

Configurazione della gestione dei certificati della soluzione UCCX

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[FQDN, DNS e domini](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Diagramma di configurazione](#)

[Certificati firmati](#)

[Installa certificati applicazione Tomcat firmati](#)

[Certificati autofirmati](#)

[Installazione Su Server Periferici](#)

[Rigenerazione dei certificati autofirmati](#)

[Integrazione e configurazione client](#)

[UCCX-to-SocialMiner](#)

[Certificato client AppAdmin UCCX](#)

[Certificato client piattaforma UCCX](#)

[Certificato client servizio di notifica](#)

[Certificato client Finesse](#)

[Certificato client SocialMiner/CCP](#)

[Certificato client CUIC](#)

[Applicazioni di terze parti accessibili da script](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Problema - ID utente/password non validi](#)

[Cause](#)

[Soluzione](#)

[Problema - CSR SAN e certificato SAN non corrispondono](#)

[Cause](#)

[Soluzione](#)

[Problema - NET::ERR_CERT_COMMON_NAME_INVALID](#)

[Cause](#)

[Soluzione](#)

[Ulteriori informazioni](#)

[Difetti del certificato](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare Cisco Unified Contact Center Express (UCCX) per l'utilizzo di certificati autofirmati e firmati.

Prerequisiti

Requisiti

Prima di procedere con le operazioni di configurazione descritte in questo documento, assicurarsi di avere accesso alla pagina Amministrazione del sistema operativo (OS) per le seguenti applicazioni:

- UCCX
- SocialMiner/CCP

Un amministratore può inoltre accedere all'archivio certificati nei PC client dell'agente e del supervisore.

FQDN, DNS e domini

È necessario che tutti i server nella configurazione UCCX siano installati con i server DNS (Domain Name System) e i nomi di dominio. È inoltre necessario che agenti, supervisori e amministratori accedano alle applicazioni di configurazione UCCX tramite il nome di dominio completo (FQDN).

Se il dominio viene modificato o popolato per la prima volta, i certificati possono essere rigenerati. Dopo aver aggiunto il nome di dominio alla configurazione del server, rigenerare tutti i certificati Tomcat prima di installarli nelle altre applicazioni, nei browser client o al momento della generazione della richiesta di firma del certificato (CSR) per la firma.

Componenti usati

Le informazioni descritte in questo documento si basano sui seguenti componenti hardware e software:

- Servizi Web UCCX
- Servizio di notifica UCCX
- Piattaforma UCCX Tomcat
- Cisco Finesse Tomcat
- Cisco Unified Intelligence Center (CUIC) Tomcat
- SocialMiner/CCP Tomcat

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Con l'introduzione del coresidente Finesse e CUIC, l'integrazione tra UCCX e SocialMiner per la posta elettronica e la chat e l'utilizzo di MediaSense per registrare, comprendere e installare certificati tramite Finesse, la capacità di risolvere i problemi relativi ai certificati è ora di fondamentale importanza.

In questo documento viene descritto l'utilizzo di certificati autofirmati e firmati nell'ambiente di configurazione UCCX per:

- Servizi di notifica UCCX
- Servizi Web UCCX
- Script UCCX
- Co-Resident Finesse
- CUIC co-residente (dati in tempo reale e report cronologici)
- SocialMiner (chat)

I certificati, firmati o autofirmati, devono essere installati sia sulle applicazioni (server) nella configurazione UCCX, sia sui desktop dell'agente e del supervisore del client.

Il supporto multi-SAN è stato aggiunto in UCCX a partire dalla versione 11.6.2.

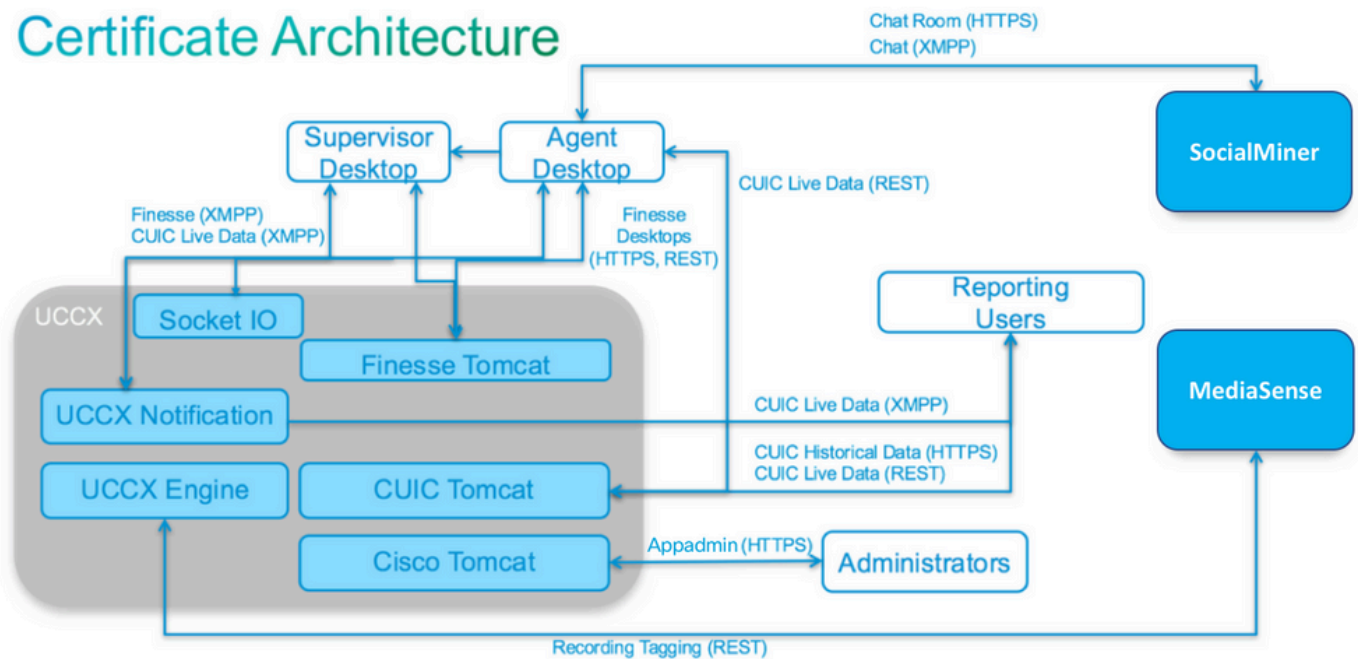
Pubblicamente, i certificati CA firmati su SocialMiner/CCP sono necessari per il funzionamento della chat esterna su Internet.

Configurazione

In questa sezione viene descritto come configurare UCCX per l'utilizzo di certificati autofirmati e firmati.

Diagramma di configurazione

Certificate Architecture



Certificati firmati

Il metodo consigliato per la gestione dei certificati per la configurazione UCCX consiste nell'utilizzare certificati firmati. Questi certificati possono essere firmati da un'Autorità di certificazione (CA) interna o da un'Autorità di certificazione (CA) di terze parti.

Nei principali browser, ad esempio Mozilla Firefox e Microsoft Edge, per impostazione predefinita vengono installati i certificati radice per le CA di terze parti conosciute. I certificati per le applicazioni di configurazione UCCX firmati da queste CA sono attendibili per impostazione predefinita, in quanto la catena di certificati termina con un certificato radice già installato nel browser.

Il certificato radice di una CA interna può inoltre essere preinstallato nel browser client tramite Criteri di gruppo o altre configurazioni correnti.

È possibile scegliere se i certificati dell'applicazione di configurazione UCCX devono essere firmati da un'autorità di certificazione di terze parti nota oppure da un'autorità di certificazione interna in base alla disponibilità e alla preinstallazione del certificato radice per le autorità di certificazione nel browser client.

Installa certificati applicazione Tomcat firmati

Completare i seguenti passaggi per ogni nodo delle applicazioni UCCX Publisher and Subscriber, SocialMiner, e MediaSense Publisher and Subscriber Administration:

1. Passare alla pagina Amministrazione del sistema operativo e scegliere Protezione > Gestione certificati.
2. Fare clic su Genera CSR.
3. Dall'elenco a discesa Elenco certificati, scegliere tomcat come nome del certificato e fare clic


su Genera CSR.

4. Passare a Sicurezza > Gestione certificati e scegliere Scarica CSR.
5. Dalla finestra popup, scegliere tomcat dall'elenco a discesa e fare clic su Download CSR.

Inviare il nuovo CSR alla CA di terze parti o firmarlo con una CA interna, come descritto in precedenza. Questo processo può produrre i certificati firmati seguenti:


- Certificato radice per la CA
- Certificato applicazione UCCX Publisher
- Certificato applicazione sottoscrittore UCCX
- Certificato applicazione SocialMiner/CCP

 Nota: lasciare il campo Distribuzione nel CSR come nome di dominio completo del server.


 Nota: il certificato SAN (Multi-Server) è supportato per UCCX a partire dalla versione 11.6. Tuttavia, la SAN può includere solo UCCX Node-1 e Node-2. Altri server, ad esempio SocialMiner, non possono essere inclusi nella SAN di UCCX. Vedere in fondo alla pagina per un esempio di SAN CUCM valido anche per UCCX.

 Nota: UCCX supporta solo lunghezze delle chiavi dei certificati di 1024 e 2048 bit.

Completare la procedura seguente in ogni server applicazioni per caricare il certificato radice e il certificato dell'applicazione nei nodi:


 Nota: se si caricano i certificati radice e intermedi in un server di pubblicazione (UCCX o MediaSense), è possibile replicarli automaticamente nel Sottoscrittore. Non è necessario caricare i certificati radice o intermedi negli altri server non publisher della configurazione se tutti i certificati delle applicazioni sono firmati tramite la stessa catena di certificati.

1. Passare alla pagina Amministrazione del sistema operativo e scegliere Protezione > Gestione certificati.
2. Fare clic su Carica certificato.
3. Caricare il certificato radice e scegliere tomcat-trust come tipo di certificato.
4. Fare clic su Upload File.
5. Fare clic su Carica certificato.
6. Caricare il certificato applicazione e scegliere tomcat come tipo di certificato.
7. Fare clic su Upload File.

 Nota: se una CA subordinata firma il certificato, caricare il certificato radice della CA subordinata come certificato tomcat-trust anziché come certificato radice. Se viene rilasciato un certificato intermedio, oltre al certificato dell'applicazione caricare il certificato nell'archivio Tomcat-trust.

8. Al termine, riavviare le seguenti applicazioni:

- Cisco MediaSense Publisher e Subscriber
- Cisco SocialMiner
- Cisco UCCX Publisher e Subscriber

 Nota: quando si utilizza UCCX e SocialMiner 11.5, è disponibile un nuovo certificato denominato tomcat-ECDSA. Quando si carica un certificato tomcat-ECDSA firmato nel server, caricare il certificato dell'applicazione come certificato tomcat-ECDSA e non come certificato tomcat. Per ulteriori informazioni su ECDSA, fare riferimento alla sezione Informazioni correlate per il collegamento che consente di comprendere e configurare i certificati ECDSA. A partire dalla versione 11.6, l'utilizzo dei certificati ECDSA è stato completamente rimosso dalla soluzione UCCX. Ciò include UCCX, SM/CCP, CUIC e Finesse.

Certificati autofirmati

Installazione Su Server Periferici

Tutti i certificati utilizzati nella configurazione UCCX sono preinstallati nelle applicazioni di configurazione e autofirmati. Questi certificati autofirmati non sono implicitamente attendibili quando vengono presentati a un browser client o a un'altra applicazione di configurazione. Sebbene sia consigliabile firmare tutti i certificati nella configurazione UCCX, è possibile utilizzare i certificati autofirmati preinstallati.

Per ogni relazione tra applicazioni, è necessario scaricare il certificato appropriato e caricarlo nell'applicazione. Per ottenere e caricare i certificati, completare i seguenti passaggi:

1. Accedere alla pagina Amministrazione del sistema operativo dell'applicazione e scegliere Protezione > Gestione certificati.
2. Fare clic sul file certificato .pem appropriato e scegliere Scarica:

Status

Status: Ready

Certificate Settings

File Name	tomcat.pem
Certificate Name	tomcat
Certificate Type	certs
Certificate Group	product-cpi
Description	Self-signed certificate generated by system

Certificate File Data

Regenerate

Download

Generate CSR

3. Per caricare un certificato nell'applicazione appropriata, passare alla pagina Amministrazione del sistema operativo e scegliere Protezione > Gestione certificati.
4. Fare clic su Carica certificato/Catena certificati:



5. Al termine, riavviare i seguenti server:

- Cisco SocialMiner
- Cisco UCCX Publisher e Subscriber

Per installare certificati autofirmati nel computer client, utilizzare Criteri di gruppo o Gestione pacchetti oppure installarli singolarmente nel browser di ogni PC agente.

Per Microsoft Edge, installare i certificati autofirmati lato client nell'archivio Autorità di certificazione radice attendibili.

Per Mozilla Firefox, completare questi passaggi:

1. Selezionare Strumenti > Opzioni.
2. Fare clic sulla scheda Avanzate.
3. Fare clic su Visualizza certificati.
4. Passare alla scheda Server.
5. Fare clic su Add Exception (Aggiungi eccezione).

Rigenerazione dei certificati autofirmati

Se i certificati autofirmati scadono, è necessario rigenerarli e ripetere le operazioni di configurazione descritte in Installazione sui server periferici.

1. Accedere all'applicazione Amministrazione del sistema operativo e scegliere Sicurezza > Gestione certificati.
2. Fate clic sul certificato appropriato e scegliete Rigenera (Regenerate).
3. È necessario riavviare il server di cui è stato rigenerato il certificato.
4. Per ogni relazione tra applicazioni, è necessario scaricare il certificato appropriato e caricarlo nell'applicazione dalla procedura di configurazione da Installazione su server periferici.

Integrazione e configurazione client

UCCX-to-SocialMiner

UCCX utilizza le API REST e di notifica di SocialMiner per gestire i contatti e la configurazione della posta elettronica. Entrambi i nodi UCCX devono utilizzare l'API REST di SocialMiner ed essere notificati dal servizio di notifica SocialMiner, quindi installare il certificato SocialMiner Tomcat su entrambi i nodi UCCX.

Caricare la catena di certificati firmata o autofirmata del server SocialMiner nel keystore UCCX tomcat-trust.

Caricare il certificato UCCX tomcat dai nodi del server di pubblicazione e del sottoscrittore nel server SocialMiner come keystore tomcat-trust.

Certificato client AppAdmin UCCX

Il certificato client UCCX AppAdmin viene utilizzato per l'amministrazione del sistema UCCX. Per installare il certificato UCCX AppAdmin per gli amministratori UCCX, nel PC client passare a <https://<UCCX FQDN>/appadmin/main> per ogni nodo UCCX e installare il certificato tramite il browser.

Certificato client piattaforma UCCX

I servizi Web UCCX vengono utilizzati per la consegna di contatti di chat ai browser client. Per installare il certificato della piattaforma UCCX per gli agenti e i supervisor UCCX, nel PC client passare a <https://<UCCX FQDN>/appadmin/main> per ciascuno dei nodi UCCX e installare il

certificato tramite il browser.

Certificato client servizio di notifica

Il servizio di notifica CCX viene utilizzato da Finesse, UCCX e CUIC per inviare informazioni in tempo reale al desktop del client tramite il protocollo XMPP (Extensible Messaging and Presence Protocol). È utilizzato per la comunicazione Finesse in tempo reale e per CUIC Live Data.

Per installare il certificato client del Servizio di notifica sul PC degli agenti e dei supervisor o degli utenti per i rapporti che utilizzano Live Data, passare a <https://<FQDN UCCX>:7443/> per ciascuno dei nodi UCCX e installare il certificato tramite il browser.

Certificato client Finesse

Il certificato client Finesse viene utilizzato dai desktop Finesse per connettersi all'istanza Finesse Tomcat ai fini della comunicazione API REST tra il desktop e il server Finesse coresidente.

Per installare il certificato Finesse per agenti e supervisor, nel PC client passare a <https://<UCCX FQDN>:8445/8445> per ciascuno dei nodi UCCX e installare il certificato tramite le richieste del browser.

Per installare il certificato Finesse per gli amministratori Finesse, nel PC client passare a <https://<UCCX FQDN>:8445/cfadmin> per ciascuno dei nodi UCCX e installare il certificato tramite le richieste del browser.

Certificato client SocialMiner/CCP

Il certificato Tomcat di SocialMiner deve essere installato nel computer client. Quando un agente accetta una richiesta di chat, il gadget Chat viene reindirizzato a un URL che rappresenta la chat room. Questa chat room è ospitata dal server SocialMiner e contiene il contatto del cliente o della chat.

Per installare il certificato SocialMiner nel browser, nel PC client passare a <https://<FQDN SocialMiner>/> e installare il certificato tramite le richieste del browser.

Certificato client CUIC

Il certificato CUIC Tomcat può essere installato sul computer client per gli agenti, i supervisor e gli utenti di report che utilizzano l'interfaccia Web CUIC per i report cronologici o i report Live Data sia nella pagina Web CUIC che nei gadget sul desktop.

Per installare il certificato CUIC Tomcat nel browser, nel PC client passare a <https://<UCCX FQDN>:8444/2010> e installare il certificato tramite le richieste del browser.

Certificato CUIC Live Data (dall'11.x)

CUIC utilizza il servizio I/O socket per i dati Live back-end. Questo certificato può essere installato sul computer client per gli agenti, i supervisor e gli utenti di report che utilizzano l'interfaccia Web

CUIC per Live Data o che utilizzano i gadget Live Data all'interno di Finesse.

Per installare il certificato di I/O socket nel browser, nel PC client passare a <https://<UCCX FQDN>:12015/12015> e installare il certificato tramite le richieste del browser.

Applicazioni di terze parti accessibili da script

Se uno script UCCX è progettato per accedere a una posizione sicura su un server di terze parti (ad esempio, il passaggio Ottieni documento URL per un URL HTTPS o Effettua una chiamata rimanente per un URL REST HTTPS), caricare la catena di certificati firmata o autofirmata del servizio di terze parti nel keystore UCCX tomcat-trust. Per ottenere questo certificato, accedere alla pagina Amministrazione del sistema operativo UCCX e scegliere Carica certificato.

Il motore UCCX è configurato in modo da ricercare nella piattaforma Tomcat keystore le catene di certificati di terze parti quando vengono presentati con questi certificati da applicazioni di terze parti quando accedono a percorsi sicuri tramite passaggi di script.

L'intera catena di certificati deve essere caricata nel keystore Tomcat della piattaforma, accessibile tramite la pagina di amministrazione del sistema operativo, poiché il keystore Tomcat non contiene certificati radice per impostazione predefinita.

Dopo aver completato queste azioni, riavviare Cisco UCCX Engine.

Verifica

Per verificare che tutti i certificati siano installati correttamente, è possibile provare le funzionalità descritte in questa sezione. Se non vengono visualizzati errori e tutte le funzionalità funzionano correttamente, i certificati vengono installati correttamente.

- Configurare Agent Web Chat tramite SocialMiner/CCP. Inserisci un contatto di chat tramite il modulo Web. Verificare che l'agente riceva il banner per accettare il contatto di chat e che, una volta accettato il contatto di chat, il modulo di chat venga caricato correttamente e l'agente possa ricevere e inviare messaggi di chat.
- Tentativo di accedere a un agente tramite Finesse. Verificare che non vengano visualizzati avvisi relativi ai certificati e che la pagina Web non richieda l'installazione dei certificati nel browser. Verificare che l'agente sia in grado di modificare correttamente gli stati e che all'agente venga presentata correttamente una nuova chiamata in UCCX.
- Dopo aver configurato i gadget Live Data nel layout del desktop dell'agente e del supervisore Finesse, accedere a un agente, a un supervisore e a un utente per i report. Verificare che i gadget Live Data vengano caricati correttamente, che i dati iniziali siano inseriti nel gadget e che i dati vengano aggiornati in caso di modifica dei dati sottostanti.
- Tentativo di connessione da un browser all'URL di AppAdmin su entrambi i nodi UCCX. Verificare che non vengano visualizzati avvisi relativi al certificato quando richiesto con la pagina di accesso.

Risoluzione dei problemi

Problema - ID utente/password non validi

Gli agenti UCCX Finesse non sono in grado di eseguire l'accesso. Errore "ID utente/password non valida".

Cause

Unified CCX genera un'eccezione "SSLHandshakeException" e non riesce a stabilire una connessione con Unified CM.

Soluzione

- Verificare che il certificato Unified CM Tomcat non sia scaduto.
- Verificare che tutti i certificati caricati in Unified CM dispongano di una delle seguenti estensioni contrassegnate come critiche:
 - Utilizzo chiave X509v3 (OID - 2.5.29.15)
 - Vincoli di base X509v3 (OID - 2.5.29.19)Se si contrassegna qualsiasi altra estensione come critica, la comunicazione tra Unified CCX e Unified CM non riesce a causa di un errore di verifica del certificato di Unified CM.

Problema - CSR SAN e certificato SAN non corrispondono

Il caricamento di un certificato firmato da un'autorità di certificazione visualizza l'errore "CSR SAN and Certificate SAN does not match".

Cause

La CA può aver aggiunto un altro dominio padre nel campo SAN (Subject Alternative Names) del certificato. Per impostazione predefinita, il CSR può avere le seguenti SAN:

```
NomeOggetto [  
  example.com (nomeDNS)  
  hostname.example.com (nomeDNS)  
]
```

Le CA possono restituire un certificato con un'altra SAN aggiunta al certificato:
www.hostname.example.com. Il certificato può avere una SAN aggiuntiva in questo caso:

```
NomeOggetto [  
  example.com (nomeDNS)  
  hostname.example.com (nomeDNS)  
  
  www.hostname.example.com (dNSName)  
]
```

Ciò causa un errore di mancata corrispondenza SAN.

Soluzione

Nella sezione 'Nome alternativo soggetto (SAN)' della pagina UCCX 'Generate Certificate Signing Request', generare il CSR con un campo Dominio padre vuoto. In questo modo, il CSR non viene generato con un attributo SAN, la CA può formattare le SAN e non vi può essere una mancata corrispondenza dell'attributo SAN quando si carica il certificato in UCCX. Si noti che il valore predefinito del campo Dominio padre corrisponde al dominio del server UCCX, pertanto il valore deve essere rimosso in modo esplicito durante la configurazione delle impostazioni per il CSR.

Problema - NET::ERR_CERT_COMMON_NAME_INVALID

Quando si accede a una qualsiasi pagina Web di UCCX, MediaSense o SocialMiner, viene visualizzato un messaggio di errore.

"La tua connessione non è privata.

Gli aggressori possono tentare di rubare le informazioni da <FQDN_server>, ad esempio password, messaggi o carte di credito. NET::ERR_CERT_COMMON_NAME_INVALID

Impossibile provare che il server è <FQDN_server>. Il certificato di protezione proviene da [missing_subjectAltName]. Ciò può essere causato da una configurazione errata o da un utente non autorizzato che intercetta la connessione."

Cause

Chrome versione 58 ha introdotto una nuova funzione di sicurezza in cui segnala che il certificato di un sito web non è sicuro se il suo nome comune (CN) non è incluso anche come SAN.

Soluzione

- È possibile passare a Avanzate > Procedi a <FQDN_server> (non sicuro) per continuare con il sito e accettare l'errore del certificato.
- È possibile evitare l'errore anche con i certificati firmati dall'autorità di certificazione. Quando si genera un CSR, l'FQDN del server viene incluso come rete SAN. L'autorità di certificazione può firmare il CSR e, dopo aver caricato nuovamente il certificato firmato nel server, il certificato del server dispone del nome di dominio completo (FQDN) nel campo SAN in modo che l'errore non possa essere presentato.

Ulteriori informazioni

Vedere la sezione "Rimuovere il supporto per la corrispondenza di commonName nei certificati" in [Deprecazioni e rimozioni in Chrome 58](#).

Difetti del certificato

- Cisco bug ID [CSCvb46250](#) - UCCX: impatto del certificato Tomcat ECDSA su Finesse Live Data
- Cisco bug ID [CSCvb58580](#) - Impossibile accedere a SocialMiner con tomcat e tomcat-ECDSA firmati da RSA CA
- ID bug Cisco [CSCvd56174](#) - UCCX: errore di accesso dell'agente Finesse a causa di SSLHandshakeException
- ID bug Cisco [CSCuv89545](#) - Vulnerabilità Finesse Logjam

Informazioni correlate

- [Comprensione dei certificati ECDSA in una soluzione UCCX](#)
- [Supporto SHA 256 per UCCX](#)
- [Esempio di configurazione del cluster di comunicazioni unificate con nome alternativo del soggetto con firma CA e più server](#)
- [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).