

Soutien SHA-256 d'UCCX

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Annonces de Microsoft et de Mozilla](#)

[Expérience utilisateur](#)

[Considérations UCCX](#)

[Notations utilisées dans ce document](#)

[UCCX 11.5](#)

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

[UCCX 10.5 et 10.6](#)

[UCCX 10.0](#)

[Instructions de Gestion de certificat](#)

[Certificats Auto-signés](#)

[Certificats racine de confiance](#)

[Certificats signés de tiers](#)

[Notes supplémentaires](#)

Introduction

Ce document décrit le soutien SHA-256 du Cisco Unified Contact Center Express (UCCX). Le cryptage SHA-1 sera désapprouvé bientôt et tous les navigateurs Web pris en charge pour UCCX commenceront à bloquer des pages Web des serveurs qui offrent des Certificats avec le cryptage SHA-1.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Unified Contact Center Express (UCCX)
- Gestion de certificat

Annonces de Microsoft et de Mozilla

[Mise à jour de la condamnation SHA-1](#)

[Continuation pour éliminer les Certificats SHA-1](#)

Dans ces notices, les fabricants de navigateur ont énoncé que les navigateurs afficheront des avertissements bypassable pour les Certificats SHA-1 produits qui sont délivrés avec des dates de

ValidFrom après le 1er janvier, 2016.

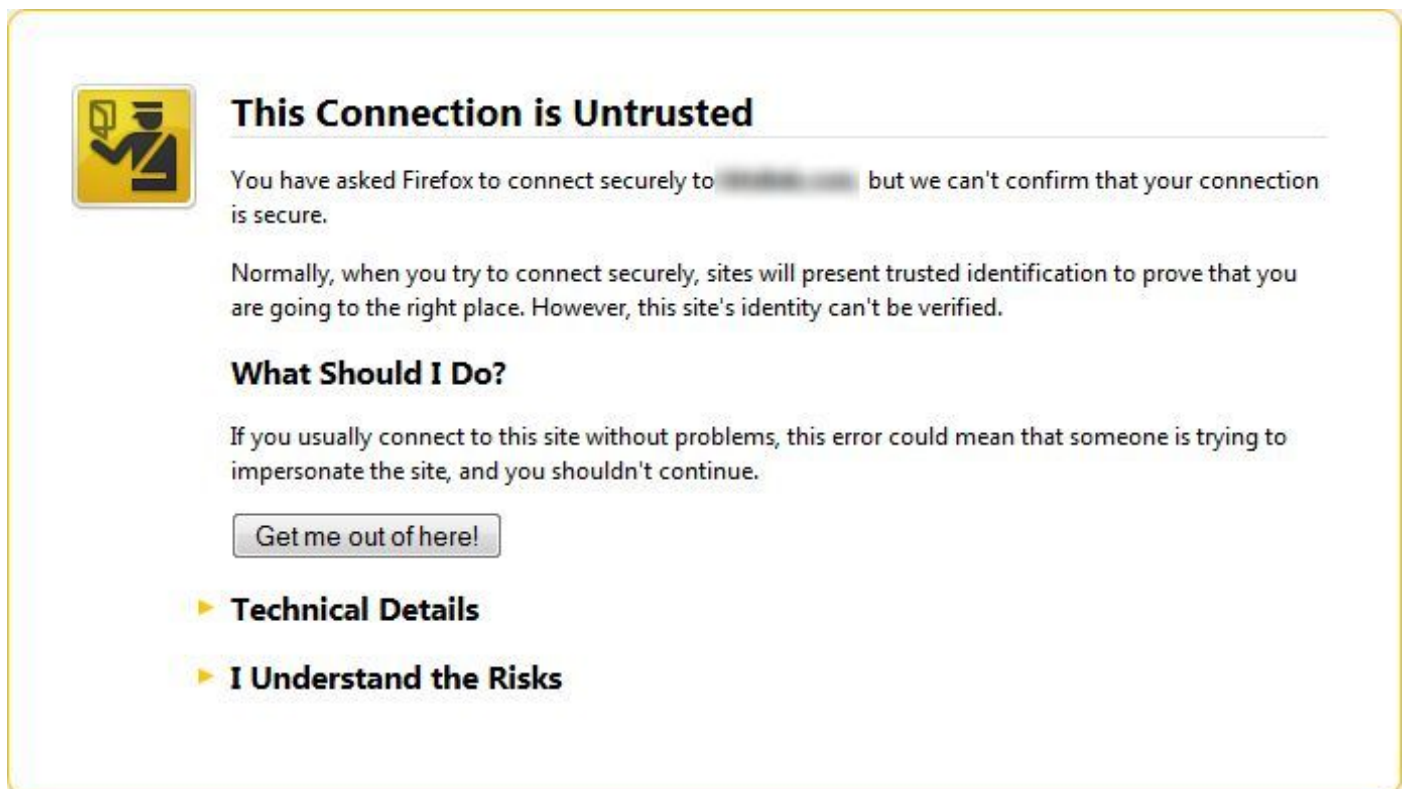
En outre, le plan en cours de l'enregistrement est de bloquer les sites Web qui utilisent les Certificats SHA-1 après le 1er janvier 2017 indépendamment de l'entrée de ValidFrom dans le certificat. Cependant, avec les attaques récentes qui visent les Certificats SHA-1, ces navigateurs pourraient relever cette chronologie et bloquer les sites Web qui utilisent les Certificats SHA-1 après le 1er janvier 2017 indépendamment de la date de parution de certificat.


Cisco informe des clients lire les annonces en détail et rester à jour sur d'autres annonces de Microsoft et Mozilla sur ce thème.

Quelques versions d'UCCX génèrent les Certificats SHA-1. Si vous accédez à des pages Web UCCX protégées par les Certificats SHA-1, elles pourraient générer un avertissement ou être bloquées selon les dates et les règles remarquables précédemment.

Expérience utilisateur

Quand un certificat SHA-1 est détecté, dépendant sur la date de ValidFrom et les règles précédemment énumérées, l'utilisateur pourrait voir un message semblable à ceci :



 **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.

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

La personne à charge sur les décisions prises, un utilisateur pourrait ou ne pourrait pas pouvoir sauter cet avertissement.

Considérations UCCX

Ces tables décrivent des stratégies d'incidence et de réduction du certificat SHA-1 pour chaque version d'UCCX actuellement sous la maintenance logicielle.

Notations utilisées dans ce document

Notation



Déjà pris en charge. Aucune autre action requise.



Le support est disponible, mais la régénération des Certificats est nécessaire.



Le support n'est pas disponible.

Description













UCCX 11.5

| | Gestion UCCX | Gestion CUIC Données vivantes # | Appareil de bureau de gestion de finesse # | Email et conversation d'agent avec SocialMiner* | Étapes de script de REPOS UCCX | Enregistrement avec MediaSense* 11.5 |
|----------------------------------|---|---|--|---|---|--|
| Frais installez | | | | | | |
| Mise à jour de version préalable | Les Certificats UCCX retiennent l'algorithme des releases plus anciennes. Si généré avec une clé SHA-11 dans des releases plus anciennes, les Certificats auto-signés sont SHA-1 basés et doivent être régénérés. | Les Certificats du centre d'intelligence UCCX Cisco Unified (CUIC) retiennent l'algorithme des releases plus anciennes. Si généré avec une clé SHA-11 dans des releases plus anciennes, les Certificats auto-signés sont SHA-1 basés et doivent être régénérés. | Les Certificats de finesse UCCX retiennent l'algorithme des releases plus anciennes. Si généré avec une clé SHA-11 dans des releases plus anciennes, les Certificats auto-signés sont SHA-1 basés et doivent être régénérés. | Les Certificats de SocialMiner et UCCX retiennent l'algorithme des releases plus anciennes. Si généré avec une clé SHA-11 dans des releases plus anciennes, les Certificats auto-signés sont SHA-1 basés et doivent être régénérés. | UCCX ne rejettera pas un web server distant qui utilise les Certificats SHA-1 en tant qu'élément de la transmission figurative de transfert d'état (REPOS). Les étapes de REPOS fonctionneront après que les Certificats soient régénérés sur l'UCCX. | Les Certificats de MediaSense et UCCX retiennent l'algorithme des releases plus anciennes. Si généré avec une clé SHA-11 dans des releases plus anciennes, les Certificats auto-signés sont SHA-1 basés et doivent être régénérés. |

Remarque: le *The a régénéré MediaSense et des certificats de SocialMiner doivent être réimportés dans UCCX.

Remarque: les actions distinctes de #No sont nécessaires pour la finesse et le CUIC. Les Certificats sont régénérés seulement une fois à la page de gestion de plate-forme UCCX.

UCCX 11.0(1)







| | Gestion UCCX | Données vivantes de gestion CUIC # | Appareil de bureau de gestion de finesse # | Email et conversation d'agent avec SocialMiner ** | Étapes de script de REPOS UCCX | Enregistrement avec MediaSense ** 11.0* et 10.5* |
|---|--|---|---|--|--|---|
| Frais installés | <p> Par défaut tous les frais auto-signés installent des Certificats sont les Certificats SHA-1 et doivent être régénérés.</p> | <p> Par défaut tous les frais auto-signés installent des Certificats sont les Certificats SHA-1 et doivent être régénérés.</p> | <p> Par défaut tous les frais auto-signés installent des Certificats sont les Certificats SHA-1 et doivent être régénérés.</p> | <p> Par défaut tous les frais auto-signés installent des Certificats sont les Certificats SHA-1 et doivent être régénérés.</p> | <p> UCCX ne rejettera pas un web server distant qui utilise les Certificats SHA-1 en tant qu'élément de la transmission de REPOS. Les étapes de REPOS fonctionneront après que les Certificats soient régénérés sur l'UCCX.</p> | <p> Le certificat auto-signé par par défaut est SHA-1. Le certificat de régénération ne fournit pas une option pour SHA-256.</p> |
| Mise à jour de version préalable | <p> Les Certificats UCCX retiennent l'algorithme des releases plus anciennes. Si généré avec une clé SHA-11 dans des releases plus anciennes, les Certificats auto-signés sont SHA-1 basés et doivent être régénérés.</p> | <p> Les Certificats UCCX CUIC retiennent l'algorithme des releases plus anciennes. Si généré avec une clé SHA-11 dans des releases plus anciennes, les Certificats auto-signés sont SHA-1 basés et doivent être régénérés.</p> | <p> Les Certificats de finesse UCCX retiennent l'algorithme des releases plus anciennes. Si généré avec une clé SHA-11 dans des releases plus anciennes, les Certificats auto-signés sont SHA-1 basés et doivent être régénérés.</p> | <p> Les Certificats de SocialMiner et UCCX retiennent l'algorithme des releases plus anciennes. Si généré avec une clé SHA-11 dans des releases plus anciennes, les Certificats auto-signés sont SHA-1 basés et doivent être régénérés.</p> | <p> UCCX ne rejettera pas un web server distant qui utilise les Certificats SHA-1 en tant qu'élément de la transmission de REPOS. Les étapes de REPOS fonctionneront après que les Certificats soient régénérés sur l'UCCX.</p> | <p> Le certificat auto-signé par par défaut est SHA-1. Le certificat de régénération ne fournit pas une option pour SHA-256.</p> |

Remarque: L'offre spéciale d'ingénierie de *An (es) sera libérée afin de permettre à MediaSense 10.5 et 11.0 pour générer et recevoir les Certificats SHA-256.

Remarque: ** Les certificats régénérés de MediaSense et de SocialMiner doivent être réimportés dans UCCX.

Remarque: les actions distinctes de #No sont nécessaires pour la finesse et le CUIC. Les Certificats sont régénérés seulement une fois à la page de gestion de plate-forme UCCX.

UCCX 10.5 et 10.6

| | Gestion UCCX | Données vivantes de gestion CUIC # | Appareil de bureau de gestion de finesse # | Email et conversation d'agent avec SocialMiner* | Étapes de script de REPOS UCCX | Enregistrement avec le *** de MediaSense 10.0**/10.5** |
|---|---|---|---|--|--|---|
| Frais installés | <p> Par défaut tous les frais auto-signés installent des Certificats SHA-1 et doivent être régénérés.</p> | <p> Par défaut tous les frais auto-signés installent des Certificats SHA-1 et doivent être régénérés.</p> | <p> Par défaut tous les frais auto-signés installent des Certificats SHA-1 et doivent être régénérés.</p> | <p> Le soutien SHA-256 de l'email d'agent et la conversation sont disponibles seulement dans SocialMiner (SM) v11 et SM v11 n'est pas compatible avec UCCX v10.x.</p> | <p> UCCX ne rejettera pas un web server distant qui utilise les Certificats SHA-1 en tant qu'élément de la transmission de REPOS. Les étapes de REPOS fonctionneront après que les Certificats soient régénérés sur l'UCCX.</p> | <p> Le certificat auto-signé par défaut est SHA-1. Le certificat de régénération ne fournit pas une option pour SHA-256.</p> |
| Mise à jour de version préalable | <p> Les Certificats retiennent l'algorithme des releases plus anciennes. Si généré avec une clé SHA-11 dans des releases plus anciennes, les Certificats auto-signés sont SHA-1 basés et doivent être régénérés.</p> | <p> Les Certificats retiennent l'algorithme des releases plus anciennes. Si généré avec une clé SHA-11 dans des releases plus anciennes, les Certificats auto-signés sont SHA-1 basés et doivent être régénérés.</p> | <p> Les Certificats retiennent l'algorithme des releases plus anciennes. Si généré avec une clé SHA-11 dans des releases plus anciennes, les Certificats auto-signés sont SHA-1 basés et doivent être régénérés.</p> | <p> Le soutien SHA-256 de l'email d'agent et la conversation sont disponibles seulement dans le SM v11 et le SM v11 n'est pas compatible avec UCCX v10.x.</p> | <p> UCCX ne rejettera pas un web server distant qui utilise les Certificats SHA-1 en tant qu'élément de la transmission de REPOS. Les étapes de REPOS fonctionneront après que les Certificats soient régénérés sur l'UCCX.</p> | <p> Le certificat auto-signé par défaut est SHA-1. Le certificat de régénération ne fournit pas une option pour SHA-256.</p> |













Remarque: L'offre spéciale d'ingénierie de *An sera libérée afin de permettre à SocialMiner 10.6 pour générer et recevoir les Certificats SHA-256.

Remarque: ** Une offre spéciale d'ingénierie (es) sera libérée afin de permettre à MediaSense 10.0 et 10.5 pour générer et recevoir les Certificats SHA-256.

Remarque: Le *** les certificats régénérés de MediaSense et de SocialMiner doit être réimporté dans UCCX.

Remarque: les actions distinctes de #No sont nécessaires pour la finesse et le CUIC. Les Certificats sont régénérés seulement une fois à la page de gestion de plate-forme UCCX.

UCCX 10.0

| | Gestion UCCX ** | Données vivantes de gestion CUIC # | Appareil de bureau de gestion de finesse # | Conversation d'agent avec SocialMiner* | Étapes de script de REPOS UCCX | Enregistrement avec le *** 10.0** de MediaSense |
|---|---|---|---|---|--|---|
| Frais installés |  Le certificat auto-signé par défaut est SHA-1. Le certificat de régénération ne fournit pas une option pour SHA-256. |  Le certificat auto-signé par défaut est SHA-1. Le certificat de régénération ne fournit pas une option pour SHA-256. |  Le certificat auto-signé par défaut est SHA-1. Le certificat de régénération ne fournit pas une option pour SHA-256. |  Le soutien SHA-256 de l'agent que la conversation est disponible seulement dans le SM v11 et le SM v11 n'est pas compatible avec UCCX v10.x. |  UCCX ne rejettera pas un web server distant qui utilise les Certificats SHA-1 en tant qu'élément de la transmission de REPOS. Les étapes de REPOS fonctionneront après que les Certificats soient régénérés sur l'UCCX. |  Le certificat auto-signé par défaut est SHA-1. Le certificat de régénération ne fournit pas une option pour SHA-256. |
| Mise à jour de version préalable |  Le certificat auto-signé par défaut est SHA-1. Le certificat de régénération ne fournit pas une option pour |  Le certificat auto-signé par défaut est SHA-1. Le certificat de régénération ne fournit pas une option pour |  Le certificat auto-signé par défaut est SHA-1. Le certificat de régénération ne fournit pas une option pour |  Le soutien SHA-256 de l'agent que la conversation est disponible seulement dans le SM v11 et le SM v11 n'est pas |  UCCX ne rejettera pas un web server distant qui utilise les Certificats SHA-1 en tant qu'élément de la transmission de REPOS. |  Le certificat auto-signé par défaut est SHA-1. Le certificat de régénération ne fournit pas une option pour SHA-256. |

SHA-256. SHA-256. SHA-256. compatible
avec UCCX
v10.x. Les étapes de
REPOS
fonctionneront
après que les
Certificats
soient
régénérés sur
l'UCCX.

Remarque: L'offre spéciale d'ingénierie de *An sera libérée afin de permettre à SocialMiner 10.6 pour générer et recevoir les Certificats SHA-256.

Remarque: ** Une offre spéciale d'ingénierie (es) sera libérée afin de permettre à MediaSense 10.0 pour générer et recevoir les Certificats SHA-256.

Remarque: Le *** les certificats régénérés de MediaSense et de SocialMiner doit être réimporté dans UCCX.

Remarque: les actions distinctes de #No sont nécessaires pour la finesse et le CUIC. Les Certificats sont régénérés seulement une fois à la page de gestion de plate-forme UCCX.

Instructions de Gestion de certificat

Il y a trois types de Certificats qui doivent être vérifiés et potentiellement régénérés :

- Certificats signés d'individu
- Certificats racine de confiance
- Certificats signés de tiers

Certificats Auto-signés

Naviguez vers la page de gestion de SYSTÈME D'EXPLOITATION. Choisissez la **Sécurité >** naviguent vers la **Gestion de certificat**. Cliquez sur **Find**.

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 |

Notez les quatre catégories de certificat :

- ipsec
- ipsec-confiance
- chat
- Tomcat-confiance

Les Certificats sous le **chat** et le type de catégorie **Auto-signés** sont ceux qui exigent la régénération. Dans l'image précédente, le troisième certificat est celui qui exige la régénération.

Terminez-vous ces étapes afin de régénérer des Certificats :

Étape 1. Cliquez sur le nom commun du certificat.

Étape 2. De la fenêtre contextuelle, **régénéré de clic**.

Étape 3. Choisissez l'algorithme de chiffrement de SHA-256.

Pour la version 10.6 UCCX, terminez-vous ces étapes afin de régénérer des Certificats :

Étape 1. Cliquez sur **générent** en fonction **nouveau**.

Étape 2. *Nom* choisi de *certificat* comme **chat**, *longueur principale* en tant que **2048** et *algorithme de hachage* comme **SHA256**.

Étape 3. Le clic **générent nouveau**.

Generate Certificate

Generate New Close

Status

Status: Ready

Generate Certificate

Certificate Name* tomcat

Key Length* 2048

Hash Algorithm* SHA256

Generate New Close

Certificats racine de confiance

Ce sont les Certificats qui sont fournis par la plate-forme. Les signatures basées par SHA-1 pour ces Certificats ne sont pas un problème parce que ces Certificats sont de confiance par les clients de Transport Layer Security (TLS) basés sur leur identité, plutôt que la signature de leurs informations parasites.

Certificats signés de tiers

Des Certificats signés par une autorité de certification de tiers avec l'algorithme SHA-1 doivent être réimportés avec les Certificats SHA-256 signés. Tous les Certificats dans une chaîne de certificat doivent être démissionnés avec SHA-256.

Notes supplémentaires

Les plus défiantes offres spéciales d'ingénierie sont signalées sur [cisco.com](https://www.cisco.com) si disponibles. Examinez les pages produit correspondantes régulièrement pour assurer les téléchargements spéciaux d'ingénierie.

- Pour n'importe quelle assistance sur la régénération de certificat ou les questions associées, ouvrez une valise de Cisco TAC.
- Les clients qui s'exécutent sur des versions 8.x ou 9.x UCCX devraient prévoir d'améliorer aux versions le plus tard prises en charge afin de mettre à jour Cisco et prise en charge du navigateur.