



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.

Genesys Info Mart Deployment Guide

Database Privileges

12/19/2025

Database Privileges

Genesys Info Mart requires access to source and target databases to perform a variety of operations. This page describes the types of database users and privileges Genesys Info Mart requires.

Database Object Owners and User IDs

Logically, there are four types of users for which you must provision user accounts:

- Info Mart — The user's account that is used by Genesys Info Mart jobs to access the Info Mart database schema for the purposes of:
 - Creating and modifying the Info Mart database schema
 - Extracting data from IDB — Applicable only to Microsoft SQL Server when the Info Mart and IDB databases are on the same server or when IDB is on a linked server (db link).
 - Processing the extracted data and storing it in the Info Mart database schema
 - Maintaining the Info Mart database schema
- ICON — The user's account that is used by Genesys Info Mart jobs to access the IDB schemas for the purposes of:
 - Modifying the IDB schemas to work with Genesys Info Mart
 - Extracting data from IDB
- Tenant Admin — The user's account that is used by a Tenant Administrator to access the Info Mart database schema and Tenant User schema(s) for the purposes of:
 - Creating and dropping the Tenant User schema(s) and views
 - Granting privileges to the read-only tenant users to access tenant-specific views in the Info Mart database schema through the Tenant User schema(s)
- Tenant User — The user's account that is used by a read-only tenant user to view tenant-specific data in the Info Mart database schema through views in the Tenant User schema.

Each User ID must have the necessary privileges to perform the required operations against the applicable database. For information about the required privileges, see [Required Database Privileges](#).

In principle, the User ID that you specify to connect to each database does not need to be the same as the Owner ID. You can create the database objects in a schema that is different from the User ID that accesses them, provided that the User ID has the required privileges, with the following exceptions:

- In PostgreSQL deployments using Genesys Info Mart releases earlier than 8.5.009, the name of the Tenant User schema must be the same as the name of the corresponding tenant User ID.
- In PostgreSQL deployments that include Reporting and Analytics Aggregates (RAA), the Info Mart

schema name must either be public or else be the same as the User ID.

Limitation

For new deployments, Genesys strongly recommends that you follow the [Recommendations for User Accounts](#) shown in the table below. Given the range of possible account setups, Genesys does not guarantee that Genesys Info Mart will function with all other user/owner account configurations that might be employed. Furthermore, internal changes in Genesys Info Mart processing over time might mean that, after migration, other user accounts that used to work no longer enable Genesys Info Mart jobs to access IDB or the Info Mart schema for certain purposes.

Refer to the [Database User Account Recommendations](#) in the *Genesys Info Mart 8.5.x Release Note* for information about possible workarounds if you encounter permissions-related issues after deployment.

Important

In Microsoft SQL Server, all database objects are contained in schemas, instead of being owned by a database owner. The SQL Server logins are mapped to database users, who can own objects in the various schemas. In addition, a default schema is configured for each database user, to contain unqualified database objects. In this document, for Microsoft SQL Server, the term *Owner ID* refers to the database user who owns the object — for example, the database user who created a view.

Recommendations for User Accounts

RDBMS	For Database	Recommendations
Microsoft SQL Server	Info Mart and IDB	<ul style="list-style-type: none"> The Info Mart database should have one Info Mart schema. IDB should have one ICON database schema. If the Info Mart schema is not dbo, contact Genesys Customer Care before executing any SQL scripts and before migration.
Oracle	Info Mart and IDB	<ul style="list-style-type: none"> User Name: <code><Database schema owner></code> default-schema (DAP option): <code><Database schema owner></code>
PostgreSQL	Info Mart and IDB	<ul style="list-style-type: none"> The Info Mart database should have one Info Mart schema. IDB should have one ICON

RDBMS	For Database	Recommendations
		<p>database schema.</p> <ul style="list-style-type: none"> See above for specific requirements for the Info Mart schema name in deployments that include RAA.

Identifying the owner and user accounts that you will use in your Genesys deployment is an important step in your deployment and installation planning. After you have identified the accounts that you will use, record the IDs and passwords on the applicable worksheet that is provided on the [Database Worksheets](#) page. You will need this information to create the database schemas and to specify connection parameters when you configure the DAP(s).

Required Database Privileges

The following table summarizes the user account privileges that are required for the respective source and target database schemas.

Important

Genesys recommends that you explicitly grant the required privileges to the respective users. Do not assume that granting DBA privileges will be sufficient to enable the user account to perform all required operations.

Required User Account Privileges

User Account	Database	Required Privileges ^a
Info Mart	IDB	<ul style="list-style-type: none"> SELECT on all tables and views (for example, include this user in the db_datareader role in IDB) <p>Note: This user account on IDB is required only for Microsoft SQL Server when Info Mart and IDB databases are on the same server or IDB is on a linked server (db link).</p>
	Info Mart schema	<ul style="list-style-type: none"> CREATE, DROP, and ALTER tables, views, indexes, procedures, and, if applicable, partitions

User Account	Database	Required Privileges ^a
		<ul style="list-style-type: none"> • SELECT on all tables and views • INSERT, UPDATE, and DELETE on all tables • RDBMS-specific privileges that are required to truncate tables • CREATE and EXECUTE on all stored procedures • (For Oracle only) EXECUTE on DBMS_LOCK • (For databases that implement partitioning) RDBMS-specific privileges that are required to CREATE, DROP, and ALTER tables, indexes, and partitions • (For PostgreSQL only, if tenant views are used) Tenant view owner permissions
	Tenant User schema(s)	(For PostgreSQL only, if tenant views are used) <ul style="list-style-type: none"> • In releases earlier than 8.5.010, Schema owner permissions • Starting with release 8.5.010, Tenant User role
ICON	IDB	<ul style="list-style-type: none"> • SELECT on all tables and views • CREATE and DROP tables, views, and indexes • INSERT, UPDATE, and DELETE on all IDB tables
Tenant Admin	Info Mart schema	<ul style="list-style-type: none"> • EXECUTE on all stored procedures • CREATE, SELECT, and INSERT on all tables • CREATE, DROP, and SELECT on all views and sequences

User Account	Database	Required Privileges ^a
Tenant User ^b		<ul style="list-style-type: none"> GRANT access to views for Tenant users
	Tenant User schema(s)	<ul style="list-style-type: none"> CREATE and DROP views
	Info Mart schema	<ul style="list-style-type: none"> SELECT on the tenant-specific view in the applicable Tenant User schema Note: Privileges for the Tenant User to access views in the Info Mart schema are granted by the Tenant Admin when the make_gim_view_for_tenant.sql script is run.
	Tenant User schema	<ul style="list-style-type: none"> SELECT on all views

a. Privileges are called *permissions* in Microsoft SQL Server.

b. Applicable only for read-only views, which are strictly required only for multi-tenant deployments.