UCCX のための SHA-256 サポート

目次

概要

この資料は Cisco Unified Contact Center Express（UCCX）の SHA-256 サポートを記述したものです。 SHA-1 暗号化はやがて非難され、UCCX のためのすべてのサポートされた Webブラウザは SHA-1 暗号化を用いる証明書を提示するサーバからの Webページをブロックし始めます。

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）
- 証明書の管理

Microsoft および Mozilla からのお知らせ

SHA-1 非推奨アップデート

SHA-1 証明書を停止し続けること

これらの注意では、ブラウザ 製造業者はブラウザが見つけられた **ValidFrom** においての日付 2016 年 1月 1 日の後の発行される SHA-1 証明書のための bypassable 警告を示すことを示しました。

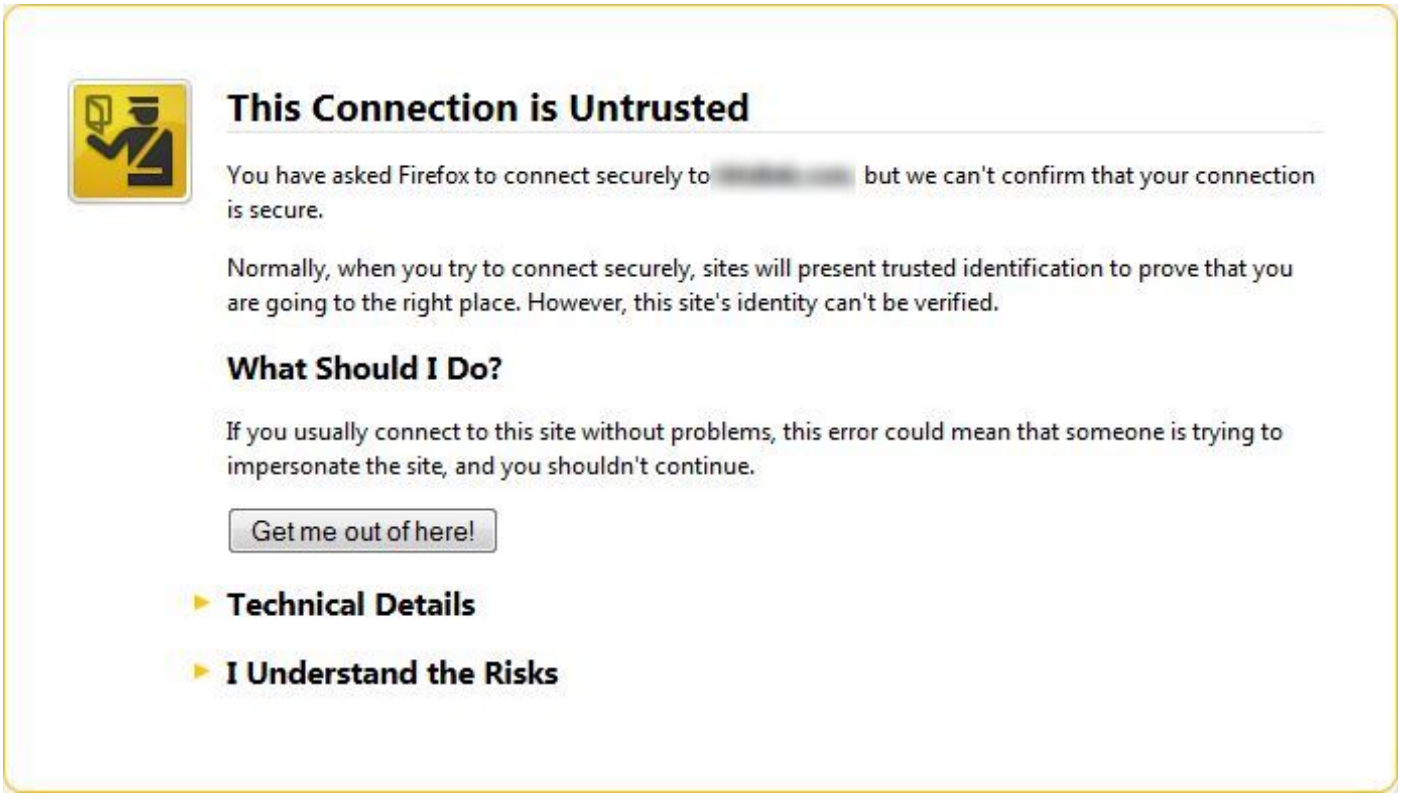
さらに、レコードの現在の計画は証明書で ValidFrom エントリに関係なく 2017 年 1月 1 日の後で SHA-1 証明書を使用する Webサイトをブロックすることです。 ただし、SHA-1 証明書を目標とする最近の不正侵入と、これらのブラウザはこのスケジュールを移動し、証明書問題日付に関係なく 2017 年 1月 1 日の後で SHA-1 証明書を使用する Webサイトをブロックするかもしれません。

Cisco は顧客に発表を詳しく読み、Microsoft からのそれ以上の発表およびこのトピックに Mozilla に最新にとどまるように助言します。

UCCX 生成する SHA-1 証明書のバージョン。 SHA-1 証明書によって保護される UCCX Webページにアクセスする場合警告を生成するか、または以前に注意される日付およびルールに従ってブロックされるかもしれません。

ユーザ エクスペリエンス

SHA-1 証明書が検出されるとき、ユーザはこれと同じようなメッセージを見るかもしれません ValidFrom 日付および以前にリストされたルールに依存した:



なされるこの警告をバイパスできないデシジョンに依存はユーザかもしれませんし、かもしれません。

UCCX 考慮事項

これらの表はソフトウェアメンテナンスの下で UCCX の各バージョンのための SHA-1 証明書影響および軽減戦略を現在記述します。

この資料で使用される表示法

表記	説明
	既にサポートされる。 必要なそれ以上の操作無し。



サポートは利用できますが、証明書の再生は必要です。

サポートは利用できません。

UCCX 11.5

	UCCX 管理	
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 証明書はより古いリリースからのアルゴリズムを保ちます。 より古いリリースの SHA-11 キーによって生成された場合、自己署名証明書は基づく SHA-1、再生する必要があります。	UCC より

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。 証明書は一度だけ UCCX プラットフォーム 管理 ページで再生します。

UCCX 11.0(1)

	UCCX 管理	
新規インストール	 デフォルトですべての自己署名新しいインストール証明書は SHA-1 証明書で、再生する必要があります。	デフ
前のバージョンからのアップグレード	 UCCX 証明書はより古いリリースからのアルゴリズムを保ちます。 より古いリリースの SHA-11 キーによって生成された場合、自己署名証明書は基づく SHA-1、再生する必要があります。	UCC より 、自

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: **再生された MediaSense および 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。 証明書は一度だけ UCCX プラットフォーム 管理 ページで再生します。

UCCX 10.5 および 10.6

	UCCX 管理	
新規インストール	デフォルトですべての自己署名新しいインストール証明書は デフ SHA-1 証明書で、再生する必要があります。	
前のバージョンからのアップグレード	証明書はより古いリリースからのアルゴリズムを保ちます。 より古いリリースの SHA-11 キーによって生成された場合 、自己署名証明書は基づく SHA-1、再生する必要があります。	証明 より 、自

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 割り当てるためにリリースされます。

注: MediaSense 10.0 および 10.5 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: ***は UCCX に再生された MediaSense および SocialMiner 証明書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。 証明書は一度だけ UCCX プラットフォーム 管理 ページで再生します。

UCCX 10.0

	UCCX 管理**	CUIC 管理ライブ データ#	
新規インストール	デフォルト自己署名証明書は SHA-1 です。 再生証明書は SHA-256 にオプ ションを提供しません。	デフォルト自己署名証明書は SHA-1 です。 再生証明書は SHA-256 にオプ ションを提供しません。	
前のバージョンからのアップグレード	デフォルト自己署名証明書は	デフォルト自己署名証明書は	

	SHA-1 です。 再生証明書は SHA-256 にオプションを提供しません。	SHA-1 です。 再生証明書は SHA-256 にオプションを提供しません。

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 割り当てる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: ***は UCCX に再生された MediaSense および SocialMiner 証明書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。 証明書は一度だけ UCCX プラットフォーム 管理 ページで再生します。

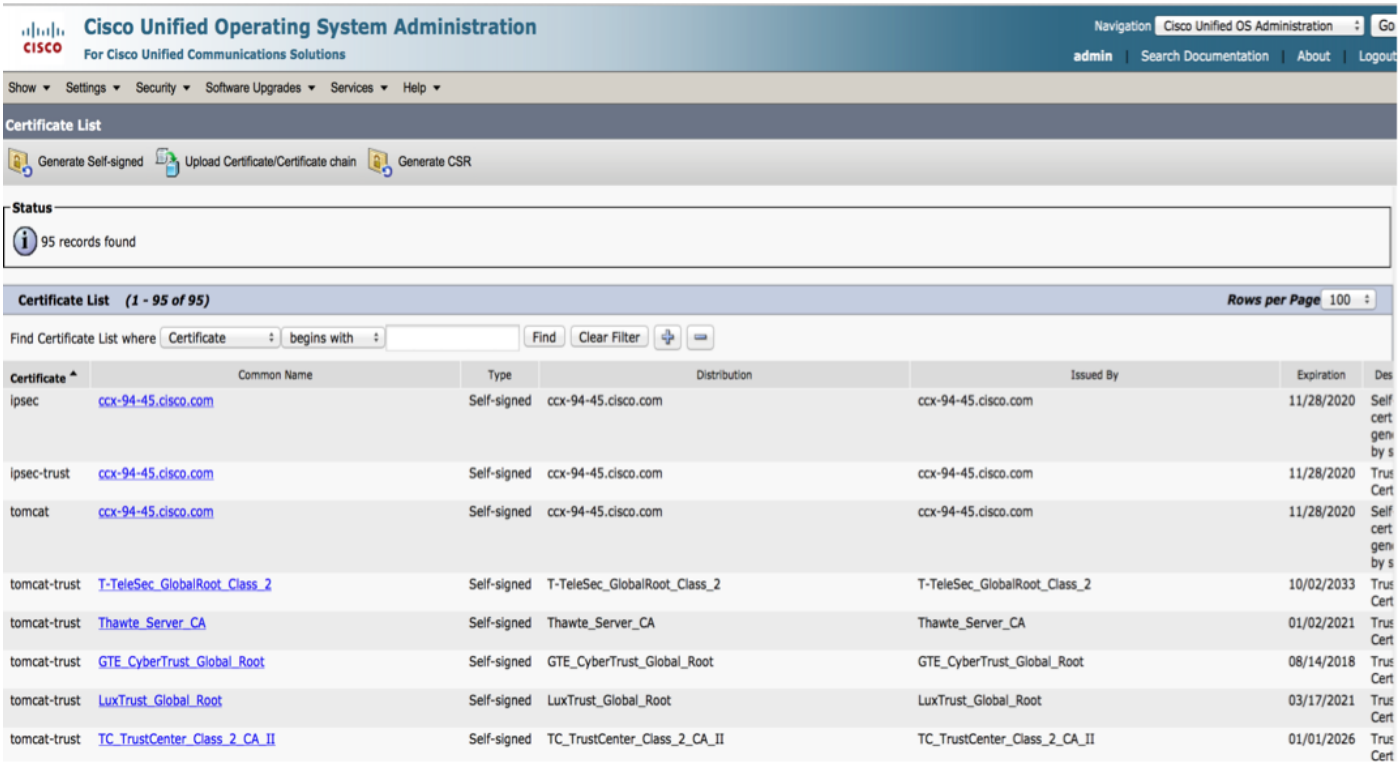
証明書管理指示

確認され、可能性としては再生する必要がある 3 つのタイプには証明書があります:

- 自己 署名入り認証
- 信頼されたルート 証明書
- サード パーティ 署名入り認証

自己署名証明書

OS 管理 ページにナビゲートして下さい。 『Security』 を選択 して下さい **> 証明書管理にナビゲートして下さい**。 [Find] をクリックします。



4 つの証明書 カテゴリーに注意して下さい:

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

自己署名カテゴリ **Tomcat** およびタイプの下の証明書は再生を必要とする物です。 前のイメージでは、第 3 証明書は再生を必要とするものです。

証明書を再生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.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 ウィンドウから、**再生を**クリックして下さい。

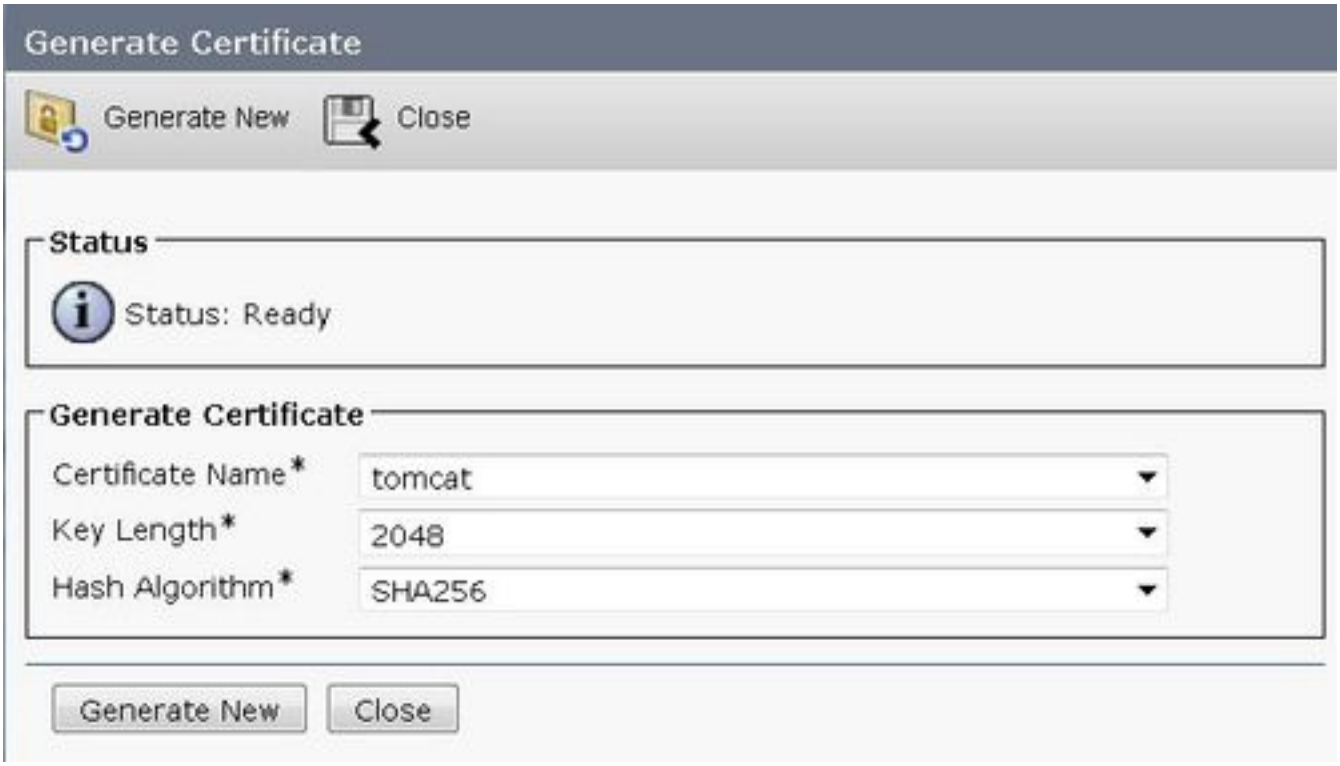
ステップ 3. SHA-256 の暗号化アルゴリズムを選択して下さい。

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。



信頼されたルート 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。 これらの証明書のための SHA-1 によって基づくシグニチャはハッシュのシグニチャよりもむしろこれらの証明書がアイデンティティに基づいて Transport Layer Security （ TLS ）クライアントによって信頼されるので問題ではないです。

サード パーティ 署名入り認証

SHA-256 署名入り認証と再インポートされる SHA-1 アルゴリズム必要性のサード パーティが認証局（ CA ）署名する証明書。 証明書 チェーンのすべての証明書は SHA-256 と辞職する必要があります。

追加情報

最新のエンジニアリング スペシャルは cisco.com 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した製品ページを規則的に確認して下さい。

- 証明書再生または関連する問題のあらゆる支援に関しては、Cisco TAC ケースをオープンして下さい。
- UCCX バージョン 8.x または 9.x で動作する顧客は Cisco およびブラウザ サポートを維持するためにサポートされているリリースにアップグレードすることを計画する必要があります。