Deltek.

CER Security Setup

Costpoint Enterprise Reporting Administrator Series

Costpoint Enterprise Reporting Administrator Series: Costpoint Enterprise Reporting (CER) Security Setup

These steps should be completed by a Costpoint/CER Cloud Administrator for the Organization.

Introduction to CER Security

In Costpoint/CER there are a number of security settings available. This document details the options and how to set up security in Costpoint Enterprise Reporting.

Overview of Security

As the Administrator for CER you have already verified your status in the system and validated access to CER. In this activity you will set up security allowing users to have access to different features, views of information, and content.

Security Planning Template

When assigning License Types to individual CER users, administrators are encouraged to download and use the Security Planning Template. Each CER user can only be assigned to one license type. The template allows you to layout the number of licenses purchased and plan users assigned to each license. The template is also used as a guide/reference for planning, setting up, and recording security in CER. The Security Planning Template is not an uploadable file and is used only as a reference guide.
Later in this document there are instructions on how to use the template.

Security Defined

Costpoint Enterprise Reporting 7.2 Series offers many security features that have not been offered in previous versions of CER. There are three main types of security that can be applied, Model Security, Capability Security and Object Security. The chart below describes these.

Security Type	Description/Features
Capability Security	Capability Security, sometimes referred to as Product Security, utilizes the defined License Types to determine product capabilities available to an end user. Each CER user should be assigned to one CER License Type/User Role based on the functions they can perform. Types of product capabilities that are available through these License Types are as follows: • Interactive Viewer – This enables a user to interact with the report output, even without the report authoring tool. It includes sorting, filtering, aggregation, grouping, changing the data container type to chart, saving changes to a new report, and interacting with charts. • Dashboards – This enables a user to gain insight into the data through the use of interactive visualizations. • Interactive Report Authoring – This is the web-based tool that enables report writers and developers to construct multi-query reports. • Data Module – This provides users that are not efficient in Framework Manager, with limited web-based modeling capabilities to leverage data sets or blend data from existing packages. • Framework Manager – This is a metadata modeling tool for Cognos Analytics 11. • Administrator Console – This is used to perform tasks such as managing schedules or user accounts. It can also be utilized for customizing the user interface and product experience.

Security Type	Description/Features
Model Security	Model Security, sometimes referred to as Data or Row Security, is enabled to restrict the data that an end user can see. This is enabled or disabled through Manage CER Settings. Some important points to note about Model Security: • The default setting during implementation for Model Security is enabled. • If using Organization or Labor Suppression Security, this setting must be set to Enabled. • If enabled, an Organization Security Group must be assigned to each user in order to retrieve data from models that have data-level security, such as Projects or Project Planning. • This is an optional security feature and can be disabled through the Manage CER Settings. Within Model Security there are three types of security available: • Organizational Security – This type of Model Security limits user access to data based on the organization security established in Costpoint. ○ Costpoint Planning (Budgeting and Planning) will use the Organizational Security that is designated within the User Maintenance (MAU1) screen. These settings will coincide with the CER__PROJ_PLAN Object Security User Group. • Labor Suppression Security – This type of Model Security limits access to labor rates or costs at the employee level based on the labor suppression settings in Costpoint. This is typically used to protect information related to Labor (rates and costs) that should not be viewed by most users. • Project Security – This type of Model Security limits access to projects based on the assigned Project Manager in Costpoint. ○ For secured models in CER that use Costpoint Planning, Project and Org security will be leveraged based on the setting in the Planning Configuration Settings screen. In this screen you will have selected if project security is based on “Org ID” or “Project Budget Security”. This security applies only to the “Project Planning” model in CER. These settings will coincide with the CER__PROJ_PLAN Object Security User Group.

Security Type	Description/Features
Object Security	Object Security determines the content users can access. Content in CER 7.2 Series is delivered in the form of packages, reports, and dashboards and is based on the specific Costpoint Domains/Modules, examples of this content are Projects, Accounts Receivables, Accounts Payable, Billing, or General Ledger. These are all located within Team Content. Object Security utilizes User Groups based on Costpoint Domains. These User Groups are preconfigured. Some important points about Object Security: • A user must belong to at least one Object Security User Group in order to see any of the shared Deltek content available within Team Content. • A user may to be assigned to multiple Object Security User Groups. • When a user is assigned to an Object Security User Group they have access to all of the reports and models for those objects. ○ If a user is not assigned to an Object Security User Group, they should be setup as a CER__Consumer. This group only has access (read only) to content that is shared with them in the Company Content folder, which is managed by the administrator. **NOTE:** If a user is assigned to an object security group they can see all the standard reports and models that apply to that group of objects. If you don't think that a user should have access to all that content (which will include reports that aren't subject to data security) assign them as a CER__Consumer.

Capability Security

Capability Security utilizes the defined License Types to determine the product capabilities that are available to an end user.

License Types/User Roles

There are currently four different License Types that can be selected through Capability Security. Each of the defined roles below is included in the CER 7.2 Series Deployment:

- CER__CONSUMER (CER Consumer) – This user will have the least amount of rights and is someone who has read only rights for existing reports. Consumer Licenses are not part of cloud licensing, however, admins may, in some cases, use this type to limit the functionality of CER uses to only view dashboards instead of allowing the user to create or modify them. **NOTE**: This type of user takes a license.
- CER__USER (CER Basic User) – This user will have rights to run and interact with reports and also create and interact with dashboards.
- CER__ADV (CER Advanced User) – This user will have the CER__USER rights along with being able to create and share reports using the Interactive Authoring tool and Access to the Data Module.
- CER__ADMIN (CER Administrator) – In most cases, one Administrator license type is provided in a CER bundle. This user will have access to all CER product capabilities.

The License Type is an optional license not typically included in the CER bundles, but can be purchased:

CER__DEV (CER Developer) – This user will have all the capabilities of CER__ADV plus the use of Framework Manager allowing for custom data model creation. It is also important to note that you will need to create a service request to gain access to Framework Manager, as this tool is accessed through a separate login.

The table below displays the Product Capabilities that belong to each of the License Types:

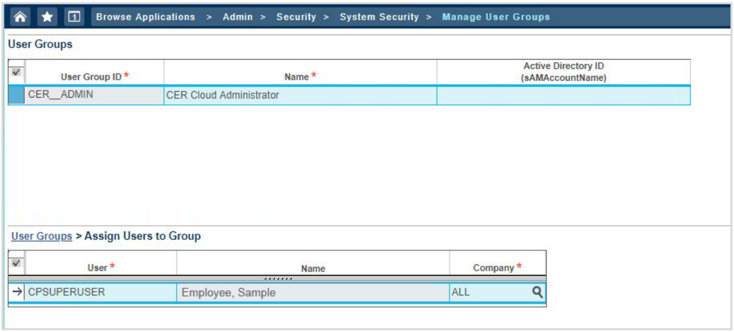
License Type/User Role	Product Capability					
	Interactive Viewer	Dashboard	Interactive Report Authoring	Data Module	Framework Manager	Admin Console
CER__ CONSUMER	X	View Only				
CER__USER	X	X				
CER__ADV	X	X	X	X		
CER__DEV	X	X	X	X	X	
CER__ADMIN	X	X	X	X	X	X

Assignment of CER Users to User Groups/Roles

Users will now need to be assigned to the User Groups located in the Admin Domain of Costpoint.

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>Navigate to: <b>Admin &gt; Security > System Security > Manage User Groups</b></td></tr>
<tr><td>2</td><td><b>Query</b> the User Group to add users to</td></tr>
<tr><td>3</td><td>Click on the subtask: <b>Assign Users to Group</b></td></tr>
<tr><td>4</td><td>Click: <b>New</b></td></tr>
<tr><td>5</td><td>Using the Security Planning Template as a guide, add Users and the company access.

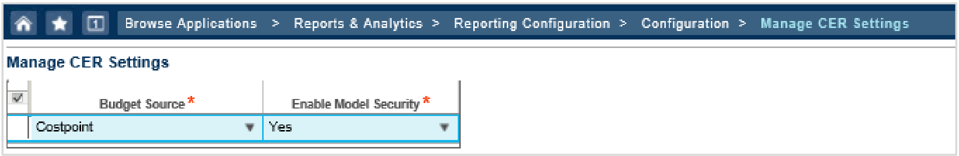
<b>NOTE</b>: The Security Planning Template is not an uploadable file to Costpoint and is used only as a reference guide.


Browse Applications > Admin > Security > System Security > Manage User Groups
User Groups
User Group ID * — Name * — Active Directory ID (sAMAccountName)
CER__ADMIN — CER Cloud Administrator
User Groups > Assign Users to Group
User * — Name — Company *
CPSUPERUSER — Employee, Sample — ALL</td></tr>
</table>

Model Security

Check to see if Model Security is applied. You can enable or disable Model Security.

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>
Navigate to: <b>Reports & Analytics > Reporting Configuration > Configuration > Manage CER Settings</b>

<b>Result:</b> The screen <b>Manage CER Settings</b> displays.

Browse Applications > Reports & Analytics > Reporting Configuration > Configuration > Manage CER Settings

Manage CER Settings
<table>
<tr><th>☑</th><th>Budget Source *</th><th>Enable Model Security *</th></tr>
<tr><td></td><td>Costpoint ▼</td><td>Yes ▼</td></tr>
</table>
<b>NOTE</b>: There are two columns with required entries, their headings are: <b>Budget Source</b> and <b>Enable Model Security</b>. The default settings are <b>Costpoint</b> and <b>Yes</b>.

<table>
<tr><td><b>Budget Source</b></td><td>This field is current not functional and should be ignored. This selection points to the source of data for your project budgeting reports in CER. The options are Costpoint or Budgeting and Planning.
Note: Currently this field only utilizes the default setting: Costpoint
Making any changes to this field will not impact the data that is used, best practice is to leave this set to Costpoint.</td></tr>
<tr><td><b>Enable Model Security</b></td><td>Options are: <b>Yes</b> or <b>No</b>
• <b>Yes</b> enables Model Security.
• <b>No</b> enables all access to for any data for any employee. This will enable the users to see all orgs, all project and all labor data in the secured models if they have been granted rights to those objects.</td></tr>
</table>
</td></tr>
<tr><td>2</td><td>
Follow the steps in the table below
<table>
<tr><th>To</th><th>Do This</th></tr>
<tr><td>Enable the Model Security</td><td>In the field, <b>Enable Model Security</b>, click the dropdown and select: <b>Yes</b></td></tr>
<tr><td>Disable the Model Security</td><td>In the field, <b>Enable Model Security</b>, click the dropdown and select: <b>No</b></td></tr>
</table>
</td></tr>
<tr><td>3</td><td>Click: <b>Save</b></td></tr>
</table>

Setting the Levels of Model Security

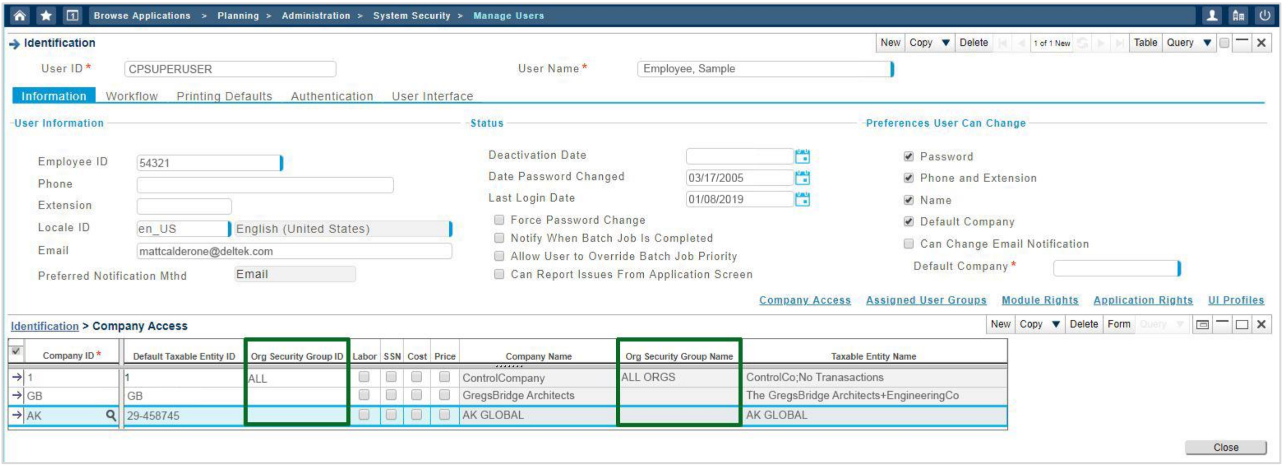
This section describes in more detail the definitions and different types of Model Security defined in the Costpoint System. It also provides information on where each system setting can be found.

Organizational Security – This type of Model Security limits user access to data based on organization security established in the Costpoint. Remember, if this type of security is turned on, a user MUST be assigned to an Org Security Group in Costpoint or they will not see any data. If org restrictions are not necessary for a specific user, it is recommended to setup a group that encompasses access to all organizations, e.g. “All Orgs”.

For secured models in CER that use Costpoint Planning, Project and Org security will be leveraged based on the setting in the Planning Configuration Settings screen. In this screen you will have selected if project security is based on “Org ID” or “Project Budget Security”. This security applies only to the “Project Planning” model in CER. These settings will coincide with the CER__PROJ_PLAN Object Security User Group.

Follow the steps in the table below to assign an Org Security Group ID in Costpoint, excluding Costpoint Planning.

Step	Action
1	Navigate to: **Admin > Security > System Security > Manage Users**
2	**Query** on the user.
3	Locate the field, **Org Security Group ID** and click the magnifying glass to select: the correct Org Security Group **Result:** The field Org Security Group Name populates automatically.



User ID * CPSUPERUSER

User Name * Employee, Sample

User Information

Employee ID 54321

Phone

Extension

Locale ID en_US English (United States)

Email mattcalderone@deltek.com

Preferred Notification Mthd Email

Status

Deactivation Date

Date Password Changed 03/17/2005

Last Login Date 01/08/2019

□ Force Password Change

□ Notify When Batch Job Is Completed

□ Allow User to Override Batch Job Priority

□ Can Report Issues From Application Screen

Preferences User Can Change

☑ Password

☑ Phone and Extension

☑ Name

☑ Default Company

□ Can Change Email Notification

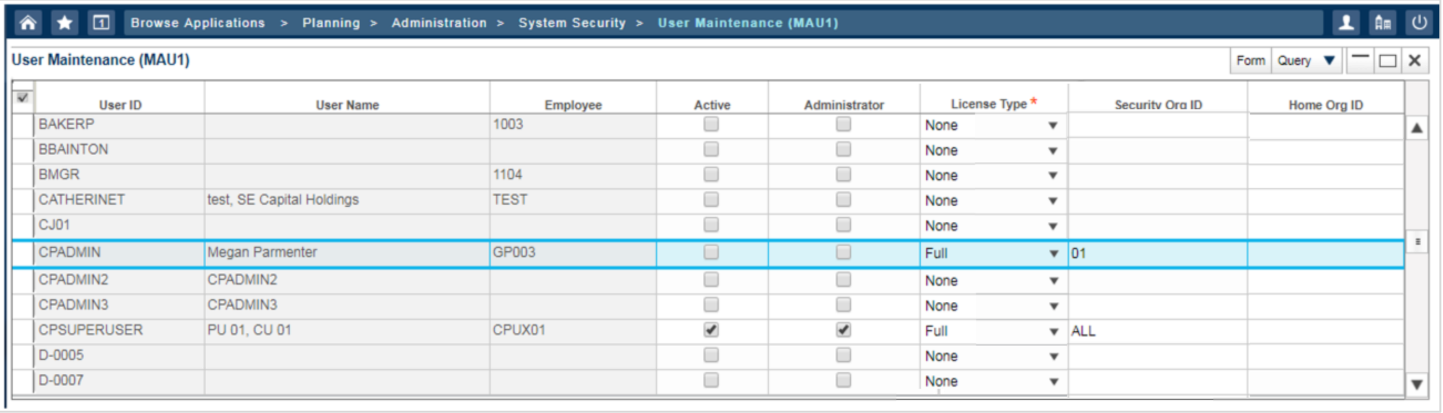
Default Company *

Company ID *	Default Taxable Entity ID	Org Security Group ID	Labor	SSN	Cost	Price	Company Name	Org Security Group Name	Taxable Entity Name
1	1	ALL	□	□	□	□	ControlCompany	ALL ORGS	ControlCo;No Tranasactions
GB	GB		□	□	□	□	GregsBridge Architects		The GregsBridge Architects+EngineeringCo
AK	29-458745		□	□	□	□	AK GLOBAL		AK GLOBAL

NOTE: Org Security Groups can be reviewed by navigating to **Admin > Security > Organizational Security > Manage Organization Security Groups**

Follow the steps in the table below to review Organization Security Setup within Costpoint Planning. Granting access to a Security Org ID will enable the user to have access to all projects that are owned by that organization:

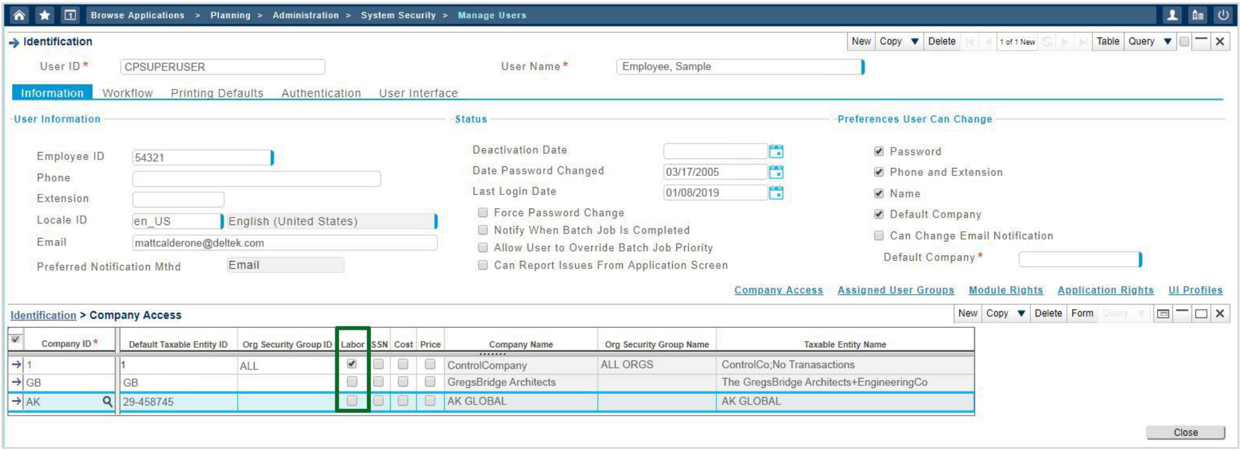
Step	Action
1	Navigate to: **Planning > Administration > System Security > User Maintenance (MAU1)**
2	**Query** on the User ID.
3	Locate the field Security Org ID. If no Security Organization has been populated in this field click on the magnifying glass to choose the correct Organization. **NOTE:** Users that are populated with Organizational Security in the Manage Users screen will have that value populate here by default, however, that value can be changed to define the Org Security specific to Planning. Items that are populated in this screen first DO NOT flow into the Manage Users screen within Administration.


Browse Applications > Planning > Administration > System Security > User Maintenance (MAU1)
User Maintenance (MAU1)
Form
Query

User ID	User Name	Employee	Active	Administrator	License Type *	Security Org ID	Home Org ID
BAKERP		1003	☐	☐	None		
BBAINTON			☐	☐	None		
BMGR		1104	☐	☐	None		
CATHERINET	test, SE Capital Holdings	TEST	☐	☐	None		
CJ01			☐	☐	None		
CPADMIN	Megan Parmenter	GP003	☐	☐	Full	01	
CPADMIN2	CPADMIN2		☐	☐	None		
CPADMIN3	CPADMIN3		☐	☐	None		
CPSUPERUSER	PU 01, CU 01	CPUX01	☑	☑	Full	ALL	
D-0005			☐	☐	None		
D-0007			☐	☐	None		

Labor Suppression Security - This type of Model Security limits access to labor rates or costs at the employee level based on the labor suppression settings in Costpoint. To enable Labor Suppression for a user:

Step	Action
1	Navigate to: **Admin > Security > System Security > Manage Users**
2	**Query** on the User ID.
3	Locate the **Labor Field** and click the checkbox if you wish to suppress the display of labor information for this user on a screen or report.



Identification

User ID *	CPSUPERUSER
User Name *	Employee, Sample

User Information

Employee ID	54321
Phone	
Extension	
Locale ID	en_US English (United States)
Email	mattcalderone@deltek.com
Preferred Notification Mthd	Email

Status

Deactivation Date	
Date Password Changed	03/17/2005
Last Login Date	01/08/2019

☐ Force Password Change
☐ Notify When Batch Job Is Completed
☐ Allow User to Override Batch Job Priority
☐ Can Report Issues From Application Screen

Preferences User Can Change

☑ Password
☑ Phone and Extension
☑ Name
☑ Default Company
☐ Can Change Email Notification

Default Company *

Identification > Company Access

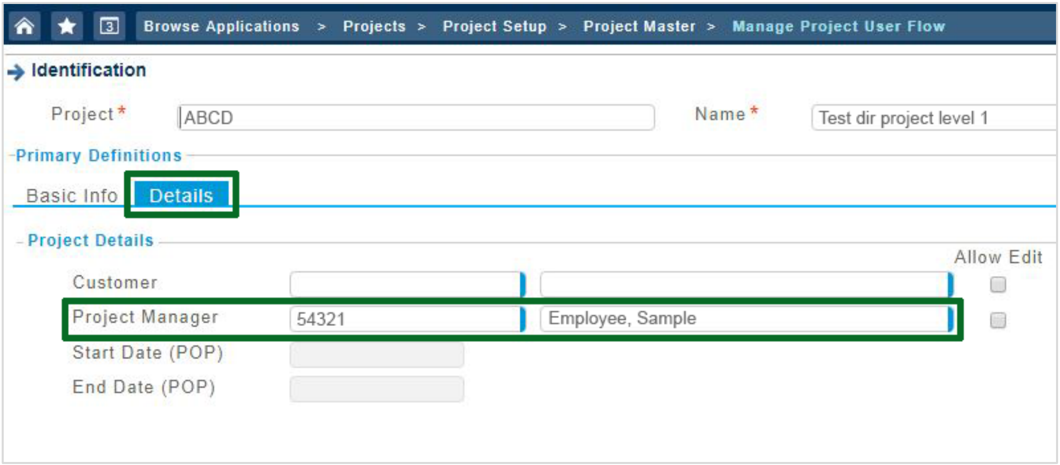
Company ID *	Default Taxable Entity ID	Org Security Group ID	Labor	SSN	Cost	Price	Company Name	Org Security Group Name	Taxable Entity Name
1	1	ALL	☑	☐	☐	☐	ControlCompany	ALL ORGS	ControlCo;No Tranasactions
GB	GB		☐	☐	☐	☐	GregsBridge Architects		The GregsBridge Architects+EngineeringCo
AK	29-458745		☐	☐	☐	☐	AK GLOBAL		AK GLOBAL

Project Security - This type of Model Security will limit access to projects based on the assigned Project Manager in Costpoint.

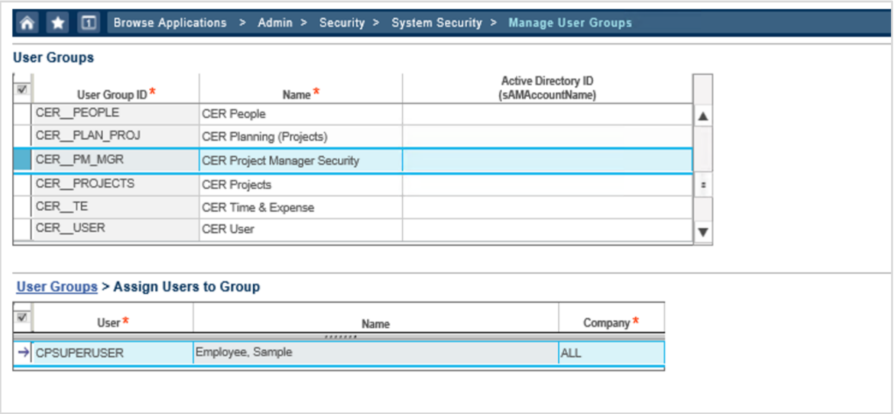
Costpoint Planning (Budgeting and Planning) will use the Project Security that has been designated in the Maintain Project Exclude Rights for Users (MAP10) screen. These settings will coincide with the CER__PROJ_PLAN Object Security User Group.

To enable Project Security for a user:

Step	Action
1	Navigate to: **Projects > Project Setup > Project Master > Manage Project User Flow**
2	**Query** on the specific project to assign.
3	Click on the tab: **Details**

Step	Action
4	In the field **Project Manager**: enter or select a Project Manager  Browse Applications > Projects > Project Setup > Project Master > Manage Project User Flow Basic Info Details Identification Project* ABCD Name* Test dir project level 1 Primary Definitions Project Details Allow Edit Customer □ Project Manager 54321 Employee, Sample □ Start Date (POP) End Date (POP)
5	Next, in order to limit the projects to only the projects that the Project Manager owns, the User must be assigned to the CER User Group CER Project Manager Security: **CER__PM_MGR** Navigate to: **Admin > Security > System Security > Manage Users Groups**
6	Locate the group: **CER__PM_MGR**
7	Click on the subtask: **Assign Users to Group**
8	Click: **New**

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>9</td><td>
Query or Enter the User to be added and select the company to which the rights apply.



Browse Applications > Admin > Security > System Security > Manage User Groups

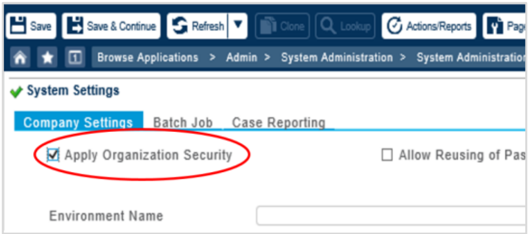
User Groups

<table>
<tr><th>User Group ID *</th><th>Name *</th><th>Active Directory ID (sAMAccountName)</th></tr>
<tr><td>CER__PEOPLE</td><td>CER People</td><td></td></tr>
<tr><td>CER__PLAN_PROJ</td><td>CER Planning (Projects)</td><td></td></tr>
<tr><td>CER__PM_MGR</td><td>CER Project Manager Security</td><td></td></tr>
<tr><td>CER__PROJECTS</td><td>CER Projects</td><td></td></tr>
<tr><td>CER__TE</td><td>CER Time &amp; Expense</td><td></td></tr>
<tr><td>CER__USER</td><td>CER User</td><td></td></tr>
</table>

User Groups > Assign Users to Group

<table>
<tr><th>User *</th><th>Name</th><th>Company *</th></tr>
<tr><td>CPSUPERUSER</td><td>Employee, Sample</td><td>ALL</td></tr>
</table>

NOTE: The option to implement Model Security in the CER Projects model without applying security in Costpoint is available. In order to do this navigate to **Admin > System Administration > System Administration Controls > Configure System Settings** and clear the checkbox marked **Apply Organization Security**.



Browse Applications > Admin > System Administration > System Administratio

System Settings

Company Settings | Batch Job | Case Reporting

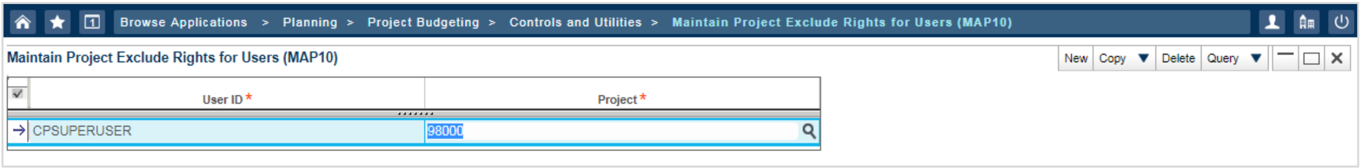
☑ Apply Organization Security

□ Allow Reusing of Pas

Environment Name
</td></tr>
</table>

Follow the steps in the table below to review/assign Project Security Setup within Costpoint Planning. Assigning exclude rights in this screen will prevent a user from accessing reporting for the assigned Project IDs:

Step	Action
1	Navigate to: **Planning > Project Budgeting > Controls and Utilities > Maintain Project Exclude Rights for Users (MAP10)**
2	All users currently assigned exclude rights will automatically populate in this screen. To add a user click the magnifying glass within the User ID field and choose the correct User ID.
3	Move to the Project field and click the magnifying glass to assign the project in which to exclude from the Users view.
4	Click **Save**.
5	Add Users and Projects as needed.


Browse Applications > Planning > Project Budgeting > Controls and Utilities > Maintain Project Exclude Rights for Users (MAP10)
New
Copy
Delete
Query

Maintain Project Exclude Rights for Users (MAP10)

User ID*	Project*
CPSUPERUSER	98000

Object Security

Determines the content users can access.

User Groups

The following User Groups are preconfigured within Costpoint for Object Security:

CER User Group	Description
CER__ACCTG – CER Reports	CER Accounting
CER__ACCT_ALL_SECURE	CER Accounting Secure
CER__ALL	CER ALL
CER__AR_SECURE	CER Accounting Receivable Secure
CER__CONTRACTS	CER Contracts
CER__CP_ADMIN	CER Costpoint Administration
CER__EXEC_SECURE	CER Executive Secure
CER__GL_SECURE	CER General Ledger Secure
CER__HR – CER Reports	CER Human Resources
CER__MATERIALS	CER Materials
CER__PEOPLE	CER People
CER__PLAN_PROJ	CER Planning (Projects)
CER__PLAN_PRJ_SECURE	CER Planning (Projects) Secure
CER__PM_MGR	CER Project Manager
CER__PROJECTS	CER Projects
CER__PROJ_SECURE	CER Projects Secure
CER__TE – CER	CER Time & Expense

The **Object Content table** below displays the individual Object Content assigned to each of the User Groups:

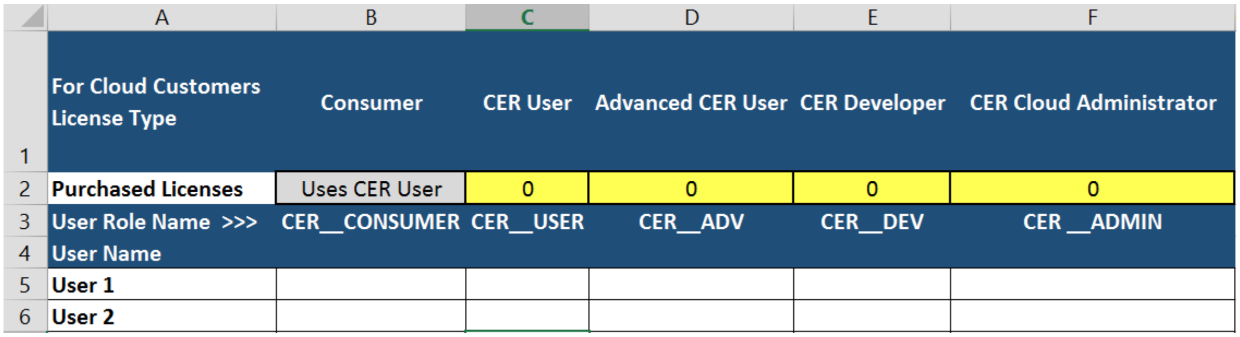
Object	CER Accounting	CER Accounting All Secure	CER Accounts Receivable Secure	CER General Ledger Secure	CER All	CER Contracts	CER Projects	CER Projects Secure	CER Planning (Projects)	CER Planning (Projects) Secure	CER Project Manager	CER People	CER Time & Expense	CER Materials	CER HR	CER CP Admin	CER Executive Secure
Team Content > *Packages* >																	
Accounts Receivable		●	●		●						●						●
Contracts Reporting					●	●											●
General Ledger		●		●	●												●
Project Analysis					●		●	●									
Project Planning Analysis					●				●	●	●						
Project Planning Reporting					●				●	●	●						
Project Reporting					●			●									●
Time and Expense TESS					●		●						●				
~Legacy Packages (CER 7.1.x)~ >																	
Accounts Payable CP	●				●												
Accounts Receivable CP	●				●												
Administration					●											●	
Basic Information CP	●				●		●					●	●	●	●		
Billing CP					●		●										
Costpoint Project Manufacturing					●									●			
Costpoint Shop Floor Time					●							●					
Fixed Assets	●				●												
General Ledger CP	●			●	●												
HR					●										●		
Labor CP					●							●					
Payroll					●										●		
Procurement CP					●									●			
Project Budgets					●				●								
Projects CP					●		●										
Purchasing CP					●									●			
Accounts Receivable		●	●		●						●						
Company content	●	●	●	●	●	●	●	●	●	●		●	●	●	●	●	●
Contracts					●	●											
Costpoint Enterprise Reporting	●				●		●		●			●	●	●	●	●	
Reports > Accounts Payable	●				●												
Reports > Accounts Receivable	●				●												
Reports > Basic Information	●				●		●					●	●	●	●		
Reports > Billing					●		●										
Reports > Drill Thru Only	●				●									●			
Reports > General Ledger	●			●	●												
Reports > Procurement					●									●			
Reports > Projects					●		●										
Reports > Purchasing					●									●			
Reports > TESS					●		●						●				
Costpoint Enterprise Reporting for Budgeting and Planning					●				●								
Costpoint Enterprise Reporting for Costpoint Administration					●											●	
Costpoint Enterprise Reporting for Fixed Assets	●				●												
Costpoint Enterprise Reporting for HR and Payroll					●										●		
Costpoint Enterprise Reporting for Project Manufacturing					●									●			
Costpoint Enterprise Reporting for Shop Floor Time					●							●					
CPSOX	●				●												
Executive					●												●
General Ledger		●		●	●												
ICS	●				●												
Planning					●				●	●	●						
Projects					●		●	●			●						
SOX Controls Reporting	●				●												
TESOX	●				●		●	●	●								

Set Up Capability Security

Using the Security Planning Template

The Security Planning template has two tabs: Capability Security and Object Security. Use these tabs to record the product capabilities that are available to an end user and determine the content users can access.

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>Open the template.</td></tr>
<tr><td>2</td><td>In row 2, enter the number of purchased licenses per License Type.



<table>
<tr><th></th><th>A</th><th>B</th><th>C</th><th>D</th><th>E</th><th>F</th></tr>
<tr><td>1</td><td>For Cloud Customers License Type</td><td>Consumer</td><td>CER User</td><td>Advanced CER User</td><td>CER Developer</td><td>CER Cloud Administrator</td></tr>
<tr><td>2</td><td>Purchased Licenses</td><td>Uses CER User</td><td>0</td><td>0</td><td>0</td><td>0</td></tr>
<tr><td>3</td><td>User Role Name >>></td><td>CER__CONSUMER</td><td>CER__USER</td><td>CER__ADV</td><td>CER__DEV</td><td>CER __ADMIN</td></tr>
<tr><td>4</td><td>User Name</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>5</td><td>User 1</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>6</td><td>User 2</td><td></td><td></td><td></td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>3</td><td>In Column A, enter the names of the people that will have CER licenses.

<b>NOTE</b>: Entries will automatically copy to the second tab: <b>Object Security</b></td></tr>
<tr><td>4</td><td>In the row/column for the type of user, enter an <b>X</b>.

<b>NOTE</b>: As you make entries the Count and Licenses Remaining will automatically update.</td></tr>
</table>

Notes about Object Security tab. A user:

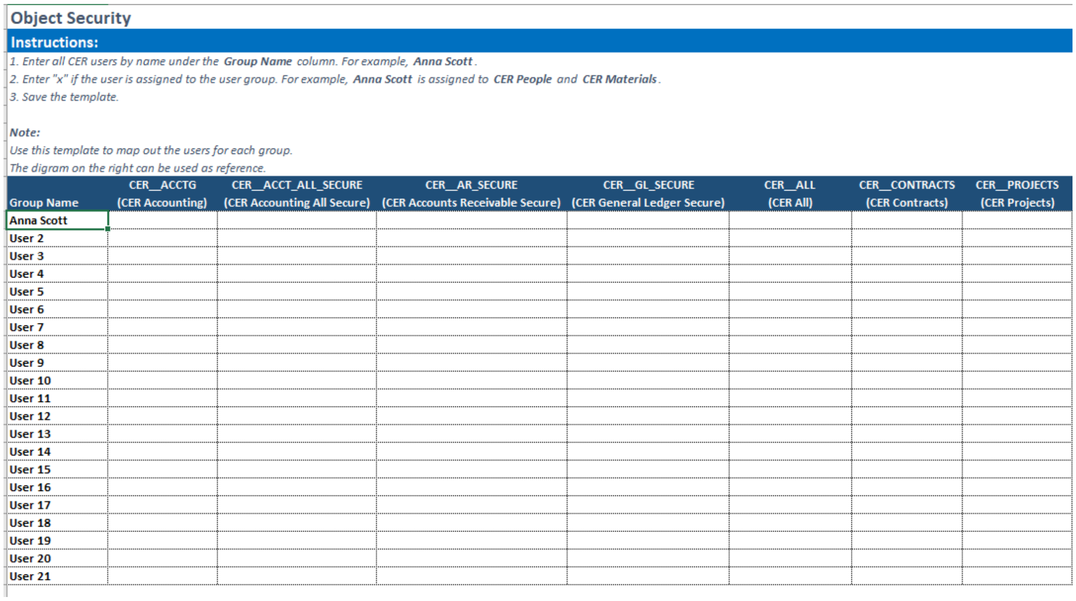
- Must belong to at least one group
- Can belong to multiple groups
- Should belong to at least one group except CER__CONSUMER
- A user with the CER__CONSUMER role should not belong to any domain group.

When you assign Object Security User Groups to individual CER users, administrators are encouraged to use the Security Planning Template. This template allow the admins map out the users for each group. This template can be downloaded from the Cloud Release Notes Hub or accessed via the following link: https://education.deltek.com/web/rsl/costpoint/cer/deltekcostpointenterprisereporting723securityplanningtemplate.xlsx

Follow the steps in the table below to record your entries for Object Security.

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>In the template, click the tab: <b>Object Security</b></td></tr>
<tr><td>2</td><td>If necessary, in the first column, enter the name of the user.

<b>NOTE</b>: The default setting for the template is to copy the user names from the first tab: <b>Capability Security</b>



Object Security

Instructions:

1. Enter all CER users by name under the **Group Name** column. For example, **Anna Scott**.
2. Enter "x" if the user is assigned to the user group. For example, **Anna Scott** is assigned to **CER People** and **CER Materials**.
3. Save the template.

Note:
Use this template to map out the users for each group.
The digram on the right can be used as reference.

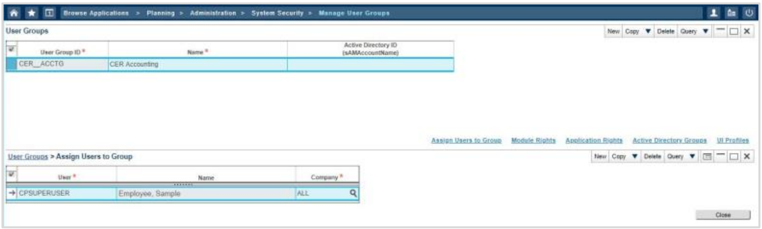
<table>
<tr><th></th><th>CER__ACCTG</th><th>CER__ACCT_ALL_SECURE</th><th>CER__AR_SECURE</th><th>CER__GL_SECURE</th><th>CER__ALL</th><th>CER__CONTRACTS</th><th>CER__PROJECTS</th></tr>
<tr><th>Group Name</th><th>(CER Accounting)</th><th>(CER Accounting All Secure)</th><th>(CER Accounts Receivable Secure)</th><th>(CER General Ledger Secure)</th><th>(CER All)</th><th>(CER Contracts)</th><th>(CER Projects)</th></tr>
<tr><td>Anna Scott</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>User 2</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>User 3</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>User 4</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>User 5</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>User 6</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>User 7</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>User 8</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>User 9</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>User 10</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>User 11</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>User 12</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>User 13</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>User 14</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>User 15</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>User 16</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>User 17</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>User 18</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>User 19</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>User 20</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>User 21</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>3</td><td>Based on the desired Module access, place an <b>X</b> in the appropriate cell.

<b>NOTE:</b> See the Object Content Table for role capability</td></tr>
<tr><td>4</td><td><b>Save</b> the template for later reference.</td></tr>
</table>

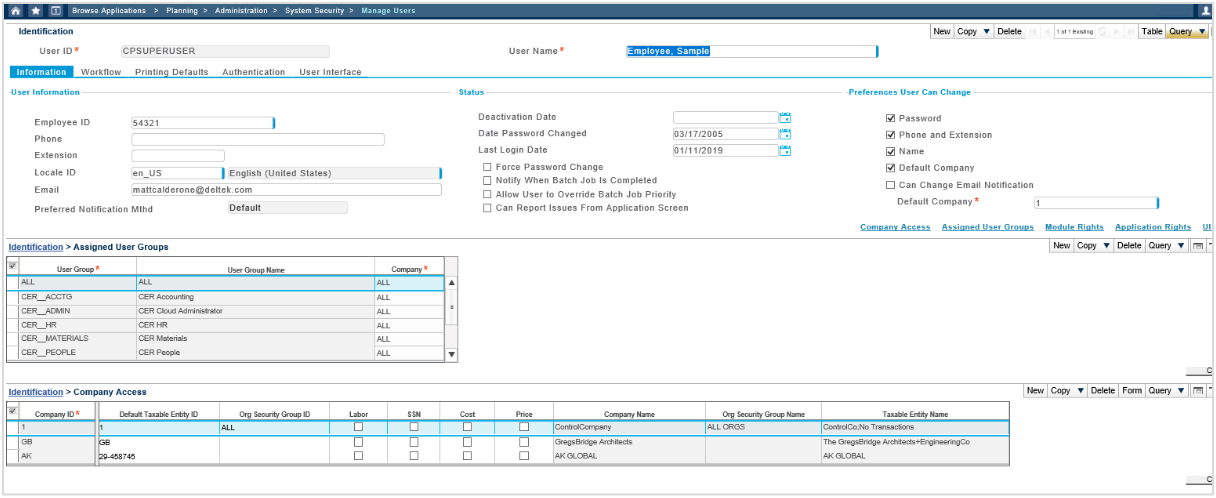
Assignment of CER Users (Manage User Groups or Manager Users)

Users are assigned in the Admin Domain of Costpoint. This can be done in two different ways depending on the number of entries, through Manager User Groups or through Manage Users.

Manage User Groups - This is used to add multiple users at one time (i.e. initial company set up).

Step	Action
1	In Costpoint, navigate to: **Admin > Security > System Security > Manage User Groups**
2	**Query** for the User Group.
3	Click on the subtask: **Assign Users to Group**
4	Click: **New**
5	Using the Security Planning Template as a guide, add users and the company. **NOTE:** The Security Planning Template is not an uploadable file to Costpoint and is used only as a reference guide.  Browse Applications > Planning > Administration > System Security > Manage User Groups New Copy Delete Query Assign Users to Group Module Rights Application Rights Active Directory Groups UI Profiles Close User Groups User Group ID * / Name * / Active Directory ID (sAMAccountName) CER__ACCTG / CER Accounting / User Groups > Assign Users to Group User * / Name / Company * CPSUPERUSER / Employee, Sample / ALL

Manage Users - This is used to add individual users, one at a time (i.e. new hire is assigned to CER).

Step	Action
1	In Costpoint, navigate to: **Admin > Security > System Security > Manage Users**
2	**Query** the User to add User Groups.
3	Click on the subtask: **Assigned User Groups**
4	Click: **New**
5	Use the Security Planning Template as a guide to add Users to User Groups and the company. **NOTE**: The Security Planning Template is not an uploadable file to Costpoint and is used only as a reference guide. 

Browse Applications > Planning > Administration > System Security > Manage Users
New | Copy ▼ | Delete | 1 of 1 Existing | Table | Query ▼
Information | Workflow | Printing Defaults | Authentication | User Interface
Company Access | Assigned User Groups | Module Rights | Application Rights | UI
New | Copy ▼ | Delete | Query ▼
New | Copy ▼ | Delete | Form | Query ▼

Identification

User ID* CPSUPERUSER

User Name* Employee, Sample

User Information

Employee ID 54321

Phone

Extension

Locale ID en_US English (United States)

Email mattcalderone@deltek.com

Preferred Notification Mthd Default

Status

Deactivation Date

Date Password Changed 03/17/2005

Last Login Date 01/11/2019

□ Force Password Change

□ Notify When Batch Job Is Completed

□ Allow User to Override Batch Job Priority

□ Can Report Issues From Application Screen

Preferences User Can Change

☑ Password

☑ Phone and Extension

☑ Name

☑ Default Company

□ Can Change Email Notification

Default Company* 1

Identification > Assigned User Groups

User Group*	User Group Name	Company*
ALL	ALL	ALL
CER__ACCTG	CER Accounting	ALL
CER__ADMIN	CER Cloud Administrator	ALL
CER__HR	CER HR	ALL
CER__MATERIALS	CER Materials	ALL
CER__PEOPLE	CER People	ALL

Identification > Company Access

Company ID*	Default Taxable Entity ID	Org Security Group ID	Labor	SSN	Cost	Price	Company Name	Org Security Group Name	Taxable Entity Name
1	1	ALL	□	□	□	□	ControlCompany	ALL ORGS	ControlCo;No Transactions
GB	GB		□	□	□	□	GregsBridge Architects		The GregsBridge Architects+EngineeringCo
AK	29-458745		□	□	□	□	AK GLOBAL		AK GLOBAL

SUMMARY

In summary, Deltek provides a template to record, store, and reference user security level/access information. The security setup in Costpoint allows/denies access to features, views, and content through Capability and Object Security. In the next step the Administrator sets up the reporting period and then validates/tests users' roles and access to desired content in CER.