UCCX的SHA-256技术支持

Contents

Introduction

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

Prerequisites

Requirements

Cisco 建议您了解以下主题：

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

从Microsoft和Mozilla的公告

[SHA-1反对更新](#)

[继续逐步淘汰SHA-1证书](#)

在这些通知，浏览器制造商陈述浏览器将显示发行与**ValidFrom**日期在2016年1月1日之后遇到的SHA-1证书的bypassable警告。

另外，记录当前计划是阻拦在2017年1月1日之后使用SHA-1证书的网站不管在认证的ValidFrom条

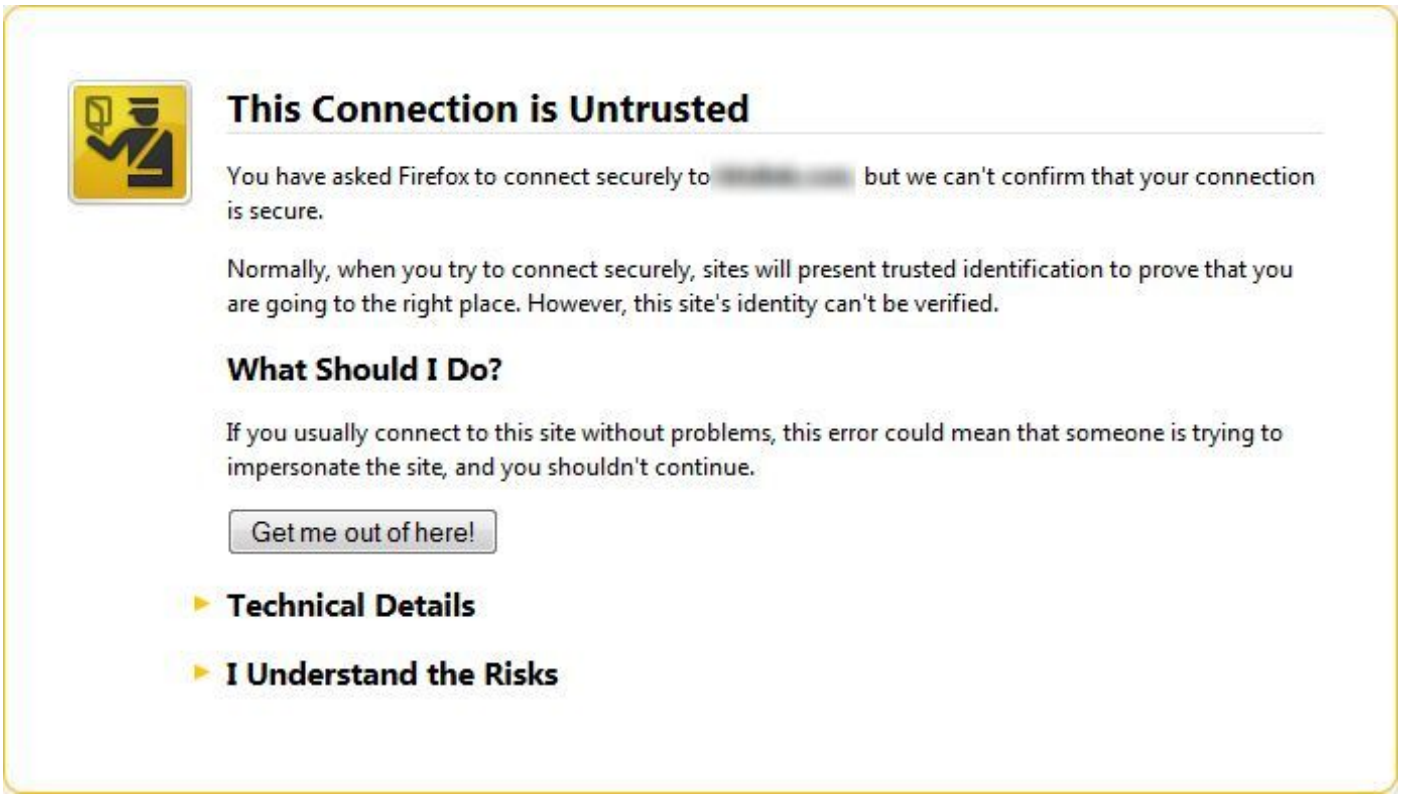
目。然而，不管认证发行日，与瞄准SHA-1证书的最近攻击，这些浏览器也许提高此时间安排和阻拦在2017年1月1日之后使用SHA-1证书的网站。

Cisco在从Microsoft的进一步公告和Mozilla建议用户详细读公告和坚持最新在此题目。

UCCX的一些版本生成SHA-1证书。如果访问SHA-1证书的保护的UCCX网页，他们也许生成警告或被阻拦符合以前注释的日期和规则。

用户体验

当发现时SHA-1认证，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：



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

这些表当前描述SHA-1认证影响和缓解策略UCCX的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。没有进一步所需操作。
⚠	技术支持是可用的，但是证书的重新生成是需要的。
−	技术支持不是可用的。

UCCX 11.5

UCCX管理

新安装

从老版本的升级 UCCX证书保留从更旧的版本的算法。
如果生成用在更旧的版本的一个SHA-11键，自署名的认证是基于的SHA-1并且需要被重新

Note:*The重新生成了MediaSense，并且必须再进口SocialMiner认证到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 默认情况下所有自已签署的新鲜的安装证书是SHA-1证书并且需要被重新生成。

从老版本的升级 UCCX证书保留从更旧的版本的算法。
如果生成用在更旧的版本的一个SHA-11键，自署名的认证是基于的SHA-1并且需要被重新

Note:将发布*An Engineering Special (ES)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认证到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 默认情况下所有自已签署的新鲜的安装证书是SHA-1证书并且需要被重新生成。

从老版本的升级 证书保留从更旧的版本的算法。
如果生成用在更旧的版本的一个SHA-11键，自署名的认证是基于的SHA-1并且需要被重新

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

Note: **将发布Engineering Special (ES)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认证到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管理实际数据#**
新安装	默认自签证书是SHA-1。 重新生成认证为SHA-256不提供一个选项。	默认自签证书是SHA-1。 重新生成认证为SHA-256不提供一个选项。
从老版本的升级	默认自签证书是SHA-1。 重新生成认证为SHA-256不提供一个选项。	默认自签证书是SHA-1。 重新生成认证为SHA-256不提供一个选项。

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

Note: **将发布Engineering Special (ES)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认证到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。

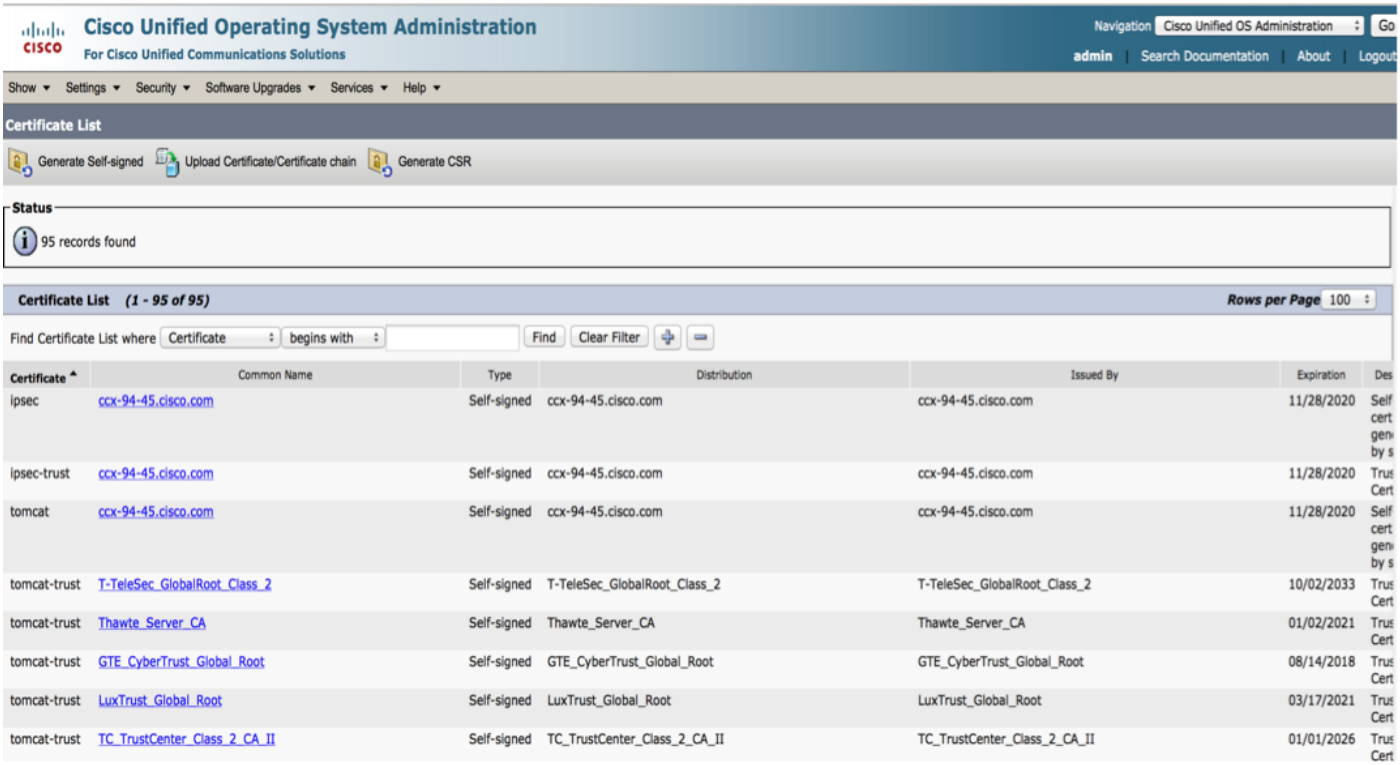
证书管理指令

有需要被验证和潜在被重新生成证书的三种类型：

- 自已签名的证书
- 可信的根证书
- 第三方签名的证书

自署名的认证

连接对OS管理页面。选择**安全>连接对证书管理**。点击**查找**。



注意四个认证类别：

- ipsec
- ipsec信任
- Tomcat
- Tomcat信任

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，第三个认证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.点击认证的普通的名字。

Step 2.从弹出窗口，请点击**重新生成**。

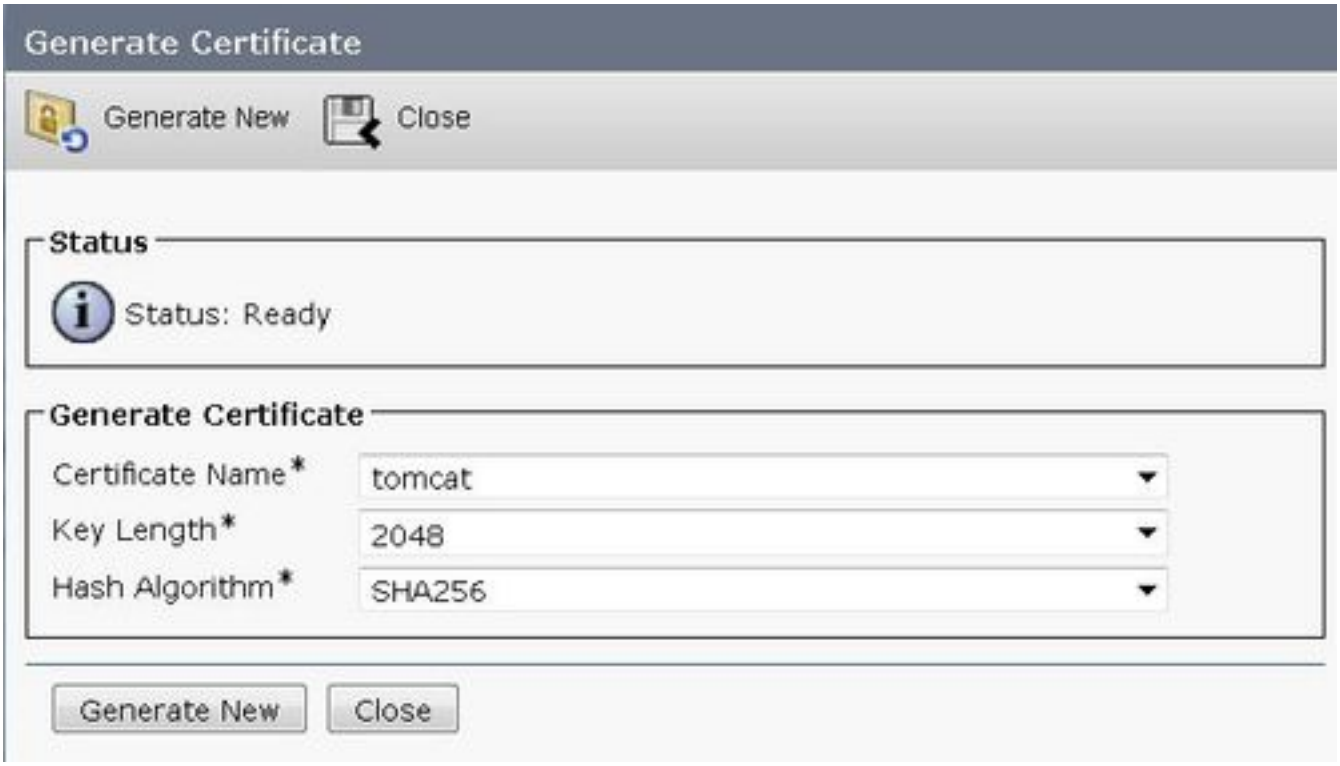
步骤3.选择SHA-256加密算法。

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.点击**生成新**。

步骤2.选择*验证名称*作为**Tomcat**，*密钥长度*作为**2048**和*Hash算法*作为**SHA256**。

步骤3.点击**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身份的传输层安全(TLS)客户端委托，而不是他们的哈希签名。

第三方签名的证书

与SHA-1算法的第三方认证机关签字的证书需要再进口与SHA-256签名的证书。必须辞职所有证书在证书链与SHA-256。

其它说明

最新的设计专用在cisco.com被张贴，当可得到时。有规律地检查对应的产品页设计专用下载。

- 对于在认证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运作的用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。