

Technische Anmerkung zum Generieren eines abgelaufenen Zertifikats für die einmalige Anmeldung

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Problem: Die Anmeldung schlägt mit "Ungültiger Benutzername oder ungültiges Kennwort" fehl.](#)

[Lösung](#)

Einführung

In diesem Dokument wird beschrieben, wie Sie ein SSO-Zertifikat (Single Sign-On) generieren, das abgelaufen ist.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse der CloudCenter-Version vor 4.7.2.1 verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf allen CloudCenter-Versionen vor 4.7.2.1.

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.

Problem: Die Anmeldung schlägt mit "Ungültiger Benutzername oder ungültiges Kennwort" fehl.

Bei der Anmeldung wird "Ungültiger Benutzername oder ungültiges Kennwort" angezeigt, obwohl das richtige Kennwort und der richtige Benutzername verwendet werden. Dies wird durch ein abgelaufenes Zertifikat für die einmalige Anmeldung verursacht. 4.7.2.1 enthält eine Fix für den Fall, dass die Zertifikate nicht ablaufen.

Lösung

Schritte zum Aktualisieren des Zertifikats:

Schritt 1: Laden Sie die angehängte Datei (**samlKeystore.jks**) in den CCM hoch. Im HA-Modus laden Sie die Datei auf beide CCMs hoch.

```
# cd /usr/local/tomcat/webapps/ROOT/WEB-INF/lib/ & mkdir ./security
# cp /tmp/samlKeystore.jks security/
```

Schritt 2: Aktualisieren der Cliqr Security-Bibliothek In diesem Beispiel verwenden wir Version 4.7.2.

```
# cp cliqr-security-4.7.2.jar ~/
# jar uf cliqr-security-4.7.2.jar security/samlKeystore.jks
# chown -R cliqruser:cliqruser cliqr-security-4.7.2.jar
# rm -rf security/
```

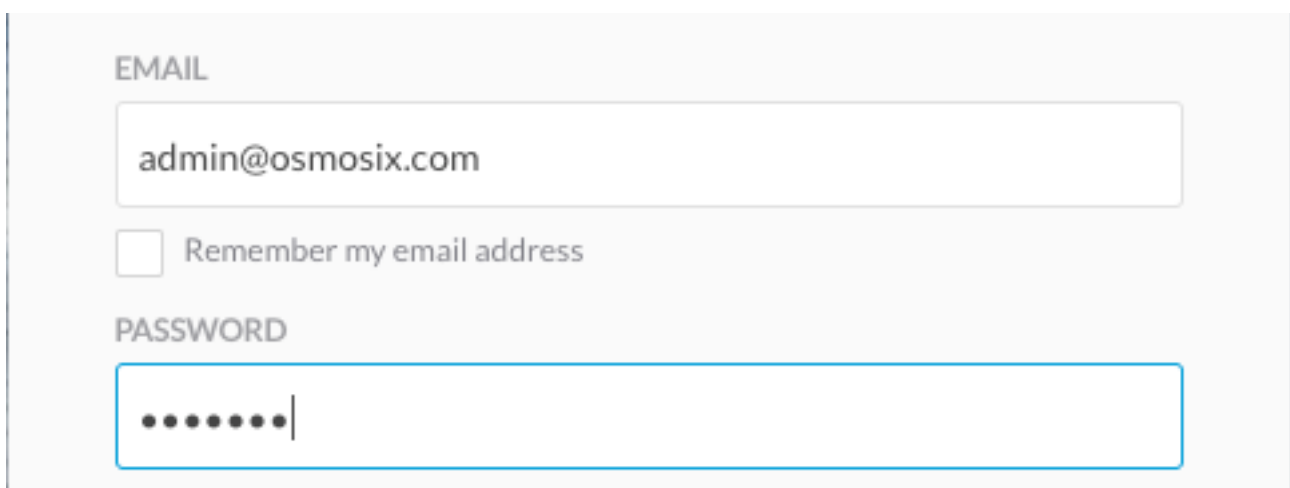
Schritt 3: Starten Sie den Tomcat-Dienst auf dem (primären) CCM neu.

```
# /etc/init.d/tomcat restart
```

Schritt 4: Beenden Sie im Fall des HA-Modus den Tomcat-Dienst auf dem sekundären CCM.

```
# /etc/init.d/tomcat stop
```

Schritt 5: Melden Sie sich beim CCM mit dem Benutzer admin@osmosix.com an.

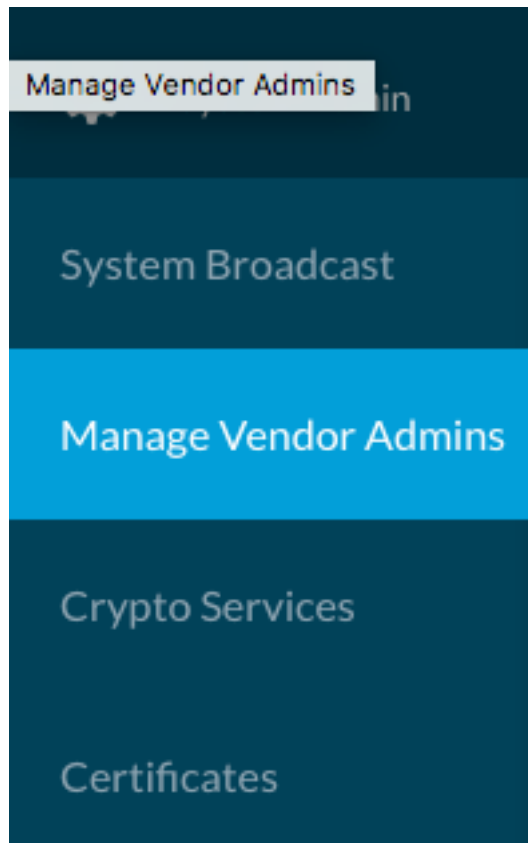


EMAIL

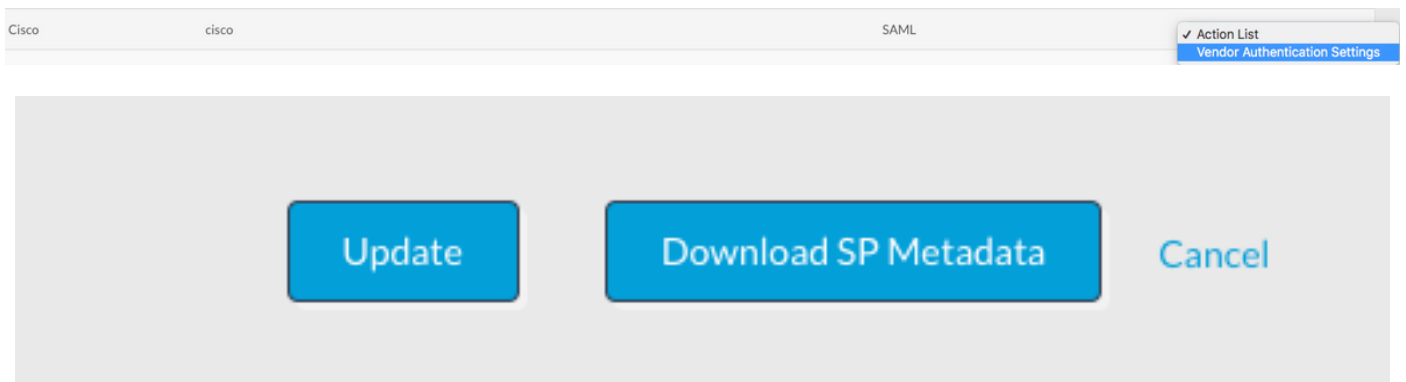
Remember my email address

PASSWORD

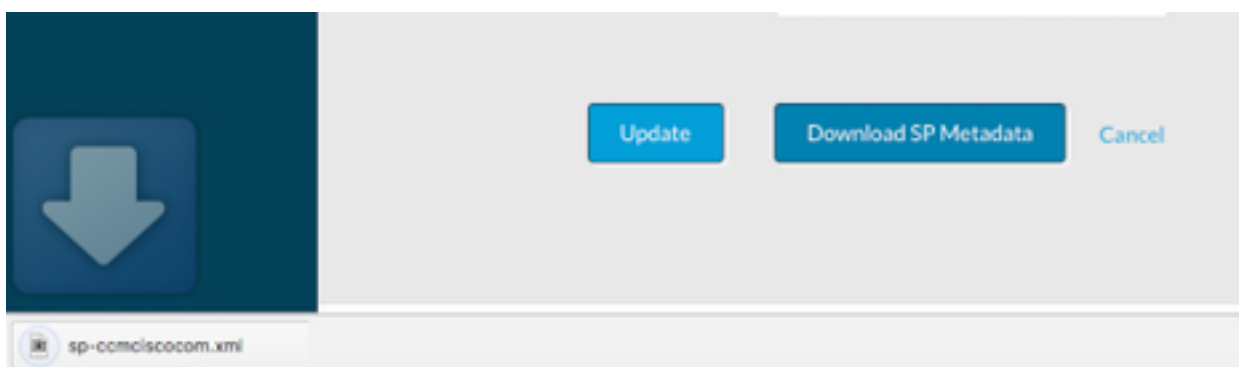
Schritt 6: Klicken Sie auf **Anbieter-Administratoren verwalten**.



Schritt 7: Wählen Sie **Authentifizierungseinstellungen** für den Tenant aus, gehen Sie zum unteren Bildschirmrand, und klicken Sie auf die **Schaltfläche Aktualisieren**. Dadurch wird die entsprechende Metadatendatei aktualisiert.



Schritt 8: Drücken Sie die Schaltfläche SP Metadata herunterladen, um die XML-Datei herunterzuladen.



Schritt 8.1. Kopieren Sie im HA-Modus die XML-Datei von CCM1 in CCM2, und stellen Sie sicher, dass die Berechtigungen mit CCM1 übereinstimmen. Speicherort des XML? in **/usr/local/osmosix/metadaten/sp/**.

```
From CCM1
# cd /usr/local/osmosix/metadata/sp
# scp <metadatafile>.xml root@CCM2:/usr/local/osmosix/metadata/sp
```

Schritt 8.2: Starten Sie den Tomcat-Dienst auf dem zweiten CCM.

```
From CCM2
# /etc/init.d/tomcat restart
```

Schritt 9: Laden Sie die XML-Datei auf IDP hoch.

Schritt 10: Wenn Sie eine CSC-Datei für Ihren IDP benötigen, öffnen Sie die XML-Datei, und kopieren Sie die Werte des privaten Schlüssels und Zertifikats in eine Textdatei. Formatieren Sie die Textdatei wie folgt:

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
<value for private key>
-----END ENCRYPTED PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
<value for certificate>
-----END CERTIFICATE-----
```

Schritt 11: Validieren Sie die Lösung, indem Sie sich anmelden.

Hinweis: Bei mehreren Tenants die Schritte 4 bis 8 für jeden Tenant wiederholen.