

SHA-256 での UCCX サポート

目次

[概要](#)

[前提条件](#)

[要件](#)

[Microsoft および Mozilla からのお知らせ](#)

[ユーザ エクスペリエンス](#)

[UCCX の考慮事項](#)

[この文書で使用されている表記法](#)

[UCCX 11.5](#)

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

[UCCX 10.5 および 10.6](#)

[UCCX 10.0](#)

[証明書管理手順](#)

[自己署名証明書](#)

[信頼できるルート証明書](#)

[サードパーティの署名証明書](#)

[補足事項](#)

概要

このドキュメントでは、Cisco Unified Contact Center Express (UCCX) の SHA-256 に対するサポートについて説明します。SHA-1 暗号化は間もなく廃止されるため、UCCX のすべてのサポート対象 Web ブラウザは、SHA-1 暗号化を使用した証明書を渡すサーバからの Web ページをブロックするようになります。

前提条件

要件

次の項目に関する知識が推奨されます。

- Cisco Unified Contact Center Express (UCCX)
- 証明書管理

Microsoft および Mozilla からのお知らせ

「[SHA-1 Deprecation Update](#)」

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

ブラウザの開発元によるこれらの告知によれば、2016 年 1 月 1 日以降の ValidFrom 日付で発行された SHA-1 証明書をブラウザが受け取った場合、ブラウザはバイパス可能な警告を表示します

。


また、現時点の計画では、2017年1月1日以降は、証明書の ValidFrom 項目にかかわらず、SHA-1 証明書を使用する Web サイトはブロックされる予定です。ただし、SHA-1 証明書をターゲットにした最近の攻撃を考慮して、ブラウザはこのタイムラインを早め、2017年1月1日以降、証明書の発行日にかかわらず、SHA-1 証明書を使用する Web サイトをブロックする可能性があります。

これらのアナウンスを読んで詳細を把握し、このトピックについて今後 Microsoft および Mozilla から発表される最新の告知を常に確認することをお勧めします。

UCCX の一部のバージョンは SHA-1 証明書を生成します。SHA-1 証明書で保護された UCCX の Web ページにアクセスする場合は、前述の日付とルールに従って、警告が表示されたり、アクセスがブロックされたりする可能性があります。

ユーザ エクスペリエンス

SHA-1 証明書が検出された場合、ValidFrom の日付と前述のルールに従って、次のようなメッセージがユーザに表示される可能性があります。



This Connection is Untrusted

You have asked Firefox to connect securely to ██████████ 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**

この警告をユーザがバイパスできるかどうかは、どのような決定が下されるかによって決まります。

UCCX の考慮事項

次の表に、現在ソフトウェア メンテナンス中の各 UCCX バージョンにおける SHA-1 証明書の影響とそのリスク軽減方法について説明します。

この文書で使用されている表記法

表記法

説明



すでにサポートされています。対応不要です。



サポートされていますが、証明書の再生成が必要です。



サポートされていません。

UCCX 11.5

UCCX Administration

新規インストール



前のバージョンからのアップグレード

UCCX の証明書のアルゴリズムは前のリリースと同じです。 UCCX Cis
前のリリースで SHA-11 キーを使用して生成した自己署名証明書は、SHA-1 ベースであるため、再生成する必要があります。

注: *The は MediaSense を再生し、SocialMiner 証明書は UCCX に再インポートする必要があります。

注: #No 個別行動は Finesse および CUIC のために必要です。証明書は UCCX プラットフォームの管理ページで一度だけ再生成されます。

UCCX 11.0(1)

UCCX Administration

新規インストール

デフォルトでは、新規インストールのすべての自己署名証明書は SHA-1 証明書であるため、再生成が必要です。

前のバージョンからのアップグレード

UCCX の証明書のアルゴリズムは前のリリースと同じです。前のリリースで SHA-11 キーを使用して生成した自己署名証明書は、SHA-1 ベースであるため、再生成する必要があります。

注: *An Engineering Special (ES) は MediaSense 10.5 および 11.0 が SHA-256 証明書を生成し、受け入れるようにリリースされます。

注: ** 再生成された MediaSense および SocialMiner の証明書を UCCX に再インポートする

必要があります。

注: #No 個別行動は Finesse および CUIC のために必要です。証明書は UCCX プラットフォームの管理ページで一度だけ再生成されます。


UCCX 10.5 および 10.6

UCCX Administration

新規インストール

 デフォルトでは、新規インストールのすべての自己署名証明書は SHA-1 証明書であるため、再生成が必要です。

前のバージョンからのアップグレード

 証明書のアルゴリズムは前のリリースと同じです。前のリリースで SHA-11 キーを使用して生成した自己署名証明書は、SHA-1 ベースであるため、再生成する必要があります。

注: 特派員を設計する *An は SHA-256 証明書を生成し、受け入れることを SocialMiner 10.6 割り当てのためにリリースされます。

注: ** MediaSense 10.0 および 10.5 で SHA-256 証明書の生成と受け入れができるように、Engineering Special (ES) がリリースされる予定です。

注: *** 再生成された MediaSense および SocialMiner の証明書を UCCX に再インポートする必要があります。



注: #No 個別行動は Finesse および CUIC のために必要です。証明書は UCCX プラットフォームの管理ページで一度だけ再生成されます。

UCCX 10.0

UCCX Administration**

CUIC Administration Live

新規インストール

 デフォルトの自己署名証明書は SHA-1 です。
 デフォルトの自己署名証明書は SHA-1 です。

証明書の再生成に SHA-256 を使用するオプションはありません。 証明書の再生成に SHA-256 を使用するオプションはありません。

前のバージョンからのアップグレード

デフォルトの自己署名証明書は SHA-1 です。 デフォルトの自己署名証明書は SHA-1 です。
証明書の再生成に SHA-256 を使用するオプションはありません。 証明書の再生成に SHA-256 を使用するオプションはありません。

注: 特派員を設計する *An は SHA-256 証明書を生成し、受け入れることを SocialMiner 10.6 割り当てのためにリリースされます。

注: MediaSense 10.0 が SHA-256 証明書を生成し、受け入れるように** Engineering Special (ES) はリリースされます。

注: *** 再生成された MediaSense および SocialMiner の証明書を UCCX に再インポートする必要があります。

注: #No 個別行動は Finesse および CUIC のために必要です。証明書は UCCX プラットフォームの管理ページで一度だけ再生成されます。

証明書の管理手順

確認が必要で、おそらくは再生成が必要になる証明書は、次の 3 タイプです。

- 自己署名証明書
- 信頼できるルート証明書
- サードパーティの署名証明書

自己署名証明書

OS の管理ページに移動します。 [Security] > [Navigate to Certificate management] の順に選択します。 [Find] をクリックします。

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

証明書には次の4つのカテゴリがあることにご注意ください。

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

再生成が必要になるのは、**tomcat** カテゴリの中の、**自己署名タイプ**の証明書です。上の図では、3番目のものが再生成が必要な証明書です。

証明書を再生成するには、次の手順を実行してください。

ステップ1. 証明書の **Common Name** をクリックして下さい。

呼び出します。ポップアップウィンドウの **[Regenerate]** をクリックします。

ステップ3. **SHA-256** の暗号化アルゴリズムを選択して下さい。

UCCXバージョン10.6に関しては、証明書を再生成するためにこれらのステップを完了して下さい:

ステップ1. **新しい『Generate』** をクリックして下さい。

ステップ2. **2048** として **Tomcat**、**変調長さ**および **SHA256** としてハッシュアルゴリズムとして名前を **『Certificate』** を選択して下さい。

ステップ3. **新しい『Generate』** をクリックして下さい。

Generate Certificate

Generate New Close

Status

Status: Ready

Generate Certificate

Certificate Name* tomcat

Key Length* 2048

Hash Algorithm* SHA256

Generate New Close

信頼できるルート証明書

これらはプラットフォームによって提供される証明書です。これらの証明書に対する SHA-1 ベースの署名は問題ありません。これらの証明書は、ハッシュの署名ではなく ID に基づいて Transport Layer Security (TLS) クライアントから信頼されるからです。

サードパーティの署名証明書

SHA-1 アルゴリズムを使用してサードパーティの認証局によって署名された証明書は、SHA-256 で署名された証明書を再インポートする必要があります。証明書チェーンに含まれるすべての証明書は、SHA-256 を使用して再署名される必要があります。

追加情報

最新のエンジニアリング スペシャルは [cisco.com](https://www.cisco.com) で利用可能な場合掲示されます。エンジニアリング特別なダウンロードがあるように対応するプロダクトページを定期的に確認して下さい。

- 証明書の再生成およびこれに関連する問題のサポートが必要な場合、Cisco TAC でケースをオープンできます。
- UCCX バージョン 8.x または 9.x を実行しているお客様は、シスコとブラウザのサポートを受け続けるため、サポートされている最新リリースへのアップグレードをご検討ください。