CA GREEN BOOKS

CA Clarity™ PPM

Implementing Security in CA Clarity™ PPM

- EXPLORE THE CA CLARITY PPM SECURITY MODEL
- USE CASES AND EXAMPLES

technologies

LEGAL NOTICE

This publication is based on current information and resource allocations as of its date of publication and is subject to change or withdrawal by CA at any time without notice. The information in this publication could include typographical errors or technical inaccuracies. CA may make modifications to any CA product, software program, method or procedure described in this publication at any time without notice.

Any reference in this publication to non-CA products and non-CA websites are provided for convenience only and shall not serve as CA's endorsement of such products or websites. Your use of such products, websites, and any information regarding such products or any materials provided with such products or at such websites shall be at your own risk.

Notwithstanding anything in this publication to the contrary, this publication shall not (i) constitute product documentation or specifications under any existing or future written license agreement or services agreement relating to any CA software product, or be subject to any warranty set forth in any such written agreement; (ii) serve to affect the rights and/or obligations of CA or its licensees under any existing or future written license agreement or services agreement relating to any CA software product; or (iii) serve to amend any product documentation or specifications for any CA software product. The development, release and timing of any features or functionality described in this publication remain at CA's sole discretion.

The information in this publication is based upon CA's experiences with the referenced software products in a variety of development and customer environments. Past performance of the software products in such development and customer environments is not indicative of the future performance of such software products in identical, similar or different environments. CA does not warrant that the software products will operate as specifically set forth in this publication. CA will support only the referenced products in accordance with (i) the documentation and specifications provided with the referenced product, and (ii) CA's then-current maintenance and support policy for the referenced product.

Certain information in this publication may outline CA's general product direction. All information in this publication is for your informational purposes only and may not be incorporated into any contract. CA assumes no responsibility for the accuracy or completeness of the information. To the extent permitted by applicable law, CA provides this document "AS IS" without warranty of any kind, including, without limitation, any implied warranties of merchantability, fitness for a particular purpose, or non-infringement. In no event will CA be liable for any loss or damage, direct or indirect, from the use of this document, including, without limitation, lost profits, lost investment, business interruption, goodwill or lost data, even if CA is expressly advised of the possibility of such damages.

COPYRIGHT LICENSE AND NOTICE

This publication may contain sample application programming code and/or language which illustrate programming techniques on various operating systems. Notwithstanding anything to the contrary contained in this publication, such sample code does not constitute licensed products or software under any CA license or services agreement. You may copy, modify and use this sample code for the purposes of performing the installation methods and routines described in this document. These samples have not been tested. CA does not make, and you may not rely on, any promise, express or implied, of reliability, serviceability or function of the sample code.

TITLE AND PUBLICATION DATE:

CA Clarity™ PPM: Implementing Security for CA Clarity PPM

Publication Date: March 31, 2011

ACKNOWLEDGEMENTS

Principal Authors

Alexandre M. Assis

The principal authors and CA Technologies would like to thank the following contributors:

- CA Services
- Development
- Engineering Services
- Marketing
- QA
- Support
- Technical Sales
- Technical Information

CA PRODUCT REFERENCES

This document references the following CA Technologies products:

- CA Clarity™ PPM
- CA Clarity™ PPM for IT Governance
- CA Clarity™ PPM for Professional Services
- CA Clarity™ PPM for New Product Development
- CA Clarity™ PPM for US Federal Government
- CA Clarity™ PPM On Demand

FEEDBACK

Please email us at greenbooks@ca.com to share your feedback on this publication. Please include the title of this publication in the subject of your email response. For technical assistance with a CA Technologies product, please contact CA Support at http://ca.com/support. For assistance with support specific to Japanese operating systems, please contact CA Technologies at http://www.casupport.jp.

PREFACE

CA Clarity™ PPM offers a flexible security model – suited for securing both the CA Clarity PPM application and its data. CA Clarity PPM security implementations are simple or complex, depending on how you design them. It is challenging to put everything together in the form of a security model, and to design a solution to solve specific security requirements.

The objective of this publication is to provide practical information about the available options for configuring data security for the CA Clarity PPM solution. The guide provides knowledge to help security administrators plan the security requirements and implement the solution successfully.

This document is based on research, product testing and information exchanges between the author and other CA Technologies experts. The best practices and knowledge provided in this document have been used in many implementations throughout the CA Technologies customer base.

Contents

Chapter 1: Introduction

Who Should Read This Book?

This book has been written to help CA Technologies customers, partners, and implementers understand how to implement security in CA Clarity PPM.

This book has been written using CA Clarity PPM 12.0.6 as its base. Not all of the content may apply to previous CA Clarity PPM releases. It is reviewed considering the CA Clarity PPM 12.1.0.

Plan for Implementation

Securing your CA Clarity PPM application may be challenging depending on your specific requirements. We recommend that you complete the following planning steps before starting to create Groups and assigning access rights:

1. Understand the CA Clarity PPM security model.
2. Plan how to secure your CA Clarity PPM implementation.
3. Determine how to apply security options, based on your requirements.
4. Implement security for your CA Clarity PPM solution.

When these steps are complete, you are ready to create resources, groups, OBS (Organization Breakdown Structure) Units and grant the necessary access rights.

This document provides information and guidance to assist you in the planning and implementation process. The different elements involved in the CA Clarity PPM security model are identified and the relationships between the elements are defined. Building on that knowledge, the possible options for granting access rights are explored. Use cases and examples of implementing security and granting access are provided for your reference.

Application Security and Data Security

Security in CA Clarity PPM has two aspects: securing the application and securing its data. Although the security mechanism is the same for both, and you can control security for both in the same way using one operation, as a good practice consider them separately – with the objective of fully understanding what configuration is required and realizing how to implement it.

Note: The partitions are not used for security. They are used to define page look and content. For more information about partitions, see the *CA Clarity PPM Studio Developers Guide*.

Application Security

Application Security is used to verify that the correct users have access to the appropriate application functionality. You define Application Security when you want to limit access to what a user can do. When you implement Application Security, you are delimiting actions.

Examples of Application Security:

- Granting resources in a Director job function with View access to a portlet.
- Granting resources in an Executive job function with View access to a Dashboard Page.
- Granting resources in a Project Manager job function with access to create Projects.
- Granting resources in a Resource Manager job function with access to book their direct reports to projects.
- Granting resources in a Human Resource job function with access to edit Department information.
- Granting resources in a Systems Administrator job function with access to run Reports or Jobs.

Data Security

Data Security helps verify that resources have access only to the assigned data. You are considering in terms of Data Security when you say one of the following:

- Everybody should be able to see this page, but only for the assigned projects.
- All project team members should be able to publish documents, but only for their projects.
- All resource managers must hard book and soft book resources, but only for those resources they directly manage.

In other words, when you consider Data Security you are limiting access to a scope of data.

Examples of Data Security

- Granting resources View access to the Projects for Business Unit IT page, but not to the Projects for Business Unit Finance page.
- Granting resources Edit access to the information about the ABC Implementation project, but not to information for another project at the same tree level under the same OBS.
- Granting resources View access to the Applications of Department Development portlet, but not to the Applications of Department Financial portlet.
- Granting resources View access to the resources in Resource Pool Enterprise Architects page, but not to the Resource Pool Support Engineers page.

A complete security model addresses both aspects: securing the application functionalities and securing the data that the application functionalities provide.

How CA Clarity PPM Handles Application and Data Security

This document explains how CA Clarity PPM handles both aspects of security: application and data security. Understanding these key concepts is important for implementing CA Clarity PPM security functionality successfully. Access rights are provided to resources on data scope to help ensure security.

Access Rights

Using Access Rights, you can manage security in CA Clarity PPM both at the application level and the data level. The Access Rights correspond to specific application functionality, such as Editing Projects, Viewing Portlets or Running Jobs. The Access Rights are granted to resources within a data scope, using the following methods:

- Directly to individual resources
- Indirectly, through OBS Units
- Indirectly, through Groups

Data Scope

The Data Scope is one of the following:

Instance

Refers to a single data unit, such as a specific Project, Application, Asset, or Resource, and so on.

OBS Unit

Refers to the instances of an object (Projects, Applications, and so on) associated with that OBS Unit.

Global

Refers to all the instances of an object (all Projects or all Applications or All Resources, and so on). Some of the access rights names display the All expression such as in Project – Approve All.

Granting Access Rights

You can use following two methods to grant access rights in CA Clarity PPM

- From within a Resource, Group or OBS Unit, you can indicate to which Object (page, portlet, etc.) Instance. Access is granted.
- From within an Instance (project, resource, and so on), you can indicate which Resources, Groups, or OBS Units have access to particular instance.

Chapter 2: Security Elements

Introduction to Security Elements

The CA Clarity PPM security model is based on a flexible mechanism that allows you to define both Application and Data security.

Application Security

Refers to specific actions that resources are allowed to do, or defines *Who does What*.

Data Security

Refers to data that resources are allowed access to, or defines *Who accesses Which Data*.

A complete security mechanism should take into consideration both, joining Application Security and Data Security into a single thought: resources that can perform action on specific data. In other words, you define **who** does **what** to **which data**.

Key Elements

Three key elements apply every time you implement or change security in CA Clarity PPM.

Actors

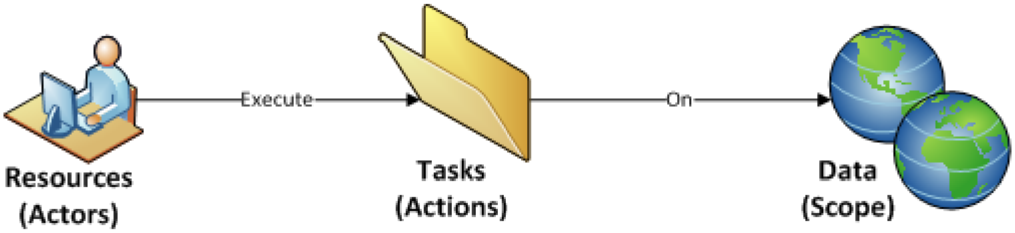
Refers to the resources that are granted or getting access rights.

Actions

Refers to the action or access right that is granted to the resource. What can the resource do when the access is granted?

Scope

Refers to the data related to the action access right. Which data will the resource be able to access?



Security is commonly viewed as two dimensional (granting something to someone). When planning security for CA Clarity PPM, it is important to realize that these two dimensions are not enough to define the security model. We recommend considering these security elements in three dimensions: the Actors, the Actions, and the Data Scope.

Defining and understanding the different possibilities for working with these elements is the basis for designing CA Clarity PPM security.

Defining Actors

Actors are granted access enabling them to execute specific tasks such as:

- View a project
- Edit a resource
- Create an idea
- Execute a report

All Actors belong to one of the following categories:

Resource

Refers to an individual resource.

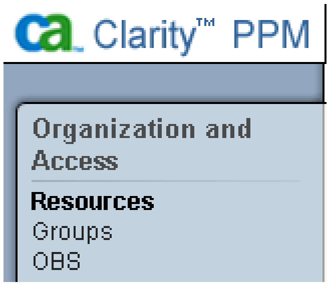
Group

Refers to the collection of resources that are members of a Group.

OBS Unit

Refers to the collection of resources who are members of a Unit in an OBS.

You can find your Actors in the Administration tool menu, under Organization and Access.



Granting Access to Resources

We do not recommend granting access directly to resources. Employees may move from one company department to another by choice, or by department reorganization. New employees may join a company while others may leave after some time. Granting access directly to individual employees may be time consuming and can become confusing if the resource population frequently changes.

We recommend granting access rights to members of Groups or OBS Units to simplify the maintenance for these changes. We recommend that you reserve granting access directly to resources only for specific cases such as a circumstance requiring access to highly sensitive or confidential data.

For some cases, CA Clarity PPM is designed to automatically grant certain access rights to an individual resource. The resource requires the access to perform the basic tasks of the assigned role. For example, when you make a resource the Project Manager in a project, CA Clarity PPM automatically grants that resource the Project - Manager (Auto) access right for that particular project.

Granting Access to Groups

Granting access through Groups is a commonly used approach. If you have many individuals that require the same access rights to the same objects or functions, using Groups simplifies the maintenance from a security perspective.

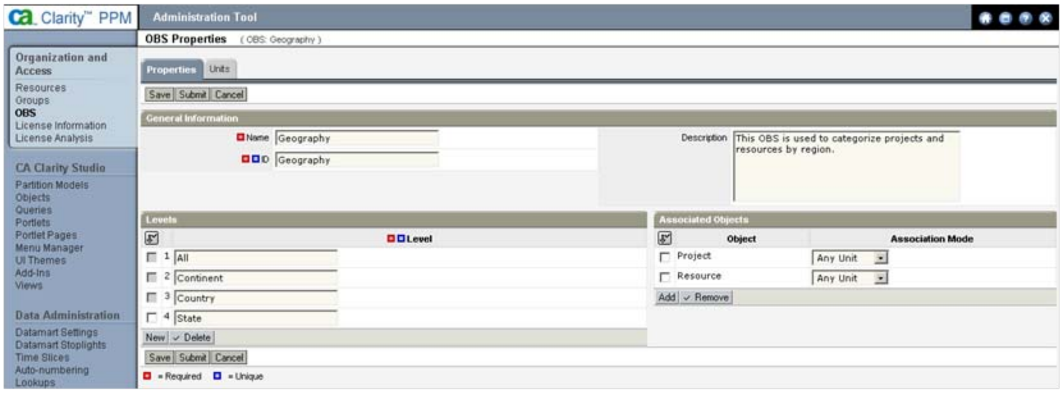
The same benefit is realized if you create a Group with special access rights that may contain only one individual at a time. You simplify the maintenance by assigning the special access to the Group and adding or removing resources in the Group as required. Repeatedly recreating or removing special access rights to individual resources as they shift in and out of a function or job role is more time consuming.

Groups are used for single-level grouping of resources. Examples of groups are Project Managers, Application Managers, Project Participants, Top Level Executives, and PMO.

Using OBS Units as Actors

The Organizational Breakdown Structure (OBS) is a tree-like form of categorizing CA Clarity PPM data. An OBS has one or more top-level nodes and can have up to ten levels. In this topic we refer to the OBS Unit as the *Actor*, or the *Who* portion of the security model. This relates to granting access to actions and objects for the OBS Unit members (the resources related to that OBS Unit).

The following screenshot illustrates an example OBS.



OBS Properties (OBS: Geography)

General Information

Name: Geography

ID: Geography

Description: This OBS is used to categorize projects and resources by region.

Levels

	Level
1	All
2	Continent
3	Country
4	State

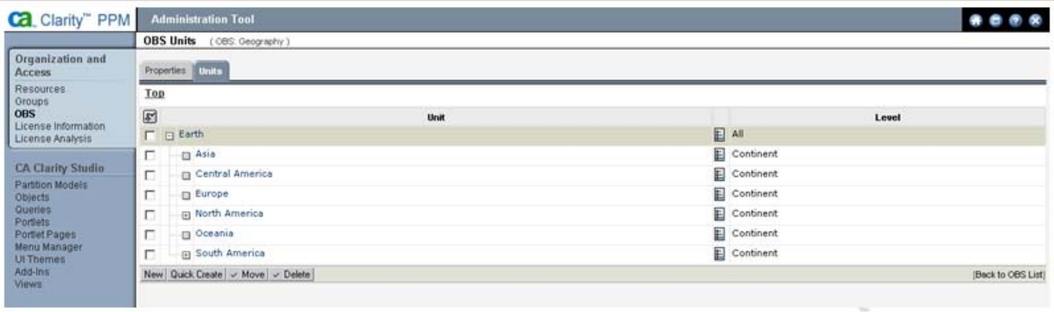
Associated Objects

Object	Association Mode
Project	Any Unit
Resource	Any Unit

🟥 = Required 🟦 = Unique

The OBS structure named Geography has four levels: All, Continent, Country, and State. The structure is used to categorize two CA Clarity PPM objects: Resource and Project. In this example, Earth is an OBS Unit in the OBS structure Geography.

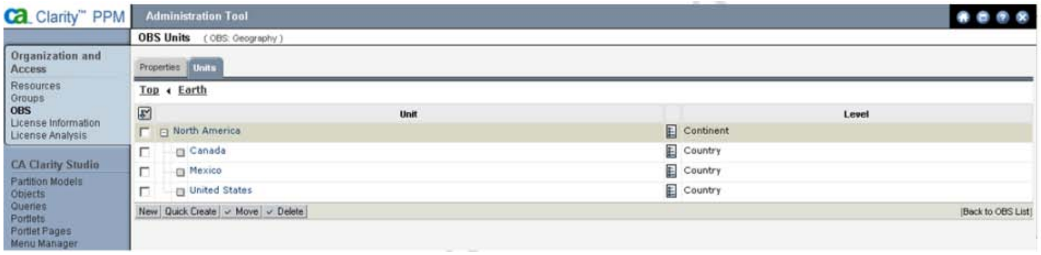
The next illustration shows the Top-Level node Earth with its children: Asia, Central America, Europe, North America, Oceania and South America, defined at the level of Continent.



OBS Units (OBS: Geography)

Unit	Level
Earth	All
Asia	Continent
Central America	Continent
Europe	Continent
North America	Continent
Oceania	Continent
South America	Continent

In a tree structure, you can have more nodes at lower levels. Clicking North America (Continent level) displays the next level below (Country) containing: Canada, Mexico, and United States.



OBS Units (OBS: Geography)

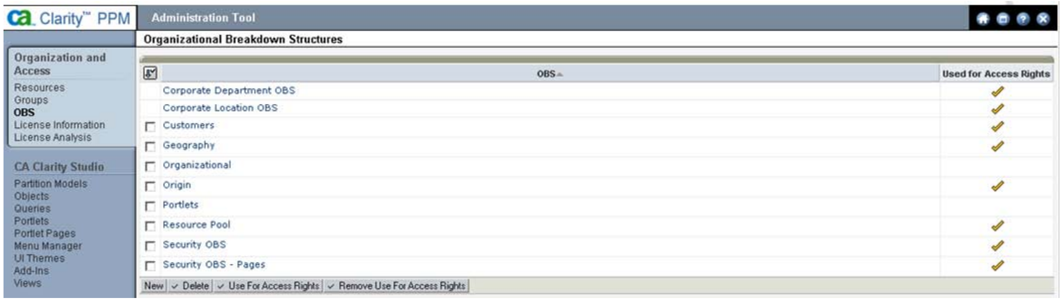
Top ◂ Earth

	Unit	Level
□	⊟ North America	Continent
□	⊡ Canada	Country
□	⊡ Mexico	Country
□	⊡ United States	Country

This tree-like structure makes the OBS useful for security, because you can grant access to Units at any level, to the ancestors (higher level nodes), and the descendants (lower-level nodes).

- You can grant access to a project for the resources related to the Earth unit. As a result, only resources related directly to the Earth unit have access to the project. The resources related to North America or Brazil (defined under South America) are not granted access.
- You can grant access to a project for resources related to the Earth unit and all its descendants, which means, everyone in the defined Continents, County and State levels under Earth have access.
- You can grant access to a project for people related to the North America unit and all its descendants. As a result, people related to North America (the unit itself) and Mexico (a descendant) are granted access to the project. People related to the top–level unit Earth or to the unit Argentina under the unit South America do not have access.
- You can grant access to a project for people related to the South America unit, all its ancestors and descendants. All people related directly to Earth (the ancestor), South America (the unit), and Brazil (a descendent) are granted access. Resources related to Mexico are related to a different branch, and therefore are not granted access.

To use an OBS for security purposes, set it as *Used for Access Rights*.



Organizational Breakdown Structures

	OBS	Used for Access Rights
	Corporate Department OBS	✓
	Corporate Location OBS	✓
□	Customers	✓
□	Geography	✓
□	Organizational	
□	Origin	✓
□	Portlets	
□	Resource Pool	✓
□	Security OBS	✓
□	Security OBS - Pages	✓

Defining Actions

Actions are represented in CA Clarity PPM as Access Rights. Access Rights are the different tasks or actions that the Actors perform on data. Each CA Clarity PPM object has its own set of Access Rights. Some of these Access Rights are specific to that functionality of the object, especially for stock objects; other Access Rights are generic.

Usually, most objects have at least a set of Access Rights similar to the following:

<Object> - Create

Refers to the access right to allow resources to create instances of that object. Examples are: Project – Create, Application – Create, Product – Create.

<Object> - Edit

Refers to the access right to allow resources to edit instances of that object. Examples are: Project – Edit, Department – Edit, Resource – Edit.

<Object> - Navigate

Refers to the access right to allow resources to navigate to the pages of an object. Examples are: Asset – Navigate, Ideas – Navigate, Location – Navigate.

<Object> - View

Refers to the access right to allow resources to view instances of that object. Examples are: Department – View, Service – View, Resource – View.

<Object> - XOG Access

Refers to the access right for importing and exporting the instances of an object using XOG. Examples are: Project – XOG Access, Application – XOG Access, Service – XOG Access.

Custom Objects Access Rights

CA Clarity PPM Studio allows you to create Objects. It does a number of tasks for you automatically when you create Objects. One of those tasks is creating Access Rights, specific to the new object. For example, create an object Strategic Goal.

Example: Create an Object using CA Clarity PPM Studio

1. Click Objects from the CA Clarity PPM Studio menu.

   The Objects page appears.

2. Click New.

   The Create Object Definition page appears.

3. Complete the following, and click Save and Exit:

   Object Name

   Define a name for the object, such as Strategic Goal.

   Object ID

   Enter a unique ID for the new object,

   Description

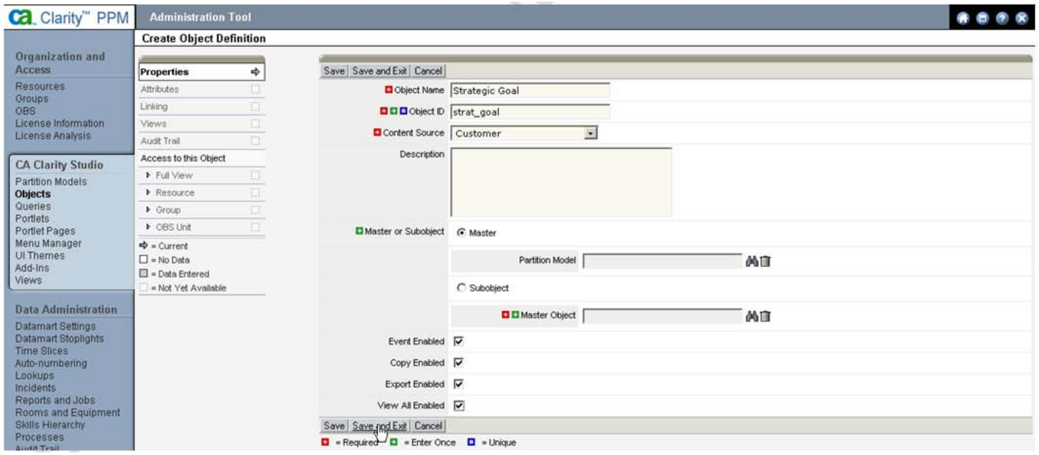
   Enter a brief description for the new object.

   Master or Sub object

   Select the type of object you are creating, such as Master object.

Note: For information about optional steps used when creating an Object, see the *CA Clarity PPM Studio Developer Guide*.

The following illustrates the example definitions:

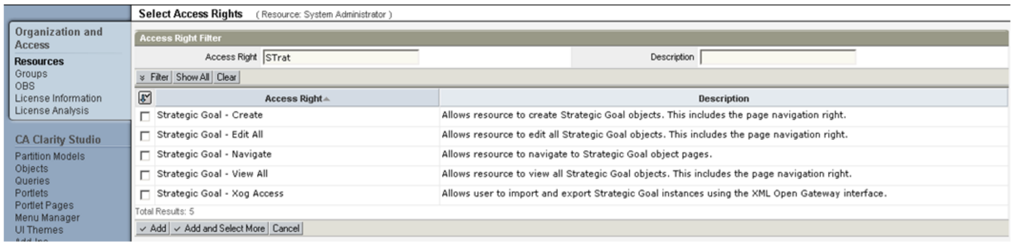


Create Object Definition

Object Name: Strategic Goal
Object ID: strat_goal
Content Source: Customer
Description:
Master or Subobject: ● Master
Partition Model:
○ Subobject
Master Object:
Event Enabled ☑
Copy Enabled ☑
Export Enabled ☑
View All Enabled ☑

🟥 = Required 🟩 = Enter Once 🟦 = Unique

The following screenshots illustrates the Access Rights available for selection for this object.



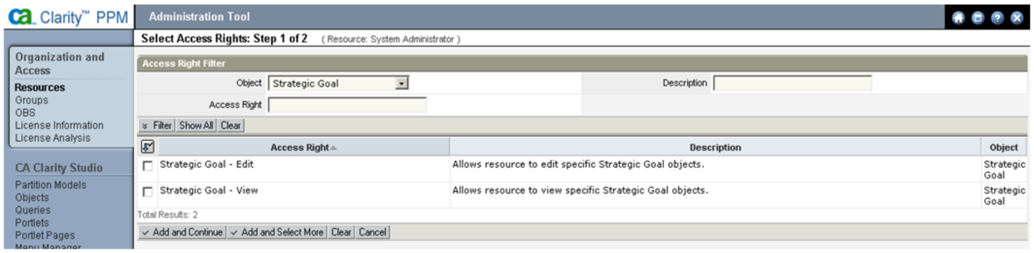
Select Access Rights (Resource: System Administrator)

Access Right: STrat
Description:

	Access Right	Description
□	Strategic Goal - Create	Allows resource to create Strategic Goal objects. This includes the page navigation right.
□	Strategic Goal - Edit All	Allows resource to edit all Strategic Goal objects. This includes the page navigation right.
□	Strategic Goal - Navigate	Allows resource to navigate to Strategic Goal object pages.
□	Strategic Goal - View All	Allows resource to view all Strategic Goal objects. This includes the page navigation right.
□	Strategic Goal - Xog Access	Allows user to import and export Strategic Goal instances using the XML Open Gateway interface.

Total Results: 5

CA Clarity PPM Studio created these Access Rights for the Custom Object “Strategic Goal”. They allow you to secure the Custom Object.



Select Access Rights: Step 1 of 2 (Resource: System Administrator)

Object: Strategic Goal
Access Right:
Description:

	Access Right	Description	Object
□	Strategic Goal - Edit	Allows resource to edit specific Strategic Goal objects.	Strategic Goal
□	Strategic Goal - View	Allows resource to view specific Strategic Goal objects.	Strategic Goal

Total Results: 2

The following table lists the Access Rights that CA Clarity PPM Studio automatically generates when you create a master object.

Note: Replace the <Object> string with the actual object name that you specify when creating the object:

Access Right	Description
<Object> Create	Allows resource to create <Object> objects. This includes the page navigation right.
<Object> Edit	Allows resource to edit specific <Object> objects.
<Object> Edit All	Allows resource to edit all <Object> objects. This includes the page navigation right.
<Object> Navigate	Allows resource to navigate to <Object> object pages.
<Object> View	Allows resource to view specific <Object> objects.
<Object> View All	Allows resource to view all <Object> objects. This includes the page navigation right.
<Object> XOG Access	Allows user to import and export <Object> instances using the XML Open Gateway interface.

Stock Access Rights

Stock Access Rights are related to specific functionalities of the CA Clarity PPM application and its stock objects. Many of these object access rights are available as installation defaults. Detailed information regarding the various types of access rights, the corresponding Investment Objects, selecting and granting the access rights is available in the CA Clarity PPM product documentation and online help.

Investment Objects Access Rights

Investment Objects (Services, Applications, Assets, Products, Projects, Ideas, and Other Work) have access rights to grant access to specific functionalities, in addition to the general access rights previously described. For a complete list of Investment Objects Access rights, see the CA Clarity PPM product documentation guides: Administration Guide, IT Service Management User Guide *and* Project Management User Guide.

Examples of Investment Object Access Rights:

Investment Object Access Rights	Description
<Investment Object> - View Financial	Allows resources to view Financial Properties for that Investment Object instances
<Investment Object> - View Allocation Information	Allows resources to view Allocation information for that Investment Object instances

Investment Object Access Rights	Description
<Investment Object> - Hierarchy – Financial Rollup – View	Allows resources to view the Financial Roll up information for that Investment Object instances hierarchy
<Investment Object> Cost Plan – View	Allows resources to view the cost plans for that Investment Object instances
<Investment Object> Benefit Plan – View	Allows resources to view the benefit plans for that Investment Object instances
<Investment Object> Budget Plan – View	Allows resources to view the budget plans for that Investment Object instances
<Investment Object> - Edit Financial	Allows resources to edit Financial Properties for that Investment Object instances
<Investment Object> - Edit Allocation Information	Allows resources to edit Allocation information for that Investment Object instances
<Investment Object> - Hierarchy – Financial Rollup – Edit	Allows resources to edit the Financial Rollup information for that Investment Object instances hierarchy

Investment Object Access Rights	Description
<Investment Object> Cost Plan – Edit	Allows resources to edit the cost plans for that Investment Object instances
<Investment Object> Benefit Plan – Edit	Allows resources to edit the benefit plans for that Investment Object instances
<Investment Object> Budget Plan – Edit	Allows resources to edit the budget plans for that Investment Object instances
<Investment Object> - Edit Access Rights	Allows resources to manage security for that Investment Object instances, granting access to users, groups, or OBS Units. Depends on <Investment> - Navigate access right being granted.
<Investment Object> - Approve	Allows resources to approve that Investment Object instances

Resource Access Rights

Several access rights are available to manage resources. Refer to the *CA Clarity PPM Resource Management Guide* for a complete list of resource-related access rights.

Examples of resource-related Access Rights:

Resource Access Right	Description
Resource – Approve Ideas	Allows users to approve Ideas for a specific Resource
Resource – Approve Time	Allows users to approve and reject Timesheets for a specific Resource
Resource – Hard Book	Allows users to hard book a resource or role to an investment
Resource – Soft Book	Allows users to soft book a resource or role to an investment
Resource – Update Skills	Allows users to create, edit and view the skills of resources for which they have Resource – View access right

Administration and CA Clarity PPM Studio Access Rights

The CA Clarity PPM Administrator has its own set of Access Rights. These access rights grant resources the ability to access the Admin Tool, manage security, and to use CA Clarity PPM Studio functionalities such as creating and editing objects, implementing partitioning, creating portlets and pages. For a complete list of CA Clarity PPM Studio Access Rights, see the *CA Clarity PPM Studio Developer Guide*.

Examples of CA Clarity PPM Studio Access Rights:

CA Clarity PPM Studio Access Rights	Description
Administration – Access	Allows users to navigate to the Admin Tool
Administration – Studio	Allows users to navigate to CA Clarity PPM Studio pages
Administration – Authorization	Allows users to manage Resources and Groups
Administration – Application Setup	Allows users to edit Clarity options and settings, including OBS, Time, Data Administration and General Settings
Portlet Create	Allow users to create portlets
Portlet Definition Editor	Allows users to edit the definitions of a portlet

CA Clarity PPM Studio Access Rights	Description
Page Definition Editor	Allows users to edit the definitions of a Page
Audit Trail – Access	Grants users access to the Audit Trail on the Data Administration Section of the Administration Menu

Jobs and Reports

Refers to a group of Access Rights specific to managing Jobs and Reports. For a complete list of Reports and Jobs access rights, see the *CA Clarity PPM Administration Guide*. Some of the access rights are Global type, some are Instance type. In some cases, multiple access rights are required to access and manage all actions related to a job or report processes.

Examples of Access Rights for Jobs and Reports:

Access Rights – Job and Reports	Description
Reports and Jobs - Create Definition	Allows you to create, edit and view Job or Report definitions in the Administration Tool. Requires Report and Jobs – Administer Access right.
Jobs – Access	Allows you to access the Jobs page. Additional access is required to run Jobs or view output.
Reports – Access	Allows you to access the Reports page. Requires additional access rights for running or editing reports or viewing output.
Job – Run	Allows you to run a specific job, edit its properties and view the output. Dependent on Jobs-Access right being granted.
Report – Run	Allows you to run the reports to which you have access, to edit report properties and review report output. You must also have the Reports - Access right.

Processes

Refers to a group of Access Rights specific to managing Processes. For a complete list of Processes access rights, see the *CA Clarity PPM Administration Guide*.

Examples of Process related Access Rights:

Access Rights - Processes	Description
Process – Start	Allows you to start a specific Process instance
Process – Cancel	Allows you to cancel an instance of a specific Process that is currently running
Process – Access	Allows you to navigate to the Processes page in the Administration Menu
Process – Manage	Allows you to manage (start, delete, or cancel) a specific Process instance

Other Stock objects Access Rights

Several other stock objects - such as Departments, Releases, Requirements, and so on - have Access Rights associated to them. For a complete list of access rights, see the *CA Clarity PPM Administration Guide* and the *CA Clarity PPM Requirements Planning User Guide*.

Examples of other Stock Object Access Rights:

Access Rights – Stock Objects Other	Description
Release Plan – Create	Allows you to create Release Plans
Release – Create	Allows you to create Releases
Release – Approve	Allows you to approve specific instance of a release
Requirement - Approve	Allows you to approve specific instances of Requirements
Requirement – Edit	Allows you to edit specific instances of Requirements
Department – Create	Allows you to create departments
Department – View Chargeback Information (Type: Instance)	Allows you to view invoices and recovery statements for specific departments
Department – View Chargeback Information (Type: Global)	Allows you to view invoices and recovery statements for ALL departments

Automatic Access Rights

The application automatically grants some access rights. These access rights typically have the string "(auto)" in their names. For a complete list of automatic access rights, see the *CA Clarity PPM Administration Guide*.

Examples of Automatic Access Rights:

Access Rights – Automatic	Description
<Investment Object> - Manager (Auto	Granted automatically to the manager of that Investment Object instance. Equivalent to <Investment Object> - Edit.
Resource – Self (Auto)	Granted automatically to a resource when created.
Resource – Manager (Auto)	Granted automatically to the person creating a resource. When the Resource Manager changes, this Access Right is transferred to the new Resource Manager.

Defining Data Scope

The Data Scope is the final component of the security model. Actors are the resources getting access rights that correspond to the actions Actors are allowed to perform, and the Data Scope determines on which data Actors are allowed to perform those actions. Data scope is the final element in **Who** does **What** to **Which** Data.

In CA Clarity PPM, you can use the following three methods to determine the data scope when you grant access rights:

Instance

Grant access rights to a specific instance of an object.

OBS Unit

Grant access rights to the instances of an object that are related to a specific Unit or Branch in an OBS.

Global

Grant access rights to all instances of an object.

Granting Access Rights Directly to Object Instances

We do not recommend granting access rights directly to object instances. This approach can result in increased maintenance complexity and overhead due to repeatedly granting access instance-by-instance. When you create a project, you must grant access to the appropriate resources that use or modify the project information. When you create a resource, you must grant access to the correct resources that can see, allocate, and approve actions related to that new resource.

There are two circumstances when granting access rights directly to object instances is recommended:

- End-users are responsible for defining security for their objects. For example, the Project Manager is responsible for granting other resources in the company access to the project information.
- You have highly sensitive information, such as a confidential project, and you do not want access to be automatically inherited because a resource is part of a department, or group. In this case, access is granted on a need-to-have basis only.

Typically, instance-level access rights are granted as an exception, used jointly with other forms of granting access, such as OBS Units and Global access.

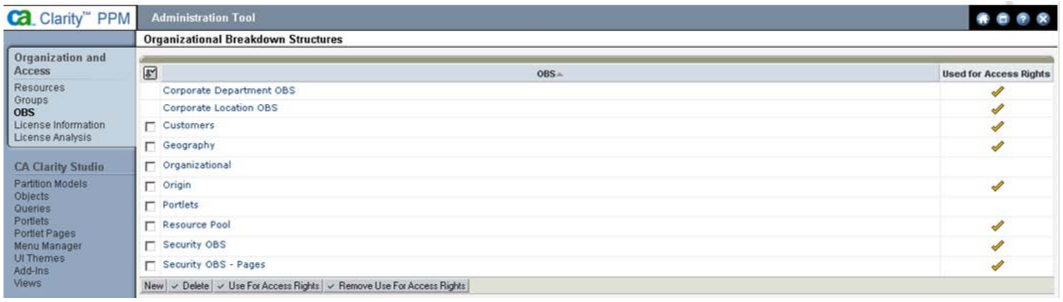
Use OBS Units to Determine Data Scope

OBS Units can be used as Actors (see page 19), and also to determine the Data Scope. OBS Unit refers to the scope, or to a data portion of the security model. This discussion refers to the OBS Unit as the “Scope”, or the “Which Data?” portion of the security model. We are discussing granting resources access to the instances of an object that are related to OBS Units. Access is granted to different objects that may be categorized and grouped through the association of a Unit in an OBS.

The following examples refer to the Geography OBS previously defined.

- Grant a resource access to projects related to the Earth unit only.
  - The resource has access to projects related directly to the Earth unit.
- Grant a resource access to projects related to the Earth unit and all its descendants, which includes projects in all Continents and Countries and States.
- Grant a resource access to projects related to the North America unit and all its descendants.
  - The resource has access to projects related to North America (the Continent level unit) and Mexico (a descendent).
  - The resource does not have access to projects related to the top–level unit Earth or to projects related to Argentina under the unit South America as this is a different branch.
- Grant a resource access to projects related to the South America unit, all its ancestors and descendants.
  - The resource has access to projects related to Earth (the ancestor), South America (the unit) and Brazil (a descendent).
  - The resource does not have access to projects related to Mexico under the unit North America, as this is a different branch.

To use an OBS for security purposes, set it as *Used for Access Rights* as illustrated below:



Organizational Breakdown Structures

	OBS	Used for Access Rights
	Corporate Department OBS	✓
	Corporate Location OBS	✓
□	Customers	✓
□	Geography	✓
□	Organizational	
□	Origin	✓
□	Portlets	
□	Resource Pool	✓
□	Security OBS	✓
□	Security OBS - Pages	✓

In summary, OBS Units are used to group object instances for several reasons, one of which is granting access rights. The OBS Units are flexible and appropriate to security because of the tree-like hierarchical structure that allows you to grant multi-level access to CA Clarity PPM objects.

Using Global Access Rights

We do not recommend using Global Access rights widely. Typically, you grant global rights when there is no other option. Examples of circumstances where you would use this method:

- The Data Scope is undefined. <Object> – Navigate or <Object> – Create are examples of scope-independent access rights. <Object> – Navigate refers to the ability to access the <Object> pages, but not to the data presented in them. Access to the data must be granted separately, using another Access Right <Object> – View, which is scope-related. <Object> - Create has no scope because the object has not been created yet, so it is not yet part of an OBS, for instance; once the created object is saved you are able to apply Instance rights and the object is subject to all OBS and Global rights that may apply.

- Use as special functionality. Some CA Clarity PPM functionalities, such as CA Clarity PPM Studio, must be granted through a Global access right, in this case, Administration – Studio. These functionalities also have an undefined Data Scope and therefore are granted as Global rights.

- Granting general access to all instances of an object. For example, if you need to grant someone with viewing access to all of the instances of an object, use a Global Right such as <Object> - View All.

This approach may be useful to grant resources access, especially read-only access, to an Object instances. We usually do not recommend that approach unless necessary, as you may start your project with one scope, and the scope may change after a while.

Other departments in the company may take an interest in Project and Portfolio Management and require access to the project investment objects. Other businesses or other companies in your group may share the same instance of CA Clarity PPM, and the need to restrict more security rights may come with that change. If you ever need a change in scope, it may take you much longer to redesign and redeploy your model.

Access Rights Use Cases

The following use cases reference the Geography OBS (see page 19). These use cases demonstrate how choosing between Global Access Rights or OBS Units Access Rights may impact the security implementation.

Use Case #1

A fictitious company based in Germany with operations all over Europe needs all members of the PMO group to have access to all of the company projects.

Solution 1

Grant the PMO Group with the Project – View Management access right for OBS Unit Europe and descendants.

Solution 2

Grant the PMO Group with the Project – View Management All Global access right.

For the current scenario the results are the same. Solution 2 gives access to all of the projects in Clarity as requested, while Solution 1 gives access to all of the projects in the OBS Unit Europe, which for now is the same scope, as all of the company projects are associated to the OBS Unit Europe.

Now, suppose there is a change in the scenario. The company has started a successful business in Argentina. A new PMO Group has been formed in Argentina to manage all South American projects.

Use Case #2

Members of the PMO Group in Europe must have access to all of the company projects in Europe. Members of the South America PMO Group must have access to all of the company projects in the South America.

The solution to this use case depends on whether you chose Solution 1 or Solution 2 in the initial use case.

- If you chose solution 1, the scenario change is more easily implemented. Create a new OBS Unit for South America. Grant access to the new South America PMO Group to the projects related to the South America OBS unit and its descendants. No changes to the access for the Europe OBS Unit are needed. You may want to, optionally, rename the PMO Group to Europe PMO Group to make it more consistent with the access rights it has now.

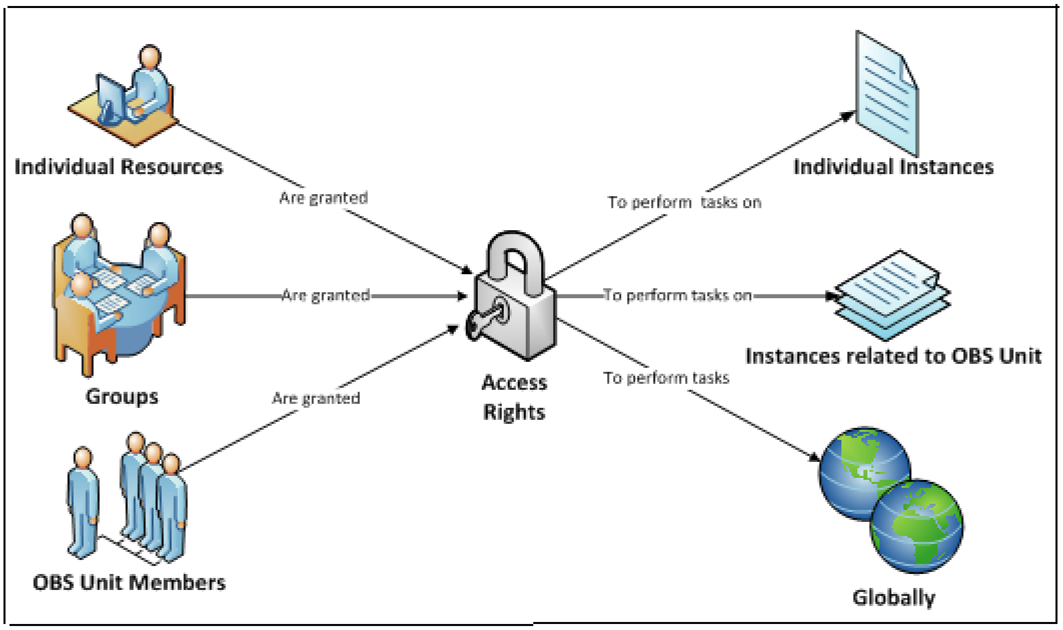
- If you chose solution 2, you have to redesign your project security. Now as you have two different PMO structures, one in Europe and one in South America, global access rights are not the correct security solution for this use case. It is necessary to revoke all global rights from the PMO Group and grant them access only to the Europe OBS unit and its descendants. Then, grant the new South America PMO Group access to the South America OBS unit and its descendants. You may also consider changing the name of the PMO group to Europe PMO to reflect the association to new access rights.

In this simplified example, to make the changes and manage is not that complex. Now, imagine you have all of the CA Clarity PPM investment objects and a much larger selection of custom objects and resources, and you have used the same Global model for everyone – and now divide it all into two or more groups. It can be very complex and time consuming.

Summary

Actors, Actions, and Data Scope are used to design security rules in CA Clarity PPM.

The possible relationships between Actors, Actions, and Data Scope are represented in the following diagram:



The OBS unit can have the following relationships:

- OBS Unit as the Scope refers to the objects (projects, applications, services, and so on) related to that OBS Unit.
- OBS Unit as an Actor refers to the resources who are members of that OBS Unit. For example, the Resource OBS.
- The Actor OBS Unit and the Scope OBS Unit in a security configuration may relate to different structures. For example, Resource members of the Department: IT OBS Unit may be granted access to view Projects related to the ProductLine: eCommerce OBS Unit.

The following tables summarize the possible options for the Object View relationships:

Actor (Who)	Action (What)	Scope (Which Data)
Resource	<Object> View	Instance
Resource	<Object> View	OBS Unit
Resource	<Object> View All	Global
Group	<Object> View	Instance
Group	<Object> View	OBS Unit
Group	<Object> View All	Global
OBS Unit	<Object> View	Instance
OBS Unit	<Object> View	OBS Unit
OBS Unit	<Object> View All	Global

The following tables provide use case examples of the Object View relationship options. The Action column identifies the Access Right associated to the use case:

Actor (Who)	Action (What)	Data Scope (Which data)	Outcome
Resource. Example: ClarityUserA	Project View	Specific instance. Example: Project named ABC Implementation	Resource ClarityUserA has Project View access to the ABC Implementation project
Resource. Example: ClarityUserA	Project View	OBS Unit. Example: Projects that are members of the Product Line:JLM OBS Unit	Resource ClarityUserA has Project View access to all of the projects in JLM unit of the Product Line OBS
Resource. Example: ClarityUserA	Project View All	Global access. Example: All Projects	Resource ClarityUserA has Project View access to all projects in Clarity

Actor (Who)	Action (What)	Data Scope (Which data)	Outcome
Group. Example: Project Managers IT	Project View	Specific instance. Example: Project named ABC Implementation	Members of the Project Managers IT group have Project View access to the ABC Implementation project
Group. Example: Project Managers IT	Project View	OBS Unit. Example: Projects that are members of the Product Line:JLM OBS Unit	Members of the Project Managers IT group have Project View access to all of the projects in JLM unit of the Product Line OBS.
Group. Example: Project Managers IT	Project View All	Global access. Example: All Projects	Members of the Project Managers IT group have Project View access to all projects in CA Clarity PPM
OBS Unit. Example: Departments: IT	Project View	Specific instance. Example: Project named ABC Implementation	Members of the IT unit of the Departments OBS have Project View access to the ABC Implementation project
OBS Unit. Example: Departments: IT	Project View	OBS Unit. Example: Projects that are members of the Product Line:JLM OBS Unit	Members of the IT unit of the Departments OBS have Project View access to all of the projects in JLM unit of the Product Line OBS.
OBS Unit. Example: Departments: IT	Project View All	Global access. Example: All Projects	Members of the IT unit of the Departments OBS have Project View access to all projects in CA Clarity PPM.

Chapter 3: Granting Access

Granting Access to Groups

The following use cases demonstrate how to grant Group Members with different types of Access Rights (actions) for different Scopes (specific instances, OBS-related instances, or Global Access) when the Actors are Groups.

Important! All the names used in the use cases represent fictitious characters created for the purpose of illustrating the functionality described in the use cases. Some of the pages, portlets, sub-pages and attributes used in the use cases represent fictitious elements and may not be available in your CA Clarity PPM installation.

Granting Instance Rights to Groups

This option is used to grant group members with access to specific instances of an object.

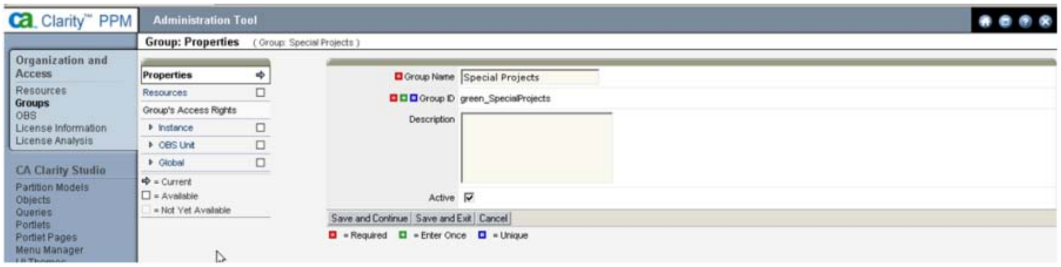
Use Case

The group is named Special Projects. Members of this group should have viewing access to project named Top Secret Telepathic Scanner. A fictitious resource, Clare Green, is a member of the Special Projects Group.

Setting Up

1. Determine the Actors.

   In this use case, the Actors (Who) are the members of the Special Projects group.



Group: Properties (Group: Special Projects)

Group Name: Special Projects

Group ID: green_SpecialProjects

Description:

Active: ☑

2. Determine the Action (What).

   In this use case, it is Project-View access.

3. Define the Scope (Which Data).

   In this use case, it is one specific instance of a project: The Top Secret Telepathic Scanner project.

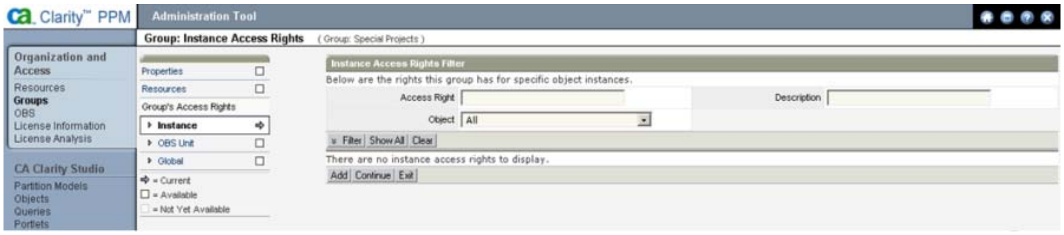
Review the Current Access Rights

1. Use the Group Properties page to define the access rights.

2. Locate the section titled Group Access Rights, and grant the required access rights to the group Special Projects defined in Group Name field.

3. Click Instance to display the Group: Instance Access Rights page.

   The group Special Projects has no Instance Rights assigned as shown in the following graphic:



Group: Instance Access Rights (Group: Special Projects)

Instance Access Rights Filter

Below are the rights this group has for specific object instances.

Access Right:

Description:

Object: All

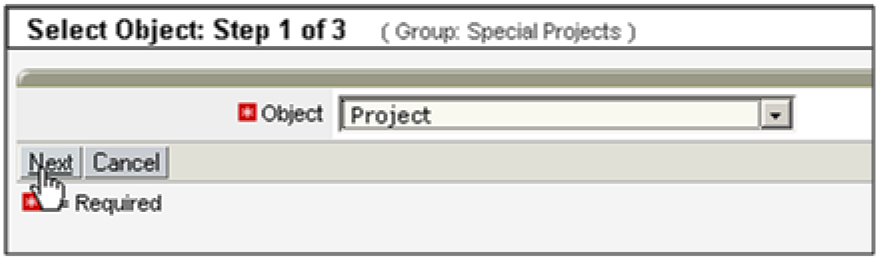
There are no instance access rights to display.

Selecting and Granting Access Rights

1. Select Add on the Group: Instance Access Rights page to begin selecting access rights.

   – Select the object that you want to set up rights for. In this example, use Project.

   – Click Next.



Select Object: Step 1 of 3 (Group: Special Projects)

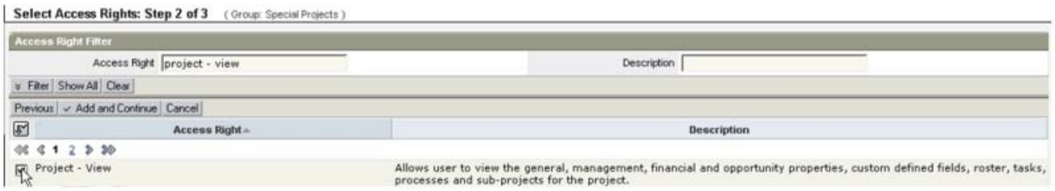
Object: Project

= Required

2. Select the Access Right Project – View to view the projects. You can filter the list to display items with Project – View in the name.

   – Select the appropriate line item.

   – Click Add and Continue.



Select Access Rights: Step 2 of 3 (Group: Special Projects)

Access Right: project - view

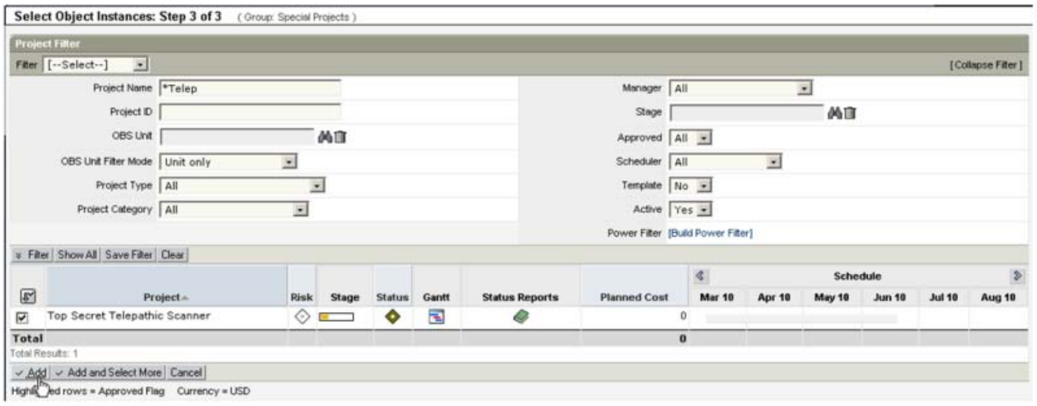
Description:

	Access Right	Description
☑	Project - View	Allows user to view the general, management, financial and opportunity properties, custom defined fields, roster, tasks, processes and sub-projects for the project.

3. Locate the actual Project instance that has View access. In this example, use the wildcard feature (*Tele) to locate the project Top Secret Telepathic Scanner.

   You can select multiple instances to grant access in a single operation using the Add and Select More feature. Locate the project instances, select and add instances until you are finished.

   Note: Verify that you click *Add* for a single selection or *Add* and *Select More* for multiple selections. Click *Add* for the last instance you are granting access to.



Select Object Instances: Step 3 of 3 (Group: Special Projects)

Filter: [--Select--]

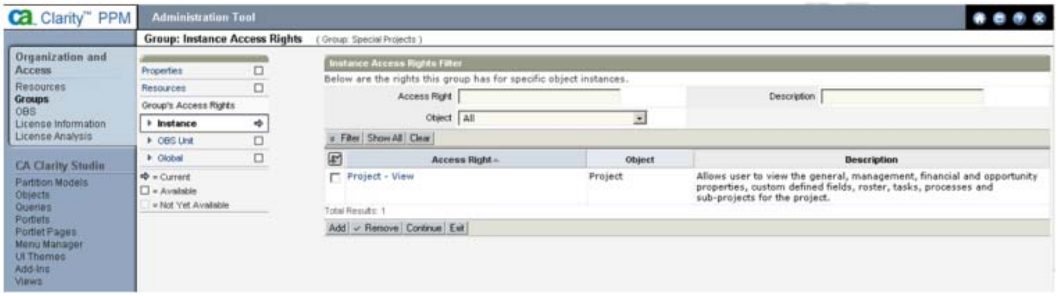
Project Name	*Telep	Manager	All
Project ID		Stage	
OBS Unit		Approved	All
OBS Unit Filter Mode	Unit only	Scheduler	All
Project Type	All	Template	No
Project Category	All	Active	Yes
		Power Filter	[Build Power Filter]

	Project	Risk	Stage	Status	Gantt	Status Reports	Planned Cost	Mar 10	Apr 10	May 10	Jun 10	Jul 10	Aug 10
☑	Top Secret Telepathic Scanner	◇		◆			0						
Total							**0**						

Total Results: 1

Highli[illegible]ed rows = Approved Flag   Currency = USD

4. Select the Instance function under Group Access Rights to confirm the Project – View access is enabled. The access right is granted as illustrated in the following graphic:



Group: Instance Access Rights (Group: Special Projects)

Below are the rights this group has for specific object instances.

Access Right:

Description:

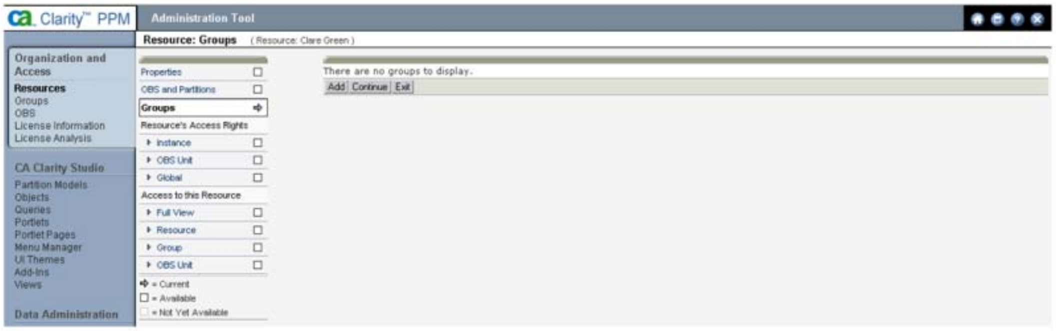
Object: All

	Access Right	Object	Description
☐	Project - View	Project	Allows user to view the general, management, financial and opportunity properties, custom defined fields, roster, tasks, processes and sub-projects for the project.

Total Results: 1

Confirmation

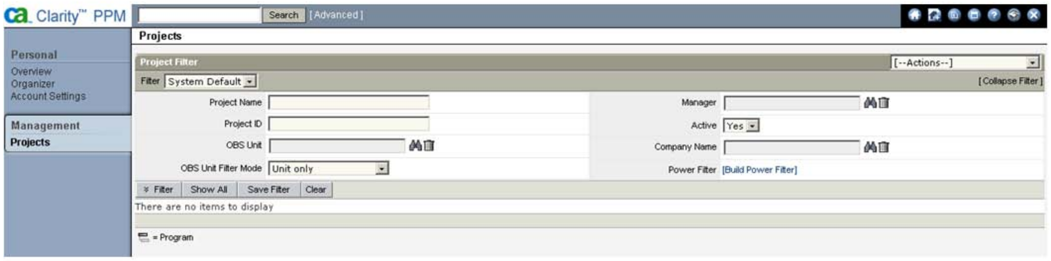
Clare Green is the resource in this example. This resource is not a member of the Group with access to the Top Secret Telepathic Scanner project.



Resource: Groups (Resource: Clare Green)

There are no groups to display.

No projects are listed on Personal view of the Management/Project page for this resource.



Projects

Filter: System Default

Project Name:

Project ID:

OBS Unit:

OBS Unit Filter Mode: Unit only

Manager:

Active: Yes

Company Name:

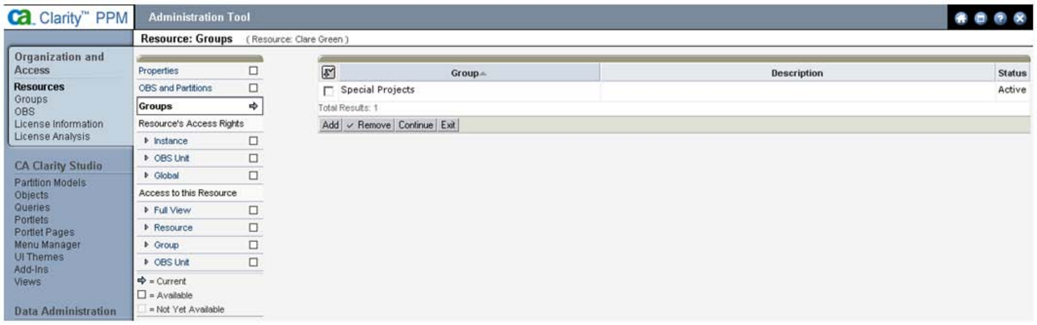
Power Filter: [Build Power Filter]

There are no items to display

Add a resource (For example, Clare Green) to the Access Rights group for Special Projects using the Resources page in the Organization and Access menu

1. Log in as the Admin.
2. Select Resources from Organization and Access Menu. The Resources page appears.
3. Filter the results for available resources on the Resources page and select the resource Clare Green.
4. Select Groups from the content menu. The Resource: Groups page appears.
5. Click Add.

6. Select the check box next to the desired group and click Add.



Resource: Groups (Resource: Clare Green)

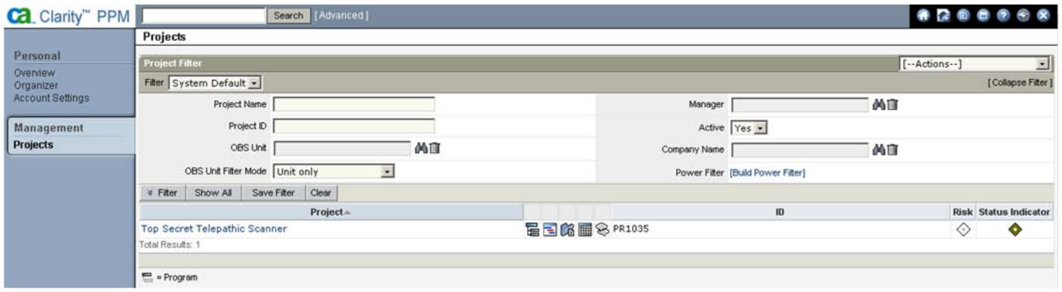
☐	Group	Description	Status
☐	Special Projects		Active

Total Results: 1

7. Log off as the Admin and log in as Clare Green to confirm the change.

8. Return to the Management menu for the resource (Clare Green).

9. Select Projects. The following screenshot illustrates how the page should display the project available to Clare Green as a member of the Special Projects group:



Projects

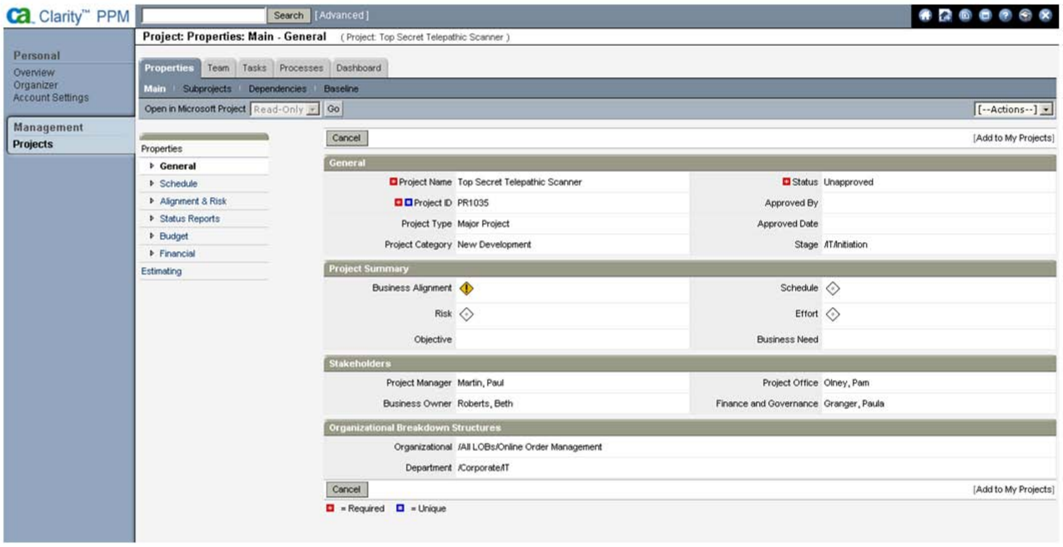
Filter: System Default

Project Name:
Project ID:
OBS Unit:
OBS Unit Filter Mode: Unit only
Manager:
Active: Yes
Company Name:
Power Filter: [Build Power Filter]

Project	ID	Risk	Status Indicator
Top Secret Telepathic Scanner	PR1035	◇	◆

Total Results: 1

10. The resource (Clare Green) clicks the Project name to see the project attributes in read-only mode as illustrated in the following screenshot:



Project: Properties: Main - General (Project: Top Secret Telepathic Scanner)

Open in Microsoft Project: Read-Only

General

Project Name: Top Secret Telepathic Scanner
Status: Unapproved
Project ID: PR1035
Approved By:
Project Type: Major Project
Approved Date:
Project Category: New Development
Stage: /IT/Initiation

Project Summary

Business Alignment: ◆
Schedule: ◇
Risk: ◇
Effort: ◇
Objective:
Business Need:

Stakeholders

Project Manager: Martin, Paul
Project Office: Olney, Pam
Business Owner: Roberts, Beth
Finance and Governance: Granger, Paula

Organizational Breakdown Structures

Organizational: /All LOBs/Online Order Management
Department: /Corporate/IT

🟥 = Required 🟦 = Unique

Granting OBS Unit Rights to Groups

This option is used to grant group members access to all instances of an object which are related to an OBS Unit, or its ancestors and descendants.

Use Case

> Add Group members to an OBS Unit named Administration in an OBS named Organizational that is associated with Projects and other investments. All members of the group Administration Stakeholders should have viewing access to the Projects related to the Administration OBS Unit.

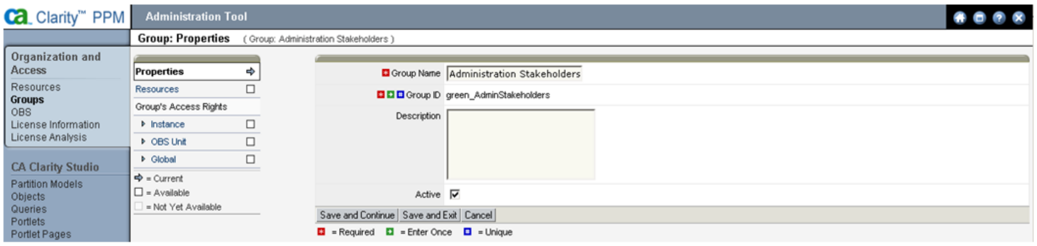
Setting Up

1. Determine the Actors. In this use case, the Actors are the members of the Administration Stakeholders group. This example assumes that this group is already defined.

2. On the Organization and Access menu, select Groups. The Group Properties page appears.

3. Select the name of the group you want to work with. Use Administration Stakeholders for this example.

4. Determine the Action. For this use case, the access to be granted is Project-View.



Group: Properties (Group: Administration Stakeholders)

Group Name: Administration Stakeholders

Group ID: green_AdminStakeholders

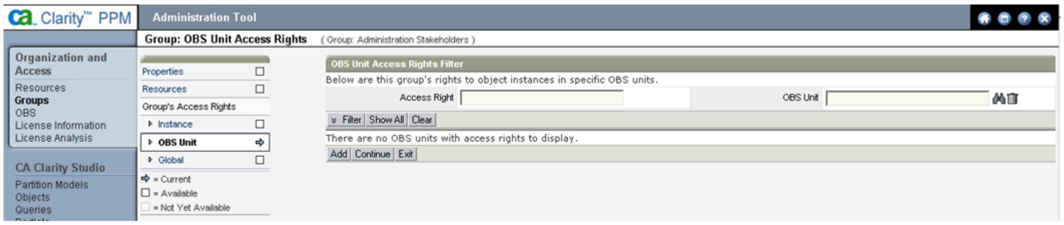
Description:

Active: ☑

5. Determine the Scope. In this use case, the Scope is comprised of all projects related to the Administration OBS unit in the Organizational OBS.

Review the Current Access Rights

Click OBS Unit under Group Access Rights to grant this Group members access rights using that OBS as the Scope delimiter. As shown below, the group members do not have any OBS Unit-related access rights yet.



Group: OBS Unit Access Rights (Group: Administration Stakeholders)

OBS Unit Access Rights Filter

Below are this group's rights to object instances in specific OBS units.

Access Right:

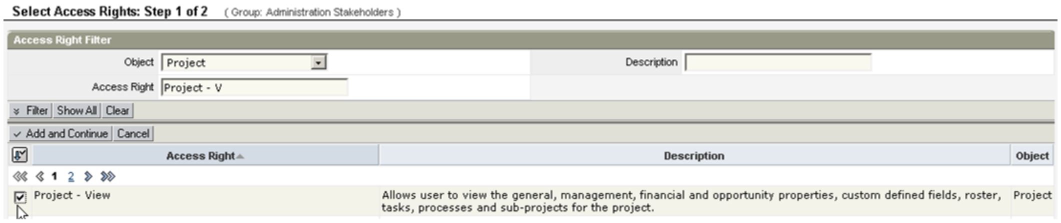
OBS Unit:

There are no OBS units with access rights to display.

Select and Grant Access Rights

1. Click Add on the Group: OBS Unit Access Rights page to select the Access Rights.

   - You can filter the access rights to narrow down your search. Select multiple access rights by using the checkboxes to the left.
   - The Project – View Access Right in the Access Rights column is the one for this example.
   - Click Add and Continue.



Select Access Rights: Step 1 of 2 (Group: Administration Stakeholders)

Access Right Filter

Object: Project

Access Right: Project - V

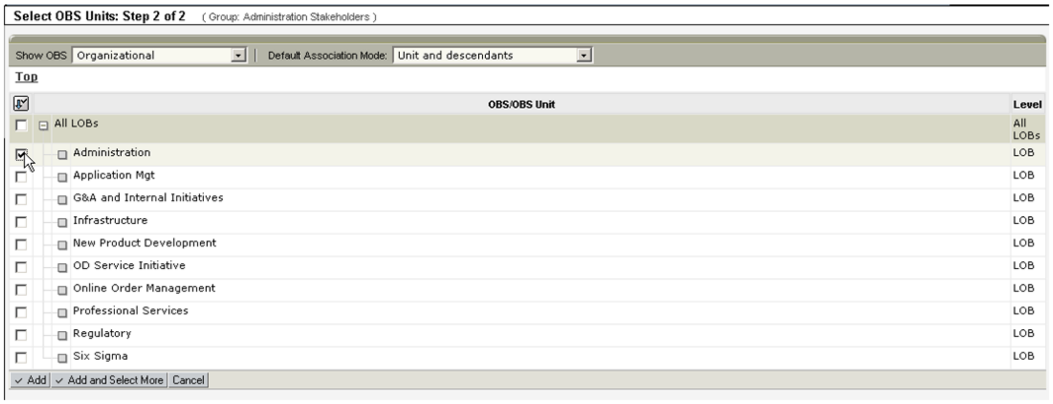
Description:

	Access Right	Description	Object
☑	Project - View	Allows user to view the general, management, financial and opportunity properties, custom defined fields, roster, tasks, processes and sub-projects for the project.	Project

2. Select the Scope - the desired OBS Unit. You select a different OBS using the Show OBS attribute. You can also select multiple OBS units at a time.

   – For this example, select the Organizational: Administration unit. Use Add and Select More to keep filtering and adding OBS units if necessary.

   – Click Add.



Select OBS Units: Step 2 of 2 (Group: Administration Stakeholders)

Show OBS: Organizational | Default Association Mode: Unit and descendants

Top

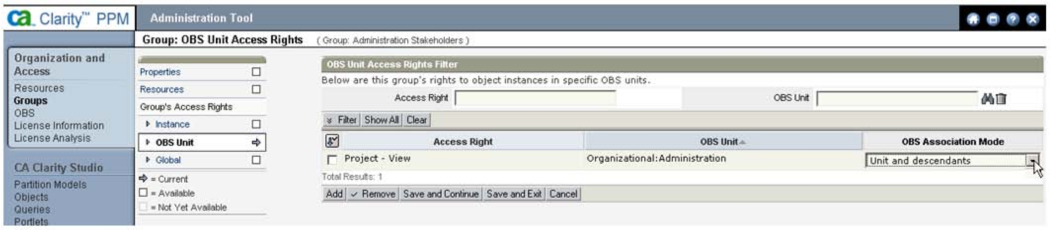
	OBS/OBS Unit	Level
□	⊟ All LOBs	All LOBs
☑	Administration	LOB
□	Application Mgt	LOB
□	G&A and Internal Initiatives	LOB
□	Infrastructure	LOB
□	New Product Development	LOB
□	OD Service Initiative	LOB
□	Online Order Management	LOB
□	Professional Services	LOB
□	Regulatory	LOB
□	Six Sigma	LOB

Define the Access for the OBS Nodes

Defining the access for the OBS nodes determines whether the Administration Stakeholders group should have access to only the Administration unit, or to its ancestors and/or descendants.

- Use the OBS Association Mode attribute to define the access to the other nodes. In this example, use the default value: Unit and descendants.

- If sub-units exist under the Administration OBS unit, and projects are related to those lower-level units, they should also be seen as part of the Administration OBS Unit and the Administration Stakeholders should be granted access to them.



Group: OBS Unit Access Rights (Group: Administration Stakeholders)

OBS Unit Access Rights Filter

Below are this group's rights to object instances in specific OBS units.

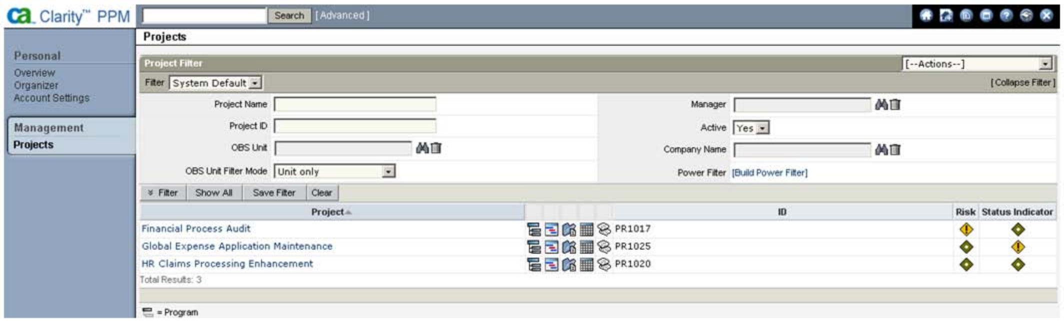
Access Right: | OBS Unit:

	Access Right	OBS Unit	OBS Association Mode
□	Project - View	Organizational:Administration	Unit and descendants

Total Results: 1

Confirmation

A member of the Administration Stakeholders group logs in to the system. The resource sees three projects in the Project List pertaining to the Administration OBS Unit as shown below:



Projects

Filter System Default

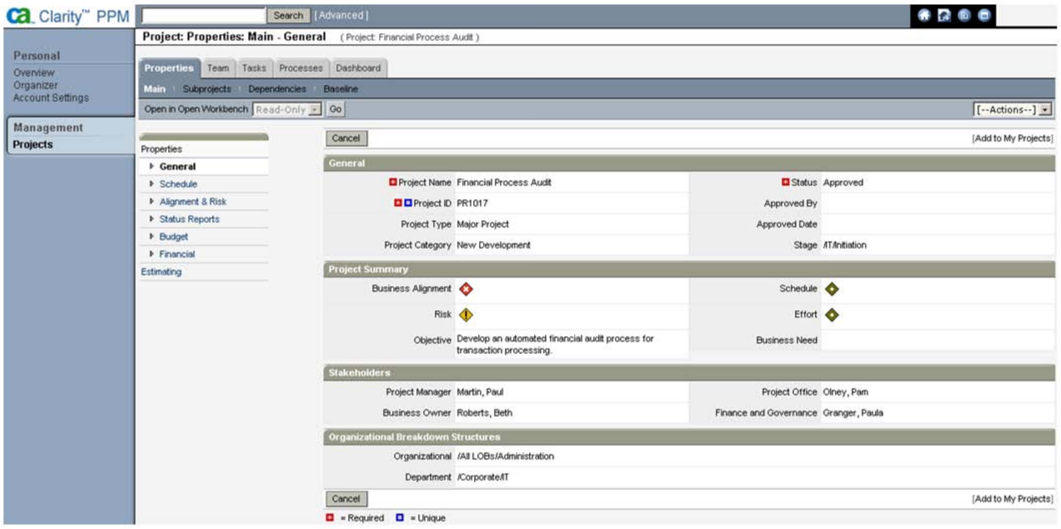
Project Name		Manager	
Project ID		Active	Yes
OBS Unit		Company Name	
OBS Unit Filter Mode	Unit only	Power Filter	[Build Power Filter]

Project	ID	Risk	Status Indicator
Financial Process Audit	PR1017	⚠	◆
Global Expense Application Maintenance	PR1025	◆	⚠
HR Claims Processing Enhancement	PR1020	◆	◆

Total Results: 3

= Program

The resource has View access to all of them as illustrated in the following screenshot:



Project: Properties: Main - General (Project: Financial Process Audit)

Open in Open Workbench Read-Only

General

Project Name	Financial Process Audit	Status	Approved
Project ID	PR1017	Approved By	
Project Type	Major Project	Approved Date	
Project Category	New Development	Stage	/IT/Initiation

Project Summary

Business Alignment	✖	Schedule	◆
Risk	⚠	Effort	◆
Objective	Develop an automated financial audit process for transaction processing.	Business Need	

Stakeholders

Project Manager	Martin, Paul	Project Office	Olney, Pam
Business Owner	Roberts, Beth	Finance and Governance	Granger, Paula

Organizational Breakdown Structures

Organizational	/All LOBs/Administration
Department	/Corporate/IT

🟥 = Required 🟦 = Unique

Granting Global Rights to Groups

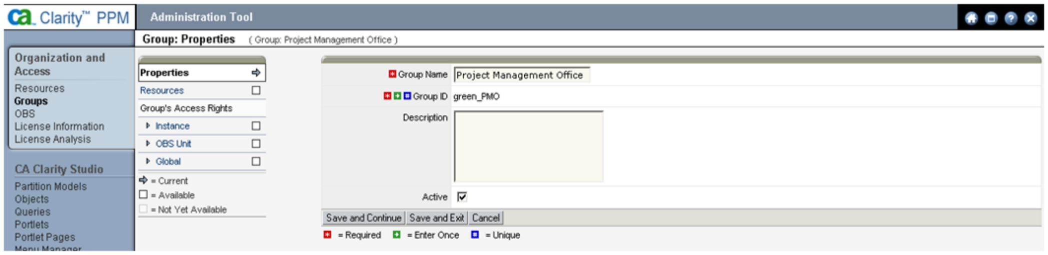
Use this option to grant group members with a global access right.

Use Case

> Members of the Project Management Office group should be able to create projects and view all existing projects.

Setting Up

- The Actors - the members of group Project Management Office.
- The Action - grant access to create projects and view existing projects.
- The Scope - all projects.



Group: Properties (Group: Project Management Office)

Group Name: Project Management Office

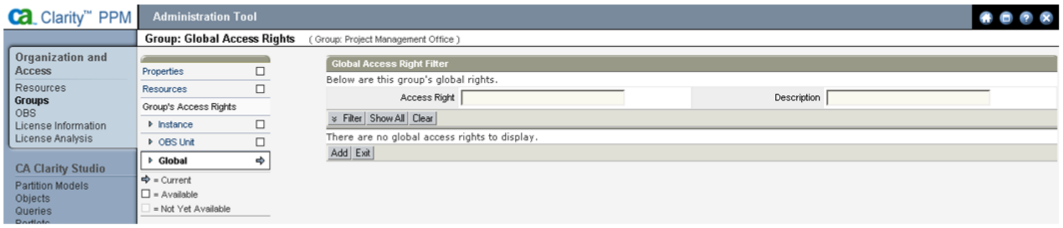
Group ID: green_PMO

Description:

Active: ☑

Review the Current Access Rights

By clicking Global under Group Access Rights you see all the Global rights the group has. In this case, this group has no Global rights yet, as illustrated in the following graphic:



Group: Global Access Rights (Group: Project Management Office)

Global Access Right Filter

Below are this group's global rights.

Access Right

Description

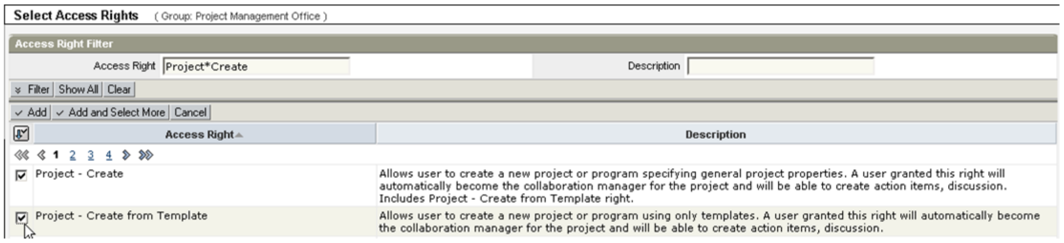
There are no global access rights to display.

Select and Grant Access Rights

1. Click Add on the Group Global Access Rights page to begin selecting the Global access rights for this group. The Select Access Rights page appears.

2. On the Select Access Rights page, use the filter to narrow the search to the access rights you want to add: Project – Create and Project – Create from Template. Select the access rights using the checkboxes to the left.

3. Click Add and Select More.



Select Access Rights (Group: Project Management Office)

Access Right Filter

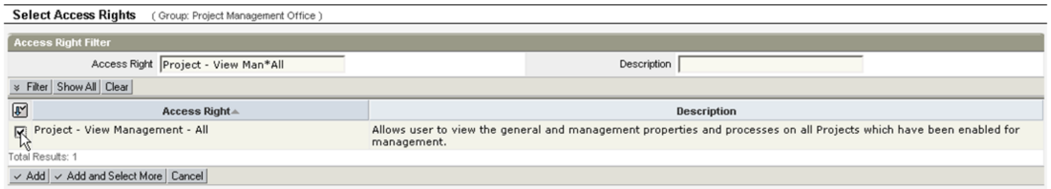
Access Right: Project*Create

Description:

	Access Right	Description
☑	Project - Create	Allows user to create a new project or program specifying general project properties. A user granted this right will automatically become the collaboration manager for the project and will be able to create action items, discussion. Includes Project - Create from Template right.
☑	Project - Create from Template	Allows user to create a new project or program using only templates. A user granted this right will automatically become the collaboration manager for the project and will be able to create action items, discussion.

4. To grant the group global access to viewing projects, select the Project – View Management – All access right.

5. Click Add.



Select Access Rights (Group: Project Management Office)

Access Right Filter

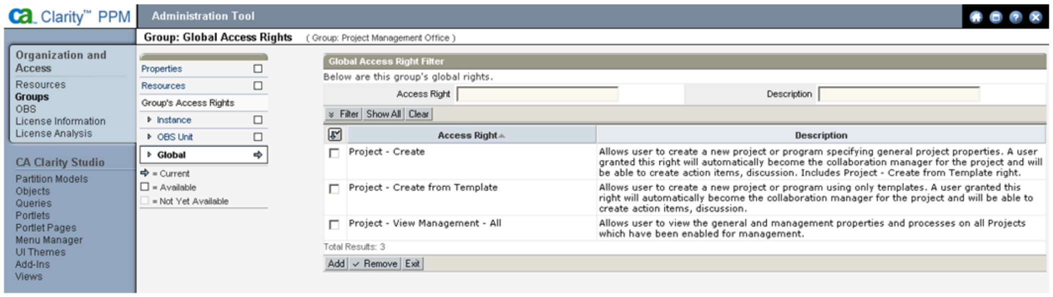
Access Right: Project - View Man*All

Description:

	Access Right	Description
☑	Project - View Management - All	Allows user to view the general and management properties and processes on all Projects which have been enabled for management.

Total Results: 1

As illustrated below, the desired Global Access Rights have been granted to the Project Management Office group.



Group: Global Access Rights (Group: Project Management Office)

Global Access Right Filter

Below are this group's global rights.

Access Right:

Description:

□	Access Right	Description
□	Project - Create	Allows user to create a new project or program specifying general project properties. A user granted this right will automatically become the collaboration manager for the project and will be able to create action items, discussion. Includes Project - Create from Template right.
□	Project - Create from Template	Allows user to create a new project or program using only templates. A user granted this right will automatically become the collaboration manager for the project and will be able to create action items, discussion.
□	Project - View Management - All	Allows user to view the general and management properties and processes on all Projects which have been enabled for management.

Total Results: 3

Confirmation

Paul Ortega, a fictitious resource, is a member of the Project Management Office group. When Paul accesses the Project list, he can see all of the company projects. He also has access to the Create actions *New* and *New from Template*.

How to Grant Access to OBS Unit Members

Granting Instance Rights to OBS Unit Members

This option is used to grant OBS Unit members with access to specific instances of an object.

Use Case

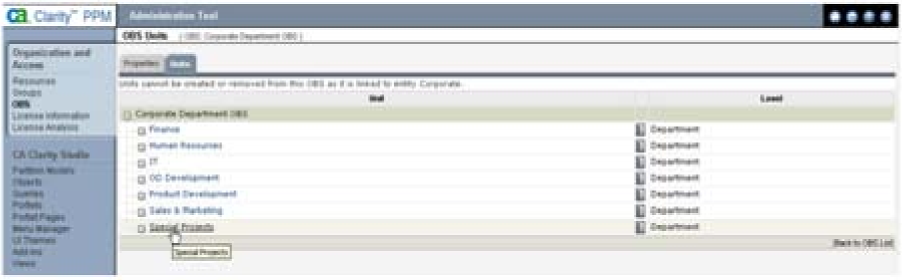
This example uses an OBS Unit named Special Projects in the Corporate Departments OBS. Members of this group should have viewing access to this project: Top Secret Telepathic Scanner. A fictitious resource, Clare Green, is added as a member of the Special Projects Group.

Setting up

- The Actors (Who) are the members of the Special Projects OBS Unit.
- The Action (What) is the Access Right to view Projects
- The Scope (Which Data) is one specific instance of a project: the Top Secret Telepathic Scanner project.

Review the Current Access Rights

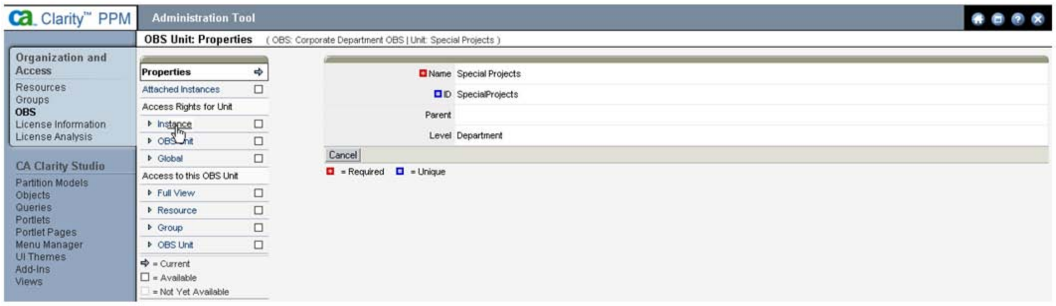
1. Navigate to the Organization and Access OBS Units page.
2. Select Special Projects.



Units cannot be created or removed from this OBS as it is linked to entity Corporate.

Unit	Level
Corporate Department OBS	
Finance	Department
Human Resources	Department
IT	Department
OD Development	Department
Product Development	Department
Sales & Marketing	Department
Special Projects	Department

3. The Properties page is displayed for Special Projects. Click Instance under Access Rights for Unit to view the access rights the Unit members have.

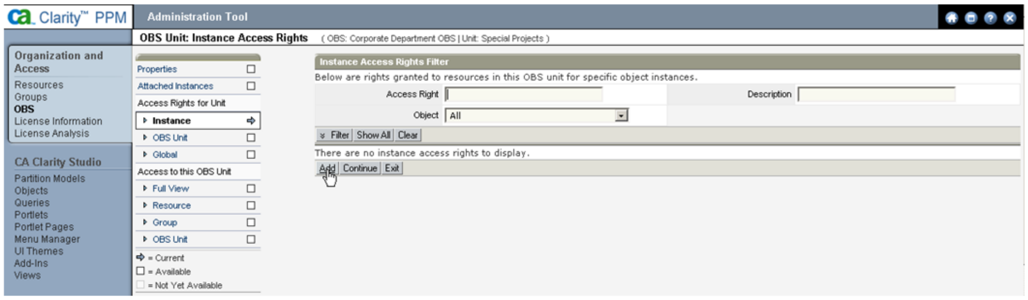


OBS Unit: Properties (OBS: Corporate Department OBS | Unit: Special Projects)

Name: Special Projects
ID: SpecialProjects
Parent:
Level: Department

🟥 = Required 🟦 = Unique

The OBS Unit Special Projects members have no Instance Rights assigned.



OBS Unit: Instance Access Rights (OBS: Corporate Department OBS | Unit: Special Projects)

Instance Access Rights Filter

Below are rights granted to resources in this OBS unit for specific object instances.

Access Right:
Description:
Object: All

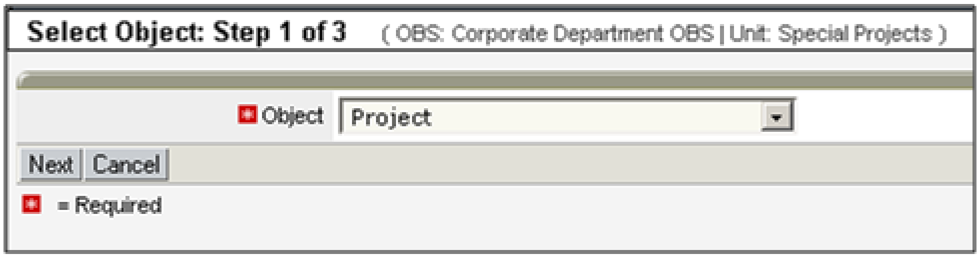
There are no instance access rights to display.

Select and Grant Access Rights

1. Click Add on the OBS Unit: Instance Access Rights page to begin the selection process as illustrated above. This takes you to the Select Object page.

   – Select the object. Project is the object in this example.

   – Click Next to continue.

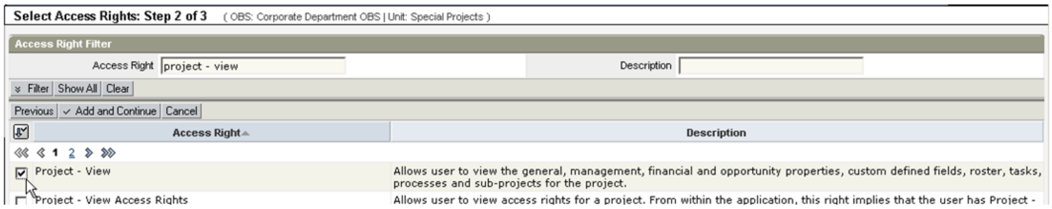


Select Object: Step 1 of 3 (OBS: Corporate Department OBS | Unit: Special Projects)

Object: Project

🟥 = Required

2. Select the Access Right named Project – View, so that the members can view projects. Click Add and Continue.



Select Access Rights: Step 2 of 3 (OBS: Corporate Department OBS | Unit: Special Projects)

Access Right Filter

Access Right: project - view

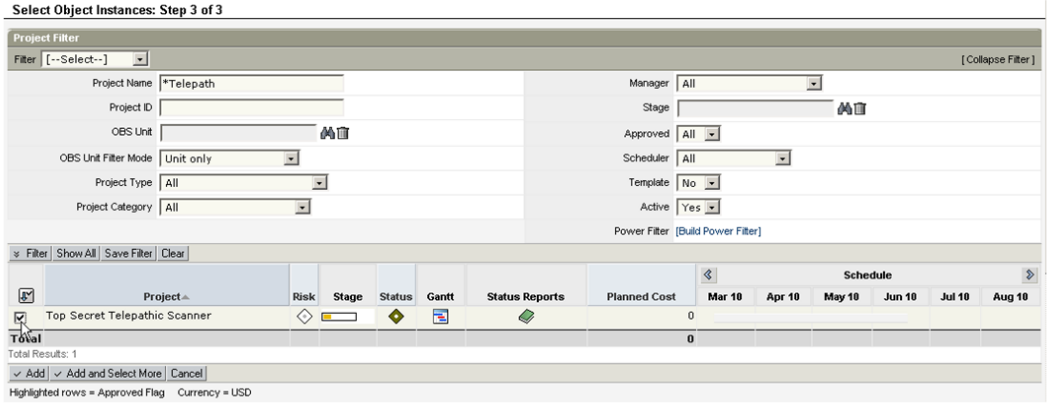
Description:

	Access Right	Description
☑	Project - View	Allows user to view the general, management, financial and opportunity properties, custom defined fields, roster, tasks, processes and sub-projects for the project.
☐	Project - View Access Rights	Allows user to view access rights for a project. From within the application, this right implies that the user has Project -

3. Select the Project instance *Top Secret Telepathic Scanner*.

   – Locate the project instance using the filter function or by scrolling.

   – Click Add.



Select Object Instances: Step 3 of 3

Project Filter

Filter: [--Select--]

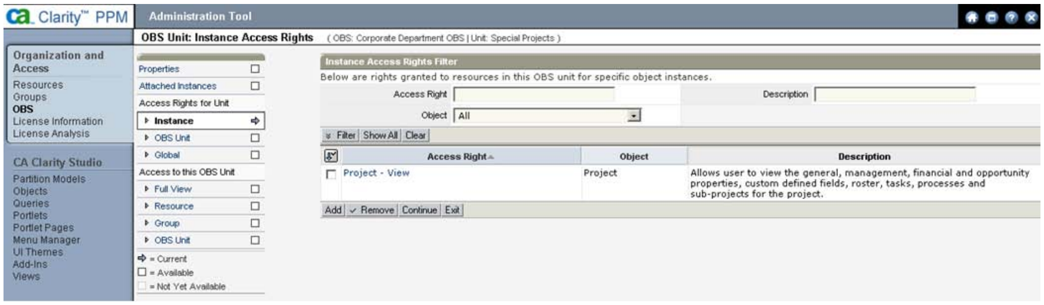
Project Name	*Telepath	Manager	All
Project ID		Stage	
OBS Unit		Approved	All
OBS Unit Filter Mode	Unit only	Scheduler	All
Project Type	All	Template	No
Project Category	All	Active	Yes
		Power Filter	[Build Power Filter]

	Project	Risk	Stage	Status	Gantt	Status Reports	Planned Cost	Mar 10	Apr 10	May 10	Jun 10	Jul 10	Aug 10
☑	Top Secret Telepathic Scanner	◇		◆			0						
Total							0						

Total Results: 1

Highlighted rows = Approved Flag Currency = USD

The access right is granted as illustrated below:



OBS Unit: Instance Access Rights (OBS: Corporate Department OBS | Unit: Special Projects)

Instance Access Rights Filter

Below are rights granted to resources in this OBS unit for specific object instances.

Access Right:

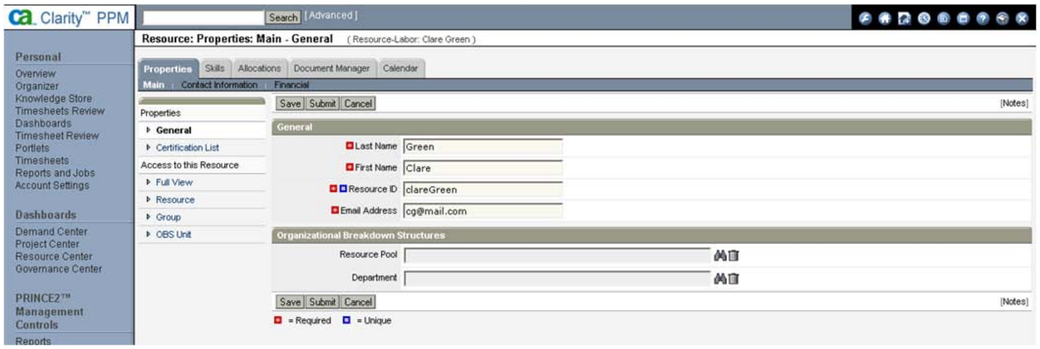
Description:

Object: All

	Access Right	Object	Description
☐	Project - View	Project	Allows user to view the general, management, financial and opportunity properties, custom defined fields, roster, tasks, processes and sub-projects for the project.

Confirmation

- Clare Green is not a member of the OBS Unit Special Projects. (Department field is blank)



Resource: Properties: Main - General (Resource-Labor: Clare Green)

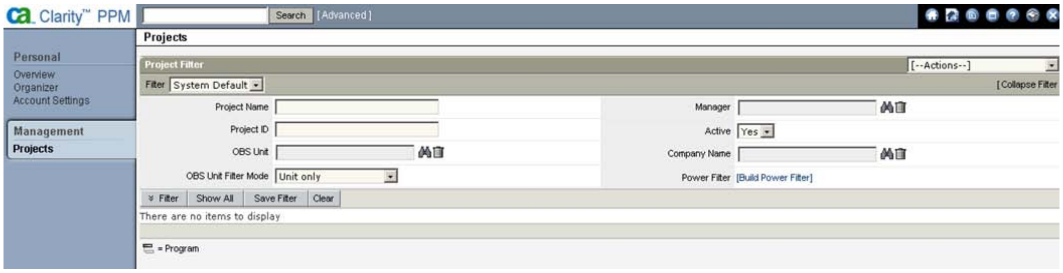
General

Last Name: Green
First Name: Clare
Resource ID: clareGreen
Email Address: cg@mail.com

Organizational Breakdown Structures

Resource Pool:
Department:

- She has no access to the Top Secret Telepathic Scanner project.



Projects

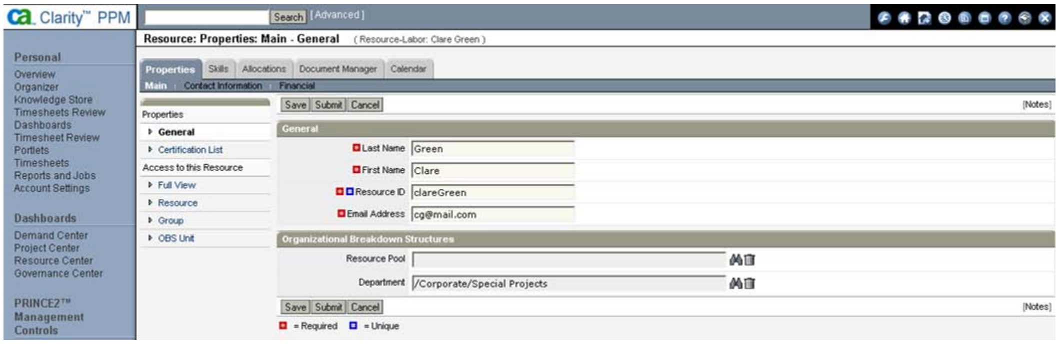
Project Filter

Filter: System Default

Project Name:
Project ID:
OBS Unit:
OBS Unit Filter Mode: Unit only
Manager:
Active: Yes
Company Name:
Power Filter: [Build Power Filter]

There are no items to display

- Now, Clare has been added to OBS Unit Special Projects.



Resource: Properties: Main - General (Resource-Labor: Clare Green)

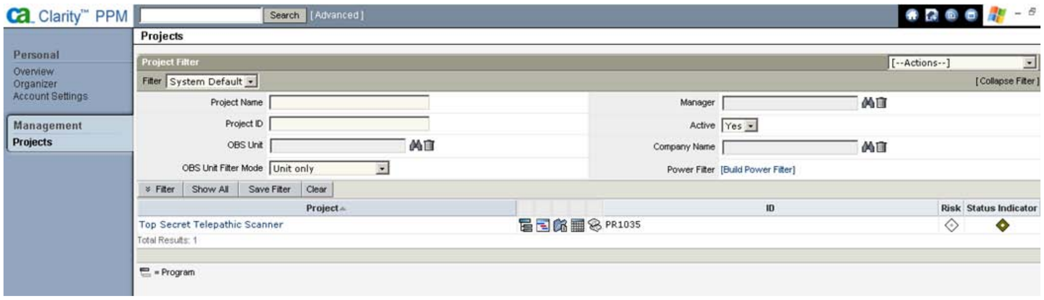
General

Last Name: Green
First Name: Clare
Resource ID: clareGreen
Email Address: cg@mail.com

Organizational Breakdown Structures

Resource Pool:
Department: /Corporate/Special Projects

- As a member of the group, she is given access for viewing the Top Secret Telepathic Scanner project.



Projects

Project Filter

Filter: System Default

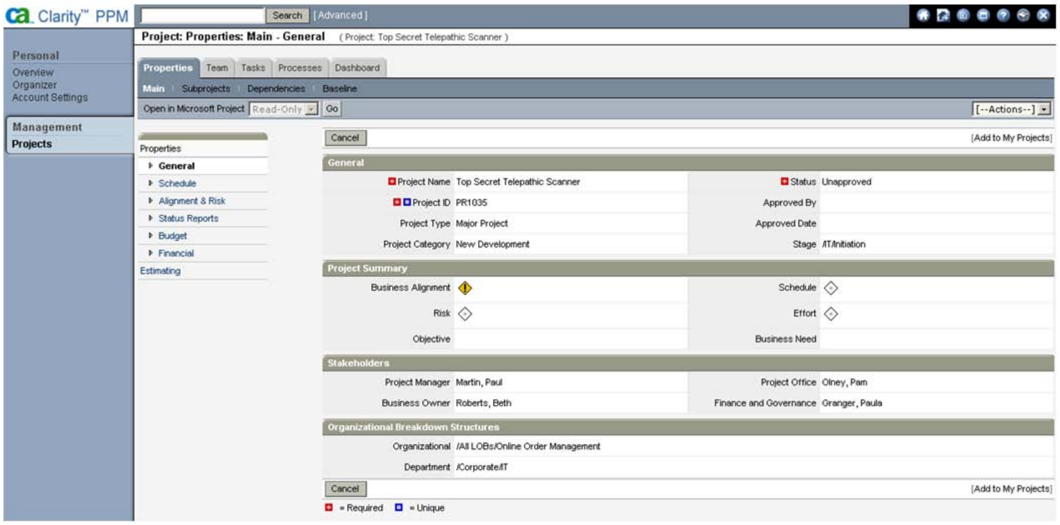
Project Name		Manager	
Project ID		Active	Yes
OBS Unit		Company Name	
OBS Unit Filter Mode	Unit only	Power Filter	[Build Power Filter]

Project	ID	Risk	Status Indicator
Top Secret Telepathic Scanner	PR1035	◇	◆

Total Results: 1

= Program

- She can view the project.



Project: Properties: Main - General (Project: Top Secret Telepathic Scanner)

Open in Microsoft Project: Read-Only

General

Project Name	Top Secret Telepathic Scanner	Status	Unapproved
Project ID	PR1035	Approved By	
Project Type	Major Project	Approved Date	
Project Category	New Development	Stage	/IT/Initiation

Project Summary

Business Alignment	◆	Schedule	◇
Risk	◇	Effort	◇
Objective		Business Need	

Stakeholders

Project Manager	Martin, Paul	Project Office	Olney, Pam
Business Owner	Roberts, Beth	Finance and Governance	Granger, Paula

Organizational Breakdown Structures

Organizational	/All LOBs/Online Order Management
Department	/Corporate/IT

🟥 = Required 🟦 = Unique

Granting OBS Unit Rights to OBS Unit Members

This option is used to grant OBS Unit members with access to all instances of an object which are related to an OBS Unit, or its ancestors and descendants.

Important! Security has three key elements: Actors, Actions, and Scope. It is important to remember the key elements as this example uses one OBS Unit to determine the Actors and another OBS Unit to determine the Scope. In the real world, the Units could be from different OBS Structures.

Use Case

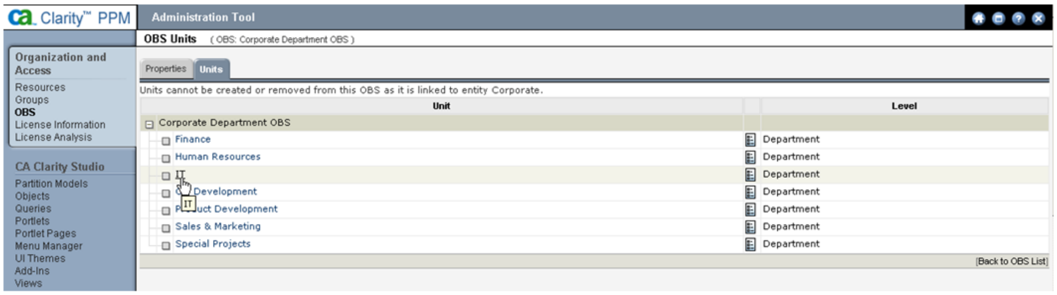
The first OBS is mapped to company departments, and named Corporate Departments OBS. A second OBS is used to separate resource groups for allocation, and named Resource Pool. All resources from the IT department should have access to viewing resource information (including Booking information) on the resources that are in the IT – Internal resource pool.

Setting Up

- The Actors are the members of the IT department, represented by the IT Unit in the Corporate Departments OBS.
- The Action is viewing resource and booking information about the IT-Internal resource pool.
- The Scope is comprised of all resources related to the IT - Internal unit in the Resource Pool OBS.

Review the Current Access Rights

1. Navigate to the OBS Units page to view the list of available department units in the OBS to view the OBS structure.



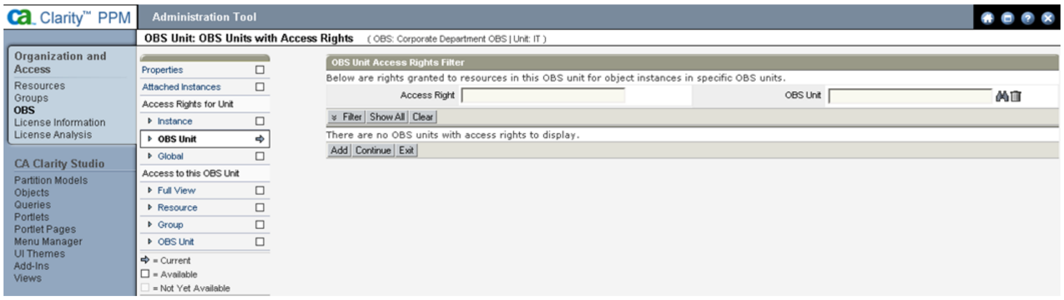
OBS Units (OBS: Corporate Department OBS)

Units cannot be created or removed from this OBS as it is linked to entity Corporate.

Unit	Level
⊟ Corporate Department OBS	
□ Finance	Department
□ Human Resources	Department
□ IT	Department
□ [illegible] Development	Department
□ Product Development	Department
□ Sales & Marketing	Department
□ Special Projects	Department

2. Select the IT Department Unit.

3. Click OBS Unit under *Access Rights for Unit* of the IT OBS Unit. As illustrated in the following graphic, the unit members do not have any OBS Unit-related access rights.



OBS Unit: OBS Units with Access Rights (OBS: Corporate Department OBS | Unit: IT)

OBS Unit Access Rights Filter

Below are rights granted to resources in this OBS unit for object instances in specific OBS units.

Access Right

OBS Unit

There are no OBS units with access rights to display.

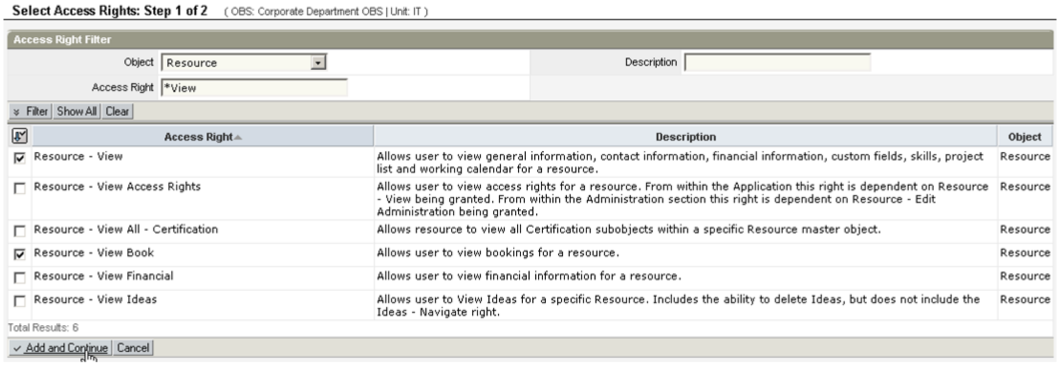
Select and Grant Access Rights

1. Click Add on the OBS Units: OBS Units with Access Rights page to begin selecting the access rights.

   – Select the Access Rights. Use the filter function to narrow down the search. You can select multiple access rights by using the checkboxes to the left.

   – Select Resource – View and Resource – View Book access rights. These are the Actions for this example.

   – Click Add and Continue.



Select Access Rights: Step 1 of 2 (OBS: Corporate Department OBS | Unit: IT)

Access Right Filter

Object: Resource

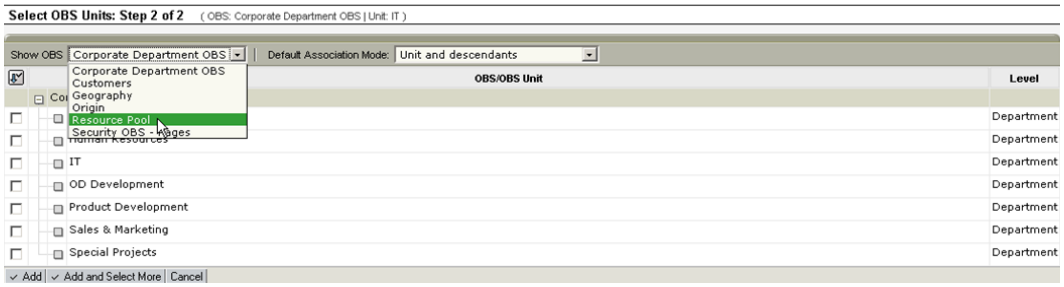
Description:

Access Right: *View

	Access Right	Description	Object
☑	Resource - View	Allows user to view general information, contact information, financial information, custom fields, skills, project list and working calendar for a resource.	Resource
☐	Resource - View Access Rights	Allows user to view access rights for a resource. From within the Application this right is dependent on Resource - View being granted. From within the Administration section this right is dependent on Resource - Edit Administration being granted.	Resource
☐	Resource - View All - Certification	Allows resource to view all Certification subobjects within a specific Resource master object.	Resource
☑	Resource - View Book	Allows user to view bookings for a resource.	Resource
☐	Resource - View Financial	Allows user to view financial information for a resource.	Resource
☐	Resource - View Ideas	Allows user to View Ideas for a specific Resource. Includes the ability to delete Ideas, but does not include the Ideas - Navigate right.	Resource

Total Results: 6

2. Next select the Scope - the desired OBS Unit. In this case, Resource Pool is the OBS related to the scope, not Corporate Departments OBS. You select a different OBS using the Show OBS attribute as illustrated in the following graphic:



Select OBS Units: Step 2 of 2 (OBS: Corporate Department OBS | Unit: IT)

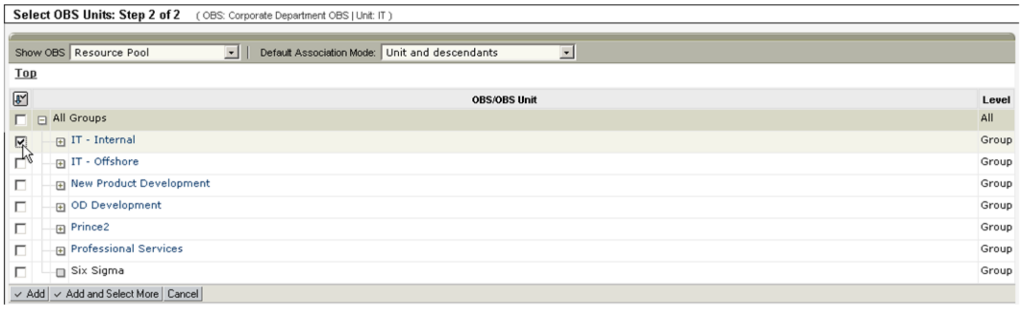
Show OBS: Corporate Department OBS | Default Association Mode: Unit and descendants

☐	OBS/OBS Unit	Level
	⊟ Co	
☐		Department
☐	Human Resources	Department
☐	IT	Department
☐	OD Development	Department
☐	Product Development	Department
☐	Sales & Marketing	Department
☐	Special Projects	Department

- Select the Resource Pool: IT - Internal unit.

- Click Add to grant the IT OBS Unit members access rights using the Resource Pool as the Scope delimiter.

  Note: You can select multiple units at a time. Use Add and Select More to keep filtering and adding units if necessary.



Select OBS Units: Step 2 of 2 (OBS: Corporate Department OBS | Unit: IT)

Show OBS: Resource Pool | Default Association Mode: Unit and descendants

Top

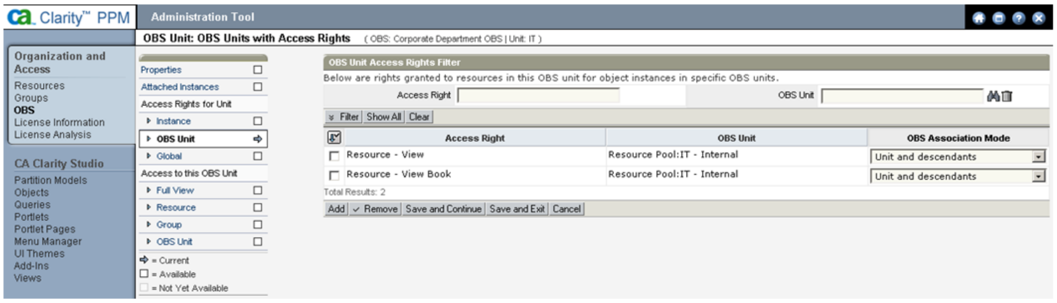
☐	OBS/OBS Unit	Level
☐	⊟ All Groups	All
☑	⊞ IT - Internal	Group
☐	⊞ IT - Offshore	Group
☐	⊞ New Product Development	Group
☐	⊞ OD Development	Group
☐	⊞ Prince2	Group
☐	⊞ Professional Services	Group
☐	Six Sigma	Group

3. Use the OBS Association Mode attribute to define whether the IT – department members should have access to that unit only, or include its ancestors, or its descendants.

   - In this case, use the default value: unit and descendants.

   - If sub-units exist under the IT - Internal resource pool, and resources are related to those lower-level units, they should also be considered as part of IT - Internal.

   - The IT department members are granted access to the sub-units.



OBS Unit: OBS Units with Access Rights (OBS: Corporate Department OBS | Unit: IT)

OBS Unit Access Rights Filter

Below are rights granted to resources in this OBS unit for object instances in specific OBS units.

Access Right

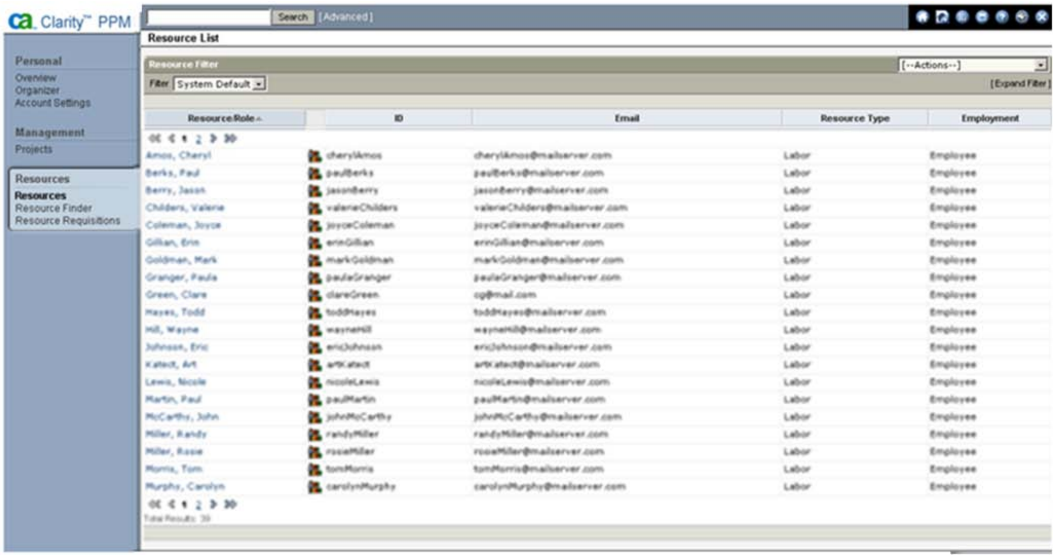
OBS Unit

	Access Right	OBS Unit	OBS Association Mode
□	Resource - View	Resource Pool:IT - Internal	Unit and descendants
□	Resource - View Book	Resource Pool:IT - Internal	Unit and descendants

Total Results: 2

Confirmation

A fictitious resource, Tom Spark, a member of the IT department logs in to the system. Tom sees all resources included in the IT - Internal OBS Unit and its lower-level units in the Resource List.



Resource List

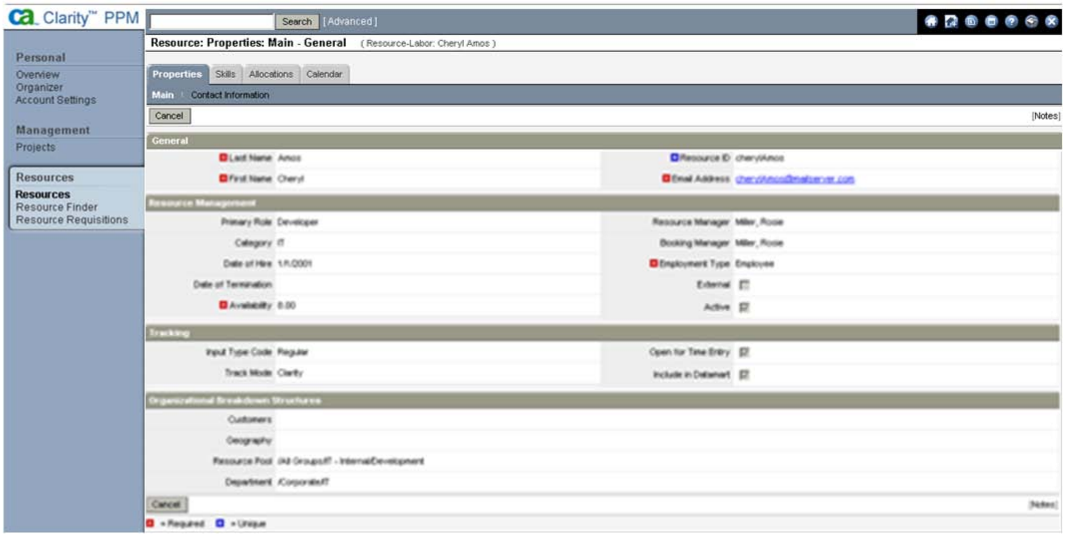
Resource Filter

Filter: System Default

Resource/Role	ID	Email	Resource Type	Employment
Amos, Cheryl	cherylAmos	cherylAmos@mailserver.com	Labor	Employee
Berks, Paul	paulBerks	paulBerks@mailserver.com	Labor	Employee
Berry, Jason	jasonBerry	jasonBerry@mailserver.com	Labor	Employee
Childers, Valerie	valerieChilders	valerieChilders@mailserver.com	Labor	Employee
Coleman, Joyce	joyceColeman	joyceColeman@mailserver.com	Labor	Employee
Gillian, Erin	erinGillian	erinGillian@mailserver.com	Labor	Employee
Goldman, Mark	markGoldman	markGoldman@mailserver.com	Labor	Employee
Granger, Paula	paulaGranger	paulaGranger@mailserver.com	Labor	Employee
Green, Clare	clareGreen	cg@mail.com	Labor	Employee
Hayes, Todd	toddHayes	toddHayes@mailserver.com	Labor	Employee
Hill, Wayne	wayneHill	wayneHill@mailserver.com	Labor	Employee
Johnson, Eric	ericJohnson	ericJohnson@mailserver.com	Labor	Employee
Katect, Art	artKatect	artKatect@mailserver.com	Labor	Employee
Lewis, Nicole	nicoleLewis	nicoleLewis@mailserver.com	Labor	Employee
Martin, Paul	paulMartin	paulMartin@mailserver.com	Labor	Employee
McCarthy, John	johnMcCarthy	johnMcCarthy@mailserver.com	Labor	Employee
Miller, Randy	randyMiller	randyMiller@mailserver.com	Labor	Employee
Miller, Rosie	rosieMiller	rosieMiller@mailserver.com	Labor	Employee
Morris, Tom	tomMorris	tomMorris@mailserver.com	Labor	Employee
Murphy, Carolyn	carolynMurphy	carolynMurphy@mailserver.com	Labor	Employee

Total Results: 39

He has View access to all of them, including the allocation information.



Resource: Properties: Main - General (Resource-Labor: Cheryl Amos)

General

Last Name	Amos	Resource ID	cherylAmos
First Name	Cheryl	Email Address	cherylAmos@mailserver.com

Resource Management

Primary Role	Developer	Resource Manager	Miller, Rosie
Category	IT	Booking Manager	Miller, Rosie
Date of Hire	1/1/2001	Employment Type	Employee
Date of Termination		External	☐
Availability	8.00	Active	☑

Tracking

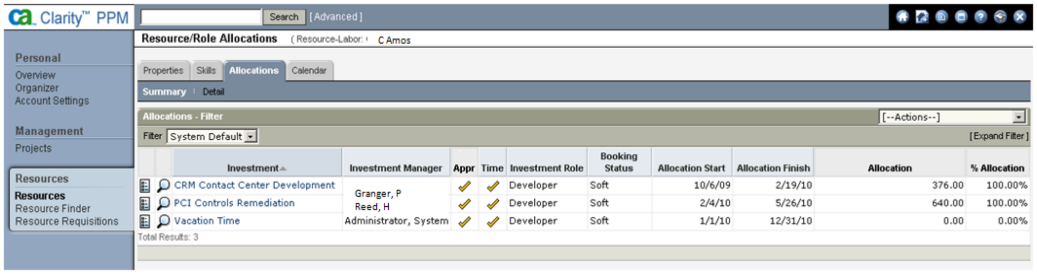
Input Type Code	Regular	Open for Time Entry	☑
Track Mode	Clarity	Include in Datamart	☑

Organizational Breakdown Structures

Customers	
Geography	
Resource Pool	/All Groups/IT - Internal/Development
Department	/Corporate/IT

🟥 = Required 🟦 = Unique

Important! Access to the Resources pages is granted through a Global Access Right Resource – Navigate. See the topic Granting Global rights to Members of an OBS Unit for information about how to grant that access.



Resource/Role Allocations (Resource-Labor: C Amos

Allocations - Filter

Filter System Default

Investment	Investment Manager	Appr	Time	Investment Role	Booking Status	Allocation Start	Allocation Finish	Allocation	% Allocation
CRM Contact Center Development	Granger, P	✓	✓	Developer	Soft	10/6/09	2/19/10	376.00	100.00%
PCI Controls Remediation	Reed, H	✓	✓	Developer	Soft	2/4/10	5/26/10	640.00	100.00%
Vacation Time	Administrator, System	✓	✓	Developer	Soft	1/1/10	12/31/10	0.00	0.00%

Total Results: 3

Grant Global Rights to Members of an OBS Unit

This option is used to grant OBS Unit members with Global Access Rights.

Use Case

Members of the IT department need to be able to navigate to the Resource pages so they can view resource information.

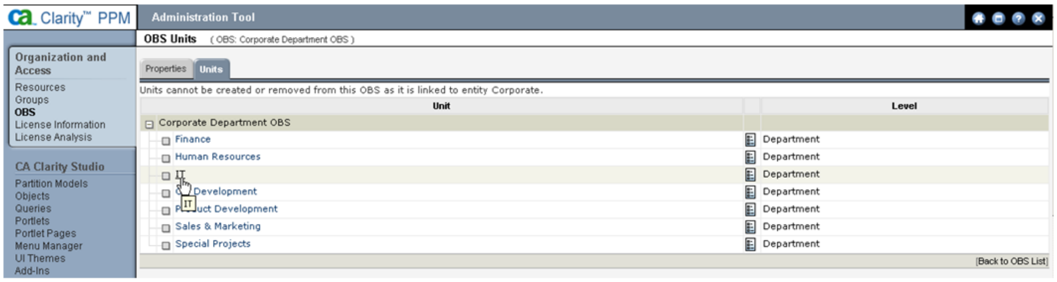
Setting Up

- The Actors are the members of Unit IT of OBS *Corporate Departments OBS*.
- The Action is navigating to the Resources pages (Resource - Navigate access right)
- The Scope is the information contained on Resource pages.

Review the Current Access Rights

1. Navigate to the OBS Units page to view the list of available department units in the OBS.

2. Select the IT department OBS unit.



OBS Units (OBS: Corporate Department OBS)

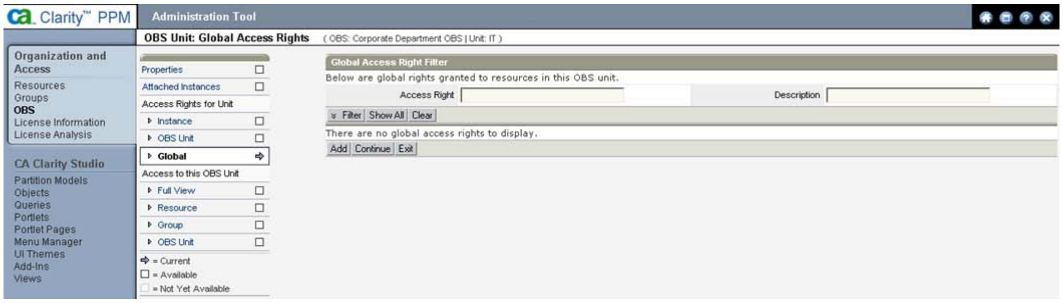
Units cannot be created or removed from this OBS as it is linked to entity Corporate.

Unit	Level
Corporate Department OBS	
Finance	Department
Human Resources	Department
IT	Department
Development	Department
Product Development	Department
Sales & Marketing	Department
Special Projects	Department

3. Click Global under Access Rights for Unit to view the Global Access Rights that the unit members have. In this case, there are none.

Select and Grant Access Rights

1. Click Add to begin the process of adding access rights to the IT OBS unit members. Use the filter to narrow the search to the access right: Resource – Navigate.


OBS Unit: Global Access Rights (OBS: Corporate Department OBS | Unit: IT)

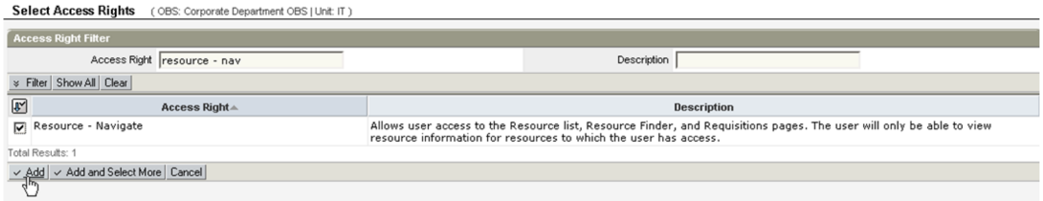
Global Access Right Filter

Below are global rights granted to resources in this OBS unit.

Access Right: Description:

There are no global access rights to display.

2. Select this item using the checkbox to the left and click Add.


Select Access Rights (OBS: Corporate Department OBS | Unit: IT)

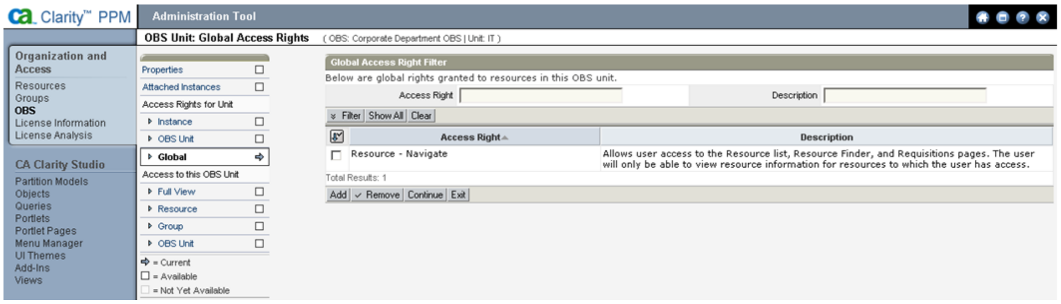
Access Right Filter

Access Right: resource - nav   Description:

	Access Right	Description
☑	Resource - Navigate	Allows user access to the Resource list, Resource Finder, and Requisitions pages. The user will only be able to view resource information for resources to which the user has access.

Total Results: 1

The Global Access Right Resource – Navigate is granted to members of the IT OBS Unit.


OBS Unit: Global Access Rights (OBS: Corporate Department OBS | Unit: IT)

Global Access Right Filter

Below are global rights granted to resources in this OBS unit.

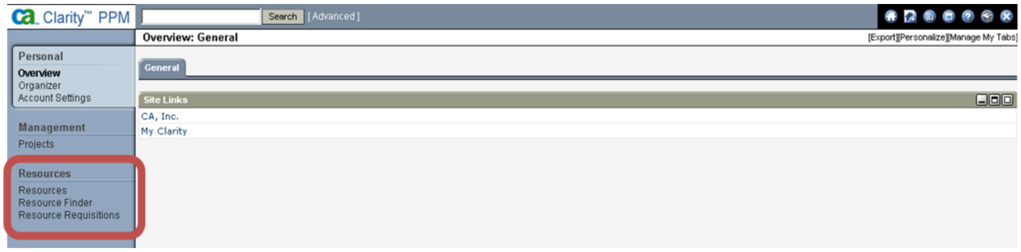
Access Right: Description:

	Access Right	Description
□	Resource - Navigate	Allows user access to the Resource list, Resource Finder, and Requisitions pages. The user will only be able to view resource information for resources to which the user has access.

Total Results: 1

Confirmation

A fictitious resource, Tom Sparks is a member of the IT OBS Unit. When Tom accesses CA Clarity PPM, he sees the Resource Pages are available to him.


Overview: General

Site Links

CA, Inc.

My Clarity

How to Grant Access to Resources

Granting Access Rights directly to resources is not considered to be a good practice because it may result in significant maintenance for replacing a resource that has left the company or simply changed departments.

Granting access is useful in some specific cases, such as securing projects with sensitive data or confidential projects.

Many companies do not want resources who are members of a group, department, or organization unit to automatically Inherit access to specific projects classified as sensitive or confidential. In this case, granting access rights through Groups or OBS Units is not the best option. Access to those specific projects may be granted using Resource Access Rights, to provide a higher level of control of the sensitive or confidential data.

Granting Instance Rights Directly to Resources

Use this option to grant individual resources with access rights to specific object instances.

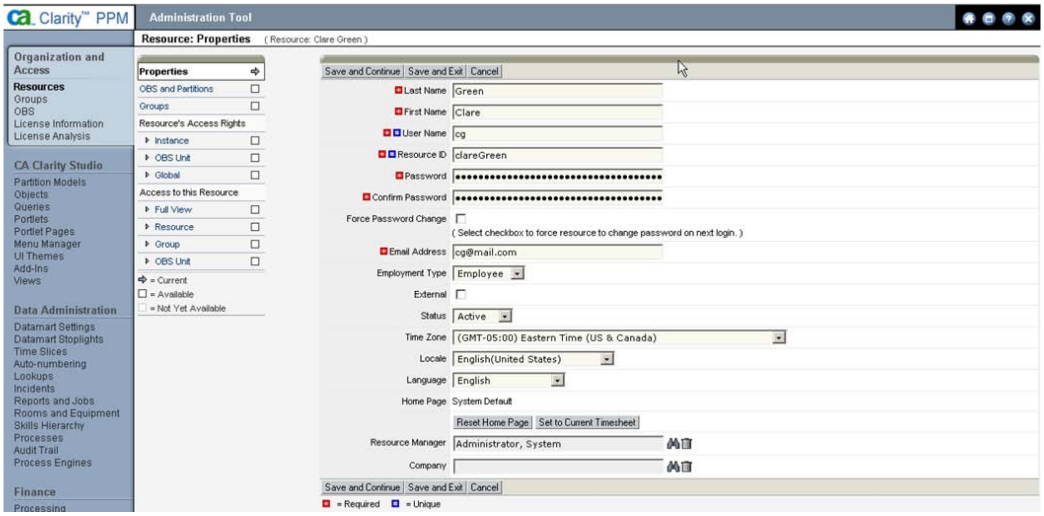
Use Case

> A resource must be granted access to view information from the Top Secret Telepathic Scanner project. Members of the same groups or units as this particular resource should NOT be granted the same access.

Setting up

- The Actor (Who) in this example is Clare Green, a fictitious resource.
- The Action (What) is Project –View access.
- The Scope (Which Data) is one specific instance of a project: the Top Secret Telepathic Scanner project.

Resource properties for this resource are illustrated in the following graphic:



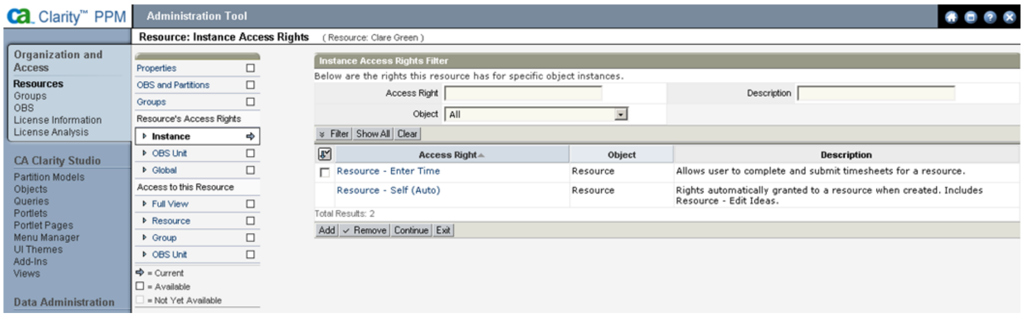
Resource: Properties (Resource: Clare Green)

🟥 Last Name	Green
🟥 First Name	Clare
🟥🟦 User Name	cg
🟥🟦 Resource ID	clareGreen
🟥 Password	••••••••••••••••••••••••••••••••••••
🟥 Confirm Password	••••••••••••••••••••••••••••••••••••
Force Password Change	□ (Select checkbox to force resource to change password on next login.)
🟥 Email Address	cg@mail.com
Employment Type	Employee
External	□
Status	Active
Time Zone	(GMT-05:00) Eastern Time (US & Canada)
Locale	English(United States)
Language	English
Home Page	System Default
Resource Manager	Administrator, System
Company	

🟥 = Required 🟦 = Unique

Review the Current Access Rights

Click Instance under Resource Access Rights to view the Access Rights granted directly to this resource.



Resource: Instance Access Rights (Resource: Clare Green)

Instance Access Rights Filter

Below are the rights this resource has for specific object instances.

Access Right
Description
Object: All

	Access Right	Object	Description
□	Resource - Enter Time	Resource	Allows user to complete and submit timesheets for a resource.
	Resource - Self (Auto)	Resource	Rights automatically granted to a resource when created. Includes Resource - Edit Ideas.

Total Results: 2

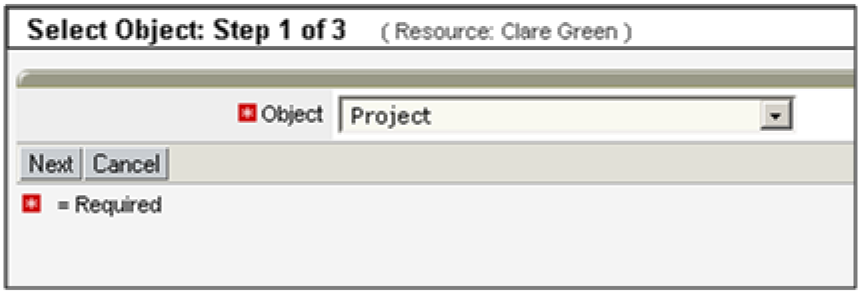
Clare Green is granted Resource – Enter Time and Resource – Self (Auto) access rights. These access rights were granted automatically when the resource record was created.

Select and Grant Access Rights

1. Click Add to grant the access rights for the Top Secret Telepathic Scanner project.

   – Select the object. For this example, the object is Project.

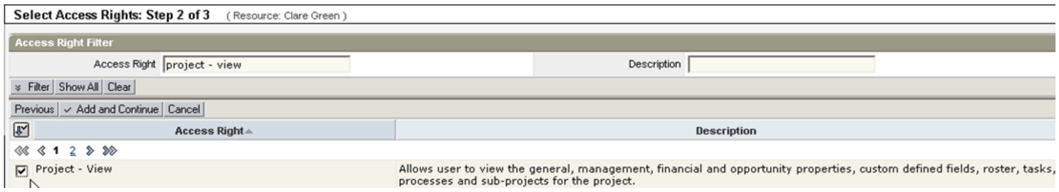
   – Click Next.



Select Object: Step 1 of 3 (Resource: Clare Green)

Object: Project

2. Select the access right. For this example, select the Access Right named Project – View. Click Add and Continue.



Select Access Rights: Step 2 of 3 (Resource: Clare Green)

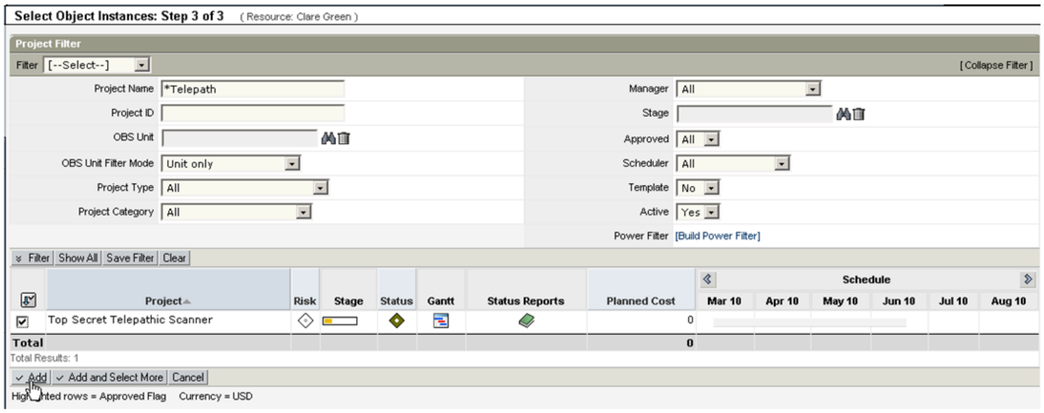
Access Right Filter

Access Right: project - view

Description:

	Access Right	Description
☑	Project - View	Allows user to view the general, management, financial and opportunity properties, custom defined fields, roster, tasks, processes and sub-projects for the project.

3. Select the Project instance Top Secret Telepathic Scanner, and click Add.



Select Object Instances: Step 3 of 3 (Resource: Clare Green)

Project Filter

Filter [--Select--] [Collapse Filter]

Project Name	*Telepath	Manager	All
Project ID		Stage	
OBS Unit		Approved	All
OBS Unit Filter Mode	Unit only	Scheduler	All
Project Type	All	Template	No
Project Category	All	Active	Yes
		Power Filter	[Build Power Filter]

Filter | Show All | Save Filter | Clear

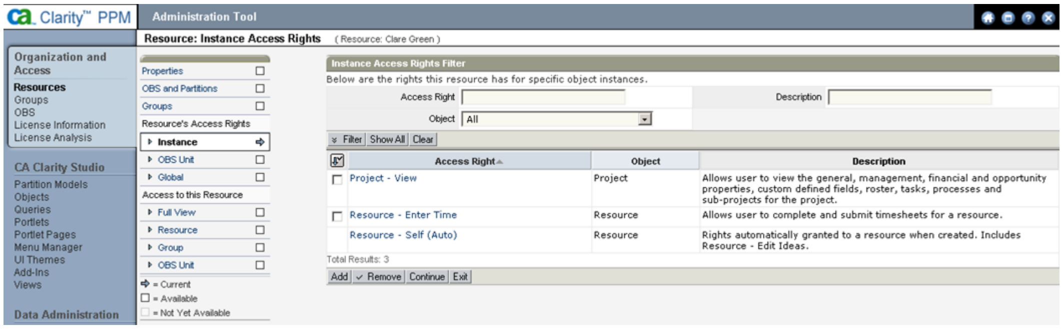
	Project	Risk	Stage	Status	Gantt	Status Reports	Planned Cost	Mar 10	Apr 10	May 10	Jun 10	Jul 10	Aug 10
☑	Top Secret Telepathic Scanner	◇		◆			0						
Total							0						

Total Results: 1

Add | Add and Select More | Cancel

Highlighted rows = Approved Flag Currency = USD

The access right is granted to the resource for the specific project.



Resource: Instance Access Rights (Resource: Clare Green)

Instance Access Rights Filter

Below are the rights this resource has for specific object instances.

Access Right		Description	
Object	All		

Filter | Show All | Clear

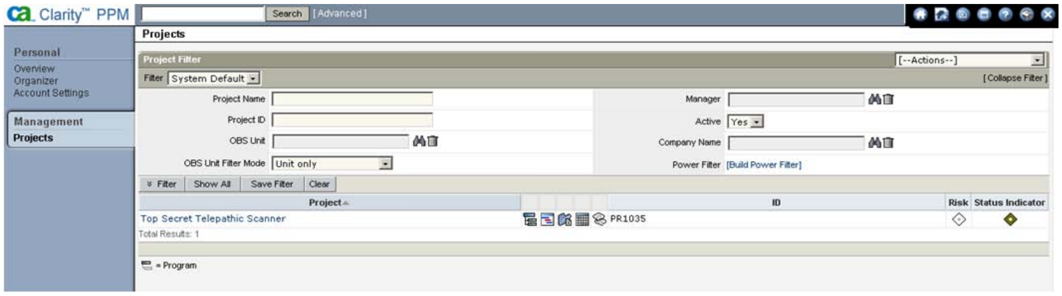
	Access Right	Object	Description
□	Project - View	Project	Allows user to view the general, management, financial and opportunity properties, custom defined fields, roster, tasks, processes and sub-projects for the project.
□	Resource - Enter Time	Resource	Allows user to complete and submit timesheets for a resource.
	Resource - Self (Auto)	Resource	Rights automatically granted to a resource when created. Includes Resource - Edit Ideas.

Total Results: 3

Add | Remove | Continue | Exit

Confirmation

- Before receiving access, Clare Green could not view the project Top Secret Telepathy Scanner.
- Now, Clare is granted access.



Projects

Project Filter [--Actions--]

Filter System Default [Collapse Filter]

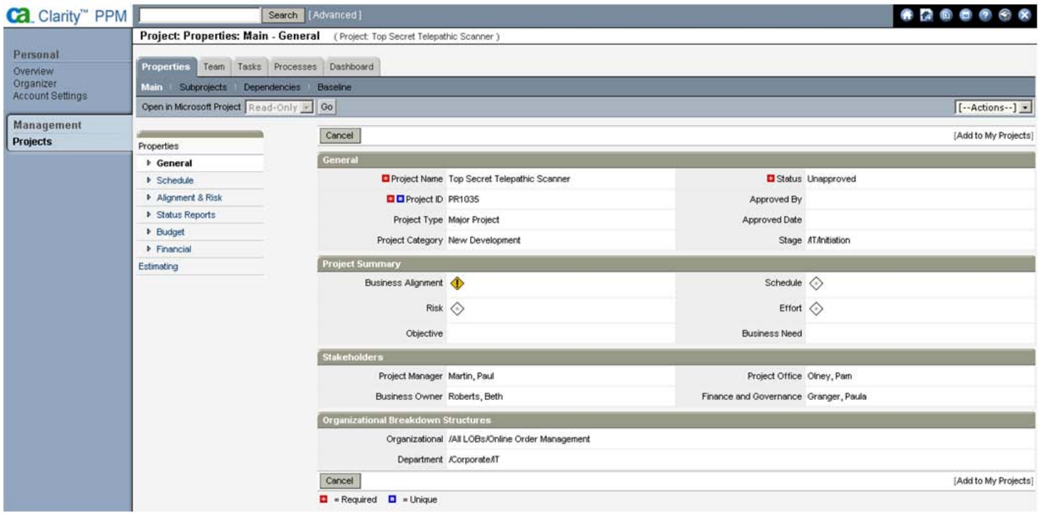
Project Name		Manager	
Project ID		Active	Yes
OBS Unit		Company Name	
OBS Unit Filter Mode	Unit only	Power Filter	[Build Power Filter]

Filter | Show All | Save Filter | Clear

Project	ID	Risk	Status Indicator
Top Secret Telepathic Scanner	PR1035	◇	◆

Total Results: 1

- Clare can view the project.



Project: Properties: Main - General (Project: Top Secret Telepathic Scanner)

General

Project Name	Top Secret Telepathic Scanner	Status	Unapproved
Project ID	PR1035	Approved By	
Project Type	Major Project	Approved Date	
Project Category	New Development	Stage	/IT/Initiation

Project Summary

Business Alignment	◆	Schedule	◇
Risk	◇	Effort	◇
Objective		Business Need	

Stakeholders

Project Manager	Martin, Paul	Project Office	Olney, Pam
Business Owner	Roberts, Beth	Finance and Governance	Granger, Paula

Organizational Breakdown Structures

Organizational	/All LOBs/Online Order Management
Department	/Corporate/IT

🟥 = Required 🟦 = Unique

Granting OBS Unit Rights to Individual Resources

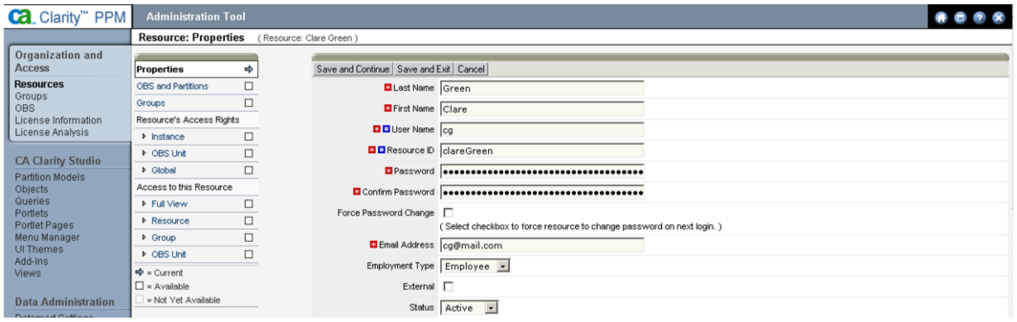
This option is used to grant individual resources with access to all instances of an object which are related to an OBS Unit, or its ancestors and descendants.

Use Case

> A resource must be granted access to view information from all Projects related to the Special Projects OBS Unit. These are confidential projects and access to them should be granted on a resource-by-resource, need-to-see basis only.

Setting Up

- The Actor is Clare Green.
- The Action is Clare can access and View information for all instances of the projects related to the Special Projects OBS unit. Other team members with access to the Special Projects OBS do not have this level of access unless it is specifically granted to them.
- The Scope comprises of all projects related to the Special Projects unit in the OBS *Corporate Departments OBS*.

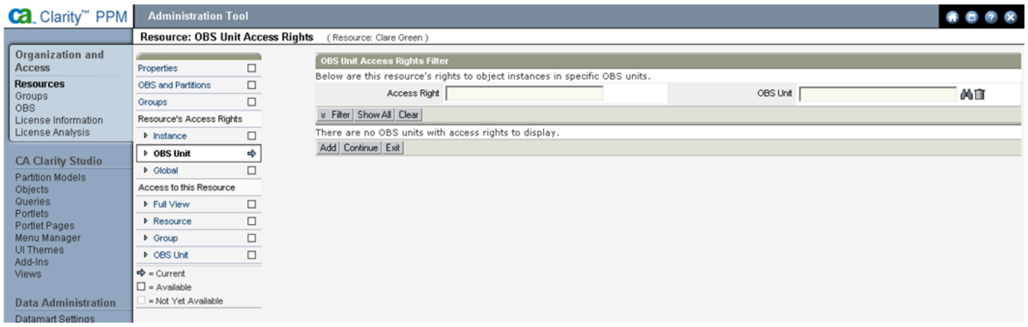


Resource: Properties (Resource: Clare Green)

Last Name	Green
First Name	Clare
User Name	cg
Resource ID	clareGreen
Password	••••••••••••••••••••••••••••••••••••
Confirm Password	••••••••••••••••••••••••••••••••••••
Force Password Change	□ (Select checkbox to force resource to change password on next login.)
Email Address	cg@mail.com
Employment Type	Employee
External	□
Status	Active

Review the Current Access Rights

Click OBS Unit under Resource Access Rights to grant Clare access rights using that OBS as the Scope delimiter. Clare does not have any OBS Unit-related access rights as illustrated in the following graphic.



Resource: OBS Unit Access Rights (Resource: Clare Green)

OBS Unit Access Rights Filter

Below are this resource's rights to object instances in specific OBS units.

Access Right

OBS Unit

There are no OBS units with access rights to display.

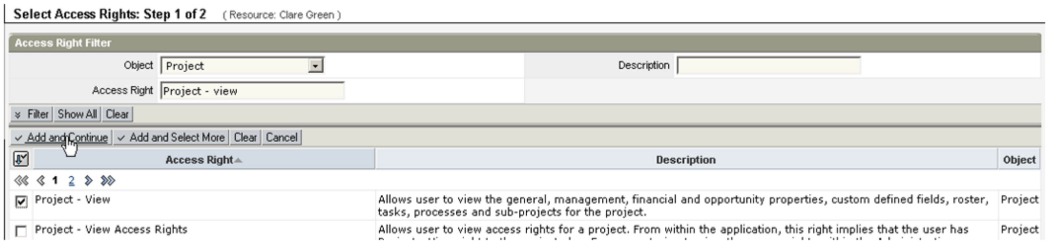
Select and Grant Access Rights

1. Click Add on the Resource: OBS Unit Access Rights page to begin selecting the access rights.

   – Use the filter function to narrow down the search. You can select multiple access rights by using the checkboxes to the left.

   – For this example, select the Project – View access right.

   – Click Add and Continue.



Select Access Rights: Step 1 of 2 (Resource: Clare Green)

Access Right Filter

Object: Project

Access Right: Project - view

Description:

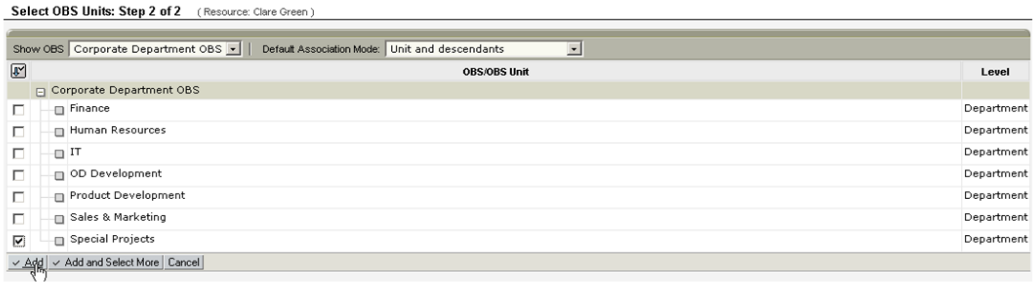
	Access Right	Description	Object
☑	Project - View	Allows user to view the general, management, financial and opportunity properties, custom defined fields, roster, tasks, processes and sub-projects for the project.	Project
□	Project - View Access Rights	Allows user to view access rights for a project. From within the application, this right implies that the user has	Project

2. Select the Scope - the desired OBS Unit. You select a different OBS using the Show OBS attribute.

   - For this example, select the Special Projects unit in the OBS Corporate Departments OBS.

   - Click Add.

     Note: You can select multiple units at a time. Use Add and Select More to keep filtering and adding units if necessary.



Select OBS Units: Step 2 of 2 (Resource: Clare Green)

Show OBS: Corporate Department OBS | Default Association Mode: Unit and descendants

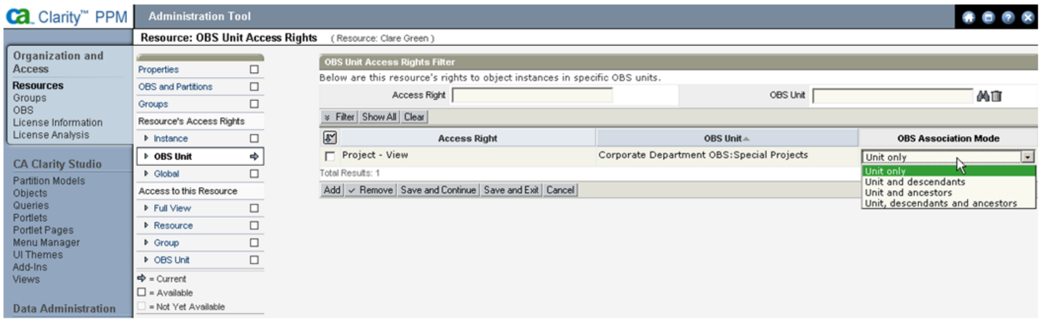
	OBS/OBS Unit	Level
	⊟ Corporate Department OBS	
□	Finance	Department
□	Human Resources	Department
□	IT	Department
□	OD Development	Department
□	Product Development	Department
□	Sales & Marketing	Department
☑	Special Projects	Department

3. Use the OBS Association Mode attribute to define whether Clare Green should have access to only the unit, its ancestors, or its descendants.

   - In this case, restrict access to the unit itself: Unit only. If sub-units exist under Special Projects, such as Administration, and projects are related to those lower-level units, they are NOT considered as part of Special Projects.

   - Clare Green is not granted access to the sub-units.

   - Click Save and Exit.



Resource: OBS Unit Access Rights (Resource: Clare Green)

OBS Unit Access Rights Filter

Below are this resource's rights to object instances in specific OBS units.

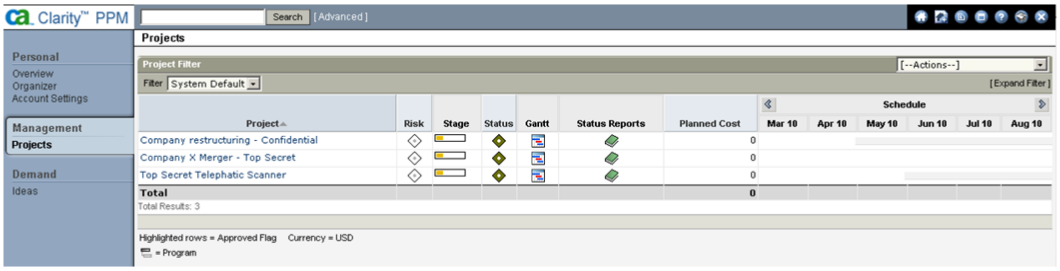
Access Right: | OBS Unit:

	Access Right	OBS Unit	OBS Association Mode
□	Project - View	Corporate Department OBS:Special Projects	Unit only

Total Results: 1

Confirmation

- Clare Green logs in to the system. She sees three projects in the Project List pertaining to the Special Projects OBS Unit.



Projects

Filter System Default

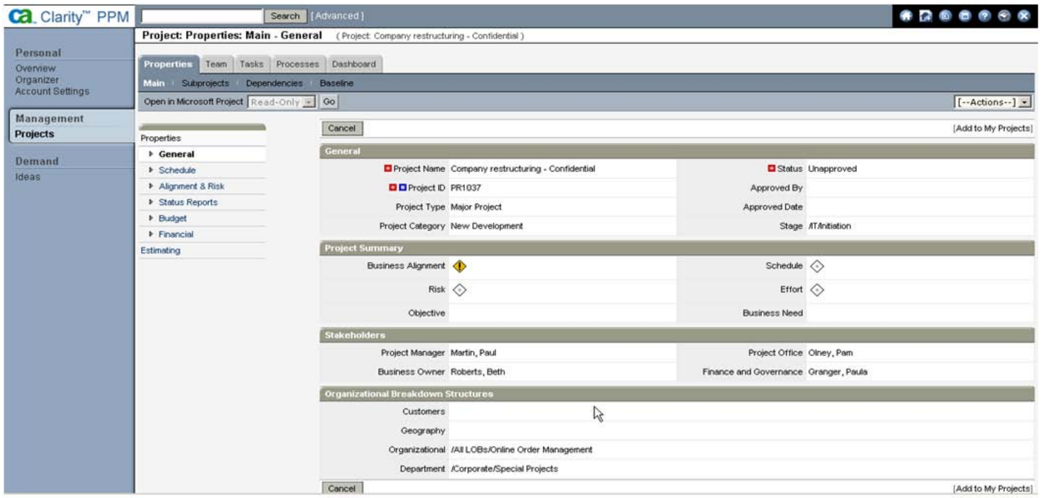
Project	Risk	Stage	Status	Gantt	Status Reports	Planned Cost	Schedule					
							Mar 10	Apr 10	May 10	Jun 10	Jul 10	Aug 10
Company restructuring - Confidential	◇	▭	◆	▤	◈	0						
Company X Merger - Top Secret	◇	▭	◆	▤	◈	0						
Top Secret Telephatic Scanner	◇	▭	◆	▤	◈	0						
Total						0						

Total Results: 3

Highlighted rows = Approved Flag Currency = USD

▤ = Program

- Clare has View access to all of them. She does not have access to the subunit Administration, and therefore, does not see any projects for that subunit.



Project: Properties: Main - General (Project: Company restructuring - Confidential)

Open in Microsoft Project Read-Only

General

Project Name Company restructuring - Confidential
Status Unapproved
Project ID PR1037
Approved By
Project Type Major Project
Approved Date
Project Category New Development
Stage /IT/Initiation

Project Summary

Business Alignment ◆
Schedule ◇
Risk ◇
Effort ◇
Objective
Business Need

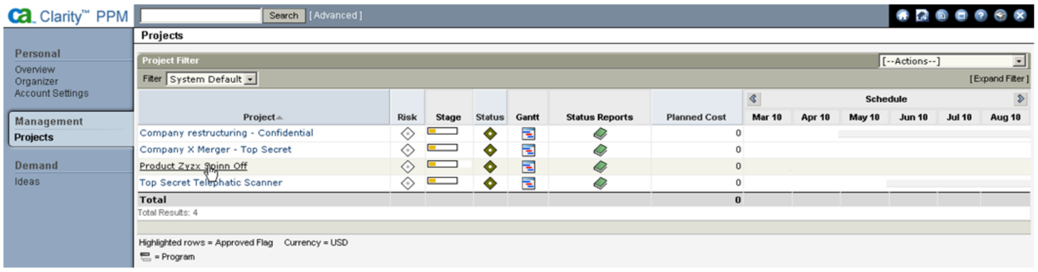
Stakeholders

Project Manager Martin, Paul
Project Office Olney, Pam
Business Owner Roberts, Beth
Finance and Governance Granger, Paula

Organizational Breakdown Structures

Customers
Geography
Organizational /All LOBs/Online Order Management
Department /Corporate/Special Projects

- When new projects are added to the Special Projects OBS Unit, Clare can see them automatically.



Projects

Filter System Default

Project	Risk	Stage	Status	Gantt	Status Reports	Planned Cost	Schedule					
							Mar 10	Apr 10	May 10	Jun 10	Jul 10	Aug 10
Company restructuring - Confidential	◇	▭	◆	▤	◈	0						
Company X Merger - Top Secret	◇	▭	◆	▤	◈	0						
Product Zyzx Spinn Off	◇	▭	◆	▤	◈	0						
Top Secret Telephatic Scanner	◇	▭	◆	▤	◈	0						
Total						0						

Total Results: 4

Highlighted rows = Approved Flag Currency = USD

▤ = Program

Granting Global Rights to Individual Resources

This option is used to grant individual resources with Global Access Rights.

Use Case

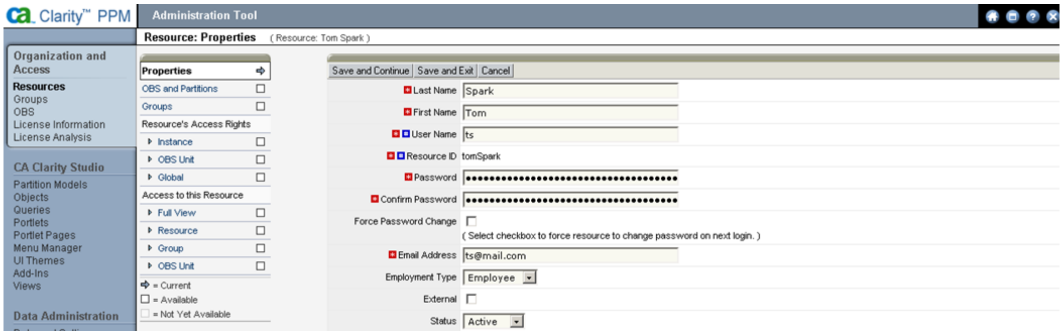
A resource has been promoted to Master Resource Manager. As part of the new responsibilities for this job assignment, the resource should be able to create resources in CA Clarity PPM.

Setting Up

- The Actor - Tom Spark, a fictitious resource
- The Action - Tom has Global Access Rights to create resources in CA Clarity PPM.
- The Scope - all OBS units that Tom may need to access to perform the create task.

Review the Current Access Rights

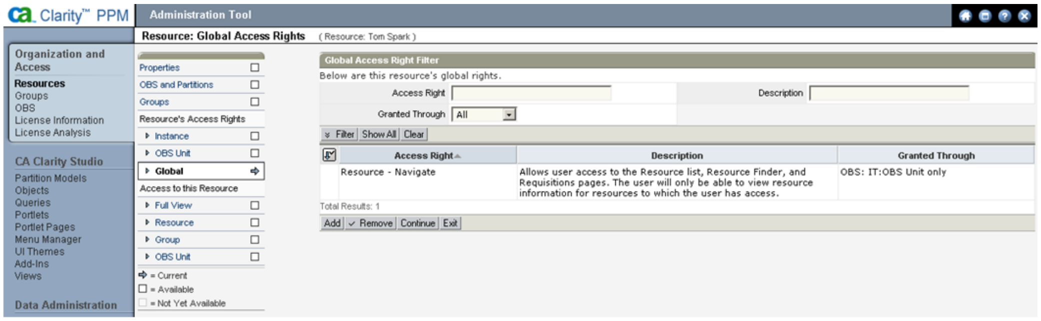
1. Navigate to the resource record for Tom Sparks in CA Clarity PPM using the Administration Tool.
2. Click Global under Resource Access Rights to view all the current Global rights Tom currently has.



Resource: Properties (Resource: Tom Spark)

Last Name: Spark
First Name: Tom
User Name: ts
Resource ID: tomSpark
Password: ••••••••••••••••••••••••••••••••••••
Confirm Password: ••••••••••••••••••••••••••••••••••••
Force Password Change: □
(Select checkbox to force resource to change password on next login.)
Email Address: ts@mail.com
Employment Type: Employee
External: □
Status: Active

Tom has Resource – Navigate. This was inherited from the OBS Unit he is a member of IT.



Resource: Global Access Rights (Resource: Tom Spark)

Global Access Right Filter

Below are this resource's global rights.

Access Right:
Description:
Granted Through: All

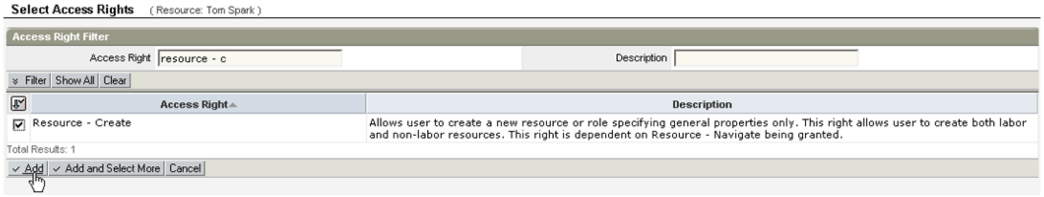
Access Right	Description	Granted Through
Resource - Navigate	Allows user access to the Resource list, Resource Finder, and Requisitions pages. The user will only be able to view resource information for resources to which the user has access.	OBS: IT:OBS Unit only

Total Results: 1

Select and Grant Access Rights

1. Click Add to add more access rights to this resource. Use the filter function to narrow the search and locate the access right: Resource – Create.

2. Select the item using the checkbox to the left and click Add.



Select Access Rights (Resource: Tom Spark)

Access Right Filter

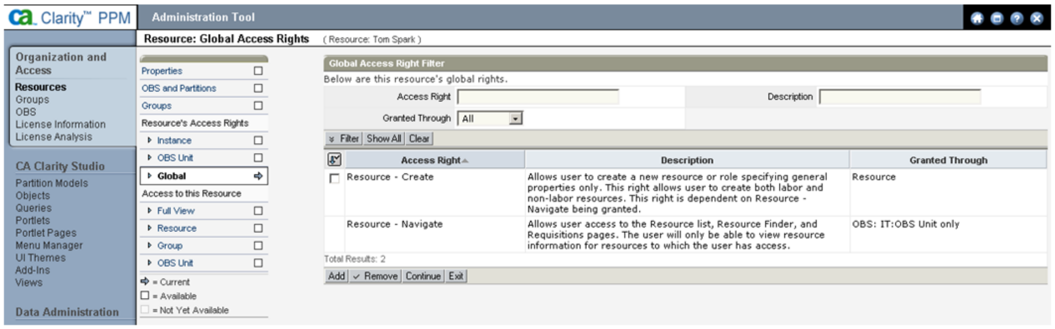
Access Right: resource - c

Description:

☑	Access Right	Description
☑	Resource - Create	Allows user to create a new resource or role specifying general properties only. This right allows user to create both labor and non-labor resources. This right is dependent on Resource - Navigate being granted.

Total Results: 1

The Resource – Create Global Right has been granted to Tom Spark.



Resource: Global Access Rights (Resource: Tom Spark)

Global Access Right Filter

Below are this resource's global rights.

Access Right:

Description:

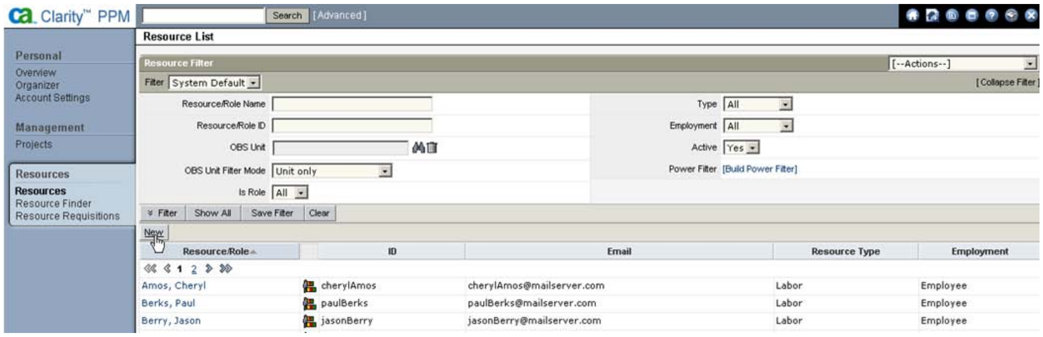
Granted Through: All

☐	Access Right	Description	Granted Through
☐	Resource - Create	Allows user to create a new resource or role specifying general properties only. This right allows user to create both labor and non-labor resources. This right is dependent on Resource - Navigate being granted.	Resource
	Resource - Navigate	Allows user access to the Resource list, Resource Finder, and Requisitions pages. The user will only be able to view resource information for resources to which the user has access.	OBS: IT:OBS Unit only

Total Results: 2

Confirmation

When Tom Spark accesses the Resource list, he now sees an action button: New. Tom uses the New button to start the process to create resources.



Resource List

Resource Filter

Filter: System Default

Resource/Role Name:

Resource/Role ID:

OBS Unit:

OBS Unit Filter Mode: Unit only

Is Role: All

Type: All

Employment: All

Active: Yes

Power Filter: [Build Power Filter]

Resource/Role	ID	Email	Resource Type	Employment
Amos, Cheryl	cherylAmos	cherylAmos@mailserver.com	Labor	Employee
Berks, Paul	paulBerks	paulBerks@mailserver.com	Labor	Employee
Berry, Jason	jasonBerry	jasonBerry@mailserver.com	Labor	Employee

How to Grant Access from Within a Specific Object Instance

Sometimes the CA Clarity PPM administrator may delegate the function of managing security for specific objects to certain resources. These resources should be able to grant access to specific data without needing to contact the administrator and without having overall security management access. The following use case describes how to do this. The resources, Paul Martin and Clare Green are fictitious.

Use Case

Paul Martin is the project manager for the Top Secret Telepathic Scanner project. He must grant viewing access to stakeholders: Clare Green needs Edit Access. Members of the IT OBS Unit need View Access. Members of the Special Projects Group need View Document access. Paul Martin does not have access to the Administration tool, but he can grant access from within the project pages.

Setting Up

The Actors– Paul Martin and the administrator

Actions

- Access rights management for Paul.
- Edit Access for Clare Green.
- Project -View access for members of the IT OBS unit.
- View Document access for members of the Special Projects group.

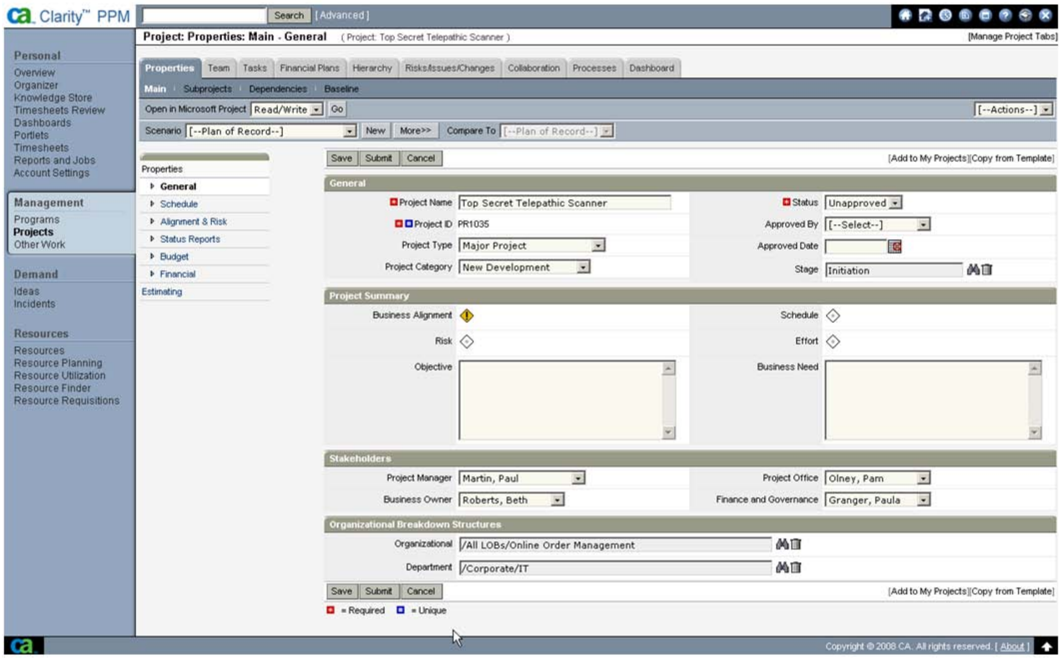
The Scope

Each resource or group is granted access to the Top Secret Telepathic Scanner project as described in Actions items 1 through 4.

Delegating Access Rights Management

The administrator must grant Paul Martin access to manage his project Access Rights.

- When Paul Martin accesses the Top Secret Telepathic Scanner project, he does not have the option to grant access.



Project: Properties: Main - General (Project: Top Secret Telepathic Scanner)

General

Project Name: Top Secret Telepathic Scanner

Project ID: PR1035

Project Type: Major Project

Project Category: New Development

Status: Unapproved

Approved By: [--Select--]

Approved Date:

Stage: Initiation

Stakeholders

Project Manager: Martin, Paul

Business Owner: Roberts, Beth

Project Office: Olney, Pam

Finance and Governance: Granger, Paula

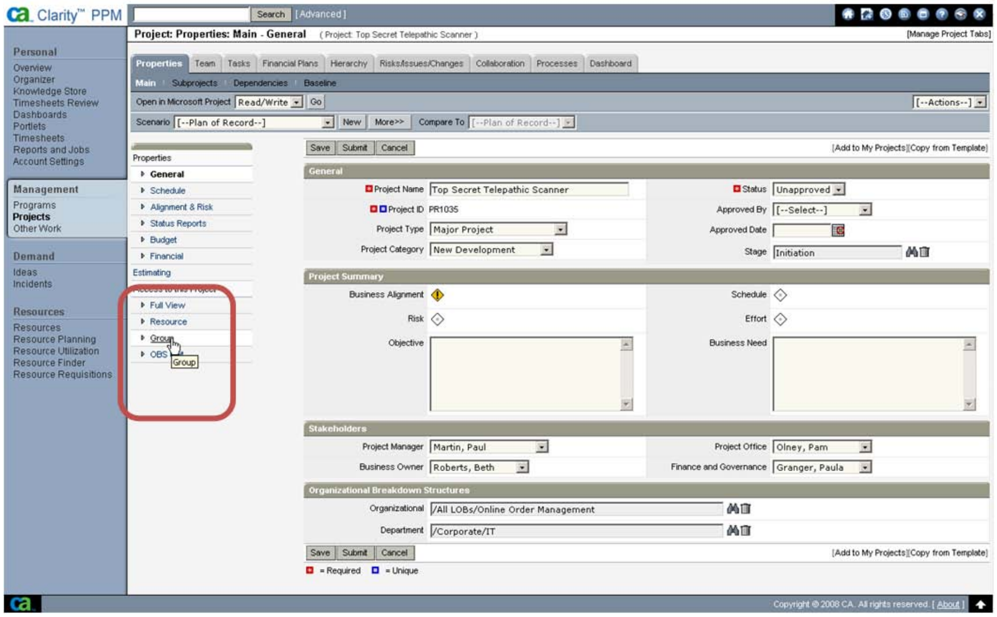
Organizational Breakdown Structures

Organizational: /All LOBs/Online Order Management

Department: /Corporate/IT

- After being granted Project – Edit Access Rights on project instance Top Secret Telepathic Scanner, a new menu option Access to the Project is available to Paul.

Now, Paul can select the option to manage Access (security) to the project.



Project: Properties: Main - General (Project: Top Secret Telepathic Scanner)

Open in Microsoft Project: Read/Write

Scenario: [--Plan of Record--]

Compare To: [--Plan of Record--]

General

Project Name	Top Secret Telepathic Scanner	Status	Unapproved
Project ID	PR1035	Approved By	[--Select--]
Project Type	Major Project	Approved Date	
Project Category	New Development	Stage	Initiation

Project Summary

Business Alignment		Schedule	
Risk		Effort	
Objective		Business Need	

Stakeholders

Project Manager	Martin, Paul	Project Office	Olney, Pam
Business Owner	Roberts, Beth	Finance and Governance	Granger, Paula

Organizational Breakdown Structures

Organizational	/All LOBs/Online Order Management
Department	/Corporate/IT

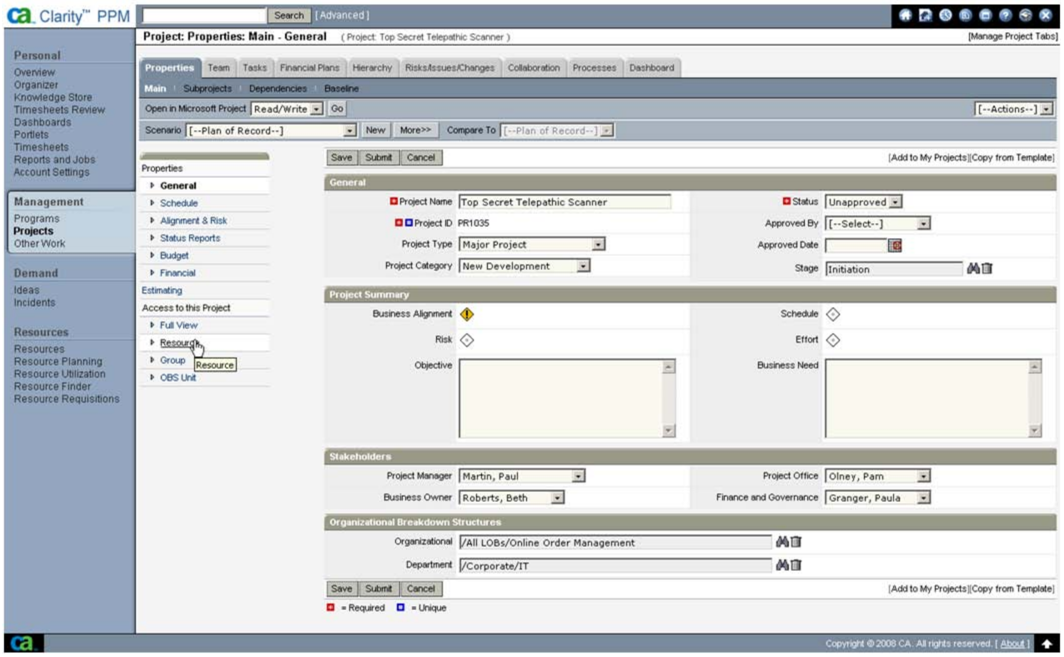
🟥 = Required 🟦 = Unique

Granting Access Directly to a Resource

You can grant access directly to a resource.

Setting Up

- Paul grants the Project – Edit Access Right (What) to Clare Green (Who) on project Top Secret Telepathic Scanner- from within the Projects page.
- Paul clicks Resource under Access to this Project.



Project: Properties: Main - General (Project: Top Secret Telepathic Scanner)

Open in Microsoft Project: Read/Write

Scenario: [--Plan of Record--] Compare To: [--Plan of Record--]

General

Project Name	Top Secret Telepathic Scanner	Status	Unapproved
Project ID	PR1035	Approved By	[--Select--]
Project Type	Major Project	Approved Date	
Project Category	New Development	Stage	Initiation

Project Summary

Business Alignment	◆	Schedule	◇
Risk	◇	Effort	◇
Objective		Business Need	

Stakeholders

Project Manager	Martin, Paul	Project Office	Olney, Pam
Business Owner	Roberts, Beth	Finance and Governance	Granger, Paula

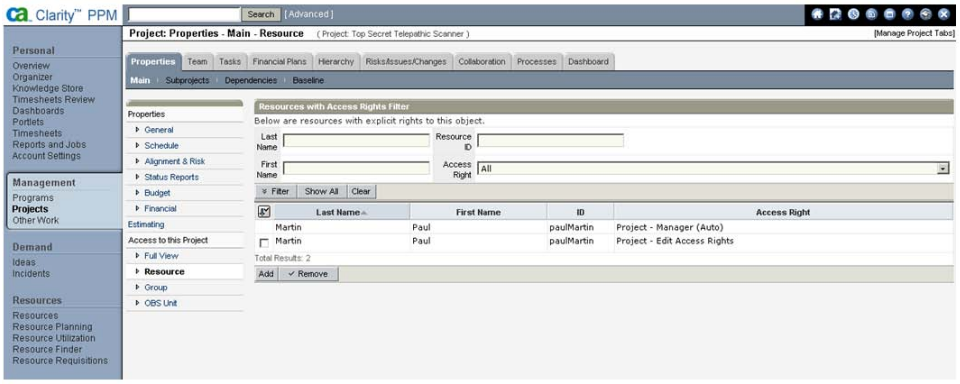
Organizational Breakdown Structures

Organizational	/All LOBs/Online Order Management
Department	/Corporate/IT

🟥 = Required 🟦 = Unique

Select and Grant Access Rights

1. Paul Martin is the only resource displayed with access to the project. Click Add to begin the process of granting access to other resources for this project.



Project: Properties - Main - Resource (Project: Top Secret Telepathic Scanner)

Resources with Access Rights Filter

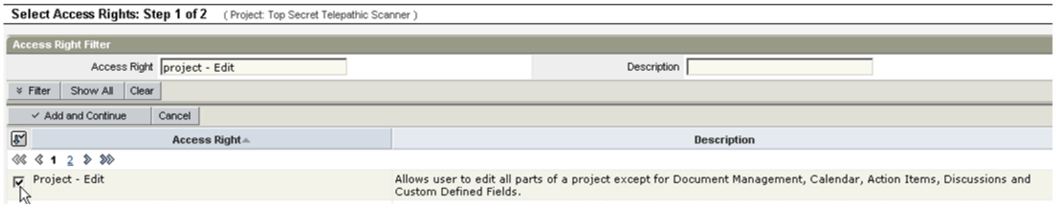
Below are resources with explicit rights to this object.

Last Name:
Resource ID:
First Name:
Access Right: All

	Last Name	First Name	ID	Access Right
	Martin	Paul	paulMartin	Project - Manager (Auto)
□	Martin	Paul	paulMartin	Project - Edit Access Rights

Total Results: 2

2. Locate and select Access Right Project - Edit. Click Add and Continue.



Select Access Rights: Step 1 of 2 (Project: Top Secret Telepathic Scanner)

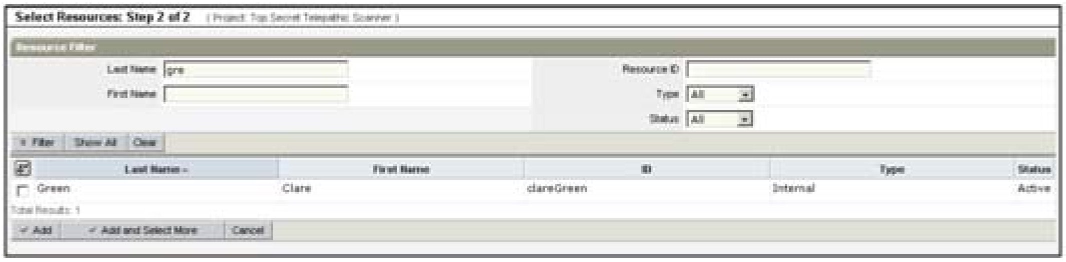
Access Right Filter

Access Right: project - Edit
Description:

	Access Right	Description
☑	Project - Edit	Allows user to edit all parts of a project except for Document Management, Calendar, Action Items, Discussions and Custom Defined Fields.

3. Locate the resource to receive the access. Filtering was used to locate Clare Green for this example.

4. Select the resource, and click Add.



Select Resources: Step 2 of 2 (Project: Top Secret Telepathic Scanner)

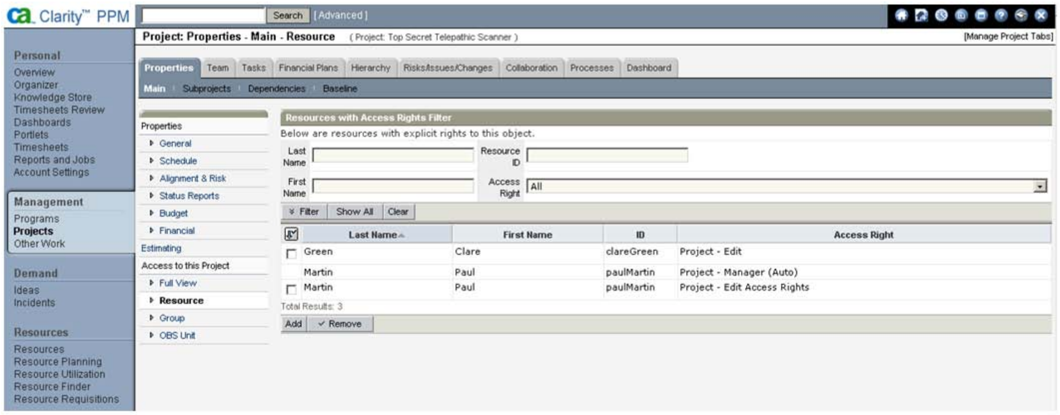
Resource Filter

Last Name: gre
First Name:
Resource ID:
Type: All
Status: All

	Last Name	First Name	ID	Type	Status
□	Green	Clare	clareGreen	Internal	Active

Total Results: 1

Clare Green has Project – Edit access to the Top Secret Telepathic Scanner project.



Project: Properties - Main - Resource (Project: Top Secret Telepathic Scanner)

Resources with Access Rights Filter

Below are resources with explicit rights to this object.

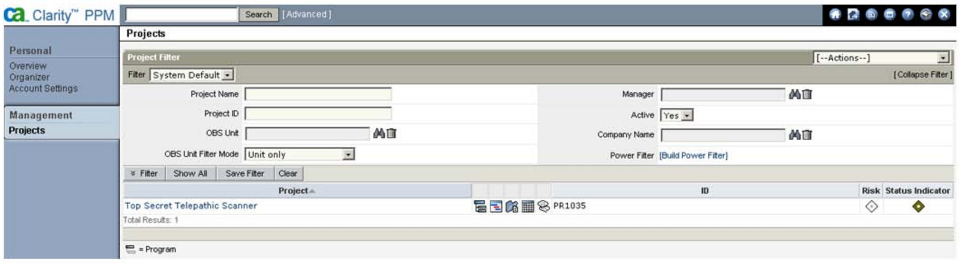
Last Name	
Resource ID	
First Name	
Access Right	All

	Last Name	First Name	ID	Access Right
☐	Green	Clare	clareGreen	Project - Edit
	Martin	Paul	paulMartin	Project - Manager (Auto)
☐	Martin	Paul	paulMartin	Project - Edit Access Rights

Total Results: 3

Confirmation

- Clare Green has Project – Edit access rights.



Projects

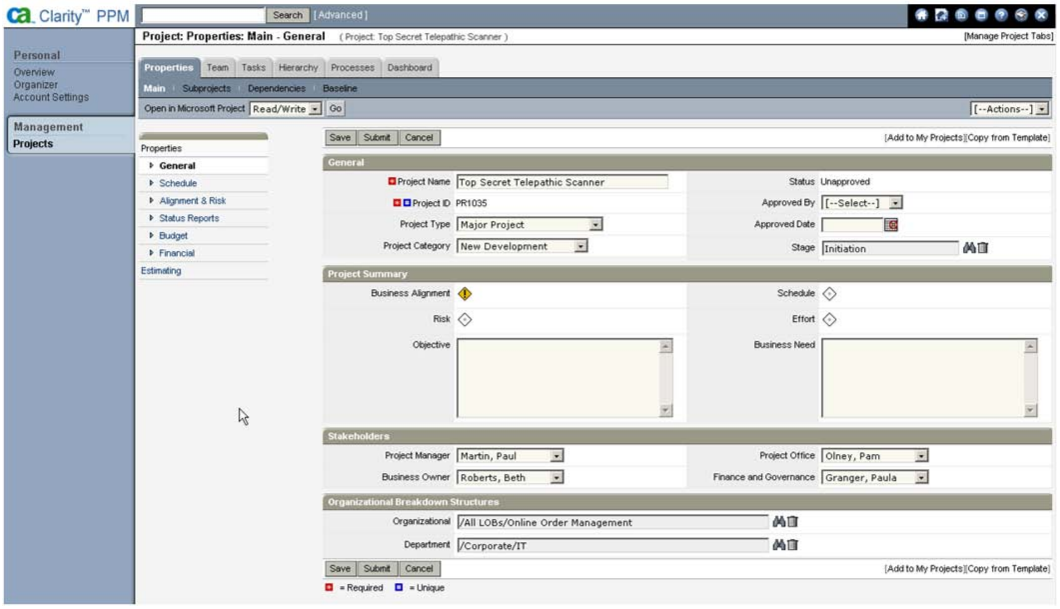
Project Filter

Filter	System Default		
Project Name		Manager	
Project ID		Active	Yes
OBS Unit		Company Name	
OBS Unit Filter Mode	Unit only	Power Filter	[Build Power Filter]

Project	ID	Risk	Status Indicator
Top Secret Telepathic Scanner	PR1035	◇	◆

Total Results: 1

- Clare can view, and edit the project information.



Project: Properties: Main - General (Project: Top Secret Telepathic Scanner)

Open in Microsoft Project: Read/Write

General

Project Name	Top Secret Telepathic Scanner	Status	Unapproved
Project ID	PR1035	Approved By	[--Select--]
Project Type	Major Project	Approved Date	
Project Category	New Development	Stage	Initiation

Project Summary

Business Alignment	◆	Schedule	◇
Risk	◇	Effort	◇
Objective		Business Need	

Stakeholders

Project Manager	Martin, Paul	Project Office	Olney, Pam
Business Owner	Roberts, Beth	Finance and Governance	Granger, Paula

Organizational Breakdown Structures

Organizational	/All LOBs/Online Order Management
Department	/Corporate/IT

🟥 = Required 🟦 = Unique

Granting Access Rights to a Group

You can also grant access rights to a group.

Setting Up

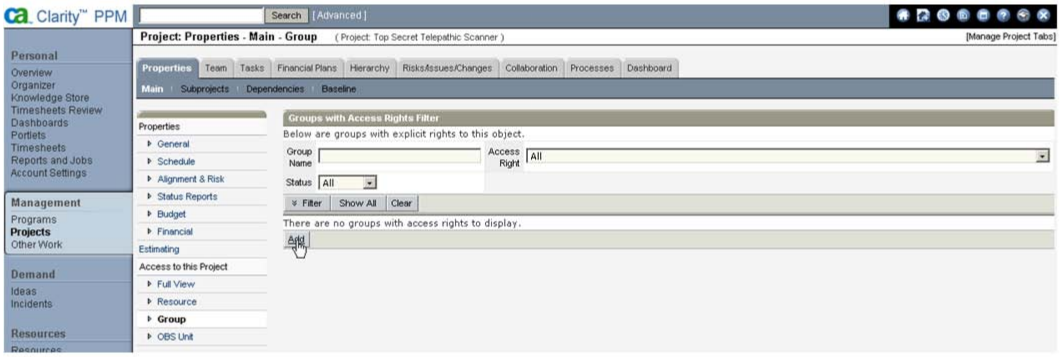
- The Actors - members of the Special Projects Group (Who)
- The Action - granting Project – View Documents Access Right (What)
- The Scope - Top Secret Telepathic Scanner project (Which Data)

Review the Current Access Rights

Click Groups under *Access to this Project* to see which Groups have access to project. No Groups have access to this project yet.

Select and Grant Access Rights

1. Click Add to grant access to a Group for this project.



Project: Properties - Main - Group (Project: Top Secret Telepathic Scanner)

Groups with Access Rights Filter

Below are groups with explicit rights to this object.

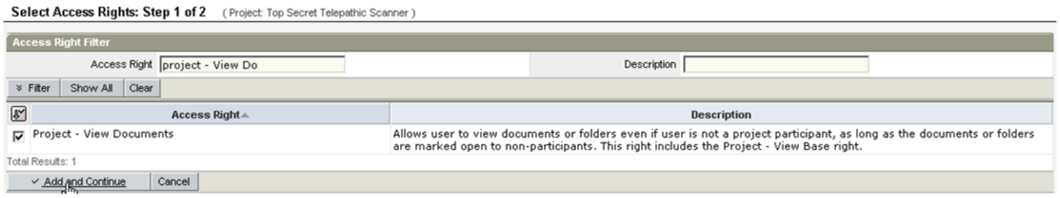
Group Name:

Access Right: All

Status: All

There are no groups with access rights to display.

- Use filtering to locate the Project – View Documents Access Right.
- Select the access right, click Add and Continue.



Select Access Rights: Step 1 of 2 (Project: Top Secret Telepathic Scanner)

Access Right Filter

Access Right: project - View Do

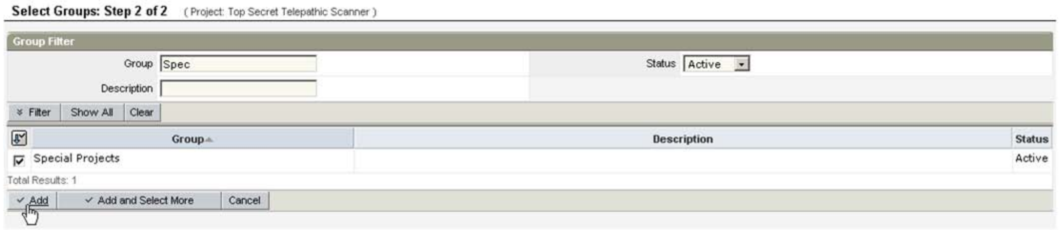
Description:

☑	Access Right	Description
☑	Project - View Documents	Allows user to view documents or folders even if user is not a project participant, as long as the documents or folders are marked open to non-participants. This right includes the Project - View Base right.

Total Results: 1

2. Use filtering to select the Group to receive the access right. In this case, the access is granted to the Special Projects group.

3. Click Add.



Select Groups: Step 2 of 2 (Project: Top Secret Telepathic Scanner)

Group Filter

Group: Spec

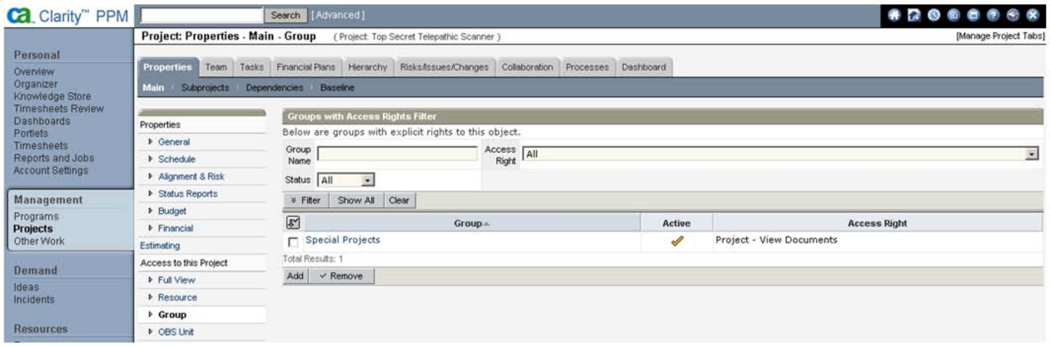
Description:

Status: Active

☑	Group	Description	Status
☑	Special Projects		Active

Total Results: 1

Access is now granted to the Special Project group members for viewing documents in the Top Secret Telepathic Scanner project.



Project: Properties - Main - Group (Project: Top Secret Telepathic Scanner)

Groups with Access Rights Filter

Below are groups with explicit rights to this object.

Group Name:

Access Right: All

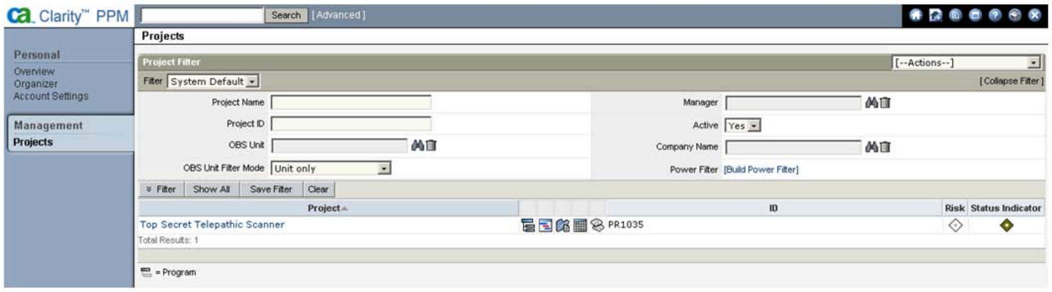
Status: All

☐	Group	Active	Access Right
☐	Special Projects	✓	Project - View Documents

Total Results: 1

Confirmation

- Tom Spark, a fictitious resource is a member of the Special Projects group. He can access the project.



Projects

Project Filter

Filter: System Default

Project Name:

Project ID:

OBS Unit:

OBS Unit Filter Mode: Unit only

Manager:

Active: Yes

Company Name:

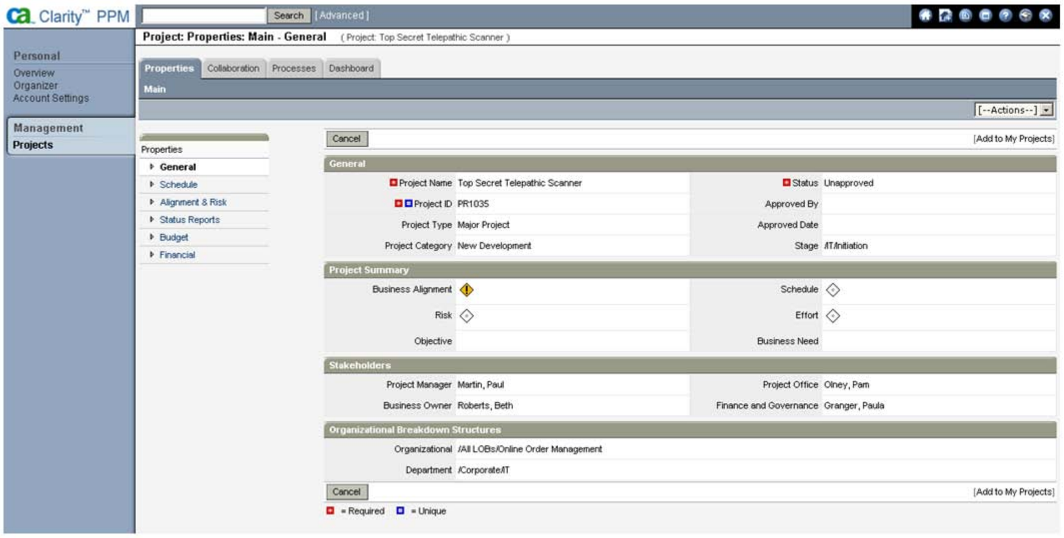
Power Filter: [Build Power Filter]

Project	ID	Risk	Status Indicator
Top Secret Telepathic Scanner	PR1035	◇	◆

Total Results: 1

= Program

- Tom has access to the Project documents folder from the Collaboration Tab. The documents are kept here for the project.



Project: Properties: Main - General (Project: Top Secret Telepathic Scanner)

General

🟥 Project Name	Top Secret Telepathic Scanner	🟥 Status	Unapproved
🟥 🟦 Project ID	PR1035	Approved By	
Project Type	Major Project	Approved Date	
Project Category	New Development	Stage	/IT/Initiation

Project Summary

Business Alignment	◆	Schedule	◇
Risk	◇	Effort	◇
Objective		Business Need	

Stakeholders

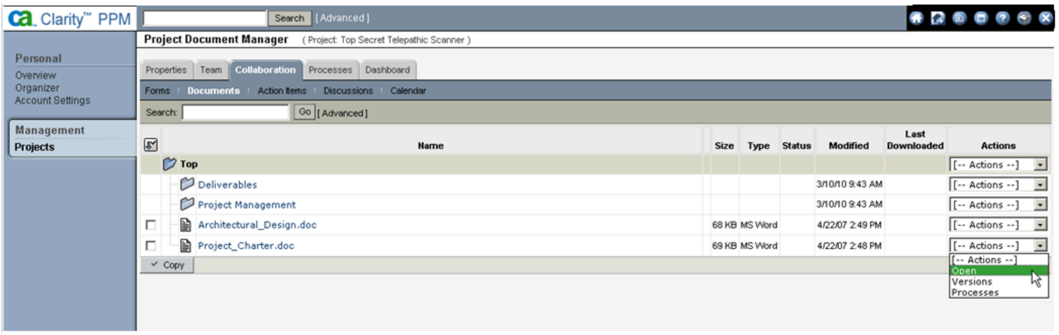
Project Manager	Martin, Paul	Project Office	Olney, Pam
Business Owner	Roberts, Beth	Finance and Governance	Granger, Paula

Organizational Breakdown Structures

Organizational	/All LOBs/Online Order Management
Department	/Corporate/IT

🟥 = Required 🟦 = Unique

- Tom has viewing access to the project documents using the Collaboration tab.



Project Document Manager (Project: Top Secret Telepathic Scanner)

	Name	Size	Type	Status	Modified	Last Downloaded	Actions
	Top						[-- Actions --]
	Deliverables				3/10/10 9:43 AM		[-- Actions --]
	Project Management				3/10/10 9:43 AM		[-- Actions --]
□	Architectural_Design.doc	68 KB	MS Word		4/22/07 2:49 PM		[-- Actions --]
□	Project_Charter.doc	69 KB	MS Word		4/22/07 2:48 PM		[-- Actions --]

Granting Access to OBS Unit Members

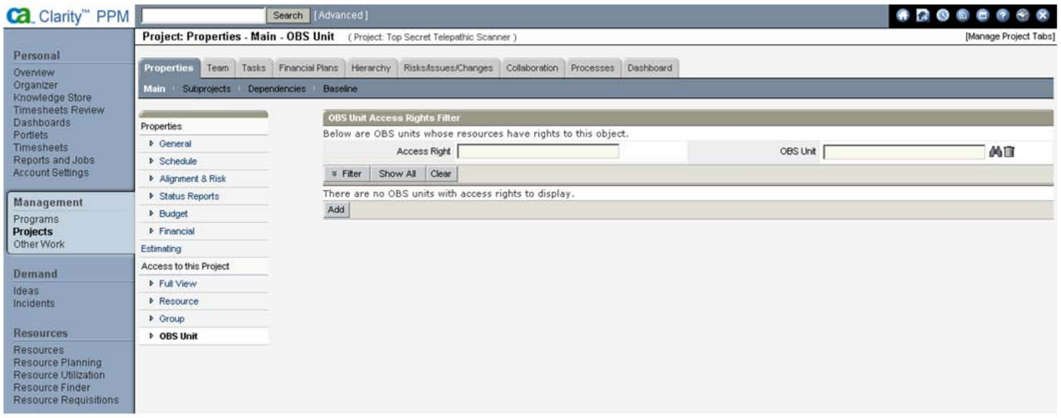
You can grant access to OBS unit members also.

Setting Up

- The Actors - members of the IT OBS Unit (Who)
- The Action - grant Project – View Access Right (What)
- The Scope - Top Secret Telepathic Scanner project (Which Data)

Review the Current Access Rights

Click OBS Unit under *Access to this Project* to see if any OBS units have access to the project. No OBS Units have access to this project.



Project: Properties - Main - OBS Unit (Project: Top Secret Telepathic Scanner)

OBS Unit Access Rights Filter

Below are OBS units whose resources have rights to this object.

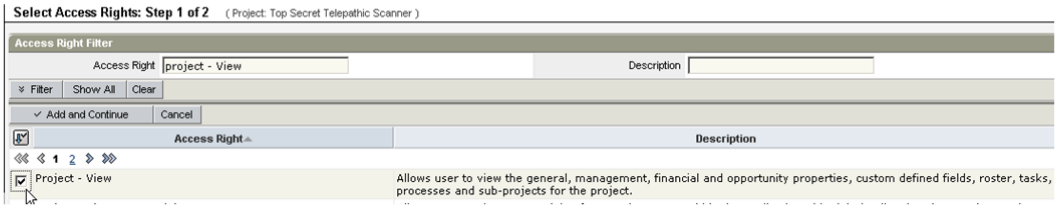
Access Right:

OBS Unit:

There are no OBS units with access rights to display.

Select and Grant Access Rights

1. Click Add to begin the process of granting access rights to the OBS Unit for selected project.
   - Use filtering to locate the access right.
   - Select the Access Right Project – View.
   - Click Add and Continue.



Select Access Rights: Step 1 of 2 (Project: Top Secret Telepathic Scanner)

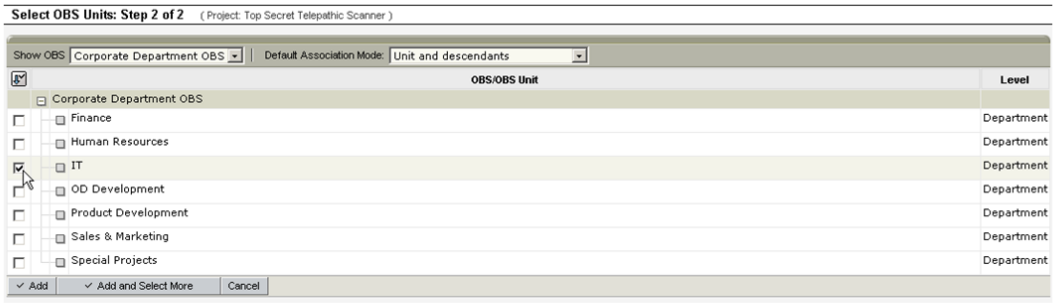
Access Right Filter

Access Right: project - View

Description:

☐	Access Right	Description
☑	Project - View	Allows user to view the general, management, financial and opportunity properties, custom defined fields, roster, tasks, processes and sub-projects for the project.

2. Select the IT OBS Unit, and click Add.

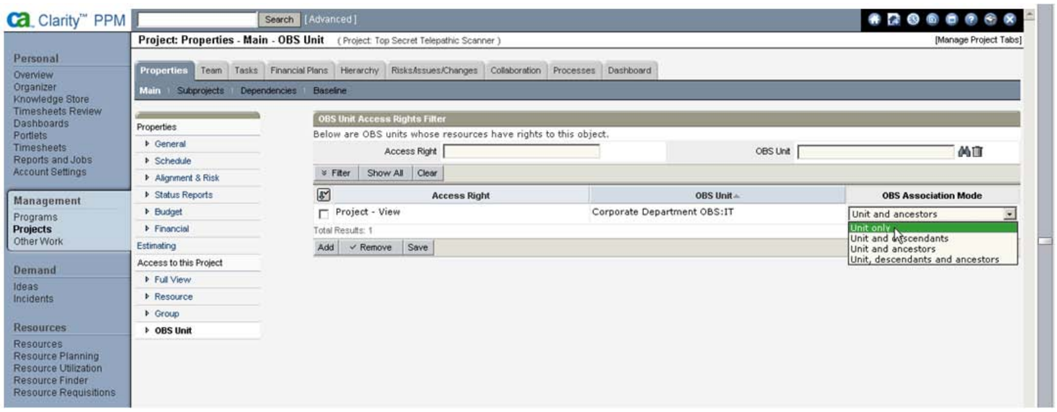


Select OBS Units: Step 2 of 2 (Project: Top Secret Telepathic Scanner)

Show OBS: Corporate Department OBS | Default Association Mode: Unit and descendants

	OBS/OBS Unit	Level
	Corporate Department OBS	
□	Finance	Department
□	Human Resources	Department
☑	IT	Department
□	OD Development	Department
□	Product Development	Department
□	Sales & Marketing	Department
□	Special Projects	Department

3. If the Access Right is granted only to the OBS Unit itself, or if it includes its ancestors, or its descendants, then select Unit Only.



Project: Properties - Main - OBS Unit (Project: Top Secret Telepathic Scanner)

OBS Unit Access Rights Filter

Below are OBS units whose resources have rights to this object.

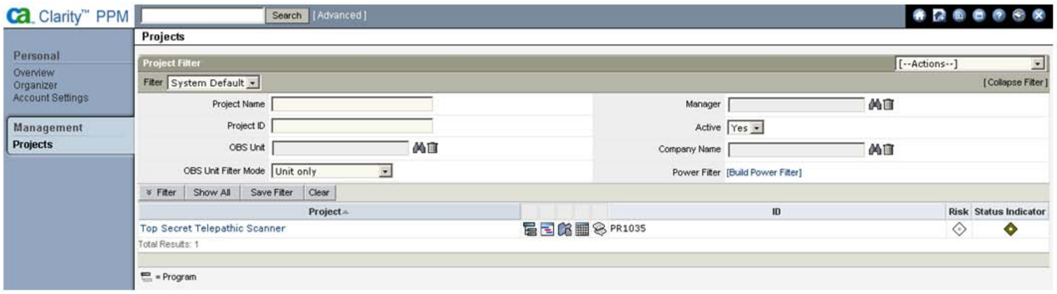
Access Right:
OBS Unit:

	Access Right	OBS Unit	OBS Association Mode
□	Project - View	Corporate Department OBS:IT	Unit and ancestors

Total Results: 1

Confirmation

- Roberta Smith, a fictitious resource, is a member of the IT OBS Unit.



Projects

Project Filter

Filter: System Default

Project Name:

Manager:

Project ID:

Active: Yes

OBS Unit:

Company Name:

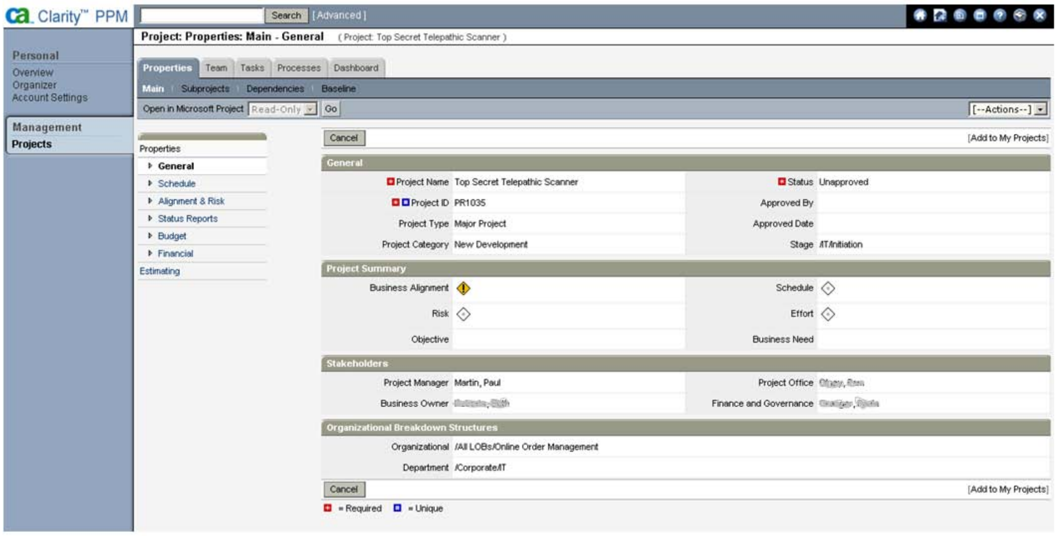
OBS Unit Filter Mode: Unit only

Power Filter: [Build Power Filter]

Project	ID	Risk	Status Indicator
Top Secret Telepathic Scanner	PR1035	◇	◆

Total Results: 1

- Roberta has View access to the project.



Project: Properties: Main - General (Project: Top Secret Telepathic Scanner)

Open in Microsoft Project: Read-Only

General

Project Name: Top Secret Telepathic Scanner

Status: Unapproved

Project ID: PR1035

Approved By:

Project Type: Major Project

Approved Date:

Project Category: New Development

Stage: IT/Initiation

Project Summary

Business Alignment: ◆

Schedule: ◇

Risk: ◇

Effort: ◇

Objective:

Business Need:

Stakeholders

Project Manager: Martin, Paul

Project Office: [redacted]

Business Owner: [redacted]

Finance and Governance: [redacted]

Organizational Breakdown Structures

Organizational: /All LOBs/Online Order Management

Department: /Corporate/IT

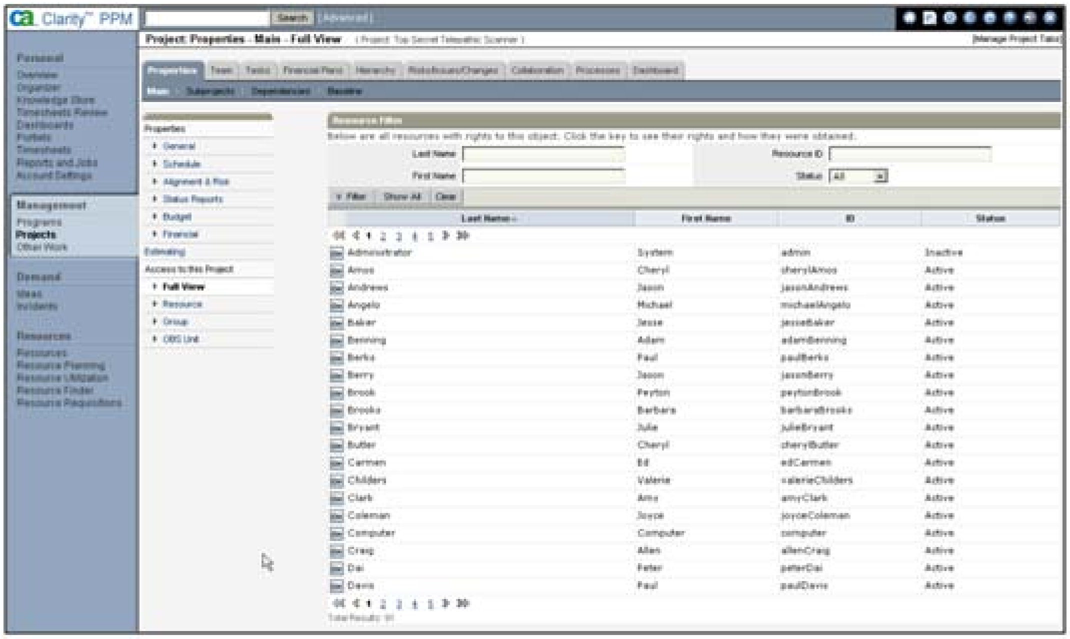
Verifying Access Rights

Resources with View Access Rights or Edit Access Rights access are able to verify who has access to data.

Paul Martin verifies which resources have access to the Top Secret Telepathic Scanner project. This can include people and other resources (computers, servers, system resources, and so on).

To verify the access rights

1. Click Full View under Access to this Project to see the list. In this example. 91 resources have access to the project.



Project: Properties - Main - Full View (Project: Top Secret Telepathic Scanner)

Below are all resources with rights to this object. Click the key to see their rights and how they were obtained.

Last Name
First Name
Resource ID
Status: All

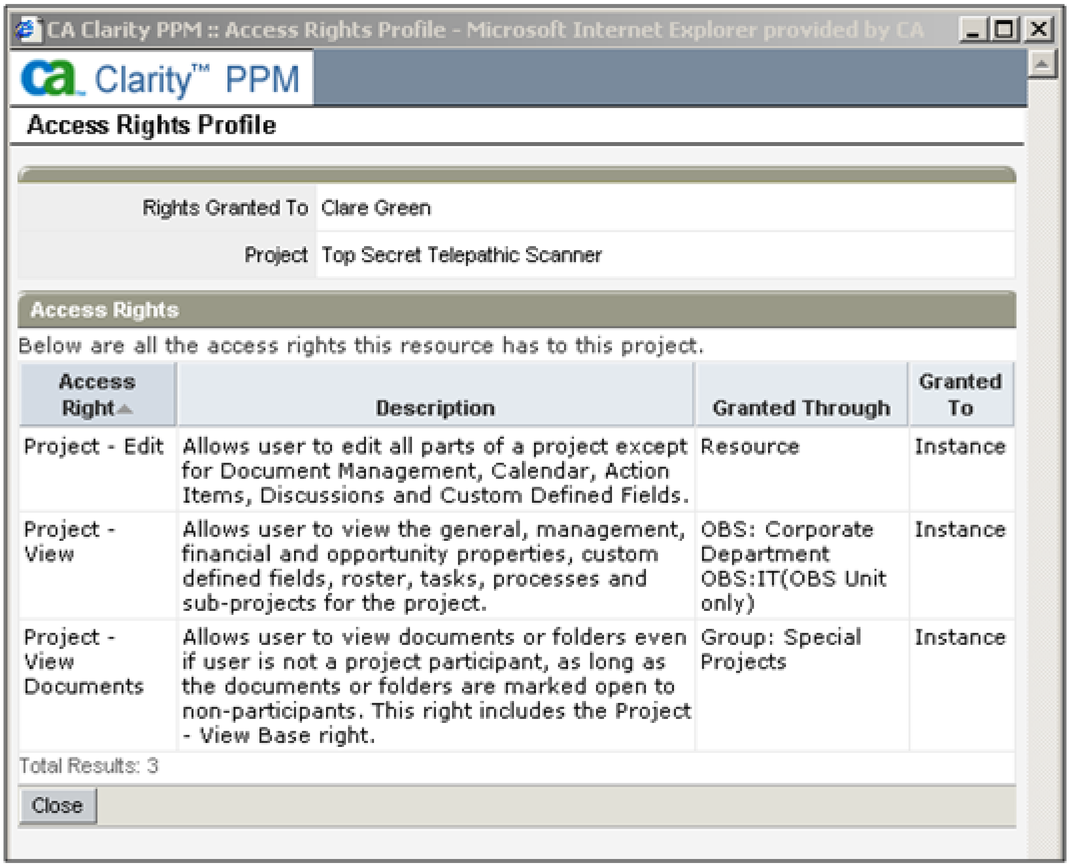
Last Name	First Name	ID	Status
Administrator	System	admin	Inactive
Amos	Cheryl	cherylAmos	Active
Andrews	Jason	jasonAndrews	Active
Angelo	Michael	michaelAngelo	Active
Baker	Jesse	jesseBaker	Active
Benning	Adam	adamBenning	Active
Berks	Paul	paulBerks	Active
Berry	Jason	jasonBerry	Active
Brook	Peyton	peytonBrook	Active
Brooks	Barbara	barbaraBrooks	Active
Bryant	Julie	julieBryant	Active
Butler	Cheryl	cherylButler	Active
Carmen	Ed	edCarmen	Active
Childers	Valerie	valerieChilders	Active
Clark	Amy	amyClark	Active
Coleman	Joyce	joyceColeman	Active
Computer	Computer	computer	Active
Craig	Allen	allenCraig	Active
Dai	Peter	peterDai	Active
Davis	Paul	paulDavis	Active

1 2 3 4 5

Total Results: 91

2. Click the key icon next to the resource name to check what type of access the resource has, and how it was granted.

   Clare Green's access is displayed.


CA Clarity PPM :: Access Rights Profile - Microsoft Internet Explorer provided by CA
ca Clarity™ PPM

Access Rights Profile

Rights Granted To: Clare Green

Project: Top Secret Telepathic Scanner

Access Rights

Below are all the access rights this resource has to this project.

Access Right	Description	Granted Through	Granted To
Project - Edit	Allows user to edit all parts of a project except for Document Management, Calendar, Action Items, Discussions and Custom Defined Fields.	Resource	Instance
Project - View	Allows user to view the general, management, financial and opportunity properties, custom defined fields, roster, tasks, processes and sub-projects for the project.	OBS: Corporate Department OBS:IT(OBS Unit only)	Instance
Project - View Documents	Allows user to view documents or folders even if user is not a project participant, as long as the documents or folders are marked open to non-participants. This right includes the Project - View Base right.	Group: Special Projects	Instance

Total Results: 3

She has been granted Project – Edit directly to her profile, Project – View was granted through the IT OBS Unit (of which she is a member) and Project - View Documents was granted through Special Projects group (of which she is also a member).

Pages Security

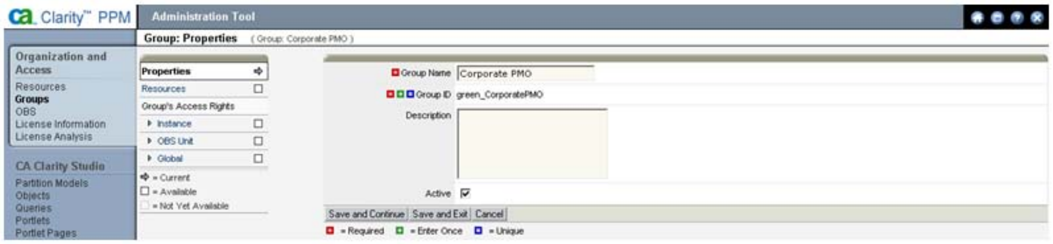
CA Clarity PPM pages are not objects but may be secured just like CA Clarity PPM objects. Access Grant rights to different Actors (Resources, Groups or OBS Units) using any of the three different types of Data Scope: by Instance, by OBS Unit, or Global.

Use Case

A PMO team, Corporate PMO, created a PMO Dashboard page. This page should only be accessible by members of this PMO group.

Setting up

- The Actor - the Corporate PMO group. This access affects the group members for this specific dashboard page.
- The Action - Page –View access right
- The Scope – the PMO Dashboard page



Group: Properties (Group: Corporate PMO)

Group Name: Corporate PMO

Group ID: green_CorporatePMO

Description:

Active: ☑

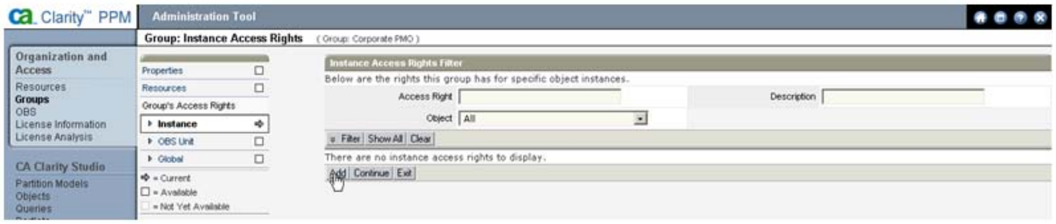
Review the Current Access Rights

Click Instance under Group Access Rights to grant this Group members access rights for the PMO Dashboard page.

As illustrated the Corporate PMO Group does not have any instance-level access rights yet.

Select and Grant Access Rights

1. Click Add on the Group: Instance Access Rights page.



Group: Instance Access Rights (Group: Corporate PMO)

Below are the rights this group has for specific object instances.

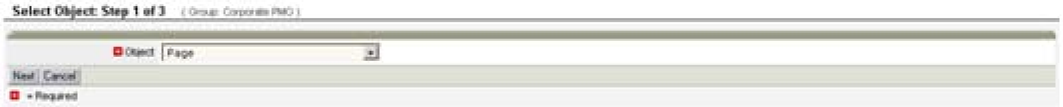
Access Right:

Description:

Object: All

There are no instance access rights to display.

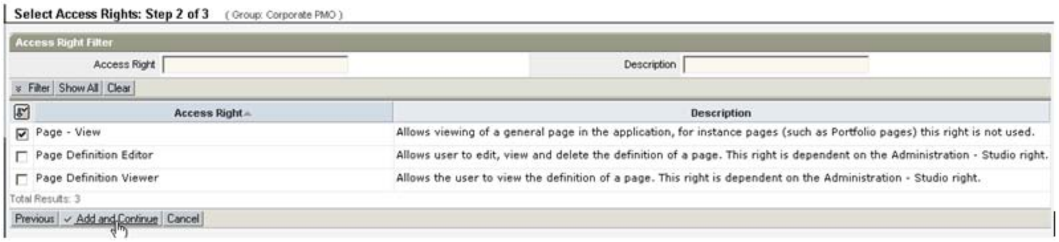
2. For the Object, select Page from the attribute menu, and click Next.



Select Object: Step 1 of 3 (Group: Corporate PMO)

Object: Page

3. Select the proper access right. In this case, select Page – View using the checkbox to the left, and click Add and Continue.



Select Access Rights: Step 2 of 3 (Group: Corporate PMO)

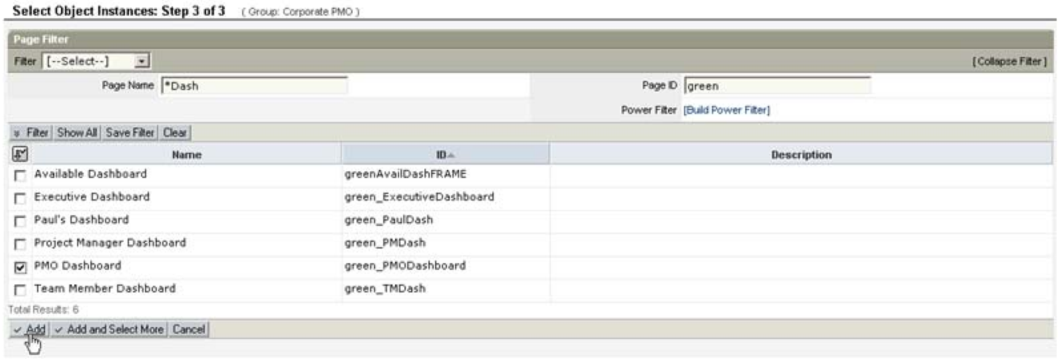
Access Right Filter

Access Right:
Description:

	Access Right	Description
☑	Page - View	Allows viewing of a general page in the application, for instance pages (such as Portfolio pages) this right is not used.
□	Page Definition Editor	Allows user to edit, view and delete the definition of a page. This right is dependent on the Administration - Studio right.
□	Page Definition Viewer	Allows the user to view the definition of a page. This right is dependent on the Administration - Studio right.

Total Results: 3

4. Define the Scope. For this example, select the PMO Dashboard page. Select it using the checkbox to the left and click Add. You can select multiple instances at a time. Use Add and Select More to keep filtering and adding instances if necessary.



Select Object Instances: Step 3 of 3 (Group: Corporate PMO)

Page Filter

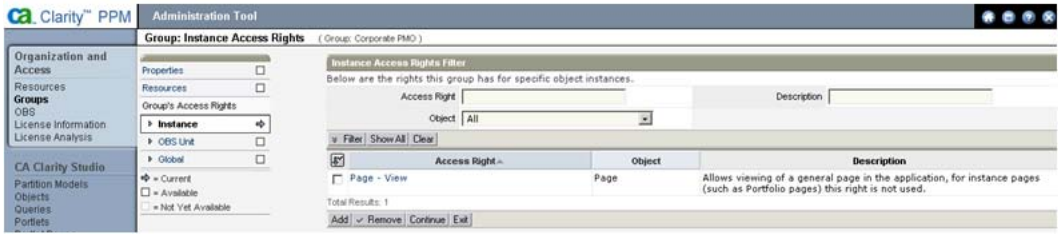
Filter: [--Select--]

Page Name: *Dash
Page ID: green
Power Filter: [Build Power Filter]

	Name	ID	Description
□	Available Dashboard	greenAvailDashFRAME	
□	Executive Dashboard	green_ExecutiveDashboard	
□	Paul's Dashboard	green_PaulDash	
□	Project Manager Dashboard	green_PMDash	
☑	PMO Dashboard	green_PMODashboard	
□	Team Member Dashboard	green_TMDash	

Total Results: 6

Page - View Access has been granted to the Corporate PMO group.



Group: Instance Access Rights (Group: Corporate PMO)

Instance Access Rights Filter

Below are the rights this group has for specific object instances.

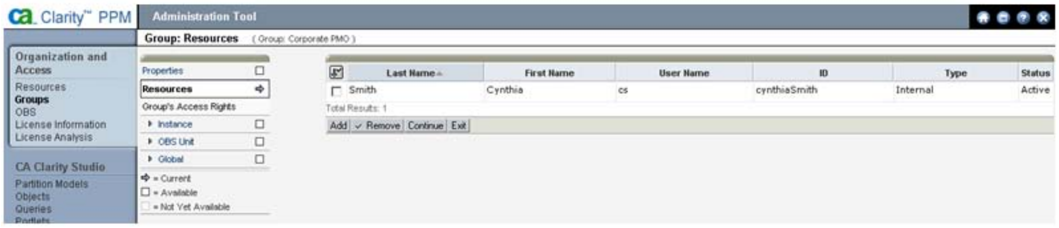
Access Right:
Description:
Object: All

	Access Right	Object	Description
□	Page - View	Page	Allows viewing of a general page in the application, for instance pages (such as Portfolio pages) this right is not used.

Total Results: 1

Confirmation

- Cynthia Smith, a fictitious resource, is a member of the Corporate PMO group.



Group: Resources (Group: Corporate PMO)

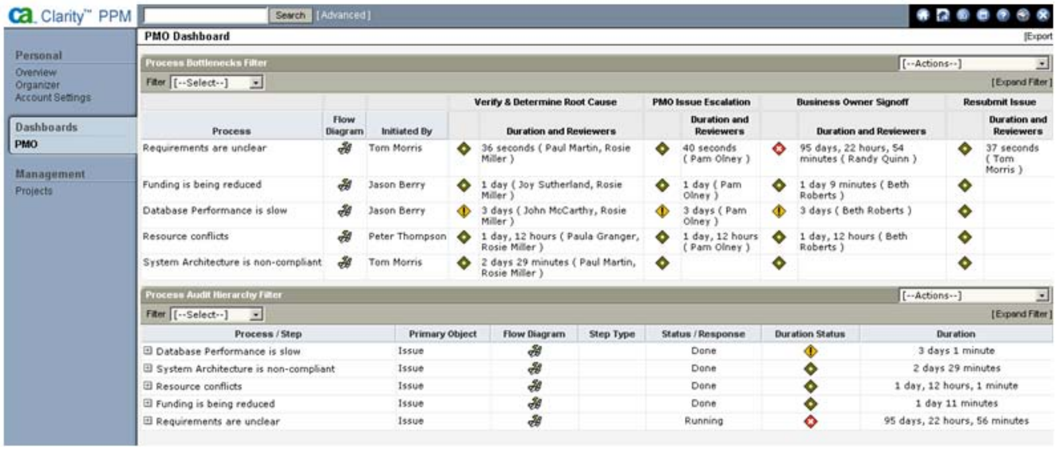
	Last Name	First Name	User Name	ID	Type	Status
□	Smith	Cynthia	cs	cynthiaSmith	Internal	Active

Total Results: 1

- When Cynthia logs in to the CA Clarity PPM, she has access to the PMO Dashboard.

Important! The group of members also needs access to the portlets on dashboard. Without access, they see a blank page.

For more information about Portlet security, see Portlet Security (see page 89) and Securing Dashboard Pages (see page 150).



PMO Dashboard

Process Bottlenecks Filter

Filter [--Select--]

			Verify & Determine Root Cause		PMO Issue Escalation		Business Owner Signoff		Resubmit Issue	
Process	Flow Diagram	Initiated By		Duration and Reviewers		Duration and Reviewers		Duration and Reviewers		Duration and Reviewers
Requirements are unclear		Tom Morris	◆	36 seconds (Paul Martin, Rosie Miller)	◆	40 seconds (Pam Olney)	✖	95 days, 22 hours, 54 minutes (Randy Quinn)	◆	37 seconds (Tom Morris)
Funding is being reduced		Jason Berry	◆	1 day (Joy Sutherland, Rosie Miller)	◆	1 day (Pam Olney)	◆	1 day 9 minutes (Beth Roberts)	◆	
Database Performance is slow		Jason Berry	⚠	3 days (John McCarthy, Rosie Miller)	⚠	3 days (Pam Olney)	⚠	3 days (Beth Roberts)	◆	
Resource conflicts		Peter Thompson	◆	1 day, 12 hours (Paula Granger, Rosie Miller)	◆	1 day, 12 hours (Pam Olney)	◆	1 day, 12 hours (Beth Roberts)	◆	
System Architecture is non-compliant		Tom Morris	◆	2 days 29 minutes (Paul Martin, Rosie Miller)	◆		◆		◆	

Process Audit Hierarchy Filter

Filter [--Select--]

Process / Step	Primary Object	Flow Diagram	Step Type	Status / Response	Duration Status	Duration
⊞ Database Performance is slow	Issue			Done	⚠	3 days 1 minute
⊞ System Architecture is non-compliant	Issue			Done	◆	2 days 29 minutes
⊞ Resource conflicts	Issue			Done	◆	1 day, 12 hours, 1 minute
⊞ Funding is being reduced	Issue			Done	◆	1 day 11 minutes
⊞ Requirements are unclear	Issue			Running	✖	95 days, 22 hours, 56 minutes

Portlets Security

Implementing security for portlets allows you to manage which resources can access the portlet and what data those resources can access in the portlet. Having access to a Dashboard may not automatically enable access to all portlets available on the dashboard. All resources accessing a dashboard may not need access to all the portlets if some lead to sensitive or highly confidential information.

Three important aspects to consider when planning to secure a portlet:

- Securing the Portlet. Manage access to the portlet.
- Securing the data displayed in the Portlet. Build secure portlets that only show data according to the security rules.
- Portlet configuration Options for the end user.

Securing Portlets

CA Clarity PPM portlets are not objects but may be secured just like CA Clarity PPM objects. Grant Security by Instance, by OBS Unit and Globally.

Use Case

Restrict the access to portlets. The portlets have been analyzed and separated in to three different categories: General, Management, and Executive

General Portlets

These portlets should be available to all end users.

Management Portlets

These portlets should be available to Project Managers, Department Managers, Resource Managers and PMO members.

Executive Portlets

These portlets should be available to all company Executives.

Setting up

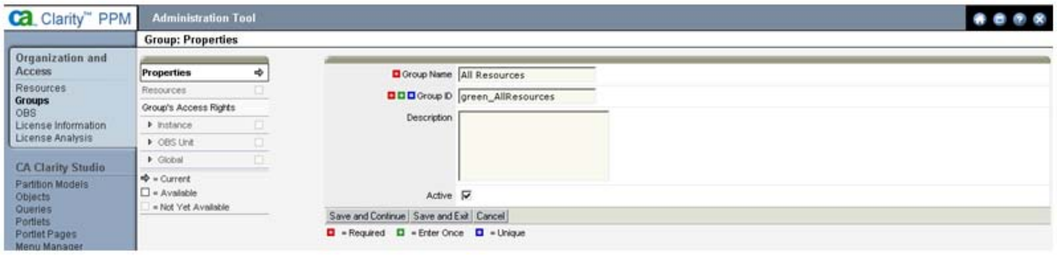
The Actors are the teams of resources. Decide how you want to group the resources that have similar roles:

- By Groups (all Project Managers, all Department Managers, all Executives, and so on.)
- By OBS units

  For this example, use Groups.

- The Action is Portlet – View – the ability to see a portlet in the Application for all the Actors.
- The Data Scope is different for each category of portlet. Not all teams have access to all of the portlets. For this example, use the following categories to group the portlets: General, Management and Executive. Create an OBS Unit to categorize the portlets.

- A new group named All Resources has been created for this example. You should assign this group to all resources, regardless of the role.

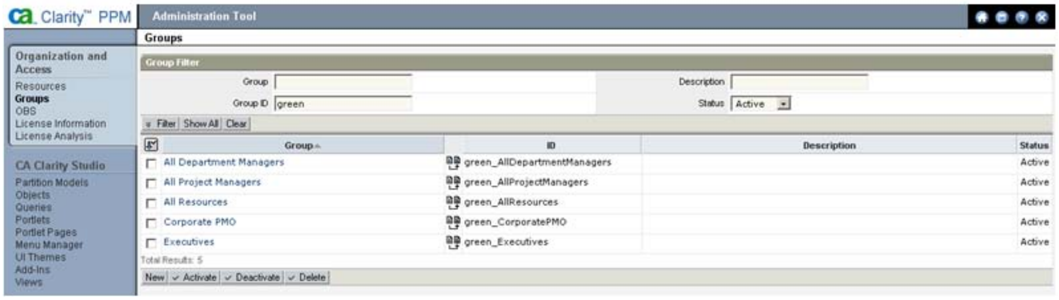


Group: Properties

🟥 Group Name	All Resources
🟥🟩🟦 Group ID	green_AllResources
Description	
Active	☑

🟥 = Required 🟩 = Enter Once 🟦 = Unique

Several other role-specific groups must be created.



Groups

Group Filter

Group		Description	
Group ID	green	Status	Active

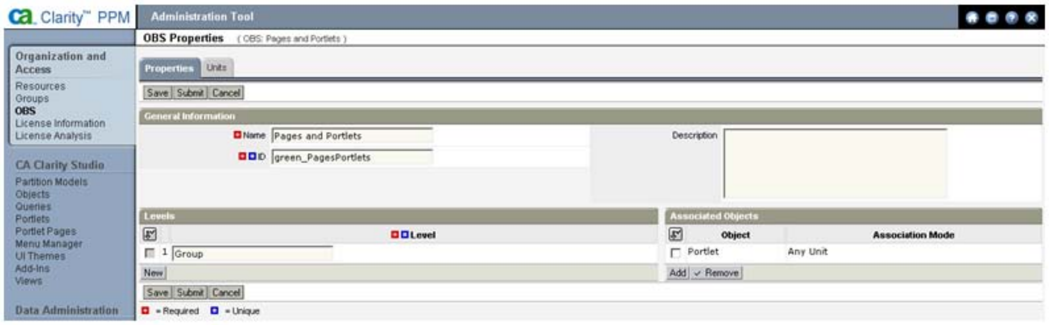
	Group	ID	Description	Status
□	All Department Managers	green_AllDepartmentManagers		Active
□	All Project Managers	green_AllProjectManagers		Active
□	All Resources	green_AllResources		Active
□	Corporate PMO	green_CorporatePMO		Active
□	Executives	green_Executives		Active

Total Results: 5

Now, the Data Scope must be delimited.

Delimit the Data Scope

1. Create an OBS that is used to categorize the portlets. The new OBS for this example is named Pages and Portlets.



OBS Properties (OBS: Pages and Portlets)

General Information

🟥 Name	Pages and Portlets	Description	
🟥🟦 ID	green_PagesPortlets		

Levels

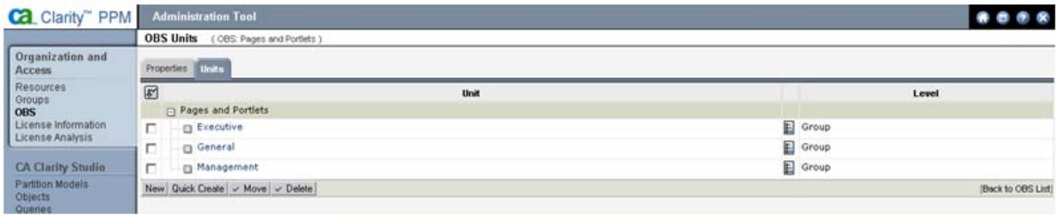
		🟥🟦 Level
□	1	Group

Associated Objects

	Object	Association Mode
□	Portlet	Any Unit

🟥 = Required 🟦 = Unique

2. Under the OBS Pages and Portlets, create the OBS units for the portal categories: Executive, General and Management.

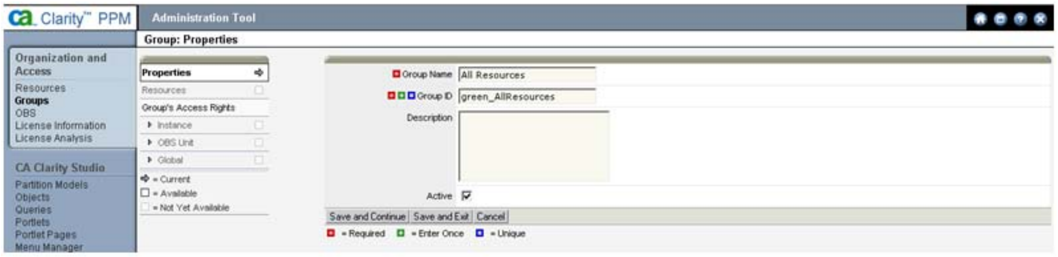


OBS Units (OBS: Pages and Portlets)

	Unit	Level
	⊟ Pages and Portlets	
□	Executive	Group
□	General	Group
□	Management	Group

Grant Access to the Resources

1. To grant access to the resources, start at the All Resources Group level for this example.



Group: Properties

Group Name: All Resources

Group ID: green_AllResources

Description:

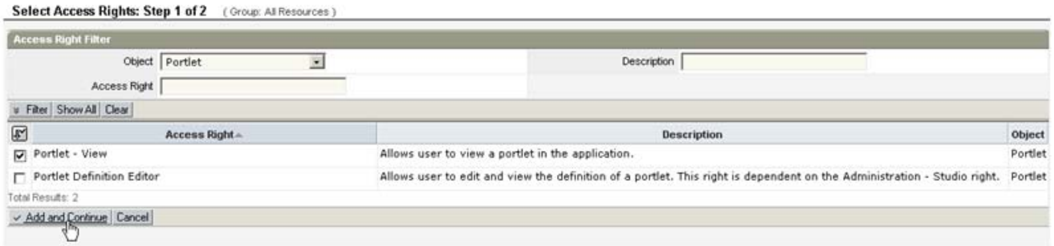
Active: ☑

2. Click OBS Unit under *Group Access Rights* to grant the All Resources Group members access rights using the OBS Pages and Portlets as the Scope delimiter. The Group All Resources does not have any OBS Unit-related access rights yet.

3. Click Add.

4. The access right to be granted is Portlet – View. Use the filter function to locate the item, select it using the checkbox to the left.

5. Click Add and Continue as illustrated in the following graphic:



Select Access Rights: Step 1 of 2 (Group: All Resources)

Object: Portlet

Access Right:

Description:

	Access Right	Description	Object
☑	Portlet - View	Allows user to view a portlet in the application.	Portlet
□	Portlet Definition Editor	Allows user to edit and view the definition of a portlet. This right is dependent on the Administration - Studio right.	Portlet

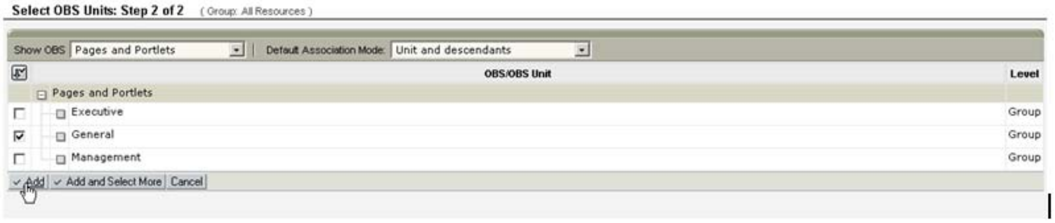
Total Results: 2

6. Select the Scope - the desired OBS Unit.

7. Select a different OBS using the Show OBS attribute. For this example, select the Pages and Portlets: General unit.

   You can select multiple units at a time. Use Add and Select More to keep filtering and adding units if necessary.

8. Click Add as illustrated in the following graphic:

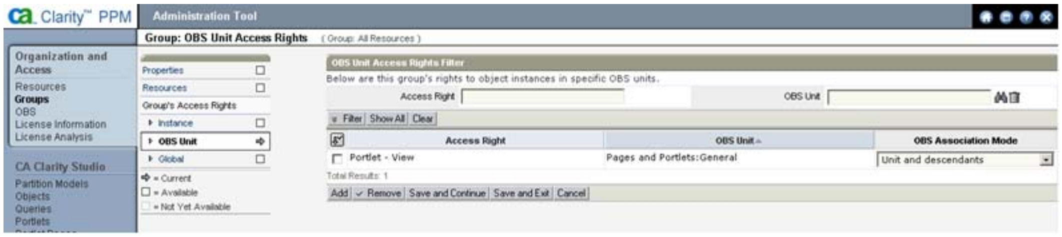


Select OBS Units: Step 2 of 2 (Group: All Resources)

Show OBS: Pages and Portlets | Default Association Mode: Unit and descendants

	OBS/OBS Unit	Level
	⊟ Pages and Portlets	
□	Executive	Group
☑	General	Group
□	Management	Group

9. Define whether the All Resources group should have access to that unit only, the ancestors and or the descendants. Use the OBS Association Mode attribute to select the access. For this example, use the default value: Unit and descendants.



Group: OBS Unit Access Rights (Group: All Resources)

OBS Unit Access Rights Filter

Below are this group's rights to object instances in specific OBS units.

Access Right:
OBS Unit:

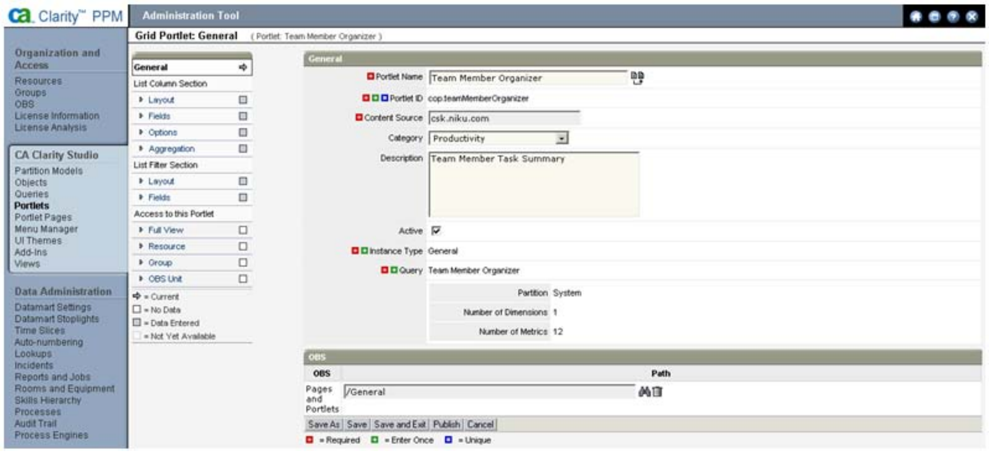
	Access Right	OBS Unit	OBS Association Mode
□	Portlet - View	Pages and Portlets:General	Unit and descendants

Total Results: 1

Note: If General unit has sub-units, then portlets related to such lower-level units should also be considered as part of the General unit. The All Resources group is granted access for those sub-units.

Confirmation

The Team Member Organizer portlet has been categorized as a General portlet. All members of the All Resources group have access to it.



Grid Portlet: General (Portlet: Team Member Organizer)

General

Portlet Name: Team Member Organizer
Portlet ID: cop.teamMemberOrganizer
Content Source: csk.niku.com
Category: Productivity
Description: Team Member Task Summary
Active: ☑
Instance Type: General
Query: Team Member Organizer
Partition: System
Number of Dimensions: 1
Number of Metrics: 12

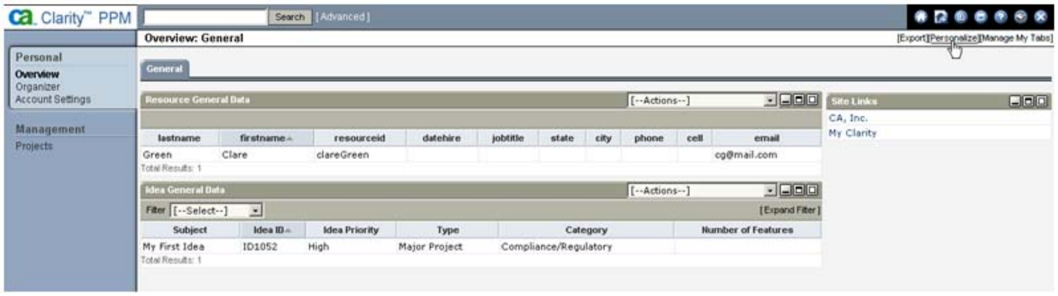
OBS

OBS	Path
Pages and Portlets	/General

Clare Green, a fictitious resource, is a member of the All Resources group. She logs in to the CA Clarity PPM to personalize her Overview Page.

To personalize an Overview page do the following

1. Click Personalize.



Overview: General

Resource General Data

lastname	firstname	resourceid	datehire	jobtitle	state	city	phone	cell	email
Green	Clare	clareGreen							cg@mail.com

Total Results: 1

Idea General Data

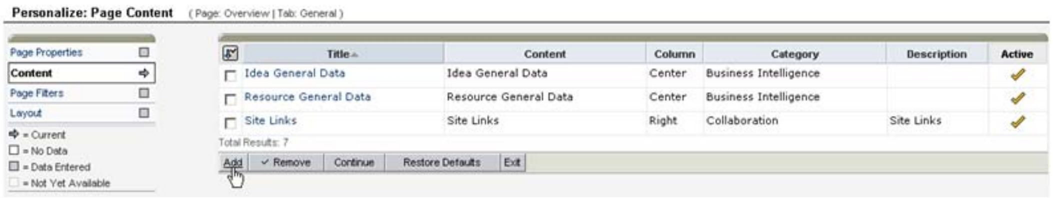
Subject	Idea ID	Idea Priority	Type	Category	Number of Features
My First Idea	ID1052	High	Major Project	Compliance/Regulatory	

Total Results: 1

Site Links

CA, Inc.
My Clarity

2. From the Content sub page, Clare clicks Add to add new portlets.



Personalize: Page Content (Page: Overview | Tab: General)

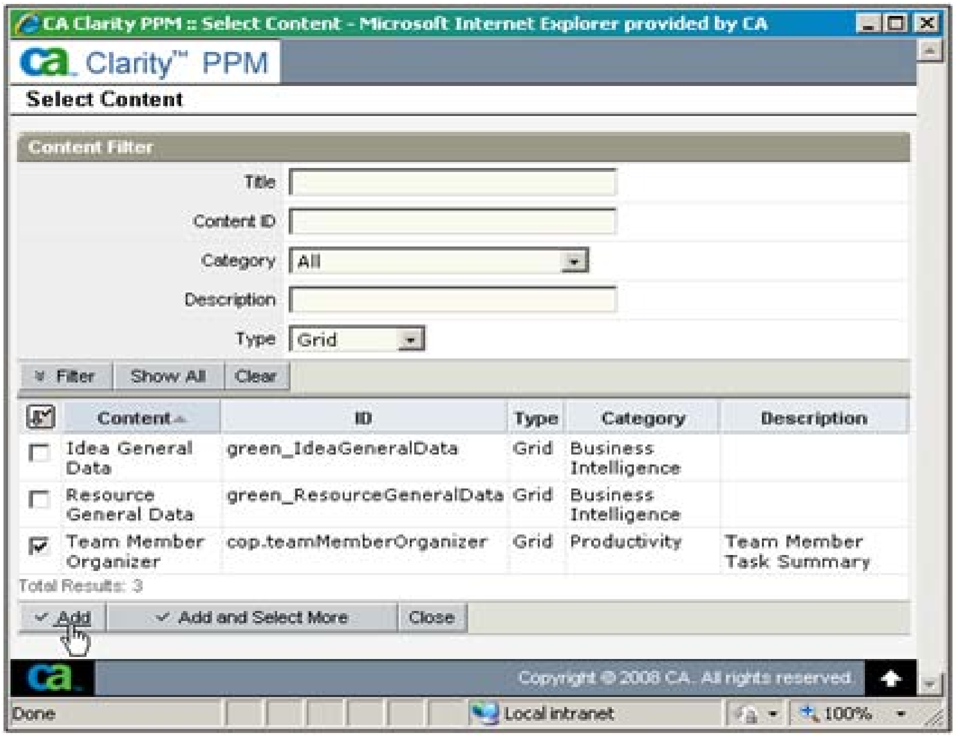
	Title	Content	Column	Category	Description	Active
□	Idea General Data	Idea General Data	Center	Business Intelligence		✓
□	Resource General Data	Resource General Data	Center	Business Intelligence		✓
□	Site Links	Site Links	Right	Collaboration	Site Links	✓

Total Results: 7

Clare sees a list of portlets that are available to her.

3. Filter the Grid portlets to find and select the Team Member Organizer.

4. Click Add.


CA Clarity PPM :: Select Content - Microsoft Internet Explorer provided by CA
Clarity™ PPM
Content Filter
Filter
Show All
Clear
Add
Add and Select More
Close
Copyright © 2008 CA. All rights reserved.
Done
Local intranet
100%

Select Content

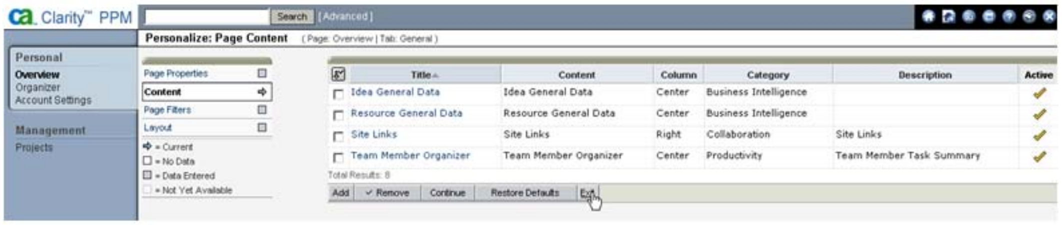
Title	
Content ID	
Category	All
Description	
Type	Grid

	Content	ID	Type	Category	Description
□	Idea General Data	green_IdeaGeneralData	Grid	Business Intelligence	
□	Resource General Data	green_ResourceGeneralData	Grid	Business Intelligence	
☑	Team Member Organizer	cop.teamMemberOrganizer	Grid	Productivity	Team Member Task Summary

Total Results: 3

The portlet has been added.

5. Click Exit to see the results.

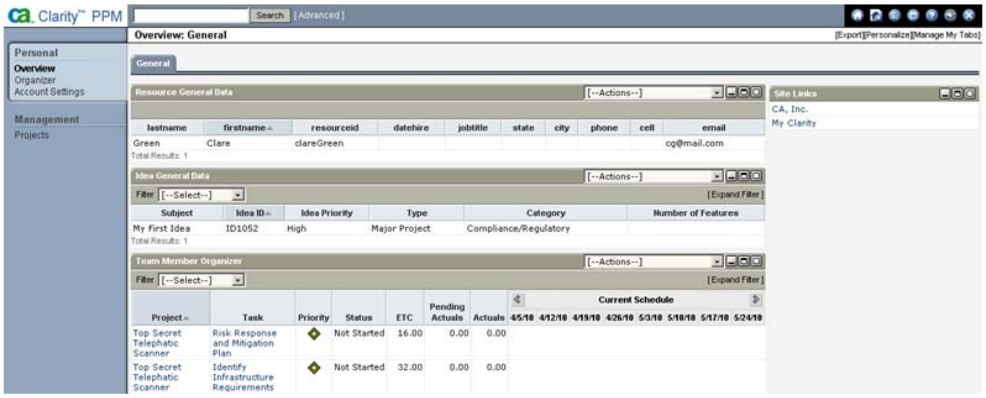


Personalize: Page Content (Page: Overview | Tab: General)

	Title	Content	Column	Category	Description	Active
□	Idea General Data	Idea General Data	Center	Business Intelligence		✓
□	Resource General Data	Resource General Data	Center	Business Intelligence		✓
□	Site Links	Site Links	Right	Collaboration	Site Links	✓
□	Team Member Organizer	Team Member Organizer	Center	Productivity	Team Member Task Summary	✓

Total Results: 8

The Team Member Organizer portlet now appears on Clare's Overview Page.



Resource General Data

lastname	firstname	resourceid	datehire	jobtitle	state	city	phone	cell	email
Green	Clare	clareGreen							cg@mail.com

Total Results: 1

Idea General Data

Subject	Idea ID	Idea Priority	Type	Category	Number of Features
My First Idea	ID1052	High	Major Project	Compliance/Regulatory	

Total Results: 1

Team Member Organizer

							Current Schedule							
Project	Task	Priority	Status	ETC	Pending Actuals	Actuals	4/5/10	4/12/10	4/19/10	4/26/10	5/3/10	5/10/10	5/17/10	5/24/10
Top Secret Telephatic Scanner	Risk Response and Mitigation Plan	◆	Not Started	16.00	0.00	0.00								
Top Secret Telephatic Scanner	Identify Infrastructure Requirements	◆	Not Started	32.00	0.00	0.00								

Do the following for the resource groups All Project Managers and All Department Managers:

1. Select the All Project Managers resource group on the Group page in the Administration Tool.
2. For this group, select OBS Unit under Group Access Rights.
3. Click Add.
4. Use the filter function to locate the access right and select it using the checkbox to the left.

   Note: The access right to be granted is Portlet – View.

5. Click Add and Continue.
6. Select the OBS Unit *Management*. This is the portlet category for the managers group.
7. Define the level of access using the OBS Association Mode attribute.
8. Use the default Unit and descendants for this example.
9. Repeat this process for the All Department Managers group.
10. When completed, these two groups have the same access for the portlets and pages.

    For the Executive group, follow the same instructions except you start with the Executive group and select the OBS Unit Executive for access to the portlets categorized in the Executive OBS unit.

When all the selections are complete, the configuration is:

- Members of the All Resources group have access to the portlets in the General OBS unit.
- Members of the All Project Managers and All Department Managers groups have access to the portlets in the Management OBS unit.
- Members of the Executive group have access to the Executives OBS Unit.

Building Secure Portlets

When you create a CA Clarity PPM portlet you may use three different types of data sources:

System

These are restricted CA Clarity PPM-provided system data sources; you do not have access to change what they do and how they behave.

Objects

Use CA Clarity PPM Objects as data source.

Queries

These are queries you may build using NSQL to be used as the data source.

CA Clarity PPM applies security rules automatically when using System and Objects for building portlets.

Note: Inform CA Clarity PPM how to apply security to a custom NSQL query as it does not happen automatically for you.

To build a secure portlet, do the following

- Apply security using NSQL query (see page 98)
- Build and Test the Query (see page 98)
- Create the Query in CA Clarity PPM Studio (see page 99)
- Create a Portlet (see page 100)

Applying Security Using an NSQL Query

Use an NSQL clause @WHERE: SECURITY to apply security for a query in CA Clarity PPM using a specific Object rules.

The syntax of this NSQL Clause is:

```
@WHERE: SECURITY :<OBJECTNAME>:<INTERNAL ID ATTRIBUTE>@
```

Example:

The following expression tells CA Clarity PPM to apply resource security to this query, and specifies that RES.ID is the attribute that corresponds to the Resource Object internal ID for identifying Resource Instances.

```
@WHERE:SECURITY:RESOURCE:RES.ID@
```

Building and Testing the Query

Build a secure Query. Build a list of resources, including defined contact data that is made available for a portlet but only lists resources relevant to the user. This should be the same resources that the end users are allowed to see when selecting Resources in the CA Clarity PPM menu.

1. Identify and define the SQL. In this case, this includes some general resource data and associated contact info. An example of the SQL query for this information:

```
SELECT
R.UNIQUE_NAME,      R.LAST_NAME,     R.FIRST_NAME,
R.DATE_OF_HIRE,     R.EMAIL,                 C.JOB_TITLE,
C.STATE_PROVINCE,   C.CITY,          C.PHONE_WORK,
C.PHONE_CELL
FROM SRM_RESOURCES R
LEFT OUTER JOIN SRM_CONTACTS C
ON C.principal_id = R.ID
AND c.principal_type = 'RESOURCE'
AND c.is_active = 1
WHERE
R.is_active = 1
    AND r.person_type=300
```

2. Edit and modify into an NSQL query by inserting NSQL clauses:

```
SELECT
@SELECT:DIM:USER_DEF:IMPLIED:RES:R.UNIQUE_NAME:ResourceID@,
@SELECT:DIM_PROP:USER_DEF:IMPLIED:RES:R.LAST_NAME:LastName@,
@SELECT:DIM_PROP:USER_DEF:IMPLIED:RES:R.FIRST_NAME:FirstName@,
@SELECT:DIM_PROP:USER_DEF:IMPLIED:RES:R.DATE_OF_HIRE:DateHire@,
@SELECT:DIM_PROP:USER_DEF:IMPLIED:RES:R.EMAIL:eMail@,
@SELECT:DIM_PROP:USER_DEF:IMPLIED:RES:C.JOB_TITLE:JobTitle@,
@SELECT:DIM_PROP:USER_DEF:IMPLIED:RES:C.STATE_PROVINCE:State@,
@SELECT:DIM_PROP:USER_DEF:IMPLIED:RES:C.CITY:City@,
@SELECT:DIM_PROP:USER_DEF:IMPLIED:RES:C.PHONE_WORK:Phone@,
@SELECT:DIM_PROP:USER_DEF:IMPLIED:RES:C.PHONE_CELL:Cell@
FROM SRM_RESOURCES R
LEFT OUTER JOIN SRM_CONTACTS C
```

```
ON C.principal_id = R.ID
AND c.principal_type = 'RESOURCE'
AND c.is_active = 1
WHERE
R.is_active = 1
    AND r.person_type=300
    AND @FILTER@
```

3. Use the NSQL statement to create a portlet.

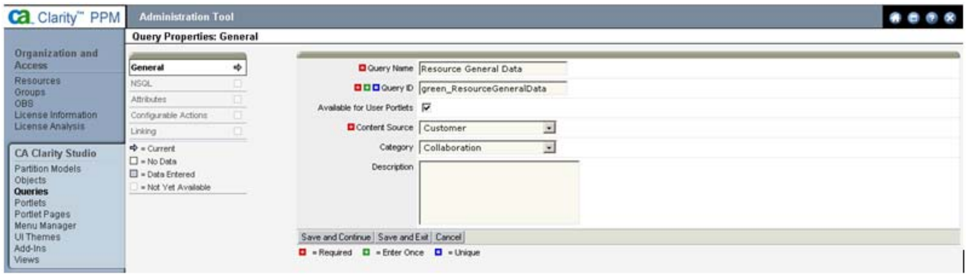
Creating the Query in CA Clarity PPM Studio

The use case shows how to create a query in two steps. First without the security statement and then adding the security statement at a later step. This helps demonstrate the effects of having queries without security and with security. The best practice is to always create queries using the appropriate security statements from the beginning.

To create a query

1. Select Queries from the CA Clarity PPM Studio Menu.

2. Select the General option. Define the properties for the new query.



Query Properties: General

🟥 Query Name: Resource General Data

🟥🟩🟦 Query ID: green_ResourceGeneralData

Available for User Portlets: ☑

🟥 Content Source: Customer

Category: Collaboration

Description:

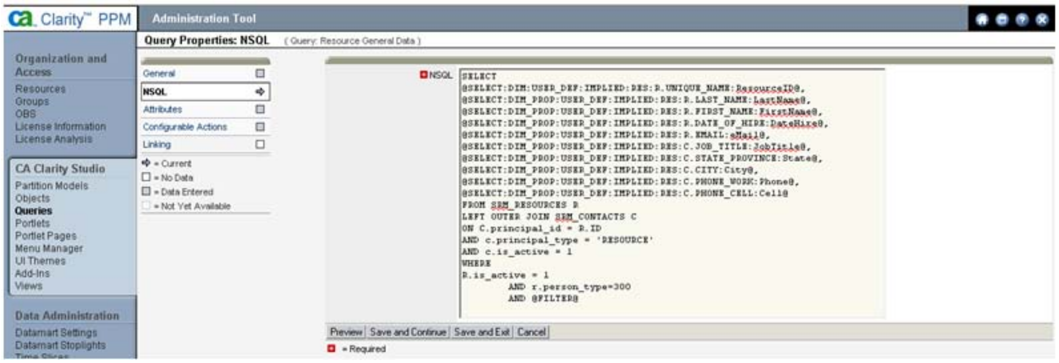
3. Click Save, and Continue.

4. Select NSQL. Insert the NSQL clauses without the security statement.

5. Click Save and Exit for this example.

6. Click Save and Continue, if you want to select other options for your query.

   Note: For more information, see the *CA Clarity PPM Studio Developers Guide*.



NSQL

```
SELECT
@SELECT:DIM:USER_DEF:IMPLIED:RES:R.UNIQUE_NAME:ResourceID@,
@SELECT:DIM_PROP:USER_DEF:IMPLIED:RES:R.LAST_NAME:LastName@,
@SELECT:DIM_PROP:USER_DEF:IMPLIED:RES:R.FIRST_NAME:FirstName@,
@SELECT:DIM_PROP:USER_DEF:IMPLIED:RES:R.DATE_OF_HIRE:DateHire@,
@SELECT:DIM_PROP:USER_DEF:IMPLIED:RES:R.EMAIL:eMail@,
@SELECT:DIM_PROP:USER_DEF:IMPLIED:RES:C.JOB_TITLE:JobTitle@,
@SELECT:DIM_PROP:USER_DEF:IMPLIED:RES:C.STATE_PROVINCE:State@,
@SELECT:DIM_PROP:USER_DEF:IMPLIED:RES:C.CITY:City@,
@SELECT:DIM_PROP:USER_DEF:IMPLIED:RES:C.PHONE_WORK:Phone@,
@SELECT:DIM_PROP:USER_DEF:IMPLIED:RES:C.PHONE_CELL:Cell@
FROM SRM_RESOURCES R
LEFT OUTER JOIN SRM_CONTACTS C
ON C.principal_id = R.ID
AND c.principal_type = 'RESOURCE'
AND c.is_active = 1
WHERE
R.is_active = 1
        AND r.person_type=300
        AND @FILTER@
```

Creating a Portlet

To create a portlet do the following

1. Navigate to the Portlets page in the Administration tool, Select New Portlet, Grid Portlet.

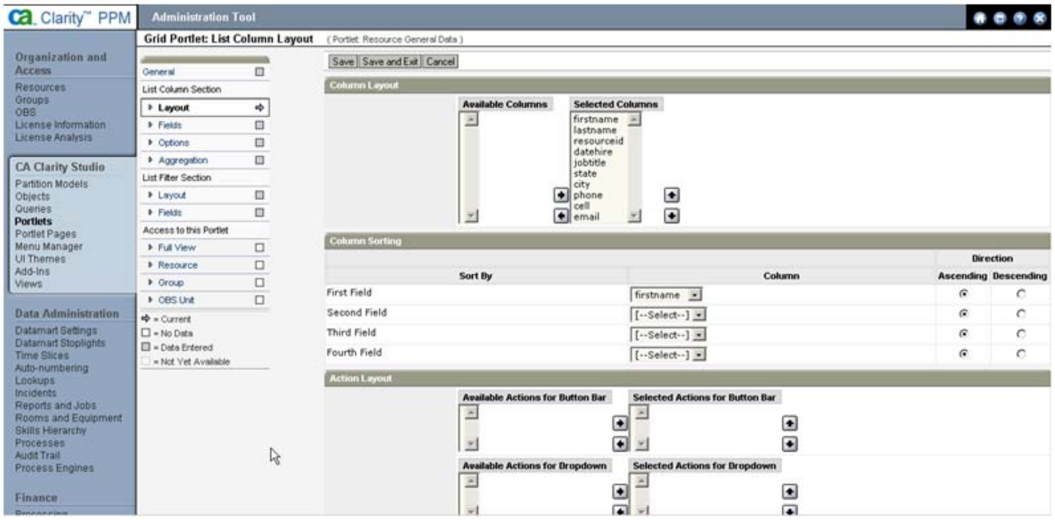
   Note: The first step of creating a portlet may differ slightly for different CA Clarity PPM versions.

2. Define the general portlet properties.

3. Select Finish, and Open when you are done.

   The new portlet Resource General Data is created. It is assigned to *OBS Portlets*: *General* so that all resources have access to this portlet.

4. Select the portlet Layout option. Select the attributes you want to display.



Selected Columns: firstname, lastname, resourceid, datehire, jobtitle, state, city, phone, cell, email

Sort By	Column	Direction Ascending	Direction Descending
First Field	firstname	●	○
Second Field	[--Select--]	●	○
Third Field	[--Select--]	●	○
Fourth Field	[--Select--]	●	○

To confirm do the following

1. Log in as Clare Green, and add the portlet to her Home Page.

   Note: Clare can see the personal data of 149 people. She does not have Resource – View access to all of these resources, so she should not be able to see them in this portlet. This is not correct; changes are required to filter the data in the portlet.

2. Apply security to the NSQL Query to correct this.

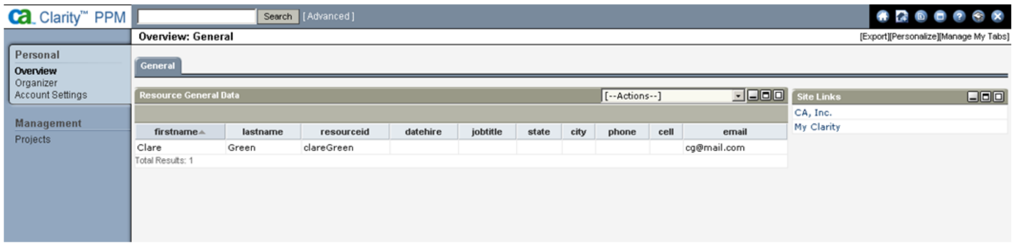
3. Add the following statement to the NSQL Query:

   ```
   AND @WHERE:SECURITY:RESOURCE:R.ID@
   ```

   so that it now reads:

   ```
   SELECT
   @SELECT:DIM:USER_DEF:IMPLIED:RES:R.UNIQUE_NAME:ResourceID@,
   @SELECT:DIM_PROP:USER_DEF:IMPLIED:RES:R.LAST_NAME:LastName@,
   @SELECT:DIM_PROP:USER_DEF:IMPLIED:RES:R.FIRST_NAME:FirstName@,
   @SELECT:DIM_PROP:USER_DEF:IMPLIED:RES:R.DATE_OF_HIRE:DateHire@,
   @SELECT:DIM_PROP:USER_DEF:IMPLIED:RES:R.EMAIL:eMail@,
   @SELECT:DIM_PROP:USER_DEF:IMPLIED:RES:C.JOB_TITLE:JobTitle@,
   @SELECT:DIM_PROP:USER_DEF:IMPLIED:RES:C.STATE_PROVINCE:State@,
   @SELECT:DIM_PROP:USER_DEF:IMPLIED:RES:C.CITY:City@,
   @SELECT:DIM_PROP:USER_DEF:IMPLIED:RES:C.PHONE_WORK:Phone@,
   @SELECT:DIM_PROP:USER_DEF:IMPLIED:RES:C.PHONE_CELL:Cell@
   FROM SRM_RESOURCES R
   LEFT OUTER JOIN SRM_CONTACTS C
   ON C.principal_id = R.ID
   AND c.principal_type = 'RESOURCE'
   AND c.is_active = 1
   WHERE
   R.is_active = 1
       AND r.person_type=300
       AND @FILTER@
       AND @WHERE:SECURITY:RESOURCE:R.ID@
   ```

   The modified results are illustrated in the following graphic. Clare only has access to her own Resource information, as this is the resource she has Resource – View rights on.



firstname	lastname	resourceid	datehire	jobtitle	state	city	phone	cell	email
Clare	Green	clareGreen							cg@mail.com

Total Results: 1

Granting End User Permission to Configure Portlets

All portlets have two available attributes in the Options subpage that may be seen as related to security, as they are used to allow or prohibit users from configuring portlets in their workspaces:

Allow Configuration

This option is set by the administrator to allow end users to configure that specific portlet. If the option is not set, end users do not have access to the Configure action in the Actions drop-down list.

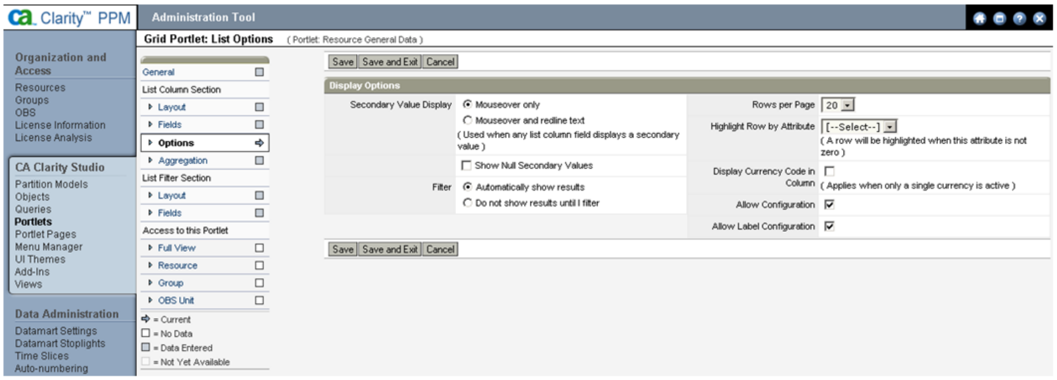
Allow Label Configuration

This option is set by the administrator to allow end users to change labels in that specific portlet. If the option is not set, end users cannot alter Labels, as they are displayed as read-only.

For this example, use the Resource General Data portlet.

Use Case: Options Enabled

The Administrator has enabled both options. This means end users can configure the portlet and can change the labels as illustrated in the following graphic:



Grid Portlet: List Options (Portlet: Resource General Data)

Display Options

Secondary Value Display ● Mouseover only ○ Mouseover and redline text

(Used when any list column field displays a secondary value)

□ Show Null Secondary Values

Filter ● Automatically show results ○ Do not show results until I filter

Rows per Page 20

Highlight Row by Attribute [--Select--]

(A row will be highlighted when this attribute is not zero)

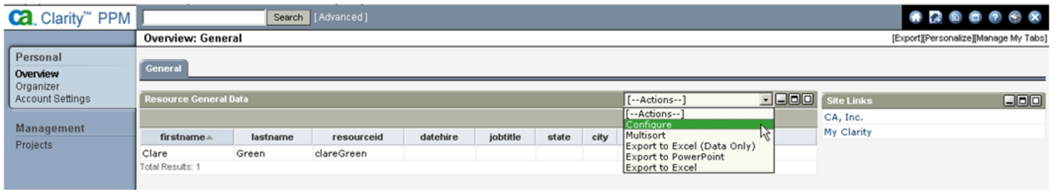
Display Currency Code in Column □

(Applies when only a single currency is active)

Allow Configuration ☑

Allow Label Configuration ☑

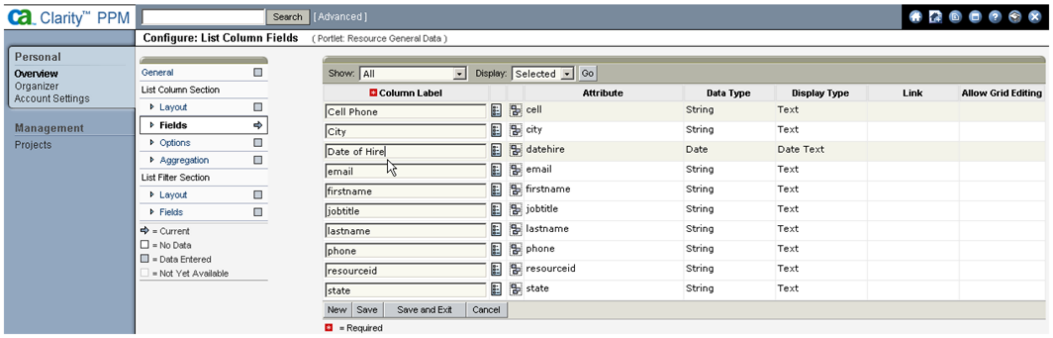
Clare Green can access the configuration action and change labels:



Overview: General

firstname	lastname	resourceid	datehire	jobtitle	state	city
Clare	Green	clareGreen				

Total Results: 1

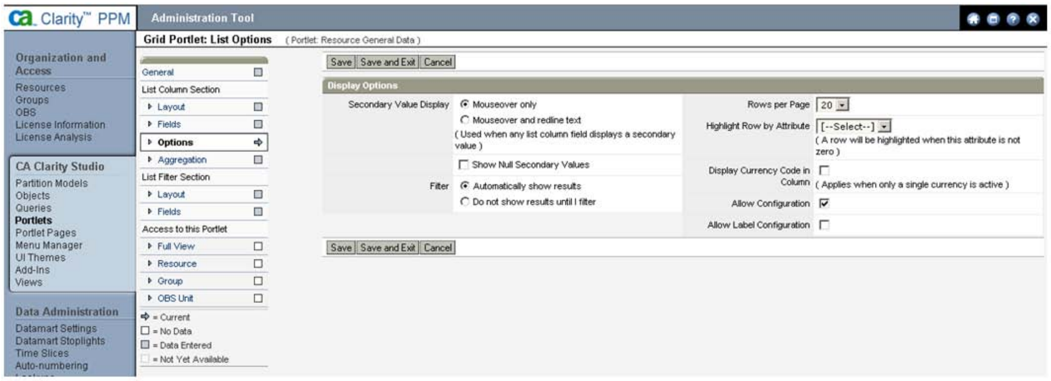


Configure: List Column Fields (Portlet: Resource General Data)

Column Label	Attribute	Data Type	Display Type	Link	Allow Grid Editing
Cell Phone	cell	String	Text		
City	city	String	Text		
Date of Hire	datehire	Date	Date Text		
email	email	String	Text		
firstname	firstname	String	Text		
jobtitle	jobtitle	String	Text		
lastname	lastname	String	Text		
phone	phone	String	Text		
resourceid	resourceid	String	Text		
state	state	String	Text		

Use Case: Options Disabled

The Administrator has disabled Allow Label Configuration for the portlet as illustrated below:



Grid Portlet: List Options (Portlet: Resource General Data)

Display Options

Secondary Value Display: ● Mouseover only ○ Mouseover and redline text
(Used when any list column field displays a secondary value)

□ Show Null Secondary Values

Filter: ● Automatically show results ○ Do not show results until I filter

Rows per Page: 20

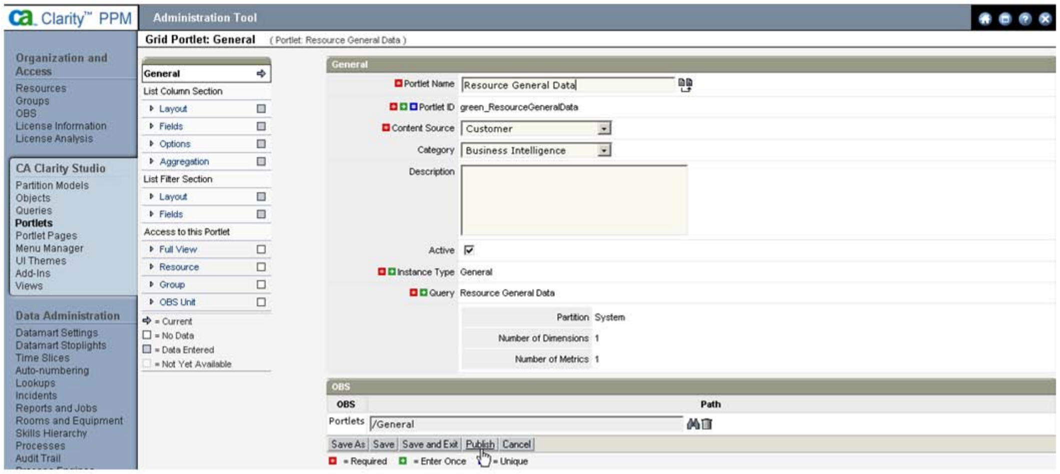
Highlight Row by Attribute: [--Select--]
(A row will be highlighted when this attribute is not zero)

Display Currency Code in Column: □ (Applies when only a single currency is active)

Allow Configuration: ☑

Allow Label Configuration: □

The Administrator has to publish the change forcing it over the end user configurations:



Grid Portlet: General (Portlet: Resource General Data)

General

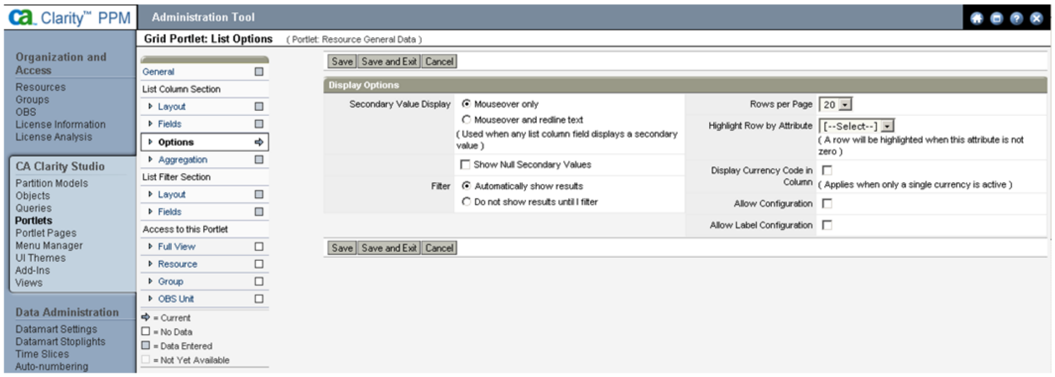
Portlet Name: Resource General Data
Portlet ID: green_ResourceGeneralData
Content Source: Customer
Category: Business Intelligence
Description:
Active: ☑
Instance Type: General
Query: Resource General Data
Partition: System
Number of Dimensions: 1
Number of Metrics: 1

OBS

OBS	Path
Portlets	/General

Clare Green can still access the portlet configuration options. She cannot change portlet labels because they are presented to her as read-only.

The Administrator decides to prohibit end users from making changes to the portlet. The option is disabled by deselecting Allow Configuration.

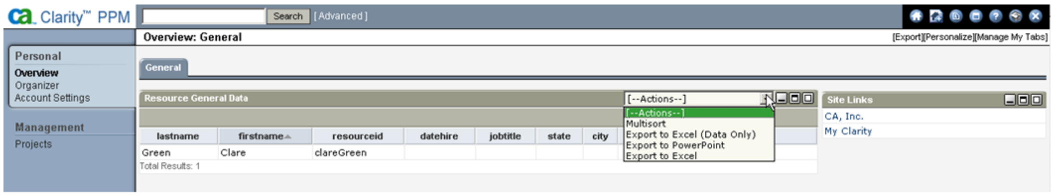


Grid Portlet: List Options (Portlet: Resource General Data)

Display Options

Secondary Value Display: ● Mouseover only ○ Mouseover and redline text
(Used when any list column field displays a secondary value)
□ Show Null Secondary Values
Filter: ● Automatically show results ○ Do not show results until I filter
Rows per Page: 20
Highlight Row by Attribute: [--Select--]
(A row will be highlighted when this attribute is not zero)
Display Currency Code in Column: □
(Applies when only a single currency is active)
Allow Configuration: □
Allow Label Configuration: □

Now, Clare does not see the Configure action in the Actions drop-down list for that portlet. She no longer has access to make configuration or label changes.



Overview: General

Resource General Data

lastname	firstname	resourceid	datehire	jobtitle	state	city
Green	Clare	clareGreen				

Total Results: 1

How to Secure Subpages and Attributes

CA Clarity PPM does not offer field-level security, but it does provide alternatives. It is not possible to determine *who-has-access-to-what-attribute* directly; it is possible to do so using subpages. Subpages are secured using one of two different functionalities, Secure Subpages or Display Conditions.

Securing Attributes Using the Secure Subpages Function

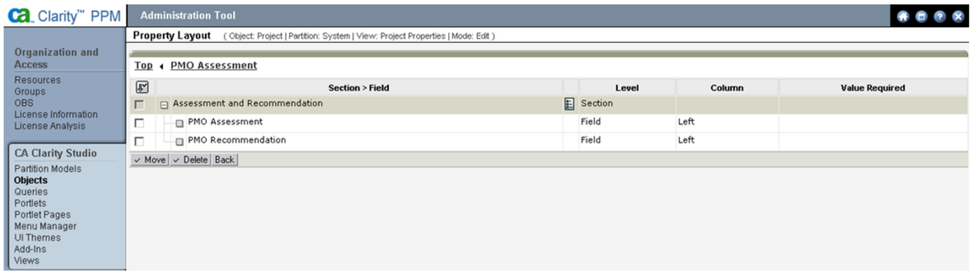
The following use case explores securing attributes using Secure Subpages functionality.

Use Case

> Some attributes in the Project object are reserved for the PMO Assessment. Only members of the Corporate PMO group should be able to view and edit them. The Project Manager team should not have access to those attributes.

Setting Up

- The Actors are the members of the Corporate PMO group. These resources should have access to the PMO attributes.
- The Action: The PMO resources should be able to edit the PMO Assessment attributes in the project.
  - The attributes are grouped in a new Subpage because field-level security is not implemented in CA Clarity PPM.
  - The members of the Corporate PMO Group are granted access to the subpage so they are able to edit the attributes.
- The Data Scope: the PMO group should be able to edit the PMO Assessment attributes for all projects that they have Project – Edit rights on.
- A new subpage, PMO Assessment, has been created in the Project Object to hold PMO Attributes. For now, anyone who has access to projects can see this Subpage.



Property Layout (Object: Project | Partition: System | View: Project Properties | Mode: Edit)

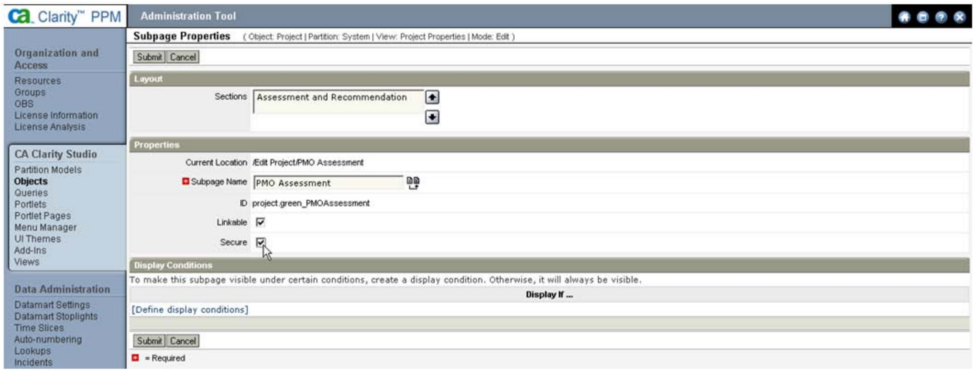
Top ◂ PMO Assessment

	Section > Field	Level	Column	Value Required
□	⊟ Assessment and Recommendation	Section		
□	PMO Assessment	Field	Left	
□	PMO Recommendation	Field	Left	

Thomas Young, a fictitious resource, is a Project Manager. When he accesses CA Clarity PPM and navigates to one of his projects he can see the PMO Assessment subpage. This is not correct; the Project Manager resources should not have access to this new subpage.

To secure and verify properties do the following

- Use Clarity Studio to edit the Subpage Properties and mark it Secure.



Subpage Properties (Object: Project | Partition: System | View: Project Properties | Mode: Edit)

Sections: Assessment and Recommendation

Current Location: /Edit Project/PMO Assessment

Subpage Name: PMO Assessment

ID: project.green_PMOAssessment

Linkable: ☑

Secure: ☑

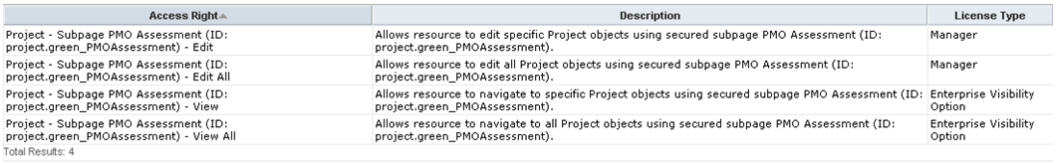
To make this subpage visible under certain conditions, create a display condition. Otherwise, it will always be visible.

Display If ...

[Define display conditions]

= Required

- When this is done, CA Clarity PPM Studio automatically creates Access Rights, which enable you to secure the subpage.



Access Right	Description	License Type
Project - Subpage PMO Assessment (ID: project.green_PMOAssessment) - Edit	Allows resource to edit specific Project objects using secured subpage PMO Assessment (ID: project.green_PMOAssessment).	Manager
Project - Subpage PMO Assessment (ID: project.green_PMOAssessment) - Edit All	Allows resource to edit all Project objects using secured subpage PMO Assessment (ID: project.green_PMOAssessment).	Manager
Project - Subpage PMO Assessment (ID: project.green_PMOAssessment) - View	Allows resource to navigate to specific Project objects using secured subpage PMO Assessment (ID: project.green_PMOAssessment).	Enterprise Visibility Option
Project - Subpage PMO Assessment (ID: project.green_PMOAssessment) - View All	Allows resource to navigate to all Project objects using secured subpage PMO Assessment (ID: project.green_PMOAssessment).	Enterprise Visibility Option

Total Results: 4

- You can verify that the group already has some OBS Unit access rights for viewing and editing projects. Navigate to the *Group: OBS Unit Access Rights* page to view the current access rights.

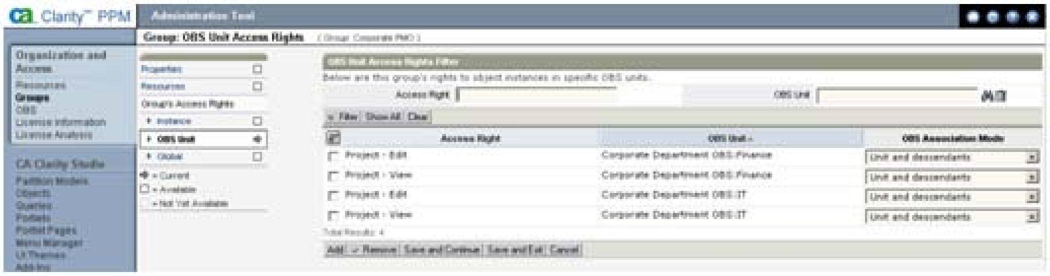
Select and Grant Access Rights to a Secured Subpage

Grant the Corporate PMO members the proper access to the PMO Assessment subpage for the same scope.

To select and grant access rights do the following

1. From the Administration Tool, Select Groups.

2. Select OBS Unit to navigate to the OBS Unit Rights for the Group Corporate PMO.



Group: OBS Unit Access Rights (Group: Corporate PMO)

OBS Unit Access Rights Filter

Below are this group's rights to object instances in specific OBS units.

Access Right

OBS Unit

	Access Right	OBS Unit	OBS Association Mode
□	Project - Edit	Corporate Department OBS:Finance	Unit and descendants
□	Project - View	Corporate Department OBS:Finance	Unit and descendants
□	Project - Edit	Corporate Department OBS:IT	Unit and descendants
□	Project - View	Corporate Department OBS:IT	Unit and descendants

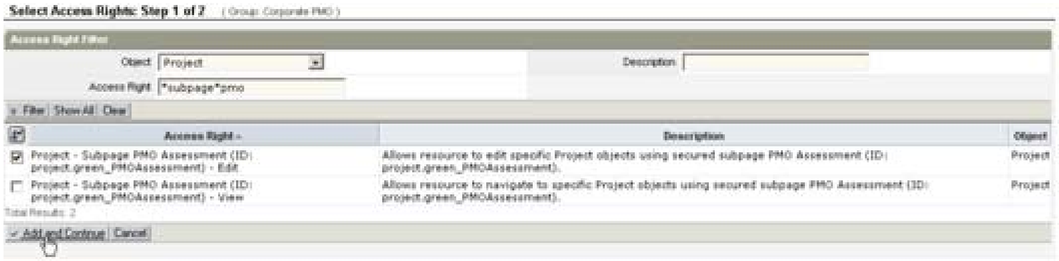
Total Results: 4

3. Click Add on the Group: OBS Unit Access Rights page.

4. Use the filter to locate the Project – Subpage PMO Assessment right.

5. Select the access right.

6. Click Add and Continue.



Select Access Rights: Step 1 of 2 (Group: Corporate PMO)

Access Right Filter

Object: Project

Description:

Access Right: *subpage*pmo

	Access Right	Description	Object
☑	Project - Subpage PMO Assessment (ID: project.green_PMOAssessment) - Edit	Allows resource to edit specific Project objects using secured subpage PMO Assessment (ID: project.green_PMOAssessment).	Project
□	Project - Subpage PMO Assessment (ID: project.green_PMOAssessment) - View	Allows resource to navigate to specific Project objects using secured subpage PMO Assessment (ID: project.green_PMOAssessment).	Project

Total Results: 2

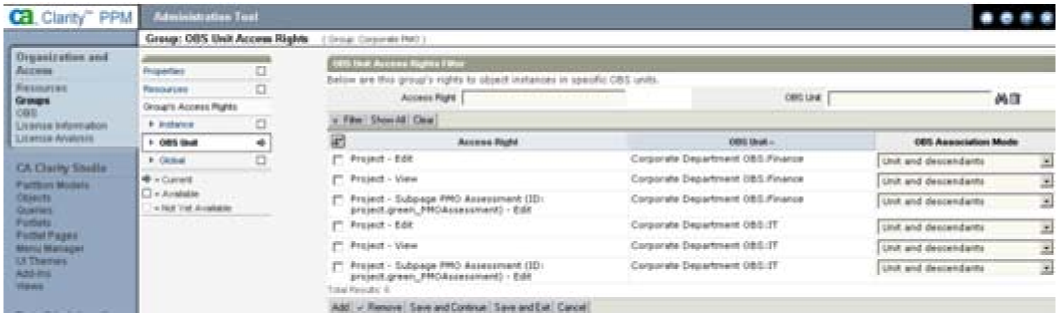
Now, delimit the Data Scope.

7. Select the same projects that the PMO group has Edit rights to.

   For this example, select the IT and Finance OBS Units.

8. Click Add.

   Access has been granted.



Group: OBS Unit Access Rights (Group: Corporate PMO)

OBS Unit Access Rights Filter

Below are this group's rights to object instances in specific OBS units.

Access Right:

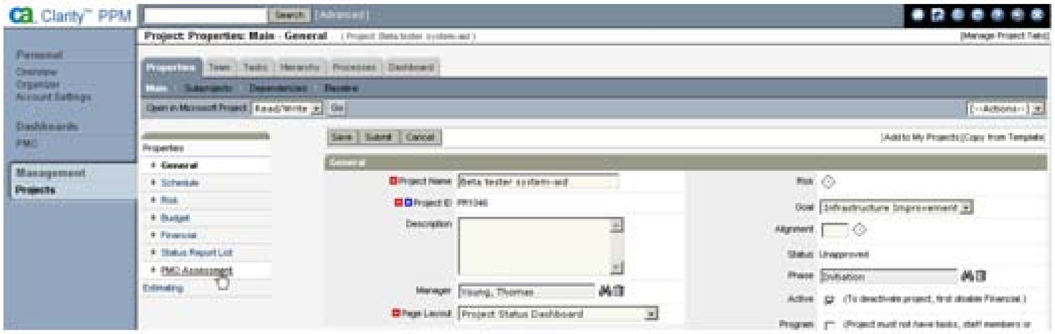
OBS Unit:

☑	Access Right	OBS Unit	OBS Association Mode
☐	Project - Edit	Corporate Department OBS:Finance	Unit and descendants
☐	Project - View	Corporate Department OBS:Finance	Unit and descendants
☐	Project - Subpage PMO Assessment (ID: project.green_PMOAssessment) - Edit	Corporate Department OBS:Finance	Unit and descendants
☐	Project - Edit	Corporate Department OBS:IT	Unit and descendants
☐	Project - View	Corporate Department OBS:IT	Unit and descendants
☐	Project - Subpage PMO Assessment (ID: project.green_PMOAssessment) - Edit	Corporate Department OBS:IT	Unit and descendants

Total Results: 6

Confirmation

- Thomas Young, the Project Manager, no longer has access to the PMO Assessment page.
- Cynthia Smith, a member of the Corporate PMO group, is able to view and edit the attributes in the PMO Assessment subpage as indicated in the following graphics.



Project Properties: Main - General (Project: Beta tester system-aid)

General

Project Name: Beta tester system-aid

Project ID: PR1346

Description:

Manager: Young, Thomas

Page Layout: Project Status Dashboard

Risk:

Goal: Infrastructure Improvement

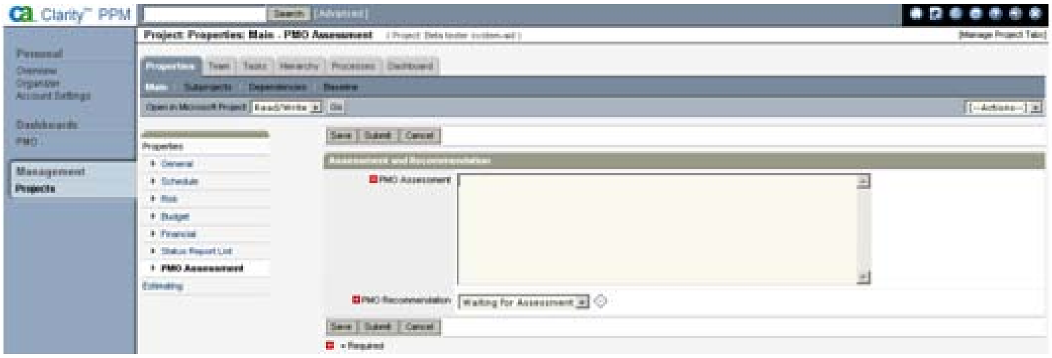
Alignment:

Status: Unapproved

Phase: Initiation

Active: ☑ (To deactivate project, first disable Financial.)

Program: ☐ (Project must not have tasks, staff members or



Project Properties: Main - PMO Assessment (Project: Beta tester system-aid)

Assessment and Recommendation

PMO Assessment:

PMO Recommendation: Waiting For Assessment

= Required

Securing Attributes Using Subpages Display Conditions

The second approach for securing attributes on subpages uses the Display Conditions functionality.

Use Case

A new attribute in the Project object has been created, named Project Manager Notes. This attribute is not intended for all Project viewers – just the members of the All Project Managers group.

Setting Up

- The Actors are the members of the All Project Managers group. These resources should have access to the Project Manager Notes attribute (PM Notes).
- The Actions: Members of the All Project Managers groups should be able to edit the Project Manager Notes attribute for their projects.
  - The attributes are grouped in a new Subpage because field-level security is not implemented in CA Clarity PPM.
  - The members of the All Project Managers Group are granted access to the subpage so they are able to edit the attributes.
- The Data Scope: the Project Manager group should be able to edit the PM Notes attributes for all projects that they have Project – Edit right.
- A new subpage, PM Notes, has been created in the Project Object to hold the Project Manager notes. Anyone who has access to projects can see this Subpage.

  Mary Lamb is a Project Participant. When she accesses CA Clarity PPM and navigates to one of her projects she can see the PM Notes page. This is not correct. The PM Notes subpage must be secured.

Secure the subpage

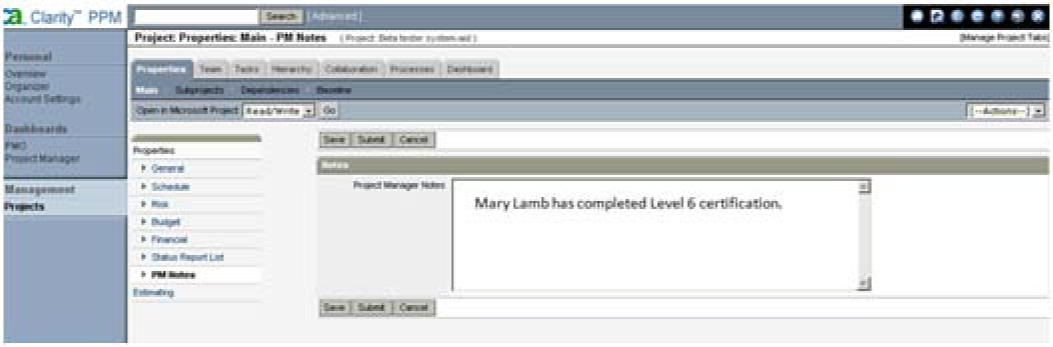
1. Use CA Clarity PPM Studio to edit the Subpage Properties and create a Display Condition.
2. Configure CA Clarity PPM to check whether the user is a member of a specific group. Under the Operation attribute, select Check Resource’s Group.
3. Under the Right attribute, select the group named All Project Managers and click Add.

Note: An expression has been created: Check Resource's Group = 'All Project Managers'.

4. Click Submit.

Confirmation

- Mary Lamb no longer has access to the PM Notes subpage. This page does not display under Properties on the Project: Properties tab.
- When Thomas Young, the Project Manager accesses the same project he can see the PM Notes as illustrated below.



Project Manager Notes: Mary Lamb has completed Level 6 certification.

Securing Lists and Object-Based Portlets

There is an option available only to portlets built having an Object as its data source (object-based portlets) and the object list view. This option is named Attribute Value Protection, and it prohibits users from configuring their portlets to see the value of attributes they should not have access to.

CA Clarity PPM allows the user of both secured Subpages and Display Conditions to define which attributes of an object a specified group of resources has access to. Subpages are only relevant in the Properties view, specifically in the Edit Layout of the view. However, users could configure their List view of an object or object-based portlet to add attributes that should not be accessed causing a security breach. The Attribute Value Protection functionality resolves this problem.

Attribute Value Protection has three possible options:

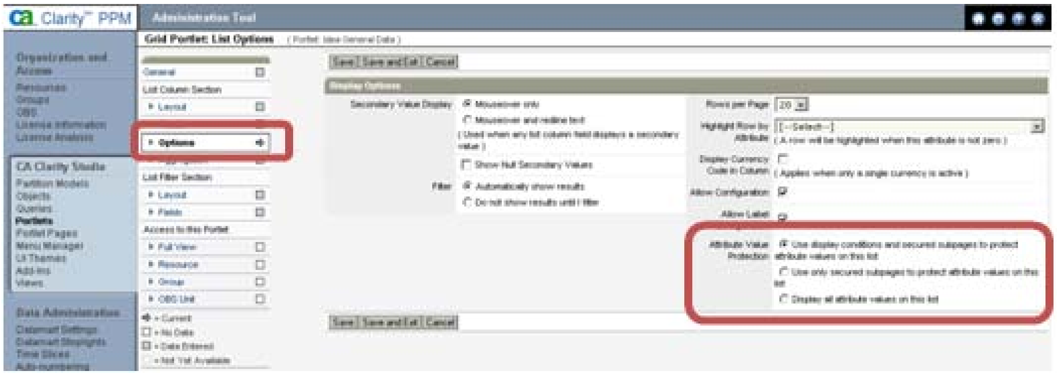
- Use display conditions and secured subpages to protect attribute values on this list
- Use only secured subpages to protect attribute values on this list
- Display all attribute values on this list

The first two options are used to verify that when display conditions or secured subpages are used to protect attributes, these features should also be applied to the List view, thus preserving the values of attributes the end user should not have access to.

The last option is used to disable the application of Display Conditions and Secured Subpages to the List View, allowing end users to access attributes they do not have access to in the Properties view of the object.

The Attribute Value Protection option is available in the Options subpage of an object-based portlet and in the Options section of an object List View.

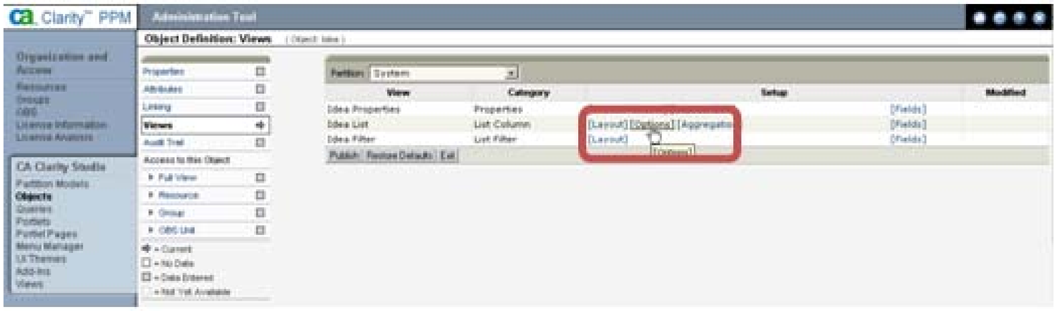
Example of an object-based portlet options subpage:



Grid Portlet: List Options (Portlet: Idea General Data)

Secondary Value Display: ● Mouseover only ○ Mouseover and redline text (Used when any list column field displays a secondary value)
□ Show Null Secondary Values
Filter: ● Automatically show results ○ Do not show results until I filter
Rows per Page: 20
Highlight Row by Attribute: [--Select--] (A row will be highlighted when this attribute is not zero)
Display Currency Code in Column: □ (Applies when only a single currency is active)
Allow Configuration: ☑
Allow Label: ☑
Attribute Value Protection: ● Use display conditions and secured subpages to protect attribute values on this list ○ Use only secured subpages to protect attribute values on this list ○ Display all attribute values on this list

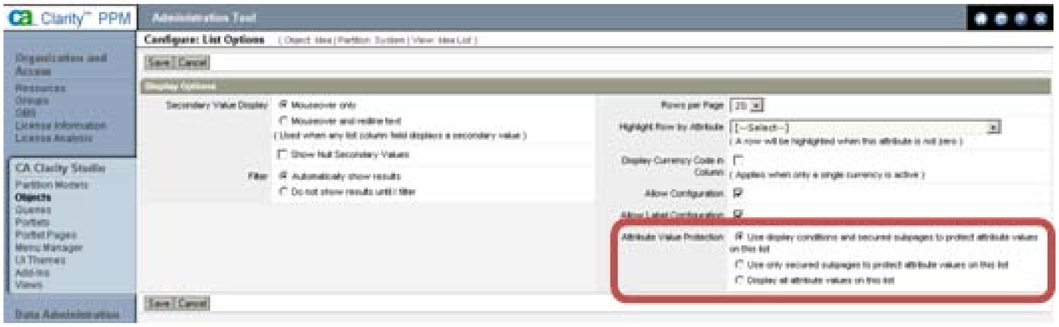
Example of an object list view option:



Object Definition: Views (Object: Idea)

Partition: System

View	Category	Setup		Modified
Idea Properties	Properties		[Fields]	
Idea List	List Column	[Layout] [Options] [Aggregatio	[Fields]	
Idea Filter	List Filter	[Layout]	[Fields]	



Configure: List Options (Object: Idea | Partition: System | View: Idea List)

Secondary Value Display: ● Mouseover only ○ Mouseover and redline text (Used when any list column field displays a secondary value)
□ Show Null Secondary Values
Filter: ● Automatically show results ○ Do not show results until I filter
Rows per Page: 20
Highlight Row by Attribute: [--Select--] (A row will be highlighted when this attribute is not zero)
Display Currency Code in Column: □ (Applies when only a single currency is active)
Allow Configuration: ☑
Allow Label Configuration: ☑
Attribute Value Protection: ● Use display conditions and secured subpages to protect attribute values on this list ○ Use only secured subpages to protect attribute values on this list ○ Display all attribute values on this list

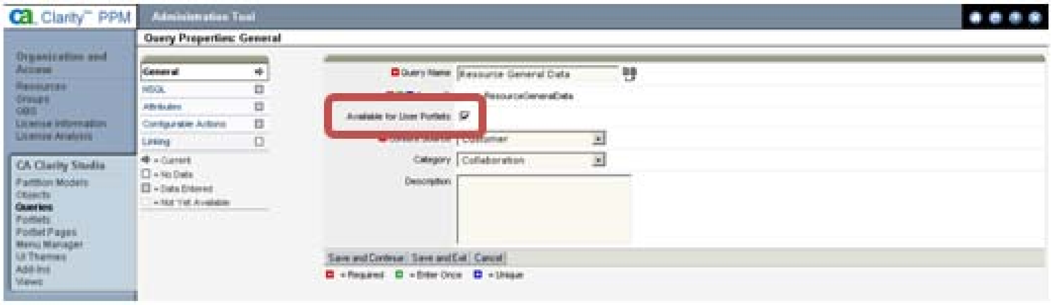
Personal Dashboarding Security

Personal Dashboarding Queries

Before the launch of the Personal Dashboarding option, queries were only available to the Administrator. Therefore, queries had no security applied to them. You could not grant or revoke security access to queries. Access to the CA Clarity PPM Studio was required to access the Queries functionality.

The new Personal Dashboarding option enables end users to create their own portlets. They are also able to use queries in their portlets. They are restricted to using queries that the Administrator has already prepared. End users must be granted access to be able to create portlets and use the pre-designed queries.

When creating a query, Administrators have the option to mark it as Available for User Portlets.



Query Properties: General

Query Name: Resource General Data

ID: ResourceGeneralData

Available for User Portlets ☑

Content Source: Customer

Category: Collaboration

Description:

End users have access to those queries that have been marked as being available for User Portlets.

Personal Dashboarding End-user Portlets

Personal Dashboarding End user portlets have the exact same characteristics as any other portlet. Refer to Securing Portlets (see page 90) for information about how to secure end user Portlets.

Allowing Users to Use Personal Dashboarding

The following four Access Rights relate to the Personal Dashboard functionality:

- To view dashboards, users need Dashboard – Navigate.
- To create dashboards, users need Dashboard – Create.
- To view and configure portlets, users need Portlet – Navigate.
- To create portlets, users need Portlet – Create.

Use Case

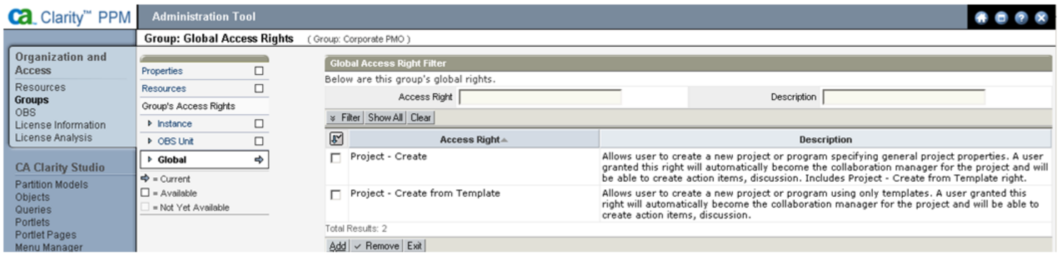
Members of the Corporate PMO group must be able to create their own dashboards and portlets. Cynthia Smith is a member of this group and requires such access.

Setting Up

- Actors - members of the Corporate PMO group
- Actions - Create dashboards and portlets and navigate to those objects
- Scope - dashboards and portlets created by the members of the Corporate PMO group

Review Current Access Rights

Click Global under Group Access Rights to see the global rights the Corporate PMO group has. For this example, assume that they have global rights to create projects.



Group: Global Access Rights (Group: Corporate PMO)

Global Access Right Filter

Below are this group's global rights.

Access Right

Description

	Access Right	Description
□	Project - Create	Allows user to create a new project or program specifying general project properties. A user granted this right will automatically become the collaboration manager for the project and will be able to create action items, discussion. Includes Project - Create from Template right.
□	Project - Create from Template	Allows user to create a new project or program using only templates. A user granted this right will automatically become the collaboration manager for the project and will be able to create action items, discussion.

Total Results: 2

Select and Grant Access Rights

1. Click Add to grant the other rights the group needs.
2. Search for the Dashboard access rights by filtering on “Dash” in the Access Right attribute box.
3. Select the access rights for Dashboard-Create and Dashboard-Navigate.

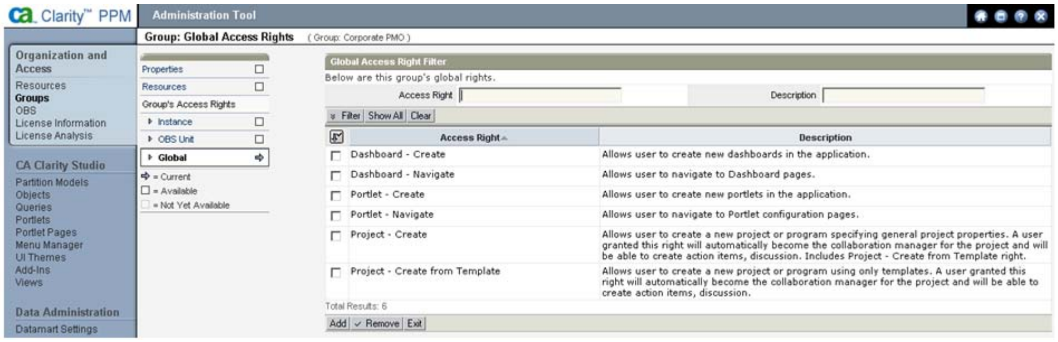
4. Click Add and Select More.

5. Search for the Portlets access rights using the filter “Portlet”.

6. Select the access rights for Portlet-Create and Portlet- Navigate.

7. Click Add.

   Access has been granted for creating and navigating portlets and dashboards as shown in the following graphic:



Group: Global Access Rights (Group: Corporate PMO)

Global Access Right Filter

Below are this group's global rights.

Access Right:

Description:

	Access Right	Description
□	Dashboard - Create	Allows user to create new dashboards in the application.
□	Dashboard - Navigate	Allows user to navigate to Dashboard pages.
□	Portlet - Create	Allows user to create new portlets in the application.
□	Portlet - Navigate	Allows user to navigate to Portlet configuration pages.
□	Project - Create	Allows user to create a new project or program specifying general project properties. A user granted this right will automatically become the collaboration manager for the project and will be able to create action items, discussion. Includes Project - Create from Template right.
□	Project - Create from Template	Allows user to create a new project or program using only templates. A user granted this right will automatically become the collaboration manager for the project and will be able to create action items, discussion.

Total Results: 6

Confirmation

Cynthia Smith is a member of the Corporate PMO group. She now has access to Dashboards and Portlets when she accesses CA Clarity PPM.

Sharing Dashboards with Other Users

The dashboards created using the Personal Dashboard functionality may be shared with other users.

To share dashboards, apply the same rule of thumb as for granting access: consider the Actors, Actions and Scope.

- Actors: Select the target audience - individual resources, Groups, OBS Units members
- Actions: Available actions for Dashboards are Manage and View. You can share management of dashboards or restrict access to viewing only.
- Scope: The Dashboard being shared

Important! Sharing a dashboard does not automatically share the portlets in it.

Note: You must also share the portlets if you want other users to be able to see them. Sharing dashboards and portlets does not ensure that users view the same information as you do, because they may not have the same level of access to the CA Clarity PPM data displayed on those portlets and dashboards, such as resources, projects, ideas, portfolios and other CA Clarity PPM objects.

Sharing a Dashboard with Other Dashboard Managers

Use case

Cynthia is the head of the PMO. She created a Dashboard and wants all PMO members to be able to manage her dashboard. The dashboard is named “Cynthia’s PMO Dashboard.”

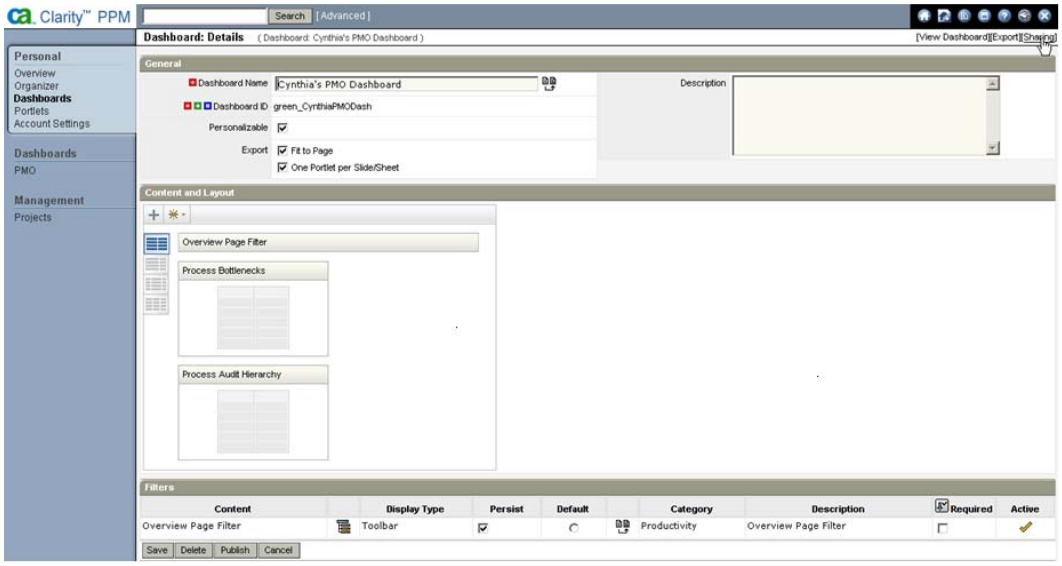
Setting Up

- Actors: all members of PMO group
- Action: granting Manager access to the dashboard Cynthia created.
- Scope: Dashboard created by Cynthia and used by all PMO members

Review the Current Access Rights

1. Cynthia navigates to her dashboard and clicks Sharing on the top right corner.
2. She clicks Groups.

   Currently, no groups have access to the dashboard.



Dashboard: Details (Dashboard: Cynthia's PMO Dashboard)

Dashboard Name: Cynthia's PMO Dashboard

Dashboard ID: green_CynthiaPMODash

Personalizable: ☑

Export: ☑ Fit to Page
☑ One Portlet per Slide/Sheet

Description:

Content		Display Type	Persist	Default		Category	Description	Required	Active
Overview Page Filter		Toolbar	☑	○		Productivity	Overview Page Filter	□	✓

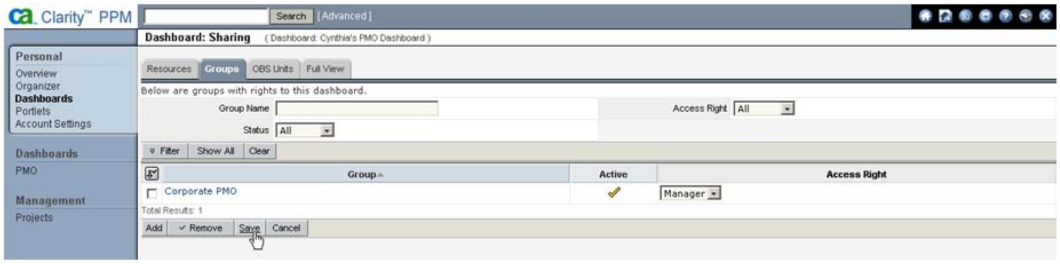
Select and Grant Access Rights

1. Navigate to the Groups tab on the Dashboard.
2. Click Add to grant the Corporate PMO group the Manager Access Right.
3. Use the filter function to locate the group. For example, filter on “c*pmo”.
4. Select the Corporate PMO group.

5. Click Add.

6. Change the Access Right to Manager.

7. Click Save to save the change.



Dashboard: Sharing (Dashboard: Cynthia's PMO Dashboard)

Below are groups with rights to this dashboard.

Group Name: ____ Access Right: All

Status: All

Group	Active	Access Right
□ Corporate PMO	✓	Manager

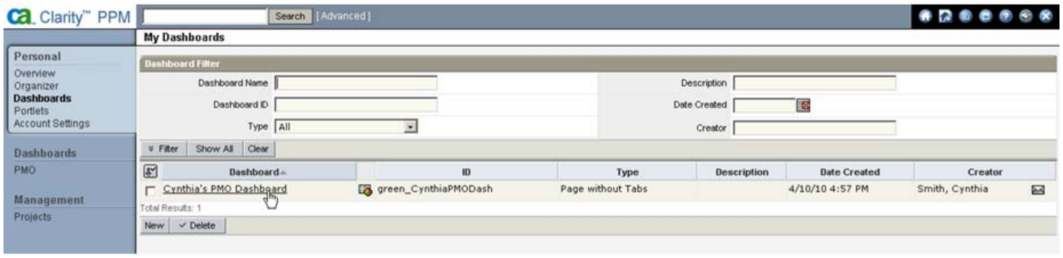
Total Results: 1

8. Click Cancel to go back to the Dashboard.

Confirmation

- Andrew McArthur, a fictitious resource, is a member of the PMO. When he accesses CA Clarity PPM, he can see the dashboard as illustrated in the graphic.

- Andrew has managing rights on this dashboard. He is able to change the layout, add new portlets, or share the dashboard with other users.



My Dashboards

Dashboard Filter

Dashboard Name: ____ Description: ____

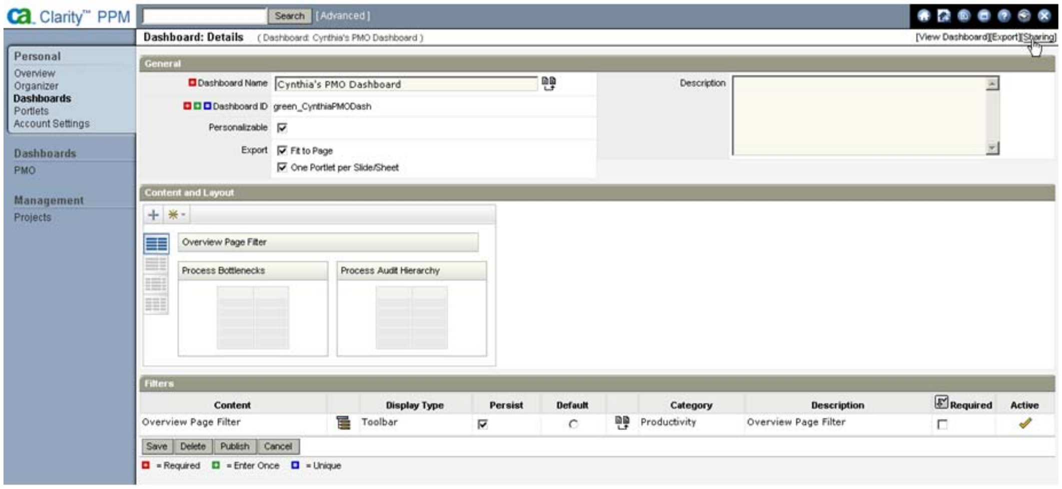
Dashboard ID: ____ Date Created: ____

Type: All Creator: ____

Dashboard	ID	Type	Description	Date Created	Creator
□ Cynthia's PMO Dashboard	green_CynthiaPMODash	Page without Tabs		4/10/10 4:57 PM	Smith, Cynthia

Total Results: 1

- Andrew moves Process Audit Hierarchy next to Process Bottlenecks as illustrated below:



Dashboard: Details (Dashboard: Cynthia's PMO Dashboard)

General

Dashboard Name: Cynthia's PMO Dashboard

Dashboard ID: green_CynthiaPMODash

Personalizable: ☑

Export: ☑ Fit to Page

☑ One Portlet per Slide/Sheet

Description:

Content and Layout

Filters

Content	Display Type	Persist	Default	Category	Description	Required	Active
Overview Page Filter	Toolbar	☑	○	Productivity	Overview Page Filter	□	✓

🟥 = Required 🟩 = Enter Once 🟦 = Unique

Sharing a Dashboard with Dashboard Users

Use case

Andrew is a member of the PMO and manages a dashboard created by Cynthia. He wants all project managers to be able to see this dashboard. Thomas Young is a project manager who will be granted access to the dashboard.

Setting up

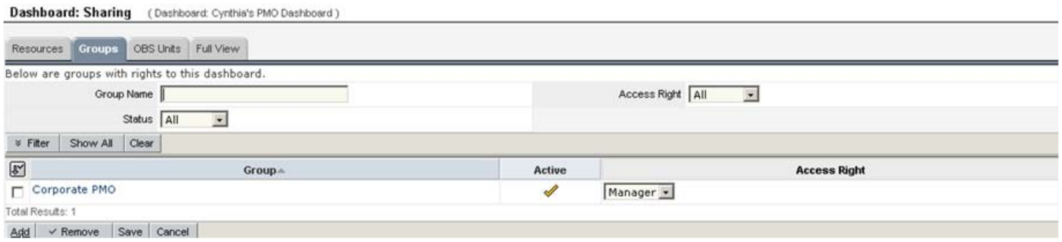
- Actors - all Project Managers
- Action - View access to dashboard created by Cynthia
- Scope – Dashboard created by Cynthia

Review the Current Access Rights

Andrew navigates to the dashboard. Andrew wants to share this dashboard with another group He clicks Sharing in the top right corner to see who is sharing to the dashboard now.

Select and Grant Access Rights

Andrew clicks the Groups tab. Currently, the Corporate PMO group has Manager access to this PMO dashboard.



Dashboard: Sharing (Dashboard: Cynthia's PMO Dashboard)

Below are groups with rights to this dashboard.

Group Name

Status: All

Access Right: All

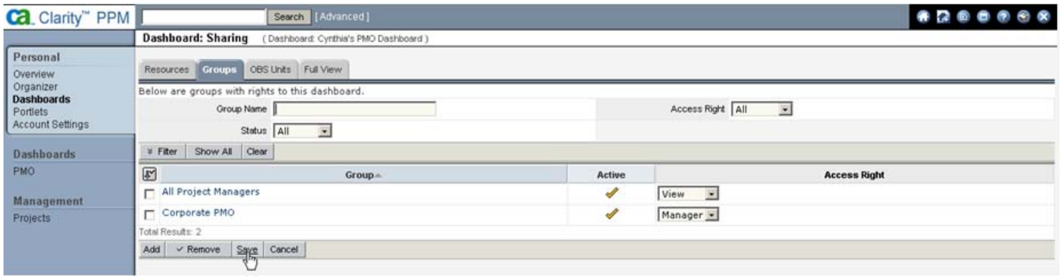
□	Group	Active	Access Right
□	Corporate PMO	✓	Manager

Total Results: 1

To share the dashboard, do the following

1. Click Add to share the dashboard.
2. Search for the All Project Managers group and select it using the checkbox to the left. For this example, use the filter “all pr” to find the group.
3. Click Add.
4. The All Project Managers group should have View access.

5. Click Save. Click Cancel to return to the Dashboard.



Dashboard: Sharing (Dashboard: Cynthia's PMO Dashboard)

Below are groups with rights to this dashboard.

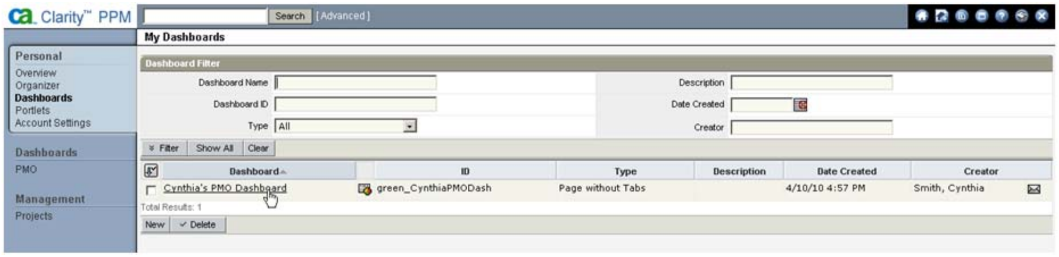
Group Name:
Access Right: All
Status: All

	Group	Active	Access Right
□	All Project Managers	✓	View
□	Corporate PMO	✓	Manager

Total Results: 2

Confirmation

Thomas Young is a Project Manager. He now has access to view Cynthia's PMO Dashboard that Andrew shared with the members of the All Project Managers group.



My Dashboards

Dashboard Name:
Description:
Dashboard ID:
Date Created:
Type: All
Creator:

	Dashboard	ID	Type	Description	Date Created	Creator
□	Cynthia's PMO Dashboard	green_CynthiaPMODash	Page without Tabs		4/10/10 4:57 PM	Smith, Cynthia

Total Results: 1

Verifying Access

Sometimes you may need to find out what resources have access to an object instance, portlet, or page. The system administrator or anyone with Project – View Access Rights is able to see this information. Use Full View functionality to do this.

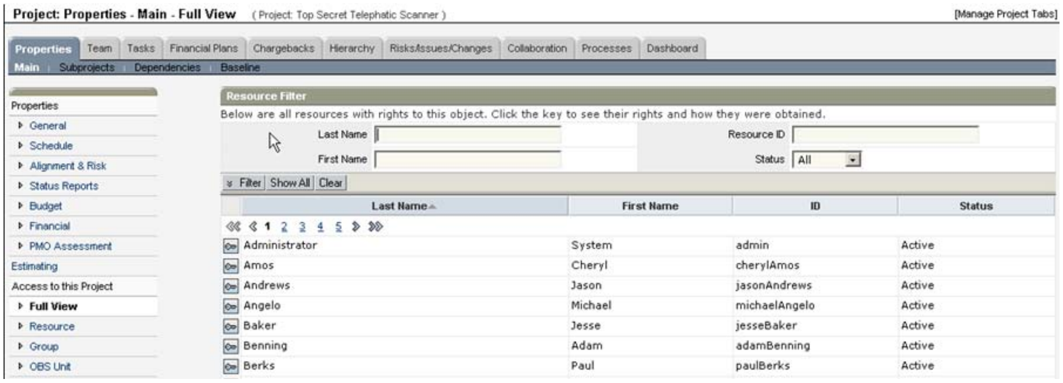
Use Case 1

Determine who has access to the Top Secret Telepathic Scanner project.

To verify access do the following

1. Navigate to the project. Select the Properties tab.
2. Click Full View under Access to this Project.

   All the resources that have access to the Top Secret Telepathic Scanner project are listed.



Project: Properties - Main - Full View (Project: Top Secret Telephatic Scanner)

Resource Filter

Below are all resources with rights to this object. Click the key to see their rights and how they were obtained.

Last Name

First Name

Resource ID

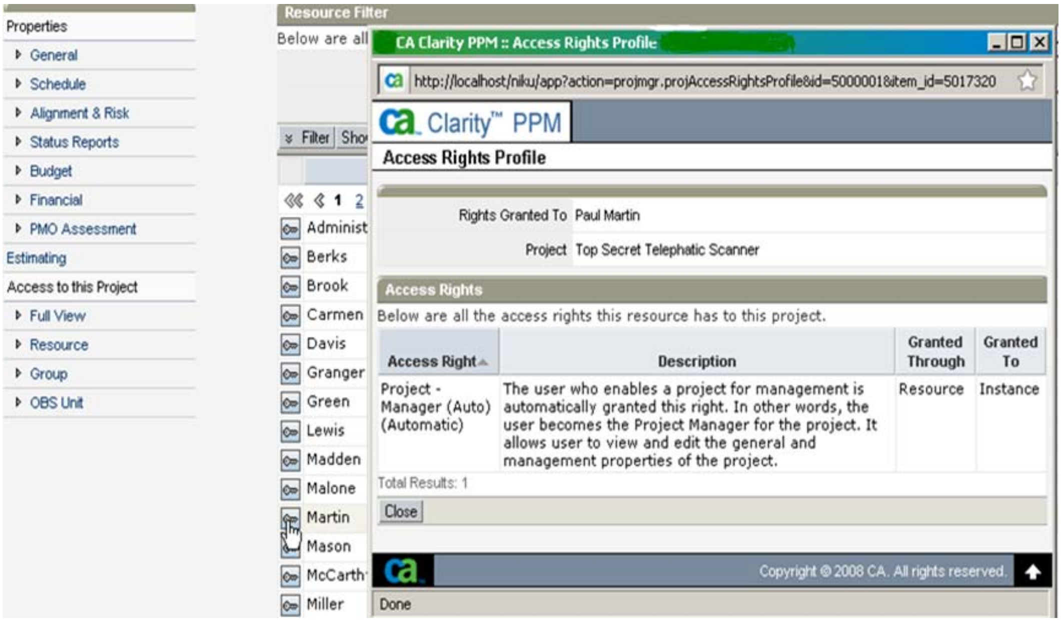
Status All

Last Name	First Name	ID	Status
Administrator	System	admin	Active
Amos	Cheryl	cherylAmos	Active
Andrews	Jason	jasonAndrews	Active
Angelo	Michael	michaelAngelo	Active
Baker	Jesse	jesseBaker	Active
Benning	Adam	adamBenning	Active
Berks	Paul	paulBerks	Active

3. To view the Access Rights Profile for a resource, click the key icon to the left of the resource name.

   A window opens displaying the Access Rights Profile of the resource.

4. Paul Martin has been granted Project – Manager (Auto) access right because he is the Project Manager.



Access Rights Profile

Rights Granted To Paul Martin

Project Top Secret Telephatic Scanner

Access Rights

Below are all the access rights this resource has to this project.

Access Right	Description	Granted Through	Granted To
Project - Manager (Auto) (Automatic)	The user who enables a project for management is automatically granted this right. In other words, the user becomes the Project Manager for the project. It allows user to view and edit the general and management properties of the project.	Resource	Instance

Total Results: 1

Use Case 2

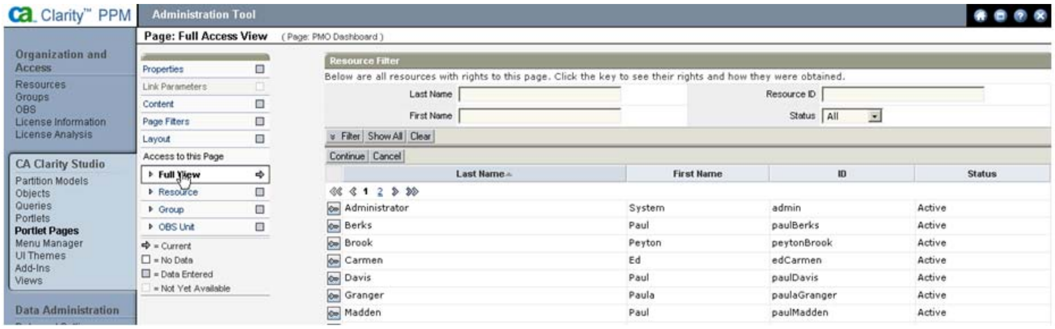
Determine who has access to the PMO Dashboard page. Thomas Young is the resource in this example.

The system administrator or anyone with access to CA Clarity PPM Studio has access to view this information.

To verify access do the following

1. Access the Administration Tool. Under Clarity Studio, select Portlet Pages. Navigate to the PMO Dashboard page
2. Click Full View under *Access to this Page* to navigate to the page.
3. The resources that have access to the page are displayed.
4. By filtering on the resource name and clicking Key icon, the Access Rights Profile appears.

   The resource Thomas Young has access to that page as a member of the All Project Managers group, which has been granted an Instance right – meaning it is specifically for this page.



Page: Full Access View (Page: PMO Dashboard)

Resource Filter

Below are all resources with rights to this page. Click the key to see their rights and how they were obtained.

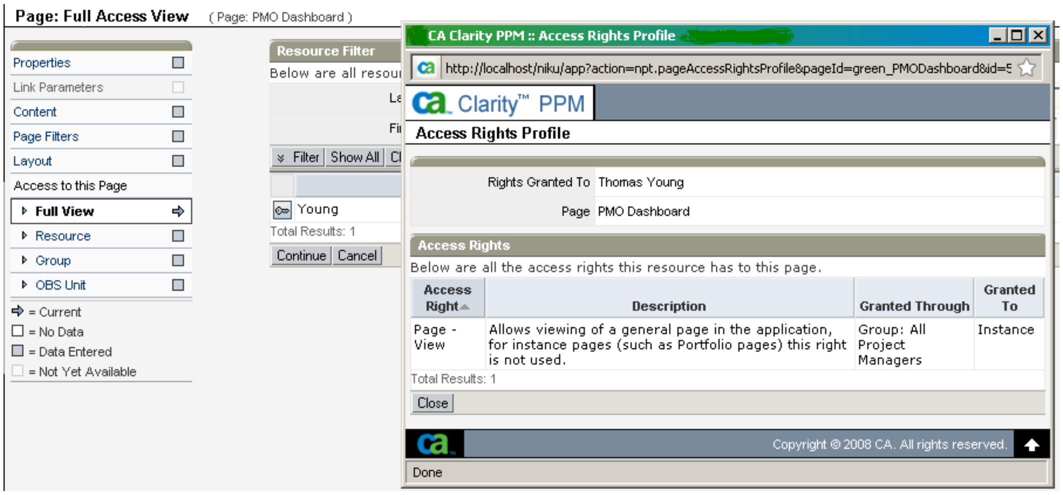
Last Name

First Name

Resource ID

Status: All

Last Name	First Name	ID	Status
Administrator	System	admin	Active
Berks	Paul	paulBerks	Active
Brook	Peyton	peytonBrook	Active
Carmen	Ed	edCarmen	Active
Davis	Paul	paulDavis	Active
Granger	Paula	paulaGranger	Active
Madden	Paul	paulMadden	Active



Page: Full Access View (Page: PMO Dashboard)

Young

Total Results: 1

CA Clarity PPM :: Access Rights Profile [redacted]

http://localhost/niku/app?action=npt.pageAccessRightsProfile&pageId=green_PMODashboard&id=5

Access Rights Profile

Rights Granted To: Thomas Young

Page: PMO Dashboard

Access Rights

Below are all the access rights this resource has to this page.

Access Right	Description	Granted Through	Granted To
Page - View	Allows viewing of a general page in the application, for instance pages (such as Portfolio pages) this right is not used.	Group: All Project Managers	Instance

Total Results: 1

Copyright © 2008 CA. All rights reserved.

Chapter 4: Use Case Examples

Introduction to Use Cases

We have discussed key concepts that are important to understand when considering how CA Clarity PPM handles application and data security, and many of the available options for granting access rights.

The use cases presented in this chapter address common use and configuration scenarios, illustrating the importance and value of implementing security in the CA Clarity PPM environment. These use cases build on the knowledge provided in the previous chapters, demonstrating the flexibility of CA Clarity PPM security configuration options.

Having the ability to restrict access or globally assign access to the application elements and objects (pages, lists, project object, portlets and so on) at varying levels (Resource, Instance, OBS Unit, or Global) allows the enterprise to configure and secure the CA Clarity PPM application.

Important! All the names used in the use cases represent fictitious characters created for the purpose of illustrating the functionality described in the use cases. Some of the pages, portlets, sub-pages and attributes used in the use cases represent fictitious elements and may not be available in your CA Clarity PPM installation.

Use Case: Implementing Department Security

One of the most common requests is to segregate projects and resources by Department. The following use case addresses this scenario.

Use Case

Use CA Clarity PPM to manage projects for two different departments: IT and Finance. The Corporate PMO department oversees the project management processes for both departments. Five different roles have been identified for both departments: Requestors, Project Participants, Project Managers, Department Managers and PMO members. The access requirements for these roles in this use case are as follows:

Requestors

Requestors should be able to enter new project requests (ideas); they can only view the ideas they create. They can also view the Projects of their departments.

Project Participants

Project Participants can view all projects and resources in their departments, including Resource Allocation information; they can enter time against project tasks they are assigned to; they can publish and view documents for the projects they participate on.

Project Managers

Project Managers can view all projects in their department but; they can edit information for the projects they manage. They can view resource information and also soft-book resources from their departments.

Department Managers

Department Managers are able to view all project information; they can edit information for resources in their department and hard-book them. They can also create resources.

PMO members

PMO members can view and edit any information for both the IT and Finance Departments in this use case.

Defining the Security Configuration

Use the information in the Use Case to identify the security requirements and plan how to implement security in CA Clarity PPM.

The following table contains the list of requirements gathered from the use case categorized by the ACTOR-ACTIONS-SCOPE relationship model.

Information from the Use Case		
Actor	**Actions**	**Data Scope**
Requestors	Create Ideas	--
	View Ideas	Ideas created by them
	View Projects	Their department projects
Project Participants	View Projects	Their department projects
	View Resources	Their department resources
	View Resource Allocation	Their department resources
	Enter Time	Their Assignments
	Publish Documents	Projects they are assigned to
Project Managers	Create Projects	--
	View Projects	Their department projects
	Edit Projects	Projects managed by them
	View Resources	Their department resources
	Soft-book resources	Their department resources
PMO	Create Projects	--
	View Projects	All department projects
	Edit Projects	All department projects
Department Managers	Create Resources	--
	Edit Resource information	Their department resources
	Hard-book resources	Their department resources
	View Projects	Their department projects

The security requirements in the following table, Security Elements in CA Clarity PPM represent the information derived from the use case expressed in the terminology used in CA Clarity PPM:

Security Elements in CA Clarity PPM		
CA Clarity PPM Actor	**CA Clarity PPM Access Right**	**CA Clarity PPM Scope**
Group: All Department Managers	Resource - Create	Global
Group: All Department Managers	Resource - Navigate	Global
Group: All Participants	Resource - Navigate	Global
Group: All Participants	Timesheets - Navigate	Global
Group: All Project Managers	Project - Create	Global
Group: All Project Managers	Project - Create from Template	Global
Group: All Requestors	Idea - Create	Global
Group: Corporate PMO	Project - Create	Global
Group: Corporate PMO	Project - Create from Template	Global
Group: Corporate PMO	Project - Edit Management	OBS Unit: Finance
Group: Corporate PMO	Project - Edit Management	OBS Unit: IT
Group: Corporate PMO	Project - View	OBS Unit: Finance
Group: Corporate PMO	Project - View	OBS Unit: IT
Group: Dept Manager Finance	Project - View	OBS Unit: Finance
Group: Dept Manager Finance	Resource - Edit	OBS Unit: Finance
Group: Dept Manager Finance	Resource - Hard Book	OBS Unit: Finance
Group: Dept Manager IT	Project - View	OBS Unit: IT
Group: Dept Manager IT	Resource - Edit	OBS Unit: IT
Group: Dept Manager IT	Resource - Hard Book	OBS Unit: IT
Group: Participants Finance	Project - View	OBS Unit: Finance

Security Elements in CA Clarity PPM		
CA Clarity PPM Actor	**CA Clarity PPM Access Right**	**CA Clarity PPM Scope**
Group: Participants Finance	Resource - View	OBS Unit: Finance
Group: Participants Finance	Resource - View Book	OBS Unit: Finance
Group: Participants IT	Project - View	OBS Unit: IT
Group: Participants IT	Resource - View	OBS Unit: IT
Group: Participants IT	Resource - View Book	OBS Unit: IT
Group: Project Manager Finance	Project - View	OBS Unit: Finance
Group: Project Manager Finance	Resource - View	OBS Unit: Finance
Group: Project Manager Finance	Resource - Soft Book	OBS Unit: Finance
Group: Project Manager IT	Project - View	OBS Unit: IT
Group: Project Manager IT	Resource - View	OBS Unit: IT
Group: Project Manager IT	Resource - Soft Book	OBS Unit: IT
Group: Requestor Finance	Project - View	OBS Unit: Finance
Group: Requestor IT	Project - View	OBS Unit: IT
Resource: All Resources	Idea - Initiator (Auto)	Instance auto-assigned access right
Resource: All Resources	Project - Edit	Instance auto-assigned access right
Resource: All Resources	Project - Participant (Auto)	Instance auto-assigned access right
Resource: All Resources	Resource - Enter Time	Instance auto-assigned access right

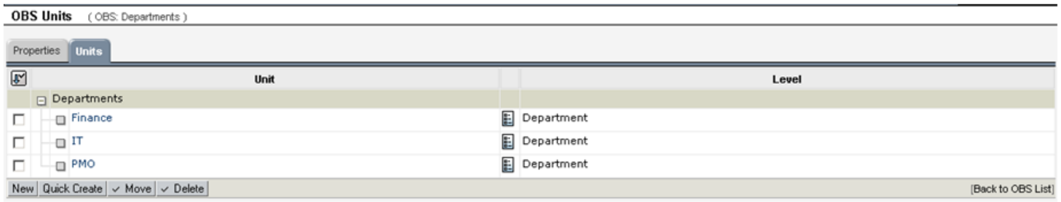
Implementing Security Requirements

To implement the security requirements do the following:

1. Create the OBS Units that categorize Projects and Resources
2. Create the Groups that are to be granted Access Rights
3. Grant groups with the appropriate Global rights
4. Grant groups with the appropriate OBS Unit rights
5. Create the resources (users)
6. Assign the resources to the correct group

The following graphics illustrate the results after the steps are completed:

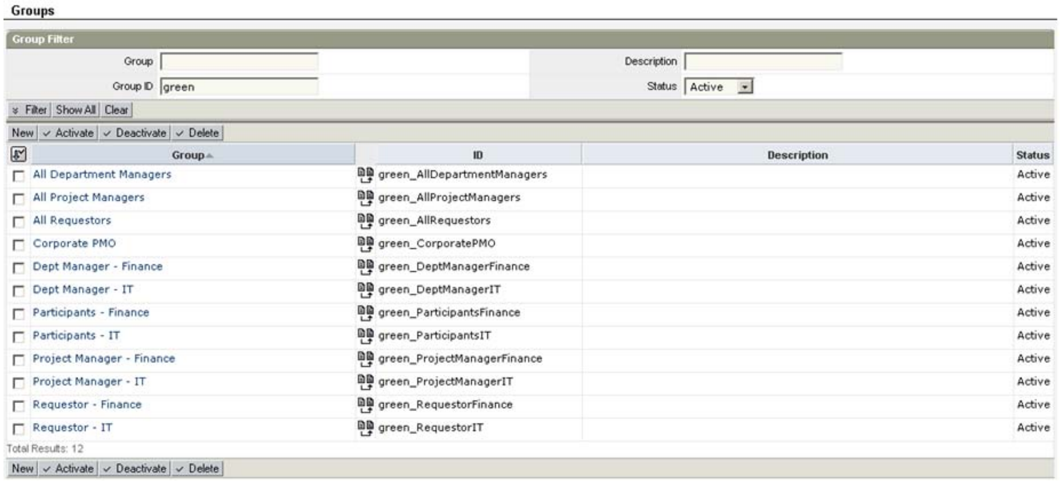
Create the OBS Units



OBS Units (OBS: Departments)

	Unit	Level
	⊟ Departments	
□	Finance	Department
□	IT	Department
□	PMO	Department

Create the Groups



Groups

Group Filter

Group:
Group ID: green
Description:
Status: Active

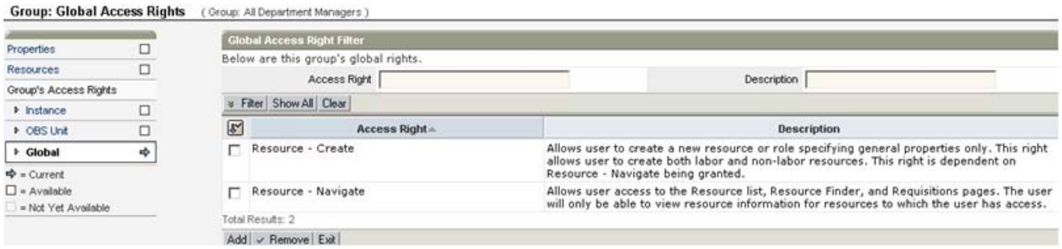
	Group	ID	Description	Status
□	All Department Managers	green_AllDepartmentManagers		Active
□	All Project Managers	green_AllProjectManagers		Active
□	All Requestors	green_AllRequestors		Active
□	Corporate PMO	green_CorporatePMO		Active
□	Dept Manager - Finance	green_DeptManagerFinance		Active
□	Dept Manager - IT	green_DeptManagerIT		Active
□	Participants - Finance	green_ParticipantsFinance		Active
□	Participants - IT	green_ParticipantsIT		Active
□	Project Manager - Finance	green_ProjectManagerFinance		Active
□	Project Manager - IT	green_ProjectManagerIT		Active
□	Requestor - Finance	green_RequestorFinance		Active
□	Requestor - IT	green_RequestorIT		Active

Total Results: 12

Grant Global Access Rights

The appropriate access rights for each group are illustrated in the graphics following each group title. The assignments are based on the requirements defined in the use case.

All Department Managers



Group: Global Access Rights (Group: All Department Managers)

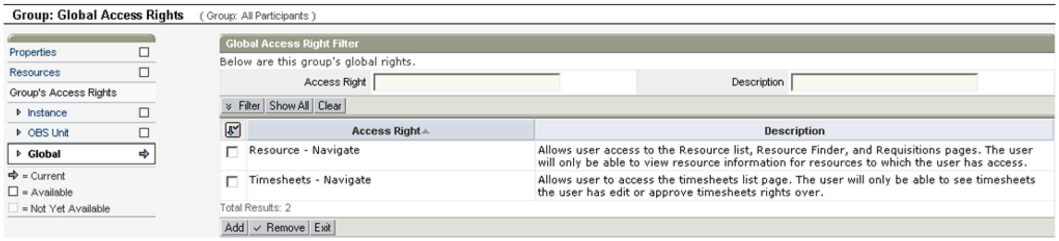
Below are this group's global rights.

Access Right | Description

	Access Right	Description
□	Resource - Create	Allows user to create a new resource or role specifying general properties only. This right allows user to create both labor and non-labor resources. This right is dependent on Resource - Navigate being granted.
□	Resource - Navigate	Allows user access to the Resource list, Resource Finder, and Requisitions pages. The user will only be able to view resource information for resources to which the user has access.

Total Results: 2

All Participants



Group: Global Access Rights (Group: All Participants)

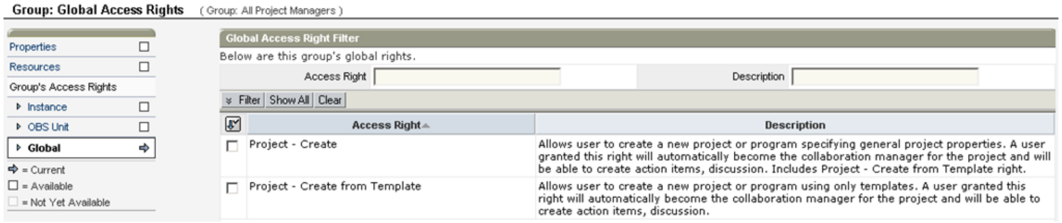
Below are this group's global rights.

Access Right | Description

	Access Right	Description
□	Resource - Navigate	Allows user access to the Resource list, Resource Finder, and Requisitions pages. The user will only be able to view resource information for resources to which the user has access.
□	Timesheets - Navigate	Allows user to access the timesheets list page. The user will only be able to see timesheets the user has edit or approve timesheets rights over.

Total Results: 2

All Project Managers



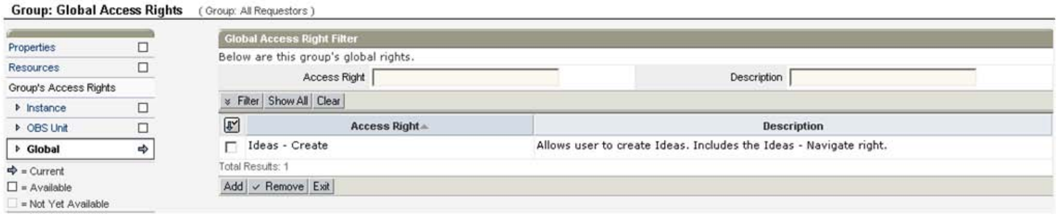
Group: Global Access Rights (Group: All Project Managers)

Below are this group's global rights.

Access Right | Description

	Access Right	Description
□	Project - Create	Allows user to create a new project or program specifying general project properties. A user granted this right will automatically become the collaboration manager for the project and will be able to create action items, discussion. Includes Project - Create from Template right.
□	Project - Create from Template	Allows user to create a new project or program using only templates. A user granted this right will automatically become the collaboration manager for the project and will be able to create action items, discussion.

All Requestors



Group: Global Access Rights (Group: All Requestors)

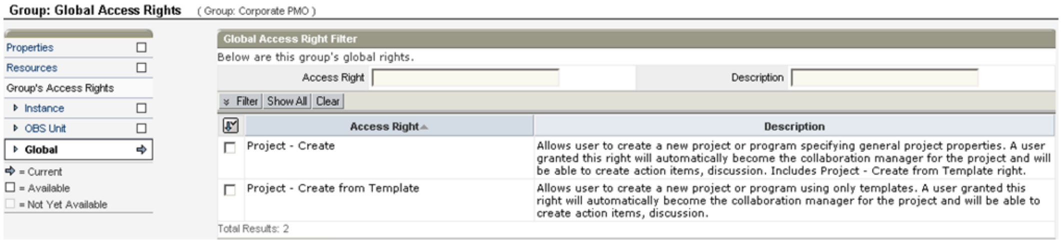
Below are this group's global rights.

Access Right | Description

	Access Right	Description
□	Ideas - Create	Allows user to create Ideas. Includes the Ideas - Navigate right.

Total Results: 1

Corporate PMO



Group: Global Access Rights (Group: Corporate PMO)

Global Access Right Filter

Below are this group's global rights.

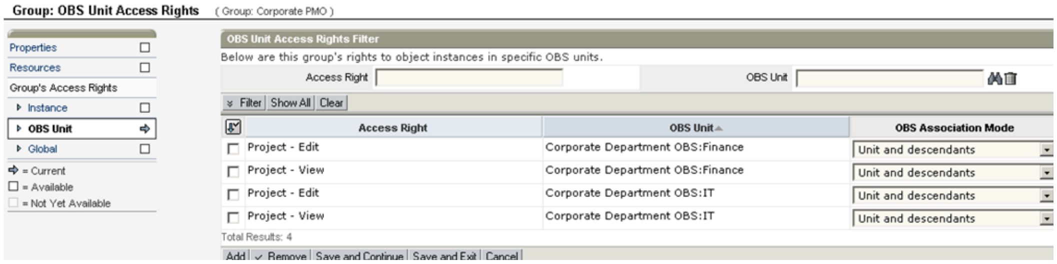
Access Right Description

Access Right	Description
Project - Create	Allows user to create a new project or program specifying general project properties. A user granted this right will automatically become the collaboration manager for the project and will be able to create action items, discussion. Includes Project - Create from Template right.
Project - Create from Template	Allows user to create a new project or program using only templates. A user granted this right will automatically become the collaboration manager for the project and will be able to create action items, discussion.

Total Results: 2

Grant OBS Unit Access Rights

Corporate PMO



Group: OBS Unit Access Rights (Group: Corporate PMO)

OBS Unit Access Rights Filter

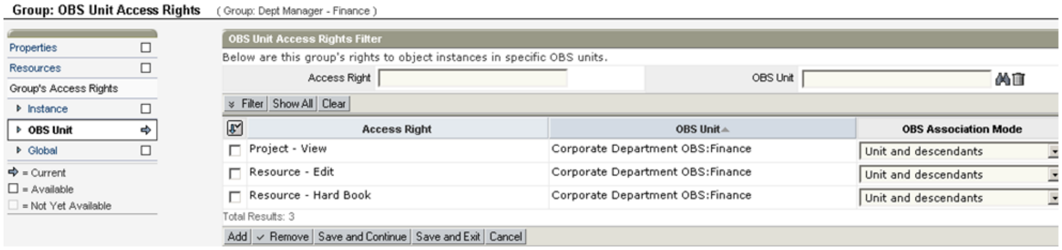
Below are this group's rights to object instances in specific OBS units.

Access Right OBS Unit

Access Right	OBS Unit	OBS Association Mode
Project - Edit	Corporate Department OBS:Finance	Unit and descendants
Project - View	Corporate Department OBS:Finance	Unit and descendants
Project - Edit	Corporate Department OBS:IT	Unit and descendants
Project - View	Corporate Department OBS:IT	Unit and descendants

Total Results: 4

Dept Manager – Finance



Group: OBS Unit Access Rights (Group: Dept Manager - Finance)

OBS Unit Access Rights Filter

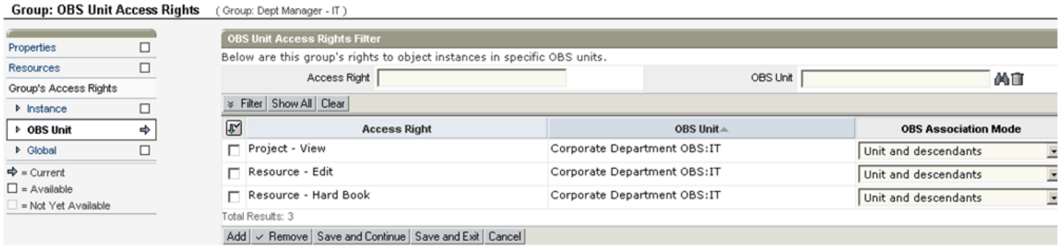
Below are this group's rights to object instances in specific OBS units.

Access Right OBS Unit

Access Right	OBS Unit	OBS Association Mode
Project - View	Corporate Department OBS:Finance	Unit and descendants
Resource - Edit	Corporate Department OBS:Finance	Unit and descendants
Resource - Hard Book	Corporate Department OBS:Finance	Unit and descendants

Total Results: 3

Dept Manager – IT



Group: OBS Unit Access Rights (Group: Dept Manager - IT)

OBS Unit Access Rights Filter

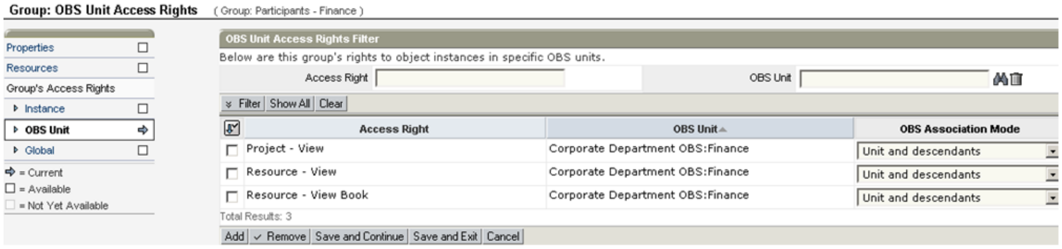
Below are this group's rights to object instances in specific OBS units.

Access Right OBS Unit

Access Right	OBS Unit	OBS Association Mode
Project - View	Corporate Department OBS:IT	Unit and descendants
Resource - Edit	Corporate Department OBS:IT	Unit and descendants
Resource - Hard Book	Corporate Department OBS:IT	Unit and descendants

Total Results: 3

Participants – Finance



Group: OBS Unit Access Rights (Group: Participants - Finance)

- Properties □
- Resources □
- Group's Access Rights
- Instance □
- **OBS Unit** ➪
- Global □

➪ = Current
□ = Available
= Not Yet Available

OBS Unit Access Rights Filter

Below are this group's rights to object instances in specific OBS units.

Access Right: ______ OBS Unit: ______

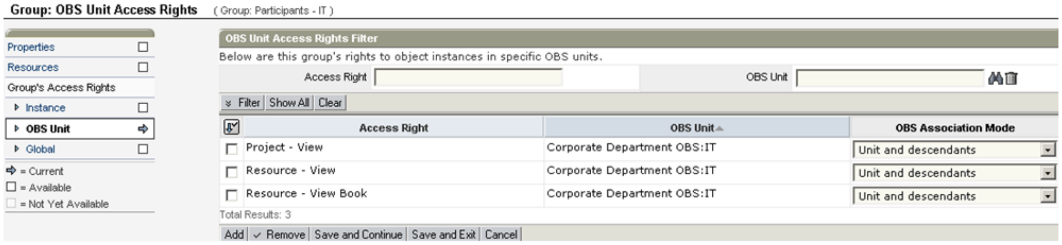
Filter | Show All | Clear

Access Right	OBS Unit	OBS Association Mode
□ Project - View	Corporate Department OBS:Finance	Unit and descendants
□ Resource - View	Corporate Department OBS:Finance	Unit and descendants
□ Resource - View Book	Corporate Department OBS:Finance	Unit and descendants

Total Results: 3

Add | Remove | Save and Continue | Save and Exit | Cancel

Participants – IT



Group: OBS Unit Access Rights (Group: Participants - IT)

- Properties □
- Resources □
- Group's Access Rights
- Instance □
- **OBS Unit** ➪
- Global □

➪ = Current
□ = Available
= Not Yet Available

OBS Unit Access Rights Filter

Below are this group's rights to object instances in specific OBS units.

Access Right: ______ OBS Unit: ______

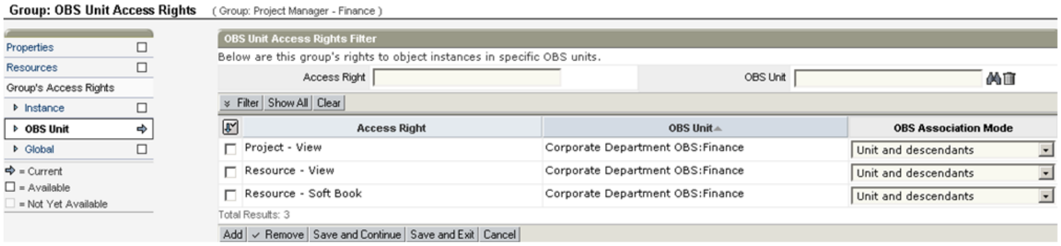
Filter | Show All | Clear

Access Right	OBS Unit	OBS Association Mode
□ Project - View	Corporate Department OBS:IT	Unit and descendants
□ Resource - View	Corporate Department OBS:IT	Unit and descendants
□ Resource - View Book	Corporate Department OBS:IT	Unit and descendants

Total Results: 3

Add | Remove | Save and Continue | Save and Exit | Cancel

Project Manager – Finance



Group: OBS Unit Access Rights (Group: Project Manager - Finance)

- Properties □
- Resources □
- Group's Access Rights
- Instance □
- **OBS Unit** ➪
- Global □

➪ = Current
□ = Available
= Not Yet Available

OBS Unit Access Rights Filter

Below are this group's rights to object instances in specific OBS units.

Access Right: ______ OBS Unit: ______

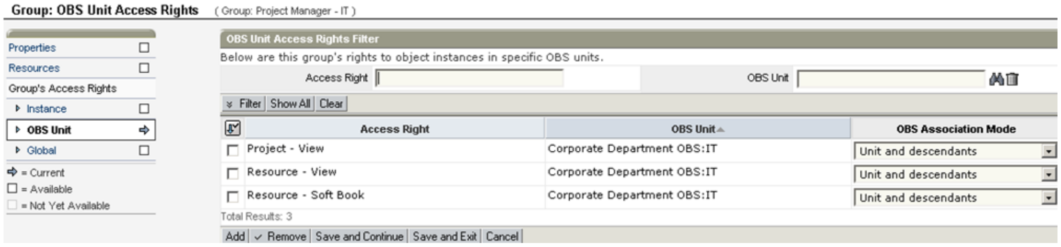
Filter | Show All | Clear

Access Right	OBS Unit	OBS Association Mode
□ Project - View	Corporate Department OBS:Finance	Unit and descendants
□ Resource - View	Corporate Department OBS:Finance	Unit and descendants
□ Resource - Soft Book	Corporate Department OBS:Finance	Unit and descendants

Total Results: 3

Add | Remove | Save and Continue | Save and Exit | Cancel

Project Manager – IT



Group: OBS Unit Access Rights (Group: Project Manager - IT)

- Properties □
- Resources □
- Group's Access Rights
- Instance □
- **OBS Unit** ➪
- Global □

➪ = Current
□ = Available
= Not Yet Available

OBS Unit Access Rights Filter

Below are this group's rights to object instances in specific OBS units.

Access Right: ______ OBS Unit: ______

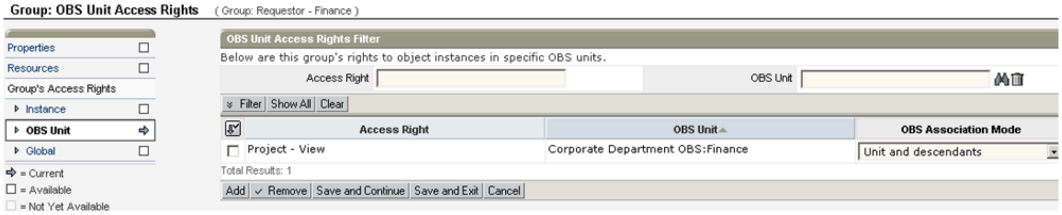
Filter | Show All | Clear

Access Right	OBS Unit	OBS Association Mode
□ Project - View	Corporate Department OBS:IT	Unit and descendants
□ Resource - View	Corporate Department OBS:IT	Unit and descendants
□ Resource - Soft Book	Corporate Department OBS:IT	Unit and descendants

Total Results: 3

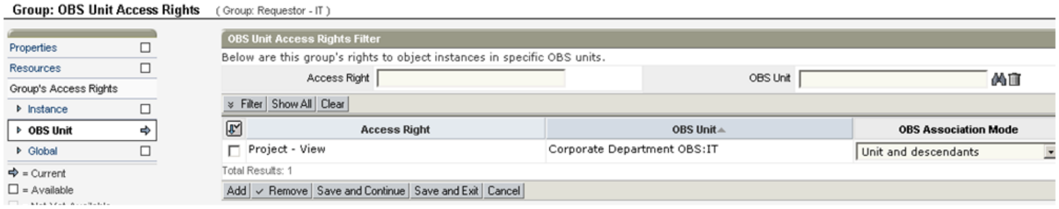
Add | Remove | Save and Continue | Save and Exit | Cancel

Requestor – Finance



Access Right	OBS Unit	OBS Association Mode
□ Project - View	Corporate Department OBS:Finance	Unit and descendants

Requestor – IT



Access Right	OBS Unit	OBS Association Mode
□ Project - View	Corporate Department OBS:IT	Unit and descendants

Create Resources

The following fictitious resources have been defined for this use case and are available to select in the Resources pool as illustrated:

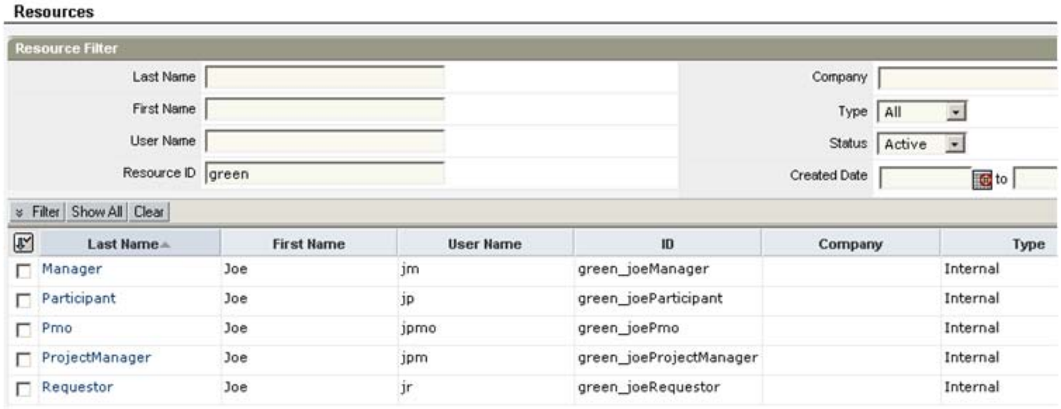
a. Joe Manager – member of the Department Manager group

b. Joe Participant – an individual resource, member of a project team

c. Joe Pmo – a member of the Corporate PMO group

d. Joe ProjectManager – a member of the Project Manager Group

e. Joe Requestor – an individual resource



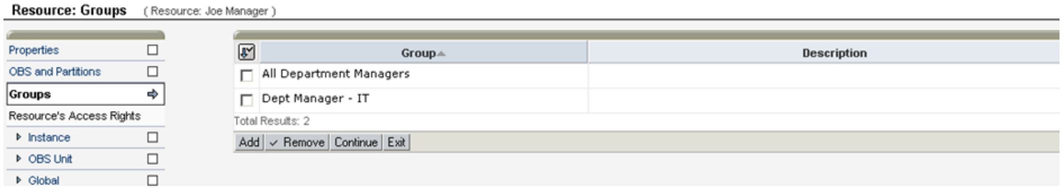
Resource ID: green
Type: All
Status: Active

	Last Name	First Name	User Name	ID	Company	Type
□	Manager	Joe	jm	green_joeManager		Internal
□	Participant	Joe	jp	green_joeParticipant		Internal
□	Pmo	Joe	jpmo	green_joePmo		Internal
□	ProjectManager	Joe	jpm	green_joeProjectManager		Internal
□	Requestor	Joe	jr	green_joeRequestor		Internal

Assigning Groups to Users

Each of the users has been assigned the correct groups, as indicated in the following graphics:

Joe Manager is the manager for the IT Department

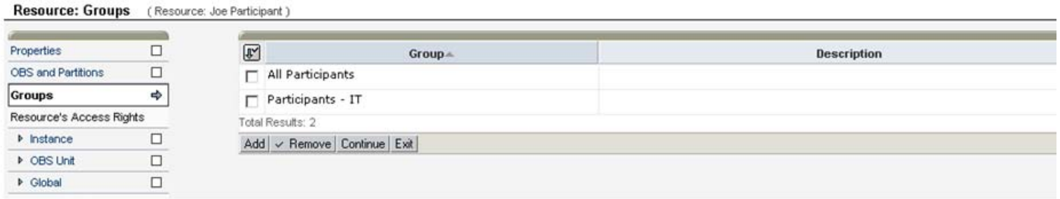


Resource: Groups (Resource: Joe Manager)

Group	Description
All Department Managers	
Dept Manager - IT	

Total Results: 2

Joe Participant is a project participant from the IT department

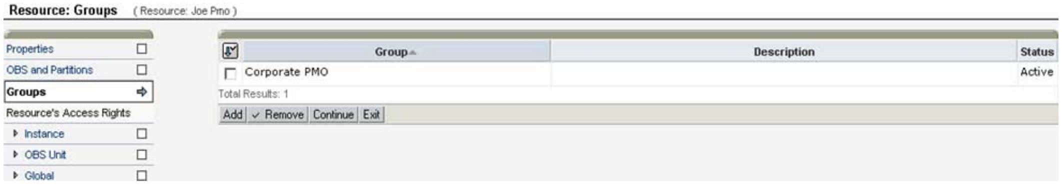


Resource: Groups (Resource: Joe Participant)

Group	Description
All Participants	
Participants - IT	

Total Results: 2

Joe Pmo is a member of the Corporate PMO department

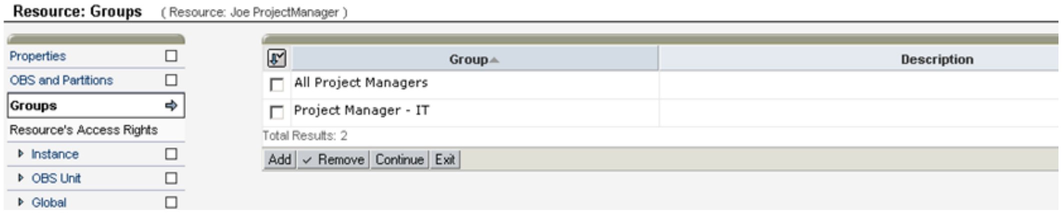


Resource: Groups (Resource: Joe Pmo)

Group	Description	Status
Corporate PMO		Active

Total Results: 1

Joe ProjectManager is a project manager from the IT department

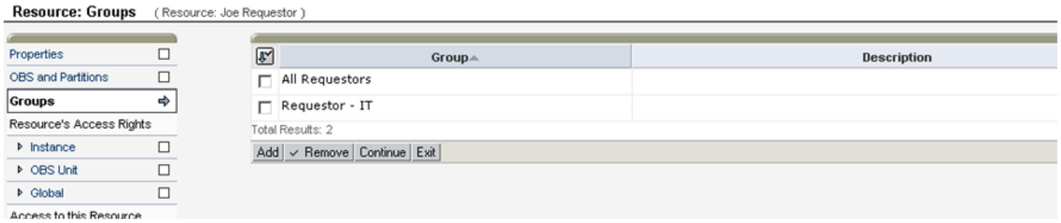


Resource: Groups (Resource: Joe ProjectManager)

Group	Description
All Project Managers	
Project Manager - IT	

Total Results: 2

Joe Requestor is a requestor from the IT department



Resource: Groups (Resource: Joe Requestor)

Group	Description
All Requestors	
Requestor - IT	

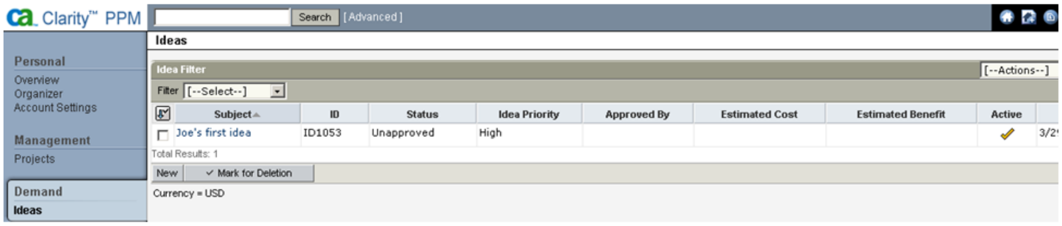
Total Results: 2

Confirmation

The following section illustrates the access that each resource has been granted based on the requirements defined in the use case and the implementation of security for those requirements. Each resource will have access to the Overview General page in Clarity PPM. The Clarity PPM navigation panel will display the links to the other areas such as Ideas, Projects or Resources that the individual resources have been granted access to.

1. Joe Requestor has access to Ideas and Projects

   – He can create Ideas but can only view the Ideas he creates.



Ideas

Idea Filter

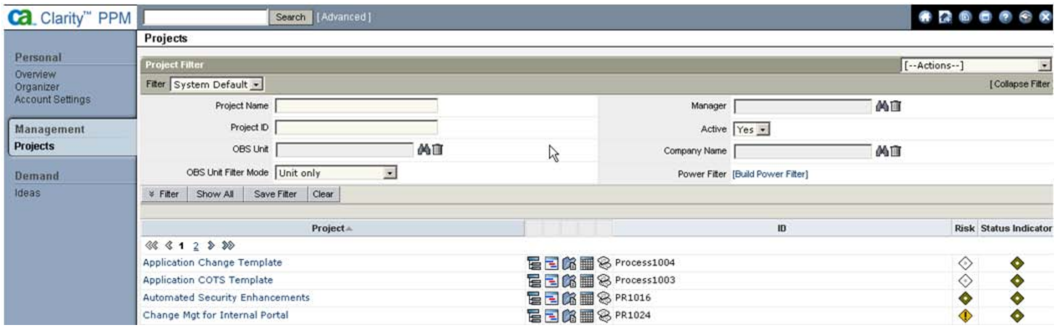
Filter [--Select--]

	Subject	ID	Status	Idea Priority	Approved By	Estimated Cost	Estimated Benefit	Active	
□	Joe's first idea	ID1053	Unapproved	High				✓	3/2

Total Results: 1

Currency = USD

   – He can view all projects from his department but only has read-only access to the Projects information.



Projects

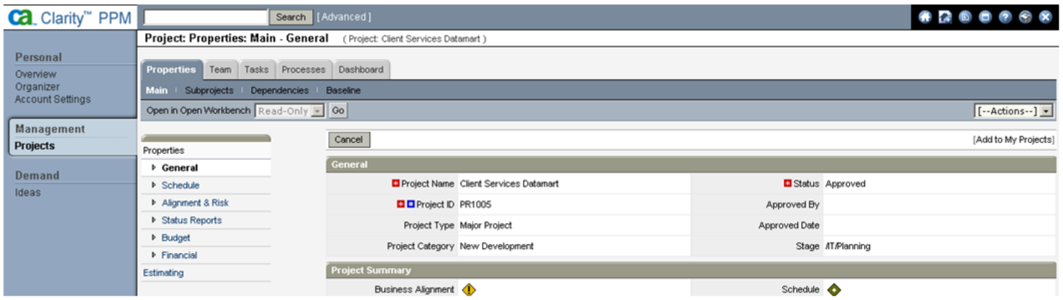
Project Filter

Filter System Default

Project Name		Manager	
Project ID		Active	Yes
OBS Unit		Company Name	
OBS Unit Filter Mode	Unit only	Power Filter	[Build Power Filter]

1 2

Project	ID	Risk	Status Indicator
Application Change Template	Process1004	◇	◆
Application COTS Template	Process1003	◇	◆
Automated Security Enhancements	PR1016	◆	◆
Change Mgt for Internal Portal	PR1024	!	◆



Project: Properties: Main - General (Project: Client Services Datamart)

Open in Open Workbench Read-Only

General

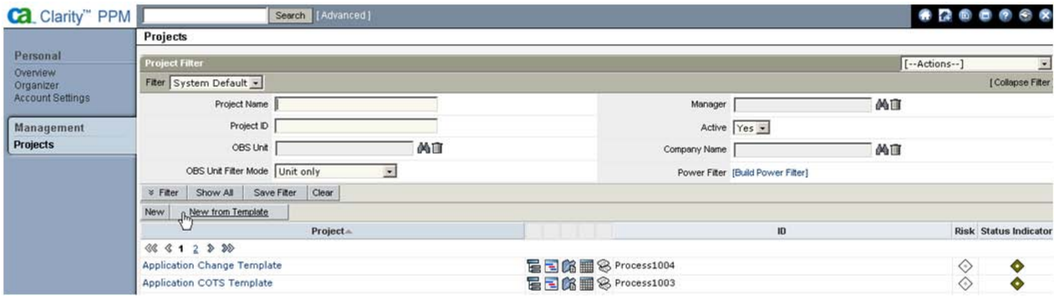
Project Name	Client Services Datamart	Status	Approved
Project ID	PR1005	Approved By	
Project Type	Major Project	Approved Date	
Project Category	New Development	Stage	IT/Planning

Project Summary

Business Alignment	!	Schedule	◆

2. Joe ProjectManager has access to Projects

   – He can create projects and see projects from his department.



Projects

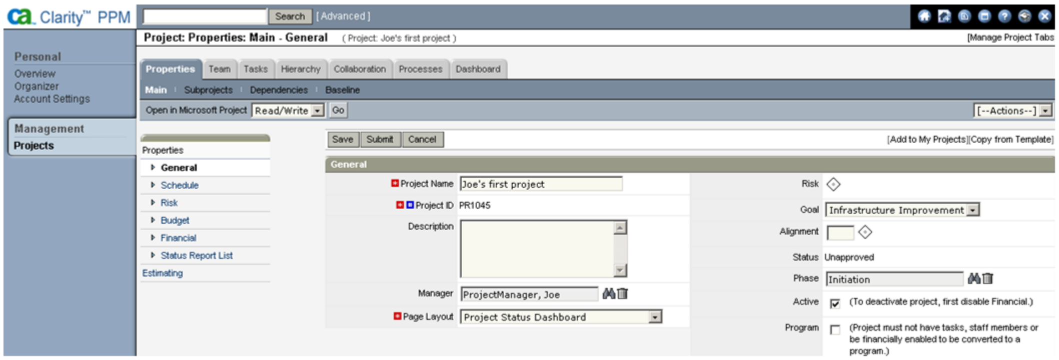
Project Filter

Filter: System Default

Project Name		Manager	
Project ID		Active	Yes
OBS Unit		Company Name	
OBS Unit Filter Mode	Unit only	Power Filter	[Build Power Filter]

Project		ID	Risk	Status Indicator
Application Change Template		Process1004	◇	◆
Application COTS Template		Process1003	◇	◆

   – He has full access to projects for which he is the manager. He can soft-book resources from the IT Department on his project.

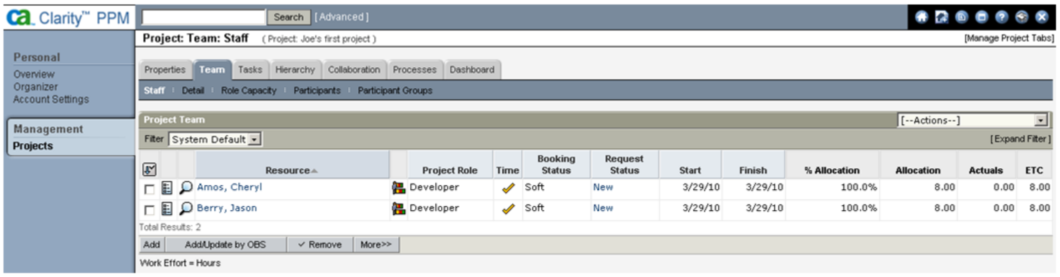


Project: Properties: Main - General (Project: Joe's first project)

Open in Microsoft Project: Read/Write

General

Project Name	Joe's first project	Risk	◇
Project ID	PR1045	Goal	Infrastructure Improvement
Description		Alignment	◇
		Status	Unapproved
		Phase	Initiation
Manager	ProjectManager, Joe	Active	☑ (To deactivate project, first disable Financial.)
Page Layout	Project Status Dashboard	Program	□ (Project must not have tasks, staff members or be financially enabled to be converted to a program.)



Project: Team: Staff (Project: Joe's first project)

Project Team

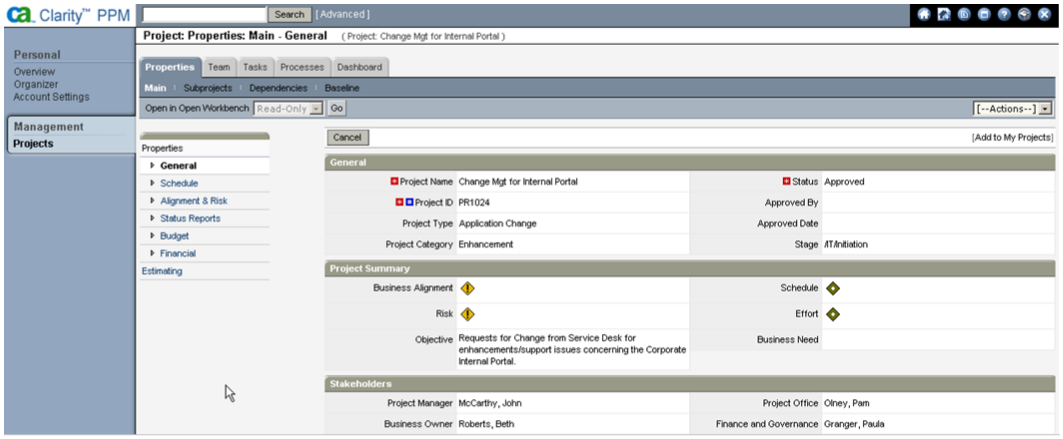
Filter: System Default

	Resource	Project Role	Time	Booking Status	Request Status	Start	Finish	% Allocation	Allocation	Actuals	ETC
□	Amos, Cheryl	Developer	✓	Soft	New	3/29/10	3/29/10	100.0%	8.00	0.00	8.00
□	Berry, Jason	Developer	✓	Soft	New	3/29/10	3/29/10	100.0%	8.00	0.00	8.00

Total Results: 2

Work Effort = Hours

- He has read-only access to projects for which he is not the manager.



Project: Properties: Main - General (Project: Change Mgt for Internal Portal)

General

Project Name: Change Mgt for Internal Portal
Status: Approved
Project ID: PR1024
Approved By:
Project Type: Application Change
Approved Date:
Project Category: Enhancement
Stage: IT/Initiation

Project Summary

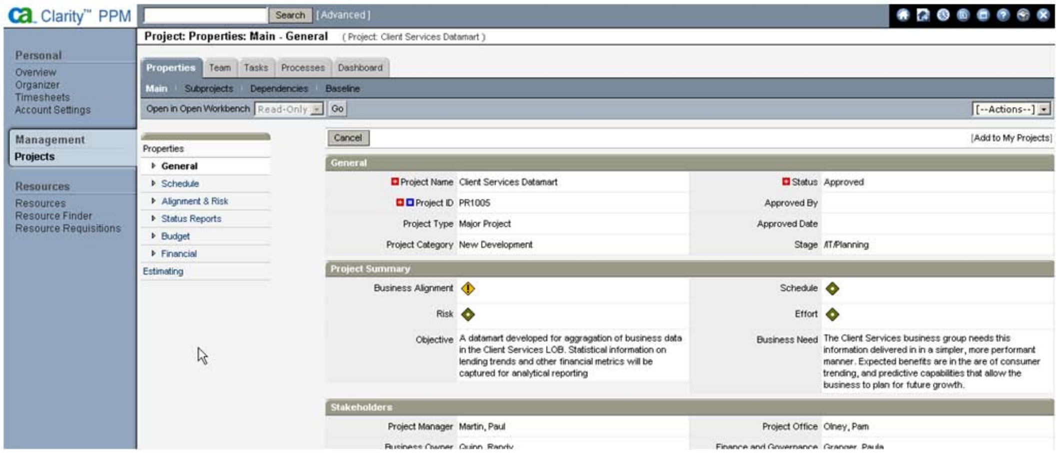
Business Alignment
Schedule
Risk
Effort
Objective: Requests for Change from Service Desk for enhancements/support issues concerning the Corporate Internal Portal.
Business Need:

Stakeholders

Project Manager: McCarthy, John
Project Office: Olney, Pam
Business Owner: Roberts, Beth
Finance and Governance: Granger, Paula

3. Joe Participant has access to Timesheets, Projects and Resources.

- Joe Participant can view Projects for his department but he has read-only access to the project information.



Project: Properties: Main - General (Project: Client Services Datamart)

General

Project Name: Client Services Datamart
Status: Approved
Project ID: PR1005
Approved By:
Project Type: Major Project
Approved Date:
Project Category: New Development
Stage: IT/Planning

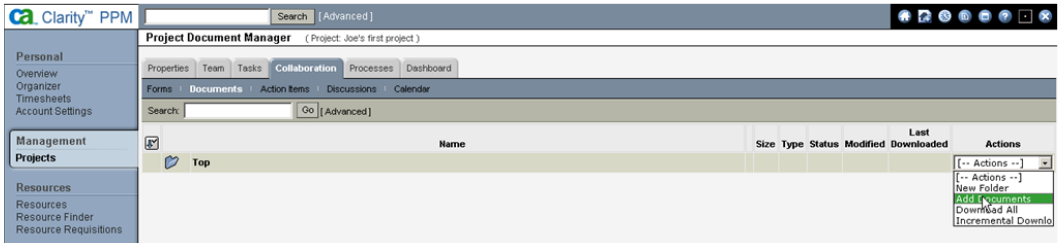
Project Summary

Business Alignment
Schedule
Risk
Effort
Objective: A datamart developed for aggragation of business data in the Client Services LOB. Statistical information on lending trends and other financial metrics will be captured for analytical reporting
Business Need: The Client Services business group needs this information delivered in in a simpler, more performant manner. Expected benefits are in the are of consumer trending, and predictive capabilities that allow the business to plan for future growth.

Stakeholders

Project Manager: Martin, Paul
Project Office: Olney, Pam
Business Owner: Quinn, Randy
Finance and Governance: Granger, Paula

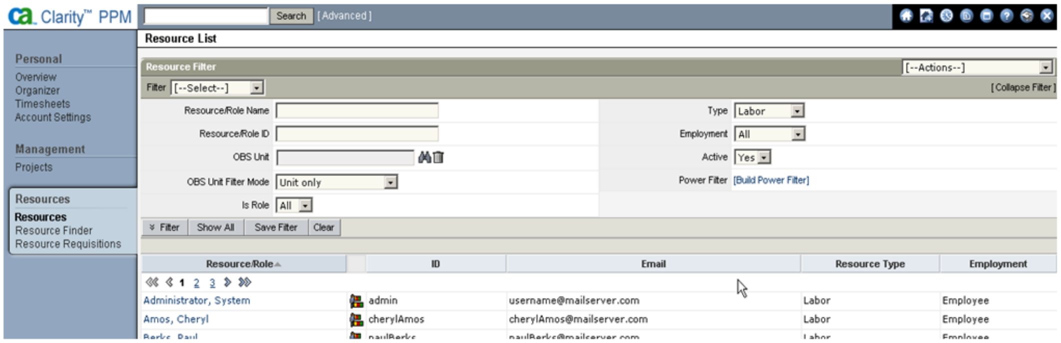
- Joe Participant can publish documents for projects where he is a participant.



Project Document Manager (Project: Joe's first project)

Name	Size	Type	Status	Modified	Last Downloaded	Actions
Top						[-- Actions --]

- He can view resources for his department and has read-only access to resource information.



Resource List

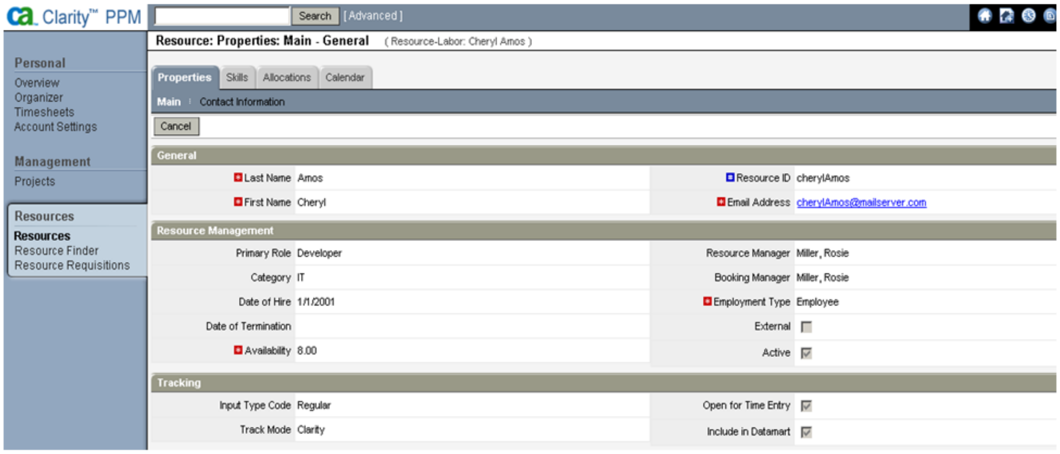
Resource Filter

Filter [--Select--]

Resource/Role Name		Type	Labor
Resource/Role ID		Employment	All
OBS Unit		Active	Yes
OBS Unit Filter Mode	Unit only	Power Filter	[Build Power Filter]
Is Role	All		

1 2 3

Resource/Role	ID	Email	Resource Type	Employment
Administrator, System	admin	username@mailserver.com	Labor	Employee
Amos, Cheryl	cherylAmos	cherylAmos@mailserver.com	Labor	Employee
Berks, Paul	paulBerks	paulBerks@mailserver.com	Labor	Employee



Resource: Properties: Main - General (Resource-Labor: Cheryl Amos)

General

Last Name	Amos	Resource ID	cherylAmos
First Name	Cheryl	Email Address	cherylAmos@mailserver.com

Resource Management

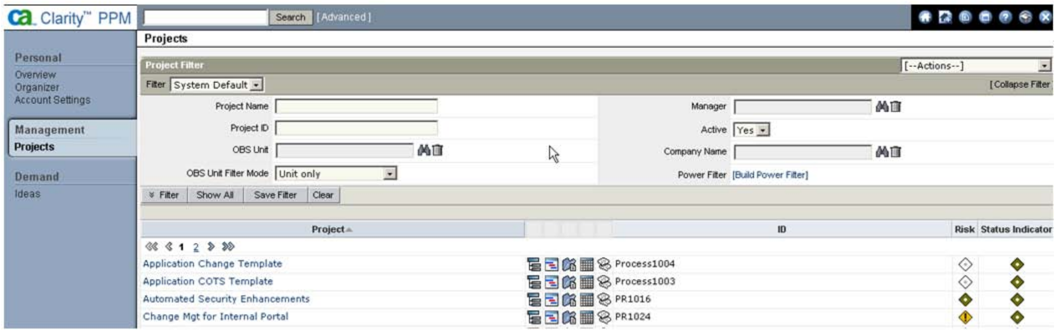
Primary Role	Developer	Resource Manager	Miller, Rosie
Category	IT	Booking Manager	Miller, Rosie
Date of Hire	1/1/2001	Employment Type	Employee
Date of Termination		External	□
Availability	8.00	Active	☑

Tracking

Input Type Code	Regular	Open for Time Entry	☑
Track Mode	Clarity	Include in Datamart	☑

4. Joe Manager is the manager for the IT department. He has access to Projects and Resources.

   - Joe Manager can view projects in his department and has read-only access to the projects.



Projects

Project Filter

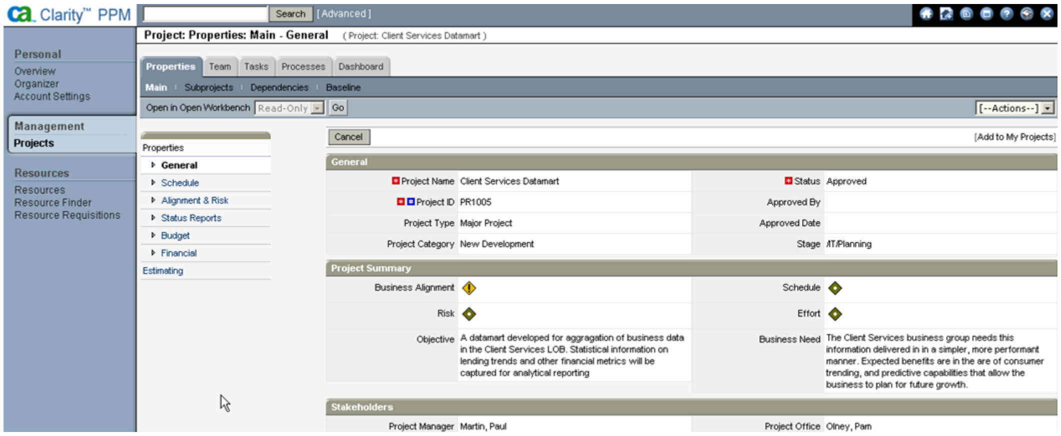
Filter System Default

Project Name		Manager	
Project ID		Active	Yes
OBS Unit		Company Name	
OBS Unit Filter Mode	Unit only	Power Filter	[Build Power Filter]

1 2

Project	ID	Risk	Status Indicator
Application Change Template	Process1004	◇	◆
Application COTS Template	Process1003	◇	◆
Automated Security Enhancements	PR1016	◆	◆
Change Mgt for Internal Portal	PR1024	⚠	◆

– Joe Manager can create resources and view resources from his department.



Project: Properties: Main - General (Project: Client Services Datamart)

Open in Open Workbench: Read-Only

General

Project Name	Client Services Datamart	Status	Approved
Project ID	PR1005	Approved By	
Project Type	Major Project	Approved Date	
Project Category	New Development	Stage	/IT/Planning

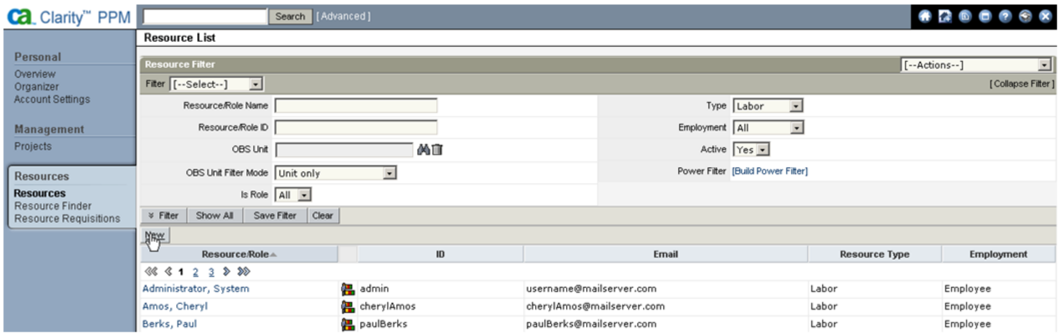
Project Summary

Business Alignment	!	Schedule	◆
Risk	◆	Effort	◆
Objective	A datamart developed for aggregation of business data in the Client Services LOB. Statistical information on lending trends and other financial metrics will be captured for analytical reporting	Business Need	The Client Services business group needs this information delivered in in a simpler, more performant manner. Expected benefits are in the are of consumer trending, and predictive capabilities that allow the business to plan for future growth.

Stakeholders

Project Manager	Martin, Paul	Project Office	Olney, Pam

– He can edit resource information for resources in his department.



Resource List

Resource Filter

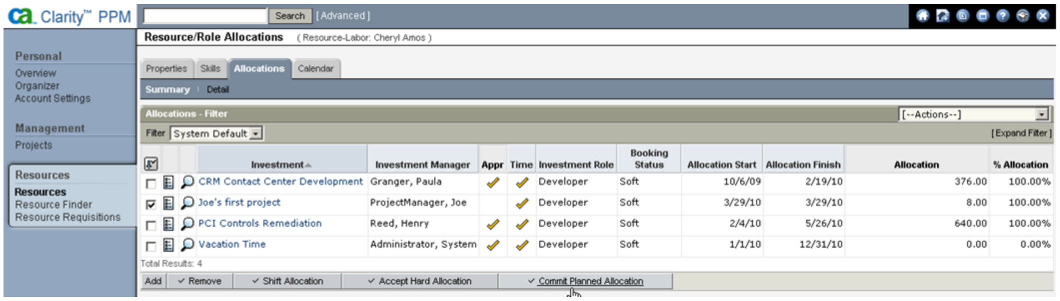
Filter: [--Select--]

Resource/Role Name		Type	Labor
Resource/Role ID		Employment	All
OBS Unit		Active	Yes
OBS Unit Filter Mode	Unit only	Power Filter	[Build Power Filter]
Is Role	All		

« ‹ 1 2 3 › »

Resource/Role	ID	Email	Resource Type	Employment
Administrator, System	admin	username@mailserver.com	Labor	Employee
Amos, Cheryl	cherylAmos	cherylAmos@mailserver.com	Labor	Employee
Berks, Paul	paulBerks	paulBerks@mailserver.com	Labor	Employee

– He can also view Allocation information for his resources and hard book resources.



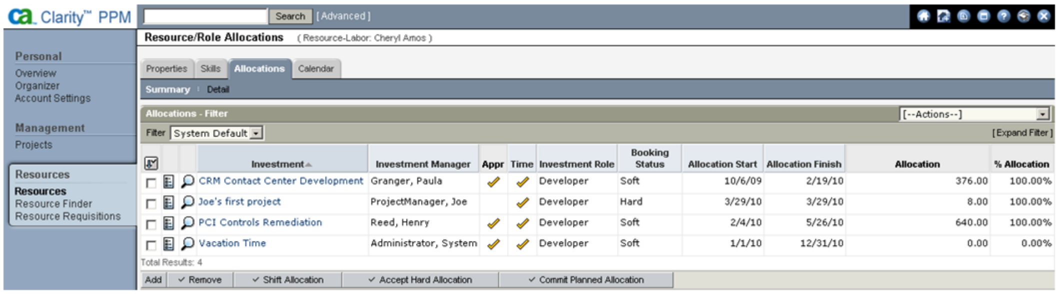
Resource/Role Allocations (Resource-Labor: Cheryl Amos)

Allocations - Filter

Filter: System Default

	Investment	Investment Manager	Appr	Time	Investment Role	Booking Status	Allocation Start	Allocation Finish	Allocation	% Allocation
□	CRM Contact Center Development	Granger, Paula	✓	✓	Developer	Soft	10/6/09	2/19/10	376.00	100.00%
☑	Joe's first project	ProjectManager, Joe		✓	Developer	Soft	3/29/10	3/29/10	8.00	100.00%
□	PCI Controls Remediation	Reed, Henry	✓	✓	Developer	Soft	2/4/10	5/26/10	640.00	100.00%
□	Vacation Time	Administrator, System	✓	✓	Developer	Soft	1/1/10	12/31/10	0.00	0.00%

Total Results: 4



Resource/Role Allocations (Resource-Labor: Cheryl Amos)

Allocations - Filter

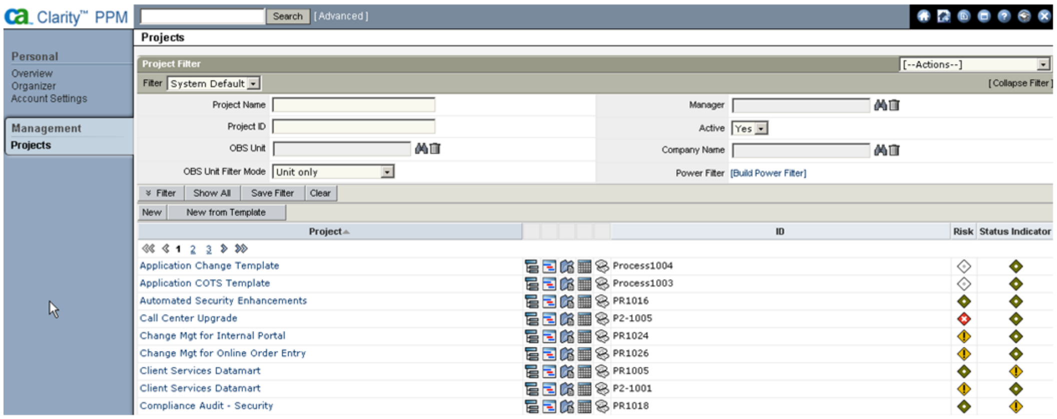
Filter: System Default

	Investment	Investment Manager	Appr	Time	Investment Role	Booking Status	Allocation Start	Allocation Finish	Allocation	% Allocation
□	CRM Contact Center Development	Granger, Paula	✓	✓	Developer	Soft	10/6/09	2/19/10	376.00	100.00%
□	Joe's first project	ProjectManager, Joe		✓	Developer	Hard	3/29/10	3/29/10	8.00	100.00%
□	PCI Controls Remediation	Reed, Henry	✓	✓	Developer	Soft	2/4/10	5/26/10	640.00	100.00%
□	Vacation Time	Administrator, System	✓	✓	Developer	Soft	1/1/10	12/31/10	0.00	0.00%

Total Results: 4

5. Joe Pmo is a member of the Corporate PMO group. He has access to Projects.

   – Joe Pmo can see all projects from IT and Finance. He has Edit rights for the projects; even though he may not be the project manager assigned the project.



Projects

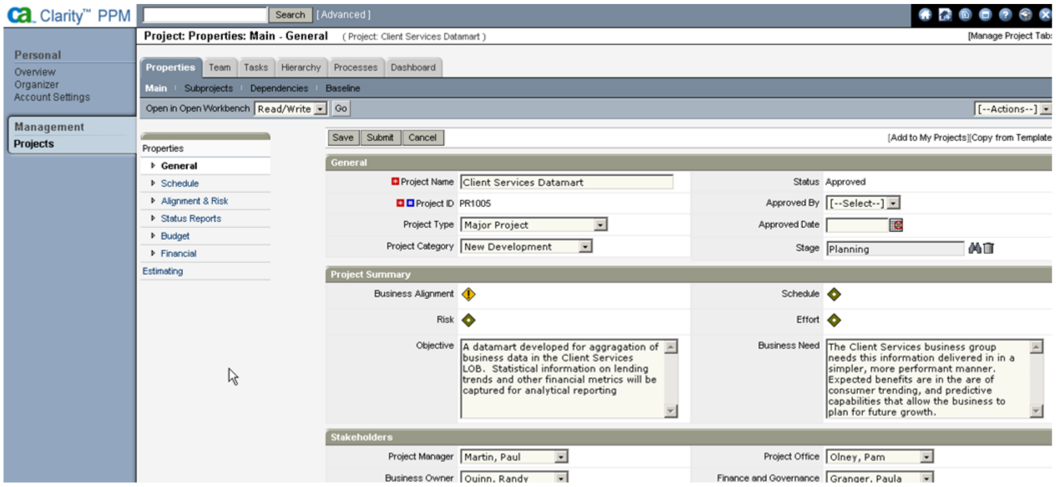
Project Filter

Filter: System Default

Project Name		Manager	
Project ID		Active	Yes
OBS Unit		Company Name	
OBS Unit Filter Mode	Unit only	Power Filter	[Build Power Filter]

« ‹ 1 2 3 › »

Project	ID	Risk	Status Indicator
Application Change Template	Process1004	◇	◆
Application COTS Template	Process1003	◇	◆
Automated Security Enhancements	PR1016	◆	◆
Call Center Upgrade	P2-1005	✖	◆
Change Mgt for Internal Portal	PR1024	⚠	◆
Change Mgt for Online Order Entry	PR1026	⚠	◆
Client Services Datamart	PR1005	◆	⚠
Client Services Datamart	P2-1001	⚠	◆
Compliance Audit - Security	PR1018	◆	⚠



Project: Properties: Main - General (Project: Client Services Datamart)

Open in Open Workbench: Read/Write

General

Project Name	Client Services Datamart	Status	Approved
Project ID	PR1005	Approved By	[--Select--]
Project Type	Major Project	Approved Date	
Project Category	New Development	Stage	Planning

Project Summary

Business Alignment	⚠	Schedule	◆
Risk	◆	Effort	◆
Objective	A datamart developed for aggregation of business data in the Client Services LOB. Statistical information on lending trends and other financial metrics will be captured for analytical reporting	Business Need	The Client Services business group needs this information delivered in in a simpler, more performant manner. Expected benefits are in the are of consumer trending, and predictive capabilities that allow the business to plan for future growth.

Stakeholders

Project Manager	Martin, Paul	Project Office	Olney, Pam
Business Owner	Quinn, Randy	Finance and Governance	Granger, Paula

Alternative Solutions to Implement Security Requirements

Alternate solutions can be applied to the use case to secure the CA Clarity PPM elements. Some of the options, advantages and disadvantages are described in the following section.

1. Use Global Rights for the Corporate PMO. Instead of granting Project – View to OBS Units IT and Finance, grant them the Project – View – All Global Right.

    – Advantage of using Global access rights:

    - If new departments start using CA Clarity PPM and the Corporate PMO is not monitoring their projects, the new projects are automatically included in the Global rule.

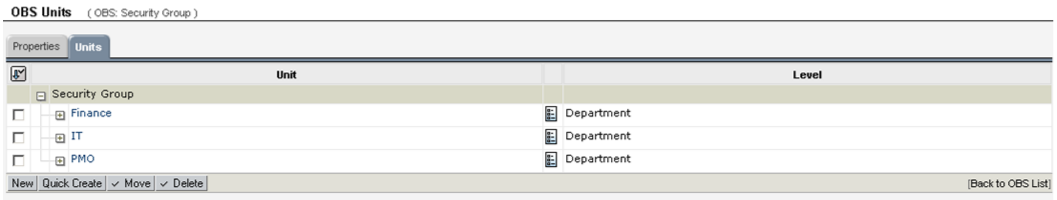
    – Advantages of using OBS Unit access rights:

    - If new departments start using CA Clarity PPM and the Corporate PMO is not monitoring their projects, using the OBS Unit approach helps ensure that they do not get unwanted access to these projects of new department.
    - Using the OBS Unit approach requires new OBS units to be set up when new departments start using CA Clarity PPM.

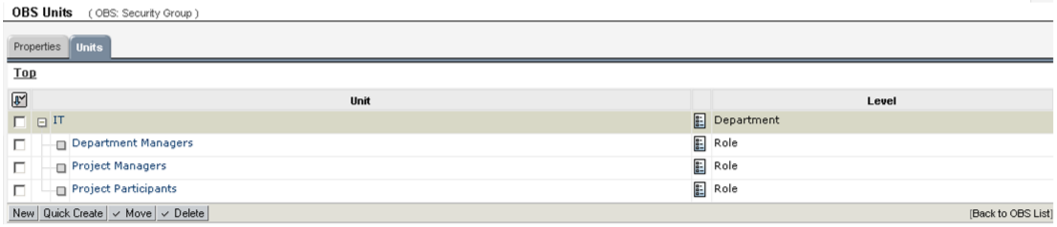
2. Use OBS Units as Actors instead of Groups.

    – Advantage: Centralize all security-related options in a single structure. An OBS may be easier to maintain depending on the number of departments involved.

    – Disadvantage: An OBS structure is more complex and more difficult to maintain in situations requiring radical changes.


OBS Units (OBS: Security Group)

	Unit	Level
	⊟ Security Group	
□	⊞ Finance	Department
□	⊞ IT	Department
□	⊞ PMO	Department


OBS Units (OBS: Security Group)

	Unit	Level
□	⊟ IT	Department
□	⊟ Department Managers	Role
□	⊟ Project Managers	Role
□	⊟ Project Participants	Role

How to Implement Attribute Security Using Subpages

It is a common request to segregate groups of attributes by role. Each resource should only have access to the attributes that are open to their role.

Use Case

> Implement Demand Management using the Idea object. The idea object is being categorized using an OBS named Organizational. The top-level of that OBS structure refers to All Lines of Business and is named All LOBs. In this example, all requestors have access to the Idea forms to enter basic and extended information about the demand. Basic information must be available in the Create and Edit layouts, in the General properties.

Extended information is comprised of additional subpages that display based on the type of demand the requestor is creating. The Type attribute defines the type of demand in this implementation example:

- Major Project
- Application Change
- Infrastructure Deployment
- Other

Advanced information such as Schedule and Budget should not be available to all requestors, but only to the Business Relationship Manager (BRM) evaluating the demands. The BRMs are members of the BRM Group.

The BRMs also must be allowed to enter opinions regarding the ideas in new attributes created for that purpose:

BRM Assessment

> Refers to a free-text attribute.

BRM Recommendation

> Uses to record the recommendation of BRM. Options are go, hold, or kill.

Defining the Security Configuration for Attribute Security

Review the use case to identify the security requirements and plan how to implement them in CA Clarity PPM. The following table provides a list of requirements gathered from the use case.

Information from the Use Case		
Actors	**Actions**	**Scope**
Requestor	Edit Idea Properties	Attributes in the General subpage
	Edit Idea Properties	Attributes in the Major Project subpage
	Edit Idea Properties	Attributes in the Application Change subpage
	Edit Idea Properties	Attributes in the Infrastructure subpage
	Edit Idea Properties	Attributes in the Other subpage
BRM	Edit Idea Properties	Attributes in the General subpage
	Edit Idea Properties	Attributes in the Major Project subpage
	Edit Idea Properties	Attributes in the Application Change subpage
	Edit Idea Properties	Attributes in the Infrastructure subpage
	Edit Idea Properties	Attributes in the Other subpage
	Edit Idea Properties	Attributes in the Schedule subpage
	Edit Idea Properties	Attributes in the Budget subpage
	Edit Idea Properties	BRM Assessment attribute
	Edit Idea Properties	BRM Recommendation attribute

Note: CA Clarity PPM uses Subpages to implement attribute-level security. You create a subpage to segregate the two new BRM attributes. The following information identifies how the subpages are organized in the CA Clarity PPM:

Organizing the Subpages				
Subpage	**New**	**Secure**	**Display Condition**	**Attributes**
General	No	No	No	Existing Attributes
Schedule	No	Yes	No	Existing Attributes
Budget	No	Yes	No	Existing Attributes
Major Project	No	No	Type =Major Project	Existing Attributes
Application Change	No	No	Type =Application Change	Existing Attributes
Infrastructure	No	No	Type =Infrastructure Deployment	Existing Attributes
BRM Assessment	Yes	Yes	No	BRM Assessment BRM Recommendation

Using the Organizing the Subpages table you can now identify the security requirements which are represented in the following table:

Security Elements in CA Clarity PPM		
CA Clarity PPM Actor	**CA Clarity PPM Access Right**	**CA Clarity PPM Scope**
Group: All Requestors	Idea – Initiator (Auto)	The ideas of requestor
Group: BRM	Idea – Edit Idea – Subpage Schedule Idea – Subpage Budget Idea – Subpage BRM Assessment	OBS: All LOBs OBS: All LOBs OBS: All LOBs OBS: All LOBs

How to Implement Security Requirements for Attribute Security

Use the information gathered to implement the security requirements:

1. Create Subpages. Mark as Secure when necessary.
2. Edit existing Subpages. Mark as Secure when necessary.
3. Create the Groups that are to be granted Access Rights.
4. Grant groups with the appropriate rights.
5. Secure the List.
6. Create the Resources.
7. Assign the Resources to the correct groups.

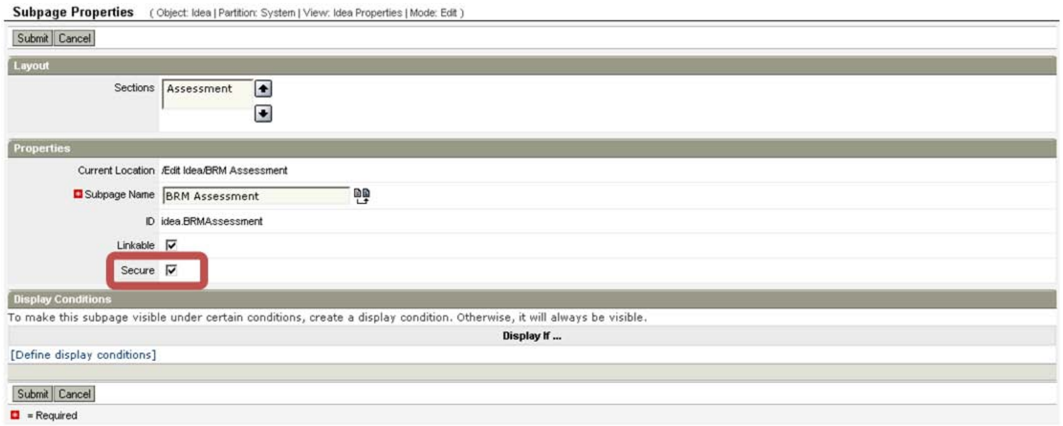
Use Case for Implementing Attribute Security

To implement Attribute Security do the following:

1. Create the Subpages

   In this example, out of eight subpages, 7 subpages exist. A subpage is created to segregate the new BRM Attributes to verify that they are secured.

   The new BRM Attributes subpage must be marked as Secure as illustrated below. The subpage properties and layout are shown in the following graphics:



Subpage Properties (Object: Idea | Partition: System | View: Idea Properties | Mode: Edit)

Submit | Cancel

Layout

Sections: Assessment

Properties

Current Location: /Edit Idea/BRM Assessment

Subpage Name: BRM Assessment

ID: idea.BRMAssessment

Linkable: ☑

Secure: ☑

Display Conditions

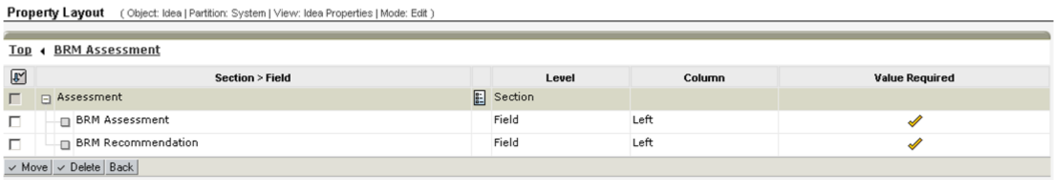
To make this subpage visible under certain conditions, create a display condition. Otherwise, it will always be visible.

Display If ...

[Define display conditions]

Submit | Cancel

= Required



Property Layout (Object: Idea | Partition: System | View: Idea Properties | Mode: Edit)

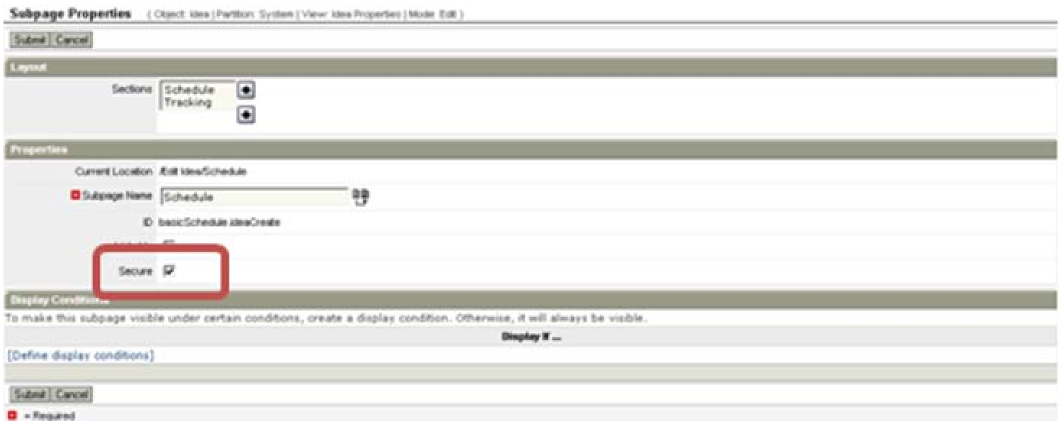
Top ◂ BRM Assessment

	Section > Field	Level	Column	Value Required
□	Assessment	Section		
□	BRM Assessment	Field	Left	✓
□	BRM Recommendation	Field	Left	✓

✓ Move | ✓ Delete | Back

2. Edit the Subpages

   Two of the existing subpages, Schedule and Budget need to be secured. Edit the subpage properties to mark them as Secure.



Subpage Properties (Object: Idea | Partition: System | View: Idea Properties | Mode: Edit)

Submit | Cancel

Layout

Sections: Schedule
Tracking

Properties

Current Location: /Edit Idea/Schedule

Subpage Name: Schedule

ID: basicSchedule.ideaCreate

Secure: ☑

Display Conditions

To make this subpage visible under certain conditions, create a display condition. Otherwise, it will always be visible.

Display If ...

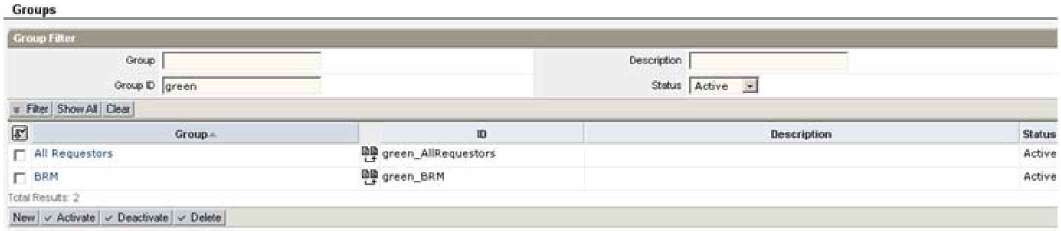
[Define display conditions]

Submit | Cancel

= Required

3. Create the Groups

   The groups for this use case All Requestors and BRM have been created as shown in the following graphic:



Groups

Group Filter

Group:

Group ID: green

Description:

Status: Active

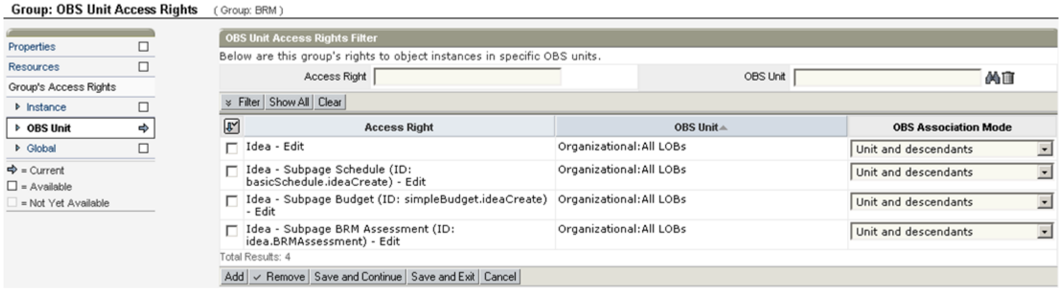
☐	Group	ID	Description	Status
☐	All Requestors	green_AllRequestors		Active
☐	BRM	green_BRM		Active

Total Results: 2

4. Grant access rights

   Use OBS security for the Ideas in this example. Use the Organizational OBS and grant access to the unit All LOBs and its descendants.

   – For the BRM group OBS Unit access rights: Idea – Edit access right to allow the BRM group to edit ideas, Idea – Subpage <subpage> access rights for the appropriate subpages.



Group: OBS Unit Access Rights (Group: BRM)

OBS Unit Access Rights Filter

Below are this group's rights to object instances in specific OBS units.

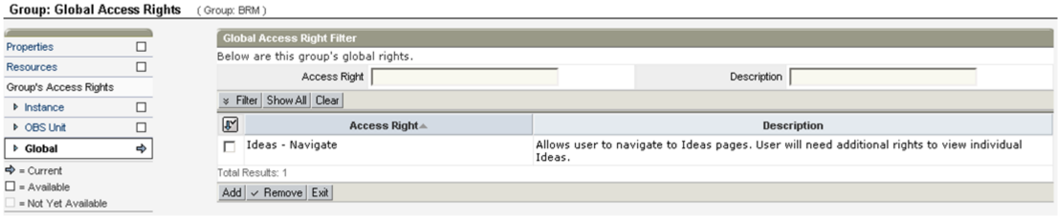
Access Right:

OBS Unit:

☐	Access Right	OBS Unit	OBS Association Mode
☐	Idea - Edit	Organizational:All LOBs	Unit and descendants
☐	Idea - Subpage Schedule (ID: basicSchedule.ideaCreate) - Edit	Organizational:All LOBs	Unit and descendants
☐	Idea - Subpage Budget (ID: simpleBudget.ideaCreate) - Edit	Organizational:All LOBs	Unit and descendants
☐	Idea - Subpage BRM Assessment (ID: idea.BRMAssessment) - Edit	Organizational:All LOBs	Unit and descendants

Total Results: 4

   – For the BRM Global access right: Ideas – Navigate to allow the group to navigate the Idea pages.



Group: Global Access Rights (Group: BRM)

Global Access Right Filter

Below are this group's global rights.

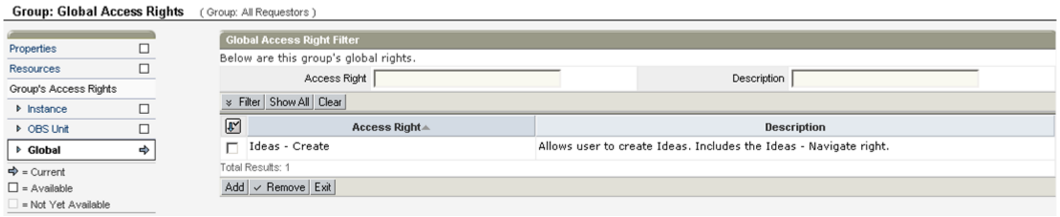
Access Right:

Description:

☐	Access Right	Description
☐	Ideas - Navigate	Allows user to navigate to Ideas pages. User will need additional rights to view individual Ideas.

Total Results: 1

- For the All Requestors group: Requestors have Automatic access rights to their ideas. No additional rights are granted other than the global rights they have.



Group: Global Access Rights (Group: All Requestors)

Global Access Right Filter

Below are this group's global rights.

Access Right	
Description	

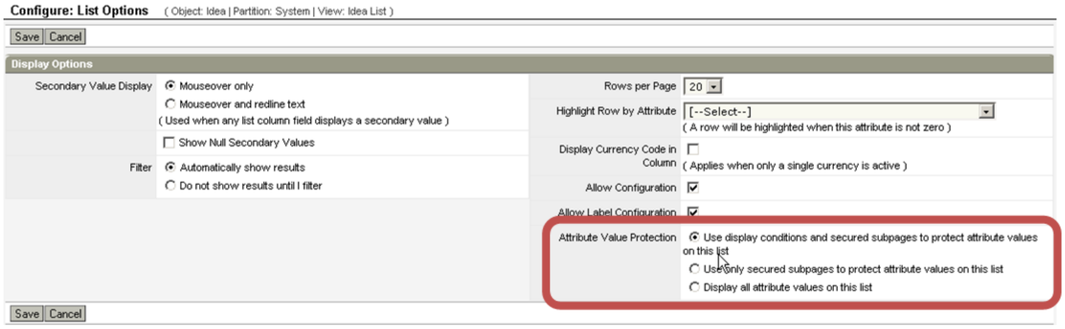
☐	Access Right	Description
☐	Ideas - Create	Allows user to create Ideas. Includes the Ideas - Navigate right.

Total Results: 1

5. Secure the List

This is an optional step. It is implemented for the example as all requestors should not have access to the BRM fields.

In the Options for the List view, the Attribute Value Protection option is set to Use display conditions and secured subpages to protect attribute values on this list.



Configure: List Options (Object: Idea | Partition: System | View: Idea List)

Display Options

Secondary Value Display: ● Mouseover only ○ Mouseover and redline text
(Used when any list column field displays a secondary value)

☐ Show Null Secondary Values

Filter: ● Automatically show results ○ Do not show results until I filter

Rows per Page: 20

Highlight Row by Attribute: [--Select--]
(A row will be highlighted when this attribute is not zero)

Display Currency Code in Column: ☐
(Applies when only a single currency is active)

Allow Configuration: ☑

Allow Label Configuration: ☑

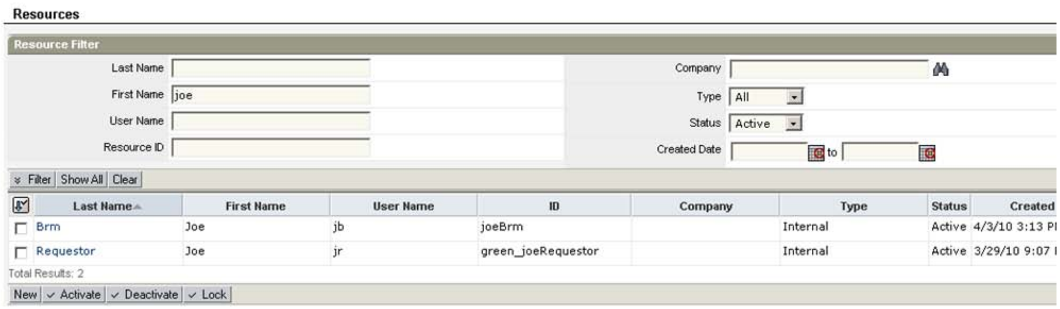
Attribute Value Protection:
● Use display conditions and secured subpages to protect attribute values on this list
○ Use only secured subpages to protect attribute values on this list
○ Display all attribute values on this list

6. Create Resources

The following fictitious resources are created for this example:

- Joe Requestor
- Joe Brm

The resources are displayed in the following graphic:



Resources

Resource Filter

Last Name	
First Name	joe
User Name	
Resource ID	
Company	
Type	All
Status	Active
Created Date	to

☐	Last Name	First Name	User Name	ID	Company	Type	Status	Created
☐	Brm	Joe	jb	joeBrm		Internal	Active	4/3/10 3:13 P
☐	Requestor	Joe	jr	green_joeRequestor		Internal	Active	3/29/10 9:07

Total Results: 2

7. Assign resources to Groups

   Each of the resources is assigned to a group.

   – Joe Requestor is a member of the All Requestors group

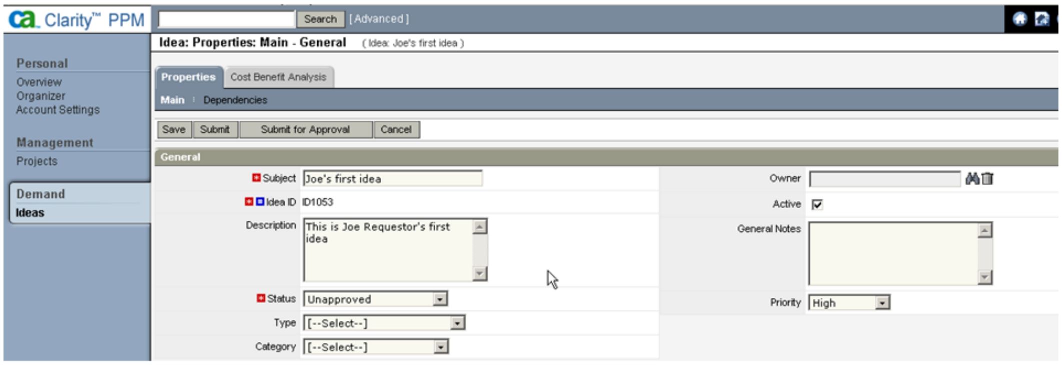
   – Joe Brm is a member of the BRM group

   Each resource should log in to confirm the appropriate access has been granted.

Confirmation

Joe Requestor

Joe Requestor can create ideas. He has access to the General subpage. He cannot view the Schedule, Budget, and BRM Assessment subpages because he is not a member of the BRM group.

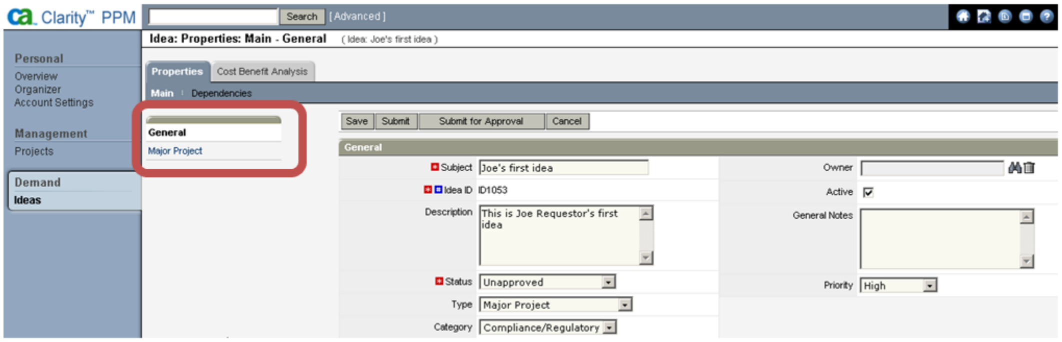


Idea: Properties: Main - General (Idea: Joe's first idea)

General

Subject	Joe's first idea	Owner	
Idea ID	ID1053	Active	☑
Description	This is Joe Requestor's first idea	General Notes	
Status	Unapproved	Priority	High
Type	[--Select--]		
Category	[--Select--]		

When he classifies an Idea as a Major Project Joe Requestor sees an option for a new subpage, named Major Project.

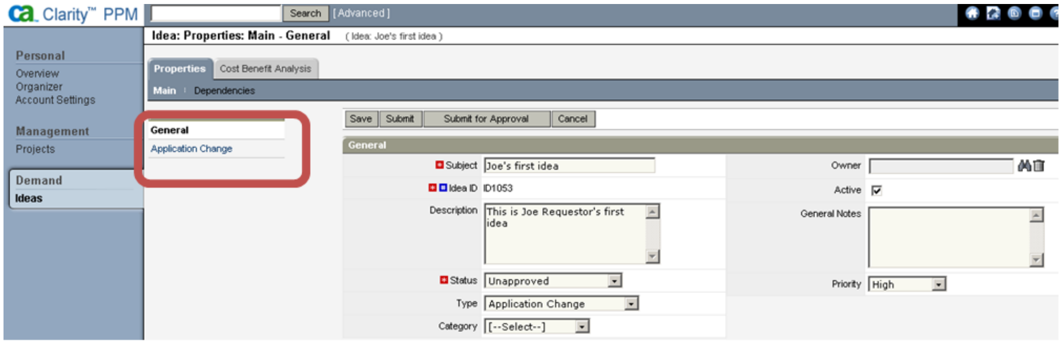


Idea: Properties: Main - General (Idea: Joe's first idea)

General

Subject	Joe's first idea	Owner	
Idea ID	ID1053	Active	☑
Description	This is Joe Requestor's first idea	General Notes	
Status	Unapproved	Priority	High
Type	Major Project		
Category	Compliance/Regulatory		

If Joe Requestor changes the Idea type to Application Change, he sees an option for a new subpage, named Application Change.

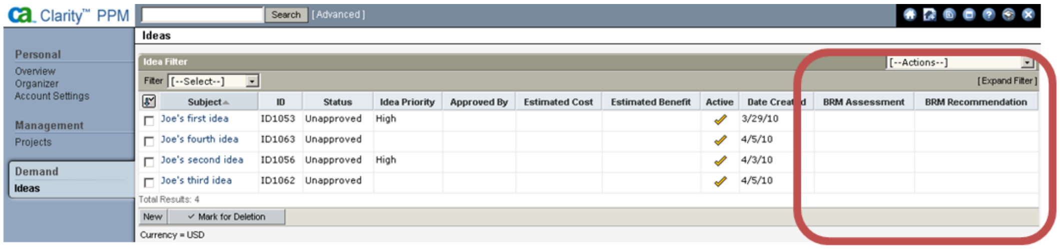


Idea: Properties: Main - General (Idea: Joe's first idea)

General

Subject: Joe's first idea
Idea ID: ID1053
Description: This is Joe Requestor's first idea
Status: Unapproved
Type: Application Change
Category: [--Select--]
Owner:
Active: ☑
General Notes:
Priority: High

If Joe Requestor tries to add the BRM attributes to his list, he does not see values of those the attributes.



Ideas

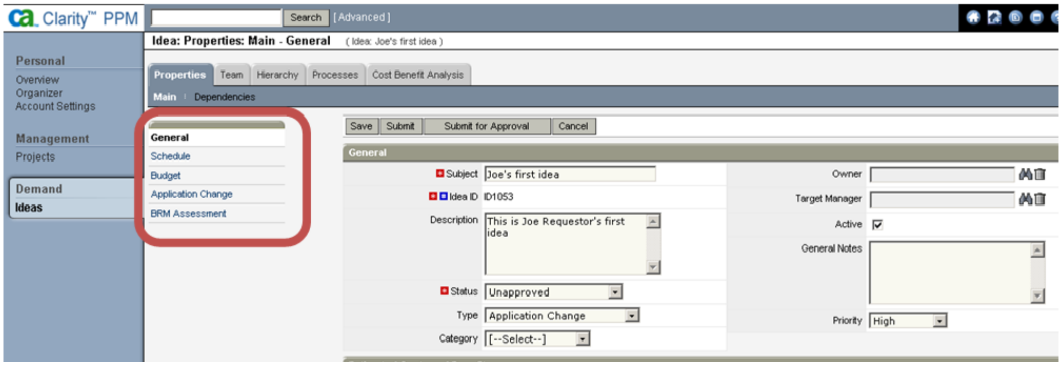
Subject	ID	Status	Idea Priority	Approved By	Estimated Cost	Estimated Benefit	Active	Date Creat d	BRM Assessment	BRM Recommendation
Joe's first idea	ID1053	Unapproved	High				✓	3/29/10		
Joe's fourth idea	ID1063	Unapproved					✓	4/5/10		
Joe's second idea	ID1056	Unapproved	High				✓	4/3/10		
Joe's third idea	ID1062	Unapproved					✓	4/5/10		

Total Results: 4

Currency = USD

Joe Brm

Joe Brm can see the ideas created by Joe Requestor. He has access to the General Schedule, Budget, and BRM Assessment subpages, and to the additional subpages.

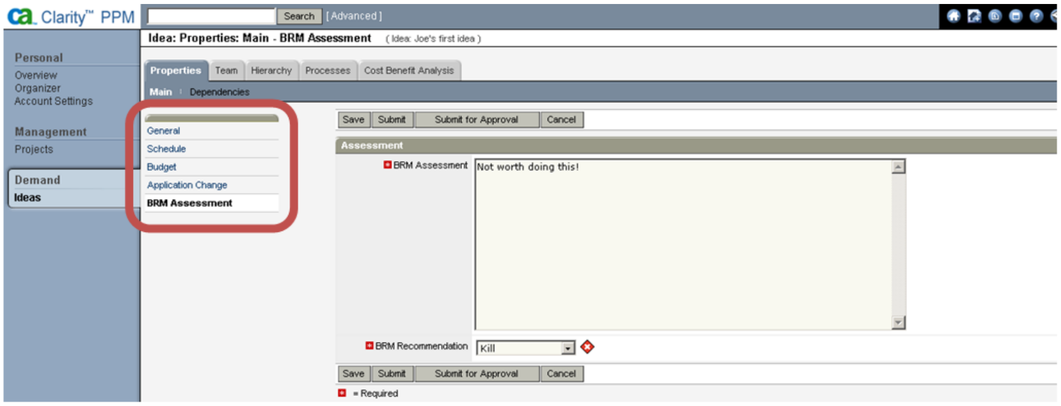


Idea: Properties: Main - General (Idea: Joe's first idea)

General

Subject: Joe's first idea
Idea ID: ID1053
Description: This is Joe Requestor's first idea
Status: Unapproved
Type: Application Change
Category: [--Select--]
Owner:
Target Manager:
Active: ☑
General Notes:
Priority: High

Joe Brm can enter values in the BRM Assessment page.



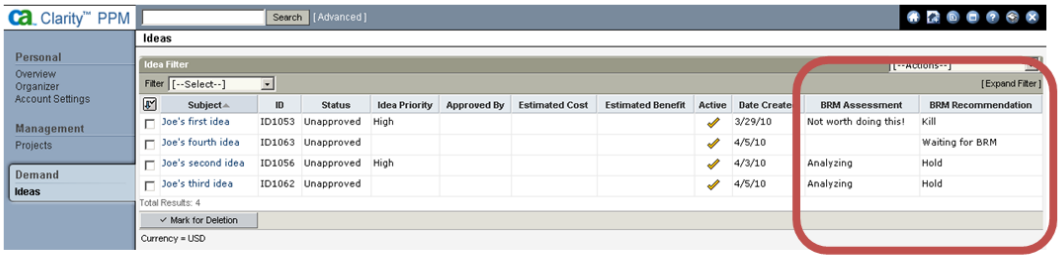
Idea: Properties: Main - BRM Assessment (Idea: Joe's first idea)

BRM Assessment: Not worth doing this!

BRM Recommendation: Kill

= Required

Joe Brm can add the BRM attributes to the list. He can see the values of those attributes in the list.



Ideas

	Subject	ID	Status	Idea Priority	Approved By	Estimated Cost	Estimated Benefit	Active	Date Create	BRM Assessment	BRM Recommendation
□	Joe's first idea	ID1053	Unapproved	High				✓	3/29/10	Not worth doing this!	Kill
□	Joe's fourth idea	ID1063	Unapproved					✓	4/5/10		Waiting for BRM
□	Joe's second idea	ID1056	Unapproved	High				✓	4/3/10	Analyzing	Hold
□	Joe's third idea	ID1062	Unapproved					✓	4/5/10	Analyzing	Hold

Total Results: 4

Currency = USD

Alternative Solutions

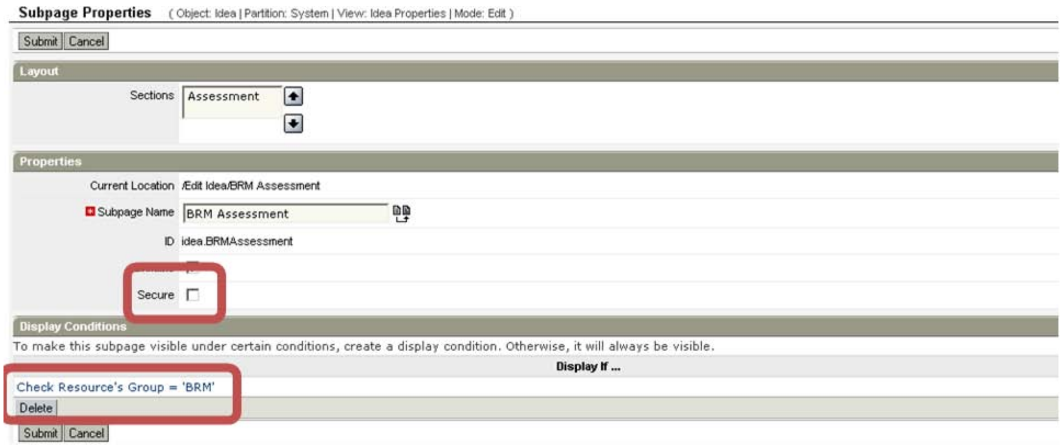
Alternate solutions can apply to the above use case (see page 144). A few of the options are provided here:

Implement security using Display Condition instead of using a secure subpage

- Advantage: You can see all of the rules in one place, both the business rules and security rules. In this case, someone who defines the business rules manages security.
- Disadvantages: More informal approach; the groups are hardcoded into the subpage display conditions, and not managed by security specialists.

- When using Display Conditions you can either show or hide the subpage, you cannot differentiate between Edit and View access.

  Note: You can differentiate between Edit and View using Secure Subpages.



Subpage Properties (Object: Idea | Partition: System | View: Idea Properties | Mode: Edit)

Sections: Assessment

Current Location: /Edit Idea/BRM Assessment

Subpage Name: BRM Assessment

ID: idea.BRMAssessment

Secure: □

To make this subpage visible under certain conditions, create a display condition. Otherwise, it will always be visible.

Display If ...

Check Resource's Group = 'BRM'

How to Secure Dashboard Pages

Another common request is to segregate dashboards between different levels of access.

Use Case

Create four different dashboards.

The first dashboard is intended to give project participants an overall situation of their currently assigned tasks and performance indicators.

The second dashboard is intended to give project managers an overview of their projects alerts and performance indicators.

The third dashboard is intended for the PMO team. The PMO team can monitor and audit all the projects of the company from this dashboard.

The last dashboard is a Top-level executive dashboard with special portlets that provide the users with important information to help them in the daily decision-making processes.

Additional requirements:

The Executive Dashboard should be visible only to the Executives group.

The PMO and Project Managers Dashboards should be visible to both PMO and Project Managers.

The Participants dashboard should be visible to all project participants.

Defining the Security Configuration for Dashboard Pages

Use the information in the use case to identify the security requirements and plan how to implement them in CA Clarity PPM.

In this example, assume that resources must also be granted access rights for the portlets in the dashboards. If access rights are not granted to the portlets in the dashboards, the users do not see the portlets or access the information available in the portlets.

The following table provides a list of requirements gathered from the use case for the dashboards:

Information from the Use Case		
Actors	**Actions**	**Scope**
Executives	View Dashboard	Executive Dashboard
PMO members	View Dashboard	PMO Dashboard
Project Managers	View Dashboard	PM Dashboard
Project Participants	View Dashboard	Team Member Dashboard

The security requirements are represented in the following table:

Security Elements in CA Clarity PPM		
CA Clarity PPM Actor	**CA Clarity PPM Access Right**	**CA Clarity PPM Scope**
Group: Executives	Page - View	Executive Dashboard
	Portlet - View	Customer Satisfaction
	Portlet - View	Employee/Outsourcing Comparison
	Portlet - View	Funding Status
	Portlet - View	YTD Spend By Initiative
	Portlet - View	Flash Alerts

Security Elements in CA Clarity PPM		
CA Clarity PPM Actor	**CA Clarity PPM Access Right**	**CA Clarity PPM Scope**
Group: Corporate PMO	Page - View	PMO Dashboard
Group: Corporate PMO	Portlet - View	Process Audit Hierarchy
	Portlet - View	Process Bottlenecks
	Portlet - View	Project Lifecycle Review
Group: All Project Managers	Page - View	Project Manager Dashboard
	Portlet - View	Cost and Effort Dashboard
	Portlet - View	Schedule Dashboard
Group: All Participants	Page - View	Team Member Dashboard
	Portlet - View	Team Member Organizer

Managing this instance by instance could become complex and time consuming in the future. It may be better to implement an OBS for grouping the Pages and Portlets.

The following table reflects the alternative of using an OBS Unit for grouping:

Security Elements in CA Clarity PPM		
CA Clarity PPM Actor	**CA Clarity PPM Access Right**	**CA Clarity PPM Scope**
Group: Executives	Page - View	OBS Unit: Pages and Portlets: Executive
	Portlet - View	OBS Unit: Pages and Portlets: Executive
Group: Corporate PMO	Page - View	OBS Unit: Pages and Portlets: Management
	Portlet - View	OBS Unit: Pages and Portlets: Management
Group: All Project Managers	Page - View	OBS Unit: Pages and Portlets: Management
	Portlet - View	OBS Unit: Pages and Portlets: Management
Group: All Participants	Page - View	OBS Unit: Pages and Portlets: General
	Portlet - View	OBS Unit: Pages and Portlets: General

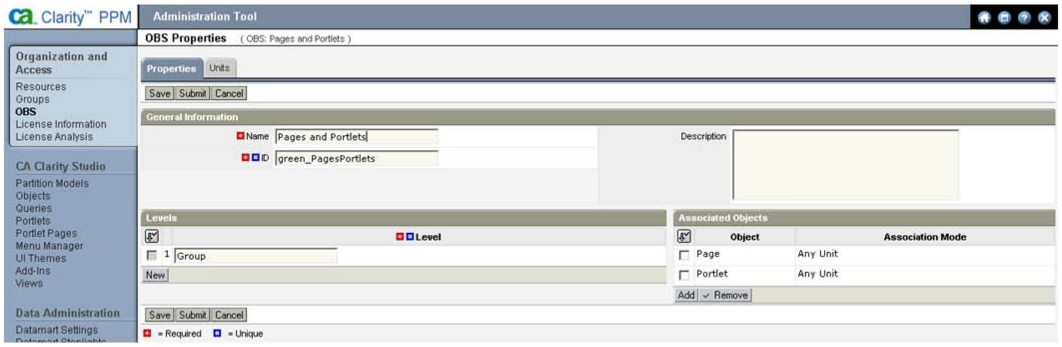
Implementing Security Requirements for Dashboard Pages

To implement security requirements for dashboard pages do the following

1. Create the OBS that will be used to categorize the Pages and Portlets.
2. Categorize the Pages and Portlets using the new OBS.
3. Create the Groups that are to be granted Access Rights.
4. Grant groups with the appropriate OBS Unit rights.
5. Create the Resources.
6. Assign the Resources to the correct groups.

Create the OBS

A new OBS named Pages and Portlets is created. It is used to group Pages and Portlets for security purposes. Three units have been created in the OBS: Executive, Management, and General.



OBS Properties (OBS: Pages and Portlets)

General Information

Name	Pages and Portlets
ID	green_PagesPortlets
Description	

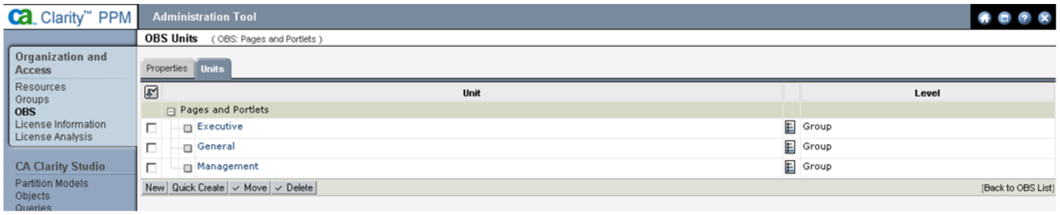
Levels

	Level
1	Group

Associated Objects

Object	Association Mode
Page	Any Unit
Portlet	Any Unit

🟥 = Required 🟦 = Unique



OBS Units (OBS: Pages and Portlets)

Unit	Level
Pages and Portlets	
Executive	Group
General	Group
Management	Group

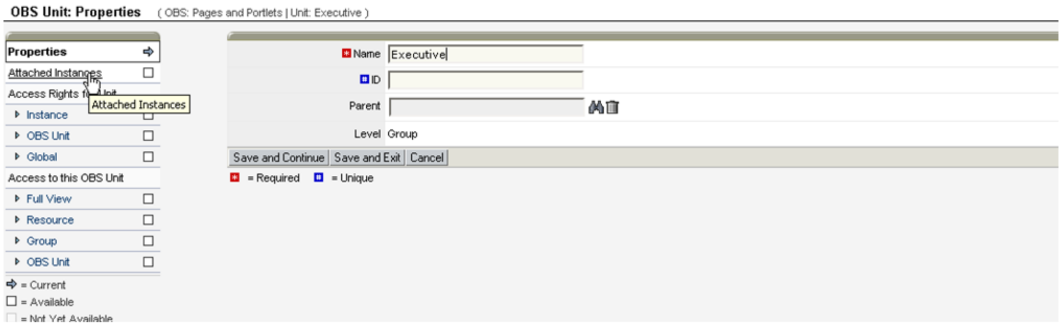
Categorize Pages and Portlets

You can categorize the Pages and Portlets using the OBS. Instead of navigating to each of the pages or portlets, you can do it all from within the OBS unit.

1. Click the Properties icon for the Executive unit.

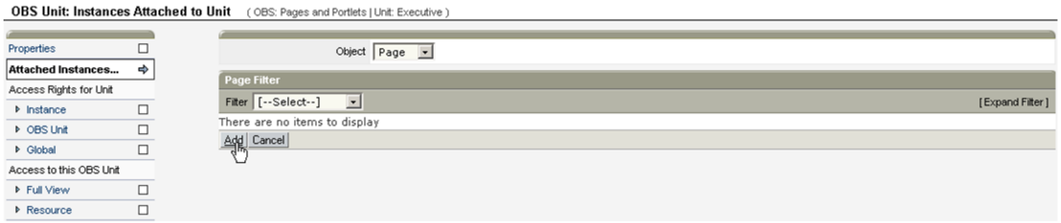
2. Click Attached Instances. This page displays the object instances (in this example, pages and portlets) that are attached to that OBS Unit.

   – Select Pages in the Object attribute menu and click Add to add more pages to the OBS unit.



OBS Unit: Properties (OBS: Pages and Portlets | Unit: Executive)

Name: Executive
ID:
Parent:
Level: Group



OBS Unit: Instances Attached to Unit (OBS: Pages and Portlets | Unit: Executive)

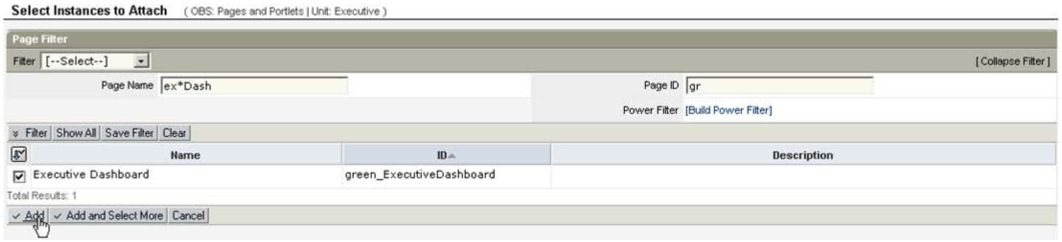
Object: Page

Page Filter

Filter: [--Select--]

There are no items to display

3. Filter the Executive Dashboard and click Add.



Select Instances to Attach (OBS: Pages and Portlets | Unit: Executive)

Page Filter

Filter: [--Select--]

Page Name: ex*Dash

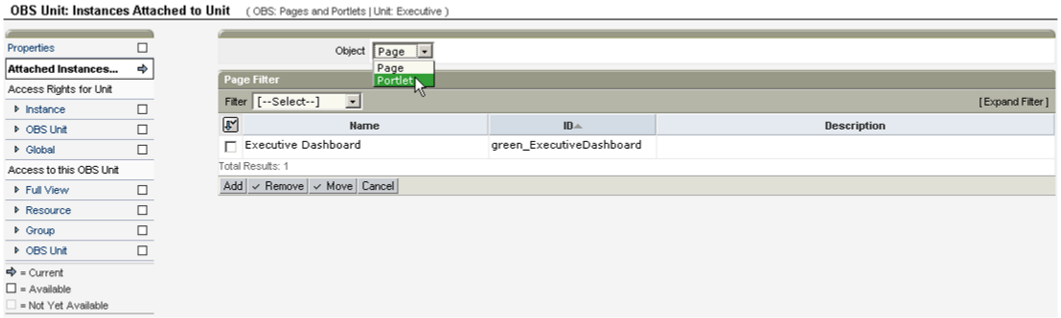
Page ID: gr

Power Filter: [Build Power Filter]

	Name	ID	Description
☑	Executive Dashboard	green_ExecutiveDashboard	

Total Results: 1

4. Change the Object to Portlet, and click Add.



OBS Unit: Instances Attached to Unit (OBS: Pages and Portlets | Unit: Executive)

Object: Page

Page Filter

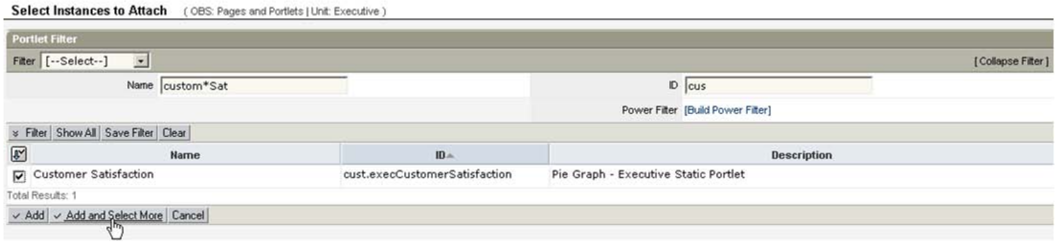
Filter [--Select--]

	Name	ID	Description
□	Executive Dashboard	green_ExecutiveDashboard	

Total Results: 1

5. Search for the appropriate portlets.

6. Select the portlets using the checkbox on the left, and click Add and Select More to continue adding portlets.



Select Instances to Attach (OBS: Pages and Portlets | Unit: Executive)

Portlet Filter

Filter [--Select--]

Name: custom*Sat

ID: cus

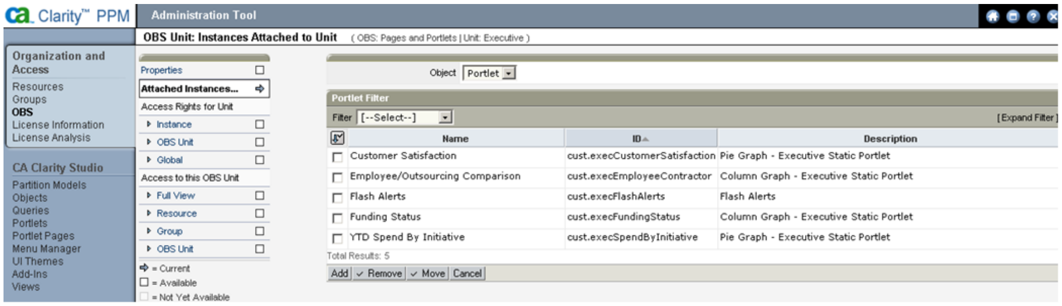
Power Filter: [Build Power Filter]

	Name	ID	Description
☑	Customer Satisfaction	cust.execCustomerSatisfaction	Pie Graph - Executive Static Portlet

Total Results: 1

When you have completed selecting portlets, click Add.

7. After all the required portlets are related to the OBS unit, click Cancel.



OBS Unit: Instances Attached to Unit (OBS: Pages and Portlets | Unit: Executive)

Object: Portlet

Portlet Filter

Filter [--Select--]

	Name	ID	Description
□	Customer Satisfaction	cust.execCustomerSatisfaction	Pie Graph - Executive Static Portlet
□	Employee/Outsourcing Comparison	cust.execEmployeeContractor	Column Graph - Executive Static Portlet
□	Flash Alerts	cust.execFlashAlerts	Flash Alerts
□	Funding Status	cust.execFundingStatus	Column Graph - Executive Static Portlet
□	YTD Spend By Initiative	cust.execSpendByInitiative	Pie Graph - Executive Static Portlet

Total Results: 5

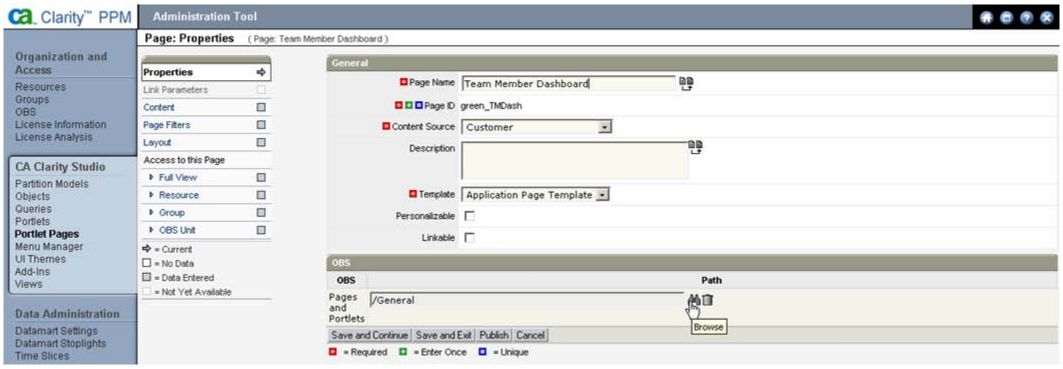
Use the same procedure to add pages and portlets as required to the other OBS Units.

Important! No access has been granted yet, only categorizing of the pages and portlets using the OBS Unit. Add Groups (or Resources) to the OBS Units and assign the desired access rights.

Create the Groups

For this example, navigate to the Team Member Dashboard page, then to the Team Member Organizer portlet, and enter the OBS Unit from there.

1. Use the OBS search field and navigate to the Team Member Dashboard page.

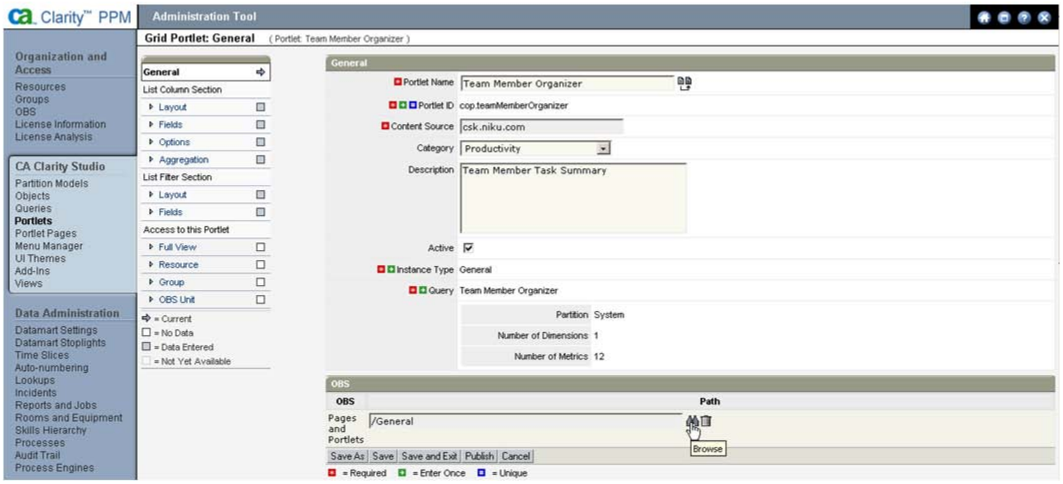


Page: Properties (Page: Team Member Dashboard)

Page Name	Team Member Dashboard
Page ID	green_TMDash
Content Source	Customer
Description	
Template	Application Page Template
Personalizable	□
Linkable	□

OBS	Path
Pages and Portlets	/General

2. Next, browse using the OBS search field, and navigate to the Team Member Organizer portlet.

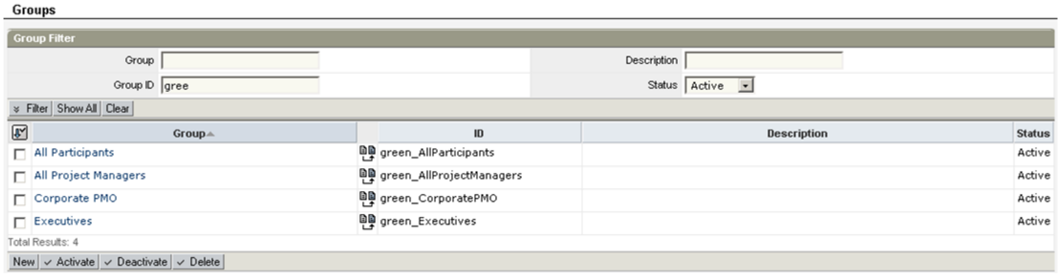


Grid Portlet: General (Portlet: Team Member Organizer)

Portlet Name	Team Member Organizer
Portlet ID	cop.teamMemberOrganizer
Content Source	csk.niku.com
Category	Productivity
Description	Team Member Task Summary
Active	☑
Instance Type	General
Query	Team Member Organizer
Partition	System
Number of Dimensions	1
Number of Metrics	12

OBS	Path
Pages and Portlets	/General

3. Select Groups from the Organization and Access menu option to review the existing Groups. Add new groups as required.



Groups

Group		Description	
Group ID	gree	Status	Active

Group	ID	Description	Status
All Participants	green_AllParticipants		Active
All Project Managers	green_AllProjectManagers		Active
Corporate PMO	green_CorporatePMO		Active
Executives	green_Executives		Active

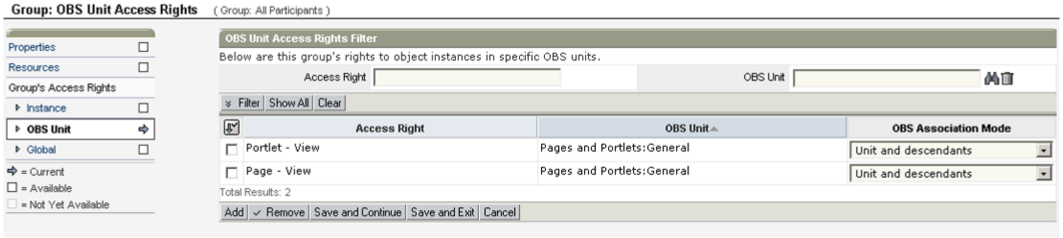
Total Results: 4

Note: For more information about adding Groups in CA Clarity PPM, see the *CA Clarity PPM Administration Guide*.

Grant Groups OBS Unit rights

This task is performed either from the Groups pages or from the OBS Units. Examples of each option are provided:

1. From within a group: All Participants group



Group: OBS Unit Access Rights (Group: All Participants)

OBS Unit Access Rights Filter

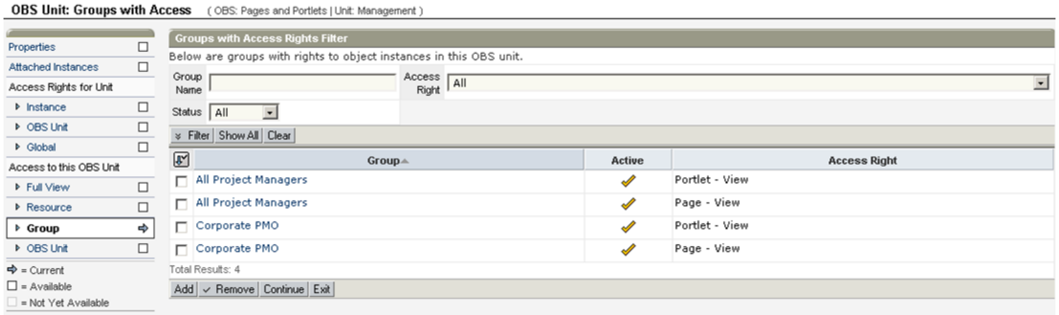
Below are this group's rights to object instances in specific OBS units.

Access Right ____ OBS Unit ____

☐	Access Right	OBS Unit	OBS Association Mode
☐	Portlet - View	Pages and Portlets:General	Unit and descendants
☐	Page - View	Pages and Portlets:General	Unit and descendants

Total Results: 2

2. From within the OBS Unit: Pages and Portlets: Management



OBS Unit: Groups with Access (OBS: Pages and Portlets | Unit: Management)

Groups with Access Rights Filter

Below are groups with rights to object instances in this OBS unit.

Group Name ____ Access Right All

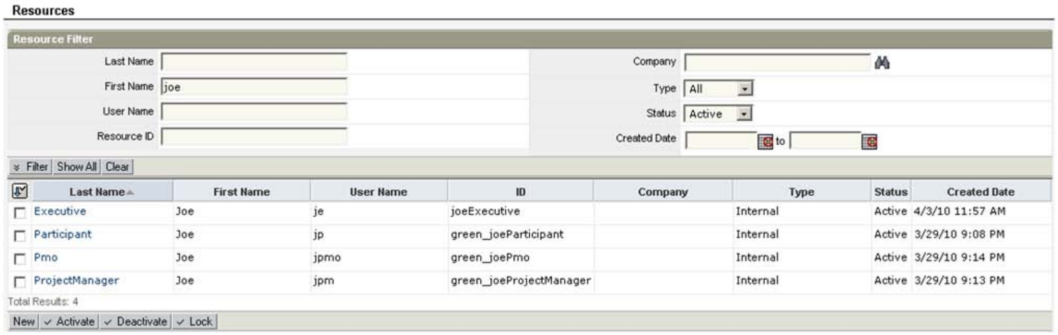
Status All

☐	Group	Active	Access Right
☐	All Project Managers	✓	Portlet - View
☐	All Project Managers	✓	Page - View
☐	Corporate PMO	✓	Portlet - View
☐	Corporate PMO	✓	Page - View

Total Results: 4

Create Resources

The following fictitious users have been created for this example: Joe Executive, Joe Participant, Joe Pmo, and Joe ProjectManager.



Resources

Resource Filter

Last Name		Company	
First Name	joe	Type	All
User Name		Status	Active
Resource ID		Created Date	to

☐	Last Name	First Name	User Name	ID	Company	Type	Status	Created Date
☐	Executive	Joe	je	joeExecutive		Internal	Active	4/3/10 11:57 AM
☐	Participant	Joe	jp	green_joeParticipant		Internal	Active	3/29/10 9:08 PM
☐	Pmo	Joe	jpmo	green_joePmo		Internal	Active	3/29/10 9:14 PM
☐	ProjectManager	Joe	jpm	green_joeProjectManager		Internal	Active	3/29/10 9:13 PM

Total Results: 4

Assign Resources to Groups

Each of the users has been assigned the correct groups, as indicated:

- Joe Executive is a member of the Executives group
- Joe Participant is a member of the All Participants group
- Joe Pmo is a member of the Corporate PMO group
- Joe ProjectManager is a member of the All Project Managers group

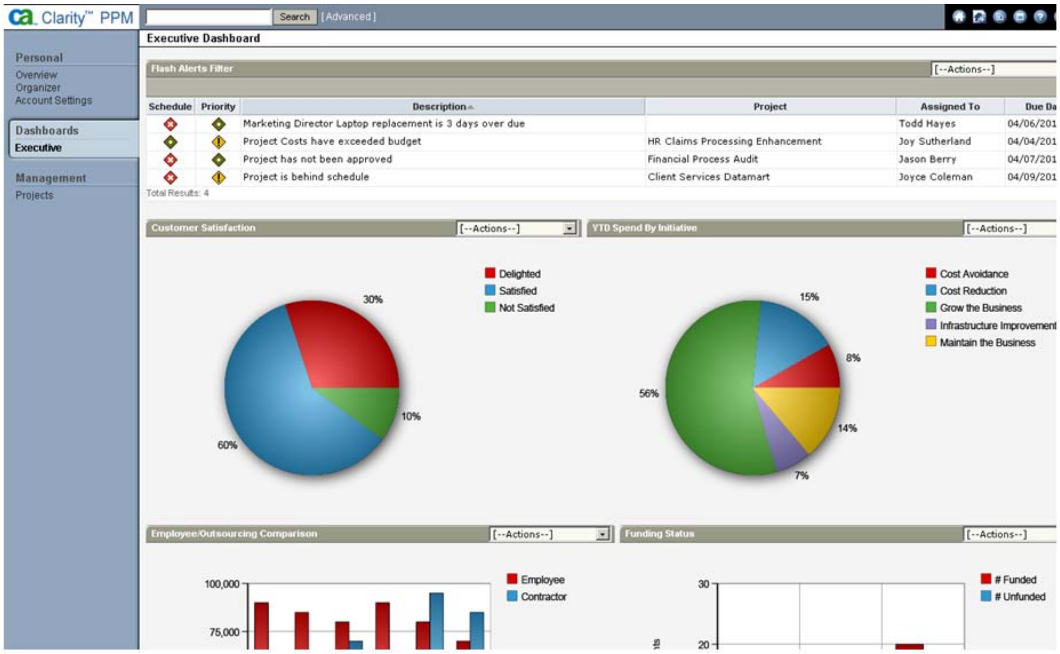
Confirmation

Log in to CA Clarity PPM to view the access the resources have to the dashboards.

- Joe Executive has access to the Executive Dashboard
- Joe Participant has access to the Team Member dashboard
- Joe ProjectManager has access to the Project Manager and PMO dashboards
- Joe Pmo has access to the Project Manager and PMO dashboards

Important! The information displayed in a dashboard varies with the access level of the resource accessing the dashboard. One resource may have View access only while another may have View and Edit. The displayed information may be limited to the individual resource’s own information while another resource may have access to information for an entire group.

Executive Dashboard – Accessed by Joe Executive

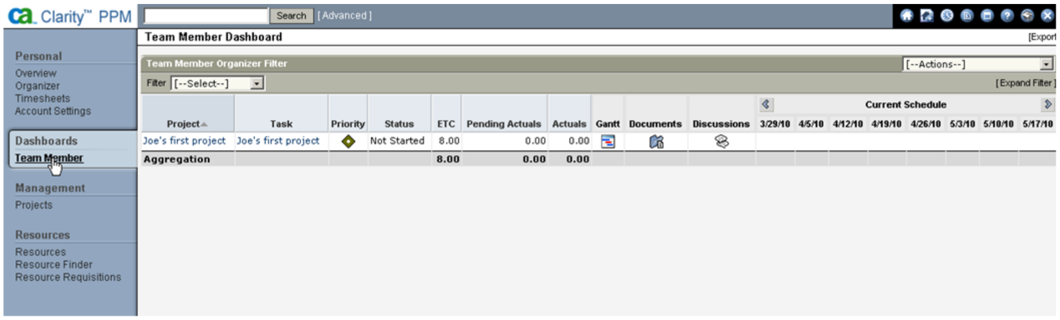


Executive Dashboard

Schedule	Priority	Description	Project	Assigned To	Due Da
⊗	◆	Marketing Director Laptop replacement is 3 days over due		Todd Hayes	04/06/201
◆	⚠	Project Costs have exceeded budget	HR Claims Processing Enhancement	Joy Sutherland	04/04/201
⊗	◆	Project has not been approved	Financial Process Audit	Jason Berry	04/07/201
⊗	⚠	Project is behind schedule	Client Services Datamart	Joyce Coleman	04/09/201

Total Results: 4

Team Member Dashboard – Accessed by Joe Participant



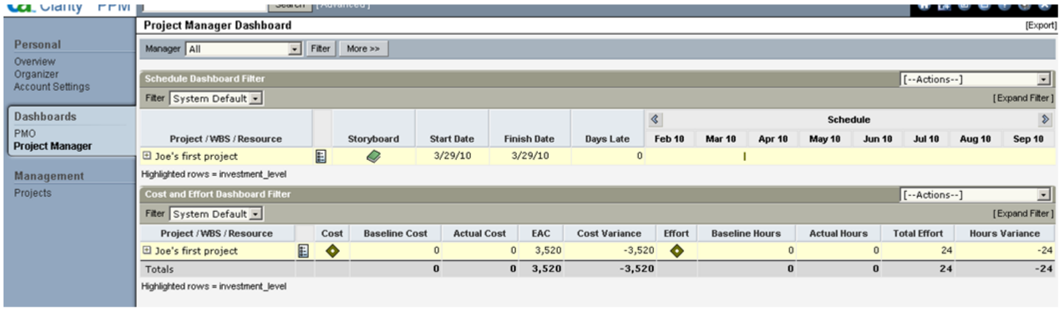
Team Member Dashboard

Filter [--Select--]

Project	Task	Priority	Status	ETC	Pending Actuals	Actuals	Gantt	Documents	Discussions	3/29/10	4/5/10	4/12/10	4/19/10	4/26/10	5/3/10	5/10/10	5/17/10
Joe's first project	Joe's first project	◆	Not Started	8.00	0.00	0.00											
Aggregation				**8.00**	**0.00**	**0.00**											

Project Manager Dashboard – Accessed by Joe Pmo and Joe ProjectManager

Note: Joe ProjectManager can only access his own projects as illustrated; Joe Pmo has access to all projects.



Project Manager Dashboard

Manager All

Filter System Default

Project / WBS / Resource		Storyboard	Start Date	Finish Date	Days Late	Feb 10	Mar 10	Apr 10	May 10	Jun 10	Jul 10	Aug 10	Sep 10
⊞ Joe's first project			3/29/10	3/29/10	0								

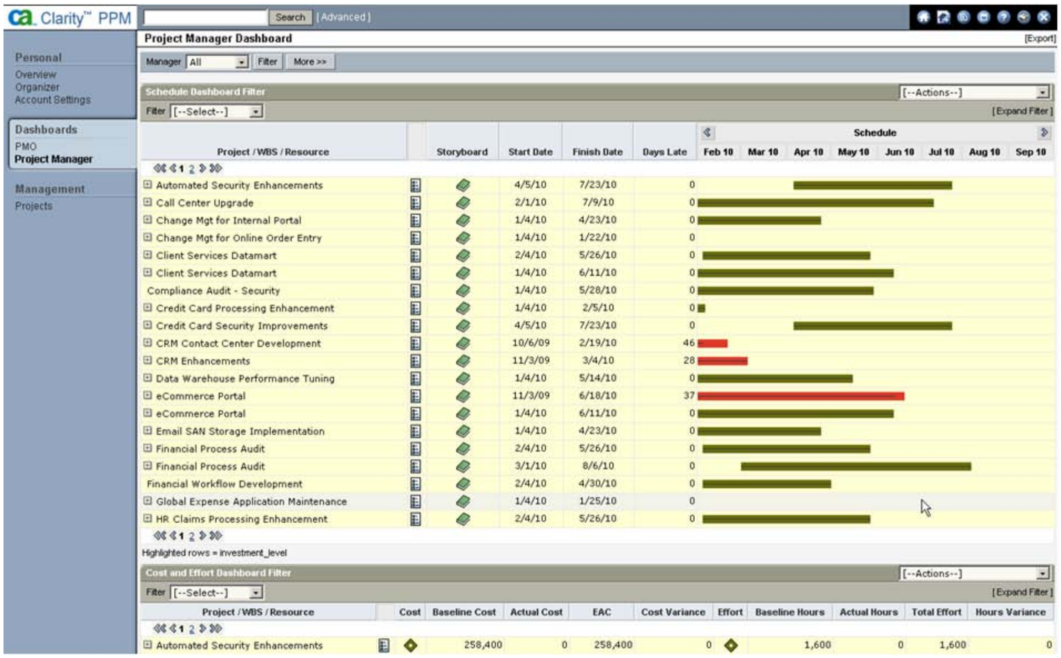
Highlighted rows = investment_level

Filter System Default

Project / WBS / Resource		Cost	Baseline Cost	Actual Cost	EAC	Cost Variance	Effort	Baseline Hours	Actual Hours	Total Effort	Hours Variance
⊞ Joe's first project		◆	0	0	3,520	-3,520	◆	0	0	24	-24
Totals			**0**	**0**	**3,520**	**-3,520**		**0**	**0**	**24**	**-24**

Highlighted rows = investment_level

Project Manager Dashboard – as accessed by Joe Pmo



Project Manager Dashboard

Schedule Dashboard Filter

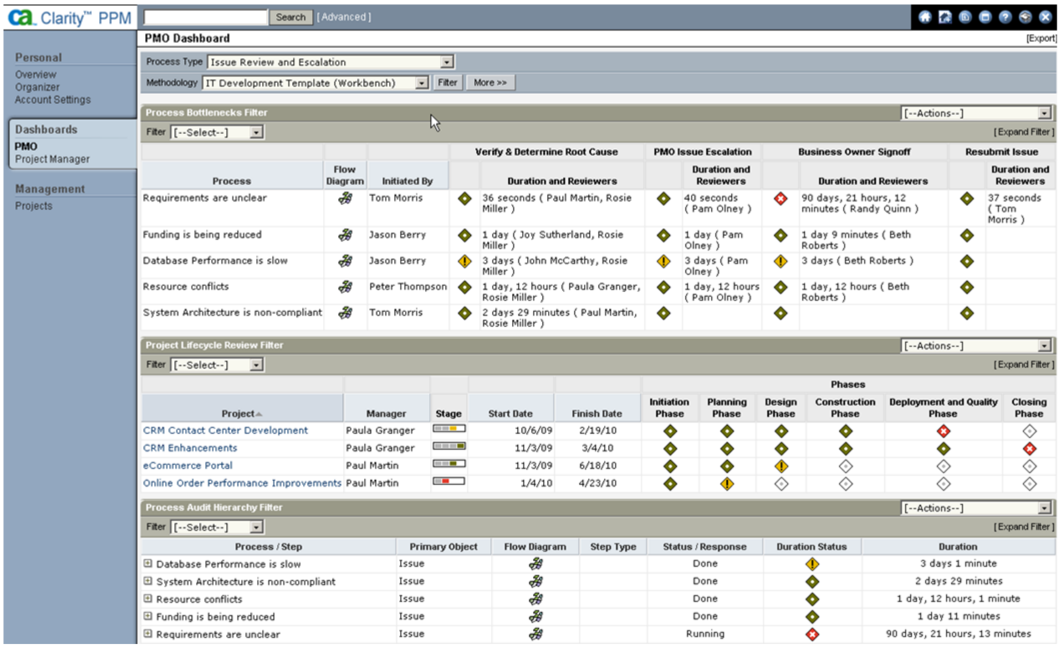
Project / WBS / Resource	Storyboard	Start Date	Finish Date	Days Late
Automated Security Enhancements		4/5/10	7/23/10	0
Call Center Upgrade		2/1/10	7/9/10	0
Change Mgt for Internal Portal		1/4/10	4/23/10	0
Change Mgt for Online Order Entry		1/4/10	1/22/10	0
Client Services Datamart		2/4/10	5/26/10	0
Client Services Datamart		1/4/10	6/11/10	0
Compliance Audit - Security		1/4/10	5/28/10	0
Credit Card Processing Enhancement		1/4/10	2/5/10	0
Credit Card Security Improvements		4/5/10	7/23/10	0
CRM Contact Center Development		10/6/09	2/19/10	46
CRM Enhancements		11/3/09	3/4/10	28
Data Warehouse Performance Tuning		1/4/10	5/14/10	0
eCommerce Portal		11/3/09	6/18/10	37
eCommerce Portal		1/4/10	6/11/10	0
Email SAN Storage Implementation		1/4/10	4/23/10	0
Financial Process Audit		2/4/10	5/26/10	0
Financial Process Audit		3/1/10	8/6/10	0
Financial Workflow Development		2/4/10	4/30/10	0
Global Expense Application Maintenance		1/4/10	1/25/10	0
HR Claims Processing Enhancement		2/4/10	5/26/10	0

Highlighted rows = investment_level

Cost and Effort Dashboard Filter

Project / WBS / Resource	Cost	Baseline Cost	Actual Cost	EAC	Cost Variance	Effort	Baseline Hours	Actual Hours	Total Effort	Hours Variance
Automated Security Enhancements	◆	258,400	0	258,400	0	◆	1,600	0	1,600	0

PMO Dashboard - Accessed by Joe Pmo and Joe ProjectManager. This graphic illustrates the dashboard as accessed by Joe Pmo.



PMO Dashboard

Process Type: Issue Review and Escalation

Methodology: IT Development Template (Workbench)

Process Bottlenecks Filter

			Verify & Determine Root Cause		PMO Issue Escalation		Business Owner Signoff		Resubmit Issue	
Process	Flow Diagram	Initiated By		Duration and Reviewers		Duration and Reviewers		Duration and Reviewers		Duration and Reviewers
Requirements are unclear		Tom Morris	◆	36 seconds (Paul Martin, Rosie Miller)	◆	40 seconds (Pam Olney)	✖	90 days, 21 hours, 12 minutes (Randy Quinn)	◆	37 seconds (Tom Morris)
Funding is being reduced		Jason Berry	◆	1 day (Joy Sutherland, Rosie Miller)	◆	1 day (Pam Olney)	◆	1 day 9 minutes (Beth Roberts)	◆	
Database Performance is slow		Jason Berry	⚠	3 days (John McCarthy, Rosie Miller)	⚠	3 days (Pam Olney)	⚠	3 days (Beth Roberts)	◆	
Resource conflicts		Peter Thompson	◆	1 day, 12 hours (Paula Granger, Rosie Miller)	◆	1 day, 12 hours (Pam Olney)	◆	1 day, 12 hours (Beth Roberts)	◆	
System Architecture is non-compliant		Tom Morris	◆	2 days 29 minutes (Paul Martin, Rosie Miller)	◆		◆		◆	

Project Lifecycle Review Filter

					Phases					
Project	Manager	Stage	Start Date	Finish Date	Initiation Phase	Planning Phase	Design Phase	Construction Phase	Deployment and Quality Phase	Closing Phase
CRM Contact Center Development	Paula Granger		10/6/09	2/19/10	◆	◆	◆	◆	✖	◇
CRM Enhancements	Paula Granger		11/3/09	3/4/10	◆	◆	◆	◆	◆	✖
eCommerce Portal	Paul Martin		11/3/09	6/18/10	◆	◆	⚠	◇	◇	◇
Online Order Performance Improvements	Paul Martin		1/4/10	4/23/10	◆	⚠	◇	◇	◇	◇

Process Audit Hierarchy Filter

Process / Step	Primary Object	Flow Diagram	Step Type	Status / Response	Duration Status	Duration
Database Performance is slow	Issue			Done	⚠	3 days 1 minute
System Architecture is non-compliant	Issue			Done	◆	2 days 29 minutes
Resource conflicts	Issue			Done	◆	1 day, 12 hours, 1 minute
Funding is being reduced	Issue			Done	◆	1 day 11 minutes
Requirements are unclear	Issue			Running	✖	90 days, 21 hours, 13 minutes

Alternative Solutions for Dashboard Pages

Alternate solutions are available for this use case. Some of the options are described here:

- Use Instance rights instead of using OBS Unit Rights. You can use Instance rights and grant access directly to each dashboard and portlet.
  - Advantages

    One less OBS in CA Clarity PPM, no need to categorize each Page or Portlet using an OBS Unit.

    Access cannot be granted by accident. This can happen if the wrong OBS unit is selected to categorize the data instance when using OBS Unit rights.
  - Disadvantages: Depending on the number of Portlets and Pages, it can be complex and time consuming to maintain.
- Do not secure Portlets. Instead of securing Pages and Portlets, secure pages and do not allow them to be personalized.

  If the data is secured (Projects, Resources, Ideas, Portfolios, and so on) and if you do not have access to the data, the portlet does not display anything you should not have access to view.

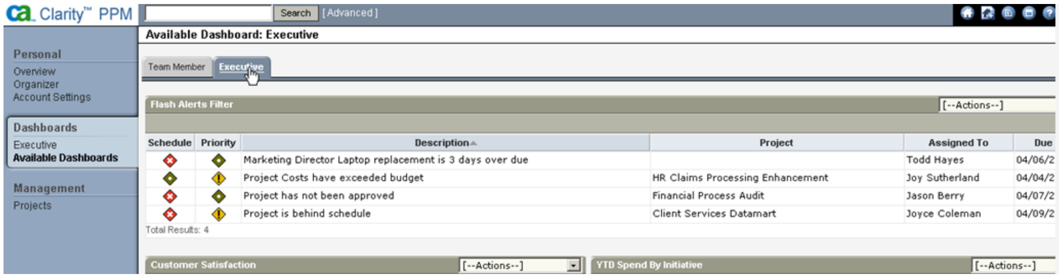
  In this case, you can grant All Resources with Portlet Viewer - All access right.
  - Advantage: Decreased maintenance. Build secure portlets that take in to account security for Projects, Resources, Portfolios and all CA Clarity PPM objects. Unless there is a specific business reason to deny access to a portlet, you do not have to secure the portlet.
  - Disadvantage: Decreased access control. There may come a time when a single portlet must be restricted and cannot be viewed by everyone. If you do not have Portlet Security implemented, implement that before releasing the new restricted portlet.

- Use a single Dashboard with multiple TABs. In the previous use case, four different dashboards were created without tabs. You can create one dashboard with multiple tabs, one for each role. Using this model, security is managed at the tab level, rather than at the dashboard level. The default dashboard is open to all users as it is the common object in this model.
  - Advantage: The default dashboard and its tabs would be accessed using one menu link, instead of having several menu links for navigation.
  - Disadvantage: Users must use at least two mouse clicks to navigate to a dashboard tab: one click the menu link and the second click to select a tab.

An example of using one menu link (named Available Dashboards) is illustrated in the following graphics.

Note: The Team Member dashboard is available for all roles and the other dashboards are secured.

The Executive Group sees the Team Member and Executive dashboards:



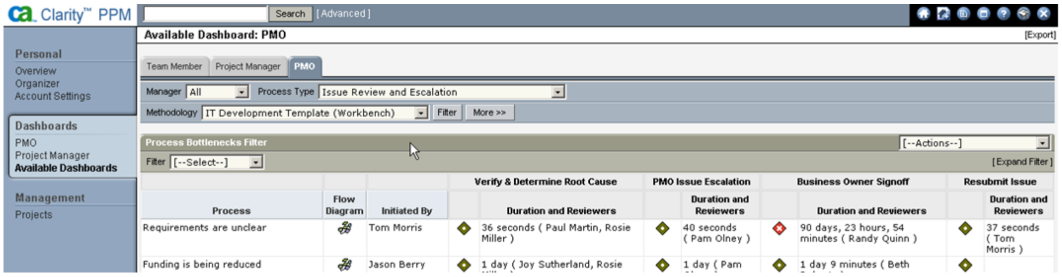
Available Dashboard: Executive

Flash Alerts Filter

Schedule	Priority	Description	Project	Assigned To	Due
✖	◆	Marketing Director Laptop replacement is 3 days over due		Todd Hayes	04/06/2
◆	⚠	Project Costs have exceeded budget	HR Claims Processing Enhancement	Joy Sutherland	04/04/2
✖	◆	Project has not been approved	Financial Process Audit	Jason Berry	04/07/2
✖	⚠	Project is behind schedule	Client Services Datamart	Joyce Coleman	04/09/2

Total Results: 4

The PMO Group sees the Team Member, Project Manager and PMO tabs as illustrated in the following graphic:



Available Dashboard: PMO

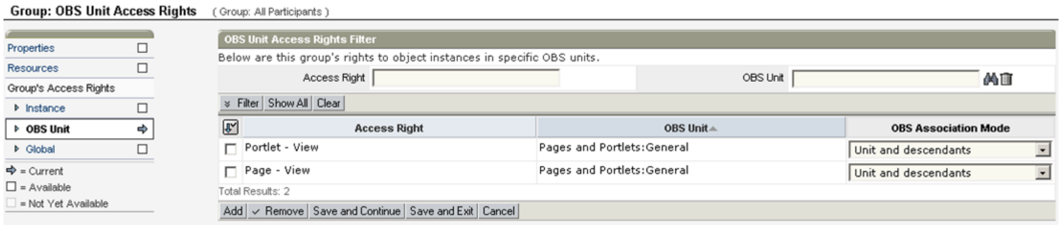
Manager: All
Process Type: Issue Review and Escalation
Methodology: IT Development Template (Workbench)

Process Bottlenecks Filter

Filter: [--Select--]

			Verify & Determine Root Cause		PMO Issue Escalation		Business Owner Signoff		Resubmit Issue	
Process	Flow Diagram	Initiated By		Duration and Reviewers		Duration and Reviewers		Duration and Reviewers		Duration and Reviewers
Requirements are unclear	⚙	Tom Morris	◆	36 seconds (Paul Martin, Rosie Miller)	◆	40 seconds (Pam Olney)	✖	90 days, 23 hours, 54 minutes (Randy Quinn)	◆	37 seconds (Tom Morris)
Funding is being reduced	⚙	Jason Berry	◆	1 day (Joy Sutherland, Rosie	◆	1 day (Pam	◆	1 day 9 minutes (Beth	◆	

- Control Portlet access rights. In the previous example, no control is defined to indicate which Portlets each of the roles has access to. You can implement portlet-level control either by Instance or by using an OBS Unit to categorize portlets.
  - Advantages: Using the same mechanism, you can implement a security solution that segregates Dashboards by role and also segregates the portlets each role has available to personalize.
  - Disadvantages: Implementing portlet control increases maintenance.
  - Consider the business unit structure. Portlets roles could be slightly different; a portlet could be used for two or more roles. It may be necessary to think of a multi-level structure for the OBS. In this situation, grant Page – View rights and Portlet – View rights as illustrated in the following graphic:



Group: OBS Unit Access Rights (Group: All Participants)

OBS Unit Access Rights Filter

Below are this group's rights to object instances in specific OBS units.

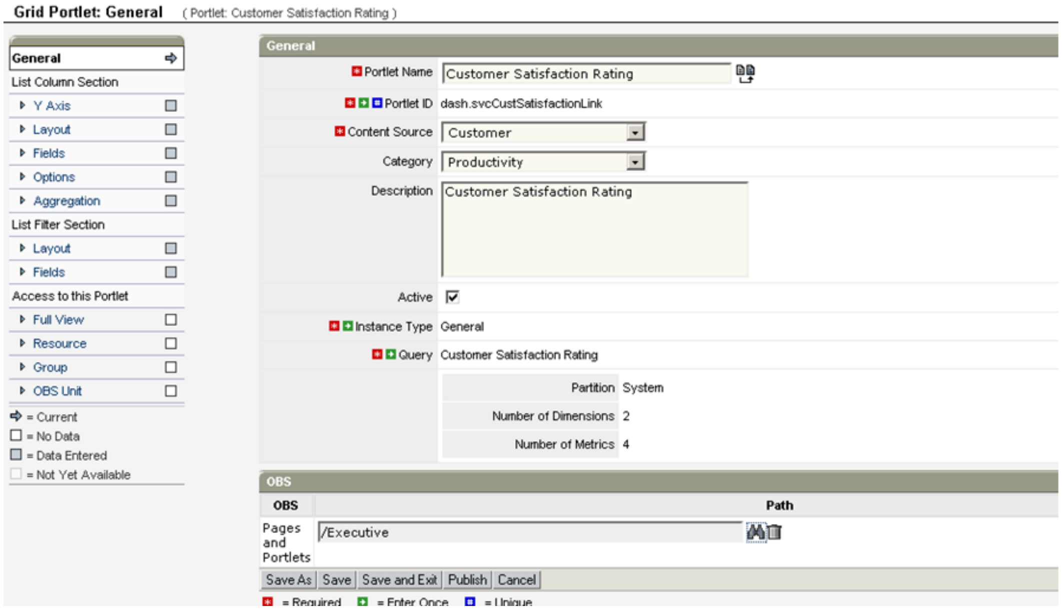
Access Right

OBS Unit

	Access Right	OBS Unit	OBS Association Mode
□	Portlet - View	Pages and Portlets:General	Unit and descendants
□	Page - View	Pages and Portlets:General	Unit and descendants

Total Results: 2

Categorize the portlets using an OBS Unit as illustrated in the following graphic:



Grid Portlet: General (Portlet: Customer Satisfaction Rating)

General

Portlet Name	Customer Satisfaction Rating
Portlet ID	dash.svcCustSatisfactionLink
Content Source	Customer
Category	Productivity
Description	Customer Satisfaction Rating
Active	☑
Instance Type	General
Query	Customer Satisfaction Rating
Partition	System
Number of Dimensions	2
Number of Metrics	4

OBS

OBS	Path
Pages and Portlets	/Executive

Appendix A: Licensing

Security and License Compliance

Access Rights are tightly linked to license compliance. Each specific Access Right in CA Clarity PPM is related to a License Type. By granting users Access Rights, you are granting them CA Clarity PPM licenses.

The Licensing model for CA Clarity PPM changed in 2008. Customers licensing the CA Clarity PPM since October of 2008 are most likely in the current license model. Customers that licensed the CA Clarity PPM before October 2008 may be in the previous license model.

If you are not sure of which license model applies to your company, contact your CA Clarity PPM Solution Strategist or CA Technologies Account Director.

User License Types in the Current Licensing Model

Following three possible user license types specific to CA Clarity PPM are available in the current license model:

Managers

Refers to the power users in CA Clarity PPM, who are allowed to use all the available functionalities.

Team Members

Refers to the average users in CA Clarity PPM, who are allowed a subset of functionalities such as entering time and publishing documents.

Enterprise Visibility Option (EVO) users (Optional package)

Refers to the users in CA Clarity PPM, who are allowed a smaller subset of functionalities that include viewing information and entering ideas and incidents for Demand Management.

Note: Not all contracts include this optional package. If you are not sure whether you have the EVO option licensed, contact your CA Clarity PPM Solution Strategist or CA Technologies Account Director.

Examples of the relationship between access rights and license types:

- You create a user and grant Ideas - Create access right. When you verify the License being used by that user, you see the Enterprise Visibility Option listed.
- If you grant this user Knowledge Store - Access, the Team Member License is used, as this access right is related to the Team Member license type.
- If you grant this user Project – Create access right, the Manager License is used, as this access right is related to the Manager License type.

User License Types in the Previous Licensing Model

In the previous license model, the following four user types were available:

Studio Developers

Refers to the power users in CA Clarity PPM, who are allowed to use all the available functionalities.

Creators

Refers to the second level in the hierarchy of users. These users manage projects, portfolios, resources, financials, and so on. They are named “Creators” because the Create access rights are linked to them. These users can create projects, new resources, new services, new portfolios, and so on. These users can also do whatever Participants can do.

Participants

Refers to the third level in the hierarchy of users. Participants can perform activities common to Project Participants such as entering time, participating in workflows, publishing documents. These users can also do whatever Viewers can do.

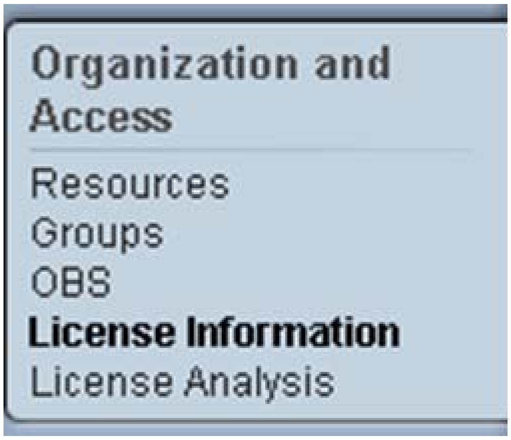
Viewers

Refers to the lowest level in the hierarchy of users. Viewers can view any information in the system but cannot change or create anything. The only exception is demand management functionality such as creating ideas or incidents.

How CA Clarity PPM Identifies Licenses Being Used

You do not assign a specific license type to a user, you assign access rights. The license type that is being used by that user is derived from the Access Rights granted to the user. To be in compliance with the CA Clarity PPM License Agreement, be careful when assigning Access Rights to CA Clarity PPM users.

CA Clarity PPM provides a set of portlets to allow you to manage your licenses and access rights. You can see these portlets in the License Information page, in the Organization and Access section of the Administration Tool.



Configure the License model used in your installation in the CA Clarity System Administration (NSA) service.

Note: For more information about how to use NSA, see the *CA Clarity PPM Installation Guide*.

License Information Portlets

The License Information Portlets can help you understand the relationship between the licenses, security and assist you with management of the user licenses. The portlets currently available and accessible in the Administration Tool are:

- User Count by License Type
- Rights by License Type

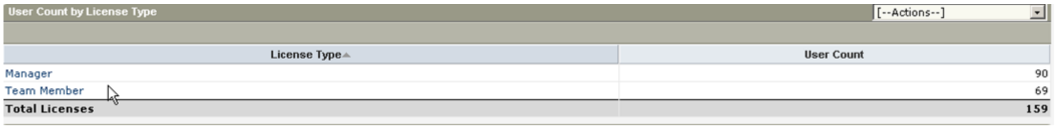
Other portlets are available by drilling down from the User Count by License Type portlet:

- User List by License Type
- Rights by User

Descriptions of the License Information Portlets and examples are provided below:

User Count by License Type

This portlet shows you how many licenses you are using for each license type. Click the name of the License Type to drill down in to the User List by License Type page.



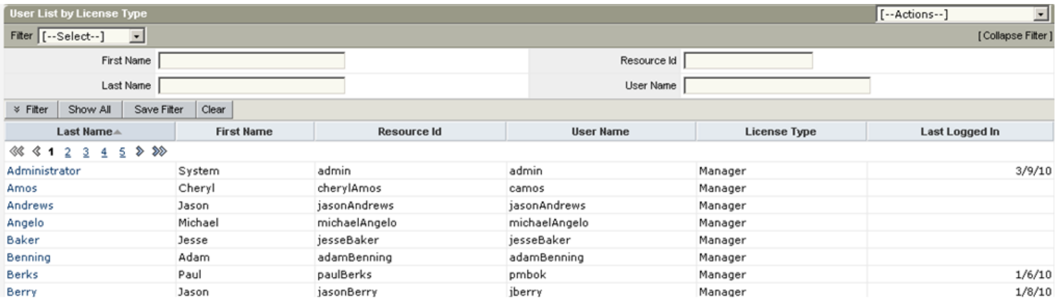
User Count by License Type

License Type	User Count
Manager	90
Team Member	69
Total Licenses	159

User List by License Type

This portlet shows you which users are consuming a specific license type, and the last login date for each user. This allows you to verify which users are actively being used and which are not.

Click the name of a user to drill down in to the Rights by User page. This is especially useful if you want to know why a specific user is consuming a license other than what is expected. For example, why is the user a Manager instead of a Team Member?

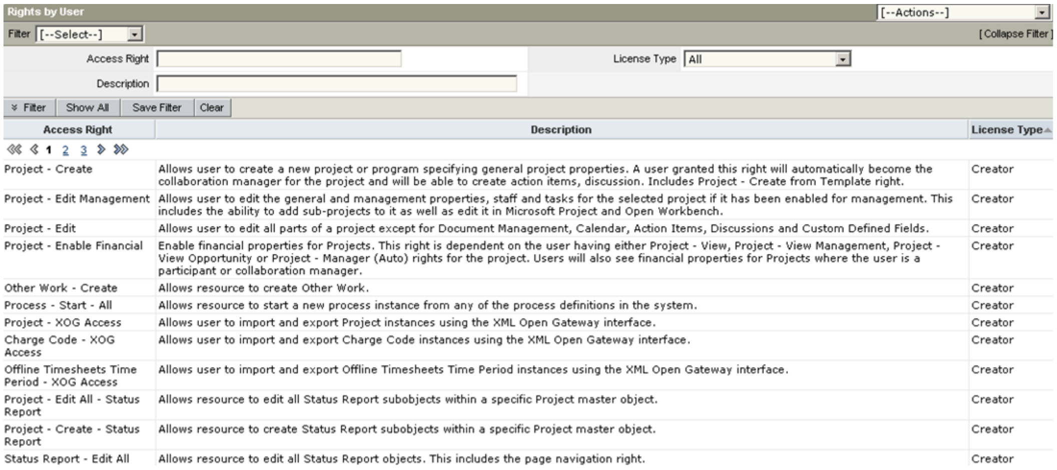


User List by License Type

Last Name	First Name	Resource Id	User Name	License Type	Last Logged In
Administrator	System	admin	admin	Manager	3/9/10
Amos	Cheryl	cherylAmos	camos	Manager	
Andrews	Jason	jasonAndrews	jasonAndrews	Manager	
Angelo	Michael	michaelAngelo	michaelAngelo	Manager	
Baker	Jesse	jesseBaker	jesseBaker	Manager	
Benning	Adam	adamBenning	adamBenning	Manager	
Berks	Paul	paulBerks	pmbok	Manager	1/6/10
Berry	Jason	jasonBerry	jberry	Manager	1/8/10

Rights by User

This portlet shows you the access rights that have been granted to a user, and the associated license type. If you see an access right that is not supposed to be there you can later remove the access right to correct the type of license that the user consumes.



Rights by User

Filter: [--Select--]

Access Right:

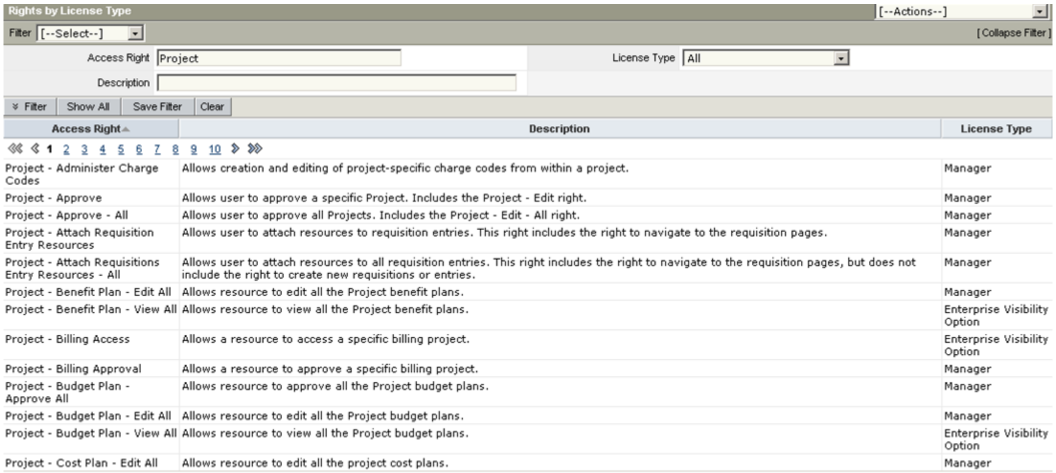
Description:

License Type: All

Access Right	Description	License Type
Project - Create	Allows user to create a new project or program specifying general project properties. A user granted this right will automatically become the collaboration manager for the project and will be able to create action items, discussion. Includes Project - Create from Template right.	Creator
Project - Edit Management	Allows user to edit the general and management properties, staff and tasks for the selected project if it has been enabled for management. This includes the ability to add sub-projects to it as well as edit it in Microsoft Project and Open Workbench.	Creator
Project - Edit	Allows user to edit all parts of a project except for Document Management, Calendar, Action Items, Discussions and Custom Defined Fields.	Creator
Project - Enable Financial	Enable financial properties for Projects. This right is dependent on the user having either Project - View, Project - View Management, Project - View Opportunity or Project - Manager (Auto) rights for the project. Users will also see financial properties for Projects where the user is a participant or collaboration manager.	Creator
Other Work - Create	Allows resource to create Other Work.	Creator
Process - Start - All	Allows resource to start a new process instance from any of the process definitions in the system.	Creator
Project - XOG Access	Allows user to import and export Project instances using the XML Open Gateway interface.	Creator
Charge Code - XOG Access	Allows user to import and export Charge Code instances using the XML Open Gateway interface.	Creator
Offline Timesheets Time Period - XOG Access	Allows user to import and export Offline Timesheets Time Period instances using the XML Open Gateway interface.	Creator
Project - Edit All - Status Report	Allows resource to edit all Status Report subobjects within a specific Project master object.	Creator
Project - Create - Status Report	Allows resource to create Status Report subobjects within a specific Project master object.	Creator
Status Report - Edit All	Allows resource to edit all Status Report objects. This includes the page navigation right.	Creator

Rights by License Type

This portlet shows what is the License Type associated to an Access Right. Use this portlet to verify that the Access Rights granted to a user are not violating the license type intended for that user.



Rights by License Type

Filter: [--Select--]

Access Right: Project

Description:

License Type: All

Access Right	Description	License Type
Project - Administer Charge Codes	Allows creation and editing of project-specific charge codes from within a project.	Manager
Project - Approve	Allows user to approve a specific Project. Includes the Project - Edit right.	Manager
Project - Approve - All	Allows user to approve all Projects. Includes the Project - Edit - All right.	Manager
Project - Attach Requisition Entry Resources	Allows user to attach resources to requisition entries. This right includes the right to navigate to the requisition pages.	Manager
Project - Attach Requisitions Entry Resources - All	Allows user to attach resources to all requisition entries. This right includes the right to navigate to the requisition pages, but does not include the right to create new requisitions or entries.	Manager
Project - Benefit Plan - Edit All	Allows resource to edit all the Project benefit plans.	Manager
Project - Benefit Plan - View All	Allows resource to view all the Project benefit plans.	Enterprise Visibility Option
Project - Billing Access	Allows a resource to access a specific billing project.	Enterprise Visibility Option
Project - Billing Approval	Allows a resource to approve a specific billing project.	Manager
Project - Budget Plan - Approve All	Allows resource to approve all the Project budget plans.	Manager
Project - Budget Plan - Edit All	Allows resource to edit all the Project budget plans.	Manager
Project - Budget Plan - View All	Allows resource to view all the Project budget plans.	Enterprise Visibility Option
Project - Cost Plan - Edit All	Allows resource to edit all the project cost plans.	Manager

Index