



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

Reporting Administrator's Guide

Genesys CX Insights User Management

8/12/2022

Contents

- 1 Managing your own account
 - 1.1 Video: Changing your own password
 - 1.2 Changing your own password
- 2 Predefined user groups and privileges
 - 2.1 Genesys Authentication
- 3 Permissions needed to manage other users
- 4 Video: Managing users
- 5 Changing another user's password
- 6 Creating a new user
- 7 Deleting a user
 - 7.1 Subtractive access rights



- 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.

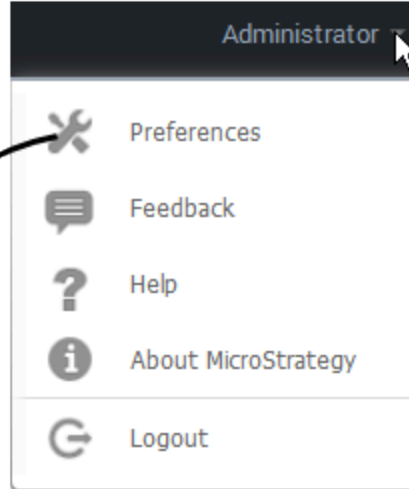
Changing your own password

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.

You can change your password in the Genesys CX Insights web interface.



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 <i>Everyone</i> 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	Account
	CX Insights reports Viewer	Viewer	Administrator	Ena
	ExampleUser	ExampleUser	Administrator	Enab
	Tenant Viewers	Tenant Viewers	Administrator	

General | Project Access | Security Filters | Groups | Authentication | Add...

Login name:

Full name:

Description:

Password:

Confirm password:

User cannot change password

User must change password at next logon

Password expiration Never
 Date/# of days

Expiration:

Expiration (days):

Expiration frequency (days):

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.

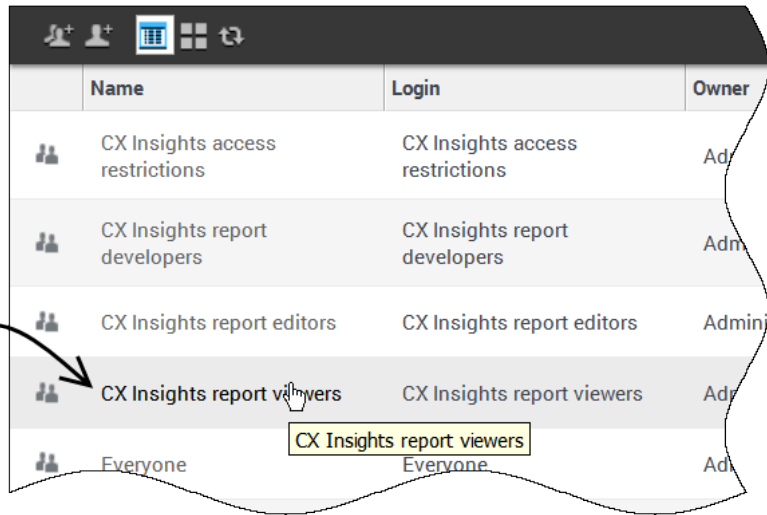
1. In your web browser, open the MicroStrategy Web Administrator page:

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

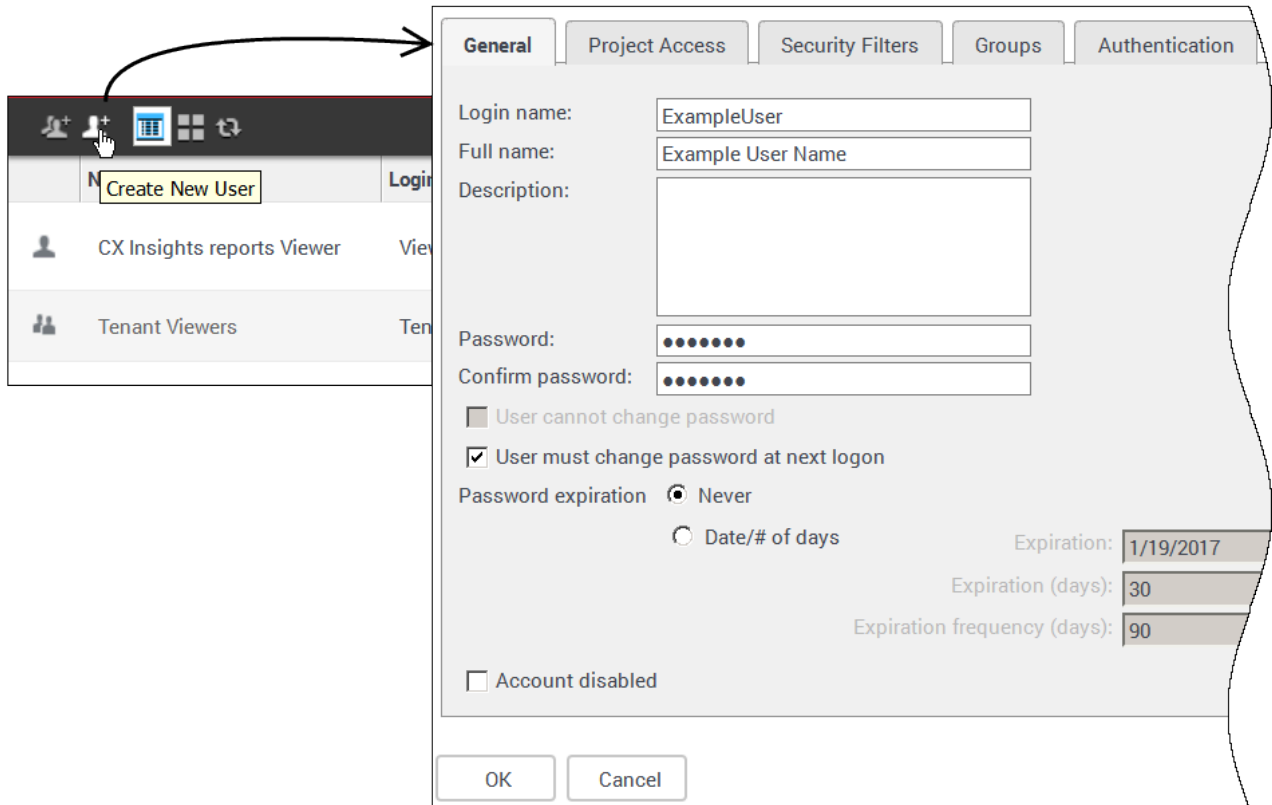
2. On the page that appears, select your server.
3. On the MicroStrategy Web Administrator login screen, enter your user name and current password, and click **Login**. The **Tools** page opens.
4. Click **User Manager**.
5. Click a group of which the user is a member. A list appears, showing all the 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

To simplify the process of creating a new user, select the group (for example, CX Insights reports Viewers) before you click Create New User.



	Name	Login	Owner
	CX Insights access restrictions	CX Insights access restrictions	Ad
	CX Insights report developers	CX Insights report developers	Adm
	CX Insights report editors	CX Insights report editors	Admin
	CX Insights report viewers	CX Insights report viewers	Ad
	Everyone	Everyone	Ad



Create New User

General | Project Access | Security Filters | Groups | Authentication

Login name:

Full name:

Description:

Password:

Confirm password:

User cannot change password

User must change password at next logon

Password expiration Never Date/# of days

Expiration:

Expiration (days):

Expiration frequency (days):

Account disabled

OK Cancel

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**

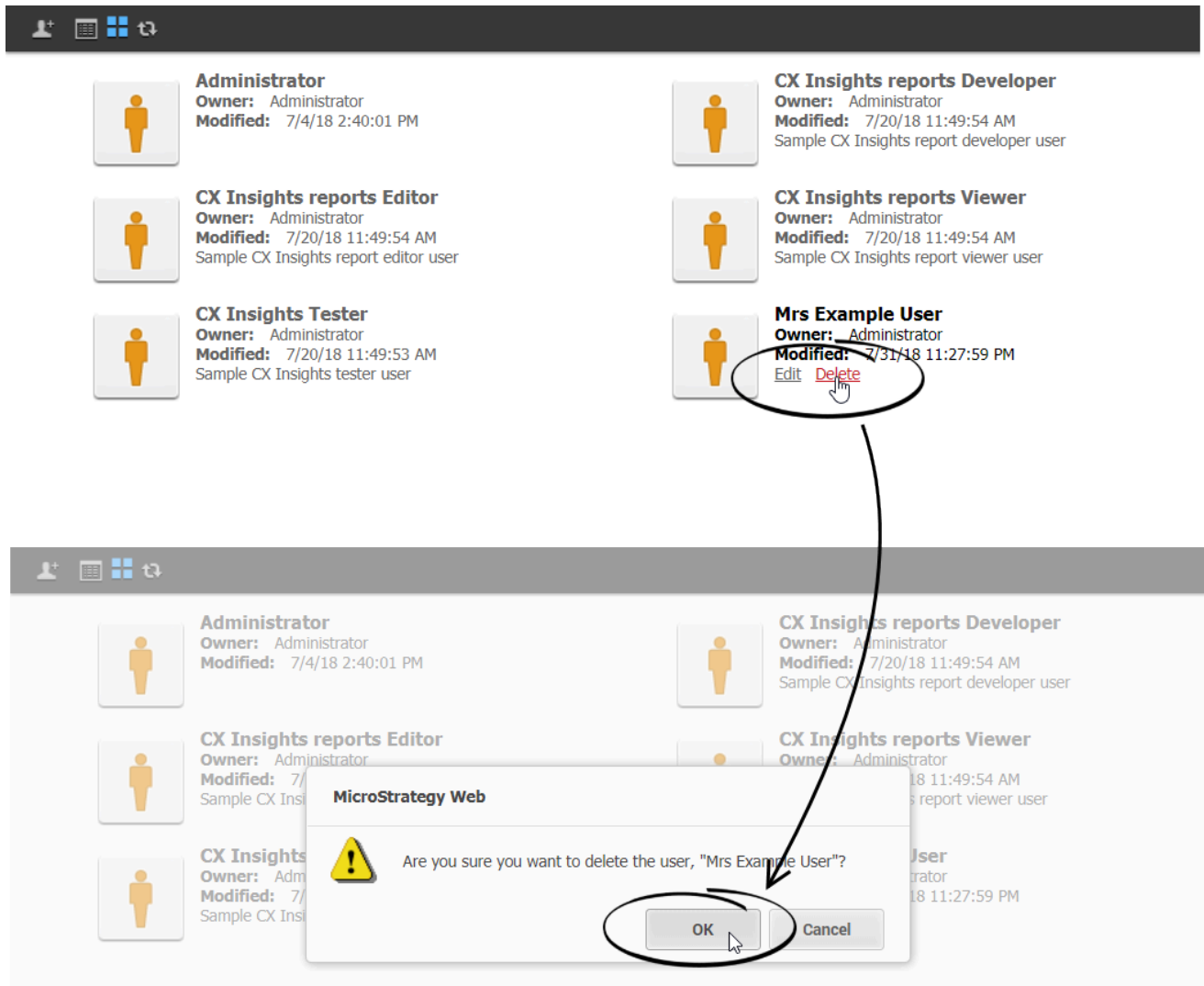
Edit Users And Groups privilege.

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.