

Nota tecnica su come generare un certificato Single Sign-On scaduto

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Problema: Accesso non riuscito con "Nome utente o password non valida"](#)

[Soluzione](#)

Introduzione

In questo documento viene descritto come generare un certificato Single Sign-On (SSO) scaduto.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di CloudCenter release precedenti alla 4.7.2.1

Componenti usati

Le informazioni di questo documento si basano su tutte le versioni di CloudCenter precedenti alla 4.7.2.1

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Problema: Accesso non riuscito con "Nome utente o password non valida"

L'accesso non riesce con "Nome utente o password non valida" nonostante siano stati utilizzati la password e il nome utente corretti. Ciò è causato da un certificato Single Sign-On scaduto.

4.7.2.1 include una correzione in cui i certificati non scadono.

Soluzione

Passaggi per l'aggiornamento del certificato:

Passaggio 1. Caricare il file allegato (**samlKeystore.jks**) in CCM. In caso di modalità HA, caricare il file in entrambi i CCM.

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

Passaggio 2. Eseguire nuovamente il package della libreria di protezione Cliqr. In questo esempio viene utilizzata la versione 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/
```

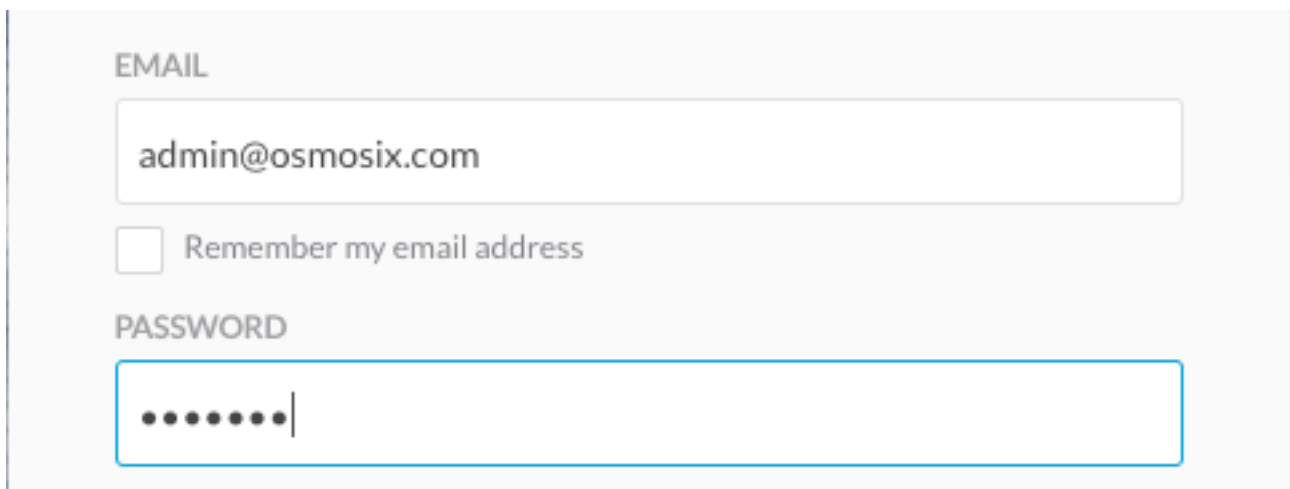
Passaggio 3. Riavviare il servizio Tomcat su CCM (principale).

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

Passaggio 4. In caso di modalità HA, arrestare il servizio Tomcat sul CCM secondario.

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

Passaggio 5. Accedere a CCM con l'utente admin@osmosix.com.

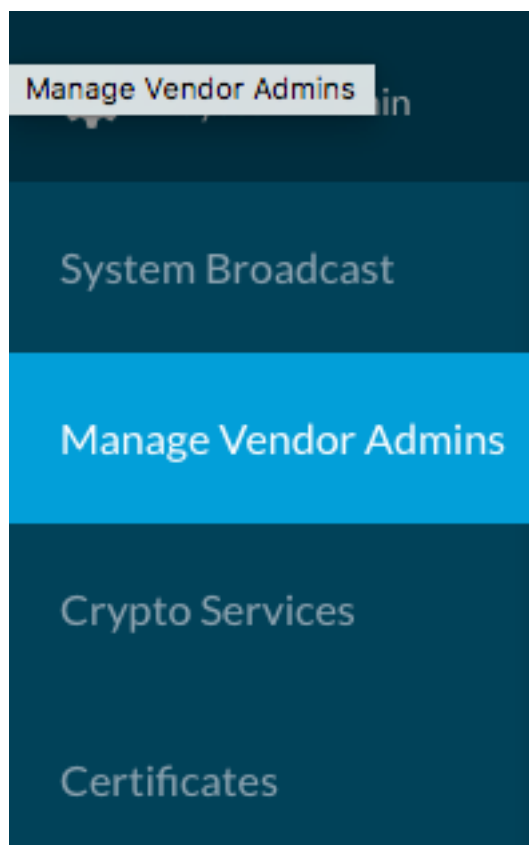


EMAIL

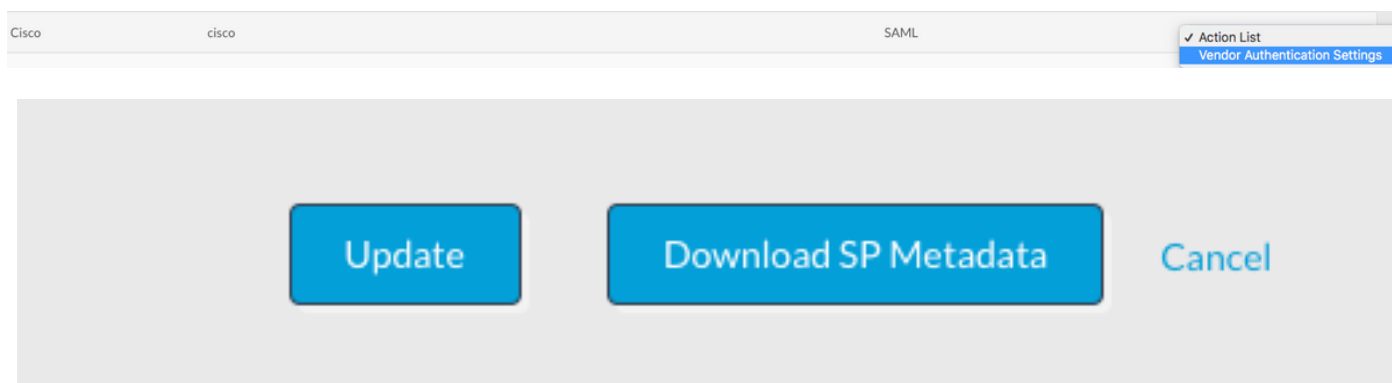
Remember my email address

PASSWORD

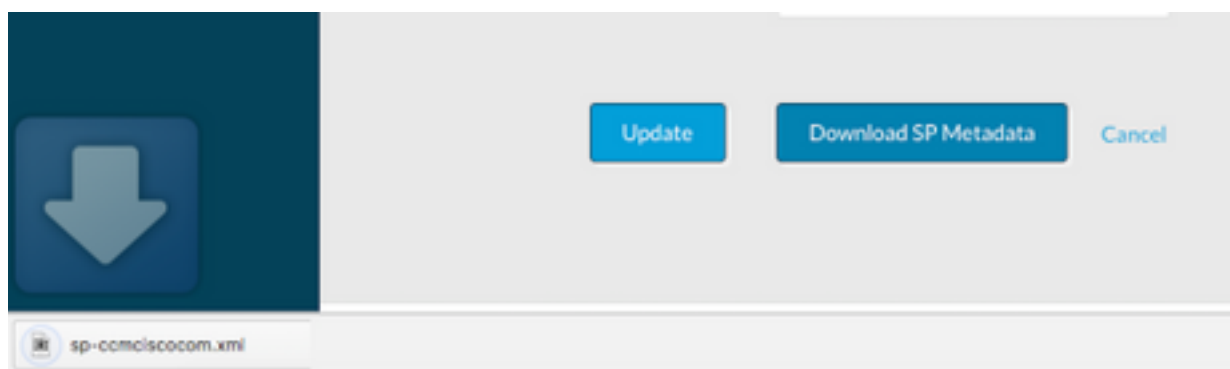
Passaggio 6. Fare clic su **Gestisci amministratori fornitori**.



Passaggio 7. Selezionare le **impostazioni di autenticazione** per il tenant, andare in fondo alla schermata e fare clic sul **pulsante Aggiorna**. In questo modo viene aggiornato il file di metadati corrispondente.



Passaggio 8. Premere il pulsante Download dei metadati SP per scaricare il file XML.



Passaggio 8.1. Per la modalità HA, copiare il file xml da CCM1 a CCM2, accertarsi che le autorizzazioni siano le stesse di CCM1. Posizione del file XML? è in **/usr/local/osmosix/metadata/sp/**.

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

Passaggio 8.2. Avviare il servizio Tomcat sul secondo CCM

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

Passaggio 9. Caricare il file XML in IDP.

Passaggio 10. Se è necessario un file con estensione cer per l'IDP, aprire il file XML e copiare i valori della chiave privata e del certificato in un file di testo. Formattare il file di testo come segue:

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

Passaggio 11. Convalidare la soluzione eseguendo l'accesso.

Nota: In caso di più tenant, ripetere i passaggi da 4 a 8 per ogni tenant.