GENESYS™

Reporting Administrator's Guide

1/2/2026

Table of Contents

Contents

Perform basic administrator tasks for your reporting tools and users.

Related documentation:

-

Manage reporting environments

Most operation, administration, and management actions are carried out by your Genesys representative.

Genesys CX Insights user administration

Many **Reporting GCXI** users can change their own passwords, and some administrator users can change passwords both for themselves, and for other users. For step-by-step instructions to change Genesys CX Insights (GCXI) passwords, manage users, and set languages, see Genesys CX Insights User Management.

Agent Workspace, Pulse, and GVP administration.

There are no user-managed administration features for these reporting tools.

If you are looking for information about an administrative task that's not described in this document, talk to your Genesys representative.

To learn more about the different types of reporting Genesys offers, see Reporting or visit the following pages:

- Navigating Agent Workspace
- Get started with Genesys CX Insights
- Get started with GVP reporting
- Get Started with Genesys Pulse

Genesys CX Insights User Management

Contents

-
- Administrator

Manage Reporting GCXI (historical reporting) user accounts.

Related documentation:

-

Genesys CX Insights credentials are managed separately from credentials for other Genesys Multicloud CX components. This page describes the steps you can take to create an account for a new user, change your password, or change another user's password.

Managing your own account

This section provides information about managing your own account.

Video: Changing your own password

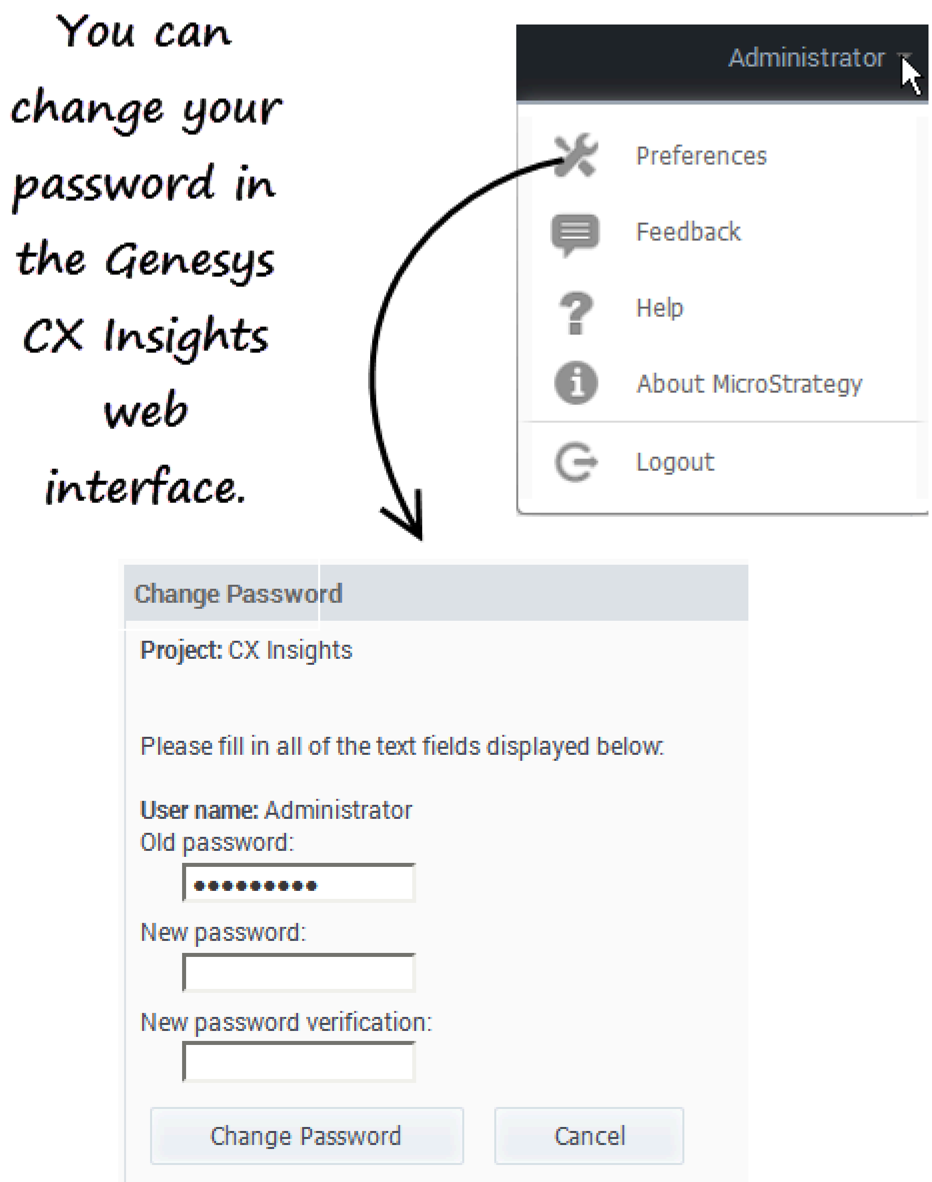
Link to video

This video describes how to change your own password, if your permissions allow it.

Changing your own password

Use the following steps to change your password. Not all users are permitted to change their password; contact your administrator to find out if the functionality described on this page is available for your use.

> **Important**
> If you have forgotten your password, or otherwise cannot log in, contact your administrator / next level of support.



1. On the Genesys Multicloud CX Portal, click **All Apps** > **Reporting GCXI**.
2. At the Genesys CX Insights login screen, enter your user name and current password.
3. On the Genesys CX Insights menu, click your user name, and click **Preferences**.
4. Click **Change Password**.
5. In the **Old Password** field, type your current password.
6. In the **New Password** field, type your new password, and retype it in the **New Password Verification** field.

    Passwords must be at least 8 characters, have at least one uppercase character, one lowercase character, and one number.

7. Click **Change Password**.

Predefined user groups and privileges

The group structure in release 9.0.011 and later is unlike earlier releases of the software.

If you require permissions different from those assigned to the predefined groups, Genesys recommends that you avoid modifying privileges for the predefined user groups, because these user groups are overwritten during upgrades. Instead, create custom groups by duplicating the user group you wish to modify, and edit the duplicate group.

The **User Groups** table lists and describes the predefined GCXI user groups.

User groups

Groups	Summary	Project Access Level*
Custom	Customer-defined user groups.	User-defined
CX Insights Developers	Members of this groups can create, edit, or view objects in the Genesys CX Insights project.	Genesys CX Insights
CX Insights Dynamic Access Restrictions	Security Filter you can use to restrict access to data based on user name, geographical location, line of business, or organizational role.	Genesys CX Insights
CX Insights Editors	Members of this groups can edit or view objects in the Genesys CX Insights project.	Genesys CX Insights
CX Insights Static Access Restrictions	Security Filter you can use you prevent members of specified user groups from viewing data for a list of objects you specify.	Genesys CX Insights
CX Insights User Administrators	Members of this group can manage users in the Genesys CX Insights project.	Genesys CX Insights
CX Insights Viewers	Members of this groups can view objects in the Genesys CX Insights project.	Genesys CX Insights
Everyone	The *Everyone* group provides a way for you to easily apply privileges, security role memberships, or permissions to all users. All users are automatically members of this group.	none
General Developers	Members of this group can create, edit, and view objects in any project.	all
General Editors	Members of this group can edit	all

	and view objects in any project.	
General User Administrators	Members of this group can manage users in any project.	all
General Viewers	Members of this group can view objects in any project.	all
iWD Developers	Members of this group can create, edit, and view objects in the CX Insights for iWD project.	iWD
iWD Editors	Members of this group can edit and view objects in the CX Insights for iWD project.	iWD
iWD User Administrators	Members of this group can manage users in the CX Insights for iWD project.	iWD
iWD Viewers	Members of this group can view objects in the CX Insights for iWD project.	iWD
MicroStrategy Groups	Built-in groups that are included in all MicroStrategy deployments.	none
System Administration	Members of this group have unrestricted management capabilities.	all

Note that some groups provide access only to a specific project:

- CX Insights — membership in groups with this prefix allows users to work within the Genesys CX Insights project only.
- General — membership in groups with this prefix allows users to work in any project.
- iWD — membership in groups with this prefix allows users to work within the iWD project only.

Genesys Authentication

When enabled, Genesys Authentication allows logged-in users to navigate across multiple applications without re-entering their credentials. For more information, see Genesys Authentication Private Edition Guide.

The **Configuration Server Access Groups** table shows how Genesys CX Insights user groups map to Configuration Server Access Groups:

To learn more about Configuration Server Access Groups, talk to your Genesys representative.

Configuration Server Access Groups

Parent folder	Config Server Access Group	Mapping to MicroStrategy Users Groups
environment/Access Groups/$customer/	$customer Administrators	CX Insights Developers, CX Insights Users Administrators
environment/Access Groups/$customer/	$customer Managers	CX Insights Editors

environment/Access Groups/$customer/	$customer Supervisors	CX Insights Viewers
environment/Access Groups/$customer/GCXI	CX Insights Users Administrators	CX Insights Users Administrator
environment/Access Groups/$customer/GCXI	CX Insights Developers	CX Insights Developers
environment/Access Groups/$customer/GCXI	CX Insights Editors	CX Insights Editors
environment/Access Groups/$customer/GCXI	CX Insights Viewers	CX Insights Viewers
environment/Access Groups/$customer/GCXI	GCXI for iWD Users Administrators	iWD Users Administrator
environment/Access Groups/$customer/GCXI	GCXI for iWD Developers	iWD Developers
environment/Access Groups/$customer/GCXI	GCXI for iWD Editors	iWD Editors
environment/Access Groups/$customer/GCXI	GCXI for iWD Viewers	iWD Viewers

Permissions needed to manage other users

To manage the accounts of other users, you must be a member of one of the *Administrator* user groups described in the following tables, which describe the types of accounts each of the Administrator types can manage, and the actions they can carry out on each.

User management capabilities

Managing Group	Administrator	General Users Administrators	CX Insights Users Administrators	iWD Users Administrators
Managed Group				
Custom	Full Control	Full Control	Full Control	Full Control
MicroStrategy Groups	Full Control	No Access	No Access	No Access
System Administrators	Full Control	No Access	No Access	No Access
Everyone	Full Control	View / Modify / Modify children	View / Modify / Modify children	View / Modify / Modify children
General Developers	Full Control	View / Modify / Modify children	No Access	No Access
General Editors	Full Control	View / Modify / Modify children	No Access	No Access
General Viewers	Full Control	View / Modify / Modify children	No Access	No Access
General Users	Full Control	View / Modify /	No Access	No Access

Managing Group	Administrator	General Users Administrators	CX Insights Users Administrators	iWD Users Administrators
Administrators		Modify children		
CX Insights Static Access Restriction	Full Control	View / Modify / Modify children	View / Modify children	No Access
CX Insights Dynamic Access Restriction	Full Control	View / Modify / Modify children	View / Modify children	No Access
CX Insights Developers	Full Control	View / Modify / Modify children	View / Modify / Modify children	No Access
CX Insights Editors	Full Control	View / Modify / Modify children	View / Modify / Modify children	No Access
CX Insights Viewers	Full Control	View / Modify / Modify children	View / Modify / Modify children	No Access
CX Insights Users Administrators	Full Control	View / Modify / Modify children	View / Modify / Modify children	No Access
iWD Developers	Full Control	View / Modify / Modify children	No Access	View / Modify / Modify children
iWD Editors	Full Control	View / Modify / Modify children	No Access	View / Modify / Modify children
iWD Viewers	Full Control	View / Modify / Modify children	No Access	View / Modify / Modify children
iWD Users Administrators	Full Control	View / Modify / Modify children	No Access	View / Modify / Modify children

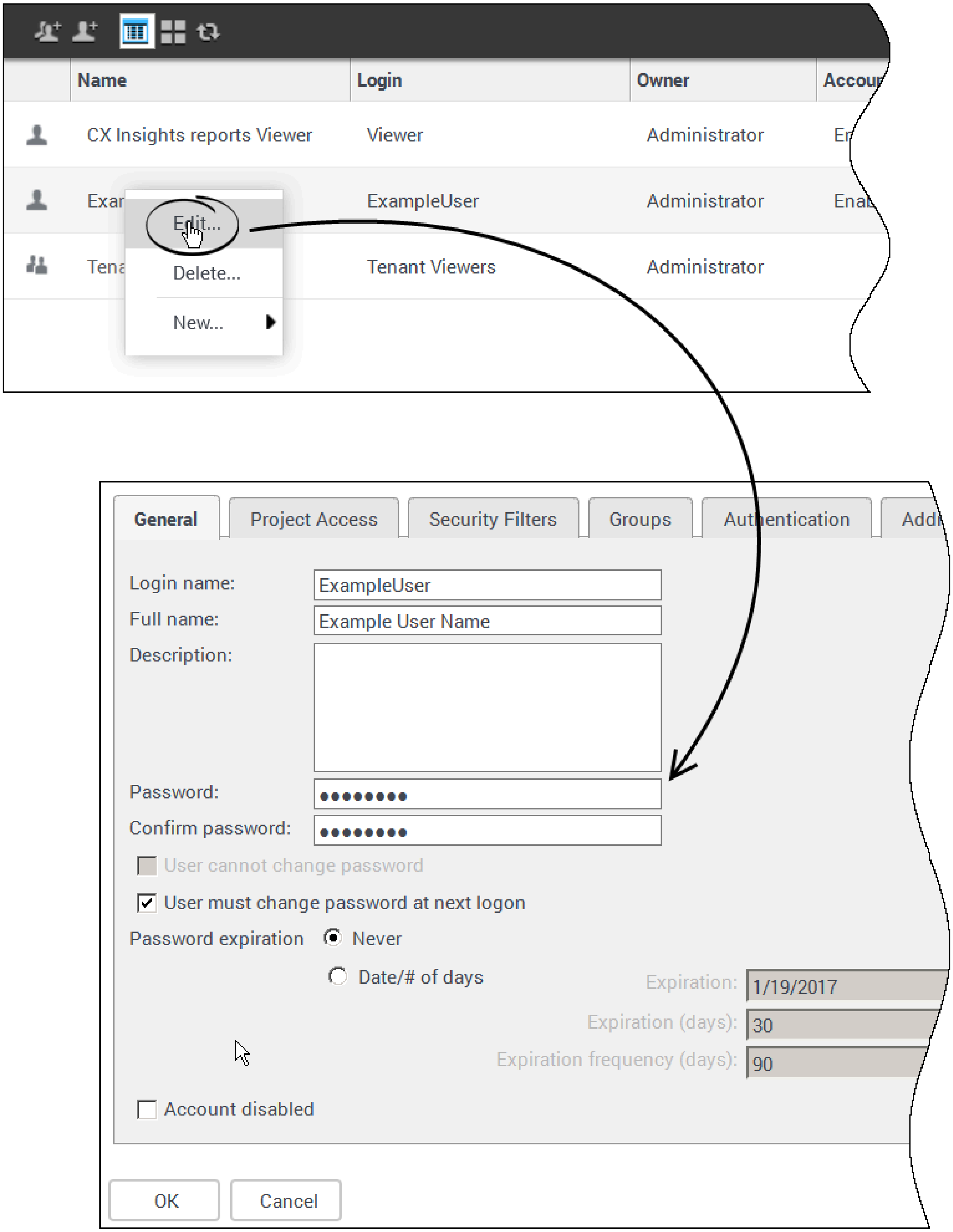
Video: Managing users

Link to video

This video describes how to manage users, including how to:

- create users
- delete users
- change users' passwords
- change users' permissions

Changing another user's password


Name
Login
Owner
Accou
CX Insights reports Viewer
Viewer
Administrator
En
Exar
ExampleUser
Administrator
Enab
Tena
Tenant Viewers
Administrator
Edit...
Delete...
New...
General
Project Access
Security Filters
Groups
Authentication
Addi
Login name:
ExampleUser
Full name:
Example User Name
Description:
Password:
Confirm password:
User cannot change password
User must change password at next logon
Password expiration
Never
Date/# of days
Expiration:
1/19/2017
Expiration (days):
30
Expiration frequency (days):
90
Account disabled
OK
Cancel

Use the following steps to change a password for another user (for example when they have forgotten their password) or to otherwise manage an existing user account.

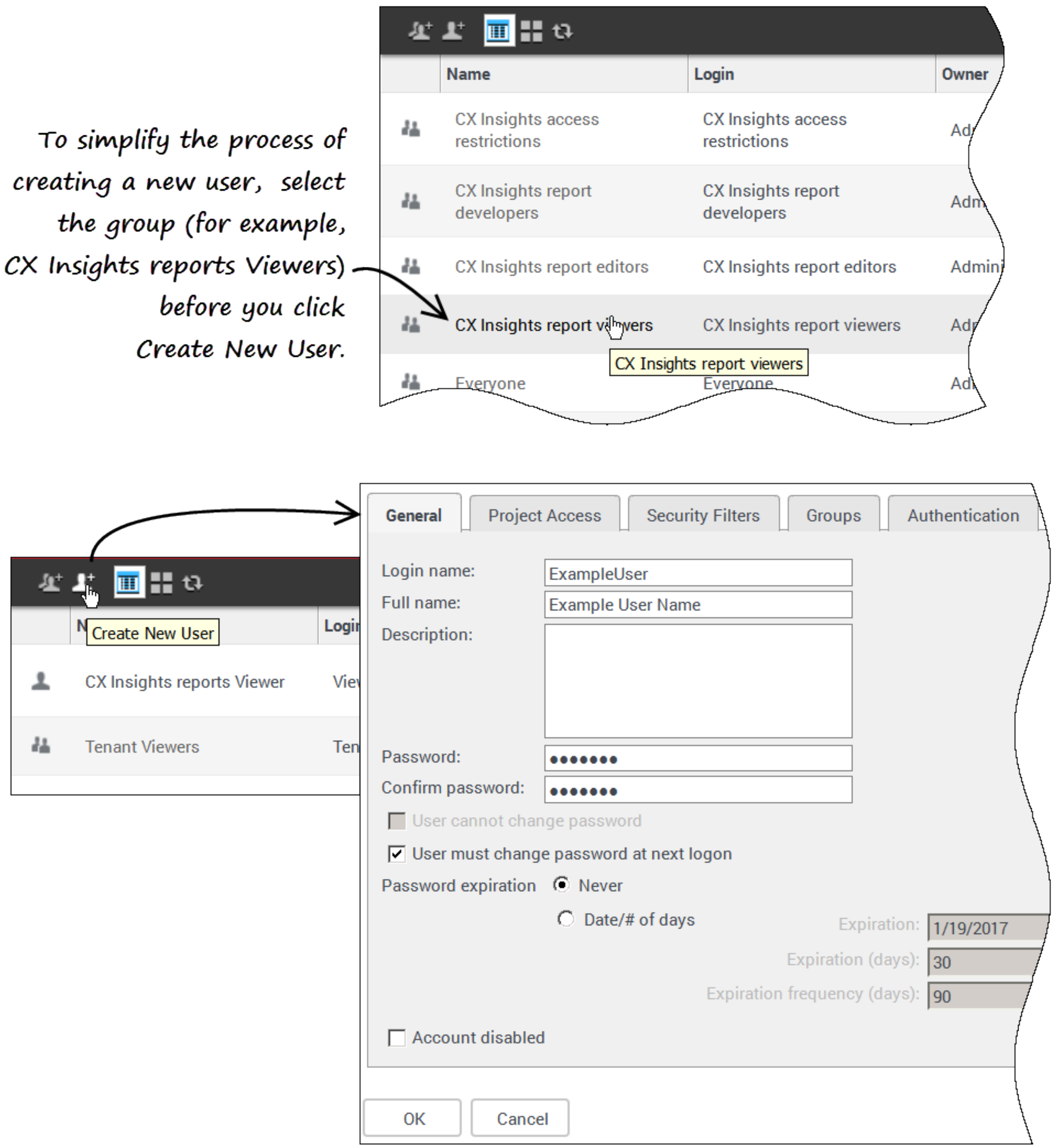
To edit another user's account, you must log in as a member of a group that has the **Create And Edit Users And Groups** privilege.

1. In your web browser, open the MicroStrategy Web Administrator page:

   `http://:/MicroStrategy/servlet/mstrServerAdmin`

2. On the page that appears, select your server.
3. On the MicroStrategy Web Administrator login screen, enter your user name and current password, and click **Login**. The **Tools** page opens.
4. Click **User Manager**.
5. Click a group of which the user is a member. A list appears, showing all the users in that group.
6. Right-click the user's name, and in the menu, click **Edit**.
7. In the **Password** field, enter the new password, and enter it again in the **Confirm Password** field.
8. Select **User must change password at next login**, and make any other changes if required.
9. Click **OK**.

Creating a new user



Use the following steps to create a new user account.

To edit another user's account, you must log in as a member of a group that has the **Create And**

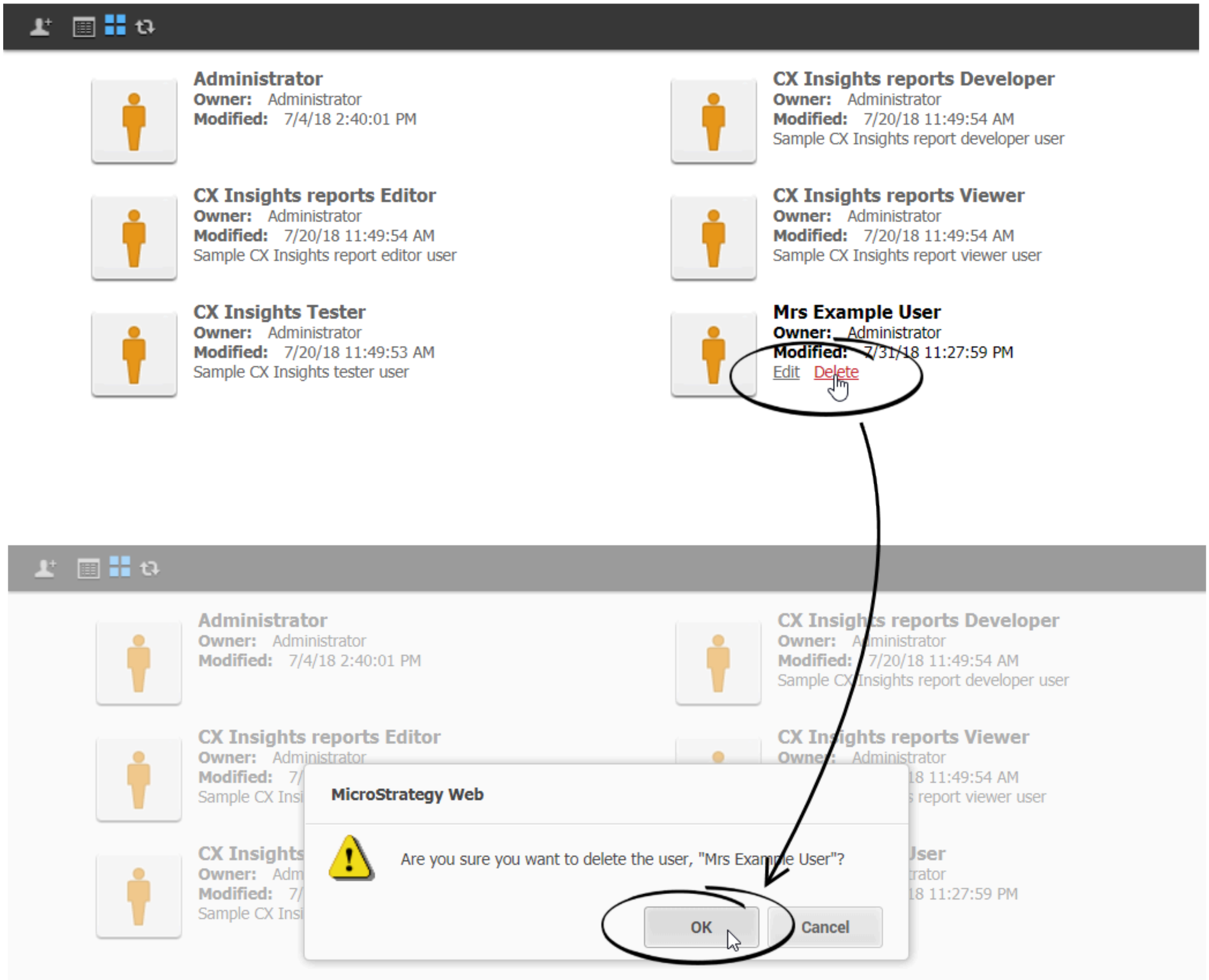
Edit Users And Groups privilege.

1. In your web browser, open the MicroStrategy Web Administrator page:

   `http://:/MicroStrategy/servlet/mstrServerAdmin`

2. On the page that appears, select your server.
3. On the MicroStrategy Web Administrator login screen, enter your user name and current password, and click **Login**. The **Tools** page opens.
4. Click **User Manager**.
5. On the menu, click **Create New User**.
6. Specify user information as appropriate, on each tab in the editor. If you need more information about any field, see the MicroStrategy Web Administrator Help. Be sure to:
   - Include a **Login Name**, **Full Name**, **Password**, **Confirm Password** and other selections in accordance with your password policies (on the **General** tab).
   - Assign at least one **Group** (on the **Groups** tab). By default, all users are also members of the group **Everyone**.
7. Click **OK**.
8. To verify that the user was created, open one of the groups to which you added the user (or open the group **Everyone**).

Deleting a user



Use the following steps to delete a user account.

To edit another user's account, you must log in as a member of a group that has the **Create And Edit Users And Groups** privilege.

1. In your web browser, open the MicroStrategy Web Administrator page:

   `http://:/MicroStrategy/servlet/mstrServerAdmin`

2. On the page that appears, select your server.
3. On the MicroStrategy Web Administrator login screen, enter your user name and current password, and click **Login**. The **Tools** page opens.
4. Click **User Manager**.

5. Open a group of which the user is a member, for example **Everyone**.
6. Hover over the user you plan to delete, and click **Delete**.
7. Click **OK**.

Subtractive access rights

In Genesys CX Insights / MicroStrategy, access rights are controlled using a *subtractive* model. User access rights are restricted based on group membership. If a user is a member of more than one group, then the access restrictions of the most restrictive group are enforced. For example, a user who is a member of the groups Tenant Developers and Tenant Editors has the privileges of Tenant Editors only. For this reason, Genesys recommends that you make each user a member of exactly oneAdmin Group and / or oneReporting Group.

If you are accustomed to historical reporting in Genesys Interactive Insights (GI2) / Business Objects, note that Genesys CX Insights uses an entirely different approach to limiting access, and while the term *access restrictions* in Genesys CX Insights refers to access rights granted to user groups, the same term in GI2 refers to restrictions placed on objects, rows, query types, and connections in the GI2 universe.

Report scheduling

Contents

- Administrator

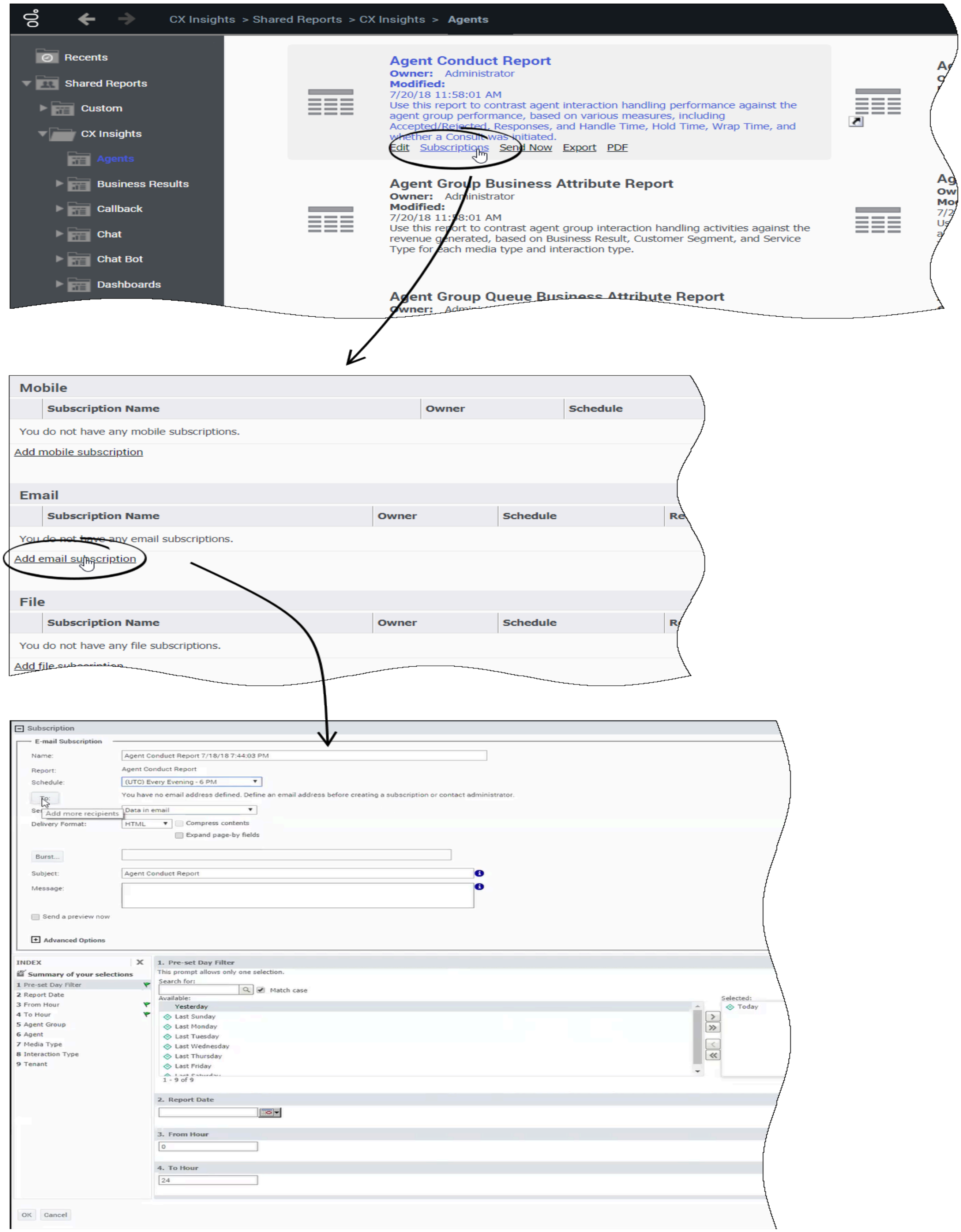
Schedule the periodic delivery of reports.

Related documentation:

-

You may find that it is helpful to run the same report regularly—every day, or every week, for example. Using Genesys CX Insights *Subscriptions*, this page describes how to schedule the delivery of a report by email in the format you prefer, to the destination of your choice, such as your email, printer, or mobile device.

Scheduling the delivery of a report by email


CX Insights > Shared Reports > CX Insights > Agents
Recents
Shared Reports
Custom
CX Insights
Agents
Business Results
Callback
Chat
Chat Bot
Dashboards
Agent Conduct Report
Owner: Administrator
Modified:
7/20/18 11:58:01 AM
Use this report to contrast agent interaction handling performance against the agent group performance, based on various measures, including Accepted/Rejected, Responses, and Handle Time, Hold Time, Wrap Time, and whether a Consult was initiated.
Edit Subscriptions Send Now Export PDF
Agent Group Business Attribute Report
Owner: Administrator
Modified:
7/20/18 11:58:01 AM
Use this report to contrast agent group interaction handling activities against the revenue generated, based on Business Result, Customer Segment, and Service Type for each media type and interaction type.
Agent Group Queue Business Attribute Report
Mobile
Subscription Name
Owner
Schedule
You do not have any mobile subscriptions.
Add mobile subscription
Email
You do not have any email subscriptions.
Add email subscription
File
You do not have any file subscriptions.
Subscription
E-mail Subscription
Name: Agent Conduct Report 7/18/18 7:44:03 PM
Report: Agent Conduct Report
Schedule: (UTC) Every Evening - 6 PM
You have no email address defined. Define an email address before creating a subscription or contact administrator.
Add more recipients
Data in email
Delivery Format: HTML
Compress contents
Expand page-by fields
Burst...
Subject: Agent Conduct Report
Message:
Send a preview now
Advanced Options
INDEX
Summary of your selections
1 Pre-set Day Filter
2 Report Date
3 From Hour
4 To Hour
5 Agent Group
6 Agent
7 Media Type
8 Interaction Type
9 Tenant
1. Pre-set Day Filter
This prompt allows only one selection.
Search for:
Match case
Available:
Yesterday
Last Sunday
Last Monday
Last Tuesday
Last Wednesday
Last Thursday
Last Friday
1 - 9 of 9
Selected:
Today
2. Report Date
3. From Hour
0
4. To Hour
24
OK
Cancel

Genesys CX Insights enables you to subscribe to a report so that it runs on a schedule you specify. You can configure Genesys CX Insights to save the report in your history list, so you can view it at your convenience, or you can configure Genesys CX Insights to automatically email the report to you.

1. Open the **Shared Reports** folder, and navigate to the report you want to schedule.
2. Hover over the report name/description, and several options appear below the description. Click **Subscriptions**.
3. On the **My Subscriptions** page, scroll down and select the type of subscription you want to create. Genesys CX Insights supports either of the following selections:
    - **Add History List subscription** to save the report in your history, so you can access it later.
    - **Add email subscription** to automatically send the report to a configured email address. The email subscription details appear.

For example, to configure an email subscription:

1. Click **Add email subscription**.
2. Select a value from the **Schedule** list to control how often the report is generated, and from the **To** list to indicate the email address to which the report is sent.
3. Select values for the various prompts as required.
4. Optionally, select **Send a preview now** to test the subscription (if you do so, an email will arrive in as little as a few minutes).
5. Optionally, add additional users in the **To** list, to send the same report to more than one user.
6. Click **OK**.

Tips:

- Subscriptions can be sent only to enabled users. If a subscription is created for a user who is, or later becomes, disabled, MicroStrategy does not send the report to that user, though it continues to send it to other subscribers.
- If you have created subscriptions for a user, and wish to transfer those subscriptions to another user (without having to recreate them from scratch), contact Genesys Customer Care for assistance.
- In some scenarios, email messages that notify users of scheduled reports can contain unexpected characters in the email subject line. If you encounter this issue, see the Known Issue GCXI-2327.

Genesys CX Insights Support for GDPR

Contents

- Administrator

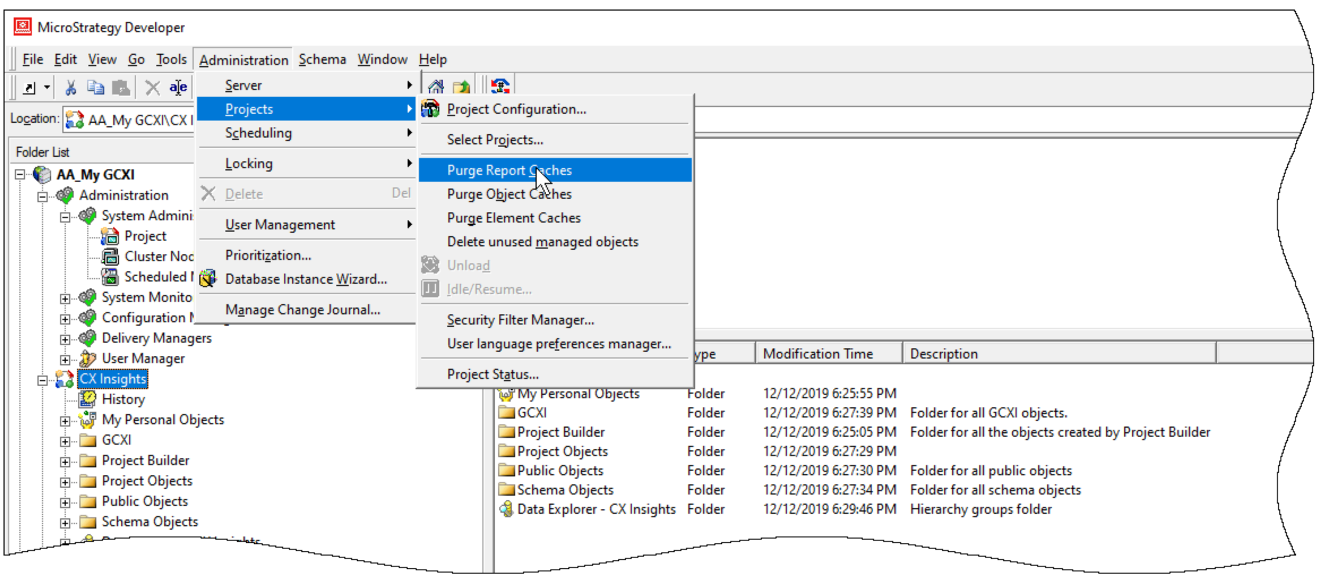
Ensure that you handle Personal Identifiable Information (PII) in accordance with General Data Protection Regulation (GDPR) standards.

Related documentation:

-

Genesys Customer Experience Insights (Genesys CX Insights or simply GCXI) can store Personal Identifiable Information (PII) in logs, history files, and in reports (in scenarios where customers include PII data in reports). Genesys recommends that you do not capture PII in reports, however, if you do so, it is your responsibility to remove any such report data within 21 days or less, if required by General Data Protection Regulation (GDPR) standards. Note that work email addresses are often used in reports, but are not considered PII.

Deleting PII from reports



If your reports contain PII, perform the following steps to remove old report results:

1. Delete any saved reports that contain PII.
2. Purge the GCXI report cache:
    1. Open MicroStrategy Developer, log in, and select your project.
    2. Select the **CX Insights** project.
    3. Click **Administration** > **Projects** > **Purge Report Caches**.

Clearing PII from logs and history

To remove PII from logs and history files, complete the following steps:

1. Clean up logs — Periodically delete the following logs, which can include login names:
   Microstrategy logs:
   - `/mnt/log/mstr/DistributionService_DeliveryDetails.log`
   - `/mnt/log/mstr/AuthenticationServer_Trace.log`
   - `/mnt/log/mstr/Kernel_UserTrace.log`
   - `/mnt/log/mstrWeb/MSTRLog.log`
   - `/mnt/log/tomcat/localhost_access_log..txt`

   GCXI utils logs:
   - `/mnt/log/gcxi/com.genesys.jdbc.driver.log`
2. Configure the maximum size and age of the history list, at the project level. For detailed steps to manage the history list, see the MicroStrategy website for information about:
   - Controlling the maximum size of the History List
   - Controlling the lifetime of History List messages (in days)
   - Scheduling History List message deletion

Other steps

Genesys does not support or recommend using cubes. If you do use them, be aware that, depending on the data uploaded, cubes can contain PII data which you might need to delete in order to comply with GDPR requirements.