




Deltek

Deltek Costpoint Business Intelligence 8.0.17

Post Installation and
Configuration Guide for
On-premises Users

December 15, 2021



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

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

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

This edition published December 15, 2021.

© 2020 Deltek, Inc.

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

All trademarks are the property of their respective owners.

Contents

About this Guide.....	1
Prerequisites.....	2
Overview.....	3
Costpoint Business Intelligence Security.....	4
Step 1- Check the Model Security Configuration.....	4
Capability Security.....	7
Object Security.....	9
Model or Row Level Security.....	11
Portal Visibility Filter.....	15
Step 8 - Map the Costpoint CER User Groups to Cognos User Groups.....	17
Step 9 - Customize Capability Permissions.....	20
Step 10 - Customize Secured Feature Permissions.....	23
Step 11 - Customize CER__ADV_LITE User.....	27
Step 12 - Add Everyone and Assign Read Access to the Team Content Folder.....	28
Step 13 - Validate User Groups.....	29
Step 14 - Add the Deltek Theme to Cognos Analytics.....	30
Step 15 - Install ExtendTime.zip Extension.....	31
Optional Task.....	32
Configure the Barcode Font for MO Pick List Report.....	32
Special Topic 1: Organization, Labor Suppression, and Project Security in Costpoint.....	33
Special Topic 2: Organization and Project Security in Costpoint Planning.....	35
Special Topic 3: Detailed Capabilities by Role.....	37

About this Guide

Welcome to the Costpoint Business Intelligence 8.0.17 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 8.0.17 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 8.0.17 must be installed on Costpoint version 8.0.17.

Make sure you have successfully completed the following:

- Installed Cognos Analytics 11.1.7 FP1 where the Content Store database and Gateway dispatcher have been updated and configured
- Installed the Costpoint Authentication Provider (CAP) 8.0.x

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.

The steps in the Post Installation and Configuration phase are:

- **Step 1** — Check the Model Security Configuration
- **Step 2** — Complete the Capabilities Security Template
- **Step 3** — Complete the Object Security Template
- **Step 4** — Complete the Security Template for the CER Project Manager Group
- **Step 5** — Assign Costpoint Users to CER User Groups
- **Step 6** — Set Up Current Reporting Period
- **Step 7** — Set the Visibility Filter
- **Step 8** — Map the Costpoint CER User Groups to Cognos User Groups
- **Step 9** — Customize Capability Permissions
- **Step 10** — Customize Secured Feature Permissions
- **Step 11** — Customize CER ADV Lite User
- **Step 12** — Add Everyone and Assign Read Access to the Team Content Folder
- **Step 13** — Validate User Groups
- **Step 14** — Add the Deltek Theme to Cognos Analytics
- **Step 15** — Install ExtendTime Extension

There are special topics included in this guide that provides more information about Costpoint BI Security.

- Organization, Labor Suppression, and Project Security in Costpoint
- Organization and Project Security in Costpoint Planning
- Detailed Capabilities by Role

Costpoint Business Intelligence Security

There are different types of data security that you can apply in Costpoint Business Intelligence 8.0.17.

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

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

Step 1- Check the Model Security Configuration

Model security is enabled as 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. If model security is set to Yes, you must have an org security group assigned to each user or they will not be able to retrieve any data in the models that have data-level security (for example, Projects, Project Planning). In addition, parts security is always applied in Business Intelligence when it is used in Costpoint. See Special Topics for more information about security in Costpoint Business Intelligence.

To disable Model Security:

1. Log in to Costpoint and launch the Manager BI Settings (BIMCERSETTINGS) screen (**Reports and Analytics » BI Configuration » Configuration » Manager BI Settings**).
2. Select **No** in the corresponding fields where you want to disable security.

Field	Description
Enable Costpoint and Planning Model Security	<p>Select No to disable model security for the Costpoint and Costpoint Planning models. Model security is enabled by default.</p> <div> <p>Note: If you select No, only Model Security is disabled. Capability and Object Security are still in place in Costpoint Business Intelligence.</p> </div>
Use CP Organization Security By Module	<p>Select No to disable organization security in the new secure models which are:</p> <ul style="list-style-type: none"> Accounts Receivable Accounts Payable General Ledger Manufacturing Materials Procurement Projects
Enable T&E Model Security	<p>Select No to disable model security for the Time model.</p>

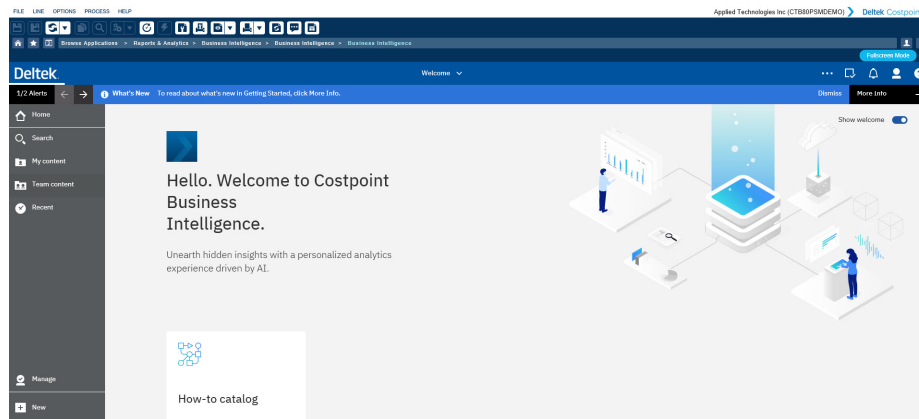
3. Click **Save**.

Assign Costpoint Business Intelligence Rights to the Administrator

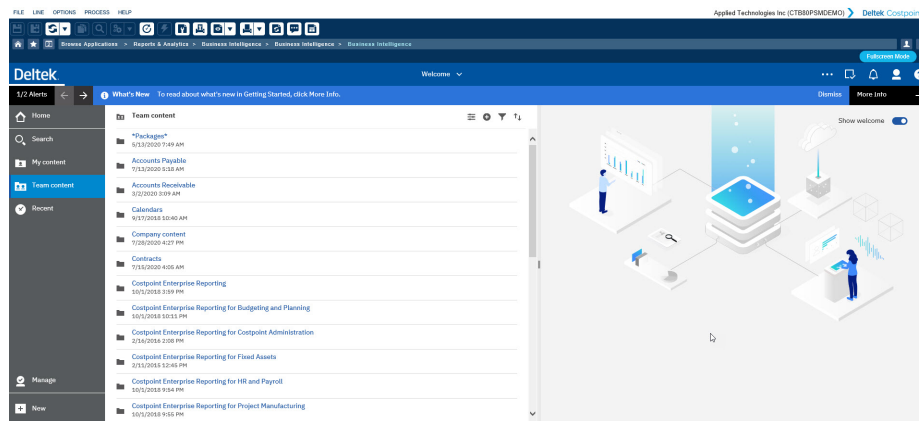
In order to access Costpoint Business Intelligence, the Administrator will need to be assigned to CER groups in Costpoint Security.

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

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

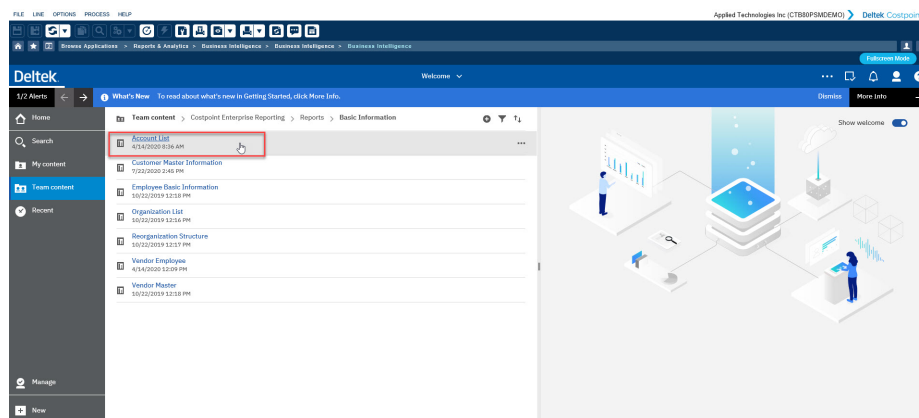


Then, click the Team content folder, and you should see the full folder structure.

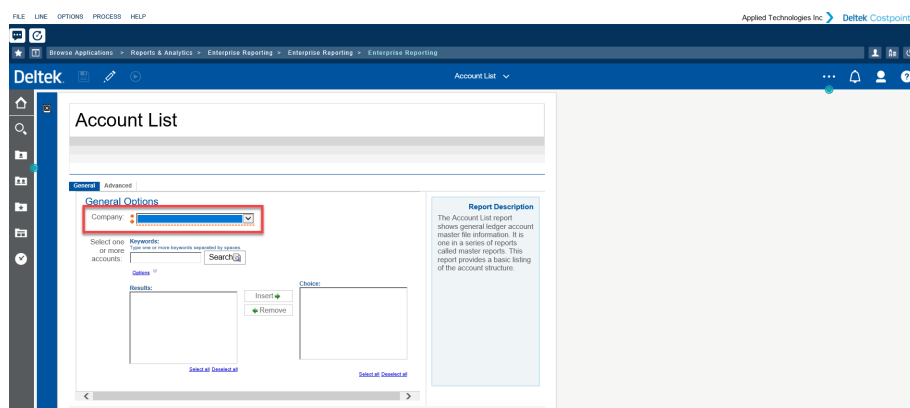


Then, run a report to ensure that you can access Costpoint data. Here is how you can run an Account List Report:

First, navigate to the report.



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



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

Capability Security

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

There is a CER user role included in your deployment for each Deltek license type. The table below displays the key functions available with each of the licenses.

Costpoint BI User Role Capabilities

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

Note: The Consumer (CER__CONSUMER) user has the least rights, basically someone who can only run and interact with existing reports. While you may not own this type of license and have CER users (**in Bundles**) and/or **Advanced CER licenses** instead, you might want to limit the capabilities for some individuals who you do not want to access or create dashboards. CER User is only available in CER Bundles (restricted).

License Types

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

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

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

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

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

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

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

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

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

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

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

Step 2 - Complete the Capabilities Security Template

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

To complete the Capabilities Security Template:

1. Launch the [Security Planning Template](#) and open the Capabilities Security tab.
2. Enter the number of licenses purchased by license type.
3. List all 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 at the parent folder or package will apply to any content contained within.

For example the **Team Content » Projects** folder, contains subfolders for packages, reports, and dashboards created from information in the Projects domain. Any user assigned to the **CER Projects** user group will be able to see all this content plus the legacy content as indicated in the table. A **CER Projects** user will see the secured project packages, reports, and dashboards plus all the legacy (or unsecured) project content as indicated in the table.

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

The permissions for all Deltek folders are set as 'RUN only' to prevent changes or modifications to the pre-established value-add which ensures a smoother upgrade path in the future. Customization of the Deltek content must be saved in the **Company content** folder.

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

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

A user must belong to at least one of these groups in order to see any Deltak content. A single user can be assigned to multiple groups. Use the [Security Planning Template](#) to plan which objects a user should have access to. If a user is assigned to one of these groups, they have access to all the reports and models for those objects. Please consider this before adding someone to one of the Object groups.

If all the content of an Object group is not assigned to a user, you do not have to assign them to a CER object group. You can only copy the content you would like them to see into the **Company content** folder. The **Company content** folder is managed by the administrator or other users designated by the administrator who can give rights to users or user groups to copies of dashboards/reports or custom dashboards/reports. So if you have a special use case that is not supported by Deltak security or folder organization, you have this area that is open to you to organize and secure based on your requirements.

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 8.0.17.

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.

Step 3 - Complete the Object Security Template

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

To complete the Object Security template:

1. Launch the [Security Planning Template](#) and open the Object Security tab.
2. List all Costpoint Business Intelligence users by name.

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

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

Model or Row Level Security

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

Note: Model/Row Level Security only applies to the Models/Reports/Dashboards contained in the secure areas such as General Ledger, Planning, Projects and others.

There are different aspects of model security.

1. **Labor Suppression** - Restricts the ability to see labor rates and dollars at the employee level using the labor suppression flag settings in Costpoint. In Costpoint Business Intelligence, the rate/cost of employees are hidden in reports when Labor Suppression is in use. See Special Topic 1 for how to leverage this capability.
2. **Organizational Security** - Restricts data based on the user's organization rights established in Costpoint or Costpoint Planning. 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 Costpoint as source, Costpoint Organization Security is enforced. If you are not planning on using this type of security, no setup or changes are required. See Special Topic 1 for more information.

For data models that use Planning as source, Costpoint Business Intelligence uses information from the Planning setup. See Special Topic 2 for more information.

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

3. **Project Security** - Restricts project data.
4. **Parts Security** - Restricts part data in support of International Traffic in Arms Regulation (ITAR).
5. **Functional Role** - Restricts data based on user's functional role.

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

To restrict access to projects in the **Projects**, **General Ledger**, and the **Accounts Receivable** folders where the user is set up as Project Manager, you will simply need to assign them to the CER__PM_MGR. In order to offer some project security options in Costpoint Business Intelligence, the assigned project manager of the project is used to determine project rights.

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

Matrix for Secure Models

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

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

The rest of the models have object and capability security.

- Costpoint Enterprise Reporting
- Costpoint Enterprise Reporting for Budgeting and Planning
- Costpoint Enterprise Reporting for Fixed Assets
- Costpoint Enterprise Reporting for HR and Payroll

- ICS Core
- ICS-Presentation
- Costpoint Enterprise Reporting for Costpoint Project Manufacturing
- Costpoint Enterprise Reporting for Shop Floor Time
- Costpoint SOX
- TE SOX
- Contracts and Opportunities

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

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

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

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

Step 5 - Assign Users to Costpoint User Groups

After completing the plan and templates for the various security elements, you can start with the actual configuration 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 **Save & Continue**.
7. Repeat steps 2 to 6 until you have assigned all users to the CER User Groups.

Step 6 - Set Up Current Reporting Period

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

FILE LINE OPTIONS PROCESS HELP

★ Browse Applications > Reports & Analytics > Reporting Configuration > Configuration > Manage Current Reporting Period

Manage Current Reporting Period

Update Mode *	End Date *	Fiscal Year	Period	Subperiod *
MANUAL	01/31/2016	2016	1	4

To set up the Costpoint Business Intelligence current reporting period:

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

Field	Description
Update Mode	<p>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.</p> <div> <p>Note: It is recommended that you use the Manual setting since the administrator can then control when the reports and dashboards run when the current period is finished, which can vary period to period. This setting controls reports and dashboards that use the field Current Period or Year settings. This means you do not need to reset the field each month when you access the data.</p> <p>If you select Auto in the Update Mode field, the default values set on the Manage Current Reporting Period screen are based on the values of your accounting periods in Costpoint. The End Date is set to the closest end date to today's date. For example, if today's date is July 10, 2018, the end date will be July 31, 2018. This is because it is the closest end date and is greater than July 10, 2018.</p> <p>Note that the current period screen in Planning should also set to the same period. This screen is found at Planning » Administration » Administration Controls » Maintain Current Period. This setting controls the updating of the reporting tables and is separate from the Costpoint Business Intelligence Current Period.</p> </div>
End Date	Enter the end date for the current reporting period .
Fiscal Year	Enter the fiscal year for the current reporting period.

Field	Description
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.

Step 7 - 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, go to **Manage » Configuration » System » Advance Settings**

The screenshot shows the 'Advanced Settings' section of the Costpoint BI configuration interface. The 'Permissions filter' field is highlighted with a red box and contains the value 'read,write,execute,t'. Below it, there is a 'Custom settings' section with a table for 'Key' and 'Value'.

Key	Value

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.

Step 8 - 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, go to **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**, go to **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, go to **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
Under Cognos » Deltek » CER Accounting All Secure	CAP » Deltek Group » CER Accounting All Secure
Under Cognos » Deltek » CER Accounts Payable Secure	CAP » Deltek Group » CER Accounts Payable Secure
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

Cognos User Group	Costpoint Cognos User Group(CAP)
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 Administrator	CAP » Deltek Group » CER CP Administrator
Under Cognos » Deltek » CER Cloud Administrator	CAP » Deltek Group » CER Cloud Administrator <i>No need to map.</i>
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 Executive Secure	CAP » Deltek Group » CER Executive Secure
Under Cognos » Deltek » CER Expense Secure	CAP » Deltek Group » CER Expense Secure
Under Cognos » Deltek » CER General Ledger Secure	CAP » Deltek Group » CER General Ledger Secure
Under Cognos » Deltek » CER HR	CAP » Deltek Group » CER HR
Under Cognos » Deltek » CER Manufacturing Secure	CAP » Deltek Group » CER Manufacturing Secure
Under Cognos » Deltek » CER Materials	CAP » Deltek Group » CER Materials
Under Cognos » Deltek » CER Materials Manufacturing All Secure	CAP » Deltek Group » CER Materials Manufacturing All Secure
Under Cognos » Deltek » CER People	CAP » Deltek Group » CER People
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 Procure Secure	CAP » Deltek Group » CER Procure Secure
Under Cognos » Deltek » CER Project Manager Security	CAP » Deltek Group » CER Project Manager Security
Under Cognos » Deltek » CER Projects	CAP » Deltek Group » CER Projects
Under Cognos » Deltek » CER Projects Secure	CAP » Deltek Group » CER Projects Secure
Under Cognos » Deltek » CER Time & Expense	CAP » Deltek Group » CER Time & Expense

Cognos User Group	Costpoint Cognos User Group(CAP)
Under Cognos » Deltek » CER Time Secure	CAP » Deltek Group » CER Time Secure
Under Cognos » Deltek » CER User	CAP » Deltek Group » CER User

Step 9 - Customize Capability Permissions

Permissions for Cognos capabilities need to be manually added as some adjustments are needed to standard capabilities. Each of the Costpoint Business Intelligence user roles that were established for license types is mapped to a predefined role in Cognos in order to minimize the setup required here. The predefined role in Cognos is a close match to the capabilities we want for each Costpoint Business Intelligence role but there are some modifications required in order to be in compliance with Deltak licensing.

To add Permissions to Capabilities:

1. In Costpoint BI, click **Manage » Administration Console**.
2. On the **IBM Cognos Administration** screen, click the **Security** tab. Click **Capabilities**.
3. Look for the **Capability** for which you want to assign a **Permission**. For example, **Administration**.
4. Click the drop-down beside the **Capability** and then click **Set Properties**.
5. Click the **Permissions** tab.
6. Click **Add...** and select the role that you want to add to the **Capability**. For example, for the **Administration** capability, select the **CER Web Administrator** role which is found in **Cognos » Deltak » CER Web Administrator**.
7. Click the yellow arrow icon to transfer the role to the **Selected entries** group box on the right. Click **OK**.
8. On the **Permissions** tab, select the added role (for example, **CER Web Administrator**), and select the permissions check box under the **Grant** column.
In our example, **CER Web Administrator**, select **Execute** and **Traverse** under the **Grant** column.

Note: Make sure that the **Override the access permissions acquired from the parent entry** check box is selected.

9. Click **OK**.
10. Repeat steps 3 to 9 for the other capabilities in the following table.

Capability	Role
Administration	Add CER Web Administrator . Grant Execute and Traverse for both roles.
AI	Add CER User and CER Advanced Lite . Grant Execute and Traverse for both roles.
Analysis Studio	Add CER Advanced Lite and grant Execute and Traverse permissions.
Cognos Insight	Remove Everyone .
Cognos Viewer	Add CER Consumer and CER Advanced Lite . Grant Execute and Traverse permissions.

Capability	Role
Collaborate	Add CER Advanced Lite and grant Execute and Traverse permissions.
Dashboard	Add CER User and CER Advanced Lite . Grant Execute and Traverse permissions to both roles.
Data sets	Add CER Advanced User and CER Developer . Grant Execute and Traverse permissions to both roles.
Detailed Errors	Add CER User , CER Advanced Lite , CER Advanced User , and CER Developer . Grant Execute and Traverse permissions to all these roles.
Execute Indexed Search	Add CER Consumer and CER Advanced Lite . Grant Execute and Traverse permissions to these roles.
Executive Dashboard	Add CER Advanced Lite . Grant Execute and Traverse permissions to these roles.
Exploration <i>Only Explorers get this capability out of the box.</i>	Add CER Consumer and CER User and grant Traverse to both of these roles. Add CER Advanced Lite and CER Advanced User . Grant Execute and Traverse permissions to these roles.
External Repositories	Add CER Web Administrator and grant Execute and Traverse to these roles.
Import Relational Metadata	Add CER Web Administrator and grant Execute and Traverse .
Manage Content	Add CER Web Administrator . Grant Execute and Traverse permissions.
Manage Own Data Source Signons	Add CER Web Administrator and grant Execute and Traverse .
Query Studio	Add CER Advanced Lite and grant Execute and Traverse .
Report Studio	Add CER Consumer , CER User and grant Traverse to both these roles. Add CER Advanced Lite and grant Execute and Traverse to these roles.
Save to Cloud	Add CER Web Administrator . Grant Execute and Traverse .

Capability	Role
Scheduling (and Subscriptions)	Add CER Consumer , CER User , and CER Advanced Lite . Grant Execute and Traverse to all of these roles.
Upload Files	Add CER Advanced User , CER Developer , and CER Web Administrator . Grant Execute and Traverse to all of these roles. Remove Everyone .
Watch Rules	Add CER Advanced Lite and grant Execute and Traverse .
Web-based Modeling	Add CER Advanced User and CER Developer . Grant Execute and Traverse . Remove Everyone .

Step 10 - Customize Secured Feature Permissions

Capabilities that are underlined indicate that there are secured features within a capability that needs to be modified to be in compliance with Deltek licensing. For example, you need to modify **Administration**, to add user roles such as the **CER Web Administrator** and secure permissions for the **Administration Tasks** feature. Click on the underlined Capability to drill into its secured feature and customize the permissions. If you do not have the license for the indicated user role in this procedure, just skip and move on to the next user role that is available.

To customize permissions for a secured feature:

1. In Costpoint BI, click **Manage » Administration Console**.
2. On the **IBM Cognos Administration** screen, click the **Security** tab. Click **Capabilities**.
3. Look for the **Capability** for which you want to assign a **Permission** to its secured feature and click it. For example, **Administration**.
4. Click the drop-down beside the secured feature (for example, **Administration » Administration tasks**) and then click **Set Properties**.
5. Click the **Permissions** tab.
6. Click **Add...** and select the role that you want to add to the secured feature. For example, for **Administration » Administration tasks** secured feature, select the **CER Web Administrator** role which is found in **Cognos » Deltek » CER Web Administrator**.
7. Click the yellow arrow icon to transfer the role to the **Selected entries** group box on the right. Click **OK**.
8. On the **Permissions** tab, select the added role (for example, **CER Web Administrator**), and select the permissions check box under the **Grant** column.
In our example, **CER Web Administrator**, select **Execute** and **Traverse** under the **Grant** column.
9. Click **OK**.
10. Repeat steps 3 to 9 for the other capabilities in the following table.

Secured Feature	Role
Administration <ul style="list-style-type: none"> ■ Collaboration Administration ■ Configure and Manage the System ■ Data Source Connections ■ Distribution Lists and Contacts 	Add CER Web Administrator . Grant Execute and Traverse .

Secured Feature	Role
<ul style="list-style-type: none"> Manage Visualizations Mobile Administration Printers Query Service Administration Run Activities and Schedules Set capabilities and manage UI profiles Styles and portlets Users, Groups, and Roles 	
AI <ul style="list-style-type: none"> Use Assistant 	Add CER User and CER Advanced Lite . Grant Execute and Traverse to all these roles. Remove Everyone .
Analysis Studio	Add CER Advanced Lite , CER Advanced User , CER Developer . Grant Execute and Traverse to all these roles.
Cognos Insight	Remove Everyone .
Cognos Viewer <ul style="list-style-type: none"> Context Menu Run With Options Selection Toolbar 	Add CER Consumer and CER Advanced Lite . Grant Execute and Traverse to these roles.
Collaborate <ul style="list-style-type: none"> Allow collaboration features Launch collaboration tools 	Add CER Advanced Lite and grant Execute and Traverse .
Dashboard <ul style="list-style-type: none"> Create/Edit 	Add CER User , CER Advanced Lite , CER Advanced User , and CER Developer . Grant Execute and Traverse to these roles.
Executive Dashboard	Add CER Advanced Lite and grant Execute and Traverse .

Secured Feature	Role
<ul style="list-style-type: none"> Use Advanced Dashboard Features Use Interactive Dashboard Features 	
External Repositories <ul style="list-style-type: none"> Manage repository connections 	Add CER Web Administrator . Grant Execute and Traverse .
Query Studio <ul style="list-style-type: none"> Advanced Create 	Add CER Advanced Lite and grant Execute and Traverse .
Report Studio <ul style="list-style-type: none"> Allow External Data 	Add CER Consumer and CER User . Grant Traverse to both of these roles. Add CER Advanced Lite , CER Advanced , and CER Developer . Grant Execute and Traverse to these roles.
Report Studio <ul style="list-style-type: none"> Create/Delete 	Add CER Advanced Lite and grant Execute and Traverse to these roles.
Report Studio <ul style="list-style-type: none"> HTML Items in Report User Defined SQL 	Add CER Consumer , CER User , and CER Advanced Lite . Grant Execute to these roles. Add CER Advanced User and CER Developer . Grant Execute and Traverse to these roles.
Save to Cloud <ul style="list-style-type: none"> Manage Connections 	Add CER Web Administrator and grant Execute and Traverse .
Scheduling (and Subscriptions) <ul style="list-style-type: none"> Schedule by Day 	Add CER Consumer , CER User , CER Advanced Lite , CER Advanced User , and CER Developer . Grant Execute and Traverse to all of these roles.
Scheduling (and Subscriptions) <ul style="list-style-type: none"> Schedule by Hour Schedule by Minute Schedule by Month Schedule by Trigger 	Add CER Advanced Lite and grant Execute and Traverse .

Secured Feature	Role
<ul style="list-style-type: none"> ▪ Schedule by Week ▪ Schedule by Year 	

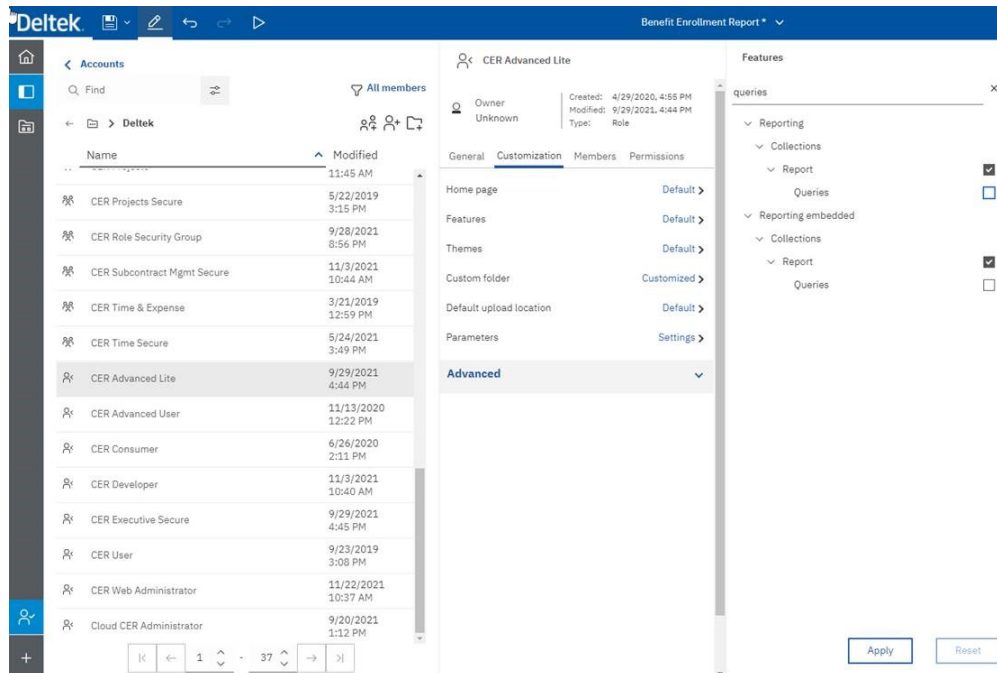
Step 11 - Customize CER__ADV_LITE User

Application of this procedure will prevent the CER__ADV_LITE user to edit MS SQL queries of existing reports.

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

To customize the CER__ADV_LITE user:

1. Login as System Administrator.
2. On the Costpoint BI Welcome screen, go to **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. Clear the **Queries** check box.
8. Click **Apply** to save changes.



Step 12 - Add Everyone and Assign Read Access to the Team Content Folder

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

To add Everyone and assign access to the Team Content folder:

1. In Cognos Analytics, click **Team Content** folder. Click the **Properties** icon beside it.



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

Step 13 - Validate User Groups

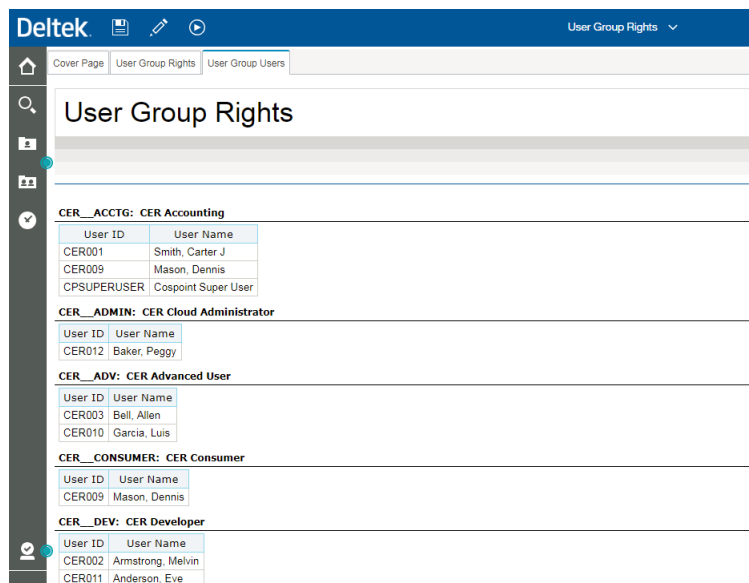
After you complete the steps in the post-installation phase, check the list of users per user group in Costpoint Business Intelligence against your accomplished Security Planning Template.

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

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

To validate the users in user groups:

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




User ID		User Name
CER__ACCTG: CER Accounting		
CER001	Smith, Carter J	
CER009	Mason, Dennis	
CPSUPERUSER	Costpoint Super User	
CER__ADMIN: CER Cloud Administrator		
CER012	Baker, Peggy	
CER__ADV: CER Advanced User		
CER003	Bell, Allen	
CER010	Garcia, Luis	
CER__CONSUMER: CER Consumer		
CER009	Mason, Dennis	
CER__DEV: CER Developer		
CER002	Armstrong, Melvin	
CER011	Anderson, Eve	

Step 14 - Add the Deltek Theme to Cognos Analytics

Deltek provides a theme as part of your Costpoint Business Intelligence installation.

To apply the Deltek theme to your Cognos Analytics portal:

1. On the pane on the left-hand side of the Welcome portal, click **Manage** and select **Customization**.
2. Click the **Upload theme**  icon and browse through the location of the **Deltek.zip** file. Click **Open**.

The default location of the **Deltek.zip** file is **C:\Program Files (x86)\Deltek\CostpointEnterpriseReporting (or CostpointBusinessIntelligence)\CER80x\Branding**.

3. When the **Deltek** theme is available on the Customization screen, select it 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.

Step 15 - Install ExtendTime.zip Extension

To avoid reaching the Costpoint timeout limit while working in Costpoint Business Intelligence, the **ExtendTime.zip** extension needs to be installed. This extension lets Costpoint recognize that you are actively working within Costpoint BI, thus, preventing the Costpoint timeout notification and potential loss of work.

You must have system administrator user permission rights to apply the **ExtendTime.zip** extension. You must also have access to the **Branding** folder of the latest Costpoint Business Intelligence installation. The said folder contains the extension file.

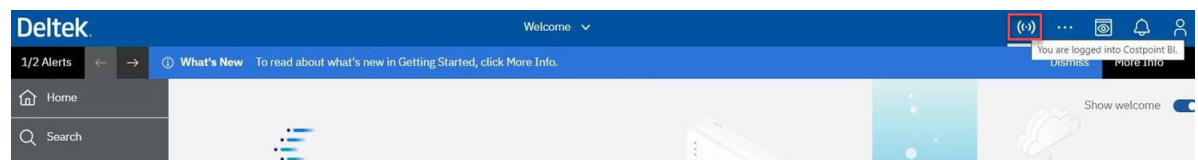
To install the ExtendTime.zip extension:

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

ExtendTime.zip file. Select the said file. Click **Open**.

The default location of the **ExtendTime.zip** file is **C:\Program Files (x86)\Delttek\CostpointEnterpriseReporting (or CostpointBusinessIntelligence)\CER80x\Branding**.

When the extension has been successfully installed, you and other users will see the icon on the upper right-hand side of the screen. A tooltip appears when you position the mouse pointer on the icon.



Optional Task

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

However, there is another task that you can do to improve the display in the MO Pick List report for Project Manufacturing users. You can install the bar code font used in the said report.

Configure the Barcode Font for MO Pick List Report

In order to display the barcodes on the MO Pick List report, 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\CER80x\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 C:\Windows\fonts folder.

Note: You also need to copy the barcode font to the C:\Windows\fonts folder for all the computers that you use for viewing the MO Pick List report. 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 MO Pick List 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.

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

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

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

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

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

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

Identification
User ID * X1101 User Name * Stephen Bridges

User Information
Employee ID 1101
Phone
Extension
Locale ID
Email stephenbridges@deltekdemo.com
Preferred Notification Mthd Default

Status
Deactivation Date
Date Password Changed 06/15/2016
Last Login Date 10/04/2018
☐ Force Password Change
☐ Notify When Batch Job Is Completed
☐ Allow User to Override Batch Job Priority
☐ Can Report Issues From Application Screen

Preferences User Can Change
☐ Password
☒ Phone and Extension
☐ Name
☒ Default Company
☐ Can Change Email Notification
Default Company * 1

Company Access

Company ID *	Default Taxable Entity ID	Org Security Group ID	Labor	SSN	Cost	Price	Company Name	Org Security Group Name	Taxable Entity Name
1	01	MANUFT	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Applied Technologies Inc	Manufacturing	Applied Technologies, Inc.
99	02		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Consolidation Company		Consolidation Taxable Entity
2	03		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	USA, Co.		USA, Co.
3	04		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Spanish, Co.		Spanish, Co.
5	05		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Nonprofit, Co.		Nonprofit Co.
6	06		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Manufacturing, Co.		Manufacturing, Co.

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

User Groups

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

User Groups > Assign Users to Group

User *	Name	Company *
--------	------	-----------

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

System Settings

Company Settings
☒ Apply Organization Security
☐ Allow HR Org Manager/Rep from Other Companies
Header Color -None-
Environment Name
☐ Display System in the Header

Email System
SMTP Server Name * SMTP.DELTEK.COM
SMTP Server User ID
E-mail Redirect
☐ Require SSL / TLS
SMTP Port Number * 25
Password

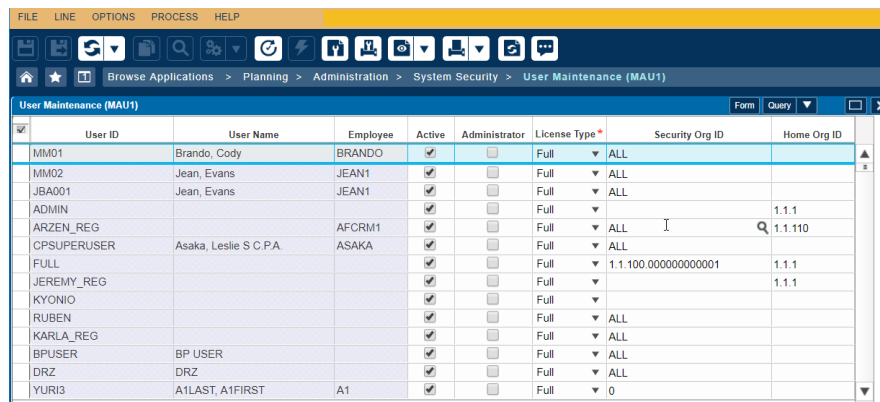
Company Defaults
☐ Print Cover Page
Report Table Purge (Days) * 7

Costpoint User Accounts
☐ Auto-create User Accounts
Authentication Method
Preferred Notification Method Email
☐ Allow Employee Override

Special Topic 2: Organization and Project Security in Costpoint Planning

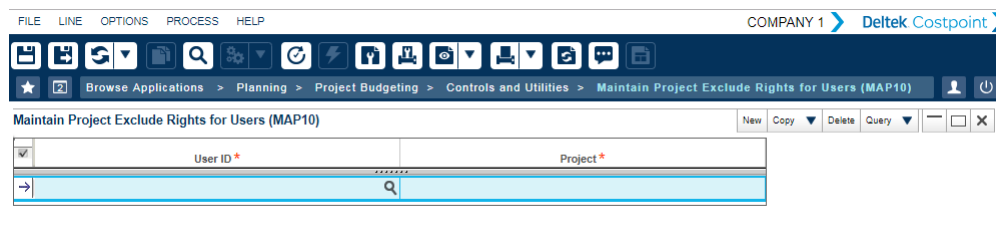
The Project Planning model in Costpoint Business Intelligence leverages the Organization/Project Security settings in the Costpoint Planning module. Costpoint Planning (formerly Budgeting and Planning) has distinct security settings related to the Planning content and does not use the Costpoint Organization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

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



User ID	User Name	Employee	Active	Administrator	License Type	Security Org ID	Home Org ID
MM01	Brando, Cody	BRANDO	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Full	ALL	
MM02	Jean, Evans	JEAN1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Full	ALL	
JBA001	Jean, Evans	JEAN1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Full	ALL	
ADMIN			<input checked="" type="checkbox"/>	<input type="checkbox"/>	Full	ALL	1.1.1
ARZEN_REG		AFCRM1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Full	ALL	1.1.110
CPSUPERUSER	Asaka, Leslie S C.P.A.	ASAKA	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Full	ALL	
FULL			<input checked="" type="checkbox"/>	<input type="checkbox"/>	Full	1.1.100.0000000000001	1.1.1
JEREMY_REG			<input checked="" type="checkbox"/>	<input type="checkbox"/>	Full		1.1.1
KYONIO			<input checked="" type="checkbox"/>	<input type="checkbox"/>	Full		
RUBEN			<input checked="" type="checkbox"/>	<input type="checkbox"/>	Full	ALL	
KARLA_REG			<input checked="" type="checkbox"/>	<input type="checkbox"/>	Full	ALL	
BPUSER	BP USER		<input checked="" type="checkbox"/>	<input type="checkbox"/>	Full	ALL	
DRZ	DRZ		<input checked="" type="checkbox"/>	<input type="checkbox"/>	Full	ALL	
YURI3	A1LAST, A1FIRST	A1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Full	0	

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



User ID *	Project *

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

Special Topic 2: Organization and Project Security in Costpoint Planning

Manage Users New Copy Delete Form Query X

ID *	Name *	Allow Saving of Personal Screen Configurations	Allow Screen Configuration Changes for UI Profiles	Employee ID	Phone	Extension	Default Locale	Locale Name	Email
AP	Armstrong, Melvin	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1008					melvinarmstrong@deltekdemo.com
BILLER	Mary Thornburn	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1113					
BUYER	Mark Davidson	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1108					
CC	CC	<input checked="" type="checkbox"/>	<input type="checkbox"/>						
CONT_ADM	Francis Zone	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1096					fzone@ati.com
CONT_MGR	Roberta Jarvis	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1134					
CPNOW1	Ken Austin	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1220					kausting@ati.com
CPNOW2	Colin Garrett	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1225					cgarrett@ati.com
CPNOW3	Derrick Harrison	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1227					dhammson@ati.com
CPSUPERUSEREXT	Administrator, Extensibili	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9999					

Identification > Company Access New Copy Delete Form Query X

Company ID *	Default Taxable Entity ID	Org Security Group ID	Labor	SSN	Cost	Price	Company Name	Org Security Group Name	Taxable Entity Name
1	ALL		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Applied Technologies Inc.	All Access	Applied Technologies, Inc.

Close

Special Topic 3: 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.

Capabilities	CER_CONSUMER	CER_USER (IBM Consumer)	CER_ADV_LITE	CER_ADV (IBM Analytics User/ IBM Authors/ IBM Consumers)	CER_DEV (IBM Analytics Explorer/ IBM Authors/IBM Consumers)	CER Web Administrator	System Administrator
Administration						ACCESS	ACCESS
Administration Tasks						ACCESS	ACCESS
Collaboration Administration						ACCESS	ACCESS
Configure and Manage the System						ACCESS	ACCESS
Data Source Connections						ACCESS	ACCESS
Distribution Lists and Contacts						ACCESS	ACCESS
Manage Visualizations						ACCESS	ACCESS
Mobile Administration						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
Use Assistant		ACCESS	ACCESS	ACCESS	ACCESS		ACCESS
Analysis Studio			ACCESS	ACCESS	ACCESS		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
Dashboard		ACCESS	ACCESS	ACCESS	ACCESS		ACCESS
Create/Edit		ACCESS	ACCESS	ACCESS	ACCESS		ACCESS
Data Manager							ACCESS
Data sets				ACCESS	ACCESS		ACCESS
Desktop Tools					ACCESS		ACCESS
Detailed Errors		ACCESS	ACCESS	ACCESS	ACCESS		ACCESS
Develop Visualizations				ACCESS	ACCESS		ACCESS
Drill Through Assistant							ACCESS
Event Studio				ACCESS	ACCESS		ACCESS
Execute Indexed Search	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
Exploration	Custom (Traverse)	Custom	ACCESS	ACCESS	ACCESS		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 Output	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
Job				ACCESS	ACCESS	ACCESS	ACCESS
Lineage	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS
Manage Content						ACCESS	ACCESS
Manage Own Data Source Signons						ACCESS	ACCESS
Mobile							ACCESS
Notebook							ACCESS
Query Studio			ACCESS	ACCESS	ACCESS		ACCESS
Advanced			ACCESS	ACCESS	ACCESS		ACCESS
Create			ACCESS	ACCESS	ACCESS		ACCESS
Report Studio	Custom (Traverse)	Custom	ACCESS	ACCESS	ACCESS		ACCESS
Allow External Data	Custom (Traverse)	Custom	ACCESS	ACCESS	ACCESS		ACCESS
Bursting				ACCESS	ACCESS		ACCESS
Create/ Delete			ACCESS	ACCESS	ACCESS		ACCESS
HTML Items in Report	Custom (Traverse)	Custom (Traverse)	Custom (Traverse)	ACCESS	ACCESS		ACCESS
User Defined SQL**	Custom (Traverse)	Custom (Traverse)	Custom (Traverse)	ACCESS	ACCESS		ACCESS
Save to Cloud				ACCESS	ACCESS	ACCESS	ACCESS
Manage Connections						ACCESS	ACCESS
Scheduling (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	ACCESS	ACCESS		ACCESS
Schedule by Month			ACCESS	ACCESS	ACCESS		ACCESS
Schedule by Trigger			ACCESS	ACCESS	ACCESS		ACCESS
Schedule by Week			ACCESS	ACCESS	ACCESS		ACCESS
Schedule by Year			ACCESS	ACCESS	ACCESS		ACCESS
Scheduling Priority							ACCESS
Self Service Package Wizard							ACCESS
Set Entry- Specific Capabilities							ACCESS
Snapshots	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*	ACCESS*
Specification Execution							ACCESS
Upload Files				ACCESS	ACCESS	ACCESS	ACCESS
Watch Rules		ACCESS	ACCESS	ACCESS	ACCESS		ACCESS
Web-based Modeling				ACCESS	ACCESS		ACCESS

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

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

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

About Deltek

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

www.deltek.com