

3.2. Steps to install Soffid PAM

Follow these steps to install Soffid PAM:

1. First of all, you must **create a folder to save the yaml files** you are going to create.

```
mkdir lab-soffid-pam
```

2. **Go inside the folder**

```
cd lab-soffid-pam
```

3. Create two folder, one to the store and other to the launcher

```
mkdir 01store
```

```
mkdir 02launcher
```

4. **JKS**

If you want a secure environment protected by TLS you will need certificates signed by a trusted third-party Certificate Authority (CA).

To work in your environment lab, you can use self-signed certificates. Visit this link to create the JKS files: <https://bookstack.soffid.com/books/soffid-internal-documentation/page/1-generate-jks-files>

5. **Create the Store container**

- 5.1. Go inside the folder 01store

```
cd 01store
```

- 5.2. Once you are inside the folder, you must create a docker-compose.yaml file with the Store service definition. To create the YAML files you can use your usual text editor.

```
version: '3.8'  
services:
```

```
pam-store:
  image: soffid/pam-store:1.4.48
  environment:
    JAVA_KEYSTORE: /opt/soffid/tomee/certificates/<STORE.jks>
    KEYSTORE_PASS: YOUR_KEYSTORE
  #ports:
    #- "8081:8443"
  networks:
    - network
  volumes:
    - store-trustedcerts:/opt/soffid/tomee/trustedcerts
    - store-certificates:/opt/soffid/tomee/certificates
    - store-data:/opt/soffid/tomee/data
  networks:
    network:
      name: YOUR_NETWORK
      driver: bridge

  volumes:
    store-trustedcerts:
      name: soffid-pam-store-trustedcerts
    store-certificates:
      name: soffid-pam-certificates
    store-data:
      name: soffid-pam-store
```

5.3 Execute this command to initialize the Store container (thanks to the -d option, containers will continue to run in the background, even if you close the terminal)

```
sudo docker-compose up -d
```

5.4. Check the containers: to check the container you can use a docker or a docker-compose command, depend on what you want to check.

5.4.1. In the folder: you can use a docker-compose command

```
sudo docker-compose ps
```

5.4.2. All of them: you can use a docker command

```
sudo docker ps
```

5.5. Check the logs: docker logs are detailed records of the activities that occur within containers. They are like a diary that records everything that happens, from starting and stopping the container to error messages, application outputs, and any other interactions.

5.5.1. You can use a docker-compose command

```
sudo docker-compose logs <SERVICE_NAME>
```

5.5.2. Or you can use a docker command

```
sudo docker logs -f <CONTAINER_NAME/CONTAINER_ID>
```

5.6. If you need to stop the container:

```
sudo docker-compose down
```

6. Create users: the Store container must be up.

6.1. Create Launcher user: once you execute this command, the terminal will return a password that you will need later. Keep it carefully.

```
sudo docker exec <STORE_CONTAINER> /opt/soffid/tomee/bin/add-user.sh user-launcher launcher
```

6.2. User Console user: once you execute this command, the terminal will return a password that you will need later. Keep it carefully.

```
sudo docker exec <STORE_CONTAINER> /opt/soffid/tomee/bin/add-user.sh user-console console
```

7. Create Launcher container

7.1. Go inside the folder 01launcher

```
cd 02launcher
```

7.2. Once you are inside the folder, you must create a docker-compose.yaml file with the Store service definition. To create the YAML files you can use your usual text editor.

```
version: '3.8'
services:
  pam-launcher:
    image: soffid/pam-launcher:1.4.48
    environment:
      JAVA_KEYSTORE: /opt/soffid/tomee/certificates/<LAUNCHER.jks>
```

```
KEYSTORE_PASS: <YOUR_KEY_PASSWORD>
STORE_SERVER: https://<URL_STORE>:8443 or http://<URL_STORE>:8081
STORE_USER: user-launcher
STORE_PASSWORD: <USER_LAUNCHER_PASSWORD>
```

ports:

- "8082:8443"

networks:

- network

volumes:

- launcher-trustedcerts:/opt/soffid/tomee/trustedcerts
- launcher-certificates:/opt/soffid/tomee/certificates
- launcher-data:/opt/soffid/tomee/launcher
- /var/run/docker.sock:/var/run/docker.sock

networks:

network:

name: YOUR_NETWORK

driver: bridge

volumes:

launcher-trustedcerts:

name: soffid-pam-launcher-trustedcerts

launcher-certificates:

name: soffid-pam-certificates

launcher-data:

name: soffid-pam-launcher

7.3 Execute this command to initialize the Launcher container (thanks to the -d option, containers will continue to run in the background, even if you close the terminal)

```
sudo docker-compose up -d
```

7.4. Check the containers: to check the container you can use a docker or a docker-compose command, depend on what you want to check.

7.4.1. In the folder: you can use a docker-compose command

```
sudo docker-compose ps
```

7.4.2. All of them: you can use a docker command

```
sudo docker ps
```

7.5. Check the logs: docker logs are detailed records of the activities that occur within containers. They are like a diary that records everything that happens, from starting and stopping the container to error messages, application outputs, and any other interactions.

7.5.1. You can use a docker-compose command

```
sudo docker-compose logs <SERVICE_NAME>
```

7.5.2. Or you can use a docker command

```
sudo docker logs -f <CONTAINER_NAME/CONTAINER_ID>
```

7.6. If you need to stop the container:

```
sudo docker-compose down
```

8. Copy the JKS files and restart the containers

8.1. To the Store container

```
docker cp <PAM_STORE.jks> <PAM_STORE_CONTAINER>:/opt/soffid/tomee/certificates
```

```
docker compose down
```

```
docker compose up -d
```

8.2. To the Launcher container

```
docker cp <PAM_LAUNCHER.jks> <PAM_LAUNCHER_CONTAINER>:/opt/soffid/tomee/certificates
```

```
docker compose down
```

```
docker compose up -d
```

9. System monitoring

9.1. Store: to connect the store the user and password will be required

```
https://<your-host>/store/check
```

9.2. Launcher

```
https://<your-host>/launch/status
```

10. Configure Soffid Console

<https://bookstack.soffid.com/books/soffid-internal-documentation/page/4-configure-soffid-console>

10.1. Add the PAM certificates to the Console container.

a. Check if the folder trustedcerts exists into the conf folder of the console container

```
docker exec -it <CONSOLE_CONTAINER> bash
```

```
cd /opt/soffid/iam-console-3/trustedcerts
```

b. If this folder does not exists, you need create a volume to save the certificates and add the volume to the Console container

```
sudo docker volume create certificates-trustedcerts-console
```

... add the volume to the Console container and restart the container

b. Copy the certificates into this volume

```
docker exec -it <CONSOLE_CONTAINER> bash
```

```
cd /opt/soffid/iam-console-3/trustedcerts
```

c. Get Store certificate

```
openssl s_client -connect URL_STORE:8443 < /dev/null | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > URL_STORE.crt
```

d. Get Launcher certificate

```
openssl s_client -connect URL_LAUNCHER:8443 < /dev/null | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > URL_LAUNCHER.crt
```

You do not need to add the certificates to cacerts, this process will be automatic when you restart the container.

10.2. Restart the console:

```
docker restart <CONSOLE_CONTAINER>
```

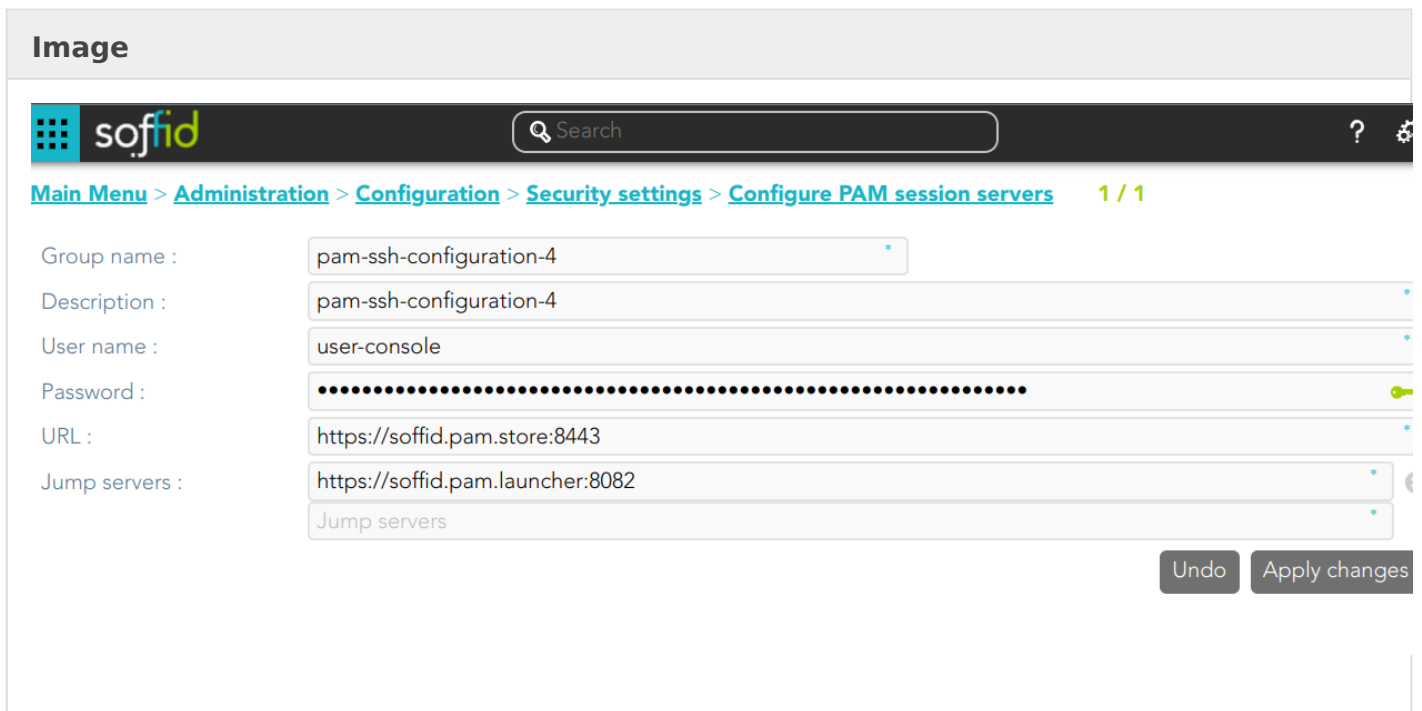
10.3. Configure PAM sessions:

Once you have running all the Soffid containers (Repository, Console, SyncServer, Store and Launcher), you must connect to the console (<http://localhost:8080/soffid>) to configure the PAM sessions. [Browse to Main Menu > Administration > Configuration > Security settings > Configure PAM session servers](#)

Now you can configure the connection. You need to type a Group name (whatever) and a description.

Then you need the user and password created previously when you create the Store container.

And finally you need to type the URL to connect to the Store and to the Launcher (or Jump Server).



The screenshot shows the Soffid web interface. At the top, there's a header with the Soffid logo and a search bar. Below the header, a breadcrumb trail reads: [Main Menu](#) > [Administration](#) > [Configuration](#) > [Security settings](#) > [Configure PAM session servers](#). The page title is '1 / 1'. The main content area contains a form with the following fields:

- Group name : pam-ssh-configuration-4
- Description : pam-ssh-configuration-4
- User name : user-console
- Password : [masked with dots]
- URL : https://soffid.pam.store:8443
- Jump servers : https://soffid.pam.launcher:8082
- Jump servers (additional field): [empty]

At the bottom right of the form, there are two buttons: 'Undo' and 'Apply changes'.

11. Configure Sync Server: add the Store certificate to the Sync Server container.

a. Connect to the container

```
docker exec -it <SYNC_SERVER_CONTAINER> bash
```

b. Browse to the conf folder

```
cd /opt/soffid/iam-sync/conf
```

c. Create the crt file

```
openssl s_client -connect URL_STORE:8443 < /dev/null | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > URL_STORE.crt
```

d. Import the certificate into Sync Server cacerts

```
keytool -import -file URL_STORE.crt -keystore cacerts -alias URL_STORE
```

password: changeit

e. Restart Sync Server

```
docker compose down
```

```
docker compose up -d
```

12. Configure Launcher:

12.1. Import Store certificate

Connect to the launcher container

```
sudo docker exec -it <LAUNCHER_CONTAINER> bash
```

b. Export the certificate from the store: soffid-pam-store:8443

```
openssl s_client -connect URL_STORE:8443 < /dev/null | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > URL_STORE.crt
```

You do not need to add the certificates to cacerts, this process will be automatic when you restart the container.

12.2. Import Sync server certificate

a) Connect to the launcher container

```
sudo docker exec -it <LAUNCHER_CONTAINER> bash
```

b) Export the certificate from the Sync server:

```
openssl s_client -connect SYNC_SERVER.netcompose:1760 < /dev/null | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > SYNC_SERVER.netcompose.crt
```


You do not need to add the certificates to cacerts, this process will be automatic when you restart the container.

12.3. Restart the Launcher container

```
docker compose down
```

```
docker compose up -d
```

12.4. Check the cacerts

```
keytool -list -keystore cacerts -v -alias URL_STORE
```

```
keytool -list -keystore cacerts -v -alias SYNC_SERVER.netcompose
```

13. Once Soffid PAM are working fine, you can **merge all the YAML** file. You can then run this YAML file to update any services or add any additional settings.

```
docker compose up -d
```

Download pasr-shh y demas imagenes!!!!1

Revision #15

Created 16 December 2024 11:28:02 by pgarcia@soffid.com

Updated 3 February 2025 10:38:27 by pgarcia@soffid.com