# Setting Up Impersonation Of Data Warehouse Accounts By Directory Groups

For Data Warehouses that support Impersonation, AtScale offers the ability to mapp directory groups to Data Warehouse accounts. This feature changes the query's user identity to that of the mapped identity, thereby reducing the number of user accounts that must be created at the Data Warehouse level. Both the AtScale Engine and Design Center use these mapping rules when querying Data Warehouses.

## About This Task

After you have mapped groups from Microsoft Active Directory to AtScale groups, allowing users in those directory groups runtime permissions on published AtScale cubes, you can also map the directory groups to Data Warehouse accounts to enforce restrictions on data visibility. These mappings allow users in the directory groups to impersonate the Data Warehouse accounts when querying data.

When a user in one of the directory groups attempts to run a query against a published cube from a client BI application or the AtScale Design Center, AtScale verifies that the user has runtime permissions on the cube and also uses delegated authorization to allow the mapped Data Warehouse account to run the query.

## Before You Begin

- If you are an administrator or Super User for your AtScale organization, Impersonation is enabled from the **Create a Data Warehouse** dialog for your Data Warehouse. To enable impersonation, choose Settings from the top navigation menu, then select **Data Warehouses**. Click on **CREATE DATA WAREHOUSE**, select the desired Data Warehouse Type, and then enable **Impersonation** from the ensuing dialog. Note that not all Data Warehouses support Impersonation. Consult the Supported Platforms Documentation to determine if your Data Warehouse supports query impersonation with AtScale.
- Ensure that the directory groups that you want to map to Data Warehouse accounts are first mapped to AtScale groups that have runtime permissions on your cubes. See Granting Runtime Permission on Cubes to Groups of Externally Authenticated Users.

## Procedure

1. Choose **Security**, select **Impersonations**.
2. In the **Mappings to Impersonation** section, map a directory group to a Data Warehouse account that you specify in the **Impersonation** field. Then, click **Add**. Repeat this step for each such mapping that you want to add.
3. If any users belong to more than one directory group and are therefore mapped to more than one impersonation, click the **Order** tab and specify the order of precedence of the Data Warehouse accounts. Precedence descends from the top to the bottom of the list. Place the account with the highest precedence at the top, the account with the next highest precedence after that, and so on until the account with the lowest precedence.

## Example

For example, suppose that you plan to publish an AtScale cube that includes social security numbers. In your directory service, you have allocated users to the two groups onshore and offshore. The users in onshore are allowed to see this sensitive data in query results, while the users in offshore are not.

You set up the two Hadoop accounts full_access and partial_access. Account full_access allow users to see social security numbers, while account partial_access does not allow users access to that information.

You want the group onshore to use Hadoop account full_access when running queries, and you want the group offshore to use Hadoop account partial_access.

To ensure that each group uses only its specified Hadoop account, you follow these steps:

1. Map both directory groups to an AtScale group that has runtime permissions on the still unpublished cube. For this, you use the Group Mappings page, as described in Granting Runtime Permission on Cubes to Groups of Externally Authenticated Users.
2. Map each directory group to its corresponding Hadoop account, as detailed in the steps above.