Deltek

Deltek Costpoint Business Intelligence 8.2.9

Post Installation and Configuration Guide for On-premises Users

March 4, 2024

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 4, 2024.

Contents

About this Guide 1
Prerequisites 2
Overview 3
Costpoint Business Intelligence Security 4
    Check the Model Security Configuration 4
    Capability Security 6
    Object Security 12
    Model or Row Level Security 14
    Portal Visibility Filter 34
Map the Costpoint CER User Groups to Cognos User Groups 35
Configure Capability Permissions 38
    Remove Associations to IBM Roles (for Upgrading Users Only) 38
    Add User Roles to Capabilities and their Children 39
    Customize a Capability for a User Role 47
    Remove a User Role Assigned to a Capability 49
Verify the CER__ADV_LITE User Query Permission 50
Add Everyone and Assign Read Access to Team Content 51
Copy the Smart AI Folder to Company Content 52
Validate User Groups 53
Apply the Deltek Theme to Cognos Analytics 54
Check Extensions 55
    Install Extensions 55
Create Custom Color Palette 57
Update Project Health Reports with Global Color Palette 59
Optional Tasks 61
    Configure the Barcode Font for Reports 61
    Data Set 62
    Hidden Packages and Dashboards 66
Troubleshooting 67
    Missing AI Assistant 67

About this Guide

Welcome to the Costpoint Business Intelligence 8.2.9 Post Installation and Configuration Guide.

This guide will walk you through the initial setup of Costpoint Business Intelligence so your environment is secured before you allow users into Costpoint Business Intelligence to run and create reports and dashboards and leverage the built-in security features. Make sure that you have successfully installed Costpoint Business Intelligence 8.2.9 before you proceed to the procedures found in this guide.

The tasks described in this guide will be implemented by the Costpoint Business Intelligence System Administrators but may need information from other groups in your company.

Prerequisites

Before you can complete the procedures described in this guide, Costpoint Business Intelligence 8.2.9 must be installed.

Make sure you have successfully completed the following:

- Installed Cognos Analytics with Watson 11.2.4 FP2 where the Content Store database and Gateway dispatcher have been updated and configured
- Installed the Costpoint Authentication Provider (CAP) 8.2

Overview

In the Post Installation and Configuration phase we explain the new security design and how to apply configuration procedures to establish the appropriate security settings for your organization. This guide will also cover other special topics like configuring Bar Code Fonts and refreshing data sets.

The steps in the Post Installation and Configuration phase are:

- Check the Model Security Configuration
- Complete the Capabilities Security Template
- Complete the Object Security Template
- Assign Costpoint Users to CER User Groups
- Set Up Current Reporting Period
- Set the Visibility Filter
- Map the Costpoint CER User Groups to Cognos User Groups
- Configure Capability Permissions
- Verify the CER__ADV_LITE User Query Permission
- Add Everyone and Assign Read Access to Team Content
- Copy the Smart AI Folder to Company Content
- Validate User Groups
- Add the Deltek Theme to Cognos Analytics
- Check Extensions

Costpoint Business Intelligence Security

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

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

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

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 Controls** » **Manage BI Settings**).
2. Select **No** in the corresponding fields where you want to disable security.

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. **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.
Use CP Organization Security By Module	Select **No** to disable organization security in the new secure models which are: ▪ Accounts Receivable ▪ Accounts Payable ▪ Employee ▪ General Ledger ▪ Labor ▪ Manufacturing ▪ Materials ▪ Procurement ▪ Projects ▪ Subcontractor
Use Project Roles Security	Select **No** to disable project roles security.
Enable T&E Model Security	Select **No** to disable model security for the Time & Expense model.

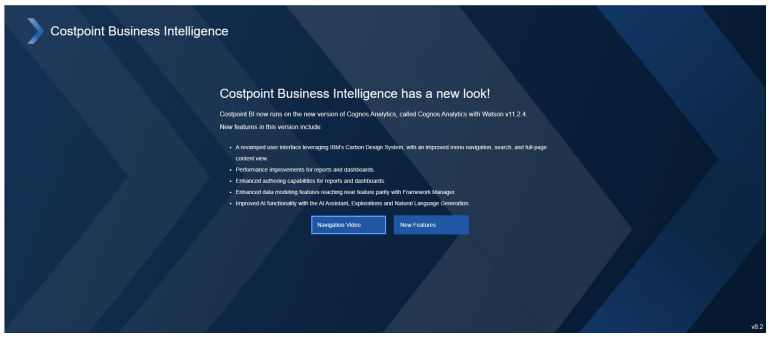
3. Click **Save**.

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.

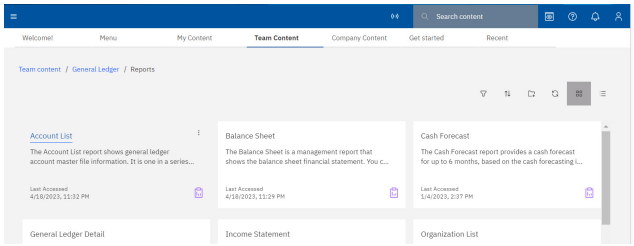
You as Administrator should then open Business Intelligence to make sure you can access the initial Costpoint Business Intelligence Welcome Screen.



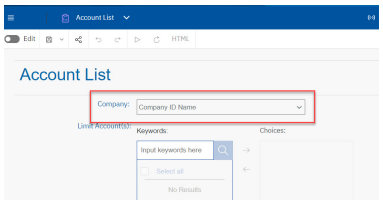
Then, click the **Team Content** tab, and you should see the full content.

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. In **Team Content**, click **General Ledger** » **Reports** » **Account List**.



Then, select the **Company** from the Prompt Page and click **Finish**. 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 Project Role 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	CER Consumer*	CER User*	CER Advanced Lite	CER Advanced User*	CER Developer	CER Web Admin	CER Cloud 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						•	•

CER Consumer* - Legacy license

CER User* - Only sold with bundles

CER Advanced User* - Customers can assign a regular or lite version of the CER Advanced User

Note: The 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 CER users
- 5% are CER Advanced users
- Plus 1 CER Administrator
- Additional licenses can be purchased on an a la carte basis. Additional user licenses typically bought, are CER Web Administrator or CER 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 CER Users
  - CER Developers
  - CER Web Admins
  - CER Administrators
  - A la Carte Licenses can be purchased as Restricted or Full Use

- Restricted: Deltek 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 Consumer users are not allowed to copy or move content. Instead, they can create views and shortcuts of objects in alternate locations.
- **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. The CER Administrator also manages the overall BI security through the Manage BI Settings (BIMCERSETTINGS) screen where you can either enable or disable security.

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

For entries that are indicated as OPTIONAL, you may assign the capability to user roles based on the need of your organization and will still be compliant with Deltek licensing.

Detailed Capabilities by Role for On-Premises Users

Capabilities	CER__CONSUMER	CER__USER	CER__ADV_LITE	CER__ADV	CER__DEV	CER Web Administrator	CER (Cloud)Admin/System Administrator
Adaptive Analytics						ACCESS	ACCESS
Administration						ACCESS	ACCESS
Adaptive Analytics Administration						ACCESS	ACCESS
Administration Tasks						ACCESS	ACCESS
Collaboration Administration						ACCESS	ACCESS
Configure and Manage the System						ACCESS	ACCESS
Controller Administration						ACCESS	ACCESS
Data Source Connections						ACCESS	ACCESS
Distribution Lists and Contacts						ACCESS	ACCESS
Manage Visualizations						ACCESS	ACCESS
Metric Studio Administration						ACCESS	ACCESS
Mobile Administration						ACCESS	ACCESS
Planning Administration						ACCESS	ACCESS
PowerPlay Servers						ACCESS	ACCESS
Printers						ACCESS	ACCESS
Query Service Administration						ACCESS	ACCESS
Run Activities and Schedules						ACCESS	ACCESS
Set capabilities and manage UI profiles						ACCESS	ACCESS
Styles and portlets						ACCESS	ACCESS
Users, Groups, and Roles						ACCESS	ACCESS
AI	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*
Learning	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*
Use Assistant		ACCESS	ACCESS	ACCESS	ACCESS		ACCESS
Analysis Studio		ACCESS	ACCESS	ACCESS	ACCESS		ACCESS
Attach Outputs	ACCESS	ACCESS	ACCESS	ACCESS	ACCESS		ACCESS
Cognos Analytics for Mobile	OPTIONAL	OPTIONAL	OPTIONAL	OPTIONAL	OPTIONAL	OPTIONAL	ACCESS
Cognos Insight							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
Controller Studio							ACCESS
Dashboard		ACCESS	ACCESS	ACCESS	ACCESS		ACCESS
Create/Edit		ACCESS	ACCESS	ACCESS	ACCESS		ACCESS
Data Manager							ACCESS
Data sets	CUSTOM (DENY E T)	CUSTOM (DENY E T)	CUSTOM (DENY E T)	ACCESS	ACCESS		ACCESS
Desktop Tools					ACCESS		ACCESS
Detailed Errors	OPTIONAL	OPTIONAL	OPTIONAL	ACCESS	ACCESS	OPTIONAL	ACCESS
Develop Visualizations				ACCESS	ACCESS		ACCESS
Drill Through Assistant							ACCESS
Email	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*
Email Delivery Option	ACCESS	ACCESS	ACCESS	ACCESS	ACCESS	ACCESS	ACCESS
Include link in email	ACCESS	ACCESS	ACCESS	ACCESS	ACCESS	ACCESS	ACCESS
Share using email	ACCESS	ACCESS	ACCESS	ACCESS	ACCESS	ACCESS	ACCESS
Type in external email	ACCESS	ACCESS	ACCESS	ACCESS	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 (GRANT T)	CUSTOM (GRANT T)	ACCESS	ACCESS	ACCESS		ACCESS
External Content							ACCESS
Watson Studio							ACCESS
External Repositories	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS
Manage Repository Connections						ACCESS	ACCESS
View External Documents	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*
Generate CSV Output	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*
Generate PDF Output	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*
Generate XLS Output	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*
Generate XML Ouput	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*
Glossary	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*
Hide Entries	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*
Import Relational Metadata					ACCESS	ACCESS	ACCESS
Job				ACCESS	ACCESS	ACCESS	ACCESS
Lineage	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*
Manage Content						ACCESS	ACCESS
Manage Own Data Source Signons						ACCESS	ACCESS
Metric Studio							ACCESS
Edit View							ACCESS
Mobile							ACCESS
Notebook							ACCESS
Planning Contributor							ACCESS
PowerPlay Studio	OPTIONAL	OPTIONAL	OPTIONAL	OPTIONAL	OPTIONAL	OPTIONAL	ACCESS
Query Studio			ACCESS	ACCESS	ACCESS		ACCESS
Advanced			ACCESS	ACCESS	ACCESS		ACCESS
Create			ACCESS	ACCESS	ACCESS		ACCESS
Report Studio	CUSTOM (GRANT T)	CUSTOM (GRANT T)	ACCESS	ACCESS	ACCESS		ACCESS
Allow External Data	OPTIONAL	OPTIONAL	OPTIONAL	OPTIONAL	OPTIONAL	OPTIONAL	ACCESS
Create/ Delete			ACCESS	ACCESS	ACCESS		ACCESS
Edit Burst Definition			ACCESS	ACCESS	ACCESS		ACCESS
Edit HTML Items				ACCESS	ACCESS		ACCESS
Edit User Defined SQL				ACCESS	ACCESS		ACCESS
Generate Burst Output			ACCESS	ACCESS	ACCESS		ACCESS
Run HTML Items	ACCESS	ACCESS	ACCESS	ACCESS	ACCESS		ACCESS
Run User Defined SQL	ACCESS	ACCESS	ACCESS	ACCESS	ACCESS		ACCESS
Save to Cloud	OPTIONAL	OPTIONAL	OPTIONAL	OPTIONAL	OPTIONAL	OPTIONAL	ACCESS
Manage Connections	OPTIONAL	OPTIONAL	OPTIONAL	OPTIONAL	OPTIONAL	OPTIONAL	ACCESS
Scheduling (and Subscriptions)	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
Schedule by Month	ACCESS	ACCESS	ACCESS	ACCESS	ACCESS		ACCESS
Schedule by Trigger							ACCESS
Schedule by Week	ACCESS	ACCESS	ACCESS	ACCESS	ACCESS		ACCESS
Schedule by Year			ACCESS	ACCESS	ACCESS		ACCESS
Scheduling Priority							ACCESS
Self Service Package Wizard							ACCESS
Set Entry- Specific Capabilities							ACCESS
Share Pin Board	OPTIONAL	OPTIONAL	OPTIONAL	OPTIONAL	OPTIONAL	OPTIONAL	ACCESS
Snapshots	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*
Specification Execution							ACCESS
Upload Files	CUSTOM (DENY E T)	CUSTOM (DENY E T)	CUSTOM (DENY E T)	ACCESS	ACCESS	ACCESS	ACCESS
View Generate Query Text	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*
Visualization Alerts	OPTIONAL	OPTIONAL	OPTIONAL	OPTIONAL	OPTIONAL	OPTIONAL	
Watch Rules		ACCESS	ACCESS	ACCESS	ACCESS		ACCESS
Web-based Modeling	CUSTOM (DENY E T)	CUSTOM (DENY E T)	CUSTOM (DENY E T)	ACCESS	ACCESS		ACCESS
Edit Data Module Defined SQL				ACCESS	ACCESS		ACCESS
Use Data Module Defined SQL	ACCESS	ACCESS	ACCESS	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 All Secure** user group will be able to see secure Accounting content found on the**Team Content** tab.

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.

Object	CER Accounting All Secure	CER Accounts Receivable Secure	CER Accounts Payable Secure	CER Employee Secure	CER Fixed Assets	CER General Ledger Secure	CER All	CER Contracts	CER Labor Secure	CER Billing Secure	CER Projects Secure	CER Planning (Project) Secure	CER Payroll Secure	CER Subcontractor Management Secure	CER Time Secure	CER Expense Secure	CER Materials Secure	CER Materials Manufacturing All Secure	CER Procurement Secure	CER Manufacturing Secure	CER HR Secure	CER CP Admin	CER Executive Secure
Team Content > *Packages* >	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Accounts Payable	•		•				•																•
Accounts Receivable	•	•					•																•
Billing							•			•													
Contracts Reporting							•	•															•
Employee				•			•																
Expense							•									•							
Fixed Assets	•				•		•																
General Ledger	•					•	•																•
Human Resources							•														•		
Labor							•		•														
Manufacturing							•										•	•		•			
Materials							•										•	•					
Payroll							•						•										
Procurement							•											•	•				
Project Analysis							•			•													
Project Planning Analysis							•				•												
Project Planning Reporting							•				•												
Project Reporting							•			•											•		•
Subcontractor Management							•						•										
Time							•							•									
~Legacy Packages (CER 7.1.x)~ >	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•			
Administration							•															•	
ICS	•						•																
Shop Floor Time							•										•						
CPSOX	•						•																
TESOX	•						•																
Accounts Payable	•		•				•																
Accounts Receivable	•	•					•																
Billing							•			•													
Costpoint Administration							•															•	
CRM & Contracts							•	•															
Employee				•			•																
Executive							•																•
Expense							•									•							
Fixed Assets	•				•		•																
General Ledger	•					•	•																
Human Resources							•														•		
Incurred Cost Submission							•																
Labor							•		•														
Manufacturing							•										•			•			
Materials							•										•	•					
Payroll							•						•										
Planning							•				•												
Procurement							•											•	•				
Projects							•			•													
Shop Floor Time							•																
SOX Controls Reporting							•																
Subcontractor Management							•						•										
Time							•							•									
Company Content > Smart AI >	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•		•	•
Executive							•																•
People				•			•														•		
Planning							•				•												
Procurement							•											•	•				
Projects							•			•													
Data Modules	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Dimensions -	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Relative Time	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Accounts Receivable	•	•					•																•
General ledger	•					•	•																•
HR Management	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Labor History							•				•												•
Planning							•					•											
Project Summary (PSR)							•				•												•
Purchase Orders							•										•	•					
Resource Management							•					•											
Data Sets	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Dimensions -	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•

Select secure user groups have access to some of the legacy packages as indicated on the table. The rest of the legacy packages are hidden.

Note: User groups with the 'Secure' suffix will have access to secured Costpoint BI packages corresponding to a domain, such as, Projects, Materials, and so on. The rest of the user groups, those without 'Secure' in their name, will have access to all domain-related content which are secured and non-secured.

A user must belong to at least one of these groups in order to see any Deltek 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 using custom object security groups in use by their organization.. 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

As best practice, Deltek recommends that custom content is separate from Deltek provided content. For this purpose, the **Company content** folder is provided in Costpoint Business Intelligence 8.x.

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.
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 Role Security**: Restricts project data based on the user's assigned project role.
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 Fixed Assets and Administration.

Row and Organization Security Matrix

Package	Module Security Profile	Organization	Project/PM	Labor Suppression	Functional Role		Parts
					BI	TE	
Accounts Payable	AR	Performing Org					
Accounts Receivable	AP	Owning Org			✓		
Administration							
Billing	BL	Owning Org			✓		
Contracts Reporting	CN and OP	Owning Org					
Employee	EM	Security Org		✓			
Expense						✓	
Fixed Assets							
General Ledger	GL	Performing Org		✓			
Human Resources	HB	Security Org					
Labor	LD	Security Org		✓			
Manufacturing	PC	Org may vary					✓
Materials	IN	Org may vary					✓
Payroll	PR	Security Org		✓			
Procurement	PO	Org may vary					✓
Project Reporting	PJ	Owning Org		✓	✓		
Project Planning Reporting		Owning Org	✓	✓			
Subcontractor Management	SM	Owning Org					
Time						✓	

The Fixed Assets and Administration models have object and capability security.

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 Row and Organization Security Matrix in the

Matrix for Secure Models section 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:

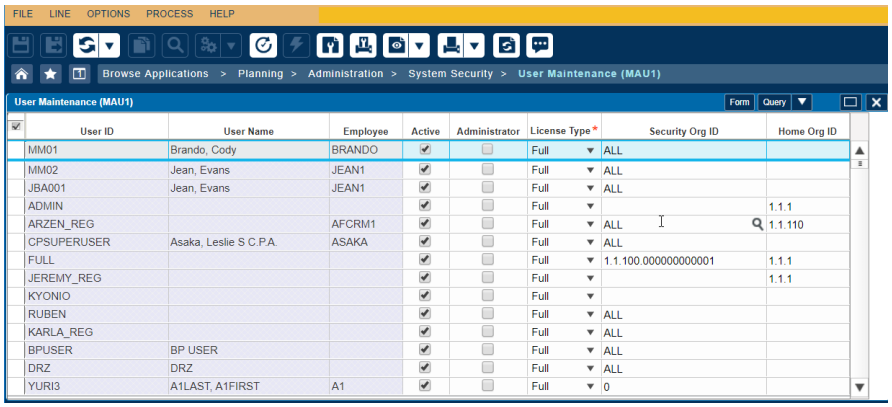
- **Enable CP and Planning Model Security** is set to **Yes** and
- **Use CP Organization Security by Module** is set to **Yes**

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.

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.



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

Deltek recommends that you also enable organization security by module when the **Use CP Organization Security By Module** is set to **Yes** on the Manage BI Settings (BIMCERSETTINGS) screen.

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.

To enable organization security in the modules and applications:

1. Go to **Admin** » **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. Enter the **Profile ID** and **Profile Name**. Select the **Apply Org Security** check box and the **Rights Application Method**.

   Tip: Press **SHIFT+F1** or go to **Help** » **Help** menu to know more about the description of the fields on this screen.
3. On the **Assign Organizations to Profile** table window, click **New**.
4. Enter the Organization of which you want to apply this organization security profile.
5. Click **Save**.
6. 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. Fill out the fields on screen. Press **SHIFT+F1** to open the help and to know more about these fields.
3. 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.
4. In the **Assign Profiles to Modules** table window, see if you like to change any of the profiles assigned to a module.
5. Click **Save**.
6. 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

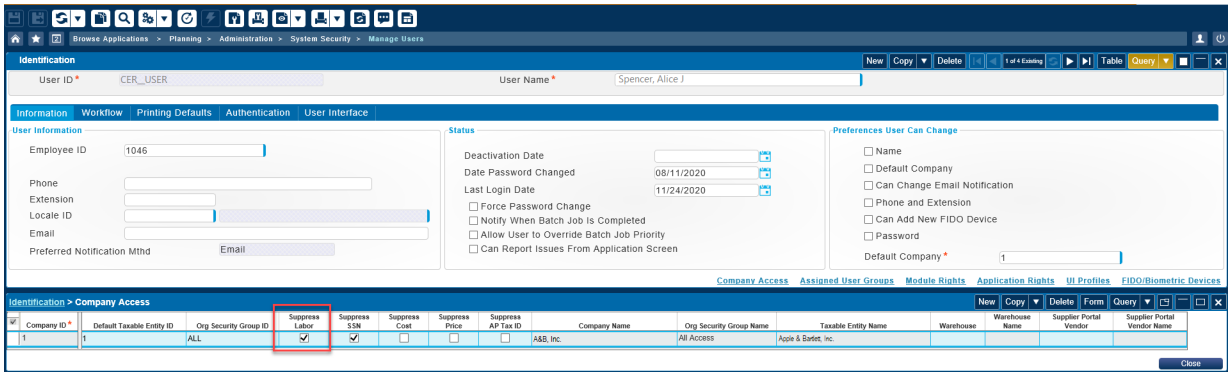
is separate from Costpoint BI. The system settings in Costpoint BI is controlled through the Manage BI Settings (BIMCERSETTINGS) screen.

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

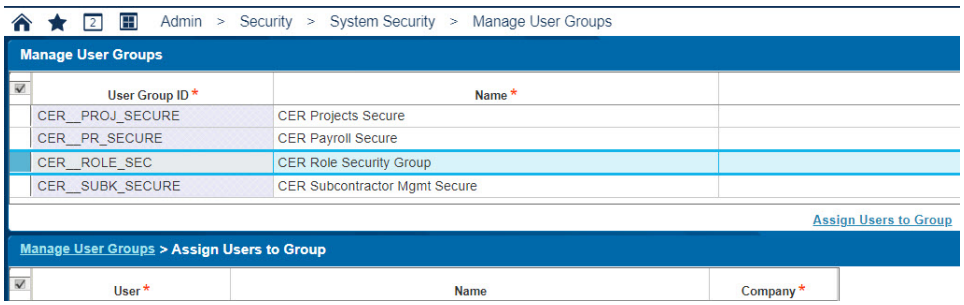
The Project model will suppress labor if the Suppress Labor flag is checked for the user and the Costpoint and Planning model security is turned on. It is important that at least one Org is assigned to the Org Security Group. If no orgs are assigned, the user will not be able to see any data.



Project Roles Security

Project Roles Security allows you to set up functional roles that are not only limited to a Project Manager. Functional roles can be assigned to users in Costpoint which can then secure the corresponding project data in BI.

Several functional roles can be assigned to a user such as, the Project Manager role. In order to limit the BI data to only the projects that the Project Manager owns, you must assign the user to the CER__ROLE_SEC user group.



Project Roles Security further enhances the implementation of Project Manager Security that was available in past Costpoint BI versions.

Project Roles Security is applicable to the Accounts Receivable, Billing, and Project Reporting packages.

Project Manager Security vs. Project Roles Security

Project Manager Security was introduced in Costpoint BI 8.1 and earlier. For Costpoint 8.2.9, the more comprehensive Project Roles Security was added that enhances PM security along with other benefits.

The following table summarizes the differences between the PM Security and Project Roles Security.

Project Manager Security	Project Roles Security
Project Manager is the only project role available	Multiple project roles can be defined
Project Managers are limited to project data found on their assigned project level	When configured, Project Managers and other project roles can view project data for their level and those at the lower levels
To enable Project Manager Security, Organization Security must be enabled too	Project Roles Security and Organization Security can be enabled separately
Project Manager Security is followed over Organization Security. For example, Project Managers assigned to a project in another organization may still see data even when Organization Security is enabled	Organization Security is followed over Project Manager Security. For example, when Organization Security is enabled, Project Managers and other project roles will not see project data outside their organization.
Uses Employee ID	Uses User ID which means that report data are not only limited to employees

Improvements in Project Roles Security

Access to secure project data has been greatly enhanced by Project Roles Security. There are several significant improvements and the major ones are described in the succeeding sections.

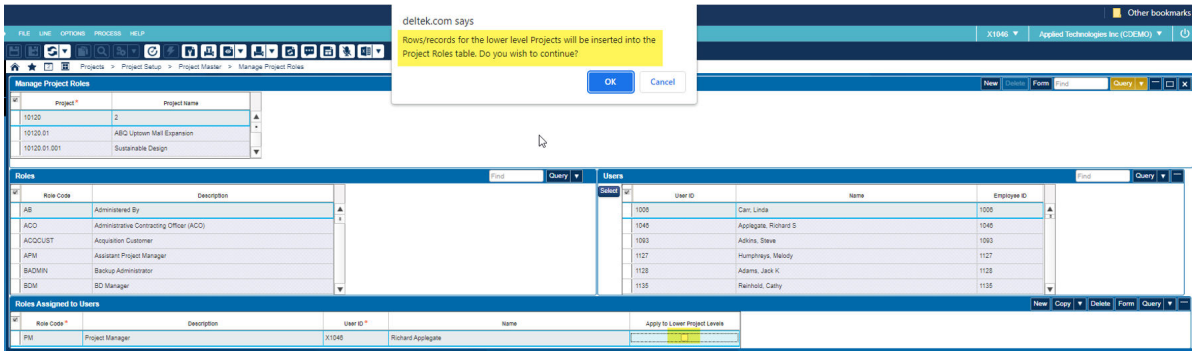
Viewing Project Data in Multiple Project Levels

If the necessary configurations are set, any project role, including project managers, can view project data at their level and in the lower project levels.

For example, Richard Applegate is the Project Manager for **Project 10120**.

Richard also oversees the projects in the lower levels and needs to view the corresponding project data. To do this, his project role setting needs to be configured to have this type of access

On the Manager Project Roles screen in Costpoint (**Projects** » **Project Setup** » **Project Master**), make a query for **Project 10120** and modify Richard's assigned user role to also access the lower levels of his project through the **Apply to Lower Level Projects** checkbox.



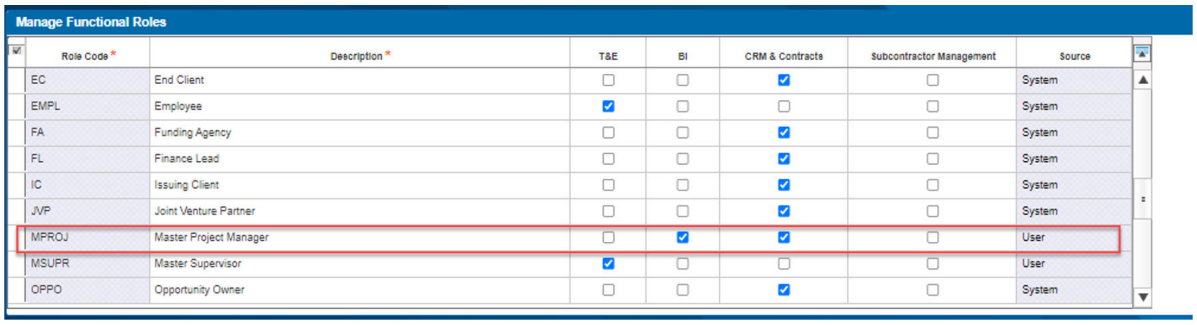
After you apply the configurations and log out and back in to Costpoint BI, the report now shows project data for all lower-level projects for Richard.

Project ID	Project Name	Project ID Name	Project Long Name	Project ID Long Name	Organization ID	Organization Name	Employee ID	Project Manager Name	Customer ID	Customer Name	Company ID
10120	2	10120 - 2	Construction and Design	10120 - Construction and Design	01.01.02	Construction Management	1046	Applegate, Richard S	100008	BND Engineering, Inc.	1
10120.01	ABQ Uptown Mall Expansion	10120.01 - ABQ Uptown Mall Expansion	ABQ Uptown Mall Expansion	10120.01 - ABQ Uptown Mall Expansion	01.01.02	Construction Management	1046	Applegate, Richard S	100008	BND Engineering, Inc.	1
10120.01.001	Sustainable Design	10120.01.001 - Sustainable Design	Sustainable Design	10120.01.001 - Sustainable Design	01.01.02	Construction Management	1046	Applegate, Richard S	100008	BND Engineering, Inc.	1
10120.01.002	Engineering	10120.01.002 - Engineering	Engineering	10120.01.002 - Engineering	01.01.02	Construction Management	1046	Applegate, Richard S	100008	BND Engineering, Inc.	1
10120.03	Portland Wastewater Sys	10120.03 - Portland Wastewater Sys	Portland Wastewater Sys	10120.03 - Portland Wastewater Sys	01.01.02	Construction Management	1014	Arnold, Deborah	100008	BND Engineering, Inc.	1
10120.03.001	Planning	10120.03.001 - Planning	Planning	10120.03.001 - Planning	01.01.02	Construction Management	1014	Arnold, Deborah	100008	BND Engineering, Inc.	1
10120.03.999	System Design	10120.03.999 - System Design	System Design	10120.03.999 - System Design	01.01.02	Construction Management	1014	Arnold, Deborah	100008	BND Engineering, Inc.	1

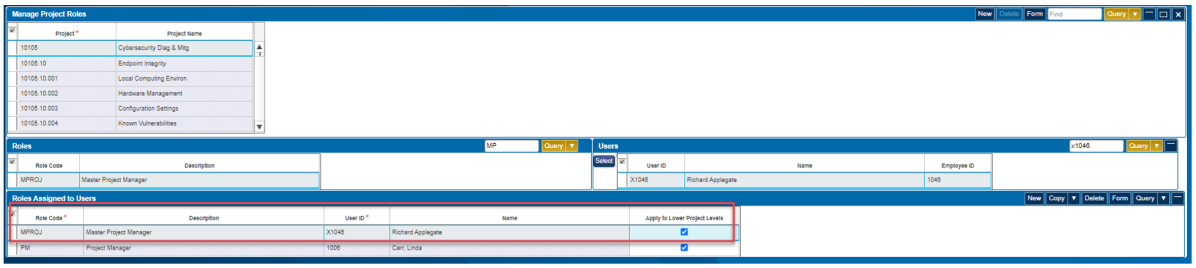
Viewing Project Data for a Different PM

In some cases, there are Costpoint BI users who oversee multiple projects that have different project managers. Let us assign the Master Project Manager Role for these users.

For example, Richard has a Master Project Manager Role who oversees some projects but does not directly manage them. First, the Master Project Manager Role must be marked as a functional role used in Costpoint BI. Do this on the Manage Functional Roles screen in **Admin** » **System Administration** » **System Administration Controls**.



And then, add Richard as a Master Project Manager to Project 10105 and apply to lower levels. Do this on the Manage Project Roles screen.



When the report is generated, Richard now sees project data for Project 10105 in addition to his original Project 10120. He sees project data for the organization he belongs and his project role.

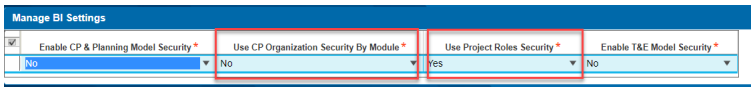
Project ID	Project Name	Project ID Name	Project Long Name	Project ID Long Name	Organization ID	Organization Name	Employee ID	Project Manager Name	Customer ID	Cu
10105	Cybersecurity Diag & Mitg	10105 - Cybersecurity Diag & Mitg	Cybersecurity Diag & Mitg	10105 - Cybersecurity Diag & Mitg	01.01.01	High Tech	1041	Boyd, Edward	100017	Dp Se
10105.10	Endpoint Integrity	10105.10 - Endpoint Integrity	Endpoint Integrity	10105.10 - Endpoint Integrity	01.01.01	High Tech	1041	Boyd, Edward	100017	Dp Se
10105.10.001	Local Computing Environ	10105.10.001 - Local Computing Environ	Local Computing Environ	10105.10.001 - Local Computing Environ	01.01.01	High Tech	1041	Boyd, Edward	100017	Dp Se
10105.10.002	Hardware Management	10105.10.002 - Hardware Management	Hardware Management	10105.10.002 - Hardware Management	01.01.01	High Tech	1041	Boyd, Edward	100017	Dp Se
10105.10.003	Configuration Settings	10105.10.003 - Configuration Settings	Configuration Settings	10105.10.003 - Configuration Settings	01.01.01	High Tech	1041	Boyd, Edward	100017	Dp Se
10105.10.004	Known Vulnerabilities	10105.10.004 - Known Vulnerabilities	Known Vulnerabilities	10105.10.004 - Known Vulnerabilities	01.01.01	High Tech	1041	Boyd, Edward	100017	Dp Se
10105.30	Boundary Protection	10105.30 - Boundary Protection	Boundary Protection	10105.30 - Boundary Protection	01.01.01	High Tech	1041	Boyd, Edward	100017	Dp Se
10105.30.001	Access Control	10105.30.001 - Access Control	Access Control	10105.30.001 - Access Control	01.01.01	High Tech	1041	Boyd, Edward	100017	Dp Se
10120	2	10120 - 2	Construction and Design	10120 - Construction and Design	01.01.02	Construction Management	1046	Applegate, Richard S	100008	BN Inc
10120.01	ABQ Uptown Mall Expansion	10120.01 - ABQ Uptown Mall Expansion	ABQ Uptown Mall Expansion	10120.01 - ABQ Uptown Mall Expansion	01.01.02	Construction Management	1046	Applegate, Richard S	100008	BN Inc
10120.01.001	Sustainable Design	10120.01.001 - Sustainable Design	Sustainable Design	10120.01.001 - Sustainable Design	01.01.02	Construction Management	1046	Applegate, Richard S	100008	BN Inc
10120.01.002	Engineering	10120.01.002 - Engineering	Engineering	10120.01.002 - Engineering	01.01.02	Construction Management	1046	Applegate, Richard S	100008	BN Inc
10120.03	Portland Wastewater Sys	10120.03 - Portland Wastewater Sys	Portland Wastewater Sys	10120.03 - Portland Wastewater Sys	01.01.02	Construction Management	1014	Arnold, Deborah	100008	BN Inc
10120.03.001	Planning	10120.03.001 - Planning	Planning	10120.03.001 - Planning	01.01.02	Construction Management	1014	Arnold, Deborah	100008	BN Inc
10120.03.999	System Design	10120.03.999 - System Design	System Design	10120.03.999 - System Design	01.01.02	Construction Management	1014	Arnold, Deborah	100008	BN Inc
10140	DHA Network Review	10140 - DHA Network Review	DHA Network Review	10140 - DHA Network Review	01.01.01	High Tech	1046	Applegate, Richard S	100017	Dp Se
10140.01	Scope and Review	10140.01 - Scope and Review	Scope and Review	10140.01 - Scope and Review	01.01.01	High Tech	1046	Applegate, Richard S	100017	Dp Se
10140.01.001	DHS Network Phase I	10140.01.001 - DHS Network Phase I	DHS Network Phase I	10140.01.001 - DHS Network Phase I	01.01.01	High Tech	1046	Applegate, Richard S	100017	Dp Se
10140.01.002	DHS Network Phase II	10140.01.002 - DHS Network Phase II	DHS Network Phase II	10140.01.002 - DHS Network Phase II	01.01.01	High Tech	1046	Applegate, Richard S	100017	Dp Se
10140.02	Network Design	10140.02 - Network Design	Network Design	10140.02 - Network Design	01.01.01	High Tech	1046	Applegate,	100017	Dp

Organization Security and Project Roles Security Work Independently

Starting in Costpoint BI 8.2, Organization Security and Project Roles Security can be controlled independently.

For example, Organization Security can be turned off while Project Roles Security is turned on.

On the Manage BI Settings screen found in **Reports & Analytics** » **BI Controls** » **Manage BI Settings** , Organization Security and Project Roles Security have different switches.



To illustrate, if the Organization Security is turned off and Project Roles Security is turned on, Richard in our example will see more project data because the filter for organizations has been turned off. He will still see those projects where he has an assigned role, but now he also sees project data for those outside his organization.

Project ID	Project Name	Project ID Name	Project Long Name	Project ID Long Name	Organization ID	Organization Name	Employee ID	Project Manager Name	Customer ID	Customer Name	Company ID	Company Name	Project Abbrv	Project Type Desc	Project Classification	Active (Y/N)	Billable Project (Y/N)
10140.02.001	Design T.O. #9489752	10140.02.001 - Design T.O. #9489752	Design T.O. #9489752	10140.02.001 - Design T.O. #9489752	01.01.01	High Tech	1046	Applegate, Richard S	100017	Dpt of Homeland Sec	1	Applied Technologies Inc		MANF	DIRECT PROJECT	N	Y
10280	IT Development Plan	10280 - IT Development Plan	IT Development Plan	10280 - IT Development Plan	01.01.01	High Tech	1046	Applegate, Richard S	100053	Booz Allen	1	Applied Technologies Inc		SEE LOWER LEVEL	DIRECT PROJECT	N	Y
10280.IT	IT Security Compliance	10280.IT - IT Security Compliance	IT Security Compliance	10280.IT - IT Security Compliance	01.01.01	High Tech	1046	Applegate, Richard S	100053	Booz Allen	1	Applied Technologies Inc		COMSERVICE	DIRECT PROJECT	N	Y
10280.RE	Records Management	10280.RE - Records Management	Records Management	10280.RE - Records Management	01.01.01	High Tech	1046	Applegate, Richard S	100053	Booz Allen	1	Applied Technologies Inc		COMSERVICE	DIRECT PROJECT	N	Y
10370	IT Staff Augmentation	10370 - IT Staff Augmentation	IT Staff Augmentation	10370 - IT Staff Augmentation	01.01.01	High Tech	1046	Applegate, Richard S	100005	Armstrong Labs	1	Applied Technologies Inc		COMSERVICE	DIRECT PROJECT	N	Y
10370.IT	Technology Consultation	10370.IT - Technology Consultation	Technology Consultation	10370.IT - Technology Consultation	01.01.01	High Tech	1046	Applegate, Richard S	100005	Armstrong Labs	1	Applied Technologies Inc		COMSERVICE	DIRECT PROJECT	N	Y
10370.RE	Help Desk Support	10370.RE - Help Desk Support	Help Desk Support	10370.RE - Help Desk Support	01.01.01	High Tech	1046	Applegate, Richard S	100005	Armstrong Labs	1	Applied Technologies Inc		COMSERVICE	DIRECT PROJECT	N	Y
10700	SCA Contract	10700 - SCA Contract	SCA Contract	10700 - SCA Contract	01.01.04	Base Operation Management	1046	Applegate, Richard S	100025	NASA Headquarters	1	Applied Technologies Inc		GOVSERVICE	DIRECT PROJECT	N	Y
10700.01	SCA Contract DO Level	10700.01 - SCA Contract DO Level	SCA Contract DO Level	10700.01 - SCA Contract DO Level	01.01.04	Base Operation Management	1046	Applegate, Richard S	100025	NASA Headquarters	1	Applied Technologies Inc		GOVSERVICE	DIRECT PROJECT	N	Y
10700.01.001	SCA Contract T&M	10700.01.001 - SCA Contract T&M	SCA Contract T&M	10700.01.001 - SCA Contract T&M	01.01.04	Base Operation Management	1046	Applegate, Richard S	100025	NASA Headquarters	1	Applied Technologies Inc		GOVSERVICE	DIRECT PROJECT	N	Y
10700.01.002	SCA Contract Cost Plus	10700.01.002 - SCA Contract Cost Plus	SCA Contract Cost Plus	10700.01.002 - SCA Contract Cost Plus	01.01.04	Base Operation Management	1046	Applegate, Richard S	100025	NASA Headquarters	1	Applied Technologies Inc		GOVSERVICE	DIRECT PROJECT	N	Y
10800	DHS Eagle GWAC	10800 - DHS Eagle GWAC	DHS Eagle GWAC	10800 - DHS Eagle GWAC	01.01.01	High Tech	1046	Applegate, Richard S	100017	Dpt of Homeland Sec	1	Applied Technologies Inc		GOVSERVICE	DIRECT PROJECT	N	Y
10800.01	DHS Eagle GWAC IT Spt	10800.01 - DHS Eagle GWAC IT Spt	DHS Eagle GWAC IT Spt	10800.01 - DHS Eagle GWAC IT Spt	01.01.01	High Tech	1046	Applegate, Richard S	100017	Dpt of Homeland Sec	1	Applied Technologies Inc		GOVSERVICE	DIRECT PROJECT	N	Y
10800.01.001	DHSE IT Spt Help Desk	10800.01.001 - DHSE IT Spt Help Desk	DHSE IT Spt Help Desk	10800.01.001 - DHSE IT Spt Help Desk	01.01.01	High Tech	1046	Applegate, Richard S	100017	Dpt of Homeland Sec	1	Applied Technologies Inc		GOVSERVICE	DIRECT PROJECT	N	Y
10800.01.002	DHSE Serve Upgrade	10800.01.002 - DHSE Serve Upgrade	DHSE Serve Upgrade	10800.01.002 - DHSE Serve Upgrade	01.01.01	High Tech	1046	Applegate, Richard S	100017	Dpt of Homeland Sec	1	Applied Technologies Inc		GOVSERVICE	DIRECT PROJECT	N	Y
10800.01.003	DHSE SQL Specialist	10800.01.003 - DHSE SQL Specialist	DHSE SQL Specialist	10800.01.003 - DHSE SQL Specialist	01.01.01	High Tech	1046	Applegate, Richard S	100017	Dpt of Homeland Sec	1	Applied Technologies Inc		GOVSERVICE	DIRECT PROJECT	N	Y
10800.02	DHS Eagle GWAC Staff Aug	10800.02 - DHS Eagle GWAC Staff Aug	DHS Eagle GWAC Staff Aug	10800.02 - DHS Eagle GWAC Staff Aug	01.01.01	High Tech	1046	Applegate, Richard S	100017	Dpt of Homeland Sec	1	Applied Technologies Inc		GOVSERVICE	DIRECT PROJECT	N	Y
10800.02.001	DHSE Staff Aug Help Desk	10800.02.001 - DHSE Staff Aug Help Desk	DHSE Staff Aug Help Desk	10800.02.001 - DHSE Staff Aug Help Desk	01.01.01	High Tech	1046	Applegate, Richard S	100017	Dpt of Homeland Sec	1	Applied Technologies Inc		GOVSERVICE	DIRECT PROJECT	N	Y

Note: Deltek recommends that the **Enable CP & Planning Model Security** and the **Use CP Organization Security By Module** switches are in sync. The first switch controls the application of the overall organization security, while the latter controls organization security by module.

Key Points in Project Roles Security

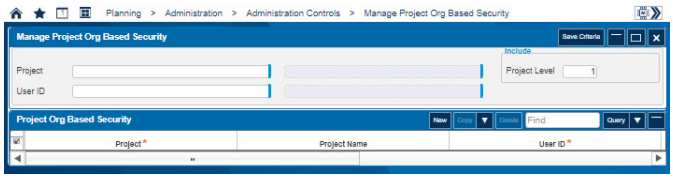
Some pointers to remember when applying Project Roles Security.

- **CER__PM_MGR** user group has been replaced by **CER__ROLE_SEC**. Project Roles Security uses the **CER__ROLE_SEC** user group.
- Project Roles Security does not overwrite Organization Security when it is enabled. When model security is turned on, Organization Security is enabled.
- If both Organization Security and Project Roles Security are turned on, then conditions for both types of security need to be met for users to see project data.

Project Security in Costpoint Planning

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.



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.

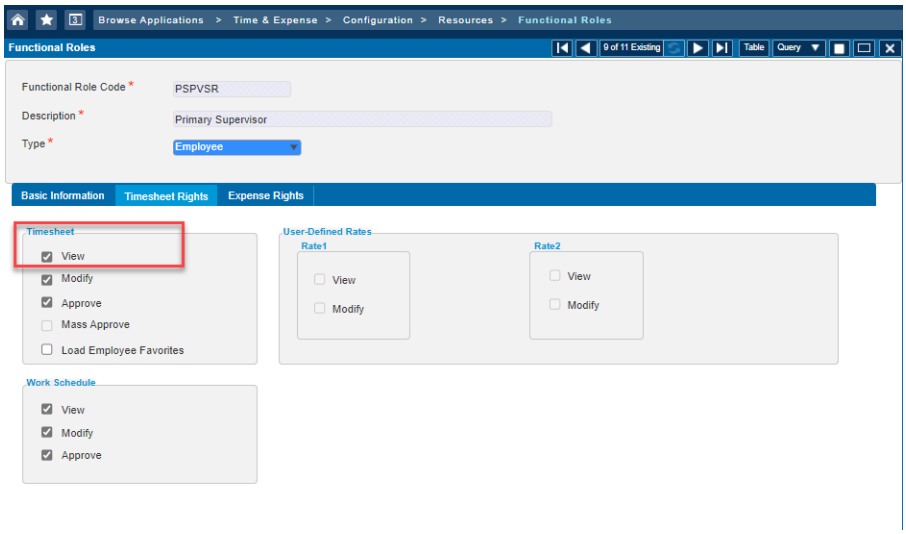
Note: Project Manager Security only shows the project WBS elements where they are assigned as PM, so if there are multiple PMs assigned to a single project structure, those PMs will not see the entire project.

Functional Roles Security

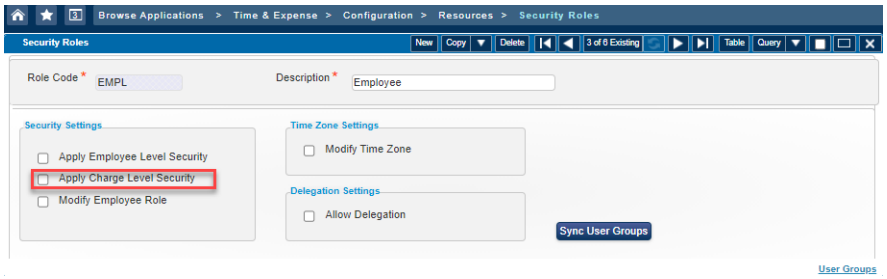
Functional Role security is currently supported in the Time model.

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.

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__BILL_SECURE	CER Billing 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__DEVELOPMENT	CER Development for Object Security	ALL
CER__EMPL_SECURE	CER Employee Secure	ALL
CER__EXEC_SECURE	CER Executive Secure	ALL
CER__EXPENSE_SECURE	CER Expense Secure	ALL
CER__FA_SECURE	CER Fixed Assets	ALL
CER__GL_SECURE	CER General Ledger Secure	ALL
CER__HR	CER HR	ALL
CER__HR_SECURE	CER Human Resources Secure	ALL
CER__LABOR_SECURE	CER Labor Secure	ALL
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

User Group	User Group Name	Company
CER__PLAN_PROJ	CER Planning (Projects)	ALL
CER__PR_SECURE	CER Payroll Secure	ALL
CER__ROLE_SEC	CER Role Security formerly known as 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

Project Roles Security Setup

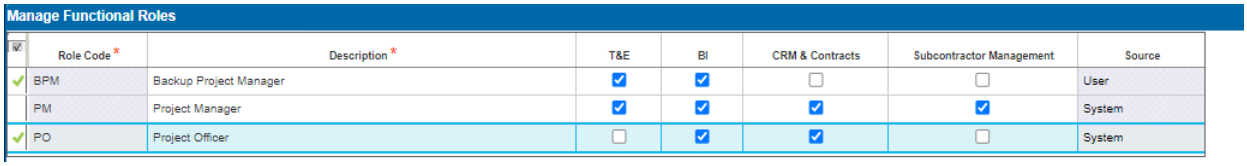
Project Roles Security can be set up through different screens in Costpoint.

Assign Functional Roles

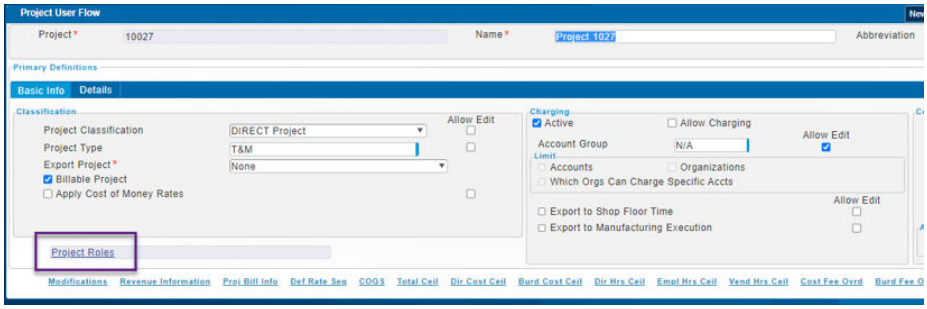
You can assign functional roles through the Manage Functional Roles and Manage Project User Flow screens.

To assign functional roles:

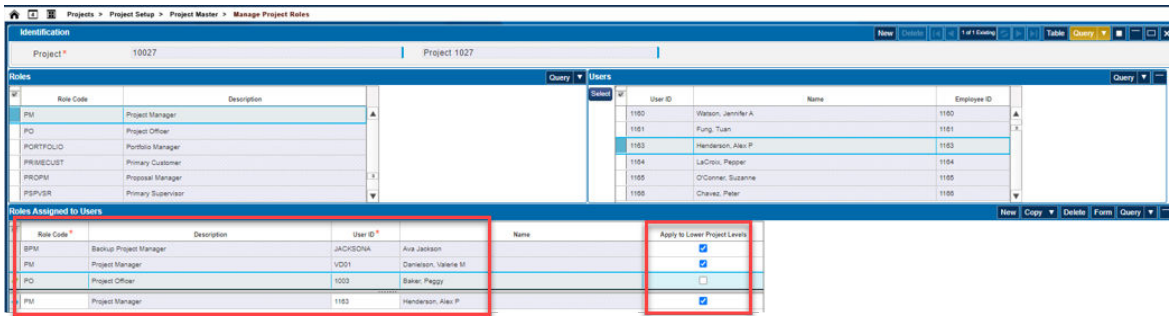
1. In Costpoint, select **Admin** » **System Administration** » **System Administration Controls** » **Manage Functional Roles**.
2. Add the functional roles on the Manage Functional Roles screen and select the corresponding **BI** check box. Click **Save**.



3. In Costpoint, select **Projects** » **Project Setup** » **Project Master** » **Manage Project User Flow**.
4. Click the **Project Roles** subtask.



5. Add roles to the project. Click **Save**.



> **Note:** Multiple users can be assigned to the same roles. Users who are assigned to the top level will automatically see all levels below. You can also assign users to lower levels.

Enable Project Role Security

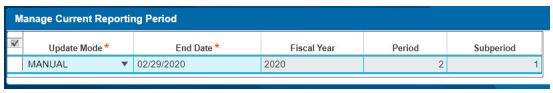
You can turn on the switch for Project Role Security through the Manage BI Settings screen.

To turn on Project Role Security:

1. In Costpoint, select **Report & Analytics** » **BI Controls** » **Manage BI Settings** .
2. Select **Yes** in the **Use Project Roles Security** drop-down list to enable Project Roles Security. Click **Save**.

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.



To set up the Costpoint Business Intelligence current reporting period:

1. In Costpoint, launch the Manage Current Reporting Period (BIMRPTCURPD) application (**Reports & Analytics** » **BI Controls** » **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. **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. 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. 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.
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**.

Portal Visibility Filter

The Portal Visibility Filter is a way to manage which content, report, and folders users can see in Costpoint Business Intelligence.

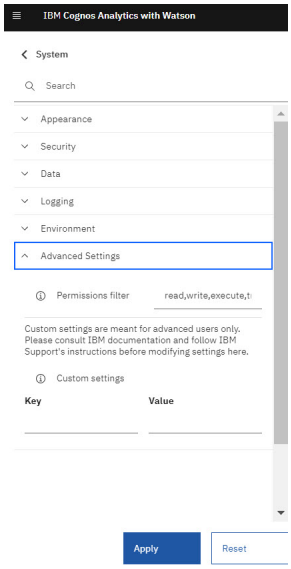
The default filters are read, write, execute, traverse, and setPolicy in Costpoint Business Intelligence, there are business cases where filters need to work alongside permissions and additional steps need to be performed.

Set the Visibility Filter

As default, the **Content_Service.permissionsFilter** parameter has values: read, write, execute, traverse, and setPolicy. In Costpoint Business Intelligence, you need to customize the values to read, write, and setPolicy in order for the permissions and visibility to work.

To change the parameter value:

1. In Costpoint BI, click ☰. And then, click **Manage** » **Configuration** » **System** » **Advance Settings**



2. Enter **Content_Service.permissionsFilter** in the **Key** field.
3. Enter the new values **read,write,setPolicy** in the **Value** field.
4. Click **Apply**.
5. Wait 20 seconds.
6. Log out.

Map the Costpoint CER User Groups to Cognos User Groups

Create the link between the user groups in Costpoint to the Cognos user groups. In this way, the Costpoint user groups can be in sync with the CER user groups. This is a one-time setup that needs to be performed by on-premise customers only.

Note: For each Costpoint CER User Group, there is a corresponding Cognos User Group with the same name. For example, the **CER Projects** in Costpoint CER User Group corresponds to the **CER Projects** in the Cognos User Group.

To map the Costpoint CER User Groups to Cognos User Groups:

1. In Costpoint BI, click ☰. And then, click **Manage** » **Administration Console**.
2. In IBM Cognos Administration, click the **Security** tab.
3. Go to the Cognos User Group that you want to map with Costpoint CER User Group and open it.

   For example, if you want to map **CER Projects**, click **Cognos** » **Deltek** » **CER Projects**.

   See the table at the end of the procedure as guide.
4. Once the user group is opened (for example, CER Projects), click the **Members** tab.
5. Click **Add...**.
6. In the **Available entries** box on the left, click **CAP** » **Deltek Groups**.
7. Select the Costpoint CER User Group that you want to map to your Cognos Group. For example, **CER Projects**.
8. Click the yellow arrow to transfer the selected user group to the **Selected entries** box on the right. Click **OK**.
9. Click **OK** again to close the Properties page for the User Group.
10. Repeat steps 3 to 10 until all Costpoint CER User Groups are mapped to Cognos User Groups.

Cognos User Group	Costpoint Cognos User Group(CAP)
Under **Cognos** » **Deltek** » **CER Accounting**	**CAP** » **Deltek Group** » **CER Accounting** *This is a legacy group. No need to map for first time BI users.*
Under **Cognos** » **Deltek** » **CER Accounting All Secure**	**CAP** » **Deltek Group** » **CER Accounting All Secure**
Under **Cognos** » **Deltek** » **CER Cloud Administrator**	**CAP** » **Deltek Group** » **CER Cloud Administrator** *No need to map.*
Under **Cognos** » **Deltek** » **CER Accounts Payable Secure**	**CAP** » **Deltek Group** » **CER Accounts Payable Secure**

Cognos User Group	Costpoint Cognos User Group(CAP)
Under **Cognos » Deltek » CER Accounts Receivable Secure**	**CAP » Deltek Group » CER Accounts Receivable Secure**
Under **Cognos » Deltek » CER Advanced Lite**	**CAP » Deltek Group » CER Advanced Lite**
Under **Cognos » Deltek » CER Advanced User**	**CAP » Deltek Group » CER Advanced User**
Under **Cognos » Deltek » CER All**	**CAP » Deltek Group » CER All**
Under **Cognos » Deltek » CER CP Administration**	**CAP » Deltek Group » CER CP Administrator**
Under **Cognos » Deltek » CER Billing Secure**	**CAP » Deltek Group » CER Billing Secure**
Under **Cognos » Deltek » CER Consumer**	**CAP » Deltek Group » CER Consumer**
Under **Cognos » Deltek » CER Contracts**	**CAP » Deltek Group » CER Contracts**
Under **Cognos » Deltek » CER Developer**	**CAP » Deltek Group » CER Developer**
Under **Cognos » Deltek » CER Development**	**CAP » Deltek Group » CER Development**
Under **Cognos » Deltek » CER Employee Secure**	**CAP » Deltek Group » CER Employee Secure**
Under **Cognos » Deltek » CER Executive Secure**	**CAP » Deltek Group » CER Executive Secure**
Under **Cognos » Deltek » CER Expense Secure**	**CAP » Deltek Group » CER Expense Secure**
Under **Cognos » Deltek » CER Fixed Assets**	**CAP » Deltek Group » CER Fixed Assets**
Under **Cognos » Deltek » CER General Ledger Secure**	**CAP » Deltek Group » CER General Ledger Secure**
Under **Cognos » Deltek » CER HR**	**CAP » Deltek Group » CER HR** *This is a legacy group. No need to map for first time BI users.*
Under **Cognos » Deltek » CER HR Secure**	**CAP » Deltek Group » CER HR Secure**
Under **Cognos » Deltek » CER Labor Secure**	**CAP » Deltek Group » CER Labor Secure**
Under **Cognos » Deltek » CER Materials**	**CAP » Deltek Group » CER Materials**

Cognos User Group	Costpoint Cognos User Group(CAP)
	This is a legacy group. No need to map for first time BI users.
Under **Cognos** » **Deltek** » **CER Materials Secure**	**CAP** » **Deltek Group** » **CER Materials Secure**
Under **Cognos** » **Deltek** » **CER Manufacturing Secure**	**CAP** » **Deltek Group** » **CER Manufacturing Secure**
Under **Cognos** » **Deltek** » **CER Materials Manufacturing All Secure**	**CAP** » **Deltek Group** » **CER Materials Manufacturing All Secure**
Under **Cognos** » **Deltek** » **CER Payroll Secure**	**CAP** » **Deltek Group** » **CER Payroll Secure**
Under **Cognos** » **Deltek** » **CER People**	**CAP** » **Deltek Group** » **CER People** *This is a legacy group. No need to map for first time BI users.*
Under **Cognos** » **Deltek** » **CER Planning (Projects)**	**CAP** » **Deltek Group** » **CER Planning (Projects)**
Under **Cognos** » **Deltek** » **CER Planning (Projects) Secure**	**CAP** » **Deltek Group** » **CER Planning (Projects) Secure**
Under **Cognos** » **Deltek** » **CER Project Manager Security**	**CAP** » **Deltek Group** » **CER Project Manager Security**
Under **Cognos** » **Deltek** » **CER Procure Secure**	**CAP** » **Deltek Group** » **CER Procurement Secure**
Under **Cognos** » **Deltek** » **CER Projects**	**CAP** » **Deltek Group** » **CER Projects** *This is a legacy group. No need to map for first time BI users.*
Under **Cognos** » **Deltek** » **CER Projects Secure**	**CAP** » **Deltek Group** » **CER Projects Secure**
Under **Cognos** » **Deltek** » **CER Subcontractor Management Secure**	**CAP** » **Deltek Group** » **CER Subcontractor Management Secure**
Under **Cognos** » **Deltek** » **CER Time & Expense**	**CAP** » **Deltek Group** » **CER Time & Expense** *This is a legacy group. No need to map for first time BI users.*
Under **Cognos** » **Deltek** » **CER Time Secure**	**CAP** » **Deltek Group** » **CER Time Secure**
Under **Cognos** » **Deltek** » **CER User**	**CAP** » **Deltek Group** » **CER User**

Configure Capability Permissions

Permissions for BI capabilities need to be manually added in order to be in compliance with Deltek licensing. Unfortunately, these settings are not imported from the deployment file.

There are different access permissions that can be applied to the capabilities per user role and the following sections will guide you on how to make these configurations. All of the procedures are based on the Detailed Capabilities by Role matrix and it should be the result of the configuration when you have completed the capability permissions setup.

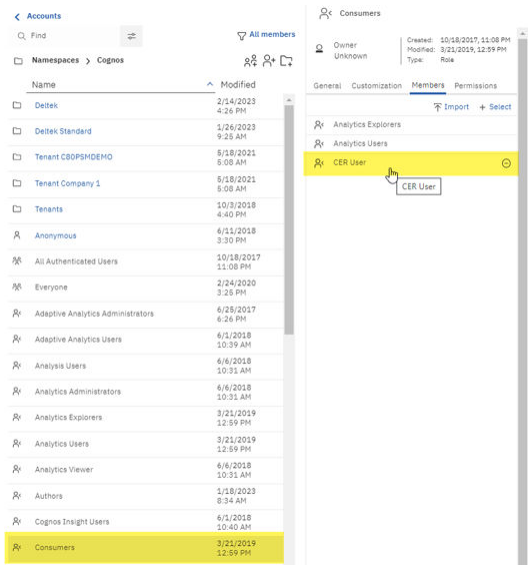
Remove Associations to IBM Roles (for Upgrading Users Only)

For users who are upgrading their Costpoint BI installation or Cognos Analytics to 11.2.4 FP2, you must remove the associations of CER roles to IBM roles. This is to preserve the appropriate Costpoint BI capabilities of users.

This procedure should only be performed by users who are upgrading the Costpoint BI or Cognos Analytics setup. Otherwise, skip this procedure.

To remove associations of CER roles to IBM roles :

1. In Costpoint BI, click the **Open menu** ☰ on the upper left-hand side of the BI screen. Click **Manage** » **People** » **Accounts** » **Cognos**.
2. Click the **More** icon (⋮) beside the **Consumers** and then click **View members**.
3. Click minus sign (-) beside any CER user. For example, **CER User**.



4. On the dialog box, click **OK** to confirm deletion.
5. Repeat step 3 and remove the rest of the CER users, if any.
6. When all CER users are removed for **Consumers**, repeat steps 2 to 5 for the following IBM roles:

- **Analytics Explorer**
- **Analytics User**

Add User Roles to Capabilities and their Children

Assign capabilities to CER users for them to perform their corresponding function.

Note: Perform this procedure if you plan to apply user roles in your BI implementation. Otherwise, skip this procedure. There are also user roles indicated in this procedure that you may not have the required licenses such as the CER Web Administrator and CER Developer. If you do not have the licenses, you may skip the configuration for them.

To add user roles to capabilities:

1. In Costpoint BI, click ☰. Click **Manage** » **People** » **Capabilities**.
2. Look for the **Capability** for which you want to assign a **Permission**. For example, **Cognos Viewer**.
3. Click the More icon (⋮) beside the **Capability** and then click **Customize access**.
4. On the **Access** tab, click the plus (+) sign beside the **Permissions** header and select the role that you want to add to the **Capability**. For example, for the **Cognos Viewer** capability, select the **CER Consumer** role which is found in **Cognos** » **Deltek** » **CER Consumer**.
5. Click **Add**.
6. On the **Access** tab, select the added role (for example, **CER Consumer**), and select the permission to assign.

   In our example, **CER Consumer**, select **Access** under the **Permissions** column.
7. Click **Apply to all children** to apply the changes to the corresponding sub-capabilities, in this case, the sub-capabilities of **Cognos Viewer**. Otherwise, skip this step. And then, click **Apply** on the dialog box.
8. Repeat steps 2 to 7 for the other capabilities in the following table.

Capability	Role
Adaptive Analytics	Add **CER Web Administrator**. Select **Access** under **Permissions** for each role.
Administration	Add **CER Web Administrator**. Select **Access** under **Permissions** for each role. Click **Apply to all children**.
AI	Add: **Cognos** » **Everyone**. Select **Access** under **Permissions** for each role.
Learning	Add: **Cognos** » **Everyone**. Select **Access** under **Permissions** for each role.

Capability	Role
Use Assistant *This is under the **Learning** capability.*	Add: ▪ **CER User** ▪ **CER Advanced Lite** ▪ **CER Advanced User** ▪ **CER Developer** Select **Access** under **Permissions** for each role.
Analysis Studio	Add: ▪ **CER User** ▪ **CER Advanced Lite** ▪ **CER Advanced User** ▪ **CER Developer** Select **Access** under **Permissions** for each role.
Attach Outputs	Add: ▪ **CER Consumer** ▪ **CER User** ▪ **CER Advanced Lite** ▪ **CER Advanced User** ▪ **CER Developer** Select **Access** under **Permissions** for each role.
Collaborate	Add: ▪ **CER User** ▪ **CER Advanced Lite** ▪ **CER Advanced User** ▪ **CER Developer** Select **Access** under **Permissions** for each role. Click **Apply to all children**.
Dashboard	Add: ▪ **CER User** ▪ **CER Advanced Lite** ▪ **CER Advanced User** ▪ **CER Developer** Select **Access** under **Permissions** for each role.

Capability	Role
	Click **Apply to all children**.
Data sets	Add: ▪ **CER Advanced User** ▪ **CER Developer** Select **Access** under **Permissions** for each role.
Desktop Tools	Add **CER Developer**. Select **Access** under **Permissions** for each role.
Detailed Errors	Add: ▪ **CER Advanced User** ▪ **CER Developer** Select **Access** under **Permissions** for each role.
Develop Visualizations	Add: ▪ **CER Advanced User** ▪ **CER Developer** Select **Access** under **Permissions** for each role.
Email	Add: **Cognos** » **Everyone**. Select **Access** under **Permissions** for each role. Click **Apply to all children**.
Event Studio	Add: ▪ **CER Advanced Lite** ▪ **CER Advanced User** ▪ **CER Developer** Select **Access** under **Permissions** for each role.
Execute Indexed Search	Add: **Cognos** » **Everyone**. Select **Access** under **Permissions** for each role.
Executive Dashboard	Add ▪ **CER User** ▪ **CER Advanced Lite** ▪ **CER Advanced User** ▪ **CER Developer** . Select **Access** under **Permissions**. Click **Apply to all children**.

Capability	Role
Exploration	Add: ▪ **CER Advanced Lite** ▪ **CER Advanced User** ▪ **CER Developer** Select **Access** under **Permissions** for each role.
External Content	Add **CER Cloud Administrator**. Select **Access** under **Permissions**. Click **Apply to all children**.
External Repositories	Add: **Cognos** » **Everyone**. Select **Access** under **Permissions** for each role. Click **Apply to all children**.
Generate CSV Output	Add: **Cognos** » **Everyone**. Select **Access** under **Permissions** for each role.
Generate PDF Output	Add: **Cognos** » **Everyone**. Select **Access** under **Permissions** for each role.
Generate XLS Output	Add: **Cognos** » **Everyone**. Select **Access** under **Permissions** for each role.
Generate XML Output	Add: **Cognos** » **Everyone**. Select **Access** under **Permissions** for each role.
Glossary	Add: **Cognos** » **Everyone**. Select **Access** under **Permissions** for each role.
Hide Entries	Add: **Cognos** » **Everyone**. Select **Access** under **Permissions** for each role.
Import Relational Metadata	Add: ▪ **CER Developer** ▪ **CER Web Administrator** Select **Access** under **Permissions** for each role.
Job	Add: ▪ **CER Advanced User** ▪ **CER Developer** ▪ **CER Web Administrator** Select **Access** under **Permissions** for each role.
Lineage	Add: **Cognos** » **Everyone**. Select **Access** under **Permissions** for each role.

Capability	Role
Manage Content	Add **CER Web Administrator**. Select **Access** under **Permissions** for each role.
Manage Own Data Source Signons	Add **CER Web Administrator**. Select **Access** under **Permissions** for each role.
Query Studio	Add: ▪ **CER Advanced Lite** ▪ **CER Advanced User** ▪ **CER Developer** Select **Access** under **Permissions** for each role. Click **Apply to all children**.
Report Studio	Add: ▪ **CER Advanced Lite** ▪ **CER Advanced User** ▪ **CER Developer** Select **Access** under **Permissions** for each role.
Create/Delete *This is under the **Report Studio** capability.*	Add: ▪ **CER Advanced Lite** ▪ **CER Advanced User** ▪ **CER Developer** Select **Access** under **Permissions** for each role. Click the **Override parent access** toggle to turn it on.
Edit Burst Definition *This is under the **Report Studio** capability.*	Add: ▪ **CER Advanced Lite** ▪ **CER Advanced User** ▪ **CER Developer** Select **Access** under **Permissions** for each role. Click the **Override parent access** toggle to turn it on.
Edit HTML Items *This is under the **Report Studio** capability.*	Add: ▪ **CER Advanced User** ▪ **CER Developer** Select **Access** under **Permissions** for each role.

Capability	Role
	Click the **Override parent access** toggle to turn it on.
Edit User Defined SQL *This is under the **Report Studio** capability.*	Add: ▪ **CER Advanced User** ▪ **CER Developer** Select **Access** under **Permissions** for each role. Click the **Override parent access** toggle to turn it on.
Generate Burst Output *This is under the **Report Studio** capability.*	Add: ▪ **CER Advanced Lite** ▪ **CER Advanced User** ▪ **CER Developer** Select **Access** under **Permissions** for each role. Click the **Override parent access** toggle to turn it on.
Run HTML Items *This is under the **Report Studio** capability.*	Add: ▪ **CER Consumer** ▪ **CER User** ▪ **CER Advanced Lite** ▪ **CER Advanced User** ▪ **CER Developer** Select **Access** under **Permissions** for each role. Click the **Override parent access** toggle to turn it on.
Run User Defined SQL *This is under the **Report Studio** capability.*	Add: ▪ **CER Consumer** ▪ **CER User** ▪ **CER Advanced Lite** ▪ **CER Advanced User** ▪ **CER Developer** Select **Access** under **Permissions** for each role. Click the **Override parent access** toggle to turn it on.
Scheduling (and Subscriptions)	Add:

Capability	Role
	▪ **CER Consumer** ▪ **CER User** ▪ **CER Advanced Lite** ▪ **CER Advanced User** ▪ **CER Developer** Select **Access** under **Permissions** for each role.
Schedule by Day *This is under the **Scheduling (and Subscriptions)** capability.*	Add: ▪ **CER Consumer** ▪ **CER User** ▪ **CER Advanced Lite** ▪ **CER Advanced User** ▪ **CER Developer** Select **Access** under **Permissions** for each role. Click the **Override parent access** toggle to turn it on.
Schedule by Hour *This is under the **Scheduling (and Subscriptions)** capability.*	Add: ▪ **CER Advanced Lite** ▪ **CER Advanced User** ▪ **CER Developer** Select **Access** under **Permissions** for each role. Click the **Override parent access** toggle to turn it on.
Schedule by Month *This is under the **Scheduling (and Subscriptions)** capability.*	Add: ▪ **CER Consumer** ▪ **CER User** ▪ **CER Advanced Lite** ▪ **CER Advanced User** ▪ **CER Developer** Select **Access** under **Permissions** for each role. Click the **Override parent access** toggle to turn it on.
Schedule by Week *This is under the **Scheduling (and Subscriptions)** capability.*	Add: ▪ **CER Consumer**

Capability	Role
	▪ **CER User** ▪ **CER Advanced Lite** ▪ **CER Advanced User** ▪ **CER Developer** Select **Access** under **Permissions** for each role. Click the **Override parent access** toggle to turn it on.
Schedule by Year *This is under the **Scheduling (and Subscriptions)** capability.*	Add: ▪ **CER Advanced Lite** ▪ **CER Advanced User** ▪ **CER Developer** Select **Access** under **Permissions** for each role. Click the **Override parent access** toggle to turn it on.
Snapshots	Add: **Cognos** » **Everyone**. Select **Access** under **Permissions** for each role.
Upload Files	Add: ▪ **CER Advanced User** ▪ **CER Developer** ▪ **CER Web Administrator** Select **Access** under **Permissions** for each role.
View Generate Query Text	Add: **Cognos** » **Everyone**. Select **Access** under **Permissions** for each role.
Watch Rules	Add: ▪ **CER User** ▪ **CER Advanced Lite** ▪ **CER Advanced User** ▪ **CER Developer** Select **Access** under **Permissions** for each role.
Web-based Modeling	Add: ▪ **CER Advanced User** ▪ **CER Developer** Select **Access** under **Permissions** for each role.

Capability	Role
Edit Data Module Defined SQL *This is under the **Web-based Modeling** capability.*	Add: ▪ **CER Advanced User** ▪ **CER Developer** Select **Access** under **Permissions** for each role. Click the **Override parent access** toggle to turn it on.
Use Data Module Defined SQL *This is under the **Web-based Modeling** capability.*	Add: ▪ **CER Consumer** ▪ **CER User** ▪ **CER Advanced Lite** ▪ **CER Advanced User** ▪ **CER Developer** Select **Access** under **Permissions** for each role. Click the **Override parent access** toggle to turn it on.

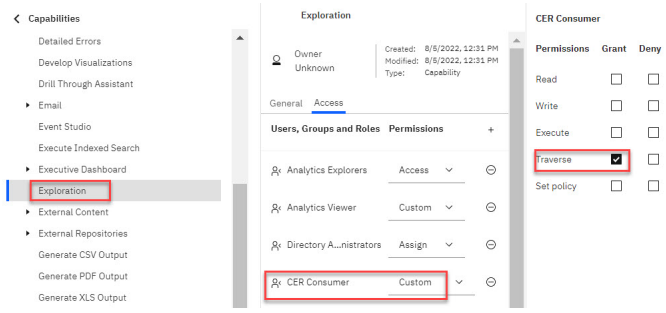
Customize a Capability for a User Role

Some user roles require a more customized set of permissions for them to use a capability or to be in compliance with Deltek licensing. You can either grant or deny access permissions of user roles to certain capabilities.

To customize a capability for a user role:

1. In Costpoint BI, click ☰. Click **Manage** » **People** » **Capabilities**.
2. Look for the **Capability** for which you want to assign a **Permission**. For example, **Exploration**.
3. Click the More icon (⋮) beside the **Capability** and then click **Customize access**.
4. On the **Access** tab, click the plus (+) sign beside the **Permissions** header and select the role that you want to add to the **Capability**. For example, for the **Cognos Viewer** capability, select the **CER Consumer** role which is found in **Cognos** » **Deltek** » **CER Consumer**.
5. Click **Add**.
6. On the **Access** tab, select the added role (for example, **CER Consumer**), and select the permission to assign.

   In our example, **CER Consumer**, select **Custom** under the **Permissions** column.
7. Click the **Traverse** check box under the **Grant** column.



8. Repeat steps 2 to 7 for the other capabilities in the following table.

Capability	Role
Data sets	Add: ▪ **CER Consumer** ▪ **CER User** ▪ **CER Advanced Lite** Select **Custom** under **Permissions**. Click the **Execute** and **Traverse** check boxes under the **Deny** column.
Exploration	Add **CER User** . Select **Custom** under **Permissions**. Click the **Traverse** check box under the **Grant** column.
Report Studio	Add **CER Consumer** and **CER User** . Select **Custom** under **Permissions**. Click the **Traverse** check box under the **Grant** column.
Upload Files	Add: ▪ **CER Consumer** ▪ **CER User** ▪ **CER Advanced Lite** Select **Custom** under **Permissions**. Click the **Execute** and **Traverse** check boxes under the **Deny** column.
Web-based Modeling	Add: ▪ **CER Consumer** ▪ **CER User** ▪ **CER Advanced Lite**

Capability	Role
	Select **Custom** under **Permissions**. Click the **Execute** and **Traverse** check boxes under the **Deny** column.

Remove a User Role Assigned to a Capability

There are instances where an assigned user role need to be removed from a Capability.

To remove a user role assignment from a Capability:

1. In Costpoint BI, click ☰. Click **Manage** » **People** » **Capabilities**.
2. Look for the **Capability** for which you want to remove an assigned role. For example, **Executive Dashboard** » **Use Advanced Dashboard Features**.
3. Click the More icon (⋮) beside the **Capability** and then click **Customize access**.
4. On the **Access** tab, look for **CER User** and click the adjacent minus sign (-) to remove the member in the list . Click **OK** on the dialog box that confirms the deletion.
5. If the capability has a parent, make sure that the **Override parent access** toggle is turned on. Otherwise, skip this step.
6. Repeat steps 2 to 6 for the other capability in the following table.

Capability	Role
Manage Repository Connections *This capability is under **External Repositories***	Remove: ▪ **CER Consumer** ▪ **CER User** ▪ **CER Advanced Lite** ▪ **CER Advanced User** ▪ **CER Developer** Turn on the **Override parent access** toggle.

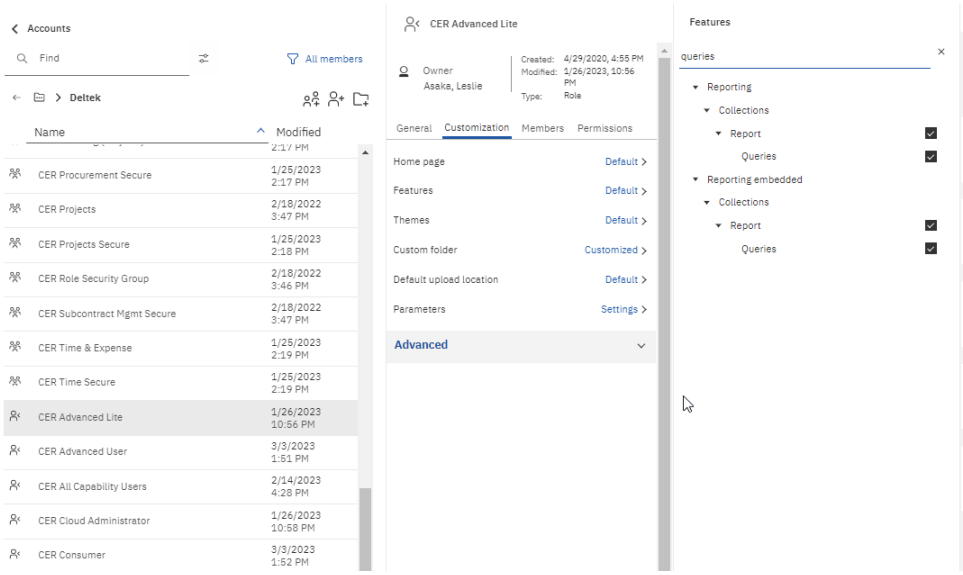
Verify the CER__ADV_LITE User Query Permission

The MS SQL query permissions for CER__ADV_LITE users should be automatically applied from the deployment file. This procedure will verify if the correct settings are in place.

You should have a system administrator role in order to perform this procedure.

To verify if the MS SQL query permission of the CER__ADV_LITE user is correct:

1. Login as System Administrator.
2. On the Costpoint BI screen, click ☰. Click **Manage** » **People** » **Accounts** » **Cognos** » **Deltek**.
3. Click the ellipsis next to **CER Advanced Lite** role and select **Properties**.
4. Click the **Customization** tab.
5. Click **Default** next to **Features**.
6. On the **Features** pane, enter **queries** on the search field on top and press **ENTER**. All items with **Queries** will display.
7. Check to see if the **Queries** check boxes are selected. If not, select them.
8. Click **Apply** to save changes.

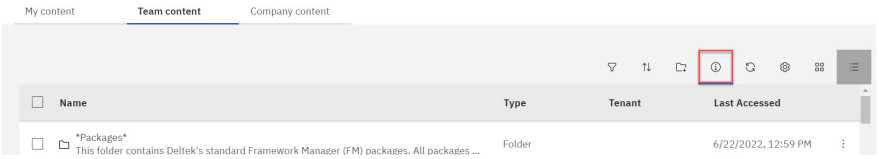


Add Everyone and Assign Read Access to Team Content

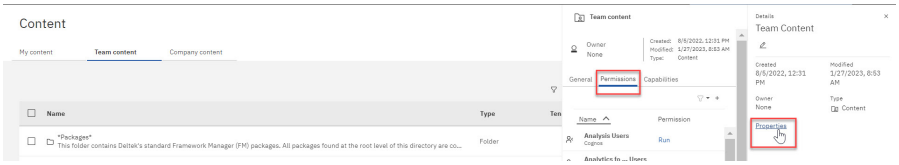
The Everyone user needs to have Read access to Team Content.

To add Everyone and assign access to Team Content:

1. In Costpoint BI, click the **Open menu** icon (☰). And then, click **Content**.
2. Click the **Team Content** tab. And then, click the **Details** icon.



3. Click **Properties**. And then, click the **Permissions** tab.



4. If there is a user displayed, remove it by clicking the minus sign adjacent to it. All users must be removed.
5. Click the **Plus** (⊕) icon to open the screen for selecting groups, users, or roles.
6. On the **Select groups, users or roles** screen, click **Cognos** » **Everyone**. Click **Add**. **Everyone** will be added to the list of roles on the **Permissions** area for the tenant folder.
7. On the **Permissions** area, select the drop-down for **Permissions** for **Everyone** and select **Read**.
8. Click **Apply**.
9. Refresh browser.

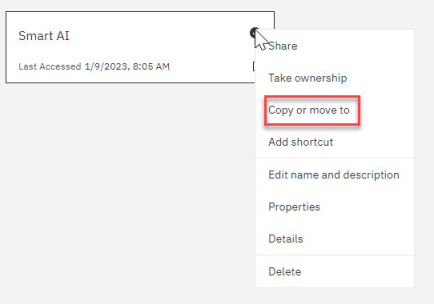
Copy the Smart AI Folder to Company Content

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, click the **Team content** tab. And then, click **Smart AI Admin**.
2. Click the action menu for **Smart AI** and click **Copy or move to**.



3. On the **Copy or move: Smart AI** dialog box, select a destination within **Company content** that you like to copy the folder into.
4. Click **Copy** 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.

Validate User Groups

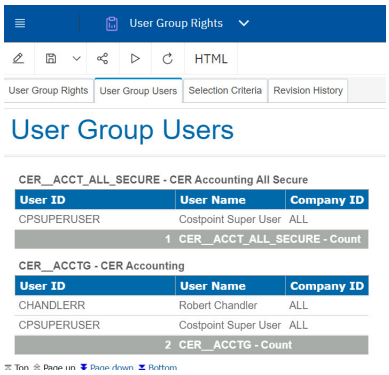
After you complete the steps in the post-installation phase, check the list of users per user group in Costpoint Business Intelligence against your accomplished Security Planning Template.

To perform this procedure, you must have access to the **User Group Rights** report in **Team Content** » **Costpoint 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, click **Team Content** » **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 **Finish**.
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.



Apply the Deltek Theme to Cognos Analytics

Deltek provides a theme as part of your Costpoint Business Intelligence installation. The theme renders a consistent look and feel such as applying colors on the banner and search field.

To apply the Deltek theme to your Cognos Analytics portal:

1. Click the open menu (☰), and then click **Manage** » **Customization**.
2. Select **Deltek** and click **Apply**.
3. Select **Theme_CSS** and click **Apply**.

> **Caution:** For on-premise users who use CAP, you may receive a message to refresh your browser to apply the theme. However, Deltek recommends that you log out of Costpoint and log back in to properly apply the theme. Otherwise, you may receive an error when you refresh your browser. If an error still occurs, log in as an active directory user when you apply the Deltek theme. This may solve the issue.

> **Note:** If any of the themes is not available, click the **Upload theme** icon and browse through the location of the file.
>
> - The default location of the**Deltek.zip** file is **C:\Program Files (x86)\Deltek \CostpointEnterpriseReporting (or CostpointBusinessIntelligence)\<Costpoint BI version>\Branding**
> - The default location of the **Theme_CSS.zip** file is **C:\Program Files (x86)\Deltek \CostpointBusinessIntelligence\<Costpoint BI version>\Extensions**

Check Extensions

Verify that the extensions to run Costpoint BI are available. Otherwise, they need to be installed.

On the Welcome page, go to **Manage** » **Customization**, and then click the **Extensions** tab. Check if the following extensions have already been installed.

- **CUSTOM_TAB**: This extension is used for the customized tab on the landing page of Costpoint BI.
- **Deltek_Custom_Media_All**: This extension enables the use of images on dashboards and reports. Currently, it is used for custom images on the HR dashboards.
- **EXCLUDE_HOME**: This extension removes the welcome banner and the **Quick Launch** section on the landing page of Costpoint BI.
- **ExtendTime**: This extension lets Costpoint recognize that you are actively working within Costpoint BI, thus, preventing the Costpoint timeout notification and potential loss of work.
- **Theme_CSS**: This extension updates the color of the Search field.
- **Learning Panel**: This extension contains links to other sources of support such as videos and IBM Documentation.
- **LinkWidget**: This extension enables the creation of buttons on dashboards that points to external web-based links.
- **responsiveLayout**: This extension helps in rendering Costpoint BI dashboards on mobile devices.
- **System_CAMobile**: This extension is used for mobile security.

Install Extensions

The extensions files are available in the **Extensions** folder in your installation

You must have system administrator user permission rights to apply the extensions. You must also have access to the **Extension** folder of the latest Costpoint Business Intelligence installation.

> **Note:** Only perform this procedure when an extension is not installed or missing in the **Extensions** tab of the **Customization** screen.

To install the extensions:

1. Log in to Costpoint as a system administrator. And then, launch **Business Intelligence** in the **Reports & Analytics** domain.
2. Go to **Manage** » **Customization**. Click the **Extensions** tab.
3. Click the **Upload extension** icon and browse through the location of the extensions files. Select the files. Click **Open**.

   The default location of the extensions files is **C:\Program Files (x86)\Deltek\CostpointBusinessIntelligence\<Costpoint BI version>\zSupport Files\Extensions**.

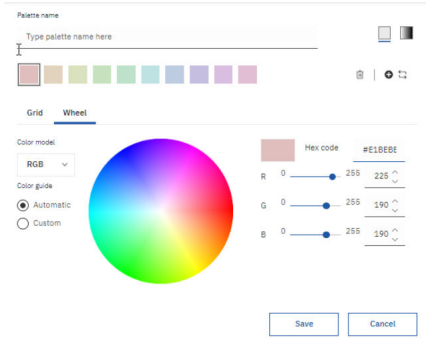
When the extension has been successfully installed, you and other users will see them on the **Extensions** tab of **Manage** » **Customization** .

Create Custom Color Palette

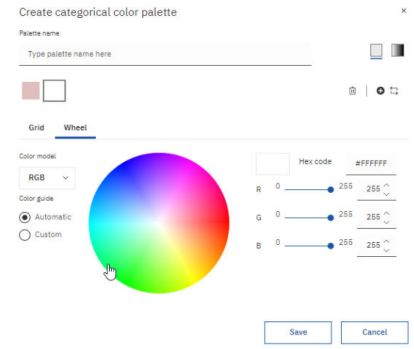
Some dashboards use a custom color palette when rendering. Perform this procedure to apply them.

To create a custom color palette:

1. Enter your first step here.
   On the main page of Costpoint BI, click the **Open menu** (☰). Click **Manage** » **Customization**.
2. Click the **Palettes** tab and click the plus sign (**+**) to add a new palette.
3. Enter **Deltek 1 - Project Hub (AR Chart)** in the **Palette name** field.
4. Click the **Wheel** tab. Click the first color box and enter **Hex code #E1BEBE**.



5. Click the second color box and enter **Hex code #FFFFFF**.



> **Tip:** You might need to click the color wheel first before you enter the **Hex code #FFFFFF**. In this way, the system will recognize your entry and will save it.

6. Click **Create**.
7. On the **Palettes** tab, click the plus (**+**) sign to add another palette.
8. Enter **Deltek 1 - Project Hub (AR Chart)** in the **Palette name** field.
9. Click the **Wheel** tab. Click the first color box and enter the **Hex code #D6D1D9**.
10. Click the second color box and enter the **Hex code #FFFFFF**.

> **Tip:** You might need to click the color wheel first before you enter the **Hex code #FFFFFF** for the system to recognize and save it.

11. Click **Create**.

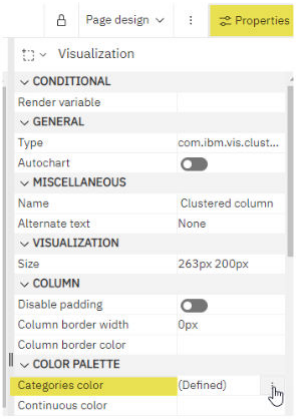
Update Project Health Reports with Global Color Palette

Perform this procedure to apply the global color palette to the Project Health report.

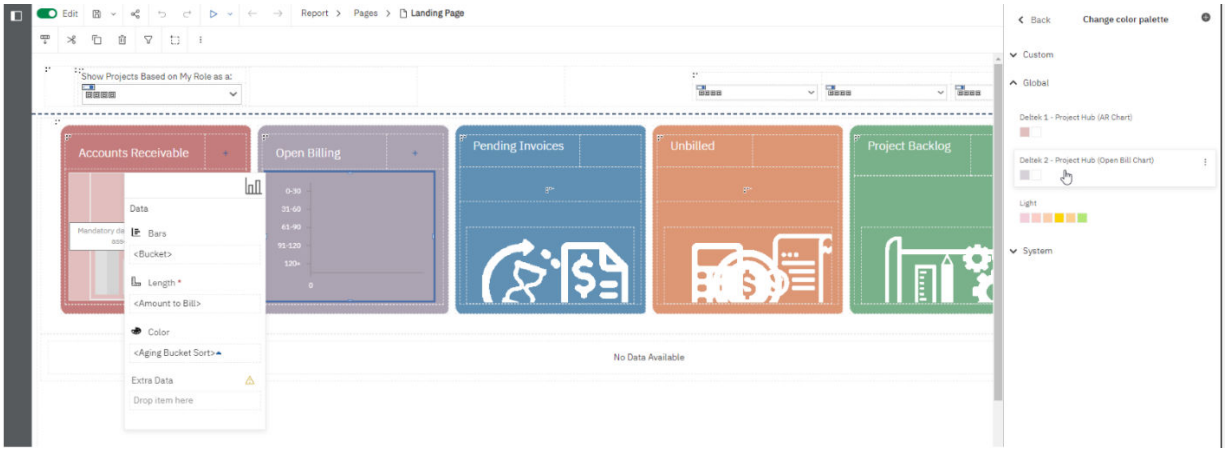
The global color palettes **Deltek 1 – Project Hub (AR Chart)** and **Deltek 2 - Project Hub (Open Bill Chart)** have already been created.

To update the report:

1. Open **Team Content** » **Projects** » **Reports** » **Project Health**.
2. Right-click **Project Health** and select **Edit report**.
3. Click on **Accounts Receivable** widget or box.
4. Open the Properties panel.
5. On the **Categories color** field under **COLOR PALETTE**, set AR Chart to **Global** » **Deltek 1 - Project Hub (AR Chart)**.



6. Click the **Open Billing** chart. On the Properties panel, select **GlobalDeltek 2 - Project Hub (Open Bill Chart)** as **Categories color**. Click **Save**.



7. Open **Team Content** » **Projects** » **Reports** » **Project Health Drill Thru**. Repeat Steps 2 to 6 to apply the global color palette.

> **Note:** A proposal has been submitted to IBM that will allow the inclusion of custom color palettes in deployment files. This proposed change will enable custom palettes to be downloaded or exported to test or production environments. Once this enhancement has been approved, you no longer need to manually customize global color palettes in reports such as Project Health. Help add this proposed change to a future release of Cognos Analytics by voting through IBM's Ideas Portal: Ability to download/upload Custom Palette. You need to sign up for an IBMid to vote.

Optional Tasks

This concludes all of the post-installation configuration tasks that must be completed prior to first-use.

However, there are other optional tasks that you can do as administrator such as to improve the display of reports by adding a bar code font and maintain a schedule to refresh data.

Configure the Barcode Font for Reports

In order to display the barcodes on reports, you need to copy the barcode font to the Cognos Server and the desktops that you use to view the report.

> **Note:** The Costpoint Business Intelligence installation includes a copy of the barcode font file, **FRE3OF9X.ttf**, in the font folder of the installation directory (for example, C:\Program Files (x86)\Deltek\CostpointBusinessIntelligence\<*Costpoint BI version*>\Support Files\font).

You will also need to map the physical font in Cognos Configuration.

To set up the barcode font:

1. On your Cognos server, copy the barcode font to the following directories:
   - C:\Windows\fonts
   - <cognos_install>\bin\fonts
   - <cognos_install>\bin64\fonts

   > **Note:** You also need to copy the barcode font to the C:\Windows\fonts folder for all the computers that you use for viewing reports with barcode. If you do not install the barcode font on a computer, you can still view the barcode when you generate a PDF copy of the report.
2. Open IBM Cognos Configuration.
3. Click **Action** » **Edit Global Configuration...** » **Fonts** tab.
4. Click **Add...**, enter **FRE3OF9X** in the **Supported Font Name** field, and click **OK**.
5. In the **Explorer** pane, click **Environment** to display the Environment - Group Properties on the right pane.
6. Under the **Font Settings**, click the **Edit** button in the **Physical fonts map** field
7. On the Value - Physical fonts map dialog box, click **Add...** , enter **FRE3OF9X** in the **Global Font Name** field, and click the **Edit** button in the **Physical Font Name** field.
8. On the Physical Font Name dialog box, click **Search Now**, select **Free 3 of 9 Extended** from the list of fonts, and click **OK**.
9. Click **OK** to save the physical fonts map.
10. Restart the Cognos service.

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.

> **Note:** When you refresh data sets, the data loaded comes from the current environment. For example, if you want to use Smart AI in your test environment, create a separate copy of the Smart AI folder and data sets in addition to the production copy. In this way, when you refresh the data sets in the test environment, the data sets in production will not be affected.

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.

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. Right-click **AR Summary Data** and select **Refresh**.

   Note: You can also click **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

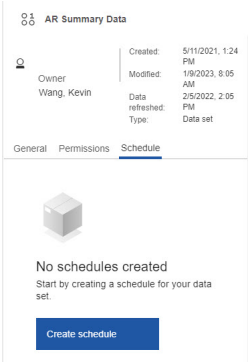
To avoid frequent data refresh, Deltek recommends to have a standard schedule to refresh data during off business hours.

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. Right -click **AR Data set** and then select **Properties**.
3. Click the **Schedule** tab. Click **Create schedule**.



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

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	

Dimensional Data Sets	Transactional Data Sets
Organizations	
Planning Project UDEFs	
Planning Projects	
Project UDEFs	
Projects	
Relative Fiscal Periods	
Resources	
Subperiods	

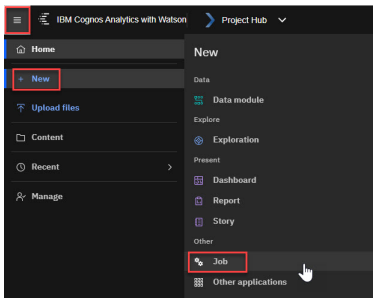
To run a job, right-click the job and select **Run as**. And then, follow the prompts on the dialog box that will display and click **Run**.

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 the **Open menu** icon (☰) and then 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. Leave the **Run options** with values:

   Run order = **Run in sequence** and **Continue on error** is **enabled**.
6. Click the **Save** icon on top of the screen to save your job.

7. 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.

Hidden Packages and Dashboards

For better generation and performance, some dashboards, for example, **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 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 the dashboards and packages in Smart AI for ease of use.

Unhide Packages and Dashboards

To unhide packages and dashboards, you should show hidden entries in Costpoint BI first in **Profile and Settings**.

You should have administrator rights to perform this procedure.

To unhide packages and dashboards:

1. On the upper right-hand side of the Costpoint BI screen, click the **Personal menu** icon ( ) and click **Profiles and settings**.
2. Click the **Settings** tab.
3. Click the **Show hidden entries** toggle to enable it.
4. Go to the package or dashboard that you want to unhide. For example, click **Team content** » **Planning**. Right-click the **Dashboards** folder and select **Copy or move to**.
5. On the dialog box, select a destination within **Company content** that you like to copy the folder into.
6. Click **Copy**.
   A confirmation message appears when the folder has been successfully copied.
7. Go to the location of the copied dashboard or package folder in **Company content** and right-click **Properties**.
8. On the **Properties** screen, click **Advanced** and clear the **Hide this entry** check box.

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