Oracle Connector

Introduction

Description

Oracle Connector could manage an Oracle database.

> Soffid's Oracle connector supports Profiles since version 2.2.6.14

Managed System

This connector is specific for integration with an Oracle database, if you want to connect a generic SQL database, please visit the following page: SQL Connector.

> For more information to check if your system may be synchronized with this connector you do not hesitate to contact us through our Contact form

Prerequisites

It is needed a user with sysdba access and permissions.

User management

Criteria:

- Any user or account created will be granted the CREATE SESSION privilege.
- Default tablespace for each user will be the USERS tablespace. It won't be changed for existing users.
- Soffid passwords expiration date will be managed by Soffid. So, Oracle won't be notified about when those passwords need to be expired.
- Roles and groups are automatically created when a user belonging to it is updated.

Exceptions:

- Error SQL: ….There was an error executing an SQL statement.
- Contact with the administrator of the database. It may be a problem of user authorizations, administrator password validity, availability of space in the database, or saturation of it.

Download and Install

This addon is located in the Connectors section and its name is **Oracle Connector**.

> For more information about the installation process you can visit the Addons Getting started page.

Agent Configuration

This connector could manage User and Role objects.

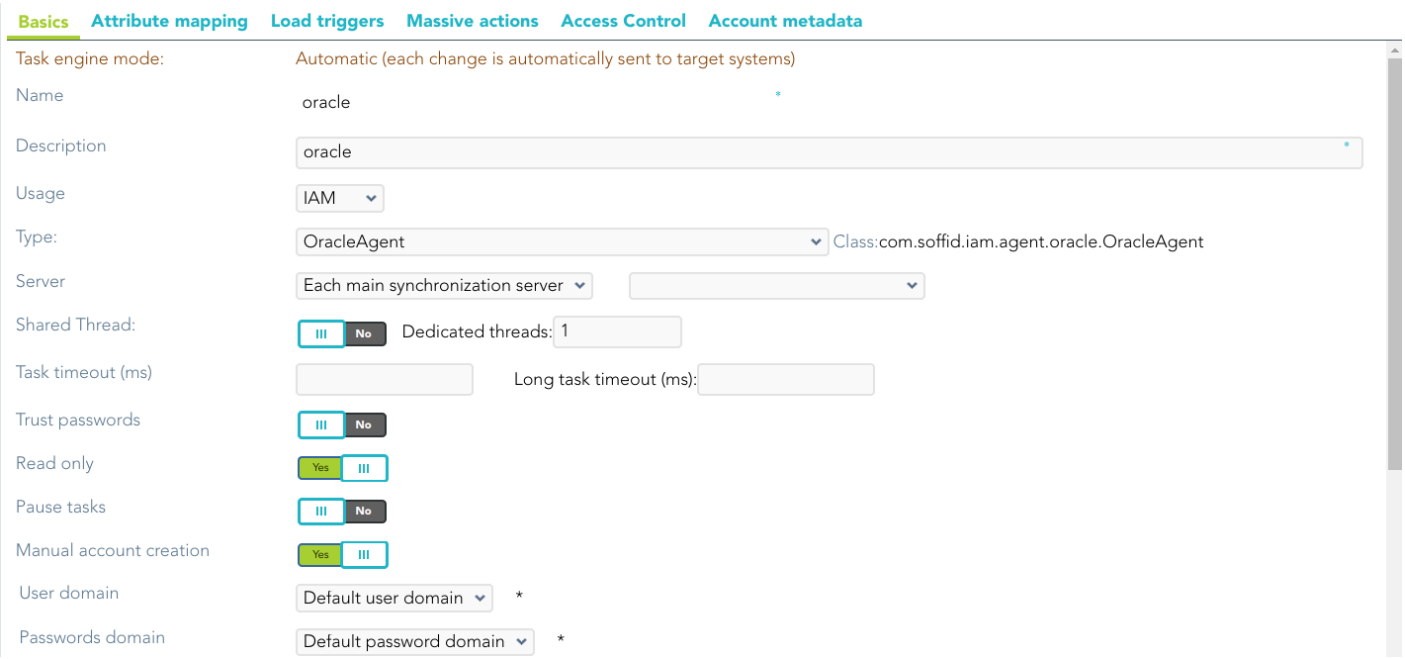
Basic

Generic parameters

After the installation of the addon, you may create and configure agent instances.

To configure this Oracle Connector you must select "OracleAgent" in the attribute "Type" of the generic parameters section in the agents' page configuration.

> For more information about how you may configure the generic parameters of the agent, see the following link: Agents configuration



Custom parameters

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 jdbc:oracle:thin:@host:port:sid
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

Load triggers

You can define JavaScript or BeanShell scripts that will be triggered when data is loaded into Soffid (incoming triggers). The trigger result will be a boolean value, true to continue or false to stop.

Triggers can be used to validate or perform a specific action just before performing an operation or just after performing an operation into Soffid objects.

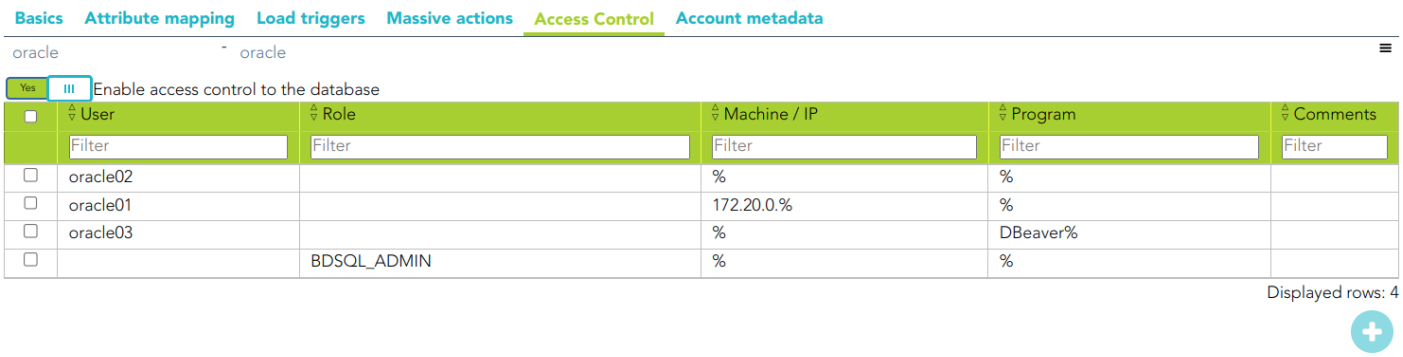
> To view some examples, visit the Incoming triggers examples page.

Access Control

Oracle connector can establish an access control for Oracle Users.

If the access control checkbox is enabled, only the users and applications that are listed on the access control page will be allowed to log in. So, you can restrict the IP address and application a user can connect from.

This restriction does not apply to DBA users.



> Check that the user/account is not unmanaged.

When the Enable access control to the database check box is checked, the UpdateAccessControl task will be launched. The following tables will be created on the SQL Server:

- **SC_OR_ACCLOG**: access log
- **SC_OR_CONACC**: rule access control
- **SC_OR_ROLE**: user roles.
- **SC_OR_VERSION**: connector versions.

When you try to connect to SQL Server, the logon_audit_trigger is launched to check if you have access or not.

You can check the Access Logs page for access controls.

Account metadata

Agents allow you to create additional data, on the "Account metadata" tab, to customize the accounts created for that agent. This additional information will be loaded with the agent's information, or calculated as defined in the mappings.
The additional data can be used in both mappings and triggers.

The attributes that you define here will be shown when you click on the proper account, on the Accounts Tabs at user page.

Operational

Monitoring

After the agent configuration you can check on the monitoring page if the service is running in the Synchronization Server, please go to:

> Start Menu > Administration > Monitoring and reporting > Syscserver monitoring

Tasks

Authoritative

If you checked "Authorized identity source", an automatic task to load identities from the managed system to Soffid is available, please go to:

> Start Menu > Administration > Monitoring and reporting > Scheduled tasks

And you will do something like "Import authoritative data from <AGENT_NAME>".

Reconcile

To manage an automatic task to synchronize user objects from the managed system to Soffid is available, please go to:

> Start Menu > Administration > Monitoring and reporting > Scheduled tasks

And you will do something like "Reconcile all accounts from <AGENT_NAME>".

Synchronization

Regarding the synchronization of the objects, there are two possible options:

- If you check the generic attribute "Read Only" in the "Basics" tab, only the changes in the managed systems will be updated in Soffid. We recommend these options until the global configuration of Soffid is tested.
- If you do not check the generic attribute "Read Only" in the "Basics" tab, all the changes in Soffid or the managed system will be updated in the other. Note that this synchronization must be configured in the "Attribute mapping" tab correctly.

> For more information about how you may configure the generic parameters of the agent, see the following link: Agents configuration

Revision #29
Created 19 April 2021 15:28:02
Updated 1 March 2024 08:13:42