

## **MooD 17 User Management and Permissions Guide**



## **Notice of Copyright and Trademarks**

MooD 17 User Management and Permissions Guide

© MooD, MooD Smarter Decisions, Performance Activation, Synchronization Activation Technology and Knowledge Map are registered trademarks of CACI Ltd. in the United Kingdom and / or other countries.

Microsoft and Windows are trademarks of Microsoft Corporation in the USA and other countries.

Rights to all other referred trademarks or registered trademarks reside with their respective owners.

Aspects of the Enterprise Business Model, Model-Driven Data Aggregation and Business Solutions to Support Smarter Decisions are protected by International Patent and Patent Pending. These include the Meta-Architecture Framework, Panels Technologies, Auto-Explorer, Business Orchestration, the Activator mechanism, Process Driven System, Performance Activation, Model-Driven Enterprise Management, Dynamic Aggregation, Smart Columns, the Variant Mechanism, and other technologies and mechanisms implemented within MooD Business Architect and MooD Active Enterprise.

© CACI Ltd., all rights reserved. No part of this document may be reproduced by any means, or transmitted, or translated into machine language without the written permission of the company.

## Contents

---

<b>Introduction</b> .....	<b>6</b>
Changes in MooD 16.....	6
Changes in MooD 15.....	6
<b>About users, user groups and permissions</b> .....	<b>7</b>
Users and user groups .....	8
The Users and Groups themes.....	9
Types of permission .....	11
Element permissions .....	12
Element permission inheritance.....	14
Root element permissions .....	14
Element ownership .....	15
Library permissions .....	15
Inheritance of library permissions .....	18
Precedence of library permissions over element permissions.....	18
Field permissions .....	18
Precedence between element and field permissions .....	19
The Anonymous user .....	19
User management on the web.....	20
<b>The Permissions tab in Business Architect</b> .....	<b>21</b>
Displaying the Permissions tab.....	21
About the Permissions tab.....	22
<b>Managing users and user groups</b> .....	<b>26</b>
Creating user groups.....	26
Creating users.....	27
Adding users to a user group.....	30
Managing passwords and disabling accounts.....	32
Configuring Single Sign-on in Business Architect .....	33

Password settings .....	34
<b>Managing permissions .....</b>	<b>36</b>
Giving user groups library permissions.....	36
Assigning element permissions by user group.....	38

## Tasks

---

<b>Task 1</b> To create a user group:.....	26
<b>Task 2</b> To create a user: .....	27
<b>Task 3</b> To add users to user groups: .....	30
<b>Task 4</b> To grant library permissions to a user group: .....	36
<b>Task 5</b> To assign element permissions by user group: .....	39

## Figures

---

Figure 1. Users, user groups and permissions .....	8
--	---

## Tables

---

Table 1. Element permissions.....	12
Table 2. Library permissions.....	17
Table 3. Field permissions.....	18
Table 4. Permissions and what they can apply to.....	24

## Introduction

---

This guide is for MooD administrators and users who have been granted permission to manage users, user groups, or permissions. It has the following sections:

- [About users, user groups and permissions](#) (page 7)  
Explains MooD users, user groups and permissions, and how they function within Business Architect.
- [The \*\*Permissions\*\* tab in Business Architect](#) (page 21)  
The **Permissions** tab is a single point for permissions management. This section outlines its functionality and behaviour.
- [Managing users and user groups](#) (page 26) and [Managing permissions](#) (page 36)  
Instructions covering key tasks. These tasks assume knowledge of what is covered in the preceding sections.

## Changes in MooD 16

- 16.032 – Removed Library permission to manage publishing schemes.
- 16.076 – Added the Library permission to manage the meta model – meaning that you can assign users to a group which is allowed special access to **Manage Themes** and **Manage Field Types**, with some limitations. Single Sign on in Business Architect added.

## Changes in MooD 15

Some changes relating to users and permissions have been introduced in MooD 15:

- Business Architect now has a single administrative point for permissions management – the **Permissions** tab.
- **Library permissions** have been introduced. These let you devolve management permissions that were previously restricted to members of the **Administrators** user group. Library permissions are available for: **Users and Groups, Styles, Model Masters, Epochs, Queries, Smart Columns, Matrices, Threshold sets, Synchronizations** and **Publishing Schemes**. Groups with permission to manage a library can edit, rename, delete, move and create within that library.
- You can set default **root element** permissions for a theme. All elements in that theme then inherit these permissions. Root elements are the first level of elements within a theme, and you can prevent users creating them.
- Added an **Anonymous** user.
- Action panels for web based user administration have been introduced.

All are covered or introduced in this guide.

## About users, user groups and permissions

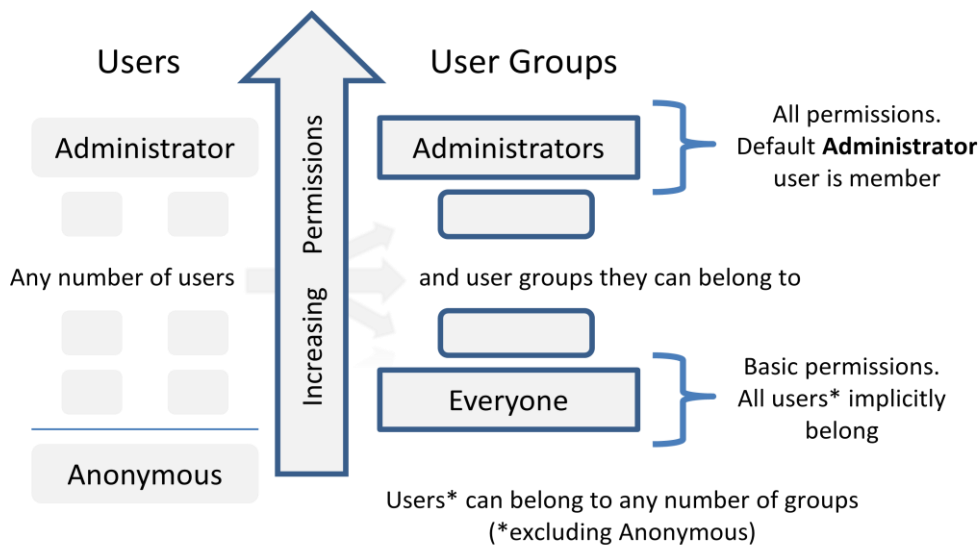
---

The relationship between users, user groups and permissions, together with the types of permission available and methodology form a permission's architecture that should provide users with the facilities needed to achieve their goals, and at the same time provide the repository security required. To help you understand the permission's model employed by MooD, this section includes the following:

- [Users and user groups](#) (page 7)  
How users belong to user groups, and the default users and user groups created for you. We recommend that you use user groups as your primary means of controlling the allocation of permissions. This helps maintenance as well as performance.
- [Types of permission](#) (page 11)  
MooD has element permissions, library permissions and field permissions. This section introduces these types. Business Architect uses a single **Permissions** tab to manage all three types, so it is important to differentiate between them.
- [Element permissions](#) (page 12)  
Information on the permissions that can be applied to elements. This includes sections on inheritance, on root element permissions, and on the ownership of elements (which does not affect permissions).
- [Library permissions](#) (page 15)  
Library permissions let you to devolve specific management permissions without granting full **Administrator** user status. This includes a section on how a user's library permissions take precedence over their element permissions.
- [Field permissions](#) (page 18)  
Information on the permissions that can be applied to the fields that define each element within a theme. It includes a section on how element and field permissions interact (precedence).
- [The Anonymous user](#) (page 19)  
Outlines this default user that lets you provide limited, login free access to a repository through the web.
- [User management on the web](#) (page 20)  
Outlines the action panels for web based user administration.

## Users and user groups

This diagram and the key points that follow cover how users, user groups and permissions interact.



**Figure 1. Users, user groups and permissions**

Key points:

- Users and user groups are elements within the **Users** and **Groups** themes respectively.
- By default, there is a user called **Administrator**. This user is the repository administrator, has full privileges, and is responsible for creating any number of users and user groups required. You cannot delete the **Administrator** user, and you cannot restrict their permissions.

---

**Note:** The only other default user is the **Anonymous** user. This provides login free, but highly limited, access to a repository on the web. See [The Anonymous user](#) on page 19 for details.

---

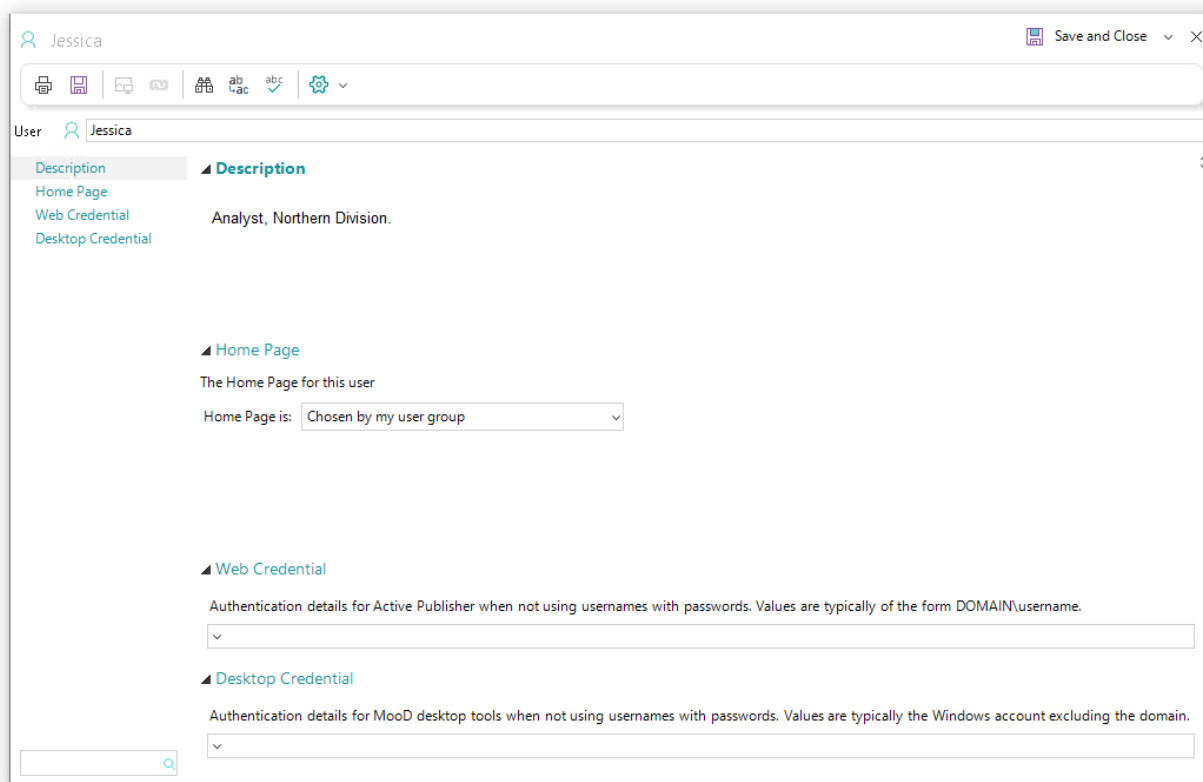
- By default, there are two user groups: **Administrators** and **Everyone**.
  - The **Administrator** user implicitly belongs to the **Administrators** user group.
  - All users (excluding the **Anonymous** user) implicitly belong to the **Everyone** user group.
- Element and library permissions can be assigned to user groups, and if necessary, elements can have explicit user permissions assigned.
- Users can belong to more than one user group.
- Users inherit their permissions from the user groups they belong to, but individual users can have permissions that override their user group permissions. Permissions are cumulative.

We recommend that you use user groups to establish levels of access, and then assign users to an appropriate user group rather than use explicit user permissions. The **Permission Resolution Report** in the **Active Enterprise Settings** window reveals your permission cache groups. Explicit user permissions can negatively affect the performance of your web site.



### The Users and Groups themes

Users and user groups are elements belonging to the **Users** and **Groups** themes respectively. You create new groups and users just like any other element in MooD.



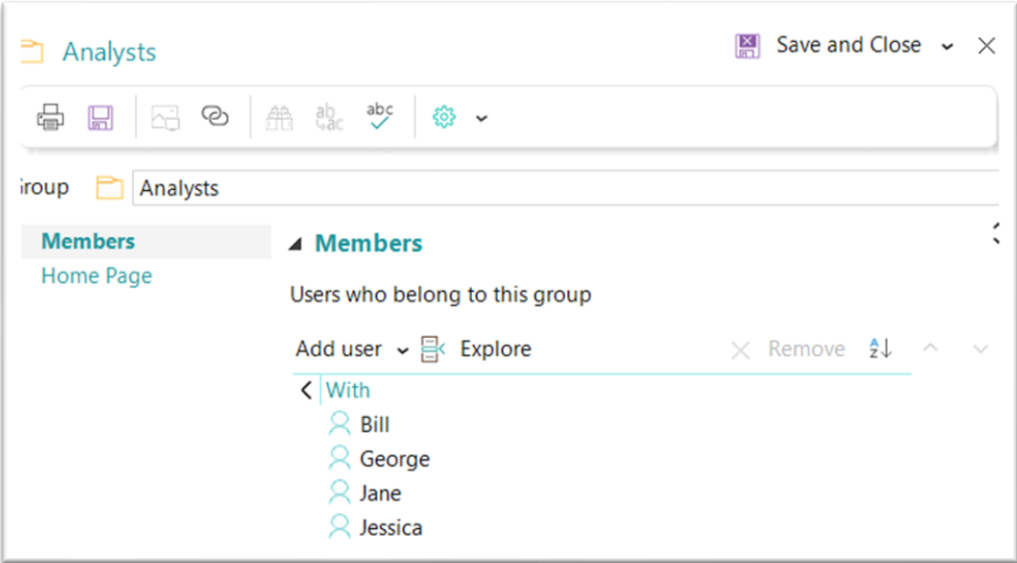
The screenshot shows the user management interface for a user named 'Jessica'. The interface is displayed in a window titled 'Jessica' with a 'Save and Close' button in the top right corner. The user's name 'Jessica' is shown in the top left. Below the name, there is a search bar and a list of tabs: 'Description', 'Home Page', 'Web Credential', and 'Desktop Credential'. The 'Description' tab is selected, showing the user's role as 'Analyst, Northern Division.' Below this, the 'Home Page' section has a dropdown menu set to 'Chosen by my user group'. The 'Web Credential' section has a text input field with a dropdown arrow, and the 'Desktop Credential' section also has a text input field with a dropdown arrow. A search bar is located at the bottom left of the form.

**Users** elements have the following default fields:

- **Description.** For you to populate as you see fit.
- **Home Page.** Each user and user group can have a Home Page. This is the model displayed when a user logs into a repository by means of Active Enterprise (the Web). The model can be the user's model, a specific element's model, or the model associated with the user group that the user is a member of.
- **Web Credential.** The Active Directory domain and user login name for use within Active Publisher.
- **Desktop Credential.** If you have configured Single-Signon, this would be the windows username in your active directory which maps to this user.

**Groups** elements have the following default fields:

- **Members.** The users who are members of the user group, and therefore inherit its permissions. For example:



- **Home Page.** This functions the same for **Users** and **Groups** elements. See the previous **Home Page** description.

## Types of permission

Before looking at the actual permissions, you should understand the three types of permission used in MooD, and how they interact.

- Element permissions

Apply to each element in a theme either individually or collectively by means of inheritance. Element permissions can be set by user group. This means that the same elements can have different permissions for different user groups. If necessary, element permissions can be set for individual users. These override any permissions attained through user group membership, but are in turn overridden by any library permissions.

See [Element permissions](#) on page 12 for reference material on the actual permissions an element can have.

- Library permissions

Grant management permissions previously exclusive to users in the **Administrator** user group to other user groups or users. Permissions are organized and granted by area (**library**), for example, **Matrices**, **Queries**, **Synchronizations**, and **Users and Groups**. This allows you to devolve management permissions without granting full **Administrator** user access. Again, if a user has specific library permissions, they take precedence over those attained by means of their user group membership.

---

**Note:** Individual **Users** elements cannot be given singular, across the board permission over an entire library. They can only have permissions for specific groups or items within a library. For example, queries can be organized into groups, with each group containing any number of individual queries. **Users** elements can be granted permission over individual queries or groups of queries, but not the entire **Queries** library itself. Only **Groups** elements can be given permission over an entire library category by means of a single permissions setting.

---

Library permissions also take precedence over any element permissions. For example, if a user belongs to one user group where editing of an element is denied, but also to one user group that has the power to manage matrices, then they will be able to edit that element's matrices.

See [Library permissions](#) on page 15 for a list of areas that you can grant control over.

- Field permissions

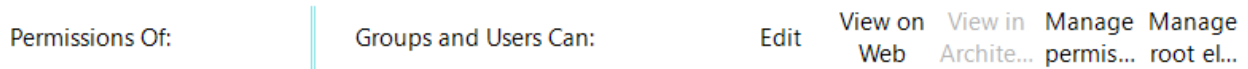
Apply to fields in themes (and consequently elements). Field permissions control whether fields are visible and editable in Business Architect, or when published on the web using Active Enterprise. See [Field permissions](#) on page 18 for details.

### Tip – Develop a 'lean permissions' architecture

As you learn about permissions and apply permissions to your repository, we recommend that you implement a **lean permissions architecture**. Fewer explicitly set permissions help performance and reduce maintenance. Achieve this by, wherever possible, applying high level group permissions and allowing inheritance to propagate permissions across your repository.

## Element permissions

Business Architect’s **Permissions** tab lists five permissions (the last five columns in the next image):



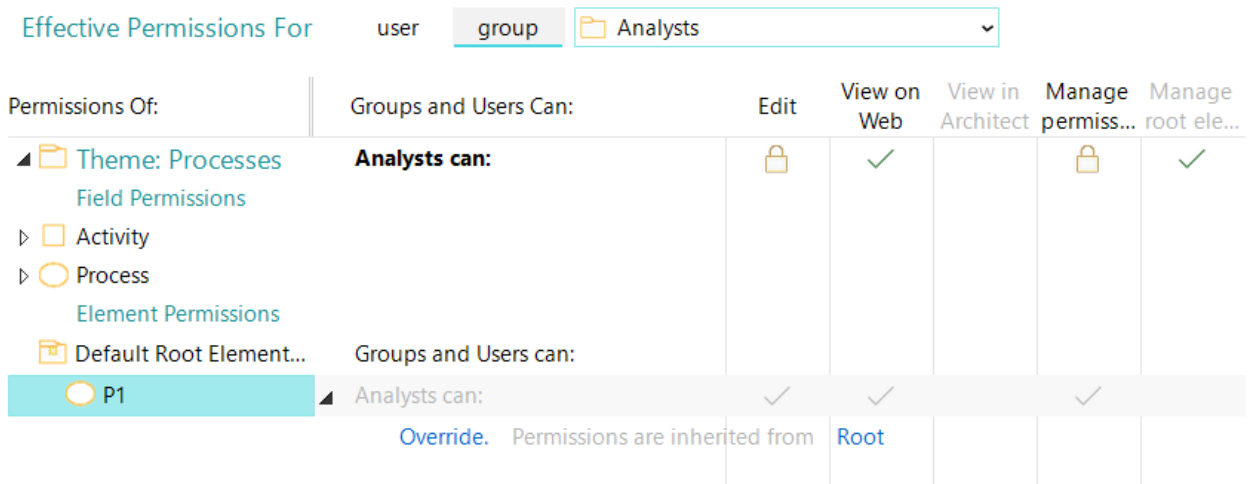
Only three of the five apply to elements. These are:

Permission	Description
<b>Edit</b>	Grants permission to manage an element. This includes editing, creating child elements, renaming, moving and deleting.
<b>View on Web</b>	The element’s model can be viewed in a browser by means of Active Enterprise.  <b>Note:</b> This permission can also apply to fields. This controls what is presented to users. See <a href="#">Field permissions</a> on page 18 for details
<b>Manage Permissions</b>	Users with this permission can edit the element’s permissions.

**Table 1. Element permissions**

**Note:** Although **View in Architect** applies to field permissions only, and **Manage Root Elements** only applies to themes, both affect what a user can do with elements. See [Field permissions](#) on page 18 and [Root element permissions](#) (page 14) for details.

As shown here, permissions appear as columns on the **Permissions** tab:



A tick means permission is granted to that user or user group. A padlock means it is denied. A blank column means the permission is not applicable to that item.

There are two types of tick, and two types of padlock:

Greyed icons indicate that the element has inherited its permissions.

## MooD 17 User Management and Permissions Guide

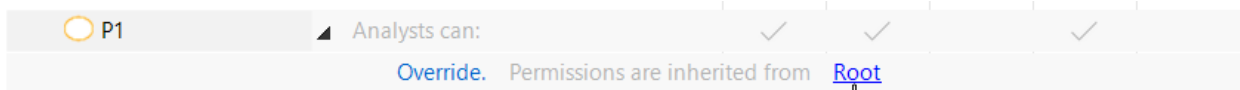


Coloured icons indicate that the element's permissions have been explicitly set.

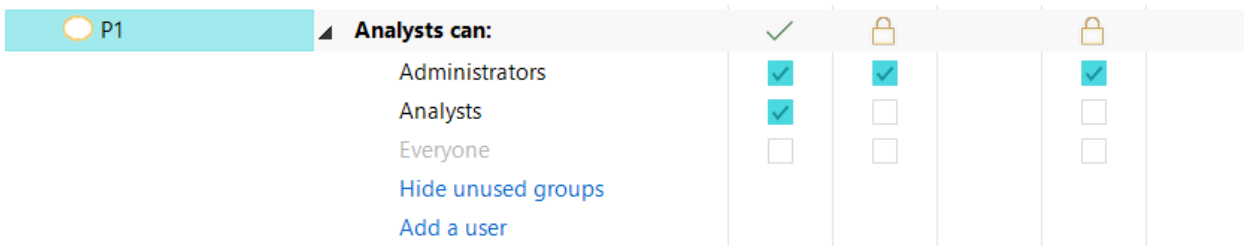
## Element permission inheritance

By default, elements inherit their permissions from their parent. You can set an element's permissions, and thereby override its inherited permissions. However, note that if you change the permissions for an element, its descendent elements will then inherit those permissions, unless they too have had their permissions overridden.

Business Architect's **Permissions** tab includes a link to the element that an element inherits its permissions from. For example, in the following image you can see that **E1** inherits its permissions from the root element.



Greyed ticks and padlocks (and the presence of the **Override** command and the *inherited from* link) indicate that the element inherits its permissions. If you click **Override**, you can set user group and user permissions for that element. The **Override** command will be removed, and the explicitly set permissions (with coloured icons) displayed instead, as shown here:



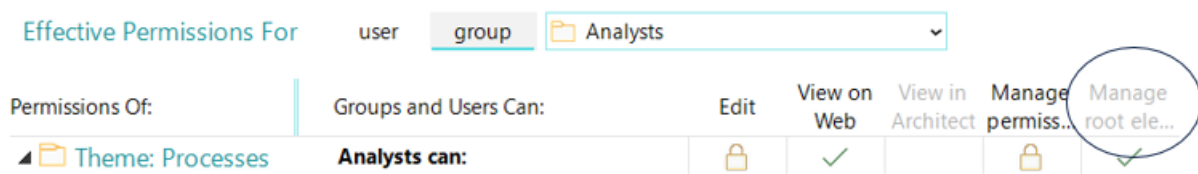
To help you manage element inheritance, the ribbon includes the following commands:

- Make descendants inherit permissions
- Remove overridden permissions

The ribbon also lets you **Pickup** and **Apply** element permissions.

## Root element permissions

For each theme, there is a **Manage Root Elements** permission (ringed in the following image):



User groups or users granted this permission can create and edit **root elements**. Root elements are the first level of elements within a theme.

You can set the default **Root Element Permissions** (ringed in the following image) for users and user groups. Each root element created within a theme inherits the root element permissions.

Permissions Of:	Groups and Users Can:	Edit	View on Web	View in Architect	Manage permis...	Manage root ele...
<ul style="list-style-type: none"> <li>▲ Theme: Processes               <ul style="list-style-type: none"> <li>Field Permissions</li> <li>▸ Activity</li> <li>▸ Process</li> <li>Element Permissions</li> <li>Default Root Element...</li> </ul> </li> </ul>	<b>Analysts can:</b>		✓			✓
	Groups and Users can:					
	Administrators	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
	Analysts	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input type="checkbox"/>	
	Everyone	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input type="checkbox"/>	
	<a href="#">Hide unused groups</a>					
	<a href="#">Add a user</a>					

Due to inheritance, all elements in a theme will inherit the root element permissions unless they are specifically overridden.

### Element ownership

MooD has the concept of element **ownership**. Typically, elements are owned by the user who created them. However, ownership can be changed (**File** tab, **Manage Repository**, **Manage Ownership**).

Element ownership does not affect permissions. Do not infer that because a user owns an element they have permissions for it. You can own an element but have no permissions over it.

### Library permissions

Library permissions grant management permission over specific, mostly reusable, features (libraries) to other user groups. If a user has **Edit** permission for a library, they can edit, rename, delete, move and create within that library. Such management powers were previously restricted to members of the **Administrators** group. Administrators continue to have all permissions, but can now devolve and control specific management responsibilities across the user base. The following image shows some of the library permissions. This is followed by a table describing them.

# MooD 17 User Management and Permissions Guide

Effective Permissions For user group Administrator

Permissions Of:	Groups and Users Can:	Edit	View on Web	View in Architect	Manage permissi...	Manage root ele...
▶  Theme: Processes	<b>Administrator can:</b>	✓	✓		✓	✓
▲  Library Permissions						
Manage Themes and F...	Administrator can:	✓				
Users and Groups	Administrator can:	✓				
Epochs	Administrator can:	✓				
▶  Matrices	Administrator can:	✓				
Model Masters	Administrator can:	✓				
▶  Threshold sets						
▶  Queries	Administrator can:	✓				
▶  Smart Columns	Administrator can:	✓				
▶  Styles and Chart Palettes	Administrator can:	✓				
▶  Synchronizations	Administrator can:	✓				























Library	Description
<b>Manage Themes and Field Types</b>	Permits users to access the Manage Themes window and Manage Field Types Window and to perform most actions including the deletion of an entire theme. Some actions are limited for security purposes, such as merging field types and setting values for the credential fields of MooD Users. This permission does not allow Synchronizer imports which manipulate the meta model to be executed.
<b>Users and Groups</b>	Manage users and user groups. This includes adding, modifying or deleting users and user groups, but excludes managing <b>Administrator</b> users and assigning library permissions.
<b>Epochs</b>	Manage epochs. This is a universal permission covering all epochs in the repository. Primarily, this relates to custom epochs, as you cannot alter the start and end dates of calendar epochs.
<b>Matrices</b>	Manage matrices.
<b>Model Masters</b>	Manage model masters. This is a universal permission covering all model masters in the repository. You cannot set this permission for individual model masters or groups of model masters.
<b>Threshold sets</b>	Manage individual Thresholds. You cannot set permissions that cover all Thresholds (this is why there is no tick in the Threshold sets' <b>Edit</b> column in the previous screenshot).
<b>Queries</b>	Manage queries.
<b>Smart Columns</b>	Manage Smart Columns.
<b>Styles</b>	Manage styles.
<b>Synchronizations</b>	Manage synchronizers (SAT).

**Table 2. Library permissions**

Just like element permissions, you set library permissions in Business Architect's **Permissions** tab. Only two (**Edit** and **Manage Permissions**) apply to libraries.

Excluding **Threshold sets**, all library permissions let you set **Edit** permission across the entire library for user groups.

In the Explorer Bar, most libraries of reusable items can be organized into groups (in this context group means a group within a library and not a user group). You see the same hierarchy on the **Permissions** tab. For example, in the following screenshot, queries are organized in the groups **General**, **Management** and **Operational**. In such cases, for both user groups and users, you can set the **Edit** and **Manage Permissions** permissions for each group, and for each item in each group. Should you require it, this gives you a fine level of control over the management of your libraries.

<ul style="list-style-type: none"> <li>▲ 🔍 Queries</li> <li>▶ 📁 General Queries</li> <li>▲ 📁 Management             <ul style="list-style-type: none"> <li>🔍 Productivity</li> <li>🔍 Trends</li> </ul> </li> <li>▶ 📁 Operational</li> </ul>	<p>Senior Management can:</p> <p><b>Senior Management can:</b></p> <p>Senior Management can:</p> <p>Senior Management can:</p> <p><b>Senior Management can:</b></p> <p>Senior Management can:</p>				
					
					
					
					

The other permissions (the **View on Web**, **View in Architect** and **Manage Root Elements** columns) do not apply to libraries.

## Inheritance of library permissions

Library groups inherit permissions in the same way as elements. Hence, you can take a top down approach to setting permissions, and only override specific exceptions. Just like elements, coloured icons indicate explicitly set permissions, and greyed icons mean inherited permissions. See [Element permissions inheritance](#) on page 14 for details on the rules of permission inheritance (the contents of libraries are all elements in their own right).

## Precedence of library permissions over element permissions

A user’s library permissions take precedence over their element permissions. For example, if a user does not have **Edit** permission for an element, but they do have the **Matrices Edit** library permission, they can manage that element’s matrices. However, they will not, for example, be able to manage the element’s queries, unless the **Queries Edit** library permission is also set.

## Field permissions

Field permissions apply to the fields that define each element within a theme. Of the five permission columns on the **Permissions** tab, only the following three apply to fields.

Permission	Description
<b>Edit</b>	<p>Grants permission to manage the field data.</p> <hr/> <p><b>Note:</b> This means the right to manage the field instance within each element belonging to a theme. It does not confer management rights over the actual definition of that field within a theme.</p> <hr/>
<b>View on Web</b>	The field can be viewed in a web browser by means of Active Enterprise.
<b>View in Architect</b>	The field can be viewed in Business Architect.

**Table 3. Field permissions**

User groups and users can be applied to field permissions. Again, we recommend that you control field permissions by user group, and let individual users inherit from their user group membership.

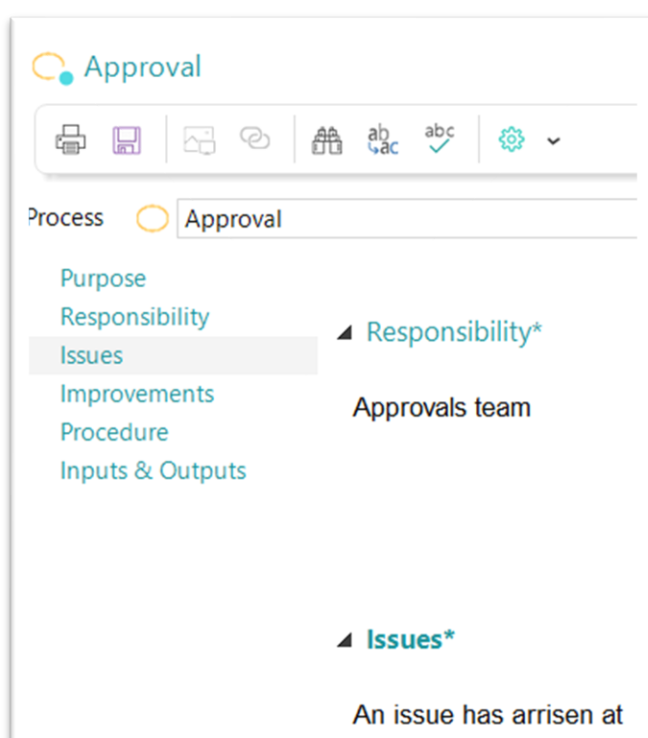
The **View on Web** and **View in Architect** permissions let you control (restrict) what fields are presented to users. This helps you create ‘uncluttered’ solutions for your different user groups. By default, all fields are visible in Business Architect, and Active Enterprise, so you need to

explicitly deny the relevant **View** permissions for your different user groups (clear the check boxes).

### Precedence between element and field permissions

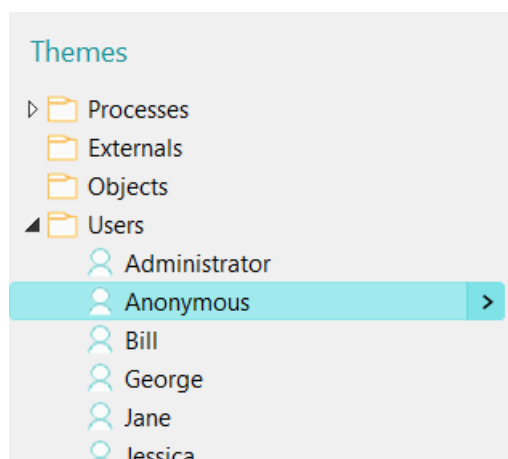
If a permission is denied in an element, it takes precedence over the corresponding field permission. Hence, if **Edit** permission is denied on an element, users cannot edit fields in that element regardless of any field permissions they might have for the theme concerned.

If a permission is granted in an element but denied in the theme's field permissions, then the field permissions takes precedence over the element permissions. Hence, a user can have **Edit** permission on an element, but be denied **Edit** permission on certain fields within that element. This can be seen in the following image (the fields with the padlock icon are locked by the denial of the **Edit** field permission):



### The Anonymous user

MooD includes an **Anonymous** user by default.

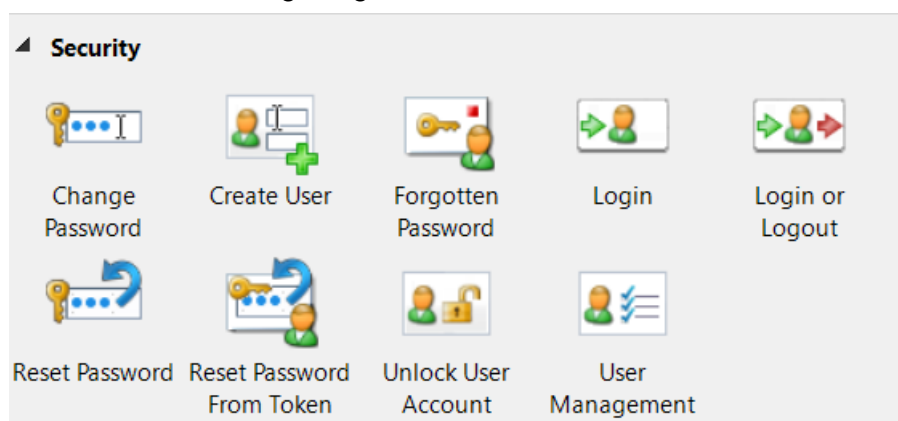


The **Anonymous** user has strictly limited permissions and cannot belong to user groups. For repositories published to the web, the **Anonymous** user can allow restricted login-free access for browsing purposes only.

Use the **Permissions** tab to set permissions for the **Anonymous** user, for example, to specify what elements they can **View on the Web**, and what elements, if any, they can **Edit** (make sure you set the **Permissions** tab's **Effective Permissions For** control to the **Anonymous** user).

## User management on the web

Action panels are available for web based user administration. On the ribbon, on the **Home** tab, in the **Insert** group, click **Actions**. In the gallery, the panels are in the **Security** group, as shown in the following image.



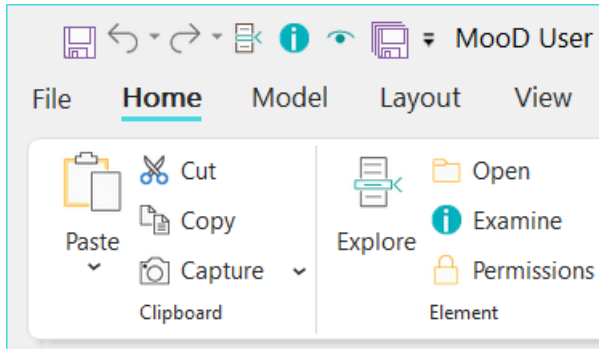
## The Permissions tab in Business Architect

Business Architect's **Permissions** tab is the single point for permissions management.

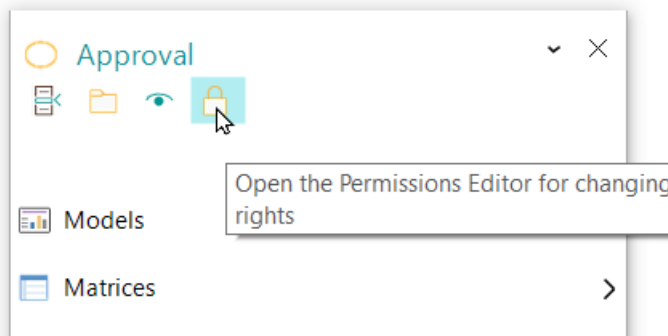
### Displaying the Permissions tab

To display the **Permissions** tab, do one of the following:

- In the Explorer Bar, click an element, and then, on the ribbon, on the **Home** tab, click **Permissions**.



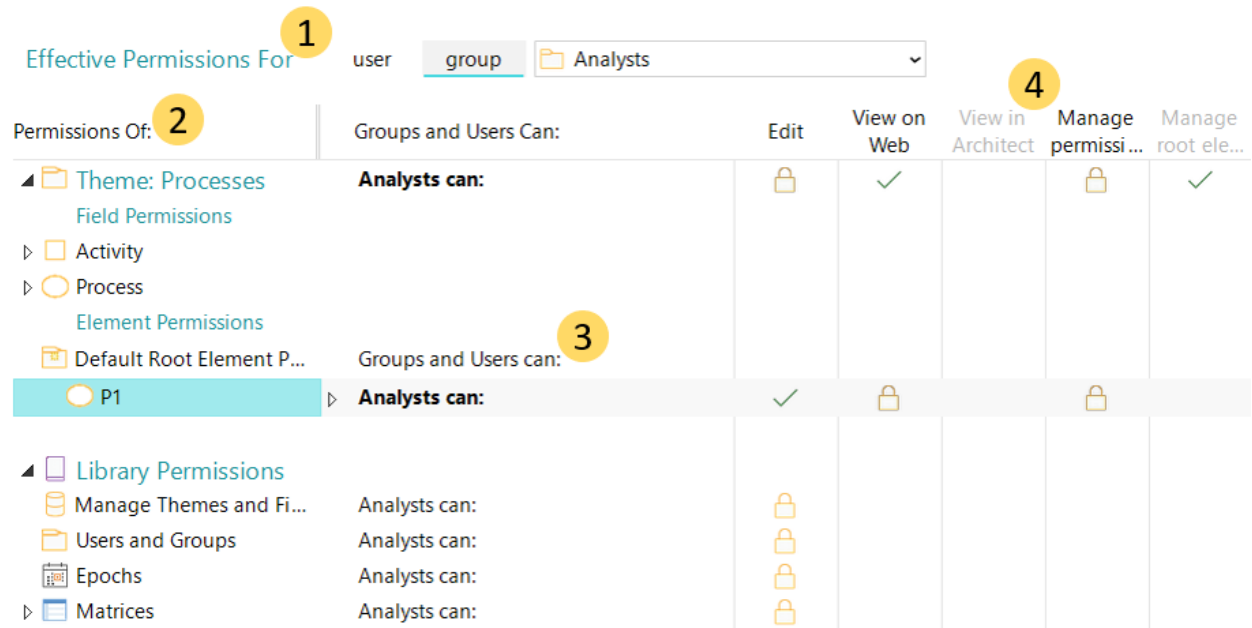
- In an element's Examine pane, click the **Padlock** button.



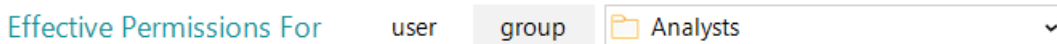
Both methods will open the **Permissions** tab for the chosen element.

## About the Permissions tab

The **Permissions** tab has four main areas identified on the following image.



1. The **Effective Permissions For** control. This sets the user or user group that the **Permissions** tab displays and manages permissions for.



Click **user** or **group** to set a category, and then select the actual user or user group from the drop-down list on the right.

---

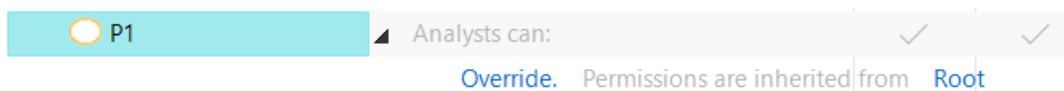
**Note:** Even with the **Effective Permissions For** control set to one user or user group, you can manage the permissions for others. The **Groups and Users Can** column (3) lets you do this. However, the **Permissions** tab's main display is always for the user or user group selected in the **Effective Permissions For** control.

---

2. The **Permissions Of** column. For the selected user or user group, this lists the repository items whose permissions you can view and set. The ribbon includes a **Track Selected** command. This synchronizes the **Permissions** tab with the Explorer Bar so that you can easily change what the **Permissions** tab is showing.
3. The **Groups and Users Can** column. For each settable item listed in the **Permissions Of** column (2), this column lists the user or user group currently selected in the **Effective Permissions For** control (1). The settings for this user or user group are then shown in the **Permissions** columns (4).

The **Groups and Users Can** column includes several pieces of functionality. From here you can:

- For the current user or user group, see where an element or field inherits its permissions from. For example:



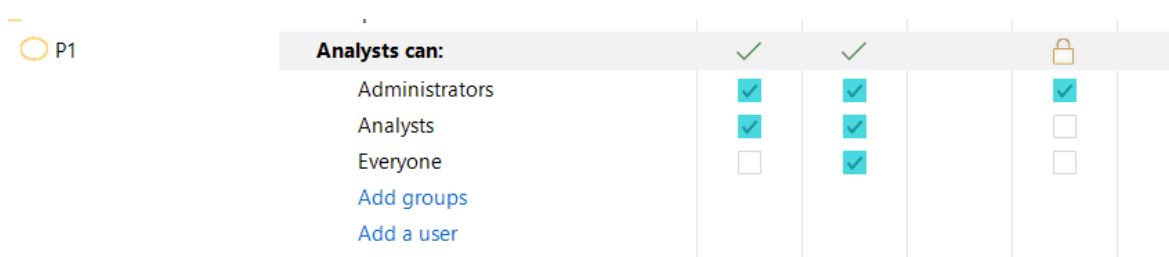
Click the ***inherited from*** link (**Root** in the preceding image) to highlight the element referenced.

**Note:** If an element does not inherit its permissions, the user or user group name appears in bold, and it does not have an **Override** command and ***inherited from*** link. Instead it shows the explicitly set permissions. The **Analysts** group in the next image demonstrates this.

- Override inherited element and field permissions. The **Override** command is shown in the previous image, and an example of what you get when you use this option is shown in the next image. When user or user group permissions are explicitly set rather than inherited, that is, overridden, the user or user group name is displayed in bold. The **Analysts** user group in the next image demonstrates this.

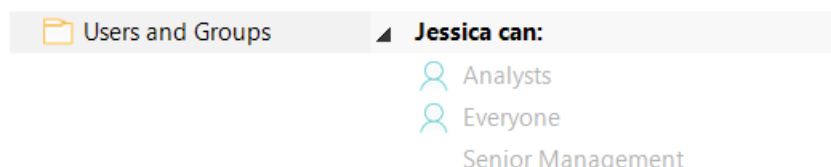
When you click **Override**, the inherited permissions for that item are explicitly set. This gives you a valid set of permissions to start with.


- See and explicitly set element, field and library permissions for the current user or user group, and for other user groups and users. For example, for an element:



**Note:** When you explicitly set permissions, you get commands to control what users and user groups are listed. For example, in the preceding image, there is an **Add a user** command. In the example, all of the groups are shown. However, if there were more groups, there would be an **Add groups** command.

- Change which users and user groups have the **Manage Root Elements** permission for the current theme, and set the actual root element permissions. Root elements are the first level of elements within a theme.
- Manage which user groups a user selected in the **Effective Permissions For** control (1) is a member of. For example:



The  icon means that the selected user is a member of that user group. You use the **Add selected use to this group** and **Remove selected user from this group** commands on the ribbon to control the current user’s user group membership.



**Note:** Although you can use this to manage a user’s user group membership, you cannot select a user group in the **Effective Permissions For** control (1) and use the **Permissions** tab to collectively manage its members. When creating user groups and users, we recommend that you open a user group’s definition page, and then add users directly to its **Members** field. See *Adding users to a user group* on page 30 for instructions.

- The **Permissions** columns. These five columns are the permissions you can set. Each permission is only applicable to certain items in the **Permissions Of** column (2) — an empty column means it’s not applicable. The following table shows what permissions apply to what.

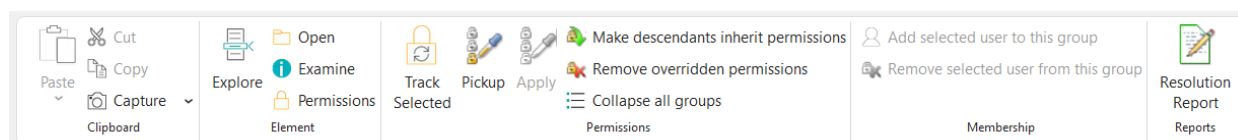
Permissions					
	Edit	View on Web	View in Architect	Manage Permissions	Manage Root Elements
Theme					✓
Field	✓	✓	✓		
Element	✓	✓		✓	
Library	✓			✓	

**Table 4. Permissions and what they can apply to**

Coloured and greyed ticks and padlocks indicate different settings, and whether those settings are explicitly applied or inherited.

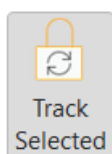
	Greyed icons indicate inherited permissions.
	Coloured icons indicate that the permissions have been explicitly set.

The **Permissions** tab also adds its own command groups to the **Home** tab on the ribbon, as shown here:



The ribbon commands relating to permissions and user group membership are:

- **Track Selected**





When this button is selected (coloured as shown), the content of the **Permissions** tab keeps itself synchronized with the Explorer Bar. Each time you click an element in the Explorer Bar, the **Permissions** tab changes to show that element.

---

**Note:** If you split the Explorer Bar into two (drag the handle at the bottom), **Track Selected** synchronizes with the first Explorer Bar.

In the Explorer Bar, under **Libraries**, if you click **Synchronize**, the tab opens. **Track Selected** does not synchronize with this item.

---

- **Pickup and Apply**



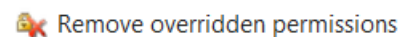
Use these buttons to pick up the permissions applied to one item, and then apply them to another.

- **Make descendants inherit permissions**



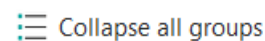
Use this to apply the currently selected element's permissions to its descendant elements. This effectively removes all descendant permissions and cleans up your permissions model from that point. It will also remove any explicitly set permissions on matrices and models.

- **Remove overridden permissions**



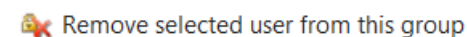
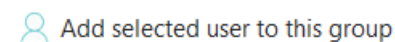
If an element's permissions are explicitly set as opposed to inherited, use this to restore its permission inheritance. This does not affect any descendant permissions.

- **Collapse all groups**



Use this to restore the **Permissions** tab to its original view by collapsing any open groups.

- **Add selected user to this group and Remove selected user from this group**



When a user is selected in the **Effective Permissions For** control (1), use this to quickly add and remove them from user groups. This excludes the **Administrators** user group which can only be managed directly.

## Managing users and user groups

This section covers the key tasks you will perform when setting up users and user groups. It covers:

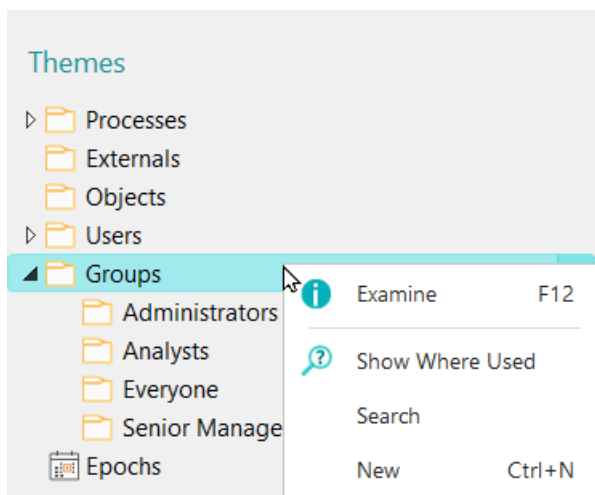
- [Creating user groups](#)
- [Creating users](#)
- [Adding users to a user group](#)
- [Managing passwords and disabling accounts](#)

### Creating user groups

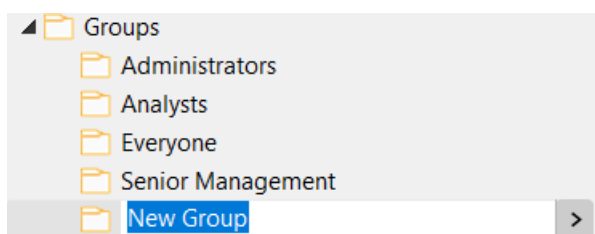
As covered in *Users and user groups* on page 7, Business Architect creates two default user groups: **Administrators** and **Everyone**. Typically, you create user groups for each role within your MooD solution.

**Task 1** To create a user group:

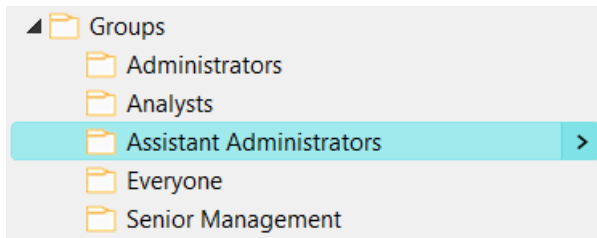
1. In the Explorer Bar, under **Themes**, right-click **Groups**, and then click **New**.



This adds a user group called **New Group**, and selects its name.



2. Give the new group a descriptive name, for example, **Assistant Administrators**.



You can now:

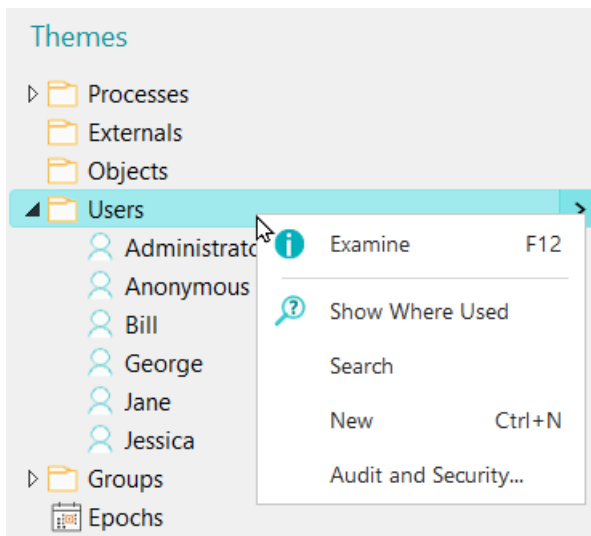
- Add users to the user group. See [Adding users to a user group](#) on page 30.
- Assign library permissions to the user group. See [Giving user groups library permissions](#) on page 36.
- Assign the user group to element permissions. See [Assigning element permissions by user group](#) on page 38.

## Creating users

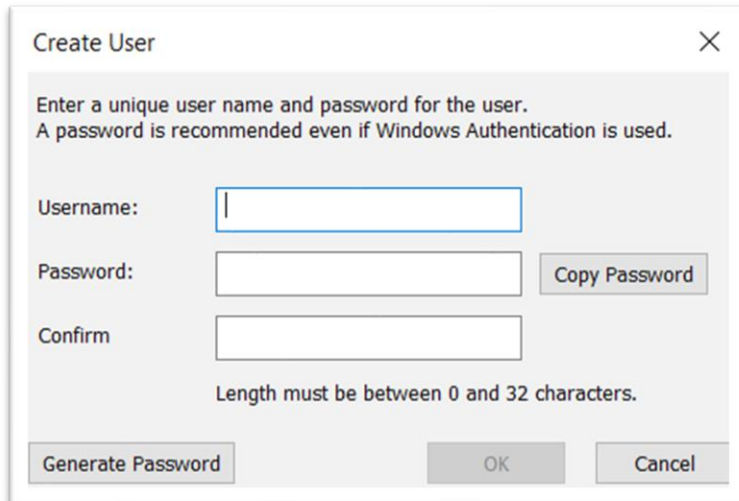
As covered in [Users and user groups](#) on page 7, Business Architect creates two default users: **Administrator** and **Anonymous**. You will need to create a user for each person wishing to log into the MooD solution.

**Task 2** To create a user:

1. In the Explorer Bar, under **Themes**, right-click **Users**, and then click **New**.



This displays the **Create User** dialog box.



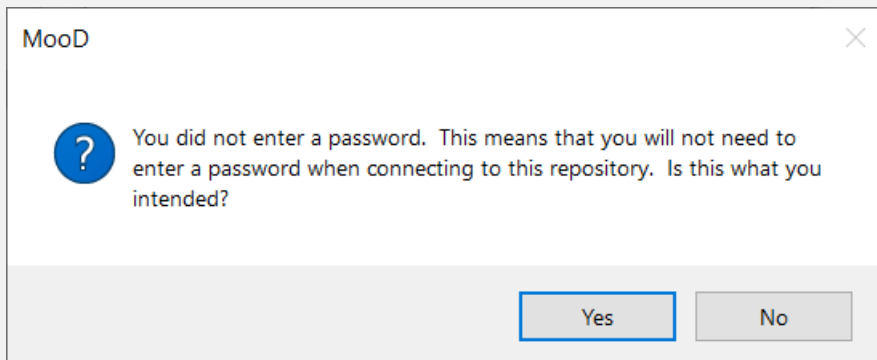
2. Complete the **Create User** dialog box.

To help you:

- **Username** is the name that your user will type into Business Architect’s login dialog box when they try and open the repository in Business Architect.
- **Password** will be valid until the user has successfully logged into the repository for the first time. Once logged in, the user will immediately be prompted to change their password.

### Users without passwords

You may be able to omit the password, in which case, when you click **OK**, Business Architect displays the following:

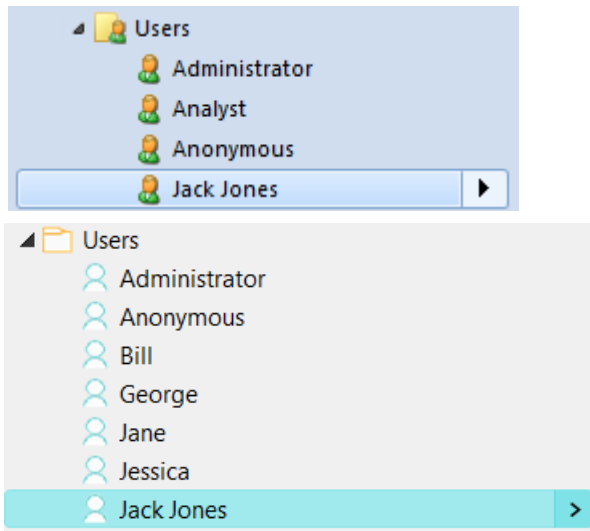


Click **Yes** to proceed, or **No** to return to the **Create User** dialog box where you can supply a password.

If you create a user without a password, that user will be prompted to create a password as soon as they open the repository in Business Architect. Again, the user can continue without supplying a password; in which case their username is unsecure. See [Managing passwords](#) on page 32 for more details.

3. Click **OK** to create the user.

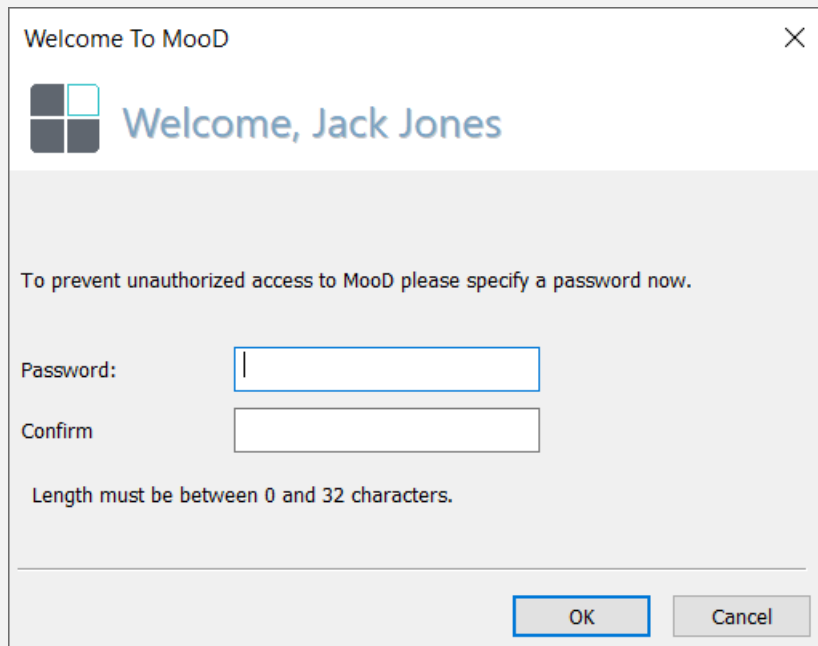
The user is listed under **Users**.



You can now add the user to the user group or groups that best match their required level of access. See [Adding users to a user group](#) on page 30 for details.

**First time log in**

When a user logs into Business Architect for the first time, they are presented with a dialog box like the following:



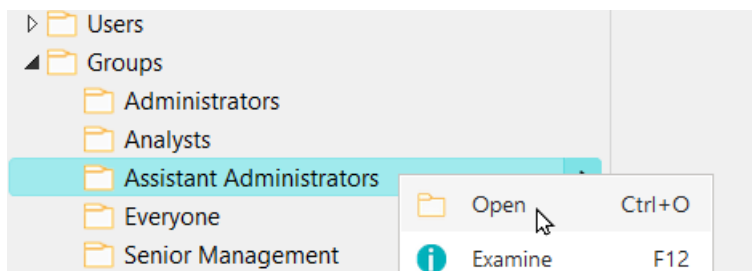
This prompts the user to change their Administrator assigned password. Should a user subsequently forget their password, it can be reset by the Administrator. See [Managing passwords](#) on page 32 for details.

## Adding users to a user group

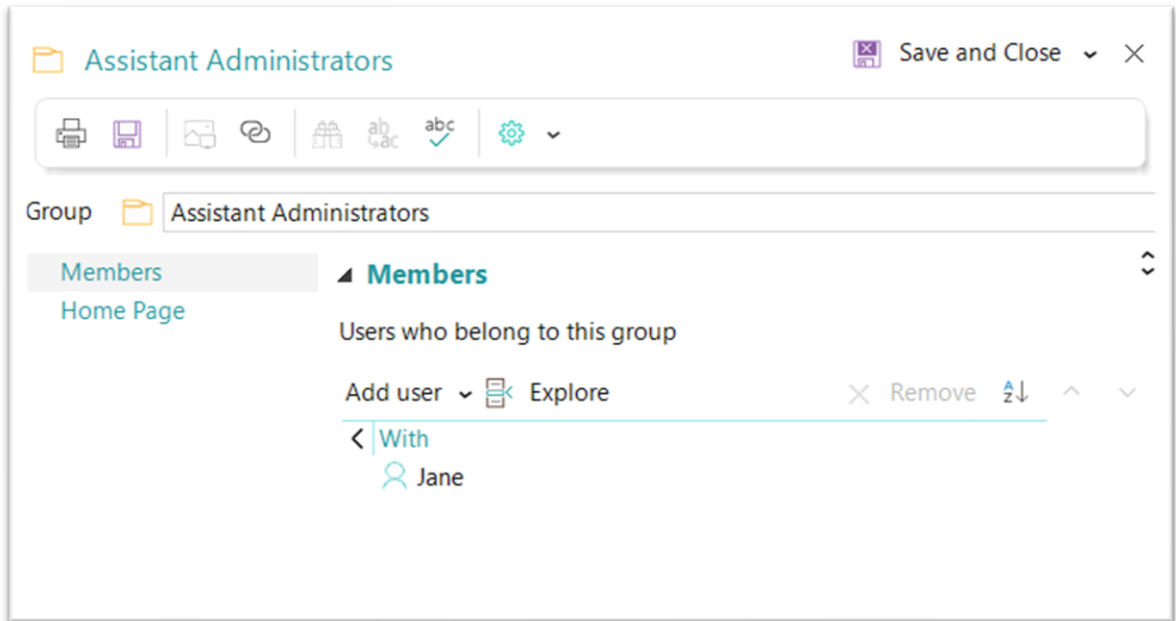
When you add users to a user group, they become members of that user group, and inherit their permissions from it. See [About users, user groups and permissions](#) on page 7 for more information.

**Task 3** To add users to user groups:

1. In the Explorer Bar, under **Themes**, under **Groups**, right-click the group, and then click **Open**.



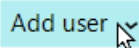
This displays the user group's definition as a tab in the workspace. The **Members** field lists the users who are members of the user group.



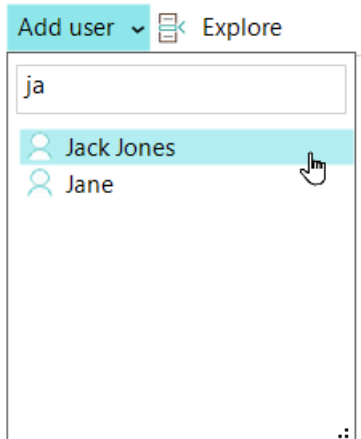
2. Add additional users to the **Members** field.

You can add users in the following ways:

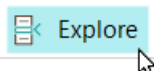
- Click **Add user**, and then select a user from a drop-down list of all users.



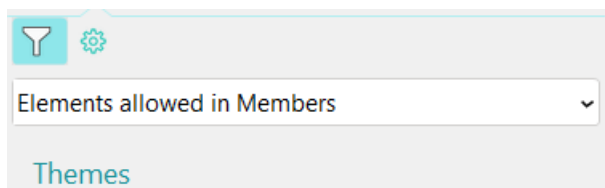
You can filter this list, for example:



- Click **Explore** to apply a filter to the Explorer Bar.

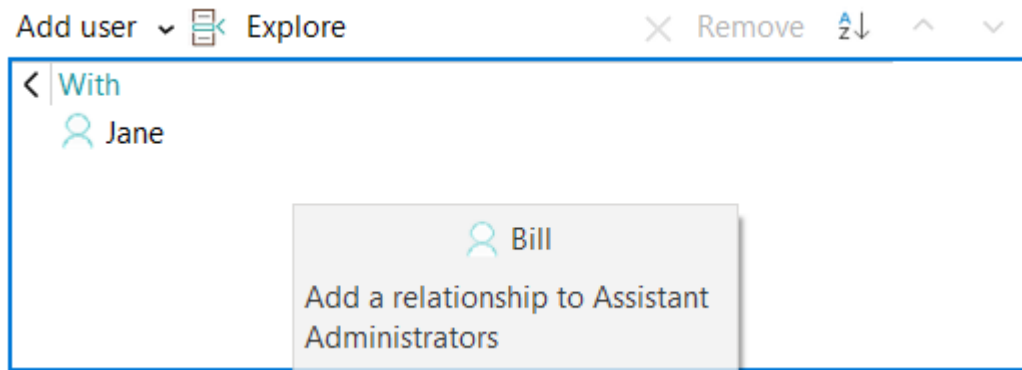


This applies the **Elements allowed in Members** filter to the Explorer Bar:

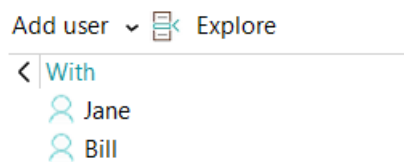


You can then see suitable elements and drag them into the **Members** field.

- Without using the **Explore** button to filter the Explorer Bar, drag a user element from the Explorer Bar into the **Members** field.



When you drop the user, they are added to the user group:



---

**Note:** Opening a **Groups** element's definition tab and using its **Member** field is the recommended method of populating user groups with users. However, you can open a user's **Permissions** tab and manage their user group membership. See the [last bullet point](#) (page 23) in the description of the **Groups and Users Can** column.

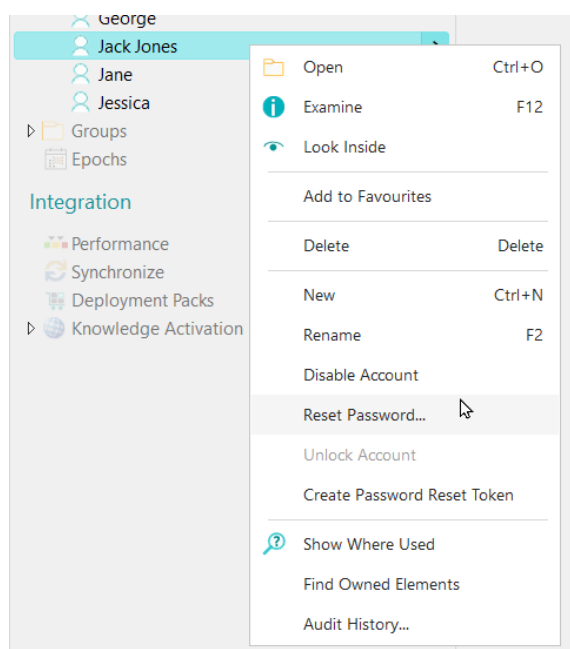
---

## Managing passwords and disabling accounts

Members of the **Administrators** group can right-click a user, and then, from the shortcut menu (shown in the following image):

- Reset users' passwords.
- Disable users' accounts to prevent access. Administrators can subsequently unlock disabled accounts.





---

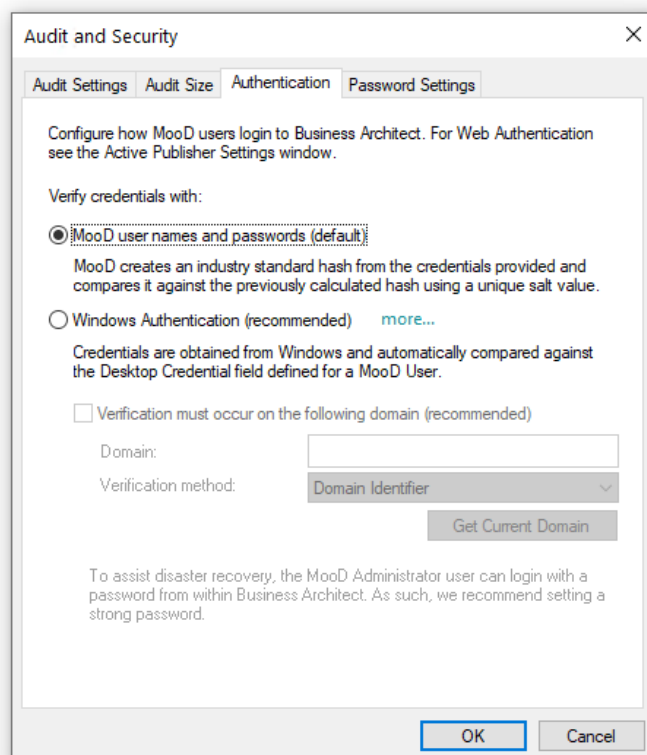
**Note:** When someone attempts to log into Business Architect using a disabled account, they get a generic message saying that their login credentials are invalid. The message does not specifically state that the account has been disabled.

---

## Configuring Single Sign-on in Business Architect

To allow users of a domain a password free experience with Business Architect, Administrators can configure options for Single Sign-on.

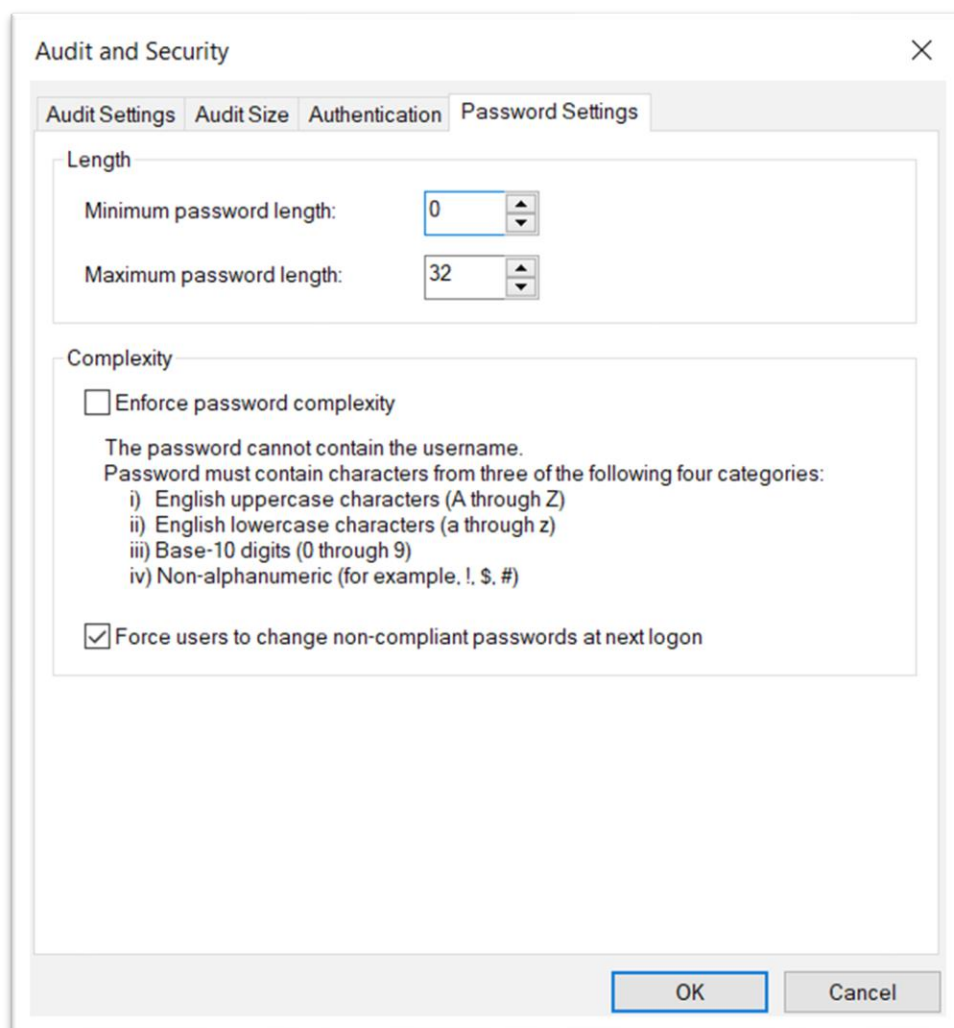
- In File->Manage Repository->Audit and Security Settings...
- Open the Authentication tab (see below)
- Here Administrators can configure varying levels of assurance that usernames are validated against a domain. Please read the details in the dialog and click the more... button for extra information.
- For full flexibility, Windows authentication for Business Architect is separately configured to the authentication method chosen for Active Enterprise.



### Password settings

Members of the **Administrators** user group can access the **Audit and Security** dialog box from the ribbon. Click **File**, point to **Manage Repository**, and then click **Audit and Security Settings** in the list of options that appears on the right.

The **Password Settings** tab on this dialog box (shown next) lets you enforce passwords and their level of security. By default, passwords are not enforced.



(As of MooD 16.075) You can also enable Single-Sign on within the **Audit and Security** dialog's **Authentication** tab (not shown) which allows you to configure password-free Windows® Authentication for **Business Architect** and **Repository Validator**. This authentication mechanism is independent of the Active Enterprise authentication.

---

**Note:** The Administrator account is always accessible by the standard Username and Password login, as a fallback when Windows® Active Directory changes or the repository has moved domains.

---

## Managing permissions

This section covers the key tasks you will perform when managing permissions:

- [Giving user groups library permissions](#)
- [Assigning element permissions by user group](#) (page 38)

**Note:** As we recommend that you control permissions by user group and allow users to inherit their permissions from their user group membership, the tasks here refer to user groups. However, both tasks are applicable to users – the only difference is what you set the **Permissions** tab's **Effective Permissions For** control to.

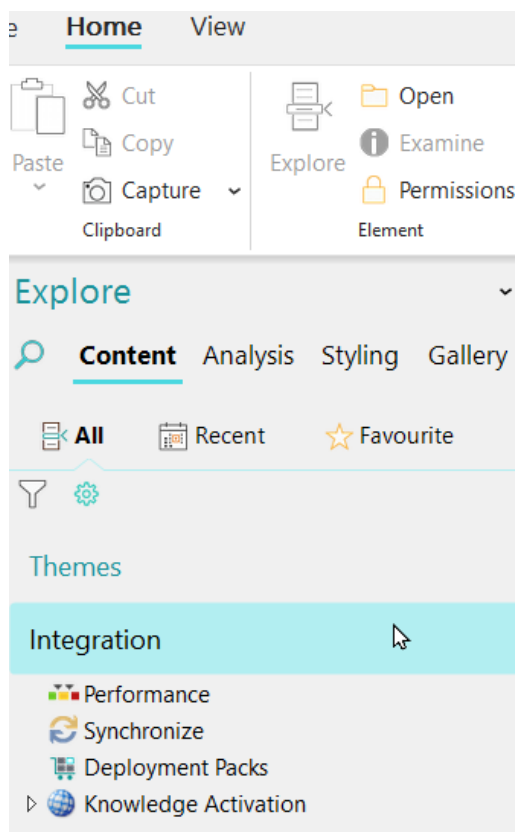
Likewise, setting field permissions is the same basic process as setting element permissions (covered in this section's second task).

### Giving user groups library permissions

See the [About users, user groups and permissions](#) topics starting on page 7 for general details on permissions, and [Library permissions](#) (page 15) for a description of the specific administrative powers you can devolve to other user groups.

**Task 4** To grant library permissions to a user group:

1. In the Explorer Bar, click **Integration (Library)**, and then, on the ribbon, click **Permissions**.



The **Permissions** tab is displayed.

**Note:** This task doesn't fully describe the **Permissions** tab's features and controls. See *The Permissions tab in Business Architect* on page 21 for full details on its user interface.

Effective Permissions For user group

Permissions Of:	Groups and Users Can:	Edit	View on Web	View in Architect
<ul style="list-style-type: none"> <li>▲ <b>Library Permissions</b></li> <li>📁 Manage Themes and...</li> <li>📁 Users and Groups</li> <li>📅 Epochs</li> <li>▶️ Matrices</li> <li>📄 Model Masters</li> <li>▶️ Threshold sets</li> <li>▶️ Queries</li> <li>▶️ Smart Columns</li> <li>▶️ Styles and Chart Palet...</li> <li>▶️ Synchronizations</li> </ul>	<ul style="list-style-type: none"> <li>Administrator can:</li> <li>Administrator can:</li> <li>Administrator can:</li> <li>Administrator can:</li> <li>Administrator can:</li> <li>Administrator can:</li> <li>Administrator can:</li> <li>Administrator can:</li> <li>Administrator can:</li> <li>Administrator can:</li> <li>Administrator can:</li> </ul>	<ul style="list-style-type: none"> <li>✓</li> <li>✓</li> <li>✓</li> <li>✓</li> <li>✓</li> <li>✓</li> <li>✓</li> <li>✓</li> <li>✓</li> <li>✓</li> <li>✓</li> </ul>		

The **Effective Permissions For** control at the top of the tab is set to the current user (**Administrator** in the preceding image).

- In the **Effective Permissions For** control, click **group**, and then select a user group from the drop-down list.

This sets the user group that you will assign library permissions for. For example:

Effective Permissions For user group

The **Groups and Users Can** column will show the selected user group and its **Edit** permission for each of the library permissions.

Permissions Of:	Groups and Users Can:	Edit
<ul style="list-style-type: none"> <li>▲ <b>Library Permissions</b></li> <li>📁 Manage Themes and...</li> <li>📁 Users and Groups</li> <li>📅 Epochs</li> <li>▶️ Matrices</li> <li>📄 Model Masters</li> <li>▶️ Threshold sets</li> <li>▶️ Queries</li> <li>▶️ Smart Columns</li> <li>▶️ Styles and Chart Palet...</li> <li>▶️ Synchronizations</li> </ul>	<ul style="list-style-type: none"> <li>Analysts can:</li> <li>Analysts can:</li> <li>Analysts can:</li> <li>Analysts can:</li> <li>Analysts can:</li> <li>Analysts can:</li> <li>Analysts can:</li> <li>Analysts can:</li> <li>Analysts can:</li> <li>Analysts can:</li> <li>Analysts can:</li> </ul>	<ul style="list-style-type: none"> <li>🔒</li> <li>🔒</li> <li>🔒</li> <li>✓</li> <li>🔒</li> <li>✓</li> <li>✓</li> <li>🔒</li> <li>🔒</li> <li>🔒</li> <li>🔒</li> </ul>

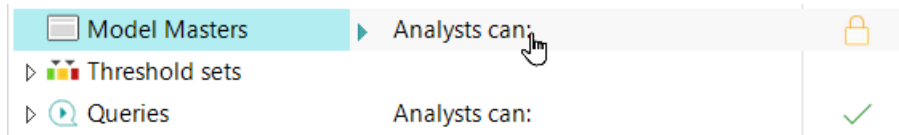
---

**Note:** You can set the **Effective Permissions For** control to a user, and then assign library permissions to that user for groups or items within a library (not the entire library). However, we recommend that you assign permissions by user group, and allow users to inherit their permissions from their user group membership.

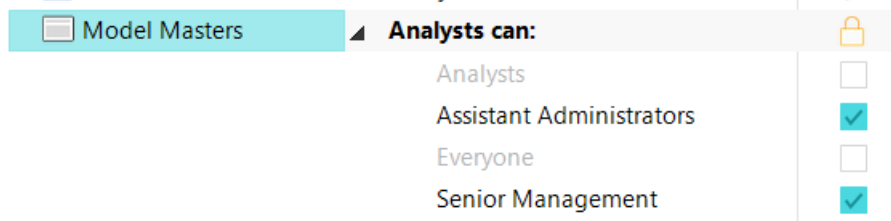
---

3. Click the library permission that you want to set.

For example:



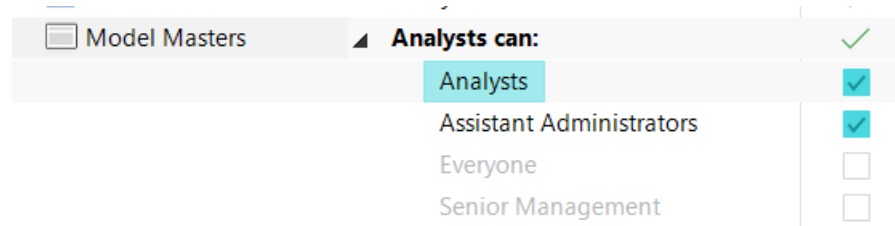
This expands to show its setting for all user groups. For example:



You can set library permissions for all user groups, not just for the user group selected in the **Effective Permissions For** control. However, the collapsed view always shows the setting for the currently selected user group.

4. Click the check boxes to grant or remove a permission.

For example, when comparing the following image to the previous image, the permission has been removed from the **Senior Management** user group, but granted to the **Analysts** user group.



Permissions are saved as soon as they are applied. You do not need to explicitly save changes.

---

**Note:** Some libraries, for example **Queries**, can be further organized into groups, with each group inheriting from its parent group within the library. You can set the **Edit** permission for each grouping within such a library. In addition, the **Manage permissions** permission may be available. See [Library permissions](#) on page 15 for full details.

---

## Assigning element permissions by user group

See the [About users, user groups and permissions](#) topics starting on page 7 for general details on permissions, and [Element permissions](#) (page 12) for details on the actual permissions you can assign to elements.

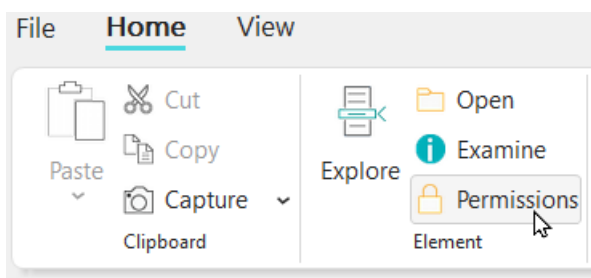
**Note:** The basic process in this task is also applicable to setting field permissions. Indeed, when you set element permissions, the **Permissions** tab also lists the field permissions from the element’s theme, and the current user or user group’s library permissions. The **Permissions** tab lets you manage all of these at once.

**Task 5** To assign element permissions by user group:

1. In the Explorer Bar, click the element that you want to set permissions for.  
This selects (highlights) the element as shown in the following image. You will be able to set permissions for the selected element and its descendants.

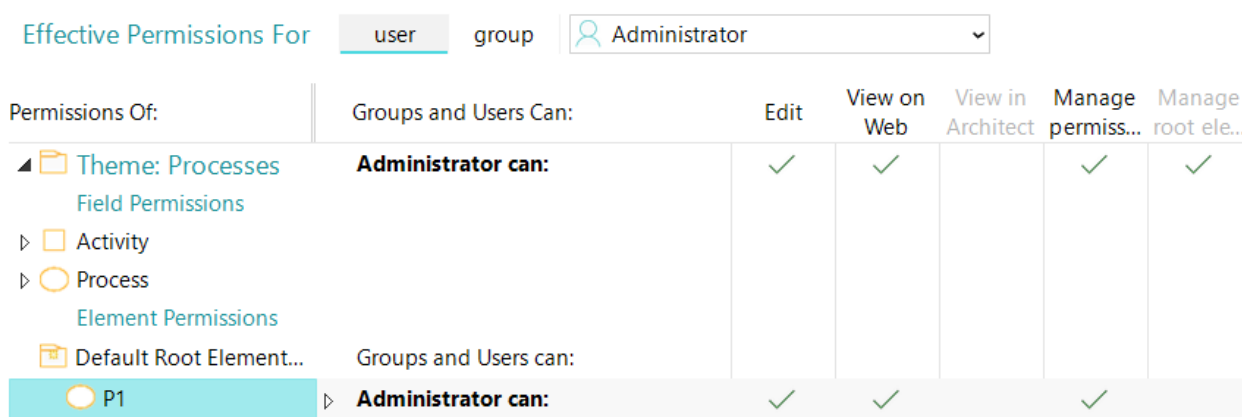


2. On the ribbon, on the **Home** tab, in the **Element** group, click **Permissions**.



The **Permissions** tab is displayed.

**Note:** This task does not fully describe the **Permissions** tab’s features and controls. See *The Permissions tab in Business Architect* on page 21 for full details.

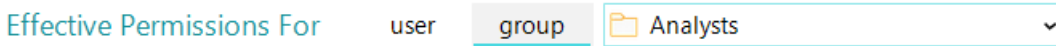


The **Effective Permissions For** control at the top of the tab is set to the current user (**Administrator** in the preceding image).

**Note:** You can also access the **Permissions** tab by clicking the **Padlock** icon on an element’s **Examine** pane. See *Displaying the Permissions tab* on page 21 for details.

3. In the **Effective Permissions For** control, click **group**, and then select a user group from the drop-down list.

This sets the user group that you will set element permissions for. For example:



The **Groups and Users Can** column will show the selected user group and its element permissions for the current element and its descendants.

Permissions Of:	Groups and Users Can:	Edit	View on Web	View in Architect	Manage permis...
<ul style="list-style-type: none"> <li>Theme: Processes                             <ul style="list-style-type: none"> <li>Field Permissions</li> <li>Activity</li> <li>Process                                     <ul style="list-style-type: none"> <li>Element Permissions</li> <li>Default Root Element...</li> <li><b>P1</b></li> </ul> </li> </ul> </li> </ul>	<b>Analysts can:</b>		<input checked="" type="checkbox"/>		
	Groups and Users can:				
	<b>Analysts can:</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		

**Note:** You can set the **Effective Permissions For** control to a user, and then assign element (or field) permissions to that user. However, we recommend that you assign permissions by user group and allow users to inherit their permissions from their group membership. Nevertheless, the process covered in this task is equally applicable to users.

- Click in the selected element's **Groups and Users Can** column, or on one of its permissions.



What happens next depends on whether the element's permissions are inherited or explicitly set:

- If explicitly set (as indicated by the user group name being in a bold font), the section expands to show the permissions settings for a number of user groups. For example:

<b>P1</b>	<b>Analysts can:</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
	Administrators	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Analysts	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Everyone	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	<a href="#">Add groups</a>			
	<a href="#">Add a user</a>			

- If inherited, the section expands to give you an **Override** command, and a link to where the element's permissions are inherited from (**Root** in the image). For example:

P1	Analysts can:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
	<a href="#">Override.</a> Permissions are inherited from <a href="#">Root</a>			



If you click **Override**, the section expands to show the permissions check boxes (in effect it will look like the image in the first bullet point).

You can set element permissions for all user groups (and users) and not just for the user group selected in the **Effective Permissions For** control. However, the collapsed view always shows the setting for the currently selected user group.

**Note:** If the selected element has descendants, you can click the element and see them. You can then select a descendant element and set its permissions

▲ ○ P1	<b>Analysts can:</b>	✓
○ P1A	Analysts can:	✓
○ P1B	Analysts can:	✓
▲ ○ P1C	Analysts can:	✓
	<a href="#">Override.</a> Permissions are inherited from <a href="#">P1</a>	
○ P1C1	Analysts can:	✓
○ P1D	Analysts can:	✓

5. Click the boxes to set or remove a permission.

Permissions are saved as soon as they are applied. You do not need to explicitly save changes.

Also, you can use the ribbon commands:

- **Make descendants inherit permissions** and **Remove overridden permissions** to control inheritance.
- **Pickup** and **Apply** to copy permissions from one element to another.

See *The Permissions tab in Business Architect* on page 21 if you need guidance on the user interface, and *Element permissions* (page 12) if you need information on the actual permissions and inheritance.