Pivotal

Validated with ca technologies

ca **Secure**center Federation Runbook for Pivotal Cloud Foundry

Legal Notice

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com or customer-service@pivotal.io

Contents

Chapter 1: SaaS Partner Introduction

This section contains the following topics:

Overview

The scope of the document is to provide the necessary steps to configure the federation partnership to achieve SSO (Single-Sign-On) between CA Single Sign-On 12.52 (formerly CA SiteMinder), acting as the Identity Provider (IDP), and Pivotal Cloud Foundry acting as the Service Provider (SP). **This integration works only for Pivotal Cloud Foundry 1.4 and above**

Partnership Process

The partnership creation for each partner involves the following steps:

1. Installing and configuring the prerequisites

2. Configuring CA Single Sign-On as an Identity Provider

3. Configuring the Service Provider

4. Testing the Federated SSO

Prerequisites

- Installation of CA Single Sign-On 12.52 Suite
- Configuration and testing of User store and Session store
- Creation of Signed Certificate by a well-known Certificate Authority such as VeriSign, Entrust, Thawte or Go Daddy for Identity Provider Digital Signature.

- **Important!** - Protect Identity Provider Authentication URL with a policy using CA Single Sign-On 12.52

Identity Provider Authentication URL is protected by creating following objects:

  - Authentication Scheme
  - Domain
  - Realm
  - Rule & Policy

Notes: Protecting the Authentication URL ensures that a user requesting a protected federated resource is presented with an authentication challenge if they do not have a CA Single Sign-On session at the Identity Provider.

- Tenant environment at Pivotal Cloud Foundry Login URL - **https://console.{system-domain}**

  Note: Replace System Domain with your Pivotal Cloud Foundry inslallatiion equivalent

Target Pivotal Cloud Foundry

The following services of Pivotal Cloud Foundry have been tested for federation using CA Single Sign-On 12.52 as Identity Provider.

1. Apps Manager
2. Cloud Foundry Command Line Interface (CF CLI)

Chapter 2: Configure CA Single Sign-On (12.52) as Identity Provider

This section contains the following topics:

Configure Identity Provider and Service Provider Entities

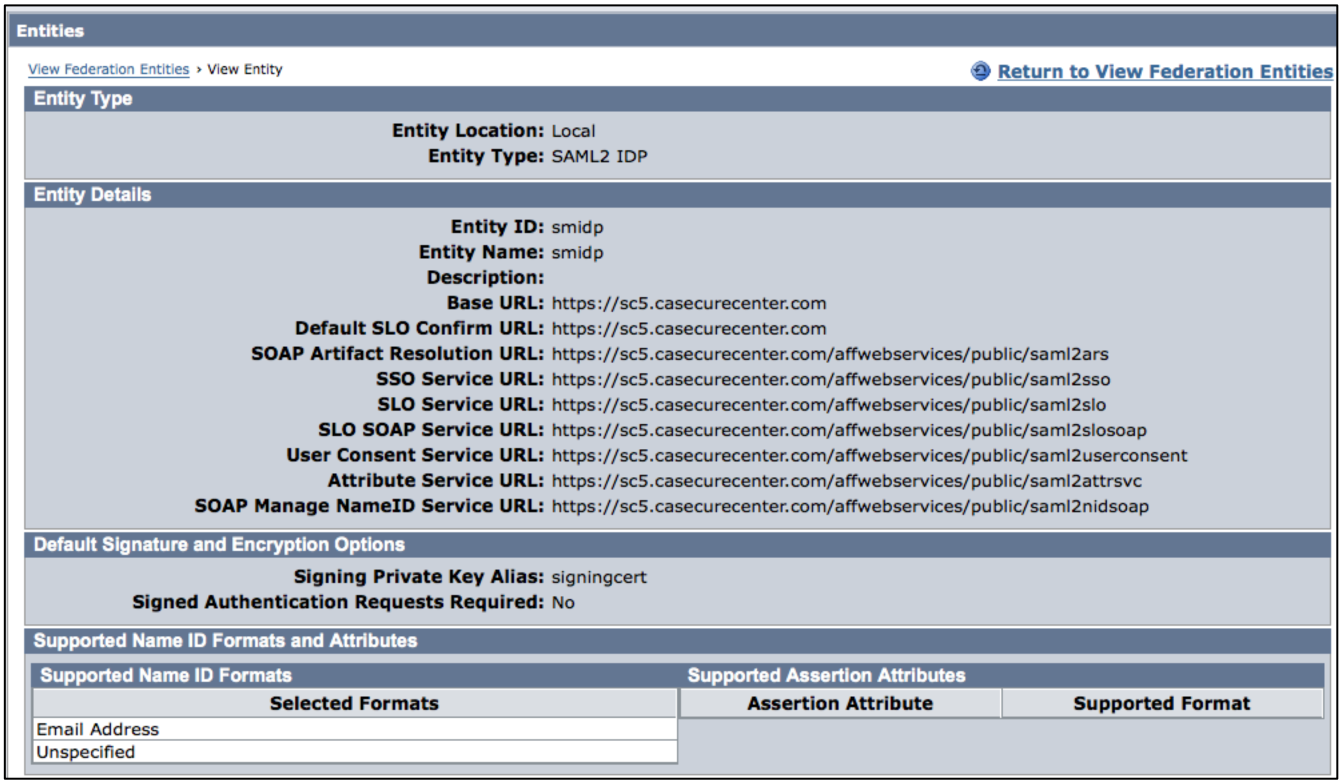
To create Entities, Login to CA Single Sign-On and get to Federation → Partnership Federation → Entity → Create Entity

Local Entity Creation

- Configure Local Identity Provider Entity with following details:
    - Entity Location – Local
    - Entity Type – SAML2 IDP
    - Entity ID – Any (e.g. https://ca-technologies.xxx.com)
    - Entity Name – Any (sampleentity)
    - Base URL – https://<FWS_FQDN> where FWS_FQDN is the fully-qualified domain name for the host serving CA Single Sign-On Federation Web Services

      (e.g. ca-technologies.xxx.com)
    - Signing Private Key Alias – Select the correct private key alias or import one if not done already (e.g. catech)
    - Signed Authentication Requests Required – No
    - Supported NameID format –
        - urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress

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



Entities

View Federation Entities › View Entity

Return to View Federation Entities

Entity Type

Entity Location: Local
Entity Type: SAML2 IDP

Entity Details

Entity ID: smidp
Entity Name: smidp
Description:
Base URL: https://sc5.casecurecenter.com
Default SLO Confirm URL: https://sc5.casecurecenter.com
SOAP Artifact Resolution URL: https://sc5.casecurecenter.com/affwebservices/public/saml2ars
SSO Service URL: https://sc5.casecurecenter.com/affwebservices/public/saml2sso
SLO Service URL: https://sc5.casecurecenter.com/affwebservices/public/saml2slo
SLO SOAP Service URL: https://sc5.casecurecenter.com/affwebservices/public/saml2slosoap
User Consent Service URL: https://sc5.casecurecenter.com/affwebservices/public/saml2userconsent
Attribute Service URL: https://sc5.casecurecenter.com/affwebservices/public/saml2attrsvc
SOAP Manage NameID Service URL: https://sc5.casecurecenter.com/affwebservices/public/saml2nidsoap

Default Signature and Encryption Options

Signing Private Key Alias: signingcert
Signed Authentication Requests Required: No

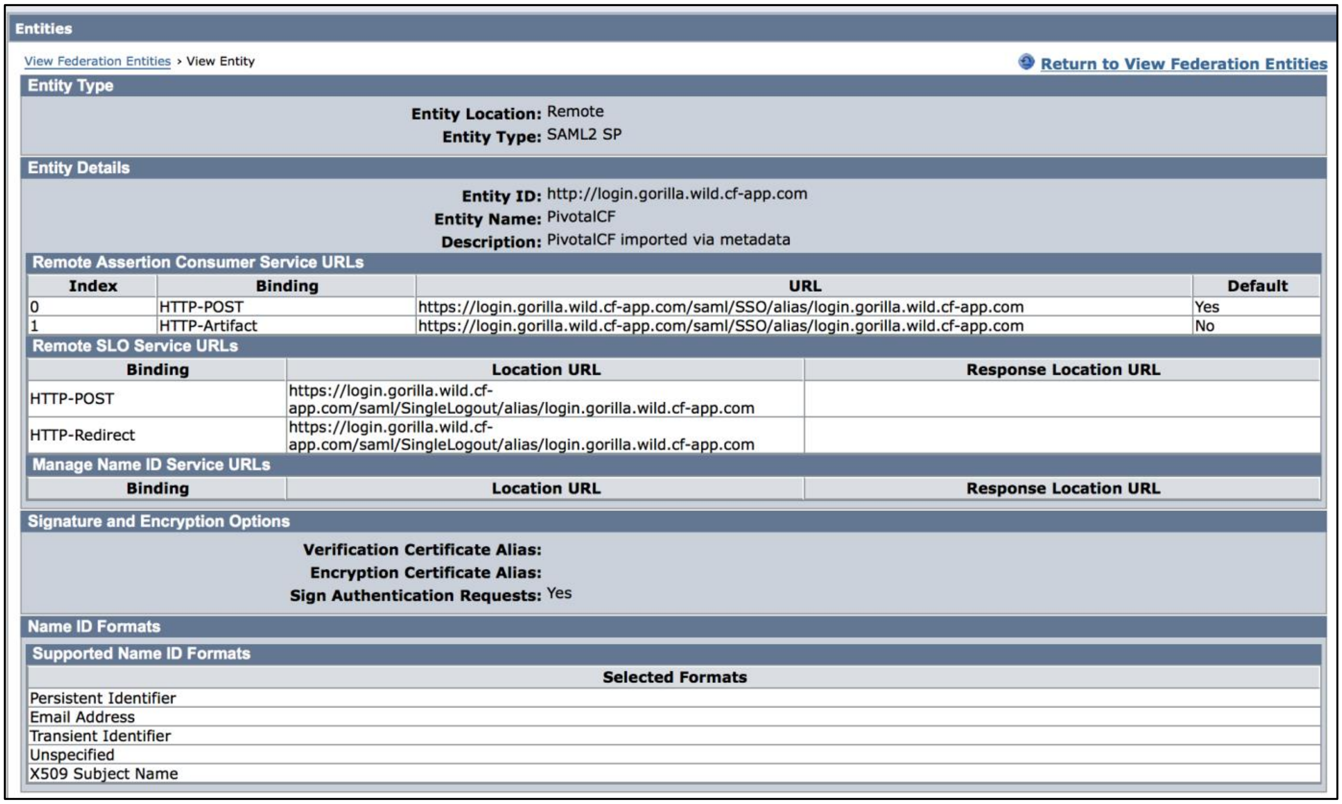
Supported Name ID Formats and Attributes

Supported Name ID Formats	Supported Assertion Attributes	
Selected Formats	**Assertion Attribute**	**Supported Format**
Email Address		
Unspecified		

Remote Entity Creation

- To configure Remote Service Provider Entity manually, click on Import Metadata Button and perform the steps below
  - Start by downloading the Service Provider Metadata from https://login.{system-domain}/saml/metadata and save to an XML file
  - Browse and select the saved XML Metadata from Previous step and continue
  - Provide a Name for the Remote Service Provider Entity
  - Provide an alias for the Signing Certificate imported from the Metadata.

    Note: Pivotal Cloud Foundry always signs the outgoing SAML Authenitcation Requests
  - Save the Remote Service Provider Entity



Entities

View Federation Entities › View Entity

Return to View Federation Entities

Entity Type

Entity Location: Remote
Entity Type: SAML2 SP

Entity Details

Entity ID: http://login.gorilla.wild.cf-app.com
Entity Name: PivotalCF
Description: PivotalCF imported via metadata

Remote Assertion Consumer Service URLs

Index	Binding	URL	Default
0	HTTP-POST	https://login.gorilla.wild.cf-app.com/saml/SSO/alias/login.gorilla.wild.cf-app.com	Yes
1	HTTP-Artifact	https://login.gorilla.wild.cf-app.com/saml/SSO/alias/login.gorilla.wild.cf-app.com	No

Remote SLO Service URLs

Binding	Location URL	Response Location URL
HTTP-POST	https://login.gorilla.wild.cf-app.com/saml/SingleLogout/alias/login.gorilla.wild.cf-app.com	
HTTP-Redirect	https://login.gorilla.wild.cf-app.com/saml/SingleLogout/alias/login.gorilla.wild.cf-app.com	

Manage Name ID Service URLs

Binding	Location URL	Response Location URL

Signature and Encryption Options

Verification Certificate Alias:
Encryption Certificate Alias:
Sign Authentication Requests: Yes

Name ID Formats

Supported Name ID Formats

Selected Formats
Persistent Identifier
Email Address
Transient Identifier
Unspecified
X509 Subject Name

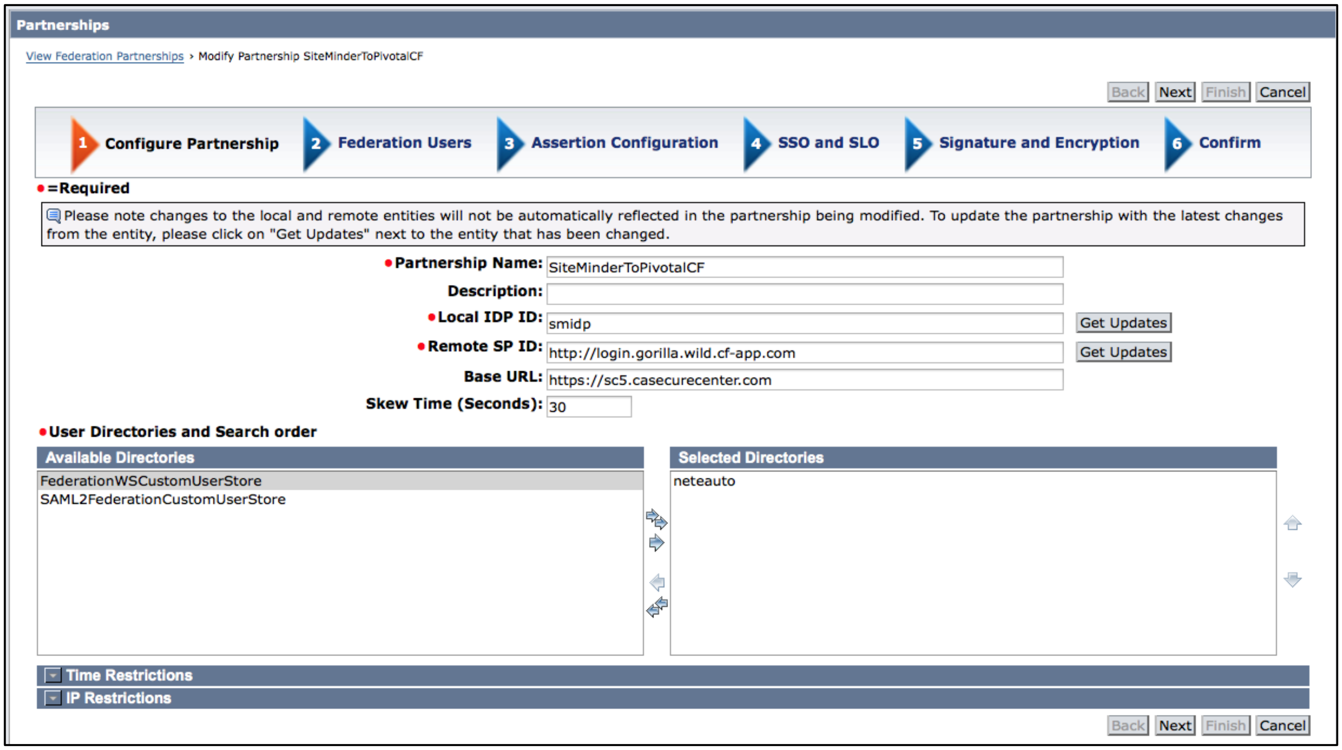
Configure Federation Partnership between CA Single Sign-On (IDP) & Pivotal Cloud Foundry (SP)

Login to CA Single Sign-On and navigate to Federation → Partnership Federation → Create Partnership (SAML 2 IDP → SP)

Configure Partnership

- Add Partnership Name – Any *(e.g. SamplePartnership_<??>)*
- Description – Any *(Relevant description)*
- Local IDP ID – Select Local IDP ID created above
- Remote SP ID – Select Remote SP ID created above

- Base URL – Will be pre-populated
- Skew Time – Any per environment requirement
- User Directories and Search Order– Select required Directories in required search order. Proceed to Next Page


Partnerships
View Federation Partnerships › Modify Partnership SiteMinderToPivotalCF
Back
Next
Finish
Cancel
1 Configure Partnership
2 Federation Users
3 Assertion Configuration
4 SSO and SLO
5 Signature and Encryption
6 Confirm

● =Required

Please note changes to the local and remote entities will not be automatically reflected in the partnership being modified. To update the partnership with the latest changes from the entity, please click on "Get Updates" next to the entity that has been changed.

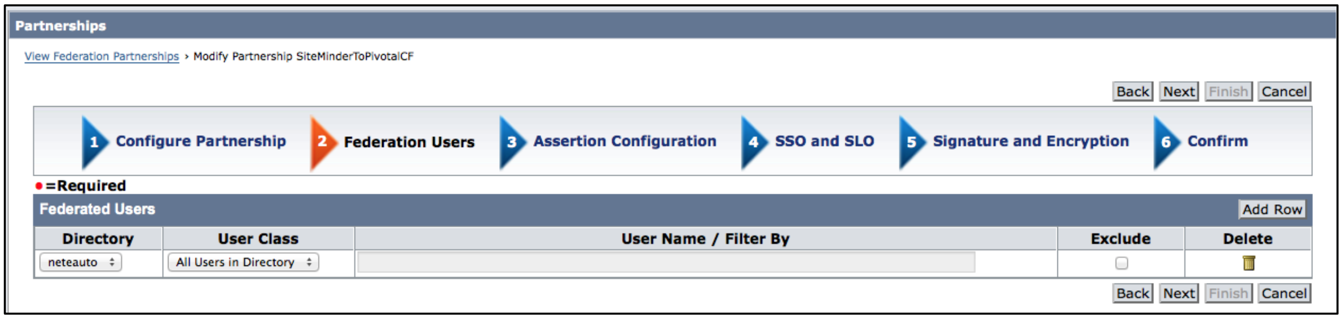
●Partnership Name:	SiteMinderToPivotalCF	
Description:		
●Local IDP ID:	smidp	Get Updates
●Remote SP ID:	http://login.gorilla.wild.cf-app.com	Get Updates
Base URL:	https://sc5.casecurecenter.com	
Skew Time (Seconds):	30	

●User Directories and Search order

Available Directories	Selected Directories
FederationWSCustomUserStore	neteauto
SAML2FederationCustomUserStore	

Federation Users

- Configure Federation Users – Accept default values


Partnerships
View Federation Partnerships › Modify Partnership SiteMinderToPivotalCF
Back
Next
Finish
Cancel
1 Configure Partnership
2 Federation Users
3 Assertion Configuration
4 SSO and SLO
5 Signature and Encryption
6 Confirm
Add Row
Back
Next
Finish
Cancel

● =Required

Federated Users

Directory	User Class	User Name / Filter By	Exclude	Delete
neteauto	All Users in Directory		□	🗑

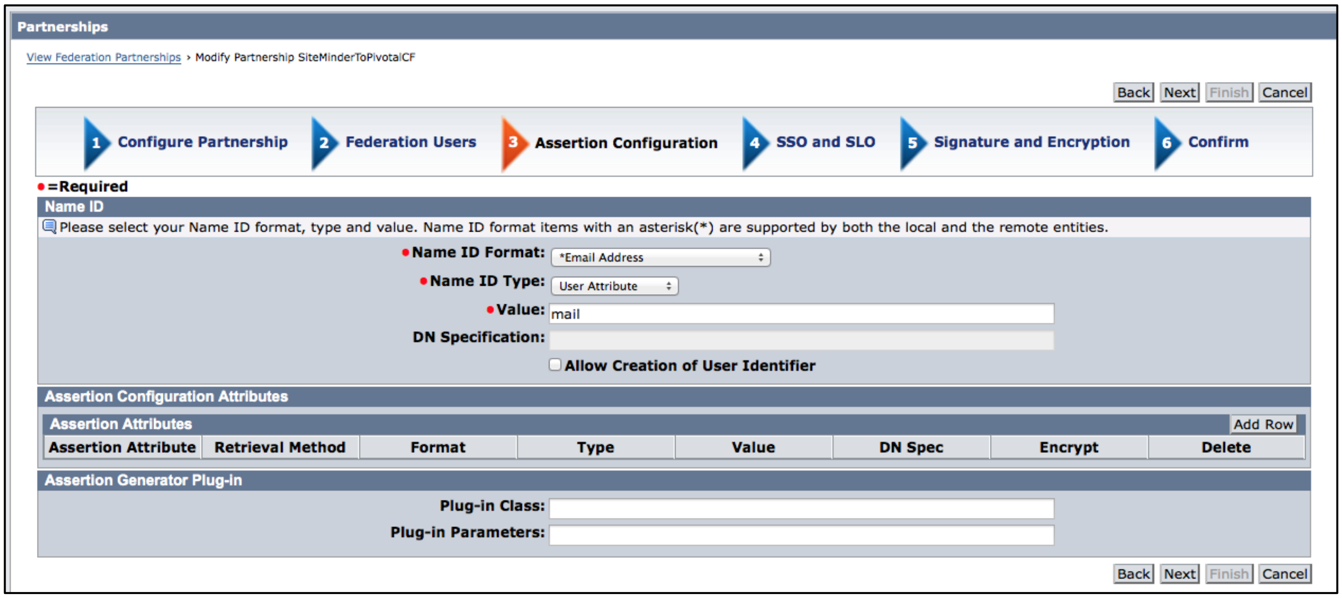
Assertion Configuration

Name ID Format:

- Name ID Format – *Email Address
- Name ID Type – User Attribute
- Value – mail

Assertion Attributes:

Pivotal Cloud Foundry doesn't support processing SAML Assertion Attributes at this time


Partnerships
View Federation Partnerships › Modify Partnership SiteMinderToPivotalCF
Back
Next
Finish
Cancel
1 Configure Partnership
2 Federation Users
3 Assertion Configuration
4 SSO and SLO
5 Signature and Encryption
6 Confirm
Add Row
Back
Next
Finish
Cancel

● =Required

Name ID

Please select your Name ID format, type and value. Name ID format items with an asterisk(*) are supported by both the local and the remote entities.

●Name ID Format: *Email Address

●Name ID Type: User Attribute

●Value: mail

DN Specification:

□ Allow Creation of User Identifier

Assertion Configuration Attributes

Assertion Attributes

Assertion Attribute	Retrieval Method	Format	Type	Value	DN Spec	Encrypt	Delete

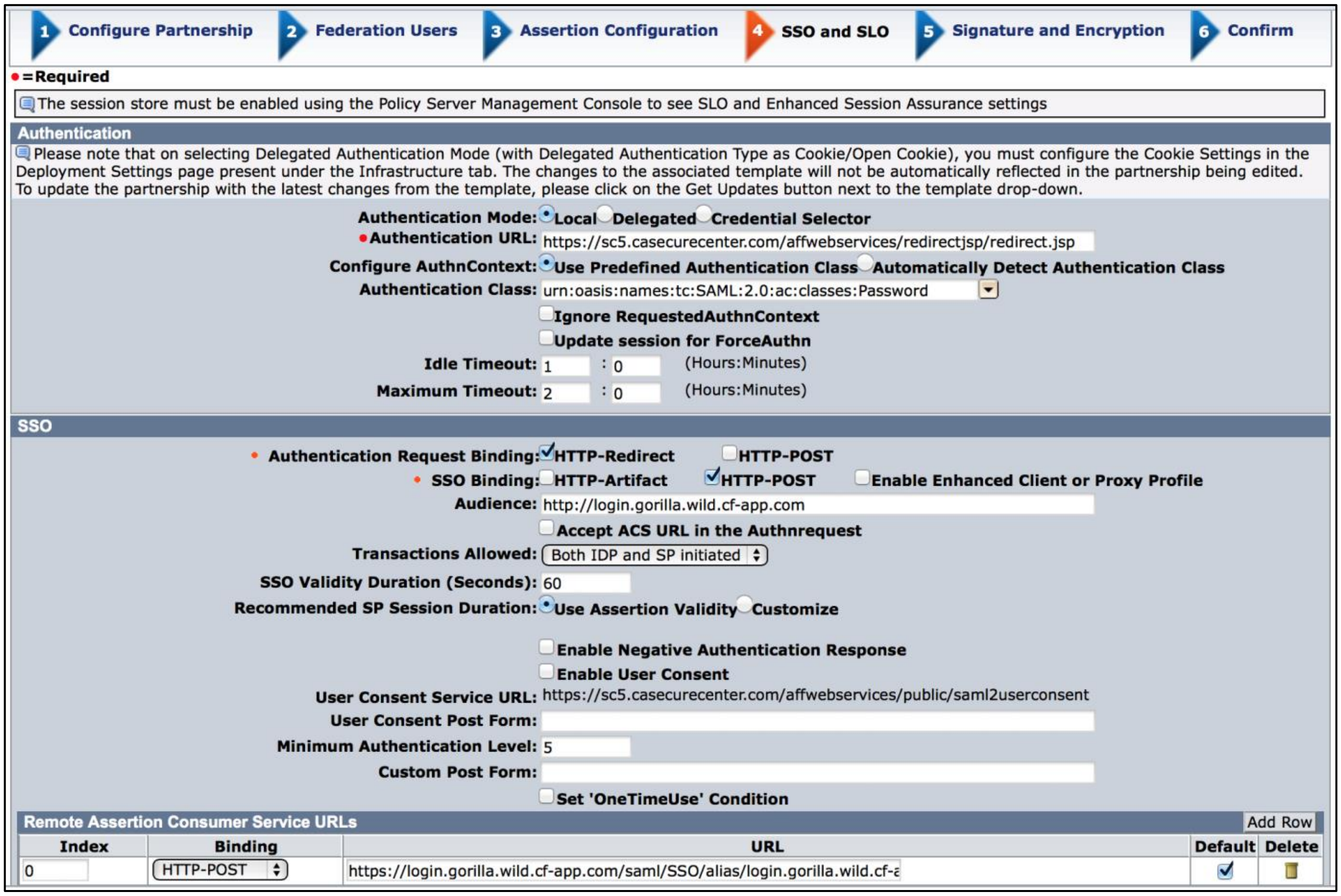
Assertion Generator Plug-in

Plug-in Class:

Plug-in Parameters:

SSO and SLO

- Add Authentication URL that is protected by CA Single Sign-On under pre-requisites
- SSO Binding – Select SSO Binding supported by the Service Provider – HTTP-Post
- Audience - http://login.{system-domain}
- Transaction Allowed – Both IDP and SP Initiated
- Assertion Consumer Service URL – Should be pre-populated using information from the Service Provider entity



● =Required

The session store must be enabled using the Policy Server Management Console to see SLO and Enhanced Session Assurance settings

Authentication

Please note that on selecting Delegated Authentication Mode (with Delegated Authentication Type as Cookie/Open Cookie), you must configure the Cookie Settings in the Deployment Settings page present under the Infrastructure tab. The changes to the associated template will not be automatically reflected in the partnership being edited. To update the partnership with the latest changes from the template, please click on the Get Updates button next to the template drop-down.

Authentication Mode:	● Local ○ Delegated ○ Credential Selector
● Authentication URL:	https://sc5.casecurecenter.com/affwebservices/redirectjsp/redirect.jsp
Configure AuthnContext:	● Use Predefined Authentication Class ○ Automatically Detect Authentication Class
Authentication Class:	urn:oasis:names:tc:SAML:2.0:ac:classes:Password
	□ Ignore RequestedAuthnContext
	□ Update session for ForceAuthn
Idle Timeout:	1 : 0 (Hours:Minutes)
Maximum Timeout:	2 : 0 (Hours:Minutes)

SSO

● Authentication Request Binding:	☑ HTTP-Redirect □ HTTP-POST
● SSO Binding:	□ HTTP-Artifact ☑ HTTP-POST □ Enable Enhanced Client or Proxy Profile
Audience:	http://login.gorilla.wild.cf-app.com
	□ Accept ACS URL in the Authnrequest
Transactions Allowed:	Both IDP and SP initiated
SSO Validity Duration (Seconds):	60
Recommended SP Session Duration:	● Use Assertion Validity ○ Customize
	□ Enable Negative Authentication Response
	□ Enable User Consent
User Consent Service URL:	https://sc5.casecurecenter.com/affwebservices/public/saml2userconsent
User Consent Post Form:	
Minimum Authentication Level:	5
Custom Post Form:	
	□ Set 'OneTimeUse' Condition

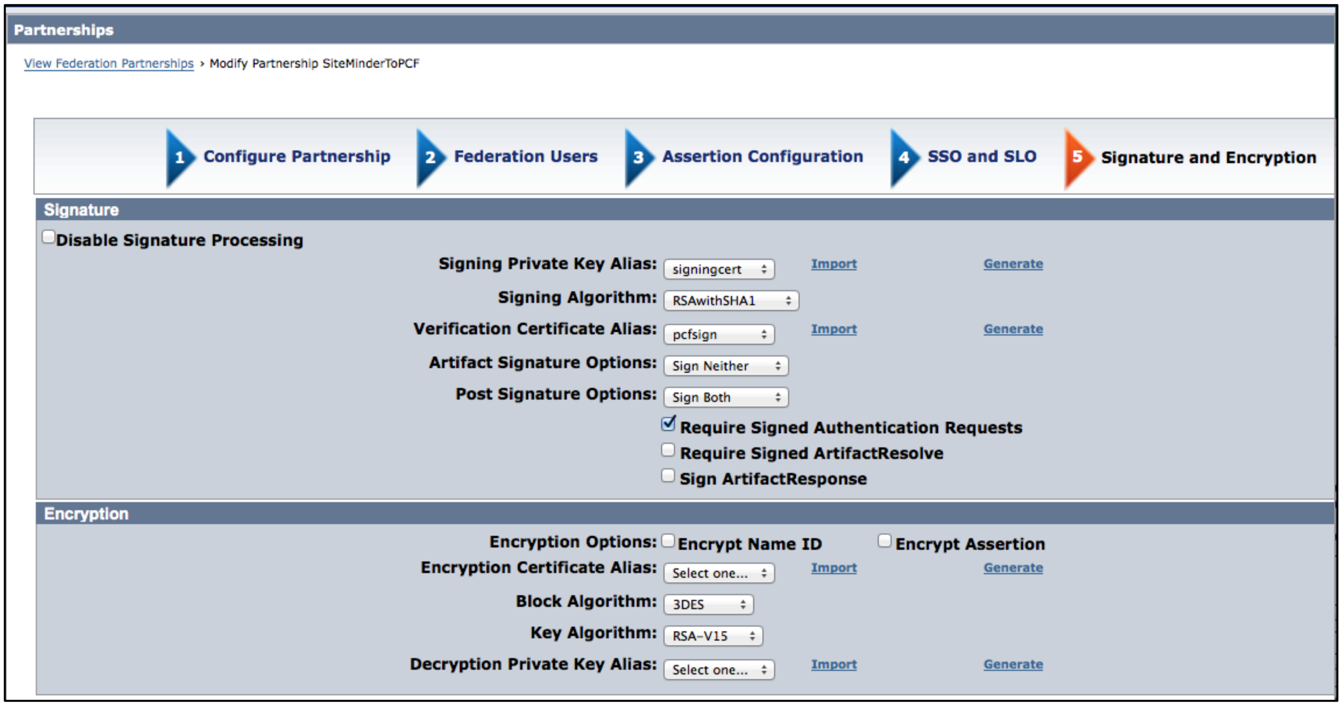
Remote Assertion Consumer Service URLs Add Row

Index	Binding	URL	Default	Delete
0	HTTP-POST	https://login.gorilla.wild.cf-app.com/saml/SSO/alias/login.gorilla.wild.cf-a	☑	

Configure Signature and Encryption

- Signing Private Key Alias – Verify if correct Private Key Alias is selected
- Verification Certificate Alias – Verify if correct Verification Certificate Alias is selected. This should be the same certificiate created during the import of the Remote Service Provider Entity ID.
    - For Post Signature select “Sign Both” (Sign both the Reponse and the Assertion)

Note: Pivotal Cloud Foundry doesn’t support the various encryption options at this time



Partnerships

View Federation Partnerships › Modify Partnership SiteMinderToPCF

Signature

□ Disable Signature Processing

Signing Private Key Alias: signingcert — Import — Generate

Signing Algorithm: RSAwithSHA1

Verification Certificate Alias: pcfsign — Import — Generate

Artifact Signature Options: Sign Neither

Post Signature Options: Sign Both

☑ Require Signed Authentication Requests

□ Require Signed ArtifactResolve

□ Sign ArtifactResponse

Encryption

Encryption Options: □ Encrypt Name ID □ Encrypt Assertion

Encryption Certificate Alias: Select one... — Import — Generate

Block Algorithm: 3DES

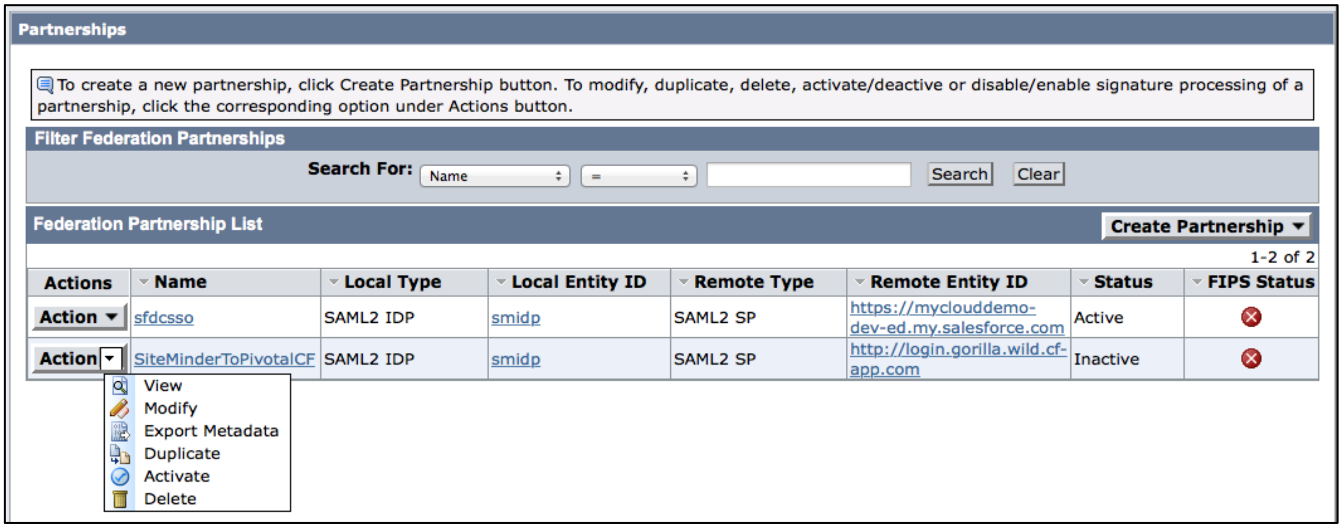
Key Algorithm: RSA-V15

Decryption Private Key Alias: Select one... — Import — Generate

- Confirm the values and finish Partnership.

Partnership Activation

- Activate the created Partnership.



Partnerships

To create a new partnership, click Create Partnership button. To modify, duplicate, delete, activate/deactive or disable/enable signature processing of a partnership, click the corresponding option under Actions button.

Filter Federation Partnerships

Search For: Name = [ ] Search Clear

Federation Partnership List Create Partnership

1-2 of 2

Actions	Name	Local Type	Local Entity ID	Remote Type	Remote Entity ID	Status	FIPS Status
Action	sfdcsso	SAML2 IDP	smidp	SAML2 SP	https://myclouddemo-dev-ed.my.salesforce.com	Active	☒
Action	SiteMinderToPivotalCF	SAML2 IDP	smidp	SAML2 SP	http://login.gorilla.wild.cf-app.com	Inactive	☒

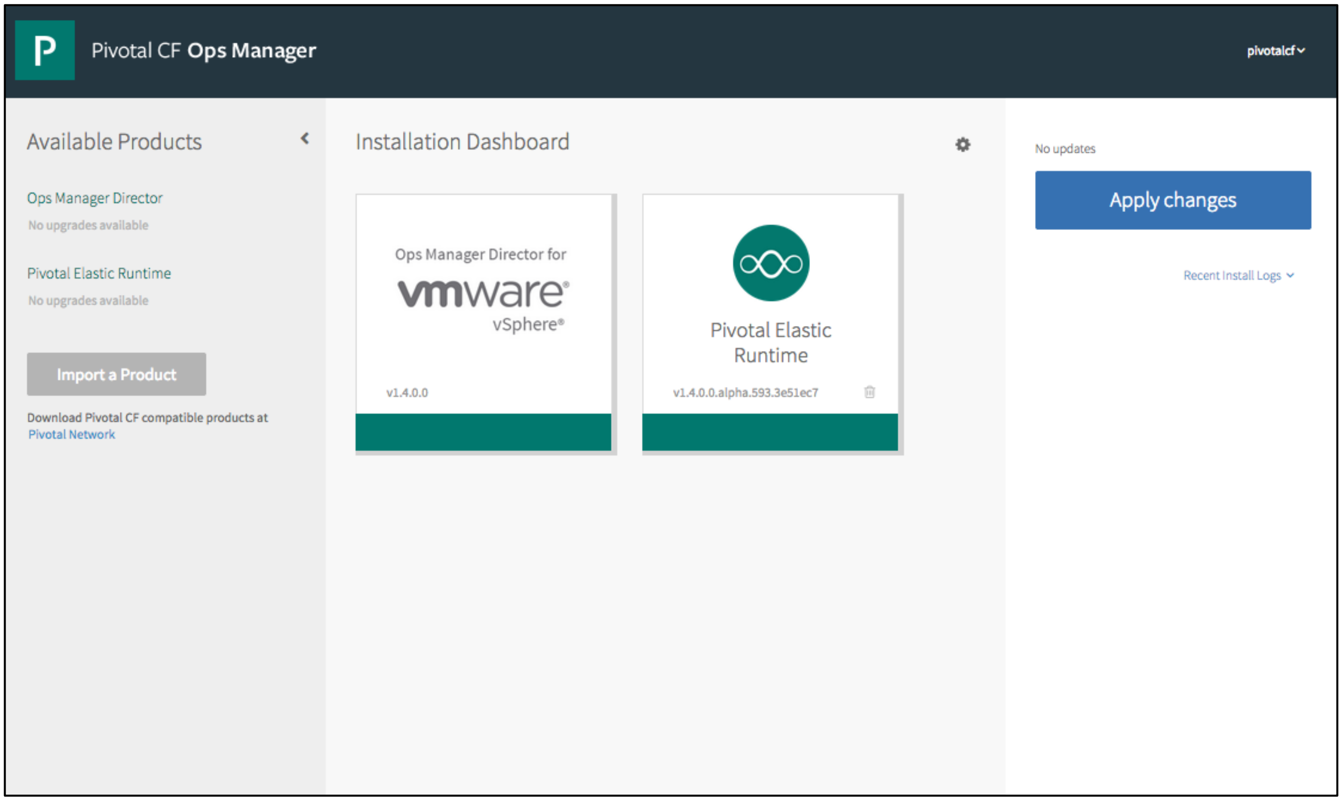
Chapter 3: Configure Service Provider

This section contains the following topics:

Configure SAML 2.0 SSO in Pivotal Cloud Foundry

Please follow the steps below for configuring Pivotal Cloud Foundry if using Ops Manager

- Log into the Ops Manager Console and Click on Pivotal Elastic Runtime tile

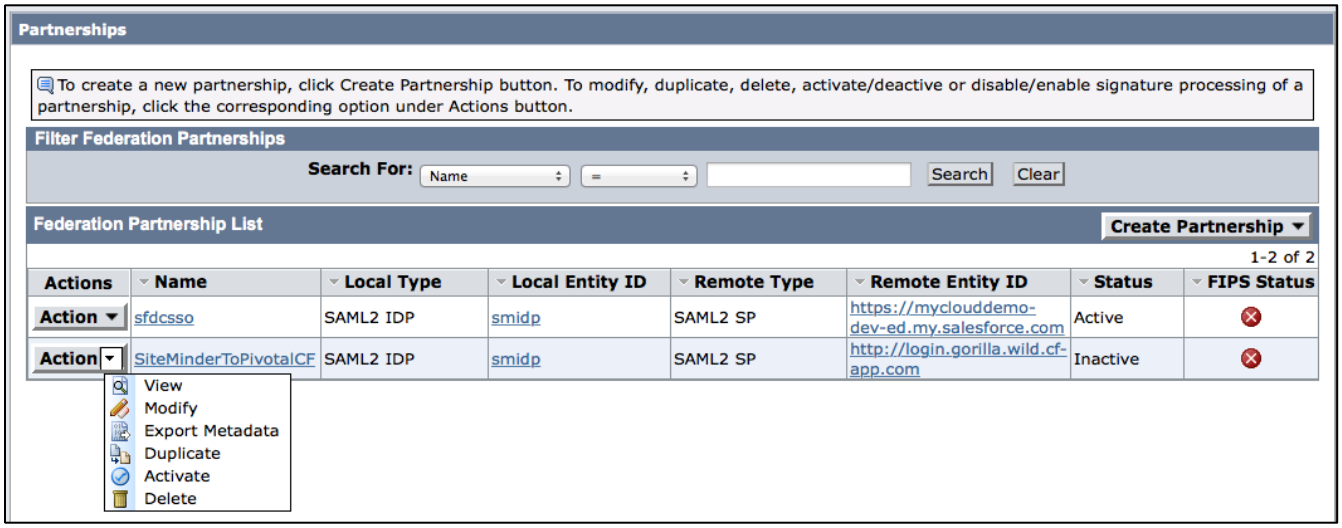


- Click on SSO Config under Settings
- Enter a name under Provider Name. This name will be displayed on the Pivotal Cloud Foundry Login Page as a link which perfoms SP Intiated Single Sign-On

- Enter the Idenity Provider Metadata.
    - Navigate to Login to CA Single Sign-On and navigate to Federation → Partnership Federation → Select the Export Metadata option in the Actions Menu of the Partnership
    - Save the Exported Metadata in an XML file
    - Paste the contents of the XML file into the Identity Provider Metadata Text Area

      Exported Identity Provider metadata doesn't contain the XML declaration tag. You will need add this at the beginning of the XML

      <?xml version="1.0" encoding="UTF-8"?>
    - Save the form
- Click on Apply Changes



Partnerships

To create a new partnership, click Create Partnership button. To modify, duplicate, delete, activate/deactive or disable/enable signature processing of a partnership, click the corresponding option under Actions button.

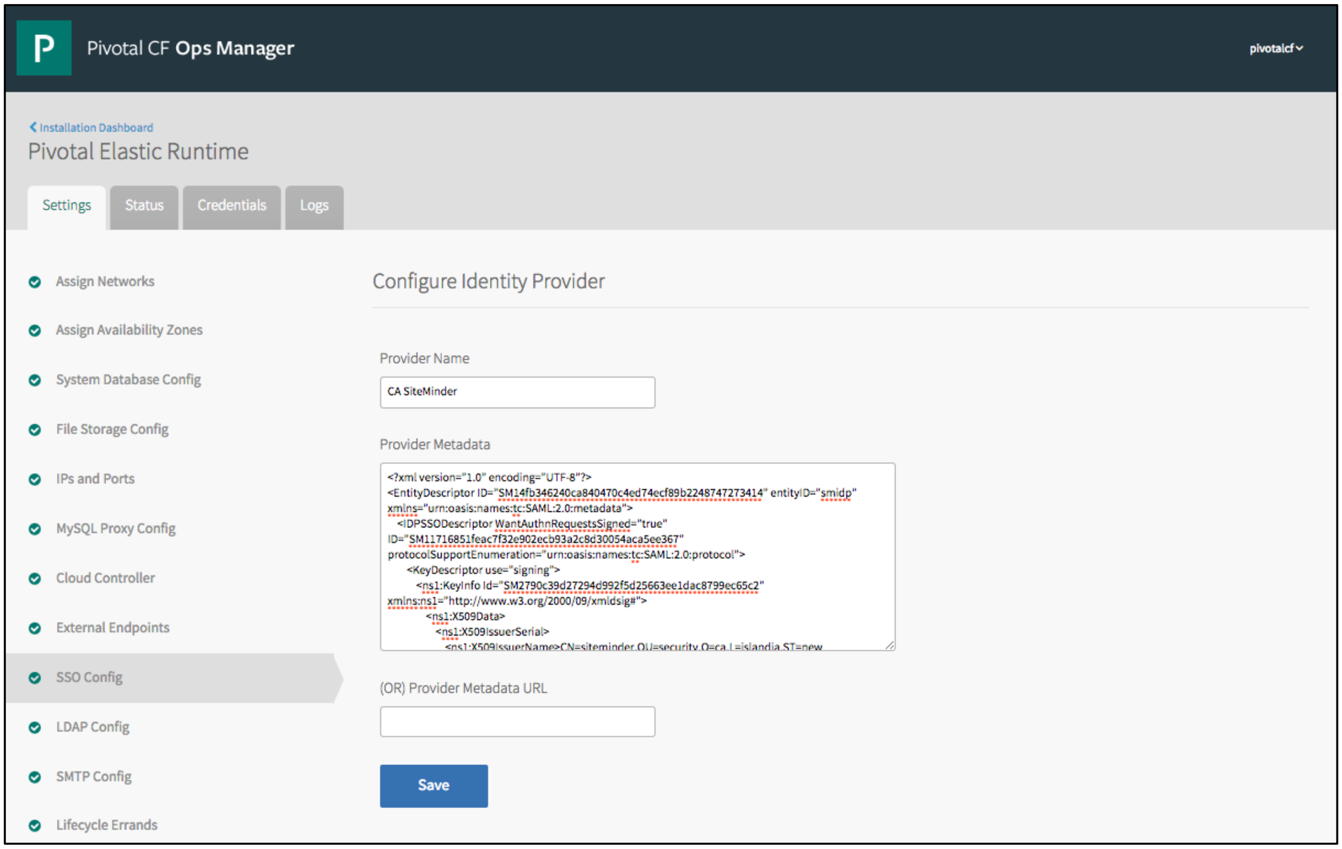
Filter Federation Partnerships

Search For: Name =

Federation Partnership List

1-2 of 2

Actions	Name	Local Type	Local Entity ID	Remote Type	Remote Entity ID	Status	FIPS Status
Action	sfdcsso	SAML2 IDP	smidp	SAML2 SP	https://myclouddemo-dev-ed.my.salesforce.com	Active	⊗
Action	SiteMinderToPivotalCF	SAML2 IDP	smidp	SAML2 SP	http://login.gorilla.wild.cf-app.com	Inactive	⊗



Configure Identity Provider

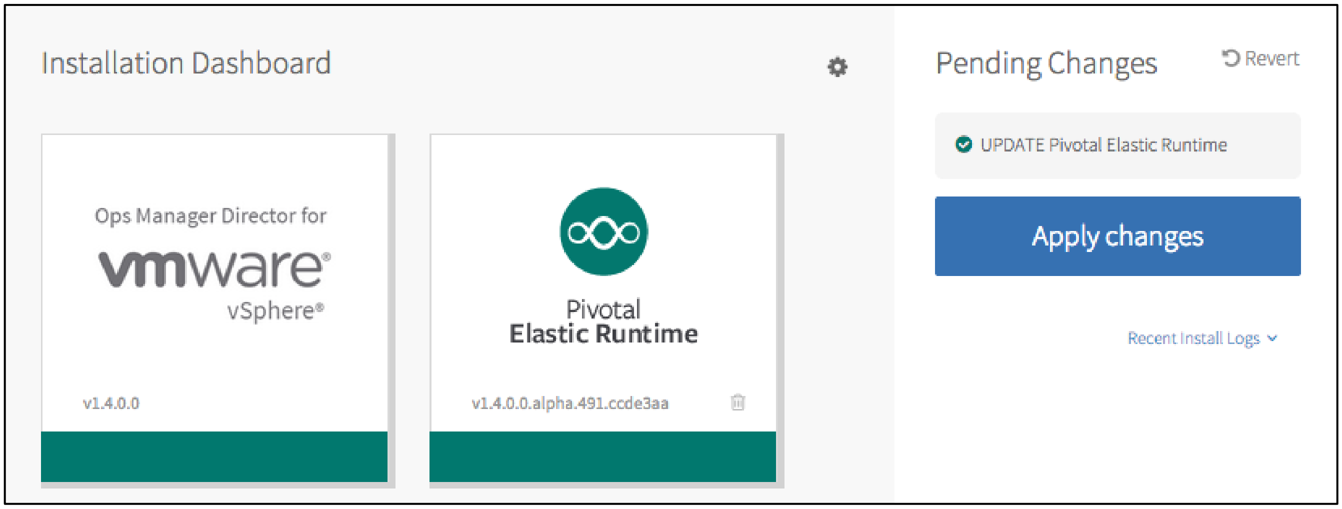
Provider Name

CA SiteMinder

Provider Metadata

```
<?xml version="1.0" encoding="UTF-8"?>
<EntityDescriptor ID="SM14fb346240ca840470c4ed74ecf89b2248747273414" entityID="smidp"
xmlns="urn:oasis:names:tc:SAML:2.0:metadata">
  <IDPSSODescriptor WantAuthnRequestsSigned="true"
ID="SM11716851feac7f32e902ecb93a2c8d30054aca5ee367"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <KeyDescriptor use="signing">
      <ns1:KeyInfo Id="SM2790c39d27294d992f5d25663ee1dac8799ec65c2"
xmlns:ns1="http://www.w3.org/2000/09/xmldsig#">
        <ns1:X509Data>
          <ns1:X509IssuerSerial>
            <ns1:X509IssuerName>CN=siteminder,OU=security,O=ca,L=islandia,ST=new
```

(OR) Provider Metadata URL



Chapter 4: Federation Testing & Target Services

This section contains the following topics:

Federation Testing

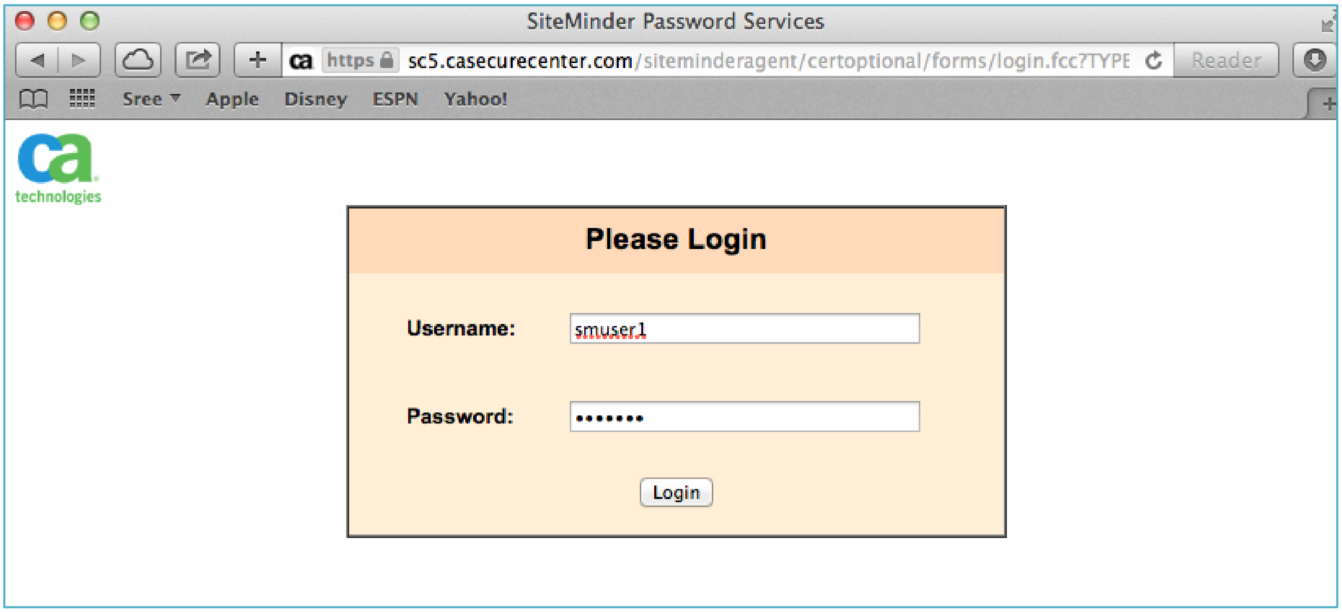
Accessing various Pivotal Cloud Foundry Federation services

Federation Testing

Both Identity Provider and Service Provider Initiated Single Sign-On were tested on <SaaS_Partner> as described below

Identity Provider initiated Testing

- Access the Identity Provider initiated login URL https://<host_FQDN>/affwebservices/public/sam2sso?SPID=<SP_ID> *(e.g.: https://<host_FQDN>/affwebservices/public/saml2sso?SPID=<SP_ID>)*
- This will automatically direct the user to the login page of Identity Provider (CA Single Sign-On).
- Enter the credentials and click login


SiteMinder Password Services
https sc5.casecurecenter.com/siteminderagent/certoptional/forms/login.fcc?TYPE
Reader
Sree
Apple
Disney
ESPN
Yahoo!
ca technologies

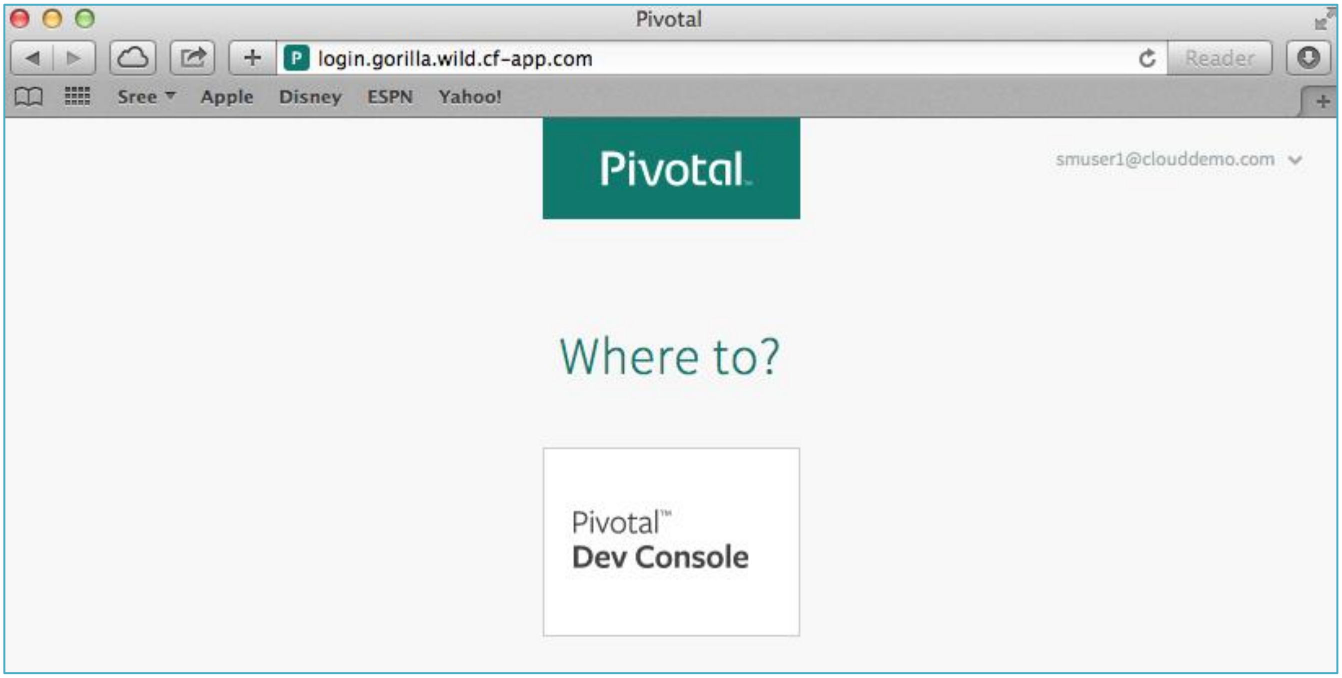
Please Login

Username: smuser1

Password: •••••••

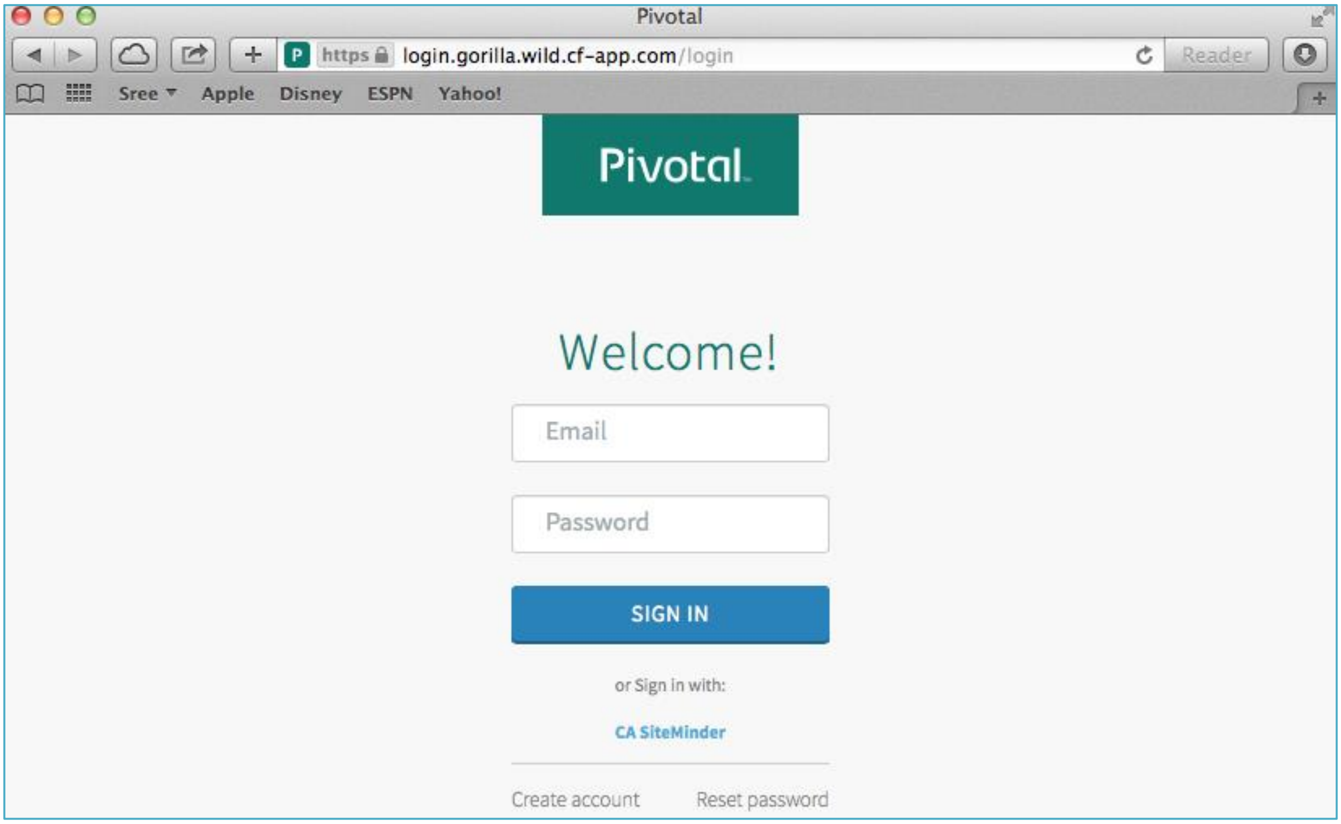
Login

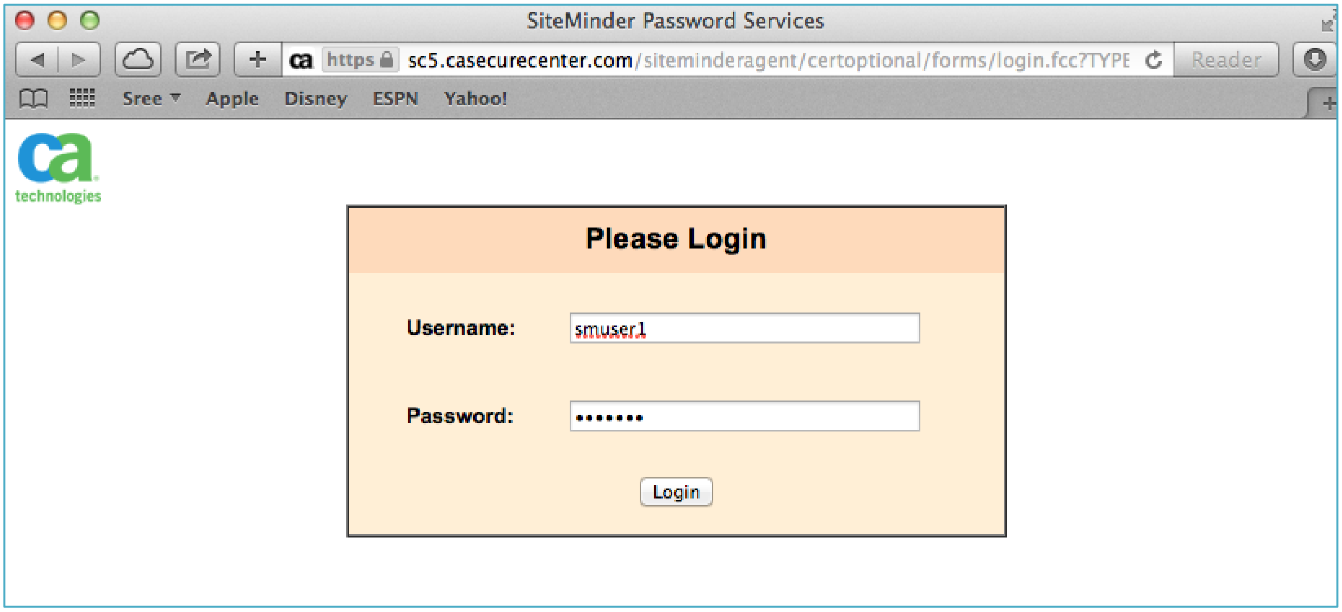
User will be landing at the Pivotal Cloud Foundry Apps Manager home page



Service Provider initiated Testing

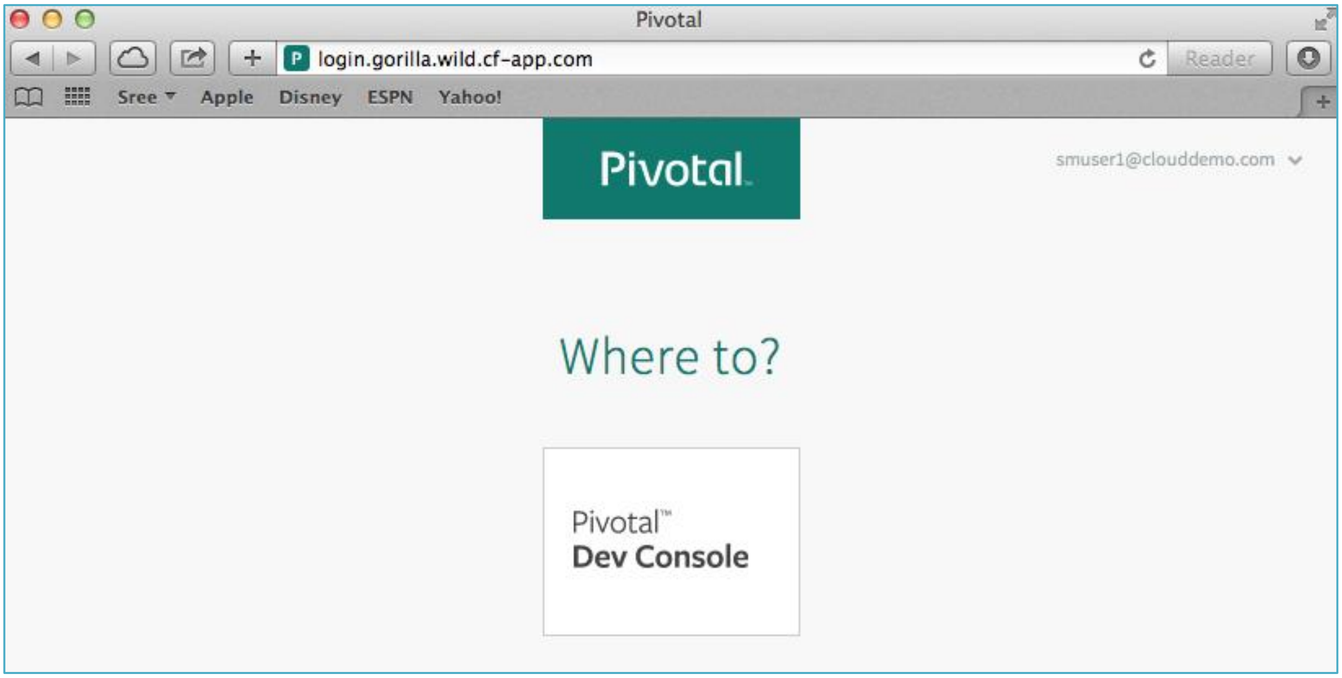
- Access Pivotal Cloud Foundry Apps Manager at https://console.{system-domain}/
- The User is redirected to the Login Page
- Click on the Identity Provider Link : "CA Single Sign-On" (The link text will vary based on what has been entered for the Identity Provider Name under Single Sign-On configuration in Ops Manager)
- This will automatically direct the user to the login page of Identity Provider (CA Single Sign-On).
- Enter the credentials on the CA Single Sign-On Login page and click login
- User will be redirected to the Apps Manager Home page




SiteMinder Password Services
https sc5.casecurecenter.com/siteminderagent/certoptional/forms/login.fcc?TYPE
Reader
Sree
Apple
Disney
ESPN
Yahoo!
ca technologies
Please Login
Login

Username: smuser1

Password: •••••••



Note: If the user is logging in for the first time they are not associated with an any Organization or Space Role in Pivotal Cloud Foundry. After the user logs in once into Apps Manager or logs in via the Cloud Foundry command line (CF CLI) a shadow account is provisioned for them in Pivotal Cloud Foundry. The Pivotal Cloud Foundry Admnisrator needs to associate the user to the right role post creation of the shadown account. This is also via execution of role membership command like set-org-role and set-space-role via the CF CLI.

Single Logout

Not yet supported

Accessing various Pivotal Cloud Foundry Federation services

Please follow the steps below for Single Sign-On to Cloud Foundry Command Line Interface (CF CLI)

- Launch the command prompt and target the CF CLI to your Pivotal Cloud Foundry Deployment
  - cf target https://api.{system-domain}
- Perform cf login using the –sso option
  - cf login –sso

- This will display a URL for generating a One Time Password
- Copy the URL in the browser
- If you aleadry not authenticated, authenticate by Clicking on the CA Single Sign-On Identity provider link on the Login Page
- After completion of authentication a One Time Password will be displayed
- Copy the One Time Password and enter in the Command Prompt
- You will be logged into CF CLI

Chapter 5: Exception Handling

This section contains the following exceptions:

When the CA Single Sign-On Partnership is Inactive

When Service Provider Entity ID was misconfigured on the CA Single Sign-On Side

When Identity Provider Entity ID was misconfigured on the CA Single Sign-On Side

When Service Provider Assertion Consumer URL was misconfigured on the CA Single Sign-On Side

Audience Field was misconfigured on the CA Single Sign-On Side

Name ID Format values was misconfigured on the CA Single Sign-On Side

Expired certificate on the CA Single Sign-On Side

When Identity Provider Entity ID was misconfigured on the Pivotal Cloud FoundrySide

When Identity Provider SSO URL was misconfigured on the Pivotal Cloud Foundry Side

When Identity Provider SLO URL was misconfigured on the Pivotal Cloud Foundry Side

When Identity Provider Certificate was misconfigured on the Pivotal Cloud Foundry Side

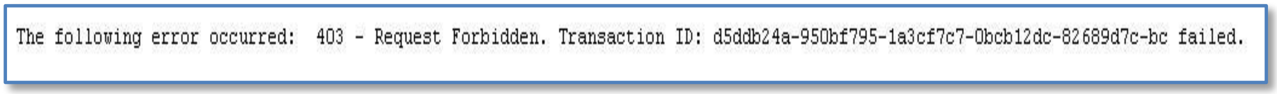
User who is not in the Pivotal Cloud Foundry trying to login through

CA Single Sign-On User who doesn't have desired attributes in the user store

Exception Cases

When the CA Single Sign-On Partnership is Inactive

When CA Single Sign-On Partnership is Inactive or not Defined, following error appears on browser



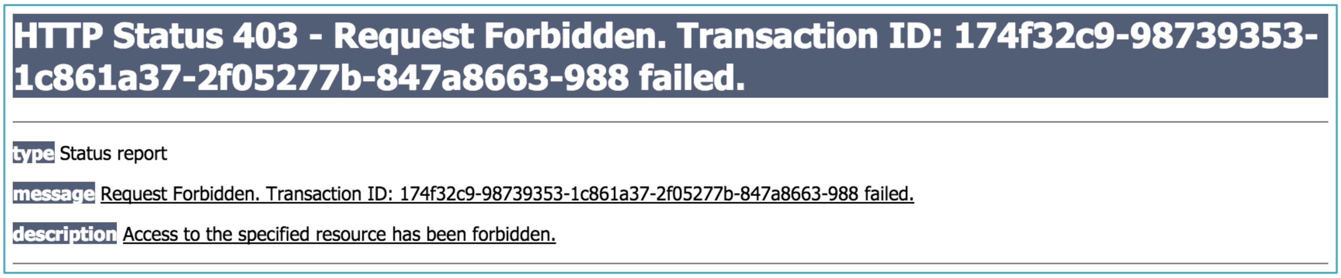
```
The following error occurred:  403 - Request Forbidden. Transaction ID: d5ddb24a-950bf795-1a3cf7c7-0bcb12dc-82689d7c-bc failed.
```

When Service Provider Entity ID was misconfigured on the CA Single Sign-On Side

Entity used → saml:entityid: http://login.blah.wild.cf-app.com

Result → Authentication at CA Single Sign-On fails and displays the error given below.

CA Single Sign-On error page is displayed on click of SSO Link



HTTP Status 403 - Request Forbidden. Transaction ID: 174f32c9-98739353-1c861a37-2f05277b-847a8663-988 failed.

type Status report

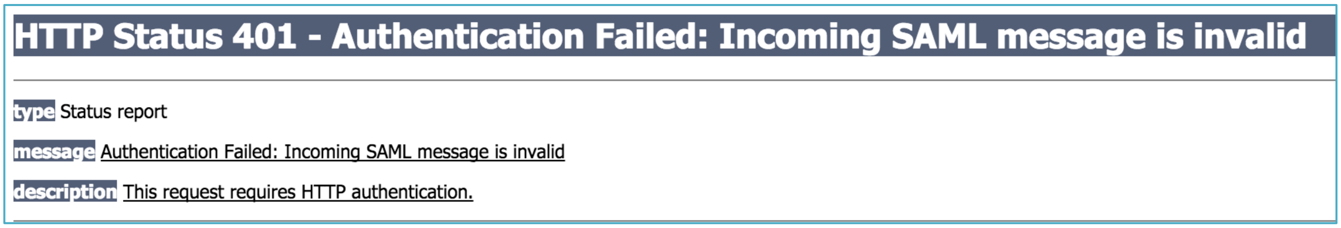
message Request Forbidden. Transaction ID: 174f32c9-98739353-1c861a37-2f05277b-847a8663-988 failed.

description Access to the specified resource has been forbidden.

When Identity Provider Entity ID was misconfigured on the CA Single Sign-On Side

Entity ID used →samlidp1

Result → Authentication at the <SaaS_Partner> fails and displays the error given below.



HTTP Status 401 - Authentication Failed: Incoming SAML message is invalid

type Status report

message Authentication Failed: Incoming SAML message is invalid

description This request requires HTTP authentication.

CA Single Sign-On Login Page Displayed

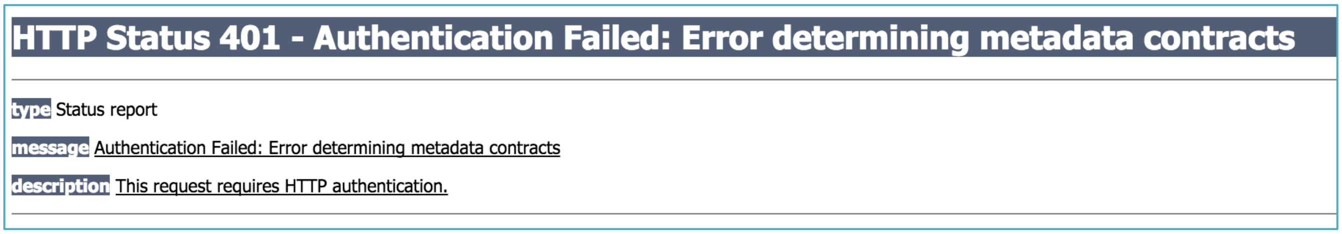
After Authenitcation Error displayed on SP side

Logs →

```
[2015-03-23 19:59:41.813] login - 12965 [http-bio-8080-exec-6] .... DEBUG --- MetadataCredentialResolver: Added 0 credentials resolved from metadata of entity smidp1

[2015-03-23 19:59:42.316] login - 12965 [http-bio-8080-exec-6] .... DEBUG --- SAMLProcessingFilter: Incoming SAML message is invalid

org.opensaml.ws.security.SecurityPolicyException: Validation of protocol message signature failed

    at org.opensaml.common.binding.security.SAMLProtocolMessageXMLSignatureSecurityPolicyRule.doEvaluate(SAMLProtocolMessageXMLSignatureSecurityPolicyRule.java:138)
```

When Service Provider Assertion Consumer URL was misconfigured on the CA Single Sign-On Side

ACS URL used →http://login.gorilla.wild.cf-app.com/saml/SSO/alias/login.blah.wild.cf-app.com



HTTP Status 401 - Authentication Failed: Error determining metadata contracts

type Status report

message Authentication Failed: Error determining metadata contracts

description This request requires HTTP authentication.

Result → Authentication at the Pivotal Cloud Foundry fails and displays the error given below.

Click on SSO Link -> Shows CA Single Sign-On Login Page. After Authenitcation -> Error Displayed on Cloud Foundry

Logs →

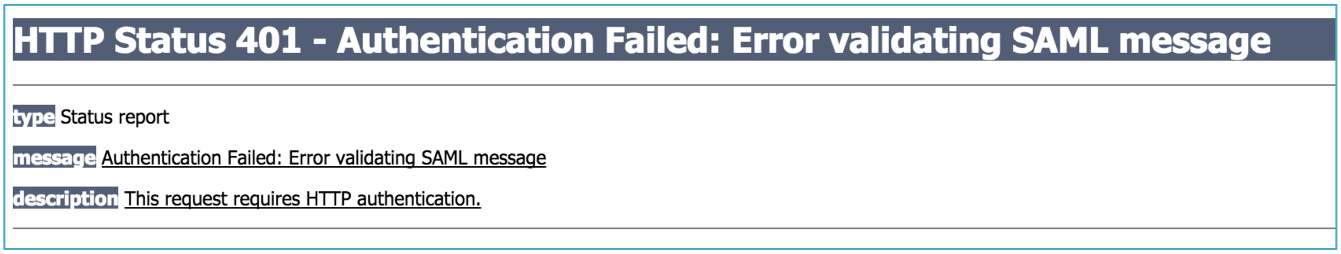
```
[2015-03-23 23:25:59.435] login - 12965 [http-bio-8080-exec-7] .... DEBUG --- SAMLProcessingFilter: Attempting SAML2 authentication using profile urn:oasis:names:tc:SAML:2.0:profiles:SSO:browser

[2015-03-23 23:25:59.436] login - 12965 [http-bio-8080-exec-7] .... DEBUG --- SAMLProcessingFilter: Error determining metadata contracts

org.opensaml.saml2.metadata.provider.MetadataProviderException: No local entity found for alias login.blah.wild.cf-app.com, verify your configuration.

	at org.springframework.security.saml.context.SAMLContextProviderImpl.populateLocalEntityId(SAMLContextProviderImpl.java:279)

	at org.springframework.security.saml.context.SAMLContextProviderImpl.getLocalEntity(SAMLContextProviderImpl.java:106)
```

Audience Field was misconfigured on the CA Single Sign-On Side

Audience used → http://login.blah.wild.cf-app.com

Result → Authentication at the Pivotal Cloud Foundry fails and displays the error given below.

Click on SSO Link -> Shows Single Sign-On Login Page. After Authenitcation -> Error Displayed on Cloud Foundry



HTTP Status 401 - Authentication Failed: Error validating SAML message

type Status report

message Authentication Failed: Error validating SAML message

description This request requires HTTP authentication.

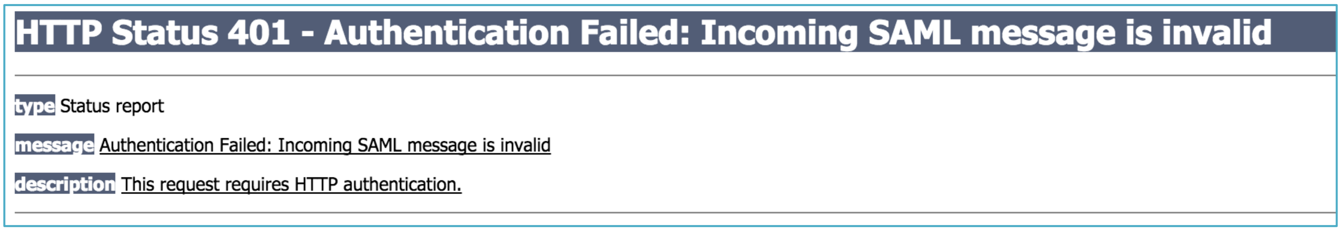
Logs →

```
[2015-03-23 23:38:16.316] login - 12965 [http-bio-8080-exec-8] ....  INFO --- SAMLDefaultLogger: AuthNResponse;FAILURE;10.80.16.46;http://login.gorilla.wild.cf-app.com;smidp;;;org.opensaml.common.SAMLException: Response doesn't have any valid assertion which would pass subject validation

    at org.springframework.security.saml.websso.WebSSOProfileConsumerImpl.processAuthenticationResponse(WebSSOProfileConsumerImpl.java:229)

    at org.springframework.security.saml.SAMLAuthenticationProvider.authenticate(SAMLAuthenticationProvider.java:82)
```

Name ID Format values was misconfigured on the CA Single Sign-On Side

Name ID Format used → Kerberos Principal Name

Result → Authentication at the <SaaS_Partner> fails and displays the error given below.



HTTP Status 401 - Authentication Failed: Incoming SAML message is invalid

type Status report

message Authentication Failed: Incoming SAML message is invalid

description This request requires HTTP authentication.

Logs →

```
[2015-03-23 23:49:06.966] login - 12965 [http-bio-8080-exec-1] .... ERROR --- BaseSAMLMessageDecoder: SAML message intended destination endpoint URI required by binding was empty

[2015-03-23 23:49:06.966] login - 12965 [http-bio-8080-exec-1] .... DEBUG --- SAMLProcessingFilter: Incoming SAML message is invalid

org.opensaml.xml.security.SecurityException: SAML message intended destination (required by binding) was not present

	at
org.opensaml.common.binding.decoding.BaseSAMLMessageDecoder.checkEndpointURI(BaseSAMLMessageDecoder.java:201)

	at
org.opensaml.saml2.binding.decoding.BaseSAML2MessageDecoder.decode(BaseSAML2MessageDecoder.java:72)
```

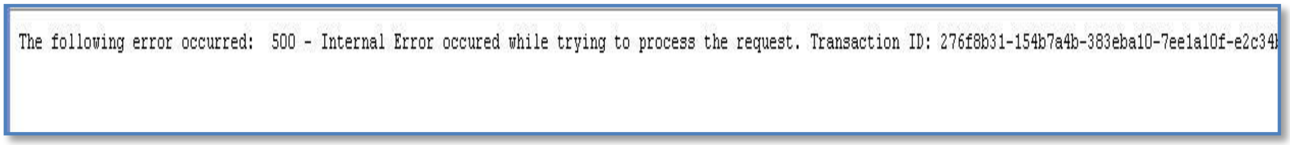
Expired certificate on the CA Single Sign-On Side

Condition – When CA Single Sign-On signing certificate is expired.

Log File Information appears to be like this →

```
<Response ID="_5e705c022c4ce8c6c8a5c39a057e3eb211d0" InResponseTo="fjedijkpiblphaigikhdieoilebpfaoibohmampl" IssueInstant="2012-12-27T13:29:00Z" Version="2.0" xmlns="urn:oasis:names:tc:SAML:2.0:protocol">

<ns1:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity" xmlns:ns1="urn:oasis:names:tc:SAML:2.0:assertion"></ns1:Issuer>

<Status>

<StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Responder"/>

<StatusMessage>Error Signing Assertion.</StatusMessage>

</Status>

</Response>
```

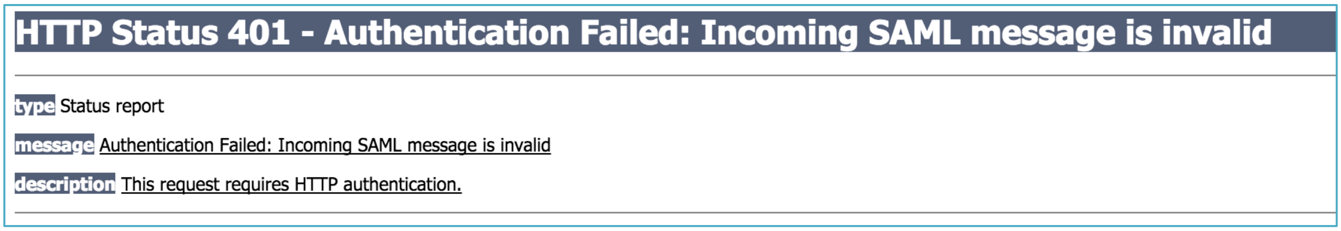
Message that appears on browser →



```
The following error occurred:  500 - Internal Error occured while trying to process the request. Transaction ID: 276f8b31-154b7a4b-383eba10-7ee1a10f-e2c34
```

When Identity Provider Entity ID was misconfigured on the Pivotal Cloud Foundry-Side

Identity Provider EntityID → samlidp1



HTTP Status 401 - Authentication Failed: Incoming SAML message is invalid

type Status report

message Authentication Failed: Incoming SAML message is invalid

description This request requires HTTP authentication.

Result → Authentication at the <SaaS_Partner> fails and displays the error given below.

[2015-03-24 00:41:27.185] login - 15186 [http-bio-8080-exec-2] .... DEBUG --- MetadataCredentialResolver: Added 0 credentials resolved from metadata of entity smidp

[2015-03-24 00:41:27.390] login - 15186 [http-bio-8080-exec-2] .... DEBUG --- SAMLProcessingFilter: Incoming SAML message is invalid

org.opensaml.ws.security.SecurityPolicyException: Validation of protocol message signature failed

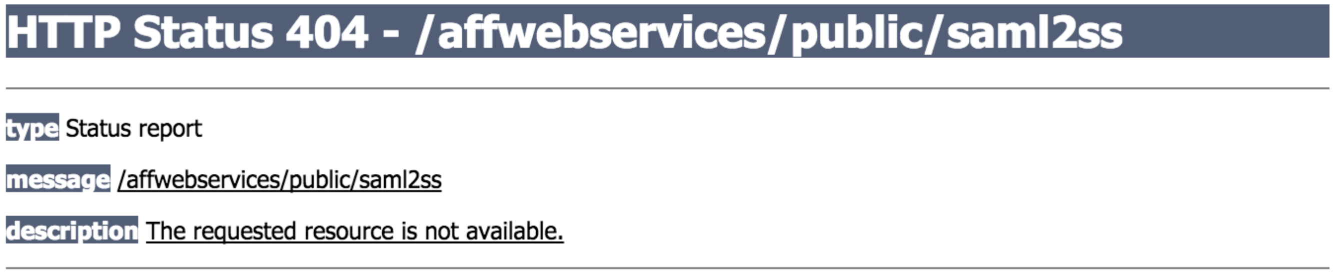
at org.opensaml.common.binding.security.SAMLProtocolMessageXMLSignatureSecurityPolicyRule.doEvaluate(SAMLProtocolMessageXMLSignatureSecurityPolicyRule.java:138)

at org.opensaml.common.binding.security.SAMLProtocolMessageXMLSignatureSecurityPolicyRule.evaluate(SAMLProtocolMessageXMLSignatureSecurityPolicyRule.java:107)

When Identity Provider SSO URL was misconfigured on the Pivotal Cloud Foundry Side

SSO URL used → https://sc5.casecurecenter.com/affwebservices/public/saml2ss

PCF Login Page -> Link Click -> Redirect to Error page on SM



HTTP Status 404 - /affwebservices/public/saml2ss

type Status report

message /affwebservices/public/saml2ss

description The requested resource is not available.

Result → Authentication at Pivotal Cloud Foundry fails and displays the error given below.

```
[2015-03-24 01:43:58.397] login - 16468 [http-bio-8080-exec-9] .... DEBUG --- ExceptionTranslationFilter: Authentication exception occurred; redirecting to authentication entry point

org.springframework.security.authentication.AuthenticationCredentialsNotFoundException: An Authentication object was not found in the SecurityContext

        at
org.springframework.security.access.intercept.AbstractSecurityInterceptor.credentialsNotFound(AbstractSecurityInterceptor.java:339)

        at
org.springframework.security.access.intercept.AbstractSecurityInterceptor.beforeInvocation(AbstractSecurityInterceptor.java:198)

        at
org.springframework.security.web.access.intercept.FilterSecurityInterceptor.invoke(FilterSecurityInterceptor.java:115)
```

When Identity Provider SLO URL was misconfigured on the Pivotal Cloud Foundry Side

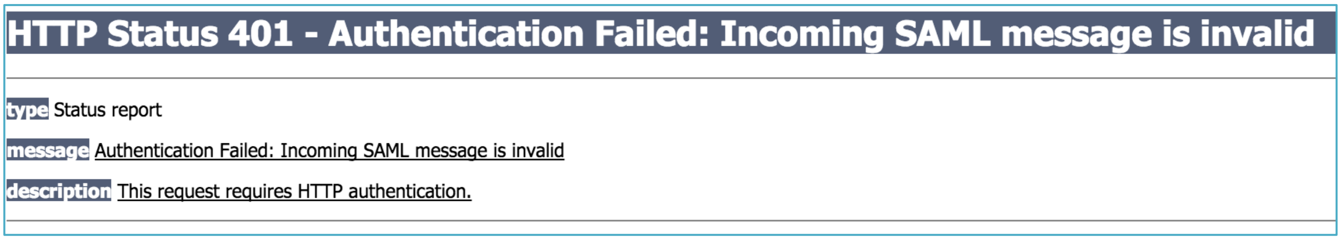
SLO is not supported

When Identity Provider Certificate was misconfigured on the Pivotal Cloud Foundry Side

After CA Single Sign-On Auth -> Error displayed

Identity Provider Certificate : Corrupted Value

Result → Authentication at the <SaaS_Partner> fails and displays the error given below.



HTTP Status 401 - Authentication Failed: Incoming SAML message is invalid

type Status report

message Authentication Failed: Incoming SAML message is invalid

description This request requires HTTP authentication.

Logs:

```
[2015-03-24 01:52:24.860] login - 17087 [http-bio-8080-exec-3] .... ERROR --- InlineX509DataProvider: Error extracting certificates from X509Data

java.security.cert.CertificateException: Unable to decode X.509 certificates

        at org.opensaml.xml.security.x509.X509Util.decodeCertificate(X509Util.java:354)

        at org.opensaml.xml.security.keyinfo.KeyInfoHelper.getCertificate(KeyInfoHelper.java:201)

        at org.opensaml.xml.security.keyinfo.KeyInfoHelper.getCertificates(KeyInfoHelper.java:176)

        at org.opensaml.xml.security.keyinfo.provider.InlineX509DataProvider.extractCertificates(InlineX509DataProvider.java:192)
```

User who is not in the Pivotal Cloud Foundry trying to login through CA Single Sign-On

This is not relevant for Pivotal Cloud Foundry. Users are provisioned just in time after successful authenitcation. However additional steps need to be perfomed by the Administrator to assign the user to the right set of roles.

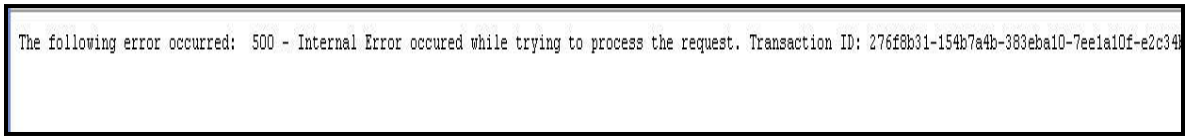
CA Single Sign-On User who doesn't have desired attributes in the user store

User ID used → feduser1

This user doesn't have the email id attribute which is the NameID Format used in the

Partnership.

Result → After authentication, following error page appears.



```
The following error occurred:  500 - Internal Error occured while trying to process the request. Transaction ID: 276f8b31-154b7a4b-383eba10-7ee1a10f-e2c34
```

Chapter 6: Summary

- Pivotal Cloud Foundry supports both Identity Provider and Service Provider-initiated scenario
- Pivotal Cloud Foundry services federation via Browser-SSO is tested
- No backchannel or artifact based profiles are implemented at Pivotal Cloud Foundry
- The SSO, assertion consumer and target URLs are all https
- This version of Pivotal Cloud Foundry Application does not support processing of SAML Assertion Attributes and Single Logout
- Signing of assertion & entire SAML response is supported
- The following services provided by Pivotal Cloud Foundry have been tested for desktop browser environment

  Pivotal Cloud Foundry Application Manager Console

  Pivotal Cloud Foundry Command Line Interface (CF CLI)