ECDSA-Zertifikate in einer UCCX-Lösung verstehen

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die Cisco Unified Contact Center Express (UCCX)-Lösung für die Verwendung von ECDSA-Zertifikaten (Elliptical Curve Digital Signature Algorithm) konfiguriert wird.

Voraussetzungen

Anforderungen

Bevor Sie mit den in diesem Dokument beschriebenen Konfigurationsschritten fortfahren, stellen Sie sicher, dass Sie Zugriff auf die Seite Betriebssystemverwaltung für diese Anwendungen haben:

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

Ein Administrator muss außerdem Zugriff auf den Zertifikatsspeicher der Agenten- und Supervisor-Client-PCs haben.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Im Rahmen der Common Criteria (CC)-Zertifizierung hat Cisco Unified Communications Manager ECDSA-Zertifikate in Version 11.0 hinzugefügt. Dies betrifft alle Voice Operating System (VOS)-Produkte wie UCCX, SocialMiner, MediaSense usw. ab Version 11.5.

Weitere Einzelheiten zum **Elliptic Curve Digital Signature Algorithm** finden Sie hier: https://www.maximintegrated.com/en/app-notes/index.mvp/id/5767

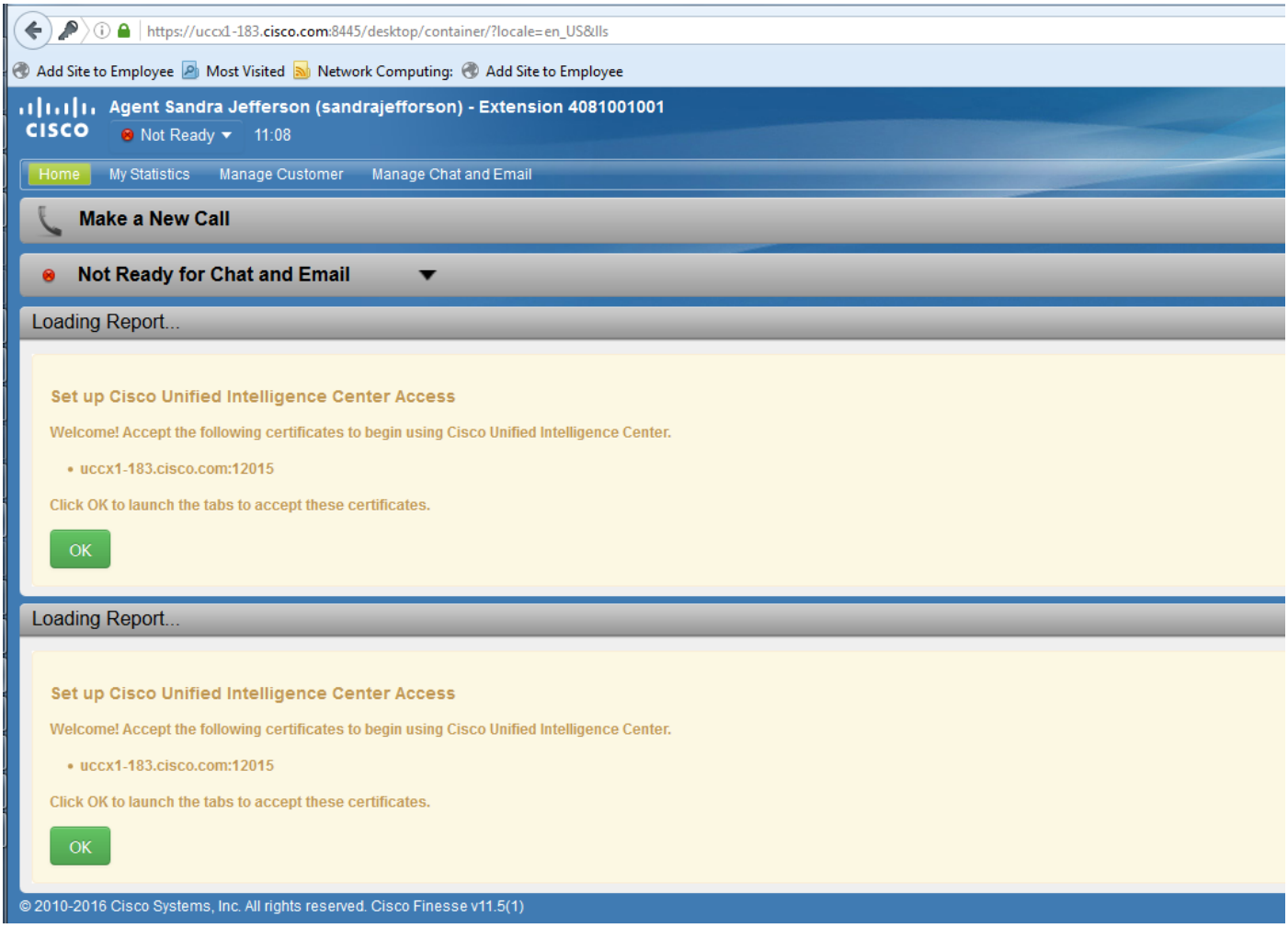
Für die UCCX-Lösung wird Ihnen beim Upgrade auf Version 11.5 ein zusätzliches Zertifikat angeboten, das zuvor nicht vorhanden war. Dies ist das Tomcat-ECDSA-Zertifikat.

Dies wurde auch in der Vorabmitteilung dokumentiert: 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

Mitarbeitererfahrung

Nach einem Upgrade auf 11.5 wird der Support-Mitarbeiter möglicherweise gebeten, Zertifikate auf dem Finesse-Desktop zu akzeptieren, je nachdem, ob das Zertifikat selbst signiert oder die Zertifizierungsstelle (Certificate Authority, CA) signiert ist.

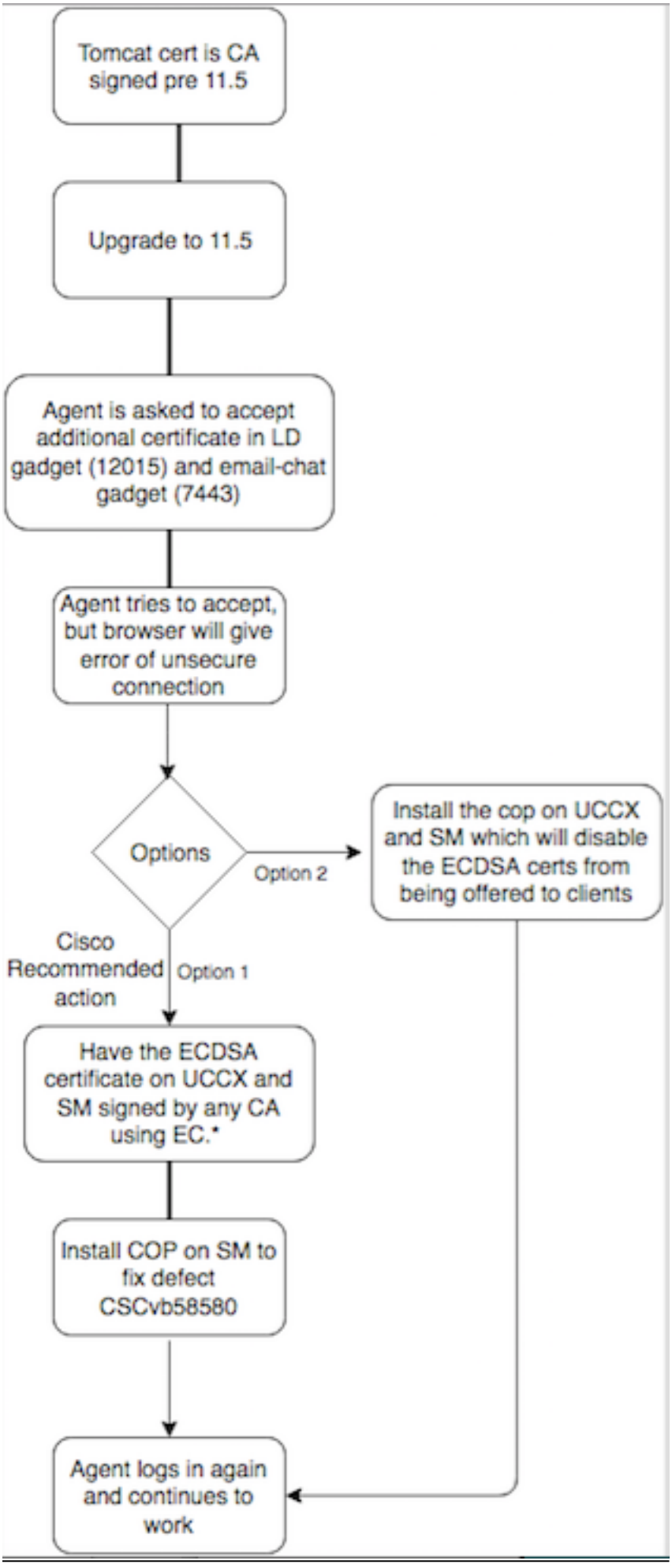
Benutzerfreundlichkeit nach dem Upgrade auf 11,5



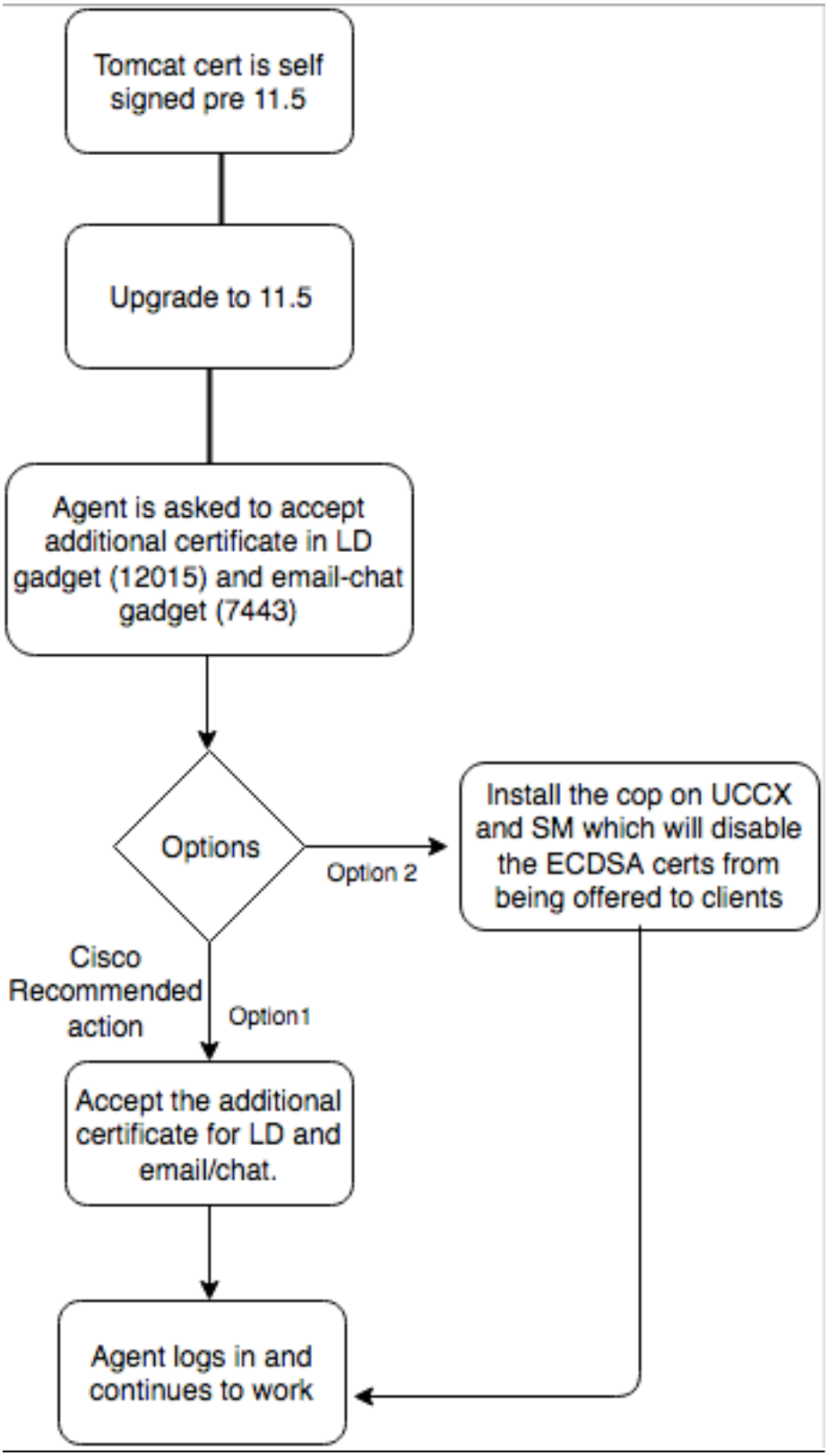
Der Grund hierfür ist, dass dem Finesse Desktop jetzt ein ECDSA-Zertifikat angeboten wird, das zuvor nicht angeboten wurde.

Vorgehensweise

Zertifikate mit CA-Signatur vor dem Upgrade


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

Selbst signierte Zertifikate vor dem Upgrade



Konfigurieren

Empfohlene Best Practice für dieses Zertifikat

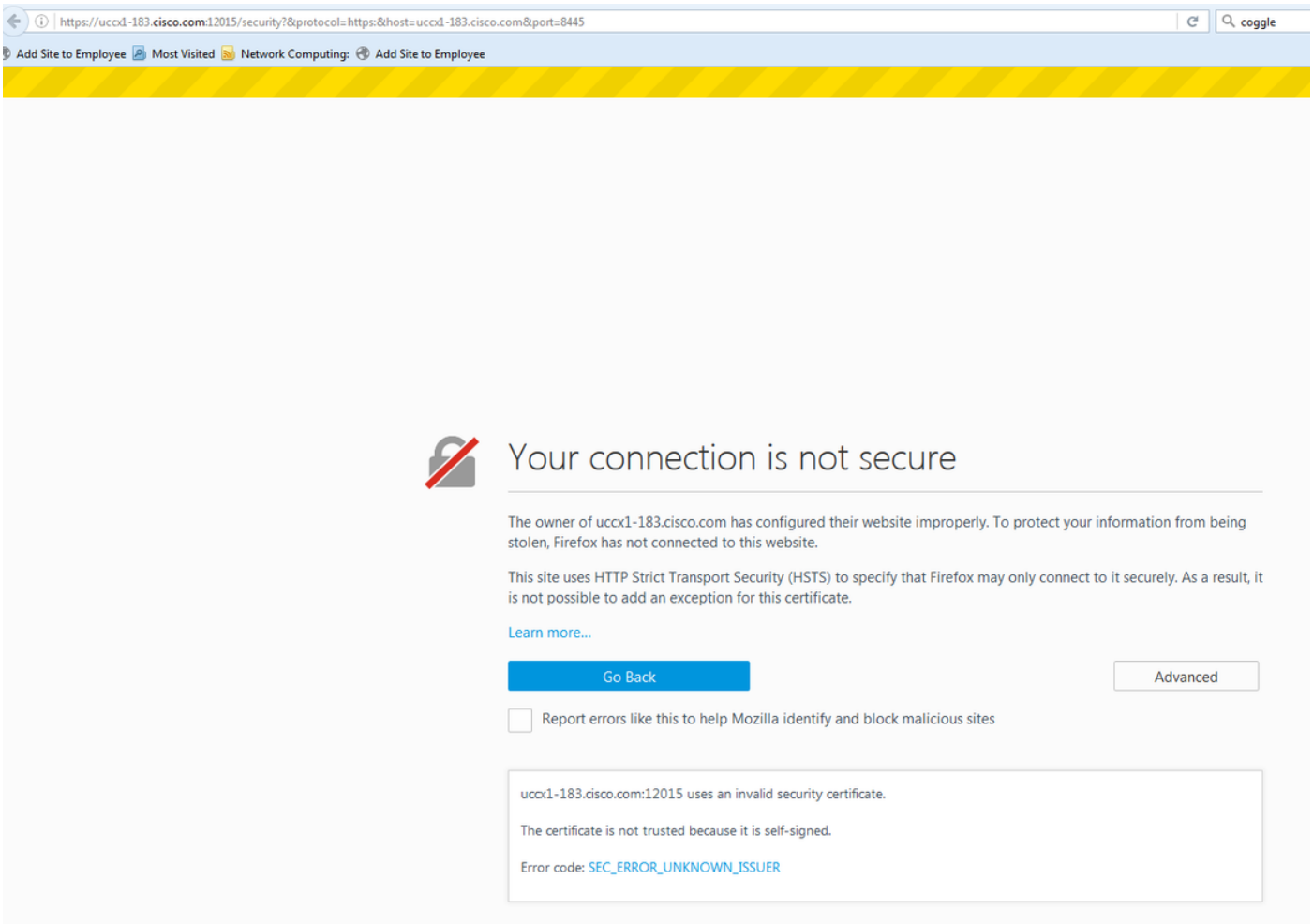
Signierte Zertifikate für UCCX und SocialMiner

Wenn Sie Zertifikate mit Zertifizierungsstellen verwenden, muss dieses ECDSA-Zertifikat zusammen mit anderen Zertifikaten von einer Zertifizierungsstelle (Certificate Authority, CA) signiert werden.

> **Hinweis**: Wenn CA dieses ECDSA-Zertifikat mit RSA unterzeichnet, wird dieses Zertifikat dem Kunden nicht vorgelegt. Zur Erhöhung der Sicherheit werden dem Kunden ECDSA-Zertifikate als Best Practice empfohlen.

> **Hinweis**: Wenn das ECDSA-Zertifikat auf SocialMiner von einer CA mit RSA signiert wird, verursacht es Probleme mit E-Mail und Chat. Dies ist im Defekt CSCvb58580 dokumentiert und es ist eine COP-Datei verfügbar. Diese COP stellt sicher, dass ECDSA-Zertifikate nicht den Kunden angeboten werden. Wenn Sie eine Zertifizierungsstelle haben, die ECDSA-Zertifikate nur mit RSA signieren kann, verwenden Sie dieses Zertifikat nicht.Verwenden Sie den Code, damit das ECDSA-Zertifikat nicht angeboten wird und Sie über eine RSA-Umgebung verfügen.

Wenn Sie Zertifikate mit CA-Signatur verwenden und nach dem Upgrade das ECDSA-Zertifikat nicht signiert und hochgeladen ist, erhalten Support-Mitarbeiter eine Nachricht, dass sie das zusätzliche Zertifikat akzeptieren. Wenn sie auf **OK** klicken**,** werden sie zur Website umgeleitet. Dies schlägt jedoch fehl, da das ECDSA-Zertifikat selbst signiert ist und Ihre anderen Webzertifikate eine Zertifizierungsstelle sind. Diese Kommunikation wird als Sicherheitsrisiko wahrgenommen.



Führen Sie nach einem Upgrade auf UCCX und SocialMiner in Version 11.5 die folgenden Schritte für jeden Knoten von UCCX Publisher, Subscriber und SocialMiner aus:

1. Navigieren Sie zur Seite **Betriebssystemverwaltung**, und wählen Sie **Sicherheit > Zertifikatsverwaltung aus**.

2. Klicken Sie auf **CSR erstellen**.

3. Wählen Sie in der Dropdown-Liste **Zertifikatliste als** Zertifikatsnamen **"tomcat-ECDSA"** aus, und klicken Sie auf **CSR generieren**.

4. Navigieren Sie zu **Sicherheit > Zertifikatsverwaltung**, und wählen Sie **CSR herunterladen aus**.

5. Wählen Sie im Popup-Fenster aus der Dropdown-Liste **tomcat-ECDSA aus**, und klicken Sie auf **CSR herunterladen**.

Senden Sie die neue CSR an die Zertifizierungsstelle eines Drittanbieters, oder unterzeichnen Sie sie mit einer internen Zertifizierungsstelle, die EG-Zertifikate unterzeichnet. Damit würden folgende unterzeichnete Zertifikate erstellt:

- Stammzertifikat für die Zertifizierungsstelle (Wenn Sie dieselbe Zertifizierungsstelle für Anwendungszertifikate und EC-Zertifikate verwenden, können Sie diesen Schritt überspringen)
- Signiertes UCCX Publisher ECDSA-Zertifikat
- Signiertes Zertifikat für UCCX-Abonnent ECDSA
- Signiertes SocialMiner ECDSA-Zertifikat

Hinweis: Wenn Sie die Root- und Zwischenzertifikate auf einen Publisher (UCCX) hochladen, wird sie automatisch auf den Subscriber repliziert. Es ist nicht erforderlich, die Root- oder Zwischenzertifikate auf die anderen Server hochzuladen, die keine Herausgeber sind, wenn alle Anwendungszertifikate über dieselbe Zertifikatkette signiert werden. Sie können diesen Upload des Root-Zertifikats auch überspringen, wenn dieselbe Zertifizierungsstelle das EC-Zertifikat signiert und dies bereits bei der Konfiguration der UCCX-Anwendungszertifikate getan wurde.

Führen Sie die folgenden Schritte auf jedem Anwendungsserver aus, um das Root-Zertifikat und das EC-Zertifikat auf die Knoten hochzuladen:

1. Navigieren Sie zur Seite **Betriebssystemverwaltung**, und wählen Sie **Sicherheit > Zertifikatsverwaltung aus**.

2. Klicken Sie auf **Zertifikat hochladen**.

3. Laden Sie das Stammzertifikat hoch, und wählen Sie **tomcat-trust** als Zertifikatstyp aus.

4. Klicken Sie auf **Datei hochladen**.

5. Klicken Sie auf **Zertifikat hochladen**.

6. Laden Sie das Anwendungszertifikat hoch, und wählen Sie **tomcat-ECDSA** als Zertifikatstyp aus.

7. Klicken Sie auf **Datei hochladen**.

   Hinweis: Wenn eine untergeordnete CA das Zertifikat signiert, laden Sie das Stammzertifikat der untergeordneten CA als *tomcat-trust*-Zertifikat anstatt als Stammzertifikat hoch. Wenn ein Zwischenzertifikat ausgestellt wird, laden Sie dieses Zertifikat zusätzlich zum Anwendungszertifikat in den *tomcat-trust*-Store hoch. Sie können diesen Upload des Root-Zertifikats auch überspringen, wenn dieselbe Zertifizierungsstelle das EC-Zertifikat signiert und dies bereits bei der Konfiguration der UCCX-Anwendungszertifikate getan wurde.
8. Starten Sie diese Anwendungen nach Abschluss des Vorgangs neu:

   Cisco SocialMinerCisco UCCX Publisher und Subscriber

Selbstsignierte Zertifikate für UCCX und SocialMiner

Wenn UCCX oder SocialMiner selbstsignierte Zertifikate verwenden, müssen die Agenten angewiesen werden, die Zertifikatswarnung zu akzeptieren, die sie im Chat-E-Mail-Gadget und in den Live-Daten-Gadgets erhalten.

Um selbstsignierte Zertifikate auf dem Client-Computer zu installieren, verwenden Sie eine Gruppenrichtlinie oder einen Paketmanager, oder installieren Sie sie einzeln im Browser jedes Agenten-PCs.

Installieren Sie für Internet Explorer die clientseitigen selbstsignierten Zertifikate im Store **Trusted Root Certifications**.

Führen Sie für Mozilla Firefox die folgenden Schritte aus:

1. Navigieren Sie zu **Extras > Optionen**.

2. Klicken Sie auf die Registerkarte **Erweitert**.

3. Klicken Sie auf **Zertifikate anzeigen**.

4. Navigieren Sie zur Registerkarte **Server**.

5. Klicken Sie auf **Ausnahme hinzufügen**.

1. **Hinweis**: Sie können auch die Sicherheitsausnahme hinzufügen, um das Zertifikat zu installieren, das dem oben beschriebenen Prozess entspricht. Dies ist eine einmalige Konfiguration auf dem Client.

Häufig gestellte Fragen (FAQ)

Wir haben Zertifikate von Zertifizierungsstellen signiert und möchten das ECDSA-Zertifikat verwenden, das von einer Zertifizierungsstelle der Europäischen Gemeinschaft unterzeichnet werden muss. Während wir auf die Verfügbarkeit des Zertifikats der Zertifizierungsstelle warten, müssen Live-Daten verfügbar sein. Was kann ich tun?

Wir möchten dieses zusätzliche Zertifikat nicht unterzeichnen oder Agenten dazu veranlassen, dieses zusätzliche Zertifikat zu akzeptieren. Was kann ich tun?

Es wird zwar empfohlen, ECDSA-Zertifikate den Browsern vorzulegen, es besteht jedoch die Möglichkeit, diese zu deaktivieren. Sie können eine COP-Datei auf UCCX und SocialMiner installieren, die sicherstellt, dass dem Client nur die RSA-Zertifikate angezeigt werden. Das ECDSA-Zertifikat verbleibt weiterhin im Keystore, wird den Kunden jedoch nicht angeboten.

Kann ich ECDSA-Zertifikate, die den Clients angeboten werden, mit diesem Cop wieder aktivieren?

Ja, es wird ein Rollback-Cop bereitgestellt. Nach der Anwendung können Sie dieses Zertifikat signieren und an die Server hochladen.

Werden alle Zertifikate ECDSA ausgestellt?

Derzeit nicht, aber weitere Sicherheitsaktualisierungen auf der VOS-Plattform in der Zukunft.

Wann installieren Sie UCCX COP?

- Wenn Sie selbstsignierte Zertifikate verwenden und Support-Mitarbeiter keine zusätzlichen Zertifikate akzeptieren möchten
- Wenn kein zusätzliches Zertifikat von CA signiert werden kann

Wann installieren Sie das SM COP?

- Wenn Sie selbstsignierte Zertifikate verwenden und Support-Mitarbeiter keine zusätzlichen Zertifikate akzeptieren möchten
- Wenn kein zusätzliches Zertifikat von CA signiert werden kann
- Wenn Sie eine Zertifizierungsstelle haben, die nur ECDSA-Zertifikate mit RSA signieren kann

Welche Zertifikate werden standardmäßig von verschiedenen Webserverinstanzen angeboten?

Zertifikatkombination/Webserver	Standard-Agent-Erfahrung nach dem Upgrade auf 11,5 (ohne CoP)	UCCX-Tomcat	UCCX OpenFire (Cisco Unified CCX Notification Service)	UCCX-Socketl
Tomcat selbst signiert, selbstsignierte Tomcat-ECDSA	Support-Mitarbeiter werden gebeten, Zertifikate im Live-Daten-Gadget und im Chat-E-Mail-Gadget zu akzeptieren.	Eigene Unterschrift	Eigene Unterschrift	Eigene Unterschr
RSA CA signiert Tomcat, RSA CA, signiert Tomcat-ECDSA	Support-Mitarbeiter können Finesse und Live-Daten verwenden, aber das E-Mail-Chat-Gadget wird nicht geladen, und die SocialMiner-Webseite wird nicht geladen.*	RSA	RSA	RSA
RSA CA unterzeichnet Tomcat,	Support-Mitarbeiter	RSA	RSA	ECDSA

EC CA, signiert Tomcat-ECDSA	können Finesse sowohl mit Live-Daten als auch mit Chat-E-Mail* verwenden.			
RSA CA signiert Tomcat, selbstsigniertes Tomcat-ECDSA	Support-Mitarbeiter werden gebeten, zusätzliche Zertifikate im Live-Daten- und E-Mail-Chat-Gadget zu akzeptieren. Akzeptieren Sie Zertifikat vom Live-Daten-Gadget fehlschlägt, akzeptieren Sie Zertifikat vom E-Mail-Chat-Gadget wäre erfolgreich.*	RSA	RSA	Selbstsignatur (Support-Mitarbei können aufgrund durch den Browse erzwungener Sicherheitsmaßna nicht akzeptieren. Siehe Screenshot oben. Sie müssen das Zertifikat von eine CA signieren lass oder den Cop auf UCCX installieren ECDSA-Zertifikat deaktivieren, die Clients angeboter werden.)

Zugehörige Informationen

- 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=
- Informationen zum UCCX-Zertifikat - http://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/118855-configure-uccx-00.html