User Security in UML Models

Enterprise Architect is an intuitive, flexible and powerful UML analysis and design tool for building robust and maintainable software.

This booklet explains the User Security feature of Enterprise Architect.

Enterprise Architect - User Security in UML Models

Printed: May 2010

Publisher

Sparx Systems

Managing Editor

Geoffrey Sparks

Technical Editors

Geoffrey Sparks
Howard Britten

Special thanks to:

All the people who have contributed suggestions, examples, bug reports and assistance in the development of Enterprise Architect. The task of developing and maintaining this tool has been greatly enhanced by their contribution.

Table of Contents

Foreword

This user guide provides an introduction to the User Security feature of Enterprise Architect.

User Security

What is User Security in Enterprise Architect?

User security in Enterprise Architect can be used to limit the access to update functions within the model. Elements can be locked per user or per group. Where user security is enabled a password is required to log in to the model. Security in Enterprise Architect is not designed to prevent unauthorized access; rather it is intended as a means of improving collaborative design and development by preventing concurrent editing and limiting the possibility of inadvertent model changes by users not designated as model authors.

With workflow administration permissions 16, you can also develop workflow scripts 21 (using the Scripter window - see *Using Enterprise Architect - UML Modeling Tool*). Workflow scripts validate and control 21 user input.

User Security Basics

User security is available in the Corporate, Business and Software Engineering, System Engineering and Ultimate editions of Enterprise Architect. It offers two policies: the standard security mode and the rigorous security mode.

- In the standard security mode all elements are unlocked and, as necessary, a user can set a user or group lock on any element or set of elements in order to make changes and protect those changes.
- Under the rigorous security mode an Enterprise Architect model is read-only and nothing in the model can be edited until explicitly checked out with a user lock.

For more detailed information on the security policies see the *Security Policy* 6 topic.

User Security Tasks

A number of security tasks can only be performed by users with Administrative rights to the model. These tasks include:

- Security Policy 6
- Enable Security 4
- Maintain Users 7
- Import User IDs From Active Directory 9
- Change User Passwords 25
- Assign User To Groups 11
- View All User Permissions 13
- Maintain Groups 14
- View and Manage Locks 18
- Password Encryption 19 (for the third-party DBMS connection password; only available for Oracle and SQL Server Repositories for Enterprise Architect releases prior to 7.1)
- Create Workflow Scripts. 21

Other Security tasks can be performed by users who do not have Administrative rights. These tasks include:

- Lock Model Elements 27
- Lock Packages 29
- Apply a User Lock 30
- Identify Who Has Locked An Object 32
- Locked Element Indicators 31
- Manage Your Own Locks 33
- Change Your Own Password 25

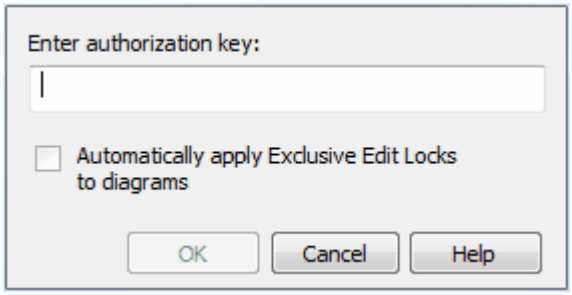
Notes:

- User security is not enabled by default in Enterprise Architect; you must enable it 4 first.
- For a number of operations in Enterprise Architect, if security is enabled a user must have the appropriate user or group access permission to perform the operation. However, if security is not enabled, the user does not have to have access permissions. See the *List of Available Permissions* 16 topic.

1 Enable Security

User security is not enabled by default in Enterprise Architect. To enable security for a project in Enterprise Architect for the first time, follow the steps below.

1. Access the *Registered Users* section of the Sparx Systems website (http://www.sparxsystems.com/registered/reg_ea_corp_ed.html), and obtain the Authorization Key. (You must have the Registered Users login and password to access this web site.)
2. In Enterprise Architect, select the **Project | Security | Enable Security** menu option. The Enter authorization dialog displays



3. In the **Enter authorization key** field, type the authorization key from the Sparx Systems website.
4. If required, select the **Automatically apply Exclusive Edit Locks to diagrams** checkbox.

Note:

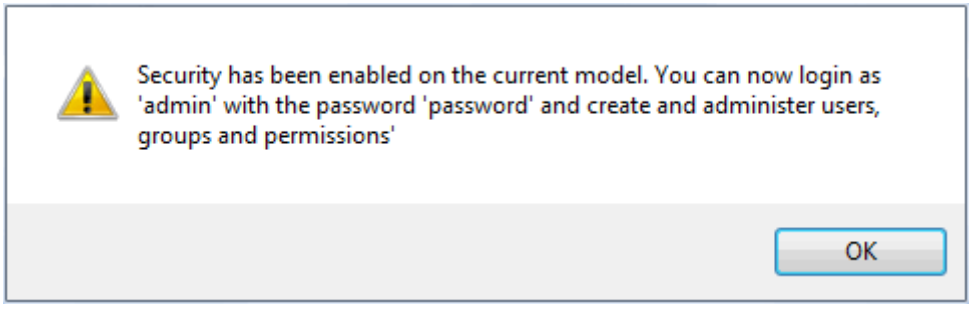
In standard (*User/Group Locking*) security mode 6, this option blocks multiple users from simultaneously attempting to modify the same diagram. As a user *modifies* a diagram, Enterprise Architect automatically applies a User Lock to the diagram, preventing any other user from modifying it. It is creating difference between the database and buffer versions of the diagram that triggers the temporary lock, and elimination of difference that releases the lock. Therefore, Enterprise Architect releases the lock when:

- The user saves the changes to the diagram, with the **Save** icon or keyboard keys
- The user undoes the last remaining action in the **Undo** list
- The user saves or discards changes via the system prompt when they close the diagram.

If the diagram already has a User Lock or Group Lock that does not exclude the current user, this lock is set aside and saved when the temporary User Lock is applied. When the temporary User Lock is released, the pre-existing lock is restored.

The option is ignored in *Require User Lock* security mode.

5. Click on the **OK** button. Security is enabled, and an Admin user and user group are created with full permissions (all access rights listed in List of Available Permissions 16) and a password of **password**.



6. Select the **Project | Security | Login as Another User** menu option, and log in as **Admin** with the initial password of **password**.

Note:

To change the Admin password, see the *Change Password* 25 topic.

7. Set up users and permissions as required.

Note:

Once security has been enabled, you must have the **Security - Enable/Disable** 16 access right to turn it off. The initial administrator automatically has this access right.

8. To disable security, click on the **Enable Security** menu option, and again type the authorization key in the Authorization dialog. Click on the **OK** button. Security is disabled.

Notes:

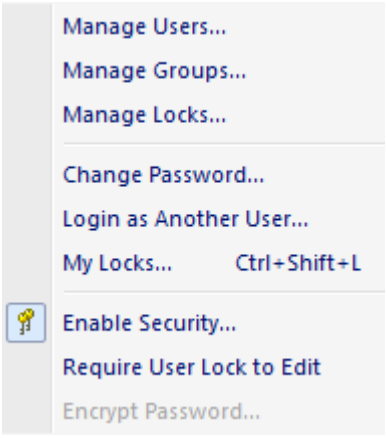
- The system prompts you to log off the project and log on again, but this is not strictly necessary.
- To re-enable security, follow the procedure above, but be aware that any changes you have made to the admin user (password and reduced access rights) are reset to **password** and full access.
- The **Automatically apply Exclusive Edit Locks to diagrams** option is not displayed when disabling security. Therefore, to toggle the setting whilst security is enabled you must disable security and re-enable it. Security settings (users, groups and permissions) and locks on elements, are NOT affected by this action.

2 Security Policy

There are two possible security policies in Enterprise Architect:

1. In the *User/Group Locking* mode, all elements and diagrams are considered unlocked and anyone can edit any part of the project. However, when you edit a diagram, package or element, you lock the element or set of elements at either the user level or group level. This mode is good for cooperative work groups where there is a solid understanding of who is working on which part of the model, and locking is used mainly to prevent further changes or to limit who has access to a part of the model.
2. The *Require User Lock* mode is more rigorous. The Enterprise Architect model is read-only - everything is locked so that nobody can edit anything unless they explicitly check out the object with a user lock. A single 'check out' function operates on a diagram to check out the diagram and all contained elements in one go. There are also functions on the context (right-click) menus of packages, diagrams and elements in the Project Browser to apply a user lock when this mode is in use. You would use this mode when there is a strict requirement to ensure only one person can edit a resource at one time. This is suitable for much larger projects where there might be less communication between users.

Toggle between these modes using the **Project | Security | Require User Lock to Edit** menu option - deselected for User/Group Locking mode, and selected for Require User Lock mode.



Notes:

- When you add new elements in Mode 1 (**Require User Lock to Edit** deselected, elements editable by default), no user lock is created automatically for the newly created element.
- When you add new elements in Mode 2 (**Require User Lock to Edit** selected, elements locked by default), a user lock is created on the new element to enable instant editing.

3 Maintain Users

If you enable security you have access to the Security Users dialog, which you can use to set up more users for your model.

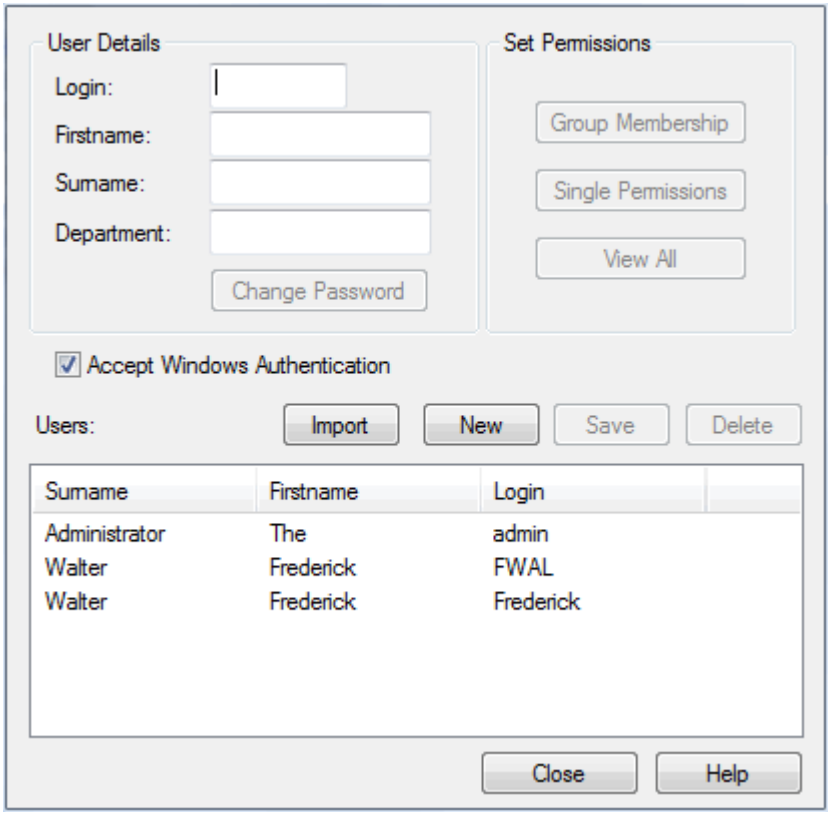
Note:

You must have **Security - Manage Users** 16 permission to maintain users, and **Change Password** 16 permission to change the password of the current user; the initial **Admin** administrator automatically has these permissions.

Set Up a User

To set up a user for your model, follow the steps below:

1. Select the **Project | Security | Manage Users** menu option. The Security Users dialog displays.



2. You can use the Security Users dialog to set up new users by providing their name and other details. You can also import user IDs from a Windows Active Directory 9, assign User IDs to groups 11, set up **Single Permissions** 12 or **View All** 13 permissions for the currently selected user.
3. To identify a new user on this dialog, click on the **New** button and type in the user's login ID, first name and last name. If required, also provide the user's department name.
4. To set the user's password, click on the **Change Password** button. The Change Password dialog displays.

5. In the **New password** field, type the user's password. This must be 12 characters or less in length.
6. In the **Retype new** field, type the user's password again, for confirmation.
7. Click on the **OK** button.
8. A *'Password Changed'* message displays. Click on the **OK** button.
9. When you have entered the details for the user, click on the **Save** button. Either click on the **New** button to add another user, or the **Close** button to exit the Security Users dialog.

Notes:

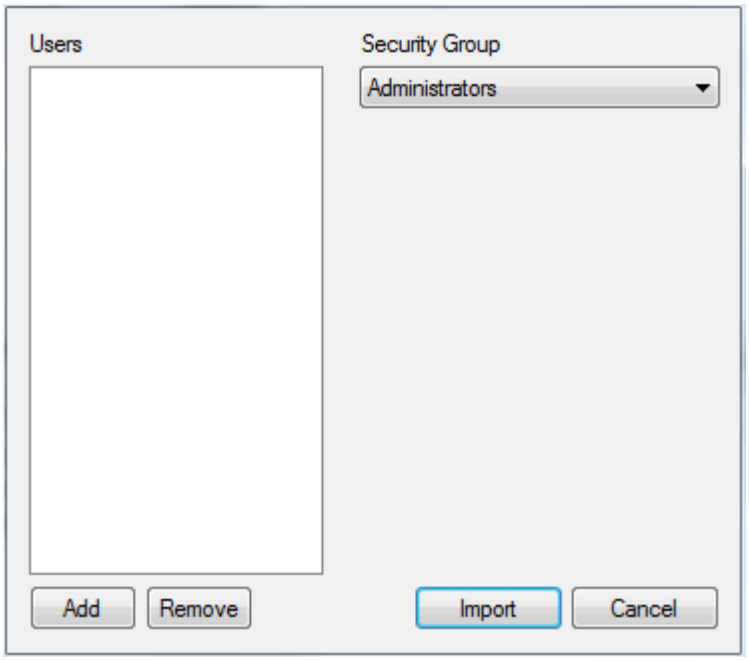
- You can transport the user definitions between models, using the **Export Reference Data** and **Import Reference Data** options on the **Tools** menu (see the *Reference Data* topic in *UML Model Management*).
- If you select the **Accept Windows Authentication** checkbox, when a user opens the model Enterprise Architect checks the users database for their Windows ID and, if it matches, automatically logs the user in without prompting for a password.
- The **Accept Windows Authentication** checkbox enables the **Import** button, which you can select to import user IDs from a Windows Active Directory.
- As a security measure, the **Accept Windows Authentication** checkbox is automatically deselected if the project .eap file is moved to a different location. Once the file has been relocated, you can select the checkbox again to apply Windows authentication from the new database.

4 Import User IDs From Active Directory

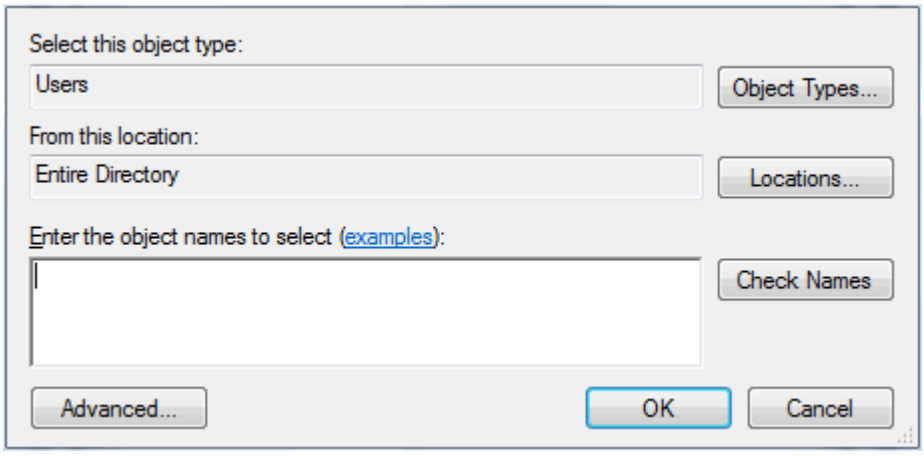
When you import user IDs from Windows Active Directory, you should create an appropriate user group 14 and assign the imported user IDs to that group. You can then assign appropriate permissions to the group. When a user logs in to Enterprise Architect under their Windows login ID, they do not have to enter a password; Enterprise Architect automatically generates a random password. However, you can assign a new password to an imported user ID if required.

To import user IDs from a Windows Active Directory, follow the steps below:

1. On the Security Users dialog select the **Accept Windows Authentication** checkbox and click on the **Import** button. The Import Users dialog displays.

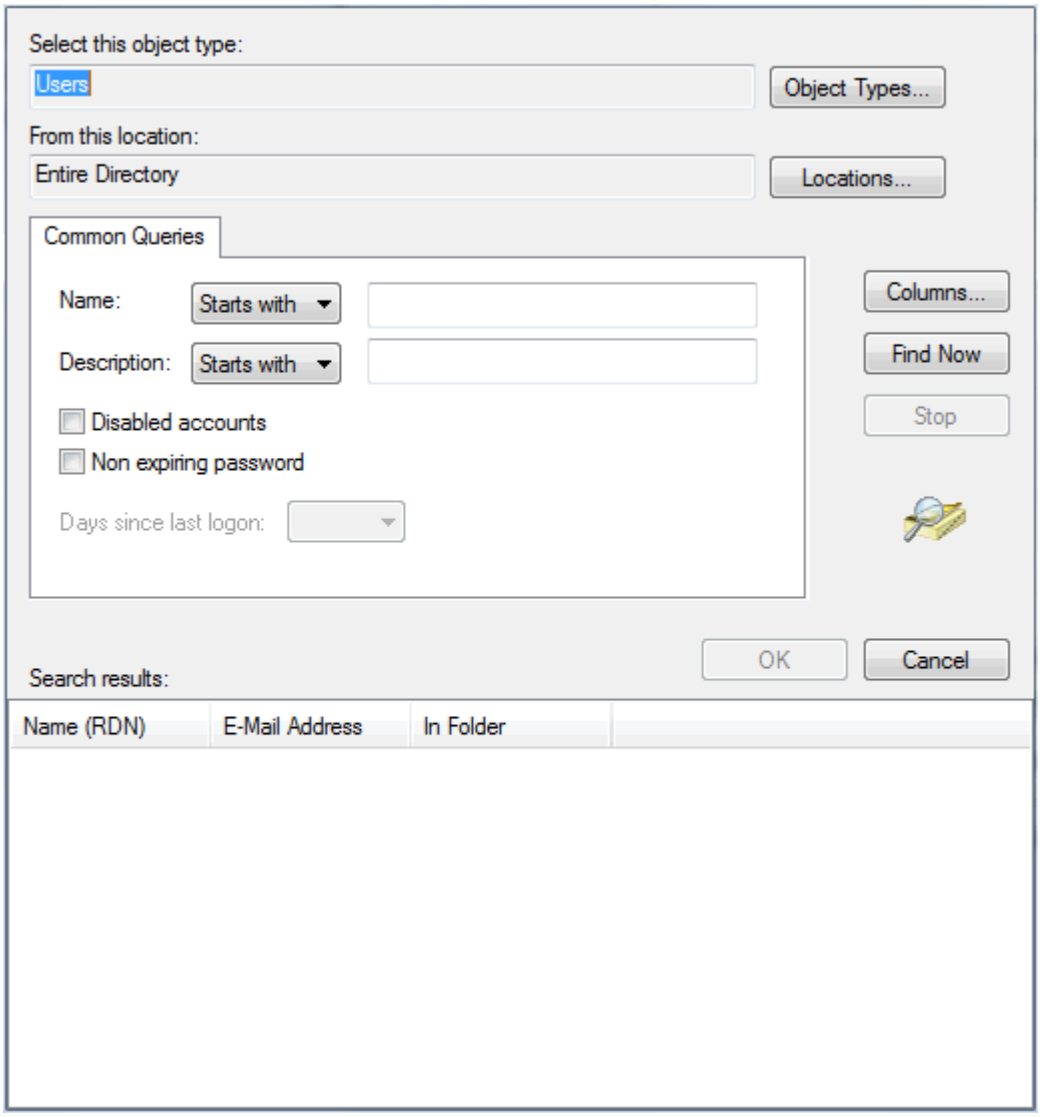


2. On the Import Users dialog, click on the down arrow in the **Security Group** field and select the appropriate security group for the imported user IDs.
3. Click on the **Add** button. The Select Users screen displays.



4. Click on the **Object Types** button, and on the Object Types dialog select the checkbox for the type of object to import from the Active Directory. Click on the **OK** button to return to the Select Users dialog.
5. Click on the **Locations** button, and on the Locations dialog browse for and select the checkbox for the location to import from within the Active Directory. Click on the **OK** button to return to the Select Users dialog.

6. In the **Enter the object names to select** field, either:
   - type in the user IDs individually (click on the **examples** link to see examples of the correct formats) or
   - click on the **Advance** button to search for IDs; the Select Users dialog redisplays with a Common Queries tab.

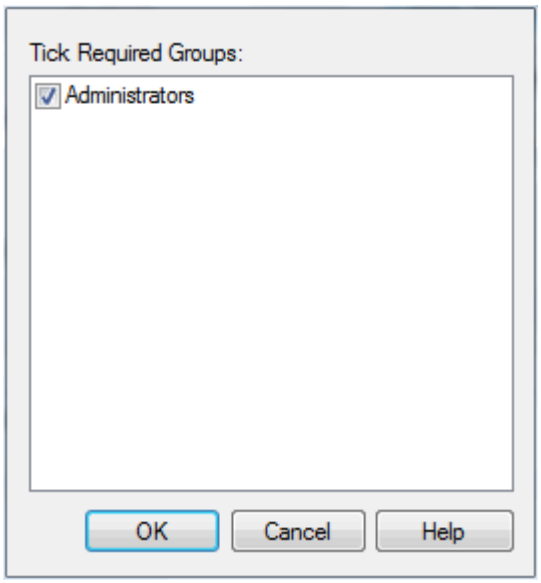


7. In the **Name** and **Description** fields, type any characters or text that helps identify the IDs you are searching for. Click on the drop-down arrow of the **Starts with** field and select the appropriate qualifier.
8. If required, select the **Disabled accounts** or **Non-expiring password** checkboxes, and/or select a value in the **Days since last logon** field, to further filter the IDs to search for.
9. Click on the **Find Now** button to initiate the search, and to display a list of IDs in the bottom panel of the dialog. You can vary the types of information shown here by clicking on the **Columns** button and selecting the column headings to display.
10. When you have identified the IDs to import, click on a required ID (or press **[Ctrl]** or **[Shift]** while you click to select several) and click on the **OK** button. The Select Users dialog redisplays, with the selected ID or IDs listed in the **Enter the object names to select** field.
11. Click on the **OK** button to redisplay the Import Users dialog with the selected users' names listed in the Users panel.
12. Click on the **Import** button to add the user IDs to the Security Users dialog. Click on a user ID to populate the dialog fields with the user ID details, and set group permissions 15 as required.

5 Assign User To Groups

To set up user groups follow the steps below:

1. Select the **Project | Security | Manage Users** menu option. The Security Users dialog displays.
2. Click on the **Group Membership** button. The User Groups dialog displays.
3. Select the checkbox against each group this user belongs to.



4. Click on the **OK** button to assign the user to each group.

Notes:

- To create new user groups, see the *Maintain Groups* 14 topic.
- You can transport these user groups between models, using the **Export Reference Data** and **Import Reference Data** options on the **Tools** menu (see the *Reference Data* topic in *UML Model Management*).

6 Set Up Single Permissions

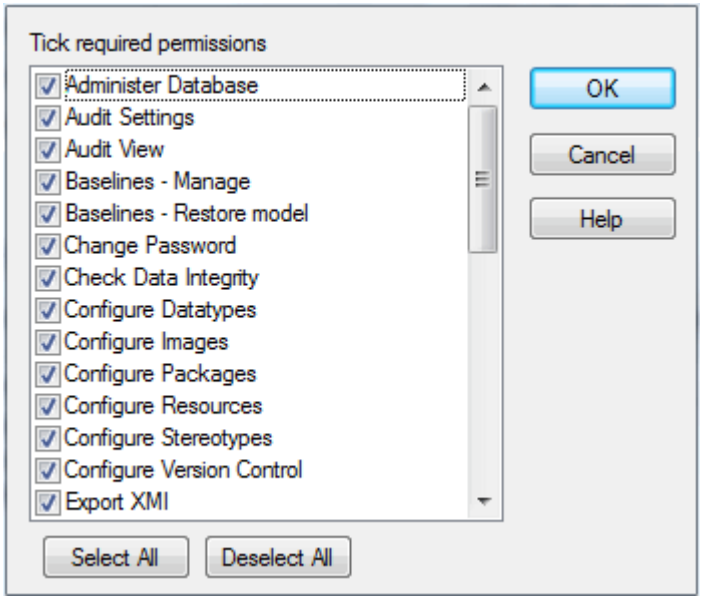
You can set specific user permissions from the User Permissions dialog. Specific user permissions are added to permissions from group membership to provide an overall permission set.

Note:

You must have **Security - Manage Users** 16 permission to assign permissions to users; the initial **Admin** administrator automatically has this permission.

To set up single permissions for a user follow the steps below:

1. Select the **Project | Security | Manage Users** menu option. The Security Users dialog displays.
2. Click on the **Single Permissions** button. The User Permissions dialog displays.



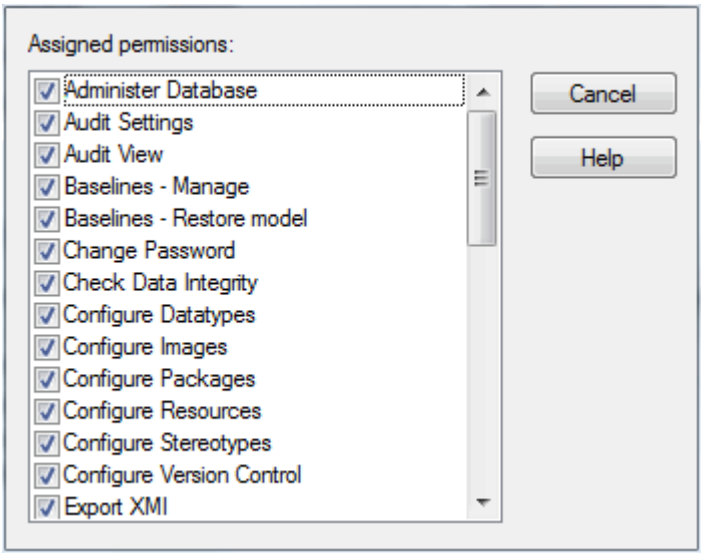
3. Select the checkbox against each specific permission to apply to this user. Click on the **Select All** button to select all permissions for the user, or click on the **Deselect All** button to clear all selected permissions.
4. Click on the **OK** button to assign the selected permissions to the user.

Notes:

- A user's total permissions are those granted by Group Membership plus those granted by specific permission assignment.
- You can transport these user permissions between models, using the **Export Reference Data** and **Import Reference Data** options on the **Tools** menu (see the *Reference Data* topic in *UML Model Management*).

7 View All User Permissions

The All user permissions dialog shows a list of all permissions a user has, derived from their individual profile and from their membership of security groups. To display the dialog, select the **Project | Security | Manage Users** menu option, then select the required user and click on the **View All** button.



8 Maintain Groups

Security groups make it easy to configure sets of permissions and apply them to a number of users in one action.

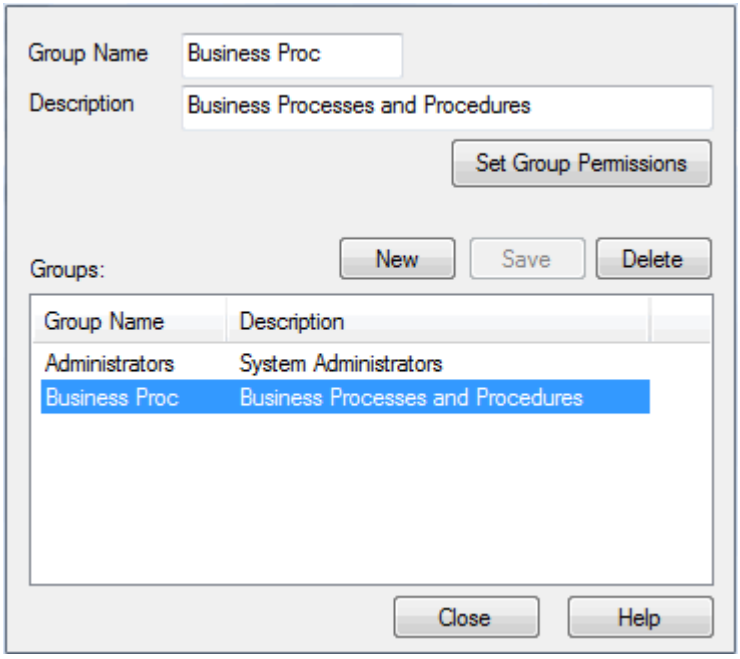
Notes:

- You must have **Security - Manage Users** 16 permission to manage user groups; the initial **Admin** administrator automatically has this permission.
- You do not define groups as group logins with passwords. If you intend to use a group login, you can define a single-user login and password 7 that all group members use (that is, Enterprise Architect allows multiple logins under one user ID).

Set Up a Security Group

To set up a security group, follow the steps below:

1. Select the **Project | Security | Manage Groups** menu option. The Security Groups dialog displays.



2. In the **Group Name** and **Description** fields, type the security group name and a description of the group.
3. Click on the **Save** button.

Note:

You can transport these security group definitions between models, using the **Export Reference Data** and **Import Reference Data** options on the **Tools** menu (see the *Reference Data* topic in *UML Model Management*).

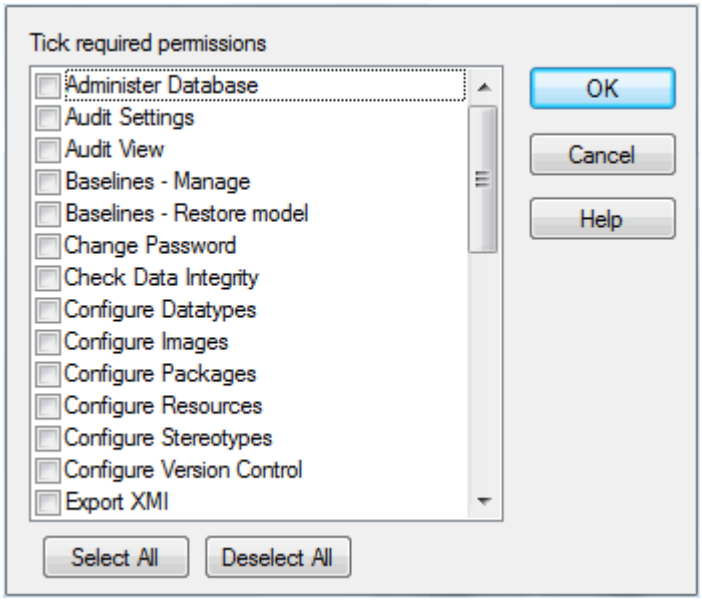
9 Set Group Permissions

Note:

You must have **Security - Manage Users** 16 permission to assign permissions to user groups; the initial **Admin** administrator automatically has this permission.

To set up permissions to apply to a security group, follow the steps below:

1. Select the **Project | Security | Manage Groups** menu option. The Security Groups dialog displays.
2. Click on the **Set Group Permissions** button. The Group Permissions dialog displays.



3. Select the checkbox against each required permission. Click on the **Select All** button to select all permissions for the user, or click on the **Deselect All** button to clear all selected permissions.
4. Click on the **OK** button to assign the permissions. All of the users assigned to this group share in this set of permissions.

Note:

You can transport these group permission definitions between models, using the **Export Reference Data** and **Import Reference Data** options on the **Tools** menu (see the *Reference Data* topic in *UML Model Management*).

10 List of Available Permissions

The following table lists the available permissions in the Corporate, Business and Software Engineering, System Engineering and Ultimate editions of Enterprise Architect. These permissions are required for the corresponding operations if security is enabled.

Note:

Some permissions take precedence over others. For example, if you set **Use Version Control** permission for a user, that user can modify model elements on import even if they do not have **Update Element** permission.

Permission	Enables the user to
Administer Database	Compact and repair project database. (See *UML Model Management*.)
Admin Workflow	Develop and manage workflow scripts 21.
Audit Settings	Change the audit settings in the Audit Settings dialog. (See *Auditing UML Models*.)
Audit View	Enable auditing and display data in the Audit View and Audit History tab. (See *Auditing UML Models*.)
Baselines - Manage	Create, delete, import and export Baselines. (See *Baseline UML Models*.)
Baselines - Restore	Merge data into the project model from a Baseline or XML file. (See *Baseline UML Models*.)
Change Password	Change your own password 7 or (Administrator) another user's password.
Check Data Integrity	Check and repair project integrity. (See *UML Model Management*.)
Configure Datatypes	Add, modify and delete datatypes. (See *UML Model Management*.)
Configure Images	Configure alternative element images. (See the *Work With Diagrams* section in *UML Modeling With Enterprise Architect - UML Modeling Tool*.)
Configure Packages	Configure controlled packages and package properties. (See *UML Model Management*.)
Configure Resources	Create and manage Resources window items: RTF templates, patterns, profiles, favorites. (See *Using Enterprise Architect - UML Modeling Tool*.)
Configure Stereotypes	Add, modify and delete Stereotypes. (See *UML Model Management*.)
Configure Version Control	Set up version control options for the current model. (See *Version Control Within UML Models Using Enterprise Architect*.)
Export XMI	Export model to XMI. (See *UML Model Management*.)
Generate Documents	Generate RTF and HTML documents from model packages. (See *Report Creation In UML Models*.)
Generate Source Code and DDL	Generate source code and DDL from model element. Synchronize code against model elements if it already exists. (See *UML Model Management*.)
Import XMI	Import model from XMI. (See *Code Engineering Using UML Models*.)
Lock Objects	Lock an element 27 or package 29.
Manage Diagrams	Create new diagrams, copy existing and delete diagrams. Also save diagram as UML Pattern. (See the *Work With Diagrams* section in *UML Modeling With Enterprise Architect - UML Modeling Tool*, and *Extending UML With Enterprise Architect*.)

Permission	Enables the user to
Manage Issues	Update and delete Issues. (See *Project Management With Enterprise Architect*.)
Manage Project Information	Update and manage resources, metrics, risks. (See *Project Management With Enterprise Architect*.)
Manage Reference Data - Update	Update and delete reference items. (See *UML Model Management*.)
Manage Replicas	Create and synchronize replicas. (See *UML Model Management*.)
Manage Tests	Update and delete Test records. (See *Project Management With Enterprise Architect*.)
Reverse Engineer from DDL and Source Code	Reverse engineer from source code or ODBC, and synchronize model elements against code. (See *Code Engineering Using UML Models*.)
Security - Enable/Disable	Disable 4 user security in Enterprise Architect.
Security - Manage Locks	View and delete 18 element locks.
Security - Manage Users	Maintain users 7, groups 11 and assigned permissions 12.
Spell Check	Spell check package and set spell check language. (See *Using Enterprise Architect - UML Modeling Tool*.)
Transfer Data	Transfer model between different repositories. (See *UML Model Management*.)
Transform Package	Perform transformations of packages and elements. (See *MDA Transformations User Guide*.)
Update Diagrams	Update diagram appearance, properties and layout, including the Page Setup dialog. (See the *Work With Diagrams* section in *UML Modeling With Enterprise Architect - UML Modeling Tool*.)
Update Element	Save model changes (including delete) for elements, packages, and relationships. (See *UML Modeling With Enterprise Architect - UML Modeling Tool*.)
Use Version Control	Check files in and out using version control. (See *Version Control Within UML Models Using Enterprise Architect*.)

11 View and Manage Locks

From time to time it might be necessary to examine or delete locks placed on elements by users. Enterprise Architect provides a function to view and manage active locks.

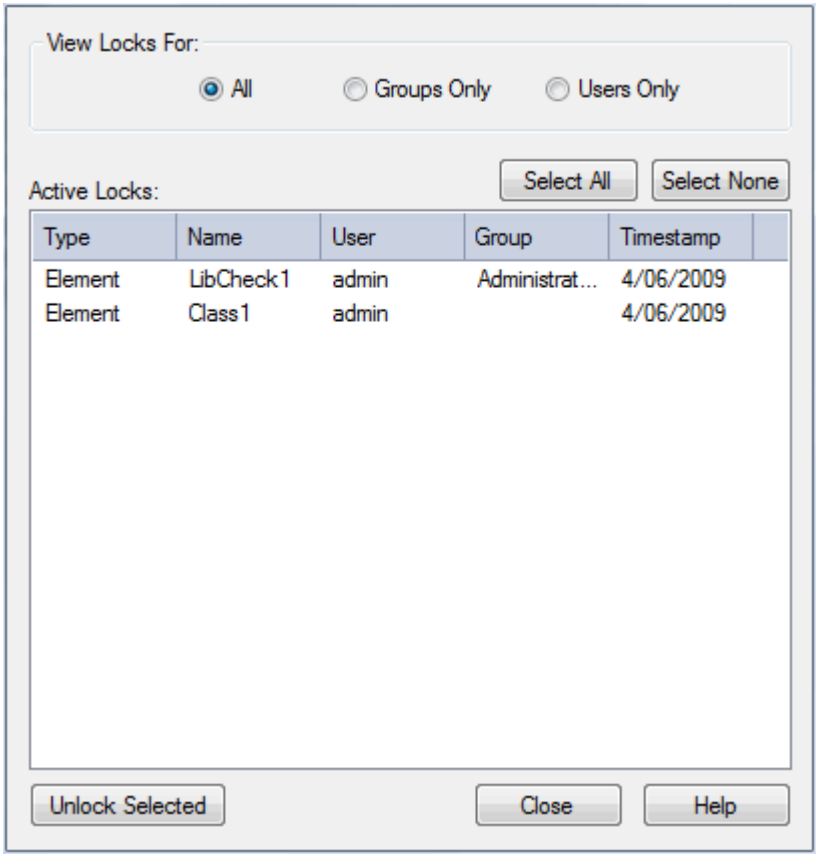
Notes:

- You must have **Security - Manage Locks** 16 permission to view and delete user locks; the initial **Admin** administrator automatically has this permission.
- If an element is locked, connectors attached to it are also locked. To unlock the connector, you must unlock the element. However, under certain circumstances you can add new connectors to a locked element 28.

Delete a Lock

To view locks and, if necessary, delete them, follow the steps below:

1. Select the **Project | Security | Manage Locks** menu option. The Active Locks dialog displays.



2. In the View Locks For panel, click on the radio button for the type of lock to view: **All**, **Groups Only** or **Users Only**. Locks of the appropriate type are listed in the Active Locks panel. If you want to display the resulting information in a more readable layout, you can resize the dialog and its columns.
3. To remove a lock, click on it and click on the **Unlock Selected** button.
4. When finished, click on the **Close** button to close the dialog.

12 Password Encryption

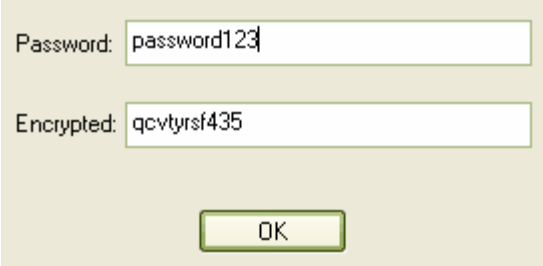
Note:

This topic is retained to support regression to releases of Enterprise Architect prior to version 7.1. For password encryption for all repositories at and beyond release 7.1, see the *Save Model Copy or Shortcut* topic in *Using Enterprise Architect - UML Modeling Tool*.

Users of SQL Server or Oracle repositories have the option of encrypting the password used to set up the connection between Enterprise Architect and the repository. The Enterprise Architect user does not have the real password, thereby preventing them from accessing the repository using other tools such as Query Analyzer or SQLPlus.

Once security is enabled, the administrator must log on to access the dialog to create encrypted passwords. To encrypt a password, follow the steps below:

1. Select the **Project | Security | Encrypt Password** menu option. The following dialog displays:

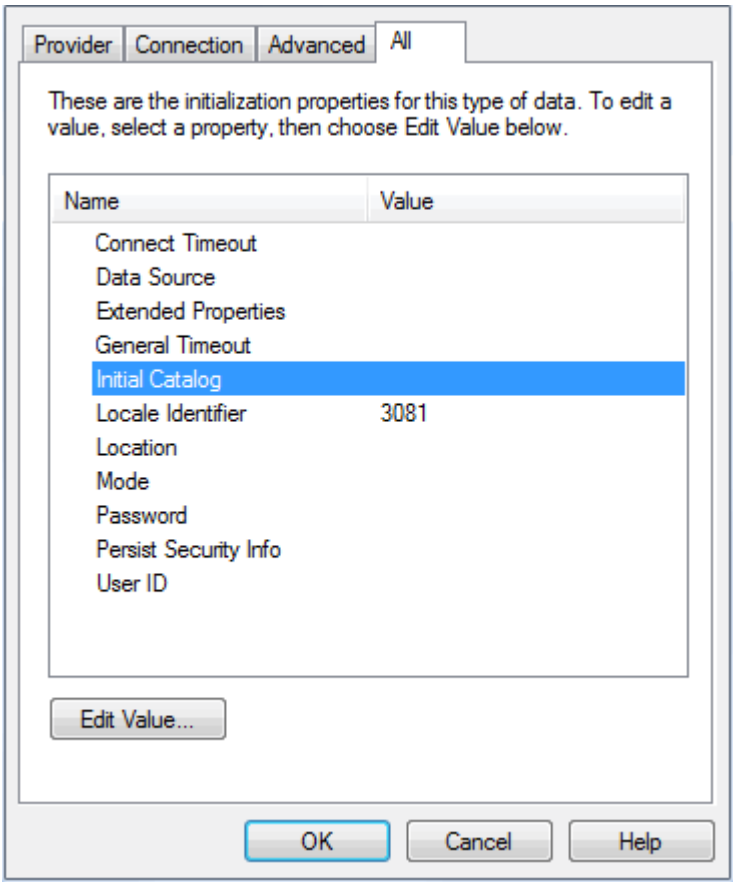


2. In the example above, the password **password123** is used to access the repository.
3. To connect Enterprise Architect to the repository, the user enters the encrypted password prefixed with **$$**, so the encrypted password becomes **$$qcvtyrsf435**.

For more information relating to connecting to Oracle and SQL Server, see the *Connect to Oracle Data Repository* and *Connect to SQL Server Data Repository* topics respectively, in *UML Model Management*.

Notes:

- Do not use the **Test Connection** button as it can cause an error with encrypted passwords.
- For SQL Server repositories, you must enter the *Initial Catalog* details from the All tab of the Data Link Properties dialog.



13 Workflow Scripts - Introduction

Good corporate governance relies on well written and transparent project development guidelines and company policy. A project might be compromised if the appropriate policies and procedures are poorly understood and not followed correctly - effective governance can be hampered by human error and the costs of recovering from the inadequate compliance of developers.

Company policy and procedures can be integrated with the development process to manage work flows, determine access rights, extend role based security permissions and respond to property change events. This approach reduces compliance costs, enhances collaborative development and gives you confidence that projects are being developed correctly the first time around. Development teams can adhere to best practice guidelines that govern model validation, change management, access controls and general development principles.

Enterprise Architect enables you to create workflow scripts 21 that provide a more robust approach to applying company policy and strengthening project development guidelines by validating against the policy and procedures within the model itself. Project administrators can write scripts to manage the way users interact with a model, such as managing security, staff compliance and model access, and monitoring changes made by users. Administrators can also use workflow scripts to control a user's capacity to change a model element, taking into account factors such as access rights, group membership and even the value of a proposed change.

When a model is launched, the Workflow Engine is initialized with the current user and group memberships. This information determines who can access and modify parts of a given model. When a selected event occurs, the script engine is initialized with values including the author's name and access rights, and the element name and version details. The workflow script implements rules governing change management, access control and model validation. If a user attempts to make changes in violation of company policy, the script denies the update. The user is notified why the validation failed and the activity is logged. These reminders help to reinforce company policy, reduce human error and provide management with valuable project feedback.

13.1 Workflow Script Functions

Workflow scripts are executed by the Enterprise Architect workflow engine, to manage user input. You write the scripts in the Scripter window, in VBScript, under the Workflow group type. (See *Using Enterprise Architect - UML Modeling Tool*.)

Functions Enterprise Architect Calls to Validate and Control User Input

For each of the following functions that Enterprise Architect calls, a set of objects 22 are filled.

Function	Use to...	Return Value
AllowPhaseUpdate(OldValue, NewValue)	Validate a change a user has made to a phase.	• **True** to allow this user to make this change. • **False** to disallow the change and revert to the previous value.
AllowStatusUpdate(OldValue, NewValue)	Validate a change a user has made to a status.	
AllowTagUpdate(TagName, OldValue, NewValue)	Validate a change a user has made to a Tagged Value.	
AllowVersionUpdate(OldValue, NewValue)	Validate a change a user has made to a version.	
CanEditPhase()	Enable or disable the control for editing a phase.	• **True** to allow this user to make changes by enabling the control. • **False** to completely disable edit of this property by disabling the control.
CanEditStatus()	Enable or disable the control for editing a status.	
CanEditTag(TagName)	Enable or disable the control for editing a Tagged Value.	

Function	Use to...	Return Value
CanEditVersion()	Enable or disable the control for editing a version.	
PreAllowPhaseUpdate(OldValue, NewValue)	Determine what information is required to validate this change.	Semi-colon separated list of additional data required in order to validate this change. See the list of supported data types 22.
PreAllowStatusUpdate(OldValue, NewValue)		
PreAllowTagUpdate(TagName, OldValue, NewValue)		
PreAllowVersionUpdate(OldValue, NewValue)		

Functions Enterprise Architect Calls to Create a Search With User Tasks

Function	Use to...	Return Value
GetWorkflowTasks	Describe the searches that this user must run.	Ignored

Supported Data Types

Tests - fill the *Tests* array in the *WorkflowContext* object.

Workflow Data Structures - Objects Enterprise Architect Fills

WorkflowUser

This object provides information about the user currently logged in to the model. It is filled by Enterprise Architect before any function is called by Enterprise Architect. It has the following properties:

- **Username** - the username for login to the system (if using Windows Authentication, this matches the Windows username)
- **Firstname** - as found in the Security Users 7 dialog
- **Surname** - as found in the Security Users dialog
- **Fullname** - the combination **<Firstname> <Surname>** (the form Enterprise Architect uses for **Author** fields and similar).

This object also calls the following function:

Function	Use to...	Return Value
IsMemberOf(GroupName)	Check group membership of the current user.	**True** if the current user is a member of the group with the specified name.

WorkflowContext

This object provides information about the object currently in context. It is filled by Enterprise Architect before any searches except **GetWorkflowTasks** 22 are run. It has the following properties:

- **MetaType** - the type of the current object, either an Enterprise Architect core type or a profile-specified metatype
- **Name** - as found in the object Properties dialog
- **Status** - as found in the object Properties dialog
- **Phase** - as found in the object Properties dialog
- **Version** - as found in the object Properties dialog
- **GUID** - the GUID of the object
- **Stereotypes** - an array of strings for the stereotypes applied to this object

- **Tags** - an array of Tagged Values, providing:
  - **Name** - the Tagged Value name
  - **Value** - the Tagged Value value
- **Tests** - an array of tests; only filled during an *Allow** call after the *PreAllow** call has specified that tests are required. Provides the following details, as found in the Testing window:
  - **Name**
  - **Status**
  - **RunBy**
  - **CheckedBy**
  - **TestClass**
  - **TestType**

The WorkflowContext object also calls the following function:

Function	Use to...	Return Value
TagValue(TagName)	Get the value from a named tag.	Returns the value of the first Tagged Value with that name, or an empty string if no Tagged Value with that name exists.

Workflow Data Structures - Objects You Can Fill

WorkflowStatus

Use this to provide information on the status of the object.

- **LogEntry** - set to **True** or **False**, to indicate whether a log item should be recorded
- **Reason** - indicate what reason should be recorded in the log
- **Action** - indicate how to display the log message; valid values are: **MessageBox**, **StatusBar**, **Output** (default).

WorkflowSearches

Provides an array of searches. Use **Redim WorkflowSearches(x)** to specify the number of searches being provided. Each search has the following attributes:

- **Name** - the name of this search
- **Group** - the name of the group that this search should appear under in the **Search** combo box
- **ID** - the unique GUID for this search
- **Tasks** - the array of tasks that this search looks for; an entry describes how to find all objects required to meet a particular task:
  - **Name** - the name of the task, as displayed in the Search view; workflow searches are grouped by this field by default
  - **Conditions** - an array of conditions, all of which must be matched for an object to be included in this task; a condition is a comparison of a single field to a value:
    - **Column** - the name of the field
    - **Operator** - operator types, either **=** (provide matching values only) or **<>** (provide non-matching values only)
    - **Value** - if this contains a comma, the string is treated as a comma separated list of values to compare against; otherwise the string is a single value to compare against.

Functions Enterprise Architect Provides For You to Call

Enterprise Architect provides the subfunction **SetLastError(message, outputMethod)** for you to call, to log and/or report the provided message to the user.

You can also call the following functions:

Function	Use to...	Return Value
NewSearch(name, group, guid, taskcount)	Create a new search object to be included in WorkflowSearches. Initializes each member.	The created search.
NewTask(name, conditioncount)	Create a new task object to be included in a search. Initializes each member.	The created task.
NewCondition(column, operator, value)	Create a new condition object to be included in a task. Initializes each member.	The created condition.

14 Change Password

There are two ways in which a user's password can be changed, when security is set:

- A user can select the **Change Password** menu option and change their own password
- The Administrator can set or change any user's password, on the Maintain Users dialog.

Note:

A user must have **Change Password** 16 permission to change a password; the initial **Admin** administrator automatically has this permission.

User Change

If security is set and you want to change your own password, follow the steps below:

1. Select the **Project | Security | Change Password** menu option. The Change Password dialog displays.

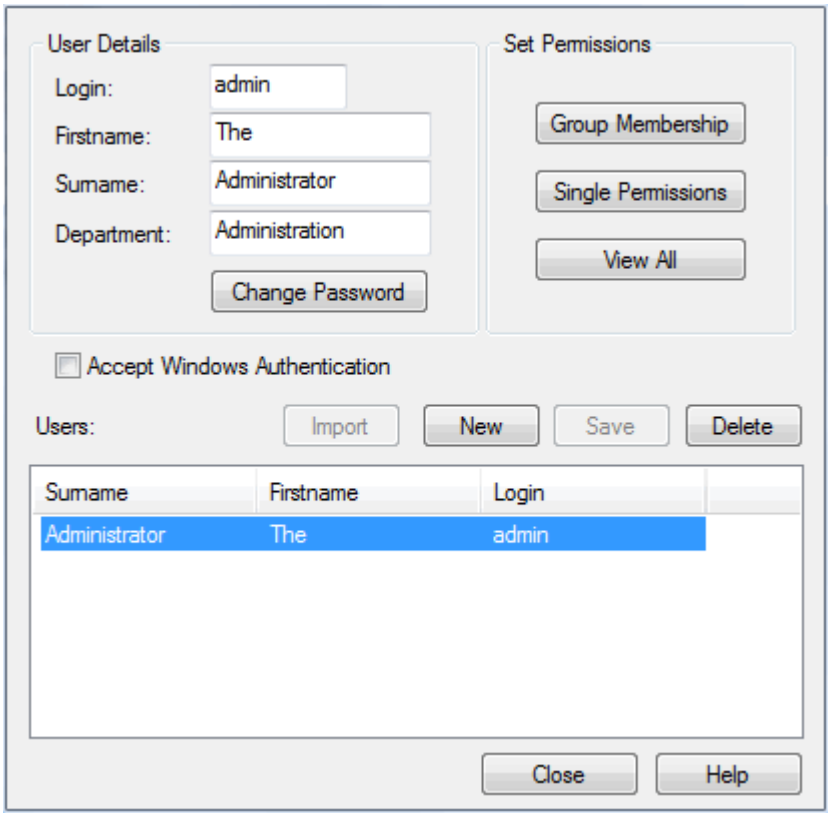
2. In the **Enter old password** field, type your current password.
3. In the **New password** field, type your new password (this must be 12 characters or less in length).
4. In the **Retype new** field, type your new password again, for confirmation.
5. Click on the **OK** button.
6. A *'Password Changed'* message displays. Click on the **OK** button to clear the message.

Your new password is effective next time you log in.

Administrator Change

To set or change any user's password, follow the steps below:

1. Select the **Project | Security | Manage Users** menu option. The Security Users dialog displays.



2. Click on the user name in the Users: panel, to display the user details in the dialog fields.
3. Click on the **Change Password** button. The Change Password dialog displays.

4. In the **New password** field, type the user's password; this must be 12 characters or less in length.

Note:

You do not have to enter the user's current password, as they might have forgotten it and therefore it is possible that nobody can provide that value.

5. In the **Retype new** field, type the user's password again, for confirmation.
6. Click on the **OK** button.
7. A *'Password Changed'* message displays. Click on the **OK** button.

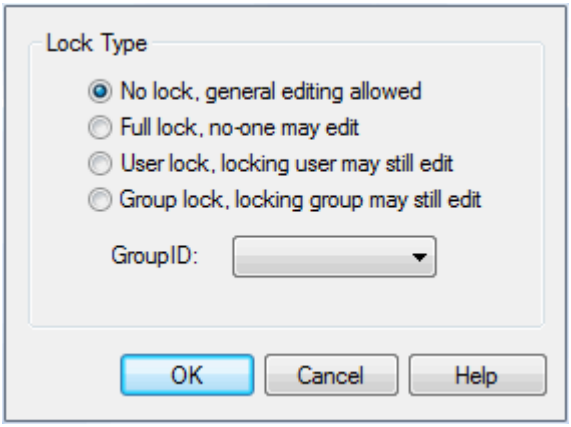
15 Lock Model Elements

Note:

When security is enabled, you must have **Lock Objects** 16 permission to lock an element.

You can lock a package, element or diagram using the corresponding **Lock** context menu option in the Project Browser, and you can lock an element or diagram using the corresponding **Lock** context menu option in the diagram.

Under the standard security policy (**Require User Lock to Edit** deselected), when you select the **Lock** option the Element Lock dialog displays:



The four lock options available are:

- **No lock** - do not lock this element; clear any existing lock
- **Full lock** - lock this element so that no-one can edit it
- **User lock** - lock this element so that only the locking user can make further edits
- **Group lock** - lock this element so that any member of the specified group (in the **GroupID** field) can update the element, but others are excluded.

Select the appropriate lock and click on the **OK** button.

If the item is already locked, only the appropriate lock option and **No lock** are available. You have to release the lock in order to set a different type of lock.

Under the rigorous security policy, a different dialog displays. See the *Apply a User Lock* 30 topic.

If a diagram is locked and you select an object on it, the object border displays in red. This indicates that you cannot change the object.

16 Add Connectors To Locked Elements

When working with locked elements, the ability to add connectors depends on the locked status of the source and target elements. The rules are:

- **Source unlocked, target unlocked**: any kind of connector can be added
- **Source unlocked, target locked**: allowed, except for composition connectors
- **Source locked, target unlocked**: prohibited, except for composition connectors
- **Source locked, target locked**: prohibited for all connectors.

That is, a connector can be added if its source is unlocked, regardless of the locking state of the destination (think of it as modifying what the source can see). The exception is composition connectors, where the target (that is, parent) must be unlocked (think of it as modifying the parent by adding children).

Connectors with locked source or target elements are also locked. To unlock the connector, you must unlock 18 the source and/or target element.

17 Lock Packages

Note:

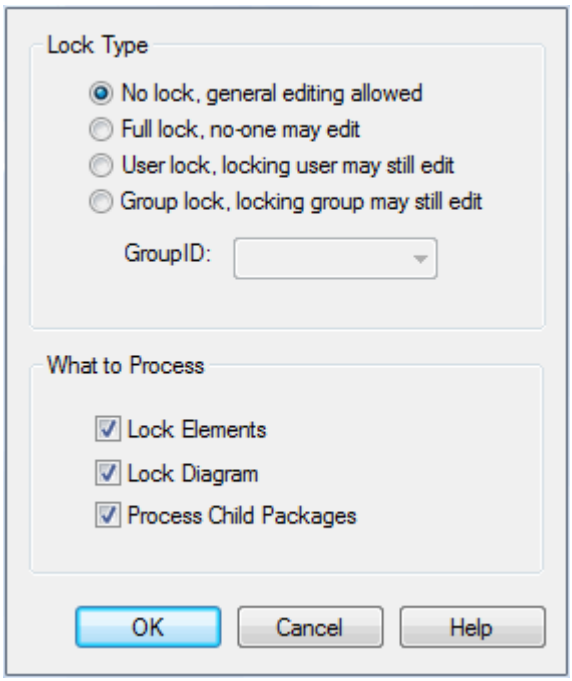
If security is enabled you must have **Lock Objects** 16 permission to lock a package.

You can lock all the contents of a package (and optionally all contents in child packages) in one step, using the *Lock Package* function. The locks are automatically applied to elements and to diagrams, as if they had been individually set or cleared. Lock types and details are the same as for locking a single element 27.

Lock a Package

To lock a package, follow the steps below:

1. Deselect the **Project | Security | Require User Lock to Edit** menu option.
2. In the Project Browser, right-click on the package to lock. The context menu displays.
3. Select the **Lock Package** menu option. The Lock/Unlock Package(s) dialog displays.

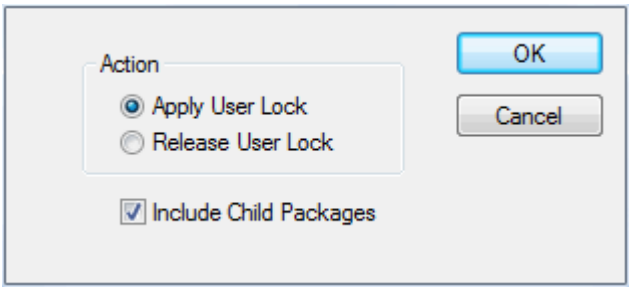


4. In the Lock Type panel, select the appropriate radio button for the lock to apply.
5. As required, select the checkboxes to lock elements and/or diagrams, and to process child packages (that is, lock the whole branch).
6. Click on the **OK** button to apply the lock.

18 Apply a User Lock

In the *Require User Lock to Edit* 6 security mode, where a User Lock is required before any edit can occur, you can set or release the lock in either a diagram or the Project Browser. Enterprise Architect adjusts the lock for the element, or for the diagram and any elements contained in the diagram.

In a diagram, you right-click on the element or diagram; in the Project Browser, you right-click on the package, diagram or element. In each case, select the **Apply/Release User Lock** context menu option for the selected item. The following dialog displays.



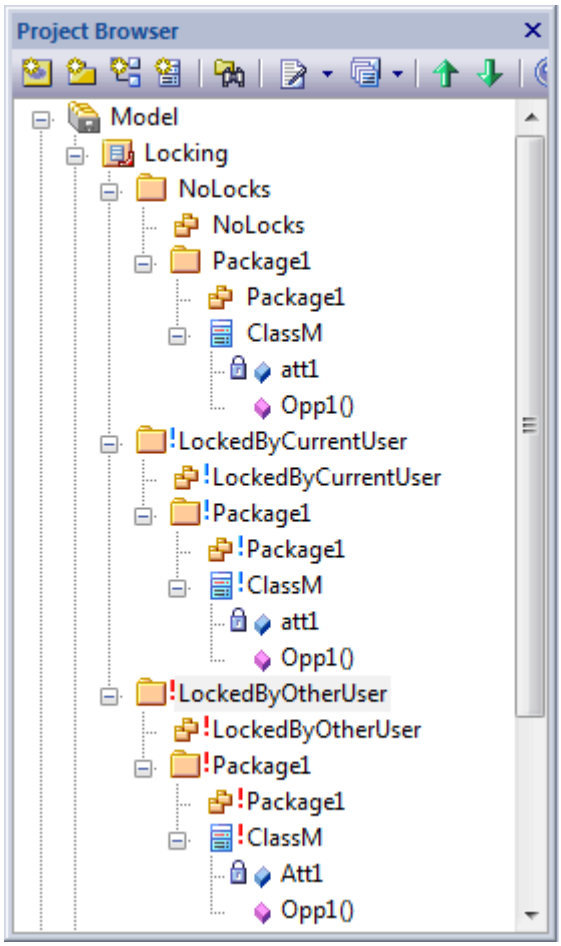
Select the appropriate radio button to apply or release a user lock on the selected item.

Note:

For a package, you can elect to also lock all child packages at the same time. If any elements in the package tree are locked by other users, a list of elements that couldn't be locked displays at the end of the process.

19 Locked Element Indicators

When an item is locked through Project Security, the lock is indicated in the Project Browser by a marker against the item, as shown below.



The meaning of the marker depends on the security mode.

If you are using the *Require User Lock to Edit* 6 security mode:

- **No** marker - there is no lock, the item is *not* editable, but any user can now apply a user lock 30 to edit the item
- **Blue** exclamation mark - the current user has applied a user lock and can edit the item; no other user can edit the item
- **Red** exclamation mark - another user has applied a user lock, and the current user cannot edit the item.

If you are using the *standard* 6 security mode 6:

- **No** marker - there is no lock, the item *is* editable, but any user can now apply a user or group lock 30
- **Blue** exclamation mark - the item has a lock set by the current user or a group having the current user as a member, and the user can edit the item
- **Red** exclamation mark - the item has a lock set by another user, or a group of which the current user is not a member; the current user cannot edit the item.

If another user has locked an item, you can identify who has locked it 32.

Note:

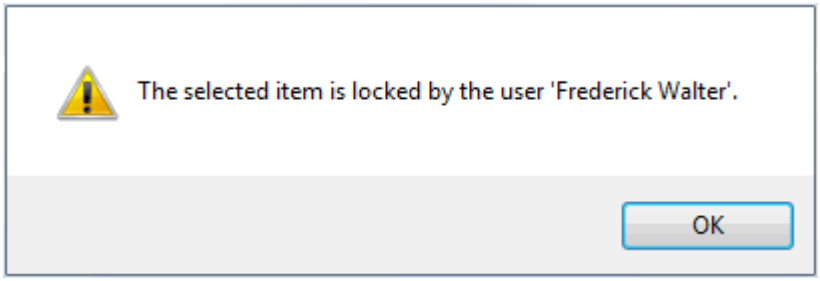
If a diagram is locked and you select an object on it, the object border displays in red. This indicates that you cannot change the object.

20 Identify Who Has Locked An Object

If you find that a diagram, package or element is locked, you can find out which group or user currently holds the lock on that item. To do this, follow the steps below:

1. In the Project Browser, right-click on the diagram, package or element that is locked by another user or user group. The context menu displays.
2. Select the **Lock** menu option.

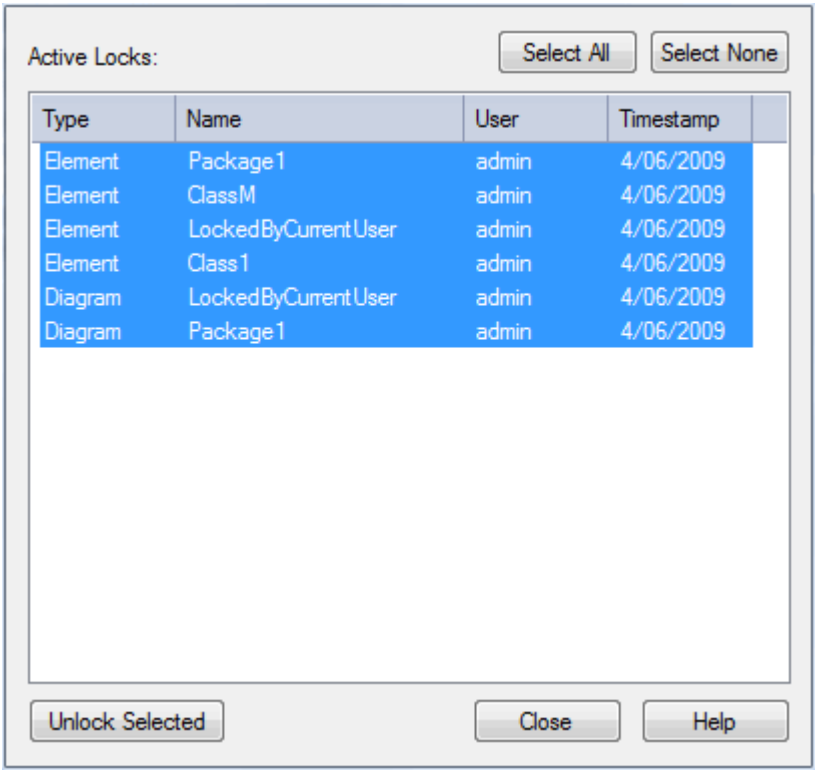
   A message box displays showing which group or user currently holds the lock on that item.



21 Manage Your Own Locks

You can view and delete your own user-level locks in Enterprise Architect. This is especially useful when working in Mode 2 security (user locks required to edit).

To manage your locks select the **Project | Security | My Locks** menu option. The My Locks dialog displays.



In the My Locks dialog you can select one or more locks and delete them (that is, unlock the object) by clicking on the **Unlock Selected** button.

Index

- A -

- B -

- C -

- D -

- E -

- G -

- I -

- L -

- M -

- O -

- P -

- R -

- S -

- U -

- V -

- W -

User Security in UML Models

www.sparxsystems.com