



PRODUCT DOCUMENTATION

# Single Sign-On for PCF<sup>®</sup>

Version 1.1

## User's Guide

Rev: 01

© 2018 Pivotal Software, Inc.

## Table of Contents

Table of Contents	2
Single Sign-On Overview	3
Installation	6
Getting Started with Single Sign-On	7
Manage Service Plans	8
Manage Service Instances	10
Configure Identity Providers	11
Bind or Register Applications	15
Manage Resources	18
Active Directory Federation Services Integration Guide Overview	20
Configure Active Directory Federation Services as an Identity Provider	21
Configure a Single Sign-On Service Provider	28
Testing	30
Troubleshooting	37
Azure Active Directory Integration Guide Overview	38
Configure Azure Active Directory as an Identity Provider	39
Configure a Single Sign-On Service Provider	46
Testing	49
Troubleshooting	56
Okta Integration Guide Overview	58
Configure Okta as an Identity Provider	59
Configure a Single Sign-On Service Provider	63
Testing	65
Troubleshooting	71
PingFederate Integration Guide Overview	73
Configure PingFederate as an Identity Provider	74
Configure a Single Sign-On Service Provider	80
Testing	82
Troubleshooting	88
PingOne Cloud Integration Guide Overview	89
Configure PingOne Cloud as an Identity Provider	90
Configure a Single Sign-On Service Provider	94
Testing	96
Troubleshooting	103
Release Notes	105

## Single Sign-On Overview

This topic provides an overview of the [Single Sign-On](#) service for Pivotal Cloud Foundry (PCF).

The Single Sign-On service is an all-in-one solution for securing access to applications and APIs on PCF. The Single Sign-On service provides support for native authentication, federated single sign-on, and authorization. Operators can configure native authentication and federated single sign-on, for example SAML, to verify the identities of application users. After authentication, the Single Sign-On service uses OAuth 2.0 to secure resources or APIs.

### Single Sign-On

The Single Sign-On service allows users to log in through a single sign-on service and access other applications that are hosted or protected by the service. This improves security and productivity since users do not have to log in to individual applications.

Developers are responsible for selecting the authentication method for application users. They can select a native authentication provided by the UAA or an external identity provider.

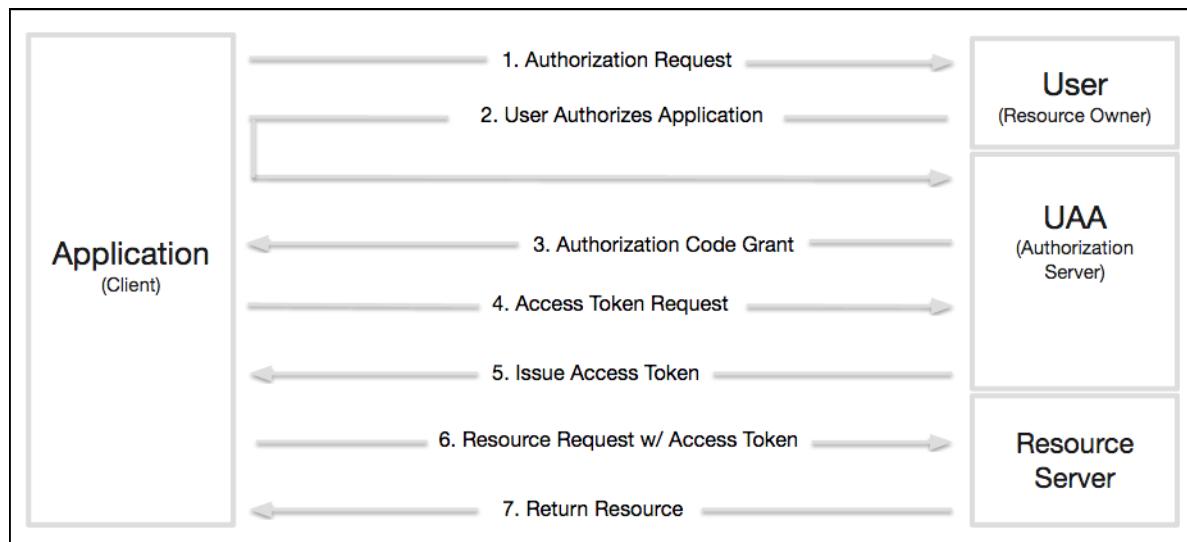
### OAuth 2.0 Concepts

After authentication, the Single Sign-On service uses OAuth 2.0 for authorization of applications and resources. The following describes the roles in an OAuth 2.0 scenario:

- **Resource Owner:** A person or system capable of granting access to a protected resource.
- **Resource Server:** The server that hosts protected resources and accepts and responds to protected resource requests using access tokens. Applications access the server through APIs.
- **Applications:** A client that makes protected requests using the authorization of the resource owner.
- **Authorization Server:** The Single Sign-On server that issues access tokens to client applications after successfully authenticating the resource owner.

### OAuth 2.0 Example Flow

The flow below shows an example of an authenticated user who is attempting to access a to-do list application. This application is backed by a resource server and both are secured by the UAA authorization server.



1. **Authorization Request:** The first time the user accesses the application, the application requests authorization to access the user's to-do items.
2. **User Authorizes Application:** The application requests access to the user's to-do items. The user clicks Yes to authorize the application to access their items.
3. **Authorization Code Grant:** After the user authorizes the to-do list app, the authorization server sends an authorization code.
4. **Access Token Request:** The application receives the authorization code and requests an access token from the authorization server. This gives the

application access to the user's to-do items.

5. **Issue Access Token:** The authorization server validates the authorization code and issues an access token.
6. **Resource Request w/ Access Token:** The to-do list application requests the resource from the resource server through the API and presents the access token.
7. **Return Resource:** If the access token is valid, the resource server returns the to-do items that the user authorized the application to receive.

The resource server runs in PCF under a given space and organization. Developers set the permissions for the resource server API endpoints. To do this, they create resources that correspond to API endpoints secured by the Single Sign-On service. Applications can then access these resources on behalf of users.

## Product Snapshot

Current [Single Sign-On](#) for Pivotal Cloud Foundry Details

- **Version:** 1.1.1
- **Release Date:** 2016-05-05
- **Software component versions:** Single Sign-On 1.1.1 Installer based on Elastic Runtime 1.7 or later
- **Compatible Ops Manager Version(s):** 1.7 or later
- **Compatible Elastic Runtime Version(s):** 1.7 or later
- **vSphere support?** Yes
- **AWS support?** Yes
- **OpenStack support?** Yes

## Upgrading to the Latest Version

Consider the following compatibility information before upgrading Single Sign-On for Pivotal Cloud Foundry®.

Elastic Runtime Version	Supported Upgrades from SSO Versions	
	From	To
1.6.x	1.0.1-1.0.15	1.0.16
1.7.x	1.0.1-1.0.16	1.1.1
	1.1.0	

 **Note:** The [Single Sign-On service tile](#) operates in lockstep with Pivotal Elastic Runtime.

- The SSO v1.0.x tiles are compatible with PCF v1.6.x
- The SSO v1.1.x tiles are compatible with PCF v1.7.x

If you are a customer upgrading from PCF 1.6 to PCF 1.7 and you are using SSO v1.0.x, you must update to a SSO v1.1.x service tile before proceeding with the upgrade.

## Single Sign-On for Pivotal Cloud Foundry

- [Installation](#)
- [Getting Started with Single Sign-On](#)
- [Manage Service Plans](#)
- [Manage Service Instances](#)
- [Configure Identity Providers](#)
- [Bind or Register Applications](#)
- [Manage Resources](#)

## Active Directory Federation Services (AD FS) Integration Guide

- [Active Directory Federation Services Integration Guide](#)
  - [Configure Active Directory Federation Services as an Identity Provider](#)
  - [Configure SSO Service](#)
  - [Testing](#)
  - [Troubleshooting](#)

## Azure Active Directory Integration Guide

- [Azure Active Directory Integration Guide](#)
  - [Configure Azure Active Directory as an Identity Provider](#)
  - [Configure SSO Service](#)
  - [Testing](#)
  - [Troubleshooting](#)

## Okta Integration Guide

- [Okta Integration Guide](#)
  - [Configure Okta as an Identity Provider](#)
  - [Configure SSO Service](#)
  - [Testing](#)
  - [Troubleshooting](#)

## PingFederate Integration Guide

- [PingFederate Integration Guide](#)
  - [Configure PingFederate as an Identity Provider](#)
  - [Configure SSO Service](#)
  - [Testing](#)
  - [Troubleshooting](#)

## PingOne Cloud Integration Guide

- [PingOne Cloud Integration Guide](#)
  - [Configure PingOne as an Identity Provider](#)
  - [Configure SSO Service](#)
  - [Testing](#)
  - [Troubleshooting](#)

## Additional Information

- [Release Notes](#)

## Installation

This topic explains how to install Single Sign-On (SSO) for Pivotal Cloud Foundry.

## Prerequisites

- Pivotal Cloud Foundry ([Ops Manager](#) and [Elastic Runtime](#)) version 1.7 or later.
- SSL Certificates.
- Application Security Groups.

## Install SSO via Ops Manager

1. From [Pivotal Network](#), select a **Single Sign-On** tile version and download the product release file.
2. From the Ops Manager Installation Dashboard, select the **Import a Product** button to upload the product file.
3. Click **Add** next to the uploaded product description in the Available Products view to add this product to your staging area.
4. Click on the **Single Sign-On** tile to enter any configurations.

 **Note:** The Single Sign-On service tile requires a network with only one subnet. The tile does not install when configured with a network that has more than one subnet.

 **Note:** The SSO Identity Service Broker is deployed as a PCF application from a BOSH errand, and has no associated BOSH VMs that require selecting a corresponding network. If you are forced to select a network during installation, select the **Deployment** network, also known as the PAS or ERT network.

5. Click **Apply Changes** to install the product.

## Update SSL and Load Balancer

You must update the SSL certificate for the domains listed below for each plan you create. Depending on your infrastructure and load balancer, you must also update your load balancer configuration for the following domains:

- \*.SYSTEM-DOMAIN
- \*.APPS-DOMAIN
- \*.login.SYSTEM-DOMAIN
- \*.uaa.SYSTEM-DOMAIN

## Configure Application Security Groups

The Single Sign-On service requires the following network connections:

- TCP connection to load balancer(s) on port 443
- TCP and UDP connection to Domain Name Servers on port 53
- (Optional) TCP connection to your external identity provider on port 80 or 443

To enable access to the Single Sign-On service, you must ensure your Application Security Group allows access to the load balancer(s) and domain name servers that provide access to Cloud Controller and UAA. Optionally, you can configure access to your external identity provider to receive SAML metadata. For more details on how to set up application security groups, see the [Application Security Groups](#) topic.

## Getting Started with Single Sign-On

This topic outlines the steps for installing and configuring the [Single Sign-On](#) service.

### Install and Set Up SSO for Applications

1. [Install Single Sign-On](#) via Ops Manager.
2. [Create a service plan](#). The Single Sign-On service is a multi-tenant service, and a service plan corresponds to a tenant. This allows an enterprise to segregate users or environments using plans. Each service plan is accessible at a tenant-specific URL in the format `https://AUTH-DOMAIN.login.SYSTEM-DOMAIN`.
3. [Create a service instance](#). Single Sign-On service plans can provide single sign-on capabilities for applications in various spaces. A service instance lets you bind an application to a service plan.
4. [Configure an identity provider](#). In addition to the [Internal User Store](#), you can configure [external identity providers](#) to provide single sign-on to applications. External identity providers must support SAML 2.0.
5. [Register your applications](#). Single Sign-On supports both Pivotal Cloud Foundry-hosted applications as well as externally hosted applications. Your applications must be able to request an OAuth or OpenID Connect token.
6. [Create resources for your applications](#). If your registered applications need to make external API calls, you can assign the API endpoints as resources permitted for the application. This will whitelist the endpoints for use by the application or client.

### SSO User Roles

A user's role determines which parts of an SSO configuration it can manage. SSO uses the existing user roles PCF Administrator and Space Developer, as well as a SSO-specific Plan Administrator role. This chart shows the management permissions for each role.

Management access by role	PCF Administrator	Plan Administrator	Space Developer
Service plans	X		
Service instances	X	X	X
Identity providers	X	X	
Applications	X	X	X
Resources	X	X	X

### Using SSO for Pivotal Cloud Foundry Components

In addition to applications, SSO supports single sign-on for components of Pivotal Cloud Foundry, including Ops Manager and Apps Manager. This allows users already managed in an external identity provider to sign into Pivotal services. Refer to the following pages for instructions on configuring SSO to enable users in an external identity store to access PCF components:

- Ops Manager, on [Amazon Web Services](#), [vSphere](#), [vCloud and vCloud Air](#), or [OpenStack](#)
- [Apps Manager](#)

## Manage Service Plans

This topic describes how Pivotal Cloud Foundry (PCF) Administrators create and delete Single Sign-On service plans.

Single Sign-On is a multi-tenant service, which enables a deployment to host multiple service plans. Each service plan corresponds to a tenant, which can represent multiple users. This lets enterprises segregate their tenants into separate plans. For example, the following tenants might require separate plans:

- Business units and geographical locations
- Employees, consumers, and partners
- Development, staging, and production instances

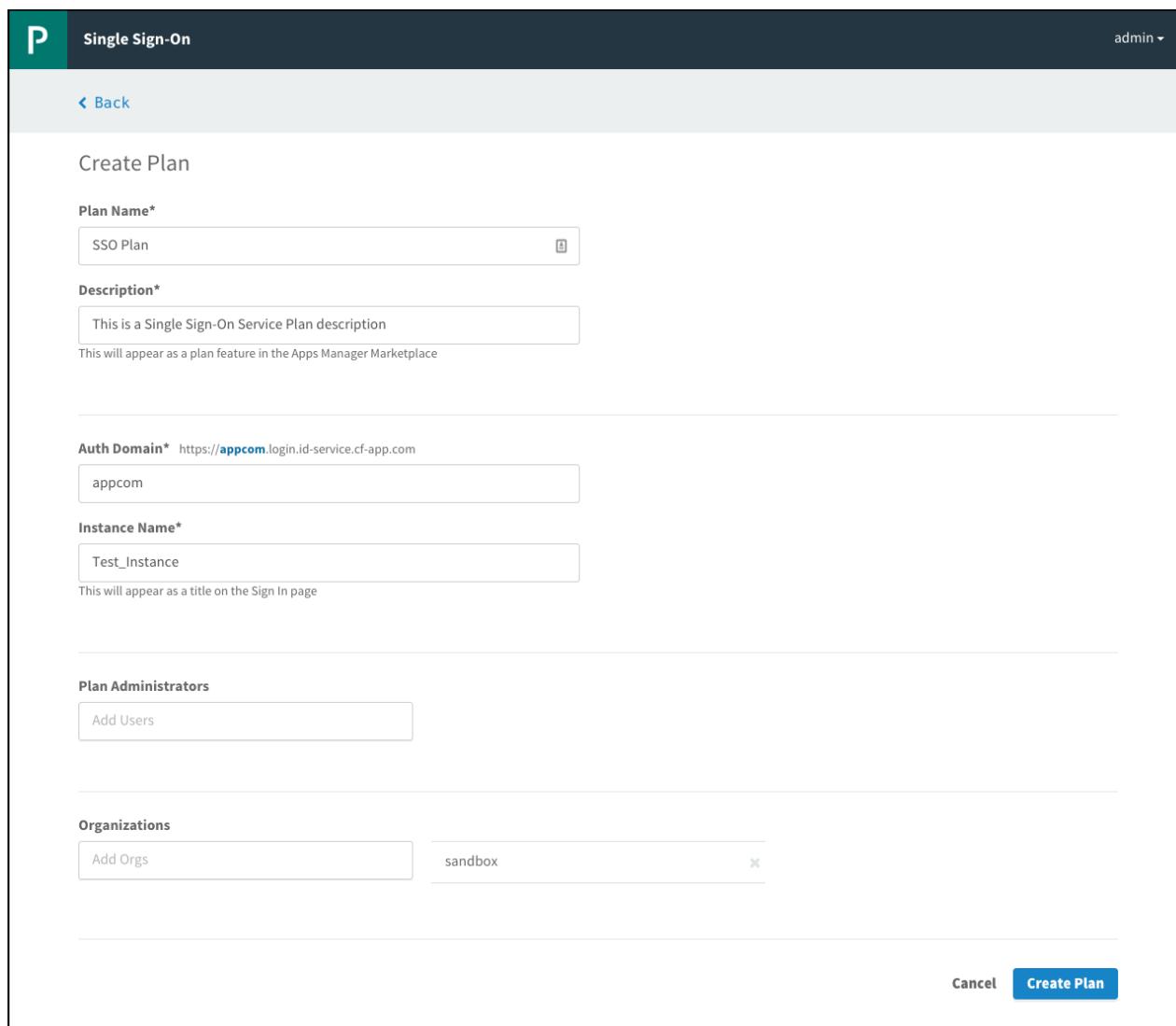
Administrators can create new Single Sign-On service plans at any time from the SSO dashboard.

## Create or Edit Service Plans

You can use the SSO dashboard to create and configure service plans at any time.

 **Note:** You must create at least one plan for any service before your applications can use it.

1. Log into the SSO dashboard at <https://p-identity.YOUR-SYSTEM-DOMAIN> using your User Account and Authentication (UAA) administrator credentials. You can find these credentials in your Pivotal Elastic Runtime tile in Ops Manager under the Credentials tab.
2. Click **New Plan** on the SSO dashboard to create a new Single Sign-On service plan.



The screenshot shows the 'Create Plan' page of the Pivotal Single Sign-On interface. The top navigation bar includes a 'P' logo, the title 'Single Sign-On', and a user dropdown labeled 'admin'. Below the title, there's a back button and a 'Create Plan' heading. The main form fields are:

- Plan Name\***: A text input field containing 'SSO Plan' with a small info icon to its right.
- Description\***: A text input field containing 'This is a Single Sign-On Service Plan description' with a note below stating 'This will appear as a plan feature in the Apps Manager Marketplace'.
- Auth Domain\***: A text input field containing 'https://appcom.login.id-service.cf-app.com' with a note below stating 'appcom'.
- Instance Name\***: A text input field containing 'Test\_Instance' with a note below stating 'This will appear as a title on the Sign In page'.
- Plan Administrators**: A button labeled 'Add Users'.
- Organizations**: A button labeled 'Add Orgs' next to a list item 'sandbox' with a delete 'X' icon.

At the bottom right of the form are 'Cancel' and 'Create Plan' buttons.

3. Enter a **Plan Name**.
4. Enter a **Description** to appear as a plan feature in the Services Marketplace.
5. Enter an **Auth Domain** to be the URL where users authenticate to access applications covered by the service plan.
6. Enter an **Instance Name** to appear on the login page and in other user-facing content, such as email communications.
7. Add **Plan Administrators**. These users can view the plan and manage identity providers.
8. Under **Org Visibility**, select which organizations in your Pivotal Cloud Foundry deployment should have access to your Single Sign-On service plan. If you do not select any organizations, the plan will not be available for use and it will not be displayed in the Services Marketplace.
9. Click **Create Plan**. Your new plan appears in the Services Marketplace in the organizations you have selected. Users in those organizations view the plan either in Apps Manager or through the CF CLI by entering `cf marketplace` in a terminal window.

## Delete Service Plans

1. Log into the SSO dashboard at <https://p-identity.YOUR-SYSTEM-DOMAIN> using your UAA administrator credentials. You can find these credentials in your Pivotal Elastic Runtime tile in Ops Manager under the Credentials tab.
2. Select the name of the plan you want to delete, and click **Edit Plan** in the dropdown menu.
3. Select **Delete** at the bottom of the page.
4. In the popup that appears, click **Delete Plan** to confirm that you want to delete the plan.

 **Note:** This action cannot be undone. Deleting a Single Sign-On service plan removes from the SSO database all of the configurations, identity providers, users, application configurations and resources associated with the plan. It also deletes the associated service instances and service bindings. You must rebind any applications bound to the deleted service instances to new service instances.

## Manage Service Instances

This topic describes how Space Developers create an instance of a Single Sign-On service plan in their space and bind it to an application.

### Create Service Instances

1. Log into Apps Manager at <https://apps.YOUR-SYSTEM-DOMAIN> as a Space Developer.
2. Navigate to the organization that the service plan is enabled for.
3. Select **Marketplace** and select the Single Sign-On service you want to create an instance of.
4. Choose your service plan and click **Select this plan**.
5. In the **Configure Instance** box, enter an **Instance Name**.
6. From the **Add to Space** dropdown menu, choose a space for the instance. This space hosts your application. The default is **development**.
7. From the **Bind to App** dropdown menu, choose an application to bind the service instance to. This option defaults to **[do not bind]**. If you do not bind the instance to an app, you can bind it at a later time.
8. Click **Add** to create the service instance.

### Delete Service Instances

1. Log into Apps Manager at <https://apps.YOUR-SYSTEM-DOMAIN> as a Space Developer.
2. Navigate to the organization and space that contain the service instance you want to delete.
3. Under **Services** in the space page, find your service instance and click **Delete**.
4. Click **Delete** on the pop-up to confirm that you want to delete the service instance and service bindings.

 **Note:** This action cannot be undone. Deleting a Single Sign-On service instance deletes the configurations on the service instance, as well as the associated service bindings. You must bind any applications bound to the deleted service instance to a new service instance.

## Configure Identity Providers

This topic describes how administrators can use an Internal User Store or an external identity provider to manage user access to a Single Sign-On (SSO) service plan.

For each plan, SSO provides an Internal User Store that manages users. As an alternative to the Internal User Store, administrators can use an external identity provider to allow users who are externally managed to access applications.

### Configure Internal User Store

1. Log into the SSO dashboard at `https://p-identity.YOUR-SYSTEM-DOMAIN` using your User Account and Authentication (UAA) administrator credentials. You can find these credentials in your Pivotal Elastic Runtime tile in Ops Manager under the Credentials tab.
2. Click the plan name and select **Manage Identity Providers** from the dropdown menu.
3. Click **Internal User Store**.
4. Enter a **Description**.
5. Under **Password Policy Settings**, select **Use Recommended Settings**, **Use Default Settings**, or enter custom settings in the fields below.
6. Click **Save Identity Provider**.

### Add Users to the Internal User Store

You cannot add users to Service Plans from the SSO dashboard. In order to add users to the Internal User Store for a given Service Plan, you must use the UAA Command Line Interface (UAAC). If you do not already have the UAAC installed, run `gem install cf-uaac` in a terminal window.

The following steps describe how to use UAAC to add users to an Internal User Store.

#### Step 1: Client Registration

1. Target your system domain.

```
$ uaac target https://login.YOUR-SYSTEM-DOMAIN
```

 **Note:** If you do not have SSL configured, you can turn off SSL validation with `--skip-ssl-validation`

2. Fetch your admin client token.

```
$ uaac token client get admin  
Client secret:
```

3. When prompted with `Client secret`, enter your **Admin Client Credentials** located in the **Credentials** tab of your **Pivotal Elastic Runtime** tile.

4. Update client registrations for `identity` and add `password` as a supported authorization grant type.

```
$ uaac client update identity --authorized_grant_types "refresh_token,password,client_credentials,authorization_code"
```

#### Step 2: Client Creation

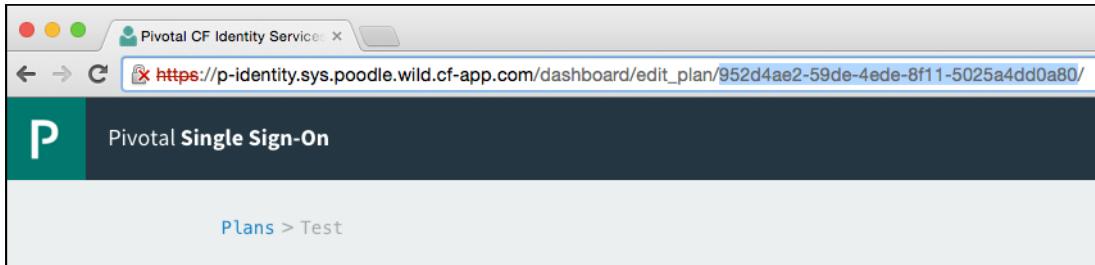
1. Target your system domain.

```
$ uaac target https://login.YOUR-SYSTEM-DOMAIN
```

2. Use the identity client and the administrator user credentials to retrieve a token which allows client creation in a given identity zone.

```
$ uaac token owner get
```

3. When prompted with **Client ID**, type **identity** and press enter.
4. For **Client secret**, enter your **Identity Client Credentials**, located in the **Credentials** tab of your **Pivotal Elastic Runtime** tile.
5. For **User name**, enter **Admin**.
6. Enter your **Password**, which is located in the **Admin Credentials** under the **Credentials** tab of your **Pivotal Elastic Runtime** tile.
7. Find the Identity Zone ID of your Service Plan by logging into the SSO dashboard, selecting **Edit Plan**, and copying the Identity Zone ID from the URL.



The highlighted

text in the example URL above is the Identity Zone ID of the Service Plan.

8. Execute the following command, replacing **YOUR-IDENTITY-ZONE-ID** with the Identity Zone ID of your Service Plan. You can also replace **service\_plan\_admin\_client** with a different name for your client, and **secret** with a different client secret.

```
uaac curl -k -H"Accept:application/json" -H"Content-Type:application/json" -H"X-Identity-Zone-Id:YOUR-IDENTITY-ZONE-ID" -XPOST --data '{"client_id":"service_plan_admin_client","client_secret": "secret"}
```

## Step 3: User Creation

1. Target the auth domain of your SSO service plan. This is the URL you provided when creating a Service Plan in the SSO dashboard.

```
$ uaac target https://YOUR-AUTH-DOMAIN.login.YOUR-SYSTEM-DOMAIN
```

2. Fetch the token for your Service Plan admin client.

```
$ uaac token client get service_plan_admin_client
Client secret:
```

3. When prompted with **Client secret**, enter the **secret** from the **uaac curl** command above.

4. Add new users by providing the user's email address, username, and password.

```
$ uaac user add --emails YOUR-USER@EMAIL.COM
User name: YOUR-USER
Password: ****
Verify password: ****
user account successfully added
```

5. (Optional) You can also create groups and add users to them.

```
$ uaac group add
Group name: YOUR-GROUP
meta
version: 0
created: 2016-02-19T23:17:17.000Z
lastmodified: 2016-02-19T23:17:17.000Z
schemas: urn:scim:schemas:core:1.0
id: 8725b5fd-8da2-4fcf-89b1-c57048f089c2
displayname: YOUR-GROUP
```

To add a member to your new group, use the following command.

```
$ uaac member add YOUR-GROUP YOUR-USER
```

## Define Password Policy for the Internal User Store

Administrators can define the password policy for SSO users that are stored in the Internal User Store. The Internal User Store password policy allows you to define and enforce password rules to manage the kind of passwords users can create.

1. Log into the SSO dashboard at <https://p-identity.YOUR-SYSTEM-DOMAIN> using your UAA administrator credentials. You can find these credentials in your Pivotal Elastic Runtime tile in Ops Manager under the Credentials tab.
2. Click the plan name and select **Manage Identity Providers** from the dropdown menu.
3. Click **Internal User Store**.
4. Configure the following under the **Password Complexity** section:
  - **Min Length:** Specify the minimum password length.
  - **Uppercase:** Specify the minimum number of uppercase characters required in a password.
  - **Lowercase:** Specify the minimum number of lowercase characters required in a password.
  - **Special Characters:** Specify the minimum number of special characters required in a password.
  - **Numerals:** Specify the minimum number of numeric characters required in a password.
5. Configure the following under the **Lockout Policy** section:
  - **Failures Allowed:** Specify the number of failed login attempts allowed per hour before a user is locked out.
  - **Lockout Period:** Specify the number of seconds a user is locked out for after excessive failed login attempts.
  - **Password Expires:** Specify the number of months passwords are valid for before users needs to enter a new password.
6. Click **Save Identity Provider**.

## Configure Service Provider SAML Settings

For each plan, the Single Sign-On service allows you to configure SAML settings when SAML is used for exchanging authentication and authorization data between the identity provider and the service provider. The SSO service provides the ability to sign authentication requests and require signed assertions from the external identity provider.

1. Log into the SSO dashboard at <https://p-identity.YOUR-SYSTEM-DOMAIN> using your UAA administrator credentials. You can find these credentials in your Pivotal Elastic Runtime tile in Ops Manager under the Credentials tab.
2. Click the plan name and select **Manage Identity Providers** from the dropdown menu.
3. Click **Configure SAML Service Provider**.
4. Configure the following settings:
  - **Perform signed authentication requests:** The service provider signs requests sent to the external identity provider.
  - **Require signed assertions:** The service provider requires that responses from the external identity provider are signed.
5. Click **Save** to save the SAML configurations.
6. Click **Download Metadata**.

## Add an External Identity Provider

1. Log into the SSO dashboard at <https://p-identity.YOUR-SYSTEM-DOMAIN> using your UAA administrator credentials. You can find these credentials in your Pivotal Elastic Runtime tile in Ops Manager under the Credentials tab.
2. Click the plan name and select **Manage Identity Providers** from the dropdown menu.
3. Click **New Identity Provider**.
4. Enter an **Identity Provider Name**.
5. Enter a **Description**. This is displayed to Space Developers when selecting an identity provider for their application.
6. Enter the external identity provider metadata in one of the following ways:
  - Option 1: Provide the **Identity Provider Metadata URL** and click **Fetch Metadata**.
  - Option 2: Click **Upload Identity Provider Metadata** to upload XML metadata that you downloaded from your external identity provider.

7. Configure any **User Attributes** to propagate from the identity provider to the service provider. These attributes can include e-mail addresses, first or last names, or external groups. They will be sent to applications via OpenID Connect tokens issued by the Single Sign-On service.
  - Select a **User Scheme Attribute** from the dropdown menu.
  - Enter a **SAML Attribute Name** with the corresponding attribute from the incoming SAML assertion.
8. Configure any **Custom Attributes** that should be propagated from the identity provider to the service provider. These attributes will be sent to applications via OpenID Connect tokens issued by the Single Sign-On service.
  - Enter a **Custom Attribute Name**.
  - Enter a **SAML Attribute Name** with the corresponding attribute from the incoming SAML assertion.
9. Click **Create Identity Provider** to save the identity provider.

 **Note:** To configure the service provider SAML settings, such as the signing of authentication requests and incoming assertions, click on **Configure SAML Service Provider** on the Identity Providers page.

## Delete an External Identity Provider

1. Log into the SSO dashboard at `https://p-identity.YOUR-SYSTEM-DOMAIN` using your UAA administrator credentials. You can find these credentials in your Pivotal Elastic Runtime tile in Ops Manager under the Credentials tab.
2. Click the plan name and select **Manage Identity Providers** from the dropdown menu.
3. Click on the name of your external identity provider.
4. Click **Delete** at the bottom of the page.
5. In the popup that appears, click **Delete Identity Provider** to confirm that you want to delete the identity provider, along with all of its configurations.

 **Note:** Deleting an external identity provider deletes all of its configurations. Users will no longer be able to authenticate using the external identity provider. This action cannot be undone.

## Configure Group Whitelist for an External Identity Provider

An administrator can configure groups from an external identity provider to be propagated in the ID token by including the group in the Group Whitelist. This will provide information to the application about the external identity groups that the user belongs to.

 **Note:** The `roles` scope must be requested by the application and the external group must be listed in the Group Whitelist.

1. Log into the SSO dashboard at `https://p-identity.YOUR-SYSTEM-DOMAIN` using your UAA administrator credentials. You can find these credentials in your Pivotal Elastic Runtime tile in Ops Manager under the Credentials tab.
2. Click the plan name and select **Manage Identity Providers** from the dropdown menu.
3. Click **Group Whitelist**.
4. Add a group name from your external identity provider.
5. Click **Save Group Whitelist**.

## Bind or Register Applications

This topic describes how Space Developers bind or register applications to their Single Sign-On (SSO) service instances.

If your application is hosted on Pivotal Cloud Foundry (PCF), refer to the [Bind an Application Hosted on PCF](#) section to bind your application to your SSO service instance from Apps Manager. If your application is externally hosted, then refer to the [Register an External Application](#) section to register your application with your SSO service instance from the SSO dashboard.

When you bind or register an application with a SSO service instance, SSO creates an OAuth client. This OAuth client acts as an OAuth 2.0 authorization server and issues tokens.

## Determine Your Application Type

Before you bind or register an application, you must know your SSO application type. Refer to the table below to determine the application type best suited for your application.

If your application authenticates end users, then your application type is `Web App`, `Native Mobile App`, or `Single Page Javascript App`. If your application does not authenticate end users, but rather accesses other services or APIs on its own behalf, then your application type is `Service-to-Service App`.

APPLICATION TYPE	SSO APPLICATION TYPE	OAUTH GRANT TYPE EQUIVALENT
Web	Web App	Authorization Code
Native Mobile, Desktop, or Command Line	Native Mobile App	Resource Owner Password
Single Page JavaScript	Single Page JavaScript App	Implicit
Service-to-Service	Service-to-Service App	Client Credentials

 **Note:** The Native Mobile App application type is intended only for highly trusted applications such as company owned and managed applications.

## Bind an Application Hosted on PCF

1. Log into Apps Manager as a Space Developer.
2. Select the space where your application is located.
3. Under **Applications**, click the name of your application.
4. Perform the following steps to add the `GRANT_TYPE` environment variable:
  - a. From the Application page, click the **Env Variables** tab.
  - b. Click **Add an Env Variable**.
  - c. For **Variable Name**, enter `GRANT_TYPE`.
  - d. For **Value**, enter your application type. For example, `Single Page JavaScript App`. If you do not provide a `GRANT_TYPE` variable, the application type defaults to `web App`.
5. Click the **Services** tab.
6. Click **Bind a Service**.
7. From the dropdown menu, select your SSO service instance. Click **Bind**, which creates an OAuth Client based on the grant type you set.
8. Click **Manage** under the SSO service instance to launch the SSO dashboard.
9. Click your application.
10. Under **Identity Providers**, select either **Internal User Store** or the name of your external identity provider. Internal User Store is the default.
11. Click **Save Config**.
12. If your Application Type is `Web App`, enter a whitelist of **Auth Redirect URIs** beneath **Redirect URIs**. The redirect query parameter specified on the

OAuth request must match the URIs specified in this list. Otherwise, SSO rejects the request.

13. Enter the **Scopes** that this application can request. This field defaults to `openid`. Scopes are permissions that the application requests on the user's behalf. If this application is purely for authentication purposes, then the `openid` scope is sufficient. If the application makes API calls on behalf of the end user, you must specify both the scopes enforced by the API and the scopes to be requested by the application.

 **Note:** Add the `user_attributes` scope to the client scopes to return user attributes from the ID token.

 **Note:** Under **Scopes**, you can select resources defined in any space if the application type is a `Web App`, `Native Mobile App`, or `Single Page Javascript App`. If the application type is a `Service-to-Service App`, you can only select resources defined within the space.

14. Under **Auto-Approved Scopes**, select which scopes should not require explicit authorization from the end user. Only scopes pertaining to company owned and managed applications should be selected. Do not select scopes that pertain to applications external to PCF.
15. Click **Create App**. The **Next Steps** page appears, describing the endpoints required for application integration. Refer to the [Application Integration](#) section below for more details.

## Register an External Application

1. Log into Apps Manager as a Space Developer.
2. Select the space where your service instance is located.
3. Under **Services**, click **Manage** next to your SSO service instance to launch the SSO dashboard.
4. Click **New App**.
5. Enter an **App Name**.
6. Under **Select an Application Type**, select `Web App`, `Native Mobile App`, `Service-to-Service App`, or `Single-Page JavaScript App`.
7. Under **Identity Providers**, select **Internal User Store** or the name of your external identity provider. Internal User Store is the default.

 **Note:** When registering an externally hosted application, a Space Developer can choose multiple internal and external identity providers. If the Space Developer selects multiple identity providers, users must select which provider to use when they sign in. This option is available for all application types except the Service-to-Service App.
8. If your Application Type is `Web App`, enter a whitelist of **Auth Redirect URIs** beneath **Redirect URIs**. The redirect query parameter specified on the OAuth request must match the URIs specified in this list. Otherwise, SSO rejects the request.
9. Enter the **Scopes** that this application can request. This field defaults to `openid`. Scopes are permissions that the application requests on the user's behalf. If this application is purely for authentication purposes, then the `openid` scope is sufficient. If the application makes API calls on behalf of the end user, you must specify both the scopes enforced by the API and the scopes to be requested by the application.

 **Note:** Under **Scopes**, you can select resources defined in any space if the application type is a `Web App`, `Native Mobile App`, or `Single Page Javascript App`. If the application type is a `Service-to-Service App`, you can only select resources defined within the space.

10. Under **Auto-Approved Scopes**, select which scopes should not require explicit authorization from the end user. Only scopes pertaining to company owned and managed applications should be selected. Do not select scopes that pertain to applications external to PCF.
11. Click **Create App**. The **Next Steps** page appears, describing the endpoints required for application integration. Refer to the [Application Integration](#) section below for more details.

## Application Integration

The SSO service is based on the OAuth protocol. As a result, you must make your applications OAuth-aware.

If you are using Java, refer to the [Single Sign-On Service Sample Applications](#). These are sample applications created using [Spring Boot](#) for all four application types (`Web App`, `Native Mobile App`, `Single Page Javascript App`, and `Service-to-Service App`). They use the SSO Service Connector, which auto-configures the application for OAuth. After binding the application to an SSO service instance, the user only has to restart the application for the new SSO

configuration to take effect.

For non-Java applications, the following information from the **Next Steps** page of the SSO dashboard must be supplied to the application after the SSO service bind:

- **App ID**, also known as OAuth Client ID.
- **App Secret**, also known as OAuth Client Secret.
- **OAuth Authorization URL**, the endpoint for client authorization.
- **OAuth Token URL**, the endpoint for token retrieval.

To validate the token, you must verify the following:

1. The token is a properly signed JSON Web Token with an appropriate public key. The key can be downloaded from the **Token Verification Key** endpoint specified on the **Next Steps** page.
2. The value of `aud` in the token matches your **App ID**.
3. The value of `iss` matches `https://AUTH-DOMAIN.uaa.YOUR-SYSTEM-DOMAIN/oauth/token`.
4. The expiry time of the token, `exp`, has not passed.

## Delete Application

To delete an application hosted on PCF, complete the following steps:

1. Log into Apps Manager as a Space Developer.
2. Select the space where your application is located.
3. Under **Applications**, click the name of your application.
4. On the Application Page, click **Delete App**.
5. On the popup, click **Delete** to confirm that you want to delete the application and its configurations from Apps Manager and the service dashboard.

To delete an external application not hosted on PCF, complete the following steps:

1. Log into Apps Manager as a Space Developer.
2. Select the space where your service instance is located.
3. Under **Services**, click **Manage** next to your SSO service instance to launch the SSO dashboard.
4. Click your application.
5. Click **Delete** at the bottom of the page .
6. On the popup, click **Delete App** to confirm that you want to delete the application and its configurations.

**Note:** Deleting an externally hosted application removes the application and its configurations from the SSO dashboard. However, it still exists on your hosted platform.

## Manage Resources

This topic describes how a Space Developer defines external resources required by an application bound to a Single Sign-On (SSO) service instance, as well as how an Administrator grants resource permissions.

 **Note:** Space Developers create resources within a space. Space Developers only see the resources created in the spaces they have access to and can only assign those to the applications in those spaces.

### Create or Edit Resources

If an application requires access to specific resources such as API endpoints, the Space Developer must define permissions for those resources in the SSO dashboard.

1. Log into Apps Manager as a Space Developer.
2. Select the space where your service instance is located.
3. Under **Services**, click **Manage** next to your SSO service instance to launch the SSO dashboard.
4. Click the **Resources** tab.
5. Click **New Resource**.
6. Enter a **Resource Name**.
7. Create **Permissions** that the OAuth client for your application needs to access from the resource server.
  - a. Enter one or more **Attributes** or **Actions** for each permission.
  - b. Enter a **Description** for each permission.
8. Click **Save Resource**. The administrator must create resource permissions so that users can access the resource. See the [Create or Edit Resource Permissions](#) section below for more details.

### Delete Resources

1. Log into Apps Manager as a Space Developer.
2. Click the **Manage** link under the SSO service instance to launch the service dashboard.
3. Click the **Resources** tab.
4. Click your resource.
5. Click **Delete** at the bottom of the page.
6. On the popup, click **Delete Resource** to delete the resource.

 **Note:** Deleting a resource removes it from the permission mappings and from the application. You must reconfigure the updated permissions in both areas.

### Create or Edit Resource Permissions

After a Space Developer defines resources required by an application, an administrator must grant access to those resources. SSO allows administrators to map groups of users from the identity provider to the resource permissions defined by the Space Developer.

1. Log into the SSO dashboard at `https://p-identity.YOUR-SYSTEM-DOMAIN` using your User Account and Authentication (UAA) administrator credentials. You can find these credentials in your Pivotal Elastic Runtime tile in Ops Manager under the Credentials tab.
2. Click the plan name and select **Manage Identity Providers** from the dropdown menu.

3. Click **Resource Permissions** for the identity provider that you want to define permissions for.
4. Click **New Permissions Mapping**.
5. Enter a **Group Name**.
6. Click **Select Permissions** to choose the permissions that users in the group should have access to.
7. Click **Save Permissions Mapping**.

 **Note:** Groups with unsupported characters in Permission Mappings are not editable.

## Delete Resource Permissions

1. Log into the SSO dashboard at <https://p-identity.YOUR-SYSTEM-DOMAIN> using your User Account and Authentication (UAA) administrator credentials. You can find these credentials in your Pivotal Elastic Runtime tile in Ops Manager under the Credentials tab.
2. Click the plan name and select **Manage Identity Providers** from the dropdown menu.
3. Click **Resource Permissions** for the identity provider that you want to define permissions for.
4. Click the group name of the resource permission you want to delete.
5. Click **Delete** at the bottom of the page.
6. On the popup, click **Delete Permissions Mapping** to delete the resource.

 **Note:** Groups with unsupported characters in Permission Mappings are not editable.

## Active Directory Federation Services Integration Guide Overview

Active Directory Federation Services (AD FS) is a standards-based service that securely shares identity information between applications. This documentation describes how to configure a single sign-on partnership between AD FS as the Identity Provider (IdP) and the Single Sign-On Service (SSO) for Pivotal Cloud Foundry as the Service Provider (SP).

SSO supports service provider-initiated authentication flow and single logout. It does not support identity provider-initiated authentication flow. All SSO communication takes place over SSL.

## Prerequisites

To integrate AD FS with Pivotal Cloud Foundry (PCF), you need the following:

### Pivotal

- PCF, version 1.7.0 or later
- Single Sign-On, version 1.1.0 or later

### Active Directory Federation Services

- Active Directory Federation Services subscription
- A user with Administrative privileges

 **Note:** To configure SAML, you must have the Single Sign-On service broker installed on your PCF deployment. You need to create a plan, grant any plan administrators, and specify any organizations this plan should be the authentication authority for. For help configuring plans, see the [Manage Service Plans](#) topic.

## Active Directory Federation Services Integration Guide

### Configuring AD FS with SSO

Complete both steps below to integrate your deployment with AD FS and SSO.

1. [Configure Active Directory Federation Services as an Identity Provider](#)
2. [Configure a Single Sign-On Service Provider](#)

### Testing and Troubleshooting

- [Testing](#)
- [Troubleshooting](#)

## Configure Active Directory Federation Services as an Identity Provider

This topic describes how to set up Active Directory Federation Services (AD FS) as your identity provider by configuring SAML integration in both Pivotal Cloud Foundry (PCF) and AD FS.

### Set up SAML in PCF

1. Log in to the Single Sign-On (SSO) dashboard at <https://p-identity.YOUR-SYSTEM-DOMAIN> as a Plan Administrator.
2. Select your plan and click **Manage Identity Providers** on the dropdown menu.

The screenshot shows the 'Plans' section of the PCF SSO dashboard. A dropdown menu for 'ADFS PCF SSO' is open, showing 'Edit Plan' and 'Manage Identity Providers'. The 'Manage Identity Providers' option is highlighted with a red box.

3. Click **Configure SAML Service Provider**.

The screenshot shows the 'Identity Providers' list. A button labeled 'Configure SAML Service Provider' is highlighted with a red box.

Name	Type	Actions
Internal User Store	Internal User Store	<a href="#">Resource Permissions</a> <a href="#">Group Whitelist</a>
ADFS PCF SSO	SAML	<a href="#">Resource Permissions</a> <a href="#">Group Whitelist</a>

4. (Optional) Select **Perform signed authentication requests** to enforce SSO private key signature and identity provider validation.

The screenshot shows the 'Configure SAML Service Provider' settings page. A checkbox for 'Perform signed authentication requests' is checked and highlighted with a red box. A 'Save' button is also highlighted with a red box.

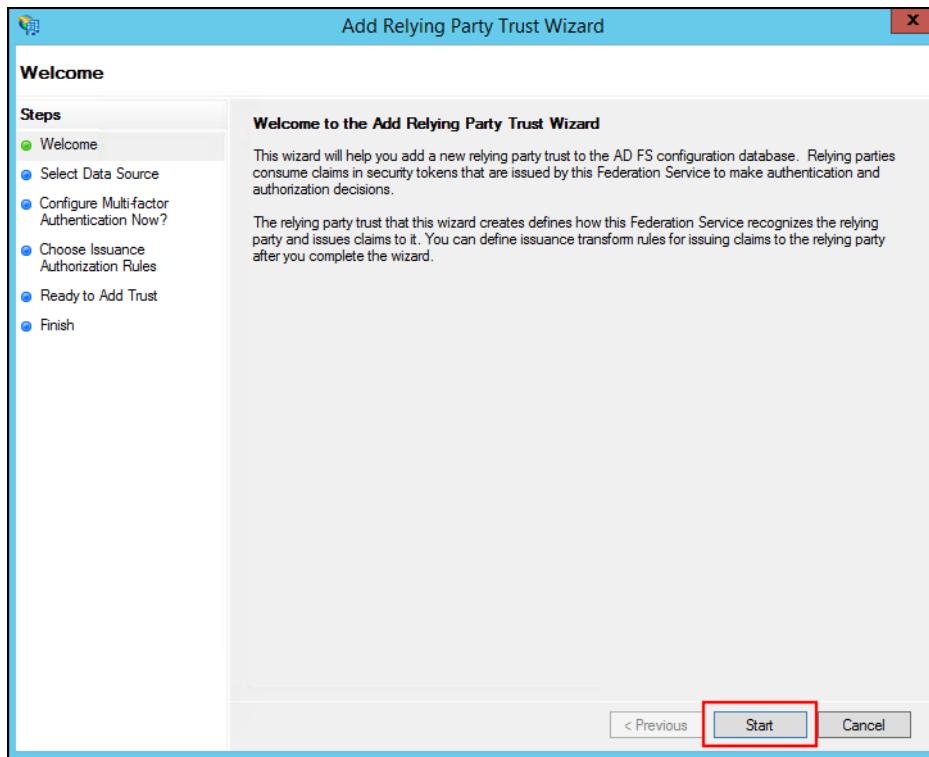
5. (Optional) Select **Require signed assertions** to validate the origin of signed responses.

6. Click **Download Metadata** to download the service provider metadata.

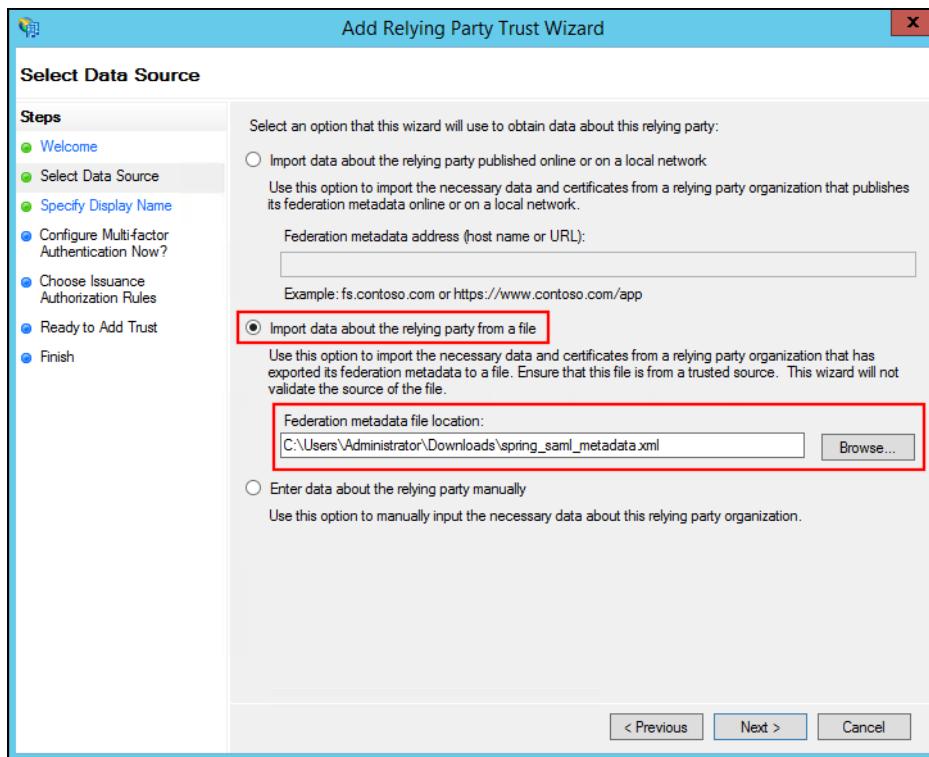
7. Click **Save**.

### Set up SAML in Active Directory Federation Services

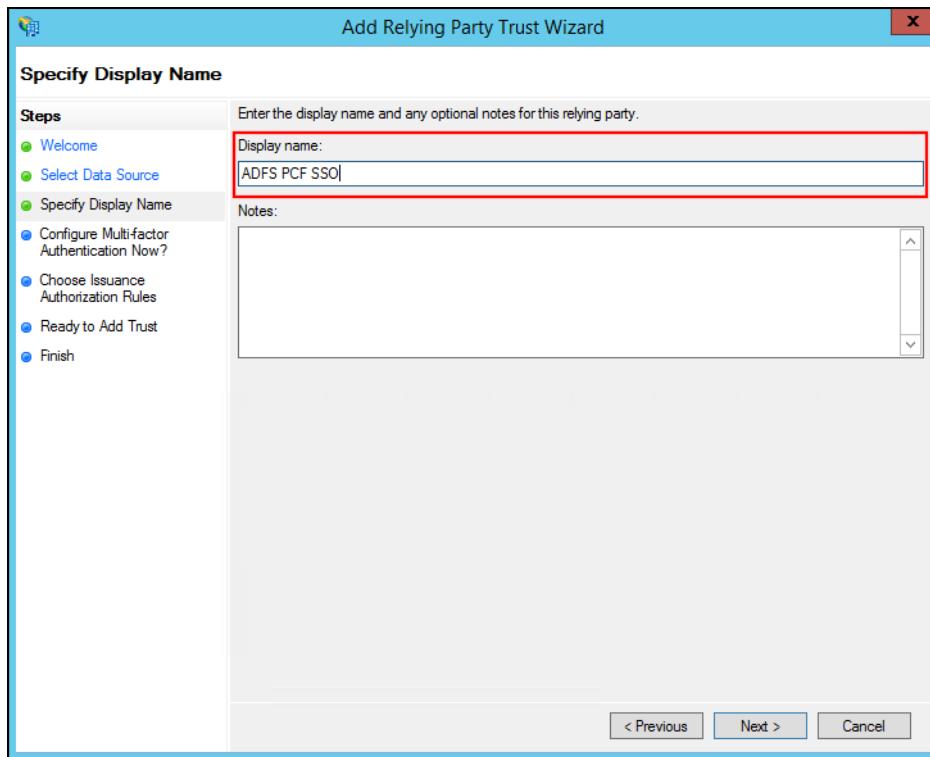
1. Open the AD FS Management console.
2. Click **Add Relying Party Trust...** in the Actions pane.
3. On the Welcome step, click **Start**.



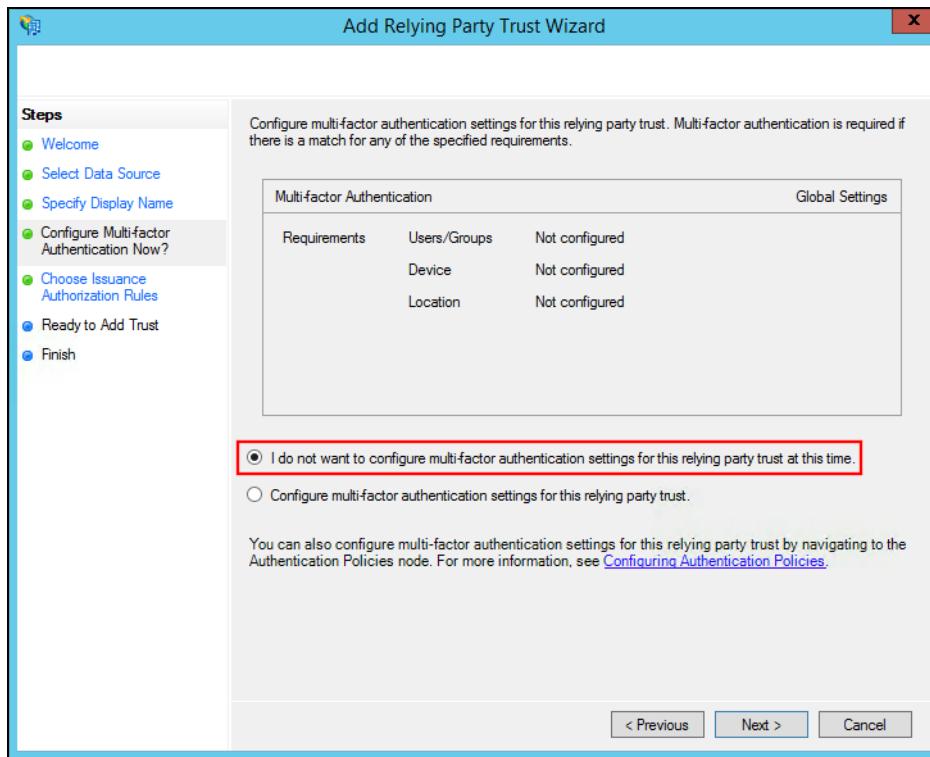
4. Select Import data about the relying party from a file, enter the path to the downloaded service provider metadata, and click Next.



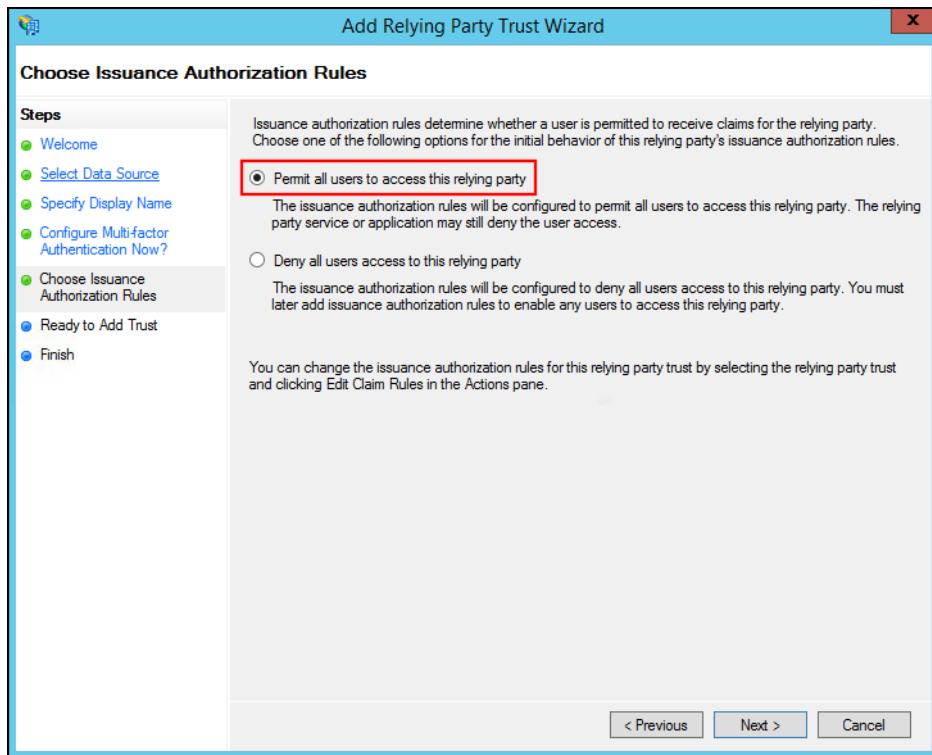
5. Enter a name for Display name and click Next.



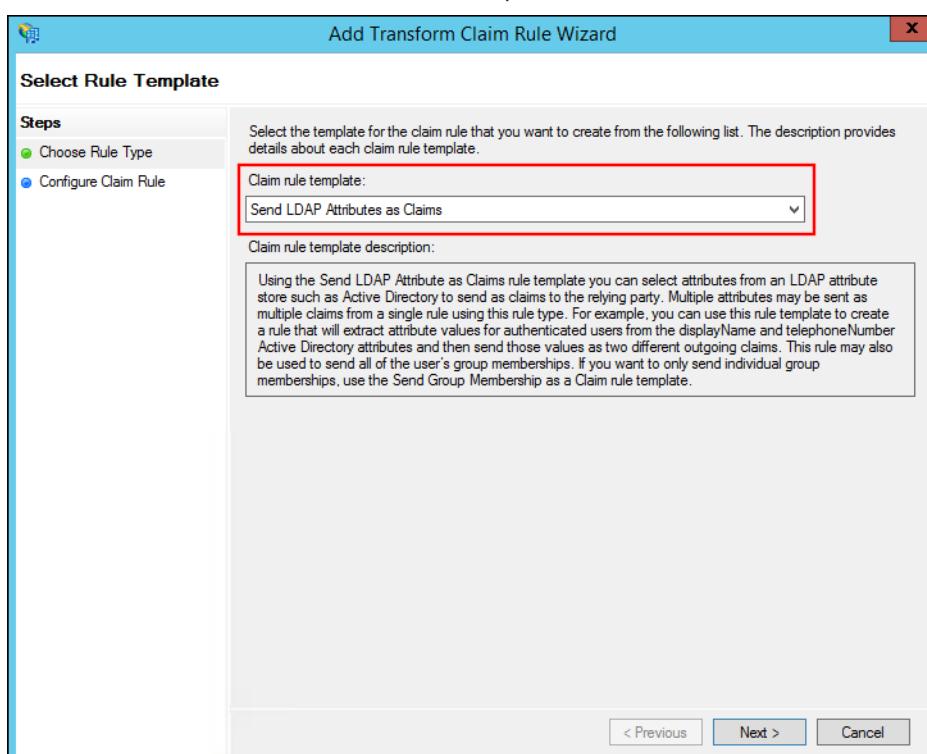
- Leave the default multi-factor authentication selection and click Next.



- Select Permit all users to access this relying party and click Next.

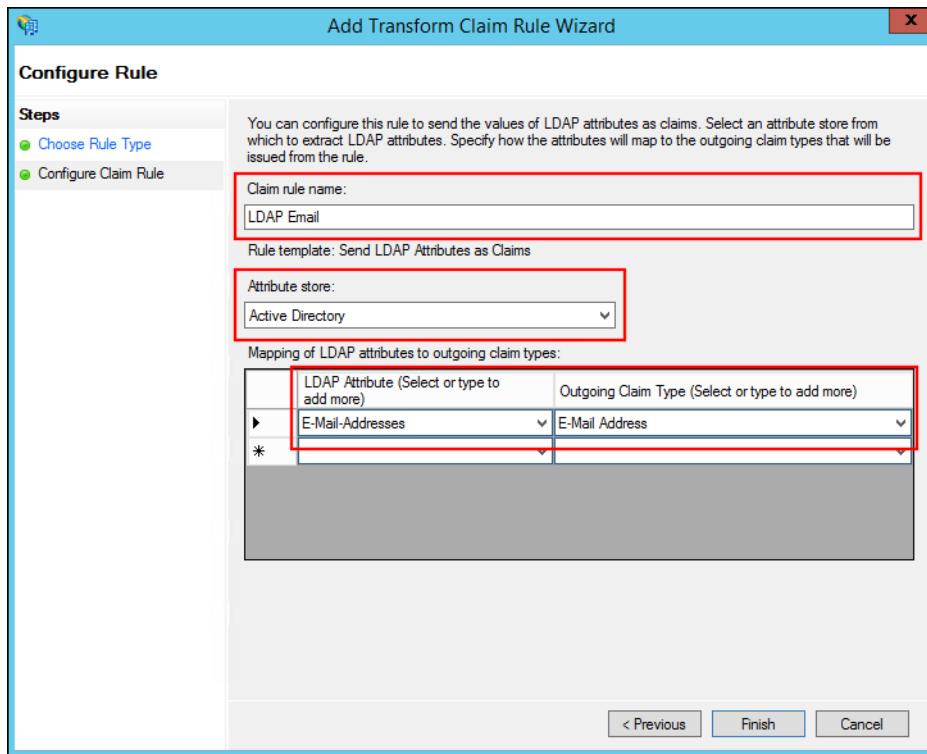


8. Review your settings and click **Next**.
9. Click **Close** to finish the wizard.
10. The claim rule editor should open by default. If it does not, select your Relying Party Trust and click **Edit Claim Rules...** in the Actions pane.
11. Create two claim rules by following these steps:
  - a. Click **Add Rule**.
  - b. Select **Send LDAP Attributes as Claims** for **Claim rule template** and click **Next**.



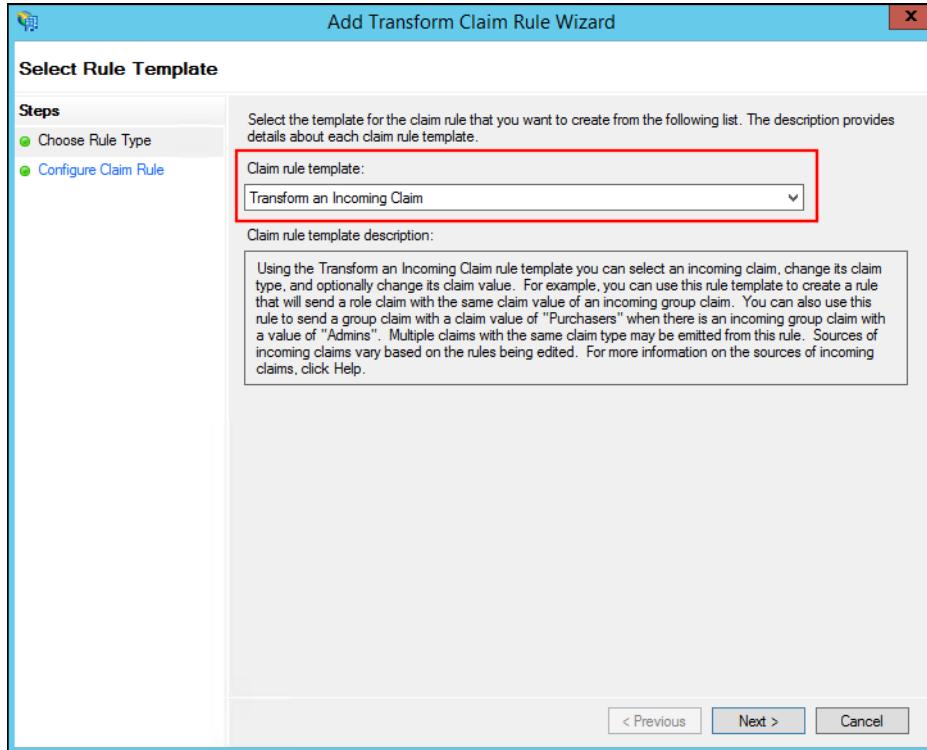
- c. Enter a **Claim rule name**.
- d. Select **Active Directory** for **Attribute store**.
- e. Select **E-Mail-Addresses** for **LDAP Attribute** and select **E-mail Address** for **Outgoing Claim Type**.

f. Click Finish.



g. Click Add Rule.

h. Select Transform an Incoming Claim for Claim rule template and click Next.



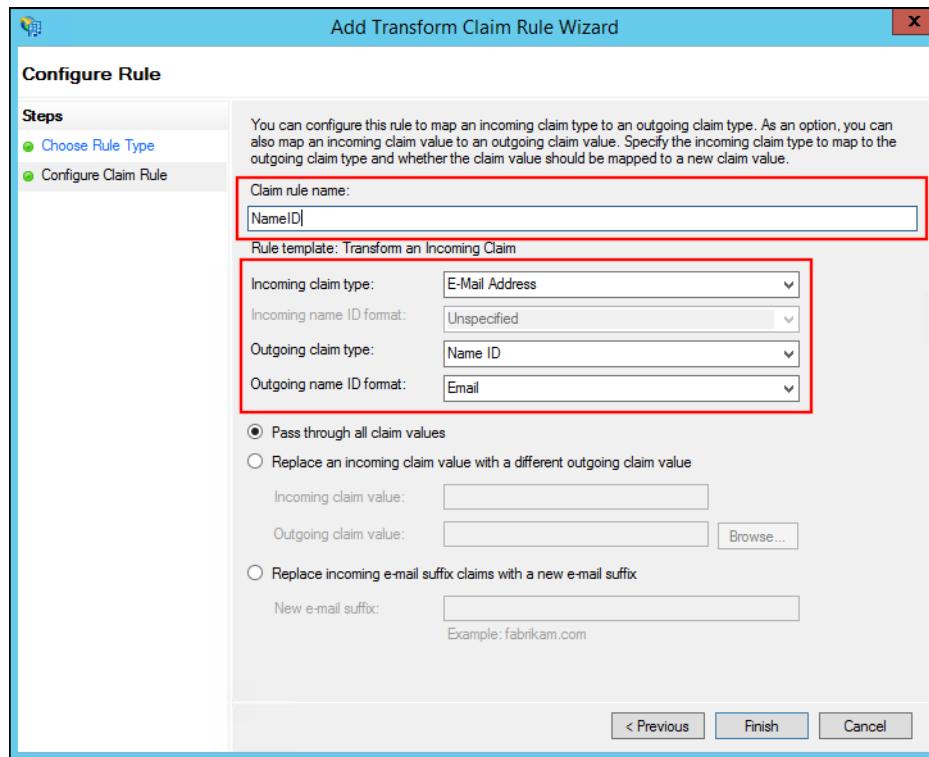
i. Enter a Claim rule name.

j. Select E-Mail Address for Incoming claim type.

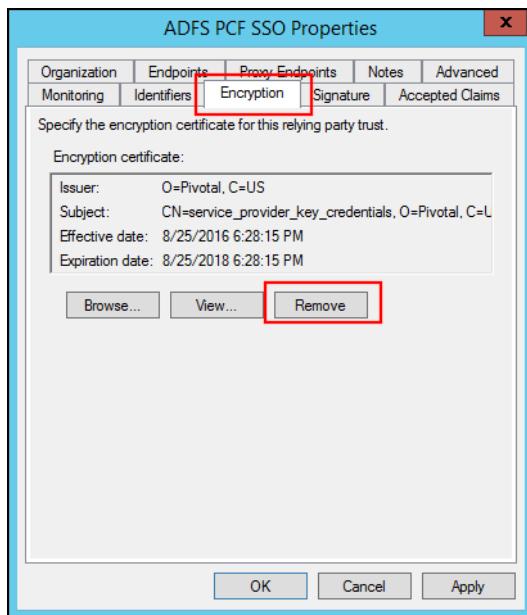
k. Select Name ID for Outgoing claim type

l. Select Email for Outgoing name ID format.

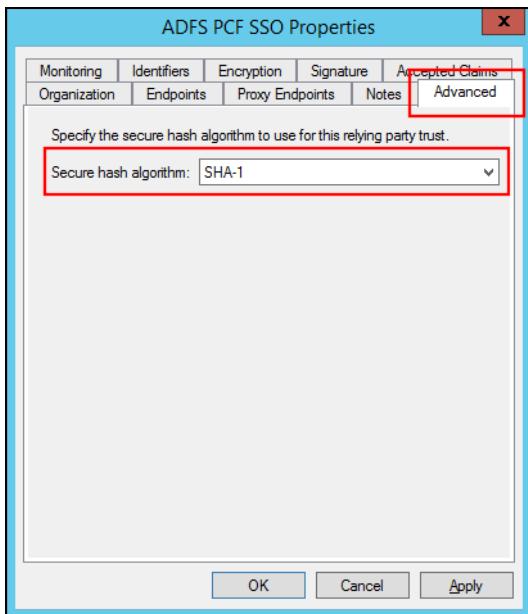
m. Click Finish.



12. Double-click on the new Relying Party Trust to open the properties.
13. Select the **Encryption** tab and click **Remove** to remove the encryption certificate.



14. Select the **Advanced** tab and select **SHA-1** for the **Secure hash algorithm**.



15. (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
```

16. (Optional) To specify any application or group attributes that you want to map to users in the ID token, click **Edit Claim Rules...** and configure **Send LDAP Attributes as Claims**.

## Configure a Single Sign-On Service Provider

This topic describes how to add an external identity provider to your Pivotal Single Sign-On (SSO) service plan.

### Download Identity Provider Metadata

1. Download the metadata from your Active Directory Federation Services server at the following URL:

`https://YOUR-ADFS-HOSTNAME/federationmetadata/2007-06/federationmetadata.xml`

### Setting up SAML

1. Log in to the SSO dashboard at `https://p-identity.YOUR-SYSTEM-DOMAIN` as a Plan Administrator.
2. Select your plan and click **Manage Identity Providers** on the dropdown menu.

The screenshot shows a 'Plans' section with one item. Below it is a table with two columns: 'Name' and 'Sign In Header'. The first row contains 'ADFS PCF SSO' and 'example'. Underneath the table, there are two buttons: 'Edit Plan' and 'Manage Identity Providers', with 'Manage Identity Providers' highlighted by a red box.

3. Click **New Identity Provider** to create a new identity provider.

The screenshot shows the 'New Identity Provider' form. It includes fields for 'Identity Provider Name\*', 'Identity Provider Description', 'Identity Provider Type\*', and sections for 'Identity Provider Metadata' and 'Advanced SAML Settings'. At the bottom right are 'Cancel' and 'Create Identity Provider' buttons, with 'Create Identity Provider' highlighted by a blue box.

**Identity Provider Name\***  
This name will show as a link on the login page

**Identity Provider Description**  
Allows  to authenticate.

**Identity Provider Type\***  
SAML

**Identity Provider Metadata**

**Identity Provider Metadata URL\***

**Fetch Metadata**

▶ SAML File Metadata (optional)

**Advanced SAML Settings**

▶ Attribute mappings (optional)

4. To create a new identity provider, perform the following steps:

- a. Enter an identity provider name in **Identity Provider Name**.

- b. (Optional) Enter a description in **Identity Provider Description**.
  - c. Click **SAML File Metadata (optional)**, then click **Upload Identity Provider Metadata** to upload your metadata XML.
  - d. (Optional) Under **Advanced SAML Settings**, click **Attribute Mappings** to enter the mappings.
5. Click **Create Identity Provider**.
  6. Click **Resource Permissions**.
  7. Click **New Permissions Mapping** and perform the following steps:
    - a. Enter a **Group Name**.
    - b. For **Select Permissions**, select the permissions to grant to the members of the group from the external identity provider.
  8. Navigate to the identity provider list.
  9. Click **Group Whitelist** and enter the group names from the external identity provider that should be propagated in the ID token.

## Testing

This topic describes how an administrator can test the connection between SSO and Active Directory Federation Services (AD FS). An administrator can test both service provider and identity provider connections.

### Test Your Service Provider Connection

1. Log in to Apps Manager at <https://apps.YOUR-SYSTEM-DOMAIN> and navigate to the organization and space where your application is located.
2. Under **Services**, locate the service instance of the Single Sign-On (SSO) plan bound to your application. Click on the service instance and click **Manage**.

The screenshot shows the Apps Manager interface. At the top, there are two tabs: "Overview" (selected) and "Settings". Below these are two main sections: "Apps" and "Services".

**Apps:**

NAME	INSTANCES	MEMORY	LAST PUSH	ROUTE
authcode-sample	1	512MB	4 days ago	<a href="http://authcode-sample.id-service.cf-ap...">http://authcode-sample.id-service.cf-ap...</a> >

**Services:**

SERVICE	NAME	BOUND APPS	PLAN
 Pivotal Single Sign-On	SI	1	free - (MONTHLY) >

The screenshot shows the "Pivotal Single Sign-On" service instance management page. At the top, it displays the SERVICE (Pivotal Single Sign-On), INSTANCE NAME (SI), and SERVICE PLAN (ADFS PCF SSO). Below this are three buttons: "Manage" (highlighted with a red box), "Docs", and "Support".

Below the service details, there are three tabs: "App Binding (1)" (selected), "Plan", and "Settings".

**App Binding (1):**

Bound Apps	Edit Bindings
authcode-sample	<a href="#">Edit Bindings</a>

3. Under the **Apps** tab, click your application.

The screenshot shows the Pivotal Apps Manager interface. On the left, there's a button labeled 'NEW APP'. To its right, the application 'authcode-sample' is listed. It is categorized as a 'Web App' and uses an 'Internal Identity Provider'. The provider listed is 'ADFS PCF SSO'. A note indicates the app was 'updated 4 days ago'.

4. Under Identity Providers, select the AD FS identity provider.

The screenshot shows the configuration page for the 'authcode-sample' application. In the 'Identity Providers' section, two options are listed: 'Internal User Store' and 'ADFS PCF SSO'. The 'ADFS PCF SSO' option is highlighted with a red box. Below this section, there's a 'Redirect URIs' section where the URL 'https://authcode-sample.id-service.cf-app.com' is entered. The 'Authorization' section includes 'Scopes' (todo, todo.read, todo.write) and 'System Provided' (openid). Under 'Select Scopes', there's a 'Auto-Approved Scopes' section with a dropdown menu set to 'None selected'. At the bottom right, there are 'Cancel' and 'Save Config' buttons.

5. Return to Apps Manager and click on the URL below your application to be redirected to the identity provider to authenticate.

Overview    Settings

Apps

NAME	INSTANCES	MEMORY	LAST PUSH	ROUTE
authcode-sample	1	512MB	4 days ago	<a href="http://authcode-sample.id-service.cf-app.net">http://authcode-sample.id-service.cf-app... &gt;</a>

6. Click the link.

Authcode sample

What do you want to do?

- [Log in via Auth Code Grant Type](#)

7. On the identity provider sign-in page, enter your credentials and click **Sign in**.

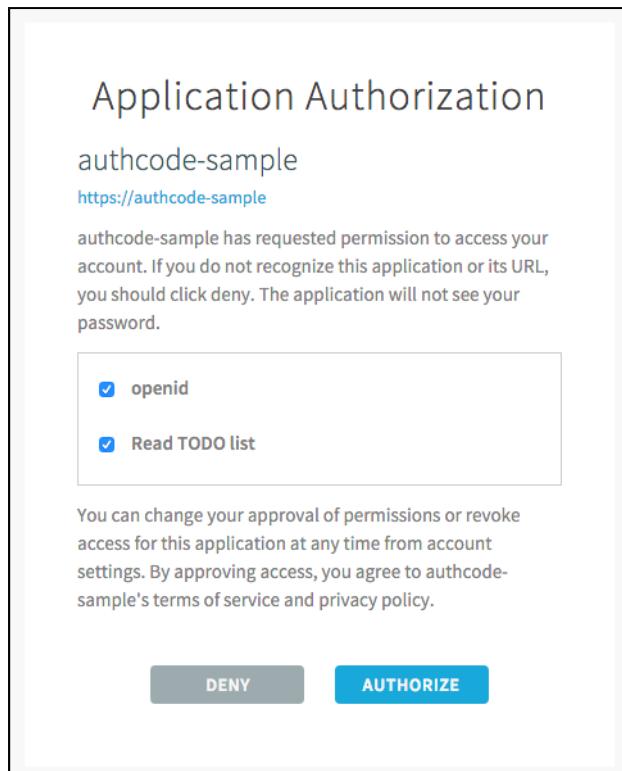
ADFS Single Sign-On

Sign in with your organizational account

**Sign in**

8. The application asks for authorization to the necessary scopes. Click **Authorize**.



9. The access token and ID token displays.

## Authcode sample

You've used the authcode flow! Here's the result of calling /userinfo:

```
{
  "user_id" : "5651953a-c864-4073-86b3-4fa97b45a0d1",
  "user_name" : "example@pivotal.io",
  "given_name" : "Example",
  "family_name" : "Example",
  "email" : "example@pivotal.io",
  "name" : "Example Example"
}
```

This is the Access Token that was used:

```
{
  "jti" : "bbe64fd09cbf4ed4a4fdf17c3ea8af04",
  "sub" : "5651953a-c864-4073-86b3-4fa97b45a0d1",
  "scope" : [ "todo.read", "openid", "todo.write" ],
  "client_id" : "bbf58e64-14f1-46b4-9fd5-ca267376ec4c",
  "cid" : "bbf58e64-14f1-46b4-9fd5-ca267376ec4c",
  "azp" : "bbf58e64-14f1-46b4-9fd5-ca267376ec4c",
  "grant_type" : "authorization_code",
  "user_id" : "5651953a-c864-4073-86b3-4fa97b45a0d1",
  "origin" : "ADFS PCF SSO",
  "user_name" : "example@pivotal.io",
  "email" : "example@pivotal.io",
  "auth_time" : 1472753888,
  "rev_sig" : "6f09b81d",
  "iat" : 1472753930,
  "exp" : 1472797130,
  "iss" : "https://example.uaa/oauth/token",
  "zid" : "2852ad03-e828-4200-9d7a-e04af30fe5bd",
  "aud" : [ "todo", "openid", "bbf58e64-14f1-46b4-9fd5-ca267376ec4c" ]
}
```

This is the ID Token:

```
{
  "sub" : "5651953a-c864-4073-86b3-4fa97b45a0d1",
  "user_name" : "example@pivotal.io",
  "origin" : "ADFS PCF SSO",
  "iss" : "https://example.uaa/oauth/token",
  "user_attributes" : { },
  "client_id" : "bbf58e64-14f1-46b4-9fd5-ca267376ec4c",
  "aud" : [ "bbf58e64-14f1-46b4-9fd5-ca267376ec4c" ],
  "zid" : "2852ad03-e828-4200-9d7a-e04af30fe5bd",
  "grant_type" : "authorization_code",
  "user_id" : "5651953a-c864-4073-86b3-4fa97b45a0d1",
  "azp" : "bbf58e64-14f1-46b4-9fd5-ca267376ec4c",
  "scope" : [ "openid" ],
  "auth_time" : 1472753888,
  "exp" : 1472797130,
  "iat" : 1472753930,
  "jti" : "bbe64fd09cbf4ed4a4fdf17c3ea8af04",
  "email" : "example@pivotal.io",
  "rev_sig" : "6f09b81d",
  "cid" : "bbf58e64-14f1-46b4-9fd5-ca267376ec4c"
}
```

## What do you want to do?

- [TODO List \(You need to configure the Resource Server sample app before using this\)](#)
- [See your account profile \(so you can de-authorize this client\)](#)
- [Log out](#)

## Test Your Identity Provider Connection

 Note: SSO does not support identity provider-initiated flow into applications, but it does redirect the user to the User Account and Authentication (UAA) page to select applications assigned to the user.

- Sign in to AD FS.

## ADFS Single Sign-On

Sign in with your organizational account

**Sign in**

2. Navigate to your application and click it.
3. You are redirected to the page that lists applications you have access to.

The screenshot shows a web application interface. At the top left is a user profile icon with the letter 'E' and the email 'example@pivotal.io'. To its right is a 'Sign out' link. On the far right is the 'Pivotal' logo. Below the header is a navigation bar with tabs: 'Apps' (which is underlined in blue), 'Profile', 'Security', 'Approvals', and 'Notifications'. The main content area displays three application cards, each featuring a teal circular icon with a white 'P' and the text 'Application 1' or 'Application 2'. At the bottom of the page is a footer with the text '©2016 Pivotal Software, Inc. All Rights Reserved. [Privacy Policy](#) — [Terms of Service](#)'.

## Test Your Single Sign-Off

Test single sign-off to ensure that when users log out of the application, they are logged out of AD FS as well.

1. Sign in to the sample application. Information about the access and ID token displays, as well as the "What do you want to do?" section.
2. Under "What do you want to do?", click **Log out**.

**What do you want to do?**

- [TODO List \(You need to configure the Resource Server sample app before using this\)](#)
- [See your account profile \(so you can de-authorize this client\)](#)
- [Log out](#)

3. You are logged out and redirected to the AD FS login page.

## ADFS Single Sign-On

Sign in with your organizational account

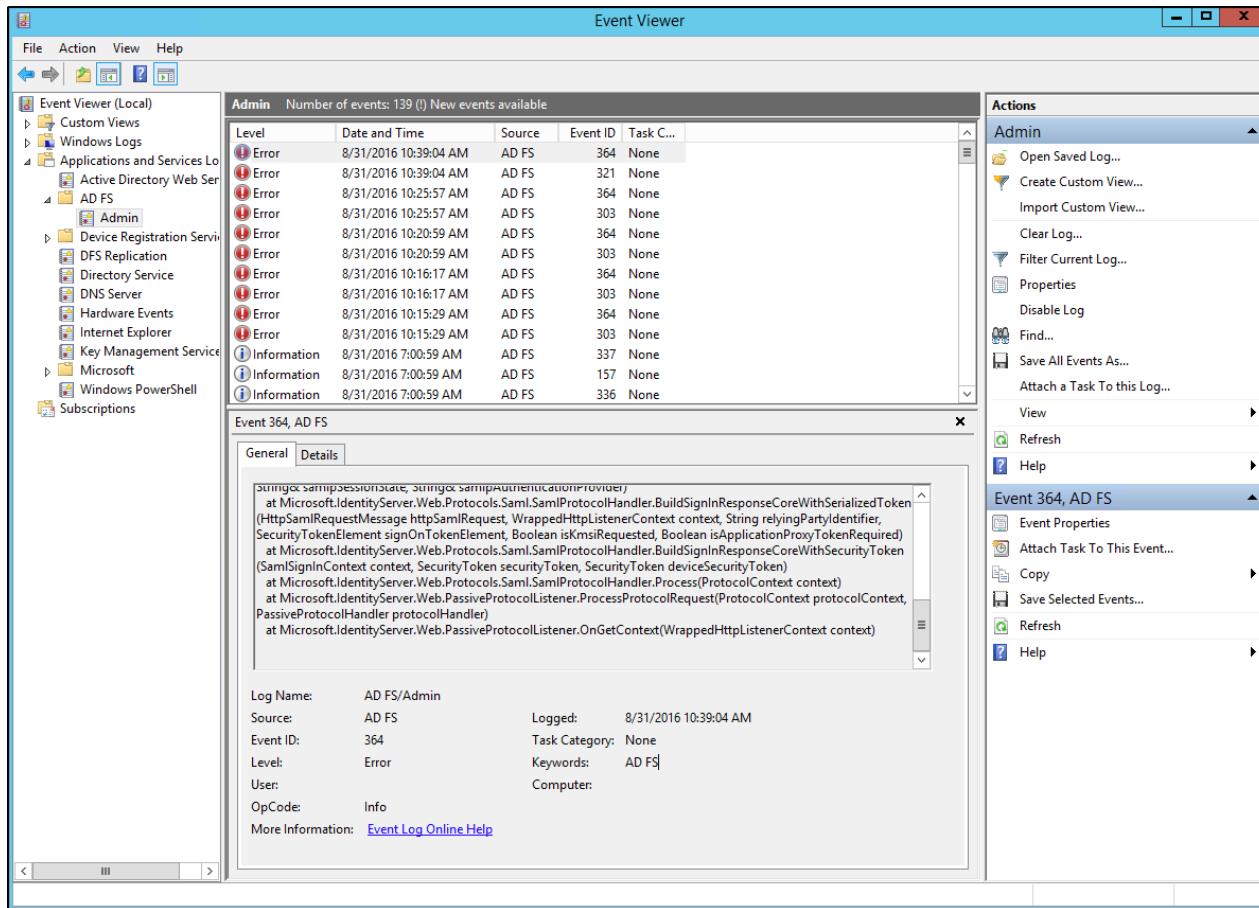
## Troubleshooting

This topic describes how to resolve errors that arise when configuring a single sign-on partnership between Active Directory Federation Services and Pivotal Single Sign-On (SSO).

### Event Viewer

1. Navigate to Administrative Tools.

2. Launch Event Viewer.



3. Examine any errors and its details to diagnose problems.

## Azure Active Directory Integration Guide Overview

Azure Active Directory (Azure AD) is Microsoft's multi-tenant cloud based directory and identity management service. This documentation describes how to configure a single sign-on partnership between Azure AD as the Identity Provider (IdP) and the Single Sign-On Service (SSO) for Pivotal Cloud Foundry® as the Service Provider (SP).

SSO supports service provider-initiated authentication flow and single logout. It does not support identity provider-initiated authentication flow. All SSO communication takes place over SSL.

## Prerequisites

To integrate Azure AD with Pivotal Cloud Foundry® (PCF), you need:

### Pivotal

- PCF, version 1.7.0 or later.
- Single Sign-On, version 1.1.0 or later.

### Azure Active Directory

- Azure Active Directory subscription.
- A user with admin privileges.

 **Note:** To configure SAML, you must have the Single Sign-On service broker installed on your PCF deployment. You need to create a plan, grant any plan administrators, and specify any organizations this plan should be the authentication authority for. For help configuring plans, see the [Manage Service Plans](#) topic.

## Azure AD Integration Guide

### Configuring Azure AD with SSO

Complete both steps below to integrate your deployment with Azure AD and SSO.

1. [Configure Azure AD as an Identity Provider](#)
2. [Configure a Single Sign-On Service Provider](#)

### Testing and Troubleshooting

- [Testing](#)
- [Troubleshooting](#)

## Configure Azure Active Directory as an Identity Provider

This topic describes how to set up Azure Active Directory (AD) as your identity provider by configuring SAML integration in both Pivotal Cloud Foundry® (PCF) and Azure AD.

### Set up SAML in PCF

1. Log into the Single Sign-On (SSO) dashboard at <https://p-identity.YOUR-SYSTEM-DOMAIN> as a Plan Administrator.
2. Select your plan and click **Manage Identity Providers** on the dropdown menu.

The screenshot shows the 'Plans' section of the PCF SSO dashboard. A single plan named 'Azure PCF SSO' is listed. Below the plan name, there are two buttons: 'Edit Plan' and 'Manage Identity Providers'. The 'Manage Identity Providers' button is highlighted with a red box.

3. Click **Configure SAML Service Provider**.

The screenshot shows the 'Identity Providers' page under the 'Azure PCF SSO' plan. It lists two providers: 'Internal User Store' (Type: Internal User Store) and 'Azure PCF SSO' (Type: SAML). Below the table, there are 'Resource Permissions' and 'Group Whitelist' links. The 'Configure SAML Service Provider' button is highlighted with a red box.

4. (Optional) Select **Perform signed authentication requests** to enforce SSO private key signature and identity provider validation.

The screenshot shows the 'Configure SAML Service Provider' dialog. It contains two checkboxes: 'Perform signed authentication requests' (checked) and 'Require signed assertions' (unchecked). At the bottom, there is a 'Save' button highlighted with a red box.

5. (Optional) Select **Require signed assertions** to validate the origin of signed responses.

6. Click **Download Metadata** to download the service provider metadata.

7. Click **Save**.

### Set up SAML in Azure Active Directory

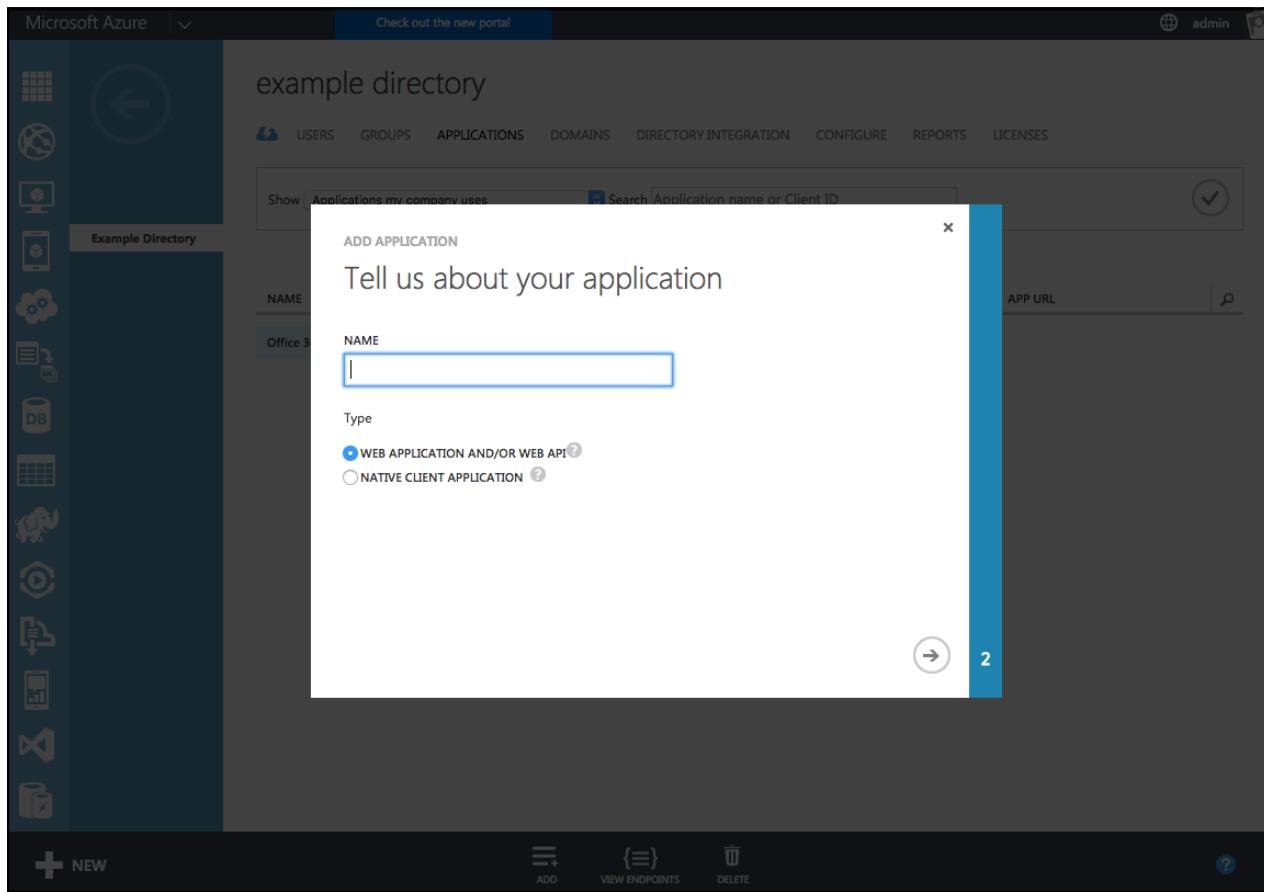
1. Sign into Azure AD at <https://manage.windowsazure.com> as an administrator.
2. Navigate to the applications dashboard by clicking on your directory and the Applications tab.
3. Click the **Add** button to add a new application.

The screenshot shows the Microsoft Azure Active Directory portal. The top navigation bar includes 'Microsoft Azure' with a dropdown, a link to 'Check out the new portal', and a user 'admin'. The main title is 'example directory'. Below the title, there are tabs for 'USERS', 'GROUPS', 'APPLICATIONS', 'DOMAINS', 'DIRECTORY INTEGRATION', 'CONFIGURE', 'REPORTS', and 'LICENSES'. A search bar at the top right allows filtering by 'Applications my company uses' or 'Application name or Client ID'. The main content area displays a table with one row for 'Office 365 Management APIs', which is a 'Web application' published by 'Microsoft Corporation'. At the bottom, there is a dark navigation bar with icons for 'NEW', 'ADD' (which is highlighted with a red box), 'VIEW ENDPOINTS', and 'DELETE'.

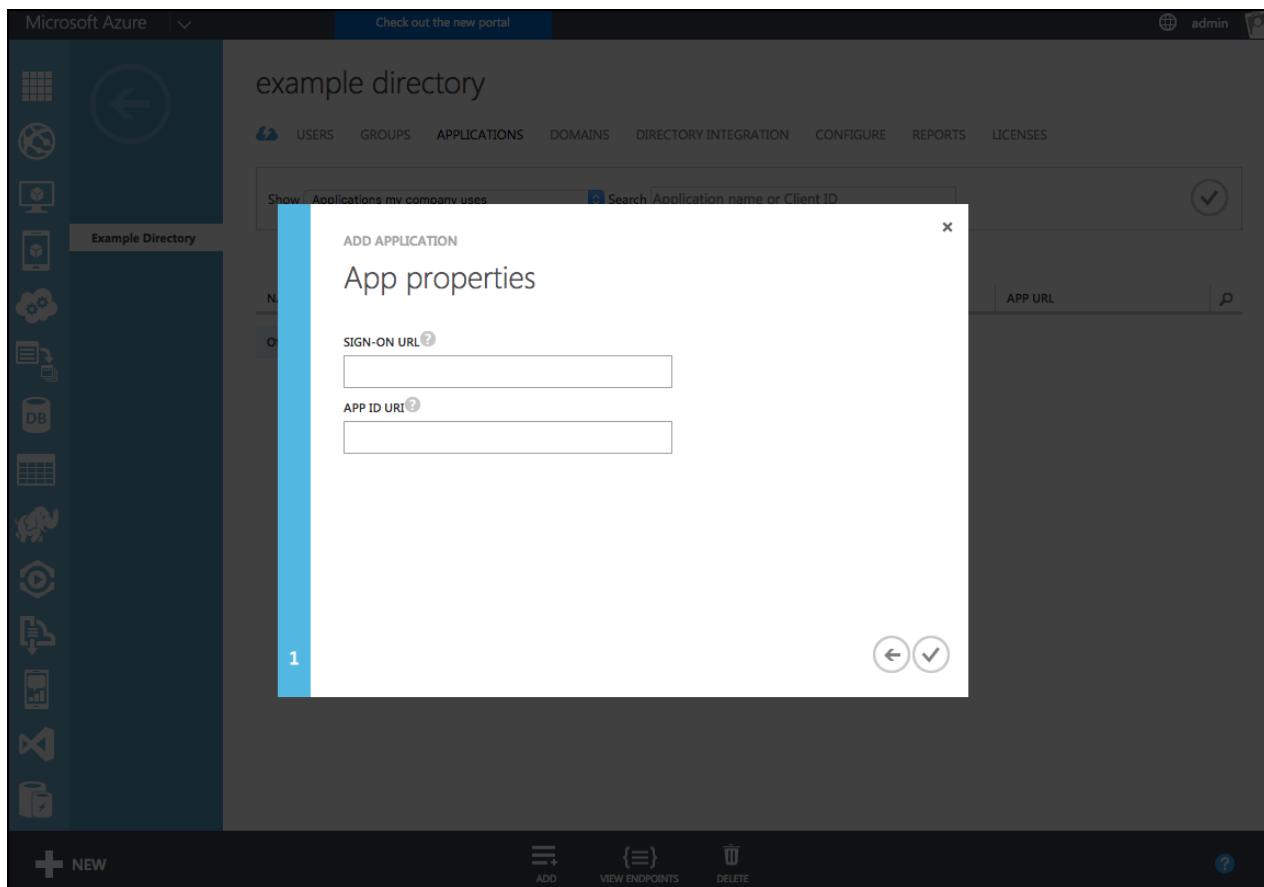
4. Select Add an application my organization is developing

The screenshot shows the Microsoft Azure Active Directory portal with a modal dialog box overlaid. The dialog has a title 'What do you want to do?' and two options: 'Add an application my organization is developing' and 'Add an application from the gallery'. The first option is highlighted with a red box. The background shows the same 'example directory' Applications page as the previous screenshot, with the 'ADD' button also highlighted with a red box.

5. Enter the Name and Type for the application.



6. Enter the **Sign-On URL** and **App ID URI** for the application.



7. Click the application and configure the following properties:

- a. Enter the application **Name**.
- b. Enter the **AssertionConsumerService Location URL** from your downloaded service provider metadata into **Sign-On URL**. For example, `https://AUTH-DOMAIN/saml/SSO/alias/AUTH-DOMAIN`.
- c. Configure the application **Logo**, **Application is Multi-Tenant** and **User Assignment Required to Access App** properties.
- d. Enter your **Auth Domain URL** into **App ID URI**.
- e. Enter the **AssertionConsumerService Location URL** from your downloaded service provider metadata into **Reply URL**.

Microsoft Azure | v Check out the new portal admin

**example app**

DASHBOARD USERS CONFIGURE OWNERS

**Example App** Office 365 Manage...

**properties**

NAME Example App

SIGN-ON URL <http://example.login.id-service.cf-app.com/saml/SSO/alias/example.login>

LOGO 

APPLICATION IS MULTI-TENANT YES NO

CLIENT ID e06bacb9-c697-4ab8-a231-907db9a647d9

USER ASSIGNMENT REQUIRED TO ACCESS APP YES NO

**keys**

Select dur... VALID FROM EXPIRES ON THE KEY VALUE WILL BE DISPLAYED AFTER YOU SAVE IT.

**single sign-on**

APP ID URI <http://example.login.id-service.cf-app.com>

REPLY URL <https://example.login.id-service.cf-app.com/saml/SSO/alias/ex> (ENTER A REPLY URL)

**permissions to other applications**

Windows Azure Active Directory Application Permissions: 1 Delegated Permissions: 5

Add application

**Actions**

NEW VIEW ENDPOINTS UPLOAD LOGO MANAGE DELETE SAVE DISCARD

- Click the Save button.

9. Click **View Endpoints** and download the **Federation Metadata Document**.

The screenshot shows the Microsoft Azure portal interface. On the left is a sidebar with various icons. The main area shows an application named "example app". Under "properties", there's a "SIGN-ON URL" field containing "https://example.login.id-service.cf-app.com/saml/SSO/alias/example.login". A modal window titled "App Endpoints" is overlaid on the page. This modal lists several endpoints:

- FEDERATION METADATA DOCUMENT: <https://login.microsoftonline.com/025c050a-9f19-4074-882f-4b52287>
- WS-FEDERATION SIGN-ON ENDPOINT: <https://login.microsoftonline.com/025c050a-9f19-4074-882f-4b52287>
- SAML-P SIGN-ON ENDPOINT: <https://login.microsoftonline.com/025c050a-9f19-4074-882f-4b52287>
- SAML-P SIGN-OUT ENDPOINT: <https://login.microsoftonline.com/025c050a-9f19-4074-882f-4b52287>
- MICROSOFT AZURE AD GRAPH API ENDPOINT: <https://graph.windows.net/025c050a-9f19-4074-882f-4b522871e8c3>
- OAUTH 2.0 TOKEN ENDPOINT: <https://login.microsoftonline.com/025c050a-9f19-4074-882f-4b52287>
- OAUTH 2.0 AUTHORIZATION ENDPOINT: <https://login.microsoftonline.com/025c050a-9f19-4074-882f-4b52287>

The "FEDERATION METADATA DOCUMENT" link is highlighted with a red box.

## Set up Claims Mapping

1. To enable user attribute mappings, grant the application the following permissions to Windows Azure Active Directory:

- Read directory data.
- Read all groups.
- Read all users' full profiles or Read all users' basic profiles.

permissions to other applications

Windows Azure Active Directory

Application Permissions: 1	Delegated Permissions: 5
<input checked="" type="checkbox"/> Read directory data	
<input type="checkbox"/> Read and write domains	
<input type="checkbox"/> Read and write directory data	
<input type="checkbox"/> Read and write devices	

Add application

NEW VIEW ENDPOINTS UPLOAD LOGO MANAGE MANIFEST DELETE SAVE DISCARD

2. To pass group membership claims to the application, perform the following steps:

- a. Click **Manage Manifest**.
- b. Click **Download Manifest** followed by **Download manifest**.
- c. Locate `groupMembershipClaims` and set the value to either:
  - `SecurityGroup` - Groups claim will contain identifiers of all security groups of which the user is a member.
  - `All` - Groups claim will contain the identifiers of all security groups and distribution lists of which the user is a member.
- d. Click **Manage Manifest**.
- e. Click **Upload Manifest** and select the modified manifest.

permissions to other applications

Windows Azure Active Directory Application Permissions: 1 Delegated Permissions: 5

Add application

VIEW ENDPOINTS UPLOAD LOGO MANAGE MANIFEST DELETE

## Configure a Single Sign-On Service Provider

This topic describes how to add an external identity provider to your Pivotal Single Sign-On (SSO) service plan.

### Configure Identity Provider Metadata

Edit the Identity Provider Metadata file you downloaded, named `federationmetadata.xml`.

- Find and remove the two `RoleDescriptor` elements from the metadata:

```
a. <RoleDescriptor xmlns:fed="http://docs.oasis-open.org/wsfed/federation/200706"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="fed:ApplicationServiceType"
    protocolSupportEnumeration="http://docs.oasis-open.org/wsfed/federation/200706">
b. <RoleDescriptor xmlns:fed="http://docs.oasis-open.org/wsfed/federation/200706"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="fed:SecurityTokenServiceType"
    protocolSupportEnumeration="http://docs.oasis-open.org/wsfed/federation/200706">
```

- The Single Sign-On service requires that the Name ID Format is specified. Replace the following text: `<SingleLogoutService`

```
Binding="urn: oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://login.microsoftonline.com/025c050a-9f19-4074-882f-4b522871e8c3/saml2" /> with:
<SingleLogoutService Binding="urn: oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://login.microsoftonline.com/025c050a-9f19-4074-882f-4b522871e8c3/saml2" />
<NameIDFormat>urn: oasis:names:tc:SAML:1.1:nameid-format:unspecified</NameIDFormat>
```

- The Single Sign-On service does not support DOS file format imports. Convert the file in one of the following ways:

- Option 1: Execute `dos2unix` on the metadata file.
- Option 2: Create a Unix file, then copy and paste the contents from the downloaded metadata file to the newly created file.

### Setting up SAML

- Log into the SSO dashboard at `https://p-identity.YOUR-SYSTEM-DOMAIN` as a Plan Administrator.
- Select your plan and click **Manage Identity Providers** on the dropdown menu.

The screenshot shows the 'Plans' section of the Pivotal SSO dashboard. There is one plan listed: 'Azure PCF SSO'. Below the plan, there are two buttons: 'Edit Plan' and 'Manage Identity Providers'. The 'Manage Identity Providers' button is highlighted with a red box.

- Click **New Identity Provider** to create a new identity provider.

### New Identity Provider

**Identity Provider Name\***

This name will show as a link on the login page

**Identity Provider Description**

Allows  to authenticate.

**Identity Provider Type\***

SAML

---

### Identity Provider Metadata

**Identity Provider Metadata URL\***

**Fetch Metadata**

- ▶ SAML File Metadata (optional)

**Advanced SAML Settings**

- ▶ Attribute mappings (optional)

Cancel
Create Identity Provider

4. To create a new identity provider, perform the following steps:
  - a. Enter an identity provider name into **Identity Provider Name**.
  - b. (Optional) Enter a description into **Identity Provider Description**.
  - c. Click **SAML File Metadata (optional)** followed by clicking the **Upload Identity Provider Metadata** button to upload your metadata XML.
  - d. (Optional) Under **Advanced SAML Settings**, click **Attribute Mappings** to enter the mappings.
5. Click **Create Identity Provider**.

## Configure Group Permissions

1. Add groups to be propagated from the external identity provider to the ID token by following these steps:
  - a. Log into the SSO dashboard at `https://p-identity.YOUR-SYSTEM-DOMAIN` as a Plan Administrator.
  - b. Select your plan and click **Manage Identity Providers** on the dropdown menu.
  - c. Click **Group Whitelist** next to your identity provider.
  - d. Enter the group names.
  - e. Click **Save Group Whitelist**.
2. Map the groups to resources defined in the SSO service by following these steps:
  - a. Log into the SSO dashboard at `https://p-identity.YOUR-SYSTEM-DOMAIN` as a Plan Administrator.
  - b. Select your plan and click **Manage Identity Providers** on the dropdown menu.
  - c. Click **Resource Permissions**.
  - d. Click **New Permissions Mapping** and perform the following steps:
    - i. Enter a **Group Name**.
    - ii. For **Select Permissions**, select the permissions that the members of the group from the external identity provider should have access to.
    - iii. Click **Save Permissions Mapping**.



## Testing

This topic describes how an administrator can test the connection between SSO and Azure Active Directory. An administrator can test both service provider and identity provider connections.

### Test Your Service Provider Connection

1. Log in to Apps Manager at <https://apps.YOUR-SYSTEM-DOMAIN> and navigate to the organization and space where your application is located.
2. Under **Services**, locate the service instance of the Single Sign-On (SSO) plan bound to your application. Click on the service instance and click **Manage**.

The screenshot shows the Apps Manager interface. At the top, there are two tabs: "Overview" (selected) and "Settings". Below these are two main sections: "Apps" and "Services".

**Apps:**

NAME	INSTANCES	MEMORY	LAST PUSH	ROUTE
authcode-sample	1	512MB	4 days ago	<a href="http://authcode-sample.id-service.cf-ap...">http://authcode-sample.id-service.cf-ap...</a> >

**Services:**

SERVICE	NAME	BOUND APPS	PLAN
 Pivotal Single Sign-On	SI	1	free - (MONTHLY) >

The screenshot shows the details of the "Pivotal Single Sign-On" service instance. It includes the service icon, name, instance name (SI), and service plan (Azure PCF SSO). Below this, there are three tabs: "App Binding (1)" (selected), "Plan", and "Settings".

**App Binding (1):**

Bound Apps	Edit Bindings
authcode-sample	<a href="#">Edit Bindings</a>

3. Under the **Apps** tab, click your application.

The screenshot shows the Pivotal Apps Manager interface. On the left, there's a button labeled 'NEW APP'. To its right, the application 'authcode-sample' is listed. The app details show it's a 'Web App' with 'Internal Identity Provider' and 'Azure PCF SSO' selected as identity providers. A note indicates it was 'updated 4 days ago'.

4. Under Identity Providers, select the Azure AD identity provider.

The screenshot shows the configuration page for the 'authcode-sample' application. In the 'Identity Providers' section, the 'Azure PCF SSO' button is highlighted with a red box. Other options like 'Internal User Store' are also present. Below this, the 'Redirect URIs' section lists 'https://authcode-sample.id-service.cf-app.com'. The 'Authorization' section includes 'Scopes' (todo, todo.read, todo.write) and 'System Provided' (openid). The 'Select Scopes' section shows 'Auto-Approved Scopes' with a dropdown menu set to 'None selected'. At the bottom, there are 'Delete', 'Cancel', and 'Save Config' buttons.

5. Return to Apps Manager and click on the URL below your application to be redirected to the identity provider to authenticate.

**Overview** **Settings**

**Apps**

NAME	INSTANCES	MEMORY	LAST PUSH	ROUTE
authcode-sample	1	512MB	4 days ago	<a href="http://authcode-sample.id-service.cf-app.com">http://authcode-sample.id-service.cf-app... &gt;</a>

6. Click the link.

Authcode sample

What do you want to do?

- Log in via Auth Code Grant Type

7. On the identity provider sign-in page, enter your credentials and click **Sign In**.

Microsoft Azure

Work or school, or personal Microsoft account

Email or phone

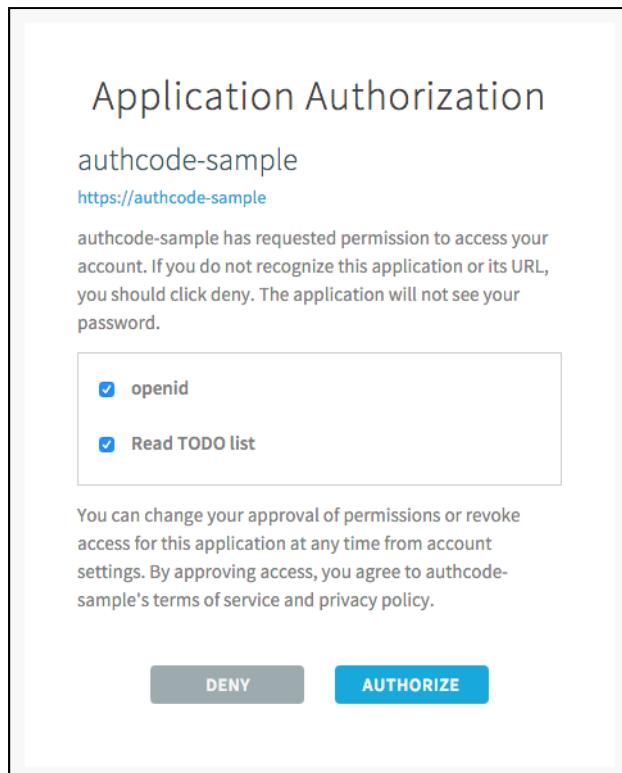
Password

Keep me signed in

**Sign in** **Back**

[Can't access your account?](#)

8. The application asks for authorization to the necessary scopes. Click **Authorize**.



9. The access token and ID token displays.

## Authcode sample

You've used the authcode flow! Here's the result of calling /userinfo:

```
{  
  "user_id" : "57a4a8e4-d5fc-426c-861d-78c8588fc65b",  
  "user_name" : "acAv4K7uBrkDx9ehb9pfAsU3whJqBIIuobxd9DHMayM",  
  "given_name" : "Example",  
  "family_name" : "Example",  
  "email" : "example@pivotal.io",  
  "name" : "Example Example"  
}
```

This is the Access Token that was used:

```
{  
  "jti" : "80785d63a02f4fef8fc5e6d65bcb2136",  
  "sub" : "57a4a8e4-d5fc-426c-861d-78c8588fc65b",  
  "scope" : [ "todo.read", "openid", "todo.write" ],  
  "client_id" : "d3092f73-ab0c-495d-91ea-79772d8d93ee",  
  "cid" : "d3092f73-ab0c-495d-91ea-79772d8d93ee",  
  "azp" : "d3092f73-ab0c-495d-91ea-79772d8d93ee",  
  "grant_type" : "authorization_code",  
  "user_id" : "57a4a8e4-d5fc-426c-861d-78c8588fc65b",  
  "origin" : "Azure PCF SSO",  
  "user_name" : "acAv4K7uBrkDx9ehb9pfAsU3whJqBIIuobxd9DHMayM",  
  "email" : "example@pivotal.io",  
  "auth_time" : 1469645071,  
  "rev_sig" : "6dade7f6",  
  "iat" : 1469645071,  
  "exp" : 1469688271,  
  "iss" : "https://example.uaa/oauth/token",  
  "zid" : "dbff701b-la02-4a0f-a141-47b2acdd5a30",  
  "aud" : [ "todo", "openid", "d3092f73-ab0c-495d-91ea-79772d8d93ee" ]  
}
```

This is the ID Token:

```
{  
  "sub" : "57a4a8e4-d5fc-426c-861d-78c8588fc65b",  
  "user_name" : "acAv4K7uBrkDx9ehb9pfAsU3whJqBIIuobxd9DHMayM",  
  "origin" : "Azure PCF SSO",  
  "iss" : "https://example.uaa/oauth/token",  
  "client_id" : "d3092f73-ab0c-495d-91ea-79772d8d93ee",  
  "aud" : [ "d3092f73-ab0c-495d-91ea-79772d8d93ee" ],  
  "zid" : "dbff701b-la02-4a0f-a141-47b2acdd5a30",  
  "grant_type" : "authorization_code",  
  "user_id" : "57a4a8e4-d5fc-426c-861d-78c8588fc65b",  
  "azp" : "d3092f73-ab0c-495d-91ea-79772d8d93ee",  
  "scope" : [ "openid" ],  
  "auth_time" : 1469645071,  
  "exp" : 1469688271,  
  "iat" : 1469645071,  
  "jti" : "80785d63a02f4fef8fc5e6d65bcb2136",  
  "email" : "example@pivotal.io",  
  "rev_sig" : "6dade7f6",  
  "cid" : "d3092f73-ab0c-495d-91ea-79772d8d93ee"  
}
```

## What do you want to do?

- [TODO List \(You need to configure the Resource Server sample app before using this\)](#)
- [See your account profile \(so you can de-authorize this client\)](#)
- [Log out](#)

## Test Your Identity Provider Connection

 Note: SSO does not support identity provider-initiated flow into applications, but it does redirect the user to the User Account and Authentication (UAA) page to select applications assigned to the user.

1. Sign in to Azure AD.

Microsoft Azure

Work or school, or personal Microsoft account

Email or phone  
Password

Keep me signed in

**Sign in** Back

[Can't access your account?](#)

2. Navigate to your application and click it.
3. You are redirected to the page that lists applications you have access to.

The screenshot shows a user profile with the email example@example.com and a sign-out link. Below the profile are five navigation tabs: Apps (underlined), Profile, Security, Approvals, and Notifications. Under the Apps tab, there are three application cards, each featuring a teal circle with a white 'P' and the application name: Application 1, Application 2, and Application 3. At the bottom of the screen, a copyright notice reads: ©2016 Pivotal Software, Inc. All Rights Reserved. [Privacy Policy](#) — [Terms of Service](#).

## Test Your Single Sign-Off

Test single sign-off to ensure that when users log out of the application, they are logged out of Azure AD as well.

1. Sign into the sample application. Information about the access and ID token displays, as well as the “What do you want to do?” section.
2. Under “What do you want to do?”, click **Log out**.

**What do you want to do?**

- [TODO List \(You need to configure the Resource Server sample app before using this\)](#)
- [See your account profile \(so you can de-authorize this client\)](#)
- [Log out](#)

3. You are logged out and redirected to the Azure AD login page.

Microsoft Azure

Work or school, or personal Microsoft account

Email or phone

Password

Keep me signed in

**Sign in** Back

[Can't access your account?](#)

## Troubleshooting

This topic describes how to resolve common errors that arise when configuring a single sign-on partnership between Azure Active Directory and Pivotal Single Sign-On (SSO).

### App ID Not Found

Symptom:

### Sign In

Sorry, but we're having trouble signing you in.

We received a bad request.

Additional technical information:  
Correlation ID: 33100be1-d5af-409f-aa63-59784905e8fe  
Timestamp: 2016-07-27 22:02:30Z  
AADSTS70001: Application with identifier 'http://example.cf-app.com' was not found in the directory 025c050a-9f19-4074-882f-4b522871e8c3

Explanations:

- The App ID URI is misconfigured on Azure AD.

### Reply URL Does Not Match

Symptom:

### Sign In

Sorry, but we're having trouble signing you in.

We received a bad request.

Additional technical information:  
Correlation ID: 148c57c2-6082-493c-9dd9-2c646bf0f0b9  
Timestamp: 2016-07-27 22:03:47Z  
AADSTS50011: The reply address 'https://example.cf-app.com/saml/SSO/alias/example.cf-app.com' does not match the reply addresses configured for the application: http://example.cf-app.com.

Explanation:

- The Reply URL is misconfigured on Azure AD.

### Missing Name ID

Symptom:

Identity Provider Metadata

Identity Provider Metadata URL\*

**Fetch Metadata**

Error processing metadata

▼ SAML File Metadata (optional)

**Upload Identity Provider Metadata** federationmetadata.xml

Explanation:

- The identity provider metadata has the `RoleDescriptor` elements or is missing configurations for Name ID. See [Configure Identity Provider Metadata](#).

## Okta Integration Guide Overview

Okta is an enterprise identity management and single sign-on service that integrates with applications in the cloud, on-premises, or on a mobile device. This documentation describes how to configure a single sign-on partnership between Okta as the Identity Provider (IdP) and the Single Sign-On Service (SSO) for Pivotal Cloud Foundry as the Service Provider (SP).

SSO supports service provider-initiated authentication flow and single logout. It does not support identity provider-initiated authentication flow. All SSO communication takes place over SSL.

## Prerequisites

To integrate Okta with Pivotal Cloud Foundry (PCF), you need:

Pivotal

- PCF, version 1.7.0 or later.
- Single Sign-On, version 1.1.0 or later.

Okta

- Okta, version 2016.07 or later.
- A user with Application Admin privileges.

 **Note:** To configure SAML, you must have the Single Sign-On service broker installed on your PCF deployment. You need to create a plan, grant any plan administrators, and specify any organizations this plan should be the authentication authority for. For help configuring plans, see the [Manage Service Plans](#) topic.

## Okta Integration Guide

### Configuring Okta with SSO

Complete both steps below to integrate your deployment with Okta and SSO.

1. [Configure Okta as an Identity Provider](#)
2. [Configure a Single Sign-On Service Provider](#)

### Testing and Troubleshooting

- [Testing](#)
- [Troubleshooting](#)

## Configure Okta as an Identity Provider

This topic describes how to set up Okta as your identity provider by configuring SAML integration in both Pivotal Cloud Foundry (PCF) and Okta.

### Set up SAML in PCF

1. Log into the Single Sign-On (SSO) dashboard at <https://p-identity.YOUR-SYSTEM-DOMAIN> as a Plan Administrator.
2. Select your plan and click **Manage Identity Providers** on the dropdown menu.

The screenshot shows the 'Plans' section of the PCF SSO dashboard. A specific plan named 'Okta PCF SSO' is selected. Below the plan name, there are two buttons: 'Edit Plan' and 'Manage Identity Providers'. The 'Manage Identity Providers' button is highlighted with a red rectangular box.

3. Click **Configure SAML Service Provider**.

The screenshot shows the 'Identity Providers' list under the 'Okta PCF SSO' plan. There are two entries: 'Okta PCF SSO' (Type: SAML) and 'Internal User Store' (Type: Internal User Store). Above the list, there are two buttons: 'New Identity Provider' and 'Configure SAML Service Provider'. The 'Configure SAML Service Provider' button is highlighted with a red rectangular box.

4. (Optional) Select **Perform signed authentication requests** to enforce SSO private key signature and identity provider validation.

The screenshot shows the 'Configure SAML Service Provider' dialog. It contains two checkboxes: 'Perform signed authentication requests' (which is checked) and 'Require signed assertions'. At the bottom right, there is a 'Download Metadata' button and a large blue 'Save' button, which is highlighted with a blue rectangular box.

5. (Optional) Select **Require signed assertions** to validate the origin of signed responses.

6. Click **Download Metadata** to download the service provider metadata.

7. Click **Save**.

### Set up SAML in Okta

1. Sign in as an Okta administrator.
2. Navigate to your application, then click the **Sign On** tab.
3. Under **Settings**, click **Edit**, and select **SAML 2.0**.

**Okta PCF SSO**

Active

General Sign On Mobile Import People Groups

**Settings**

**SIGN ON METHODS**

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

SAML 2.0

Default Relay State

**SAML 2.0** is not configured until you complete the setup instructions.

[View Setup Instructions](#)

Identity Provider metadata is available if this application supports dynamic configuration.

**CREDENTIALS DETAILS**

Application username format      Okta username

Password reveal       Allow users to securely see their password (Recommended)

**About**

SAML 2.0 streamlines the end user experience by not requiring the user to know their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuration in the 3rd party application may be required to complete the integration with Okta.

**Application Username**

Choose a format to use as the default username value when assigning the application to users.

If you select None you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

4. Click the **General** tab.
5. Under SAML Settings, click the **Edit** button followed by the **Next** button to configure SAML.

## Edit SAML Integration

1 General Settings    2 Configure SAML    3 Feedback

**A SAML Settings**

**GENERAL**

Single sign on URL <small>?</small>	<input type="text" value="https://example.login.id-service.cf-app.com/saml/SSO/alias/example"/>
<input checked="" type="checkbox"/> Use this for Recipient URL and Destination URL	
Audience URI (SP Entity ID) <small>?</small>	<input type="text" value="example.login.id-service.cf-app.com"/>
Default RelayState <small>?</small>	<input type="text"/>
Name ID format <small>?</small>	<input type="text" value="EmailAddress"/>
Application username <small>?</small>	<input type="text" value="Okta username"/>

[Show Advanced Settings](#)

**ATTRIBUTE STATEMENTS (OPTIONAL)** [LEARN MORE](#)

Name	Name format (optional)	Value
<input type="text" value="firstName"/>	<input type="text" value="Unspecified"/>	<input type="text" value="user.firstName"/>
<input type="text" value="lastName"/>	<input type="text" value="Unspecified"/>	<input type="text" value="user.lastName"/>
<input type="text" value="email"/>	<input type="text" value="Unspecified"/>	<input type="text" value="user.email"/>

[Add Another](#)

---

**GROUP ATTRIBUTE STATEMENTS (OPTIONAL)**

Name	Name format (optional)	Filter
<input type="text"/>	<input type="text" value="Unspecified"/>	<input type="text" value="Starts with"/>

[Add Another](#)

6. In the **SAML Settings** section, perform the following steps:

- a. Enter the **AssertionConsumerService Location URL** from your downloaded service provider metadata into **Single sign on URL**. For example, `https://AUTH-DOMAIN/saml/SSO/alias/AUTH-DOMAIN`.
- b. Enter your Auth Domain URL into **Audience URI (SP Entity ID)**. You can view the Auth Domain for a plan by logging into the SSO dashboard, clicking the name of your plan, and selecting **Edit Plan**. For example, `https://AUTH-DOMAIN.login.SYSTEM-DOMAIN`.
- c. Select a **Name ID format**.
- d. Select an **Application username**.

7. (Optional) To configure single logout, perform the following steps:

- a. Click **Show Advanced Settings**.
- b. For **Enable Single Logout**, select **Allow application** to initiate single logout.
- c. Enter the **SingleLogoutService Location URL** from your downloaded service provider metadata into **Single Logout URL**.
- d. Enter your **Auth Domain URL** into **SP Issuer**.
- e. Click **Upload Signature Certificate** to upload the signature certificate from your downloaded service provider metadata.

8. (Optional) Under **Attribute Statements (Optional)**, specify any attribute statements that you want to map to users in the ID token.
9. (Optional) Under **Group Attribute Statements (Optional)**, specify any group attribute statements that you want to map to users in the ID token. This is a group that users are in within Okta.
10. Click the **Next** button followed by the **Finish** button.
11. Click **Identity Provider metadata** to download the metadata, or copy and save the link address of the **Identity Provider metadata**.

**Okta PCF SSO**

Active

General Sign On Mobile Import People Groups

**Settings** Edit

**SIGN ON METHODS**

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

SAML 2.0

Default Relay State

**SAML 2.0** is not configured until you complete the setup instructions. [View Setup Instructions](#)

**Identity Provider metadata** is available if this application supports dynamic configuration.

**CREDENTIALS DETAILS**

Application username format Okta username

Password reveal  Allow users to securely see their password (Recommended)

**About**

SAML 2.0 streamlines the end user experience by not requiring the user to know their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuration in the 3rd party application may be required to complete the integration with Okta.

**Application Username**

Choose a format to use as the default username value when assigning the application to users.

If you select None you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

## Configure a Single Sign-On Service Provider

This topic describes how to add an external identity provider to your Pivotal Single Sign-On (SSO) service plan.

### Setting up SAML

1. Log into the SSO dashboard at <https://p-identity.YOUR-SYSTEM-DOMAIN> as a Plan Administrator.
2. Select your plan and click **Manage Identity Providers** on the dropdown menu.

A screenshot of the Pivotal SSO dashboard. The top navigation bar has 'Plans' and 'New Plan' tabs. Below that is a table with two columns: 'Name' and 'Sign In Header'. One row shows 'Okta PCFSSO-' and 'example'. At the bottom of the table are 'Edit Plan' and 'Manage Identity Providers' buttons, with 'Manage Identity Providers' having a red border around it.

3. Click **New Identity Provider** to create a new identity provider.

The 'New Identity Provider' form is displayed. It includes fields for 'Identity Provider Name\*' (with a note: 'This name will show as a link on the login page'), 'Identity Provider Description' (with a note: 'Allows \_\_\_\_\_ to authenticate.'), 'Identity Provider Type\*' (set to 'SAML'), and 'Identity Provider Metadata' sections. Under 'Identity Provider Metadata', there's a 'Metadata URL\*' field containing 'https://idp.company.com/SAML2', a 'Fetch Metadata' button, and a note about optional SAML File Metadata. Below that is an 'Advanced SAML Settings' section with an optional Attribute mappings link. At the bottom right are 'Cancel' and 'Create Identity Provider' buttons.

4. To create a new identity provider, perform the following steps:
  - a. Enter an identity provider name into **Identity Provider Name**.
  - b. (Optional) Enter a description into **Identity Provider Description**.
  - c. Specify Identity Provider Metadata from Step 11 of the [Configure Okta as an Identity Provider](#) topic.
    - i. Option 1: Enter your **Input Identity Provider Metadata URL** and **Fetch Metadata** to fetch your identity provider metadata from an endpoint.
    - ii. Option 2: Click **SAML File Metadata (optional)** to upload your metadata XML manually.
  - d. (Optional) Under Advanced SAML Settings, click **Attribute Mappings** to enter the mappings.
5. Click **Create Identity Provider**.

6. Click **Resource Permissions**.
7. Click **New Permissions Mapping** and perform the following steps:
  - a. Enter a **Group Name**.
  - b. For **Select Permissions**, select the permissions that the members of the group from the external identity provider should have access to.
8. Navigate to the identity provider list.
9. Click **Group Whitelist** and enter the group names from the external identity provider that should be propagated in the ID token.

## Testing

This topic describes how an administrator can test the connection between SSO and Okta services. An administrator can test both service provider and identity provider connections.

### Test Your Service Provider Connection

1. Log in to Apps Manager at <https://apps.YOUR-SYSTEM-DOMAIN> and navigate to the organization and space where your application is located.
2. Under **Services**, locate the service instance of the Single Sign-On (SSO) plan bound to your application and click **Manage**.

NAME	INSTANCES	MEMORY	LAST PUSH	ROUTE
authcode-sample	1	512MB	4 days ago	<a href="http://authcode-sample.id-service.cf-app.com">http://authcode-sample.id-service.cf-ap...</a>

SERVICE	NAME	BOUND APPS	PLAN
Pivotal Single Sign-On	SI	1	free - (MONTHLY)

SERVICE	INSTANCE NAME	SERVICE PLAN
Pivotal Single Sign-On	SI	Okta PCF SSO

APP BINDING (1)	PLAN	SETTINGS
authcode-sample		

3. Under the **Apps** tab, click your application.

APP TYPE
Web App

IDENTITY PROVIDER
Okta PCF SSO

INTERNAL IDENTITY PROVIDER
Internal Identity Provider

4. Under **Identity Providers**, select the Okta identity provider.

authcode-sample Web App

**App Name\***  
authcode-sample

**Identity Providers**

Select a Identity Provider

**Okta PCF SSO** (highlighted with a red box)

**Internal User Store**

**Redirect URIs**

The Authentication Response will be sent to the following locations:

**Auth Redirect URIs\***  
Provide a comma-separated list of URIs  
https://authcode-sample.id-service.cf-app.com

**Authorization**

**Scopes**  
Permissions requested by the application  
todo

todo.read X todo.write X

System Provided

openid X

**Select Scopes**

**Auto-Approved Scopes**  
Permissions automatically approved on behalf of the user  
None selected ▾

**Delete**

Cancel Save Config

5. Return to Apps Manager and click on the URL below your application to be redirected to the identity provider to authenticate.

**Overview** **Settings**

**Apps**

NAME	INSTANCES	MEMORY	LAST PUSH	ROUTE
authcode-sample	1	512MB	4 days ago	<a href="http://authcode-sample.id-service.cf-ap...">http://authcode-sample.id-service.cf-ap...</a>

6. Click the link.

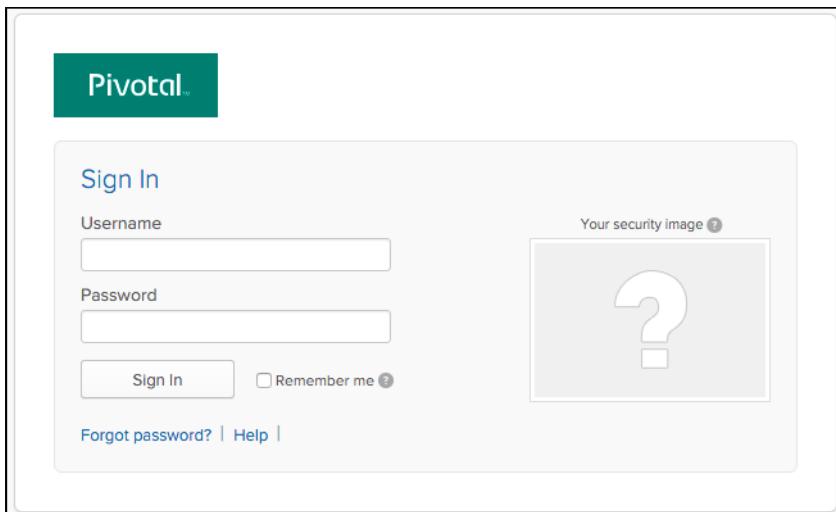
https://authcode-sample

## Authcode sample

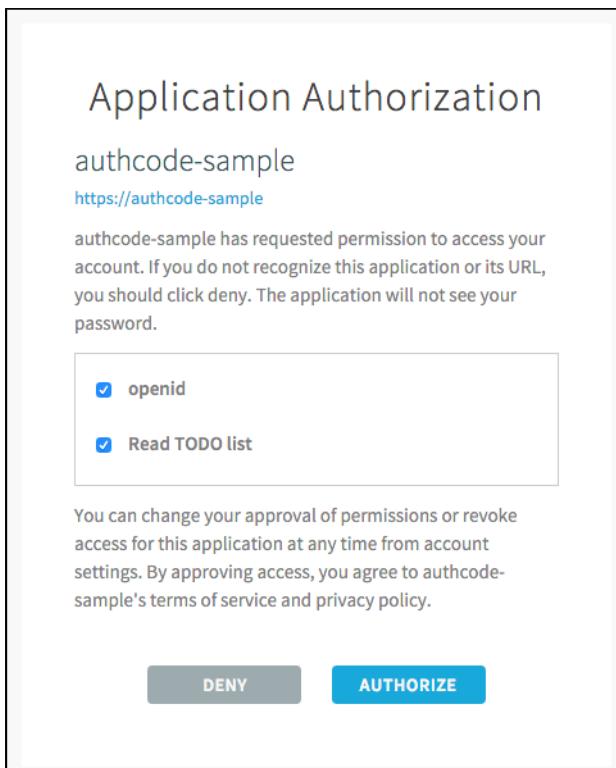
What do you want to do?

- Log in via Auth Code Grant Type

7. On the identity provider sign-in page, enter your credentials and click **Sign In**.



8. The application asks for authorization to the necessary scopes. Click **Authorize**.



9. The access token and ID token displays.

## Authcode sample

You've used the authcode flow! Here's the result of calling /userinfo:

```
{
  "user_id" : "1bd4153a-08eb-4aed-bb9c-929b45df026d",
  "user_name" : "example@pivotal.io",
  "given_name" : "Example",
  "family_name" : "Example",
  "email" : "example@pivotal.io",
  "name" : "Example Example"
}
```

This is the Access Token that was used:

```
{
  "jti" : "c1148dda64a840589b2936deba1149a9",
  "sub" : "1bd4153a-08eb-4aed-bb9c-929b45df026d",
  "scope" : [ "todo.read", "openid", "todo.write" ],
  "client_id" : "27b2d43c-2f0d-48e8-979c-b11f841e972d",
  "cid" : "27b2d43c-2f0d-48e8-979c-b11f841e972d",
  "azp" : "27b2d43c-2f0d-48e8-979c-b11f841e972d",
  "grant_type" : "authorization_code",
  "user_id" : "1bd4153a-08eb-4aed-bb9c-929b45df026d",
  "origin" : "Okta PCF SSO",
  "user_name" : "example@pivotal.io",
  "email" : "example@pivotal.io",
  "auth_time" : 1465240181,
  "rev_sig" : "f59bcff6",
  "iat" : 1465240182,
  "exp" : 1465283382,
  "iss" : "https://example.uaa/oauth/token",
  "zid" : "23835dc6-7f12-4c27-bf22-3ed29923d590",
  "aud" : [ "todo", "openid", "27b2d43c-2f0d-48e8-979c-b11f841e972d" ]
}
```

This is the ID Token:

```
{
  "sub" : "1bd4153a-08eb-4aed-bb9c-929b45df026d",
  "user_name" : "example@pivotal.io",
  "origin" : "Okta PCF SSO",
  "iss" : "https://example.uaa/oauth/token",
  "client_id" : "27b2d43c-2f0d-48e8-979c-b11f841e972d",
  "aud" : [ "27b2d43c-2f0d-48e8-979c-b11f841e972d" ],
  "zid" : "23835dc6-7f12-4c27-bf22-3ed29923d590",
  "grant_type" : "authorization_code",
  "user_id" : "1bd4153a-08eb-4aed-bb9c-929b45df026d",
  "azp" : "27b2d43c-2f0d-48e8-979c-b11f841e972d",
  "scope" : [ "openid" ],
  "auth_time" : 1465240181,
  "exp" : 1465283382,
  "iat" : 1465240182,
  "jti" : "c1148dda64a840589b2936deba1149a9",
  "email" : "example@pivotal.io",
  "rev_sig" : "f59bcff6",
  "cid" : "27b2d43c-2f0d-48e8-979c-b11f841e972d"
}
```

## What do you want to do?

- [TODO List \(You need to configure the Resource Server sample app before using this\)](#)
- [See your account profile \(so you can de-authorize this client\)](#)
- [Log out](#)

## Test Your Identity Provider Connection

 Note: SSO does not support identity provider-initiated flow into applications, but it does redirect the user to the User Account and Authentication (UAA) page to select applications assigned to the user.

- Sign into Okta.

Pivotal.

Sign In

Username

Password

Sign In  Remember me

Your security image ?

Forgot password? | Help |

2. Navigate to the application tile and click it.



3. You are redirected to the page that lists applications you have access to.

example@pivotal.io

Sign out

Pivotal.

Apps Profile Security Approvals Notifications

**Application 1**

**Application 2**

**Application 2**

©2016 Pivotal Software, Inc. All Rights Reserved. [Privacy Policy](#) — [Terms of Service](#)

## Test Your Single Sign-Off

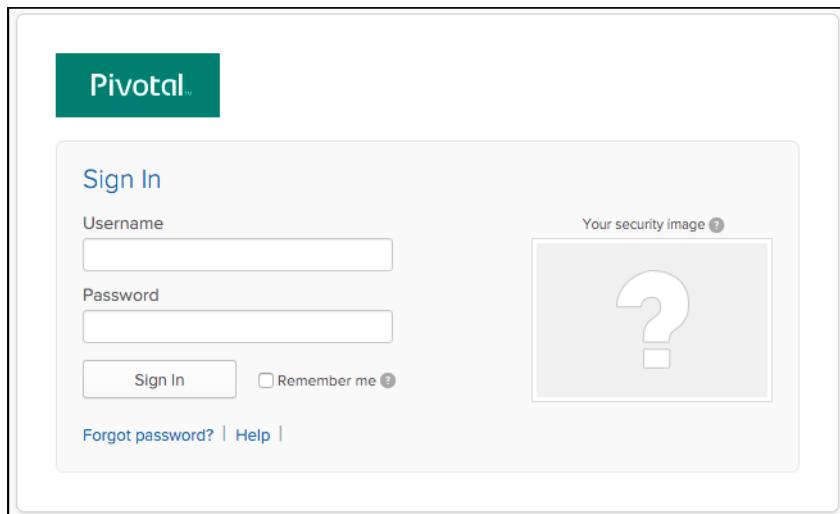
Test single sign-off to ensure that when users log out of the application, they are logged out of Okta as well.

1. Sign into the sample application. Information about the access and ID token displays, as well as the “What do you want to do?” section.
2. Under “What do you want to do?”, click **Log out**.

**What do you want to do?**

- [TODO List \(You need to configure the Resource Server sample app before using this\)](#)
- [See your account profile \(so you can de-authorize this client\)](#)
- [Log out](#)

3. You are logged out and redirected to the Okta login page.



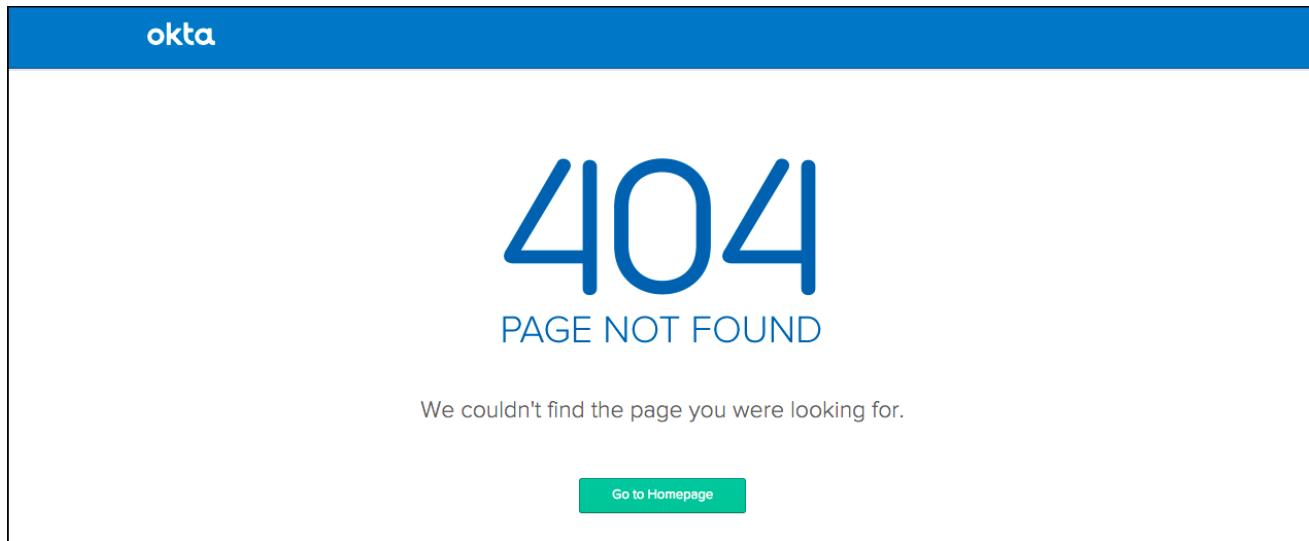
The screenshot shows the Pivotal sign-in interface. At the top left is the Pivotal logo. Below it, the word "Sign In" is displayed in blue. The form contains fields for "Username" and "Password", each with a corresponding input box. To the right of these fields is a placeholder box labeled "Your security image" with a question mark icon inside. Below the input fields are two buttons: "Sign In" and "Remember me". At the bottom of the form are links for "Forgot password?" and "Help".

## Troubleshooting

This topic describes how to resolve common errors that arise when configuring a single sign-on partnership between Okta and Pivotal Single Sign-On (SSO).

### Page Not Found

Symptom:

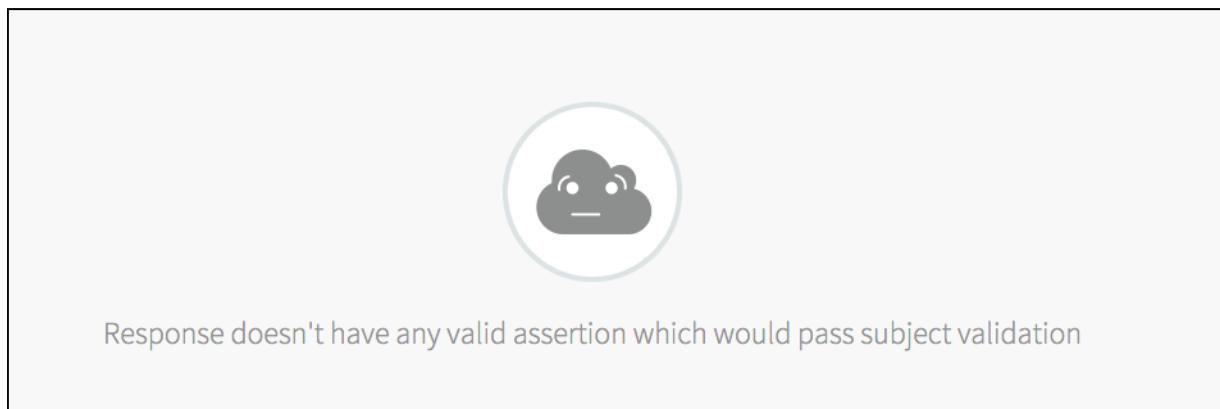


Explanations:

- The Okta instance is inactive.
- The Recipient URL is misconfigured in Okta.
- The identity provider SSO URL is misconfigured in the SSO plan settings.

### No Valid Assertion

Symptom:



## Explanations:

- The service provider Entity ID is misconfigured in Okta.
- The Destination URL is misconfigured in Okta.

## Webpage Not Available

### Symptom:



This webpage is not available

DNS\_PROBE\_FINISHED\_NXDOMAIN

[Details](#)

### Explanation:

- The SSO URL is misconfigured in Okta.

## Metadata Not Found

### Symptom:



Metadata for issuer <http://www.okta.com/exk5s2s8y0ugC73JY0h7> wasn't found

### Explanation:

- The identity provider Entity ID is misconfigured in the SSO plan settings.

## PingFederate Integration Guide Overview

PingFederate is a federation server that provides identity management, single sign-on, and API security for the enterprise. This documentation describes how to configure a single sign-on partnership between PingFederate as the Identity Provider (IdP) and the Single Sign-On Service (SSO) for Pivotal Cloud Foundry as the Service Provider (SP).

SSO supports service provider-initiated authentication flow and single logout. It does not support identity provider-initiated authentication flow. All SSO communication takes place over SSL.

## Prerequisites

To integrate PingFederate with Pivotal Cloud Foundry (PCF), you need:

Pivotal

- PCF, version 1.7.0 or later.
- Single Sign-On, version 1.1.0 or later.

Ping

- PingFederate
- A user with Administrator privileges.

 **Note:** To configure SAML, you must have the Single Sign-On service broker installed on your PCF deployment. You need to create a plan, grant any plan administrators, and specify any organizations this plan should be the authentication authority for. For help configuring plans, see the [Manage Service Plans](#) topic.

## PingFederate Integration Guide

### Configuring PingFederate with SSO

Complete both steps below to integrate your deployment with PingFederate and SSO.

1. [Configure PingFederate as an Identity Provider](#)
2. [Configure a Single Sign-On Service Provider](#)

### Testing and Troubleshooting

- [Testing](#)
- [Troubleshooting](#)

## Configure PingFederate as an Identity Provider

This topic describes how to set up PingFederate as your identity provider by configuring SAML integration in both Pivotal Cloud Foundry (PCF) and PingFederate.

### Set up SAML in PCF

1. Log into the Single Sign-On (SSO) dashboard at <https://p-identity.YOUR-SYSTEM-DOMAIN> as a Plan Administrator.
2. Select your plan and choose **Manage Identity Providers** from the dropdown menu.

The screenshot shows the 'Plans' section of the PCF SSO dashboard. A single plan named 'PingFederate PCF SSO' is listed. Below the plan name, there are two buttons: 'Edit Plan' and 'Manage Identity Providers'. The 'Manage Identity Providers' button is highlighted with a red border.

3. Click **Configure SAML Service Provider**.

The screenshot shows the 'Identity Providers' list. It lists two entries: 'Internal User Store' (Type: Internal User Store) and 'PingFederate PCF SSO' (Type: SAML). For the 'PingFederate PCF SSO' entry, there are 'Actions' links for 'Resource Permissions' and 'Group Whitelist'. To the right of the table, there is a blue link labeled 'Configure SAML Service Provider' which is also highlighted with a red border.

4. (Optional) Select **Perform signed authentication requests** to enforce SSO private key signature and identity provider validation.

The screenshot shows the 'Configure SAML Service Provider' dialog. It contains two checkboxes: 'Perform signed authentication requests' (which is checked) and 'Require signed assertions' (which is unchecked). At the bottom of the dialog is a blue 'Save' button.

5. (Optional) Select **Require signed assertions** to validate the origin of signed responses.

6. Click **Download Metadata** to download the service provider metadata.

7. Click **Save**.

### Set up SAML in PingFederate

#### Configure the Connection

1. Sign in as a PingFederate administrator.
2. Navigate to your identity provider configurations by clicking on the **IDP Configuration** tab.
3. Under **SP Connections**, click the **Create New** button.

The screenshot shows the PingFederate interface under the 'IDP Configuration' tab. In the top right, there is a 'SP CONNECTIONS' section with a count of 0. It contains three buttons: 'Manage All', 'Create New' (which is highlighted with a red box), and 'Import'. Below this section, there are several other configuration tabs like 'APPLICATION INTEGRATION', 'AUTHENTICATION POLICIES', and 'FEDERATION INFO'.

4. Select the **Browser SSO Profiles** connection template on the **Connection Type** tab and click **Next**.
5. Select **Browser SSO** on the **Connection Options** tab and click **Next**.
6. Select **File** as the method for importing metadata and click **Choose file** to choose the SSO metadata on the **Import Metadata** tab. Click **Next**.

The screenshot shows the 'SP Connection' configuration screen. On the top navigation bar, the 'Import Metadata' tab is selected. In the main area, there is a section for importing metadata from a file. A radio button labeled 'FILE' is selected, and a 'Choose file' button is highlighted with a red box. At the bottom right, there are 'Cancel', 'Previous', and 'Next' buttons.

7. Review the information on the **Metadata Summary** tab and click **Next**.
8. Ensure that the **Partner's Entity ID**, **Connection Name**, and **Base URL** fields pre-populate based on the metadata. Click **Next**.

The screenshot shows the 'SP Connection' configuration screen with the 'Metadata Summary' tab selected. The 'Activation & Summary' section contains detailed information about the connection. The 'PARTNER'S ENTITY ID (CONNECTION ID)' field is populated with 'example.login.id-serv'. The 'CONNECTION NAME' field is also populated with 'example.login.id-serv'. The 'VIRTUAL SERVER IDS' and 'BASE URL' fields are present but not yet filled. At the bottom right, there are 'Cancel', 'Previous', and 'Next' buttons.

## Configure Browser SSO

1. Click **Configure Browser SSO** on the **Browser SSO** tab.
2. Select the **IdP-Initiated SSO** and **SP-Initiated SSO** options on the **SAML Profiles** tab and click **Next**.

SP Connection | Browser SSO

**Protocol Settings**

A SAML Profile defines what kind of messages may be exchanged between an Identity Provider and a Service Provider, and how the messages are transported (bindings). As an IdP, you configure this information for your SP connection.

Single Sign-On (SSO) Profiles	Single Logout (SLO) Profiles
<input checked="" type="checkbox"/> IDP-INITIATED SSO	<input type="checkbox"/> IDP-INITIATED SLO
<input checked="" type="checkbox"/> SP-INITIATED SSO	<input type="checkbox"/> SP-INITIATED SLO

Cancel Save Draft Next

3. Enter your desired assertion validity time from on the **Assertion Lifetime** tab and click **Next**.

## Assertion Creation

1. Click **Configure Assertion Creation** on the **Assertion Creation** tab.
2. Choose the **Standard** option on the **Identity Mapping** tab and click **Next**.
3. Select a **Subject Name Format** for the **SAML SUBJECT** on the **Attribute Contract** tab and click **Next**.

SP Connection | Browser SSO | Assertion Creation

**Attribute Contract**

An Attribute Contract is a set of user attributes that this server will send in the assertion.

Action
Extend the Contract
Attribute Name Format

SAML SUBJECT: urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

Add

Cancel Save Draft Previous Next

4. Click **Map New Adapter Instance** on the **Authentication Source Mapping** tab.
5. Select an **Adapter Instance** and click **Next**. The adapter must include the user's email address.

**PingFederate**

MAIN

SP Connection | Browser SSO | Assertion Creation | IdP Adapter Mapping

Adapter Instance    Mapping Method    Attribute Contract Fulfillment    Issuance Criteria    Summary

Select an IdP adapter instance that may be used to authenticate users for this partner. Attributes returned by the adapter instance you choose (the Adapter Contract) may be used to fulfill the Attribute Contract with your partner.

ADAPTER INSTANCE    Adapter   

Adapter Contract

username

OVERRIDE INSTANCE SETTINGS

6. Select the Use only the adapter contract values in the SAML assertion option on the Mapping Method tab and click Next.

**PingFederate**

MAIN

SP Connection | Browser SSO | Assertion Creation | IdP Adapter Mapping

Adapter Instance    **Mapping Method**    Attribute Contract Fulfillment    Issuance Criteria    Summary

You can choose to fulfill the Attribute Contract with your partner using either the values provided by the "HTTP Basic IdP Adapter" adapter, or you can use these values plus additional attributes retrieved from local data stores.

Adapter Contract

email

givenName

username

RETRIEVE ADDITIONAL ATTRIBUTES FROM MULTIPLE DATA STORES USING ONE MAPPING  
 RETRIEVE ADDITIONAL ATTRIBUTES FROM A DATA STORE – INCLUDES OPTIONS  
 TO USE ALTERNATE DATA STORES AND/OR A FAILSAFE MAPPING  
 USE ONLY THE ADAPTER CONTRACT VALUES IN THE SAML ASSERTION

7. Select your adapter instance as the Source and the email as the Value on the Attribute Contract Fulfillment tab and click Next.

**PingFederate**

MAIN

SP Connection | Browser SSO | Assertion Creation | IdP Adapter Mapping

Adapter Instance    Mapping Method    **Attribute Contract Fulfillment**    Issuance Criteria    Summary

Fulfill your Attribute Contract with values from the authentication adapter or with dynamic text values.

Attribute Contract	Source	Value	Actions
SAML_SUBJECT	Adapter <input type="button" value="▼"/>	email <input type="button" value="▼"/>	None available

8. (Optional) Select any authorization conditions you would like on the Issuance Criteria tab and click Next.

9. Click Done on the Summary tab.

10. Click Next on the Authentication Source Mapping tab.

11. Click Done on the Summary tab.

12. Click **Next** on the Assertion Creation tab.

## Protocol Settings

1. Click **Configure Protocol Settings** on the **Protocol Settings** tab.
2. Select POST for **Binding** and specify the single sign-on endpoint url in the **Endpoint URL** field on the **Assertion Consumer Service URL** tab. Click **Next**

Default	Index	Binding	Endpoint URL	Action
default	0	POST	https://example.login.id-service.cf-app.com/saml/SSO/alias/example.login.id-service.cf-app.com	<a href="#">Edit   Delete</a>

3. Select POST on the Allowable SAML Bindings tab and click **Next**.

4. Select your desired signature policies for assertions on the **Signature Policy** tab and click **Next**.
5. Select your desired encryption policy for assertions on the **Encryption Policy** tab and click **Next**.
6. Click **Done** on the **Protocol Settings Summary** tab.
7. Click **Done** on the **Browser SSO Summary** tab.

## Configure Credentials

1. Click **Configure Credentials** on the **Credentials** tab.
2. Select the **Signing Certificate** to use with the Single Sign-On service and select **Include the certificate in the signature element**. Click **Next**.

SP Connection | Credentials

Digital Signature Settings      Summary

You may need to digitally sign SAML messages or security tokens to protect against tampering. Please select a key/certificate to use from the list below.

SIGNING CERTIFICATE: 21:51:3D:A7:E1:5F (cn=Pivotal)

INCLUDE THE CERTIFICATE IN THE SIGNATURE <KEYINFO> ELEMENT.  
 INCLUDE THE RAW KEY IN THE SIGNATURE <KEYVALUE> ELEMENT.

SIGNING ALGORITHM: RSA SHA256

Manage Certificates

Cancel      Save Draft      Next

3. Click **Done** on the **Summary** tab.
4. Click **Next** on the **Credentials** tab.
5. Select **Active** for the **Connection Status** on the **Activation & Summary** tab and click **Save**.
6. Click **Manage All** under **SP Connections**.
7. Click **Export Metadata** for the desired service provider connection.
8. Choose a **Signing Certificate** on the **Metadata Signing** tab and click **Next**.
9. Click **Export** on the **Export & Summary** tab and click **Done**.

## Configure a Single Sign-On Service Provider

This topic describes how to add an external identity provider to your Pivotal Single Sign-On (SSO) service plan.

### Setting up SAML

1. Log into the SSO dashboard at <https://p-identity.YOUR-SYSTEM-DOMAIN> as a Plan Administrator.
2. Select your plan and choose **Manage Identity Providers** from the dropdown menu.

The screenshot shows a 'Plans' section with a single item. Below it is a table with two columns: 'Name' and 'Sign In Header'. A dropdown menu is open under 'Name', showing 'PingOne PCF SSO' and other options. Underneath the table, there are two buttons: 'Edit Plan' and 'Manage Identity Providers', with 'Manage Identity Providers' highlighted by a red box.

3. Click **New Identity Provider**.

The screenshot shows the 'New Identity Provider' form. It includes fields for 'Identity Provider Name\*' (with a note: 'This name will show as a link on the login page'), 'Identity Provider Description' (with a note: 'Allows \_\_\_\_\_ to authenticate.'), 'Identity Provider Type\*' (set to 'SAML'), and 'Identity Provider Metadata' sections. The 'Identity Provider Metadata URL\*' field contains 'https://idp.company.com/SAML2'. There are 'Fetch Metadata' and 'Advanced SAML Settings' buttons, both with expandable sections. At the bottom right are 'Cancel' and 'Create Identity Provider' buttons.

4. To create a new identity provider, perform the following steps:
  - a. Enter an identity provider name into **Identity Provider Name**.
  - b. (Optional) Enter a description into **Identity Provider Description**.
  - c. Click **SAML File Metadata (optional)**, then click the **Upload Identity Provider Metadata** button to upload your metadata XML.
  - d. (Optional) Under **Advanced SAML Settings**, click **Attribute Mappings** to enter the mappings.
5. Click **Create Identity Provider**.
6. Click **Resource Permissions**.

7. Click **New Permissions Mapping** and perform the following steps:
  - a. Enter a **Group Name**.
  - b. For **Select Permissions**, select the permissions that the members of the group from the external identity provider should have access to.
8. Navigate to the identity provider list.
9. Click **Group Whitelist** and enter the group names from the external identity provider to propagate in the ID token when a user authenticates.

## Testing

This topic describes how an administrator can test the connection between SSO and PingFederate. An administrator can test both service provider and identity provider connections.

### Test Your Service Provider Connection

1. Log in to Apps Manager at <https://apps.YOUR-SYSTEM-DOMAIN> and navigate to the organization and space where your application is located.
2. Under **Services**, locate the service instance of the Single Sign-On (SSO) plan bound to your application. Click the service instance and then click **Manage**.

The screenshot shows the Apps Manager interface. At the top, there are two tabs: "Overview" (selected) and "Settings". Below these are two main sections: "Apps" and "Services".

**Apps:**

NAME	INSTANCES	MEMORY	LAST PUSH	ROUTE
authcode-sample	1	512MB	4 days ago	<a href="http://authcode-sample.id-service.cf-app.com">http://authcode-sample.id-service.cf-app...</a> >

**Services:**

SERVICE	NAME	BOUND APPS	PLAN
Pivotal Single Sign-On	SI	1	free - (MONTHLY) >

The screenshot shows the management page for the "Pivotal Single Sign-On" service instance. At the top, it displays the SERVICE (Pivotal Single Sign-On), INSTANCE NAME (SI), and SERVICE PLAN (PingFederate PCF SSO). Below this are three tabs: "Manage" (selected), "Docs", and "Support".

**App Binding (1)**

App Binding (1)	Plan	Settings
<b>Bound Apps</b>		<a href="#">Edit Bindings</a>
authcode-sample		

3. Under the **Apps** tab, click your application.

The screenshot shows the Pivotal Apps Manager interface. On the left, there's a button labeled 'NEW APP'. To its right, the 'authcode-sample' application card is displayed. The card includes the app name, 'authcode-sample', its type as a 'Web App', and its identity provider settings: 'Internal Identity Provider' and 'PingFederate PCF SSO'. Below the card, it says 'updated 4 days ago'.

- Under Identity Providers, select the PingFederate identity provider. a

The screenshot shows the configuration page for the 'authcode-sample' application. In the 'Identity Providers' section, two options are listed: 'Internal User Store' and 'PingFederate PCF SSO'. The 'PingFederate PCF SSO' option is highlighted with a red box. Other sections of the form include 'App Name\*' (set to 'authcode-sample'), 'Auth Redirect URIs\*' (containing 'https://authcode-sample.id-service.cf-app.com'), 'Scopes' (with 'todo' and 'todo.read' selected), 'System Provided' (with 'openid' selected), and 'Select Scopes' (which is currently empty). At the bottom, there are 'Delete', 'Cancel', and 'Save Config' buttons.

- Return to Apps Manager and click the URL below your application to authenticate with the identity provider.

**Overview** **Settings**

**Apps**

NAME	INSTANCES	MEMORY	LAST PUSH	ROUTE
authcode-sample	1	512MB	4 days ago	<a href="http://authcode-sample.id-service.cf-app.com">http://authcode-sample.id-service.cf-app... &gt;</a>

6. Click the link to **Log in via Auth Code Grant Type**.

Authcode sample

What do you want to do?

- [Log in via Auth Code Grant Type](#)

7. On the identity provider sign-in page, enter your credentials and click **Sign On**.

Sign On

Username

Password

Login

8. The application asks for authorization to the necessary scopes. Click **Authorize**.

Application Authorization

authcode-sample  
<https://authcode-sample>

authcode-sample has requested permission to access your account. If you do not recognize this application or its URL, you should click deny. The application will not see your password.

openid

Read TODO list

You can change your approval of permissions or revoke access for this application at any time from account settings. By approving access, you agree to authcode-sample's terms of service and privacy policy.

DENY AUTHORIZE

9. View the access token and ID token.

## Authcode sample

You've used the authcode flow! Here's the result of calling /userinfo:

```
{
  "user_id" : "a112e6d9-8a23-47be-8f53-a2142a8e449c",
  "user_name" : "example@pivotal.io",
  "given_name" : "Example",
  "family_name" : "Example",
  "email" : "example@pivotal.io",
  "name" : "Example Example"
}
```

This is the Access Token that was used:

```
{
  "jti" : "22a45c21e05f4c038e146bfb4b27f4d5",
  "sub" : "a112e6d9-8a23-47be-8f53-a2142a8e449c",
  "scope" : [ "todo.read", "openid", "todo.write" ],
  "client_id" : "ac2a00fb-1a04-4ed6-b818-2a4f7bd8c783",
  "cid" : "ac2a00fb-1a04-4ed6-b818-2a4f7bd8c783",
  "azp" : "ac2a00fb-1a04-4ed6-b818-2a4f7bd8c783",
  "grant_type" : "authorization_code",
  "user_id" : "a112e6d9-8a23-47be-8f53-a2142a8e449c",
  "origin" : "PingFederate PCF SSO",
  "user_name" : "example@pivotal.io",
  "email" : "example@pivotal.io",
  "auth_time" : 1466471054,
  "rev_sig" : "df3la473",
  "iat" : 1466471057,
  "exp" : 1466514257,
  "iss" : "https://example.uaa/oauth/token",
  "zid" : "700cdf33-b0df-4b3c-9a9f-d0586782f664",
  "aud" : [ "todo", "ac2a00fb-1a04-4ed6-b818-2a4f7bd8c783", "openid" ]
}
```

This is the ID Token:

```
{
  "sub" : "a112e6d9-8a23-47be-8f53-a2142a8e449c",
  "user_name" : "example@pivotal.io",
  "origin" : "PingFederate PCF SSO",
  "roles" : [ "Everyone" ],
  "iss" : "https://example.uaa/oauth/token",
  "client_id" : "ac2a00fb-1a04-4ed6-b818-2a4f7bd8c783",
  "aud" : [ "ac2a00fb-1a04-4ed6-b818-2a4f7bd8c783" ],
  "zid" : "700cdf33-b0df-4b3c-9a9f-d0586782f664",
  "grant_type" : "authorization_code",
  "user_id" : "a112e6d9-8a23-47be-8f53-a2142a8e449c",
  "azp" : "ac2a00fb-1a04-4ed6-b818-2a4f7bd8c783",
  "scope" : [ "openid" ],
  "auth_time" : 1466471054,
  "exp" : 1466514257,
  "iat" : 1466471057,
  "jti" : "22a45c21e05f4c038e146bfb4b27f4d5",
  "email" : "example@pivotal.io",
  "rev_sig" : "df3la473",
  "cid" : "ac2a00fb-1a04-4ed6-b818-2a4f7bd8c783"
}
```

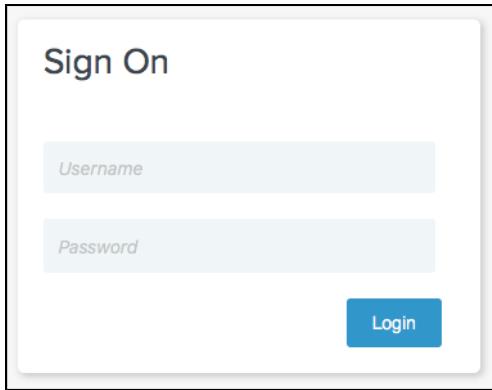
## What do you want to do?

- [TODO List \(You need to configure the Resource Server sample app before using this\)](#)
- [See your account profile \(so you can de-authorize this client\)](#)
- [Log out](#)

## Test Your Identity Provider Connection

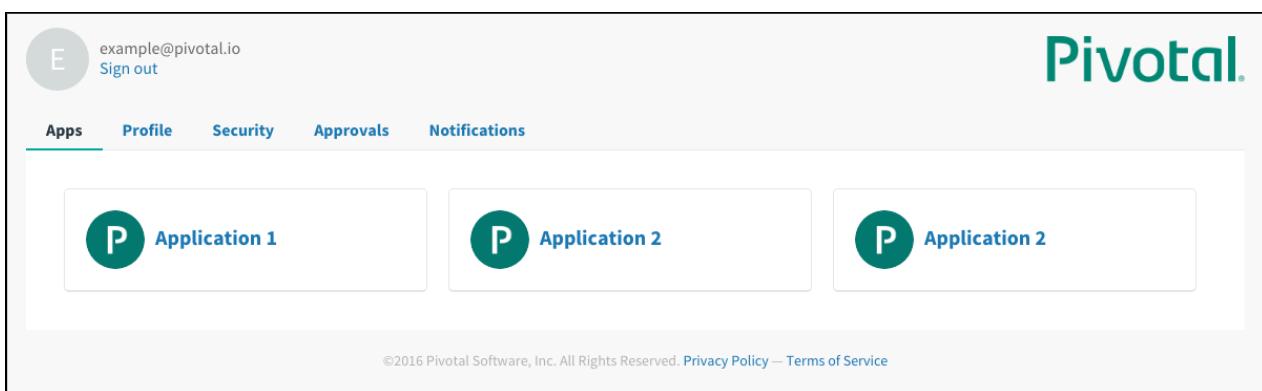
 Note: SSO does not support identity provider-initiated flow into applications, but it does redirect the user to the User Account and Authentication (UAA) page to select applications assigned to the user.

1. Sign in to PingFederate.



The image shows a 'Sign On' form with a light gray background. It contains two input fields: 'Username' and 'Password', both with placeholder text. Below the fields is a blue 'Login' button.

2. Navigate to your application and click it.
3. View the list of applications you have access to.

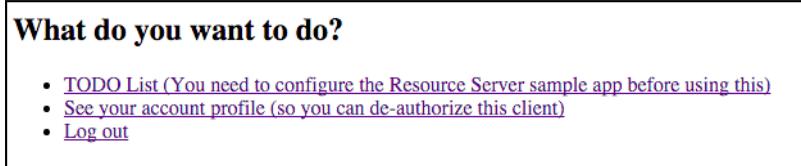


The image shows a user interface for managing applications. At the top left is a profile icon with the letter 'E' and the email 'example@pivotal.io'. To its right are 'Sign out' and the Pivotal logo. Below this is a navigation bar with tabs: 'Apps' (which is underlined in green), 'Profile', 'Security', 'Approvals', and 'Notifications'. The main content area displays three application cards, each featuring a teal circular icon with a white 'P' and the text 'Application 1' or 'Application 2'. At the bottom of the page is a copyright notice: '©2016 Pivotal Software, Inc. All Rights Reserved. [Privacy Policy](#) — [Terms of Service](#)'.

## Test Your Single Sign-Off

Test single sign-off to ensure that when users log out of the application, they are logged out of PingFederate as well.

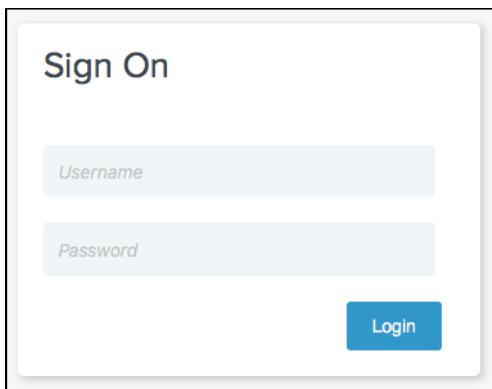
1. Sign into the sample application. Information about the access and ID token displays, as well as the "What do you want to do?" section.
2. Under **What do you want to do?**, click **Log out**.



The image shows a modal window titled 'What do you want to do?'. Inside, there is a list of options:

- [TODO List \(You need to configure the Resource Server sample app before using this\)](#)
- [See your account profile \(so you can de-authorize this client\)](#)
- [Log out](#)

3. Ensure that you are logged out and redirected to the PingFederate login page.



The image shows a 'Sign On' form with a light gray background, identical to the one at the top of the page. It contains two input fields: 'Username' and 'Password', both with placeholder text. Below the fields is a blue 'Login' button.

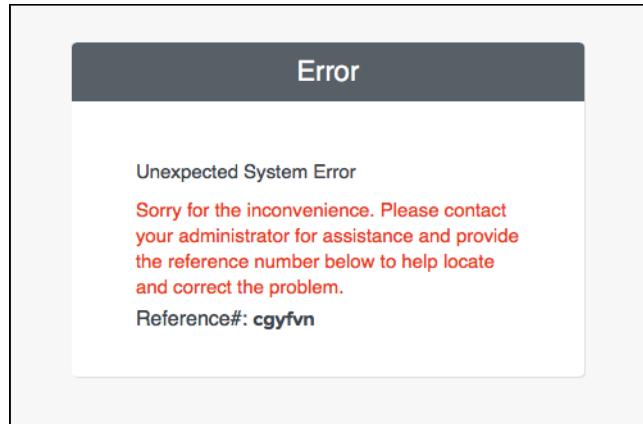


## Troubleshooting

This topic describes how to resolve common errors that arise when configuring a single sign-on partnership between PingFederate and Pivotal Single Sign-On (SSO).

### Error

Symptom:

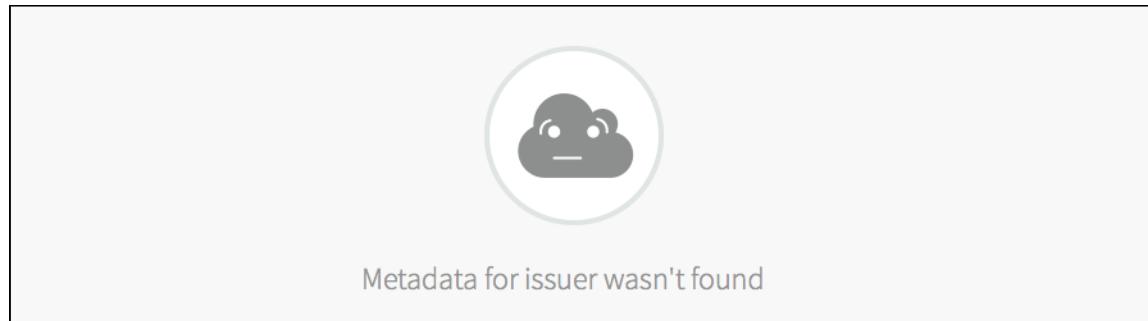


Explanations:

- Connection Status is disabled on PingFederate.
- The service provider Entity ID is misconfigured on PingFederate.
- The identity provider Single Sign-On URL is misconfigured in the SSO plan settings.

### Metadata Not Found

Symptom:



Explanation:

- The identity provider Entity ID is misconfigured in the SSO plan settings.

## PingOne Cloud Integration Guide Overview

PingOne Cloud is an identity-as-a-service solution that delivers secure single sign-on to SaaS, legacy and web applications. This documentation describes how to configure a single sign-on partnership between PingOne Cloud as the Identity Provider (IdP) and the Single Sign-On Service (SSO) for Pivotal Cloud Foundry as the Service Provider (SP).

SSO supports service provider-initiated authentication flow and single logout. It does not support identity provider-initiated authentication flow. All SSO communication takes place over SSL.

## Prerequisites

To integrate PingOne Cloud with Pivotal Cloud Foundry (PCF), you need:

### Pivotal

- PCF, version 1.7.0 or later.
- Single Sign-On, version 1.1.0 or later.

### PingOne Cloud

- PingOne Cloud
- A user with Application Admin privileges.

 **Note:** To configure SAML, you must have the Single Sign-On service broker installed on your PCF deployment. You need to create a plan, grant any plan administrators, and specify any organizations this plan should be the authentication authority for. For help configuring plans, see the [Manage Service Plans](#) topic..

## PingOne Cloud Integration Guide

### Configuring PingOne Cloud with SSO

Complete both steps below to integrate your deployment with PingOne Cloud and SSO.

1. [Configure PingOne Cloud as an Identity Provider](#)
2. [Configure a Single Sign-On Service Provider](#)

### Testing and Troubleshooting

- [Testing](#)
- [Troubleshooting](#)

## Configure PingOne Cloud as an Identity Provider

This topic describes how to set up PingOne Cloud as your identity provider by configuring SAML integration in both Pivotal Cloud Foundry (PCF) and PingOne Cloud.

### Set up SAML in PCF

1. Log into the Single Sign-On (SSO) dashboard at <https://p-identity.YOUR-SYSTEM-DOMAIN> as a Plan Administrator.
2. Select your plan and click **Manage Identity Providers** on the dropdown menu.

The screenshot shows the 'Plans' section of the PCF SSO dashboard. A dropdown menu is open under a plan named 'PingOne PCF SSO'. The 'Manage Identity Providers' option is highlighted with a red box.

3. Click **Configure SAML Service Provider**.

The screenshot shows the 'Identity Providers' section of the PCF SSO dashboard. Under the 'PingOne PCF SSO' provider, the 'Configure SAML Service Provider' button is highlighted with a red box.

4. (Optional) Select **Perform signed authentication requests** to enforce SSO private key signature and identity provider validation.

The screenshot shows the 'Configure SAML Service Provider' dialog. The 'Perform signed authentication requests' checkbox is checked. The 'Save' button is highlighted with a blue box.

5. (Optional) Select **Require signed assertions** to validate the origin of signed responses.

6. Click **Download Metadata** to download the service provider metadata.

7. Click **Save**.

### Set up SAML in PingOne Cloud

1. Sign in as a PingOne Cloud administrator.
2. Navigate to your application by clicking on the **Applications** tab.
3. Click the **Add Application** button and choose **New SAML Application**.

The screenshot shows the Ping Identity application management interface. At the top, there's a navigation bar with links for Dashboard, Applications (which is selected and highlighted in blue), Users, Setup, Account, Help, and Sign Off. Below the navigation bar, there are two tabs: 'My Applications' (selected) and 'Application Catalog'. The main content area is titled 'My Applications' and contains a message stating: 'Applications you've added to your account are listed here.' followed by a bulleted list: '• Active applications are enabled for single sign-on (SSO). • Details displays the application details.' Below this, there's a search bar labeled 'Search Application Catalog' and a button labeled 'Add Application'. Underneath the search bar, there are three options: 'New SAML Application' (highlighted with a red box), 'New Basic SSO Application', and a link to 'Request Ping Identity add a new application to the application catalog'. On the right side of the main content area, there's a button labeled 'Pause All SSO'.

4. Enter the Application Name, Application Description, Category and any Graphics.

5. Click the Continue to Next Step button to configure SAML.

## 2. Application Configuration

I have the SAML configuration

I have the SSO URL

You will need to download this SAML metadata to configure the application:

SAML Metadata [Download](#)

Provide SAML details about the application you are connecting to:

Protocol Version  SAML v 2.0  SAML v 1.1

Upload Metadata  [Select File](#) [Or use URL](#)

Assertion Consumer Service (ACS)  \*

Entity ID  \*

Application URL

Single Logout Endpoint   https://example.login.id-service.cf-app

Single Logout Response Endpoint

Single Logout Binding Type  Redirect  Post

Verification Certificate  [Choose File](#) No file chosen  
saml20metadata.cer

Signing Algorithm

Force Re-authentication

Keep the following in mind when creating your connection:

1. Both SP- and IdP-Initiated SSO are allowed
2. Map SAML SUBJECT in your attribute contract, plus any attributes (configure them in PingOne later)
3. Allow outbound POST or redirect bindings
4. Allow inbound POST

NEXT: SSO Attribute Mapping

[Cancel](#)

[Back](#)

[Continue to Next Step](#)

6. In the **Application Configuration** section, perform the following steps:

- a. Select **I have the SAML configuration**.
- b. For **SAML Metadata**, click [Download](#) to download the identity provider metadata.
- c. For **Protocol Version**, select **SAML v 2.0**.
- d. For **Upload Metadata**, click [Select File](#) and select the service provider metadata.
- e. Click the [Continue to Next Step](#) button.

7. (Optional) Under **SSO Attribute Mapping**, specify any application or group attributes that you want to map to users in the ID token.

### 3. SSO Attribute Mapping

Map the necessary application provider (AP) attributes to attributes used by your identity provider (IdP).

	Application Attribute	Identity Bridge Attribute or Literal Value	Required
1	firstName	First Name <input type="checkbox"/> As Literal <input type="button" value="Advanced"/>	<input type="checkbox"/> <input type="button" value="X"/>
2	lastName	Last Name <input type="checkbox"/> As Literal <input type="button" value="Advanced"/>	<input type="checkbox"/> <input type="button" value="X"/>
3	email	Email <input type="checkbox"/> As Literal <input type="button" value="Advanced"/>	<input type="checkbox"/> <input type="button" value="X"/>
4	group	memberOf <input type="checkbox"/> As Literal <input type="button" value="Advanced"/>	<input type="checkbox"/> <input type="button" value="X"/>

**NEXT: Review Setup**

- Click the **Save & Publish** button followed by the **Finish** button.

## Configure a Single Sign-On Service Provider

This topic describes how to add an external identity provider to your Pivotal Single Sign-On (SSO) service plan.

### Configure Identity Provider Metadata

1. Edit the Identity Provider Metadata file which is typically named `saml2-metadata-idp.xml`.

- The Single Sign-On service requires that the Name ID Format is specified. Replace the following text:

```
<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" Name="PingOne.idpid"
 xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"/>
```

with:

```
<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" Name="PingOne.idpid"
 xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"/> <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
 format:unspecified</md:NameIDFormat>
```

### Setting up SAML

1. Log into the SSO dashboard at <https://p-identity.YOUR-SYSTEM-DOMAIN> as a Plan Administrator.

2. Select your plan and click **Manage Identity Providers** on the dropdown menu.

The screenshot shows a user interface for managing a Pivotal SSO plan. At the top, there's a navigation bar with 'Plans 1' and a 'New Plan' button. Below this, a table lists one item: 'PingOne PCF SSO' under the 'Name' column and 'example' under the 'Sign In Header' column. At the bottom of the table, there are two buttons: 'Edit Plan' and 'Manage Identity Providers'. The 'Manage Identity Providers' button is highlighted with a red rectangular box.

3. Click **New Identity Provider** to create a new identity provider.

### New Identity Provider

**Identity Provider Name\***  
 This name will show as a link on the login page

**Identity Provider Description**  
Allows  Enter a group name to authenticate.

**Identity Provider Type\***  
SAML

### Identity Provider Metadata

**Identity Provider Metadata URL\***

**Fetch Metadata**  
▶ SAML File Metadata (optional)

**Advanced SAML Settings**  
▶ Attribute mappings (optional)

Cancel Create Identity Provider

4. To create a new identity provider, perform the following steps:
  - a. Enter an identity provider name into **Identity Provider Name**.
  - b. (Optional) Enter a description into **Identity Provider Description**.
  - c. Click **SAML File Metadata (optional)** followed by clicking the **Upload Identity Provider Metadata** button to upload your metadata XML.
  - d. (Optional) Under **Advanced SAML Settings**, click **Attribute Mappings** to enter the mappings.
5. Click **Create Identity Provider**.
6. Click **Resource Permissions**.
7. Click **New Permissions Mapping** and perform the following steps:
  - a. Enter a **Group Name**.
  - b. For **Select Permissions**, select the permissions that the members of the group from the external identity provider should have access to.
8. Navigate to the identity provider list.
9. Click **Group Whitelist** and enter the group names from the external identity provider that should be propagated in the ID token.

## Testing

This topic describes how an administrator can test the connection between SSO and PingOne Cloud. An administrator can test both service provider and identity provider connections.

### Test Your Service Provider Connection

1. Log in to Apps Manager at <https://apps.YOUR-SYSTEM-DOMAIN> and navigate to the organization and space where your application is located.
2. Under **Services**, locate the service instance of the Single Sign-On (SSO) plan bound to your application. Click on the service instance and click **Manage**.

The screenshot shows the Apps Manager interface. At the top, there are two tabs: "Overview" (selected) and "Settings". Below these are two main sections: "Apps" and "Services".

**Apps:**

NAME	INSTANCES	MEMORY	LAST PUSH	ROUTE
authcode-sample	1	512MB	4 days ago	<a href="http://authcode-sample.id-service.cf-ap...">http://authcode-sample.id-service.cf-ap...</a> >

**Services:**

SERVICE	NAME	BOUND APPS	PLAN
Pivotal Single Sign-On	SI	1	free - (MONTHLY) >

The screenshot shows the details of the "Pivotal Single Sign-On" service instance. At the top, it displays the SERVICE, INSTANCE NAME (SI), and SERVICE PLAN (PingOne PCF SSO). Below this are three buttons: "Manage" (which is highlighted with a red box), "Docs", and "Support".

Below the service details, there are three tabs: "App Binding (1)" (selected), "Plan", and "Settings".

**App Binding (1):**

Bound Apps	Edit Bindings
authcode-sample	<a href="#">Edit Bindings</a>

3. Under the **Apps** tab, click your application.

The screenshot shows the Pivotal Apps Manager interface. On the left, there's a button labeled 'NEW APP'. To its right, the application 'authcode-sample' is listed. It is categorized as a 'Web App' and uses 'Internal Identity Provider' and 'PingOne PCF SSO' for authentication. The status bar indicates it was 'updated 4 days ago'.

- Under Identity Providers, select the PingOne identity provider.

The screenshot shows the configuration page for the 'authcode-sample' application. In the 'Identity Providers' section, two options are listed: 'Internal User Store' and 'PingOne PCF SSO'. The 'PingOne PCF SSO' option is highlighted with a red box. Below this section, there are fields for 'Auth Redirect URIs\*', 'Scopes', 'Select Scopes', and 'Auto-Approved Scopes'. At the bottom right, there are 'Cancel' and 'Save Config' buttons.

- Return to Apps Manager and click on the URL below your application to be redirected to the identity provider to authenticate.

**Overview** **Settings**

**Apps**

NAME	INSTANCES	MEMORY	LAST PUSH	ROUTE
authcode-sample	1	512MB	4 days ago	<a href="http://authcode-sample.id-service.cf-app.net">http://authcode-sample.id-service.cf-app... &gt;</a>

6. Click the link.

Authcode sample

What do you want to do?

- Log in via Auth Code Grant Type

7. On the identity provider sign-in page, enter your credentials and click **Sign On**.

Ping Identity

Sign On

USERNAME

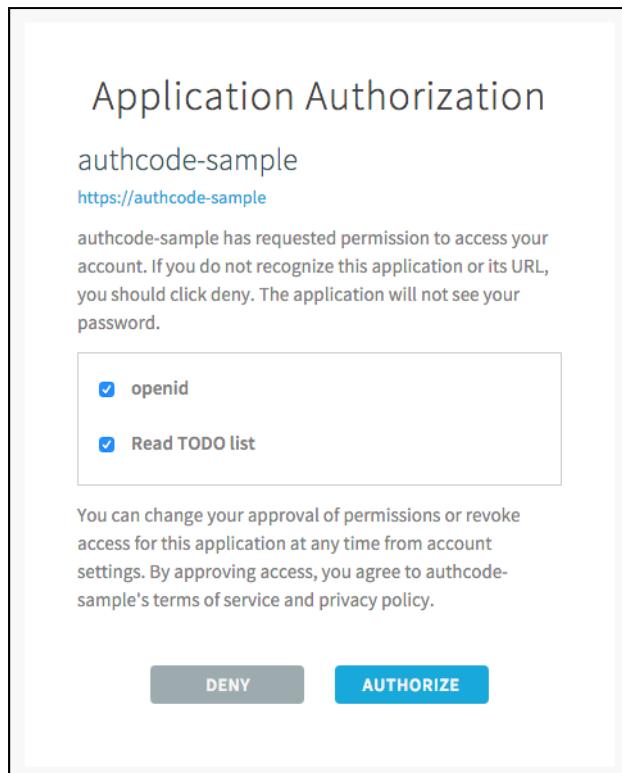
PASSWORD

Remember Me

Sign On

[Forgot Password](#)

8. The application asks for authorization to the necessary scopes. Click **Authorize**.



9. The access token and ID token displays.

## Authcode sample

You've used the authcode flow! Here's the result of calling /userinfo:

```
{  
  "user_id" : "1bd4153a-08eb-4aed-bb9c-929b45df026d",  
  "user_name" : "example@pivotal.io",  
  "given_name" : "Example",  
  "family_name" : "Example",  
  "email" : "example@pivotal.io",  
  "name" : "Example Example"  
}
```

This is the Access Token that was used:

```
{  
  "jti" : "c1148dda64a840589b2936deba1149a9",  
  "sub" : "1bd4153a-08eb-4aed-bb9c-929b45df026d",  
  "scope" : [ "todo.read", "openid", "todo.write" ],  
  "client_id" : "27b2d43c-2f0d-48e8-979c-b11f841e972d",  
  "cid" : "27b2d43c-2f0d-48e8-979c-b11f841e972d",  
  "azp" : "27b2d43c-2f0d-48e8-979c-b11f841e972d",  
  "grant_type" : "authorization_code",  
  "user_id" : "1bd4153a-08eb-4aed-bb9c-929b45df026d",  
  "origin" : "PingOne PCF SSO",  
  "user_name" : "example@pivotal.io",  
  "email" : "example@pivotal.io",  
  "auth_time" : 1465240181,  
  "rev_sig" : "f59bcff6",  
  "iat" : 1465240182,  
  "exp" : 1465283382,  
  "iss" : "https://example.uaa/oauth/token",  
  "zid" : "23835dc6-7f12-4c27-bf22-3ed29923d590",  
  "aud" : [ "todo", "openid", "27b2d43c-2f0d-48e8-979c-b11f841e972d" ]  
}
```

This is the ID Token:

```
{  
  "sub" : "1bd4153a-08eb-4aed-bb9c-929b45df026d",  
  "user_name" : "example@pivotal.io",  
  "origin" : "PingOne PCF SSO",  
  "iss" : "https://example.uaa/oauth/token",  
  "client_id" : "27b2d43c-2f0d-48e8-979c-b11f841e972d",  
  "aud" : [ "27b2d43c-2f0d-48e8-979c-b11f841e972d" ],  
  "zid" : "23835dc6-7f12-4c27-bf22-3ed29923d590",  
  "grant_type" : "authorization_code",  
  "user_id" : "1bd4153a-08eb-4aed-bb9c-929b45df026d",  
  "azp" : "27b2d43c-2f0d-48e8-979c-b11f841e972d",  
  "scope" : [ "openid" ],  
  "auth_time" : 1465240181,  
  "exp" : 1465283382,  
  "iat" : 1465240182,  
  "jti" : "c1148dda64a840589b2936deba1149a9",  
  "email" : "example@pivotal.io",  
  "rev_sig" : "f59bcff6",  
  "cid" : "27b2d43c-2f0d-48e8-979c-b11f841e972d"  
}
```

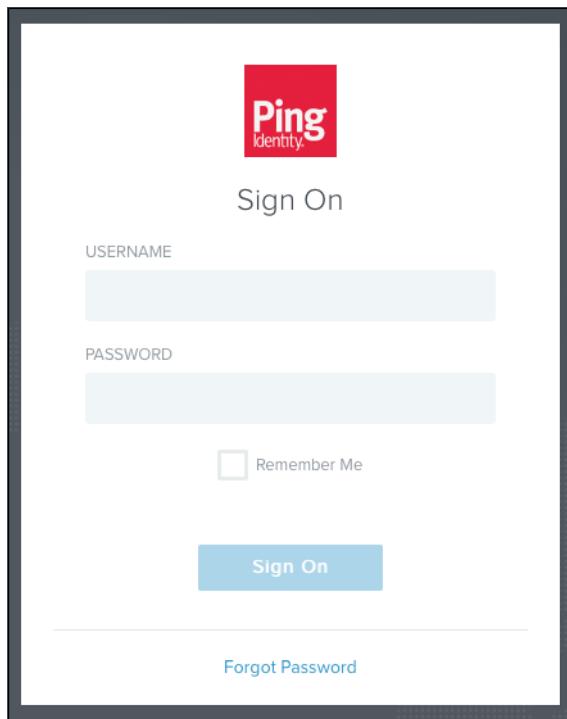
## What do you want to do?

- [TODO List \(You need to configure the Resource Server sample app before using this\)](#)
- [See your account profile \(so you can de-authorize this client\)](#)
- [Log out](#)

## Test Your Identity Provider Connection

 Note: SSO does not support identity provider-initiated flow into applications, but it does redirect the user to the User Account and Authentication (UAA) page to select applications assigned to the user.

1. Sign in to PingOne.



2. Navigate to your application and click it.
3. You are redirected to the page that lists applications you have access to.

A screenshot of a Pivotal application dashboard. At the top left is a user profile icon with the letter "E" and the email "example@pivotal.io", with a "Sign out" link. At the top right is the Pivotal logo. Below the header is a navigation bar with tabs: Apps (which is underlined), Profile, Security, Approvals, and Notifications. The main content area shows three application cards, each with a teal "P" icon and the text "Application 1", "Application 2", and "Application 2" respectively. At the bottom of the page is a footer with the text "©2016 Pivotal Software, Inc. All Rights Reserved. [Privacy Policy](#) — [Terms of Service](#)".

## Test Your Single Sign-Off

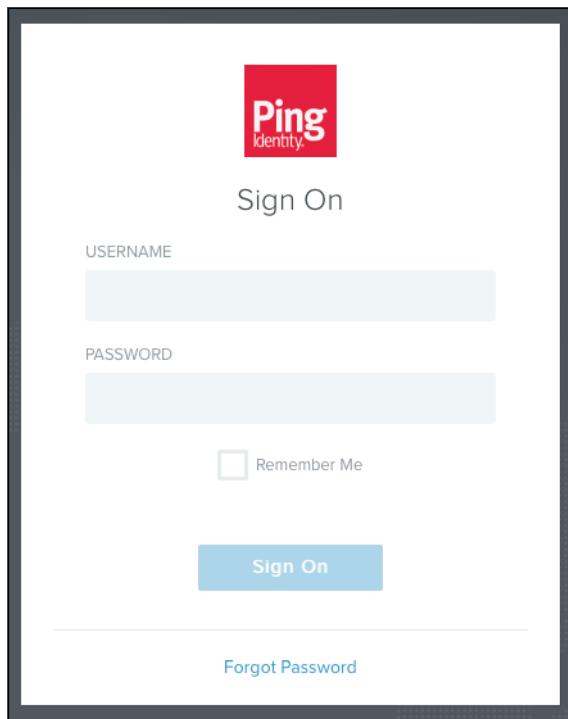
Test single sign-off to ensure that when users log out of the application, they are logged out of PingOne as well.

1. Sign into the sample application. Information about the access and ID token displays, as well as the "What do you want to do?" section.
2. Under "What do you want to do?", click **Log out**.

### What do you want to do?

- [TODO List \(You need to configure the Resource Server sample app before using this\)](#)
- [See your account profile \(so you can de-authorize this client\)](#)
- [Log out](#)

3. You are logged out and redirected to the PingOne login page.

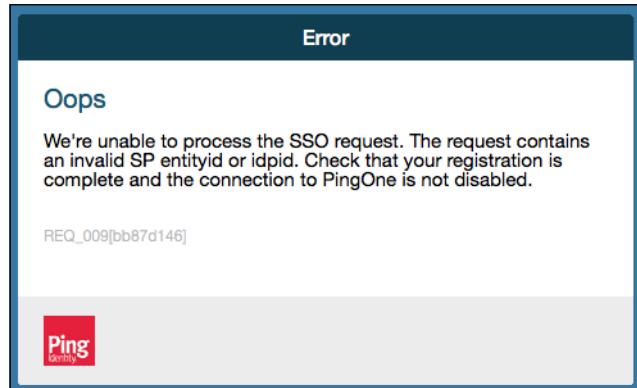


## Troubleshooting

This topic describes how to resolve common errors that arise when configuring a single sign-on partnership between PingOne Cloud and Pivotal Single Sign-On (SSO).

### Error

Symptom:

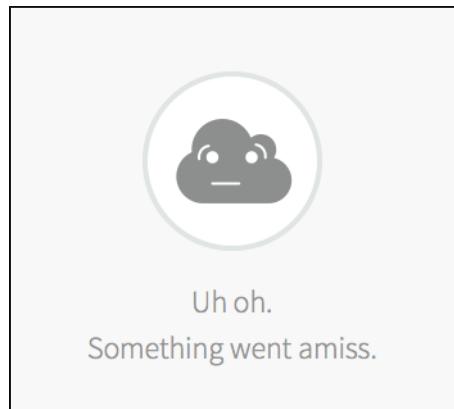


Explanations:

- Single Sign-On is disabled on PingOne.
- The service provider Entity ID is misconfigured on PingOne.
- The identity provider Single Sign-On URL is misconfigured in the SSO plan settings.

### Something went amiss

Symptom:

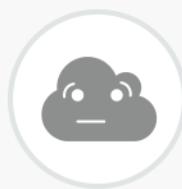


Explanation:

- The service provider Assertion Consumer Service (ACS) is misconfigured on PingOne.

## Metadata Not Found

Symptom:



Metadata for issuer https://pingone.com/idp/cd-2128514304.pivotal wasn't found

Explanation:

- The identity provider Entity ID is misconfigured in the SSO plan settings.

## Missing Name ID

Symptom:

Identity Provider Metadata

Identity Provider Metadata URL\*

**Fetch Metadata**

Error processing metadata

▼ SAML File Metadata (optional)

**Upload Identity Provider Metadata** saml2-metadata-idp.xml

Explanation:

- The identity provider metadata is missing configurations for Name ID. See [Configure Identity Provider Metadata](#).

## Release Notes

### View Release Notes for Another Version

To view the release notes for another product version, select the version from the drop-down list at the top of this page.

#### v1.1.x

##### v1.1.1

Release date: 5 May 2016

- Single Sign-On (SSO) for Pivotal Cloud Foundry (PCF) now defaults the access token and refresh token validity time to UAA defaults, 12 hours and 30 days, respectively. For any plans created in SSO 1.1.0, please resolve this bug in one of the following ways:
  - Option 1: Recreate the plan(s) created in SSO 1.1.0.
  - Option 2: Edit the identity zone within UAA and set your desired token validity time.
- PCF updated stemcell to 3232.2. This is a security upgrade that resolves the following:
  - [USN-2959-1](#)
  - [USN-2957-1](#)
  - [USN-2949-1](#)
  - [USN-2943-1](#)
  - [USN-2935-2](#)
- [Updated 18 May 2016] PCF updated stemcell to 3232.4. This is a security upgrade that resolves the following:
  - [USN-2977-1](#)
- [Updated 10 June 2016] PCF updated stemcell to 3232.6. This is a security upgrade that resolves the following:
  - [USN-2966-1](#)
  - [USN-2970-1](#)
  - [USN-2981-1](#)
  - [USN-2983-1](#)
  - [USN-2985-1](#)
  - [USN-2985-2](#)
  - [USN-2994-1](#)
- [Updated 14 June 2016] PCF updated stemcell to 3232.8. This is a security upgrade that resolves the following:
  - [USN-3001-1](#)
- [Updated 30 June 2016] PCF updated stemcell to 3232.12. This is a security upgrade that resolves the following:
  - [USN-3020-1](#)

Additional information can be found at <https://pivotal.io/security>.

#### v1.1.0

Release date: 29 April 2016

##### What's New

-  Note: The Single Sign-On service tile [operates in lockstep with Pivotal Elastic Runtime](#).
  - The SSO v1.0.x tiles are compatible with [PCF v1.6.x](#)
  - The SSO v1.1.x tiles are compatible with [PCF v1.7.x](#)

If you are a customer upgrading from PCF 1.6 to PCF 1.7 and you are using SSO v1.0.x, you must update to the SSO v1.1.0 service tile before proceeding with the upgrade.

- Single Sign-On (SSO) for Pivotal Cloud Foundry (PCF) provides the ability for PCF Administrators to delete plans.
- SSO provides the ability for administrators to delete identity providers.
- SSO now supports SAML NameID other than email address.
- SSO provides the ability for administrators to manage SAML assertion signing configurations.
- SSO provides support for propagation of user attributes and group memberships from external identity providers in OpenID Connect tokens.
- SSO provides the ability for administrators to assign API permissions to users through External Group Mappings with external identity providers.
- SSO provides the ability to Group Whitelist groups so that they will be sent in the ID token.
- SSO provides the ability for administrators to set password and lockout policy for internal users.
- SSO provides the ability for developers to create resources and permissions for clients.
- SSO now supports SAML single logout flow which ends UAA and external identity provider sessions.

## v1.0.16

Release date: 23 August 2016

- PCF updated stemcell to 3232.17. This is a security upgrade that resolves the following:
  - [USN-3064-1](#)

Additional information can be found at <https://pivotal.io/security>.

## v1.0.15

Release date: 30 June 2016

- PCF updated stemcell to 3232.12. This is a security upgrade that resolves the following:
  - [USN-3020-1](#)

Additional information can be found at <https://pivotal.io/security>.

## v1.0.14

Release date: 14 June 2016

- PCF updated stemcell to 3232.8. This is a security upgrade that resolves the following:
  - [USN-3001-1](#)

Additional information can be found at <https://pivotal.io/security>.

## v1.0.13

Release date: 10 June 2016

- PCF updated stemcell to 3232.6. This is a security upgrade that resolves the following:
  - [USN-2966-1](#)
  - [USN-2970-1](#)
  - [USN-2981-1](#)
  - [USN-2983-1](#)
  - [USN-2985-1](#)
  - [USN-2985-2](#)
  - [USN-2994-1](#)

Additional information can be found at <https://pivotal.io/security>.

## v1.0.12

Release date: 18 May 2016

- PCF updated stemcell to 3232.4. This is a security upgrade that resolves the following:
  - [USN-2977-1 ↗](#)

Additional information can be found at <https://pivotal.io/security> ↗.

## v1.0.11

Release date: 5 May 2016

- PCF updated stemcell to 3146.11. This is a security upgrade that resolves the following:
  - [USN-2959-1 ↗](#)
  - [USN-2957-1 ↗](#)
  - [USN-2949-1 ↗](#)
  - [USN-2943-1 ↗](#)
  - [USN-2935-2 ↗](#)

Additional information can be found at <https://pivotal.io/security> ↗.

## v1.0.10

Release date: 16 March 2016

- PCF updated stemcell to 3146.10. This is a security upgrade that resolves the following:
  - [CVE-2016-0800 ↗](#)

Additional information can be found at <https://pivotal.io/security> ↗.

## v1.0.9

Release date: 24 February 2016

- PCF updated stemcell to 3146.9. This is a security upgrade that resolves the following:
  - [USN-2910-1 ↗](#)

Additional information can be found at <https://pivotal.io/security> ↗.

## v1.0.8

Release date: 19 February 2016

- PCF updated stemcell to 3146.8. This is a security upgrade that resolves the following:
  - [USN-2900-1 ↗](#), a critical GNU C lib (glibc) CVE
  - [USN-2897-1 ↗](#)
  - [USN-2896-1 ↗](#)

Additional information can be found at <https://pivotal.io/security> ↗.

## v1.0.7

Release date: 2 February 2016

- PCF updated stemcell to 3146.6. This is a security upgrade that resolves the following:

- [USN-2882-1 ↗](#)
- [USN-2879-1 ↗](#)
- [USN-2875-1 ↗](#)
- [USN-2874-1 ↗](#)
- [USN-2871-1 ↗](#)
- [USN-2868-1 ↗](#)
- [USN-2865-1 ↗](#)
- [USN-2861-1 ↗](#)

Additional information can be found at <https://pivotal.io/security> ↗.

## v1.0.6

Release date: 22 January 2016

- PCF updated stemcell to 3146.5. This is a security upgrade that resolves the following:
  - [USN-2871-1 ↗](#)

Additional information can be found at <https://pivotal.io/security> ↗.

## v1.0.5

Release date: 18 January 2016

- PCF updated stemcell to 3146.3. This is a security upgrade that resolves the following:
  - [USN-2869-1 ↗](#)
  - [CVE-2016-0715 ↗](#).

Additional information can be found at <https://pivotal.io/security> ↗.

## v1.0.4

Release date: 07 January 2016

- PCF updated stemcell to 3146.2. This is a security upgrade that resolves the following Ubuntu Security Notices:
  - [USN-2857-1 ↗](#)
  - [USN-2842-1 ↗](#)
  - [USN-2842-2 ↗](#)
  - [USN-2836-1 ↗](#)
  - [USN-2834-1 ↗](#)
  - [USN-2830-1 ↗](#)
  - [USN-2829-1 ↗](#)

Additional information can be found at <https://pivotal.io/security> ↗.

## v1.0.3

Release date: 03 December 2015

- PCF updated stemcell to 3146. This is a security upgrade that resolves the following Ubuntu Security Notices:
  - [USN-2821-1 ↗](#)

Additional information can be found at <https://pivotal.io/security> ↗.

## v1.0.2

Release date: 14 November 2015

- PCF updated stemcell to 3130. This is a security upgrade that resolves the following Ubuntu Security Notices:

- [USN-2806-1 ↗](#)
- [USN-2798-1 ↗](#)

Additional information can be found at <https://pivotal.io/security>.

## v1.0.1

**Release date:** 02 November 2015

- PCF updated stemcell to 3112. This is a security upgrade that resolves the following Ubuntu Security Notices:

- [USN-2778-1 ↗](#)

Additional information can be found at <https://pivotal.io/security>.

## v1.0.0

**Release date:** 2 November 2015

### What's New

- Single Sign-On (SSO) for Pivotal Cloud Foundry (PCF) introduces an easy-to-use self-service user interface for tenant management and identity provider on-boarding.
- SSO introduces an interface for registering applications and associating identity providers for applications.
- SSO allows developers to integrate applications with SAML 2.0 based enterprise identity providers.
- SSO secure all types of applications (web, mobile, and native), as well as the API's hosted on and off of the PCF platform.
- SSO secures Java applications with a single click via the SSO Service Connector.
- SSO supports multi-tenancy to allow for segregation of applications and identities based on the unique needs of the organization.
- SSO supports role-based access controls for Plan Administrators and Space Developers.
- SSO includes an OAuth 2.0 Authorization Server with support for all four OAuth 2.0 grant types.
- SSO is certified with industry-leading federated identity providers including CA Single Sign-On, Ping Identity, OpenAM, VMware Identity Management, Okta and more.