

Soluzione Package CCE: procedura per ottenere e caricare certificati CA di terze parti

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Procedura](#)

[Genera e scarica CSR](#)

[Ottieni certificato radice, intermedio \(se applicabile\) e applicazione da CA](#)

[Carica certificati nei server](#)

[Server Finesse](#)

[Server CUIC](#)

[Dipendenze certificato](#)

[Carica certificato radice server CUIC sul server primario Finesse](#)

[Carica certificato radice/intermedio Finesse sul server primario CUIC](#)

Introduzione

In questo documento viene descritto come ottenere e installare un certificato di un'Autorità di certificazione (CA), generato da un fornitore di terze parti per stabilire una connessione HTTPS tra i server Finesse e Cisco Unified Intelligence Center (CUIC).

Per utilizzare HTTPS per una comunicazione sicura tra i server Finesse e CUIC, è necessario configurare i certificati di sicurezza. Per impostazione predefinita, questi server forniscono certificati autofirmati che vengono utilizzati per consentire ai clienti di acquistare e installare certificati CA. Questi certificati CA possono essere ottenuti da un fornitore di terze parti come VeriSign, Thawte, GeoTrust o possono essere prodotti internamente.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Package Contact Center Enterprise (PCCE)
- CUIC
- Cisco Finesse
- Certificati CA

Componenti usati

Le informazioni utilizzate nel documento si basano sulla versione 11.0 (1) di PCCE.

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, verificare di aver compreso l'impatto potenziale di qualsiasi passaggio.

Procedura

Per impostare i certificati per la comunicazione HTTPS nei server Finesse e CUIC, eseguire la procedura seguente:

- Genera e scarica richiesta di firma del certificato (CSR)
- Ottenere dalla CA il certificato radice, intermedio (se applicabile) e di applicazione con l'utilizzo di CSR
- Carica certificati nei server

Genera e scarica CSR

1. Le operazioni descritte di seguito sono finalizzate alla generazione e al download di CSR. Questa procedura è la stessa per i server Finesse e CUIC.
2. Aprire la pagina di amministrazione del sistema operativo Cisco Unified Communications con l'URL e accedere con l'account di amministratore del sistema operativo (OS) creato durante il processo di installazione. <https://hostname del server principale/cmplatform>
3. Generare la richiesta di firma del certificato.
 - a. Passare a Sicurezza > Gestione certificati > Genera CSR.
 - b. Dall'elenco a discesa Scopo certificato*, selezionare tomcat.
 - c. Selezionare Algoritmo hash come SHA256.
 - d. Fare clic su Generate (Genera) come mostrato nell'immagine.

Generate Certificate Signing Request



Generate



Close

Status



Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

Generate Certificate Signing Request

Certificate Purpose*	tomcat	▼
Distribution*	livedata.ora.com	▼
Common Name	livedata.ora.com	
<input checked="" type="checkbox"/> Required Field		
Subject Alternate Names (SANs)		
Parent Domain	ora.com	
Key Length*	2048	▼
Hash Algorithm*	SHA256	▼

Generate

Close

4. Scaricare CSR.

a. Selezionare Protezione > Gestione certificati > Scarica CSR.

b. Dall'elenco a discesa Scopo certificato*, selezionare tomcat.

c. Fare clic su Download CSR come mostrato nell'immagine.



Show ▾ Settings ▾ Security ▾ Software Upgrades ▾ Services ▾ Help ▾

Certificate Management

Certificate List



Generate Self-signed



Upload Certificate/Certificate chain




Generate CSR



Download CSR



 Nota: per ottenere i CSR per CA, eseguire questi passaggi sul server secondario con l'URL <https://hostname del server secondario/cmplatform>.

Otteni certificato radice, intermedio (se applicabile) e applicazione da CA

1. Fornire le informazioni CSR del server primario e secondario a CA di terze parti quali VeriSign, Thawte, GeoTrust e così via.
2. Da CA, è necessario ricevere la seguente catena di certificati per i server principale e secondario:
 - Server Finesse: radice, intermedio e certificato applicazione
 - Server CUIC: certificato radice e applicazione

Carica certificati nei server

In questa sezione viene descritto come caricare correttamente la catena di certificati sui server Finesse e CUIC.

Server Finesse

1. Caricare il certificato radice del server Finesse primario:

a. Nella pagina Cisco Unified Communications Operating System Administration (Amministrazione del sistema operativo di Cisco Unified Communications) del server principale, selezionare Sicurezza > Gestione certificati > Carica certificato.

b. Dall'elenco a discesa Scopo certificato, selezionare tomcat-trust.

c. Nel campo Carica file, fare clic su Sfoglia e sfogliare il file del certificato radice.

d. Fare clic su Upload File (Carica file).

2. Caricare il certificato intermedio del server Finesse primario:


a. Dall'elenco a discesa Scopo certificato, selezionare tomcat-trust.

b. Nel campo Root Certificate (Certificato radice), immettere il nome del certificato radice caricato nel passaggio precedente. Si tratta di un file .pem generato al momento dell'installazione del certificato radice/pubblico.

Per visualizzare questo file, passare a Gestione certificati > Trova. Nell'elenco dei certificati, il nome file .pem viene elencato rispetto a tomcat-trust.

c. Nel campo Carica file, fare clic su Sfoglia e cercare il file del certificato intermedio.

d. Fare clic su Upload File (Carica file).

 Nota: poiché l'archivio di attendibilità tomcat viene replicato tra i server primario e secondario, non è necessario caricare il certificato radice o intermedio del server Finesse primario nel server Finesse secondario.

3. Caricare il certificato dell'applicazione server Finesse principale:

a. Dall'elenco a discesa Scopo certificato, selezionare tomcat.


b. Nel campo Certificato radice, immettere il nome del certificato intermedio caricato nel passaggio precedente. Includere l'estensione .pem, ad esempio TEST-SSL-CA.pem.

c. Nel campo Carica file, fare clic su Sfoglia e sfogliare il file del certificato dell'applicazione.

d. Fare clic su Upload File (Carica file).

4. Caricare la radice del server Finesse secondario e il certificato intermedio:

a. Seguire la stessa procedura descritta nei passaggi 1 e 2 sul server secondario per i relativi certificati.

 Nota: poiché l'archivio di attendibilità tomcat viene replicato tra i server primario e secondario, non è necessario caricare il certificato radice o intermedio del server Finesse secondario nel server Finesse primario.

5. Caricare il certificato secondario dell'applicazione server Finesse:

a. Seguire la stessa procedura descritta al passaggio 3 sul server secondario per i propri certificati.

6. Riavviare i server:

a. Accedere alla CLI sui server Finesse primario e secondario ed eseguire il comando utilizza il riavvio del sistema per riavviare i server.

Server CUIC


1. Carica certificato radice (pubblico) del server primario CUIC:

a. Nella pagina Cisco Unified Communications Operating System Administration (Amministrazione del sistema operativo di Cisco Unified Communications) del server principale, passare a Sicurezza > Gestione certificati > Carica certificato.

b. Dall'elenco a discesa Scopo certificato, selezionare tomcat-trust.

c. Nel campo Carica file, fare clic su Sfoglia e sfogliare il file del certificato radice.

d. Fare clic su Upload File (Carica file).

 Nota: poiché l'archivio Tomcat-trust viene replicato tra i server primario e secondario, non è necessario caricare il certificato radice del server CUIC primario nei server CUIC secondari.

2. Carica certificato (primario) applicazione server primaria CUIC:

a. Dall'elenco a discesa Scopo certificato, selezionare tomcat.

b. Nel campo Certificato radice, immettere il nome del certificato radice caricato nel passaggio precedente.

Si tratta di un file con estensione pem generato al momento dell'installazione del certificato radice/pubblico. Per visualizzare questo file, passare a gestione certificati > Trova.


Nell'elenco dei certificati il nome file .pem è elencato rispetto a tomcat-trust. Includere l'estensione .pem, ad esempio TEST-SSL-CA.pem.

c. Nel campo Carica file, fare clic su Sfoglia e sfogliare il file del certificato (primario) dell'applicazione.

d. Fare clic su Upload File (Carica file).

3. Caricare il certificato radice (pubblico) del server secondario CUIC:

a. Sul server CUIC secondario, eseguire gli stessi passaggi indicati nel passaggio 1. per il relativo certificato radice.


 Nota: poiché l'archivio di attendibilità tomcat viene replicato tra i server primario e secondario, non è necessario caricare il certificato radice del server CUIC secondario nel server CUIC primario.

4. Caricare il certificato (primario) dell'applicazione server secondaria CUIC:

a. Seguire la stessa procedura descritta al passaggio 2 sul server secondario per ottenere il proprio certificato.

5. Riavviare i server:

a. Accedere alla CLI sui server CUIC primario e secondario ed eseguire il comando utilizza il riavvio del sistema per riavviare i server.

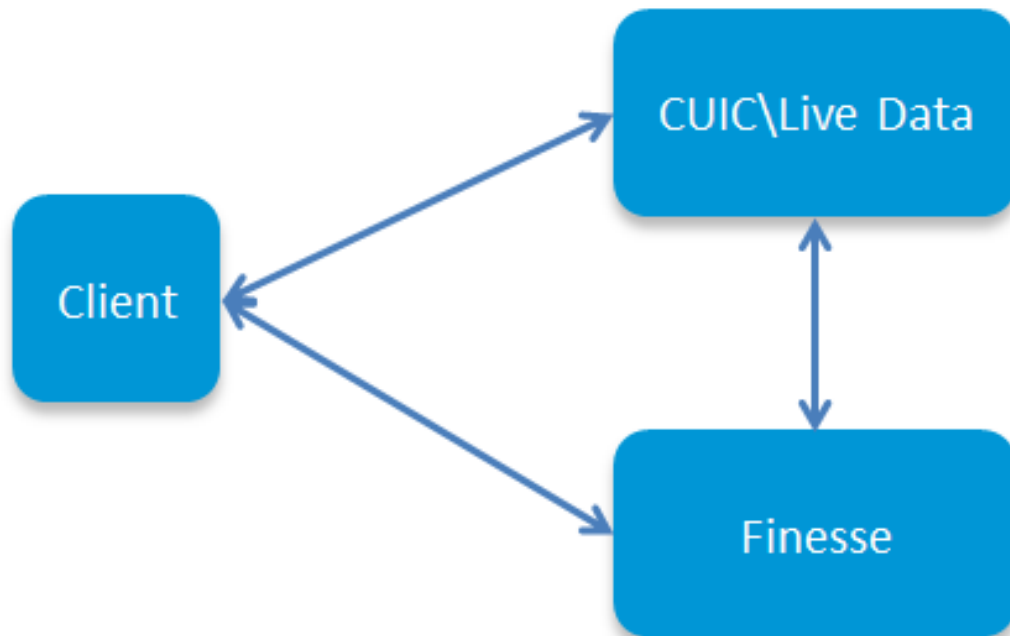
 Nota: per evitare l'avviso di eccezione certificato, è necessario accedere ai server utilizzando il nome di dominio completo (FQDN, Fully Qualified Domain Name).

Dipendenze certificato

Poiché gli agenti Finesse e i supervisor utilizzano i gadget CUIC per la creazione di report, è necessario caricare anche i certificati radice di questi server, nell'ordine indicato qui per mantenere le dipendenze dei certificati per la comunicazione HTTPS tra questi server e come mostrato nell'immagine.

- Carica il certificato radice dei server CUIC sul server primario Finesse
- Carica certificato radice\intermedio Finesse sul server primario CUIC

Certificate Dependencies



Carica certificato radice server CUIC sul server primario Finesse

1. Sul server Finesse primario, aprire la pagina di amministrazione del sistema operativo Cisco Unified Communications con l'URL e accedere con l'account di amministratore del sistema operativo creato al momento del processo di installazione:

<https://hostname del server/piattaforma Finesse principale>

2. Caricare il certificato radice CUIC primario.

a. Passare a Sicurezza > Gestione certificati > Carica certificato.

b. Dall'elenco a discesa Scopo certificato, selezionare tomcat-trust.

c. Nel campo Carica file, fare clic su Sfogliare e sfogliare il file del certificato radice.

d. Fare clic su Upload File (Carica file).

3. Caricare il certificato radice CUIC secondario.

a. Passare a Sicurezza > Gestione certificati > Carica certificato.

b. Dall'elenco a discesa Scopo certificato, selezionare tomcat-trust.

c. Nel campo Carica file, fare clic su Sfogliare e sfogliare il file del certificato radice.

d. Fare clic su Upload File (Carica file).



Nota: poiché l'archivio di attendibilità tomcat viene replicato tra i server primario e secondario, non è necessario caricare i certificati radice CUIC nel server Finesse secondario.

4. Accedere alla CLI sui server Finesse primario e secondario ed eseguire il comando utilizza il riavvio del sistema per riavviare i server.

Carica certificato radice/intermedio Finesse sul server primario CUIC

1. Sul server CUIC primario, aprire la pagina di amministrazione del sistema operativo Cisco Unified Communications con l'URL e accedere con l'account di amministratore del sistema operativo creato al momento del processo di installazione:

`https://hostname di server/piattaforma CUIC principale`

2. Caricare il certificato radice Finesse primario:

a. Passare a Sicurezza > Gestione certificati > Carica certificato.

b. Dall'elenco a discesa Scopo certificato, selezionare tomcat-trust.

c. Nel campo Carica file, fare clic su Sfoglia e sfogliare il file del certificato radice.

d. Fare clic su Upload File (Carica file).

3. Caricare il certificato intermedio Finesse primario:

a. Dall'elenco a discesa Scopo certificato, selezionare tomcat-trust.

b. Nel campo Root Certificate (Certificato radice), immettere il nome del certificato radice caricato nel passaggio precedente.

c. Nel campo Carica file, fare clic su Sfoglia e cercare il file del certificato intermedio.

d. Fare clic su Upload File (Carica file).

4. Eseguire gli stessi passaggi 2 e 3 per i certificati secondari radice\Intermediate Finesse sul server dati primario.



Nota: poiché l'archivio di attendibilità tomcat viene replicato tra i server primario e secondario, non è necessario caricare il certificato radice/intermedio Finesse nei server CUIC secondari.

5. Accedere alla CLI sui server CUIC primario e secondario ed eseguire il comando utilizza il riavvio del sistema per riavviare i server.

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).