Deltek

Deltek Costpoint Cloud

Configuring Microsoft Azure with SAML

October 30, 2018

This edition published October 2018.

Contents

Overview 1
Step One: Submit the CAP Cutover Service Request 2
Populate the Costpoint User Groups 2
Move My Folder content to shared location 3
Submit the CAP Cutover Service Request 3
Step Two: Submit the SSO Setup Service Request 4
Step Three: Add and Configure Costpoint into your MS Azure Admin Portal 5
Step Four: Submit your MS Azure SAML Certificate to Deltek 7
Step Five: Set Up Your Costpoint User Accounts for MS Azure or Azure/SAML 8

Overview

There are five steps to setting up Microsoft Azure for Deltek Costpoint Cloud:

- Step One: Submit the CAP Cutover Service Request
- Step Two: Submit the SSO Setup Service Request
- Step Three: Add and Configure Costpoint into your MS Azure Admin Portal
- Step Four: Submit your MS Azure SAML Certificate to Deltek
- Step Five: Set up your Costpoint User Accounts for MS Azure or Azure/SAML

Step One: Submit the CAP Cutover Service Request

Populate the Costpoint User Groups

Note: Cloud customers who are deployed on CER v7.2.1 in the cloud can skip Step One and start with Step Two.

Implementing MS Azure requires that you change the way your users are authenticated and authorized to use Costpoint Enterprise Reporting (CER). Currently CER users are assigned to security groups within User Manager which identifies their role and Costpoint Systems they have access to when using CER. When implementing MS Azure you must switch to the new Cognos Authentication Provider (CAP) model. CAP uses Costpoint User Groups for authentication and authorization in CER. CAP supports users regardless of how they are authenticating into Costpoint. CAP will support users who are authenticating using Okta as well as support users authenticating using the Cloud Active Directory.

Deltek has added the following Costpoint User Groups to your Costpoint system. Populate your users into the appropriate groups to identify the user CER functional role and CER database access

If you are operating in the Production Environment you must populate these groups in your PROD system. If you are operating in the Implementation Environment you must choose either your CONFIG or TEST system to populate the groups. You only need to populate the Costpoint User Groups in one of your Costpoint systems.

Costpoint User Group Name	CER Functional Role
CER__ADMIN	CER Cloud Administrator
CER__DEV	CER Developer
CER__ADV	CER Advanced User
CER__USER	CER User

Note: These groups must also be granted access to the ERCOGNOS module in Costpoint.

Populate your users into the appropriate groups to identify which Costpoint systems the users will have access to. Populate the Costpoint Groups in the same Costpoint system (either PROD, CONFIG, or TEST) you selected for the above groups.

Costpoint User Group Name	CER Database Access
CER__DB_SBOX	Sandbox
CER__DB_TEST	Test
CER__DB_CONFIG	Config
CER__DB_DEV	Development
CER__DB_PREV	Preview

Note: All CER Functional Role Groups are granted access to Production database.

Move My Folder Content to Shared Location

All users who have content (that is, custom reports) in their My Folder area must move this content to a shared location. Content in the My Folder location will not be accessible once the CAP Cutover Service Request is completed.

Users can move their content to a shared location by creating a folder in the Public folder area. This new folder can be named whatever the user wants. The user should copy their content from their My Folder to their newly created folder in the Public Folder area. Once you have switched over to CAP you can move your content from the Public Folder area to a different folder.

Submit the CAP Cutover Service Request

Once you have populated your users into the appropriate Costpoint User Groups and you have moved your My Folder content to a shared location you are ready to submit the CAP Cutover Service Request. The CAP Cutover Service Request will require you to identify which Costpoint system CER should reference to find the populated Costpoint User Groups. If you are operating in the Production Environment you should choose PROD. If you are operating in the Implementation Environment you should choose CONFIG or TEST. You only need to populate the Costpoint User Groups in one of these systems.

Step Two: Submit the SSO Setup Service Request

Provide the following information in the Service Request:

- **Fully Qualified Domain:** This is the domain that your users authenticate against (for example, **ACME.Local**).
- **MS Azure Host Name**: This is the Entity ID (for example, **login.microsoftonline.com**).
- **MS Azure Tenant ID**: For example, **ab5c173d-bcdd-4e56-97a8-79f9u715e806**
- **SAML Certificate**: You can add this to the SSO Setup Service Request ticket after you complete Step Three.

Deltek will provide you with the Enterprise Application URL needed to configure MS Azure in Step Three.

- If you are a Costpoint Foundations or Essentials customer Deltek will provide you with one XML file.
- If you are a Costpoint Enterprise customer Deltek will provide you with three XML files.

The files will be attached to your SSO Setup Service Request ticket.

Step Three: Add and Configure Costpoint into Your MS Azure Admin Portal

Important: Costpoint Enterprise customers should repeat this step for each Cloud Environment (Production, Implementation/Test/Preview, Dev) for which you want to set up MS Azure.

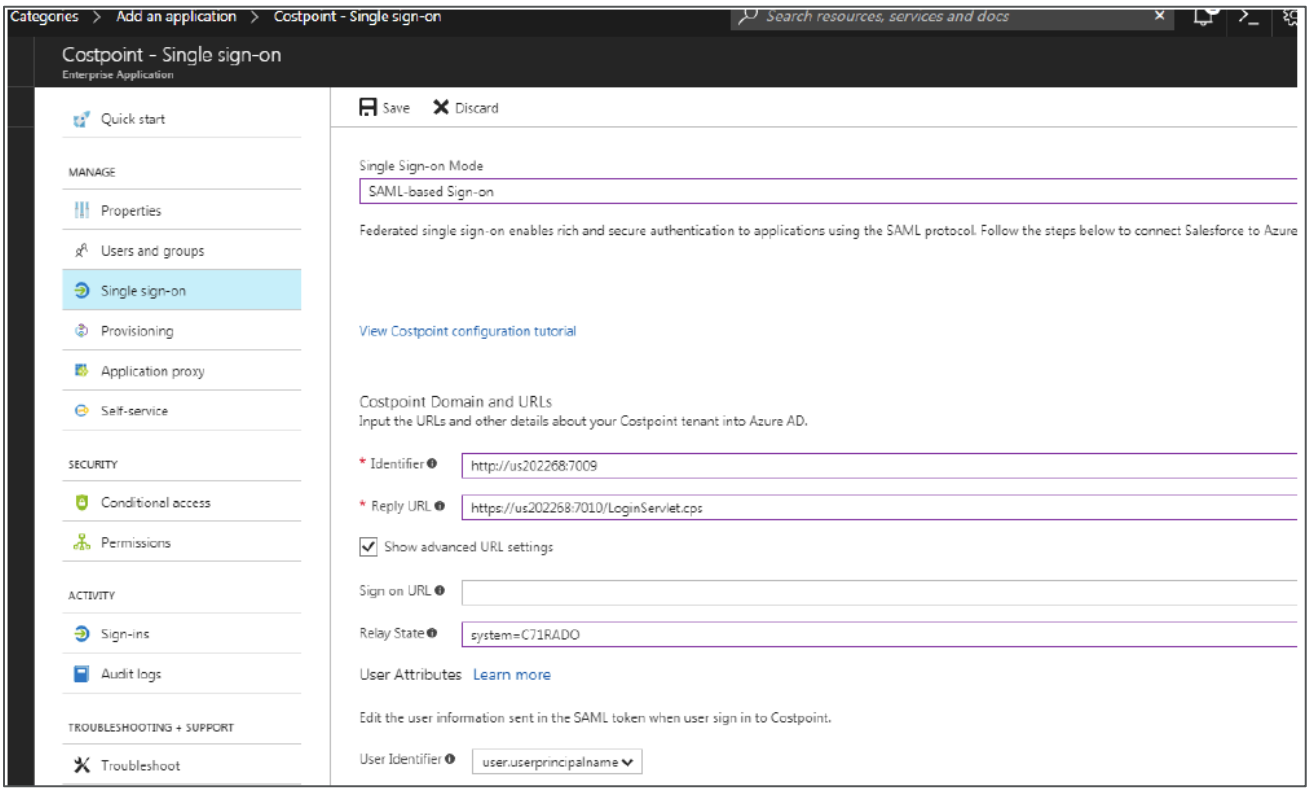
To add and configure Costpoint into the MSAzure Admin portal:

1. Log into the MS Azure Admin Portal.
2. Navigate to **Azure Active Directory » Enterprise Applications » All Applications**.
3. Click **+ New Application**, and select the **Non-gallery Application** option.
4. In the **Name** field, enter **Costpoint**, and click **Add**.
5. Click **Assign a user for testing**, or go to **Costpoint » Users and groups** on the left pane and click **Select** and **Assign** to select and assign users and/or user groups to have access to Costpoint.
6. Click **Configure single sign-on** or go to **Costpoint » Single sign-on** on the left pane.
7. For **Single Sign-on Mode**, select **SAML-based Sign-on**.
8. On the **SAML-based Sign-on** page, perform the following actions:
   - For **Identifier**, enter the Costpoint application URL.

     The value must be the same URL from **Costpoint Configuration Utility » Product » Enterprise App External URL or enterprise.properties » enterpriseAppUrl** property.
   - For **Reply URL**, enter the HTTPS/SSL Costpoint host/address URL ending with /LoginServlet.cps. This URL will be used by Azure to send the SAML token back to Costpoint.

     For example, **https://<client>-cpd.deltekenterprise.com/cpweb/LoginServlet.cps**
   - Click **Show Advanced URL settings**, and for **Relay State**, enter the **Costpoint System Name**, in ALL CAPS, as **system=<YOUR SYSTEM NAME>**.

     For example, **system=<CLIENTNAME>CONFIG**



9. Click **Save** to save the **Single sign-on** configuration.
10. Click **Configure Costpoint** and download the SAML XML Metadata file.

    Use this file as the **Azure Metadata File** to send to Deltek in Step Four.

Step Four: Submit your MS Azure SAML Certificate to Deltek

Please attach the following information to the SSO Setup Service Request ticket that was created in Step Two.

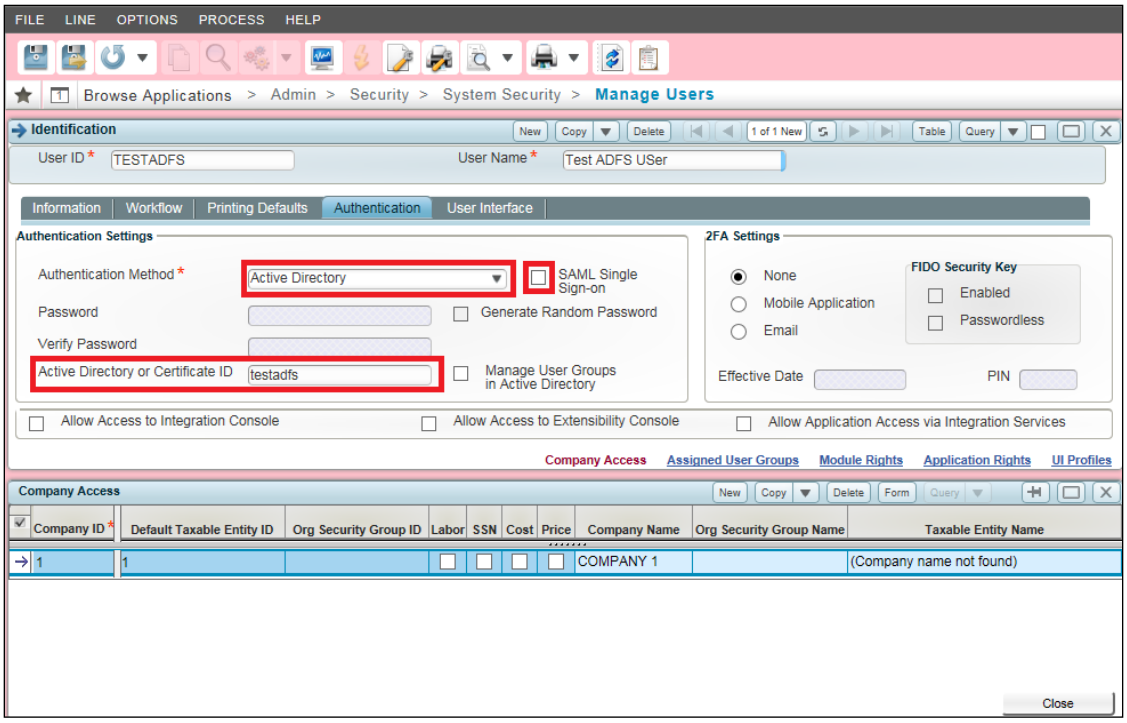
- SAML Certificate: Exported as metadata XML

Step Five: Set Up Your Costpoint User Accounts for MS Azure or Azure/SAML

In order to log into Costpoint with your MS Azure credentials, you must first modify the authentication properties of your Costpoint user account.

To modify the authentication properties:

1. Login into your Costpoint systems using a Cloud Active Directory (User Manager) account that has access to the Manage Users application within Costpoint.
2. Navigate to **Admin > Security > System Security > Manage Users**.
3. Pull up the account that you'd like to modify, and click the Authentication tab.



4. For **Authentication Method**, select **Active Directory** from the drop-down list.
5. In the **Active Directory or Certificate ID** field, enter your user's Active Directory user name in your domain.

   This can be just the username or the username in UPN format (for example, **user@mydomain.local**).
6. If the user will be using SAML, select the **SAML Single Sign-on** check box.
7. Save the record.
8. Repeat steps 3 thru 7 for each user in each Costpoint system for whom you want to use ADFS authentication.

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