

如何從CUCM為思科網真IX5000/IX5200沈浸式終端安裝CAPF證書

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本檔案介紹如何從Cisco Unified Communications Manager(CUCM)為IX5000/IX5200沈浸式終端使用憑證授權代理功能(CAPF)安裝憑證。

必要條件

需求

思科建議您瞭解以下主題：

- IX系統 (沈浸式合作系統) 的工作知識
- CUCM知識(思科統一通訊管理器)

採用元件

本檔案中的資訊是根據以下元件：

- IX5000/IX5200
- CUCM

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

當Cisco TelePresence IX系統收到來自身份驗證器的身份驗證質詢時，裝置會使用製造安裝證書(MIC)或本地有效證書(LSC)進行響應。

如果同時安裝了MIC和LSC，系統將使用LSC進行身份驗證。如果未安裝LSC，在這種情況下

，Cisco TelePresence IX裝置會使用MIC，因為MIC由製造商內建到系統中。

為了使用LSC驗證Cisco TelePresence IX系統，您必須使用Unified CM中的證書頒發機構代理功能(CAPF)，將其手動安裝到系統上。

設定

本節提供了所需的配置步驟。

步驟1.登入到CUCM管理介面。

步驟2. 完成後續步驟，將安全配置檔案新增到Cisco TelePresence IX系統：

1. 選擇**Device > Phone**
 2. 選擇Findto查詢要配置的現有Cisco TelePresence IX系統
 3. 向下滾動到**Protocol Specific Information**框，並找到**Device Security**下拉選單
 4. 在「**Device Security Profile**」下拉選單中，選擇「**Secure security profile**」
 5. 向下滾動到「**Certification Authority Proxy Function(CAPF)Information**」框，然後更改這些設定
- 對於**Certificate Operation**，選擇**Install/Upgrade**
 - 對於**Authentication Mode**，選擇**By Authentication String**

此圖提供憑證授權單位代理功能(CAPF)資訊框的範例：

Certification Authority Proxy Function (CAPF) Information

Certificate Operation*

Authentication Mode*

Authentication String

Key Size (Bits)*

Operation Completes By (YYYY:MM:DD:HH)

Certificate Operation Status: Upgrade Success

Note: Security Profile Contains Addition CAPF Settings.

6.選擇**Generate String**以生成唯一字串。

記下生成的字串，因為您必須進一步使用此字串。

步驟3. 選擇**儲存**，然後選擇**應用配置**以儲存設定。

步驟4.登入到IX5000/IX5200管理介面。

1. **SelectConfiguration > Call Control Manager**
2. 在「**CAPF Authentication String**」欄位中，輸入在上一步中從CUCM生成的身份驗證字串
3. **SelectApply**並**重新啟動IX5000/IX5200**

此示例提供了IX呼叫控制管理器介面的示例：



驗證

使用本節內容，確認您的組態是否正常運作。

IX5000/IX5200系統啟動並運行後，在成功完成CAPF過程後，登入到IX5000/IX5200管理介面。

步驟1. **SelectConfiguration > Certificates**

步驟2. 在憑證清單中會看到檔案名稱為capf0.pem的CAPF憑證

此圖提供IX5000/IX5200系統的證書列表示例：

Filename	Type
sudiPub.pem	Misc Certificate
LSC01.pem	Locally Significant Certificate
capf0.pem	CAPF Certificate
sudiCAroot.pem	Misc Certificate
ccm2.pem	Call Manager Certificate
sudiCAsub.pem	Misc Certificate
ccm1.pem	Call Manager Certificate
ccm0.pem	Call Manager Certificate

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

如果CAPF過程失敗，則不會在證書清單中看到CAPF證書（如上圖所示）。使用以下步驟排除此類情況的故障：

步驟1. 登入到IX5000/IX5200命令列介面(CLI)。運行命令**show security authstring**。

如果此命令返回與CUCM之前生成的字串相同的字串，則確認身份驗證已完成，但IX5000/IX5200無法下載證書。

步驟2.登入到IX5000/IX5200管理介面：

1. **SelectConfiguration > Call Control Manager**
2. 選擇**Delete Certificate Trust List**按鈕
3. 選擇**Apply**,IX5000/IX5200將重新啟動

此示例提供了IX呼叫控制管理器介面的示例：



Call Control Manager

TFTP

Automatic Manual

TFTP Server 1
[Redacted IP]6

TFTP Server 2

TFTP Server 4

TFTP Server 5

CAPF Authentication String

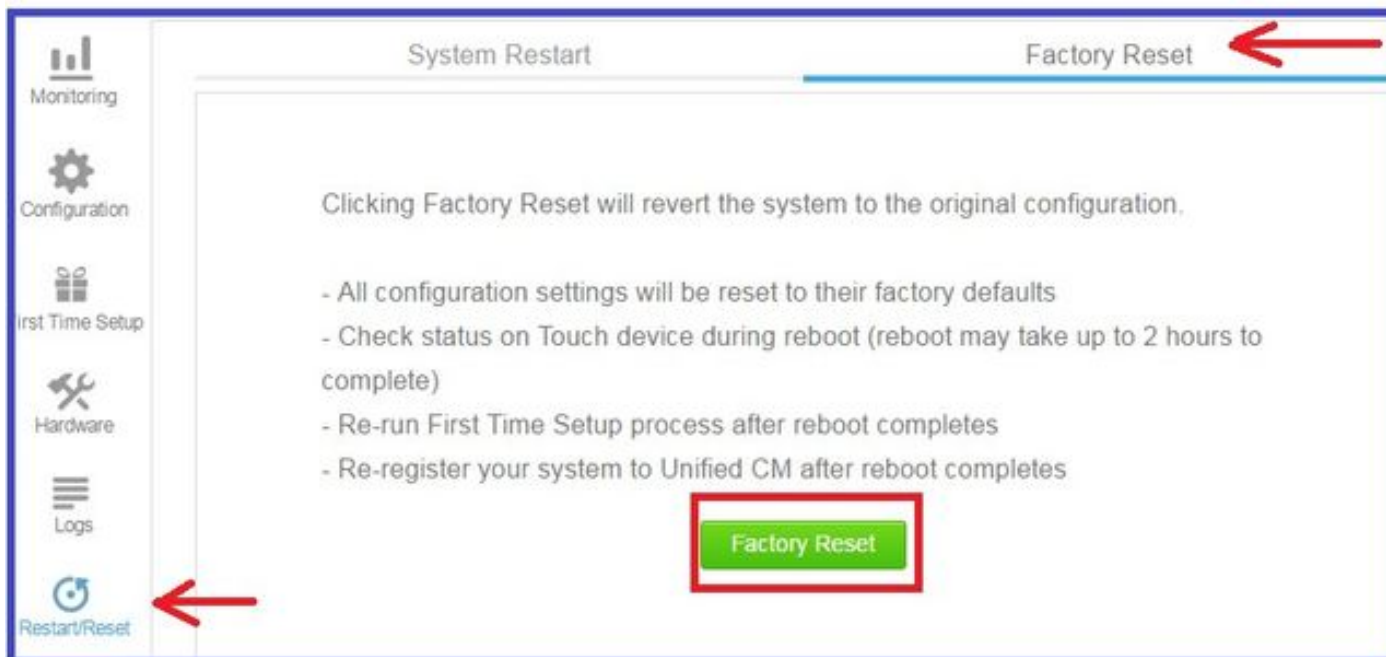
Delete Certificate Trust List ←

如果CAPF證書在Certificate清單中仍然看不到，則使用步驟3中提供的步驟出廠重置裝置。

步驟3.登入到IX5000/IX5200管理介面：

1. 選擇**Restart/Reset > Factory Reset**
2. **SelectFactory**重置

此映像提供如何在IX5000/IX5200系統上執行出廠重設的範例：



相關資訊

- [技術支援與文件 - Cisco Systems](#)
- [Cisco TelePresence IX5000系列](#)
- [Cisco TelePresence IX2000系列](#)