

有關如何生成過期單點登入證書的技術說明

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[問題：登入失敗並顯示「無效的使用者名稱或密碼」](#)

[解決方案](#)

簡介

本文說明如何生成已過期的單一登入(SSO)證書。

必要條件

需求

思科建議您瞭解4.7.2.1之前的CloudCenter版本

採用元件

本檔案中的資訊是根據4.7.2.1之前的所有CloudCenter版本

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。

問題：登入失敗並顯示「無效的使用者名稱或密碼」

儘管使用了正確的密碼和使用名稱，但登入仍失敗，顯示「無效使用者名稱或密碼」。這是由一次登入證書過期造成的。 4.7.2.1包含證書未到期的修補程式。

解決方案

更新證書的步驟：

步驟1.將附加的檔案(samlKeystore.jks)上傳到CCM。在HA模式中，將檔案上傳到兩個CCM。

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

步驟2.重新打包Cliqr安全庫。在本例中，我們使用的是4.7.2版。

```
# 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/
```

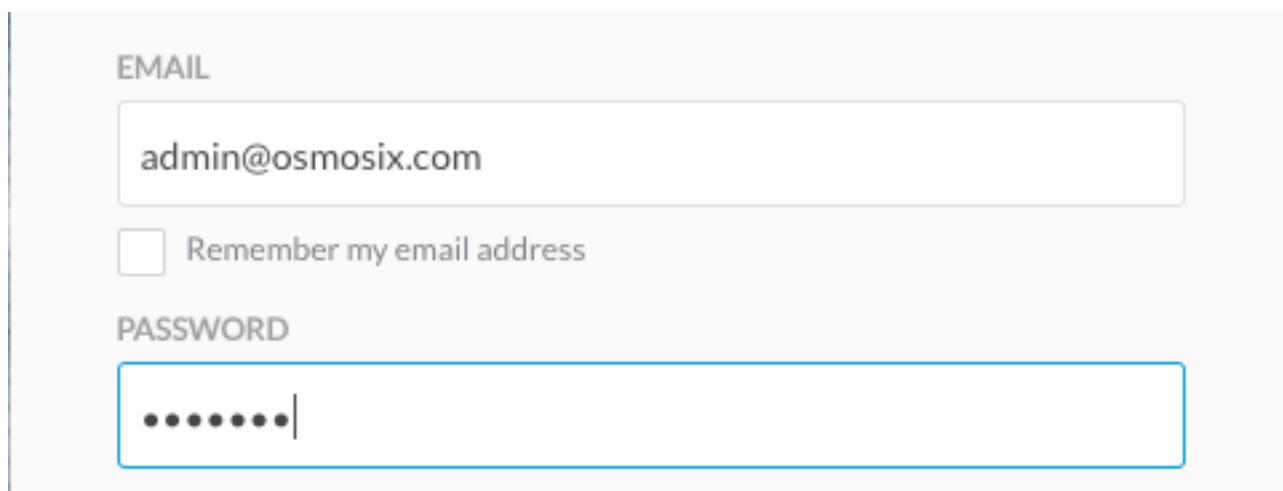
步驟3.在 (主) CCM上重新啟動Tomcat服務。

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

步驟4.在HA模式的情況下，停止輔助CCM上的Tomcat服務。

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

步驟5.使用admin@osmosix.com使用者登入CCM。

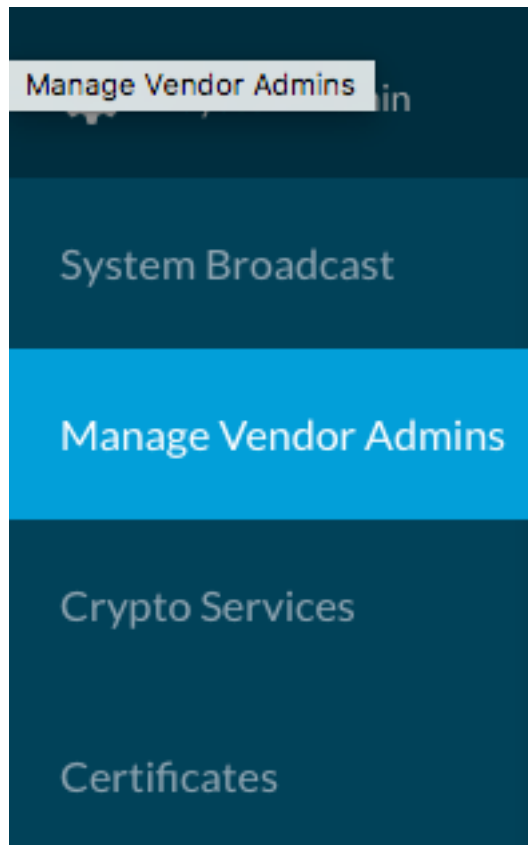


EMAIL

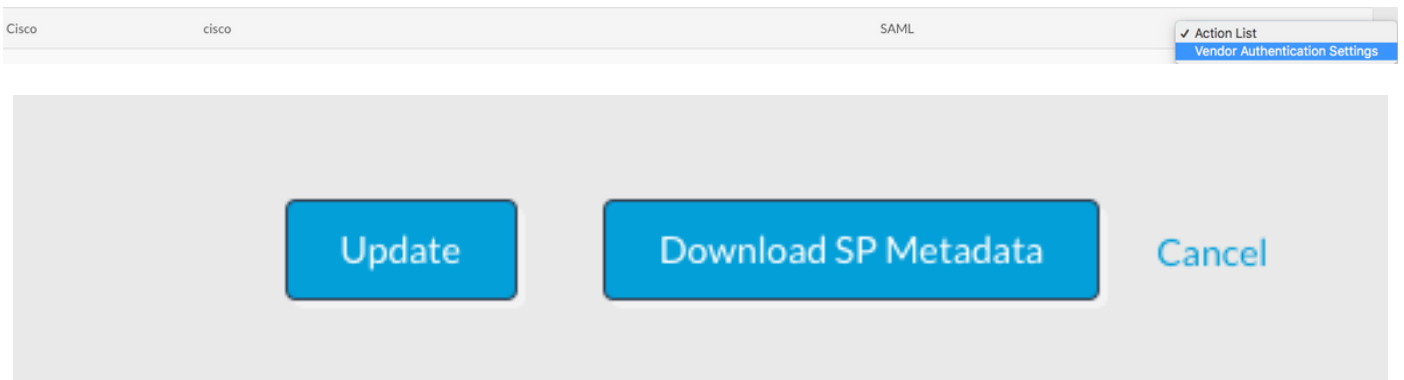
Remember my email address

PASSWORD

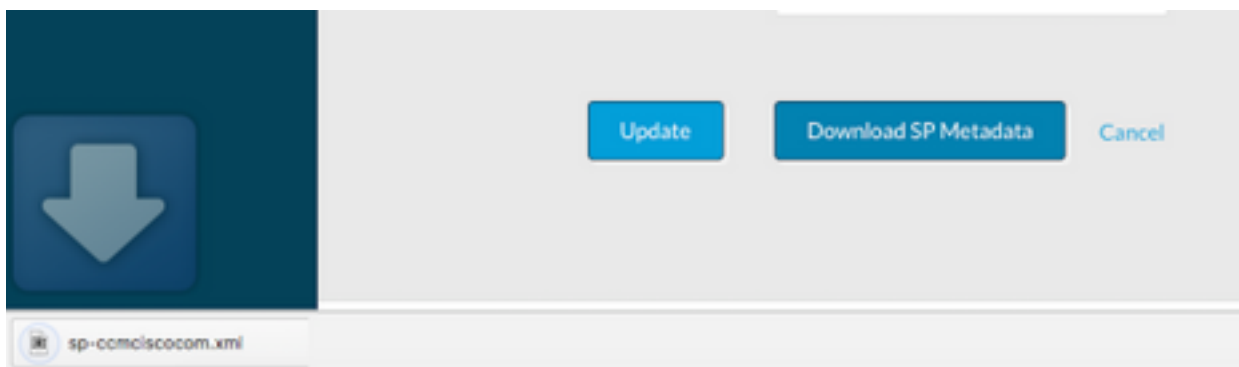
步驟6.按一下**Manage Vendor Admins**。



步驟7.選擇租戶的**Authentication settings**，轉至螢幕底部，然後按一下**Update**按鈕。這將更新相應的後設資料檔案。



步驟8.按「下載SP後設資料」按鈕下載XML檔案。



步驟8.1.對於HA模式，將xml檔案從CCM1複製到CCM2，確保許可權與CCM1相同。XML的位置

? 位於/usr/local/ossix/metadata/sp/。

From CCM1

```
# cd /usr/local/osmosix/metadata/sp
```

```
# scp <metadata>file.xml root@CCM2:/usr/local/osmosix/metadata/sp
```

步驟8.2.在第二個CCM上啟動Tomcat服務

From CCM2

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

步驟9.將XML檔案上傳到IDP。

步驟10.如果您的IDP需要.cer檔案，請開啟XML檔案，並將私鑰和證書的值複製到文本檔案中。文本檔案格式如下：

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
```

```
<value for private key>
```

```
-----END ENCRYPTED PRIVATE KEY-----
```

```
-----BEGIN CERTIFICATE-----
```

```
<value for certificate>
```

```
-----END CERTIFICATE-----
```

步驟11.通過登入驗證解決方案。

附註：對於多個租戶，對每個租戶重複步驟4至8。