

UCCX解決方案證書管理指南

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[FQDN、DNS和域](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[組態圖表](#)

[簽名的證書](#)

[安裝簽名的Tomcat應用程式證書](#)

[自簽名證書](#)

[在外圍伺服器上安裝](#)

[重新生成自簽名證書](#)

[整合和客戶端配置](#)

[UCCX到MediaSense](#)

[MediaSense到Finesse](#)

[UCCX到SocialMiner](#)

[UCCX AppAdmin客戶端證書](#)

[UCCX平台客戶端證書](#)

[通知服務客戶端證書](#)

[Finesse客戶端證書](#)

[SocialMiner客戶端證書](#)

[CUIC客戶端證書](#)

[可從指令碼訪問的第三方應用程式](#)

[驗證](#)

[疑難排解](#)

[問題 — 使用者ID/密碼無效](#)

[原因](#)

[解決方案](#)

[問題 — CSR SAN和證書SAN不匹配](#)

[原因](#)

[解決方案](#)

[問題 — NET::ERR_CERT_COMMON_NAME_INVALID](#)

[原因](#)

[解決方案](#)

[更多資訊](#)

[證書缺陷](#)

[相關資訊](#)

簡介

本文檔介紹如何配置Cisco Unified Contact Center Express(UCCX)以使用自簽名和簽名證書。

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
- MediaSense

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

FQDN、DNS和域

UCCX配置中的所有伺服器都必須安裝域名系統(DNS)伺服器和域名。還需要代理、主管和管理員通過完全限定域名(FQDN)訪問UCCX配置應用程式。

UCCX版本10.0+要求在安裝時填充域名和DNS伺服器。由UCCX版本10.0+安裝程式生成的證書包含FQDN (視情況而定)。在升級到UCCX版本10.0+之前，將DNS伺服器和域新增到UCCX群集。

如果域首次更改或填充，應重新生成證書。將域名新增到伺服器配置後，先重新生成所有Tomcat證書，然後再將它們安裝在其他應用程式上、在客戶端瀏覽器中或在生成用於簽名的證書簽名請求(CSR)時進行安裝。

採用元件

本檔案所述的資訊是根據以下硬體和軟體元件：

- UCCX Web服務
- UCCX通知服務
- UCCX平台Tomcat
- Cisco Finesse Tomcat
- 思科整合情報中心(CUIC)Tomcat
- SocialMiner Tomcat
- MediaSense Web服務

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

隨著共同駐留Finesse和CUIC的推出、UCCX與SocialMiner在電子郵件和聊天方面的整合，以及使用MediaSense通過Finesse記錄、瞭解和安裝證書，對證書問題進行故障排除的能力現在變得至關重要。

本文檔介紹如何在涵蓋以下內容的UCCX配置環境中使用自簽名和簽名證書：

- UCCX通知服務
- UCCX Web服務
- UCCX指令碼
- 共住Finesse
- 共存CUIC (即時資料和歷史報告)
- MediaSense (基於Finesse的記錄和標籤)
- SocialMiner (聊天)

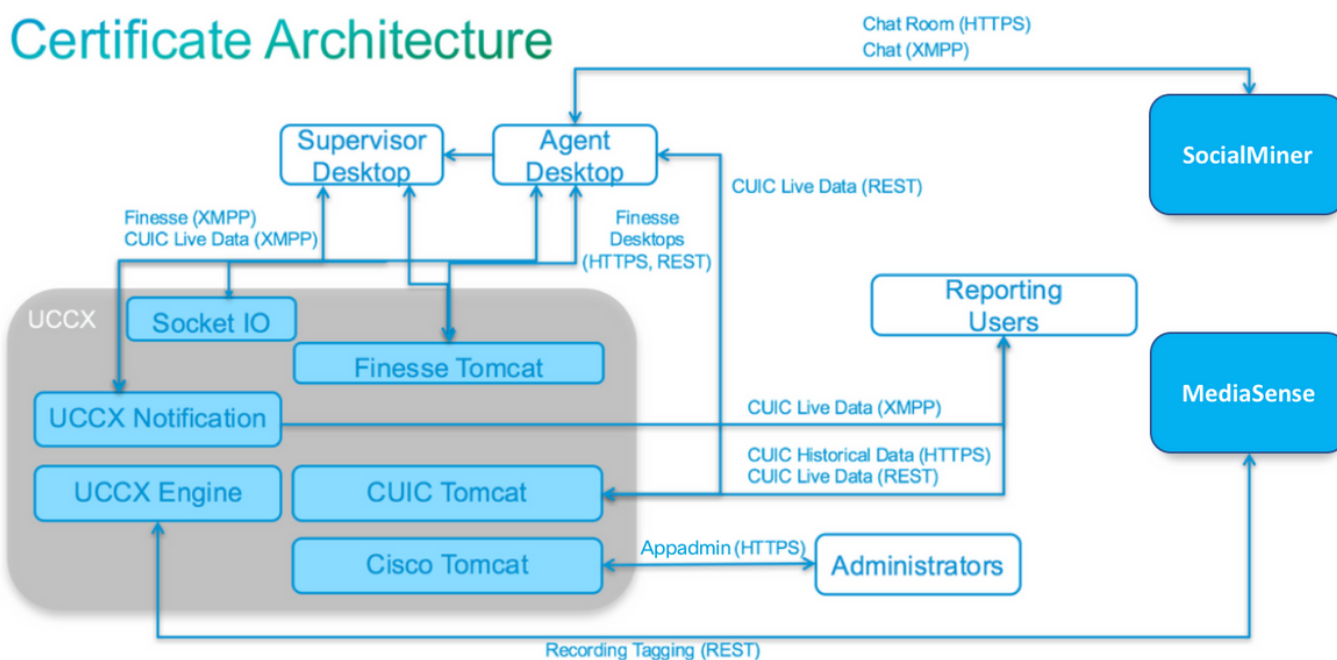
必須在UCCX配置中的應用程式 (伺服器) 以及代理和主管客戶端案頭上安裝已簽名或自簽名的證書。

在Unified Communications Operating System(UCOS)10.5中，新增了多伺服器證書，以便可以為集群生成單個CSR，而無需為集群中的每個節點簽署單個證書。UCCX、MediaSense和SocialMiner明確不支援此型別的證書。

設定

本節介紹如何配置UCCX以使用自簽名和簽名證書。

組態圖表



UCCX解決方案體系結構自UCCX 11.0起有效。HTTPS通訊圖。

簽名的證書

對於UCCX配置，推薦的證書管理方法是利用已簽名的證書。這些憑證可以由內部憑證授權單位 (CA)或公認的第三方CA簽署。

在Mozilla Firefox和Internet Explorer等主要瀏覽器中，預設情況下會安裝已知第三方CA的根證書。預設情況下，由這些CA簽名的UCCX配置應用程式的證書是受信任的，因為它們的證書鏈以已在瀏覽器中安裝的根證書結尾。

內部CA的根證書也可能通過組策略或其他當前配置預先安裝到客戶端瀏覽器中。

您可以根據客戶端瀏覽器中CA的根證書的可用性和預安裝情況，選擇是否讓知名第三方CA或內部CA簽署UCCX配置應用程式證書。

安裝簽名的Tomcat應用程式證書

針對UCCX發佈伺服器 and 訂閱伺服器、SocialMiner以及MediaSense發佈伺服器和訂閱伺服器管理應用程式的每個節點，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」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，然後按一下Download CSR。

將新CSR傳送到第三方CA或使用內部CA簽署（如前所述）。此程式應會產生以下簽署的憑證：

- CA的根證書
- UCCX發佈伺服器應用證書
- UCCX使用者應用證書
- SocialMiner應用證書
- MediaSense發佈器應用程式證書
- MediaSense使用者應用程式證書

附註：將CSR中的Distribution欄位保留為伺服器的FQDN。

附註：從11.6版開始，UCCX支援「多伺服器(SAN)」證書。但是，SAN應僅包括UCCX節點1和節點2。其他伺服器（如SocialMiner）不應包含在UCCX的SAN中。

附註：UCCX僅支援1024位和2048位的證書金鑰長度。

在每個應用伺服器上完成以下步驟，以便將根證書和應用證書上傳到節點：

附註：如果將根證書和中間證書上傳到發佈伺服器（UCCX或MediaSense）上，應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傳到配置中的其他非發佈伺服器中。

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，則除了應用證書外，還要將此證書上傳到tomcat-trust儲存。

8. 完成後，重新啟動這些應用程式：Cisco MediaSense發佈者和訂閱者Cisco SocialMinerCisco UCCX發佈者和訂閱者

附註：使用UCCX、MediaSense和SocialMiner 11.5及更高版本時，有一個名為tomcat-ECDSA的新證書。將簽名的tomcat-ECDSA證書上傳到伺服器時，將應用程式證書上傳為tomcat-ECDSA證書，而不是tomcat證書。有關ECDSA的詳細資訊，請參閱相關資訊部分中的連結以瞭解和配置ECDSA證書。

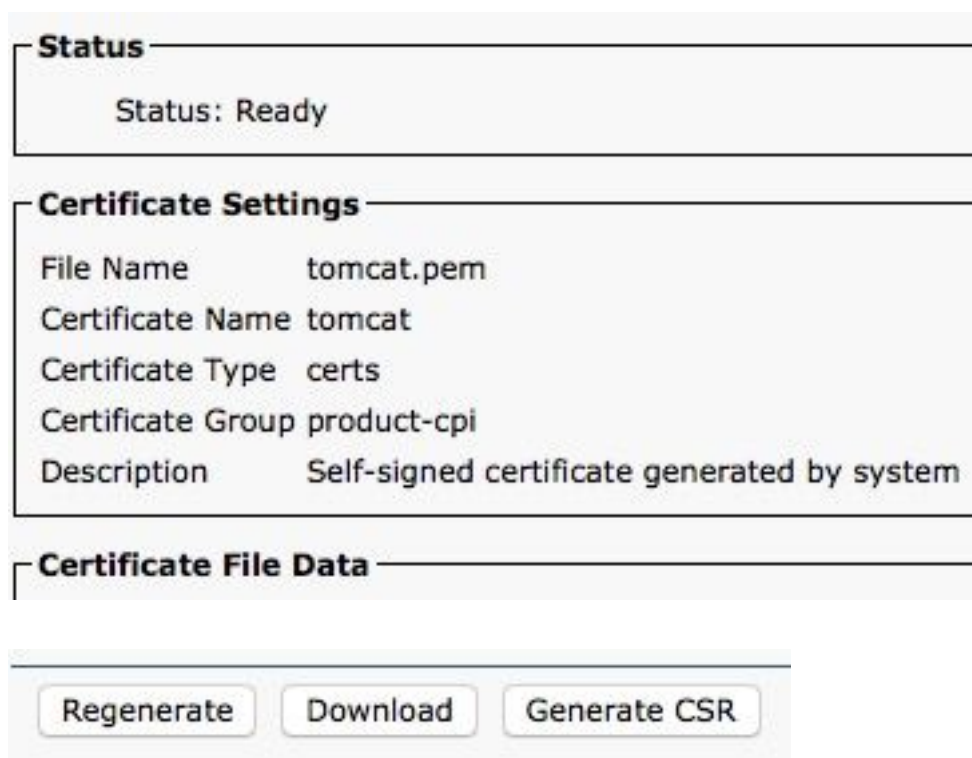
自簽名證書

在外圍伺服器上安裝

UCCX配置中使用的所有證書都預先安裝在配置應用程式上，並且是自簽名證書。向客戶端瀏覽器或其他配置應用程式顯示時，這些自簽名證書不可隱式信任。雖然建議對UCCX配置中的所有證書進行簽名，但您可以使用預安裝的自簽名證書。

對於每個應用程式關係，您必須下載相應的證書並將其上傳到應用程式。完成以下步驟即可取得和上傳憑證：

1. 訪問應用程式OS Administration頁，然後選擇Security > Certificate Management。
2. 按一下適當的憑證.pem檔案，然後選擇Download:



The screenshot displays the 'Certificate Management' interface. It is divided into three sections: 'Status', 'Certificate Settings', and 'Certificate File Data'. Below these sections are three buttons: 'Regenerate', 'Download', and 'Generate CSR'.

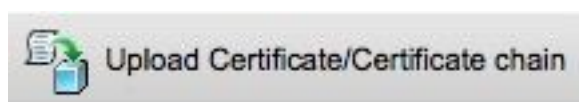
Status	
Status:	Ready

Certificate Settings	
File Name	tomcat.pem
Certificate Name	tomcat
Certificate Type	certs
Certificate Group	product-cpi
Description	Self-signed certificate generated by system

Certificate File Data	
-----------------------	--

Regenerate Download Generate CSR

3. 若要將憑證上傳到適當的應用程式上，請導覽至OS Administration頁面，然後選擇Security > Certificate Management。
4. 按一下「Upload Certificate/Certificate Chain:



5. 完成後，重新啟動這些伺服器：

Cisco MediaSense發佈者和訂閱者Cisco SocialMinerCisco UCCX發佈者和訂閱者
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**。

重新生成自簽名證書

如果自簽名證書過期，需要重新生成這些證書，並且需要再次執行在外圍伺服器上安裝的配置步驟。

1. 訪問應用程式 **作業系統管理** 頁面並選擇 **安全>證書管理**。
2. 按一下相應的證書並選擇**Regenerate**。
3. 必須重新啟動其證書重新生成的伺服器。
4. 對於每個應用程式關係，必須按照**在外圍伺服器上安裝**中的配置步驟下載相應的證書並將其上傳到應用程式。

整合和客戶端配置

UCCX到MediaSense

UCCX使用MediaSense Web服務REST應用程式程式設計介面(API)有兩個用途：

- 訂閱在Cisco Unified Communications Manager(CUCM)上呼叫的新錄製的通知。
- 使用代理和聯絡服務隊列(CSQ)資訊標籤UCCX代理的錄製。

UCCX使用MediaSense管理節點上的REST API。任何MediaSense群集中最多有兩台。UCCX不通過REST API連線到MediaSense擴展節點。兩個UCCX節點必須使用MediaSense REST API，因此請在兩個UCCX節點上安裝兩個MediaSense Tomcat證書。

將MediaSense伺服器的簽名或自簽名證書鍵上傳到UCCX *tomcat-trust*金鑰庫。

MediaSense到Finesse

MediaSense使用Finesse Web服務REST API來對Finesse上的MediaSense搜尋和播放小工具的代理進行身份驗證。

在「搜尋和播放」小工具的Finesse XML佈局上配置的MediaSense伺服器必須使用Finesse REST API，因此請在該MediaSense節點上安裝兩個UCCX Tomcat證書。

將UCCX伺服器的簽名或自簽名證書鏈上傳到MediaSense *tomcat-trust*金鑰庫。

UCCX到SocialMiner

UCCX使用SocialMiner REST和通知API來管理電子郵件聯絡人和配置。兩個UCCX節點必須使用SocialMiner REST API並由SocialMiner通知服務通知，因此請在兩個UCCX節點上安裝SocialMiner Tomcat證書。

將SocialMiner伺服器的簽名或自簽名證書鏈上傳到UCCX *tomcat-trust*金鑰庫。

UCCX AppAdmin客戶端證書

UCCX AppAdmin客戶端證書用於管理UCCX系統。若要為UCCX管理員安裝UCCX AppAdmin證書，請在客戶端PC上為每個UCCX節點導航到<https://<UCCX FQDN>/appadmin/main>，然後通過瀏覽器安裝證書。

UCCX平台客戶端證書

UCCX Web服務用於向客戶端瀏覽器交付聊天聯絡人。若要安裝UCCX代理和主管的UCCX平台證書，請在客戶端PC上導航到每個UCCX節點的<https://<UCCX FQDN>/appadmin/main>，然後通過瀏覽器安裝證書。

通知服務客戶端證書

Finesse、UCCX和CUIC使用CCX通知服務，以便通過可擴展消息傳送和線上狀態協定(XMPP)將即時資訊傳送到客戶端案頭。它用於即時Finesse通訊以及CUIC Live Data。

要在使用Live Data的代理和主管或報告使用者的PC上安裝Notification Service客戶端證書，請針對每個UCCX節點導航到<https://<UCCX FQDN>:7443/>，然後通過瀏覽器安裝證書。

Finesse客戶端證書

Finesse客戶端證書由Finesse案頭使用，用於連線到Finesse Tomcat例項，以便在案頭和共駐的Finesse伺服器之間進行REST API通訊。

若要為代理和主管安裝Finesse證書，請在客戶端PC上為每個UCCX節點導航到<https://<UCCX FQDN>:8445/>，然後通過瀏覽器提示安裝證書。

若要為Finesse管理員安裝Finesse證書，請在客戶端PC上為每個UCCX節點導航到<https://<UCCX FQDN>:8445/cfadmin>，然後通過瀏覽器提示安裝證書。

SocialMiner客戶端證書

客戶端電腦上必須安裝SocialMiner Tomcat證書。代理接受聊天請求後，聊天小工具將重定向到代表聊天室的URL。此聊天室由SocialMiner伺服器託管，包含客戶或聊天聯絡人。

若要在瀏覽器中安裝SocialMiner證書，請在客戶端PC上導航到<https://<SocialMiner FQDN>/>，然後通過瀏覽器提示安裝證書。

CUIC客戶端證書

CUIC Tomcat證書應安裝在客戶端電腦上，供在CUIC網頁或案頭小工具中使用CUIC Web介面進行歷史報告或即時資料包告的代理、主管和報告使用者使用。

若要在瀏覽器中安裝CUIC Tomcat證書，請在客戶端PC上導航至<https://<UCCX FQDN>:8444/>，然後按照瀏覽器提示安裝證書。

CUIC即時資料證書 (自11.x起)

CUIC對後端Live資料使用套接字IO服務。對於使用Live Data的CUIC Web介面或在Finesse中使用Live Data小工具的代理、主管和報告使用者，應將證書安裝在客戶端電腦上。

若要在瀏覽器中安裝Socket IO證書，請在客戶端PC上導航到<https://<UCCX FQDN>:12015/>，然後通過瀏覽器提示安裝證書。

可從指令碼訪問的第三方應用程式

如果設計UCCX指令碼是為了訪問第三方伺服器上的安全位置(例如，*Get URL Document*步驟到HTTPS URL或*Make Rest Call*到HTTPS REST URL)，請將第三方服務的已簽名或自簽名證書鏈上傳到UCCX *tomcat-trust*金鑰庫。要獲取此證書，請訪問UCCX OS Administration頁面並選擇**Upload Certificate**。

配置UCCX引擎的目的是當第三方應用程式在通過指令碼步驟訪問安全位置時提供這些證書時，在平台Tomcat金鑰庫中搜尋第三方證書鏈。

必須將整個證書鏈上傳到平台Tomcat金鑰庫(可通過OS Administration頁面訪問)，因為Tomcat金鑰庫預設情況下不包含根證書。

完成這些操作後，重新啟動Cisco UCCX引擎。

驗證

為了驗證是否正確安裝了所有證書，您可以測試本節中介紹的功能。如果未出現證書錯誤，且所有功能均正常工作，則證書安裝正確。

- 配置Finesse，使其通過工作流自動記錄代理。座席處理呼叫後，請使用MediaSense搜尋和播放應用程式查詢呼叫。驗證呼叫是否在MediaSense中已將座席、CSQ和團隊標籤附加到錄製後設資料。
- 通過SocialMiner配置座席網路聊天。通過Web表單插入聊天聯絡人。確認座席收到接受聊天聯絡人的標語，並確認接受聊天聯絡人後，聊天表單正確載入，座席可以接收和傳送聊天消息。
- 嘗試通過Finesse登入代理。確認未出現證書警告，網頁未提示將證書安裝到瀏覽器中。驗證代理是否可以正確更改狀態，並且向UCCX發出的新呼叫是否正確呈現給代理。
- 在代理和Supervisor Finesse案頭佈局中配置「即時資料」小工具後，請登入代理、Supervisor和報告使用者。驗證「即時資料」小工具是否正確載入，初始資料是否填充到該小工具中，以及當基礎資料發生更改時資料是否刷新。
- 嘗試從瀏覽器連線到兩個UCCX節點上的AppAdmin URL。確認系統提示登入頁面時沒有出現憑證警告。

疑難排解

問題 — 使用者ID/密碼無效

UCCX Finesse代理無法登入，錯誤為「Invalid User ID/Password」。

原因

Unified CCX引發異常「SSLHandshakeException」，並且無法與Unified CM建立連線。

解決方案

- 驗證Unified CM Tomcat證書是否未過期。
- 確保您在Unified CM中上載的任何證書均具有標籤為關鍵擴展的任何一個：
 - X509v3金鑰用法(OID - 2.5.29.15)
 - X509v3基本限制(OID - 2.5.29.19)如果將任何其他擴展標籤為重要，由於Unified CM證書驗證失敗，Unified CCX和Unified CM之間的通訊將失敗。

問題 — CSR SAN和證書SAN不匹配

上傳CA簽名的憑證會顯示錯誤「CSR SAN和憑證SAN不匹配」。

原因

CA可能已在證書使用者替代名稱(SAN)欄位中新增另一個父域。預設情況下，CSR將具有以下SAN:

```
SubjectAltName [  
  example.com(dNSName)  
  hostname.example.com(dNSName)  
]
```

CA可能傳回具有新增到憑證中的其他SAN的憑證：www.hostname.example.com。在這種情況下，憑證將具有額外的SAN:

```
SubjectAltName [  
  example.com(dNSName)  
  hostname.example.com(dNSName)  
  
  www.hostname.example.com(dNSName)  
]
```

這會導致SAN不匹配錯誤。

解決方案

在UCCX「生成證書簽名請求」頁的「主體替代名稱(SAN)」部分中，生成帶有空父域欄位的CSR。如此一來，不會使用SAN屬性來產生CSR，CA可以格式化SAN，且將憑證上傳到UCCX時

，不會出現SAN屬性不相符的情況。請注意，「父域」欄位預設為UCCX伺服器的域，因此在配置CSR的設定時必須明確刪除該值。

問題 — NET::ERR_CERT_COMMON_NAME_INVALID

當您訪問任何UCCX、MediaSense或SocialMiner網頁時，會收到錯誤消息。

「您的連線不是專用的。」

攻擊者可能正在嘗試從<Server_FQDN>竊取您的資訊（例如，密碼、消息或信用卡）。
NET::ERR_CERT_COMMON_NAME_INVALID

此伺服器無法證明它是<Server_FQDN>;其安全證書來自[missing_subjectAltName]。這可能是由配置錯誤或攻擊者攔截您的連線造成的。」

原因

Chrome版本58引入了新的安全功能，它報告網站的公共名稱(CN)沒有作為SAN包含時，其證書是不安全的。

解決方案

- 您可以導航到**Advanced > Proceed to <Server_FQDN>(unsafe)**，以繼續訪問站點並接受證書錯誤。
- 您可以使用CA簽名的憑證完全避免錯誤。生成CSR時，伺服器的FQDN作為SAN包括在內。CA可以對CSR進行簽名，在將已簽名的證書上傳回伺服器後，伺服器的證書將在SAN欄位中具有FQDN，因此不會顯示錯誤。

更多資訊

請參見[Chrome 58中Deprecations and Removing](#)中的「[刪除證書中對commonName匹配的支援](#)」部分。

證書缺陷

- 思科錯誤ID [CSCvb46250](#) - UCCX:Tomcat ECDSA證書對Finesse Live Data的影響
- 思科錯誤ID [CSCvb58580](#) — 無法使用RSA CA簽名的tomcat和tomcat-ECDSA登入到SocialMiner
- 思科錯誤ID [CSCvd56174](#) - UCCX:由於SSLHandshakeException，Finesse代理登入失敗
- 思科漏洞ID [CSCuv89545](#) - Finesse日誌堵塞漏洞

相關資訊

- [瞭解UCCX解決方案中的ECDSA證書](#)
- [適用於UCCX的SHA 256支援](#)
- [UCCX簽名和自簽名證書配置示例](#)

- [技術支援與文件 - Cisco Systems](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。