Active Directory as User Data Source for SAP GRC

Active Directory is usually the main source of user information inside the company, therefore should be connected to a SAP GRC system to be used as the main source of information. This practice will help to have the information that is stored inside the SAP system updated.

In order to connect Active Directory to a SAP system it is important to follow the next steps:

- RFC communication.
- LDAP configuration.
- GRC synchronization.

RFC Communication

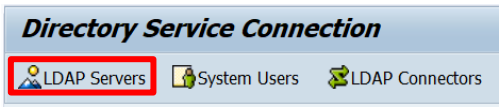
The communication between Active Directory and SAP GRC requires the definition of a TCP/IP Connection. The Key fields from the Connection are:

- Gateway Host
- Gateway Service
- Registered Program ID

Gateway Host and Gateway Service, both of them, are related with the GRC system only. Registered Program ID should be having the same name as the RFC connection. It is important to state, that there could be some issues when registered the program ID if the gateway is having a restriction in the register.

LDAP Configuration

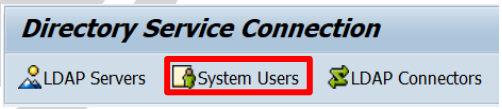
The next step is the connection to the LDAP Server. This configuration is performed thought the LDAP Transaction.



The Key fields are:

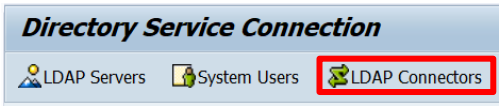
- Host Name
- Port Number
- Base Entry
- System Logon

SAP provides by default a specific mapping to be used for Active Directory, you just need to press "F8". Please contact your System Administration Team to ensure that the Active Directory Mapping is correct. Furthermore, it is required to define the user that exists in the Active Directory and will be used for the connection. This configuration needs to be performed inside "System Users" option.



Remember to include the Base Entry to find the Location of the System User inside the Active Directory

Once the LDAP Server is configured, it is required to define a LDAP connector.



The name of the connector MUST be the same as the RFC connector. The application name of the LDAP Connector MUST have the following naming convention:

Gateway Host_SID of the GRC system_Gateway Service Instance Number:

i.e → SAPGRC00_GRP_00

Furthermore, it is required to Activate this LDAP Connector.

Some common issues when activating this LDAP connector are:

- The Registered Program ID inside the SM59 was not registered.
- The Gateway Host and Service inside the SM59 are not correct.
- The LDAP library inside the SAP GRC system is missing and needs to be installed.

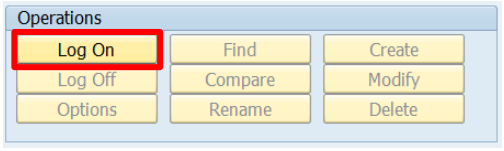
Once the LDAP connector is Active, you can perform the "Connection Test" inside for the TCP/IP Connection inside SM59 Transaction:

GRC Synchronization

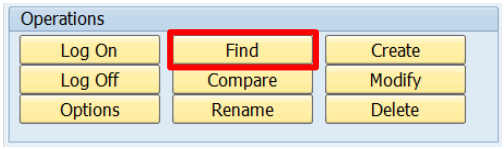
Once all the previous tasks were completed it is required to execute a synchronization operation to be able to establish Active Directory as User Data Source.

As a first step ensure that all the previous configuration is correct.

Execute "LDAP" Transaction and press "Log On":



After successfully connected to Active Directory, press "Find" button:



Use the following sentence to find out SAP User ID:

(&(samaccountname=SAP_USER_ID))

(&(mail=mail_address))

On the other side, it is required to perform some configuration steps inside the GRC system. First, define the Connector Group for LDAP connector using "SPRO" Transaction:

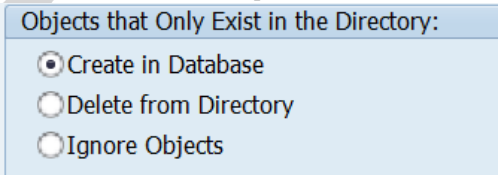
- Maintain Connectors and Connection Types.

Then, assign the LDAP Connector to the "PROV" and "AUTH" Scenario using "SPRO" Transaction:

- Maintain Connection Settings

Once the previous steps were completed it important to run "RSLDAPSYNC_USER" SAP Program with "SE38" Transaction. Include the LDAP Server and Connector that was defined before and then Execute:

- You can search for a Specific User in the beginning but it is important to test the full search.
- In case that you want to create all the records of the Active Directory inside the SAP you should include the option:



As soon as the Full Search is completed, it is required to perform the Full Synchronization using the SAP Program "GRAC_REPOSITORY_OBJECT_SYNC". Include the LDAP Connect and execute the "Full Sync Mode".

ACTIVE DIRECTORY as the MAIN USER DATA SOURCE

The previous steps details How to connect Active Directory to SAP GRC but this section will describe the strategy to have Active Directory as the Main User Data Source. It is required to Setup Active Directory as GRC User Data Source using "SPRO" Transaction:

- Maintain Data Sources Configuration.

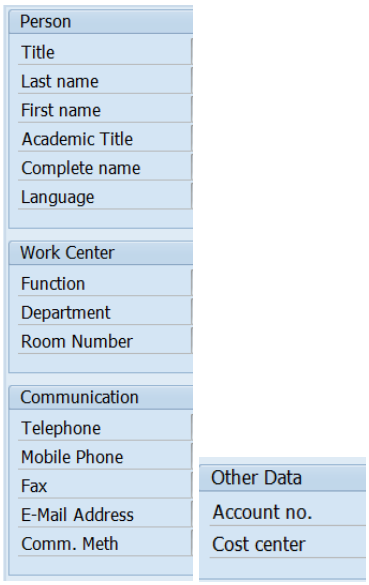
Then, include Active Directory as:

- User Search Data Source.
- User Detail Data Source.

After that, it is required to perform the mapping of the fields that are going to be used from the Active Directory to the SAP fields. This mapping is performed using SPRO Transaction:

- Maintain Mapping for Actions and Connector Groups

The recommendation is to map as much relevant fields as possible. The recommendation will be to map the following fields that matches the fields inside "SU01" Transaction:



i.e (SAP Field → Active Directory Field)

- USERID→SAMACCOUNTNAME
- LASTNAME →SN
- FIRSTNAME→ givenName
- FUNCTION→ title
- DEPARTMENT → Department
- TELEPHONE → telephoneNumber
- TELNUMBER → mobile
- EMAIL→MAIL
- PERSONNEL_NUMBER→ employeeID

The following field could be required for the provisioning process:

- MANAGERID→ MANAGER

The following fields could be required for the definition of User Defaults:

- LOCATION→ country
- COMPANY→company

The Usage of User Defaults functionality avoid to include manually the following fields:

- Logon Language
- Decimal Notation
- Date Format

If you have a requirement to use a specific field from the Active Directory inside SAP GRC, you need to create a Custom Field and perform the mapping also inside:

- Maintain Mapping for Actions and Connector Groups.

Finally, and in order to avoid changes, it is required to restrict manual changes of those fields that are being pulled from Active Directory. This configuration is performed through "SPRO" Transaction:

- Maintain End User Personalization

This option will allow to make all fields that have a value that comes from the Active Directory and Non-Editable.