PingFederate Single Sign-On Configuration for Pivotal Cloud Foundry

Please follow the steps below to configure Single Sign-On between Ping Federate and Pivotal Cloud Foundry.

Configuring PingFederate as the SAML 2.0 Identity Provider on Pivotal Cloud Foundry

1. Download the Identity Provider Metadata from PingFederate Server. Click Metadata Export under Administrative Functions on the Main Menu of the PingFederate Administrative Console. If your PingFederate server is configured to act as both an IdP and an SP, indicate which type of configuration you will export and click Next. The Signing key can be exported. You can skip the options related to Encryption Keys and Metadata Attribute Contract as both these are not supported at this time.
2. Follow the steps listed @ 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 Ping Federate

1. Download the Service Provider Metadata from: https://login.{system-domain}/saml/metadata
2. Import the Service Provider Metadata to PingFederate. Navigate to Main Menu -> IdP Configuration-> SP Connection and Click Import. In the Import Connection screen, browse and select the xml file downloaded from the previous step. Click Import and Done.
3. Pivotal Cloud Foundry expects the NameID format to be email address (*urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress*) and the value to be the currently logged in user's email. **Please note the SSO will not function without this setting.**
    a. Click the connection name on the Main Menu. Click Manage All SP, if needed, to see a full list of connections.
    b. Click Browser SSO under the SP Connection tab.
    c. Click Configure Browser SSO.
    d. Click Assertion Creation under the Browser SSO tab.
    e. Click Configure Assertion Creation.
    f. Click Identity Mapping on the Summary screen.
    g. Select "Standard" as the option and map the NameID format to be email address and the value to be the email address of the user.

4. Select the Authentication Source
    a. Click **Browser SSO** under the SP Connection tab.
    b. Click **Configure Browser SSO**.
    c. Click **Assertion Creation** under the Browser SSO tab.
    d. Click **Configure Assertion Creation**.
    e. Click **IdP Adapter Mapping** on the Summary screen.
    f. Click the Adapter Instance Name.
    g. Click **Adapter Instance** on the Summary screen.

5. Enable the SSO Browser Profiles
    a. Click Browser SSO under the SP Connection tab.
    b. Click Configure Browser SSO.
    c. Click SAML Profiles on the Summary screen.
    d. Please make sure that IdP & SP initiated SSO are selected.

    Note: Pivotal Cloud Foundry doesn't support SLO profiles at this time and they can be left unchecked

6. Activate the SP Connection