Genesys Interactive Insights Deployment Guide

After Installation, What Additional Steps Do I Perform?

12/17/2025

Contents

After Installation, What Additional Steps Do I Perform?

After you have installed Genesys Interactive Insights (GI2), you must manually perform additional setup steps before you operate the GI2 reports.

Readying Genesys Info Mart for Aggregation

A Genesys Info Mart 8.5 installation that has the Reporting and Analytics Aggregates (RAA) option deployed contains the tables and views that are referenced by the GI2 reports. To prepare the Genesys Info Mart environment for GI2 operation, you must perform additional setup steps, including:

- **Reposition the \agg Subdirectory**: The GI2 installation routine deploys the **\agg** subdirectory to the Interactive Insights root folder. This subdirectory and its contents, however, must be placed in the Genesys Info Mart root folder in order to be recognized by Genesys Info Mart. Copy this directory to the Genesys Info Mart root folder.
- **Set Aggregation-Related Configuration Options**: To enable aggregation, you must appropriately set aggregation-related configuration options (such as **aggregation-engine-class-name**, **run-aggregates**, and business-specific aggregation thresholds) in the Genesys Info Mart application object in Configuration Manager. These options are described in the *Reporting and Analytics Aggregates Deployment Guide*.

Utility Views Specific to GI2

Running aggregation for the first time executes an internal script against your Genesys Info Mart database to set up the necessary views that mostly facilitate data processing for the GI2 reports.

Genesys Info Mart Multi-Tenant Environments: For Genesys Info Mart environments that contain more than one tenant, run RAA with the **updateAliases** runtime parameter to create tenant views of GI2 objects. For a description of this parameter and an example of its use, refer to the *Reporting and Analytics Aggregates Deployment Guide* and the *Reporting and Analytics Aggregates User's Guide*, respectively.

Customizing BO

Use the procedures in this section to apply, or re-apply, customizations to BO.

Procedure: After Full Installation

Purpose: The GI2 installation routine silently runs the script **gi2_customize_bo.bat/sh** to customize the appearance of BO, which also replaces some files in the BI Tomcat webapps directory. After installation, complete the following steps to restore the contents of the BI Tomcat webapps directory.

Steps

1. Stop Tomcat.
2. Delete the directory **BOE_TOMCAT_ROOT%\work\Catalina\localhost\BOE**
3. Restart Tomcat.

Procedure: After Fix Pack Installation

Purpose: The fix packs that are provided by SAP come with their own installer. The latest supported fix pack, if any, is provided in the Genesys-provided installation package. This software provides a patch to BI software that you install manually after BI installation. Instructions for installing the fix pack are provided with the installation package. If you install this fix pack after installation of GI2, you must also re-execute the **gi2_customize_bo** script. (The **gi2_customize_bo.bat** (Windows) script is described in What Application Files Are Installed?)

Steps

1. Execute the **gi2_customize_bo** script.
2. Stop Tomcat.
3. Delete the directory **BOE_TOMCAT_ROOT%\work\Catalina\localhost\BOE**
4. Restart Tomcat.

Procedure: Customizing Date and Time Display

Purpose: Optionally, you can configure the date and time values that appear in GI2 reports. By default, the prompts for dates and times do not save custom values you enter, and reports

always show default date and time values. To change this behavior, complete the following steps.

Steps

1. Open the Information Design Tool.
2. In the GI2 universe, enable **Keep Last Value** for the following date/time related parameters: **Pre-set Day Filter, Pre-set Date Filter, Start Date, End Date, Report Date**.
3. Restart the BI server.

Procedure: Customizing GI2 User Rights

Purpose: Use this procedure to manually configure rights that are not provided in the LCMBIAR file.

Steps

1. Start the Central Management Console (CMC).
2. On the **Applications** tab, right-click the **Central Management Console** application element, and in the context menu, select **CMC Tab Access Configuration**.
3. In the **CMC Tab Access Configuration: CMC** dialog box, select **Restricted**, and click **Save**.
4. Set the following permissions:
   - **Inboxes**: For each GI2 user, select **User Security -> Add Principal**, and assign the user access level **Full Control (Owner)**.
   - **Personal Folders**: For each GI2 user, select **User Security -> Add Principal**, and assign the user access level **Full Control (Owner)**.

Setting Up Attached Data

Reports are based on the configuration of user data in your environment—user data that is highly customizeable within any given environment. To use the GI2 reports without modifying the universe or measure definitions, you must configure user-data data structures within Genesys Info Mart in a specific manner.

For a detailed example that demonstrates how to configure user-data data structures, see the Configuring Social Media User Data section in the *Genesys Interactive Insights User's Guide*.

Linking the Universe to Your Data Mart

The GI2 reports call upon measures that were designed using the Information Design Tool. These measures are predefined in the GI2 universe that you imported but they are not pre-connected to your specific Genesys data source out of the box. You must define such a connection and assign it within Information Design Tool so that the reports that reference these measures will pull contact center data from your Info Mart database.

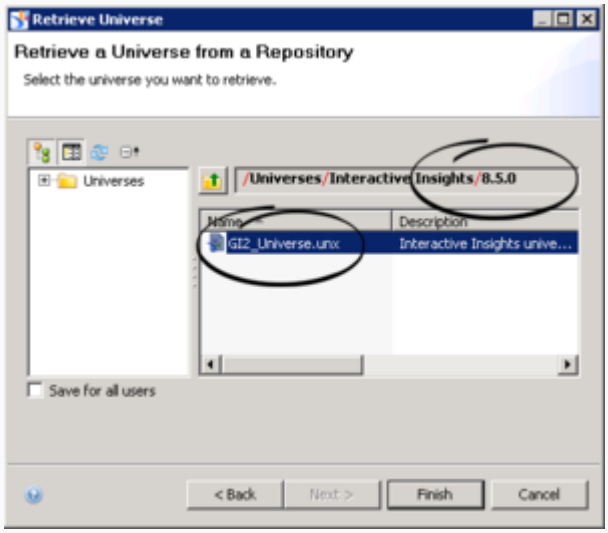
> **Important**
>
> The **GI2_GIM_DB** connection that the GI2 installation routine deploys is reserved for Genesys use. Use or modify this connection only if directed, for example, as described in Using the Default Connection.

Use the following procedures to link the GI2 Universe to your Info Mart database.

Procedure: Importing the Universe to the Information Design Tool

Purpose: There are many ways to define database connections. In all cases, however, the first step is to import the GI2 universe to your local Information Design Tool application, as follows:

Steps



Importing a Universe Into the Information Design Tool

1. From the Start menu, select **SAP Business Intelligence** > **Information Design Tool**.
2. In the **Open** dialog box, specify the system and user credentials, and click **OK**.
3. In the Information Design Tool, from the **File** menu, click **New** > **Project**.
   The **New Project** dialog box appears. Enter a **Project Name** (this is the local project where your files will be stored while you edit them) and optionally choose a different location.
4. In the Information Design Tool, from the **File** menu, click **Retrieve a Published Universe**, and **From a Repository**.
5. In the **Retrieve Universe** dialog box, click **Next**, select the **Interactive Insights** folder. Double-click the release subfolder, and click **OK**.
   The Figure **Importing a Universe Using the Information Design Tool** shows this dialog box with the 8.5.0 folder selected.
6. Select the GI2_Universe from the list of available universes, and click **Finish**.

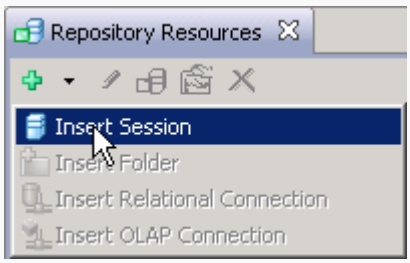
Next Steps

The Information Design Tool imports the universe and displays its classes, objects, and table relationships in the Universe Window. This local copy of the universe is now available on your workstation for viewing and editing universe elements. Any changes you make to the definitions of universe elements do not take effect until you publish the universe back to the repository. See Customizing Measure Definitions and Publishing the Universe Back to the Repository for further information.

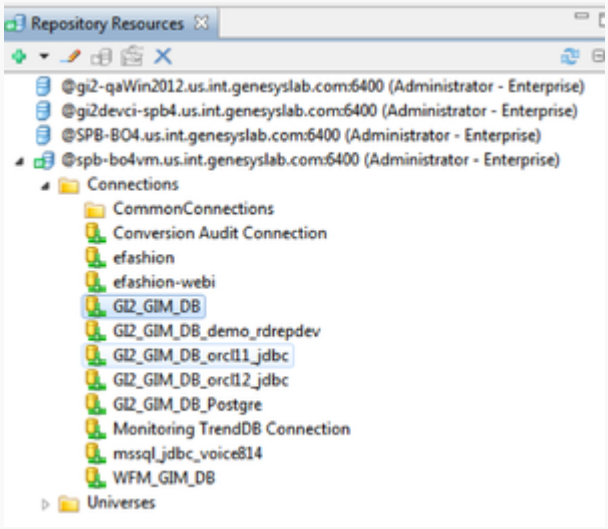
Procedure: Using the Default Connection

Purpose: Use this procedure to update the default GI2_GIM_DB connection to point to your data source, so that you can use it to link the universe objects to the tables in your Data Mart. Alternatively, you can create a new connection by following the steps in Defining a New Connection.

Steps



Repository Resources: Insert Session



Select the GI2_GIM_DB Connection

1. Open the Information Design Tool.
2. Select **File > New > Project**. Enter the Project Name, and click **Finish**. A new project is created, and appears on the **Local Projects** tab.
3. On the **Repository Resources** tab, click **+** (Insert), and select **Insert Session** as shown in the Figure **Repository Resources: Insert Session**.
4. In the **System** field, enter the BI instance name. Enter the User name (Administrator) and associated password, and click **OK**.
5. Open the **Connections** folder, and select the **GI2_GIM_DB connection**, as shown in the Figure **Select the GI2_GIM_DB Connection**.
6. Click the right mouse button and, in the context menu, select **Open**.
7. Click **Change Driver**, select a driver, and enter appropriate connection parameters.
8. Test the connection, then choose **File > Save** to save the connection.

9. Close the **Connection** tab.

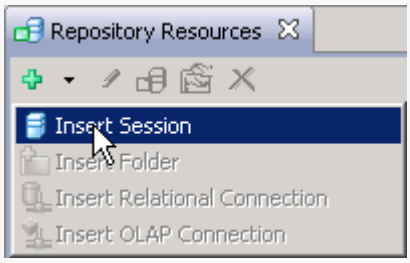
Next Steps

Next, publish the universe back to the repository using the steps in Publish the Universe Back to the Repository.

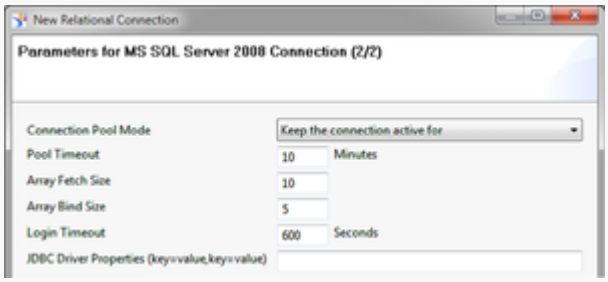
Procedure: Defining a New Connection

Purpose: Use this procedure to define a new connection, which you can use to link the universe objects to the tables in your Data Mart. Alternatively, you can reuse the default connection by following the steps in Using the Default Connection.

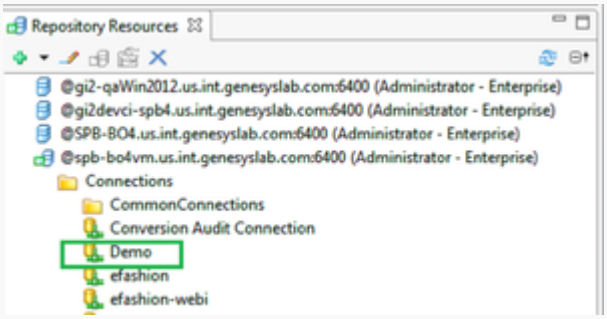
Steps



Repository Resources: Insert Session



MS SQL Connection Parameters



The Newly Created Connection

1. Open the Information Design Tool
2. On the **Repository Resources** tab, click **Open session**, or click **+** (Insert), and select **Insert Session** as shown in the Figure **Repository Resources: Insert Session**.
   The **Open Session** dialog box appears.
3. In the appropriate fields, enter the BI instance name, the User Name (Administrator), and associated Password.
4. Click **OK**.
5. Click **+** (Insert), and select **Insert Relation Connection**.
   The **New Relational Connection** dialog box appears.
6. Type a name for the new connection, and click **Next**.
7. Select the appropriate driver for your database middleware, and click **Next**.
   Note: To create a JDBC connection, you must also configure the JDBC driver. SAP provides more information, in the 'Creating JDBC Connections' section of the Data Access Guide for SAP BusinessObjects Business Intelligence platform.
8. Enter appropriate connection parameters.
   The parameters available vary depending on the driver type you selected for the connection; the Figure **MS SQL Connection Parameters** shows parameters for MSSQL server.
9. Test the connection before clicking **Next**.
10. Click **Finish**.
    The created connection appears in the list of available connections for the BI server, as shown in the Figure **The Newly Created Connection**.

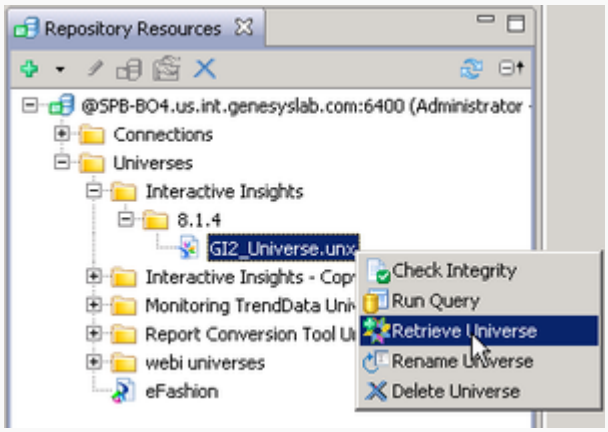
Next Steps

Next, link your connection to the universe by using the steps in Connecting to the GI2 Universe, and then publish the universe back to the repository using the steps in Publish the Universe Back to the Repository.

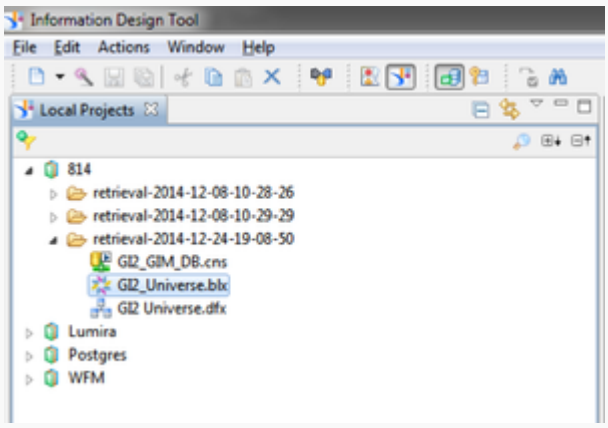
Procedure: Connecting to the GI2 Universe

Purpose: Once you have created a connection (Defining a New Connection) or changed the default connection (Using the Default Connection), use this procedure to link the universe objects to the connection.

Steps



Retrieve Universe



Select the Local Project

1. Open the Information Design Tool
2. Make sure your project is open in the Information Design Tool.
3. In the **Repository Resources** pane, expand **Connections**, right-click the connection you want to link to the universe, and select **Create Relational connection shortcut**.
   The **Select A Local Project** dialog box appears.
4. Select the project created.

5. On the **Local Projects** pane, double-click **GI2 Universe.dfx** to open it.
6. On the **GI2 Universe.dfx** pane, click **Connection**, and in the **Connection** navigation tree, right-click the existing connection and select **change**.
   The **Change Connection** dialog box appears.
7. Select the connection shortcut created in Step 2, and click **Finish**.
8. Click **Save** to save **GI2 Universe.dfx**.

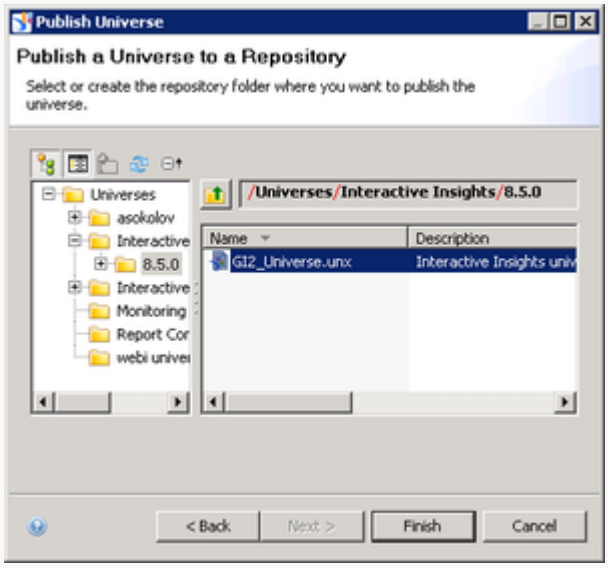
Next Steps

Next, publish the universe back to the repository using the steps in Publish the Universe Back to the Repository.

Procedure: Publishing the Universe Back to the Repository

Purpose: The changes that you make to the universe are local. To make them available to others who might run reports, you must publish the universe back to the repository, as follows:

Steps



Publishing Changes Back to the Repository

1. Open the Information Design Tool.
2. In the **Repository Resources** pane, open the folder: **Universes > Interactive Insights >**

8.5.0.

3. Right-click **GI2_Universe.unx**, and in the context menu select **Retrieve Universe**, as shown in the Figure **Retrieve Universe**.
4. Select the local project you want to publish, as shown in the Figure **Select the Local Project**.
5. In the local projects pane, open the folder, which has a name in the format *retrieval-<date>*, such as **retrieval-2016-12-24-19-08-50**.
6. Select the **GI2_Universe.blx** element, click the right mouse button and from the context menu, select **Publish > To a Repository**.
7. In the **Publish a Universe to a Repository** dialog box, for the first step (Check Universe Integrity) click **Next**. The next step (Select or create the repository folder where you want to publish the universe.) appears.
8. Open the folder: **Universes\Interactive Insights\8.5.0**, and select **GI2_Universe.unx** as shown in the Figure **Publishing Changes Back to the Repository**.
9. Click **Finish**.
   The message **Overwrite published universe?** appears.
10. Click **Yes**, and close the dialog box.
11. From the **File** menu, select **Publish** > **Publish Connection to a Repository**.
12. From the **Groups** list, select all of the groups to which this connection applies.
13. From the **Universes** list, select the name of your universe (for example, **GI2_Universe**).
14. Click **OK**.

The updated universe—with connection to your data source defined—is now available to the user groups that you specified.

Manually Setting Up GI2 Access Levels, Groups, and Permissions

The GI2 installation routine silently deploys the GI2 objects that are stored in the **insights.lcmbiar** file, and assigns permissions to these and other objects.

As a BI administrator, you can use the Import Wizard to import these objects with their permissions applied to universe elements (see Manually Importing Objects and Data Elements), or create the objects yourself from scratch and assign permissions to various objects by following the instructions in the following four procedures.

> **Tip**
> If your installation of GI2 was successful, remove any GI2 objects that exist in the BI

repository prior to importing the universe manually by using the Import Wizard, so as to avoid creating duplicate objects (following Step 3 in Additional Manual Steps to Finish the Uninstall).

Procedure: Setting Up Access Levels

Purpose: If you opt not to run the Import Wizard to deploy the Interactive Insights report access levels (which are groupings of permissions that are applied to groups and/or users), you can create them manually as the administrative user within the CMC. GI2 predefines the following access levels:

- Interactive Insights report developer access level
- Interactive Insights report editor access level
- Interactive Insights report viewer access level
- Interactive Insights report basic access level

Though these access levels correspond to the GI2 groups, the access levels are progressive—that is, they build upon the access levels of others. Use this procedure to manually create these access levels.

Steps

1. Within the Central Management Console (CMC), select the **Access Levels** section.
2. Click **Manage > New > Create Access Level**.
3. Enter the name for the new access level: "`Interactive Insights report developer access level`".
4. Click **OK**.
5. Double-click the access level that you just created to open its properties.
6. Under **Included Rights**, click **Add or Remove Rights**, select the appropriate rights for each collection (shown in the Table: **Definitions of the Predefined Interactive Insights Access Levels**).
7. Click **OK**.
8. Repeat Steps 2–7 for the remaining two GI2 access levels.

Table: Definitions of the Predefined Interactive Insights Access Levels

Collection	Type	Name of Right	D	E	V	B
System	Connection	Data Access	✓	✓	✓	✓
General	General	Add objects	✓	✓		

		to folders that the users owns				
General	General	Add objects to the folder	✓	✓		
General	General	Copy objects that the user owns to another folder	✓	✓		
General	General	Copy objects to another folder	✓	✓		
General	General	Delete instance	✓			
General	General	Delete instances that the user owns	✓			
General	General	Delete objects	✓			
General	General	Delete objects that the user owns	✓			
General	General	Edit objects	✓	✓		
General	General	Edit objects that the user owns	✓	✓	✓	
General	General	Modify the rights users have to objects	✓			
General	General	Modify the rights users have to objects that the user owns	✓			
General	General	Schedule document that the user owns			✓	
Application	WebI	Data Tracking: Enable for users			X	
Application	WebI	Data Tracking: Enable			X	

		format display changes by users				
Application	WebI	Enable drill mode		✓	✓	
Application	WebI	Enable formula and variable creation			X	
Application	WebI	Enable HTML Report Panel		✓	X	
Application	WebI	Enable interactive HTML viewing (if license permits)			X	
Application	WebI	Enable Java Report Panel			X	
Application	WebI	Enable Query - HTML			X	
Application	WebI	Extend scope of analysis		✓	✓	
Application	WebI	Edit this object		✓		
Application	WebI	Interactive: Formatting - Enable toolbar and menus			X	
Application	WebI	Interactive: General - Ability to hide / show toolbars			X	
Application	WebI	Interactive: General - Edit 'My Preferences'			X	
Application	WebI	Interactive: General - Enable right click menu			X	
Application	WebI	Interactive: Left pane - Enable available objects,			X	

		tables and charts				
Application	WebI	Interactive: Left pane - Enable data summary			X	
Application	WebI	Interactive: Left pane - Enable document structure and filters			X	
Application	WebI	Interactive: Left pane - Enable document summary			X	
Application	WebI	Interactive: Reporting - Apply and remove existing alerts			X	
Application	WebI	Interactive: Reporting - Create and edit break			X	
Application	WebI	Interactive: Reporting - Create and edit predefined calculation			X	
Application	WebI	Interactive: Reporting - Create and edit report filter			X	
Application	WebI	Interactive: Reporting - Create and edit sort			X	
Application	WebI	Interactive: Reporting - Insert and remove report, table, chart and cell			X	
Application	WebI	View SQL			X	
Application	WebI	Web Intelligence			X	

		Rich Client: Save a document locally on the file system				
Application	WebI	Web Intelligence Rich Client: Create a document			X	
Application	WebI	Web Intelligence Rich Client: Enable a client to use it			X	
Application	WebI	Web Intelligence Rich Client: Export a document			X	
Application	WebI	Web Intelligence Rich Client: Import a document			X	
Application	WebI	Web Intelligence Rich Client: Print a document			X	
Application	WebI	Web Intelligence Rich Client: Save a document for all users			X	
Application	WebI	Web Intelligence Rich Client: Send by mail			X	
Content	WebI	Edit Query	✓			
Content	WebI	View SQL	✓			
Content	WebI	Export the report's data			✓	
Content	WebI	Refresh List of Values			✓	
Content	WebI	Refresh the report's data			✓	
Content	WebI	Save as CSV			✓	

Key:

- D=Developer Access Level
- E=Editor Access Level
- V=Viewer Access Level
- B=Basic Access Level
- A ✓ signifies that the right applies to the indicated access level.
- An X signifies that the right is blocked for the indicated access level.

Procedure: Creating GI2 Groups

Purpose: In addition to the Interactive Insights access levels, the Import Wizard also deploys GI2 user groups. Use this procedure to create them manually and add users.

Steps

1. In the CMC, select the **Users and Groups** section and over **Group List**, right-click **New**, and select **New Group**.
   The **Create New User Group** page appears.
2. In the **Group Name** field, type `Interactive insights report developers`.
3. In the **Description** field, type an appropriate description.
4. Click **OK**.
5. Select **User List**.
6. From the **Available users or groups** list, select **Developer** and any other user who belongs to this group, and move your selection to the **Selected users/groups** list.
7. Click **Close** to close the user security properties.
8. Repeat Steps 2–7 to create the following user groups: **Interactive Insights report editors**, **Interactive Insights report viewers**, **Interactive Insights report basic**, **Interactive Insights access restrictions**, and finally create **Interactive Insights custom access restrictions** as a subgroup of **Interactive Insights access restrictions**.

   To maintain flexibility, permissions (other than the default) are not assigned to the GI2 users or groups. Instead, Genesys recommends that you assign permissions directly to the objects that users access, as described in Setting Permissions for BI Objects.

Procedure: Hiding Unused Folders

Purpose: BI 4.1 software includes folders that are not used by GI2. Among them are the following: **Auditing, Report Conversion Tool, and Report Samples**. Use this procedure to hide these folders from users in the GI2 report groups.

Steps

1. In CMC, click the **Folders** section.
2. For each folder you want to hide, right-click the folder, and select **User Security**.
3. Click **Add Principals**. The **Add Principals** page appears.
4. Select the **Group List**.
5. From the **Available users or /groups** list, select the **Interactive Insights [*]** user groups and click **>** to move them to the **Selected users or groups** list box.
6. Click **Add and Assign Security**. The **Assign Security** page appears.
7. Clear the **Inherit From Parent Folder** and **Inherit From Parent Group** check boxes, and click **OK**.
   Because no access levels were explicitly selected, a dialog box appears, prompting you to confirm this action.
8. Click **OK**.
   CMC returns to the User Security properties of your selected folder and displays the added groups.
9. Click **Close**.

   With these changes applied to each folder, the folders are invisible to GI2 users. However, administrative users continue to see the hidden folders.

Procedure: Setting Permissions for BI Objects

Purpose: Use this procedure to manually set permissions on the objects used by GI2, including the universe, the **Interactive Insights** folder and connection, and even the BI Launch Pad and Web Intelligence applications.
The Table **Mapping of Access Levels to BI Objects** lists the user security properties of objects that the GI2 installation routine sets. To set these manually, perform the following steps within Central Management Console (you must be administrative user):

Steps

1. Set top-level security for root objects or user security for other objects:
   - To set top-level security, open the appropriate CMC section (such as Connections, Folders, or Universes), select **Manage** > **Top-Level Security** > **All <Objects>**.
   - To set user permissions, open the appropriate CMC section (such as Connections, Folders, or Universes), right-click the desired object from that section, and select **User Security**.
2. Click the **Add Principals** button, and select **Group List**.
3. From the **Available Users or Groups** list box, select the groups indicated for the object (see the Table below) and move them to the **Selected users or groups** list box.
4. Click the **Add and Assign Security** button, either clear or mark the **Inherit From Parent Folder** and **Inherit From Parent Group** boxes as indicated for the object on the Table **Mapping of Access Levels to BI Objects**, and apply your changes.
   - On the **Access Levels** tab, select the appropriate access level from the **Available Access Levels** list, and move it to the **Assigned Access Levels** list.
   - Apply your changes, and click **OK**.
5. Click **Close** to close the user security properties.

Table: Mapping of Access Levels to BI Objects

CMC Section	Object Name	Principal[1]	Inheritance From Parent ...		Access Level[2]						
			...Folder	...Group	D	E	V	B	Full	Vw	VOD
Connections	<Connections root folder>	Developers	✓	✓	✓		✓				
	GI2_GIM_DB	Restrictions	✓	✓			✓				
		Basic	✓	✓				✓			
		Developers	✓	✓	✓		✓				
		Editors	✓	✓			✓				
		Viewers	✓	✓			✓				
Universes	<Universe root folder>	Developers	✓	✓						✓	
	Interactive Insights (folder)	Developers	✓	✓					✓		
	GI2_Universe	Restrictions	✓	✓			✓				
		Developers	✓	✓					✓		
		Editors	✓	✓		✓	✓				

		Viewers	✓	✓			✓				
Application	Web Intelligence	Restrictions	✓	✓			✓				
		Basic	✓	✓				✓			
		Developers	✓	✓					✓		
		Editors	✓	✓		✓					
		Viewers	✓	✓			✓				
	BI Launch Pad	Restrictions	✓	✓							✓
		Basic	✓	✓				✓			
		Developers	✓	✓							✓
		Editors	✓	✓							✓
		Viewers	✓	✓							✓
	Information Design Tool	Developers	✓	✓					✓		
Folders	<InfoView root>	Restrictions	✓	✓			✓				
		Basic	✓	✓			✓				
		Developers	✓	✓			✓				
		Editors	✓	✓			✓				
		Viewers	✓	✓			✓				
	Interactive Insights	Restrictions	✓	✓			✓				
		Basic	✓	✓				✓			
		Developers	✓	✓	✓	✓	✓				
		Editors	✓	✓		✓	✓				
		Viewers	✓	✓			✓				

Key:
[1] **Principals:**

- Interactive Insights access restrictions
- Interactive Insights report developers
- Interactive Insights report viewers
- Interactive Insights report editors
- Interactive Insights report basic

[2] **Access Levels:**

- D= Interactive Insights report developer access level
- E = Interactive Insights report editor access level
- V = Interactive Insights report viewer access level
- B = Interactive Insights report basic access level
- Full = Full Control

- Vw = View
- VOD = View On Demand

Setting Data-Access Restrictions for Multi-Tenant Environments

In addition to the permissions that you can set within CMC to control access to various BI repository elements, you can also set restrictions on user access to data by limiting the objects, rows, query types, and connections that are available to users through the Universe Design Tool application. BI defines a restriction as a named group of constraints that can be applied to a group or user account for a universe.

Through the use of restrictions, administrators can control what data users see in the GI2 reports. Use this feature if your data source stores data for more than one tenant. For instance, within one universe, you can define several connections—each of which accesses a different tenant view within the same Info Mart—and then create and apply connection restrictions to each tenant to ensure that its users see only the data that is pertinent to that tenant.

The login to Web Intelligence identifies the user (and hence the user group) and the access permissions that are assigned to that user within the repository; the restriction defines which connection the user can use to access data within a specific universe. No changes to the definitions of dimensions or measures, for instance, or to the design of the reports are then required to provide tenant-specific data in your reports.

The benefits of this one-universe approach include:

- Consistency in measure definitions across the enterprise.
- Reduced maintenance costs—having to manage only one universe (instead of one universe per tenant).
- Single source.
- Optimized use of network resources.

Genesys Info Mart supports several methods of configuring multi-tenant environments, including:

- A separate schema for each tenant.
- A separate schema for each group of tenants.
- One database/one schema for all tenants (where each tenant can see other tenants' data).

Configuration depends largely on the capabilities that are provided by your chosen RDBMS and on the data access security measures that are established within your enterprise. Please refer to the *Genesys Info Mart Deployment Guide* for further information.

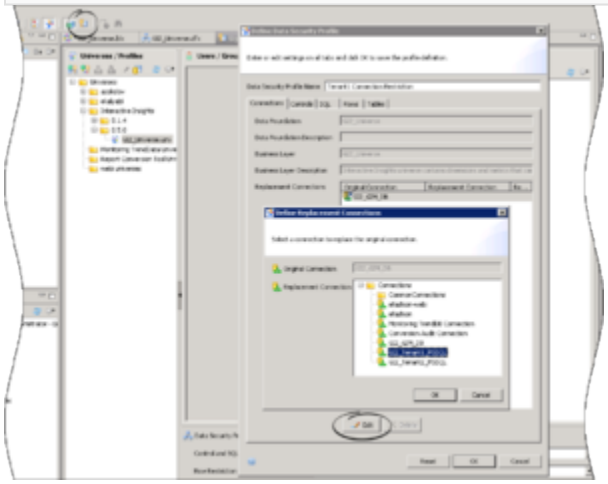
For Microsoft SQL 2005 RDBMS, note the following: In the scenario in which a separate schema has been created within one database for each tenant, you must ensure that individual tenant logins map to the respective database owner for the tenant schema or that the default schema for each tenant login matches that of the owner for that schema. Furthermore, this login must not be *sysadmin*; otherwise, elements in the GI2 universe might point to an unintended set of objects in the Info Mart database.

Procedure: Creating Users and Groups in Multi-Tenant Environments

Purpose: The steps that are provided in Manually Setting Up GI2 Access Levels, Groups, and Permissions describe the procedures for creating GI2 users and groups and assigning users and groups to various repository elements. The naming convention used for the users and groups and the presentation of the steps is suitable for a single-tenant environment. However, with the exception of the names that you choose for users/groups, the procedures are identical for multi-tenant environments.

Steps

1. If you have not done so already, complete the steps that are defined in the following sections to add GI2 views to each tenant schema (or database, as applicable) and to define connections to them, respectively: Utility Views Specific to GI2 and Linking the Universe to Your Data Mart. When you are naming data-source connections (Step 6 of Defining a New Connection), give them tenant-identifying names, such as *Tenant1Connection* or *GI2_Tenant_Oracle10g*.
2. To set up users and groups for your tenants, follow the steps that are provided in Manually Setting Up GI2 Access Levels, Groups, and Permissions—again, giving them tenant-identifying names, such as *Tenant1 Report Viewers (group)* and *Tenant1 Viewer (user)*. The concept of assigning user and group permissions in CMC to connections (discussed in Setting Permissions for BI Objects) is different from the concept of assigning connection restrictions to users and groups within the Information Design Tool. Unlike the Information Design Tool, CMC does not enable you to define a connections map within one universe to map different data-source connections to defined users and/or groups.



Profiles in the Security Editor

Procedure: Creating Profiles to Restrict Access

Purpose: Within the Information Design Tool, use the steps in this procedure to create and define restrictions in the Security Editor, and apply them to the tenant users and groups that you created earlier in Creating Users and Groups in Multi-Tenant Environments.

Steps

1. In the Information Design Tool, click **Security Editor**.
   The Figure **Profiles in the Security Editor** shows the Security Editor.
2. On the **Universe/Profiles** tree, open the folder where the GI2_universe.unx file is stored, select **GI2_universe.unx**, and click **Insert Data Security Profile**.
   The **Define Data Security Profile** dialog box appears, in which you can create a new restriction.
3. In the **Data Security Profile Name** field, enter a suitable name for a restriction for a particular tenant—for example, *Tenant1 Connection Restriction*, where *Tenant1* is the name of the tenant.
4. Click **Edit**.
   The **Define Replacement Connections** dialog box appears.
5. From the **Replacement Connection** list, select the appropriate data-source connection for the tenant—for example, **GI2_Tenant1_MSSQL**.
6. Click **OK** to save the restriction, and **OK** again to close the **Define Data Security Profile** dialog box.
7. Repeat Steps 2 through 6 for each connection restriction that you want to define.
   Tip: Because the Define Data Security Profile dialog box does not have an **Apply** button, you might want to save your changes periodically by closing the dialog box (clicking **OK**) and reopening it, especially if you have several restrictions to define.
8. In the Security Editor, from the list of users and groups on the right, select all of the users whose access to this universe you want to restrict, and click **<** to add them to the **Users / Groups** list.
9. One by one, assign the available restrictions that you created to the appropriate group and/or user.
10. Click **Save** on the main menu to save your changes.

Setting Integrated Data Access Restrictions

Data access restrictions are integrated with data access roles. These restrictions control access to objects within the Info Mart database so that BI users who are members of BI groups with associated access restrictions see data only for appropriate contact center resource groups (Agent Groups or Queue Groups that are configured in the Configuration Layer). There are two types of these restrictions:

- **Static Access Restrictions**: Enable you to configure a list of objects for which no data appears when reports are viewed by users who are members of restricted groups. For example, you can use this feature to prevent group members from viewing data for 'system' objects (such as Queue/Queue Groups).
- **Dynamic Access Restrictions**: Enable you to restrict access to data based on each BI user name and the attributes you configure to describe the user's geographical location, line of business, or organizational role. For example, you can use this feature to ensure that a supervisor sees data only from agents in specified locations, on specified teams.

Custom Data Access Restrictions

You can customize integrated data access restrictions by configuring the following Data Access Visibility (DAV) attributes, which are available on each object's Annex tab:

- ORG (Organizational Role)
- GEO (Geographic Location)
- LOB (Line of Business)

You restrict access to data by defining values on the Annex tab, as follows:

- For each Person: BI login, plus one or more DAV attributes
- For each contact center group: one or more DAV attributes

As long as a user has at least one DAV attribute that matches a group, then that user can see data from that group. For example:

- Agent Group1 has the following annex value: RPT_GEO=Daly City
- Agent Group2 has the following annex value: RPT_GEO=San Francisco
- Agent SuperVisor1 has the following annex value: RPT_GEO=Daly City
- Agent SuperVisor2 has the following annex value: RPT_GEO=San Francisco
- When Agent SuperVisor1 runs a report, the report contains data from Agent Group1, but not data from Agent Group2. The reverse is true for Agent_Supervisor2.

Data access restrictions use a small amount of system resources, so configuring them can result in a slight decrease in system performance.

Procedure: Configuring Access Restrictions

Purpose: Define DAV attributes using Configuration Manager, and define access restrictions using the Information Design Tool.

Steps

1. In Configuration Manager, open **View > Options**, and ensure that **Show Annex tab in object properties** is selected.
2. Using Configuration Manager, perform the following steps for each user (Person):
   a. If it is not already present, add the RPT section.
   b. Within the RPT section, add an option with:
      - `Option Name = BOE_USER`
      - `Option Value = <username>`
   c. If they are not already present, add one or more of the following sections:
      - **RPT_GEO**
      - **RPT_ORG**
      - **RPT_LOB**
   d. Within each of the sections you added in Step c, assign suitable options. For example, within the RPT_GEO section, you might add an option and assign it an Option Name that describes the geographical location of a group, such as `Daly City`.

   Neither Genesys Info Mart nor GI2 processes the Option Value for options in the [RPT_GEO], [RPT_ORG], or [RPT_LOB] sections, so you can leave the option value blank, and enter only the option name (unless the Configuration Server installed in your environment requires a value, as is the case in Configuration Server 7.6 and earlier).
3. Using Configuration Manager, perform the following steps for each contact center Group (Agent Groups and DN [ACD Queue] Groups):
   a. If they are not already present, add one or more of the following sections:
      - **RPT_GEO**
      - **RPT_ORG**
      - **RPT_LOB**
   b. Within each of the sections you added in Step a, assign suitable options. For example, within the **RPT_GEO** section, add an option and give it an **Option Name** that describes the geographical location of a group, such as `Daly City`.
4. Using the Information Design Tool assign Access Restrictions to the relevant BI groups. To apply more than one access restriction (for example, both the default Static Access Restriction and Dynamic Access Restriction), you must:
   a. Create two or more groups (or create one group, and for the other, use the default group **Interactive Insights access restrictions**).
   b. Assign one access restriction to each group (using the default access restrictions, custom restrictions that you create, or a combination of the two).
   c. Organize a Group Hierarchy, so that one group is a sub-group of the other. You can assign priorities to the access restrictions associated with each group, and the BI software applies

these access restrictions starting with the highest-level priority within the hierarchy.

For more information about working in Genesys Configuration Manager, see *Framework Configuration Manager Help*.

Data Access Restriction Configuration Example

This example creates restrictions so that when the user **boeuser1** views GI2 reports, the data in the reports comes only from **Agent Group 1** (and agents in that group) and **Queue Group 1** (and queues in that group).

1. Log in to Configuration Manager, and in the Annex of **cmperson1**, create the section **RPT** with option **BOE_USER=boeuser1** and section **RPT_GEO** with option **Daly City=<any value>** as follows:

   ```
   [RPT]
   BOE_USER=boeuser1
   [RPT_GEO]
   Daly City=<any value>
   ```

2. In the Annex of **Agent Group 1**, create the section **RPT_GEO**, and add the option **Daly City=<any value>**, as follows:

   ```
   [RPT_GEO]
   Daly City=<any value>
   ```

3. In the Annex of **Queue Group 1**, create the section **RPT_GEO**, and add the option **Daly City=<any value>**, as follows:

   ```
   [RPT_GEO]
   Daly City=<any value>
   ```

4. Run Genesys Info Mart and execute one ETL cycle. All data for objects with configured Annex are added in GIM tables: RESOURCE_ANNEX and GROUP_ANNEX.

> **Tip**
>
> GI2 relies on Interaction Concentrator and Genesys Info Mart to populate the RESOURCE_ANNEX and GROUP_ANNEX tables. Refer to the *Interaction Concentrator Deployment Guide* and *Genesys Info Mart Deployment Guide* for information about how to configure the population of Annex data (using the Interaction Concentrator **cfg-annex** option).

5. Log in to Central Management Console (CMC) as Administrator.
6. Create the user **boeuser1**, and add the newly created user to the **Interactive Insights access restriction** group.
7. Log in to the Information Design Tool as Administrator, and open the Security Editor.
8. In the Security Editor, apply **Dynamic Access Restriction** to the **Interactive Insights access**

restriction group.

The user **boeuser1** now sees report data only from Agent Group 1 and Queue Group 1.

Translating the Universe, GI2 Reports, and BI GUI

Genesys provides GI2 product installation packages in several languages, while BI langauge packs are available from SAP. The steps to install BI language packs are described in the *SAP BusinessObjects Business Intelligence platform 4.1 Installation Guide*.

To display the reports and use the universe and BI in a language other than English, complete the following steps:

Procedure: Translating the Universe, GI2 Reports, and BI GUI

Steps

1. Change the host's browser locale to match the language you plan to install.

CMC Preferences – Changing the Product Locale

2. Install the target BI language pack (see *SAP BusinessObjects Business Intelligence platform 4.1 Installation Guide*).
3. In CMC, click **Preferences > Administrator**. Change the BI product locale as shown in the Figure **CMC Preferences – Changing the Product Locale**.
4. Install the GI2 language pack.

> **Important**
>
> Check the appropriate GI2 Language Pack Release Note to ensure that the release of the language pack you plan to install is compatible with the installed release of GI2.

The updated universe—with connection to your data source defined—is now available to the user groups that you specified.

Customizing Measure Definitions

Genesys supports limited customization of the following GI2 measures:

- In the Activity class:
  - Avg Handle Time
  - Handle Time
- In the BA Customer class:
  - % First Response Time Service Level
  - % First Response Time Service Level 80
- In the Queue class:
  - % Accepted
  - % Accepted 80
  - Avg Handle Time
  - Handle Time
- In the Summarized State class:
  - % Occupancy

You can redefine these measures within the Universe Design Tool, as prescribed within each measure's properties within the universe. Refer to the *Genesys Interactive Insights User's Guide* for information about how to customize measures. After you have customized measure definitions, be sure to publish the universe back to the BI repository by following the steps in Publishing the Universe Back to the Repository.