SHA-256 Support for UCCX

Contents

Introduction

This document describes SHA-256 support for Cisco Unified Contact Center Express (UCCX). SHA-1 encryption will be deprecated soon and all supported web browsers for UCCX will begin to block web pages from servers that offer certificates with the SHA-1 encryption.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Unified Contact Center Express (UCCX)
- Certificate Management

Announcements from Microsoft and Mozilla

[SHA-1 Deprecation Update](#)

[Continuing to Phase Out SHA-1 Certificates](#)

In these notices, the browser manufacturers have stated the browsers will show bypassable warnings for SHA-1 certificates encountered that are issued with **ValidFrom** dates after January 1, 2016.

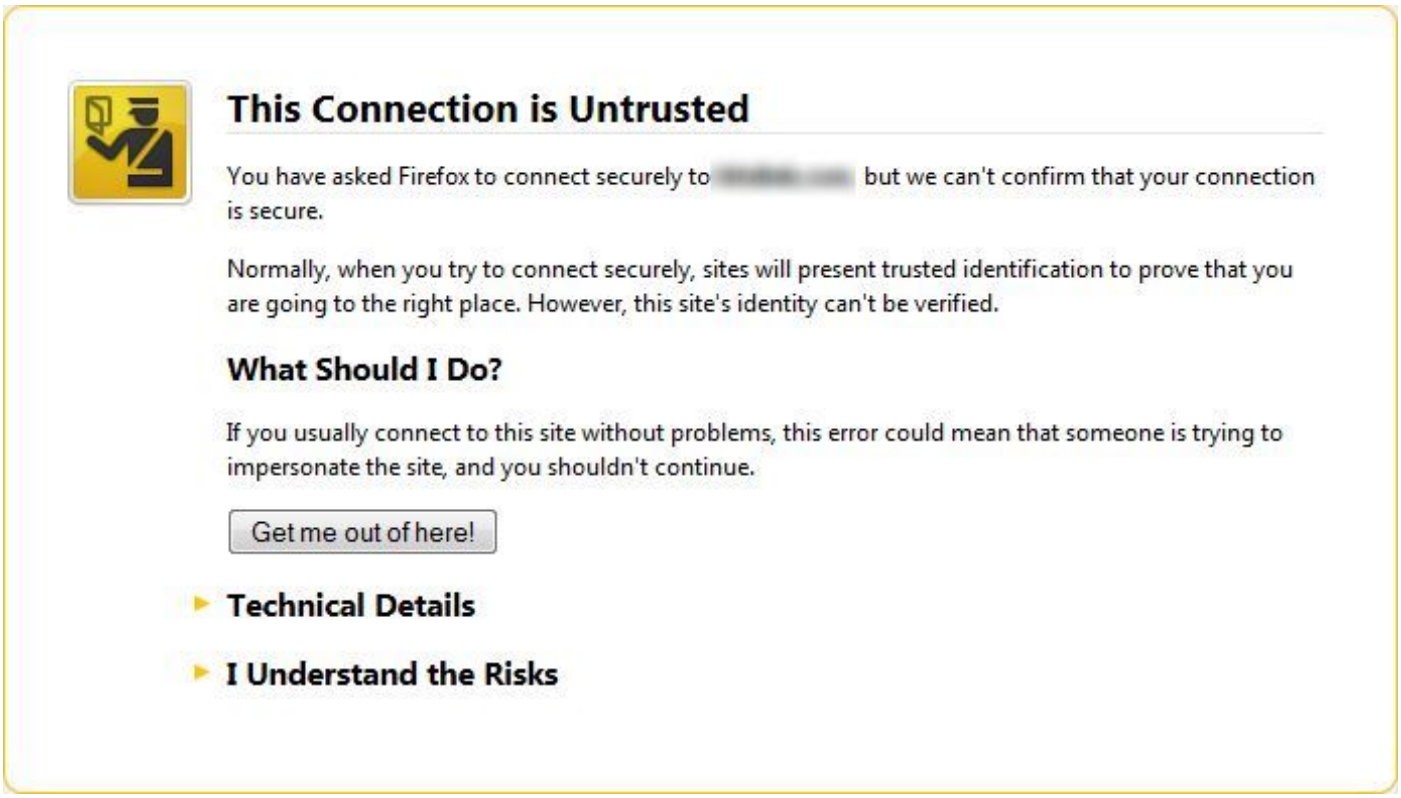
In addition, the current plan of record is to block websites that use SHA-1 certificates after January 1, 2017 regardless of the ValidFrom entry in the certificate. However, with recent attacks that target SHA-1 certificates, these browsers might move up this timeline and block websites that use SHA-1 certificates after January 1, 2017 regardless of the certificate issue date.

Cisco advises customers to read the announcements in detail and stay up-to-date on further announcements from Microsoft and Mozilla on this topic.

Some versions of UCCX generate SHA-1 certificates. If you access UCCX web pages protected by SHA-1 certificates, they might generate a warning or be blocked in accordance with the dates and rules noted previously.

User Experience

When a SHA-1 certificate is detected, dependent upon the ValidFrom date and the previously listed rules, the user might see a message similar to this:



Dependent upon the decisions made, a user might or might not be able to bypass this warning.

UCCX Considerations

These tables describe SHA-1 certificate impact and mitigation strategies for each version of UCCX currently under software maintenance.

Notations Used in This Document

Notation	Description
✅	Already supported. No further action required.
⚠	Support is available, but regeneration of certificates is needed.

Support is not available.

UCCX 11.5

	UCCX Administration	CUIC Administration Live Data#	Finesse Administration Desktop#	Agent Email and Chat with SocialMiner*	UCCX REST Scripting Steps	Recording with MediaSense* 11.5
Fresh Install						
Upgrade from Previous Version	The UCCX certificates retain the algorithm from older releases. If generated with a SHA-11 key in older releases, the self-signed certificates are SHA-1 based and need to be regenerated.	The UCCX Cisco Unified Intelligence Center (CUIC) certificates retain the algorithm from older releases. If generated with a SHA-11 key in older releases, the self-signed certificates are SHA-1 based and need to be regenerated.	The UCCX Finesse certificates retain the algorithm from older releases. If generated with a SHA-11 key in older releases, the self-signed certificates are SHA-1 based and need to be regenerated.	The SocialMiner **and** UCCX certificates retain the algorithm from older releases. If generated with a SHA-11 key in older releases, the self-signed certificates are SHA-1 based and need to be regenerated.	UCCX will not reject a remote web server that uses SHA-1 certificates as part of the Representational State Transfer (REST) communication. The REST steps will work after the certificates are regenerated on the UCCX.	The MediaSense **and** UCCX certificates retain the algorithm from older releases. If generated with a SHA-11 key in older releases, the self-signed certificates are SHA-1 based and need to be regenerated.

Note: *The regenerated MediaSense and SocialMiner certificate(s) must be reimported into UCCX.

Note: #No separate actions are needed for Finesse and CUIC. The certificates are regenerated only once on the UCCX platform administration page.

UCCX 11.0(1)

	UCCX Administration	CUIC Administration Live Data#	Finesse Administration Desktop#	Agent Email and Chat with SocialMiner**	UCCX REST Scripting Steps	Recording With MediaSense* 11.0* and 10.5*
Fresh Install	By default all self-signed fresh install certificates are SHA-1	By default all self-signed fresh install certificates are SHA-1	By default all self-signed fresh install certificates are SHA-1	By default all self-signed fresh install certificates are SHA-1	UCCX will not reject a remote web server that uses SHA-1 certificates as	The default self-signed certificate is SHA-1. The

	certificates and need to be regenerated.	certificates and need to be regenerated.	certificates and need to be regenerated.	certificates and need to be regenerated.	part of the REST communication. The REST steps will work after the certificates are regenerated on the UCCX.	regeneration certificate does not provide an option for SHA-256.
Upgrade from Previous Version	⚠ The UCCX certificates retain the algorithm from older releases. If generated with a SHA-11 key in older releases, the self-signed certificates are SHA-1 based and need to be regenerated.	⚠ The UCCX CUIC certificates retain the algorithm from older releases. If generated with a SHA-11 key in older releases, the self-signed certificates are SHA-1 based and need to be regenerated.	⚠ The UCCX Finesse certificates retain the algorithm from older releases. If generated with a SHA-11 key in older releases, the self-signed certificates are SHA-1 based and need to be regenerated.	⚠ The SocialMiner **and** UCCX certificates retain the algorithm from older releases. If generated with a SHA-11 key in older releases, the self-signed certificates are SHA-1 based and need to be regenerated.	⚠ UCCX will not reject a remote web server that uses SHA-1 certificates as part of the REST communication. The REST steps will work after the certificates are regenerated on the UCCX.	⛔ The default self-signed certificate is SHA-1. The regeneration certificate does not provide an option for SHA-256.

Note: *An Engineering Special (ES) will be released in order to allow MediaSense 10.5 and 11.0 to generate and accept SHA-256 certificates.

Note: **The regenerated MediaSense and SocialMiner certificate(s) must be reimported into UCCX.

Note: #No separate actions are needed for Finesse and CUIC. The certificates are regenerated only once on the UCCX platform administration page.

UCCX 10.5 and 10.6

	UCCX Administration	**CUIC Administration Live Data#**	**Finesse Administration Desktop#**	**Agent Email and Chat with SocialMiner***	**UCCX REST Scripting Steps**	**Recording With MediaSense** 10.0** / 10.5****
Fresh Install	⚠ By default all self-signed fresh install certificates are SHA-1	⚠ By default all self-signed fresh install certificates are SHA-1	⚠ By default all self-signed fresh install certificates are SHA-1	⛔ SHA-256 support for agent email and chat are available	⚠ UCCX will not reject a remote web server that uses SHA-1 certificates as	⛔ The default self-signed certificate is SHA-1. The

	certificates and need to be regenerated.	certificates and need to be regenerated.	certificates and need to be regenerated.	only in SocialMiner (SM) v11 and SM v11 is not compatible with UCCX v10.x.	part of the REST communication. The REST steps will work after the certificates are regenerated on the UCCX.	regeneration certificate does not provide an option for SHA 256.
Upgrade from Previous Version	The certificates retain the algorithm from older releases. If generated with a SHA-11 key in older releases, the self-signed certificates are SHA-1 based and need to be regenerated.	The certificates retain the algorithm from older releases. If generated with a SHA-11 key in older releases, the self-signed certificates are SHA-1 based and need to be regenerated.	The certificates retain the algorithm from older releases. If generated with a SHA-11 key in older releases, the self-signed certificates are SHA-1 based and need to be regenerated.	SHA-256 support for agent email and chat are available only in SM v11 and SM v11 is not compatible with UCCX v10.x.	UCCX will not reject a remote web server that uses SHA-1 certificates as part of the REST communication. The REST steps will work after the certificates are regenerated on the UCCX.	The default self-signed certificate is SHA-1. The regeneration certificate does not provide an option for SHA 256.

Note: *An Engineering Special will be released in order to allow SocialMiner 10.6 to generate and accept SHA-256 certificates**.**

Note: **An Engineering Special (ES) will be released in order to allow MediaSense 10.0 and 10.5 to generate and accept SHA-256 certificates.

Note: ***The regenerated MediaSense and SocialMiner certificate(s) must be reimported into UCCX.

Note: #No separate actions are needed for Finesse and CUIC. The certificates are regenerated only once on the UCCX platform administration page.

UCCX 10.0

	UCCX Administration**	**CUIC Administration Live Data#**	**Finesse Administration Desktop#**	**Agent Chat with SocialMiner***	**UCCX REST Scripting Steps**	**Recording With MediaSense 10.0****
Fresh Install	The default self-signed certificate is SHA-1. The regeneration certificate does not provide an	The default self-signed certificate is SHA-1. The regeneration	The default self-signed certificate is SHA-1. The regeneration	SHA-256 support for agent chat is available only in SM v11 and SM	UCCX will not reject a remote web server that uses SHA-1 certificates as part of the	The default self-signed certificate is SHA-1. The regeneratio

	option for SHA-256.	certificate does not provide an option for SHA-256.	certificate does not provide an option for SHA-256.	v11 is not compatible with UCCX v10.x.	REST communication. The REST steps will work after the certificates are regenerated on the UCCX.	certificate do not provide a option for SH 256.
Upgrade from previous version	The default self-signed certificate is SHA-1. The regeneration certificate does not provide an option for SHA-256.	The default self-signed certificate is SHA-1. The regeneration certificate does not provide an option for SHA-256.	The default self-signed certificate is SHA-1. The regeneration certificate does not provide an option for SHA-256.	SHA-256 support for agent chat is available only in SM v11 and SM v11 is not compatible with UCCX v10.x.	UCCX will not reject a remote web server that uses SHA-1 certificates as part of the REST communication. The REST steps will work after the certificates are regenerated on the UCCX.	The default self-signed certificate is SHA-1. The regeneratio certificate do not provide a option for SH 256.

Note: *An Engineering Special will be released in order to allow SocialMiner 10.6 to generate and accept SHA-256 certificates**.**

Note: **An Engineering Special (ES) will be released in order to allow MediaSense 10.0 to generate and accept SHA-256 certificates.

Note: ***The regenerated MediaSense and SocialMiner certificate(s) must be reimported into UCCX.

Note: #No separate actions are needed for Finesse and CUIC. The certificates are regenerated only once on the UCCX platform administration page.

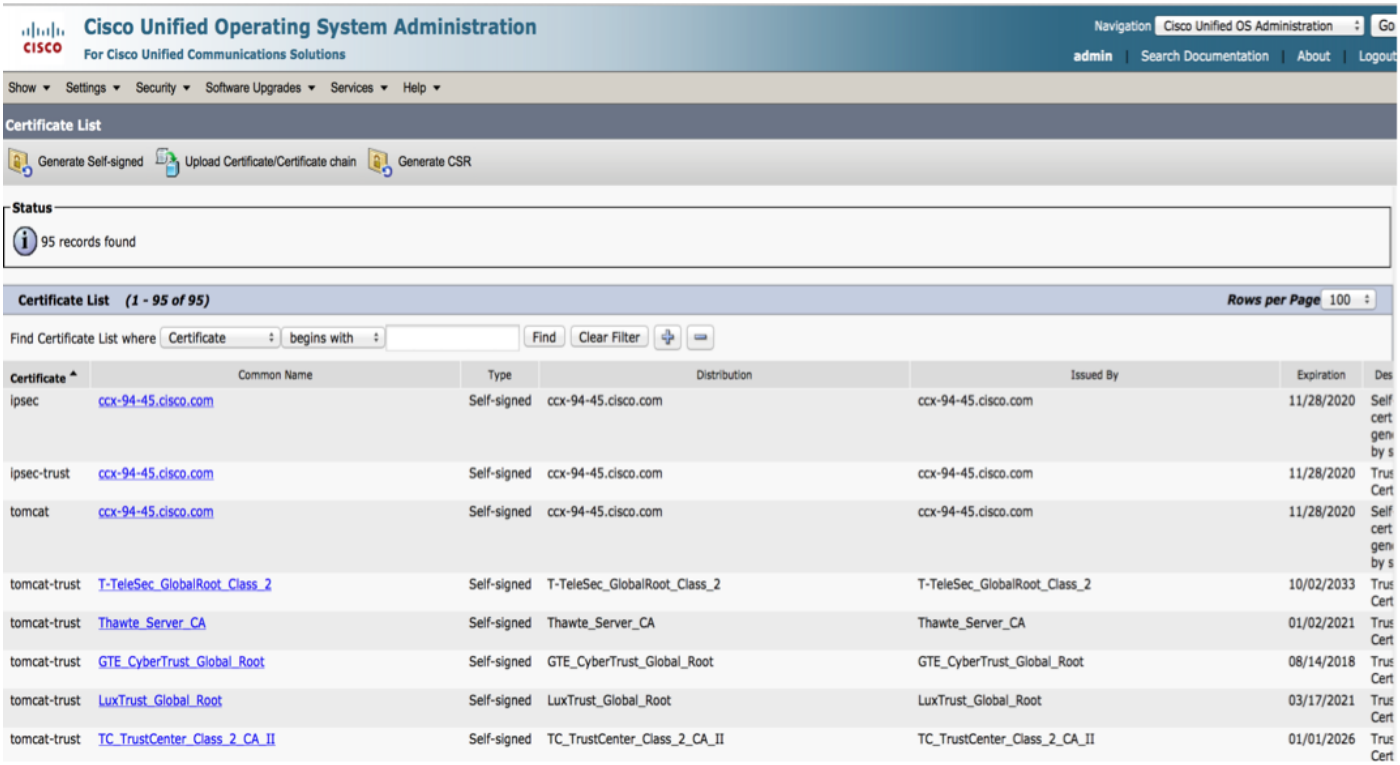
Certificate Management Instructions

There are three types of certificates that need to be verified and potentially regenerated:

- Self signed certificates
- Trusted root certificates
- Third party signed certificates

Self-Signed Certificates

Navigate to the OS Administration page. Choose **Security > Navigate to Certificate management**. Click **Find**.



Notice the four certificate categories:

- ipsec
- ipsec-trust
- tomcat
- tomcat-trust

The certificates under the category **tomcat** and type **Self-signed** are the ones that require regeneration. In the previous image, the third certificate is the one that requires regeneration.

Complete these steps in order to regenerate certificates:

Step 1. Click the Common Name of the certificate.

Step 2. From the popup window, click **Regenerate**.

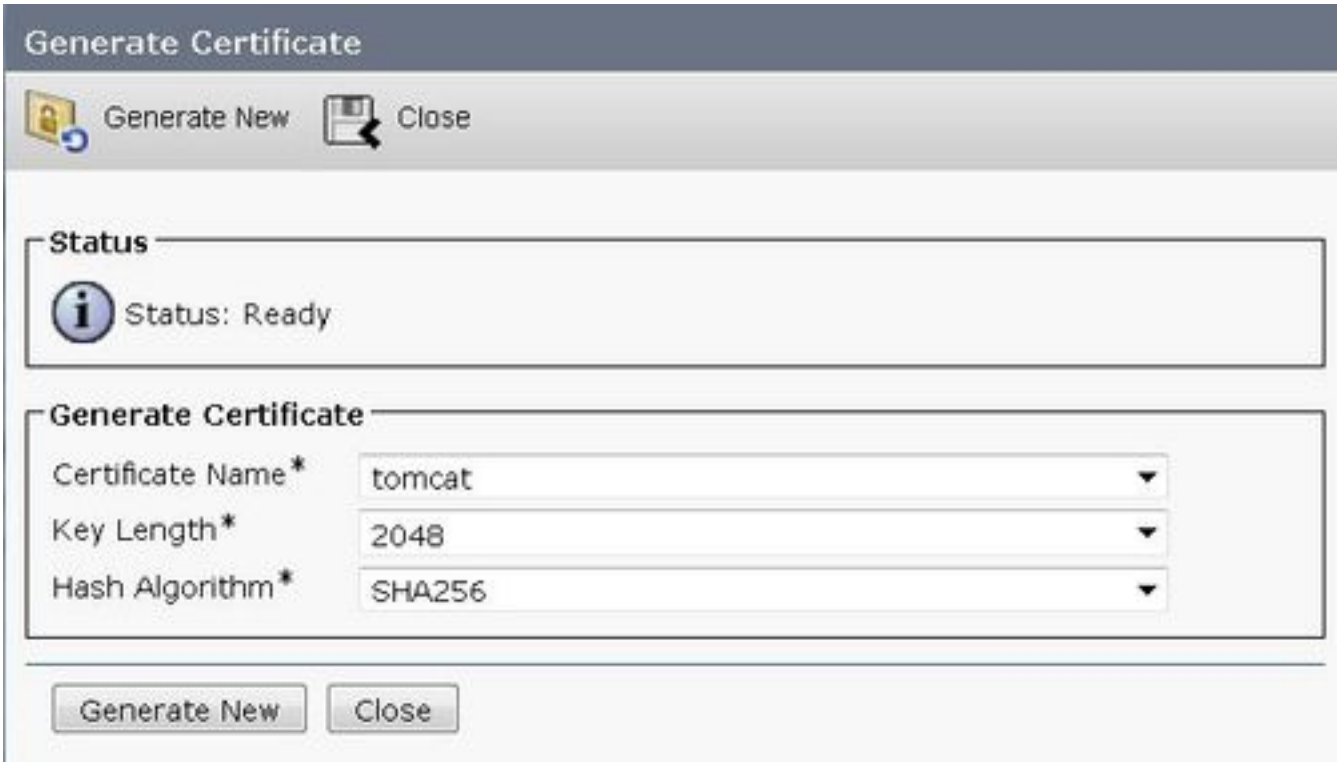
Step 3. Choose the encryption algorithm of SHA-256.

For UCCX version 10.6, complete these steps in order to regenerate certificates:

Step 1. Click on **Generate New**.

Step 2. Select *Certificate Name* as **tomcat**, *Key Length* as **2048** and *Hash Algorithm* as **SHA256.**

Step 3. Click **Generate New.**



Trusted Root Certificates

These are the certificates that are provided by the platform. SHA-1 based signatures for these certificates are not a problem because these certificates are trusted by the Transport Layer Security (TLS) clients based on their identity, rather than the signature of their hash.

Third Party Signed Certificates

Certificates signed by a third party Certificate Authority with the SHA-1 algorithm need to be reimported with SHA-256 signed certificates. All certificates in a certificate chain must be resigned with SHA-256.

Additional Notes

The latest Engineering Specials are posted on cisco.com when available. Check the corresponding product pages regularly for the Engineering Special downloads.

- For any assistance on certificate regeneration or associated issues, open a Cisco TAC case.
- Customers that run on UCCX versions 8.x or 9.x should plan to upgrade to the latest supported releases in order to maintain Cisco and browser support.