Deltek

Deltek Costpoint Cloud

Configuring Microsoft® Azure (Entra ID)

February 12, 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 May 2020.

Contents

Microsoft Azure Active Directory Gallery

You can access Deltek Costpoint via a SAML-based Single Sign On with your Azure Active Directory account. Setting up the SSO with Microsoft Azure AD is a simple, three-step process.

Step	Procedure
1	Submit the SSO Setup Service Request
2	Add and Configure Costpoint into your MS Azure Admin Portal
3	Set up your Costpoint User Accounts for MS Azure

Note: If you are already set up for SAML SSO authentication in Costpoint Cloud, you will need to set up a second configuration for the Costpoint Mobile T&E in the Cloud. Follow the instructions in this guide to set up your configuration. See the *Deltek Costpoint Mobile Time and Expense in the Cloud Administrator Guide* for more information on Costpoint Mobile T&E in the Cloud.

Submit the SSO Setup Service Request

To submit the SSO setup service request:

1. Provide the following information in the Service Request:
   - Fully Qualified Domain that your users authenticate against (for example, ACME.Local).
   - Indicate which systems you want SAML enabled on.
2. Deltek will provide you with one XML file per Costpoint system on your account.

   The files will be attached to your SSO Setup Service Request ticket. You will need these files to complete the remaining steps.

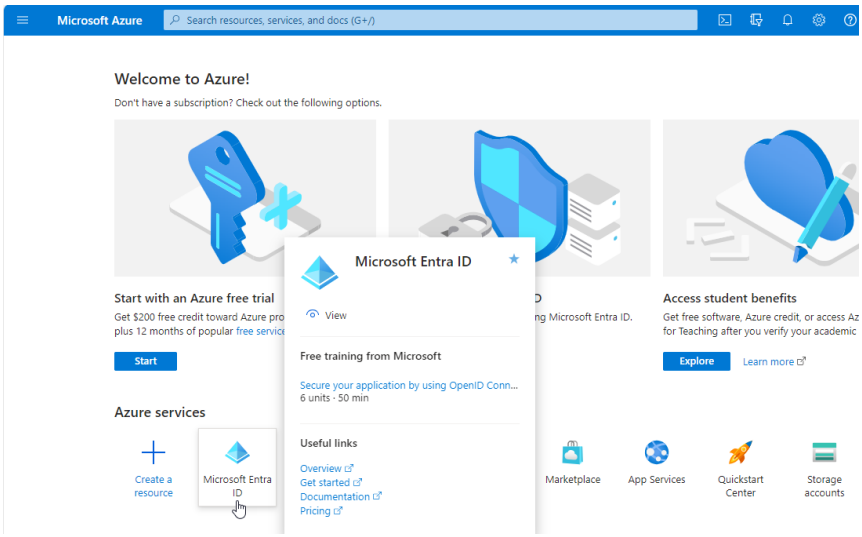
   Note: If you are a Costpoint Mobile T&E customer, Deltek will provide you with two sets of URLs (one for Costpoint and one for Costpoint Mobile T&E).

Add and Configure Costpoint into Your Azure Admin Portal

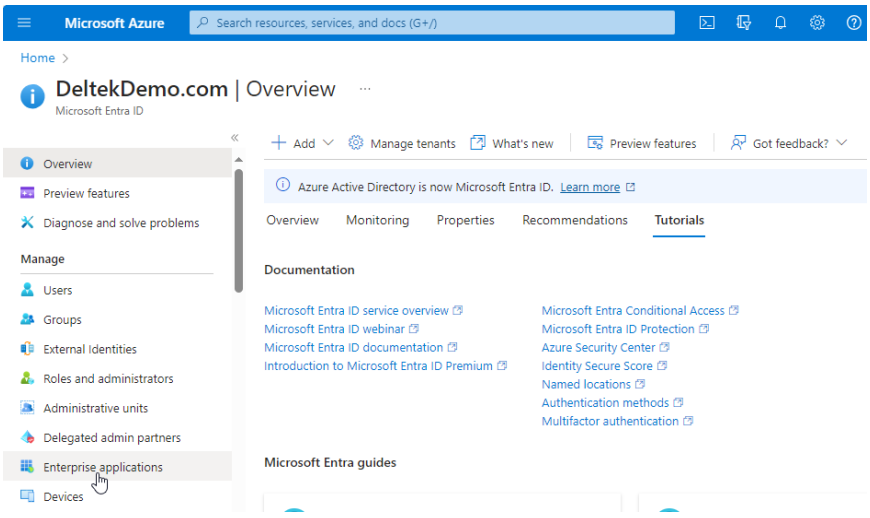
Use the information provided in the SSO Setup Service Request to perform the initial configuration of MS Azure.

To add and configure Costpoint into your MS Azure Admin portal:

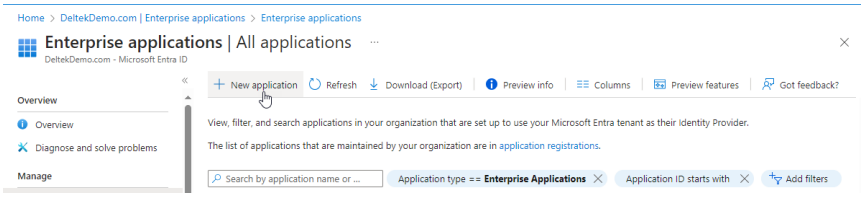
1. Log into the MS Azure Admin Portal using the admin account with your company and select Microsoft Entra ID.



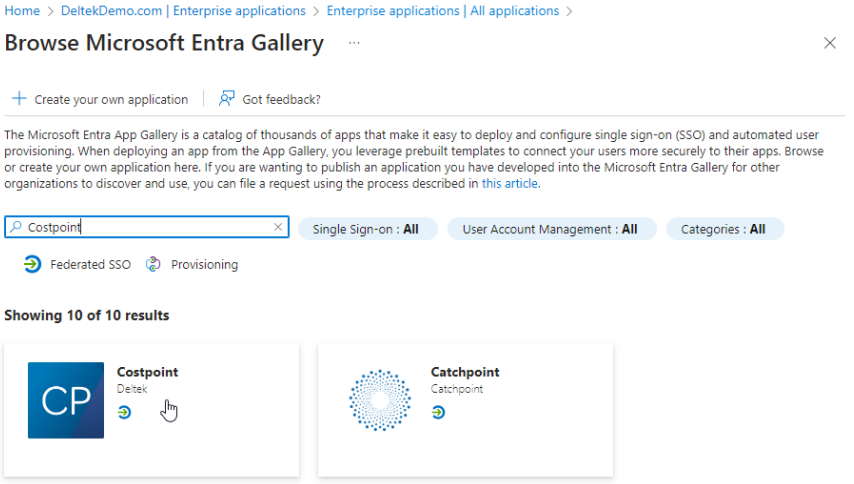
2. Click **Enterprise Applications**.



3. To add new application, click **New application**.



4. In the **Browse Microsoft Entra Gallery** section, enter **Costpoint** in the search box.



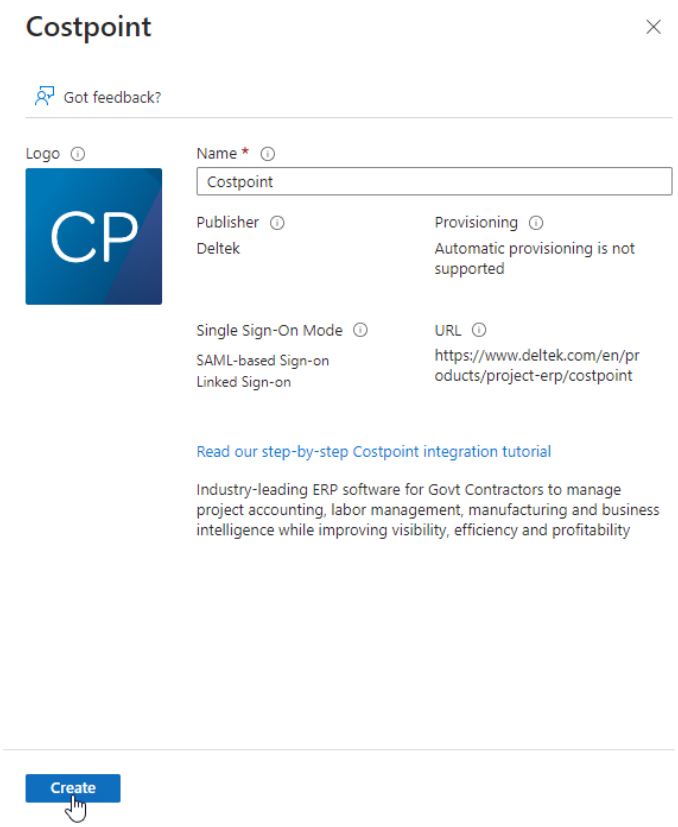
5. Perform the following:

   a. Select **Costpoint** from results panel.

   b. Give it a name related to the system you are connecting to that makes sense to you and/or your users.

   c. Click **Create**.

   Wait a few seconds while the application is added to your tenant.

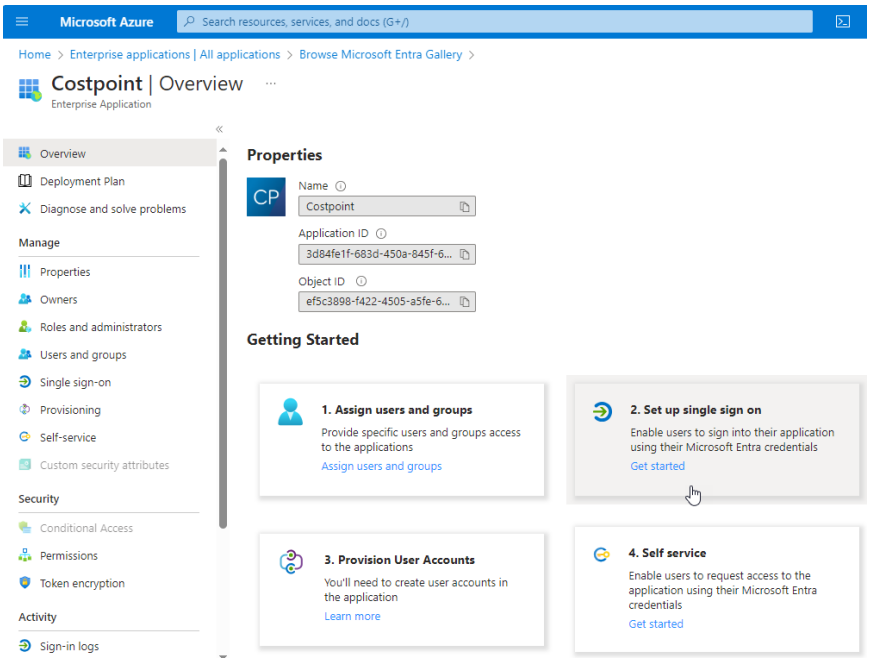


The above example uses **Costpoint Prod** for the application name. You may want to name additional instances **Costpoint Sandbox**, **Costpoint**, **Test**, or use your Costpoint system name where you log in. Anything that will clearly identify the system you are logging into for your users will work. Since the application definition will include that system in the configuration, you will not have the opportunity to specify into which Costpoint system you are logging. When you access the application icon from the portal, you will be logged into that Costpoint system directly.

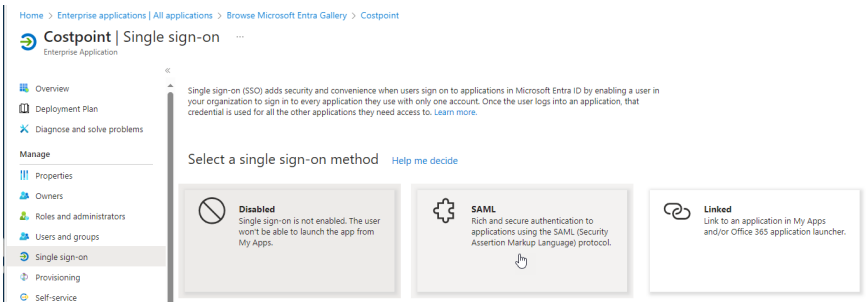
> **Note:** For Costpoint Mobile T&E users, you must perform this step for each Costpoint Mobile T&E environment that you would like to set up Azure for.

> **Note:** If you already have one Azure setup for Costpoint and you would like to add another one for Costpoint Mobile T&E, you must use a different entity ID for Costpoint Mobile T&E.

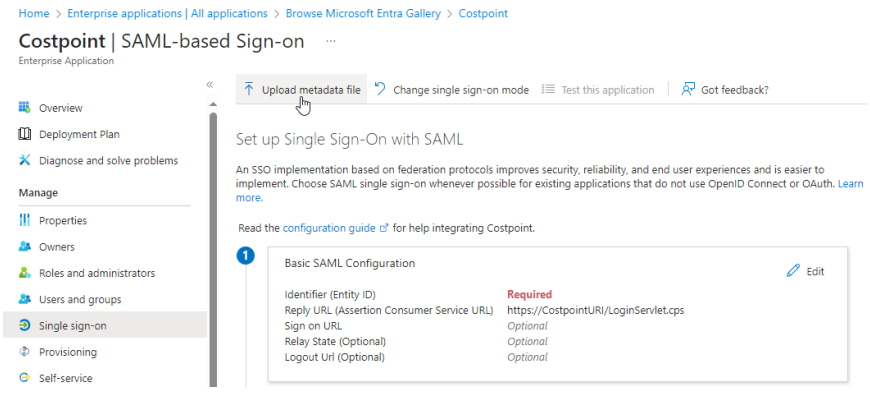
6. Once added, select **Configure single sign-on**.



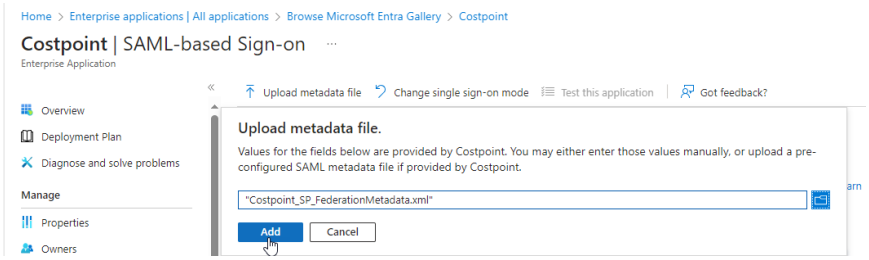
7. Select **SAML**.



8. Click **Upload metadata file**.



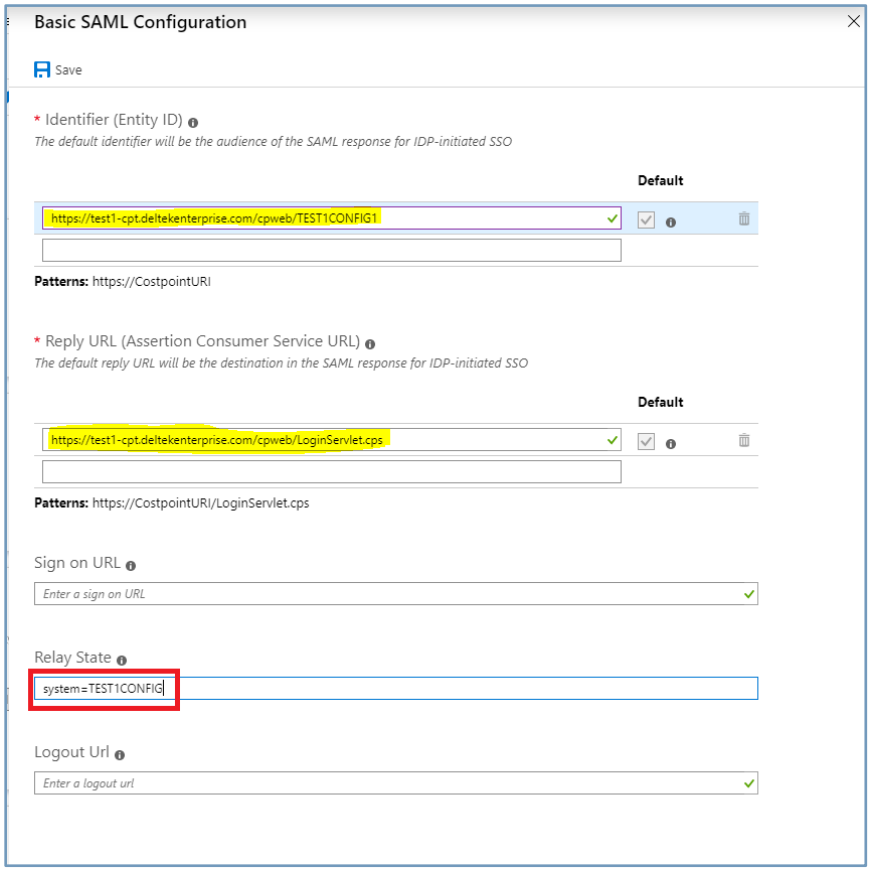
9. Browse to where you downloaded the *.xml files provided to you in the service request case, select the XML file for that specific Costpoint system, and click **Add**.



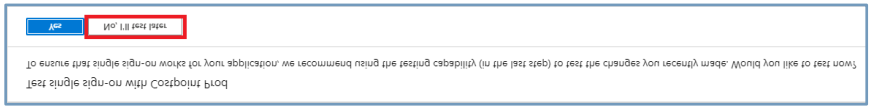
10. On the Basic SAML configuration screen, the **Identifier** and **Reply URL** fields are automatically populated. Do not edit these values.
11. In the **Relay State** field, enter **system=<*COSTPOINT SYSTEM NAME*>** and save the record.

    This is the Costpoint system name you are logging into (for example, **TEST1CONFIG**).

> **Warning:** These values are case-sensitive. The word **system** MUST be in lowercase, and the Costpoint system name should be in upper case.



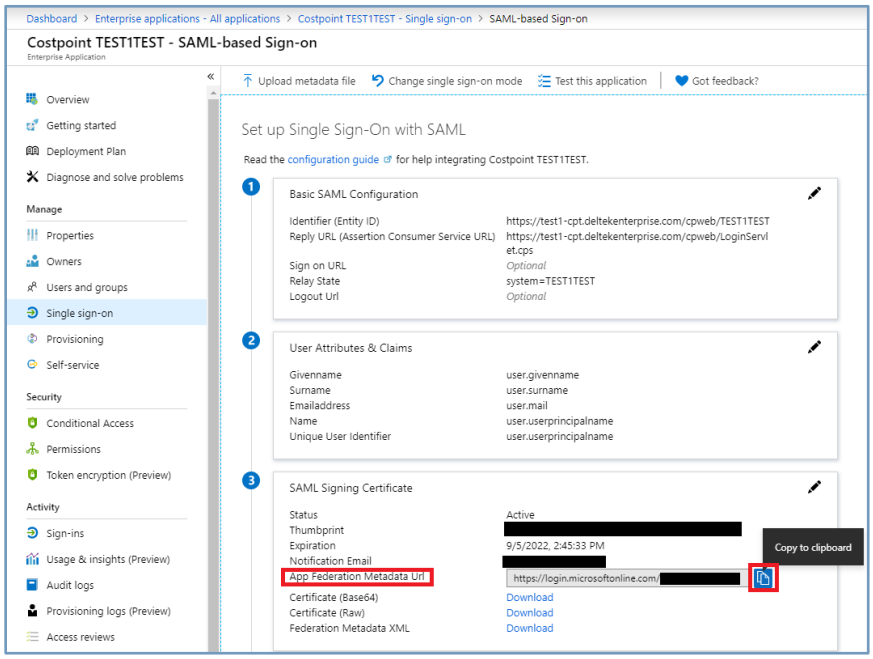
12. When prompted to test, click **No, I'll test later** since you have additional steps to complete before it will work.



13. For each application you set up, you need to capture the **App Federation Metadata Url** and send that with the corresponding Costpoint system name.

    Deltek needs this information to complete your Azure SSO setup. Add this information to your Service Request ticket as shown in the following example. The x's will be replaced with your specific identifiers. Repeat for each system you are configuring:

    `TEST1CONFIG  https://login.microsoftonline.com/xxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx/federationmetadata/2007-06/federationmetadata.xml?appid=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxx`



14. After receiving this information, Deltek will complete the Costpoint backend configuration and send you a confirmation that it has been completed.

15. Continue with the next step to set up your users.

Attach Your Azure/Entra ID XML Certificate to Your SSO Setup Service Request Ticket

Attach the Entra ID XML certificate you created in Step 3 (Configure Entra ID) to the SSO Setup Service Request ticket you created in Step 2 (Submit the SSO Setup Service Request).

You also need to let the cloud team if your SAML ID Attribute is an email account or a unique identifier like an employee number. Your users will all need to use the same type of attribute.

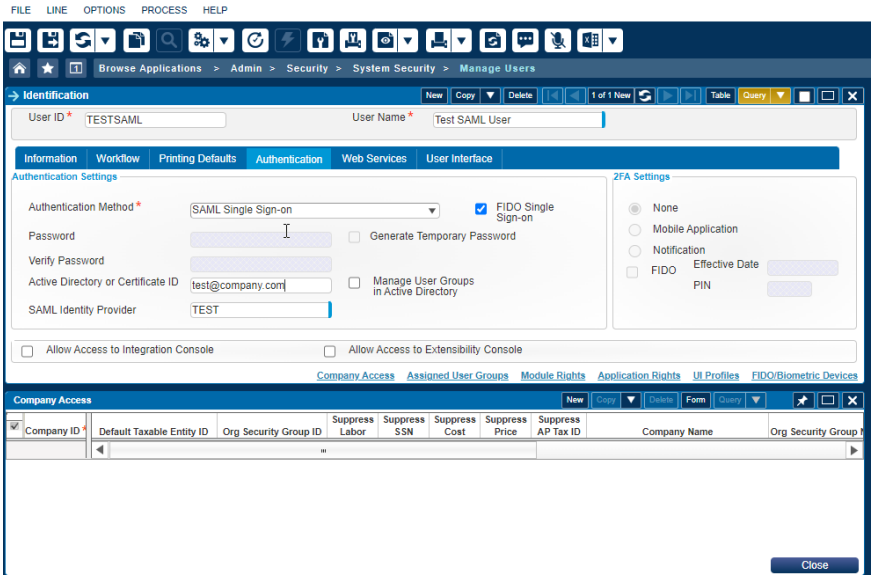
Set Up Costpoint User Accounts for Azure Authentication

To enable logging into Costpoint with your Azure credentials, you must first modify the authentication properties of your Costpoint user account.

To set up your Costpoint user accounts:

1. Primary SaaS Admin will need to login and adjust the authentication properties of your users.
    a. **GCCM Customers:** Log into your Costpoint systems using the Primary SaaS Admins SAML Attribute (i.e., the email address(upn) or a unique identifier).
        i. When logging into Costpoint, use the SAML Attribute as the Costpoint Username.
        ii. Developers will need 2 Costpoint accounts in the DEV system, their end user account for testing that uses SAML and a second account that uses Active Directory as the authentication method. The attribute will be clientid.developerfirstname.developerlast name, for example 50053.Mickey.Mouse. You can find more information on setting up the Cloud Active Directory for your developers here.
    b. **GCC Customers:** Log 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** and locate the account to modify.
3. Click the Authentication tab.
4. Perform the following:
    - In **Authentication Method**, select **Active Directory**.
    - In the **Active Directory or Certificate ID** field, enter the user's Active Directory username in your domain.

      This can be the username or the username in UPN format (for example, user@mydomain.local).
    - If the user will be using SAML, select the **SAML Single Signon** check box.



5. Save the record.
6. Repeat steps 3 through 5 for each user in each Costpoint system with whom you would like to use MS Azure authentication.

> **Note:** Repeat steps 3 through 7 for each user in the Costpoint Mobile T&E system who want to use the Azure authentication.

7. After your Costpoint accounts are set up, go back to Azure Administration and grant permissions to use the application you provisioned earlier, if you have not done so already.

Logging into the Costpoint User Interface Environments

Here are examples of the client URLs - the ABC needs to be replaced by your client System Name.

1. Development Environment

This environment is used to build your extensions or web services as needed.
URL for front end access https://cp-ABC01-dev.npr.mydeltekgcc.com/cpweb
System Names: ABCDEV

2. Non-Production Environment

This environment is used to test your data as it goes into the cloud and for future use to test new functionality or features of future Costpoint releases.
URL for front end access https://cp-ABC-tst.npr.mydeltekgcc.com/cpweb
System Names: ABCTEST, ABCCONFIG, ABCSBOX

3. Production Environment

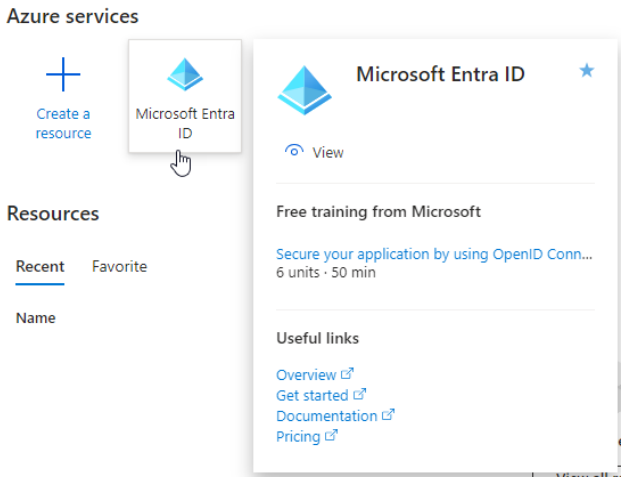
This environment is used to test your data as it goes into the cloud and for future use to test new functionality or features of future Costpoint releases.
URL for front end access https://cp-ABC.prd.mydeltekgcc.com/cpweb
System Names: ABCPROD

Configure Costpoint GCCM Developer Accounts for Citrix Access with Azure SSO

To enable logging into Costpoint with your Azure credentials to Citrix, you will need to configure the Citrix application within your Azure solution.

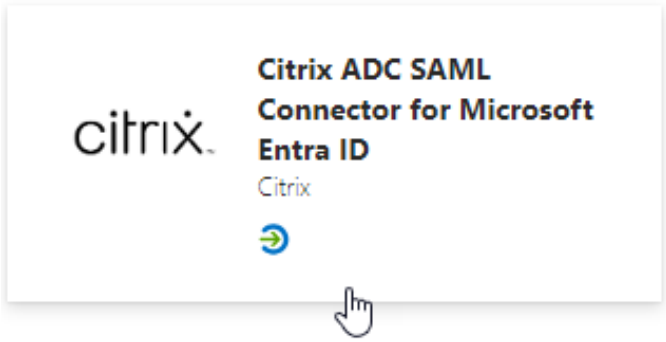
NOTE: You will need to submit the Service Request for Citrix Access to establish the SAML SSO connectivity with our Citrix, in addition to creating the Citrix Access within Entra ID.

1. Azure already has created the Citrix ADC SAML Connector application and is currently available in the Azure portal to configure and assign to users.
2. Customer must have an Azure Admin login to the portal and select Microsoft Entra ID.

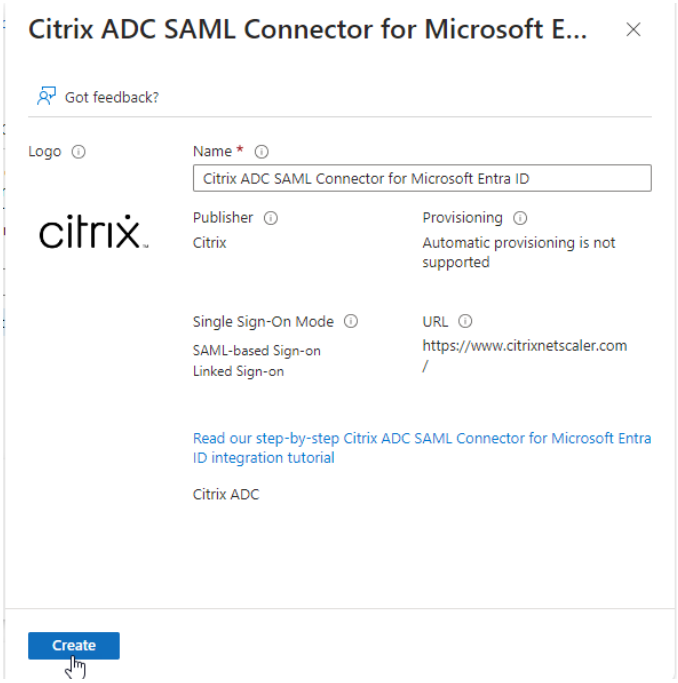


3. Search Citrix

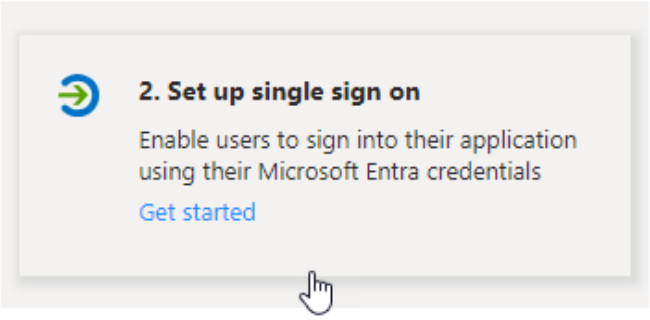
4. Select Citrix ADC SAML Connector for Microsof Entra ID



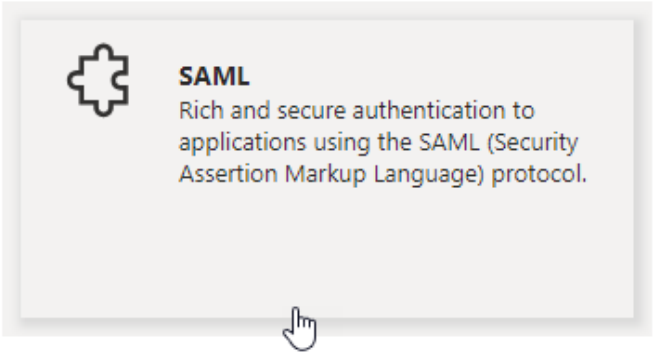
5. Select Create to create the Application



6. Select Set up single sign on



7. Select SAML



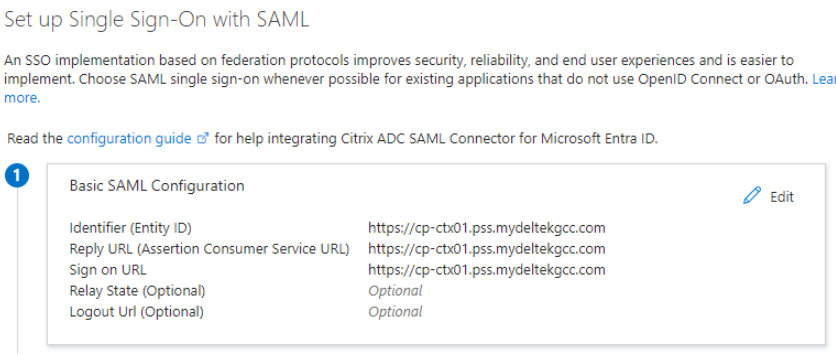
8. This will open a new page to Set up Single Sign-on with SAML.

   Enter the following values in the Basic SAML Configuration

   Identifier (Entity ID): https://cp-ctx01.pss.mydeltekgcc.com

   Reply URL (Assertion Consumer Service URL): https://cp-ctx01.pss.mydeltekgcc.com

   Sign on URL: https://cp-ctx01.pss.mydeltekgcc.com



9. You will need to add the developers into this new application to enable their ability to log into Citrix.
10. The SaaS Admin will need to login to Cloud AD Manager and create an AD account and grant access to DEV Groups.

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