

# Integrating District Active Directory Federation Services (ADFS) with DataHub ADFS

# Prerequisites

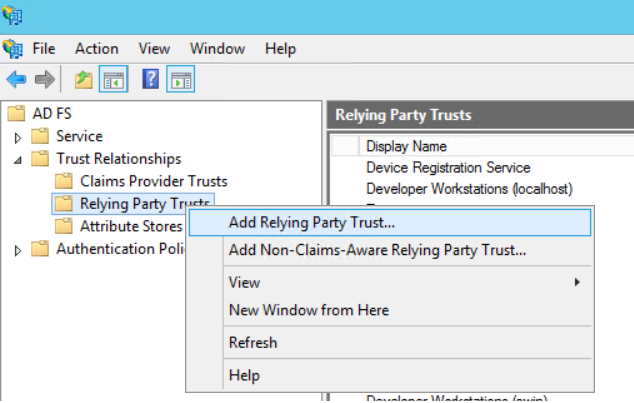
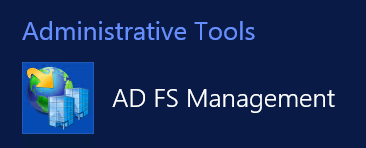
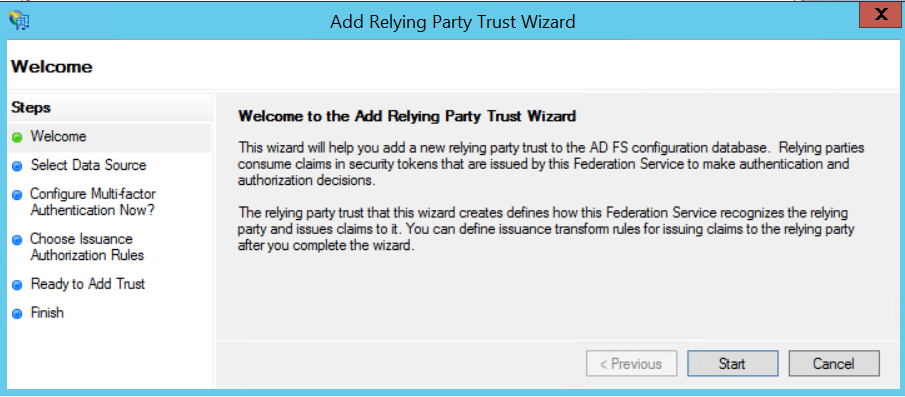
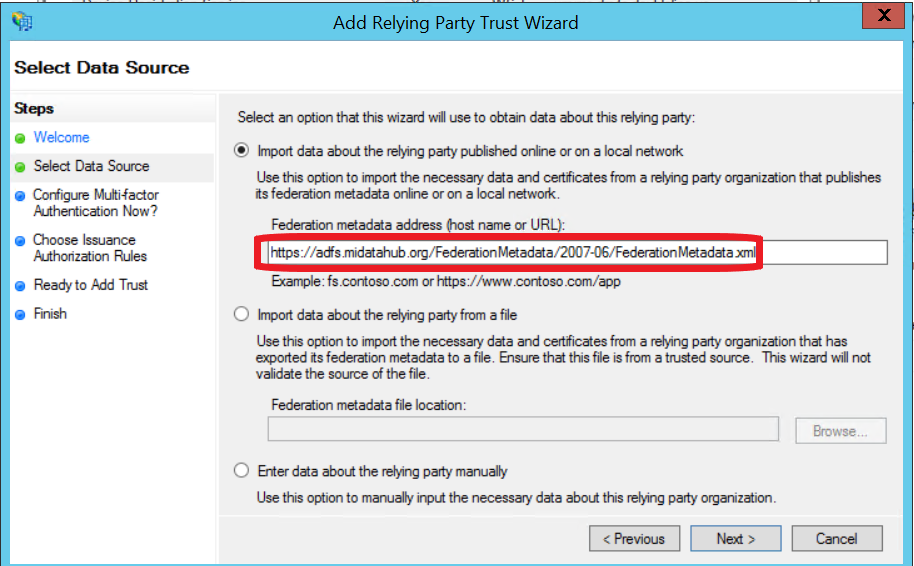
Given:

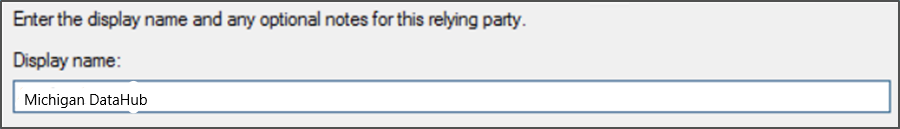
* A District ADFS (role: SAML Identity Provider - IdP)
* An OAuth 2 Michigan DataHub using ADFS (role: SAML Service Provider - SP)

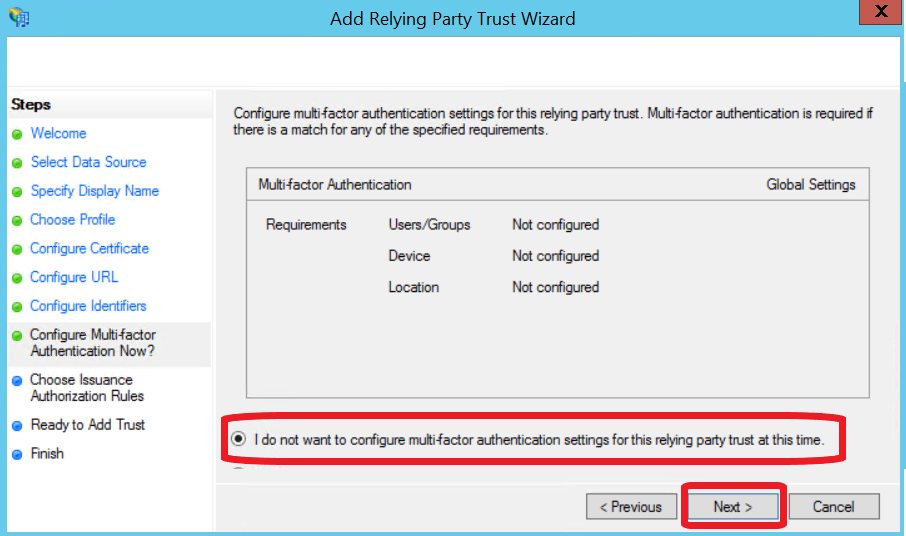
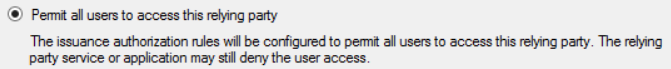
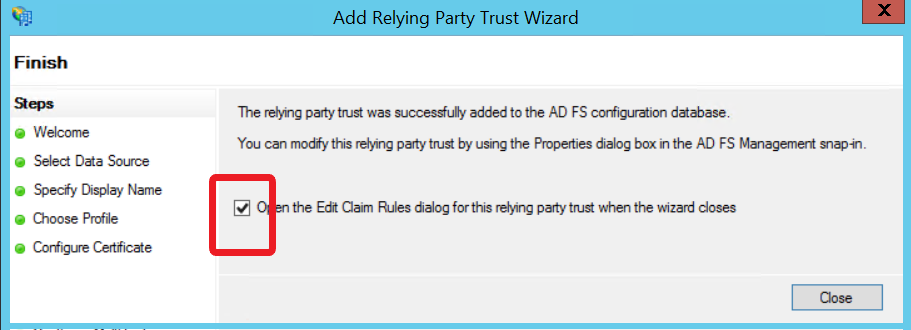
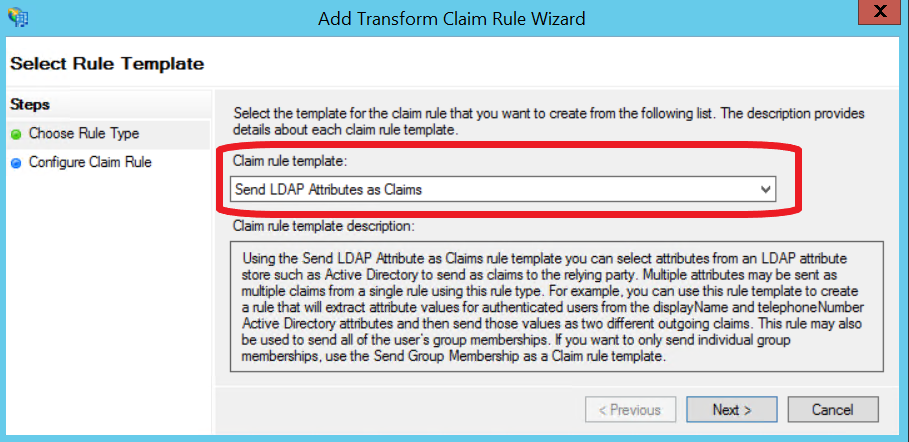
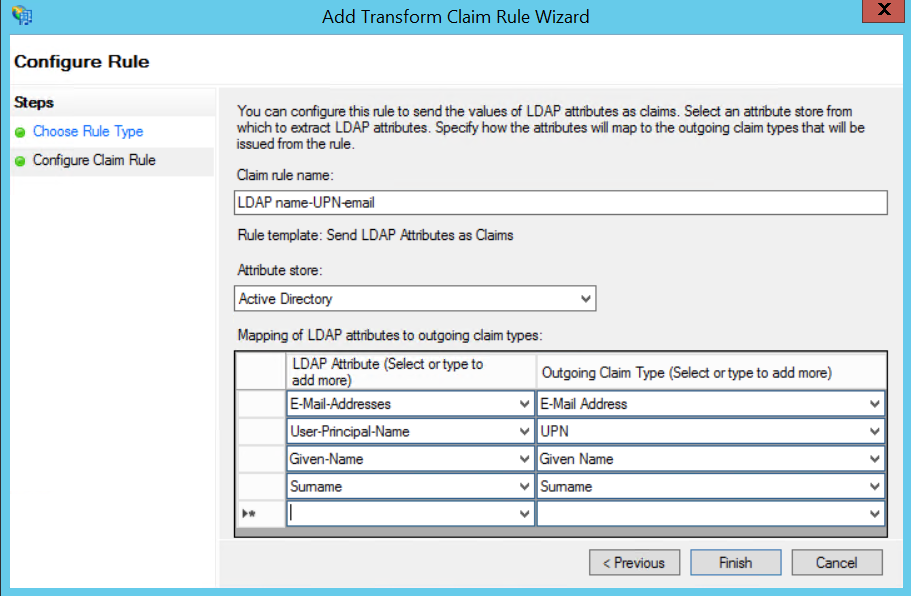
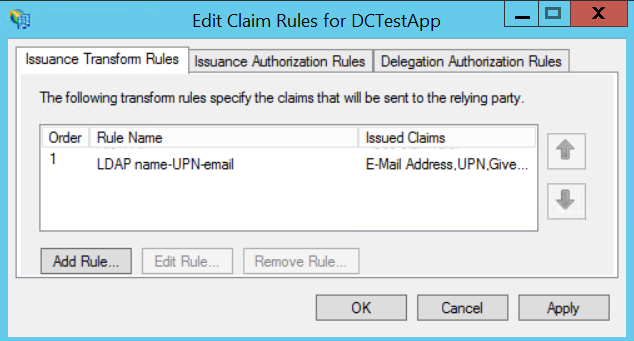
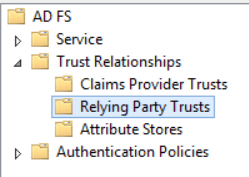
# Goal

The following procedure will configure single sign-on for applications connected to the DataHub ADFS, allowing claims to be retrieved from (i.e. allowing authentication by) a second, District ADFS. Throughout this document, these services will be referred to as "DataHub ADFS" and "District ADFS".

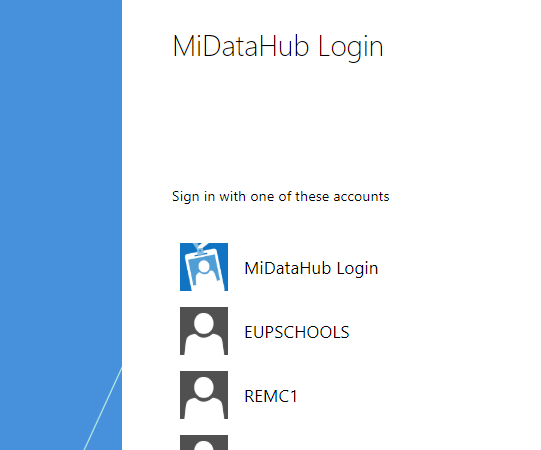
# District ADFS steps (for District I.T. Administrator team)

1. Before starting, the following should have already been completed:
   1. The district has delivered their metadata URL to the MiDataHub SSO team
   2. The district has identified for the MiDataHub SSO team the field in which the email address value is expected to be found (i.e., EmailAddress, UPN, etc.)
   3. The MiDataHub SSO team has added the district ADFS as an Identity Provider to the midatahub.org ADFS
2. Open the ADFS management console (found in the Admin Tools of the Active Directory Domain Controller or dedicated ADFS server). Right-click the **Relying Party Trusts** node and click the menu item **Add Relying Provider Trust …**
3. On the first step of the wizard, click **Start**.
4. On the second step of the wizard, select the option **Import data about the relying party published online.** Use the URL:   
   https://adfs.midatahub.org/FederationMetadata/2007-06/FederationMetadata.xml   
   Click **Next**. 
5. On the next step, enter the name of the application as you would wish an I.T. administrator to see it displayed.

  
  
(Continued on next page)

1. Accept the default for the **Multi-Factor Authentication** step. This can be changed at a later time if desired.  
   
2. Accept the default for the **Choose Issuance** step. This can be changed at a later time if desired.   
   
3. On the step **Ready to Add Trust**, click **Next**.
4. On the step **Finish**, leave the checkbox **Edit Claims Rules** checked.  
   
5. Add a claims rule to send Active Directory information using the "**Send LDAP Attributes**" template:  
     
     
   Note: The "Claim Rule Name" is arbitrary, but other entries in the screenshot below should be exactly as displayed.  
     
     
     
   Click **Finish** to finalize adding the rule.  
     
   
6. The Relying Party Trust you added is complete and should now be visible in the list of ADFS's Relying Party Trusts.  
     
   

1. To test, open a browser window and navigate to <https://adfs.doubleline.us/test_midatahub/>. You should land on the MiDataHub Login page which looks similar to the below screenshot.



Scroll down the list, find your district (organization), and select it. Sign in and you will be taken to a page that displays claims. You should find an email claim with the email address of the account you are using for verification testing.