

# 了解在UCCX解决方案的ECDSA证书

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[步骤](#)

[升级前CA的签名证书](#)

[升级前的自签名证书](#)

[配置](#)

[UCCX和SocialMiner的签名证书](#)

[UCCX和SocialMiner的自签名证书](#)

[常见问题\(FAQ\)](#)

[相关信息](#)

## 简介

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。

## 先决条件

### 要求

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
- Cisco Unified Communications Manager (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

### 使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络实际，请保证您了解所有命令潜在影响。

## 背景信息

作为普通的标准(CC)一部分证明，Cisco Unified Communications Manager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信息此处：<https://www.maximintegrated.com/en/app-notes/index.mvp/id/5767>

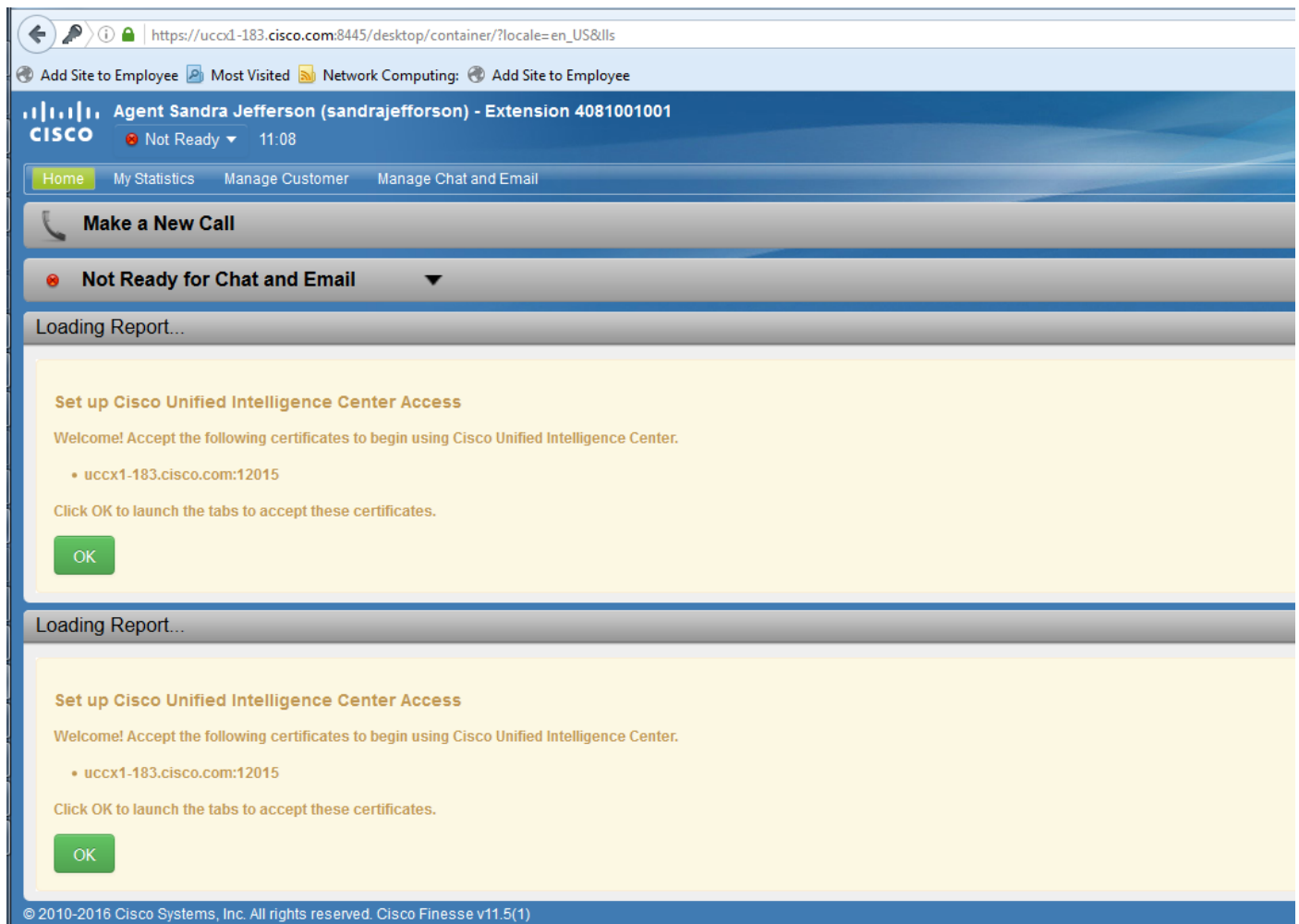
关于UCCX解决方案，当您升级到11.5时，您提供不现在前的一另外的证书。这是Tomcat ECDSA证书。

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>

## 代理程序体验

在升级到11.5，代理程序也许询问接受在精良签字的桌面基于的证书是否自己签署的后或Certificate Authority (CA)的证书。

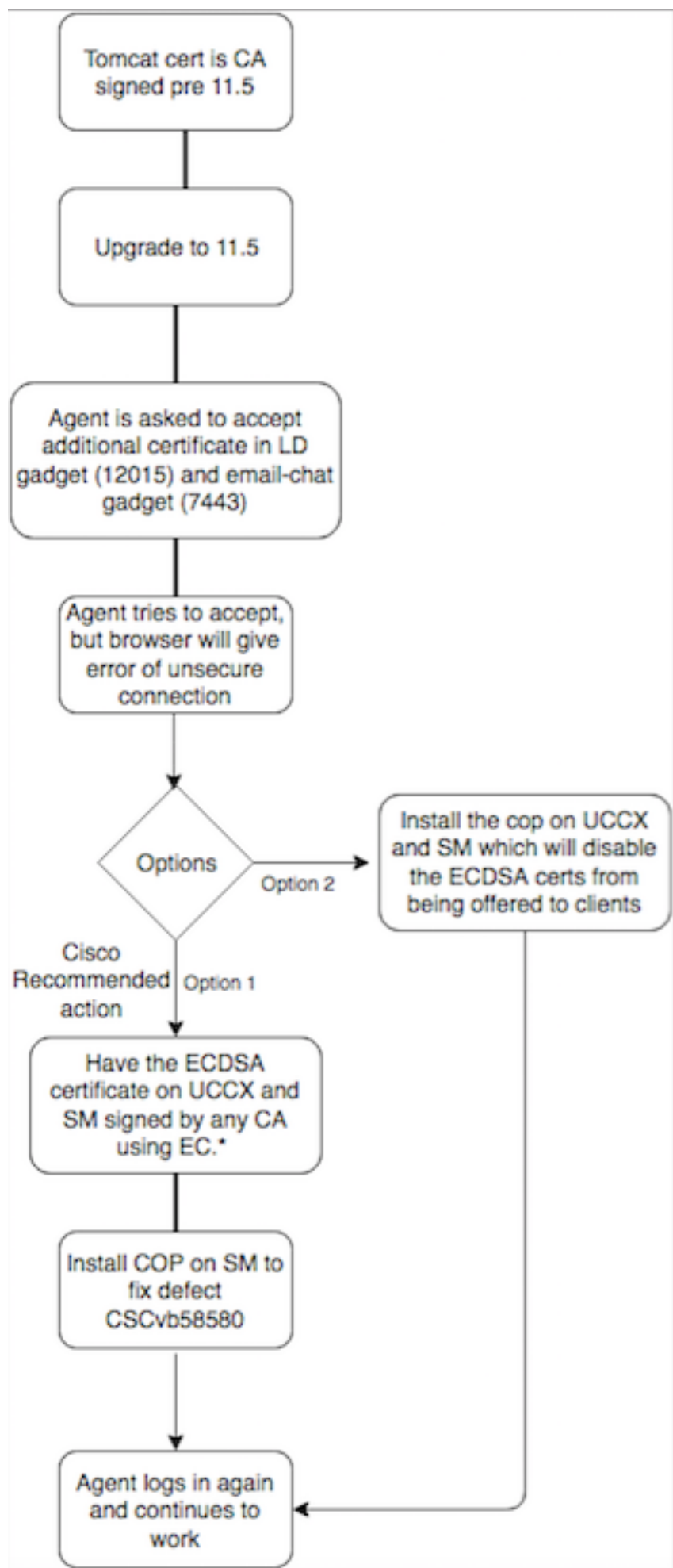
## 用户体验发表物升级到11.5



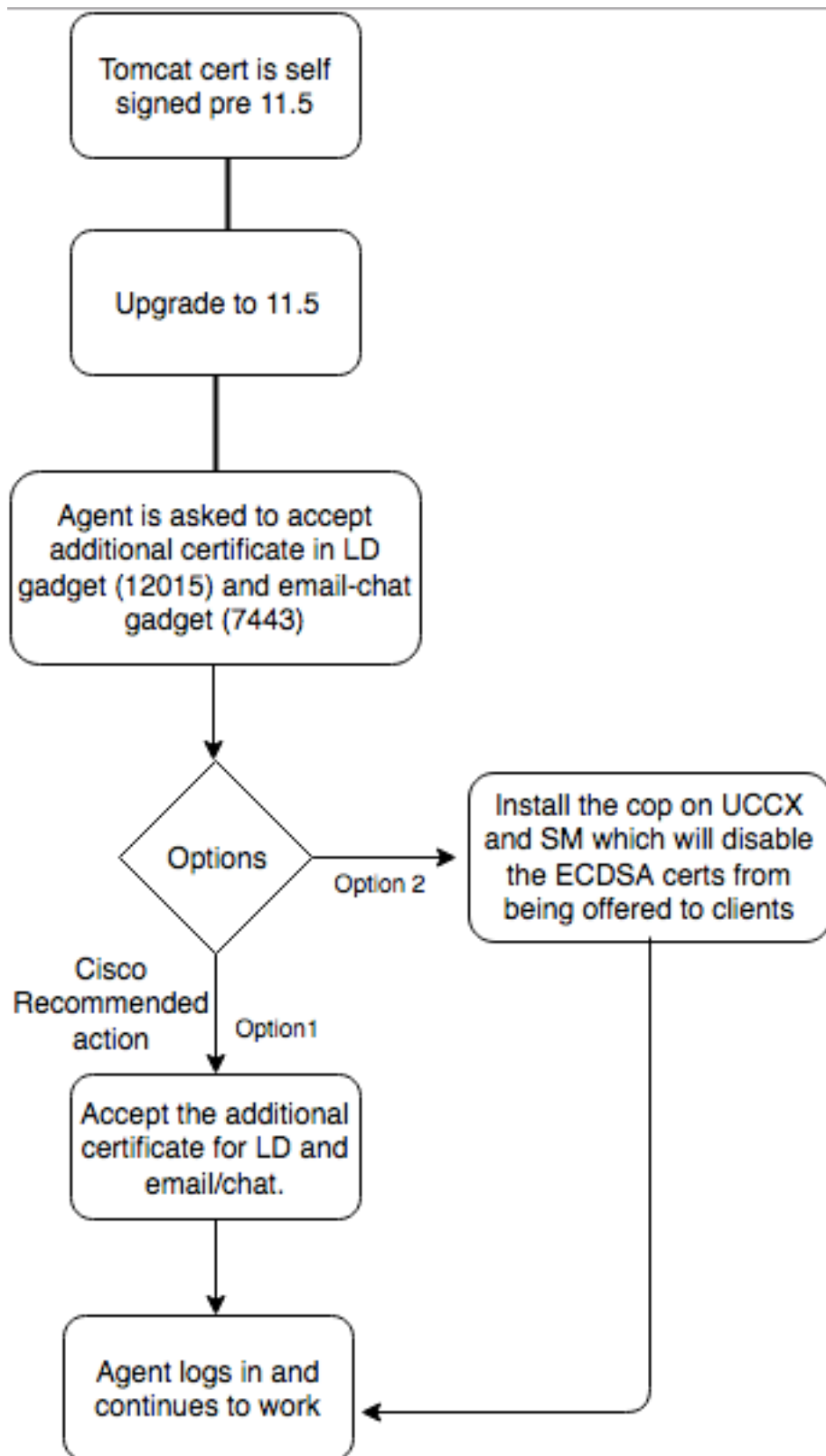
这是因为精良桌面当前提供未提供前的ECDSA证书。

## 步骤

升级前CA的签名证书



## 升级前的自签名证书



## 配置

为此证书推荐的最佳实践

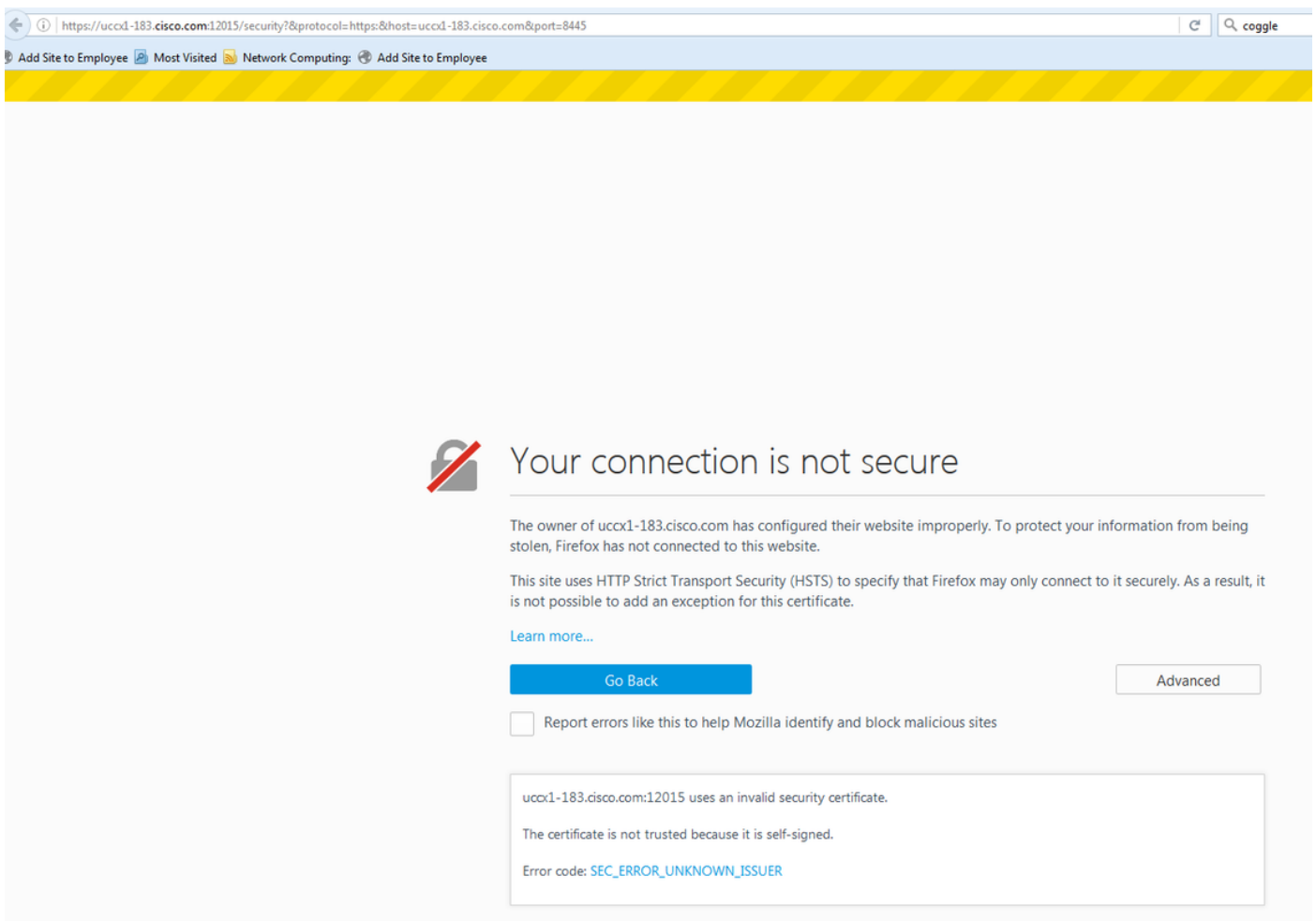
UCCX和SocialMiner的签名证书

如果使用CA签名证书，必须由Certificate Authority (CA)签字此ECDSA证书与其他证书一起

**注意：**如果CA签署与RSA的此ECDSA证书，此certificat不会提交给客户端。对于高级安全，ECDSA证书提供对客户端是建议的最佳实践。

**注意：**如果在SocialMiner的ECDSA证书由与RSA的CA签字，导致与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证书没有提供给客户端。如果有能力签署与仅RSA的ECDSA证书的有CA，请勿使用此证书。请使用策略，以便ECDSA证书没有提供，并且您有仅一个RSA环境。

如果使用CA签名证书，并且，在升级您没有签字和上传后的ECDSA证书，代理程序体验消息接受另外的证书。当他们点击好时，他们重定向到网站。然而，此失效由于从浏览器侧的行使抵押权，因为ECDSA证书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security风险。



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

1. 导航对OS管理页面并且选择安全> Certificate Management。
2. 单击生成CSR。
3. 从证书列表下拉列表，请选择Tomcat ECDSA作为验证名称并且单击生成CSR。

4. 导航对**安全 > Certificate Management**并且选择**下载CSR**。

5. 从弹出窗口，请从下拉列表选择Tomcat **ECDSA**并且点击**下载CSR**。

发送新的CSR对第三方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发行商ECDSA签名证书
- UCCX用户ECDSA签名证书
- SocialMiner ECDSA签名证书

**注意：**如果上传根和中间证书在发行商(UCCX)，将自动地复制给用户。如果所有应用程序证书通过同一条证书链，签字没有需要上传根或中间证书在其他上，非发行商服务器在配置里。并且您能跳过根证明此加载，如果同样CA签署EC证书，并且已经执行此，当您配置UCCX应用程序证书。

完成在每个应用服务器的这些步骤为了上传根证明和EC证书到节点：

1. 导航对**OS管理页面**并且选择**安全 > Certificate Management**。

2. 点击**加载证书**。

3. 上传根证明并且选择Tomcat**托拉斯**作为证书类型。

4. 单击 **Upload File**。

5. 点击**加载证书**。

6. 上传应用程序证书并且选择Tomcat **ECDSA**作为证书类型。

7. 单击 **Upload File**。

**注意：**如果辅助CA签署证书，请上传辅助CA的根证明作为Tomcat**托拉斯**证书而不是根证明。如果中间证书发出，除应用程序证书之外，请上传此证书到Tomcat**托拉斯**存储。并且您能跳过根证明此加载，如果同样CA签署EC证书，并且已经执行此，当您配置UCCX应用程序证书。

8. 一旦完整，请重新启动这些应用程序：

思科SocialMiner思科UCCX发布服务器和用户

## UCCX和SocialMiner的自签名证书

如果UCCX或SocialMiner使用自签名证书，代理程序需要建议接受证书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。

为了安装在客户端机器的自签名证书，使用组策略或包管理器或者单个安装他们在每个代理程序PC浏览器。

对于Internet Explorer，请安装客户端自签名证书到**可靠的根证书颁发机构**存储。

对于Mozilla Firefox，请完成这些步骤：

1. 导航对Tools>选项。
2. 单击 **Advanced** 选项卡。
3. 单击**视图证书**。
4. 导航对**服务器**选项卡。
5. 单击**添加例外**。

1. **注意**：您能也添加安全例外安装与上述进程是等同的证书。这是在客户端的一一次配置。

## 常见问题(FAQ)

我们有CA签名证书，并且要使用需要由EC CA签字的ECDSA证书。当我们等待CA签名证书是可用的时，我们需要有Live数据。我该怎么办？

我们不要签署此另外的证书或安排代理程序接受此另外的证书。我该怎么办？

虽然建议是安排ECDSA证书被提交到浏览器，有选项禁用它。您能安装在保证的UCCX和SocialMiner的一个策略文件仅RSA证书被提交给客户端。ECDSA证书在keystore仍然保持，但是不会提供给客户端。

如果我使用此策略禁用ECDSA证书提供对客户端，能启用它回到？

是，有提供的回退策略。一旦那应用，您能获得此证书签字和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？

- 当您使用自签名证书，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证书签字由CA

什么时候安装SM COPS？

- 当您使用自签名证书，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证书签字由CA
- 当是有能力签署与仅RSA的ECDSA证书的您有CA

什么是默认情况下由不同的Web服务器实例提供的证书？

证书组合/Web服务器

默认在升级以后的代理程序体验到11.5 (没

赛弗签署了Tomcat，赛弗签署了Tomcat 代理程序将询问接受在Live数据小配件和聊天电子邮件小配件的证



## ECDSA

RSA CA签字的Tomcat，RSA CA签署了Tomcat ECDSA

代理程序能使用精良和Live数据，但是电子邮件聊天小配件不会装

RSA CA签字的Tomcat，EC CA签署了Tomcat ECDSA

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Tomcat ECDSA

代理程序将询问接受在Live数据和电子邮件聊天小配件的另外的证书  
接受从Live数据小配件的证书出故障，接受从电子邮件聊天小配件

## 相关信息

- UCCX ECDSA COPS -  
[https://software.cisco.com/download/release.html?mdfid=286309734&softwareid=280840578&release=11.5\(1\)&flowid=80822](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=](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>