Comprenez les Certificats ECDSA dans une solution UCCX

Contenu

Introduction

Ce document décrit comment configurer la solution du Cisco Unified Contact Center Express (UCCX) pour l'usage des Certificats elliptiques de l'algorithme de signature numérique de curve (ECDSA).

Conditions préalables

Exigences

Avant que vous poursuiviez les étapes de configuration qui sont décrites dans ce document, assurez-vous que vous avez accès à la page du système d'exploitation de gestion (de SYSTÈME D'EXPLOITATION) pour ces applications :

- UCCX
- SocialMiner
- Gestionnaire de communications unifiées de Cisco (version CUCM)
- Configuration de certificat de solution UCCX - http://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/118855-configure-uccx-00.html

Un administrateur doit également avoir accès à la mémoire de certificat sur les PC de client d'agent et de superviseur.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

En tant qu'élément de la certification commune des critères (cc), Cisco Unified Communications Manager a ajouté des Certificats ECDSA dans la version 11.0. Ceci affecte tous les Produits du système d'exploitation de Voix (VOS) tels qu'UCCX, SocialMiner, MediaSense, etc. de version 11.5.

Plus de détails au sujet de l'**algorithme elliptique de signature numérique de curve** peuvent être trouvés ici : https://www.maximintegrated.com/en/app-notes/index.mvp/id/5767

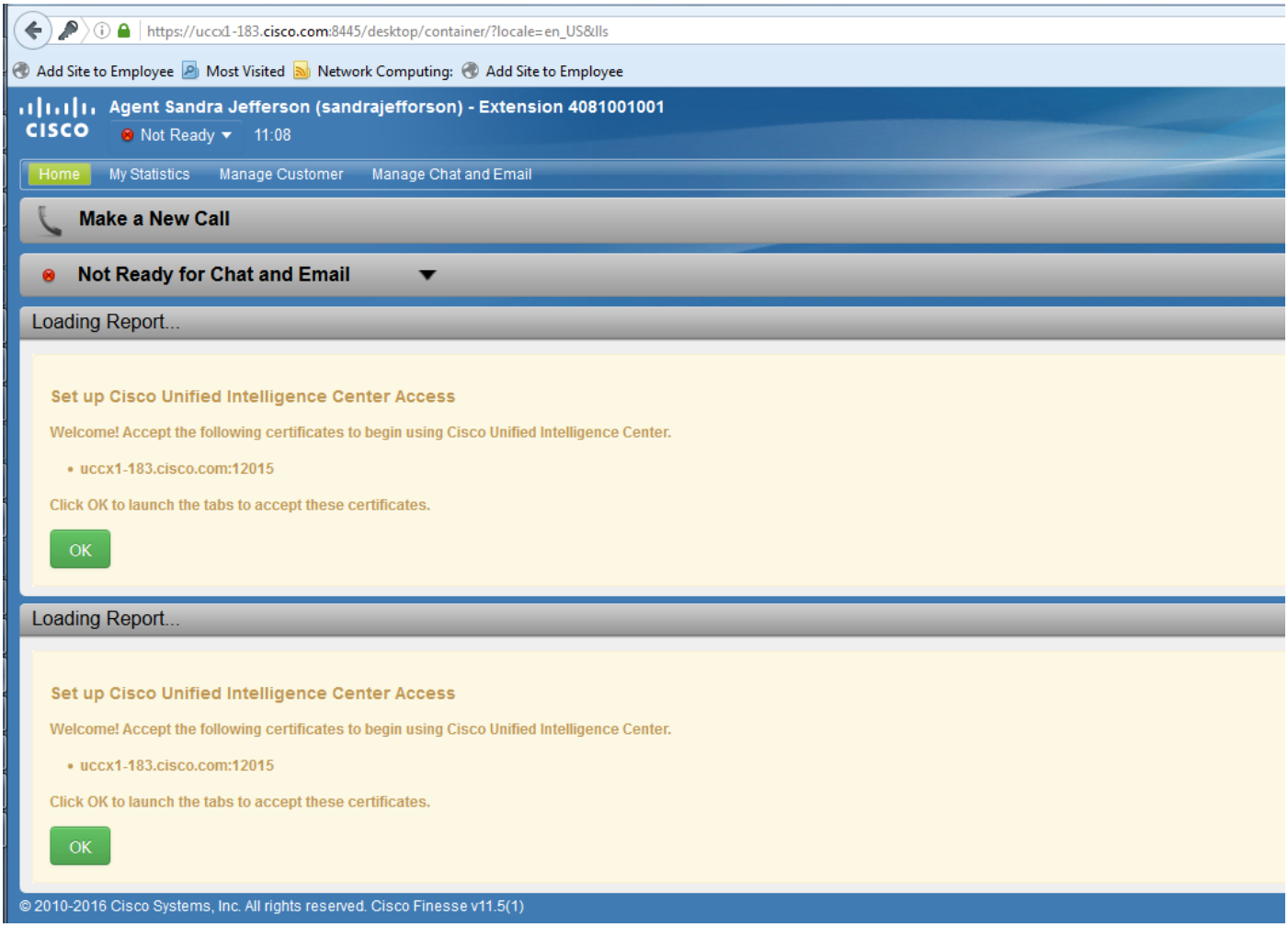
En ce qui concerne la solution UCCX, quand vous améliorez à 11.5, vous êtes offert un certificat supplémentaire qui n'était pas plus tôt actuel. C'est le certificat de Tomcat-ECDSA.

Ceci a été également documenté dans la transmission de pré-version : 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

Expérience d'agent

Après qu'une mise à jour à 11.5, l'agent pourrait être invitée pour recevoir des Certificats sur l'appareil de bureau de finesse basé en fonction si le certificat auto-est signé ou l'Autorité de certification (CA) signé.

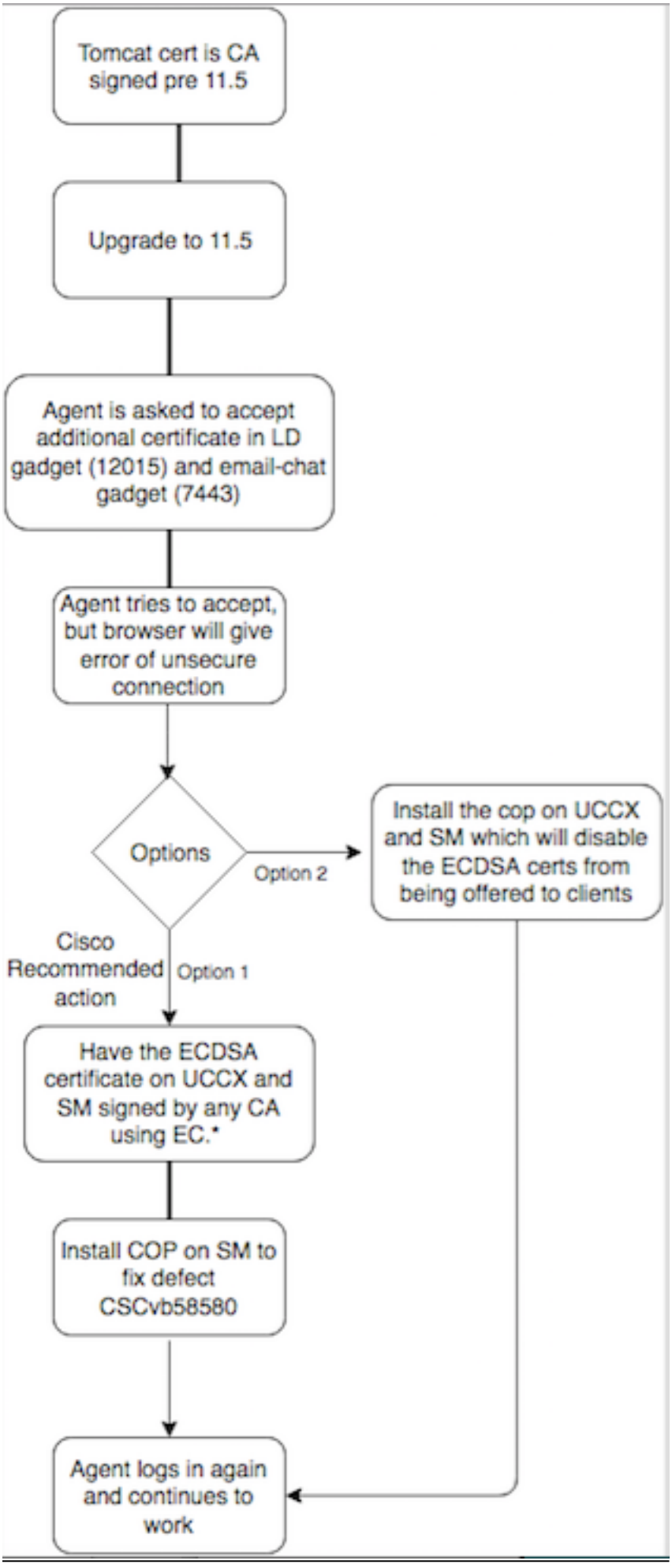
Mise à jour de courrier d'expérience utilisateur à 11.5



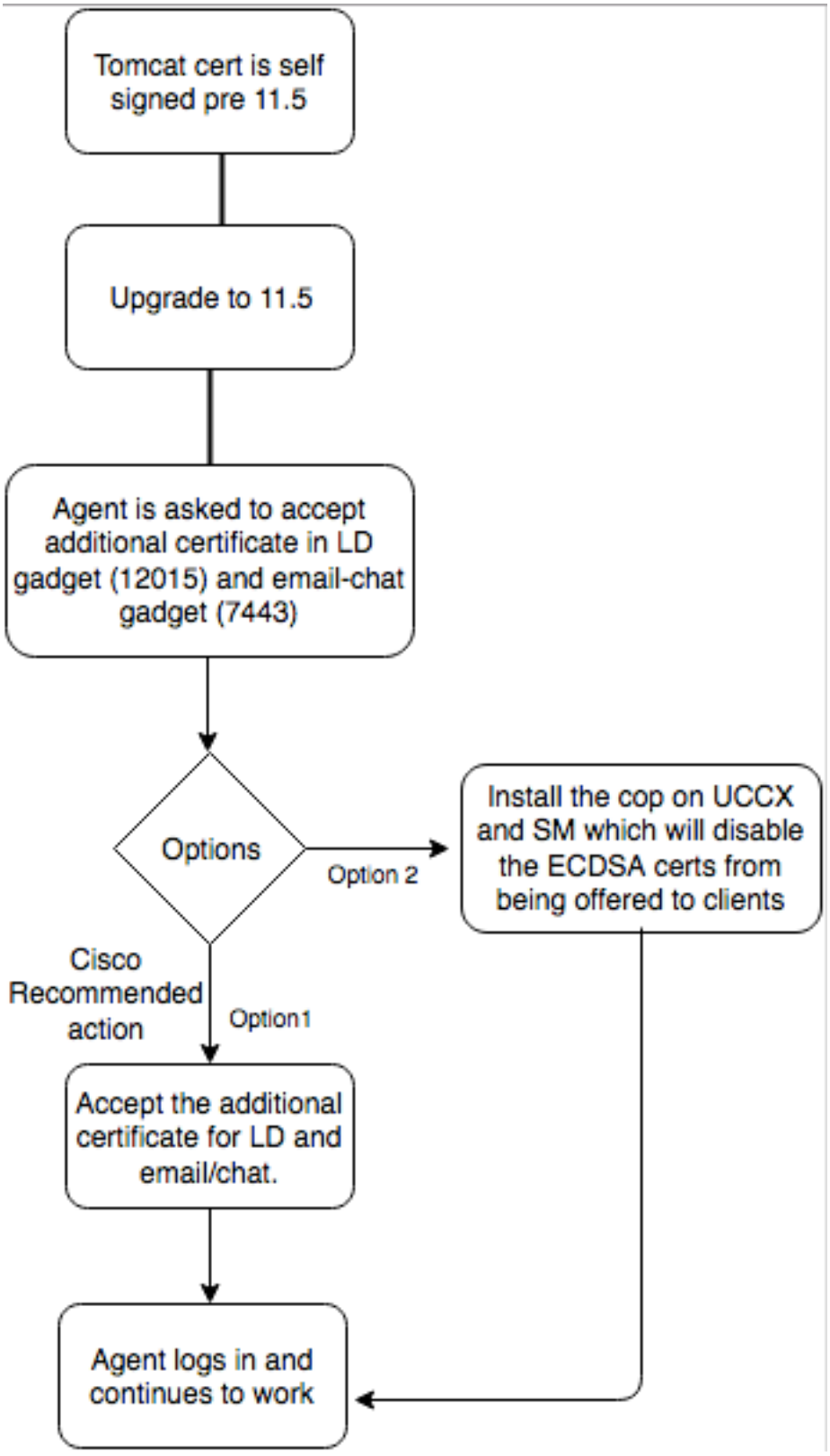
C'est parce que l'appareil de bureau de finesse est maintenant offert un certificat ECDSA qui n'a pas été offert plus tôt.

Procédure

Pré-mise à jour de Certificats signés 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

Pré-mise à jour Auto-signée de Certificats



Configurer

La pratique recommandée recommandée pour ce certificat

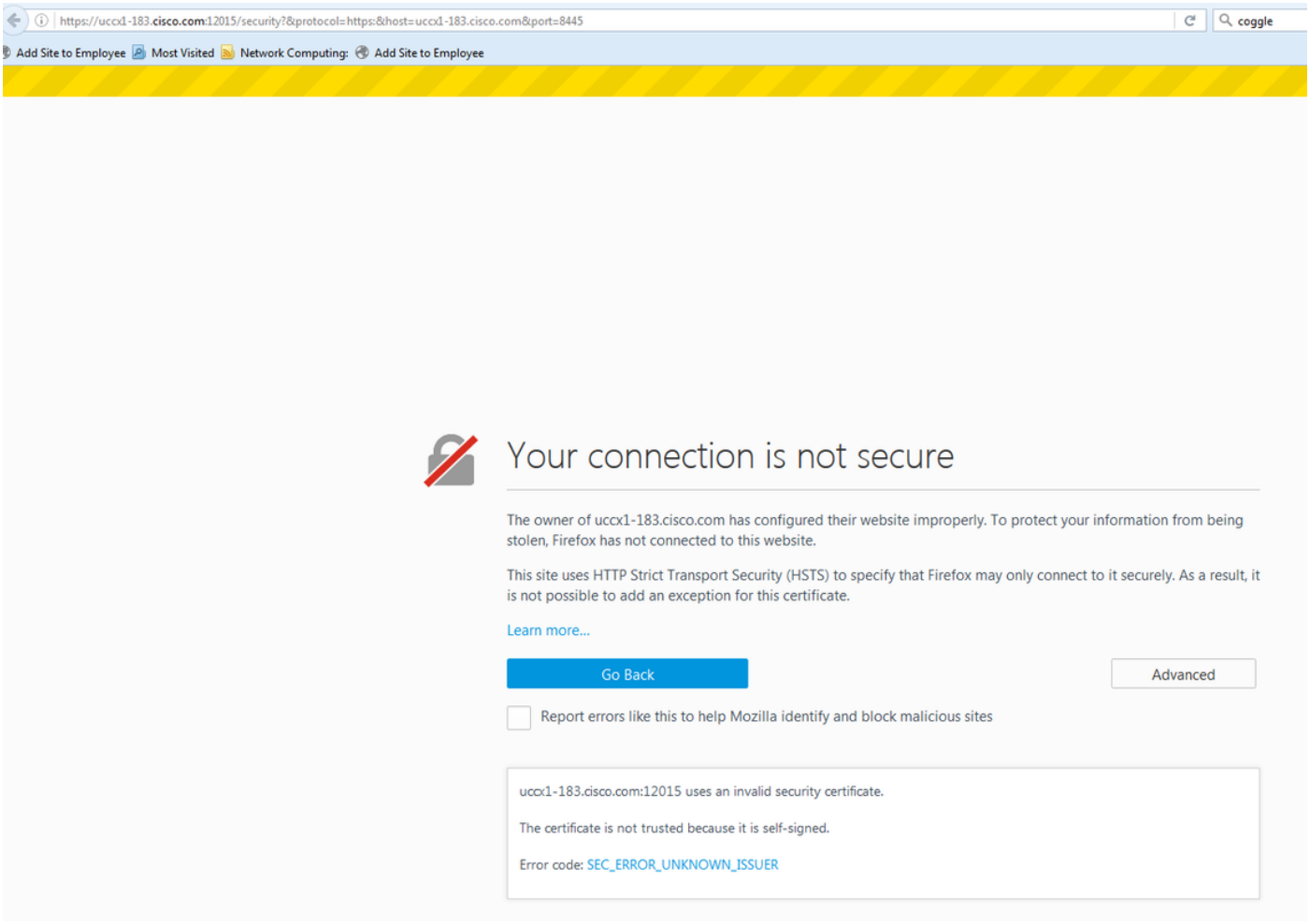
Certificats signés pour UCCX et SocialMiner

Si vous utilisez les Certificats signés CA, ce certificat ECDSA doit être signé par un Autorité de certification (CA) avec d'autres Certificats

> **Note**: Si le CA signe ce certificat ECDSA avec la RSA, ce certifictate ne serait pas présenté au client. Pour la sécurité optimisée, les Certificats ECDSA offerts au client sont la pratique recommandée recommandée.

> **Note**: Si le certificat ECDSA sur SocialMiner est signé par un CA avec la RSA, il entraîne des questions avec l'email et la conversation. Ceci est documenté dans le défaut CSCvb58580 et un fichier de cop est disponible. Ce COP s'assure que des Certificats ECDSA ne sont pas offerts aux clients. Si vous avez un CA qui est capable pour signer des Certificats ECDSA avec la RSA seulement, n'utilisez pas ce certificat. Utilisez le cop de sorte que le certificat ECDSA ne soit pas offert et vous ayez un environnement RSA seulement.

Si vous utilisez les Certificats signés CA et après que la mise à jour vous n'ont pas le certificat ECDSA signé et téléchargé, les agents éprouvent un message pour recevoir le certificat supplémentaire. Quand ils cliquent sur en fonction **CORRECT,** ils sont réorientés au site Web. Cependant, cet échouer en raison de l'application de Sécurité du côté de navigateur puisque le certificat ECDSA est individu signé et vos autres Certificats de Web sont CA signé. Cette transmission est perçue comme risque securiry.



Terminez-vous ces étapes sur chaque noeud d'UCCX Publisher et abonné et SocialMiner, après une mise à jour à UCCX et à SocialMiner sur la version 11.5 :

1. Naviguez vers la page de **gestion de SYSTÈME D'EXPLOITATION** et choisissez la **Gestion**

de Sécurité > de certificat.

2. Le clic **génèrent le CSR**.

3. De la liste déroulante de **liste de certificat**, choisissez **Tomcat-ECDSA** comme le nom et le clic de certificat **génèrent le CSR**.

4. Naviguez vers la **Gestion de Sécurité > de certificat** et choisissez le **CSR de téléchargement**.

5. De la fenêtre externe, choisissez **Tomcat-ECDSA de la** liste déroulante et cliquez sur Download le **CSR**.

Envoyez le nouveau CSR à la tierce partie CA ou signez-le avec un CA interne qui signe des Certificats EC. Ceci produirait ces Certificats signés :

- Certificat racine pour le CA (si vous utilisez le même CA pour des Certificats d'application et des Certificats EC, vous pouvez ignorer cette étape)
- Certificat signé UCCX Publisher ECDSA
- Certificat signé de l'abonné ECDSA UCCX
- Certificat signé de SocialMiner ECDSA

Note: Si vous téléchargez les Certificats de racine et d'intermédiaire sur un éditeur (UCCX), il serait automatiquement répliqué vers l'abonné. Il n'y a aucun besoin de télécharger les Certificats de racine ou d'intermédiaire sur l'autre, des serveurs de non-Publisher dans la configuration si tous les Certificats d'application sont signés par l'intermédiaire de la même chaîne de certificat. Également vous pouvez ignorer ce téléchargement de certificat racine si le même CA signe le certificat EC et vous avez déjà fait ceci quand vous avez configuré les Certificats d'application UCCX.

Terminez-vous ces étapes sur chaque serveur d'applications afin de télécharger le certificat racine et le certificat EC aux Noeuds :

1. Naviguez vers la page de **gestion de SYSTÈME D'EXPLOITATION** et choisissez la **Gestion de Sécurité > de certificat**.

2. Cliquez sur Upload le **certificat**.

3. Téléchargez le certificat racine et choisissez la Tomcat-**confiance** comme le type de certificat.

4. Cliquez sur Upload le **fichier**.

5. Cliquez sur Upload le **certificat**.

6. Téléchargez le certificat d'application et choisissez **Tomcat-ECDSA** comme le type de certificat.

7. Cliquez sur Upload le **fichier**.

Note: Si un subalterne CA signe le certificat, téléchargez le certificat racine du subalterne CA

comme certificat de Tomcat-*confiance* au lieu du certificat racine. Si un certificat intermédiaire est délivré, téléchargez ce certificat à la mémoire de Tomcat-*confiance* en plus du certificat d'application. Également vous pouvez ignorer ce téléchargement de certificat racine si le même CA signe le certificat EC et vous avez déjà fait ceci quand vous avez configuré des Certificats d'application UCCX.

8. Une fois complet, redémarrez ces applications :

   Cisco SocialMinerCisco UCCX Publisher et abonné

Certificats Auto-signés pour UCCX et SocialMiner

Si l'utilisation UCCX ou de SocialMiner auto-signait des Certificats, les agents doivent être informés recevoir l'avertissement de certificat qu'ils sont offerts dans l'instrument de conversation-email et vivent des instruments de données.

Afin d'installer auto-a signé des Certificats sur la machine cliente, utilise un gestionnaire de stratégie de groupe ou de module, ou les installe individuellement dans le navigateur de chaque PC d'agent.

Pour l'Internet Explorer, installez le côté client les Certificats auto-signés dans la mémoire d'**Autorités de certification racine approuvée**.

Pour Mozilla Firefox, terminez-vous ces étapes :

1. Naviguez vers des **outils > des options**.
2. Cliquez sur l'onglet **Advanced**.
3. **Certificats de vue de** clic.
4. Naviguez vers l'onglet de **serveurs**.
5. Cliquez sur Add l'**exception**.

1. **Note**: Vous pouvez également ajouter l'exception de Sécurité pour installer le certificat qui est équivalent au processus ci-dessus. C'est une configuration d'une fois sur le client.

Forums aux questions (Foire aux questions)

Nous avons les Certificats signés CA, et voulons utiliser le certificat ECDSA qui les besoins d'être signé par une EC CA. Tandis que nous attendons le certificat signé CA pour être disponibles, nous devons avoir des données vivantes. Que puis-je faire ?

Nous ne voulons pas signer ce certificat supplémentaire ou faire recevoir des agents ce certificat supplémentaire. Que puis-je faire ?

Bien que la recommandation soit de faire présenter des Certificats ECDSA aux navigateurs, il y

a une option de la désactiver. Vous pouvez installer un fichier de cop sur UCCX et SocialMiner qui s'assure que seulement les Certificats RSA sont présentés au client. Le certificat ECDSA reste toujours dans le keystore, mais ne serait pas offert aux clients.

Si j'emploie ce cop pour désactiver des Certificats ECDSA offerts aux clients, est-ce que je peux l'activer de retour ?

Oui, il y a un cop de repositionnement fourni. Une fois que c'est appliqué, vous pouvez obtenir ce certificat signé et uplaoded aux serveurs.

Est-ce que Certificats seraient tout faits à ECDSA ?

Actuellement pas, mais d'autres mises à jour de sécurité sur la plate-forme VOS à l'avenir.

Quand installez-vous le COP UCCX ?

- Quand vous utilisez les Certificats auto-signés et ne voulez pas que les agents reçoivent les Certificats supplémentaires
- Quand vous ne pouvez pas obtenir le certificat supplémentaire signé par CA

Quand installez-vous le COP SM ?

- Quand vous utilisez les Certificats auto-signés et ne voulez pas que les agents reçoivent les Certificats supplémentaires
- Quand vous ne pouvez pas obtenir le certificat supplémentaire signé par CA
- Quand vous avez un CA qui est capable pour signer des Certificats ECDSA avec la RSA seulement

Quels sont les Certificats qui sont offerts par différents exemples de web server par défaut ?

Combinaison/serveur Web de certificat	Une expérience par défaut d'agent après mise à jour à 11.5 (sans tout cop)	UCCX Tomcat	UCCX Openfire (le service de notification de Cisco Unified CCX)	UCCX SocketIO	SocialMiner Tomc
Tomcat signé par individu, individu a signé Tomcat-ECDSA	Des agents seraient invités à recevoir le certificat dans l'instrument vivant de données et l'instrument de conversation-email	Auto-signé	Auto-signé	Auto-signé	Auto-signé
RSA Tomcat signé par CA, RSA CA a signé Tomcat-ECDSA	Les agents peuvent utiliser la finesse et les données vivantes, mais l'instrument d'email-conversation ne chargera pas et la page Web de SocialMiner ne fait pas load.*	RSA	RSA	RSA	RSA
RSA Tomcat signé par CA, l'EC CA a	Les agents peuvent utiliser la finesse avec des	RSA	RSA	ECDSA	RSA

signé Tomcat-ECDSA	les deux vivent les données et le chat-email*				
RSA Tomcat signé par CA, individu a signé Tomcat-ECDSA	Des agents seraient invités à recevoir le certificat supplémentaire dans l'instrument vivant de données et d'email-conversation. Recevez le certificat de l'instrument vivant de données échoue, reçoit le certificat de l'instrument d'email-conversation serait successful.*	RSA	RSA	Auto-signé (les agents ne peuvent pas recevoir en raison de la mesure de sécurité imposée par navigateur. Référez-vous au tir d'écran ci-dessus. Vous devez obtenir le certificat signé par une EC CA ou installer le cop sur UCCX pour désactiver des Certificats ECDSA offerts aux clients.)	RSA

Informations connexes

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