The Reuse Company

SES ENGINEERING Studio:

Security Management Basics

By The REUSE Company

Keep the concept of requirements quality and leverage other Systems Engineering activities by providing lifecycle management, traceability management, verification, and validation support with the SES ENGINEERING Studio.

SES ENGINEERING STUDIO: SECURITY MANAGEMENT BASICS

The REUSE Company et. al

2025 Edition

SES ENGINEERING STUDIO: SECURITY MANAGEMENT BASICS

Version 1.1

The REUSE Company
Calle Margarita Salas, 16 2-D
Parque Tecnológico LEGATEC
28919 Leganés – Madrid
SPAIN – EU

http://www.reusecompany.com
Phone: (+34) 912 17 25 96
Fax: (+34) 916 80 98 26
Twitter: @ReuseCompany
E-mail: contact@reusecompany.com

Changes History:

Version	Date	Changes
1.0	October 2022	Initial version
1.1	January 2025	New version 23.4

Table of Contents

1 Introduction 9

2 Objectives of the Security Management Capability 11

3 Security Philosophy in SES ENGINEERING Studio 13

3.1 SES Server Configuration 13

3.2 User administrator by default 14

4 Security Levels: at Application / at Connection 15

5 Concepts 17

5.1 Security Modules 17

5.2 Roles and Users 17

5.3 Tool Operations Groups and Tool Operations 17

6 Concepts for Managing Security in SES 19

6.1 Metamodel 19

6.2 Security Levels 21

7 Permissions 23

8 Custom Code Security Management 25

9 Security GUI Views 27

10 Start Using Security Management 33

10.1 How to create roles 33

10.2 How to Assign Users to Specific Roles and Roles to Specific Connection Modules 35

10.3 How to Create a Security Template 39

10.4 How to create a connection-level security module 40

10.5 How to Create a Connection and use the Roles and Security Modules inside 42

10.6 Executing the Quality Management capability with permissions 43

10.7 Summary 46

Annex 1: Security Permissions List 49

Annex 2: Minimum Security Configuration permissions 53

1 Introduction

This document applies to the 23.4 version of the product.

The SES ENGINEERING Studio is the main tool developed by The REUSE Company to manage the systems engineering life cycle and requirements.

The SES ENGINEERING Studio allows any systems engineer to manage different types of workproducts. From goals and high-level requirements to system or subsystem requirements, risks, verification actions… On top of that, and thanks to the *connectivity* capabilities of the SES ENGINEERING Studio, external repositories can also be connected. This includes, among others, SysML/UML/Capella models, simulation models, MS Excel worksheets, MS Word documents, requirements managed in many types of repositories (IBM DOORS, Teamcenter, Polarion…).

All in all, the number of different sources that are to be considered in a complex systems engineering project is huge and, at the same time, maintaining traceability among all these elements is key for the success of the projects and, in many cases, required by standards, guidelines, best practices or recommendations.

Therefore, the SES ENGINEERING Studio provides mechanisms to identify all the different documents (models, physical documents, and other types of containers of engineering workproducts) that conforms a project, and to define the different semantics of the traces to be eventually created among the items contained in those elements. All this, in most of the cases, without even opening the source tool where the items were created and managed.

This tool is designed to group all Engineering Suite capabilities using only one interface. The capabilities supported are related to quality management, verification and validation, life cycle, and traceability, among others.

Specifically, the capabilities included are:

- LIFECYCLE Management
- Quality Assurance: RQA – QUALITY Studio
- V&V Assurance: V&V Studio
- Traceability Management
- Knowledge Management: KM – KNOWLEDGE Manager
- Requirements writing assistance: RAT – AUTHORING Tool

All these capabilities are interdependent through the SES ENGINEERING Studio, but the customer may contract some of them separately. Because of this, each capability has its user guide, supplied to the appropriate customer as contracted.

This guide refers specifically to the Security Management capability. You can use the SES ENGINEERING Studio using the MS Windows authentication, but it has also in-built a capability to manage authentication and access control to the different features of the tool. This is accessible at the repositories home menu:

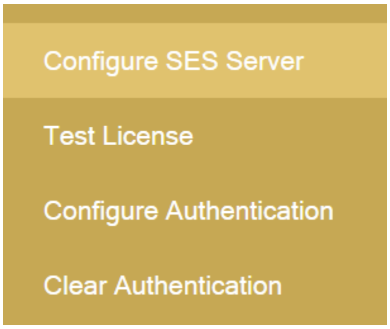
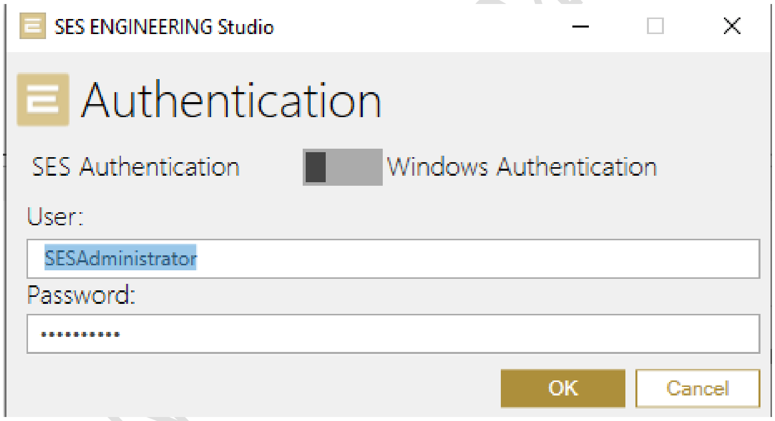


FIGURE 1

Choosing *Configure Authentication* allows the user to select the authentication preferred.



Authentication

SES Authentication Windows Authentication

User:

SESAdministrator

Password:

•••••••••••

FIGURE 2

In any case, you can use the Security Management capability to select the functions and features each user is permitted to execute inside the tool.

In this guide, we are detailing the basics, options and concepts related to this capability. For more information, please, use the *SES ENGINEERING Studio: User Guide*.

2 Objectives of the Security Management Capability

The Objective of the Security Management tool is to provide security control to the whole operational environment of SES ENGINEERING Studio.

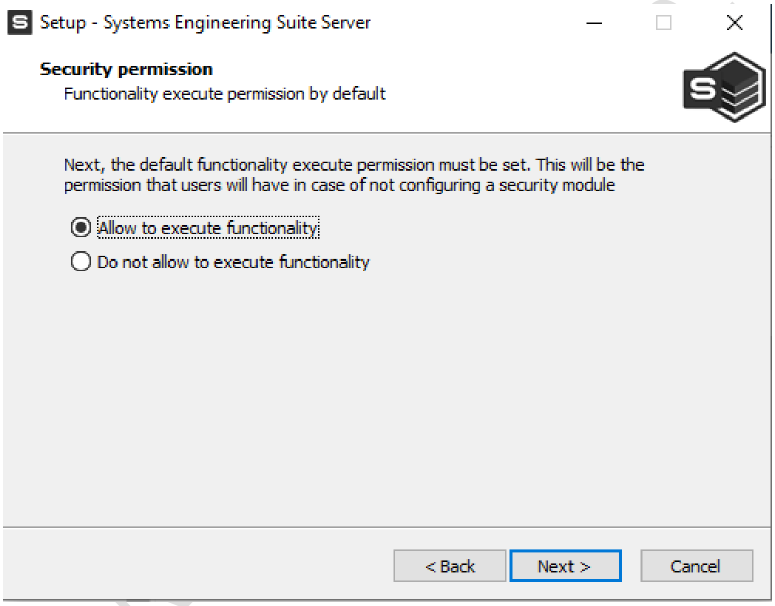
Through the creation of roles, execution permissions can be assigned on specific functionality operation. These roles contain sets of users or Active Directory rules and may be assigned to individual operations or to groups of operations that are related.

3 Security Philosophy in SES ENGINEERING Studio

3.1 SES Server Configuration

It is possible to set from the SES Server tool an execute permission for all functionality operations. This permission consists of allowing or disallowing the execution of operations for all users as long as there are no security modules (to be explained in 5.1 in this guide).

This execute permission is set for the first time during the SES Server installation. Following, the step where this permission is configured during installation is shown.



Setup - Systems Engineering Suite Server

Security permission

Functionality execute permission by default

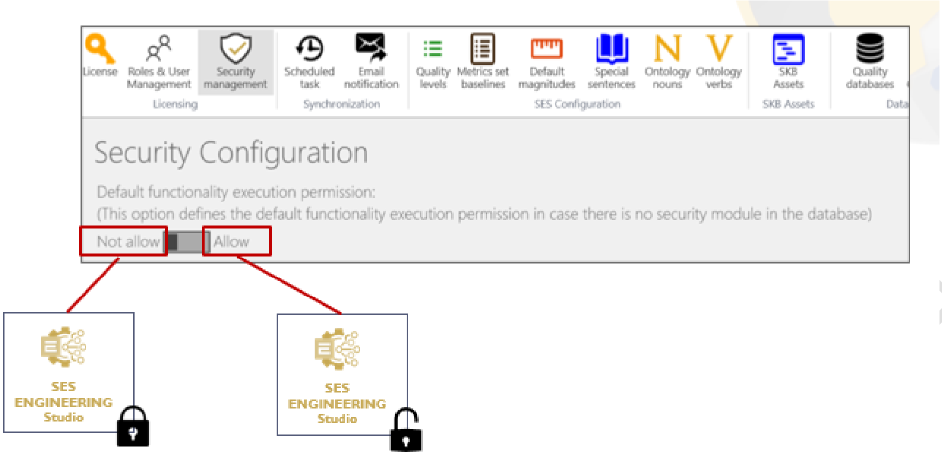
Next, the default functionality execute permission must be set. This will be the permission that users will have in case of not configuring a security module

● Allow to execute functionality

○ Do not allow to execute functionality

FIGURE 3

The assignment can be modified from the Security Management section on the SES Server as it is shown in the next figure:



Security Configuration

Default functionality execution permission:

(This option defines the default functionality execution permission in case there is no security module in the database)

FIGURE 4

3.2 User administrator by default

There is a default user with the ability to execute all functionality operations. This user is: SESAdministrator and will have permission to execute the operations as long as there is no security module created and the default permission configured on the SES Server is "Allow".

If there are security modules created, this user will have to be given specific permissions in the corresponding module operations.

NOTE: It is a good security practice to change the default password for the SESAdministrator profile.

4 Security Levels: at Application / at Connection

Security configuration via modules is set at two possible levels:

- **Security at application level**: Security control of global functionality in ENGINEERING Studio tool
- **Security at connection level**: Security control of functionality set to specific *Connectors* affecting all the modules included in the derived *Connection*.

Please, to know more about *Connectors*, *Connections,* and *Connection modules* please refer to the *SES ENGINEERING Studio: User Guide*.

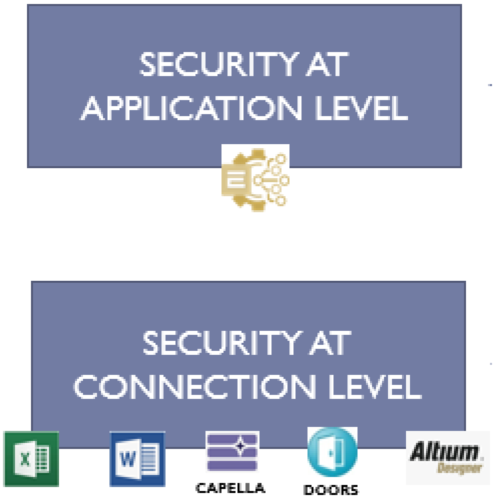


FIGURE 5

5 Concepts

5.1 Security Modules

The *Security Modules* contain the assignment of users to functionality execution permissions, therefore, are used to perform the security control of the execution of operations and also custom codes.

Types of *Security Modules*:

- **At application level**: to manage security for global functionality and custom codes. For example: create, edit or delete connectors, open an interoperability module or assign a role to a specific operation
- **At connection level:** to manage security functionality for specific *connectors*. For instance: run RQA metrics, create a workproduct, or run a project lifecycle.
- **Templates:** to be used to create a *Security Module at connection level* after assigned permissions to *Roles*.

5.2 Roles and Users

Roles are used to store a set of users. These users can be:

- **KM Users:** Users created with TRC tools, and stored in the *Repository* or *Knowledge database*
- **Active Directory rules:** Users, machines, and user groups of Windows security system, including a combination of those elements

5.3 Tool Operations Groups and Tool Operations

An *operation* represents the executable functionality of the tools. For instance, *calculate metrics* with RQA – QUALITY Studio, *modify requirements* in SES ENGINEERING Studio.

Executing operations can be grouped in terms of the *application domain* as a way for simplifying the security administration of one specific tool or application.

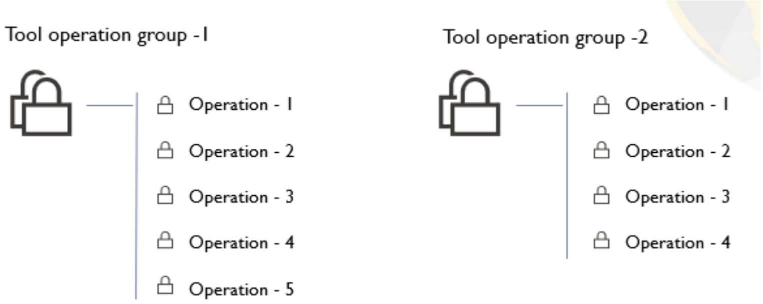

Tool operation group -1
Operation - 1
Operation - 2
Operation - 3
Operation - 4
Operation - 5
Tool operation group -2
Operation - 1
Operation - 2
Operation - 3
Operation - 4

FIGURE 6

6 Concepts for Managing Security in SES

6.1 Metamodel

To manage security, we have a *metamodel* or a conceptual model, representing the relationships between the concepts presented in chapter 1, as shown in the next figure:

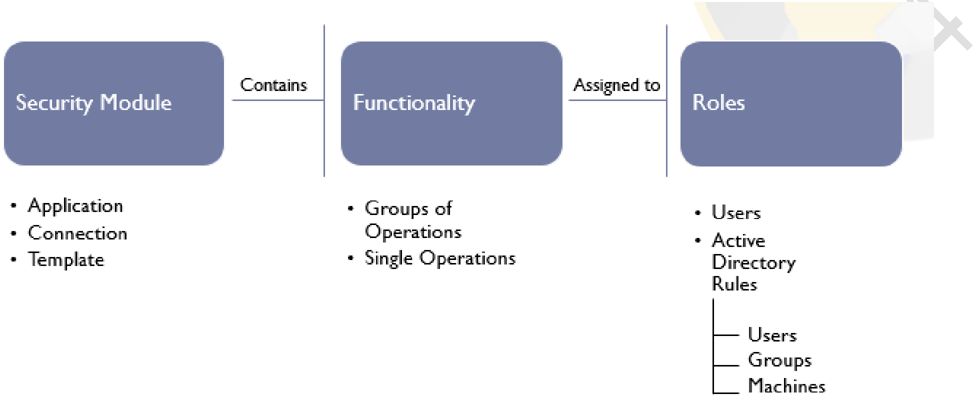


FIGURE 7

Example of a security management workflow:

- First, we create sets of Users and Active Directory rules through Roles, as shown in the next figure:

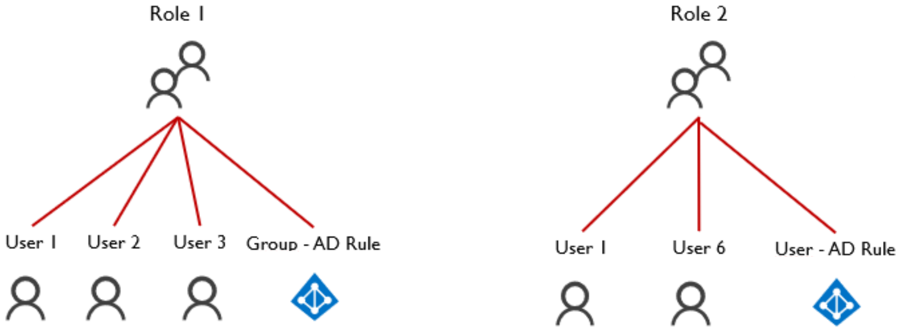


FIGURE 8

- Second, we create an *Application Security Module* that contains different *tool operation groups*, as shown in the next figure:

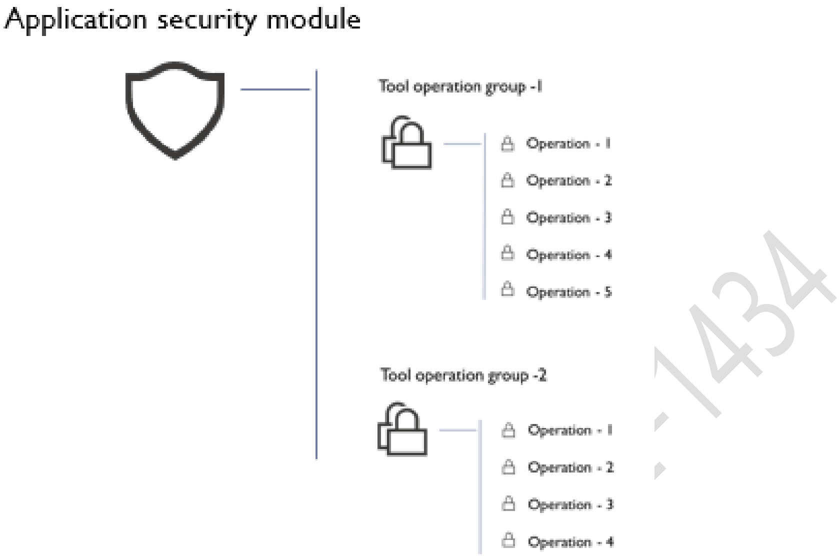


FIGURE 9

- After that, we must assign *roles* to operations or *operations groups*, as shown in the next figure:

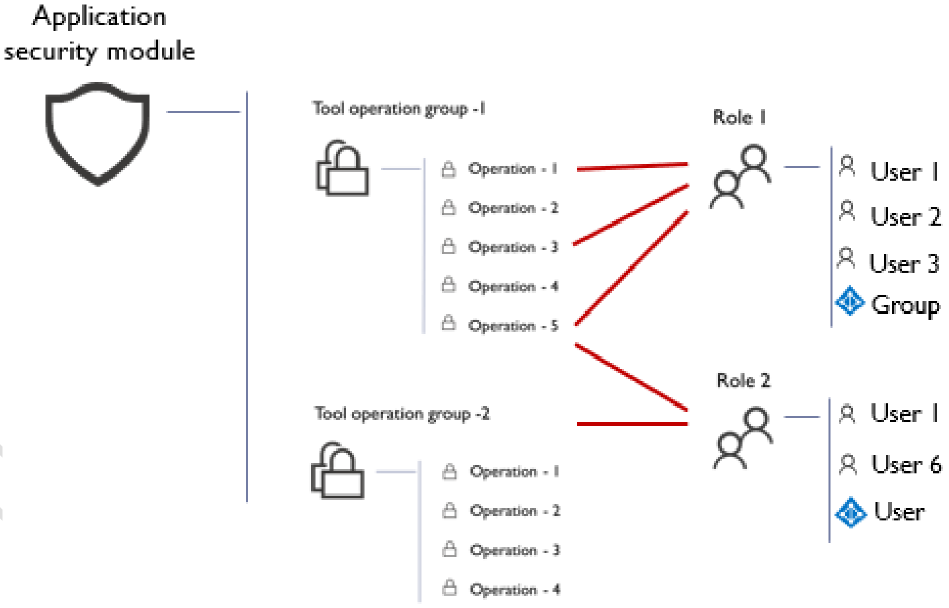
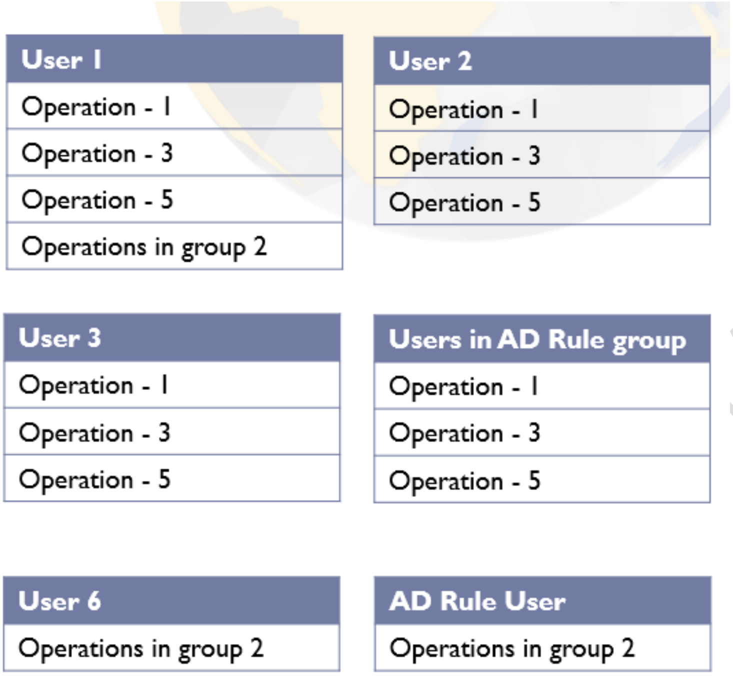


FIGURE 10

The result is that the users can execute the following operations:



User 1
Operation - 1
Operation - 3
Operation - 5
Operations in group 2

User 2
Operation - 1
Operation - 3
Operation - 5

User 3
Operation - 1
Operation - 3
Operation - 5

Users in AD Rule group
Operation - 1
Operation - 3
Operation - 5

User 6
Operations in group 2

AD Rule User
Operations in group 2

FIGURE 11

Notice that, for example, the user 1 can execute operations 1, 3, and 5 and all the operations in group 2 (operations group 2) since this user belongs to both roles.

6.2 Security Levels

As mentioned above, there are security modules at the application level and at the connection level. This section will explain the different levels of permission control based on these settings.

The first check when a functionality is executed is if there are security modules. If they don't exist, it checks the execute permission set on the server. If it is set to "Allow" the operation can be executed, if it is set to "Not Allow" the operation cannot be executed.

In the case of existing security modules, first it is verified that there are modules at the connection-level.

If there is a module at the connection level, it is checked if the user is in a role assigned to the operation, if it is, it will be able to execute the functionality, if it is not, the same check will be carried out in the module at the application level.

If the user is not within any role assigned to the specific operation or to the group of operations that contains it, the functionality cannot be executed.

7 Permissions

There are several different *operations groups* for an *Application Security Module* and a *Connection Security Module*:

- The *Security management operations* contains the functionality for the Security Management itself, for example: create users, create roles, assign roles, assign operations to roles…
- The *Application execution operations* that control de execution of tools or capabilities in the SES ENGINEERING Studio.
- Lifecycle management, including all Lifecycle Management capability operations. See the Lifecycle *Management Capabilities for the SES ENGINEERING Studio: User Guide* for more information.
- Traceability management, including all TRACEABILITY Management capability operations. See the *TRACEABILITY Management Capabilities for the SES ENGINEERING Studio: User Guide* for more information.

Following, the groups of operations that contain the application-level module and the connection level module are presented:

TABLE 1

Application security module
Security Management Operations
Application Execution Operations
RQA Operations
Lifecycle Management Operations
Risks & Alerts Operations
V&V Operations
Traceability Management Operations
Content Manager Operations
SES ENIGINEERING Studio Operations
Universal Report System Operations

TABLE 2

Connection security module
RQA Operations
Risks & Alerts Operations
V&V Operations
Content Manager Operations

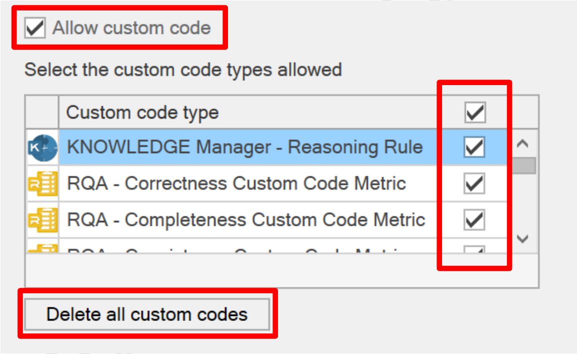
SES ENIGINEERING Studio Operations
Universal Report System Operations

8 Custom Code Security Management

A *Custom Code* is the *extensibility mechanism* that allows to program and executes C# code against SES ENGINEERING Studio for specific purposes: Quality metrics, V&V, suggest traceability, filter information...

Codes must be controlled for security reasons. To configure *code security management*, we have three options:

- Allow or not the execution of *custom code* checkbox, affecting all the SES ENGINEERING Studio environment.
- If *Allow custom code* is enabled, it is possible to select the *custom codes* types allowed in SES ENGINEERING Studio, one by one or the whole, to control the execution and creation of *Custom code*.
- *Delete all custom codes* in the database button will delete all the existing *Custom Codes* inside the *Repository* or *Knowledge database*.



☑ Allow custom code

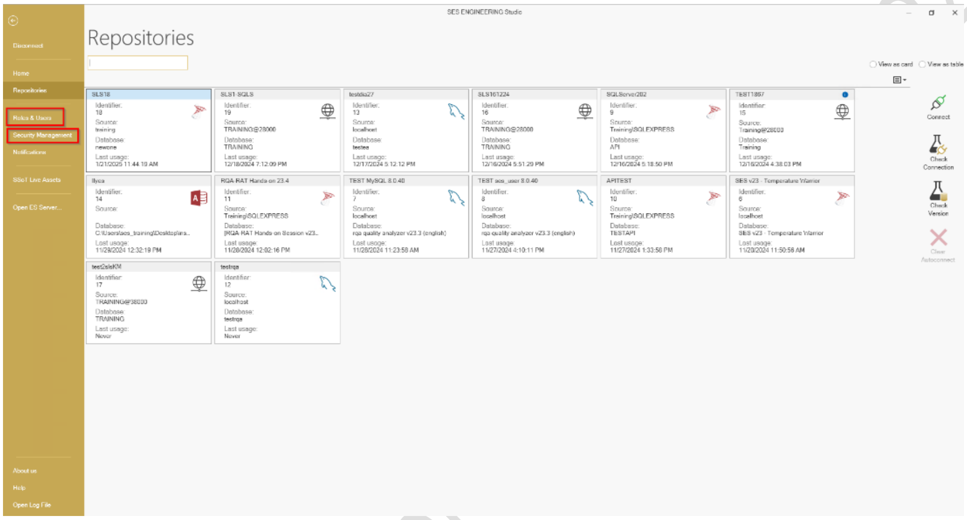
Select the custom code types allowed

Custom code type	☑
KNOWLEDGE Manager - Reasoning Rule	☑
RQA - Correctness Custom Code Metric	☑
RQA - Completeness Custom Code Metric	☑

FIGURE 12

9 Security GUI Views

To access *Roles & Users Management* and *Security Management* tools, note that SES ENGINEERING Studio has two ways for it, as represented in the next figure also showing the *Repositories* of *Knowledge databases*, but also in the SES menu of the SES ENGINEERING Studio tool.



SLS18
Identifier: 18
Source: training
Database: newone
Last usage: 1/21/2025 11:44:19 AM

SLS1-SQLS
Identifier: 19
Source: TRAINING@28000
Database: TRAINING
Last usage: 12/18/2024 7:12:09 PM

testdia27
Identifier: 13
Source: localhost
Database: testea
Last usage: 12/17/2024 5:12:12 PM

SLS161224
Identifier: 16
Source: TRAINING@28000
Database: TRAINING
Last usage: 12/16/2024 5:51:29 PM

SQLServer202
Identifier: 9
Source: Training\SQLEXPRESS
Database: API
Last usage: 12/16/2024 5:18:50 PM

TEST1867
Identifier: 15
Source: Training@28000
Database: Training
Last usage: 12/16/2024 4:38:03 PM

Ilyes
Identifier: 14
Source:
Database: C:\Users\ses_training\Desktop\ins...
Last usage: 11/29/2024 12:32:19 PM

RQA-RAT Hands-on 23.4
Identifier: 11
Source: Training\SQLEXPRESS
Database: [RQA-RAT Hands-on Session v23...
Last usage: 11/28/2024 12:02:16 PM

TEST MySQL 8.0.40
Identifier: 7
Source: localhost
Database: rqa quality analyzer v23.3 (english)
Last usage: 11/28/2024 11:23:58 AM

TEST ses_user 8.0.40
Identifier: 8
Source: localhost
Database: rqa quality analyzer v23.3 (english)
Last usage: 11/27/2024 4:10:11 PM

APITEST
Identifier: 10
Source: Training\SQLEXPRESS
Database: TESTAPI
Last usage: 11/27/2024 1:33:58 PM

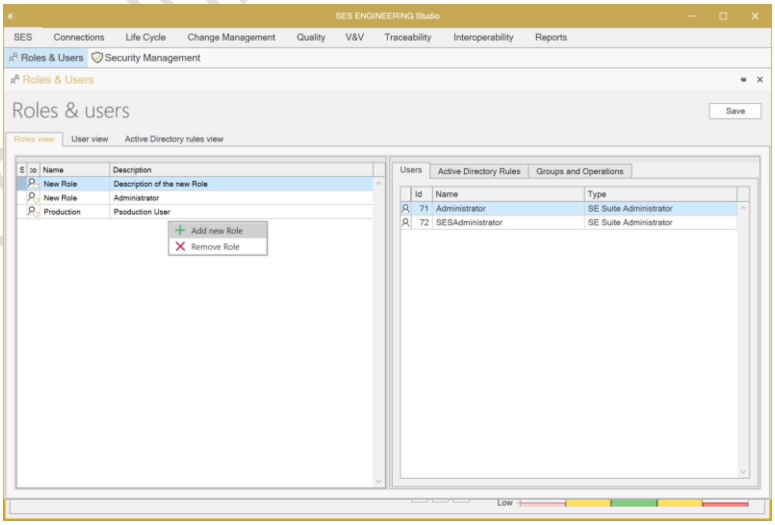
SES v23 - Temperature Warrior
Identifier: 6
Source: localhost
Database: SES v23 - Temperature Warrior
Last usage: 11/20/2024 11:50:56 AM

test2slsKM
Identifier: 17
Source: TRAINING@38000
Database: TRAINING
Last usage: Never

testrqa
Identifier: 12
Source: localhost
Database: testrqa
Last usage: Never

FIGURE 13

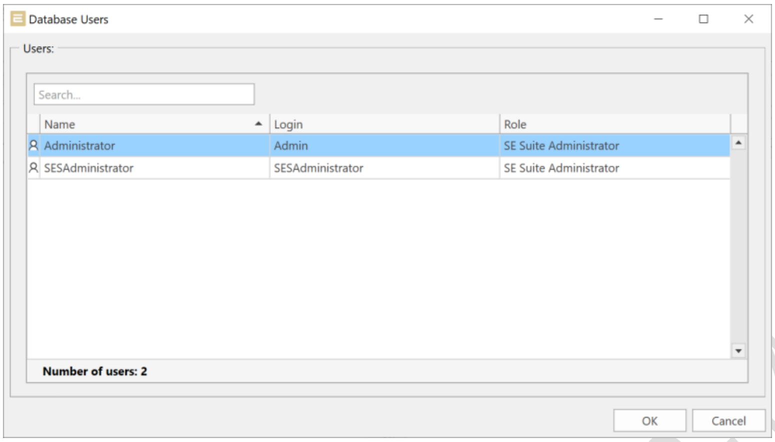
Roles & Users Management panels allow to create/add or remove Roles from the left panel (Figure 14) and add Users in the existing Roles from the right panel (Figure 15).



S	co	Name	Description
		New Role	Description of the new Role
		New Role	Administrator
		Production	Psoduction User

	Id	Name	Type
	71	Administrator	SE Suite Administrator
	72	SESAdministrator	SE Suite Administrator

FIGURE 14



Name	Login	Role
Administrator	Admin	SE Suite Administrator
SESAdministrator	SESAdministrator	SE Suite Administrator

Number of users: 2

FIGURE 15

It is also possible to create /delete Users previously created in the *Repository* or *Knowledge database* for the *SES ENIGINEERING Studio User* role from the previous window, by using the next menus shown in Figure 16.

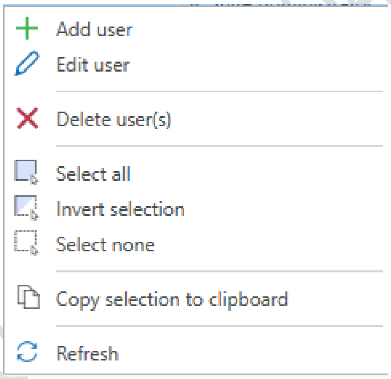
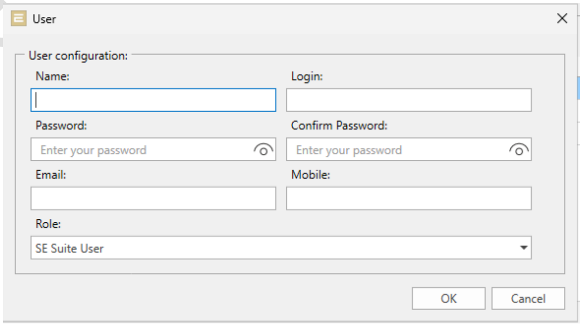


FIGURE 16



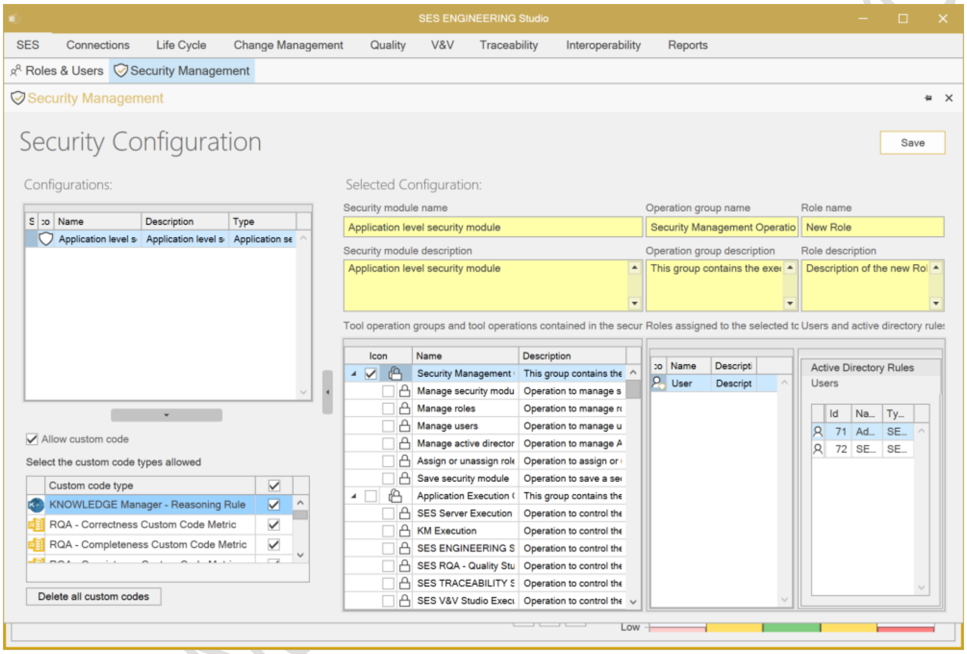
Role: SE Suite User

FIGURE 17

Security Management panels allow to manage security, allowing to create the different kinds of *Security Modules*.

Notice that the *Security Configuration* has two stages, *Configurations* actions, and *Selected Configurations* actions, and different panels too inside of each stage:

- *Configurations*
    - Security Modules (at application, functionality, and roles levels)
    - Custom code security management (to manage custom code use)
- *Selected Configurations*
    - Functionality (Operations and Groups of operations)
    - Roles (to be assigned to Operations)
    - Users (included in Roles)



Security Configuration

Configurations:

S	:o	Name	Description	Type
		Application level s	Application level s	Application se

☑ Allow custom code

Select the custom code types allowed

	Custom code type	☑
	KNOWLEDGE Manager - Reasoning Rule	☑
	RQA - Correctness Custom Code Metric	☑
	RQA - Completeness Custom Code Metric	☑

Selected Configuration:

Security module name: Application level security module

Security module description: Application level security module

Operation group name: Security Management Operatio

Operation group description: This group contains the exe

Role name: New Role

Role description: Description of the new Rol

Tool operation groups and tool operations contained in the secur

Icon		Name	Description
◢ ☑		Security Management	This group contains the
☐		Manage security modu	Operation to manage s
☐		Manage roles	Operation to manage r
☐		Manage users	Operation to manage u
☐		Manage active director	Operation to manage A
☐		Assign or unassign role	Operation to assign or
☐		Save security module	Operation to save a se
◢ ☐		Application Execution (	This group contains the
☐		SES Server Execution	Operation to control the
☐		KM Execution	Operation to control the
☐		SES ENGINEERING S	Operation to control the
☐		SES RQA - Quality Stu	Operation to control the
☐		SES TRACEABILITY S	Operation to control the
☐		SES V&V Studio Execu	Operation to control the

Roles assigned to the selected tc

:o	Name	Descripti
	User	Descript

Users and active directory rules

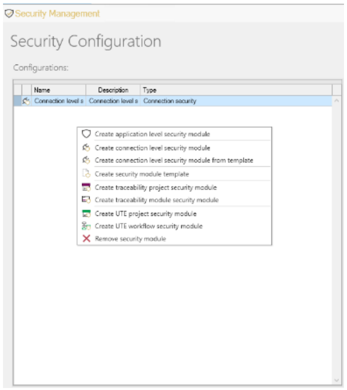
Active Directory Rules

Users

	Id	Na...	Ty...
	71	Ad...	SE...
	72	SE...	SE...

FIGURE 18

To create a new *Security Module,* right click on configuration panel we use the menus shown in:



Security Management

Security Configuration

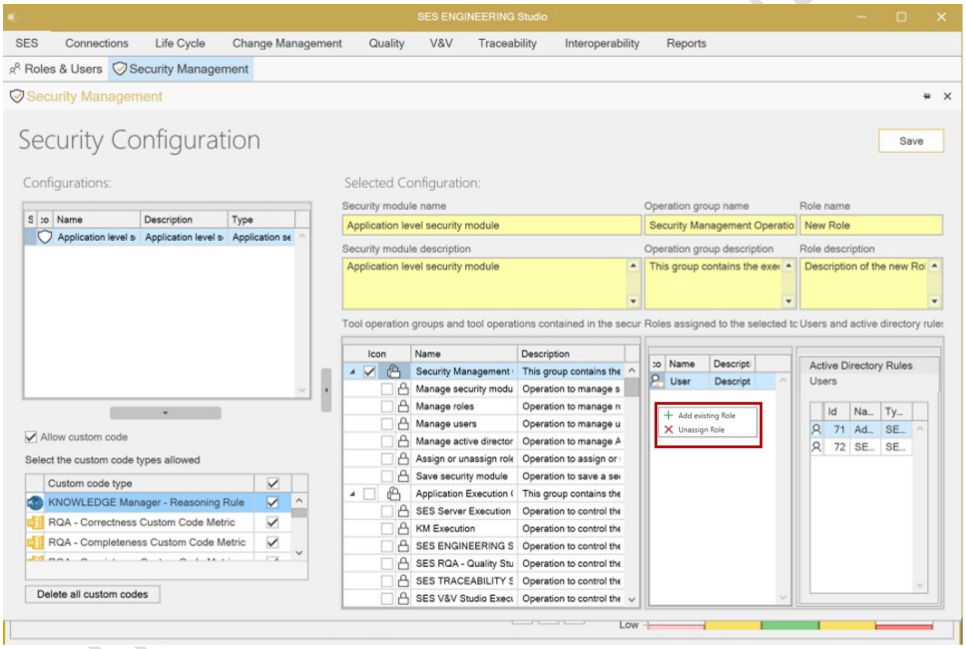
Configurations:

Name	Description	Type
Connection level s	Connection level s	Connection security

- Create application level security module
- Create connection level security module
- Create connection level security module from template
- Create security module template
- Create traceability project security module
- Create traceability module security module
- Create UTE project security module
- Create UTE workflow security module
- Remove security module

FIGURE 19

To assign Roles to Operations groups and/or operations we use the menu shown in Figure 20.



Security Management

Security Configuration

Configurations:

S	:o	Name	Description	Type
		Application level s	Application level s	Application se

☑ Allow custom code

Select the custom code types allowed

Custom code type	☑
KNOWLEDGE Manager - Reasoning Rule	☑
RQA - Correctness Custom Code Metric	☑
RQA - Completeness Custom Code Metric	☑

Delete all custom codes

Selected Configuration:

Security module name: Application level security module

Operation group name: Security Management Operatio

Role name: New Role

Security module description: Application level security module

Operation group description: This group contains the exe

Role description: Description of the new Rol

Tool operation groups and tool operations contained in the secur

	Icon	Name	Description
☑		Security Management	This group contains the
□		Manage security modu	Operation to manage s
□		Manage roles	Operation to manage r
□		Manage users	Operation to manage u
□		Manage active director	Operation to manage A
□		Assign or unassign role	Operation to assign or
□		Save security module	Operation to save a se
□		Application Execution (	This group contains the
□		SES Server Execution	Operation to control the
□		KM Execution	Operation to control the
□		SES ENGINEERING S	Operation to control the
□		SES RQA - Quality Stu	Operation to control the
□		SES TRACEABILITY S	Operation to control the
□		SES V&V Studio Execu	Operation to control the

Roles assigned to the selected tc

:o	Name	Descript
	User	Descript

Users and active directory rule:

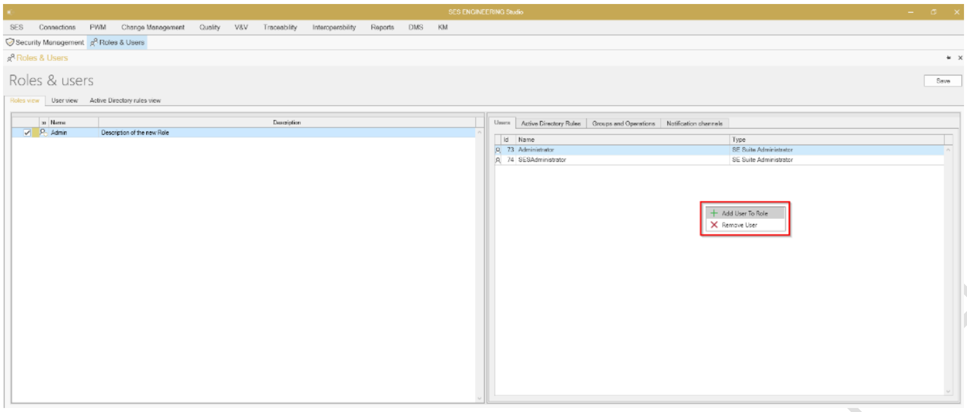
Active Directory Rules

Users

	Id	Na...	Ty...
	71	Ad...	SE...
	72	SE...	SE...

FIGURE 20

To assign *Users* to *Roles* we use the menus shown in Figure 21 (Roles View).

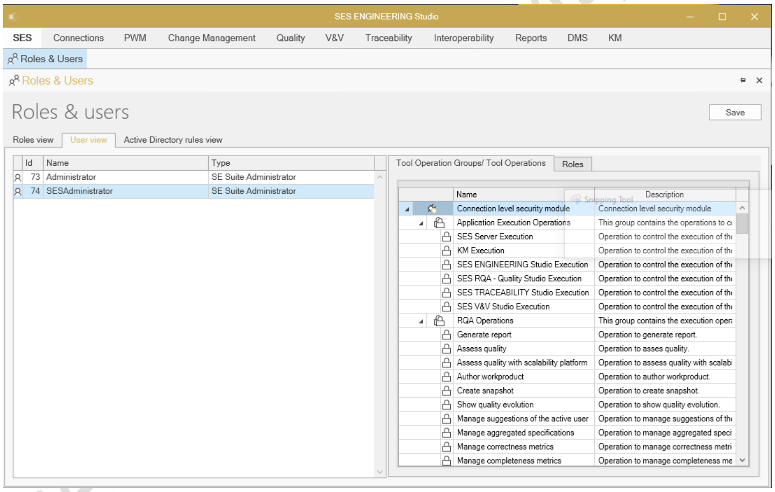


	Name	Description
✓	Admin	Description of the new Role

Id	Name	Type
73	Administrator	SE Suite Administrator
74	SESAdministrator	SE Suite Administrator

FIGURE 21

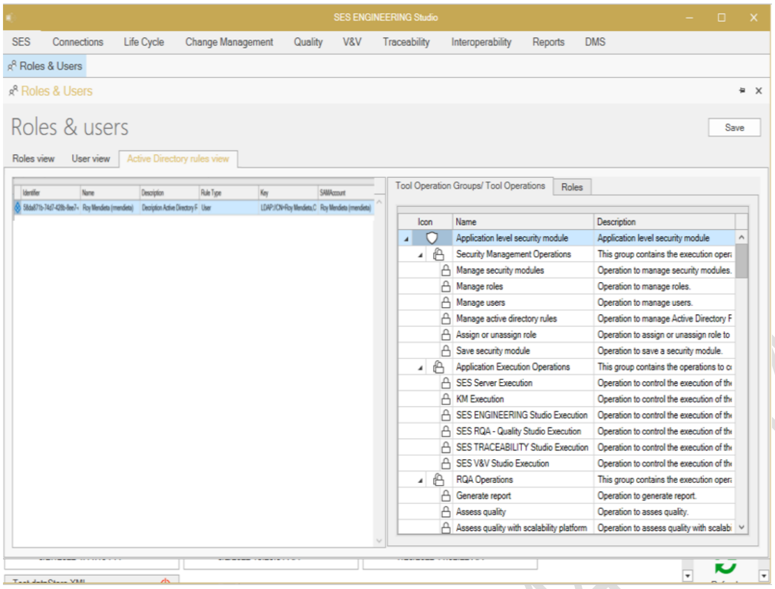
The User view (Figure 22) and Active Directory rules view (Figure 23) tabs provide a summary of specific information per user and Active Directory rules. Note that these views are not editable.



Id	Name	Type
73	Administrator	SE Suite Administrator
74	SESAdministrator	SE Suite Administrator

Name	Description
Connection level security module	Connection level security module
Application Execution Operations	This group contains the operations to c
SES Server Execution	Operation to control the execution of the
KM Execution	Operation to control the execution of the
SES ENGINEERING Studio Execution	Operation to control the execution of the
SES RQA - Quality Studio Execution	Operation to control the execution of the
SES TRACEABILITY Studio Execution	Operation to control the execution of the
SES V&V Studio Execution	Operation to control the execution of the
RQA Operations	This group contains the execution opera
Generate report	Operation to generate report.
Assess quality	Operation to asses quality.
Assess quality with scalability platform	Operation to assess quality with scalabi
Author workproduct	Operation to author workproduct.
Create snapshot	Operation to create snapshot.
Show quality evolution	Operation to show quality evolution.
Manage suggestions of the active user	Operation to manage suggestions of the
Manage aggregated specifications	Operation to manage aggregated speci
Manage correctness metrics	Operation to manage correctness metri
Manage completeness metrics	Operation to manage completeness me

FIGURE 22



Roles & users

Identifier	Name	Description	Rule Type	Key	SAMAccount
58da871b-74d7-428b-8ee7-	Roy Mendieta (mendieta)	Decription Active Directory F	User	LDAP://CN=Roy Mendieta,C	Roy Mendieta (mendieta)

Icon	Name	Description
◢ 🛡	Application level security module	Application level security module
◢ 🔒	Security Management Operations	This group contains the execution oper:
🔒	Manage security modules	Operation to manage security modules.
🔒	Manage roles	Operation to manage roles.
🔒	Manage users	Operation to manage users.
🔒	Manage active directory rules	Operation to manage Active Directory F
🔒	Assign or unassign role	Operation to assign or unassign role to
🔒	Save security module	Operation to save a security module.
◢ 🔒	Application Execution Operations	This group contains the operations to c
🔒	SES Server Execution	Operation to control the execution of th
🔒	KM Execution	Operation to control the execution of th
🔒	SES ENGINEERING Studio Execution	Operation to control the execution of th
🔒	SES RQA - Quality Studio Execution	Operation to control the execution of th
🔒	SES TRACEABILITY Studio Execution	Operation to control the execution of th
🔒	SES V&V Studio Execution	Operation to control the execution of th
◢ 🔒	RQA Operations	This group contains the execution oper:
🔒	Generate report	Operation to generate report.
🔒	Assess quality	Operation to asses quality.
🔒	Assess quality with scalability platform	Operation to assess quality with scalabi

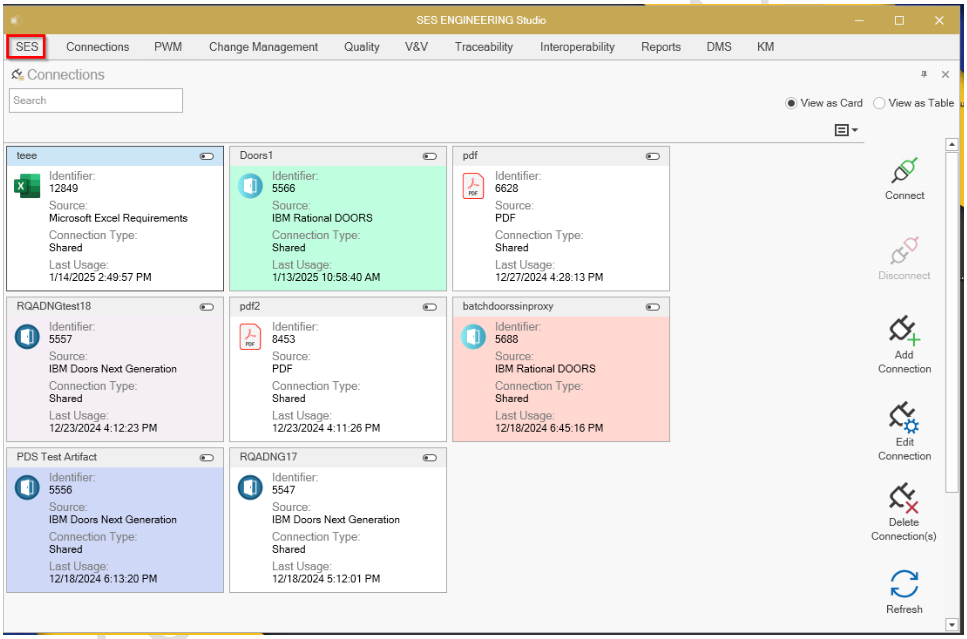
FIGURE 23

10 Start Using Security Management

This chapter explains a typical example of the use of Security Management for SES ENGINEERING Studio with the next simplified scope of work:

10.1 How to create roles

1. Open **SES Engineering Studio** and select a *Repository* or *Knowledge database*
2. Connect to that **Repository or Database**
3. Click on **SES** tab



teee
Identifier: 12849
Source: Microsoft Excel Requirements
Connection Type: Shared
Last Usage: 1/14/2025 2:49:57 PM

Doors1
Identifier: 5566
Source: IBM Rational DOORS
Connection Type: Shared
Last Usage: 1/13/2025 10:58:40 AM

pdf
Identifier: 6628
Source: PDF
Connection Type: Shared
Last Usage: 12/27/2024 4:28:13 PM

RQADNGtest18
Identifier: 5557
Source: IBM Doors Next Generation
Connection Type: Shared
Last Usage: 12/23/2024 4:12:23 PM

pdf2
Identifier: 8453
Source: PDF
Connection Type: Shared
Last Usage: 12/23/2024 4:11:26 PM

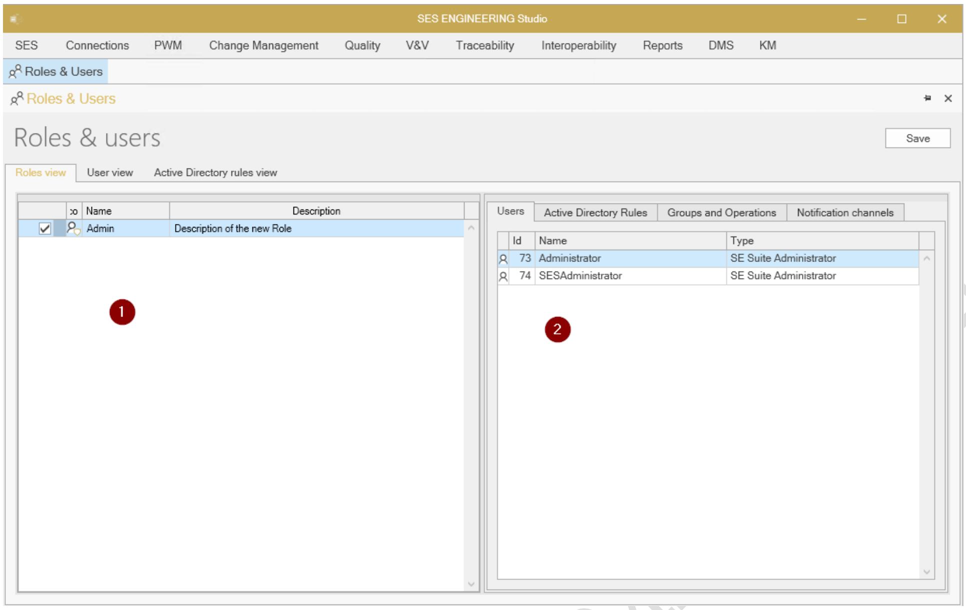
batchdoorssinproxy
Identifier: 5688
Source: IBM Rational DOORS
Connection Type: Shared
Last Usage: 12/18/2024 6:45:16 PM

PDS Test Artifact
Identifier: 5556
Source: IBM Doors Next Generation
Connection Type: Shared
Last Usage: 12/18/2024 6:13:20 PM

RQADNG17
Identifier: 5547
Source: IBM Doors Next Generation
Connection Type: Shared
Last Usage: 12/18/2024 5:12:01 PM

FIGURE 24

4. Go to Roles and Users.



Name	Description
☑ Admin	Description of the new Role

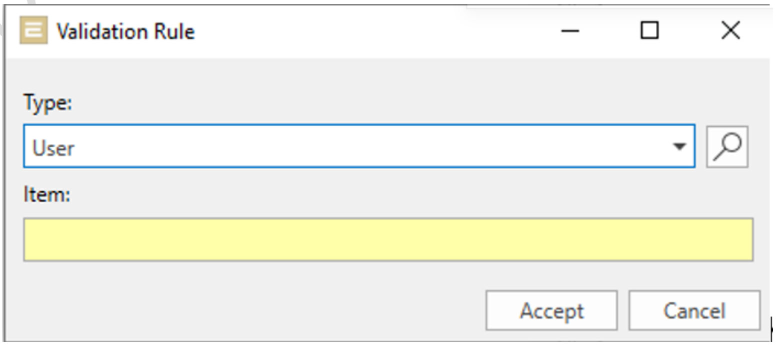
Id	Name	Type
73	Administrator	SE Suite Administrator
74	SESAdministrator	SE Suite Administrator

FIGURE 25

- **Window 1**: Where **roles** are created.
- **Window 2**: Where **user**, **AD Users or AD Groups** are selected to be inside the role selected in **Window 1**.

5. Inside Window 2 there are 2 principal Tabs

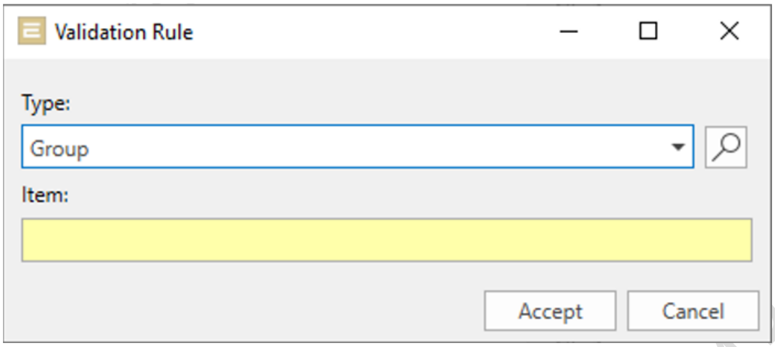
- **Users**: Users created inside SES Server.
- **Active Directory Rules**: Here it can be selected **User**, **Machines** or **Groups** of the **Active Directory**. **Right click** on the **Window 2**, **add Active Directory Rule**, then select the **type (User, Group or Machine**), then **click on the magnifying glass**, this window will appear (image 29), then write down the criteria desired to look for the item**, select it** and **click on OK button**.



Type: User

Item:

FIGURE 26

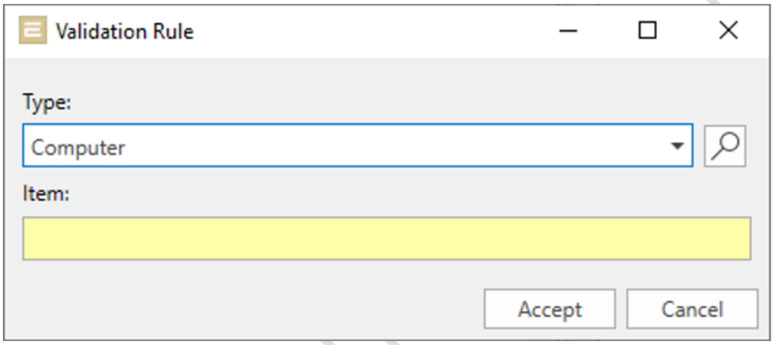


Validation Rule

Type: Group

Item:

FIGURE 27

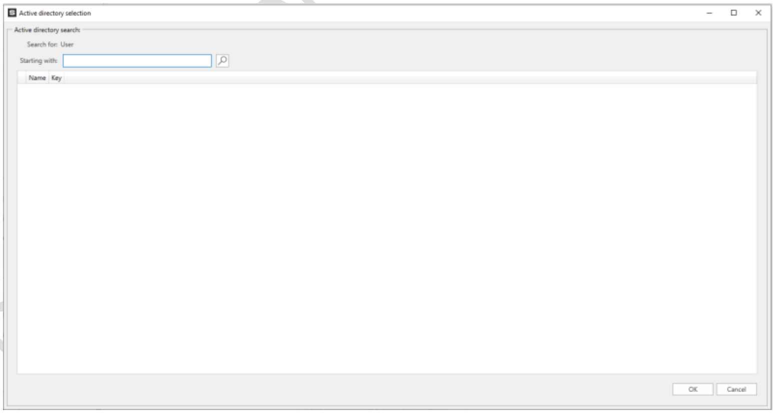


Validation Rule

Type: Computer

Item:

FIGURE 28



Active directory selection

Active directory search:

Search for: User

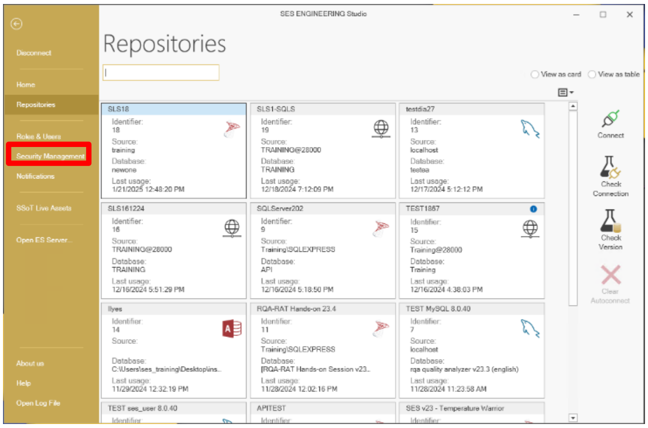
Starting with:

Name	Key

FIGURE 29

10.2 How to Assign Users to Specific Roles and Roles to Specific Connection Modules

1. Using the ***SES*** tab on top, access to the *Repositories* window and select ***Security Management*** on the Main menu (on the left).



SLS18 — Identifier: 18, Source: training, Database: newone, Last usage: 1/21/2025 12:48:20 PM

SLS1-SQLS — Identifier: 19, Source: TRAINING@28000, Database: TRAINING, Last usage: 12/18/2024 7:12:09 PM

testdia27 — Identifier: 13, Source: localhost, Database: testea, Last usage: 12/17/2024 5:12:12 PM

SLS161224 — Identifier: 16, Source: TRAINING@28000, Database: TRAINING, Last usage: 12/16/2024 5:51:29 PM

SQLServer202 — Identifier: 9, Source: Training\SQLEXPRESS, Database: API, Last usage: 12/16/2024 5:18:50 PM

TEST1867 — Identifier: 15, Source: Training@28000, Database: Training, Last usage: 12/16/2024 4:38:03 PM

Ilyes — Identifier: 14, Source:, Database: C:\Users\ses_training\Desktop\ins..., Last usage: 11/29/2024 12:32:19 PM

RQA-RAT Hands-on 23.4 — Identifier: 11, Source: Training\SQLEXPRESS, Database: [RQA-RAT Hands-on Session v23..., Last usage: 11/28/2024 12:02:16 PM

TEST MySQL 8.0.40 — Identifier: 7, Source: localhost, Database: rqa quality analyzer v23.3 (english), Last usage: 11/28/2024 11:23:58 AM

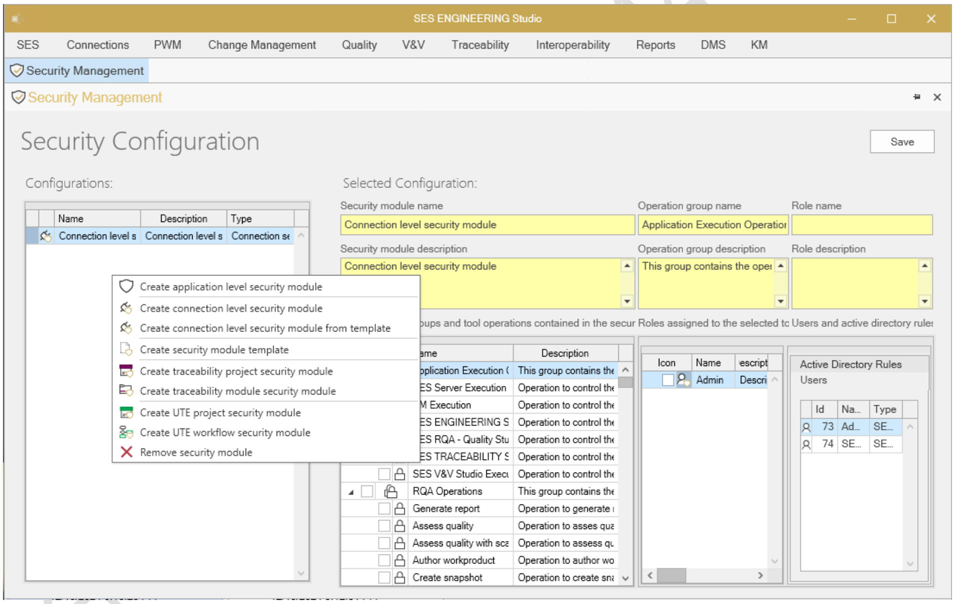
TEST ses_user 8.0.40 — Identifier

APITEST — Identifier

SES v23 - Temperature Warrior — Identifier

FIGURE 30

2. Right-click on the left panel and use the contextual menu to select. ***Create application level security module***.


SES ENGINEERING Studio
SES
Connections
PWM
Change Management
Quality
V&V
Traceability
Interoperability
Reports
DMS
KM
Security Management
Security Management
Security Configuration
Save
Configurations:
Selected Configuration:
Create application level security module
Create connection level security module
Create connection level security module from template
Create security module template
Create traceability project security module
Create traceability module security module
Create UTE project security module
Create UTE workflow security module
Remove security module
Active Directory Rules
Users

Name	Description	Type
Connection level s	Connection level s	Connection se

Security module name: Connection level security module

Operation group name: Application Execution Operatior

Role name:

Security module description: Connection level security module

Operation group description: This group contains the oper

Role description:

ups and tool operations contained in the secur Roles assigned to the selected tc Users and active directory rules

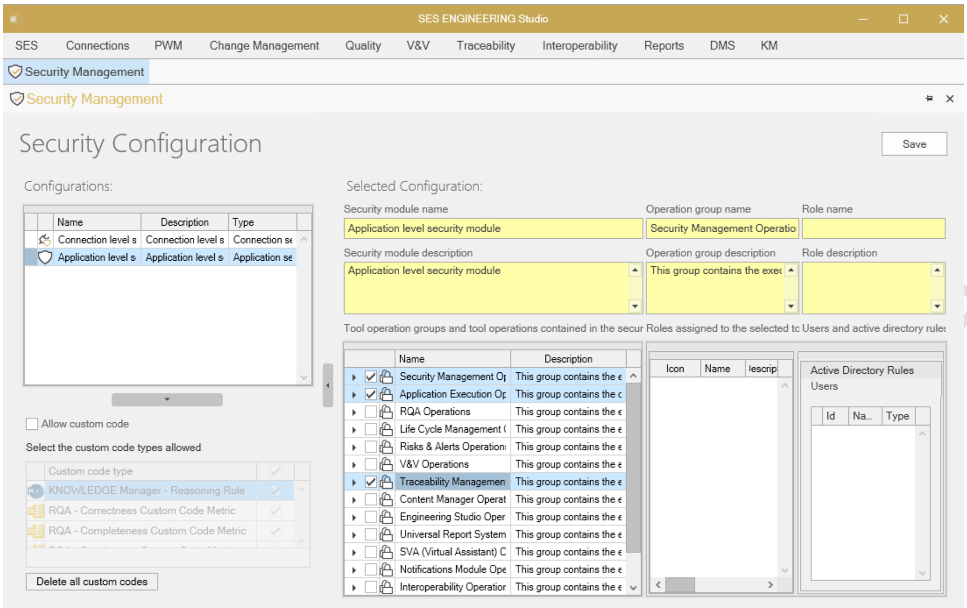
ame	Description
pplication Execution (	This group contains the
ES Server Execution	Operation to control the
M Execution	Operation to control the
ES ENGINEERING S	Operation to control the
ES RQA - Quality Stu	Operation to control the
ES TRACEABILITY S	Operation to control the
SES V&V Studio Execu	Operation to control the
RQA Operations	This group contains the
Generate report	Operation to generate i
Assess quality	Operation to asses qua
Assess quality with sca	Operation to assess qu
Author workproduct	Operation to author wo
Create snapshot	Operation to create sna

Icon	Name	escript
□	Admin	Descri

Id	Na...	Type
73	Ad...	SE...
74	SE...	SE...

FIGURE 31

3. This is going to populate the middle pane. Select a few groups of operation for the security module.



Security Configuration

Configurations:

Name	Description	Type
Connection level s	Connection level s	Connection se
Application level s	Application level s	Application se

□ Allow custom code

Select the custom code types allowed

Custom code type	✓
KNOWLEDGE Manager - Reasoning Rule	✓
RQA - Correctness Custom Code Metric	✓
RQA - Completeness Custom Code Metric	✓

Selected Configuration:

Security module name: Application level security module

Operation group name: Security Management Operatio

Role name:

Security module description: Application level security module

Operation group description: This group contains the exec

Role description:

Tool operation groups and tool operations contained in the secur

	Name	Description
☑	Security Management Op	This group contains the e
☑	Application Execution Op	This group contains the c
□	RQA Operations	This group contains the e
□	Life Cycle Management (	This group contains the e
□	Risks & Alerts Operation:	This group contains the e
□	V&V Operations	This group contains the e
☑	Traceability Managemen	This group contains the e
□	Content Manager Operat	This group contains the e
□	Engineering Studio Oper	This group contains the e
□	Universal Report System	This group contains the e
□	SVA (Virtual Assistant) C	This group contains the e
□	Notifications Module Ope	This group contains the e
□	Interoperability Operatior	This group contains the e

Roles assigned to the selected tc

Icon	Name	lescrip

Users and active directory rules

Active Directory Rules | Users

Id	Na...	Type

FIGURE 32

4. Now we are adding this configuration to the *Admin* role. Right-click on the right pane and select *Add existing Role* in the contextual menu.

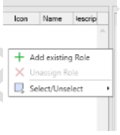
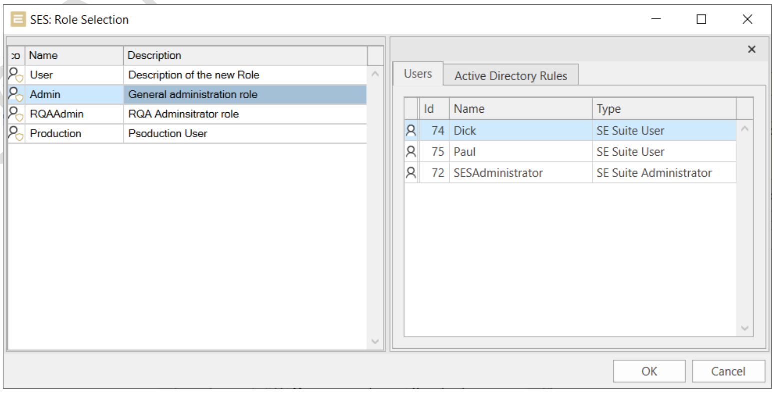


FIGURE 33

5. Select the ***Admin* role** in the window and click ***OK***. You are going to see that another panel is going to appear on the right. **Save** the changes.



:o	Name	Description
	User	Description of the new Role
	Admin	General administration role
	RQAAdmin	RQA Adminsitrator role
	Production	Psoduction User

	Id	Name	Type
	74	Dick	SE Suite User
	75	Paul	SE Suite User
	72	SESAdministrator	SE Suite Administrator

FIGURE 34

6. Now we are assigning the role to a specific connection. Click on the *Connections* tab and then Select the *Connections* button.

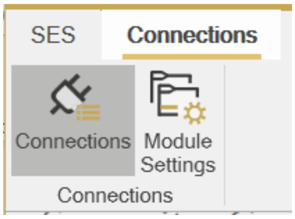
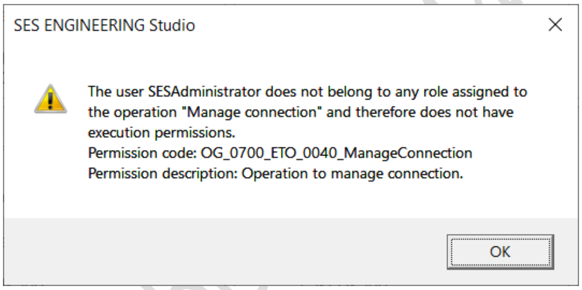


FIGURE 35

7. Select *Add Connection* in the right menu or the contextual menu. A message pop-up showing that SES Administrator does not belong to any role assigned to "Manage connection" and therefore has no execution permissions. Notice that the message also indicates Permission code: OG_0700_ETO_0040_ManageConnection, and Permission description: Operation to manage connection.


SES ENGINEERING Studio

The user SESAdministrator does not belong to any role assigned to the operation "Manage connection" and therefore does not have execution permissions.
Permission code: OG_0700_ETO_0040_ManageConnection
Permission description: Operation to manage connection.

FIGURE 36

8. Let's go back the ***Roles & Users*** tab, using the top menu. Select the *Admin* **role** and **use** ***Add User to Role*** in the contextual menu of the right panel to see the *Database Users* window. Add the *SESAdministrator* user. Click ***Save***.

9. Now, repeat the step 6. The *SESAdministrator* has permissions for establishing connections, so you will get an *Adding new connection* window. Select the *Microsoft Excel Requirements* option.

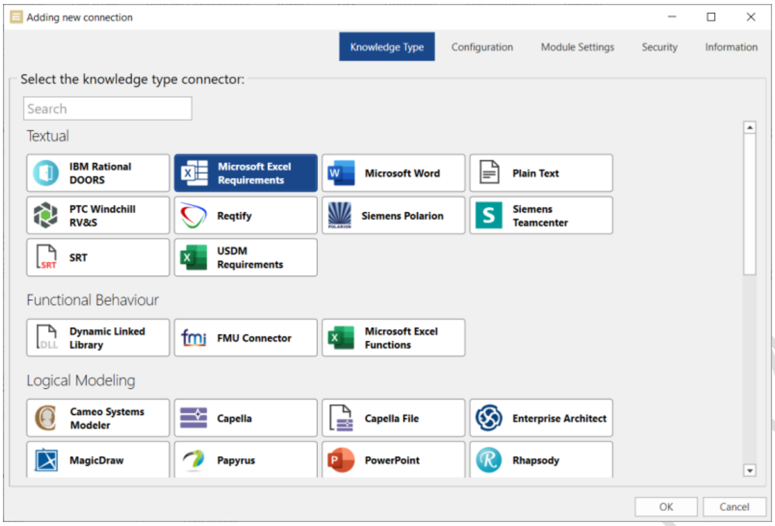
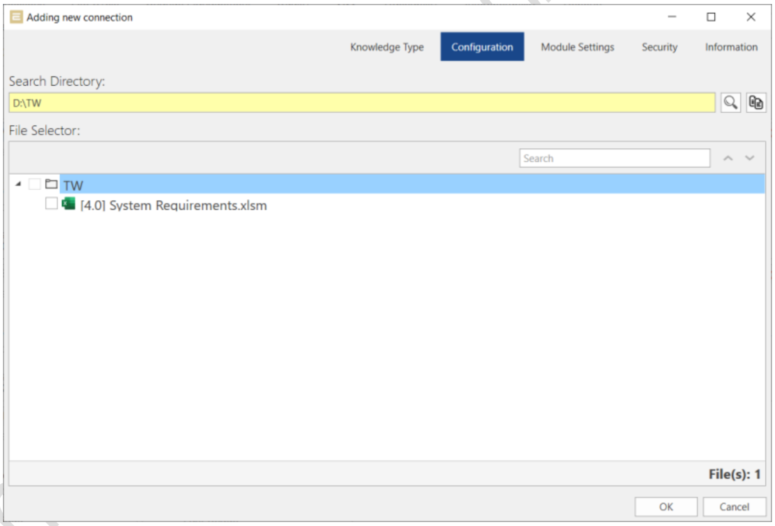


FIGURE 37

10. Click on the *Configuration* option on top and select the proper directory and file.



Search Directory: D:\TW

File Selector:

TW

[4.0] System Requirements.xlsm

File(s): 1

FIGURE 38

11. Click on the *Information* option on top to assign a name. Give it a proper name and save.

10.3 How to Create a Security Template

1. Go back to the **Security Management tab** and, using the top-left panel contextual menu, select ***Create security module template***.

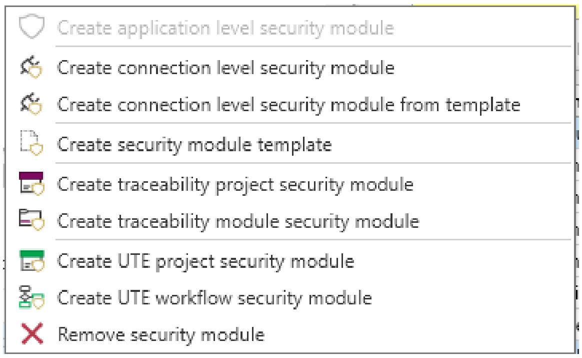
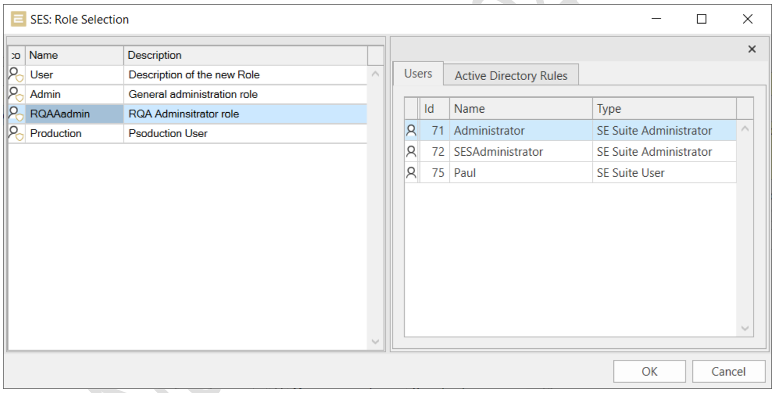

Create application level security module
Create connection level security module
Create connection level security module from template
Create security module template
Create traceability project security module
Create traceability module security module
Create UTE project security module
Create UTE workflow security module
Remove security module

FIGURE 39

2. The new template is added. Notice that there is no *Custom-code* panel during its configuration because a template can be only used to configure *connection-level security modules*. *RQA Operations* should be selected in the middle panel. Now select *Add existing Role* in the contextual menu of the right panel. You will get the *SES Role Selection* window. Select *RQAAdmin* and click *OK*. Save the template.



:o	Name	Description
	User	Description of the new Role
	Admin	General administration role
	RQAAdmin	RQA Adminsitrator role
	Production	Psoduction User

	Id	Name	Type
	71	Administrator	SE Suite Administrator
	72	SESAdministrator	SE Suite Administrator
	75	Paul	SE Suite User

FIGURE 40

10.4 How to create a connection-level security module

1. Now we are *security template* in the *Security Configuration* again in the Security Manager area. Select the *Create connection security module from template* option right-clicking on the left panel.

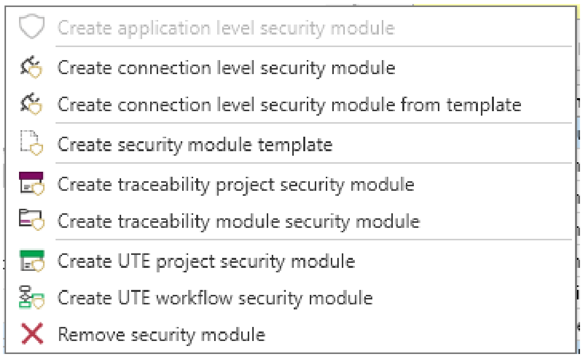
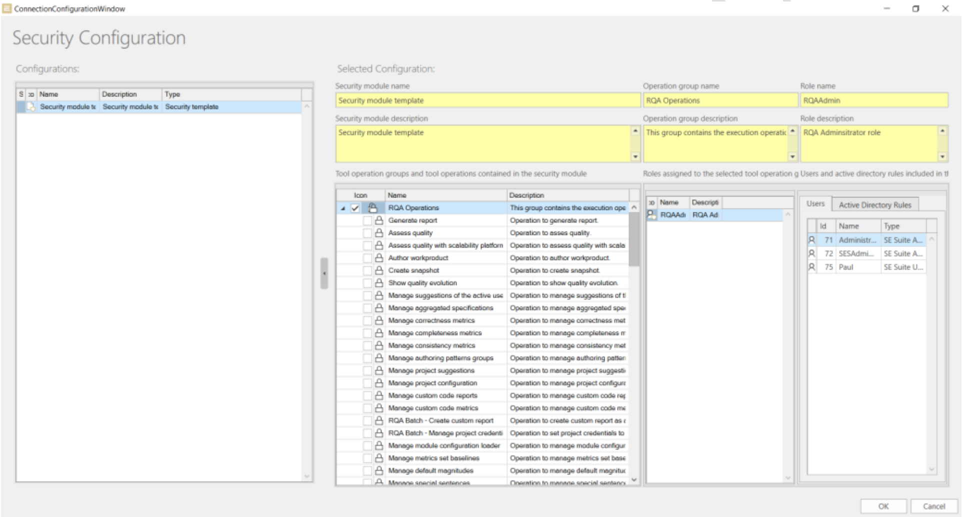

Create application level security module
Create connection level security module
Create connection level security module from template
Create security module template
Create traceability project security module
Create traceability module security module
Create UTE project security module
Create UTE workflow security module
Remove security module

FIGURE 41

2. You will a get a new *Security Configuration* window. Make it bigger to ease the operations.



Security Configuration

Configurations:

S	:o	Name	Description	Type
		Security module te	Security module te	Security template

Selected Configuration:

Security module name: Security module template

Security module description: Security module template

Operation group name: RQA Operations

Operation group description: This group contains the execution operatic

Role name: RQAAdmin

Role description: RQA Adminsitrator role

Tool operation groups and tool operations contained in the security module

Icon	Name	Description
☑	RQA Operations	This group contains the execution ope
□	Generate report	Operation to generate report.
□	Assess quality	Operation to asses quality.
□	Assess quality with scalability platform	Operation to assess quality with scala
□	Author workproduct	Operation to author workproduct.
□	Create snapshot	Operation to create snapshot.
□	Show quality evolution	Operation to show quality evolution.
□	Manage suggestions of the active use	Operation to manage suggestions of tl
□	Manage aggregated specifications	Operation to manage aggregated spe
□	Manage correctness metrics	Operation to manage correctness met
□	Manage completeness metrics	Operation to manage completeness m
□	Manage consistency metrics	Operation to manage consistency met
□	Manage authoring patterns groups	Operation to manage authoring patter
□	Manage project suggestions	Operation to manage project suggesti
□	Manage project configuration	Operation to manage project configur
□	Manage custom code reports	Operation to manage custom code rep
□	Manage custom code metrics	Operation to manage custom code me
□	RQA Batch - Create custom report	Operation to create custom report as a
□	RQA Batch - Manage project credenti	Operation to set project credentials to
□	Manage module configuration loader	Operation to manage module configur
□	Manage metrics set baselines	Operation to manage metrics set base
□	Manage default magnitudes	Operation to manage default magnituc
□	Manage special sentences	Operation to manage special sentenc

Roles assigned to the selected tool operation g

:o	Name	Descripti
	RQAAdı	RQA Ad

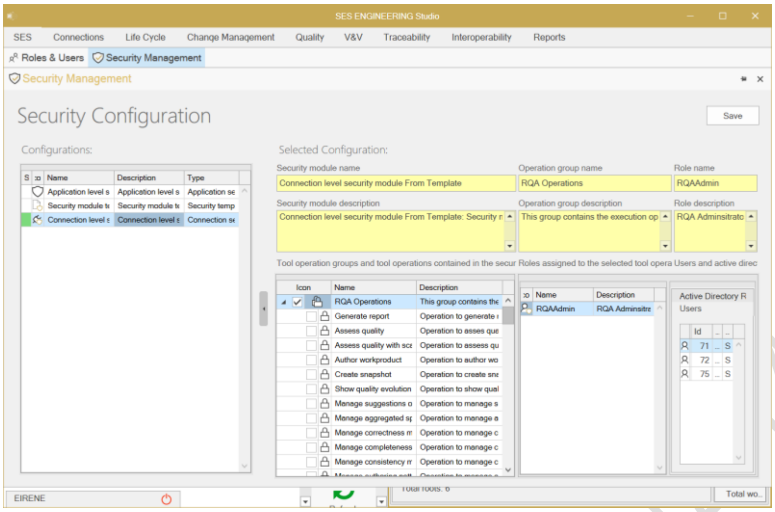
Users and active directory rules included in tl

Users | Active Directory Rules

	Id	Name	Type
	71	Administr...	SE Suite A...
	72	SESAdmi...	SE Suite A...
	75	Paul	SE Suite U...

FIGURE 42

3. Select the Operations or Group of Operations for the Security Module, keeping it selected, using the checkboxes. Click *OK* when done to return to the main *Security Configuration* window.



Security Configuration

Configurations:

S		Name	Description	Type
		Application level s	Application level s	Application se
		Security module te	Security module te	Security temp
🟩		Connection level s	Connection level s	Connection se

Selected Configuration:

Security module name: Connection level security module From Template

Operation group name: RQA Operations

Role name: RQAAdmin

Security module description: Connection level security module From Template: Security n

Operation group description: This group contains the execution op

Role description: RQA Adminsitrato

Tool operation groups and tool operations contained in the secur

Icon		Name	Description
☑		RQA Operations	This group contains the
□		Generate report	Operation to generate r
□		Assess quality	Operation to asses qua
□		Assess quality with sca	Operation to assess qu
□		Author workproduct	Operation to author wo
□		Create snapshot	Operation to create sna
□		Show quality evolution	Operation to show qual
□		Manage suggestions o	Operation to manage s
□		Manage aggregated sp	Operation to manage a
□		Manage correctness m	Operation to manage c
□		Manage completeness	Operation to manage c
□		Manage consistency m	Operation to manage c

Roles assigned to the selected tool opera

	Name	Description
	RQAAdmin	RQA Adminsitra

Users and active direc

Active Directory R
Users

	Id	...	...
	71	...	S
	72	...	S
	75	...	S

Total Tools: 6

FIGURE 43

10.5 How to Create a Connection and use the Roles and Security Modules inside

1. Now we are creating a connection using the security roles already created. Click on the *Connections* tab and then Select the *Connections* button.

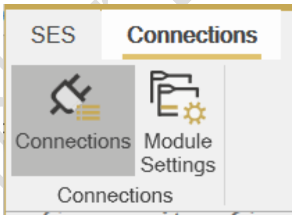
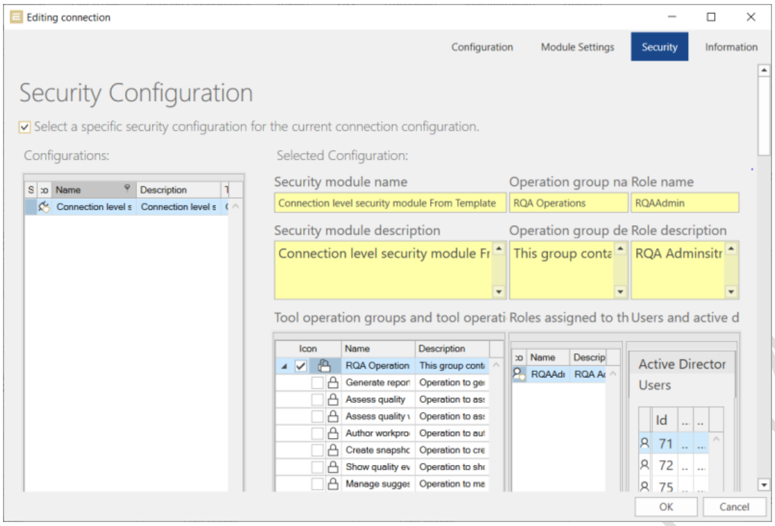


FIGURE 44

2. Edit the connection already created and go to the *Security* tab. Click on the *Select a specific configuration for the current connection configuration box* if it is not to access the different options. Check also that the RQA Operations group is selected.



Editing connection

Security Configuration

☑ Select a specific security configuration for the current connection configuration.

Configurations:

S	ꝏ	Name	Description	T
		Connection level s	Connection level s	(

Selected Configuration:

Security module name: Connection level security module From Template

Operation group na: RQA Operations

Role name: RQAAdmin

Security module description: Connection level security module Fr

Operation group de: This group conta

Role description: RQA Adminsitr

Tool operation groups and tool operati

	Icon	Name	Description
◢ ☑		RQA Operation	This group conti
□		Generate repor	Operation to ge
□		Assess quality	Operation to as:
□		Assess quality \	Operation to as:
□		Author workpro	Operation to aut
□		Create snapshc	Operation to cre
□		Show quality ev	Operation to sh
□		Manage sugge:	Operation to me

Roles assigned to th

ꝏ	Name	Descrip
	RQAAdı	RQA A

Users and active d

Active Director
Users

Id	...	..
71	..	...
72	..	...
75	..	...

FIGURE 45

10.6 Executing the Quality Management capability with permissions

1. Now you are not allowed to execute a quality analysis using the Quality Management capability. We are going to try doing it. Open the connection already created using the *Connections* button (Figure 44) and select the *Quality* view.

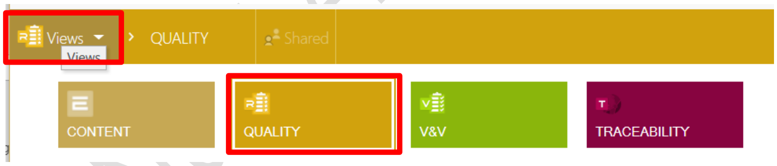


FIGURE 46

2. Using the contextual menu, select the *Complete authentication option* -> *Correctness* option.

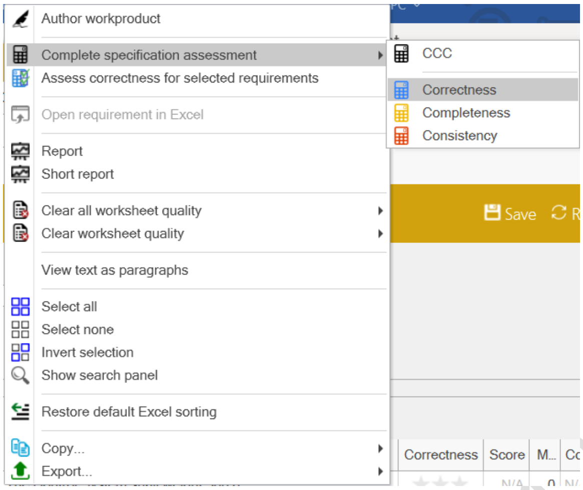
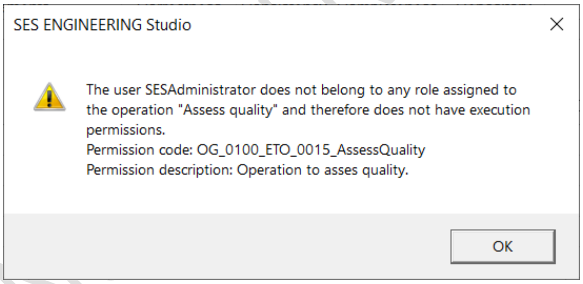


FIGURE 47

3. A message pop-up showing that SES Administrator does not belong to any role assigned to "Assess quality" and therefore has no execution permissions. The message also indicates Permission code: *OG_0100_ETO_0015_AssessQuality*, and Permission description: Operation to assess quality.



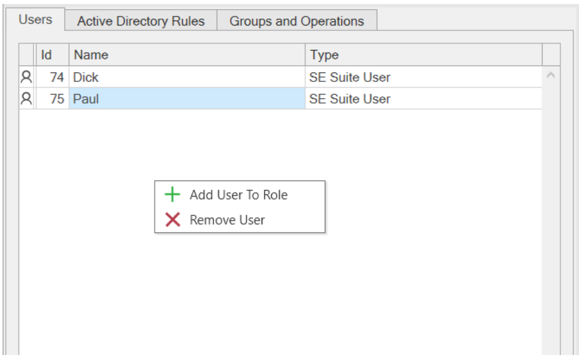
SES ENGINEERING Studio

The user SESAdministrator does not belong to any role assigned to the operation "Assess quality" and therefore does not have execution permissions.
Permission code: OG_0100_ETO_0015_AssessQuality
Permission description: Operation to asses quality.

FIGURE 48

4. That means that SESAdministrator is not included in the Role RQAAdmin, which is a Role with all the RQA operations execution permissions, so we are proceeding to assign SES Administrator to that role.

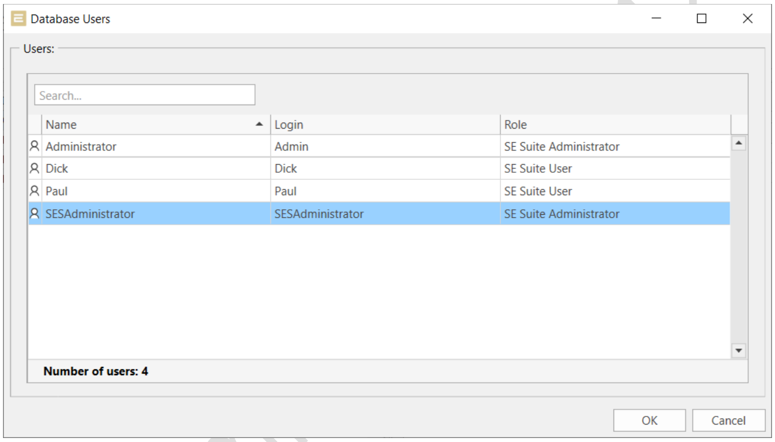
5. Let's go back to *Roles & Users*. On the right pane, right-click and select *Add User to Role.*



	Id	Name	Type
👤	74	Dick	SE Suite User
👤	75	Paul	SE Suite User

FIGURE 49

6. Now select the SESAdministrator user in the list and click *OK*.

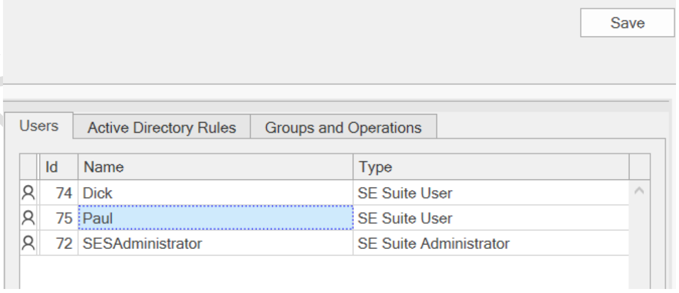


Name	Login	Role
Administrator	Admin	SE Suite Administrator
Dick	Dick	SE Suite User
Paul	Paul	SE Suite User
SESAdministrator	SESAdministrator	SE Suite Administrator

Number of users: 4

FIGURE 50

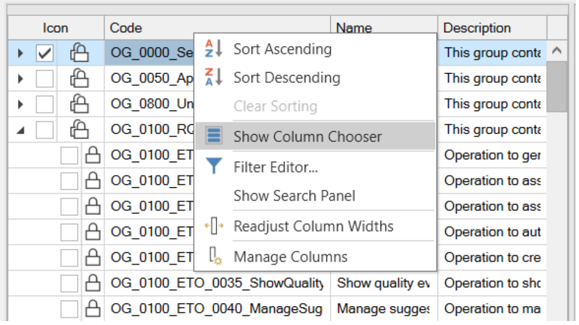
7. Check that SESAdministrator is properly listed and *Save* the role view.



	Id	Name	Type
👤	74	Dick	SE Suite User
👤	75	Paul	SE Suite User
👤	72	SESAdministrator	SE Suite Administrator

FIGURE 51

8. To help the security manager(s), you can know the affected Code editing the columns of the operations in the Security Management to show the Code column, which is not shown by default. Right-click on the titles of the middle pane to get a menu. Select *Show Column Chooser*.



	Icon	Code	Name	Description
▸	☑	OG_0000_Se		This group conta
▸	□	OG_0050_Ap		This group conta
▸	□	OG_0800_Un		This group conta
◢	□	OG_0100_RC		This group conta
	□	OG_0100_ET		Operation to ger
	□	OG_0100_ET		Operation to ass
	□	OG_0100_ET		Operation to ass
	□	OG_0100_ET		Operation to aut
	□	OG_0100_ET		Operation to cre
	□	OG_0100_ETO_0035_ShowQuality	Show quality ev	Operation to shc
	□	OG_0100_ETO_0040_ManageSug	Manage sugges	Operation to ma

FIGURE 52

9. Click on the *Code* box to show the column.

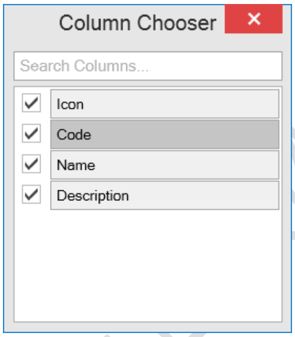


FIGURE 53

10. Now you should be able to execute the quality assessment. Follow the steps 1 to 3 of this section to perform it.

10.7 Summary

In the next figure it is represented a Summary of the previous exercise:

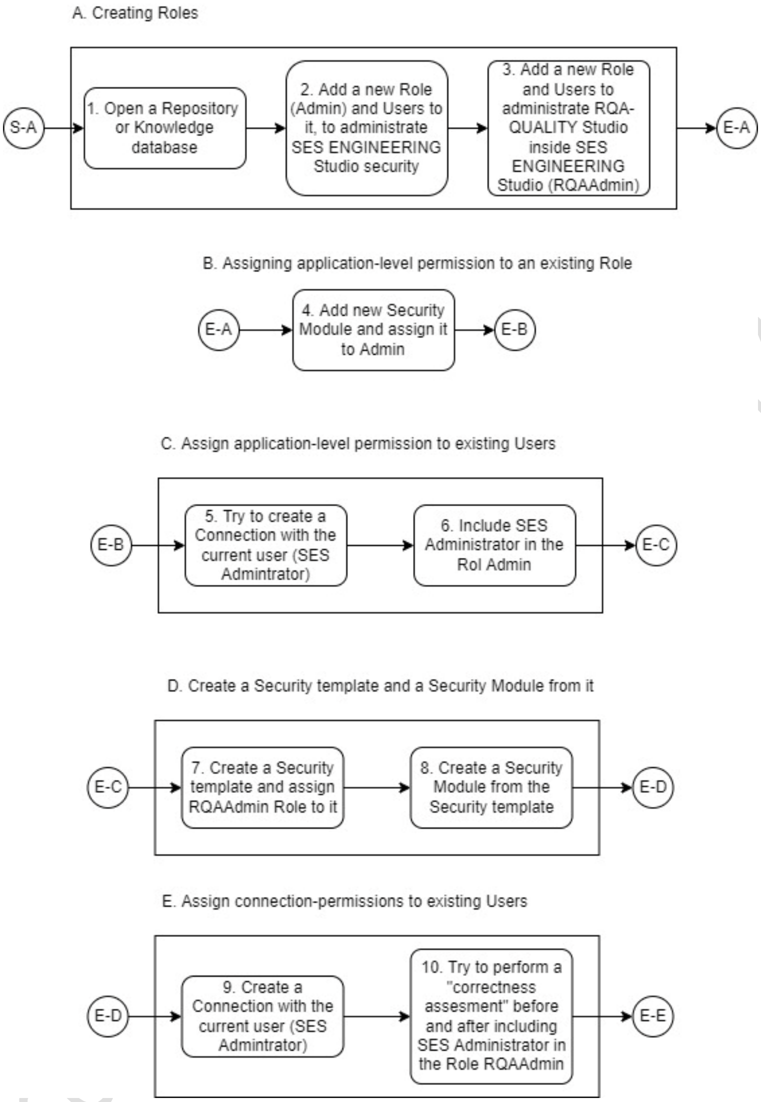

A. Creating Roles
S-A
1. Open a Repository or Knowledge database
2. Add a new Role (Admin) and Users to it, to administrate SES ENGINEERING Studio security
3. Add a new Role and Users to administrate RQA-QUALITY Studio inside SES ENGINEERING Studio (RQAAdmin)
E-A
B. Assigning application-level permission to an existing Role
E-A
4. Add new Security Module and assign it to Admin
E-B
C. Assign application-level permission to existing Users
E-B
5. Try to create a Connection with the current user (SES Admintrator)
6. Include SES Administrator in the Rol Admin
E-C
D. Create a Security template and a Security Module from it
E-C
7. Create a Security template and assign RQAAdmin Role to it
8. Create a Security Module from the Security template
E-D
E. Assign connection-permissions to existing Users
E-D
9. Create a Connection with the current user (SES Admintrator)
10. Try to perform a "correctness assesment" before and after including SES Administrator in the Role RQAAdmin
E-E

FIGURE 54

Annex 1: Security Permissions List

Security Management Operations	
OG_0000_SecurityManagementOperations	Security Management Operations
OG_0000_ETO_0010_ManageSecurityModules	Manage security modules
OG_0000_ETO_0020_ManageRoles	Manage roles
OG_0000_ETO_0030_ManageUsers	Manage users
OG_0000_ETO_0040_ManageActiveDirectoryRules	Manage active directory rules
OG_0000_ETO_0050_AssignOrUnassignRole	Assign or unassign role
OG_0000_ETO_0060_SaveSecurityModule	Save security module

Application Execution Operations	
OG_0050_ApplicationExecutionOperations	Application Execution Operations
OG_0050_ETO_0010_SESServerExecution	SES Server Execution
OG_0050_ETO_0015_KMExecution	KM Execution
OG_0050_ETO_0020_SESENGINEERINGStudioExecution	SES ENGINEERING Studio Execution
OG_0050_ETO_0025_SESRQAQualityStudioExecution	SES RQA - Quality Studio Execution
OG_0050_ETO_0030_SESTRACEABILITYStudioExecution	SES TRACEABILITY Studio Execution
OG_0050_ETO_0035_SESVVStudioExecution	SES V&V Studio Execution

RQA Operations	
OG_0100_RQAOperations	RQA Operations
OG_0100_ETO_0010_GenerateReport	Generate report
OG_0100_ETO_0015_AssessQuality	Assess quality
OG_0100_ETO_0020_AssessQualityScalability	Assess quality with scalability platform
OG_0100_ETO_0025_AuthorWorkproduct	Author workproduct
OG_0100_ETO_0030_CreateSnapshot	Create snapshot
OG_0100_ETO_0035_ShowQualityEvolution	Show quality evolution
OG_0100_ETO_0040_ManageSuggestionsOfTheActiveUser	Manage suggestions of the active user
OG_0100_ETO_0045_ManageAggregatedSpecifications	Manage aggregated specifications
OG_0100_ETO_0050_ManageCorrectnessMetrics	Manage correctness metrics
OG_0100_ETO_0055_ManageCompletenessMetrics	Manage completeness metrics
OG_0100_ETO_0060_ManageConsistencyMetrics	Manage consistency metrics
OG_0100_ETO_0065_ManageAuthoringPatternsGroups	Manage authoring patterns groups
OG_0100_ETO_0070_ManageProjectSuggestions	Manage project suggestions
OG_0100_ETO_0075_ManageProjectConfiguration	Manage project configuration
OG_0100_ETO_0080_ManageCustomCodeReports	Manage custom code reports
OG_0100_ETO_0085_ManageCustomCodeMetrics	Manage custom code metrics
OG_0100_ETO_0090_RQABatchCreateCustomReport	RQA Batch - Create custom report
OG_0100_ETO_0095_RQABatchProjectCredentials	RQA Batch - Manage project credentials
OG_0100_ETO_0100_ManageModuleConfigurationLoader	Manage module configuration loader
OG_0100_ETO_0105_ManageMetricsSetBaselines	Manage metrics set baselines
OG_0100_ETO_0110_ManageDefaultMagnitudes	Manage default magnitudes
OG_0100_ETO_0115_ManageSpecialSentences	Manage special sentences
OG_0100_ETO_0120_ManageOntologyNouns	Manage ontology nouns
OG_0100_ETO_0125_ManageOntologyVerbs	Manage ontology verbs

OG_0100_ETO_0130_ManageWhitelistManager	Manage whitelist manager
OG_0100_ETO_0135_ManageBlacklistManager	Manage blacklist manager
OG_0100_ETO_0140_RecalculateDictionaries	Recalculate dictionaries
OG_0100_ETO_0145_ManageSpellcheckerSettings	Manage spellchecker settings

Lifecycle Management Operations	
OG_0200_LifeCycleManagementOperations	Lifecycle Management Operations
OG_0200_ETO_0010_ShowProjectsList	Show projects list
OG_0200_ETO_0020_OpenProject	Open project
OG_0200_ETO_0030_ManageProject	Manage project
OG_0200_ETO_0040_ShowGraphicalInformationInProject	Show graphical information
OG_0200_ETO_0050_ViewLogInProject	View log
OG_0200_ETO_0060_ManageConfigurationInProject	Manage configuration
OG_0200_ETO_0070_ManageVersionInProject	Manage version
OG_0200_ETO_0080_SaveProject	Save project
OG_0200_ETO_0100_ManageActivityInProject	Manage activity
OG_0200_ETO_0110_AssessInProject	AssessQuality
OG_0200_ETO_0120_ManageProgressAndState	Manage progress and state
OG_0200_ETO_0130_ManageGantt	Manage gantt
OG_0200_ETO_0140_UpdateTechnicalManagementInProject	Update technical management
OG_0200_ETO_0150_ShowTemplatesList	Show templates list
OG_0200_ETO_0160_OpenTemplate	Open template
OG_0200_ETO_0170_ManageTemplate	Manage template
OG_0200_ETO_0180_SaveTemplate	Save template
OG_0200_ETO_0190_FinishTemplate	Finish template
OG_0200_ETO_0200_ShowGraphicalInformationInTemplate	Show graphical information
OG_0200_ETO_0210_ManageVersionInTemplate	Manage version
OG_0200_ETO_0220_ViewLogInTemplate	View log
OG_0200_ETO_0240_ManageActivityInTemplate	Manage activity

Risks & Alerts Operations	
OG_0300_RisksAndAlertsOperations	Risks & Alerts Operations
OG_0300_ETO_0010_CanAddAlertPackages	Add Alert Packages from SES ENIGINEERING Studio
OG_0300_ETO_0020_CanEditAlertPackages	Edit Alert Packages from SES ENIGINEERING Studio
OG_0300_ETO_0030_CanRemoveAlertPackages	Remove Alert Packages from SES ENIGINEERING Studio
OG_0300_ETO_0040_CanAddAlerts	Add Alerts from SES ENIGINEERING Studio
OG_0300_ETO_0050_CanEditAlerts	Edit Alerts from SES ENIGINEERING Studio
OG_0300_ETO_0060_CanRemoveAlerts	Remove Alerts from SES ENIGINEERING Studio
OG_0300_ETO_0070_CanCheckAlerts	Check Alerts from SES ENIGINEERING Studio
OG_0300_ETO_0060_CanRemoveAlerts	Remove Alerts from SES ENIGINEERING Studio
OG_0300_ETO_0070_CanCheckAlerts	Check Alerts from SES ENIGINEERING Studio
OG_0300_ETO_0050_CanEditAlerts	Edit Alerts from SES ENIGINEERING Studio
OG_0300_ETO_0060_CanRemoveAlerts	Remove Alerts from SES ENIGINEERING Studio

V&V Operations	
OG_0400_VVOperations	V&V Operations
OG_0400_ETO_0010_OpenSystemVerificationTemplates	Open System Verification templates
OG_0400_ETO_0015_ManageSystemVerificationTemplates	Manage System Verification templates

OG_0400_ETO_0020_OpenSystemValidationTemplates	Open System Validation templates
OG_0400_ETO_0025_ManageSystemValidationTemplates	Manage System Validation templates
OG_0400_ETO_0030_OpenBlockVerificationTemplates	Open Block Verification templates
OG_0400_ETO_0035_ManageBlockVerificationTemplates	Manage Block Verification templates
OG_0400_ETO_0040_OpenBlockValidationTemplates	Open Block Validation templates
OG_0400_ETO_0045_ManageBlockValidationTemplates	Manage Block Validation templates
OG_0400_ETO_0050_OpenActionVerificationTemplates	Open Verification Action templates
OG_0400_ETO_0055_ManageActionVerificationTemplates	Manage Verification Action templates
OG_0400_ETO_0060_OpenActionValidationTemplates	Open Validation Action templates
OG_0400_ETO_0065_ManageActionValidationTemplates	Manage Validation Action templates
OG_0400_ETO_0070_OpenActionVerification	Open Verification Actions
OG_0400_ETO_0075_ManageActionVerification	Manage Verification Actions
OG_0400_ETO_0080_OpenActionValidation	Open Validation Actions
OG_0400_ETO_0085_ManageActionValidation	Manage Validation Actions
OG_0400_ETO_0090_EvaluateVerificationAccess	Evaluate Verification Access
OG_0400_ETO_0095_EvaluationValidationAccess	Evaluate Validation Access
OG_0400_ETO_0100_ReportDocumentVerificationAccess	Verification Reporting Access
OG_0400_ETO_0115_ReportDocumentValidationAccess	Validation Reporting Access
OG_0400_ETO_0120_ReportMatrixVerificationAccess	Verification RTVM Access
OG_0400_ETO_0125_ReportMatrixValidationAccess	Validation RTVM Access
OG_0400_ETO_0130_FormGenerationVerificationAccess	Verification Form Generation Access
OG_0400_ETO_0135_FormGenerationValidationAccess	Validation Form Generation Access
OG_0400_ETO_0140_FormImportingVerificationAccess	Verification Form Import Access
OG_0400_ETO_0145_FormImportingValidationAccess	Validation Form Import Access

Traceability Management Operations	
OG_0500_TraceabilityManagementOperations	Traceability Management Operations
OG_0500_ETO_0010_OpenTraceabilityProject	Open traceability project
OG_0500_ETO_0015_ManageTraceabilityProjects	Manage traceability projects
OG_0500_ETO_0020_LoadUnloadTraceabilityModule	Load/Unload traceability module
OG_0500_ETO_0025_OpenTraceabilityModule	Open traceability module
OG_0500_ETO_0030_ManageTraceabilityModules	Manage traceability modules
OG_0500_ETO_0035_ShowModuleMapPanel	Show module map panel
OG_0500_ETO_0040_GenerateReport	Generate Report
OG_0500_ETO_0045_ManageTraces	Traceability Management Operations
OG_0500_ETO_0050_ShowTraceDetails	Open traceability project
OG_0500_ETO_0055_ShowImpactAnalysis	Manage traceability projects
OG_0500_ETO_0060_ChangeTraceState	Load/Unload traceability module
OG_0500_ETO_0065_ShowTraceabilityMatrix	Open traceability module

Content Manager Operations	
OG_0600_ContentManagerOperations	Content Manager Operations
OG_0600_ETO_0010_ManageViews	Manage views
OG_0600_ETO_0015_SaveContentManager	Save content manager
OG_0600_ETO_0020_SaveAsContentManager	Save as content manager
OG_0600_ETO_0025_ModifyGridVisualization	Modify grid visualization
OG_0600_ETO_0030_ModifyAttributesValue	Modify attributes value
OG_0600_ETO_0035_ShowMenuBar	Show menu bar
OG_0600_ETO_0040_ShowDocumentPane	Show document pane

OG_0600_ETO_0045_ShowContentPane	Show content pane
OG_0600_ETO_0050_ManageInteroperability	Manage interoperability
OG_0600_ETO_0055_ManageRowProperties	Manage row properties
OG_0600_ETO_0060_ManageColumnsAndAttributes	Manage columns and attributes

SES ENGINEERING Studio Operations	
OG_0700_EngineeringStudioOperations	SES ENIGINEERING Studio Operations
OG_0700_ETO_0015_ManageRolesAndUsers	Manage roles and users
OG_0700_ETO_0020_ManageSecurity	Manage security
OG_0700_ETO_0025_ManageTraceability	Manage traceability
OG_0700_ETO_0030_ManageReportTemplate	Manage report template
OG_0700_ETO_0035_OpenConnection	Open connection
OG_0700_ETO_0040_ManageConnection	Manage connection
OG_0700_ETO_0045_ManageModuleConfiguratorLoader	Manage module configurator loader
OG_0700_ETO_0050_CanAddRequirementEngineering	Add requirement from SES ENIGINEERING Studio
OG_0700_ETO_0055_CanEditRequirementEngineering	Edit requirement from SES ENIGINEERING Studio
OG_0700_ETO_0060_CanRemoveRequirementEngineering	Remove requirement from Engineering
OG_0700_ETO_0061_CanShowModulesConfiguration	Show Modules Configuration
OG_0700_ETO_0062_CanManageModuleConfiguration	Manage Module Configuration
OG_0700_ETO_0065_CanManageFormalization	Manage Formalization
OG_0700_ETO_0067_CanManageRolesInAccessLevel	Manage Roles In Access Level
OG_0700_ETO_0071_CanManageUseChangeRequest	Manage Use Change Request
OG_0700_ETO_0072_CanManageRolesInChangeRequest	Manage Roles In Change Request
OG_0700_ETO_0075_CanManageVisualWorkproductID	Manage Visual Workproduct ID
OG_0700_ETO_0079_CanManagePendingChangeRequests	Manage Pending Change Requests
OG_0700_ETO_0080_CanShowChangeRequestsHistory	Show Change Requests History
OG_0700_ETO_0082_CanManageRequestedChanges	Manage Requested Changes
OG_0700_ETO_0083_CanManageResolution	Manage Resolution
OG_0700_ETO_0084_CanManageExclusiveAccessLevel	Manage Exclusive Access Level
OG_0700_ETO_0085_CanDeleteContentInRepository	Delete content in Repository

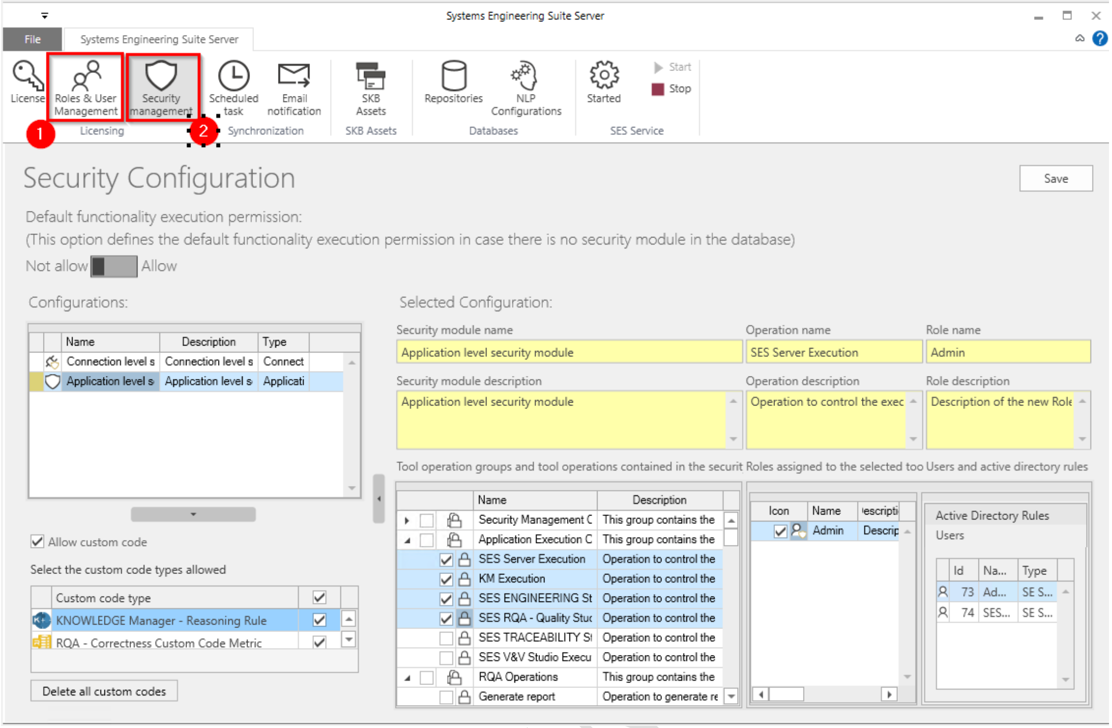
Universal Report System Operations	
OG_0800_UniversalReportSystemOperations	Universal Report System Operations
OG_0800_ETO_0010_CanAddNewDocumentTemplateOperation	Add new document template
OG_0800_ETO_0015_CanEditDocumentTemplateOperation	Edit document template
OG_0800_ETO_0020_CanRemoveDocumentTemplateOperation	Remove document template
OG_0800_ETO_0025_CanViewTemplateOperation	View template
OG_0800_ETO_0030_CanExportSelectedTemplatesOperation	Export selected templates
OG_0800_ETO_0035_CanImportTemplatesOperation	Import templates
OG_0800_ETO_0040_CanCreateReportFromTemplate	Create report from template
OG_0800_ETO_0045_CanPersistReportAsME	Persist report as ME
OG_0800_ETO_0050_CanSaveReportInLocal	Save report in local

Annex 2: Minimum Security Configuration permissions

The SES Suite provides a series of different capabilities like generation of Roles (Bullet 1 in Figure 55**Error! Reference source not found.**) and Security Management (Bullet 2 in Figure 55).
These capabilities are defined inside SES Server application, managed by any Admin user. Based on this scope, the set of capabilities to analyze are the following:

- Application Execution Operations
  - SES Server Execution
  - KM Execution
  - SES ENGINEERING Studio Execution
  - SES RQA – Quality Studio Execution
- RQA Operations
  - Generate report
  - Assess quality
  - Show quality evolution
- Content Manager Operations
  - Manage views
  - Save content manager
  - Save as content manager
  - Modify grid visualization
  - Modify attributes value
  - Show menu bar
  - Show document pane
  - Show content pane
  - Manage interoperability
  - Manage row properties
  - Manage columns and attributes
- Engineering Studio Operations
  - Open connection
  - Manage connection
  - Show Modules Configuration
  - Show Change Requests History

The other sections shall remain unchecked.



Security Configuration

Default functionality execution permission:
(This option defines the default functionality execution permission in case there is no security module in the database)
Not allow ▮ Allow

Configurations:

Name	Description	Type
Connection level s	Connection level s	Connect
Application level s	Application level s	Applicati

☑ Allow custom code

Select the custom code types allowed

Custom code type	☑
KNOWLEDGE Manager - Reasoning Rule	☑
RQA - Correctness Custom Code Metric	☑

Delete all custom codes

Selected Configuration:

Security module name: Application level security module
Operation name: SES Server Execution
Role name: Admin
Security module description: Application level security module
Operation description: Operation to control the exec
Role description: Description of the new Role

Tool operation groups and tool operations contained in the securit

	Name	Description
▸ □	Security Management C	This group contains the
◢ □	Application Execution C	This group contains the
☑	SES Server Execution	Operation to control the
☑	KM Execution	Operation to control the
☑	SES ENGINEERING St	Operation to control the
☑	SES RQA - Quality Stuc	Operation to control the
□	SES TRACEABILITY St	Operation to control the
□	SES V&V Studio Execu	Operation to control the
◢ □	RQA Operations	This group contains the
□	Generate report	Operation to generate re

Roles assigned to the selected too

Icon	Name	escripti
☑	Admin	Descrip

Users and active directory rules

Active Directory Rules
Users

Id	Na...	Type
73	Ad...	SE S...
74	SES...	SE S...

FIGURE 55

This section provides the description of each feature, including the eventual dependencies between features (if any) and the columns corresponding to the abovementioned roles, indicating whether or not the feature shall be assigned to this role.

NOTE: this configuration of permissions is just a suggestion from The REUSE Company; the customer shall decide which is the proper configuration to be assigned.

Main Operation	Sub operation/Feature	Description	Dependencies	Admin	Onto Mngr	Quality Mngr	Project Mngr	Req Author
Application Execution Operations	SES Server Execution	Allows the execution of SES Server. You must have it, to connect to the different databases in SES Server	None	x				
	KM Execution	Allows the execution of Knowledge Manager. You must have it, to connect to the different databases in KM		x	x			
	SES ENGINEERING Studio Execution	Allows the execution of SES ENGINEERING Studio. You must have it, to connect to the different databases		x		x	x	x
	SES RQA – Quality Studio Execution	Allows the execution of RQAStudio.exe as an independent application		x		x	x	x
	SES TARCEABILITY Studio Execution	Allows the execution of TRACEABILITYStudio.exe as an independent application						
	SES V&V Studio Execution	Allows the execution of V&VStudio.exe as an independent application						
RQA Operations	Generate report	Enables Short worksheet Quality Report and Full worksheet Quality Report tabs inside RQA Quality view	SES ENGINEERING Studio Execution			x	x	

Main Operation	Sub operation/Feature	Description	Dependencies	Admin	Onto Mngr	Quality Mngr	Project Mngr	Req Author
			Open Connection					
	Assess quality	Enables Assess Quality functionality inside RQA Quality view	SES ENGINEERING Studio Execution Open Connection			x	x	
RQA Operations	Show Quality evolution	Enables Evolution Scoreboard option in the Quality Scoreboard Panel	SES ENGINEERING Studio Execution Open Connection			x	x	
	Author workproduct	Operation to author workproduct	SES ENGINEERING Studio Execution Open Connection			x	x	x
	Create snapshot	Operation to create snapshot	SES ENGINEERING Studio Execution Open Connection			x	x	
	Show quality evolution	Operation to show quality evolution	SES ENGINEERING Studio Execution Open Connection			x	x	
	Manage suggestions of the active user	Operation to manage suggestions of the active user	SES ENGINEERING Studio Execution Open Connection			x	x	
RQA Operations	Manage aggregated specifications	Operation to manage aggregated specifications	SES ENGINEERING Studio Execution Open Connection			x	x	
	Manage correctness metrics	Operation to manage correctness metrics	SES ENGINEERING Studio Execution Open Connection			x	x	

Main Operation	Sub operation/Feature	Description	Dependencies	Admin	Onto Mngr	Quality Mngr	Project Mngr	Req Author
	Manage completeness metrics	Operation to manage completeness metrics	SES ENGINEERING Studio Execution Open Connection			x	x	
	Manage consistency metrics	Operation to manage consistency metrics	SES ENGINEERING Studio Execution Open Connection			x	x	
	Manage authoring patterns groups	Operation to manage authoring patterns groups	SES ENGINEERING Studio Execution Open Connection			x	x	
RQA Operations	Manage project suggestions	Operation to manage project suggestions	SES ENGINEERING Studio Execution Open Connection				x	
	Manage project configuration	Operation to manage project configuration	SES ENGINEERING Studio Execution Open Connection				x	
	Manage custom code reports	Operation to manage custom code reports	SES ENGINEERING Studio Execution Open Connection					
	Manage custom code metrics	Operation to manage custom code metrics	SES ENGINEERING Studio Execution Open Connection					
	RQA Batch - Create custom report	Operation to RQA batch - create custom report	SES ENGINEERING Studio Execution Open Connection				x	
RQA Operations	RQA Batch - Manage project credentials	Operation to RQA batch - manage project credentials	SES ENGINEERING Studio Execution Open Connection				x	
		Operation to manage module configuration loader	SES ENGINEERING Studio Execution				x	

Main Operation	Sub operation/Feature	Description	Dependencies	Admin	Onto Mngr	Quality Mngr	Project Mngr	Req Author
	Manage module configuration loader		Open Connection					
	Manage metrics set baselines	Operation to manage metrics set baselines	SES ENGINEERING Studio Execution Open Connection			x	x	
	Manage default magnitudes	Operation to manage default magnitudes	SES ENGINEERING Studio Execution Open Connection			x	x	
	Manage special sentences	Operation to manage special sentences	SES ENGINEERING Studio Execution Open Connection			x	x	
RQA Operations	Manage ontology nouns	Operation to manage ontology nouns	SES ENGINEERING Studio Execution Open Connection		x			
	Manage ontology verbs	Operation to manage ontology verbs	SES ENGINEERING Studio Execution Open Connection		x			
	Manage whitelist manager	Operation to manage whitelist manager	SES ENGINEERING Studio Execution Open Connection		x			
	Manage blacklist manager	Operation to manage blacklist manager	SES ENGINEERING Studio Execution Open Connection		x			
	Recalculate dictionaries	Operation to recalculate dictionaries	SES ENGINEERING Studio Execution Open Connection		x			
RQA Operations	Manage spellchecker settings	Operation to manage spellchecker settings	SES ENGINEERING Studio Execution Open Connection		x			

Main Operation	Sub operation/Feature	Description	Dependencies	Admin	Onto Mngr	Quality Mngr	Project Mngr	Req Author
Content Manager Operations	Manage views	Enables Manage views functionality inside a connection. Right click -> views -> Manage views	SES ENGINEERING Studio Execution Open Connection	x		x	x	x
	Save content	Enables Save views functionality inside a connection. Right click -> Save views	SES ENGINEERING Studio Execution Open Connection	x		x	x	x
Content Manager Operations	Save as content manager	Enables Save current view as new inside a connection. Right click -> Save current view as new	SES ENGINEERING Studio Execution Open Connection	x		x	x	x
	Modify grid visualization	Enables all Functionalities from Visualization Model folder inside a connection. Right click -> Visualization Model	SES ENGINEERING Studio Execution Open Connection	x		x	x	x
	Modify attributes value	Allows to modify attribute / property values inside a connection	SES ENGINEERING Studio Execution Open Connection Manage columns and attributes	x		x	x	x
	Show document pane	Enables panes functionality that Shows the documentary area inside a connection. Right click -> panes-> Document pane	SES ENGINEERING Studio Execution Open Connection	x		x	x	x
	Show content pane	Enables panes functionality that displays the content zone inside a connection. Right click -> panes-> Content pane	SES ENGINEERING Studio Execution Open Connection	x		x	x	x

Main Operation	Sub operation/Feature	Description	Dependencies	Admin	Onto Mngr	Quality Mngr	Project Mngr	Req Author
	Manage interoperability[1]	Enables start binding functionality to manage interoperability CRUD.	SES ENGINEERING Studio Execution	x			x	
		Right click -> Start Binding	Open Connection					
	Manage row properties	Enables the functionality to manage the rows properties.	SES ENGINEERING Studio Execution	x		x	x	x
		Right click -> Rows	Open Connection					
	Manage columns and attributes	Enables the functionality to manage CRUD functions on columns and on attributes / properties.	SES ENGINEERING Studio Execution	x		x	x	x
		Right click -> columns -> manage columns	Open Connection					
ENGINEERING Studio Operations	Open connection	Allows to open a connection in SES ENGINEERING Studio	SES ENGINEERING Studio Execution	x	x	x	x	x
	Manage connection	Allows to manage a connection in SES ENGINEERING Studio (Add, Edit or Delete a connection)	SES ENGINEERING Studio Execution	x		x	x	
	Show Modules Configuration	Enables Modules Settings option in the Connections tab	SES ENGINEERING Studio Execution	x	x	x	x	x
	Show Change Requests History	Allows view history window in the Change Management tab	SES ENGINEERING Studio Execution	x			x	

[1] This process requires an additional license for interoperability.

The REUSE Company

The REUSE Company is an organization specialized in the application of Semantic Representation and Analysis Technologies to a wide range of industries (Aerospace, Defense, Automotive, Naval, Health, ...). Our customers are usually (but not limited to) safety-oriented organizations.

Our focus is on System/Software Reuse, Traceability and Quality applied to all types of work-products throughout the whole SE lifecycle (requirements, SysML Models, physical models, tests cases, data results, manuals, natural language descriptions, fault trees, etc.). The integration of tools and technology from The REUSE Company facilitates the representation, analysis and exploitation of knowledge allowing for a knowledge-centric system engineering approach.

Our mission is to promote system/software and knowledge reuse within any organization, by offering processes, methods, tools and services that make it possible. We offer technology that is fully integrated within the organization's production chain.

THE REUSE COMPANY