

# MooD 15

User Management and Permissions Guide

Document Number: MooD15UMP01

© MooD Enterprises Ltd., all rights reserved**.** 31/05/12

##### Notice of Copyright and Trademarks

MooD 15 User Management and Permissions Guide

® MooD, MooD Smarter Decisions, Performance Activation, Synchronization Activation Technology and Knowledge Map are registered trademarks of MooD Enterprises 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.

© MooD Enterprises 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.

2

**Contents**

[Introduction 5](#_bookmark0)

[Changes in MooD 15 5](#_bookmark1)

[About users, user groups and permissions 6](#_bookmark2)

[Users and user groups 6](#_bookmark3)

[The Users and Groups themes 7](#_bookmark5)

[Types of permission 9](#_bookmark6)

[Element permissions 10](#_bookmark7)

[Element permission inheritance 11](#_bookmark9)

[Root element permissions 11](#_bookmark10)

[Element ownership 12](#_bookmark11)

[Library permissions 12](#_bookmark12)

[Inheritance of library permissions 14](#_bookmark14)

[Precedence of library permissions over element permissions 14](#_bookmark15)

[Field permissions 14](#_bookmark16)

[Precedence between element and field permissions 15](#_bookmark18)

[The Anonymous user 15](#_bookmark19)

[User management on the web 16](#_bookmark20)

[The Permissions tab in Business Architect 17](#_bookmark21)

[Displaying the Permissions tab 17](#_bookmark22)

[About the Permissions tab 18](#_bookmark23)

[Managing users and user groups 22](#_bookmark26)

[Creating user groups 22](#_bookmark27)

[Creating users 23](#_bookmark29)

[Adding users to a user group 25](#_bookmark31)

[Managing passwords and disabling accounts 27](#_bookmark33)

[Password settings 28](#_bookmark34)

[Managing permissions 29](#_bookmark35)

3

[Giving user groups library permissions 29](#_bookmark36)

[Assigning element permissions by user group 31](#_bookmark38)

**Tasks**

[**Task 1** To create a user group: 22](#_bookmark28)

[**Task 2** To create a user 23](#_bookmark30)

[**Task 3** To add users to user groups 25](#_bookmark32)

[**Task 4** To grant library permissions to a user group 29](#_bookmark37)

[**Task 5** To assign element permissions by user group 32](#_bookmark39)

## Figures

[**Figure 1** Users, user groups and permissions 7](#_bookmark4)

## Tables

[**Table 1** Element permissions 10](#_bookmark8)

[**Table 2** Library permissions 13](#_bookmark13)

[**Table 3** Field permissions 14](#_bookmark17)

[**Table 4** Permissions and what they can apply to 20](#_bookmark25)

4

# 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](#_bookmark2) (page [6](#_bookmark2))

Explains MooD users, user groups and permissions, and how they function within Business Architect.

* [The **Permissions** tab in Business Architect](#_bookmark21) (page [17](#_bookmark21))

The **Permissions** tab is a single point for permissions management. This section outlines its functionality and behaviour.

* [Managing users and user groups](#_bookmark26) (page [22](#_bookmark26)) and [Managing permissions](#_bookmark35) (page [29](#_bookmark35))

Instructions covering key tasks. These tasks assume knowledge of what is covered in the preceding sections.

### 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.
* There is an **Anonymous** user.
* Action panels for web based user administration have been introduced. All are covered or introduced in this guide.

**Note:** MooD 15’s *Getting Started Guide* includes a list of new features covering all product areas. This is available as a PDF from Business Architect’s **File** tab.

5

# About users, user groups and permissions

The relationship between users, user groups and permissions, together with the types of permission available and their application and inheritance, form a permission’s architecture that should provide your users with the facilities they need to achieve their goals, and at the same time provide the repository security you may require. To help you understand the permission’s model employed by MooD, this section includes the following:

* [Users and user groups](#_bookmark3) (page [6](#_bookmark3))

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.

* [Types of permission](#_bookmark6) (page [9](#_bookmark6))

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](#_bookmark7) (page [10](#_bookmark7))

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](#_bookmark12) (page [12](#_bookmark12))

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](#_bookmark16) (page [14](#_bookmark16))

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](#_bookmark19) (page [15](#_bookmark19))

Outlines this default user that lets you provide limited, login free access to a repository through the web.

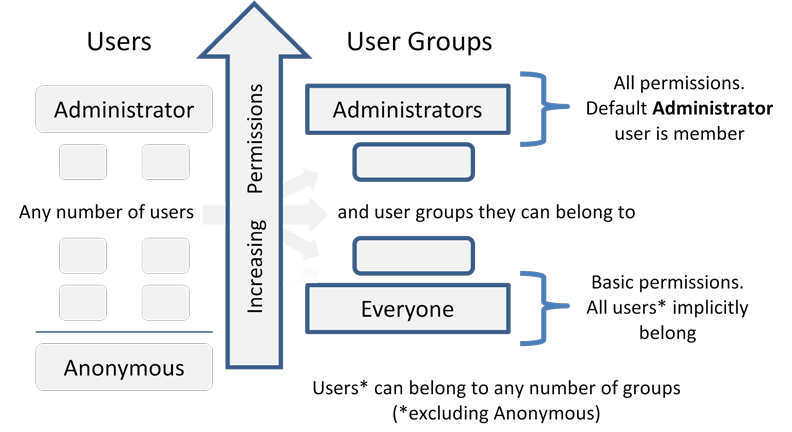
* [User management on the web](#_bookmark20) (page [16](#_bookmark20))

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.

6



##### 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*](#_bookmark19)[*Anonymous user*](#_bookmark19) on page [15](#_bookmark19) 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 are assigned to user groups, but can also be assigned to individual users if required.
* 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.

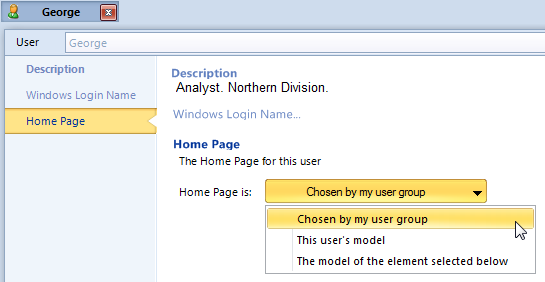
#### The Users and Groups themes

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

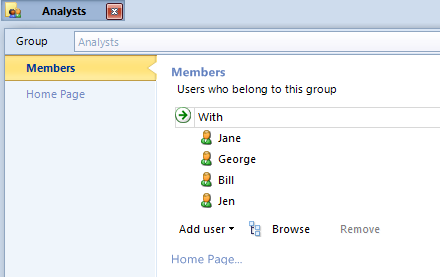
**Users** elements have the following default fields:

##### Description.

7

* **Windows Login Name**. The Active Directory domain and user login name for use within Active Publisher.
* **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 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. For example:

**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.

8

### 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 also 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*](#_bookmark7) on page [10](#_bookmark7) 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*](#_bookmark12) on page [12](#_bookmark12) 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 or Web Publisher. See [*Field permissions*](#_bookmark16) on page [14](#_bookmark16) 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. |

9

### Element permissions

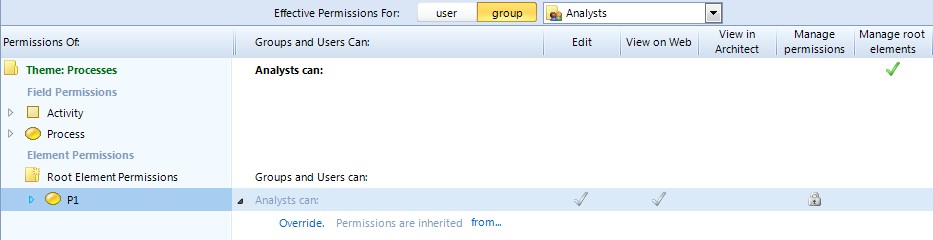
PermissionsTabHeader.pngBusiness Architect’s **Permissions** tab lists five permissions (the last five columns in the next image):

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

|  |  |
| --- | --- |
| **Permission** | **Description** |
| **Edit** | Grants permission to manage an element. This includes editing, creating child elements, renaming, moving and deleting. |
| **View on Web** | The element’s model can be viewed in a browser by means of Active Enterprise.  **Note:** This permission can also apply to fields. This controls what is presented to users, and what is output by Web Publisher (element permissions do not affect Web Publisher but field permissions can). See [*Field permissions*](#_bookmark16) on page [14](#_bookmark16) for details. |
| **Manage Permissions** | 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*](#_bookmark16) on page [14](#_bookmark16) and [*Root element permissions*](#_bookmark10) (page [11](#_bookmark10)) 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.

ColouredTick.pngColouredPadlock.pngThere are two types of tick, and two types of padlock:

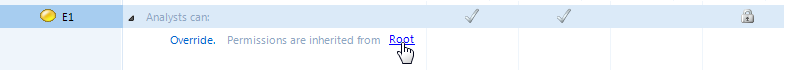
|  |
| --- |
| Greyed icons indicate that the element has inherited its permissions. |
| Coloured icons indicate that the element’s permissions have been explicitly set. |

GreyedTick.pngGreyedPadlock.png

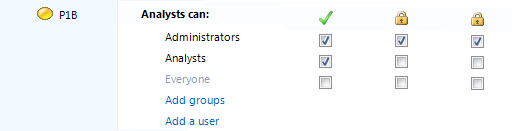
10

#### 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:



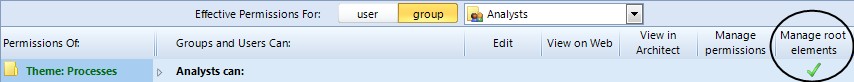
To help you manage element inheritance, the ribbon includes the following commands:

 MakeDescendantsInheritPermissionsButton.png

 RemoveOverridenPermissionsButton.png

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

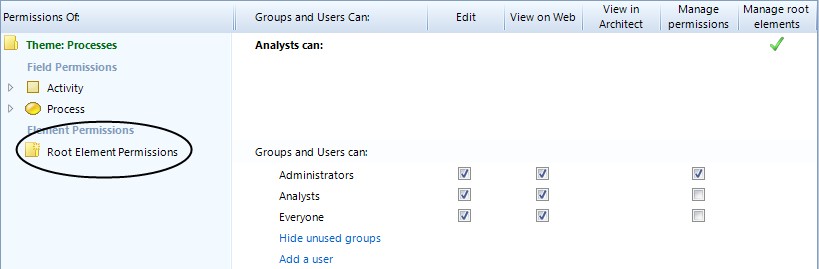
#### Root element permissions

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.

11



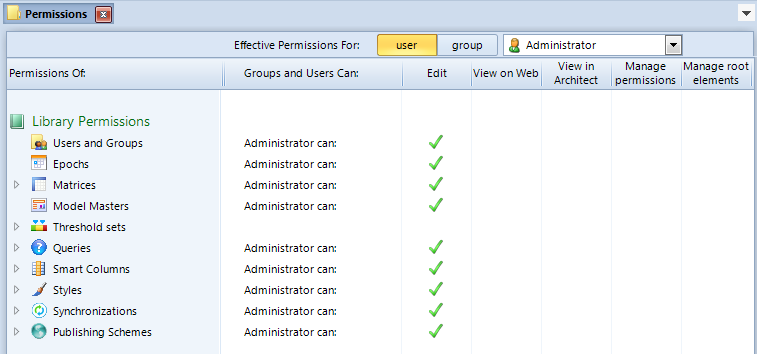
Due to inheritance, all elements in a theme will inherit the root element permissions unless they are specifically overridden.

#### Element ownership

MooD has the concept of element ***ow******nership***. 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 the library permissions. This is followed by a table describing them.

12

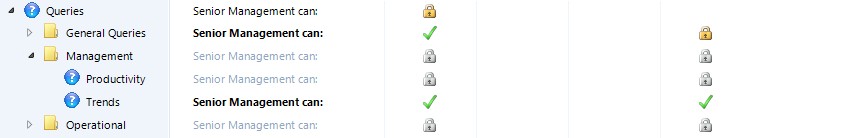
|  |  |
| --- | --- |
| **Library** | **Description** |
| **Users and Groups** | Manage users and user groups. This includes adding, modifying or deleting users and user groups, but excludes managing **Administrator** users and assigning library permissions. |
| **Epochs** | Manage epochs. This is a 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. |
| **Matrices** | Manage matrices. |
| **Model Masters** | 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. |
| **Threshold sets** | Manage individual Thresholds. You cannot set permissions that cover all Thresholds (this is why there is no tick in the Threshold sets’ **Edit** column in the previous screenshot). |
| **Queries** | Manage queries. |
| **Smart Columns** | Manage Smart Columns. |
| **Styles** | Manage styles. |
| **Synchronizations** | Manage synchronizers (SAT). |
| **Publishing Schemes** | Manage Web Publishing schemes. Publishing schemes are listed individually. They cannot be organized into groups. |

##### 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.

The other permissions (the **View on Web**, **View in Architect** and **Manage Root Elements**

columns) do not apply to libraries.

13

#### 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*](#_bookmark9) on page [11](#_bookmark9) 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** |
| **Edit** | Grants permission to manage the field data.  **Note:** 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. |
| **View on Web** | The field can be viewed in a web browser by means of Active Enterprise, or published through Web Publisher.  **Note:** In the previous release, the equivalent of the **View in Architect** permission within a theme governed what was included in Web Publisher’s output. This is now controlled by the **View on Web** field permission. Because of this, user group specific outputs can be created. |
| **View in Architect** | The field can be viewed in Business Architect. |

##### Table 3. Field permissions

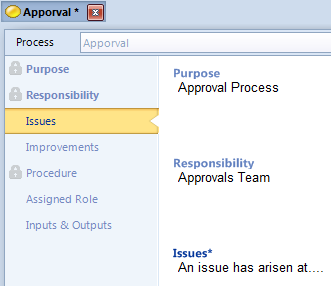
User groups and users can be applied to field permissions. Again, we recommend that you control field permissions by user group, and let individual users inherit from their user group membership.

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, Active Enterprise and Web Publisher, so you need to explicitly deny the relevant **View** permissions for your different user groups (clear the check boxes).

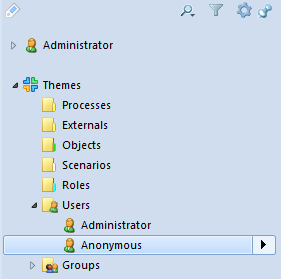
14

#### 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

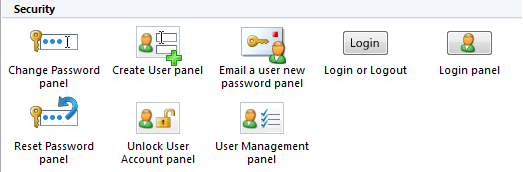
MooD now includes an **Anonymous** user by default.

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.

15

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.

16

# The Permissions tab in Business Architect

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

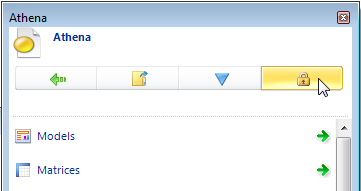
### Displaying the Permissions tab

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

##### PermissionsButton.pngPermissions.

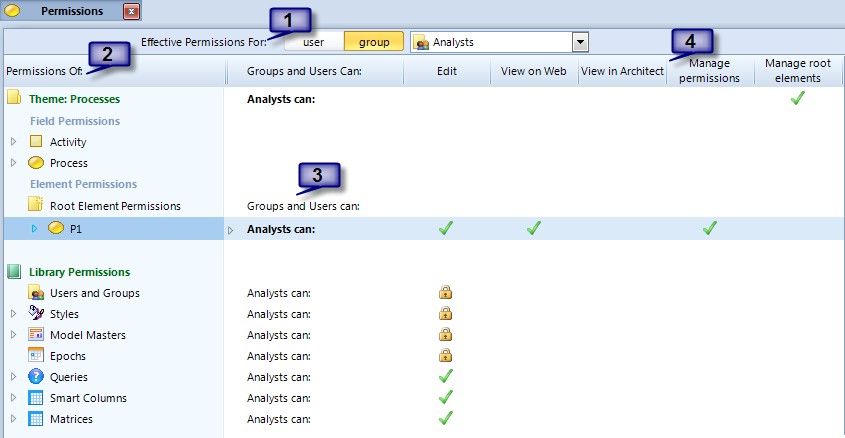
* In an element’s Examine pane, click the **Padlock** button.



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

17

### 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

EffectivePermissionsForControl.png**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.

1. 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.
2. 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:

* + InheritedFromWithRootShort.pngFor the current user or user group, see where an element or field inherits its permissions from. For example:

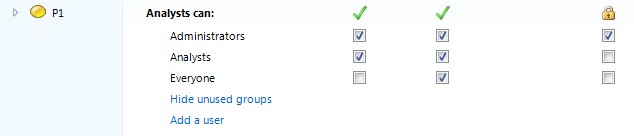
18

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.

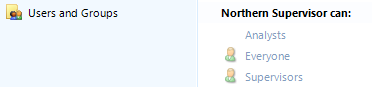
* Override inherited element and field permissions. The **Override** command is shown in the previous image, and an example of what you get when you use this option is shown in the next image. When user or user group permissions are explicitly set rather than inherited, that is, overridden, the user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

19

you open a user group’s definition page, and then add users directly to its **Members** field. See [*Adding users to a user group*](#_bookmark31) on page [25](#_bookmark31) for instructions.

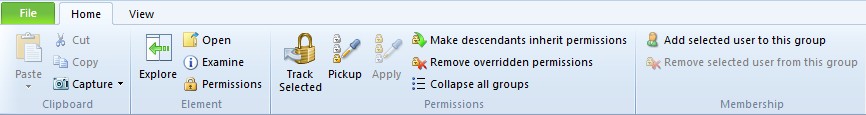
1. The **Permissions** columns. These five columns are the permissions you can set. Each permission is only applicable to certain items in the **Permissions Of** column (**2**) — an empty column means it’s not applicable. The following table shows what permissions apply to what.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Permissions** | | | | | |
|  | **Edit** | **View on Web** | **View in Architect** | **Manage Permissions** | **Manage Root Elements** |
| **Theme** |  |  |  |  | ColouredTick.png |
| **Field** | ColouredTick.png | ColouredTick.png | ColouredTick.png |  |  |
| **Element** | ColouredTick.png | ColouredTick.png |  | ColouredTick.png |  |
| **Library** | ColouredTick.png |  |  | ColouredTick.png |  |

##### 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.

|  |  |
| --- | --- |
| GreyedTick.png GreyedPadlock.png | Greyed icons indicate inherited permissions. |
| ColouredTick.png ColouredPadlock.png | 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:

##### TrackSelectedButton.pngTrack 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.

20

In the Explorer Bar, under **Libraries**, if you click **Synchronize** or **Web Publish**, their tabs open. **Track Selected** does not synchronize with these items.

* PickupButton.pngApplyButton.png**Pickup** and **Apply**

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

##### MakeDescendantsInheritPermissionsButton.pngMake 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.

##### RemoveOverridenPermissionsButton.pngRemove 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.

##### CollapseAllGroupsButton.pngCollapse all groups

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

##### AddSelectedUserToThisGroup.pngAdd selected user to this group and Remove selected user from this group

RemoveSelectedUserFromThisGroup.png

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.

21

# Managing users and user groups

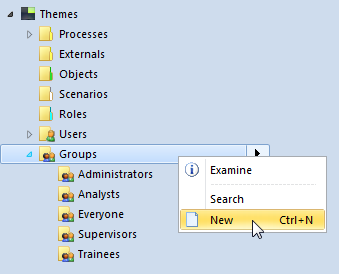
This section covers the key tasks you will perform when setting up users and user groups. It covers:

* + [Creating user groups](#_bookmark27)
  + [Creating users](#_bookmark29)
  + [Adding users to a user group](#_bookmark31)
  + [Managing passwords and disabling accounts](#_bookmark33)

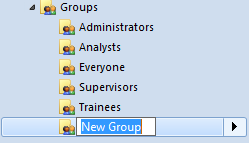
### Creating user groups

As covered in [*Users and user groups*](#_bookmark3) on page [6](#_bookmark3), Business Architect creates two default user groups: **Administrators** and **Everyone**. Typically, you create user groups for each role within your MooD solution.

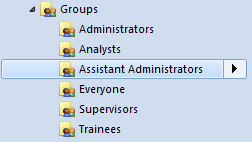
**Task 1** To create a user group:

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.



22

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

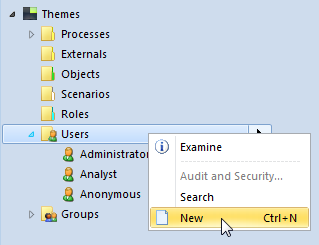
You can now:

* + Add users to the user group. See [*Adding users to a user group*](#_bookmark31) on page [25](#_bookmark31).
  + Assign library permissions to the user group. See [*Giving user groups library permissions*](#_bookmark36) on page [29](#_bookmark36).
  + Assign the user group to element permissions. See [*Assigning element permissions by user group*](#_bookmark38) on page [31](#_bookmark38).

### Creating users

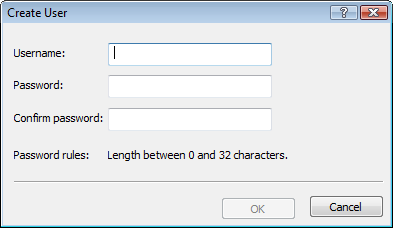
As covered in [*Users and user groups*](#_bookmark3) on page [6](#_bookmark3), Business Architect creates two default users: **Administrator** and **Anonymous**. You will need to create a user for each person wishing to log into the MooD solution.

**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.

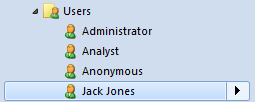
23



1. 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:  CreateUserPasswordWarning.png  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*](#_bookmark33) on page [27](#_bookmark33) for more details. |

1. Click **OK** to create the user. The user is listed under **Users**.



24

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*](#_bookmark31) on page [25](#_bookmark31) 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:  WelcomeToMooD.png  This prompts the user to change their Administrator assigned password. Should a user subsequently forget their password, it can be reset by the Adminstrator. See [*Managing*](#_bookmark33)[*passwords*](#_bookmark33) on page [27](#_bookmark33) 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*](#_bookmark2) on page [6](#_bookmark2) for more information.

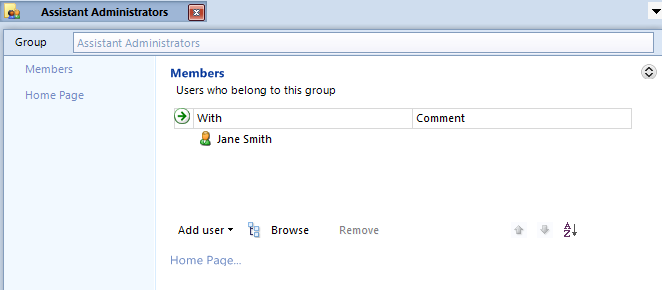
**Task 3** To add users to user groups:

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

##### AddUsersToGroupOpen.pngOpen.

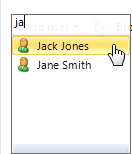
This displays the user group’s definition as a tab in the workspace. The **Members** field lists the users who are members of the user group.

25



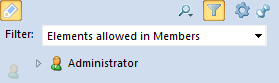
1. Add additional users to the **Members** field. You can add users in the following ways:
   * AddUserControl.pngClick **Add user**, and then select a user from a drop-down list of all users.

You can filter this list, for example:



* + BrowseButton.pngClick **Browse** to apply a filter to the Explorer Bar.

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

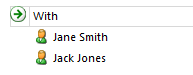


You can then see suitable elements, and drag them into the **Members** field.

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

26

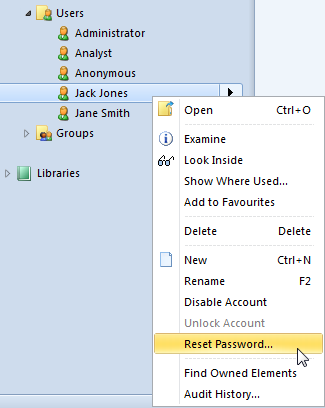


When you drop the user, they are added to the user group:

**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](#_bookmark24) (page [19](#_bookmark24)) 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):

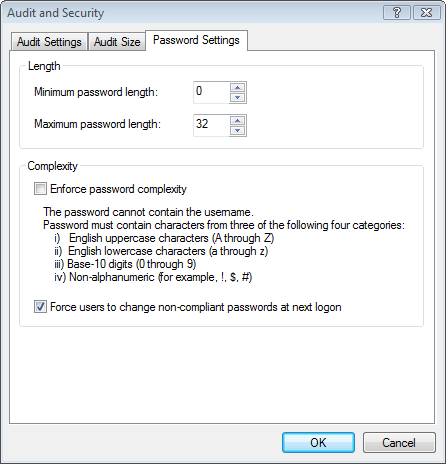
* + Reset users’ passwords.
  + Disable users’ accounts to prevent access. Administrators can subsequently unlock disabled accounts.

27

**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.

### 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.

28

# Managing permissions

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

* + [Giving user groups library permissions](#_bookmark36)
  + [Assigning element permissions by user group](#_bookmark38) (page [31](#_bookmark38))

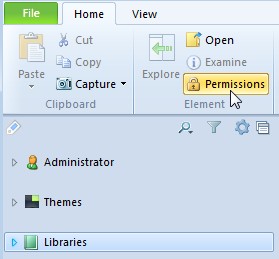
**Note:** As we recommend that you control permissions by user group and allow users to inherit their permissions from their user group membership, the tasks here refer to user groups. However, both tasks are applicable to users ─ the only difference is what you set the **Permissions** tab’s **Effective 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*](#_bookmark2) topics starting on page [6](#_bookmark2) for general details on permissions, and [*Library permissions*](#_bookmark12) (page [12](#_bookmark12)) for a description of the specific administrative powers you can devolve to other user groups.

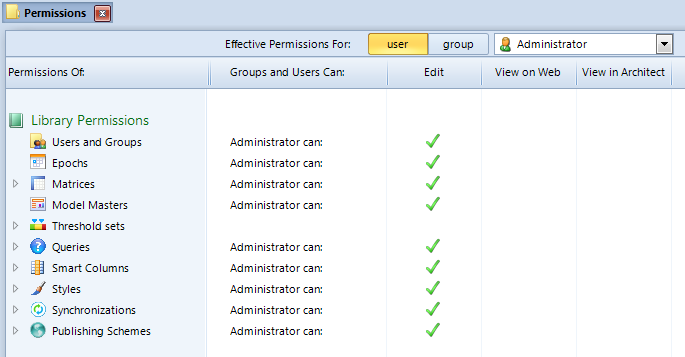
**Task 4** To grant library permissions to a user group:

1. In the Explorer Bar, click **Libraries**, 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*](#_bookmark21) on page [17](#_bookmark21) for full details on its user interface.

29

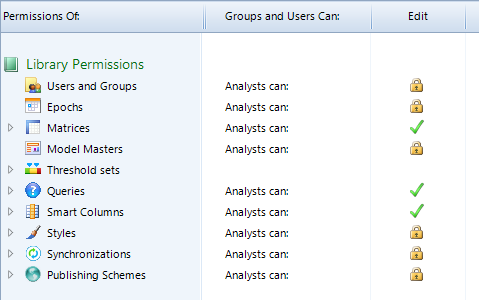


The **Effective Permissions For** control at the top of the tab is set to the current user (**Administrator** in the preceding image).

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

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

The **Groups and Users Can** column will show the selected user group and its **Edit**

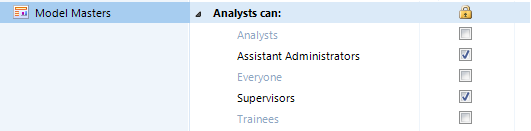
permission for each of the library permissions.

**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.

30

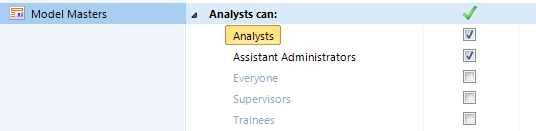
1. Click the library permission that you want to set. For example:



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.

1. 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 **Supervisors** 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*](#_bookmark12) on page [12](#_bookmark12) for full details.

### Assigning element permissions by user group

See the [*About users, user groups and permissions*](#_bookmark2) topics starting on page [6](#_bookmark2) for general details on permissions, and [*Element permissions*](#_bookmark7) (page [10](#_bookmark7)) for details on the actual permissions you can assign to elements.

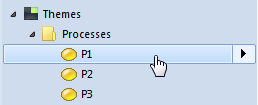
**Note:** The basic process in this task is also applicable to setting field permissions.

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.

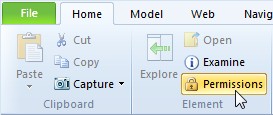
31

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

1. In the Explorer Bar, click the element that you want to set permissions for.

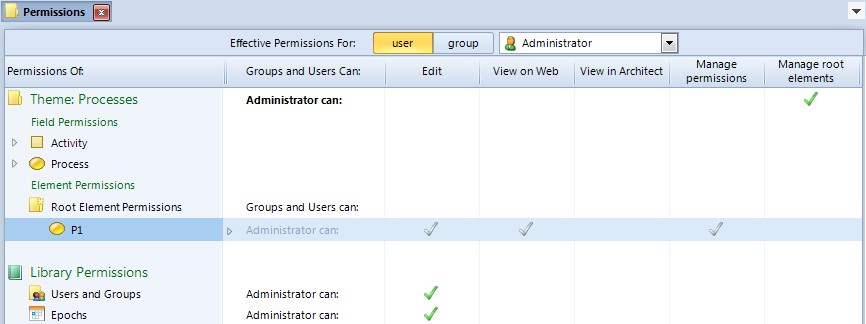
This selects (highlights) the element as shown in the following image. You will be able to set permissions for the selected element and its descendants.

1. 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*](#_bookmark21) on page [17](#_bookmark21) 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).

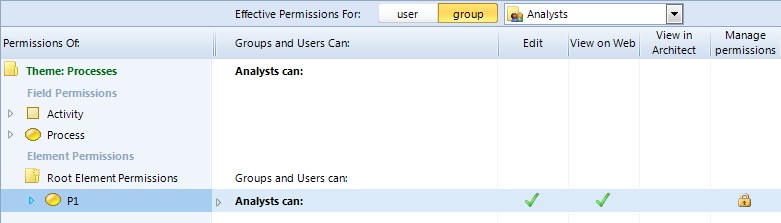
**Note:** You can also access the **Permissions** tab by clicking the **Padlock** icon on an element’s **Examine** pane. See [*Displaying the Permissions tab*](#_bookmark22) on page [17](#_bookmark22) for details.

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

EffectivePermissionsForSetToGroup.pngThis 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.

32



**Note:** You can set the **Effective Permissions For** control to a user, and then

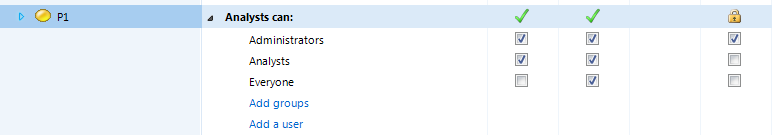
assign element (or field) permissions to that user. However, we recommend that you assign permissions by user group and allow users to inherit their permissions from their group membership. Nevertheless, the process covered in this task is equally applicable to users.

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

TaskElementRevealPermissions.png

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:



* + 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:

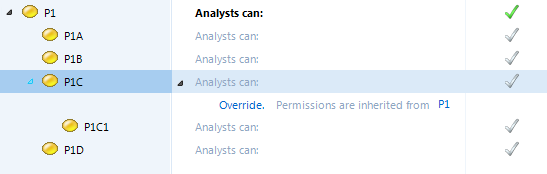
ElementsTaskInheritLink.png

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.

33

**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.



1. 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*](#_bookmark21) on page [17](#_bookmark21) if you need guidance on the user interface, and [*Element permissions*](#_bookmark7) (page [10](#_bookmark7)) if you need information on the actual permissions and inheritance.

34