Deltek

Deltek Costpoint Cloud

Configuring Active Directory Federation Services (ADFS)

October 30, 2018

This edition published October 2018.

Contents

Overview

There are four steps to setting up Active Directory Federation Services (ADFS) for Deltek Costpoint Cloud:

- Step One: Submit the CAP Cutover Service Request
- Step Two: Submit the SSO Setup Service Request
- Step Three: Use the XML files provided in the SSO Setup Service Request to configure ADFS
- Step Four: Set up your Costpoint User Accounts for ADFS

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 ADFS 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 ADFS 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

You need the following information to complete the SSO Setup Service Request:

- **Fully Qualified Domain Name**: This is the full name of the domain in which users will authenticate against (for example: **FARM.LOCAL**).
- **Fully Qualified Domain Name Active Directory Federation Services Host Name**: This is the fully qualified name of the server that is hosting Active Directory Federation Services (for example: **AD.FARM.LOCAL**).
- **XML file(s) provided by Deltek**:
  - 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.

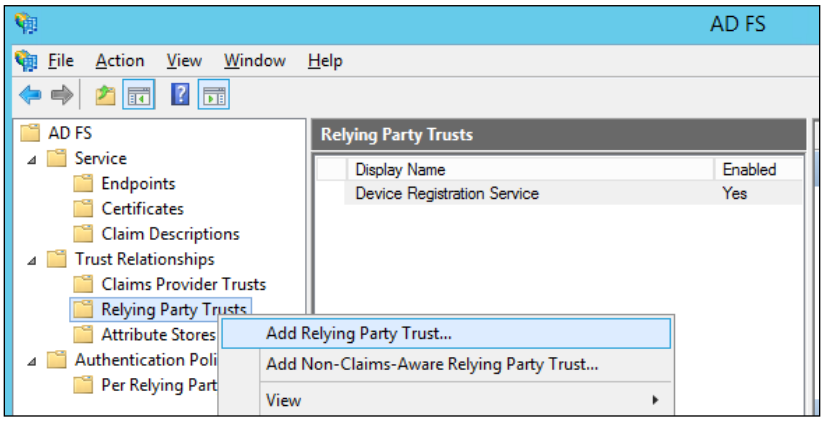
  The files will be attached to your SSO Setup Service Request ticket.

Step Three: Use the XML Files Provided in Your SSO Setup Service Request to Configure ADFS

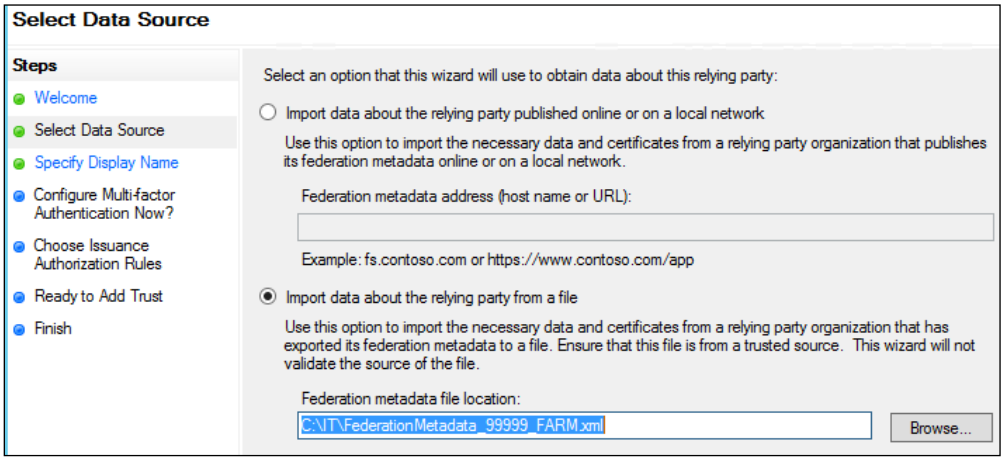
Important: Costpoint Enterprise customers should repeat this step for each Cloud Environment (Production, Implementation/Test/Preview, Dev) for which you want to set up ADFS.

To use the XML files to configure ADFS:

1. Copy the **FederationMetadata_ClientID_ClientNAME_ClientSystem.xml** that was provided to you in the SSO Setup Service Request onto your ADFS server.
2. Start the Active Directory Federation Services Management Console.
3. Select **Relying Party Trusts**, and click **Add Relying Party Trust**.

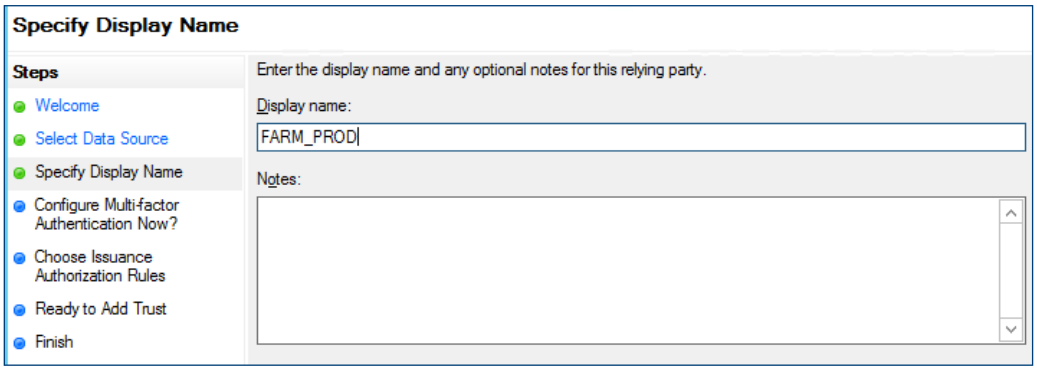


4. On Welcome page of the Add Relying Party Trust Wizard, click **Start**.
5. On the Select Date Source page, complete the following:
   a. Select the **Import data about the relying party from a file** option.
   b. Enter or browse to the **FederationMetadata_ClientID_ClientNAME_ClientSystem.xml** file you saved earlier, and click **Next**.

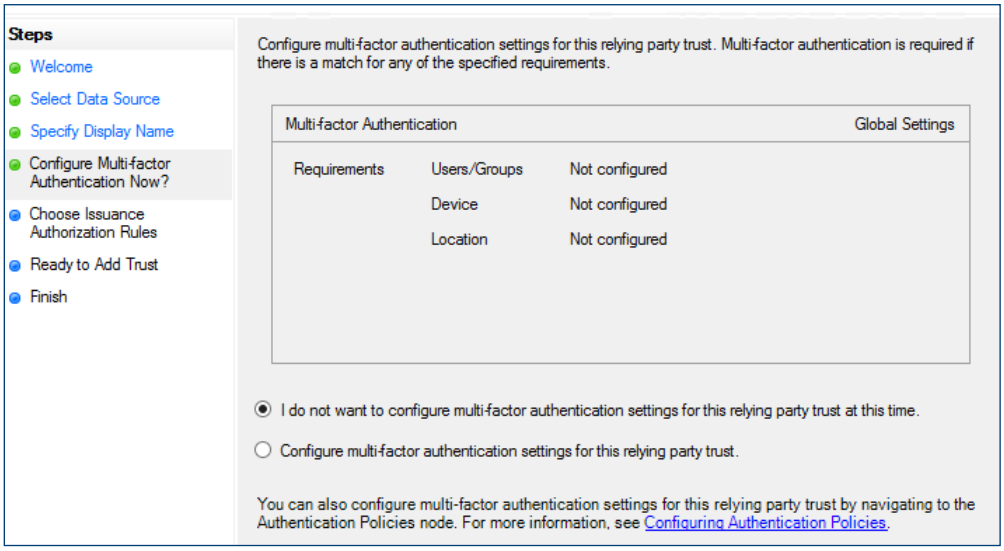


6. On the Specify Display Name page, enter a unique value for each system in the **Display name** field (for example, **<ClientName>_PROD**), and click **Next**.

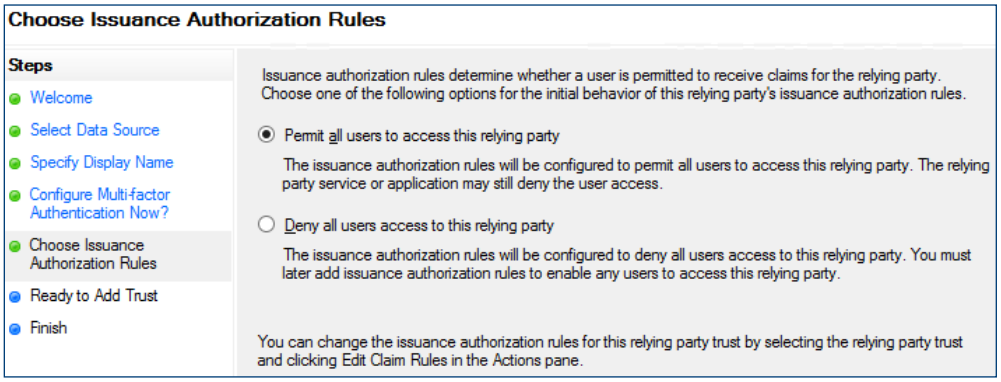
   The relying party **Display name** entered here should allow you to easily identify the Costpoint system that is being configured.



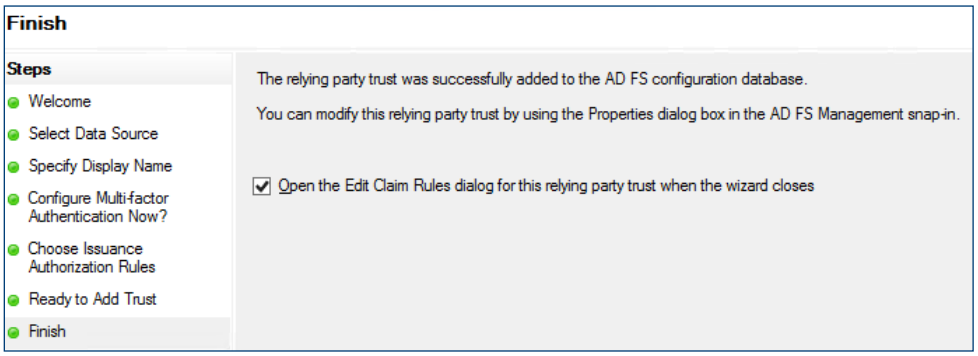
7. On the Steps page, accept the defaults, ensure that the **I do not want to configure multi-factor authentication settings for this relying Party trust at this time** option is selected, and click **Next**.



8. On the Choose Issuance Authorization Rules page, ensure that the **Permit all users to access this relying party option** is selected, and click **Next**.

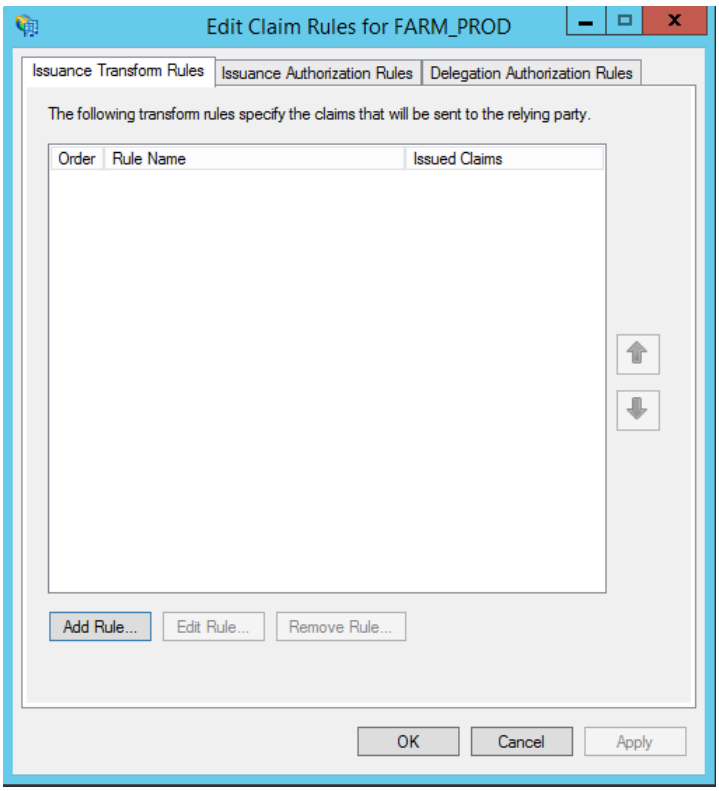


9. On the Ready to Add Trust page, accept defaults and click **Next**.
10. On the Finish page, ensure that the **Open the Edit Claim Rules for this relying party** check box is selected, and click **Close**.

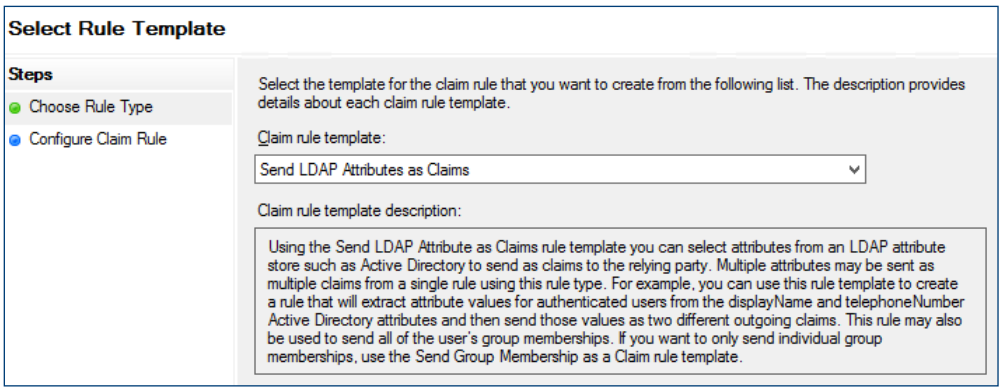


11. On the Edit Claim Rules for Costpoint dialog box, click **Add Rule**.

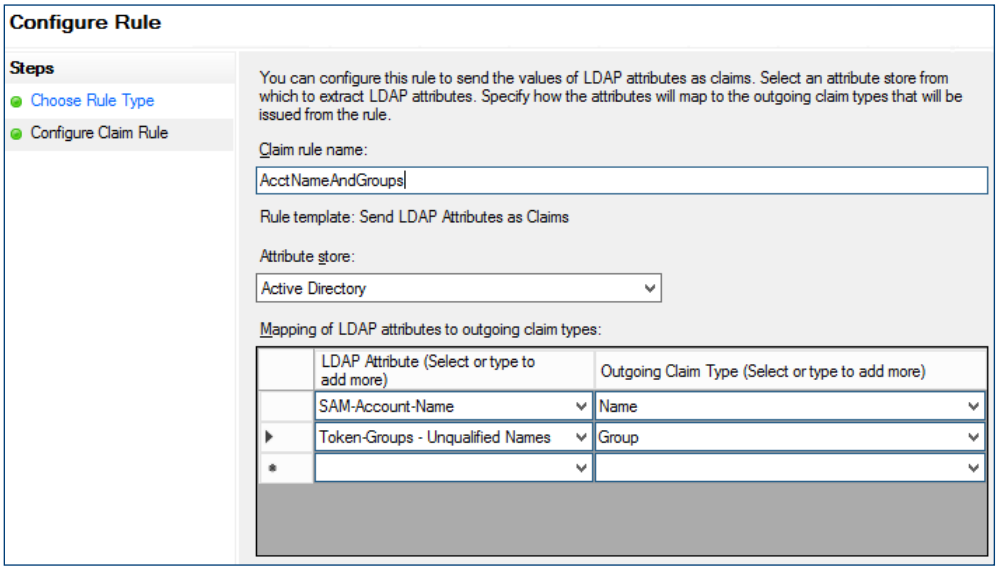
> **Note:** This section explains how to add an ADFS claim rule that will allow Costpoint to retrieve the group membership information from Active Directory Federation Services/Active Directory and synchronize this information with the Costpoint User Groups data.



12. On the Select Rule Template page of the Add Transform Claim Rule Wizard, select **Send LDAP Attributes as Claims** in the **Claims rule template** drop-down list, and click **Next**.



13. On the Configure Rule page, perform the following:
    - **Claim rule name**: Enter AcctNameAndGroups
    - **Attribute store**: Select **Active Directory** from the drop-down list.
    - **Mapping of LDAP attributes to outgoing claim types**: Take one of the following actions:
        - If you are using your company email address as your username, complete the following:
            - **LDAP Attribute**: Select **User-Principal-Name** from the drop-down list
            - **Outgoing Claim Type**: Select **Name** from the drop-down list
            - **LDAP Attribute**: Select **Token-Groups – Unqualified Names** from the drop-down list
            - **Outgoing Claim Type**: Select **Group** from the drop-down list
        - If you are NOT using your company email address as your username: complete the following:
            - **LDAP Attribute**: Select **SAM-Account-Name** from the drop-down list
            - **Outgoing Claim Type**: Select **Name** from the drop-down list
            - **LDAP Attribute**: Select **Token-Groups – Unqualified Names** from the drop-down list
            - **Outgoing Claim Type**: Select **Group** from the drop-down list



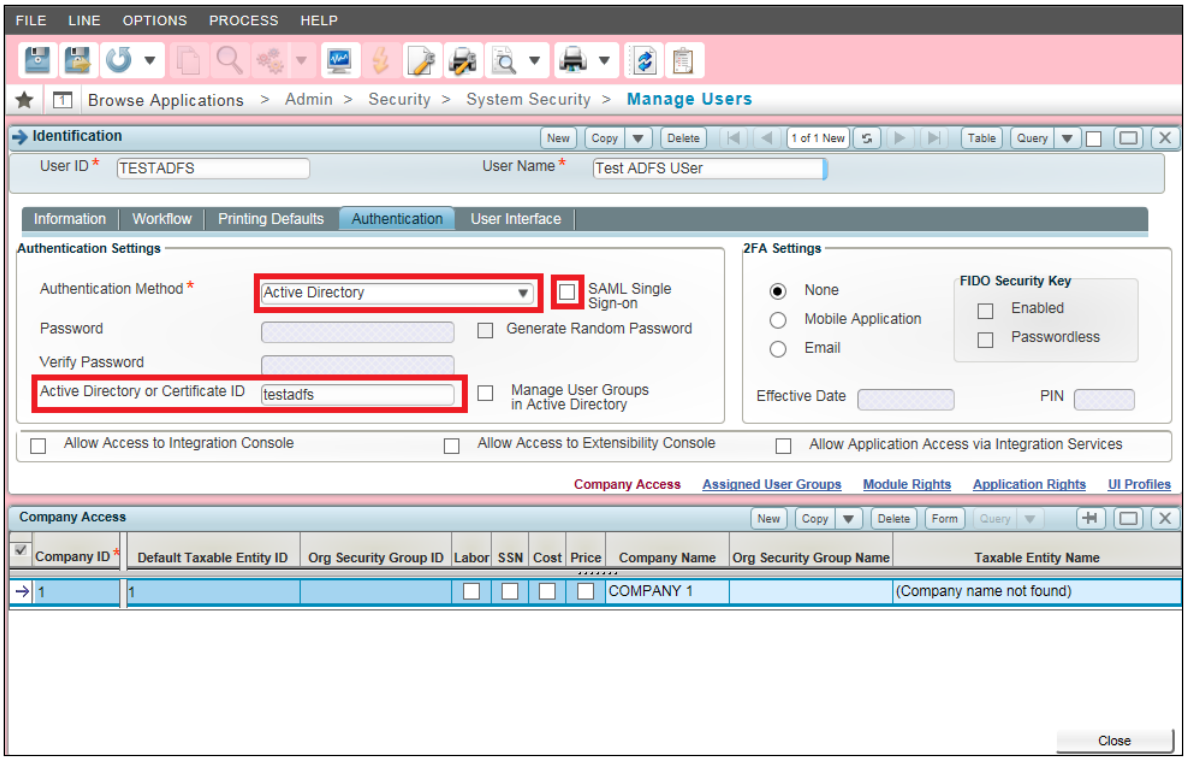
14. Click **Finish**, and then click **Ok**.

Step Four: Set up your Costpoint User Accounts for ADFS

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

To modify the authentication properties:

1. 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**.
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