Active Directory Federation Services (AD FS) Single Sign-On Configuration for Pivotal Cloud Foundry

Please follow the steps below to configure Single Sign-On between Active Directory Federation Services (AD FS) and Pivotal Cloud Foundry.

Configuring Active Directory Federation Services as the SAML 2.0 Identity Provider on Pivotal Cloud Foundry

1. Download the identity provider metadata from the Active Directory Federation Services server:
   https://<server_host_name>/federationmetadata/2007-06/federationmetadata.xml
2. Follow the steps listed at http://docs.pivotal.io/pivotalcf/opsguide/sso.html to set the identity provider metadata on Pivotal Cloud Foundry

Configuring PIvotal Cloud Foundry as the SAML 2.0 Service Provider on Active Directory Federation Services

1. Download the service provider metadata: https://login.<system_domain>/saml/metadata
2. Open the **AD FS Management** console.
3. Click **Add Relying Party Trust…** in the Actions pane.
4. On the Welcome step, click **Start**.
5. Select **Import data about the relying party from a file**, enter the path to the downloaded service provider metadata, and click **Next**.
6. Enter a name for **Display name** and click **Next**.
7. Leave the default multi-factor authentication selection and click **Next**.
8. Select **Permit all users to access this relying party** and click **Next**.
9. Review your settings and click **Next**.
10. Click **Close** to finish the wizard.
11. Select the **Encryption** tab and click **Remove** to remove the encryption certificate.
12. Select the **Advanced** tab and select **SHA-1** for the **Secure hash algorithm**.
13. (Optional) If you are using a self-signed certificate and want to disable CRL checks, follow these steps:
    a. Open **Windows Powershell** as an Administrator
    b. Execute the following command: `set-ADFSRelyingPartyTrust -TargetName "< Relying Party Trust >" -SigningCertificateRevocationCheck None`