Entienda los Certificados ECDSA en una solución UCCX

Contenido

Introducción

Este documento describe cómo configurar la solución del Cisco Unified Contact Center Express (UCCX) para el uso de los Certificados elípticos del algoritmo de la firma digital de la curva (ECDSA).

Prerrequisitos

Requisitos

Antes de que usted proceda con los pasos para la configuración que se describen en este documento, asegúrese de que usted tenga acceso a la página de administración del sistema operativo (OS) para estas aplicaciones:

- UCCX
- SocialMiner
- Cisco Unified Communications Manager (CUCM)
- Configuración del certificado de la solución UCCX - http://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/118855-configure-uccx-00.html

Un administrador debe también tener acceso al almacén de certificados en las PC del cliente del agente y del supervisor.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Como parte de la certificación común de los criterios (CC), el encargado de las Comunicaciones unificadas de Cisco agregó los Certificados ECDSA en la versión 11.0. Esto afecta a todos los Productos del sistema operativo de la Voz (VOS) tales como UCCX, SocialMiner, MediaSense, etc de la versión 11.5.

Más detalles sobre el **algoritmo elíptico de la firma digital de la curva** se pueden encontrar aquí: https://www.maximintegrated.com/en/app-notes/index.mvp/id/5767

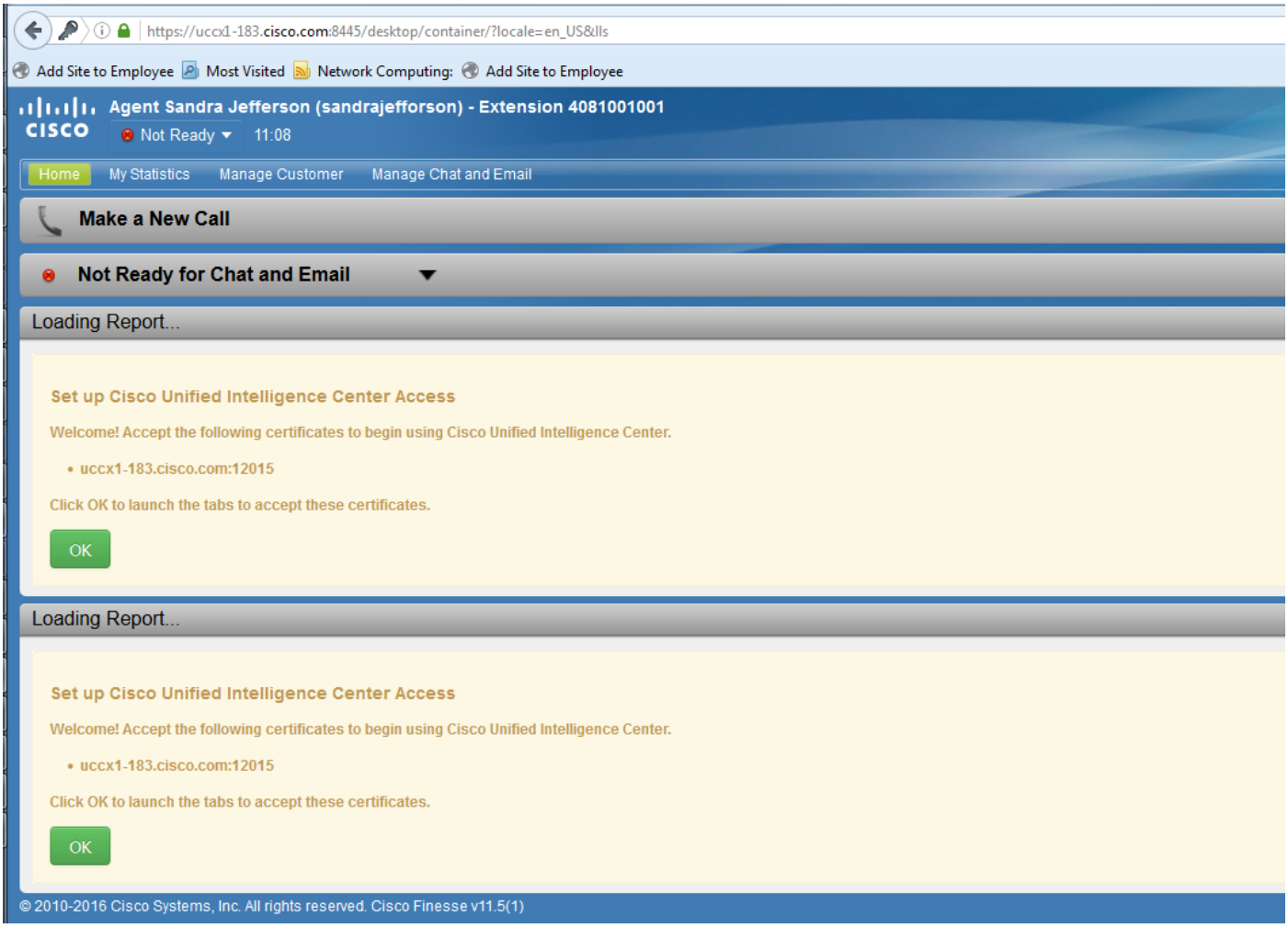
En cuanto a la solución UCCX, cuando usted actualiza a 11.5, le ofrecen un certificado adicional que no era actual anterior. Éste es el certificado de Tomcat-ECDSA.

Esto también se ha documentado en la comunicación de la pre-versión: 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

Experiencia del agente

Después de que una mejora a 11.5, el agente se pudiera pedir para validar los Certificados en el escritorio de la delicadeza basado encendido si el certificado uno mismo-está firmado o el Certificate Authority (CA) firmado.

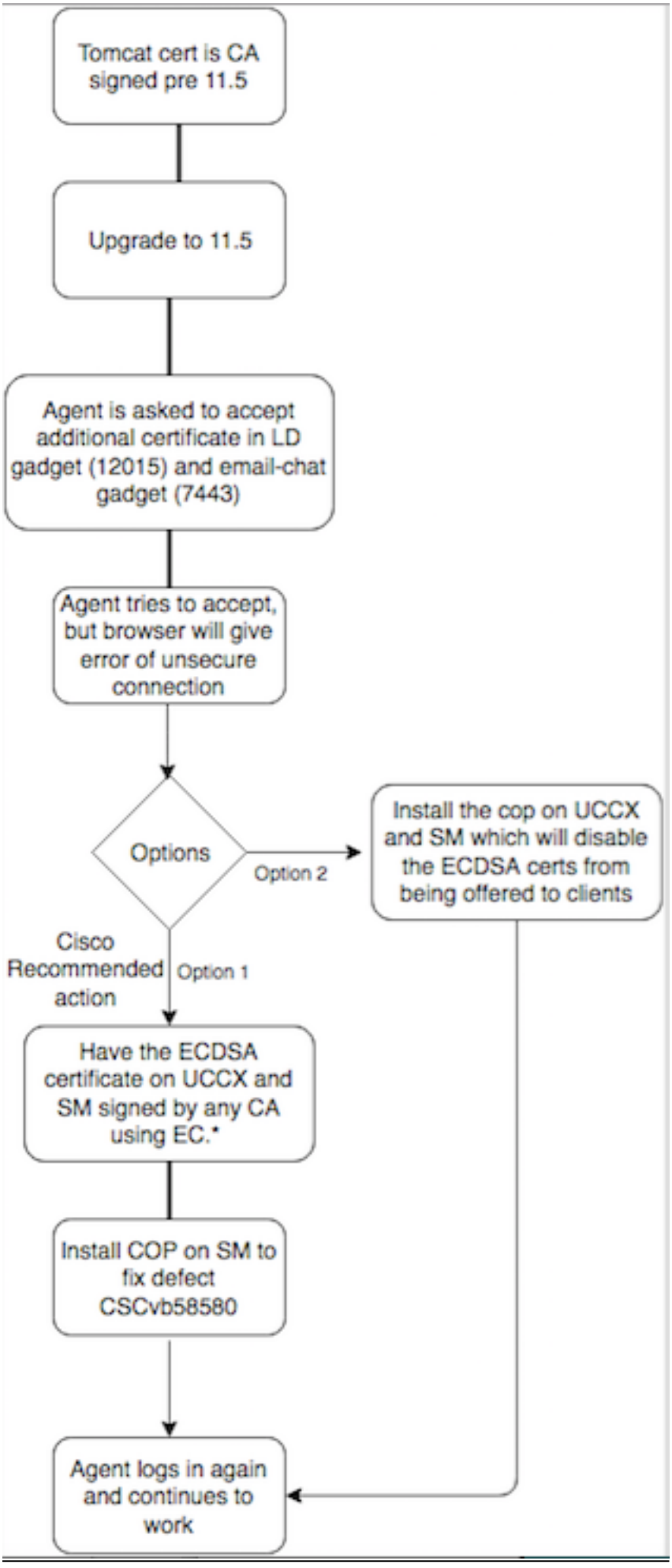
Mejora del poste de la experiencia del usuario a 11.5



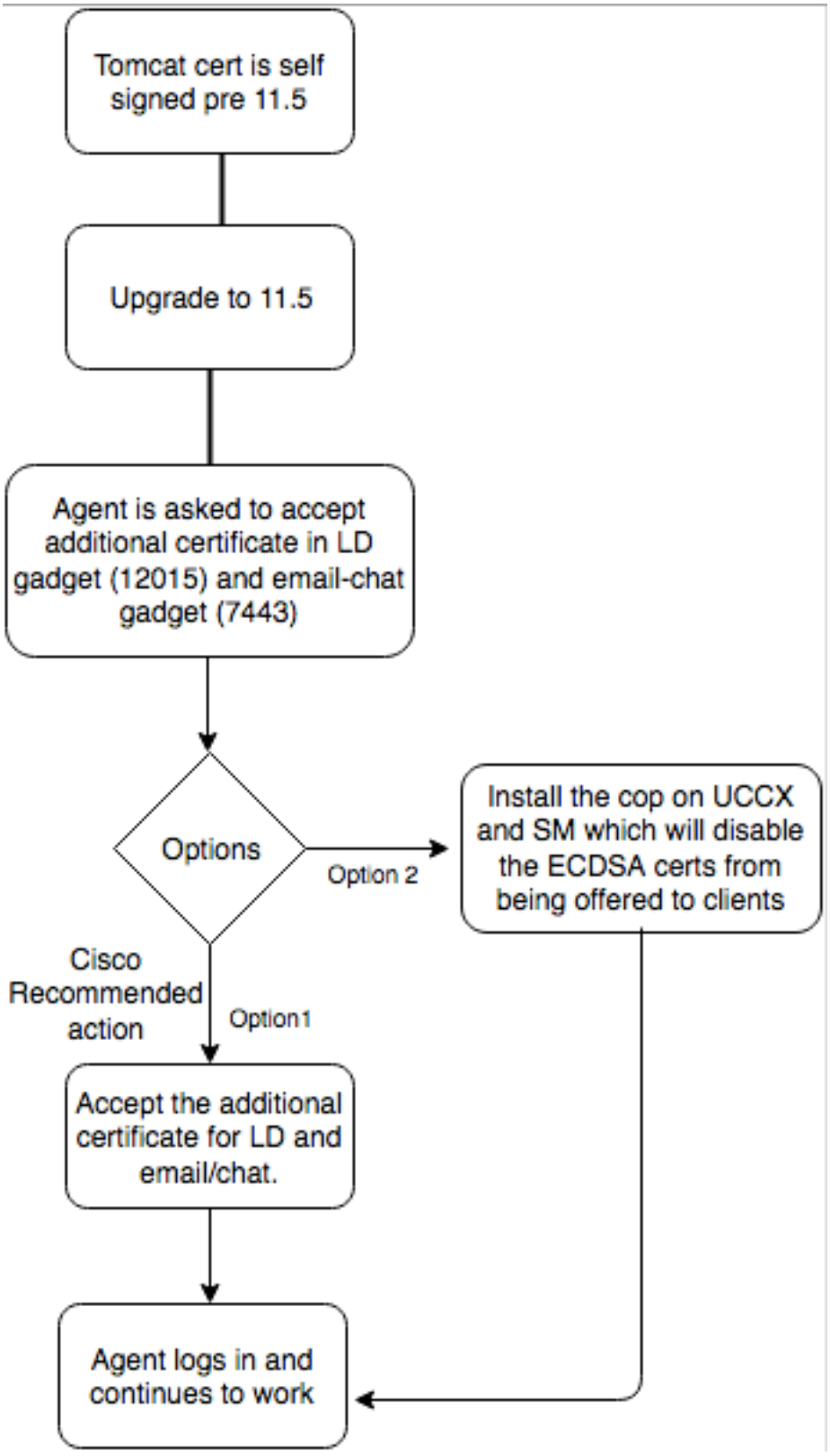
Esto es porque el escritorio de la delicadeza ahora se ofrece un certificado ECDSA que no fue ofrecido anterior.

Procedimiento

Pre-mejora de los certificados firmados 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

Pre-mejora de los certificados autofirmados



Configurar

La mejor práctica recomendada para este certificado

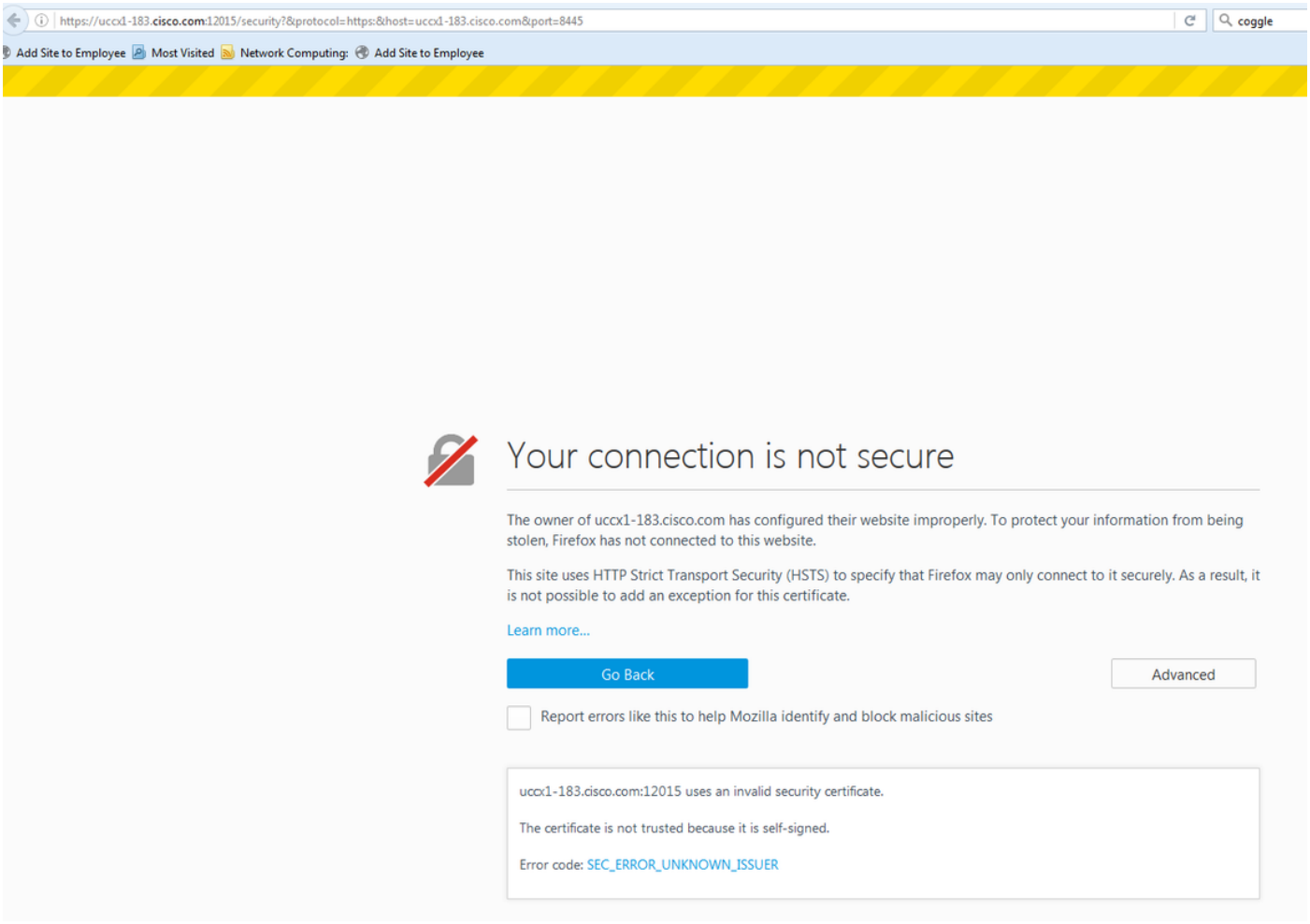
Certificados firmados para UCCX y SocialMiner

Si usted utiliza los certificados firmados CA, este certificado ECDSA se debe firmar por un Certificate Authority (CA) junto con otros Certificados

> **Note**: Si el CA firma este certificado ECDSA con el RSA, este certifictate no sería presentado al cliente. Para la seguridad mejorada, los Certificados ECDSA ofrecidos al cliente son la mejor práctica recomendada.

> **Note**: Si el certificado ECDSA en SocialMiner es firmado por un CA con el RSA, causa los problemas con el correo electrónico y la charla. Esto se documenta en el defecto CSCvb58580 y un fichero del poli está disponible. Este POLI se asegura de que los Certificados ECDSA no estén ofrecidos a los clientes. Si usted tiene un CA que sea capaz firmar los Certificados ECDSA con el RSA solamente, no utilice este certificado. Utilice el poli para no ofrecer el certificado ECDSA y usted tenga un entorno RSA solamente.

Si usted utiliza los certificados firmados CA y después de que la mejora usted no tiene el certificado ECDSA firmado y cargado por teletratamiento, los agentes experimentan un mensaje para validar el certificado adicional. Cuando hacen clic en la **AUTORIZACIÓN,** los reorientan al sitio web. Sin embargo, este fall debido a la aplicación de Seguridad del lado del navegador puesto que el certificado ECDSA es uno mismo firmado y sus otros Certificados de la red son CA firmado. Esta comunicación se percibe como riesgo securiry.



Complete estos pasos en cada nodo del editor y suscriptor y de SocialMiner UCCX, después de una mejora a UCCX y a SocialMiner en la versión 11.5:

1. Navegue a la **página de administración OS** y elija el **Certificate Management (Administración**

de certificados) de la Seguridad.

2. El tecleo genera el CSR.

3. De la lista desplegable de la lista del certificado, elija Tomcat-ECDSA como el nombre del certificado y el tecleo genera el CSR.

4. Navegue al Certificate Management (Administración de certificados) de la Seguridad y elija el CSR de la transferencia directa.

5. De la ventana emergente, elija Tomcat-ECDSA de la lista desplegable y haga clic el CSR de la transferencia directa.

Envíe el nuevo CSR al CA de tercera persona o fírmelo con un CA interno que firme los Certificados EC. Esto presentaría estos certificados firmados:

- Certificado raíz para el CA (si usted utiliza el mismo CA para los Certificados de la aplicación y los Certificados EC, usted puede saltar este paso)
- Certificado firmado del editor ECDSA UCCX
- Certificado firmado del suscriptor ECDSA UCCX
- Certificado firmado de SocialMiner ECDSA

Note: Si usted carga por teletratamiento los Certificados de la raíz y del intermedio en un editor (UCCX), sería replicada automáticamente al suscriptor. No hay necesidad de cargar por teletratamiento los Certificados de la raíz o del intermedio sobre el otro, los servidores del no-editor en la configuración si todos los Certificados de la aplicación se firman vía la misma Cadena de certificados. También usted puede saltar esta carga por teletratamiento del certificado raíz si el mismo CA firma el certificado EC y usted ha hecho ya esto cuando usted configuró los Certificados de la aplicación UCCX.

Complete estos pasos en cada servidor de aplicaciones para cargar por teletratamiento el certificado raíz y el certificado EC a los Nodos:

1. Navegue a la página de administración OS y elija el Certificate Management (Administración de certificados) de la Seguridad.

2. Haga clic el certificado de la carga por teletratamiento.

3. Cargue por teletratamiento el certificado raíz y elija la Tomcat-confianza como el tipo de certificado.

4. Haga clic el fichero de la carga por teletratamiento.

5. Haga clic el certificado de la carga por teletratamiento.

6. Cargue por teletratamiento el certificado de la aplicación y elija Tomcat-ECDSA como el tipo de certificado.

7. Haga clic el fichero de la carga por teletratamiento.

Note: Si un subordinado CA firma el certificado, cargue por teletratamiento el certificado raíz del subordinado CA como el certificado de la Tomcat-*confianza* en vez del certificado raíz. Si se publica un certificado intermedio, cargue por teletratamiento este certificado al almacén de la Tomcat-*confianza* además del certificado de la aplicación. También usted puede saltar esta carga por teletratamiento del certificado raíz si el mismo CA firma el certificado EC y usted ha hecho ya esto cuando usted configuró los Certificados de la aplicación UCCX.

8. Una vez completo, recomience estas aplicaciones:

   Cisco SocialMinerEditor y suscriptor de Cisco UCCX

Certificados autofirmados para UCCX y SocialMiner

Si los certificados autofirmados del uso UCCX o de SocialMiner, los agentes necesitan ser aconsejados para validar la advertencia del certificado se ofrecen en el gadget del charla-correo electrónico y viven los gadgets de los datos.

Para instalar los certificados autofirmados en la máquina del cliente, utilice a un encargado de la directiva o del paquete del grupo, o instalelos individualmente en el navegador de cada PC del agente.

Para el Internet Explorer, instale los certificados autofirmados del cliente-lado en el almacén de los **Trusted Root Certification Authority**.

Para Mozilla Firefox, complete estos pasos:

1. Navegue a las **herramientas > a las opciones**.
2. Haga clic en la ficha Advanced (Opciones avanzadas).
3. Haga clic los **Certificados de la visión**.
4. Navegue a los **servidores** cuadro.
5. El tecleo **agrega la excepción**.

1. **Note**: Usted puede también agregar la excepción de seguridad para instalar el certificado que es equivalente al proceso antedicho. Esto es una configuración de una vez en el cliente.

Preguntas con frecuencia hechas (FAQ)

Tenemos certificados firmados CA, y queremos utilizar el certificado ECDSA que las necesidades de ser firmado por una EC CA. Mientras que esperamos el certificado firmado CA para estar disponibles, necesitamos tener datos vivos para arriba. ¿Qué puedo hacer?

No queremos firmar este certificado adicional o hacer que los agentes validen este certificado adicional. ¿Qué puedo hacer?

Aunque la recomendación sea hacer los Certificados ECDSA presentar a los navegadores, hay una opción para inhabilitarlo. Usted puede instalar un fichero del poli en UCCX y SocialMiner que se asegure de que solamente los Certificados RSA estén presentados al cliente. El certificado ECDSA todavía permanece en el keystore, pero no sería ofrecido a los clientes.

¿Si utilizo este poli para inhabilitar los Certificados ECDSA ofrecidos a los clientes, puedo activarlo detrás?

Sí, hay poli de la restauración no actualizada proporcionado. Una vez que eso es aplicado, usted puede conseguir este certificado firmado y uplaoded a los servidores.

¿Todos los Certificados serían hechos ECDSA?

Actualmente no, solamente otras actualizaciones de seguridad en la plataforma VOS en el futuro.

¿Cuándo usted instala el POLI UCCX?

- Cuando usted utiliza los certificados autofirmados y no quisiera que los agentes validaran los Certificados adicionales
- Cuando usted no puede conseguir el certificado adicional firmado por el CA

¿Cuándo usted instala el POLI SM?

- Cuando usted utiliza los certificados autofirmados y no quisiera que los agentes validaran los Certificados adicionales
- Cuando usted no puede conseguir el certificado adicional firmado por el CA
- Cuando usted tiene un CA que sea capaz firmar los Certificados ECDSA con el RSA solamente

¿Cuáles son los Certificados que son ofrecidos por diversos casos del servidor Web por abandono?

Combinación/servidor Web del certificado	Experiencia del agente del valor por defecto después de la mejora a 11.5 (sin cualquier poli)	UCCX Tomcat	UCCX Openfire (Cisco unificó el servicio de notificación CCX)	UCCX SocketIO	SocialMine
Tomcat firmado uno mismo, uno mismo firmó Tomcat-ECDSA	Los agentes serían pedidos validar el certificado en el gadget vivo de los datos y el gadget del charla-correo electrónico	Uno mismo-firmado	Uno mismo-firmado	Uno mismo-firmado	Uno mismo
El RSA Tomcat firmado CA, RSA CA firmó Tomcat-ECDSA	Los agentes pueden utilizar la delicadeza y los datos vivos, pero el gadget de la correo electrónico-charla no cargará y la página web de SocialMiner no hace load.*	RSA	RSA	RSA	RSA
El RSA Tomcat firmado CA, EC CA	Los agentes pueden utilizar la delicadeza	RSA	RSA	ECDSA	RSA

firmó Tomcat-ECDSA	con ambos viven los datos y chat-email*				
El RSA Tomcat firmado CA, uno mismo firmó Tomcat-ECDSA	Los agentes serían pedidos validar el certificado adicional en el gadget vivo de los datos y de la correo electrónico-charla. Valide el certificado del gadget vivo de los datos falla, valida el certificado del gadget de la correo electrónico-charla sería successful.*	RSA	RSA	Uno mismo-firmado (los agentes no pueden validar debido a la medida de Seguridad aplicada navegador. Refiera al tiro de pantalla arriba. Usted debe conseguir el certificado firmado por una EC CA o instalar el poli en UCCX para inhabilitar los Certificados ECDSA ofrecidos a los clientes.)	RSA

Información Relacionada

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