

適用於UCCX的SHA-256支援

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[來自Microsoft和Mozilla的公告](#)

[使用者體驗](#)

[UCCX注意事項](#)

[本文中使用的符號](#)

[UCCX 11.5](#)

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

[UCCX 10.5和10.6](#)

[UCCX 10.0](#)

[證書管理說明](#)

[自簽名證書](#)

[受信任的根證書](#)

[第三方簽名的證書](#)

[附加說明](#)

簡介

本文檔介紹對Cisco Unified Contact Center Express(UCCX)的SHA-256支援。SHA-1加密不久將被棄用，UCCX所有受支援的Web瀏覽器都將開始阻止來自提供SHA-1加密證書的伺服器的網頁。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco Unified Contact Center Express(UCCX)
- 憑證管理

來自Microsoft和Mozilla的公告

[SHA-1 棄用更新](#)

[繼續逐步淘汰 SHA-1 證書](#)

在這些通知中，瀏覽器製造商宣告，瀏覽器將顯示在2016年1月1日之後以ValidFrom日期發佈的SHA-1證書的可繞行警告。

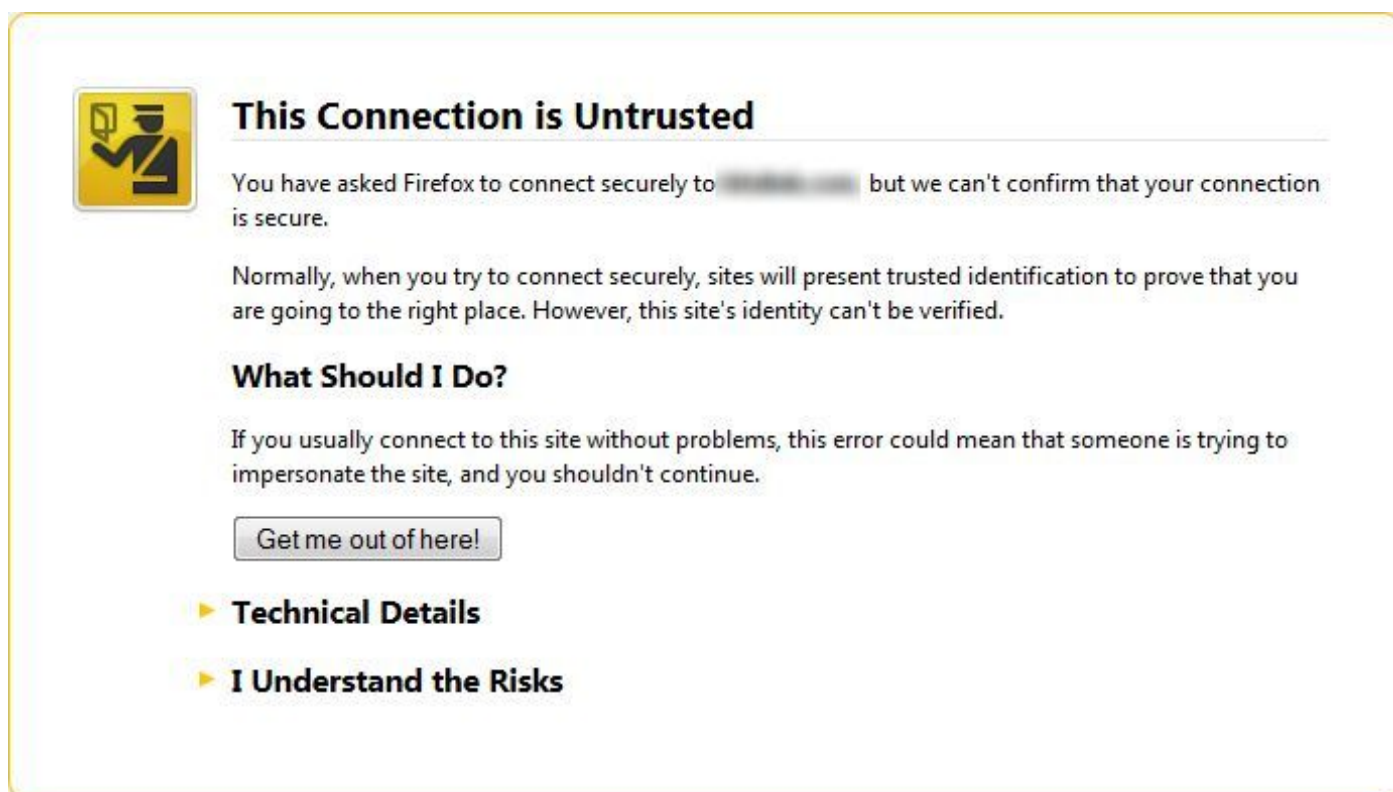
此外，目前的記錄計畫是封鎖在2017年1月1日後使用SHA-1證書的網站，而不管證書中的ValidFrom條目。但是，由於最近針對SHA-1證書的攻擊，這些瀏覽器可能會在此時間線上移動，並在2017年1月1日後阻止使用SHA-1證書的網站，無論證書頒發日期如何。

思科建議客戶詳細閱讀公告，並及時瞭解Microsoft和Mozilla就此主題發佈的最新公告。

某些版本的UCCX會產生SHA-1憑證。如果您訪問受SHA-1證書保護的UCCX網頁，則可能會根據前面所述的日期和規則生成警告或阻止這些網頁。

使用者體驗

當檢測到SHA-1證書時（取決於ValidFrom日期和先前列出的規則），使用者可能會看到類似以下內容的消息：



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.

[Get me out of here!](#)


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



根據所做的決策，使用者可能能夠或不能繞過此警告。

UCCX注意事項

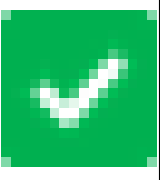
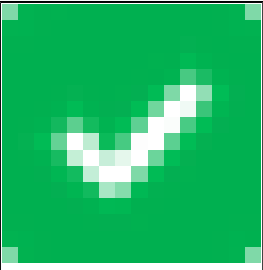
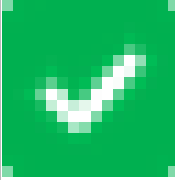
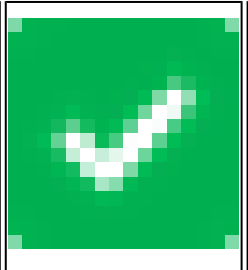
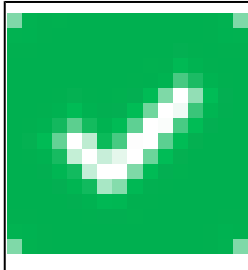





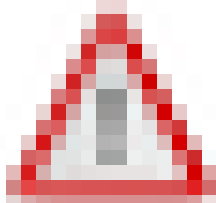
下表說明當前軟體維護的每個版本的UCCX的SHA-1證書影響和緩解策略。

本文中使用的符號

表示法	說明
	已支援。無需進一步操作。

	支援可用，但需要重新生成證書。
	無支援。

UCCX 11.5

	UCCX管理	CUIC管理 即時資料#	Finesse管理 案頭#	座席電子郵件和 與 SocialMiner的 聊天*	UCCX REST指令碼 編寫步驟	使用 MediaSense* 11.5錄製
全新安裝						
從早期版本升級	 UCCX證書保留舊版本的演算法。 如果在舊版本中使用SHA-11金鑰生成，則自簽名證書基於SHA-1，需要重新生成。	 UCCX Cisco Unified Intelligence Center(CUIC)證書保留舊版本的演算法。 如果在舊版本中使用SHA-11金鑰生成，則自簽名證書基於SHA-1，需要重新生成。	 UCCX Finesse證書保留舊版本的演算法。 如果在舊版本中使用SHA-11金鑰生成，則自簽名證書基於SHA-1，需要重新生成。	 SocialMiner和UCCX證書保留較舊版本的演算法。 如果在舊版本中使用SHA-11金鑰生成，則自簽名證書基於SHA-1，需要重新生成。	 UCCX不會拒絕將SHA-1證書用作代表狀態傳輸 (REST)通訊一部分的遠端Web伺服器。在UCCX上重新生成證書後，REST步驟將生效。	 MediaSense和UCCX證書保留舊版中的演算法。 如果在舊版本中使用SHA-11金鑰生成，則自簽名證書基於SHA-1，需要重新生成。

註: *重新生成的MediaSense和SocialMiner證書必須重新匯入到UCCX中。

註:Finesse#NoCUIC需要單獨的操作。證書在UCCX平台管理頁面上僅重新生成一次。

UCCX 11.0(1)

	UCCX管理	CUIC管理 即時資料#	Finesse管理 案頭#	座席電子郵件和 與SocialMiner的 聊天**	UCCX REST指 令碼編寫步驟	使用 MediaSense** 11.0*和10.5*錄 製
全新安裝	 <p>預設情況下，所有自簽名的新安裝證書都是SHA-1證書，需要重新生成。</p>	 <p>預設情況下，所有自簽名的新安裝證書都是SHA-1證書，需要重新生成。</p>	 <p>預設情況下，所有自簽名的新安裝證書都是SHA-1證書，需要重新生成。</p>	 <p>預設情況下，所有自簽名的新安裝證書都是SHA-1證書，需要重新生成。</p>	 <p>UCCX不會拒絕使用SHA-1證書作為REST通訊一部分的遠端Web伺服器。在UCCX上重新生成證書後，REST步驟將生效。</p>	 <p>預設自簽署憑證為SHA-1。 重新生成證書不提供SHA-256選項。</p>
從早期版本升級	 <p>UCCX證書保留舊版本的演算法。 如果在舊版本中使用SHA-11金鑰生成，則自簽名證書基於SHA-1，需要重新生成。</p>	 <p>UCCX CUIC證書保留舊版本的演算法。 如果在舊版本中使用SHA-11金鑰生成，則自簽名證書基於SHA-1，需要重新生成。</p>	 <p>UCCX Finesse證書保留舊版本的演算法。 如果在舊版本中使用SHA-11金鑰生成，則自簽名證書基於SHA-1，需要重新生成。</p>	 <p>SocialMiner和UCCX證書保留較舊版本的演算法。 如果在舊版本中使用SHA-11金鑰生成，則自簽名證書基於SHA-1，需要重新生成。</p>	 <p>UCCX不會拒絕使用SHA-1證書作為REST通訊一部分的遠端Web伺服器。在UCCX上重新生成證書後，REST步驟將生效。</p>	 <p>預設自簽署憑證為SHA-1。 重新生成證書不提供SHA-256選項。</p>

註: *將發佈工程特別計畫(ES), 以允許MediaSense 10.5和11.0生成和接受SHA-256證書。

註: **重新生成的MediaSense和SocialMiner證書必須重新匯入到UCCX中。

註:Finesse#NoCUIC需要單獨的操作。證書在UCCX平台管理頁面上僅重新生成一次。

UCCX 10.5和10.6

	UCCX管理	CUIC管理 即時資料#	Finesse管理 案頭#	座席電子郵件和與 SocialMiner的聊天*	UCCX REST指令碼 編寫步驟	使用 MediaSense*** 10.0** / 10.5**進行錄製
全新安裝	 <p>預設情況下, 所有自簽名的新安裝證書都是SHA-1證書, 需要重新生成。</p>	 <p>預設情況下, 所有自簽名的新安裝證書都是SHA-1證書, 需要重新生成。</p>	 <p>預設情況下, 所有自簽名的新安裝證書都是SHA-1證書, 需要重新生成。</p>	 <p>只有在SocialMiner(SM)v11中才提供SHA-256代理電子郵件和聊天支援, 而SM v11與UCCX v10.x不相容。</p>	 <p>UCCX不會拒絕使用SHA-1證書作為REST通訊一部分的遠端Web伺服器。在UCCX上重新生成證書後, REST步驟將生效。</p>	 <p>預設自簽署憑證為SHA-1。 重新生成證書不提供SHA-256選項。</p>
從早期版本升級	 <p>憑證會保留較舊版本的演算法。 如果在舊版本中使用SHA-11金鑰生</p>	 <p>憑證會保留較舊版本的演算法。 如果在舊版本中使用SHA-11金鑰生</p>	 <p>憑證會保留較舊版本的演算法。 如果在舊版本中使用SHA-11金鑰生成, 則自簽名證書基</p>	 <p>只有在SM v11中才提供SHA-256代理電子郵件和聊天支援, 而SM v11與UCCX v10.x不相容。</p>	 <p>UCCX不會拒絕使用SHA-1證書作為REST通訊一部分的遠端Web伺服器。在UCCX上重新生成證書後</p>	 <p>預設自簽署憑證為SHA-1。 重新生成證書不提供SHA-256選項。</p>

	成，則自簽名證書基於SHA-1，需要重新生成。	成，則自簽名證書基於SHA-1，需要重新生成。	於SHA-1，需要重新生成。		，REST步驟將生效。	
--	-------------------------	-------------------------	----------------	--	-------------	--




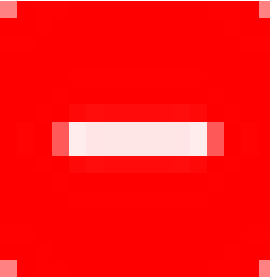
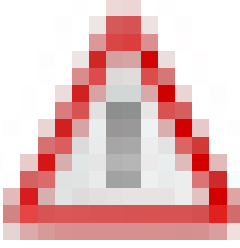

註：*將發佈工程特別計畫，以允許SocialMiner 10.6生成和接受SHA-256證書。


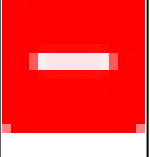


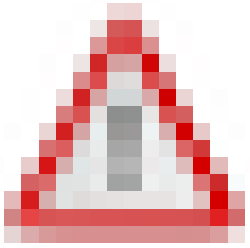

注意：**將發佈工程特別計畫(ES)，以允許MediaSense 10.0和10.5生成和接受SHA-256證書。

注意：***重新生成的MediaSense和SocialMiner證書必須重新匯入到UCCX中。

註：#No和CUIC需要單獨操作。證書在UCCX平台管理頁面上僅重新生成一次。

UCCX 10.0

	UCCX管理**	CUIC管理即時資料#	Finesse管理案頭#	與SocialMiner進行座席聊天*	UCCX REST指令碼編寫步驟	使用MediaSense*** 10.0進行錄**
全新安裝	 預設自簽署憑證為SHA-1。 重新生成證書不提供SHA-256選項。	 預設自簽署憑證為SHA-1。 重新生成證書不提供SHA-256選項。	 預設自簽署憑證為SHA-1。 重新生成證書不提供SHA-256選項。	 只有在SM v11中才提供SHA-256代理聊天支援，而SM v11與UCCX v10.x不相容。	 UCCX不會拒絕使用SHA-1證書作為REST通訊一部分的遠端Web伺服器。在UCCX上重新生成證書後，REST步驟將生效。	 預設自簽署憑證為SHA-1。 重新生成證書不提供SHA-256選項。

從早期版本升級	 預設自簽署憑證為SHA-1。 重新生成證書不提供SHA-256選項。	 預設自簽署憑證為SHA-1。 重新生成證書不提供SHA-256選項。	 預設自簽署憑證為SHA-1。 重新生成證書不提供SHA-256選項。	 只有在SM v11中才提供SHA-256代理聊天支援，而SM v11與UCCX v10.x不相容。	 UCCX不會拒絕使用SHA-1證書作為REST通訊一部分的遠端Web伺服器。在UCCX上重新生成證書後，REST步驟將生效。	 預設自簽署憑證為SHA-1。 重新生成證書不提供SHA-256選項。
---------	--	--	--	--	--	--

註：*將發佈工程特別計畫，以允許SocialMiner 10.6生成和接受SHA-256證書。

注意：**將發佈工程特別計畫(ES)，以允許MediaSense 10.0生成和接受SHA-256證書。

注意：***重新生成的MediaSense和SocialMiner證書必須重新匯入到UCCX中。

註：#No和CUIC需要單獨操作。證書在UCCX平台管理頁面上僅重新生成一次。

證書管理說明

有三種型別的證書需要驗證並可能重新生成：

- 自簽名證書
- 受信任的根證書
- 第三方簽名的證書

自簽名證書

導航到OS Administration頁面。選擇Security > Navigate to Certificate management。按一下「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

請注意以下四種證書類別：

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

tomcat類別和型別Self-signed下的證書需要重新生成。在上圖中，第三個憑證是需要再生的憑證。

完成以下步驟即可重新生成證書：

步驟 1. 按一下證書的公用名。

步驟 2. 在彈出視窗中，按一下Regenerate。

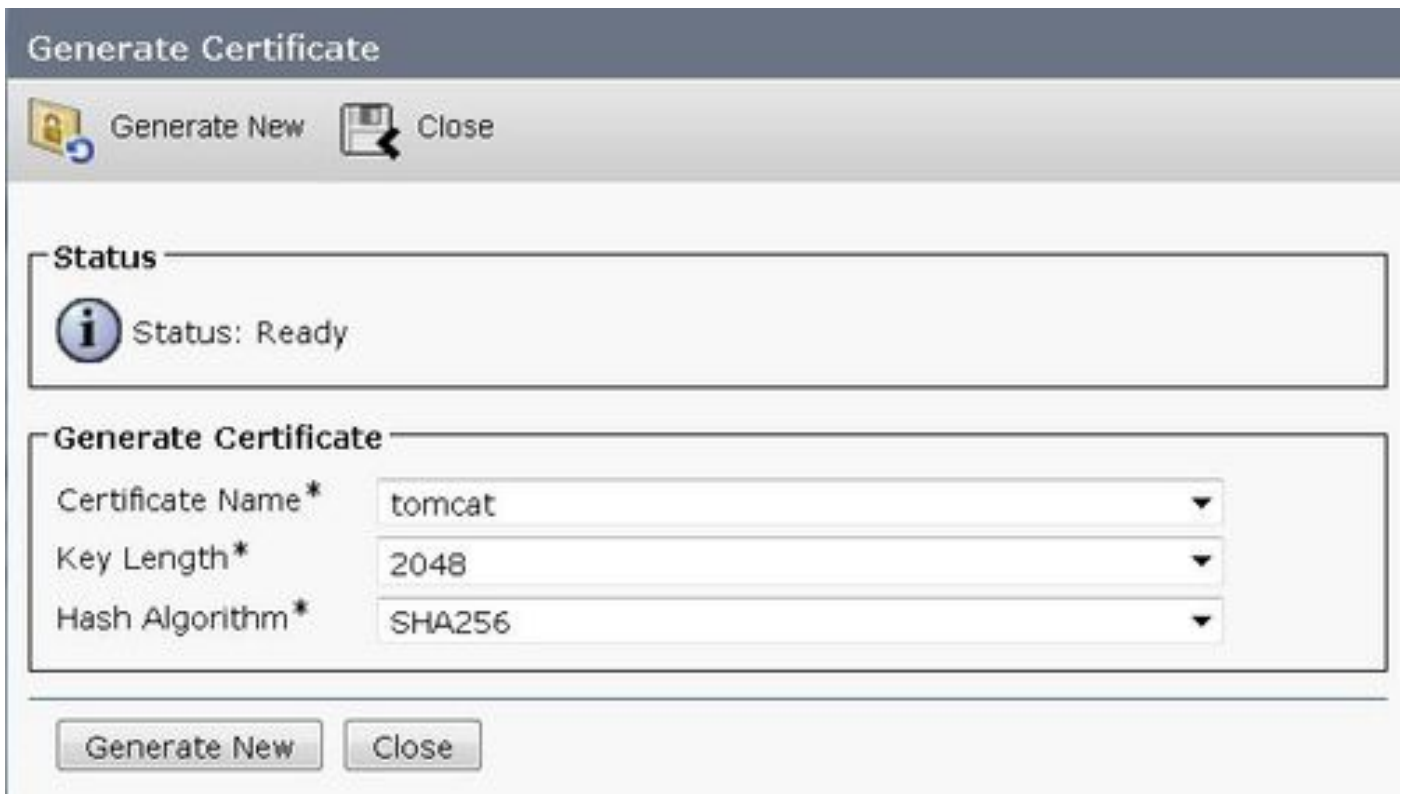
步驟 3. 選擇SHA-256加密演算法。

對於UCCX版本10.6，請完成以下步驟以重新生成證書：

步驟 1. 按一下Generate New。

步驟 2. 選擇Certificate Name as tomcat、Key Length as 2048和Hash Algorithm as SHA256。

步驟 3. 按一下「Generate New」。



受信任的根證書

以下是平台提供的證書。這些證書的基於SHA-1的簽名沒有問題，因為這些證書受傳輸層安全 (TLS)客戶端的信任，這是基於它們的身份，而不是它們的雜湊簽名。

第三方簽名的證書

由第三方憑證授權機構使用SHA-1演演算法簽署的憑證需要使用SHA-256簽署的憑證重新匯入。憑證鏈結中的所有憑證必須使用SHA-256來遞送。

附加說明

最新的工程特別計畫將在[cisco.com](https://www.cisco.com)上發佈（如果可用）。定期檢視相應的產品頁面以獲取「工程特殊」下載。

- 如需有關憑證再生或相關問題的任何協助，請開啟Cisco TAC案例。
- 在UCCX版本8.x或9.x上運行的客戶應計畫升級到最新的受支援版本，以保持思科和瀏覽器支援。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。