Sopheon Accolade®

Administration - User Administration Training Guide

Version: 16.0

About Sopheon Accolade®

Document Name:	Administration - User Administration Training Guide
Document Version:	1
Software Version:	Sopheon Accolade 16.0
Document Date:	August 2023

Contents

About the Accolade Education Program

This module is part of the Sopheon Accolade Education Program (AEP). The AEP modules are designed to help Accolade users perform the tasks in their company's business process using the Accolade application. The content in the modules is meant to be used side-by-side with the application, and is part of the overall documentation suite provided for Accolade.

The benefits of using Accolade as part of your company's innovation development process include the following:

- Reduced cycle time by displaying clear structure and visibility.
- Reduced rework through timely, properly sequenced completion of all key tasks and milestones.
- Assured positive user experience through properly developed product requirements.
- Improved communication by automating collaboration between multifunctional team members.
- Provided decision-making information. Poor projects are stopped or placed on hold so resources can be redirected to more promising and higher value projects and products.
- Provided clear project requirements. Expectations of a project team and project manager at each stage are clearly spelled out.
- Managed business risk. Break resource commitments into increments or stages.
- Established key baseline information and metrics.

The Accolade documentation suite contains the following additional components:

Document	Contents
Sopheon Accolade What's New in This Release	For each release, review this document for an overview of the new features and changes within the release.
Accolade Online Help	Accessible directly through Accolade, the online Help provides comprehensive how-to and reference information about all aspects of using Accolade.
Sopheon Accolade Administrator's Guide	Provides information for administrative professionals regarding Accolade setup. This information is also provided in the online Help.
Sopheon Accolade Installation Guide	Provides information about the installation of the application and its required databases.
Dashboards for Accolade Installation Guide	Provides installation information for installing the Dashboards for Accolade component.
Quick Reference Cards	A PDF that can be printed double-sided that provides quick tips and navigation information for using Accolade.

Document	Contents
Online Help for Accolade Add-ins	Accolade add-ins, including Accolade Office Extensions, Accolade SmartDocuments for Google, Accolade SmartDocuments for Office, Accolade Portfolio Optimizer, and Accolade's integration with Microsoft Project, each include their own Sopheon created Help file accessible directly from the application after the add-in is installed. Each Help file describes how to use the features of that particular add-in.

Prerequisites for Using this Module

The contents of this training module assumes you are assigned the Accolade user roles and have a basic understanding of the terms and concepts listed below and how they are used in your installation. In addition, the content in the related training modules listed below may be helpful before reviewing the contents of this module.

Accolade User Roles

- Administrator

Terms and Concepts

- Access Groups
- Security Lists*
- Security Profiles*

Related Training Modules

- Information Security

*If in use at your company.

Important! Your company has a license agreement for an agreed number of Accolade users. As the Accolade administrator, be aware of the number of users allowed per your license agreement. If the number of users exceeds the agreed number of licenses, your company may need to revisit the license agreement.

Users and User Accounts Overview

Each employee who uses Accolade has an Accolade user account that contains information that defines who the employee is and what he or she can do and see within Accolade.

Administrators create user accounts that identify a user by login, name, email address, and chat address. Administrators also assign each user a set of attributes that determines what the user can see and do, email notifications they receive about system activity, and the default language in which the application displays.

> See "User Roles Reference" on page 29 for information about user roles and their permissions within Accolade.

To help streamline user creation in your system, consider the following:

- **Template Users** - Create template users that represent various employee responsibilities in your organization. For example, to configure all your Project Managers in your Europe office the same, create a template user account called ProjectManager-Europe. Configure that user with the roles, access group, security settings, and so on that you want to assign to your Europe-based Project Managers. When you create a user account for a new Project Manager in Europe, you can select to copy the account's attributes into the new account.
- **Importing and Updating User Accounts** - You can import multiple users using a specially formatted spreadsheet file. Importing users in this manner is useful when you are first setting up your system.
- **Synchronizing with Active Directory** - If your company uses Microsoft's Active Directory for user authentication and administration, you can synchronize the user accounts defined in Accolade to those defined in your Active Directory server. Synchronizing the user data between your Active Directory and Accolade allows you to maintain user data such as email addresses and user names in the Active Directory without having to maintain the information in multiple locations.

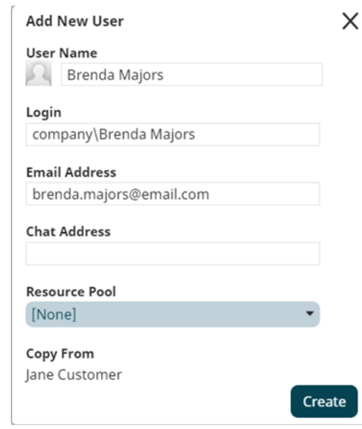
Creating Accolade User Accounts

Create an Accolade user account for each employee that accesses Accolade. The user account contains the attributes the employee needs to do their job and to log in to Accolade.

The procedure below details how to create an individual account. To create multiple users at the same time, see "Importing and Updating Accolade User Accounts" on page 10. If your company uses

Microsoft's Active Directory for user authentication and administration, you can synchronize the user accounts in Accolade to those defined in your Active Directory.

To create a user account:



1. From the **System** menu, select **Collaboration & Groups > User Admin**.
2. Click to display the **Add New User** dialog box.
3. Complete the following information about the user:

   Required fields display with **red** text and an asterisk * if the field is empty.

Field	Description
User Name	Enter the user's name as you want it to display in Accolade. *(Optional)* If the **Enable User Profile Images** system parameter is enabled, add a user profile image that displays with the user's name in various locations within Accolade, click next to the user name, click **Choose Image**, navigate to and select the image to add, and click **Upload File**. To remove a profile image, click the image next to the user name and click **Remove**. **Note:** To display as an image within Accolade, an image file must be one of the following file types: .bmp, .dib, .gif, .jpg, .jpeg, .jpe, jfif, or .png.
Login	Enter the login the user uses to access Accolade. You may consider keeping logins consistent, such as first initial and last name (jdoe) or first name.last name (jane.doe). Depending on how Accolade is installed, a user's login name could be the same as the login in their Windows domain account, LDAP server, or local machine account. For Windows Authentication, logins are <*domain*>\<*login name*> where <domain> is the network domain and <login name> is the login assigned to the user.

Field	Description
Email Address	*(Optional)* Enter the user's corporate email address. Accolade uses this address for email notifications and for email links throughout the system.
Chat Address	*(Optional)* Enter the user's address for your company's selected chat tool.
Resource Pool	*(Optional)* Select the resource pool to which the user belongs. Users are grouped into resource pools for resource planning purposes for assignments to projects. **Note:** This field is only available if your company uses the resource planning components within Accolade and at least one resource pool is defined.
Copy From	*(Optional)* Click **[None]** and select the user whose configuration details you want to copy to this user. To filter the list of users, enter one or more search criteria to filter by name, login name, email address, function, or extended field. • Clicking **Select current user** will assign the role to the current user (if they have the appropriate rights). • Selecting a **Function** in the drop-down will display available users that are assigned to the function. The current selection defaults to the function to which you are assigning a user, however depending on the project configuration, you can assign any user. • Clicking the **Show advanced filters** check box displays or hides the additional filter options. • Clicking **Clear** removes the current user assignment and displays **[None]** to indicate that no user is assigned. Copying configuration details from existing users ensures that users that you want to have the same permissions are set up identically. It allows you to assign most of the details automatically, including the initial **My Work** page and **Stages** page column configurations, and only make a few changes to the user. For example, you may have a set of Process Managers in your organizations that all receive the same configuration. Create one, and then copy the configuration to all others. Create a group of template users that have the appropriate functions, roles, extended fields, and other details that apply to all users in a group.

Field	Description
	💡 Associating a template with each user applies details automatically as part of the create process.

4. Click **Create** to create the user account.
5. Complete the user setup by adding or updating the following:
   - Assign general user details.
   - Add user roles and rights.
   - Grant access group permissions.
   - Add custom details and extended fields, if set as active for the user.
   - Define security list and/or security profiles, if in use by your company.
   - Define user functions.
   - Set up user-specific menu items and links.
   - Set up project email notifications.
   - Set up HTML report notifications.

Importing and Updating Accolade User Accounts

Accolade provides Administrators and Process Designers the ability to export user accounts to update information, and to move configuration between environments. For example, if you are first setting up your system or opening a new office and have multiple user accounts to create at once, or if you need to update accounts such as renewing a user's access on a periodic basis, you can use a spreadsheet file with worksheet tabs to create and update the user accounts within Accolade. Current user accounts can be downloaded from an Accolade environment, changes made to the data, and then uploaded either into the same environment, or moved into a new environment.

> 💡 Create a group of template users that have the appropriate functions, roles, extended fields, and other details that apply to all users in a group. Associating a template with each user applies details automatically as part of the import process. Using filters allows you to assign details to a variety of sub-groups or combinations of groups.

A download of current user accounts exports the user account configuration information into a spreadsheet file with the parts grouped into tabs.

To download user accounts:

1. From the **System** menu, select **Collaboration & Groups > User Admin**.
2. Select the users that you want to download.

   To narrow the list by function or user name, add the criteria to filter by in the appropriate filter text box. These filters are case insensitive. To download all users, clear all search filters.
3. Click ⬇ in the users panel.

By default, the file exports automatically to a temporary internet files directory. Save it to a more accessible location.

To import user accounts into Accolade:

1. Ensure the data within the spreadsheet meets the requirements for a successful import.
2. Remove any user account information that you do not want to include in the upload from the spreadsheet and save the file.
3. From the **System** menu, select **Collaboration & Groups > User Admin**.
4. Click in the users panel.
5. Click **Load File** and select the spreadsheet file to load.
6. Click **Upload File**.

   Accolade uploads the changes to the user accounts in the spreadsheet and adds any new user accounts with unique user logins.

User Account Settings Included in the Spreadsheet File

The columns in the downloaded spreadsheet include the settings for each user account in the order listed below. For a description of each user account setting, see the Creating Accolade User Accounts or User Attributes Overview topics in the online Help.

Important! Using the import and export tools to update configuration can result in unintended changes if information is missing or creates an error during the import process. Sopheon recommends reviewing Importing and Exporting Configuration Best Practices in the online help before making changes in a production environment.

- Import Users

Column Name	Accepted Values on Upload*	Additional Notes
User Name	Alphanumeric characters, underscore**	If blank, the user account does not upload.
User Login	Any	Use the format *(company)\(user login name)* without the parentheses. Used for matching for upload. If a user account exists, its settings are changed with the values in the uploaded file. If a new, unique system name exists in the file when uploaded, a new user account is created. If blank, the user account does not upload.
Email	Valid email address	Can be blank.

Column Name	Accepted Values on Upload*	Additional Notes
Address		
Chat Address	Valid chat address	Can be blank.
Resource Pool	Valid resource pool display name	Can be blank.
Copy From User	User login of user account to copy from	Use the format *(company)\(user login name)* without the parentheses. If the import creates a new user account, the copy from user account settings will be used for the new user setup, and all other tabs in the import worksheet will be ignored. If the import is modifying a current user account, the information in this field is ignored. Can be blank.
Language	An active language	If blank, defaults to English.
Date Format	A valid date format enum	If blank, defaults to MMM dd, yyyy (Feb 28, 2020).
Expiration Date	Valid date	Use the format MM/DD/YYYY. Can be blank.
Active	Yes, Y, True, 1, X*	All other values are treated as **No** on upload.
Show Messages	Yes, Y, True, 1, X*	All other values are treated as **No** on upload.
Enable Auto Search	Yes, Y, True, 1, X*	All other values are treated as **No** on upload.
Reporting Rights	None Refresh AllRights	If blank, defaults to **None**.
My Project Page Updates	Yes, Y, True, 1, X*	All other values are treated as **No** on upload.
Email Format	HTML Plain Text	If blank, defaults to **Plain Text**.
Send Email Number of Days before Defined Date	Valid number	If blank, defaults to **7**.
Delete	Yes, Y, True, 1, X*	All other values are treated as **No** on upload.

* For any column that accepts **Yes**, **Y**, **True**, **1**, or **X**, you can also enter **No**, **N**, **False**, or **0** if it helps you when entering data in the spreadsheet. All values other than **Yes**, **Y**, **True**, **1**, or **X** are treated as **No** when you upload the spreadsheet.

** Limited to characters between a - z, A - Z, and 0 - 9, and the underscore (_).

- Security Lists

  Security lists are optional when importing user accounts. The worksheet must be included in the spreadsheet file, but can be left blank if the users do not have security list assignments.

Column Name	Accepted Values on Upload	Additional Notes
User Login	Valid Accolade user login	Used for matching for upload. Must match a user login from the **Import Users** worksheet. If a user account exists, its settings are changed with the values in the uploaded file.
Security List Name	Valid security list system name	Can be blank.
Security List Value	Valid security list value system name	For each security list field above, include the value for that field to assign to each user. For multi-select extended fields, include a separate row for each value. On import, if a security list value is not included in the sheet, the existing settings for that user are preserved for that field. If a value currently assigned to a user is not included in the sheet, the value is removed from the user.

- Functions

Column Name	Accepted Values on Upload	Additional Notes
User Login	Valid Accolade user login	Used for matching for upload. Must match a user login from the **Import Users** worksheet. If a user account exists, its settings are changed with the values in the uploaded file.
Function	Valid function system name	Include a separate row for each function.

- Roles

Column Name	Accepted Values on Upload	Additional Notes
User Login	Valid Accolade user login	Used for matching for upload. Must match a user login from the **Import Users** worksheet.

Column Name	Accepted Values on Upload	Additional Notes
		If a user account exists, its settings are changed with the values in the uploaded file.
Role	Valid Accolade user role	Include a separate row for each role.

- Portfolio Optimizer Rights

  Portfolio Optimizer is an optional Accolade component that may not be used by your company. The worksheet must be included in the spreadsheet file, but can be left blank if you do not use Portfolio Optimizer.

Column Name	Accepted Values on Upload	Additional Notes
User Login	Valid Accolade user login	Used for matching for upload. Must match a user login from the **Import Users** worksheet. If a user account exists, its settings are changed with the values in the uploaded file.
Right	PortfolioLoad PortfolioSave ScenarioLoad ScenarioSave	Include a separate row for each right to be assigned.

- Pools Rights

  Resource Planning is an optional Accolade component that may not be used by your company. The worksheet must be included in the spreadsheet file, but can be left blank if you do not use Resource Planning.

Column Name	Accepted Values on Upload	Additional Notes
User Login	Valid Accolade user login	Used for matching for upload. Must match a user login from the **Import Users** worksheet. If a user account exists, its settings are changed with the values in the uploaded file.
Pool Name	Valid resource pool display name	Include a separate row for each pool. Can be blank.

- Extended Fields

Column Name	Accepted Values on Upload	Additional Notes
User Login	Valid Accolade user login	Used for matching for upload. Must match a user login from the **Import Users** worksheet. If a user account exists, its settings are changed with the values in the uploaded file.
Extended Field 1...10	Valid extended field name	Enter **ExtendedField_** and the field ID of the field being updated.

Column Name	Accepted Values on Upload	Additional Notes
		This entry, in combination with the data type field in the next column, identify the field being updated. For example, use the following format: ExtendedField_1 or ExtendedField_24.
Extended Field Data Type	Date List Long String Multi-Select Number String	Enter the data type of the field being updated. This entry, in combination with the Extended Field value in the previous column, identify the field being updated.
Value	Valid extended field value	For each extended field above, include the value for that field to assign to each user. For multi-select extended fields, separate values using a pipe (|) character. On import, if an extended field value is not included in the sheet, the existing settings for that user are preserved for that field. If a value currently assigned to a user is not included in the sheet, the value is removed from the user. If an extended field that is defined as required is not included or does not include a value, the user is set to inactive.

- Access Groups

Column Name	Accepted Values on Upload	Additional Notes
User Login	Valid Accolade user login	Used for matching for upload. Must match a user login from the **Import Users** worksheet. If a user account exists, its settings are changed with the values in the uploaded file.
Access Group	Valid access group system name	Include a separate row for each access group. If users are assigned a root level or parent access group, they will be automatically assigned to the child groups of that access group. **Important!** Access group permissions are not always additive to what is already defined in the Accolade environment. The Administrator doing the import can

Column Name	Accepted Values on Upload	Additional Notes
		only make changes to access groups that they can manage. With matching access, the import will add or replace access groups according to what is specified in the file. Do not leave the column blank unless you intend to clear out the settings for the specified user.
Access	Yes, Y, True, 1, X*	All other values are treated as **No** on upload.
Manage Team	Yes, Y, True, 1, X*	All other values are treated as **No** on upload.
Manage Process	Yes, Y, True, 1, X*	All other values are treated as **No** on upload.
Add Project	Yes, Y, True, 1, X*	All other values are treated as **No** on upload.
Migrate Project	Yes, Y, True, 1, X*	All other values are treated as **No** on upload.
Delete Project	Yes, Y, True, 1, X*	All other values are treated as **No** on upload.
Delete Activity	Yes, Y, True, 1, X*	All other values are treated as **No** on upload.
View Configuration	Yes, Y, True, 1, X*	All other values are treated as **No** on upload.
Edit Configuration	Yes, Y, True, 1, X*	All other values are treated as **No** on upload. If **Edit Configuration** is selected as **Yes**, **View Configuration** will automatically default to **Yes**.
Member Of	Yes, Y, True, 1, X*	All other values are treated as **No** on upload. MemberOf access *does not* propagate down to child groups.
Admin Of	Yes, Y, True, 1, X*	All other values are treated as **No** on upload. AdminOf access *does* propagate down to child groups.

* For any column that accepts **Yes**, **Y**, **True**, **1**, or **X**, you can also enter **No**, **N**, **False**, or **0** if it helps you when entering data in the spreadsheet. All values other than **Yes**, **Y**, **True**, **1**, or **X** are treated as **No** when you upload the spreadsheet.

- Security Profiles

  Security profiles are optional when importing user accounts. The worksheet must be included in the spreadsheet file, but can be left blank if the users do not have security profile assignments.

Column Name	Accepted Values on Upload	Additional Notes
User Login	Valid Accolade user login	Used for matching for upload. Must match a user login from the **Import Users** worksheet. If a user account exists, its settings are changed with the values in the uploaded file.
Security Profile	Valid security profile system name	If system name is entered, then the value is **TRUE** for that system name.

- User Links

Column Name	Accepted Values on Upload	Additional Notes
User Login	Valid Accolade user login	Used for matching for upload. Must match a user login from the **Import Users** worksheet. If a user account exists, its settings are changed with the values in the uploaded file.
Title	Alphanumeric characters, underscore**	If blank, the link does not upload.
Link	http:// https:// ftp:// file:// qvp:// mailto: callto:	If blank, the link does not upload.
URL	Valid link URL	If blank, the link does not upload.
Link Number	Any number 1-5	If blank, the link does not upload.

** Limited to characters between a - z, A - Z, and 0 - 9, and the underscore (_).

- Email Notifications

Column Name	Accepted Values on Upload*	Additional Notes
User Login	Valid Accolade user login	Used for matching for upload. Must match a user login from the **Import Users** worksheet. If a user account exists, its settings are changed with the values in the uploaded file.

Column Name	Accepted Values on Upload*	Additional Notes
Notification	Valid email notification option See the Email Notification Distribution Reference topic in the online Help for options.	Can be blank.
On Selected Days	Yes, Y, True, 1, X*	If **YES** is entered, select at least one of the day options on the **Email Days** worksheet. All other values are treated as **No** on upload.
Immediately	Yes, Y, True, 1, X*	All other values are treated as **No** on upload.
Notification System Name	Valid notification system name	If blank, the notification does not upload.

* For any column that accepts **Yes**, **Y**, **True**, **1**, or **X**, you can also enter **No**, **N**, **False**, or **0** if it helps you when entering data in the spreadsheet. All values other than **Yes**, **Y**, **True**, **1**, or **X** are treated as **No** when you upload the spreadsheet.

- Email Days

Column Name	Accepted Values on Upload*	Additional Notes
User Login	Valid Accolade user login	Used for matching for upload. Must match a user login from the **Import Users** worksheet. If a user account exists, its settings are changed with the values in the uploaded file.
Monday	Yes, Y, True, 1, X*	All other values are treated as **No** on upload.
Tuesday	Yes, Y, True, 1, X*	All other values are treated as **No** on upload.
Wednesday	Yes, Y, True, 1, X*	All other values are treated as **No** on upload.
Thursday	Yes, Y, True, 1, X*	All other values are treated as **No** on upload.
Friday	Yes, Y, True, 1, X*	All other values are treated as **No** on upload.
Saturday	Yes, Y, True, 1, X*	All other values are treated as **No** on upload.
Sunday	Yes, Y, True, 1, X*	All other values are treated as **No** on upload.

* For any column that accepts **Yes**, **Y**, **True**, **1**, or **X**, you can also enter **No**, **N**, **False**, or **0** if it helps you when entering data in the spreadsheet. All values other than **Yes**, **Y**, **True**, **1**, or **X** are treated as **No** when you upload the spreadsheet.

- Assignment Notifications

Column Name	Accepted Values on Upload*	Additional Notes
User Login	Valid Accolade user login	Used for matching for upload. Must match a user login from the **Import Users** worksheet. If a user account exists, its settings are changed with the values in the uploaded file.
Past Stages	Yes, Y, True, 1, X*	All other values are treated as **No** on upload.
Current Stages	Yes, Y, True, 1, X*	All other values are treated as **No** on upload.
Future Stages	Yes, Y, True, 1, X*	All other values are treated as **No** on upload.

* For any column that accepts **Yes**, **Y**, **True**, **1**, or **X**, you can also enter **No**, **N**, **False**, or **0** if it helps you when entering data in the spreadsheet. All values other than **Yes**, **Y**, **True**, **1**, or **X** are treated as **No** when you upload the spreadsheet.

Deactivating and Removing User Accounts

As employees change roles or leave your company, you can choose to remove their Accolade user all together, or disable their access by deactivating the user account.

- **Deactivating User Accounts** - Deactivating a user account removes the access for that user, allowing Administrators to save the account information, but ensuring the user cannot access Accolade. Reactivation reinstates assignments and email notification settings as they were set prior to deactivation. Deactivate accounts for situations such as a leave of absence, or a time period when an employee does not require Accolade access. If you use Active Directory to maintain user information in Accolade, you can disable users in Active Directory to deactivate them in Accolade; however, you cannot reactivate an Accolade user account using Active Directory.
- **Removing User Accounts** - Removing a user account removes the user from any default assignments within process models, and removes the user from any project teams. However, the user is not removed as the owner of deliverable or activities in either completed or currently in progress documents. Create reports identifying the deleted user's assignments to identify what needs reassignment.

  Removing a user does not delete the user name from the system. For historical record and auditability purposes, projects and other areas of the system will still reference the original user name even when that user is removed. To mask the user name, change the user's name to a generic placeholder like Bob M######. Deleted users display in *grey italics* throughout the system.

  Removing a user deletes the following user data:

  - User Image
  - User Email

- Chat Address
- User extended field values

Additionally, when a user is deleted, the system maintains the state of the user account at the time of deletion for historical and auditability purposes. For example, if a user is active at the time of deletion, the user account will still be marked as active in the database.

To deactivate a user account:

1. From the **System** menu, select **Collaboration & Groups > User Admin**.

   To filter the list of users, enter one or more search criteria to filter by name, login name, email address, function, or extended field by selecting one or more of the following options and clicking **Search**.

   - Selecting a **Function** in the drop-down will display available users that are assigned to the function.
   - Select a **Group By** option to arrange the user list by roles, functions, resource pools, or access groups.
   - Click **More options** check box displays or hides the additional filter options.
   - In the **Active/Inactive** drop-down, select to filter users by active, inactive, and deleted status from the following options:
     - **Active Users Only** - excludes deleted and inactive users.
     - **Show All Users** - displays active, inactive, and deleted users.
     - **Inactive or Deleted Users** - displays only users marked as inactive or deleted. Both display as *grey italics*.
   - In the **Roles** drop-down, select a specific role to apply to filter the user list.
2. In the **Users** list, select the user(s) to modify.
3. In the **General Details** section, clear the **Active** check box to indicate the user is deactivated.
4. Click **Save** to save your changes.

To remove a user account:

1. From the **System** menu, select **Collaboration & Groups > User Admin**.

   To filter the list of users, enter one or more search criteria to filter by name, login name, email address, function, or extended field by selecting one or more of the following options and clicking **Search**.

   - Selecting a **Function** in the drop-down will display available users that are assigned to the function.
   - Select a **Group By** option to arrange the user list by roles, functions, resource pools, or access groups.
   - Click **More options** check box displays or hides the additional filter options.
   - In the **Active/Inactive** drop-down, select to filter users by active, inactive, and deleted status from the following options:

        - **Active Users Only** - excludes deleted and inactive users.
        - **Show All Users** - displays active, inactive, and deleted users.
        - **Inactive or Deleted Users** - displays only users marked as inactive or deleted. Both display as *grey italics*.
    - In the **Roles** drop-down, select a specific role to apply to filter the user list.
2. In the **Users** list, select the user(s) to modify.
3. Click **Delete User(s)** and click **OK** at the prompt.

> **Notes:**
>
> - Remove user accounts when employees are no longer with your company or if a user withdraws consent in accordance with GDRP regulations. If you remove a user, inform the Process Designers in your organization to update default assignments on process models, as necessary. Understand that deleting a user is a permanent action and cannot be restored. If a user might be reactivated in the future, consider deactivating the user account instead of deleting it.

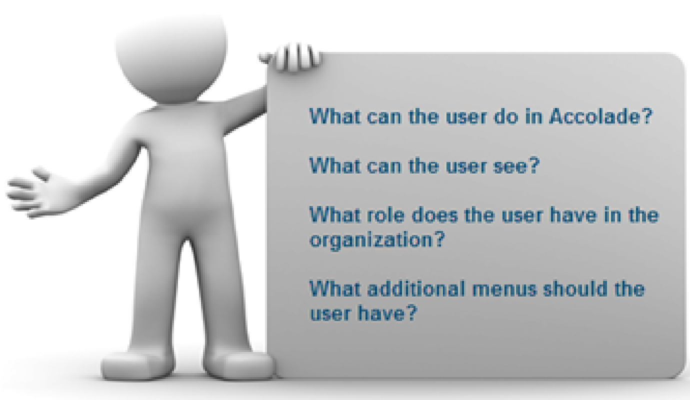
Exercises - Creating Users

Try out what you have learned!

- Create a user about for Jane User, or a name of your choosing.
- Ensure that Jane is setup to have an email address and a login to the system.
- Save Jane as a user. Deactivate her user.

User Attributes Overview

After creating a user account, administrators also assign each user a set of attributes that defines the following:



- **Active Status** - Determines if the user account is active or deactivated.
- **Default Language** - Determines the language in which text within Accolade displays.
- **Date Format** - Determines the format, such as MM/dd/yyyy or dd/MM/yyyy in which dates display and are entered in Accolade.

- **User Roles** - Determines the portions of the application the user can see and what types of tasks he or she can complete in Accolade. The user role, like their login name and email address, belongs to the user regardless of which projects or access groups the user is assigned.
- **Rights to Additional Accolade Features** - Determines what permissions the user has when using Accolade Office Extensions for creating reports and spreadsheets, and for portfolio analysis using Accolade Portfolio Optimizer.
- **Access Groups and Security Settings** - Determines which projects, documents, and process models the user can view and/or edit.
- **Project Management Rights** - For the Process Manager and Idea Manager roles, determines the projects that the user has project management rights, such as the ability to delete a project, based on access group.
- **Email Notifications** - Identifies which events generate and send an automated email notification to the user.
- **Links to Additional Sites and Content** - Provides access to websites, FTP sites, email, or local intranet sites through additional menu options. Links defined here are user-specific.

The **Restrict Administrators From Updating Their Account** system parameter determines if an Administrator can update the attributes of their own user account through the User Admin page or through a spreadsheet file import. Individual users can modify and add some details within their user profile, such as email notifications and subscribing to reports.

Important! Prior to assigning attributes to user accounts, ensure that your company's access groups and security lists are defined.

Searching for and Modifying Existing Users

To find a specific user in the list of users, use the User Search options above the user list. You can search for an individual, or individuals belonging to groups such as user roles, functions, resource pools, and access groups.

To update existing users, select a user from user list and click the user's name. To update the attributes for multiple users at once, select more than one user in the list and click

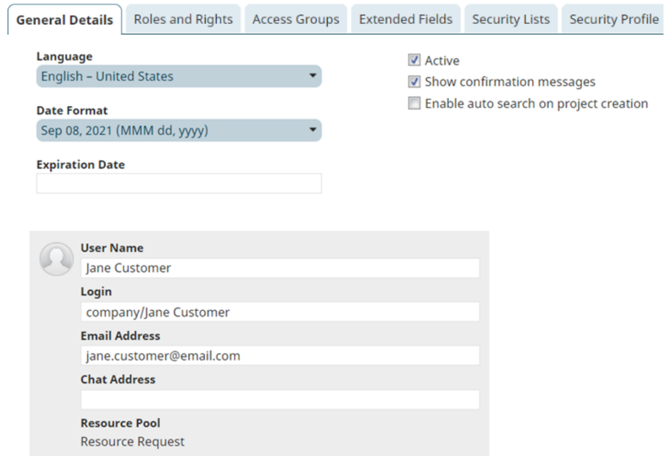
Assigning General User Details

For each user account you create, assign general settings including whether the user account is active, receives confirmation messages for successful actions within Accolade, expires after a specific date, and the default display language and date format for the user.

Users can change settings for all general details except their user name, login, and active status within their own user profile.

To assign general user settings:

1. From the **System** menu, select **Collaboration & Groups > User Admin**.



   To filter the list of users, enter one or more search criteria to filter by name, login name, email address, function, or extended field by selecting one or more of the following options and clicking **Search**.

   - Selecting a **Function** in the drop-down will display available users that are assigned to the function.
   - Select a **Group By** option to arrange the user list by roles, functions, resource pools, or access groups.
   - Click **More options** check box displays or hides the additional filter options.
   - In the **Active/Inactive** drop-down, select to filter users by active, inactive, and deleted status from the following options:
     - **Active Users Only** - excludes deleted and inactive users.
     - **Show All Users** - displays active, inactive, and deleted users.
     - **Inactive or Deleted Users** - displays only users marked as inactive or deleted. Both display as *grey italics*.
   - In the **Roles** drop-down, select a specific role to apply to filter the user list.
2. In the **Users** list, click the name of the user to open the user details for editing .
3. Ensure the **General Details** tab is selected and specify the following information for the user:

Field	Description
Language	Select the language in which the application text displays. The default language is English.
Date Format	Select the display and entry format for dates. The default date format is MMM dd, yyyy (Feb 28, 2016).
Expiration Date	Enter the last date on which the user's account is active. After this date, the user's account is automatically deactivated. Deactivated users are not removed from Accolade; however, they do not have access to any Accolade information.

Field	Description
	For example, you may set an expiration date if you require users to submit access requests on a yearly or more frequent basis, or if a user only requires temporary access to Accolade information. Use a spreadsheet file to import the expiration date for multiple users at once.
User Name	Update the user's name as you want it to display in Accolade. *(Optional)* If the **Enable User Profile Images** system parameter is enabled, add a user profile image that displays with the user's name in various locations within Accolade, click next to the user name, click **Choose Image**, navigate to and select the image to add, and click **Upload File**. To remove a profile image, click the image next to the user name and click **Remove**. **Note:** To display as an image within Accolade, an image file must be one of the following file types: .bmp, .dib, .gif, .jpg, .jpeg, .jpe, jfif, or .png.
Login	Update the login the user uses to access Accolade. Depending on how Accolade is installed, a user's login name could be the same as the login in their Windows domain account, LDAP server, or local machine account. For Windows Authentication, logins are <*domain*>\<*login name*> where <domain> is the network domain and <login name> is the login assigned to the user. **Note:** You may consider keeping logins consistent, such as first initial and last name (jdoe) or first name.last name (jane.doe).
Email Address	*(Optional)* Enter the user's corporate email address. Accolade uses this address for email notifications and for email links throughout the system.
Chat Address	*(Optional)* Enter the user's address for your company's selected chat tool.
Resource Pool	*(Optional)* Select the resource pool to which the user belongs. Users are grouped into resource pools for resource planning purposes for assignments to projects. **Note:** This field is only available if your company

Field	Description
	uses the resource planning components within Accolade and at least one resource pool is defined.
Show confirmation messages	Select this check box to enable or disable the display of confirmation messages as the user successfully completes actions within the system. Disabling this option does not disable the display of error messages.
Enable Auto Search on Project Creation	Select this check box to enable or disable an automatic search for projects with the same or similar names or descriptions when creating new projects. When enabled, Quick Search finds and displays existing projects that match the new project name or description. Use this feature to help discover if like-projects exist so Process Managers do not duplicate efforts when creating projects.

4. Select the **Active** check box to activate or deactivate the user.
5. Click **Save** to save your changes.

Notes:

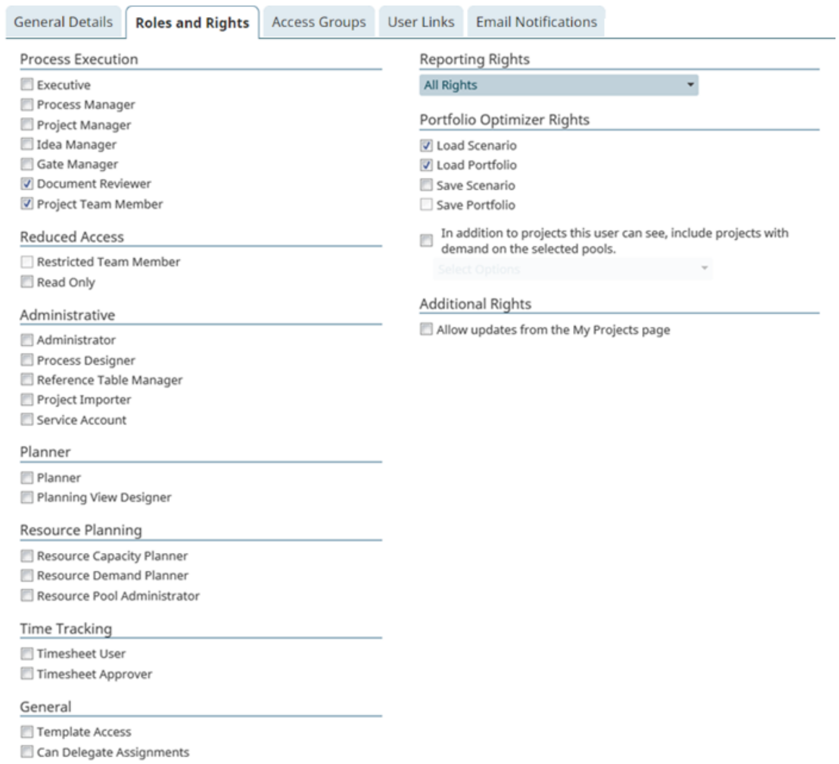
- User details, such as name, login, email, and chat, show for each user when editing multiple users.

Assigning User Roles and Rights

User roles determine the portions of the application the user can see and what types of tasks the user can complete in Accolade. The user role belongs to the user regardless of which projects or access groups the user is assigned.

Rights determine what permissions the user has when creating Accolade online reports or reports with the Accolade Office Extensions add-in, and for portfolio analysis using Accolade Portfolio Optimizer.

Use a spreadsheet file to import or update the roles and rights for multiple users at once.



To assign roles and rights to one or more users:

1. From the **System** menu, select **Collaboration & Groups > User Admin**.

   To filter the list of users, enter one or more search criteria to filter by name, login name, email address, function, or extended field by selecting one or more of the following options and clicking **Search**.

   - Selecting a **Function** in the drop-down will display available users that are assigned to the function.
   - Select a **Group By** option to arrange the user list by roles, functions, resource pools, or access groups.
   - Click **More options** check box displays or hides the additional filter options.
   - In the **Active/Inactive** drop-down, select to filter users by active, inactive, and deleted status from the following options:
     - **Active Users Only** - excludes deleted and inactive users.
     - **Show All Users** - displays active, inactive, and deleted users.
     - **Inactive or Deleted Users** - displays only users marked as inactive or deleted. Both display as *grey italics*.
   - In the **Roles** drop-down, select a specific role to apply to filter the user list.
2. In the **Users** list, click the name of the user to open the user details for editing.
3. Select the **Roles and Rights** tab.

4. Select the check boxes next to the roles to assign.
5. In the Reporting Rights section, select the permissions to grant to this user when creating and viewing reports containing Accolade data in the Accolade Office Extensions add-in or Accolade online reports.
   - **None** - The user cannot create or refresh reports created using the add-in or online reports.
   - **Refresh Workbook Data** - The user can refresh to view the most current data in reports, but cannot create or modify the reports. This is the only option for users assigned only the Read Only role.
   - **All Rights** - The user has full permissions to create and refresh reports.
6. In the **Portfolio Optimizer Rights** section, select the permissions to grant to this user in Portfolio Optimizer.

   If a user has **Load Portfolio** rights, projects load as follows in Portfolio Optimizer:

   - If a user has the Process Manager user role, all projects in access groups to which they have Manage Process rights are loaded when they select to load a portfolio. They can choose to select the **Include All Projects I Can Access** option to load all projects that they have security access to, which may include projects they do not have Manage Process rights to.
   - If a user *does not* have the Process Manager user role, or has the role without Manage Process rights, they must select the **Include All Projects I Can Access** option within Portfolio Optimizer when loading portfolio data. They can work with the data within Portfolio Optimizer; however, they cannot commit changes to projects in Accolade.
   - If a Process Manager cannot load all the projects that have demand on a given resource pool, demand data for that pool is incomplete, preventing resource availability from being calculated accurately. To give managers complete demand data in Portfolio Optimizer, you can allow them to load all the projects that have demand on those pools using the check box and selecting all the pools. However, allowing managers to load projects over which they do not have Manage Process rights also enables them to reschedule resource demand and gate meeting dates in those projects using Portfolio Optimizer.

   Users must have **Save Portfolio** rights, the Process Manager user role, and Manage Process rights in all projects that have changed to save changes made in Portfolio Optimizer back to Accolade.

   See the *Portfolio Optimizer Online Help*, available within the Portfolio Optimizer application, for additional information.
7. In the **Additional Rights** section, select the **Allow Updates from My Work page** option to allow the user to update multiple projects at once using the download and upload feature for projects from the My Work page.

   This setting applies only to Project Managers, Idea Managers, and Project Team Members.
8. Click **Save** to save your changes.

User Roles Reference

A user role is an attribute assigned within a user account that determines what pages the user can see and what tasks the user can complete within Accolade. A user role determines:

- The default Home page displayed when first entering Accolade. The default home pages listed in the descriptions below are the Home pages that display if only that role is assigned. Administrators and Process Designers have the ability to set different home pages for different user roles using Global Links.
- The menus available in the menu bar.
- Tasks the user can complete.

Note: Role names within Accolade are configurable. The roles referred to throughout this documentation use the default role names provided in Accolade.

A user role *does not* determine which projects and documents users can see. That visibility depends on the user's place in the access groups hierarchy and on the user's security profile, if any.

Process Execution Roles

Several different types of managers have control over various objects such as projects, project gates, and reference tables, while other roles are necessary to participate in projects. Process execution roles include:

Role	Description
Document Reviewer *	Document Reviewers review and edit deliverable documents through a structured process defined in a workflow. This role is required to assign someone as an action owner in a workflow process. This role is typically combined with other roles to allow users to review documents in addition to their other tasks. Document Reviewers can: • Be assigned to an action in a workflow. • Complete an action in a workflow. • Enter decisions in the details of a deliverable's workflow. Access groups control a Document Reviewer's access to deliverables. The Document Reviewer role exists only if your company has purchased the Collaborative Workflow features. **Default Home Page:** My Work
Executive	Executives monitor projects and serve as gatekeepers at gate meetings, and are typically upper-level management employees. Executives are people in the organization that make Go or No Go decisions throughout the Phase Gate process. Executives can: • Be assigned as a gatekeeper on a project.

Role	Description
	• View dates for upcoming gate meetings and view project information through Upcoming Gates. • Search for and view published documents. • Use discussions and email to communicate with other gatekeepers on a project. • View summaries and comparisons of project information using charts and reports. Executives cannot modify data in the system unless they are assigned a role that allows them to do so. **Default Home Page:** Charts & Reports
Gate Manager	Gate Managers oversee gate details and the creation and completion of gate documents. A user with the Gate Manager role receives the management rights over the data in a specific gate when assigned as the gate owner of that gate. Gate Managers can: • Be assigned as gate owners. • Manage gate details, upload gate documents, and change gatekeepers on gates they own. **Default Home Page:** Upcoming Gates
Idea Manager *	Idea Managers filter submitted ideas and guide idea projects through the evaluation process. Idea Managers throughout your company may have different responsibilities depending on their management rights. Idea Managers with sufficient rights can: • Review new ideas and either begin work on the project, migrate, close, or delete the idea project. • Request that the idea submitter resubmit the idea, if necessary, and cancel resubmissions. • Update idea project details such as project name, project manager, and description. • Upload versions of unowned deliverables, activities, and gate documents. • Delete deliverables and activities that do not apply. • Update gate meeting details, change a gatekeeper for a gate meeting, enter gate meeting decisions, and upload gate documents for gates with no owner. • Act as the project manager or gate owner when an idea project or gate has no assigned owner. The Idea Manager role exists only if your company has purchased the Idea Submission or Accolade Idea Lab. **Default Home Page:** My Work

Role	Description
Process Manager	Process Managers guide projects through the Phase Gate process from project creation to staffing to deleting the project when it is complete. Process Managers throughout your company may have different responsibilities depending on their management rights. Process Managers with sufficient management rights can: • Create, edit, migrate, close, and delete projects. • Add and remove team members, including the project manager. • Update project details such as project name, description, and group. • Upload versions of unowned deliverables, activities, and gate documents. • Delete activities that do not apply. • Enter project status. • Set gate dates, enter gate meeting decision, and change a gatekeeper for a gate meeting. • Act as the project manager or gate owner when a project or gate has no assigned owner. **Default Home Page:** Upcoming Gates
Project Manager	Project Managers oversee the completion of one or more projects. Process Managers assign Project Managers to projects when the project is created. Users assigned the Project Manager role can be assigned as a Project Manager to a project. When assigned to a project, Project Managers can do the following within that project: • Add team members (if the Project Manager has Manage Team rights) • Assign ownership of deliverables and activities. • Upload versions of unowned deliverables and activities. • Change the project name, description, and enter project status and metrics. • Maintain related documents. • Request resources. Project managers cannot: • Change the project manager or gate owners. • Enter gate details and results. • Create, close, or delete projects.

Role	Description
	Some members of a project team may have both the Project Team Member and Project Manager roles. However, if they are added to the project as a Project Team Member, they only have Team Member rights in that project. **Default Home Page:** My Work
Project Team Member	Project Team Members research and complete work on one more assigned projects. Team Members can: • Locate projects and assignments through My Work. • View project information and communicate with other project members through the project pages. • Create and publish deliverable and activity versions for documents they own. • Assign activities for deliverables that they own to other members of the team. • Add related documents to the project. • Refresh charts and reports based on assigned rights. • View any project that is visible to them or to which they are assigned using Search. **Default Home Page:** My Work

* These roles are available with purchase of their respective features.

Reduced Access Roles

Assign reduced access roles to users that need only visibility or limited rights to edit into one or more projects within your organization. Reduced access roles include:

Role	Description
Restricted Team Member	Restricted Team Members work on deliverables or activities in projects. They are not able to see any project information other than the deliverables and activities they own, nor do they have permission to use reporting mechanisms. Assign this role to consultants or other outside experts (either outside the company or outside the project team) to produce a deliverable in a project without being given access to any other project information. Restricted Team Members can: • Locate and edit deliverables and activities assigned to them through My Work. • Create and publish deliverable and activity versions for documents they own.

Role	Description
	• Enter time on timesheets if the company has purchased Time Tracking features. Restricted Team Members can only enter time on projects that contain the activities and deliverables they own. **Default Home Page:** My Work
Read Only	The Read Only role provides access for company staff who need to search for documents and information throughout the company, but do not have a need to update information. Read Only users can: • Browse, search for and view existing projects, activities, deliverables and published documents to which they have access group or security list access. • View charts and reports. This role does not have any editing or reporting functions, and is restricted from adding or editing projects, related data and documents, creating or printing reports, or viewing dashboards. **Important!** If a user who was previously not set to Read Only is assigned as the owner of any deliverables or activities, removing their other assigned roles and assigning them the Read Only role *does not* remove their access from the project or the ability to update project information by uploading new versions of the assigned documents. To ensure a user is truly Read Only, the assigned Project Manager must remove the user as the document owner from any assigned documents in the project. **Default Home Page:** Search

Administrative Roles

Assign administrative roles to users that configure security, define how Accolade is configured, and design and maintain the development process for your company. Depending on your organization, you may have one or more people in these roles. In order to assign a user to an Administrative role, you must have Admin Of the root access group. Administrative roles include:

Role	Description
Administrator	Administrators maintains Accolade users, access groups, templates, and configuration. Process Designers throughout your company may have different configuration rights. Administrators with sufficient rights can: • Create, modify, deactivate, and remove Accolade user accounts. • Create, modify, and delete access groups.

Role	Description
	• Create queries, charts, reports, classes, link types, spreadsheet workbooks, reference tables, global links, workflows, quick grids, functional areas, functions, and configure Accolade parameters. • Create resource pools and assign resource pool owners. • Edit existing metric definitions. • Download, edit, delete, and add templates to the Template Library, when combined with the Template Access user role. Administrators cannot access projects unless they are assigned a role that allows them to do so. In order to be assigned Admin Of an access group, you must have the Administrator role. See "Granting Access Group Permissions to Users" on page 38 **Default Home Page:** User Administration
Process Designer	Process Designers manage the overall Phase Gate process of a company or division. Process Designers throughout your company may have different configuration rights. Process Designers with sufficient rights can: • Create, modify, and delete models and migration maps. • Create, modify, and delete reference tables. • Create, modify, download, and delete templates in the Template Library, when combined with the Template Access user role. • Create queries, charts, reports, metrics, classes, link types, spreadsheet workbooks, reference tables, global links, workflows, quick grids, functional areas, functions, and configure Accolade parameters. Process Designers cannot access projects unless they are assigned a role that allows them to do so. See "Granting Access Group Permissions to Users" on page 38. **Default Home Page:** Models
Reference Table Manager	Reference Table Managers update reference table values using new versions of existing reference tables that they own. This role is assigned with other user roles. Reference Table Managers can: • Upload a new version of a reference table that they own. • Modify reference table details in tables that they own. Only Administrators and Process Designers can create and upload new reference tables. Users assigned the Reference Table Manager user role can be assigned as the table's owner and can update new versions of the tables they own. **Default Home Page:** Reference Tables

Role	Description
Project Importer	Project Importers import data into Accolade from external files. Project Importers can import multiple projects, project links, matrices and related documents. Paired with the Process Designer role, the Project Importer can also import resource data including demands, pools, curves, and others. A user who imports projects may also need the Reference Table Manager role to edit the reference tables used in the import, and the Process Manager role, to confirm the results of the import. **Default Home Page:** Imports
Service Account	The Service Account role is not intended for assignment to an actual Accolade user. Assign this role to the user account for the Accolade Autoloader Service, which uploads reference tables and related documents automatically from a designated drop box at a scheduled time. If Accolade is configured with Windows Authentication, this user account must also be a user account on the domain, although it does not have to be the account of an actual person. To ensure that reference tables assigned to a specific access group are uploaded successfully when enabled for automatic upload, assign the user with the System Service user role access to all access groups defined in the system. See "Granting Access Group Permissions to Users" on page 38.
Data Analyst	The Data Analyst own the creation and maintenance of API keys that can access Accolade data to be used for queries and reporting.

Planner Roles

Assign one or more planner roles to update objects and views within Innovation Planning. These roles exist only if your company has purchased the Innovation Planning features. Planner roles include:

Role	Description
Planner *	Planners develop and maintain innovation plans in Accolade Innovation Planning. Users with the Planner role can see the **Planning** menu and access the Innovation Planning application. The Planner role can be assigned with the Process Manager role to allow Planners to create planning elements. In addition, a Planner can also be a Project Team Member to allow assignment to planning element teams, and the Process Manager role that grants administrative privileges based on assigned management rights. A Planner's additional rights within Innovation Planning are defined through Accolade security lists and access group rights. If your company does not run Innovation Planning, but uses Accolade's integration with Microsoft Project, assign this role to users for access to the My Project Gantt view.

Role	Description
	Default Home Page: Planning Board
Planning View Designer *	Planning View Designers can share the planning views they create with other Planners by making the views public, and they can also update the settings in other public views to which they have access. Planning View Designers must also have the Planner role to access the **Planning** menu, and cannot change values within planning elements in a view unless they have the other user roles that allows them to do so.

* These roles are available with purchase of their respective features.

Resource Planning Roles

Assign one or more resource planning roles to users that manage resource capacity and demand within your company. Combine these roles with other roles if a user has more than one role within your company. These roles exist only if your company has purchased the Resource Planning features. Resource planning roles include:

Role	Description
Resource Capacity Planner *	Resource Capacity Planners maintain resource capacity levels for resources (both employee and material) throughout the company. Pair with the Resource Demand Planner role to provide access to Resource Editor. **Default Home Page:** Resource Planning
Resource Demand Planner *	Resource Demand Planners plan and assign the resources, personnel and material, each project needs. They adjust resource assignments from stage to stage and balance resource requests against resource availability. Resource Demand Planners can: • Enter resource demand for projects. • Apply demand curves to projects. • Add resources to an individual project and modify resource demand. • Adjust demand values in demand curves for resources in pools they own on the Demand Curve page. • Transfer a resource from pools they own pool to a different pool on the Edit Resource page. **Default Home Page:** Resource Planning
Resource Pool Administrator *	Resource Pool Administrators create and maintain resource pools. Resource pools group your resources by geographical region, job function, or any other grouping that fits into your organization. Resource Pool Administrators can:

Role	Description
	• Create resource pools, add or remove members from a pool, and delete pools. • Assign pool owners. • Link pools together. • Create and edit demand curves. **Default Home Page:** Pools

* These roles are available with purchase of their respective features.

Time Tracking Roles

Assign time tracking roles to users participating in projects and managers needing to approve project time entries. These roles exist only if your company has purchased the Time Tracking feature. Time tracking roles include:

Role	Description
Timesheet User *	Timesheet Users can access timesheets, which is where users can track their time against various projects within Accolade. This role can be the only role available to users who are required to log their time, but do not require access to additional information within Accolade. The Time Sheet Approver role exists only if your company has purchased the Time Tracking features. **Default Home Page:** Timesheet Entry
Timesheet Approver *	Timesheet Approvers can access the Timesheet Approval page, where they can review timesheets for all employees who report to them. This role can be the only role assigned to users who are required to approve time worked, but do not require access to additional information within Accolade, or combined with any other role. Users with the Timesheet Approver role can be assigned as the timesheet approver for a resource pool. If combined with the Resource Pool Administrator user role, the timesheet approver can define and configure resource pools for time tracking purposes. **Note:** Project Managers have access to approve time for projects they manage, without having the Timesheet Approver role. **Default Home Page:** Timesheet Approval

* These roles are available with purchase of their respective features.

General Roles

Assign general roles to enhance the ability of other user roles within Accolade. For example, allow managers to delegate responsibilities when they are on leave, or give the template access role to users configuring or designing processes to easily add or update templates. General roles include:

Role	Description
Template Access	Template Access users can access the Template Library, which is where templates for documents created in your company are stored. This role is combined with other user roles, and the role combination determines what type of access the user has: • Administrators and Process Designers with this role can view existing templates and add templates to the library. In addition, Administrators and Process Designers can create and modify Quick Grid and Workflow templates. • Process Managers, Idea Managers, Project Managers, and Project Team Members with this role can view templates that are labeled as **Other**. These are typically templates that are not formatted or populated with any data types. **Default Home Page:** N/A
Can Delegate Assignments	Users with this role are able to delegate their assignments to another user for a specific time period; for example, while they are out of the office. Delegating assignments helps to ensure that project work, including workflows, continues while a team member is unavailable. This role does not determine who is available to delegate assignments to. Assignments can be delegated to any user with the Project Manager, Idea Manager, Project Team Member, or Document Reviewer role. **Default Home Page:** N/A

Granting Access Group Permissions to Users

An access group is a container of projects, users, reference tables, and/or planning elements (in Accolade Innovation Planning) that enforces information security. Access groups restrict which process models, projects, reference tables, or planning elements users can see or find using search.

Assign each user account within your system to one or more access groups to grant access to the data available within that group.

Note: Selecting the top-level access group (i.e. Root) grants permission to all access groups in the tree. Additionally, selecting a parent within the tree structure grants permissions to all access groups within that tree.

To assign permissions to an access group:

1. From the **System** menu, select **Collaboration & Groups > User Admin**.

   To filter the list of users, enter one or more search criteria to filter by name, login name, email address, function, or extended field by selecting one or more of the following options and clicking **Search**.

- Selecting a **Function** in the drop-down will display available users that are assigned to the function.
- Select a **Group By** option to arrange the user list by roles, functions, resource pools, or access groups.
- Click **More options** check box displays or hides the additional filter options.
- In the **Active/Inactive** drop-down, select to filter users by active, inactive, and deleted status from the following options:
    - **Active Users Only** - excludes deleted and inactive users.
    - **Show All Users** - displays active, inactive, and deleted users.
    - **Inactive or Deleted Users** - displays only users marked as inactive or deleted. Both display as *grey italics*.
- In the **Roles** drop-down, select a specific role to apply to filter the user list.

2. In the **Users** list, click the name of the user to open the user details for editing.
3. Click the **Access Groups** tab.

   The access groups display in the tree on the left. Use the check boxes to grant the user certain permissions within selected access groups.

Note: Selecting a parent access group in the tree structure automatically includes the child access groups, except for the Member Of column.

4. Define user admin rights for users with the Administrator role:

User Admin Right	Description
Member Of	When checked, the user becomes a member of that particular access group. Users must be a **Member Of** at least one access group.
Admin Of	Only enabled if the user has the Administrator role checked on the Roles and Rights tab. Administrators are granted create/edit ability only within the access groups for which they have **Admin Of** checked. All other rows will be disabled. Users with the Administrator role must be the Admin Of at least 1 Access Group. Only a root level administrator can grant a user **Admin Of** rights if they are not already an Administrator (roles and rights). If multiple users are selected and the editor does not select **Admin Of** for ALL users, they will appear to be read only.

5. Check the access group that the user belongs to for project access in the **Access** column.
6. Define project management rights for users with the Process Manager, Project Manager or Idea Manager user roles:
   - The Project Manager role will be disabled if the user being edited has Manage Team checked in their Access Groups tab.
   - The Process Manager and Idea Manager roles will be disabled if the user being edited has any of the following components checked in their Access Groups tab outside of the editors Admin Of groups.
     - Manage Team
     - Manage Process
     - Migrate Project
     - Add Project
     - Delete Project
     - Delete Activity
   - Only Administrators at the highest level of the Access Group hierarchy (Root) can Create/Edit/Remove the following roles on the Roles and Rights tab:
     - Administrator
     - Process Designer
     - Service Account

Note: When creating a new user through **Copy From**, the same access group logic applies. Access group permissions will apply based on the administration permissions of the user creating the user profile. Administrator, Process Designer, and Service Account roles will not be copied over unless the editor is a root level Administrator.

Management Right	Description
Manage Team	The ability to edit the members of a team. Your company may have highly sensitive data and projects that require restriction around who can be assigned to the project. Use this option to define which Project Managers and Process Managers within your organization have the ability to add team members to their projects and change project team leaders. For example, if you are developing products in other countries, or developing products or services that require specific security clearance, it becomes increasingly important to manage the team based on location or specific security credentials. You want to ensure that once a team is set for the product, team members who do not meet the criteria for working on the project are not added.

Management Right	Description
Manage Process	The ability to assign gate owners and project managers, add team members to upload documents without a document owner and to enter metric values. As a best practice, only one user should have Manage Process rights for a project. Keeping Manage Process rights separate helps to prevent accidentally overwriting another user's changes.
Add	The ability to add a new project using an existing class and model.
Migrate	The ability to migrate or copy a project to a different process model.
Delete	The ability to delete a closed project from the system.
Delete Activity	The ability to delete activities that do not apply from within projects.

7. Define configuration permissions for users with the Administrator or Process Designer user role:

Configuration Rights	Description
Edit	The ability to edit configuration components. Your organization may be structured to have multiple Administrators or Process Designers in different branches. Restrict users to edit only the configuration components relevant to their branch of the organization. View is automatically checked when Edit is selected.
View	The ability to view configuration components. Your organization may be structured to have multiple Administrators or Process Designers in different branches. When you grant users View access only, configuration components such as process models, gate documents, and deliverables and activities will display as read-only.

8. *(Optional)* Define the Security permissions via the **Security Lists** or **Security Profiles** tabs.
   - Security Lists provide a regional list.
   - Security Profiles provide a list of access for Class and Metrics to choose from for a user account.
9. Click **Save** to save your changes.

Assigning Custom Details to Users

If extended fields are set as active for users, an **Extended Fields** section displays for each user record defined within Accolade. Use these fields to assign custom details, such as department information, to each user. How extended fields are used, and whether they are required for users, is specific to your company.

The **Extended Fields** section is disabled if multiple users are selected to modify. To assign extended fields to multiple users at once, use a spreadsheet file to import the extended field settings.

To assign an extended field values to a user:

1. From the **System** menu, select **Collaboration & Groups > User Admin**.

   To filter the list of users, enter one or more search criteria to filter by name, login name, email address, function, or extended field by selecting one or more of the following options and clicking **Search**.

   - Selecting a **Function** in the drop-down will display available users that are assigned to the function.
   - Select a **Group By** option to arrange the user list by roles, functions, resource pools, or access groups.
   - Click **More options** check box displays or hides the additional filter options.
   - In the **Active/Inactive** drop-down, select to filter users by active, inactive, and deleted status from the following options:
     - **Active Users Only** - excludes deleted and inactive users.
     - **Show All Users** - displays active, inactive, and deleted users.
     - **Inactive or Deleted Users** - displays only users marked as inactive or deleted. Both display as *grey italics*.
   - In the **Roles** drop-down, select a specific role to apply to filter the user list.
2. In the **Users** list, click the name of the user to open the user details for editing .
3. Select the **Extended Fields** tab.
4. Enter the custom information as needed for each user.
5. Click **Save** to save your changes.

Notes:

- Use the **User Details** column set in the **Users** subject within Accolade Office Extensions and Accolade Online Reporting to report on extended fields assigned to users.

Assigning Users to Security Lists

When security lists are first added to Accolade, they are configured with no users assigned to the list. Administrators must configure the security for all existing users.

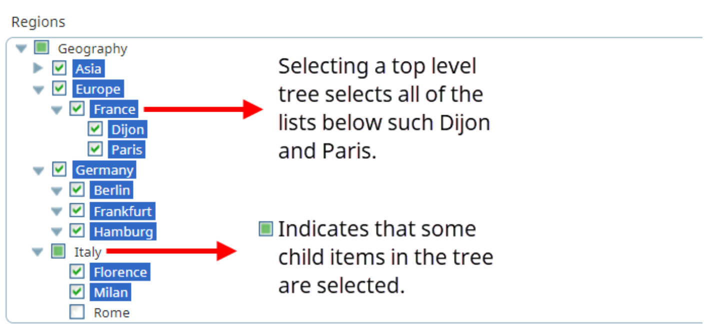
To assign a user to a security list:

1. From the **System** menu, select **Collaboration & Groups > User Admin**.

   To filter the list of users, enter one or more search criteria to filter by name, login name, email address, function, or extended field by selecting one or more of the following options and clicking **Search**.

   - Selecting a **Function** in the drop-down will display available users that are assigned to the function.
   - Select a **Group By** option to arrange the user list by roles, functions, resource pools, or access groups.
   - Click **More options** check box displays or hides the additional filter options.
   - In the **Active/Inactive** drop-down, select to filter users by active, inactive, and deleted status from the following options:
     - **Active Users Only** - excludes deleted and inactive users.
     - **Show All Users** - displays active, inactive, and deleted users.
     - **Inactive or Deleted Users** - displays only users marked as inactive or deleted. Both display as *grey italics*.
   - In the **Roles** drop-down, select a specific role to apply to filter the user list.
2. In the **Users** list, click the name of the user to open the user details for editing .
3. Select the **Security Lists** tab.
4. Select the check boxes for each security list to assign to the user, noting the tree structure.

   Selecting a top level of a tree selects all the lists below it. A check box filled with indicates that some of its child items are selected, but does not provide access to the corresponding list.



5. Click **Save** to save your changes.

Assigning Functions to Users

Functions help identify the type of specialist within your company that owns a deliverable, activity, workflow action, or gatekeeper position in a project. By assigning users to functional areas and functions, you can ensure that project team members are assigned to the appropriate events within a project, as well as allowing team members to see who is responsible for each functional area within projects. See the Assigning Team Members to Projects topic in the online Help for more information.

To assign functions to a user:

1. From the **System** menu, select **Collaboration & Groups > User Admin**.

   To filter the list of users, enter one or more search criteria to filter by name, login name, email address, function, or extended field by selecting one or more of the following options and clicking **Search**.

   - Selecting a **Function** in the drop-down will display available users that are assigned to the function.
   - Select a **Group By** option to arrange the user list by roles, functions, resource pools, or access groups.
   - Click **More options** check box displays or hides the additional filter options.
   - In the **Active/Inactive** drop-down, select to filter users by active, inactive, and deleted status from the following options:
     - **Active Users Only** - excludes deleted and inactive users.
     - **Show All Users** - displays active, inactive, and deleted users.
     - **Inactive or Deleted Users** - displays only users marked as inactive or deleted. Both display as *grey italics*.
   - In the **Roles** drop-down, select a specific role to apply to filter the user list.
2. In the **Users** list, click the name of the user to open the user details for editing .
3. Select the **Functions** tab.
4. Select the applicable function check boxes for each user.
5. Click **Save** to save your changes.

Adding User-Specific Menu Items

User links provide access to websites, FTP sites, email, local intranet sites, or files available on your network through an additional Accolade menu available to individual users. Administrators can define up to five links for each user.

User-specific links display under the **My Links** menu, which is only available if the user account has a user-specific link defined, or if a global link is defined to display in that menu.

To create a user link for one or more users:

1. From the **System** menu, select **Collaboration & Groups > User Admin**.

   To filter the list of users, enter one or more search criteria to filter by name, login name, email address, function, or extended field by selecting one or more of the following options and clicking **Search**.

- Selecting a **Function** in the drop-down will display available users that are assigned to the function.
- Select a **Group By** option to arrange the user list by roles, functions, resource pools, or access groups.
- Click **More options** check box displays or hides the additional filter options.
- In the **Active/Inactive** drop-down, select to filter users by active, inactive, and deleted status from the following options:
  - **Active Users Only** - excludes deleted and inactive users.
  - **Show All Users** - displays active, inactive, and deleted users.
  - **Inactive or Deleted Users** - displays only users marked as inactive or deleted. Both display as *grey italics*.
- In the **Roles** drop-down, select a specific role to apply to filter the user list.

2. In the **Users** list, click the name of the user to open the user details for editing.
3. Select the **User Links** tab.
4. In the **Title** field, click **None** and enter the name of the link, up to 64 characters in length, as you want it to display.
5. In the **Link** field, select the link type to create:
   - **http** or **https** - A URL to a Web page or secure Web page. The **Disable Link to Website** system parameter settings determines if you can link to Web page.
   - **ftp** - A link to an FTP download site.
   - **file** - A link to a file or executable on your company's intranet. The **Disable Link to File** system parameter setting determines if you can link to a file.
   - **qvp** - A link to a Qlik application file. The **Disable Link to File** system parameter setting determines if you can link to a file.
   - **mailto** - Opens the user's email application and displays a blank email addressed to this email address.
   - **callto** - Opens your selected chat and collaboration tool, which invites the person at the address you define to a chat.
6. Is the adjacent field, enter the path to complete the link address.

   For example, if you select **http://** from the **Link** field, enter the remainder of the web site address, www.google.com.
7. Click **Save** to save your changes.

Notes:

- To delete a user-specific link, clear the information entered in all the fields for the link and click **Save**.

Setting User Email Notifications for System Events

You can configure most users to receive an email notification when Accolade events occur, such as activity and deliverable deadlines. Email notifications about system events allow users to receive notification of changes in the system or upcoming events, without having to login to Accolade to check the status of their projects. You can select to notify users about events immediately or on specific days each week.

To set email notifications for one or more user:

1. From the **System** menu, select **Collaboration & Groups > User Admin**.

   To filter the list of users, enter one or more search criteria to filter by name, login name, email address, function, or extended field by selecting one or more of the following options and clicking **Search**.

   - Selecting a **Function** in the drop-down will display available users that are assigned to the function.
   - Select a **Group By** option to arrange the user list by roles, functions, resource pools, or access groups.
   - Click **More options** check box displays or hides the additional filter options.
   - In the **Active/Inactive** drop-down, select to filter users by active, inactive, and deleted status from the following options:
     - **Active Users Only** - excludes deleted and inactive users.
     - **Show All Users** - displays active, inactive, and deleted users.
     - **Inactive or Deleted Users** - displays only users marked as inactive or deleted. Both display as *grey italics*.
   - In the **Roles** drop-down, select a specific role to apply to filter the user list.
2. In the **Users** list, click the name of the user to open the user details for editing .
3. Select the **Email Notifications** tab.
4. Select when to send emails to the users:
   - **To provide the users with scheduled emails** - Select one or more days of the week in the **Send me emails every** row and one or more events in the **On Selected Days** column. Emails are sent at midnight before the selected days and include a report about the selected events. You must select at least one day of the week and at least one event in the **On Selected Days** column for the report to send.
   - **To provide the users with immediate notifications** - Select one or more check boxes in the **Immediately** column.

   It is possible to send both an immediate notification and a scheduled notification about the same event.

If you are modifying settings for multiple users, some settings may be different for different users in the group. Check boxes with different values display with a blue filled in center . Click the check box once to clear it for all users and a second time to select it for all users.

5. To limit the stages for which assignment notifications are sent, select one or more stage selections in the **Send notifications for assignments in** options.

   For example, if your deliverable and activity owners only want to receive notifications for their assignments in the current stage of a project, select **Current Stage** and ensure the **Past Stages** and **Future Stages** options are cleared.

6. At the bottom of the event list, select whether to send emails in either plain text or HTML format.
7. Click **Save** to save your changes.

Notes:

- The **Number of days before...is due** events occur at midnight before the relevant day, and any immediate notifications for them are sent out then. The events for the late notifications, such as **Deliverable is late**, occur at midnight after the relevant day, and any “immediate” notifications are sent out then.
- Set users with the Document Reviewer user role to receive a notification that a deliverable is ready for their review, as that notification alerts them that their workflow action has started.
- Emails to users set as Restricted Team Members do not contain any project links that emails to other roles or assignments because of a Restricted Team Member's limited navigation ability within Accolade.

Exercises - Creating Users

Try out what you have learned!

- Find the user you created in the previous set of exercises and reactivate the user.
- Assign that user the Process Manager role with the ability to create and manage projects, but not delete or migrate projects.
- Create another user as an Executive with the ability to refresh Table Wizard and Report Generator reports.

Synchronizing Users with Active Directory Overview

Note: The information in this section assumes that you have a working knowledge of Active Directory and how it is setup and defined at your company.

If your company uses Microsoft's Active Directory for user authentication and administration, you can synchronize the user accounts defined in Accolade to those defined in your Active Directory server. Synchronizing the user data between your Active Directory and Accolade allows you to maintain user data such as email addresses and user names in the Active Directory without having to maintain the information in multiple locations. If you disable users in the Active Directory those users are deactivated within Accolade when the synchronization runs. However, you cannot activate users in Accolade using Active Directory.

Synchronize additional data from your Active Directory users to user accounts in Accolade using extended fields.

A service runs once an hour to synchronize the data from Active Directory to Accolade.

EXAMPLE Example

If an employee changes their name or their login information changes, if you synchronize user data with Active Directory, you need only to make the changes within Active directory. An Accolade service runs in the background that keeps the information synchronized with the user information mapped in Accolade.

In addition, when you create user accounts in Accolade, you can search Active Directory for users and pull the user information directly from Active Directory into the user profile within Accolade.

After the **Active Directory Enabled** parameter is set in the Administration Console, continue with the following sections to map the server and create accounts.

Mapping the Active Directory Server

To synchronize users with Active Directory, you must first tell Accolade where to find the Active Directory instance, and then map attributes available within Active Directory used to identify users.

To sync users between Accolade and the Active Directory at any time, click **Sync** on the Active Directory page. A synchronization service runs in the background once an hour.

To add an Active Directory and define the server information:

1. Ensure that the **Active Directory Enabled** system parameter is set to **1** in the Administration Console.

   The functionality is disabled by default.

2. Within Accolade, from the **System** menu, select **System > Active Directory**.
3. Do one of the following:
   - **To add a new Active Directory** - Click ⊕ in the lower left corner of the page.
   - **To edit an existing Active Directory** - Click inside the field that you want to edit.
4. Enter the following information:

Field	Description
Display Name	Enter the name of the server, as it displays in the Active Directory page.
System Name	Enter a unique identifier for the Active Directory for within Accolade, for example, companyNameAD. The system name is not displayed to users and can be abbreviated to make it easy to use in queries. The system name must be unique and can include only letters (English alphabet), numbers, and the underscore.
URL	Enter the path to the Active Directory in your network using LDAP syntax. LDAP is case sensitive, and the URL must contain a forward slash after the port to be valid. For example: LDAP://server1.sopheon.com:389/.
Search Distinguished Name	Enter the attributes separated by commas that make up the distinguished name in Active Directory that defines users. For example: OU=Sopheon Users, DC=Sopheon, DC=com. This example includes the organizationUnitName and domainComponent attributes. The distinguished name is set of attributes you have chosen to identify users.

5. Click **Apply** to save your changes.
6. Continue with the next procedure to complete the required mapping to active directory attributes.

To map Accolade fields to objects in the Active Directory structure:

1. Ensure that the **Active Directory Enabled** parameter is set to **1** in the Administration Console.
2. Within Accolade, from the **System** menu, select **System > Active Directory**.
3. Click the plus next to the Active Directory server you want to map.
4. In the **Row Value** column, enter the attribute name from Active Directory that corresponds to each **Row Label**. The mapping created using these fields determines which attributes are matched to map users between Accolade and the Active Directory.

Note: The **Domain** option is an actual value that is used to create the user login and is not a mapping option. It is concatenated with the **Row Value** for **Login** to create the user login.

5. Any extended field that has the **AD Sync** check box selected is also available to map data to from Active Directory. Map those fields, as necessary.
6. Click **Apply** to save your changes.

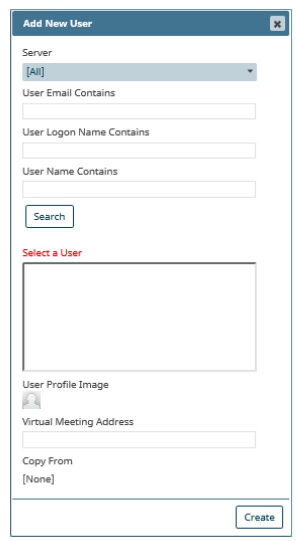
> **Notes:**
>
> - To sync Active Directory with Accolade, the user must have at least read-only rights to the configured domains on the server and be an Accolade user with the Service Account role.

Creating User Accounts from Active Directory

When you add a user using Active Directory, Accolade imports the user information such as the user's name and email address from the Active Directory objects you indicated when you mapped the Active Directory server to fields within Accolade.

Prior to creating users in Accolade using Active Directory:

- Define the users within the Active Directory. After Active Directory is enabled in Accolade, you can only add user accounts that are defined within Active Directory.
- Create and map the Active Directory server within Accolade.



To add a user account from Active Directory:

1. From the **System** menu, select **Collaboration & Groups > User Admin**.

   The current list of users displays.
2. Click to display the Add New User dialog box.
3. In the **Server** field, select the Active Directory in which you want to search for the user.

   To search all servers you have defined, select **All**.
4. Enter any or all of the following as it exists in the Active Directory and click **Search** to search the domain for the user:

Field	Description
User Email Contacts	Enter any part of the user's corporate email address.
User Login Name Contains	Enter any part of the name the user uses to log on to your network.
User Name Contains	Enter any part of the user's user name.

Users matching the information you entered display in the **Select a User** list.

5. Select the user in the list to add.
6. In the **Chat Address** field, enter the user's address for your selected chat tool.

   This can be the same or different than the user's standard email address.
7. *(Optional)* If the **Enable User Profile Images** system parameter is enabled, add a user profile image that displays along with the user's name in various locations within Accolade, click  next to the user name, click **Choose Image**, navigate to and select the image to add, and click **Upload Image**. To remove a profile image, click the image next to the user name and click **Remove**.

   To display as an image within Accolade, an image file must be one of the following file types: .bmp, .dib, .gif, .jpg, .jpeg, .jpe, jfif, or .png.
8. *(Optional)* In the **Copy From User** field, select the user whose configuration details you want to copy to this user.

   Copying configuration details from existing users allows you to assign most of the details automatically, and only make a few changes to the user, and helps to ensure that users that you want to have the same permissions are set up identically. For example, you may have a set of Process Managers in your organizations that all receive the same configuration. Create one, and then copy the configuration to all others.
9. Click **Create** to create the user account.

Notes:

- The users that exist in Accolade prior to enabling Active Directory and running a sync are not removed from Accolade if they do not exist in the Active Directory when a sync runs.
- After Active Directory is enabled, you cannot change the values in the fields for any user within Accolade, such as the users email address.
- To import users, disable Active Directory, run the import, and then re-enable the Active Directory functionality.

Synchronizing Users with Slack Integration

To synchronize users with Slack, you must first have configurations set in Slack and a valid token provided by Slack. The Slack bot token is needed when setting the Slack integration in Accolade. If a Slack user identification changes, you can resynchronize a user.

When configuring the Slack integration in Accolade, note the following:

- The token field is required.
- If the Slack token is changed, the integration will not work and needs to be updated in Accolade.
- When populating the chat address in Accolade, use the Slack prefix with user ID. All Slack user

IDs need to have the Slack prefix. For example: SLACK:A1B2

- Accolade and Slack email addresses need to be the same.

To resynchronize a user:

1. In Accolade, from the **System** menu, select **Collaboration & Groups > User Admin**.
2. Select the user from the list.
3. In the **General Details** tab, add the email address and the chat address.
4. Click **Save**.

Company Functions Overview

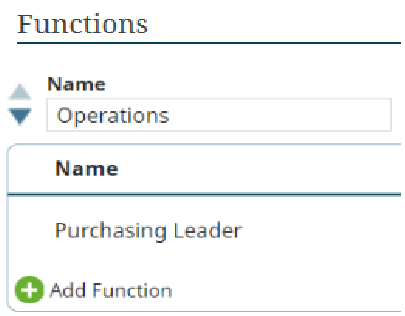
A function is a label that helps identify the type of specialist within your company who should own a deliverable, activity, workflow action, or gatekeeper position in a project. Within process models, Process Designers can select a function to identify the default functional owner of deliverables, activities, workflow actions, or gatekeeper positions that make up the model. When defining a project team within a project, the Project Manager or a Process Manager can select which user assigned to the function is a member of the project. That user is automatically assigned to all the documents that have that function assigned in the project, streamlining the assignment creation process.

Functional areas serve as categories to sort functions into logical groups and typically reflect departments within your company: Engineering, Marketing, Manufacturing, and so on. Functional areas can be as large or as granular as what fits your company's needs. Functions typically reflect job titles or positions that fall within a functional area. For example, a functional area of Engineering could have functions defined for Electrical Engineer, Mechanical Engineer, and Chemical Engineer.

Note: Although functional areas and functions typically reflect departments and job titles or positions within your company, you can use them to identify users in other classifications.

EXAMPLE Example

Company A has a functional area defined for Operations, which includes members of its purchasing department. Within the Operations functional area, there is a function defined called Purchasing Leader.



Company A requires Purchasing Leaders to gather Non-Disclosure Agreements (NDAs) from parts vendors during the first phase of any project that requires manufacturing. A Process Designer defines a process model to use for manufacturing projects that contains a deliverable in the first stage called Vendor-NDA. The Vendor-NDA deliverable indicates the Purchasing Leader as the function assigned.

Within a project based on the process model, the Process Manager or Project Manager assigned to the project can select the employee assigned to the Purchasing Leader function to add to the project team. Within the deliverable assignments for the Vendor-NDAs with the project, the user list now includes the team member selected for the Purchasing Leader function as owner of that deliverable.

Creating Functional Areas and Functions

Functions and functional areas help identify the type of specialist within your company that owns a deliverable, activity, workflow action, or gatekeeper position in a project. A function typically identifies users by the user’s job title or position within a functional area; however, you can use them to categorize users as you see fit for your company.

To create a functional area:

1. From the **System** menu, select **Collaboration & Groups > Functions**.
2. Do one of the following:
   - **To add a new functional area** - Click **Add Functional Area** in the lower right corner of the page.
   - **To edit an existing functional area** - Click the field within the area that you want to edit.
3. Complete the following information:

   Required fields display with **red** text and an asterisk * if the field is empty.

Field	Description
Name	Enter a name, up to 64 characters long, which identifies the functional area.
System Name	Enter a unique, shorter name that identifies the functional area in queries, reporting views, field codes, and other places in Accolade.

Field	Description
	The name must be unique among functional areas and can contain only letters (English alphabet), numbers, and the underscore.
Order	Click on the arrows near the area's name to adjust its order. The areas will display in other locations in the same order that you arrange them on this page.

4. Click **Apply** to save your changes.

To create a function within a functional area:

1. From the **System** menu, select **Collaboration & Groups > Functions**.
2. Click **Add Function** in the lower left corner of any functional area and complete the following information:

Field	Description
Name	Enter a name that identifies the function.
System Name	Enter a unique, shorter name that identifies the function in queries, reporting views, field codes, and other places in Accolade. The name must be unique among functions and can contain only letters (English alphabet), numbers, and the underscore.
Functional Area	Select the functional area in which this function is categorized. For example, if you are creating a function for Mechanical Engineer, the functional area might be Engineering.
Order	Enter a number to specify the function's place when it displays within a list of functions. Lower numbered functions display higher in the list. This also determines the order of functions listed for a project team on the project's Team page. If no order is specified, the function is added to the top of the list within the assigned functional area.
Members	Click to select the user(s) to assign to this function. To filter the list of users, enter one or more search criteria to filter by name, login name, email address, function, or extended field. • Clicking **Select current user** will assign the role to the current user (if they have the appropriate rights). • Selecting a **Function** in the drop-down will display available users that are assigned to the function. The current selection defaults to the function to which you are assigning a user, however depending on the project configuration, you can assign any user.

Field	Description
	• Clicking the **Show advanced filters** check box displays or hides the additional filter options. • Clicking **Clear** removes the current user assignment and displays **[None]** to indicate that no user is assigned. Highlight the user name(s) in the Available Users window and click **Select**, or double-click each user's name to move them from the **Available** list to the **Selected** list.

3. Select the **Active** check box when the function is ready to use in projects.
4. Click **Apply** to save your changes.

Notes:

- To delete a function, click the ⊗ at the end of the function's row, and click **Apply** to save your change. If the function is in use, you can select the function that replaces the one you are deleting when prompted to move the users into the selected function. Select **None** to manually move users to a different function and manually modify document assignments, as necessary.
- To delete a functional area, click **Delete Functional Area** on the upper right corner of a functional area. Any functions within the functional area are moved to the Default functional area when you confirm the deletion.

Merging Functions Together

If you find that you have duplicate or unnecessary job functions, merge the users from one function into another function. After the users are merged into one function, the system deletes the original function.

To merge a function into another function:

1. From the **System** menu, select **Collaboration & Groups > Functions**.

   The current list of functions displays both by display name and system name.

2. Select the check boxes in the **Merge** column next to one or more functions that you want to merge.
3. Select one check box in the **Merge To** column to identify the function that you want to merge the other functions into.
4. Click **Apply** to merge the users in the merge from function to the merge to function.

   The functions selected to merge *from* are removed from Accolade.

Exercises - Grouping Users by Company Function

Try out what you have learned!

- Create a functional area called Marketing.
- Within the Marketing functional area, create two functions of your choice. For example, Marketing Lead, Marketing Associate, etc.
- Assign the user you created in previous exercises to the one of the Marketing functions.

Sopheon Corporation

6870 West 52nd Avenue, Suite 215

Arvada, CO 80002