



---

# Sopheon Accolade<sup>®</sup>

## Administration - Information Security Training Guide

Version: 17.1



## About Sopheon Accolade®

**Document Name:** Administration - Information Security Training Guide  
**Document Version:** 1  
**Software Version:** Sopheon Accolade 17.1  
**Document Date:** November 2024

## Ownership of Software and Documentation

The Sopheon® software described in this documentation is furnished under a license agreement and may be used only in accordance with the terms of that license agreement.

Sopheon Corporation and its associated Sopheon Group companies, including its subsidiaries, its immediate holding company and its ultimate holding company (together, "Sopheon") have created and own all rights to the software and documentation. Licensees of the software have purchased a limited right to use the software in accordance with their license agreement.

## Copyright Notice

All materials in this documentation or in the software, including software code, pages, documents, graphics, audio and video, are copyright © 2024 Sopheon. All rights reserved.

Certain Sopheon software modules incorporate portions of third party software, and the copyright of the authors of such third party software are hereby acknowledged. All rights reserved.

All the information on this documentation is proprietary and no part of this publication may be copied without the express written permission of Sopheon.

## Trademarks

"Accolade", "Sopheon", and the Sopheon logo are registered trademarks of Sopheon. "Vision Strategist", the Vision Strategist logos, "Idea Lab", and "Process Manager" are trademarks of Sopheon. A more complete list of Sopheon trademarks is available at [www.sopheon.com](http://www.sopheon.com).

"Microsoft", "Windows", "Excel", "PowerPoint" and "Microsoft Teams" are registered trademarks of Microsoft Corporation. A complete list of Microsoft trademarks is available at [www.microsoft.com](http://www.microsoft.com). "Lotus Notes" is a registered trademark of International Business Machines Corporation. "WinZip" is a registered trademark of WinZip Computing, Inc. "Stage-Gate" is a registered trademark of the Product Development Institute. Other product names mentioned in this Help system may be trademarks of their respective companies and are hereby acknowledged.

"Slack" is a registered trademark of Salesforce Technologies, LLC.

Names of persons or companies and other data contained in examples set forth in this user documentation are fictitious unless otherwise noted.

## No Warranty

The technical documentation is being delivered to you AS-IS, and Sopheon makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Sopheon reserves the right to make changes without prior notice. In no circumstances will Sopheon, its agents or employees be liable for any special, consequential or indirect loss or damage arising from any use of or reliance on any materials in this documentation or in the software.

## Patents

Aspects of Sopheon software are protected by U.S. Patents 5634051, 6632251, and 6526404; European Patent EP0914637; and by U.K. Patent GB2341252A.

# Contents

<b>About the Accolade Education Program .....</b>	<b>5</b>
<b>Prerequisites for Using this Module .....</b>	<b>6</b>
<b>Information Access and Security Overview .....</b>	<b>7</b>
<b>Access Groups Overview .....</b>	<b>7</b>
Access Group Best Practices .....	8
Information Security Examples .....	9
Designing the Access Group Hierarchy .....	10
Creating Access Groups .....	13
Granting Access Group Permissions to Users .....	13
Restricting Configuration via Access Groups Overview .....	17
Restricting Configuration for Classes .....	17
Restricting Configuration for Process Models .....	18
Restricting Configuration for Gate Documents .....	19
Restricting Configuration for Layouts .....	19
Restricting Configuration for Deliverables and Activities .....	21
Restricting Configuration for Metrics .....	21
Restricting Configuration for Matrices .....	22
Restricting Configuration for Templates .....	23
Restricting Configuration for Quick Grids .....	24
Restricting Configuration for Workflows .....	24
Restricting Configuration for Functions .....	25
Restricting Configuration for Charts and Reports .....	26
Reporting on Access Group Contents .....	27
Reports created using the Accolade Office Extensions add-in and Accolade Online Reports ..	27
Query in an HTML Report .....	27
Deleting Access Groups .....	27
<b>Security Lists Overview .....</b>	<b>28</b>
Building Security Lists Using Reference Tables .....	29
Creating the Spreadsheet File .....	30
Adding the Reference Table to Accolade .....	31
Building Security Lists Manually .....	32

Assigning Users to Security Lists .....	35
<b>Security Profiles Overview .....</b>	<b>36</b>
Security Profiles Best Practices .....	37
Creating Security Profiles .....	37

# 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
<i>Sopheon Accolade What's New in This Release</i>	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.
<i>Sopheon Accolade Administrator's Guide</i>	Provides information for administrative professionals regarding Accolade setup. This information is also provided in the online Help.
<i>Sopheon Accolade Installation Guide</i>	Provides information about the installation of the application and its required databases.
<i>Dashboards for Accolade Installation Guide</i>	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

---

**Important!** The contents of this training module assumes that you have had extensive discussions internally and with Sopheon implementation personnel about the access requirements and security needs at your company. After having those discussions, or to make changes to security settings within your implementation, continue with the contents of 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

- Your internal information access strategy

### Related Training Modules

- User Administration

# Information Access and Security Overview

Accolade offers several methods to secure the data within it. You can use any or all of the following security methods to define the security layers that are appropriate within your company.

- **Access Groups** - Access groups are containers that determine what information users can access and is assigned to users, process models, projects, reference tables, and planning elements in Accolade Innovation Planning. The access groups hierarchy does not control navigation rights to go to the project or visibility within the project if the user is part of the project team, including gate owners and gatekeepers. See ["Access Groups Overview" on page 7](#).
- **Security Lists** - Security lists are hierarchical lists of different object types that control access to projects and unowned resource pools. See ["Security Lists Overview" on page 28](#).
- **Security Profiles** - Security profiles define project access based on classes and metric values associated with a project and a user. See ["Security Profiles Overview" on page 36](#).

In addition, you can use user roles, such as the Restricted Team member user role to limit the information that a user sees within a project, and the system as a whole. User roles determine the kinds of tasks users are allowed to do by controlling which pages they can open and what they can see on those pages.

## Access Groups Overview

An access group is a container that determines what information users can access. Access groups can be assigned to all areas of a project, including classes, process models, projects, reference tables, layouts, metrics, templates, quick grids, and planning elements in Accolade Innovation Planning. Access groups operate in combination with security lists and security profiles. If your company uses security lists, then users must have access to both access groups and security lists to have access to project information.

Access groups restrict project and information access in the following areas:

- Reporting in Accolade Office Extensions and Accolade Online Reporting
- Upcoming Gates
- Reference Tables
- Planning Elements in Accolade Innovation Planning
- Portfolio Optimizer Scenarios
- Classes
- Process Models
- Layouts
- Deliverables and Activities
- Metrics

- Matrices
- Templates
- Quick Grids
- Workflows
- Functions
- Search

**Note:** A user still has access to a project through search if the user is a member of the project team, even if the user does not have access group access.

These areas only display project data for access groups to which a user belongs. The access group settings in a user's account must match the settings for a project, reference table, or planning element for information access. However, an access group assignment does not restrict who can be added a project team, unless the **Enforce Project Security for Add Team Member** system parameters is enabled



## Access Group Best Practices

Keep the following set of best practice recommendations in mind when designing the access groups structure:

- **Design Early** - The access groups hierarchy design is a critical process and should happen early in the Accolade implementation. Changing the hierarchy after a large number of users and projects are entered into the system can be a time-consuming process.
- **Keep it Simple** - Keeping the structure simple makes it easier to assign users and projects correctly and efficiently. It minimizes unintended denials of information, and is easier for other administrators to understand the system.
- **Limited Use of Root Access Group** - Assign few or no users to the **Root** access group. Keeping the Root group sparsely populated reduces maintenance in case you decide to redesign the groups structure or to add restricted groups high in the hierarchy.
- **Restricted Users** - Create a special group for Restricted Team Members and do not add any projects to it. All users must be assigned to at least one access group. Because users still have access to projects to which they are assigned, assign users with the Restricted Team Members role to this access group.
- **Idea Project** - Create a special group for the initial assignment of all idea projects. (Deprecated) Idea Managers can re-assign promising ideas to other groups after the initial evaluation.
- **Automate the Access Group Assignment** - Create a calculated metric that automates a project's access group classification. Using a metric at the model level allows you to make a project more or less secure based on a metric's value.
- **Restrict Access Group Assignment at the Process Model Level** - To help ensure that portfolios and other projects are created in the correct access group, set restrictions on where projects created using a model can exist. Without restrictions, Process Managers and



(Deprecated) Idea Managers can create and move projects to the access groups that are assigned to their user. With access group restrictions, they can only create and move projects to the access groups that are assigned to their user that are also part of the restricted list.

- **Tests and Training** - Create a special group for test projects and training new employees. This allows users to learn and experiment in Accolade without mixing practice and training projects in with real, ongoing company projects.
- **Project Assignments** - Whenever possible, assign users to projects within their access group assignments. Users can still participate in projects outside those access group when assigned on the project. For example, as a Document Reviewer.

## Information Security Examples

Consider the following information security examples as you are planning the security framework at your company.

- Using the Restricted Team Member role and the access groups tree, you can set up several different levels of information security in your projects. For example, use the access groups hierarchy to restrict the information in some projects to project members only while making the information from other projects available to everyone.
- Using the Restricted Team Member role to prevent users from seeing any information other than the deliverable and activity pages that they own. They cannot see other projects, other team member assignments in their own projects, or other project information available.
- Assigning Project Team Members and Project Managers to an access group that contains no projects and has no children that contain projects, restricts those users to accessing only the project pages of projects to which they are assigned. They cannot search for any projects or documents. They can see all the deliverables and activities in their own projects, but none in other projects.
- Assigning Project Team Members and Project Managers to an access group that contains their own project but that has no children, allows them to search for documents in their own projects only. They can access deliverables in their own project both through Search and through the Project pages, but they cannot see other projects.
- Creating all access groups as children of the Root access group and assigning Project Team Members and Project Managers only to projects in their own group allows these users to see and search for information in all of the projects in their group but prevents them from seeing any information from projects in any other groups.
- Assigning users to an access group that contains multiple projects or one with children that contain multiple projects, allows the users to search for and access many projects and their documents. These users can access the projects that they can see both through the Project pages and through Search.
- Assigning Process Managers, Executives, and other users who cannot be members of a project to a group that is part way down the access groups tree completely hides project information in the portions of the tree above where they are assigned. For example, a Process Manager assigned in this manner only sees a portion of the total number of projects when viewing projects through the Upcoming Gates page. Making this kind of assignment can cause unexpected

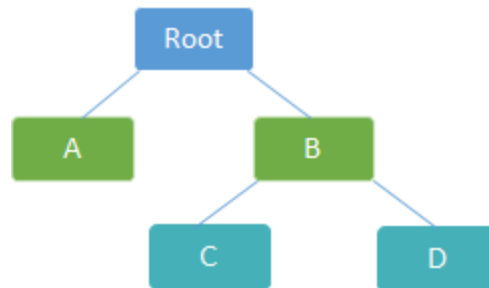
problems. For example, a Resource Planner would not see all of the projects that might be pulling resources from one of her pools.

- To give users access to all projects in Accolade, assign them to the Root access group.

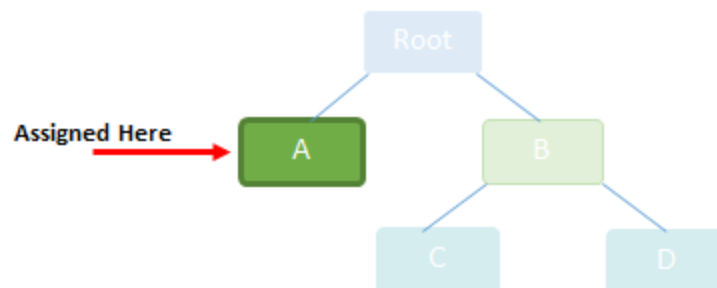
## Designing the Access Group Hierarchy

Access groups are arranged in a hierarchical tree structure. The tree determines ease of maintenance and openness of information flow. Simpler trees make it easier to provide adequate information access. Complex trees are more time consuming to maintain but offer more specific information control. The access group tree and information control is specific to your company. Use the information below to guide you in building your access group structure.

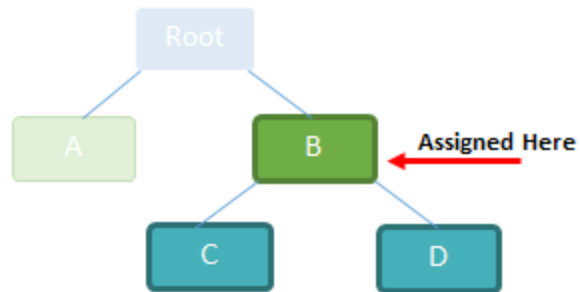
Accolade installs with a default access group called **Root**, which is always at the top of the tree. You cannot delete this group; however, you can rename it. All additional groups are either a child of **Root**, or a child of another access group in the tree. Thus, a user who is a member of **Root** has access to every project and document in the system.



Users can search for documents, projects, see links to projects, and see chart and report information about projects and reference tables that are assigned to the same access group to which the user is assigned, or an access group that is in the same branch. In the hierarchy above, a user assigned to Group A is able to access projects and information in Group A, but not access to projects and information in Groups B, C, or D.



A user assigned to access Group B is able to see information in Groups B, C, and D (because Groups C and D are children of Group B), but cannot see information in Group A.



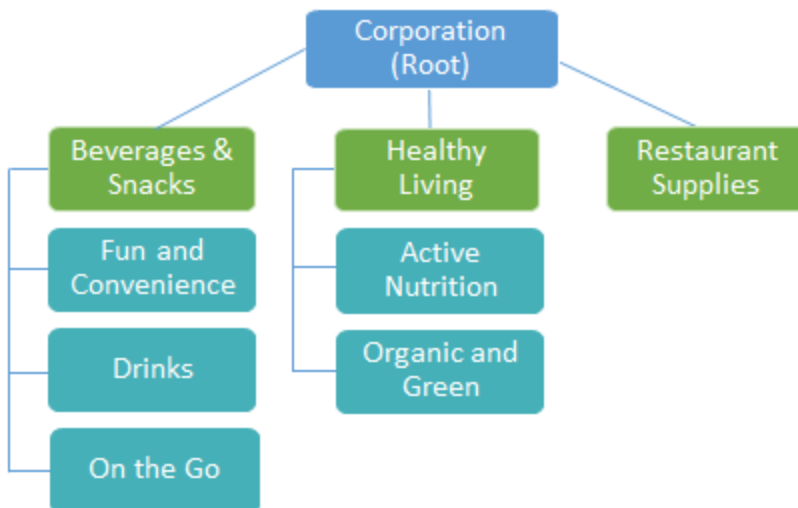
#### EXAMPLE

#### Example

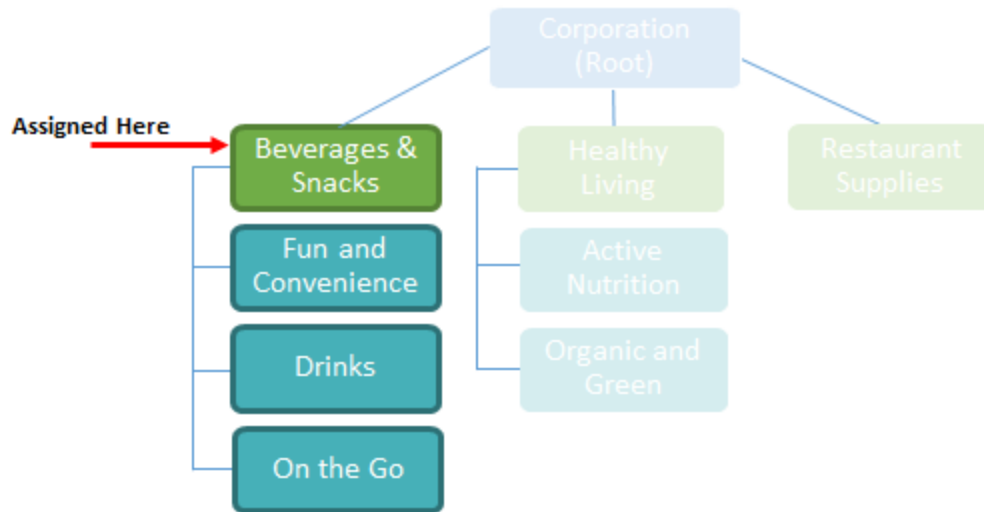
A consumer goods company has business units named for the general categories of the product types they develop, such as:

- Beverages & Snacks
- Healthy Living
- Restaurant Supplies

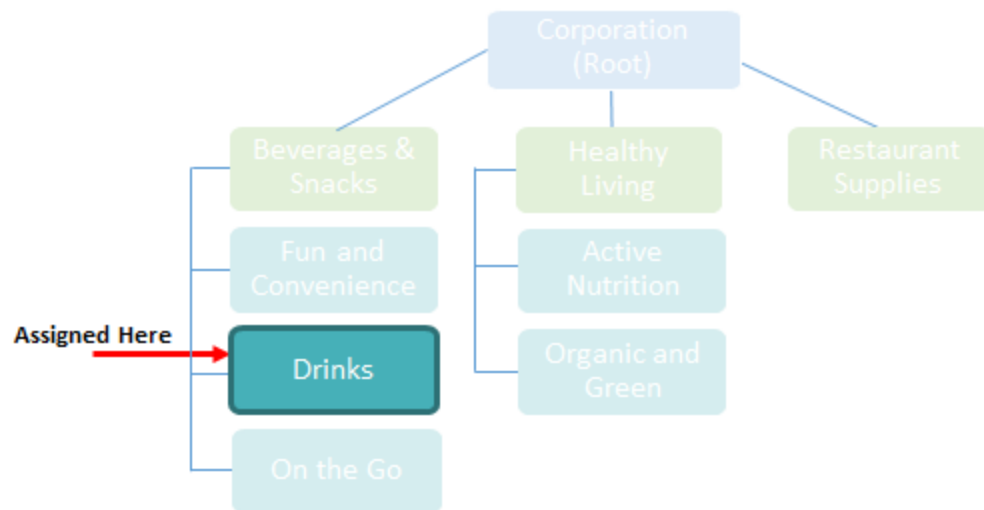
The company has created access groups named for each business unit. Optionally, a company could create access groups under each business unit representing brands within each unit. For example, in the Beverages & Snacks business unit, there are brands for Drinks, Fun and Convenience, and On the Go products.



Depending on security needs, users can be assigned at the brand level (Drinks) or at the business unit level (Beverages & Snacks). A user added to the Beverages & Snacks access group can see everything in Drinks, Fun and Convenience, and On the Go, but cannot access any projects in the Healthy Living or Restaurant Supplies business unit.



If a user is assigned at the Drinks brand level, they can access all the projects in the Drinks brand but not in the Fun and Convenience or On the Go brand.



**Note:** If Accolade Innovation Planning is enabled, a second default group, **[Innovation Planner Default]** is added as a child of **Root**. It is the group to which all planning elements are added when they are created. You cannot delete this default group; however, you can rename it, and you can assign planning elements to a different access group once they are created.

In the most open tree, everyone is assigned to **Root** and has access to all information. Or, perhaps only a few users are assigned to **Root** and a few others are in groups part way down the tree. In the later of the structure, team members can access only the information in projects to which they belong. Only a few users, such as Executives, can see project information from more than one group.

## Creating Access Groups

Access groups are arranged in a hierarchical tree that Administrators and Process Designers create in Accolade by adding groups in a nested structure.


### To create an access group:


1. From the **System** menu, select **Security & Groups > Access Groups**.

The current access group tree displays.


2. In the **Access Groups** list, select the group to which you want to add a child group.

To create the first group in a new hierarchy, select the top most group (Root).

 Based on your company's configuration, the top level group may have been named something other than Root.

3. In the upper right corner of the **Access Groups** list, click  to add a new access group.
4. In the **Name** field, enter a unique name for the new group.
5. In the **System Name** field, enter a unique system name for the new group.
6. Click **Create** to create the new group.

The new group displays in the hierarchy.

 To rename an existing group, select the group to rename in the hierarchy, update the name in the **Name** field, and click **Apply**.

## 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 **Security & 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 and inactive status from the following options:
    - **Active Users Only** - excludes inactive users.
    - **Show All Users** - displays active and inactive users.
    - **Inactive Users** - displays only users marked as inactive. Inactive status is indicated with *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
<b>Member Of</b>	<p>When checked, the user becomes a member of that particular access group.</p> <p>💡 Users must be a <b>Member Of</b> at least one access group.</p>
<b>Admin Of</b>	<p>Only enabled if the user has the Administrator role checked on the Roles and Rights tab.</p> <p>Administrators are granted create/edit ability only within the access groups for which they have <b>Admin Of</b> checked. All other rows will be disabled.</p> <p>Users with the Administrator role must be the Admin Of at least 1 Access Group. Only a root level administrator can grant a user <b>Admin Of</b> rights if they are not already an Administrator (roles and rights).</p> <p>If multiple users are selected and the editor does not select <b>Admin Of</b> for ALL users, they will appear to be read only.</p>


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 (Deprecated) 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 (Deprecated) 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
<b>Manage Team</b>	<p>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.</p> <p>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.</p>

Management Right	Description
<b>Manage Process</b>	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.
<b>Add</b>	The ability to add a new project using an existing class and model.
<b>Migrate</b>	The ability to migrate or copy a project to a different process model.
<b>Delete</b>	The ability to delete a closed project from the system.
<b>Delete Activity</b>	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
<b>Edit</b>	<p>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.</p> <p> View is automatically checked when Edit is selected.</p>
<b>View</b>	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.



---

## Exercises - Creating Access Groups



Try out what you have learned!

- Create two access groups under the Root access group.
  - Rename the Root access group to Corporation, or something that is fitting for your company.
  - Assign your user and one other user to each access group.
- 

## Restricting Configuration via Access Groups Overview

Use access groups to restrict reporting and configuration components within Accolade. Defining who can view and edit components in the system allows your company to establish corporate guardrails and mitigate risk of Process Designers accidentally making changes to items outside of their business group or division. Establishing an access group hierarchy and restricting edit rights within that hierarchy allows for configuration flexibility while still ensuring corporate standards for configuration are met.

A Process Designer might be able to view a corporate-level process model but not be able to edit it. They would, however, be able to edit components within the process model such as deliverables specific to their business unit or division. By segmenting configuration and restricting configuration edit permissions, you can ensure business units across your company follow corporate guidelines such as processes for process models while still granting autonomy at the lower division levels. When designing access group hierarchies, consider the corporate use of configuration and the local autonomy of employees that need to view and/or edit items within their business unit or division.

For example, Process Designer Sandy has access group view and edit permissions at the corporate level. She can view and edit configuration for all the business groups and divisions in the organizational hierarchy. She might set corporate standards that apply across the organization.

Process Designer Jeff can only edit requirements for his business group and the divisions below. However, he has view access group permissions for the Electronics business group and corporate configurations so he can view configurations and collaborate across the organization.

Restricting configuration components is driven by the access group assignment of the configuration component **and** the access group assignment of the user. When assigning users to access groups, assign them additional view and edit permissions within the access group.

Configuration components that respect access group restrictions include all levels of process model and reporting setup, to include classes, process models, gate documents, layouts, deliverables and activities, metrics, matrices, templates, quick grids, workflows, functional areas and functions, online charts and reports, and Accolade Office Extensions reports.

## Restricting Configuration for Classes

Restrict who can view and edit classes by assigning the class to one or more access groups. Process Designers with matching access group permissions set in their user profile will be able to view or edit the class.

**Note:** The access groups that display for selection are based on your access group permissions as defined in your user profile. Additionally, access group settings for the class must match the user permissions of other Process Designers in order to display for them.

#### To restrict class configuration:

1. From the **System** menu, select **Process > Classes**.

To narrow the class list, search by the class name, system name, or category.

2. Either select the class to edit.
3. Click the **Security** tab to display the configuration access group settings.
4. Select the access group(s) to which this class belongs.

The access group(s) displayed are based on the current user's access group permissions. Only access group(s) to which you have Edit permissions are selectable. However, parent access group information is visible for access groups to which you have View permission.

The class is selected to the highest level access group listed by default. Note that the class is only added to access groups that are checked. It does not propagate to child access groups unless those child groups are checked.

Process Designers with matching access group permissions will be able to navigate to and edit the class, depending on their individual access group permissions.

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

### Restricting Configuration for Process Models

Restrict who can view and edit process models by assigning the process model to one or more access groups. Process Designers with matching access group permissions set in their user profile will be able to view or edit process model components.

**Note:** The access groups that display for selection are based on your access group permissions as defined in your user profile and the access groups assigned to the class the model is being attached to. Additionally, access group settings on the process model must match the user permissions of other Process Designers in order to display for them.

#### To restrict process model configuration:

1. From the **System** menu, select **Process > All Models** and select the model to edit.
2. Click the **Security** tab to display the configuration access group settings.
3. Select the access group(s) to which this process model belongs.

The access group(s) displayed are based on the current user's access group permissions. Only access group(s) to which you have Edit permissions are selectable. However, parent access group information is visible for access groups to which you have View permission.

The process model is selected to the highest level access group listed by default. Note that the process model is only added to access groups that are checked. It does not propagate to child access groups unless those child groups are checked.

Process Designers with matching access group permissions will be able to navigate to and edit the process model, depending on their individual access group permissions.

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


## Restricting Configuration for Gate Documents

Restrict who can view and edit gate documents by assigning the gate document to one or more access groups. Process Designers with matching access group permissions set in their user profile will be able to view or edit the gate document.

**Note:** The access groups that display for selection are based on your access group permissions as defined in your user profile. Additionally, access group settings for the gate document must match the user permissions of other Process Designers in order to display for them.

Gate documents inherit the access group visibility assigned for the model. All deliverables and activities on the model display regardless of their individual access group assignments.

### To restrict gate document configuration:

1. From the **System** menu, select **Process > All Models** and select the model to edit.
2. Do one of the following:
  - **To add a new gate document** - In the **Component Tree** tab, click  next to the gate to add the gate document.
  - **To edit an existing gate document** - Expand the gate within the component tree and select the gate document.
4. Select the access group(s) to which the gate document belongs.

The access groups displayed are based on the current user's access group permissions. Only access group(s) to which you have Edit permissions are selectable. However, parent access group information is visible for access groups to which you have View permission.

The gate document is selected to the highest level access group listed by default. Note that the gate document is only added to access groups that are checked. It does not propagate to child access groups unless those child groups are checked.

Process Designers with matching access group permissions will be able to navigate to and edit the gate document, depending on their individual access group permissions.

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


## Restricting Configuration for Layouts

Restrict who can view and edit layouts by assigning the layout to one or more access groups. Process Designers with matching access group permissions set in their user profile will be able to view or edit the

layout.

**Note:** The access groups that display for selection are based on your access group permissions as defined in your user profile. Additionally, access group settings for the layout must match the user permissions of other Process Designers in order to display for them.

**To restrict layout configuration:**

1. From the **System** menu, select **Page Design > Layouts**.
2. Do one of the following:
  - **To add a new page layout** - Click **Add New** in the upper right corner of the page and create the layout.
  - **To edit an existing page layout** - Click the name of the layout to open it for editing.
3. In the Layout section under **Configuration Access Groups**, click  to select the access group(s) to which this layout belongs.

The access group(s) displayed are based on the current user's access group permissions. Only access group(s) to which you have Edit permissions are selectable. However, parent access group information is visible for access groups to which you have View permission.

The layout is selected to the highest level access group listed by default. Note that the layout is only added to access groups that are checked. It does not propagate to child access groups unless those child groups are checked.

Process Designers with matching access group permissions will be able to navigate to and edit the layout, depending on their individual access group permissions.

4. Click **Apply** to save your changes.
5. Click **Save** or **Save and Close** to save the layout to Accolade.



## Restricting Configuration for Deliverables and Activities

Restrict who can view and edit deliverables and activities by assigning the deliverable or activity to one or more access groups. Process Designers with matching access group permissions set in their user profile will be able to view or edit the deliverable or activity.

**Note:** The access groups that display for selection are based on your access group permissions as defined in your user profile. Additionally, access group settings for the deliverable or activity must match the user permissions of other Process Designers in order to display for them.

Deliverables and activities inherit the access group visibility assigned for the model. All deliverables and activities on the model display regardless of their individual access group assignments.

### To restrict deliverable and activity configuration:

1. From the **System** menu, select **Process > All Models** and select the model to edit.
2. Do one of the following:
  - **To add a new deliverable** - In the Model tree, click  next to the stage to add the deliverable to.
  - **To add a new activity** - In the Model tree, click  next to the deliverable to which the activity applies.
  - **To edit an existing deliverable or activity** - Expand the stage or deliverable within the Model tree and select the deliverable or activity.
3. Select the access group(s) to which the deliverable or activity belongs.

The access groups displayed are based on the current user's access group permissions. Only access group(s) to which you have Edit permissions are selectable. Parent access group information is visible for access groups to which you have View permission.

The deliverable/activity is selected to the highest level access group listed by default. Note that the deliverable/activity is only added to access groups that are checked. It does not propagate to child access groups unless those child groups are checked.

Process Designers with matching access group permissions will be able to navigate to and edit the deliverable and activity, depending on their individual access group permissions.

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

## Restricting Configuration for Metrics

Restrict who can view and edit metrics by assigning the metric to one or more access groups. Process Designers with matching access group permissions set in their user profile will be able to view or edit the metric.

**Note:** The access groups that display for selection are based on your access group permissions as defined in your user profile. Additionally, access group settings for the metric must match the user permissions of other Process Designers in order to display for them.

**To restrict metric configuration:**

1. From the **System** menu, select **Content Sources > Metrics**.
2. Do one of the following:
  - **To add a new metric** - Click **Add New** in the upper right corner of the page and create the metric.
  - **To edit an existing metric** - Click the name of the metric to open it for editing.
3. Click the **Security** tab to display the configuration access group settings.
4. Select the access group(s) to which this metric belongs.

The access group(s) displayed are based on the current user's access group permissions. Only access group(s) to which you have Edit permissions are selectable. However, parent access group information is visible for access groups to which you have View permission.

The metric is selected to the highest level access group listed by default. Note that the metric is only added to access groups that are checked. It does not propagate to child access groups unless those child groups are checked.

Process Designers with matching access group permissions will be able to navigate to and edit the metric, depending on their individual access group permissions.

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

## Restricting Configuration for Matrices

Restrict who can view and edit matrices by assigning the matrix to one or more access groups. Process Designers with matching access group permissions set in their user profile will be able to view or edit the matrix.

**Note:** The access groups that display for selection are based on your access group permissions as defined in your user profile. Additionally, access group settings for the matrix must match the user permissions of other Process Designers in order to display for them.

**To restrict matrix configuration:**

1. From the **System** menu, select **Content Sources > Matrices**.
2. Do one of the following:
  - **To add a new matrix** - Click **Add New** in the upper right corner of the page and create the matrix.
  - **To edit an existing matrix** - Click the name of the matrix to open it for editing.

3. Click the **Security** tab to display the configuration access group settings.

4. Select the access group(s) to which this matrix belongs.

The access group(s) displayed are based on the current user's access group permissions. Only access group(s) to which you have Edit permissions are selectable. However, parent access group information is visible for access groups to which you have View permission.

The matrix is selected to the highest level access group listed by default. Note that the matrix is only added to access groups that are checked. It does not propagate to child access groups unless those child groups are checked.

Process Designers with matching access group permissions will be able to navigate to and edit the matrix, depending on their individual access group permissions.

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

## Restricting Configuration for Templates

Restrict who can view and edit templates by assigning the template to one or more access groups. Process Designers with matching access group permissions set in their user profile will be able to view or edit the template.

**Note:** The access groups that display for selection are based on your access group permissions as defined in your user profile. Additionally, access group settings for the template must match the user permissions of other Process Designers in order to display for them.

### To restrict template configuration:

1. From the **System** menu, select **Page Design > Template Library**.

2. Do one of the following:

- **To add a new template** - Click **Add New** in the upper right corner of the page and create the template.
- **To edit an existing template** - Click the name of the template to open it for editing.

3. Select the access group(s) to which this template belongs.

The access group(s) displayed are based on the current user's access group permissions. Only access group(s) to which you have Edit permissions are selectable. However, parent access group information is visible for access groups to which you have View permission.

The template is selected to the highest level access group listed by default. Note that the template is only added to access groups that are checked. It does not propagate to child access groups unless those child groups are checked.

Process Designers with matching access group permissions will be able to navigate to and edit the template, depending on their individual access group permissions.


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

## Restricting Configuration for Quick Grids

Restrict who can view and edit quick grids by assigning the quick grid to one or more access groups. Process Designers with matching access group permissions set in their user profile will be able to view or edit the quick grid.

**Note:** The access groups that display for selection are based on your access group permissions as defined in your user profile. Additionally, access group settings for the quick grid must match the user permissions of other Process Designers in order to display for them.

### To restrict quick grid configuration:

1. From the **System** menu, select **Page Design > Quick Grids**.
2. Do one of the following:
  - **To add a new quick grid** - Click **Add New** in the upper right corner of the page and create the quick grid.
  - **To edit an existing quick grid** - Click the name of the quick grid to open it for editing.
3. In the Quick Grid Design section under **Configuration Access Groups**, click  to select the access group(s) to select the access group(s) to which this quick grid belongs.

The access group(s) displayed are based on the current user's access group permissions. Only access group(s) to which you have Edit permissions are selectable. However, parent access group information is visible for access groups to which you have View permission.

The quick grid is selected to the highest level access group listed by default. Note that the quick grid is only added to access groups that are checked. It does not propagate to child access groups unless those child groups are checked.

Process Designers with matching access group permissions will be able to navigate to and edit the quick grid, depending on their individual access group permissions.

4. Click **Apply** to save your changes.
5. Click **Save** or **Save and Close** to save the quick grid to Accolade.

## Restricting Configuration for Workflows

Restrict who can view and edit workflows by assigning the workflow to one or more access groups. Process Designers with matching access group permissions set in their user profile will be able to view or edit the workflow.

**Note:** The access groups that display for selection are based on your access group permissions as defined in your user profile. Additionally, access group settings for the workflow must match the user permissions of other Process Designers in order to display for them.



### To restrict workflow configuration:

1. From the **System** menu, select **Process > Workflows**.
2. Do one of the following:
  - **To add a new workflow** - Click **Add New** in the upper right corner of the page and create the workflow.
  - **To edit an existing workflow** - Click the name of the workflow to open it for editing.
3. Click the **Security** tab to display the configuration access group settings.
4. Select the access group(s) to which this workflow belongs.

The access group(s) displayed are based on the current user's access group permissions. Only access group(s) to which you have Edit permissions are selectable. However, parent access group information is visible for access groups to which you have View permission.

The workflow is selected to the highest level access group listed by default. Note that the workflow is only added to access groups that are checked. It does not propagate to child access groups unless those child groups are checked.


Process Designers with matching access group permissions will be able to navigate to and edit the workflow, depending on their individual access group permissions.
5. Click **Apply** to save your changes.

## Restricting Configuration for Functions

Restrict who can view and edit functions by assigning the function to one or more access groups. Process Designers with matching access group permissions set in their user profile will be able to view or edit the function.

**Note:** The access groups that display for selection are based on your access group permissions as defined in your user profile. Additionally, access group settings for the function must match the user permissions of other Process Designers in order to display for them.

### To restrict function configuration:

1. From the **System** menu, select **Security & Groups > Functions**.
2. Do one of the following:
  - **To add a new function** - Click  in the lower left corner of any functional area and create the function.
  - **To edit an existing function** - Click on the function field you want to edit.
3. To configure access groups, click on the function's access group cell to open a dialog where the function's access group(s) may be edited.
4. Select the access group(s) to which this function belongs.

The access group(s) displayed are based on the current user's access group permissions. Only access group(s) to which you have Edit permissions are selectable. However, parent access group information is visible for access groups to which you have View permission.

The function is selected to the highest level access group listed by default. Note that the function is only added to access groups that are checked. It does not propagate to child access groups unless those child groups are checked.

Process Designers with matching access group permissions will be able to navigate to and edit the function, depending on their individual access group permissions.

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



## Restricting Configuration for Charts and Reports

Restrict who can view and edit configurable Accolade charts and reports by assigning the chart or report to one or more access groups. Process Designers with matching access group permissions set in their user profile will be able to view or edit the chart or report.

**Note:** The access groups that display for selection are based on your access group permissions as defined in your user profile. Additionally, access group settings for the chart or report must match the user permissions of other Process Designers in order to display for them.

### To restrict online charts and reports configuration:

1. From the **System** menu, select **Content Sources > Charts & Reports Manager**.
2. Do one of the following:
  - **To add a new chart or report** - Click **Add New** in the upper right corner of the page and create the chart or report.
  - **To edit an existing chart or report** - Click the name of the chart or report to open it for editing.

 You must either be an owner of the existing chart or report, or it must be set as **Available to Configuration** in the **Shared Charts & Reports** section.
3. Under **Configuration Access Groups**, click  to select the access group(s) to which this chart or report belongs.

The access group(s) displayed are based on the current user's access group permissions. Only access group(s) to which you have Edit permissions are selectable. However, parent access group information is visible for access groups to which you have View permission.

The chart or report is selected to the highest level access group listed by default. Note that the chart or report is only added to access groups that are checked. It does not propagate to child access groups unless those child groups are checked.

Process Designers with matching access group permissions will be able to navigate to and edit the chart or report, depending on their individual access group permissions.
4. Click **Save** to save your changes.

## Reporting on Access Group Contents

An access group is assigned to users, projects, reference tables, and planning elements in Accolade Innovation Planning. Use a report to determine if an access group currently contains any of the items listed above.

Knowing an access group's contents can help you better understand an existing access group structure, or to identify items that need moving prior to deleting an access group.

See the online Help for information about using the Accolade reporting tools.

## Reports created using the Accolade Office Extensions add-in and Accolade Online Reports

Using the Access Groups subject, add the following columns:

- Access Group Name
- Project Name
- User Name
- Table Display Name

## Query in an HTML Report

Create SQL queries that select columns from the following reporting views:

- **RVP\_ProjectsByGroup** - Select the ProjectName and AccessGroupName columns to return information about the projects assigned to an access group.
- **RV\_ReferenceTables** - Select the RTableName and RTableAccessGroup columns to return information about the reference tables assigned to an access group.
- **RV\_UsersByGroup** - Select the UserID and AccessGroupName columns to return information about the users assigned to an access group.

Include the **ParentGroupName** column in any of the above reporting views to also select the parent group's name.

## Deleting Access Groups

You can delete an access group if it does not contain any configuration items (process model, layout, metric, ...) in the access group hierarchy. As an Administrator, you can move users and reference tables to a different access group and delete empty child access groups. However, a Process Manager must move projects to a different access group. A Process Designer or someone with Root access group permission must move process models to a different access group.

An access group may be deleted while referenced in a snapshot; however, when the access group is deleted it is also deleted from the snapshot.

To determine what is currently assigned to an access group, see ["Reporting on Access Group Contents" on page 27](#).

### To delete an empty access group:

1. From the **System** menu, select **Security & Groups > Access Groups**.  
The current access group tree displays.
2. In the **Access Groups** list, select the group to delete.  
Select the lowest child of the access group, or the group itself if it has no children.  
The name of the selected group displays in the **Name** field in the Access Group editor.
3. Click **Delete** to remove the access group.

## Security Lists Overview

Security lists are hierarchical lists of different object types that control access to projects and unowned resource pools. Security lists grant access based on matches between security list selections in a user account and security list selections in projects and resource pools. Security lists manage access based on a combination of factors rather than just on the structure of the access groups tree. Accolade supports the definition of up to five security lists, with a maximum of 10 levels in each list.

Security lists prevent the following:

- Users without access from seeing or navigating to project data in Upcoming Gates, Charts and Reports, or in optional components such as Accolade Portfolio Optimizer, Dashboards for Accolade, Accolade Innovation Planning, and the Accolade Office Extensions add-ins
- Users without access from linking to a related project to which they do not have access.
- Process Managers without access from managing projects to which they have Manage Process rights.
- Resource Pool Administrators from seeing or creating pools that are outside their scope of access.
- Resource Planners without access from seeing and modifying demand on resource pools they do not own.
- Resource Planners without access from modifying capacity.

Users can still access projects of which they are a member of the project team through All My Work, My Project, and through Search, regardless of their security list settings. Project members not assigned to the project cannot search for project data or refresh Accolade Office Extensions reports on their projects.

If security lists are enabled, the combination of both access groups and security lists controls access to projects. User settings for both access groups and security lists must match those set for a project for users to have access to that project. To base access primarily on security lists, you can give most users high level access or even access at the Root level within the access groups. However, because security lists do not affect the management rights of Process Managers and (Deprecated) Idea Managers or access to data in Reference Tables, the access groups must be developed at least to the level at which you want to define these rights.

**Note:** Security lists do not control access to reference tables, and they do not affect the management rights of Process Managers and (Deprecated) Idea Managers. Access groups control access for these roles.

Once defined, security lists are assigned to user accounts, projects, and resource pools.

#### EXAMPLE Example

A user with Paris selected in the hierarchy below could see reports on projects that also had Paris selected as long as the user and project also had the same check boxes selected in the other security lists in the system.



But this user could not search for projects in Dijon, Asia, or in projects that only had France selected.

Note also that check boxes that are filled in ☒ do not provide access. They indicate that one or more of their child items are selected.

Combine the settings from multiple security lists to create a more intricate security framework. For example, one security list could define sales territory as in the example above. A second security list could define products by division, product type, and brand. Access to project information would be based on a combination of location and product responsibilities.

Security list selections are available throughout the system to grant access to projects, resource pools, or planning elements in Accolade Innovation Planning.

## Building Security Lists Using Reference Tables

Administrators and Process Designers can create security lists manually or by using a reference table for each list.

To build a security list using a reference table, complete the following tasks:

- Create a spreadsheet file containing the security list information.
- Add the file to Accolade as a reference table.

See ["Building Security Lists Manually" on page 32](#) if you are an Administrator and prefer to build security lists manually.

## Creating the Spreadsheet File

Each reference table can contain one security list. Accolade supports up to five security lists, with a maximum of 10 levels in each list.

Create a spreadsheet file titled **SGM\_SecurityList\_<number>** that includes a worksheet named **SGM\_RefTableSheet** which contains the security list data and meets the requirements and specifications. Column headings are in the first row of the worksheet.

---

**Important!** The columns in the spreadsheet ***must be*** present and in the order listed for the security list to upload successfully.

---

Component	Requirements
<b>ID</b>	Enter a unique ID that identifies the item in the security list. IDs can include letters (English alphabet), numbers, and the underscore.
<b>ParentID</b>	Enter the ID number of this item's parent item. The parent is the item in the list hierarchy that this item appears to be contained in. <ul style="list-style-type: none"><li>• The top item in the security list, which is the root item of the list, must have an empty cell in this column. If you were to create a second item with an empty cell in the <b>ParentID</b> column, you would create two separate lists.</li><li>• For every value that exists in the <b>Parent ID</b> column, there must exist an item that has that value in its <b>ID</b> column.</li></ul>
<b>Name</b>	Enter this item's name as it should appear in the displayed list hierarchy. This is the item's label within Accolade.
<b>Level</b>	Enter an integer specifying this item's level in the list hierarchy. The level numbers specify the parent-child relationship in the hierarchy. <ul style="list-style-type: none"><li>• There should be one item at the top level that is equivalent to the root level. This item should have level 1, and when this top level is selected, all levels are selected.</li><li>• Each level should only have one associated level name.</li></ul>
<b>Level Name</b>	Enter the name of the type of items that should be in this level.  The level name is not displayed in the security hierarchy. It is used by the table owner who maintains the reference table as a reminder to enter consistent and appropriate items in each level.



## Example

	A	B	C	D	E
1	ID	ParentID	Name	Level	LevelName
2	Geography		Geography	1	Geographical Location
3	Asia	Geography	Asia	2	Continent Name
4	Europe	Geography	Europe	2	Continent Name
5	France	Europe	France	3	Country Name
6	Dijon	France	Dijon	4	City Name
7	Paris	France	Paris	4	City Name
8					

SGM\_RefTableSheet

Note the following in the example above:

- This example builds the list under a root list of Geography as follows:



- The column headings in order from left to right, on the first row of the worksheet. The worksheet is named **SGM\_RefTableSheet** and is loaded to Accolade as **SGM\_SecurityList\_1**.

## Adding the Reference Table to Accolade

After creating the worksheet with the security list information, save the file and add it to Accolade as a reference table.

Keep the following in mind when uploading the reference table to Accolade:

- Security list reference tables must have a **System Name** of **SGM\_SecurityList\_<number>** where <number> is 1 to 5. For example, "SGM\_SecurityList\_2", "SGM\_SecurityList\_3", and so on.
- The reference table display name is used as the list's name where the list is displayed within Accolade.

After a reference table is added to Accolade, its table owner can then upload later versions to maintain the contents of the table.

### Notes:

- If projects already exist and you change the access value to a value other than the default, after uploading the security list reference table, also run a project import for the existing projects, specifying the values to set in the **Security List** data columns for those projects.

## Building Security Lists Manually

Administrators can create security lists manually or using reference tables. How you choose to create security lists is up to you. The procedure below provides instructions to manually build security lists. See ["Building Security Lists Using Reference Tables" on page 29](#) if you prefer to use reference tables.


Each security list contains a Default level, which provides access to the entire list. The additional levels that you define within the list are its primary categories. For example, in a list based on geography, the levels might be Country, Region, and City.

As you add security lists to your system, consider the following:

- User accounts have no security list options selected. Administrators must set security access for all users.
- Existing projects have all security list options selected. Process Managers and Project Managers must clear check boxes to limit access appropriately.
- Resource Pools have no check boxes selected. Resource Pool Administrators and Administrators must select security list options to grant Resource Planners, Resource Planners, and other users the appropriate access.


Accolade supports the definition of up to five security lists, with a maximum of 10 levels in each list.

### To build a security list manually:

1. From the **System** menu, select **Security & Groups > Security Lists**.
2. Click  to activate the security list you want to define.  
By default, all security lists are inactive.
3. Enter the following information to identify the security list:


Field	Description
<b>Name</b>	Enter a name, up to 64 characters long, which identifies the security list.
<b>System Name</b>	<i>(Read Only)</i> Displays the system name of the list selected.
<b>Active</b>	Select the check box when the security list is ready to use. If list is inactive, the levels information will not be displayed in the security list tree.
<b>Levels</b>	<b>Level 1:</b> Enter the description name of the first level in the security list. This will be the highest level of access within the security list. Displays <b>Default Access</b> as a default.



Field	Description
	<p>Once the first level is created, Click  to add additional level description names to the security list.</p> <p><b>Note:</b> All security lists must contain a minimum of one level, and have a maximum of 10 levels on one security list.</p>

4. Click **Done** to save changes to the security list details.

5. To enter levels and categories:

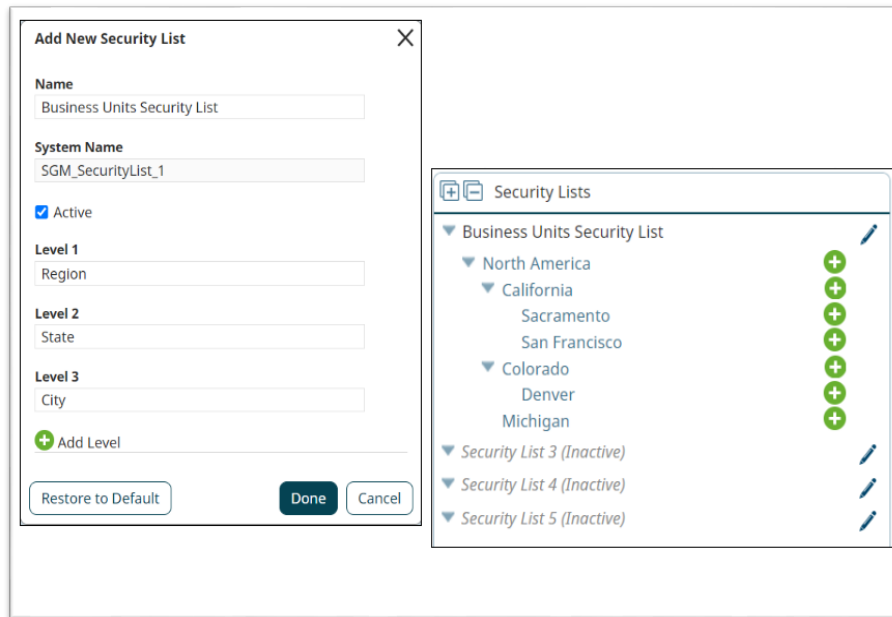
- Under the security list just created, click the **Default Access** to open the list editor. In the **Name** field, enter the name to define this parent node.
- To enter additional levels or entries in the security list tree, click  to the right of the node. This will add a new entry to the level below it.
- To add children levels, click on the **Children** field and enter the name of the child. Press **Enter** to continue add additional child levels to this node.

**Note:** Children categories can only be deleted prior to clicking **Apply**. Once saved, they are considered "in use" and cannot be deleted.

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



#### **EXAMPLE**

A user wants to manage their Accolade projects by managing their business units access within a security list. The business is within North America, in the states of California, Colorado, and Michigan. There are different operations areas in California and Colorado that will need to have separate access.





In the example above:

- There are 3 distinct levels defined in the business - Level 1 (Region), Level 2 (State), and Level 3 (City).
- Level 1 is the highest access level. It is defined as the Regional level, and in the system it is named North America.
- Level 2 is the next access level down. It is defined as the State level, and in the system it contains the entries California, Colorado, and Michigan.
- Level 3 is the lowest access level in the example. It is defined as the City level, and in the system it contains the entries Sacramento, San Francisco and Denver.

Remember that additional levels and/or entries can be added by clicking  on the security list tree, and entries are added beneath the level clicked. So for example, if the user wanted to add Detroit to the City level under Michigan, they would click  to the right of the Michigan entry.

#### Notes:

- To move an item up or down in the list, click an item and drag it to the new location.
- To remove a security list, click  next to the list and click **Restore to Default**. This will deactivate the list and clear all levels and nodes.
- To remove an entire heading row or an item, click  next to the heading row or item to delete. You must remove all child items before removing its parent, and entries that are already in use cannot be deleted.

# 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:

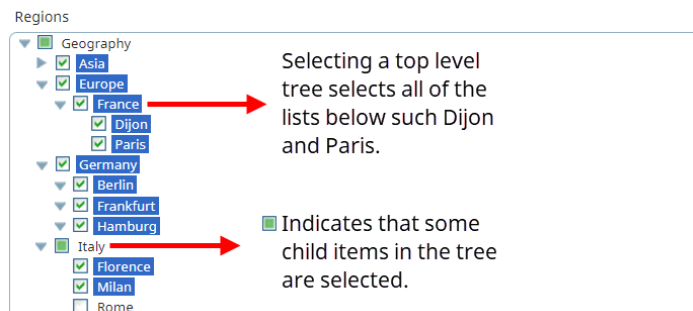
1. From the **System** menu, select **Security & Groups > User Admin**.

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 and inactive status from the following options:
  - **Active Users Only** - excludes inactive users.
  - **Show All Users** - displays active and inactive users.
  - **Inactive Users** - displays only users marked as inactive. Inactive status is indicated with *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.

---

## Exercises - Creating Security Lists



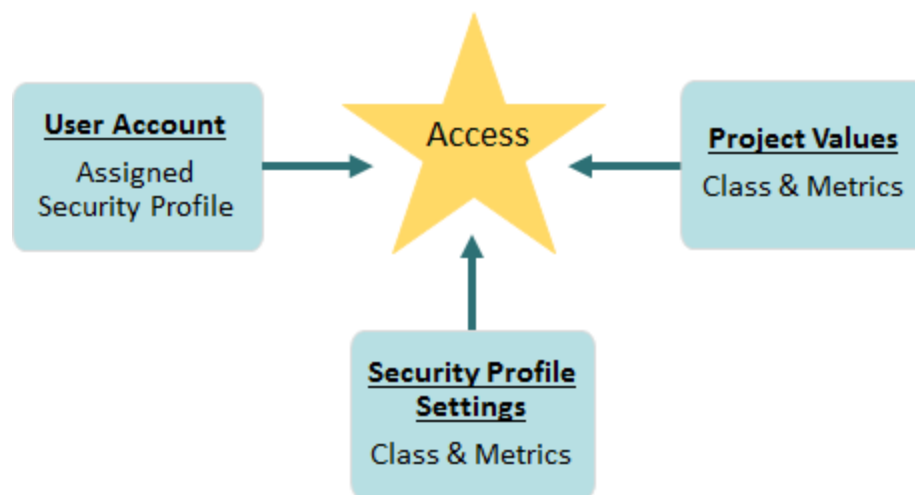
Try out what you have learned!

- Create a Security List 1 using a reference table.
- Create Security List 2 manually.
- Assign your user and one other user to each security list.

---

## Security Profiles Overview

Security profiles define project access based on classes and metric values associated with a project and a user. The class and metric value settings assigned to a project must match those assigned in the profile that is assigned to a user for the user to have access to the project information. Two users in the same access group can have access to separate sets of projects in that group using two different security profiles.



---

**Important!** A profile can distinguish user access within an access group, but cannot grant access to projects or reference tables that the access group hierarchy denies.

---

Security profiles restrict project and information access in the following areas:

- Reporting in Accolade Office Extensions and Accolade Online Reporting
- Upcoming Gates
- Reference Tables
- Planning Elements in Accolade Innovation Planning
- Portfolio Optimizer Scenarios

A security profile *does not* prevent users assigned to a project from navigating to it through All My Work or through Search. If a Process Manager is assigned as the project manager to a project that is restricted based on a security profile, the Process Manager only has the rights and permissions on the project that an assigned project manager has. The Process Manager loses all management rights for that project, except for Manage Team rights.



## Security Profiles Best Practices

Keep the following set of best practice recommendations in mind when designing security profiles for your organization:

- Use security profiles only when necessary. They can introduce additional risk that unintentionally blocks project information that your users need.
- Carefully analyze the class and metric structure before implementing security profiles. Can you accomplish the same security set up with access groups?
- Metrics used in security profiles must be a List, Multi-Select List, or String type metric. Number, Date, and Long String metric types are not available for use in security profiles.
- Metrics whose value is initialized from another metric, and calculated metrics are not available for use in security profiles.
- Accolade allows the definition of up to 250 profiles. However, keep it simple!

## Creating Security Profiles

Security profiles define project access based on classes and metric values associated with a project and a user. Associating a metric with a security profile further refines the access based on the values assigned to the metrics. The available metrics are those associated with models in the selected classes, so the metrics in a profile can distinguish access only within the selected classes.

**Note:** Prior to creating a security profile, ensure that the classes and metrics exist within Accolade.

### To create a security profile:

1. From the **System** menu, select **Security & Groups > Security Profiles**.  
To narrow the list, search by the category.
2. Do one of the following:
  - **To add a new security profile** - Click **Add New** in the top right corner of the page.
  - **To edit an existing security profile** - Click the name of the security profile to open it for editing.
3. Enter the following information to identify the security profile:

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


Field	Description
<b>Name</b>	Enter a name, up to 64 characters long, which identifies the security profile.
<b>System Name</b>	Enter a unique, shorter name that identifies the security profile in queries, reporting views, field codes, and other places in Accolade.  The name must be unique among security profiles, and can only contain letters (English alphabet), numbers, and the underscore.
<b>Description</b>	Enter a description of the purpose or nature of the security profile. This description helps other users identify the profile throughout the system.
<b>Category</b>	Enter or select the group to which this security profile belongs.  Use categories to organize like profiles together. <ul style="list-style-type: none"> <li>• Leave this field blank to add to the <b>Default</b> category.</li> <li>• To define a new category, select <b>New Category</b> and enter the category name.</li> <li>• To delete a category, remove every item from the category. Empty categories are deleted automatically.</li> </ul>
<b>Order</b>	Enter a number to specify the security profile's place in the list of profiles on the <b>Security Profiles</b> page. A smaller number places the profile higher in the list.
<b>Visible</b>	Select this check box when this security profile is ready for use.
<b>Classes</b>	Select which classes to include in this security profile.  <b>Note:</b> A security profile must have at least one class.

- In the **Metrics** section, click **Add Metrics** and select one or more metrics to add from the **Available Metrics** list. Use the **Category**, **Name** or **System Name** options to filter the list of available metrics. Click **Select** to select the metrics, and then click **Done** when finished.

A metric must be a List, Multi-Select List, or String type and be associated with at least one model in a class selected in the profile to add it to a security profile. Additionally, security lists cannot include initialized or calculated metrics.

- For each profile metric, click the **Value** column to specify the values.
  - **For List type metrics** - Select the values the metric must have to allow access to the project.
  - **For String type metrics** - Enter the exact string of characters that this metric must have to allow access to the project.
- (Optional) To allow access to projects whose assigned process model does not include this metric, select the **Extended Access** check box. Extended access allows access to projects that do not contain the metric itself, not to projects that contain a different value for the metric.
- Click **Create** to create the new security profile or **Apply** to save changes to an existing security profile.

**Notes:**

- To delete a security profile, ensure the profile is not in use, select the profile, and click **Delete**.
- Select  to print the list of security profiles.

**Sopheon Corporation**

6870 West 52nd Avenue, Suite 215

Arvada, CO 80002