Pivotal Cloud Foundry®

Security and Single Sign-On (SSO)

For the platform and hosted applications

Pivotal

Topics

- **UAA Overview**
- Cloud Foundry Platform Users
- Pivotal SSO Service
- Service Plans

This module shows how OAuth 2.0 is implemented in Cloud Foundry, securing the platform and allowing you to secure your cloud-native applications

User Authentication and Authorization (UAA) Server-Overview (1 of 2)

- Multi-tenant component of the Elastic Runtime
- Secures Elastic Runtime components, applications and APIs (e.g. Apps Manager and Cloud Controller API)
  - Can also secure access to other applications/APIs using the Pivotal Single Sign-On (SSO) Service
- Open source component based on industry standards such as SAML, OAuth 2.0 and OpenID Connect

Pivotal

User Authentication and Authorization (UAA) Server-Overview (2 of 2)

- Authenticates users
  - Can store user credentials internally or using an external identity provider (Ping Identity, CA SSO, Azure ADFS, Okta ...)
- Acts as an authorization server
  - Issues tokens to client applications on behalf of users
  - Enables the convenience and security of single sign-on (SSO) for platform applications (e.g. Apps Manager) and other applications (using the Pivotal SSO Service)

Pivotal

Topics

- UAA Overview
- **Cloud Foundry Platform Users**
- Pivotal SSO Service
- Service Plans

Pivotal

Cloud Foundry Platform Users

- Cloud Foundry platform users are developers and operators using platform applications like Apps Manager or the cf CLI
- There are three ways to store platform user credentials:
  1. Internal store- user information is stored in the UAA database
  2. LDAP- user information is stored in an LDAP server
     - Configured on the Elastic Runtime's *LDAP Config* tab
  3. Enterprise Identity Provider- user information is stored in an external service like CA SSO or ADFS
     - Configured on the Elastic Runtime's *SSO Config* tab
     - This is the recommended approach for external platform users- it is more secure than LDAP

Note: Populate the LDAP Config tab or the SSO Config tab, but not both

Pivotal

1) Using the Internal Store for Platform Users

- The internal store uses the UAA database
- Users can be added using Apps Manager
- They can also be added with the cf CLI

sbyrnes — -bash — 69×7

```
greylag:~ sbyrnes$ cf help create-user
NAME:
   create-user - Create a new user

USAGE:
   cf create-user USERNAME PASSWORD
```

2) Using LDAP for Platform Users

The Elastic Runtime's LDAP Config tab configures the LDAP integration with the UAA

Pivotal Elastic Runtime

Settings | Status | Credentials | Logs

- Assign Networks
- Assign Availability Zones
- System Database Config
- File Storage Config
- IPs and Ports
- Security Config
- MySQL Proxy Config
- Cloud Controller
- System Logging
- SSO Config
- LDAP Config

Configure an LDAP endpoint for the UAA

Server URL

LDAP Credentials

Username

Password

User Search Base

User Search Filter *

cn={0}

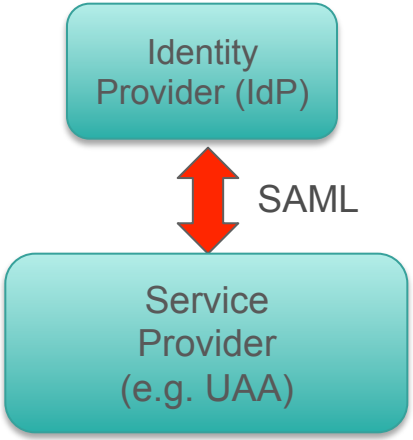
Admin Groups*

No Groups

Enable Admin Groups

Security Assertion Markup Language (SAML)

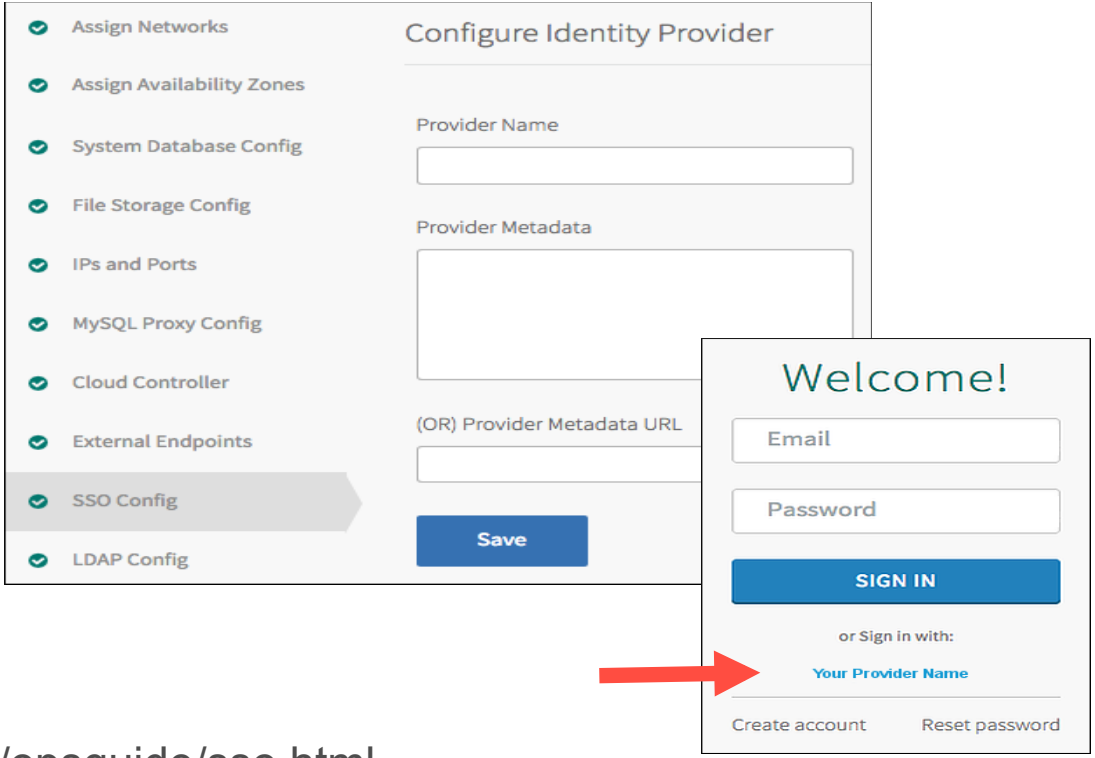
- XML-based, open-standard for exchanging authentication and authorization data between security domains
- In Cloud Foundry, used to exchange user data between an external identity provider and the UAA
- The UAA acts as the service provider



3) Configuring the UAA as a SAML Service Provider

- Use the Elastic Runtime SSO Config tab to configure the UAA as a SAML service provider
- Platform users will have the option to click on the “Your Provider Name” link on the login page
- Your identity provider must also be configured to recognize Cloud Foundry as a service provider

https://docs.pivotal.io/pivotalcf/opsguide/sso.html



Topics

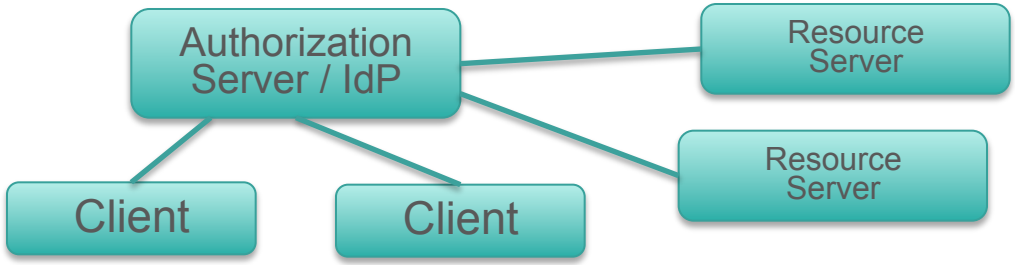
- UAA Overview
- Cloud Foundry Platform Users
- **Pivotal SSO Service**
- Service Plans

Pivotal

Pivotal Single Sign-On Service for Applications

- Provides SSO security and convenience to applications hosted on or external to the Cloud Foundry platform
- Uses an internal user store (the UAA database) or an external SAML 2.0 compliant federated identity provider
  - Certified with Ping Identity, CA SSO, Azure ADFS, ForgeRock Open AM, VMWare Identity Management, Okta
- Implemented as a managed service (available in the marketplace)

The Benefits of SSO



- A main point of SSO is to prevent clients from directly passing user credentials to resource servers
- Pass tokens from the authorization server instead
  - Centralized identity and security policy management
  - Better user experience / avoids multiple logins
  - More secure
  - Scales well in distributed environments (e.g. microservices)

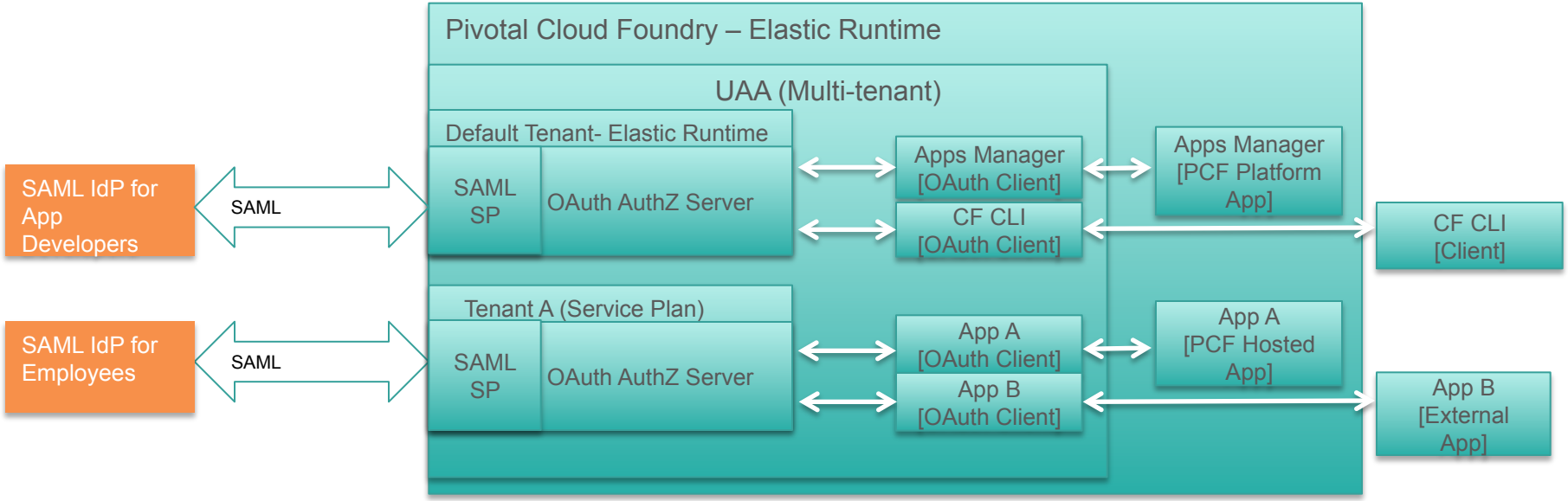
Platform vs. Application SSO

- Platform SSO- Used for securing platform components and applications such as the Cloud Controller or the cf CLI
  - Users are Cloud Foundry operators and developers
- Application SSO- The Pivotal Single Sign-On Service can be used to add security and SSO capabilities to applications
  - The applications can be hosted on or external to the platform

Pivotal

Pivotal Single Sign-on Architecture

- Single high availability multi-tenant UAA for securing platform and hosted applications
- Each tenant gets its own virtual authorization server
- Multiple SAML 2.0 external identity providers are supported
- Each application has an associated OAuth client in the UAA
- All applications must be OAuth 2.0-aware



Configuring an External Identity Provider

- Metadata is exchanged between the service provider and the identity provider (IdP) to establish trust
  - Administrators onboard identity providers using https://p-identity.[system_domain] and the IdP administrative console
  - This is analogous to using the Elastic Runtime's SSO Config tab to configure an external identity provider for platform applications

https://p-identity.coral.springapps.io/dashboard/identity-zones/3b396813-abcf-4a55-9007-19588c5ea3eb/user_stores

Pivotal **Single Sign-On** admin

Plans > Enterprise SSO Plan > User Stores

User Stores 2 **New User Store** Service Provider Metdata

Name	Type
CA SiteMinder	SAML
Internal User Store	Internal User Store

Tasks
- Infrastructure
- Policies
- Federation
  - Partnership Federation
    - Partnerships
    - Entities
    - Metadata Exchange Configurat
    - Authentication Context Templa
  - Legacy Federation
- Reports
- Administration

Entities

To create a new entity, click Create Entity button. To import metadata into an entity, click Import Metadata button. To modify, duplicate, delete or export metadata into an entity, click the corresponding option under Actions button.

Filter Federation Entities

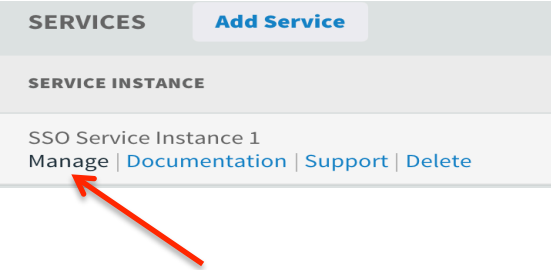
Search For: Entity Id = Search Clear

Federation Entity List Creat Entity Import Metadata

Actions	Entity Name	Entity Id	Location	Entity Type	Partnership Count
Action	smidp	smidp	Local	SAML2 IDP	6
Action	idp2	idp2	Local	SAML2 IDP	0
Action	sfdc	https://myclouddemo-dev-ed.my.salesforce.com	Remote	SAML2 SP	1
Action	uaaacceptance	login.identity.cf-app.com	Remote	SAML2 SP	1
Action	uaazone	testsaml.login.identity.cf-app.com	Remote	SAML2 SP	0
Action	PWS-CF-Identity-Org	ssotest.login.run.pivotal.io	Remote	SAML2 SP	1
		ringdev.login.run.pivotal.io	Remote	SAML2 SP	1
		otest.login.staging.cf-app.com	Remote	SAML2 SP	1
		tp://sso.login.coral.springapps.io	Remote	SAML2 SP	1

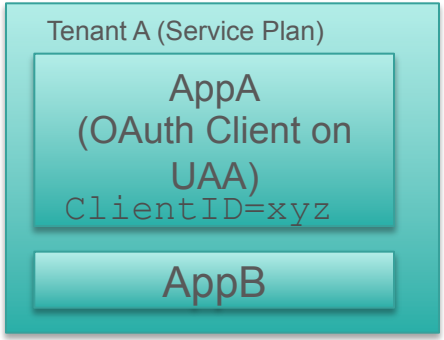
https://www.youtube.com/watch?v=jttpVGpp6Qc

OAuth Clients on the UAA



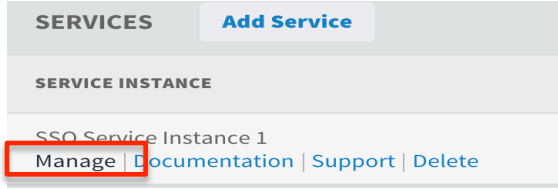
- An OAuth client is created on the UAA for each application
  - When you bind your application to the Pivotal SSO Service…
  - … or register your application from the Pivotal Single Sign-On Service dashboard
- This is the manual client registration stage of OAuth
  - ClientID and ClientSecret are created

UAA (Authorization Server)

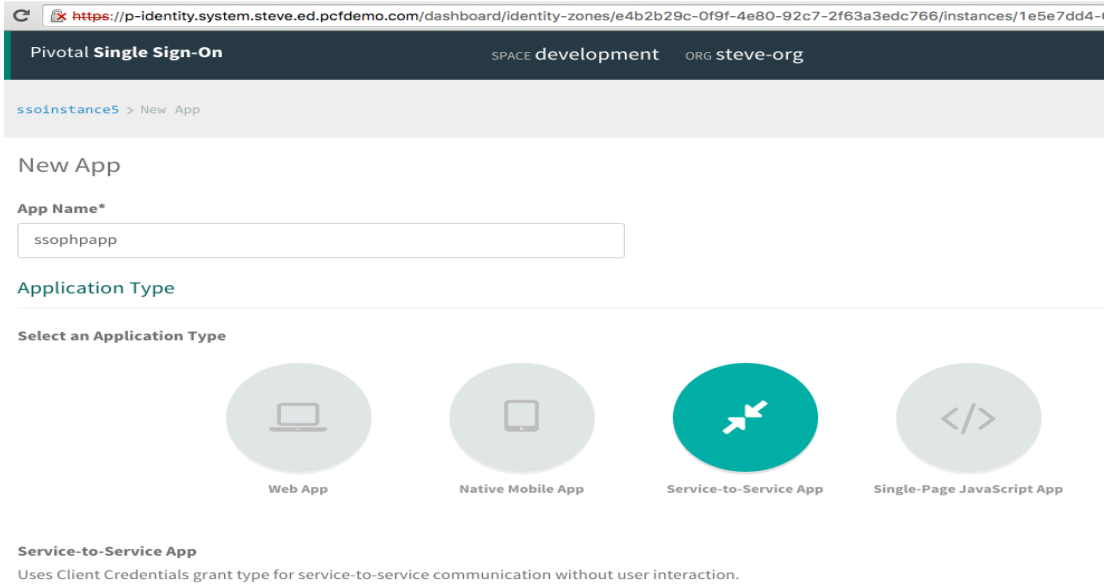


Client (OAuth-aware)

Dashboard



- Click on the Manage link for a service instance in a space to view the dashboard
- Shows all of the OAuth clients on the UAA for the service instance
- Can register a new OAuth client/app
  - The OAuth client app name does not need to match the Cloud Foundry app name



Dashboard

- When you register an OAuth client, you receive the ClientID (App ID) and ClientSecret (App Secret)

https://p-identity.system.steve.ed.pcfdemo.com/dashboard/identity-zones/e4b2b29c-0f9f-4e80-92c7-2f63a3edc766/instanc

Pivotal **Single Sign-On** SPACE development ORG steve-org

ssoinstance5 > ssophpapp

ssophpapp Service-to-Service App

App ID
Unique Identifier for the application
c469d0a7-e6c4-444f-8e43-78e56a80aa63

App Secret
Authenticates the application
••••••••••••••••••••••••••••••••••••

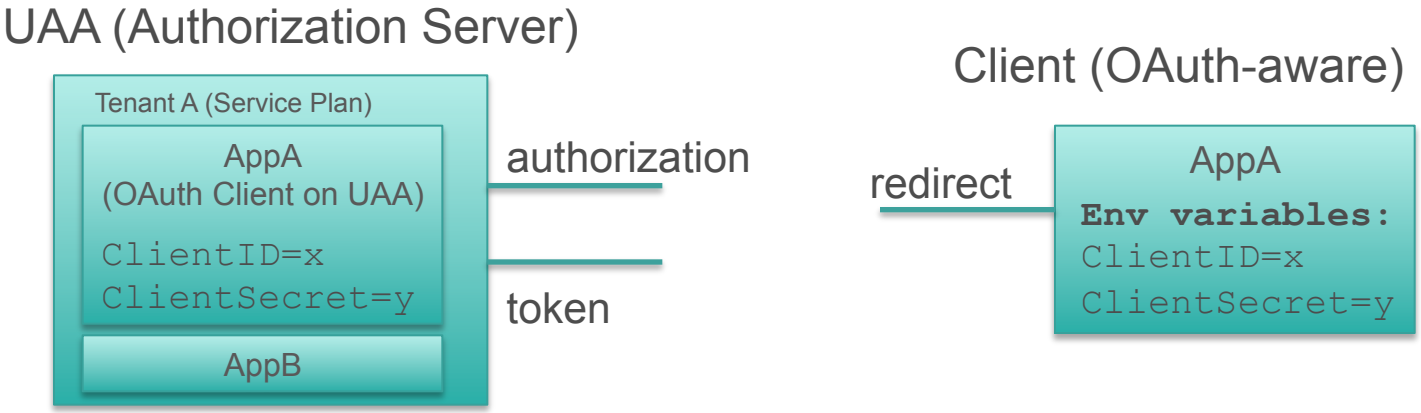
The App Secret can only be displayed once. Regenerate app secret

SSO Service URL
Auth domain for single sign-on
https://sso2.login.system.steve.ed.pcfdemo.com

OAuth Token URL
Client retrieves token from this endpoint
https://sso2.login.system.steve.ed.pcfdemo.com/oauth/token

Cloud Foundry Hosted Applications

- If the application being protected is an application hosted on Cloud Foundry:
  - Binding or registering the service using the dashboard adds the ClientID and ClientSecret as environment variables to app instances
  - Those values are used to authorize the user and obtain tokens



Cloud Foundry Hosted Applications- Environment Variables

- GRANT_TYPE is under user provided environment variables
- The credentials (client_id and client_secret) are system provided and are under the p-identity service

Events | Services | Env Variables | Routes | Logs

USER PROVIDED

+ Add an Env Variable

GRANT_TYPE

client_credentials

SKIP_SSL_VALIDATION

true

SYSTEM PROVIDED


```
{
  "staging_env_json": {},
  "running_env_json": {},
  "system_env_json": {
    "VCAP_SERVICES": {
      "p-identity": [
        {
          "name": "ssoinstance5",
          "label": "p-identity",
          "tags": [],
          "plan": "sso2",
          "credentials": {
            "client_id": "c469d0a7-e6c4-444f-8e43-78e56a80aa63",
            "client_secret": "aebade51-5fe2-401d-9817-e0e8e41f6c40",
            "auth_domain": "https://sso2.login.system.steve.ed.pcfdemo.com"
```


Pivotal

OAuth-Aware Applications

- If you are using Java, there are Spring Boot-based sample applications for each of the four flows / grant types
  - Uses the SSO Service Connector, which auto configures the application for OAuth
- For non-Java applications, your application is responsible for OAuth integration and for validating tokens

Pivotal

Application Types

- The type of OAuth client created on the Pivotal Single Sign-On server depends on the application type:
  - Web App (grant_type=authorization_code)
  - Native Mobile App (grant_type=password)
  - Single Page JavaScript App (grant_type=implicit)
  - Service-to-Service App (grant_type=client_credentials)
- The application type is set in the GRANT_TYPE environment variable for the application needing to be secured
  - The grant_type is sent with requests to the token endpoint of the UAA
- Each application type represents a different authorization flow

Pivotal

Topics

- UAA Overview
- Cloud Foundry Platform Users
- Pivotal SSO Service
- **Service Plans**

Pivotal

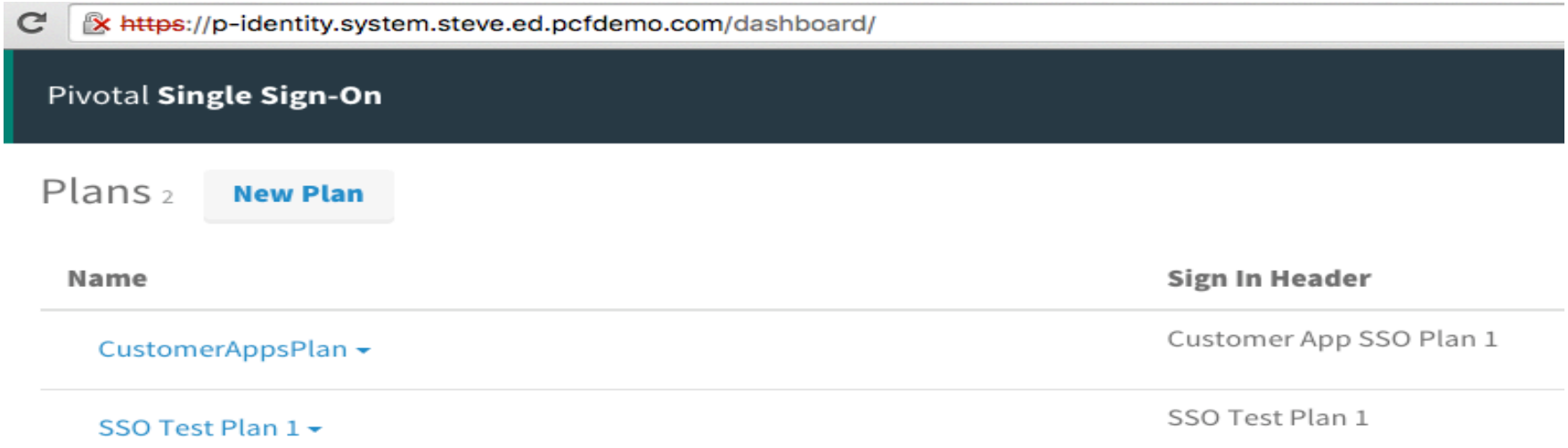
Managed Service

- The Pivotal Single Sign-On service is implemented as a managed service
  - Available in the marketplace as service plans
- Installing the SSO service creates a System > identity-service-space containing an identity-service-broker app
  - Can access SSO logs from Apps Manager or the cf CLI
- Enable SSO for an application in one of two ways:
  - Bind the application to the service instance
  - Register the application with the Pivotal Single Sign-On service dashboard
- The application must be OAuth 2.0 aware

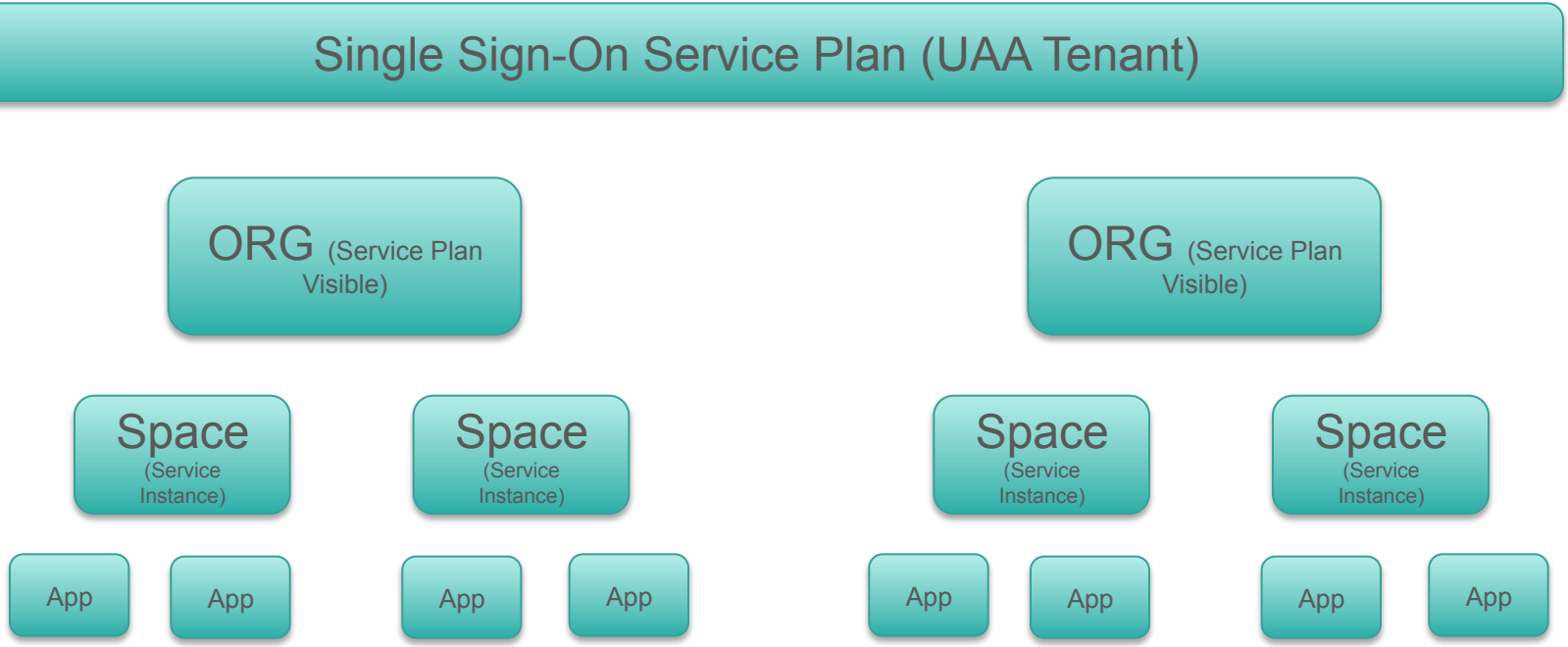
Pivotal

Creating and Viewing Service Plans

- Use https://p-identity.[system domain] to create and view service plans (UAA tenants)



Service Plan Visibility



- Enable a service plan for an org with `cf enable-service-access`

Role-based Access

PCF Admin

- Manage service plans
- Enable service plans in orgs
- On-board Identity Providers

Space Developer

- Create service instance
- Bind applications to SSO Service
- Associate apps with Identity Providers
- Limited to app SSO configuration within space boundary

Pivotal

Topics

- UAA Overview
- Cloud Foundry Platform Users
- Pivotal SSO Service
- Service Plans

Pivotal

Lab

- Set up a Single Sign-On Service plan
- Obtain an access token
- Secure an app with access tokens

Pivotal