eas

ESSENTIAL PROJECT

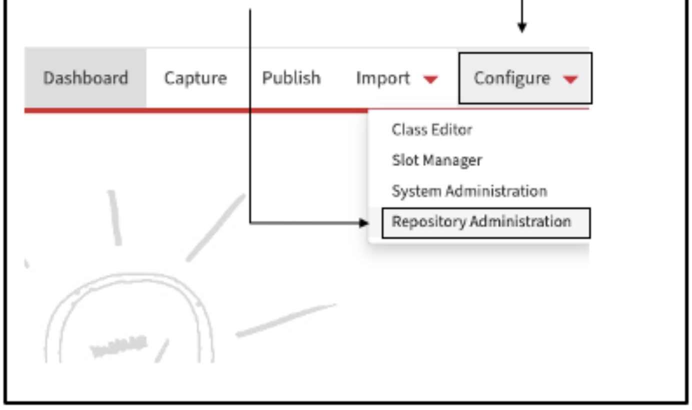
SECURITY CLASSIFICATION INSTRUCTIONS

Table of Contents

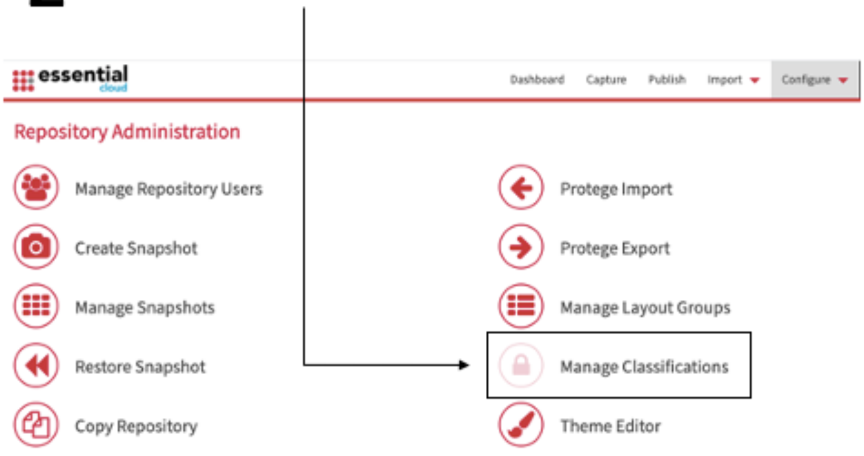
Allow user to only access certain reports/views

This scenario will allow you to make only certain reports/views accessible to a user depending on what you want them to be able to see. Instead of hiding each view individually, this will help to speed up that process and hide as many as you need to all at once.

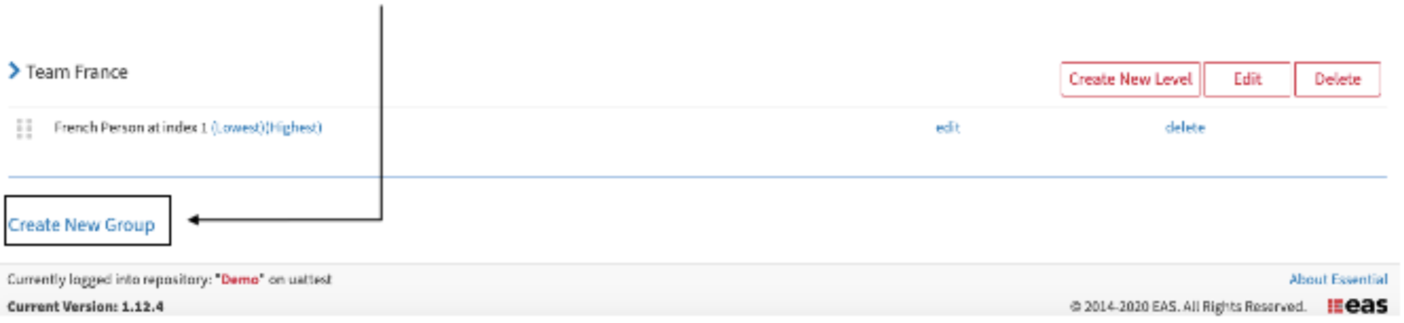
1 Go to Tool/Modeller and select 'Configure', then 'Repository Administration'.



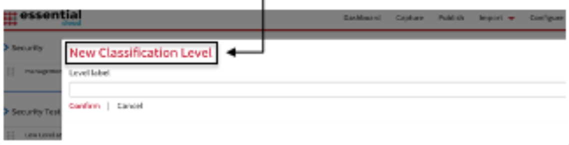
2 Select 'Manage Classifications'.



3 'Create New (Security) Group', or take note of the levels within the group.


Team France
Create New Level
Edit
Delete
French Person at index 1 (Lowest)(Highest)
edit
delete
Create New Group
Currently logged into repository: "Demo" on uattest
Current Version: 1.12.4
About Essential
© 2014-2020 EAS. All Rights Reserved.
eas

If adding New Classification Level, enter Name and confirm.

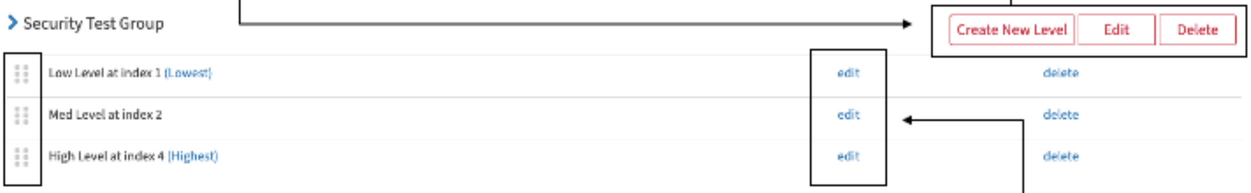


New Classification Level

Level label

Confirm | Cancel

4 Create New Levels, Edit the group name, or Delete the group.



Security Test Group

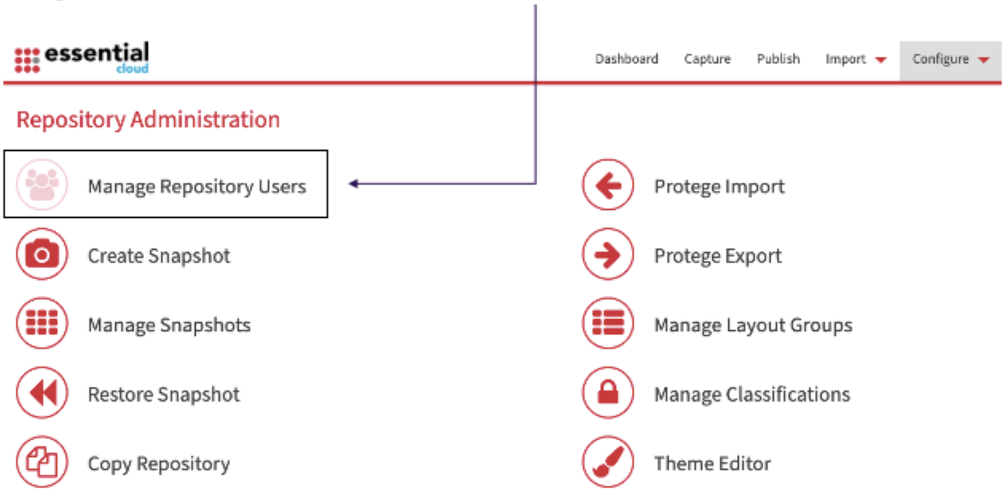
Create New Level | Edit | Delete

Low Level at index 1 (Lowest)	edit	delete
Med Level at index 2	edit	delete
High Level at index 4 (Highest)	edit	delete

6 Change the order of the index by dragging the dots to desired order.

5 'Edit' the level name, or delete it.

7 Return to configure and select 'Manage Repository Users'.

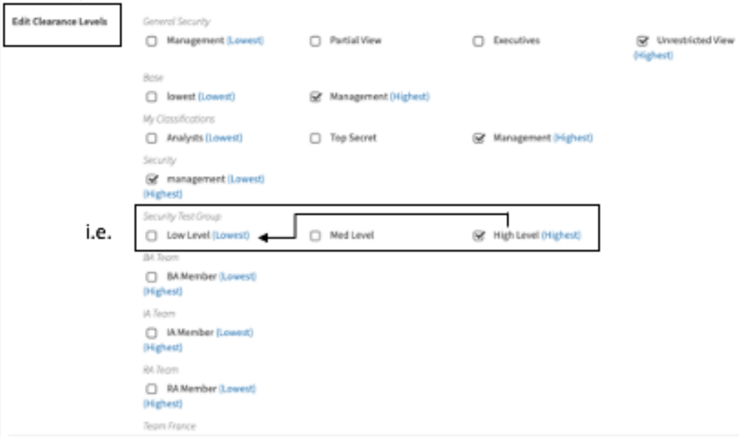


Repository Administration

- Manage Repository Users
- Create Snapshot
- Manage Snapshots
- Restore Snapshot
- Copy Repository
- Protege Import
- Protege Export
- Manage Layout Groups
- Manage Classifications
- Theme Editor

8 Change User Edit Clearance Level to 'Low'.

Select the user you wish to apply a security classification to.



Edit Clearance Levels

General Security
□ Management (Lowest) □ Partial View □ Executives ☑ Unrestricted View (Highest)

Base
□ lowest (Lowest) ☑ Management (Highest)

My Classifications
□ Analysts (Lowest) □ Top Secret ☑ Management (Highest)

Security
☑ management (Lowest) (Highest)

i.e.

Security Test Group
□ Low Level (Lowest) □ Med Level ☑ High Level (Highest)

BA Team
□ BA Member (Lowest) (Highest)

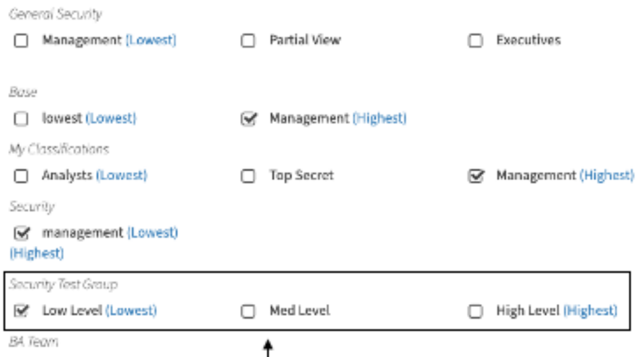
IA Team
□ IA Member (Lowest) (Highest)

RA Team
□ RA Member (Lowest) (Highest)

Team France

9 Change the Read Clearance Levels to 'Low'.

Read Clearance Levels



General Security

☐ Management (Lowest) ☐ Partial View ☐ Executives

Base

☐ lowest (Lowest) ☑ Management (Highest)

My Classifications

☐ Analysts (Lowest) ☐ Top Secret ☑ Management (Highest)

Security

☑ management (Lowest) (Highest)

Security Test Group

☑ Low Level (Lowest) ☐ Med Level ☐ High Level (Highest)

BA Team

Once the default is applied, user will need at least the low-level clearances to access and edit the instance.

To apply a new security group to a user, select the applicable security group created under *Edit* and/or *Read*

If you select Level 1 and it will be available in the Security Classification for selection.

Select Level 2 and both Level 1 and 2 will be available

Select Level 3 all levels will be available for selection

10 Give a set of people access to certain Views only

Allow a set of people to access only specific Views. Note:

- Access to the Views is only defined at the View level
- Can be combined with Scenario 2 to control access to Portals and Views

Options:

- Use the Default Security classification and then de-classify the Views that the set of people are allowed to access (including the Home page and a Portal)
- Classify all the Views to which these people are not allowed to access, with a classification that exceeds their clearance levels

Recommended approach

- Classify all the Views (and Portals) to which the people must **not** have access

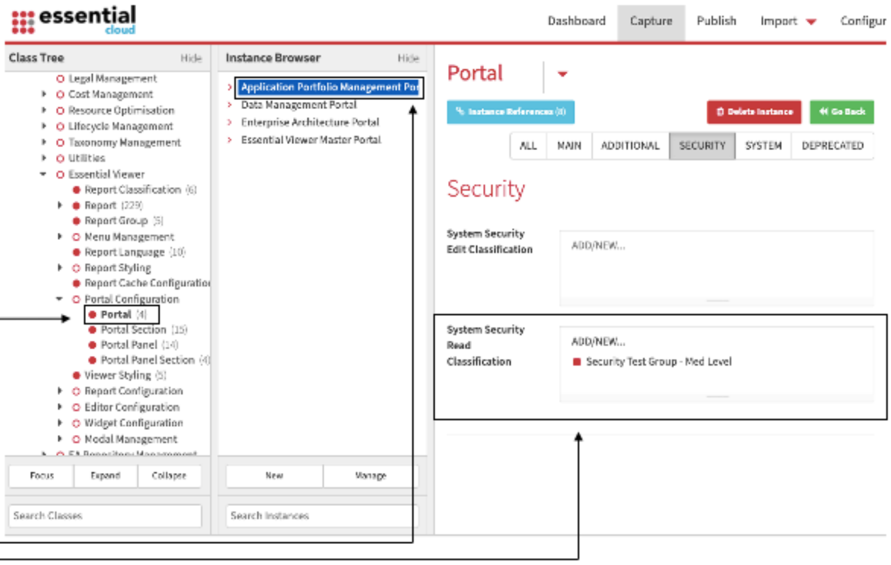
Example will use this approach.

11 Now apply a higher classification to the portal(s) than the user has to hide the views/classes you don't want them to access. E.g. *Application Portfolio Management Portal* (will also apply it to *Data Management Portal*)

EA Class > EA Support > Essential Viewer > Portal Configuration > Portal

Select the Portal to be classified.

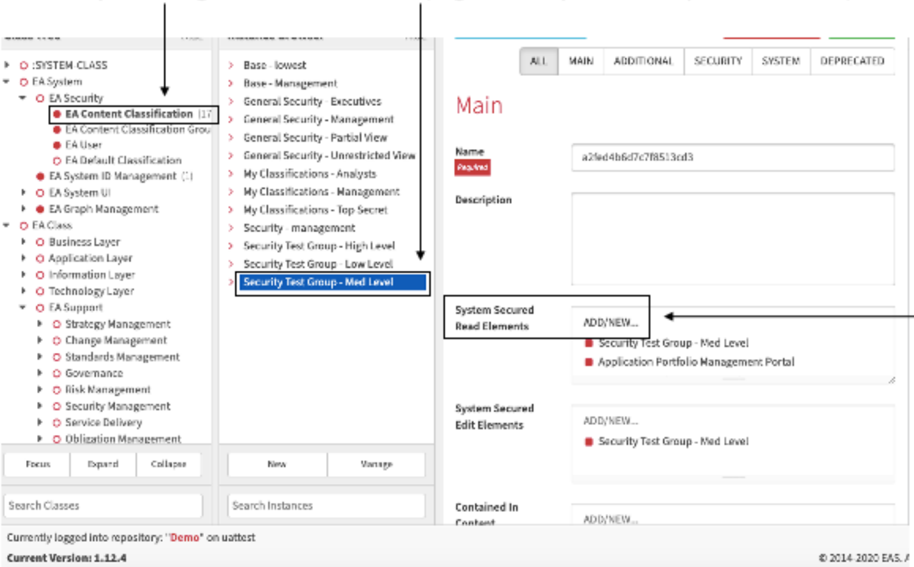
Select ADD/NEW in System Security Read Classification.



System Security Edit Classification: ADD/NEW...

System Security Read Classification: ADD/NEW...
■ Security Test Group - Med Level

12 Select EA System > EA Security > EA Content Classification, and the security classification that will require a higher level to access (e.g. Security Test Group – Med Level)



Name Required: a2fed4b6d7c7f8513cd3

Description:

System Secured Read Elements: ADD/NEW...
- Security Test Group - Med Level
- Application Portfolio Management Portal

System Secured Edit Elements: ADD/NEW...
- Security Test Group - Med Level

Contained In Content: ADD/NEW...

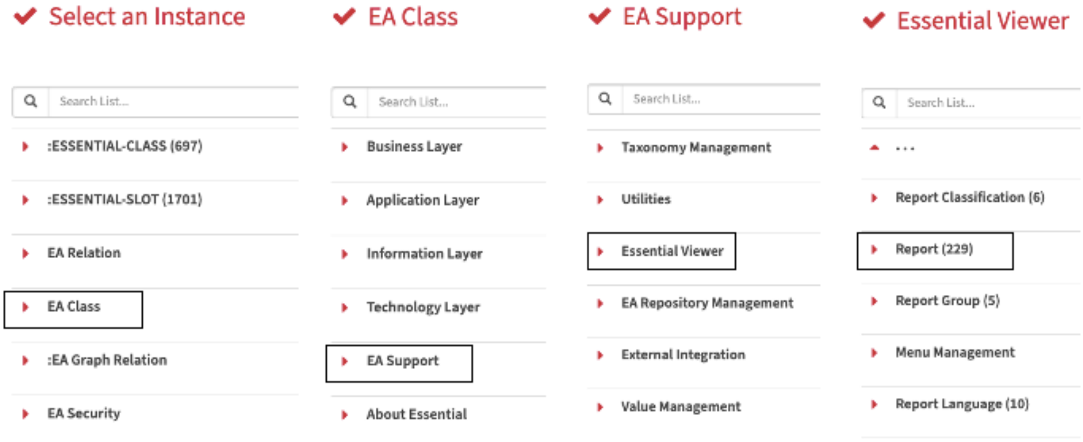
Currently logged into repository: "Demo" on uattest

Current Version: 1.12.4

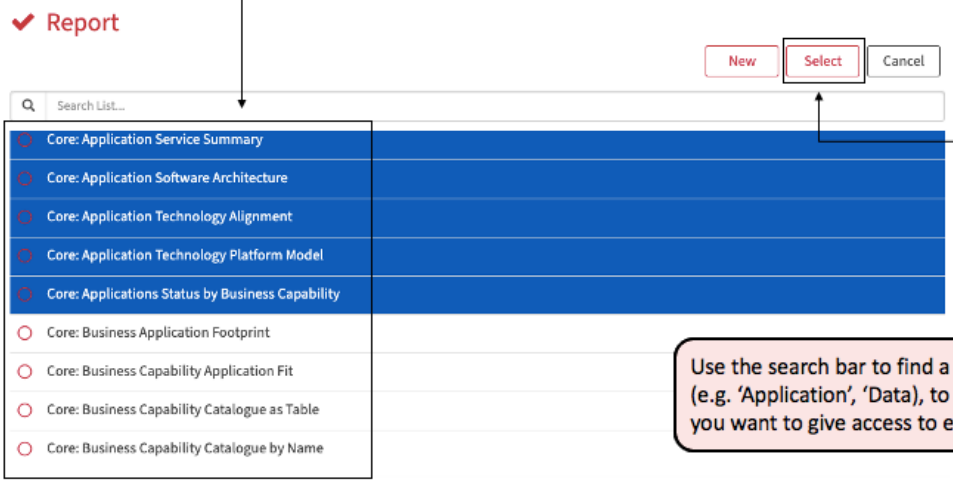
© 2014-2020 EAS. /

13 Then ADD/NEW to the System Secured Read Elements.

14 To hide certain views/reports, select EA Class > EA Support > Essential Viewer > Report.



15 Select all the reports/views you want to be hidden from the user.

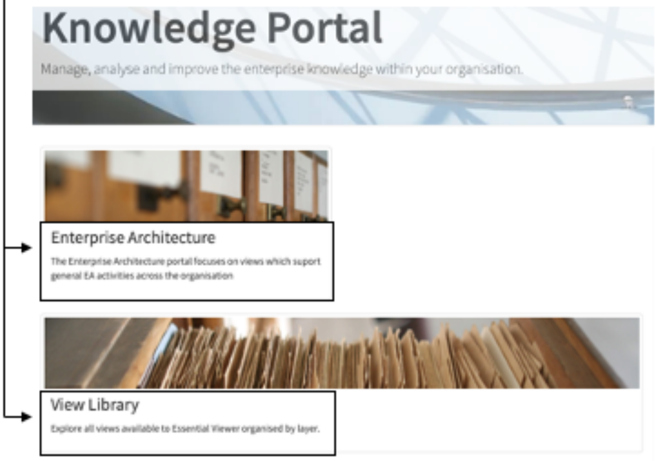


- ○ Core: Application Service Summary
- ○ Core: Application Software Architecture
- ○ Core: Application Technology Alignment
- ○ Core: Application Technology Platform Model
- ○ Core: Applications Status by Business Capability
- ○ Core: Business Application Footprint
- ○ Core: Business Capability Application Fit
- ○ Core: Business Capability Catalogue as Table
- ○ Core: Business Capability Catalogue by Name

16 Click 'select' once all the desired reports have been highlighted.

Use the search bar to find a specific report or category (e.g. 'Application', 'Data), to make finding the reports you want to give access to easier.

17 Only the portals without classifications are now visible, along with any application/data related views also being classified



Knowledge Portal

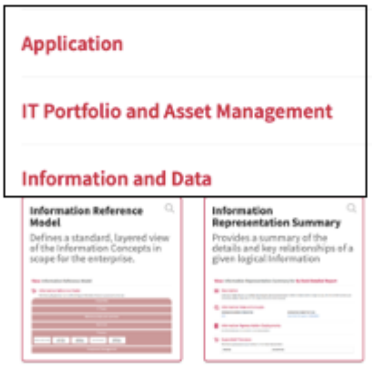
Manage, analyse and improve the enterprise knowledge within your organisation.

Enterprise Architecture

The Enterprise Architecture portal focuses on views which suport general EA activities across the organisation

View Library

Explore all views available to Essential Viewer organised by layer.



Application

IT Portfolio and Asset Management

Information and Data

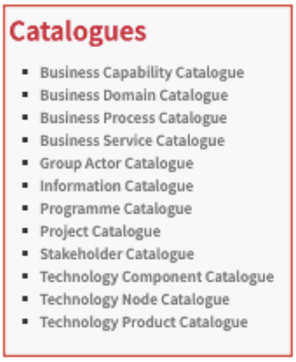
Information Reference Model

Defines a standard, layered view of the Information Concepts in scope for the enterprise.

Information Representation Summary

Provides a summary of the details and key relationships of a given logical Information

18 Catalogues also now classified if they're application or data related.

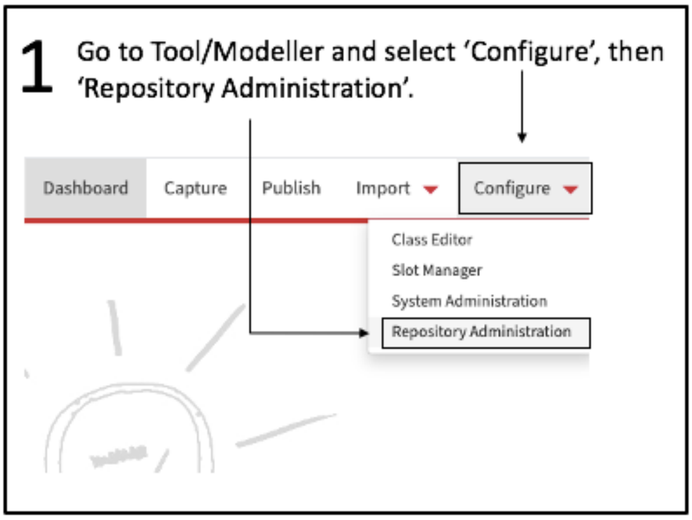


Catalogues

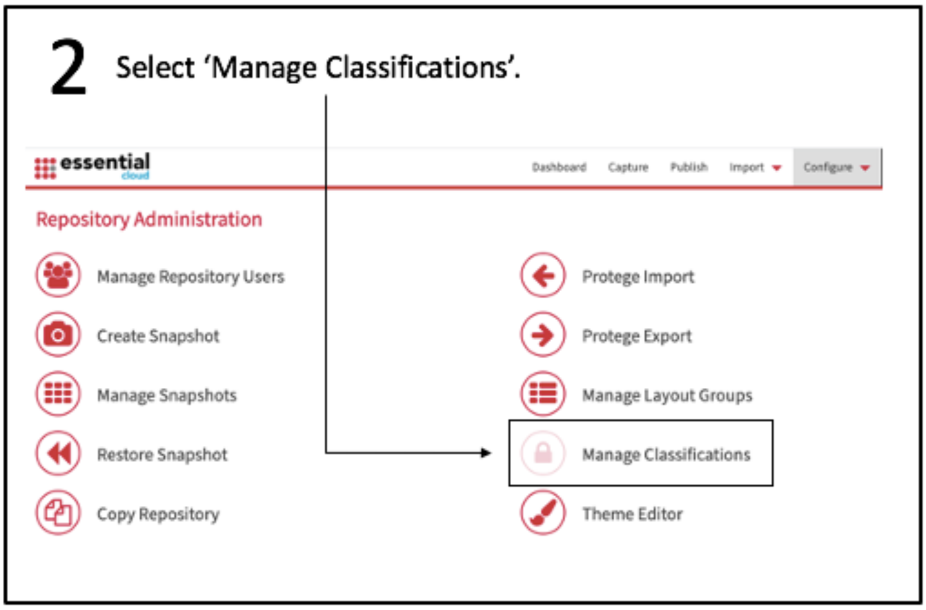
- Business Capability Catalogue
- Business Domain Catalogue
- Business Process Catalogue
- Business Service Catalogue
- Group Actor Catalogue
- Information Catalogue
- Programme Catalogue
- Project Catalogue
- Stakeholder Catalogue
- Technology Component Catalogue
- Technology Node Catalogue
- Technology Product Catalogue

Hide a Slot (e.g., Costs)

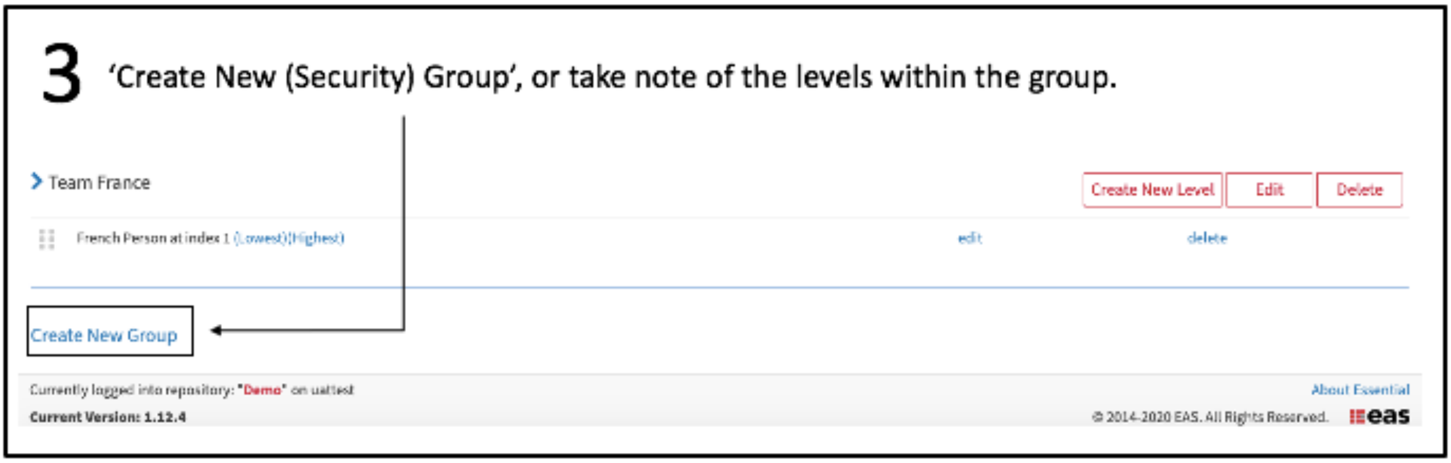
This scenario will take you through how to hide a slot from a user. Adding classifications to slots will hide certain aspects of the organisation from the user (e.g., costs) in order to protect that information, but still allow a user to view things related to those costs.



1 Go to Tool/Modeller and select 'Configure', then 'Repository Administration'.



2 Select 'Manage Classifications'.



3 'Create New (Security) Group', or take note of the levels within the group.

Team France

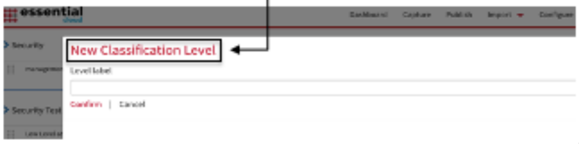
French Person at index 1 (Lowest)(Highest)

Currently logged into repository: "Demo" on uattest

Current Version: 1.12.4

© 2014-2020 EAS. All Rights Reserved.

If adding New Classification Level, enter Name and confirm.

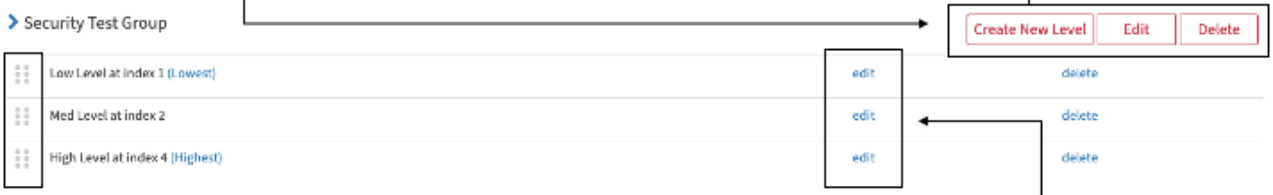


New Classification Level

Level label

Confirm | Cancel

4 Create New Levels, Edit the group name, or Delete the group.



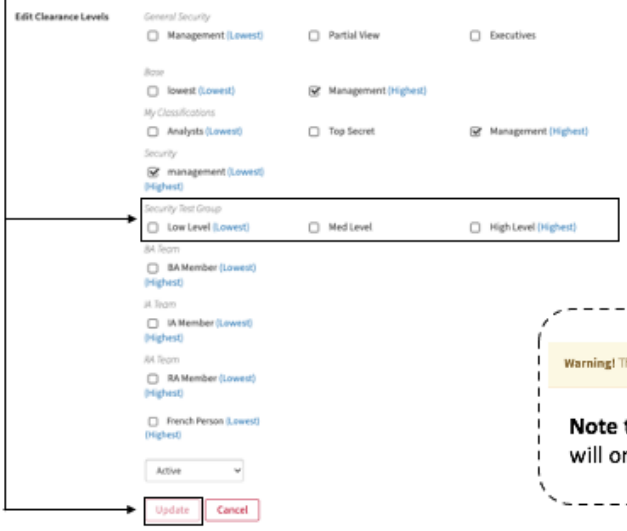
Security Test Group

Low Level at index 1 (Lowest)	edit	delete
Med Level at index 2	edit	delete
High Level at index 4 (Highest)	edit	delete

6 Change the order of the index by dragging the dots to desired order.

5 'Edit' the level name, or delete it.

7 Next go to Manage Repository Users, select the user(s) you want to make security classification changes to. For the example, this user has no Security Test Group clearances. After this, select Update.



Edit Clearance Levels

General Security

☐ Management (Lowest) ☐ Partial View ☐ Executives ☑ Unrestricted View (Highest)

Base

☐ lowest (Lowest) ☑ Management (Highest)

My Classifications

☐ Analysts (Lowest) ☐ Top Secret ☑ Management (Highest)

Security

☑ management (Lowest) (Highest)

Security Test Group

☐ Low Level (Lowest) ☐ Med Level ☐ High Level (Highest)

BA Team

☐ BA Member (Lowest) (Highest)

IA Team

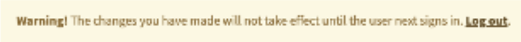
☐ IA Member (Lowest) (Highest)

RA Team

☐ RA Member (Lowest) (Highest)

☐ French Person (Lowest) (Highest)

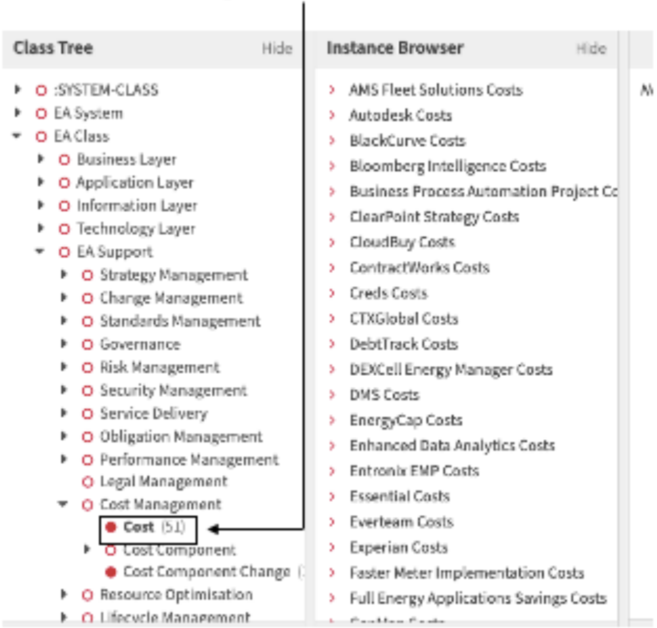
Active



Warning! The changes you have made will not take effect until the user next signs in. Log out.

Note the warning after clicking update. Updates will only be applied when the user next logs in.

8 You can see ‘Cost’, and all the costs of the organisation



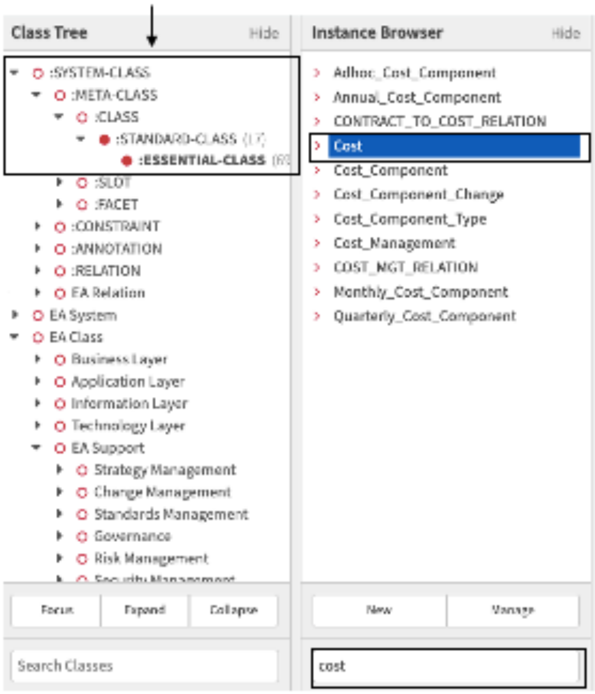
Class Tree Hide

- :SYSTEM-CLASS
- EA System
- EA Class
  - Business Layer
  - Application Layer
  - Information Layer
  - Technology Layer
  - EA Support
    - Strategy Management
    - Change Management
    - Standards Management
    - Governance
    - Risk Management
    - Security Management
    - Service Delivery
    - Obligation Management
    - Performance Management
    - Legal Management
    - Cost Management
      - Cost (51)
      - Cost Component
      - Cost Component Change (
    - Resource Optimisation
    - Lifecycle Management

Instance Browser Hide

- AMS Fleet Solutions Costs
- Autodesk Costs
- BlackCurve Costs
- Bloomberg Intelligence Costs
- Business Process Automation Project Cc
- ClearPoint Strategy Costs
- CloudBuy Costs
- ContractWorks Costs
- Creds Costs
- CTXGlobal Costs
- DebtTrack Costs
- DEXCell Energy Manager Costs
- DMS Costs
- EnergyCap Costs
- Enhanced Data Analytics Costs
- Entronix EMP Costs
- Essential Costs
- Everteam Costs
- Experian Costs
- Faster Meter Implementation Costs
- Full Energy Applications Savings Costs

9 Go to :SYSTEM-CLASS > :META-CLASS > :CLASS > :STANDARD-CLASS > :ESSENTIAL-CLASS.



Class Tree Hide

- :SYSTEM-CLASS
  - :META-CLASS
    - :CLASS
      - :STANDARD-CLASS (17)
        - :ESSENTIAL-CLASS (6
    - :SLOT
    - :FACET
  - :CONSTRAINT
  - :ANNOTATION
  - :RELATION
  - EA Relation
- EA System
- EA Class
  - Business Layer
  - Application Layer
  - Information Layer
  - Technology Layer
  - EA Support
    - Strategy Management
    - Change Management
    - Standards Management
    - Governance
    - Risk Management
    - Security Management

Instance Browser Hide

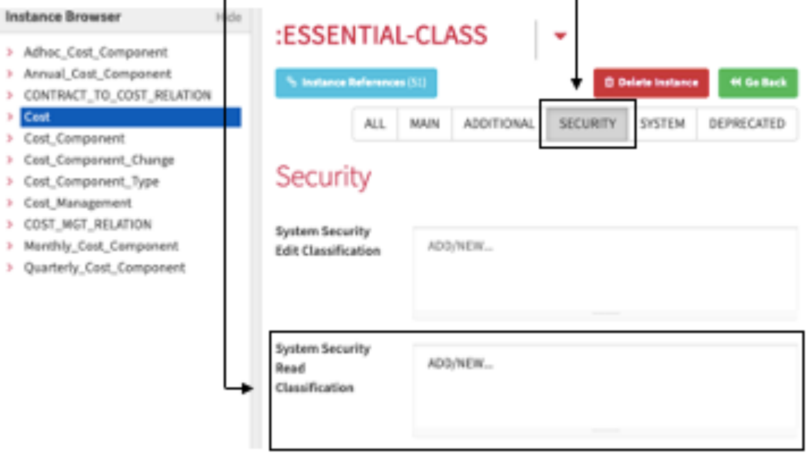
- Adhoc_Cost_Component
- Annual_Cost_Component
- CONTRACT_TO_COST_RELATION
- Cost
- Cost_Component
- Cost_Component_Change
- Cost_Component_Type
- Cost_Management
- COST_MGT_RELATION
- Monthly_Cost_Component
- Quarterly_Cost_Component

cost

11 Select ‘Cost’.

10 Search ‘Cost’ in search bar.

12 In 'Cost', select Security, then ADD/NEW in System Security Read Classification.



Instance Browser Hide

- Adhoc_Cost_Component
- Annual_Cost_Component
- CONTRACT_TO_COST_RELATION
- Cost
- Cost_Component
- Cost_Component_Change
- Cost_Component_Type
- Cost_Management
- COST_MGT_RELATION
- Monthly_Cost_Component
- Quarterly_Cost_Component

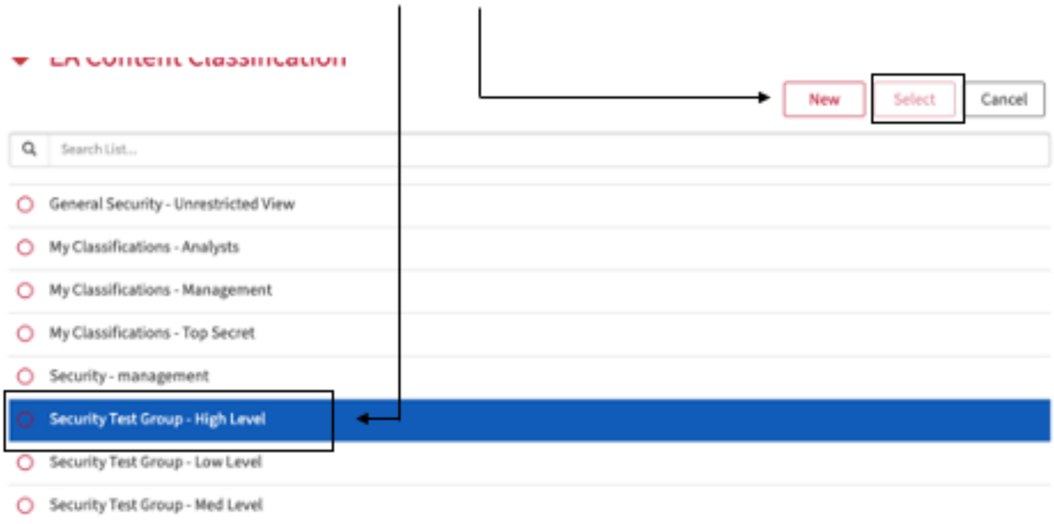
:ESSENTIAL-CLASS

Security

System Security Edit Classification: ADD/NEW...

System Security Read Classification: ADD/NEW...

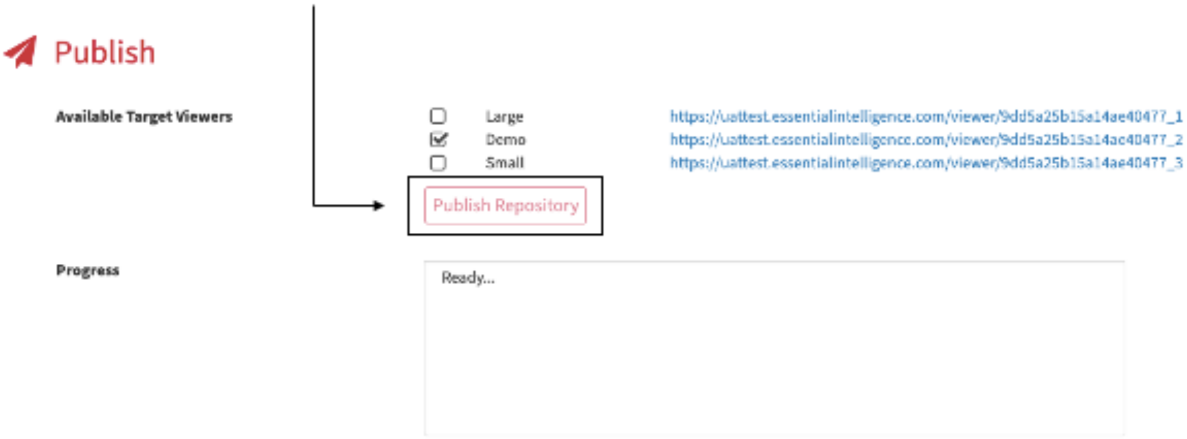
13 Select security level, highest option as the slot is being hidden. Then 'Select'.



EA Content Classification

- ○ General Security - Unrestricted View
- ○ My Classifications - Analysts
- ○ My Classifications - Management
- ○ My Classifications - Top Secret
- ○ Security - management
- ○ Security Test Group - High Level
- ○ Security Test Group - Low Level
- ○ Security Test Group - Med Level

14 Publish the new security classification.



Publish

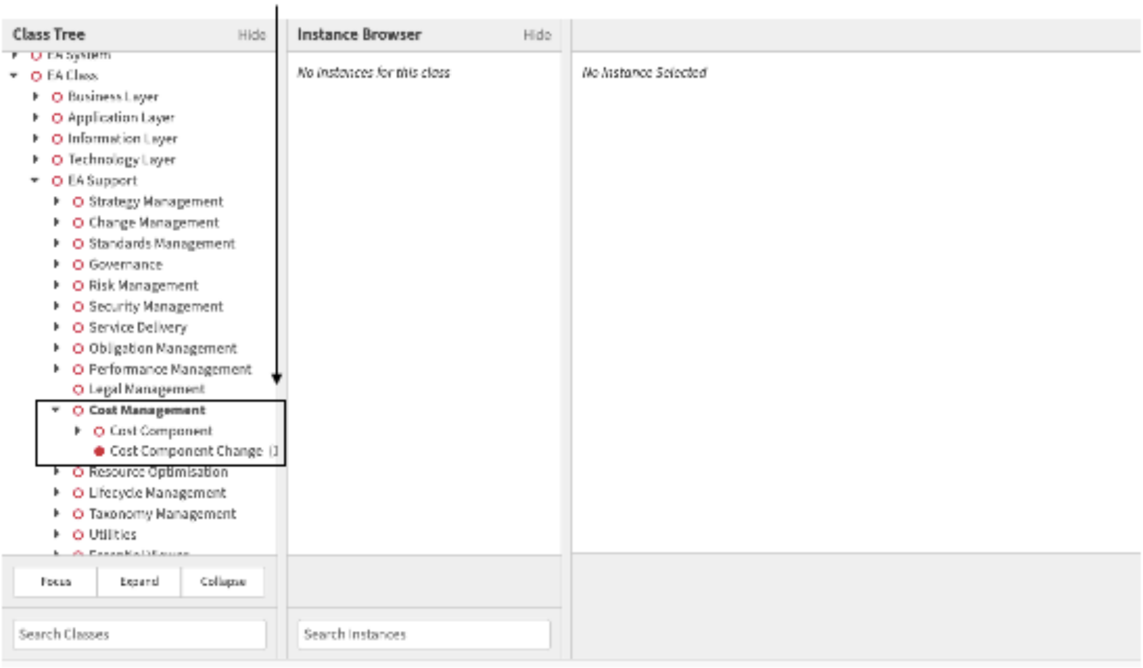
Available Target Viewers

□	Large	https://uattest.essentialintelligence.com/viewer/9dd5a25b15a14ae40477_1
☑	Demo	https://uattest.essentialintelligence.com/viewer/9dd5a25b15a14ae40477_2
□	Small	https://uattest.essentialintelligence.com/viewer/9dd5a25b15a14ae40477_3

Progress

Ready...

15 When the user goes to ‘Cost Management’ in the Class Tree, can no longer see ‘Cost’ and the instances in it.



Class Tree Hide

- EA System
- EA Class
  - Business Layer
  - Application Layer
  - Information Layer
  - Technology Layer
  - EA Support
    - Strategy Management
    - Change Management
    - Standards Management
    - Governance
    - Risk Management
    - Security Management
    - Service Delivery
    - Obligation Management
    - Performance Management
    - Legal Management
    - **Cost Management**
      - Cost Component
      - Cost Component Change (1
    - Resource Optimisation
    - Lifecycle Management
    - Taxonomy Management
    - Utilities
    - Essential Viewer

Focus Expand Collapse

Search Classes

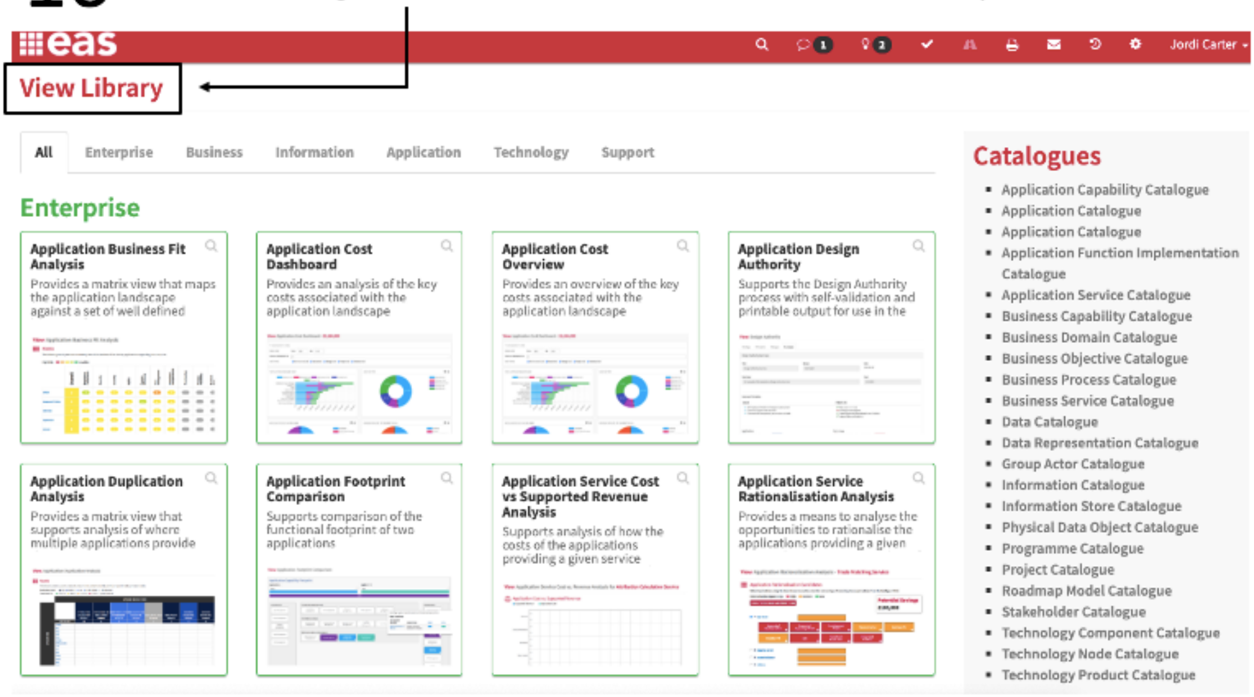
Instance Browser Hide

No instances for this class

Search Instances

No Instance Selected

16 Go to Knowledge Portal from Dashboard and select ‘View Library’.



View Library

All Enterprise Business Information Application Technology Support

Enterprise

Application Business Fit Analysis
Provides a matrix view that maps the application landscape against a set of well defined

Application Cost Dashboard
Provides an analysis of the key costs associated with the application landscape

Application Cost Overview
Provides an overview of the key costs associated with the application landscape

Application Design Authority
Supports the Design Authority process with self-validation and printable output for use in the

Application Duplication Analysis
Provides a matrix view that supports analysis of where multiple applications provide

Application Footprint Comparison
Supports comparison of the functional footprint of two applications

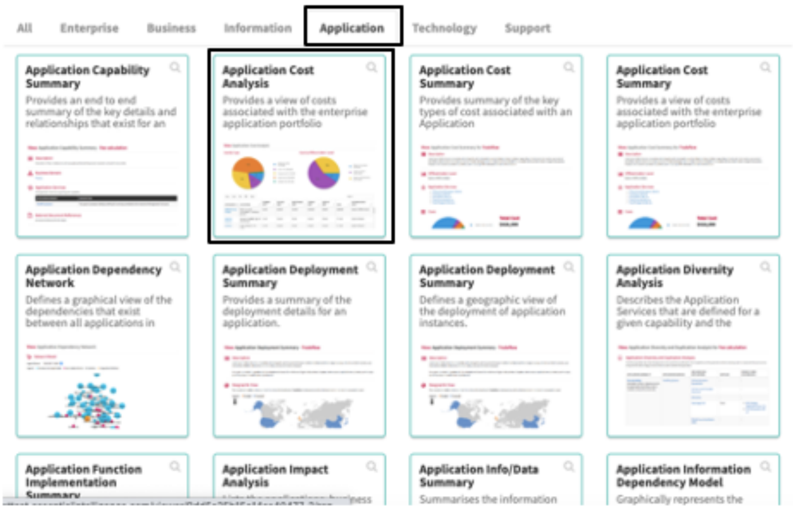
Application Service Cost vs Supported Revenue Analysis
Supports analysis of how the costs of the applications providing a given service

Application Service Rationalisation Analysis
Provides a means to analyse the opportunities to rationalise the applications providing a given

Catalogues

- Application Capability Catalogue
- Application Catalogue
- Application Catalogue
- Application Function Implementation Catalogue
- Application Service Catalogue
- Business Capability Catalogue
- Business Domain Catalogue
- Business Objective Catalogue
- Business Process Catalogue
- Business Service Catalogue
- Data Catalogue
- Data Representation Catalogue
- Group Actor Catalogue
- Information Catalogue
- Information Store Catalogue
- Physical Data Object Catalogue
- Programme Catalogue
- Project Catalogue
- Roadmap Model Catalogue
- Stakeholder Catalogue
- Technology Component Catalogue
- Technology Node Catalogue
- Technology Product Catalogue

17 In the Application section of the View Library, when the user selects ‘Application Cost Analysis’…



Application Capability Summary
Provides an end to end summary of the key details and relationships that exist for an

Application Cost Analysis
Provides a view of costs associated with the enterprise application portfolio

Application Cost Summary
Provides summary of the key types of cost associated with an Application

Application Cost Summary
Provides a view of costs associated with the enterprise application portfolio

Application Dependency Network
Defines a graphical view of the dependencies that exist between all applications in

Application Deployment Summary
Provides a summary of the deployment details for an application.

Application Deployment Summary
Defines a geographic view of the deployment of application instances.

Application Diversity Analysis
Describes the Application Services that are defined for a given capability and the

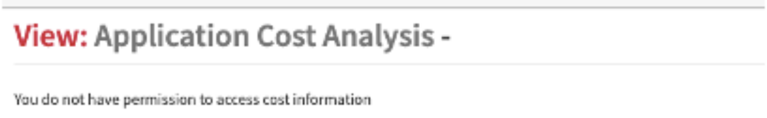
Application Function Implementation Summary

Application Impact Analysis

Application Info/Data Summary
Summarises the information

Application Information Dependency Model
Graphically represents the

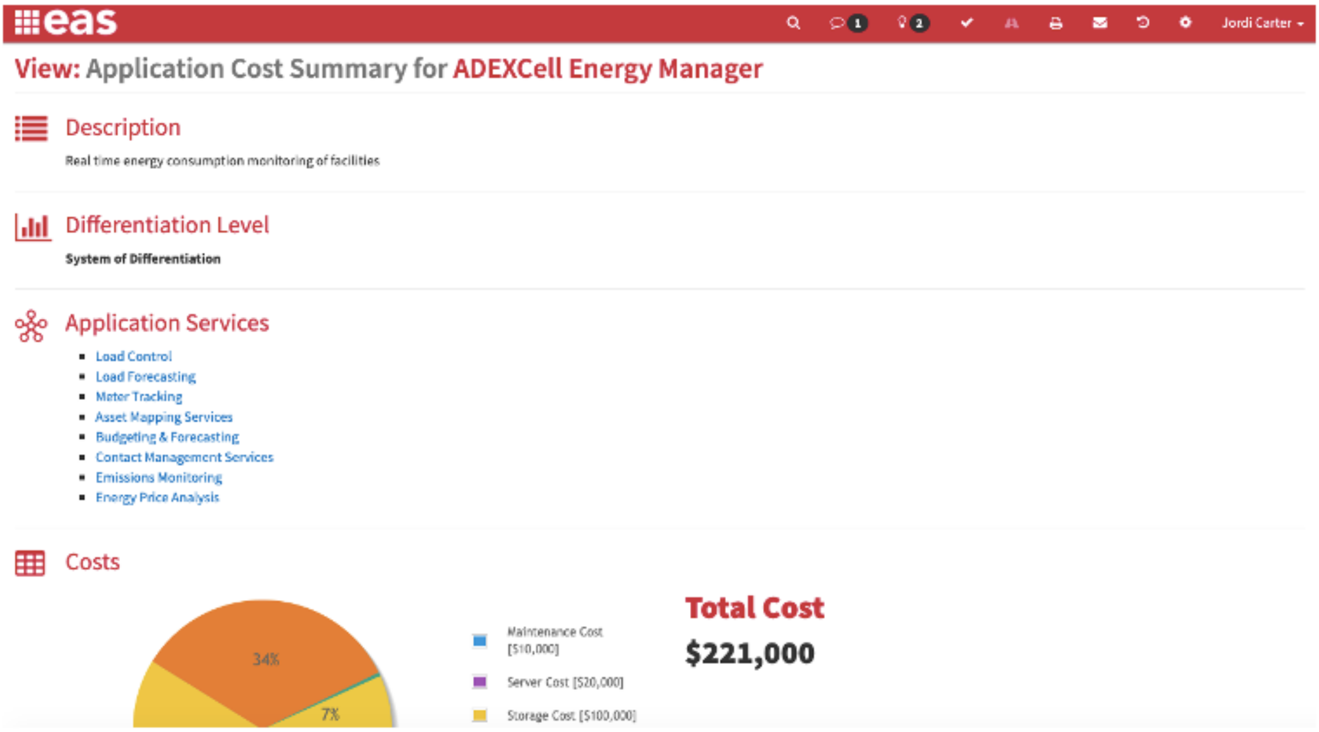
18 …it will take them to this screen.



View: Application Cost Analysis -

You do not have permission to access cost information

19 You can see here that access was blocked to only one of the Cost Analysis viewers.



View: Application Cost Summary for ADEXCell Energy Manager

Description

Real time energy consumption monitoring of facilities

Differentiation Level

System of Differentiation

Application Services

- Load Control
- Load Forecasting
- Meter Tracking
- Asset Mapping Services
- Budgeting & Forecasting
- Contact Management Services
- Emissions Monitoring
- Energy Price Analysis

Costs

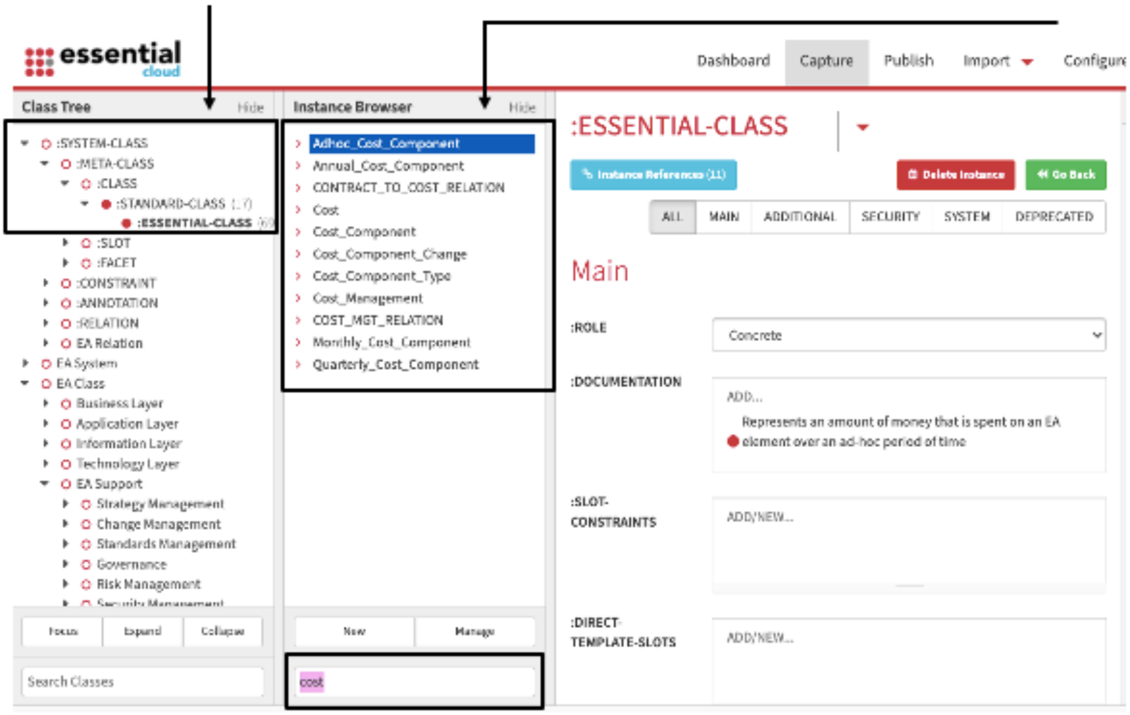
- 🟦 Maintenance Cost [$10,000]
- 🟪 Server Cost [$20,000]
- 🟨 Storage Cost [$100,000]

Total Cost

$221,000

20 Go to :SYSTEM-CLASS > :META-CLASS > :CLASS :STANDARD-CLASS > :ESSENTIAL-CLASS.

21 Return to add security classifications to add each cost individually.



Adhoc_Cost_Component
Annual_Cost_Component
CONTRACT_TO_COST_RELATION
Cost
Cost_Component
Cost_Component_Change
Cost_Component_Type
Cost_Management
COST_MGT_RELATION
Monthly_Cost_Component
Quarterly_Cost_Component

cost

:ESSENTIAL-CLASS

Main

:ROLE Concrete

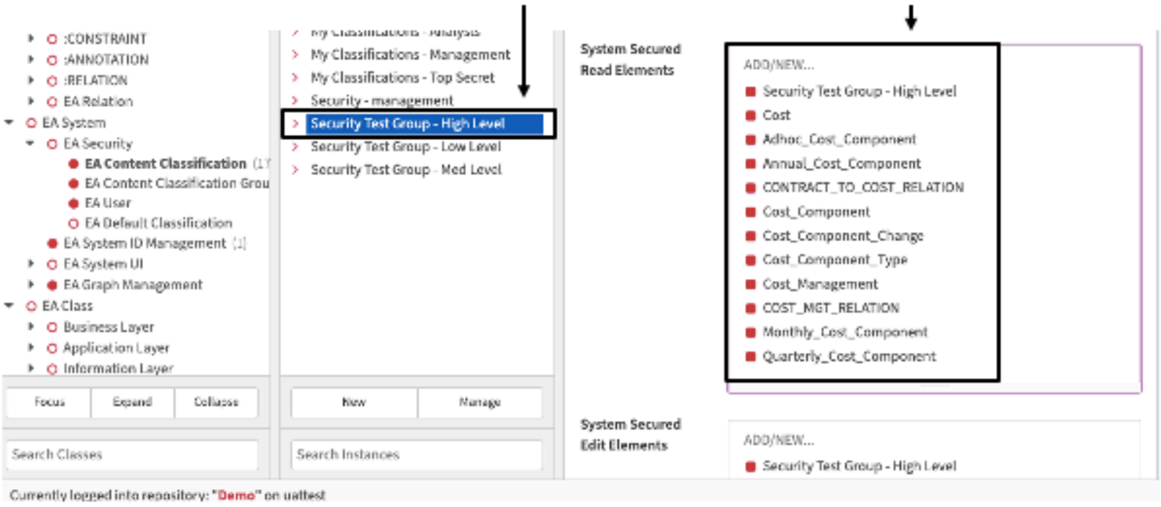
:DOCUMENTATION ADD...
Represents an amount of money that is spent on an EA element over an ad-hoc period of time

:SLOT-CONSTRAINTS ADD/NEW...

:DIRECT-TEMPLATE-SLOTS ADD/NEW...

Use instance browser search bar to view all cost related instances (e.g. “cost”).

22 You can see that all cost related instances have now had the high level security classification applied to them.



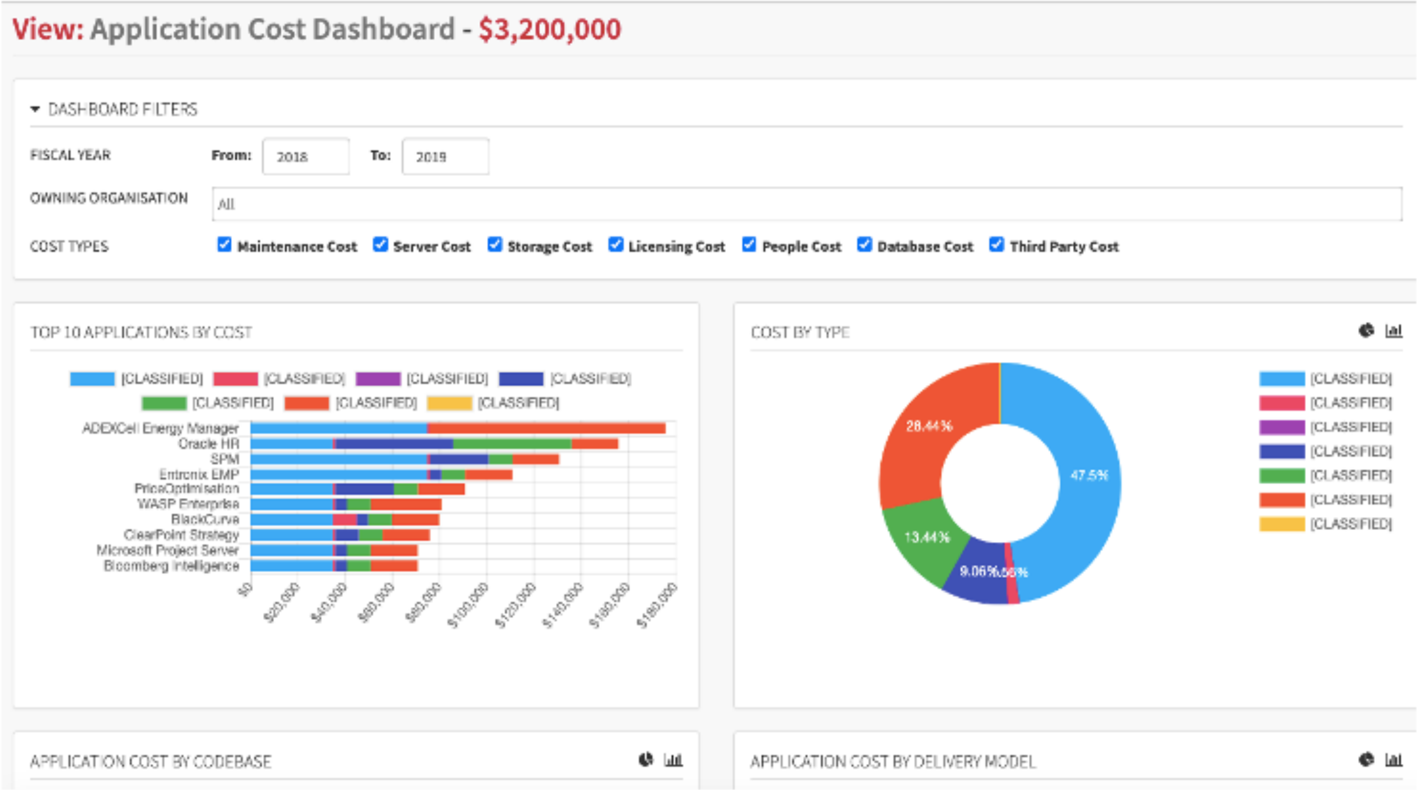
My Classifications - Analysis
My Classifications - Management
My Classifications - Top Secret
Security - management
Security Test Group - High Level
Security Test Group - Low Level
Security Test Group - Med Level

System Secured Read Elements
ADD/NEW...
- Security Test Group - High Level
- Cost
- Adhoc_Cost_Component
- Annual_Cost_Component
- CONTRACT_TO_COST_RELATION
- Cost_Component
- Cost_Component_Change
- Cost_Component_Type
- Cost_Management
- COST_MGT_RELATION
- Monthly_Cost_Component
- Quarterly_Cost_Component

System Secured Edit Elements
ADD/NEW...
- Security Test Group - High Level

Currently logged into repository: "Demo" on uattest

23 Now opening the Dashboard you can see the applications, but actual details of the costs are classified.



View: Application Cost Dashboard - $3,200,000

▾ DASHBOARD FILTERS

FISCAL YEAR **From:** 2018 **To:** 2019

OWNING ORGANISATION All

COST TYPES ☑ **Maintenance Cost** ☑ **Server Cost** ☑ **Storage Cost** ☑ **Licensing Cost** ☑ **People Cost** ☑ **Database Cost** ☑ **Third Party Cost**

TOP 10 APPLICATIONS BY COST

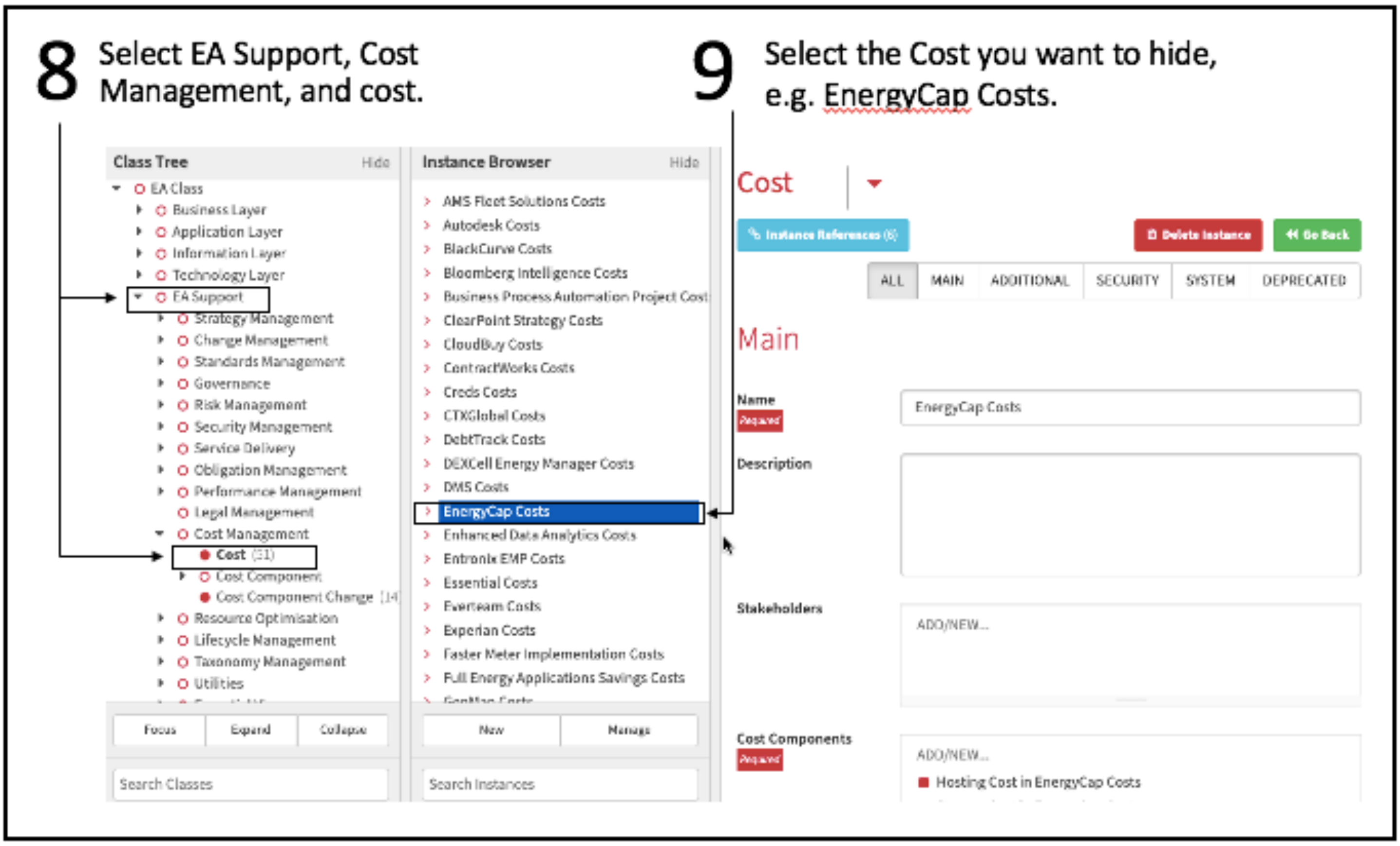
COST BY TYPE

APPLICATION COST BY CODEBASE

APPLICATION COST BY DELIVERY MODEL

Hide a Single Slot

To hide a single slot, follow the instructions up to 7 in 2a, and then follow the steps below:

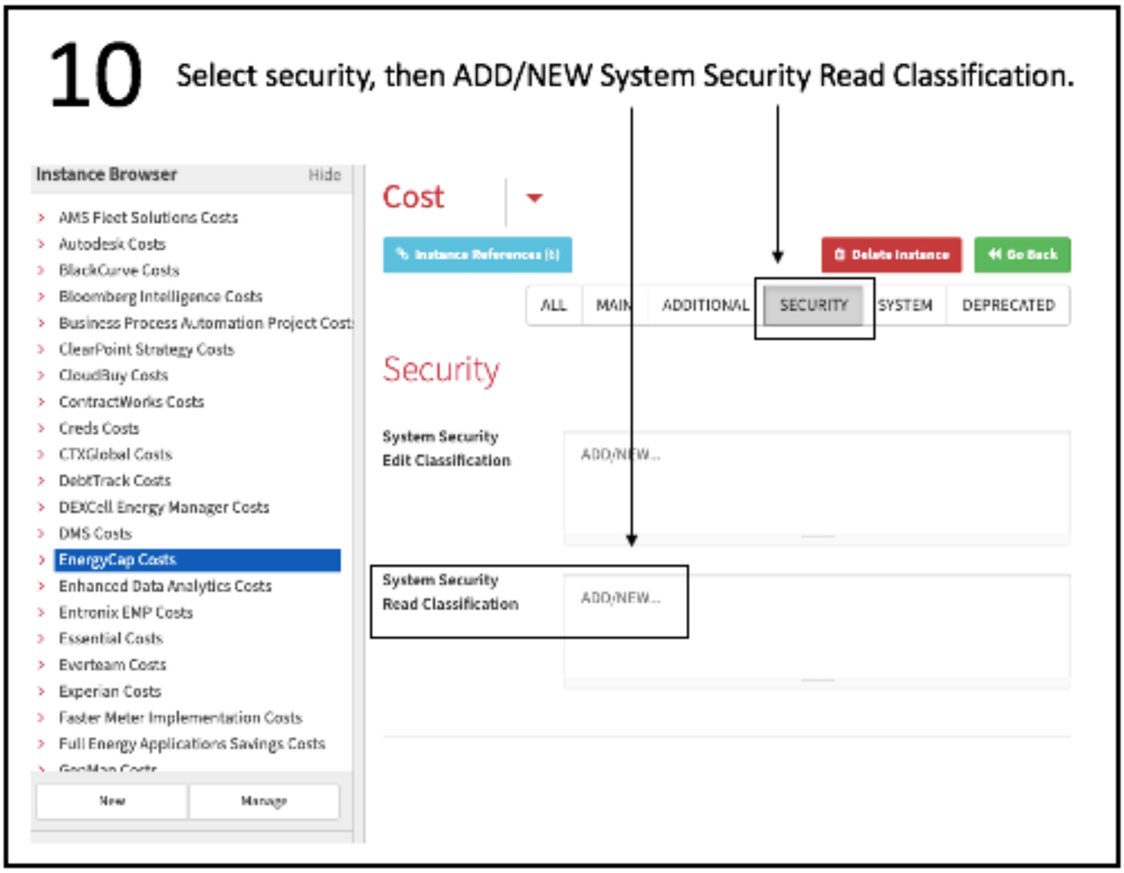


8 Select EA Support, Cost Management, and cost.

9 Select the Cost you want to hide, e.g. EnergyCap Costs.

Name: EnergyCap Costs

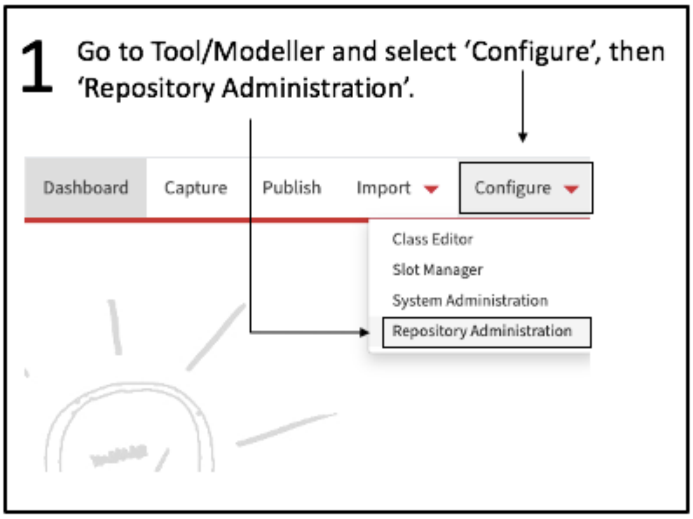
Cost Components: Hosting Cost in EnergyCap Costs



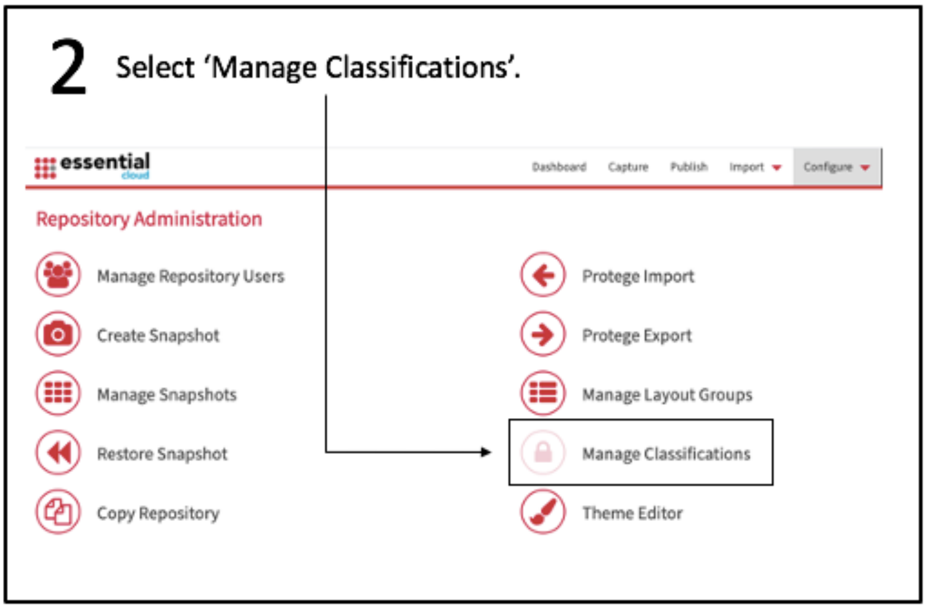
10 Select security, then ADD/NEW System Security Read Classification.

Give a User Access to Only One Layer (e.g., Business Layer)

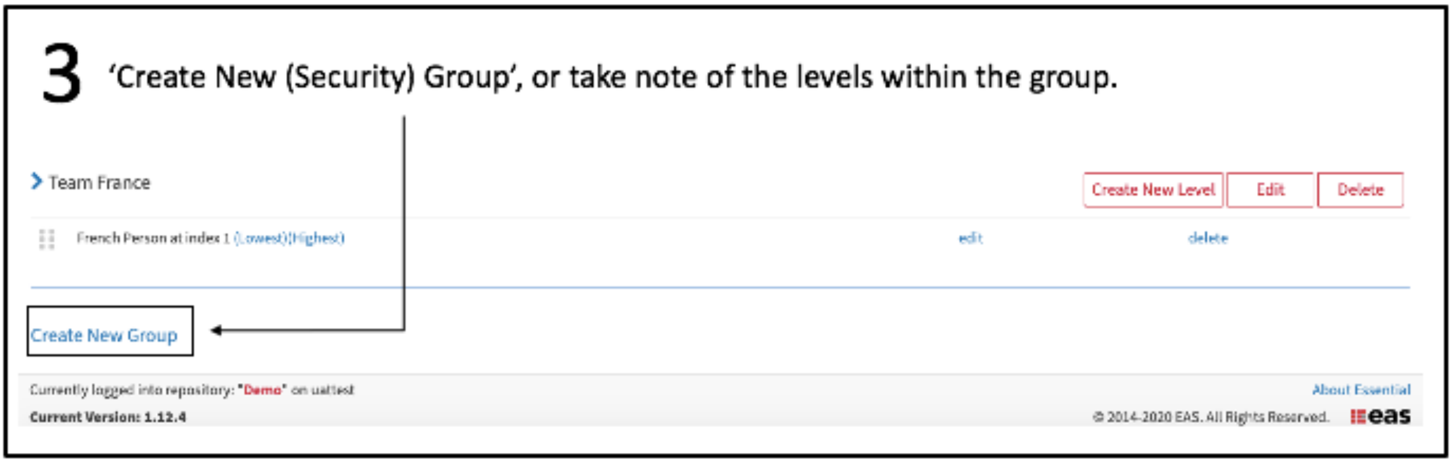
This scenario will show you how to provide access to only one layer (e.g., Business Layer), meaning a user can only see the area they are working on, and other areas of the organisation is kept secret from users without appropriate clearances.



1 Go to Tool/Modeller and select ‘Configure’, then ‘Repository Administration’.



2 Select ‘Manage Classifications’.



3 ‘Create New (Security) Group’, or take note of the levels within the group.

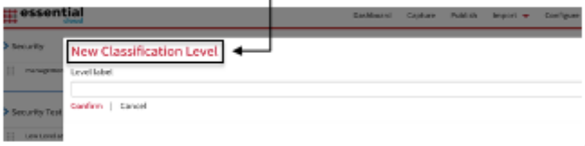
French Person at index 1 (Lowest)(Highest)

Currently logged into repository: "Demo" on ualtest

Current Version: 1.12.4

© 2014-2020 EAS. All Rights Reserved.

If adding New Classification Level, enter Name and confirm.

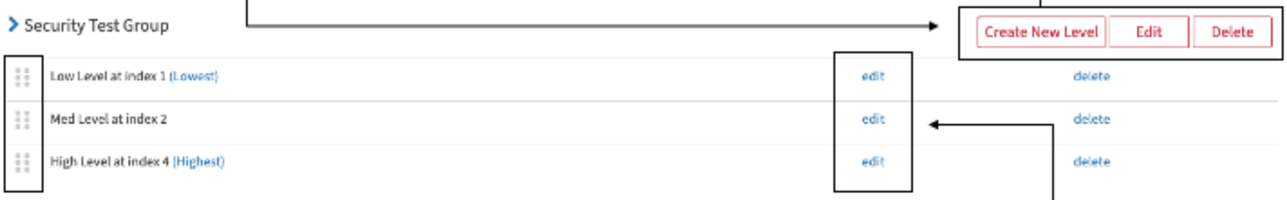


New Classification Level

Level label

Confirm | Cancel

4 Create New Levels, Edit the group name, or Delete the group.



Security Test Group

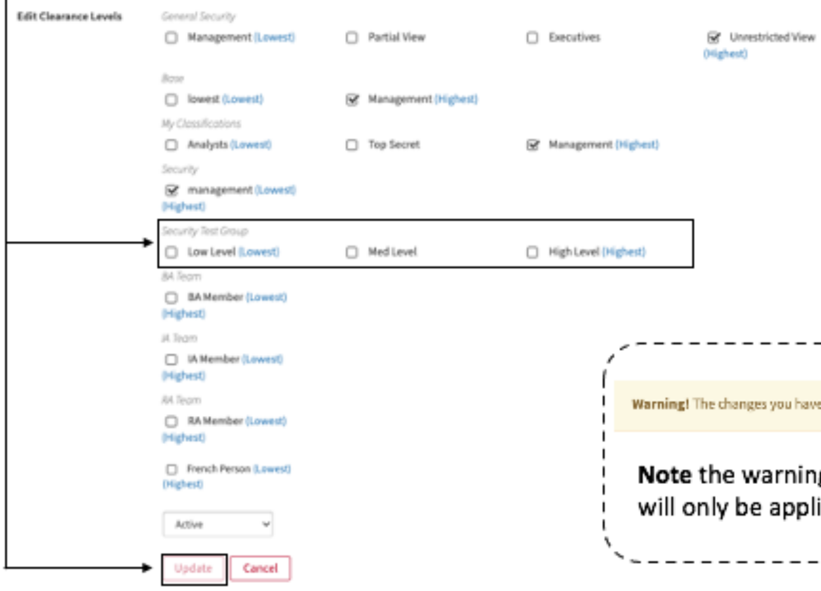
Create New Level | Edit | Delete

Low Level at index 1 (Lowest)	edit	delete
Med Level at index 2	edit	delete
High Level at index 4 (Highest)	edit	delete

6 Change the order of the index by dragging the dots to desired order.

5 'Edit' the level name, or delete it.

7 Next go to Manage Repository Users, select the user(s) you want to make security classification changes to. For the example, this user has no Security Test Group clearances. After this, select Update.



Edit Clearance Levels

General Security
☐ Management (Lowest) ☐ Partial View ☐ Executives ☑ Unrestricted View (Highest)

Base
☐ lowest (Lowest) ☑ Management (Highest)

My Classifications
☐ Analysts (Lowest) ☐ Top Secret ☑ Management (Highest)

Security
☑ management (Lowest) (Highest)

Security Test Group
☐ Low Level (Lowest) ☐ Med Level ☐ High Level (Highest)

BA Team
☐ BA Member (Lowest) (Highest)

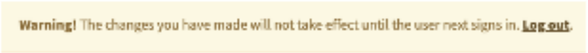
IA Team
☐ IA Member (Lowest) (Highest)

RA Team
☐ RA Member (Lowest) (Highest)

☐ French Person (Lowest) (Highest)

Active

Update Cancel



Warning! The changes you have made will not take effect until the user next signs in. Log out.

Note the warning after clicking update. Updates will only be applied when the user next logs in.

8 Recommended to do this, so now classify everything other than the business layer.

- Classify everything in the repository ***except*** the Business Layer with a specific classification
  - Business Layer has no classifications
  - Do not clear the set of people for this classification
  - No way to classify the Business Layer for other users, e.g. Application Layer users, such that they cannot see it

Recommended approach

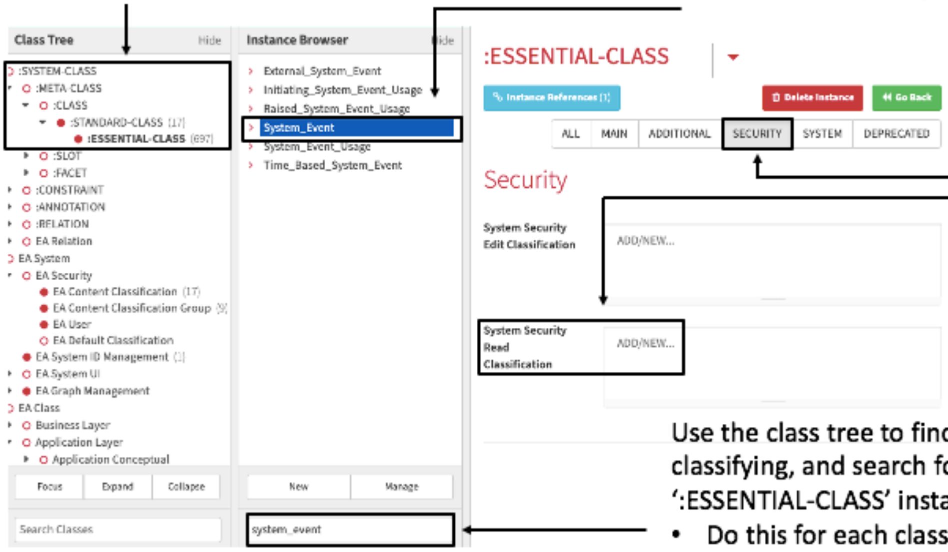
- Classify all **classes** in the repository except the Business Layer classes approach is recommended for this use case

- Current:
  - Build a DUP that makes use of a library script to define the set of "allowed" classes
  - Script performs the following steps
    - Create the new Security Classification Group and Security Classifications in that group
    - Using the library script, classify all classes except those in the meta model tree of the Business Layer class
- Planned:
  - Invoke API to implement the required security

Current best way to select entire layers to be classified, API or build a DUP. Otherwise very time consuming for admin to apply classifications.

9 Go to 1. :SYSTEM-CLASS > :META-CLASS > :CLASS > :STANDARD-CLASS > :ESSENTIAL-CLASS

10 Select the Class that needs classifying.

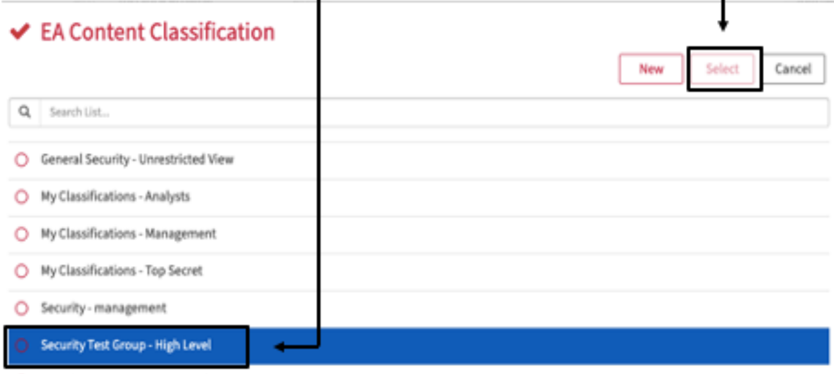


11 Go to security and select ADD/NEW System Security Read Classification.

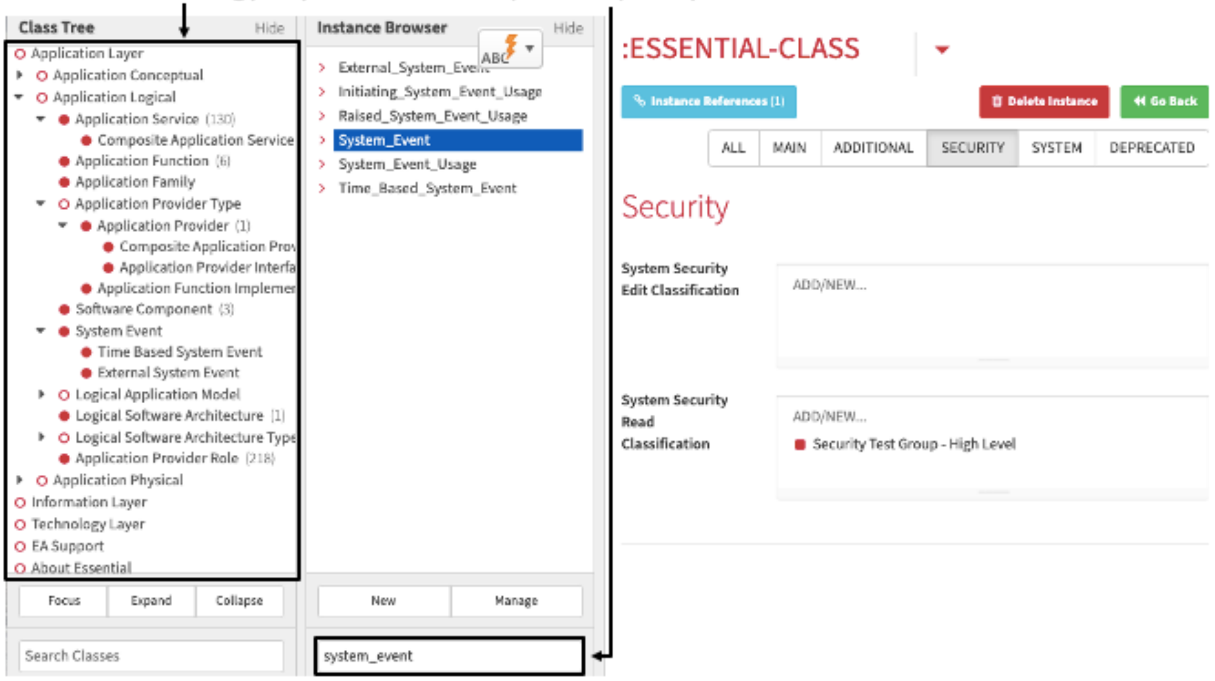
Use the class tree to find which areas need classifying, and search for that class in the ':ESSENTIAL-CLASS' instance browser.

- Do this for each class that needs classifying, then repeat steps 2-4.
- Will need to do this for each class of every layer.

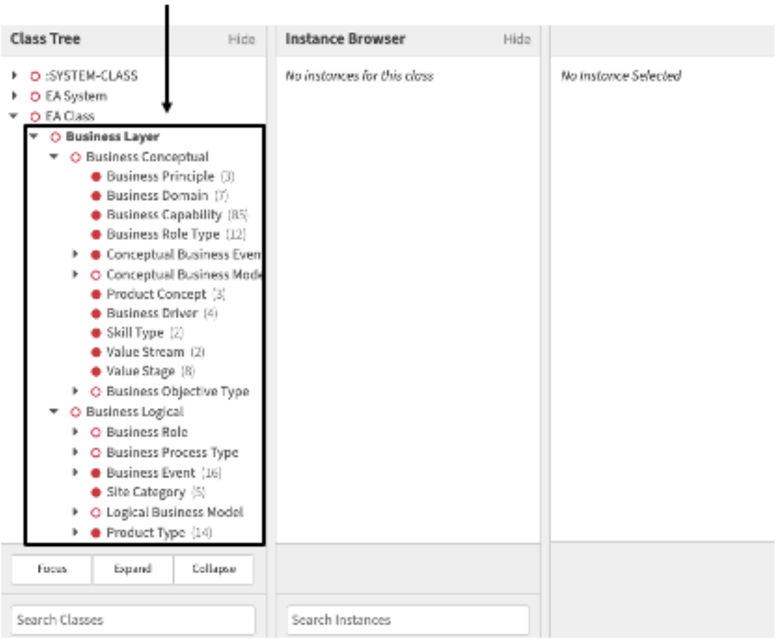
12 Add the desired level of classification.

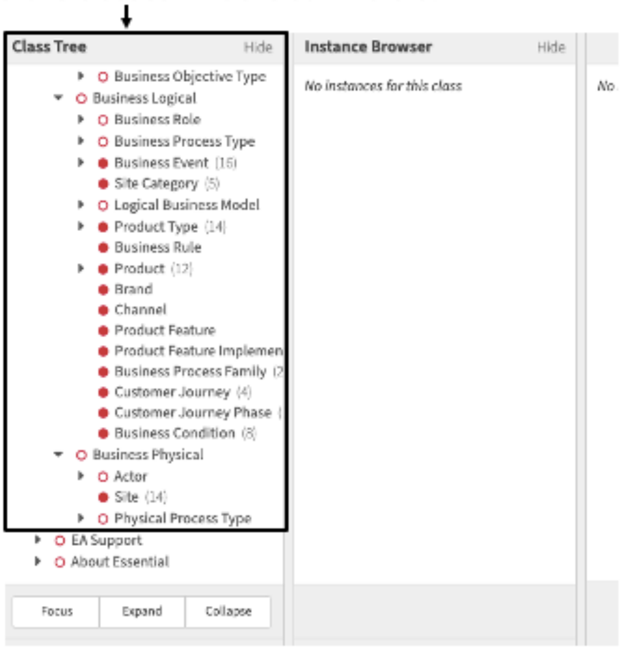

✓ EA Content Classification
New
Select
Cancel
Search List...
General Security - Unrestricted View
My Classifications - Analysts
My Classifications - Management
My Classifications - Top Secret
Security - management
Security Test Group - High Level

13 Use the expanded Class Tree to help when searching for the classes in the instance browser. You will need to do the same for every class in the Information and Technology Layers as well – repeat steps of previous slide to do so.



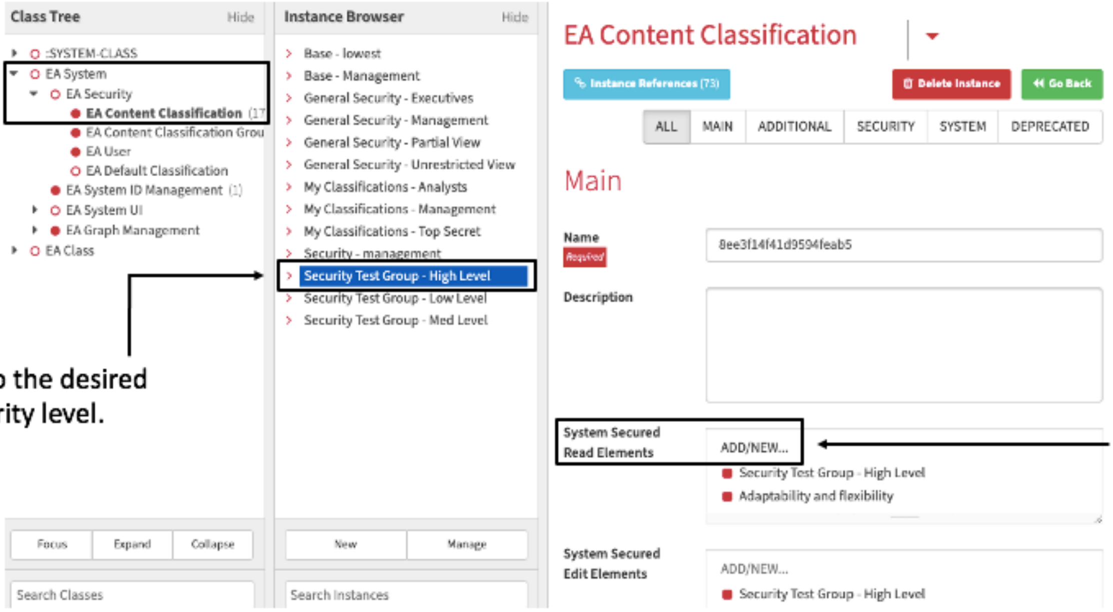
14 Once complete, all layers and classes classified will be invisible to any user without appropriate clearances. In this case, only the Business Layer and the classes in it are still visible.





The next slides will go through the second method of classifying all layers except one – works for leaving specific instances unclassified if that is what is required, otherwise ignore.

Without a DUP or API, there are a number of ways to classify the layers that you want to be.


Class Tree
Hide
:SYSTEM-CLASS
EA System
EA Security
EA Content Classification (17
EA Content Classification Grou
EA User
EA Default Classification
EA System ID Management (1)
EA System UI
EA Graph Management
EA Class
Focus
Expand
Collapse
Search Classes
Instance Browser
Hide
Base - lowest
Base - Management
General Security - Executives
General Security - Management
General Security - Partial View
General Security - Unrestricted View
My Classifications - Analysts
My Classifications - Management
My Classifications - Top Secret
Security - management
Security Test Group - High Level
Security Test Group - Low Level
Security Test Group - Med Level
New
Manage
Search Instances
EA Content Classification
Instance References (73)
Delete Instance
Go Back
ALL
MAIN
ADDITIONAL
SECURITY
SYSTEM
DEPRECATED
Main
Required
ADD/NEW...
ADD/NEW...

Name: 8ee3f14f41d9594feab5

Description:

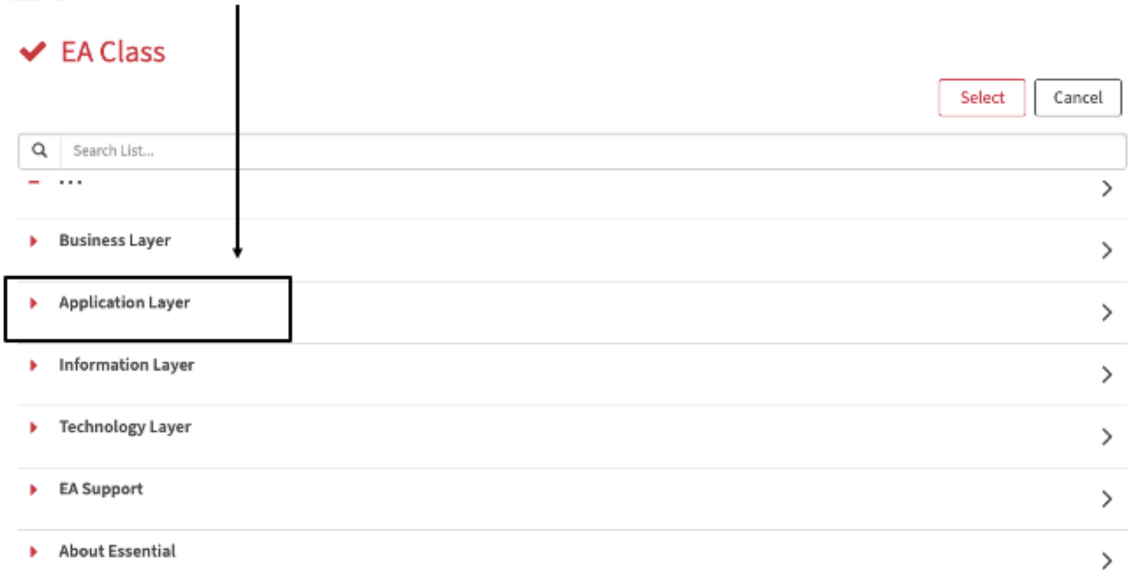
System Secured Read Elements: Security Test Group - High Level; Adaptability and flexibility

System Secured Edit Elements: Security Test Group - High Level

15 Go to the desired security level.

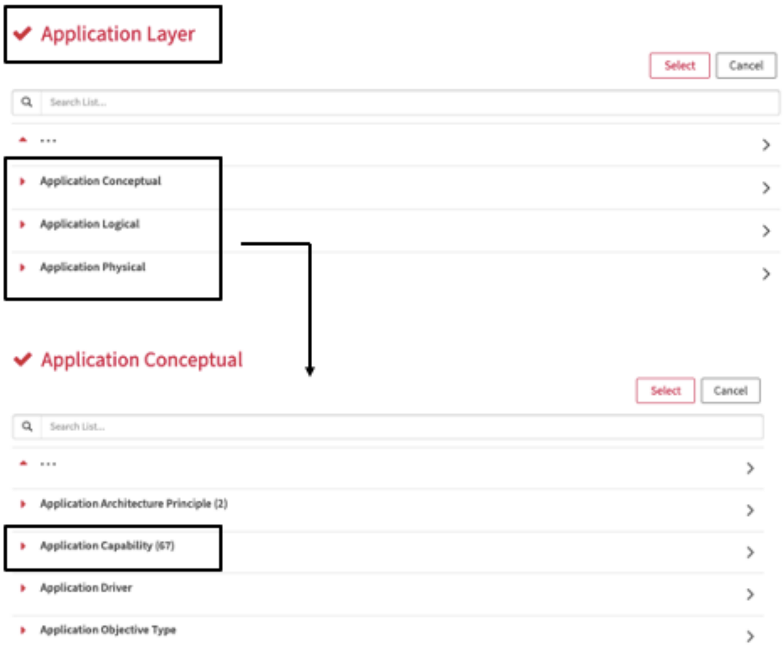
16 ADD/NEW in System Secured Read Elements.

17 Now add classifications to the Layers you want to hide, e.g. Application Layer.



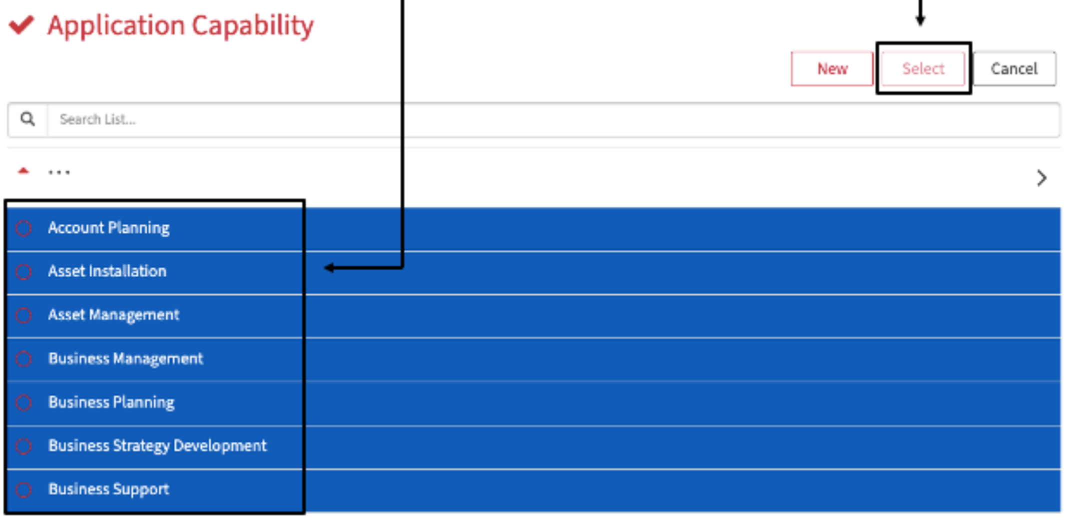
18 Within Application Layer, one after the other enter Conceptual, Physical, and Logical.

19 In each of these select the class to add classifications to. (e.g. Application Capability).
Note that you will need to do this for each class individually i.e. Application Architecture Principle, Application Driver, and Application Objective Type.

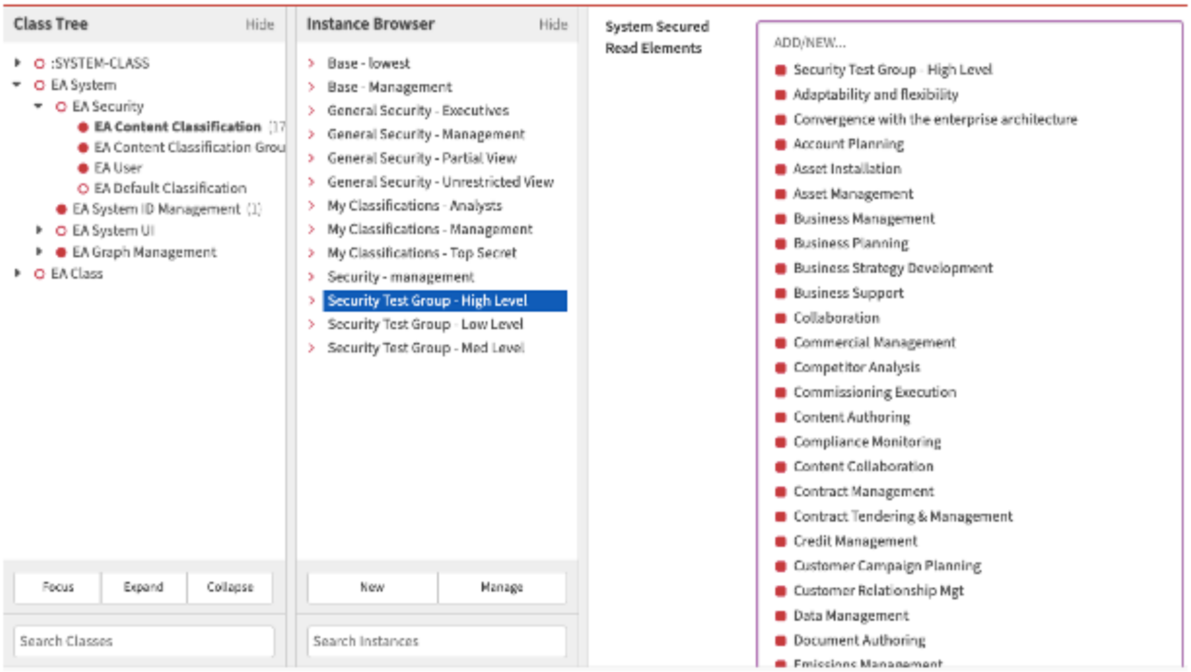


20 As the entire layer is being classified, select all the instances.

21 Then Select once done.



22 The classes/instances now show in Read Elements. Repeat steps 15-21 for every layer that the user is not going to have access to.



Class Tree

- :SYSTEM-CLASS
- EA System
  - EA Security
    - EA Content Classification (17
    - EA Content Classification Grou
    - EA User
    - EA Default Classification
  - EA System ID Management (1)
  - EA System UI
  - EA Graph Management
- EA Class

Instance Browser

- Base - lowest
- Base - Management
- General Security - Executives
- General Security - Management
- General Security - Partial View
- General Security - Unrestricted View
- My Classifications - Analysts
- My Classifications - Management
- My Classifications - Top Secret
- Security - management
- Security Test Group - High Level
- Security Test Group - Low Level
- Security Test Group - Med Level

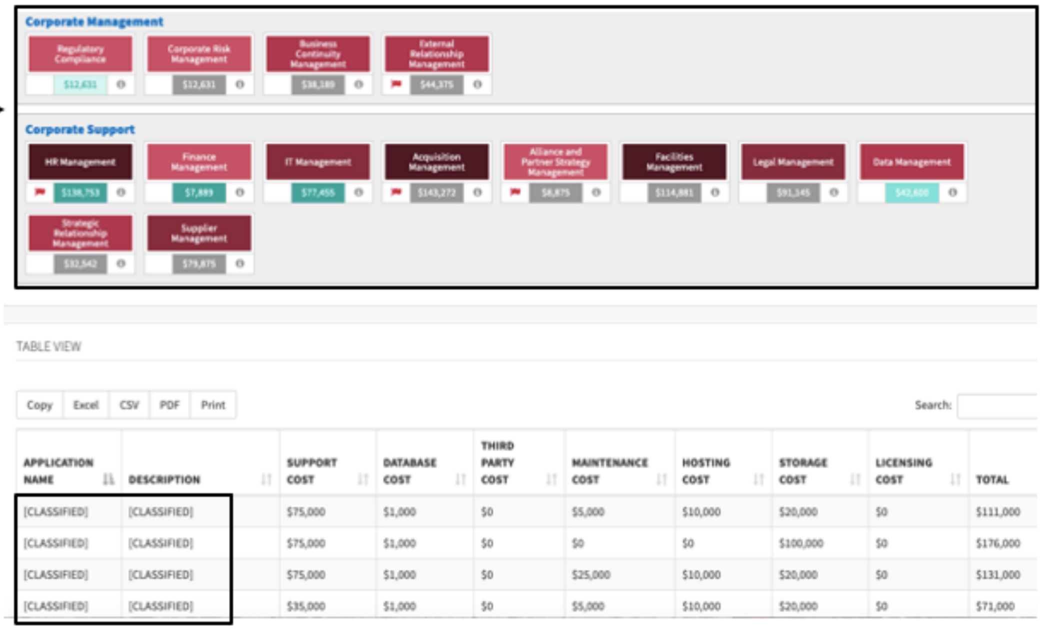
System Secured Read Elements

- Security Test Group - High Level
- Adaptability and flexibility
- Convergence with the enterprise architecture
- Account Planning
- Asset Installation
- Asset Management
- Business Management
- Business Planning
- Business Strategy Development
- Business Support
- Collaboration
- Commercial Management
- Competitor Analysis
- Commissioning Execution
- Content Authoring
- Compliance Monitoring
- Content Collaboration
- Contract Management
- Contract Tendering & Management
- Credit Management
- Customer Campaign Planning
- Customer Relationship Mgt
- Data Management
- Document Authoring
- Emissions Management

23 After either of these methods have been completed, only anything related to the (e.g. Business) layer will be accessible to a user without clearances to view more. Users will still be able to view areas that are related to multiple instances, but anything unrelated to the (e.g. Business) layer will not be accessible/viewable.

You can see in this view that business capabilities are still visible.

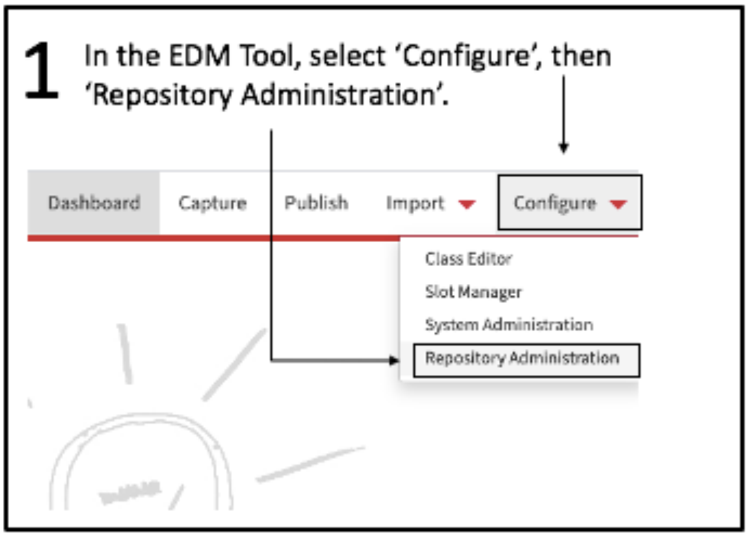
The applications (unrelated to anything in the business layer) are now classified.



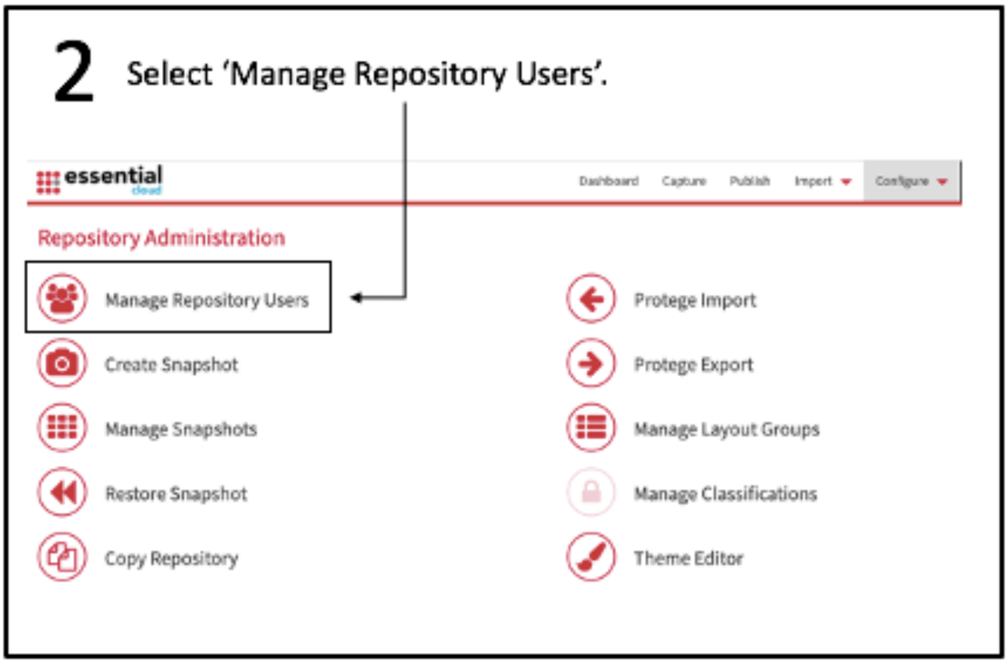
APPLICATION NAME	DESCRIPTION	SUPPORT COST	DATABASE COST	THIRD PARTY COST	MAINTENANCE COST	HOSTING COST	STORAGE COST	LICENSING COST	TOTAL
[CLASSIFIED]	[CLASSIFIED]	$75,000	$1,000	$0	$5,000	$10,000	$20,000	$0	$111,000
[CLASSIFIED]	[CLASSIFIED]	$75,000	$1,000	$0	$0	$0	$100,000	$0	$176,000
[CLASSIFIED]	[CLASSIFIED]	$75,000	$1,000	$0	$25,000	$10,000	$20,000	$0	$131,000
[CLASSIFIED]	[CLASSIFIED]	$35,000	$1,000	$0	$5,000	$10,000	$20,000	$0	$71,000

Changing Clearances for Multiple Users at Once

This scenario will show you how to change the clearances of multiple users at once, rather than having to give each one individual access, you can add/remove clearance from one user to as many as all of them, customisable to your specification.



1 In the EDM Tool, select 'Configure', then 'Repository Administration'.

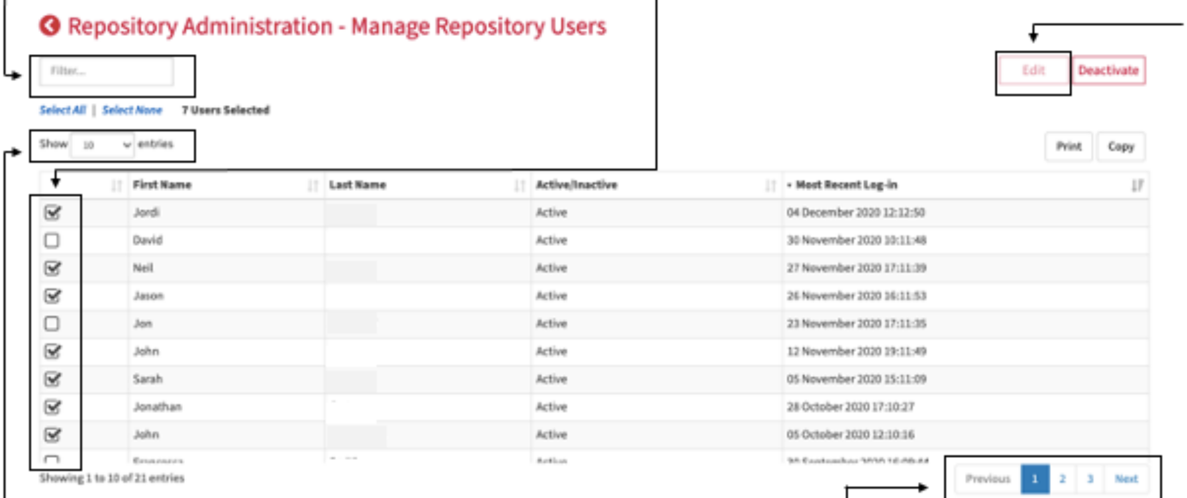


2 Select 'Manage Repository Users'.

Use filter to search for specific users, and select All/None if required.

3 Select all the users you want to change account roles and edit & read clearances for.

4 Once all desired users have been selected, select edit.



Repository Administration - Manage Repository Users

Select All | Select None 7 Users Selected

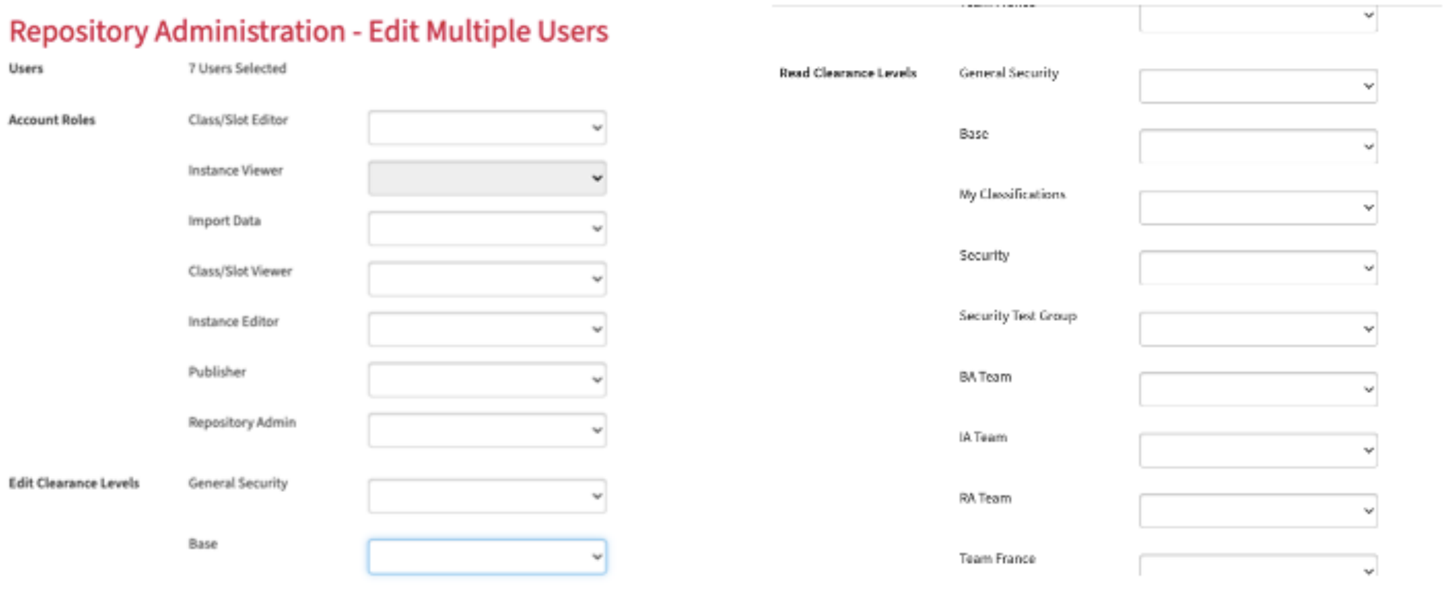
Show 10 entries

	First Name	Last Name	Active/Inactive	Most Recent Log-in
☑	Jordi		Active	04 December 2020 12:12:50
□	David		Active	30 November 2020 10:11:48
☑	Neil		Active	27 November 2020 17:11:39
☑	Jason		Active	26 November 2020 16:11:53
□	Jon		Active	23 November 2020 17:11:35
☑	John		Active	12 November 2020 19:11:49
☑	Sarah		Active	05 November 2020 15:11:09
☑	Jonathan		Active	28 October 2020 17:10:27
☑	John		Active	05 October 2020 12:10:16

Showing 1 to 10 of 21 entries

Navigate pages of users, also increase/decrease the number of users per page.

5 You can now edit all of the selected user's account roles, their edit clearance levels, and their read clearance levels.



Repository Administration - Edit Multiple Users

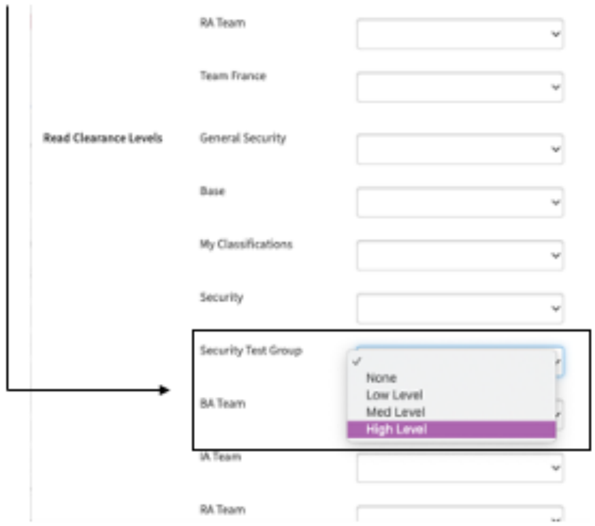
Users 7 Users Selected

Account Roles
- Class/Slot Editor
- Instance Viewer
- Import Data
- Class/Slot Viewer
- Instance Editor
- Publisher
- Repository Admin

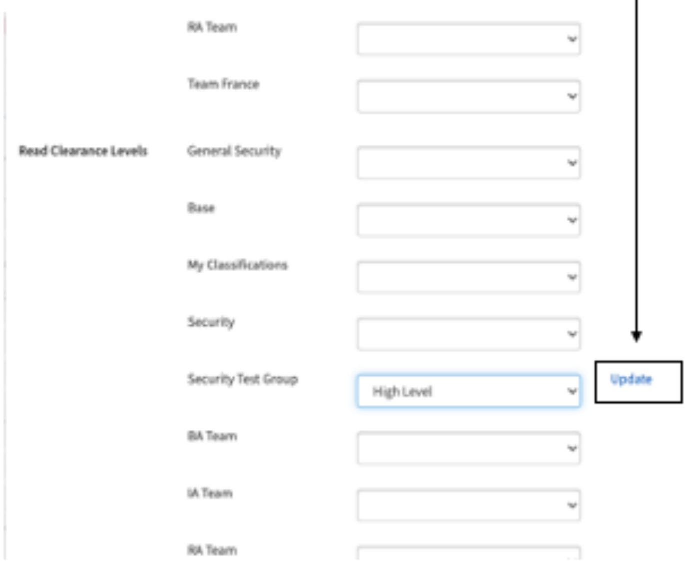
Edit Clearance Levels
- General Security
- Base

Read Clearance Levels
- General Security
- Base
- My Classifications
- Security
- Security Test Group
- BA Team
- IA Team
- RA Team
- Team France

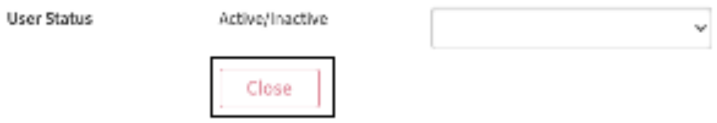
6 Add/remove the desired security clearance(s). E.g. Read Clearance: Security Test Group – High Level.



7 Once added/removed, select update.



8 When all changes have been made and updated, select close.



Security Clearances and Classification Summaries

Set a Default Classification

- This scenario allows you to set a default classification for all users in the repository that it's applied to. Once applied, only users with matching or higher security clearance than the default will be able to access every class and instance that the default has been applied to.

Hiding a portal

- This scenario demonstrates how to hide a portal from a user, portals can define which views that the users see. E.g., hiding the entire data management portal will restrict access to that portal, but not strictly to the views within it, which will have to be classified separately if they are going to be hidden from all portals, they can be accessed from.

Hiding a view

- This scenario will show you how to hide a view (report) from a user. Simple process that will demonstrate how to hide a view from a user, hiding a certain view if there is one aspect you want to hide from a user. (e.g., IT Asset Dashboard) will mean the user cannot get an overview of the IT assets, but can still access other, more specific views involving these assets.

Hiding an instance

- This scenario will take you through hiding an instance from a user. Once applied the instance will be hidden from all users that don't have the security clearances. E.g., Can hide Equipment Management as a capability from the user and can apply to any capability that needs to be hidden.

Hiding a class

- This scenario shows how to hide a class from a user. Areas of each layer can be split so that a user can only access certain aspects of that layer. E.g., Classify the entire Business Conceptual class, but allow other aspects of the business layer to still be visible, i.e. business logical and physical, as well as catalogues such as business services catalogue.

Hiding a set of classes

- This scenario allows you to hide a set of classes from a user, providing a quicker method of hiding multiple classes at once rather than having to apply classifications to different classes individually.

Hide a slot

- This scenario will take you through how to hide a slot from a user. Adding classifications to slots will hide certain aspects of the organisation from the user (e.g. costs) in order to protect that information, but still allow a user to view things related to those costs, e.g. the applications being used still visible, but not the cost of those applications

Changing clearances for multiple users at once

- This scenario involves changing the clearances of multiple users at once, rather than having to give each one individual access, you can add/remove clearance from one user to as many as all of them, customisable to your specification.

Give a user access to one layer

- This scenario will show you how to provide access to only one layer (e.g., Business Layer), meaning a user can only see the area they are working on, and other areas of the organisation is kept secret from the users without appropriate clearances.

Give a user access to certain reports/views

- This scenario will allow you to make only certain reports/views accessible to a user depending on what you want them to be able to see. Instead of hiding each view individually, this will help to speed up that process and hide as many as you need to all at once.