Deltek Costpoint Business Intelligence 8.0.x

Cloud Setup Guide

March 11, 2021

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 March 2021.

Contents

About this Guide

Welcome to the Costpoint Business Intelligence 8.0.x Setup Guide for Costpoint Cloud Customers.

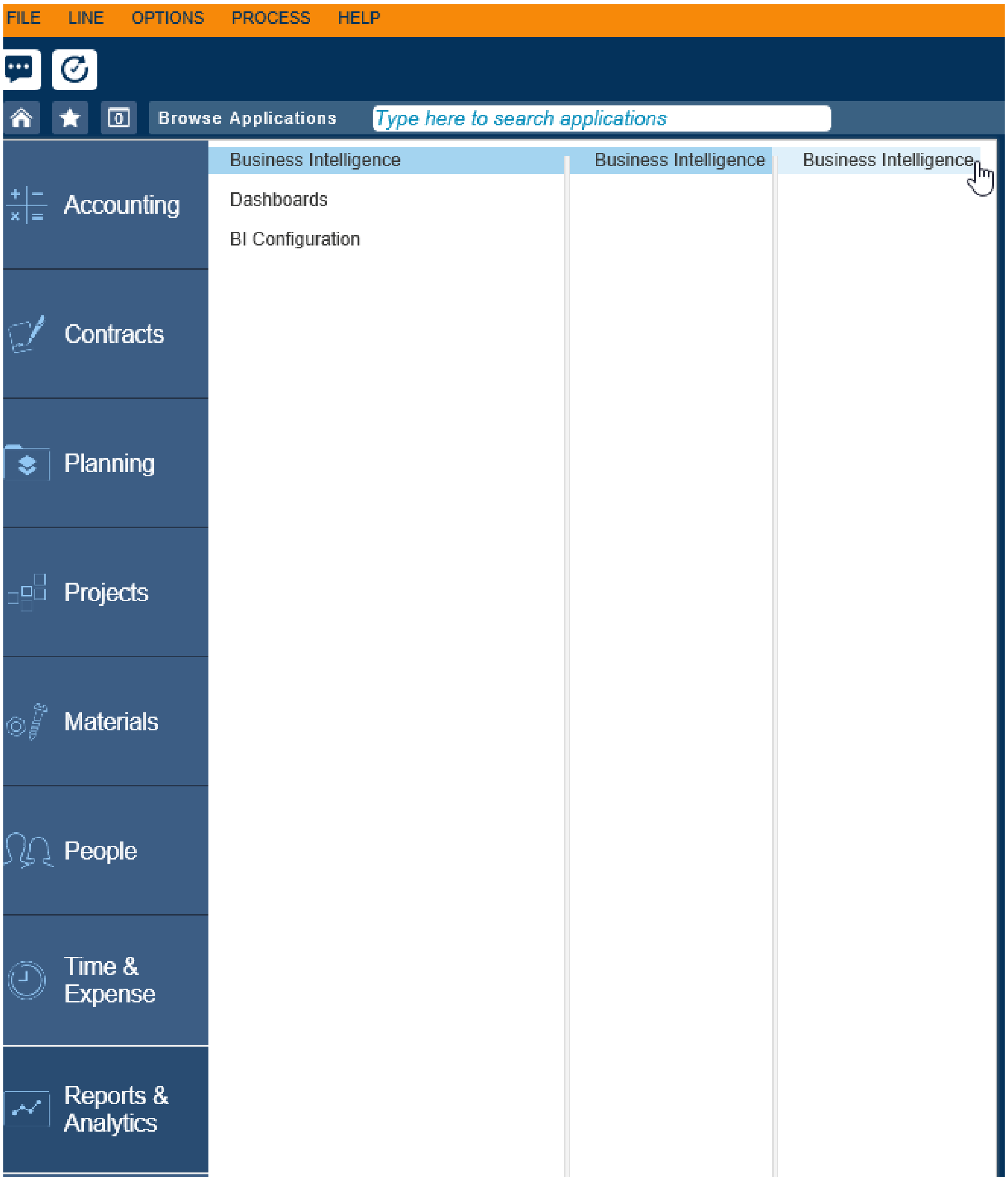
This guide is used after you receive administrative rights to Costpoint BI and will walk you through the initial setup of Costpoint BI so your environment is secured before you allow users into Costpoint BI to run and create reports and Dashboards and leverage the built-in security features in Costpoint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

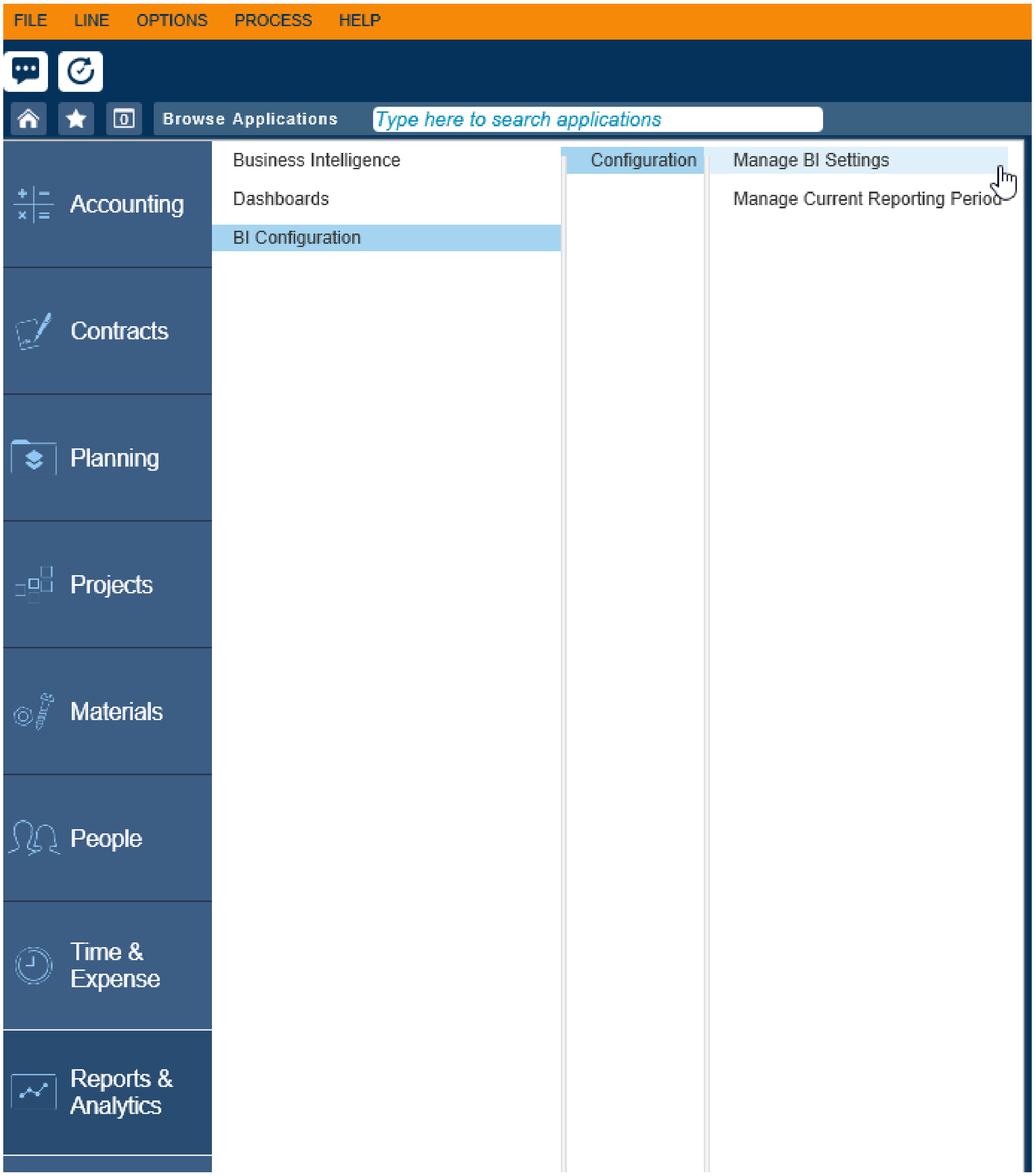
Costpoint Enterprise Reporting to Costpoint BI

Starting in Costpoint 8.0, the name “Costpoint Enterprise Reporting” or “CER” has been changed to “Costpoint Business Intelligence”. The name was changed to align with the product’s capabilities which are beyond reporting. You may still see references to the former name, CER, in some of the names and objects throughout this document. For more details, see Costpoint Enterprise Reporting Name Change.

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 Business Intelligence application (ERCOGNOS), Manage BI Settings (BIMCERSETTINGS), and Manage Current Accounting Period (BIMRPTCURPD).




FILE
LINE
OPTIONS
PROCESS
HELP
Browse Applications
Type here to search applications
Accounting
Contracts
Planning
Projects
Materials
People
Time & Expense
Reports & Analytics
Business Intelligence
Dashboards
BI Configuration
Configuration
Manage BI Settings
Manage Current Reporting Period

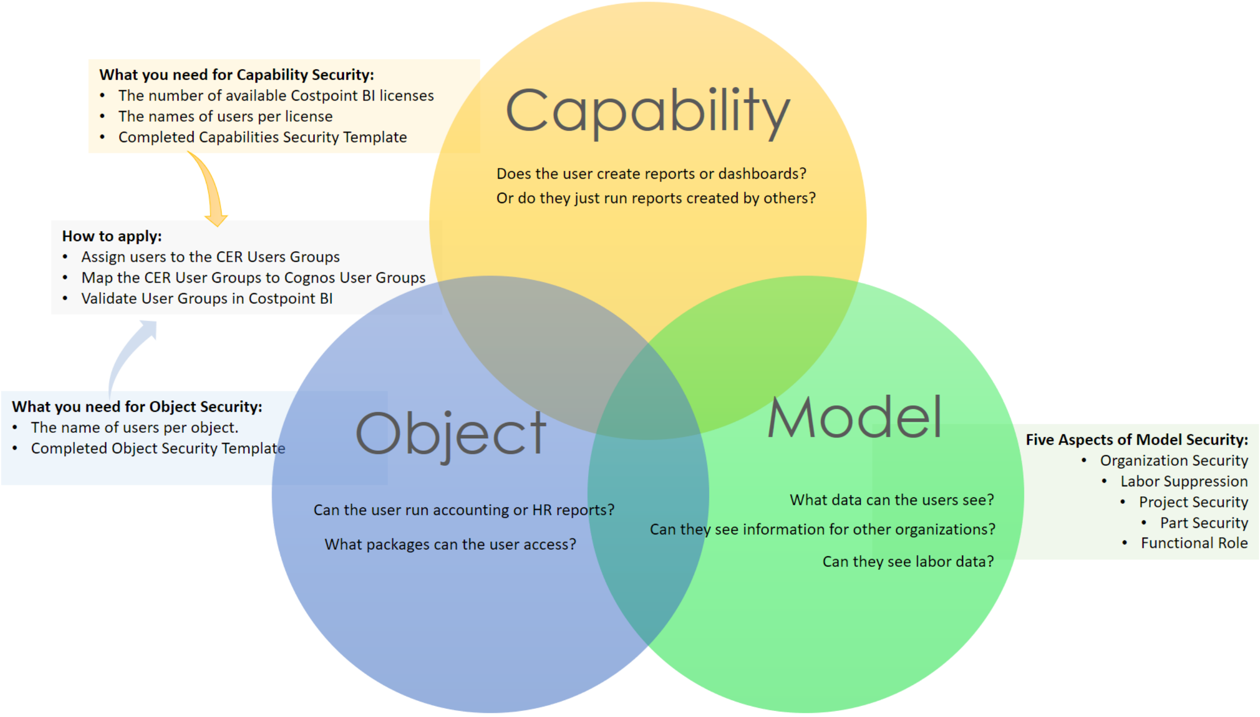
Overview

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 Costpoint BI Security

There are different types of data security that you can apply in Costpoint Business Intelligence 8.0.x


What you need for Capability Security:
- The number of available Costpoint BI licenses
- The names of users per license
- Completed Capabilities Security Template
How to apply:
- Assign users to the CER Users Groups
- Map the CER User Groups to Cognos User Groups
- Validate User Groups in Costpoint BI
What you need for Object Security:
- The name of users per object.
- Completed Object Security Template
Capability
Does the user create reports or dashboards?
Or do they just run reports created by others?
Object
Can the user run accounting or HR reports?
What packages can the user access?
Model
What data can the users see?
Can they see information for other organizations?
Can they see labor data?
Five Aspects of Model Security:
- Organization Security
- Labor Suppression
- Project Security
- Part Security
- Functional Role

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 usercreate 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, Costpoint Planning, and Time and Expense or T&E. There are five aspects in this type which are:
   - Labor Suppression
   - Organization Security
   - Project Security
   - Parts Security
   - Functional Role

Step 1: Check the Model Security Configuration

The Costpoint, Costpoint Planning, and TE Model Security is enabled by default. If you do not want to apply it, you can disable it 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 model security is set on or off. The best practice is to keep the Costpoint, Costpoint Planning, and T&E model security on.

Note: Skip this procedure if you want to use Model Security for your Costpoint BI implementation. Remember that Model Security utilizes the settings in Costpoint, Costpoint Planning, and/or T&E.

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. See Organization Security for information about setting up org security.

To disable Model Security:

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

Field	Description
Enable CP and Planning Model Security	Select **No** to disable model security for the Costpoint and Costpoint Planning models. Model security is enabled by default.
Use CP Organization Security By Module	Select **No** to disable organization security in the new secure models which are: ▪ Accounts Receivable ▪ Accounts Payable ▪ General Ledger ▪ Manufacturing ▪ Materials ▪ Procurement ▪ Projects
Enable T&E Model Security	Select **No** to disable model security for the Time model. Model security is enabled by default.

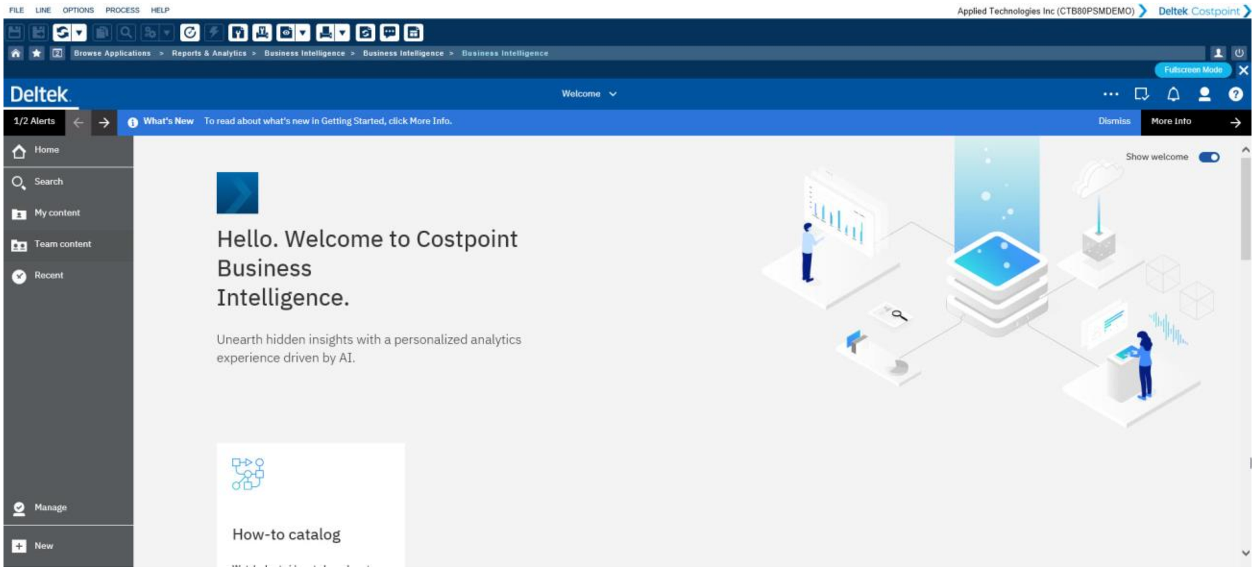
Note: When Model Security is disabled, Capability and Object Security are still in place in Costpoint BI.

3. Click **Save**.

Assign Costpoint BI Rights to the Administrator

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

The Administrator should then log in to Costpoint Business Intelligence to make sure you can access the initial Costpoint BI Welcome Screen.

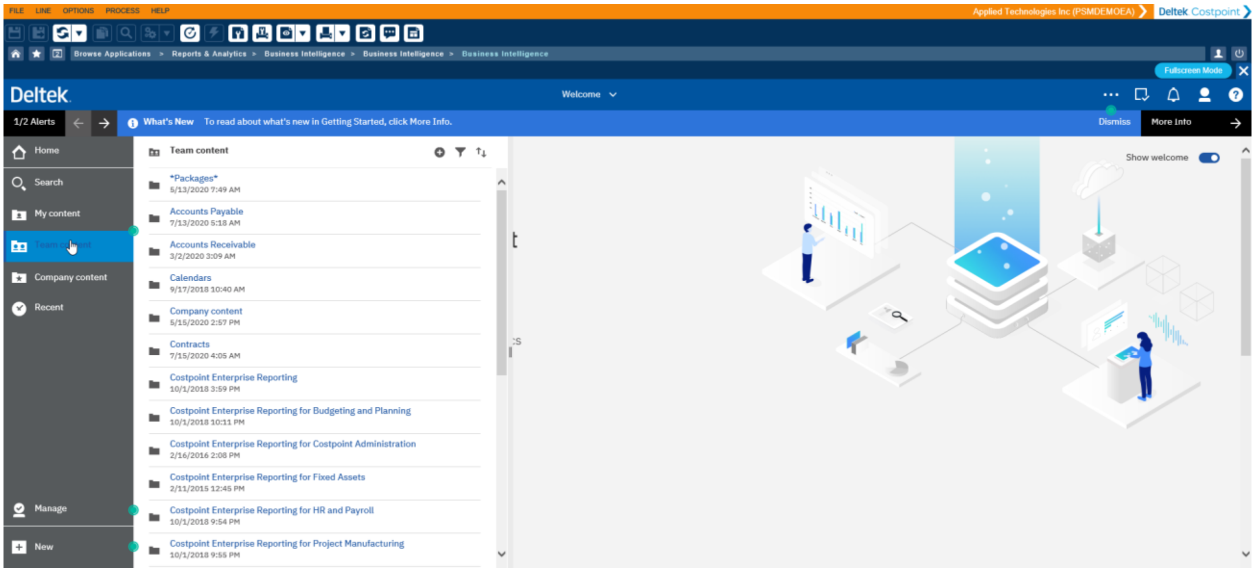

FILE LINE OPTIONS PROCESS HELP
Applied Technologies Inc (CTB80PSMDEMO)
Deltek Costpoint
Browse Applications > Reports & Analytics > Business Intelligence > Business Intelligence > Business Intelligence
Fullscreen Mode
Deltek
Welcome
1/2 Alerts
What's New
Dismiss
More Info
Home
Search
My content
Team content
Recent
Manage
New
Show welcome
How-to catalog

To read about what's new in Getting Started, click More Info.

Hello. Welcome to Costpoint Business Intelligence.

Unearth hidden insights with a personalized analytics experience driven by AI.

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


FILE LINE OPTIONS PROCESS HELP
Applied Technologies Inc (PSMDEMOEA)
Deltek Costpoint
Browse Applications > Reports & Analytics > Business Intelligence > Business Intelligence > Business Intelligence
Fullscreen Mode
Deltek
Welcome
1/2 Alerts
What's New
Dismiss
More Info
Home
Search
My content
Team content
Company content
Recent
Manage
New
Show welcome

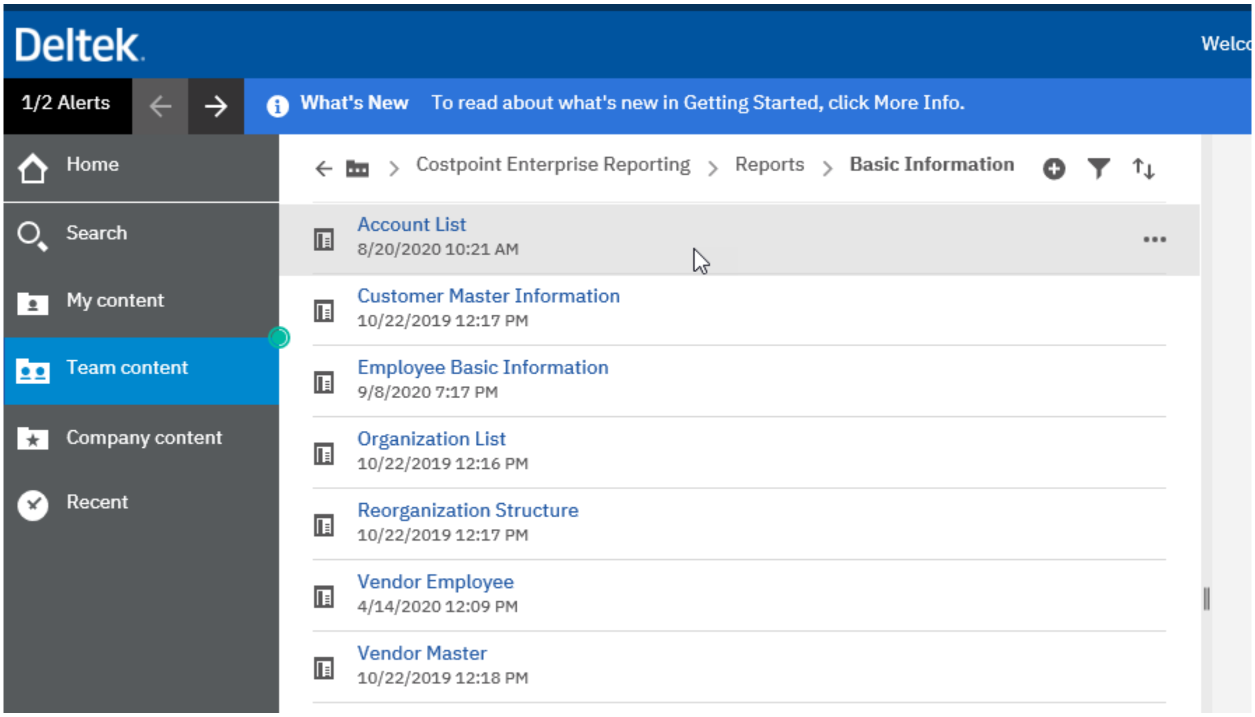
To read about what's new in Getting Started, click More Info.

Team content

- *Packages* 5/13/2020 7:49 AM
- Accounts Payable 7/13/2020 5:18 AM
- Accounts Receivable 3/2/2020 3:09 AM
- Calendars 9/17/2018 10:40 AM
- Company content 5/15/2020 2:57 PM
- Contracts 7/15/2020 4:05 AM
- Costpoint Enterprise Reporting 10/1/2018 3:59 PM
- Costpoint Enterprise Reporting for Budgeting and Planning 10/1/2018 10:11 PM
- Costpoint Enterprise Reporting for Costpoint Administration 2/16/2016 2:08 PM
- Costpoint Enterprise Reporting for Fixed Assets 2/11/2015 12:45 PM
- Costpoint Enterprise Reporting for HR and Payroll 10/1/2018 9:54 PM
- Costpoint Enterprise Reporting for Project Manufacturing 10/1/2018 9:55 PM

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.


Deltek
Welc
1/2 Alerts
What's New
To read about what's new in Getting Started, click More Info.
Home
Search
My content
Team content
Company content
Recent
Costpoint Enterprise Reporting > Reports > Basic Information

Account List
8/20/2020 10:21 AM

Customer Master Information
10/22/2019 12:17 PM

Employee Basic Information
9/8/2020 7:17 PM

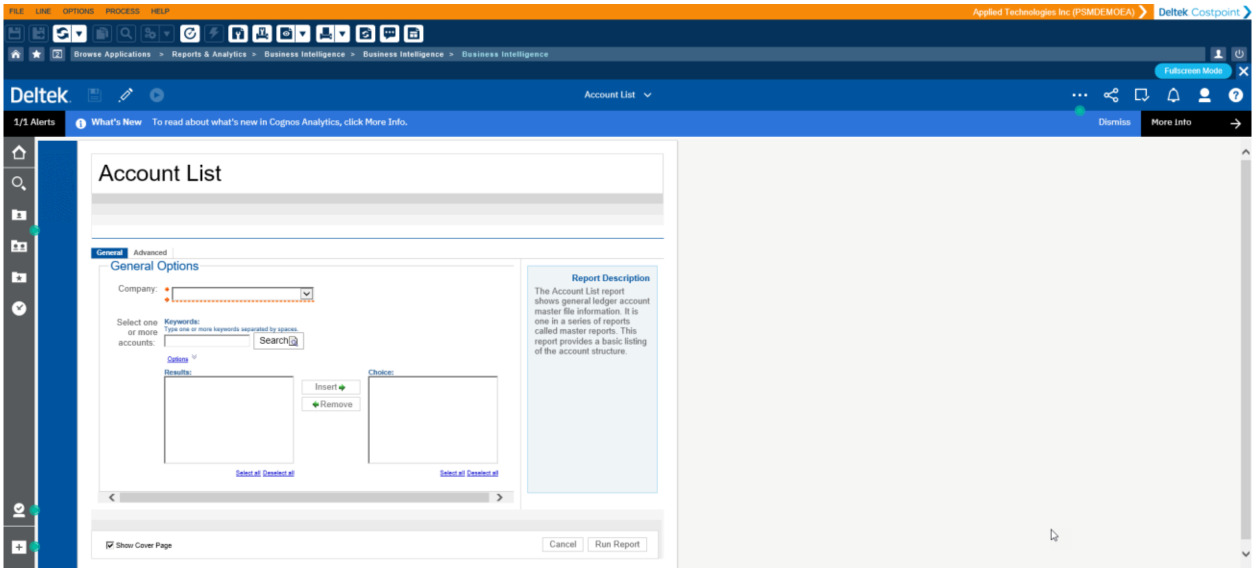
Organization List
10/22/2019 12:16 PM

Reorganization Structure
10/22/2019 12:17 PM

Vendor Employee
4/14/2020 12:09 PM

Vendor Master
10/22/2019 12:18 PM

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


FILE
LINE
OPTIONS
PROCESS
HELP
Applied Technologies Inc (PSMDEMOEA)
Deltek Costpoint
Browse Applications > Reports & Analytics > Business Intelligence > Business Intelligence > Business Intelligence
Fullscreen Mode
Deltek
Account List
1/1 Alerts
What's New
To read about what's new in Cognos Analytics, click More Info.
Dismiss
More Info
General
Advanced
Options
Insert
Remove
Select all
Deselect all
Select all
Deselect all
Cancel
Run Report

Account List

General Options

Company:

Select one or more accounts: Keywords: Type one or more keywords separated by spaces. Search

Results:

Choice:

Report Description

The Account List report shows general ledger account master file information. It is one in a series of reports called master reports. This report provides a basic listing of the account structure.

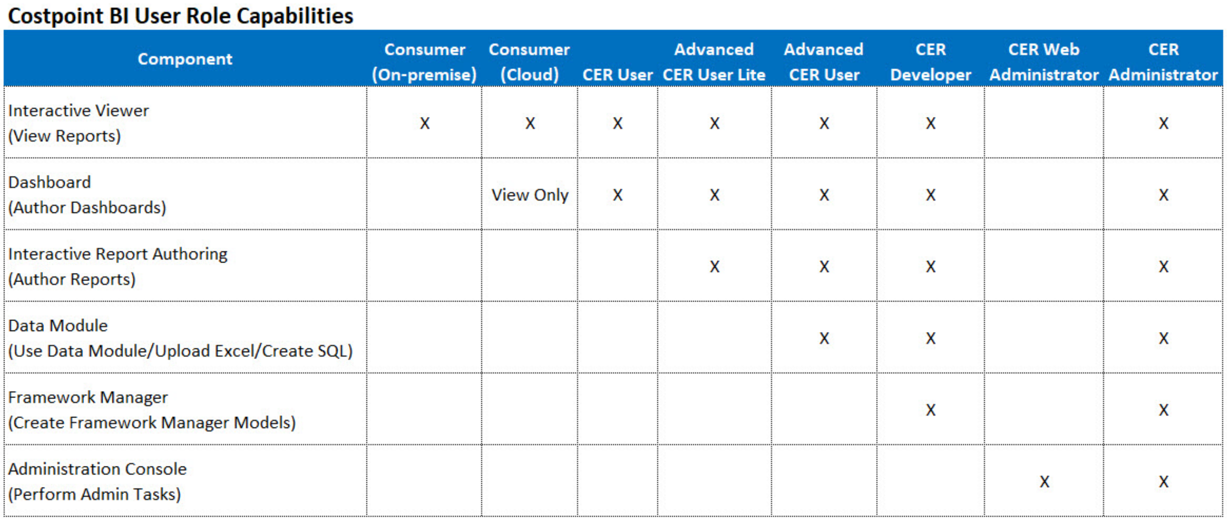
☑ Show Cover Page

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 the licenses.



Costpoint BI User Role Capabilities

Component	Consumer (On-premise)	Consumer (Cloud)	CER User	Advanced CER User Lite	Advanced CER User	CER Developer	CER Web Administrator	CER Administrator
Interactive Viewer (View Reports)	x	x	x	x	x	x		x
Dashboard (Author Dashboards)		View Only	x	x	x	x		x
Interactive Report Authoring (Author Reports)				x	x	x		x
Data Module (Use Data Module/Upload Excel/Create SQL)					x	x		x
Framework Manager (Create Framework Manager Models)						x		x
Administration Console (Perform Admin Tasks)							x	x

For a more detailed list of capabilities by role, see the Detailed Capabilities by Role table.

Note: Consumer licenses are not part of cloud licensing; however, administrators may want to limit the functionality of some CER users to only view dashboards and not be able to 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.

CER User is only available in CER Bundles (restricted).

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 do not 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. **Advanced CER User Lite (CER__ADV_LITE)** is also available and is similar to Advanced CER User, but with some limited capabilities such as the inability to use data modules, upload MS Excel, and create SQL.
- **CER Developer (CER__DEV)**: This type of user is not included in the typical Costpoint BI 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 Costpoint BI bundle. This user has access to all capabilities of the license types and some

administrative functions. The rest of the administrative functions are handled by the Deltek Cloud Operations team.

Every CER user should be assigned to one Costpoint BI 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 Costpoint Cloud Information Center.

For the 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

Detailed Capabilities by Role

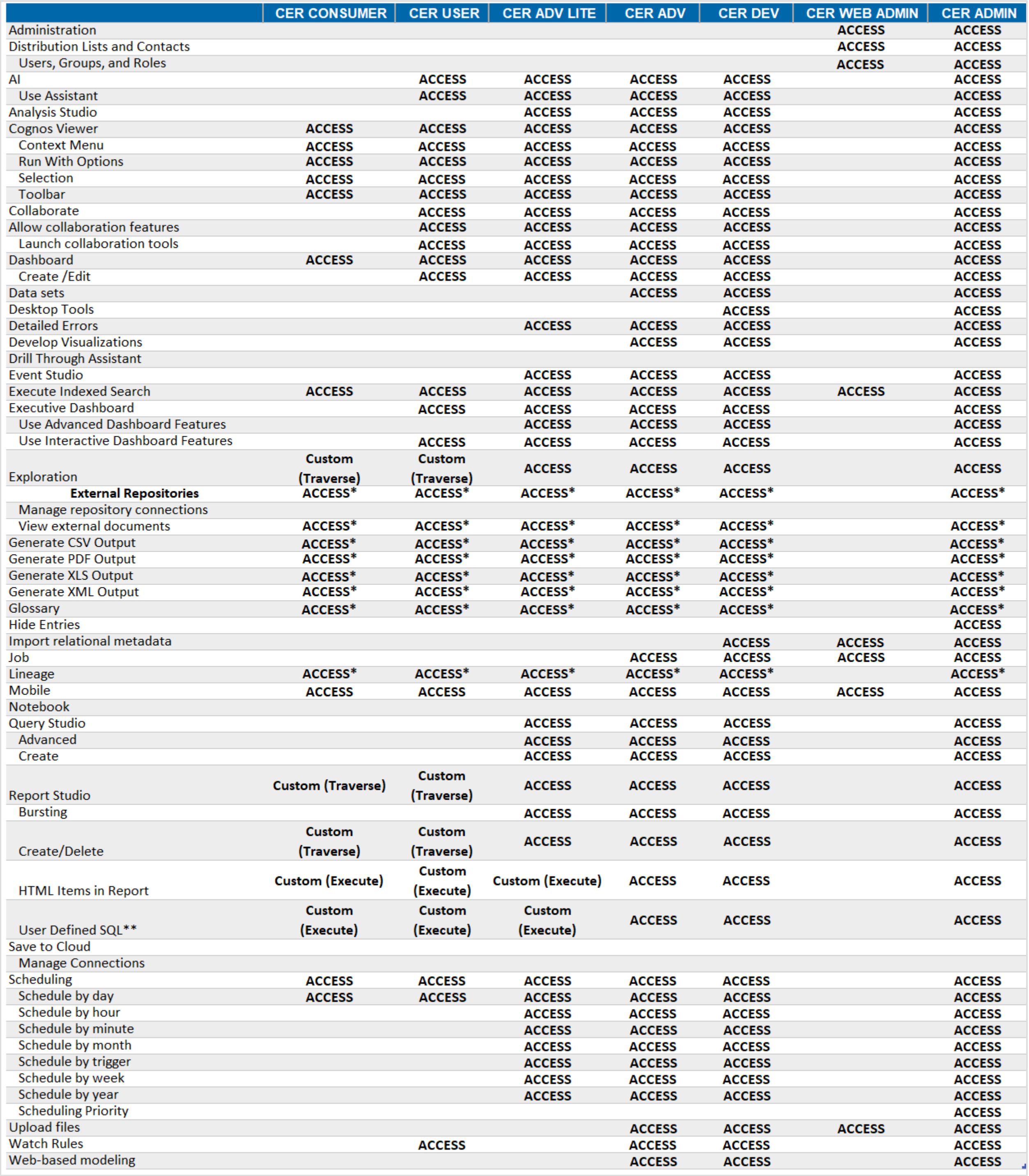
User Roles have unique sets of capabilities assigned to them upon installation. You should assign users to roles that are appropriate to their function in the organization.

*Everyone has this capability so this is automatically applied to new roles.

**User Defined SQL is turned off for the following packages. This prevents unauthorized users to bypass security through SQL.

- Projects
- Planning
- General Ledger
- Accounts Receivable
- Accounts Payable
- Procurement
- Materials

- Manufacturing
- Time



	CER CONSUMER	CER USER	CER ADV LITE	CER ADV	CER DEV	CER WEB ADMIN	CER ADMIN
Administration						ACCESS	ACCESS
Distribution Lists and Contacts						ACCESS	ACCESS
Users, Groups, and Roles						ACCESS	ACCESS
AI		ACCESS	ACCESS	ACCESS	ACCESS		ACCESS
Use Assistant		ACCESS	ACCESS	ACCESS	ACCESS		ACCESS
Analysis Studio			ACCESS	ACCESS	ACCESS		ACCESS
Cognos Viewer	ACCESS	ACCESS	ACCESS	ACCESS	ACCESS		ACCESS
Context Menu	ACCESS	ACCESS	ACCESS	ACCESS	ACCESS		ACCESS
Run With Options	ACCESS	ACCESS	ACCESS	ACCESS	ACCESS		ACCESS
Selection	ACCESS	ACCESS	ACCESS	ACCESS	ACCESS		ACCESS
Toolbar	ACCESS	ACCESS	ACCESS	ACCESS	ACCESS		ACCESS
Collaborate		ACCESS	ACCESS	ACCESS	ACCESS		ACCESS
Allow collaboration features		ACCESS	ACCESS	ACCESS	ACCESS		ACCESS
Launch collaboration tools		ACCESS	ACCESS	ACCESS	ACCESS		ACCESS
Dashboard	ACCESS	ACCESS	ACCESS	ACCESS	ACCESS		ACCESS
Create /Edit		ACCESS	ACCESS	ACCESS	ACCESS		ACCESS
Data sets				ACCESS	ACCESS		ACCESS
Desktop Tools					ACCESS		ACCESS
Detailed Errors			ACCESS	ACCESS	ACCESS		ACCESS
Develop Visualizations				ACCESS	ACCESS		ACCESS
Drill Through Assistant							
Event Studio			ACCESS	ACCESS	ACCESS		ACCESS
Execute Indexed Search	ACCESS	ACCESS	ACCESS	ACCESS	ACCESS	ACCESS	ACCESS
Executive Dashboard		ACCESS	ACCESS	ACCESS	ACCESS		ACCESS
Use Advanced Dashboard Features			ACCESS	ACCESS	ACCESS		ACCESS
Use Interactive Dashboard Features		ACCESS	ACCESS	ACCESS	ACCESS		ACCESS
Exploration	Custom (Traverse)	Custom (Traverse)	ACCESS	ACCESS	ACCESS		ACCESS
External Repositories	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*		ACCESS*
Manage repository connections							
View external documents	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*		ACCESS*
Generate CSV Output	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*		ACCESS*
Generate PDF Output	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*		ACCESS*
Generate XLS Output	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*		ACCESS*
Generate XML Output	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*		ACCESS*
Glossary	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*		ACCESS*
Hide Entries							ACCESS
Import relational metadata					ACCESS	ACCESS	ACCESS
Job				ACCESS	ACCESS	ACCESS	ACCESS
Lineage	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*		ACCESS*
Mobile	ACCESS	ACCESS	ACCESS	ACCESS	ACCESS	ACCESS	ACCESS
Notebook							
Query Studio			ACCESS	ACCESS	ACCESS		ACCESS
Advanced			ACCESS	ACCESS	ACCESS		ACCESS
Create			ACCESS	ACCESS	ACCESS		ACCESS
Report Studio	Custom (Traverse)	Custom (Traverse)	ACCESS	ACCESS	ACCESS		ACCESS
Bursting			ACCESS	ACCESS	ACCESS		ACCESS
Create/Delete	Custom (Traverse)	Custom (Traverse)	ACCESS	ACCESS	ACCESS		ACCESS
HTML Items in Report	Custom (Execute)	Custom (Execute)	Custom (Execute)	ACCESS	ACCESS		ACCESS
User Defined SQL**	Custom (Execute)	Custom (Execute)	Custom (Execute)	ACCESS	ACCESS		ACCESS
Save to Cloud							
Manage Connections							
Scheduling	ACCESS	ACCESS	ACCESS	ACCESS	ACCESS		ACCESS
Schedule by day	ACCESS	ACCESS	ACCESS	ACCESS	ACCESS		ACCESS
Schedule by hour			ACCESS	ACCESS	ACCESS		ACCESS
Schedule by minute			ACCESS	ACCESS	ACCESS		ACCESS
Schedule by month			ACCESS	ACCESS	ACCESS		ACCESS
Schedule by trigger			ACCESS	ACCESS	ACCESS		ACCESS
Schedule by week			ACCESS	ACCESS	ACCESS		ACCESS
Schedule by year			ACCESS	ACCESS	ACCESS		ACCESS
Scheduling Priority							ACCESS
Upload files				ACCESS	ACCESS	ACCESS	ACCESS
Watch Rules		ACCESS		ACCESS	ACCESS		ACCESS
Web-based modeling				ACCESS	ACCESS		ACCESS

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

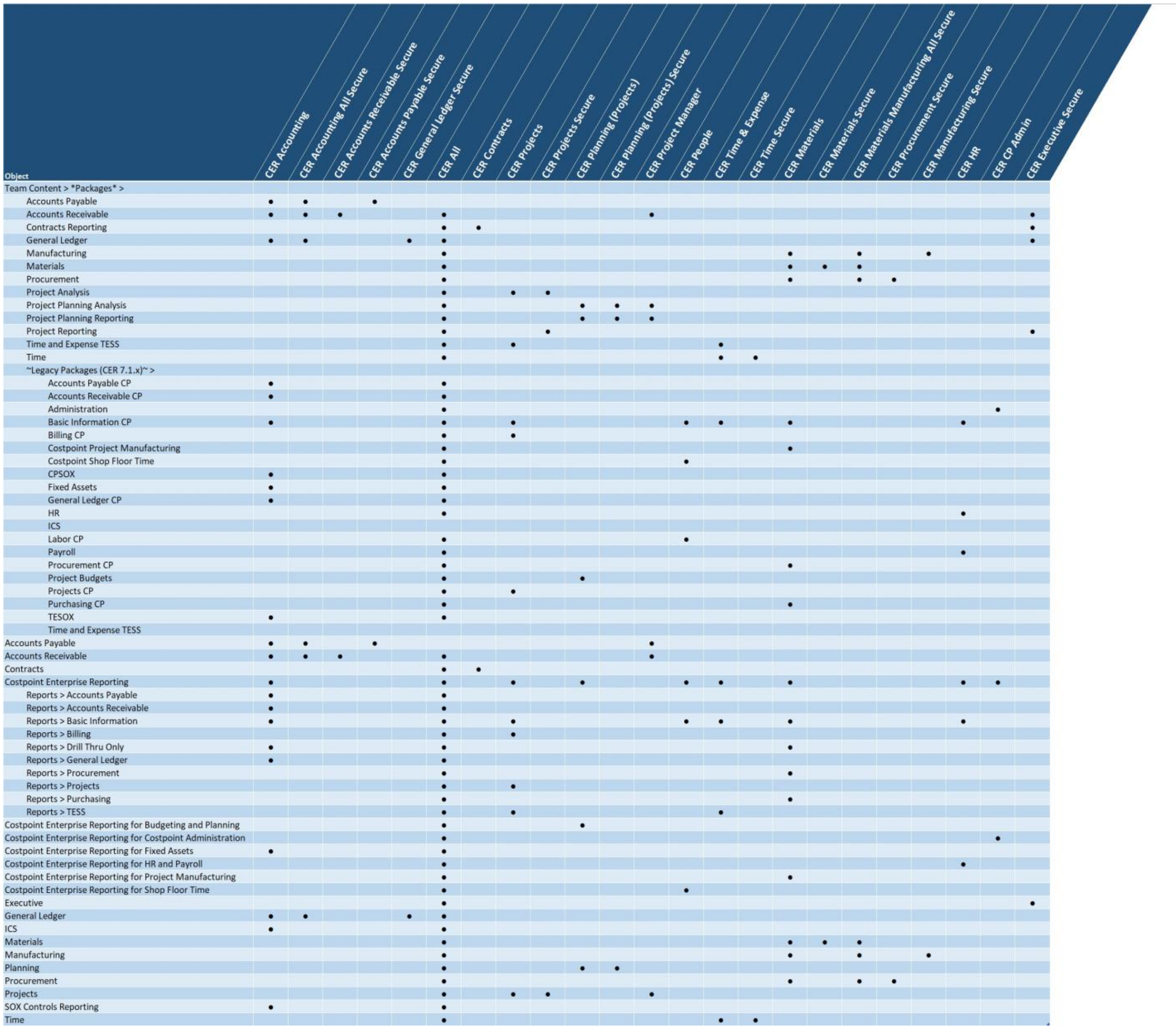
Deltek delivers content in the form of packages, reports, and dashboards organized in folders under **Team Content**.

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 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 in the following table.

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 Accounts Payable 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 Time Secure	CER Materials	CER Materials Secure	CER Materials Manufacturing All Secure	CER Procurement Secure	CER Manufacturing Secure	CER HR	CER CP Admin	CER Executive Secure
Team Content > *Packages* >																							
Accounts Payable	●	●		●																			
Accounts Receivable	●	●	●			●						●											●
Contracts Reporting						●	●																●
General Ledger	●	●			●	●																	●
Manufacturing						●										●		●		●			
Materials						●										●	●	●					
Procurement						●										●		●	●				
Project Analysis						●		●	●														
Project Planning Analysis						●				●	●	●											
Project Planning Reporting						●				●	●	●											
Project Reporting						●			●														●
Time and Expense TESS						●		●						●									
Time						●								●	●								
~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						●							●										
CPSOX	●					●																	
Fixed Assets	●					●																	
General Ledger CP	●					●																	
HR						●															●		
ICS																							
Labor CP						●							●										
Payroll						●															●		
Procurement CP						●										●							
Project Budgets						●				●													
Projects CP						●		●															
Purchasing CP						●										●							
TESOX	●					●																	
Time and Expense TESS																							
Accounts Payable	●	●		●								●											
Accounts Receivable	●	●	●			●						●											
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						●							●										
Executive						●																	●
General Ledger	●	●			●	●																	
ICS	●					●																	
Materials						●										●	●	●					
Manufacturing						●										●		●		●			
Planning						●				●	●												
Procurement						●										●		●	●				
Projects						●		●	●			●											
SOX Controls Reporting	●					●																	
Time						●								●	●								

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 will not see any content out of the box, which assures the Administrator that the consumers will not 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:

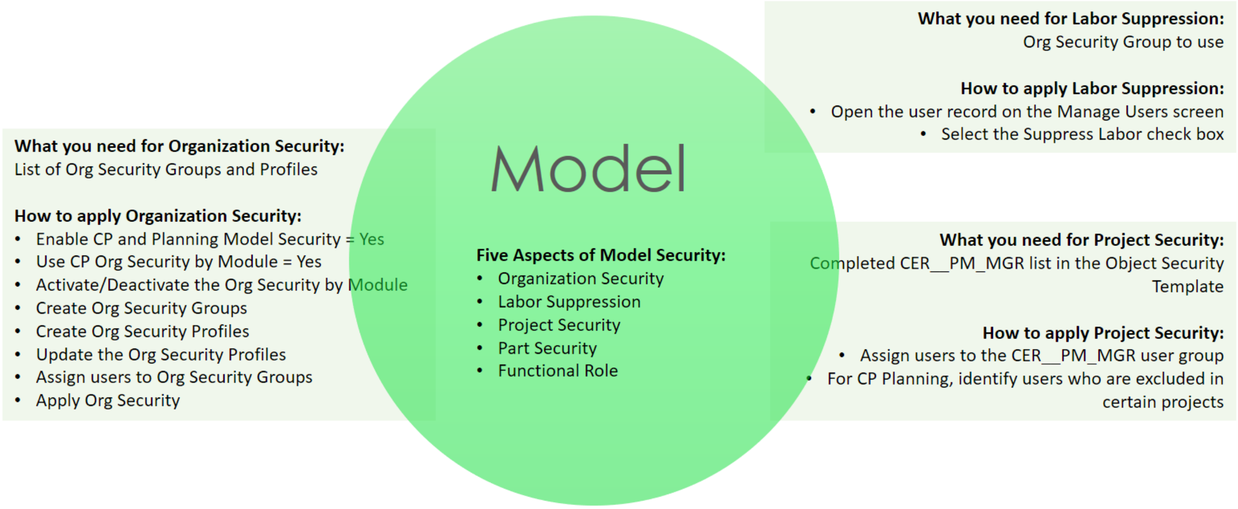
1. Launch the Security Planning Template and open the Object Security tab.
2. List all CER users by user ID, name, and company.

> **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.



Model

What you need for Organization Security:
List of Org Security Groups and Profiles

How to apply Organization Security:
- Enable CP and Planning Model Security = Yes
- Use CP Org Security by Module = Yes
- Activate/Deactivate the Org Security by Module
- Create Org Security Groups
- Create Org Security Profiles
- Update the Org Security Profiles
- Assign users to Org Security Groups
- Apply Org Security

Five Aspects of Model Security:
- Organization Security
- Labor Suppression
- Project Security
- Part Security
- Functional Role

What you need for Labor Suppression:
Org Security Group to use

How to apply Labor Suppression:
- Open the user record on the Manage Users screen
- Select the Suppress Labor check box

What you need for Project Security:
Completed CER__PM_MGR list in the Object Security Template

How to apply Project Security:
- Assign users to the CER__PM_MGR user group
- For CP Planning, identify users who are excluded in certain projects

There are five aspects of model or row level security.

1. **Organization Security**: Restricts data based on the user's organization rights established in Costpoint or Costpoint Planning. In this type of security, theproject data for the owning or performing organization are secured. If Organization Security is not established in Costpoint or Costpoint Planning, Costpoint BI models will not be able to restrict data by organization or company.

   For data models that use Costpoint as source, Costpoint Organization Security is enforced. If you are not planning on using this type of security, no setup or changes are required.

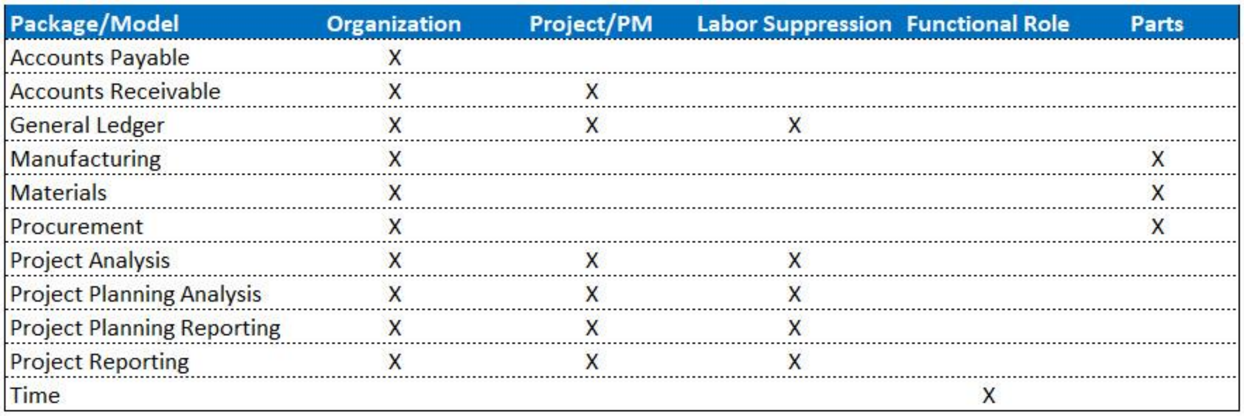
   For data models that use Planning as source, Costpoint BI uses information from the Planning setup.

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

2. **Labor Suppression**: Restricts the ability to see labor rates and dollars at the employee level using the labor suppression flag settings in Costpoint. In Costpoint BI, the rate/cost of employees are hidden in reports when Labor Suppression is in use. See the Labor Suppression section for how to leverage this capability.
3. **Project Security**: Restricts project data.
4. **Parts Security**: Restricts part data in support of International Traffic in Arms Regulation (ITAR).
5. **Functional Role**: Restricts data based on user's functional role.

Matrix for Secure Models

Different types of model and/or row level security are applied to the secure models or package in Costpoint Business Intelligence.



Package/Model	Organization	Project/PM	Labor Suppression	Functional Role	Parts
Accounts Payable	X				
Accounts Receivable	X	X			
General Ledger	X	X	X		
Manufacturing	X				X
Materials	X				X
Procurement	X				X
Project Analysis	X	X	X		
Project Planning Analysis	X	X	X		
Project Planning Reporting	X	X	X		
Project Reporting	X	X	X		
Time				X	

The rest of the models have object and capability security.

- 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
- Contracts and Opportunities

Organization Security

There are models in Costpoint Business Intelligence that can leverage the Organization Security settings in Costpoint. If model 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 organizations.

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 Costpoint Business Intelligence 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.

To apply the Organization security by module, you must also set the following two conditions on the Manage BI Settings screen:

- **Enable CP and Planning Model Security** is set to **Yes** and
- **Use CP Organization Security by Module** is set to **Yes**

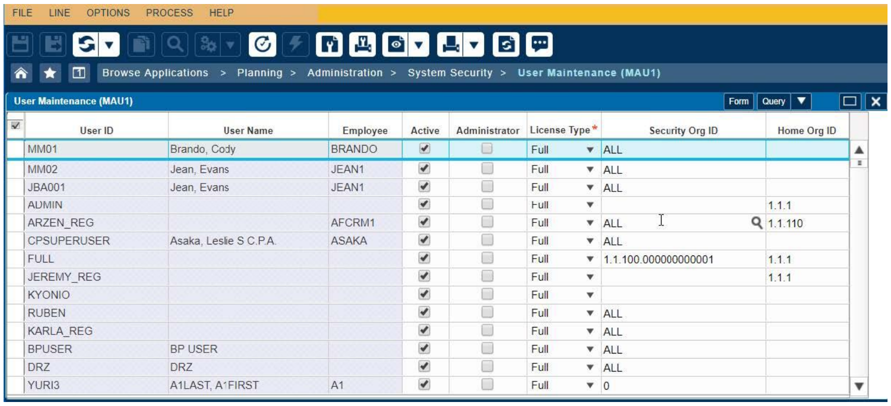
In case the **Enable CP and Planning Model Security** is set to **Yes** and the **Use CP Organization Security by Module** is set to **No**, organization security will still apply for the secure packages which are listed in the following table. The type of module and organization used per package are presented as well.

Secured Package	Module Security Profile Used	Organization Secured
Accounts Receivable	AR	Owning Org
Accounts Payable	AP	Performing Org
General Ledger	GL	Performing Org
Project Reporting	PJ	Owning Org
Project Analysis	PJ	Owning Org
Procurement	PO	Organization may vary
Materials	IN	Organization may vary
Manufacturing	PC	Organization may vary
Time	(Not applicable)	(Not applicable)

Organization Security in Costpoint Planning

The Project Planning model in Costpoint Business Intelligence leverages the Organization/Project Security settings in the Costpoint Planning module. Costpoint Planning (formerly known as 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.


FILE
LINE
OPTIONS
PROCESS
HELP
Browse Applications > Planning > Administration > System Security > User Maintenance (MAU1)
Form
Query

User Maintenance (MAU1)

☑	User ID	User Name	Employee	Active	Administrator	License Type*	Security Org ID	Home Org ID
	MM01	Brando, Cody	BRANDO	☑	□	Full ▼	ALL	
	MM02	Jean, Evans	JEAN1	☑	□	Full ▼	ALL	
	JBA001	Jean, Evans	JEAN1	☑	□	Full ▼	ALL	
	ADMIN			☑	□	Full ▼		1.1.1
	ARZEN_REG		AFCRM1	☑	□	Full ▼	ALL	1.1.110
	CPSUPERUSER	Asaka, Leslie S C.P.A.	ASAKA	☑	□	Full ▼	ALL	
	FULL			☑	□	Full ▼	1.1.100.000000000001	1.1.1
	JEREMY_REG			☑	□	Full ▼		1.1.1
	KYONIO			☑	□	Full ▼		
	RUBEN			☑	□	Full ▼	ALL	
	KARLA_REG			☑	□	Full ▼	ALL	
	BPUSER	BP USER		☑	□	Full ▼	ALL	
	DRZ	DRZ		☑	□	Full ▼	ALL	
	YURI3	A1LAST, A1FIRST	A1	☑	□	Full ▼	0	

Note: Currently, security in Planning only applies to existing projects and not new business projects. Users will still be able to see all new business projects.

Procedures in Setting Up Organization Security

There are several procedures in setting up the Organization Security:

- Activate/Deactivate the Organization Security by Module
- Manage Organization Security Profiles
- Manage Organization Security Groups
- Update the Organization Security Profiles
- Assign the Organization Security Group to Users
- Apply Organization Security

Warning: Follow the procedures in setting up the Organization Security when you use Model Security in Costpoint BI. If you do not use Model Security, you can skip the Organization Security procedures. Costpoint BI follows the Capability and Object security instead.

Activate/Deactivate the Organization Security by Module

Before you start to apply organization security, you must first enable the modules and applications of which you want to apply this type of security through the Activate/Inactivate the Organization Security by Module (SYSMORGFN) screen.

Perform this procedure if the **Use CP Organization Security By Module** is set to **Yes** on the Manage BI Settings (BIMCERSETTINGS) screen.

To enable organization security in the modules and applications:

1. Go to **Administration » Security » Organizational Security » Activate/Inactivate Organization Security By Module**.
2. In the **Modules** table window, search for the module that you like to apply organization security. Select the **Apply Org Security** check box for that module.

   The applications for the selected module will appear in the **Applications** table window.

3. In the **Applications** table window, search for the application that you like to apply organization security. Select the **Apply Org Security** check box for that application. Repeat this step until organization security is set for all the applications in the module.
4. Click **Save**.
5. Repeat steps 2 to 4 until organization security is set in all necessary modules and applications.

> **Note:** To know more about the description of the fields on the Activate/Inactivate Organization By Module screen, see the Costpoint online help. You can access the help by pressing **SHIFT+F1** or go to **Help » Help** menu while the said screen is being displayed**.**

Manage Organization Security Profiles

Next step is to create organization security profiles and assign the organizations where they will be applied. You will need to create the profiles and use them when you establish the organization security groups.

For example, there are two top-level organizations in a company, Apple & Bartlett and ACME.

The ALLAB org security profile is assigned to Apple & Bartlett that has access to all organizations that start with 1 org ID, while ALLACME is assigned to ACME that has access to 2.

Profile ID	Profile Name	Relation	Org ID	Org Name	Apply Org Security
ALLAB	All Orgs in Apple & Bartlett	Begins with	1	Apple & Bartlett, Inc.	Yes
ALLACME	All ACME	Begins with	2	ACME	Yes
ORG101	Org 101 R&D	Equals	1.01	A&B Research & Development	Yes
ORG102	Org 102 Marketing	Equals	1.02	A&B Marketing	Yes
ORG201	Org 201 R&D	Equals	2.01	ACME Research & Development	Yes

ORG101 and ORG102 are organizations within Apple & Bartlett, while ORG201 belongs to ACME.

Create the Organization Security Profiles

To create the organization security profiles:

1. Go to **Admin » Security » Organizational Security » Manage Organization Security Profiles**.
2. Click **New** to start adding a profile.
3. Enter the **Profile ID** and **Profile Name**. Select the **Apply Org Security** check box and the **Rights Application Method** drop-down list.

> **Tip:** Press **SHIFT+F1** or go to **Help » Help** menu to know more about the description of the fields on this screen.

4. On the **Assign Organizations to Profile** table window, click **New**.
5. Enter the Organization of which you want to apply this organization security profile.
6. Click **Save**.
7. Repeat steps 2 to 6 until all organization security profiles are added.

Manage Organization Security Groups

In this procedure, you will assign organization security profiles to each module by creating organization security groups.

Using the Apple & Bartlett and ACME examples in the previous section, let us create org security groups. For example, the Engineering group in Apple & Bartlett may only see information for the Research & Development group. We will use the ORG101 org security profile for all modules.

Organization Security Profile				
Profile ID	Profile Name	Relation	Org ID	Org Name
ORG101	Org 101 R&D	Equals	1.01	A&B Research & Development

Organization Security Group				
Org Sec Group	Name	Module	Org Sec Profile	Profile Name
ENGAB	Engineering Group for A&B	*All modules*	ORG101	Org 101 R&D

Another group in Apple & Bartlett, the Federal Division group, may see all projects in the organizations. In this case, we can use the ALLAB org security profile and assign to all modules.

Organization Security Profile				
Profile ID	Profile Name	Relation	Org ID	Org Name
ALLAB	All Orgs in Apple & Bartlett	Begins with	1	Apple & Bartlett, Inc.

Organization Security Group				
Org Sec Group	Name	Module	Org Sec Profile	Profile Name
FEDDIV	Federal Division	*All modules*	ALLAB	All Orgs in Apple & Bartlett

Create the Organization Security Group

To set the organization security groups:

1. Go to **Admin » Security » Organizational Security » Manage Organization Security Groups**.
2. Click **New** to start adding an organization security group.
3. Fill out the fields on screen. Press **SHIFT+F1** to open the help and to know more about these fields.
4. In the **Organization Security Profile to Assign** field, select a profile. Click the **Assign Profiles** button to apply the selected profile to all modules in Costpoint. This button also populates the **Assign Profiles to Modules** table window.
5. In the **Assign Profiles to Modules** table window, see if you like to change any of the profiles assigned to a module.
6. Click **Save**.
7. Repeat steps 2 to 6 until all Organization Security Groups are created.

Update the Organization Security Profiles

After updating and creating new organization security profiles, you need to run the Update Organization Security Profiles screen process.

To update the organization security profiles:

1. Go to **Admin » Security » Organizational Security » Update Organization Security Profiles**.
2. Click **New** to create a record for the update.
3. Fill out the screen and click **Save**.
4. Go to **Process » Action Menu » Update Org Security Profiles.** Wait until the process completes.

Assign the Organization Security Group to Users

Prerequisite: The organization security groups that you will assign to users should already exist and have been entered through the Manage Organization Security Groups screen.

To assign an organization security group to a user:

1. Go to **Admin » Security » System Security » Manage Users**.
2. Enter or select, the **User Name** that you like to assign to an organization security group.
3. Click the **Company Access** subtask and click **New** to add a line.
4. Enter the details including the **Org Security Group ID** that you like to assign to the user.
5. Click **Save**.
6. Perform steps 2 to 5 for the other users.

Apply Organization Security

Next, enable organization security in Costpoint through the Configure System Settings (SYMSETNG) screen.

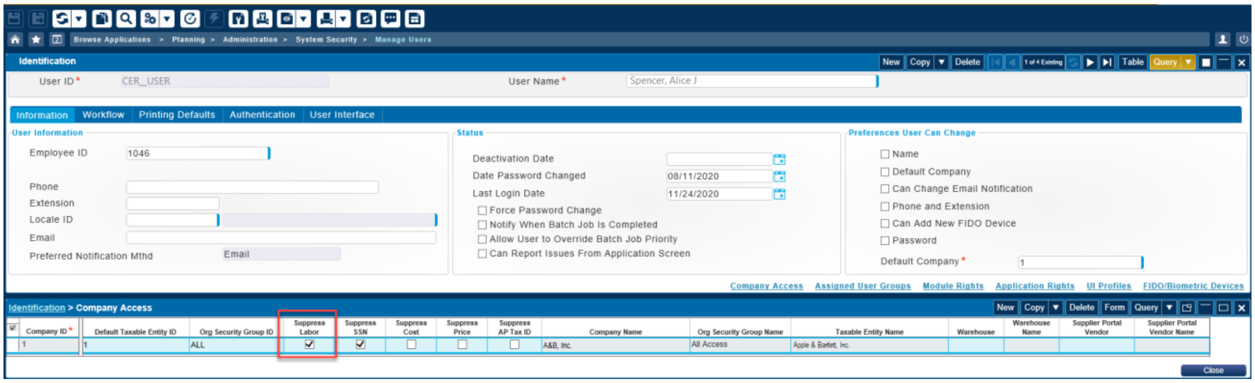
Note: The Configure System Settings screen controls the Costpoint settings and is separate from Costpoint BI. The system settings in Costpoint BI is controlled through the Manage BI Settings (BIMCERSETTINGS) screen.

To turn on organization security in Costpoint:

1. Go to **Admin » System Administration » System Administration Controls » Configure System Settings**.
2. Select the **Apply Organization Security** check box.
3. Click **Save**.

Labor Suppression

The Project model will suppress labor if the **Suppress 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.



Identification

User ID * CER_USER

User Name * Spencer, Alice J

User Information

Employee ID 1046

Phone

Extension

Locale ID

Email

Preferred Notification Mthd Email

Status

Deactivation Date

Date Password Changed 08/11/2020

Last Login Date 11/24/2020

☐ 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

☐ Name

☐ Default Company

☐ Can Change Email Notification

☐ Phone and Extension

☐ Can Add New FIDO Device

☐ Password

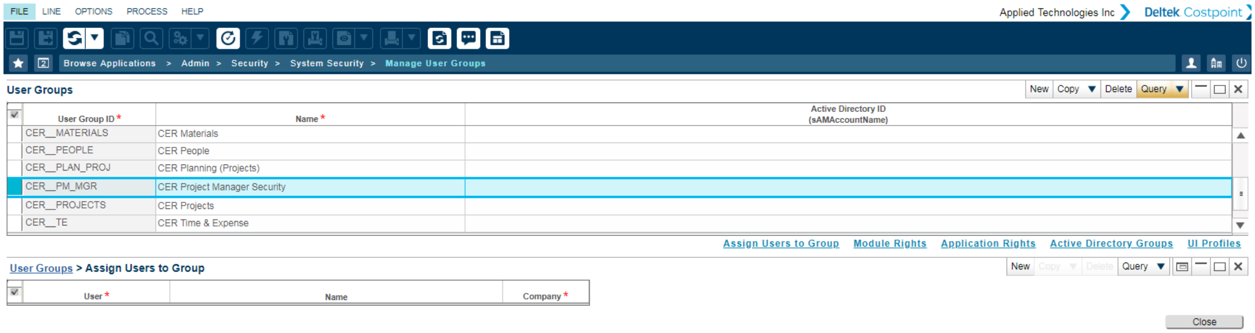
Default Company * 1

Identification > Company Access

Company ID *	Default Taxable Entity ID	Org Security Group ID	Suppress Labor	Suppress SSN	Suppress Cost	Suppress Price	Suppress AP Tax ID	Company Name	Org Security Group Name	Taxable Entity Name	Warehouse	Warehouse Name	Supplier Portal Vendor	Supplier Portal Vendor Name
1	1	ALL	☑	☑	☐	☐	☐	A&B, Inc.	All Access	Apple & Barlett, Inc.				

Project Security

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.



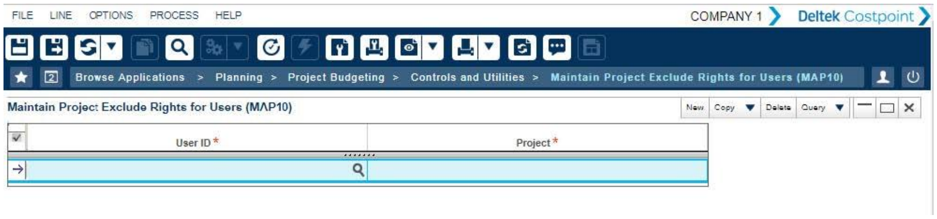
User Groups

User Group ID *	Name *	Active Directory ID (sAMAccountName)
CER__MATERIALS	CER Materials	
CER__PEOPLE	CER People	
CER__PLAN_PROJ	CER Planning (Projects)	
CER__PM_MGR	CER Project Manager Security	
CER__PROJECTS	CER Projects	
CER__TE	CER Time & Expense	

User Groups > Assign Users to Group

User *	Name	Company *

For Projects Security in Costpoint Planning, 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.


FILE
LINE
OPTIONS
PROCESS
HELP
COMPANY 1
Deltek Costpoint
Browse Applications > Planning > Project Budgeting > Controls and Utilities > Maintain Project Exclude Rights for Users (MAP10)
Maintain Project Exclude Rights for Users (MAP10)
New
Copy
Delete
Query
User ID*
Project*

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.

To restrict access to projects in the Projects, General Ledger, and the Accounts Receivable folders 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 Costpoint Business Intelligence, 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 Project 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__PM_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:

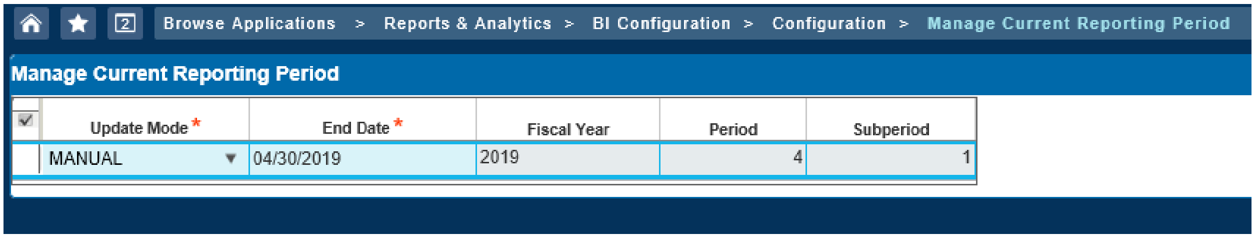
1. Log on to Costpoint and open the Manage User Groups (SYMGRP) screen.
2. Query the CER User Group to which you want to assign existing users.

   > **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.

5. On the completed Security Planning Template, open the **Object Security** tab and use it as reference. Look for the records for the CER User Group that you just selected on the Manage Users Groups screen.
6. On the Manage User Groups screen, enter or select the user and enter the **Company**.Click **Save & Continue**.
7. Repeat steps 2 to 6 until you have assigned all users to the CER User Groups.

Step 6: Set Up Current Reporting Period


2
Browse Applications > Reports & Analytics > BI Configuration > Configuration > Manage Current Reporting Period

Manage Current Reporting Period

☑	Update Mode *	End Date *	Fiscal Year	Period	Subperiod
	MANUAL ▾	04/30/2019	2019	4	1

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

To set up the Costpoint BI current reporting period:

1. In Costpoint, launch the Manage Current Reporting Period (BIMRPTCURPD) application (**Reports and Analytics** » **BI 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:** Deltek recommends 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. 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 Planning should also set to the same period. This screen is found at **Planning » Administration » Administration Controls » Maintain Current Period**. This setting controls the updating of the reporting tables and is separate from the Costpoint Business Intelligence Current Period.

Field	Description
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.

3. Click **Save**.

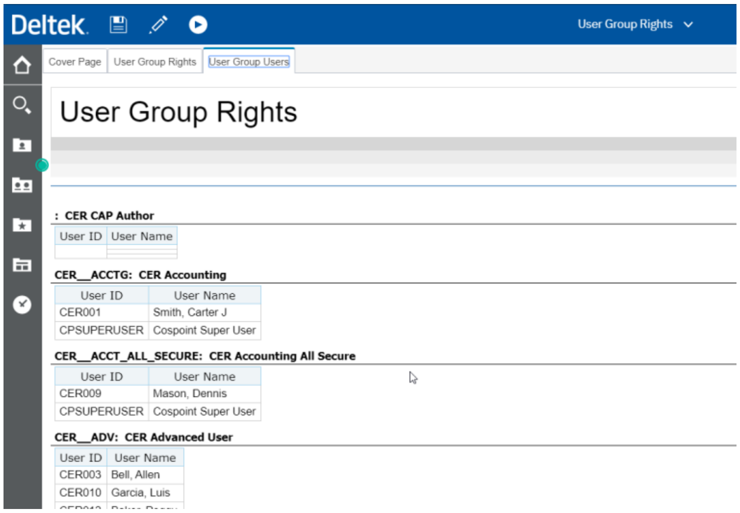
Step 7: Validate User Groups

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 Costpoint BI, 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 completed Security Planning Template. Check if all users are accounted for.



User Group Rights

: CER CAP Author

User ID	User Name

CER__ACCTG: CER Accounting

User ID	User Name
CER001	Smith, Carter J
CPSUPERUSER	Cospoint Super User

CER__ACCT_ALL_SECURE: CER Accounting All Secure

User ID	User Name
CER009	Mason, Dennis
CPSUPERUSER	Cospoint Super User

CER__ADV: CER Advanced User

User ID	User Name
CER003	Bell, Allen
CER010	Garcia, Luis

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
- Save a report to “My Content” folder

Completing these steps finishes the initial setup of Costpoint Business Intelligence.

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