

How to add a certificate to cacerts

Step by step

This procedure is valid for the docker environment, but it is not for Kubernetes.

How to add the Sync server certificate to the Java key store of Soffid console or Soffid PAM launcher.

1. Start by downloading the certificate from the Sync server:

a. Connect to <https://<SYNC-SERVER>:1760/SAML/metadata.xml?tenant=<your-tenant>>

To get the master's certificate:

```
https://iam-sync.soffidnet:1760/SAML/metadata.xml?tenant=master
```

To get a tenant's certificate:

```
https://iam-sync.soffidnet:1760/SAML/metadata.xml?tenant=demolab
```

b. Download the certificate:

The screenshot shows a web browser window. At the top, a red warning bar states "No es seguro" (Not safe) for the URL "https://iam-sync.soffidnet:1760/SAML/metadata.xml?te...". Below this, a modal dialog box is open, titled "iam-sync.soffidnet:1760". The dialog contains a red warning icon and the text: "La conexión con este sitio web no es segura" (The connection to this website is not secure). It explains that sensitive information should not be entered and offers a link for "Más información" (More information). Below this, it states "Has elegido desactivar las advertencias de seguridad para este sitio" (You have chosen to disable security warnings for this site) and offers a link to "Activar advertencias" (Enable warnings). At the bottom of the dialog, there are three items: "El certificado no es válido" (The certificate is not valid), "Cookies" (1 en uso), and "Configuración del sitio". In the background, the XML document is displayed, showing SAML metadata for "iam-sync.soffidnet:1760".

←

→

↻

⚠ No es seguro

https://iam-sync.soffidnet:1760/SAML/metadata.xml?te...

➤

☆

ff

G

🔍

🔧

☰

Aplicaciones

This XML file does not appear to have a valid MIME type (application/xml).

▼<EntitiesDescriptor xmlns=

▼<EntitiesDescriptor Name

▼<EntityDescriptor xmlns

entityID="tenantidp001

▼<IDPSSODescriptor pro

urn:oasis:names:tc:S

▼<KeyDescriptor>

▼<ds:KeyInfo>

▼<ds:X509Data>

<ds:X509Certif

cDAwMTEcMBoGA1

MDUwMzEyMzMwOF

VQQLDBNGZWRLcm

BQADgY0AMIGJAo

fYyALv1srfkXIV

asnV9ZVMdiTvKX

GrDb2wkbojKR28

EaJm3pMvJJYRo1

</ds:X509Certi

</ds:X509Data>

</ds:KeyInfo>

</KeyDescriptor>

<ArtifactResolution

tenantidp.soffidnet

<ArtifactResolution

tenantidp.soffidnet

<SingleLogoutServic

tenantidp.soffidnet

<SingleLogoutServic

tenantidp.soffidnet

<SingleLogoutServic

tenantidp.soffidnet

<NameIDFormat>urn:o

<NameIDFormat>urn:o

<NameIDFormat>urn:o

<SingleSignOnServic

tenantidp.soffidnet

Visor de certificados: iam-sync.soffidnet

General

Detalles

Jerarquía de certificados

iam-sync.soffidnet

Campos de certificado

▼ iam-sync.soffidnet

▼ Certificado

Versión

Número de serie

Algoritmo de firma de certificado

Emisor

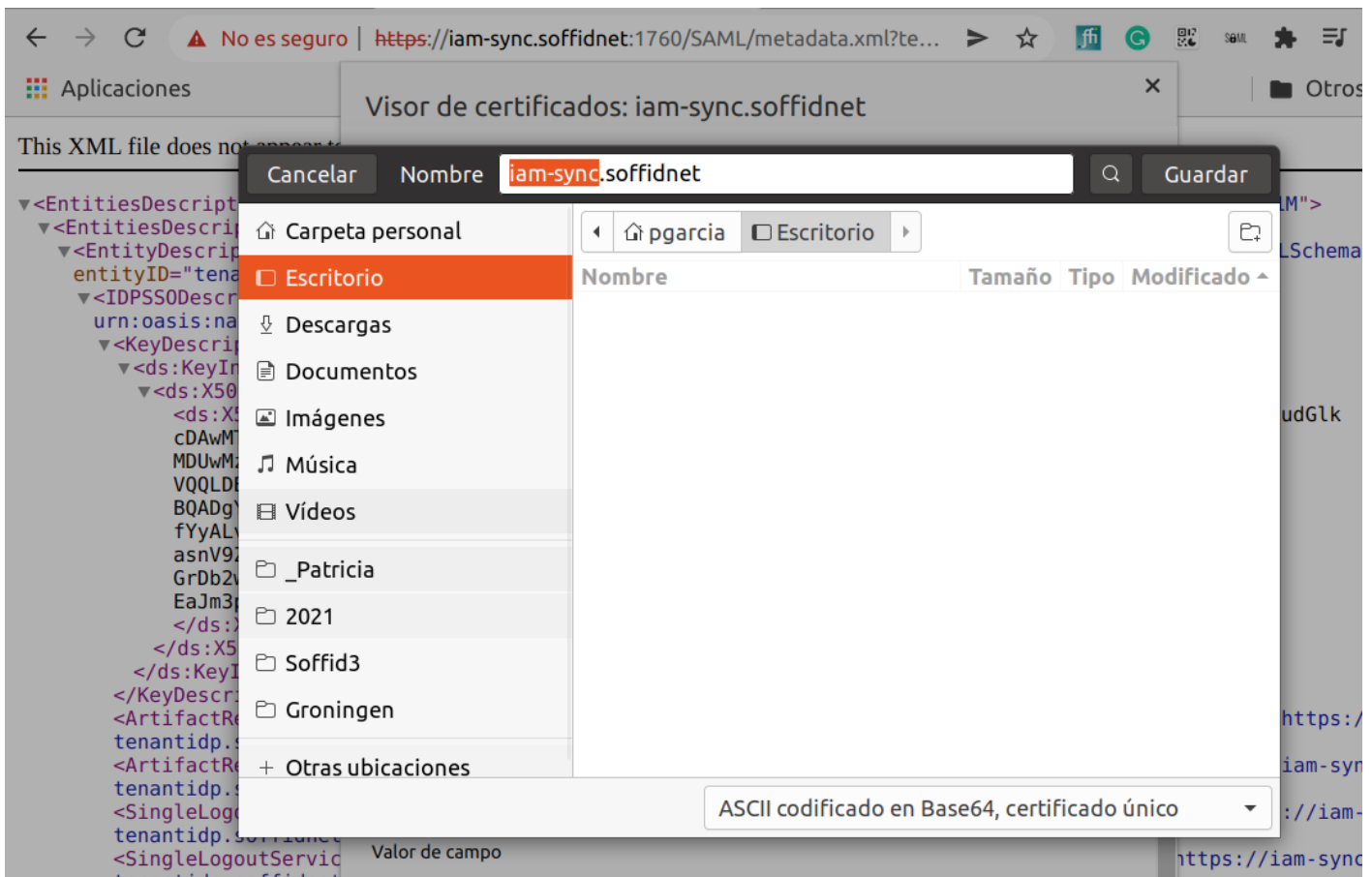
▼ Validez

Posterior a

Anterior a

Valor de campo

Exportar...



2. Copy the certificate file to the container (Soffid Console or Soffid PAM Launcher):

Sample how to copy the file to the tmp folder:

```
sudo docker cp iam-sync.woffidnet iam-console:tmp
```

Sample how to copy the file to the root folder:

```
sudo docker cp iam-sync.woffidnet iam-console: /
```

3. Connect to the container

```
sudo docker exec -it iam-console /bin/bash
```

4. Import the certificate:

```
keytool -import -file /tmp/iam-sync.woffidnet -cacerts
```

- password: **changeit**
- Trust this certificate? [no]: **yes**
- Certificate was added to Keystore

5. Restart the container

If you want to display the current certificate:

```
openssl s_client -connect iam-sync.woffidnet:1760 -showcert
```

Revision #10

Created 18 May 2022 13:27:28 by pgarcia@woffid.com

Updated 30 November 2022 08:38:45 by pgarcia@woffid.com