Genesys Customer Experience Insights Deployment Guide

After Installing Genesys CX Insights

5/9/2025

Contents

After Installing Genesys CX Insights

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

Getting Started

Check to ensure that you can now view reports and dashboards. You can also optionally hide unwanted objects, and check the GCXI release and schema number.

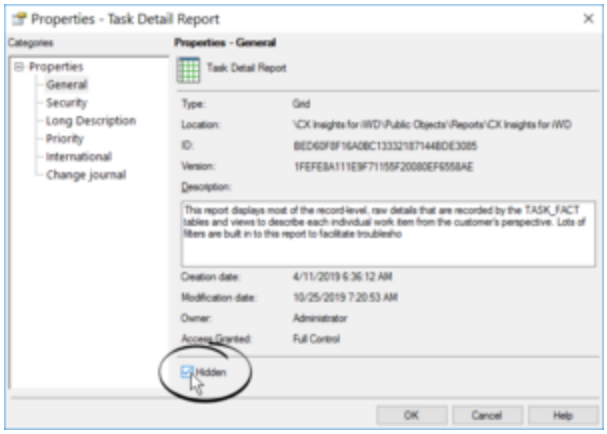
View the reports

Viewing Historical Reports

To view (or edit) the Genesys CX Insights historical reports, open MicroStrategy Web by pointing your web browser to `http://<servername>:<port>/MicroStrategy/servlet/mstrWeb*`, where `<servername>:<port>` are the server name and port provided by your administrator.

Verify that an assortment of report folders are present (Agents, Business Results, Callback, and so on) and that each one contains one or more reports. Note that, before you can view a report, you must run the report in order to populate data. For more information, see Accessing CX Insights GUIs and the *Genesys CX Insights User's Guide*.

*Redirecting the base URL — By default, users can enter simply `http://<server>:8080/MicroStrategy` (where `<server>` is the URL of your server) instead of `http://<server>:8080/MicroStrategy/servlet/mstrWeb`. Optionally, you can further simplify this by creating a URL redirect that allows users to access reports by entering `http://<server>`. For more information, see the *Other Properties* section of Procedure: Enter database information in the properties file.



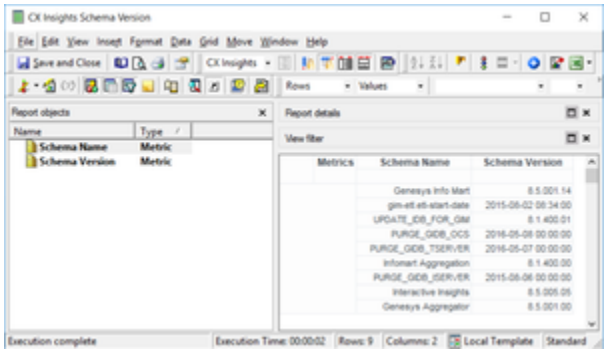
Hiding a Report

Hide unwanted reports

Some reports are needed only in certain scenarios, or there may be reports you don't want your users to see, for whatever reason. Optionally, you can hide unwanted reports (or other objects):

1. In MicroStrategy Developer, open your project, and navigate to the location where the report is stored.
2. Right-click the report name, and select **Properties**.
3. Click the **Hidden** check box.
4. Click **OK**.

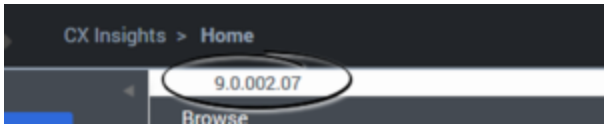
View the schema version



CX Insights Schema Version dialog

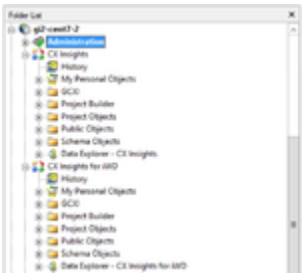
In MicroStrategy Developer, select **CX Insights** > **Public Objects** > **Reports**, and open the object **CX Insights Schema Version**. The *CX Insights Schema Version* dialog appears, where you can can view the current schema version for various Genesys components.

View the Genesys CX Insights Release number

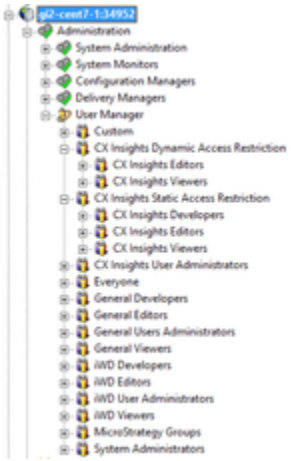


CX Insights Release Number

You can view the Genesys CX Insights release number when you open the project in MicroStrategy Web. It appears just below the breadcrumbs, when you first open the project, as shown in the figure **CX Insights Release Number**. You can also view the release number when you select the project in MicroStrategy Developer.



GCXI folders



CX Insights User Manager

View the project

If you have installed the optional report editing software (see Installing report editing software), you can view and edit the CX Insights project in MicroStrategy Developer, a desktop application available on the system where you installed MicroStrategy. For information about MicroStrategy Developer, see the Microstrategy ReadMe, and other MicroStrategy documentation (see Additional Resources for links to many useful MicroStrategy documents).

> **Important**
>
> Early releases of Genesys CX Insights comprised one project, called **Genesys CX Insights**. Beginning with release 9.0.010, a second project, **CX Insights for iWD** is included for iWD customers. The **Genesys CX Insights for iWD** project has structure and features similar to the **CX Insights** project. For additional information about **CX Insights for iWD**, see CX Insights for iWD reports.

Note that Genesys does not support customization of the underlying metadata, but does support customization of the reports. You can create your own reports, though Genesys recommends that you first familiarize yourself with the existing reports, as it is easier to modify one of them, than it is to start from scratch. For more information about the included reports, and how to customize or create reports, see the *Genesys CX Insights User's Guide*.

Genesys CX Insights is organized in a folder hierarchy, as shown in the figure **GCXI folders**. The subfolders you will most often be concerned with include:

- **GCXI > Administration > User Manager** — Note that the **User Manager** folder is reorganized in release 9.0.010.
- **GCXI > CX Insights > GCXI**
- **GCXI > CX Insights for iWD > iWD** (in release 9.0.010 and later)

The following table (**Most-used folders**) list the elements you will most often access in the MicroStrategy Developer file list:

Most-used folders

Administration	This folder contains administration and management tools you can use to manage such elements as user objects, database instances, and connections.
Administration > User Manager — This folder contains groups. Each group can contain users, or other groups.	Often-used groups in **release 9.0.010 and later:** • The following User Groups in the **User Manager >CX Insights Dynamic Access Restrictions** folder: CX Insights Editors, CX Insights Viewers • The following User Groups in the **User Manager >CX Insights Static Access Restrictions'** folder: CX Insights Developers, CX Insights Editors, CX Insights Viewers • The following User Groups in the **User Manager** folder: General Developers, General Editors, General Viewers, General Users Administrators, iWD Developers, iWD Editors, iWD Users Administrators, iWD Viewers Most other groups are seldom-used in Genesys CX Insights deployments. For more information about users and groups, see Users and Groups and Managing Users, Groups, and Privileges in

	the *Genesys CX Insights User's Guide*.
	CX Insights project (Includes GCXI reports, and the objects used to build them)
CX Insights — The root of the CX Insights project.	This folder contains all GCXI report objects, as well as administration and management tools you can use to manage such elements as user objects, database instances, and connections.
CX Insights > GCXI	Various subfolders that contain the objects (metrics, attributes, and prompts) that make up each report.
CX Insights > Public Objects > Reports	More than fifty reports and dashboards in subfolders within the **CX Insights > Public Objects > Reports > CX Insights > Reports** folder. Subfolders include: **Agents**, **Business Results**, **Callback**, **Chat**, **Dashboards** , **Designer**, **Details**, **Outbound Contact**, **Queues**, **Callback**, and various other folders. Dashboards are found in many of the report folders, in addition to those in the **Dashboards** folder.
CX Insights for iWD (release 9.0.010 and later — includes iWD reports, and the objects used to build them)	
CX Insights for iWD — The root of the CX Insights for iWD project.	This folder contains all iWD report objects, as well as administration and management tools you can use to manage such elements as user objects, database instances, and connections.
CX Insights for iWD > iWD	Various subfolders that contain the objects (metrics, attributes, and prompts) that make up each report.
CX Insights for iWD > Public Objects > Reports	The iWD reports, within the subfolder **CX Insights for iWD > Public Objects > Reports > CX Insights for iWD**.

*For more information about data access restrictions, see Data Access Restrictions and subsequent sections on this page.

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 Genesys CX Insights reports. To prepare the Genesys Info Mart environment for Genesys CX Insights operation, you must perform additional setup steps, including:

- **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 the Genesys Administration Extension (GAX) Configuration Manager. These options are described in the How Do I Configure Genesys Info Mart for Aggregation? section of the *Reporting and Analytics Aggregates Deployment Guide*. For information about how to configure options using GAX Configuration Manager, see the *Genesys Administrator Extension Help*.

> **Tip**
>
> There are two GUIs called *Configuration Manager* discussed on this page. One is part of GAX (so is referred to on this page as GAX Configuration Manager), and is used to configure options, such as **run-aggregates**. The other is part of MicroStrategy Developer, and is used to configure database information in MicroStrategy.

Utility Views Specific to Genesys CX Insights

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

Setting Up Attached Data

Genesys CX Insights reports are based on the configuration of user data in your environment — user data that is highly customizable within any given environment. To use the Genesys CX Insights reports without modifying the CX Insights Project or metric definitions, you must configure user-data data structures within Genesys Info Mart in a specific manner. For more information, contact your Genesys representative.

Linking the CX Insights Project to Your Data Mart

The Genesys CX Insights reports call upon metrics that are predefined in the CX Insights Project, 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 so that the reports that reference these metrics can pull contact center

data from your Info Mart database.

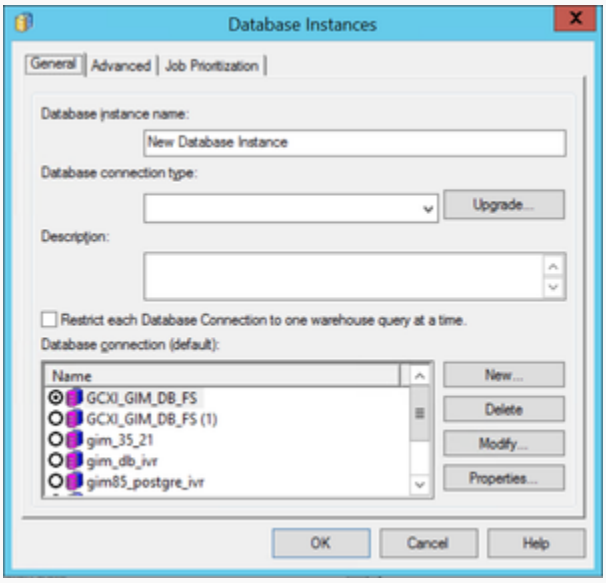
Use the following procedures to link the CX Insights Project to your Info Mart database.

Establishing communication between Genesys CX Insights / MicroStrategy and your database is an essential first step in configuring the software for reporting and analysis of your data. This section explains the steps required to set up this communication.

Procedure: Creating a new database instance using the default database connection

Purpose: Use this procedure to create a database instance, which is a MicroStrategy object that represents a connection to a data source. A database instance specifies connection information, including the name of the data source, login credentials, and other information about the data source.

Steps



Create a new database instance

1. Open MicroStrategy Developer.
2. In the **Folder List** list, expand **Administration** > **Configuration Managers**, and select **Database Instances**.
3. On the **File** menu, select **New** > **Database Instance**. The **Database Instances** editor appears.
4. In the **Database Instances** list, select the **GCXI_GIM_DB connection**. Instead of using the

default connection, you can optionally create a new connection by following the steps in Creating a new database connection.

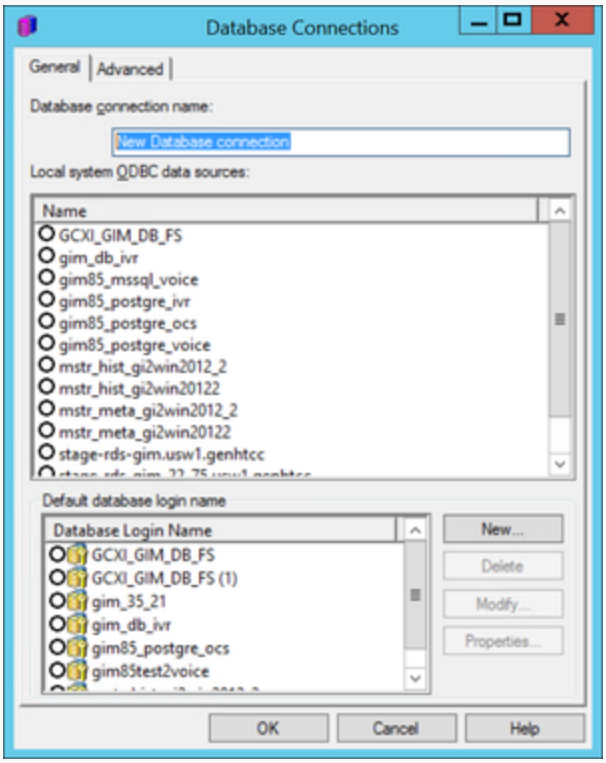
5. On the **General** tab, in the **Database instance name** field, type a name for the database instance, and in the Database connection (default) list, select the default data source connection.
6. From the **Database connection type** list, select a data source connection type suitable for the data source hosting your database.
7. On the **Advanced** tab, optionally configure additional options for the database instance.
8. On the **Job Prioritization tab**, optionally configure how jobs are prioritized for the database instance. For more information about prioritization, see the MicroStrategy System Administration Help.
9. Click **OK** to save your changes and close the dialog.

> **Tip**
>
> To learn more about the specific options you can configure in the **Database Instances** editor, click **Help**.

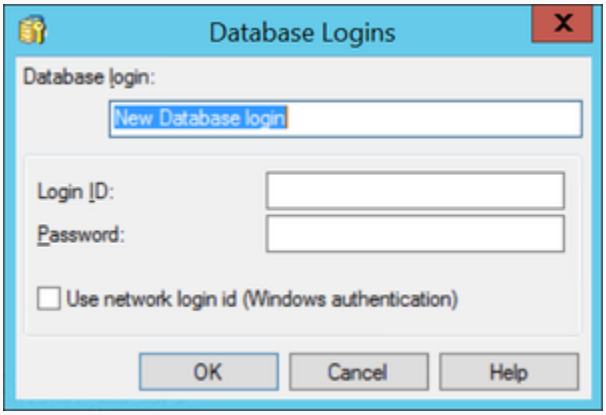
Procedure: Creating a new database connection

Purpose: Use this procedure to define a new connection, which you can use to link the CX Insights Project objects to the tables in your Data Mart. The database connection specifies the Date Source Name (DSN) and database login information used to access the data source. Alternatively, you can reuse the default connection by following the steps in Creating a new database instance using the default database connection.

Steps



Database Connections



Database Logins

1. Open MicroStrategy Developer.
2. In the **Folder List** list, expand **Administration** > **Configuration Managers**, and select **Database Instances**.

3. On the **File** menu, select **New** > **Database Instance**. The **Database Instances** editor appears.
4. Next to the **Database connection (default)** list, click **New**. The **Database Connections** editor appears.
5. On the **General** tab, in the **Database connection name** field, type a name to identify the database connection.
6. From the **Local system ODBC data sources** list, select the data source name.
7. On the **Advanced** tab, optionally configure additional options as required for the database to which you are connecting.
8. On the **General** tab, in the **Default database login name** list, select the default database login and click **OK**.

If the database login you require does not exist, you can create one as follows:

1. Next to **Default database login name**, click **New**.
2. In the **Database login** field, type a name for the database login.
3. Choose one of the following:
   - In the **Login ID** field, type the user name for the database login, and in the **Password** field, type the password associated with the user name.
   - Select **Use network login ID** to connect to the data source using the network user credentials that are used to run Intelligence Server.
4. Click **OK**.

> **Tip**
> To learn more about the specific options that you can configure (in the **Database Connections** editor, for example), click **Help**.

Users and Groups

The Genesys CX Insights installation routine silently deploys a variety of Genesys CX Insights objects, including Genesys CX Insights groups and users.

> **Important**
>
> Beginning with release 9.0.013, the default user accounts (Developer, Editor, Viewer), are disabled by default. A new container management variable, `GCXI_USERS_ENABLED=false|true`, is added, which you can use to enable the default accounts.

Some groups are distinguished by type, as shown in the table **Group types**.

Table: Group types

Group type	Capabilities
General (For example, **General Developers**, **General Users Administrators**)	Members of these groups have access to all installed projects (GCXI, iWD, and any others).
CX Insights (For example, **CX Insight Developers**, **CX Insights User Administrators**)	Members of these groups have access only to the CX Insights project (other projects, for example iWD, is not visible to them). Members of **CX Insights User Administrators** are able to manage only CX Insights groups (and users in these groups).
iWD (For example, **iWD Developers**, **iWD User Administrators**)	Members of these groups have access only to the CX Insights for iWD project (other projects, for example iWD, is not visible to them). Members of **iWD Administrators** are able to manage only CX Insights for iWD groups (and users in these groups).

You can import these objects with their permissions applied to project elements, or create the objects yourself from scratch and assign permissions to various objects by following the instructions in the following procedures. Each object in the Genesys CX Insights project has an Access Control List (ACL), which dictates which users can view or modify the object. The Table, **Mapping of Access Levels to selected objects**, lists the user security properties of objects that the Genesys CX Insights installation routine sets.

Table: Mapping of Access Levels to selected objects

Object type	User Group	Object Permission	Permission passed to children
Folder objects within the project	Administrator	Full Control	Default
	Everyone	Custom	View
	Public / Guest	Custom	View
Default report objects	CX Insights report developers	Custom	
	CX Insights report editors	Custom	
	CX Insights report viewers	Custom	
	System Administrators	Modify	
Default objects in the	CX Insights report	Custom	

Public Objects folder, including metrics, and prompts	developers		
	Everyone	View	
	Public / Guest	View	
	System Administrators	Modify	
Default objects in the Schema Objects folder, including attributes	Administrator	Full Control	
	CX Insights access restrictions	Custom	
	CX Insights report developers	Custom	
	Everyone	View	
	MicroStrategy Architect	View	
	Public / Guest	View	
	System Administrators	Modify	

Controlling access to Genesys CX Insights

Genesys CX Insights, through MicroStrategy, provides several tools to help you control access the historical reports. The easiest way to assign privileges to users is by assigning the user to a group that has the desired privilege; the user inherits permissions from the group object. You can also control access at the object level using an Access Control List (ACL).

> ### Important
> In scenarios where agents or queues are members of more than one group, and access restrictions are configured for all groups of which the agent or queue is the member, data can be double-counted in reports.

By default, a newly created object has an ACL consisting of:

- The user who created the object: Full Control
- Permissions for other users: as inherited from the parent folder

Procedure: Setting Access at the object level

Purpose: Use this procedure to manually set permissions on the objects used by Genesys CX Insights, including the Project, the **CX Insights** folder and connection, and even the

MicroStrategy applications. You must be an administrative user to make these changes.

Steps

1. In MicroStrategy Developer, log in to a project source (as a user with the 'Create And Edit Users And Groups' privilege).
2. Expand **Administration** > **User Manager**.
3. Right-click an object, and select **Properties**.
4. In the **Categories** list, click **Security**. Modify access as required, and click **OK**.

For detailed information about what access level settings you can apply, see the MicroStrategy documentation.

Procedure: Creating GCXI Users

Purpose: Use this procedure to create users and assign them to groups.

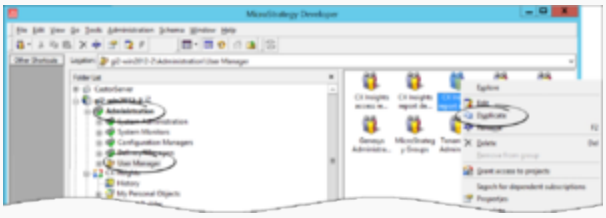
Steps

1. In MicroStrategy Developer, log in to a project source (as a user with the 'Create And Edit Users And Groups' privilege).
2. Expand **Administration** > **User Manager**, and then expand a group in which to add the new user. If you do not want the user to be a member of a group, select **Everyone**.
3. Select the menu item **File** > **New** > **User**. The **User Editor** opens.
4. Specify a user name and other information as appropriate, and click **OK**.

Procedure: Creating GCXI Groups

Purpose: In many cases, you can simply assign your users to the default groups. Alternatively, use this procedure to make a copy of an existing group, and modify the copy.

Steps



Duplicating a user group

1. In Microstrategy Developer, log in to a project source (as a user with the 'Create And Edit Users And Groups' privilege).
2. Expand **Administration** > **User Manager**, and then right-click an existing group, and choose **duplicate**. The **Group Editor** appears.
3. Right-click the new group, and click **Edit**. Edit the name of the new group, and other information as appropriate.
4. Click **OK**.

About Data-Access Restrictions for Multi-Tenant Environments

In addition to the permissions that you can set to control access to various MicroStrategy repository elements, you can also restrict the data that users can access by limiting the objects, rows, query types, and connections that are available to users. Through the use of these restrictions, you can control what data users see in the CX Insights reports.

Use this feature if your data source stores data for more than one tenant. For instance, within one project, 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 credentials that a user enters when logging in to MicroStrategy identify 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 CX Insights Project.

The benefits of this one-project approach include:

- Consistency in metric definitions across the enterprise.
- Reduced maintenance costs—having to manage only one project (instead of one 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.

About 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 MicroStrategy users who are members of MicroStrategy 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). Beginning with release 9.0.010, 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.

Limitations

The following limitations apply to data access restrictions:

- Agent hierarchy — Normally, dynamic access restrictions are applied everywhere that objects from the **Agent/Queue/Other** and **Agent/Queue Groups** are used. However, in the Interaction Flow Report (in release 9.0.009.00 and later) restrictions are applied only on Target resources; Source data from the **Agent/Queue/Other** and **Agent/Queue Groups** hierarchies is displayed in the report without access restrictions.
- Co-browse hierarchy — In the Co-Browse Details report, the Agent Name prompt and attribute always show all agents, regardless of Dynamic Access Restriction filters.
- Details hierarchy — The following reports, in the **Details** folder, have no access restrictions on specific objects, as follows:
  - Interaction Handling Attempt Report — Access restrictions are applied only on Agents. Queue data is displayed without restrictions, including the lists of values in prompts, and queues in the report itself.
  - Transfer Details Report — In release 9.0.008.00 and later, restrictions are applied only on Source Agents; Target Agent and Queue data appears without access restrictions, including the lists of

values in prompts.

  - Agent Group Membership Details Report — is not under any restriction, and always shows data for all groups and agents.

- **Reports with Agent Group prompts** — In some scenarios where agents are members in more than one group, data that users expect to see does not appear in a report. This can happen when the user who runs the report is permitted to see the agent's data, but is not permitted to see data for a group of which the agent is a member. In this scenario, when the user runs the report, the restricted group appears on the prompts page, allowing the user to select the group; however data for that group does not appear in the report.
- **Drilling to groups**— In some scenarios, after a user runs a report and then drills from agent to agent group, the report shows duplicated data rows for agents who are members of more than one group. This also causes totals in the report to be incorrect.
- **Groups reports** — In scenarios where agents or queues are members of more than one group, and at least one of the groups has Data Access Visibility (DAV) attributes configured, Group reports can duplicate data for those agents/queues, attributing it to each of the groups in which the agent/queue is a member. This also causes totals in the report to be incorrect.

Configuring Data Access Restrictions

You can customize Dynamic 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,

- If the following values are configured:
  - 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
- Then, 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 GAX Configuration Manager (for Dynamic Access Restrictions only), and define access restrictions using MicroStrategy Developer.

- For information about working in GAX Configuration Manager, see Configuration Manager.
- For information about MicroStrategy Developer, and other MicroStrategy tools, see the resources listed on the Additional Resources page.

> ### Tip
> There are two GUIs called *Configuration Manager* discussed on this page. One is part of GAX (so is referred to on this page as GAX Configuration Manager), and is used to configure options, such as **run-aggregates**. The other is part of MicroStrategy Developer, and is used to configure database information in MicroStrategy.

Steps

1. To ensure that access restrictions are enabled, use either of the following methods to manage security filters:
   - In any Genesys CX Insights release, using MicroStrategy Developer:
     1. Open the User Manager.
     2. Right-click the **CX Insights Dynamic Access Restriction** user group, and select **Edit**. The **Group Editor** appears.
     3. Click **Security Filters**, then click **View**.
     4. Ensure that the Dynamic Access Restriction type is in the **Selected** list (the right-hand list). If it is not, add it from the **Available** list, and click **OK**, then **OK** again.
     5. Right-click the **CX Insights Static Access Restriction** user group, and select **Edit**. The **Group Editor** appears.
     6. Click **Security Filters**, then click **View**.
     7. Ensure that the Static Access Restriction type is in the **Selected** list (the right-hand list). If it is not, add it from the **Available** list, and click **OK**, then **OK** again.

        OR
   - In Genesys CX Insights release **9.0.010 or later**, using the web interface:

1. Open the following URL in your web browser:

   ```
   http://<Server>:<Port>/MicroStrategy/servlet/mstrServerAdmin
   ```

   where <Server>:<Port> is the IP address and port of your Genesys CX Insights deployment.
2. Click the **Server** icon, and open the **User Manager**.
3. Right-click the **CX Insights Dynamic Access Restriction** user group, and select **Edit**. The **Group Editor** appears.
4. Select the **Security Filters** tab.
5. Ensure that the Dynamic Access Restriction type is in the **Selected** list (the right-hand list). If it is not, add it from the **Available** list, and click **OK**, then **OK** again.
6. Right-click the **CX Insights Static Access Restriction** user group, and select **Edit**. The **Group Editor** appears.
7. Select the **Security Filters** tab.
8. Ensure that the Static Access Restriction type is in the **Selected** list (the right-hand list). If it is not, add it from the **Available** list, and click **OK**, then **OK** again.

2. For both Dynamic Access Restrictions and Static Access Restrictions — to assign users to the appropriate groups, complete the following actions using MicroStrategy Developer:
   1. Create users as required.
   2. Assign each user to the following groups:
      - For Dynamic Access Restrictions, choose from: **CX Insights Dynamic Access Restriction** and **CX Insights Developers**, or **CX Insights Editors**, or **CX Insights Viewers**.
      - For Static Access Restrictions, choose from: **CX Insights Static Access Restriction** and **CX Insights Developers**, or **CX Insights Editors**, or **CX Insights Viewers**.
3. For Dynamic Access Restrictions — define DAV attributes in GAX Configuration Manager, as follows:
   1. Open **View > Options**, and ensure that **Show Annex tab in object properties** is selected. Perform the following steps for each user (Person):
      1. If it is not already present, add the RPT section.
      2. Within the RPT section, add an option with:
         - **Option Name = BOE_USER**
         - **Option Value = <username>**
      3. If they are not already present, add one or more of the following sections:
         - **RPT_GEO**
         - **RPT_ORG**

- **RPT_LOB**

4. Within each of the sections you added, 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 Genesys CX Insights 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).

2. Perform the following steps for each contact center Group (Agent Groups and DN [ACD Queue] Groups):

   1. If they are not already present, add one or more of the following sections:

      - **RPT_GEO**
      - **RPT_ORG**
      - **RPT_LOB**

   2. Within each of the sections you added, 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`.

Link to video

Dynamic Access Restriction Configuration Example

The following example creates restrictions so that when the user **cxiuser1** views Genesys CX Insights 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. To ensure that access restrictions are enabled, use either of the following methods to manage security filters:

   - In any Genesys CX Insights release, using MicroStrategy Developer:

     1. Open the User Manager.
     2. Right-click the **CX Insights Dynamic Access Restriction** user group, and select **Edit**. The **Group Editor** appears.
     3. Click **Security Filters**, then click **View**.
     4. Ensure that the Dynamic Access Restriction type is in the **Selected** list (the right-hand list). If it is not, add it from the **Available** list, and click **OK**, then **OK** again.
     5. Right-click the **CX Insights Static Access Restriction** user group, and select **Edit**. The **Group Editor** appears.
     6. Click **Security Filters**, then click **View**.

7. Ensure that the Static Access Restriction type is in the **Selected** list (the right-hand list). If it is not, add it from the **Available** list, and click **OK**, then **OK** again.

OR

- In Genesys CX Insights release **9.0.010 or later**, using the web interface:
  1. Open the following URL in your web browser:

     ```
     http://<Server>:<Port>/MicroStrategy/servlet/mstrServerAdmin
     ```

     where <Server>:<Port> is the IP address and port of your Genesys CX Insights deployment.
  2. Click the **Server** icon, and open the **User Manager**.
  3. Right-click the **CX Insights Dynamic Access Restriction** user group, and select **Edit**. The **Group Editor** appears.
  4. Select the **Security Filters** tab.
  5. Ensure that the Dynamic Access Restriction type is in the **Selected** list (the right-hand list). If it is not, add it from the **Available** list, and click **OK**, then **OK** again.
  6. Right-click the **CX Insights Static Access Restriction** user group, and select **Edit**. The **Group Editor** appears.
  7. Select the **Security Filters** tab.
  8. Ensure that the Static Access Restriction type is in the **Selected** list (the right-hand list). If it is not, add it from the **Available** list, and click **OK**, then **OK** again.

2. Create the user **cxiuser1**, and add the newly created user to the following groups: **CX Insights Dynamic Access Restriction** and **CX Insights Developers**, or **CX Insights Editors**, or **CX Insights Viewers**.
3. Log in to GAX Configuration Manager, and in the Annex of **cmperson1**, create the section **RPT** with option **BOE_USER=cxiuser1** and section **RPT_GEO** with option **Daly City=<any value>** as follows:

   ```
   [RPT]
   BOE_USER=cxiuser1
   [RPT_GEO]
   Daly City=<any value>
   ```

4. 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>
   ```

5. 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>
   ```

6. 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**
>
> Genesys CX Insights 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).

The user **cxiuser1** now sees report data only from Agent Group 1 and Queue Group 1.

User and account management

Genesys recommends that you immediately change the default Microstrategy administrator password. For information about how to do so, and other procedures needed to create and manage users, see Managing the MicroStrategy environment.