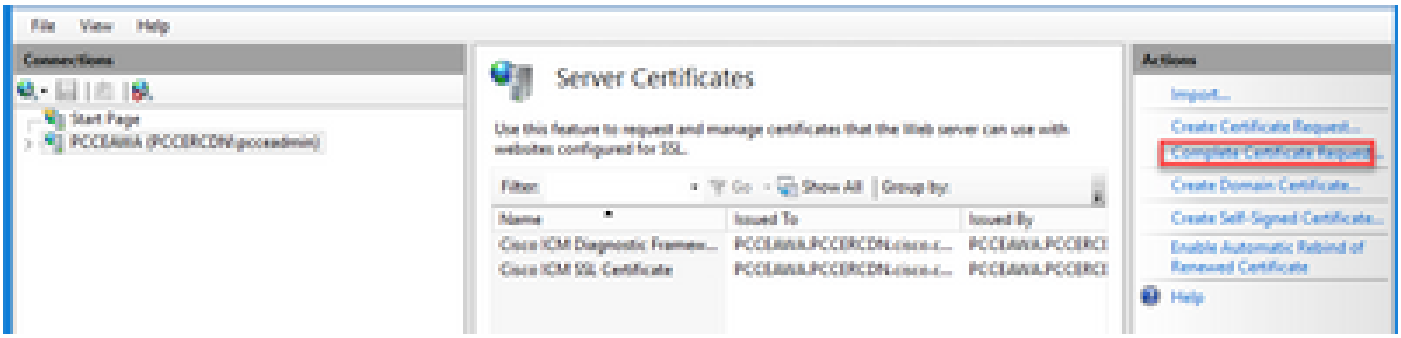
Passaggio 2. Nel riquadro Connessioni fare clic sul nome del server.



Passaggio 3. Nell'area IIS fare doppio clic su Certificati server.



Passaggio 4. Nel riquadro Azioni fare clic su Completa richiesta certificato.



Passaggio 5. Nella finestra di dialogo Completa richiesta certificato completare i campi seguenti:

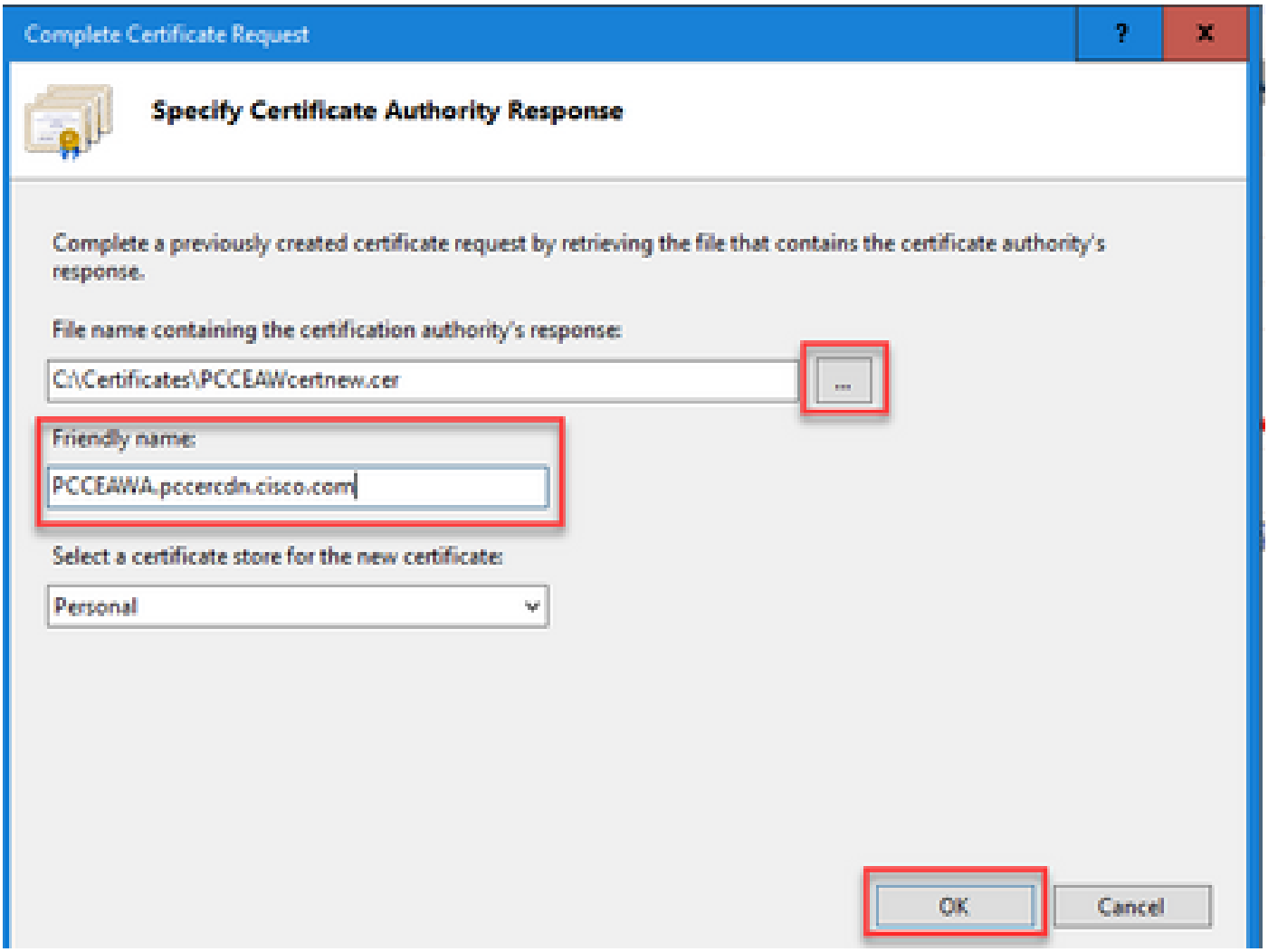
Nel campo Nome file contenente la risposta dell'Autorità di certificazione fare clic sul pulsante ....

Individuare il percorso in cui è archiviato il certificato dell'applicazione firmato e quindi fare clic su Apri.

Nota: se si tratta di un'implementazione di CA a 2 livelli e il certificato radice non è già presente nell'archivio certificati del server, è necessario caricare la radice nell'archivio di Windows prima di importare il certificato firmato. Fare riferimento a questo documento se è necessario caricare la CA radice nel Windows Store https://docs.microsoft.com/en-us/skype-sdk/sdn/articles/installing-the-trusted-root-certificate.

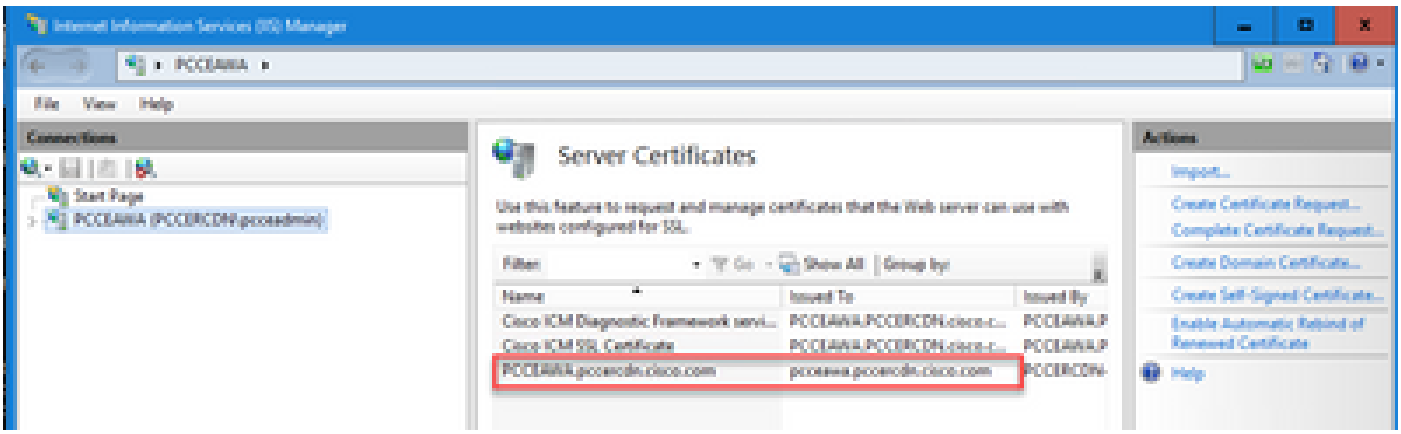
Nel campo Nome descrittivo immettere il nome di dominio completo (FQDN) del server o qualsiasi

nome significativo. Verificare che l'elenco a discesa Selezionare un archivio certificati per il nuovo certificato rimanga Personale.



Passaggio 6. Scegliere OK per caricare il certificato.

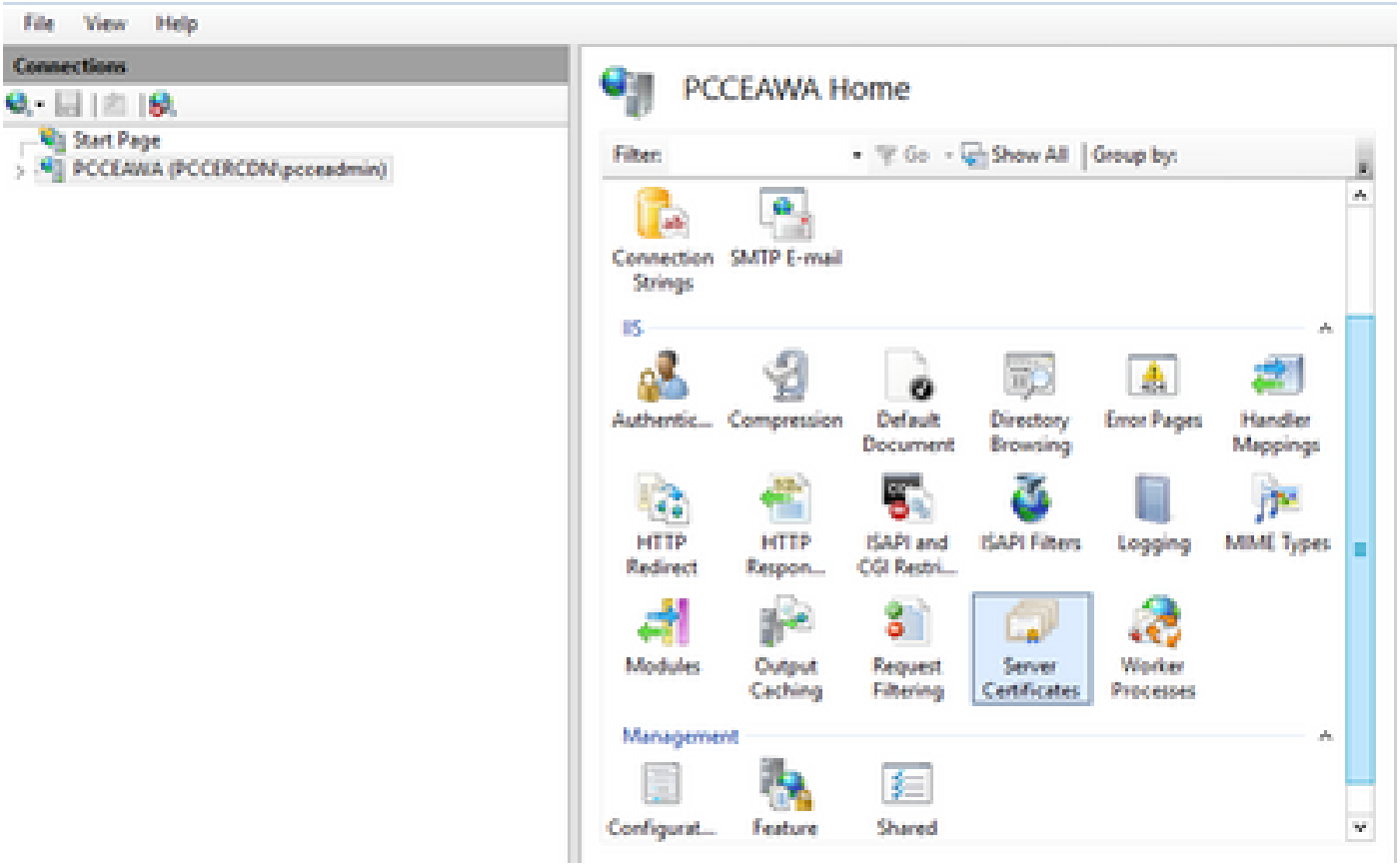
Se il caricamento del certificato ha esito positivo, il certificato verrà visualizzato nel riquadro Certificati server.



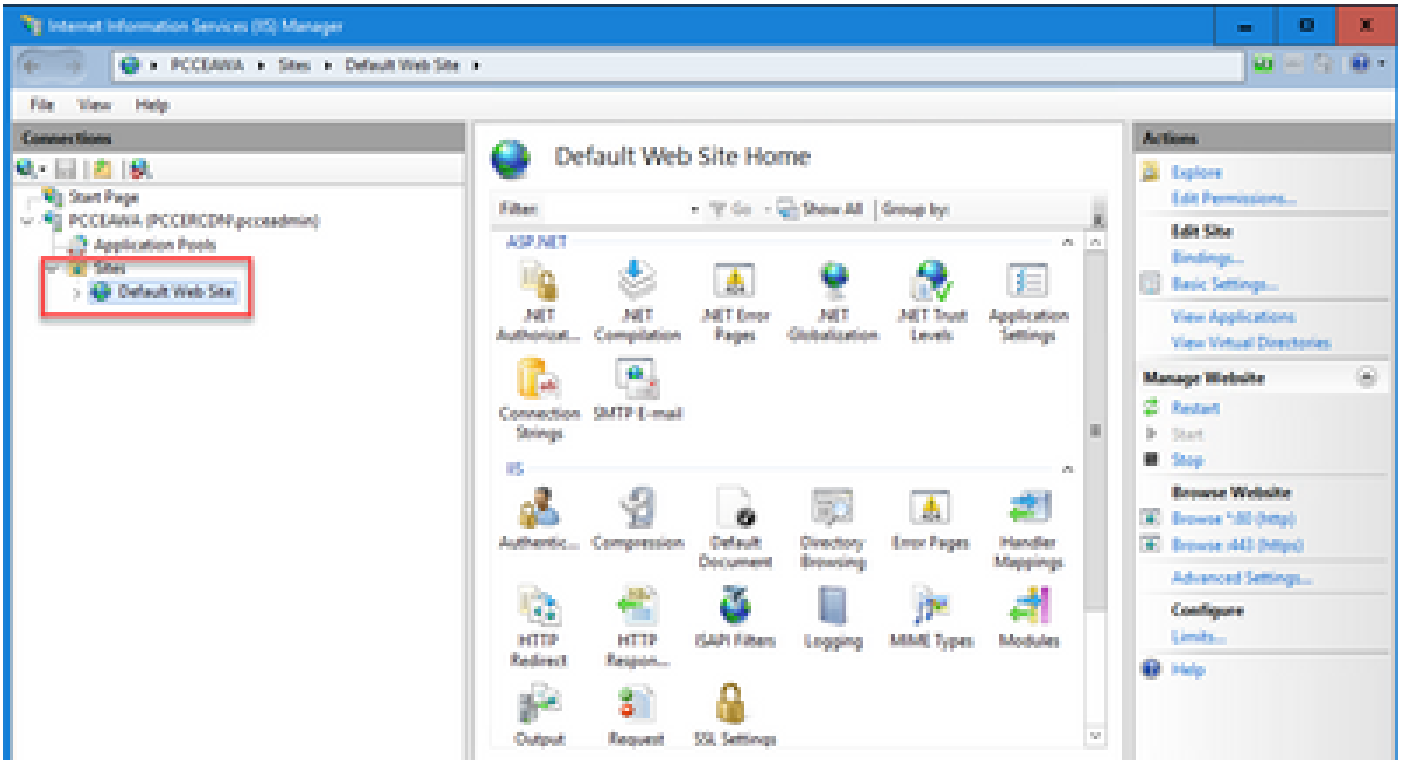
4. Associare il certificato firmato dalla CA a IIS

In questa procedura viene illustrato come associare un certificato firmato da una CA in Gestione IIS.

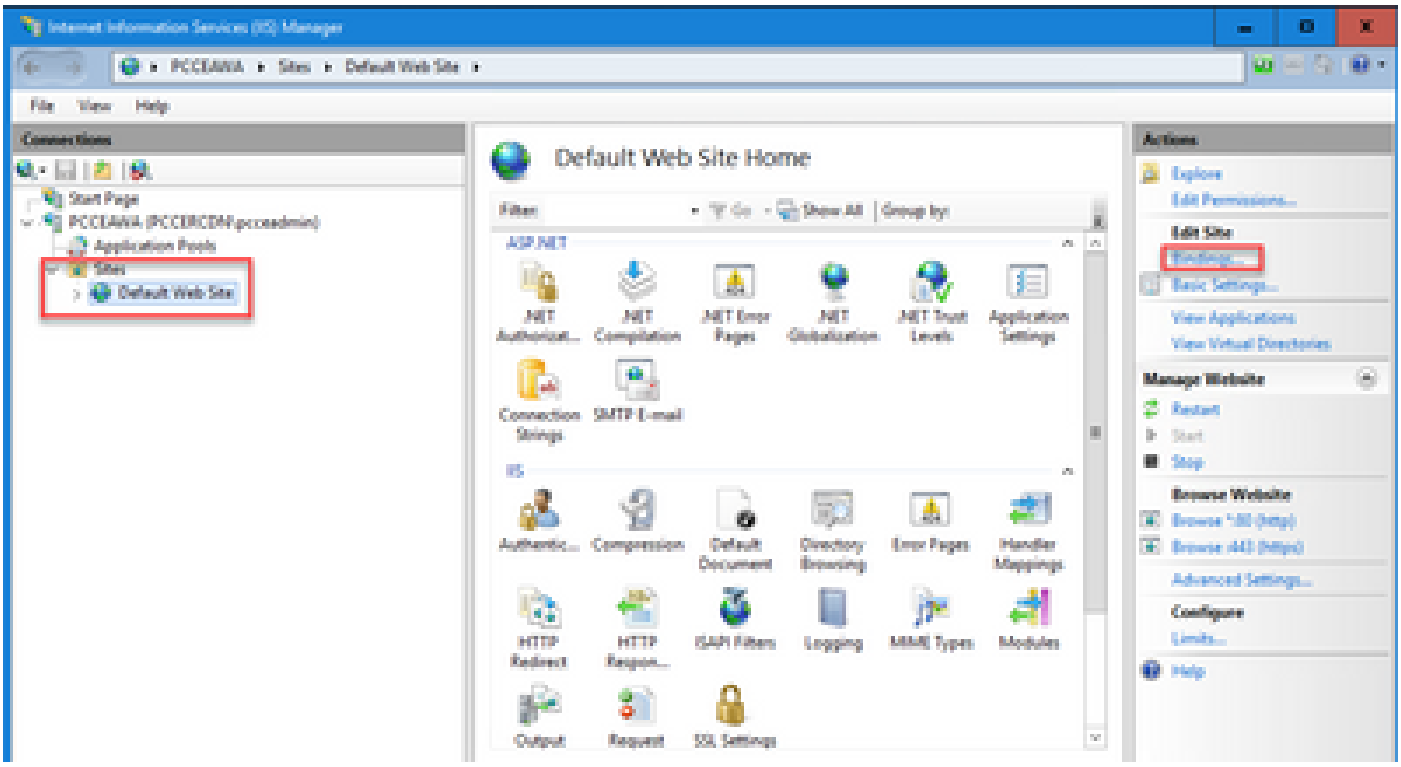
Passaggio 1. Accedere a Windows e scegliere Pannello di controllo > Strumenti di amministrazione > Gestione Internet Information Services (IIS).



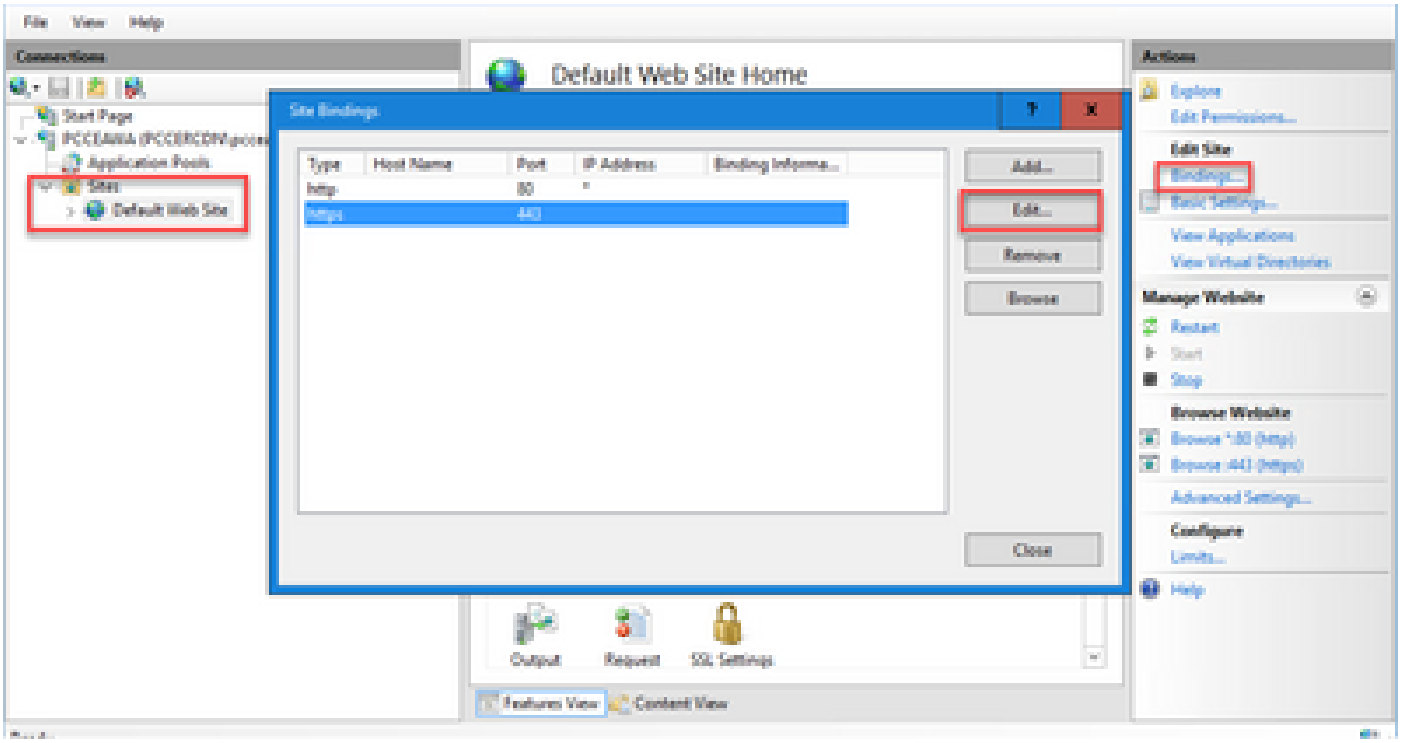
Passaggio 2. Nel riquadro Connessioni scegliere <nome_server> > Siti > Sito Web predefinito.



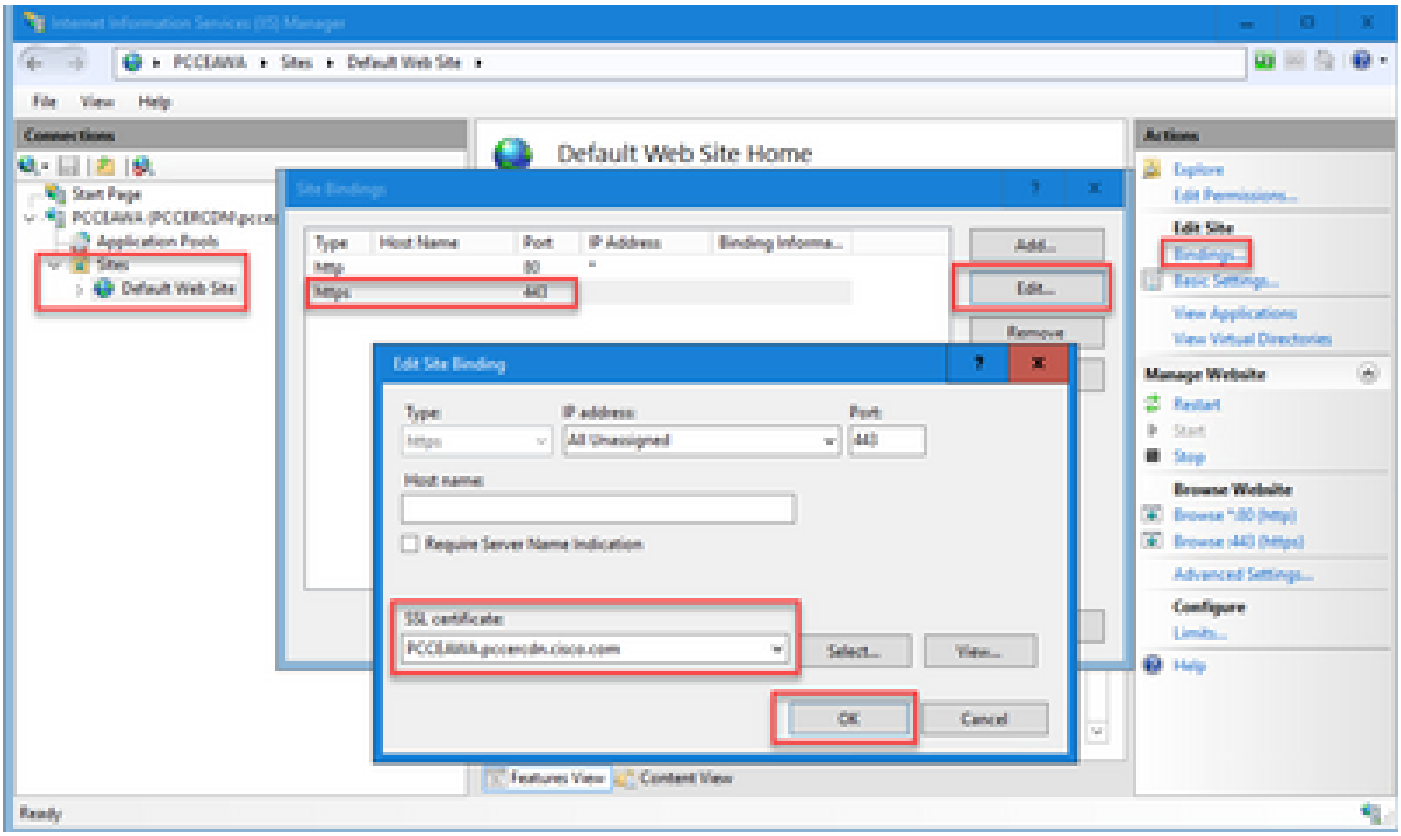
Passaggio 3. Nel riquadro Azioni fare clic su Associazioni....



Passaggio 4. Fare clic sul tipo https con porta 443, quindi su Modifica....

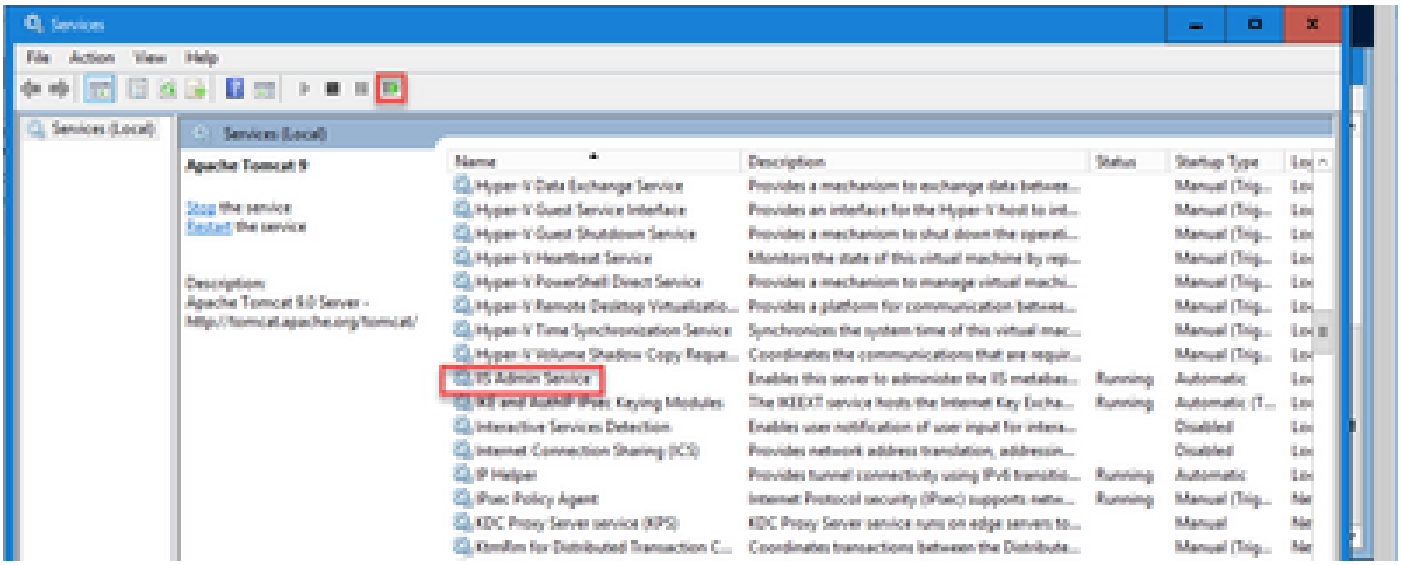


Passaggio 5. Dall'elenco a discesa Certificato SSL selezionare il certificato con lo stesso nome descrittivo indicato nel passaggio precedente.



Passaggio 6. Fare clic su OK.

Passaggio 7. Passare a Start > Esegui > services.msc e riavviare il servizio Amministrazione di IIS.



Se IIS viene riavviato correttamente, gli avvisi relativi agli errori dei certificati non vengono visualizzati all'avvio dell'applicazione.

5. Associare il certificato firmato dalla CA al portico di diagnostica

In questa procedura viene illustrato come associare un certificato firmato da un'autorità di certificazione nel portico di diagnostica.

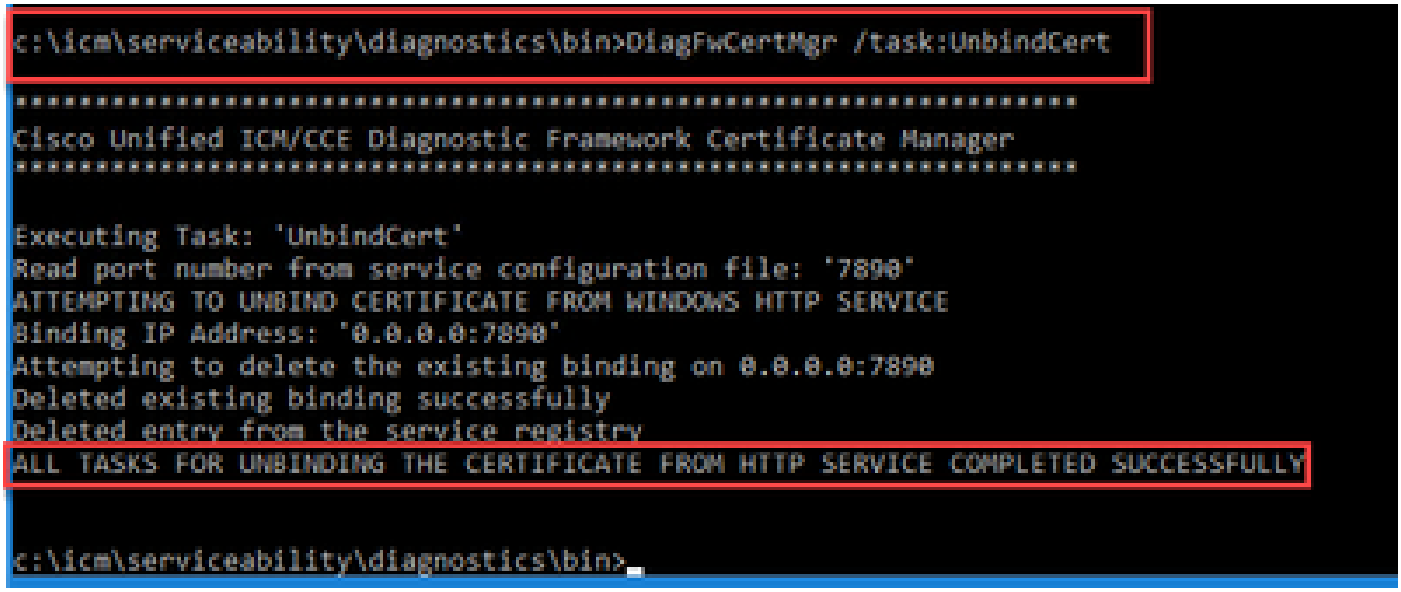
Passaggio 1. Aprire il prompt dei comandi (Esegui come amministratore).

Passaggio 2. Passare alla home directory di Diagnostic Portico. Eseguire questo comando:

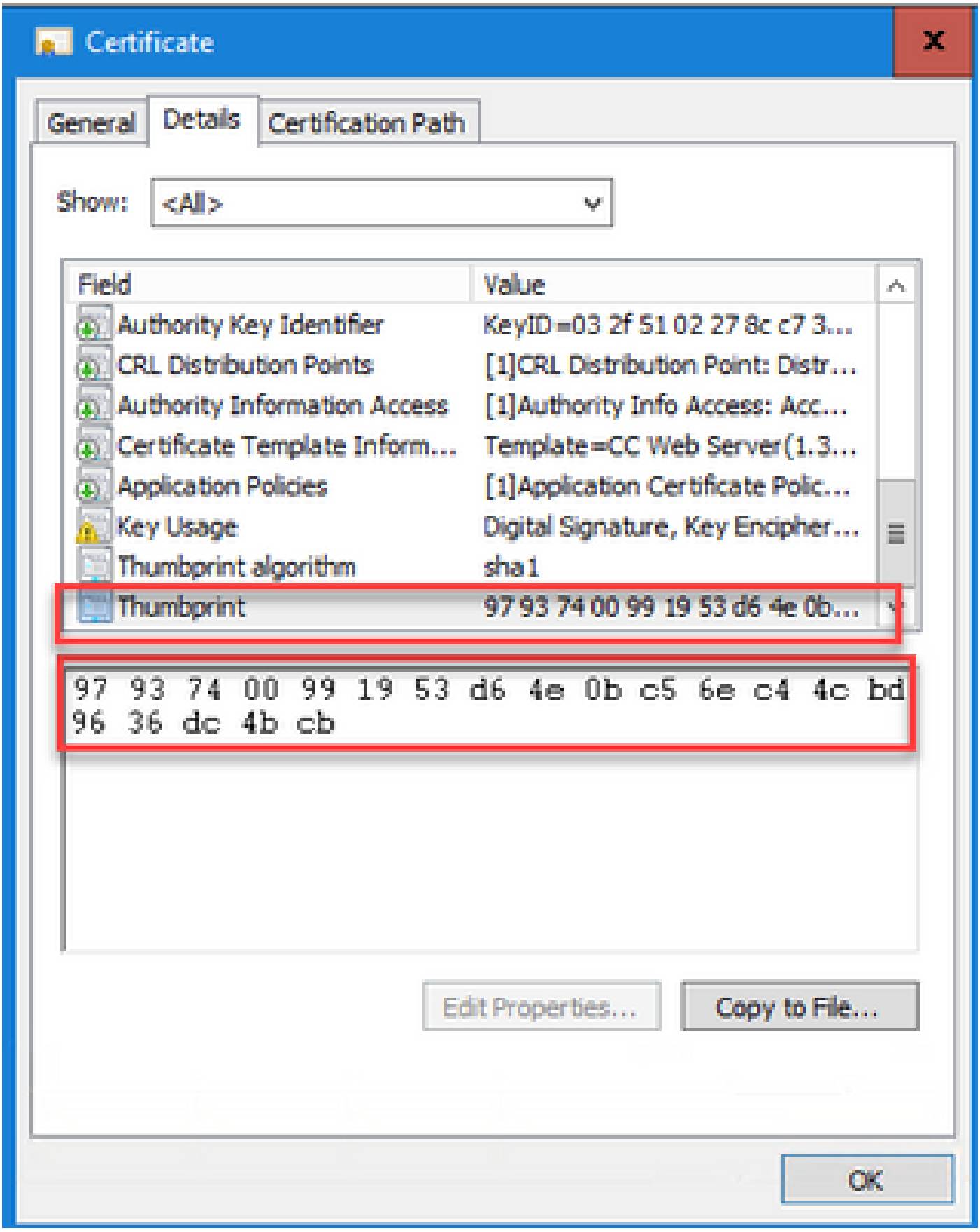
```
cd c:\icm\serviceability\diagnostics\bin
```

Passaggio 3. Rimuove il binding del certificato corrente al portico di diagnostica. Eseguire questo comando:

```
DiagFwCertMgr /task:UnbindCert
```

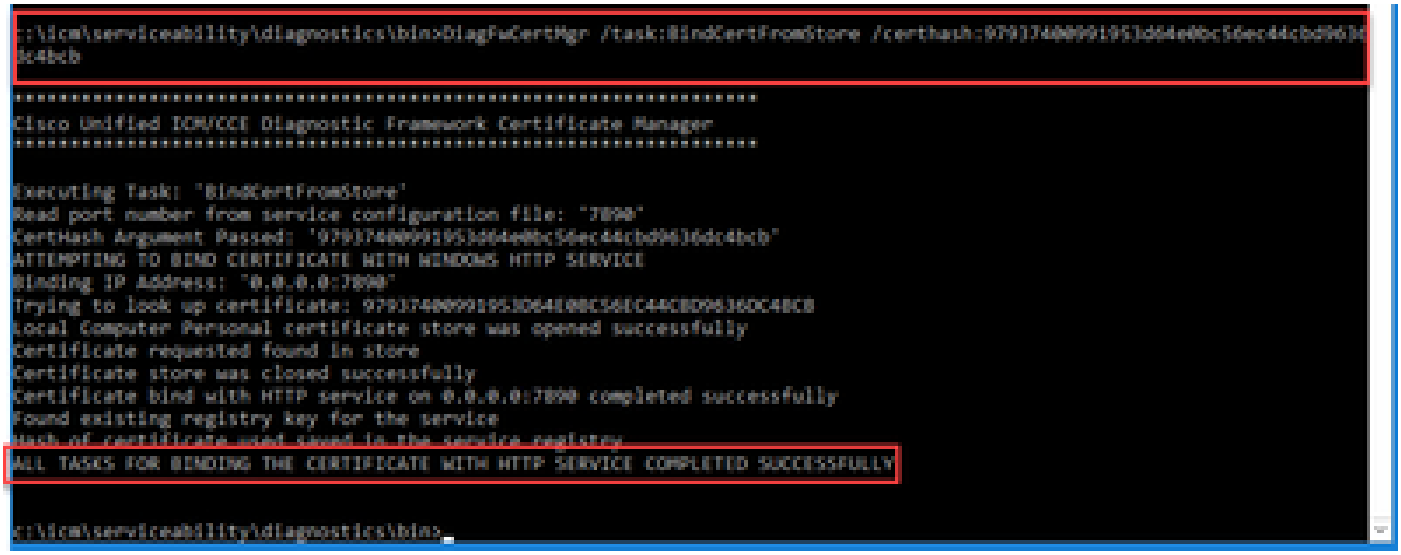


Passaggio 4. Aprire il certificato firmato e copiare il contenuto hash (senza spazi) del campo Identificazione personale.



Passaggio 5. Eseguire questo comando e incollare il contenuto hash.

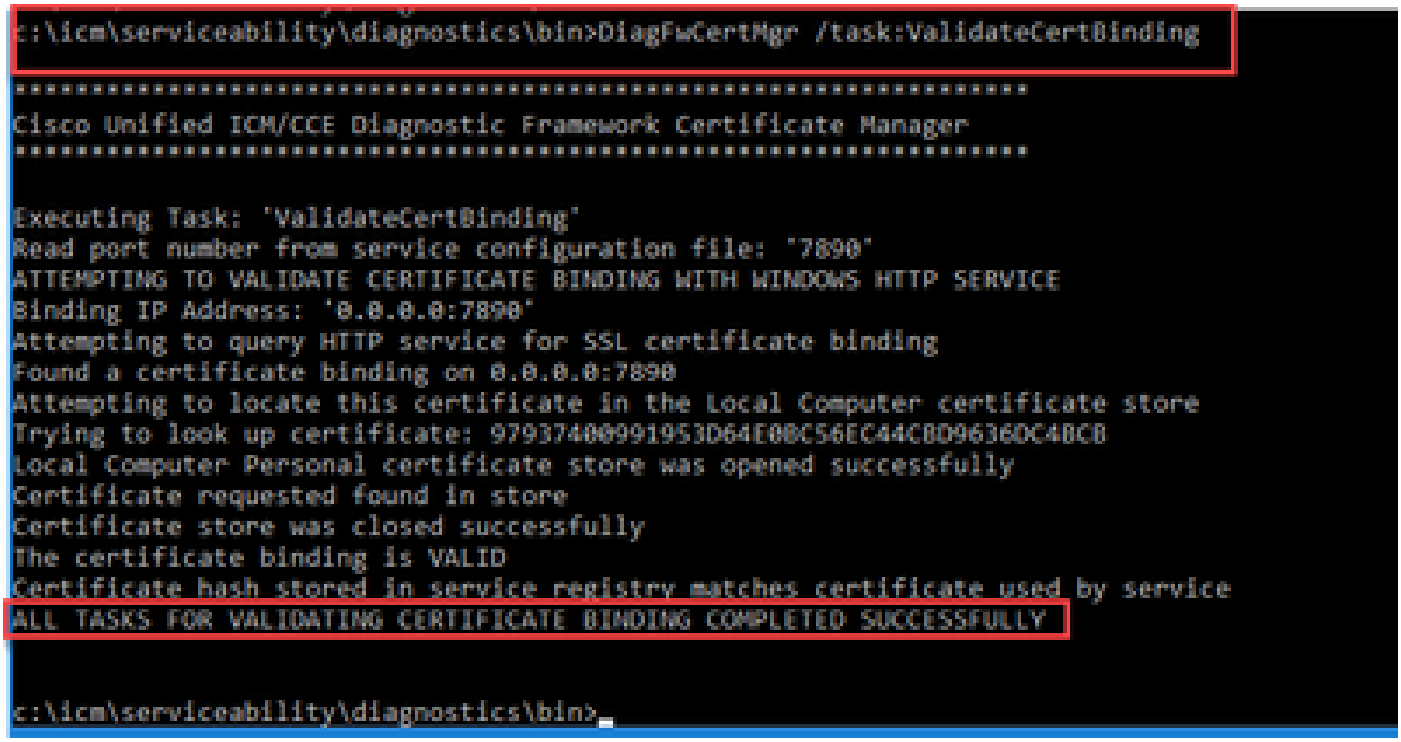
```
DiagFwCertMgr /task:BindCertFromStore /certhash:<hash_value>
```



Se il binding dei certificati ha esito positivo, viene visualizzato il messaggio Il binding dei certificati è VALIDO.

Passaggio 6. Convalida se il binding dei certificati è riuscito. Eseguire questo comando:

```
DiagFwCertMgr /task:ValidateCertBinding
```



Nota: per impostazione predefinita, DiagFwCertMgr utilizza la porta 7890.

Se il binding dei certificati ha esito positivo, viene visualizzato il messaggio Il binding dei certificati

è VALIDO.

Passaggio 7. Riavviare il servizio Framework di diagnostica. Eseguire i seguenti comandi:

```
net stop DiagFwSvc
net start DiagFwSvc
```

Se Diagnostic Framework viene riavviato correttamente, gli avvisi relativi agli errori dei certificati non vengono visualizzati all'avvio dell'applicazione.

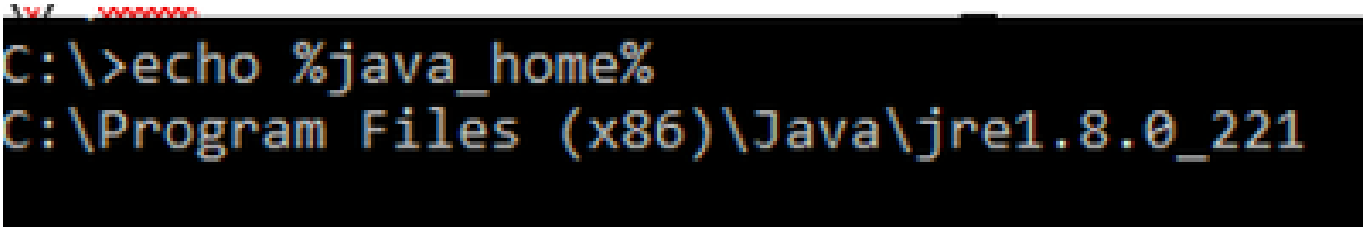
6. Importare il certificato principale e intermedio in Java Keystore

---

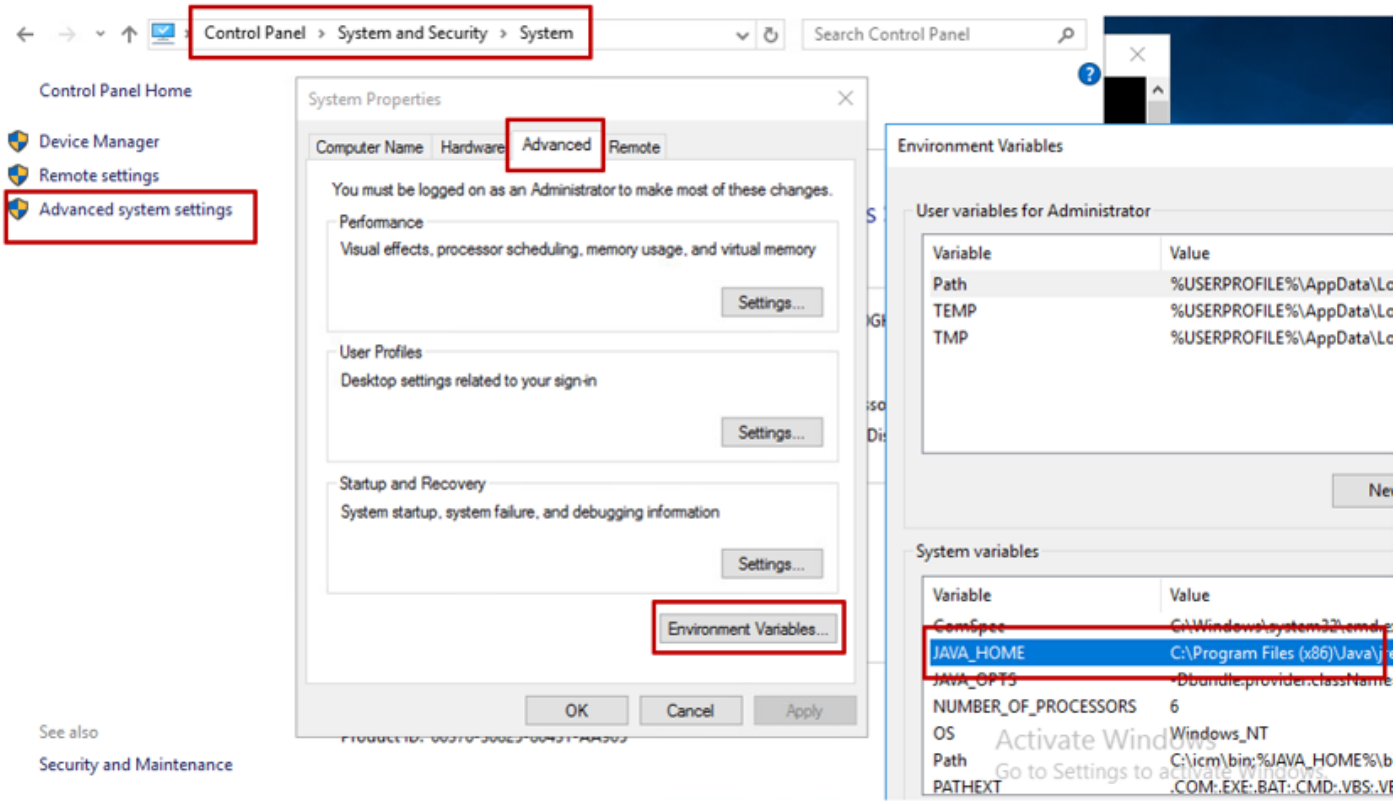
⚠ Attenzione: prima di iniziare, è necessario eseguire il backup del keystore ed eseguire i comandi dalla java home come amministratore.

Passaggio 1. Conoscere il percorso della directory principale Java per verificare la posizione in cui è ospitato lo strumento chiave Java. Ci sono due modi per trovare il percorso di casa java.

Opzione 1: comando CLI: echo %JAVA_HOME%



Opzione 2: Manualmente tramite Impostazioni di sistema avanzate, come mostrato nell'immagine



Nota: in UCCE 12.5 il percorso predefinito è C:\Program Files (x86)\Java\jre1.8.0_221\bin. Tuttavia, se è stato utilizzato il programma di installazione 12.5(1a) o se è installato 12.5 ES55 (obbligatorio OpenJDK ES), utilizzare CCE_JAVA_HOME anziché JAVA_HOME poiché il percorso dell'archivio dati è stato modificato con OpenJDK. Per ulteriori informazioni sulla migrazione di OpenJDK in CCE e CVP, consultare i seguenti documenti: Install and Migrate to OpenJDK in CCE 2.5(1) e Install and Migrate to OpenJDK in CVP 12.5(1).

Passaggio 2. Eseguire il backup del file cacerts dalla cartella C:\Program Files (x86)\Java\jre1.8.0_221\lib\security. È possibile copiarlo in un'altra posizione.

Passaggio 3. Aprire una finestra di comando come Amministratore per eseguire il comando:

```
keytool.exe -keystore ./cacerts -import -file <path where the Root, or Intermediate certificate are sto
```

Nota: i certificati specifici richiesti dipendono dalla CA utilizzata per firmare i certificati. In una CA a due livelli, tipica delle CA pubbliche e più sicura delle CA interne, è necessario importare i certificati radice e intermedi. In una CA standalone senza componenti intermedi, generalmente presente in un'autorità di certificazione lab o in una CA interna più semplice, è sufficiente importare solo il certificato radice.

Soluzione CVP

1. Genera certificati con FQDN

In questa procedura viene illustrato come generare certificati con FQDN per i servizi Web Service Manager (WSM), Voice XML (VXML), Call Server e Operations Management (OAMP).

Nota: quando si installa CVP, il nome del certificato include solo il nome del server e non il nome di dominio completo, pertanto è necessario rigenerare i certificati.

Attenzione: prima di iniziare, eseguire questa operazione:
1. Ottenere la password del keystore. Eseguire il comando: more %CVP_HOME%\conf\security.properties. La password è necessaria per eseguire i comandi keytool.
2. Copiare la cartella %CVP_HOME%\conf\security in un'altra cartella.
3. Aprire una finestra di comando come Amministratore per eseguire i comandi.

Server CVP

Passaggio 1. Per eliminare i certificati dei server CVP, eseguire i comandi seguenti:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -a

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -a

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -a
```

Quando richiesto, immettere la password del keystore.

Passaggio 2. Per generare il certificato WSM eseguire questo comando:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai
```

Quando richiesto, immettere la password del keystore.

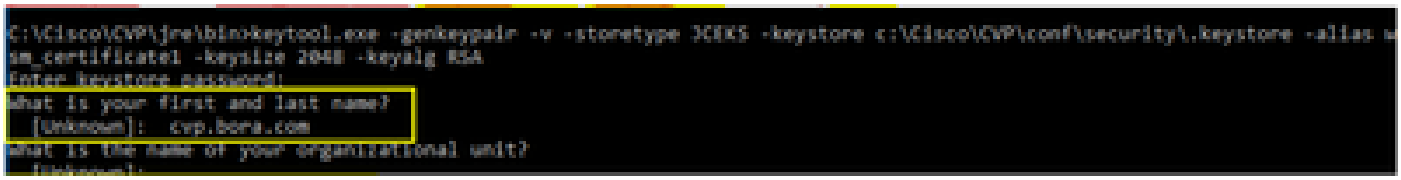
Nota: per impostazione predefinita, i certificati vengono generati per due anni. Utilizzare -valid XXXX per impostare la data di scadenza per la rigenerazione dei certificati. In caso contrario, i certificati saranno validi per 90 giorni e dovranno essere firmati da una CA prima di questo periodo. Per la maggior parte di questi certificati, 3-5 anni devono essere un periodo di convalida ragionevole.

Di seguito sono riportati alcuni input di validità standard:

Un anno	365
Due anni	730
Tre anni	1095
Quattro anni	1460
Cinque anni	1895
Dieci anni	3650

⚠ Attenzione: in 12.5 i certificati devono essere SHA 256, Key Size 2048 e encryption Algorithm RSA, utilizzare questi parametri per impostare i seguenti valori: -keyalg RSA e -keysize 2048. È importante che i comandi del keystore CVP includano il parametro -storetype JCEKS. In caso contrario, il certificato, la chiave o, peggio, il keystore potrebbe danneggiarsi.

Specificare il nome di dominio completo (FQDN) del server, alla domanda qual è il nome e il cognome?



Rispondere alle seguenti domande:

Qual è il nome dell'unità organizzativa?

[Sconosciuto]: <specificare OU>

Qual è il nome dell'organizzazione?

[Sconosciuto]: <specificare il nome dell'organizzazione>

Indicare il nome della città o della località.

[Sconosciuto]: <specificare il nome della città/località>

Qual è il nome della provincia?

[Sconosciuto]: <specificare il nome della provincia>

Qual è il codice paese di due lettere per questo apparecchio?

[Sconosciuto]: <specifica il codice paese a due lettere>

Specificare yes per i due input successivi.

Passaggio 3. Eseguire la stessa procedura per vxml_certificate e callserver_certificate:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai
```

Server di report CVP

Passaggio 1. Per eliminare i certificati di WSM e del server di report, eseguire i comandi seguenti:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -a
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -a
```

Quando richiesto, immettere la password del keystore.

Passaggio 2. Per generare il certificato WSM eseguire questo comando:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai
```

Quando richiesto, immettere la password del keystore.

Specificare il nome di dominio completo (FQDN) del server per la query che cos'è il nome e il cognome? e continuare con la stessa procedura utilizzata per i server CVP.

Passaggio 3. Eseguire la stessa procedura per callserver_certificate:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai
```

CVP OAMP (distribuzione UCCE)

Poiché nella soluzione PCCE versione 12.x tutti i componenti della soluzione sono controllati da

SPOG e OAMP non è installato, questi passaggi sono necessari solo per una soluzione di distribuzione UCCE.

Passaggio 1. Per eliminare i certificati del server WSM e OAMP, eseguire i comandi seguenti:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -a

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -a
```

Quando richiesto, immettere la password del keystore.

Passaggio 2. Per generare il certificato WSM eseguire questo comando:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai
```

Quando richiesto, immettere la password del keystore.

Specificare il nome di dominio completo (FQDN) del server per la query che cos'è il nome e il cognome? e continuare con la stessa procedura utilizzata per i server CVP.

Passaggio 3. Eseguire la stessa procedura per oamp_certificate:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai
```

Quando richiesto, immettere la password del keystore.

2. Generare il CSR

Nota: il browser conforme allo standard RFC5280 richiede che in ogni certificato sia incluso il nome alternativo del soggetto (SAN, Subject Alternative Name). A tale scopo, è possibile utilizzare il parametro -ext con SAN durante la generazione di CSR.

Nome alternativo soggetto

Il parametro -ext consente all'utente di utilizzare estensioni specifiche. Nell'esempio riportato viene aggiunto un nome alternativo del soggetto (SAN) con il nome di dominio completo (FQDN) del server e localhost. È possibile aggiungere ulteriori campi SAN come valori separati da virgole.

I tipi di SAN validi sono:

```
ip:192.168.0.1
dns:myserver.mydomain.com
email:name@mydomain.com
```

Ad esempio: -ext san=dns:mycvp.mydomain.com,dns:localhost

Server CVP

Passaggio 1. Generare la richiesta di certificato per l'alias. Eseguire questo comando e salvarlo in un file (ad esempio, wsm_certificate):

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -
```

Quando richiesto, immettere la password del keystore.

Passaggio 2. Eseguire la stessa procedura per vxml_certificate e callserver_certificate:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -
```

Quando richiesto, immettere la password del keystore.

Server di report CVP

Passaggio 1. Generare la richiesta di certificato per l'alias. Eseguire questo comando e salvarlo in un file (ad esempio, wsmreport_certificate):

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -
```

Quando richiesto, immettere la password del keystore.

Passaggio 2. Eseguire la stessa procedura per callserver_certificate:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -
```

Quando richiesto, immettere la password del keystore.

CVP OAMP (distribuzione UCCE)

Passaggio 1. Generare la richiesta di certificato per l'alias. Eseguire questo comando e salvarlo in un file, ad esempio oamp_certificate:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -
Ensure to replace "mycvp.mydomain.com" with your OAMP FQDN.
Enter the keystore password when prompted.
```

Passaggio 2. Eseguire la stessa procedura per oamp_certificate:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -
```

Quando richiesto, immettere la password del keystore.

3. Ottenere i certificati firmati CA

Passaggio 1. Firmare i certificati su una CA (WSM, Callserver e server VXML per il server CVP; WSM e OAMP per il server CVP OAMP e WSM e Callserver per il server di report).

Passaggio 2. Scaricare i certificati dell'applicazione e il certificato radice dall'autorità CA.

Passaggio 3. Copiare il certificato radice e i certificati firmati dalla CA nella cartella %CVP_HOME%\conf\security\ di ogni server.

4. Importazione dei certificati firmati dalla CA

Applica questi passaggi a tutti i server della soluzione CVP. Solo i certificati per i componenti su tale server devono avere il certificato firmato dalla CA importato.

Passaggio 1. Importare il certificato radice. Eseguire questo comando:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v
```

Quando richiesto, immettere la password del keystore. Al prompt Considera attendibile il certificato digitare Sì.

Se è presente un certificato intermedio, eseguire questo comando:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias intermediate_ca -file
```

Quando richiesto, immettere la password del keystore. Al prompt Considera attendibile il certificato digitare Sì.

Passaggio 2. Importare il modulo WSM firmato dalla CA per il certificato server (CVP, Reporting and OAMP). Eseguire questo comando:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v
```

Quando richiesto, immettere la password del keystore. Al prompt Considera attendibile il certificato digitare Sì.

Passaggio 3. Nei server CVP e nei server di report importare il certificato firmato dalla CA del server di chiamata. Eseguire questo comando:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v
```

Quando richiesto, immettere la password del keystore. Al prompt Considera attendibile il certificato digitare Sì.

Passaggio 4. Nei server CVP importare il certificato firmato dalla CA del server VXML. Eseguire questo comando:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v
```

Passaggio 5. Nel server CVP OAMP (solo per UCCE) importare il certificato firmato dalla CA del server OAMP. Eseguire questo comando:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v
```

Passaggio 6. Riavviare i server.

Nota: nella distribuzione UCCE, assicurarsi di aggiungere i server (Reporting, CVP Server e così via) in CVP OAMP con il nome di dominio completo fornito durante la generazione del CSR.

Server VOS

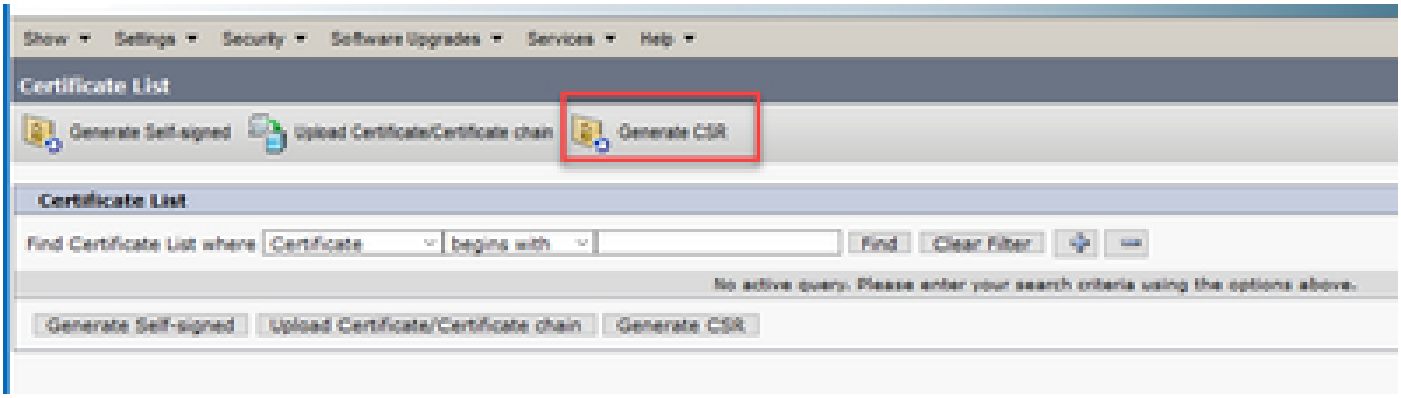
1. Genera certificato CSR

In questa procedura viene illustrato come generare il certificato CSR Tomcat da una piattaforma basata su VOS (Cisco Voice Operating System). Questo processo è applicabile a tutte le applicazioni basate su VOS, quali:

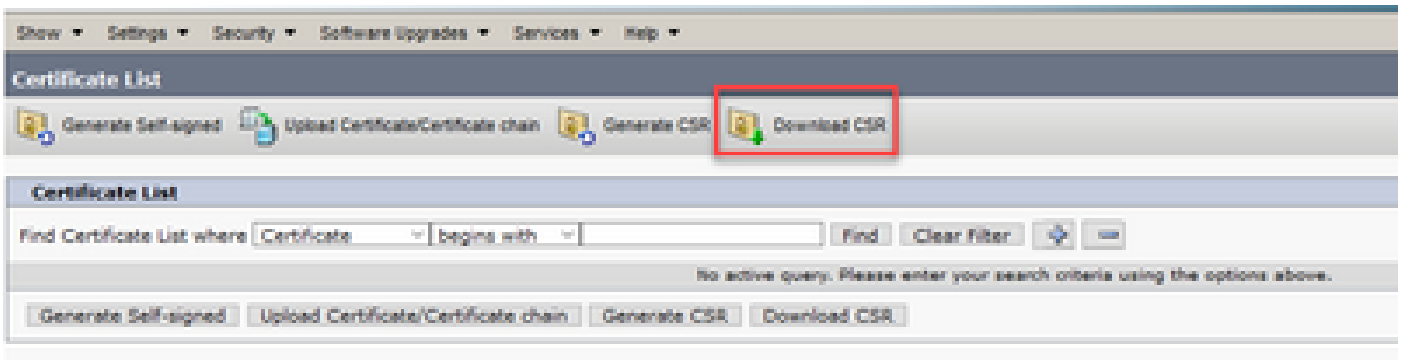
- CUCM
- Finesse
- CUIC \ Live Data (LD) \Identity Server(IDS)
- Cloud Connect
- Cisco VB

Passaggio 1. Passare alla pagina di amministrazione del sistema operativo Cisco Unified Communications: https://FQDN:<8443 o 443>/cmplatform.

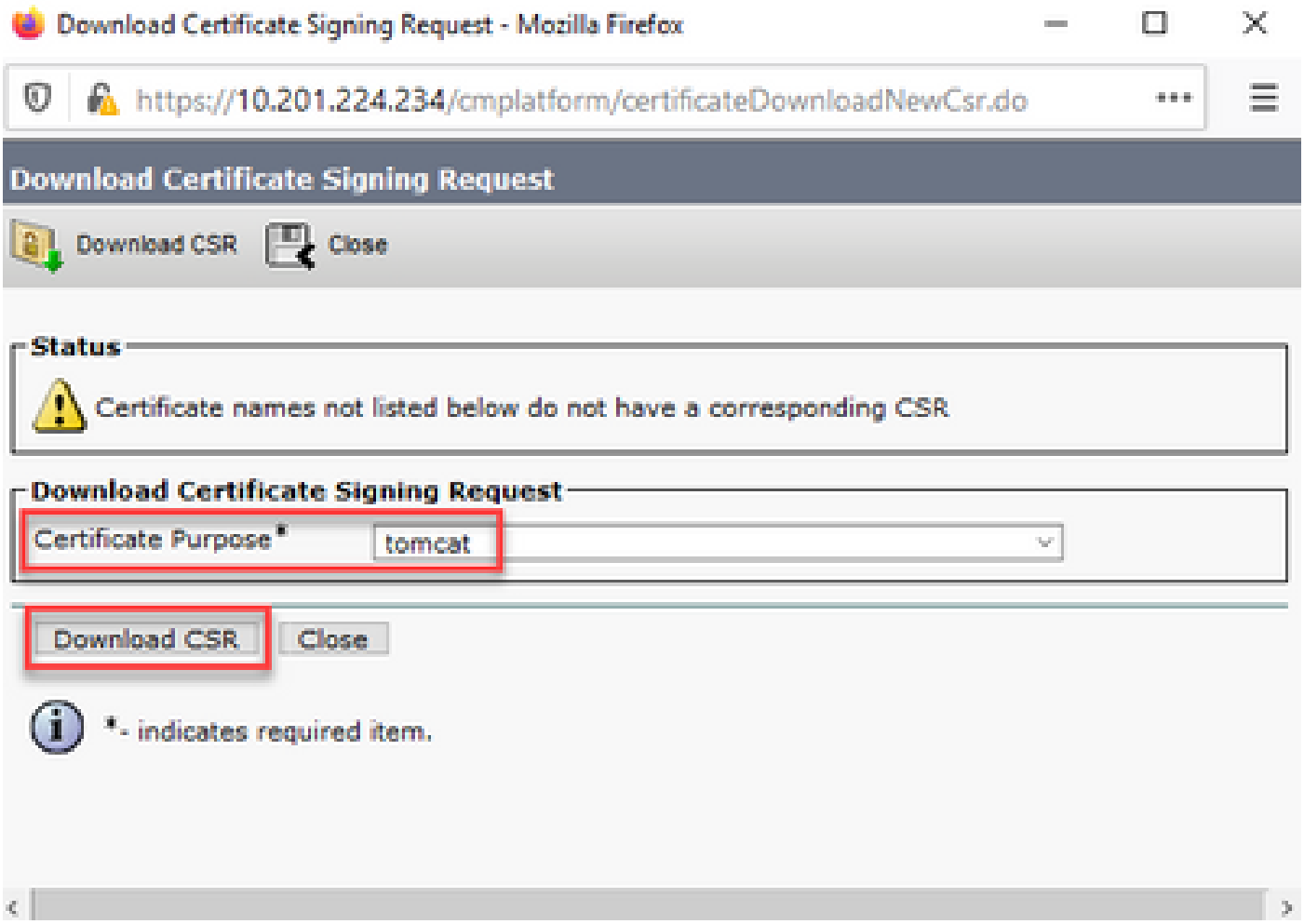
Passaggio 2. Passare a Sicurezza > Gestione certificati e selezionare Genera CSR.



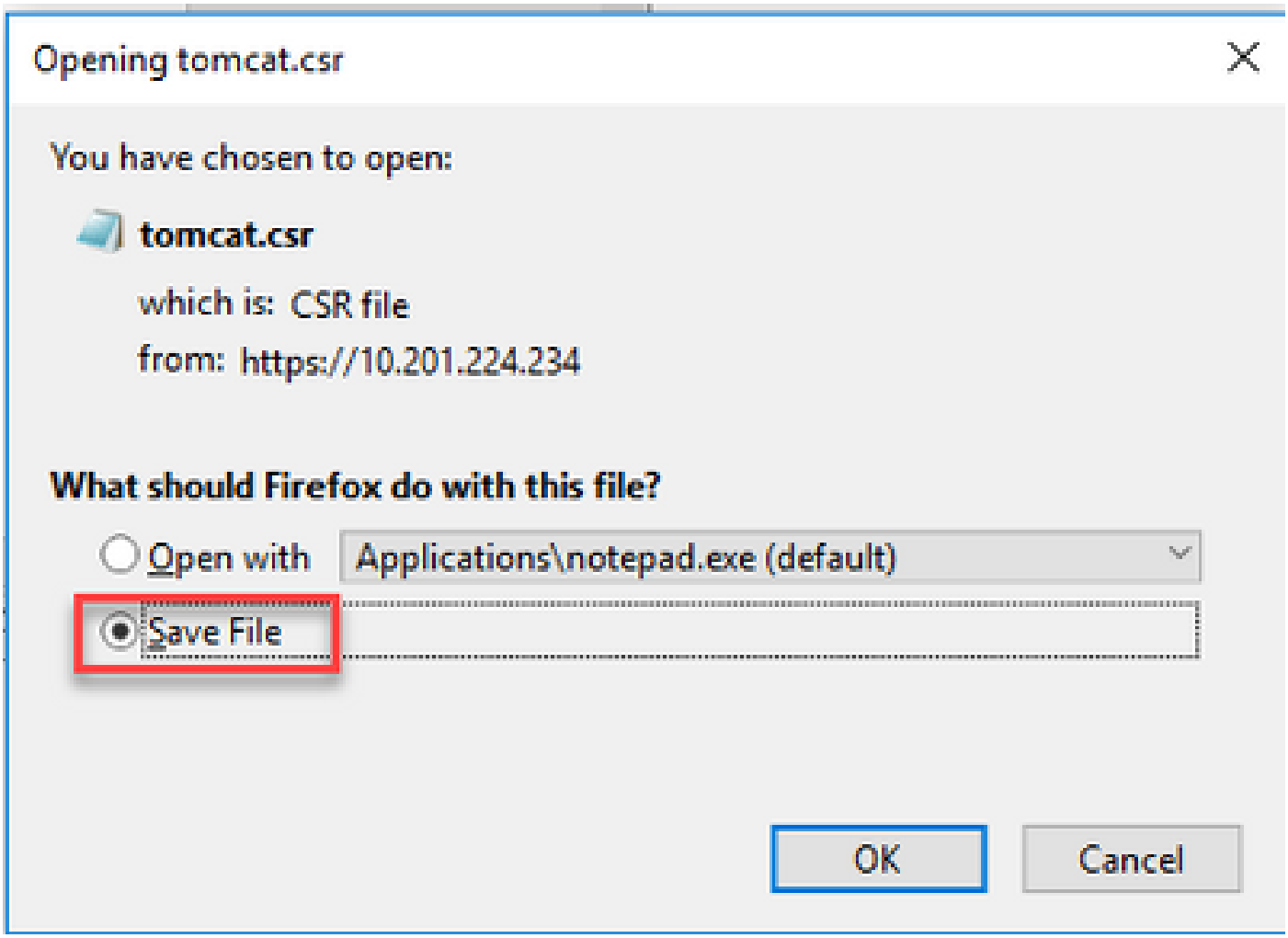
Passaggio 3. Una volta generato il certificato CSR, chiudere la finestra e selezionare Download CSR.



Passaggio 4. Verificare che lo scopo del certificato sia tomcat e fare clic su Download CSR.



Passaggio 5. Fare clic su Salva file. Il file viene salvato nella cartella Download.



2. Ottenere i certificati firmati dalla CA

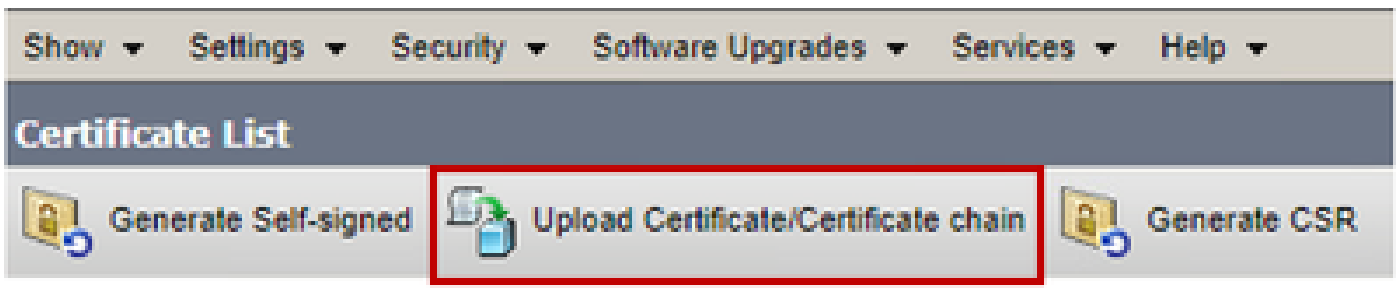
Passaggio 1. Firmare il certificato tomcat esportato su una CA.

Passaggio 2. Scaricare l'applicazione e la radice certificata dall'autorità CA.

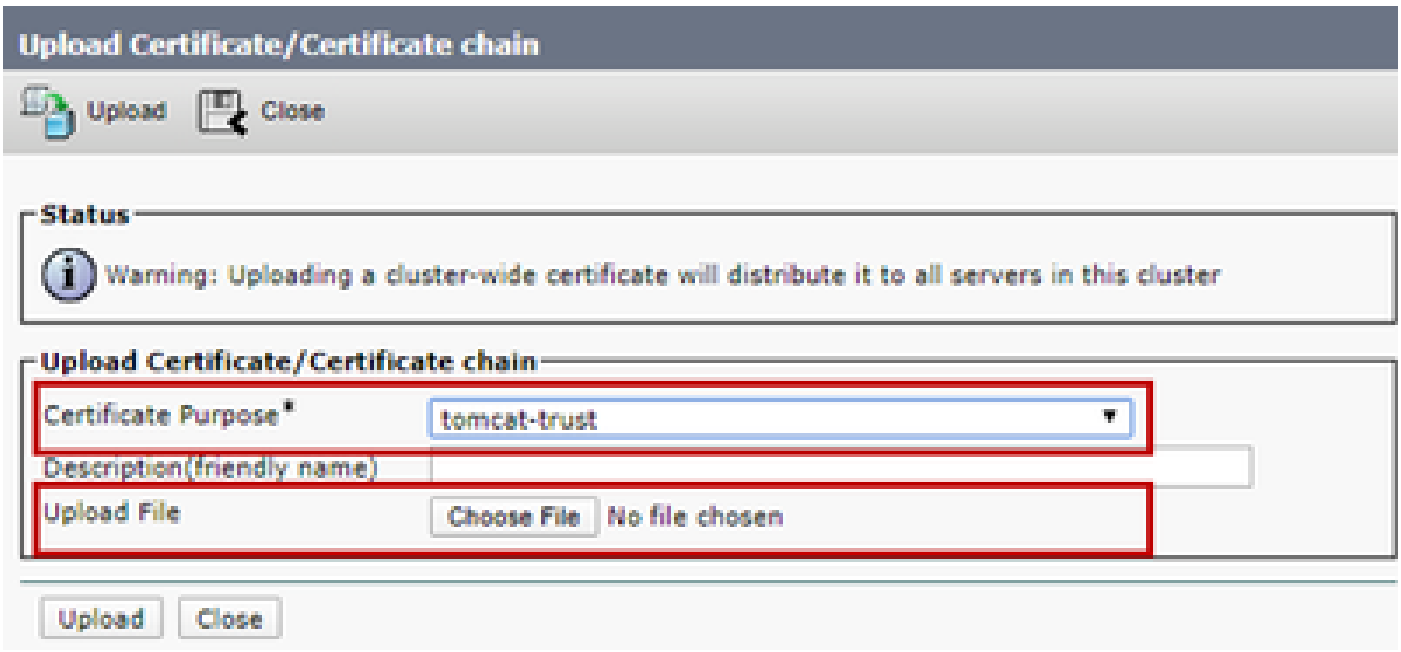
3. Caricare l'applicazione e i certificati radice

Passaggio 1. Passare alla pagina di amministrazione del sistema operativo Cisco Unified Communications: https://FQDN:<8443 o 443>/cmplatform.

Passaggio 2. Passare a Protezione > Gestione certificati e selezionare Carica catena certificati/certificati.

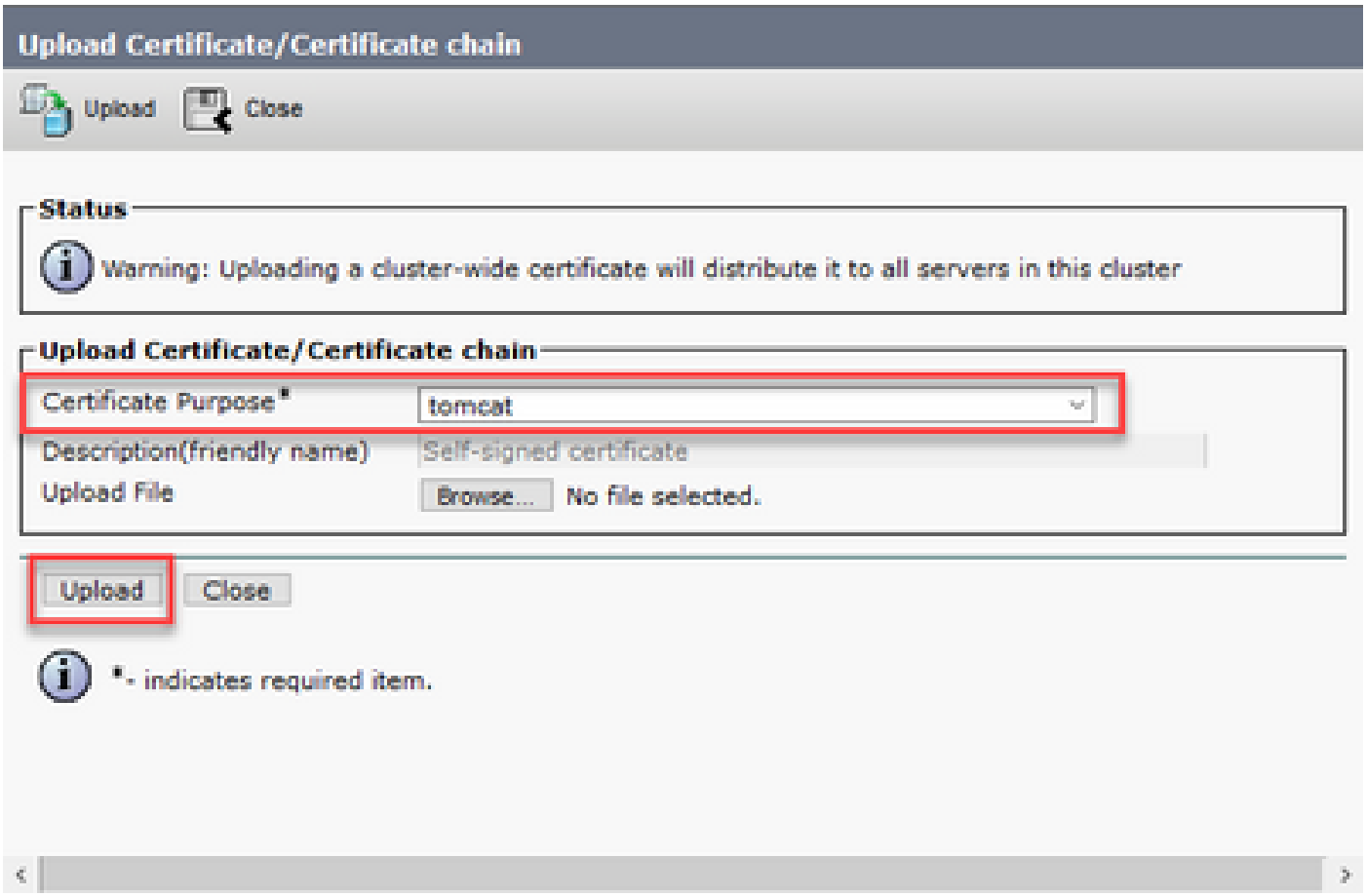


Passaggio 3. Nella finestra Carica catena di certificati/certificati selezionare tomcat-trust nel campo Scopo del certificato e caricare il certificato radice.



Passaggio 4. Caricare un certificato intermedio (se presente) come tomcat-trust.

Passaggio 5. Nella finestra Carica certificato/catena di certificati selezionare ora per passare al campo Scopo certificato e caricare il certificato firmato dalla CA dell'applicazione.



Passaggio 6. Riavviare il server.

Verifica

Dopo aver riavviato il server, eseguire la procedura seguente per verificare l'implementazione della CA firmata:

Passaggio 1. Aprire un browser Web e cancellare la cache.

Passaggio 2. Chiudere e aprire di nuovo il browser.

A questo punto è necessario visualizzare l'opzione del certificato per iniziare il certificato firmato dalla CA e l'indicazione nella finestra del browser che il certificato è autofirmato e quindi non attendibile deve scomparire.

Risoluzione dei problemi

In questa Guida non è disponibile alcuna procedura per la risoluzione dei problemi relativi all'implementazione dei certificati firmati da un'autorità di certificazione.

Informazioni correlate

- Guida alla configurazione di CVP: Guida alla configurazione di CVP - Sicurezza

- Guida alla configurazione UCCE: Guida alla configurazione UCCE - Sicurezza
- Guida all'amministrazione di PCCE: PCE Administration Guide - Security
- Certificati autofirmati UCCE: certificati autofirmati UCCE di Exchange
- Certificati autofirmati PCCE: certificati autofirmati PCCE di Exchange
- Installazione e migrazione a OpenJDK in CCE 12.5(1): CCE OpenJDK Migration
- Installazione e migrazione a OpenJDK in CVP 12.5(1): CVP OpenJDK Migration

Documentazione e supporto tecnico – Cisco Systems

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).