

UCCX的SHA-256支持

目录

[简介](#)

[先决条件](#)

[要求](#)

[从Microsoft和Mozilla的通告](#)

[用户体验](#)

[UCCX考虑事项](#)

[用于本文的符号](#)

[UCCX 11.5](#)

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

[UCCX 10.5和10.6](#)

[UCCX 10.0](#)

[证书管理说明](#)

[自签名证书](#)

[可信的根证书](#)

[第三方签名证书](#)

[其他说明](#)

简介

本文描述Cisco Unified Contact Center Express的(UCCX) SHA-256支持。SHA-1加密很快将贬抑，并且UCCX的所有支持的Web浏览器将开始阻塞从提示与SHA-1加密的证书的服务器的网页。

[先决条件](#)

[要求](#)

Cisco 建议您了解以下主题：

- Cisco Unified Contact Center Express (UCCX)
- 证书管理

从Microsoft和Mozilla的通告

[SHA-1反对更新](#)

[逐步淘汰SHA-1证书的继续](#)

在这些通知，浏览器制造商陈述浏览器将显示发出与ValidFrom日期在一月1以后遇到的SHA-1证书的bypassable警告，2016。

另外，记录当前规划是阻塞在一月1以后使用SHA-1证书的网站，2017不管在证书的ValidFrom条目

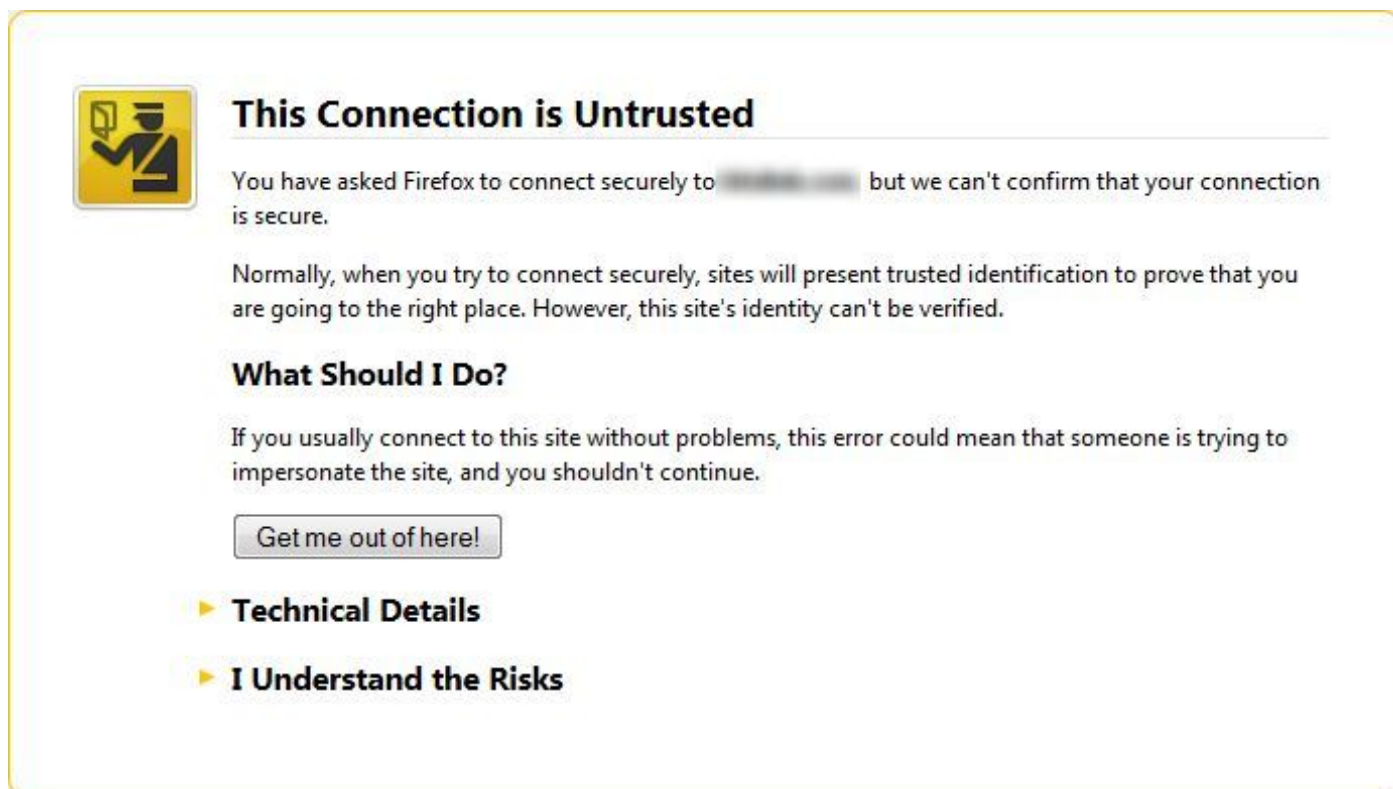
。然而，不管证书发行日，与瞄准SHA-1证书的最近的攻击，这些浏览器也许提高此时间安排和阻塞在一月1以后使用SHA-1证书的网站，2017。

思科在从Microsoft的进一步通告和Mozilla建议客户详细读通告和坚持最新在此主题。

UCCX一些版本生成SHA-1证书。如果访问SHA-1证书保护的UCCX网页，他们也许生成警告或阻塞符合以前注释的日期和规则。

用户体验

当SHA-1证书检测时，从属在ValidFrom日期和以前列出的规则，用户也许发现消息类似于此：



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**

从属在做出的决定，用户也许或也许不能绕过此警告。

UCCX考虑事项

这些表当前描述SHA-1证书影响和缓解策略UCCX每个版本的在软件维护下。

用于本文的符号

符号	说明
	已经支持的。没有进一步所需操作。
	支持是可用的，但是证书的重新生成是需要的。
	支持不是可用的。

UCCX 11.5

新安装



从以前版本的升级

UCCX证书保留从更旧的版本的算法。
如果生成与在更旧的版本的一SHA-11密钥，自签名证书是基于的SHA-1并且需要被重新生成。

Note: *The重新生成了MediaSense，并且必须再进口SocialMiner证书到UCCX。

Note: #No个别行动为精良和CUIC是需要的。证书在UCCX平台管理页面只一次被重新生成。

UCCX 11.0(1)

UCCX管理

新安装

默认情况下所有自己签署的新鲜的安装证书是SHA-1证书并且需要被重新生成。

从以前版本的升级

UCCX证书保留从更旧的版本的算法。
如果生成与在更旧的版本的一SHA-11密钥，自签名证书是基于的SHA-1并且需要被重新生成。

Note: *An Engineering Special (ES)将发布为了允许MediaSense 10.5和11.0生成和接受SHA-256证书。

Note: **必须再进口被重新生成的MediaSense和SocialMiner证书到UCCX。

Note: #No个别行动为精良和CUIC是需要的。证书在UCCX平台管理页面只一次被重新生成。

UCCX 10.5和10.6

UCCX管理

新安装

默认情况下所有自己签署的新鲜的安装证书是SHA-1证书并且需要被重新生成。

从以前版本的升级

证书保留从更旧的版本的算法。
如果生成与在更旧的版本的一SHA-11密钥，自签名证书是基于的SHA-1并且需要被重新生成。

Note: *An设计专用将发布为了允许SocialMiner 10.6生成和接受SHA-256证书。

Note: ** Engineering Special (ES)将发布为了允许MediaSense 10.0和10.5生成和接受SHA-256证书。

Note:必须再进口***被重新生成的MediaSense和SocialMiner证书到UCCX。

Note: #No个别行动为精良和CUIC是需要的。证书在UCCX平台管理页面只一次被重新生成。

UCCX 10.0

UCCX管理**

CUIC管理Live数据#

新安装

默认自签名证书是SHA-1。
重新生成证书为SHA-256不提供一个选项。

默认自签名证书是SHA-1。
重新生成证书为SHA-256不提供一个选项。

从以前版本的升级

默认自签名证书是SHA-1。
重新生成证书为SHA-256不提供一个选项。

默认自签名证书是SHA-1。
重新生成证书为SHA-256不提供一个选项。

Note:*An设计专用将发布为了允许SocialMiner 10.6生成和接受SHA-256证书。

Note: ** Engineering Special (ES)将发布为了允许MediaSense 10.0生成和接受SHA-256证书。

Note:必须再进口***被重新生成的MediaSense和SocialMiner证书到UCCX。

Note: #No个别行动为精良和CUIC是需要的。证书在UCCX平台管理页面只一次被重新生成。

证书管理说明

有需要验证和潜在被重新生成证书的三种类型：

- 赛弗签名证书
- 可信的根证书
- 第三方签名证书

自签名证书

导航到OS管理页面。选择安全>导航到证书管理。单击 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

注意四个证书类别：

- ipsec
- ipsec托拉斯
- tomcat
- Tomcat托拉斯

在**自己签署**的类别的Tomcat和的类型下的证书是要求重新生成的那个。在前一个镜像，第三证书是要求重新生成的那个。

完成这些步骤为了重新生成证书：

步骤1.点击证书的公用名称。

第二步：从弹出窗口，请点击**重新生成**。

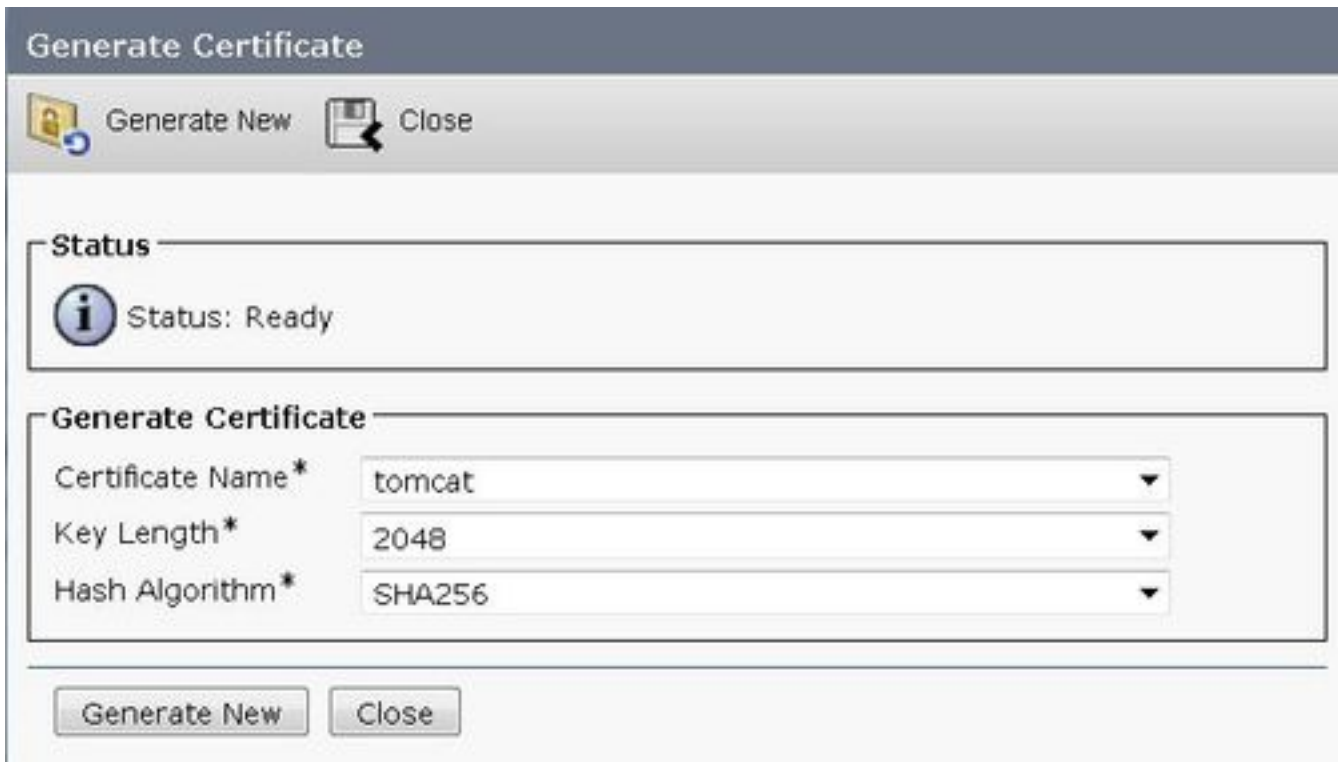
步骤3.选择SHA-256加密算法。

对于UCCX版本10.6，请完成这些步骤为了重新生成证书：

步骤1.单击**生成新**。

步骤2.选择**验证名称**作为Tomcat、**密钥长度**作为2048和**散列算法**作为SHA256。

步骤3.单击**生成新**。



可信的根证书

这些是平台提供的证书。SHA-1这些证书的基于签名不是问题，因为这些证书由根据他们的标识的传输层安全(TLS)客户端委托，而不是他们的哈希签名。

第三方签名证书

第三方签字的证书认证机关有SHA-1算法需要的再进口与SHA-256签名证书。必须辞职所有证书在证书链与SHA-256。

其他说明

最新的设计专用在cisco.com被张贴，当联机。有规律地检查对应的产品网页设计专用下载。

- 对于在证书重新生成或相关的问题的所有协助，请开Cisco TAC案例。
- 在UCCX版本8.x或9.x运作的客户应该计划升级到最新的支持的版本为了维护Cisco和浏览器支持。