Calabrio ONE

ADVANCED REPORTING ADMINISTRATOR GUIDE
FOR ON-PREMISES DEPLOYMENTS

Version 11.5
November 26, 2019

Produced in the United States of America.

Notice

While reasonable effort was made to ensure that the information in this document was complete and accurate at the time of release, Calabrio, Inc. cannot assume responsibility for any errors. Changes and/or corrections to the information contained in this document may be incorporated into future issues. The information in this document is subject to change without notice.

Contents

Advanced Reporting Administration

To use the Advanced Reporting Administration, your user account must have User Admin permission. User Admin permission gives you rights to a portion of your organization's account hierarchy.

Open the Administration tool by going to the following link in a new tab:

https://login.calabrioadvancedreporting.com/admin

If you are already logged in to Advanced Reporting, the Administration page opens. If you are not logged in to Advanced Reporting, the log in page opens. If your account does not have User Admin permission, an error screen displays.

> **NOTE** The email address you use to sign in to Advanced Reporting is not necessarily the email address you use for communication.

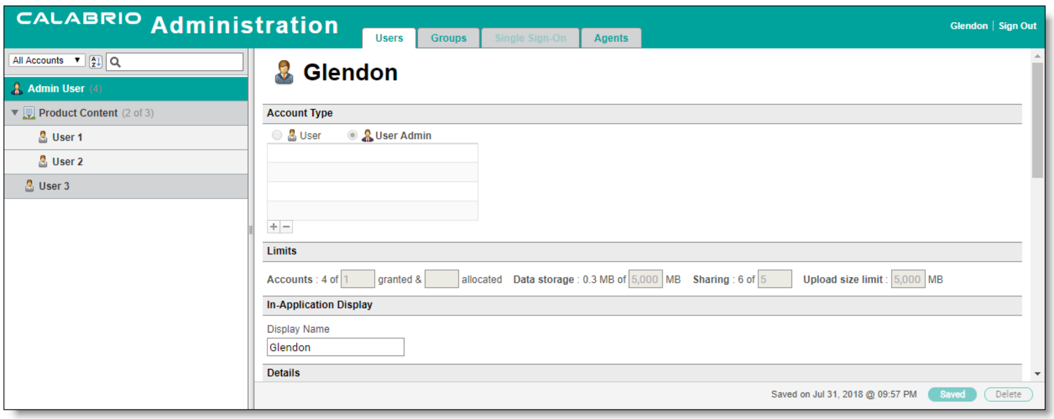
WORK WITH ADMINISTRATION

Use the Administration page to take the following actions:

- Create and manage accounts
- Create and manage groups to facilitate sharing

Users

The Advanced Reporting Administration interface opens on the Users page. The Users page is separated into two sections: an Accounts list and the Account Details pane.



The Accounts list includes all users in your organization. Hierarchy is displayed by nesting users in the list. You can search or filter the list using the filters at the top of the list.

The Users page allows you to take the following actions:

- Create and manage user or organization accounts
- Distribute administrative control
- Control behavior and permissions with attributes

The following table describes the two types of accounts in Advanced Reporting:

ACCOUNT TYPE	DESCRIPTION
User	A user account represents a person who will log in to Advanced Reporting to work with reports, dashboards, and data. User accounts can be configured as User Administrators

ACCOUNT TYPE	DESCRIPTION
	(essentially making them Advanced Reporting Administrators), which provides them with administrative rights. User Administrators: ▪ Can log in to Advanced Reporting to work with reports, dashboards, and data ▪ Can act as a parent of other accounts to create a hierarchy ▪ Can inherit account attributes from parent accounts
Organization	Organization accounts represent business units, such as teams or departments, and are used to organize and simplify the administration of user accounts. Organization accounts act as containers; user accounts inside a given organization account will inherit most of the settings configured on the organization account. Organization accounts: ▪ Can only use the Advanced Reporting Administration. They cannot log in to Advanced Reporting to work with reports, dashboards, and data ▪ Can act as a parent of other accounts to create a hierarchy ▪ Can inherit account attributes from parent accounts

CREATE AND MANAGE ACCOUNTS

If you are a User Admin, you can create, manage, and delete accounts in Advanced Reporting. User accounts are arranged by hierarchy in the Accounts list on the left side of the page. Child accounts are nested beneath their parent account.

NOTE Child accounts inherit account attribute settings and licensing limits from their parent account.

Remember the following points when creating a new user account:

- You must provide a username and password for each user. All other fields are optional.
- Usernames must be formatted as an email address.
- Grant User Admin accounts only to those who require access to Advanced Reporting Administration.

To create a new user account:

1. In the Accounts list, hover over the account that will be the parent account for the new user. The Create a New Organization icon and Create a New User icon appear beside the account name:

2. Click the Create a New User icon, which is outlined in the previous image. The Account Details pane will display the information that the new user account inherited from the parent account.

   The Username/Email Address field and the Password fields will be outlined, because they are required.

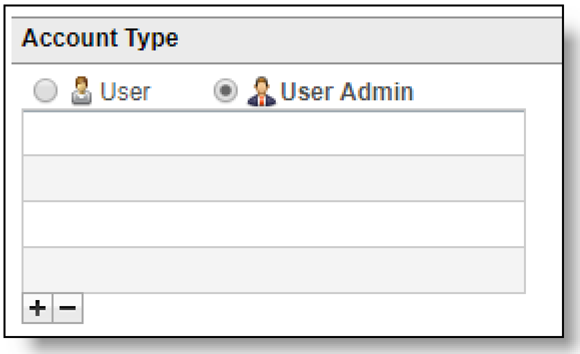
3. Complete the required fields and any other fields according to the requirements of the account.

   BEST PRACTICE Enter a unique name in the Display Name field so you can identify the account in the Accounts list. This is also the name that appears in Advanced Reporting.

4. Click **Save**.

To create a User Admin account:

1. Take the same steps you would take to create a new user account.
2. Mark the **User Admin** field under Account Type at the top of the Account Details pane. Below the Account Type, the Administering Accounts table opens.



3. If the new User Admin will be administering accounts that already exist in the Accounts list but are not hierarchically arranged as children of that account, click the Add icon at the bottom of the table. If the new User Admin will be administering accounts that have not been created yet, leave the table blank.
4. Click **Save**.

To create a new organization account:

1. In the Accounts list, hover over the account that will be the parent of the new organization. The Create a New Organization icon and Create a New User icon appear beside the account name:

2. Click the Create a New Organization icon, which is outlined in the previous image. The Account Details pane will display the information that the new user account inherited from the parent account.

The Username/Email Address field and the Password fields will be outlined, because they are required.

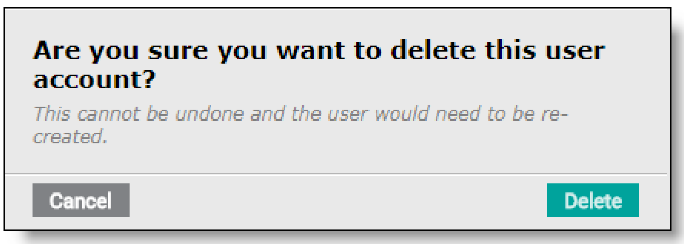
3. Complete the required fields and any other fields according to the requirements of the account.

    BEST PRACTICE Enter a unique name in the Display Name field so you can identify the account in the Accounts list. This is also the name that appears in Advanced Reporting.

4. Click **Save**.

To delete an account:

1. In the Accounts list, select the account to delete.
2. In the bottom right corner of the Users page, click **Delete**. The following dialog box opens to verify your intention to delete the account.



3. Click **Delete**. The account is deleted.

Account Fields

The following tables describe the fields that appear in the Account Details pane. Each table describes the fields beneath the section heading.

Account Type

These fields apply only the user accounts. Advanced Reporting User accounts can be configured as one of two types, Users or User Admins.

FIELD	DESCRIPTION
User	A user that will be logging in and using Advanced Reporting for reporting, data modeling, or both.
User Admin	A user that needs to sign in to the Advanced Reporting Administration Tool for general management of users, organizations, groups, agents, and tasks. User Admin accounts can be given administrative rights to manage specific sections of the user and organization hierarchy. This will allow them to see and alter details of the accounts that belong to the specified hierarchies. User Admins can modify aspects of their organization and its users such as modifying display names and passwords, however they cannot change any of the Limits settings, such as Data Storage, Sharing, and Upload size limit. User Admins can use Advanced Reporting for reporting and data modeling.

Limits

These fields apply to both the user accounts and the organization accounts. Your Advanced Reporting license determines the number of accounts you can have. These limits can be distributed and controlled using the account hierarchy, and the number of sub-accounts are listed and controlled on the account properties page for each account.

For most accounts, you do not need to make any changes to the Limits settings. The account at the top of the hierarchy (your root user account) shows the totals for your Advanced Reporting license.

FIELD	DESCRIPTION
Accounts	The number of accounts determined by the Advanced

FIELD	DESCRIPTION
	Reporting license
Data Storage	The amount of storage available to the user and the amount in use
Sharing	The number of accounts between which data sets can be shared
Upload Size Limit	The largest size allowed for a single data contribution upload

In-Application Display

These fields apply to both the user accounts and the organization accounts.

FIELD	DESCRIPTION
Display Name	The friendly name for the account. This name is shown: ▪ In the top corner of Advanced Reporting when the user is signed in ▪ In the Advanced Reporting Administration Tool ▪ When configuring delivery settings for reports and dashboards **NOTE** The Display Name is not used to sign in to Advanced Reporting and does not have to be the same as the username. It does not have to be a unique name, but a unique name is helpful.

Details

These fields apply to both the user accounts and the organization accounts. In the Details section, you can configure additional, mostly optional information about the account. The type of additional information varies slightly between user accounts and some of this will be inherited from a parent user or organization account.

FIELD	DESCRIPTION
Company/Organization	The name of the user's company.
Username/Email Address	(Required) The username for the user or organization. This must be formatted as an email.
Phone	The phone number associated with the account.
Ex	The phone extension associated with the account.
Industry	The industry in which the organization or user works.
Communication Email Address	The email address for the account. This is not necessarily the same email used for the Username.
First Name	(User account only) The user's first name.
Last Name	(User account only) The user's last name.
Department	The user's department.
Title	The user's job title.

Password

The password fields are required when creating an account. This is also where you can reset passwords for existing accounts. The passwords must match. Users can change their password on the Settings page in Advanced Reporting. A user administrator can change a user's password using these fields. These fields are the only way an organization's password can be changed.

Settings

These fields apply to both the user accounts and the organization accounts. In the Settings section for accounts, you can configure the following options.

FIELD	DESCRIPTION
Status	Toggle an account between Active and Suspended
Role	Specifies if this user will be a Consumer or Content Provider. ▪ Consumer accounts can view reports and dashboards that have been shared with them. ▪ Content Provider accounts can view and create reports and dashboards.
Default Landing Page	Specifies which dashboard should be displayed when the user signs in. The landing page can only be selected from a list of landing pages that was configured on the parent account using the indicee.landing_pages user attribute. **NOTE** This setting may appear on organization accounts, however it does not apply to accounts of this type. **IMPORTANT** When creating Consumer accounts, you must also set a default Landing Page. If you do not set a Landing Page, the user will not be able to see any reports or dashboards.
Parent Account	The parent of this account in the account hierarchy. **NOTE** This is for reference only and cannot be edited here.
Child Accounts	The number of accounts below the current account in the hierarchy.
Add	Add an existing account as a child to the current account. **NOTE** This moves the account within the account hierarchy and is the recommended method of doing so.

Groups

These fields apply to both the user accounts and the organization accounts. With groups, you can logically organize accounts to make sharing content easier.

FIELD	DESCRIPTION
Auto-Group	Mark the check box to create a group based on this account. All child accounts will automatically become members of this group. Auto-Groups can simplify managing groups by automatically updating as child user accounts are created or deleted.
Group Name	The name of the group created by the Auto-Group check box.

Extra Attributes

These fields apply to both the user accounts and the organization accounts. The Extra Attributes section of the account settings page displays the attributes of the current account. Each account has a set of attributes, some required and some optional. An Advanced Reporting administrator can configure attributes to control behavior (for example, how dashboard elements are displayed or application timeout values). Other attributes are read-only and update automatically, such as the last login time.

WORKING WITH ACCOUNT ATTRIBUTES

User account attributes are the details of an account. They provide a flexible method of configuring how Advanced Reporting behaves at the user account level. Each user account has a set of attributes that control or record behavior.

Some attributes are configurable by Advanced Reporting administrators. Other attributes are read-only and update automatically, such as the last login time. Administrators can configure user account attributes in the Advanced Reporting Administration Tool.

Account Attribute Inheritance

Many user account attributes are inheritable. Advanced Reporting will search up the account hierarchy for inheritable attributes. If it finds inheritable attributes, their settings will apply to all child accounts. An example of an attribute that can be inherited by child accounts is Department.

Other attributes, such as a username, are not designed to propagate in this way. Each of these attributes is unique to a specific account.

Some attributes are designed to track metrics and accumulating values, such as the number of reports run by each user. These can accumulated by account attributes located at the root of the hierarchy.

> **NOTE** The attributes that control functionality and access follow the principle of least privilege. This means that a denial of permission will override a grant of permission. Following this principle, users will have the total of all access and rights granted to the hierarchy in which their account exists.

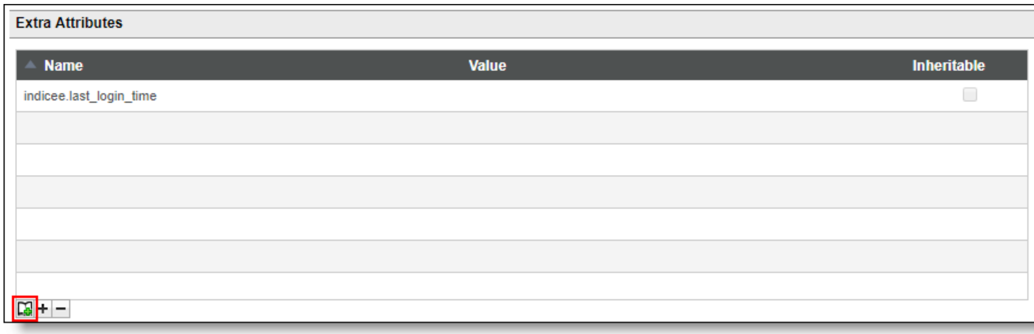
Managing Account Attributes

On the Users page, you can add, create, and delete account attributes.

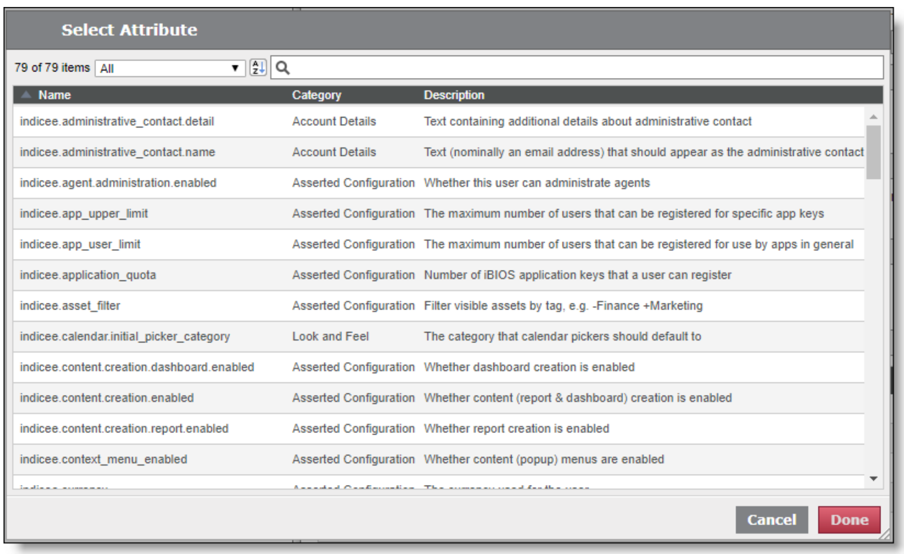
> **NOTE** To make changes to a user or organization account's attributes, you must be logged in to a User Admin account that has permission to manage that user account.

To add an account attribute:

1. In the Accounts list on the Users page, click the user or organization to which you want to add an attribute.
2. At the bottom of the account properties in the Extra Attributes section, click the **Add an Indicee Attribute** icon. The icon is highlighted in the lower left corner of the following image.



The Select Attribute dialog box opens.



3. Click the attribute you want to add.

   NOTE Use the search box to locate an attribute.

4. Click **Done**.
5. Locate the new attribute in the Extra Attributes section and click in the Value column.
6. Replace the contents with the correct value.
7. Press **Enter**.

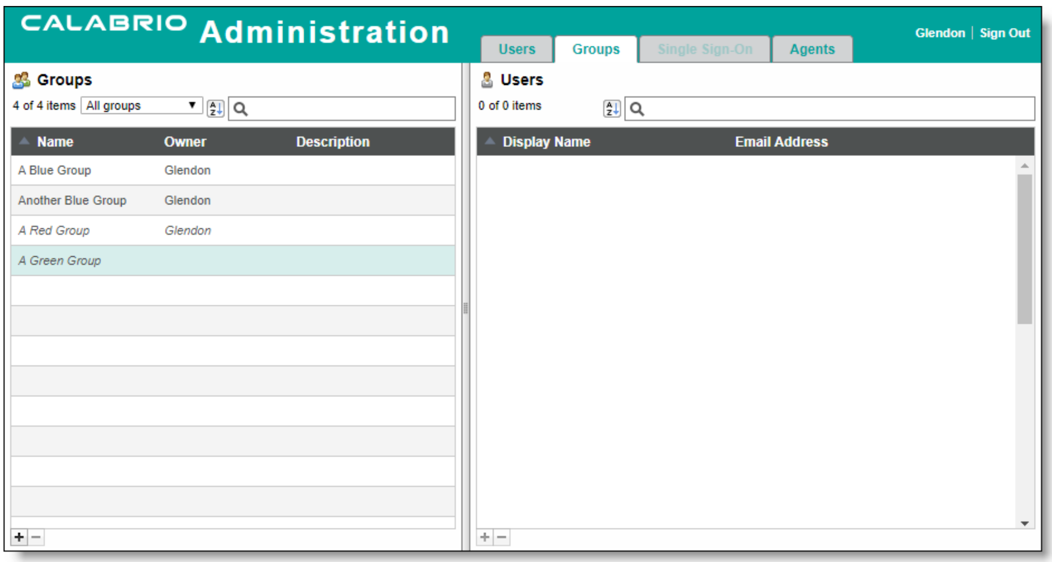
8. (Optional) Mark the Inheritable check box if you want child accounts to inherit this attribute value.
9. Click **Save**.

Add or Delete Account Attributes

To add or delete account attributes, click the Add a New Attribute (+) icon or Remove the Selected Attribute (-) icon at the bottom of the Account Attributes list.

Groups

The Groups tab allows users with administrator permission to create, modify, and delete groups in Advanced Reporting. The Groups page consists of a Groups list, which includes all of the groups that you can manage and a Users list, which includes all of the users in the group that is selected in the Groups list.



Groups are logical organizations of users created by the Advanced Reporting Administrator. Users who belong to a group have access to all the data resources that are shared with that group.

> **EXAMPLE** If User A belongs to groups 1, 3, and 5, they will have access to all the data for each of those groups. If group 3 can access data that groups 1 and 5 don't have access to, User A will have access to the data.

When working in the Advanced Reporting Administration Tool, you create a hierarchy of users. This parent-child arrangement allows you to organize accounts and control the inheritance of account attributes as well as account limits. Similarly, groups help organize users, however membership in a group simply provides users with access to shared resources. When resources such as data, reports, and dashboards are shared with a group, all group members have access to those resources. Data resources can only be shared with groups.

> **NOTE** Group membership in Advanced Reporting doesn't grant administration privileges or other types of system permissions.

SHARING AND OWNERSHIP

By default, only the user who created a data resource, the owner, can access it. The owner can choose to allow access by sharing with one or more groups.

Data Collection

To use reports or dashboards, you must first have access to the data they contain. Data is shared using logical bundles of data called Data Collections. The user who created the Data Collection, the owner, can choose to allow access to it by sharing it with one or more groups.

Report

To see and open a report, you must have been given access to the report itself. The user who created the report, the owner, can choose to allow access to it by sharing it with one or more groups. When you have share access to a report, it will appear on your Reports page.

When you open the report, Advanced Reporting will consult the Data Collection used by the report. If you are not member of a group with share access to that Data Collection, you will be unable to view the contents of the report. To see a report and the data it presents, you must have share access to the data collection and the report.

Dashboard

To see and open a dashboard, you must have been given access to the dashboard itself. The user who created the dashboard, the owner, can choose to allow access to it by sharing it with one or more groups. When you have share access to a dashboard, it will appear on your Reports page.

When you open the dashboard, Advanced Reporting will open each of the individual reports contained in that dashboard. Any reports to which you do not have share access, or that use Data Collections to which you do not have permission, will not be displayed on the dashboard. To see a report and the data it presents, you must have share access to the data collection, the report, and the dashboard.

CREATE AND MANAGE GROUPS

If your account is a User Admin account, you can create, delete , and manage groups.

To create a new group:

1. Click the plus sign (**+**) in the bottom left corner of the Groups list.
2. A new group will appear in the groups list.
3. Double-click the name of the new group.
4. Enter a unique name for the group.
5. Click **Enter** to save the group name.

When you create a new group, you are the only member of the group. You must add members to the group.

To delete a group:

1. Click the group in the Groups list.
2. Click the minus sign (-) in the bottom left corner of the Groups list.
3. Confirm you intention to remove the user from the group.

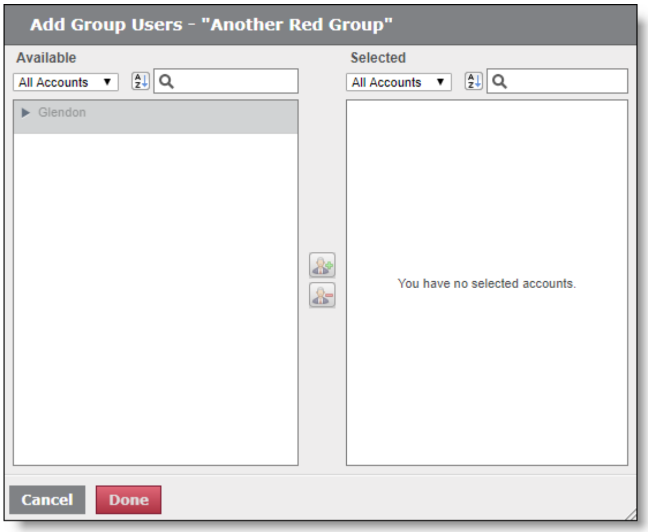
Manage Group Members

When working with groups, you can add members, remove members, and change the owner.

To add members to a group:

1. Click the group to which you are adding members. The Users list will display the current members of that group.
2. Click the plus sign (**+**) in the bottom left corner of the Users list. The Add Group

Users dialog box opens.



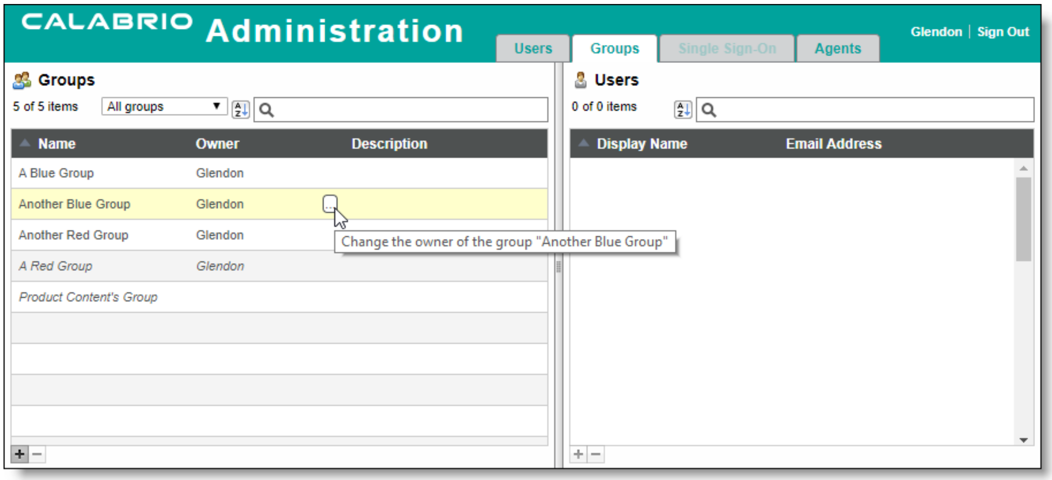
3. Click your account to view the drop-down list with all the available users.
4. Select the user you would like to add to the group. Select more than one user at a time by holding the **Ctrl** or **Shift** key (Mac users hold **Cmd** or **Shift** key) while clicking.
5. Click the Add the Selected Accounts icon to add the users to the group.
6. Click **Done**.

To remove a member from a group:

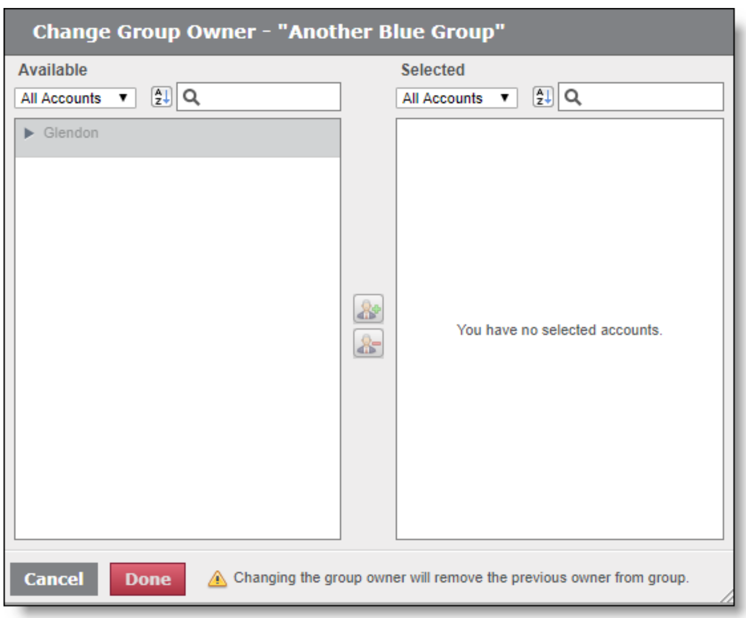
1. On the Group page, click the group in the Groups list. The users that make up that group will appear in the Users list.
2. Select the user to remove.
3. Click the minus sign (-) in the lower left corner of the Users list.
4. Confirm you intention to remove the user from the group.

To change the owner of a group:

1. On the Groups page, hover over the group whose owner you want to change. The Change the Owner of the Group button appears as an icon with an ellipsis (...).



2. Click Change the Owner of the Group. The Change Group Owner dialog box opens.



3. Click your account to expand the hierarchy of all the available users.
4. Select the user you would like to make the owner of the group.
5. Click the Add the Selected Accounts icon to make the user the owner of the group.
6. Click **Done**.

Using Auto-Group

As a User Admin, you can create groups as needed, however often the groups required will match the structure of your organization. People in the same department will often have the same shared resource needs. To take advantage of this, you can use Auto-Group to automatically create groups that follow your account hierarchy.

When Auto-Group is enabled on an account, a group is automatically created using that account's Display Name. All child accounts automatically become members of this group.

Auto-Group can be enabled at any point in the hierarchy, but is often created at a point of organization within your company. For example, you could enable Auto-Group on a manager's account, and all child accounts will automatically be added to a their Auto-Group.