Guía de administración de certificados de la solución UCCX

Contenido

Introducción

Este documento describe cómo configurar Cisco Unified Contact Center Express (UCCX) para el uso de certificados autofirmados y firmados.

Prerequisites

Requirements

Antes de continuar con los pasos de configuración descritos en este documento, asegúrese de que tiene acceso a la página de administración del sistema operativo (SO) para estas aplicaciones:

- UCCX
- SocialMiner
- MediaSense

Un administrador también debe tener acceso al almacén de certificados en los equipos cliente agente y supervisor.

FQDN, DNS y dominios

Es obligatorio que todos los servidores de la configuración UCCX se instalen con servidores DNS (Sistema de nombres de dominio) y nombres de dominio. También es necesario que los agentes, supervisores y administradores accedan a las aplicaciones de configuración UCCX mediante el nombre de dominio completo (FQDN).

UCCX versión 10.0+ requiere que el nombre de dominio y los servidores DNS se rellenen durante la instalación. Los certificados generados por el instalador de UCCX versión 10.0+ contienen el FQDN, según corresponda. Agregue los servidores DNS y un dominio al clúster UCCX antes de actualizar a UCCX versión 10.0+.

Si el dominio cambia o se rellena por primera vez, los certificados deben regenerarse. Después de agregar el nombre de dominio a la configuración del servidor, regenere todos los certificados Tomcat antes de instalarlos en las otras aplicaciones, en los exploradores del cliente o tras generar la solicitud de firma de certificado (CSR) para la firma.

Componentes Utilizados

La información descrita en este documento se basa en estos componentes de hardware y software:

- Servicios web UCCX
- Servicio de notificación UCCX
- Plataforma UCCX Tomcat
- Cisco Finesse Tomcat
- Tomcat de Cisco Unified Intelligence Center (CUIC)
- Tomcat de SocialMiner
- Servicios web MediaSense

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

Con la introducción de Finesse y CUIC, la integración entre UCCX y SocialMiner para el correo electrónico y el chat, y el uso de MediaSense para registrar, comprender e instalar certificados a través de Finesse, la capacidad de solucionar problemas de certificados es ahora de vital importancia.

Este documento describe el uso de certificados autofirmados y firmados en el entorno de configuración UCCX que cubre:

- Servicios de notificación UCCX
- Servicios web UCCX
- Scripts UCCX
- Coresidente Finesse
- CUIC co-residente (datos en directo e informes históricos)
- MediaSense (grabación y etiquetado basados en Finesse)
- SocialMiner (chat)

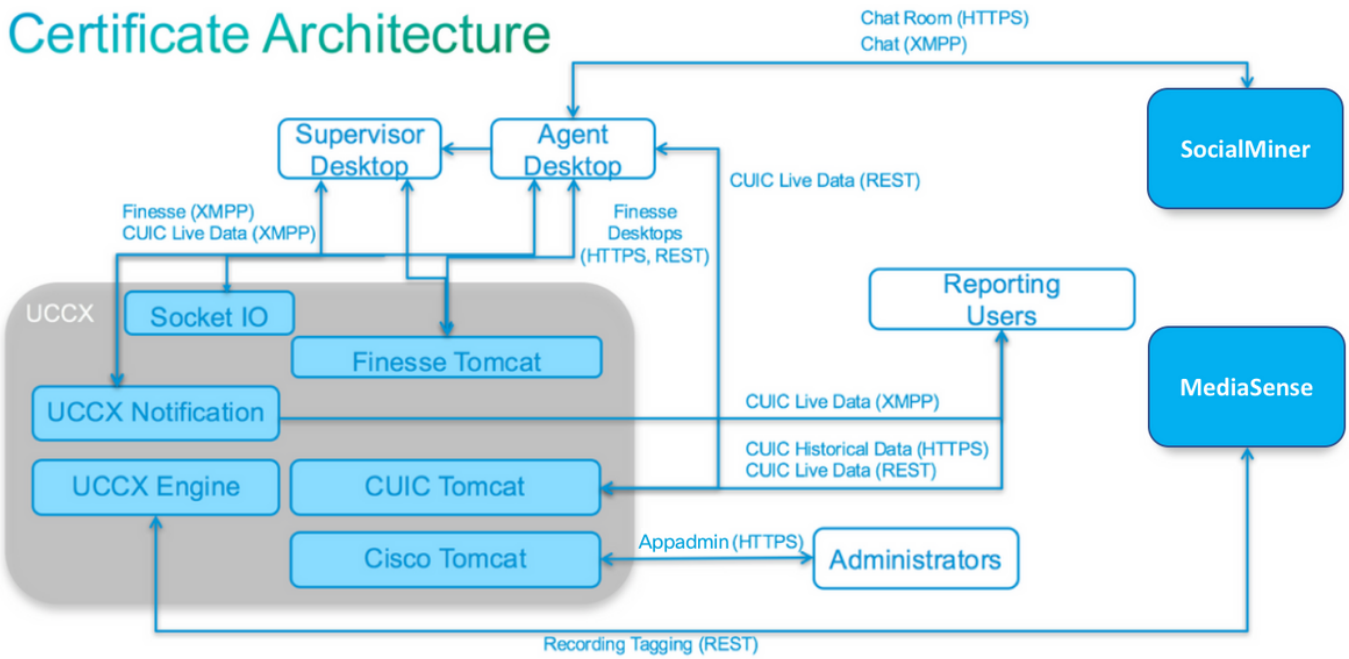
Los certificados, firmados o autofirmados, deben instalarse tanto en las aplicaciones (servidores) de la configuración UCCX como en los escritorios de los clientes agente y supervisor.

En Unified Communications Operating System (UCOS) 10.5, se agregaron certificados de varios servidores para que se pudiera generar un único CSR para un clúster en lugar de tener que firmar un certificado individual para cada nodo del clúster. Este tipo de certificado no es compatible con UCCX, MediaSense y SocialMiner.

Configurar

En esta sección se describe cómo configurar UCCX para el uso de certificados autofirmados y firmados.

Diagrama de configuración



Arquitectura de la solución UCCX válida a partir de UCCX 1.0. Diagrama de comunicación HTTPS.

Certificados firmados

El método recomendado de administración de certificados para la configuración UCCX es aprovechar los certificados firmados. Estos certificados pueden estar firmados por una autoridad de certificación (CA) interna o por una CA de terceros conocida.

En los exploradores principales, como Mozilla Firefox e Internet Explorer, los certificados raíz para entidades emisoras de certificados de terceros conocidas se instalan de forma predeterminada. Los certificados de las aplicaciones de configuración UCCX firmados por estas CA son de confianza de forma predeterminada, ya que su cadena de certificados termina en un certificado raíz que ya está instalado en el explorador.

El certificado raíz de una CA interna también se puede preinstalar en el explorador cliente mediante una directiva de grupo u otra configuración actual.

Puede elegir si desea que los certificados de la aplicación de configuración UCCX estén firmados por una CA de terceros conocida o por una CA interna en función de la disponibilidad y la preinstalación del certificado raíz de las CA en el explorador cliente.

Instalar certificados de aplicación Tomcat firmados

Complete estos pasos para cada nodo de las aplicaciones de administración de editor y suscriptor de UCCX, SocialMiner y editor y suscriptor de MediaSense:

1. Navegue hasta la página **Administración del SO** y elija **Seguridad > Administración de certificados**.
2. Haga clic en **Generar CSR**.
3. En la lista desplegable **Lista de certificados**, elija **tomcat** como nombre del certificado y haga clic en **Generar CSR**.
4. Navegue hasta **Seguridad > Administración de certificados** y elija **Descargar CSR**.

5. En la ventana emergente, elija **tomcat** en la lista desplegable y haga clic en **Descargar CSR**.

Envíe la nueva CSR a la CA de terceros o fírmela con una CA interna, como se ha descrito anteriormente. Este proceso debe producir estos certificados firmados:

- Certificado raíz para la CA
- Certificado de aplicación de editor UCCX
- Certificado de aplicación de suscriptor UCCX
- Certificado de aplicación de SocialMiner
- Certificado de aplicación de editor MediaSense
- Certificado de aplicación de suscriptor MediaSense

Nota: Deje el campo **Distribution** en CSR como FQDN del servidor.

Nota: El certificado "Multi-server (SAN)" es compatible con UCCX a partir de la versión 11.6. Sin embargo, la SAN sólo debe incluir el nodo 1 y el nodo 2 de UCCX. Otros servidores, como SocialMiner, no deben incluirse en la SAN de UCCX.

Nota: UCCX sólo admite longitudes de clave de certificado de 1024 y 2048 bits.

Complete estos pasos en cada servidor de aplicaciones para cargar el certificado raíz y el certificado de aplicación en los nodos:

Nota: Si carga los certificados raíz e intermedios en un editor (UCCX o MediaSense), se debe replicar automáticamente en el suscriptor. No es necesario cargar los certificados raíz o intermedios en los otros servidores que no son editores de la configuración si todos los certificados de aplicación están firmados a través de la misma cadena de certificados.

1. Navegue hasta la página **Administración del SO** y elija **Seguridad > Administración de certificados**.
2. Haga clic en **Cargar certificado**.
3. Cargue el certificado raíz y elija **tomcat-trust** como tipo de certificado.
4. Haga clic en **Cargar archivo**.
5. Haga clic en **Cargar certificado**.
6. Cargue el certificado de aplicación y elija **tomcat** como tipo de certificado.
7. Haga clic en **Cargar archivo**. **Nota:** Si una CA subordinada firma el certificado, cargue el certificado raíz de la CA subordinada como el certificado *tomcat-trust* en lugar del certificado raíz. Si se emite un certificado intermedio, cargue este certificado en el almacén *tomcat-trust* además del certificado de aplicación.
8. Una vez completadas, reinicie estas aplicaciones: Publicador y suscriptor de Cisco MediaSenseCisco SocialMinerEditor y suscriptor de Cisco UCCX

Nota: Cuando utiliza UCCX, MediaSense y SocialMiner 11.5 y versiones posteriores, hay un nuevo certificado llamado tomcat-ECDSA. Al cargar un certificado firmado de tomcat-ECDSA en el servidor, cargue el certificado de aplicación como un certificado de tomcat-ECDSA, no como un certificado de tomcat. Para obtener más información sobre ECDSA, consulte la Sección Información Relacionada para obtener el enlace para comprender y configurar los certificados ECDSA.

Certificados con firma automática

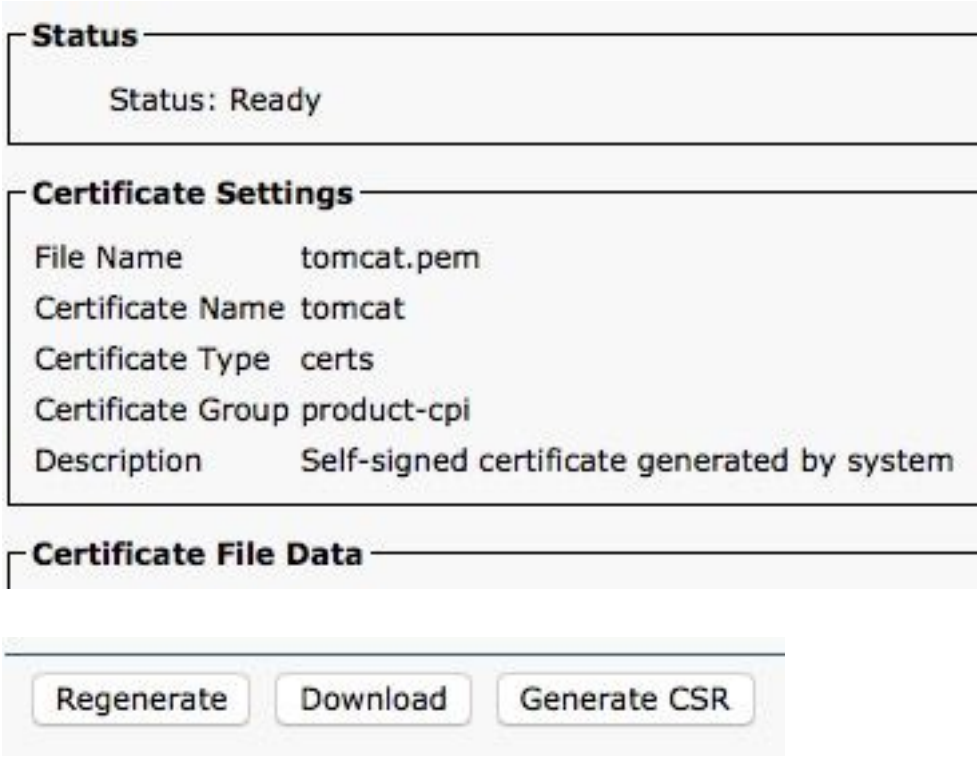
Instalación En Servidores Periféricos

Todos los certificados que se utilizan en la configuración UCCX vienen preinstalados en las aplicaciones de configuración y se firman automáticamente. Estos certificados autofirmados no son de confianza implícita cuando se presentan a un explorador cliente u otra aplicación de configuración. Aunque se recomienda firmar todos los certificados de la configuración UCCX, puede utilizar los certificados autofirmados preinstalados.

Para cada relación de aplicación, debe descargar el certificado correspondiente y cargarlo en la aplicación. Complete estos pasos para obtener y cargar los certificados:

1. Acceda a la página **Administración del SO de la** aplicación y seleccione **Seguridad > Gestión de Certificados**.

2. Haga clic en el archivo **.pem del** certificado correspondiente y seleccione **Descargar**:



3. Para cargar un certificado en la aplicación apropiada, navegue hasta la página **Administración del SO** y elija **Seguridad > Administración de certificados**.
4. Haga clic en **Cargar certificado / Cadena de certificado:**

5. Una vez completados, reinicie estos servidores:

   Publicador y suscriptor de Cisco MediaSenseCisco SocialMinerEditor y suscriptor de Cisco UCCX

Para instalar certificados autofirmados en el equipo cliente, utilice una directiva de grupo o un

administrador de paquetes, o instálelos individualmente en el explorador de cada equipo agente.

Para Internet Explorer, instale los certificados autofirmados del lado del cliente en el almacén **Entidades de certificación raíz de confianza**.

Para Mozilla Firefox, siga estos pasos:

1. Vaya a **Herramientas > Opciones**.
2. Haga clic en la ficha Advanced (Opciones avanzadas).
3. Haga clic en **Ver certificados**.
4. Vaya a la pestaña **Servidores**.
5. Haga clic en **Agregar excepción**.

Regeneración de certificados autofirmados

En caso de que caduquen los certificados autofirmados, deberán regenerarse y los pasos de configuración de **Instalación en servidores periféricos** deberán realizarse nuevamente.

1. Acceder a la aplicación **Administración del SO** y seleccione **Security > Certificate Management**.
2. Haga clic en el certificado correspondiente y seleccione **Regenerar**.
3. Se debe reiniciar el servidor cuyo certificado se regeneró.
4. Para cada relación de aplicación, debe descargar el certificado correspondiente y cargarlo en la aplicación siguiendo los pasos de configuración de **Instalación en servidores periféricos.**

Integración y configuración del cliente

UCCX-to-MediaSense

UCCX utiliza la interfaz de programación de aplicaciones (API) REST de servicios web MediaSense con dos fines:

- Para suscribirse a notificaciones de nuevas grabaciones que se invocan en Cisco Unified Communications Manager (CUCM).
- Para etiquetar las grabaciones de los agentes UCCX con la información del agente y de la cola de servicio de contacto (CSQ).

UCCX utiliza la API REST en los nodos de administración de MediaSense. Hay un máximo de dos en cualquier clúster MediaSense. UCCX no se conecta a través de la API REST a los nodos de expansión MediaSense. Ambos nodos UCCX deben consumir la API REST de MediaSense, por lo que debe instalar los dos certificados Tomcat de MediaSense en ambos nodos UCCX.

Cargue la cadena de certificados firmados o autofirmados de los servidores MediaSense en el almacén de claves UCCX *tomcat-trust*.

MediaSense-to-Finesse

MediaSense utiliza la API REST de los servicios web de Finesse para autenticar los agentes del gadget Búsqueda y reproducción de MediaSense en Finesse.

El servidor MediaSense configurado en el diseño XML de Finesse para el gadget Buscar y ejecutar debe consumir la API REST de Finesse, por lo que debe instalar los dos certificados Tomcat de UCCX en ese nodo MediaSense.

Cargue la cadena de certificados firmados o autofirmados de los servidores UCCX en el almacén de claves MediaSense *tomcat-trust*.

UCCX-to-SocialMiner

UCCX utiliza las API REST y Notification de SocialMiner para administrar los contactos de correo electrónico y la configuración. Ambos nodos UCCX deben consumir la API REST de SocialMiner y recibir una notificación del servicio de notificación de SocialMiner, por lo que debe instalar el certificado Tomcat de SocialMiner en ambos nodos UCCX.

Cargue la cadena de certificados firmados o autofirmados del servidor de SocialMiner en el almacén de claves UCCX *tomcat-trust*.

Certificado de cliente de UCCX AppAdmin

El certificado de cliente de UCCX AppAdmin se utiliza para la administración del sistema UCCX. Para instalar el certificado de UCCX AppAdmin para administradores UCCX, en el equipo cliente, navegue hasta **https://<UCCX FQDN>/appadmin/main** para cada uno de los nodos UCCX e instale el certificado a través del navegador.

Certificado de cliente de plataforma UCCX

Los servicios web de UCCX se utilizan para la entrega de contactos de chat a los navegadores cliente. Para instalar el certificado de plataforma UCCX para agentes y supervisores UCCX, en el equipo cliente, navegue hasta **https://<UCCX FQDN>/appadmin/main** para cada uno de los nodos UCCX e instale el certificado a través del navegador.

Certificado de cliente de servicio de notificación

Finesse, UCCX y CUIC utilizan el servicio de notificación de CCX para enviar información en tiempo real al escritorio del cliente a través del protocolo extensible de mensajería y presencia (XMPP). Se utiliza para la comunicación Finesse en tiempo real, así como para datos en directo de CUIC.

Para instalar el certificado de cliente del servicio de notificación en el equipo de los agentes y supervisores o de los usuarios de informes que utilizan datos en directo, vaya a **https://<UCCX FQDN>:7443/** para cada uno de los nodos UCCX e instale el certificado a través del explorador.

Certificado de cliente Finesse

Los escritorios Finesse utilizan el certificado de cliente Finesse para conectarse a la instancia de Tomcat Finesse con el fin de la comunicación API REST entre el escritorio y el servidor Finesse co-residente.

Para instalar el certificado Finesse para agentes y supervisores, en el equipo cliente, navegue hasta **https://<UCCX FQDN>:8445/** para cada uno de los nodos UCCX e instale el certificado a

través de las indicaciones del navegador.

Para instalar el certificado Finesse para los administradores de Finesse, en el equipo cliente, navegue hasta **https://<UCCX FQDN>:8445/cfadmin** para cada uno de los nodos UCCX e instale el certificado a través de las indicaciones del navegador.

Certificado de cliente de SocialMiner

El certificado Tomcat de SocialMiner debe estar instalado en el equipo cliente. Una vez que un agente acepta una solicitud de chat, el gadget Chat se redirige a una URL que representa la sala de chat. Esta sala de chat se aloja en el servidor de SocialMiner y contiene el cliente o contacto de chat.

Para instalar el certificado de SocialMiner en el explorador, en el equipo cliente, vaya a **https://<FQDN de SocialMiner>/** e instale el certificado a través de las indicaciones del explorador.

Certificado de cliente CUIC

El certificado Tomcat de CUIC debe instalarse en el equipo cliente para los agentes, supervisores y usuarios de informes que utilizan la interfaz web de CUIC para informes históricos o informes de datos en directo, ya sea en la página web de CUIC o en los gadgets del escritorio.

Para instalar el certificado Tomcat de CUIC en el explorador, en el equipo cliente, navegue hasta **https://<UCCX FQDN>:8444/** e instale el certificado a través de las indicaciones del explorador.

Certificado CUIC Live Data (desde 11.x)

CUIC utiliza el servicio E/S de socket para los datos activos del servidor. Este certificado debe instalarse en el equipo cliente para los agentes, supervisores y usuarios de informes que utilizan la interfaz web de CUIC para datos en directo o que utilizan los gadgets de datos en directo de Finesse.

Para instalar el certificado de E/S de socket en el explorador, en el equipo cliente, navegue hasta **https://<UCCX FQDN>:12015/** e instale el certificado a través de las indicaciones del explorador.

Aplicaciones de terceros accesibles desde scripts

Si un script UCCX está diseñado para acceder a una ubicación segura en un servidor de terceros (por ejemplo, el paso *Get URL Document* a una URL HTTPS o un *Make Rest Call* a una URL HTTPS REST), cargue la cadena de certificados firmada o autofirmada del servicio de terceros en el almacén de claves UCCX *tomcat-trust*. Para obtener este certificado, acceda a la página UCCX **OS Administration** y elija **Upload Certificate**.

El motor UCCX se configura para buscar en el almacén de claves de Tomcat de la plataforma cadenas de certificados de terceros cuando las aplicaciones de terceros les presentan estos certificados cuando acceden a ubicaciones seguras mediante pasos de secuencia de comandos.

La cadena de certificados completa debe cargarse en el almacén de claves de Tomcat de la plataforma, al que se puede acceder a través de la página **Administración del SO**, ya que el almacén de claves de Tomcat no contiene certificados raíz de forma predeterminada.

Una vez completadas estas acciones, reinicie el motor Cisco UCCX.

Verificación

Para comprobar que todos los certificados están instalados correctamente, puede probar las características descritas en esta sección. Si no aparecen errores de certificado y todas las características funcionan correctamente, los certificados se instalan correctamente.

- Configure Finesse para que registre automáticamente a un agente mediante el flujo de trabajo. Después de que el agente maneje una llamada, utilice la aplicación MediaSense Search and Play para encontrar la llamada. Compruebe que la llamada tiene el agente, una cola de servicio de contacto y etiquetas de equipo asociadas a los metadatos de grabación en MediaSense.
- Configure el chat web de agentes a través de SocialMiner. Inserte un contacto de chat a través del formulario web. Compruebe que el agente recibe el banner para aceptar el contacto de chat y también que una vez que se acepta el contacto de chat, el formulario de chat se carga correctamente y el agente puede recibir y enviar mensajes de chat.
- Intente iniciar sesión en un agente mediante Finesse. Compruebe que no aparece ninguna advertencia de certificado y que la página Web no solicita la instalación de certificados en el explorador. Compruebe que el agente puede cambiar de estado correctamente y que se presenta correctamente al agente una nueva llamada a UCCX.
- Después de configurar los gadgets de Live Data en el diseño de escritorio de Finesse agente y supervisor, inicie sesión en un agente, un supervisor y un usuario de informes. Compruebe que los gadgets de Live Data se cargan correctamente, que los datos iniciales se rellenan en el gadget y que los datos se actualizan cuando cambian los datos subyacentes.
- Intente conectarse desde un explorador a la URL de AppAdmin en ambos nodos UCCX. Verifique que no aparezca ninguna advertencia de certificado cuando se le solicite en la página de inicio de sesión.

Troubleshoot

Problema: ID de usuario/contraseña no válidos

Los agentes de UCCX Finesse no pueden iniciar sesión con el error "**ID de usuario/contraseña no válidos**".

Causas

Unified CCX produce una excepción "SSLHandshakeException" y no puede establecer una conexión con Unified CM.

Solución

- Compruebe que el certificado Tomcat de Unified CM no ha caducado.
- Asegúrese de que cualquier certificado que haya cargado en Unified CM tiene una de estas extensiones marcada como crítica:
  Uso de claves de X509v3 (OID - 2.5.29.15)

Restricciones básicas de X509v3 (OID - 2.5.29.19)

Si marca otras extensiones como críticas, la comunicación entre Unified CCX y Unified CM fallará debido a un error en la verificación del certificado de Unified CM.

Problema - La SAN CSR y la SAN de certificado no coinciden

La carga de un certificado firmado por CA muestra el error "CSR SAN y Certificate SAN no coinciden".

Causas

Es posible que la CA haya agregado otro dominio primario en el campo de nombres alternativos de sujeto (SAN) del certificado. De forma predeterminada, CSR tendrá estas SAN:

SubjectAltName [
  example.com (dNSName)
  hostname.example.com (dNSName)
]

Las CA pueden devolver un certificado con otra SAN agregada al certificado: www.hostname.example.com. El certificado tendrá una SAN adicional en este caso:

SubjectAltName [
  example.com (dNSName)
  hostname.example.com (dNSName)

  www.hostname.example.com (dNSName)
]

Esto provoca el error de discordancia de SAN.

Solución

En la sección "Nombre alternativo del sujeto (SAN)" de la página "Generar solicitud de firma de certificado" de UCCX, genere el CSR con un campo Dominio principal vacío. De esta manera, la CSR no se genera con un atributo SAN, la CA puede formatear las SAN y no habrá una discordancia de atributo SAN cuando cargue el certificado en UCCX. Tenga en cuenta que el campo Dominio principal toma de forma predeterminada el dominio del servidor UCCX, por lo que el valor debe eliminarse explícitamente mientras se configuran los parámetros de CSR.

Problema - NET::ERR_CERT_COMMON_NAME_INVALID

Al acceder a cualquier página web de UCCX, MediaSense o SocialMiner, recibirá un mensaje de error.

"Su conexión no es privada.

Es posible que los atacantes intenten robar su información de <FQDN_servidor> (por ejemplo, contraseñas, mensajes o tarjetas de crédito). NET::ERR_CERT_COMMON_NAME_INVALID

Este servidor no pudo probar que es <Server_FQDN>; su certificado de seguridad es de [missing_subjectAltName]. Esto puede deberse a un error de configuración o a que un atacante intercepte su conexión".

Causas

Chrome versión 58 introdujo una nueva función de seguridad donde se informa de que el certificado de un sitio web no es seguro si su nombre común (CN) no se incluye también como una SAN.

Solución

- Puede navegar hasta **Advanced >** Proceed to <Server_FQDN> (unsafe) para continuar al sitio y aceptar el error del certificado.
- Puede evitar el error junto con los certificados firmados por la CA. Al generar una CSR, el FQDN del servidor se incluye como una SAN. La CA puede firmar el CSR y, después de volver a cargar el certificado firmado en el servidor, el certificado del servidor tendrá el FQDN en el campo SAN para que no se presente el error.

Más información

Consulte la sección "Quitar compatibilidad con coincidencia de commonName en certificados" en Deprecaciones y eliminaciones en Chrome 58.

Defectos de certificado

- ID de bug de Cisco CSCvb46250 - UCCX: Impacto del certificado ECDSA de Tomcat en los datos en directo de Finesse
- Id. de error de Cisco CSCvb58580: no se puede iniciar sesión en SocialMiner con tomcat y tomcat-ECDSA firmados por RSA CA
- ID de bug de Cisco CSCvd56174 - UCCX: Error de conexión del agente Finesse debido a SSLHandshakeException
- ID de bug de Cisco CSCuv89545 - Vulnerabilidad de Logjam de Finesse

Información Relacionada

- Entender los certificados ECDSA en una solución UCCX
- Compatibilidad con SHA 256 para UCCX
- Ejemplo de Configuración de Certificados Firmados y Autofirmados UCCX
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).