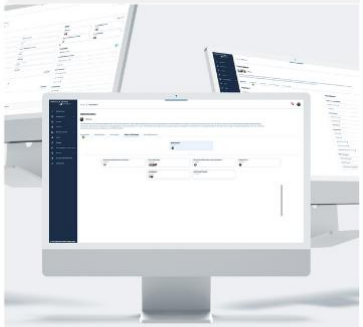
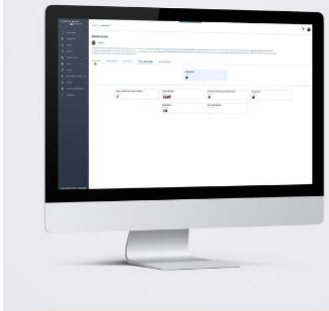
PINNACLE SERIES
by EAGLE POINT SOFTWARE

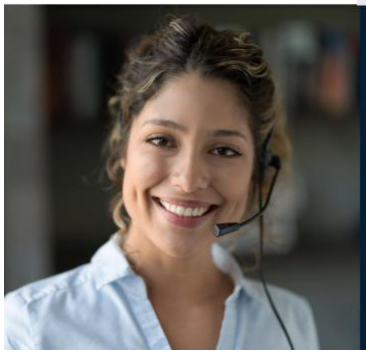
Navigating Platform Permissions

Smarter access. Stronger control.

Learn how to optimize user access, content control, and group hierarchies. Whether you need centralized control or group-level autonomy, this guide will help you manage permissions seamlessly.







PERMISSIONS OVERVIEW

TABLE OF CONTENTS

INTRODUCTION

The **Permissions Overview** document provides a detailed breakdown of the various permission levels available within the platform, explaining what each role can and cannot do. This guide will help administrators and users understand the scope of their access, from managing content and users to handling external learning, live events, and reporting. By aligning permissions with your organizational structure, this document ensures that the right individuals have the appropriate level of control and visibility, supporting a streamlined and secure user experience.

PERMISSION TYPES

Inherit Permissions (Toggle)

This toggle allows users to inherit **visibility**—not permissions—from the groups they are assigned to. When enabled, the user can see and interact with users in child groups (for assignments and reporting) if they are a **Manager** or **Group Owner**. However, **permissions like Assignor or Content Author must still be assigned directly at each group level**. Inherit Permissions only affects **who** a user can see and assign to—not **what** they are allowed to do.

Nested Groups and Inherited Permissions

In Pinnacle Series, **group hierarchy** controls assignment visibility, not role-based permissions. If **Inherit Permissions** is enabled, users listed as **Group Owners or Managers** can assign training to users in their own group and any nested child groups.

Group hierarchy in Pinnacle Series governs **visibility**, not permission inheritance. While Inherit Permissions allows Assignors, Managers, and Group Owners to see users in child groups for assignment and reporting, roles such as Assignor or Content Author must be directly assigned at the needed group level.

This structure supports large, multi-tiered organizations by enabling broad oversight with localized access — particularly helpful in architecture, engineering, construction, and manufacturing environments.

Group Owners and Managers: These designations unlock broader visibility for Assignors, without granting them full platform-wide control.

Important: **Permissions (roles)** do not cascade. Each group must have roles like Assignor or Content Publisher explicitly assigned.

Example:
Maria is the Manager of the "A Team" group, which contains four child groups (A1–A4). If Inherit Permissions is toggled on, Maria can assign learning to users in A1–A4, but she must still have the Assignor role at each group level where she needs to take action.

Impact of Inherit Permissions:

Enabling **Inherit Permissions** supports consistent learning oversight by allowing managers, group owners, and assignors to see users in both their group and any child groups. This expanded visibility makes it easier to manage assignments across nested structures without needing to assign roles repeatedly at each level.

Importantly, **permissions themselves do not inherit** — roles must still be explicitly assigned at each group level. Inherit Permissions only affects who the user can see and assign learning to, not what they are permitted to do.

This approach strikes a balance between centralized oversight and decentralized execution, making it especially valuable for complex organizations in architecture, engineering, construction, and manufacturing where team structures often mirror project hierarchies.

Assignments and External Learning

Assignment Administrator

What They Can Do:

- Access the **Assignments** and **External Learning** sections in the Admin Portal.
- Assign learning and create **auto-enrollments** for any user or group across the platform.
- Approve or deny **external learning requests** submitted by any user.
- Create and manage **external learning tracking records** and their attributes.
- Review and export **learning reports** for all users (*currently available via the Management Utility*).

What They Cannot Do:

- There are no functional limitations. Assignment Administrators have full assignment capabilities across the platform, regardless of group ownership, manager status, or Inherit Permissions settings.

Assignor

What They Can Do:

- Access the **Assignments** and **External Learning** sections in the Admin Portal.

- Assign and track Pinnacle Series and external learning for users they can see — specifically:
    - Users they are listed as the **Manager** of
    - Users in groups where they are the assigned **Group Owner**
- Approve or deny **external learning requests** for users within their visible scope.

Visibility can include child groups if:

- **Inherit Permissions** is enabled
- The Assignor is the Group Owner or Manager of the parent group

What They Cannot Do:

- Cannot assign or track learning for users **outside of their managed or owned groups**.
- Cannot see users unless they have been granted visibility through **manager status**, **group ownership**, and (optionally) **inheritance**.

Content Management

Content Administrator

What They Can Do:

- Access the **Manage Content** and **Libraries** areas.
- View and manage **all content folders**, unless folder-specific restrictions are applied.
- Perform full **Library Management**, including:
    - Creating and managing custom libraries.
    - Sharing libraries with specific groups or all users.
    - Organizing content using topics, subtopics, and keywords for granular control.
- Manage metadata types: topics, subtopics, keywords, and learning tags.
- Assign visibility to content and libraries.
- Author, edit, publish, and delete any content.
- Delete content in any state (draft, published, archived) from any library.
- Restore deleted content from the Recycle Bin.
- View and manage content suggestions and submitted changes.
- Approve or request content approval (if approval workflows are enabled).
- Manage and customize content templates and company certificates.
- Modify transcripts and manage default mappings to KnowledgeSmart Assessments.

What They Cannot Do:

- Cannot access or edit content **if explicitly restricted by folder-level permissions**.

Content Publisher

What They Can Do:

- Publish content **only within libraries that have been shared with them by a Content Administrator.**
- Author, publish, and manage custom content within libraries that have been explicitly shared with them.
- Create and manage various content types, including:
    - Workflows, Pinnacle Series documents, and external documents (Word, Excel, PPT, etc.)
    - Videos, Live Events, Learning Paths, and Courses
- Delete content (in any state) from libraries they are associated with.
- Restore deleted content from the Recycle Bin (within their shared libraries).
- Assign metadata such as Topics, Subtopics, Keywords, Learning Tags, and Related Learning Commands to their content.
- Publish and unpublish content in their assigned libraries.
- View and respond to content suggestions and change requests.
- Modify video transcripts associated with their shared libraries.

What They Cannot Do:

- Cannot create, edit, or delete libraries.
- Cannot share libraries with other users or groups.
- Cannot access content outside of the libraries that have been shared with them by a Content Administrator.

Content Author

What They Can Do:

- Work only within **libraries that have been explicitly shared with them by a Content Administrator**
- Create and manage **unpublished** custom content, including:
    - Workflows, Pinnacle Series documents, external file types (e.g., Word, Excel, PPT), videos, Live Events, Learning Paths, and Courses
- Work only within **libraries that have been explicitly shared** with them
- Delete content that is in **draft state**
- Restore deleted **draft content** from the Recycle Bin
- Create folders for unpublished content
- Move content within the **draft stage**
- Assign metadata — including Topics, Subtopics, Keywords, Learning Tags, and Related Learning Commands — to **unpublished** content
- Modify transcripts for videos that have **not yet been published**

What They Cannot Do:

- Cannot publish or approve content

- Cannot access, edit, or delete **published** content
- Cannot create, edit, delete, or share libraries
- Cannot manage content settings such as templates, KnowledgeSmart mappings, or default certificates

User Administration - Administrator

What They Can Do:

- Access the **Admin Browser** to manage users and groups.
- Add and manage users, either manually or via **Microsoft Entra ID (formerly Azure AD) synchronization**.
- Assign users to groups.
- Assign platform-level permissions (e.g., Assignor, Content Author, etc.).
- Enable and manage **Single Sign-On (SSO)**.
- Assign **Product Expertise** to users.
- Manage platform-wide and individual user settings, including:
    - Email notifications
    - Language preferences
    - Workflow display options
- View and edit data marked as **sensitive** (e.g., group visibility, manager assignments), if Administrator rights are granted.

What They Cannot Do:

- Cannot create, manage, or publish content unless also assigned **Content Administrator** permissions.
- Cannot access content-related areas such as **Manage Content**, **Assignments**, or **Libraries** unless given the appropriate additional roles.
- Limited to managing platform configuration, users, groups, security, integrations, and system settings only.

User Administration - View Reports

What They Can Do:

- Access the MU for reporting.
- View and export usage reports, including data on Unique Active Users, Top Learners, Learning Path Progress, Custom Content, Top Content Contributors, etc.

What They Cannot Do:

- Cannot modify or create new reports.
- Cannot access content directly through reporting.

User Administration - View Sensitive Information

What They Can Do:

- View user or group attributes marked as sensitive, provided they have Admin permissions.

Technical Support Disabled

What They Can Do:

- Restrict users from accessing technical support.
- Block access to support buttons in the Web Portal.

What They Cannot Do:

- This restriction grants no additional permissions.

User Administration - Manage Portal Branding and Customization

What They Can Do:

- Access to the Branding & Customization area of the platform.
- Ability to customize the platform's logo, colors, and theme.
- Ability to alter the platform's layout for a tailored user experience.

Role-Based Permission Scenarios

Content Administrator

Important: Content Administrator permissions do **not** override library visibility. Libraries must be explicitly shared to the user's role to create, manage, or publish content.

Scenario 1:
A manager at an architecture firm creates Revit learning paths and limits access to certain design teams.

→ Requires Content Administrator permission and access to the relevant shared library to author, publish, and assign visibility.

Scenario 2:
A training lead in a manufacturing company manages libraries tagged for different product teams.

→ Requires Content Administrator permission and shared access to those libraries in order to manage content and metadata.

Scenario 3:
A compliance lead publishes updated training across all regional offices.

→ Requires Content Administrator permission and shared access to all relevant libraries to publish and manage visibility settings.

Assignor

Scenario 1
A project lead assigns safety training to new hires within their team.

→ Requires Assignor permission, with visibility over users in their assigned group or any child groups (if Inherit Permissions is enabled).

Scenario 2
A regional supervisor reviews and approves external learning submissions from their department.

→ Requires Assignor permission to manage assignments and external learning for users in groups they own or manage, as shown in the Admin Browser.

Scenario 3
A manager wants to track training progress for their direct reports only.

→Requires Assignor permission, with visibility limited to users for whom they are listed as Manager in the user's group profile.

The group must be visible in the Admin Browser. If users are spread across child groups,

Inherit Permissions must be enabled for full visibility.

Assignment Administrator

Scenario 1:
A global compliance officer monitors mandatory certification completion across all departments.

→ *Requires Assignment Administrator permission for platform-wide learning*
→ *assignment and reporting.*

Scenario 2:
A learning manager sets up auto-enrollments for machinery safety training across multiple locations.

→ *Requires Assignment Administrator permission to configure global enrollment rules.*

Scenario 3:
The head of L&D manages and approves external learning requests across the entire organization.

→ *Requires Assignment Administrator permission for full external learning oversight.*

Content Publisher

Scenario 1:
A content team member updates CAD training content but should not have access to library settings.

→ *Requires Content Publisher permission and access to a shared library, without library management rights.*

Scenario 2:
A trainer edits content in machine specific libraries without needing access to other departments.

→ *Requires Content Publisher permission with access limited to designated libraries.*

Scenario 3:
A training manager customizes templates and updates content for specific teams but shouldn't oversee broader content governance.

→ Requires Content Publisher permission to manage and publish content in shared libraries only.

Content Author

Scenario 1:
A subject matter expert drafts a product assembly guide and applies tags and topics before review.

→ Requires Content Author permission to create draft content and apply metadata in a shared library.

Scenario 2:
An instructional designer develops a BIM course and quiz to be approved by another team.

→ Requires Content Author permission to build unpublished content in a library they have access to.

Scenario 3:
A technical trainer creates and organizes learning materials in folders and assigns metadata but does not manage publication.

→ Requires Content Author permission to draft content and apply metadata in accessible libraries.