



This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

Decisions Deployment Guide

Security

Contents

- [1 Security](#)
 - [1.1 Decisions Application Security](#)
 - [1.2 Decisions Data Mart Security](#)

Security

This page describes the requirements that must be fulfilled prior to Decisions installation.

Decisions Application Security

The following topics provide information about recommended procedures to follow to securely manage your Decisions applications:

- [Decisions_Administrators Active Directory Group](#)
- [Decisions_Users Active Directory Group](#)
- [User Management](#)

Decisions_Administrators Active Directory Group

The Decisions_Administrators Active Directory (AD) group contains the users that will be responsible for adding/updating configuration and mapping, building simulation models, managing Data Mart users, and importing weekly data.

Important

Genesys recommends that you limit access to the administration application because changes to the configuration and simulation models impact the outputs in the user application.

Create the Decisions_Administrators AD group for your enterprise prior to deployment of Genesys Decisions. The person who deploys Decisions in your enterprise requires the AD group information; the group will be entered in the Database Deploy tool as the AD Group for administrative access.

To create the Decisions_Administrators AD group:

- Create an AD group for Decisions_Administrators.
 - Add this AD group to the SQL server as a new login.
 - Set the server role to Public.
 - On the User Mapping page, select the checkbox next to the Decisions database.
 - In the Database role membership window, check `ctb_admin`, `db_datareader`, `db_datawriter`, and `public`.

Decisions_Users Active Directory Group

The Decisions_Users AD group contains the users that generate, maintain and develop what-if plans, run reports, and so on, in the user application. Users need to understand the configuration in order to effectively develop and interpret plans.

Create the Decisions_Users AD group for your enterprise prior to deployment of Genesys Decisions. The person who deploys Decisions in your enterprise requires the AD group information; the group will be entered in the Database Deploy tool as the AD group for user access.

To create the Decisions_Users AD group:

- Create an AD group for Decisions_Users.
- Add this AD group to the SQL Server as a new login.
 - Set the server role to `Public`.
 - On the User Mappings page, select the checkbox next to the Decisions database.
 - In the database role membership window, make sure that `public` is the only role that is checked.

User Management

To add a new user to the Decisions applications, the user will need to be added to the appropriate active directory group.

Decisions Data Mart Security

Service Account

- A Service Account is required for the Data Bus log in and must be configured as the owner of the Data Mart database.
 - In Active Directory create a user account to serve as a Service User
 - Password should be set to never expire
 - Service User account must have the rights to start and stop a service
- Administrators and Users will have to have accounts in the SQL Server. These can be individual accounts or Active Directory groups.

Data Mart Roles

There are two roles built into the Decisions Data Mart:

Data Mart Administrators Active Directory Group

- Data Mart Administrators can enable/disable Data Mart Security, give permission to a database user to

become a Data Mart user and can grant or revoke permissions to any Folder to any user.

- To be a Data Mart Administrator the SQL user must be assigned the DataMartAdmins database role.
- A user that is only a member of the DataMartAdmins database role does not have access to the actual data inside the Data Mart. A member of the DataMartAdmins database role only has access to those artefacts needed to perform administrative tasks.

Data Mart Users Activity Directory

- Data Mart Users are those people who either need to publish data to the Data Mart from the Decisions application or report on data from the Data Mart.
- To be a Data Mart User, the SQL user must be assigned the DataMartUsers database role.

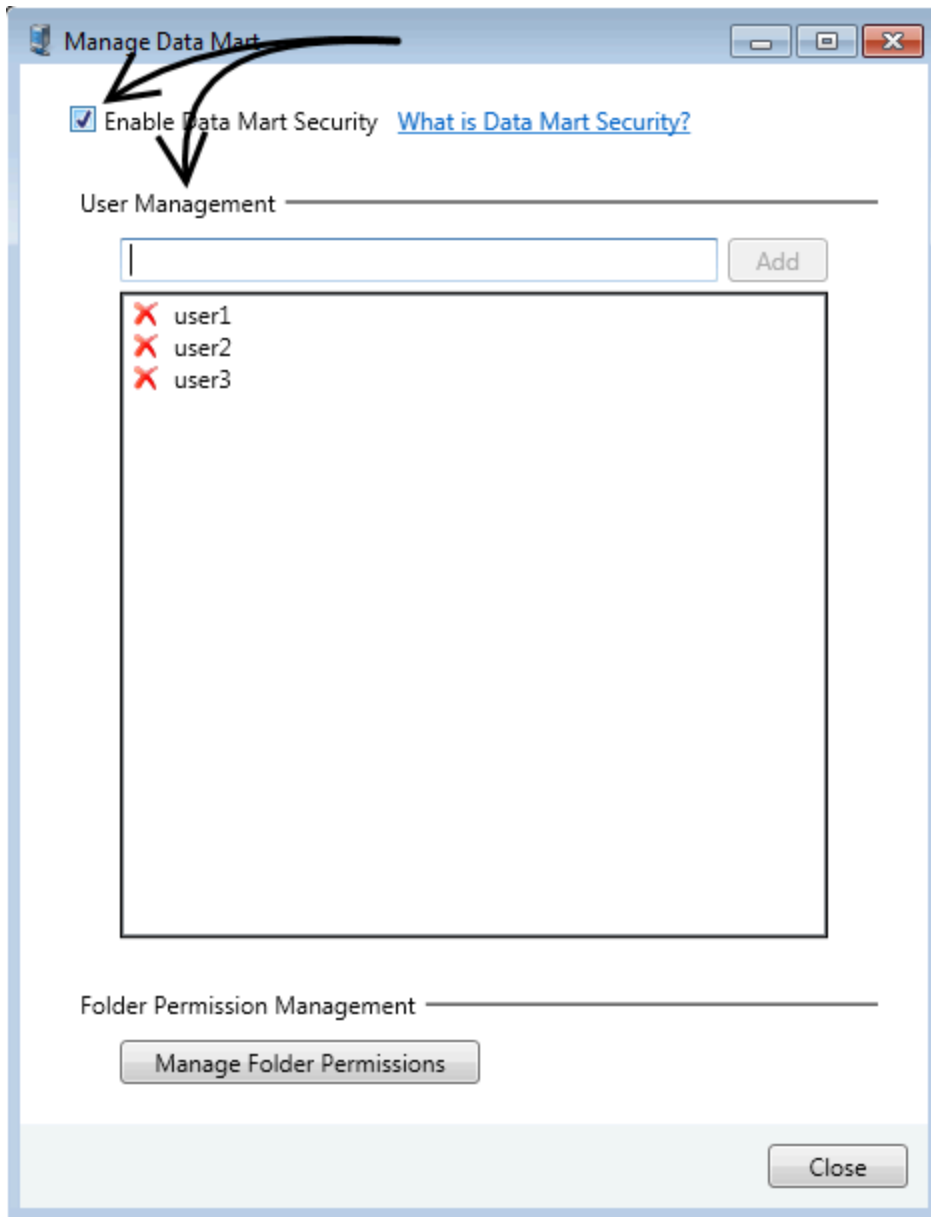
Enable Data Mart Advanced Security

Advanced Security for the Data Mart can be enabled or disabled by a Data Mart Administrator. Advanced Security is disabled by default.

- With Data Mart Advanced Security disabled, every user who has the DataMartUsers role can access the data in the Decisions Data Mart.

User Management

To add a new user to the Decisions Data Mart, you must add the user to the appropriate active directory groups. A user can be a member of the Data Mart Admin and/or the Data Mart User group.



In addition to the active directory groups, you must also add Data Mart users to the Data Mart through the Decisions Administration application.

- For users who will only publish scenarios to Data Mart, enter the Windows login name, including domain, as the new user name.
- For users who will create reports using the Data Mart data, but who will not publish to the Data Mart, enter the Windows or SQL login name, including domain, as the new user name. Whether you use the Windows or SQL login name depends, of course, on how the user will typically access the Data Mart.

Add a new Data Mart user

1. In the **User Management** text box on the **Manage Data Mart** dialog box (see the figure), enter the username of the new user.
Enter usernames that are either a Windows or SQL login name.
2. Click **Add**.