

Step 4. Register additional resources (Optional)

- [Step 4.1. Add database \(Optional\)](#)
- [Step 4.2. Create an agent \(Optional\)](#)
- [Step 4.3. Reconcile \(Optional\)](#)

Step 4.1. Add database (Optional)

The fourth step, to add a database, is an **optional** step. You only need to configure when there is any database (SQL Server or Oracle) in some of the discovered hosts and you want to manage its accounts as privileged or shared accounts.

Step-by-step

The network discovery process can discover and connect to the hosts. Then Soffid allows you to add databases as account repositories in the proper host.

1. First of all, the agent must be created on Soffid. That agent could be a SQL Server agent or an Oracle agent. To create an agent you can visit the next page [Step 4.2. Create an agent \(Optional\)](#)
2. Then, you must access the network discovery page in the following path:

Main Menu > Administration > Configuration > Integration engine > Network discovery

3. Once you have accessed the network discovery page, Soffid will display all the networks.

3.1. First, you must identify the network and click on the plus icon (+) to display all the hosts discovered.

Name	IP Address	Operating system	Managed
<input type="text" value="Filter"/>	<input type="text" value="Filter"/>	<input type="text" value="Filter"/>	<input type="text" value="Filter"/>
<input type="checkbox"/> loopback			
<input type="checkbox"/> lab100			
<input checked="" type="checkbox"/> lab200			

Tota

3.2. Then, you must identify the host.

Name	IP Address	Operating system	Managed
Filter	Filter	Filter	Filter
⊕ loopback			
⊕ lab100			
⊖ lab200			
⊕ soffid.pat.lab	192.168.122.1	ALT	No
⊕ WIN-6O4SNJ52GPC	192.168.122.250	NTS	No
⊕ 192.168.122.69	192.168.122.69	LIN	No

Total

You can consult the information retrieved

Name : 192.168.122.69

IP Address : 192.168.122.69

Description :

Operating system :

Port	Description
Filter	Filter
22/tcp	OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux; protocol 2.0)
3306/tcp	MariaDB (unauthorized)

Displayed

3.3. Finally, on the "Account repositories" you must click the "Add new" button.

⊖ lab3
⊕ 10.129.122.1
⊕ 10.129.122.22
⊖ 10.129.122.25
⊕ Account protected services
⊖ Account repositories
10.129.122.25 Agent definition Accounts
Add new
⊕ Entry points
⊕ 10.129.122.252
⊕ 10.129.122.253

4. When you click "Add new" Soffid will display a wizard to add the database.

New account repository

Select system type → Finish

Select system type : - Select value -

- Select value -
- Linux local accounts
- MySql or MariaDB database
- Other

Name	IP	System Type	OS	Account Type
loopback				
lab100				
lab200				
soffid.pat.lab	192.168.122.1	ALT		No
WIN-6O4SNJ52GPC	192.168.122.250	NTS		No
192.168.122.69	192.168.122.69	LIN		No
Account repositories				
Add new				
Entry points				

Total rows: 8

5. You must select the option "Other" on the "Select system type", and click the "Next" button.

5.1. If you click the "Next" button, the wizard will allow you to search the system using Quick, Basic, or Advanced search. When you run the search, Soffid will display all the systems that apply to the search criteria. Be in mind, the agent must have been previously created.

5.2. You must select the proper system from the result list and click the "Next" button. Then Soffid will add the agent to the "Account repositories" list and close the wizard.

Name

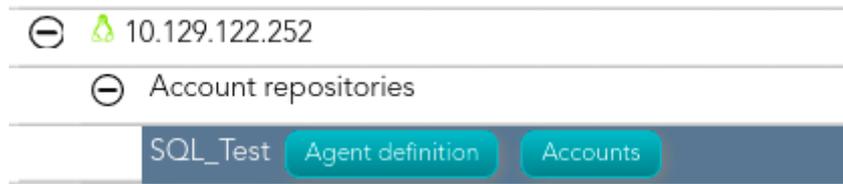
Filter

- loopback
- lab3
- 10.129.122.1
- 10.129.122.22
- 10.129.122.252
- Account repositories
 - SQL_Test Agent definition Accounts
 - Add new
- Entry points
- 10.129.122.253
- ADSERVER
- test

* When you are in the wizard and click the "Undo" button, the wizard will browse to the previous page of the wizard, or close and no operation will execute if it is the first page.

6. Once the database is added to the host, the next step will be to run the reconcile process to get all the accounts and permissions from the database to load into Soffid.

6.1. To access the agent definition, you must click the "Agent definition" button. The button is located close to the name of the agent, inside the "Account repositories" of a specific host, on the network discovery tree.



6.2. Once you click the button, Soffid will browse to the agent definition.

6.3. Then you must click the "Massive actions" tab.

6.4. At the "Massive actions" tab you must click the button "Reconcile (load target system objects)". That process is in charge to load into Soffid the accounts and permissions defined on the database.

6.4.1. If the process is successfully completed you could continue with the next step of the PAM implementation.

6.4.2. In another case, you must check the agent configuration and run again the process.

Screen overview

<https://www.youtube.com/embed/HL4nsuEKSGo?rel=0>

Step 4.2. Create an agent (Optional)

That step will be an **optional** step, and it will be mandatory only when the **SQL Server agent** or the **Oracle agent** was not created previously on Soffid Console and you need to add a database to manage its accounts.

Step-by-step

1. First of all, to create an agent you must access the agent page in the following path:

Main Menu > Administration > Configure Soffid > Integration engine > Agents

2. Once you have accessed the agent page, Soffid will display all the active agents created on Soffid. You must click the button with the add symbol (+) to add a new agent. Then Soffid will display a new empty page to fill in the agent data.

2.1. You must fill, at least the required fields (fields with an asterisk) to create an agent.

- ○ ○ The **Name** should be an identificative and unique agent name
- The **Description** should be a brief description of the agent.
- The **Type** allows you to select the connector type to use, the SQL Server connector or the Oracle connector. Be in mind that you need to load the connector on Soffid if you did not do it previously.
- The **Server** allows you to select the synchronization server that will perform the agent tasks. It is allowed to select two servers in cases high disponibility will be necessary. If you choose two servers, when one fails, the other will be used.
 - If "*-disabled-*" is selected, the agent will be disabled-
- The **User domain** allows you to select how to generate account names. If the account name is the same as the user name (as it is normally the case), the "Default user domain" should be used. The user domain values are defined on the Account naming rules page.

- The **Password domain** allows you to select the password policies that will be used. If the "Default password domain" is selected, Soffid passwords will be shared with the managed systems. The user domain values are defined on the [Password policies](#) page.

You can visit the [Plugins page](#) for more information about how to load a connector on Soffid Console.

2.2. You must fill in the optional parameters that you need to config the agent.

2.3. You must fill in the "Connector parameters". Those parameters depend on the agent.

2.3.1. SQL Server connector:

Below there are the specific parameters for this agent implementation:

Parameter	Description
User name	Database user name to authenticate
Password	The password of the database user
Driver	Identifies the driver of the relational database to use. Currently, these are the supported databases: MySQL (& MariaDB), PostgreSQL, Oracle, MS SQL Server, Informix, DB2/400, DB2 Universal, Sybase, ODBC

Parameter	Description
DB URL	<p>URL that identifies the connection properties. Please refer to the specific database vendor documentation to build this URL.</p> <pre>jdbc:mariadb://<HOST>/<DATA_BASE></pre> <pre>jdbc:mysql://<HOST>/<DATA_BASE></pre> <pre>jdbc:postgresql://<HOST>/<DATA_BASE></pre> <pre>jdbc:oracle:<drivertype>:@<database></pre> <pre>jdbc:sqlserver://<HOST>;databaseName=<DATA_BASE></pre> <p>(*) <i>More documentation about the DB URL</i></p>
SQL Sentence to execute at startup	Each time the connection to the agent is established, this SQL statement will be executed.
Password hash algorithm	The algorithm is used to encrypt the password. For instance SHA1, SHA256, MD5, etc
Password hash prefix	<p>Prefix to add it to the password.</p> <pre>{SHA1}BzE/DjIPIsv6Nc/CIFCOs/9FfH4=</pre> <pre>{SHA256}AIEM+LINb8ucXeSE077EGHYgs+KHblmquQ2FL+Dxj7Y=</pre>
Enable debug	<p>Two options: Yes, and No.</p> <p>It enables or not more log traces in the Synchronization Server log</p>
Synchronization method	<ul style="list-style-type: none"> • Full synchronization: persists the changes made in Soffid, regardless of the possible changes made in the final system. • Incremental synchronization: this type of synchronization is used to avoid losing changes that have been made to the target system. First, Soffid's changes will be propagated to the target system, and then the changes on the target system will be made in the Soffid system. If the changes are in the same attribute, the Soffid value is the one that will persist. <p>(**)</p>

2.3.1. Oracle connector:

Below there are the specific parameters for this agent implementation:

Parameter	Description
User	Sysdba user name to authenticate
Oracle password	Password of the user to authenticate
Connection string to database	Database URL. Use something like <u>jdbc:oracle:thin:@host:port:sid</u>
Password to protect roles	Optional password to use on password protected roles
Default user profile	Optional profile to set limits on the database resources and the user password
Default tablespace	Optional tablespace for user creation
Temporary tablespace	Optional temporary tablespace for user creation
Enable debug	Two options: [Yes / No]. When it is enabled more log traces are printed in the Synchronization Server log

3. Then, you should click the "Apply changes" button to save the new agent. Then Soffid will close the form, and display the agent list including the new agent created.

If you click the "Undo" button, the form will be closed and updates will not be saved.

Once the agent is configured, it could be assigned to the host to continue with the PAM implementation process: [Step 4. Add database](#)

Screen overview

SQL Server agent

Name: SQL_Test

Description: SQL_Test

Type: Class: com.soffid.iam.agent.sqlserver.SqlServerAgent

Server:

Shared Thread: Yes No Dedicated threads:

Task timeout (ms): Long task timeout (ms):

Trust passwords: Yes No

Read only: Yes No

Manual account creation: Yes No

User domain: *

Passwords domain: *

Connector parameters:

User:

Oracle password:

Connection string to database:

Create agents for each database:

Enable debug:

Oracle agent

Name: SQL_Test

Description: SQL_Test

Type: Class: com.soffid.iam.agent.oracle.OracleAgent

Server:

Shared Thread: Yes No Dedicated threads:

Task timeout (ms): Long task timeout (ms):

Trust passwords: Yes No

Read only: Yes No

Manual account creation: Yes No

User domain: *

Passwords domain: *

Connector parameters:

User:

Oracle password:

Connection string to database:

Password to protect roles:

Default user profile:

Default tablespace:

Temporary tablespace:

Enable debug:

Step 4.3. Reconcile (Optional)

To request the accounts you must launch the reconciliation process. The main purpose of reconciling process is to provide a mechanism to ensure that all users are aligned on the specific roles and responsibilities.

Step-by-step

1. First of all, you need to edit the agent must access the agent page in the following path:

Main Menu > Administration > Configure Soffid > Integration engine > Agents

2. Once you have accessed the agent page, Soffid will display all the active agents created on Soffid. You must click on the record of the agent you want to reconcile. Then Soffid will display a new window with the agent data.

3. Then, you must click on the "Massive actions" tab.

4. At the "Massive actions" tab, you must click on the "Reconcile (load target system objects)" button to launch the reconciliation process.

5. Once completion of the conciliation process, Soffid will show the result of the process execution. You could click on the alert to view the process result.

5.1. Green alert: the process finished ok.

5.2. Red alert: the process finished with an error.

Screen overview

SSO

- External SSO accounts

 Provision all users on to managed systems.

 Propagate groups to agent

Reconcile (load target system objects)

Generate target system potential impact