



Deltek

Deltek Costpoint®
Business
Intelligence 8.1
Cloud Setup Guide

November 15, 2022



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 publication contains proprietary information that is protected by copyright. All rights are reserved. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, or translated into another language, without the prior written consent of Deltek, Inc.

This edition published November 15, 2022.

© 2022 Deltek, Inc.

Deltek's software is also protected by copyright law and constitutes valuable confidential and proprietary information of Deltek, Inc. and its licensors. The Deltek software, and all related documentation, is provided for use only in accordance with the terms of the license agreement. Unauthorized reproduction or distribution of the program or any portion thereof could result in severe civil or criminal penalties.

All trademarks are the property of their respective owners.

Contents

About this Guide.....	1
Costpoint Enterprise Reporting to Costpoint BI.....	1
Prerequisites.....	2
Overview.....	4
Check the Model Security Configuration.....	4
Capability Security.....	7
Object Security.....	13
Model or Row Level Security.....	15
Copy the Smart AI Folder to Company Content.....	30
Data Set.....	30
Validate User Groups.....	35
Hidden Analysis Packages and Dashboards.....	36
Unhide Analysis Packages and Dashboards.....	36
Have Users Run and Validate Reports.....	38
Troubleshooting.....	39
Missing AI Assistant.....	39

About this Guide

Welcome to the Costpoint Business Intelligence 8.1 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.

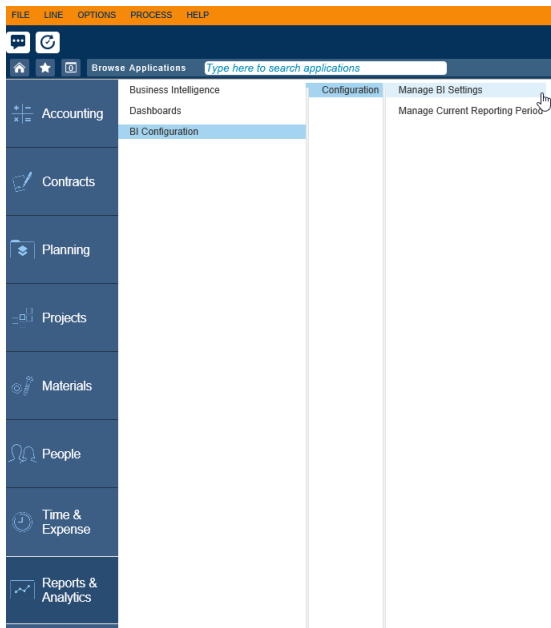
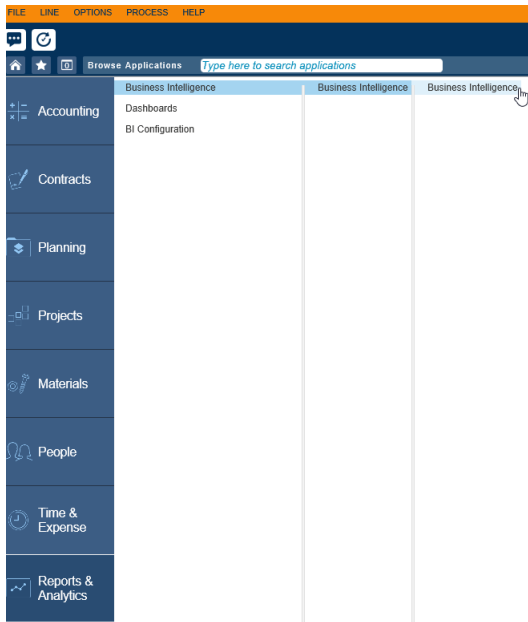
Costpoint Enterprise Reporting to Costpoint BI

Starting in Costpoint 8.0, the name "Costpoint Enterprise Reporting" or "CER" has been changed to "Costpoint Business Intelligence".

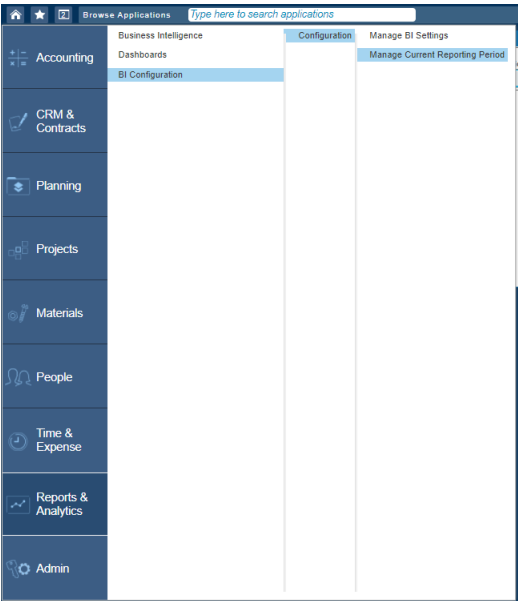
The name was changed to align with the product's capabilities which are beyond reporting. You may still see references to the former name, CER, in some of the names and objects throughout this document. For more details, see [Costpoint Enterprise Reporting Name Change](#).

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 Reporting Period (BIMRPTCURPD).



Prerequisites



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:

- Check the Model Security Configuration
- Complete the Capabilities Security Template
- Complete the Object Security Template
- Complete the Security Template for the CER Project Manager Group
- Assign Users to Costpoint User Groups
- Set Up Current Reporting Period
- Copy the Smart AI Folder to Company Content
- Validate User Groups
- Have Users Run and Validate Reports

Check the Model Security Configuration

The Costpoint, Costpoint Planning, and TE Model security are enabled by default. If you do not want to apply it, you can disable model security in Costpoint's Manage BI Settings (BIMCERSETTINGS) screen. The best practice is to keep the model security on.

Note: Skip this procedure if you want to use model security for your Costpoint Business Intelligence implementation. Remember that model security utilizes settings in Costpoint, Costpoint Planning, and/or T&E. If model security is set to Yes, you must have the necessary setup in place to retrieve any data using the models that have data-level security. For example, when Costpoint model security is enabled, each user must have an assigned organization security group, Time & Expense requires functional roles, and Planning has its own security setup. In addition, parts security is always applied in Business Intelligence when it is used in Costpoint regardless of whether model security is enabled or not.

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 corresponding fields where you want to disable security.

Field	Description
Enable Costpoint and Planning Model Security	Select No to disable model security for the Costpoint and Costpoint Planning models. Model security is enabled by default.

Field	Description
	<p>Note: If you select No, only Model Security is disabled. Capability and Object Security are still in place in Costpoint Business Intelligence. If Parts Security is applied in Costpoint, they are implemented as well regardless of the settings for model security.</p>
Use CP Organization Security By Module	<p>Select No to disable organization security in the new secure models which are:</p> <ul style="list-style-type: none"> ▪ Accounts Receivable ▪ Accounts Payable ▪ Employee ▪ Expense ▪ General Ledger ▪ Labor ▪ Manufacturing ▪ Materials ▪ Procurement ▪ Projects ▪ Subcontractor
Enable T&E Model Security	<p>Select No to disable model security for the Time model.</p>

3. Click **Save**.

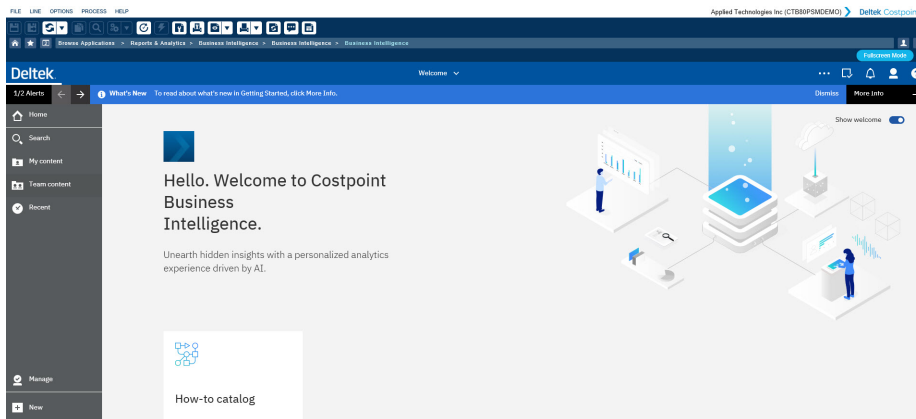
Assign Costpoint Business Intelligence Rights to the Administrator

In order to access Costpoint Business Intelligence, the Administrator will need to be assigned to CER groups in Costpoint Security.

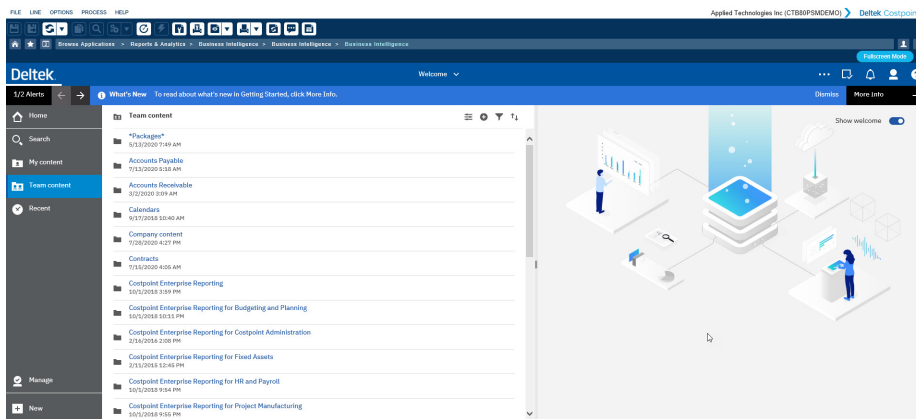
It is recommended that you as Administrator assign yourself initially to CER__Admin and then to CER__ALL.

You as Administrator should then open Business Intelligence to make sure you can access the initial Costpoint Business Intelligence Welcome Screen.

Overview

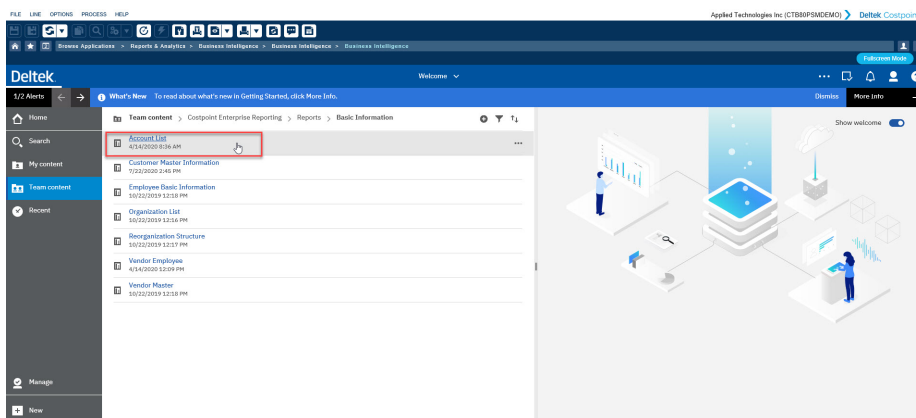


Then, click the Team content folder, and you should see the full folder structure.

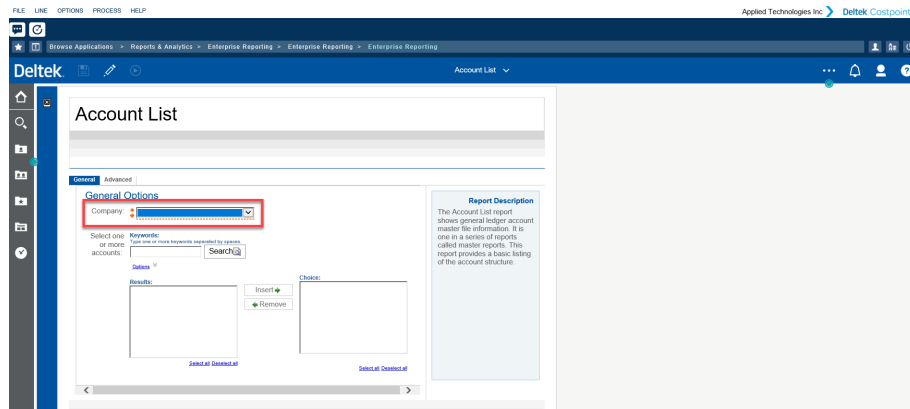


Then, run a report to ensure that you can access Costpoint data. Here is how you can run an Account List Report:

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 Costpoint BI or CER user role, a set of capabilities are assigned that designate the secure features or functions that an end user can perform.

There is a Costpoint BI 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 *	CP BI User *	Advanced CP BI User Lite	Advanced CP BI User *	CP BI Developer	Web Admin	CP BI Admin
Interactive Viewer – Running, Viewing, and Subscribing to Reports	•	•	•	•	•		•
AI Assistant		•	•	•	•		•
Viewing and Authoring Dashboards		•	•	•	•		•
Explorations			•	•	•		•
Interactive Report Authoring			•	•	•		•
Event Studio			•	•	•		•
Data Module				•	•		•
Data Sets				•	•		•
Excel Upload				•	•		•
Framework Manager					•		•
Administration Console						•	•

Consumer* - Legacy license

Costpoint BI User* - Only sold with bundles

Advanced CP BI User* - Customers can assign a regular or lite version of the Advanced Costpoint BI User

Note: The Consumer (CER__CONSUMER) 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 (**in Bundles**) and/or **Advanced CER licenses** instead, you might want to limit the capabilities for some individuals who you do not want to access or create dashboards. CER User is only available in CER Bundles (restricted).

Costpoint cloud customers own the Advanced Costpoint Business Intelligence Bundle where the:

- Total number of licenses matches the number of employees in the Costpoint license
- 95% of users are Costpoint Business Intelligence users
- 5% are Advanced Costpoint Business Intelligence users
- Plus 1 Costpoint Business Intelligence Administrator
- Additional Users can be purchased on an a la carte basis. Additional Users typically bought, are Costpoint Business Intelligence Web Administrator or Costpoint Business Intelligence Developers.

For Costpoint on-premises or those who use a hosted environment, there are a la carte licenses available in addition to the Costpoint Business Intelligence Bundle.

- A la Carte Licenses:
 - Advanced Costpoint Business Intelligence Users
 - Costpoint Business Intelligence Developers
 - Costpoint Business Intelligence Web Admins
 - Costpoint Business Intelligence Administrators
 - A la Carte Licenses can be purchased as Restricted or Full Use
 - Restricted: Deltak Data Sources Only (Excel data as a source is allowed)
 - Full Use: Other 3rd Party data can be used as data sources

License Types

Every Costpoint Business Intelligence user should be assigned to one Costpoint BI user role based on the functions they can perform and the license purchased. Costpoint BI roles are depicted by the prefix CER.

The [Security Planning Template](#) has been provided for planning your capability security to help ensure license compliance.

- **Consumer (CER__CONSUMER):** This user has the least rights, basically someone who can only run and interact with existing reports and dashboards. While you may not own this type of license and have Costpoint BI users instead, you might want to limit the capabilities for some individuals who you do not want to access dashboards.
- **CER User (CER__USER):** This user is someone who can run and interact with reports and can also create dashboards.

- **Advanced CER User (CER__ADV):** In addition to the capabilities of the Costpoint BI 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 Costpoint BI capabilities.

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).

Reports can run in limited interactivity or full interactivity mode. When a report is set to run with limited interactivity, the report runs in the Costpoint BI Viewer. Report viewers can answer prompts, drill up, drill down, and drill through. When a report is set to run with full interactivity, the report runs in the Costpoint BI interactive viewer. By clicking various icons in the report object toolbar that appears when an object is selected, the functions that you can perform on the report are Sort, Group, Summarize, Drill, Add Calculations, Filter, and Interact with Charts. Hide or Swap rows and columns in a crosstab report.

For example, you 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, from a list to a chart
- Save the changes as new report
- Interact with charts

AI Assistant is an embedded assistant in Costpoint BI, leveraging IBM's Watson that supports text-based input where you can gain quick insights into data and simplify analytics. In just a few steps, you can access key data sources, create visualizations, and drag them onto the Exploration or Dashboard canvas.

Explorations offer a flexible workspace where to explore data from a data module or an uploaded excel data. There is also the option to explore an existing visualization from a dashboard, story, or report. Correlated insights are represented by a green icon with a number on either the x-axis or y-axis of a visualization. The system analyzes the data and identifies interesting items. The relationship diagram plots these fields based on a statistical evaluation of related items. The relationship diagram is not a picture of the data model. However, the model might be an influencing factor in the analysis.

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

Interactive Dashboard Viewing: Costpoint BI provides dashboards and stories to communicate identified insights and analysis. By leveraging this capability, you can view and interact with dashboards and stories by filtering, selecting within or changing visualizations, or drilling through and to reports.

Interactive Dashboard Authoring: Costpoint BI provides dashboards and stories to communicate identified insights and analysis. Authors can create dashboards and stories from a blank canvas or using the AI Assistant in using Packages, Data Modules, or uploaded Excel files and share with Dashboard Users.

Dashboards & Stories: A dashboard helps monitor events or activities at a glance by providing key insights and analysis about the data on one or more pages or screens. A story however, is a type of view that contains a set of scenes that are displayed in sequence over time. Stories are similar to dashboards because they also use visualizations to share revealed insights. Stories differ from dashboards because they provide an over-time narrative and can convey a conclusion or recommendation.

Event Studio is a web-based product for creating and managing agents that monitor data and perform tasks when the data meets predefined thresholds. It can be used to notify your key decision makers of events as they happen, in order to make timely decisions. You also have the ability to create agents that monitor your organization's data to detect occurrences of business events. An event is a situation that can affect the success of a business.

Data Module: Costpoint BI provides web-based, self-service data modeling capabilities. Data modeling can help fuse many sources of data together, including relational databases, Microsoft Excel spreadsheets, text files, and so on. Using these sources, a data module is created that can then be used in reports, dashboards, or explorations. Enhance a data module by creating calculations, defining filters and navigation paths, and more. After saving a data module, other users can access it to create BI content. Save the data module in a folder that users, groups, and roles have appropriate permissions to access.

Data Sets are customized collections of data items that are used frequently. As updates are made to the data set, the dashboards, stories, or explorations that use that data set are also updated for the next time. You can create data sets from Framework Manager Packages or data modules, and use as sources to create dashboards, stories, explorations, and data modules. It's not an option to create a report directly from a data set. However, to use the data from the data set in a report, create a data module from the data set, and then use the data module as a source for a report.

Excel Upload: To conduct a quick analysis or create simple visualizations with data files (Excel, delimited files), users can upload the files to Costpoint BI on their own. The data files must meet size and structure requirements, and the data in the files must be in a simple columnar format. Pivot tables or crosstabs are not supported.

Framework Manager is used to create business model of metadata derived from one or more data sources. It is a Windows-based tool which is used to publish the business models to Cognos BI in the form of packages which can be used for analytical reporting and analysis.

Administration Console: BI Administrators can perform server administration, data management, security and content administration, activities management, and services administration.

Note: Administration capabilities are limited in the Cloud since Deltak Cloud Operations will perform certain tasks.

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.

The succeeding table display the detailed capabilities for users.

For entries with double asterisks (**), it signifies that user-defined SQL is turned off for the following packages. This prevents unauthorized users to bypass security through SQL.

For entries with an asterisk (*), it signifies that Everyone has the capability. If you establish new Roles, they will receive this capability.

- Accounts Receivable
- Accounts Payable
- Employee
- Expense
- General Ledger
- Labor
- Materials
- Manufacturing
- Procurement
- Project Reporting
- Project Planning Reporting
- Subcontractor Management
- Time

Detailed Capabilities by Role for Cloud Users

Capabilities	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
Run activities and schedules						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
Collaborate		ACCESS	ACCESS	ACCESS	ACCESS		ACCESS
Allow collaboration features			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
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
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
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 (Traverse)	Custom (Traverse)	Custom (Traverse)	ACCESS	ACCESS		ACCESS
User Defined SQL**	Custom (Traverse)	Custom (Traverse)	Custom (Traverse)	ACCESS	ACCESS		ACCESS
Save to Cloud				ACCESS	ACCESS	ACCESS	ACCESS
Manage Connections						ACCESS	ACCESS
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 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

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 Costpoint Business Intelligence 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 Costpoint BI or CER user groups included in your deployment. The user groups are based on Costpoint domains. The succeeding table describes the user groups that have permissions to the objects in the Deltek content. The permissions of most parent folders or packages will apply to any content contained within.

For example any user assigned to the **CER Accounting** user group will be able to see both secured and non-secured legacy content as indicated in the following table.

Alternatively, a user assigned to **CER Accounting All Secure** will only be limited to the secured Accounting content found under the **Team Content** folder plus the secured Accounting packages.

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 must be saved in the **Company content** folder.

Note: Because future Costpoint Business Intelligence upgrades may overwrite the Deltek folders, it is best practice to use the **Company content** folder to store customization.

Overview

Object	CEB Accounting	CEB Accounting All Secure	CEB Accounts Receivable Secure	CEB Accounts Payable Secure	CEB Employee Secure	CEB General Ledger Secure	CEB All	CEB Contracts	CEB Labor Secure	CEB Projects	CEB Projects Secure	CEB Planning (Projects)	CEB Planning (Projects) Secure	CEB Project Manager	CEB People	CEB Subcontractor Management Secure	CEB Time & Expense	CEB Time Secure	CEB Expense Secure	CEB Materials	CEB Materials Secure	CEB Materials Manufacturing All Secure	CEB Procurement Secure	CEB Manufacturing Secure	CEB CP Admin	CEB Executive Secure
Team Content > "Packages" >	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Accounts Payable	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Accounts Receivable	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Contracts Reporting	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Employee	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Expense	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
General Ledger	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Labor	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Manufacturing	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Materials	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Procurement	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Project Planning Reporting	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Project Reporting	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Subcontractor Management	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
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	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Calendars	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
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	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
CRM & Contracts	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Employee	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Executive	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Expense	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
General Ledger	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
ICS	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Labor	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Manufacturing	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Materials	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Planning	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Procurement	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Projects	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
SOX Controls Reporting	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Subcontractor Management	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Time	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Company Content > Smart AI >	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Executive	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
People	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Planning	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Procurement	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Projects	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Data Modules	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Dimensions -	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Accounts Receivable	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
General Ledger	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
HR Mgmt	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Labor History	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Planning	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Project Summary (PSR)	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Purchase Orders	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
Resource Mgmt	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	

A user must belong to at least one of these groups in order to see any Deltak 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.

Company Content

Cloud users are required to have the **Company content** folder to store custom content that is only accessible to them.

The Company content folder is included in your navigation pane that you can use for your company's own folder structure.

Administrators have full rights to this folder where they can assign and manage permissions.

Complete the Object Security Template

The Object Security Template is part of the Security Planning Template which is included in 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 Costpoint Business Intelligence users by name.

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 [Complete the Security Template for the CER Project Manager Group](#) section.

3. Designate the user group that 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, Costpoint Planning, and Time & Expense settings.

There are different aspects of model security.

1. **Organizational 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 or performing organization are secured. If Organizational security is not established in Costpoint or Costpoint Planning, Costpoint Business Intelligence models will not be able to restrict data by organization or company.

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

Note: Multi-company security for Costpoint and Costpoint Planning is not enforced in Costpoint Business Intelligence.

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 Business Intelligence, 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 to the level that the project manager is assigned.

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 as established in Time & Expense.

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 with the exception of the Contracts Reporting package.

Row and Organization Security Matrix					
Package	Organization	Project/PM	Labor Suppression	Functional Role	Parts
Accounts Payable	Performing Org				
Accounts Receivable	Owning Org	✓			
Contracts Reporting					
Employee	Home Org		✓		
Expense				✓	
General Ledger	Performing Org		✓		
Labor	Home Org		✓		
Manufacturing	Org may vary				✓
Materials	Org may vary				✓
Procurement	Org may vary				✓
Project Reporting	Owning Org	✓	✓		
Project Planning Reporting	Owning Org	✓	✓		
Subcontractor Management	Owning Org				
Time				✓	

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
Employee	EM	Home Org
General Ledger	GL	Performing Org
Labor	LD	Home 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
Subcontractor	SM	Owning Org
Time	N/A	(Not applicable)
Expense	N/A	(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 model.

The 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.

FILE LINE OPTIONS PROCESS HELP							
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
	MM01	Brando, Cody	BRANDO	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Full	ALL
	MM02	Jean, Evans	JEAN1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Full	ALL
	JBA001	Jean, Evans	JEAN1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Full	ALL
	ADMIN			<input checked="" type="checkbox"/>	<input type="checkbox"/>	Full	ALL
	ARZEN_REG		AFCRM1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Full	ALL
	CPSUPERUSER	Asaka, Leslie S C.P.A.	ASAKA	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Full	ALL
	FULL			<input checked="" type="checkbox"/>	<input type="checkbox"/>	Full	1.1.100.0000000000001
	JEREMY_REG			<input checked="" type="checkbox"/>	<input type="checkbox"/>	Full	ALL
	KYONIO			<input checked="" type="checkbox"/>	<input type="checkbox"/>	Full	ALL
	RUBEN			<input checked="" type="checkbox"/>	<input type="checkbox"/>	Full	ALL
	KARLA_REG			<input checked="" type="checkbox"/>	<input type="checkbox"/>	Full	ALL
	BPUSER	BP USER		<input checked="" type="checkbox"/>	<input type="checkbox"/>	Full	ALL
	DRZ			<input checked="" type="checkbox"/>	<input type="checkbox"/>	Full	ALL
	YURI3	A1LAST, A1FIRST	A1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	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

Create the Organization Security Profiles through the Manage Organization Security Profiles screen.

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, 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

Use the Manage Organization Security Groups screen to set up the groups.

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

Use the Manage Users screen to assign organization security groups to users.

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. 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 and the Costpoint and Planning model security is turned on. It is important that at least one Org is

Overview

assigned to the Org Security Group. If no orgs are assigned, the user will not be able to see any data.

The screenshot shows the 'Identification' section of the Delttek user management interface. The user 'CER_USER' (Spencer, Alice J) is selected. The 'Company Access' tab is active, showing a table of company assignments. The 'Suppression' column for 'ALL' is checked, indicating that the user is not allowed to see any data.

Company ID	Default Taxable Entity ID	Org Security Group ID	Suppression	Suppression S/S	Suppression Cost	Suppression Price	Suppression A/P Tax ID	Company Name	Org Security Group Name	Taxable Entity Name	Warehouse	Warehouse Name	Supplier Portal Vendor	Supplier Portal Vendor Name
1	1	ALL	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	ASB, Inc.	All Access	Apple & Sordis, 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. Project security is applicable to the Accounts Receivable, Project Analysis, Project Planning Analysis, Project Planning Reporting, or Project Reporting folders.

To restrict access to projects in the Accounts Receivable, Project Analysis, Project Planning Analysis, Project Planning Reporting, or Project Reporting 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 is used to determine project rights.

The screenshot shows the 'User Groups' section of the Delttek user management interface. The 'CER_PM_MGR' group is selected, which is assigned to the 'CER Project Manager Security' role. Below the table, there is a section for 'Assign Users to Group' with a 'User' and 'Company' dropdown menu.

User Group ID	Name	Active Directory ID
CER_MATERIALS	CER Materials	
CER_PROFILE	CER Profile	
CER_PLAN_PROD	CER Planning (Projects)	
CER_PM_MGR	CER Project Manager Security	
CER_PROJECTS	CER Projects	
CER_TE	CER Time & Expense	

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.

The screenshot shows the 'Maintain Project Exclude Rights for Users (MAP10)' screen. It has a table with columns for 'User ID' and 'Project'. The 'User ID' field is currently empty, and the 'Project' field is also empty.

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.

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.

Functional Role Security

Functional Role security is currently supported in the Time model.

As a resource manager using Time & Expense, certain functional roles may be assigned such as having rights to view timesheets or see data for assigned projects. The data in reports are based on the configuration made on screens where functional roles are set up. Some examples of these screens are the Functional Roles (ADMFUNCTIONALROLE) and Security Roles (ADMSECURITYROLE).

On the Functional Roles screen, timesheet rights may be set up for each type of role.

On the Security Roles screen, you can limit data access of employees to projects assigned to them through the **Charge Level Security** check box.

When the **Apply Charge Level Security** check box is selected, the user for the functional role, for example Employee, will be restricted to projects where Employees have rights.

A user may be assigned to multiple roles over a single project. When this happens, Costpoint BI will check if the user has rights to view timesheets for the project and will grant access if needed.

Sample Scenario: Functional Role Security

For example, Alice is assigned to a functional role that has rights to view timesheets of select employees and projects.

Alice can see the timesheets for the following employees and projects:

Employees
EMPL = Phil
EMPL = Niki
Projects
PROJ = 0001
PROJ = 0003

The records in the database are the following:

Timesheet Date	EMPL	PROJECT	ACCT	HRS	Charge Level Security = Y	Charge Level Security = N
3/1/2020	Phil	0001	50-100	20	O	#
3/1/2020	Phil	0002	50-100	20	O	#
3/15/2020	Phil	0001	50-100	40	O	#
3/1/2020	Rick	0003	50-100	40	#	#
3/15/2020	Rick		50-100	40		
3/1/2020	Niki		50-100	10	O	O
3/1/2020	Niki	0005	50-100	30	O	#
3/15/2020	Niki	0002	50-100	40	O	#
3/1/2020	Heather	0001	50-100	20	#	#
3/1/2020	Heather	0002	50-100	20		#
3/15/2020	Heather	0005	50-100	30		#
3/15/2020	Heather		50-100	20		

- O - When Charge Level Security is applied, Alice will see all the rows of data for her employees Phil and Niki, plus all the rows of data for her projects 0001 and 0003.
- # - When Charge Level Security is NOT applied, Alice will have access to all projects plus rows of data for her employees.

Note: If all transactions require projects, Alice will see all records when charge level security is not applied.

Parts Security

The International in Arms Regulations or ITAR controls the export of defense and military technologies.

ITAR information includes the list of military and defense components and parts stored in databases, which are sensitive data that government contractors and developers work on. Costpoint BI supports Parts Security in report and dashboards, so as to restrict data to only those who need to access them.

Parts Security is enabled through the Configure Product Definitions Settings screen (PDMITRU) in **Materials » Product Definition » Product Definition Controls**. Select the **Use Part Data Security Controls** check box to enable Parts Security.

When Parts Security is enabled, the user must also belong to an active Security Group that is defined through the Manage Security Groups screen (PDMSCGRP) in **Materials Product Definition Part Data Security**. Part data are not accessible to inactive Security Groups.

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 Costpoint Business Intelligence users by name that will be part of the CER Project Manager (CER__PM_MGR) group.
3. Save the completed template for reference later.

Assign Users to Costpoint User Groups

After completing the plan and templates for the various security elements, you can start with the actual configuration set up 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 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. Enter or select the user and enter the **Company**.
6. Click the **New** button in the **Assign Users to Groups** table window.
7. Enter the default super user, for example, CPSUPERUSER, and enter the **Company**.

Note: The super user or CPSUPERUSER should be assigned to all CER User Groups as well. See the [Costpoint BI User Group List](#) topic as reference of all available CER User Groups.

8. Click **Save & Continue**.
9. Repeat steps 2 to 8 until you have assigned all users to the CER User Groups.

Costpoint BI User Group List

The CPSUPERUSER must be added to all CER User Groups.

User Group	User Group Name	Company
CER__ACCT_ALL_SECURE	CER Accounting All Secure	ALL
CER__ACCTG	CER Accounting	ALL
CER__ADMIN	CER Cloud Administrator	ALL
CER__ADV	CER Advanced User	ALL
CER__ADV_LITE	CER Advanced Lite	ALL
CER__ALL	CER All	ALL
CER__AP_SECURE	CER Accounts Payable Secure	ALL
CER__AR_SECURE	CER Accounts Receivable Secure	ALL
CER__CONSUMER	CER Consumer	ALL
CER__CONTRACTS	CER Contracts	ALL
CER__CP_ADMIN	CER CP Administrator	ALL
CER__DEV	CER Developer	ALL
CER__EMPL_SECURE	CER Employee Secure	ALL
CER__EXEC_SECURE	CER Executive Secure	ALL
CER__EXPENSE_SECURE	CER Expense Secure	ALL
CER__GL_SECURE	CER General Ledger Secure	ALL
CER__HR	CER HR	ALL
CER__LABOR_SECURE	CER Labor Secure	ALL

User Group	User Group Name	Company
CER__MATERIAL_SECURE	CER Materials Secure	ALL
CER__MATERIALS	CER Materials	ALL
CER__MFG_SECURE	CER Manufacturing Secure	ALL
CER__MM_ALL_SECURE	CER Materials Manufacturing All Secure	ALL
CER__PEOPLE	CER People	ALL
CER__PLAN_PRJ_SECURE	CER Planning (Projects) Secure	ALL
CER__PLAN_PROJ	CER Planning (Projects)	ALL
CER__PM_MGR	CER Project Manager Security	ALL
CER__PROCURE_SECURE	CER Procurement Secure	ALL
CER__PROJ_SECURE	CER Projects Secure	ALL
CER__PROJECTS	CER Projects	ALL
CER__SUBK_SECURE	CER Subcontractor Management Secure	ALL
CER__TE	CER Time & Expense	ALL
CER__TIME_SECURE	CER Time Secure	ALL
CER__USER	CER User	ALL

Set Up Current Reporting Period

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

FILE LINE OPTIONS PROCESS HELP

[Browse Applications](#) > [Reports & Analytics](#) > [Reporting Configuration](#) > [Configuration](#) > [Manage Current Reporting Period](#)

Manage Current Reporting Period

<input checked="" type="checkbox"/>	Update Mode *	End Date *	Fiscal Year	Period	Subperiod *
	MANUAL	01/31/2016	2016	1	4

To set up the Costpoint Business Intelligence 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 or Manual . Deltek recommends that you select Manual , so you can set the End Date , Fiscal Year , Period , and Subperiod of your choice.

Field	Description
	<p>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.</p> <p>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, 2021, the end date will be July 31, 2021. This is because it is the closest end date and is greater than July 10, 2018. Do note however that the End Date, Fiscal Year Period, Period, and Subperiod fields may not display the corresponding period dates, but Costpoint BI will consider the system date in report and dashboard creation.</p> <p>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.</p>
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**.

Copy the Smart AI Folder to Company Content

Copy Smart AI from **Team content** to **Company content** to provide Smart AI content to qualified users.

Log in as CER__ADMIN or administrator.

To copy Smart AI from Team content to Company content:

1. In Costpoint BI, go to **Team content » Smart AI Admin**.
2. Right-click or click the adjacent ellipsis (...) on the **Smart AI** folder and click **Copy or Move**.
3. On the **Copy or move:** dialog box, select a destination within **Company content** that you like to copy the folder into.
4. Click **Copy to** and a confirmation message appears when the folder has been successfully copied.

Smart AI uses data sets as source for dashboards and reports. Deltek recommends that you regularly refresh the content of data sets. To know more about data sets and the procedure to refresh them, see [Data Set](#) within this document.

Data Set

You can leverage data sets when you have data that are frequently used in reports or dashboards.

Using data sets also improve performance when generating reports and dashboards, since data comes from in-memory processing and not directly from the database. An administrator can use the pre-built jobs that refresh the data of data sets or set schedules as to when to refresh the data that will align with your report generation activities.

You cannot create reports directly from data sets, but you can create a data module from a data set. And then, use that data module as source for your report. You can also use data sets for dashboards and explorations.

The key building blocks are data sets of two categories, dimensional and transactional. Data Sets are extractions of data from Costpoint into a file format, while it is called Parquet format, which is similar to a flat file, rows and columns of data that are stored in a highly compressed and indexed format. For Smart AI, the sources are the standard Costpoint BI packages.

The Parquet format is great for performance when querying this data for a report, dashboard or exploration. In the Smart AI model, dimensional data sets are based on the key architectural components (Project, Account, Company/Organization) of Costpoint as well as other attributes (Customer, Vendor, fiscal periods, and others) that will help define the actual data in Costpoint.

The actual data is contained in the transactional data sets which include the measures and metrics that are important to understand performance. Examples of transactional data sets are General Ledger detail, labor detail, PSR data, and so on. These data sets will include Hours and Dollars that relate to the dimensional data. So where a General Ledger line will have an account

number, the dimensional Account data set will include fields such as the Account Name, Account Levels, and Active Flag to expand the analysis of the data.

Data Sets are refreshed on a regular basis, typically creating a job that is scheduled to update multiple data sets periodically which is usually on a daily basis. The job will run the data set update to query Costpoint and update the data.

To learn more about data set refresh, see [Refresh Data Sets](#), [Schedule Data Set Refresh](#), or [Create a Job to Refresh Data Sets](#) sections in this guide.

Pre-Built Jobs in Smart AI

Jobs that can refresh all transactional and dimensional data sets are available in Smart AI. To get the latest data for Smart AI and its dashboards, you need to refresh your data set.

The pre-built jobs to refresh data sets are located in **Team content » Smart AI Admin » Smart AI » *Jobs***. These jobs are categorized into two:

- **Refresh All Dimensional Data Sets Job:** Dimensional data sets contain descriptive information or attributes. They also contain information that some may also refer to as maintenance tables. Examples of these are list of Accounts, Organizations, and Projects.
- **Refresh All Transactional Data Sets Job:** Transactional data sets are information in business transactions. For example, the Purchase Order data set contains information such as the items ordered, the number of items, the amount, needed date, and delivery date.

In Smart AI, the dimensional and transactional data sets are listed in the following table.

Dimensional Data Sets	Transactional Data Sets
Accounts	AR Summary Data
Companies	GL Summary Data
Customers	Labor History Data
Employee Certifications	Planning Data
Employee Degrees	Project Summary (PSR) Data
Employee Salary Information	Purchase Order Data
Employee Skills	Receipt Data
Employee UDEFs	Resource Management Data
Employees	
GL Financial Statement Lines	
Items	
Organizations	
Planning Project UDEFs	
Planning Projects	
Project UDEFs	

Dimensional Data Sets	Transactional Data Sets
Projects	
Relative Fiscal Periods	
Resources	
Subperiods	

To run a job, simply click the ellipsis (...) adjacent to it and select **Run as**. And then, follow the prompts on the dialog box that will display and click **Run**.

Refresh Data Sets

If you only need to refresh one or few data sets and not all, you can do so by selecting the data sets individually. An alternative method to refresh all data sets is done through the pre-built jobs. See the Pre-Built Jobs to Refresh Data Sets section in this guide for details.

Log on as a Costpoint BI Administrator (CER__ADMIN) with full access to database tables.

To refresh individual data sets:

1. In Costpoint BI, go to the location of the data sets in Smart AI. For example: **Company content » [Your tenant folder] » Smart AI » *Data Sets***.

Note: The tenant folder is available to cloud users only.

2. Adjacent to the **AR Summary Data**, click the ellipsis (...) and select **Refresh**.

Note: You can also go to the **Properties** of the data set and refresh the schedule based on your desired frequency.

3. Repeat step 2 with the other data sets until you have refreshed those that you need.

The other data sets are:

- GL Summary Data
- Labor History Data
- Planning Data
- Project Summary (PSR) Data
- Purchase Order Data
- Receipt Data
- Resource Management Data

Schedule Data Set Refresh

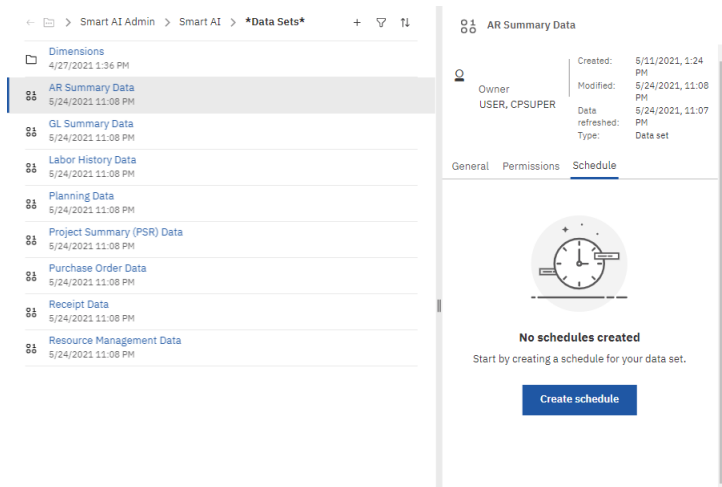
To avoid frequent data refresh, Deltek recommends to have a standard schedule to refresh data during off business hours.

To schedule data set refresh:

1. Go to the location of the data set that you like to apply a data set refresh schedule. For example, **Company content » [Your tenant folder] » Smart AI » *Data sets* » AR Data set**.

Note: The tenant folder is available to cloud users only.

2. Click the adjacent ellipsis (...) and then select **Properties**.
3. Click the **Schedule** tab. Click **Create schedule**.



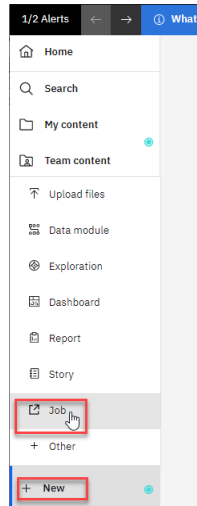
4. Enter the schedule of the data refresh and click **Save**.

Create a Job to Refresh Data Sets

You can create a job that refreshes one or more data sets. Schedules can be established so that the job can run automatically.

To create a job to refresh data sets:

1. On the main screen of Costpoint BI, click **+ New** and select **Job**.



2. On the **New job*** screen, click the **Start by adding some steps** icon.
3. On the **Add job step** dialog box, go to **Company content** » **[Your tenant folder]** > » **Smart AI** » ***Datasets***.

Note: The tenant folder is available to cloud users only.

4. Select each data set that you want to include in the job to add in them in the **Job steps to add** field. Click the **Add job steps** button.
5. Next, on the Steps table, click the plus (+) icon on the heading.
6. Leave the **Run options** with values:
Run order = **Run in sequence** and **Continue on error** is **enabled**.
7. Click the **Save** icon on top of the screen to save your job.
8. On the **Create a new job** dialog box, select a location where you want to save the job and enter a name. Click **Save**.

The **Run now** button and **Schedule** link display after saving. You have the option to either run the job or schedule it to run some other time.

Validate User Groups

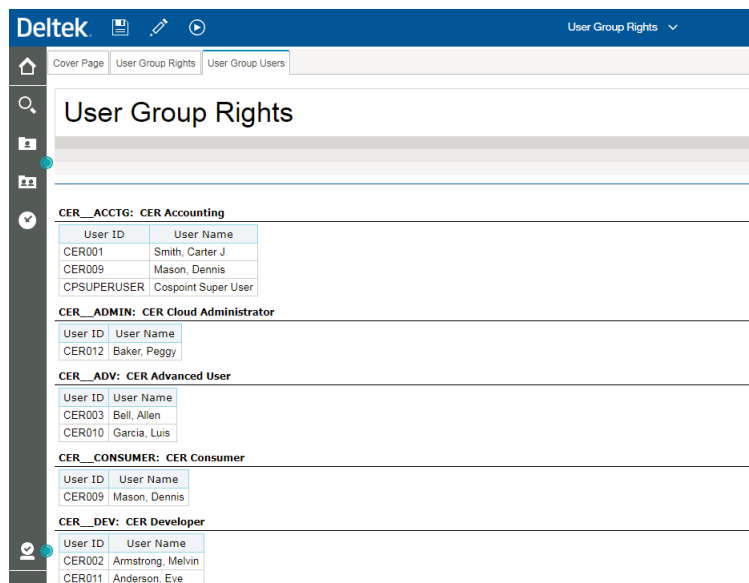
After you complete the steps in the post-installation phase, check the list of users per user group in Costpoint Business Intelligence against your accomplished Security Planning Template.

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

Note: If you do not have access to the **User Group Rights** report, you can also use the **Print User Group Rights Report (SYRGRPR)** in Costpoint which is located in **Admin » Security » Security Reports/Inquiries » Print User Group Rights Report**.

To validate the users in user groups:

1. In Costpoint Business Intelligence, 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 to the list of users that are in your [Security Planning Template](#). Check if all users are accounted for.



User ID	User Name
CER001	Smith, Carter J
CER009	Mason, Dennis
CPSUPERUSER	Costpoint Super User

User ID	User Name
CER012	Baker, Peggy

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

User ID	User Name
CER009	Mason, Dennis

User ID	User Name
CER002	Armstrong, Melvin
CER011	Anderson, Eve

Hidden Analysis Packages and Dashboards

For better generation and performance, the dashboards for **Planning** and **Projects** are now available in **Smart AI** which uses data modules as source of data. This new version leverages the features of Smart AI.

The dashboards and packages for **Planning** and **Projects** in Costpoint BI 8.0.x and beyond that uses dimensional data have been hidden but can be made visible by administrators for users especially if they have customized reports. Making these dashboards and packages visible is an optional step depending on the needs of your organization. Deltek recommends the use of the new versions of these dashboards and packages in Smart AI for ease of use.

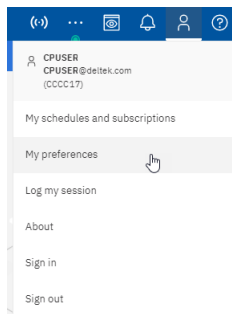
Unhide Analysis Packages and Dashboards

To unhide the Analysis Packages and Dashboards, you should show hidden entries in Costpoint BI first in **My preferences**.

You should have administrator rights to perform this procedure.

To unhide the Planning and Projects packages and dashboards:

1. On the upper right-hand side of the Welcome page of Costpoint BI, click the **Personal menu** icon and select **My preferences**.



2. Click **Show hidden entries** check box.
3. Go to **Team content » Planning**. Click the ellipsis (...) beside the **Dashboards** folder and select **Copy or move**.
4. On the dialog box, select a destination within **Company content** that you like to copy the folder into.
5. Click **Copy to**.
A confirmation message appears when the folder has been successfully copied.
6. Copy the following folders to **Company content** by repeating steps 3 to 5:
 - **Team content » Planning » Packages**
 - **Team content » Projects » Dashboards**
 - **Team content » Projects » Packages**
7. Go to the location of the copied **Dashboards** and **Packages** folders in **Company content** and click the ellipsis (...) adjacent to them and select **Properties**.

8. On the **Properties** screen, click **Advanced** and clear the **Hide this entry** check box.

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 perform a few steps to validate reports.

Users 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.

Troubleshooting

Some installations require you to perform extra steps to avoid errors.

Missing AI Assistant

After the Smart AI folder is copied and the job to refresh data was performed, the AI Assistant may be missing when exploring some data modules.

To fix this, the admin should open the data module with the missing AI Assistant and then save it. The save action should display the AI Assistant once again when the data module is reopened. This issue has been reported to IBM awaiting solution.

About Deltek

Better software means better projects. Deltek delivers software and information solutions that enable superior levels of project intelligence, management, and collaboration. Our industry-focused expertise makes your projects successful and helps you achieve performance that maximizes productivity and revenue.

www.deltek.com