管理SPOG的PCCE元件證書

目錄

簡介

本檔案介紹如何將管理工作站(AW)自簽名SSL憑證交換至客戶語音入口網站(CVP)、Finesse、思科企業聊天與電子郵件(ECE)、思科整合情報中心(CUIC)、思科身分識別服務(idS)和適用於套裝客服中心企業版(PCCE)單一平台(SPOG)的虛擬化語音瀏覽器(VVB)。

作者：Nagarajan Paramasivam和Robert Rogier，思科TAC工程師。

必要條件

需求

思科建議您瞭解以下主題：

- 套裝/整合客服中心企業版(PCCE/UCCE)
- VOS平台
- 憑證管理
- 證書金鑰庫

採用元件

本檔案中的資訊是根據以下元件：

- 管理工作站(CCEADMIN/SPOG)
- CVP
- Finesse
- CUIC、IDS
- VVB
- Cisco ECE

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。

PCCE PCCE

新使用者介面 — SPOG

Packaged CCE 12.0擁有新的使用者介面，與其他聯絡中心應用程式一致。使用者介面允許您通過一個應用程式配置解決方案。登入新的Unified CCE Administration，網址為https://<IP Address>/cceadmin。<IP Address>是A端或B端Unified CCE AW或可選外部HDS的地址。

在此版本中，Unified CCE Administration介面允許您進行以下配置：

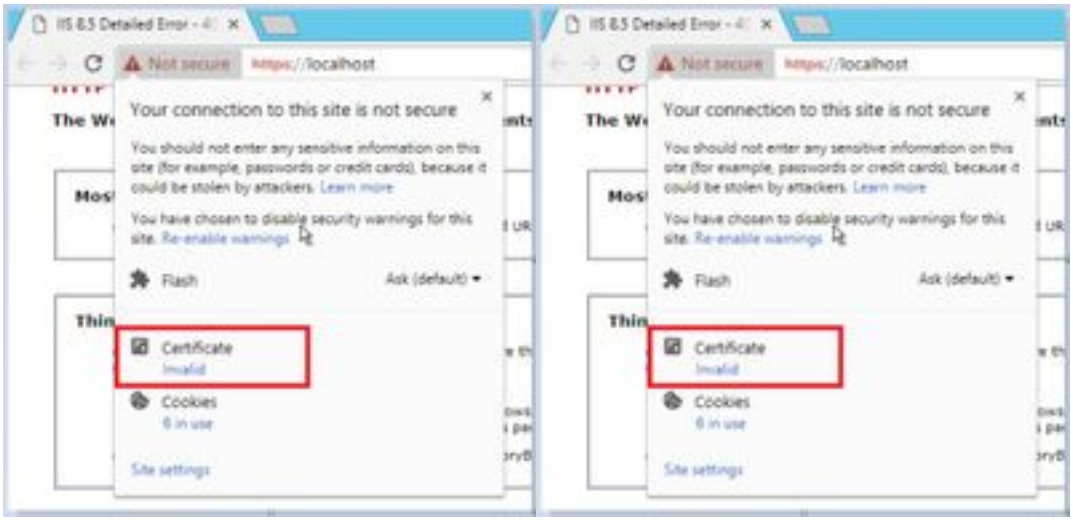
- 活動
- 禮貌回撥
- SIP伺服器組
- 檔案傳輸：只能通過主體AW傳輸檔案(在2000代理部署中為A端AW，在4000代理和代理部署12000配置AW)。
- 路由模式：統一CVP操作控制檯中的撥號號碼模式現在稱為統一CCE管理中的路由模式。
- 位置：在Unified CCE管理中，路由代碼現在是位置字首而不是站點ID。
- 裝置配置：Unified CCE Administration允許您配置以下裝置：CVP伺服器、CVP報告伺服器、VVB、Finesse、身份服務（單點登入設定）。
- 團隊資源：Unified CCE Administration允許您為座席小組定義和關聯以下資源：呼叫變數佈局、案頭佈局、電話簿、工作流、原因（未就緒、註銷、話後工作）。
- 電子郵件和聊天

在嘗試通過SPOG管理系統之前，需要在客戶語音門戶(CVP)、Finesse、思科企業聊天與電子郵件(ECE)、思科統一情報中心(CUIC)、思科身份服務(idS)和虛擬語音瀏覽器(VVB)以及管理工作站(AW)之間交換SSL證書，以建立信任通訊。

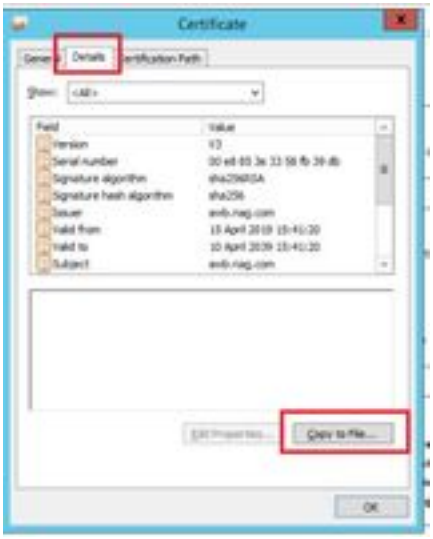
SSL憑證匯出

管理工作站(AW)

步驟1.訪問AW伺服器中的https://localhost URL，並下載伺服器SSL證書。



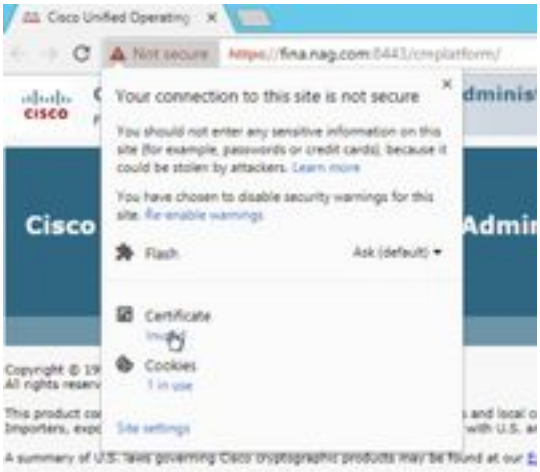
步驟2.在證書視窗中，導航到「詳細資訊」頁籤，然後按一下「複製到檔案」按鈕。



步驟3.選擇Base-64編碼的X.509(CER)，並將證書儲存在本地儲存中。

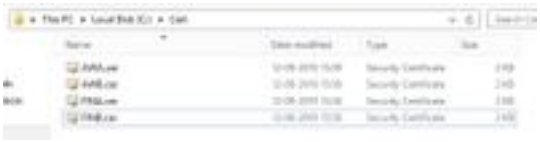
Finesse

步驟1。存取https://Finesseserver:8443/cmplatform並下載tomcat憑證。



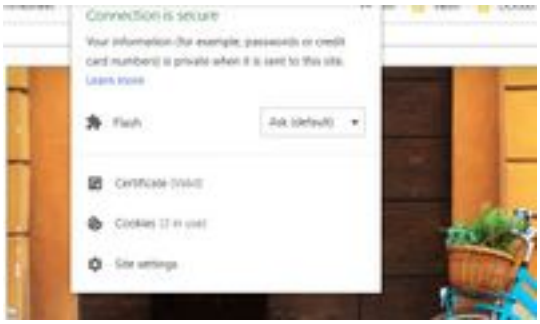
步驟2.在證書視窗中，導航到「詳細資訊」頁籤，然後按一下「複製到檔案」按鈕。

步驟3.選擇Base-64 encoded X.509(CER)，將證書儲存在本地儲存中。



Cisco ECE

步驟1.訪問https://ECEWebServer並下載伺服器SSL證書。

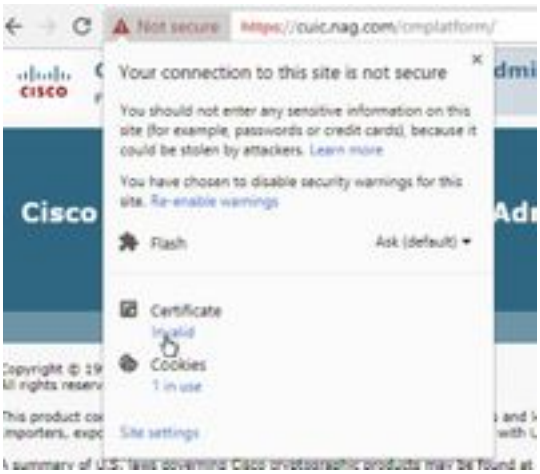


步驟2.在證書視窗中，導航到「詳細資訊」頁籤，然後按一下「複製到檔案」按鈕。

步驟3.選擇Base-64 encoded X.509(CER)，將證書儲存在本地儲存中。

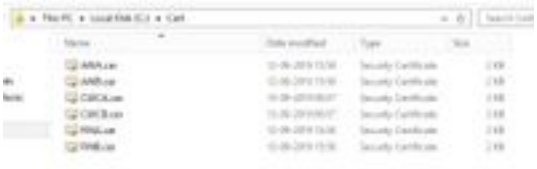
CUIC

步驟1。存取https://CUICServer:8443/cmplatform並下載tomcat憑證。



步驟2.在證書視窗中，導航到「詳細資訊」頁籤，然後按一下「複製到檔案」按鈕。

步驟3.選擇Base-64 encoded X.509(CER)，將證書儲存在本地儲存中。

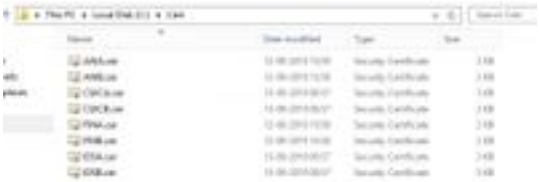


Cisco idS

步驟1。存取https://IDSServer:8553/idsadmin/並下載tomcat憑證。

步驟2.在證書視窗中，導航到「詳細資訊」頁籤，然後按一下「複製到檔案」按鈕。

步驟3.選擇Base-64 encoded X.509(CER)，將證書儲存在本地儲存中。

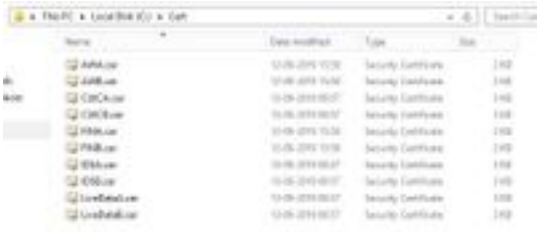


LiveData

步驟1。存取https://LiveDataServer:8444/cuic/gadget/LiveData/並下載tomcat憑證。

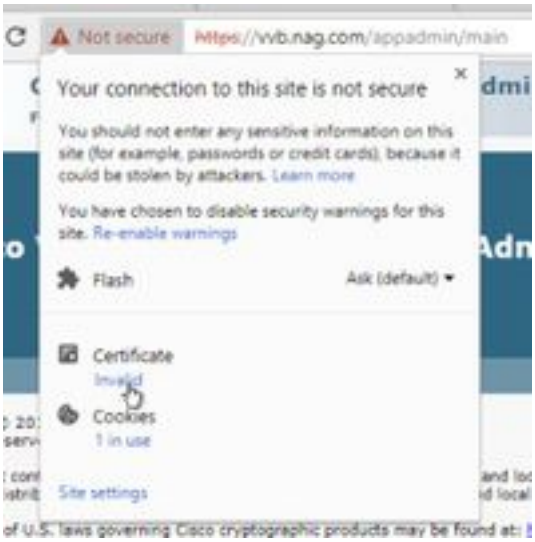
步驟2.在證書視窗中，導航到「詳細資訊」頁籤，然後按一下「複製到檔案」按鈕。

步驟3.選擇Base-64 encoded X.509(CER)，將證書儲存在本地儲存中。



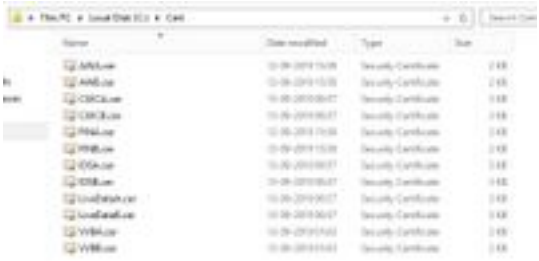
VVB

步驟1。存取https://VVBServer/appadmin/main並下載tomcat憑證。



步驟2.在證書視窗中，導航到「詳細資訊」頁籤，然後按一下「複製到檔案」按鈕。

步驟3.選擇Base-64 encoded X.509(CER)，將證書儲存在本地儲存中。



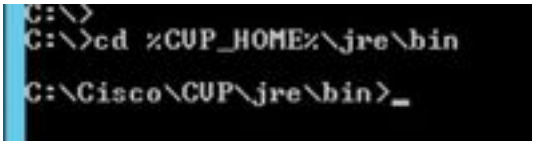
SSL證書匯入到金鑰庫

CVP通話伺服器和報告伺服器

步驟1.登入到CVP伺服器，並將AW CCE管理員證書複製到**C:\cisco\cvp\conf\security**。

步驟2.導航到**%CVP_HOME%\conf**，然後開啟security.properties以複製金鑰庫密碼。

步驟3.以管理員身份開啟命令提示符並運行命令**cd %CVP_HOME%\jre\bin**。



步驟4.使用此命令將AW證書匯入CVP伺服器。

keytool -import -trustcacerts -keystore %CVP_HOME%\conf\security\.keystore -storetype JCEKS -alias awa.nag.com -file C:\Cisco\CVP\conf\security\AWA.cer

步驟5.在密碼提示時，貼上從security.properties複製的密碼。

步驟6.鍵入**yes**以信任證書，並確保您獲得已將結**果證書新增到金鑰庫中。**

步驟7.成功匯入時系統提示警告。這是由於專有格式Keystore造成的，您可以忽略它。

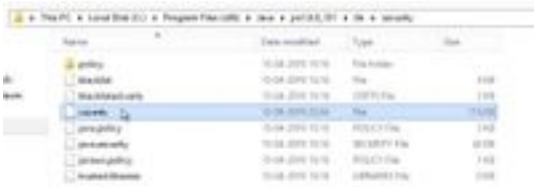
警告：

JCEKS金鑰庫使用專有格式。建議使用"keytool -importkeystore -srckeystore C:\Cisco\CVP\conf\security\.keystore -destkeystore C:\Cisco\CVP\conf\security\.keystore -deststoretype pkcs12"遷移到作為行業標準格式的PKCS12。

管理工作站

步驟1.登入到AW伺服器並以管理員身份開啟命令提示符。

步驟2.導航到C:\Program Files(x86)\Java\jre1.8.0_181\lib\security，並確保cacerts檔案存在。



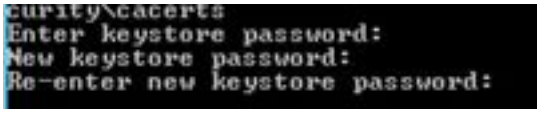
步驟3.鍵入命令**cd %JAVA_HOME%**並輸入。

步驟4.使用此命令將Finesse證書匯入AW伺服器。

keytool -import -file C:\Users\Administrator.NAG\Downloads\Cert\FINA.cer -alias fina.nag.com-keystore .\lib\security\cacerts

步驟5.首次使用此金鑰工具時，請使用密碼changeit來更改證書儲存的密碼。

步驟6.輸入金鑰庫的新密碼，然後重新輸入以確認該密碼。



步驟7.鍵入yes以信任證書，並確保獲得已將**結果證書新增到金鑰庫。**

附註：對於所有其他Finesse節點和所有CUIC節點，應重複第1步至第7步

步驟8.如果金鑰庫密碼輸入錯誤，或者執行步驟時未重置，則預計會出現此異常。

是否信任此證書？[否]: 是

證書已新增到金鑰庫

keytool錯誤：java.io.FileNotFoundException:.\lib\security\cacerts（系統找不到指定的路徑）

輸入金鑰庫密碼：
keytool錯誤：java.io.IO異常：**金鑰庫被篡改，或密碼不正確**

步驟9.若要變更金鑰庫密碼，請使用此命令，並使用新密碼重新開始步驟4中的過程。

keytool -storepasswd -keystore .\lib\security\cacerts

步驟10.成功匯入後，使用此命令檢視金鑰庫中的證書。

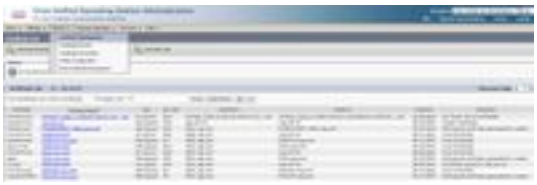
keytool -list -keystore .\lib\security\cacerts -alias fina.nag.com

keytool -list -keystore .\lib\security\cacerts -alias cuic.nag.com

Finesse、CUIC、Cisco idS和VVB

步驟1.登入到Finesse伺服器作業系統管理頁面並上傳tomcat信任中的AW SSL證書。

步驟2.導覽至**OS Administration > Security > Certificate Management。**



步驟3.點選Upload Certificate\Certificate Chain並從下拉選單中選擇tomcat-trust。

步驟4.瀏覽本地儲存中的證書儲存並點選Upload按鈕。

步驟5.重複以上步驟，將所有AW伺服器證書上傳到Finesse群集。

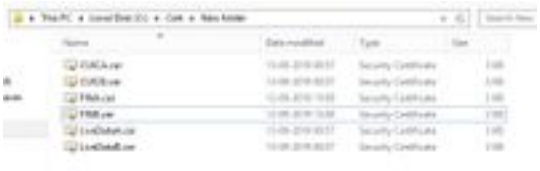
tomcat-trust

步驟6.重新啟動tomcat服務以使證書更改生效。

步驟7.在CUIC、IDS和VVB中，執行從2到4的步驟並上傳AW證書。

Finesse和CUIC/LiveData之間的證書交換

步驟1.將Finesse、CUIC和LiveData證書儲存在單獨的資料夾中。



2.Finesse、CUIC和LiveData OS管理頁面。

步驟3.導覽至**OS Administration > Security > Certificate Management。**

步驟4.點選Upload Certificate\Certificate Chain並從下拉選單中選擇tomcat-trust。

步驟5.瀏覽本地儲存中的證書儲存區並選擇Servers certificate（如下所述），然後按一下Upload（上傳）按鈕。

在Finesse伺服器中 — 作為Tomcat信任的CUIC和LiveData

在CUIC伺服器中 — Finesse和LiveData作為tomcat信任

在LiveData Server — 作為Tomcat信任的CUIC和Finesse

附註：不要求將tomcat-trust證書上傳到輔助節點，這將自動複製。

步驟6.在每個節點上重新啟動tomcat服務以使證書更改生效。