# 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 <u>PAM Jump Server Installation page</u> 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 (<u>https://docs.docker.com/compose/install/</u>)
- 3. Install Soffid PAM (store container and launcher container)

You can visit the <u>PAM Jump Server Installation page</u> 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]:



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:



#### 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.

#### soffid

#### <u>Main Menu > Administration > Configuration > Global Settings > Metadata</u> < 9 / 13 >

Object type :		com.soffid.iam.api.Use	r				
Description :		Builtin user object	Attribute m	etadata			
• Order		Code					
Filter		Filter	Attribute me	etadata ┥ 42	/ 42		
28		AUDIT_	Code :		ssh_key		
29		createdByUser	Label :		SSH Public key	1	
30		createdDate	Edber.		State a		
31		modifiedByUser	Data type:		String	*	
32		modifiedDate	User hint :		User hint		
33		RegisterServiceProvider	Description	11	Description		
34		ActivationKey					
35		OTHER DATA_	Required :		III No		
36		language	Include in c	Include in quick search :			
37		country	Prevent du	olicated values	III No		
38		Color	Multiple va	ues ·	Yes III		
104		office	Maximum	Martiple values .		to display.	
104		company	Maximum	lumber of rows	Maximum num	abor of rows to display	
105		IAMIndicator				iber of rows to display	
9999		ssh_key	Size :		Size		
			Values :		Values		
			Administrat	tor visibility :	Read only 🐱		
			Operator v	isibility :	Read only 🔹		
			User visibili	ty :	Read/write 🗸		
			Visibility ex	pression :	Visibility expre	ession	
Common attributes				Organization			
User name :	pgarcia		•	Туре :	Internal user 👻		
First name :	patricia	•		Primary group :	admingroup	OU=admingroup,DC=testora,DC=la	
Middle name :	Middle name			Profile server :			
Full name :	patricia garcia			Manager :			
Birth date :	5/3/80			Contract type : Fotografía :	· ·		
Mail service				Other	at de la sa		
Internal eMail :				NIF :			
Mail alias :				PHONE :	~		
External email : Mail server :							
User status				Audit information			
Enabled :	Yes			Created by :	admin	Soffid Administrator	
Multi session : Comments :	Comments			Created on :	5/31/21 14:16		
			ĥ	Modified last on :	admin 4/8/22 10:13	Soffid Administrator	
				RegisterServiceProvider :	RegisterServiceProvider		
				ActivationKey :			
OTHER DATA							
SSH Public key :	ssh-rsa AAAAB3Nza	aC1yc2EAAAADAQABAAABgQCfuHHJovqlwybPUL	_gkxhK8fR3U0Ymetok980k3InJNCE				

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCfuHHJovqlwybPULgkxhK8fR3U0Ymetok980k3InJNCE

https://es.wikipedia.org/wiki/Secure\_Shell