瞭解UCCX解決方案中的ECDSA證書

目錄

簡介

本文說明如何配置Cisco Unified Contact Center Express(UCCX)解決方案，以使用橢圓曲線數位簽章演算法(ECDSA)證書。

必要條件

需求

繼續執行本文檔中介紹的配置步驟之前，請確保您有權訪問這些應用程式的作業系統(OS)管理頁面：

- UCCX
- SocialMiner
- 思科整合通訊管理員(CUCM)
- UCCX解決方案證書配置 — http://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/118855-configure-uccx-00.html

管理員還必須具有對代理和Supervisor客戶端PC上的證書儲存的訪問許可權。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

作為通用標準(CC)認證的一部分，Cisco Unified Communications Manager在11.0版中新增了ECDSA證書。這將影響11.5版中的所有語音作業系統(VOS)產品，如UCCX、SocialMiner、MediaSense等。

有關橢圓曲線**數位簽章演算法的更**多詳細資訊可參閱：https://www.maximintegrated.com/en/app-notes/index.mvp/id/5767

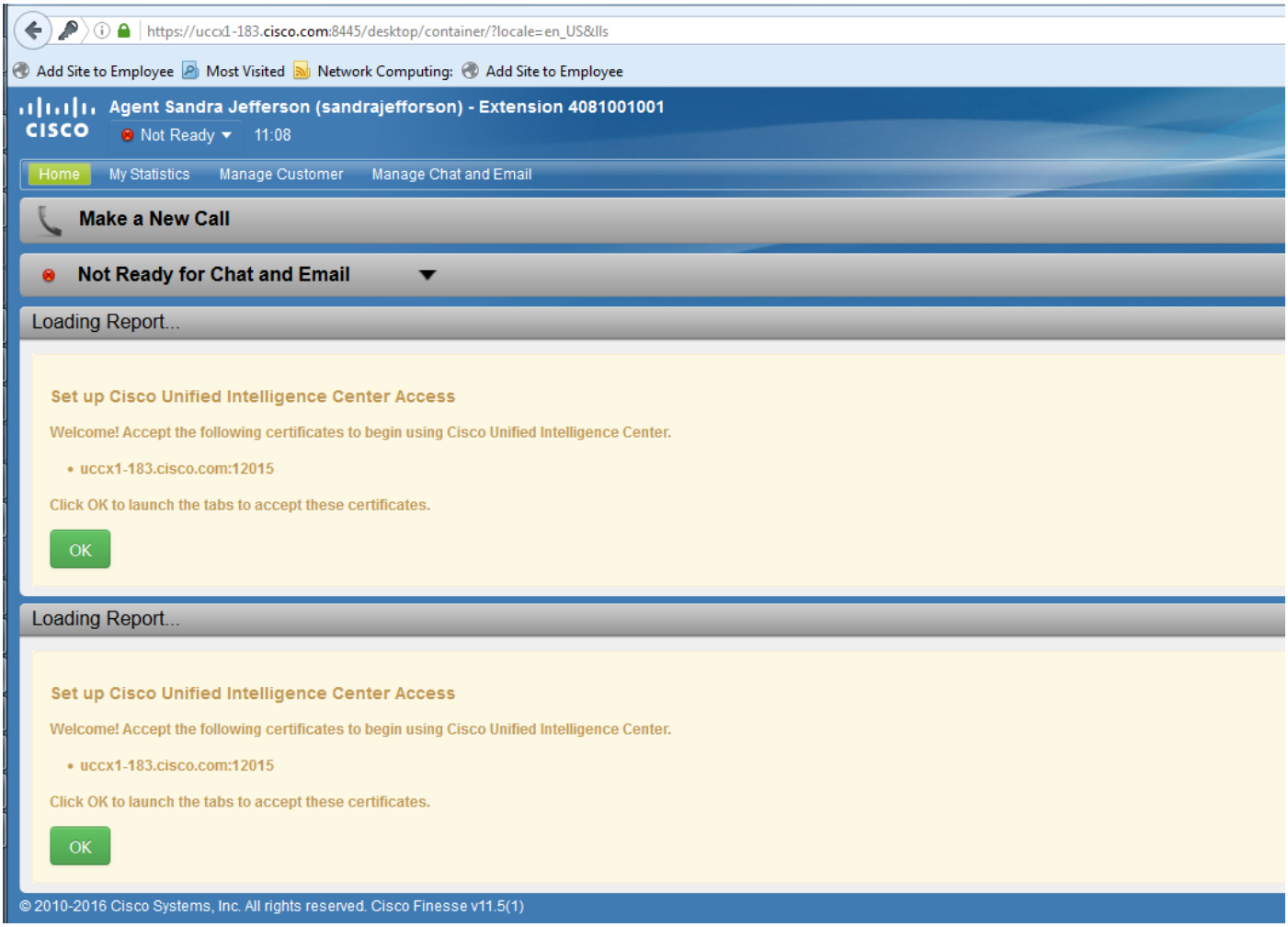
對於UCCX解決方案，在升級到11.5時，會向您提供以前未提供的附加證書。這是Tomcat-ECDSA證書。

發佈前通訊中也有相關記錄：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

座席體驗

升級到11.5後，可能會要求代理根據證書是自簽名證書還是證書頒發機構(CA)簽名證書，接受Finesse案頭上的證書。

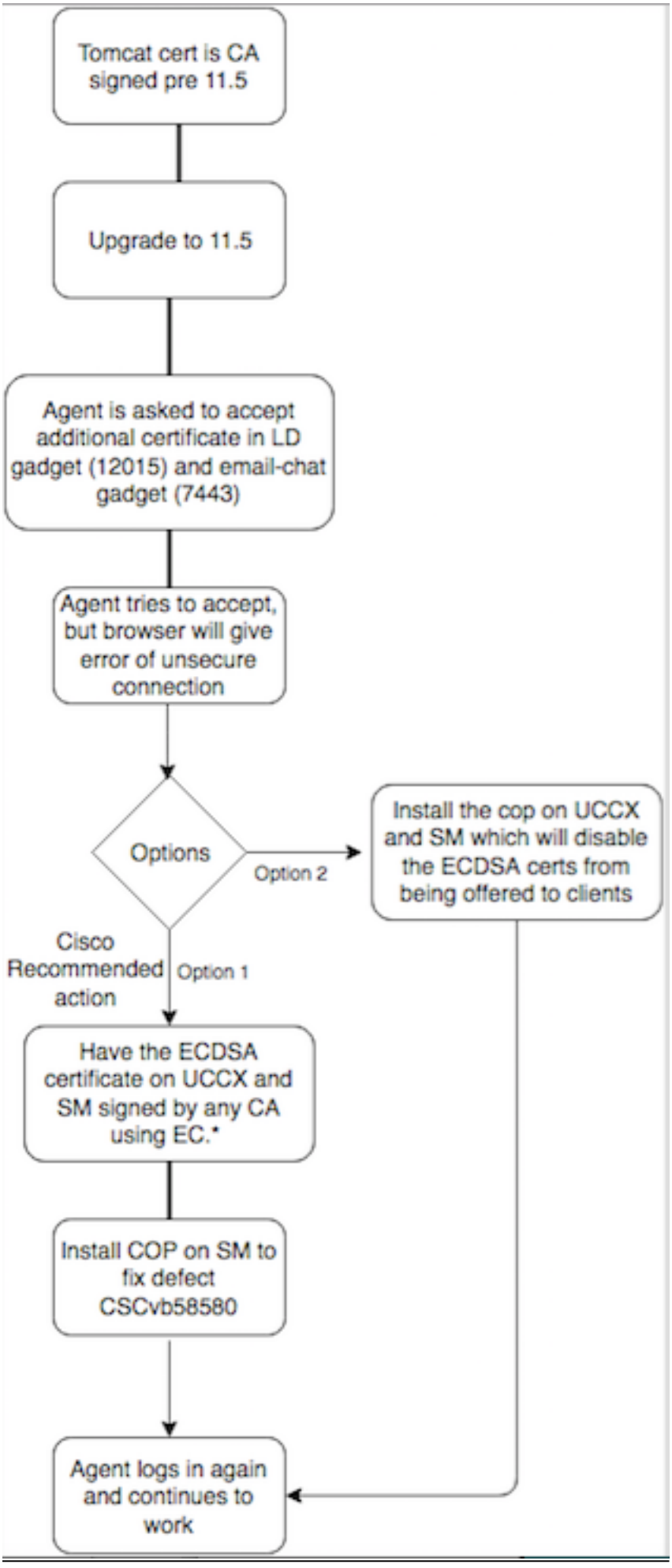
升級到11.5後的使用者體驗



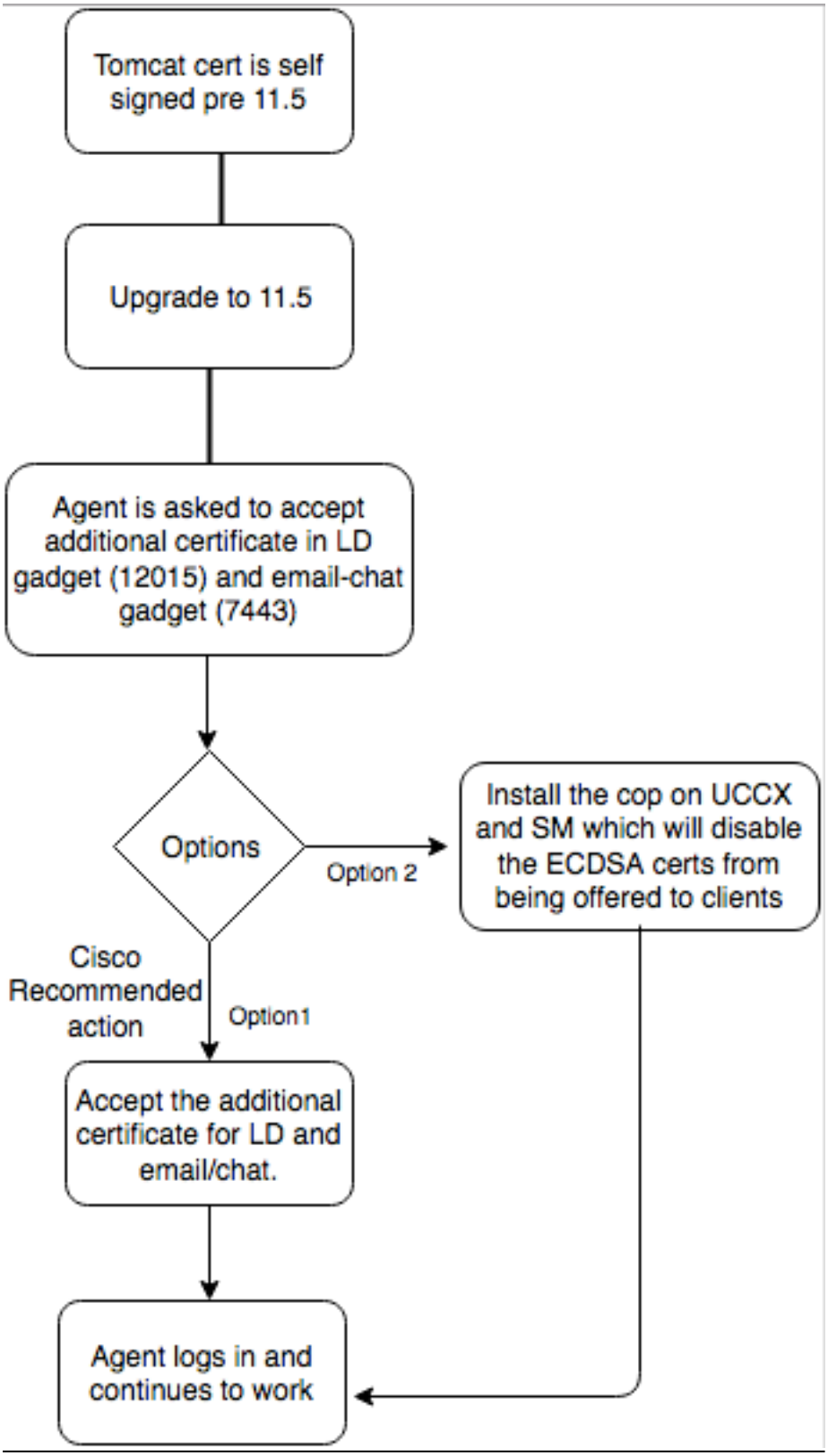
這是因為現在已為Finesse案頭提供以前未提供的ECDSA證書。

程式

CA簽名的證書預升級


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

升級前自簽名證書



設定

建議用於此證書的最佳實踐

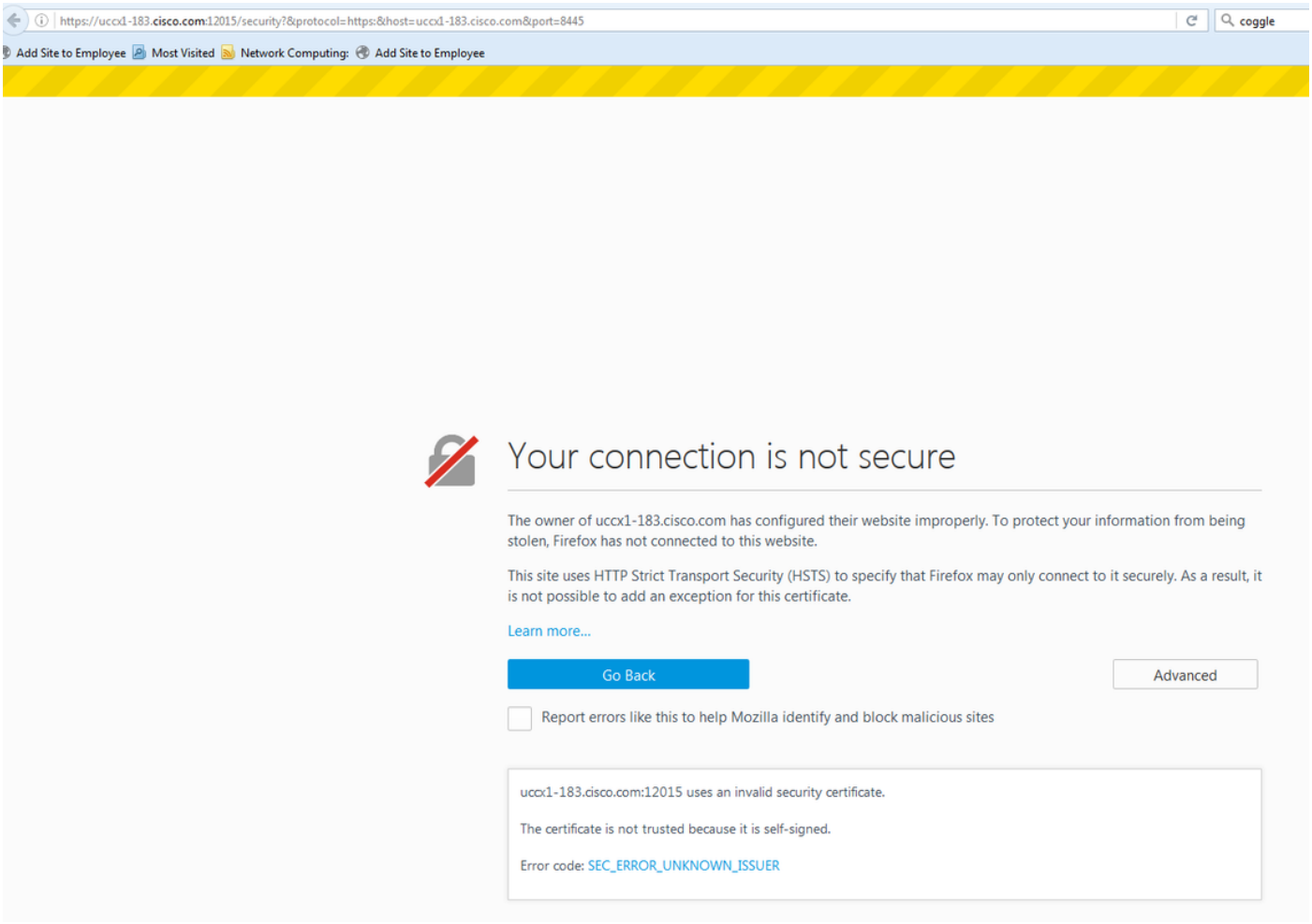
UCCX和SocialMiner的簽名證書

如果使用CA簽署的憑證，此ECDSA憑證必須透過憑證授權單位(CA)與其他憑證簽署

附註：如果CA使用RSA簽署此ECDSA證書，則此證書不會提供給客戶端。為了增強安全性，推薦的最佳做法是提供給客戶端的ECDSA證書。

注意：如果SocialMiner上的ECDSA證書是由具有RSA的CA簽名的，則會導致電子郵件和聊天出現問題。這一點在CSCvb58580缺陷中都有記錄，並且有一個複製檔案可用。此COP確保不向客戶端提供ECDSA證書。如果您的CA只能使用RSA簽署ECDSA證書，請不要使用此證書。使用cop可使不提供ECDSA證書，並且您擁有僅限RSA的環境。

如果您使用CA簽名的證書，並且升級後您沒有簽名並上傳ECDSA證書，代理會收到一條接受附加證書的消息。當他們點選**OK**時，會重定向到網站。但是，由於ECDSA證書是自簽名的，而您的其他Web證書是CA簽名的，因此由於來自瀏覽器端的安全實施，此操作會失敗。這種通訊被視為一種安全風險。



升級到11.5版的UCCX和SocialMiner後，在UCCX發佈伺服器和使用者及SocialMiner的每個節點上完成以下步驟：

1. 導航到**OS Administration**頁，然後選擇**Security > Certificate Management**。
2. 按一下「**Generate CSR**」。
3. 在「**Certificate List**」下拉式清單中，選擇「**tomcat-ECDSA**」作為憑證名稱，然後按一下「**Generate CSR**」。

4. 導覽至**Security > Certificate Management**，然後選擇**Download CSR**。

5. 在彈出視窗中，從下拉選單中選擇**tomcat-ECDSA**，然後按一下**Download CSR**。

將新CSR傳送到第三方CA，或使用簽署EC憑證的內部CA簽署。這麼做會產生以下簽署的憑證：

- CA的根憑證（如果對應用憑證和EC憑證使用相同的CA，則可以跳過此步驟）
- UCCX發佈伺服器ECDSA簽名證書
- UCCX訂戶ECDSA簽名證書
- SocialMiner ECDSA簽名證書

附註：如果將根證書和中間證書上傳到發佈伺服器(UCCX)上，則會自動將其複製到訂閱伺服器。如果所有應用證書都是通過同一證書鏈簽名的，則無需將根或中間證書上載到配置中的其他非發佈伺服器中。此外，如果同一CA簽署EC證書，並且您在配置UCCX應用證書時已經完成了此操作，則還可以跳過根證書的上傳。

在每個應用伺服器上完成以下步驟，以便將根證書和EC證書上傳到節點：

1. 導航到**OS Administration**頁，然後選擇**Security > Certificate Management**。

2. 按一下「**Upload Certificate**」。

3. 上傳根證書並選擇**tomcat-trust**作為證書型別。

4. 按一下「**Upload File**」。

5. 按一下「**Upload Certificate**」。

6. 上傳應用證書並選擇**tomcat-ECDSA**作為證書型別。

7. 按一下「**Upload File**」。

附註：如果從屬CA簽署憑證，請上傳從屬CA的根憑證作為*tomcat-trust*憑證，而不是根憑證。如果發佈了中間證書，則除了應用程式證書外，還可以將此證書上載到*tomcat-trust*儲存。如果同一CA對EC證書進行了簽名，並且您在配置UCCX應用程式證書時已經完成了此操作，則還可以跳過根證書的此上載。

8. 完成後，重新啟動這些應用程式：

Cisco SocialMinerCisco UCCX發佈者和訂閱者

UCCX和SocialMiner的自簽名證書

如果UCCX或SocialMiner使用自簽名證書，則需要建議代理接受聊天電子郵件小工具和Live Data小工具中提供的證書警告。

要在客戶端電腦上安裝自簽名證書，請使用組策略或軟體包管理器，或在每個代理PC的瀏覽器中單獨安裝它們。

對於Internet Explorer，將客戶端自簽名證書安裝到**受信任的根證書頒發機構**儲存中。

對於Mozilla Firefox，請完成以下步驟：

1. 導覽至**工具>選項**。
2. 按一下**Advanced**頁籤。
3. 按一下「**View Certificates**」。
4. 導航到**Servers**頁籤。
5. 按一下**Add Exception**。

1. **附註**：您還可以新增安全例外來安裝與上述過程相同的證書。這是客戶端上的一次性配置。

常見問題 (FAQ)

我們具有CA簽名的證書，並且希望使用需要由EC CA簽名的ECDSA證書。在我們等待CA簽名的證書可用時，需要啟用Live Data。我能做什麼？

我們不希望簽署此附加證書，也不希望代理接受此附加證書。我能做什麼？

雖然建議將ECDSA證書呈現給瀏覽器，但也可選擇禁用它。您可以在UCCX和SocialMiner上安裝一個強制檔案，以確保僅向客戶端提供RSA證書。ECDSA證書仍保留在金鑰庫中，但不會提供給客戶端。

如果我使用此命令禁用提供給客戶端的ECDSA證書，是否可以重新啟用它？

是的，提供了回滾策略。應用此證書後，您可以簽署此證書並將其上傳到伺服器。

是否所有證書都進行ECDSA?

目前沒有，但將來會對VOS平台進行進一步的安全更新。

何時安裝UCCX COP?

- 使用自簽名證書並且不希望代理接受其他證書時
- 無法獲得CA簽署的其他證書時

何時安裝SM COP?

- 使用自簽名證書並且不希望代理接受其他證書時
- 無法獲得CA簽署的其他證書時
- 如果您的CA只能使用RSA對ECDSA證書進行簽名

預設情況下，不同的Web伺服器例項提供哪些證書？

證書組合/Web伺服器	升級到11.5後的預設代理體驗（無任何複製）

自簽名Tomcat，自簽名Tomcat-ECDSA	代理將被要求接受Live Data小工具和聊天電子郵件小工具中
RSA CA簽署Tomcat，RSA CA簽署Tomcat-ECDSA	代理可以使用Finesse和Live Data，但電子郵件聊天小工具無
RSA CA簽署Tomcat，EC CA簽署Tomcat-ECDSA	，SocialMiner網頁無法載入。* 代理可以將Finesse與即時資料和聊天電子郵件結合使用*
RSA CA簽名為Tomcat，自簽名為Tomcat-ECDSA	座席將被要求接受即時資料和電子郵件聊天小工具中的附加 接受來自Live Data小工具的證書失敗，接受來自電子郵件聊 證書將成功。*

相關資訊

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