Supporto SHA-256 per UCCX

Sommario

Introduzione

Questo documento descrive il supporto SHA-256 per Cisco Unified Contact Center Express (UCCX). La crittografia SHA-1 sarà presto deprecata e tutti i browser Web supportati per UCCX inizieranno a bloccare le pagine Web dai server che offrono certificati con la crittografia SHA-1.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Unified Contact Center Express (UCCX)
- Gestione certificati

Annunci da Microsoft e Mozilla

Aggiornamento deprecazione SHA-1

Continuazione dell'eliminazione graduale dei certificati SHA-1

In questi avvisi, i produttori di browser hanno dichiarato che i browser mostreranno avvisi ignorabili

per i certificati SHA-1 rilevati che sono stati rilasciati con date ValidFrom dopo il 1 gennaio 2016.

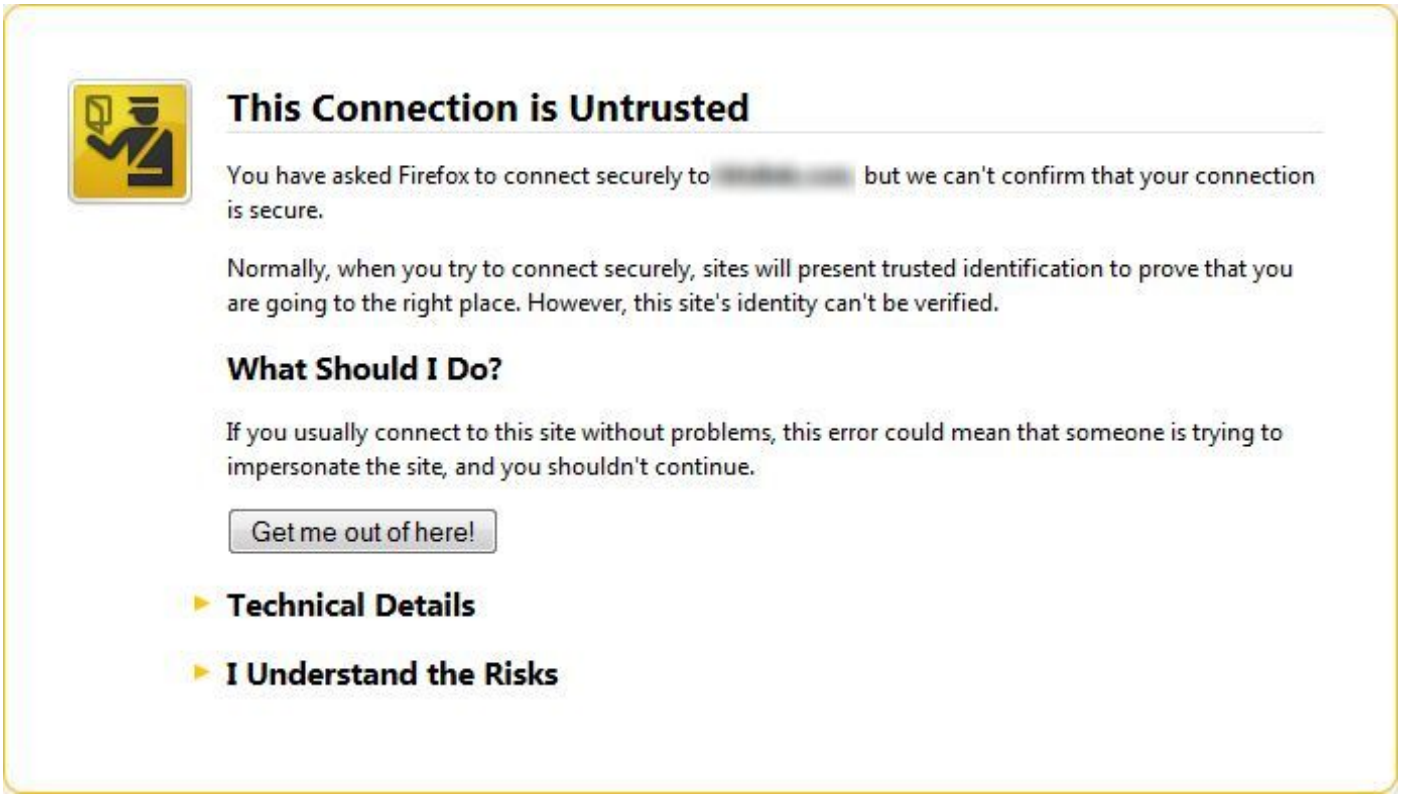
Inoltre, l'attuale piano di registrazione prevede il blocco dei siti Web che utilizzano certificati SHA-1 dopo il 1 gennaio 2017, indipendentemente dalla voce ValidFrom nel certificato. Tuttavia, con gli attacchi recenti che colpiscono i certificati SHA-1, questi browser potrebbero spostarsi verso l'alto e bloccare i siti Web che utilizzano i certificati SHA-1 dopo il 1 gennaio 2017, indipendentemente dalla data di rilascio del certificato.

Cisco consiglia ai clienti di leggere attentamente gli annunci e di tenersi aggiornati su ulteriori annunci di Microsoft e Mozilla su questo argomento.

Alcune versioni di UCCX generano certificati SHA-1. Se si accede a pagine Web UCCX protette da certificati SHA-1, è possibile che generino un avviso o che vengano bloccate in base alle date e alle regole indicate in precedenza.

Esperienza utente

Quando viene rilevato un certificato SHA-1, a seconda della data ValidFrom e delle regole elencate in precedenza, l'utente potrebbe visualizzare un messaggio simile al seguente:

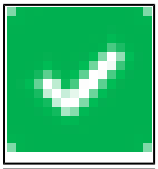
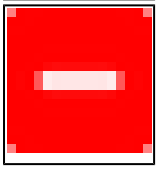


A seconda delle decisioni prese, un utente potrebbe ignorare o meno questo avviso.

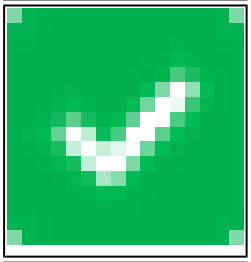
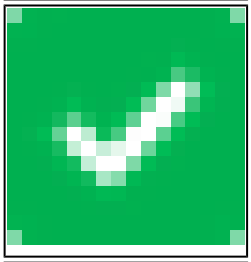
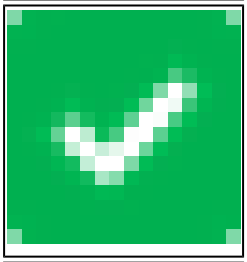
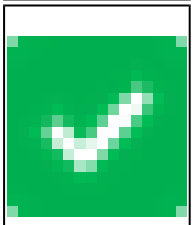
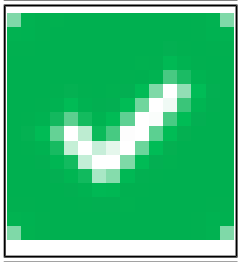
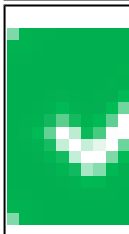
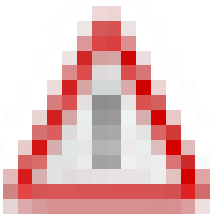
Considerazioni su UCCX

Le tabelle seguenti descrivono l'impatto dei certificati SHA-1 e le strategie di mitigazione per ciascuna versione di UCCX attualmente in manutenzione software.

Notazioni utilizzate nel documento

Notazione	Descrizione
	Già supportato. Non sono necessarie ulteriori azioni.
	Il supporto è disponibile, ma è necessaria la rigenerazione dei certificati.
	Supporto non disponibile.

UCCX 11.5

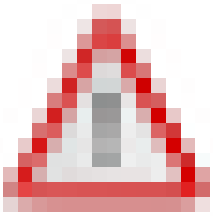
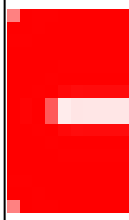
	Amministrazione UCCX	Amministrazione CUIC Live Data#	Desktop di amministrazione Finesse#	E-mail e chat dell'agente con SocialMiner*	Passi di script REST UCCX	Registraz con MediaSe 11.5
Nuova installazione						
Aggiorna da versione precedente	 I certificati UCCX mantengono l'algoritmo delle versioni precedenti.	 I certificati UCCX Cisco Unified Intelligence Center (CUIC) conservano l'algoritmo delle	 I certificati UCCX Finesse mantengono l'algoritmo delle release precedenti.	 I certificati SocialMiner e UCCX mantengono l'algoritmo delle versioni precedenti.	 UCCX non rifiuterà un server Web remoto che utilizza certificati SHA-1 come parte	 I certifi MediaSe e UCC mantenç l'algorit delle ver precede

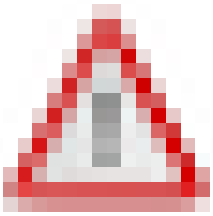
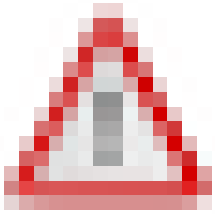
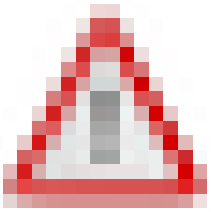
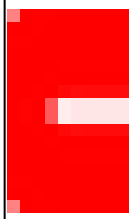
	Se nelle versioni precedenti viene generata una chiave SHA-1, i certificati autofirmati sono basati su SHA-1 e devono essere rigenerati.	versioni precedenti. Se nelle versioni precedenti viene generata una chiave SHA-1, i certificati autofirmati sono basati su SHA-1 e devono essere rigenerati.	Se nelle versioni precedenti viene generata una chiave SHA-1, i certificati autofirmati sono basati su SHA-1 e devono essere rigenerati.	Se nelle versioni precedenti viene generata una chiave SHA-1, i certificati autofirmati sono basati su SHA-1 e devono essere rigenerati.	della comunicazione REST (Representative State Transfer). I passi REST funzioneranno dopo la rigenerazione dei certificati nell'UCCX.	Se ne versio preced viene generata chiave S 1, i certi autofirm sono ba su SHA devon esser rigener

Nota: *I certificati MediaSense e SocialMiner rigenerati devono essere reimportati in UCCX.

Nota: #Non sono necessarie azioni separate per Finesse e CUIC. I certificati vengono rigenerati una sola volta nella pagina di amministrazione della piattaforma UCCX.

UCCX 11.0(1)

	Amministrazione UCCX	Amministrazione CUIC Live Data#	Desktop di amministrazione Finesse#	E-mail e chat dell'agente con SocialMiner**	Passi di script REST UCCX	Registra con MediaSe 11.0* e
Nuova installazione	 Per impostazione predefinita, tutti i certificati di installazione nuovi autofirmati sono certificati SHA-1 e devono essere rigenerati.	 Per impostazione predefinita, tutti i certificati di installazione nuovi autofirmati sono certificati SHA-1 e devono essere rigenerati.	 Per impostazione predefinita, tutti i certificati di installazione nuovi autofirmati sono certificati SHA-1 e devono essere	 Per impostazione predefinita, tutti i certificati di installazione nuovi autofirmati sono certificati SHA-1 e	 UCCX non rifiuterà un server Web remoto che utilizza certificati SHA-1 come parte della comunicazione REST. I passi	 Il certifi autofirm predefi SHA- Il certific rigenera non forn un'opzi per SHA

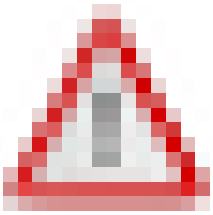
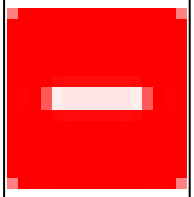
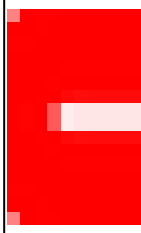
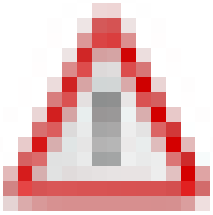
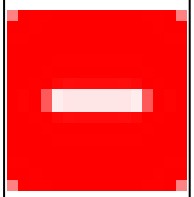
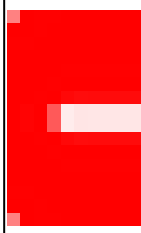
			rigenerati.	devono essere rigenerati.	REST funzioneranno dopo la rigenerazione dei certificati nell'UCCX.	
Aggiorna da versione precedente	 I certificati UCCX mantengono l'algoritmo delle versioni precedenti. Se nelle versioni precedenti viene generata una chiave SHA-1, i certificati autofirmati sono basati su SHA-1 e devono essere rigenerati.	 I certificati UCCX CUIC mantengono l'algoritmo delle release precedenti. Se nelle versioni precedenti viene generata una chiave SHA-1, i certificati autofirmati sono basati su SHA-1 e devono essere rigenerati.	 I certificati UCCX Finesse mantengono l'algoritmo delle release precedenti. Se nelle versioni precedenti viene generata una chiave SHA-1, i certificati autofirmati sono basati su SHA-1 e devono essere rigenerati.	 I certificati SocialMiner e UCCX mantengono l'algoritmo delle versioni precedenti. Se nelle versioni precedenti viene generata una chiave SHA-1, i certificati autofirmati sono basati su SHA-1 e devono essere rigenerati.	 UCCX non rifiuterà un server Web remoto che utilizza certificati SHA-1 come parte della comunicazione REST. I passi REST funzioneranno dopo la rigenerazione dei certificati nell'UCCX.	 Il certifi autofirm predefir SHA- Il certific rigenera non forr un'opzi per SHA

Nota: *Verrà rilasciato un programma speciale di progettazione (ES) per consentire a MediaSense 10.5 e 11.0 di generare e accettare certificati SHA-256.

Nota: **I certificati MediaSense e SocialMiner rigenerati devono essere reimportati in UCCX.

Nota: #Non sono necessarie azioni separate per Finesse e CUIC. I certificati vengono rigenerati una sola volta nella pagina di amministrazione della piattaforma UCCX.

UCCX 10.5 e 10.6

	Amministrazione UCCX	Amministrazione CUIC Live Data#	Desktop di amministrazione Finesse#	E-mail e chat dell'agente con SocialMiner*	Passi di script REST UCCX	Registraz con MediaSer 10.0** / 1
Nuova installazione	 Per impostazione predefinita, tutti i certificati di installazione nuovi autofirmati sono certificati SHA-1 e devono essere rigenerati.	 Per impostazione predefinita, tutti i certificati di installazione nuovi autofirmati sono certificati SHA-1 e devono essere rigenerati.	 Per impostazione predefinita, tutti i certificati di installazione nuovi autofirmati sono certificati SHA-1 e devono essere rigenerati.	 Il supporto SHA-256 per la posta elettronica e la chat degli agenti è disponibile solo in SocialMiner (SM) v11 e SM v11 non è compatibile con UCCX v10.x.	 UCCX non rifiuterà un server Web remoto che utilizza certificati SHA-1 come parte della comunicazione REST. I passi REST funzioneranno dopo la rigenerazione dei certificati nell'UCCX.	 Il certifi autofirm predefin SHA- Il certifica rigeneraz non forn un'opzion SHA-2
Aggiorna da versione precedente	 I certificati mantengono l'algoritmo delle release precedenti. Se nelle versioni	 I certificati mantengono l'algoritmo delle release precedenti. Se nelle versioni	 I certificati mantengono l'algoritmo delle release precedenti. Se nelle	 Il supporto SHA-256 per la posta elettronica e la chat degli agenti è disponibile solo in SM	 UCCX non rifiuterà un server Web remoto che utilizza certificati SHA-1 come parte della	 Il certifi autofirm predefin SHA- Il certifica rigeneraz non forn

	precedenti viene generata una chiave SHA-1, i certificati autofirmati sono basati su SHA-1 e devono essere rigenerati.	precedenti viene generata una chiave SHA-1, i certificati autofirmati sono basati su SHA-1 e devono essere rigenerati.	versioni precedenti viene generata una chiave SHA-1, i certificati autofirmati sono basati su SHA-1 e devono essere rigenerati.	v11 e SM v11 non è compatibile con UCCX v10.x.	comunicazione REST. I passi REST funzioneranno dopo la rigenerazione dei certificati nell'UCCX.	un'opzion SHA-2

Nota: *Verrà rilasciato un programma speciale di progettazione per consentire a SocialMiner 10.6 di generare e accettare certificati SHA-256.

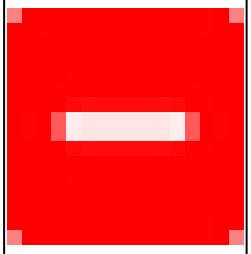
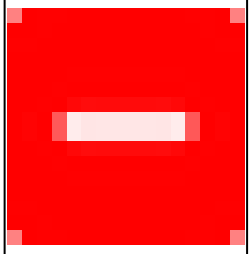
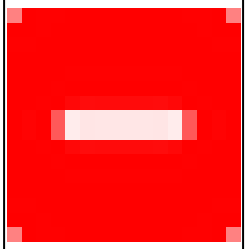
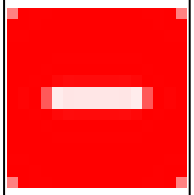
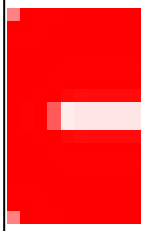
Nota: **Verrà rilasciato un programma speciale di progettazione (ES) per consentire a MediaSense 10.0 e 10.5 di generare e accettare certificati SHA-256.

Nota: ***I certificati MediaSense e SocialMiner rigenerati devono essere reimportati in UCCX.

Nota: #Non sono necessarie azioni separate per Finesse e CUIC. I certificati vengono rigenerati una sola volta nella pagina di amministrazione della piattaforma UCCX.

UCCX 10.0

	Amministrazione UCCX**	Amministrazione CUIC Live Data#	Desktop di amministrazione Finesse#	Chat agente con SocialMiner*	Passi di script REST UCCX	Registraz con MediaSer 10.0*
Nuova installazione	Il certificato autofirmato predefinito è SHA-1.	Il certificato autofirmato predefinito è SHA-1.	Il certificato autofirmato predefinito è SHA-1.	Il supporto SHA-256 per la chat agente è disponibile	UCCX non rifiuterà un server Web remoto che	Il certifi autofirm predefin SHA-

	Il certificato di rigenerazione non fornisce un'opzione per SHA-256.	Il certificato di rigenerazione non fornisce un'opzione per SHA-256.	Il certificato di rigenerazione non fornisce un'opzione per SHA-256.	solo in SM v11 e SM v11 non è compatibile con UCCX v10.x.	utilizza certificati SHA-1 come parte della comunicazione REST. I passi REST funzioneranno dopo la rigenerazione dei certificati nell'UCCX.	Il certifica rigenera non forn un'opzion SHA-2
Aggiorna da versione precedente	 Il certificato autofirmato predefinito è SHA-1. Il certificato di rigenerazione non fornisce un'opzione per SHA-256.	 Il certificato autofirmato predefinito è SHA-1. Il certificato di rigenerazione non fornisce un'opzione per SHA-256.	 Il certificato autofirmato predefinito è SHA-1. Il certificato di rigenerazione non fornisce un'opzione per SHA-256.	 Il supporto SHA-256 per la chat agente è disponibile solo in SM v11 e SM v11 non è compatibile con UCCX v10.x.	 UCCX non rifiuterà un server Web remoto che utilizza certificati SHA-1 come parte della comunicazione REST. I passi REST funzioneranno dopo la rigenerazione dei certificati nell'UCCX.	 Il certifi autofirm predefin SHA- Il certifica rigenera non forn un'opzion SHA-2

Nota: *Verrà rilasciato un programma speciale di progettazione per consentire a SocialMiner 10.6 di generare e accettare certificati SHA-256.

Nota: **Verrà rilasciato un programma speciale di progettazione (ES) per consentire a MediaSense 10.0 di generare e accettare certificati SHA-256.

Nota: ***I certificati MediaSense e SocialMiner rigenerati devono essere reimportati in

UCCX.

Nota: #Non sono necessarie azioni separate per Finesse e CUIC. I certificati vengono rigenerati una sola volta nella pagina di amministrazione della piattaforma UCCX.

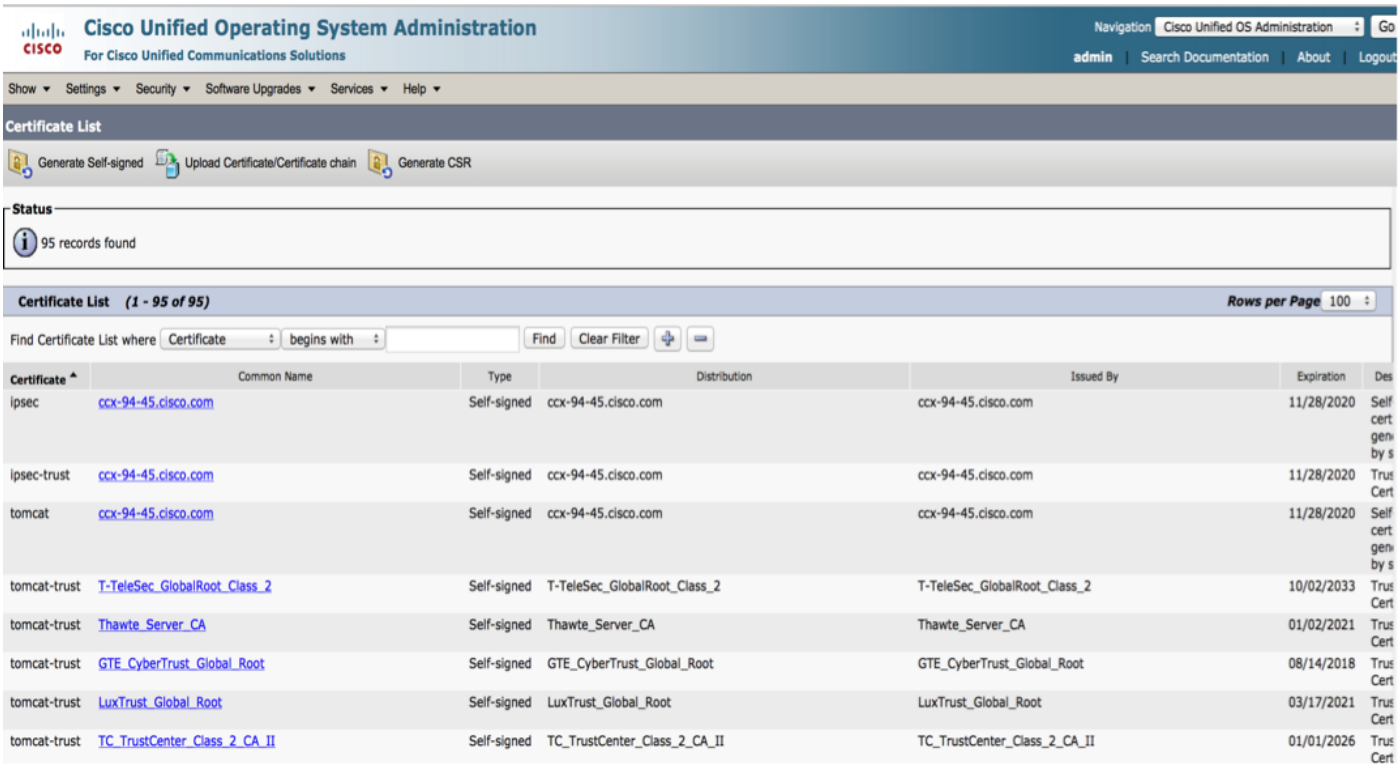
Istruzioni per la gestione dei certificati

È necessario verificare e potenzialmente rigenerare tre tipi di certificati:

- Certificati autofirmati
- Certificati radice attendibili
- Certificati firmati da terze parti

Certificati autofirmati

Passare alla pagina Amministrazione del sistema operativo. Scegliere Protezione > Passa a Gestione certificati. Fare clic su Trova.



Si notino le quattro categorie di certificati:

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

I certificati appartenenti alla categoria tomcat e tipo autofirmato sono quelli che richiedono la rigenerazione. Nell'immagine precedente, il terzo certificato è quello che richiede la rigenerazione.

Per rigenerare i certificati, completare i seguenti passaggi:

Passaggio 1. Fare clic sul nome comune del certificato.

Passaggio 2. Nella finestra popup, fare clic su Rigenera.

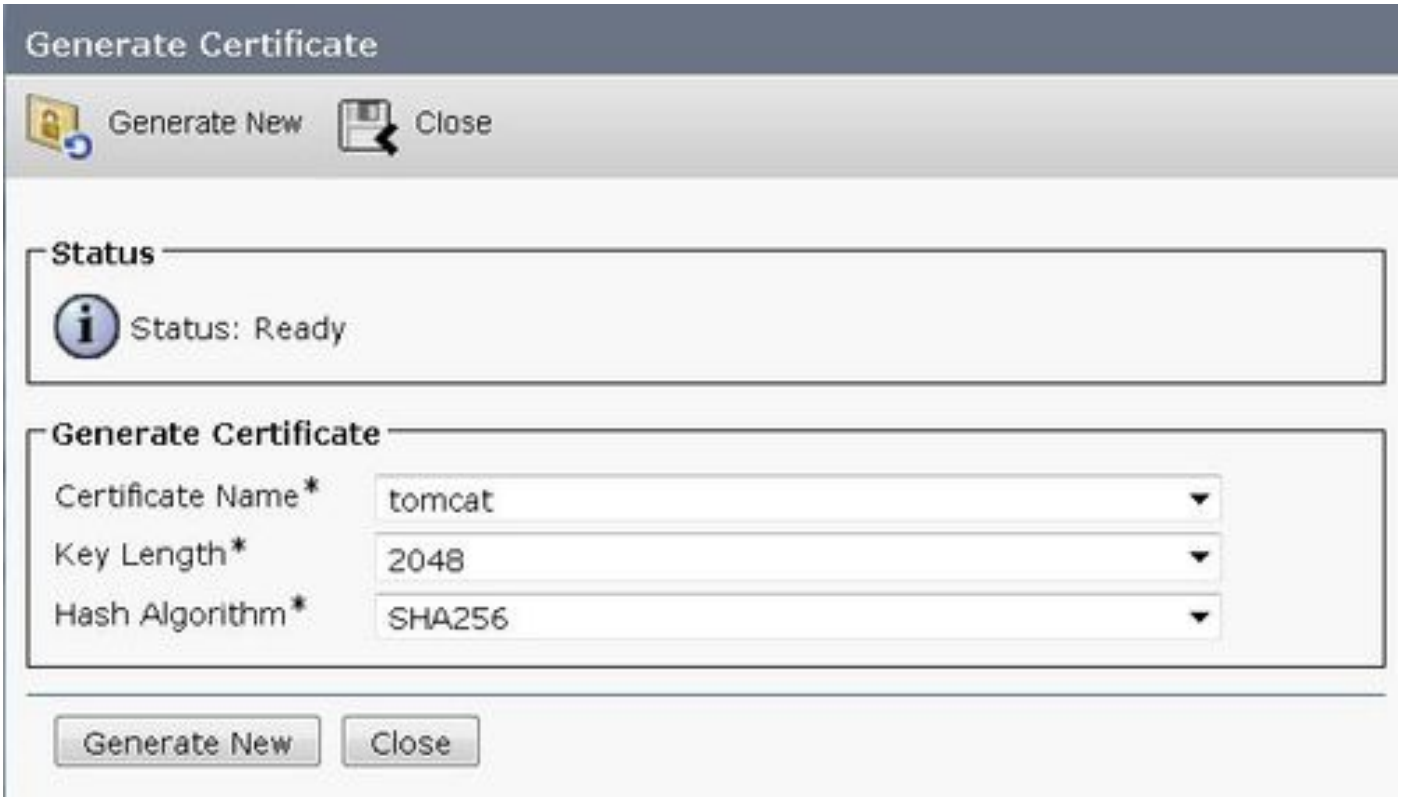
Passaggio 3. Scegliere l'algoritmo di crittografia SHA-256.

Per UCCX versione 10.6, completare i seguenti passaggi per rigenerare i certificati:

Passaggio 1. Fare clic su Generate New.

Passaggio 2. Selezionare Nome certificato come tomcat, Lunghezza chiave come 2048 e Algoritmo hash come SHA256.

Passaggio 3. Fare clic su Genera nuovo.



Certificati radice attendibili

Si tratta dei certificati forniti dalla piattaforma. Le firme basate su SHA-1 per questi certificati non costituiscono un problema perché questi certificati sono considerati attendibili dai client Transport Layer Security (TLS) in base alla loro identità, piuttosto che dalla firma del loro hash.

Certificati firmati da terze parti

I certificati firmati da un'Autorità di certificazione di terze parti con l'algoritmo SHA-1 devono essere reimportati con certificati firmati SHA-256. Tutti i certificati di una catena devono essere rassegnati con SHA-256.

Note aggiuntive

I più recenti Programmi speciali per il settore tecnico sono pubblicati su cisco.com quando disponibili. Consultate regolarmente le pagine dei prodotti corrispondenti per i download del Programma speciale per la progettazione.

- Per assistenza sulla rigenerazione dei certificati o sui problemi associati, aprire una richiesta Cisco TAC.
- I clienti che utilizzano UCCX versioni 8.x o 9.x devono pianificare l'aggiornamento alle ultime versioni supportate per mantenere il supporto di Cisco e del browser.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).