

SSH gateway

- [SSH Gateway Docker Installation](#)
- [SSH Gateway Docker Compose Installation](#)
- [SSH Gateway Connection](#)

SSH Gateway Docker Installation

Introduction

Soffid allows you to deploy a new docker container with the **ssh gateway**. The configuration is similar to the sync server configuration, the main difference is the ssh container is listening in ssh.

Prerequisites

The SSH Service is only released as a docker service.

1. Install docker (<https://docs.docker.com/install/>)
2. Install Soffid PAM (store container and launcher container)

You can visit the [PAM Jump Server Installation page](#) for more information about how to install PAM

3. Create a Docker network(*), that network allows you to connect containers to the same bridge network to communicate:

```
sudo docker network create -d bridge NETWORKNAME
```

* You can use the same network defined in the Console and Sync Server installation to avoid visibility problems.

Installation

The steps required to install SSH container are:

1. Create a user

We need to create a user in the pam store container. To do this, we need to connect to the store container.

```
sudo docker exec -it soffid-pam-store /bin/bash
```

Once, we are connected to the container, we need to run a script to create the user. This script has two parameters, the user name, and the role. We have to type launcher in the role parameter

```
root@soffid-pam-store:/# /opt/soffid/tomee/bin/add-user.sh proxysshtest launcher
Password: c4ZRcmgemq3nMr1VQJCD1pJRhPbdX5hrmmrP6RX7zBE4HSs3RV3+cGwDdL1WaaqZ
root@soffid-pam-store:/#
```

As a result of the script, we receive the password for the created user. This password will be needed later when we create the container.

2. Create volume

We need to create a volume that will be used by the docker container

```
sudo docker volume create soffid-ssh
```

3. Create a docker container

Finally, we need to execute the command to create the ssh gateway container

```
docker run \
--name soffid-ssh \
-e SOFFID_SERVER=https://iam-sync.soffidnet:1760 \
-e SOFFID_USER=admin \
-e SOFFID_PASS=changeit \
-e SOFFID_HOSTNAME=ssh-gateway \
-e STORE_SERVER=http://soffid-pam-store:8080 \
-e STORE_PASSWORD=kDH0vh8MFWWn843Vhzmj0Np7uzMEfbqFYM1ELCQqOf+ +tF0xfd=Ve2eGq81OXvqy \
-e STORE_USER=proxysshtest \
-v soffid-ssh:/opt/soffid/iam-sync/conf \
--publish 2222:22 \
--network=soffidnet \
```

Environment Variables

To create the new SSH container you need to set the following environment variables:

Variable	Description	Example
SOFFID_SERVER	Sync Server URL	https://syncserver01.soffid.com:1760
SOFFID_USER	Soffid user to join the security domain	admin
SOFFID_PASSWORD	Soffid user password	changeit
SOFFID_HOSTNAME	The hostname used to access the ssh gateway	ssh-gateway
STORE_SERVER	Store URL	http://soffid-pam-store:8080
STORE_PASSWORD	Password received when you created the user in the store container.	*****
STORE_USER	Store user	proxyssh

SSH Gateway Docker Compose Installation

Introduction

Soffid allows you to deploy a new docker container with the **ssh gateway**. The configuration is similar to the sync server configuration, the main difference is the ssh container is listening in ssh.

Prerequisites

The SSH Service is only released as a docker service.

1. Install docker (<https://docs.docker.com/install/>)
2. Install docker compose (<https://docs.docker.com/compose/install/>)
3. Install Soffid PAM (store container and launcher container)

You can visit the [PAM Jump Server Installation page](#) for more information about how to install PAM

Installation

The steps required to install SSH container are:

1. Create a user

We need to create a user in the pam store container. To do this, we need to connect to the store container.

```
sudo docker exec -it soffid-pam-store /bin/bash
```

Once, we are connected to the container, we need to run a script to create the user. This script has two parameters, the user name, and the role. We have to type launcher in the role parameter

```
root@soffid-pam-store:/# /opt/soffid/tomee/bin/add-user.sh proxyssh-user launcher
Password: c4ZRcmgemq3nMr1VQJCD1pJRhPbdX5hrmmrP6RX7zBE4HSs3RV3+cGwDdL1WaaqZ
root@soffid-pam-store:/#
```

As a result of the script, we receive the password for the created user. This password will be needed later when we create the container.

2. Execute the YAML

```
version: '3.8'

services:
  ssh-gateway:
    image: soffid/pam-ssh:1.4.47
    environment:
      SOFFID_SERVER: https://syncserver01.soffid.com:1760
      SOFFID_USER: soffidUser
      SOFFID_PASS: SoffidPassword
      SOFFID_HOSTNAME: ssh-gateway
      STORE_SERVER: https://soffid-pam-store:8443
      STORE_PASSWORD: c4ZRcmgemq3nMr1VQJCD1pJRhPbdX5hrmmrP6RX7zBE4HSs3RV3+cGwDdL1WaaqZ
      STORE_USER: proxyssh-user
    ports:
      - "2222:22"
    networks:
      - network
    volumes:
      - ssh-gateway-data:/opt/soffid/iam-sync/conf

networks:
  network:
    name: netcompose
    driver: bridge

volumes:
```

ssh-gateway-data:

name: compose-ssh-gateway-data

Execute:

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

Environment Variables

To create the new SSH container you need to set the following environment variables:

Variable	Description	Example
SOFFID_SERVER	Sync Server URL	https://syncserver01.soffid.com:1760
SOFFID_USER	Soffid user to join the security domain	admin
SOFFID_PASSWORD	Soffid user password	*****
SOFFID_HOSTNAME	The hostname used to access the ssh gateway	ssh-gateway
STORE_SERVER	Store URL	http://soffid-pam-store:8080
STORE_PASSWORD	Password received when you created the user in the store container.	*****
STORE_USER	Store user	proxyssh

SSH Gateway Connection

Introduction

We can establish a connection to the target system using the SSH remote access protocol.

How to connect 1

You can establish the connection with the ssh gateway and then Soffid will ask your password and the target system parameters to connect:

- **Password:** password of your account to connect to Soffid.
- **Target server:** system to which you want to connect.
- **Account to use:** account to use to connect to the target system.
- **Account source system**

```
root@soffid:~# ssh -p 2222 dilbert@ssh-gateway
```

```
Password:
```

```
Target server: 10.129.120.5
```

```
Account to use: patricia
```

```
Account source system [leave blank to use a target system local account]:
```

```

|           _           |
|          _/          |
| _ _ _/_/_|_° _|      | | | |
| |_ / \ | | | / |      |
| _|\_ / | | | \_ / SSH GATEWAY |
|          _/          |
|           |           |
| Hello dilbert          |
| NOTICE: This session is being recorded |
|_____|
```

```
Connecting to 10.129.120.5 as patricia
```

```
Last login: Fri Apr 8 08:39:23 2022 from 10.129.120.6
```


How to connect 2

You can establish the connection with the target system typing all the parameters to connect in one line AccountName__HostName__TargetAccount. At the end, Soffid will ask the password of your account to connect.

- **Account name:** account to connect to Soffid.
- **Host name:** target system to which you want to connect.
- **Target account:** account to connect to the target system.
- **Password:** password of your account to connect to Soffid.

```
root@soffid:~# ssh -p 2222 dilbert__10.129.120.5__patricia@ssh-gateway
```

Password:

```

|           _           |
|          _/          |
| _ _ _/_/_o _|        | | | | |
| |_ / \ | | | / |      |
| _|\_/_| | | \_/_ SSH GATEWAY |
|          _/          |
|           |           |
| Hello dilbert          |
| NOTICE: This session is being recorded |
|_____|
```

Connecting to 10.129.120.5 as patricia

Last login: Fri Apr 8 09:57:22 2022 from 10.129.120.6

```
[patricia@forgecentos ~]$
```

How to connect 3

You can establish the connection with the target system typing all the parameters to connect in one line AccountName__HostName__TargetAccount and using a ssh key.

- **Account name:** account to connect to Soffid.
- **Host name:** target system to which you want to connect.
- **Target account:** account to connect to the target system.

You can generate an ssh key to connect or use your existing ssh key.

- Generate a new ssh key: `ssh-keygen -t rsa`
- Read an existing ssh key: `cat .ssh/id_rsa.pub`

Then you need to include it in Soffid Console in your user data.

Finally you can establish the connection.

```
pgarcia@soffid:~$ ssh -p 2222 pgarcia_10.129.120.5_patricia@ssh-gateway
```

```

|      _      |
|      _/    |      | | | |
| _ _ _/_|_° _|      |
| |_ / \ | | / |      |
| _|\_/ | | |\_/ SSH GATEWAY |
|      _/      |
|              |
| Hello pgarcia      |
| NOTICE: This session is being recorded |
|_____|
```

Connecting to 10.129.120.5 as patricia

Last login: Fri Apr 8 11:57:19 2022 from 10.129.120.6

[patricia@forgecentos ~]\$

Soffid needs the **ssh_key** attribute in the user object metadata, please check the attribute is created properly, and the fill in with your public key.

Object type : com.soffid.iam.api.User

Description : Built-in user object

▼ Order	Code
Filter	Filter
28	__AUDIT__
29	createdByUser
30	createdDate
31	modifiedByUser
32	modifiedDate
33	RegisterServiceProvider
34	ActivationKey
35	__OTHER DATA__
36	language
37	country
38	Color
104	office
104	company
105	IAMIndicator
9999	ssh_key

Attribute metadata

Attribute metadata ◀ 42 / 42

Code : ssh_key

Label : SSH Public key

Data type: String ▼

User hint : User hint

Description : Description

Required : ☒ NoInclude in quick search : ☒ NoPrevent duplicated values : ☒ NoMultiple values : ☒ Yes ☒ No

Maximum number of rows to display :

Maximum number of rows to display

Size : Size

Values : Values

Administrator visibility : Read only ▼

Operator visibility : Read only ▼

User visibility : Read/write ▼

Visibility expression : Visibility expression

Common attributes

User name : pgarcia

First name : patricia

Last Name : garcia

Middle name : Middle name

Full name : patricia garcia

Birth date : 5/3/80

Mail service

Internal eMail : Internal eMail

Mail alias : Mail alias

External email : External email

Mail server : Mail server

User status

Enabled : ☒ No ☒ Yes

Multi session : ☒ No ☒ Yes

Comments : Comments

OTHER DATA

SSH Public key : ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGCfuHHJovqlwybPULgkxhK8fR3U0Ymetok980k3lnJNCI

Organization

Type : Internal user

Primary group : admingroup OU=admingroup,DC=testora,DC=lab

Home server : Home server

Profile server : Profile server

Manager : Manager

Contract type : Contract type

Fotografia : Fotografia

Other

NIF : NIF

PHONE : PHONE

Audit information

Created by : admin Soffid Administrator

Created on : 5/31/21 14:16

Modified by : admin Soffid Administrator

Modified last on : 4/8/22 10:13

RegisterServiceProvider : RegisterServiceProvider

ActivationKey : ActivationKey

https://es.wikipedia.org/wiki/Secure_Shell