SHA-256-Unterstützung für UCCX

Inhalt

Einführung

Dieses Dokument beschreibt die SHA-256-Unterstützung für Cisco Unified Contact Center Express (UCCX). Die SHA-1-Verschlüsselung wird bald veraltet sein, und alle unterstützten Webbrowser für UCCX werden Webseiten von Servern blockieren, die Zertifikate mit der SHA-1-Verschlüsselung anbieten.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco Unified Contact Center Express (UCCX)
- Zertifikatsverwaltung

Ankündigungen von Microsoft und Mozilla

[SHA-1-Verfall-Update](#)

[Fortsetzung des Auslaufens von SHA-1-Zertifikaten](#)

In diesen Mitteilungen haben die Browser-Hersteller angegeben, dass die Browser umgehbare Warnungen für SHA-1-Zertifikate anzeigen werden, die mit **ValidFrom-**Daten nach dem 1. Januar

2016 ausgestellt wurden.

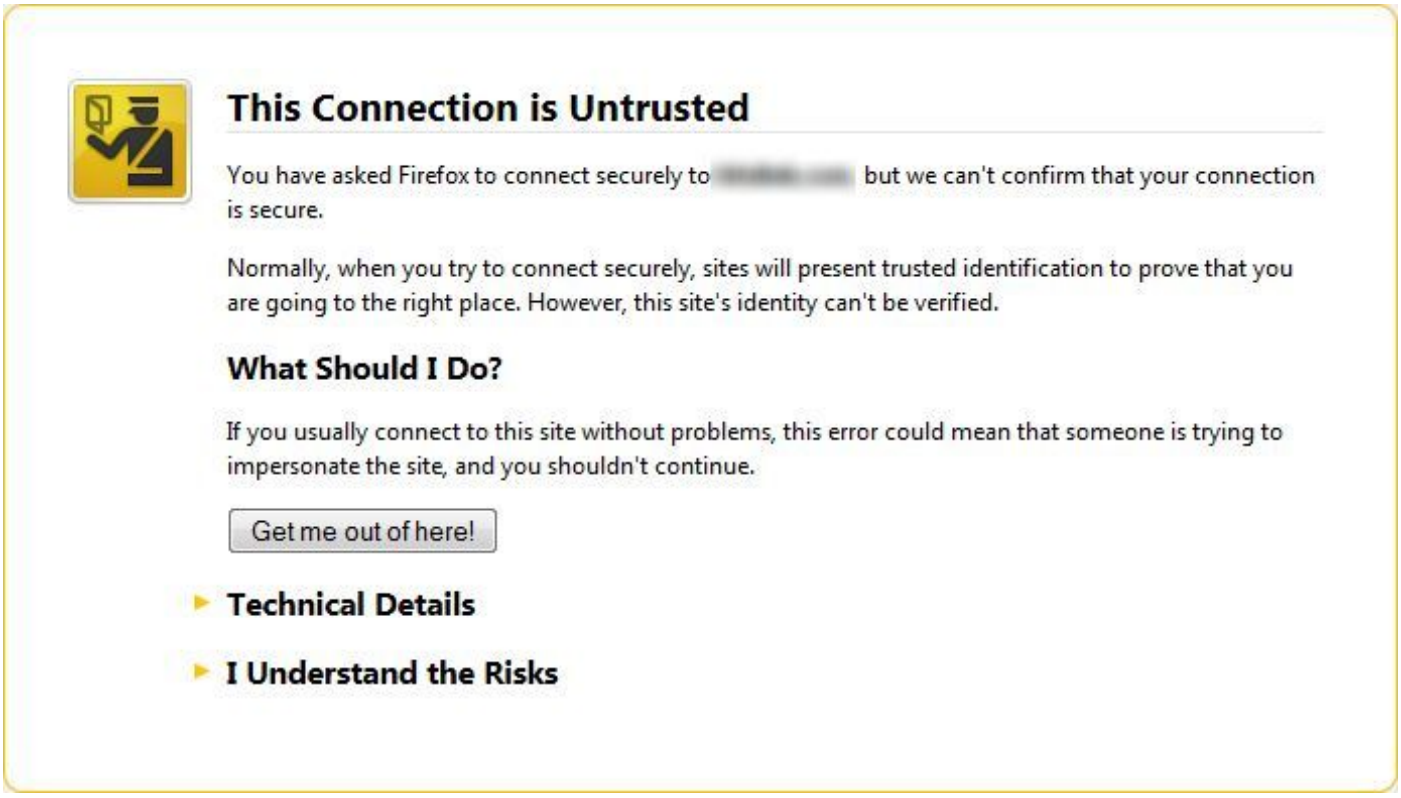
Darüber hinaus besteht der aktuelle Plan der Aufzeichnung darin, Websites zu blockieren, die nach dem 1. Januar 2017 SHA-1-Zertifikate verwenden, unabhängig vom ValidFrom-Eintrag im Zertifikat. Bei jüngsten Angriffen, die auf SHA-1-Zertifikate abzielen, können diese Browser diesen Zeitrahmen jedoch erhöhen und Websites blockieren, die nach dem 1. Januar 2017 SHA-1-Zertifikate verwenden, unabhängig vom Datum der Zertifikatausgabe.

Cisco empfiehlt Kunden, die Ankündigungen ausführlich zu lesen und über weitere Ankündigungen von Microsoft und Mozilla zu diesem Thema auf dem Laufenden zu bleiben.

Einige Versionen von UCCX generieren SHA-1-Zertifikate. Wenn Sie auf UCCX-Webseiten zugreifen, die durch SHA-1-Zertifikate geschützt sind, wird möglicherweise eine Warnung generiert oder gemäß den zuvor angegebenen Daten und Regeln blockiert.

Anwendererlebnis

Wenn ein SHA-1-Zertifikat erkannt wird, wird dem Benutzer je nach dem ValidFrom-Datum und den zuvor aufgeführten Regeln möglicherweise eine Meldung ähnlich der folgenden angezeigt:



Abhängig von den getroffenen Entscheidungen kann ein Benutzer diese Warnung umgehen.

UCCX - Überlegungen

In diesen Tabellen werden die Auswirkungen auf das SHA-1-Zertifikat und die Strategien zur Risikominimierung für jede Version von UCCX beschrieben, die derzeit von der Software verwaltet wird.

In diesem Dokument verwendete Benachrichtigungen

Notation	Beschreibung
✓	Bereits unterstützt. Keine weiteren Maßnahmen erforderlich.
⚠	Unterstützung ist verfügbar, aber die Erneuerung von Zertifikaten ist erforderlich.
−	Support ist nicht verfügbar.

UCCX 11,5

	UCCX-Administration	CUIC-Verwaltung Live-Daten#	Finesse Administration Desktop#	Agent-E-Mail und Chat mit SocialMiner*	UCCX Skript
Neuinstallation	✓	✓	✓	✓	✓
Upgrade von vorheriger Version	⚠ Die UCCX-Zertifikate behalten den Algorithmus älterer Versionen bei. Wenn die Zertifikate in älteren Versionen mit einem SHA-11-Schlüssel generiert werden, basieren die selbstsignierten Zertifikate auf SHA-1 und müssen regeneriert werden.	⚠ Die UCCX Cisco Unified Intelligence Center (CUIC)-Zertifikate behalten den Algorithmus älterer Versionen bei. Wenn die Zertifikate in älteren Versionen mit einem SHA-11-Schlüssel generiert werden, basieren die selbstsignierten Zertifikate auf SHA-1 und müssen regeneriert werden.	⚠ Die UCCX Finesse-Zertifikate behalten den Algorithmus älterer Versionen bei. Wenn die Zertifikate in älteren Versionen mit einem SHA-11-Schlüssel generiert werden, basieren die selbstsignierten Zertifikate auf SHA-1 und müssen regeneriert werden.	⚠ Die Zertifikate SocialMiner **und** UCCX behalten den Algorithmus älterer Versionen bei. Wenn die Zertifikate in älteren Versionen mit einem SHA-11-Schlüssel generiert werden, basieren die selbstsignierten Zertifikate auf SHA-1 und müssen regeneriert werden.	⚠ UCCX le Remote- ab, der Zertifikate REST-Kon (Repres State T verwen REST- funktio nachd Zertifikat UCCX ne wur

Hinweis: * Die generierten MediaSense- und SocialMiner-Zertifikate müssen in UCCX reimportiert werden.

Hinweis: Für Finesse und CUIC sind keine separaten Aktionen erforderlich. Die Zertifikate werden nur einmal auf der Verwaltungsseite für die UCCX-Plattform regeneriert.

UCCX 11.0(1)

	UCCX-Administration	CUIC Administration Live Data#	Finesse Administration Desktop#	Agent-E-Mail und Chat mit SocialMiner**	UCCX Skript

Neuinstallation	⚠ Standardmäßig sind alle selbst signierten Zertifikate für neue Installationen SHA-1-Zertifikate und müssen neu generiert werden.	⚠ Standardmäßig sind alle selbst signierten Zertifikate für neue Installationen SHA-1-Zertifikate und müssen neu generiert werden.	⚠ Standardmäßig sind alle selbst signierten Zertifikate für neue Installationen SHA-1-Zertifikate und müssen neu generiert werden.	⚠ Standardmäßig sind alle selbst signierten Zertifikate für neue Installationen SHA-1-Zertifikate und müssen neu generiert werden.	⚠ UCCX le Remote-V ab, der Zertifikate REST-Kon verwen REST-funktio nachd Zertifikat UCCX ne wur
Upgrade von vorheriger Version	⚠ Die UCCX-Zertifikate behalten den Algorithmus älterer Versionen bei. Wenn die Zertifikate in älteren Versionen mit einem SHA-11-Schlüssel generiert werden, basieren die selbstsignierten Zertifikate auf SHA-1 und müssen regeneriert werden.	⚠ Die UCCX CUIC-Zertifikate behalten den Algorithmus älterer Versionen bei. Wenn die Zertifikate in älteren Versionen mit einem SHA-11-Schlüssel generiert werden, basieren die selbstsignierten Zertifikate auf SHA-1 und müssen regeneriert werden.	⚠ Die UCCX Finesse-Zertifikate behalten den Algorithmus älterer Versionen bei. Wenn die Zertifikate in älteren Versionen mit einem SHA-11-Schlüssel generiert werden, basieren die selbstsignierten Zertifikate auf SHA-1 und müssen regeneriert werden.	⚠ Die Zertifikate SocialMiner **und** UCCX behalten den Algorithmus älterer Versionen bei. Wenn die Zertifikate in älteren Versionen mit einem SHA-11-Schlüssel generiert werden, basieren die selbstsignierten Zertifikate auf SHA-1 und müssen regeneriert werden.	⚠ UCCX le Remote-V ab, der Zertifikate REST-Kon verwen REST-funktio nachd Zertifikat UCCX ne wur

Hinweis: * Eine Engineering-Sonderaktion (ES) wird veröffentlicht, um MediaSense 10.5 und 11.0 das Generieren und Akzeptieren von SHA-256-Zertifikaten zu ermöglichen.

Hinweis: **Die neu generierten MediaSense- und SocialMiner-Zertifikate müssen in UCCX reimportiert werden.

Hinweis: #Für Finesse und CUIC sind keine separaten Aktionen erforderlich. Die Zertifikate werden nur einmal auf der Verwaltungsseite für die UCCX-Plattform regeneriert.

UCCX 10.5 und 10.6

	UCCX-Administration	CUIC Administration Live Data#	Finesse Administration Desktop#	Agent-E-Mail und Chat mit SocialMiner*	U S
Neuinstallation	⚠	⚠	⚠	⛔	

	Standardmäßig sind alle selbst signierten Zertifikate für neue Installationen SHA-1-Zertifikate und müssen neu generiert werden.	Standardmäßig sind alle selbst signierten Zertifikate für neue Installationen SHA-1-Zertifikate und müssen neu generiert werden.	Standardmäßig sind alle selbst signierten Zertifikate für neue Installationen SHA-1-Zertifikate und müssen neu generiert werden.	SHA-256-Unterstützung für E-Mail- und Chat-Agenten ist nur in SocialMiner (SM) v11 verfügbar, und SM v11 ist nicht kompatibel mit UCCX v10.x.	UC Ren al Zerti REST ve R f r Zer UCC
Upgrade von vorheriger Version	Die Zertifikate behalten den Algorithmus älterer Versionen bei. Wenn die Zertifikate in älteren Versionen mit einem SHA-11-Schlüssel generiert werden, basieren die selbstsignierten Zertifikate auf SHA-1 und müssen regeneriert werden.	Die Zertifikate behalten den Algorithmus älterer Versionen bei. Wenn die Zertifikate in älteren Versionen mit einem SHA-11-Schlüssel generiert werden, basieren die selbstsignierten Zertifikate auf SHA-1 und müssen regeneriert werden.	Die Zertifikate behalten den Algorithmus älterer Versionen bei. Wenn die Zertifikate in älteren Versionen mit einem SHA-11-Schlüssel generiert werden, basieren die selbstsignierten Zertifikate auf SHA-1 und müssen regeneriert werden.	SHA-256-Unterstützung für E-Mail- und Chat-Agenten ist nur in SM v11 verfügbar, und SM v11 ist nicht mit UCCX v10.x kompatibel.	UC Ren al Zerti REST ve R f r Zer UCC

Hinweis: * Es wird eine Engineering-Sonderaktion veröffentlicht, die es SocialMiner 10.6 ermöglicht, SHA-256-Zertifikate zu generieren und zu akzeptieren.

Hinweis: **Es wird eine Engineering-Sonderaktion (ES) veröffentlicht, um MediaSense 10.0 und 10.5 das Generieren und Akzeptieren von SHA-256-Zertifikaten zu ermöglichen.

Hinweis: ***Die generierten MediaSense- und SocialMiner-Zertifikate müssen in UCCX reimportiert werden.

Hinweis: #Für Finesse und CUIC sind keine separaten Aktionen erforderlich. Die Zertifikate werden nur einmal auf der Verwaltungsseite für die UCCX-Plattform regeneriert.

UCCX 10.0

	UCCX-Administration**	CUIC Administration Live Data#	Finesse Administration Desktop#	Agent-Chat m SocialMiner*
Neuinstallation				

	Das selbstsignierte Standardzertifikat ist SHA-1. Das Regenerationszertifikat bietet keine Option für SHA-256.	Das selbstsignierte Standardzertifikat ist SHA-1. Das Regenerationszertifikat bietet keine Option für SHA-256.	Das selbstsignierte Standardzertifikat ist SHA-1. Das Regenerationszertifikat bietet keine Option für SHA-256.	SHA-256-Unterstü für Agent-Chat ist SM v11 verfügbar SM v11 ist nicht UCCX v10.x kompatibel.
Upgrade von vorheriger Version	Das selbstsignierte Standardzertifikat ist SHA-1. Das Regenerationszertifikat bietet keine Option für SHA-256.	Das selbstsignierte Standardzertifikat ist SHA-1. Das Regenerationszertifikat bietet keine Option für SHA-256.	Das selbstsignierte Standardzertifikat ist SHA-1. Das Regenerationszertifikat bietet keine Option für SHA-256.	SHA-256-Unterstü für Agent-Chat ist SM v11 verfügbar SM v11 ist nicht UCCX v10.x kompatibel.

Hinweis: * Es wird eine Engineering-Sonderaktion veröffentlicht, die es SocialMiner 10.6 ermöglicht, SHA-256-Zertifikate zu generieren und zu akzeptieren.

Hinweis: **Es wird eine Engineering-Sonderaktion (ES) veröffentlicht, damit MediaSense 10.0 SHA-256-Zertifikate generieren und akzeptieren kann.

Hinweis: ***Die generierten MediaSense- und SocialMiner-Zertifikate müssen in UCCX reimportiert werden.

Hinweis: #Für Finesse und CUIC sind keine separaten Aktionen erforderlich. Die Zertifikate werden nur einmal auf der Verwaltungsseite für die UCCX-Plattform regeneriert.

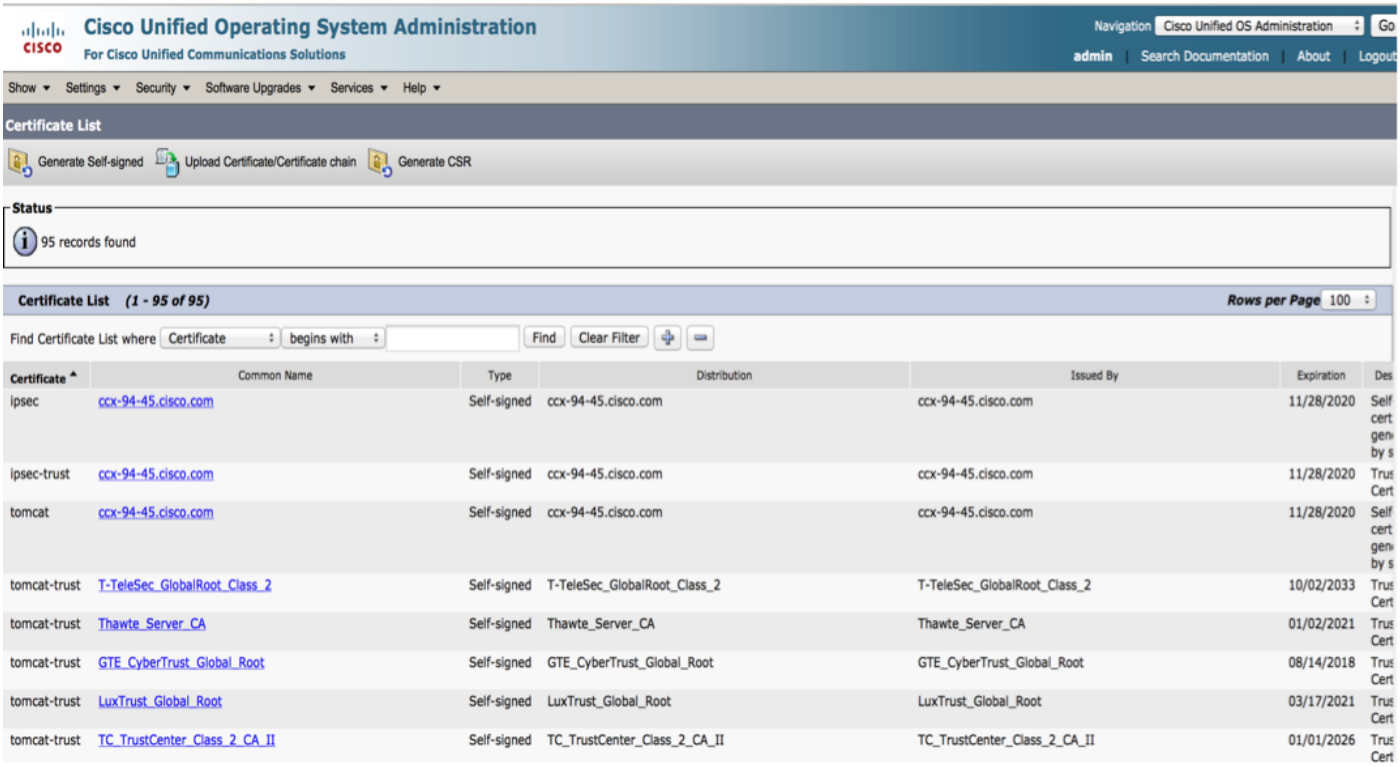
Anweisungen zur Zertifikatsverwaltung

Es gibt drei Arten von Zertifikaten, die überprüft und möglicherweise neu generiert werden müssen:

- Selbst signierte Zertifikate
- Vertrauenswürdige Stammzertifikate
- Von Dritten unterzeichnete Zertifikate

Selbstsignierte Zertifikate

Navigieren Sie zur Seite Betriebssystemverwaltung. Wählen Sie **Sicherheit > Navigieren Sie zu Zertifikatsverwaltung**. Klicken Sie auf **Suchen**.



Beachten Sie die vier Zertifikatskategorien:

- IPS
- ipsec-trust
- Tomate
- tomcat trust

Die Zertifikate unter der Kategorie **tomcat** und type **Self-signed** sind die Zertifikate, die eine Regeneration erfordern. Im vorherigen Bild ist das dritte Zertifikat das Zertifikat, das regeneriert werden muss.

Gehen Sie wie folgt vor, um Zertifikate neu zu generieren:

Schritt 1: Klicken Sie auf den allgemeinen Namen des Zertifikats.

Schritt 2: Klicken Sie im Popup-Fenster auf **Neuerstellen**.

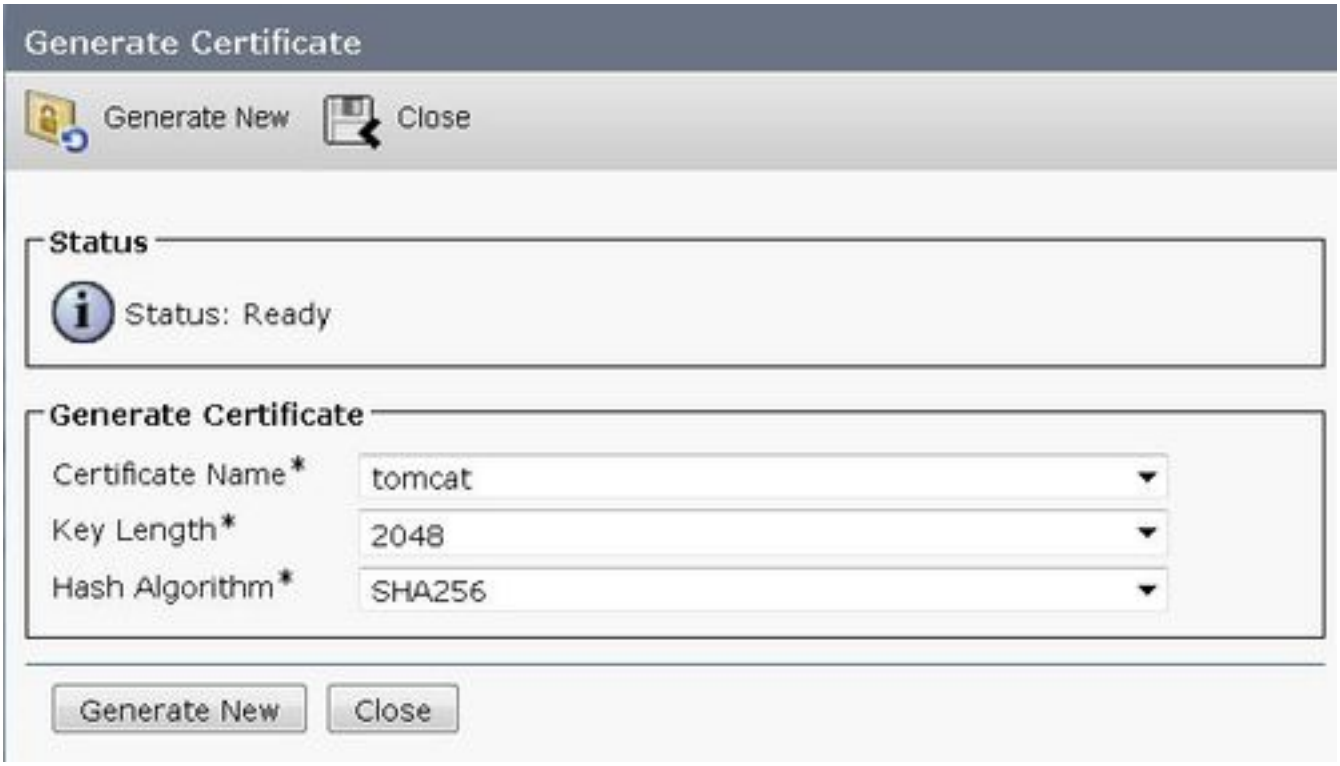
Schritt 3: Wählen Sie den Verschlüsselungsalgorithmus SHA-256 aus.

Führen Sie für UCCX Version 10.6 die folgenden Schritte aus, um Zertifikate neu zu generieren:

Schritt 1: Klicken Sie auf **Neues generieren**.

Schritt 2: Wählen Sie *Zertifikatsname* als **tomcat**, *Schlüssellänge* als **2048** und *Hash-Algorithmus als SHA256 aus.*

Schritt 3: Klicken Sie auf **Neues generieren.**



Vertrauenswürdige Stammzertifikate

Dies sind die Zertifikate, die von der Plattform bereitgestellt werden. SHA-1-basierte Signaturen für diese Zertifikate sind kein Problem, da diese Zertifikate von den TLS-Clients (Transport Layer Security) auf Grundlage ihrer Identität als vertrauenswürdig eingestuft werden und nicht aufgrund der Signatur ihres Hashs.

Von Dritten unterzeichnete Zertifikate

Zertifikate, die von einer Zertifizierungsstelle eines Drittanbieters mit dem SHA-1-Algorithmus signiert wurden, müssen mit SHA-256-signierten Zertifikaten erneut importiert werden. Alle Zertifikate in einer Zertifikatskette müssen mit SHA-256 zurückgesendet werden.

Zusätzliche Hinweise

Die neuesten technischen Sonderaktionen werden, sofern verfügbar, auf cisco.com veröffentlicht. Suchen Sie regelmäßig auf den entsprechenden Produktseiten nach Downloads für die Engineering Special.

- Wenn Sie Hilfe bei der Erneuerung von Zertifikaten oder damit zusammenhängenden Problemen benötigen, erstellen Sie ein Cisco TAC-Ticket.
- Kunden, die UCCX-Versionen 8.x oder 9.x verwenden, sollten ein Upgrade auf die neuesten unterstützten Versionen planen, um die Unterstützung von Cisco und dem Browser aufrechtzuerhalten.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.