了解在UCCX解决方案的ECDSA证书

Contents

Introduction

本文描述如何配置Cisco Unified Contact Center Express (UCCX)解决方案为使用省略曲线数字签名算法(ECDSA)证书。

Prerequisites

Requirements

在您继续进行在本文描述的配置步骤前，请保证您访问这些应用程序的操作系统(OS)管理页面：

- UCCX
- SocialMiner
- 思科统一通信管理器 (CUCM)
- UCCX解决方案身份验证配置- http://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/118855-configure-uccx-00.html

管理员必须也访问在代理程序和Supervisor客户端PC机的证书存储。

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

作为普通的标准(CC)一部分证明， Cisco Unified通信管理器添加了在版本11.0的ECDSA证书。这影响所有语音操作系统的(VOS)产品例如UCCX、SocialMiner、MediaSense等等从版本11.5。

可以找到关于**椭圆曲线数字签名算法的**更多详细资料这里
：https://www.maximintegrated.com/en/app-notes/index.mvp/id/5767

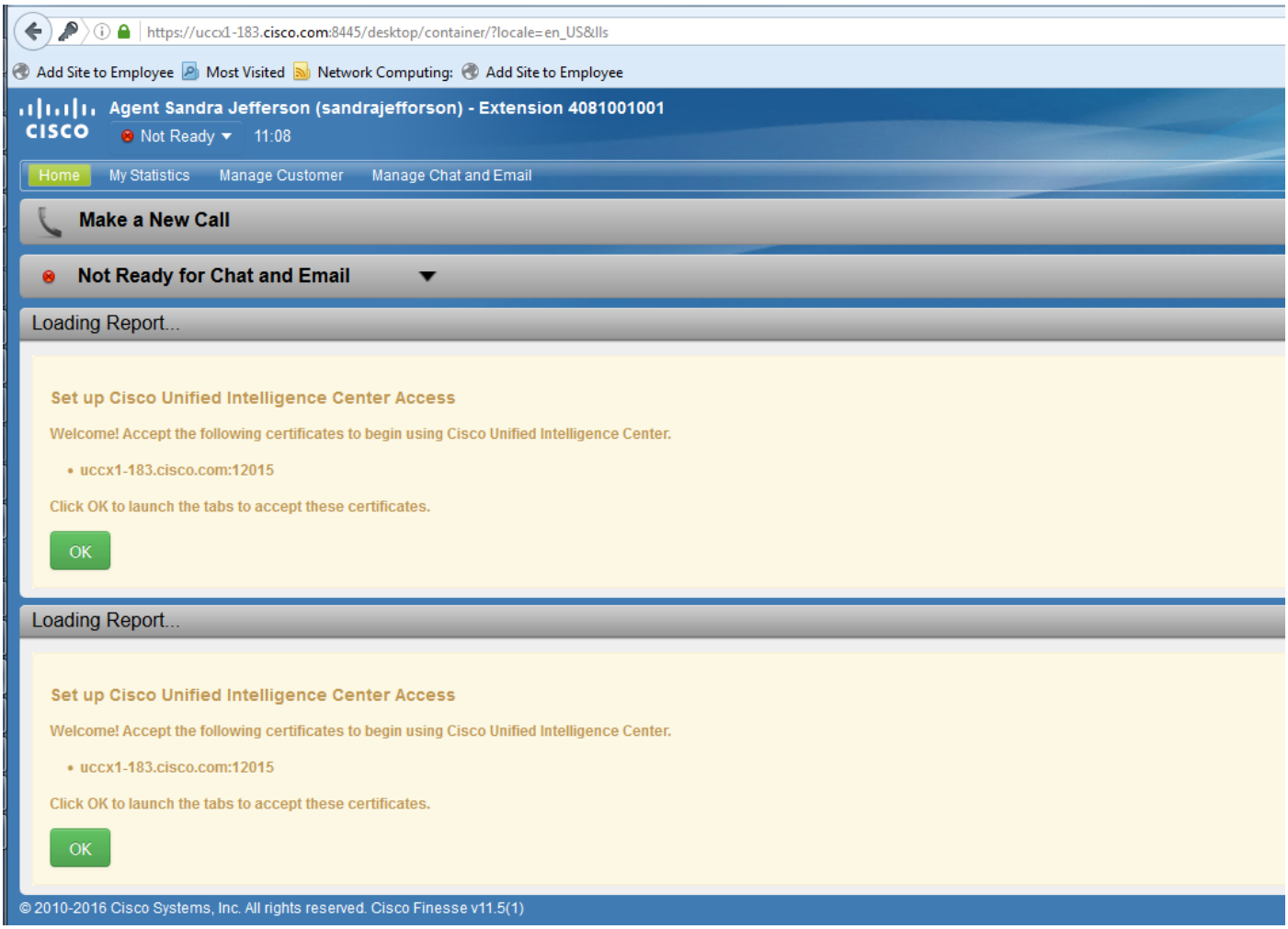
关于UCCX解决方案，当您升级到11.5时，提供不当前前您的一个另外的认证。这是TomcatECDSA认证。

这在预发布通信也描述了：https://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/200651-UCCX-Version-11-5-Prerelease-Field-Commu.html?cachemode=refresh

代理程序经验

在升级到11.5，代理程序也许请求接受在精良签字的桌面基于的认证是否自已签署的后或Certificate Authority (CA)上的证书。

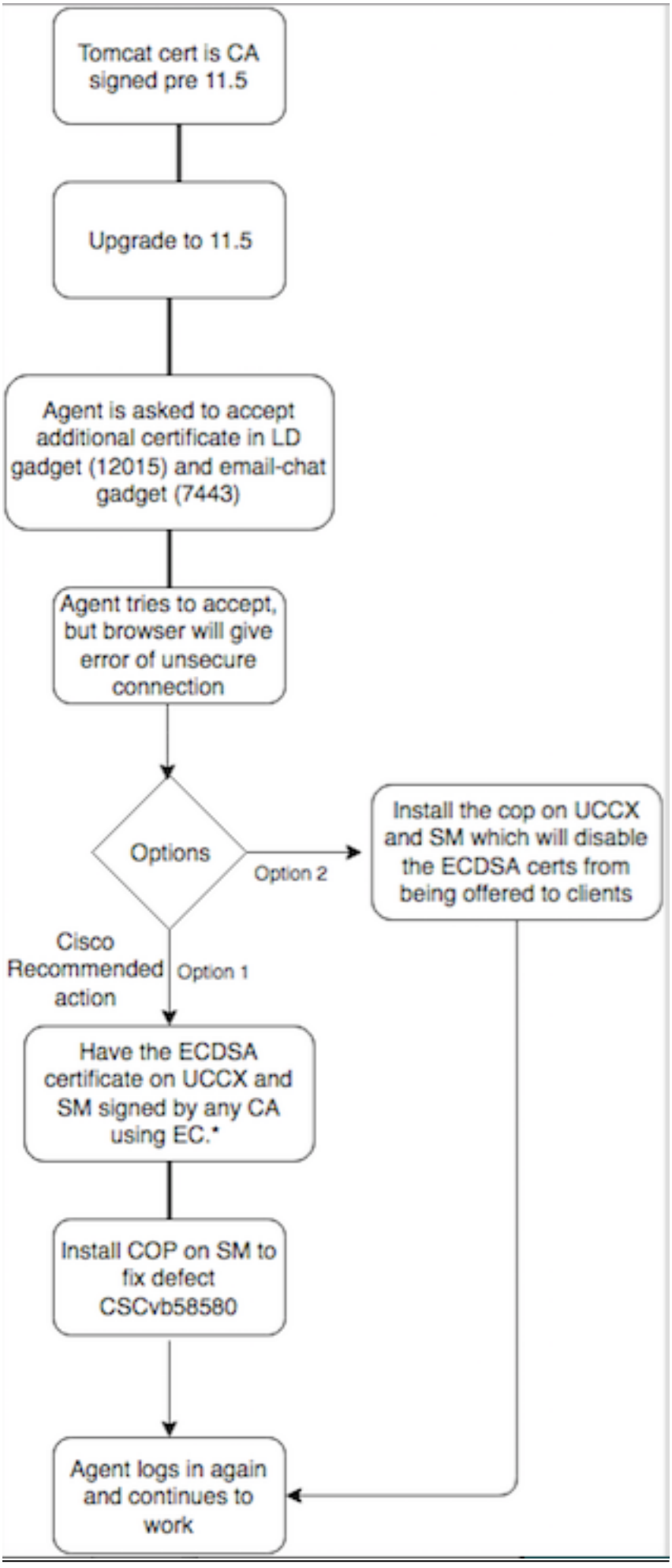
用户体验过帐升级到11.5



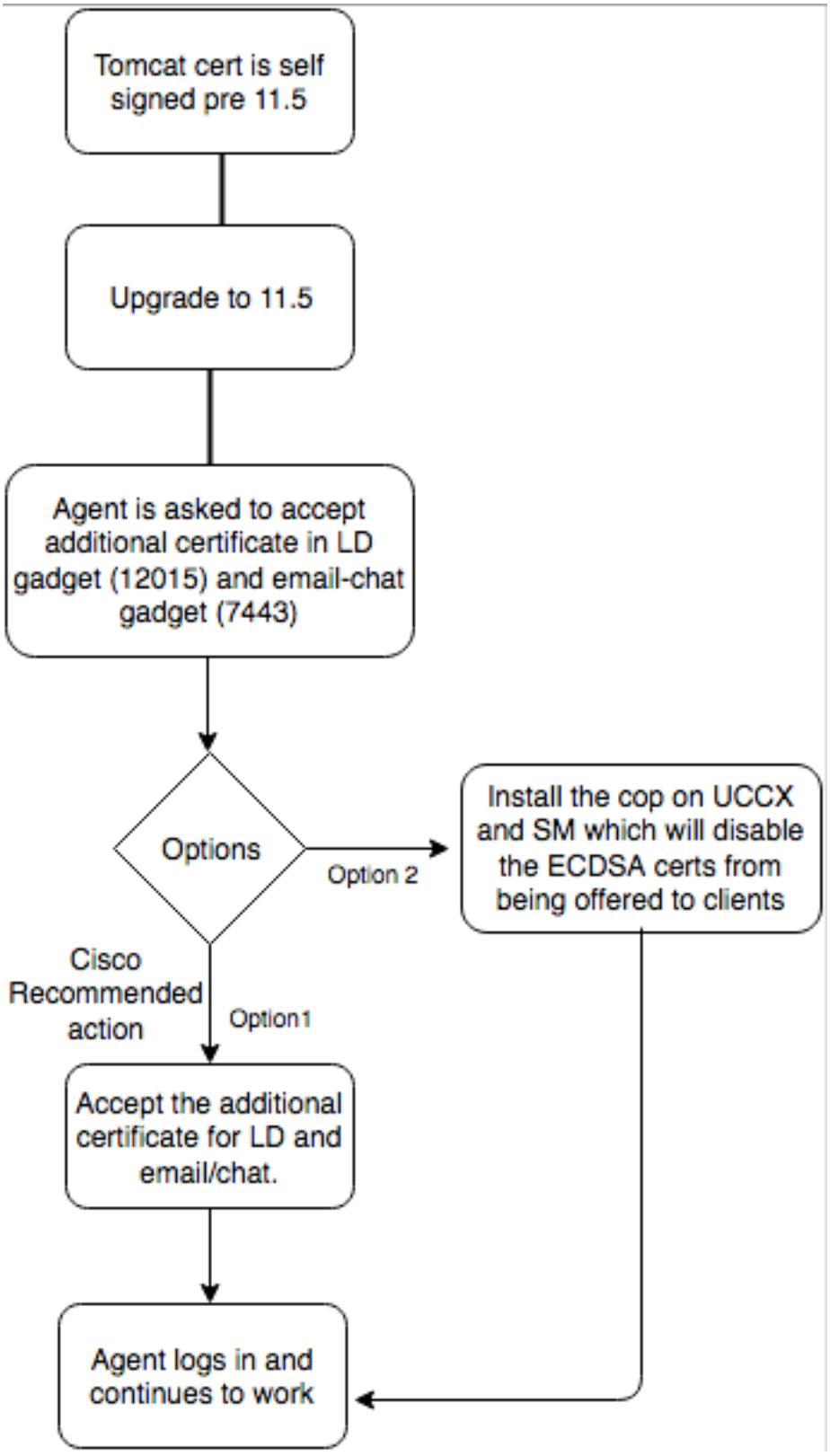
这是因为当前提供未提供前精良桌面的一个ECDSA认证。

程序

升级前CA的签名的证书


Tomcat cert is CA signed pre 11.5
Upgrade to 11.5
Agent is asked to accept additional certificate in LD gadget (12015) and email-chat gadget (7443)
Agent tries to accept, but browser will give error of unsecure connection
Options
Option 2
Install the cop on UCCX and SM which will disable the ECDSA certs from being offered to clients
Cisco Recommended action
Option 1
Have the ECDSA certificate on UCCX and SM signed by any CA using EC.*
Install COP on SM to fix defect CSCvb58580
Agent logs in again and continues to work

升级前的自署名的认证



Configure

为此认证建议使用的最佳实践

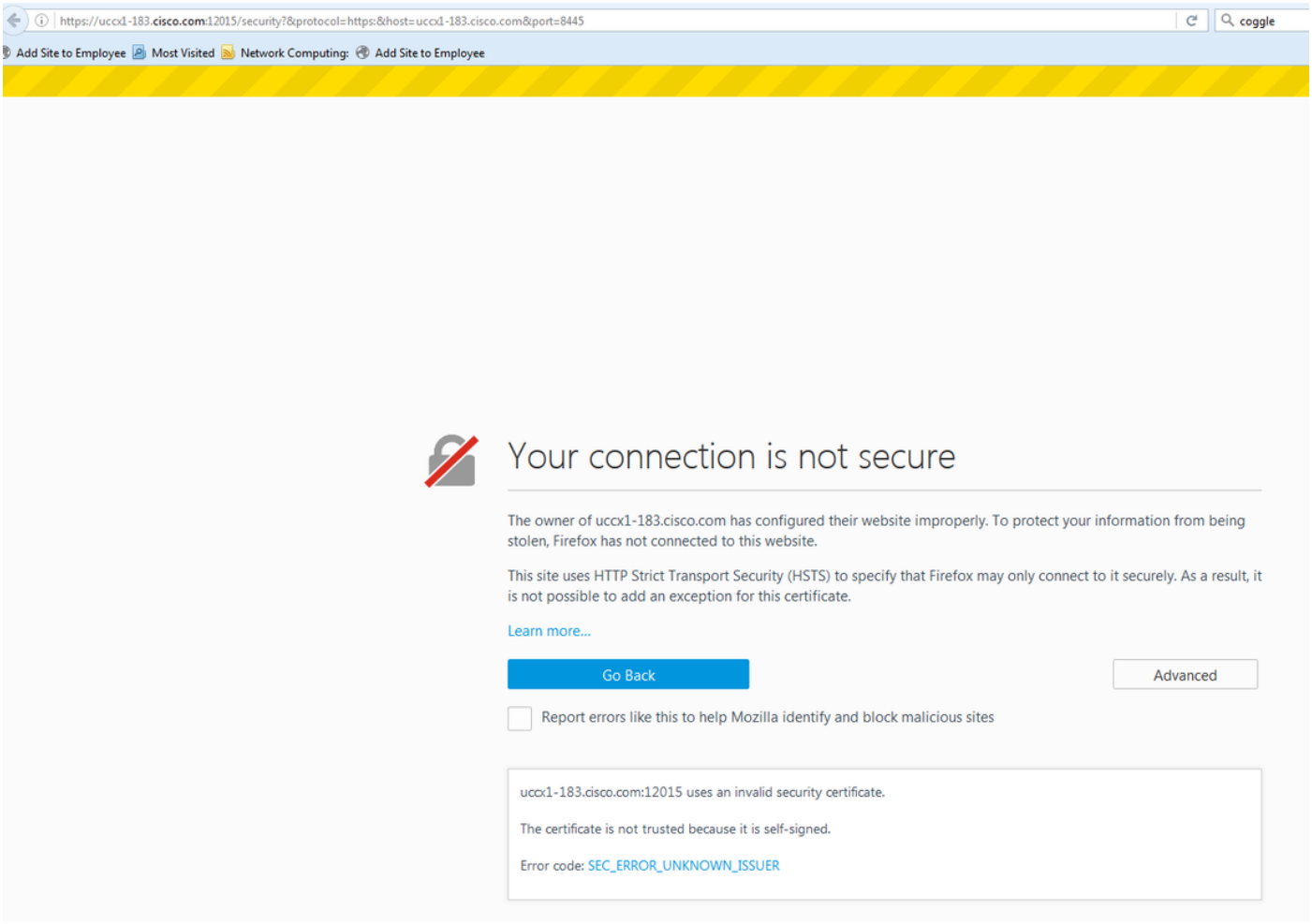
UCCX和SocialMiner的签名的证书

如果使用CA签名的证书，必须由Certificate Authority (CA)签字此ECDSA认证与其他证书一起

Note:如果CA签署与RSA的此ECDSA认证，此certifictate不会被提交给客户端。对于高级安全，为客户端提供的ECDSA证书是建议的最佳实践。

Note: 如果在SocialMiner的ECDSA认证由与RSA的CA签字，导致电子邮件和聊天的问题。这在缺陷CSCvb58580描述，并且策略文件是可用的。此COPS保证ECDSA证书为客户端没有提供。 如果是能够的签署与仅RSA的ECDSA证书的有CA，请勿使用此认证。请使用策略，以便没有提供ECDSA认证，并且您有仅一个RSA环境。

如果使用CA签名的证书，并且，在升级您没有签字和被加载后的ECDSA认证，代理程序体验消息接受另外的认证。当他们点击**OK时，**他们重定向到网站。然而，此失效由于从浏览器边的行使抵押权，因为ECDSA认证是签字的自己和您的其他Web证书是签字的CA。此通信被察觉作为一种securiry风险。



在升级以后完成在UCCX发布服务器和用户每个节点和SocialMiner的这些步骤，对UCCX和SocialMiner在版本11.5 ：

1. 连接对**OS管理页面**并且选择**安全> Certificate Management**。
2. 点击**生成CSR**。
3. 从**认证列表**下拉列表，请选择**TomcatECDSA**作为验证名称并且点击**生成CSR**。

4. 连接对**安全> Certificate Management**并且选择**下载CSR**。

5. 从弹出式窗口，从下拉列表请选择**TomcatECDSA**并且点击**下载CSR**。

发送新的CSR到第三方CA或签署签署EC证书的它与内部CA。这将生产这些签名的证书：

- CA的(如果使用同样CA应用程序证书和EC证书，您根证明能跳到此步骤)
- UCCX发布人ECDSA签名的证书
- UCCX订户ECDSA签名的证书
- SocialMiner ECDSA签名的证书

Note:如果加载根和中间证书在发布人(UCCX)，将自动地被复制给订户。如果所有应用程序证书通过同一条证书链，签字没有需要加载根或中间证书在其他上，非发布人服务器在配置。并且您能跳过根证明此加载，如果同样CA签署EC认证，并且已经执行此，当您配置了UCCX应用程序证书。

完成在每个应用服务器的这些步骤为了加载根证明和EC认证到节点：

1. 连接对**OS管理页面**并且选择**安全> Certificate Management**。

2. 点击**加载认证**。

3. 加载根证明并且选择Tomcat**信任**作为证书类型。

4. 单击 **Upload File**。

5. 点击**加载认证**。

6. 加载应用程序认证并且选择**TomcatECDSA**作为证书类型。

7. 单击 **Upload File**。

   Note:如果辅助CA签署认证，请加载辅助CA的根证明作为Tomcat*信任*认证而不是根证明。如果发出中间证书，除应用程序认证之外，请加载此认证到Tomcat*信任*存储。 并且您能跳过根证明此加载，如果同样CA签署EC认证，并且已经执行此，当您配置了UCCX应用程序证书。
8. 一旦完全，请重新启动这些应用程序：

   Cisco SocialMinerCisco UCCX发布服务器和用户

UCCX和SocialMiner的自署名的认证

如果UCCX或SocialMiner使用自署名的认证，代理程序需要建议接受认证警告他们在聊天电子邮件小配件提供并且居住数据小配件。

为了在客户端机器上安装自署名的认证，请使用一个组策略或程序包管理器或者在每个代理程序PC浏览器上单个安装他们。

对于Internet Explorer，请安装客户端自署名的认证到**可靠的根证书颁发机构**存储。

对于Mozilla Firefox，请完成这些步骤：

1. 连接对**Tools>选项**。

2. 点击**高级选项卡**。

3. 点击**视图证书**。

4. 连接对**服务器**选项。

5. 点击**添加例外**。

1. **Note**:您能也添加安全例外安装与上述进程是等同的认证。这是在客户端的一种一次配置。

常见问题(FAQ)

我们有CA签名的证书，并且要使用需要由EC CA签字的ECDSA认证。当我们等待CA签名的证书是可用的时，我们需要有实际数据。我能做什么?

我们不要签署此另外的认证或安排代理程序接受此另外的认证。我能做什么?

虽然推荐是安排ECDSA证书被提交到浏览器，有禁用它的选项。您能在保证的UCCX和SocialMiner上安装策略文件仅RSA证书被提交给客户端。ECDSA认证在keystore仍然保持，但是为客户端不会提供。

如果我使用此策略禁用为客户端提供的ECDSA证书，能I enable (event)它？

是，有提供的回退策略。一旦那适用，您能获得此认证签字和uplaoded对服务器。

所有证书是否将做ECDSA ？

目前没有，但是在VOS平台的更加进一步的安全更新在将来。

什么时候安装UCCX COPS ？

- 当您使用自署名的认证，并且不希望代理程序接受另外的证书
- 当您不能获得另外的认证签字由CA

什么时候安装SM COPS ？

- 当您使用自署名的认证，并且不希望代理程序接受另外的证书
- 当您不能获得另外的认证签字由CA
- 当是能够的签署与仅RSA的ECDSA证书的您有CA

什么是不同的Web服务器实例提供默认情况下的证书？

认证组合/Web服务器	在升级以后默认代理程序经验到1
自已签字的Tomcat，自已签署了TomcatECDSA	代理程序将请求接受在实际数据小配件和聊天电子邮件小
RSA CA签字的Tomcat， RSA CA签署了TomcatECDSA	代理程序能使用精良和实际数据，但是电子邮件聊天小配

RSA CA签字的Tomcat， EC CA签署了TomcatECDSA	代理程序能以两使用精良居住数据和chat-email*
RSA CA签字的Tomcat，自己签署了TomcatECDSA	代理程序将请求接受在实际数据和电子邮件聊天小配件的接受从实际数据小配件的认证出故障，接受从电子邮件聊

Related Information

- UCCX ECDSA COPS - https://software.cisco.com/download/release.html?mdfid=286309734&softwareid=280840578&release=11.5(1)&flowid=80822
- SocialMiner ECDSA COPS - https://software.cisco.com/download/release.html?mdfid=283613136&flowid=73189&release=11.5(1)&softwareid=283812550&sortparam=
- UCCX证书信息- http://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/118855-configure-uccx-00.html