Cisco PingFederate Integration Guide for Salesforce.com

ATS-Security Services

Cisco IT DCPS ATS Security Services Team (asp-web-security@cisco.com)

Aakash Wasnik

Last Edited: 3/7/2013 11:05:10 AM

This document contains the necessary information to integrate Salesforce.com portal with Cisco-PingFederate infrastructure.

Table of Contents

1 *Introduction*

1.1 How to Use This Document

This document contains the necessary information to integrate Salesforce.com portal with Cisco-PingFederate infrastructure.

1.2 Benefits of using Cisco-PingFederate Infrastructure

- Cisco employees can use their CEC Credentials to login to Salesforce.com portal. They do not need to use separate credentials to login to Salesforce.com portal.
- In a browser, if Cisco employee already has session created with Enterprise authentication platform (Oracle Access Manager) then Cisco employee can seamlessly access Salesforce.com portal without having to login again. Single Sign on would happen for Cisco employee seamlessly & transparently.
- Cisco.com registered customer /partner / guest can also leverage the Cisco-PingFederate infrastructure as long as their account / access have been setup in the Salesforce.com portal.

1.3 Salesforce.com Use Cases

Following use cases are typically supported & implemented using Cisco-PingFederate Infrastructure.

Use Case Name	**Use Case Description**
End user accesses Salesforce.com portal URL in browser	End user can access bookmarked Salesforce.com URL / Salesforce.com portal's deep link URL / Salesforce.com's my domain URL
Access Salesforce.com Web Services programmatically (via non-browser)	Application needs to invoke / pull Salesforce.com data via Web Services
User Provisioning	User's account gets created in Salesforce.com via automated way.

1.4 Engagement Process to Initiate Project

ATS-Security Services team manages the PingFederate solution within Cisco enterprise environment. It is important to discuss the project timelines and integration effort required to setup the Single Sign on integration for particular Salesforec.com portal. Resource allocation & timelines needs to be fit into overall ATS – Security services Program Plan. To initiate the engagement process and to get more information please drop email to asp-web-security@cisco.com mentioning brief information about the project and its timelines.

2 Browser Based Use Cases

End user may access Salesforce.com URL in many ways. It serves as starting point or entry gate to initiate Salesforce.com portal session.

- Bookmarked Salesforce.com URL
- Deep link URL within Salesforce.com portal

If you need Single-Sign-On for any of the above mentioned scenarios "MyDomain-SAML" Setup is the recommended solution.

2.1 MyDomain-SAML Setup

2.1.1 My Domain Setup in SFDC

"My Domain" feature of Salesforce.com allows creating custom sub domain. This sub domain helps in creating "Easy-To-Remember" URL. For example: https://sales.my.salesforce.com is one such example of "My Domain" feature.

"My Domain" is a must requirement for SAML setup. "My Domain" URL acts as a unique SAML entity ID.

https://login.salesforce.com/help/doc/en/domain_name_overview.htm URL provides the detailed information about "My Domain" feature & how to enable it.

There are lots of benefits provided by "My Domain" feature apart from unique SAML entity ID. This feature should be thoroughly understood by the Cisco Business owner / Application Team / Specific group managing the Salesforce portal.

Important Note:

1. Cisco Business owner / Application Team / Specific group should take the ownership and responsibility of enabling the "My Domain" feature. It is expected that they understand this feature thoroughly.
2. If there is any issue with enabling "My Domain" Cisco Business owner / Application Team / Specific group should consult with Salesforce.com support team via opening the case.
3. Cisco-PingFederate team does not own this feature and therefore can only provide the necessary guidance.
4. Please review Section 2.2 – Hybrid Setup before deploying "My Domain" feature. Deploy refers to "Deploy to all users" step in "My Domain" configuration.

2.1.2 User Setup in SFDC

User's profile in Salesforce.com should have one of these attributes correctly configured. One of these attributes is used in Authentication process.

Federation ID: Federation ID is the attribute (in Salesforce.com user profile) populated with unique information from user's Cisco profile. For example: CEC ID / CCO ID is the unique identifier in user's Cisco profile. CEC ID / CCO ID can be specified as "Federation ID" in user's Salesforce.com profile. Please see screenshot mentioned in Section 5.3.

Username Format: Legitimate user must have user account in SFDC portal. "Username" is the required field in user's account. Format of the username should be ***<CEC ID / CCO ID>***@salesforce.com***.<text specific to project>*** *For example: awasnik@salesforce.com.sales in this example awasnik is CEC ID and "sales" is "text specific to project".*

2.1.3 Identity Provider (Cisco-PingFederate) Setup

Please send following information to engineer (from Cisco-PingFederate team) assigned to the project.

1. Username format
2. My Domain url *(Please note this information is case sensitive)*
3. Screen shot of the "Single Sign On Settings" page of Salesforce.com portal

a. ("Single Sign On Settings" page is located @ Setup -> Administration Setup -> Security Controls -> Single Sign On Settings OR search for "single sign on" in the Quick Search text box located on the left)
b. Please look at the screen shot provided in the next section.

4. (Required only for Salesforce.com customer & partner portal) If Single Sign On is configured for Salesforce.com customer or partner portal. Please send "Organization ID" & "Portal ID" as well.
   a. "Organization ID" is located at Setup -> Administration Setup -> Company Profile -> Company Information OR Search for "company information" in the Quick Search text box located on the left. Please look at the screenshot in Section 5.1
   b. "Portal ID" is located at Setup -> App Setup -> Customize -> Customer Portal -> Settings -> Select "Customer Portal" link. Please look at the screenshot in Section 5.2.

Engineer will complete the required setup in the PingFederate environment based on the information provided.

2.1.4 Single Sign on Settings in SFDC

Application owner / team managing the Salesforce.com portal is expected to do the following configuration in the Salesforce.com portal.

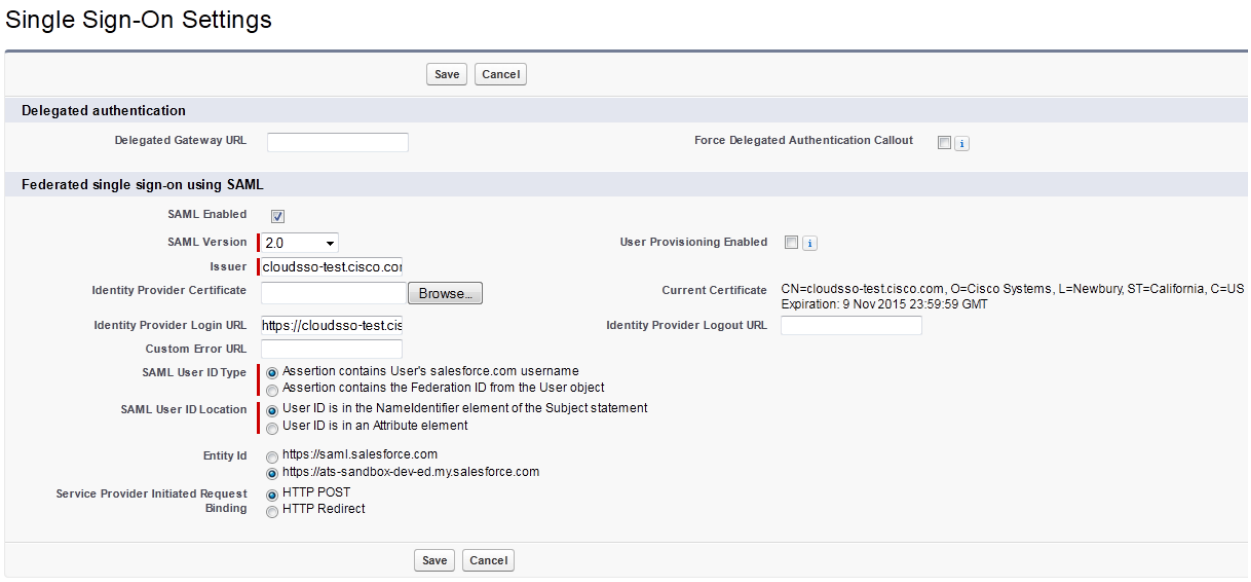
Please see below table for the information required to complete the "Single Sign On" configuration in Salesforce.com portal. Go to "Single Sign On Settings" page. ("Single Sign On Settings" page is located @ Setup -> Administration Setup -> Security Controls -> Single Sign On Settings OR search for "single sign on" in the Quick Search text box located on the left.

Parameter Name	Parameter Value	Description
SAML Enabled	Select the checkbox in front of this parameter.	Specifies if SAML is enabled for this Salesforce.com portal.
User Provisioning Enabled	DO NOT SELECT this checkbox. Keep the default.	This is related to Just-In-Time user provisioning capability.
SAML Version	Select "2.0" from the drop-down list.	Specifies SAML version.
Issuer	**For Stage Environment:** cloudsso-test.cisco.com **For Prod Environment:** cloudsso.cisco.com	Specified the unique identifier for the SAML setup at Identity Provider / Cisco-PingFederate.

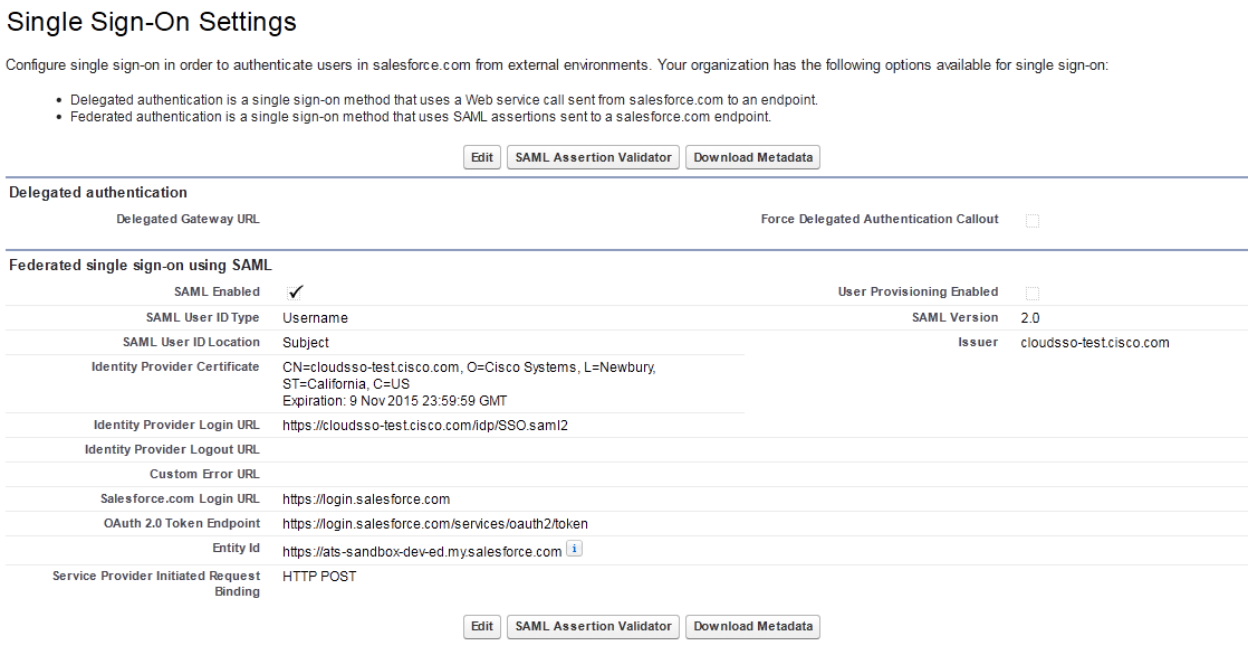
Identity Provider Certificate	**For Stage Environment:** https://cloudsso-test2.cisco.com/download/cloudsso-test.zip **For Prod Environment:** https://cloudsso-test2.cisco.com/download/cloudsso.zip	Specifies Certificate used for validating the Digital Signature of SAML assertion. Zip file contains the ".cer" file. Please upload the appropriate certificate as per environment.
Identity Provider Login URL	**For Stage Environment:** https://cloudsso-test.cisco.com/idp/SSO.saml2 **For Prod Environment:** https://cloudsso.cisco.com/idp/SSO.saml2	Specifies the URL where Single Sign On request / SAML request will be sent.
Identity Provider Logout URL	Please keep this field blank.	
Custom Error URL	Please keep this field blank.	
SAML User ID Type	Select "***Assertion contains User's salesforce.com username***" radio button.	Specifies that the SAML assertion will contain the username.
SAML User ID Location	Select "***User ID is in the NameIdentifier element of the Subject statement***" radio button.	Specifies the location of SFDC username in the SAML assertion.
Entity Id	Select the radio button in front of "My Domain URL". Do not Select https://saml.salesforce.com radio button.	Specifies unique identifier for SAML service at SFDC.
Service Provider Initiated Request Binding	Select "HTTP POST" radio button.	Specifies the communication channel used for SAL transactions.

Please see below screenshots for example configurations.

"Single Sign On Settings" in Edit mode:



"Single Sign On Settings" in Read-Only mode:



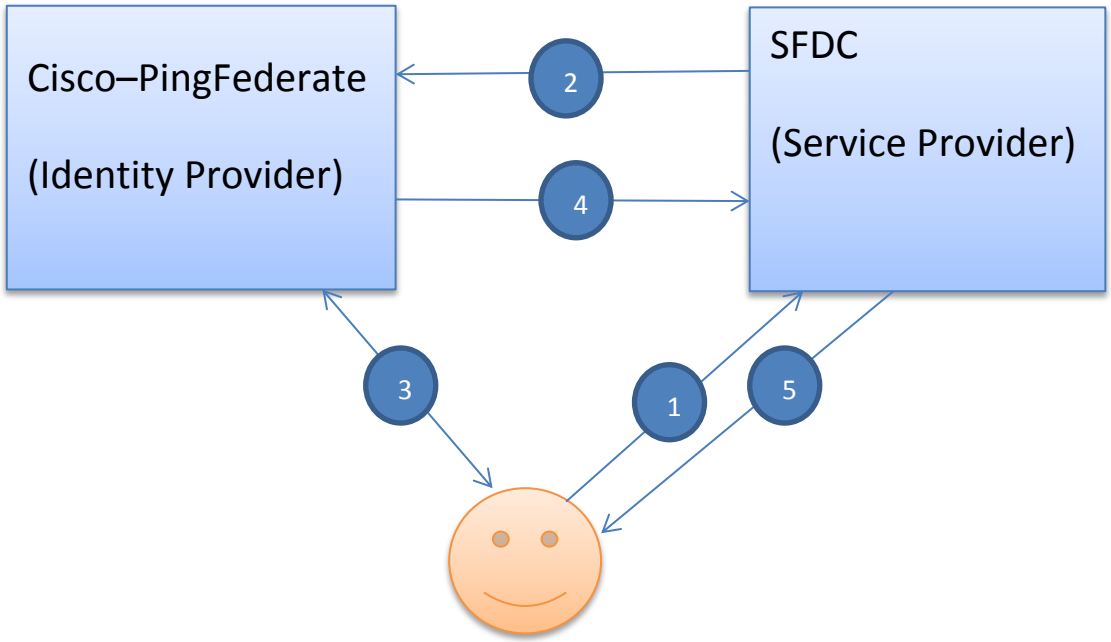
2.1.5 Testing

To test the SSO setup, please follow below steps.

1. Open a fresh browser (clear all the cookies if required) , access “My Domain URL”
2. You will be redirected to login page. Provide your CEC credentials.
3. On Successful authentication, you will see the Home page of the Salesforce.com portal.

If you get any error message, please contact engineer assigned to the project or send email to asp-web-security@cisco.com email alias.

2.1.6 Flow



Step 1: End user requests SFDC "My Domain URL" via browser.

Step 2: SFDC sends SAML request using HTTP POST mechanism to Cisco-PingFederate via browser.

Step 3: Cisco-PingFederate checks if the configuration for specific "My Domain" URL exists. If yes then it checks if end user has been previously authenticated and session exists. If end user has not authenticated before in same browser session, end user is presented with Login page. End user provides its credentials.

Step 4: Cisco-PingFederate creates the SAML assertion based on the end user's authenticated session & sends SAML assertion using HTTP POST mechanism via browser.

Step 5: SFDC validates the digital signature of the SAML assertion and checks if user account exists for the user in SFDC. If yeas end user is granted access to SFDC portal.

2.2 Hybrid Setup

Does your Salesforce.com portal needs to be accessed by Cisco Users as well as Non Cisco users (who uses separate credentials specific to Salesforce.com portal)?

If answer is yes then you would have to choose option of "NOT TO DEPLOY MY DOMAIN". This step would makes sure that specific Salesforce.com portal is accessed via My Domain URL (for Cisco users) & via Salesforce.com regular domain urls such as test.salesforce.com / login.salesforce.com (for non-cisco users).

3 Non-Browser Based Use Cases (SFDC Web Services)

SFDC web services are available to extract data programmatically. These web services are OAuth enabled. OAuth token needs to be sent along with web service request to get the appropriate response. Please look at the SFDC documentation for more information.

There are multiple ways to generate OAuth token. This section talks about only "SAML Assertion Flow".

3.1 SAML Assertion Flow

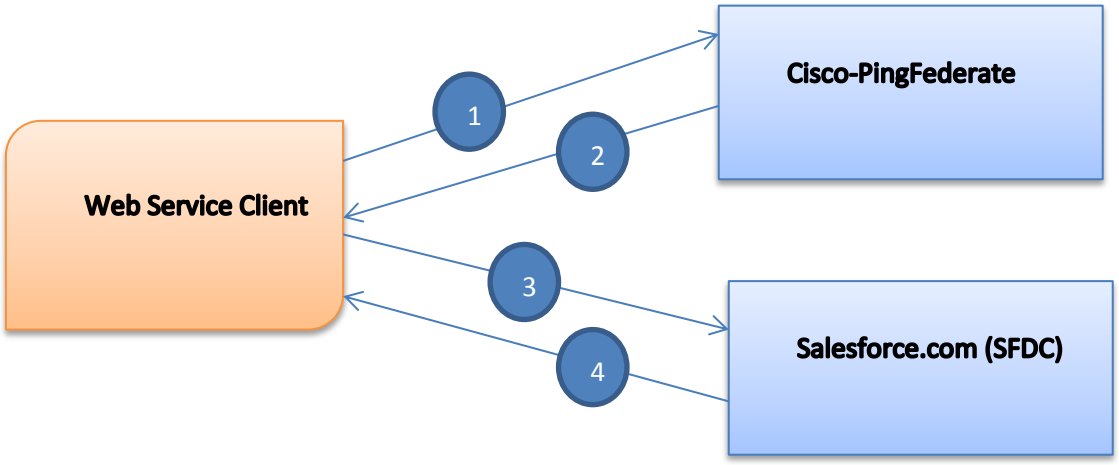
In this flow, Web Service Client receives SAML assertion from PingFederate which in turn sends it to SFDC OAuth token endpoint to receive OAuth Access Token.

3.1.1 Pre-requisite

Please see below pre-requisite required for implementing this flow.

1. Web Service Client should have access to User's session cookie (ObSSOCookie). Domain of this cookie is ".cisco.com".
2. MyDomain-SAML setup should be completed. Please refer to Section 2.1.
3. Cisco-PingFederate team will provide the IDP initiated SSO URL to be invoked from Web Service Client.

3.1.2 Flow Diagram



Step 1: Web Service Client sends User's session cookie (ObSSOCookie – represents User's authenticated session) to Cisco-PingFederate's ***IDP Initiated SSO URL***.

Step 2: Cisco-PingFederate validates the User's session cookie (ObSSOCookie) and responds back with HTML response containing SAML Assertion.

Step 3: Web Service Client has to extract the SAML Assertion from the HTML response and send the SAML assertion to ***SFDC OAuth 2.0 Token endpoint*** along with required parameters.

Step 4: SFDC validates the SAML assertion and sends back OAuth Access Token which can be used to invoke the SFDC Web Services.

3.1.3 Important URLs

IDP initiated SSO URL: Please contact asp-web-security team (asp-web-security@cisco.com) to get this URL.

SFDC OAuth 2.0 token endpoint: This url is mentioned on the "Single Sign on" settings page in SFDC instance. Go to "Single Sign On Settings" page. ("Single Sign On Settings" page is located @ Setup -> Administration Setup -> Security Controls -> Single Sign On Settings OR search for "single sign on" in the Quick Search text box located on the left. Please take a look at the screen shot of "Single Sign On" settings.

3.1.4 Sample Code

Please note this is a sample code and not production ready code. This code is provided only for PoC purpose. Application team should evaluate all the necessary error conditions / exception and incorporate them in the program code.

Sample code can be downloaded from below URL:

https://cloudsso-test2.cisco.com/download/BrowserSAMLSFDC.zip

3.1.5 SFDC Documentation

More information about this flow can be found at this SFDC URL. https://login.salesforce.com/help/doc/en/remoteaccess_oauth_web_sso_flow.htm

3.1.6 SFDC OAuth token – Expiry

SFDC OAuth Access Token is valid till Session timeout configured in SFDC portal. Default Access Token timeout is 2 hours whereas max timeout configurable is 12 hours. Session / Access token timeout can be set in SFDC portal @ Setup->Security Controls -> Session Settings

SFDC Refresh token is valid till it is explicitly revoked.

4 User Provisioning

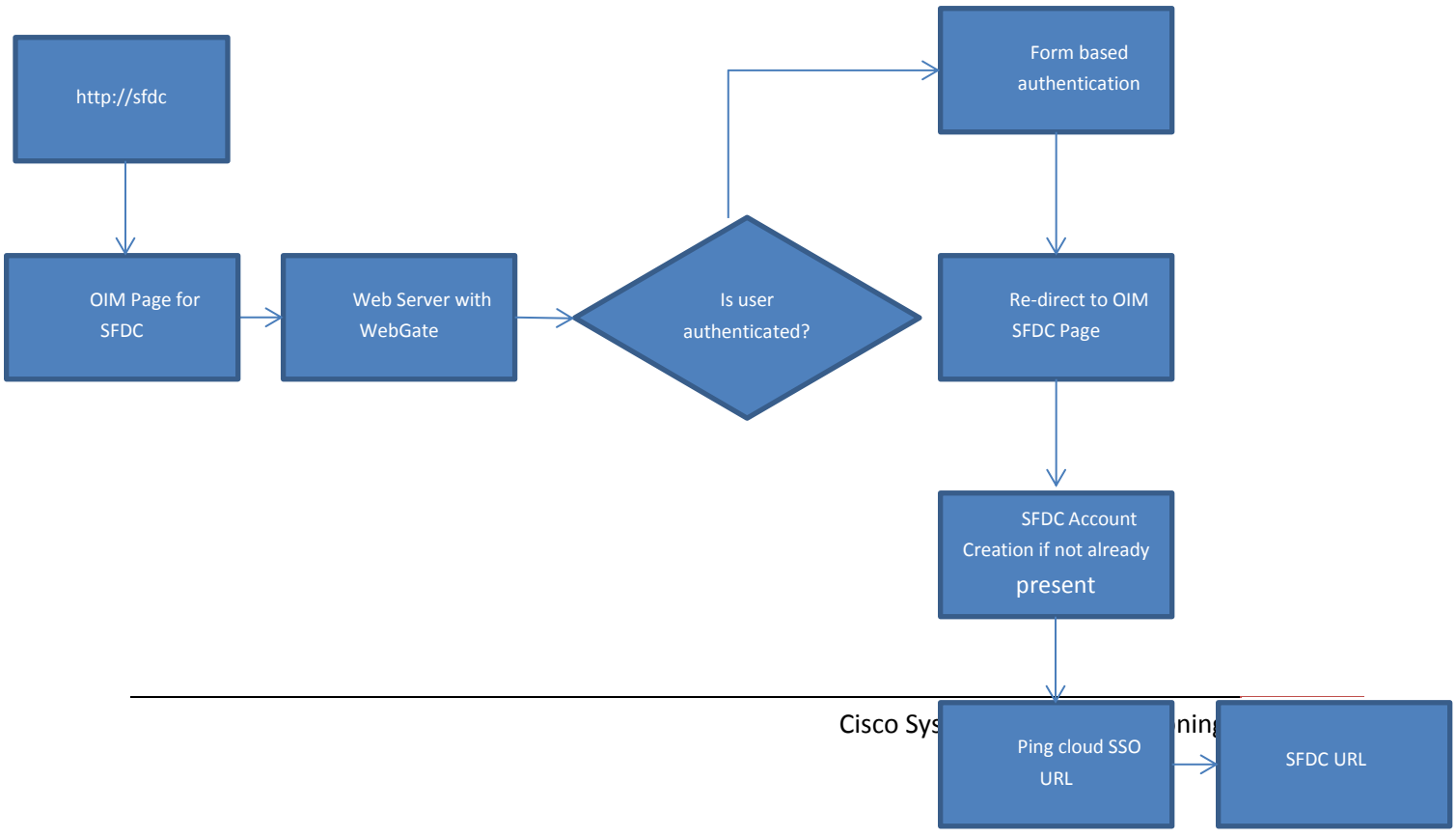
User provisioning is the process by which user's profile is created in Salesforce.com portal. There are multiple flows possible based on the requirements.

4.1 OIM – Oracle Identity Manager

Oracle Identity Manager (OIM) is the enterprise user provisioning solution. It offers features such as auditing, user provisioning, user de-provisioning. To get more information about OIM capabilities / user provisioning flows, please contact oim-team@cisco.com

4.1.1 Just-In-Time Provisioning

User account can be created in SFDC Just In Time, leveraging the OAM SSO flow and the OIM-OAM integration. Following flow illustrates the JIT provisioning:

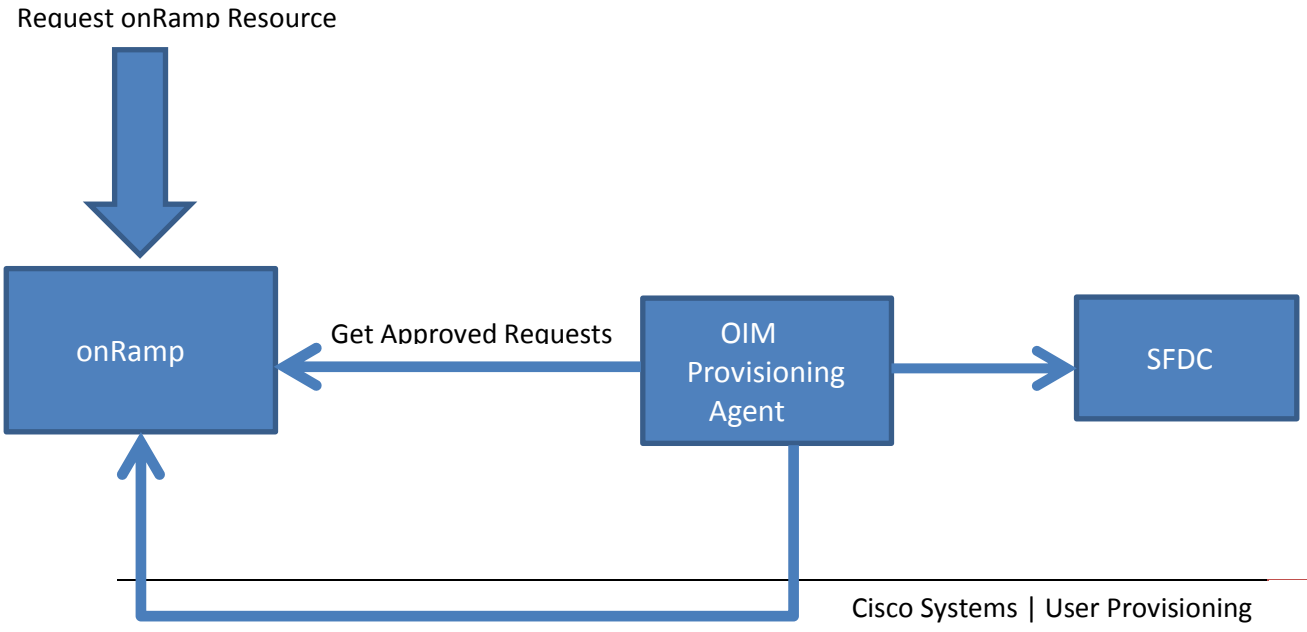


Following would be the execution steps:

1. Consumers can define a vanity url like http://sfdc or the flow can start with the OIM SFDC page
2. If a vanity URL is defined by the consumer, end user would start with the vanity URL. There would be a re-direct from the vanity URL http://sfdc to the OIM SFDC Page
3. The OIM SFDC page would be protected with OAM
4. If the user is not already authenticated, user would be re-directed to the standard SSO login page
5. After successful authentication a re-direct to the OIM SFDC page would happen and the OIM SFDC page would be served.
6. OIM page would check if the account for the user exists in SFDC. If account doesn't exist, OIM would create the account and then re-direct the flow to the Ping cloud SSO URL. If account exists OIM page would re-direct the flow to the Ping cloud SSO URL. SAML federation flow commences and the user is re-directed to the SFDC URL

4.1.2 Request-Based Provisioning

User account can also be pre-created in SFDC, leveraging the OIM-onRamp integration. In this case the user would need to request onRamp resource re-presenting the SFDC application. Once the request is approved, OIM provisioning agent would pick up the request and process it creating the user account in SFDC and closing the request in onRamp. Following is the flow for request based provisioning:



Close onRamp Request

4.2 Browser Based Just-In-Time Provisioning

In browser based Just-In-Time provisioning, user's profile is created during login process. Browser based login process is described in Section 2.1.6.

Information required to create user in Salesforce is passed in the SAML assertion. This information is referred as SAML attributes.

There are different User License types available in Salesforce.com portal. Each User license type required certain attributes to be passed in SAML assertion to create user in Salesforce.com portal.

4.2.1 Single Sign On Settings in SFDC

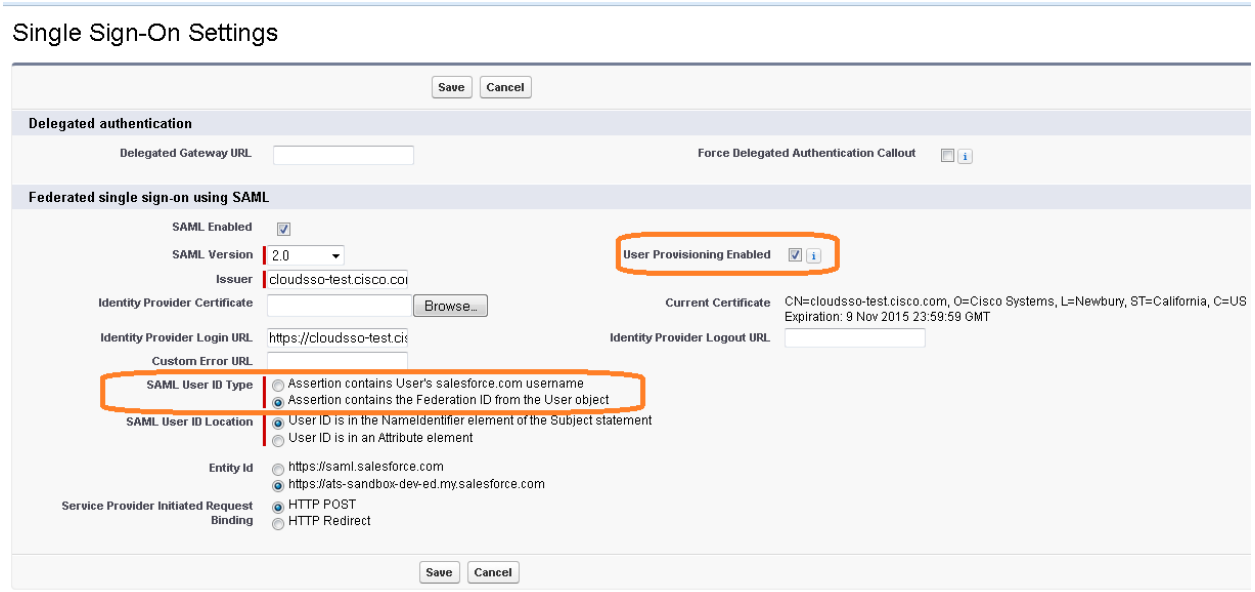
Below "Single Sign On Settings" in SFDC is required for Just-In-Time user provisioning. This configuration is required for both regular and portal user provisioning.

Go to "Single Sign On Settings" page. ("Single Sign On Settings" page is located @ Setup -> Administration Setup -> Security Controls -> Single Sign On Settings OR search for "single sign on" in the Quick Search text box located on the left.

Parameter Name	Parameter Value	Description
User Provisioning Enabled	SELECT this checkbox.	Specifies if Just-In-Time user provisioning capability is enabled.
SAML User ID Type	Select "***Assertion contains the Federation ID from the User Object***" radio button.	This is required for Just-In-Time user provisioning capability.

Apart from these two parameters, keep rest of the parameter's value as per Table mentioned in Section 2.1.4.

For reference please see below screenshot.



4.2.2 Regular User Provisioning

For Regular User provisioning via Just-In-Time provisioning method requires

1. "Single Sign On" settings mentioned in the Section 4.2.1
2. Attributes to be passed in SAML assertion is stated here https://na7.salesforce.com/help/doc/en/sso_jit_requirements.htm

4.2.3 Portal User Provisioning

For Portal User provisioning via Just-In-Time provisioning method requires

1. "Single Sign On" settings mentioned in the Section 4.2.1
2. Attributes to be passed in SAML assertion is stated here https://na7.salesforce.com/help/doc/en/sso_jit_portal_requirements.htm

4.3 Non-Browser Based Just-In-Time Provisioning

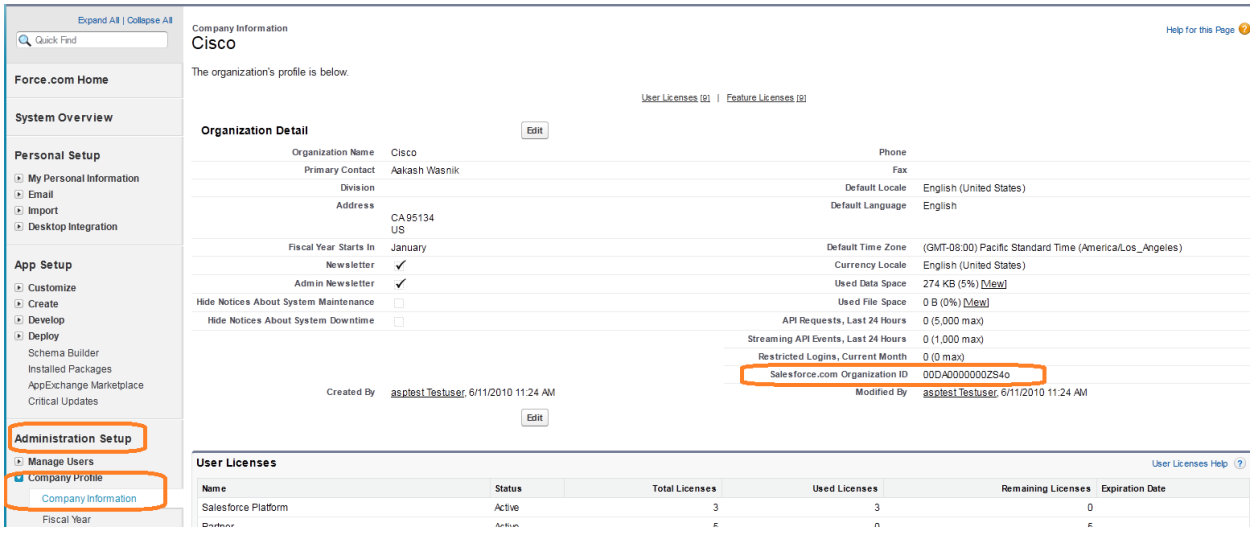
In non-browser based Just-In-Time user provisioning, user is created during non-browser call to SFDC OAuth Token endpoint. Non-browser call is typically initiated from web service client to get the OAuth Access token. This flow is described in the Section 3.1.2.

Just-In-Time user provisioning via non-browser call requires two important configurations.

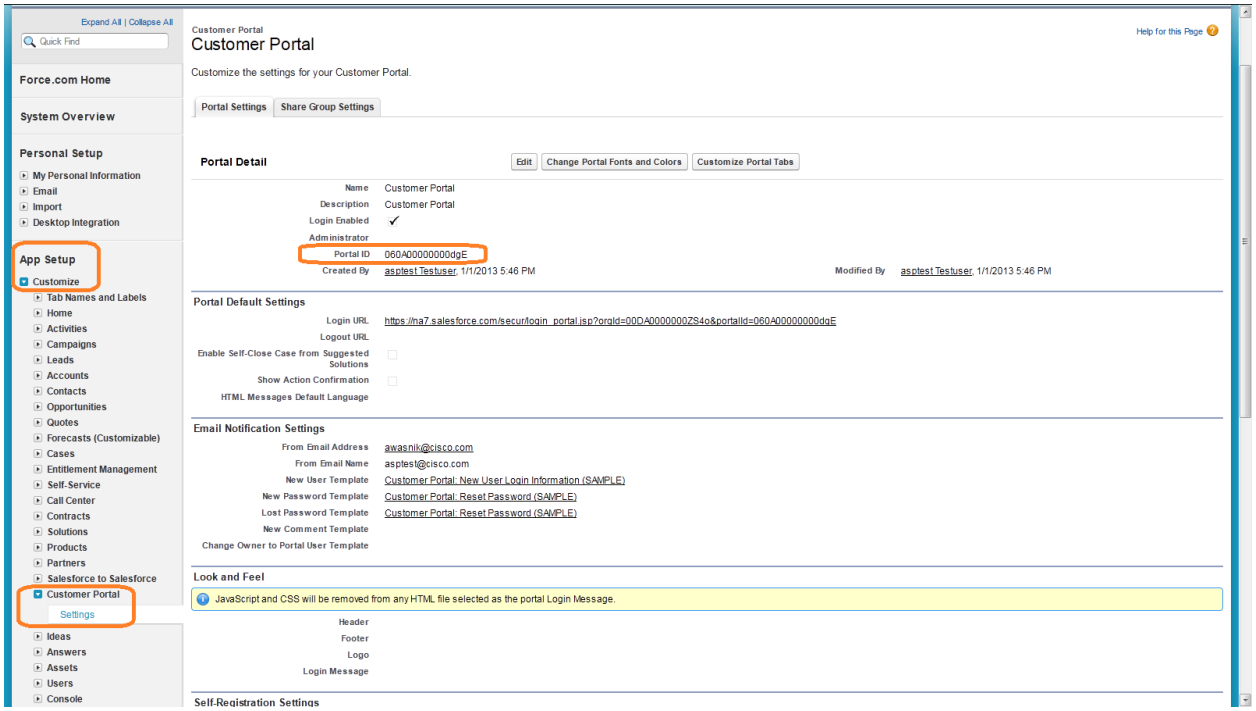
1. "Single Sign On" Settings is described in Section 4.2.1.
2. Based on "User license type" or Regular / Portal user required attributes needs to be sent in the SAML assertion. Information about attributes is mentioned in Section 4.2.2 & 4.2.3.

5 Appendix

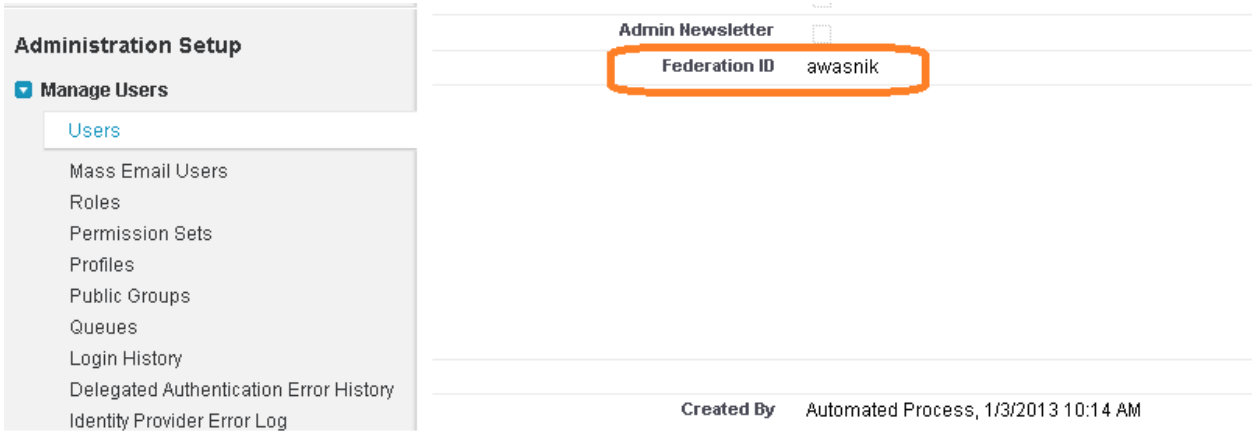
5.1 Organization ID – Screenshot



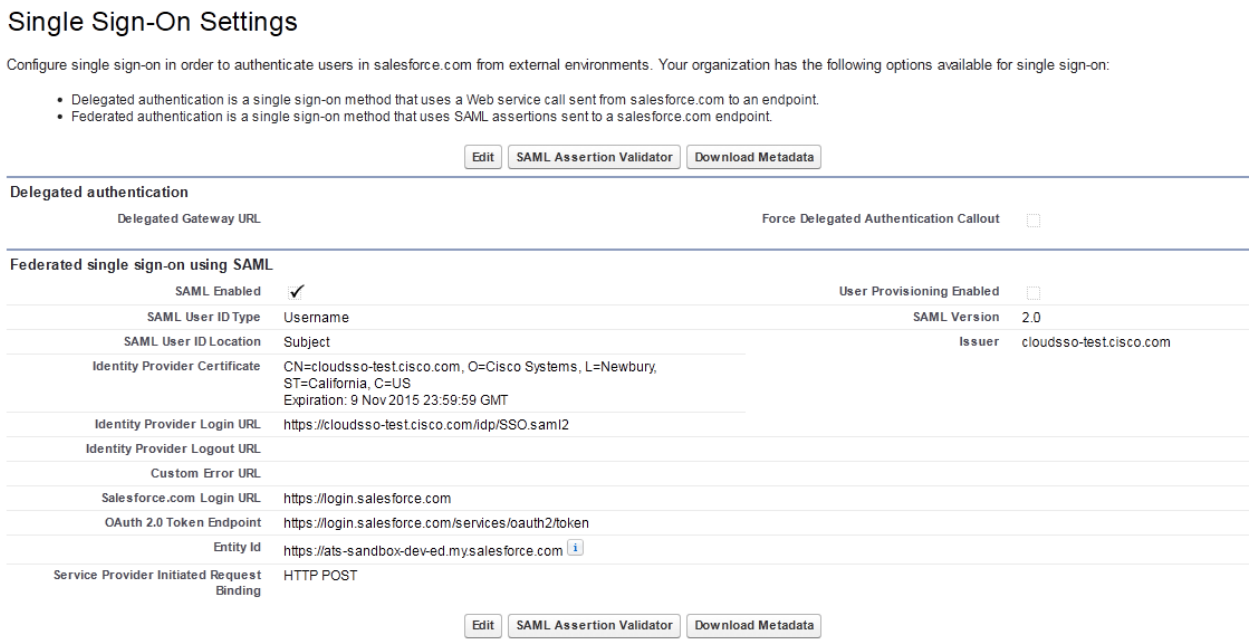
5.2 Portal ID – Screenshot



5.3 Federation ID – Screenshot



5.4 Single Sign On Settings



Single Sign-On Settings

Configure single sign-on in order to authenticate users in salesforce.com from external environments. Your organization has the following options available for single sign-on:

- Delegated authentication is a single sign-on method that uses a Web service call sent from salesforce.com to an endpoint.
- Federated authentication is a single sign-on method that uses SAML assertions sent to a salesforce.com endpoint.

Edit | SAML Assertion Validator | Download Metadata

Delegated authentication

Delegated Gateway URL		Force Delegated Authentication Callout	☐

Federated single sign-on using SAML

SAML Enabled	✓	User Provisioning Enabled	☐
SAML User ID Type	Username	SAML Version	2.0
SAML User ID Location	Subject	Issuer	cloudsso-test.cisco.com
Identity Provider Certificate	CN=cloudsso-test.cisco.com, O=Cisco Systems, L=Newbury, ST=California, C=US Expiration: 9 Nov 2015 23:59:59 GMT		
Identity Provider Login URL	https://cloudsso-test.cisco.com/idp/SSO.saml2		
Identity Provider Logout URL			
Custom Error URL			
Salesforce.com Login URL	https://login.salesforce.com		
OAuth 2.0 Token Endpoint	https://login.salesforce.com/services/oauth2/token		
Entity Id	https://ats-sandbox-dev-ed.my.salesforce.com		
Service Provider Initiated Request Binding	HTTP POST		

Edit | SAML Assertion Validator | Download Metadata

6 Revision History

Revision	Date	Revision Author	Reviewer / Approvers	Description
1.0	02-04-2012	Aakash Wasnik	Ranjan Jain	First Version of the Integration Document.