Informazioni sui certificati ECDSA in una soluzione UCCX

Sommario

Introduzione

Questo documento descrive come configurare la soluzione Cisco Unified Contact Center Express (UCCX) per l'utilizzo dei certificati ECDSA (Elliptical Curve Digital Signature Algorithm).

Prerequisiti

Requisiti

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

- UCCX
- SocialMiner
- Cisco Unified Communications Manager (CUCM)
- Configurazione del certificato della soluzione UCCX - http://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/118855-configure-uccx-00.html

L'amministratore deve inoltre avere accesso all'archivio certificati nei PC client dell'agente e del supervisore.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

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

Come parte della certificazione CC (Common Criteria), Cisco Unified Communications Manager ha aggiunto i certificati ECDSA nella versione 11.0. Ciò riguarda tutti i prodotti VOS (Voice Operating System), quali UCCX, SocialMiner, MediaSense e così via, a partire dalla versione 11.5.

Per ulteriori informazioni sull'**algoritmo di firma digitale a curva ellittica,** visitare il sito: https://www.maximintegrated.com/en/app-notes/index.mvp/id/5767

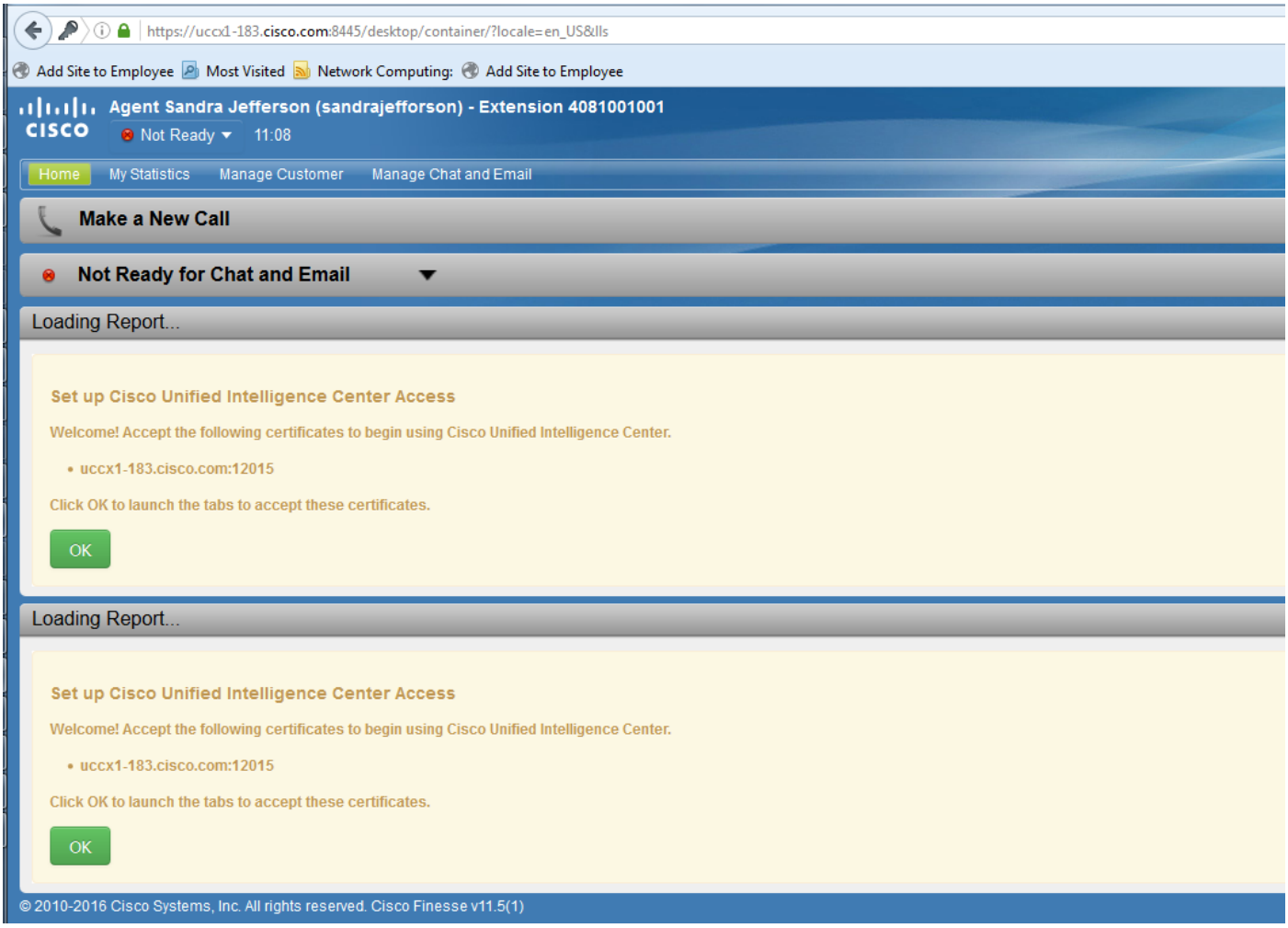
Per quanto riguarda la soluzione UCCX, quando si esegue l'aggiornamento alla versione 11.5, viene offerto un certificato aggiuntivo che non era presente in precedenza. Questo è il certificato Tomcat-ECDSA.

Questo è stato documentato anche nella comunicazione preliminare: https://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/200651-UCCX-Version-11-5-Prerelease-Field-Commu.html?cachemode=refresh

Esperienza agente

Dopo un aggiornamento alla versione 11.5, all'agente potrebbe essere richiesto di accettare i certificati sul desktop Finesse a seconda che il certificato sia autofirmato o firmato da CA (Certification Authority).

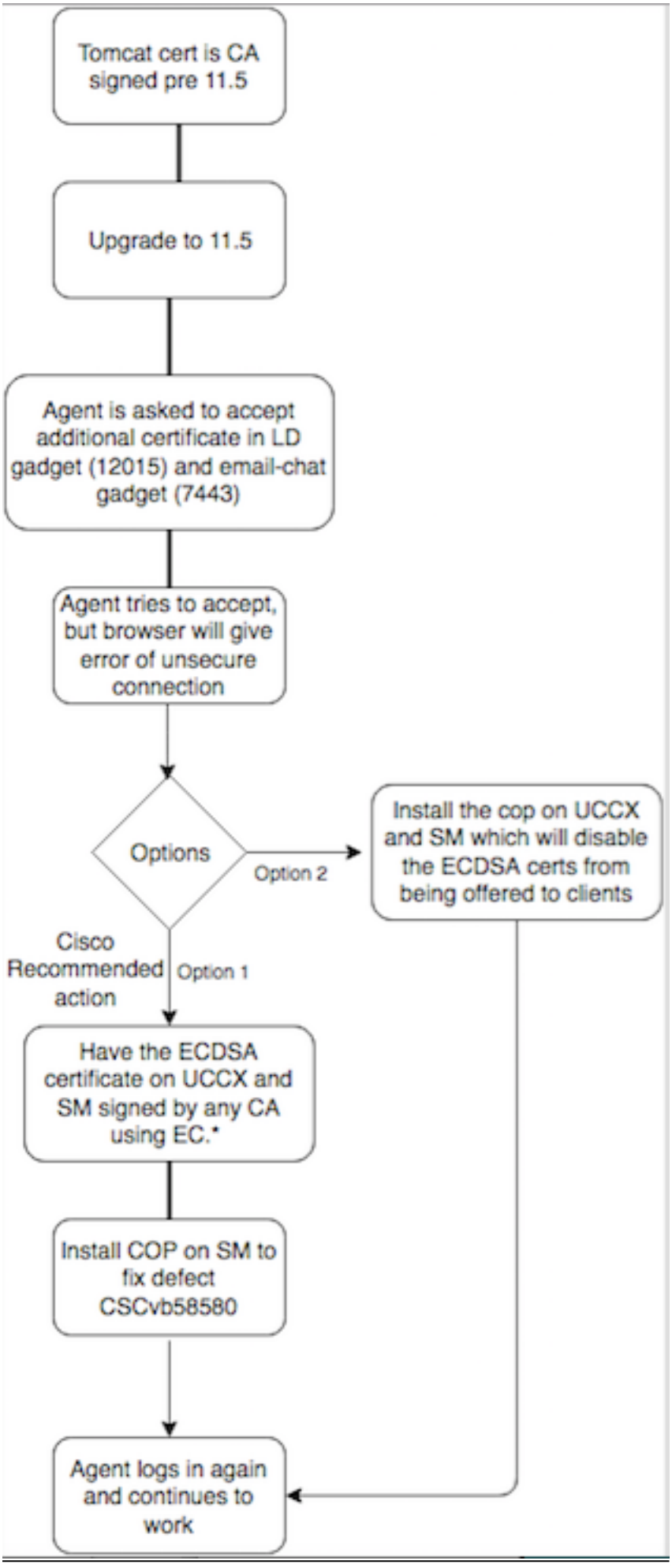
Esperienza utente dopo l'aggiornamento alla versione 11.5



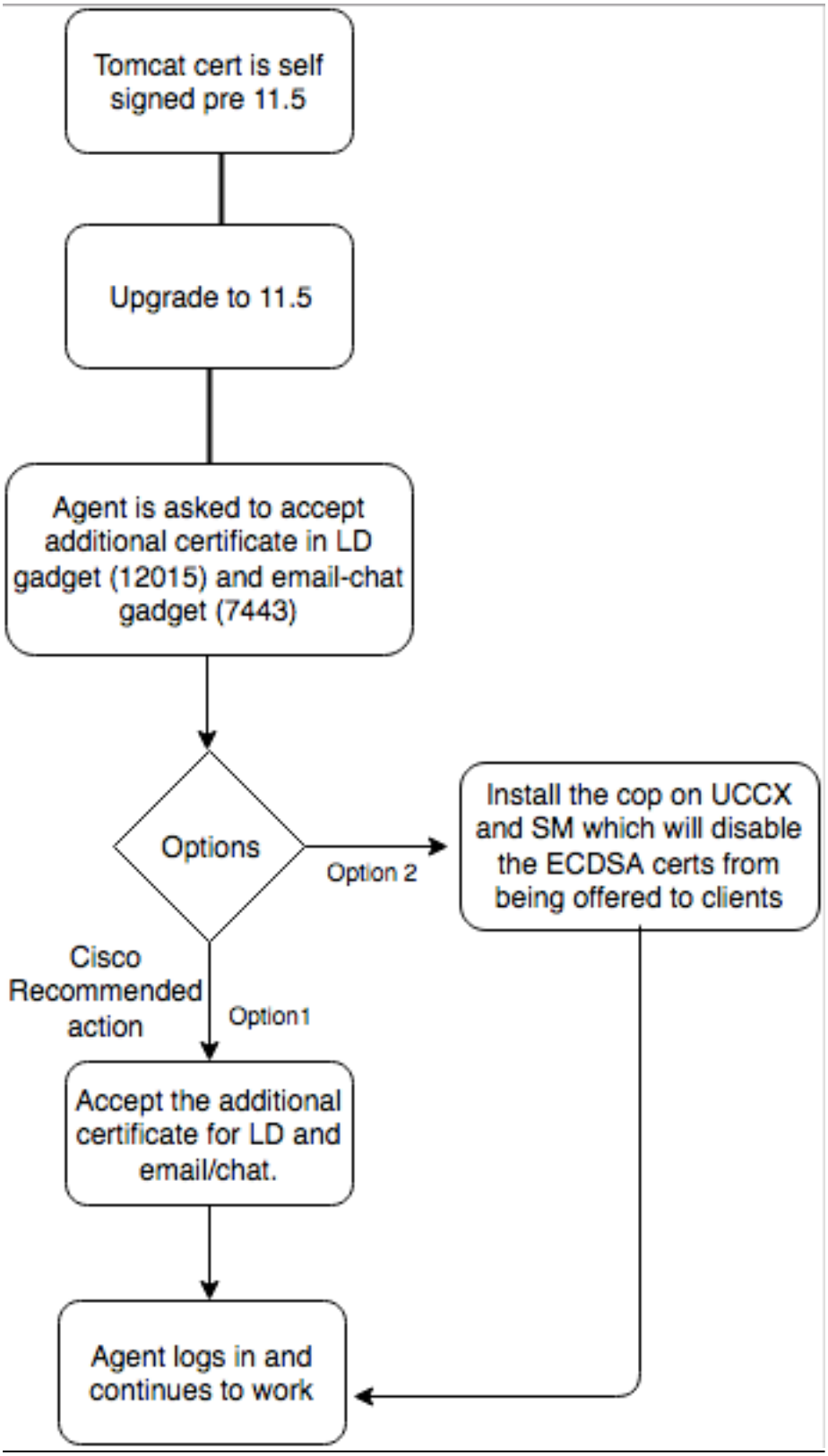
Questo perché al desktop Finesse viene ora offerto un certificato ECDSA che non era stato offerto in precedenza.

Procedura

Pre-aggiornamento certificati firmati CA


Tomcat cert is CA signed pre 11.5
Upgrade to 11.5
Agent is asked to accept additional certificate in LD gadget (12015) and email-chat gadget (7443)
Agent tries to accept, but browser will give error of unsecure connection
Options
Option 2
Install the cop on UCCX and SM which will disable the ECDSA certs from being offered to clients
Cisco Recommended action
Option 1
Have the ECDSA certificate on UCCX and SM signed by any CA using EC.*
Install COP on SM to fix defect CSCvb58580
Agent logs in again and continues to work

Certificati autofirmati pre-aggiornamento



Configurazione

La procedura consigliata per questo certificato

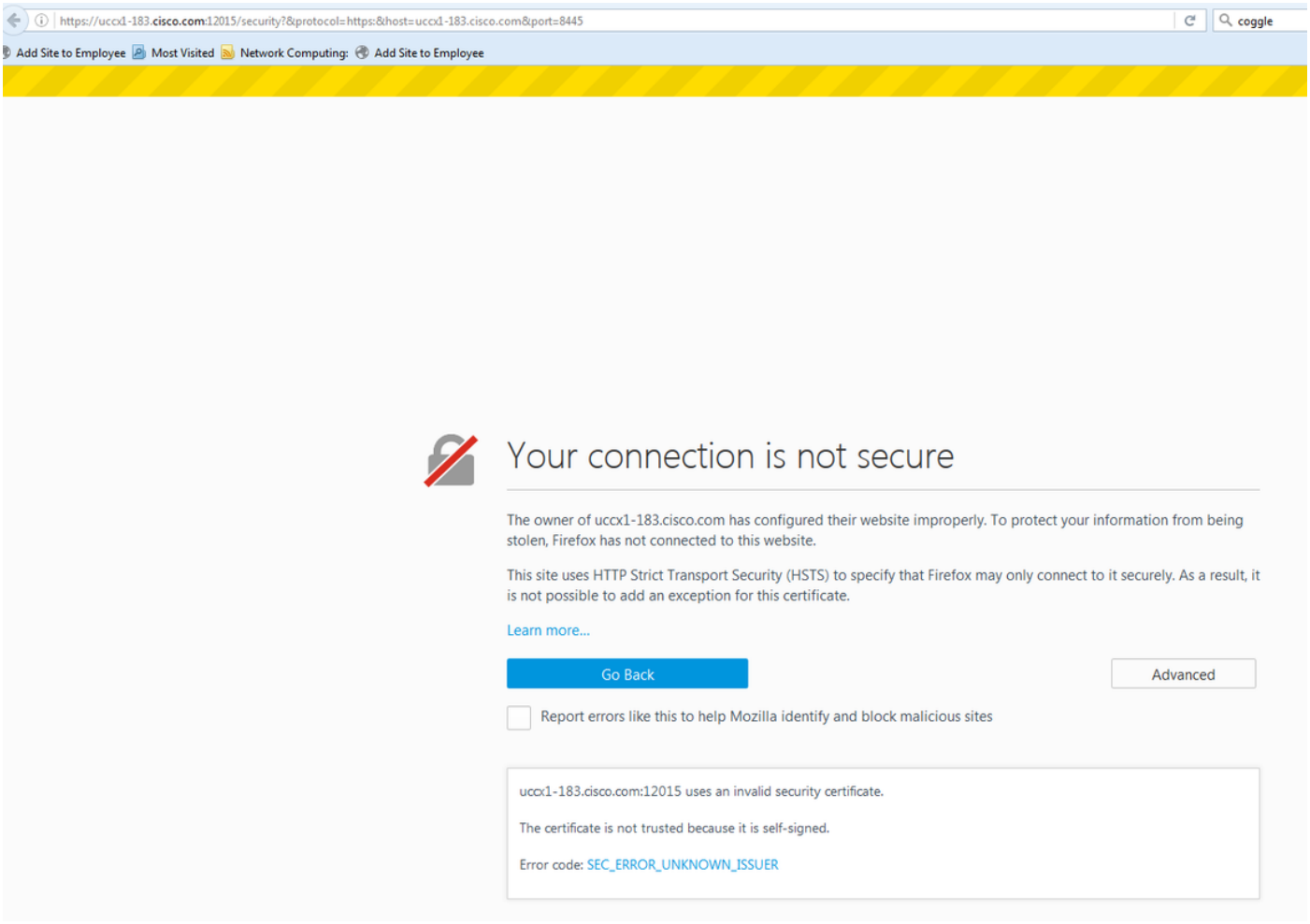
Certificati firmati per UCCX e SocialMiner

Se si utilizzano certificati firmati dall'autorità di certificazione, questo certificato ECDSA deve essere firmato da un'autorità di certificazione (CA) insieme ad altri certificati

> **Nota:** Se l'autorità di certificazione firma il certificato ECDSA con RSA, il certificato non verrà presentato al client. Per una maggiore sicurezza, i certificati ECDSA offerti al client sono la procedura consigliata.

> **Nota**: se il certificato ECDSA su SocialMiner è firmato da una CA con RSA, si verificano problemi con la posta elettronica e la chat. Questa condizione è documentata nel caso del difetto CSCvb58580 ed è disponibile un file cop. Questo COP garantisce che i certificati ECDSA non vengano offerti ai client. Se si dispone di una CA in grado di firmare i certificati ECDSA solo con RSA, non utilizzare questo certificato.Utilizzare la copia in modo che il certificato ECDSA non venga offerto e si disponga di un ambiente solo RSA.

Se si utilizzano certificati firmati dall'autorità di certificazione e dopo l'aggiornamento non si dispone del certificato ECDSA firmato e caricato, gli agenti riceveranno un messaggio per accettare il certificato aggiuntivo. Facendo clic su **OK,** vengono reindirizzati al sito Web. Tuttavia, l'operazione non riesce a causa dell'imposizione della protezione dal lato del browser, poiché il certificato ECDSA è autofirmato e gli altri certificati Web sono firmati dalla CA. Tale comunicazione è percepita come un rischio per la sicurezza.



Completare questi passaggi su ogni nodo di UCCX Publisher e Subscriber e SocialMiner, dopo un aggiornamento a UCCX e SocialMiner nella versione 11.5:

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-ECDSA** 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-ECDSA** dall'elenco a discesa e fare clic su **Download CSR**.

Inviare il nuovo CSR all'autorità di certificazione di terze parti o firmarlo con un'autorità di certificazione interna che firma i certificati CE. Verranno generati i certificati firmati seguenti:

- Certificato radice per la CA (se si utilizza la stessa CA per i certificati delle applicazioni e per i certificati CE, è possibile ignorare questo passaggio)
- Certificato firmato ECDSA di UCCX Publisher
- Certificato firmato ECDSA sottoscrittore UCCX
- Certificato firmato ECDSA SocialMiner

Nota: Se si caricano i certificati radice e intermedi in un server di pubblicazione (UCCX), questi verranno replicati 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. È inoltre possibile ignorare il caricamento del certificato radice se la stessa CA firma il certificato EC e questa operazione è già stata eseguita durante la configurazione dei certificati dell'applicazione UCCX.

Completare questi passaggi su ciascun server applicazioni per caricare il certificato radice e il certificato EC nei nodi:

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 dell'applicazione e scegliere **tomcat-ECDSA** come tipo di certificato.

7. Fare clic su **Upload File**.

Nota: Se il certificato viene firmato da una CA subordinata, caricare il certificato radice della CA subordinata come certificato *tomcat-trust* anziché come certificato radice. Se viene rilasciato un certificato intermedio, caricare il certificato nell'archivio *tomcat-trust* oltre al

certificato dell'applicazione. È inoltre possibile ignorare il caricamento del certificato radice se la stessa CA firma il certificato EC e questa operazione è già stata eseguita durante la configurazione dei certificati dell'applicazione UCCX.

8. Al termine, riavviare le seguenti applicazioni:

   Cisco SocialMinerCisco UCCX Publisher e Subscriber

Certificati autofirmati per UCCX e SocialMiner

Se UCCX o SocialMiner utilizzano certificati autofirmati, gli agenti devono essere avvisati di accettare l'avviso relativo al certificato che vengono visualizzati nel gadget e-mail di chat e nei gadget Live Data.

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

Per Internet Explorer, 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 **Aggiungi eccezione**.

1. **Nota:** È inoltre possibile aggiungere l'eccezione di protezione per installare il certificato che equivale al processo descritto in precedenza. Si tratta di una configurazione unica sul client.

Domande frequenti (FAQ)

Si dispone di certificati firmati da un'autorità di certificazione e si desidera utilizzare un certificato ECDSA che deve essere firmato da un'autorità di certificazione dell'autorità di certificazione. In attesa che il certificato firmato dalla CA sia disponibile, è necessario che Live Data sia attivo. Cosa posso fare?

Non si desidera firmare questo certificato aggiuntivo o chiedere agli agenti di accettarlo. Cosa posso fare?

Sebbene si consiglia di presentare i certificati ECDSA ai browser, è possibile disabilitarli. È possibile installare un file cop su UCCX e SocialMiner per garantire che solo i certificati RSA vengano presentati al client. Il certificato ECDSA rimane ancora nel keystore, ma non verrà offerto ai client.

Se si utilizza questa copia per disabilitare i certificati ECDSA offerti ai client, è possibile riabilitarla?

Sì, è disponibile una copia di rollback. Una volta applicato, il certificato potrà essere firmato e caricato nei server.

Tutti i certificati verrebbero resi ECDSA?

Al momento no, ma in futuro continueremo ad aggiornare la sicurezza sulla piattaforma VOS.

Quando si installa UCCX COP?

- Quando si utilizzano certificati autofirmati e non si desidera che gli agenti accettino certificati aggiuntivi
- Quando non è possibile ottenere un certificato aggiuntivo firmato dalla CA

Quando si installa SM COP?

- Quando si utilizzano certificati autofirmati e non si desidera che gli agenti accettino certificati aggiuntivi
- Quando non è possibile ottenere un certificato aggiuntivo firmato dalla CA
- Se si dispone di una CA in grado di firmare i certificati ECDSA solo con RSA

Quali sono i certificati offerti dalle diverse istanze del server Web per impostazione predefinita?

Combinazione di certificati/server Web	Esperienza agente predefinita dopo l'aggiornamento alla versione 11.5 (senza copia)	UCCX Tomcat	UCCX Openfire (servizio di notifica Cisco Unified CCX)	UCCX SocketIO	SocialMiner Tomcat	SocialMiner Openfire
Autoscritto Tomcat, autoscritto Tomcat-ECDSA	Agli agenti verrà richiesto di accettare il certificato nel gadget Live Data e chat-email	Autofirmato	Autofirmato	Autofirmato	Autofirmato	Autofirmato
RSA CA ha firmato Tomcat, RSA CA ha firmato Tomcat-ECDSA	Gli agenti possono utilizzare Finesse e Live Data, ma non è possibile caricare il gadget e-mail-chat e la pagina Web di SocialMiner non viene caricata.*	RSA	RSA	RSA	RSA	RSA (installare cop - CSCvb58580)
RSA CA ha firmato Tomcat,	Gli agenti possono	RSA	RSA	ECDSA	RSA	ECDSA

EC CA ha firmato Tomcat-ECDSA	utilizzare Finesse sia con Live Data che con chat-email*					
RSA CA ha firmato Tomcat, Tomcat-ECDSA	Agli agenti verrà richiesto di accettare un certificato aggiuntivo nel gadget Live Data e e-mail-chat. Accetta certificato dal gadget Live Data non riuscito. Accetta certificato dal gadget chat-posta elettronica non riuscito.*	RSA	RSA	Autofirmato (gli agenti non possono accettare a causa di una misura di sicurezza applicata dal browser. Fare riferimento alla schermata precedente. Per disabilitare i certificati ECDSA offerti ai client, è necessario ottenere il certificato firmato da una CA CE o installare la copia su UCCX.)	RSA	Autofirmato

Informazioni correlate

- UCCX ECDSA COP - https://software.cisco.com/download/release.html?mdfid=286309734&softwareid=280840578&release=11.5(1)&flowid=80822
- SocialMiner ECDSA COP - https://software.cisco.com/download/release.html?mdfid=283613136&flowid=73189&release=11.5(1)&softwareid=283812550&sortparam=
- Informazioni sul certificato UCCX - http://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/118855-configure-uccx-00.html