



Enterprise Architect

User Guide Series

The Modeling Team

How to support modeling in teams? Sparx Systems Enterprise Architect is a team modeling platform, with a free readable Light version, many deployment options, version control, reusable assets, reviews, Team Library, user security and Workflow Scripts.

Author: Sparx Systems

Date: 2021-09-02

Version: 15.2

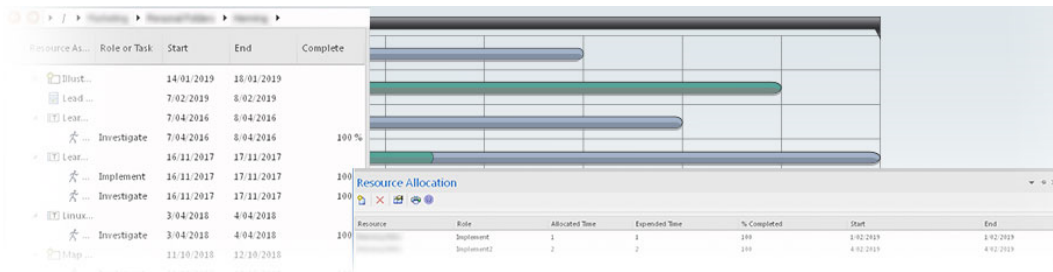
CREATED WITH  ENTERPRISE
ARCHITECT

Table of Contents

The Modeling Team	5
Project Roles	10
Summary of Typical Tasks	13
Business Analysts	17
Software Architects	20
Software Engineers	22
Developers	25
Project Managers	29
Testers	31
Implementation Managers	33
Technology Developers	35
Database Developers	39
User Security	42
Enable/Disable Security	45
Set Security Policy	49
Maintain Groups	52
Security Group Workflow	57
Maintain Users	62
Set User Avatar	68
Single Sign-On (SSO)	70
Single Sign-On (SSO) Options	72
Configure OpenID	75
Import User IDs From Active Directory	82

List of Available Permissions.....	87
View All User Permissions.....	96
View and Manage Locks.....	98
Change Password.....	101
Hide Project Root.....	105
Lock Model Elements.....	106
Lock Objects Under User/Group Locking.....	108
Lock Packages Under User/Group Locking.....	112
Lock Objects Under Require User Lock to Edit.....	116
Locked Element Indicators.....	120
Identify Who Has Locked An Object.....	123
Manage Your Own Locks.....	125

The Modeling Team












Enterprise Architect has been built from the ground up as a team modeling platform, and has extensive support for groups of people working together on the same projects, sharing information, ideas and models. Features in team support include **Baselines**, **Version Control** and a **Reusable Asset Service**, which protect the valuable modeling assets in a team environment, plus tools such as a Discussion Forum, **Library window** and Gantt Charts to facilitate collaboration between project members. The role-based security system has also been designed to encourage collaboration, allowing team members to work together confident that there will be no conflicts in accessing or changing model data.



A choice of deployment options will support any team development environment, allowing people to work centrally or remotely in highly distributed environments. Corporate policy and standards can also be built into the models with the use of **Workflow Scripts**. A free 'Lite' version of Enterprise Architect offers team members 'view only' access to their models, yet also allow them to generate high quality corporate documentation in a wide number of formats to communicate with people outside the modeling

platform.

Overview

Facility	Description
<p>Team Development</p> 	<p>Set up a collaborative modeling environment, taking advantage of security, workflow and shared reference data, as discussed in the rest of this topic.</p>
<p>Formal Model Reviews</p> 	<p>A simple yet powerful mechanism for capturing, in real time, reviews of a section of the model in line with a particular event. Typically, a Project Manager or coordinator will create a Review element specifically to discuss one or more elements for a project phase or other category of review, over a defined period.</p>
<p>Project Management</p> 	<p>Explore some of the ways you can manage your project and team within Enterprise Architect.</p>
<p>Project Resources</p>	<p>Track and manage the people and resources in your project.</p>

	
<p>Glossary</p> 	Define a common vocabulary between your different teams, ensuring common understanding.
<p>Task Allocation</p> 	Assign and Track team tasks in a Gantt View .
<p>Personal Tasks</p> 	Record and manage your personal tasks within the project.
<p>Model Mail</p> 	Use Model Mail in the Collaborations window to securely communicate with your team via an internal email system embedded within the model.
<p>Project Calendar</p> 	Track the deployment of resources, time-frames for tasks, and upcoming project events such as meetings and milestones, in a calendar format.
<p>Use Case Estimation</p>	Form an estimate of the complexity of a system and an indication of the effort required to implement the model.

	
<p data-bbox="225 360 411 472">Library Window</p> 	<p data-bbox="518 360 1430 539">Provides access to a team-based library of documents to record and discuss the development and progress of the project.</p>

Making Project Data Available in a Distributed Environment

Enterprise Architect offers a diverse set of functionality designed specifically for sharing projects in team-based and distributed development environments; for example: Cloud-based solutions, network deployment of model repositories, replication and XMI Import/Export.

Applying Security to the Model

User Security is a means of improving collaborative design and development by preventing concurrent editing and inadvertent model changes by users not designated as model authors.

Using an Internal Discussion Forum

The **Discussions** facility provides several mechanisms to support your development team community, generally in discussing the development and progress of the model across the project, or specifically in discussing individual elements in the model, the discussions becoming a component of each element.

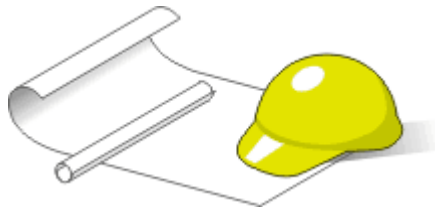
Building Company Policy and Project Development Guidelines into the Project

You can create workflow scripts that provide a robust approach to applying company policy and strengthening project development guidelines, by validating the work against the policy and procedures within the model itself.

Standardizing and Re-using Project Data

You can import and export Reference data (including Glossary and Issue information) from .XML files of another iteration of the same model, or of a different model.

Project Roles



Enterprise Architect is a powerful multi-disciplinary modeling platform that supports common work practices and provides features to assist the entire spectrum of roles and disciplines across enterprise, business, engineering and software projects. Each role will typically use different features of the tool. A number of the roles and their responsibilities that the system supports are outlined here.

You can review a summary of the typical tasks supported for each role, or review the Help topic for the appropriate role title to explore how Enterprise Architect can assist you in carrying out that role within a model-driven project.

Roles and Responsibilities

Role	Responsibilities
Business Analyst	Create high-level models of business processes.
Software Architect	Map functional requirements, perform real time modeling of objects, design the Deployment model and detail the

	deliverable components.
Software Engineer	Map Use Cases onto Class diagrams, detail the interactions between Classes, define the system deployment and define software Packages.
Developer	Perform round trip code engineering, including reverse engineering of existing code and generation of code from Class elements.
Project Manager	Assign resources to elements, measure risk and effort, estimate project sizes, and manage element status, change control and maintenance.
Tester	Create test scripts against elements in the modeling environment.
Implementation Manager	<ul style="list-style-type: none">• Track and assign maintenance-related items to elements within Enterprise Architect• Rapidly capture and keep records of maintenance tasks such as features, changes, documents, issues, defects and tasks• Trace the maintenance of the items and processes involved in system

	deployment
Technology Developer	Create customized additions to the functionality already present within Enterprise Architect.
Database Developer	Develop databases, including modeling database structures, importing database structures from an existing database and generating DDL for rapidly creating databases from a model.

Summary of Typical Tasks

Throughout a design and development project there are many different tasks to be performed, which could be carried out either by one person or - more probably - by members of a team with different responsibilities. In either case, Enterprise Architect supports most - if not all - of the responsibilities you might have on your project. The descriptions in this topic identify a number of job roles that the system supports. For those that most resemble your role on a project, refer to the Help topic for that job title to read a description of how that role might make use of Enterprise Architect, then use the references within those topics to explore some of the features of importance to the role.

Summary of Typical Job Roles

Most of these roles work with specific types of diagram, so you might want to learn more about diagram types in general and specific types of diagram in particular.

Several types of project team member might want to generate documentation on their work and report on how the project is developing and changing. Using Enterprise Architect you can generate project reports in either document or web format.

Role	Responsibilities

Business Analyst	<p>For modeling:</p> <ul style="list-style-type: none">• Requirements• High-level business processes• Business activities• Work flows• System behavior
Database Developer	<ul style="list-style-type: none">• Developing databases• Modeling database structures• Creating logical data models• Generating schema• Reverse engineering databases
Software Architect	<ul style="list-style-type: none">• Mapping functional requirements of the system• Mapping objects in real time• Mapping the deployment of objects• Defining deliverable components
Tester	<ul style="list-style-type: none">• Developing test cases• Importing requirements, constraints and scenarios• Creating Quality Test documentation• Tracking element defects and changes
Software Engineer	<ul style="list-style-type: none">• Mapping Use Cases into detailed Classes

	<ul style="list-style-type: none">• Defining the interaction between Classes• Defining system deployment• Defining software Packages and the software architecture
Project Manager	<ul style="list-style-type: none">• Providing project estimates• Resource Management• Risk Management• Maintenance Management
Developer	<ul style="list-style-type: none">• Forward, reverse and round-trip engineering• Visualizing the system states• Visualizing Package arrangements• Mapping the flow of code
Implementation Manager	<ul style="list-style-type: none">• Modeling the tasks in rolling-out a project, including network and hardware deployment• Assigning and tracking maintenance items on elements (issues, changes, defects and tasks)
Technology Developer	For creating or customizing: <ul style="list-style-type: none">• UML Profiles• Patterns

	<ul style="list-style-type: none">• Code Templates• Tagged Value Types• MDG Technologies• Add-Ins
--	--

Notes

- The Corporate, Unified and Ultimate Editions of Enterprise Architect have a User Security feature that can be applied or turned off; if security is turned on, you need to have the appropriate access permissions to use many of the facilities

Business Analysts

A Business Analyst can use Enterprise Architect to create high-level models of business processes, including business requirements, activities, workflow, and the display of system behavior.

Using Enterprise Architect, a Business Analyst can describe the procedures that govern what a particular business does. Such a model is intended to deliver a high-level overview of a proposed system.

Business Analyst Tasks

Task	Detail
Model High Level Business Processes	Using Analysis diagrams, you can model the high-level processes of the business. Analysis diagrams are a subset of UML 2.5 Activity diagrams and are less formal than other diagram types, but they provide a useful means for expressing essential business characteristics and requirements.
Model Requirements	Gathering requirements is typically the first step in developing a solution, be it for developing a software application or

	<p>for detailing a business process; it is an important step in the implementation of a project.</p> <p>Using Enterprise Architect, you can define the Requirement elements, connect Requirements to the model elements for implementation, connect Requirements together into a hierarchy, report on Requirements, and move Requirements out of model element responsibilities.</p>
Model Business Activities	<p>You can use Activity diagrams to model the behavior of a system and the way in which these behaviors are related to the overall flow of the system.</p> <p>Activity diagrams do not model the exact internal behavior of the system but show instead the general processes and pathways at a high level.</p>
Model Workflow	<p>To visualize the cooperation between elements involved in the workflow, you can use an Interaction Overview diagram, which provides an overview of sub activities that are involved in a system.</p>
Display System Behavior	<p>In displaying the behavior of a system as a Use Case diagram, Enterprise Architect provides an easily understood tool for</p>

	mapping the functional requirements and behavior of a system.
--	---

Software Architects

Software Architects can use Enterprise Architect to map functional requirements with Use Cases, perform real time modeling of objects using Interaction diagrams (Sequence, Timing, Communication or Interaction Overview), design the Deployment model and detail the deliverable components using Component diagrams.

Software Architect Tasks

Task	Detail
Map Functional Requirements of the System	With Enterprise Architect you can take the high level business processes that have been modeled by the Business Analyst and create detailed Use Cases. Use Cases describe the proposed functionality of a system and are only used to detail a single unit of discrete work.
Map Objects in Real Time	You can use Interaction diagrams (Sequence and Communication diagrams) to model the dynamic design of the system. Sequence diagrams detail the messages

	<p>that are passed between objects, and the lifetimes of the objects.</p> <p>Communication diagrams are similar to Sequence diagrams, but instead display the way in which the object interacts with other objects.</p>
Map Deployment of Objects	<p>You can use Deployment diagrams to provide a static view of the run-time configuration of processing nodes and the components that run on the nodes.</p> <p>Deployment diagrams show the connections between hardware, software and any middleware that is used on a system.</p>
Detail Deliverable Components	<p>Using Component diagrams, you can model the physical aspects of a system. Components can be executables, libraries, data files or another physical resource that is part of a system.</p> <p>The component model can be developed from scratch from the Class model or can be brought in from existing projects and from third-party vendors.</p>

Software Engineers

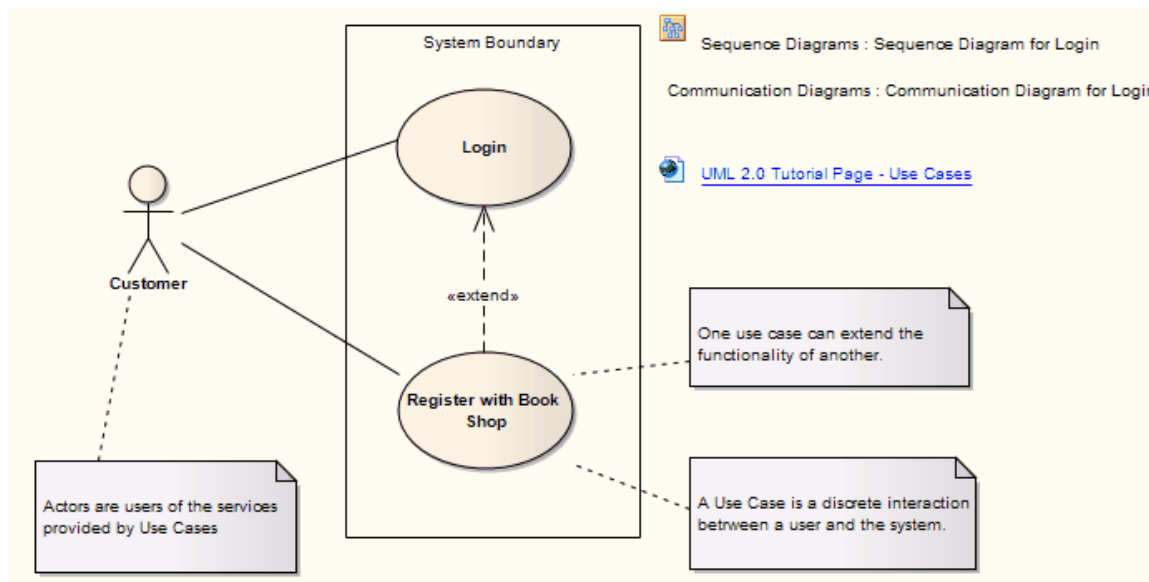
Software Engineers using Enterprise Architect can manually map Use Cases onto Class diagrams, detail the interactions between Classes, define the system deployment with Deployment diagrams and define software Packages with Package diagrams.

Software Engineering Tasks

Task	Detail
Map Use Cases into Detailed Classes	<p>Within Enterprise Architect you can study the Use Cases developed by the Software Architect, and with that information create Classes that fulfill the objectives defined in the Use Cases.</p> <p>A Class is one of the standard UML constructs that is used to detail the pattern from which objects are produced at run time; to record the relationships between Use Cases and Classes, you can create diagrams linking the elements with Realization connectors, and/or map the Realization connectors in the Relationship Matrix.</p>

<p>Detail Interaction Between Classes</p>	<p>You can use Interaction diagrams (Sequence and Communication diagrams) to model the dynamic design of the system.</p> <p>Sequence diagrams are used to detail the messages passed between objects, and the lifetimes of the objects.</p> <p>Communication diagrams are similar to Sequence diagrams, but instead display the way in which objects interact with other objects.</p>
<p>Define System Deployment</p>	<p>Deployment diagrams provide a static view of the run-time configuration of processing nodes and the components that run on the nodes.</p> <p>Deployment diagrams can be used to show the connections between hardware, software and any middleware that is used on a system, to explain the connections and relationships of the components.</p>
<p>Define Software Packages</p>	<p>You can use Package diagrams to detail the software architecture.</p> <p>Package diagrams are used to organize diagrams and elements into manageable groups, declaring the dependencies.</p>

Simple Use Case diagram



Developers

Developers can use Enterprise Architect to perform round trip code engineering, which includes reverse engineering of existing code and generation of code from Class elements.

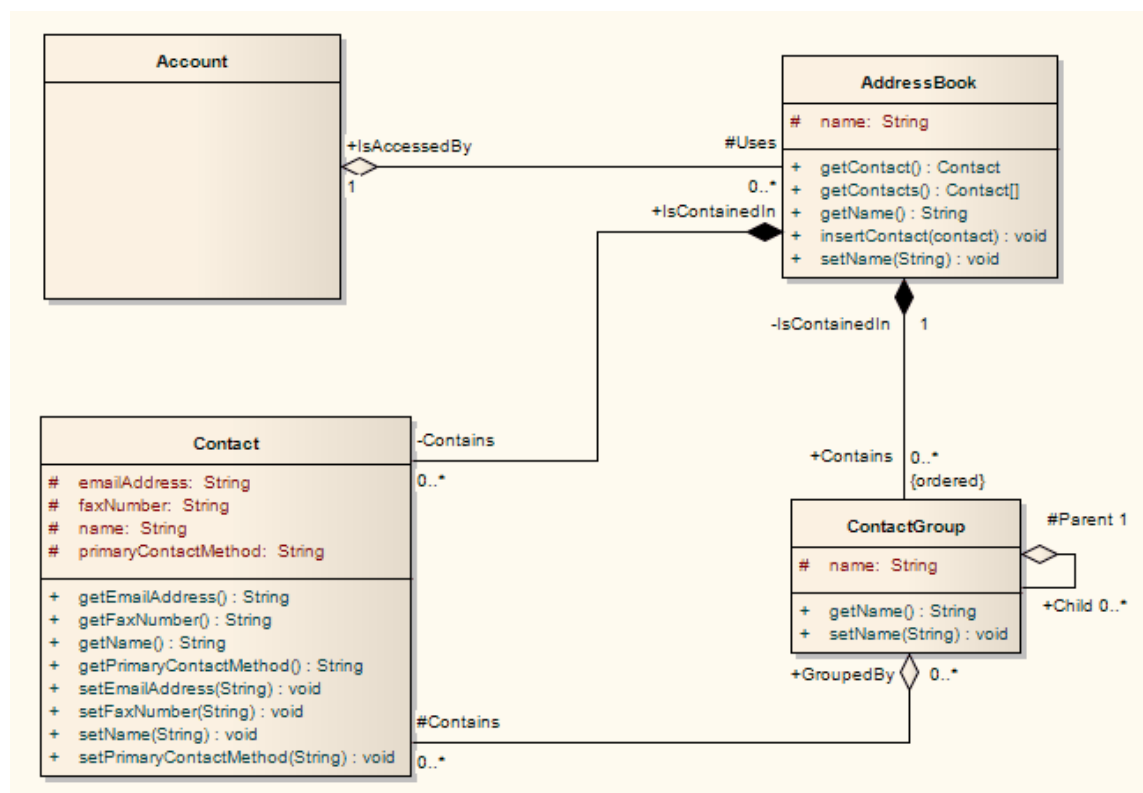
Developer Tasks

Task	Detail
Round Trip Engineering	<p>Enterprise Architect gives you unparalleled flexibility in 'round tripping' software from existing source code to UML 2.5 models and back again.</p> <p>Round trip engineering involves both forward and reverse engineering of code, keeping the model and code synchronized.</p>
Reverse Engineering	<p>In Enterprise Architect, you can reverse engineer code from a number of supported languages and view the existing code as Class diagrams, which illustrate the static design view of the system.</p> <p>Class diagrams show Classes and interfaces, and the relationships between</p>

	<p>them; the Classes defined in UML Class diagrams can have direct counterparts in the implementation of a programming language.</p>
Forward Engineering	<p>As well reverse engineering your code into your model, you can forward engineer elements of your model into code (code generation).</p> <p>This way you can make changes to your model with Enterprise Architect and quickly implement the changes in the source code.</p>
Determine the System State	<p>To visualize the state of the system you can use StateMachine diagrams to describe how elements move between States, classifying their behavior according to transition triggers and constraining guards.</p> <p>StateMachine diagrams capture system changes over time, typically being associated with particular Classes; often a Class can have one or more StateMachine diagrams to fully describe its potential states.</p>
Visualize Package	<p>Package diagrams help you design the architecture of the system; they are used</p>

Arrangement	to organize diagrams and elements into manageable groups, and to declare their dependencies.
Follow the Flow of Code	Activity diagrams help you develop a better understanding of the flow of code. Activity diagrams illustrate the dynamic nature of the system; you can model the flow of control between Activities and represent the changes in state of the system.

Simple Class Diagram



Notes

- You can use StateMachine, Package and Activity diagrams to better understand the interaction between code elements and the arrangement of the code

Project Managers

Enterprise Architect provides support for the management of projects. Project Managers can use the system to assign resources to elements, measure risk and effort, estimate project sizes, and manage element status, change control and maintenance.

Project Manager Tasks

Task	Detail
Provide Project Estimates	In Enterprise Architect you have access to a comprehensive project estimation tool that calculates effort from Use Case and Actor objects, coupled with project configurations defining the technical and environmental complexity of the work environment.
Resource Management	Managing the allocation of resources in the design and development of system components is an important and sometimes difficult task; Enterprise Architect provides you with an effective tool for assigning resources directly to model elements and tracking progress

	over time.
Risk Management	You can use the Risks window to assign risk to an element within a project; using risk types you can name the risk, define the type of risk and give it a weighting.
Maintenance	<p>Within Enterprise Architect you can assign maintenance-related items to elements and track them, providing rapid capture and record keeping for items such as features, changes, documents, issues, defects and tasks.</p> <p>You can also create and maintain a Project Glossary of processes, procedures, terms and descriptions.</p>

Testers

Enterprise Architect provides a design testing facility for Testers and Quality Assurance personnel to create a range of test scripts against elements in the modeling environment.

Testing Tasks

Task	Detail
Test Cases	<p>With Enterprise Architect, you can set up a series of tests for each model element. The test types include Unit, Acceptance, System, Integration, Inspection and Scenario tests.</p>
Import requirements, constraints and scenarios	<p>To use testing to maintain the integrity of the entire business process, you can import requirements, constraints and scenarios defined in earlier iterations of the development life cycle.</p> <p>Requirements indicate contractual obligations that elements must perform within the model.</p> <p>Constraints are conditions that must be met in order to pass the testing process; constraints can be:</p>

	<ul style="list-style-type: none">• Pre-conditions (states that must be true before an event is processed)• Post-conditions (events that must occur after the event is processed) or• Invariant constraints (which must remain true through the duration of the event) <p>Scenarios are textual descriptions of an object's action over time and can be used to describe the way a test works.</p>
Create quality test documentation	Enterprise Architect provides the facility to generate high quality test documentation in .RTF, DOCX and PDF file formats.
Element defect changes	In defect tracking you can allocate defect reports to any element within the model, so that all who are involved in the project can quickly view the status of defects and see which defects have to be addressed and which have been dealt with.

Implementation Managers

Enterprise Architect provides support for the management of project implementation. You can track and assign maintenance -related items to elements within Enterprise Architect, and rapidly capture and update records of maintenance tasks such as features, changes, documents, issues, defects and tasks. By providing a centralized facility for each element involved in the deployment process Enterprise Architect offers a powerful solution for tracing the maintenance of the items and processes involved in system deployment.

Implementation Tasks and Tools

Task	Detail
Develop Deployment Diagrams	<p>Using Deployment diagrams, you can model the roll out of a project, including network deployment and workstation deployment.</p> <p>Users involved in project deployment can add maintenance tasks to the diagram elements.</p> <p>Deployment diagrams provide a static view of the run-time configuration of nodes on the network or of workstations,</p>

	and the components that run on the nodes or are used in the workstations.
--	--

Technology Developers

Technology Developers are Enterprise Architect users who create customized additions to the functionality already present within Enterprise Architect.

Additions include UML Profiles, Patterns, Code Templates, **Tagged Value Types**, Scripts, Custom Queries, Transformations, MDG Technologies and Enterprise Architect **Add-Ins**. By creating these extensions the Technology Developer can customize the Enterprise Architect modeling process to specific tasks and speed up development.

Developing Technologies

Extension	Detail
UML Profiles	<p>By creating UML Profiles you can create a customized extension for building UML models that are specific to a particular domain.</p> <p>Profiles are stored as XML files and can be imported into any model as required.</p>
Patterns	<p>Patterns are sets of collaborating Objects and Classes that provide a generic template for repeatable solutions to</p>

	<p>modeling problems.</p> <p>As Patterns are discovered in any new project, you can publish the basic Pattern template.</p> <p>Patterns can be re-used with the appropriate variable names modified for any future project.</p>
Code Templates	<p>Code templates are used to customize the output of source code generated by Enterprise Architect; in this way you can generate code languages not specifically supported by Enterprise Architect and define how the system generates source code to comply with your own company style guidelines.</p>
Tagged Value Types	<p>Tagged Values are used in Enterprise Architect to extend the information relating to an element in addition to the information directly supported by the UML language.</p> <p>A Tagged Value, strictly, is the value of a property of a modeling item, the property being called a tag; for example: a Class element called Person might have a tag called 'Age' with the Tagged Value of '42'.</p> <p>More loosely, the combination of tag and</p>

	<p>value can be referred to as a Tagged Value.</p> <p>A Tagged Value Type is a group of parameters that define and/or limit the possible values of a tag and, in many instances, how a specific value is assigned to the tag; for example, the tag 'Age' might have a Tagged Value Type of 'Integer', so the user simply types in a numeric value.</p> <p>Alternatively, the type could be 'Spin', with lower and upper limits of, say, 20 and 120, so the user sets a value by clicking on arrows in the field to increment or decrement the value within the limits of 20 and 120.</p> <p>Typically, Tagged Values are used during the code generation process, or by other tools to pass on information that is used to operate on elements in particular ways.</p>
MDG Technologies	MDG Technologies can be used to create a logical collection of resources that can contain UML Profiles, Patterns, Code Templates, Image files and Tagged Value types that are accessed through a technology file.
Enterprise	Using Add-Ins you can build your own

Architect Add-Ins	functionality into Enterprise Architect, creating your own mini programs that can extend the capabilities of the system, defining your own menus, and creating your own Custom Views.
----------------------	---

Database Developers

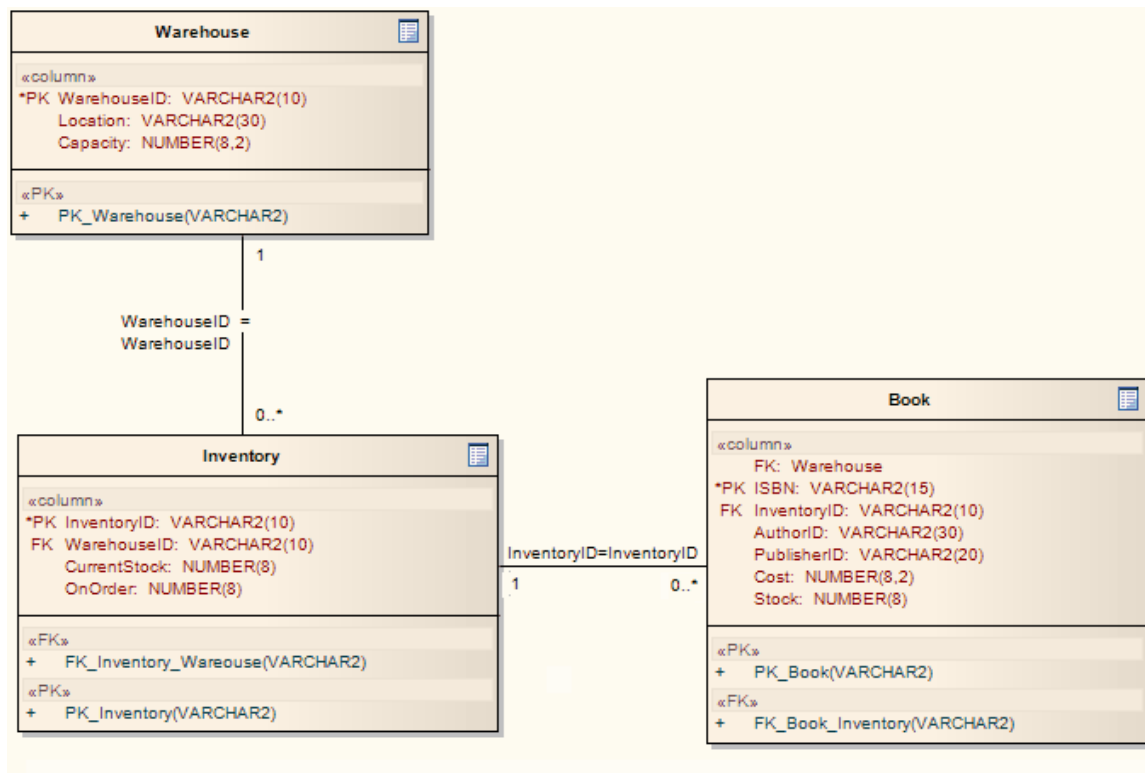
Enterprise Architect supports a range of features for the development of databases, including modeling database structures, importing database structures from an existing database and generating DDL for rapidly creating databases from a model.

Database Development Tasks

Task	Detail
Create Logical Data Models	<p>With Enterprise Architect you can build database diagrams using the built-in UML Data Modeling Profile.</p> <p>This supports the definition of Primary and Foreign Keys, cardinality, validation, triggers, constraints and indexes.</p>
Generate Schema	<p>By using Enterprise Architect's DDL generation function you can create a DDL script to create the database table structure from the model.</p> <p>Enterprise Architect currently supports:</p> <ul style="list-style-type: none">• DB2• Firebird

	<ul style="list-style-type: none">• MS Access• MySQL• MS SQL Server• Oracle• PostgreSQL
Reverse Engineer Database	<p>Using an ODBC data connection you can import a database structure from an existing database to create a model of the database.</p> <p>By generating the model directly from the database you can quickly document your work and create a diagrammatic account of a complex database through the graphical benefits of UML.</p>

Example Data Model Diagram



User Security

User Security in Enterprise Architect is a means of blocking the use of model update functions across the model by means of access permissions for each function, and protecting specific elements and diagrams from change by means of user **locks**. The intent is not to prevent access to information, but to prevent inadvertent changes to data.

Security is an optional facility in the system. If required it is enabled by the Security Administrator, who at the same time sets the security policy to either:

- Require User Lock to Edit - the whole project is blocked against editing and the user locks an object to open it and edit it, or
- User/group locking - the whole project is open for editing and the user locks an object to protect it from being edited

The Security Administrator also sets up the user and group IDs and passwords, which every user requires to log in to the model when security is enabled. Access permissions are assigned to the user IDs to determine which update functions the user can apply. The users can still view any information in the project. If security is not enabled in the project, no login is required and users do not have to have access permissions to perform update functions.

Access

Ribbon	Configure > Security
--------	----------------------

Security Operations

Operations For	Detail
Administrators	<p>A number of security tasks can be performed only by users with Administrative permissions to the security operations. The person who enables security receives online instructions to login as Admin. This login ID automatically:</p> <ul style="list-style-type: none">• Has access permissions to perform all security operations• Is a member of an Administrators user group, which also has access permissions to perform all security operations
Users	<p>Other security tasks can be performed by users who do not have Administrative rights, on work performed under their own user ID. These users must still have</p>

	the appropriate access permissions to perform many of these 'user' tasks.
--	---

Notes

- User Security can be enabled in the Corporate, Unified and Ultimate Editions of Enterprise Architect

Enable/Disable Security

User security is not automatically enabled on the system. If your organization requires the security facilities, the Security Administrator enables them using an authorization key obtained from the Sparx Systems website. Similarly, if security facilities are no longer required, the Security Administrator explicitly disables security, again using the authorization key.

Access

Ribbon	Configure > Security > Administer > Enable Security
--------	---

Enable and Disable User Security

Step	Action
1	Obtain the authorization key from the Sparx Systems website on: <ul style="list-style-type: none">the 'Team Modeling Resources' section (Trial

	<p>User) or</p> <ul style="list-style-type: none">the 'Registered Users' section (Registered User; you must also have your Registered Users login and password) <p>The two authorization keys are not interchangeable - the Trial User key does not work on a registered user installation.</p>
2	<p>In Enterprise Architect, select the 'Enable Security' menu option.</p> <p>The 'Enter authorization' dialog displays.</p>
3	<p>In the 'Enter authorization key' field, type the authorization key from the Sparx Systems website.</p>
4	<p>If required, select the 'Automatically apply Exclusive Edit Locks to diagrams' checkbox.</p> <p>In standard (User/Group Locking) mode, this option blocks multiple users from simultaneously attempting to modify the same diagram (see <i>Notes</i>).</p> <p>This option is ignored in 'Require User Lock to Edit' security mode.</p>
5	<p>Click on the OK button.</p> <p>Security is enabled, and an Admin user and Administrators user group are created, both with all access permissions; the Admin user has the password of 'password'.</p>

6	Select the 'Configure > Security > Administer > Login as Another User' ribbon option, and log in as 'admin' with the initial password of 'password'. It is recommended that you change the Admin password immediately.
7	Set up users and permissions as required.

Notes

- Once security has been enabled, you must have 'Security-Enable/Disable' permission to turn it off - the initial Admin administrator and Administrators group automatically have this permission; the system prompts you to log off the project and log on again, but this is not strictly necessary
- If you re-enable security, be aware that any changes you have made to the Admin user (password and reduced access permissions) are reset to 'password' and full access; similarly, the Administrators user group is reinstated with full access permissions
- 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

- If the 'Automatically apply Exclusive Edit Locks to diagrams' option is selected, as a user modifies a diagram the system automatically applies a User Lock to the diagram, preventing any other user from modifying it. It is creating a difference between the database and buffer versions of the diagram that triggers the temporary lock, and elimination of difference that releases the lock; therefore, the system 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

Set Security Policy

The security policy determines how security mechanisms are applied and interpreted on the system. There are two possible security policies in Enterprise Architect:

- User/Group Locking mode - All elements and diagrams are considered unlocked and anyone can edit any part of the model; 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 and no other user can edit the object

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 write access to a part of the model

- Require User Lock to Edit mode - More rigorous: the model is read-only, and 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 **Browser window** 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

For element locking, the two policies are modified by the 'Apply Locks to Connectors' menu option. If this option is:

- Selected, security **locks** on elements are applied to all connectors owned by the locked elements (users other than the locking user cannot edit the connectors)
- Unselected, security locks on elements do not apply to the owned connectors

Access

Ribbon	Configure > Security > Administer > Require User Lock to Edit (select for 'Require User Lock to Edit' mode, deselect for 'User/Group Locking' mode)
--------	---

Notes

- Only the Admin Security Administrator, with Admin permissions, is able to set the security policy applied
- When you add new elements in 'User/Group Locking' mode (elements editable by default), no user lock is created automatically for the newly created element

- When you add new elements in 'Require User Lock to Edit' mode (elements locked by default), a user lock is created on the new element to enable instant editing
- For all connectors other than Aggregations, the connector is owned by the source element in the relationship (as currently applied in **Version Control**)

Maintain Groups

Whilst you can apply access permissions to each user individually, it is easier and more convenient to assign all users who are to have the same access permission(s) to a security group, and assign the permissions to the group in a single action.

The security group also acts as a mailbox for **Model Mail**, where the group name can be selected as the addressee; when an internal mail is sent to the group, all members of the group receive that email in their Model Mail inbox. The group name can act as either:

- A mail list, in which case each group member receives their own copy of the message, or
- A mail box, in which case the email is a single entity and the group members do not receive separate instances of it; if one group member responds to or deletes the email, the other group members see that action as if they had performed it themselves

Having created a security group, you can create a Perspective Setting and/or a Ribbon Set for the group, to hide the **Perspectives** and ribbons that the group members are unlikely to use or are not permitted to use. See the *Perspectives for Security Groups* Help topic.

Access

Ribbon	Configure > Security > Groups
--------	-------------------------------

Set up a security group

Field/Button	Action
New	Click on this button to clear the fields ready to define a new group.
Group Name	Type the security group name.
Description	Type a description of the group.
Save	Click on this button to save the group definition and add it to the Groups list.
Link to Active Directory	Select this checkbox to enable linking to a Windows Active Directory Group from which to import users. The 'Select Group' dialog displays on which you specify the Windows Active Directory Group to attach to. You then start importing the users when you click on the Sync button . You must have 'Accept Active Directory Authentication' permission in Windows

	to link to the Active Directory; an error message displays if you do not have this.
OpenID Group	<p>This feature is available from Enterprise Architect Release 14.1.</p> <p>OpenID groups can be linked to local model groups - this is used if the option to automatically create or modify OpenID users is set. When a new user logs in they will be assigned to the local groups that correspond with the OpenID groups they belong to. When an existing user logs in they will be assigned to the linked OpenID groups they belong to and removed from any they don't belong to.</p> <p>If OpenID login has been enabled for the model, then local groups can be linked to OpenID groups.</p> <p>Type the name of the OpenID group to be linked to the local model group, note that the group name is case sensitive.</p> <p>Note: OpenID login must be enabled in the 'Security Users' dialog; see the <i>Maintain Users</i> Help topic.</p>
Shared Mail	<p>To make the group name act as a mail box, select this checkbox against the name in the list.</p> <p>To use the group name as a mail list,</p>

	leave the checkbox unselected.
Active Directory Link	Displays the address of the Active Directory Group that this user group is linked to, if any.
Sync	Enabled if the group is linked to a Windows Active Directory. Click on this button to synchronize the group with the Active Directory (that is, import specific users into the model from the Active Directory). You use this option when you initially set up the User Group; subsequent user IDs must be added to the user group manually.
Permissions	Lists the permissions that can be assigned to the user group. Select the checkbox against each permission the members of the group are to have.
Users	After you add users to the user group, they are listed in this panel.
Close	Click on this button to close the dialog.

Notes

- You must have 'Security - Manage Users' permission to manage user groups; the initial Admin administrator and Administrators group automatically have 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 that all group members use (that is, Enterprise Architect allows multiple logins under one user ID)
- Users that have been imported from an Active Directory are listed in the 'Manage Users' dialog; if the 'Accept Windows Authentication' option is enabled on that dialog, when a user opens the model the system checks the database for their Windows ID and, if it matches, automatically logs the user in without prompting for a password
- Emails already sent to a group as a mail list and those sent to a group as a mailbox cannot be interchanged; if you change the status of the 'Shared Mail' checkbox, the only way to change the distribution of past emails is to forward them to the group name again
- You can subsequently edit the group name; changes are automatically reflected in the internal **Model Mail** mail list or mail box

Security Group Workflow

The security group workflow is a means of managing the transition of elements through a series of stages defined by an element property such as the Status, so that the elements can only pass from one stage to the defined next stage and not get arbitrarily set to a much later (or earlier) stage. Control is applied when the user changes an element's property through the **Properties window** or 'Properties' dialog, or through a Kanban diagram bound to the element property.

You can manage workflow through the Workflow Scripting Engine, but by setting up a workflow definition in the User Security facility you can make use of the existing security groups to finely and tightly control which users can move an element between certain states. For example, applying the element 'Status' property:

- Developers (Security Group 'Dev') can change Status only from:
 - 'Proposed' to 'In Progress'
 - 'In Progress' to 'Implemented'
 - 'Reviewed' to 'Merged'
- Reviewers (Security Group 'Rev') can change Status only from:
 - 'Implemented' to 'Reviewed' or
 - 'Implemented' to 'In Progress'
- Testers (Security Group 'Test') can change Status only from:

- 'Merged' to 'Tested'

- Project Managers (Security Group 'PMan') can change Status from any value to any previous value

Note: Currently, the Security Group Workflows can be set only on the 'Status' element property.

Prerequisites

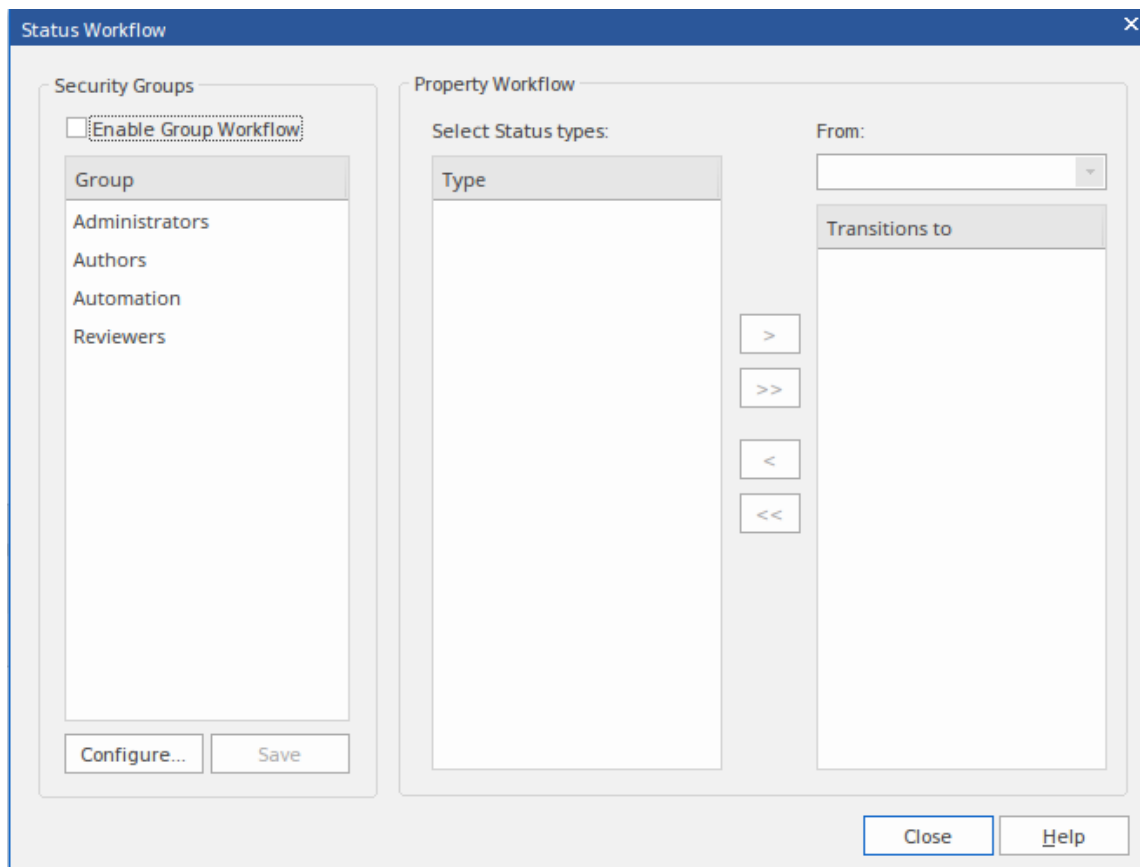
User Security must be enabled, and the appropriate User Security Groups set up (although you can add and delete Security Groups during the process described here).

Access







Ribbon	Configure > Security > Administer > Group Workflow
--------	--

Set up Workflow on Security Groups

The 'Status Workflow' dialog is displayed.



Step	Action
1	<p>Select the 'Enable Group Workflow' checkbox to enable security group workflows.</p> <p>(Later, clear the checkbox if you want to suspend any currently-defined workflows for a period.)</p>
2	<p>In the 'Group' panel, click on the required security group.</p> <p>(If the required group is not listed, click on the Configure button to display the 'Security Groups' dialog and create the group.)</p>

	The available values for the Status property are listed in the 'Type' panel.
3	In the 'From' field, click on the drop-down arrow and select the Status value that the users in the selected security group can change.
4	<p>In the 'Type' panel, click on the value that the users can change the status <i>to</i>, and then click on the  button to transfer that value to the 'Transitions to' panel. You can transfer all values to the 'Transitions to' panel by clicking on the  button.</p> <p>If you need to correct or otherwise remove values from the 'Transitions to' panel, use one of these two buttons:</p> <div> </div> <p>As an example, if you wanted to allow Reviewers to transition elements from 'Implemented' to 'Reviewed' or 'In Progress', you would select 'Implemented' in the 'From' field and click on 'Reviewed' and the  button, and then click on 'In Progress' and the  button.</p>
5	Click on the Save button .

You can now either:

- Repeat steps 3-5 and assign another rule to the same security group, to allow them to transition from another value
- Repeat steps 2-5 and assign rules to a different security group, to allow them to transition from one value to one or more others
- Click on the **Close button** and stop defining security group workflows

Maintain Users

When you have enabled security, you create the user definition for each user that has access to the model. The user definition consists of the user ID and password, the permissions the user has, the user groups the user is a member of, and whether the user ID is provided and validated by external user authentication mechanisms.

Access

Ribbon	Configure > Security > Users: New The 'Security Users' dialog displays.
--------	--

Set up a user for your model

Security Users

User Details

Login:

Firstname: Surname:

Department:

☒ Add User to Authors

Users:

Surname	Firstname	Login
Lockley	Alistair	alesliehughes
Loyd	Hugh	hloyd
Maguire	Stephen	smaguire
Mega	Stephen	smeagher
Meter	Miles	mma
Montique	Paul	pmathers
Nichols	Greg	_gregnichols
Nielsen	Ken	_kennielson
Minrace	Campbell	crinrace

☒ Allow 'Remember Me'

☒ Accept Windows Authentication ☐ Allow non-domain users (insecure)

☐ Accept OpenID Authentication

☐ Restrict access to Windows & OpenID users only

☐ Automatically create or modify Windows or OpenID users

User Groups

☐ Administrators

☐ Authors

☐ Automation

☐ Help Review

☐ Reviewers

User Permissions

☐ Configure Model Add-Ins

☐ Configure External Data Sources

☐ Visibility Level Admin

☐ Run Scripts

☐ Edit Scripts

☐ Configure Project Prerequisites

☐ Manage Project Calendar

☐ Manage Glossary

☐ Admin Workflow

☐ Baselines - Restore model

☐ Baselines - Manage

☐ Transform Package

☐ Audit View

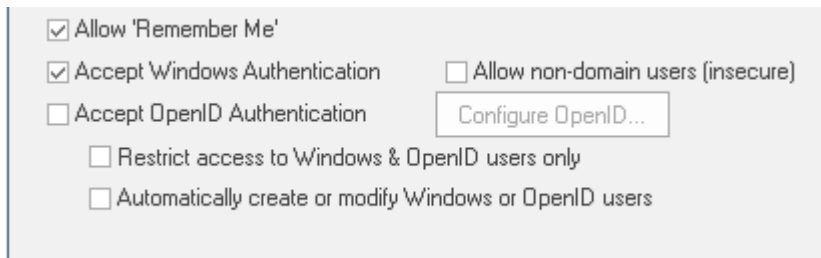
☐ Audit Settings

☐ Use Version Control

☐ Configure Version Control

Step	Action
1	<p>You can manage users in multiple ways:</p> <ul style="list-style-type: none"> • Set up the user manually, as described here • Import the user IDs from a Windows Active Directory • Trust the user information from a third-party Single Sign-On system and allow it to manage users <p>If you are importing the user IDs from a Windows Active Directory, do not complete any user detail fields on this dialog, but select the 'Accept Windows Authentication' checkbox and go to the <i>Import User IDs from Active Directory</i> Help topic. Note that the option 'Allow non-domain users (insecure)' will, if selected, also allow auto-login of a user who is not a</p>

user of the domain. If the option is not selected and the user is not a user of the domain, the auto-login is aborted. The option defaults to unselected when security is being enabled, but in existing enabled systems it will be selected.



The screenshot shows a configuration window with the following options:

- ☒ Allow 'Remember Me'
- ☒ Accept Windows Authentication
- ☐ Accept OpenID Authentication
- ☐ Restrict access to Windows & OpenID users only
- ☐ Automatically create or modify Windows or OpenID users
- ☐ Allow non-domain users (insecure)
- [Configure OpenID...](#)

To allow automatic management of users by a single Sign-On (SSO) system, tick the SSO mechanism to use (either 'Accept Windows Authentication' or 'Accept OpenID Authentication') and tick 'Automatically create or modify Windows or OpenID users'. See the *Single Sign-On (SSO) Options* Help topic for more details.

2

In the:

- 'Login' field, type the user ID
- 'Firstname' field, type the user's first name
- 'Surname' field, type the user's last name

Optionally, in the 'Department' field, type the name of the user's department.

The 'Add User to Authors' checkbox defaults to selected, to add the new user to the list of authors of model elements. If the user is not to be added to the list of authors, deselect the checkbox.

3	<p>Click on the Save button, and then click on the Change Password button.</p> <p>The 'Change Password' dialog displays.</p>
4	<p>In the 'New password' field, type the user's password.</p> <p>This can be any number of characters in length.</p> <p>(As this is a new user, the 'Enter old password' field is disabled.)</p>
5	<p>In the 'Retype new' field, type the user's password again, for confirmation.</p>
6	<p>Click on the OK button.</p> <p>A <i>Password Changed</i> message displays.</p> <p>Click on the OK button to return to the 'Security Users' dialog.</p>
7	<p>In the 'User Groups' panel, select the checkbox against each user group that the user is to be a member of. This assigns to the user all permissions that the selected groups have.</p>
8	<p>In the 'User Permissions' panel, select the checkbox against each permission that you want to assign to the user as an individual. If a permission is grayed out and already ticked, the user already has that permission as a member of a User Group.</p>

9	The top right corner of the Enterprise Architect display shows your user ID, with a short drop-down menu providing personal access options including whether your login credentials are stored and automatically applied when you open the model ('Remember Me'). If you want to use this option, you must select the 'Allow 'Remember Me" checkbox on this 'Security Users' dialog.
10	The user definition is complete. You can now either: <ul style="list-style-type: none">• Click on the New button to add another user, or• Click on the Close button to exit the 'Security Users' dialog

Notes

- You must have 'Security - Manage Users' permission to maintain users; the initial Admin administrator and Administrators group automatically have this permission
- You can transport the user definitions between models as Reference Data, using the 'Configure > Model > Transfer > Export Reference Data' and 'Import Reference Data' options
- In communications between users, such as in Chats or **Discussions**, it is possible to represent each user by a

personalized Avatar against their messages and postings;
to load and assign the images for these Avatars, see the
Set User Avatar Help topic

Set User Avatar

When you are contributing to element discussions or Chats, your contributions are indicated by your user ID. You can also define an icon that represents your User ID - that is, an avatar - to display in front of your ID, so that your statements can be more easily recognized in the conversation. This avatar is defined for your user ID within the model.

User security must be enabled in order to identify each user and hence display their avatars in the discussions.

Define an Avatar

1. Create and/or locate a suitable image to use as your avatar.
2. In Enterprise Architect, drag the 'Image Asset' icon from the 'Artifact' page of the **Diagram Toolbox** onto a diagram.
3. The 'Select an Image' dialog automatically displays; browse for and select the image you have identified to use as your avatar.
4. Save the diagram.

Assign the Avatar

1. Select the 'Configure > Security > Administer > Set Avatar' ribbon option.
 2. The 'Select image for avatar' dialog displays. Browse for and select the Image Asset Artifact you created earlier.
 3. Click on the **OK button**. The image is associated with your user ID.
 4. Open the **Collaborate window (Ctrl+9)** and create a discussion item, then click away from it. Your avatar should now display against the message you have created.
- You can repeat the process with a different image if you decide to change your avatar.

Single Sign-On (SSO)

Single Sign-On (SSO) enables a model to trust a third-party authentication system to log in to a model. Instead of logging in to Enterprise Architect, the user logs into a third-party system that authenticates the user as valid and allows them access to Enterprise Architect. Enterprise Architect trusts the authentication returned from the SSO system and logs the user in to the model.

Enterprise Architect supports two SSO systems:

- Windows authentication with Active Directory
- OpenID - This feature is available from Enterprise Architect Release 14.1

SSO systems

Windows Authentication	<p>Windows Authentication allows a model to trust the currently logged in Windows user. If the username returned from the Windows system matches a model user, then the model is logged in as that user.</p> <p>Windows Authentication works best when run with an Active Directory Domain.</p> <p>You can enable Windows Authentication</p>

	by selecting the 'Accept Windows Authentication' checkbox on the 'Security Users' dialog.
OpenID	<p>OpenID is the current preferred standard for SSO authentication for web sites. It also works well for applications such as Enterprise Architect. To use OpenID, an OpenID server must be configured and accessible by Enterprise Architect.</p> <p>There are many options for OpenID servers, including self-hosted servers and online services. Enterprise Architect requires an OpenID server that supports the 'OpenID Connect' standard and is able to return a unique user identifier in the 'user_info' request. This user identifier will be matched to a local model user.</p>

Single Sign-On (SSO) Options

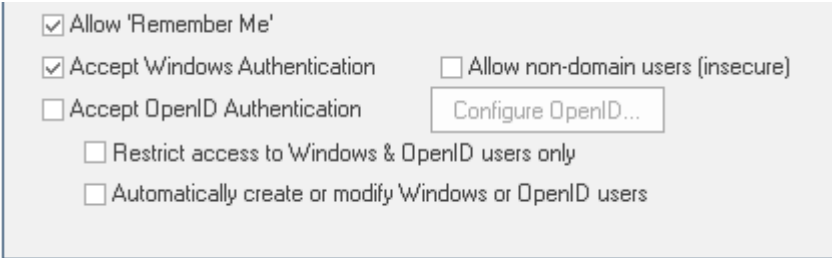
These options are available from Enterprise Architect Release 14.1.

After enabling SSO there are two main options that can be set:

- Restrict access to Windows and OpenID user only
- Automatically create or modify Windows or OpenID users

These options are detailed here.

Access

Ribbon	<p>Configure > Security > Users</p> 
--------	--

Restrict access to Windows and OpenID users only

Enabling this option will stop local model users from being able to log in to the model. Only users validated through either Windows or OpenID SSO will be able to log in.

An exception is made for local users who have the 'Security - Manager Users' permission set. This allows a local administrator to still have access and be able to update or modify the SSO settings.

Automatically create or modify Windows or OpenID users

Enabling this option will allow the model to create new users derived from the trusted SSO source. Users will be assigned local group permissions based on the groups linked to the SSO provider. Existing users will be assigned to or revoked from linked groups based on their SSO groups.

Notes:

- A new user that is not in any SSO groups that are linked to model groups, will not be automatically created
- An existing user that is not in any SSO groups that are linked to model groups, will not be logged in
- An existing user's individual permissions will not be modified automatically
- An existing user will not be removed from a group that is not linked to an SSO group

Note

It is recommended that you always keep a local model administrator account (with a strong password) to allow recovery in the case the SSO authentication fails (for example, if the OpenID server is offline or mis-configured)

Configure OpenID

This feature is available from Enterprise Architect Release 14.1.

To enable users to log in with an OpenID account, an OpenID server that supports the 'OpenID Connect' standard must be available.

These settings will be used by Enterprise Architect, Pro Cloud Server, and WebEA.

Access

Ribbon	Configure > Security > Users > Accept OpenID Authentication Configure > Security > Users > Configure OpenID
--------	--

Settings

Configure OpenID...

OpenID URL:

The following URL will be used to discover the OpenID configuration:

Callback URL - add this as a callback on the OpenID server:

Client ID:

Client Secret:

Scope:

Claim to Match to Local User:

Claim to Match to Local Groups:

Field	Action
OpenID URL	<p>Enter the full path to the discovery URL of the OpenID server, minus the standard <code>"/.well-known/openid-configuration"</code> (this will be appended automatically).</p> <p>Include the protocol (<code>http://</code> or <code>https://</code>), and the Port if running on a non-standard Port (that is, not 80 or 443).</p> <p>You should be able to copy the address with the <code>"/.well-known/openid-configuration"</code> appended and open it in a browser and see a text-based response.</p>

	Press the Test button now and click on 'Login with OpenID' to open a browser to the correct address. If the URL is incorrect or OpenID returns a malformed configuration response, an error message will display.
Client ID	OpenID needs to be configured with a client to allow Enterprise Architect to use its services. Enter the Client ID here.
Client Secret - (optional)	Some OpenID clients require a Client Secret to further secure the requests. If the client requires a secret, enter it here. It will be saved as an encrypted value.
Scope	Enter the OpenID scopes required to return a response with the required information. A scope of 'openid' is mandatory according to the standard. Other common scopes include 'profile' or 'email'.
Claim to Match to Local User	Enter the claim that will be returned when querying the OpenID 'user_info' that will be used to match the OpenID user to an existing model user login. 'Claims' are information fields that the OpenID server is claiming are true about

	<p>the authenticated user. Most OpenID servers allow this to be customized so it can be set up to return a claim field specifically for use with Enterprise Architect, if desired.</p> <p>Note: The only claim that is guaranteed to be unique for a user is 'sub'. This is the 'subject' of the claim. For new models this would be a good default setting in the claim field.</p> <p>For existing models where there are already users in the model that should be matched to OpenID, it is recommended to use a 'username' field of some sort. Either the standard 'preferred_username', 'email' (if email is used, it is recommended that email validation is enabled) or a custom 'EA username' would make sense in this situation.</p> <p>If using a claim other than 'sub' it is up to the maintainer of the OpenID server to ensure that the claim is unique and secure, and to ensure the claim can not be edited by the user.</p>
Claim to Match to Local Groups	<p>This option is used if the additional setting 'Automatically create or modify Windows or OpenID users' is enabled. It is not used otherwise. See the <i>Single</i></p>

Sign-On (SSO) Options Help topic.

Enter the claim that will be returned when querying the OpenID 'user_info' that will be used to match the OpenID user's groups to existing model groups.

'Claims' are information fields that the OpenID server is claiming are true about the authenticated user. Most OpenID servers allow this to be customized so it can be set up to return a claim field specifically for use with Enterprise Architect, if desired.

The OpenID standard does not specify anything in regards to user groups. Some OpenID servers have this functionality built in but still need to be enabled so the groups can be returned in the 'user_info'. The returned groups can be either a single JSON field or a JSON array containing multiple group names.

Testing Connection

Once all fields are completed, press the **Test button**. A window will pop up with a 'Log in to OpenID' button. Click the button to open a web browser to the OpenID server

authentication page.

Provide valid credentials and allow Enterprise Architect access to the OpenID server account (this might or might not be required depending on the OpenID environment).

If successful, the browser should close automatically and Enterprise Architect will show a success window with the OpenID user's details, including any groups returned and the model groups they are linked to.

Example of a valid 'user_info' response

This is an example response for a 'KeyCloak' OpenID server.

Claim to Match to Local User: username

Claim to Match to Local Groups: groups

```
{
  "sub": "6da812c4-8f2c-400f-b602-13bab1d4605e",
  "address": {},
  "name": "Example Person",
  "groups": [
    "EA Special Users",
    "EA Administrators"
  ],
  "given_name": "Example",
  "family_name": "Person",
```



```
"email": "eperson@example.com",  
"username": "eperson"  
}
```

Import User IDs From Active Directory

Whilst you can define each of your model users individually and specifically for Enterprise Architect security, you can also import your Windows user IDs from Windows Active Directory and use those as the security user IDs with Windows Authentication. If you set up your security user IDs in this way, when a user opens the model the system checks the users database for their Windows ID and, if it matches, automatically logs the user in without prompting for a password.

As a pre-requisite, you create an appropriate user group into which to import the user IDs; you can also use this to assign appropriate permissions to the user IDs as a whole.

Access

Ribbon	Configure > Security > Users
--------	------------------------------

Import user IDs from Windows Active Directory

Ste	Action
-----	--------

p	
1	<p>On the 'Security Users' dialog do not complete any user details fields. Instead, select the 'Accept Windows Authentication' checkbox and click on the Import button.</p> <p>The 'Import Users' dialog displays.</p>
2	<p>In the 'Security Group' panel, select the checkbox against the appropriate security group to contain the imported user IDs.</p>
3	<p>Click on the Add button.</p> <p>The 'Select Users' dialog displays.</p>
4	<p>If the 'Select this object type' field has not defaulted to 'Users':</p> <ol style="list-style-type: none">1. Click on the Object Types button; the 'Object Types' dialog displays2. Select the checkbox against 'Users' (the type of object to import from the Active Directory).3. Click on the OK button to return to the 'Select Users' dialog.
5	<p>Click on the Locations button.</p> <p>The 'Locations' dialog displays.</p>
6	<p>Browse for and select the location to import from,</p>

	<p>within the Active Directory.</p> <p>Click on the OK button to return to the 'Select Users' dialog.</p>
7	<p>In the 'Enter the object names to select' field, either:</p> <ul style="list-style-type: none">• Type in the user IDs individually (click on the examples link to see examples of the correct formats) and go to step 13, or• Click on the Advanced button to search for IDs; the 'Select Users' dialog redisplay shows a 'Common Queries' tab
8	<p>In the 'Name' and 'Description' fields, type any characters or text that help identify the IDs you are searching for.</p>
9	<p>In the 'Starts with' field, click on the drop-down arrow and, if necessary, select a different qualifier.</p>
10	<p>Optionally, to further filter the IDs to search for, select the 'Disabled accounts' or 'Non-expiring password' checkboxes, and/or select a value in the 'Days since last logon' field.</p>
11	<p>Click on the Find Now button to initiate the search, and to display a list of IDs in the bottom panel of the dialog.</p> <p>You can vary the types of information shown here by clicking on the Columns button and selecting the</p>

	column headings to display, then dragging the column titles into the sequence you prefer.
12	<p>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.</p> <p>The 'Select Users' dialog redisplay, with the selected ID or IDs listed in the 'Enter the object names to select' field.</p>
13	<p>Click on the OK button to redisplay the 'Import Users' dialog with the selected users' names listed in the 'Users' panel.</p>
14	<p>Click on the Import button to add the user IDs to the 'Security Users' dialog.</p>
15	<p>Click on a user ID to populate the dialog fields with the user ID details.</p> <p>You can also set group membership and/or single permissions here.</p>

Notes

- You must have 'Security - Manage Users' permission to maintain users; the initial Admin administrator and

Administrators group automatically have this permission

- As a security measure, the Windows Authentication is automatically deactivated if the project file is moved to a different location; once the file has been relocated, you can toggle the 'Accept Windows Authentication' checkbox to reactivate Windows Authentication
- Enterprise Architect generates random passwords for Windows user IDs; however, if necessary you can assign a new password to an imported user ID

List of Available Permissions

In the Corporate, Unified and Ultimate Editions, if security is enabled, users can update information if they have the appropriate access permissions for the data update tasks for that type of data. From version 16 and onwards, access restrictions can also be applied to specific users and groups, to prevent certain actions. These restrictions are aimed at preventing inadvertent deletion of model content. The tasks that a user can perform with each access permission and tasks that are prevented with each restriction are listed here.

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

Permissions

Permission	Enables the user to
Administer Database	Compact and repair a project database.
Admin Workflow	Develop and manage workflow scripts.

Audit Settings	Change the audit settings in the 'Audit Settings' dialog.
Audit View	Enable auditing and display data in the ' Audit View ' and 'Audit History' tab.
Baselines - Manage	Create, delete, import and export Baselines .
Baselines - Restore model	Merge data into the project model from a Baseline or XML file.
Change Password	Change your own password.
Check Data Integrity	Check and repair project data integrity.
Configure Datatypes	Add, modify and delete datatypes.
Configure External Data Sources	When importing data from an external tool you need this permission to configure the default mapping values that determine what type of local elements are created in Enterprise Architect when the data is imported.

Configure Images	Configure alternative element images.
Configure Model Add-Ins	Allows users to enable and modify access to Add-In scripts according to the accessing user's membership of the defined security user group.
Configure Packages	Configure controlled Packages and Package properties.
Configure Project Prerequisites	Set up the: <ul style="list-style-type: none">• MDG Technologies that are mandatory, permitted or blocked for the project• Minimum version and build of Enterprise Architect required for the model
Configure Resources	Create and manage: <ul style="list-style-type: none">• 'Resources' tab items: document templates, Design Patterns, profiles• Available Project resources• CSV Specifications
Configure Stereotypes	Add, modify and delete Stereotypes.

Configure Version Control	Set up Version Control options for the current model.
Edit Scripts	Add, edit, delete and regroup model scripts.
Export-XML	Export a model to XMI or Enterprise Architect's Native XML format. Also required for CSV Import and Export, and for creating and editing CSV Specifications.
Generate Documents	Generate document and web reports from model Packages.
Generate Source Code and DDL	Generate source code and DDL from a model element, and synchronize code against model elements if it already exists.
Import XMI	Import a model from XMI or Enterprise Architect's Native XML format. Also required for CSV Import and Export, and for creating and editing CSV Specifications.
Lock Elements	Lock an element or Package.

Manage Diagrams	Create new diagrams, copy and delete existing diagrams, and publish a diagram as a Pattern.
Manage Glossary	Create, edit and delete glossary items in the Project Glossary .
Manage Issues	Update and delete model Issues.
Manage Project Calendar	Add, update and delete Project Calendar events; those without this permission can view calendar items.
Manage Project Settings	<p>Update and manage project-wide settings including:</p> <ul style="list-style-type: none">• The default element font size and type for the model• The model default diagram• Resource metrics, risks, efforts and allocation• Auto-created Diagram Image and Image Map• WebEA URL and Index
Manage Reference	Update and delete reference items.

Data - Update	
Manage Replicas	Create and synchronize replicas.
Manage Tests	Update and delete Test records.
Reverse Engineer from DDL and Source Code	Reverse engineer from source code or ODBC, and synchronize model elements against code.
Run Scripts	Run and debug a script.
Security - Enable/Disable	Disable user security in Enterprise Architect.
Security - Manage Locks	Delete element locks set by other users.
Security - Manage Users	Maintain users, groups and assigned permissions.

Spell Check	Spell check a Package and set the spell check language.
Transfer Data	Transfer model between different repositories.
Transform Package	Perform transformations of Packages and elements.
Update Diagrams	Update diagram appearance, properties and layout, including on the 'Page Setup' dialog.
Update Elements	Save model changes (including deletions) for elements, Packages, and relationships.
Use Version Control	Check files in and out using Version Control .
View Locks	Display all locks that have been set in the model.
Visibility Level Admin	Assign Visibility Levels to Packages in a model configured for Visibility Levels, on Oracle 8+ and Microsoft SQL Server 2016 databases, hosted on the Cloud by the Pro Cloud Server.

Restrictions

Restriction	Prevents the user from
Delete Package	Deleting packages
Delete Diagram	Deleting diagrams
Delete Element	Deleting elements
Delete Attribute	Deleting attributes from elements, or columns from data tables
Delete Operation	Deleting operations from elements, or constraints from data tables
Delete Connector	Deleting connectors
Import XMI	Importing XML package files (but does not prevent version control imports)
Restore from Baseline	'Restoring' a package from a previously saved baseline

Delete Baseline	Deleting saved package baselines
--------------------	----------------------------------

View All User Permissions

When a user has been set up on the system with their appropriate access permissions, you can periodically monitor the list of permissions to verify what they are able to do and check that their profile is up to date. The access permissions shown as selected are derived from their individual profile and from their membership of security groups.

Access

Ribbon	Configure > Security > Users
--------	------------------------------

Display the permissions assigned to a user ID

Step	Action
1	On the 'Security Users' dialog, select the user ID in the 'Users' list so that the details display in the 'User Details' panel.

2	Review the list of permissions in the 'User Permissions' panel. The user has all access permissions for which the checkbox is selected, and does not have the permissions for which the checkbox is clear.
---	--

Notes

- You must have 'Security - Manage Users' permission to maintain users; the initial Admin administrator and Administrators group automatically have this permission
- On this dialog you can select and deselect checkboxes in the 'User Permissions' panel to edit the user's individual access permissions, but you cannot change permissions assigned via the User Groups; click on the **Save button** to save any changes

View and Manage Locks

When security is enabled, users lock and unlock model elements in order to work on them, which can require monitoring and control. You can periodically view and, if necessary, delete the active **locks** placed on elements by users.

Access

Ribbon	Configure > Security > Locks
--------	------------------------------

Manage user locks

Step	Action
1	<p>On the 'Manage Locks' dialog, in the 'View Locks For' panel, click on the radio button for the type of lock to view.</p> <ul style="list-style-type: none">• All• Groups Only• Users Only

	Locks of the selected type are listed in the 'Active Locks' panel.
2	<p>To remove a lock, click on it and click on the Unlock Selected button.</p> <p>You can select (and deselect) multiple locks by pressing Ctrl as you click on each one, or Shift as you click on the last lock in a range.</p> <p>You can also select all locks in the list by clicking on the Select All button, and clear that selection by clicking on the Select None button (or by clicking off the list).</p>
3	When you have finished reviewing the locks , click on the Close button to close the dialog.

Notes

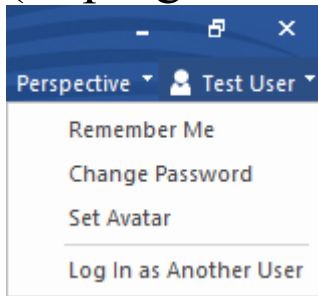
- You must have 'Security - Manage Locks' permission to delete user **locks**; the initial Admin administrator and Administrators group automatically have this permission
- You can view locks without the 'Manage Locks' permission, so that you can contact the lock owner if necessary
- The 'Manage Locks' dialog does not currently show any Full locks set in the model

- If you want to display the resulting information in a more readable layout, you can resize the dialog and its columns

Change Password

It is recommended that users of any computer system change their passwords - or have them changed - at regular intervals. When security is enabled in Enterprise Architect, users can change their own passwords or, if the user is unable or not authorized to do this, a Security Administrator can set or change the user's password.

Access

Ribbon	Configure > Security > Administer > Change Password (User) Configure > Security > Administer > Users (Administrator)
Other	(Top right corner of screen) >  > Change Password

User - Change your own user password

Step	Action
1	On the 'Change Password' dialog, in the 'Enter old password' field, type your current password.
2	In the 'New password' field, type your new password. This can be any number of characters in length.
3	In the 'Retype new' field, type your new password again, for confirmation.
4	Click on the OK button . The <i>Password Changed</i> message displays.
5	Click on the OK button to clear the message. Use your new password next time you log in.

Administrator - Set or change any user's password

Step	Action
------	--------

p	
1	<p>On the 'Security Users' dialog, in the 'Users:' panel, click on the user's name.</p> <p>The user's details display in the dialog fields.</p>
2	<p>Click on the Change Password button.</p> <p>The 'Change Password' dialog displays.</p>
3	<p>In the 'New password' field, type the user's new password.</p> <p>This can be any number of characters in length.</p> <p>You do not have to enter the user's current password.</p>
4	<p>In the 'Retype new' field, type the user's password again, for confirmation.</p>
5	<p>Click on the OK button.</p> <p>The <i>Password Changed</i> message displays.</p>
6	<p>Click on the OK button.</p>
7	<p>By secure means, notify the user of their new password.</p>

Notes

- A user must have 'Change Password' permission to change their own password; the initial Admin administrator and Administrators group automatically have this permission
- A Security Administrator must have 'Security - Manage Users' permission to change other users' passwords; the initial Admin administrator and Administrators group automatically have this permission

Hide Project Root

A project often contains a number of models to support different areas of development or administration. Any one user - other than perhaps the Project Manager or Administrator - is unlikely to be working across the whole structure, and would not need to see the entire project. Therefore, Enterprise Architect provides a facility to hide project Root Nodes and their contents on the basis of security group **locks**. The facility is not available on locks set on individual user IDs.

When you set a Group Lock on a Root Node, you can also select a checkbox to hide the Package in the **Browser window** from users who are not members of the locking group or Administrators. If you change the type of lock, or remove the lock altogether, the Package becomes visible to all users.

This feature hides the Root Package and its contents from initial view in the Browser window. It does not prevent the contents of the Package from being exposed in Model Searches. If you want to completely hide a Package from groups of users, consider Pro Cloud Server Visibility Levels.

Lock Model Elements

If you need to set a lock on a Package, element or diagram, or clear that lock, you can do so from either the **Browser window** or - for an element or diagram - from within a diagram. You follow one of three procedures, depending on whether you are:

- Locking an element or diagram under the 'User/Group Locking' security policy
- Locking a Package under the 'User/Group Locking' security policy
- Locking an element or diagram under the 'Require User Lock to Edit' security policy

You can also lock all elements, diagrams or Packages in a selected group, at once. The procedures are the same as for locking individual objects, subject to the comments provided here.

Notes

- You must have 'Lock Elements' permission to lock an element or diagram

Locking multiple objects together

You can select multiple objects in the **Browser window**, and lock them at the same time. The multiple objects should be of the same type; that is, several Packages OR several diagrams OR several elements. The selected objects must also have the same parent and therefore be peers.

When you have selected the objects to lock, right-click on one of them and:

- Under 'User/Group Locking' policy, select:
 - Lock Element(s)
 - Lock Diagrams(s) or
 - Lock Package(s)
- Under 'Require User Lock to Edit' policy, select:
 - Apply/Release User Lock(s)

If there is a locking conflict with any item to be locked - for example, a different user or group has locked the individual item - that item is ignored by the locking process and a warning error is added to the **System Output** window; this avoids multiple popup dialog warnings.

Lock Objects Under User/Group Locking

Under the User/Group Locking security policy, if you need to set or release a lock on an element or diagram, you can do so from either the **Browser window** or from within the diagram.

Access

Ribbon	<ul style="list-style-type: none">• Design > Diagram > Manage > Lock (on selected diagram)• Design > Element > Manage > Lock (on selected element)
Context Menu	<p>Select one of:</p> <ul style="list-style-type: none">• Browser window Right-click on diagram Lock• Browser window Right-click on element Lock• Browser window Select a Package, diagram or element and press Ctrl+Shift+L• On a diagram Right-click on diagram background Lock Diagram

	<ul style="list-style-type: none">• On a diagram Right-click on element Lock Element or• On a diagram Select an element and press Ctrl+Shift+L
--	---

Set a lock on an element or diagram

Step	Action
1	<p>On the 'Lock Element' or 'Lock Diagram' dialog, in the 'Lock Type' panel, select the radio button for the required option:</p> <ul style="list-style-type: none">• 'No lock' - do not set a lock on this object; clear any existing lock that you have set, or clear any Full lock that other users have set• 'Full lock' - lock this object so that no-one can edit it without specifically clearing the lock• 'User lock' - lock this object so that only you can make further edits; other users cannot unlock or edit the object• 'Group lock' - lock this object so that any member of the specified group can edit the object; other users cannot unlock or edit the object

2	<p>If you have selected the 'Group lock' option, in the 'GroupID' field click on the drop-down arrow and select the group containing users that can edit the object.</p> <p>The 'GroupID' drop-down list only includes groups that you are a member of.</p>
3	<p>Click on the OK button.</p>

Notes

- To check whether the project security is in User/Group locking mode, select 'Configure > Security > Administer'; the 'Require User Lock to Edit' option should be deselected
- You must have 'Lock Elements' permission to lock an element or diagram
- If the item already has a lock, only the corresponding lock option and the 'No lock' option are highlighted; you have to release the lock in order to set a different type of lock
- If a diagram is locked and you select an element on it, the element border displays in red, indicating that you cannot move it or resize it
- If an element is locked and you click on it on a diagram, the element border displays in black; you can display the properties but not change them

- If you select the 'Full Lock, no-one may edit' option, a red exclamation mark displays against the object in the **Browser window**
- If you select the 'User Lock, locking user may still edit' or 'Group lock, locking group may still edit' options, a blue exclamation mark displays against the object in the Browser window; other users see a red exclamation mark

Lock Packages Under User/Group Locking

If, in User/Group locking mode, you want to lock or unlock the contents of a Package, you can do so in a single operation. You can set the lock on the entire contents (including child Packages), just on the top-level Package content, or just on the elements or diagrams in the Package.

Access

Ribbon	Design > Model > Manage > Lock (on selected Package)
Context Menu	Browser window Right-click on Package Package Control Lock Package
Keyboard Shortcuts	On selected Package, Ctrl+Shift+L

Lock or Unlock a Package

Step	Action
1	<p>In the 'Lock Type' panel, select the appropriate radio button for the lock to apply:</p> <ul style="list-style-type: none">• No lock - do not set a lock on this Package; clear any existing lock that you have set, or clear any Full lock that other users have set• Full lock - lock this Package so that no-one can edit it without specifically clearing the lock• User lock - lock this Package so that only you can make further edits; other users cannot unlock or edit the Package• Group lock - lock this Package so that any member of the specified group can edit the object; other users cannot unlock or edit the Package
2	<p>If you have selected the 'Group lock' option, in the 'GroupID' field click on the drop-down arrow and select the group containing users that can edit the object.</p> <p>The 'GroupID' drop-down list only includes groups that you are a member of.</p> <p>Additionally, if you are setting the Group Lock on a Root node, you can select the 'Hide for other Groups' checkbox to hide the Package and its contents from users who are not part of the security group or the 'Administrators' group. This hides the Package from</p>

	general view in the Browser window , but does not prevent the Package content from being exposed in model searches.
3	<p>The 'What to Process' checkboxes default to selected to also lock:</p> <ul style="list-style-type: none">• Elements and/or diagrams in the Package• The contents of child Packages (that is, the whole branch) <p>If you want to exclude any type of Package content from the change in lock status, deselect each appropriate checkbox.</p>
4	Click on the OK button to apply the lock.

Notes

- To check whether the project security is in User/Group locking mode, select 'Configure > Security > Administer'; the 'Require User Lock to Edit' option should be deselected
- You must have 'Lock Elements' permission to lock a Package
- If the Package is already locked, only the corresponding lock option and the 'No lock' option are highlighted; you have to release the lock in order to set a different type of

lock

- If you select the 'Full Lock, no-one may edit' option, a red exclamation mark displays against the Package in the **Browser window**
- If you select the 'User Lock, locking user may still edit' or 'Group lock, locking group may still edit' options, a blue exclamation mark displays against the Package in the Browser window; other users see a red exclamation mark

Lock Objects Under Require User Lock to Edit

In the 'Require User Lock to Edit' security mode, if you want to edit one or more of the diagrams or elements in a Package, you must set a User Lock on either the specific objects or the Package that contains them. You can set or release the lock from either a diagram or the **Browser window**. Once you have set a lock, only you or the Security Administrator can release it again; no other user can release your **locks**.

Access

Ribbon	Design > Model > Manage > Lock (on selected Package) Design > Diagram > Manage > Lock (on selected open diagram) Design > Element > Manage > Lock (on selected element)
Context Menu	Select one of: <ul style="list-style-type: none">• Browser window Right-click on Package Package Control Apply/Release User Lock, or

	<ul style="list-style-type: none">• Browser window Right-click on diagram Apply/Release User Lock, or• Browser window Right-click on element Apply/Release User Lock, or• Browser window Select a Package, diagram or element, then press Ctrl+Shift+L, or• On a diagram Right-click on background Apply/Release User Lock, or• On a diagram Right-click on element Apply/Release User Lock, or• On a diagram Click on an element, then press Ctrl+Shift+L
--	--

Set or clear a user lock in Require User Lock to Edit security mode

Step	Action
1	On the 'Set User Lock' dialog, click on either the: <ul style="list-style-type: none">• 'Apply User Lock' radio button to set the lock or• 'Release User Lock' radio button to clear the lock

2	<p>For a Package, if you want to also lock all child Packages, select the 'Include Child Packages' checkbox.</p> <p>If any elements in the Package tree are locked by other users, a list of elements that couldn't be locked displays.</p>
3	<p>Click on the OK button.</p> <p>The system locks or unlocks:</p> <ul style="list-style-type: none">• The selected element• The selected diagram and the diagram settings for elements on the diagram (not the elements themselves), or• The Package and all elements and diagrams in the top level of the Package

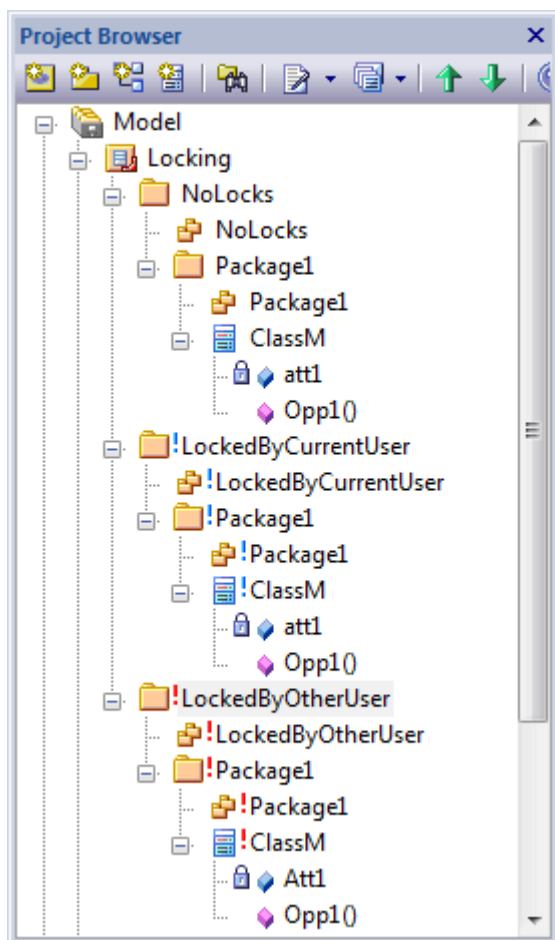
Notes

- To check whether the project security is in Require User Lock to Edit mode, select 'Configure > Security > Administer'; the 'Require User Lock to Edit' option should be selected
- You must have 'Lock Elements' permission to lock either an element on a diagram or a Package
- When you set a user lock, a blue exclamation mark

displays against the object or objects that are locked; other users see these as red exclamation marks

Locked Element Indicators

When a user sets a lock on an item through User Security, the lock status of the item is indicated in the **Browser window** by a marker against the item - a red or blue exclamation mark - as shown:



These indicators also display against the locked element on any diagram in which the element is represented.

The effect of the lock and the meaning of the status marker depend on the security policy applied to your project.

Require User Lock to Edit

Marker	Meaning
No marker	There is no lock, the item is not editable, but any user can now apply a user lock to edit the item.
Blue exclamation mark	You have applied a user lock and can edit the item; no other user can release the lock, set their own lock or edit the item.
Red exclamation mark	Another user has applied a user lock, and you cannot release the lock, set your own lock or edit the item. You can find out which user has locked the item.

User/Group Lock

Marker	Meaning
No marker	There is no lock, the item is editable, but any user can now apply a user or group lock.

Blue exclamation mark	The item has a lock set by you or a group including your user ID as a member, and you can edit the item.
Red exclamation mark	<p>The item has a lock set by another user, or a group of which you are not a member; you cannot edit the item.</p> <p>You can find out which user has locked the item.</p> <p>The red exclamation mark also indicates that you or another user has set a full lock on the item. Any user can clear that lock.</p>

Notes

- 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 location or size of the object on the diagram

Identify Who Has Locked An Object

When you are working in your model, you might find that you are unable to update an element, diagram or Package. If you cannot update any object, this might mean that you do not have the access permissions to update diagrams or elements. However, if the object in the **Browser window** has a red exclamation mark next to it this indicates that either another person has placed a user lock or group lock on the object, or you or another user have put a full lock on the object.

You can quickly establish if the lock is a full lock (which you can remove) or which user has set a user or group lock.

Access

Context Menu	<ul style="list-style-type: none">• Browser window Right-click on Package Package Control Lock Package• Browser window Right-click on a diagram Lock Diagram• Browser window Right-click on element Lock
--------------	--

Identify the lock holder

Step	Action
1	<p>In the Browser window right-click on the diagram, Package or element that has a red lock indicator, and select the appropriate 'Lock' option (for a Package, the option is in the Package Control submenu).</p> <p>If the lock is:</p> <ul style="list-style-type: none">• A Full lock, the 'Lock <object>' dialog displays, and you can delete the lock and set your own• A user lock or group lock, a message displays showing the user ID of the person or group who currently holds the lock on that item; click on the OK button to close the dialog

Notes

- You must have Lock Elements permission to lock or clear the lock on a Package, element or diagram

Manage Your Own Locks

As you are working in your model, you might set user **locks** on elements, diagrams and Packages so that you can work on them and protect that work while it is progress. Having completed your work, you might then want to remove those locks. You can do this on each object individually, using the same procedure as you used to set the lock. You can also display a list of all the locks you have set, and remove selected locks or all locks at once. This is especially useful when working under the 'Require user locks to edit' security policy.

Access

Ribbon	Configure > Security > Administer > Manage My Locks
Keyboard Shortcuts	Ctrl+Shift+L

Manage your own locks

Notes

- You must have 'Lock Elements' access permission to set user **locks** on modeling elements, but you do not require any access permission to list or clear them using this procedure

Step	Action
1	All the locks that you have set in the model are listed on the 'My Locks' dialog. This dialog does not show Full locks or Group locks.
2	If you intend to clear locks , either: <ul style="list-style-type: none">• Select a single lock you intend to clear• Press Ctrl or Shift as you select a number of locks or a range of locks respectively, to clear• Click on Select All to select all of your locks, or• Click on Select None to clear your selection, if you have made an error
3	If you have selected locks to clear, click on the Unlock Selected button . The objects that were locked are now unlocked.

