Nota técnica en cómo generar solo expirada Muestra-en el certificado

Contenido

[Introducción](#)
[prerrequisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Problema: El login falla con el “nombre de usuario inválido o la contraseña”](#)
[Solución](#)

Introducción

Este documento describe cómo generar un solo Muestra-en el certificado (SSO) que ha expirado.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento de la versión anteriormente 4.7.2.1 de CloudCenter

Componentes Utilizados

La información en este documento se basa en todas las versiones de CloudCenter antes de 4.7.2.1

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Problema: El login falla con el “nombre de usuario inválido o la contraseña”

El login falla con el “nombre de usuario inválido o la contraseña” a pesar de la contraseña y el nombre de usuario correctos que son utilizados. Esto es causada por un solo expirada Muestra-en el certificado. 4.7.2.1 incluye un arreglo a donde no expiran los Certificados.

Solución

Pasos para poner al día el certificado:

Paso 1. Cargue el archivo adjunto (**samlKeystore.jks) a** CCM. En caso del modo HA, cargue el archivo a ambos CCM.

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

Paso 2. Empaquete la biblioteca de la Seguridad de nuevo de Cliqr. En este ejemplo, estamos utilizando la versión 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/
```

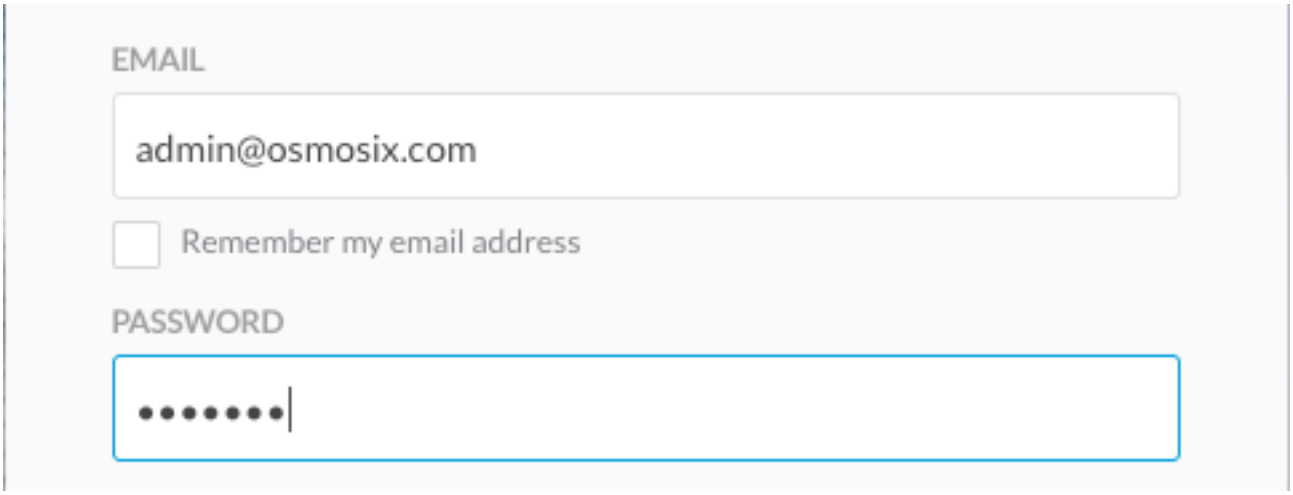
Paso 3. Servicio de Tomcat del reinicio en CCM (primario).

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

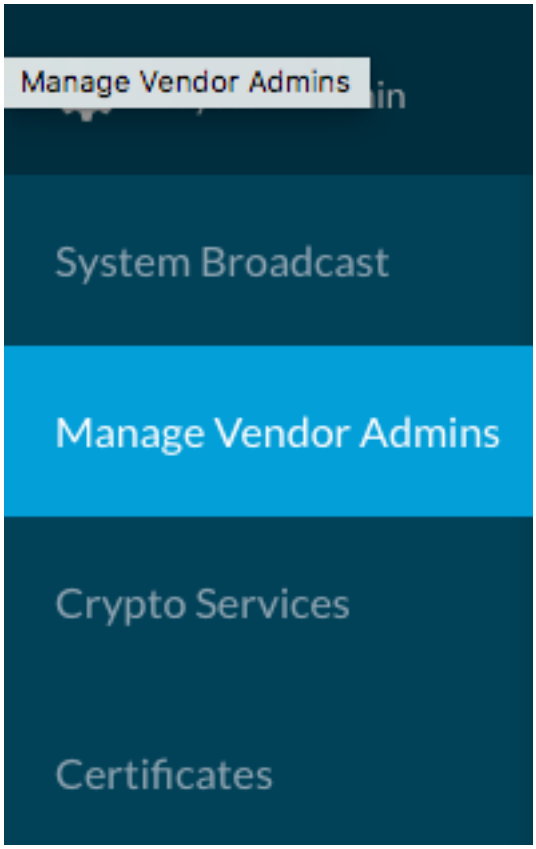
Paso 4. En caso del modo HA, pare el servicio de Tomcat en CCM secundario.

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

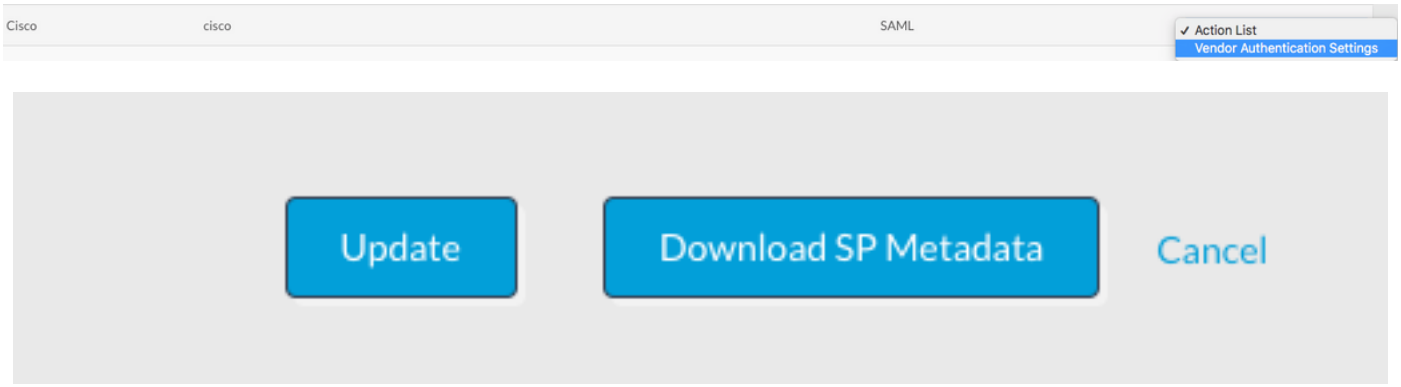
Paso 5. Login a CCM con el usuario de admin@osmosix.com.



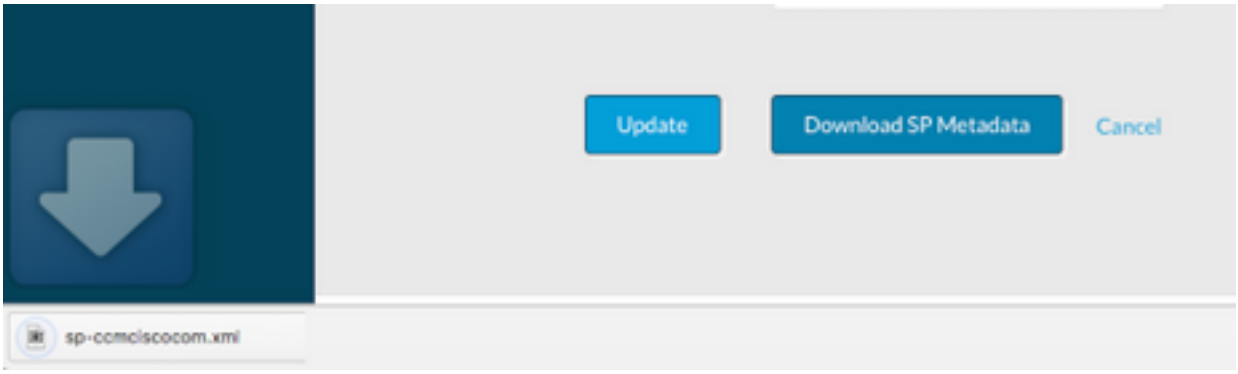
Paso 6. Haga clic en **manejan al vendedor Admins**.



Paso 7. Seleccione las **configuraciones de la autenticación** para el arrendatario, vaya a la parte inferior de la pantalla y haga clic en el **botón Update Button**. Esto pone al día el archivo de metadatos correspondiente.



Paso 8. Presione la descarga el botón de los meta datos SP para descargar el archivo XML.



El modo del paso 8.1.For HA, copia el archivo del xml de CCM1 a CCM2, se aseegura los permisos es lo mismo que CCM1. ¿Ubicación del XML? está en **/usr/local/osmosix/metadata/sp/**.

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

Paso 8.2. Comience el servicio de Tomcat en segundo CCM

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

Paso 9. Cargue el archivo XML a IDP.

Paso 10. Si usted necesita un archivo de .cer para su IDP, abra el archivo XML, y copie los valores de la clave privada y del certificado en un archivo de texto. Formate el archivo de texto como éstos:

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

Paso 11 Valide la solución abriendo una sesión.

Nota: En caso de los arrendatarios múltiples, relance los pasos 4 - 8 para cada arrendatario.