

Soporte del SHA-256 para UCCX

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Avisos de Microsoft y del Mozilla](#)

[Experiencia del usuario](#)

[Consideraciones UCCX](#)

[Notaciones usadas en este documento](#)

[UCCX 11.5](#)

[UCCX 11.0\(1\)](#)

[UCCX 10.5 y 10.6](#)

[UCCX 10.0](#)

[Instrucciones de la administración de certificados](#)

[Certificados autofirmados](#)

[Certificados de la Raíz confiable](#)

[Certificados firmados del otro vendedor](#)

[Notas complementarias](#)

Introducción

Este documento describe el soporte del SHA-256 para el Cisco Unified Contact Center Express (UCCX). El cifrado SHA-1 será desaprobadado pronto y todos los buscadores Web soportados para UCCX comenzarán a bloquear las páginas web de los servidores que ofrecen los Certificados con el cifrado SHA-1.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Unified Contact Center Express (UCCX)
- Administración de certificados

Avisos de Microsoft y del Mozilla

[Actualización de la deprecación SHA-1](#)

[Continuación eliminar los Certificados SHA-1](#)

En estos avisos, el navegador que los fabricantes han expuesto a los navegadores mostrará las advertencias bypassable para los Certificados SHA-1 encontrados que se publican con las fechas

de **ValidFrom** después del 1 de enero, 2016.

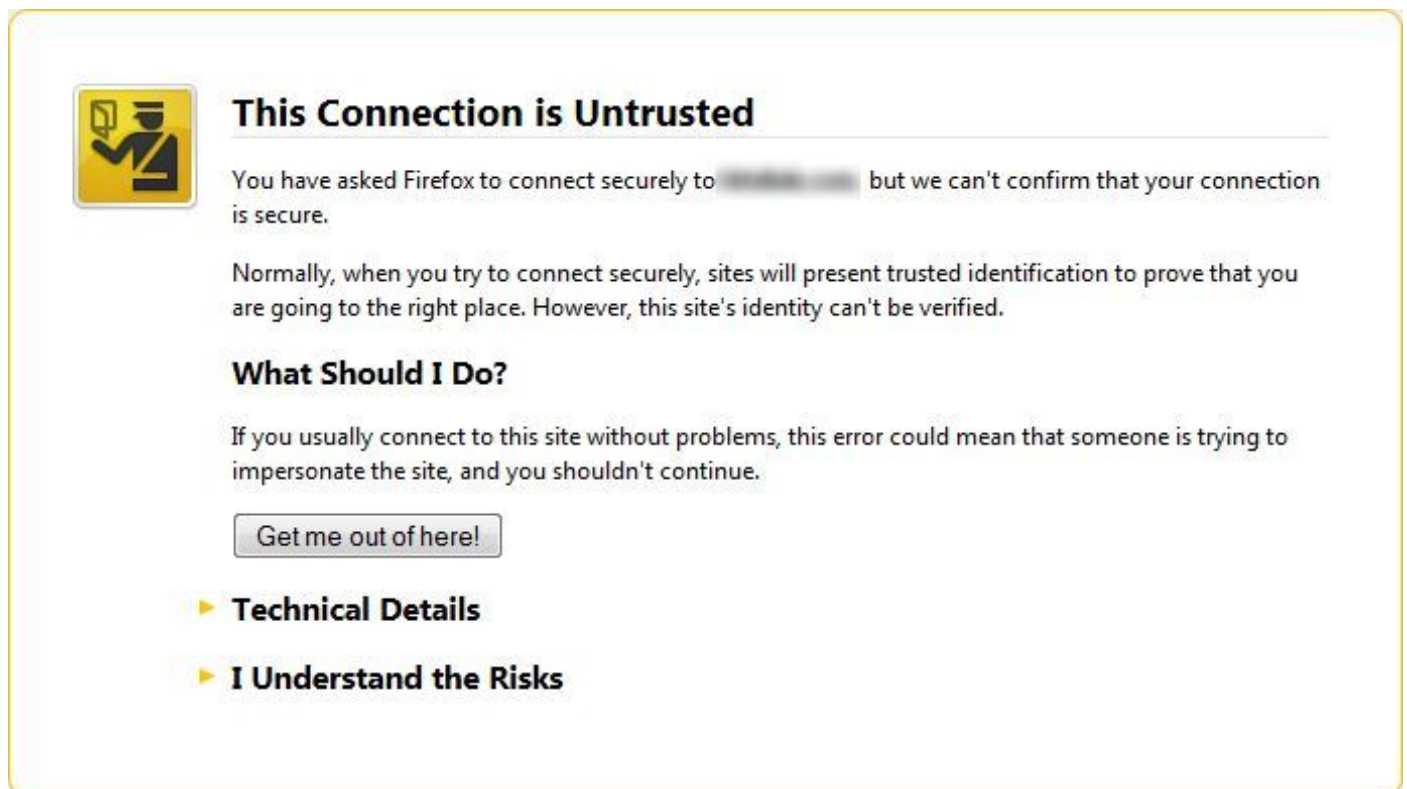
Además, el plan actual del expediente es bloquear los sitios web que utilizan los Certificados SHA-1 después del 1 de enero de 2017 sin importar la entrada de ValidFrom en el certificado. Sin embargo, con los ataques recientes que apuntan los Certificados SHA-1, estos navegadores pudieron levantar este timeline y bloquear los sitios web que utilizan los Certificados SHA-1 después del 1 de enero de 2017 sin importar la fecha de problema del certificado.


Cisco aconseja a los clientes leer los avisos detalladamente y permanecer actualizados en otros avisos de Microsoft y el Mozilla en este tema.

Algunas versiones de UCCX generan los Certificados SHA-1. Si usted accede las páginas web UCCX protegidas por los Certificados SHA-1, puede ser que generen una advertencia o sean bloqueadas de acuerdo con las fechas y las reglas conocidas previamente.

Experiencia del usuario

Cuando se detecta un certificado SHA-1, dependiente sobre la fecha de ValidFrom y las reglas previamente mencionadas, el usuario pudo ver un mensaje similar a esto:



 **This Connection is Untrusted**

You have asked Firefox to connect securely to [redacted] but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

[Get me out of here!](#)

- ▶ **Technical Details**
- ▶ **I Understand the Risks**

El dependiente sobre las decisiones tomadas, un usuario pudo o no pudo poder desviar esta advertencia.

Consideraciones UCCX

Estas tablas describen las estrategias del impacto y de la mitigación del certificado SHA-1 para cada versión de UCCX actualmente bajo mantenimiento de software.

Notaciones usadas en este documento

Notación



Soportado ya. Ninguna otra acción requerida.



El soporte está disponible, pero la regeneración de los Certificados es necesaria.



El soporte no está disponible.

Descripción

UCCX 11.5













	La administración UCCX	La administración CUIC Datos vivos #	Escritorio de la administración de la delicadeza #	Correo electrónico y charla del agente con SocialMiner*	Pasos del scripting del RESTO UCCX	Grabación MediaSense 11.5
Fresco instale						
Actualización de la versión anterior	 Los Certificados UCCX conservan el algoritmo de más viejas versiones. Si están generados con una clave SHA-11 en más viejas versiones, los certificados autofirmados son SHA-1 basado y necesitan ser regenerados.	 Los Certificados unificados Cisco del centro de la inteligencia UCCX (CUIC) conservan el algoritmo de más viejas versiones. Si están generados con una clave SHA-11 en más viejas versiones, los certificados autofirmados son SHA-1 basado y necesitan ser regenerados.	 Los Certificados de la delicadeza UCCX conservan el algoritmo de más viejas versiones. Si están generados con una clave SHA-11 en más viejas versiones, los certificados autofirmados son SHA-1 basado y necesitan ser regenerados.	 Los Certificados de SocialMiner y UCCX conservan el algoritmo de más viejas versiones. Si están generados con una clave SHA-11 en más viejas versiones, los certificados autofirmados son SHA-1 basado y necesitan ser regenerados.	 UCCX no rechazará a un servidor Web remoto que utilice los Certificados SHA-1 como parte de la comunicación representativa de la transferencia del estado (RESTO). Los pasos del RESTO trabajarán después de que los Certificados se regeneren en el UCCX.	 Los Certificados MediaSense UCCX conservan el algoritmo de más viejas versiones. Si están generados con una clave SHA-11 en más viejas versiones, los certificados autofirmados son SHA-1 basado y necesitan ser regenerados.

Nota: el *The regeneró MediaSense y los certificados de SocialMiner se deben reimportar en UCCX.

Nota: las acciones separadas del #No son necesarias para la delicadeza y CUIC. Los Certificados se regeneran solamente una vez en la página de administración de la plataforma UCCX.

UCCX 11.0(1)

La Datos vivos de Escritorio de la Correo Pasos del Grabación con













	administración UCCX	la administración CUIC #	administración de la delicadeza #	electrónico y charla del agente con SocialMiner **	scripting del RESTO UCCX	MediaSense * 11.0* y 10.5*
Fresco instale	 Por abandono todos los frescos uno mismo-firmada instalan los Certificados son los Certificados SHA-1 y necesitan ser regenerados.	 Por abandono todos los frescos uno mismo-firmada instalan los Certificados son los Certificados SHA-1 y necesitan ser regenerados.	 Por abandono todos los frescos uno mismo-firmada instalan los Certificados son los Certificados SHA-1 y necesitan ser regenerados.	 Por abandono todos los frescos uno mismo-firmada instalan los Certificados son los Certificados SHA-1 y necesitan ser regenerados.	 UCCX no rechazará a un servidor Web remoto que utilice los Certificados SHA-1 como parte de la comunicación del RESTO. Los pasos del RESTO trabajarán después de que los Certificados se regeneren en el UCCX.	 El certificado autofirmado predeterminado es SHA-1. El certificado de la regeneración no proporciona una opción para el SHA-256.
Actualización de la versión anterior	 Los Certificados UCCX conservan el algoritmo de más viejas versiones. Si están generados con una clave SHA-11 en más viejas versiones, los certificados autofirmados son SHA-1 basado y necesitan ser regenerados.	 Los Certificados UCCX CUIC conservan el algoritmo de más viejas versiones. Si están generados con una clave SHA-11 en más viejas versiones, los certificados autofirmados son SHA-1 basado y necesitan ser regenerados.	 Los Certificados de la delicadeza UCCX conservan el algoritmo de más viejas versiones. Si están generados con una clave SHA-11 en más viejas versiones, los certificados autofirmados son SHA-1 basado y necesitan ser regenerados.	 Los Certificados de SocialMiner y UCCX conservan el algoritmo de más viejas versiones. Si están generados con una clave SHA-11 en más viejas versiones, los certificados autofirmados son SHA-1 basado y necesitan ser regenerados.	 UCCX no rechazará a un servidor Web remoto que utilice los Certificados SHA-1 como parte de la comunicación del RESTO. Los pasos del RESTO trabajarán después de que los Certificados se regeneren en el UCCX.	 El certificado autofirmado predeterminado es SHA-1. El certificado de la regeneración no proporciona una opción para el SHA-256.

Nota: El *An que dirige el Special (ES) será liberado para permitir que MediaSense 10.5 y 11.0 genere y que valide los Certificados del SHA-256.

Nota: ** Los certificados regenerados de MediaSense y de SocialMiner se deben reimportar en UCCX.

Nota: las acciones separadas del #No son necesarias para la delicadeza y CUIX. Los Certificados se regeneran solamente una vez en la página de administración de la plataforma UCCX.

UCCX 10.5 y 10.6

	La administración UCCX	Datos vivos de la administración CUIX #	Escritorio de la administración de la delicadeza #	Correo electrónico y charla del agente con SocialMiner*	Pasos del scripting del RESTO UCCX	Grabación con el *** 10.0**/10.5** de MediaSense
Fresco instale	 Por abandono todos los frescos uno mismo-firmada instalan los Certificados son los Certificados SHA-1 y necesitan ser regenerados.	 Por abandono todos los frescos uno mismo-firmada instalan los Certificados son los Certificados SHA-1 y necesitan ser regenerados.	 Por abandono todos los frescos uno mismo-firmada instalan los Certificados son los Certificados SHA-1 y necesitan ser regenerados.	 El soporte del SHA-256 para el correo electrónico del agente y la charla están disponibles solamente en SocialMiner (SM) v11 y SM v11 no es compatibles con UCCX v10.x.	 UCCX no rechazará a un servidor Web remoto que utilice los Certificados SHA-1 como parte de la comunicación del RESTO. Los pasos del RESTO trabajarán después de que los Certificados se regeneren en el UCCX.	 El certificado autofirmado predeterminado es SHA-1. El certificado de la regeneración no proporciona una opción para el SHA-256.
Actualización de la versión anterior	 Los Certificados conservan el algoritmo de más viejas versiones. Si están generados con una clave SHA-11 en más viejas versiones, los certificados autofirmados son SHA-1 basado y necesitan ser regenerados.	 Los Certificados conservan el algoritmo de más viejas versiones. Si están generados con una clave SHA-11 en más viejas versiones, los certificados autofirmados son SHA-1 basado y necesitan ser regenerados.	 Los Certificados conservan el algoritmo de más viejas versiones. Si están generados con una clave SHA-11 en más viejas versiones, los certificados autofirmados son SHA-1 basado y necesitan ser regenerados.	 El soporte del SHA-256 para el correo electrónico del agente y la charla están disponibles solamente en SM v11 y SM v11 no es compatibles con UCCX v10.x.	 UCCX no rechazará a un servidor Web remoto que utilice los Certificados SHA-1 como parte de la comunicación del RESTO. Los pasos del RESTO trabajarán después de que los Certificados se regeneren en el UCCX.	 El certificado autofirmado predeterminado es SHA-1. El certificado de la regeneración no proporciona una opción para el SHA-256.













Nota: El *An que dirige el Special será liberado para permitir que SocialMiner 10.6 genere y que valide los Certificados del SHA-256.

Nota: ** Un Special de la ingeniería (ES) será liberado para permitir que MediaSense 10.0 y 10.5 genere y que valide los Certificados del SHA-256.

Nota: El *** los certificados regenerados de MediaSense y de SocialMiner se debe reimportar en UCCX.

Nota: las acciones separadas del #No son necesarias para la delicadeza y CUIC. Los Certificados se regeneran solamente una vez en la página de administración de la plataforma UCCX.

UCCX 10.0

	La administración UCCX **	Datos vivos de la administración CUIC #	Escritorio de la administración de la delicadeza #	Charla del agente con SocialMiner*	Pasos del scripting del RESTO UCCX	Grabación con el *** 10.0** de MediaSense
Fresco instale	 El certificado autofirmado predeterminado es SHA-1. El certificado de la regeneración no proporciona una opción para el SHA-256.	 El certificado autofirmado predeterminado es SHA-1. El certificado de la regeneración no proporciona una opción para el SHA-256.	 El certificado autofirmado predeterminado es SHA-1. El certificado de la regeneración no proporciona una opción para el SHA-256.	 El soporte del SHA-256 para el agente que la charla está disponible solamente en SM v11 y SM v11 no es compatible con UCCX v10.x.	 UCCX no rechazará a un servidor Web remoto que utilice los Certificados SHA-1 como parte de la comunicación del RESTO. Los pasos del RESTO trabajarán después de que los Certificados se regeneren en el UCCX.	 El certificado autofirmado predeterminado es SHA-1. El certificado de la regeneración no proporciona una opción para el SHA-256.
Actualización de la versión anterior	 El certificado autofirmado predeterminado es SHA-1. El certificado de la regeneración no proporciona una opción para el SHA-256.	 El certificado autofirmado predeterminado es SHA-1. El certificado de la regeneración no proporciona una opción para el SHA-256.	 El certificado autofirmado predeterminado es SHA-1. El certificado de la regeneración no proporciona una opción para el SHA-256.	 El soporte del SHA-256 para el agente que la charla está disponible solamente en SM v11 y SM v11 no es	 UCCX no rechazará a un servidor Web remoto que utilice los Certificados SHA-1 como parte de la comunicación del RESTO. Los pasos	 El certificado autofirmado predeterminado es SHA-1. El certificado de la regeneración no proporciona una opción para el SHA-256.

compatible
con UCCX
v10.x.

del RESTO
trabajarán
después de
que los
Certificados
se regeneren
en el UCCX.

Nota: El *An que dirige el Special será liberado para permitir que SocialMiner 10.6 genere y que valide los Certificados del SHA-256.

Nota: ** Un Special de la ingeniería (ES) será liberado para permitir que MediaSense 10.0 genere y que valide los Certificados del SHA-256.

Nota: El *** los certificados regenerados de MediaSense y de SocialMiner se debe reimportar en UCCX.

Nota: las acciones separadas del #No son necesarias para la delicadeza y CUIIC. Los Certificados se regeneran solamente una vez en la página de administración de la plataforma UCCX.

Instrucciones de la administración de certificados

Hay tres tipos de Certificados que necesiten ser verificados y potencialmente ser regenerados:

- Certificados firmados del uno mismo
- Certificados de la Raíz confiable
- Certificados firmados del otro vendedor

Certificados autofirmados

Navegue a la página de administración OS. Elija la **Seguridad > navegan a la administración de certificados**. Haga clic en Find (Buscar).

Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions

Navigation Cisco Unified OS Administration Go
admin | Search Documentation | About | Logout

Show Settings Security Software Upgrades Services Help

Certificate List

Generate Self-signed Upload Certificate/Certificate chain Generate CSR

Status
95 records found

Certificate List (1 - 95 of 95) Rows per Page 100

Find Certificate List where Certificate begins with Find Clear Filter

Certificate	Common Name	Type	Distribution	Issued By	Expiration	Description
ipsec	ccx-94-45.cisco.com	Self-signed	ccx-94-45.cisco.com	ccx-94-45.cisco.com	11/28/2020	Self cert gen by s
ipsec-trust	ccx-94-45.cisco.com	Self-signed	ccx-94-45.cisco.com	ccx-94-45.cisco.com	11/28/2020	Trus Cert
tomcat	ccx-94-45.cisco.com	Self-signed	ccx-94-45.cisco.com	ccx-94-45.cisco.com	11/28/2020	Self cert gen by s
tomcat-trust	T-TeleSec_GlobalRoot_Class_2	Self-signed	T-TeleSec_GlobalRoot_Class_2	T-TeleSec_GlobalRoot_Class_2	10/02/2033	Trus Cert
tomcat-trust	Thawte_Server_CA	Self-signed	Thawte_Server_CA	Thawte_Server_CA	01/02/2021	Trus Cert
tomcat-trust	GTE_CyberTrust_Global_Root	Self-signed	GTE_CyberTrust_Global_Root	GTE_CyberTrust_Global_Root	08/14/2018	Trus Cert
tomcat-trust	LuxTrust_Global_Root	Self-signed	LuxTrust_Global_Root	LuxTrust_Global_Root	03/17/2021	Trus Cert
tomcat-trust	TC_TrustCenter_Class_2_CA_II	Self-signed	TC_TrustCenter_Class_2_CA_II	TC_TrustCenter_Class_2_CA_II	01/01/2026	Trus Cert

Note las cuatro categorías del certificado:

- IPsec
- IPsec-confianza
- tomcat
- Tomcat-confianza

Los Certificados conforme al **tomcat** y al tipo de la categoría **Uno mismo-firmados** son los que requieren la regeneración. En la imagen anterior, el tercer certificado es el que requiere la regeneración.

Complete estos pasos para regenerar los Certificados:

Paso 1. Haga clic el Common Name del certificado.

Paso 2. De la ventana emergente, **regenerado del** tecleo.

Paso 3. Elija el algoritmo de encriptación del SHA-256.

Para la versión 10.6 UCCX, complete estos pasos para regenerar los Certificados:

Paso 1. Haga clic en **generan nuevo**.

Paso 2. Seleccione el *nombre del certificado* como **tomcat**, la *longitud de clave* como **2048** y el *algoritmo de troceo* como **SHA256**.

Paso 3. El tecleo **genera nuevo**.

Generate Certificate

Generate New Close

Status

Status: Ready

Generate Certificate

Certificate Name* tomcat

Key Length* 2048

Hash Algorithm* SHA256

Generate New Close

Certificados de la Raíz confiable

Éstos son los Certificados que son proporcionados por la plataforma. Las firmas basadas SHA-1 para estos Certificados no son un problema porque estos Certificados son confiados en por los clientes de Transport Layer Security (TLS) basados en su identidad, bastante que la firma de su hash.

Certificados firmados del otro vendedor

Los Certificados firmados por un Certificate Authority del otro vendedor con el algoritmo SHA-1 necesitan ser reimportados con los certificados firmados del SHA-256. Todos los Certificados en una Cadena de certificados se deben dimitir con el SHA-256.

Notas complementarias

Los últimos especiales de ingeniería se fijan en [cisco.com](https://www.cisco.com) cuando están disponibles. Marque las páginas de productos correspondientes regularmente para saber si hay las descargas especiales de la ingeniería.

- Para cualquier ayuda en la regeneración del certificado o los problemas asociados, abra un caso del TAC de Cisco.
- Los clientes que se ejecutan en las versiones 8.x o 9.x UCCX deben planear actualizar a las últimas versiones admitidas para mantener Cisco y el soporte de buscador.