

Configurazione di comunicazioni protette tra Finesse e il server CTI

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[CCE CTI Server Secure](#)

[Finesse Secure Configuration](#)

[Genera certificato PG agente \(server CTI\)](#)

[Ottenere il certificato CSR firmato da una CA](#)

[Importa certificati firmati CA CCE PG](#)

[Genera certificato Finesse](#)

[Firma certificato Finesse da una CA](#)

[Importa certificati firmati radice e applicazione Finesse](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come implementare i certificati firmati da CA (Certification Authority) tra Cisco Finesse e Computer Telephony Integration (CTI) Server nella soluzione Cisco Contact Center Enterprise (CCE).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- CCE release 12.0(1)
- Finesse release 12.0(1)
- Server CTI

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

- Packaged CCE (PCCE) 12.0(1)

- Finesse 12.0(1)

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

Nella versione 11.5 di CCE, Cisco ha iniziato a supportare la versione 1.2 di Transport Layer Security (TLS), che consente il trasporto sicuro dei messaggi Session Initiation Protocol (SIP) e Real-time Transport Protocol (RTP) tramite TLS 1.2. Dalla versione 12.0 di CCE e nell'ambito della protezione dei dati in movimento, Cisco ha iniziato a supportare TLS 1.2 sulla maggior parte dei flussi di chiamate del contact center: Dip. voce in entrata e in uscita, multicanale ed esterna del database. Lo scopo di questo documento è la voce in entrata, in particolare la comunicazione tra Finesse e CTI Server.

Il server CTI supporta le seguenti modalità di connessione:

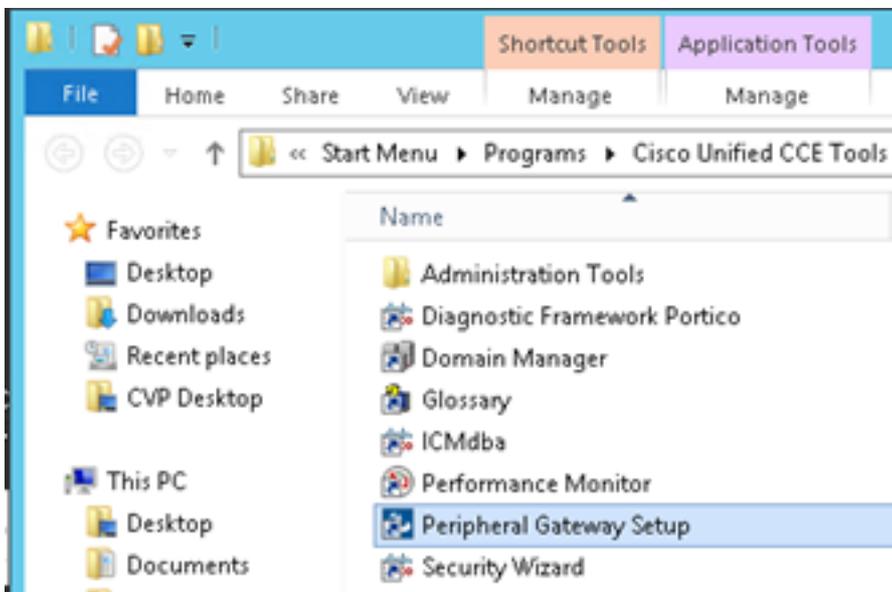
- **Connessione protetta:** Consente una connessione protetta tra il server CTI e i client CTI (Finesse, dialer, CTIOS e ctitest).
- **Connessione protetta e non protetta (modalità mista):** Consente connessioni protette e non protette tra il server CTI e i client CTI. Questa è la modalità di connessione predefinita. Questa modalità viene configurata quando si aggiornano le versioni precedenti a CCE 12.0(1).

Nota: Modalità non protetta non supportata.

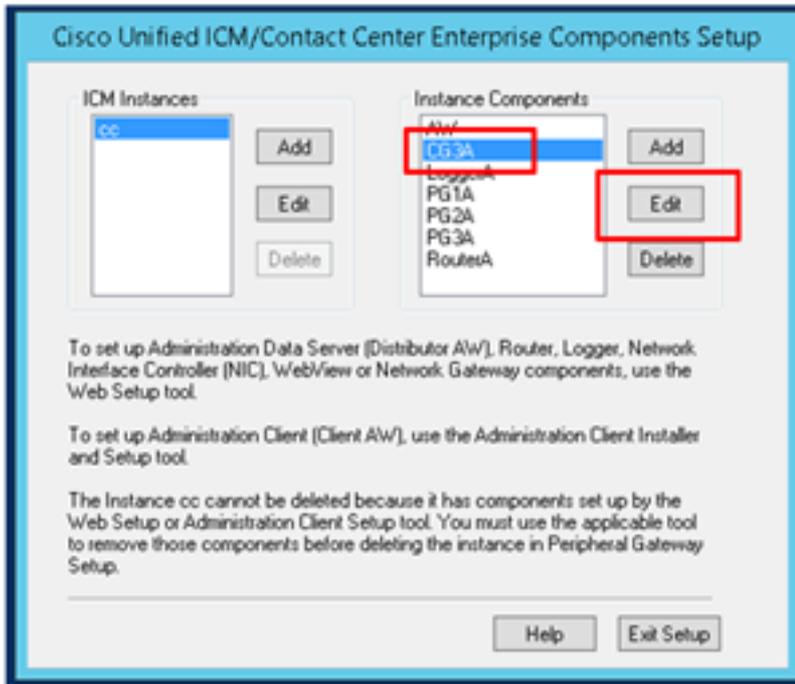
Configurazione

CCE CTI Server Secure

Passaggio 1. Sulla stazione di lavoro amministrativa PCCE (AW), aprire la cartella **Unified CCE Tools** e fare doppio clic su **Peripheral Gateway Setup**.

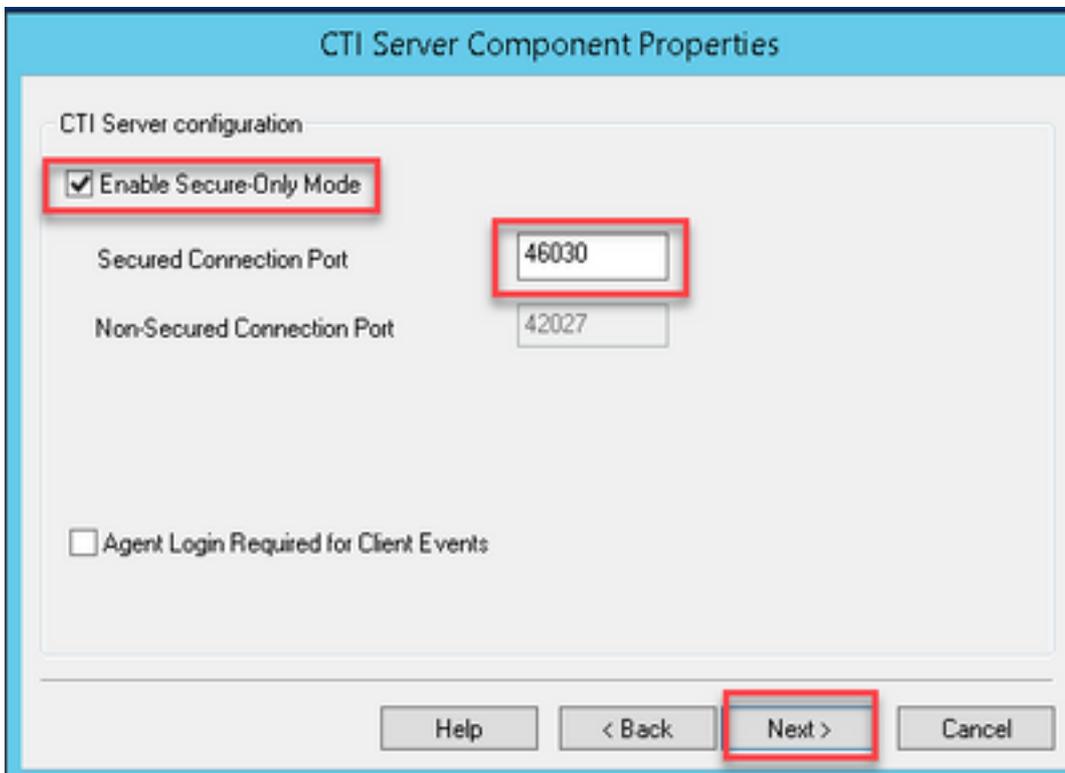


Passaggio 2. Selezionare **CG3A** e fare clic su **Modifica**.



Passaggio 3. Nelle proprietà del server CTI, fare clic su **Avanti**. Per informazioni sull'arresto del servizio **CG3A** durante l'installazione, selezionare **Sì**.

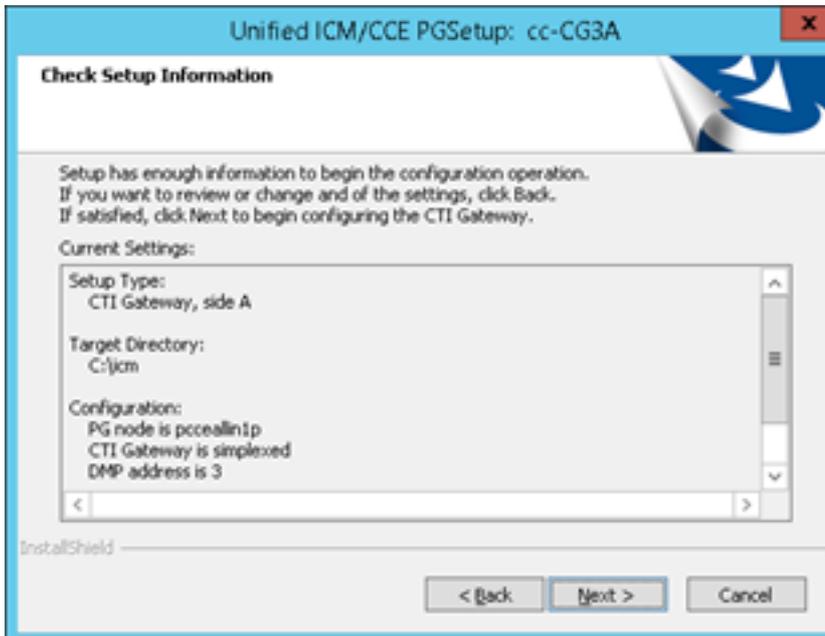
Passaggio 4. Nelle **proprietà dei componenti server CTI**, selezionare **Attiva modalità di sola protezione**. Prendere nota della **porta di connessione protetta (46030)**, in quanto nell'esercizio successivo sarà necessario configurare la stessa porta in Finesse. Fare clic su **Next** (Avanti).



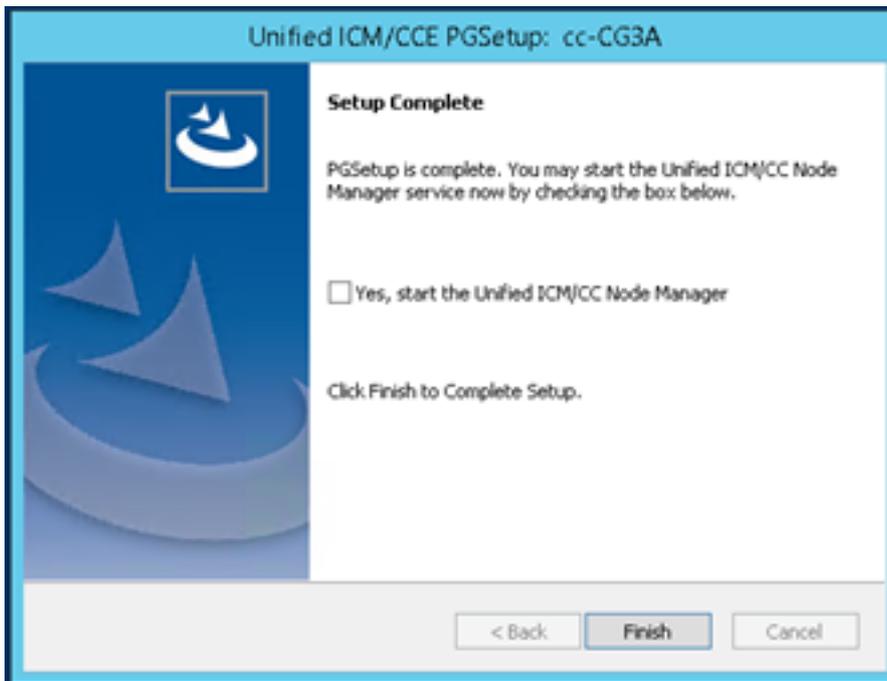
Nota: La comunicazione protetta predefinita è 42030, tuttavia l'lab utilizzata per questo documento è 40630. Il numero di porta fa parte di una formula che include l'ID sistema ICM. Quando l'ID di sistema è 1 (CG1a), il numero di porta predefinito, in generale, è 42030.

Poiché l'ID di sistema nel lab è 3 (CG3a), il numero di porta predefinito è 46030.

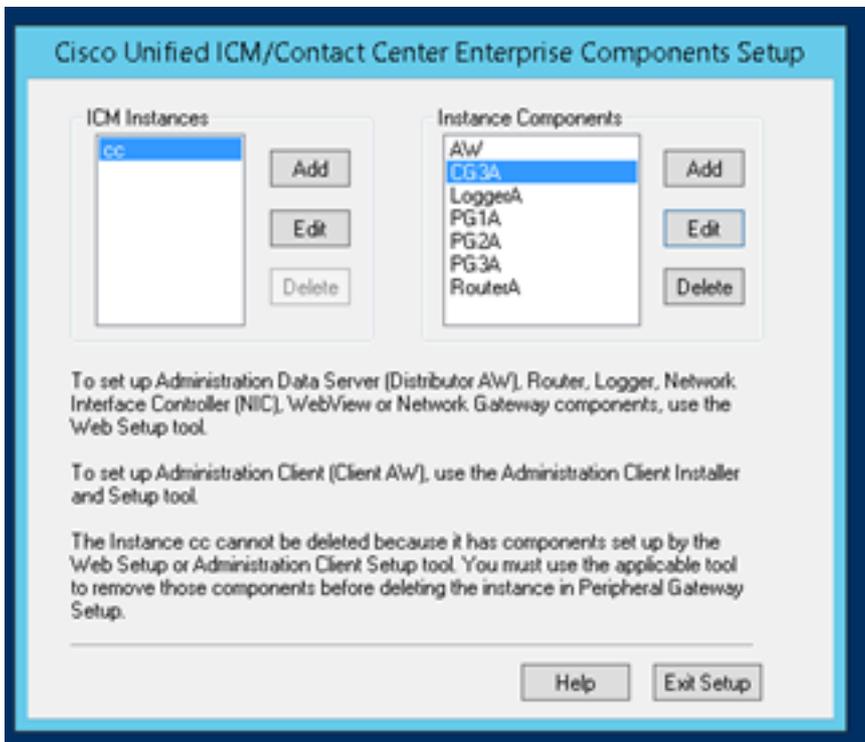
Passaggio 5. In **CTI Network Interface Properties**, fare clic su **Next**. Controllare le **informazioni di installazione** e fare clic su **Avanti**.



Passaggio 6. Fare clic su **Finish** (Fine) come mostrato nell'immagine.



Passaggio 7. Fare clic su **Exit Setup** (Esci dall'installazione) e attendere la chiusura della finestra di installazione, come mostrato nell'immagine.



Passaggio 8. Sul desktop PCCEAllin1, fare doppio clic su **Unified CCE Service Control**.

Passaggio 9. Selezionare Cisco ICM cc CG3A e fare clic su **Start**.

Finesse Secure Configuration

Passaggio 1. Aprire un browser Web e passare a **Amministrazione Finesse**.

Passaggio 2. Scorrere verso il basso fino alla sezione **Contact Center Enterprise CTI Server Settings** (Impostazioni server CTI Contact Center Enterprise) come mostrato nell'immagine.

Passaggio 3. Nell'esercizio precedente, modificare la porta laterale A per la porta di comunicazione protetta configurata su CG3A: **46030**. Selezionare **Abilita crittografia SSL** e fare clic su **Salva**.

Contact Center Enterprise CTI Server Settings

Note: Any changes made to the settings on this gadget require a restart of Cisco Finesse Tomcat to take effect.

Contact Center Enterprise CTI Server Settings

A Side Host/IP Address*	<input type="text" value="10.10.10.10"/>	B Side Host/IP Address	<input type="text"/>
A Side Port*	<input type="text" value="46030"/>	B Side Port	<input type="text"/>
Peripheral ID*	<input type="text" value="5000"/>		

Enable SSL encryption

Nota: Per eseguire il test della connessione, è necessario riavviare prima Finesse Tomcat Service o il server Finesse.

Passaggio 4. Uscire dalla pagina Amministrazione Finesse.

Passaggio 5. Aprire una sessione SSH con Finesse.

Passaggio 6. Nella sessione SSH FINESSEA, eseguire il comando:

riavvio del sistema utils

Quando viene richiesto se si desidera riavviare il sistema, immettere **yes**.

```

# Using username "administrator".
Command Line Interface is starting up, please wait ...

Welcome to the Platform Command Line Interface

VMware Installation:
 2 vCPU: Intel(R) Xeon(R) CPU E5-2680 0 @ 2.70GHz
 Disk 1: 146GB, Partitions aligned
 8192 Mbytes RAM

admin:utils system restart

Do you really want to restart ?

Enter (yes/no)? yes

Appliance is being Restarted ...
Warning: Restart could take up to 5 minutes.
Stopping Service Manager...

```

Genera certificato PG agente (server CTI)

Cisco CertUtils è un nuovo strumento rilasciato su CCE versione 12. È possibile utilizzare questo strumento per gestire tutti i certificati CCE per la voce in entrata. In questo documento vengono

usati questi CiscoCertUtils per generare le richieste di firma di certificati (CSR) dei gateway periferiche (PG).

Passaggio 1. Eseguire questo comando per generare un certificato CSR: **CiscoCertUtil /generateCSR**

```
C:\Users\Administrator.CC>
C:\Users\Administrator.CC>CiscoCertUtil /generateCSR

Key already exists at C:\nicm\ssl\keys\host.key. It will be used to generate the
CSR.

SSL config path = C:\nicm\ssl\cfg\openssl.cfg
SYSTEM command is C:\nicm\ssl\bin\openssl.exe req -new -key C:\nicm\ssl\keys\host.
key -out C:\nicm\ssl\certs\host.csr
You are about to be asked to enter information that will be 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 will be a default value.
If you enter '.', the field will be left blank.

-----
```

Fornire le informazioni richieste, ad esempio:

Nome paese: STATI UNITI

Nome provincia: MA

Nome località: BXB

Nome organizzazione: Cisco

Unità organizzativa: CX

Nome comune: PCCEAllin1.cc.lab

Email: jdoe@cc.lab

Password di verifica: Treno1ng!

Nome società facoltativo: Cisco

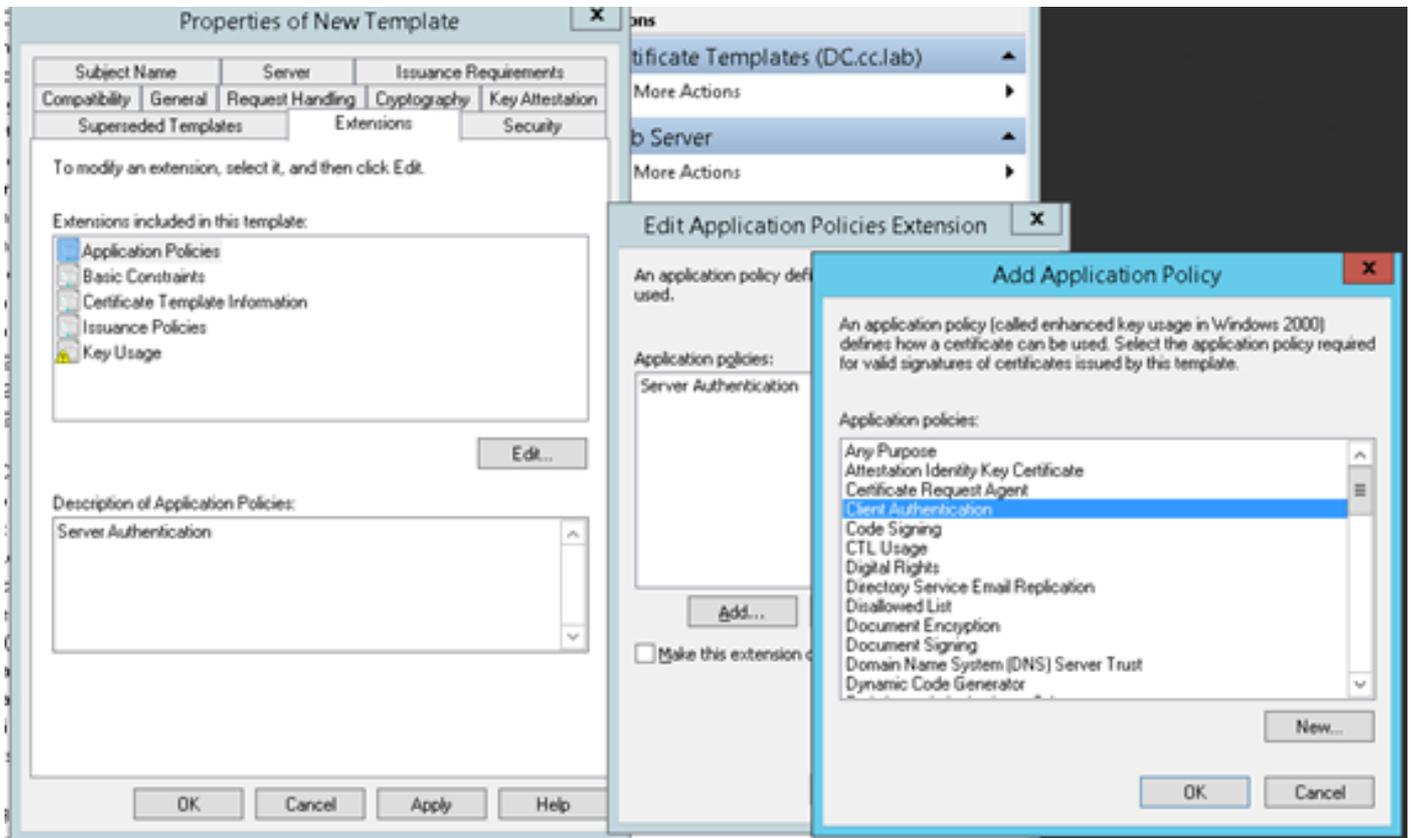
Il certificato e la chiave host sono memorizzati nei percorsi **C:\nicm\ssl\certs** e **C:\nicm\ssl\keys**.

Passaggio 2. Passare alla cartella **C:\nicm\ssl\certs** e verificare che il file **host.csr** sia stato generato.

Ottieni certificato CSR Firmato da una CA

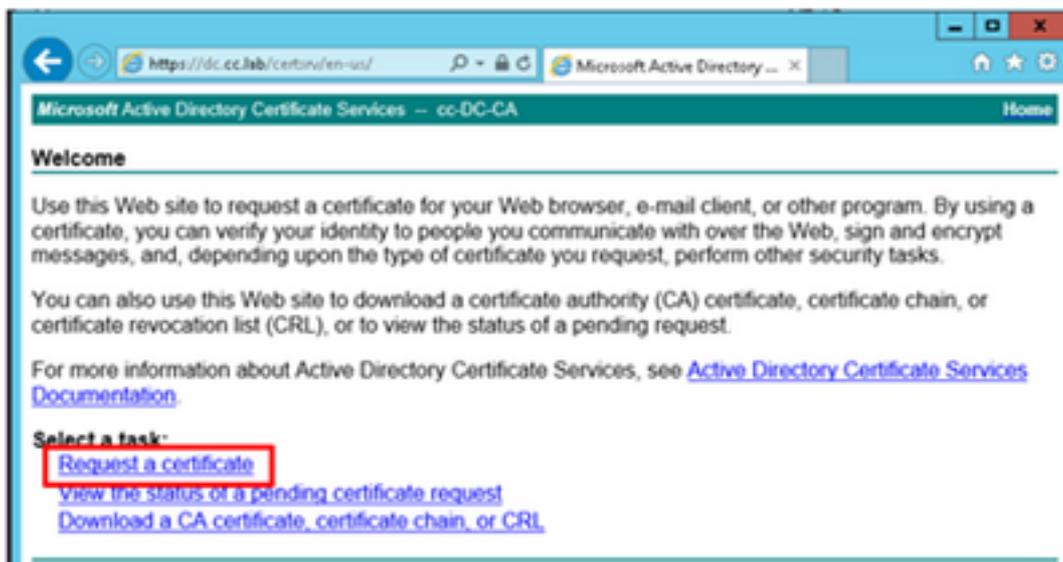
Dopo la generazione, i certificati CSR devono essere firmati da un'autorità di certificazione di terze parti. In questo esercizio, l'autorità di certificazione Microsoft installata nel controller di dominio viene utilizzata come autorità di certificazione di terze parti.

Verificare che il modello di certificato utilizzato dalla CA includa l'autenticazione client e server, come illustrato nell'immagine quando si utilizza la CA Microsoft.

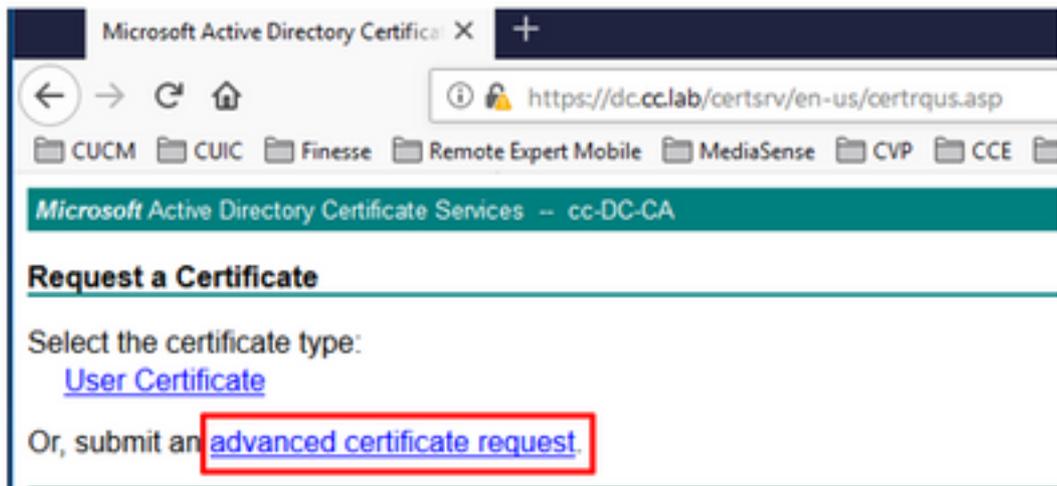


Passaggio 1. Aprire un browser Web e passare alla CA.

Passaggio 2. In **Servizi certificati Microsoft Active Directory**, selezionare **Richiedi certificato**.

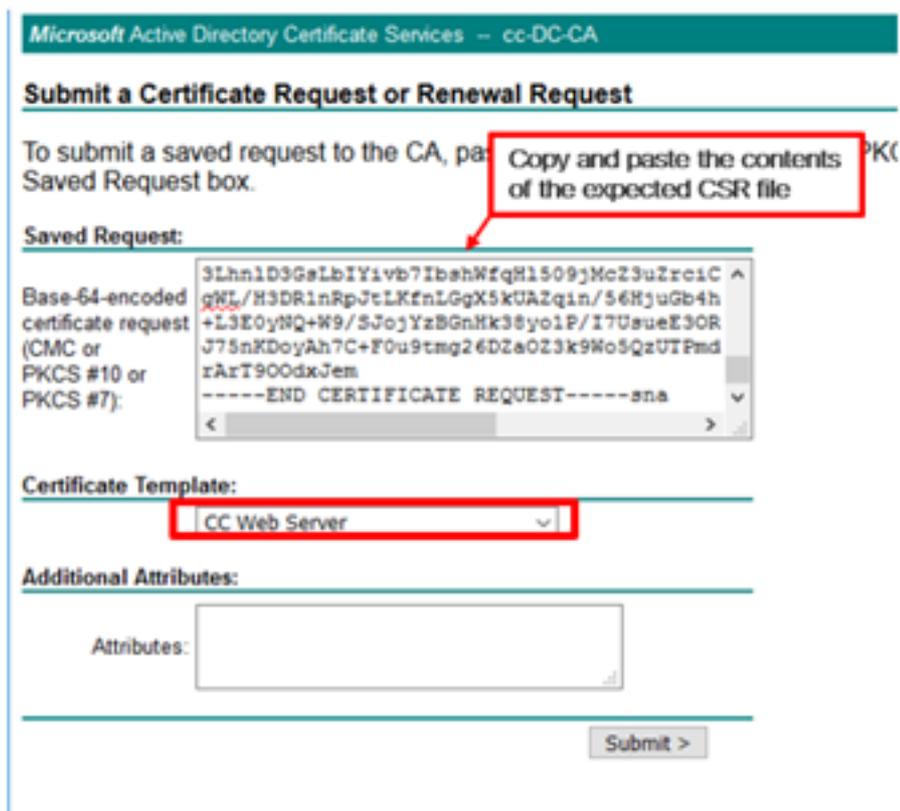


Passaggio 3. Selezionare l'opzione **Advanced certificate request**.



Passaggio 4. Nella **richiesta di certificato avanzata**, copiare e incollare il contenuto del certificato CSR di PG Agent nella casella **Richiesta salvata**.

Passaggio 5. Selezionare il modello **Server Web** con l'autenticazione client e server. In laboratorio, il modello CC Web Server è stato creato con l'autenticazione client e server.



Passaggio 6. Fare clic su **Sottometti**.

Passaggio 7. Selezionare **Base 64 encoded** (Codificato Base 64) e fare clic su **Download Certificate** (Scarica certificato), come mostrato nell'immagine.

Certificate Issued

The certificate you requested was issued to you.

DER encoded or Base 64 encoded



[Download certificate](#)

[Download certificate chain](#)

Passaggio 8. Salvare il file e fare clic su **OK**. Il file viene salvato nella cartella **Download**.

Passaggio 9. Rinominare il file **host.cer** (facoltativo).

Passaggio 10. È inoltre necessario generare un certificato radice. Tornare alla pagina Certificato CA e selezionare **Scarica certificato CA, catena di certificati o CRL**. È sufficiente eseguire questa operazione una sola volta, poiché il certificato radice sarà lo stesso per tutti i server (PG Agent e Finesse).

Welcome

Use this Web site to request a certificate for your Web browser, e people you communicate with over the Web, sign and encrypt m security tasks.

You can also use this Web site to download a certificate authority status of a pending request.

For more information about Active Directory Certificate Services,

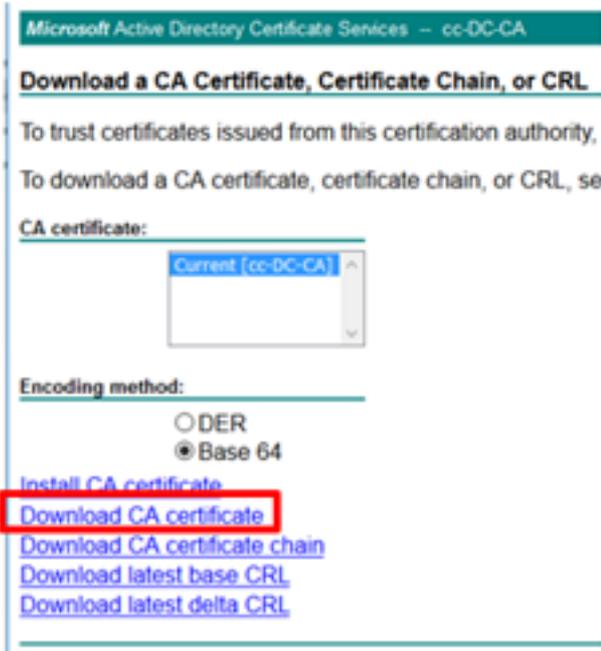
Select a task:

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

Passaggio 11. Fare clic su **Base 64** e selezionare **Scarica certificato CA**.



Passaggio 12. Fare clic su Salva file e selezionare OK. Il file verrà salvato nel percorso predefinito Download.

Importa certificati firmati CA CCE PG

Passaggio 1. In PG Agent passare a C:\icm\ssl\certs e incollare qui i file radice e PG Agent firmati.

Passaggio 2. Rinominare il certificato host.pem in c:\icm\ssl\certs come selfhost.pem.

Passaggio 3. Rinominare host.cer in host.pem nella cartella c:\icm\ssl\certs.

Passaggio 4. Installare il certificato radice. Al prompt dei comandi, eseguire questo comando:
CiscoCertUtil /install C:\icm\ssl\certs\rootAll.cer

```
C:\Users\Administrator.CC>CiscoCertUtil /install C:\icm\ssl\certs\rootAll.cer
Install String is certutil -enterprise -addstore -f Root C:\icm\ssl\certs\rootAll.cer
Root "Trusted Root Certification Authorities"
Signature matches Public Key
Related Certificates:

Exact match:
Element #1:
Serial Number: 488a8f1b836a58b54c66a65f5298faae
Issuer: CN=cc-DC-CA, DC=cc, DC=lab
NotBefore: 2/8/2017 3:43 PM
NotAfter: 2/8/2028 3:53 PM
Subject: CN=cc-DC-CA, DC=cc, DC=lab
CA Version: 00.0
Signature matches Public Key
Root Certificate: Subject matches Issuer
Cert Hash(sha1): ec 49 6e f7 cb 9a c8 3a f5 46 2b ae 4f 1f 1b 15 fd 38 81 5f

Certificate "cc-DC-CA" already in store.
CertUtil: -addstore command completed successfully.
C:\Users\Administrator.CC>
```

Passaggio 5. Installare il certificato firmato dall'applicazione che esegue lo stesso comando:
CiscoCertUtil /install C:\icm\ssl\certs\host.pem

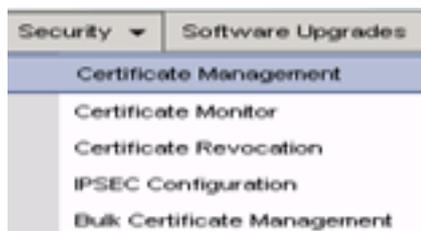
```
C:\Users\Administrator.CC>CiscoCertUtil /install C:\icm\ssl\certs\host.pem
Install String is certutil -enterprise -addstore -f Root C:\icm\ssl\certs\host.pem
Root "Trusted Root Certification Authorities"
Certificate "PCCALLini.cc.lab" added to store.
CertUtil: -addstore command completed successfully.
C:\Users\Administrator.CC>
```

Passaggio 6. Ciclare il PG. Aprire Unified CCE Service Control e riaccendere Cisco ICM Agent PG.

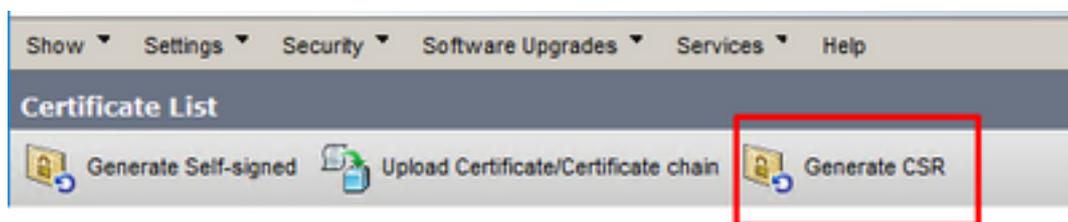
Genera certificato Finesse

Passaggio 1. Aprire il browser Web e passare a **Finesse OS Admin**.

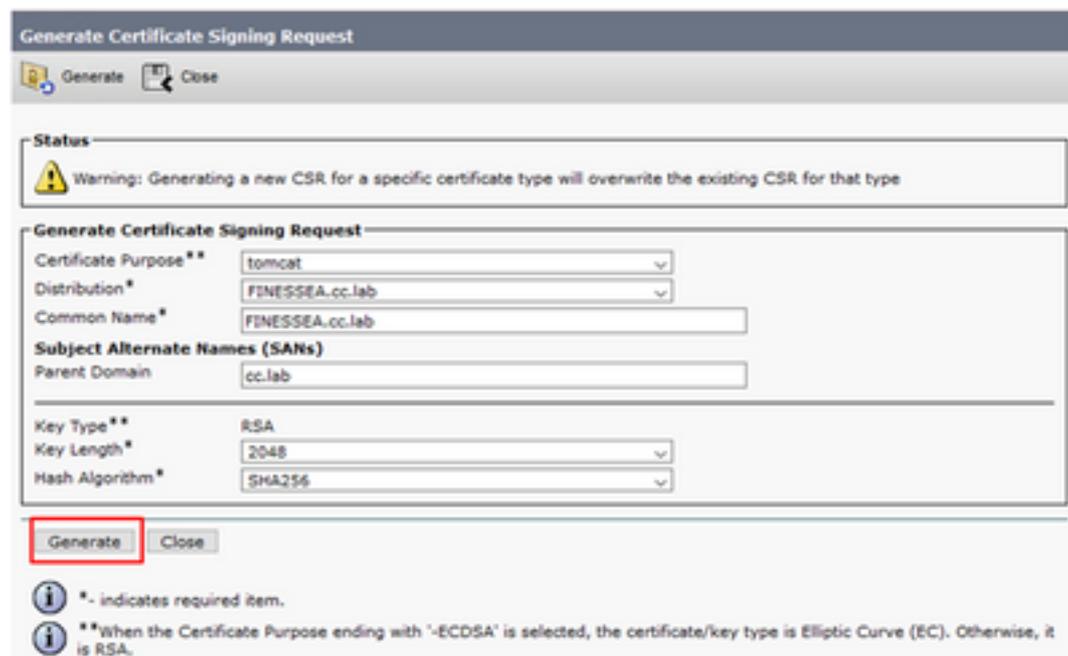
Passaggio 2. Accedere con le credenziali di Amministratore del sistema operativo e selezionare **Security > Certificate Management**, come mostrato nell'immagine.



Passaggio 3. Fare clic su **Generate CSR (Genera CSR)** come mostrato nell'immagine.



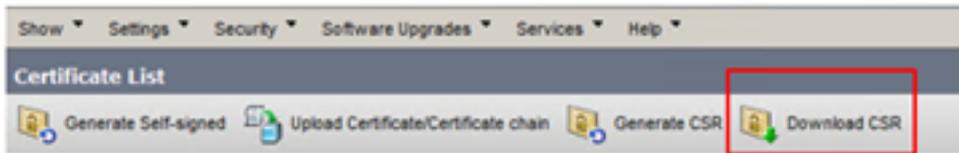
Passaggio 4. In **Genera richiesta di firma certificato**, utilizzare i valori predefiniti e fare clic su **Genera**.

A screenshot of the 'Generate Certificate Signing Request' dialog box. The dialog has a title bar and a 'Generate' button (highlighted with a red box) and a 'Close' button. A warning message is displayed: 'Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type'. The form contains the following fields:

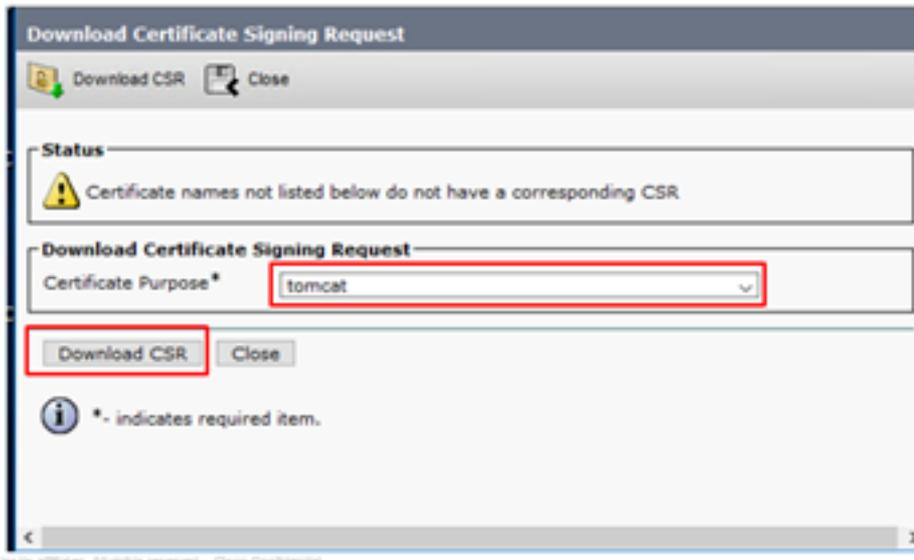
- Certificate Purpose: tomcat
- Distribution: FINESSEA.cc.lab
- Common Name: FINESSEA.cc.lab
- Subject Alternate Names (SANs):
 - Parent Domain: cc.lab
- Key Type: RSA
- Key Length: 2048
- Hash Algorithm: SHA256

At the bottom, there are two informational icons: one indicating that an asterisk (*) denotes a required item, and another explaining that when a certificate purpose ending in '-ECDSA' is selected, the certificate/key type is Elliptic Curve (EC), otherwise it is RSA.

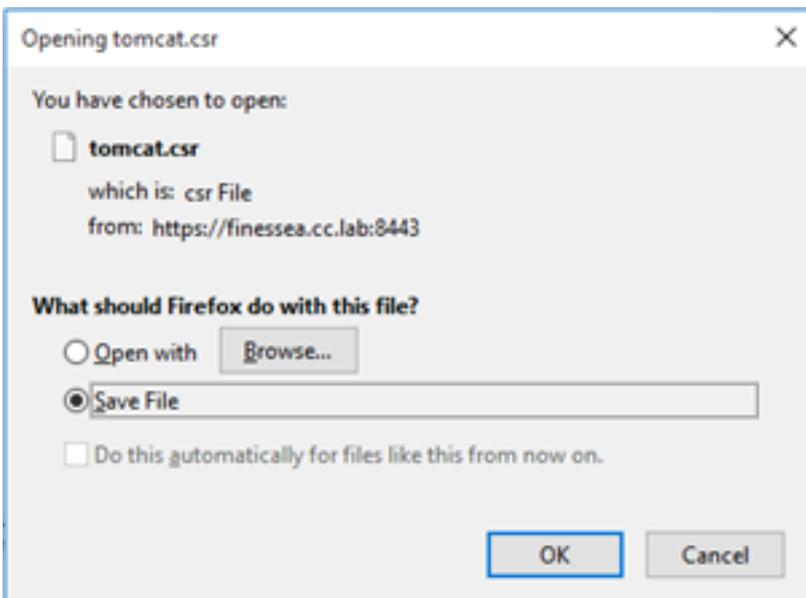
Passaggio 5. Chiudere la finestra **Genera richiesta di firma certificato** e selezionare **Scarica CSR**.



Passaggio 6. Nello scopo del certificato, selezionare **tomcat** e fare clic su **Download CSR**.



Passaggio 7. Selezionare **Save File** (Salva file) e fare clic su **OK**, come mostrato nell'immagine.



Passaggio 8. Chiudere la finestra **Scarica richiesta di firma certificato**. Il certificato viene salvato nel percorso predefinito (**Questo PC > Download**).

Passaggio 9. Aprire Esplora risorse e individuare la cartella. Fare clic con il pulsante destro del mouse sul certificato e rinominarlo: **finessetomcat.csr**

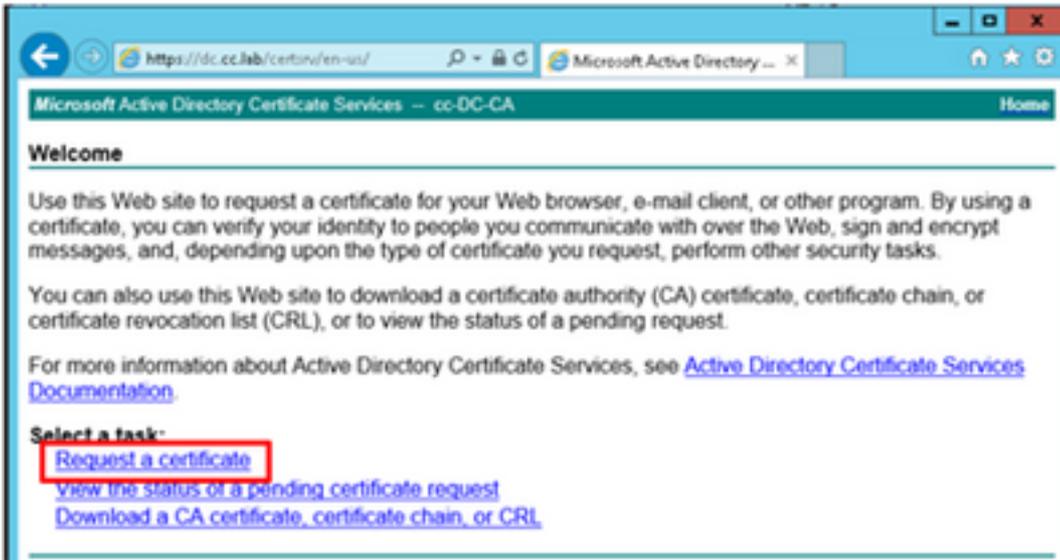
Firma certificato Finesse da una CA

In questa sezione viene utilizzata la stessa CA Microsoft utilizzata nel passaggio precedente come CA di terze parti.

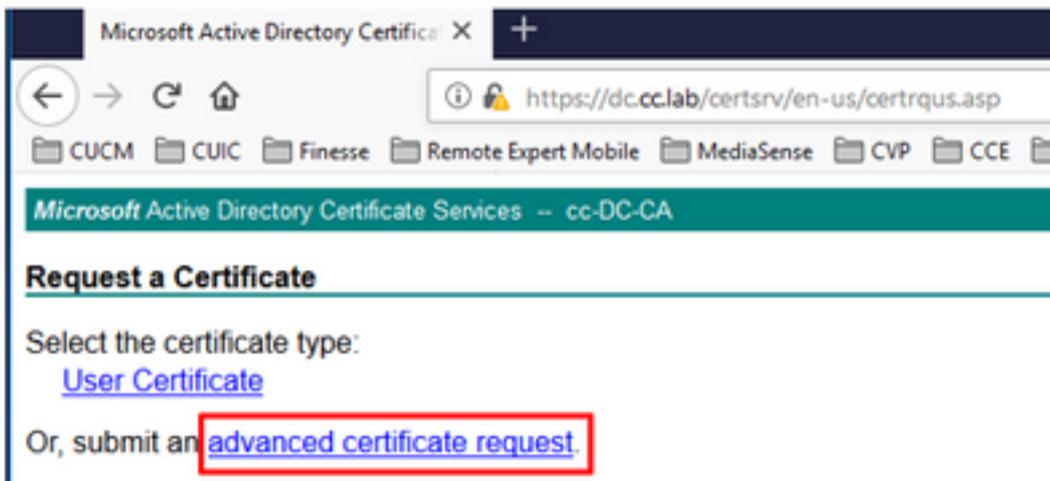
Nota: Verificare che il modello di certificato utilizzato dalla CA includa l'autenticazione client e server.

Passaggio 1. Aprire un browser Web e passare alla CA.

Passaggio 2. In **Servizi certificati Microsoft Active Directory**, selezionare **Richiedi certificato**.



Passaggio 3. Selezionare l'opzione **Advanced certificate request** come mostrato nell'immagine.



Passaggio 4. Nella **richiesta di certificato avanzata**, copiare e incollare il contenuto del certificato CSR Finesse nella casella **Richiesta salvata**.

Passaggio 5. Selezionare il modello di server Web con l'autenticazione client e server. In questa esercitazione il modello CC Web Server è stato creato con l'autenticazione client e server.

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste the contents of the Saved Request box.

Copy and paste the contents of the expected CSR file

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
3Lhn1D3GcLbIYivb7IbshWfqH1509jMcZ3uZrciC
gKl/H3DR1nRpJcLKfnLGgX5kUAZqin/56HjuGb4h
+L3E0yNQ+W9/SJoJYzBGnHk38yo1P/I7UaueE3OR
J75nKDoyAh7C+F0u9tmq26D2a0Z3k9No5QzUTPmd
rArT900dxJem
-----END CERTIFICATE REQUEST-----sna
```

Certificate Template:

CC Web Server

Additional Attributes:

Attributes:

Submit >

Passaggio 6. Fare clic su **Sottometti**.

Passaggio 7. Selezionare **Base 64 encoded** (Codificato Base 64) e fare clic su **Download certificate** (Scarica certificato), come mostrato nell'immagine.

Certificate Issued

The certificate you requested was issued to you.

DER encoded or Base 64 encoded



[Download certificate](#)

[Download certificate chain](#)

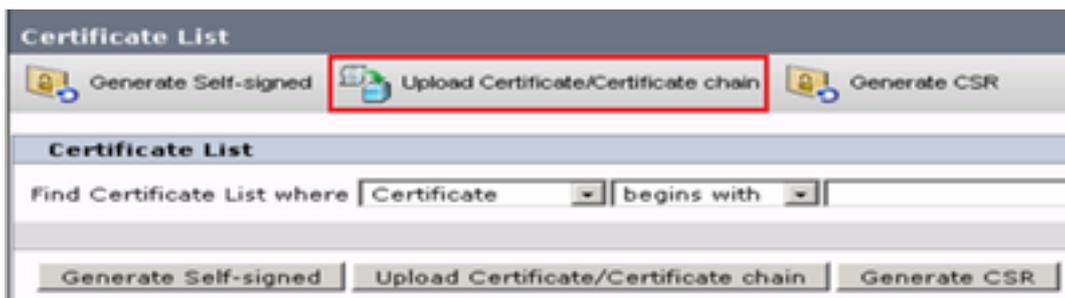
Passaggio 8. Salvare il file e fare clic su **OK**. Il file viene salvato nella cartella **Download**.

Passaggio 9. Rinominare il file **finesse.cer**.

Importa certificati firmati radice e applicazione Finesse

Passaggio 1. In un browser Web aprire la pagina **Finesse OS Admin** e passare a **Sicurezza > Gestione certificati**.

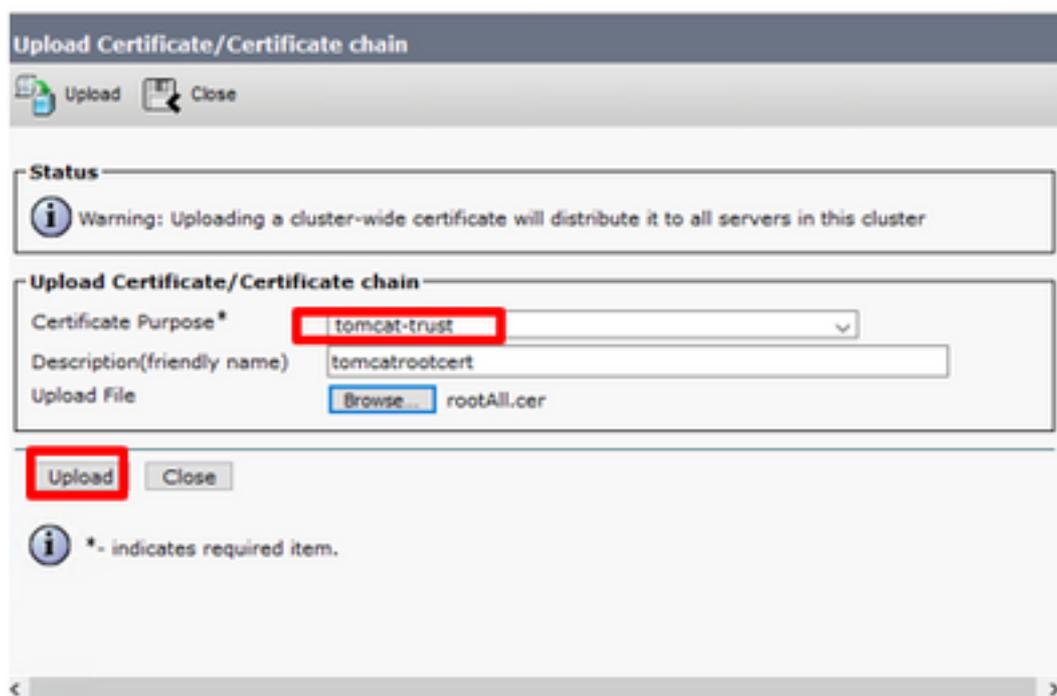
Passaggio 2. Fare clic sul pulsante **Carica certificato/catena di certificati** come mostrato nell'immagine.



Passaggio 3. Nella finestra popup selezionare **tomcat-trust** for **Certificate Purpose**.

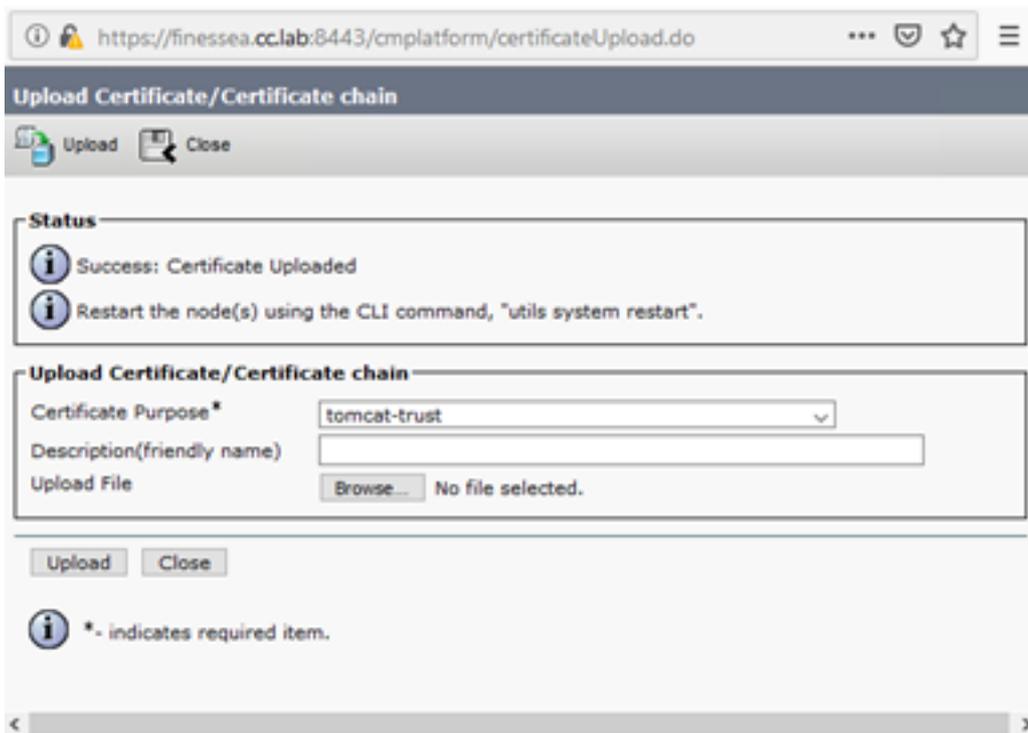
Passaggio 4. Fare clic sul pulsante **Sfoglia...** e selezionare il file del certificato radice da importare. Quindi, fare clic sul pulsante **Apri**.

Passaggio 5. Nella descrizione, scrivere qualcosa come **tomcatrootcert** e fare clic sul pulsante **Upload**, come mostrato nell'immagine.

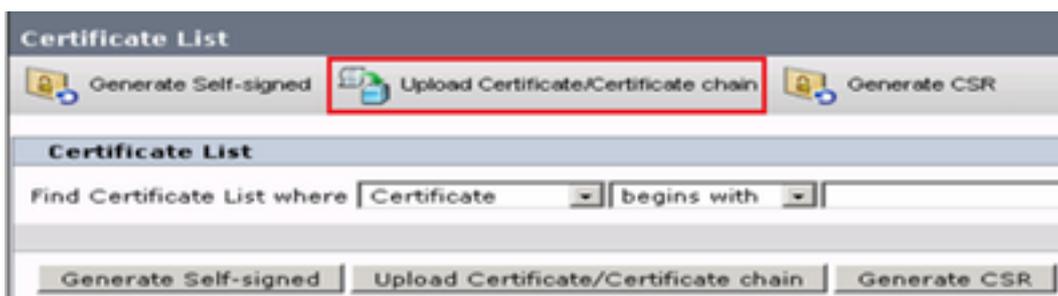


Passaggio 6. Attendere fino a quando non viene visualizzata la schermata **Operazione riuscita**: Messaggio di **caricamento certificato** per chiudere la finestra.

Verrà richiesto di riavviare il sistema, ma prima continuare con il caricamento del certificato firmato dell'applicazione Finesse, quindi riavviare il sistema.



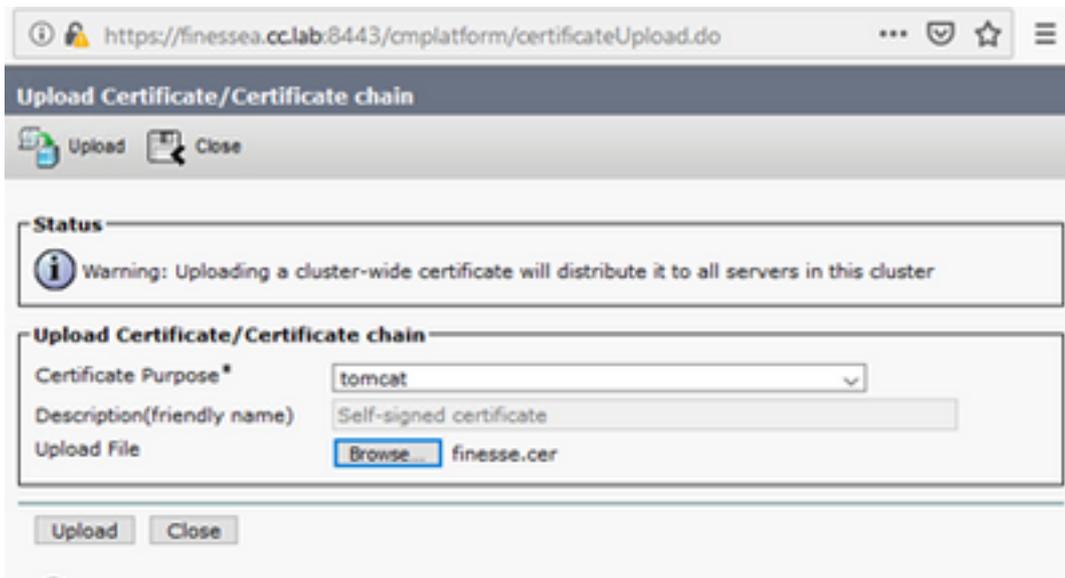
Passaggio 7. Fare clic sul pulsante **Carica catena di certificati/certificati** per dedicare più tempo all'importazione del certificato dell'applicazione Finesse.



Passaggio 8. Nella finestra popup selezionare **tomcat** for **Certificate Purpose**.

Passaggio 9. Fare clic sul pulsante **Sfoggia...** e selezionare il file firmato Finesse CA, **finesse.cer**. Quindi, fare clic sul pulsante **Apri**.

Passaggio 10. Fare clic sul pulsante **Upload**.



Passaggio 11. Attendere finché non viene visualizzata la schermata **Operazione riuscita: Messaggio di certificato caricato**.

Viene nuovamente richiesto di riavviare il sistema. Chiudere la finestra e continuare a riavviare il sistema.

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.