Deltek

Deltek Costpoint Enterprise Reporting 7.2.3

Cloud Setup Guide

October 21, 2019

While Deltek has attempted to verify that the information in this document is accurate and complete, some typographical or technical errors may exist. The recipient of this document is solely responsible for all decisions relating to or use of the information provided herein.

The information contained in this publication is effective as of the publication date below and is subject to change without notice.

This edition published October 2019.

Contents

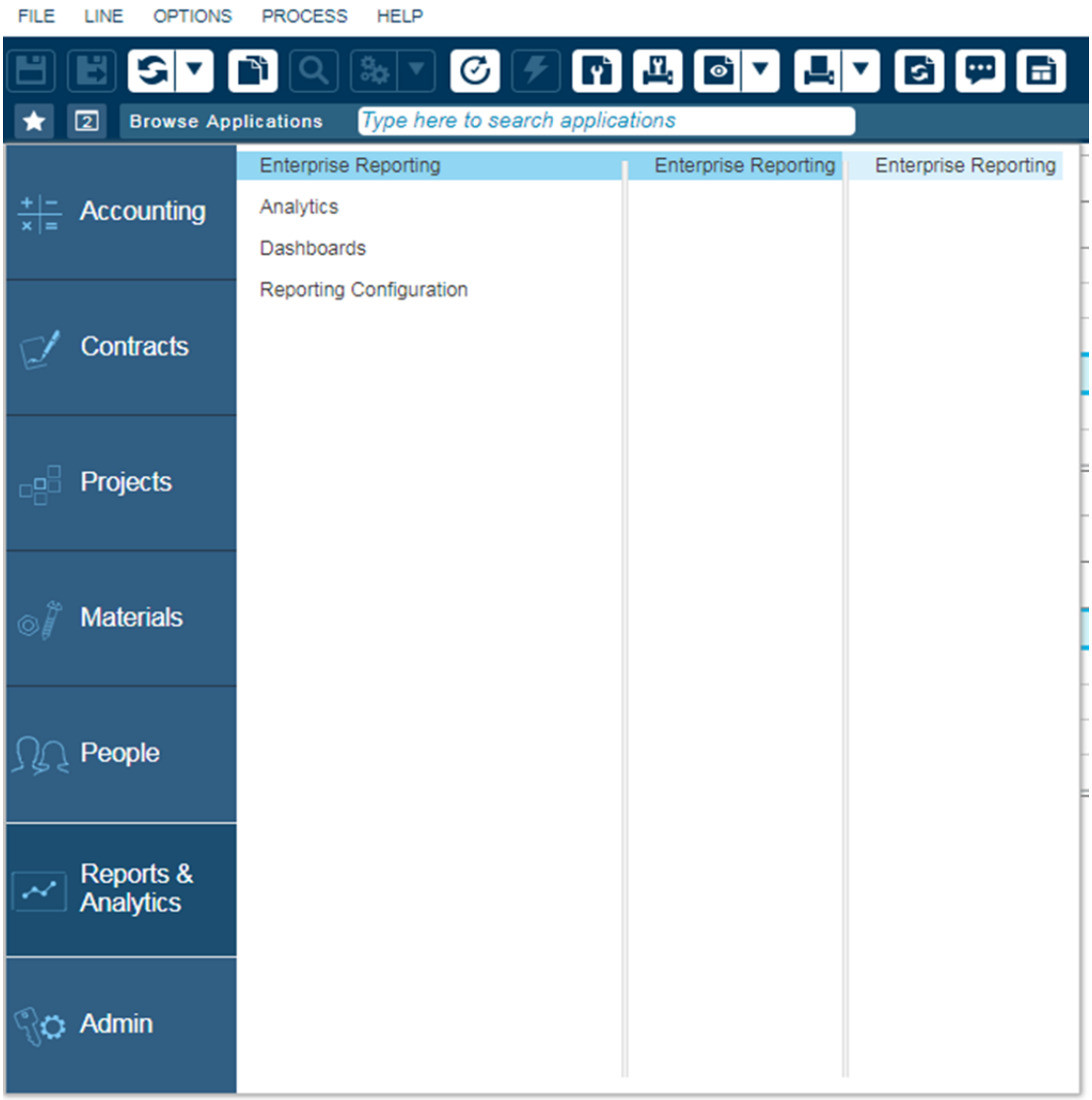
About this Guide

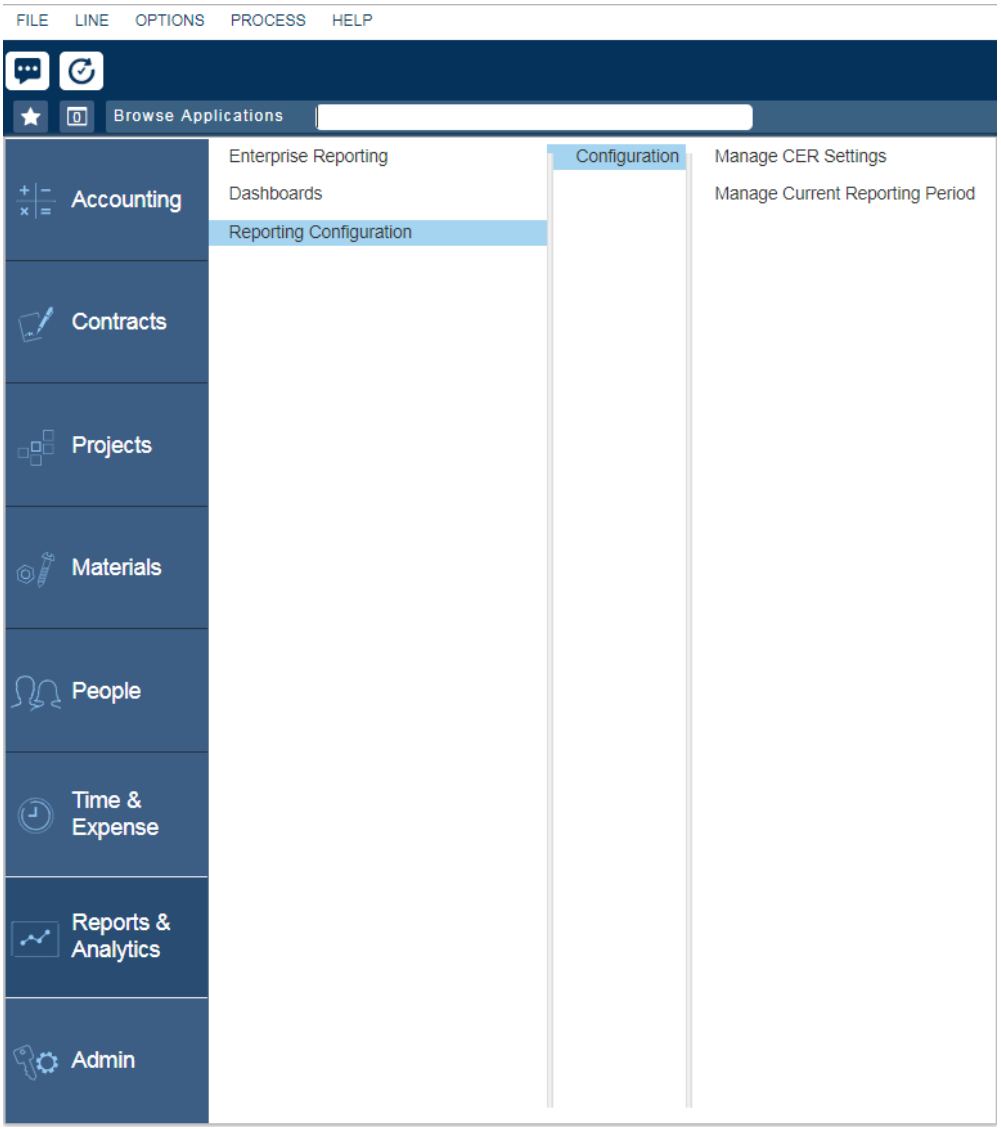
Welcome to the Costpoint Enterprise Reporting 7.2.3 Setup Guide for Costpoint Cloud Customers.

This guide is used after you receive administrative rights to CER and will walk you through the initial setup of CER so your environment is secured before you allow users into CER to run and create reports and Dashboards and leverage the built-in security features in CER.

Prerequisites

Before you can complete the procedures described in this guide, you (logged in as your Costpoint Administrator) should have received Costpoint Access from Deltek and access to the Enterprise Reporting application (ERCOGNOS), Manage CER Settings (BIMCERSETTINGS), and Manage Current Accounting Period (BIMRPTCURPD).




FILE
LINE
OPTIONS
PROCESS
HELP
Browse Applications
Accounting
Contracts
Projects
Materials
People
Time & Expense
Reports & Analytics
Admin
Enterprise Reporting
Dashboards
Reporting Configuration
Configuration
Manage CER Settings
Manage Current Reporting Period

Overview

In the post provisioning phase, we explain the new security design and how to set up your users to establish the appropriate security settings for your organization. The steps in the setup phase are:

- **Step 1:** Check the Model Security Configuration
- **Step 2:** Complete the Capabilities Security Template
- **Step 3:** Complete the Object Security Template
- **Step 4:** Complete the Security Template for the CER Project Manager Group
- **Step 5:** Assign the Users to the Costpoint User Groups
- **Step 6:** Set Up Current Reporting Period
- **Step 7:** Validate User Groups
- **Step 8:** Have Users Run and Validate Reports

Overview of CER Security

There are different types of data security that you can apply in Costpoint Enterprise Reporting 7.2.3.

The different types of security that will be addressed in this guide include:

1. **Capability Security**: This type of security utilizes user roles to determine the product capabilities that are available to an end user. For example, does this end user create reports or dashboards or simply run reports that were created by others?
2. **Object Security**: This type of security determines what content an end user can see. User groups based on Costpoint domains are used to establish content security. For example, should the end user be able to access HR, Project, or Accounting type reports?
3. **Model or Row Level Security**: This type of security is enabled in order to restrict the data that an end user can see by utilizing settings in Costpoint and Costpoint Planning.

Step 1: Check the Model Security Configuration

The Model Security is enabled as default. If you do not want to apply it, you can disable the Model Security in Costpoint. Note that this setting applies only to data security for Organization and Labor suppression security; both object security and capability security will apply whether the security is set on or off. The best practice is to keep the model security on.

> **Note:** Skip this procedure if you want to use Model Security for your CER implementation.

> **Note:** If Model Security is set to **Yes**, you must have an org security group assigned to each user or they will not be able to retrieve any data in the models that have data-level security (Projects, Project Planning). See Special Topics for information about setting up org security.

To disable Model Security:

1. Log in to Costpoint and launch the Manage CER Settings (BIMCERSETTINGS) screen (**Reports and Analytics** » **Reporting Configuration** » **Configuration** » **Manage CER Settings**).
2. Select **No** in the **Enable Model Security** drop-down list.

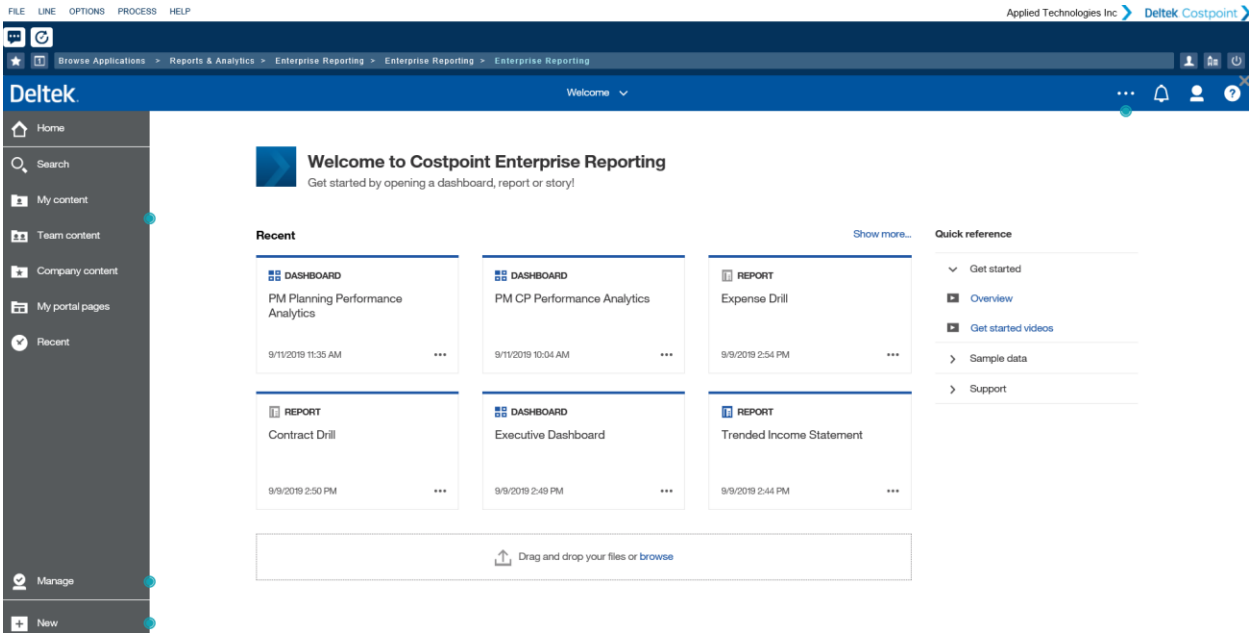
   > **Note:** If you select **No**, it is only Model Security that is disabled. Capability and Object Security are still in place in CER.

3. Click **Save**.

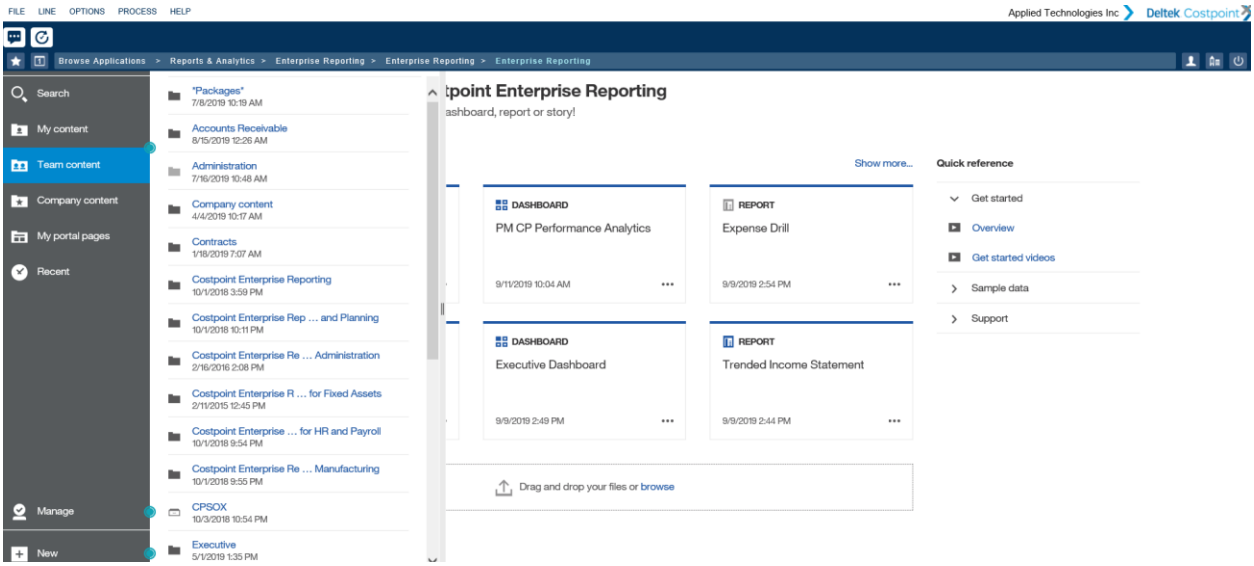
Assign CER Rights to the Administrator

In order to access CER, the Administrator will need to be assigned to CER groups in Costpoint Security, It is recommended that the Administrator assign themselves initially to CER__Admin and then CER__ALL.

The Administrator should then log in to Enterprise Reporting to make sure you can access the initial Enterprise Reporting Welcome Screen.

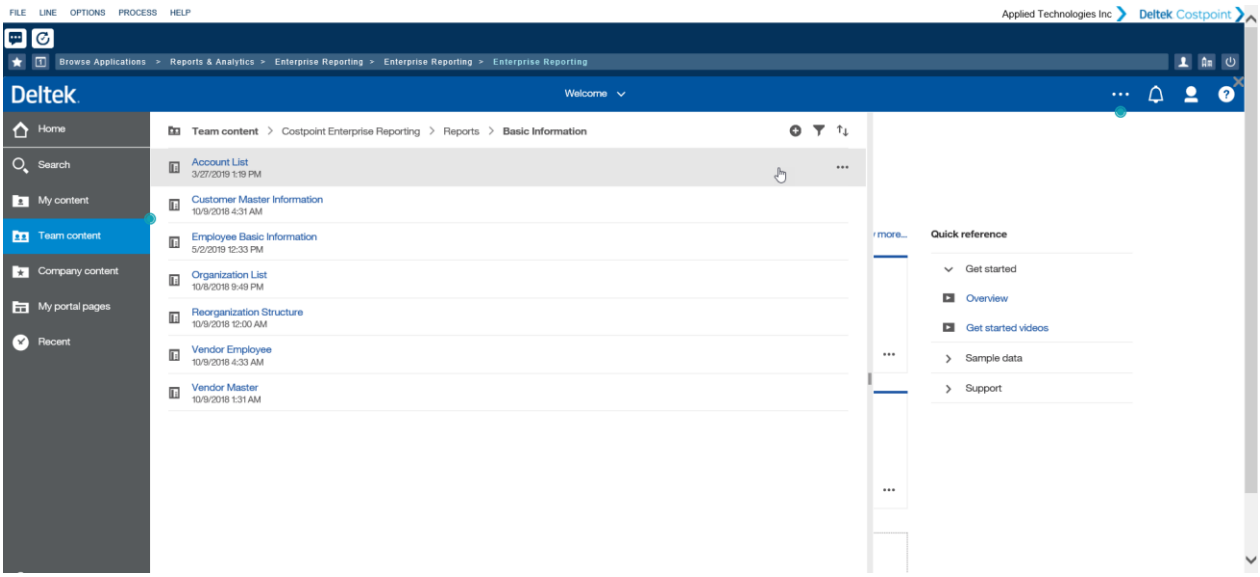


Then, click the Team content folder, and you should see the full folder structure.

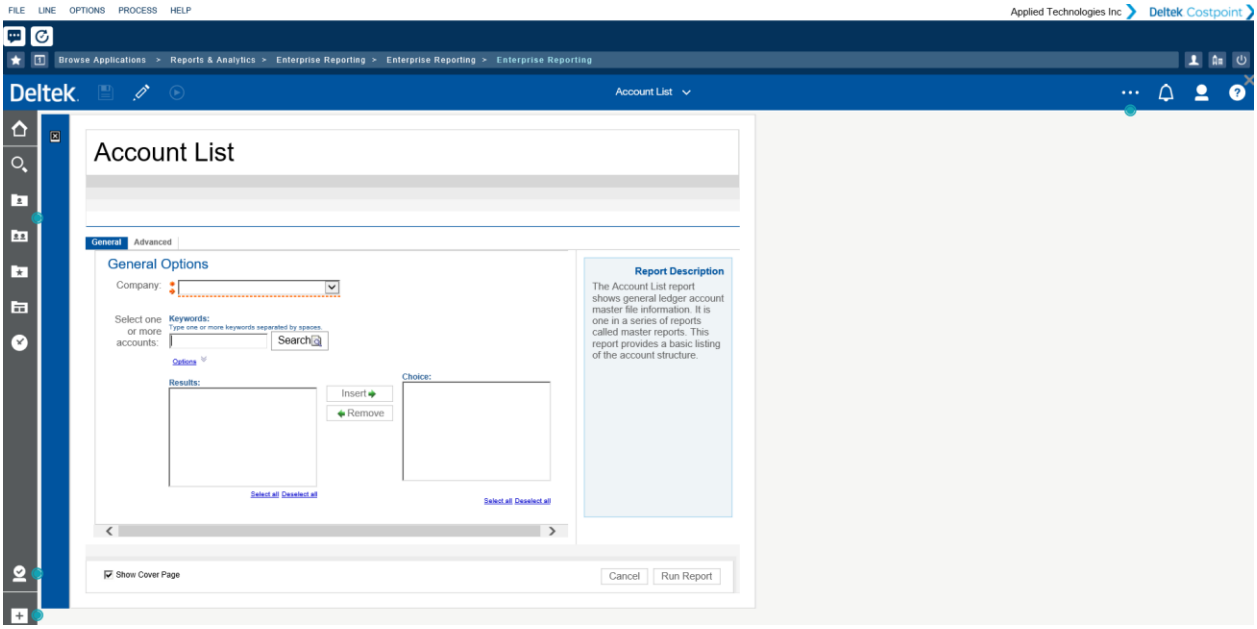


Then, run a report to ensure that you can access Costpoint Data. Here is how you can run an Account List Report:

First, navigate to the report.



Then, select the **Company** from the Prompt Page and click **Run Report**. The resulting report will show your account structure and validates you are connecting to your Costpoint data.



Now, you are ready to add functional users for Capabilities, Object, and PM Security, where applicable. There is a spreadsheet that accompanies the documentation that makes it easier to set up your user.

Capability Security

For each CER user role, a set of capabilities is assigned that designates the secure features or functions that an end user can perform.

There is a CER user role included in your deployment for each Deltek license type. The table below displays the key functions available with each of our licenses. (For a more detailed list of capabilities by role, see Special Topic 3.)

CER User Role Capabilities

Component	CER__CONSUMER*	CER__USER	CER__ADV	CER__DEV	CER__ADMIN
Interactive Viewer	X	X	X	X	X
Dashboard	View Only	X	X	X	X
Interactive Report Authoring			X	X	X
Data Module			X	X	X
Framework Manager				X**	X
Administration Console					X

* Consumer licenses are not part of cloud licensing; however, administrators might want to limit the functionality of some CER users to only view dashboards and not be able create or modify them.

** If you own CER Developer licenses, you will need to create a service request to get access to Framework Manager since FM is accessed through a separate login.

License Types

- Consumer (CER__CONSUMER): This user has the least rights, basically someone who can only run and interact with existing reports. While you may not own this type of license and have CER users instead, you might want to limit the capabilities for some individuals who you don't want to access or create dashboards.
- CER User (CER__USER): This user is someone who can run and interact with reports and can also interact and create dashboards.
- Advanced CER User (CER__ADV): In addition to the capabilities of the CER user, this type of user can create and share reports using interactive authoring and access the data module.
- CER Developer (CER__DEV): This type of user is not included in the typical CER bundles but can be purchased separately. In addition to all the capabilities of the Advanced CER user, a developer can use Framework Manager, which allows for custom data model creation.
- CER Administrator (CER__ADMIN): Typically, one Administrator license is provided in a CER bundle. This user has access to all CER capabilities.

Every CER user should be assigned to one CER user role based on the functions they can perform and the license purchased. The Security Planning Template has been provided for planning your capability security to help ensure license compliance. This Excel template can be downloaded from the Cloud Release Notes Hub.

For initial setup, you might not want to set up every user versus a sample of users who will be initially testing the system; you can always go back and add other users later.

Interactive Viewer enables a user to interact with the report output (even without report authoring capabilities). With interactive viewer, a user can:

- Change the sort order of a data container
- Set or edit filters
- Change the aggregation
- Group a column
- Change the type of a data container, that is, to a chart
- Save the changes as new report
- Interact with charts

Dashboards help you gain insight into your data at a glance through the use of interactive visualizations that can be arranged on one or more tabs.

Interactive Report Authoring is a web-based report authoring tool that enables developers to construct professional multi-query reports.

Data Module allows some limited web-based modeling capabilities allowing users (without Framework Manager expertise) to leverage data sets or blend data from existing packages.

Framework Manager is a metadata modeling tool for Cognos Analytics 11.

Administrator Console is used to perform tasks such as managing schedules and user accounts, and customizing the product experience and user interface

Step 2: Complete the Capabilities Security Template

The Capabilities Template is part of the Security Planning Template which is included in the documentation for this release.

To complete the Capabilities Security Template:

1. Launch the Security Planning Template and open the Capabilities Security tab.
2. Enter the number of licenses purchased by license type.
3. List all CER users by name.
4. Designate the role or license each user belongs to.
5. Save the completed template for reference later.

Object Security

Deltek delivers content in the form of packages, reports, and dashboards organized in folders under **Team Content**.

This content comes secured using CER user groups included. The user groups are based on Costpoint domains. The table below describes the user groups that have permissions to the objects in the Deltek content. The permissions at the parent folder or package will apply to any content contained within.

For example, the **Team Content** » **General Ledger** folder, which is new for CER 7.2.3, contains a subfolder for reports created from information in the General Ledger module. Any user assigned to the CER General Ledger Secure user group will be able to see all this content as indicated below.

The permissions for all Deltek folders are set as 'RUN only' to prevent changes or modifications to the pre-established value add, which ensures a smoother upgrade path in the future.

Customization of the Deltek content should be saved in another folder. For cloud customers, the customized Deltek content should be saved in their “Company content” folder.

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	•				•												

A user must belong to at least one of these groups in order to see any of the shared Deltek content that will appear in Team Content. A single user can be assigned to multiple groups. Use the Security Planning Template to plan which objects a user should have access to. If a user is assigned to one of these groups, they have access to all the reports and models for those objects. Please consider this before adding someone to one of the Object groups.

If a user is not assigned to any of the Object groups, he or she will only see content that is shared in the “Company content” folder. This folder is managed by the administrator or other users designated by the

administrator who can give rights to users or user groups to copies of dashboards/reports or custom dashboards/reports. So if you assign a user as a consumer, they won't see any content out of the box, which assures the Administrator that the consumers won't see any reports or dashboards that they don't want them to see.

Step 3: Complete the Object Security Template

The Object Security tab is part of the Security Planning Template which is part of the documentation for this release.

To complete the Object Security template:

1. Launch the Security Planning Template and open the Object Security tab.
2. List all CER users by user ID, name, and company.

   > **Note:** You can add users to all the groups and leave the CER__PM_MGR column for now. You will use this column in the **Step 4: Complete the Security Template for the CER Project Manager Group** section.

3. Designate the user group each user belongs to.
4. Save the completed template for reference later.

Model or Row Level Security

This security could also be called data security as it limits the data that is available to an end user based on Costpoint and Costpoint Planning settings.

> **Note:** Model/Row Level Security only applies to the Models/Reports/Dashboards contained in the Projects and Planning folders.

There are three aspects of model or row level security.

1. **Labor Suppression**: Restricts the ability to see labor rates and dollars at the employee level using the labor suppression flag settings in Costpoint. In CER, the rate/cost of employees are hidden in reports when Labor Suppression is in use. See Special Topic 1 for how to leverage this capability.
2. **Organization Security**: Restricts data based on the user's organization rights established in Costpoint or Costpoint Planning. In this type of security, the project data for the owning organization are secured instead of the performing organization. If Organization Security is not established in Costpoint or Costpoint Planning, CER models will not be able to restrict data by organization or company.

   For the Projects Model, Costpoint Organization Security is enforced. If you are not planning on using this type of security, not setup or changes are required. See Special Topic 1 for more information.

   For the Planning model, CER uses the Organization Security information from the Planning setup. See Special Topic 2 for more information.

   > **Note:** Multi-company security for Costpoint and Costpoint Planning is not enforced in CER.

3. **Project Security**: Restricts project data.

In the Planning folder, there is no specific capability for project security; however, organization security and project exclusion can, in effect, limit what a user sees relating to projects. See Special Topics for more details on setting up security in Planning.

To restrict Project access in the Projects folder to those projects where the user is set up as Project Manager, you will simply need to assign them to the CER__PM_MGR. In order to offer some project security options in CER, the assigned project manager of the project is used to determine project rights.

> **Note:** Project Manager Security only shows the project WBS elements where they are assigned as PM, so if there are multiple PMs assigned to a single project structure, those PMs will not see the entire project.

Step 4: Complete the Security Template for the CER Project Manager Group

If you want to apply Model Security, complete the Object Security tab of the Security Planning Template to create the list of users that will be part of the CER Project Manager group.

To complete the Security Template for the CER Project Manager Group:

1. Launch the Security Planning Template and open the Object Security tab.
2. List all CER users by name that will be part of the CER Project Manager (CER__PROJ_MGR) group.
3. Save the completed template for reference later.

Step 5: Assign Users to Costpoint User Groups

After completing the plan and templates for the various security elements, you can start with the actual configuration setup by first assigning users to user groups.

Use the completed Security Planning Template as reference when you perform this procedure.

To assign existing Costpoint users to CER User Groups:

1. Log on to Costpoint and open the Manage User Groups (SYMGRP) screen.
2. Query the CER User Group to which you want to assign existing users.

   > **Note:** The CER User Groups in Costpoint start with “CER__”. Take note of the double underscore.
3. Once the CER User Group has been selected, click the **Assign Users to Group** subtask.
4. Click the **New** button in the **Assign Users to Groups** table window.

> **Note:** There are two ways to fill out the **Assign Users to Groups** table window. You can either:
>
> - Type in the users per row or
> - Do a copy-and-paste method where you get data from the Security Planning Template. This method is detailed in the succeeding steps.
>
> Either way is acceptable so choose the most convenient way for you.

5. On the Security Planning Template, open the **Object Security** tab.
6. On the Security Planning Template spreadsheet, look for the records for the CER User Group that you just selected on the Manage Users Groups screen.
7. On the spreadsheet, highlight the records for the three columns—**User ID**, **Name**, and **Company**. And then, copy them or press CTRL+C.

User ID	Name	Company
User001SS	Sam Smith	One
User002JS	Jon Snow	One
User003AS	Anna Scott	One
User 4		
User 5		

   If the names or company values do not appear on screen, you need to press the TAB key for each row for the system to display the corresponding name and company.
8. Click **Save & Continue**.
9. Repeat steps 2 to 8 until you have assigned all users to the CER User Groups.

Security in Legacy Content and New Models

Model Security, Object Level, and Capability Security are applied to the new models in CER 7.2.3. The legacy content has Object and Capability Security.

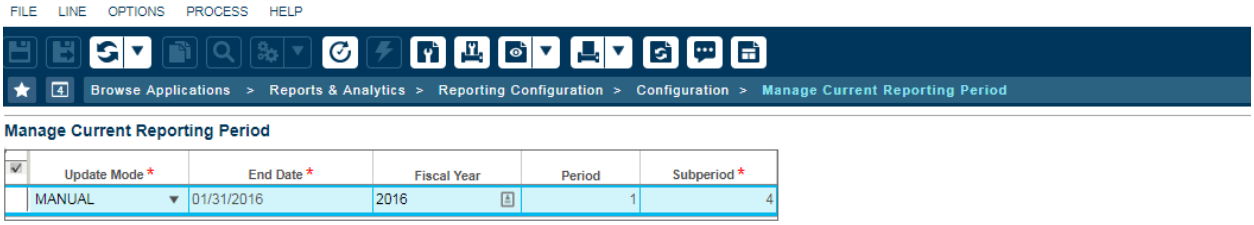
The Legacy models are:

- Costpoint Enterprise Reporting
- Costpoint Enterprise Reporting for Budgeting and Planning
- Costpoint Enterprise Reporting for Fixed Assets
- Costpoint Enterprise Reporting for HR and Payroll
- ICS Core
- ICS-Presentation
- Costpoint Enterprise Reporting for Costpoint Project Manufacturing
- Costpoint Enterprise Reporting for Shop Floor Time
- Costpoint SOX
- TE SOX

The new models are:

- Accounts Receivable
- Contracts
- General Ledger
- Projects
- Planning

Step 6: Set Up Current Reporting Period



Use the Manage Current Reporting Period (BIMRPTCURPD) application in Costpoint to set up the period that CER will use in reporting.

To set up the CER current reporting period:

1. In Costpoint, launch the Manage Current Reporting Period (BIMRPTCURPD) application (**Reports and Analytics** » **Reporting Configuration** » **Configuration** » **Manage Current Reporting Period**).
2. Enter the relevant information in the fields of the screen.

Field	Description
Update Mode	Select either **Auto (default setting)** or **Manual**. Deltek recommends that you select **Manual** so you can set the **End Date**, **Fiscal Year**, **Period**, and **Subperiod** of your choice. **Note:** It is recommended that you use the **Manual** setting since the administrator can then control when the reports and dashboards run when the current period is finished, which can vary period to period. This setting controls reports and dashboards that use the field **Current Period or Year** settings. This means you do not need to reset the field each month when you access the data.
End Date	Enter the end date for the current reporting period.
Fiscal Year	Enter the fiscal year for the current reporting period.
Period	Enter the period for the current reporting period.
Subperiod	Enter the subperiod for the current reporting period.

> **Note:** If you select **Auto** in the **Update Mode** field, the default values set on the Manage Current Reporting Period screen are based on the values of your accounting periods in Costpoint. The **End Date** is set to the closest end date to today's date. For example, if today's date is July 10, 2018, the end date will be **July 31, 2018**. This is because it is the closest end date and is greater than July 10, 2018.

Note that the current period screen in Costpoint Planning should also set to the same period. This screen is found in Costpoint at **Planning » Administration » Administration Controls » Maintain Current Period**.

This setting controls the updating of the reporting tables and is separate from the CER Current Period.

3. Click **Save**.

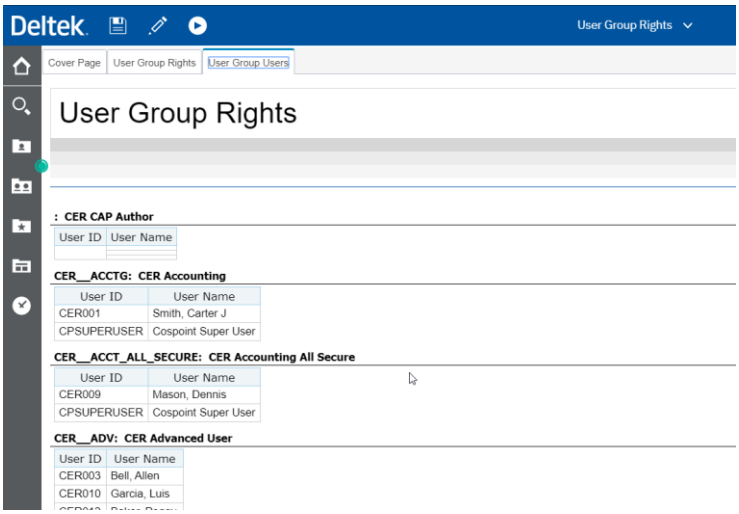
Step 7: Validate User Groups

After you complete the steps in the post-installation phase, check the list of users per user group in CER against your accomplished Security Planning Template.

To perform this procedure, you must have access to the User Group Rights report in **Team Content » Costpoint Enterprise Reporting** for **Costpoint Administration » Security**.

To validate the users in user groups:

1. In CER 7.2.3, go to **Team Content » Costpoint Enterprise Reporting for Costpoint Administration » Security** and run the User Group Rights report.
2. On the prompt screen, enter **CER** in the **User Group(s):** field. Click **Search**.
3. Select all the user groups that start with CER that you have created, and click **Insert** to transfer them to the selection box on the right.
4. Click **Run Report**.
5. On the report, click the **User Group Users** tab.
6. Compare the list of users in the report against the list of users that are in your Security Planning Template. Check if all users are accounted for.



Step 8: Have Users Run and Validate Reports

Once you have data in your Costpoint database and your users have watched the Overview and Navigation training videos from the Help menu, they should:

- Make sure they have rights to the areas that have been granted to them
- Run some of the standard reports in their area and validate the results
- Schedule Reports
- View Dashboards (Projects and Planning only)
- Save a report to “My Content” folder

Completing these steps finishes the initial setup of Enterprise Reporting. To learn more about how to manage reports and dashboards that you modify or create, see the “Managing Custom Content” guide.

Special Topics

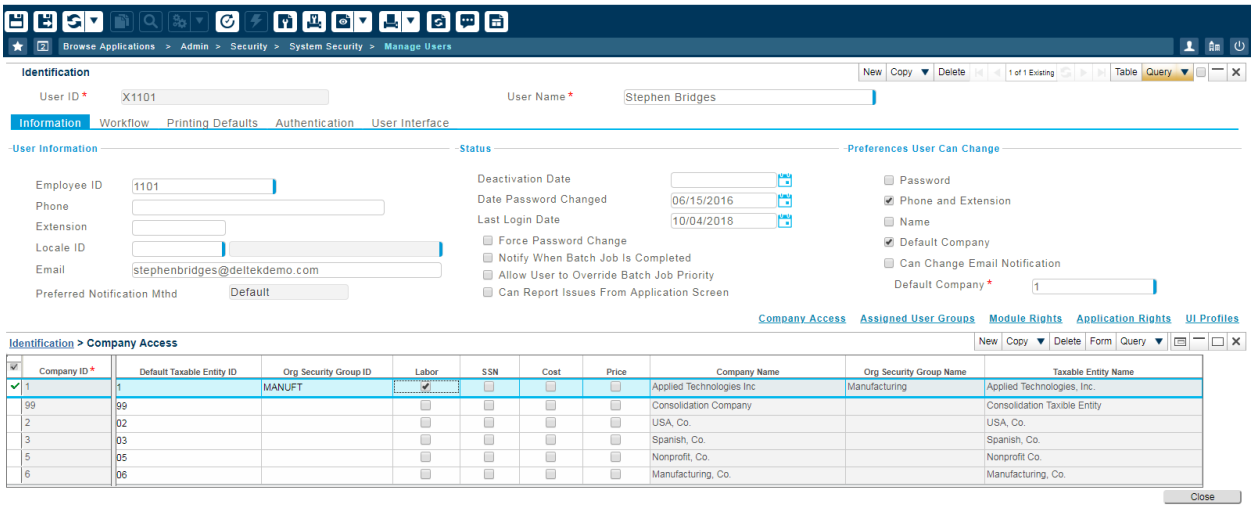
Special Topic 1: Organization, Labor Supression, and Project Security in Costpoint

CER's Project model leverages the Organization Security settings in Costpoint. If CER Security is turned on, a user MUST be assigned an Org Security Group or they will not see any data. If you do not want org restrictions on the user, you would assign them to an "All Orgs" security group that has access to all orgs.

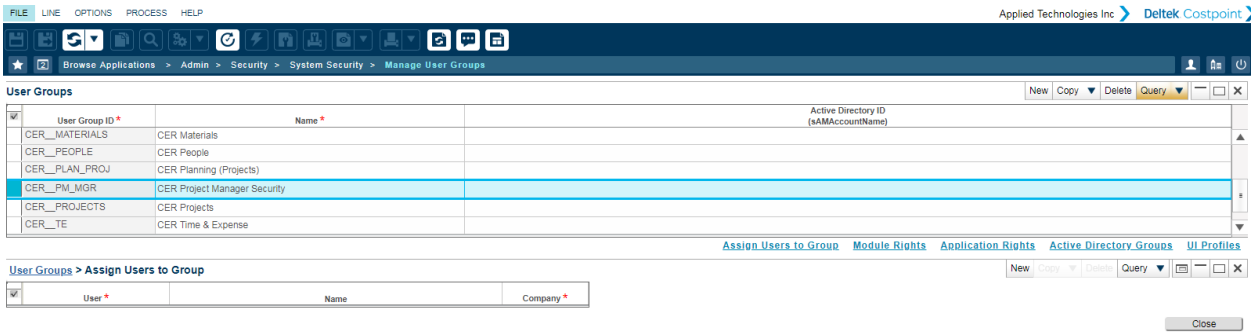
Once a user is set up and assigned an Org Security Group ID, they will have access to all the projects that are linked to that organization. An Org Security Group ID is linked to an Org Security Profile by module. For CER to determine the security to apply, it looks for the profile associated with a specific module. The following table shows the corresponding model security profile for each secured package.

Secured Package	Module Security Profile Used	Organization Secured
Accounts Receivable	AR	Owning Org
General Ledger	GL	Performing Org
Project Reporting	PJ	Owning Org
Project Analysis	PJ	Owning Org

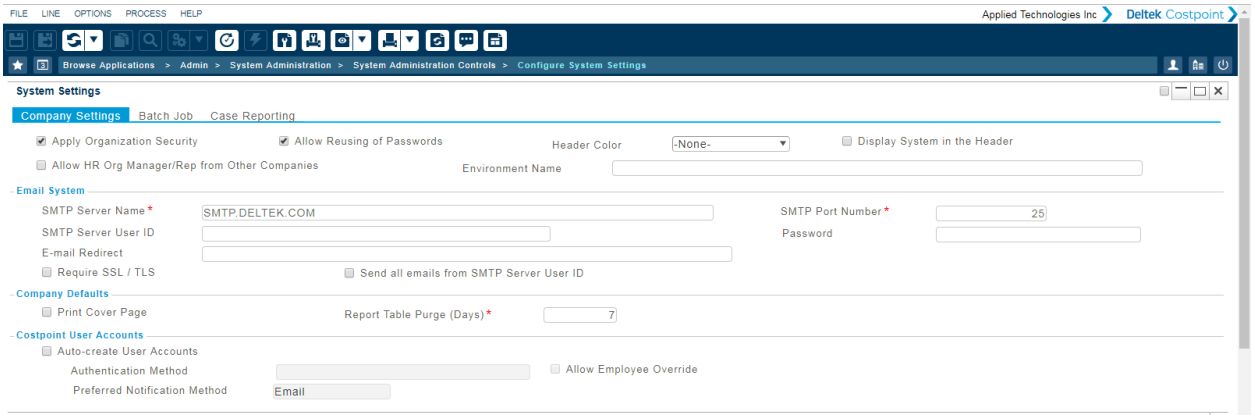
In addition, the Project model will suppress labor if the Labor flag is checked for the user. It is important that at least one Org is assigned to the Org Security Group. If no orgs are assigned, the user will not be able to see any data.



When a user is set up as Project Manager, this organization group they are assigned to is irrelevant, since they will only see the projects they are assigned to, regardless of org. In order to limit the projects to only the projects that the Project Manager owns, you must assign the user to the group, CER PM_MGR. Project Security applies to Accounts Receivable and Projects models.



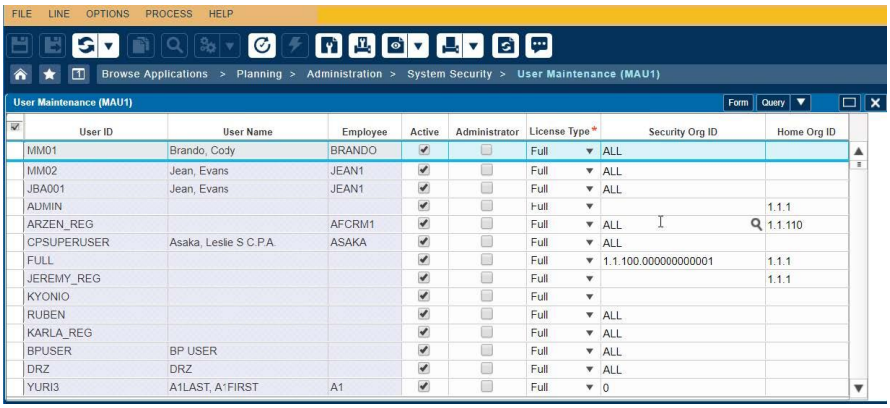
Note: It is possible to implement model security in the CER Projects model without applying security in Costpoint. In order to do this, simply clear the **Apply Organization Security** check box under Configure System Settings.



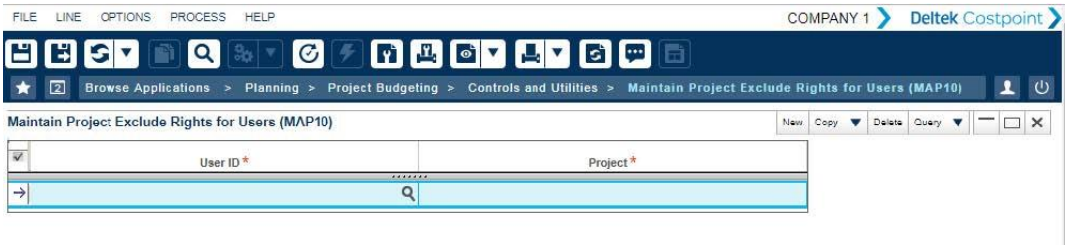
Special Topic 2: Organization and Project Security in Costpoint Planning

CER's Project Planning model leverages the Organization/Project Security settings in the Costpoint Planning module. Costpoint Planning (formerly Budgeting and Planning) has distinct security settings related to the Planning content and does not use the Costpoint Organization Security used in the core Projects CER model.

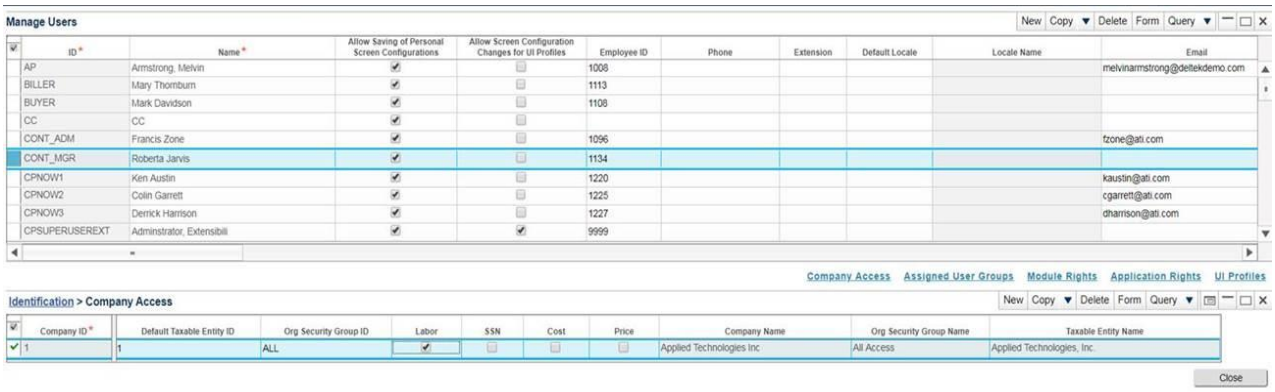
The CER Project Planning models leverage the Organization Security set up in the User Maintenance application shown below. Once a user is set up and given a Security Org ID, they will have access to all the projects that are owned by that Organization. In addition, if a user is set up as Project Manager for a project that is owned by an organization that they do not have access to, they will be granted access to those projects.



There is currently no way to limit the projects to only the projects that the PM owns. However, there is a way to exclude specific projects from a user's list using the following screen. Once a user and a project is added here, they will no longer be able to access that project.



Labor suppression settings made in the Manage User application (same application for Costpoint and Planning) are leveraged in Planning and in the CER Project Planning models. (See prior Special Topic 1 on org security in Costpoint for information about labor suppression.)



Special Topic 3: Detailed Capabilities by Role

Capabilities	CER__CONSUMER	CER__USER	CER_ADV	CER_DEV	CER_ADMIN
Administration					x
Distribution Lists and Contacts					x
Run activities and schedules					x

Capabilities	CER__CONSUMER	CER__USER	CER_ADV	CER_DEV	CER_ADMIN
Users, Groups, and Roles					x
Analysis Studio			X	x	x
Cognos Viewer	x	x	X	x	x
Context Menu	x	X	X	x	x
Run With Options	x	X	X	x	x
Selection	x	X	X	x	x
Toolbar	x	X	X	x	x
Collaborate		X	X	x	x
Allow collaboration features		X	X	x	x
Launch collaboration tools		X	X	x	x
Dashboard	x (View Only)	X	X	x	x
Data sets			X	x	x
Desktop Tools				x	x
Detailed Errors			X	x	x
Event Studio			X	x	x
Executive Dashboard		X	X	x	x
Use Advanced Dashboard Features			X	x	x
Use Interactive Dashboard Features		X	X	x	x
External Repositories	x	X	X	x	x
View external documents	x	X	X	x	x
Generate CSV Output	x	X	X	x	x
Generate PDF Output	x	X	X	x	x
Generate XLS Output	x	X	X	x	x
Generate XML Output	x	X	X	x	x
Glossary	x	X	X	x	x
Hide Entries					x
Import relational metadata				x	x
Lineage	x	X	X	x	x
Mobile		X	X	x	x
Query Studio			X	x	x
Advanced			X	x	x
Create			X	x	x
Report Studio			X	x	x
Bursting			X	x	x

Capabilities	CER__CONSUMER	CER__USER	CER_ADV	CER_DEV	CER_ADMIN
Create/Delete			X	x	x
HTML Items in Report			X	x	x
User Defined SQL*			X	x	x
Scheduling			X	x	x
Schedule by day			X	x	x
Schedule by hour			X	x	x
Schedule by minute			x	x	x
Schedule by month			x	x	x
Schedule by trigger			x	x	x
Schedule by week			x	x	x
Schedule by year			x	x	x
Scheduling Priority			x	x	x
Watch Rules		X			x
Web-based modeling			x	x	x
* Turned off for Projects, Planning, General Ledger, and Accounts Receivable folder packages and all models with model security.					

About Deltek

Better software means better projects. Deltek is the leading global provider of enterprise software and information solutions for project-based businesses. More than 23,000 organizations and millions of users in over 80 countries around the world rely on Deltek for superior levels of project intelligence, management and collaboration. Our industry-focused expertise powers project success by helping firms achieve performance that maximizes productivity and revenue. www.deltek.com