Installation des CAPF-Zertifikats für Cisco TelePresence IX5000/IX5200 immersive Endgeräte vom CUCM

Inhalt

Einführung

Dieses Dokument beschreibt die Installation des Zertifikats mithilfe der CAPF (Certificate Authority Proxy Function) für die immersiven IX500/IX5200-Endpunkte von Cisco Unified Communications Manager (CUCM).

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Arbeitskenntnisse der IX-Systeme (Immersive Collaboration-Systeme)
- Kenntnisse von CUCM (Cisco Unified Communications Manager)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Komponenten:

- IX5000/IX5200
- CUCM

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Wenn das Cisco TelePresence IX-System eine Authentifizierungsproblem von einem Authentifizierer erhält, antwortet das Gerät entweder mit dem MIC (Manufacturing Installed Certificate) oder dem LSC (Locally Significant Certificate).

Wenn sowohl MIC als auch LSC installiert sind, authentifiziert das System das LSC. Wenn das LSC nicht installiert ist, verwendet die Cisco TelePresence IX-Einheit das MIC, da das MIC vom Hersteller in das System integriert wurde.

Um das Cisco TelePresence IX-System mithilfe des LSC zu authentifizieren, müssen Sie es manuell mithilfe der CAPF (Certificate Authority Proxy Function) des Unified CM auf Ihrem System installieren.

Konfigurieren

Dieser Abschnitt enthält die erforderlichen Konfigurationsschritte.

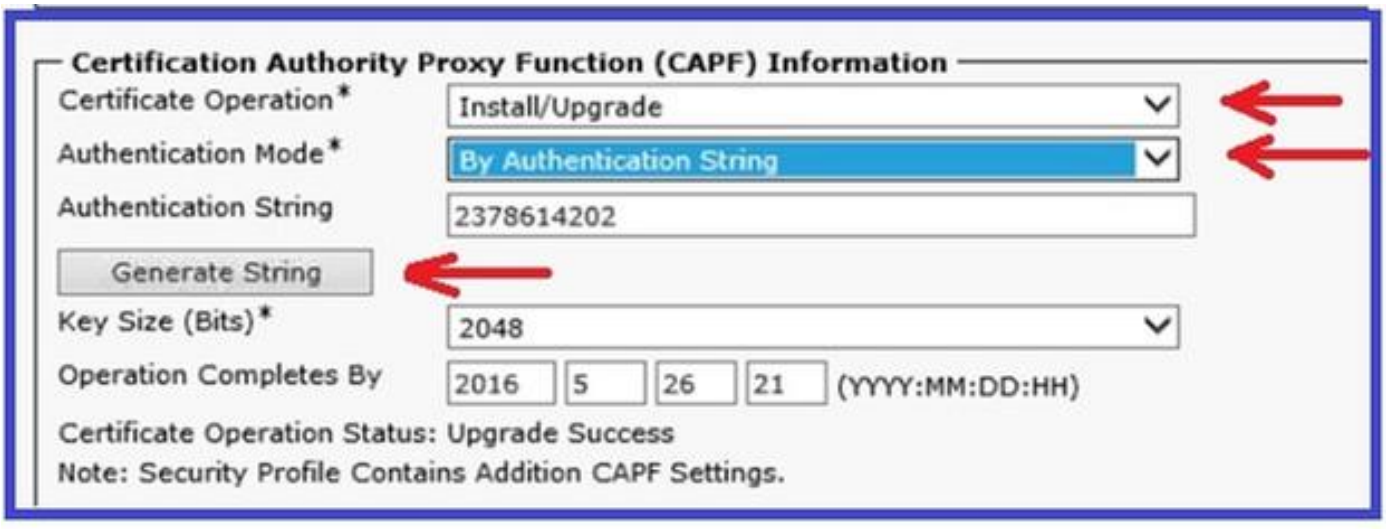
Schritt 1: Melden Sie sich bei der CUCM-Verwaltungsschnittstelle an.

Schritt 2: Fügen Sie das Sicherheitsprofil zum Cisco TelePresence IX-System hinzu, indem Sie die folgenden Schritte ausführen:

1. Wählen Sie **Gerät > Telefon aus**
2. Wählen Sie Suchen aus, um das vorhandene Cisco TelePresence IX-System zu finden, das Sie konfigurieren möchten.
3. Blättern Sie nach unten zum Feld **Protocol Specific Information (Protokollspezifische Informationen**), und suchen Sie die Dropdown-Liste **Device Security (Gerätesicherheit)**.
4. Wählen Sie in der Dropdown-Liste **Device Security Profile (Gerätesicherheitsprofil**) das **Secure Security**-Profil aus.
5. Blättern Sie nach unten zum Feld **Certification Authority Proxy Function** (CAPF)-Informationen, und ändern Sie diese Einstellungen.

- Wählen Sie für **Zertifikatvorgang Installation/Upgrade** aus.
- Wählen Sie im **Authentifizierungsmodus nach Authentifizierungszeichenfolge** aus.

Dieses Beispiel zeigt ein Beispiel für das CAPF-Informationsfeld (Certification Authority Proxy Function):



6. Wählen Sie **String generieren**, um eine eindeutige Zeichenfolge zu generieren.

Notieren Sie sich die generierte Zeichenfolge, da Sie diese Zeichenfolge weiter verwenden müssen.

Schritt 3: **Wählen Sie Speichern** und dann **Konfig. übernehmen**, um die Einstellungen zu speichern.

Schritt 4: Melden Sie sich an der Verwaltungsschnittstelle IX5000/IX5200 an.

1. Wählen SieKonfiguration > Anrufsteuerungs-Manager aus
2. Geben Sie im Feld **CAPF Authentication String** (CAPF-Authentifizierungszeichenfolge) die Authentifizierungszeichenfolge ein, die im vorherigen Schritt vom CUCM generiert wurde.
3. **Wählen Sie Apply aus, und der IX5000/IX5200 wird neu gestartet.**

Dieses Beispiel zeigt eine IX Call Control Manager-Schnittstelle:

Überprüfen

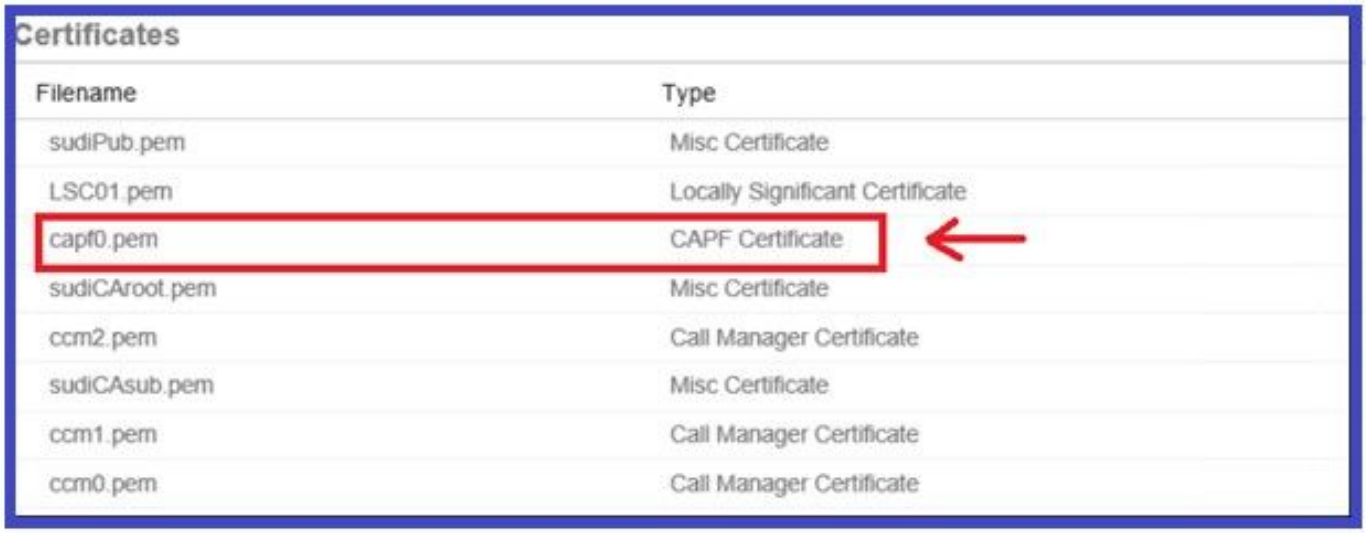
In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Sobald das IX5000/IX5200-System betriebsbereit ist und der CAPF-Prozess erfolgreich abgeschlossen ist, melden Sie sich an der IX5000/IX5200-Administrationsoberfläche an.

Schritt 1: Wählen SieKonfiguration > Zertifikate aus

Schritt 2: Das CAPF-Zertifikat wird in der Zertifikatsliste mit dem Dateinamen **capf0.pem** angezeigt.

Dieses Bild enthält ein Beispiel für eine Zertifikatsliste eines IX500/IX5200-Systems:



Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Wenn der CAPF-Prozess nicht erfolgreich ist, wird das CAPF-Zertifikat nicht in der Zertifikatsliste angezeigt (siehe vorheriges Bild). Führen Sie die folgenden Schritte aus, um eine Fehlerbehebung für ein solches Szenario durchzuführen:

Schritt 1: Melden Sie sich bei der IX5000/IX5200-Befehlszeilenschnittstelle (CLI) an. Führen Sie den Befehl **show security authstring aus**.

Wenn dieser Befehl die gleiche Zeichenfolge zurückgibt, die zuvor vom CUCM generiert wurde, bestätigt dies, dass die Authentifizierung erfolgt ist, das IX500/IX5200-Zertifikat kann jedoch nicht heruntergeladen werden.

Schritt 2: Melden Sie sich bei der Verwaltungsschnittstelle IX5000/IX5200 an:

1. Wählen SieKonfiguration > Anrufsteuerungs-Manager aus
2. Wählen Sie die Schaltfläche **Liste der Zertifikatsvertrauenslisten löschen**
3. Wählen Sie **Apply aus**, und der IX5000/IX5200 wird neu gestartet.

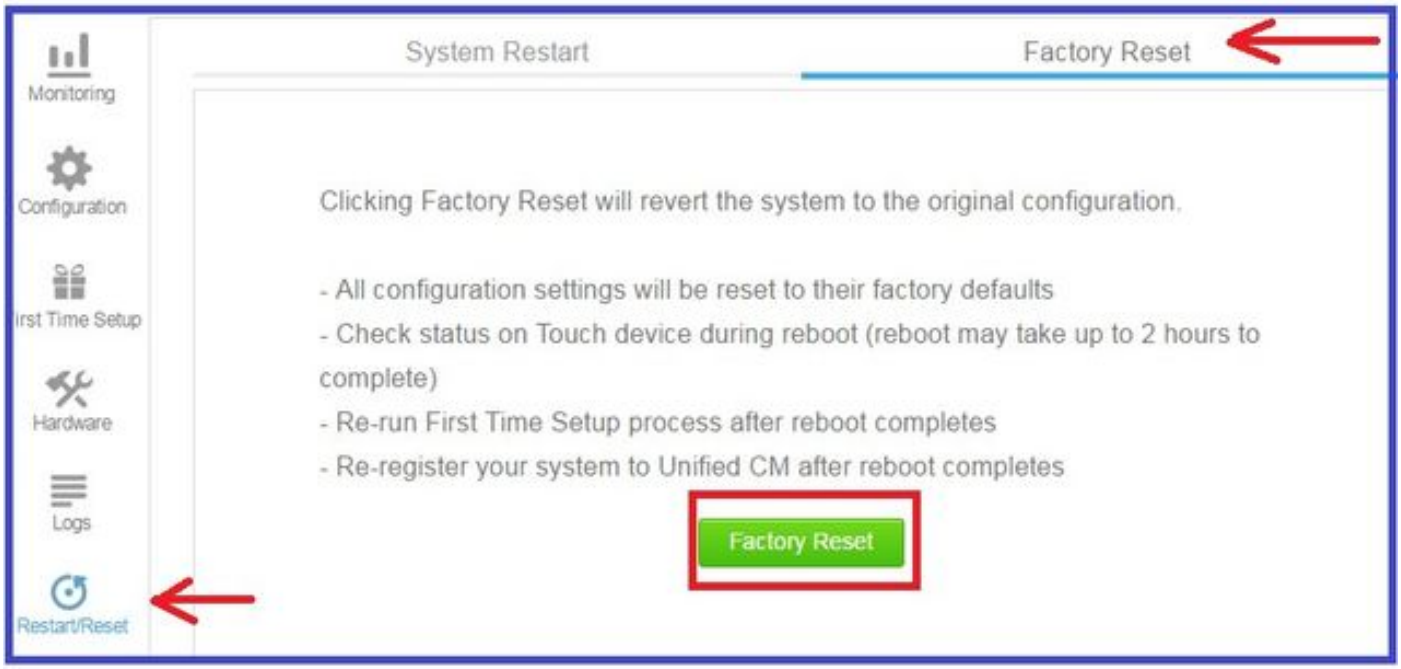
Dieses Beispiel zeigt eine IX Call Control Manager-Schnittstelle:

Wenn das CAPF-Zertifikat immer noch nicht in der Zertifikatsliste aufgeführt ist, setzen Sie das Gerät mithilfe der in Schritt 3 beschriebenen Schritte auf die Werkseinstellungen zurück.

Schritt 3: Melden Sie sich bei der Verwaltungsschnittstelle IX5000/IX5200 an:

1. Wählen Sie **Neu starten/Zurücksetzen > Werkseinstellungen aus.**
2. SelectFactory Zurücksetzen

Dieses Bild zeigt ein Beispiel für die Durchführung eines Zurücksetzens auf die Werkseinstellungen auf dem IX500/IX5200-System:



Zugehörige Informationen

- Technischer Support und Dokumentation - Cisco Systems

- Cisco TelePresence IX5000-Serie
- Cisco TelePresence IX2000-Serie